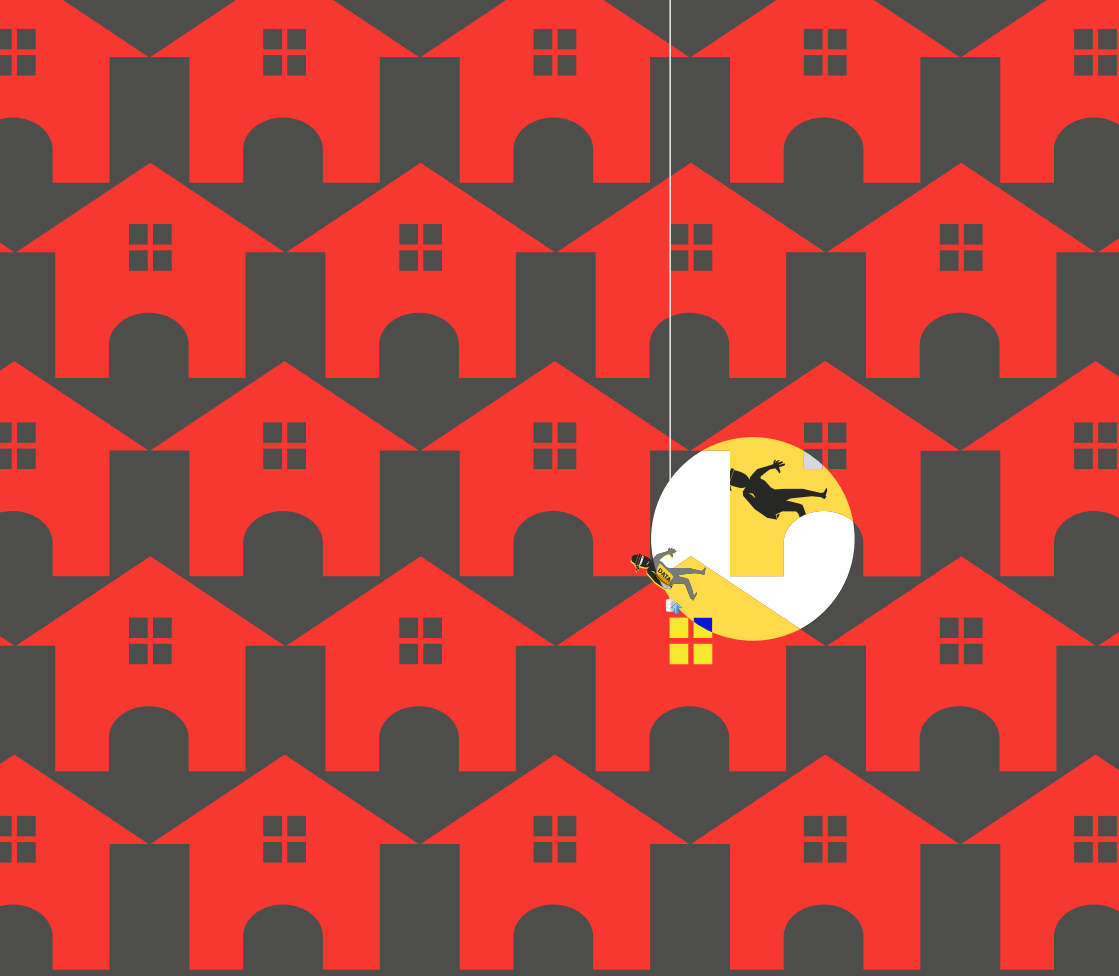


บทความเผยแพร่

CYBER SECURITY ARTICLES 2012

โดย

ThaiCERT

Thailand Computer Emergency Response Team

a member of ETDA

inner cover

บทความ Cyber Threats 2012
โดย ThaiCERT

ชื่อเรื่อง	บทความ Cyber Threats 2012 โดย ThaiCERT
เรียบเรียงโดย	นายสรณันท์ จิวะสุรัตน์, นายเสฏฐวุฒิ แสนนาม, นายไพชยนต์ วิมุกตะนันทน์, นายศุภกร ฤกษ์ดีถีพร, นายพรพรหม ประภากิตติกุล, นายเจษฎา ช้างสีสังข์, นายวิศัลย์ ประสงค์สุข, ธงชัย ศิลปวรางกูร และ ทีม ไทยเซิร์ต
พิมพ์ครั้งที่ 1	มกราคม 2556
พิมพ์จำนวน	1,500 เล่ม
ราคา	300 บาท

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย
(Thailand Computer Emergency Response Team)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ.
เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : 0-2142-2483 | โทรสาร : 0-2143-8071
เว็บไซต์ไทยเซิร์ต : www.thaicert.or.th | เว็บไซต์ สพธอ. : www.etda.or.th | เว็บไซต์กระทรวงฯ : www.mict.go.th

คำนำ

ศูนย์ประสานงานการรักษาความมั่นคงระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต ได้เริ่มดำเนินการภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มาตั้งแต่วันที่ 1 กรกฎาคม พ.ศ. 2554 โดยให้บริการรับแจ้งเหตุภัยคุกคามด้านสารสนเทศ และประสานงานกับหน่วยงานที่เกี่ยวข้องในการแก้ไขปัญหาที่ได้รับแจ้ง

ไทยเซิร์ตมีวิสัยทัศน์ให้สังคมออนไลน์มีความมั่นคงปลอดภัย เกิดความเชื่อมั่นกับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ และมีพันธกิจมุ่งเน้นการประสานงานกับหน่วยงานในเครือข่าย และหน่วยงานที่เกี่ยวข้องในการดำเนินการแก้ไขเหตุภัยคุกคามด้านสารสนเทศที่ได้รับแจ้ง

ไทยเซิร์ตมีพันธกิจเชิงรุกในการเพิ่มขีดความสามารถของทรัพยากรบุคคลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และมีกิจกรรมสร้างความตระหนักและพัฒนาทักษะความรู้ต่างๆ เช่น การซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ และการแลกเปลี่ยนและเผยแพร่ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามด้านสารสนเทศ

หนังสือเล่มนี้เป็นรวบรวมบทความที่ได้เผยแพร่ผ่านเว็บไซต์ของไทยเซิร์ต (www.thaicert.or.th) ในช่วงระยะเวลาวันที่ 1 ธันวาคม 2554 - 31 ธันวาคม พ.ศ. 2555 ซึ่งมีเนื้อหาสำหรับกลุ่มบุคคลทั่วไป และผู้ดูแลระบบสารสนเทศ ผู้จัดทำหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้ จะมีส่วนช่วยในการสร้างภูมิคุ้มกันให้กับสังคมออนไลน์ของประเทศไทย

สุรางคณา วายุภาพ

ผู้อำนวยการสำนักงานพัฒนาธุรกรรม
ทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สารบัญ

สารบัญรูป

เอกสารเผยแพร่ สำหรับผู้ใช้ทั่วไป

01 แนวทางการบริหารจัดการเครือข่ายไร้สายส่วนบุคคลกับภัยคุกคามที่เกี่ยวข้อง

ผู้เขียน: พรพรหม ประภากิตติกุล
วันที่เผยแพร่: 16 ธ.ค. 2554
ปรับปรุงล่าสุด: 25 ธ.ค. 2554

ปัจจุบันเทคโนโลยีเครือข่ายไร้สายหรือที่เรียกว่า Wireless Network เป็นที่แพร่หลายอย่างมาก ดังจะสังเกตเห็นได้ตามตรอกซอกซอย ซึ่งเป็นแหล่งที่พักอาศัยของบุคคลทั่วไป ก็จะพบว่าสามารถค้นเจอสัญญาณเครือข่ายไร้สายมากมาย ทั้งนี้คงเป็นเพราะเหตุผลของเทคโนโลยีทางด้านเครือข่ายไร้สายที่เจริญเติบโต ขึ้นอย่างรวดเร็วและงบประมาณที่ใช้ในการจัดตั้งจุดเชื่อมต่อเครือข่ายไร้สาย มีราคาถูกลงมาก รวมถึงอุปกรณ์ที่หาซื้อได้ง่ายและสามารถเรียนรู้วิธีการเพื่อจัดตั้งจุดเชื่อมต่อเครือข่ายไร้สายได้ไม่ยากเย็น จากข้อมูลที่มีอยู่มากมายบนอินเทอร์เน็ต ซึ่งวัตถุประสงค์ของการจัดตั้งเครือข่ายไร้สายเหล่านี้ส่วนหนึ่งคือตั้งใจ เพิ่มความสะดวกสบายให้กับผู้ใช้เทคโนโลยีพกพา เช่น โทรศัพท์มือถือ Smart Phone หรือเครื่องคอมพิวเตอร์โน้ตบุค สำหรับการเข้าถึงอินเทอร์เน็ต แต่ในความตั้งใจดังกล่าวอาจจะถูกเจือปนด้วยความไม่รู้ซึ่งนำไปสู่อันตราย ซึ่งแอบแฝงมากับจุดเชื่อมต่อของเครือข่ายไร้สายนั้นๆ เหตุที่กล่าวเช่นนี้ เพราะจากคุณลักษณะทางกายภาพของการใช้งานเครือข่ายไร้สายที่ เป็นการเชื่อมต่อสัญญาณผ่านตัวกลางที่เป็นคลื่นวิทยุ (Radio wave) ซึ่งไม่สามารถระบุได้ว่าใครบ้างที่กำลังทำอะไรกับเครือข่ายไร้สายของเราหรือ แม้จะตรวจสอบว่าผู้ที่กำลังเชื่อมต่ออยู่กับเครือข่ายไร้สายของเรานั้นอยู่ ที่พิกัดไหนก็ยังคงเป็นเรื่องยาก ซึ่งจะไม่ได้เหมือนการเชื่อมต่อสัญญาณผ่านสาย LAN (Local Area Network) ที่จะรู้ต้นสายปลายทางจากการเชื่อมต่อนั้นๆ ได้อย่างง่าย เพราะฉะนั้นการคิดจะจัดตั้งจุดเชื่อมเครือข่ายไร้สาย ควรต้องศึกษาข้อมูลให้ละเอียดถึงการทำงานในส่วนต่างๆ ข้อดี/ข้อเสียของอุปกรณ์แต่ละชนิด และสุดท้ายจำเป็นต้องรู้เท่าทันเหตุการณ์ที่อาจจะเกิดขึ้นในอนาคต เพื่อเตรียมพร้อมรับมือและทำให้เครือข่ายไร้สายของเรามีความมั่นคงปลอดภัยมากที่สุด โดยเอกสารฉบับนี้จัดทำขึ้นเพื่อให้ผู้ที่ต้องการให้บริการเครือข่ายไร้สาย ส่วนบุคคล (Private Wireless Network) หรือผู้ที่ให้บริการเครือข่ายไร้สายส่วนบุคคลอยู่แล้วก็ตาม ได้รับทราบถึงข้อมูลของภัยคุกคามและแนวทางในการบริหารจัดการเครือข่ายไร้สาย ให้มีความมั่นคงปลอดภัยมากที่สุด โดยรูปแบบการนำเสนอจะขออธิบายตามโครงสร้างข้อมูลดังต่อไปนี้

รูปแบบของการให้บริการเครือข่ายไร้สาย

สามารถจำแนกได้เป็น 2 ประเภทตามลักษณะการให้บริการ

- **ให้บริการในพื้นที่สาธารณะ (Public Wireless Network) โดยส่วนใหญ่จะเป็นผู้ให้บริการที่มีความเชี่ยวชาญและมีความรู้เฉพาะที่ เกี่ยวกับการให้บริการเครือข่ายไร้สายอยู่แล้ว เช่น True Wi-Fi, 3BB Hotspot, TOT Wi-Fi เป็นต้น โดยจะพบเห็นบริการไร้สายเหล่านี้ในพื้นที่สาธารณะส่วนใหญ่หรือในบางครั้งอาจ พบว่าตามสถานที่ราชการทั่วไปก็จะมีบริการเครือข่ายไร้สายของผู้ให้บริการต่างๆ เปิดให้บริการอยู่ ซึ่งการขอใช้บริการส่วนใหญ่จำเป็นต้องเปิดการให้บริการโดยการลงทะเบียนรับ เอกสารข้อมูลการยืนยันตัวตน เช่น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเข้าใช้งานต่อไป**
- **ให้บริการในพื้นที่ส่วนบุคคล (Private Wireless Network) เช่น ในบริเวณบ้าน หรือในบริเวณสำนักงานเล็กๆ เป็นต้น ซึ่งมีข้อสังเกตคือมักจะเป็นการให้บริการที่ไม่มีผลประโยชน์เข้ามาเกี่ยวข้อง คือไม่มีการคิดค่าบริการและขอบเขตการให้บริการค่อนข้างแคบหรือจำกัด ซึ่งหมายความว่าการให้บริการส่วนใหญ่จะเปิดให้ใช้งานเพื่ออำนวยความสะดวกให้ กลุ่มผู้ที่มีความเกี่ยวข้องด้วยโดยตรง เช่น เป็นบุคคลในครอบครัว หรือเป็นพนักงานในสำนักงานนั้นๆ เป็นต้น และการใช้งานจะครอบคลุมพื้นที่การใช้งานในระยะใกล้**

องค์ประกอบหลักของการใช้งานเครือข่ายไร้สาย

อุปกรณ์เชื่อมต่อสัญญาณอินเทอร์เน็ต เป็นอุปกรณ์หลักที่ทำหน้าที่เชื่อมต่อเครือข่ายอินเทอร์เน็ตหรือที่เรียกว่า โมเด็ม (Modem) โดยปัจจุบันพบว่ามีผู้ผลิตโมเด็มออกมาเพื่อรองรับการใช้งานเช่น Modem 56K, Modem ADSL, Modem 3G ซึ่งแต่ละมาตรฐานก็มีการรองรับความเร็วในการรับส่งข้อมูลแตกต่างกันไป

อุปกรณ์กระจายสัญญาณสำหรับเครือข่ายไร้สาย เป็นอุปกรณ์หลักที่ทำหน้าที่เป็นสถานีรับส่งข้อมูลผ่านเครือข่ายไร้สาย โดยบางครั้งจะเชื่อมต่อกับโมเด็มเพื่อทำให้สามารถรับส่งข้อมูลกับเครือข่าย อินเทอร์เน็ตได้ และสามารถตั้งชื่อของสถานีเครือข่ายไร้สาย (SSID) ดังกล่าวได้เอง ซึ่งอุปกรณ์ที่กล่าวถึงจะเรียกว่า Access Point [1-1] หรือในบางอุปกรณ์จะจับความสามารถของการเชื่อมต่อสัญญาณอินเทอร์เน็ตและความสามารถในการกระจายสัญญาณไร้สายรวมไว้ในอุปกรณ์เดียวกันแล้วเรียกว่าเป็น Wireless Modem Router ซึ่งปัจจุบันมีผู้ผลิตสินค้าออกมาหลายยี่ห้อหลายรุ่น โดยความแตกต่างของอุปกรณ์แต่ละรุ่นหรือยี่ห้อมักจะเป็นเรื่องการรองรับจำนวน การเชื่อมต่อสูงสุดที่อุปกรณ์สามารถรับได้ (บางรุ่นรองรับได้ที่ 10-15 การเชื่อมต่อ) รวมถึงความเร็วของการรับส่งข้อมูลบนเครือข่ายไร้สายที่แตกต่างกัน เช่น Wireless N จะรองรับความเร็วสูงสุดในการรับส่งข้อมูลที่ 300 Mbps ส่วน Wireless G จะรองรับความเร็วสูงสุดในการรับส่งข้อมูลที่ 54 Mbps เป็นต้น นอกจากนี้ คอมพิวเตอร์โน้ตบุ๊คหรือโทรศัพท์มือถือ Smart Phone รุ่นใหม่ๆ ยังสามารถปล่อยสัญญาณอินเทอร์เน็ตเพื่อทำหน้าที่เป็น Access Point ได้อีกด้วย

ซอฟต์แวร์บริหารจัดการเครือข่ายไร้สายเป็นหัวใจการของควบคุมการเข้าถึงเครือข่ายไร้สายให้มีความมั่นคงปลอดภัย โดยมีลักษณะการทำงานเป็นซอฟต์แวร์สำหรับตั้งค่าการใช้งานเครือข่ายไร้สาย เช่น การระบุเครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อมายังเครือข่ายไร้สายได้โดย ตรวจเช็คจากหมายเลข MAC Address (MAC Filter) การตั้งค่าชื่อเครือข่ายไร้สาย Service Set Identifier (SSID) การตั้งค่าการเข้ารหัสลับข้อมูลเพื่อการใช้งานเครือข่ายไร้สาย (Encryption) เป็นต้น โดยซอฟต์แวร์ดังกล่าวผู้ผลิตจะผนวกไว้ในอุปกรณ์กระจายสัญญาณไร้สาย ทำให้ไม่ต้องจัดหาหรือดูแลอุปกรณ์อื่น ๆ เพิ่มเติม

มาตรฐานการเข้ารหัสลับสัญญาณในเครือข่ายไร้สายรูปแบบต่างๆ

การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายถือเป็นเรื่องสำคัญ จึงมีผู้คิดค้นรูปแบบในการเข้ารหัสลับสัญญาณในเครือข่ายไร้สาย เพื่อป้องกันการดักรับข้อมูล (Sniff) และยังใช้เป็นแนวทางในการจำกัดสิทธิในการเข้าใช้งานเครือข่ายไร้สาย ซึ่งมาตรฐานที่นิยมใช้งานบนอุปกรณ์เชื่อมต่อไร้สายที่พบโดยทั่วไปมีดังนี้

WEP (Wired Equivalent Privacy) เป็นอัลกอริทึมในการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สายลำดับแรกที่พัฒนาขึ้น [1-2] ตามมาตรฐาน IEEE 802.11 ในช่วงปี คศ. 1999 ใช้ในการพิสูจน์ตัวตนโดยอาศัยหลักการแชร์กุญแจล่วงหน้า (Pre-shared Key) ผู้ใช้ทุกคนที่ใช้งานบนเครือข่ายจะต้องทราบกุญแจสมมาตร (Symmetric key) ที่จะใช้ [1-3] ซึ่งทุกคนที่เข้าใช้งานจะต้องได้รับกุญแจตัวเดียวกัน กุญแจมีขนาด 64 bit หรือ 128 bit (จะสังเกตได้ จากหน้าระบบบริหารจัดการเครือข่ายไร้สายจะให้เลือกว่าจะใช้งาน WEP 64 bit หรือ WEP 128 bit) โดยกุญแจดังกล่าวนอกจากจะใช้ในการยืนยันตัวตนแล้ว ยังถูกใช้ในการเข้าและถอดรหัสลับข้อมูลที่รับส่งภายในเครือข่ายด้วย ซึ่งวิธีการเช่นนี้เป็นช่องโหว่ให้ผู้โจมตีสามารถเจาะระบบเครือข่ายผ่านเทคนิคต่างๆ เช่น การใช้โปรแกรมดักรับข้อมูลที่รับส่งระหว่างอุปกรณ์ที่เชื่อมต่อแล้วนำมาวิเคราะห์เพื่อหากุญแจที่ใช้สำหรับเข้าระบบ ซึ่งสามารถ ทำได้ในเวลาอันรวดเร็ว ถึงแม้จะมีการใช้งานกุญแจขนาด 128 bit ซึ่งเป็นกุญแจขนาดใหญ่สุดแล้วก็ตาม [1-4] [1-5] ดังนั้นการป้องกันการเข้าถึงด้วยวิธี WEP จึงไม่เป็นที่นิยมในปัจจุบัน ต่อมาได้มีการพัฒนามาตรฐานเครือ ข่ายไร้สายแบบใหม่ขึ้นมา เพื่อเพิ่มความมั่นคงปลอดภัยให้มากขึ้น โดยมีชื่อเรียกของมาตรฐานดังกล่าวว่า IEEE 802.11i [1-6] ซึ่งมาตฐานดังกล่าวได้เพิ่มอัลกอริทึมการเข้ารหัสลับแบบใหม่ คือ WPA และ WPA2 WPA และ WPA2 (Wi-Fi Protected Access)

WPA คืออัลกอริทึมในการเข้ารหัสลับการเชื่อมต่อเครือข่ายไร้สายที่มีความมั่นคงปลอดภัยมากกว่า WEP มีกลไกการเข้ารหัสลับและถอดรหัสลับแบบ TKIP (Temporal Key Integrity Protocol) [1-7] โดยกุญแจที่ใช้ในการเข้าหรือถอดรหัสลับจะถูกเปลี่ยนแปลงโดยอัตโนมัติอยู่เสมอ ตามผู้ใช้งานแต่ละคนและกลุ่มข้อมูล (Packet) ที่มีการรับส่ง แต่อย่างไรก็ตามปัจจุบันพบว่าวิธีการเข้ารหัสลับด้วย WPA สามารถถูกเจาะได้โดยการดักข้อมูลที่รับส่งระหว่างอุปกรณ์และ Access Point ในระหว่างที่อุปกรณ์ดังกล่าวแลกเปลี่ยนกุญแจด้วยวิธีการทำ Handshake [1-8] [1-9] ดังนั้นจึงมีการพัฒนาเทคนิคการเข้ารหัสลับรูปแบบใหม่ขึ้นมาเรียกว่า WPA2 ซึ่งนอกจากรองรับ TKIP แล้วยังเพิ่มกลไกการเข้ารหัสลับที่มีความมั่นคงปลอดภัยมากขึ้น คือ CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) ซึ่งถูก

พัฒนามาจากมาตรฐาน AES (Advanced Encryption Standard) [1-10] โดยมีหลักการเบื้องต้นคือแบ่งข้อมูลออกเป็นส่วนๆ (Block) โดยแต่ละส่วนต้องมีขนาด 128 bit เป็นอย่างต่ำ จากนั้นใช้กุญแจขนาด 128 bit เข้ารหัสลับข้อมูลจนครบทุก Block ซึ่งการทำเช่นนี้จะแตกต่างจาก WEP และ WPA ที่ใช้การเข้ารหัสลับข้อมูลทั้งชุด (Stream) โดยจากการตรวจสอบข้อมูลจะเห็นได้ว่าการใช้กลไกการเข้ารหัสลับแบบ CCMP มีความมั่นคงปลอดภัยและยากต่อการโจมตีกว่าการใช้ WEP หรือ WPA [1-11] [1-12] ดังนั้นสำหรับผู้ดูแลเครือข่ายไร้สายทั่วไปแล้วในการเลือกรูปแบบการเข้ารหัสลับข้อมูลเพื่อป้องกันผู้โจมตี จึงควรตั้งค่ารหัสการเชื่อมต่อเครือข่ายไร้สายที่เป็น WPA2 ในโหมด AES ตามที่ได้กล่าวมาข้างต้น

ภัยคุกคามที่เกิดขึ้นกับการจัดตั้งบริการเครือข่ายไร้สาย

ภัยคุกคามจากซอฟต์แวร์ที่ใช้ในการบริหารจัดการเครือข่ายไร้สาย โดยซอฟต์แวร์ที่ทำงานผิดพลาดอาจส่งผลกระทบรุนแรงจนทำให้เกิดช่องโหว่ที่ผู้โจมตีสามารถเข้าถึงเครือข่ายไร้สายหรือเข้าควบคุมระบบการบริหารจัดการเครือข่ายไร้สายได้

ภัยคุกคามจากการใช้เทคนิคหลอกลวง โดยพบว่าผู้โจมตีจะสร้างสถานีเครือข่ายไร้สายเพื่อหลอกลวงผู้ใช้งานให้หลงเชื่อว่าเป็นเครือข่ายไร้สายชื่อเดียวกัน ซึ่งเมื่อผู้ใช้งานทำการกรอกรหัสผ่านเพื่อเข้าใช้งานก็จะทำให้ถูกดักรับ ข้อมูลได้ และจากนั้นผู้โจมตีจะนำรหัสผ่านดังกล่าวไปใช้งานต่อไป

ภัยคุกคามจากการโจมตีเครือข่ายไร้สายที่จัดตั้งขึ้น เกิดจากผู้ไม่หวังดีซึ่งสืบทราบถึงกระบวนการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สายที่จัดตั้งขึ้น และพยายามโจมตีเครือข่ายไร้สายดังกล่าวในลักษณะของการขโมยรหัสผ่านโดยวิธีการและอุปกรณ์ที่หาซื้อได้ตามทั่วไป ยกตัวอย่างเช่น การประมวลผลเพื่อแกะรอยรหัสผ่านของการเข้ารหัสลับสัญญาณแบบ WEP

ภัยคุกคามจากการตั้งค่าเครือข่ายไร้สายอย่างไม่ถูกวิธี เกิดจากผู้จัดตั้งเครือข่ายไม่มีความรู้ความเข้าใจในการจัดตั้งเครือข่ายไร้สาย จนทำให้ผู้โจมตีสามารถเข้าถึงเครือข่ายไร้สายได้อย่างง่ายดาย เช่น ผู้ดูแลเครือข่ายไร้สายไม่ตั้งค่าโหมดการยืนยันรหัสผ่านไว้ ทำให้บุคคลใดก็ตามที่ค้นพบสัญญาณเครือข่ายไร้สายดังกล่าวสามารถเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตได้ทันที

ภัยคุกคามจากการบอกรหัสผ่านผู้อื่นสำหรับเข้าใช้งานเครือข่ายไร้สายได้ การให้รหัสผ่านกับผู้อื่นในการเข้าใช้งานเครือข่ายไร้สาย ถือเป็นความเสี่ยงอย่างรุนแรง เนื่องจากผู้ดูแลเครือข่ายไร้สายเอง จะไม่ทราบเลยว่าผู้ใช้งานคนนั้นได้ใช้งานเครือข่ายไร้สายที่จัดตั้งขึ้นในทางที่ผิดอย่างไรบ้าง เช่น ผู้ใช้งานอาจใช้งานอินเทอร์เน็ตเพื่อโพสต์ข้อความหมิ่นประมาทผู้อื่น ผู้ใช้งานนำข้อมูลรหัสผ่านนี้ไปบอกต่อแก่บุคคลอื่น หรือแม้กระทั่งผู้ใช้งานมีความพยายามจะขโมยข้อมูลหรือลักลอบเข้าไปในระบบบริหารจัดการเครือข่าย เพื่อให้ได้สิทธิ์ในการควบคุมเครือข่ายไร้สายดังกล่าว ซึ่งหากเป็นเพียงการโจมตีภายในอาจพบว่าสามารถแก้ไขได้ไม่ยาก แต่หากพบว่าเป็นการใช้งานต่อสาธารณะในความผิดที่ต้องได้รับโทษทางกฎหมาย ก็จะทำให้ผู้ดูแลเครือข่ายไร้สายหรือผู้เช่าใช้งานอินเทอร์เน็ตบนเครือข่ายไร้สายนั้นๆ ต้องกลางเป็นผู้รับผิดชอบแทนในฐานะ

ที่เป็นผู้กระทำความผิด โดยส่วนใหญ่ อุปกรณ์เครือข่ายไร้สายส่วนบุคคลจะไม่สามารถจัดเก็บข้อมูลบันทึกการใช้งาน (Log) ไว้ในตัวอุปกรณ์

ข้อแนะนำสำหรับการให้บริการเครือข่ายไร้สายในพื้นที่ส่วนบุคคล

- **เลือกซื้ออุปกรณ์การเชื่อมต่อสำหรับเครือข่ายไร้สายจากผู้ผลิตที่มีความน่าเชื่อถือ โดยสังเกตสัญลักษณ์คำว่า Wi-Fi CERTIFIED ดังรูปที่ 1 (1-1) และมีข้อมูลฟังก์ชั่นการใช้งานประกอบเพื่อเป็นข้อมูลในการตัดสินใจเลือกซื้อ รวมถึงเพื่อให้สามารถวางแผนการให้บริการเครือข่ายไร้สาย และกำหนดความต้องการสำหรับการตั้งค่าการเข้าถึงต่างๆได้**

รูปที่ 1 (1-1) WI-FI CERTIFIED [1-13]

- **อัพเดทซอฟต์แวร์ (Firmware) ส่วนที่ใช้ในการบริหารจัดการเครือข่ายไร้สายให้ใหม่อยู่เสมอ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการค้นพบช่องโหว่ต่างๆ ในซอฟต์แวร์เวอร์ชั่นที่ใช้งาน หรือในบางครั้งการอัพเดทซอฟต์แวร์ทำให้สามารถขยายความสามารถบางอย่างของการบริหารจัดการ เช่น ทำให้สามารถใช้งานการเข้ารหัสลับสัญญาณของเครือข่ายไร้สายแบบ WPA ได้เพิ่มเติม จากเดิมที่มีให้เลือกใช้เพียง WEP**
- **เปิดการให้บริการ Firewall เพื่อป้องกันการบุกรุกจากภายนอกเครือข่าย การตั้งค่ารหัสผ่านหรือ Passphrase ในการเข้าใช้งานระบบเครือข่ายไร้สายควรตั้งค่าให้มีความยาวมากกว่า 20 ตัวอักษร และไม่สื่อถึงคำที่อยู่ในพจนานุกรม เพื่อป้องกันการคาดเดาหรือสุ่มรหัสผ่านในการเข้าใช้งานเครือข่ายไร้สาย [1-14]**
- **เปิดโหมดการยืนยันรหัสผ่านในการเชื่อมต่อเครือข่ายไร้สาย โดยแนะนำใช้เลือกใช้งานการเข้ารหัสลับสัญญาณแบบ WPA2 และ เข้ารหัสลับข้อมูลด้วย AES รวมถึงต้องไม่ใช้การเข้ารหัสลับสัญญาณแบบ WEP โดยเด็ดขาด เนื่องจากปัจจุบันพบว่าผู้ไม่หวังดีสามารถโจมตีเครือข่ายที่ใช้การเข้ารหัส ลับสัญญาณแบบ WEP เพื่อแกะรอยรหัสผ่านได้โดยง่าย**
- **ปรับแก้ไขค่าตั้งต้นในส่วนต่างๆที่ใช้ในการบริหารจัดการเครือข่ายไร้สายสาธารณะ เพื่อป้องกันการพยายามโจมตีด้วยค่ากรอกตั้งต้นจากโรงงานผู้ผลิต โดยมีการตั้งค่าที่ควรปรับปรุงดังนี้**

- o รหัสผ่านของระบบบริหารจัดการเครือข่ายไร้สาย ซึ่งโดยปกติจะมีการตั้งค่ามาจากโรงงานผู้ผลิต จึงควรจำเป็นต้องเปลี่ยนแปลง เพื่อป้องกันการคาดเดาหรือสุ่มรหัสผ่านในการเข้าถึงหน้าการตั้งค่า
- o ชื่อ SSID ของเครือข่ายไร้สาย ซึ่งในบางครั้งการใช้ค่าตั้งต้นที่มาจากโรงงานผู้ผลิตอาจทำให้สื่อถึงตัวผลิตภัณฑ์ได้ในทันที [1-15] โดยอาจถูกใช้เป็นข้อมูลสนับสนุนสำหรับผู้โจมตีเครือข่ายได้ง่ายขึ้น
- o ปิดโหมดการเผยแพร่สถานีกระจายสัญญาณของเครือข่ายไร้สายหรือที่เรียกว่า Broadcast SSID เพื่อป้องกันบุคคลทั่วไปสามารถเห็นสถานีเครือข่ายไร้สายได้โดยง่าย

- **ใช้งานฟังก์ชั่นการทำงานการคัดกรองผู้ใช้งานจากหมายเลข MAC Address ของเครื่องผู้ใช้งานหรือที่เรียกว่า MAC Address Filter เพื่อจำกัดการเข้าใช้งานเฉพาะผู้ใช้งานที่ได้รับอนุญาติเท่านั้น**
- **ปิดการใช้งานของ DHCP Server ในการกำหนดหมายเลข IP Address ให้แก่เครื่องที่เชื่อมต่อเครือข่ายไร้สาย โดยให้กำหนดเป็น Static IP ที่เครื่องผู้ใช้งานเอง เพื่อป้องกันผู้ไม่หวังดีลักลอบเข้าถึงเครือข่ายไร้สายได้อย่างง่ายดาย โดยหากสามารถเจาะรหัสผ่านในการเชื่อมต่อกับเครือข่ายไร้สายได้ แต่ก็จำเป็นต้องคาดเดากลุ่มของ IP Address เป้าหมายอีกชั้นหนึ่ง**

ปิดการใช้งาน Remote login ซึ่งเป็นฟังก์ชั่นการทำงานเพื่อเรียกใช้หน้าระบบบริหารจัดการเครือข่ายไร้สายจากเครือข่ายภายนอก เพื่อเป็นการป้องกันการโจมตีด้วยการสุ่มรหัสผ่านมายังอุปกรณ์กระจายสัญญาณโดยตรง เนื่องจากพบว่ามีโอกาสสูงที่ผู้โจมตีจะใช้ข้อมูลการตั้งค่าเริ่มต้นของอุปกรณ์นั้นๆ ในการพยายามล็อกอินเพื่อเข้าควบคุมระบบบริหารจัดการเครือข่ายไร้สาย โดยหากพบว่ามีความจำเป็นต้องเปิดการใช้งาน Remote Login ก็ให้ระบุถึงหมายเลข IP Address ของผู้ใช้งานที่จะเข้าถึงบริการดังกล่าว

หากพบว่ามีความผิดปกติในระบบบริหารจัดการเครือข่ายไร้สาย เช่น การตั้งค่าต่างๆ มีความเปลี่ยนแปลงไป หรือพบว่ามีผู้ใช้งานที่ไม่รู้จักเข้ามาเชื่อมต่อเครือข่ายไร้สายที่ดูแลอยู่ (โดยปกติอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายทั่วไปจะมีหน้าสำหรับตรวจสอบการ เชื่อมต่อจากผู้ใช้งานอยู่ โดยอาจจะแสดงข้อมูลเป็นหมายเลข MAC Address หรือข้อมูลชื่อเครื่องคอมพิวเตอร์ที่ทำการเชื่อมต่อ) ให้รีบเปลี่ยนรหัสผ่านสำหรับการเข้าสู่หน้าบริหารจัดการและควรเปลี่ยนการ ตั้งค่าดังที่กล่าวมาทั้งหมดใหม่ เพื่อลดความเสี่ยงที่จะถูกนำเครือข่ายไร้สายดังกล่าวไปใช้ในทางที่ผิด

ควรเปลี่ยนแปลงรหัสผ่านของผู้ดูแลเครือข่ายไร้สายในระบบบริหารจัดการเครือข่ายไร้สายและรหัสผ่านในการเข้าถึงเครือข่ายไร้สายทุกๆ 6 เดือน เพื่อป้องกันความผิดพลาดที่อาจถูกผู้ประสงค์ร้ายขโมยข้อมูลรหัสผ่าน เพื่อใช้ในการเข้าถึงเครือข่ายไร้สายหรือควบคุมเครือข่ายไร้สายนั้นๆ

อ้างอิง

[1-1] http://en.wikipedia.org/wiki/Wireless_access_point

[1-2] http://ezinearticles.com/?Wireless-Network-Encryption-Standards&id=124796

[1-3] http://sammana3.googlecode.com/svn/trunk/การเปรียบเทียบการใช้งานระบบเข้ารหัสแบบWEPและWPA.doc

[1-4] http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack

[1-5] http://blog.anidear.com/2010/09/hack-wireless-wep.html

[1-6] http://en.wikipedia.org/wiki/IEEE_802.11i-2004

[1-7] http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

[1-8] http://airodump.net/capturing-wpa-psk-handshake/

[1-9] http://www.aircrack-ng.org/doku.php?id=cracking_wpa

[1-10] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[1-11] http://www.mindterra.com/blog/?p=42

[1-12] http://www.maxi-pedia.com/WPA+WPA2+WiFi+protected+access

[1-13] http://www.mobicom.com.tr/pinfo.asp?pid=7

[1-14] http://technicallyeasy.net/2010/12/why-the-length-of-the-wpa-passphrase-is-important

[1-15] http://compnetworking.about.com/od/wirelessrouters/ss/router_ssid.htm

02 ชื่อไวรัสคอมพิวเตอร์บ่งบอกอะไรบ้าง?

ผู้เขียน: พรพรหม ประภากิตติกุล
วันที่เผยแพร่: 15 ธ.ค. 2554
ปรับปรุงล่าสุด: 15 ธ.ค. 2554

หลายคนคงเคยใช้งานโปรแกรมแอนตี้ไวรัส (Antivirus) และคงเคยเจอกับสภาพหน้าจอคอมพิวเตอร์ที่มีการแจ้งเตือนการพบเจอไวรัส (Virus alert) ดังเช่นรูปที่ 2 (2-1)

รูปที่ 2 (2-1) การแจ้งเตือนไวรัส [2-1][2-2]

ซึ่งเหตุการณ์ดังกล่าวมักจะเกิดขึ้นตอนที่เครื่องคอมพิวเตอร์กำลังดาวน์โหลดไฟล์ไวรัสหรือกำลังประมวลผลไฟล์ไวรัส โดยส่วนใหญ่แล้วการแสดงข้อมูลแจ้งเตือนไวรัสจะบอกถึงข้อมูลสำคัญสองส่วนหลักๆ คือ ตำแหน่งที่อยู่ของไฟล์ไวรัส และชื่อของไวรัสที่พบ ซึ่งหลายคนคงเคยมีความสงสัยถึงชื่อของไวรัสที่แสดงว่ามีความหมายว่าอย่างไร และแต่ละชื่อมีมาตรฐานหรือใช้กฎเกณฑ์ใดในการตั้งชื่อของไวรัสหรือไม่ ในบทความนี้จะอธิบายถึงข้อมูลที่เกี่ยวข้องกับรูปแบบการตั้งชื่อไวรัสและ ความหมายของชื่อไวรัส เพื่อให้ผู้อ่านเข้าใจถึงรายละเอียดจากชื่อไวรัสได้ในเบื้องต้น โดยมีข้อมูลที่สำคัญดังต่อไปนี้

ไวรัสคืออะไร

ไวรัสคือโปรแกรมไม่พึงประสงค์หรือมัลแวร์ (Malware) ประเภทหนึ่งที่ถูกเผยแพร่โดยใช้เทคนิคหรือกลยุทธ์ต่างๆ เพื่อหลอกล่อให้ผู้ใช้งานหรือเหยื่อติดไวรัสดังกล่าว โดยส่วนใหญ่จะใช้การหลอกให้ดาวน์โหลดและติดตั้งโดยอัตโนมัติ ซึ่งผลจากการติดไวรัส จะทำให้เครื่องคอมพิวเตอร์ของเหยื่อตกอยู่ในการควบคุมของไวรัสดังกล่าว โดยในตัวอย่างของไวรัสประเภทหนึ่ง พบว่ามีการขโมยข้อมูลบนเครื่องคอมพิวเตอร์ของเหยื่อเพื่อส่งไปยังเครื่องคอมพิวเตอร์ของผู้โจมตี

รูปแบบการตั้งชื่อไวรัส

ปัจจุบัน ชื่อไวรัสที่ค้นพบใหม่ จะถูกกำหนดโดยบริษัทผู้พัฒนาโปรแกรมแอนตี้ไวรัส เนื่องจากใช้เป็นข้อมูลอ้างอิงเพื่อบอกผู้ใช้งานให้ทราบถึงข้อมูลไวรัสที่พบ โดยไม่ได้มีมาตรฐานกลางหรือองค์กรใดองค์กรหนึ่งเป็นผู้กำหนดรูปแบบหรือชื่อไวรัสดังกล่าว สาเหตุหลักคือบางครั้งการอ้างอิงชื่อไวรัสจากแหล่งอื่น ๆ เป็นไปได้ยาก เนื่องจากเป็นไวรัสที่ถูกค้นพบใหม่ จะยังไม่อยู่ในฐานข้อมูลของบริษัทใดบริษัทหนึ่ง ซึ่งทำให้ไวรัสตัวเดียวกันสามารถมีชื่อเรียกที่แตกต่างกันได้ [2-3] แต่ส่วนใหญ่จะพบว่าในแต่ละผู้พัฒนาโปรแกรมแอนตี้ไวรัสจะมีการกำหนดรูปแบบของชื่อไวรัสไปในทิศทางเดียวกัน ซึ่งมีการระบุข้อมูลออกเป็น 4 ส่วนหลักคือ การระบุประเภทไวรัสหรือมัลแวร์ (Prefix) การระบุชื่อของไวรัส (Name) การระบุสายพันธุ์ของไวรัส (Suffix) และการระบุวิธีการแพร่กระจายของไวรัส (Modifer) ตามลำดับ [2-4] โดยมีรายละเอียดดังต่อไปนี้

Prefix ใช้ในการระบุประเภทหรือลักษณะของการโจมตีของไวรัสหรือมัลแวร์ หรืออาจใช้เป็นข้อมูลของระบบที่มีผลกระทบของไวรัสดังกล่าว ยกตัวอย่างเช่น W32 หรือ Win32 หมายถึงเป็นไวรัสที่มีผลกระทบต่อ Windows 32-bit เป็นหลัก (พบว่าผู้ใช้ Windows 64-bit สามารถติดไวรัสที่เป็น W32 ได้ [2-5]) หรือ OM หมายถึงมาโครไวรัสบน Microsoft Office เป็นต้น โดยปกติแต่ละบริษัทผู้พัฒนาโปรแกรมแอนตี้ไวรัสจะมีตารางแสดงถึงข้อมูลอธิบาย ชื่อและความหมายเพื่อให้ผู้ใช้งานทราบถึงความหมายเบื้องต้น เช่น Symantec [2-6] หรือ Avira [2-7]

Name เป็นส่วนที่ผู้ค้นพบไวรัสมักใช้เพื่อบอกชื่อสายพันธุ์ของไวรัสนั้นๆ โดยอาจจะเป็นการตั้งชื่อใหม่หรือใช้เป็นชื่อเดิม [2-8] เพื่อบ่งบอกถึงสายพันธุ์ของไวรัสนั้นๆ โดยปกติการระบุข้อมูลชนิดนี้ มักจะใช้เครื่องหมาย เช่น _ . หรือ / เพื่อคั่นระหว่างข้อมูล Prefix เช่น W32/Bagle โดย Bagle เป็นชื่อเรียกของไวรัส และ W32 เป็นข้อมูล Prefix ที่แสดงถึงไวรัสดังกล่าวสามารถทำงานได้บน Windows 32-bit

- **Suffix เป็นส่วนที่ระบุสายพันธุ์ไวรัสย่อยที่มีความแตกต่างกันไป โดยลักษณะของการระบุข้อมูลจะใช้ตัวอักษรภาษาอังกฤษ และใช้เครื่องหมายเช่น _ - หรือ . เพื่อคั่นระหว่างข้อมูลชื่อไวรัสและสายพันธุ์ย่อยดังกล่าว เช่น W32/Bagle.A หรือ W32/Bagle-B โดยลักษณะของการระบุสายพันธุ์ย่อยนอกจะเรียงตามตัวอักษร A ถึง Z แล้ว หากจบตัวอักษรสุดท้ายแล้วจะเริ่มต้นใหม่ที่ AA ไปจนถึง ZZ ไปเรื่อยๆ**
- **Modifer เป็นส่วนที่ระบุคุณสมบัติเพิ่มเติมของไวรัสตัวดังกล่าว เช่น วิธีการแพร่กระจายของไวรัสที่พบ โดยส่วนใหญ่จะถือเป็น Optional หมายถึงอาจไม่จำเป็นต้องใส่ก็ได้ และถือเป็นข้อมูลส่วนสุดท้ายในการตั้งชื่อไวรัส โดยลักษณะของการระบุข้อมูลดังกล่าวขึ้นอยู่กับความเข้าใจของแต่ละผู้สื่อสาร ว่าจะสื่อถึงข้อมูลแบบไหน ซึ่งอาจไม่มีกฎเกณฑ์ที่ตายตัว โดยจากข้อมูลเบื้องต้นสามารถอธิบายตัวอย่างที่พบได้ดังนี้ [2-9]**

* ใช้เครื่องหมาย @ แล้วตามด้วยตัวอักษรย่อของวิธีการเผยแพร่ไวรัส เช่น @mm หมายถึง ไวรัสชนิดนี้ถูกเผยแพร่ผ่านทางอีเมล โดย mm ย่อมาจาก mass-mailing
* ใช้เครื่องหมาย : แล้วตามด้วยตัวอักษรย่อที่ระบุถึง Encoding ที่สนับสนุนการทำงานของไวรัส เช่น :Uni หมายถึงไวรัสชนิดนี้สามารถทำงานภายใต้แพลตฟอร์มของระบบที่รองรับการอ่าน เขียนข้อมูลแบบ Unicode

ตัวอย่างการอ่านชื่อไวรัส

Bagle.BB@mm เป็นไวรัสสายพันธุ์ชื่อ Bagle เป็นไวรัสสายพันธุ์ย่อยชื่อ BB เผยแพร่ผ่านอีเมลและส่งผลต่อระบบปฏิบัติการ Windows 32-bit

I-Worm/Gaobot.BOW. เป็นไวรัสสายพันธุ์ชื่อ Gaobot เป็นไวรัสสายพันธุ์ย่อยชื่อ BOW และมีลักษณะการทำงานที่เป็น Internet Worm

การเรียนรู้ข้อมูลการตั้งชื่อไวรัสอาจไม่ได้ทำให้เราสามารถ เข้าใจการทำงานหรือคุณลักษณะเฉพาะของไวรัสได้ทุกตัว แต่อย่างน้อยก็เป็นแนวทางในการสืบค้นข้อมูลบนอินเทอร์เน็ต เพื่อช่วยให้เราเข้าใจลักษณะการทำงานของไวรัสนั้นได้มากขึ้น

อ้างอิง

[2-1] http://www.prlog.org/11360953-how-to-remove-antivirus-software-alert.html
[2-2] http://0100101110101101.org/download/biennalepy.html
[2-3] http://www.cknow.com/cms/vtutor/virus-names.html
[2-4] http://antivirus.about.com/od/whatisavirus/a/virusnames.htm
[2-5] http://computervirus.uw.hu/ch04lev1sec3.html
[2-6] http://www.symantec.com/security_response/virusnaming.jsp
[2-7] http://www.avira.ro/en/virus_information/malware_naming_conventions.html
[2-8] http://en.wikipedia.org/wiki/List_of_computer_viruses
[2-9] http://www.caro.org/articles/namingupdated.html

03 แนวทางการใช้งานโทรศัพท์มือถือให้ปลอดภัยจากภัยคุกคาม

ผู้เขียน: พรพรหม ประภากิตติกุล และศุภกร ฤกษ์ดิถีพร

วันที่เผยแพร่: 30 ธ.ค. 2554
ปรับปรุงล่าสุด: 30 ธ.ค. 2554

เนื่องด้วยความเจริญก้าวหน้าของเทคโนโลยีการสื่อสาร ส่งผลให้มีผู้พัฒนาและผลิตโทรศัพท์เคลื่อนที่หรือโทรศัพท์มือถือ ออกมาเป็นจำนวนมาก โดยแต่ละผู้พัฒนาก็มีแนวคิดคล้ายกันคือต้องการอำนวยความสะดวกให้ผู้ใช้งานมากที่สุด สังเกตได้จากสื่อโฆษณาทั่วไปที่มีการโฆษณาถึงความสามารถของโทรศัพท์มือถือในแต่ละฟังก์ชั่นการทำงาน เช่น สามารถเชื่อมต่อกับเครือข่ายไร้สายเพื่อความสะดวกในการเข้าถึงอินเทอร์เน็ตบนโทรศัพท์มือถือ สามารถรับชมวีดีโอบนโทรศัพท์มือถือเพื่อความบันเทิง เป็นต้น แต่จากความสามารถและข้อดีหลายประการของโทรศัพท์มือถือ ก็ยังถูกเจือปนหรือแอบแฝงไปด้วยภัยอันตรายหรือภัยคุกคามหลายประการ ซึ่งผู้ใช้งานอีกจำนวนมากที่อาจจะยังไม่เคยทราบถึงภัยคุกคามจากการใช้งานโทรศัพท์มือถือส่งผลให้ผู้ไม่หวังดีสามารถโจมตีหรือขโมยข้อมูลต่างๆ ได้โดยง่าย เช่น การปลดล็อคโทรศัพท์มือถือเพื่อนำไปติดตั้งซอฟต์แวร์ผิดกฎหมาย ส่งผลให้ระบบปฏิบัติการบนโทรศัพท์มือถือมีช่องโหว่ เป็นต้น และจากสภาพแวดล้อมในปัจจุบัน เป็นที่ยอมรับกันว่าโทรศัพท์มือถือได้กลายเป็นเครื่องมือที่จำเป็นสำหรับ องค์กรหรือบริษัทส่วนใหญ่ที่ต้องการให้พนักงานใช้ในการติดต่อสื่อสารเพื่อ ภารกิจขององค์กร หรือใช้เพื่ออำนวยความสะดวกในการค้นหาข้อมูล ซึ่งโทรศัพท์มือถือขนาดย่อมและมีราคาไม่สูงมากที่วางขายตามท้องตลาดก็ยังมีความสามารถเทียบเท่าและสามารถใช้งานเพื่อสนับสนุนภารกิจขององค์กรได้ เช่น การใช้งาน VoIP [3-1] (Voice over IP) ขององค์กร การเข้าถึงเอกสารที่จัดเก็บอยู่บนเว็บไซต์ขององค์กร รวมถึงการรับส่งจดหมายอิเล็กทรอนิกส์ขององค์กร เป็นต้น ซึ่งในขณะที่อุปกรณ์เหล่านี้ก่อให้เกิดประโยชน์มากมาย แต่ในทางกลับกันก็ส่งผลให้เกิดความเสี่ยงในรูปแบบใหม่ที่องค์กรอาจจะไม่เคยคาดคิดมาก่อน ทำให้องค์กรอาจมีความจำเป็นต้องหาแนวทางปกป้องหรือรักษาความมั่นคงปลอดภัยของ ข้อมูลให้ได้มากที่สุด หรือในอีกมุมหนึ่ง องค์กรอาจจำเป็นต้องกำหนดนโยบายการใช้งานโทรศัพท์มือถือของพนักงานทั้งหมด เพื่อควบคุมหรือจำกัดการเข้าถึงข้อมูลขององค์กรเป็นหลัก ซึ่งในเอกสารฉบับนี้จะอธิบายถึงความสามารถของโทรศัพท์มือถือในปัจจุบัน ข้อแตกต่างระหว่างโทรศัพท์มือถือทั่วไปที่มีราคาต่ำ ไปจนถึงโทรศัพท์มือถือที่เรียกกันว่า Smart Phone ที่มีราคาและความสามารถสูงขึ้น รวมถึงได้มีการรวบรวมรายละเอียดเกี่ยวกับภัยคุกคามและความ

เสี่ยงของเทคโนโลยีที่เกี่ยวข้องกับการใช้อุปกรณ์เหล่านี้ มาตรการป้องกันและแนวทางปฏิบัติของผู้ใช้งานโทรศัพท์มือถือ เพื่อควบคุมมิให้เกิดความเสียหายต่อตัวผู้ใช้งานและองค์กร

ประเภทของโทรศัพท์มือถือ

Basic Phone เป็นโทรศัพท์มือถือทั่วไปที่มักจะมีเพียงฟังก์ชั่นพื้นฐานในการโทรศัพท์และ การรับส่งข้อความสั้น (SMS) อาจมีวิวัฒนาการในการแสดงผลแบบจอภาพสีหรือขาวดำ ตัวอย่างเช่น Nokia 3310 เป็นต้น

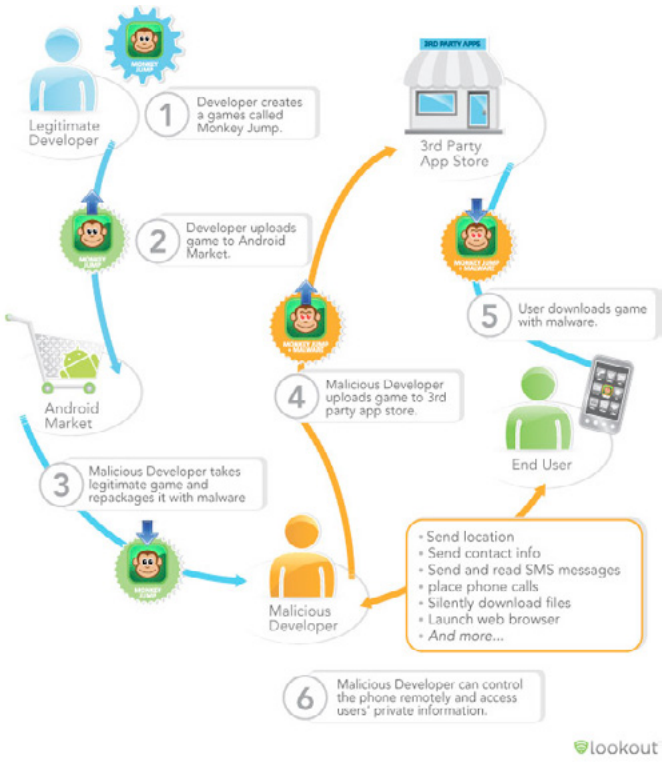
Smart Phone เป็นโทรศัพท์มือถือที่มีความสามารถพิเศษคล้ายคอมพิวเตอร์ รองรับระบบปฏิบัติการต่างๆ ที่เพิ่มเติมความสามารถของ PDA (Personal Digital Assistant) ให้มีประสิทธิภาพเพิ่มขึ้น รองรับการทำงานมัลติมีเดียหลายรูปแบบ รองรับการติดต่อสื่อสารแบบไร้สาย เช่น Bluetooth, GPRS, EDGE, 3G และ WiFi เป็นต้น ในการติดต่อสื่อสาร โดยส่วนใหญ่มักจะใช้ควบคู่กับบริการเสริมจากโอเปอเรเตอร์ โดยในประเทศไทยมีโอเปอเรเตอร์หลักๆ อยู่ 3 รายด้วยกัน คือ AIS, DTAC และ Truemove ดังนั้น Smart Phone จึงไม่ได้เป็นแค่โทรศัพท์มือถือที่เพียงใช้ในการรับสายเข้า โทรออก ฟังเพลง หรือ ถ่ายวีดีโอ เท่านั้น แต่ยังสามารถรองรับการใช้งานระดับเครือข่ายที่มีการติดต่อสื่อสารทั่วโลก เช่น การติดต่อสื่อสารผ่านเครือข่ายสังคมออนไลน์ แบ่งปันข้อมูลออนไลน์ การโทรศัพท์ผ่าน VoIP เป็นต้น ยังไม่รวมถึงระบบปฏิบัติการบนมือถือของแต่ละค่ายที่มีอยู่ในตลาดอย่างมากมาย [3-2] ไม่ว่าจะเป็น Apple iOS Google Android Microsoft Windows Phone Nokia Symbian และ Research in Motion (RIM) BlackBerry OS เป็นต้น ซึ่งระบบปฏิบัติการแต่ละค่ายต่างก็มีความสามารถในการติดตั้งโปรแกรมเพิ่มเติม และยังสามารถอัพเดทข้อมูลที่เป็นจดหมายอิเล็กทรอนิกส์ ตารางนัดหมาย ระหว่างมือถือกับเครื่องคอมพิวเตอร์ให้ตรงกันได้ ซึ่งจากข้อมูลความสามารถของโทรศัพท์ที่ได้กล่าวไป ทำให้เห็นว่าวิวัฒนาการของโทรศัพท์มือถือในปัจจุบันสามารถทำงานได้เปรียบ เสมือนคอมพิวเตอร์ขนาดย่อมเคลื่อนที่เลยก็ว่าได้ โดยต่อไปจะเป็นการอธิบายถึงภัยคุกคามต่างๆ ที่เกี่ยวข้องกับการใช้งานโทรศัพท์มือถือในปัจจุบันและแนวทางในการป้องกัน เพื่อให้ผู้อ่านได้รับทราบและป้องกันภัยได้ด้วยตนเอง ซึ่งได้มีการรวบรวมข้อมูลต่างๆ ไว้ดังนี้

ภัยคุกคามบนโทรศัพท์มือถือ

- **ภัยคุกคามจากการใช้งานโปรแกรมบนโทรศัพท์มือถือ (Application-Based Threats)**
- **โปรแกรมจำนวนมากที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนอุปกรณ์มือถือ พบว่ายังไม่สามารถตรวจสอบลักษณะการทำงานในด้านความมั่นคงปลอดภัยได้ ทำให้ผู้ใช้งานไม่สามารถล่วงรู้ได้เลยว่าโปรแกรมที่ติดตั้งไปเพื่อใช้ ประโยชน์มากมายนั้น จะถูกแฝงมาด้วยปัญหาด้านความมั่นคงปลอดภัยหรือไม่ โดยภัยคุกคามที่มากับโปรแกรมที่ติดตั้งสามารถเป็นได้มากกว่าหนึ่งประเภทดัง ที่จะกล่าวดังต่อไปนี้**
    - มัลแวร์ (Malware) คือโปรแกรมที่ถูกออกแบบมาเพื่อแสดงพฤติกรรมที่เป็นอันตรายต่อข้อมูลในโทรศัพท์มือถือนั้นๆ ตัวอย่างเช่น สั่งให้โทรศัพท์มือถือเครื่องนั้นๆ ส่งข้อความที่ไม่พึงประสงค์ออกไปยังรายการผู้ติดต่อในโทรศัพท์ โดยที่ผู้ใช้งานหรือเจ้าของโทรศัพท์นั้นไม่รู้

ตัว หรือขโมยข้อมูลบนโทรศัพท์มือถือนั้น ซึ่งในกรณีที่ผู้ใช้งานเก็บข้อมูลบัญชีผู้ใช้ของตนเองหรือของผู้เกี่ยวข้อง ไว้ในโทรศัพท์ก็อาจทำให้เกิดการเข้าโจรกรรมข้อมูลที่เกี่ยวข้องต่อไปได้

- สปายแวร์ (Spyware) คือโปรแกรมที่ถูกออกแบบมาเพื่อเก็บรวบรวมข้อมูลต่างๆ ของผู้ใช้งาน โดยเป้าหมายส่วนใหญ่ของสปายแวร์มักมุ่งไปยัง ประวัติการใช้งานโทรศัพท์ ข้อความที่อยู่ รายชื่อผู้ติดต่อ อีเมล รวมถึงภาพถ่าย ซึ่งสปายแวร์โดยทั่วไปมักได้รับการออกแบบสำหรับการเฝ้าติดตามการใช้งานของบุคคลใดบุคคลหนึ่ง หรือการใช้งานที่เกี่ยวข้องกับองค์กร ทั้งนี้ขึ้นอยู่กับวิธีการที่จะใช้สปายแวร์ที่กำหนดเป้าหมาย ซึ่งไม่จำเป็นเสมอไปที่ผู้ลักลอบติดตั้งโปรแกรมประเภทนี้จะเป็นผู้มีจุดประสงค์ร้ายทั้งหมด เนื่องจากมีความเป็นไปได้ว่าโปรแกรมประเภทนี้ถูกติดตั้งโดยผู้ที่เป็นผู้ปกครองซึ่งมีความหวังดีต่อผู้ใช้งาน เช่น ผู้ปกครองติดตั้งโปรแกรมการตรวจสอบสถานที่การใช้งานบนโทรศัพท์มือถือของลูกที่อยู่ในการดูแล การเข้าโจมตีผู้ใช้งานและโทรศัพท์มือถือด้วยมัลแวร์และ สปายแวร์ ส่วนใหญ่ จะพบว่าใช้เทคนิคในการหลอกลวงผู้ใช้งานให้การดาวน์โหลดโปรแกรมมาติดตั้งโดย ไม่รู้ตัว เช่น ให้คลิกที่ลิงก์ซึ่งดูเหมือนไม่น่าจะมีความผิดปกติอะไร แต่จริงๆ แล้วนั่นคือการสั่งให้ดาวน์โหลดและติดตั้งมัลแวร์ลงในโทรศัพท์มือถือดังกล่าว และเมื่อมัลแวร์หรือสปายแวร์ติดตั้งโปรแกรมเสร็จแล้วก็จะสู่กระบวนการโจมตี ในลักษณะต่างๆ ต่อไป นอกจากนี้ยังมีการหลอกลวงในลักษณะที่พบเห็นได้บ่อยครั้งคือการ Repackaging ซึ่งเป็นเทคนิคที่พบบ่อยมากในนักเขียนมัลแวร์ที่พยายามจะใช้ชื่อโปรแกรมที่มีการทำงานถูกต้องตามกฎหมาย แต่ได้มีการปรับเปลี่ยนการทำงานของโปรแกรม รวมถึงแทรกโค้ดที่เป็นอันตรายไว้ในเวอร์ชันที่เตรียมจะเผยแพร่ จากนั้นจึงทำการเผยแพร่ไปยังแหล่งให้ดาวน์โหลดโปรแกรมต่างๆ ทั่วไป รวมถึงบนเว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมบนโทรศัพท์มือถือ เพื่อหลอกให้ผู้ใช้งานเข้าใจผิดและติดตั้งโปรแกรมดังกล่าวบนโทรศัพท์มือถือ ซึ่งเทคนิคการ Repackaging ได้ผลลัพธ์ในการโจมตีค่อนข้างสูง เนื่องจากการอ้างอิงชื่อโปรแกรมที่เคยพัฒนามาแล้ว โดยจะพบได้จากในช่วงต้นปี 2011 นักเขียนมัลแวร์บนระบบปฏิบัติการ Android ใช้เทคนิคในการ Repackaging ซึ่งสามารถอ้างอิงข้อมูลได้ตามรูปที่ 3 (3-1) ด้านล่าง



รูปที่ 3 (3-1) การ Repackaging [3-3]

* ช่องโหวในโปรแกรมที่ใช้งาน คือ พฤติกรรมการทำงานของโปรแกรมที่มีความผิดพลาด โดยถูกค้นพบและสามารถนำมาใช้ประโยชน์เพื่อวัตถุประสงค์ที่เป็นอันตราย ซึ่งการค้นพบช่องโหว่ดังกล่าวมักจะส่งผลให้ผู้ค้นพบสามารถโจมตีโดยการเข้าถึงข้อมูลที่สำคัญหรือการดำเนินการที่ไม่พึงประสงค์ ซึ่งช่องโหว่ดังกล่าวมักถูกแจ้งไปยังผู้พัฒนา เพื่ออัพเดทโปรแกรมแก้ไข โดยหลังจากมีการแก้ไขช่องโหว่แล้ว ผู้พัฒนาจะแจ้งการอัพเดทโปรแกรมกลับมายังผู้ใช้งานอีกครั้งหนึ่ง

ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์บนโทรศัพท์มือถือ (Web-based Threats)

- **เนื่องจากโทรศัพท์มือถือส่วนใหญ่สามารถใช้งานการเชื่อมต่ออินเทอร์เน็ตได้จากเครือข่ายไร้สายทั่วไป ซึ่งทำให้เกิดความสะดวกสำหรับผู้ใช้งานในการเข้าถึงเว็บไซต์หรือบริการอื่นๆ ซึ่งโดยทั่วไปบริการส่วนใหญ่สามารถใช้งานผ่านหน้าเว็บไซต์ได้เป็นหลักและเป็นบริการ**

ที่ผู้ใช้งานมีความต้องการใช้งาน เช่น การอ่านอีเมล การใช้งานธุรกรรมออนไลน์ การเข้าระบบที่เป็นสื่อสังคมออนไลน์ เป็นต้น โดยภัยคุกคามที่เกิดขึ้นกับเว็บไซต์มักไม่มีข้อจำกัดทางด้านระบบปฏิบัติการที่ใช้อยู่ ณ ขณะนั้น เช่น การโจมตีแบบฟิชชิ่ง ซึ่งจะกล่าวในรายละเอียดต่อไป โดยภัยคุกคามดังที่กล่าวนี้แต่ก่อนอาจพบว่ามีแต่ที่เจอในการใช้งานบนเครื่องคอมพิวเตอร์ทั่วไป ในปัจจุบันได้ขยายวงกว้างมายังโทรศัพท์มือถือด้วย เนื่องจากลักษณะการใช้งานที่ค่อนข้างจะใกล้เคียงกันมากในทุกวันนี้ โดยสามารถระบุภัยคุกคามต่างๆ ได้ดังนี้

* ฟิชชิ่ง (Phishing) [3-4] คือการหลอกลวงชนิดหนึ่งโดยใช้หน้าเว็บไซต์หรือส่วนติดต่อผู้ใช้อื่นๆ ที่ออกแบบให้มีลักษณะคล้ายคลึงกับของจริง เพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้หลอกลวง เช่น ผู้หลอกลวงพัฒนาหน้าเว็บไซต์ล็อกอินของ Facebook และส่งลิงก์หลอกลวงโดยแจ้งข้อมูลอันเป็นเท็จให้ผู้ใช้งานเข้าอัพเดทข้อมูล ส่วนบุคคลโดยเป็นลิงก์ของหน้าล็อกอินที่ทำขึ้นมาดังที่กล่าวไว้ตอนต้น เมื่อผู้ใช้งานพยายามล็อกอินเข้าไปยังระบบ จะทำให้ผู้หลอกลวงดังกล่าวสามารถดักจับข้อมูลอันน่าเชื่อได้ว่าเป็นข้อมูลล็อกอินของผู้ใช้งานคนนั้นๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้นๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออกไป ซึ่งลิงก์ที่เป็นการฟิชชิ่งเหล่านี้ส่วนใหญ่มักจะแนบไปกับอีเมล หรือเป็นลิงก์ซึ่งมีเนื้อหาเชิญชวนต่างๆ โดยความรุนแรงของการถูกขโมยข้อมูลดังกล่าวอาจไม่ส่งผลกระทบในทันทีถ้าหากมี การเข้ายับยั้งได้ทัน เช่น เมื่อทราบว่าได้มีการส่งข้อมูลเข้าหน้าเว็บไซต์ฟิชชิ่งไปแล้ว จึงรีบเข้าเปลี่ยนรหัสผ่านในหน้าเว็บไซต์ของระบบจริงทันที ก็จะทำให้ความเสียหายไม่เกิดขึ้นในวงกว้าง แต่หากผู้ใช้งานปล่อยให้ผู้หลอกลวงสามารถเข้าถึงบัญชีการใช้งานต่างๆ ซึ่งในกรณีที่เป็นระบบที่มีความเสียหายรุนแรง เช่น ระบบธุรกรรมออนไลน์ (e-Transaction) นั่นเท่ากับผู้หลอกลวงจะสามารถใช้เงินในบัญชีผู้ใช้งานนั้นได้ทันที

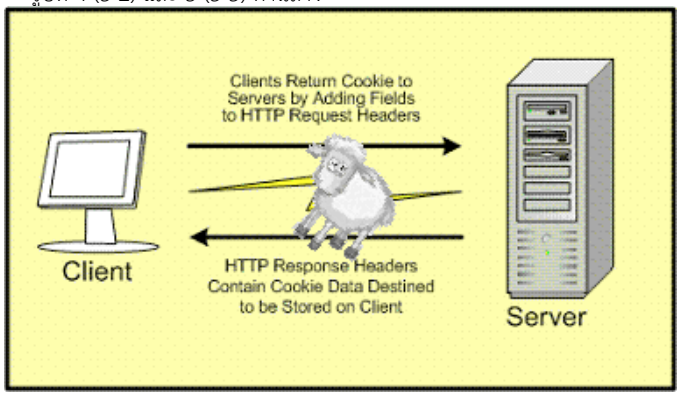
* ช่องโหว่ของโปรแกรมประเภทเบราว์เซอร์ คือ ช่องโหว่ที่ถูกพบในโปรแกรมเบราว์เซอร์หรือโปรแกรมปลั๊กอินที่สามารถติดตั้ง เพิ่มเติมได้ในเบราว์เซอร์ เช่น Flash player หรือ PDF Reader เพื่อวัตถุประสงค์อันตราย โดยลักษณะและวิธีการโจมตีอาจเป็นเพียงแค่การให้ผู้ใช้งานเข้าชมหน้าเว็บไซต์ เท่านั้น จากนั้นจะทำให้ผู้ใช้งานติดมัลแวร์หรือโปรแกรมอันตรายต่างๆ ที่ผู้โจมตีใช้สำหรับช่องโหว่ดังกล่าว

ภัยคุกคามจากการใช้งานเครือข่าย (Network Threats)

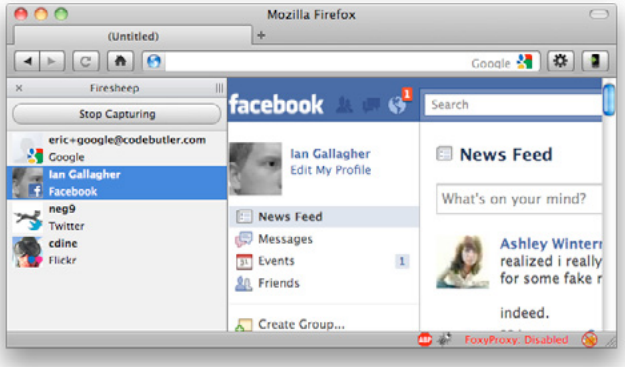
- **โทรศัพท์มือถือในปัจจุบันมักจะสนับสนุนการใช้งานเครือข่ายไร้สาย ซึ่งมีผู้ให้บริการเป็นจำนวนมาก ทั้งที่น่าเชื่อถือและไม่สามารถตรวจสอบได้ โดยมีภัยคุกคามที่สามารถส่งผลกระทบต่อการใช้งานบนโทรศัพท์มือถือต่างๆ ได้ดังนี้**

* การเปลี่ยนสถานะจากผู้ใช้งานเป็นผู้โจมตี ผ่านข้อบกพร่องของระบบปฏิบัติการบนโทรศัพท์เคลื่อนที่ ส่งผลให้โทรศัพท์เคลื่อนที่สามารถส่งต่อหรือแพร่กระจายมัลแวร์ได้โดย อัตโนมัติผ่านการทำงานบนเครือข่าย เช่น เครือข่ายไร้สาย (WiFi) หรือ บลูทูธ (Bluetooth)

* การถูกดักจับข้อมูลบนเครือข่ายไร้สาย (WiFi sniffing) [3-5] คือลักษณะการขโมยข้อมูลบนเครือข่ายไร้สาย ซึ่งโดยทั่วไปเป็นข้อมูลที่รับส่งกันโดยไม่ได้มีการเข้ารหัสความมั่นคงปลอดภัยที่เหมาะสม ทำให้มีโอกาสถูกลักลอบขโมยข้อมูลได้โดยง่าย เพียงแค่ใช้เทคนิคและวิธีในการดักจับข้อมูลจากโปรแกรมประเภท Sniffer ซึ่งหาข้อมูลได้ตามเว็บไซต์ทั่วไป โดยในที่นี้ขอยกตัวอย่างวิธีการใช้งานโปรแกรมชื่อ Firesheep ซึ่งเป็นปลั๊กอินบนเบราว์เซอร์ Firefox ที่ใช้ในการดักจับข้อมูลในเครือข่ายเดียวกัน ซึ่งส่วนใหญ่เป้าหมายมักใช้งานเครือข่ายไร้สายสาธารณะ และไม่ได้เชื่อมต่อบริการเว็บไซต์ที่มีการเข้ารหัส HTTPS โดยลักษณะการทำงานของโปรแกรมจะมีการดักจับข้อมูลแล้วกรองข้อมูลเพื่อค้นหา Cookie ซึ่งคือข้อมูลที่ใช้ระบุตัวตนกับเว็บไซต์ที่เข้าใช้บริการ โดยข้อมูล Cookie ที่กล่าวถึงจะถูกเก็บไว้ในเบราว์เซอร์ของผู้ใช้งานหลังจากที่มีการล็อกอินเว็บไซต์ จากนั้นโปรแกรมจะแสดงรายการที่ดักจับได้ทั้งหมด ซึ่งผู้ใช้งานโปรแกรมสามารถคลิกที่รายการดังกล่าวเพื่อสวมรอยเข้าเป็นผู้ใช้งานนั้นๆ ดังแสดงในรูปที่ 4 (3-2) และ 5 (3-3) ด้านล่าง



รูปที่ 4 (3-2) การทำงานของ Firesheep [3-6]



รูปที่ 5 (3-3) ผลการทำงานของ Firesheep [3-7]

ภัยคุกคามจากการดูแลรักษาโทรศัพท์(Physical Threats)

- **เนื่องจากโทรศัพท์มือถือเป็นอุปกรณ์ซึ่งออกแบบให้พกพาและติดตัวไปมาได้สะดวก จึงมีรูปแบบที่ค่อนข้างเล็ก ซึ่งจากสภาพการณ์ปัจจุบันโทรศัพท์เป็นของมีค่าสำหรับมิจฉาชีพ รวมไปถึงมีค่าสำหรับกลุ่มคนบางกลุ่มที่ต้องการได้มาซึ่งข้อมูลส่วนบุคคล จึงได้แยกภัยคุกคามที่เกิดจากการดูแลรักษาโทรศัพท์มือถือไว้เพื่อพิจารณา ความสำคัญอยู่ 2 ประเภทดังนี้**
  - การสูญหายหรือการถูกขโมยโทรศัพท์มือถือ เนื่องด้วยปัจจุบันโทรศัพท์มือถือมีราคาสูงขึ้นอาจเพราะสาเหตุของเทคโนโลยีที่อยู่ในอุปกรณ์โทรศัพท์มือถือ หรือเพราะค่านิยมทางสังคมที่ทำให้ต้องใช้โทรศัพท์มือถือราคาแพง แต่ไม่ว่าจะกรณีไหนก็ตามการใช้งานโทรศัพท์มือถือในปัจจุบันนับเป็นเป้าหมายของกลุ่มมิจฉาชีพทั่วไป เนื่องจากเป็นอุปกรณ์พกพาขนาดเล็กมีโอกาสถูกขโมยได้ง่าย และมีตลาดที่มีความต้องการหรือรองรับการซื้อขายได้มากมายโดยที่ไม่มีการตรวจสอบแหล่งที่มา ทำให้มีความเสี่ยงสูงที่ผู้ใช้งานจะมีโอกาสถูกกลุ่มมิจฉาชีพขโมยโทรศัพท์มือถือ หรือด้วยขนาดของอุปกรณ์มือถือที่เล็กอยู่แล้วอาจทำให้มีโอกาสที่จะลืมหรือทำตกหล่นได้ง่าย
  - การถูกขโมยข้อมูลส่วนบุคคล สามารถเกิดขึ้นได้ตลอดเวลาและทุกสถานการณ์ทั้งโดยตั้งใจแต่แรกหรือเป็นเพราะโอกาสที่เปิดกว้างจนทำให้ผู้อื่นสบโอกาสที่จะขโมยข้อมูลส่วนบุคคลมักเกิดขึ้นจากความไม่ใส่ใจและความไม่ตระหนักถึงความมั่นคงปลอดภัยของข้อมูลภายในโทรศัพท์มือถือ ทำให้ผู้ไม่หวังดีขโมยข้อมูลส่วนบุคคลไปได้โดยง่าย เช่น การแอบดูข้อมูล การล็อกอินเข้าสู่ระบบจากโทรศัพท์มือถือ หรือการนำโทรศัพท์มือถือไปซ่อมที่ร้านโดยไม่ได้ทำการเคลียร์ข้อมูลการใช้งาน ก่อน โดยข้อมูลส่วนบุคคลที่หมายถึงอาจไม่ใช่เพียงข้อมูลส่วน

ตัวเพียงเท่านั้นแต่ จะพบว่าเป็นข้อมูลขององค์กรด้วย อาจเป็นเอกสารขององค์กร ข้อมูลรายชื่อผู้ติดต่องาน รวมไปถึงข้อมูลที่อยู่ในระบบต่างๆ เช่น ข้อมูลบัญชีธนาคาร ข้อมูลอีเมลขององค์กร ซึ่งข้อมูลทั้งหมดที่กล่าวมานั้น หากถูกขโมยข้อมูลขึ้นมาจริงแล้ว คงไม่สามารถประเมินมูลค่าความเสียหายได้เป็นอย่างแน่นอน

แนวทางการปฏิบัติสำหรับผู้ใช้งานโทรศัพท์มือถือและข้อมูลให้มีความมั่นคงปลอดภัย

ดูแลรักษาโทรศัพท์มือถืออย่างใกล้ชิด ผู้ใช้งานควรพึงระลึกไว้เสมอว่าความเสียหายที่เกิดขึ้นเมื่อมีการสูญหายหรือ โดยขโมยโทรศัพท์มือถือไป จะส่งผลกระทบทั้งในแง่ของทรัพย์สินและข้อมูลที่อยู่ในโทรศัพท์มือถือ ยิ่งมีการเก็บข้อมูลสำคัญในโทรศัพท์มือถือมากเท่าไหร่ยิ่งมีโอกาสก่อให้เกิดปัญหาตามมามากขึ้นเท่ากัน ยังไม่รวมถึงการเก็บข้อมูลที่เกี่ยวข้องกับองค์กร เช่น อีเมล ซึ่งจะส่งผลกระทบกับองค์กรโดยตรง เพราะฉะนั้นผู้ใช้งานควรมีความรอบคอบและระวังรักษาโทรศัพท์มือถืออย่างใกล้ ชิด

ตั้งค่าการล็อกโทรศัพท์มือถือเมื่อไม่ใช้งาน แม้การล็อกการใช้งานโทรศัพท์มือถือ จะไม่ได้เป็นการป้องกันการเข้าถึงข้อมูลที่ได้ผลร้อยเปอร์เซ็นต์ แต่ก็สามารถเป็นแนวทางเบื้องต้นในการชะลอหรือป้องกันการเข้าถึงข้อมูลสำคัญ บนโทรศัพท์มือถือจากผู้ไม่หวังดี ซึ่งอาจจะเกิดจากการถูกขโมยโทรศัพท์มือถือ และยังเป็นแนวทางที่ผู้ใช้งานสามารถทำได้โดยง่าย ซึ่งกระบวนการดังกล่าวสามารถทำได้โดยการตั้งค่า Pin หรือรหัสผ่านบนโทรศัพท์มือถือนั้นๆ (วิธีการสามารถตรวจสอบจากเว็บไซต์ผู้ผลิตโทรศัพท์มือถือนั้นๆ หรือสอบถามที่ศูนย์บริการโทรศัพท์มือถือที่ซื้อมา)

สำรองข้อมูลจากโทรศัพท์มือถือไว้ในแหล่งอื่นที่ปลอดภัย การสำรองข้อมูลถือเป็นเรื่องที่สำคัญที่ต้องมีการปฏิบัติอยู่เสมอ เนื่องจากเมื่อเกิดเหตุฉุกเฉินเช่น โทรศัพท์หาย หรือโทรศัพท์ชำรุดหรือใช้งานไม่ได้ ปัญหาอย่างแรกที่จะตามมานอกจากการทำให้โทรศัพท์กลับมาใช้งานได้หรือหา โทรศัพท์ให้พบ คือการเข้าถึงข้อมูลบนโทรศัพท์มือถือเช่น ข้อมูลผู้ติดต่อ (Contact book) ซึ่งข้อดีของการสำรองข้อมูลคือ นอกจากจะมีข้อมูลที่สามารถใช้ได้เมื่อเกิดกรณีฉุกเฉินแล้ว ยังทำให้รู้ขอบเขตของข้อมูลที่สูญหายไปด้วย เช่น อาจจะเก็บข้อมูลเลขที่บัญชีธนาคารและรหัสผ่านของ e-Transaction เอาไว้ ทำให้สามารถแจ้งระงับการเข้าใช้งานได้ก่อนจะเกิดความเสียหาย ซึ่งกระบวนการสำรองข้อมูลของโทรศัพท์มือถือแต่ละยี่ห้อหรือแต่ละรุ่นอาจมีความแตกต่างกันไป วิธีการต่างๆ สามารถตรวจสอบจากเว็บไซต์ผู้ผลิตโทรศัพท์มือถือนั้นๆ หรือสอบถามที่ศูนย์บริการโทรศัพท์มือถือที่ซื้อมา

พิจารณาเก็บเฉพาะข้อมูลที่จำเป็นในโทรศัพท์มือถือ การเก็บข้อมูลบนโทรศัพท์มือถือ ควรพิจารณาถึงความสำคัญและความเหมาะสมของข้อมูลที่จะจัดเก็บ ไม่ควรเก็บข้อมูลที่มีความสำคัญมากๆ เช่น ข้อมูลบัตรเครดิต หรือข้อมูลรหัสผ่านสำหรับล็อกอินเข้าใช้งานระบบ เนื่องจากหากโทรศัพท์เกิดสูญหาย หรือโดนผู้ประสงค์ร้ายลักลอบขโมยไปได้ อาจทำให้เกิดความเสียหายที่รุนแรงมากกว่าเดิม แต่ก็ไม่ใช่ข้อมูลเหล่านี้จะไม่สามารถเก็บบนโทรศัพท์มือถือได้ เนื่องจากปัจจุบันผู้พัฒนาโปรแกรมบนระบบปฏิบัติการบนโทรศัพท์มือถือต่างๆ ได้พัฒนาโปรแกรมสำหรับจัดเก็บข้อมูลส่วนตัวออกมามากมายและมีการรักษาความมั่นคงปลอดภัยของข้อมูล ยกตัวอย่างเช่น ผู้พัฒนาโปรแกรมบนระบบปฏิบัติการ Symbian ได้พัฒนาโปรแกรมชื่อ Wallet โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งานเก็บข้อมูลส่วนตัวต่างๆ ลงในโทรศัพท์มือถือและมีการรักษาความมั่นคงปลอดภัยของข้อมูล โดยให้มีการล็อกอินก่อนผู้ใช้งานจะเข้าถึงข้อมูล

ปิดโหมดการเชื่อมต่อบลูทูธหรือหลีกเลี่ยงการเชื่อมต่อบลูทูธจากแหล่งที่มาที่ไม่รู้จัก ปัจจุบันผู้ใช้งานมักมีการใช้งานการเชื่อมต่อบลูทูธบนโทรศัพท์มือถือในหลาย ด้าน เช่น ใช้สำหรับการรับส่งไฟล์ระหว่างโทรศัพท์มือถือกับเครื่องคอมพิวเตอร์ หรือใช้สำหรับเป็นโมเด็มเพื่อให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ ที่เชื่อมต่อบลูทูธอยู่ ซึ่งหากเป็นการใช้งานตามปกติกับอุปกรณ์หรือบุคคลต่างๆ ที่รู้จักและรับทราบถึงจุดประสงค์ในการเข้าใช้งานการเชื่อมต่อนั้นๆ ก็อาจไม่ก่อให้เกิดผลเสีย แต่ผลเสียจะเกิดต่อเมื่อไม่ทราบว่าผู้ที่ต้องการเชื่อมต่อบลูทูธกับโทรศัพท์มือถือของเรานั้นเป็นใครและมีจุดประสงค์ในการใช้อย่างไร เนื่องจากผู้ไม่หวังดีส่วนใหญ่มักจะอาศัยความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานในการลักลอบใช้งานหรือดึงข้อมูลสำคัญบนโทรศัพท์มือถือ เช่น รูปภาพ หรือ SMS ไปได้ ซึ่งข้อดีของการใช้งานเครือข่ายบลูทูธคือจะต้องได้รับการยินยอมให้มีการเชื่อมต่อก่อน มิเช่นนั้นจะไม่สามารถเชื่อมต่อได้ ซึ่งหากผู้ใช้งานมีความรู้เท่าทันผู้ไม่หวังดีแล้วนั้น ก็จะทำให้การใช้งานโทรศัพท์มือถือมีความมั่นคงปลอดภัยมากขึ้นเท่านั้น โดยหากไม่มีการใช้งานบลูทูธก็สมควรปิดโหมดการเชื่อมต่อบลูทูธไว้ เพราะในบางครั้งอาจพบว่าผู้ใช้งานไม่ได้ตั้งใจกดยอมรับการเชื่อมต่อแต่พลาดไปโดนตอนโทรศัพท์มือถืออยู่ในกระเป๋า (การปิดโหมดเชื่อมต่อบลูทูธของโทรศัพท์มือถือปกติสามารถเข้าตรวจสอบได้จากเมนู"การเชื่อมต่อ" ซึ่งแต่ละยี่ห้อหรือแต่ละรุ่นอาจมีความแตกต่างกันไป โดยสามารถตรวจสอบจากเว็บไซต์ผู้ผลิตโทรศัพท์มือถือนั้นๆ หรือสอบถามที่ศูนย์บริการโทรศัพท์มือถือที่ซื้อมา)

แจ้งผู้ให้บริการต่างๆ ที่เกี่ยวข้องเมื่อโทรศัพท์สูญหาย เมื่อพบว่าโทรศัพท์สูญหาย ไม่ว่าจะด้วยกรณีโดนขโมยหรือทำตกหล่นที่ไหนก็ตาม สิ่งแรกที่ผู้ใช้งานโทรศัพท์มือถือควรทำคือการแจ้งไปยังผู้ให้บริการรายต่างๆ เพื่อปิดบริการ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น โดยมีขอบเขตการแจ้งปิดบริการตามรายการข้อมูลที่มีอยู่ในโทรศัพท์มือถือนั้นๆ เช่น แจ้งผู้ให้บริการสัญญาณโทรศัพท์มือถือที่ใช้งานระงับสัญญาณโทรศัพท์มือถือของตนเองชั่วคราวเพื่อป้องกันการใช้งาน หรือหากมีการเก็บข้อมูลรหัสผ่านของระบบต่างๆ ก็ควรแจ้งปิดการใช้งานด้วย เช่น แจ้งปิดการใช้งานระบบ e-Transaction ชั่วคราว แจ้งผู้ดูแลระบบอีเมลขององค์กรเพื่อเปลี่ยนรหัสผ่าน เป็นต้น

เลือกติดตั้งโปรแกรมในโทรศัพท์มือถือเท่าที่จำเป็นและจากแหล่งที่มาที่น่าเชื่อถือ แม้ระบบปฏิบัติการบนโทรศัพท์มือถือทั่วไปจะอนุญาตให้สามารถติดตั้งโปรแกรมเสริมเพื่ออำนวยความสะดวกในการใช้งานมากขึ้น แต่ก็มีความเสี่ยงที่ผู้ใช้งานจะเจอกับโปรแกรมที่มีความสามารถในการขโมยข้อมูลหรือโปรแกรมไม่พึงประสงค์ต่างๆ ตามที่ได้กล่าวไว้ในหัวข้อภัยคุกคาม เพราะฉะนั้นทางป้องกันที่ดีที่สุดคือดาวน์โหลดเฉพาะโปรแกรมที่จำเป็นจริงๆ และพิจารณาดาวน์โหลดจากเว็บไซต์

ของผู้พัฒนาเท่านั้น หรือดาวน์โหลดจากแหล่งดาวน์โหลดที่ได้รับการควบคุมและรับรองความมั่นคงปลอดภัยจาก ผู้พัฒนาระบบปฏิบัติการเช่น Android Market สำหรับระบบปฏิบัติการ Android หรือ App Store สำหรับระบบปฏิบัติการ iOS

เชื่อมต่อไปยังระบบงานต่างๆ ผ่าน VPN หรือช่องทางการเชื่อมต่อเครือข่ายที่มีการเข้ารหัสลับ จากที่ได้กล่าวไว้ข้างต้นถึงการใช้งานโทรศัพท์มือถือที่เกี่ยวข้องกับองค์กร ซึ่งนอกจากที่จะให้ผู้ใช้งานทำตามแนวทางการใช้งานโทรศัพท์มือถือแล้วนั้น องค์กรเองควรต้องมีส่วนช่วยกำหนดขอบเขตการใช้งาน เพื่อให้เกิดการรักษาความมั่นคงปลอดภัยในการใช้งานโทรศัพท์อย่างเหมาะสม หมายถึงองค์กรควรจะขยายการจัดการรักษาความมั่นคงปลอดภัยและการควบคุมให้ในส่วนที่โทรศัพท์มือถือทั่วไปไม่สามารถจัดการให้ได้ เช่น พัฒนาระบบการทำงานที่สามารถเข้าถึงได้จากโทรศัพท์มือถือผ่านช่องการเข้ารหัสแบบ HTTPS หรือจัดหาช่องทางการใช้งาน VPN เพื่อเชื่อมต่อเข้าระบบงานภายในองค์กร โดยจากที่ได้กล่าวมานี้ สามารถแนะนำเป็นแนวทางการปฏิบัติขององค์กรในการควบคุมการใช้งานโทรศัพท์ภายในองค์กรได้

พิจารณาลิงก์ที่อยู่บนเว็บไซต์ก่อนการคลิกทุกครั้ง ภัยคุกคามที่เกิดขึ้นจากการใช้งานเว็บไซต์สามารถเกิดขึ้นได้ง่ายและส่งผล กระทบต่อผู้ใช้งานได้มากที่สุด เนื่องมาจากโดยส่วนใหญ่เป็นการโจมตีโดยใช้เทคนิคทางจิตวิทยา โดยไม่จำเป็นต้องใช้ความรู้ทางเทคนิคมากนัก ซึ่งผู้ใช้งานโดยส่วนใหญ่ที่ตกเป็นเหยื่อมักจะไม่รู้เท่าทันวิธีการของผู้โจมตี ผู้โจมตีจะใช้เทคนิคต่างๆ หลอกล่อให้ผู้ใช้งานคลิกไปยังลิงก์เพื่อส่งต่อไปยังเว็บไซต์ที่มีอันตราย เพราะฉะนั้นทางที่ดีที่สุดคือใช้วิจารณญาณก่อนการคลิกที่ลิงก์ใดๆ

อัพเดทระบบปฏิบัติการหรือโปรแกรมบนโทรศัพท์มือถือที่ใช้อยู่ให้เป็นเวอร์ชั่นใหม่อย่างสม่ำเสมอ โดยปกติหากมีการดาวโหลดโปรแกรมจากผู้พัฒนาต่างๆ และโปรแกรมนั้นๆ มีการปรับปรุงเกิดขึ้น จะมีการแจ้งอัพเดทโปรแกรมผ่านทางช่องทางต่างๆ เช่น อีเมล หรือ ผ่านระบบแจ้งเตือนของตัวระบบปฏิบัติการเอง เนื่องจากส่วนใหญ่การปรับปรุงเวอร์ชันใหม่ของโปรแกรมต่างๆ จะทำเพื่อปรับปรุงช่องโหว่หรือความผิดพลาดที่เกิดขึ้นในโปรแกรมเวอร์ชั่นก่อนหน้า ดังนั้นเมื่อผู้พัฒนามีการปรับปรุงเวอร์ชันของโปรแกรม ผู้ใช้ก็ควรทำการอัพเดทโปรแกรมนั้นๆ ให้เป็นเวอร์ชันล่าสุดโดยทันที

ใช้โทรศัพท์มือถือทำธุรกรรมออนไลน์อย่างระมัดระวัง ทุกวันนี้การใช้โทรศัพท์มือถือในการทำธุรกรรมออนไลน์กับหน่วยงานทางการเงิน ที่ให้บริการผ่านเว็บไซต์ สร้างความสะดวกสบายให้กับผู้ใช้งานในการทำธุรกรรมเพิ่มขึ้น แต่การใช้งานโทรศัพท์มือถือโดยเลือกใช้ผู้ให้บริการอินเทอร์เน็ตไร้สาย สาธารณะที่มีความน่าเชื่อถือถือเป็นเรื่องสำคัญ เพราะหากผู้ใช้มองข้ามและเลือกใช้เครือข่ายสาธารณะที่ไม่น่าเชื่อถือ อาจถูกโจรกรรมข้อมูลผ่านเครือข่ายได้ นอกจากนี้ ผู้ใช้งานโทรศัพท์มือถือในการทำธุรกรรมออนไลน์ ควรเลือกอยู่ในบริเวณที่ผู้ไม่ประสงค์ดีไม่สามารถแอบมองและขโมยข้อมูลส่วนตัวที่สำคัญ (Eavesdropping) ได้

อ้างอิง

[3-1] http://en.wikipedia.org/wiki/Voice_over_IP

[3-2] http://en.wikipedia.org/wiki/Mobile_operating_system

[3-3] http://www.techlicious.com/blog/study-finds-explosion-in-mobile-security-threats/

[3-4] http://www.trusteer.com/blog/mobile-users-three-times-more-vulnerable-phishing-attacks

[3-5] http://en.wikipedia.org/wiki/Packet_analyzer

[3-6] http://itiswhatitis.wadewilliams.com/2010/11/firesheep-exposes-security-issues-on.html

[3-7] http://bare516.posterous.com/?tag=wireless

04 ความเป็นมาของไทยเซิร์ต จากกระทรวงวิทย์ฯ สู่กระทรวงไอซีที

ผู้เขียน: สรณันท์ จิวะสุรัตน์ และ ชัยชนะ มิตรพันธ์
วันที่เผยแพร่: 6 ก.พ. 2555
ปรับปรุงล่าสุด: 6 ก.พ. 2555

ในเดือนกุมภาพันธ์ที่ผ่านมา คณะรัฐมนตรีได้มีมติให้จัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และได้มีการโอนภารกิจของศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ประเทศไทย หรือ ไทยเซิร์ต จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยีมายัง สพธอ. เพื่อให้การดำเนินงานของ สพธอ. ด้านการสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์มีความเข้มแข็ง

ไทยเซิร์ตได้เปิดให้บริการอย่างเต็มรูปแบบภายใต้ สพธอ. มาตั้งแต่วันที่ 1 กรกฎาคม 2554 และได้ปรับเปลี่ยนชื่อทางการของไทยเซิร์ตเป็น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team) โดยมีวิสัยทัศน์ให้สังคมออนไลน์มีความมั่นคงปลอดภัย เกิดความเชื่อมั่นกับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ พันธกิจของไทยเซิร์ต มุ่งเน้นการประสานงานกับหน่วยงานในเครือข่าย และหน่วยงานที่เกี่ยวข้องในการดำเนินการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยี สารสนเทศและการสื่อสารที่ได้รับแจ้ง นอกจากนี้ไทยเซิร์ตยังมีพันธกิจเชิงรุกที่ให้ความสำคัญกับการพัฒนาทรัพยากร บุคคลเพื่อเพิ่มขีดความสามารถด้านการรักษาความมั่นคงปลอดภัย

เนื่องจากงานของไทยเซิร์ตมีลักษณะเป็นการประสานงานกับหน่วยงานต่างๆ ไทยเซิร์ตจึงมุ่งมั่นที่จะสร้างความร่วมมือกับหน่วยงานทุกประเภททั้งในและ ต่างประเทศในการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร เช่น ผู้ให้บริการอินเทอร์เน็ต และ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ไทยเซิร์ตสร้างความร่วมมือระหว่างประเทศผ่านเวที FIRST (Forum of Incident Response and Security Teams) สำหรับความร่วมมือกับประเทศทั่วโลก และเวที APCERT (Asia Pacific CERT) สำหรับความร่วมมือกับประเทศในภาคพื้นเอเชียแปซิฟิก

ด้านการพัฒนาทรัพยากรบุคคล ไทยเซิร์ตให้ความสำคัญกับการเผยแพร่ความรู้และข้อมูลข่าวสารเกี่ยวกับการ รักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อเป็นการสร้างภูมิคุ้มกันเบื้องต้นทางด้านไอที และจัดอบรมสัมมนาให้กับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์เฉพาะกลุ่มที่มีความ ต้องการข้อมูลข่าวสารเป็นการเฉพาะ เช่น กลุ่มธุรกิจการเงินการธนาคาร หรือกลุ่มสถาบันวิจัยและสถาบันการศึกษา นอกจากนี้เพื่อให้เกิดความเข้าใจและได้ลงมือปฏิบัติ ไทยเซิร์ตยังจัดและร่วมในกิจกรรมซักซ้อมการรับมือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงาน ทั้งในประเทศและต่างประเทศอีกด้วย

บริการของไทยเซิร์ต

ในการสนับสนุนให้สังคมออนไลน์มีความมั่นคงปลอดภัยและเกิดความเชื่อมั่นกับ ผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ ไทยเซิร์ต ให้บริการหลัก คือ บริการประสานงานแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร บริการข้อมูลข่าวสารความมั่นคงปลอดภัยสารสนเทศ และบริการวิชาการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

บริการประสานงานแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ปัจจุบันไทยเซิร์ตให้บริการประสานงานแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารทางโทรศัพท์และทางอีเมลแก่บุคคลทั่วไป สถาบันการศึกษาและสถาบันวิจัย หน่วยงานภาครัฐและเอกชนทั่วโลก เมื่อได้รับแจ้งเหตุผู้เชี่ยวชาญของไทยเซิร์ตจะตรวจสอบข้อมูลที่ได้รับแจ้ง เพื่อยืนยันว่าเหตุภัยคุกคามที่ได้รับแจ้งได้เกิดขึ้นและมีอยู่จริง แล้วจึงวิเคราะห์ข้อมูลต่อเพื่อหาหน่วยงานที่เป็นต้นเหตุของปัญหา และดำเนินการประสานงานไปยังหน่วยงานดังกล่าวเพื่อให้ดำเนินการแก้ไขปัญหา ไทยเซิร์ตมีระบบการติดตามความคืบหน้าของการจัดการปัญหาภัยคุกคาม และได้กำหนดมาตรฐานการให้บริการไว้คือ ไทยเซิร์ตจะดำเนินการแจ้งหน่วยงานที่เกี่ยวข้องเพื่อแก้ปัญหาที่ได้รับแจ้ง และรายงานสถานะการดำเนินงานภายใน 2 วันทำการ มีการติดตามผลการดำเนินงานทุก 3 วันทำการ

บริการข้อมูลข่าวสารความมั่นคงปลอดภัยสารสนเทศ

ไทยเซิร์ตอยู่ในเครือข่ายความร่วมมือของหน่วยงานที่มีบทบาทในการตอบสนองต่อ การแจ้งเหตุภัยคุกคาม (Computer Security Incident Response Team: CSIRT หรือ Computer Emergency Response Team: CERT) ซึ่งมีภารกิจในการแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับแจ้งจากหน่วยงาน CSIRT อื่นๆ ในเครือข่ายหรือที่ตรวจพบกับผู้ใช้งานภายในประเทศไทยเพื่อสร้างความตระหนักและความพร้อมในการรับมือต่อภัยคุกคามที่เกิดขึ้น โดยผู้เชี่ยวชาญของไทยเซิร์ตจะวิเคราะห์ข้อมูลภัยคุกคามที่มีผลกระทบสูงกับผู้ใช้งาน พร้อมเสนอแนะข้อควรปฏิบัติในการรับมือ แก้ไขหรือป้องกันภัยคุกคามในบทความแจ้งเตือนภัยคุกคามของไทยเซิร์ต นอกจากนั้น ไทยเซิร์ตจัดทำข้อมูลเชิงสถิติของภัย

คุกคามที่รายงานมาที่ไทยเซิร์ตเผยแพร่ บนเว็บไซต์ไทยเซิร์ตเป็นรายเดือน เพื่อใช้วิเคราะห์แนวโน้มของภัยคุกคามที่เกิดภายในประเทศไทย

บริการวิชาการในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ไทยเซิร์ตมีผู้เชี่ยวชาญที่มีศักยภาพและความรู้ที่สามารถให้บริการวิชาการในการรักษาความมั่นคงปลอดภัยสารสนเทศกับหน่วยงานทั้งภายในและต่างประเทศ ไทยเซิร์ตให้บริการกับหน่วยงานภายในประเทศในส่วนของการให้คำปรึกษาในการวิเคราะห์ข้อมูลภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร การจัดทำแผนและนโยบายทางด้านเทคโนโลยีสารสนเทศ เพื่อให้สอดคล้องกับมาตรฐานสากลทางด้านเทคโนโลยีสารสนเทศและสอดคล้องกับข้อกำหนดของกฎหมาย จัดฝึกอบรมสัมมนา เพื่อสร้างความตระหนักหรือเสริมสร้างศักยภาพของบุคลากรของหน่วยงานให้สามารถ ป้องกันและแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารจัดการซักซ้อม รับมือภัยคุกคาม เพื่อเสริมทักษะและสร้างความพร้อมในการรับมือภัยคุกคามของหน่วยงาน รวมถึงการสนับสนุนวิทยากรในการบรรยาย เพื่อสร้างความตระหนักและให้ความรู้กับหน่วยงานทั้งในและต่างประเทศ

สถิติภัยคุกคามที่รายงานมาที่ไทยเซิร์ต

ตั้งแต่วันที่ 1 กรกฎาคม ไทยเซิร์ตได้รับแจ้งเหตุภัยคุกคามจากหน่วยงานทั้งในและต่างประเทศโดยเฉลี่ยมากกว่า 100 เรื่องต่อเดือน ข้อมูลเชิงสถิติเกี่ยวกับเหตุภัยคุกคามที่ไทยเซิร์ตได้รับแจ้งสามารถจำแนก เป็น 9 ประเภทตามที่ได้กำหนดโดย The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรป ดังตารางต่อไปนี้

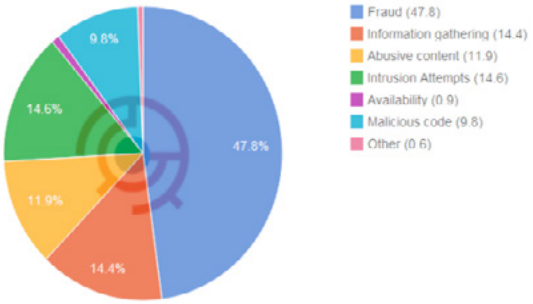
ตารางที่ 1 (4-1) ประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดย eCSIRT

ประเภทภัยคุกคาม	คำอธิบาย
1 เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)	ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)
2 โปรแกรมไม่พึงประสงค์ (Malicious Code)	ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้ เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ
3 ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่างๆที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
4 ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE- Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหวใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆ ของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชี ชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
5 การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

6 การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DoS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ
7 การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหา ผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ
8 การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหา ผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ
9 ภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุก คามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

เหตุภัยคุกคามที่ได้รับรายงานใน 6 เดือนแรก (ในระหว่างวันที่ 1 กรกฎาคม ถึง 31 ธันวาคม 2554) มาที่ไทยเซิร์ตซึ่งดำเนินการภายใต้ สพธอ. มีจำนวนทั้งสิ้น 646 เรื่อง และสามารถแสดงสัดส่วนแบ่งแยกตามประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร แสดงดังรูปที่ 6 (4-1) โดยสามารถจัดลำดับตามจำนวนเหตุภัยคุกคามได้รับแจ้งได้เป็นประเภทใหญ่ๆได้ 5 ด้าน ภัยคุกคามส่วนใหญ่ประมาณ 47.8% จะเป็นภัยคุกคามด้าน การฉ้อฉล ฉ้อโกงหรือหลอกลวง เพื่อผลประโยชน์ (Fraud) ซึ่งทั้งหมดในส่วนนี้เป็น

กรณี Phishing ที่เกิดกับสถานบันการเงินทั้งในประเทศและต่างประเทศ ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบต่อโดยตรงผู้ใช้บริการชำระเงินทาง อิเล็กทรอนิกส์ ในส่วนภัยคุกคามที่รองลงมาเป็นภัยคุกคามที่เกี่ยวความพยายามที่จะโจมตีและ เจาะระบบ โดยเป็นภัยคุกคามในการพยายามบุกรุกหรือเจาะระบบ (Intrusion Attempts) จำนวน 14.6% และภัยคุกคามด้านความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) จำนวน 14.4% สำหรับภัยคุกคามในลำดับถัดไปเป็นภัยคุกคามทางด้านเนื้อหาที่เป็นภัยคุกคาม (Abusive Content) จำนวน 11.9% ซึ่งทั้งหมดเป็นรายงานภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่ได้รับแจ้งจากหน่วยงานในต่างประเทศ และพบว่ามีลักษณะเป็นการแจ้งเตือนเหตุภัยคุกคามของเครื่องคอมพิวเตอร์ที่ใช้ สำหรับส่งอีเมลสแปม (SPAM) ในลำดับสุดท้ายเป็นภัยคุกคามทางด้าน โปรแกรมไม่พึงประสงค์ (Malicious Code) จำนวน 9.8%



รูปที่ 6 (4-1) สถิติภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ในระหว่างวันที่ 1 กรกฎาคม ถึง 31 ธันวาคม 2554 แยกตามประเภทภัยคุกคาม

ไทยเซิร์ตได้ดำเนินการแก้ไขปัญหาภัยคุกคามที่ได้รับแจ้งไปได้ประมาณ 80% ส่วนอีก 20% ที่เหลือมีการติดตามความคืบหน้าของการแก้ไขปัญหาทุก 3 วัน สำหรับข้อมูลเชิงสถิติเกี่ยวกับภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อ สาร สามารถดูได้ที่ www.thaicert.or.th/statistics.html

ช่องทางการติดต่อกับไทยเซิร์ต

ไทยเซิร์ตได้จัดเตรียมช่องทางการติดต่อเพื่อแจ้งเหตุภัยคุกคามไว้ 2 ช่องทาง ประกอบด้วย ทางโทรศัพท์ หมายเลข 02-142-2483 เวลา 8.30 – 17.30 น. ทุกวันยกเว้นวันหยุดราชการ และทางอีเมลที่ report@thaicert.or.th และในกรณีที่ผู้แจ้งมีความประสงค์จะรักษาความลับของข้อมูลในอิเล็กทรอนิกส์ เมลที่ส่งถึงไทยเซิร์ต ผู้ส่งสามารถดำเนินการเข้ารหัสลับข้อมูลด้วยเทคโนโลยี PGP ด้วยกุญแจสาธารณะของไทยเซิร์ตดังต่อไปนี้

- **อิเล็กทรอนิกส์เมล: report@thaicert.or.th**
- **หมายเลขของกุญแจ (Key ID): 0x9C57FF14**

- ประเภทของกุญแจ (Key Type): RSA
- วันหมดอายุ (Expires): 2012-06-30
- ขนาดความยาว (Key size): 2048
- Fingerprint: 6D81 3D72 DC3E 2B15 09C2 CA51 92D2 9387 9C57 FF14

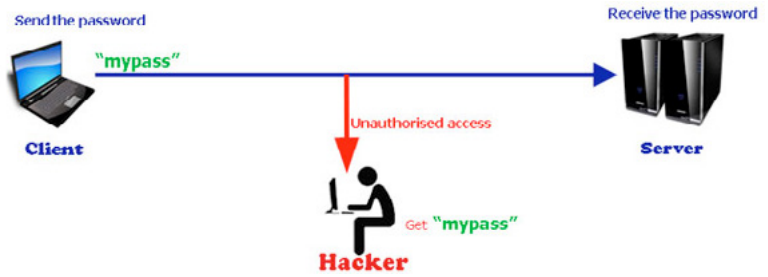
05 วันนี้คุณใช้ HTTPS หรือยัง

ผู้เขียน: ศุภกร ฤกษ์ดิถีพร
วันที่เผยแพร่: 17 ก.พ. 2555
ปรับปรุงล่าสุด: 17 ก.พ. 2555

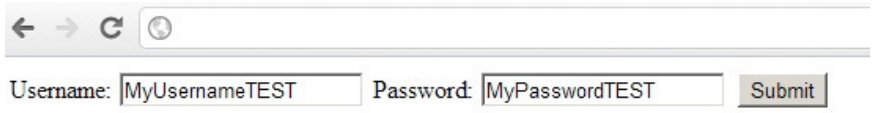
คนจำนวนมากยังไม่ค่อยเข้าใจวิธีการรักษาความมั่นคงปลอดภัยบนเว็บไซต์ และมักจะมีคำถามอยู่เสมอว่า การที่พวกเขากรอกข้อมูลชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลบัตรเครดิตสำหรับการทำธุรกรรมออนไลน์ต่างๆ นั้น จะแน่ใจได้อย่างไรว่าการส่งข้อมูลมีความมั่นคงปลอดภัย ข้อมูลที่ส่งถึงผู้รับมีความถูกต้องครบถ้วนสมบูรณ์และไม่มีบุคคลอื่นล่วงรู้ ข้อมูลสำคัญเหล่านี้ เพื่อตอบข้อสงสัยดังกล่าว ผู้ใช้จึงต้องทำความเข้าใจเกี่ยวกับการรับ-ส่งข้อมูลบนอินเทอร์เน็ตในแบบ HTTP คือที่ใช้งานทั่วไป และแบบที่เพิ่มความมั่นคงปลอดภัยให้กับข้อมูลที่เรียกว่า HTTPS เสียก่อน

HTTP (Hypertext Transfer Protocol)

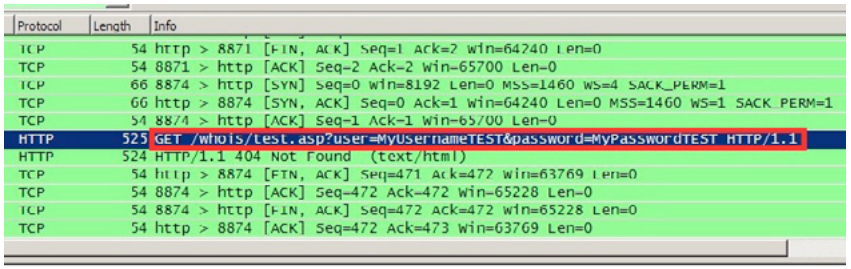
HTTP เป็นโพรโทคอลที่ใช้กับเว็บไซต์ ในการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้งานและเครื่องให้บริการ ดังจะเห็นได้จากเวลาที่เราเข้าเว็บไซต์ด้วยโปรแกรมเว็บเบราว์เซอร์ เช่น Internet Explorer, Firefox หรือ Google Chrome เมื่อต้องการเรียกดูเว็บไซต์ เช่น Facebook ก็ต้องพิมพ์ http://www.facebook.com จะเห็นว่า ชื่อเว็บไซต์ที่เราพิมพ์ต้องขึ้นต้นด้วย “http” แล้วตามด้วยชื่อเว็บไซต์ ลักษณะการทำงานแบบนี้เป็นการส่งข้อมูลแบบข้อความธรรมดา (Cleartext) คือ ไม่มีการเข้ารหัสลับ ทำให้สามารถถูกผู้ไม่หวังดีขโมยข้อมูลได้ง่าย [5-1] ดังรูปที่ 7 (5-1) -9 (5-3)



รูปที่ 7 (5-1) การส่งข้อมูลแบบ HTTP



รูปที่ 8 (5-2) ตัวอย่างการกรอกข้อมูล Username และ Password ผ่าน HTTP



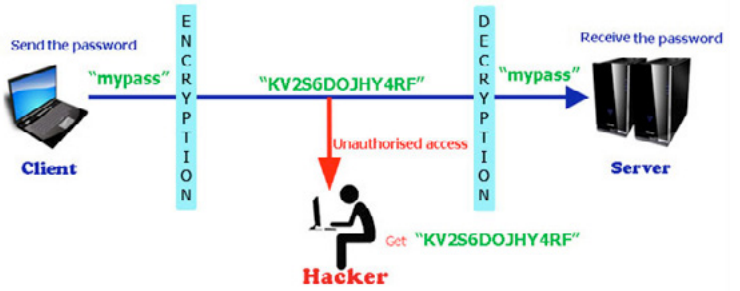
รูปที่ 9 (5-3) ตัวอย่างการดักจับข้อมูล username และ password ผ่าน HTTP

เมื่อผู้ใช้งานส่งรหัสผ่านถึงเครื่องให้บริการเว็บไซต์ ข้อมูลจะถูกส่งเป็นข้อมูลธรรมดา (ไม่เข้ารหัสลับ) Hacker สามารถขโมยรหัสผ่านและนำไปใช้ได้ทันทีซึ่งอาจจะส่งผลให้แก่ผู้ใช้งานได้ เช่น หากผู้ใช้งานโดน Hacker ขโมยรหัสผ่านของร้านค้าออนไลน์แห่งหนึ่งที่มีข้อมูลบัตรเครดิต Hacker สามารถนำข้อมูลไปใช้ซื้อสินค้าได้อย่างง่ายดาย ผลที่ตามมาคือความสูญเสียของผู้ใช้งาน ซึ่งยังไม่รวมถึงปัญหาและความยุ่งยากในเรื่องของคดีความที่จะเกิดขึ้นตามมา อีกด้วย หรือที่มีข่าวมากมายเกี่ยวกับหลายองค์กรที่ถูกขโมยข้อมูลพนักงานหรือลูกค้า เช่น ชื่อ เบอร์โทรศัพท์ อีเมล Hacker ก็อาจจะนำข้อมูลที่ได้ไปขายให้กับกลุ่มคนที่ขายของทางโทรศัพท์จำพวกบัตร เครดิต สินเชื่อ ประกัน เป็นต้น

จะเห็นได้ว่าการใช้งานอินเทอร์เน็ตที่ไม่มีความมั่นคง ปลอดภัยนั้น มีความเสี่ยงที่จะส่งผลกับชีวิตของเราอย่างไร ดังนั้นหากผู้พัฒนาเทคโนโลยีที่มองเห็นถึงความสำคัญของข้อมูลก็จะสามารถ สร้างความน่าเชื่อถือให้กับองค์กรได้ โดยการหาวิธีปกป้องข้อมูลดังกล่าว โดยจะขอเสนออีกหนึ่งวิธีนั่นคือการเพิ่มการเข้ารหัสของข้อมูลที่เรียกว่า HTTPS

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS เป็นโพรโทคอลที่ถูกพัฒนามาเพื่อแก้ปัญหาของ HTTP โดยมีการเพิ่มความมั่นคงปลอดภัยด้วยการเข้ารหัสลับข้อมูลระหว่างผู้ใช้งาน และเครื่องให้บริการ หากมีผู้ไม่หวังดีดักรับข้อมูลก็จะไม่สามารถเข้าใจข้อมูลนั้นได้ ดังรูปที่ 10 (5-4) [5-2] การเข้าใช้งานเว็บไซต์จะระบุการเชื่อมต่อแบบ https:// แทนที่จะเป็น http://



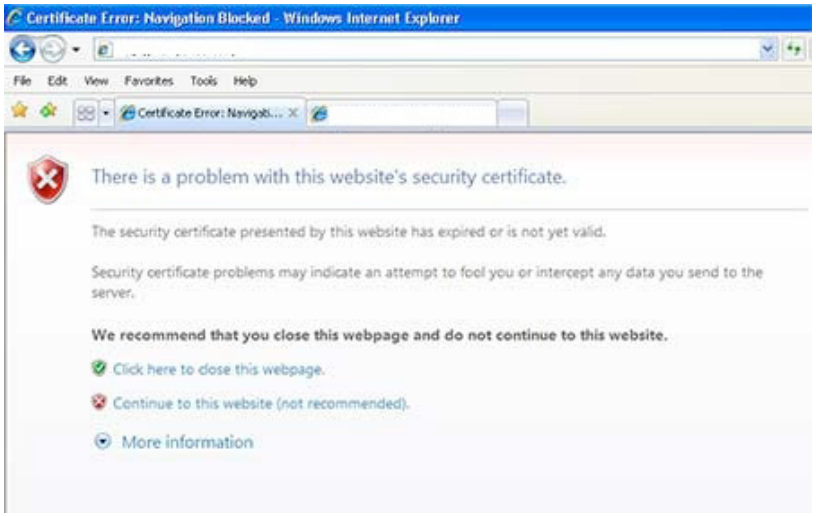
รูปที่ 10 (5-4) การส่งข้อมูลแบบ HTTPS

เมื่อผู้ใช้งานส่งรหัสผ่านถึงเครื่องให้บริการเว็บไซต์ ข้อมูลจะถูกส่งเป็นข้อมูลเข้ารหัสลับ Hacker ไม่สามารถนำข้อมูลไปใช้ได้

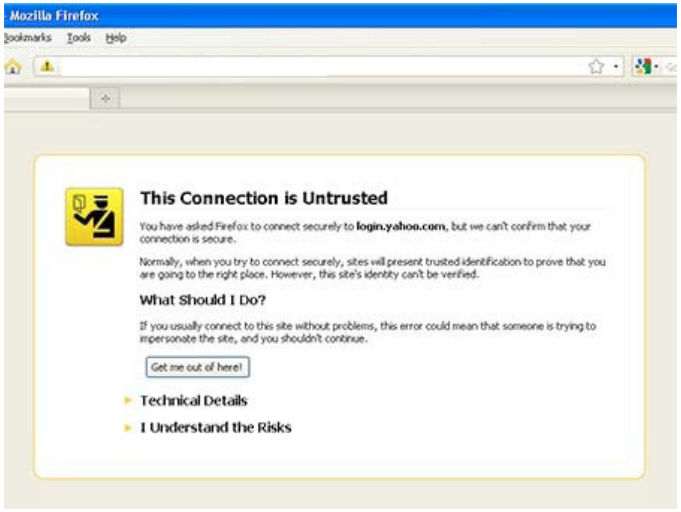
การที่จะใช้งานโพรโทคอล HTTPS ได้นั้น เครื่องให้บริการเว็บไซต์จะต้องทำการติดตั้งใบรับรองความมั่นคงปลอดภัยทางอิเล็กทรอนิกส์ (Certificate) เสียก่อน ซึ่งใบรับรองความมั่นคงปลอดภัยทางอิเล็กทรอนิกส์สามารถทำขึ้นเองหรือซื้อจากผู้ให้ บริการรับรองที่น่าเชื่อถือ (Trusted certificate authority) ก็ได้ เพียงแต่ใบรับรองที่ทำขึ้นเองนั้น ป้องกันเว็บเบราว์เซอร์จะแจ้งเตือนความผิดปกติเนื่องจากไม่มีผู้รับรองความน่าเชื่อถือ ดังจะเห็นจากรูปที่ 11 (5-5)- 13 (5-7)

ทั้งนี้ใบรับรองจะเป็นตัวบ่งบอกความถูกต้องของข้อมูลที่เกี่ยวข้องกับเว็บไซต์นั้น เช่น การยืนยันความเป็นเจ้าของเว็บไซต์ ความสมบูรณ์ของการเข้ารหัสลับข้อมูล ช่วยเพิ่มความมั่นใจให้กับผู้ใช้งานขณะที่มีการรับ-ส่งข้อมูล

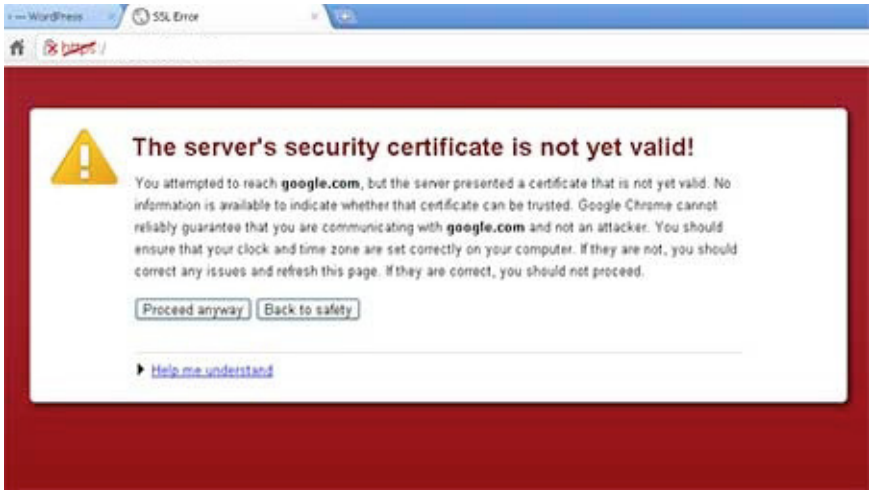
ตัวอย่างการแจ้งเตือนใบรับรองผิดปกติ



รูปที่ 11 (5-5) แสดงตัวอย่างหน้าจอโปรแกรม Internet Explorer พบใบรับรองที่ผิดปกติ



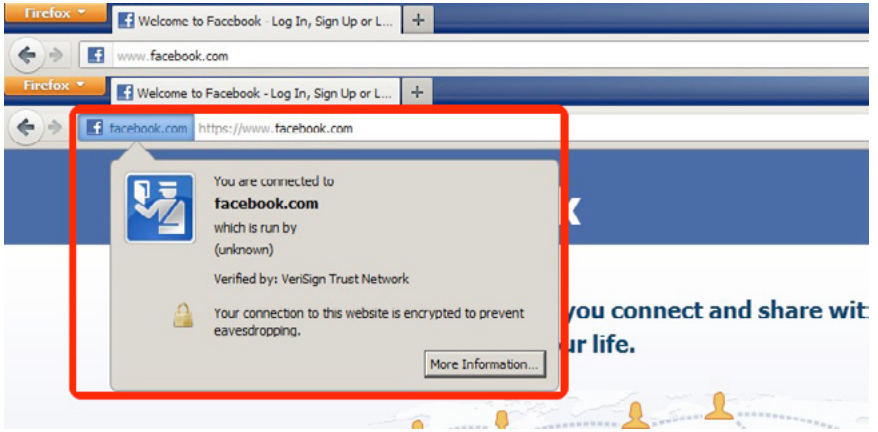
รูปที่ 12 (5-6) แสดงตัวอย่างหน้าจอโปรแกรม Firefox พบใบรับรองที่ผิดปกติ



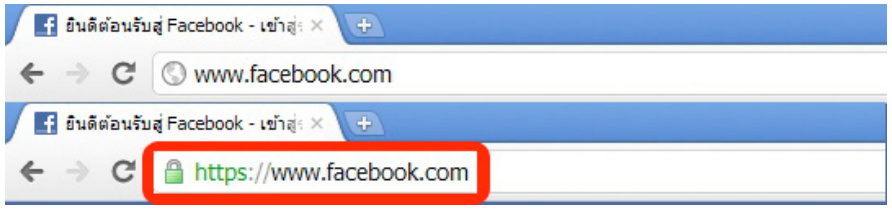
รูปที่ 13 (5-7) แสดงตัวอย่างหน้าจอโปรแกรม Google Chrome พบใบรับรองที่ผิดปกติ

วิธีสังเกตเว็บไซต์ที่เรากำลังใช้งานอยู่นั้นเป็น HTTP หรือ HTTPS หรือไม่? สำหรับการสังเกตจากเครื่องคอมพิวเตอร์ทั่วไป ให้มองหาสัญลักษณ์รูปกุญแจ

รูปที่ 14 (5-8) เปรียบเทียบ HTTP กับ HTTPS จากเว็บเบราว์เซอร์ Internet Explorer



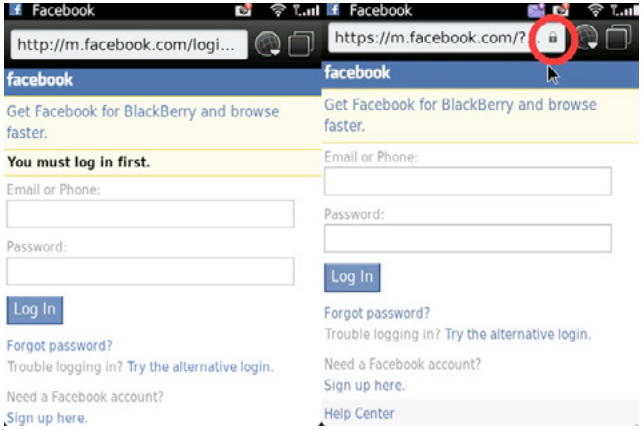
รูปที่ 15 (5-9) ภาพเปรียบเทียบ HTTP กับ HTTPS จากเว็บเบราว์เซอร์ Firefox



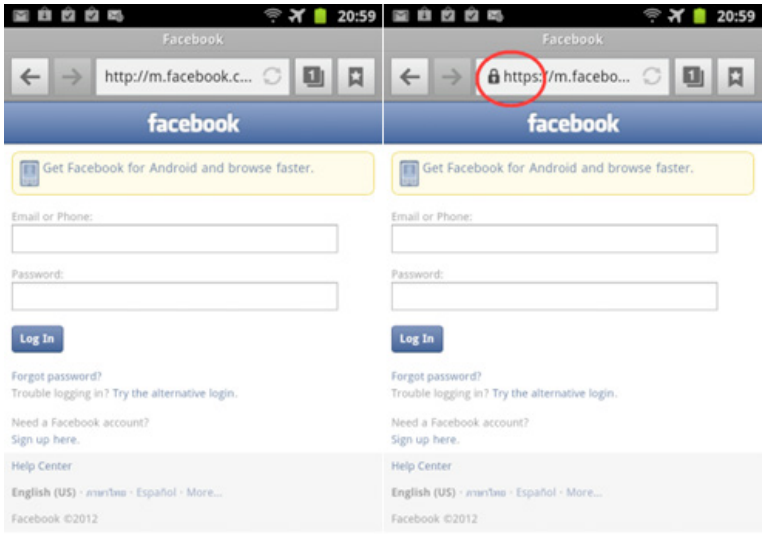
รูปที่ 16 (5-10) ภาพเปรียบเทียบ HTTP กับ HTTPS จากเว็บเบราว์เซอร์ Google Chrome

นอกจากเครื่องคอมพิวเตอร์แล้วเราสามารถใช้ HTTPS กับโทรศัพท์เคลื่อนที่ได้อีกเช่นกัน โดยใช้วิธีสังเกตสัญลักษณ์รูปกุญแจเหมือนกับเครื่องคอมพิวเตอร์ทั่วไป ดังรูปที่ 17 (5-11) - 19 (5-13)

รูปที่ 17 (5-11) เปรียบเทียบ HTTP กับ HTTPS จากเว็บเบราว์เซอร์บน iPhone



รูปที่ 18 (5-12) เปรียบเทียบ HTTP กับ HTTPS จากเว็บเบราว์เซอร์บน BlackBerry



รูปที่ 19 (5-13) เปรียบเทียบ HTTP กับ HTTPS จากเว็บเบราว์เซอร์บน Android

ผู้เขียนขอแนะนำให้เลือก “ใช้ HTTPS ทุกครั้ง” ที่เราจำเป็นต้องกรอกข้อมูลสำคัญ เช่น ชื่อ-นามสกุล ที่อยู่ วัน/เดือน/ปี เกิด หมายเลขโทรศัพท์ หมายเลขบัตรเครดิต เป็นต้น เพื่อป้องกันการขโมยข้อมูลจาก Hacker สำหรับการใช้งานบริการต่างๆบนระบบอินเทอร์เน็ต เช่น การทำธุรกรรมทางการเงินบนเว็บไซต์กับธนาคาร ร้านค้าออนไลน์ บริการด้านอีเมล์ Gmail Hotmail Yahoo บริการเครือข่ายสังคมออนไลน์ (Social Network) twitter facebook เป็นต้น

อ้างอิง

[5-1] http://simple.wikipedia.org/wiki/Cleartext
[5-2] http://en.wikipedia.org/wiki/HTTP_Secure

06 การตรวจสอบและกำจัดมัลแวร์ด้วย MSRT

ผู้เขียน: เจษฎา ช้างสีสังข์
วันที่เผยแพร่: ๒๔ ก.พ. ๒๕๕๕
ปรับปรุงล่าสุด: ๒๔ ก.พ. ๒๕๕๕

ปัจจุบันมีผู้ใช้งานระบบปฏิบัติการหลากหลายระบบ ซึ่งเปรียบเสมือนตัวกลางระหว่างฮาร์ดแวร์และโปรแกรมประยุกต์ที่ผู้ใช้ใช้กัน อยู่ทั่วไป และ Windows ก็เป็นหนึ่งในระบบปฏิบัติการที่ผู้ใช้ทั่วไปนิยมใช้งาน จากสถิติการใช้งานในปี พ.ศ. 2554 พบว่ามีผู้ใช้งานระบบปฏิบัติการ Windows ถึง 93% เมื่อเทียบกับจำนวนผู้ใช้งานระบบปฏิบัติการอื่นๆ [6-1] หากมองในแง่ของความมั่นคงปลอดภัยแล้ว ก็อาจเป็นเหตุผลหนึ่งที่ทำให้ ผู้ไม่หวังดีพุ่งเป้ามาเพื่อโจมตีระบบปฏิบัติการ Windows ดังนั้น ผู้ใช้งานระบบปฏิบัติการ Windows จึงควรให้ความสนใจในการป้องกันการโจมตีจากผู้ไม่หวังดี เพื่อลดความเสียหายที่อาจจะเกิดขึ้นกับระบบ โดยการที่ผู้ใช้ควรมีการอัพเดทระบบปฏิบัติการอยู่เสมอ ซึ่งช่วยให้สามารถแก้ปัญหาช่องโหว่ของระบบ ตรวจสอบและกำจัดมัลแวร์ รวมทั้งเพิ่มประสิทธิภาพของระบบด้วย ในส่วนของโปรแกรมที่ทำหน้าที่ตรวจสอบและกำจัดมัลแวร์นั้น มีเครื่องมือหนึ่งที่แนะนำคือ Microsoft® Windows® Malicious Software Removal Tool (MSRT) เป็นเครื่องมือที่พัฒนาโดย Microsoft โดยสาเหตุที่แนะนำเครื่องมือนี้เนื่องจากติดตั้งได้ง่ายโดยจะมาพร้อมกับ การอัพเดทระบบปฏิบัติการ สามารถใช้งานได้ฟรี เรียกใช้ได้ง่าย และมีการอัพเดทเวอร์ชันอย่างสม่ำเสมอทุกเดือน

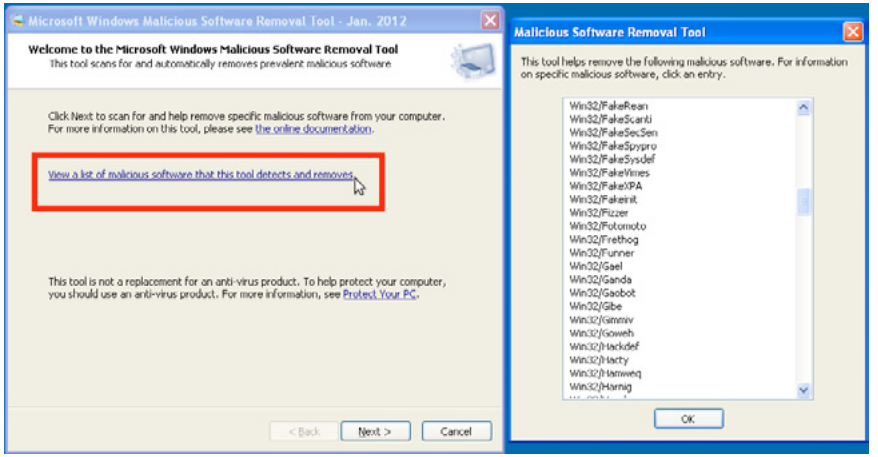
ในบทความนี้ไม่ได้เป็นการประชาสัมพันธ์ทางการค้าเพื่อ Microsoft แต่เป็นการแนะนำเครื่องมือที่มีความเหมาะสมกับผู้ใช้ทั่วไป โดยบทความนี้จะอธิบายถึงคุณลักษณะและการทำงานของโปรแกรมเบื้องต้น ข้อดีข้อเสียของเครื่องมือ รูปแบบการใช้เครื่องมือ และตัวอย่างวิธีการใช้งาน

คุณลักษณะและการทำงานของโปรแกรม

MSRT ถูกเผยแพร่ครั้งแรกเมื่อวันที่ 1 มกราคม พ.ศ. 2548 โดยทำงานภายใต้ระบบปฏิบัติการ Windows 7, Windows Vista, Windows XP, Windows Server 2008 และ Windows Server 2003 MSRT นั้นไม่ได้ถูกออกแบบมาเพื่อใช้แทนโปรแกรมแอนตี้ไวรัส (Antivirus) แต่ใช้เพื่อทำงานร่วมกันกับโปรแกรมแอนตี้ไวรัส โดย MSRT นั้นมีความแตกต่างจากโปรแกรมแอนตี้ไวรัสอยู่ 2 ข้อ ดังนี้

1. MSRT จะกำจัดมัลแวร์ออกจากระบบได้ก็ต่อเมื่อเครื่องของผู้ใช้ติดมัลแวร์แล้ว ส่วนโปรแกรมแอนตี้ไวรัสจะสามารถยับยั้งไม่ให้มัลแวร์ติดตั้งตัวเอง ลงไปยังเครื่องของผู้ใช้ ดังนั้นผู้ใช้จึงควรติดตั้งโปรแกรมแอนตี้ไวรัสเพื่อใช้งานร่วมกับ MSRT
2. MSRT จะกำจัดได้เฉพาะมัลแวร์ที่อยู่ในรายชื่อของ Microsoft เท่านั้น ซึ่งเป็นมัลแวร์ที่เป็นอันตรายต่อระบบปฏิบัติการ Windows และมีอัตราการแพร่ระบาดสูง [6-2]

MSRT จะมีการอัพเดทเวอร์ชันใหม่ในทุกวันอังคารที่สองของเดือน ผ่านระบบ Windows Update, Microsoft Update และ Microsoft Download Center [6-3] [6-4] ซึ่งทุกครั้งที่มีการอัพเดทจะมีการเพิ่มข้อมูลของมัลแวร์ที่โปรแกรมสามารถ ตรวจสอบและกำจัดได้ โดยในขั้นตอนแรกที่ผู้ใช้เปิดโปรแกรมขึ้นมา สามารถตรวจสอบรายชื่อของมัลแวร์ด้วยการคลิกที่ลิงก์ ดังรูปที่ 20 (6-1)



รูปที่ 20 (6-1) แสดงรายชื่อมัลแวร์ที่สามารถตรวจสอบและกำจัดได้

การเรียกใช้งาน MSRT นั้นสามารถเรียกใช้ได้ ๒ วิธี ดังนี้

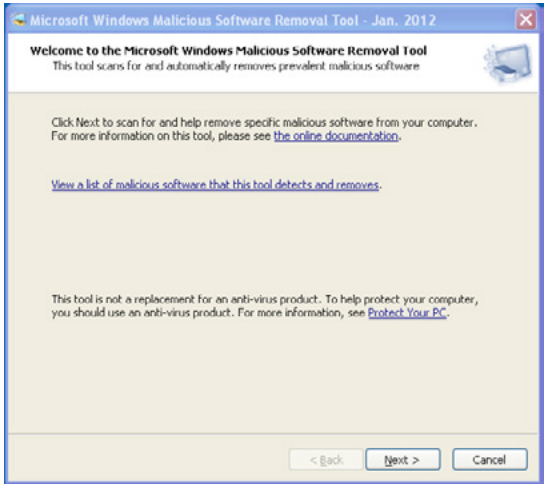
1. เรียกใช้ MSRT โดยตรง ซึ่งการเรียกใช้ดังกล่าว จะต้องทำการดาวน์โหลดจากเว็บไซต์ Microsoft Download Center มายังเครื่องผู้ใช้ก่อน โดยมีข้อดีคือ สามารถกำหนดรูปแบบการตรวจสอบได้ (มีอธิบายในหัวข้อถัดไป) และ สามารถเรียกใช้งาน MSRT เวลาใดก็ตามที่ผู้ใช้ต้องการ เช่นในกรณีที่พบความผิดปกติของระบบหรือ สงสัยว่าระบบติดมัลแวร์ ส่วนข้อเสียคือ ผู้ใช้จำเป็นต้องดาวน์โหลดโปรแกรมใหม่ทุกครั้งที่มีการอัพเดทเวอร์ชัน

2. เรียกใช้ MSRT โดยอัตโนมัติ หลังจากมีการอัพเดทเวอร์ชัน MSRT ผ่านระบบ Windows Update หรือ Microsoft Update ซึ่งเกิดขึ้นในวันอังคารที่สองของทุกเดือน โดยมีข้อดีคือ มีการอัพเดทเวอร์ชัน MSRT โดยอัตโนมัติ ส่วนข้อเสียคือ มีการเรียกใช้งานเพียงครั้งเดียวในช่วงเวลาหนึ่งเดือน

หลังจากที่มีการตรวจสอบระบบด้วย MSRT หากตรวจพบมัลแวร์ โปรแกรมจะทำการกำจัด มัลแวร์ออกโดยอัตโนมัติ และรายงานผลไปยัง Microsoft (มีกำหนดอยู่ในข้อตกลงการใช้งานโปรแกรม เรียกว่า EULA หรือ End-User License Agreement) [6-5][6-6] โดยผลการตรวจสอบที่ส่งไปยัง Microsoft จะถูกใช้ในการวิเคราะห์ข้อมูล เช่น การติดตามจำนวนการแพร่กระจายของมัลแวร์

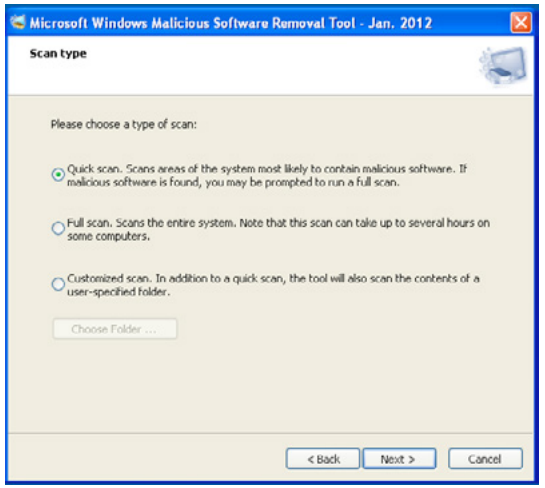
ตัวอย่างการใช้งาน

1. เมื่อผู้ใช้เรียกใช้ MSRT จะพบกับหน้าต่างแสดงรายละเอียดของโปรแกรม ดังรูปที่ 21 (6-2) ได้แก่ ลิงก์ไปยังหน้าเอกสารของโปรแกรมและรายชื่อมัลแวร์ที่สามารถตรวจจับได้



รูปที่ 21 (6-2) แสดงหน้าต่างเมื่อเริ่มต้น MSRT

2. คลิกปุ่ม Next จะแสดงหน้าต่างดังรูปที่ 22 (6-3) เพื่อให้ผู้ใช้เลือกรูปแบบการสแกน (Scan type) โดยแต่ละรูปแบบมีความแตกต่างกันดังนี้



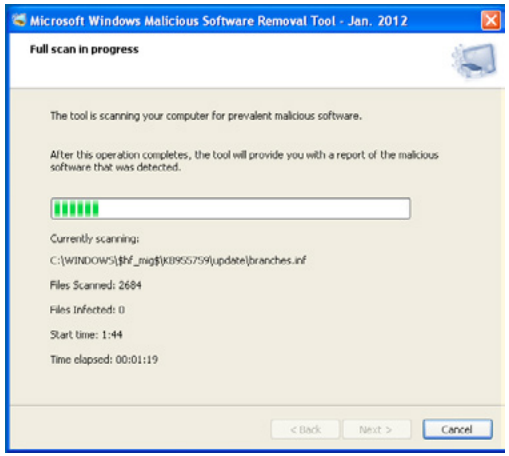
รูปที่ 22 (6-3) แสดงหน้าต่างการเลือกรูปแบบการสแกนมัลแวร์

2.1 Quick scan
เป็นการตรวจสอบพื้นที่ของระบบที่มัลแวร์ส่วนใหญ่ใช้เป็นที่ฝังตัวอยู่ ถ้าพบมัลแวร์ โปรแกรมจะให้ทำการตรวจสอบแบบ Full Scan อีกครั้ง

2.2 Full scan
เป็นการสแกนทุกส่วนของระบบ โดยจะตรวจสอบทุกไดรฟ์ที่อยู่ในระบบ แต่ไม่รวมไดรฟ์ของเครือข่ายที่เชื่อมต่อกับระบบ การสแกนแบบนี้ใช้เวลามากกว่า แบบ Quick scan

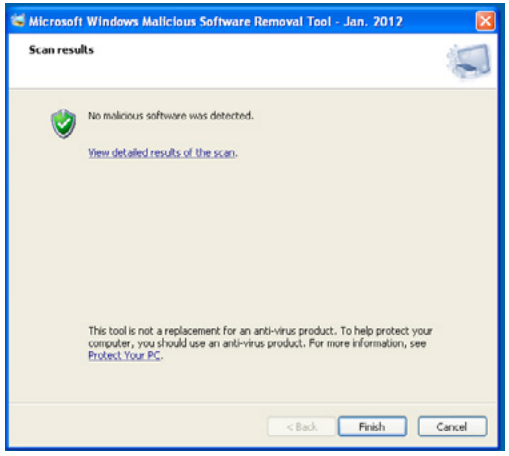
2.3 Customized scan
เป็นการสแกนแบบ Quick scan โดยที่ผู้ใช้สามารถระบุโฟลเดอร์ที่ต้องการตรวจสอบเพิ่มเติมได้

3. เมื่อผู้ใช้เลือกรูปแบบการตรวจสอบแล้ว สามารถเริ่มดำเนินได้โดยการคลิกปุ่ม Next เพื่อทำการตรวจสอบ ดังรูปที่ 23 (6-4)



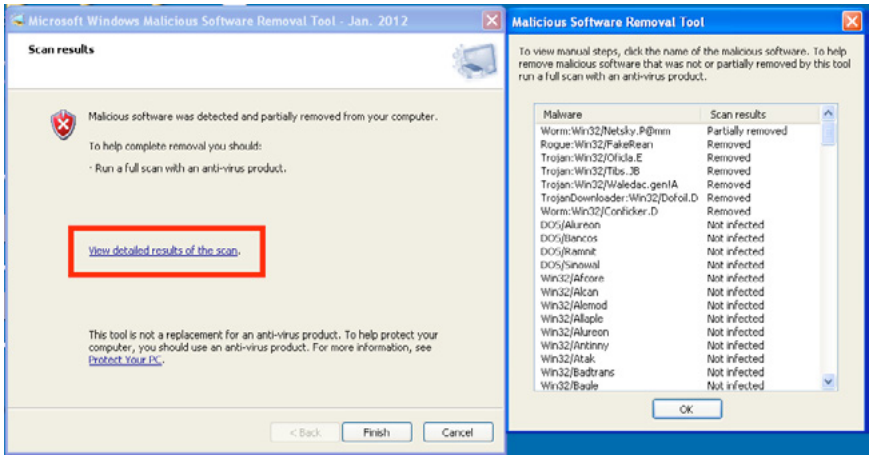
รูปที่ 23 (6-4) แสดง MSRT ขณะตรวจสอบระบบของเครื่องผู้ใช้

4. หลังจาก MSRT ตรวจสอบระบบเสร็จสิ้นแล้ว ในกรณีที่โปรแกรมไม่พบมัลแวร์ในระบบ จะแสดงหน้าต่างดังรูปที่ 24 (6-5)



รูปที่ 24 (6-5) แสดงหน้าต่าง MSRT แจ้งว่าตรวจไม่พบมัลแวร์

5. ในกรณีที่ MSRT ตรวจพบมัลแวร์ จะแสดงรายละเอียดที่พบ โดยผู้ใช้สามารถคลิกลิงก์แสดงผลการสแกน ดังรูปที่ 25 (6-6)



รูปที่ 25 (6-6) แสดงหน้าต่าง MSRT แจ้งว่าตรวจพบมัลแวร์

จะเห็นได้ว่า MSRT นั้น สามารถเพิ่มความมั่นคงปลอดภัยให้กับระบบได้ในระดับหนึ่ง โดยที่ผู้ใช้ไม่ต้องเสียค่าใช้จ่ายและเวลาในการสรรหาหรือติดตั้งโปรแกรม เพียงแค่ทำการตรวจสอบการอัพเดทระบบปฏิบัติการและเรียกใช้ MSRT อยู่เสมอ

อ้างอิง

[6-1] http://netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0&qptimeframe=Y&qpsp=2011

[6-2] http://support.microsoft.com/kb/890830/

[6-3] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=16/

[6-4] http://www.microsoft.com/security/pc-security/malware-removal.aspx

[6-5] http://blogs.computerworld.com/what_you_dont_know_about_the_windows_malicious_software_removal_tool

[6-6] http://www.brighthub.com/computing/smb-security/articles/46694.aspx#

07 9 พฤติกรรมเสี่ยงอันตราย เรื่องง่ายๆ ที่ไม่ควรมองข้าม

ผู้เขียน: เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่: 9 มี.ค. 2555
ปรับปรุงล่าสุด: 11 มี.ค. 2555

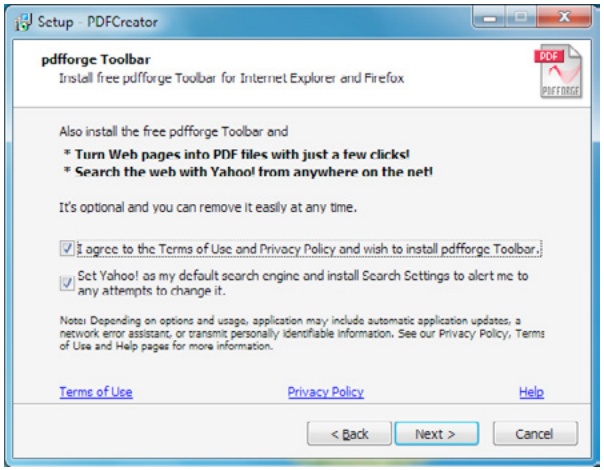
ในการใช้งานคอมพิวเตอร์โดยทั่วไป ผู้ใช้ส่วนใหญ่มักจะไม่ค่อยเห็นความสำคัญของความมั่นคงปลอดภัยเท่าไรนัก เนื่องจากหากกำหนดค่าให้คอมพิวเตอร์มีความมั่นคงปลอดภัยมากๆ ก็จะทำให้การใช้งานในแต่ละวันลำบากขึ้นตามไปด้วย เปรียบเสมือนกับการล็อกประตูบ้านอย่างแน่นหนาด้วยกุญแจหลายสิบชั้น ถึงจะช่วยป้องกันไม่ให้ผู้บุกรุกเข้ามาในบ้านได้ง่าย แต่ก็ทำให้เจ้าของบ้านต้องเสียแรงเสียเวลาไปกับการปลดล็อกกุญแจทั้งหลายสิบ ชั้นนั้นตามไปด้วย ดังนั้นเมื่อผู้ใช้คอมพิวเตอร์ส่วนใหญ่เน้นความสะดวกสบายเป็นหลัก จึงอาจทำให้พฤติกรรมการใช้งานคอมพิวเตอร์ในแต่ละวัน มีความเสี่ยงที่จะถูกโจมตี หรือถูกหลอกลวงจากผู้ไม่หวังดีได้ง่าย มาดูกันว่ามีพฤติกรรมอะไรบ้างที่จะทำให้เกิดความเสี่ยงเหล่านั้น

1. ติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด

เมื่อพูดถึงการติดตั้งโปรแกรมคอมพิวเตอร์ ผู้ใช้ส่วนใหญ่มักจะเข้าใจว่าเป็นการคลิกที่ปุ่ม Next, Next, Next ต่อไปเรื่อยๆ จนสุดท้ายคือคลิกปุ่ม Finish ซึ่งแน่นอนว่า คนที่อ่าน End User License Agreement (EULA) [7-1] หรือพันธะสัญญาทางกฎหมายของแต่ละโปรแกรมนั้นแทบจะไม่มี หรือแม้กระทั่งหากถามว่าในหน้าจอการติดตั้งนั้นมีข้อมูลอะไรปรากฏอยู่บ้าง บางคนเมื่อติดตั้งโปรแกรมเสร็จแล้วก็ยังไม่รู้ด้วยซ้ำ ซึ่งจากพฤติกรรมดังกล่าวนี้ ทำให้มีผู้พัฒนาโปรแกรมหลายราย ใส่ Adware เข้ามาในโปรแกรมของตนด้วย

แล้ว Adware คืออะไร? เนื่องจากผู้พัฒนาโปรแกรมหลายราย เผยแพร่โปรแกรมของตนให้ผู้ใช้สามารถนำไปใช้งานได้ฟรีๆ แต่ทางผู้พัฒนาเองก็มีความจำเป็นต้องใช้เงิน จึงได้ติดต่อกับผู้สนับสนุน เพื่อขอให้ช่วยจ่ายเงินให้กับผู้พัฒนาโปรแกรมนั้นๆ โดยแลกกับการที่จะแนบโปรแกรมของผู้สนับสนุนไปกับโปรแกรมของผู้พัฒนาด้วย ตัวโปรแกรมของผู้สนับสนุนนั้นอาจทำมาเพื่อการประชาสัมพันธ์หรือโฆษณาตัวผู้สนับสนุนเอง ดังนั้นโปรแกรมที่มีลักษณะดังกล่าวนี้จึงถูกเรียกว่า Adware ซึ่งหมายถึง โปรแกรมที่มีโฆษณา การโฆษณานั้นอาจจะมาในหลายรูปแบบ เช่น Toolbar ของโปรแกรมเบราว์เซอร์ หรือการเปลี่ยนหน้าจอ Home page ของเบราว์เซอร์ให้ไปที่เว็บไซต์ของผู้สนับสนุน เป็นต้น ตัวอย่างโปรแกรม Adware ที่พบเห็นได้บ่อย เช่น Google toolbar, Ask.com toolbar เป็นต้น แต่โปรแกรม Adware หลายตัวก็ถูกสร้างขึ้นมาโดยมีวัตถุประสงค์แอบแฝง โดยทำหน้าที่เป็น Spyware ด้วย ซึ่งจะแอบเก็บข้อมูลของผู้ใช้แล้วส่งไปให้กับผู้พัฒนา Adware นั้นๆ [7-2]

ดังนั้น การอ่าน EULA หรือการสังเกตข้อมูลที่ปรากฏในหน้าจอการติดตั้งโปรแกรม จึงเป็นเรื่องสำคัญ เนื่องจากในหลายโปรแกรม ได้เขียนข้อตกลงการใช้งานไว้ว่า ผู้ใช้ต้องยอมให้มีการติดตั้งโปรแกรม Adware ไว้ในเครื่องด้วยถึงจะสามารถใช้งานโปรแกรมนั้นได้ ซึ่งหากผู้ใช้ไม่ยอมรับก็จะไม่สามารถติดตั้งและใช้งานโปรแกรมนั้น ในบางโปรแกรม ระหว่างการติดตั้งจะมีการถามว่าต้องการติดตั้งโปรแกรม Adware ด้วยหรือไม่ ดังรูปที่ 26 (7-1) ซึ่งโปรแกรมโดยส่วนใหญ่จะอนุญาตให้ผู้ใช้สามารถติดตั้งโปรแกรมนั้นได้โดยไม่จำเป็นต้องติดตั้ง Adware



รูปที่ 26 (7-1) หน้าจอการถามว่าต้องการติดตั้งโปรแกรม Adware หรือไม่

หากผู้ใช้เผลอติดตั้ง Adware ไปโดยไม่ตั้งใจ ก็ยังสามารถลบ Adware นั้นออกจากเครื่องได้ง่ายโดยการ Uninstall ออก แต่โปรแกรม Adware บางตัวอาจไม่ยอมให้ผู้ใช้ลบ เพราะถึงแม้จะตามไปลบไฟล์ของ Adware นั้นออกจากระบบแล้ว แต่เมื่อเชื่อมต่อกับอินเทอร์เน็ต Adware นั้นก็จะถูกดาวน์โหลดมาติดตั้งใหม่อยู่ดี ซึ่งการกำจัด Adware ที่มีพฤติกรรมดังกล่าวนี้ จำเป็นต้องใช้โปรแกรมประเภท Anti-Adware หรือ Anti-Spyware ช่วย

2. แอบเล่นอินเทอร์เน็ตไร้สายฟรี

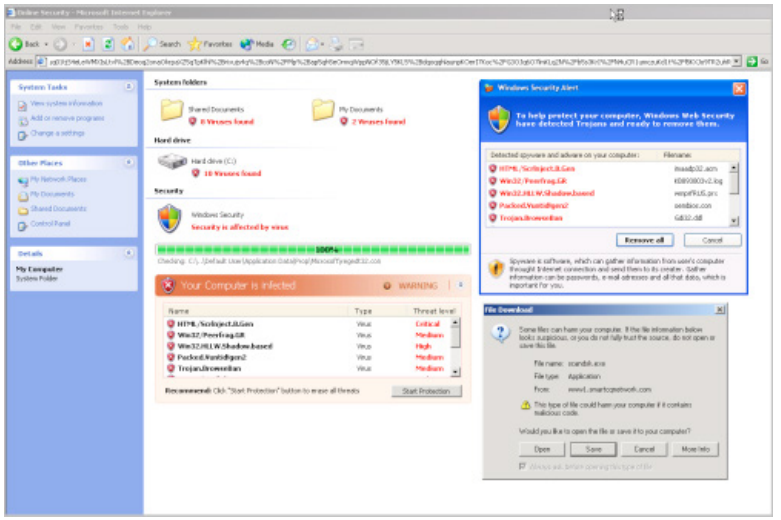
คุณจะทำอย่างไรหากพบว่าสามารถเชื่อมต่อเข้ากับเครือข่ายไร้สายของเพื่อนบ้านที่ปล่อยออกมาให้เล่นอินเทอร์เน็ตได้ฟรีๆ? สิ่งหนึ่งที่ผู้ใช้หลายคนมองข้ามไป คือ เมื่อเครื่องคอมพิวเตอร์เชื่อมต่อเข้ากับระบบเครือ

ข่ายไร้สายใดๆ ก็จะต้องทำการรับส่งข้อมูลกับอุปกรณ์ที่เป็นตัวรับส่งสัญญาณไร้สายนั้นๆ ดังนั้นหากผู้ใช้เชื่อมต่อคอมพิวเตอร์เพื่อแอบเล่นอินเทอร์เน็ตไร้สายของข้างบ้าน ข้อมูลต่างๆ ที่รับส่ง ไม่ว่าจะเป็น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลสำคัญอื่นๆ ก็จะถูกส่งออกไปด้วย ซึ่งแน่นอนว่าหากมีใครที่สามารถเชื่อมต่อเข้ากับระบบไร้สายนี้ได้ แล้วทำการดักรับข้อมูล (Sniff) ก็จะได้ข้อมูลทุกอย่างไปอย่างง่ายดาย

แต่ถึงแม้ผู้ใช้จะมั่นใจว่าใช้การเชื่อมต่อแบบ HTTPS ที่มีการเข้ารหัสลับข้อมูลที่รับส่งแล้วก็ตาม ผู้ที่สร้างระบบเครือข่ายไร้สายอาจทำสิ่งที่เรียกว่า SSL Strip [7-3] ซึ่งเป็นการหลอกผู้ใช้ว่าได้เชื่อมต่อแบบ HTTPS แล้ว ทั้งที่จริงๆ เป็นการเชื่อมต่อแบบ HTTP ธรรมดาก็เป็นได้ โดยเฉพาะอย่างยิ่งในโลกทุกวันนี้ที่อุปกรณ์เคลื่อนที่สามารถหาได้ง่ายและมี ราคาถูก และอุปกรณ์เหล่านั้นสามารถเชื่อมต่อกับอินเทอร์เน็ตแล้วทำหน้าที่เป็น Access point เพื่อให้เครื่องอื่นสามารถเชื่อมต่อเข้ามาเพื่อใช้งานอินเทอร์เน็ตได้ ดังนั้นจึงอาจมีผู้ไม่หวังดีใช้อุปกรณ์เหล่านี้ในการสร้าง Access point ปลอม เพื่อให้มีคนหลงเชื่อแล้วเชื่อมต่อเข้ามา แล้วก็จะได้ข้อมูลที่สำคัญของคนๆ นั้นไป [7-4] ซึ่งสถานที่ที่เหมาะสมในการโจมตีโดยวิธีนี้มักจะเป็นบริเวณที่มีคนอยู่เยอะและมีโอกาสที่คนจะใช้อุปกรณ์เคลื่อนที่ในการเชื่อมต่ออินเทอร์เน็ต เช่น โรงอาหาร หรือ ห้างสรรพสินค้า เป็นต้น ดังนั้น ถึงแม้จะมีอินเทอร์เน็ตมาใช้ฟรีๆ แต่สิ่งที่ต้องเสียไปนั้นอาจมากมายมหาศาลกว่าที่คิดก็เป็นได้

3. ติดตั้งโปรแกรมแอนตี้ไวรัสปลอม

ผู้ใช้จำนวนไม่น้อยถูกหลอกลวงโดย Banner หรือ Popup ที่โผล่ขึ้นมาเมื่อเปิดเว็บไซต์ แล้วหลงเชื่อและติดตั้งโปรแกรมแอนตี้ไวรัสปลอม (Rogue Antivirus) ซึ่งจะมีลักษณะเหมือนกับโปรแกรมแอนตี้ไวรัสธรรมดาทั่วไป แต่มีจุดประสงค์เพื่อหลอกลวงและไม่สามารถกำจัดไวรัสได้จริง เมื่อผู้ใช้เผลอติดตั้งและเรียกใช้งานโปรแกรมแอนตี้ไวรัสปลอม โปรแกรมนั้นจะปรากฏหน้าจอที่ดูเหมือนกับกำลังทำการสแกนไฟล์ในระบบ แล้วจะแจ้งผลการสแกนขึ้นมาแจ้งว่ามีโปรแกรมอันตรายอยู่ในระบบอยู่เป็นจำนวน มาก แต่ผู้ใช้จะยังไม่สามารถกำจัดโปรแกรมอันตรายเหล่านั้นออกได้ จนกว่าจะจ่ายเงินให้กับผู้พัฒนาโปรแกรมแอนตี้ไวรัสปลอมนี้ก่อน ดังรูปที่ 27 (7-2) โปรแกรม แอนตี้ไวรัสปลอมหลายตัว นอกจากจะไม่สามารถกำจัดไวรัสได้แล้ว ยังดาวน์โหลดโปรแกรมอันตรายอื่นๆ มาติดตั้งเพิ่มเติมในเครื่องของผู้ใช้ด้วย



รูปที่ 27 (7-2) ตัวอย่างโปรแกรมแอนตี้ไวรัสปลอม (ที่มา The Hacker News [7-5])

โปรแกรม ที่ทำงานในลักษณะแบบนี้มีชื่อเรียกว่า Rogueware หรือ Scareware ซึ่งมีความหมายโดยรวมหมายถึงโปรแกรมที่หลอกลวงผู้ใช้ให้ทำการจ่ายเงิน [7-6] โดยทั่วไป Rogueware มักจะมาในรูปแบบของโปรแกรมรักษาความมั่นคงปลอดภัย เนื่องจากง่ายต่อการล่อลวงให้ผู้ใช้ดาวน์โหลดโปรแกรมไปทำการติดตั้ง เช่น อาจจะทำ Banner หรือ Popup ที่ปรากฏขึ้นเมื่อผู้ใช้เข้าสู่เว็บไซต์ โดยเนื้อหาของข้อความข้างในนั้นจะเป็นการแจ้งเตือนว่าตรวจพบโปรแกรมอันตราย อยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้ ต้องรีบดาวน์โหลดโปรแกรมแอนตี้ไวรัสไปทำการตรวจสอบโดยด่วน [7-7]

ในการป้องกันตัวจาก Rogueware ก่อนทำการดาวน์โหลดโปรแกรมที่เกี่ยวข้องกับความมั่นคงปลอดภัย ผู้ใช้ควรตรวจสอบรายชื่อโปรแกรมใน List of rogue security software [7-8] เพื่อให้แน่ใจว่าจะได้ไม่ตกเป็นเหยื่อของโปรแกรมหลอกลวง

4. คลิกลิงก์หรือเปิดไฟล์แนบที่มากับอีเมลโดยไม่ตรวจสอบ

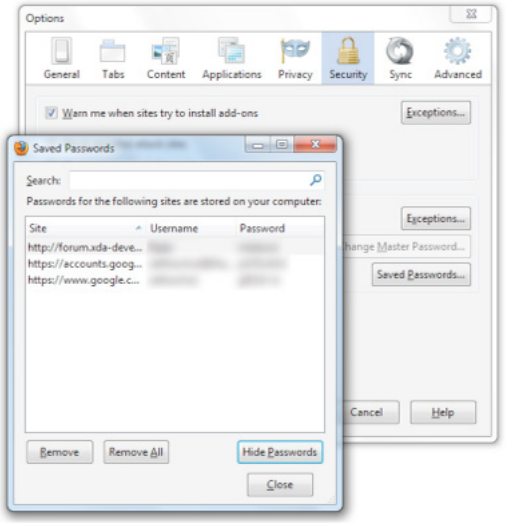
การโจมตีผ่านอีเมล เป็นวิธีการที่มีมานานแล้ว และปัจจุบันก็ยังคงใช้ได้ผล ซึ่งวิธีการโจมตีก็มีหลายรูปแบบแตกต่างกันไป ไม่ว่าจะเป็นการโจมตีแบบสร้างความเสียหายน้อย เช่น เผยแพร่ข่าวสารหลอกลวง (Hoax) ซึ่งมีจุดมุ่งหมายเพื่อให้คนหลงเชื่อและทำการส่งต่อ (Forward) อีเมลฉบับนั้นไปให้ได้เยอะๆ เพื่อให้ผู้ที่เผยแพร่ข่าวสารหลอกลวงนั้นจะได้ทำการรวบรวมรายชื่ออีเมล และจะได้ทำการส่งสแปม (Spam) ออกไป เป็นต้น [7-9]

ส่วนการโจมตีที่มีจุดประสงค์เพื่อต้องการสร้างความเสียหายก็มีหลายแบบ ไม่ว่าจะเป็น การสร้างหน้าเว็บไซต์หลอกลวง (Phishing) แล้วเผยแพร่ลิงก์ของเว็บไซต์นั้นทางอีเมล ซึ่งเป้าหมายของการทำหน้าเว็บไซต์หลอกลวงโดยส่วนใหญ่จะปลอมเป็นเว็บไซต์ของ สถาบันการเงิน เช่น ผู้โจมตีจะสร้างหน้า Login ให้เหมือนกับหน้าเว็บไซต์ของธนาคาร เพื่อหลอกให้ลูกค้าของธนาคารนั้นหลงเชื่อและกรอกข้อมูลชื่อผู้ใช้และรหัส ผ่านลงไป ข้อสังเกตของอีเมล Phishing คือ จะมีลิงก์ที่บอกว่าเป็นเว็บไซต์ของธนาคารอยู่ในอีเมลแต่ URL ของลิงก์นั้นไม่ใช่เว็บไซต์ของธนาคารที่ถูกกล่าวอ้าง [7-10]

การเผยแพร่มัลแวร์ (Malware) ด้วยวิธีการแนบไฟล์มากับอีเมลนั้นปัจจุบันก็ยังคงได้ผลอยู่ ถึงแม้ว่าผู้ให้บริการอีเมลหลายรายจะมีบริการสแกนไวรัสในไฟล์แนบทั้งอีเมลที่ได้รับเข้ามาแล้วอีเมลที่ถูกส่งออกไปแล้วก็ตาม [7-11] แต่ก็ยังมีโอกาสที่มัลแวร์บางตัวจะหลุดรอดการตรวจจับและเข้ามาอยู่ในกล่องอีเมลของผู้ใช้ได้ ปัจจุบันมัลแวร์ไม่ได้เผยแพร่ผ่านไฟล์ที่มีนามสกุล .exe เพียงอย่างเดียว แต่ยังสามารถเผยแพร่ผ่านไฟล์เอกสารทั่วไป เช่น ไฟล์ของโปรแกรม Office ไฟล์ .pdf หรือแม้กระทั่งไฟล์รูปภาพได้อีกด้วย [7-12] ดังนั้นควรตรวจสอบกับผู้ส่ง และทำการสแกนไวรัสก่อนเปิดไฟล์แนบทุกครั้ง

5. Remember my password

ความสามารถหนึ่งของโปรแกรมเบราว์เซอร์ที่คนส่วนใหญ่นิยมใช้ คือ การสั่งให้เบราว์เซอร์จำชื่อผู้ใช้และรหัสผ่านของเว็บไซต์นั้น เพื่อจะได้ไม่ต้องพิมพ์ใหม่ในภายหลัง ซึ่งวิธีการที่ว่านี้ก็สามารถทำได้ง่ายๆ โดยการคลิกที่ปุ่ม Remember my password เมื่อล็อกอินเข้าสู่เว็บไซต์ แต่การสั่งให้เบราว์เซอร์จำรหัสผ่านก็มีข้อเสียเช่นกัน คือ หากเครื่องคอมพิวเตอร์สูญหายหรือถูกเข้าถึงได้โดยบุคคลอื่น ผู้ที่สามารถเข้าถึงโปรแกรมเบราว์เซอร์ได้ก็จะสามารถเข้าใช้งานเว็บไซต์ที่ ถูกสั่งให้จำรหัสผ่านได้เลย แต่ที่สำคัญกว่านั้น คือ เบราว์เซอร์โดยส่วนใหญ่อนุญาตให้ผู้ใช้สามารถดูรหัสผ่านทั้งหมดที่ถูกเก็บ ไว้ได้ง่ายเพียงแค่ไม่กี่คลิก ดังรูปที่ 28 (7-3)



รูปที่ 28 (7-3) ตัวอย่างการแสดงรหัสผ่านทั้งหมดที่เก็บไว้ใน Mozilla Firefox

อย่างไรก็ตาม ในบางเบราว์เซอร์ เช่น Mozilla Firefox ผู้ใช้สามารถกำหนด Master Password เพื่อป้องกันการแอบดูรหัสผ่านที่ถูกบันทึกไว้ได้ โดยผู้ที่ต้องการดูข้อมูลรหัสผ่าน จะต้องใส่ Master Password ให้ถูกต้องถึงจะสามารถเข้าดูได้ [7-13]

6. เปิดใช้งานฟังก์ชั่น Autorun ใน Removable drive

Autorun เป็นความสามารถหนึ่งของ Windows ที่ใช้ระบุว่า เมื่อเชื่อมต่อดิสก์เข้ากับเครื่องคอมพิวเตอร์แล้วจะทำอะไรต่อไป ตัวอย่างประโยชน์ของฟังก์ชั่น Autorun เช่น เมื่อใส่แผ่นซีดีสำหรับติดตั้งโปรแกรมเข้าไปในไดรฟ์ จะปรากฏหน้าจอการติดตั้งโปรแกรมขึ้นมาโดยอัตโนมัติ ซึ่งการกระทำดังกล่าวนี้จะถูกระบุในไฟล์ชื่อ autorun.inf ซึ่งเป็นไฟล์ข้อความธรรมดา [7-14] ฟังก์ชั่น Autorun นอกจากจะทำงานเมื่อเชื่อมต่อดิสก์เข้ากับเครื่องแล้ว หากว่าผู้ใช้ทำการดับเบิ้ลคลิกที่ไอคอนของไดรฟ์นั้น ฟังก์ชั่น Autorun ก็จะถูกเรียกใช้งานเช่นกัน

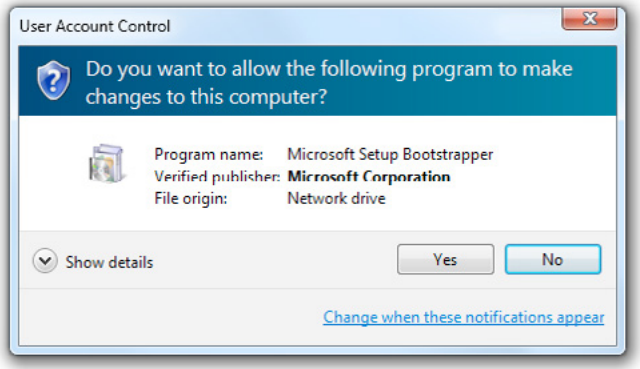
จากประโยชน์ของฟังก์ชั่น Autorun ที่สามารถสั่งให้ระบบเปิดโปรแกรมที่กำหนดโดยอัตโนมัติเมื่อผู้ใช้เชื่อมต่อ ไดรฟ์หรือดับเบิ้ลคลิกที่ไอคอน ทำให้มีผู้พัฒนามัลแวร์ที่เผยแพร่ผ่านทาง USB Drive เนื่องจากมีการใช้งานที่แพร่หลายและสามารถเขียนไฟล์ได้ ที่สำคัญ ผู้ใช้งานส่วนใหญ่นิยมเปิดดูข้อมูลใน USB Drive ด้วยการดับเบิ้ลคลิกที่ไอคอน ทำให้มัลแวร์แพร่กระจายได้ไม่ยาก

ดังนั้น ก่อนที่จะเปิดดูข้อมูลใน USB Drive ควรทำการสแกนไวรัส รวมถึงใช้โปรแกรมประเภท Auto-run remover เพื่อลบไฟล์ autorun.inf ออกจาก USB Drive ด้วย นอกจากนี้ การปิดฟังก์ชั่น Autorun ใน Windows ก็ยังสามารถช่วยป้องกันปัญหานี้ได้ โดย Microsoft ได้เผยแพร่โปรแกรมอัพเดทหมายเลข 967940 เพื่อปิดการทำงานของฟังก์ชั่น Autorun ในไดรฟ์แบบถอดได้ (Removable drive) เพื่อช่วยลดการแพร่กระจายของไวรัส Autorun [7-15]

7. Login เป็น Administrator

ในระบบปฏิบัติการ Windows มีการแบ่งประเภทของบัญชีผู้ใช้ออกเป็น 2 แบบ คือ Administrator และ Limited โดยที่ Administrator หมายถึงผู้ดูแลระบบ ซึ่งมีสิทธิในการทำงานทุกอย่างในระบบ ไม่ว่าจะเป็นการติดตั้งโปรแกรม แก้ไขการตั้งค่าของระบบ รวมถึงสร้างบัญชีผู้ใช้ใหม่ ส่วน Limited หมายถึงผู้ใช้งานธรรมดา ที่ถูกจำกัดสิทธิให้สามารถเข้าใช้งานหรือเปลี่ยนแปลงการตั้งค่าของระบบได้ ภายในขอบเขตที่ถูกกำหนดเท่านั้น เช่น ไม่สามารถติดตั้งโปรแกรมเพิ่มเติมได้ เป็นต้น [7-16] เนื่องจากข้อจำกัดของบัญชีผู้ใช้แบบ Limited ทำให้ผู้ใช้ทั่วไปนิยมใช้งานคอมพิวเตอร์โดยใช้สิทธิของ Administrator ซึ่งหากผู้ใช้เผลอเรียกใช้งานโปรแกรมมัลแวร์ ก็จะทำให้ระบบติดมัลแวร์นั้นได้โดยง่าย

ตั้งแต่ Windows Vista เป็นต้นมา ได้มีการพัฒนาระบบ User Account Control (UAC) ซึ่งจะกำหนดไม่ให้ผู้ใช้งานระบบมีสิทธิเป็น Administrator เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับระบบ หากผู้ใช้จำเป็นต้องใช้งานสิทธิของผู้ดูแลระบบ เช่น ติดตั้งโปรแกรม หรือ เปิดโปรแกรมที่มีสิทธิแก้ไขค่าของระบบ ก็จะปรากฏหน้าจอเพื่อสอบถามความต้องการและให้ผู้ใช้คลิกเพื่อยืนยันการทำงาน อีกที [7-17] ตัวอย่างหน้าจอของระบบ User Account Control เป็นดังรูปที่ 29 (7-4)



รูปที่ 29 (7-4) ตัวอย่างหน้าจอของระบบ User Account Control (ที่มา MSDN [7-17])

ผู้ใช้หลายรายปิดการทำงานของระบบ User Account Control หรือเข้าสู่ระบบโดยใช้สิทธิของ Administrator ซึ่งนั่นอาจเป็นช่องทางหนึ่งที่ทำให้ระบบถูกโจมตีจากมัลแวร์ได้ง่าย สิ่งสำคัญที่ควรคำนึง คือ

ความสะดวกสบายและความมั่นคงปลอดภัย เป็นสิ่งที่อยู่ตรงข้ามกัน ดังนั้นหากเพิ่มความสะดวกสบายจนเกินไป ก็อาจไม่มีความมั่นคงปลอดภัยเหลืออยู่เลยก็เป็นได้

8. ปิด Windows Update

Windows Update เป็นระบบที่ Microsoft สร้างขึ้นมาเพื่อปรับปรุงแก้ไขช่องโหว่ของระบบปฏิบัติการ Windows และซอฟต์แวร์อื่นของ Microsoft ที่ติดตั้งอยู่ในระบบ โดยทั่วไปแล้ว Microsoft จะเผยแพร่อัพเดทย่อยในทุกสัปดาห์ และจะเผยแพร่อัพเดทใหญ่ที่แก้ไขช่องโหว่ร้ายแรงในวันอังคารที่สองของทุกเดือน โดยใช้ชื่อเรียกว่า Patch Tuesday [7-18]

ปกติแล้วเมื่อระบบ Windows Update ตรวจสอบพบว่ามีการเผยแพร่อัพเดทใหม่ออกมา ก็จะทำการดาวน์โหลดและติดตั้งอัพเดทใหม่นั้นโดยอัตโนมัติ แต่ผู้ใช้หลายรายทำการปิดระบบ Windows Update ด้วยเหตุผลบางประการ เช่น ไม่มีอินเทอร์เน็ต เชื่อมต่อกับอินเทอร์เน็ตความเร็วต่ำ หรือใช้งาน Windows แบบละเมิดลิขสิทธิ์ เป็นต้น จึงทำให้ไม่สามารถติดตั้งการอัพเดทล่าสุดได้

การปิด Windows Update นั้นทำให้ระบบมีความเสี่ยงต่อการถูกโจมตีจากช่องโหว่ 0-day ซึ่งเป็นช่องโหว่ที่ได้รับการเปิดเผยแล้วแต่ยังไม่ได้มีการแก้ไข [7-19] หากเป็นไปได้ ผู้ใช้ควรดาวน์โหลดอัพเดทที่แก้ไขช่องโหว่ร้ายแรงมาทำการติดตั้งด้วยตนเอง ซึ่งสามารถดาวน์โหลดได้จากเว็บไซต์ของ Microsoft สามารถติดตั้งได้โดยไม่ต้องเชื่อมต่ออินเทอร์เน็ต

9. ไม่อัพเดทโปรแกรมแอนตี้ไวรัส

โปรแกรมแอนตี้ไวรัสจะมีวิธีการตรวจสอบไวรัสโดยหลักๆ อยู่ 2 วิธี คือ ตรวจสอบจาก Signature และตรวจสอบแบบ Heuristics โดยการตรวจสอบจาก Signature นั้นจะเป็นการวิเคราะห์ว่าไฟล์ที่ตรวจสอบนั้นมีลักษณะเฉพาะตรงกับข้อมูลของ ไวรัสที่มีอยู่หรือเปล่า ถ้าตรงกัน ก็แสดงว่าไฟล์นั้นมีโอกาสที่จะเป็นไวรัส การตรวจสอบด้วยวิธีนี้มีข้อดีคือทำงานได้เร็วและมีโอกาสผิดพลาดน้อย แต่มีข้อเสียคือถ้าเจอไวรัสที่ไม่รู้จักมาก่อนและไม่มีในฐานข้อมูล ก็จะไม่สามารถตรวจจับไวรัสนั้นได้ ส่วนการตรวจสอบแบบ Heuristics จะไม่ได้ดูเนื้อหาของไฟล์ แต่จะเป็นการวิเคราะห์พฤติกรรมของโปรแกรม ว่ามีการทำงานที่เข้าข่ายที่จะสร้างความเสียหายให้กับระบบหรือเปล่า ถ้าใช่ก็จะแจ้งเตือนให้กับผู้ใช้ทราบ ข้อดีของวิธีนี้คือสามารถตรวจจับไวรัสที่ไม่เคยรู้จักมาก่อนได้ แต่ข้อเสียคือมีโอกาสสูงที่จะมองว่าโปรแกรมที่ทำงานตามปกตินั้นเป็นไวรัส [7-20] [7-21]

โดยทั่วไปแล้ว โปรแกรมแอนตี้ไวรัสส่วนใหญ่จะเน้นไปที่การตรวจสอบไวรัสจาก Signature เป็นหลัก หากผู้พัฒนาโปรแกรมแอนตี้ไวรัสค้นพบไวรัสชนิดใหม่ ก็จะสร้างไฟล์ Signature update แล้วเผยแพร่ออกมาให้ผู้ใช้งานโปรแกรมแอนตี้ไวรัสดาวน์โหลดไปอัพเดทฐานข้อมูล ของโปรแกรม หากผู้ใช้ไม่ทำการอัพเดทฐานข้อมูล โปรแกรมก็อาจจะไม่สามารถตรวจจับไวรัสชนิดใหม่ได้ และที่สำคัญ ผู้พัฒนาโปรแกรมแอนตี้ไวรัสหลายราย จะไม่อนุญาตให้ผู้ที่ใช้ซอฟต์แวร์แอนตี้ไวรัสแบบละเมิดลิขสิทธิ์เข้าไปดาวน์โหลดไฟล์อัพเดท

ฐานข้อมูลไวรัสได้ ดังนั้นต่อให้ผู้ใช้ใช้งานโปรแกรมแอนตี้ไวรัสที่ทำงานได้ดีขนาดไหน แต่ถ้าไม่อัพเดท ก็จะตรวจจับไวรัสไม่ได้ผล

สรุป

เครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบอินเทอร์เน็ตได้ มีโอกาสเสี่ยงที่จะถูกโจมตีง่ายกว่าเครื่องที่ไม่ได้เชื่อมต่ออินเทอร์เน็ต ดังนั้นหากมีการใช้งานอินเทอร์เน็ตอยู่เป็นประจำ ผู้ใช้ควรติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับความมั่นคงปลอดภัยอยู่อย่างสม่ำเสมอ เพราะนอกจากที่จะป้องกันระบบของตนแล้ว ยังช่วยป้องกันไม่ให้เครื่องคอมพิวเตอร์ที่ใช้งานอยู่ถูกใช้เป็นเครื่องมือในการโจมตีผู้อื่นด้วย

พฤติกรรมการใช้งานหลายอย่าง เป็นสาเหตุหลักที่ทำให้เกิดความเสี่ยงในเรื่องของความมั่นคงปลอดภัย และเป็นช่องทางให้ผู้ไม่หวังดีใช้ในการโจมตีระบบ ดังนั้นการป้องกันภัยคุกคามที่ดีที่สุดจึงเป็นการป้องกันที่ตัวผู้ใช้ นั่นเอง

อ้างอิง

[7-1] http://www.webopedia.com/TERM/E/EULA.html
[7-2] http://books.google.com/books?id=Fo2a7YtU1GUC&pg=PA10
[7-3] http://www.thoughtcrime.org/software/sslstrip/
[7-4] http://www.wi-fiplanet.com/tutorials/article.php/1564431
[7-5] http://thehackernews.com/2012/03/rogue-antivirus-advertised-on-200000.html
[7-6] http://www.pandasecurity.com/img/enc/The Business of Rogueware.pdf
[7-7] http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx
[7-8] http://en.wikipedia.org/wiki/List_of_rogue_security_software
[7-9] http://urbanlegends.about.com/cs/nethoaxes/ht/emailhoax.htm
[7-10] http://www.webopedia.com/TERM/P/phishing.html
[7-11] http://support.google.com/mail/bin/answer.py?hl=en&answer=25760
[7-12] http://computer.howstuffworks.com/question339.htm
[7-13] http://kb.mozillazine.org/Master_password
[7-14] http://msdn.microsoft.com/en-us/library/cc144206(VS.85).aspx
[7-15] http://technet.microsoft.com/en-us/security/advisory/967940
[7-16] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua_c_account_types.mspx?mfr=true
[7-17] http://msdn.microsoft.com/en-us/library/windows/desktop/aa511445.aspx
[7-18] http://download.microsoft.com/download/a/9/4/a94af289-a798-4143-a3f8-77004f7c2fd3/Windows Update Explained.docx
[7-19] http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm
[7-20] http://www.antivirusworld.com/articles/antivirus.php
[7-21] http://antivirus.about.com/od/antivirusglossary/g/heuristics.htm

08 PASSWORD1 สัญญาณอันตรายที่มากับรหัสผ่าน

ผู้เขียน: พรพรหม ประภากิตติกุล
วันที่เผยแพร่: 23 มี.ค. 2555

ปรับปรุงล่าสุด: 23 มี.ค. 2555

เมื่อตั้งคำถามถึงการรักษาความมั่นคงปลอดภัยบนระบบคอมพิวเตอร์ ผู้ใช้งานหลายท่านอาจให้คำนิยามด้วยภาพของการเข้าสู่ระบบปฏิบัติการหรือการเข้าสู่หน้าเว็บไซต์ด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นอย่างแรก เนื่องจากเป็นวิธีการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์แบบหนึ่งที่พบได้บ่อยครั้งเมื่อมีความต้องการเข้าใช้งานข้อมูลที่เป็นส่วนบุคคลหรือเป็นความลับ แต่ระบบคอมพิวเตอร์ที่ให้ล็อกอินโดยการใช้งานชื่อผู้ใช้และรหัสผ่าน ก็มีความเสี่ยงสูงต่อการถูกโจมตี เนื่องจากปัจจัยที่จะทำให้การถูกโจมตีสำเร็จนั้น มักขึ้นอยู่กับการตั้งค่ารหัสผ่านของผู้ใช้งานเป็นหลัก หากรหัสผ่านที่ใช้งานไม่มีความมั่นคงปลอดภัยแล้วนั้น ก็เท่ากับเปิดโอกาสให้ผู้โจมตีสามารถคาดเดารหัสผ่านเพื่อเข้าถึงระบบคอมพิวเตอร์ได้โดยง่าย

ตามรายงานข่าวจาก CNN มีการระบุว่าบริษัทวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ที่ชื่อว่า Trustwave ได้เปิดเผยรายงานที่เกี่ยวข้องกับสถิติการใช้งานรหัสผ่านในเอกสาร “Trustwave 2012 Global Security Report” [8-1] โดยมีเนื้อหาที่เกี่ยวข้องว่าองค์กรทางด้านธุรกิจทั่วโลกมีการใช้รหัสผ่าน “Password1” อย่างแพร่หลายและอาจเป็นสาเหตุส่วนใหญ่ที่ทำให้ระบบคอมพิวเตอร์ขององค์กรต่างๆ ถูกเข้าควบคุมได้สำเร็จจากการโจมตีผ่านการล็อกอินด้วยรหัสผ่านดังกล่าว และจากข้อมูลเพิ่มเติมพบว่ารหัสผ่านดังกล่าวเป็นค่าที่ได้จากการกำหนดค่า Default Password ที่ได้จากบริการของ Microsoft Active Directory [8-2] [8-3] ที่เป็นบริการที่ใช้สำหรับบริหารจัดการสิทธิผู้ใช้งานบนเครือข่ายโดเมนของระบบปฏิบัติการวินโดวส์ ซึ่งอาจทำให้ผู้ใช้งานบางคนอาจเข้าใจว่ารหัสผ่านดังกล่าวมีความซับซ้อนอยู่แล้วจึงไม่ดำเนินการเปลี่ยนรหัสผ่าน

จากรายงานข้างต้นแสดงให้เห็นถึงสภาพปัญหาสำคัญของการใช้งานระบบคอมพิวเตอร์จากทั่วโลกว่ายังคงขาดความใส่ใจในเรื่องความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานรหัสผ่านและการขาดกระบวนการตรวจสอบที่ดี ซึ่งในกรณีที่เป็นระบบขององค์กรที่มีความสำคัญและถูกขโมยบัญชีผู้ใช้งานไปได้ อาจส่งผลกระทบร้ายแรงทำให้องค์กรนั้นหมดความน่าเชื่อถือจากลูกค้า และไม่สามารถประเมินค่าความเสียหายที่จะเกิดขึ้นในอนาคตหากยังเปิดโอกาสให้ผู้โจมตีเข้ามายังระบบได้ง่ายดายเช่นนี้ บทความนี้จะรวบรวมข้อมูลแนวทางการใช้งานรหัสผ่าน เพื่อให้ผู้อ่านสามารถนำไปปรับใช้งานกับการใช้งานในระบบหรือบริการต่างๆ ที่ต้องการได้ โดยมีรายละเอียดดังนี้

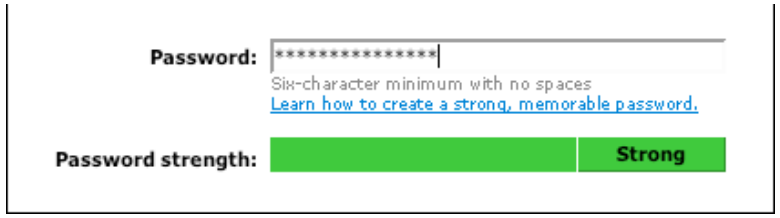
1.ไม่ใช้ Default Password

Default Password หรือค่ารหัสผ่านเริ่มต้นของอุปกรณ์หรือซอฟต์แวร์ หมายถึง รหัสผ่านที่ถูกตั้งค่ามาจากผู้พัฒนาอุปกรณ์หรือซอฟต์แวร์ตั้งแต่ครั้งแรก เช่น รหัสผ่านสำหรับล็อกอินระบบบริหารจัดการของอุปกรณ์ Router ที่มีการตั้งค่ามาจากผู้พัฒนา หรือกรณีที่ใช้เทมเพลตของรหัสผ่านที่ออกแบบโดยระบบ Active Directory ดังเช่นในตัวอย่างรายงานที่ได้กล่าวไป โดยมีจุดประสงค์หลักเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่เกี่ยวข้อง แต่ช่องโหว่ของการใช้งานรหัสผ่านแบบ Default Password คือ รหัสผ่านมักจะเป็นค่าเดียวกันทั้งผลิตภัณฑ์หรือรุ่นนั้นๆ และเมื่อผู้ใช้งานไม่เปลี่ยนแปลงค่ารหัสผ่านเริ่มต้น ก็สามารถทำให้รหัสผ่านเหล่านี้ถูกคาดเดาเพื่อใช้ในการโจมตีได้ไม่ยาก เพราะปัจจุบันข้อมูลรหัสผ่านเหล่านี้สามารถค้นหาได้ทั่วไปบนเว็บไซต์อินเทอร์เน็ต ดังเช่นเว็บไซต์ในรูปที่ 30 (8-1) ซึ่งเป็นแหล่งรวบรวมข้อมูล Default Password จากผู้ให้บริการเกี่ยวกับระบบคอมพิวเตอร์ทั่วโลก

รูปที่ 30 (8-1) ตัวอย่างเว็บไซต์ที่รวบรวม Default Password จากผู้ให้บริการ

2. ตั้งค่ารหัสผ่านที่มีความซับซ้อน

ผู้ใช้งานหลายท่านคงเคยได้ยินคำเตือนจากผู้เกี่ยวข้องด้านความมั่นคงปลอดภัยให้เปลี่ยนรหัสผ่านส่วนตัวให้เป็นรหัสผ่านที่มีความซับซ้อน หรือบางท่านอาจพบเห็นด้วยตัวเองจากการใช้งานหน้าเว็บไซต์ต่างๆ ที่มีการแจ้งเตือนให้ตั้งค่ารหัสผ่านที่มีความมั่นคงหรือที่เรียกว่า Password Strength ดังเช่นตัวอย่างในรูปที่ 31 (8-2) ซึ่งทั้งหมดที่กล่าวมาถือเป็นคำนิยามเดียวกัน โดยมีจุดประสงค์เพื่อลดโอกาสที่ผู้โจมตีจะสามารถคาดเดารหัสผ่านของผู้ใช้งานได้โดยง่าย เนื่องจากคำว่ารหัสผ่านที่มีความซับซ้อนจะหมายถึง รหัสผ่านที่คาดเดายาก ซึ่งประกอบไปด้วย ตัวเลข อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ อักษรภาษาอังกฤษตัวพิมพ์เล็ก และอักขระพิเศษ โดยอาจจะมีหลักเกณฑ์เพิ่มเติม เช่น ต้องกำหนดความยาวของรหัสผ่านมากกว่า 8 ตัวอักษร ผู้ใช้งานควรปรับทัศนคติว่ารหัสผ่านที่ซับซ้อนจะทำให้จำได้ยาก และปรับทัศนคติที่ว่าการตั้งค่ารหัสผ่านโดยการเลือกใช้ข้อมูลเฉพาะกลุ่ม เช่น ใช้เฉพาะข้อมูลกลุ่มที่เป็นตัวเลข มีโอกาสเสี่ยงต่อการถูกโจมตีสำเร็จสูง เนื่องจากความน่าจะเป็นมีขอบเขตน้อย ยกตัวอย่างเช่น หากมีการตั้งค่ารหัสผ่าน 5 หลักเป็นตัวเลขทั้งหมด จะเทียบเท่ากับมีโอกาสที่จะสุ่มรหัสผ่านถูกต้องไม่เกิน 500 ครั้ง โดยอาศัยการผสมของอักขระพิเศษและพยัญชนะรูปแบบต่างๆ เช่น ตัวเลข พยัญชนะภาษาอังกฤษตัวเล็ก พยัญชนะภาษาอังกฤษตัวใหญ่ เป็นต้น



รูปที่ 31 (8-2) แสดงการตั้งรหัสผ่านที่มีความซับซ้อนคาดเดายากจากเว็บไซต์ hotmail.com

3. ไม่ตั้งค่ารหัสผ่านใหม่ซ้ำกับรหัสผ่านก่อนหน้า

ผู้ใช้งานหลายท่านคงเคยเห็นอีเมลแจ้งเตือนให้เปลี่ยนรหัสผ่าน ตามช่วงเวลาที่องค์กรหรือระบบที่ให้บริการต่างๆได้กำหนดไว้ ส่วนใหญ่มักจะเป็นไปตามนโยบายขององค์กรที่ต้องการให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่เพื่อความมั่นคงปลอดภัย แต่ก็ยังพบว่าผู้ใช้งานอีกหลายคนที่มีแนวคิดตรงกันข้ามคือต้องการใช้รหัสผ่านเดิมไปตลอด เพราะฉะนั้นเมื่อถึงรอบเปลี่ยนรหัสผ่าน ผู้ใช้งานกลุ่มนี้ก็จะทำการเพื่อเปลี่ยนรหัสผ่านแต่การเปลี่ยนรหัสผ่านที่ว่าคือการเปลี่ยนไปเป็นรหัสผ่านตัวเดิม หรือในกรณีที่ระบบออกแบบมาให้มีตรวจสอบว่าการเปลี่ยนรหัสผ่านจะต้องไม่ซ้ำเดิมเป็นจำนวน 3 ครั้ง ผู้ใช้งานก็จะทำการเปลี่ยนรหัสผ่านเป็นจำนวนทั้งหมด 4 ครั้ง โดยครั้งสุดท้ายก็จะยังคงเปลี่ยนเป็นรหัสผ่านเดิม เพื่อหลีกเลี่ยงกระบวนการตรวจสอบนี้ ซึ่งเป็นสิ่งที่ไม่ควรทำอย่างยิ่งเพราะนอกจากจะผิดจุดประสงค์ของการเปลี่ยนรหัสผ่านแล้ว ยังเท่ากับเพิ่มโอกาสที่จะทำให้ผู้โจมตีสามารถเจาะรหัสผ่านได้ เพราะฉะนั้นทางเลือกที่ดีที่สุดคือการเปลี่ยนรหัสผ่านที่ไม่ซ้ำกับค่าเดิม รวมถึงระบบที่ให้บริการก็ต้องมีกระบวนการที่ไม่ยอมให้ผู้ใช้งานสามารถตั้งค่ารหัสผ่านซ้ำเดิมด้วย โดยอาจจะดำเนินการพัฒนากระบวนการตรวจสอบเพิ่มเติมเช่น ระบบที่ให้บริการเปลี่ยนรหัสผ่านต้องมีกระบวนการตรวจสอบรหัสผ่านที่จะตั้งค่าใหม่กับรหัสผ่านเดิมทุกครั้ง หรือให้มีกระบวนการทำ Minimum password age [8-4] เพื่อกำหนดช่วงเวลาที่อนุญาตให้ผู้ใช้งานสามารถเข้ามาเปลี่ยนรหัสผ่านได้อีกครั้ง

4. ไม่ตั้งค่ารหัสผ่านที่เหมือนกันทุกระบบ

การตั้งค่ารหัสผ่านให้เหมือนกันในทุกระบบไม่ว่าจะเป็น อีเมล ระบบงาน ระบบปฏิบัติการ หรือระบบใดก็ตามล้วนแล้วแต่เป็นการเพิ่มช่องทางที่จะทำให้ความเสียหายขยายตัวได้ง่ายมากยิ่งขึ้น ยกตัวอย่างเช่น กรณีของผู้ใช้งานที่มีบัญชีผู้ใช้งานเว็บไซต์เฟซบุ๊ค (Facebook) ที่ใช้รหัสผ่านเดียวกับบัญชีผู้ใช้งานจีเมล (Gmail) โดยเมื่อพบว่ารหัสผ่านของผู้ใช้งานถูกขโมยจากระบบใดระบบหนึ่งแล้ว เท่ากับผู้ใช้งานคนนั้นมีความเสี่ยงสูงที่จะถูกเข้าถึงอีกระบบหนึ่งที่ใช้รหัสผ่านเดียวกันได้โดยง่าย ซึ่งแสดงให้เห็นว่าการเลือกใช้รหัสผ่านเดียวกันในทุกระบบย่อมส่งผลเสียได้เร็วและง่ายขึ้น แต่ในปัจจุบันจะพบว่าในองค์กรใหญ่ๆที่มีผู้ใช้งานมากมักจะมีการประยุกต์ใช้ระบบการเก็บรหัสผ่านที่เดียวเพื่อรองรับการเข้าถึงข้อมูลบัญชีการล็อกอินที่เหมือนกันในทุกระบบหรือที่เรียกว่า Centralize Authentication [8-5] เพื่อให้ผู้ใช้งานมีความสะดวกมากยิ่งขึ้นและลดความซับซ้อนของการเก็บข้อมูลบัญชีผู้ใช้งานรวมถึงรหัสผ่าน เพราะฉะนั้นรหัสผ่านที่ใช้ในกรณีนี้จำเป็นจะต้องมีการรักษาความมั่นคงปลอดภัยที่ดีมาก ซึ่งอาจสามารถทำตามคำแนะนำทั้งหมดในบทความนี้ เพื่อลดโอกาศที่จะถูกผู้บุกรุกสามารถเข้าถึงข้อมูลสำคัญได้ทั้งหมด

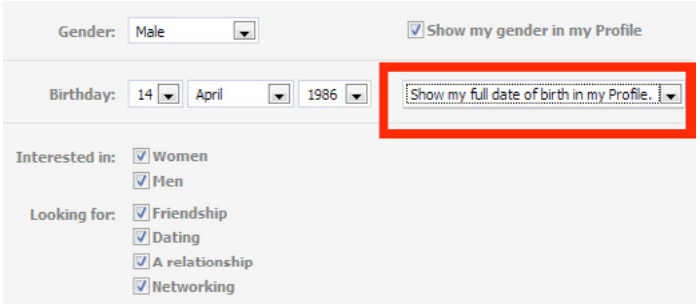
5. ไม่ตั้งค่ารหัสผ่านที่เป็นคำในพจนานุกรมหรือคำทั่วไปที่คาดเดาได้โดยง่าย

ในทางการรักษาความมั่นคงปลอดภัยบนระบบคอมพิวเตอร์ได้มีการ พบการโจมตีรหัสผ่านรูปแบบหนึ่งที่ชื่อว่า Dictionary Attack [8-6] ซึ่งเป็นการโจมตีโดยการนำเอาคำในไฟล์ข้อความ (Text File) หรือในอีกความหมายหนึ่งคือพจนานุกรม (Dictionary) ที่จัดทำขึ้นส่วนตัวหรืออาจจะหาซื้อได้จากแหล่งต่างๆ มาใช้ในการโจมตีระบบคอมพิวเตอร์ โดยนำค่าในไฟล์ดังกล่าวไปประมวลผลล็อกอินลงในระบบคอมพิวเตอร์ ซึ่งการโจมตีในรูปแบบนี้มักได้ผลกับผู้ใช้งานที่ตั้งค่ารหัสผ่านที่ไม่ซับซ้อนและส่วนมากเป็นคำทั่วไปที่ผู้ใช้งานมักจะตั้งกัน เช่น คำว่า password , secret เป็นต้น

6. ไม่ตั้งค่ารหัสผ่านจากข้อมูลส่วนบุคคล

สิ่งแรกที่สร้างแรงจูงใจให้เกิดการขโมยบัญชีผู้ใช้งานในระบบหรือบริการต่างๆนั่นคือ ผู้ใช้งานมักมีการตั้งค่ารหัสผ่านโดยใช้ข้อมูลส่วนบุคคล เพื่อให้ผู้ใช้งานเองสามารถจดจำได้ง่าย ซึ่งข้อมูลส่วนบุคคลที่กล่าวมาคงปฏิเสธไม่ได้ว่าจะเป็นข้อมูลซึ่งรู้เฉพาะผู้ใช้งานคนเดียว และมักเป็นข้อมูลที่เปิดเผยและคาดเดาได้ไม่ยาก เช่น เบอร์โทรศัพท์ หมายเลขทะเบียนรถ หรือวันเดือนปีเกิด เป็นต้น ในบางกรณีที่ผู้ใช้งานตั้งค่ารหัสผ่านจากข้อมูลส่วนบุคคลและคิดว่าตนเองถูกขโมยรหัสผ่านจากคนใกล้ตัวที่รู้ข้อมูลส่วนบุคคล แต่จริงๆแล้วผู้ใช้งานลืมคิดไปว่าข้อมูลดังกล่าว ไม่ได้เป็นความลับหรือรู้เฉพาะคนใกล้ตัวเท่านั้น ปัจจุบันข้อมูลส่วนบุคคลบางอย่างได้

ถูกเผยแพร่อยู่บนหน้าเว็บไซต์เครือข่ายสังคมออนไลน์ที่ตนเองสมัครใช้บริการอยู่ ดังรูปที่ 32 (8-3) ฉะนั้นจึงไม่แปลกที่การตั้งค่ารหัสผ่านจากข้อมูลส่วนบุคคลจะไม่มีความมั่นคงปลอดภัยพอ



รูปที่ 32 (8-3) การเปิดเผยข้อมูลผ่านเว็บไซต์เครือข่ายสังคมออนไลน์

7. ใช้งาน Two Factor Authentication

Two Factor Authentication เป็นวิธีการล็อกอินเพื่อเข้าถึงระบบหรือบริการต่างๆโดยอาศัยปัจจัยสองอย่างที่นำมายืนยันร่วมกัน ซึ่งจะต้องไม่มีความสัมพันธ์เหมือนกัน เพื่อจุดประสงค์ในการสร้างความมั่นคงปลอดภัยให้มีประสิทธิภาพมากยิ่งขึ้น โดยในทางด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ได้มีการจำแนกปัจจัยดังกล่าวออกเป็น 3 ส่วน [8-7] คือ

7.1 การยืนยันตัวตนด้วยสิ่งที่รู้ (Something you know) เช่น รหัสผ่าน

7.2 การยืนยันตัวตนด้วยสิ่งที่มี (Something you have) เช่น รหัสบัตรเติมเงิน รหัสผ่านแบบครั้งเดียวที่ส่งผ่านข้อความสั้นเข้าโทรศัพท์มือถือ (SMS OTP)

7.3 การยืนยันตัวตนด้วยข้อมูลทางชีวภาพ (Something you are) เช่น การสแกนลายนิ้วมือ

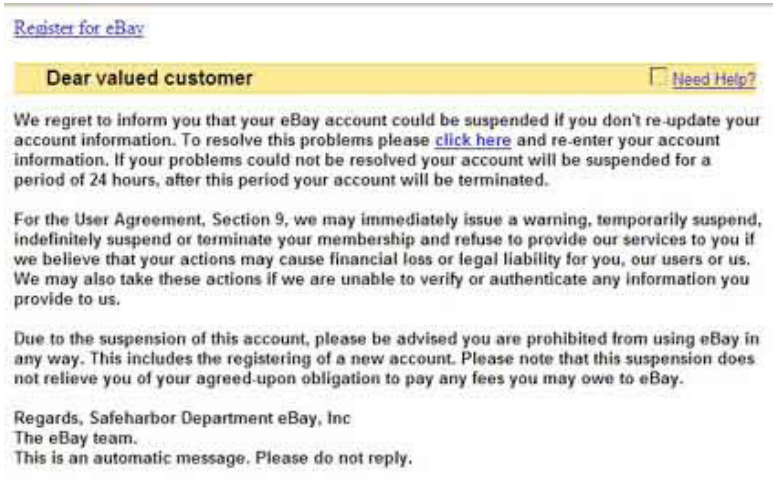
ซึ่งในปัจจุบันพบว่าระบบหรือบริการต่างๆมีแนวโน้มในการปรับเปลี่ยนให้สามารถรองรับการทำงานร่วมกับ Two Factor Authentication ดังจะเห็นได้จากเว็บไซต์ใหญ่ๆที่มีการเปิดให้ใช้งานแล้ว เช่น Google หรือ Amazon

8. เปลี่ยนรหัสผ่านอย่างสม่ำเสมอและตรวจสอบข้อมูลช่องทางการเปลี่ยนรหัสผ่าน

การเปลี่ยนรหัสผ่านอย่างสม่ำเสมอช่วยให้ผู้ใช้งานมั่นใจว่ารหัสผ่านส่วนตัวจะยังคงเป็นความลับอยู่เสมอ และในระหว่างนั้นผู้ใช้งานควรมีการตรวจสอบข้อมูลอื่นๆที่ใช้ร่วมกับการล็อกอินด้วย เช่น ข้อมูลอีเมลสำรองที่ใช้ในการเปลี่ยนรหัสผ่าน ข้อมูลคำถามสำหรับการเปลี่ยนรหัสผ่าน เป็นต้น เพื่อลดโอกาสที่ผู้ไม่หวังดีจะแฝงตัวอยู่กับบัญชีผู้ใช้งาน ซึ่งโดยทั่วไป มักเกิดกับการโจมตีที่ผู้โจมตีได้บัญชีการใช้งานและรหัสผ่านมาแล้วและทำการลักลอบอยู่ในระบบโดยไม่แสดงพฤติกรรมใดๆ ในบางกรณีผู้ใช้งานเองอาจไม่เคยทราบเลยก็เป็นได้ว่ามีการขโมยรหัสผ่านสำเร็จแล้ว และผู้โจมตีกำลังแฝงตัวเพื่อลักลอบขโมยข้อมูลส่วนบุคคลจากการใช้งาน เช่น ผู้โจมตีจะเฝ้าดูการใช้งานอีเมล เป็นต้น และเมื่อผู้โจมตีได้ข้อมูลตามที่ต้องการแล้วจึงจะแสดงตัวออกมาต่อไปหรือในบางรายอาจไม่แสดงตัวเลยก็เป็นได้

9. อย่าหลงกลเชื่ออีเมลที่แจ้งให้เปลี่ยนรหัสผ่าน

ก่อนที่จะตกลงปลงใจเชื่อข้อมูลในอีเมล โดยเฉพาะอย่างยิ่ง ข้อมูลที่มีผลกระทบกับการใช้งานรหัสผ่าน ควรพิจารณาให้รอบคอบว่าเป็นอีเมลที่มาจากระบบหรือจากผู้เกี่ยวข้องจริงๆ หรือไม่ แนวทางที่ใช้ในการวิเคราะห์ข้อมูลเบื้องต้นคือการตรวจสอบสถานะการเปลี่ยนรหัสผ่านจากผู้ดูแลระบบหรือจากการเช็คจากข้อมูลที่บริการนั้นๆ จัดเตรียมไว้ให้ แต่หากไม่สามารถติดต่อหรือตรวจสอบข้อมูลใดๆ ได้เลย ก็อาจจะใช้วิธีการทั่วไปที่ค่อนข้างปลอดภัยคือเข้าไปเปลี่ยนรหัสผ่านยังเว็บไซต์หรือบริการที่แจ้งเตือนมาด้วยตนเองเพื่อป้องกันโอกาสในการหลอกลวงด้วยเทคนิค Phishing [8-8] โดยผู้ใช้งานจะต้องไม่คลิกลิ้งก์ที่แนบมากับอีเมลเป็นอันขาด หากต้องการเปลี่ยนรหัสผ่านบนเว็บไซต์ ให้ผู้ใช้งานเข้าไปยังหน้าเว็บไซต์โดยตรงและทำการเปลี่ยนรหัสผ่าน ตัวอย่างของอีเมลหลอกลวงเป็นดังรูปที่ 33 (8-5)


Register for eBay

Dear valued customer Need Help?

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

รูปที่ 33 (8-5) แสดงตัวอย่างอีเมลหลอกลวง

แนวทางการใช้งานรหัสผ่านดังที่ได้กล่าวมาทั้งหมดเป็นเพียงแนวคิดเบื้องต้นที่จะช่วยสร้างลักษณะนิสัยและความตระหนักถึงความมั่นคงปลอดภัยในการใช้งานรหัสผ่านและการเข้าถึงระบบหรือบริการต่างๆ โดยสิ่งที่ชี้ให้เห็นอย่างหนึ่งคือนอกเหนือจากจะให้ความรู้ผู้ใช้งานแล้ว ผู้ดูแลระบบควรมีการสนับสนุนช่องทางหรือกลไกในการเพิ่มประสิทธิภาพด้านความมั่นคงปลอดภัยในการเข้าถึงระบบต่างๆเพิ่มเติมด้วย เช่น การพัฒนาฟังก์ชั่นการตรวจสอบการเปลี่ยนรหัสผ่านให้สอดคล้องกับนโยบายขององค์กร การพัฒนาระบบการทำ Two Factor Authentication เพื่อเพิ่มระดับในการเข้าถึงระบบให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้น เป็นต้น

อ้างอิง

[8-1] https://www.trustwave.com/global-security-report

[8-2] http://money.cnn.com/2012/03/01/technology/password_security/?source=cnn_bin

[8-3] http://en.wikipedia.org/wiki/Active_Directory

[8-4] http://netsecurity.about.com/od/secureyourwindowspc/qt/pwminage.htm

[8-5] http://www.windowsitpro.com/article/ldap/sso-vs-centralized-authentication

[8-6] http://en.wikipedia.org/wiki/Dictionary_attack

[8-7] http://www.cs.cornell.edu/courses/cs513/2005fa/nnlauthpeople.html

[8-8] http://www.etda.or.th/main/contents/display/233

09 ผู้ใช้ IOS ระวังถูกขโมย ACCOUNT

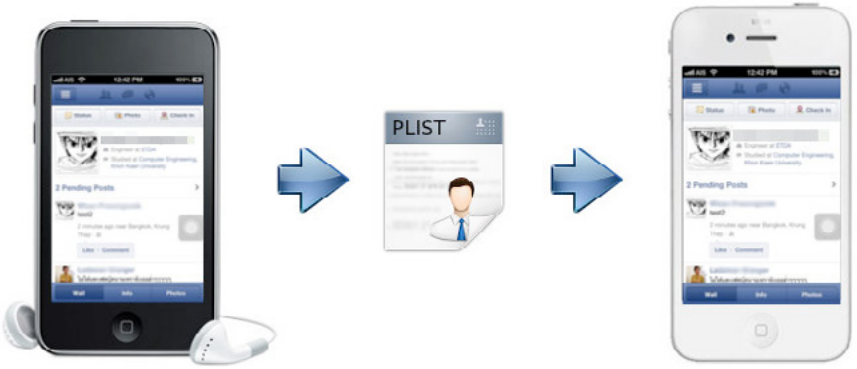
ผู้เขียน: ทีมไทยเซิร์ต

วันที่เผยแพร่: 11 เม.ย. 2555
ปรับปรุงล่าสุด: 11 เม.ย. 2555

เมื่อวันที่ 3 เมษายน 2555 นาย Gareth Wright นักออกแบบและพัฒนาเว็บไซต์ ได้ค้นพบช่องโหว่ของแอปพลิเคชั่น Facebook บนระบบปฏิบัติการ iOS ซึ่งเก็บข้อมูลการล็อกอินของผู้ใช้ไว้ในตัวเครื่องโดยไม่มีการเข้ารหัสลับ อีกทั้งยังไม่มีการป้องกันการคัดลอกข้อมูลออกจากตัวเครื่อง ทำให้ผู้ไม่หวังดีสามารถขโมยไฟล์ที่เก็บข้อมูลการล็อกอินจากเครื่องของเหยื่อไปใส่ในเครื่องของตนเอง แล้วสวมรอยเป็นผู้ใช้คนนั้นได้อย่างง่ายดาย เขาได้แจ้งช่องโหว่ดังกล่าวไปยัง Facebook แต่ได้รับการตอบกลับมาว่า ช่องโหว่มีผลกับอุปกรณ์ iOS ที่ถูก Jailbreak แล้วเท่านั้น แต่นาย Gareth Wright ยืนยันว่าช่องโหว่นี้มีผลกับอุปกรณ์ iOS ทุกเครื่อง รวมทั้งเครื่องที่ไม่ได้ Jailbreak ด้วย [9-1] เพื่อตอบข้อสงสัยเหล่านี้ ทางทีมไทยเซิร์ตจึงได้ทำการทดสอบช่องโหว่ดังกล่าว

อุปกรณ์ที่ใช้ในการทดสอบ ประกอบด้วย iPod Touch Gen 4, iPhone 4 และ iPhone 4S โดยทำการอัพเดทเฟิร์มแวร์ให้เป็นเวอร์ชันล่าสุด คือ iOS เวอร์ชัน 5.1 (9B176) และติดตั้งแอปพลิเคชั่น Facebook เวอร์ชัน 4.1.1 (อัพเดทล่าสุด 2 เมษายน 2012) โดยอุปกรณ์ทุกเครื่องไม่ได้ทำการ Jailbreak แต่อย่างใด

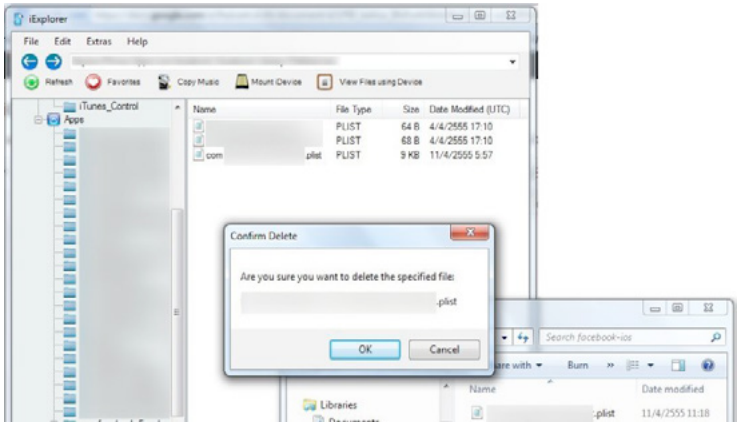
ทีมไทยเซิร์ตได้ทำการทดสอบโดยการล็อกอินผ่านแอปพลิเคชั่น Facebook ในเครื่อง iPod แล้วนำไฟล์ที่เก็บข้อมูลการล็อกอินไปแทนที่ไฟล์ชื่อเดียวกันที่อยู่ใน อุปกรณ์ iPhone ดังแสดงในรูปที่ 34 (9-1) ปรากฏว่าเครื่อง iPhone สามารถเข้าใช้งานบัญชี Facebook ที่ถูกล็อกอินในอุปกรณ์ iPod ได้ทันที และสามารถทำงานได้เสมือนกับเจ้าของ Account เป็นผู้ล็อกอินในเครื่องนั้นโดยตรง ไม่ว่าจะเป็นการอ่าน โพสต์ข้อความ หรือแม้กระทั่งการยกเลิก Account ยกเว้นแต่การเปลี่ยนอีเมลที่ผูกกับ Account จะไม่สามารถทำได้ เนื่องจากแอปพลิเคชั่น Facebook จะขอให้ใส่ Password เพื่อเป็นการยืนยันอีกครั้งหนึ่ง รวมถึงไม่สามารถเปลี่ยน Password ได้ เนื่องจากแอปพลิเคชั่น Facebook ไม่รองรับการกระทำดังกล่าว



รูปที่ 34 (9-1) แสดงการนำไฟล์ที่เก็บข้อมูลการล็อกอินจากเครื่อง iPod ไปใส่ในเครื่อง iPhone

และจากการทดสอบเพิ่มเติมกับแอปพลิเคชั่น Dropbox และ Gmail พบว่าสามารถสวมรอยการใช้งานได้เช่นเดียวกับแอปพลิเคชั่น Facebook และมีความเป็นไปได้สูงว่าจะพบแอปพลิเคชั่นอื่นๆ ที่มีจุดอ่อนแบบเดียวกัน ซึ่งจะส่งผลอันตรายกับผู้ใช้งาน หากถูกผู้ไม่หวังดีขโมยอุปกรณ์ iOS หรือนำอุปกรณ์ iOS ไปเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ที่สามารถคัดลอกข้อมูลออกจากตัว เครื่องได้

ในการทดสอบครั้งนี้ ทีมไทยเซิร์ตได้ใช้โปรแกรม iExplorer ในการเข้าถึงข้อมูลของอุปกรณ์ iOS ซึ่งโปรแกรมดังกล่าวสามารถเข้าถึงข้อมูลไฟล์การตั้งค่าของแอปพลิเคชั่นบน อุปกรณ์ iOS ได้ทั้งหมด ดังรูปที่ 35 (9-2) และยังพบว่าโปรแกรมนี้สามารถมองเห็นข้อมูลดังกล่าวได้ทันทีที่เชื่อมต่อ อุปกรณ์เข้ากับเครื่องคอมพิวเตอร์ผ่านสาย USB ถึงแม้อุปกรณ์ iOS นั้นจะไม่ได้ผ่านการ Jailbreak ก็ตาม ซึ่งผู้ใช้รวมถึงผู้พัฒนาแอปพลิเคชั่นบางรายยังคงมีความเข้าใจผิดว่าไฟล์ ต่างๆ เหล่านี้จะไม่สามารถมองเห็นได้หากอุปกรณ์ iOS ยังไม่ได้ Jailbreak



รูปที่ 35 (9-2) แสดงการใช้โปรแกรม iExplorer ในการเข้าถึงข้อมูลที่อยู่ในอุปกรณ์ iOS

สาเหตุของปัญหา เกิดจากการที่แอปพลิเคชั่นหลายตัว เก็บข้อมูลการล็อกอินไว้ในไฟล์นามสกุล .plist ซึ่งเป็นไฟล์ที่ระบบปฏิบัติการ iOS ใช้ในการเก็บข้อมูลของแต่ละแอปพลิเคชั่น เช่น สถานะการล็อกอิน เป็นต้น โดยไม่ได้มีการป้องกันที่เหมาะสม จึงทำให้ผู้ไม่หวังดีสามารถขโมยไฟล์ข้อมูลดังกล่าวไปใช้งานได้ทันที

ดังนั้น ผู้ใช้งานอุปกรณ์ iOS ต้องพึงระวังไว้ว่า อย่าปล่อยให้อุปกรณ์อยู่ห่างตัวเป็นอันขาด และผู้ใช้ควรมีความตระหนักในการใช้งานโดยทำการล็อกเอาท์จากแอปพลิเคชั่นทุกครั้งเมื่อเลิกใช้ หรือหากผู้ใช้งานสงสัยว่าจะถูกขโมย Account ด้วยวิธีนี้ ผู้ใช้สามารถแก้ไขได้โดยการเปลี่ยนรหัสผ่าน ซึ่งจะทำให้ไฟล์ที่เก็บข้อมูลการล็อกอินที่ถูกขโมยไปไม่สามารถใช้งานได้อีก แต่อย่างไรก็ตามวิธีการดังกล่าว จากการทดสอบของทีมไทยเซิร์ต พบว่าสามารถใช้ได้กับแอปพลิเคชั่น Facebook และ Gmail แต่สำหรับ แอปพลิเคชั่น Dropbox ต้องใช้วิธี Unlink ออกจาก Account ของ Dropbox [9-2] หากสงสัยว่าถูกขโมยไฟล์ที่เก็บข้อมูลการล็อกอิน

จากรายงานของ The Next Web ระบุว่า Dropbox ทราบปัญหาดังกล่าวแล้ว และจะแก้ไขปัญหานี้ในเวอร์ชันถัดไป โดยจะมีการปรับปรุงการเก็บข้อมูลให้ปลอดภัยมากยิ่งขึ้น [9-3] ส่วน Facebook ยังไม่มีรายงานการแก้ไขแต่อย่างใด ซึ่งหากมีความคืบหน้าในกรณีนี้ ทางทีมไทยเซิร์ตจะนำมาแจ้งให้ทราบต่อไป

อ้างอิง

[9-1] http://garethwright.com/blog/facebook-mobile-security-hole-allows-identity-theft

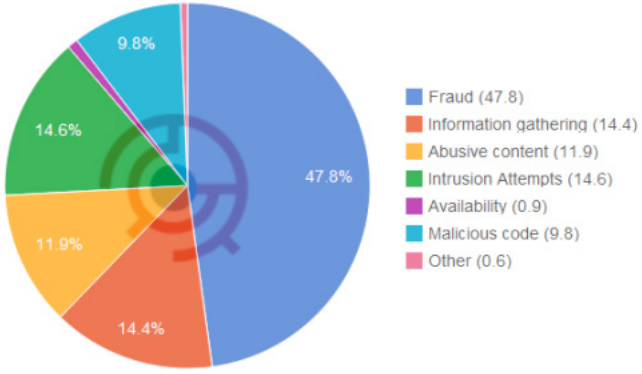
[9-2] http://www.wikihow.com/Unlink-a-Computer-from-a-Dropbox-Account

[9-3] http://thenextweb.com/mobile/2012/04/06/security-hole-in-facebook-ios-app-doesnt-require-jailbreak-or-theft-and-dropbox-has-it-too/

10 รู้จัก PHISHING และการป้องกัน

ผู้เขียน: วิศัลย์ ประสงค์สุข
วันที่เผยแพร่: 27 เม.ย. 2555
ปรับปรุงล่าสุด: 30 เม.ย. 2555

ในปี 2554 ที่ผ่านมา สถิติภัยคุกคามที่แจ้งมายังไทยเซิร์ตมากที่สุดคือภัยคุกคามประเภทการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ดังรูปที่ 36 (10-1) ซึ่งแทบจะทั้งหมดเป็นเรื่องเกี่ยวกับ Phishing ดังนั้นบทความนี้จึงขอนำท่านผู้อ่านให้ทำความรู้จักและระวังตัวจากภัยชนิดนี้



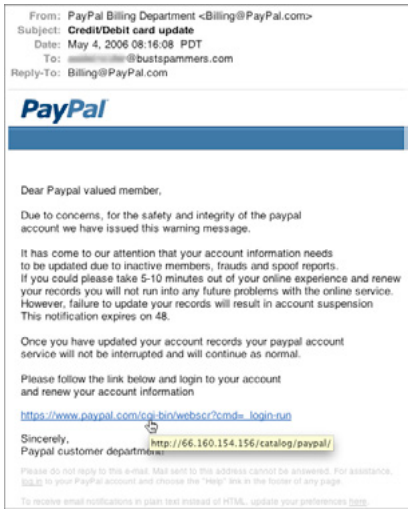
รูปที่ 36 (10-1) สถิติภัยคุกคามระหว่างเดือนกรกฎาคมถึงธันวาคมปี 2554 จำแนกตามประเภทภัยคุกคาม [10-1]

Phishing คือคำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน เป็นต้น ในบทความนี้จะเน้นในเรื่องของ Phishing ที่มีจุดมุ่งหมายเพื่อหลอกลวงทางการเงิน เนื่องจากจะทำให้ผู้อ่านมองเห็นผลกระทบได้ง่าย

คำว่า Phishing เป็นคำพ้องเสียงจากคำว่า Fishing ซึ่งหมายถึงการตกปลา หากจะเปรียบเทียบง่าย ๆ ผู้อ่านสามารถจินตนาการได้ว่า เหยื่อล่อที่ใช้ในการตกปลา ก็คือกลวิธีที่ผู้โจมตีใช้ในการหลอกลวงผู้เสียหาย ซึ่งเหยื่อล่อที่เด่น ๆ ในการหลอกลวงแบบ Phishing มักจะเป็นการปลอมอีเมล หรือปลอมหน้าเว็บไซต์ที่มีข้อความซึ่งทำให้ผู้เสียหายอ่านแล้วหลงเชื่อ เช่น ปลอมอีเมลว่าอีเมลฉบับนั้นถูกส่งออกมาจากธนาคารที่ผู้เสียหายใช้บริการอยู่ โดยเนื้อความในอีเมลแจ้งว่า ขณะนี้ธนาคารมีการปรับเปลี่ยนระบบรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้า และธนาคารต้องการให้ลูกค้าเข้าไปยืนยันความถูกต้องของข้อมูลส่วนบุคคลผ่านทางลิงก์ที่แนบมาในอีเมล เป็นต้น เมื่อผู้เสียหายคลิกที่ลิงก์ดังกล่าว ก็จะพบกับหน้าเว็บไซต์ปลอมของธนาคาร ซึ่งผู้โจมตีได้เตรียมไว้ เมื่อผู้เสียหายเข้าไปล็อกอิน ผู้โจมตีก็จะได้ชื่อผู้ใช้และรหัสผ่านของผู้เสียหายไปในทันที ในหลาย ๆ ครั้งการหลอกลวงแบบ Phishing จะอาศัยเหตุการณ์สำคัญที่เกิดในช่วงเวลานั้น ๆ เพื่อเพิ่มโอกาสของการหลอกลวงสำเร็จ เช่น อาศัยช่วงเวลาที่มีภัยธรรมชาติหรือโรคระบาด โดยปลอมเป็นอีเมลจากธนาคารเพื่อขอรับบริจาค เป็นต้น [10-2]

หน้าเว็บไซต์ปลอมบางหน้าจะใช้วิธีการที่แยบยล นั่นคือการฝังโทรจันที่สามารถขโมยข้อมูลที่ต้องการมากับหน้าเว็บไซต์ปลอมนั้นด้วย เช่น โทรจันที่ทำหน้าที่เป็น Key-logger ซึ่งจะคอยติดตามว่าผู้เสียหายพิมพ์คีย์บอร์ดอะไรบ้าง เป็นต้น เมื่อผู้เสียหายหลงกล กดลิงก์ตามเข้ามาที่หน้าเว็บไซต์ปลอมก็จะติดโทรจันชนิดนี้ไปโดยอัตโนมัติ และหากผู้เสียหายทำการล็อกอินเข้าใช้งานระบบใด ๆ ข้อมูลชื่อผู้ใช้ และรหัสผ่าน ของระบบนั้นก็จะถูกส่งไปยังผู้ไม่ประสงค์ดี [10-3] [10-4]

ตัวอย่างของอีเมลและหน้าเว็บไซต์หลอกลวง มีอยู่มากมายเต็มไปหมดในโลกอินเทอร์เน็ต เช่นรูปที่ 37 (10-2) ด้านล่าง เป็นรูปของสถาบันทางการเงินแห่งหนึ่ง หากสังเกตดีๆ จะเห็นว่า URL ที่แสดงขึ้นมา ไม่ใช่ URL ที่ถูกต้องของสถาบันการเงินนั้น


From: PayPal Billing Department <Billing@PayPal.com>
Subject: Credit/Debit card update
Date: May 4, 2006 08:16:08 PDT
To: [redacted]@bustspammers.com
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Sincerely,
Paypal customer department

http://66.160.154.156/catalog/paypal/

รูปที่ 37 (10-2) ตัวอย่างหน้าเว็บไซต์หลอกลวงของสถาบันการเงินแห่งหนึ่ง [10-6]

นอกจาก Phishing แล้วยังมีเทคนิคการหลอกลวงอื่น ๆ ที่คล้ายคลึงกัน ซึ่งแต่ละวิธีก็มีชื่อเรียกแตกต่างกันออกไป เช่น

Vishing และ Smishing: หลายคนคงเคยได้ยินหรือเคยประสบกับแก๊งคอลเซ็นเตอร์อยู่บ้าง พฤติกรรมของแก๊งเหล่านี้เข้าข่ายของ Vishing โดยตัวอักษร 'V' นี้มาจากคำว่า Voice ซึ่งแปลว่าเสียง ดังนั้น Vishing จึงเป็นการใช้ Voice ร่วมกับ Phishing ซึ่งมักเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์นั่นเอง แต่หากเป็น Smishing ก็จะเป็นการหลอกลวงโดยใช้ SMS เช่น การได้รับ SMS อ้างว่ามาจากธนาคารเพื่อแจ้งลูกค้าว่าบัญชีของท่านถูกระงับ กรุณาติดต่อกลับที่หมายเลข ดังต่อไปนี้ ซึ่งเมื่อโทรตามหมายเลขที่ระบุไว้ ก็จะเข้าสู่กระบวนการ Vishing ต่อไป เป็นต้น [10-9]

Spear-phishing และ Whaling: อย่างที่กล่าวมาแล้วในข้างต้นเกี่ยวกับกลวิธีของ Phishing ในการนำไปใช้งาน ผู้ไม่ประสงค์ดีบางคนก็ได้เล็งองค์กร หรือบุคคลที่เป็นเป้าหมายไว้ชัดเจนอยู่แล้ว บุคคลที่มักตกเป็นเป้าหมายส่วนใหญ่จะเป็นผู้ที่มีบทบาทสำคัญในองค์กร มีความสามารถหรือรู้วิธีการเข้าถึงข้อมูลสำคัญขององค์กร การหลอกลวงแบบ Phishing ที่มีเป้าหมายชัดเจนนี้มีคำเรียกเฉพาะคือ Spear-phishing และหากเป้าหมายของ Spear-phishing นี้เป็นบุคคลที่มีตำแหน่งสูงหรือเป็นบุคคลสำคัญในองค์กร จะเรียกการหลอกลวงนี้ว่า Whaling (ตลกร้ายที่เปรียบเทียบบุคคลสำคัญเป็นปลาตัวโต ในที่นี้คือปลาวาฬนั่นเอง) [10-10]

แล้วผู้อ่านควรระวังตัวอย่างไร? ข้อแนะนำต่อไปนี้ สามารถลดโอกาสไม่ให้ผู้อ่านถูกหลอกลวงได้ [10-2] [10-6] [10-7] [10-8]

1. ไม่เปิดลิงก์ที่แนบมาในอีเมล เนื่องจากมีโอกาสสูงที่จะถูกหลอกลวง เพราะบางครั้งลิงก์ที่มองเห็นในอีเมลว่าเป็นเว็บไซต์ของธนาคาร แต่เมื่อคลิกไปแล้วอาจจะไปที่เว็บไซต์ปลอมที่เตรียมไว้ก็เป็นได้ เนื่องจากในการสร้างลิงก์นั้นสามารถกำหนดให้แสดงข้อความหรือรูปภาพได้ตามต้องการ ดังนั้นบางเว็บไซต์ปลอมจึงทำ URL ให้สังเกตความแตกต่างจาก URL จริงได้ยาก
2. พึงระวังอีเมลที่ขอให้กรอกข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นอีเมลที่มาจากสถาบันการเงิน ทั้งนี้ธนาคารหลายแห่งได้แจ้งอย่างชัดเจนว่า ธนาคารไม่มีนโยบายในการขอให้ลูกค้าเปิดเผยเลขประจำตัว หรือข้อมูลที่มีความสำคัญอื่น ๆ ผ่านทางอีเมลโดยเด็ดขาด
3. ไม่เปิดลิงก์ที่แนบมาในอีเมล เนื่องจากในปัจจุบัน ผู้โจมตีมีเทคนิคมากมายในการปลอมชื่อผู้ส่งให้เหมือนมาจากองค์กรนั้นจริง ๆ หากต้องการเข้าใช้งานเว็บไซต์นั้น ขอให้พิมพ์ URL ด้วยตัวเอง
4. สังเกตให้แน่ใจว่าเว็บไซต์ที่ใช้งานเป็น HTTPS ก่อนให้ข้อมูลส่วนบุคคลที่สำคัญ เช่น เลขบัตรเครดิต หรืออื่น ๆ
5. ลบอีเมลน่าสงสัยออกไป เพื่อไม่ให้พลั้งเผลอกดเปิดครั้งถัดไป

6. ติดตั้งโปรแกรม Anti-Virus, Anti-Spam และ Firewall เนื่องจากผลพลอยได้อย่างหนึ่งของการติดตั้ง Firewall คือสามารถทำการยับยั้งไม่ให้โทรจันแอบส่งข้อมูลออกไปจากระบบได้ นอกจากนี้ ผู้ใช้ควรหมั่นศึกษาและอัพเดทโปรแกรมดังกล่าวให้เป็นรุ่นปัจจุบันเสมอ
7. หากท่านผู้อ่านพบเห็นเว็บไซต์หลอกลวงซึ่งมีจุดประสงค์ในการขโมยข้อมูลส่วน บุคคล สามารถแจ้งเหตุภัยคุกคามได้ที่เจ้าของบริการเหล่านั้น หรือส่งอีเมลมาที่ report@thaicert.or.th ตลอด 24 ชั่วโมง หรือโทร 02-142-2483 ในเวลา 8.30-17.30 ทุกวันทำการ

หากรู้ตัวว่าพลาดท่าไปแล้ว จะทำอย่างไรดี? ข้อแนะนำต่อไปนี้เป็นสิ่งที่ผู้เสียหายควรปฏิบัติตามโดยทันที [10-2]

1. ในกรณีที่เป็นข้อมูลสำคัญขององค์กร ผู้เสียหายควรแจ้งเรื่องไปยังบุคคลที่เหมาะสมรวมทั้งผู้ดูแลระบบเพื่อเป็นการเตรียมมาตราการปกป้องค์กรต่อไป
2. ในกรณีที่เป็นข้อมูลบัญชีธนาคาร ผู้เสียหายควรแจ้งเรื่องไปยังธนาคารที่ใช้บริการ และทำการปิดบัญชีที่คาดว่าสามารถถูกขโมยได้ หรือเฝ้าระวังการใช้งานบัญชีอย่างต่อเนื่อง
3. ทำการเปลี่ยนรหัสผ่าน ในทุกระบบที่ใช้รหัสผ่านเดียวกัน และไม่กลับมาใช้รหัสผ่านนั้นอีก

ถึงแม้ Phishing เป็นภัยคุกคามที่สร้างความเสียหายมากมาย แต่ก็สามารถระมัดระวังตัวได้ หากผู้ใช้มีความตระหนักในการใช้งานอินเทอร์เน็ต รวมถึงปฏิบัติตามคำแนะนำข้างต้น

อ้างอิง

[10-1] http://www.thaicert.or.th/statistics2011.html

[10-2] http://www.us-cert.gov/cas/tips/ST04-014.html

[10-3] http://www.focus.com/fyi/44-ways-protect-phishing/

[10-4] http://www.theregister.co.uk/2007/02/23/trojan_phishing_attack/

[10-5] http://www.bustspammers.com/phishing_links.html

[10-6] http://www.scb.co.th/th/about-scb/phishing-mail

[10-7] http://www.kasikornbank.com/TH/Phishing_Website_Report/Pages/PhishingWebsiteReport.aspx

[10-8] http://www.tmbbank.com/personal/e-banking/popup/Phishing.html

[10-9] http://www.usatoday.com/tech/news/story/2011-10-18/smishing-bank-scam/50817688/1

[10-10] http://blogs.iss.net/archive/SpearPhishing.html

11 การโจมตีผ่านเว็บเบราว์เซอร์และการป้องกัน

ผู้เขียน: เสฏฐวุฒิ แสนนาม

วันที่เผยแพร่: 11 พ.ค. 2555
ปรับปรุงล่าสุด: 11 พ.ค. 2555

เว็บเบราว์เซอร์ (Web Browser) หรือเรียกสั้นๆ ว่า เบราว์เซอร์ (Browser) คือโปรแกรมที่ช่วยให้ผู้ใช้คอมพิวเตอร์สามารถเข้าใช้งานเว็บไซต์ได้ เว็บเบราว์เซอร์จะทำการแปลงโค้ดภาษา HTML ให้ออกมาแสดงผลเป็นข้อความ รูปภาพ เสียง หรือคลิปวิดีโออื่นๆ ตามที่ผู้ออกแบบเว็บไซต์กำหนด [11-1] ตัวอย่างเว็บเบราว์เซอร์ที่ได้รับความนิยม เช่น Internet Explorer, Firefox, Chrome, Safari, Opera ดังรูปที่ 38 (11-1)

รูปที่ 38 (11-1) เว็บเบราว์เซอร์ที่ได้รับความนิยม

จากการพัฒนาของเทคโนโลยี เว็บไซต์สมัยใหม่จึงไม่ได้ถูกใช้เพียงแค่แสดงข้อมูลเพียงอย่างเดียวอีกต่อไป แต่ได้ถูกพัฒนาให้สามารถทำงานได้หลากหลายมากขึ้น เช่น เล่นเกม ตกแต่งภาพ ตัดต่อวิดีโอ จัดทำเอกสาร [11-2] หรือแม้กระทั่งใช้เป็นระบบปฏิบัติการเลยก็ยังได้ [11-3] ซึ่งการทำงานต่างๆ เหล่านี้ก็ต้องอาศัยความสามารถของเว็บเบราว์เซอร์ที่มากขึ้นตามไปด้วย

จากความสามารถที่มากขึ้น ช่องโหว่ และความเสี่ยง ก็จะเพิ่มมากขึ้นตามไปด้วย ปัจจุบันการโจมตีผ่านเว็บเบราว์เซอร์นั้นมีแนวโน้มที่จะเพิ่มมากขึ้น [11-4] เนื่องจากเป็นสิ่งที่ผู้ใช้อินเทอร์เน็ตทุกคนจำเป็นต้องใช้ ดังนั้นการศึกษาถึงรูปแบบภัยคุกคาม และการรับมือการโจมตีจึงเป็นสิ่งที่จำเป็น เพื่อให้มีความมั่นคงปลอดภัยในการใช้งานอินเทอร์เน็ต

การโจมตีผ่านเว็บเบราว์เซอร์

การโจมตีผ่านเว็บเบราว์เซอร์ โดยหลักๆ จะมีอยู่ด้วยกัน 3 ช่องทาง คือ โจมตีผ่านช่องโหว่ของตัวเว็บเบราว์เซอร์เอง โจมตีผ่านช่องโหว่ของปลั๊กอินจากผู้พัฒนาภายนอก และการสร้าง Extension ที่เป็นอันตรายเพื่อใช้ในการโจมตี

การโจมตีผ่านช่องโหว่ของเว็บเบราว์เซอร์

ในการเขียนโปรแกรมคอมพิวเตอร์ จะมีการจองพื้นที่ในหน่วยความจำเพื่อใช้ในการเก็บข้อมูลชั่วคราว พื้นที่ดังกล่าวเรียกว่า Buffer ซึ่งพื้นที่ของ Buffer นั้นมีขนาดจำกัด หากผู้เขียนโปรแกรมไม่ทำการตรวจสอบขนาดของข้อมูลที่จะนำมาจัดเก็บ ปล่อยให้โปรแกรมเก็บข้อมูลที่มีขนาดใหญ่กว่าความจุของ Buffer ข้อมูลที่เก็บนั้นก็จะล้นออกมา สถานการณ์เช่นนี้เรียกว่า Buffer Overflow ซึ่งข้อมูลที่ล้นออกมานั้นก็จะไปทับกับข้อมูลส่วนอื่นๆ ที่อยู่ในหน่วยความจำ เช่น โค้ดของโปรแกรมที่กำลังทำงานอยู่ ทำให้โปรแกรมทำงานผิดพลาดหรือไม่สามารถทำงานต่อได้ [11-5]

การโจมตีผ่านช่องโหว่ของเว็บเบราว์เซอร์ โดยส่วนใหญ่จะเป็นการใช้เทคนิค Buffer Overflow ผู้โจมตีจะทำการสร้างข้อมูลที่มีขนาดใหญ่กว่าความจุของ Buffer ซึ่งภายในบรรจุโค้ดอันตรายไว้ เมื่อโปรแกรมโหลดข้อมูลดังกล่าวเข้ามาในหน่วยความจำ ข้อมูลส่วนที่ล้นออกมานั้นก็จะไปทับกับส่วนที่เป็นโค้ดของโปรแกรมที่กำลัง ทำงานอยู่ ทำให้โค้ดอันตรายที่แฮ็กเกอร์ใส่เข้ามานั้นถูกนำไปประมวลผลแทน ซึ่งเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อก็จะตกอยู่ภายใต้การควบคุมของ แฮ็กเกอร์ในท้ายที่สุด ตัวอย่างวิดีโอการโจมตีด้วยวิธี Buffer Overflow สามารถดูได้จาก http://youtu.be/znO1Mc8EiDE

การโจมตีผ่านช่องโหว่ของปลั๊กอิน

ปลั๊กอิน (Plugin) คือโปรแกรมที่สามารถติดตั้งเพื่อให้เว็บเบราว์เซอร์สามารถแสดงผลเนื้อหาอื่นๆ เพิ่มเติมได้ ตัวอย่างปลั๊กอินที่ได้รับความนิยม เช่น Adobe Flash Player ที่ติดตั้งเพื่อให้เว็บเบราว์เซอร์สามารถเล่นไฟล์ Flash ได้ หรือ Java Runtime ที่ติดตั้งเพื่อใช้งาน Java Application ผ่านเว็บเบราว์เซอร์ เป็นต้น [11-6]

ปลั๊กอินโดยส่วนใหญ่จะถูกพัฒนาโดยผู้พัฒนาภายนอก ซึ่งอาจไม่มีการรับรองเรื่องความมั่นคงปลอดภัย และปลั๊กอินแทบทั้งหมดจะเป็นไฟล์โปรแกรมหรือไลบรารีที่เว็บเบราว์เซอร์จะต้องโหลดเข้ามาในทุกครั้งที่เปิดโปรแกรม เนื่องจากปลั๊กอินเป็นโปรแกรมที่อยู่ภายนอก ทำให้การทำงานของปลั๊กอินต่างๆ นั้นอยู่นอกเหนือการควบคุมของเว็บเบราว์เซอร์ หากปลั๊กอินที่ติดตั้งเพิ่มเข้ามามีช่องโหว่ ก็จะเพิ่มความเสี่ยงที่จะทำให้เบราว์เซอร์ถูกโจมตีผ่านปลั๊กอินดังกล่าวได้ด้วย ตัวอย่างวิดีโอการโจมตีผ่านช่องโหว่ของปลั๊กอินสามารถดูได้จาก http://youtu.be/7MvimAN9fQ8 ซึ่งเป็นการโจมตี Mozilla Firefox ผ่านปลั๊กอิน Adobe Reader

การสร้าง Extension ที่เป็นอันตราย

Extension คือโปรแกรมเสริมที่สามารถติดตั้งเพิ่มเติมเพื่อช่วยขยายความสามารถในการทำงานของเว็บเบราว์เซอร์ เช่น Extension ที่ชื่อ FireFTP ที่ช่วยให้เบราว์เซอร์ Mozilla Firefox สามารถทำงานเป็นโปรแกรม FTP Client ได้ [11-7]

เนื่องจาก Extension เป็นโปรแกรมที่ทำงานร่วมกับเว็บเบราว์เซอร์โดยตรง ทำให้มีผู้พัฒนา Extension เพื่อใช้สร้างความเสียหาย เช่น หลอกลวงผู้ใช้ หรือขโมยข้อมูล เป็นต้น ตัวอย่าง Extension อันตราย เช่น หลอกผู้ใช้ว่าเป็นปลั๊กอินปลอมของ YouTube [11-8] หรือสวมรอยโพสต์ข้อความด้วยบัญชี Facebook ของผู้ใช้ [11-9] เป็นต้น

วิธีการโจมตี

หากเป็นการโจมตีผ่านช่องโหว่ของเว็บเบราว์เซอร์หรือการโจมตีผ่านปลั๊กอิน โดยส่วนใหญ่แฮ็กเกอร์จะสร้างเว็บไซต์ที่ฝังโค้ดอันตรายไว้ แล้วหลอกล่อให้เหยื่อเข้าไปยังเว็บไซต์นั้น ทันทีที่เหยื่อเข้าสู่หน้าเว็บไซต์โค้ดดังกล่าวก็สามารถทำงานได้ทันทีโดยที่เหยื่อแทบไม่รู้ตัว ตัวอย่างการโจมตี เช่น การฝัง Java Script ไว้ในเว็บไซต์เพื่อขโมยข้อมูล เป็นต้น [11-10]

หากเป็นการโจมตีผ่าน Extension ผู้โจมตีจะหลอกล่อให้เหยื่อเปิดเข้าไปที่เว็บไซต์ที่มีให้ดาวน์โหลด Extension มาติดตั้ง โดยจะหลอกว่าเป็น Extension ที่จำเป็นในการใช้งานเว็บไซต์ เพื่อให้เหยื่อหลงเชื่อและเผลอติดตั้ง Extension ดังกล่าว

การโจมตีโดยส่วนใหญ่แฮ็กเกอร์จะใช้วิธีส่งอีเม ลที่มีลิงก์ให้ผู้ใช้คลิก ซึ่งหากผู้ใช้คลิกเข้าสู่ลิงก์ดังกล่าวก็จะตกเป็นเหยื่อโดยทันที ในปัจจุบันมีการพัฒนารูปแบบการโจมตีไปอีกขั้นโดยการโพสต์ลิงก์อันตรายไว้ใน Social Network และเมื่อผู้ใช้หลงคลิกเข้าไปก็จะถูกสวมรอยบัญชีผู้ใช้และเผยแพร่ลิงก์ อันตรายนั้นให้กับผู้อื่นต่อไป ตัวอย่างการเผยแพร่ลิงก์อันตรายใน Social Network เป็นดังรูปที่ 39 (11-2)

รูปที่ 39 (11-2) ตัวอย่างการเผยแพร่ลิงก์อันตรายใน Social Network [11-11]

การป้องกัน

เนื่องจากการที่จะถูกโจมตีผ่านเว็บเบราว์เซอร์ได้นั้น ผู้ที่ตกเป็นเหยื่อต้องเข้าไปยังเว็บไซต์ที่แฮ็กเกอร์สร้างไว้ก่อน ดังนั้น การป้องกันที่ง่ายที่สุดคือการตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ปลายทาง ก่อนที่จะทำการคลิกลิงก์ เช่น ถ้าต้องการเปิดลิงก์จากเว็บบริการย่อ URL ควรนำลิงก์นั้นไปตรวจสอบกับเว็บไซต์ที่ให้บริการขยาย URL เต็ม เช่น http://longurl.org เสียก่อนเพื่อให้แน่ใจว่าปลายทางเป็น URL อะไร รวมถึงการติดตั้งโปรแกรมแอนตี้ไวรัสที่สามารถสแกนเนื้อหาในเว็บไซต์ ก็สามารถช่วยป้องกันอันตรายจากการโจมตีผ่านเว็บเบราว์เซอร์ได้ และสิ่งที่สำคัญที่สุดคือการอัพเดทโปรแกรมเว็บเบราว์เซอร์และปลั๊กอินทุกตัวที่ติดตั้งให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ เพื่อเป็นการปรับปรุงช่องโหว่ไม่ให้แฮ็กเกอร์ใช้ในการโจมตีได้

อ้างอิง

[11-1] http://whatismyipaddress.com/web-browser

[11-2] https://chrome.google.com/webstore

[11-3] http://tech-tweak.com/2011/08/browser-based-operating-systems.html

[11-4] http://www.pcworld.com/businesscenter/article/144490/hackers_increasingly_target_browsers.html

[11-5] http://www.windowsecurity.com/articles/analysis_of_buffer_overflow_attacks.html

[11-6] http://www.tech-faq.com/browser-plugins.html

[11-7] http://fireftp.mozdev.org/

[11-8] http://www.thaicert.or.th/alerts/home/2012/al2012ho0001.html

[11-9] http://www.thaicert.or.th/papers/technical/2012/pp2012te0005.html

[11-10] http://thehackernews.com/2012/01/one-million-pages-infected-by.html

[11-11] http://www.switched.com/2011/04/04/facebook-photoshop-scam-spreading-like-wildfire/

12 อัพโหลดภาพขึ้นสู่สังคมออนไลน์ เรื่องง่ายๆ ที่ต้องระวัง

ผู้เขียน: ปิยเนตร อินทยารักษ์

ผู้ให้คำแนะนำ: เสฏฐวุฒิ แสนนาม

วันที่เผยแพร่: 18 พ.ค. 2555

ปรับปรุงล่าสุด: 18 พ.ค. 2555

ในปัจจุบัน การถ่ายภาพแล้วอัพโหลดขึ้นสู่อินเทอร์เน็ตกำลังเป็นที่นิยม โดยเฉพาะการอัพโหลดขึ้นไปบน Social Network ไม่ว่าจะเป็น Facebook, Twitter หรือนำไปโพสต์ในเว็บบอร์ดต่างๆ โดยปกติแล้ว คนทั่วไปมักเข้าใจว่าข้อมูลในรูปภาพนั้นมีเพียงแค่ภาพถ่ายธรรมดา แต่น้อยคนที่จะรู้ว่าในภาพนั้นมีข้อมูลที่อาจก่อให้เกิดการละเมิดสิทธิส่วนบุคคลหรือความเป็นส่วนตัว จนถึงขั้นก่อให้เกิดอันตรายต่อผู้ที่ถ่ายภาพหรือผู้ที่อยู่ในภาพได้ เช่น ข้อมูลตำแหน่งพิกัดที่อยู่ในเวลาที่ภาพนั้นถูกถ่าย เนื่องจากกล้องดิจิทัลหรือโทรศัพท์มือถือรุ่นใหม่ จะมีความสามารถ GeoTagging [12-1] ซึ่งเป็นการใช้ GPS ในการระบุพิกัดตำแหน่ง แล้วบันทึกข้อมูลเหล่านี้ลงใน Metadata ของภาพ โดยทั่วไปแล้ว ผู้ที่ใช้งาน Social Network ส่วนใหญ่จะไม่ระบุข้อมูลส่วนตัวที่สำคัญ เช่น บ้านเลขที่ของตนเองไว้ใน Profile แต่เมื่อไหร่ก็ตามที่ผู้ใช้ถ่ายภาพในบริเวณบ้านของตนเองแล้วโพสต์ภาพนั้นขึ้นสู่อินเทอร์เน็ต ก็อาจเป็นการเปิดเผยให้ผู้อื่นสามารถทราบที่อยู่ของผู้ใช้คนนั้นได้ ดังนั้น การศึกษาเรื่อง Metadata ในภาพถ่าย ความสามารถของ GeoTagging และอันตรายที่อาจเกิดขึ้น รวมถึงวิธีป้องกันและแก้ไข ก็สามารถช่วยป้องกันไม่ให้ข้อมูลสำคัญที่เป็นความลับถูกเผยแพร่ออกไปได้

ในการถ่ายภาพนั้นนอกจากจะมีข้อมูลที่เป็นตัวภาพแล้ว ยังมีส่วนที่เป็น Metadata ซึ่งเป็นส่วนอธิบายข้อมูลเพิ่มเติมของภาพนั้นๆ

Metadata คืออะไร

Metadata คือ ข้อมูลที่ใช้อธิบายรายละเอียดเพิ่มเติมของข้อมูลหรือสารสนเทศต่างๆ เช่น ไฟล์เอกสารจะมีส่วนแสดงรายละเอียดของไฟล์ เช่น ชื่อผู้สร้างเอกสาร ชื่อหน่วยงาน ชื่อคอมพิวเตอร์ที่ใช้สร้างเอกสาร เป็นต้น หรือแม้กระทั่ง ID3 ในไฟล์ MP3 ก็จะเก็บข้อมูลชื่อเพลง ชื่อศิลปิน ชื่ออัลบั้ม เป็นต้น ในกรณีที่เป็นภาพถ่ายดิจิทัลก็จะมีข้อมูลเพิ่มเติมของภาพนั้นๆ เช่น วันและเวลาที่ถ่ายภาพ การตั้งค่าของกล้อง เป็นต้น [12-2]

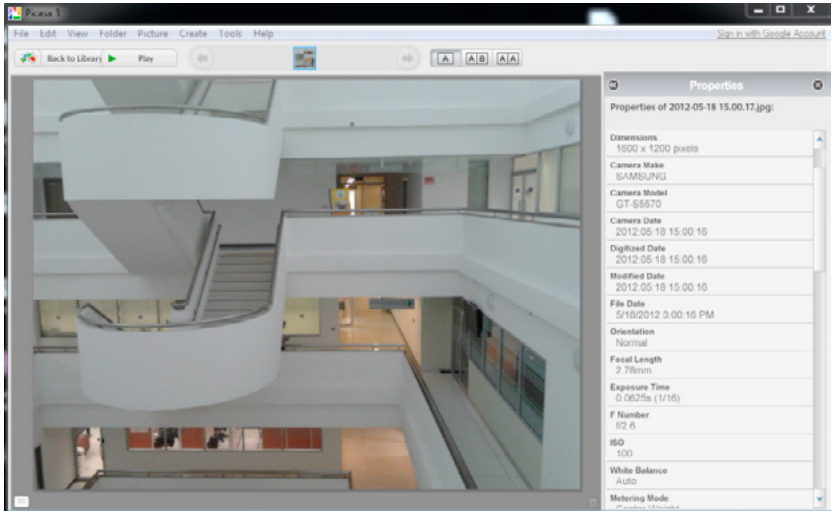
Metadata ของภาพถ่าย

Metadata ของภาพถ่าย จะเก็บไว้ในส่วนที่เรียกว่า EXIF (Exchangeable Image File Format) ซึ่งเป็นข้อมูลที่อธิบายรายละเอียดค่าต่างๆ ของรูปภาพที่ถ่ายจากกล้องดิจิทัล ดังรูปที่ 40 (12-1) โดยปกติแล้วไฟล์รูปภาพที่รองรับการใส่ข้อมูล EXIF คือไฟล์ชนิด JPEG และ TIFF [12-3] ตัวอย่างค่า EXIF ที่สำคัญ เช่น

Model – รุ่นของกล้อง

Date Time Original – วันเวลาที่ถ่ายภาพ

GPS - ตำแหน่งที่ถ่ายภาพ



รูปที่ 40 (12-1) แสดงค่า EXIF

จะดูค่า EXIF ได้อย่างไร

การดูค่า EXIF สามารถทำได้หลายวิธี ตัวอย่างเช่นการดูภาพจาก Windows Explorer ทำได้โดยการคลิกขวาที่รูปภาพ เลือก Properties และเลือกที่ Details จะเห็นข้อมูลเพิ่มเติมของภาพนั้น นอกจากนี้ยังมีโปรแกรมดูรูปภาพอีกมากมายที่สามารถดูข้อมูล EXIF ได้ เช่น PhotoScape, Picasa เป็นต้น

ในส่วนของการดูค่า EXIF ของรูปภาพในเว็บไซต์ต่างๆ โดยไม่ต้องบันทึกรูปภาพนั้นลงในเครื่อง สามารถทำได้โดยการติดตั้ง Extension ให้กับเบราว์เซอร์ เช่น Google Chrome และ Mozilla Firefox สามารถติดตั้ง Extension ที่ชื่อ Exif Viewer เพื่อดูข้อมูล EXIF ได้

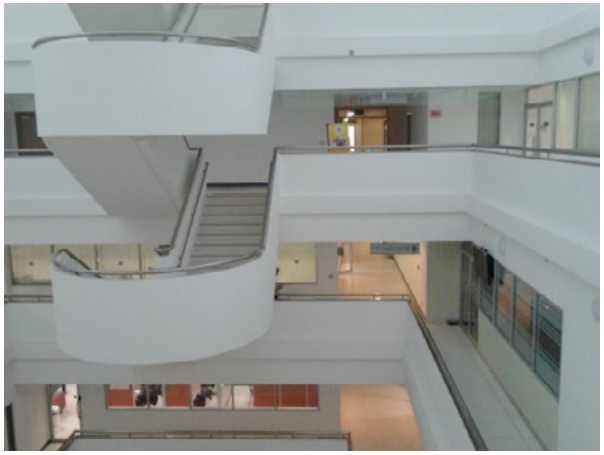
จากข้อมูลในภาพถ่ายที่สามารถบ่งบอกรายละเอียดต่างๆ ที่เกี่ยวข้องกับผู้ถ่ายภาพหรือผู้ที่อยู่ในภาพได้ ทำให้หลายฝ่ายมีความวิตกกังวลถึงข้อมูลส่วนตัวที่อาจหลุดออกไปเผยแพร่สู่อินเทอร์เน็ต ซึ่งมีผลต่อความเป็นส่วนตัว (Privacy) จนอาจก่อให้เกิดอันตรายต่อชีวิตและทรัพย์สินได้

Privacy สำคัญอย่างไร

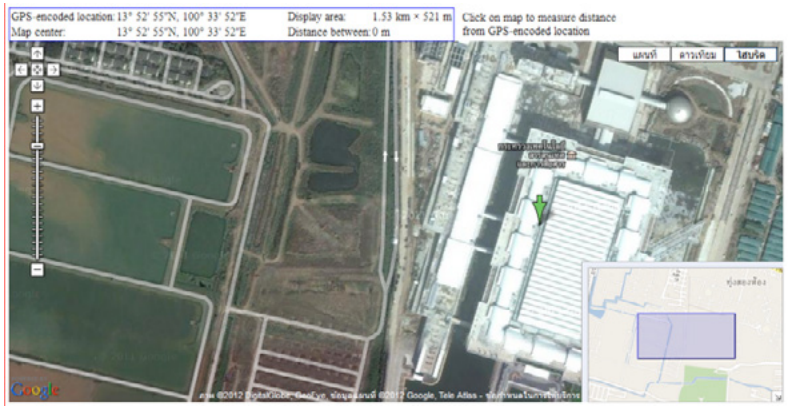
Privacy คือ ความเป็นส่วนตัวในการเก็บรักษาข้อมูล หรือการเผยแพร่ข้อมูลให้แก่ผู้อื่น ในโลกของอินเทอร์เน็ตแล้ว การนำข้อมูลส่วนตัวขึ้นไปเผยแพร่นั้นเป็นสิ่งที่ต้องระมัดระวัง เนื่องจากข้อมูลบางอย่างอาจส่งผลต่อภาพลักษณ์ หน้าที่การทำงาน หรืออาจมีผลเสียหายต่อชีวิตและทรัพย์สินเลยก็เป็นได้ [12-4] ตัวอย่างกรณีศึกษาที่เกี่ยวข้องกับ Privacy ที่น่าสนใจ คือ ภรรยาของหัวหน้าสายลับที่ MI6 ได้นำรูปภาพที่ถ่ายกับสามีและรูปบ้านของเธอไปโพสต์ไว้ใน Facebook ทำให้บุคคลอื่นล่วงรู้ว่าสามีของเธอเป็นสายลับพร้อมทั้งรู้บ้านเลขที่ สมาชิกในครอบครัวและเครือญาติ ซึ่งการที่ข้อมูลดังกล่าวถูกเปิดเผยทำให้ให้สามีของเธอไม่สามารถทำงานเป็น สายลับได้อีกต่อไป [12-5]

ข้อมูลในภาพบอกตำแหน่งได้อย่างไร

ในการถ่ายภาพ กล้องที่มีความสามารถ GeoTagging ก็จะบันทึกข้อมูล GPS ณ ตำแหน่งที่ถ่ายลงไปในภาพด้วย และหากมีการนำภาพนั้นขึ้นสู่อินเทอร์เน็ตก็จะทำให้ผู้อื่นสามารถรู้สถานที่ ที่ถ่ายภาพนั้นได้ ในปัจจุบันมีเครื่องมือมากมายที่ช่วยอำนวยความสะดวกในการดูข้อมูลสถานที่ที่ ถ่ายภาพ เช่น การดูข้อมูลในภาพด้วยเว็บไซต์ http://regex.info/exif.cgi ซึ่งนอกจากจะบอกรายละเอียดของ EXIF ของภาพนั้นแล้ว ยังสามารถแสดงภาพถ่ายจากดาวเทียมของสถานที่นั้นได้ด้วย ดังรูปที่ 41 (12-2) และ 42 (12-3)



รูปที่ 41 (12-2) แสดงถึงภาพที่จะนำไปดูผ่านทางเว็บไซต์ http://regex.info/exif.cgi

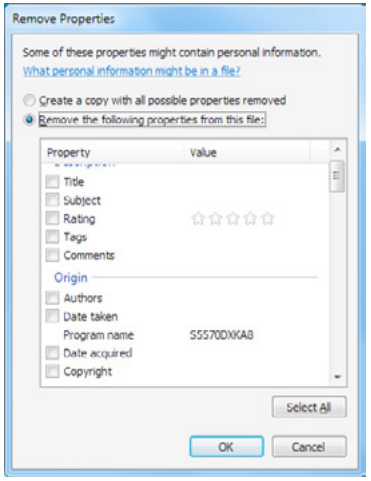


รูปที่ 42 (12-3) แสดงภาพถ่ายดาวเทียมของตำแหน่งที่ถ่ายรูปที่ 41 (12-2)

วิธีป้องกัน

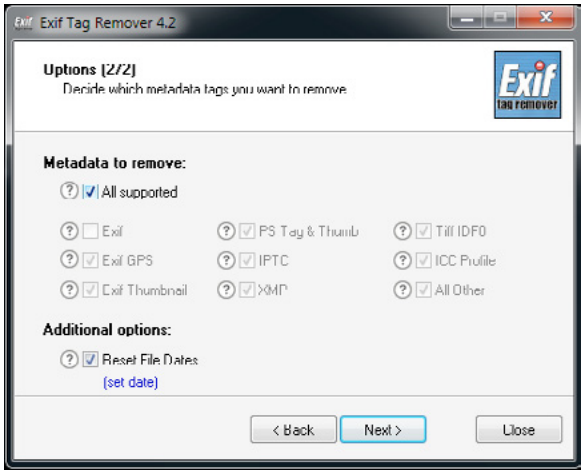
ในการถ่ายภาพด้วยกล้องดิจิทัลหรือโทรศัพท์มือถือ หากไม่มีความจำเป็นที่จะต้องระบุข้อมูลสถานที่ถ่ายภาพ ก็ควรจะปิดการทำงานของ GeoTagging แต่หากเป็นภาพที่ถูกถ่ายมาแล้วและต้องการนำภาพนั้นขึ้นสู่อินเทอร์เน็ต ควรมีการป้องกันไม่ให้ภาพถ่ายเปิดเผยข้อมูลส่วนตัวของผู้ใช้งาน ซึ่งสามารถทำได้โดยการลบข้อมูล EXIF ออกจากภาพนั้นก่อนที่จะอัพโหลดขึ้นสู่อินเทอร์เน็ต การลบ EXIF สามารถทำได้หลายวิธี เช่น

1. ลบข้อมูล EXIF โดยใช้ Windows Explorer ด้วยการคลิกขวาที่ไฟล์ภาพ เลือก Properties และเลือกที่ Details จากนั้นคลิกที่ Remove Properties and Personal Information เลือกค่า EXIF ที่ต้องการลบ [12-6] ดังรูปที่ 43 (12-4)



รูปที่ 43 (12-4) แสดงการลบข้อมูล EXIF จาก Windows Explorer

2. ลบข้อมูล EXIF โดยใช้ซอฟต์แวร์ที่ทำขึ้นมาโดยเฉพาะ เช่น Exif Tag Remover เป็นต้น ดังรูปที่ 44 (12-5)



รูปที่ 44 (12-5) แสดงการลบค่า EXIF ด้วยโปรแกรม Exif Tag Remover

จากความอันตรายของการเปิดเผยตำแหน่งที่อยู่ ผู้ใช้งานควรตรวจสอบข้อมูลในรูปภาพก่อนที่จะอัพโหลดขึ้นสู่อินเทอร์เน็ต เพื่อให้แน่ใจว่าข้อมูลนั้นสามารถถูกเผยแพร่ได้ หากพบข้อมูลที่ไม่เหมาะสมก็ไม่ควรที่จะโพสต์ภาพนั้นหรือหากจำเป็นต้องโพสต์ ก็ควรทำการลบข้อมูล EXIF ออกจากภาพ เพื่อป้องกันการเผยแพร่ข้อมูลสำคัญออกไปโดยไม่ตั้งใจ เพราะถ้าหากเผลอปล่อยให้ข้อมูลดังกล่าวถูกเผยแพร่ออกไปแล้ว การที่จะลบหรือแก้ไขความผิดพลาดนั้นอาจจะไม่สามารถทำได้เลย

อ้างอิง

[12-1] http://en.wikipedia.org/wiki/Geotagging
[12-2] http://graphicssoft.about.com/od/glossary/f/metadata.htm
[12-3] http://www.cipa.jp/english/hyoujunka/kikaku/pdf/DC-008-2010_E.pdf
[12-4] http://en.wikipedia.org/wiki/Privacy
[12-5] http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html
[12-6] http://www.labnol.org/software/remove-photograph-metadata/19588/

13 ป้องกันบัญชีผู้ใช้ GMAIL / HOTMAIL จากการถูกแฮ็กด้วยวิธีง่ายๆ

ผู้เขียน: ณราพร ดวงศรี
ผู้ให้คำแนะนำ: เจษฎา ช้างสีสังข์
วันที่เผยแพร่: 1 มิ.ย. 2555
ปรับปรุงล่าสุด: 1 มิ.ย. 2555

อีเมลนับเป็นสิ่งจำเป็นที่เข้ามามีบทบาทและมีความสำคัญต่อชีวิตประจำวันของเราเป็นอย่างมาก เพราะเป็นวิธีการติดต่อสื่อสารที่รวดเร็วและแทบจะไม่มีต้นทุน หลายคนเก็บข้อมูลสำคัญไว้ในอีเมลหรือใช้อีเมลในการติดต่อทางด้านธุรกิจ ซึ่งหากผู้ใช้เข้าใช้งานอีเมลผ่านการเชื่อมต่อที่ไม่มีความมั่นคงปลอดภัย ก็อาจทำให้บัญชีผู้ใช้นั้นถูกโจรกรรมได้โดยง่าย

Gmail และ Hotmail เป็นบริการฟรีอีเมลที่มีผู้นิยมใช้กันมากเป็นอันดับต้นๆ (ในปี ค.ศ. 2011 ทั่วโลกมีจำนวนของผู้ใช้งาน Hotmail ประมาณ 350 ล้านคน และ Gmail ประมาณ 260 ล้านคน) [13-1] ผู้เขียนจึงได้เลือกบริการอีเมลเหล่านี้มาแนะนำเพื่อให้ผู้อ่านได้ปฏิบัติ ในปัจจุบันนั้น ถึงแม้ว่าผู้ให้บริการจะมีระบบที่มีความมั่นคงปลอดภัยอยู่แล้ว แต่ตัวผู้ใช้เองก็ควรที่จะเรียนรู้ข้อปฏิบัติเบื้องต้นรวมถึงวิธีการป้องกัน แบบต่างๆ เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้น ด้วยวิธีการต่างๆ ดังนี้

1. การตั้งค่า Gmail ให้มีการยืนยันแบบ 2 ขั้นตอน (2-step verification)

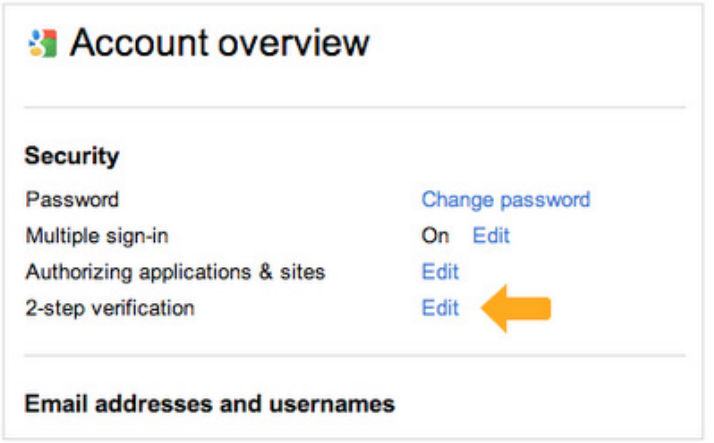
เป็นการใช้ Two Factor Authentication [13-2] ซึ่งเป็นวิธีการพิสูจน์ตัวตนที่ต้องใช้ข้อมูล 2 ส่วนร่วมกันเพื่อเพิ่มความมั่นคงปลอดภัยให้กับการเข้าสู่ระบบหรือบริการ โดยหลักๆ แล้วจะใช้ข้อมูลจาก 2 ใน 3 ส่วนนี้คือ

1) สิ่งที่รู้ (Something you know) เช่น รหัสผ่าน

2) สิ่งที่มี (Something you have) เช่น โทรศัพท์มือถือ, รหัสบัตรเติมเงิน

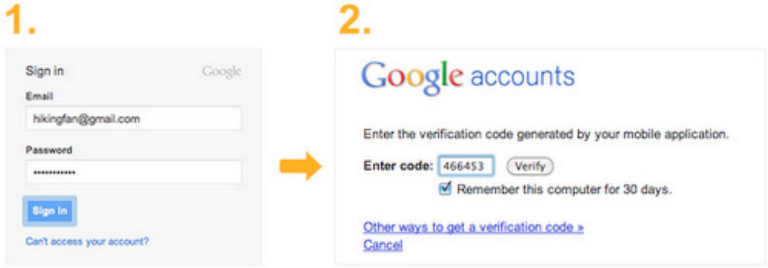
3) สิ่งที่เป็น (Something you are) เช่น ลายนิ้วมือ, ม่านตา

การยืนยันอีเมลแบบ 2 ขั้นตอน [13-3] [13-4] ช่วยลดโอกาสในการถูกขโมยข้อมูลส่วนตัวในบัญชีอีเมลของเราลงได้ เพราะต่อให้ใส่ชื่อผู้ใช้และรหัสผ่านถูกต้องแล้ว ก็ยังไม่สามารถเข้าถึงบัญชีอีเมลได้ จนกว่าจะใส่รหัส Pin 6 หลักที่ได้รับจาก SMS ผ่านโทรศัพท์มือถือที่ลงทะเบียนไว้กับ Google เสียก่อน การตั้งค่าการยืนยันยืนยันด้วยวิธีนี้สามารถทำได้โดยไปที่ การตั้งค่าบัญชี และเลือก 2-step verification ตามรูปที่ 45 (13-1) แล้วทำตามขั้นตอนของเว็บไซต์



รูปที่ 45 (13-1) แสดงการตั้งค่าการยืนยันแบบ 2 ขั้นตอน
ที่มา http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html

ในการใช้งาน หากเราตั้งค่าการยืนยันแบบ 2 ขั้นตอนแล้วนั้น เมื่อเราเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่ถูกต้อง จะมี SMS แจ้งรหัส Pin 6 หลัก เพื่อให้เรานำมาป้อนเข้าระบบก่อนจึงจะสามารถเข้าใช้งานอีเมลได้ ตามรูปที่ 46 (13-2) และสามารถเลือกบันทึกรหัสผ่านไว้ในเครื่องได้ 30 วัน ส่วน Hotmail นั้นในปัจจุบันนี้ยังไม่มีฟังก์ชั่นที่รองรับ Two Factor Authentication

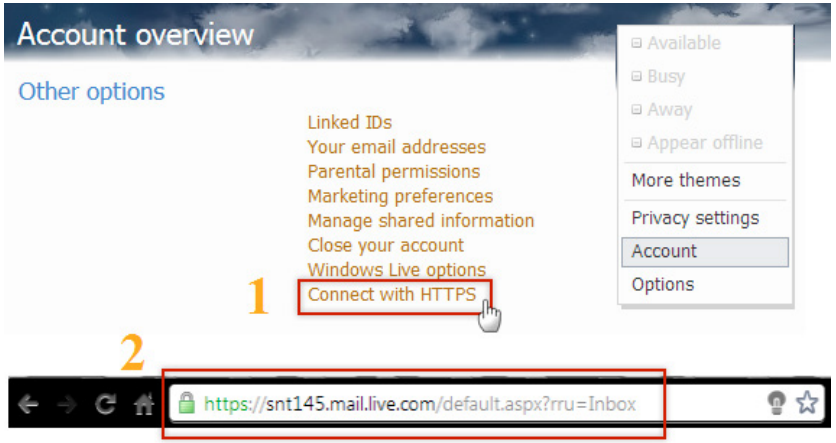


รูปที่ 46 (13-2) แสดงการเข้าใช้งานเมื่อมีการตั้งค่าการยืนยันแบบ 2 ขั้นตอน
ที่มา http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html

นอกจากการรับรหัส Pin 6 หลักผ่าน SMS แล้ว ยังสามารถใช้วิธีการรับรหัสด้วยการให้ Google โทรศัพท์เข้ามาแจ้งหมายเลข Pin หรือผู้ที่ใช้ Smart Phone สามารถติดตั้งแอปพลิเคชั่นที่ชื่อ Google Authenticator เพื่อสร้างรหัส Pin สำหรับเข้าใช้งาน Gmail ได้ด้วย

2. การใช้งาน Hotmail แบบ HTTPS

ปัจจุบัน ค่าเริ่มต้นในการใช้งาน Gmail จะเป็นการใช้งานผ่านโพรโทคอล HTTPS แต่สำหรับ Hotmail จะใช้งานผ่านโพรโทคอล HTTP ซึ่งไม่มีการเข้ารหัสลับข้อมูล ดังนั้นการใช้งานให้มีความมั่นคงปลอดภัยควรตั้งค่าให้ใช้งานผ่านโพรโทคอล HTTPS ซึ่งเป็นการเข้ารหัสลับข้อมูลด้วยโพรโทคอล TLS/SSL (Transport Layer Security/Secure Sockets Layer) การตั้งค่าการเชื่อมต่อแบบ HTTPS ทำได้โดยการคลิกที่ ตั้งค่าบัญชีผู้ใช้ (Account) ที่หน้า Account Overview ในหัวข้อ Other options ให้คลิก Connect with HTTPS [13-5] ตามรูปที่ 47 (13-3) หลังจากทำการตั้งค่าเสร็จเรียบร้อยแล้ว จะทำให้การรับส่งข้อมูลบนเว็บไซต์ Hotmail ถูกเข้ารหัสลับเสมอ



รูปที่ 47 (13-3) (1) แสดงการตั้งค่าการใช้งาน Hotmail แบบ HTTPS เข้ารหัสลับ (2) แสดง URL ที่มีการตั้งค่า HTTPS แล้ว

3. คำแนะนำในการตั้งค่าโปรแกรมอีเมลไคลเอ็นต์ในการรับส่งอีเมลจาก Gmail

โปรแกรมอีเมลไคลเอ็นต์ (Email client) คือโปรแกรมที่ใช้รับและส่งอีเมล โดยมีโปรแกรมที่ได้รับความนิยม เช่น Microsoft Outlook, Thunderbird เป็นต้น ในการรับส่งอีเมลจากโปรแกรมอีเมลไคลเอ็นต์ จะรับอีเมลด้วยโพรโทคอล POP3, IMAP และส่งอีเมลด้วยโพรโทคอล SMTP โดยการที่จะเชื่อมต่อเพื่อใช้งานเมลไคลเอ็นต์นั้น ควรมีการเชื่อมต่อผ่านช่องทางที่มีการเข้ารหัสลับข้อมูลด้วย ซึ่งในปัจจุบันบริการ Gmail และ Hotmail เองก็มีการเข้ารหัสลับข้อมูลทุกครั้งที่มีการรับส่งด้วยโพรโทคอล SSL/TLS ที่รองรับทั้ง POP, IMAP และ SMTP ซึ่งโพรโทคอลที่รับส่งมีความหมายเบื้องต้นดังนี้

POP (Post Office Protocol) เป็นโพรโทคอลที่ใช้ในการรับอีเมลจากเซิร์ฟเวอร์ ปัจจุบันเวอร์ชันล่าสุดคือ POP3 การทำงานของ POP เป็นการอ่านอีเมลแบบออฟไลน์ คืออีเมลที่เข้ามาจะถูกเก็บอยู่ในเซิร์ฟเวอร์ เมื่อใช้โปรแกรมอีเมลไคลเอ็นต์ในการเข้าใช้งานอีเมล จะทำการดาวน์โหลดอีเมลมาเก็บไว้ในเครื่องของเราก่อน จึงจะสามารถอ่านอีเมลได้ และสามารถกลับมาอ่านอีเมลเดิมได้ในภายหลัง แม้ไม่ได้เชื่อมต่อกับอินเทอร์เน็ต หรือหากว่าเราทำการลบอีเมลใดในโปรแกรมอีเมลไคลเอ็นต์ อีเมลนั้นทางเซิร์ฟเวอร์ก็จะยังคงอยู่

IMAP (Internet Message Access Protocol) เป็นโพรโทคอลที่ใช้ในการรับอีเมลจากเซิร์ฟเวอร์ ปัจจุบันเวอร์ชันล่าสุดคือ IMAP4 การทำงานของ IMAP จะแตกต่างกับ POP3 เนื่องจาก IMAP เป็นโพรโทคอลที่สนับสนุนการอ่านอีเมล ทั้งแบบออฟไลน์และออนไลน์ โดยแบบออนไลน์นั้น จะเป็นการโต้ตอบกับเซิร์ฟเวอร์ คือเมื่อใช้โปรแกรมอีเมลไคลเอ็นต์ในการเข้าใช้งานอีเมล ก็เหมือนเราเข้าใช้งานผ่านทางเว็บเบราว์เซอร์ หากว่าเราทำการลบอีเมลในเครื่องอีเมลไคลเอ็นต์ ทางเซิร์ฟเวอร์ก็จะลบอีเมลนั้นด้วย นอกจากนี้ยังสามารถเลือกดาวน์โหลดเฉพาะอีเมลที่เราต้องการได้ด้วย

SMTP (Simple Mail Transfer Protocol) เป็นโพรโทคอลที่ใช้ในการส่งอีเมลในเครือข่ายอินเทอร์เน็ต สำหรับในกรณีที่เราต้องการนำ Gmail หรือ Hotmail ไปใช้กับโปรแกรมอีเมลไคลเอ็นต์นั้น สามารถปฏิบัติตามคำแนะนำ ซึ่งในที่นี้จะยกตัวอย่างการตั้งค่า Thunderbird เพื่อใช้งานร่วมกับ Gmail ส่วน Hotmail นั้นมีการตั้งค่าที่คล้ายคลึงกัน ผู้อ่านสามารถประยุกต์การใช้งาน ดังตัวอย่างดังนี้

ตัวอย่างการตั้งค่า Thunderbird ให้รองรับ POP, IMAP และ SMTP ใน Gmail

ก่อนที่จะทำการตั้งค่าให้กับโปรแกรมไคลเอ็นต์ เราต้องตั้งค่า POP/IMAP ในบัญชีอีเมลของเราก่อน โดยเปิดการใช้งาน SSL จากนั้นจึงทำการตั้งค่าโปรแกรมอีเมลไคลเอนต์ เป็นดังรูปที่ 48 (13-4), 49 (13-5) และ 50 (13-6)

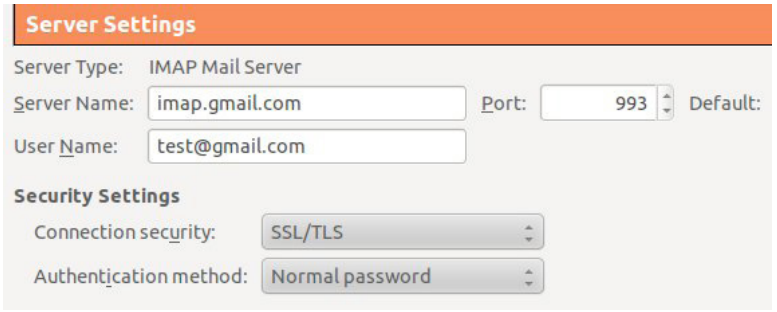
การตั้งค่าสำหรับ IMAP

Server Name : imap.gmail.com

User Name : ที่อยู่อีเมล (username@gmail.com หรือ username@your_domain.com)

Port : 993 (ใช้ได้ทั้ง Gmail และ Hotmail)

Password : รหัสผ่าน



รูปที่ 48 (13-4) แสดงการตั้งค่า IMAP ให้กับโปรแกรมอีเมลไคลเอ็นต์

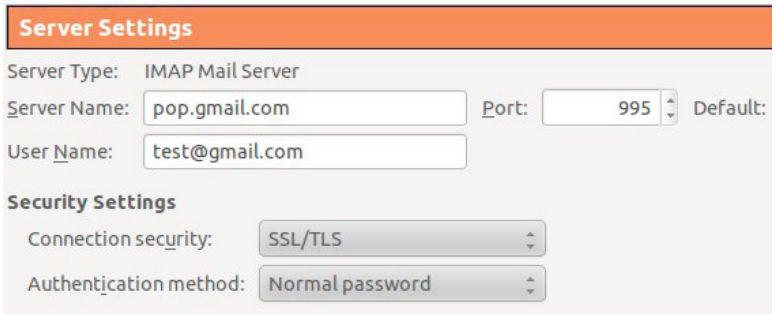
การตังค่าสำหรับ POP

Server Name : pop.gmail.com

User Name : ที่อยู่อีเมล (username@gmail.com หรือ username@your_domain.com)

Port : 995 (ใช้ได้ทั้ง Gmail และ Hotmail)

Password : รหัสผ่าน



รูปที่ 49 (13-5) แสดงการตั้งค่า POP ให้กับโปรแกรมอีเมลไคลเอ็นต์

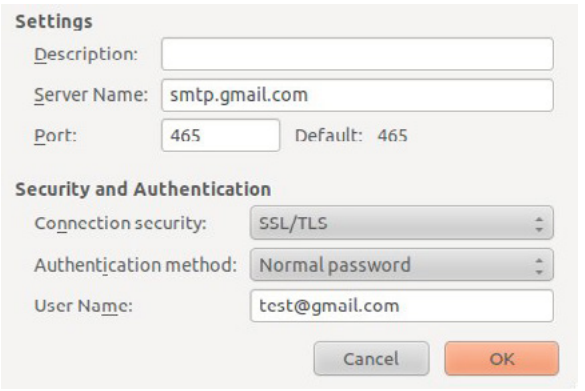
การตังค่าสำหรับ SMTP

Server Name : smtp.gmail.com

User Name : ที่อยู่อีเมล (username@gmail.com หรือ username@your_domain.com)

Port : 465 หรือ 587 (สำหรับ Gmail) และ 25 (สำหรับ Hotmail)

Password : รหัสผ่าน



รูปที่ 50 (13-6) แสดงการตั้งค่า SMTP ให้กับโปรแกรมอีเมลไคลเอ็นต์

4. การตรวจสอบข้อมูลกิจกรรมในบัญชีอีเมลอย่างสม่ำเสมอ

การตรวจสอบข้อมูลกิจกรรมในบัญชีอีเมล [13-6] เป็นบริการของ Gmail ซึ่งทำให้ผู้ใช้สามารถเช็คได้ว่ามีผู้อื่นเข้าใช้งานอีเมลของเราโดยไม่ได้ รับอนุญาตหรือไม่ และยังสามารถตรวจสอบ IP Address ของเครื่องที่ใช้ในการเข้าสู่บัญชีอีเมลของเราได้อีกด้วย

การเรียกดูข้อมูลกิจกรรมของบัญชีอีเมล ทำได้โดยการเข้าสู่ระบบ Gmail จากนั้นเลื่อนลงมาที่กิจกรรมล่าสุดของบัญชีและคลิกที่รายละเอียด ภายในกิจกรรมล่าสุดของบัญชีจะแสดงประเภทของการเข้าถึง (เช่น เบราว์เซอร์, มือถือ, POP) ตำแหน่ง (IP Address ของเครื่องที่ใช้ในการเข้าสู่บัญชีอีเมล) มีการระบุประเทศและวัน/เวลา ของกิจกรรมที่เกิดขึ้นในอีเมลของเรา ตามรูปที่ 51 (13-7) หากพบว่ามี IP Address อื่นที่ไม่รู้จักหรือวัน/เวลา ที่เราไม่ได้เข้าใช้งาน อาจเป็นสัญญาณบอกว่าบัญชีของเราถูกแฮ็ก ให้ทำการเปลี่ยนรหัสผ่านทันที

กิจกรรมในบัญชีนี้

เครื่องมือนี้ให้ข้อมูลเกี่ยวกับกิจกรรมล่าสุดในบัญชีอีเมลนี้และกิจกรรมอื่นๆ ที่เกิดขึ้นพร้อมกัน อ่านเพิ่มเติม

เราไม่พบว่ามีการเปิดบัญชีนี้ที่อื่น

กิจกรรมล่าสุด:

ประเภทการเข้าถึง [?] (เบราว์เซอร์, มือถือ, POP3 เป็นต้น)	ตำแหน่ง (ที่อยู่ IP) [?]	วัน/เวลา (แสดงตามเขตเวลาของคุณ)
เบราว์เซอร์	* ไทย (203.113.103.201)	10:32 (3 ชั่วโมงที่แล้ว)
เบราว์เซอร์	* ไทย (180.180.246.114)	11 เม.ย. (23 ชั่วโมงที่แล้ว)
เบราว์เซอร์	* ไทย (180.180.246.114)	11 เม.ย. (1 วันที่แล้ว)
เบราว์เซอร์	* ไทย (180.180.246.114)	11 เม.ย. (1 วันที่แล้ว)
เบราว์เซอร์	* ไทย (124.122.62.239)	9 เม.ย. (3 วันที่แล้ว)

ค่ากำหนดของการเตือน: แสดงการแจ้งเตือนสำหรับกิจกรรมที่ผิดปกติ เปลี่ยน

รูปที่ 51 (13-7) แสดงตารางข้อมูลกิจกรรมของบัญชีอีเมล

5. ข้อควรระวังในการเข้าใช้งานจากเครื่องคอมพิวเตอร์สาธารณะ

ในการใช้งานเครื่องคอมพิวเตอร์สาธารณะ เราไม่สามารถรู้ได้เลยว่าเครื่องนั้นมีซอฟต์แวร์อะไรติดตั้งอยู่บ้าง บางเครื่องอาจมีโปรแกรม Keylogger แอบแฝงอยู่ ซึ่งเป็นโปรแกรมที่จะคอยดักจับการใช้งานต่างๆ เช่น การกดปุ่มคีย์บอร์ด [13-7] หากเราทำการล็อกอินเข้าใช้งานบัญชีอีเมลผ่านเครื่องคอมพิวเตอร์สาธารณะที่มีโปรแกรม Keylogger อยู่ ข้อมูลชื่อผู้ใช้และรหัสผ่านของเราหรือทุกอย่างที่เราพิมพ์ลงไปก็จะถูก บันทึกไว้ทั้งหมด หากจำเป็นต้องใช้คอมพิวเตอร์สาธารณะในการเช็คอีเมล ควรใช้วิธีการพิมพ์ผ่าน On-Screen Keyboard [13-8] ซึ่งเป็นโปรแกรมที่จำลองการทำงานของคีย์บอร์ด โดยการใช้เมาส์คลิกแทนการกดปุ่มในคีย์บอร์ด ทำให้เราสามารถป้อนข้อมูลต่างๆ ได้เหมือนการพิมพ์ในคีย์บอร์ดจริง ซึ่งจะช่วยป้องกันซอฟต์แวร์ Keylogger ได้ โปรแกรม On-Screen Keyboard จะถูกติดตั้งมาพร้อมกับระบบปฏิบัติการ Windows ตั้งแต่ XP ขึ้นไป สามารถเรียกใช้งานได้ตามรูปที่ 52 (13-8) แต่หากไม่มีก็สามารถดาวน์โหลดโปรแกรม On-Screen Keyboard ของผู้พัฒนาภายนอกมาติดตั้งเพิ่มเติมได้

รูปที่ 52 (13-8) (1) แสดงการเรียกใช้โปรแกรม On Screen Keyboard ในระบบปฏิบัติการวินโดวส์ 7 (2) ตัวอย่างของโปรแกรม On Screen Keyboard

6. การตั้งรหัสผ่านที่ทำให้คาดเดาได้ยาก

การตั้งรหัสผ่านที่ดีก็เป็นสิ่งสำคัญในการที่จะป้องกันอีเมล เพราะ จะทำให้ยากต่อการคาดเดา หรืออาจต้องใช้เวลานานมาก ส่วนการตั้งรหัสผ่านที่ไม่ดี จะทำให้ผู้ที่ไม่ประสงค์ดี สามารถเข้าสู่ระบบของเราได้โดยง่าย (ศึกษาการตั้งค่ารหัสผ่านเพิ่มเติมได้ที่ http://www.thaicert.or.th/papers/normal/2012/pp2012no0005.html)

คำแนะนำเบื้องต้นในการการตั้งรหัสผ่าน

1. ใช้อักษรไม่ต่ำกว่า 6-8 ตัวอักษร
2. ไม่ใช้รหัสผ่านซ้ำกับที่เคยใช้ไปแล้วในระบบอื่นๆ หรือ เหมือนกับชื่อบัญชี หรือ ชื่อ-นามสกุลของผู้ใช้ เป็นต้น
3. รหัสผ่านควรประกอบด้วยตัวอักษรหลากหลายตัวผสมกันเช่น ตัวพิมพ์เล็ก, ตัวพิมพ์ใหญ่, ตัวเลข และอักขระพิเศษ
4. ใช้คำที่ไม่ปรากฏในพจนานุกรม หรือหาความหมายไม่ได้
5. ควรเปลี่ยนรหัสผ่านให้บ่อยที่สุดเท่าที่ทำได้ เช่น อย่างน้อย 3 เดือนต่อครั้ง

นอกจากการตั้งรหัสผ่านที่ดีแล้ว ผู้ใช้เองก็มีส่วนในการป้องกันด้วย เช่น

ไม่จดชื่อบัญชี / รหัสผ่าน ใส่กระดาษ
ไม่บอก ชื่อบัญชี / รหัสผ่าน กับใคร ไม่ว่าจะทางใดก็ตาม
ไม่ใช้ตัวเลือกในเบราว์เซอร์ในการช่วยจำรหัสผ่าน

สรุป

ผู้ที่ใช้งานอีเมล ไม่ว่าจะในด้านธุรกิจ หรือติดต่อสื่อสารข้อมูลทั่วไปก็ ควรที่จะเรียนรู้ข้อปฏิบัติที่เป็นประโยชน์ในการเสริมสร้างความมั่นคงปลอดภัยในการใช้งาน เพื่อเป็นการป้องกันการถูกแฮ็กอีเมลจากผู้ไม่หวังดี ซึ่งอาจใช้บัญชีของเราในการเข้าถึงข้อมูลส่วนบุคคล หรืออาจนำไปใช้ในการสร้างความเสียหายอื่นๆ ที่ไม่คาดคิดได้

อ้างอิง

[13-1] http://www.email-marketing-reports.com/metrics/email-statistics.htm
[13-2] http://www.rsa.com/glossary/default.asp?id=1056
[13-3] http://support.google.com/accounts/bin/topic.py?hl=en&topic=28786
[13-4] http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html
[13-5] http://windows.microsoft.com/th-TH/hotmail/hacked-account-faq
[13-6] http://support.google.com/mail/bin/answer.py?hl=th&answer=45938&topic=1669043&ctx=topic
[13-7] http://compnetworking.about.com/od/networksecurityprivacy/g/keylogger.htm
[13-8] http://windows.microsoft.com/en-us/windows7/Type-without-using-the-keyboard-On-Screen-Keyboard

14 WEB BROWSER กับการป้องกัน PHISHING WEBSITE

ผู้เขียน: ไพชยนต์ วิมุกตะนันทน์

วันที่เผยแพร่: 29 มิถุนายน 2555
ปรับปรุงล่าสุด: 29 มิถุนายน 2555

สำหรับผู้ที่ใช้บริการธนาคารทางอินเทอร์เน็ตคงจะเคยเห็นคำเตือนให้ระวังเว็บไซต์ หลอกลวงหรืออีเมล์หลอกลวงที่ธนาคารแต่ละแห่งประกาศเตือน บางท่านที่อยู่ในแวดวง IT อาจจะทราบดีอยู่แล้วว่าปัจจุบันอาชญากรทางอินเตอร์เน็ตได้หันมาประกอบ อาชญากรรมในรูปแบบที่หวังผลกำไรมากขึ้นกว่าแต่ก่อน การสร้างเว็บไซต์ปลอมของธนาคารทางอินเตอร์เน็ตเพื่อหลอกลวงผู้ใช้งานก็เป็น รูปแบบหนึ่งที่ทำรายได้ให้กับอาชญากรทางคอมพิวเตอร์อย่างสำคัญ เนื่องจากหากมีผู้ที่ตกเป็นเหยื่อของการหลอกลวงรูปแบบนี้ก็เท่ากับว่า อาชญากรคอมพิวเตอร์สามารถเข้าถึงบัญชีเงินฝากของเหยื่อในธนาคารได้โดยตรงนั่นเอง

อาชญากรรมที่ใช้เว็บไซต์หลอกลวงแบบนี้เรียกว่า Phishing ซึ่งรายละเอียดผู้เขียนจะไม่ขอกล่าวซ้ำอีก เนื่องจากได้มีการอธิบายอยู่แล้ว ที่ http://www.thaicert.or.th/papers/normal/2012/pp2012no0007.html ซึ่งท่านผู้อ่านก็คงได้เห็นแล้วว่าเป็นภัยคุกคามที่สำคัญในโลกอินเตอร์เน็ต อย่างไรก็ตาม นอกจากธนาคารต่างๆ จะมีการประชาสัมพันธ์คำเตือนในเรื่องนี้ให้แก่ลูกค้า เพื่อเป็นการเพิ่มความตระหนักรู้ (Awareness) แล้ว ผู้สร้าง Web browser เอง ทั้ง Mozilla foundation, Microsoft, Google, Apple หรือ Opera software ต่างก็ไม่ได้นิ่งนอนใจเช่นกัน โดยได้เพิ่มความสามารถในการตรวจสอบและแจ้งเตือนผู้ใช้งาน หากมีการพยายามเข้าถึงเว็บไซต์หลอกลวงเหล่านี้มาตั้งแต่ปี 2006 โดยเริ่มจาก Firefox เวอร์ชัน 2, Internet Explorer เวอร์ชัน 7 และ Opera เวอร์ชัน 9.1 ตัวอย่างการแจ้งเตือนเป็นดังรูปที่ 53 (14-1)

รูปที่ 53 (14-1) ตัวอย่างการแจ้งเตือนเมื่อผู้ใช้งานพยายามเข้าถึงเว็บไซต์หลอกลวง ของ Firefox เวอร์ชัน 13

กลไกการป้องกันของบราวเซอร์เหล่านี้ดูจะเป็นปัจจัยสำคัญที่ช่วยป้องกันไม่ ให้ผู้ใช้งานตกเป็นเหยื่อของ Phishing อย่างได้ผล นอกจากเว็บไซต์หลอกลวงแล้ว กลไกเหล่านี้ยังสามารถป้องกันผู้ใช้จากเว็บไซต์ที่มี Malware อยู่ได้อีกด้วย แต่เพราะเหตุใดจึงยังมีข่าวว่ามีผู้ตกเป็นเหยื่อของการหลอกลวงแบบนี้ได้อยู่เสมอ ถ้าจะหาคำตอบในเรื่องนี้ เราต้องมาทำความเข้าใจกับการทำงานของกลไกเหล่านี้ก่อน

การที่ Web browser จะรู้ได้ว่าเว็บไซต์ใดเป็นเว็บไซต์หลอกลวงหรือไม่นั้น Web browser ไม่ได้ใช้กลไกการตรวจสอบทำซับซ้อนอะไรเลย ความจริงแล้ว Web browser ใช้วิธีเปรียบเทียบ URL ที่ผู้ใช้กำลังจะเข้าถึงกับรายการของเว็บไซต์หลอกลวงที่มีการรวบรวมไว้ล่วงหน้า แหล่งข้อมูลของรายการเว็บไซต์หลอกลวงเหล่านี้ได้แก่ Google, Phishtank และ Netcraft เป็นต้น ซึ่งแต่ละแหล่งข้อมูลก็อาจมีแหล่งที่มาและกระบวนการทำงานภายในแตกต่างกัน

ดังนั้น ในบางกรณี เว็บไซต์หลอกลวงแห่งหนึ่งอาจจะไม่ถูกตรวจพบใน Web browser ตัวหนึ่งว่าเป็น Phishing site ขณะที่ Web browser อีกตัวหนึ่งอาจจะตรวจพบได้แล้วเตือนผู้ใช้ได้อย่างถูกต้อง ทั้งนี้ก็ขึ้นอยู่กับแหล่งข้อมูลที่ Web browser ตัวนั้นเลือกใช้นั่นเอง ว่ามีการปรับปรุงข้อมูลรวดเร็วเพียงใด นอกจากนี้เนื่องจากเว็บไซต์หลอกลวงเหล่านี้เกิดขึ้นใหม่ทุกวัน หรือถ้าจะกล่าวให้ถูกต้องคือเกิดขึ้นได้วันละหลายๆ เว็บไซต์ทำให้เป็นเรื่องที่เข้าใจได้ว่าเว็บไซต์หลอกลวงจำนวนหนึ่งจะยังไม่ปรากฏอยู่ ในแหล่งข้อมูลใดๆ เป็นระยะเวลาหนึ่ง ซึ่งในช่วงเวลานี้เอง ผู้ใช้งานเว็บจำนวนไม่น้อยก็อาจตกเป็นเหยื่อของการหลอกลวงไปเรียบร้อยแล้ว

สำหรับผู้ใช้งานที่มีการอัพเดทเวอร์ชันของ Web browser อยู่เสมอก็คงวางใจได้ว่า จะได้รับการแจ้งเตือน Phishing site และเว็บไซต์อันตรายต่างๆ จาก Web browser ที่ใช้งานอยู่อย่างแน่นอน และนอกจากนั้น Web browser เวอร์ชันใหม่ๆ มักจะปิดช่องโหว่ด้านความมั่นคงปลอดภัยอื่นๆ ที่อาจจะมีในเวอร์ชันเก่าๆ อีกด้วย อย่างไรก็ตาม สำหรับผู้ที่มีเหตุผลบางประการที่ไม่สามารถอัพเดทเวอร์ชันของ Web browser ได้อย่างน้อยเพื่อให้มั่นใจว่า Web browser ที่ใช้งานอยู่ สามารถแจ้งเตือนเว็บไซต์อันตรายได้ ควรเลือกให้แน่ใจว่า Web browser เป็นรุ่นที่ออกแจกจ่าย (Release) หลังจากปี 2006 เช่น

Firefox เวอร์ชัน 2 ขึ้นไป (ขณะที่เขียนบทความเป็นเวอร์ชัน 13)
Internet Explorer เวอร์ชัน 7 ขึ้นไป (ขณะที่เขียนบทความเป็นเวอร์ชัน 9)
Opera เวอร์ชัน 9.1 ขึ้นไป (ขณะที่เขียนบทความเป็นเวอร์ชัน 11.64)
Chrome จะมีความสามารถในการเตือนเว็บไซต์อันตรายมาตั้งแต่เวอร์ชันแรกแล้ว (ขณะที่เขียนบทความเป็นเวอร์ชัน 20.0.1132.43)

ไม่ว่าธนาคารหรือผู้สร้าง Web browser หรือแม้แต่ผู้รักษากฎหมายจะมีมาตรการใดในการป้องกันเว็บไซต์หลอกลวงก็ตาม ความสำคัญของเรื่องนี้ก็ยังคงตกแก่ผู้ใช้ที่จำเป็นจะต้องมีความระมัดระวังในการใช้บริการต่างๆ บนอินเตอร์เน็ต และในกรณีที่มีข้อสงสัยโดยเฉพาะกรณี Internet banking เช่นนี้ ควรติดต่อสอบถามกับธนาคารของท่านโดยตรงผ่านช่องทางที่น่าเชื่อถือก่อนทุกครั้ง

15 MAN-IN-THE-MIDDLE 102 - PART 1 : ARP SPOOF

ผู้เขียน: เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่: 27 ก.ค. 2555
ปรับปรุงล่าสุด: 27 ก.ค. 2555

ในบทความ Man-in-the-Middle 101 ผู้เขียนได้กล่าวถึงการโจมตีด้วยวิธี Man-in-the-Middle ซึ่งเป็นวิธีการโจมตีที่มีผู้ไม่หวังดีเข้ามาแทรกตรงกลางระหว่างคู่สนทนา ทำให้สามารถรับรู้ข้อมูลที่คู่สนทนากำลังคุยกันอยู่ได้ นอกจากนั้นยังได้กล่าวถึงเทคนิคการโจมตีในรูปแบบต่างๆ ที่นำหลักการ Man-in-the-Middle มาประยุกต์ใช้ เช่น Man-in-the-Browser หรือ Man-in-the-Mailbox เป็นต้น

สำหรับบทความ Man-in-the-Middle 102 นี้จะกล่าวถึงวิธีการโจมตีแบบหลักๆ ที่ผู้ไม่หวังดีนิยมใช้ พร้อมทั้งเสนอวิธีการตรวจสอบและป้องกันตัวจากการโจมตีด้วยวิธีดังกล่าว โดยจะแบ่งเนื้อหาออกเป็น 3 ตอนด้วยกัน คือ ARP Spoof, DNS Spoof และ SSL Spoof ตามลำดับ ซึ่งในบทความตอนที่ 1 นี้จะเป็นส่วนของการโจมตีด้วยวิธี ARP Spoof แต่ก่อนที่จะทำความรู้จักกับการโจมตีด้วยวิธีที่กล่าวไปแล้วนั้น จำเป็นต้องเข้าใจกลไกการทำงานของ Internet Protocol และ ARP Protocol เสียก่อน

Internet Protocol

การติดต่อสื่อสารในระบบเครือข่ายอินเทอร์เน็ต จะทำผ่าน Internet Protocol (IP) ซึ่งจะใช้ IP Address ในการอ้างถึงอุปกรณ์ที่เชื่อมต่ออยู่ โดยแต่ละอุปกรณ์จะมี IP Address ไม่ซ้ำกัน IP Address ที่ใช้งานอยู่ในปัจจุบันคือเวอร์ชัน 4 (IPv4) โดยจะประกอบด้วยตัวเลข 4 ชุด แบ่งตามเครื่องหมาย . เช่น 192.168.0.1 แต่เนื่องจากปัญหาของ IPv4 ที่จำนวน IP Address ที่รองรับได้ไม่เพียงพอกับความต้องการใช้งานที่มีเพิ่มมากขึ้นเรื่อยๆ จึงได้มีการพัฒนา IP เวอร์ชัน 6 (IPv6) ขึ้นมาเพื่อใช้งานแทน โดยประกอบด้วยตัวเลขและตัวอักษร 6 ชุดแบ่งตามเครื่องหมาย : เช่น 2ac1:db8:0:5678:0:123:4:1 [15-1] เนื่องจาก IP Address เป็นค่าที่ผู้ให้บริการแจกจ่ายให้กับผู้ใช้บริการเมื่อเชื่อมต่อเข้ากับระบบเครือข่าย ดังนั้นค่า IP Address ของแต่ละเครื่องจึงอาจไม่คงที่ เพราะสามารถถูกเปลี่ยนแปลงได้เมื่อมีการเชื่อมต่อใหม่

อุปกรณ์ที่สามารถเชื่อมต่อกับระบบเครือข่ายได้ จะถูกกำหนดค่า MAC (Media Access Control) มาตั้งแต่โรงงานที่ผลิต ซึ่งเป็นค่าประจำตัวที่ใช้ในการอ้างอิงถึงอุปกรณ์นั้นๆ ในทางทฤษฎีแล้ว แต่ละอุปกรณ์จะต้องมีค่า MAC ไม่ซ้ำกัน โดยค่า MAC Address จะประกอบด้วยตัวเลขหรือตัวอักษร 6 ชุด แบ่งตามเครื่องหมาย - หรือ : เช่น 01-23-45-67-89-ab หรือ 01:23:45:67:89:ab [15-2]

ความสัมพันธ์ระหว่าง IP Address และ MAC Address

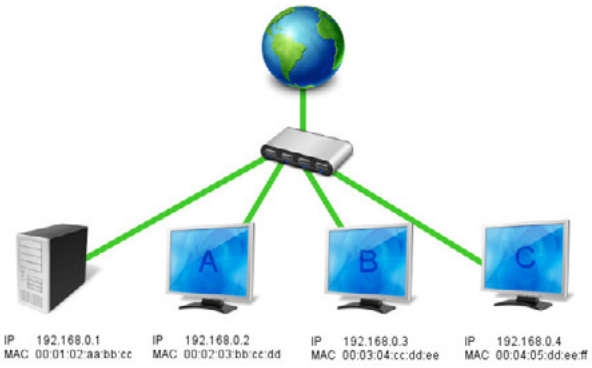
เนื่องจาก MAC Address เป็นค่าประจำตัวของอุปกรณ์นั้นๆ และยังสามารถใช้ระบุตัวอุปกรณ์โดยตรงได้ จึงเรียกได้อีกอย่างว่าเป็น Physical Address ในขณะที่ IP Address เป็นค่าที่กำหนดขึ้นมาเพื่อใช้อ้างอิงถึงอุปกรณ์นั้นๆ ในขณะที่เชื่อมต่ออุปกรณ์เข้ากับระบบเครือข่าย จึงเรียกได้อีกอย่างว่าเป็น Logical Address

การส่งข้อมูลใน OSI Layer 2 จะอ้างอิงถึงอุปกรณ์ที่เชื่อมต่ออยู่โดยใช้ MAC Address แต่การส่งข้อมูลใน OSI Layer 3 จะอ้างอิงถึง IP Address ดังนั้นเมื่อเครื่องที่อยู่ในระบบเครือข่าย ต้องการติดต่อกับเครื่องอื่นๆ ที่อยู่ในเครือข่ายเดียวกัน จึงจำเป็นต้องทราบข้อมูล IP Address และ MAC Address ของเครื่องที่จะติดต่อด้วย เพื่อให้สามารถสื่อสารกันได้

ARP คืออะไร

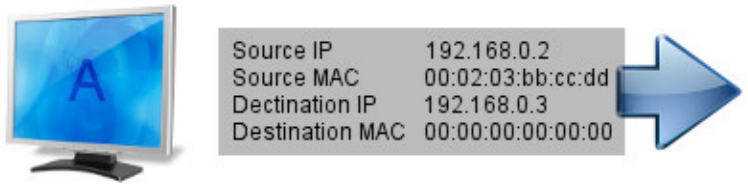
ARP ย่อมาจาก Address Resolution Protocol เป็นโพรโทคอลที่ใช้ในการค้นหา MAC Address ของอุปกรณ์จาก IP Address การทำงานของ ARP หากมีเครื่องในเครือข่ายต้องการติดต่อกับเครื่องอื่น โดยทราบแค่ IP Address แต่ไม่ทราบ MAC Address ของเครื่องปลายทาง เครื่องที่ต้องการติดต่อก็จะส่ง ARP Request แบบ Broadcast ออกไปในเครือข่าย เพื่อสอบถามว่าเครื่องที่มี IP ดังกล่าวมี MAC Address เป็นอะไร พอเครื่องที่มี IP ตรงกับที่ระบุได้รับ ARP Request ก็จะส่ง ARP Reply (หรือ ARP Response) ตอบ MAC Address ของตัวเองกลับไป [15-3]

สมมุติว่าระบบเครือข่ายมีการเชื่อมต่อดังรูปที่ 54 (15-1)



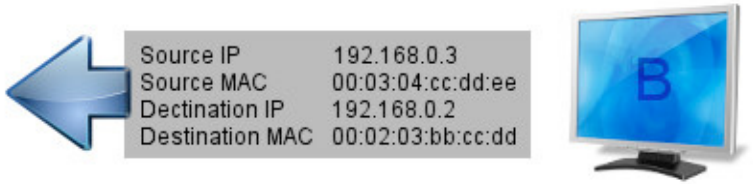
รูปที่ 54 (15-1) อุปกรณ์ในระบบเครือข่าย

เมื่อเครื่องคอมพิวเตอร์ A ที่มี IP 192.168.0.2 ต้องการติดต่อกับเครื่องคอมพิวเตอร์ที่มี IP 192.168.0.3 แต่ยังไม่ทราบ MAC Address ของเครื่องปลายทาง จึงส่ง Packet ออกไปในระบบเครือข่ายแบบ Broadcast (Destination MAC เป็น ff:ff:ff:ff:ff:ff) โดยภายใน Packet จะมี ARP Request ที่ระบุ Destination MAC เป็น 00:00:00:00:00:00 ดังรูปที่ 55 (15-2)



รูปที่ 55 (15-2) เครื่องคอมพิวเตอร์ A ส่ง ARP Request

เมื่อเครื่องคอมพิวเตอร์ B ได้รับ ARP Request และพบว่ามีการระบุ Destination IP เป็น IP Address ของตัวเอง จึงส่ง ARP Reply เพื่อบอก MAC Address ของตัวเองกลับไป ดังรูปที่ 56 (15-3)



รูปที่ 56 (15-3) เครื่องคอมพิวเตอร์ B ส่ง ARP Reply

เมื่อเครื่องคอมพิวเตอร์ A ได้รับ ARP Reply ก็จะทราบได้ว่าเครื่องคอมพิวเตอร์ที่มี IP 192.168.0.3 มี MAC Address เป็น 00:03:04:cc:dd:ee และจะเก็บข้อมูลที่หาได้ไว้ใน ARP Table หากต้องการติดต่อกับเครื่องที่มี IP 192.168.0.3 อีกในครั้งถัดไป ก็สามารถระบุข้อมูลในช่อง Destination MAC เป็น 00:03:04:cc:dd:ee ได้ทันที

ARP Table หรือ ARP Cache เป็นตารางที่ใช้บันทึกข้อมูลของเครื่องที่เคยติดต่อแล้ว ข้อมูลหลักๆ ที่จัดเก็บ คือ IP Address และ MAC Address [15-4] ตัวอย่าง ARP Table เป็นดังรูปที่ 57 (15-4) อย่างไรก็ตาม ข้อมูลใน ARP Table จะถูกลบทิ้งเมื่อปิดเครื่องหรือปิดการทำงานของ Interface Card

```
bigta@bigta-PORTEGE-R830:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.10.20.101             ether   84:00:d2:dd:de:4d   C                     wlan0
10.10.20.1               ether   08:00:27:4a:ee:36   C                     wlan0
```

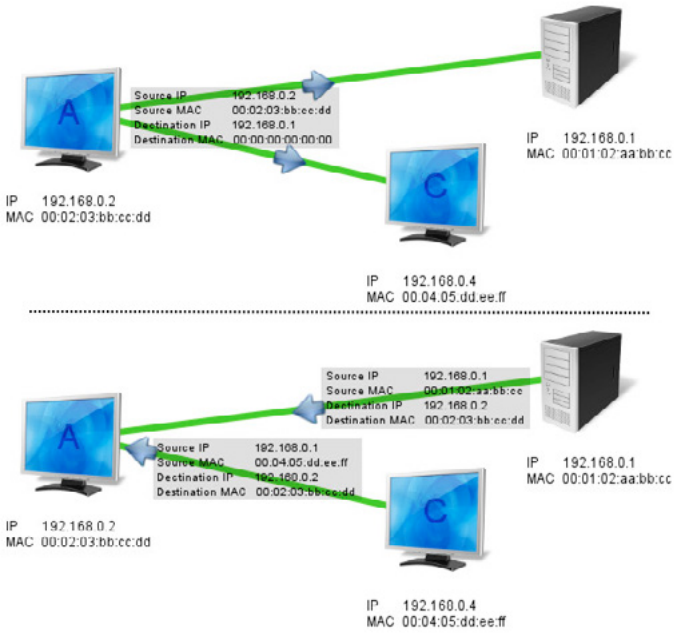
รูปที่ 57 (15-4) ตัวอย่าง ARP Table

หากเป็นการค้นหา IP Address จาก MAC Address จะทำโดยใช้โพรโทคอล RARP (Reverse ARP) ซึ่งมีการทำงานเหมือน ARP แต่ทำตรงข้ามกัน โดยจะระบุ Destination IP เป็น 0.0.0.0 และฝั่งรับก็จะส่ง RARP Reply ตอบ IP Address ของตัวเองกลับมา [15-5]

ARP Spoof

เนื่องจากการทำงานของ ARP จะมีการส่ง ARP Request ออกไป แล้วรอให้มี ARP Reply ตอบกลับมา ถ้าหากว่าระหว่างที่กำลังรอคำตอบอยู่นั้นมีผู้ไม่หวังดีตอบ ARP Reply ปลอมๆ ส่งไปให้ ผู้ที่ได้รับก็จะไม่สามารถทราบได้ว่า ARP Reply นั้นไม่ได้มาจากตัวจริง และจะบันทึกข้อมูล MAC Address ที่ไม่ถูกต้องนั้นไว้ใน ARP Table การส่ง ARP Reply ปลอมออกไปนั้นเรียกว่า ARP Spoof หรือ ARP Cache Poison [15-6] [15-7]

ตัวอย่าง การทำ ARP Spoof เครื่องคอมพิวเตอร์ A ส่ง ARP Request ออกไปถามว่าเครื่องที่มี IP Address 192.168.0.1 มี MAC Address เป็นเท่าไหร่ แต่ถูกเครื่องคอมพิวเตอร์ C แย่งส่ง ARP Reply ตอบ MAC Address ของตัวเองมาให้ก่อนที่เครื่องตัวจริงจะตอบ ARP Reply กลับมาได้ทัน ดังนั้นเมื่อเครื่องคอมพิวเตอร์ A ได้รับ ARP Reply ดังกล่าวก็จะเข้าใจว่าเครื่องคอมพิวเตอร์ C เป็นเครื่องที่ต้องการติดต่อด้วยจริง ดังรูปที่ 58 (15-5)



รูปที่ 58 (15-5) ตัวอย่าง ARP Table

ตัวอย่างโปรแกรมที่สามารถทำ APR Spoof ได้ เช่น ARPspoof, Cain & Abel, Ettercap, Dsniff เป็นต้น จุดประสงค์ของการทำ ARP Spoof มีได้หลากหลาย เช่น อาจจะทำ Man-in-the-Middle เพื่อดักรับข้อมูล หรือบล็อกไม่ให้เครื่องคอมพิวเตอร์ในระบบเครือข่ายเชื่อมต่อกับอินเทอร์เน็ต ได้ โดยการส่ง ARP Reply บอก Gateway ปลอมออกไป เป็นต้น ซึ่งวิธีการดังกล่าวนี้ถูกใช้ในโปรแกรมชื่อ NetCut [15-8]

การตรวจสอบและป้องกัน ARP Spoof

การทำ ARP Spoof จะทำได้ก็ต่อเมื่อเครื่องของผู้โจมตีและเครื่องของเหยื่ออยู่ในเครือข่ายเดียวกัน แต่การตรวจสอบ ARP Spoof ในระบบเครือข่ายนั้นทำได้ยาก เนื่องจากโพรโทคอล ARP ไม่ได้ถูกออกแบบมาเพื่อให้ตรวจสอบความถูกต้องของผู้รับและผู้ส่งตั้งแต่แรก อย่างไรก็ตาม ได้มีผู้พัฒนาเครื่องมือเพื่อช่วยวิเคราะห์ความผิดปกติในระบบเครือข่ายซึ่ง อาจเกิดจาก ARP Spoof ได้ เช่น โปรแกรม **arpwatch** หรือ **ArpON** เป็นต้น ซึ่งทั้ง 2 โปรแกรมนี้เป็นซอฟต์แวร์ Open Source

การป้องกันตัวเบื้องต้นจาก ARP Spoof สามารถทำได้โดยการทำ Static ARP ซึ่งเป็นการระบุค่า IP Address และ MAC Address ลงไปใน ARP Table ด้วยตนเอง [15-9] ซึ่งสามารถทำได้โดยใช้คำสั่ง

arp -s <IP ADDRESS> <MAC ADDRESS>

เช่น เครื่องคอมพิวเตอร์ A สามารถเพิ่มเครื่องคอมพิวเตอร์ B ลงใน ARP Table ด้วยการใช้คำสั่งด้านล่าง

arp -s 192.168.0.3 00:03:04:cc:dd:ee

อย่างไรก็ตาม การทำ Static ARP อาจไม่สะดวกในการใช้งานกับระบบเครือข่ายขนาดใหญ่ เพราะหากมีเครื่องคอมพิวเตอร์อยู่ในระบบจำนวนมากก็ต้องเพิ่ม Static ARP ให้กับเครื่องเหล่านั้นในทุกครั้งที่เปิดเครื่อง รวมถึงผู้ที่ใช้งานอินเทอร์เน็ตสาธารณะหรือผู้ที่เชื่อมต่อผ่านบริการอินเทอร์เน็ตของที่พัก (ที่ไม่ใช่ Broadband ส่วนตัว) ก็อาจไม่สามารถทราบข้อมูล IP Address หรือ MAC Address ของเครื่องที่สำคัญในระบบเครือข่าย เช่น Gateway หรือ DNS Server ได้

อ้างอิง

[15-1] http://mashable.com/2011/02/03/ipv4-ipv6-guide/

[15-2] http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm

[15-3] http://wiki.wireshark.org/AddressResolutionProtocol

[15-4] http://linux.about.com/od/lna_guide/a/gdelna50.htm

[15-5] http://wiki.wireshark.org/RARP

[15-6] http://resources.infosecinstitute.com/mitm-arp/

[15-7] http://www.windowsecurity.com/articles/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html

[15-8] http://www.arcai.com/arcai-netcut-faq.html

[15-9] http://www.dummies.com/how-to/content/cisco-networking-static-arp-entry-managment.html

16 การใช้ PGP เพื่อการสื่อสารอย่างมั่นคงปลอดภัยบนระบบปฏิบัติการ Mac OS X

ผู้เขียน: รงชัย ศิลปวรางกูร
วันที่เผยแพร่: 31 กรกฎาคม 2555
ปรับปรุงล่าสุด: 31 กรกฎาคม 2555

PGP (Pretty Good Privacy) เป็นโปรแกรมที่สร้างขึ้นเพื่อใช้ในการเข้ารหัสลับ (Encryption) ถอดรหัสลับ (Decryption) และลงลายมือชื่อ (Sign) ในการรับส่งข้อมูลประเภทต่าง ๆ โดยเฉพาะอีเมล ผู้อ่านสามารถศึกษาข้อมูลเพิ่มเติมเกี่ยวกับ PGP รวมถึงการใช้งาน PGP บนระบบปฏิบัติการ Windows ได้จาก http://www.thaicert.or.th/papers/normal/2011/email_security_with_pgp.pdf เนื่องจากในที่นี้จะกล่าวถึงแต่เพียงการติดตั้งและการใช้งาน PGP บนระบบปฏิบัติการ Mac OS X สำหรับผู้ใช้ทั่วไปเท่านั้น

การติดตั้ง GPGTools

เกี่ยวกับ GPGTools

GPGTools เป็นชุดโปรแกรมที่ประกอบด้วยโปรแกรมต่าง ๆ ดังนี้

MacGPG: โปรแกรมหลักของชุดโปรแกรม GPGTools ซึ่งพอร์ตมาจากโปรแกรม GnuPG เพื่อให้สามารถติดตั้งและใช้งานบนระบบปฏิบัติการ Mac OS X ได้อย่างสะดวก

GPG Keychain Access: โปรแกรมจัดการกุญแจ

GPGMail: ส่วนเสริมของโปรแกรม Mail.app สำหรับเข้า-ถอดรหัสลับและลงลายมือชื่อบนอีเมล

Enigmail: ส่วนเสริมของโปรแกรม Thunderbird สำหรับเข้า-ถอดรหัสลับและลงลายมือชื่อบนอีเมล

GPGServices: ส่วนเสริมของเซอร์วิสเมนูในระบบปฏิบัติการ Mac OS X สำหรับเข้า-ถอดรหัสลับ ลงลายมือชื่อ และตรวจสอบลายมือชื่อของไฟล์หรือโฟลเดอร์

GPGPreferences: ส่วนการตั้งค่าเบื้องต้นของชุดโปรแกรม GPGTools ใน System Preferences

หมายเหตุ

โปรแกรม MacGPG, GPG Keychain Access และ GPGMail รองรับระบบปฏิบัติการเวอร์ชัน 10.5 (Leopard) เป็นต้นไป

โปรแกรม GPGServices และ GPGPreferences รองรับระบบปฏิบัติการเวอร์ชัน 10.6 (Snow Leopard) เป็นต้นไป

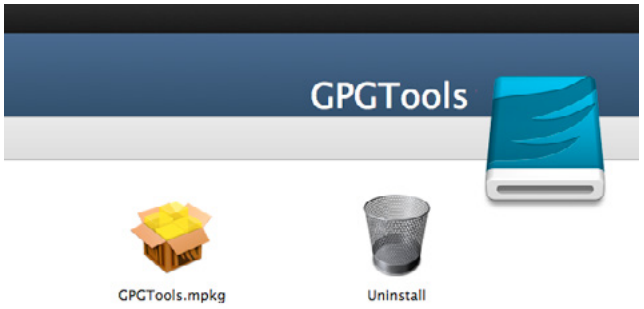
โปรแกรม Enigmail รองรับโปรแกรม Thunderbird เวอร์ชัน 3 ขึ้นไป

ตัวอย่างการติดตั้ง GPGTools บนระบบปฏิบัติการ Mac OS X 10.7 (Lion)

1. ดาวน์โหลดตัวติดตั้งชุดโปรแกรม GPGTools จาก https://www.gpgtools.org/installer

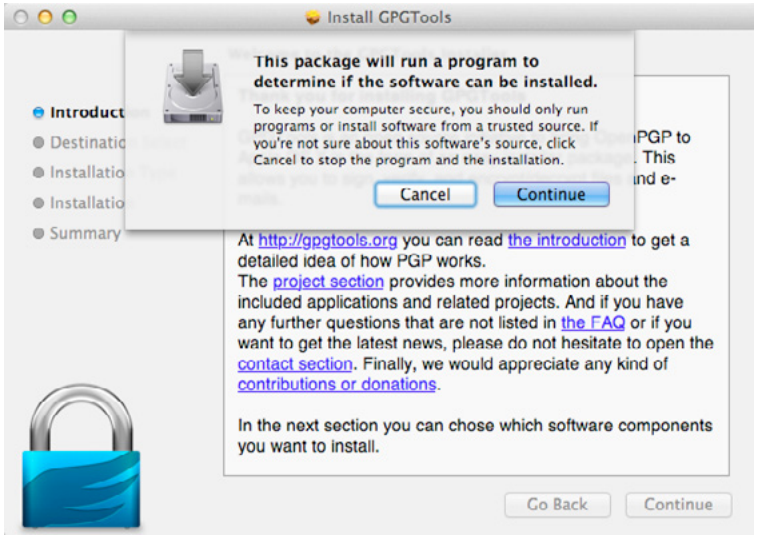
หมายเหตุ: เนื่องจากโปรแกรมบางตัวในชุดโปรแกรม GPGTools เวอร์ชันปัจจุบัน (2012.03.18) ยังอยู่ในสถานะ Alpha หรือ Beta ซึ่งอาจพบปัญหาบางอย่างระหว่างการใช้งาน เช่น การค้นหากุญแจสาธารณะจากเซิร์ฟเวอร์ ดังนั้นผู้อ่านสามารถดาวน์โหลด Nightly Builds ซึ่งคอมไพล์จาก source code เวอร์ชันล่าสุดที่ยังไม่ได้ทดสอบการใช้งานมาติดตั้งทดลองใช้แทนได้จาก http://nightly.gpgtools.org

2. ดับเบิลคลิกที่ไอคอนของตัวติดตั้ง จะพบกับหน้าต่างที่ดังรูปที่ 59 (16-1) ให้ดับเบิลคลิกที่ GPGTools.mpkg



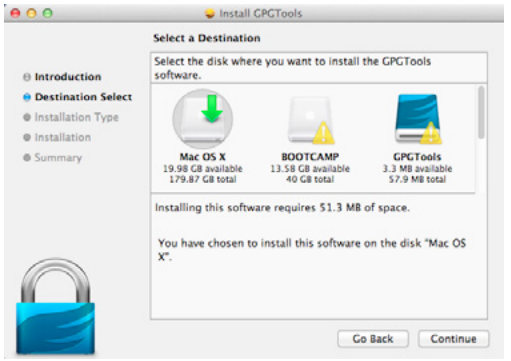
รูปที่ 59 (16-1) หน้าต่างหลักของตัวติดตั้งชุดโปรแกรม GPGTools

3. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 60 (16-2) ให้คลิกปุ่ม Continue หลังจากนั้นตัวติดตั้งอาจแจ้งเตือนผู้ใช้ในกรณีที่มีการเปิดโปรแกรมอื่น ๆ ที่เกี่ยวข้องกับการติดตั้ง GPGTools เช่น Mail.app ให้ปิดโปรแกรมดังกล่าวก่อนแล้วคลิกปุ่ม Continue



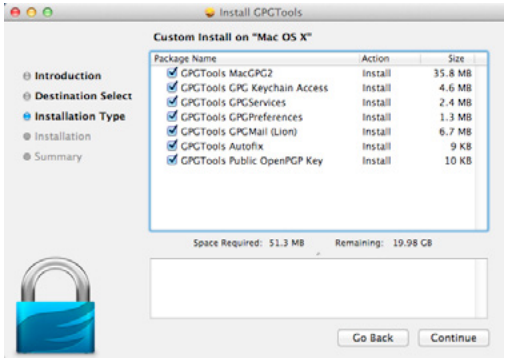
รูปที่ 60 (16-2) หน้าต่างเริ่มต้นติดตั้งโปรแกรม

4. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 61 (16-3) ให้เลือกดิสก์ที่ปกติใช้งานเป็นหลักในการติดตั้งโปรแกรม โดยทั่วไปคือดิสก์ที่ติดตั้งระบบปฏิบัติการ Mac OS X มักอยู่ในตำแหน่งแรกของลิสต์ที่ให้เลือก และมีลูกศรสีเขียวซึ่งหมายถึงสามารถติดตั้งโปรแกรมลงในดิสก์นั้นได้ จากนั้นคลิกปุ่ม Continue



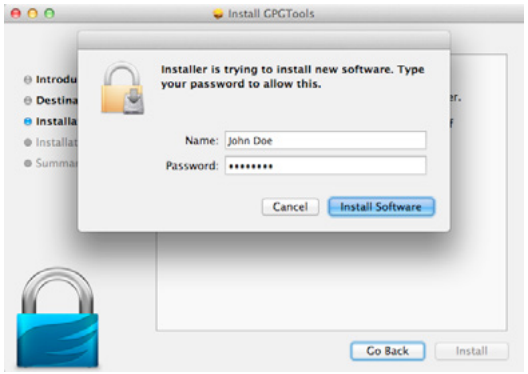
รูปที่ 61 (16-3) หน้าต่างเลือกดิสก์ปลายทางที่จะติดตั้งโปรแกรม

5. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 62 (16-4) ให้เลือกโปรแกรมที่ต้องการติดตั้ง ในที่นี้จะเลือกติดตั้งทุกโปรแกรม จากนั้นคลิกปุ่ม Continue



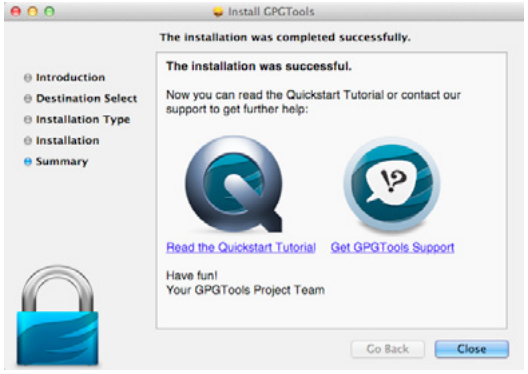
รูปที่ 62 (16-4) หน้าต่างเลือกโปรแกรมที่ต้องการจะติดตั้ง

6. หน้าต่างใหม่จะปรากฏขึ้นเพื่อให้ยืนยันการติดตั้ง ให้คลิกปุ่ม Install จากนั้นจะมีหน้าต่าง pop-up ขึ้นมาดังรูปที่ 63 (16-5) ให้พิมพ์รหัสของบัญชีผู้ใช้ระบบแล้วคลิกปุ่ม Install Software



รูปที่ 63 (16-5) หน้าต่างยืนยันการติดตั้งโปรแกรม

7. รอสักครู่จนกระทั่งระบบติดตั้งโปรแกรมเสร็จจะพบกับหน้าต่างดังรูปที่ 64 (16-6) ให้คลิกปุ่ม Close หรือสามารถดูตัวอย่างการใช้งานเบื้องต้นจากเว็บไซต์ของผู้พัฒนาโปรแกรมโดยคลิกที่ Read the Quickstart Tutorial หน้าต่างใหม่จะเปิดขึ้นในเว็บเบราว์เซอร์

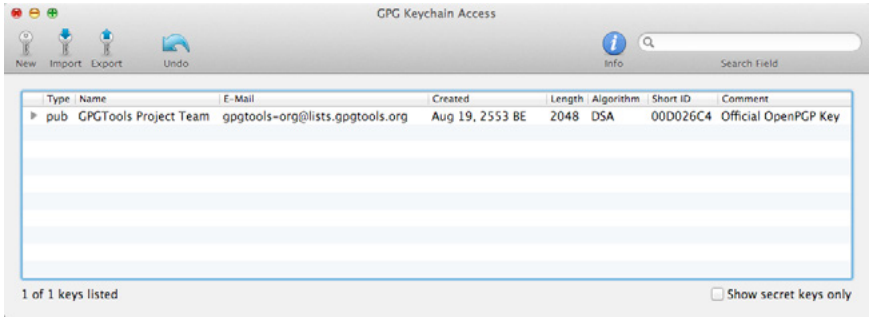


รูปที่ 64 (16-6) หน้าต่างเสร็จสิ้นการติดตั้งโปรแกรม

การใช้งาน GPGTools

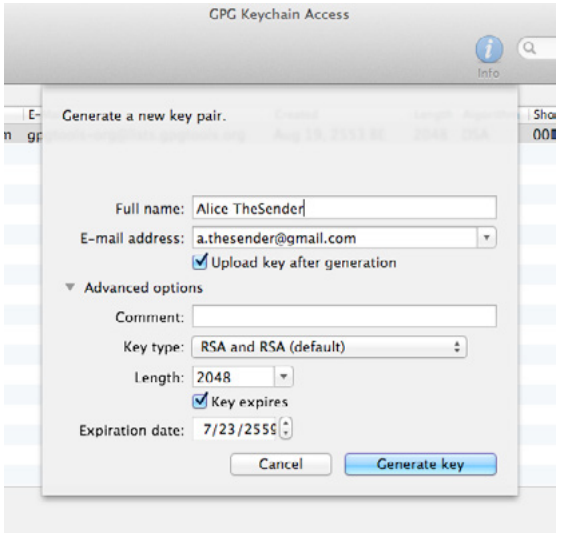
การสร้างคู่กุญแจ

1. เปิดโปรแกรม GPG Keychain Access (ปกติจะถูกติดตั้งอยู่ใน /Applications) จะพบกับหน้าต่างหลักของโปรแกรมดังรูปที่ 65 (16-7) จะเห็นว่าในรายการของกุญแจจะมีกุญแจสาธารณะของผู้พัฒนาชุดโปรแกรม GPGTools เป็นค่าเริ่มต้น เมื่อติดตั้งโปรแกรมใหม่ ให้คลิกที่ไอคอน New



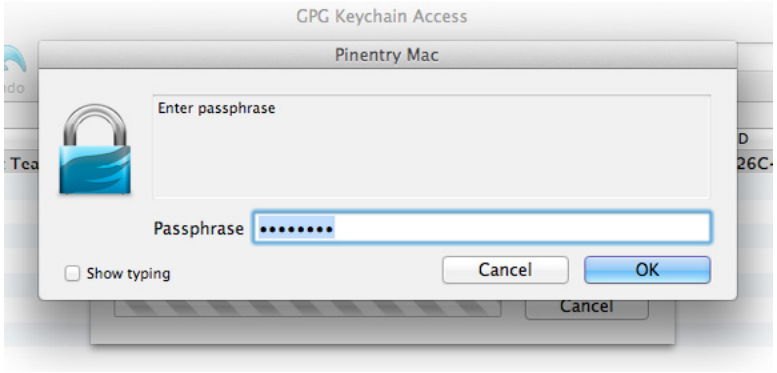
รูปที่ 65 (16-7) หน้าต่างหลักของโปรแกรม GPG Keychain Access

2. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 66 (16-8) ให้ระบุชื่อและอีเมล โดยในส่วนของ Advanced options สามารถระบุ comment, อัลกอริทึมที่ใช้ในการเข้า-ถอดรหัสและลงลายมือชื่อ, ความยาวของกุญแจ และวันที่คู่กุญแจหมดอายุการใช้งาน จากนั้นคลิกปุ่ม Generate key



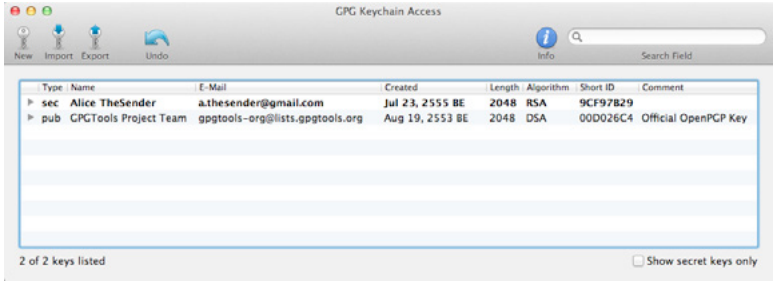
รูปที่ 66 (16-8) หน้าต่างระบุค่าเริ่มต้นเพื่อสร้างคู่กุญแจใหม่

3. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 67 (16-9) ให้ระบุ passphrase หรือรหัสส่วนตัวสำหรับใช้งานคู่กุญแจ ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร มีตัวเลขและอักขระพิเศษผสมอยู่ เมื่อระบุค่าเสร็จแล้วให้คลิกปุ่ม OK จากนั้นโปรแกรมจะให้ระบุ passphrase ซ้ำอีกครั้ง ให้ทำเช่นเดิม



รูปที่ 67 (16-9) หน้าต่างระบุ passphrase ของคู่กุญแจ

โปรแกรมจะใช้เวลาในการสร้างคู่กุญแจสักครู่ ระหว่างนี้โปรแกรมจะแนะนำให้ผู้ใช้พิมพ์ตัวอักษร เลื่อนเมาส์ หรือใช้งานดิสก์เพื่อทำให้สามารถสร้างคู่กุญแจได้ดีขึ้น เมื่อสร้างคู่กุญแจเสร็จแล้วจะพบว่ามีกุญแจใหม่ในรายการ โดยกุญแจที่ผู้ใช้สร้างเองจะเป็นตัวพิมพ์หนาดังรูปที่ 68 (16-10)



รูปที่ 68 (16-10) หน้าต่างหลักแสดงคู่กุญแจใหม่ที่ถูกสร้างขึ้น

คอลัมน์ในรายการของกุญแจมีดังนี้

Type: ชนิดของกุญแจ โดย pub คือกุญแจสาธารณะ (public key), sec คือกุญแจส่วนตัว (secret key), sub คือกุญแจย่อย (subkey) และ uid คือ user ID เป็นชื่อของบุคคลหรือองค์กรที่ใช้งานกุญแจนั้น ๆ โดยอาจมีหลายชื่อในกุญแจดอกเดียวกัน

Name: ชื่อเจ้าของกุญแจ

E-mail: อีเมลของเจ้าของกุญแจ

Created: วันที่สร้างกุญแจ

Length: ความยาวของกุญแจ

Algorithm: อัลกอริทึมที่ใช้เข้า-ถอดรหัสหรือลงลายมือชื่อของกุญแจ

Short ID: หมายเลขประจำกุญแจสำหรับใช้อ้างอิง

Comment: รายละเอียดเกี่ยวกับกุญแจ

การแลกเปลี่ยนกุญแจสาธารณะ

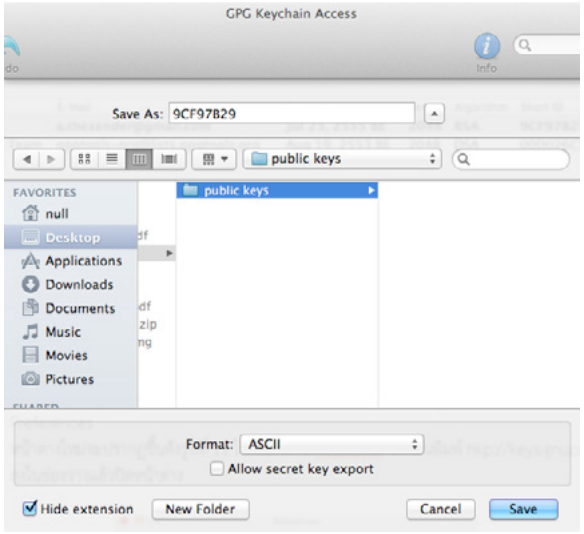
กุญแจสาธารณะนั้นถูกนำไปใช้งานอยู่สองกรณีด้วยกัน นั่นคือ กรณีที่ผู้ที่มาติดต่อนำกุญแจสาธารณะของเราไปใช้ในการเข้ารหัสอีเมลก่อนที่จะส่งมาให้ ซึ่งเราสามารถเปิดอ่านอีเมลที่ได้รับโดยใช้กุญแจส่วนตัวของเราเอง และอีกกรณีคือใช้ในการตรวจสอบว่าอีเมลที่ได้รับนั้นมาจากผู้ส่งจริง โดยการตรวจสอบจากลายเซ็นดิจิทัล (digital signature) ที่ผู้ส่งเซ็นมาในอีเมล

การส่งกุญแจสาธารณะ

การส่งกุญแจสาธารณะให้กับผู้รับสามารถทำได้หลายวิธี เช่น

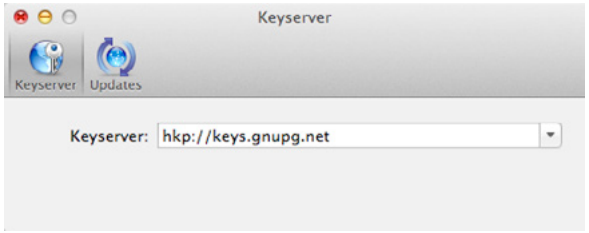
ส่งเป็นส่วนหนึ่งของข้อความที่จะส่งให้ผู้อื่น โดยการคัดลอกกุญแจสาธารณะที่อยู่ในรูปของ ASCII Armor (รูปแบบข้อความพิเศษที่ PGP แปลงจากข้อมูล binary ตามที่ระบุไว้ในมาตรฐาน RFC 2440) เริ่มจาก -----BEGIN PGP PUBLIC KEY BLOCK----- จนถึง -----END PGP PUBLIC KEY BLOCK----- แล้วใส่ต่อท้ายข้อความที่จะส่งให้ผู้อื่น

ส่งเป็นไฟล์ เริ่มจากหน้าต่างหลักของโปรแกรม GPG Keychain Access เลือกกุญแจที่ต้องการส่ง แล้วคลิกที่ไอคอน Export จากนั้นเลือกสถานที่ปลายทางที่ต้องการเซฟไฟล์ เลือก Format เป็น ASCII ไม่ต้องเช็คเครื่องหมายถูกที่ Allow secret key export แล้วคลิกปุ่ม Save ดังรูปที่ 69 (16-11) จะได้ไฟล์นามสกุล .asc ให้ส่งไฟล์ดังกล่าวไปให้ผู้อื่น เช่น แนบไปพร้อมกับอีเมล



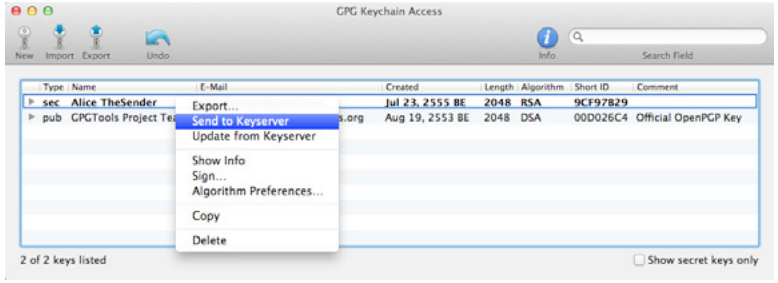
รูปที่ 69 (16-11) หน้าต่างเลือกสถานที่ปลายทางที่จะเซฟกุญแจสาธารณะ

ส่งผ่านเซิร์ฟเวอร์บริการกุญแจสาธารณะ (keyserver) เริ่มจากไปที่เมนู GPG Keychain Access -> Preferences หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 70 (16-12) ให้เลือกแท็บ Keyserver จากนั้นพิมพ์ hkp://keys.gnupg.net ลงในช่องว่างแล้วปิดหน้าต่าง



รูปที่ 70 (16-12) หน้าต่างระบุ URL ของ keyserver

จากนั้นในหน้าต่างหลัก คลิกขวาที่กุญแจที่ต้องการจะอัพโหลดแล้วเลือก Send to Keyserver ดังรูปที่ 71 (16-13)

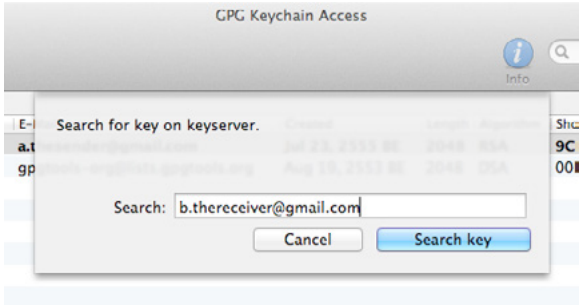


รูปที่ 71 (16-13) การอัพโหลดกุญแจที่ต้องการส่งไปยังเซิร์ฟเวอร์

การค้นหาและนำเข้ากุญแจสาธารณะจากเซิร์ฟเวอร์บริการกุญแจสาธารณะ

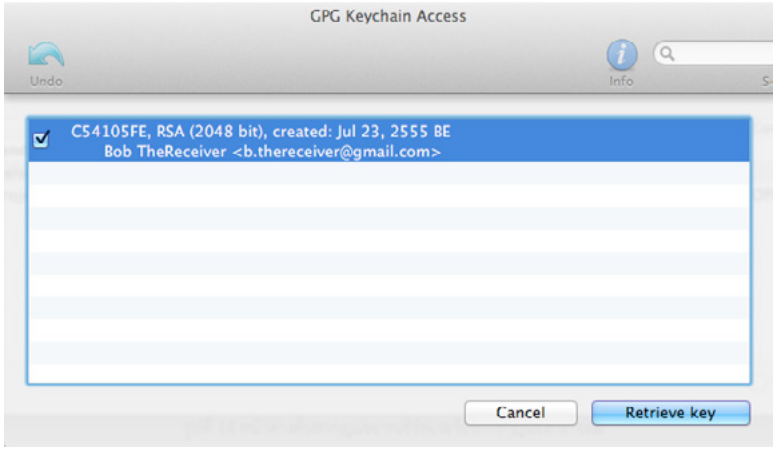
1. เปิดโปรแกรม GPG Keychain Access แล้วไปที่เมนู Key -> Search for Key หรือกดปุ่ม Command + F บนคีย์บอร์ด

2. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 72 (16-14) เราสามารถค้นหากุญแจโดยระบุชื่อเจ้าของกุญแจหรืออีเมลเจ้าของกุญแจ เมื่อระบุค่าเสร็จแล้วให้คลิกปุ่ม Search key



รูปที่ 72 (16-14) หน้าต่างค้นหากุญแจจากเซิร์ฟเวอร์บริการกุญแจสาธารณะ

3. หากค้นหากุญแจพบจะได้ผลลัพธ์คล้ายกับรูปที่ 73 (16-15) ให้เช็คเครื่องหมายถูกหน้ากุญแจที่ต้องการนำเข้าสู่โปรแกรมแล้วคลิกปุ่ม Retrieve key



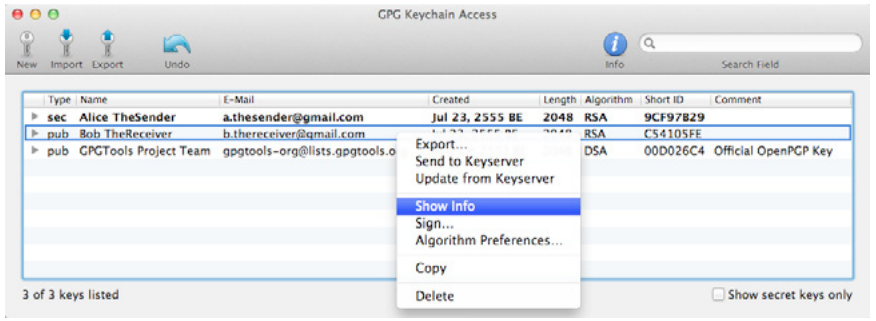
รูปที่ 73 (16-15) หน้าต่างแสดงรายชื่อกุญแจที่ค้นพบบนเซิร์ฟเวอร์

การนำเข้ากุญแจสาธารณะยังสามารถทำได้โดยการไปที่หน้าต่างหลักของโปรแกรม GPG Keychain Access คลิกที่ไอคอน Import แล้วเลือกไฟล์กุญแจที่ต้องการนำเข้าจากโฟลเดอร์ที่เก็บไฟล์ไว้ หรือคลิกขวาที่ไฟล์กุญแจที่ต้องการนำเข้าแล้วเลือกเมนู Services -> OpenPGP: Import Key from File (กรุณาศึกษาวิธีการใช้งาน GPGServices เพิ่มเติมจากหัวข้อ “การเข้ารหัส ถอดรหัส ลงลายมือชื่อ และตรวจสอบลายมือชื่อของไฟล์หรือโฟลเดอร์”)

การตรวจสอบและกำหนดระดับความน่าเชื่อถือของกุญแจสาธารณะของผู้อื่น

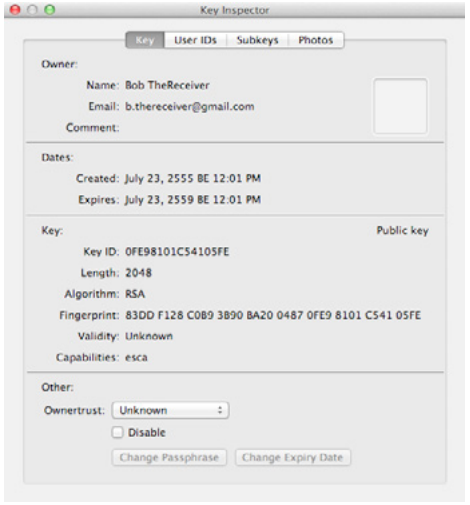
เราควรตรวจสอบกุญแจสาธารณะของผู้อื่นที่นำเข้ามาว่าถูกต้องและเป็นของจริงหรือไม่ เพื่อที่จะลงลายมือชื่อและกำหนดระดับความน่าเชื่อถือของกุญแจนั้น ๆ ก่อนที่จะนำไปใช้งาน เริ่มจากการเปรียบเทียบค่า fingerprint ของตัวกุญแจกับค่าที่เจ้าของกุญแจได้แจ้งไว้ดังนี้

1. จากหน้าต่างหลักของโปรแกรม GPG Keychain Access คลิกขวาที่กุญแจสาธารณะของผู้อื่นที่จะตรวจสอบ แล้วเลือก Show info ดังรูปที่ 74 (16-16)



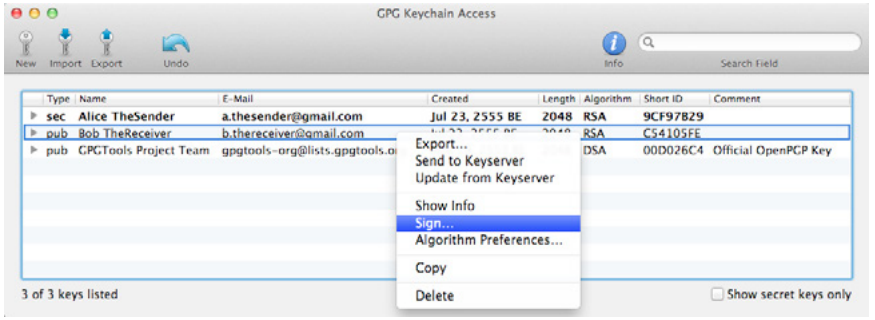
รูปที่ 74 (16-16) การเลือกดูรายละเอียดของกุญแจ

2. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 75 (16-17) เลือกแท็บ Key แล้วเปรียบเทียบค่า fingerprint ที่พบในหมวด Key กับค่าที่เจ้าของกุญแจได้แจ้งไว้ หากมีค่าตรงกันให้ทำขั้นตอนต่อไป



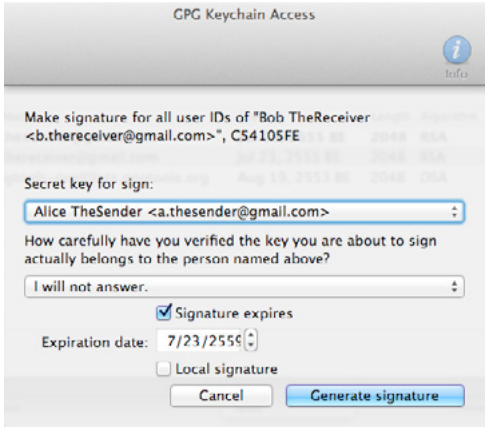
รูปที่ 75 (16-17) หน้าต่างแสดงรายละเอียดของกุญแจ

3. ลงลายมือชื่อกุญแจ โดยการไปที่หน้าต่างหลักของโปรแกรม GPG Keychain Access คลิกขวาที่กุญแจที่ผ่านการตรวจสอบ fingerprint แล้วเลือก Sign ดังรูปที่ 76 (16-18)



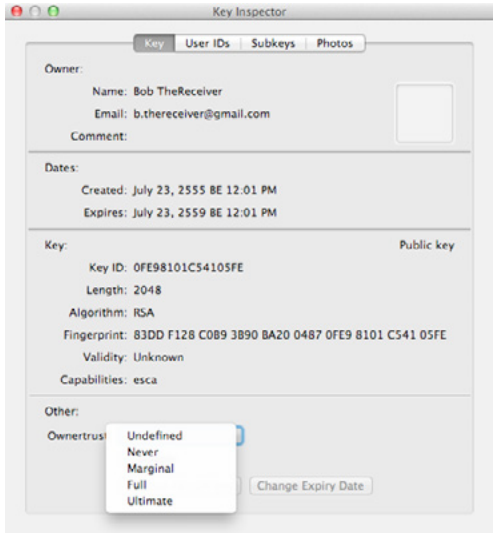
รูปที่ 76 (16-18) การเลือกกุญแจที่จะลงลายมือชื่อ

4. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 77 (16-19) ให้เลือกกุญแจส่วนตัวของเราที่จะใช้ลงลายมือชื่อ และเลือกว่าได้ตรวจสอบกุญแจที่จะถูกลงลายมือชื่อในระดับใด จากนั้นคลิกปุ่ม Generate signature



รูปที่ 77 (16-19) หน้าต่างการลงลายมือชื่อกุญแจสาธารณะ

5. เมื่อลงลายมือชื่อแล้วให้กำหนดระดับความน่าเชื่อถือของกุญแจดังกล่าว โดยการดูรายละเอียดของกุญแจ (คลิกขวาที่กุญแจแล้วเลือก Show info) จากนั้นเลือกแท็บ Key แล้วดูในหมวด Other จะพบกับส่วนของ Ownertrust ที่สามารถกำหนดระดับความน่าเชื่อถือดังรูปที่ 78 (16-20) เมื่อกำหนดเสร็จแล้วให้ปิดหน้าต่าง



รูปที่ 78 (16-20) หน้าต่างแสดงเมนูกำหนดระดับความน่าเชื่อถือของกุญแจ

ระดับความน่าเชื่อถือที่สามารถกำหนดได้มีดังนี้

Undefined: ไม่กำหนดระดับความน่าเชื่อถือ

Never: ไม่เชื่อถือ

Marginal: เชื่อถือเล็กน้อย โดยกุญแจดังกล่าวจะมีความน่าเชื่อถือเมื่อมีผู้อื่นกำหนดความน่าเชื่อถือในระดับ Marginal เช่นเดียวกันจำนวน 3 คน

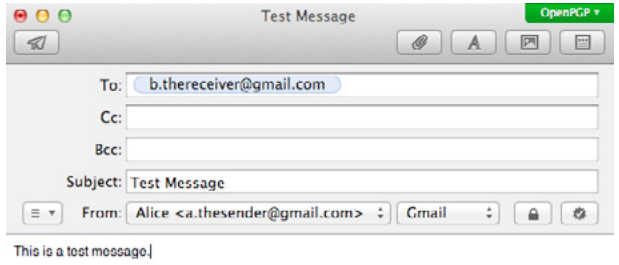
Full: เชื่อถือ

Ultimate: เชื่อถืออย่างยิ่ง ควรกำหนดระดับความน่าเชื่อถือนี้กับกุญแจของตัวเองเท่านั้น

การเข้ารหัส ถอดรหัส และลงลายมือชื่อของอีเมล

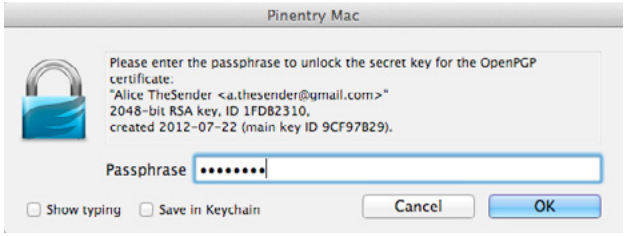
ในชุดโปรแกรม GPGTools มีโปรแกรม GPGMail ทำให้สามารถใช้งาน PGP บนโปรแกรม Mail.app ที่มาพร้อมกับระบบปฏิบัติการได้อย่างสะดวก ตัวอย่างต่อไปนี้จะแสดงการเข้ารหัสและการลงลายมือชื่อของอีเมลก่อนที่จะส่งไปยังผู้รับ รวมถึงการถอดรหัสเมื่อผู้รับได้รับอีเมล

1. หลังจากนำเข้ากุญแจสาธารณะของผู้รับอีเมลแล้ว ขณะกำลังส่งอีเมลไปยังผู้รับด้วยโปรแกรม Mail.app ให้คลิกปุ่มรูปแม่กุญแจเพื่อเข้ารหัส และคลิกปุ่มที่อยู่ด้านข้างปุ่มรูปแม่กุญแจให้เป็นรูปเครื่องหมายถูกเพื่อลงลายมือชื่อ เมื่อคลิกแล้วแถบข้อความ OpenPGP ที่อยู่มุมขวาบนจะกลายเป็นสีเขียวดังรูปที่ 79 (16-21)



รูปที่ 79 (16-21) การเปิดใช้งานการเข้ารหัสและลงลายมือชื่อของอีเมล

2. เมื่อคลิกปุ่มส่งอีเมลแล้วจะพบกับหน้าต่างดังรูปที่ 80 (16-22) ให้ระบุ passphrase ของกุญแจของผู้ส่งอีเมล จากนั้นคลิกปุ่ม OK

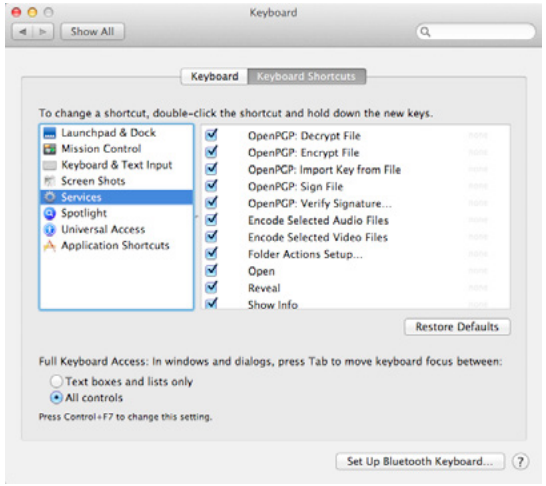


รูปที่ 80 (16-22) หน้าต่างระบุ passphrase ของกุญแจของผู้ส่งอีเมล

3. เมื่อผู้รับที่ใช้โปรแกรม Mail.app เปิดอ่านอีเมลที่ได้รับ จะพบกับหน้าต่างเช่นเดียวกับข้อ 2 ให้ระบุ passphrase ของกุญแจของผู้รับอีเมลแล้วคลิกปุ่ม OK

การเข้ารหัส ถอดรหัส ลงลายมือชื่อ และตรวจสอบลายมือชื่อของไฟล์หรือโฟลเดอร์

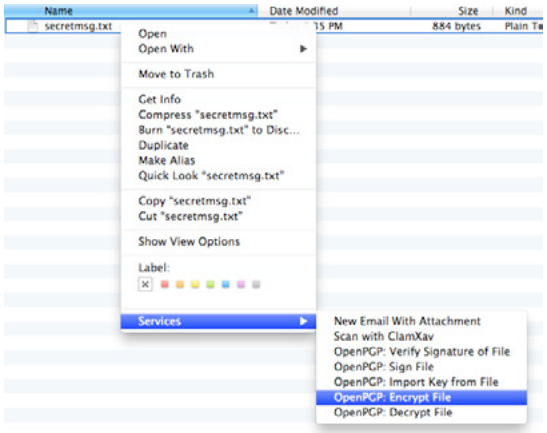
นอกจากการเข้า-ถอดรหัสและลงลายมือชื่อของอีเมลแล้ว โปรแกรม GPGServices ที่มาพร้อมกับชุดโปรแกรม GPGTools ยังช่วยให้เราสามารถกระทำการดังกล่าวกับไฟล์หรือโฟลเดอร์ได้เช่นเดียวกัน ในการใช้งานส่วนนี้แนะนำให้ดาวน์โหลดโปรแกรม Growl จาก http://growl.info/downloads (ราคา $1.99 สำหรับระบบปฏิบัติการเวอร์ชัน 10.7 (Lion) หรือดาวน์โหลดฟรีสำหรับเวอร์ชันที่เก่ากว่า) หรือดาวน์โหลดโปรแกรมฟรีชื่อ Growl Fork จาก https://bitbucket.org/pmetzger/growl/downloads สำหรับระบบปฏิบัติการเวอร์ชัน 10.7 (Lion) ขึ้นไป ซึ่งเป็นโปรแกรมแจ้งสถานะการทำงานของโปรแกรมอื่น ๆ มาติดตั้งก่อน จากนั้นให้ตรวจสอบว่าระบบได้เปิดการทำงาน GPGServices หรือไม่ โดยไปที่ System Preferences -> Keyboard แล้วเลือกแท็บ Keyboard Shortcuts จากนั้นเลือก Services จากช่องด้านซ้าย แล้วดูว่ารายการในช่องด้านขวาที่ขึ้นต้นด้วย OpenPGP มีการเช็คเครื่องหมายถูกหรือไม่ดังรูปที่ 81 (16-23)



รูปที่ 81 (16-23) ตรวจสอบการเปิดใช้งานของ GPGServices

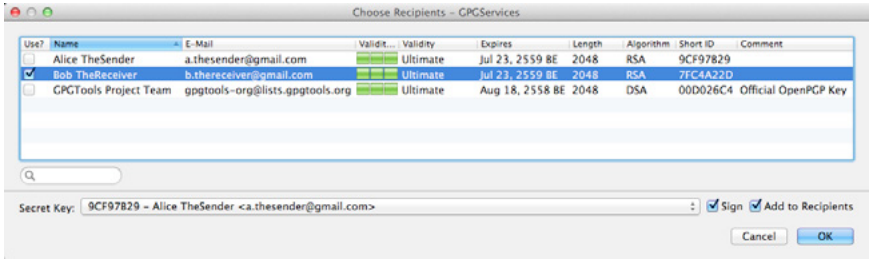
การเข้ารหัสไฟล์หรือโฟลเดอร์

1. คลิกขวาที่ไฟล์หรือโฟลเดอร์ที่ต้องการเข้ารหัส แล้วเลือกเมนู Services -> OpenPGP: Encrypt File ดังรูปที่ 82 (16-24)



รูปที่ 82 (16-24) การเลือกเมนูเพื่อเข้ารหัสไฟล์หรือโฟลเดอร์

2. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 83 (16-25) ให้เช็คเครื่องหมายถูกหน้ากุญแจของผู้รับ นอกจากนี้ยังสามารถเลือกกุญแจส่วนตัวของผู้ส่งและเช็คเครื่องหมายถูกที่ Sign เพื่อลงลายมือชื่อยืนยันว่าไฟล์หรือโฟลเดอร์ดังกล่าวถูกส่งมาจากผู้ส่งจริง จากนั้นคลิกปุ่ม OK

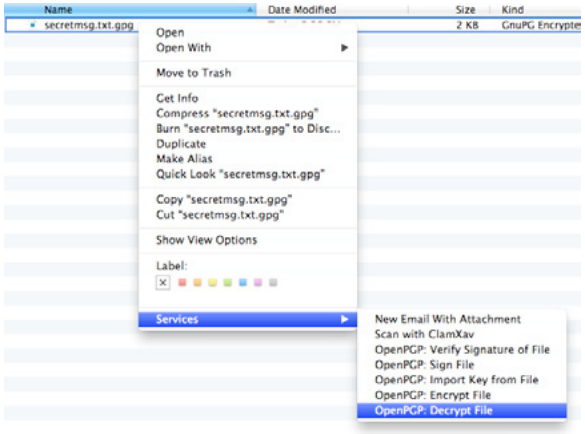


รูปที่ 83 (16-25) หน้าต่างสำหรับเลือกผู้รับไฟล์หรือโฟลเดอร์

3. หน้าต่างใหม่จะปรากฏขึ้น ให้ระบุ passphrase ของกุญแจของผู้ส่งแล้วคลิกปุ่ม OK รอสักครู่จนระบบเข้ารหัสเสร็จจะมีข้อความแสดงบนหน้าจอว่า “Encryption finished” ตามด้วยชื่อของไฟล์ที่ถูกเข้ารหัสแล้ว และจะพบว่ามีไฟล์ที่ถูกเข้ารหัสแล้วเพิ่มขึ้นมาโดยมีชื่อไฟล์เดียวกันกับไฟล์ต้นฉบับแต่มีนามสกุลของไฟล์เป็น .gpg (ในกรณีของโฟลเดอร์ โฟลเดอร์จะถูกบีบอัดเป็นไฟล์ .zip ก่อนที่จะถูกเข้ารหัส)

การถอดรหัสไฟล์หรือโฟลเดอร์

1. คลิกขวาที่ไฟล์หรือโฟลเดอร์ที่ต้องการถอดรหัส แล้วเลือกเมนู Services -> OpenPGP: Decrypt File ดังรูปที่ 84 (16-26)

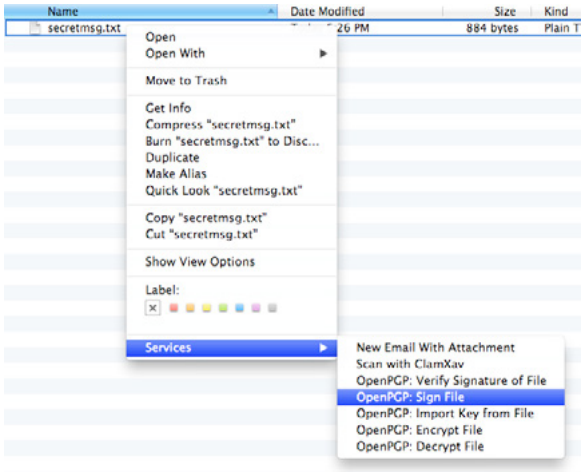


รูปที่ 84 (16-26) การเลือกเมนูเพื่อถอดรหัสไฟล์หรือโฟลเดอร์

2. หน้าต่างใหม่จะปรากฏขึ้น ให้ระบุ passphrase ของกุญแจของผู้รับแล้วคลิกปุ่ม OK รอสักครู่จนระบบถอดรหัสเสร็จจะมีข้อความแสดงบนหน้าจอว่า “Decryption finished” ตามด้วยชื่อของไฟล์ที่ถูกถอดรหัส หากไฟล์ดังกล่าวมีการลงลายมือชื่อก็จะมีการตรวจสอบโดยอัตโนมัติ และหากถูกต้องก็จะมีข้อความแสดงบนหน้าจอว่า “Verification for <ชื่อไฟล์> Signed (ชื่อผู้ส่ง <อีเมลของผู้ส่ง>)” และจะพบว่ามีไฟล์ใหม่เพิ่มขึ้นมาซึ่งเป็นไฟล์ที่ถอดรหัสแล้ว

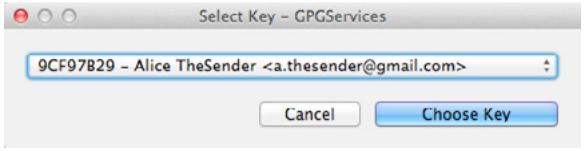
การลงลายมือชื่อบนไฟล์หรือโฟลเดอร์

1. คลิกขวาที่ไฟล์หรือโฟลเดอร์ที่ต้องการลงลายมือชื่อ แล้วเลือกเมนู Services -> OpenPGP: Sign File ดังรูปที่ 85 (16-27)



รูปที่ 85 (16-27) การเลือกเมนูเพื่อลงลายมือชื่อบนไฟล์หรือโฟลเดอร์

2. หน้าต่างใหม่จะปรากฏขึ้นดังรูปที่ 86 (16-28) ให้เลือกกุญแจที่จะเซ็นลายมือชื่อบนไฟล์หรือโฟลเดอร์ จากนั้นคลิกปุ่ม Choose Key

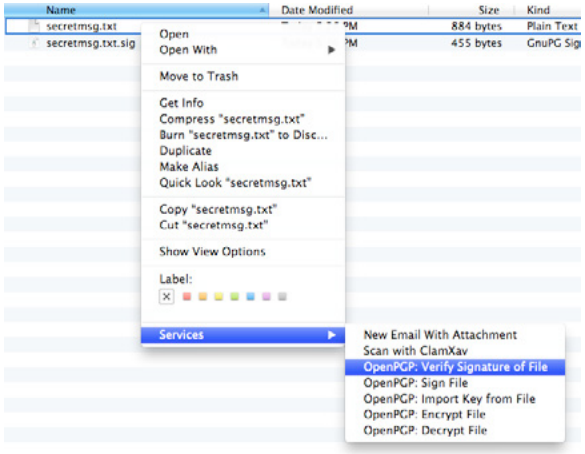


รูปที่ 86 (16-28) หน้าต่างสำหรับเลือกกุญแจที่จะเซ็นลายมือชื่อบนไฟล์หรือโฟลเดอร์

3. หน้าต่างใหม่จะปรากฏขึ้น ให้ระบุ passphrase ของกุญแจของผู้ส่งแล้วคลิกปุ่ม OK รอสักครู่จนระบบลงลายมือชื่อเสร็จจะมีข้อความแสดงบนหน้าจอว่า “Signing finished” ตามด้วยชื่อไฟล์ที่ถูกลงลายมือชื่อ และจะพบว่ามีไฟล์ลายมือชื่อเพิ่มขึ้นมาโดยมีชื่อไฟล์เดียวกันกับไฟล์ต้นฉบับ แต่มีนามสกุลของไฟล์เป็น .sig (ในกรณีของโฟลเดอร์ จะมีนามสกุล .zip.sig ต่อท้ายชื่อไฟล์)

การตรวจสอบลายมือชื่อของไฟล์หรือโฟลเดอร์

1. นำไฟล์ลายมือชื่อที่มีนามสกุล .sig ไปไว้ในที่เดียวกันกับไฟล์ที่จะตรวจสอบ จากนั้นคลิกขวาที่ไฟล์ที่ต้องการตรวจสอบลายมือชื่อ แล้วเลือกเมนู Services -> OpenPGP: Verify Signature of File ดังรูปที่ 87 (16-29)



รูปที่ 87 (16-29) การเลือกเมนูเพื่อตรวจสอบลายมือชื่อของไฟล์หรือโฟลเดอร์

2. ระบบจะตรวจสอบสักครู่ หากลายมือชื่อดังกล่าวเป็นของไฟล์ที่จะตรวจสอบจริง จะมีข้อความแสดงบนหน้าจอว่า “Verification for <ชื่อไฟล์> Signed (ชื่อผู้ส่ง <อีเมลของผู้ส่ง>)”

อ้างอิง

[16-1] http://en.wikipedia.org/wiki/Binary-to-text_encoding

[16-2] http://en.wikipedia.org/wiki/Pretty_Good_Privacy

[16-3] http://support.gpgtools.org/kb/how-to

[16-4] http://tools.ietf.org/html/rfc2440

[16-5] http://www.robertsosinski.com/2008/02/18/working-with-pgp-and-mac-os-x

17 MAN-IN-THE-MIDDLE 102 - PART 2 : DNS SPOOF

ผู้เขียน: เสฏฐวุฒิ แสนนาม

วันที่เผยแพร่: 31 ส.ค. 2555
ปรับปรุงล่าสุด: 31 ส.ค. 2555

จากที่ผู้เขียนได้นำเสนอถึงวิธีการโจมตีแบบ Man-in-the-Middle และได้อธิบายการโจมตีด้วยวิธี ARP Spoof ไปแล้วในบทความก่อนหน้า จะสังเกตได้ว่า การโจมตีโดยวิธี Man-in-the-Middle นั้น เป็นการใช้ช่องโหว่ของการตรวจสอบข้อมูลที่รับส่ง ซึ่งทำให้ผู้ไม่หวังดีสามารถแทรกตัวเข้ามาเพื่อดักรับหรือปลอมแปลงข้อมูลที่ อยู่ระหว่างการสื่อสารได้ ในบทความ Man-in-the-Middle 102 ตอนที่ 2 นี้จะกล่าวถึงการโจมตีด้วยวิธี DNS Spoof หรือการปลอมแปลง DNS

DNS คืออะไร

เครื่องคอมพิวเตอร์ในระบบอินเทอร์เน็ต จะติดต่อสื่อสารกันผ่านทาง IP Address เช่น 122.248.233.179 เป็นต้น ซึ่งหาก IP Address ดังกล่าวนี้เป็นของเครื่องเซิร์ฟเวอร์ที่ให้บริการเว็บไซต์ ผู้ใช้ก็สามารถพิมพ์ IP Address นี้ลงในช่อง Address Bar ของเบราว์เซอร์เพื่อเข้าถึงเว็บไซต์นี้ได้ แต่อย่างไรก็ตาม การใช้ IP Address ในการเข้าถึงเว็บไซต์นั้นจำยากและไม่สะดวกในการใช้งาน จึงมีการคิดค้นสิ่งที่เรียกว่า Domain Name ขึ้นมา ซึ่งเป็นการใช้ชื่อที่เป็นตัวอักษรที่มีความหมายในการเรียกแทน IP Address เช่น www.thaicert.or.th สามารถใช้เรียกแทน IP Address 122.248.233.179 ได้ เป็นต้น การทำงานของระบบดังกล่าวนี้เปรียบได้กับการจดบันทึกรายชื่อผู้ติดต่อลงใน สมุดโทรศัพท์ ซึ่งเป็นการแทนที่หมายเลขโทรศัพท์ด้วยชื่อของผู้ติดต่อที่จำง่ายกว่า โพรโทคอลที่ใช้ในการสืบค้น Domain Name เพื่อหา IP Address ที่สัมพันธ์กับ Domain Name นั้น เรียกว่า Domain Name System (DNS) [17-1]

การทำงานของ DNS

เพื่อให้เข้าใจหลักการทำงานของ DNS ง่ายขึ้น จะขออธิบายลำดับการทำงานของเครื่องคอมพิวเตอร์เมื่อผู้ใช้ต้องการเข้าใช้งาน เว็บไซต์ไทยเซิร์ต โดยเมื่อผู้ใช้พิมพ์ www.thaicert.or.th ที่ช่อง Address Bar ของเบราว์เซอร์ จะมีการทำงานดังนี้

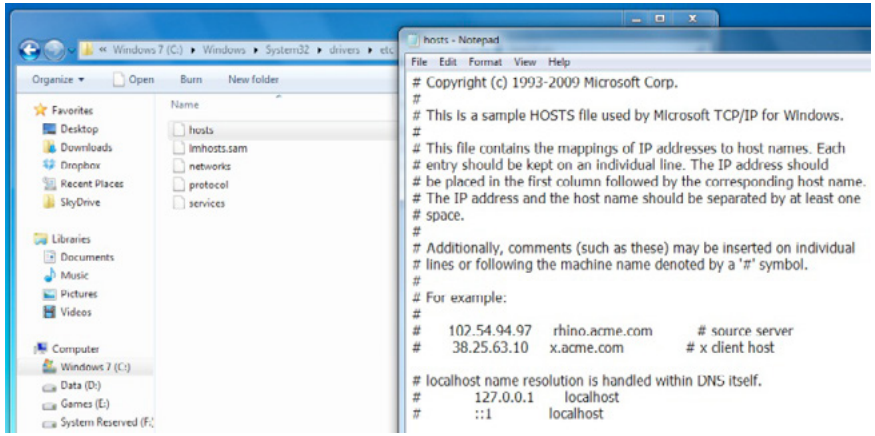
1. ค้นหาข้อมูลจากไฟล์ hosts ไฟล์ hosts เป็นไฟล์ที่ใช้สำหรับกำหนดค่า IP Address และ Domain Name โดยปกติแล้วระบบปฏิบัติการต่างๆ จะเก็บไฟล์ hosts ไว้ที่ตำแหน่งดังนี้

Windows อยู่ที่ Windows\System32\drivers\etc\hosts

Mac OS X อยู่ที่ /private/etc/hosts

Linux อยู่ที่ /etc/hosts

ไฟล์ hosts เป็นไฟล์ข้อความธรรมดา สามารถใช้โปรแกรม Text Editor เปิดขึ้นมาเพื่อดูหรือแก้ไขได้ ดังรูปที่ 88 (17-1) อย่างไรก็ตาม การแก้ไขไฟล์ดังกล่าวนี้สามารถทำได้เฉพาะผู้ที่มีสิทธิของผู้ดูแลระบบ เท่านั้น หากเครื่องคอมพิวเตอร์ไม่พบข้อมูลของ www.thaicert.or.th ในไฟล์ hosts ก็จะไปค้นข้อมูลจาก DNS Table



รูปที่ 88 (17-1) ตัวอย่างข้อมูลในไฟล์ hosts ในระบบปฏิบัติการ Windows 7

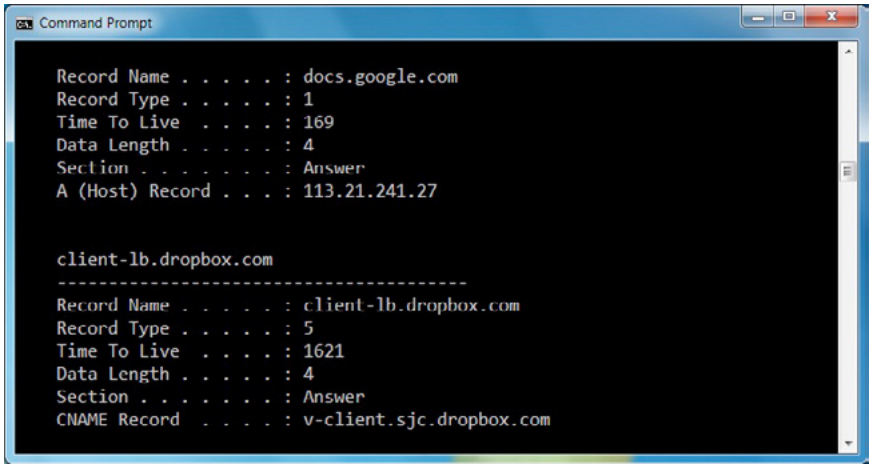
2. ค้นหาข้อมูลจาก DNS Table

DNS Table หรือ DNS Cache ใช้ในการเก็บข้อมูล Domain Name และ IP Address ที่เคยค้นหามาแล้ว เพื่อที่จะได้ไม่ต้องสอบถามกับ DNS Server เมื่อต้องการเรียกใช้งาน Domain Name นี้อีกในครั้งถัดไป การตรวจสอบข้อมูลใน DNS Table สามารถทำได้ดังนี้

Windows ใช้คำสั่ง ipconfig /displaydns

Mac OS X ใช้คำสั่ง dscacheutil -cachedump -entries

Linux โดยปกติแล้วจะไม่มีการทำ DNS Table แต่ในบาง Distro อาจมีการติดตั้งโปรแกรมเพิ่มเติมเพื่อมาจัดการในส่วนนี้ เช่น โปรแกรม nscd (Name Service Cache Daemon)

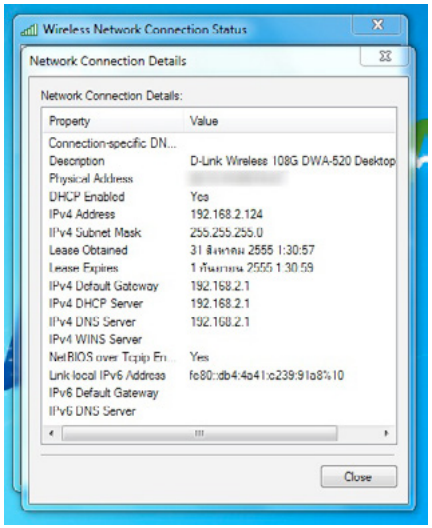


รูปที่ 89 (17-2) ตัวอย่างข้อมูล DNS Table ในระบบปฏิบัติการ Windows 7

หากเปิดเครื่องขึ้นมาใหม่ ระบบจะยังไม่มีข้อมูลใน DNS Table เครื่องคอมพิวเตอร์จะต้องสอบถามกับ DNS Server เพื่อขอทราบ IP Address ของ Domain Name นั้น

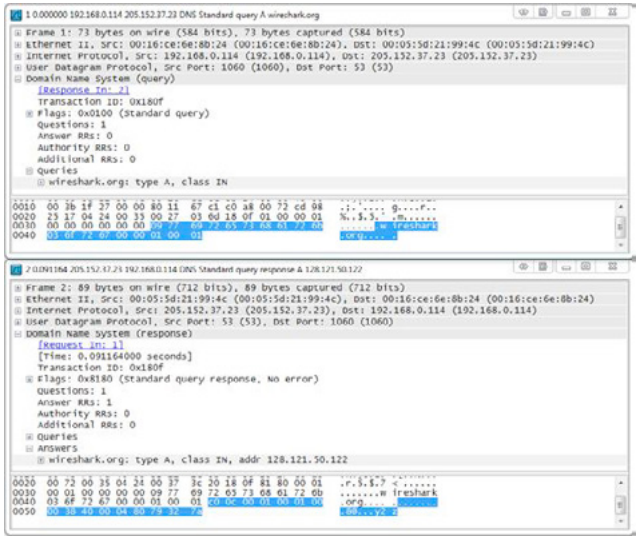
3. ค้นหาข้อมูลจาก DNS Server

DNS Server เป็นเครื่องเซิร์ฟเวอร์ที่มีฐานข้อมูลของ Domain Name และ IP Address โดยปกติแล้วการตั้งค่า DNS Server จะถูกกำหนดมาให้จาก ISP หรือ Router ในตอนที่ผู้ใช้เชื่อมต่อเข้ากับระบบเครือข่าย ตัวอย่างการตั้งค่า DNS Server เป็นดังรูปที่ 90 (17-3) อย่างไรก็ตาม ผู้ใช้สามารถกำหนดการตั้งค่า DNS Server เองได้



รูปที่ 90 (17-3) ตัวอย่างการตั้งค่า DNS Server ในระบบปฏิบัติการ Windows 7

ในการทำงาน เมื่อเครื่องของผู้ใช้ส่ง DNS Query ไปหา DNS Server ผ่าน UDP Port 53 โดยระบุ Domain Name ที่ต้องการหาข้อมูล เครื่องเซิร์ฟเวอร์จะค้นหา Domain Name นั้นในฐานข้อมูล หากพบก็จะส่ง DNS Response ตอบ IP Address กลับไปให้ [17-2] ตัวอย่าง DNS Query และ DNS Response เป็นดังรูปที่ 91 (17-4)



รูปที่ 91 (17-4) ตัวอย่าง DNS Query และ DNS Response (ที่มา WindowsSecurity.com)

อย่างไรก็ตาม ขั้นตอนการทำงานของ DNS นั้นไม่มีการตรวจสอบความถูกต้องของข้อมูลที่รับส่ง จึงเป็นช่องโหว่ให้ผู้ไม่หวังดีโจมตีผ่านจุดนี้ได้โดยการทำ DNS Spoof

DNS Spoof

การทำ DNS Spoofing หรือ DNS Cache Poisoning คือการเปลี่ยนข้อมูลของ DNS ให้วิ่งไปที่ IP Address ปลายทางที่อื่นที่ไม่ใช่ของจริง ซึ่งวิธีการโจมตีแบบนี้จะสังเกตเห็นความผิดปกติได้ยาก เนื่องจากใน Address Bar ของเบราว์เซอร์จะแสดง URL ที่ถูกต้อง แต่เว็บไซต์ปลายทางนั้นไม่ใช่เว็บไซต์ที่แท้จริง จุดประสงค์หลักๆ ของการโจมตีด้วยวิธีนี้อาจจะเป็นการขโมยข้อมูลหรือเพื่อเผยแพร่มัลแวร์ [17-3] ตัวอย่างการโจมตีด้วยวิธี ARP Spoof เช่น

แก้ไขไฟล์ hosts

เนื่องจากไฟล์ hosts เป็นไฟล์ข้อความธรรมดา จึงสามารถใช้โปรแกรม Text Editor เปิดขึ้นมาแก้ไขได้ ดังนั้นหากมีการแก้ไขไฟล์ดังกล่าวโดยใส่ Domain Name และ IP Address ที่ไม่มีอยู่จริงลงไป ก็จะไม่สามารถเข้าใช้งานเว็บไซต์ที่มี Domain Name ดังกล่าวได้ หรือหากมีผู้ไม่หวังดีแก้ไขไฟล์ hosts โดยให้ Domain Name ของเว็บไซต์ใดๆ ชี้ไปที่ IP ของเว็บไซต์อื่นก็สามารถทำได้เช่นกัน ซึ่งการแก้ไขข้อมูลในไฟล์ hosts เพื่อให้ชี้ไปที่เว็บไซต์อื่น อาจเกิดจากการกระทำของผู้ไม่หวังดีหรืออาจเกิดจากมัลแวร์ก็ได้

จากช่องโหว่ดังกล่าวนี้ ทาง Microsoft จึงได้เพิ่มระบบป้องกันการแก้ไขไฟล์ hosts ใน Windows 8 โดยจะมีโปรแกรม Windows Defender คอยตรวจสอบว่ามีการแก้ไขค่า DNS ของเว็บไซต์สำคัญๆ เช่น Facebook.com ในไฟล์ hosts หรือไม่ หากพบก็จะลบข้อมูลนั้นออกเพื่อให้ป้องกันไม่ให้ผู้ใช้ถูกหลอกลวงจากเว็บไซต์ปลอม อย่างไรก็ตาม ผู้ใช้ยังสามารถปิดการทำงานของระบบดังกล่าวนี้ได้ [17-4] การปลอมแปลง DNS ด้วยการแก้ไขไฟล์ hosts เรียกว่า Local DNS Spoofing

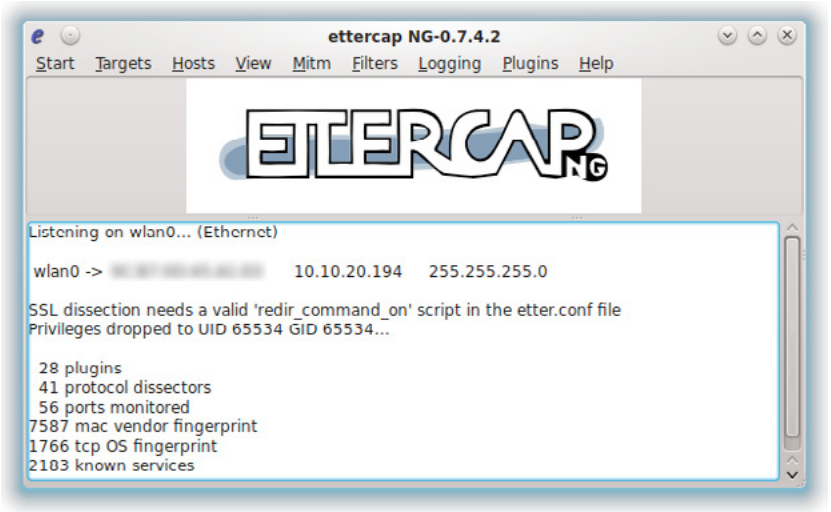
กำหนดค่าให้ติดต่อไปยัง DNS Server ปลอม

เนื่องจากการทำงานของ DNS ต้องมีการติดต่อไปยัง DNS Server เพื่อขอข้อมูล IP Address ของเว็บไซต์ที่ต้องการเข้าชม ดังนั้นจึงมีผู้ไม่หวังดีพัฒนามัลแวร์ขึ้นมาเพื่อเปลี่ยนแปลงการตั้งค่า DNS Server ในเครื่องของผู้ใช้ให้วิ่งมาที่เครื่อง DNS Server

ของผู้สร้างมัลแวร์ ตัวอย่างมัลแวร์ที่โจมตีด้วยวิธีการนี้ เช่น DNS Changer [17-5]

ส่ง DNS Response ปลอม

เนื่องจากการติดต่อขอข้อมูล IP Address จากเครื่อง DNS Server จำเป็นต้องมีการส่ง DNS Request ออกไปแล้วรอให้เซิร์ฟเวอร์ตอบ DNS Response กลับมา ในระหว่างที่กำลังรอคำตอบจากเครื่อง DNS Server อยู่นั้น หากมีผู้ไม่หวังดีส่ง DNS Response ตอบ IP Address ที่ไม่ถูกต้องกลับมาให้ เครื่องคอมพิวเตอร์ก็จะเข้าใจว่าคำตอบนั้นเป็น IP Address จริงของ Domain Name ที่ต้องการติดต่อด้วย ตัวอย่างโปรแกรมที่ใช้ในการโจมตีด้วยวิธีนี้ เช่น dsniff หรือ ettercap ดังรูปที่ 92 (17-3) การโจมตีด้วยวิธีการส่ง DNS Response ปลอม เรียกว่า Remote DNS Spoofing

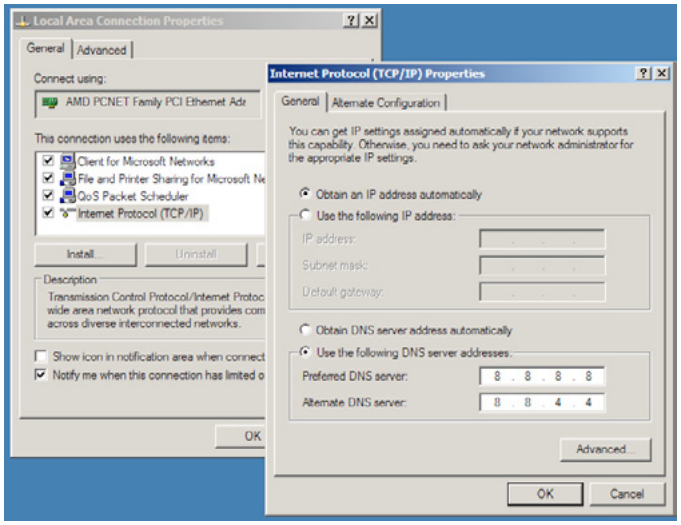


รูปที่ 92 (17-3) ตัวอย่างโปรแกรม ettercap

การตรวจสอบและป้องกัน

การตรวจสอบว่าถูกโจมตีด้วยวิธี DNS Spoof หรือไม่นั้นอาจทำได้ยาก เนื่องจากเป็นวิธีการโจมตีที่แนบเนียนและแทบจะไม่เห็นความผิดปกติ อย่างไรก็ตาม ผู้ใช้อาจตรวจสอบข้อมูลจากไฟล์ hosts ของเครื่องว่ามีการตั้งค่า Domain Name ที่มีลักษณะผิดปกติบ้างหรือไม่ รวมทั้งอาจตรวจสอบจากการตั้งค่า DNS Server ในเครื่องด้วย

นอกจากนี้ ผู้ใช้สามารถกำหนดการตั้งค่า DNS Server ให้ใช้ข้อมูลจาก Public DNS Server ที่เชื่อถือได้ เช่น **OpenDNS** หรือ **Google Public DNS** เป็นต้น ตัวอย่างการตั้งค่าการเชื่อมต่อให้ใช้ Google Public DNS Server เป็นดังรูปที่ 93 (17-6)



รูปที่ 93 (17-6) การกำหนดค่าให้ใช้ DNS Server ของ Google

อ้างอิง

[17–1] http://www.howtogeek.com/122845/htg-explains-what-is-dns/

[17–2] http://www.windowsecurity.com/articles/understanding-man-in-the-middle-attacks-arp-part2.html

[17–3] http://resources.infosecinstitute.com/dns-hacking/

[17–4] http://www.howtogeek.com/122404/how-to-block-websites-in-windows-8s-hosts-file/

[17–5] http://www.thaicert.or.th/alerts/corporate/2012/al2012co0006.html

18 วิธีปิดการทำงานของ JAVA ใน เว็บเบราว์เซอร์

ผู้เขียน: วิศัลย์ ประสงค์สุข
วันที่เผยแพร่: 14 ก.ย. 2555
ปรับปรุงล่าสุด: 14 ก.ย. 2555

Java เป็นภาษาหนึ่งที่ใช้ในการพัฒนาโปรแกรมคอมพิวเตอร์ ถูกคิดค้นโดยบริษัท Sun Microsystems โปรแกรมที่พัฒนาโดยภาษา Java สามารถทำงานได้โดยไม่จำเป็นต้องยึดติดกับระบบปฏิบัติการใดเพียงระบบเดียว เนื่องจากโปรแกรมที่เขียนขึ้นโดยภาษา Java จะทำงานผ่าน Java Runtime Environment (JRE) ซึ่งจะเป็นการจำลองระบบขึ้นมาเพื่อประมวลผลคำสั่งภาษา Java ทำให้โปรแกรมที่พัฒนาขึ้นมาสามารถนำไปใช้งานบนระบบปฏิบัติการอื่นได้โดยไม่ ต้องแก้ไขโค้ดของโปรแกรม [18-1]

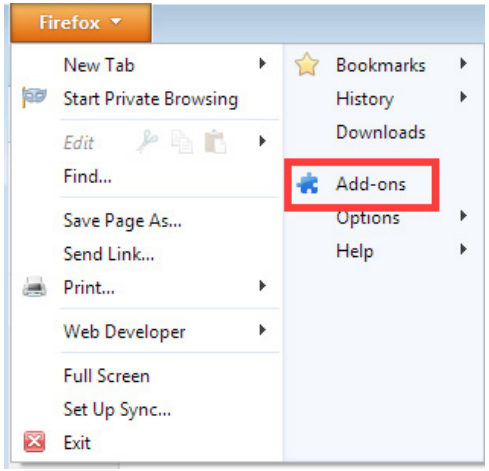
เมื่อวันที่ 28 สิงหาคม 2555 ทางไทยเซิร์ตได้ประกาศแจ้งเตือนเกี่ยวกับช่องโหว่ด้านความมั่นคงปลอดภัยของ JRE เวอร์ชัน 7 โดยหากผู้ใช้เข้าไปยังเว็บไซต์ที่มีการเรียกใช้งาน Java Applet ที่เป็นอันตราย (Java Applet คือโปรแกรมขนาดเล็กที่พัฒนาโดยภาษา Java ซึ่งสามารถแสดงผลเป็นส่วนหนึ่งของหน้าเว็บไซต์ได้) ช่องโหว่นี้จะทำให้เครื่องคอมพิวเตอร์ของผู้ใช้ดาวน์โหลดโปรแกรมไม่พึง ประสงค์เข้ามาติดตั้งโดยผู้ใช้ไม่รู้ตัว ผู้เชี่ยวชาญได้ออกมาให้คำแนะนำว่าควรปิดการทำงานของ Java ในเว็บเบราว์เซอร์ หรือหากไม่มีความจำเป็นต้องใช้งาน Java Applet ควรลบโปรแกรม JRE ออกจากระบบ [18-2]

ดังนั้น บทความนี้จึงขอนำเสนอวิธีการปิดการทำงานของ Java ในเว็บเบราว์เซอร์ที่ได้รับความนิยมสูงในประเทศไทย อันได้แก่ Mozilla Firefox, Google Chrome, Safari และ Internet Explorer การปิด Java ในที่นี้จะเป็นการปิดการทำงานของ JRE ในเว็บเบราว์เซอร์ แต่ JavaScript ยังคงทำงานได้ตามปกติ

การปิดการทำงานของ Java ใน Mozilla Firefox

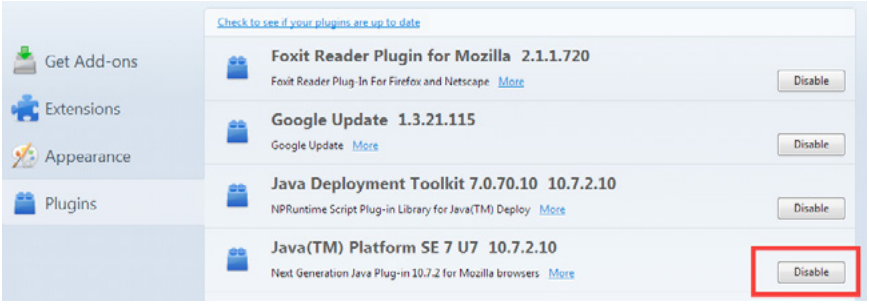
ในตัวอย่างนี้จะใช้ Mozilla Firefox เวอร์ชัน 15 ซึ่งมีวิธีการทำดังนี้

1. คลิกที่ปุ่มเมนู Firefox ด้านบนซ้ายของหน้าต่าง และคลิกที่ Add-ons ดังรูปที่ 94 (18-1)



รูปที่ 94 (18-1) คลิกที่ Add-ons

2. เมื่อหน้าต่าง Add-ons Manager ปรากฏขึ้นมา ให้คลิกที่แถบ Plugins จากนั้นค้นหา Java (TM) Platform แล้วคลิกที่ปุ่ม Disable ดังรูปที่ 95 (18-2)

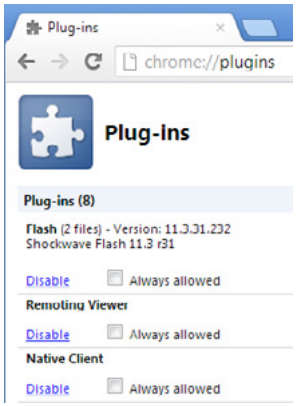


รูปที่ 95 (18-2) Disable Java (TM) Platform

การปิดการทำงานของ Java ใน Google Chrome

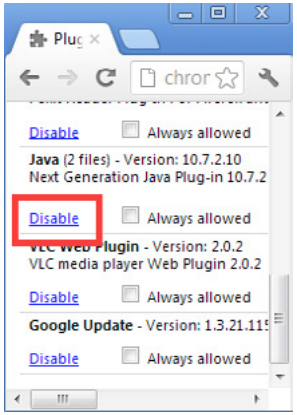
ในตัวอย่างนี้จะใช้ Google Chrome เวอร์ชัน 21 ซึ่งมีวิธีการทำดังนี้

1. พิมพ์ “chrome://plugins” ลงในช่อง Address bar ของเบราว์เซอร์ จะปรากฏรายการ Plug-ins ทั้งหมดที่ติดตั้งอยู่ใน Chrome ดังรูปที่ 96 (18-3)



รูปที่ 96 (18-3) แสดงรายการ Plug-in ที่ติดตั้งใน Chrome

2. คลิกที่ปุ่ม Disable ภายใต้กรอบ Java ดังรูปที่ 97 (18-4)

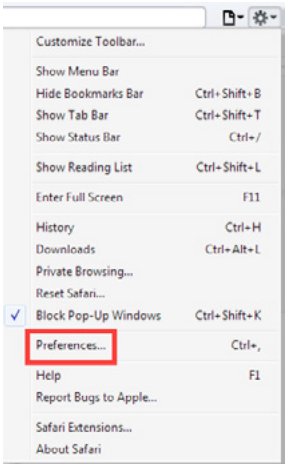


รูปที่ 97 (18-4) Disable Java

การปิดการทำงานของ Java ใน Safari

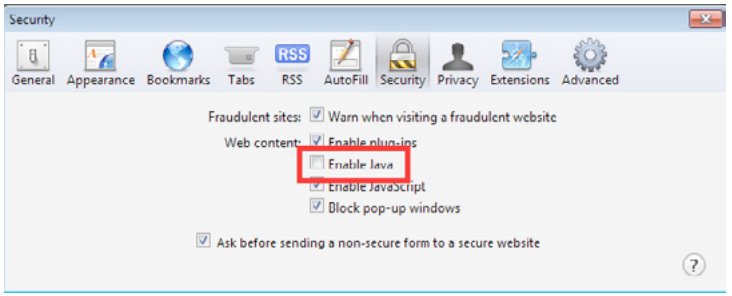
ในตัวอย่างนี้จะใช้ Safari เวอร์ชัน 5 ซึ่งมีวิธีการทำดังนี้ [18-3]

1. คลิกที่รูปเฟืองด้านขวามือของหน้าต่าง Safari และเลือกที่ Preferences... ดังรูปที่ 98 (18-5)



รูปที่ 98 (18-5) คลิกที่ Preferences...

2. เมื่อหน้าต่างการตั้งค่าปรากฏขึ้น คลิกที่แถบ Security และนำเครื่องหมายถูกออกจาก Enable Java ดังรูปที่ 99 (18-6)

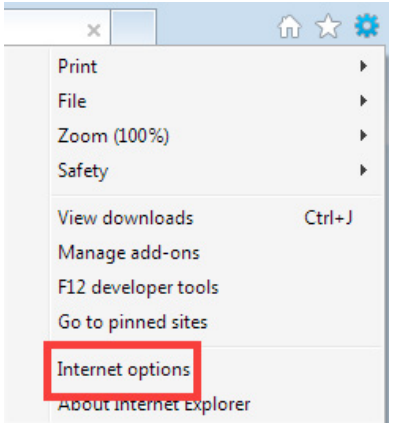


รูปที่ 99 (18-6) นำเครื่องหมายถูกออกจาก Enable Java

การปิดการทำงานของ Java ใน Internet Explorer

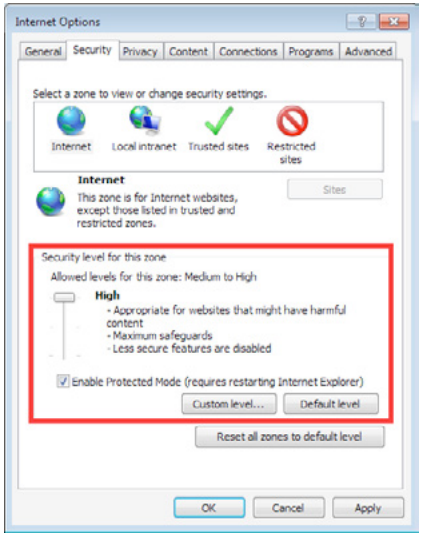
การปิดการทำงานของ Java ใน Internet Explorer (IE) นั้น ไม่สามารถทำได้โดยการ Disable ปลั๊กอินของ Java เหมือนในเว็บเบราว์เซอร์ตัวอื่น ๆ เนื่องจาก IE นั้นไม่ได้มอง Java เป็นส่วนเสริมของเบราว์เซอร์เหมือนกับปลั๊กอินทั่วไป ทาง Microsoft ได้แนะนำให้ผู้ใช้แก้ไขค่า Registry ของระบบเพื่อปิดการทำงานของ Java ด้วยตนเอง [18-4] แต่เนื่องจากการแก้ไข Registry มีความเสี่ยงที่หากแก้ไขผิดพลาดอาจทำให้ระบบไม่สามารถทำงานต่อได้ ดังนั้นผู้ที่ใช้งาน IE จึงควรกำหนดค่า Security ให้อยู่ที่ระดับ High จนกว่าจะมีมาตรการแก้ไขที่สามารถทำได้สะดวกและปลอดภัยกว่านี้ใน IE เวอร์ชัน 9 สามารถกำหนดค่า Security ได้ดังนี้

1. คลิก ที่รูปเฟืองด้านขวาของหน้าต่าง IE เลือก Internet options ดังรูปที่ 100 (18-7) (ใน IE เวอร์ชันอื่น สามารถคลิกที่เมนู Tools และเลือก Internet options)



รูปที่ 100 (18-7) เลือก Internet options

2. เมื่อหน้าต่าง Internet options ปรากฏขึ้น คลิกที่แถบ Security และปรับ Security level for this zone ให้เป็น High ดังรูปที่ 101 (18-8)



รูปที่ 101 (18-8) ปรับ Security level for this zone ให้เป็น High

อย่างไรก็ตาม การกำหนดค่า Security ให้อยู่ในระดับ High นั้นเป็นการปิดการทำงานของความสามารถที่อาจเป็นอันตรายต่อระบบ ให้เหลือเพียงความสามารถในการเข้าใช้งานเว็บไซต์ขั้นพื้นฐานเท่านั้น ซึ่งผู้ใช้อาจพบปัญหาในการเข้าใช้งานบางเว็บไซต์ที่ต้องการความสามารถอื่นๆ นอกเหนือจากการแสดงผลเว็บไซต์

เช่น เว็บไซต์ที่มีการใช้งาน JavaScript หรือเว็บไซต์ที่มีคลิปวิดีโอ เป็นต้น ซึ่งหากจำเป็นต้องเข้าถึงเว็บไซต์ที่มีความสามารถดังกล่าว ควรเปลี่ยนไปใช้เบราว์เซอร์อื่นแทน

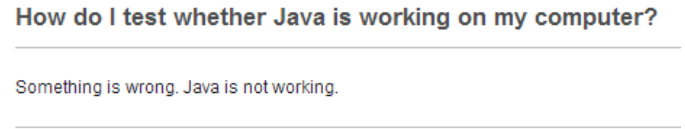
การทดสอบการทำงานของ Java

ผู้ใช้สามารถทำการทดสอบว่าได้ปิดการทำงานของ Java แล้วหรือยัง โดยการเข้าเว็บไซต์ที่ใช้ Java applet ในการแสดงผลหน้าเว็บไซต์ ในที่นี้ขอยกตัวอย่างหน้าเว็บไซต์ของ java.com ซึ่งมี URL คือ

http://www.java.com/en/download/testjava.jsp

หาก Java ยังใช้งานในเว็บเบราว์เซอร์ได้ จะมีข้อความแจ้งว่า “Your Java is working” ดังรูปที่ 102 (18-9) แต่หากปิดการทำงานของ Java แล้ว เว็บเบราว์เซอร์จะแสดงข้อความว่าไม่พบปลั๊กอินของ Java ในระบบ ซึ่งแต่ละเบราว์เซอร์อาจแสดงผลต่างกัน เช่น หากเป็น Firefox จะแสดงข้อความ “Something is wrong. Java is not working ” ดังรูปที่ 103 (18-10)

รูปที่ 102 (18-9) เมื่อไม่ปิดการทำงานของ Java



รูปที่ 103 (18-10) การแสดงผลของ Firefox เมื่อปิดการทำงานของ Java แล้ว

เนื่องจาก Java เป็นโปรแกรมที่มีการแจ้งช่องโหว่ค่อนข้างบ่อย และการปล่อยอัพเดทเพื่อแก้ไขปัญหานั้นใช้เวลานาน การปิดการทำงานของ Java ในเว็บเบราว์เซอร์ จึงเป็นวิธีการหนึ่งที่สามารถช่วยในการป้องกัน

ตัวจากภัยคุกคามซึ่งเกิดจาก ช่องโหว่ของ Java ดังที่ได้กล่าวไว้ในข้างต้นได้ แต่หากผู้ใช้มีความจำเป็นต้องใช้งานเว็บไซต์ที่มี Java Applet เช่น เว็บไซต์ภายในหน่วยงาน ก็อาจเปิดใช้งาน Java ได้ เพียงแต่ต้องมั่นใจว่าเว็บไซต์นั้นปลอดภัยจริง ๆ และเมื่อใช้งานเสร็จแล้ว ก็ควรปิดการทำงานของ Java ไว้ตามเดิม

อ้างอิง

[18-1] http://searchsoa.techtarget.com/definition/Java

[18-2] http://www.thaicert.or.th/alerts/corporate/2012/al2012co0018.html

[18-3] http://support.apple.com/kb/HT5241

[18-4] http://support.microsoft.com/kb/2751647

19 ดูแลการเข้าเว็บไซต์ของเด็ก ๆ ด้วย WINDOWS LIVE FAMILY SAFETY

ผู้เขียน: วิศัลย์ ประสงค์สุข

วันที่เผยแพร่: 21 กันยายน 2555
ปรับปรุงล่าสุด: 21 กันยายน 2555

ผู้ปกครองหลายท่านคงเป็นกังวล เมื่อเห็นเด็ก ๆ เล่นคอมพิวเตอร์เป็นเวลานาน โดยที่ไม่รู้ว่าเล่นอะไรบ้าง ยิ่งทุกวันนี้มีเว็บไซต์ที่เนื้อหาไม่เหมาะสมกับเด็กและเยาวชนอยู่มาก และผู้ปกครองก็ไม่สามารถที่จะดูแลการเข้าเว็บไซต์ของบุตรหลานได้ตลอดเวลา วิธีการหนึ่งที่ช่วยในการป้องกันไม่ให้เด็กเข้าเว็บไซต์ไม่เหมาะสมเหล่านี้ ก็คือการติดตั้งโปรแกรมที่ช่วยควบคุมการเข้าถึงเว็บไซต์

โปรแกรมที่กล่าวถึงนี้ มีให้เลือกใช้อยู่หลากหลาย แต่สำหรับผู้ที่ใช้ระบบปฏิบัติการ Windows7 ขึ้นไป สามารถติดตั้งโปรแกรม Windows Live Family Safety ได้ ซึ่งเป็นโปรแกรมที่ไมโครซอฟต์ให้ใช้งานได้ฟรี โดยโปรแกรม Windows Live Family Safety นี้ นอกจากจะสามารถควบคุมการเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมกับเยาวชนได้แล้ว ยังมีความสามารถอื่น ๆ ดังนี้ [19-1]

กำหนดช่วงเวลาในการใช้งานคอมพิวเตอร์ได้

ป้องกันการใช้งานโปรแกรม หรือเล่นเกมที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตได้

โปรแกรม Windows Live Family Safety นี้ถูกบรรจุอยู่ในชุดโปรแกรม Windows Essentials ซึ่งสามารถดาวน์โหลดได้จากเว็บไซต์ของ ไมโครซอฟต์ (http://windows.microsoft.com/en-US/windows-live/essentials-home) ในการใช้งานโปรแกรม มีสิ่งที่ผู้ปกครองต้องจัดเตรียมดังนี้

ผู้ปกครองจะต้องใช้ข้อมูลบัญชีผู้ใช้ของ Windows Live (บัญชีเดียวกันกับที่ใช้เข้าสู่ระบบ MSN หรือ Hotmail) ในการเข้าสู่ระบบของโปรแกรม Windows Live Family Safety

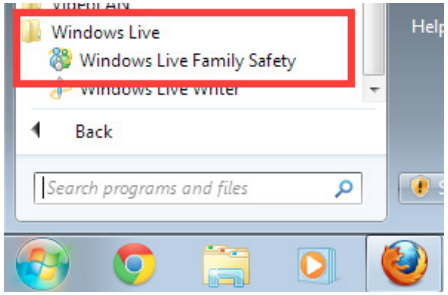
เตรียมบัญชีผู้ใช้คอมพิวเตอร์สำหรับเด็กและผู้ปกครอง โดยที่

* บัญชีผู้ใช้สำหรับผู้ปกครอง เป็นบัญชีผู้ใช้ประเภท Administrator
* บัญชีผู้ใช้สำหรับเด็ก เป็นบัญชีผู้ใช้ประเภท Standard

ปกติแล้วในการติดตั้งระบบปฏิบัติการ (การลง Windows) จะมีการให้ผู้ใช้สร้างบัญชีผู้ใช้สำหรับใช้งานคอมพิวเตอร์อยู่แล้ว ซึ่งบัญชีผู้ใช้นั้นจะเป็นประเภท Administrator สำหรับการสร้างบัญชีผู้ใช้สำหรับเด็กให้เป็นบัญชีประเภท Standard นั้น สามารถทำได้ในโปรแกรม Windows Live Family Safety ซึ่งจะอธิบายในลำดับถัดไป

หลังจากติดตั้งชุดโปรแกรม Windows Essentials แล้ว ผู้ปกครองสามารถเข้าใช้งาน Windows Live Family Safety ได้ดังนี้

1. คลิกเข้าไปที่ Start > All programs > Windows Live > Windows Live Family Safety ดังรูปที่ 104 (19-1)



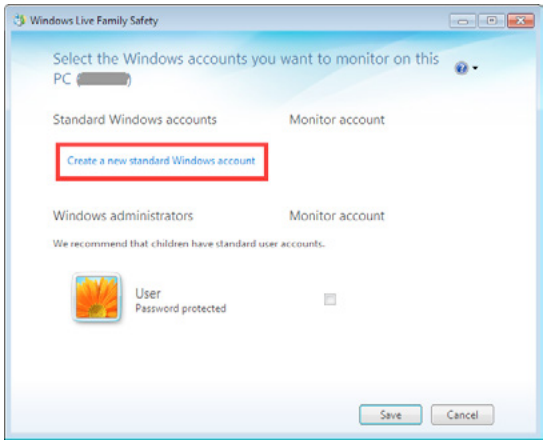
รูปที่ 104 (19-1) คลิก Windows Live Family Safety

2. เมื่อหน้าต่างโปรแกรม Windows Live Family Safety ปรากฏขึ้นมา ให้ทำการเข้าสู่ระบบโดยใช้บัญชีผู้ใช้ Windows Live ดังรูปที่ 105 (19-2)

รูปที่ 105 (19-2) เข้าสู่ระบบของโปรแกรม Windows Live Family Safety

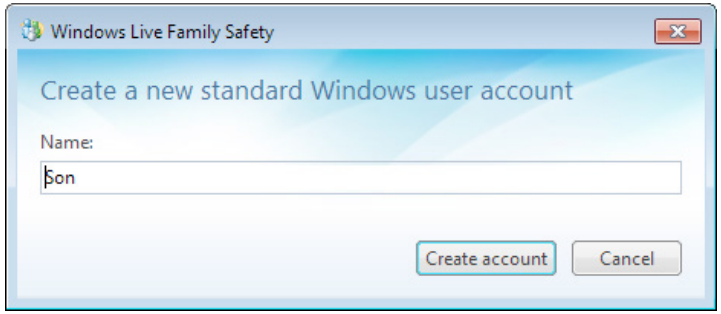
3. เมื่อเข้าสู่โปรแกรม Windows Live Family Safety แล้ว หากในเครื่องคอมพิวเตอร์ยังไม่มีผู้ใช้ Standard สำหรับเด็ก สามารถสร้างได้โดยคลิกที่ข้อความ “Create a new standard Windows Account”

ดังรูปที่ 106 (19-3) หากมีบัญชีผู้ใช้ประเภท Standard สำหรับเด็กอยู่แล้ว สามารถข้ามไปยังขั้นตอนที่ 5 ได้

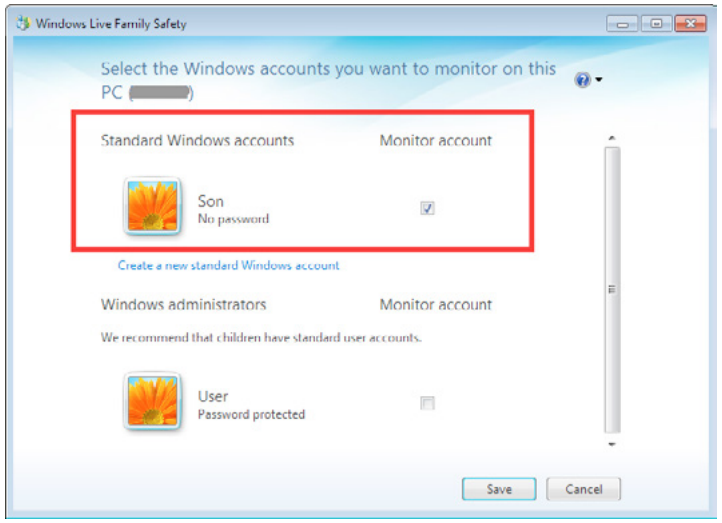


รูปที่ 106 (19-3) การสร้างบัญชีผู้ใช้ประเภท Standard สำหรับเด็ก

4. ทำการตั้งชื่อบัญชีผู้ใช้ ซึ่งในตัวอย่าง ได้กำหนดชื่อของบัญชีผู้ใช้เป็น “Son” ดังรูปที่ 107 (19-4) หลังจากสร้างบัญชีผู้ใช้สำหรับเด็กแล้ว จะปรากฏบัญชีผู้ใช้ใหม่ อยู่ในรายการ Standard Windows accounts ในหน้าต่างโปรแกรม Windows Live Family Safety ดังรูปที่ 108 (19-5)

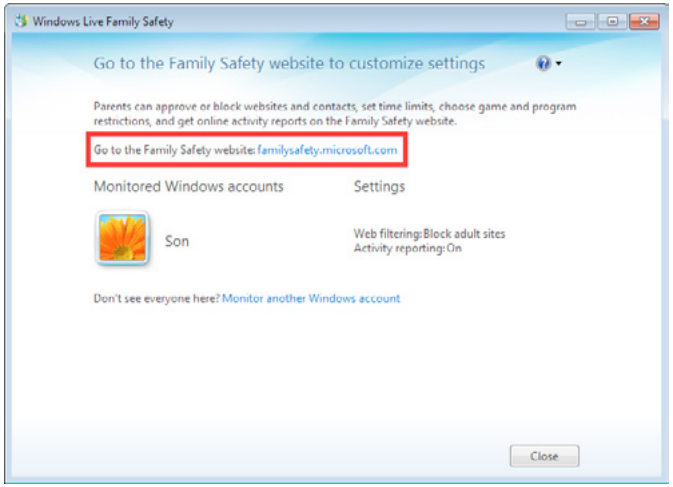


รูปที่ 107 (19-4) การกำหนดชื่อบัญชีผู้ใช้ สำหรับเด็ก



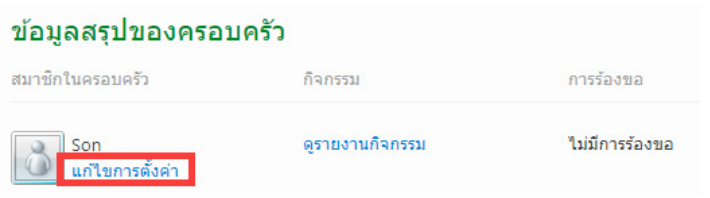
รูปที่ 108 (19-5) บัญชีผู้ใช้ใหม่ ปรากฏในรายการ Standard Windows accounts

5. เลือกบัญชีผู้ใช้ที่ต้องการดูแลและกดปุ่ม Save จากนั้น จะปรากฏหน้าต่างแจ้งให้ผู้ปกครองคลิกไปที่เว็บไซต์ familysafety.microsoft.com เพื่อทำการตั้งค่าการควบคุมบัญชีผู้ใช้ของเด็ก ดังรูปที่ 109 (19-6)



รูปที่ 109 (19-6) คลิกที่ familysafety.microsoft.com เพื่อทำการตั้งค่าการควบคุม

6. เมื่อเข้าสู่ระบบของเว็บไซต์ familysafety.microsoft.com แล้ว ผู้ปกครองสามารถตั้งค่าการควบคุมบัญชีของเด็กได้ โดยคลิกที่ ข้อความ “แก้ไขการตั้งค่า” ดังรูปที่ 110 (19-7)

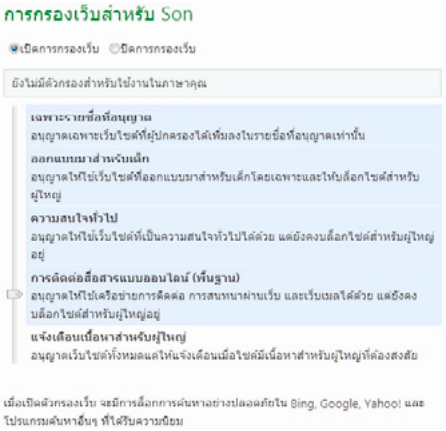


รูปที่ 110 (19-7) คลิกเพื่อแก้ไขการตั้งค่า เพื่อตั้งค่าการควบคุม

7. ที่หน้าต่างตั้งค่าการควบคุม จะพบว่ามีเมนูการควบคุมบัญชีผู้ใช้อยู่ในด้านซ้ายมือ คลิกที่ข้อความ “การกรองเว็บ” เพื่อกำหนดค่าการควบคุมการเข้าถึงเว็บไซต์ ดังรูปที่ 111 (19-8)

รูปที่ 111 (19-8) กำหนดค่าการควบคุมการเข้าถึงเว็บไซต์

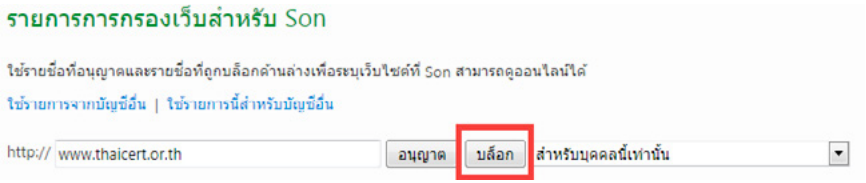
8. ทำการเลือกระดับการควบคุมที่ต้องการ โดยรายการของเว็บไซต์สำหรับผู้ใหญ่นั้น ทีมงานของ Windows Live Family Safety จะเป็นผู้รวบรวมไว้ ดังรูปที่ 112 (19-9)



รูปที่ 112 (19-9) เลือกระดับการควบคุมการเข้าถึงเว็บไซต์

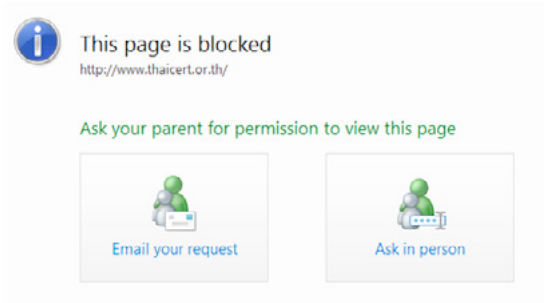
9. ผู้ปกครองสามารถระบุเว็บไซต์ที่ไม่ต้องการให้เด็กเข้าได้ด้วยการคลิกที่ข้อ ความ “รายการการกรองเว็บ” ในเมนูการควบคุมบัญชีผู้ใช้ในด้านซ้ายมือ และทำการบล็อกการเข้าถึงเว็บไซต์ โดยการป้อน URL ที่

ต้องการลงในช่อง http:// และกดปุ่มบล็อก ดังรูปที่ 113 (19-10) ในตัวอย่างนี้จะทำบล็อกไม่ให้ผู้ใช้เข้าเว็บไซต์ www.thaicert.or.th



รูปที่ 113 (19-10) ป้อน URL ที่ไม่ต้องการให้เด็กเข้า และกดปุ่มบล็อก

ซึ่งหลังจากนี้บัญชีผู้ใช้เด็ก จะไม่สามารถเข้าสู่เว็บไซต์ www.thaicert.or.th ได้ดังแสดงในรูปที่ 114 (19-11)



รูปที่ 114 (19-11) หน้าต่างแสดงผลเมื่อผู้ใช้เข้าเว็บไซต์ที่ถูกกำหนดไว้

จากรูปที่ 114 (19-11) จะพบว่า ผู้ใช้บัญชีเด็กไม่สามารถเข้าสู่เว็บไซต์ที่บล็อกไว้ได้ และโปรแกรม Windows Live Family Safety จะมีการให้ขออนุญาต หากเด็ก ๆ ต้องการเข้าถึงเว็บไซต์นั้นจริง ๆ โดยสามารถขออนุญาตผู้ปกครองได้ 2 ช่องทางด้วยกัน คือ

Email your request ในกรณีที่ผู้ปกครองไม่อยู่ด้วย เด็ก ๆ สามารถส่งอีเมลเพื่อขอให้ผู้ปกครองอนุญาตได้

Ask in person ในกรณีที่ผู้ปกครองอยู่ด้วย เด็ก ๆ สามารถขอให้ผู้ปกครองป้อนรหัสผ่าน Windows Live ในหน้าต่างที่ปรากฏหลังคลิกเลือก Ask in person ได้

เพียงเท่านี้ ผู้ปกครองก็สามารถอุ่นใจได้ระดับหนึ่งว่าเด็ก ๆ ที่ท่านดูแล เข้าใช้งานอินเทอร์เน็ตได้อย่างเหมาะสม นอกจากนี้โปรแกรม Windows Live Family Safety ยังมีความสามารถอื่น ๆ เช่น การกำหนดช่วงเวลาในการใช้งานคอมพิวเตอร์ การป้องกันการใช้งานโปรแกรม การเล่นเกมที่ไม่เหมาะสมหรือไม่ได้รับอนุญาต ผู้ใช้สามารถศึกษาเพิ่มเติมด้วยตนเองได้ เนื่องจากมีวิธีการตั้งค่าการใช้งานที่คล้ายกัน

อ้างอิง

[19-1] http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety

20 SOCIAL ENGINEERING

ผู้เขียน: วิศัลย์ ประสงค์สุข, เสฏฐวุฒิ แสนนาม และ พรพรหม ประภากิตติกุล
วันที่เผยแพร่: 2 พฤศจิกายน 2555
ปรับปรุงล่าสุด: 8 พฤศจิกายน 2555

Social Engineering เป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผย ข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย [20-1] ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อในที่นี้ก็มักจะเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือบัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตามซึ่งหลงเชื่อการหลอกลวงนั้น

การที่ผู้ไม่หวังดีจะหลอกลวงเหยื่อให้ได้ข้อมูลที่ต้องการมานั้น ไม่ได้มีวิธีการที่ตายตัว ทำให้หากจะยกตัวอย่างวิธีการของ Social Engineering ในเอกสารนี้ให้ครบถ้วนนั้น จึงแทบจะเป็นไปไม่ได้ ในที่นี้จึงขอกล่าวถึงวิธีการที่ผู้ไม่หวังดีใช้เพื่อให้ได้มาซึ่งข้อมูลที่ ต้องการโดยสังเขป ดังนี้ [20-2] [20-3]

Telephone เป็นการโทรศัพท์เข้ามาหลอกลวงเหยื่อ เพื่อให้เปิดเผยข้อมูลสำคัญหรือหลอกล่อให้เหยื่อกระทำการตามที่ผู้ไม่หวังดี ต้องการ หรือถ้าเป็นในองค์กรต่าง ๆ กลุ่มที่มักจะตกเป็นเหยื่ออาจจะเป็นฝ่ายประสัมพันธ์, HR, หรือฝ่ายบริการลูกค้า เป็นต้น ซึ่งเป็นกลุ่มที่มีหน้าที่คอยให้ข้อมูลกับบุคคลอื่นอยู่แล้ว ดังนั้นกลุ่มคนเหล่านี้จึงมีความเสี่ยงสูงที่อาจจะเผลอเปิดเผยข้อมูลสำคัญ บางอย่างออกมา ตัวอย่างของการหลอกลวงในลักษณะนี้เช่น ผู้ไม่หวังดีโทรมาหลอกลวงเหยื่อ ว่าเหยื่อได้รับสิทธิในการลดหย่อนภาษีจากกรมสรรพากรจึงอยากจะโอนเงินภาษีคืน ให้ผ่านทางธนาคาร ขอให้เหยื่อแจ้งหมายเลขบัญชีธนาคารให้ทราบ และขอให้ทำการโอนเงินเข้ามายังบัญชีของผู้โจมตีเพื่อเป็นการยืนยันว่า เหยื่อเป็นเจ้าของบัญชีนั้นจริง ซึ่งหากเหยื่อหลงเชื่อก็จะทำการโอนเงินไปให้ผู้โจมตี

Online เป็นการหลอกลวงเหยื่อผ่านทางอินเทอร์เน็ต ไม่ว่าจะผ่านการเข้าใช้งานเว็บไซต์ อีเมล หรือการแชต การหลอกลวงในรูปแบบนี้ผู้ไม่หวังดีมักจะมีเป้าหมายเพื่อขโมยรหัสผ่าน ของบริการต่าง ๆ ตัวอย่างการหลอกลวงในลักษณะนี้เช่น ผู้ไม่หวังดีส่งอีเมลถึงลูกค้าของธนาคารโดยอ้างว่าธนาคารได้มีการปรับปรุง ระบบรักษาความมั่นคงปลอดภัย จึงอยากให้ลูกค้าเข้าสู่ระบบเพื่อยืนยันข้อมูลส่วนบุคคลโดยคลิกที่ลิงก์ที่ ส่งมาในอีเมล หากผู้ใช้คลิกลิงก์

เพื่อที่จะเข้าสู่ระบบ ผู้โจมตีก็จะได้ชื่อผู้ใช้และรหัสผ่านสำหรับการเข้าใช้งานธนาคารของเหยื่อไป เป็นต้น (การโจมตีในลักษณะนี้เรียกว่า Phishing สามารถศึกษาเพิ่มเติมได้ในบทความ รู้จัก Phishing และการป้องกัน) นอกจากนี้หากเหยื่อใช้งานรหัสผ่านตัวเดียวกันกับบริการอื่น ผู้โจมตีก็อาจจะสามารถเข้าสู่ระบบของบริการอื่นได้อีกด้วย **Dumpster Diving** เป็นเทคนิคการค้นหาข้อมูลสำคัญจากถังขยะของบุคคลหรือองค์กรที่เป็นเป้าหมาย เพื่อที่จะได้ข้อมูลสำคัญ เช่น รหัสผ่านที่จดบันทึกไว้ในกระดาษ แผนผังองค์กร หมายเลขโทรศัพท์ รวมถึงข้อมูลสำคัญอื่น ๆ ที่เก็บไว้บนสื่อบันทึกข้อมูลทุกประเภท [20-4] การทำ Dumpster Diving นี้อาจจะทำให้ผู้โจมตีได้ข้อมูลที่เพียงพอสำหรับนำไปใช้หลอกลวงด้วยวิธีการอื่นต่อไป **Shoulder Surfing** เป็นการแอบสังเกตุขณะที่เหยื่อกำลังทำการป้อนข้อมูล หรือเข้าถึงข้อมูลที่ต้องการ ดังรูปที่ 115 (20-1) ซึ่งวิธีการนี้ไม่ได้จำกัดอยู่เพียงการแอบมองขณะที่เหยื่อใช้งานคอมพิวเตอร์ เท่านั้น หากแต่รวมถึงสถานการณ์อื่น เช่นการกดรหัส ATM หรือ การกรอกแบบฟอร์มด้วยปากกา และนอกจากผู้ไม่หวังดีจะแอบสังเกตุเหยื่อในระยะประชิดแล้ว ยังรวมถึงการสังเกตุจากระยะไกลที่ใช้เครื่องมืออย่างกล้องส่องทางไกลด้วย [20-5]

รูปที่ 115 (20-1) Shoulder Surfing

Reverse Social Engineering เป็นวิธีการที่ผู้ไม่หวังดีสามารถทำให้เหยื่อติดต่อกลับเข้ามาหาตนเอง โดยอาจจะติดต่อกลับมาเพื่อขอความช่วยเหลือ หรือสอบถามข้อมูลจากผู้โจมตี ซึ่งเหตุการณ์เช่นนี้อาจเป็นผลมาจากการที่ผู้ไม่หวังดีเคยหลอกลวงเหยื่อเอา ไว้แล้วในครั้งก่อน ทันทีที่เหยื่อติดต่อมายังผู้โจมตี เหยื่อก็แทบจะไม่มีทางรู้ตัวได้เลยว่าตนกำลังถูกหลอกลวงอยู่ ทั้งนี้ก่อนจะหลอกให้เหยื่อติดต่อกลับมานั้นผู้ไม่หวังดีจะต้องทำการบ้านมา เป็นอย่างดี เพื่อไม่ให้เหยื่อที่ติดต่อกลับมาหานั้น เกิดความสงสัย ตัวอย่างง่าย ๆ ของการหลอกลวงลักษณะนี้เช่น ผู้ไม่หวังดีแนะนำเหยื่อว่าหากมีปัญหากับการใช้งานอินเทอร์เน็ต สามารถปรึกษากับตนได้ ซึ่งเมื่อเวลาผ่านไปเหยื่ออาจจะติดต่อกลับมา ซึ่งจะเป็นโอกาสที่ดีของผู้ไม่หวังดีที่จะหลอกเอาชื่อผู้ใช้ และรหัสผ่านของการเข้าใช้งานอินเทอร์เน็ตของเหยื่อได้

เนื่องจาก Social Engineering มีเหยื่อเป็นบุคคล การให้ความรู้ความเข้าใจในเรื่อง Social Engineering จึงเป็นสิ่งสำคัญ หากมองในมุมขององค์กรแล้ว นอกจากจะให้ความรู้ความเข้าใจกับพนักงาน ยังควรจะต้องมีการกำหนดนโยบาย และขั้นตอนการปฏิบัติงานที่ชัดเจนเพื่อป้องกัน Social Engineering [20-6] ไม่ว่าจะเป็นการกำหนดขั้นตอนการปฏิบัติงานของแผนกต่าง ๆ เช่น Helpdesk ซึ่งควรจะต้องมีการตรวจสอบข้อมูลของผู้สอบถามก่อนจะให้ข้อมูล การกำหนด Password policy ที่จะกำหนดแนวทางการใช้งานรหัสผ่าน เช่น ห้ามจดบันทึกรหัสผ่าน หรือ ห้ามใช้รหัสผ่านร่วมกับผู้อื่น การกำหนดชั้นความลับของเอกสาร ที่จะทำให้มีการปฏิบัติต่อเอกสารอย่างเหมาะสม ไม่ว่าจะเป็นการเก็บรักษา หรือการทำลายเอกสาร เป็นต้น

สำหรับมุมมอง ในระดับบุคคลนั้น สามารถระวังตนจากผู้ไม่หวังดีได้ โดยอาศัยการเป็นคนช่างสงสัยและมีสติ เมื่อสื่อสารกับคนแปลกหน้าไม่ว่าจะเป็นทางโทรศัพท์ ทางอีเมล หรือพูดคุยกันซึ่งหน้า ที่ต้องการข้อมูลส่วนบุคคล หรือข้อมูลภายในขององค์กร ซึ่งไม่ว่าคนแปลกหน้านั้นจะแสดงตนว่าเป็นบุคคลจากองค์กรใดก็ตาม ก็ควรจะมีการตรวจสอบกับองค์กรนั้นโดยตรงก่อนเสมอ [20-7]

อ้างอิง

[20-1] http://www.etda.or.th/etda_website/mains/display/747
[20-2] http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-manipulating-source_32914
[20-3] http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
[20-4] http://www.etda.or.th/etda_website/mains/display/406
[20-5] http://searchsecurity.techtarget.com/definition/shoulder-surfing
[20-6] http://www.sans.org/reading_room/whitepapers/engineering/social-engineering_1365
[20-7] http://www.us-cert.gov/cas/tips/ST04-014.html

เอกสารเผยแพร่

สำหรับผู้เชี่ยวชาญ

21 SECURE WEB SERVER

ผู้เขียน: ไพชยนต์ วิมุกตะนันทน์
วันที่เผยแพร่: 16 ม.ค. 2555
ปรับปรุงล่าสุด: 16 ม.ค. 2555

ทุกวันนี้การที่ Web server สักเครื่องหนึ่งที่ให้บริการบน Internet จะถูกโจมตีจากผู้ไม่ประสงค์ดีถือเป็นเรื่องปกติธรรมดา จากข้อมูลของ zone-h.org พบว่า เฉพาะการโจมตีประเภท Defacement ที่มีการรายงานมาที่ zone-h.org ในปี 2011 และ 2010 มีถึงเกือบ 1.5 ล้านครั้งในแต่ละปี โดยเพิ่มขึ้นจากปีก่อนหน้า (2009 ลงไป) เกือบ 3 เท่า [21-1] อาจจะดูไม่มากนักเมื่อเทียบกับจำนวน Web site ทั้งหมดที่มีมากกว่า 500 ล้านแห่ง [21-2] ในปี 2011 แต่ต้องอย่าลืมว่า zone-h รายงานเฉพาะการโจมตีประเภท Defacement ที่มีการแจ้งมาโดยตรงเท่านั้น การโจมตีแบบอื่น (ที่อาจร้ายแรงกว่า) หรือการโจมตีที่ไม่ต้องการให้เป็นที่รับรู้ของสาธารณะชน หรือไม่ได้มีการแจ้งมาโดยตรง ก็จะไม่ได้รวมอยู่ใน 1.5 ล้านครั้งนี้ แต่ไม่ว่าจะมากหรือน้อย ผู้ที่อยู่ในแวดวงด้านความมั่นคงปลอดภัย หรือผู้ที่มีหน้าที่ดูแลเครื่องแม่ข่ายทั้งหลาย ก็คงทราบดีกว่า ปัจจุบันการโจมตีเว็บไซต์นั้น พบได้เกือบตลอดเวลา เพียงแค่ดูจาก Log file ของเครื่องแม่ข่ายเว็บ ก็อาจจะพบร่องรอยความพยายามในการโจมตีได้อย่างไม่ยากนัก ทั้งนี้ด้วยความรวดเร็วของการเผยแพร่ข้อมูลเกี่ยวกับช่องโหว่ใหม่ๆ และความสามารถของ Google ในการหาเครื่องแม่ข่ายเว็บที่เป็นเป้าหมายที่มีช่องโหว่นั้น เช่น บริการ “Google Dork” หรือ “Google Hacking Database: GHDB” ทำให้ผู้ดูแลระบบต้องพบกับความยุ่งยากในการ คอยติดตามข่าวสารเรื่องช่องโหว่และหาทางป้องกันเครื่องแม่ข่ายเว็บที่ตนดูแล อยู่มานักต่อนักแล้ว

ส่วนมากจุดอ่อนของเครื่องแม่ข่ายเว็บ นั้นไม่ได้อยู่ที่ระบบปฏิบัติของเครื่องแม่ข่ายหรือซอฟต์แวร์สำหรับให้ บริการเว็บ (Web Server) แต่อยู่ที่เว็บแอพพลิเคชั่น (Web Application) เป็นหลัก หากเว็บไซต์ใดมีข้อมูลเฉพาะ Static Web page หรือ Flat page [21-3] โดยไม่มีไฟล์สคริปต์ PHP, ASP หรือ Dynamic content ใดๆ อยู่เลยก็อาจจะเรียกได้ว่ามีความเสี่ยงน้อยมากที่จะถูกเจาะระบบหรือโจมตีได้ สำเร็จ ซึ่งการพัฒนาเว็บไซต์ที่ใช้งานเฉพาะ Static web page หรือ Flat page แทบจะเป็นไปไม่ได้เลยในยุคที่เว็บไซต์เปรียบเสมือนช่องทางหลักในการทำธุรกิจ หรือแม้แต่การเผยแพร่ข้อมูลโดยทั่วไปก็ยังมีการนำ Web application ประเภท CMS เข้ามาใช้เพื่อความสะดวกในการจัดรูปแบบเนื้อหาและให้ความสะดวกแก่ผู้ใช้บริการ ยิ่งหาก Web application เหล่านี้ซับซ้อนเท่าไหร่ ก็ยิ่งมีโอกาสที่จะพบช่องโหว่มากขึ้นเท่านั้น และเมื่อ

Web application มีช่องโหว่ ก็เท่ากับระบบต่างๆที่ทำงานร่วมกับเว็บไซต์มีช่องโหว่ด้วย ซึ่งอาจจะทำให้เกิดจุดอ่อนกับระบบปฏิบัติการหรือแม้แต่เกิดจุดอ่อนกับ เครื่องแม่ข่ายเครื่องอื่นๆ ที่อยู่บนเครือข่ายเดียวกันได้

คงไม่มีวิธีการใดที่สามารถป้องกันการโจมตีเว็บไซต์ได้อย่างสมบูรณ์ ผู้เชี่ยวชาญมักจะแนะนำให้เลือกใช้ Web application ที่เชื่อถือได้ และมีการ Update สม่ำเสมอ โดยเฉพาะในด้านความมั่นคงปลอดภัย แต่อย่าลืมว่าการ Update เหล่านี้ มักจะเกิดขึ้นหลังจากที่ผู้พัฒนาได้พบจุดอ่อนที่เกิดจากการโจมตีได้สำเร็จอยู่เสมอ หรือถึงแม้จะยังไม่มีการพบช่องโหว่ใน Web application ที่ใช้งานอยู่ก็ตาม ผู้ดูแลระบบก็ควรทราบว่า แม้แต่การ Configuration บางรูปแบบเพื่อตอบสนองความต้องการของ User ก็อาจทำให้เกิดช่องโหว่ขึ้นมาได้เช่นเดียวกัน

ดังนั้นเพื่อรักษาความมั่นคงปลอดภัยของเว็บไซต์ ทางทีมไทยเซิรต์ได้รวบรวมและนำเสนอแนวปฏิบัติในการดูแลเครื่องบริการเว็บ โดยอาศัยหลักการ Security in-depth กับพิจารณาถึงองค์ประกอบแวดล้อมในเครื่องบริการเว็บทั้งหมด โดยไม่เจาะจงลงไปในตัว Web application เพียงอย่างเดียว เพื่อลดโอกาสหรือลดความรุนแรงที่จะเกิดขึ้นเมื่อถูกโจมตี

1. **ระมัดระวังเรื่อง Web server Process privilege** ส่วนมาก Web application จะทำงานภายใต้สิทธิ์ (User ID) ของโพรเซส Web server ให้ลองจินตนาการว่า หาก Web application จะทำอันตรายระบบของเรา ด้วยสิทธิ์ที่เทียบเท่า Web server จะเกิดผลอย่างไรบ้าง ส่วนมากระบบปฏิบัติการรุ่นใหม่ๆ จะไม่ค่อยให้ Web server ทำงานในสิทธิผู้ดูแลระบบ (root หรือ Administrator) แล้ว แต่อาจจะต้องตรวจสอบดูให้แน่ใจอีกครั้งเป็นรายกรณีไป

2. **จำกัดสิทธิในการเขียนไฟล์ของ Web Application** Web Application อาจจำเป็นต้องเขียนไฟล์ลงใน File system บ้าง เช่นในกรณีที่มีการ Upload ข้อมูล หรือเขียน Temp แต่ Web application ไม่จำเป็นต้องเขียนข้อมูลลงในทุกๆ Directory ดังนั้นควรจำกัดสิทธิ์ของ Web application ให้เขียนข้อมูลได้ในที่ๆ จำเป็นต้องเขียนเท่านั้น

3. **แยกโซนอันตราย** พื้นที่หรือ Directory ที่ Web Application ใช้เป็นพื้นที่สำหรับใช้งานชั่วคราว เช่นพื้นที่ Upload ข้อมูลจาก User ให้ถือว่าเป็นพื้นที่อันตราย เนื่องจากเราไม่สามารถรับประกันได้ว่าข้อมูลที่ User ใส่เข้ามาจะเป็น Malicious code หรือไม่ ดังนั้นการป้องกันไม่ให้ Execute หรือ Run ข้อมูลที่อยู่ในพื้นที่อันตรายนี้จึงเป็นสิ่งที่ต้องพิจารณาดำเนินการ

4. **พิจาณาใช้งาน Chroot หรือ Jail (FreeBSD)** ถ้าเป็นไปได้ ควร Chroot หรือ Jail Web server [21-4] เพื่อป้องกันไม่ให้ Web application สามารถเข้าถึงไฟล์อื่นๆบนระบบปฏิบัติการได้โดยอิสระ การใช้ MAC (Mandatory Access Control) หรือ RBAC (Role-Based Access Control) เช่น SELinux [21-5], AppArmor [21-6], Tomoyo [21-7] หรือ Grsecurity [21-8] ก็เป็นอีกทางเลือกที่ผู้ดูแลระบบน่าจะพิจารณาเลือกใช้ได้

5. **ควบคุมการใช้งาน Script** คล้ายกับข้อ 3 แต่เป็นข้อกำหนดในเชิง Web programming คือการกำหนดให้ Script หรือ Web application code สามารถ Run หรือ Execute ใน Directory ที่กำหนดไว้เท่านั้น เพื่อลดความเสี่ยงที่จะโดนโจมตีในโซนพื้นที่อันตรายเช่น พื้นที่สำหรับเก็บรูปภาพที่มีโอกาสถูกอัพโหลดไฟล์ Malicious code จากผู้ไม่ประสงค์ดี ประกอบกับการใช้ช่องโหว่ในการเข้าโจมตีแบบ Remote File Inclusion ที่สั่งให้ Run ไฟล์บน Directory ต่างๆได้ โดยใช้หลักการ Include file

6. **จับตาดู Error message** 404/403 response อาจเป็นเรื่องปกติที่พบได้ทั่วไปใน Log ของ Web server แต่ถ้าพบในจำนวนมาก ในระยะเวลาสั้นๆ อาจแสดงถึงความพยายาม Scan หรือ Probe จากผู้ไม่ประสงค์ดี แต่ในปัจจุบันที่มีการใช้ Botnet กันอย่างกว้างขวาง Request เหล่านี้ อาจจะไม่ได้มาจาก IP เดียวกันก็ได้ จึงจำเป็นต้องระมัดระวังในการพิจารณาเป็นพิเศษ

7. **ควบคุม Web server ในการเรียกข้อมูลภายนอก** Web server ไม่ควรมีความจำเป็นต้องเรียกข้อมูลจาก Internet โดยตรง หากมีความจำเป็นต้องดึงข้อมูลมา Update ควรให้ทำผ่าน Proxy และมีการควบคุม URL ปลายทางอย่างเคร่งครัด และควรมีการ Monitor การเรียกข้อมูลที่นอกเหนือจากที่กำหนดด้วย เพราะอาจแสดงให้เห็นว่าผู้ไม่ประสงค์ดี สามารถควบคุม Web server เอาไว้ได้แล้ว

8. **Privilege ของ Database user ก็สำคัญ** Web application แต่ละตัว ควรใช้ User บน Database ที่แตกต่างกัน เพื่อความสะดวกในการ Audit และแยกสิทธิ์การเขียน/อ่าน ข้อมูลด้วย ถ้า Web application ตัวใดไม่ต้อง Update ข้อมุลใน Database อย่าให้ User ของ Web application นั้นมีสิทธิ์เขียนข้อมูลเด็ดขาด และควรจำกัดสิทธิ์การในระดับ Table ด้วยถ้าเป็นไปได้ วิธีการนี้จะช่วยลดความรุนแรงของการโจมตีประเภท SQLi (SQL Injection) ได้

9. **พิจารณา Data type ของ Web application parameter** การพัฒนา Web application ที่ดี ควรจำกัดและตรวจสอบชนิดของข้อมูลที่รับส่งกับ User ทุกครั้ง เช่นถ้าข้อมูลที่จะรับเข้ามาเป็น ID ของบทความ ก็ไม่ควรยอมให้มีข้อมูลอื่นนอกจาก Digit เข้ามาใน Parameter นั้น หรือถ้าเป็น Alpha-numeric ก็ไม่ควรให้มีสัญลักษณ์เข้ามาปะปน เป็นต้น

10. **จับตาดูการเปลี่ยนแปลง** เครื่องมือสำหรับตรวจสอบการเปลี่ยนแปลงของไฟล์อย่าง Tripwire หรือ AIDE เป็นเครื่องมือที่ดีที่จะใช้บอกว่ามีสิ่งไม่ชอบมาพากลขึ้นใน Web server เพราะบางครั้ง ผู้ไม่ประสงค์ดีจะทิ้งโปรแกรมประเภท Backdoor ไว้เพื่อให้สะดวกในการควบคุม Web server หรืออาจเป็นการติดตั้งโปรแกรมประเภท Trojan หรือ Bot ก็ได้ แต่ควรใช้อย่างระมัดระวัง เพราะการเปลี่ยนแปลงของไฟล์ในระบบบางอย่าง อาจไม่ได้หมายถึงสิ่งผิดปกติก็ได้ เช่น Log หรือ Temp ที่มีการเปลี่ยนแปลงอยู่เป็นปกติอยู่แล้ว

11. **ถือว่าข้อมูลจาก Client เป็น Untrusted** Script อะไรก็ตามที่ทำงานในฝั่ง Client เช่น Javascript หรือแม้แต่ Flash หรือ Java ทั้งหลายเหล่านี้อาจจะถูก Compromise ได้ไม่ยาก เพราะฉะนั้น Web application ที่ดีไม่ควรใช้วิธีการตรวจสอบการส่งข้อมูลโดยวิธีการเหล่านี้เป็นอันขาด เช่น การใช้

Javascript ตรวจสอบข้อมูลที่ User ป้อนเข้ามา เพราะผู้ไม่ประสงค์ดีสามารถ Bypass การตรวจสอบนี้ได้อย่างง่ายดายจากโปรแกรมทั่วไป เช่น NoScript [21-9] หรือแม้แต่สิ่งที่รับมาจาก Client เช่นค่าจากตัวแปรต่างๆ ก็ควรสงสัยไว้ก่อนว่ามีโอกาสเป็นข้อมูลไม่พึงประสงค์ได้

12. **ควรเลือกใช้เครื่องมือที่ชำนาญ** การเลือกใช้เครื่องมือต่างๆ เช่น Web server, Web application platform หรือ CMS ควรเลือกที่ความคุ้นเคยมากกว่าความสวยงามหรือทันสมัย เพราะเวลามีปัญหาจะสามารถเข้าตรวจสอบและแก้ไขได้ง่าย และอย่าลืมว่าเครื่องมือที่ดีกว่าหรือใหม่กว่า ไม่ได้แปลว่าจะไม่มีโอกาสเกิดปัญหาเลย หรือในอีกมุมหนึ่งการใช้งานเครื่องมือที่พัฒนาขึ้นใหม่อาจเหมือนเป็นหนูทดลองสำหรับการทดสอบผลิตภัณฑ์ก็เป็นได้ ซึ่งจะก่อให้เกิดปัญหาด้านความมั่นคงปลอดภัยตามมา

13. **พยายามทำตามมาตรฐาน** การเข้ารหัสแบบคิดค้นเอง การจัดการ Session แบบไม่มีมาตรฐาน หรือแม้แต่การพัฒนา Web application ในรูปแบบแปลกๆ มักจะเกิดปัญหาได้ง่ายกว่าแบบเดิมที่นิยมใช้กัน หลายคนเชื่ออย่างผิดๆ ว่าการใช้สิ่งที่คนทั่วไปใช้กัน หรือการใช้ Opensource/Open Standard ที่เปิดโอกาสให้คนเห็น Source code หรือ Algorithm อย่างเปิดเผยนั้นไม่มีความมั่นคงปลอดภัย แต่ก็ต้องอย่าลืมว่า โปรแกรมเข้ารหัสที่ยอมรับกันว่าปลอดภัยที่สุดในขณะนี้ก็เป็น Open standard อยู่ เช่น OpenSSL [21-10]

14. **ไม่ควรแสดง Error message ให้ User เห็น** ข้อผิดพลาดของ Web application (Error message) ที่แสดงให้คนอื่นเห็นโดยไม่ตั้งใจ ถือเป็นเรื่องที่รับไม่ได้และน่าอับอายสำหรับคนพัฒนา Web application เพราะแสดงให้ถึงความไม่เป็น Professional ซ้ำร้ายยังกลายเป็นผู้สนับสนุนข้อมูลในการเข้าโจมตีเว็บไซต์จากข้อมูลที่แสดงออกไปอีกด้วย เช่น ข้อผิดพลาดแสดงที่อยู่ของไฟล์ในระบบ หรือชื่อของ Database เป็นต้น เพราะฉะนั้น Web application ที่ดี ต้องไม่แสดง Error message ออกมาให้เห็นเมื่อเกิดความผิดพลาด ซึ่งการจัดการ Exception ที่ดีในถือเป็นอีกวิธีหนึ่งที่จะลดปัญหาข้อนี้

15. **จับดาการ Re-attempt** โดยปกติคนที่ลืม Password ย่อมไม่อดทนใส่ Password ที่ผิดเป็นสิบๆ ครั้งต่อเนื่อง เช่นเดียวกับคงไม่มีใครส่งค่า Parameter ตัวเดียวไปเรื่อยๆ อย่างต่อเนื่องเช่นกัน การ Re-attempt ในลักษณะนี้ อาจเกิดจากเครื่องมือพิเศษที่ใช้หาช่องโหว่ของระบบ (Brute Force) หรือเครื่องมือเดา Password มากกว่า

16. **Web application ตัวอื่นก็สำคัญ** Web application ที่เขียนขึ้นอย่างดี มีความมั่นคงปลอดภัยสูง แต่เมื่อไปอยู่ร่วมกับ Web application ที่มีช่องโหว่ บน Web server ตัวเดียวกัน ย่อมมีความเสี่ยงที่เกิดขึ้นเทียบเท่ากัน เว้นแต่ Web server จะมีการแยก Privilege ระหว่าง Web application แต่ละตัวได้ เช่น การใช้ suEXEC [21-11]

อ้างอิง

[21-1] http://www.zone-h.org/stats/ymd

[21-2] http://news.netcraft.com/archives/2011/12/09/december-2011-web-server-survey.html

[21-3] http://en.wikipedia.org/wiki/Static_web_page

[21-4] http://en.wikipedia.org/wiki/Chroot

[21-5] http://selinuxproject.org/page/Main_Page

[21-6] http://wiki.apparmor.net/index.php/Main_Page

[21-7] http://tomoyo.sourceforge.jp

[21-8] http://grsecurity.net/index.php

[21-9] https://addons.mozilla.org/en-US/firefox/addon/noscript

[21-10] http://www.openssl.org

[21-11] http://httpd.apache.org/docs/2.0/suexec.html

22 SECURE WEBSITE ด้วยการตรวจสอบข้อมูลที่ติดต่อกับผู้ใช้งาน (INPUT/OUTPUT VALIDATION)

ผู้เขียน: พรพรหม ประภากิตติกุล
วันที่เผยแพร่: 16 ม.ค. 2555
ปรับปรุงล่าสุด: 16 ม.ค. 2555

ปัญหาด้านความมั่นคงปลอดภัยของเว็บไซต์ในปัจจุบัน ถูกเผยแพร่ผ่านบทความและเว็บไซต์บนโลกอินเทอร์เน็ตนับครั้งไม่ถ้วน ด้วยการโจมตีแบบเดิมๆ ที่ยังคงได้ผลมาจนถึงทุกวันนี้ไม่ใช่เพราะเทคโนโลยีที่ ทันสมัยขึ้น แต่เป็นเพราะการพัฒนาเว็บไซต์ที่ไม่มีประสิทธิภาพมากกว่า ยกตัวอย่างในกรณีข่าวที่เกิดขึ้นเมื่อไม่นานมานี้เรื่อง “One million pages infected by Lilupophilupop SQL injection” [22-1][22-2] ซึ่งจากการตรวจสอบของไทยเซิร์ตพบว่ามีเว็บไซต์ภายใต้การจดทะเบียนโดเมนเนมใน ประเทศไทย (.th) ได้รับผลกระทบจากกรณีดังกล่าวไม่น้อยกว่า 1 หมื่นเว็บไซต์ และจากข้อมูลที่ได้จากเว็บไซต์ SANS [22-3] พบว่าการโจมตีดังกล่าวเป็นการใช้เทคนิค SQL Injection [22-4][22-5] ซึ่งเป็นเทคนิคดั้งเดิมที่ใช้ในการโจมตีเว็บไซต์ต่างๆ มานานแล้ว แต่ก็ยังคงใช้ได้ผลอยู่กับเว็บไซต์จำนวนมาก สาเหตุหลักๆ ที่วิเคราะห์ได้คือเว็บไซต์จำนวนมากที่ไม่มีการรักษาความมั่นคงปลอดภัยที่ดีพอและไม่มีการตรวจสอบข้อมูลที่ติดต่อกับผู้ใช้งาน จึงทำให้ผู้โจมตีสามารถส่งค่าอันตรายเข้าไปยังเว็บไซต์ได้อย่างง่ายดาย บทความนี้จะอธิบายถึงแนวทางการตรวจสอบข้อมูลที่ติดต่อกับผู้ใช้งานหรือที่ เรียกว่า Input / Output Validation ซึ่งเป็นกระบวนการที่มีความสำคัญมากต่อการรักษาความมั่นคงปลอดภัยของ เว็บไซต์และการป้องกันการโจมตีด้วยเทคนิค SQL Injection XSS [22-6][22-7] โดยหวังว่าจะช่วยให้เกิดการพัฒนาเว็บไซต์ที่มีความมั่นคงปลอดภัยมากยิ่งขึ้นและช่วยลดสถิติของประเทศไทยในการการถูกโจมตีจากช่องโหว่ดังกล่าวสำเร็จ

Input / Output Validation คืออะไร

Input Validation เป็นการตรวจสอบข้อมูลที่ส่งมาจากผู้ใช้งาน ซึ่งข้อมูลดังกล่าวอาจอยู่ในรูปที่ผู้ใช้งานเห็นโดยตรง เช่น การลงทะเบียนสมัครเป็นสมาชิกเว็บไซต์ หรือเป็นการส่งข้อมูลในตัวแปรแบบซ่อนในเว็บไซต์ที่มีเนื้อหาแบบไดนามิก [22-8] โดยการตรวจสอบข้อมูลจากผู้ใช้งานสามารถเกิดขึ้นได้ที่ฝั่งผู้ใช้งานโดยตรง เช่น ใช้วิธีการตรวจสอบข้อมูลที่ส่งมาจากผู้ใช้งานด้วยภาษาจาวาสคริปต์ (Javascript) ที่ทำงานในฝั่งผู้ใช้งาน แต่ก็ยังพบว่าไม่สามารถช่วยป้องกันการโจมตีได้เท่าที่ควรเนื่องจากผู้โจมตี สามารถหลบเลี่ยงการตรวจสอบข้อมูลด้วยวิธีการดังกล่าวได้โดยไม่ยาก หรือใช้วิธีการตรวจสอบข้อมูลผู้ใช้งานที่ทำงานในฝั่งของเว็บไซต์ เพื่อให้แน่ใจว่าค่าที่ได้มีความถูกต้องก่อนส่งเข้าไปประมวลผลในฟังก์ชั่น หลักของเว็บไซต์ ซึ่งวิธีการนี้จะช่วยลดความเสี่ยงในการถูกเปลี่ยนแปลงฟังก์ชั่นการตรวจสอบ ข้อมูลได้ดีที่สุด เนื่องจากเป็นซอร์สโค้ดที่ถูกฝังอยู่ในฝั่งเว็บไซต์

Output Validation เป็นการตรวจสอบข้อมูลจากการประมวลผลของเว็บไซต์ก่อนจะนำออกมาแสดงผลในฝั่งผู้ใช้งาน ซึ่งการตรวจสอบข้อมูลดังกล่าวมีความสำคัญไม่แพ้การทำ Input validation โดยจุดประสงค์หลักคือเพื่อป้องกันการแสดงผลข้อมูลที่ไม่เหมาะสม เช่น ข้อมูลบัตรเครดิตในเว็บไซต์ที่มีการลงทะเบียนชำระเงินควรจะต้องมีการป้องกัน การมองเห็นข้อมูลทั้งหมดโดยใส่สัญลักษณ์ที่บอกว่าเป็นการซ่อนข้อมูลบางอย่าง เช่น สัญลักษณ์ Asterisk (*) [22-9] ข้อความแสดงความผิดพลาดต่างๆ (Error message) ซึ่งอาจจะเป็นข้อมูลที่เป็นประโยชน์แก่ผู้ไม่ประสงค์ดีในการวางแผนโจมตีเว็บไซต์ต่อไป หรือ แม้แต่การแสดงผลเนื้อหาในลักษณะที่อาจมีส่วนประกอบของสคริปต์อันตรายที่ส่งผลกับผู้ใช้งานบนเว็บไซต์ ซึ่งในกรณีนี้เว็บไซต์ที่ดีควรจะต้องมีการแปลงสัญลักษณ์พิเศษบางอย่างเพื่อ ไม่ให้เนื้อหาที่แอบแฝงด้วยสคริปต์อันตรายสามารถทำงานได้โดยอัตโนมัติใน เว็บเบราว์เซอร์ของผู้ใช้งาน

ทำไมจึงต้องทำ Input / Output Validation

ในทุกเว็บไซต์มีโอกาสในการถูกโจมตีได้เท่าเทียมกันทั้งนั้น หากผู้ดูแลเว็บไซต์ลองตรวจสอบข้อมูลล็อกไฟล์ (Logfile) ของการเรียกใช้งานเว็บไซต์ ก็อาจพบว่ามีการพยายามเรียกหน้าเว็บไซต์อย่างผิดปกติซ้ำๆ ในระยะเวลาไล่เรี่ยกัน นั่นเป็นเพราะผู้โจมตีส่วนใหญ่จะใช้วิธีการสุ่มเรียกเว็บไซต์โดยการพยายามส่งค่าอันตรายต่างๆ ทั้งที่ส่งค่าเป็นรายครั้งเพื่อทดสอบสมมติฐานบางอย่างที่ใช้ในการโจมตี หรือพัฒนาเป็นโปรแกรมอัตโนมัติเพื่อโจมตีเว็บไซต์ ซึ่งแท้จริงแล้วการทำ Input / Output Validation ไม่ได้เป็นอะไรที่ใหม่ เพียงแต่ผู้พัฒนาเว็บไซต์เองอาจไม่เคยสนใจหรือใส่ใจต่อการรักษาความมั่นคงปลอดภัยของเว็บไซต์เพียงพอหรือในบางรายอาจคิดว่าไม่จำเป็นต้องทำ แต่ถ้าลองพิจารณาถึงแนวโน้มและผลกระทบที่เกิดขึ้นจากการถูกโจมตีสำเร็จแล้ว นั้นคงทำให้ผู้พัฒนาเว็บไซต์ต้องกลับมาคิดเสียใหม่ เนื่องจากปัจจุบันคงเป็นเรื่องที่หลีกเลี่ยงยากในการพัฒนาเว็บไซต์ต่อเทรนด์ของเว็บไซต์สมัยใหม่ที่ต้องการให้ผู้ใช้งานสามารถโต้ตอบกับเว็บไซต์ได้อย่างเสรี อย่างเช่นในเว็บไซต์ Facebook และในบางครั้งอาจจำเป็นต้องมีการซื้อขายทำธุรกรรมออนไลน์ซึ่งหากเว็บไซต์ไม่ ได้มีกระบวนการป้องกันที่ดีก็คงยากที่จะทำให้เว็บไซต์ปลอดภัยจากการโจมตีและ อาจเป็นผลให้เว็บไซต์หมดความน่าเชื่อถือไปในที่สุด

ปัญหาของการทำ Input / Output Validation

ผู้พัฒนาเว็บไซต์ไม่มีความตระหนักถึงความมั่นคงปลอดภัยของเว็บไซต์ ทำให้ไม่มีการวางแผนหรือการคาดการณ์ในเรื่องของการป้องกันการโจมตีในรูปแบบต่างๆ

ผู้พัฒนาเว็บไซต์ไม่มีความรู้และความเข้าใจถึงการทำ Input / Output Validation อย่างถูกต้อง ส่งผลทำให้เว็บไซต์ยังคงมีช่องโหว่ในการโจมตี

ผู้พัฒนาเว็บไซต์ไม่ต้องการปรับปรุงเว็บไซต์เพื่อการทำ Input / Output Validation เนื่องจากทำให้เกิดความยุ่งยากในการตรวจสอบข้อมูลที่ส่งมาจากผู้ใช้งานซึ่ง มีอยู่เป็นจำนวนมาก

ในบางเว็บไซต์ที่เป็นการจ้างพัฒนาจากบริษัทภายนอก การทำ Input / Output Validation หรือปรับปรุงเว็บไซต์จะทำให้มีค่าใช้จ่ายเพิ่มเติม ส่งผลทำให้อาจไม่ได้รับการดูแลหรือส่งเสริม

ผู้พัฒนาเว็บไซต์ใช้ซอร์ฟแวร์บริหารจัดการเว็บไซต์เนื้อหาบนเว็บไซต์ (CMS) ซึ่งอาจไม่มีโมดูลการทำ Input / Output Validation ส่งผลให้เว็บไซต์มีความเสี่ยงต่อการถูกโจมตี

ข้อแนะนำในการทำ Input / Output Validation

ไทยเซิร์ตได้รวบรวมข้อมูลข้อแนะนำในการทำ Input / Output Validation โดยข้อมูลส่วนใหญ่เป็นข้อมูลที่รวบรวมมาจากเว็บไซต์ของ OWASP [22-10] ซึ่งเป็นเว็บไซต์ที่ให้ข้อมูลเกี่ยวกับการพัฒนาเว็บไซต์ให้มีความมั่นคงปลอดภัยตามข้อมูลดังต่อไปนี้

1. **อย่ากลัวการเปลี่ยน**แปลง ในเว็บไซต์ที่มีการพัฒนาขึ้นแล้วและมีความคิดที่จะปรับปรุงเว็บไซต์ให้มีกระบวนการตรวจสอบข้อมูลที่ติดต่อกับผู้ใช้งาน นับว่าเป็นความคิดที่มาถูกทางแล้วในการป้องกันไม่ให้เกิดความเสียหายต่อเว็บไซต์ เพียงแต่การเปลี่ยนแปลงที่กล่าวอาจมีการวางแผนที่ดี และอาศัยความละเอียดรอบคอบในการดำเนินการ ซึ่งจะช่วยลดเวลาและความผิดพลาดที่เกิดขึ้นได้

2. **ไม่ควรใช้จาว**าสคริปต์ซึ่งทำงานในฝั่งผู้ใช้งานเป็นองค์ประกอบหลักในการตรวจสอบข้อมูลที่ส่งมาจากผู้ใช้งาน โดยหากมีการใช้งานจาวาสคริปต์ในกรณีดังกล่าว ควรต้องมีการตรวจสอบร่วมกับซอร์สโค้ดที่มีการประมวลผลในฝั่งเว็บไซต์ด้วย เพื่อป้องกันการเปลี่ยนแปลงกระบวนการตรวจสอบข้อมูลในฝั่งผู้ใช้งาน

3. การทำ Input / Output Validation จะต้องทำในทุกๆส่วนที่มีการติดต่อกับผู้ใช้งานบน**เว็บไซต์** ต้องไม่สุ่มทำเพียงส่วนใดส่วนหนึ่ง เพราะหากยกเว้นหรือลืมการตรวจสอบไม่ว่าจะส่วนใดก็ตาม นั่นหมายถึงการเปิดโอกาสให้ผู้โจมตีสามารถมีโอกาสโจมตีเว็บไซต์ได้สำเร็จ

4. **ควรมีการกำหนดขอบเขตของตัวแปรและประเภทของตัวแปรที่ใช้ในเว็บไซต์ทั้งหมด** เช่นตัวแปร A เป็นข้อมูลประเภท Text ตัวแปร B เป็นข้อมูลประเภท Number เพื่อใช้เป็นข้อมูลตั้งต้นสำหรับการพัฒนาฟังก์ชั่นการตรวจสอบข้อมูลจากผู้ใช้งาน โดยฟังก์ชั่นที่พัฒนาขึ้นจะต้องไม่ประมวลผลตัวแปรที่ไม่อยู่ในขอบเขตที่กำหนดไว้

5. **ควรมีการกำหนดและตรวจสอบรูปแบบของข้อมูลที่อนุญาติ (Whitelist) และข้อมูลที่ไม่อนุญาติ (Blacklist) ให้ประมวลผลบนเว็บไซต์** โดยอ้างอิงจากข้อมูลในแต่ละตัวแปรว่ามีจุดประสงค์จะให้ใส่ข้อมูลใดบ้าง เช่น ข้อมูลอีเมล ควรจะมีการตรวจสอบรูปแบบของข้อมูลเฉพาะที่แสดงให้รู้ว่าข้อมูลที่ส่งมาจาก ผู้ใช้งานเป็นรูปแบบของอีเมลจริง เพื่อไม่ให้เกิดข้อผิดพลาดในการรับค่าผิดรูปแบบเข้ามาประมวลผลในเว็บไซต์ หรือกรณีที่ตัวแปรมีขอบเขตหรือรูปแบบการรับค่าจากผู้ใช้งานที่เปิดกว้างไม่ มีรูปแบบที่แน่นอน เช่น ข้อมูลจากหน้ากระดานสนทนา ซึ่งเปิดให้รับข้อมูลแบบอิสระและมีความสุ่มเสี่ยงที่ผู้โจมตีจะส่งค่า อันตรายเข้ามาโจมตียังเว็บไซต์ เพราะฉะนั้นควรมีการพิจารณาค่าบางประเภท เช่น “<script>” โดยไม่ควรให้สามารถส่งค่าเข้ามาประมวลผลยังเว็บไซต์ได้

6. ควรมีการกำหนดและตรวจสอบความยาวของข้อมูลในแต่ละตัวแปร เพื่อตรวจสอบความผิดปกติในการส่งค่าจากผู้ใช้งานเข้ามาประมวลผลยังเว็บไซต์ เนื่องจากการส่งค่าอันตรายในบางครั้งจำเป็นต้องพิมพ์จำนวนมาก

7. ควรมีการพัฒนาฟังก์ชั่นการเข้ารหัสข้อมูลหรือที่เรียกว่า Encoding เพื่อใช้งานควบคู่ไปกับการตรวจสอบข้อมูลที่ส่งมาจากผู้ใช้งาน โดยจะช่วยลดความเสี่ยงที่ผู้โจมตีจะโจมตีโดยการแอบส่งค่าที่เป็นสคริปต์ อันตรายเข้ามาประมวลผลยังเว็บไซต์ได้สำเร็จ

8. ในกรณีที่เว็บไซต์มีฟังก์ชั่นการอัพโหลดไฟล์ ควรมีการกำหนดและตรวจสอบประเภทของไฟล์ที่อนุญาติให้สามารถอัพโหลดเข้าไปประมวลผลยังเว็บไซต์ได้ ซึ่งสามารถตรวจสอบจากนามสกุลบนชื่อไฟล์ร่วมกับข้อมูลที่เว็บไซต์แสดงจากรายละเอียดของไฟล์ หรือในบางครั้งอาจจำเป็นต้องใช้งานฟังก์ชั่นหรือไลบรารี่เสริมในการตรวจสอบ ประเภทของไฟล์ เพื่อช่วยยืนยันความถูกต้องอีกครั้งหนึ่ง เช่น ฟังก์ชั่น fileinfo [22-11] ในภาษา PHP โดยจะช่วยลดความเสี่ยงที่ผู้โจมตีจะอัพโหลดไฟล์สคริปต์อันตราย เช่น Web shell [22-12][22-13] ขึ้นไปประมวลผลยังเว็บไซต์ได้สำเร็จ

9. ควรใช้งานกลไกการป้องกันการโจมตีจากโปรแกรมอัตโนมัติหรือบอทที่พยายามสุ่มค่าอันตรายมายังเว็บไซต์ โดยตัวอย่างของกลไลที่ได้รับความนิยมในปัจจุบัน เช่น Captcha [22-14] ถูกออกแบบมาเพื่อใช้ยืนยันว่าข้อมูลที่ถูกส่งมาเป็นข้อมูลจากผู้ใช้งานที่เป็นมนุษย์

10. ควรปิดการแสดงผลข้อมูลข้อผิดพลาดของเว็บไซต์ (Error Message) ในทุกๆกรณี เช่น การแสดงข้อผิดพลาดของเว็บไซต์ที่บ่งบอกว่าไม่สามารถเชื่อมต่อฐานข้อมูลได้ โดยการปิดการแสดงผลดังกล่าวเพื่อลดโอกาสที่จะทำให้ผู้ไม่หวังดีสามารถนำข้อมูลดังกล่าวไปใช้วางแผนโจมตี เว็บไซต์ต่อไปได้

11. ควรเลือกใช้ข้อความแสดงความผิดพลาดของการกรอกข้อมูลที่เป็นกลาง ยกตัวอย่างกรณีของการกรอกแบบฟอร์มล็อกอินเข้าสู่ระบบ ซึ่งผู้ใช้งานได้ส่งค่า username ที่ผิดพลาด ไปยังเว็บไซต์ จากนั้นเว็บไซต์ได้แสดงผลลัพธ์ของการล็อกอินว่า “ไม่พบ username นี้ในฐานข้อมูลเว็บไซต์” ซึ่งจากกรณี

ดังกล่าวถือเป็นการแสดงผลลัพธ์ที่ไม่เหมาะสม เนื่องจากมีโอกาสเสี่ยงสูงที่ทำให้ผู้ไม่หวังดีสามารถตีความจากผลลัพธ์ได้ โดยตรง และทำให้ผู้โจมตีสามารถวางแผนการโจมตีเว็บไซต์ได้อย่างง่ายดาย โดยข้อแนะนำสำหรับกรณีดังกล่าวควรจะต้องแจ้งว่า “username หรือ password ของท่านผิดพลาด”

12. ใช้ไลบรารี่ภายนอกที่มีความสามารถในการตรวจสอบข้อมูลที่ติดต่อกับจากผู้ใช้งาน ซึ่งจะช่วยลดเวลาและความผิดพลาดในการพัฒนาฟังก์ชั่นการตรวจสอบข้อมูลด้วยตนเอง โดยมีไลบรารี่ตัวอย่างที่ชื่อว่า ESAPI จากเว็บไซต์ OWASP ซึ่งมีข้อดีที่สนับสนุนการทำงานในหลากหลายภาษาเช่น PHP ASP.NET JAVA PYTHON และผู้ใช้งานสามารถศึกษาวิธีการใช้งานจากเว็บไซต์ผู้พัฒนาได้โดยตรง [22-15]

อ้างอิง

[22-1] http://thehackernews.com/2012/01/one-million-pages-infected-by.html
[22-2] http://isc.sans.org/diary/Lilupophilupop+tops+1million+infected+pages/12304
[22-3] http://www.sans.org/
[22-4] http://www.unixwiz.net/techtips/sql-injection.html
[22-5] https://www.owasp.org/index.php/SQL_Injection
[22-6] http://www.acunetix.com/websitesecurity/xss.htm
[22-7] https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
[22-8] http://en.wikipedia.org/wiki/Dynamic_web_page
[22-9] https://www.owasp.org/index.php/Output_Validation
[22-10] http://www.owasp.com/index.php/Data_Validation
[22-11] http://php.net/manual/en/book.fileinfo.php
[22-12] http://www.thisislegal.com/tutorials/2
[22-13] http://www.madirish.net/node/271
[22-14] http://www.captcha.net/
[22-15] https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

23 รู้ทันและป้องกัน MALWARE ในระบบปฏิบัติการ ANDROID

ผู้เขียน: เสฏฐวุฒิ แสนนาม

วันที่เผยแพร่: ๒๔ ม.ค. ๒๕๕๕
ปรับปรุงล่าสุด: ๒๔ ม.ค. ๒๕๕๕

ในยุคแห่งการติดต่อสื่อสาร คงไม่อาจปฏิเสธได้ว่าการใช้งานโทรศัพท์มือถือนั้นเป็นสิ่งจำเป็น เนื่องจากความก้าวหน้าทางเทคโนโลยี ทำให้ระบบปฏิบัติการในโทรศัพท์มือถือนั้นสามารถทำงานหลายอย่างได้เทียบเท่า กับคอมพิวเตอร์ทั่วไป โดยเฉพาะโทรศัพท์มือถือ Smartphone [23-1] นั้น นอกจากจะใช้เป็นโทรศัพท์ได้แล้วยังสามารถติดตั้งโปรแกรมเพิ่มเติมเพื่อให้ สามารถทำงานในส่วนอื่นๆ ได้อีกด้วย เช่น เชื่อมต่อกับเครือข่ายสังคมออนไลน์ หรือทำธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น แต่การอนุญาตให้ผู้ใช้ติดตั้งโปรแกรมเพิ่มเติมได้ ก็เป็นการเปิดโอกาสให้ผู้ไม่หวังดีพัฒนาโปรแกรมไม่พึงประสงค์ (Malware) เพื่อเข้ามาโจมตีโทรศัพท์มือถือของผู้ใช้ได้เช่นกัน

ระบบปฏิบัติการ ในโทรศัพท์มือถือในปัจจุบันมีอยู่หลากหลาย ไม่ว่าจะเป็น Apple iOS, Microsoft Windows Phone, BlackBerry OS, Symbian หรือ Android แต่ระบบปฏิบัติการที่ได้รับความนิยมสูงสุดและมีส่วนแบ่งในตลาดมากที่สุดใน ปัจจุบันนี้คือ Android จากข้อมูลของ Gartner ซึ่งเป็นบริษัทที่วิจัยเกี่ยวกับเทคโนโลยี พบว่าในเดือนพฤศจิกายน พ.ศ. 2554 ระบบปฏิบัติการ Android มีส่วนแบ่งในตลาดถึง 52.5% [23-2] นั่นเท่ากับว่า ครึ่งหนึ่งของผู้ใช้โทรศัพท์มือถือทั่วโลกใช้ระบบปฏิบัติการ Android

ในปัจจุบันระบบปฏิบัติการ Android ถูกพัฒนาโดย Google โดยมีพื้นฐานมาจากระบบปฏิบัติการ Linux [23-3] Android ออกเวอร์ชัน 1.0 ในปี พ.ศ. 2551 ปัจจุบันพัฒนามาถึงเวอร์ชัน 4.0 ซึ่งมีชื่อทางการว่า Ice Cream Sandwich [23-4] ในตอนแรกนั้นระบบปฏิบัติการ Android ถูกพัฒนามาเพื่อใช้ในโทรศัพท์มือถือเพียงอย่างเดียว จนกระทั่งเวอร์ชัน 3.0 หรือที่มีชื่อทางการว่า Honeycomb ได้ถูกพัฒนาให้ใช้งานได้กับแท็บเล็ต (Tablet) ด้วย เนื่องจาก Google แจกจ่ายระบบปฏิบัติการ Android ในรูปแบบของโอเพนซอร์ส (Open Source) ทำให้ผู้ผลิตสามารถนำระบบปฏิบัติการ Android ไปพัฒนาลงในอุปกรณ์ของตนเอง เช่น โทรศัพท์มือถือ หรือ แท็บเล็ต ได้โดยไม่เสียค่าใช้จ่าย ดังนั้นเราจึงพบการใช้งานอุปกรณ์ที่มีการติดตั้งระบบปฏิบัติการ Android อยู่เป็นจำนวนมาก โดยมีราคาแตกต่างกันไปตามคุณสมบัติของตัวอุปกรณ์

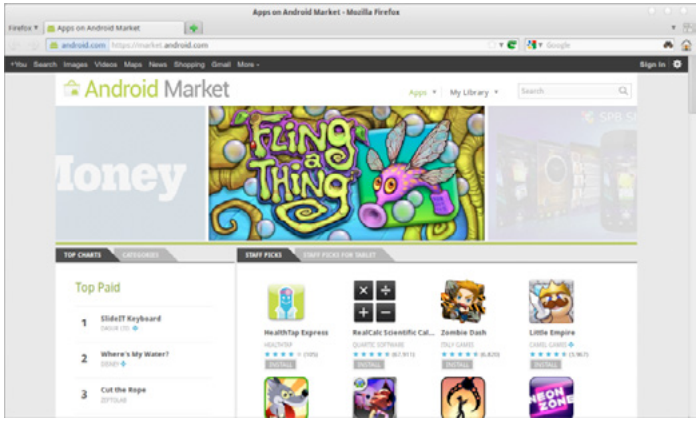
เนื่องจากความนิยมของระบบปฏิบัติการ Android จึงมีผู้พัฒนา Malware ออกมาเผยแพร่เป็นจำนวนมาก จากแต่ก่อนที่มีการเผยแพร่ผ่านไฟล์ .apk (ไฟล์สำหรับติดตั้งโปรแกรมของ Android) เพียงอย่างเดียว แต่ในปัจจุบันนี้พบว่า ใน Android Market ที่เป็นรูปแบบหลักในการเผยแพร่โปรแกรมของระบบปฏิบัติการ Android ซึ่งดูแลโดย Google นั้นพบว่าไม่มีการตรวจสอบโปรแกรมที่ผู้พัฒนาส่งเข้ามา ทำให้มีการส่ง Malware เข้ามาใน Android Market อยู่บ่อยครั้ง [23-5] และจากข้อมูลของ Juniper Networks Global Threat Center พบว่า ตั้งแต่เดือนกรกฎาคมถึงเดือนพฤศจิกายน 2554 อัตราการเพิ่มขึ้นของ Malware ในระบบปฏิบัติการ Android มีถึง 472% [23-6] จากความเสี่ยงดังกล่าว ผู้ใช้อุปกรณ์ที่ติดตั้งระบบปฏิบัติการ Android จึงควรศึกษาวิธีการติดตั้งโปรแกรมและปรับการใช้งานให้เหมาะสม เพื่อเป็นการป้องกัน Malware ไม่ให้ติดโทรศัพท์มือถือหรือแท็บเล็ตของตนเอง

การติดตั้งโปรแกรมในระบบปฏิบัติการ Android

โดยปกติแล้ว การติดตั้งโปรแกรมในระบบปฏิบัติการ Android สามารถทำได้ 2 ทาง คือ ติดตั้งจาก Android Market และดาวน์โหลดไฟล์ .apk มาติดตั้งเอง ซึ่งแต่ละแบบมีวิธีการดังนี้

ติดตั้งจาก Android Market

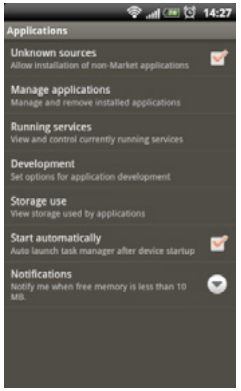
Android Market คือศูนย์รวมโปรแกรมของระบบปฏิบัติการ Android ที่ Google เปิดให้ผู้ใช้สามารถเข้ามาค้นหาและดาวน์โหลดโปรแกรมที่มาจากผู้พัฒนาภายนอกได้ผ่านทางเว็บไซต์ https://market.android.com/ หรือเข้าจากโปรแกรม Market ในโทรศัพท์มือถือ หากผู้ใช้ต้องการติดตั้งโปรแกรมใดๆ ก็สามารถคลิกที่ปุ่ม Install หรือ Purchase ที่อยู่ใต้ชื่อของโปรแกรมนั้นๆ หลังจากเลือกอุปกรณ์ที่ต้องการติดตั้งโปรแกรมแล้ว หากผู้ใช้เชื่อมต่ออุปกรณ์ดังกล่าวเข้ากับอินเทอร์เน็ต โปรแกรมที่เลือกก็จะถูกดาวน์โหลดและติดตั้งลงในอุปกรณ์ดังกล่าวให้โดยอัตโนมัติ ตัวอย่างหน้าจอเว็บไซต์ Android Market เป็นดังรูปที่ 116 (23-1)



รูปที่ 116 (23-1) เว็บไซต์ Android Market

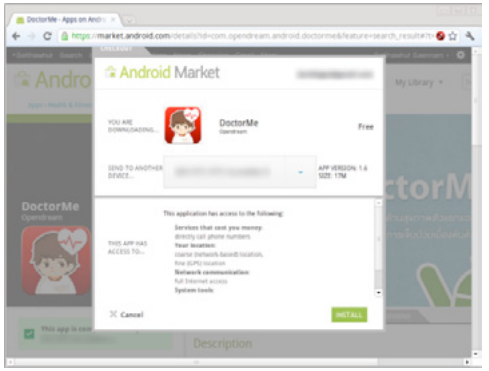
ติดตั้งจากไฟล์ .apk

ไฟล์ .apk เป็นไฟล์ที่ใช้สำหรับติดตั้งโปรแกรมของระบบปฏิบัติการ Android ซึ่งผู้ใช้อาจดาวน์โหลดมาจากเว็บไซต์ของผู้พัฒนาโปรแกรมเอง หรือดาวน์โหลดมาจากเว็บไซต์ที่แจกโปรแกรมละเมิดลิขสิทธิ์ โดยปกติแล้วระบบปฏิบัติการ Android จะรองรับการติดตั้งโปรแกรมอื่นๆ ที่ไม่ได้อยู่ใน Android Market ได้ โดยผู้ใช้ต้องมากำหนดค่าจากเมนู Setting เลือก Applications แล้วเลือก Unknown sources เพื่อยอมรับการติดตั้งโปรแกรมที่ไม่รู้แหล่งที่มา ดังรูปที่ 117 (23-2)



รูปที่ 117 (23-2) การยอมรับการติดตั้งโปรแกรมที่ไม่รู้แหล่งที่มา

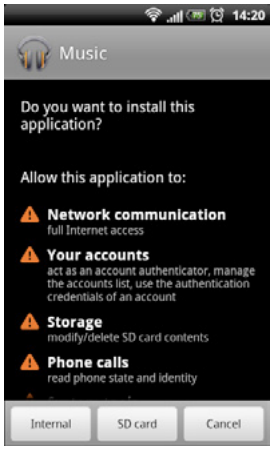
ผู้ใช้สามารถใช้โปรแกรมประเภท File Manager เพื่อทำการติดตั้งโปรแกรมจากไฟล์ .apk ที่ดาวน์โหลดมาได้ แต่ไม่ว่าจะเป็นการติดตั้งโปรแกรมจาก Android Market หรือจากไฟล์ .apk ระบบปฏิบัติการ Android จะแสดงหน้าจอ Permission เพื่อให้ผู้ใช้ตรวจสอบและยอมรับสิทธิการเข้าถึงของโปรแกรมที่จะติดตั้ง ดังรูปที่ 118 (23-3) โดยรายละเอียดของ Permission จะกล่าวถึงในหัวข้อถัดไป



รูปที่ 118 (23-3) ตัวอย่างหน้าจอ Permission เมื่อทำการติดตั้งโปรแกรมจากเว็บไซต์ Android Market

Permission ใน Android คืออะไร

ระบบปฏิบัติการ Android นั้นถูกออกแบบมาให้มีความมั่นคงปลอดภัยตั้งแต่แรก โปรแกรมทุกตัวในระบบจะสามารถเข้าถึงได้แค่คุณสมบัติพื้นฐานของระบบ เช่น ส่วนติดต่อกับผู้ใช้ การแสดงผลทางหน้าจอ เป็นต้น หากผู้พัฒนาต้องการให้โปรแกรมของตนมีการเรียกใช้คุณสมบัติพิเศษเพิ่มเติมจากระบบปฏิบัติการ เช่น อ่านข้อมูลบัญชีผู้ใช้ หรือเขียนข้อมูลใน SD Card ก็จำเป็นต้องเพิ่มส่วนที่เป็นการขอใช้สิทธิ (Permission) ดังกล่าวในโปรแกรมของตนด้วย [23-7] [23-8] [23-9] ซึ่งรายการสิทธิทั้งหมดที่โปรแกรมต้องการใช้งานนั้นจะปรากฏตั้งแต่แรกตอนผู้ใช้ติดตั้งโปรแกรม ดังรูปที่ 119 (23-4) เพื่อให้ผู้ใช้ได้รับทราบและพิจารณาการทำงานของโปรแกรมก่อนทำการติดตั้ง



รูปที่ 119 (23-4) ตัวอย่างการขอ Permission ในการติดตั้งโปรแกรม

ตัวอย่าง Permission ที่ควรพิจารณาก่อนทำการติดตั้งโปรแกรม มีดังนี้ [23-10]

- **Services that cost you money**
  - Make phone calls
    - อนุญาตให้โปรแกรมโทรออกได้
- **Send SMS or MMS**
  - อนุญาตให้โปรแกรมส่ง SMS หรือ MMS ได้
- **Storage**
  - Modify/delete SD card contents
    - อนุญาตให้โปรแกรมสร้าง แก้ไข หรือลบข้อมูลที่อยู่ใน SD Card ได้ ซึ่งจำเป็นในบางโปรแกรม เพราะต้องเก็บข้อมูลลงใน SD Card
- **Your personal information**
  - Read contact data, write contact data
    - อนุญาตให้โปรแกรมอ่านหรือสร้างรายชื่อผู้ติดต่อในสมุดโทรศัพท์ได้
  - Read calendar data, write calendar data
    - อนุญาตให้โปรแกรมอ่านข้อมูลหรือสร้างกำหนดการให้ปฏิทินได้
  - Read/write Browser history and bookmarks
    - อนุญาตให้โปรแกรมดูข้อมูลเว็บไซต์ที่ผู้ใช้เคยเข้าหรือดู Bookmark ได้
  - Read logs / Read sensitive logs
    - อนุญาตให้โปรแกรมสามารถอ่าน log ของโปรแกรมอื่นหรือ log ของระบบได้ ซึ่งโดยปกติแล้วโปรแกรมที่ใช้ Permission นี้มีแค่โปรแกรมของ Google
- **Phone calls**
  - Read phone state and identity
    - อนุญาตให้โปรแกรมอ่านหมายเลข IMEI และ IMSI ของเครื่อง
- **Your location**
  - Fine (GPS) location
    - อนุญาตให้โปรแกรมตรวจสอบตำแหน่งที่อยู่ของผู้ใช้จาก GPS
  - Coarse (network-based) location
    - อนุญาตให้โปรแกรมตรวจสอบตำแหน่งที่อยู่ของผู้ใช้จากผู้ให้บริการโทรศัพท์
- **Network Communication**
  - Create Bluetooth connection
    - อนุญาตให้โปรแกรมสร้างการเชื่อมต่อผ่าน Bluetooth จำเป็นต้องใช้ในโปรแกรมที่ใช้ในการรับส่งไฟล์หรือเชื่อมต่อหูฟังไร้สาย
  - Full internet access
    - อนุญาตให้โปรแกรมเชื่อมต่อกับอินเทอร์เน็ต
  - View network state / Wi-Fi state
    - อนุญาตให้โปรแกรมตรวจสอบว่าผู้ใช้เชื่อมต่ออินเทอร์เน็ตผ่าน Data หรือ Wi-Fi
- **Your accounts**
  - Discover Known Accounts
    - อนุญาตให้โปรแกรมสามารถอ่าน Username ของผู้ใช้ได้ (เฉพาะ Username ไม่รวม Password)
  - Manage Accounts
    - อนุญาตให้โปรแกรมสร้าง Account ใหม่เพิ่มในระบบได้ ซึ่งจำเป็นต้องใช้ในโปรแกรมประเภท Social media
  - Use Credentials
    - อนุญาตให้โปรแกรมเข้าถึง User account ของผู้ใช้ ซึ่งรวมถึง Username และ Password

- **Your messages**
  - Read/modify Gmail
    - อนุญาตให้โปรแกรมสามารถเข้าถึงบัญชี Gmail ของผู้ใช้ได้
- **System tools**
  - Install Packages
    - อนุญาตให้โปรแกรมสามารถติดตั้งโปรแกรมอื่นเพิ่มเติมได้ โปรแกรมโดยทั่วไปไม่ควรร้องขอสิทธินี้ ยกเว้นจะเป็นโปรแกรมประเภท Market หากไม่ใช่ ให้สงสัยไว้ก่อนว่าโปรแกรมนั้นอาจจะเป็น Malware
  - Prevent phone from sleeping
    - อนุญาตให้โปรแกรมป้องกันไม่ให้เครื่องเข้าสู่สถานะ Sleep หากผู้ใช้ไม่ได้ทำอะไรกับเครื่องตามระยะเวลาที่กำหนด ความสามารถนี้อาจถูกใช้ในโปรแกรมบางประเภท เช่น โปรแกรมเล่นวีดีโอ
  - Modify global system settings
    - อนุญาตให้โปรแกรมแก้ไขค่าของระบบ ซึ่งจำเป็นต้องใช้ในบางโปรแกรมเท่านั้น เช่น Widget หรือโปรแกรมปรับแต่งระบบ
  - Read sync settings
    - อนุญาตให้โปรแกรมตรวจสอบว่าผู้ใช้เปิดการ Synchronize ข้อมูลให้กับโปรแกรมที่ทำงานอยู่เบื้องหลัง (เช่น Facebook, Gmail) หรือเปล่า
  - Restart other applications
    - อนุญาตให้โปรแกรมทำการ Restart โปรแกรมอื่นหรือเปล่า
  - Retrieve running applications
    - อนุญาตให้โปรแกรมตรวจสอบรายชื่อของโปรแกรมที่กำลังทำงานอยู่ โดยทั่วไปจะใช้กับโปรแกรมประเภท Task killer
  - Automatically start at boot
    - อนุญาตให้โปรแกรมเริ่มทำงานโดยอัตโนมัติทุกครั้งที่เปิดเครื่อง
- **Hardware controls**
  - Control Vibrator
    - อนุญาตให้โปรแกรมทำให้เครื่องสั่นได้ ซึ่งจำเป็นต้องใช้ในบางโปรแกรม เช่น ทำให้เครื่องสั่นเมื่อมีสายเข้าหรือแจ้งเตือนกำหนดการ
  - Take Pictures & Video
    - อนุญาตให้โปรแกรมสามารถถ่ายรูปหรือวีดีโอได้

จะเห็นได้ว่า Permission บางอย่างอาจถูกผู้ไม่หวังดีนำไปใช้ในทางที่ผิดได้ เช่น สร้าง Malware เพื่อแอบอ่านข้อมูลรายชื่อผู้ติดต่อของผู้ใช้ แอบถ่ายรูปผู้ใช้ รวมถึงแอบส่งข้อมูลของผู้ใช้งานผ่านอินเทอร์เน็ตกลับไปให้ผู้พัฒนา Malware เป็นต้น Malware ที่ถูกสร้างมาเพื่อขโมยข้อมูล อาจมาในรูปของโปรแกรมธรรมดา

เช่น เครื่องคิดเลข แต่มีความต้องการ Permission ที่ไม่น่าจะเกี่ยวข้องกับการทำงานของโปรแกรม เช่น เข้าถึงข้อมูลรายชื่อผู้ติดต่อ เข้าถึงกล้องถ่ายรูป หรือเชื่อมต่อกับอินเทอร์เน็ต เป็นต้น ดังนั้นก่อนทำการติดตั้งโปรแกรมทุกครั้งควรตรวจสอบให้แน่ใจว่าโปรแกรมนั้น ไม่ได้มีการขอใช้สิทธิเกินความจำเป็น

หากผู้ใช้ต้องการตรวจสอบว่า โปรแกรมที่ติดตั้งไปแล้วนั้น มีการขอ Permission อะไรบ้าง สามารถทำได้ด้วยการเข้าไปที่เมนู Settings เลือก Applications แล้วเลือก Manage applications จากนั้นจะปรากฏรายชื่อโปรแกรมที่ติดตั้งในระบบ ซึ่งสามารถเลือกดูรายละเอียด Permission ของแต่ละโปรแกรมได้

หากโปรแกรมที่ได้ติดตั้งไปแล้ว แจ้งให้ทำการ Update แบบ Manual update หมายความว่าทางผู้พัฒนามีการปรับเปลี่ยน Permission บางอย่างจากเวอร์ชันก่อนหน้า ก่อนทำการติดตั้งโปรแกรมเวอร์ชันใหม่ควรตรวจสอบ Permission เพื่อความแน่ใจอีกครั้งหนึ่ง

อันตรายและการป้องกันภัยจาก Malware

จากเหตุการณ์ที่ผ่านมา พบว่าผู้พัฒนา Malware ในระบบปฏิบัติการ Android โดยส่วนใหญ่จะใช้วิธีการสร้างโปรแกรมที่ดูเหมือนจะไม่มีอันตรายแต่แอบแฝง โค้ดอันตรายมาด้วย ซึ่งหากผู้ใช้ไม่ตรวจสอบ Permission ให้ดีก่อนทำการติดตั้งโปรแกรม ก็จะตกเป็นเหยื่อของ Malware ได้โดยง่าย นอกจากนี้ ผู้พัฒนา Malware ส่วนใหญ่จะใช้วิธีการหลอกลวงแบบวิศวกรรมทางสังคม (Social engineering) ร่วมด้วย เช่น สร้างโปรแกรมโดยตั้งชื่อให้เหมือนกับเป็นเวอร์ชันฟรีของโปรแกรมที่ต้องเสีย เงินซื้อ เพื่อหลอกให้คนดาวน์โหลดไปติดตั้ง เป็นต้น [23-11]

ก่อนหน้านี้ Malware ในระบบปฏิบัติการ Android โดยส่วนใหญ่จะเน้นไปในด้านการขโมยข้อมูล เนื่องจากผู้ใช้อาจมีการเก็บข้อมูลสำคัญที่เป็นความลับ เช่น บัญชีธนาคารหรือไฟล์เอกสารสำคัญ ไว้ในโทรศัพท์มือถือ ตัวอย่าง Malware ที่โจมตีด้วยวิธีนี้คือโทรจันชื่อ Antammi ซึ่งหลอกว่าเป็นโปรแกรมที่เอาไว้สำหรับดาวน์โหลดเสียงเรียกเข้า (Ringtone) [23-12] แต่ในปัจจุบัน Malware ในระบบปฏิบัติการ Android ได้ถูกพัฒนาให้สามารถทำงานได้หลากหลายและสร้างความเสียหายได้มากขึ้น ตัวอย่างเช่น Zitmo ที่ถูกพัฒนามาจาก Zeus ซึ่งเป็นโทรจันใน PC โดยทำหน้าที่เป็น Man-in-the-Middle คอยดักรับและแก้ไขข้อมูลการใช้งาน e-Banking ของผู้ใช้ [23-13] และล่าสุด Kaspersky Labs ได้ค้นพบ Malware ตัวใหม่ที่ทำหน้าที่เป็น IRC Bot [23-14] ซึ่งเปิดโอกาสให้ผู้โจมตีเข้ามาควบคุมเครื่องของผู้ใช้จากระยะไกลได้ ถึงแม้ว่าปัจจุบันนี้จะมีโปรแกรม Antivirus สำหรับระบบปฏิบัติการ Android ออกมามากมาย แต่จากผลการทดสอบของสำนักวิจัยหลายแห่งพบว่าการติดตั้งโปรแกรม Antivirus ในระบบนั้นไม่สามารถช่วยในการตรวจจับ Malware ได้มากเท่าไหร่นัก แต่กลับทำให้เครื่องทำงานช้าลงและทำให้สิ้นเปลืองพลังงานมากขึ้น [23-15] [23-16]

เนื่องจากจุดอ่อนของ Android Market ที่ไม่มีมาตรการตรวจสอบโปรแกรมก่อนปล่อยให้ดาวน์โหลดมีเพียงแค่การ แจ้งลบโปรแกรมที่ไม่เหมาะสม และระบบปฏิบัติการ Android อนุญาตให้ผู้ใช้ติดตั้งโปรแกรมที่อยู่ในรูปแบบของไฟล์ .apk ได้ ทำให้ผู้ใช้ต้องระมัดระวังตนเองในการใช้งาน เช่น ตรวจสอบเว็บไซต์ของผู้พัฒนา พิจารณาจากผลการ Review ที่น่าเชื่อถือก่อนทำการติดตั้งโปรแกรมใดๆ รวมถึงไม่ติดตั้งโปรแกรม

ละเมิดลิขสิทธิ์หรือโปรแกรมที่มาจากแหล่งที่ไม่น่า เชื่อถือ เช่น เว็บไซต์สำหรับฝากไฟล์ เนื่องจากอาจมี Malware แอบแฝงมาได้ หากสงสัยว่าระบบติด Malware ผู้ใช้อาจจะสามารถตรวจสอบเบื้องต้นได้โดยการดูบันทึกของระบบ เช่น บันทึกการโทรออก หรือบันทึกการใช้งาน Mobile data เป็นต้น

อ้างอิง

[23-1] http://en.wikipedia.org/wiki/Smartphone

[23-2] http://www.gartner.com/it/page.jsp?id=1848514

[23-3] http://developer.android.com/guide/basics/what-is-android.html

[23-4] http://www.android.com/about/ice-cream-sandwich/

[23-5] http://www.droid-life.com/2011/03/02/droiddream-malware-enters-official-android-market-chaos-ensues-after-root-exploit-found-embedded

[23-6] http://globalthreatcenter.com/?p=2492

[23-7] http://source.android.com/tech/security/index.html

[23-8] http://developer.android.com/guide/topics/security/security.html

[23-9] http://www.vogella.de/articles/Android/article.html#overview_permissions

[23-10] http://alostpacket.com/2010/02/20/how-to-be-safe-find-trusted-apps-avoid-viruses/

[23-11] http://www.androidpolice.com/2011/11/05/psa-no-this-is-not-msn-2012-angry-birds-2-or-modern-warfare-for-android-what-you-can-do-if-you-see-malware-in-the-market/

[23-12] http://www.net-security.org/malware_news.php?id=1889

[23-13] http://blog.fortinet.com/zitmo-hits-android/

[23-14] http://www.androidpolice.com/2012/01/13/first-irc-bot-for-android-shows-up-allows-full-remote-control-of-your-device/

[23-15] http://www.zdnetasia.com/android-antivirus-freeware-near-to-useless-62302868.htm

[23-16] http://news.cnet.com/8301-1009_3-57325078-83/free-android-antivirus-apps-fail-to-cut-it/

24 เสริมความมั่นคงปลอดภัยให้กับซอฟต์แวร์ด้วย EMET

ผู้เขียน: วิศัลย์ ประสงค์สุข

วันที่เผยแพร่: ๒ มี.ค. ๒๕๕๕
ปรับปรุงล่าสุด: ๒ มี.ค. ๒๕๕๕

ปัญหาหนึ่งของผู้ใช้งานคอมพิวเตอร์ในยุคที่เทคโนโลยีมีความเจริญก้าวหน้าอย่างรวดเร็ว คือ ผู้ใช้ไม่สามารถติดตามข่าวสารและแก้ไขช่องโหว่ของซอฟต์แวร์ที่ใช้งานได้อย่างทันท่วงที นอกจากนี้ในฝั่งของผู้พัฒนาเอง บางครั้งถึงแม้จะรู้ว่าซอฟต์แวร์ที่ตนพัฒนามีช่องโหว่ ก็ยังไม่สามารถแก้ไขช่องโหว่เหล่านั้นได้ทันที เนื่องจากจะต้องมีการทดสอบให้แน่ใจว่า การแก้ปัญหานั้นไม่ส่งผลกระทบกับการทำงานปรกติของซอฟต์แวร์แล้วในช่วงเวลาเช่นนี้ผู้ใช้จะป้องกันตนเองได้อย่างไร

โปรแกรม Enhanced Mitigation Experience Toolkit หรือ EMET เป็นทางเลือกหนึ่งสำหรับผู้ใช้งานระบบปฏิบัติการ Windows เนื่องจากการทำงานภายใน EMET ประกอบไปด้วยเทคโนโลยีต่าง ๆ ที่มีคุณสมบัติเรียกว่า Mitigation Technology โดยจะทำหน้าที่ขัดขวางการทำงานที่ผิดปรกติ จึงสามารถช่วยลดโอกาสของผู้ไม่หวังดีในการโจมตีผู้ใช้งานระบบปฏิบัติการ Windows ได้สำเร็จ ซึ่งจากข้อมูลของ EMET ได้ระบุถึงรายละเอียดของเทคนิค Mitigation Technology ต่าง ๆ โดยจะอธิบายในหัวข้อถัดไป

ปัจจุบัน EMET พัฒนามาถึงเวอร์ชัน 2.1 โดยผู้ใช้สามารถใช้งานได้ทั้งในรูปแบบ Graphic User Interface (GUI) และแบบ Command-line Interface (CLI) ผู้ใช้สามารถดาวน์โหลด EMET ไปติดตั้งได้ด้วยตนเองจาก เว็บไซต์ของ Microsoft โปรแกรม EMET สามารถทำงานได้บนระบบปฏิบัติการดังต่อไปนี้

- **Windows XP ที่ติดตั้ง Service Pack 3 หรือเวอร์ชันใหม่กว่า**
- **Windows Vista ที่ติดตั้ง Service Pack 1 หรือเวอร์ชันใหม่กว่า**
- **Windows 7 ทุกเวอร์ชัน**
- **Windows Server 2003 หรือเวอร์ชันใหม่กว่า**
- **Windows Server 2008 ทุกเวอร์ชัน**

* หมายเหตุ การใช้งาน EMET ในรูปแบบ GUI ผู้ใช้จำเป็นต้องติดตั้ง .NET Framework 2.0 หรือใหม่กว่า

Mitigation Technology

Mitigation Technology ที่เกี่ยวข้องกับ Microsoft จะหมายถึงเทคโนโลยีที่ทาง Microsoft พัฒนาขึ้นมาเอง โดยมีวัตถุประสงค์เพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบปฏิบัติการ ซึ่งโดยส่วนใหญ่มักจะอัพเดทเทคโนโลยีดังกล่าวเข้ามาร่วมกับ Windows เวอร์ชันใหม่หรือเวอร์ชันล่าสุด ณ ช่วงเวลานั้น แต่ข้อเสียคือเทคโนโลยีดังกล่าวจะสามารถตรวจสอบและป้องกันได้เพียงโปรแกรม ที่ติดตั้งมาพร้อมกับระบบปฏิบัติการเท่านั้น ซึ่งในโปรแกรม EMET ที่มีหลักการทำงานของ Mitigation Technology อยู่แล้วนั้น ผู้ใช้สามารถกำหนดให้ใช้ Mitigation Technology กับโปรแกรมอื่น ๆ ที่ติดตั้งเพิ่มเติมภายหลังได้ จึงทำให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้น โดย Mitigation Technology ที่มีในโปรแกรม EMET เวอร์ชัน 2.1 มีดังต่อไปนี้

1. **Structure Exception Handler Overwriter Protection [24-1] [24-9]**

SEHOP จะตรวจสอบการทำงานของ Structure Exception Handler (SEH) ซึ่งเป็นส่วนที่ทำหน้าที่จัดการกับข้อผิดพลาดที่เกิดขึ้นในระหว่างการประมวล ผล (Exception Handlind) โดยจะป้องกันไม่ให้มีการนำคำสั่งอันตรายเข้ามาประมวลผลในระหว่างการจัดการ Exception ทำให้การโจมตีโดยใช้วิธี Stack Overflow ทำได้ยากขึ้น

2. **Dynamic Data Execution Prevention [24-2] [24-9]**

DEP จะเป็นการตรวจสอบการใช้งานหน่วยความจำ โดยจะป้องกันไม่ให้มีการนำค่าในตำแหน่งของหน่วยความจำที่มีไว้สำหรับเก็บข้อมูลไปประมวลผล ทำให้การโจมตีด้วยวิธี Buffer Overflow ทำได้ยากขึ้น

3. **Heap Spray Allocation [24-3] [24-9]**

HSA จะเป็นการจองพื้นที่ในหน่วยความจำในส่วนของ Heap ให้กับโพรเซสนั้นๆ ไว้ล่วงหน้า เพื่อทำให้การโจมตีโดยวิธี Heap spray ทำได้ยากขึ้น

4. **Null Page Allocation [24-3] [24-9]**

NPA ช่วยให้การโจมตีโดยใช้เทคนิค Null Dereference ทำได้ยากขึ้น (Null Dereference คือการใช้ Pointer กำหนดค่า Null ให้กับหน่วยความจำ ทำให้โพรเซสไม่สามารถทำงานต่อได้) ปัจจุบันยังไม่พบการโจมตีด้วยวิธีนี้

5. **Address Space Layout Randomization [24-5] [24-9]**

ASLR จะสลับตำแหน่ง (Shuffle) โมดูลในแต่ละส่วนของโปรแกรม แล้วสุ่มตำแหน่งของหน่วยความจำที่จะเก็บโมดูลนั้นไว้ ก่อนจะโหลดโปรแกรมเข้าไปในหน่วยความจำเพื่อทำการประมวลผล ทำให้การโจมตีโดยการสั่ง Jump ไปยังตำแหน่งในหน่วยความจำเป็นไปได้ยาก

6. **Bottom-Up Randomization [24-3] [24-4] [24-9]**

BUR เป็นการใส่ Offset เข้าไปในส่วนท้ายของ Stack หรือ Heap เพื่อให้แต่ละครั้งที่มีการโหลดไลบรารีเข้าไปในหน่วยความจำจะไม่ได้อยู่ที่ ตำแหน่งเดิม ทำให้การโจมตีโดยการคาดการณ์ที่อยู่ของไลบรารีทำได้ยาก

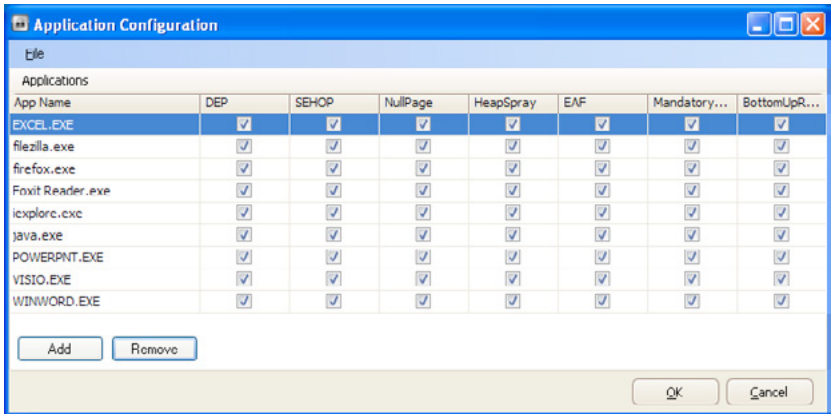
7. **Export Address Table Access Filtering [24-3] [24-9]**

EAF จะป้องกันการค้นหาตำแหน่งของฟังก์ชั่นของระบบปฏิบัติการใน Export Address Table (EAT) โดยจะทำการตรวจสอบว่าฟังก์ชั่นนั้นสามารถเรียกใช้งาน EAT ได้หรือไม่ ทำในการโจมตีโดยใช้ Shell code บางประเภทนั้นทำได้ยาก

การใช้งานโปรแกรม EMET

เอกสารฉบับนี้จะแสดงวิธีการใช้งานโปรแกรม EMET ในรูปแบบ GUI บนระบบปฏิบัติการ Windows XP โดยมีวิธีการดังนี้

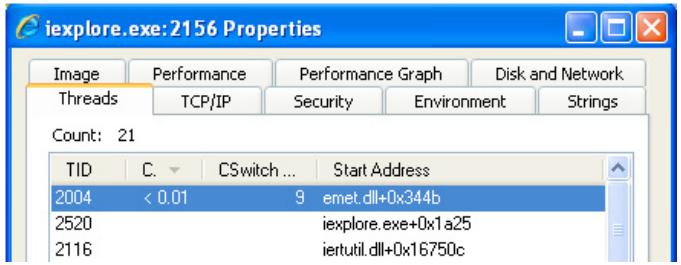
เมื่อเปิดโปรแกรม EMET ขึ้นมาจะพบหน้าต่างแสดงส่วนประกอบของโปรแกรมดังรูปที่ 120 (24-1)



รูปที่ 120 (24-1) หน้าต่างเริ่มต้นเมื่อเปิดโปรแกรม EMET

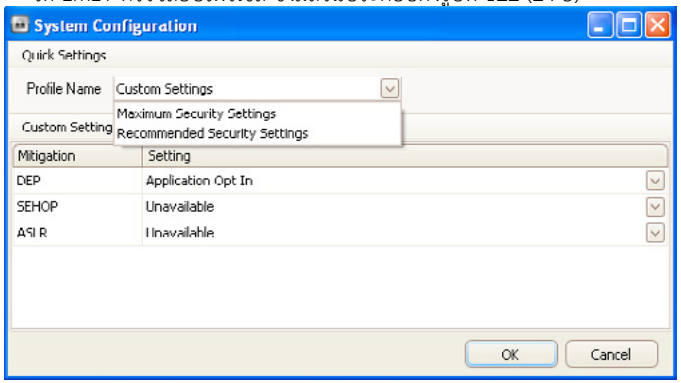
จากรูปที่ 120 (24-1) ส่วนประกอบของหน้าต่างโปรแกรม EMET มีดังต่อไปนี้

- **System Status** เนื่องจากในระบบปฏิบัติการ Windows XP มีการติดตั้ง DEP ไว้ในระบบแล้วแต่ยังไม่ได้มีการติดตั้ง SEHOP และ ASLR ดังนั้นหน้าต่างโปรแกรม EMET จึงแสดงค่าเป็น Unavailable อย่างไรก็ตามผู้ใช้ยังสามารถใช้งาน SEHOP และ ASLR ได้เนื่องจาก EMET ได้รับการพัฒนาให้ใช้ SEHOP และ ASLR กับโปรแกรมต่าง ๆ ได้
  - **Configure System** เป็นปุ่มเรียกหน้าต่างการตั้งค่าโหมดการทำงานของ Mitigation ที่รองรับให้กับระบบ ซึ่งในที่นี้คือ DEP โดยหน้าต่างการตั้งค่ามีส่วนประกอบดังรูปที่ 121 (24-2)



รูปที่ 121 (24-2) หน้าต่างการตั้งค่า DEP ให้กับระบบ

- Profile name
  - **Maximum Secutiy Settings** จะเป็นเปลี่ยนค่าให้ DEP ทำงานในโหมด AlwaysOn
  - **Recommended Security Settings** จะเป็นการเปลี่ยนให้ DEP ทำงานในโหมด OptIn
  - ***หมายเหตุ** โหมดการทำงานของ DEP มีดังต่อไปนี้ [24-2]
    - **OptIn:** เป็นการตั้งค่าให้ DEP ตรวจสอบเฉพาะไบนารีของระบบปฏิบัติการ โหมดการทำงานนี้เป็นค่าตั้งต้นของระบบ
    - **OptOut:** เป็นการตั้งค่าเพื่อเลือกโปรแกรมที่ไม่ต้องใช้ DEP
    - **AlwaysOn:** เป็นการตั้งค่าเพื่อให้ DEP ตรวจสอบทุกโพรเซสที่รันอยู่ในระบบ ไม่ว่าโพรเซสนั้นจะเป็นของโปรแกรมที่ระบุใน OptOut หรือไม่
    - **AlwaysOff:** ตั้งค่าเพื่อไม่ใช้งาน DEP
- **Running Processes เป็นรายการของโพรเซสที่กำลังทำงานอยู่ในขณะนั้น รายการนี้โปรแกรม EMET จะตรวจสอบการเปลี่ยนแปลงทุก ๆ 30 วินาที**
  - **Configure Apps** เป็นปุ่มเรียกหน้าต่างตั้งค่าเพื่อให้ผู้ใช้สามารถเลือกโปรแกรมที่ต้องการให้ EMET ตรวจสอบโพรเซส ซึ่งมีส่วนประกอบดังรูปที่ 122 (24-3)



รูปที่ 122 (24-3) หน้าต่างเลือกโปรแกรมที่ต้องการให้ EMET ตรวจสอบ

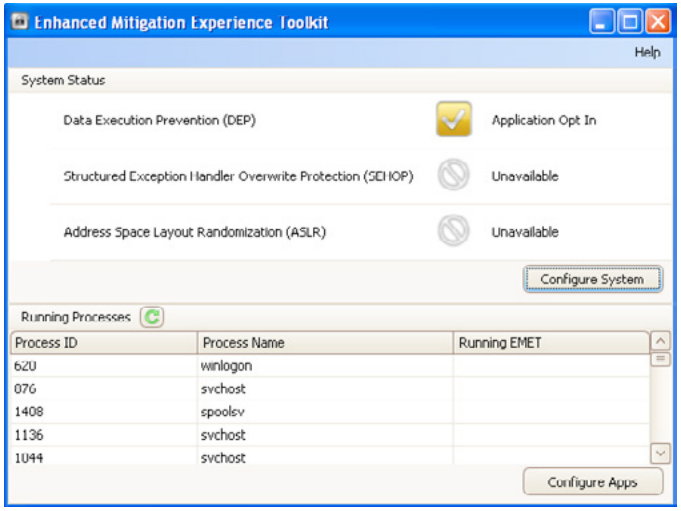
ผู้ใช้สามารถเพิ่มหรือลดโปรแกรมที่ต้องการให้ EMET ตรวจสอบการทำงานได้โดยคลิกที่ปุ่ม Add หรือ Remove ในด้านล่างซ้าย ในการเลือกโปรแกรมนั้นจะต้องระบุพาธที่โปรแกรมนั้นติดตั้งอยู่

ในการพิจารณาเลือกโปรแกรมเพื่อใช้งานกับ EMET ผู้ใช้ควรเลือกโปรแกรมที่ใช้งานในชีวิตประจำวัน เพราะว่าโปรแกรมที่ใช้งานบ่อยมักจะเป็นเป้าหมายของการโจมตี [24-6] ตัวอย่างโปรแกรมที่ใช้งานบ่อยเช่น โปรแกรมเว็บเบราว์เซอร์ โปรแกรมสำนักงาน (Microsoft Office, OpenOffice) โปรแกรมด้านมัลติมีเดีย และโปรแกรม Adobe Reader, Adobe Acrobat เป็นต้น

หลังจากเลือกโปรแกรมเรียบร้อยแล้วจะต้องทำการเริ่มโปรแกรมนั้นใหม่เพื่อให้ EMET ทำงาน

***หมายเหตุ** บางเทคนิคไม่สามารถใช้งานได้กับบางโปรแกรม เนื่องจากอาจทำให้โปรแกรมนั้นทำงานผิดปรกติได้ ดังนั้นหลังจากเลือกโปรแกรมใช้งานแล้ว จึงควรทดสอบให้แน่ใจว่าโปรแกรมนั้น ๆ ทำงานได้ปรกติ [24-7]

เนื่องจาก EMET เป็นเครื่องมือที่มีการทำงานอยู่เบื้องหลัง ทำให้ผู้ใช้ไม่สามารถตรวจสอบว่า EMET ทำงานอยู่หรือไม่ได้โดยตรง แต่สามารถตรวจสอบได้โดยดูจากโปรแกรมที่มีความสามารถตรวจสอบโพรเซสของโปรแกรม ต่าง ๆ ที่กำลังทำงานอยู่เช่น โปรแกรม Process Explorer [24-8] เป็นต้น ในรูปที่ 123 (24-4) เป็นการใช้โปรแกรม Process Explorer ตรวจสอบโพรเซสของ Internet Explorer



รูปที่ 123 (24-4) EMET กำลังตรวจสอบการทำงานในขณะที่ใช้โปรแกรม Internet Explorer

การใช้งาน EMET ช่วยให้ซอฟต์แวร์ต่าง ๆ มีความมั่นคงปลอดภัยเพิ่มขึ้นระดับหนึ่ง อย่างไรก็ตามผู้ใช้ควรหมั่นติดตามข่าวสารและอัพเดทซอฟต์แวร์ให้เป็นเวอร์ชั่นล่าสุดอยู่เสมอ และที่สำคัญ ผู้ใช้ควรระมัดระวังการเปิดเว็บไซต์ ไฟล์ หรือสิ่งอื่น ๆ ที่ไม่น่าไว้ใจซึ่งอาจเป็นอันตรายต่อระบบคอมพิวเตอร์ได้

อ้างอิง

[24-1] http://blogs.technet.com/b/srd/archive/2009/02/02/preventing-the-exploitation-of-seh-overwrites-with-sehop.aspx

[24-2] http://support.microsoft.com/kb/875352

[24-3] http://blogs.technet.com/cfs-filesystemfile.ashx/__key/communityserver-components-postattachments/00-03-35-03-78/Users-Guide.pdf

[24-4] http://blog.didierstevens.com/2011/09/29/add-bottom-up-randomization-to-your-own-source-code/

[24-5] http://blog.didierstevens.com/2011/08/16/so-how-good-is-pseudo-aslr/

[24-6] http://rationallyparanoid.com/articles/microsoft-emet-2.html

[24-7] http://support.microsoft.com/kb/2458544

[24-8] http://technet.microsoft.com/en-us/sysinternals/bb896653

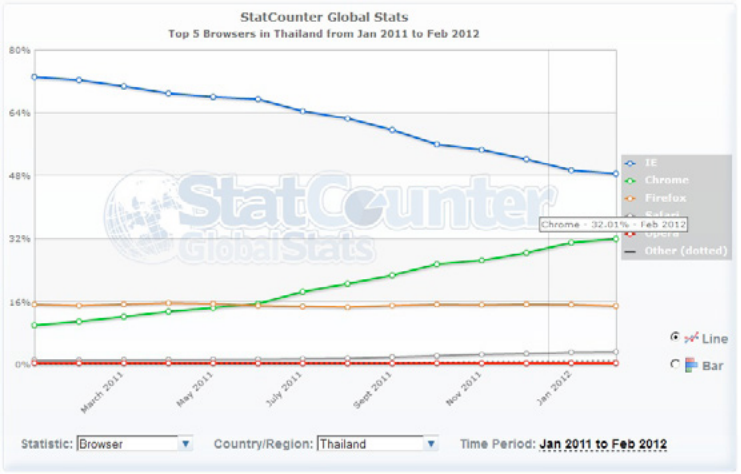
[24-9] http://www.infoworld.com/t/microsoft-windows/microsoft-shuffles-windows-security-deck-emet-21-831

25 EXTENSION ใน GOOGLE CHROME สวมรอยบัญชีผู้ใช้ FACEBOOK

ผู้เขียน: ศุภกร ฤกษ์ดิถีพร

วันที่เผยแพร่: 30 มีนาคม 2555
ปรับปรุงล่าสุด: 30 มีนาคม 2555

เว็บเบราว์เซอร์ คือส่วนหนึ่งที่สำคัญในการเข้าสู่โลกออนไลน์เพื่อซื้อสินค้า ติดตามข่าวสาร ดูวีดีโอออนไลน์ หรือแม้กระทั่งการทำธุรกรรมออนไลน์ ปัจจุบันมีเว็บเบราว์เซอร์มากมายให้เลือกใช้ หนึ่งในนั้นคือ Google Chrome ซึ่งเป็นเว็บเบราว์เซอร์ที่ถูกพัฒนาขึ้นโดย Google เปิดตัวครั้งแรกเมื่อวันที่ 2 กันยายน พ.ศ. 2551 ในประเทศไทยมีผู้ใช้งาน Google Chrome มากถึง 32% จากจำนวนผู้ใช้เว็บเบราว์เซอร์ทั้งหมด โดยแซงหน้า Mozilla Firefox ที่เคยเป็นเบราว์เซอร์อันดับ 2 มาก่อน ดังรูปที่ 124 (25-1)



รูปที่ 124 (25-1) สถิติการใช้งานเว็บเบราว์เซอร์ในประเทศไทย [25-1]

Extension คือโปรแกรมเสริมที่ถูกพัฒนาขึ้นมาเพื่อเพิ่มความสามารถให้กับเว็บ เบราว์เซอร์ เช่น แจ้งเตือนเมื่อมีอีเมลเข้ามาใหม่ หรือ แจ้งเตือนเมื่อมีคนมาคอมเมนต์ในหน้า Facebook เป็นต้น

ใน Google Chrome สามารถติดตั้ง Extension ได้ผ่าน Chrome Web Store

นักวิจัยจากบริษัท Kaspersky ซึ่งเป็นผู้ผลิตซอฟต์แวร์ป้องกันไวรัส ได้ค้นพบ Extension ของ Google Chrome ที่เป็นอันตราย โดยมีจุดประสงค์เพื่อขโมยข้อมูลบัญชีผู้ใช้งาน Facebook ผ่านทางหน้าเพจที่ชื่อ “Aprenda tirar virus do face” ดังรูปที่ 125 (25-2) [25-2]

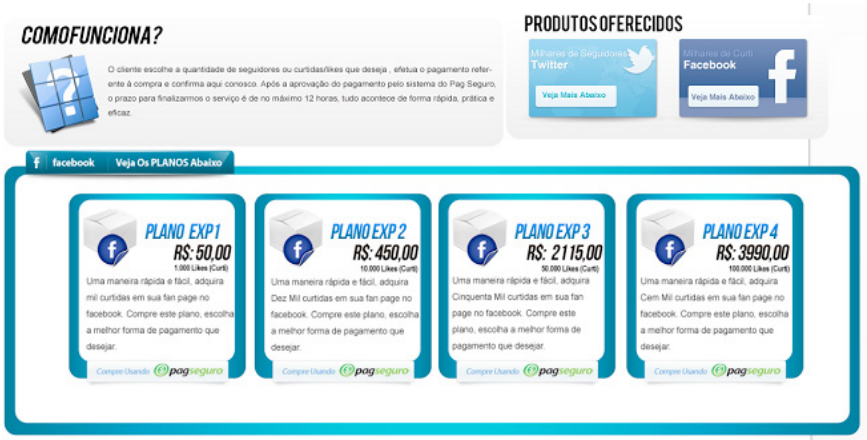
รูปที่ 125 (25-2) โปรไฟล์ Facebook ที่ใช้เป็นช่องทางหลอกให้ติดตั้ง Extension [25-3]

หน้าโปรไฟล์นี้ได้แนะนำให้ผู้ใช้ติดตั้ง Extension เพิ่มเติม หลังจากคลิกที่ข้อความ Install aplicativo จะนำผู้ใช้งานไปที่เว็บไซต์ Chrome Web Store เพื่อให้ติดตั้ง Extension ชื่อ Adobe Flash Player ซึ่งถูกพัฒนาโดย AppFace ดังรูปที่ 126 (25-3)

รูปที่ 126 (25-3) แสดงการติดตั้ง Extension Adobe Flash Player [25-4]

นักวิจัยระบุว่า Extension นี้เป็นโทรจันชื่อ Trojan.JS.Agent.bxo เมื่อเหยื่อหลงกลติดตั้งไปแล้ว ตัว Extension จะใช้บัญชี Facebook ของผู้ใช้ในการส่งคำเชิญไปให้กับเพื่อนของเหยื่อเพื่อหลอกให้ติดตั้ง Extension นี้ และกด “Like” หน้าเพจตามที่ผู้ไม่ประสงค์ดีต้องการ จากการตรวจสอบโดย Kaspersky พบว่าผู้ใช้งานในประเทศบราซิลตกเป็นเหยื่อของโทรจันนี้มากที่สุด [25-5]

หลายคนคงมีความสงสัยว่าทำไมผู้ไม่ประสงค์ดีถึงพยายามปล่อย Extension ที่มาพร้อมกับ Trojan.JS.Agent.bxo จุดประสงค์หลักๆ คือ การสร้างรายได้ให้กับตัวเองเพื่อขายบริการกด “Like” Facebook ให้กับบริษัทที่ต้องการประชาสัมพันธ์โปรไฟล์ของพวกเขาเพื่อส่งเสริมให้คนมาสนใจมากขึ้น ดังรูปที่ 127 (25-4)



รูปที่ 127 (25-4) ตัวอย่างการขายบริการ 1,000 Like เป็นเงินประมาณ 850 บาท [25-6]

หากผู้ใช้เผลอติดตั้ง Extension ดังกล่าว สามารถออกจาก Google Chrome ได้โดย

1. คลิกไอคอนประแจ ที่มุมขวาบนของเว็บเบราวเซอร์
2. คลิก เครื่องมือ (Tools)
3. เลือก ส่วนขยาย (Extensions) ที่ชื่อ Adobe Flash Player 12.1.102.55
4. คลิกที่ปุ่ม ลบออก (Uninstall)

เพื่อหลีกเลี่ยงการติดตั้ง Extension ที่ไม่พึงประสงค์และอาจถูกขโมยโปรไฟล์ Facebook ผู้ใช้งานควรศึกษารายละเอียด Extension ที่เกี่ยวข้องกับการใช้งานก่อนการติดตั้งลงบนเครื่องคอมพิวเตอร์ เช่น ตรวจสอบเว็บไซต์ของผู้พัฒนา รายละเอียดเกี่ยวกับผู้พัฒนา รุ่นที่พัฒนา (Version) แสดงรายละเอียดเกี่ยวกับวัน เดือน ปี ที่พัฒนา วันที่อัพเดท ไม่ควรเลือกติดตั้ง Extension ที่ขาดการอัพเดทนานเกินไป รวมทั้งตรวจสอบความคิดของผู้ใช้งานร่วมด้วย

อ้างอิง

[25-1] http://gs.statcounter.com/#browser-TH-monthly-201101-201202

[25-2] http://www.theregister.co.uk/2012/03/25/chrome_web_store_malware_hijacks_facebook_profiles/

[25-3] http://arstechnica.com/business/news/2012/03/googles-chome-web-store-used-to-spread-malware.ars

[25-4] http://www.zdnet.com/blog/security/malicious-chrome-extensions-hijack-facebook-accounts/11074

[25-5] http://www.thehackernews.com/2012/03/facebook-profiles-can-be-hijacked-by.html

[25-6] http://www.securelist.com/en/blog/208193414/Think_twice_before_installing_Chrome_extensions

26 SECURE FTP SERVER

ผู้เขียน: เจษฎา ช้างสีสังข์

วันที่เผยแพร่: 5 เม.ย. 2555
ปรับปรุงล่าสุด: 5 เม.ย. 2555

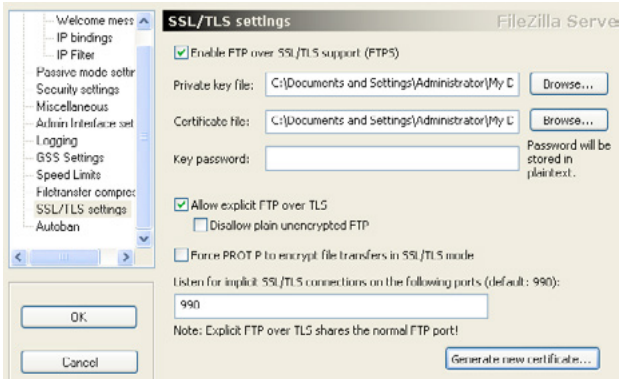
FTP (File Transfer Protocol) คือโพรโทคอลที่ออกแบบมาเพื่อใช้ในการรับส่งไฟล์ระหว่าง Client และ Server โดยจะมีพอร์ตที่ใช้งานอยู่ 2 พอร์ต คือ พอร์ต 20 ใช้ในการรับส่งไฟล์ ส่วนอีกพอร์ตคือ พอร์ต 21 ใช้ในการควบคุมหรือส่งคำสั่ง FTP เช่น ตรวจสอบการเข้าถึงโปรแกรมจากผู้ใช้งาน เป็นต้น และในปัจจุบันผู้ให้บริการ Web hosting โดยส่วนใหญ่มักจะให้บริการแลกเปลี่ยนไฟล์ผ่าน FTP Server เพราะการการติดตั้งระบบและการบริหารจัดการไฟล์ทำได้ง่าย

เนื่องจาก FTP เป็นโพรโตคอลที่รับส่งข้อมูลโดยไม่มีการเข้ารหัสลับ จึงทำให้ข้อมูลที่รับส่ง ไม่ว่าจะเป็น Username หรือ Password สามารถถูกดักรับ (Sniff) จากผู้ไม่หวังดีได้ [26-1] ซึ่งวิธีการแก้ไขนั้น ผู้ดูแลระบบควรเปลี่ยนมาใช้โพรโทคอลสำหรับแลกเปลี่ยนข้อมูลที่มีการเข้ารหัสลับข้อมูลที่รับส่งเสมอ ซึ่งมีโพรโทคอลที่ถูกออกแบบมาเพื่อแก้ปัญหาดังกล่าว คือ FTPS [26-2]

การใช้งาน FTP ที่มีการเข้ารหัสลับ

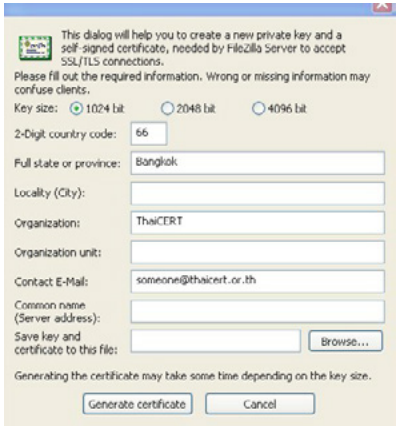
จากปัญหาที่ได้กล่าวข้างต้น ผู้ดูแลระบบจึงควรตั้งค่า FTP Server ให้รองรับการเข้ารหัสลับข้อมูล โดยในบทความนี้ จะยกตัวอย่างการตั้งค่าเพื่อใช้งานโพรโทคอล FTPS บนซอฟต์แวร์ FileZilla Server [26-3]

1. ผู้ดูแลระบบสามารถกำหนดให้ระบบรองรับ FTPS ได้ด้วยการคลิกที่เมนู Edit เลือก Settings จากนั้นเลือก SSL/TLS setting คลิกที่ช่อง Enable FTP over SSL/TLS support (FTPS) ดังรูปที่ 128 (26-1)



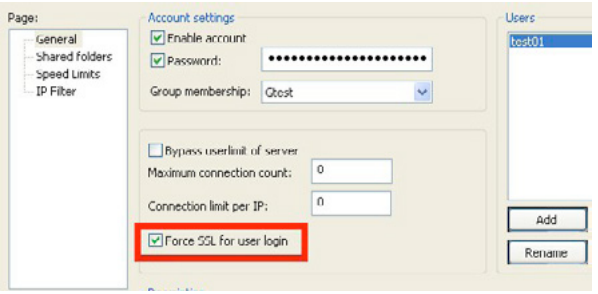
รูปที่ 128 (26-1) แสดงการตั้งค่าให้โปรแกรมรองรับ FTPS

2. ทำการกำหนดใบรับรองดิจิทัลให้กับซอฟต์แวร์ FTP Server เพื่อใช้ในกระบวนการเข้ารหัสลับข้อมูลที่ใช้รับส่งระหว่าง Server-Client ในกรณีที่ผู้ดูแลระบบมีใบรับรองดิจิทัลอยู่แล้ว สามารถใช้งานได้โดยระบุตำแหน่งของไฟล์ Certificate และไฟล์ Private key ให้กับระบบ แต่หากผู้ดูแลระบบยังไม่มีใบรับรองดิจิทัล สามารถสร้างขึ้นมาใหม่ได้โดยการคลิกที่ปุ่ม Generate new certificate จากนั้นใส่ข้อมูลของผู้ให้บริการ ดังที่แสดงตัวอย่างในรูปที่ 129 (26-2)



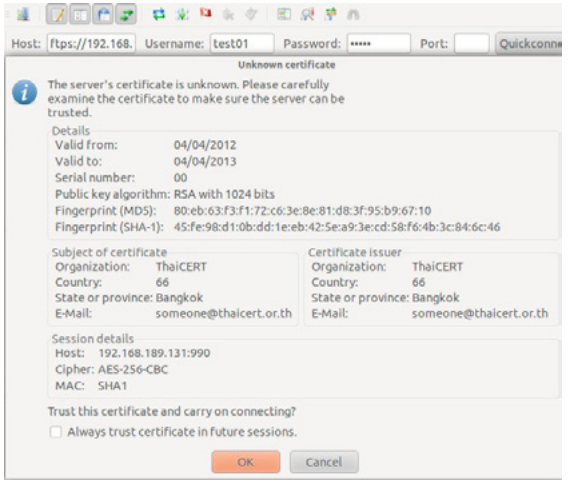
รูปที่ 129 (26-2) แสดงหน้าต่างการสร้างใบรับรอง

3. หากผู้ดูแลระบบต้องการบังคับให้ผู้ใช้ล็อกอินได้เฉพาะในโหมด FTPS เท่านั้น สามารถทำได้โดยการไปที่เมนู Edit เลือก Users จากนั้นคลิกที่ช่อง Force SSL for user login ดังรูปที่ 130 (26-3)



รูปที่ 130 (26-3) แสดงการตั้งค่าให้ User ล็อกอินด้วย FTPS เท่านั้น

4. ที่ฝั่ง Client ทดลองเชื่อมต่อไปยัง FTP Server โดยกำหนดค่า Host ขึ้นต้นด้วย ftps:// ในการเชื่อมต่อครั้งแรก ระบบจะแจ้งให้ผู้ใช้ทราบถึงใบรับรองของเครื่อง Server ที่จะใช้ในการเชื่อมต่อ หากผู้ใช้ยอมรับความถูกต้องของใบรับรองนี้ สามารถคลิกที่ปุ่ม OK เพื่อเริ่มการเชื่อมต่อ ดังรูปที่ 131 (26-4)



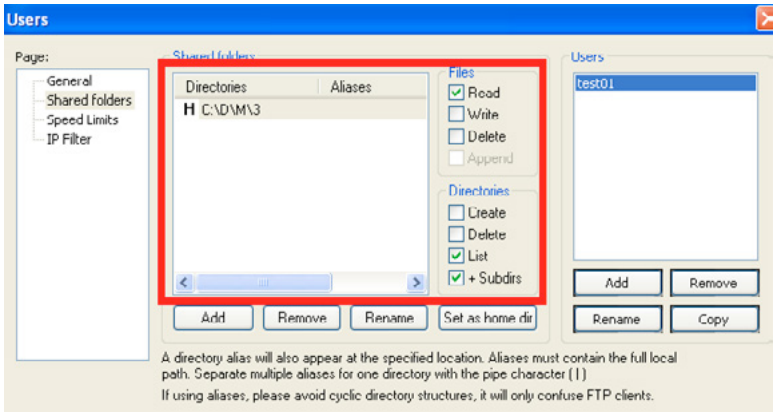
รูปที่ 131 (26-4) แสดงใบรับรองของเครื่อง Server

ข้อแนะนำเพิ่มเติม

อย่างไรก็ตาม นอกจากจะตั้งค่าให้ FTP Server รองรับการรับส่งข้อมูลที่มีการเข้ารหัสลับแล้ว ผู้ดูแลระบบควรมีการตั้งค่า Server ให้มีประสิทธิภาพด้วย เช่น การกำหนดสิทธิในการเข้าถึงระบบ การกำหนดพื้นที่การใช้งานให้กับผู้ใช้ ตามข้อแนะนำ [26-4][26-5][26-6] ดังนี้

1. กำหนดสิทธิในการเข้าถึงไฟล์ให้กับผู้ใช้งาน

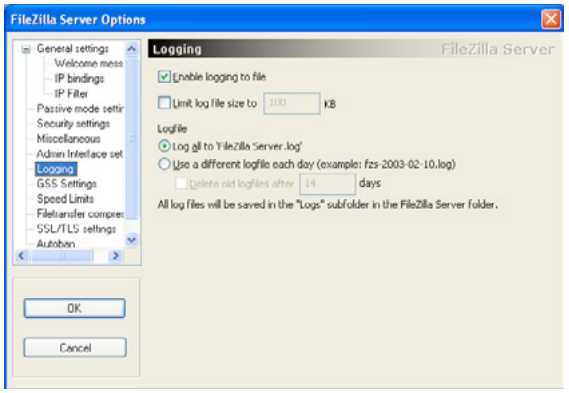
ในการกำหนดสิทธิในการเข้าถึงไฟล์ให้กับผู้ใช้งาน ผู้ดูแลระบบควรกำหนดสิทธิให้เท่าที่จำเป็นเท่านั้น จากรูปที่ 132 (26-5) เป็นการกำหนดสิทธิให้ผู้ใช้ชื่อ test01 สามารถดาวน์โหลดไฟล์ที่อยู่ภายใต้ไดเรกทอรี C:\D\M\3 ได้เท่านั้น



รูปที่ 132 (26-5) แสดงตัวอย่างการตั้งค่าสิทธิในการเข้าถึงไฟล์ให้กับผู้ใช้

๒. เปิดใช้งานการบันทึก Log

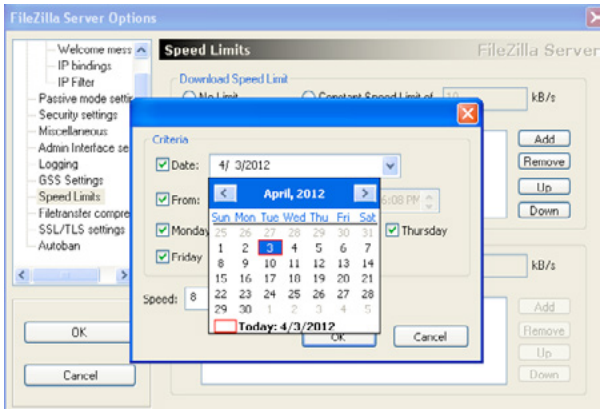
เป็นการตั้งค่าระบบให้บันทึกการทำงานต่างๆ ที่เกิดขึ้นกับระบบ เช่น การล็อกอินเข้าใช้งาน การดาวน์โหลดหรืออัพโหลดไฟล์ เป็นต้น การบันทึก Log ใช้เพื่อวิเคราะห์ในกรณีที่ระบบเกิดปัญหา เช่น การติดตามหา IP Address ของผู้ที่โจมตีระบบ นอกจากนี้ยังทำให้ระบบมีความสอดคล้องตาม พรบ.คอมพิวเตอร์ พ.ศ. 2550 ซึ่งได้ระบุว่า ผู้ให้บริการจะต้องสามารถระบุตัวตนของผู้ใช้งานได้ พร้อมเก็บข้อมูลการจราจรคอมพิวเตอร์ไม่น้อยกว่า 90 วัน ในระยะเวลา 1 ปี [26-7]



รูปที่ 133 (26-6) แสดงตัวอย่างการตั้งค่าให้ระบบรองรับการบันทึก Log

๓. จำกัดความเร็วของข้อมูลที่รับส่งระหว่าง Server-Client

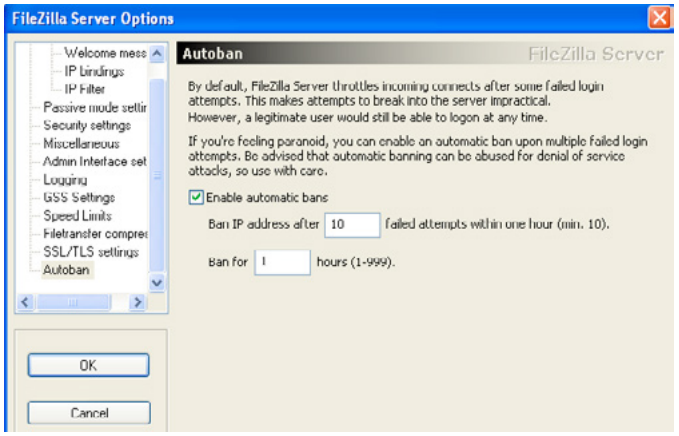
ผู้ดูแลระบบควรจำกัดความเร็วในการรับส่งข้อมูลให้กับระบบ เพื่อลดความเสี่ยงที่อาจเกิดความเสียหายต่อระบบ เช่น แบนด์วิธเต็มทำให้ไม่สามารถให้บริการอื่นๆ ได้ และยังเป็นการกำหนดความเร็วสูงสุดที่ระบบที่สามารถรองรับได้ ในบางซอฟต์แวร์นั้นยังสามารถกำหนดได้ว่าจะให้สามารถใช้ความเร็วเท่าใด ในช่วงวันเวลาต่างๆ ดังรูปที่ 134 (26-7)



รูปที่ 134 (26-7) แสดงตัวอย่างการตั้งค่าวันเวลาเพื่อกำหนดความเร็วให้กับระบบ

๔. ระงับบัญชีผู้ใช้ชั่วคราวหากล็อกอินผิดเกินจำนวนครั้งที่กำหนด

เพื่อป้องกันการโจมตีด้วย Brute Force Attack ผู้ดูแลระบบสามารถกำหนดให้โปรแกรม ทำการระงับบัญชีผู้ใช้ไม่ให้สามารถล็อกอินได้ในระยะเวลาหนึ่ง จากรูปที่ 135 (26-8) เป็นการตั้งค่าให้ระงับบัญชีผู้ใช้ทำการล็อกอินจาก IP Address เดียวกันเป็นระยะเวลา 1 ชม. หากพบว่ามีการล็อกอินที่ไม่ถูกต้องเกิน 10 ครั้ง



รูปที่ 135 (26-8) แสดงตัวอย่างการตั้งค่าการระงับบัญชีผู้ใช้

5. กำหนดขนาดพื้นที่การใช้งานให้กับผู้ใช้

การกำหนดขนาดพื้นที่การใช้งานให้กับผู้ใช้ เพื่อช่วยในการบริการจัดการพื้นที่ของระบบ และลดความเสี่ยงที่เกิดขึ้น เช่นใช้แก้ปัญหากรณีที่ผู้ใช้อัพโหลดไฟล์จำนวนมาก จนทำให้ระบบไม่สามารถรองรับได้

6. ปิดการล็อกอินแบบ Anonymous

ผู้ดูแลระบบควรปิดการล็อกอินแบบ Anonymous เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามายังระบบ

7. อัพเดทเวอร์ชันของซอฟต์แวร์ให้ใหม่อยู่เสมอ

ผู้ดูแลระบบควรติดตามข่าวสารด้านความมั่นคงปลอดภัยของซอฟต์แวร์ที่ ใช้ รวมถึงมีการตรวจสอบเวอร์ชันของซอฟแวร์ที่ใช้ และทำการอัพเดทให้เป็นเวอร์ชันล่าสุดอยู่เสมอ เพื่อทำให้ระบบมีประสิทธิภาพและลดปัญหาช่องโหว่ที่อาจเกิดขึ้นต่อระบบได้

สิ่งสำคัญที่ควรตระหนักในการแลกเปลี่ยนไฟล์ผ่าน FTP คือ การรักษาความลับของข้อมูลที่รับส่ง ดังนั้น ผู้ดูแลระบบจึงควรกำหนดให้มีการเข้ารหัสลับข้อมูล รวมถึงปรับแต่งค่าอื่นๆ เพิ่มเติม เพื่อให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้น

อ้างอิง

[26-1] http://searchsecurity.techtarget.com/tip/FTP-security-best-practices-for-the-enterprise

[26-2] http://tools.ietf.org/id/draft-murray-auth-ftp-ssl-00.txt

[26-3] http://wiki.filezilla-project.org/FTPS_using_Explicit_SSL/TLS_howto_%28Server%29

[26-5] http://www.windowsecurity.com/articles/secure_ftp_server.html

[26-6] http://blog.jscape.com/jscape/2008/06/best-practices.html

[26-7] http://www.g6ftpserver.com/forum/index.php?/topic/1214-hardening-your-ftp-server/

[26-8] http://www.ratchakitcha.soc.go.th/DATA/PDF/2550/E/102/5.PDF

27 MAC OS X คือเป้าหมายใหม่ของผู้สร้างมัลแวร์

ผู้เขียน: เสฏฐวุฒิ แสนนาม

วันที่เผยแพร่: 11 เม.ย. 2555
ปรับปรุงล่าสุด: 12 เม.ย. 2555

Mac OS X คือระบบปฏิบัติการที่ถูกพัฒนาขึ้นโดยบริษัท Apple Inc. สำหรับใช้งานบนเครื่องคอมพิวเตอร์ตระกูล Mac (Macintosh) เช่น iMac, MacBook ตัวระบบปฏิบัติการมีพื้นฐานมาจากระบบ UNIX จึงได้รับความน่าเชื่อถือในเรื่องของความเสถียรและความมั่นคงปลอดภัย ปัจจุบัน Mac OS X นั้นพัฒนามาถึงเวอร์ชัน 10.7 โดยใช้ชื่อว่า OS X Lion [27-1]

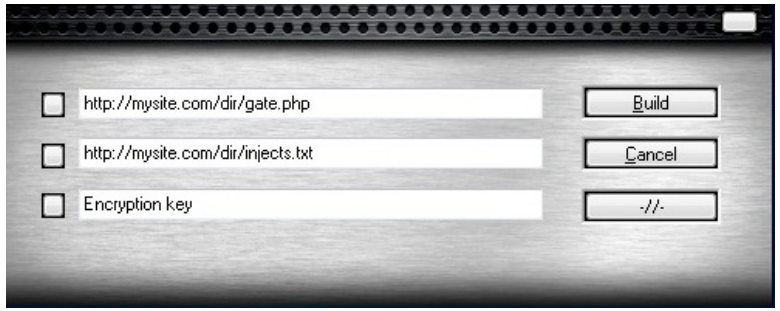
ในอดีตจุดเด่นข้อหนึ่งที่ Apple Inc. ใช้ในการโฆษณา Mac OS X ไม่ว่าจะเป็นข้อความโฆษณาในเว็บไซต์ของ Apple เอง [27-2] หรือโฆษณาทางโทรทัศน์ก็ตาม [27-3] คือการบอกว่า Mac นั้นปลอดภัยและปราศจากไวรัส เนื่องจากตัวระบบปฏิบัติการมีพื้นฐานมาจากระบบ UNIX ทำให้มัลแวร์บน Windows ไม่สามารถทำงานบน Mac OS X ได้อยู่แล้ว แต่สาเหตุที่แท้จริงคือจำนวนผู้ใช้งานระบบปฏิบัติการ Mac OS X นั้นยังมีไม่ถึง 10% จากจำนวนผู้ใช้ระบบปฏิบัติการคอมพิวเตอร์ทั้งหมด [27-4] ทำให้ไม่เป็นที่สนใจสำหรับแฮ็กเกอร์ในการที่จะพัฒนามัลแวร์ขึ้นมาเพื่อโจมตี ผู้ใช้งาน Mac OS X โดยเฉพาะ แต่ในปัจจุบัน หลังจากที่จำนวนผู้ใช้งานระบบปฏิบัติการ Mac OS X มีแนวโน้มที่จะเพิ่มมากขึ้น [27-5] ทำให้ผู้พัฒนามัลแวร์หลายรายมีแนวโน้มที่จะหันมาพัฒนามัลแวร์ลง Mac OS X

มัลแวร์ใน Mac OS X

จากข้อมูลของ F-Secure ซึ่งเป็นบริษัทพัฒนาซอฟต์แวร์ด้านความมั่นคงปลอดภัย พบว่า มัลแวร์ที่มีเป้าหมายเพื่อโจมตีผู้ใช้งาน Mac โดยตรงนั้นเริ่มปรากฏตัวเมื่อเดือนตุลาคม ปี 2007 โดย F-Secure เรียกโทรจันนี้ว่า Trojan:OSX/DNSChanger ซึ่งจะล่อลวงให้ผู้ใช้ติดตั้งโปรแกรมที่หลอกว่าเป็นปลั๊กอิน QuickTime เพื่อใช้สำหรับดูวิดีโอบนเว็บไซต์ จากนั้นจะแก้หมายเลข DNS Server ในเครื่องผู้ใช้ให้ชี้ไปที่ที่ผู้สร้างมัลแวร์ต้องการ [27-6] และหลังจากนั้นก็ได้มีการค้นพบมัลแวร์บน Mac มากขึ้นเรื่อยๆ มัลแวร์โดยส่วนใหญ่จะเป็นโทรจัน ซึ่งแพร่กระจายผ่านวิธี Social Engineer เช่น ในเดือนมกราคม ปี 2009 มีการค้นพบโทรจัน Trojan.

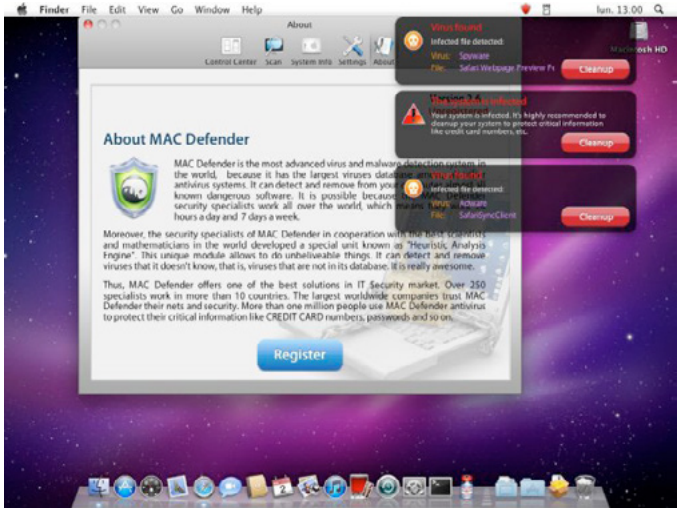
iServices.A ที่มาพร้อมกับโปรแกรม iWork '09 แบบละเมิดลิขสิทธิ์ที่แจกจ่ายผ่านระบบ Torrent [27-7] และต่อมาไม่นาน ก็มีการค้นพบโทรจัน Trojan.iServices.B ที่มาพร้อมกับโปรแกรม Adobe Photoshop CS4 แบบละเมิดลิขสิทธิ์เช่นกัน [27-8] จากเหตุการณ์ดังกล่าว ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจาก Symantec และ McAfee จึงได้ออกมาประกาศแจ้งเตือนให้กับผู้ใช้ Mac OS X ว่าได้ตกเป็นเป้าหมายของผู้พัฒนามัลแวร์แล้ว [27-9]

ในปี 2011 แฮ็กเกอร์ได้หันมาสนใจโจมตีผู้ใช้ Mac อย่างเต็มตัว โดยได้มีการพัฒนาเครื่องมือที่ใช้สำหรับ "สร้าง" มัลแวร์ เพื่อโจมตีระบบปฏิบัติการ Mac OS X โดยเฉพาะ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจาก CSIS Security Group ได้ค้นพบว่ามีซอฟต์แวร์ชื่อ Weyland-Yutani BOT ขายอยู่ในเว็บไซต์ใต้ดิน ซึ่งผู้ใช้ซอฟต์แวร์ดังกล่าวสามารถสร้างมัลแวร์ที่ขโมยข้อมูลผู้ใช้ด้วยการ แทรก Web form เข้ามาในเบราว์เซอร์ที่ทำงานบนระบบปฏิบัติการ Mac OS X ได้ [27-10] หน้าจอของซอฟต์แวร์ดังกล่าวเป็นดังรูปที่ 136 (27-1)



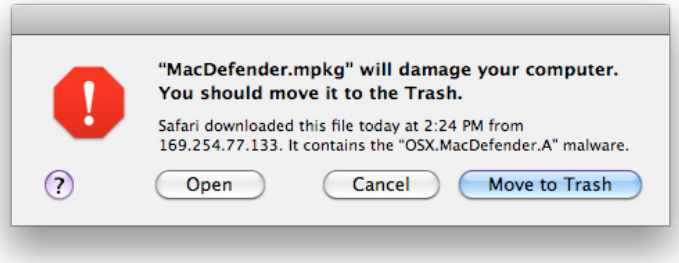
รูปที่ 136 (27-1) หน้าจอโปรแกรม Weyland-Yutani BOT [27-10]

หลังจากที่ผู้ใช้ Mac เริ่มถูกคุกคามจากมัลแวร์ จึงมีผู้พัฒนาซอฟต์แวร์รักษาความมั่นคงปลอดภัยบน Mac ออกมาหลายราย แฮ็กเกอร์จึงฉวยโอกาสนี้พัฒนาซอฟต์แวร์ชื่อ Mac Defender ซึ่งหลอกผู้ใช้ว่าเป็นโปรแกรมรักษาความมั่นคงปลอดภัย แต่ที่จริงแล้วเป็นโทรจันที่ขโมยข้อมูลส่วนตัวของผู้ใช้ เช่น หมายเลขบัตรเครดิต [27-11] ตัวอย่างหน้าตาของโปรแกรม Mac Defender เป็นดังรูปที่ 137 (27-2)



รูปที่ 137 (27-2) ตัวอย่างหน้าตาของโปรแกรม Mac Defender **[27-11]**

มัลแวร์ดังกล่าวนี้ถูกติดตั้งลงบนเครื่องของผู้ใช้ได้โดยง่าย ผ่านความสามารถของเบราว์เซอร์ Safari บน Mac OS X ที่จะเปิดไฟล์ที่ผู้ใช้ดาวน์โหลดสำเร็จให้โดยอัตโนมัติ ถึงแม้ก่อนการติดตั้งซอฟต์แวร์ดังกล่าว ระบบปฏิบัติการจะแสดงหน้าจอแจ้งเตือนว่าการกระทำนี้อาจเป็นอันตรายต่อระบบ และให้ผู้ใช้ป้อนรหัสผ่านเพื่อยืนยัน แต่ผู้ใช้ส่วนใหญ่ก็ไม่สนใจและยอมใส่รหัสผ่านเพื่อให้โปรแกรมได้ติดตั้งต่อ [27-12] จากปัญหาดังกล่าว Apple Inc. จึงได้ออกแพทช์มาเพื่อเพิ่มระบบตรวจสอบไฟล์ที่ผู้ใช้ดาวน์โหลดก่อนทำการเปิดไฟล์ โดยหากพบว่าไฟล์ที่ดาวน์โหลดมามีลักษณะที่น่าจะเป็นมัลแวร์ ระบบจะแนะนำให้ผู้ใช้ทำการลบไฟล์นั้นทันที [27-13] ดังรูปที่ 138 (27-3)



รูปที่ 138 (27-3) ตัวอย่างการแจ้งเตือนไฟล์ที่ไม่ปลอดภัย **[27-13]**

อัตราการแพร่ระบาดของมัลแวร์บน Mac OS X นั้นมีแนวโน้มที่จะเพิ่มมากขึ้นเรื่อยๆ จากข้อมูลของ iAntivirus ซึ่งเป็นผู้พัฒนาซอฟต์แวร์แอนตี้ไวรัสบน Mac พบว่า ปัจจุบันมีมัลแวร์บน Mac มากกว่า 100

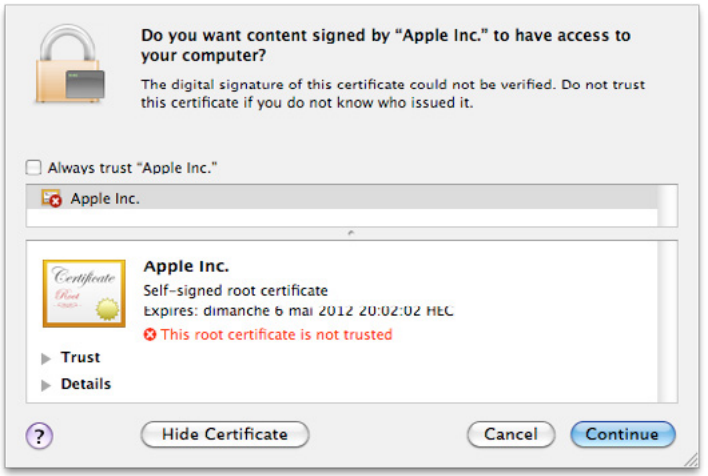
สายพันธุ์ ถึงแม้จะเป็นจำนวนที่น้อย แต่มัลแวร์ส่วนใหญ่ถูกจัดให้อยู่ในระดับความรุนแรงขั้นสูงสุดแทบทั้งสิ้น [27-14] หนึ่งในนั้นมีมัลแวร์ที่น่าสนใจคือโทรจันชื่อ Flashback

Flashback

มัลแวร์ Flashback ถูกค้นพบครั้งแรกเมื่อเดือนกันยายน 2011 โดยหลอกว่าเป็นตัวติดตั้งปลั๊กอิน Adobe Flash Player ในตอนนั้นยังไม่มีการสร้างความเสียหายอะไรเป็นพิเศษ นอกจากส่งข้อมูล MAC Address ของเครื่องผู้ใช้ออกไปยังเครื่อง Server และเปิดช่องทางให้ผู้โจมตีสามารถทราบได้ว่า เครื่องดังกล่าวติดมัลแวร์แล้ว [27-15] ในเวลานั้น Flashback ถูกจัดให้เป็นมัลแวร์ที่มีความอันตรายต่ำ ทำให้ Apple Inc. ไม่ได้ปล่อยแพทช์เพื่อตรวจสอบและกำจัดมัลแวร์นี้โดยทันที [27-16]

อย่างไรก็ตาม เนื่องจากมัลแวร์ Flashback มีความสามารถในการติดต่อกับเครื่อง Server เพื่ออัพเดทเวอร์ชันของตัวเองได้ ทำให้ในเวอร์ชันต่อๆ มา มัลแวร์ Flashback ได้ถูกเพิ่มความสามารถใหม่ๆ เข้ามาด้วย เช่น จะไม่ทำงานถ้าพบว่าถูกรันอยู่ในระบบที่เป็น Virtual Machine (ความสามารถ Anti-forensics) [27-17] รวมถึงปิดการทำงานของระบบ XProtect ซึ่งเป็นระบบป้องกันมัลแวร์บน Mac OS X และเขียนทับโปรแกรม XProtectUpdater เพื่อไม่ให้สามารถดาวน์โหลดแพทช์มากำจัดมัลแวร์สายพันธุ์ใหม่ๆ ได้อีก [27-18] ซึ่งความสามารถใหม่ๆ เหล่านี้ถูกพัฒนาเพิ่มเข้ามาในเวลาเพียง 1 เดือน และตอนนี้ Flashback มีเป้าหมายที่แน่นอนแล้ว นั่นคือ การขโมยข้อมูลส่วนตัวของผู้ใช้

ในเดือนกุมภาพันธ์ 2012 สายพันธุ์ใหม่ของมัลแวร์ Flashback ก็ได้ปรากฏขึ้น โดยในครั้งนี้ได้โจมตีผ่านช่องโหว่ของ Java เวอร์ชันเก่า (CVE-2011-3544 และ CVE-2008-5353) เมื่อผู้ใช้เข้าไปยังเว็บไซต์ที่มี Javascript เรียกใช้ Java-applet ที่โจมตีผ่านช่องโหว่ดังกล่าว จะปรากฏหน้าจอ Certificate ปลอมของ Apple Inc. ดังรูปที่ 139 (27-4) เพื่อหลอกให้ผู้ใช้ติดตั้งโปรแกรม ซึ่งหากผู้ใช้ติดตั้ง Java เวอร์ชันเก่าไว้ในเครื่อง (เวอร์ชันก่อนเดือนพฤศจิกายน 2011) มัลแวร์จะสามารถติดตั้งตัวเองลงในเครื่องของผู้ใช้ได้โดยที่ผู้ใช้ไม่สังเกต เห็นความผิดปกติเลย แต่หากเป็น Java เวอร์ชันใหม่ ระบบจะแจ้งเตือนว่า Certificate นั้นไม่น่าเชื่อถือ (Untrusted) แต่ผู้ใช้ก็ยังสามารถติดตั้งโปรแกรมดังกล่าวได้ อย่างไรก็ตาม กลุ่มผู้ใช้ที่โดนโจมตีผ่านช่องโหว่นี้โดยส่วนใหญ่จะเป็นผู้ใช้ Mac OS X เวอร์ชัน 10.6 ลงไป เนื่องจากใน Mac OS X เวอร์ชัน 10.7 นั้น Apple Inc. ได้ถอดโปรแกรม Java ออกจากระบบปฏิบัติการแล้ว [27-19]



รูปที่ 139 (27-4) หน้าจอ Certificate ปลอมของ Apple Inc. **[27-19]**

ในเดือนมีนาคม 2012 มัลแวร์ Flashback พัฒนาไปอีกขั้นด้วยการรับคำสั่งในการทำงานจาก Twitter ซึ่งต่างจากมัลแวร์สมัยก่อนที่จะระบุหมายเลข IP ของเครื่องที่ส่งคำสั่งไว้ในโค้ดของโปรแกรม ทำให้เครื่องนั้นสามารถตรวจพบและถูกสั่งปิดได้ง่าย [27-20] บริษัท Intego ผู้พัฒนาซอฟต์แวร์แอนตี้ไวรัส ได้ลองวิเคราะห์ข้อมูลของมัลแวร์ Flashback แล้วพบว่า มัลแวร์ตัวนี้น่าจะถูกสร้างโดยผู้พัฒนาเดียวกันกับ MacDefender [27-21]

ในวันที่ 2 เมษายน 2012 นักวิจัยจากบริษัท Dr.Web ซึ่งเป็นผู้พัฒนาซอฟต์แวร์ป้องกันไวรัส ได้รายงานการค้นพบสายพันธุ์ใหม่ของมัลแวร์ Flashback ซึ่งจะโจมตีผ่านช่องโหว่ของ Java (CVE-2012-0507) [27-22] โดยทาง Dr.Web คาดว่า มีเครื่อง Mac ที่ติดมัลแวร์ดังกล่าวไปแล้วไม่ต่ำกว่า 600,000 เครื่อง [27-23] สายพันธุ์ใหม่ของ Flashback ได้รับการตั้งชื่อว่า OSX/Flashback.K ซึ่งจะติดเข้าสู่เครื่องของผู้ใช้ผ่านการเปิดเว็บไซต์ที่มีโค้ดอันตรายฝังอยู่ ส่วนข้อมูลจากบริษัท F-Secure ระบุว่า ช่องโหว่ของ Java ที่มัลแวร์ใช้ในการโจมตีนั้น ถูกแก้ไขโดยบริษัท Oracle และได้เผยแพร่แพทช์เพื่อแก้ไขช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 กุมภาพันธ์ ปี 2012 แล้ว โดยเผยแพร่ทั้งบนระบบปฏิบัติการ Windows, Linux และ UNIX [27-24] [27-25] แต่บริษัท Apple Inc. กลับไม่ยอมปล่อยแพทช์ดังกล่าวผ่านระบบอัพเดท [27-26] จนกระทั่งวันที่ 4 เมษายน 2012 ถึงมีแพทช์เพื่อแก้ไขช่องโหว่ดังกล่าวออกมาทางระบบ Software Update ของ Mac OS X [27-27] และเมื่อวันที่ 6 เมษายน 2012 Software engineer จากบริษัท Garmin International ได้พัฒนาเครื่องมือ FlashbackChecker เพื่อใช้ในการตรวจสอบเครื่อง Mac ว่าติดมัลแวร์ Flashback หรือไม่ ซึ่งผู้ใช้สามารถดาวน์โหลดได้จากเว็บไซต์ https://github.com/jils/FlashbackChecker

No system is safe.

ปัจจุบัน Apple Inc. ได้พัฒนาระบบ Gatekeeper ซึ่งเป็นการกำหนดให้ผู้พัฒนาซอฟต์แวร์เข้ามาลงทะเบียนกับ Apple เพื่อรับ Developer ID และส่งซอฟต์แวร์มาให้ Apple เป็นผู้ตรวจสอบและ Sign ซอฟต์แวร์นั้น ก่อนที่จะเผยแพร่ให้กับผู้ใช้ ซึ่งระบบ Gatekeeper นี้จะเริ่มใช้ใน Mac OS X เวอร์ชัน 10.8 [27-28]

มัลแวร์บน Mac นั้นมีมานาน และมีแนวโน้มที่จะถูกพัฒนาต่อไปให้สามารถแพร่กระจายและสร้างความเสียหายได้ มากขึ้นเรื่อยๆ Flashback เป็นตัวอย่างที่ดีที่แสดงให้เห็นถึงความสามารถในการโจมตีผ่านช่องโหว่ต่างๆ ของระบบ ผู้ใช้งาน Mac OS X ไม่ควรนิ่งนอนใจ และควรหมั่นติดตามข่าวสารเรื่องความมั่นคงปลอดภัยอยู่เสมอ เพราะในตอนนี้ การที่คำโฆษณาของ Apple Inc. เปลี่ยนจาก “Mac ไม่มีไวรัส” มาเป็น “Mac ไม่ติดไวรัสของ PC” [27-29] นั้นเป็นสัญญาณเตือนที่ดีว่า ผู้ใช้ Mac อาจถึงเวลาที่จะต้องติดตั้งซอฟต์แวร์แอนตี้ไวรัสแล้วก็เป็นได้

อ้างอิง

[27-1] http://www.apple.com/macosx

[27-2] http://web.archive.org/web/20080319080218/

[27-3] http://www.youtube.com/watch?v=ZwQpPqPKbAw

[27-4] http://www.w3schools.com/browsers/browsers_os.asp

[27-5] http://www.cultofmac.com/139839/mac-market-share-continues-to-rise-while-pc-shipments-decline-report/

[27-6] http://www.f-secure.com/v-descs/trojan_osx_dnschanger.shtml

[27-7] http://www.macrumors.com/2009/01/22/iwork-09-torrent-carrying-os-x-trojan/

[27-8] http://us.norton.com/theme.jsp?themeid=ibotnet

[27-9] http://edition.cnn.com/2009/TECH/04/22/first.mac.botnet/index.html

[27-10] http://www.csis.dk/en/csis/blog/3195/

[27-11] http://www.pcworld.com/article/226846/fake_macdefender_brings_malware_to_macs.html

[27-12] http://www.zdnet.com/blog/bott/an-applecare-support-rep-talks-mac-malware-is-getting-worse/3342

[27-13] http://support.apple.com/kb/HT4651

[27-14] http://www.iantivirus.com/threats/

[27-15] http://arstechnica.com/apple/news/2011/09/mac-trojan-pretends-to-be-flash-player-installer-to-get-in-the-door.ars

[27-16] http://www.theregister.co.uk/2011/09/27/apple_updates_mac_malware_protection/

[27-17] http://www.theregister.co.uk/2011/10/13/mac_trojan_innovates/

[27-18] http://threatpost.com/en_us/blogs/flashback-trojan-now-disabling-mac-xprotect-101911

[27-19] http://www.h-online.com/security/news/item/Flashback-malware-uses-new-infection-technique-1442810.html

[27-20] http://www.intego.com/mac-security-blog/flashback-mac-malware-uses-twitter-as-command-and-control-center/

[27-21] http://www.intego.com/mac-security-blog/new-flashback-variant-changes-tack-to-infect-macs/

[27-22] http://news.drweb.com/?i=2341

[27-23] http://thehackernews.com/2012/04/more-than-600000-macs-system-infected.html

[27-24] https://www.f-secure.com/weblog/archives/00002341.html

[27-25] http://nakedsecurity.sophos.com/2012/02/15/oracle-java-and-adobe-shockwave-patches-for-february-too/

[27-26] http://nakedsecurity.sophos.com/2012/04/04/apple-patches-java-hole-that-was-being-used-to-compromise-mac-users/

[27-27] http://news.cnet.com/8301-13579_3-57410389-37/fighting-flashback-apple-issues-second-mac-update/

[27-28] http://www.apple.com/macosx/mountain-lion/security.html

[27-29] http://www.apple.com/why-mac/better-os/

28 WEB APPLICATION SECURITY รายสะดวก #1

ผู้เขียน: ไพชยนต์ วิมุกตะนันทน์
วันที่เผยแพร่: ๔ พ.ค. ๒๕๕๕
ปรับปรุงล่าสุด: ๔ พ.ค. ๒๕๕๕

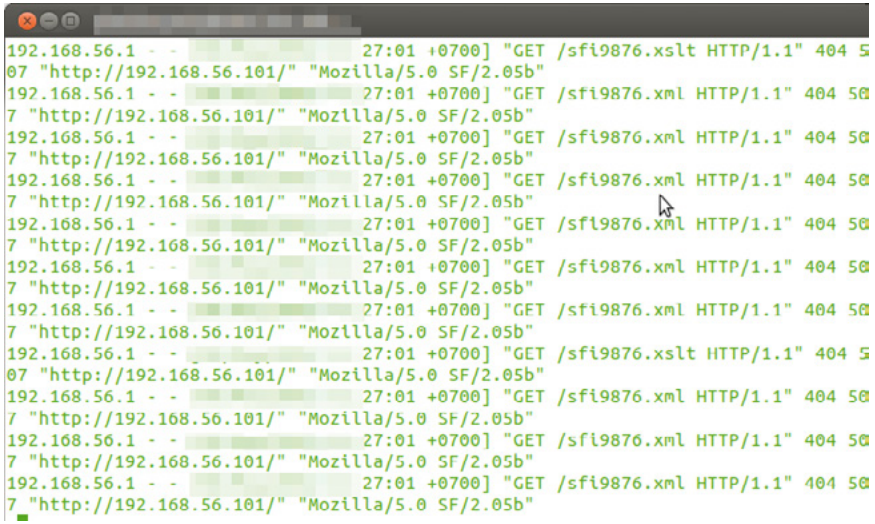
ขอออกตัวก่อนว่าบทความนี้อาจจะมีหลายๆ ส่วนที่อ้างอิงมาจากบทความเดิม http://www.thaicert.or.th/papers/technical/2012/pp2012te0001.html) ซึ่งไม่ได้มีรายละเอียดในเชิงลึกมากนัก ส่วนมากจะเป็นการแนะนำให้ทำอะไรบางอย่าง แต่ไม่ได้อธิบายว่าทำอย่างไรหรือทำไปเพื่ออะไร ดังนั้นบทความนี้จะนำข้อแนะนำเหล่านั้นมาขยายความให้ชัดเจนขึ้น เพื่อให้ผู้ที่อาจไม่มีประสบการณ์มากนักสามารถนำไปประยุกต์ใช้ หรือแม้แต่ทำตามตัวอย่างไปเลยได้อย่างง่ายดาย

ถ้าพูดถึง Web application ท่านผู้อ่านก็คงทราบดีอยู่แล้วว่าประกอบด้วยของ 2 อย่าง นั่นคือ Web server และ Application อย่างแรกก็ได้แก่ Apache และ IIS ที่เรารู้จักกันดี เดี๋ยวนี้อาจจะมีตัวอื่นเข้ามาปนบ้าง เช่น lighttpd หรือ nginx หรือพวกที่กลายพันธุ์ไปอย่าง Apache Tomcat แต่ก็อยู่ในพื้นฐานเดียวกันทั้งสิ้น ส่วนอย่างหลังก็ได้แก่ PHP, JSP และ ASP เป็นหลัก และก็มีตัวอื่นๆ เช่น Ruby, C#, python รวมถึงของเก่าที่ยังเชื่อถือได้เสมออย่าง perl ก็ยังมีการใช้งานอยู่ไม่น้อย

แต่ไม่ว่าส่วน Application นี้จะเป็นอะไรก็ตาม ส่วนแรกคือ Web server ก็ยังทำงานเหมือนเดิมเสมอ ไม่มีการเปลี่ยนแปลง นั่นคือทำหน้าที่เป็นสื่อกลางระหว่างผู้ใช้งานกับ Application เบื้องหลัง และในกรณีที่มีการโจมตี Web application เกิดขึ้น Web server นี้เอง ก็จะเป็นพยานปากสำคัญ ที่มองเห็นเหตุการณ์การโจมตีโดยตลอด และเก็บบันทึกรายละเอียดเอาไว้ใน Log file ดังที่หลายๆ ท่านอาจจะได้เรียนรู้ความสำคัญของ Log file จากประสบการณ์จริงกันมาแล้ว เมื่อ Web application ของท่าน ตกเป็นเป้าหมายของเหล่าผู้ไม่ประสงค์ดี

แต่การที่รู้ว่าถูกโจมตีหลังจากถูกโจมตีสำเร็จแล้วก็ไม่น่าจะดีเท่าไหร่ ถึงแม้การที่ได้ทราบรายละเอียดการโจมตีอย่างละเอียดจาก Log จะช่วยให้ท่านสามารถแก้ไขช่องโหว่ได้อย่างถูกต้องครบถ้วนมากขึ้น สิ่งที่ดีกว่านั้นก็คือ ท่านสามารถรู้ได้ก่อนที่การโจมตีจริงๆ จะเกิดขึ้น หรือแม้แต่ก่อนที่การโจมตีจะสำเร็จ ซึ่งทั้งหมดนี้ อาจจะทำได้โดยการพิจารณาจาก Log ของ Web server นั่นเอง

ถ้า Web application ของท่านไม่ได้มีช่องโหว่ (Vulnerability) ชนิดที่รู้กันอยู่แล้วจนมีผู้สร้างเครื่องมือโจมตี (Exploit) แจกจ่ายกันอย่างแพร่หลาย คือท่านเป็นผู้ดูแลระบบที่มีความระมัดระวังตามสมควรอยู่แล้วนั่นเอง สิ่งแรกที่ผู้ไม่ประสงค์ดีมักจะทำก่อนที่จะโจมตีท่านก็คือ การตรวจสอบระบบของท่านเพื่อรวบรวมข้อมูล (Information gathering) การกระทำนี้บางครั้งอาจเรียกว่าการ Probe หรือ Scan หรือบางครั้งอาจเรียกว่า Footprinting สำหรับวิธีการก็มีได้หลากหลาย ส่วนมากมักจะใช้เครื่องมืออัตโนมัติเช่น Nikto, W3af หรือ Skipfish ซึ่งเป็นเครื่องมือที่มีการแจกจ่ายอย่างไม่คิดมูลค่าบน Internet



รูปที่ 140 (28-1) แสดง Log ของ Apache ที่ถูก Scan ด้วยโปรแกรม Skipfish

ตัวอย่างที่แสดงให้เห็นจากโปรแกรม Skipfish ข้างต้นนั้น อาจจะเห็นได้ค่อนข้างชัดเจนเนื่องจากเป็นการ Scan โดยไม่ได้มีการปรับแต่งค่าการทำงานใดๆ ของโปรแกรม Skipfish เลย และทำการทดลองในเครื่องแม่ข่ายที่ไม่มีการใช้งานจริง แต่ในกรณีที่เป็นเครื่องแม่ข่ายหลักที่มีผู้เข้ามาใช้บริการเป็นจำนวนมาก และผู้ไม่ประสงค์ดี ที่ต้องการหาช่องโหว่ใน Web application ของท่าน มีการปรับแต่งค่าให้โปรแกรมทำงานในลักษณะที่ทำให้สังเกตเห็นได้ยากขึ้น เช่น เปลี่ยนค่า User Agent ให้เป็นของ Web browser จริง (ในตัวอย่างเป็น Mozilla/5.0 SF/2.05b ซึ่งเป็นของ Skipfish โดยเฉพาะ) และปรับการทำงานให้ช้าลง แทนที่จะ Scan ด้วยความอัตราความเร็วหลายสิบครั้งใน 1 วินาทีตามตัวอย่าง เพื่อให้ผลของการ Scan ดูกลมกลืนไปกับการใช้งานจริงบนเครื่องแม่ข่าย ดังนั้นหากท่านกลับไปดู Log ของ Web server ของท่านในวันนี้ ท่านอาจไม่สามารถสังเกตเห็นความผิดปกติอะไรเลย ทั้งๆ ที่อาจจะมีผู้ไม่ประสงค์ดี ทำการ Scan ไปแล้วหลายต่อหลายครั้งก็ตาม

แต่การตรวจสอบในรูปแบบนี้ ไม่ว่าจะตั้งค่าโปรแกรมอย่างไรก็ตาม สิ่งที่ต้องเกิดขึ้นอย่างแน่นอนก็คือ 404 error ซึ่งจะเกิดขึ้นเมื่อโปรแกรมที่ตรวจหาช่องโหว่เหล่านี้ พยายามเดาชื่อไฟล์ที่อาจมีอยู่ในระบบ โดยไฟล์เหล่านี้อาจเป็นช่องโหว่ ที่สามารถนำมาใช้เป็นประโยชน์ในการเจาะเข้าสู่ระบบจริงๆ ได้ ชื่อไฟล์ที่

โปรแกรมเหล่านี้นำมาลองเดา อาจจะมาจากฐานข้อมูลที่มีการรวบรวมเอาไว้ล่วงหน้า ว่าเป็นไฟล์ที่มักจะเป็นช่องโหว่ หรือมีข้อมูลที่น่าสนใจ หรืออาจเป็นการเดาในลักษณะ Brute-force ก็ได้ ผลลัพธ์ของการเดาชื่อไฟล์ มักจะผิดมากกว่าถูก และทุกครั้งที่ผิด Web server ก็จะบันทึกเอาไว้ใน Log ว่าเป็น 404 error ซึ่งแปลว่า file not found นั่นเอง

Log ของการ Scan ของโปรแกรมเหล่านี้อาจจะดูว่ามีปริมาณมาก (ในตัวอย่างมีประมาณ 10000 บรรทัด เป็น 404 ประมาณ 1200 บรรทัด) แต่เมื่อเทียบกับ Log ของ Web server ที่มีจำนวนผู้เข้าชมจำนวนมากๆ แล้ว ก็อาจเรียกได้ว่าเป็นแค่ส่วนเล็กๆ ในจำนวน Log มหาศาล ดังนั้นจะตรวจหาความผิดปกตินี้ได้อย่างไร ท่านผู้อ่านที่คุ้นเคยกับเครื่องมือใน Unix อาจจะนึกถึงเครื่องมือ grep และ wc ซึ่งต้องอาศัยความรู้ในการเขียน grep pattern ที่เหมาะสมและต้อง login เข้าไปใน Web server หรืออุปกรณ์ที่เก็บ Log ทุกครั้งที่ต้องการตรวจสอบ นอกจากไม่สะดวกแล้ว หากพบว่ามีสิ่งผิดปกติอยู่ใน Log ท่านก็ยังต้องดำเนินการเองอีกด้วย เช่น Block IP address ต้องสงสัยที่ Firewall หรือเขียน ACL บน Apache เอง ซึ่งอาจจะล่าช้าไม่ทันการ หรือเกิดความผิดพลาดได้โดยง่าย

เพื่อช่วยให้การตรวจสอบความผิดปกติใน Log เป็นไปโดยอัตโนมัติ และสามารถทำการรับมือ (Mitigate) กับการโจมตีได้โดยอัตโนมัติด้วย สิ่งที่จำเป็นต้องมีก็คือโปรแกรมประเภท Log monitoring หรือบางท่านอาจจะจัดว่าเป็น Host-based IPS ประเภทหนึ่ง ซึ่งโปรแกรมเหล่านี้จะทำการตรวจสอบ Log ที่กำหนดเป็นระยะๆ เมื่อพบว่ามีรายการ Log ที่ผิดปกติตามเงื่อนไขที่เรากำหนด มันก็จะดำเนินการตามคำสั่งที่เรากำหนดไว้ล่วงหน้า เช่นท่านอาจกำหนดให้โปรแกรมดังกล่าว คอยตรวจสอบสถานะ 404 บน Log ของ Apache โดยระบุเงื่อนไขว่า หากมีรายการ 404 จาก IP เดียวกันตั้งแต่ 20 ครั้งใน 1 วินาที ให้สั่ง Block IP address นั้นด้วย iptables ทันที

ตัวอย่างของโปรแกรมประเภทนี้ตัวหนึ่ง ได้แก่ Fail2Ban (http://www.fail2ban.org) ซึ่งถูกออกแบบมาให้ป้องกันการโจมตีประเภท Brute-force โดยอาศัย iptables เป็นตัว block การโจมตี ซึ่งในกรณีนี้ เราจะกำหนดเงื่อนไขให้ Fail2ban ตรวจสอบ Apache log ที่มีผลลัพธ์เป็น 404 error (file not found) ที่มีความถี่มากกว่า 20 ครั้งต่อ 1 วินาที โดยใช้รูปแบบของ configuration ดังต่อไปนี้

```
# Fail2Ban configuration file

# Modified from https://rem.co/en/article/fail2ban-
phpmyadmin-script/ - PHPMyAdmin protection rules


[Definition]


failregex = <HOST> -.*"(GET|POST) .*" 404 .*

ignoreregex =
```

สำหรับผู้ใช้งาน Debian GNU/Linux และ Ubuntu ให้บันทึกไฟล์นี้เป็นชื่อ /etc/fail2ban/filter.d/apache-404.conf ส่วนผู้ใช้งาน Distribution อื่นให้ตรวจสอบตำแหน่งที่เก็บไฟล์ filter ของ Fail2ban จากคู่มือของ Distribution นั้นๆ

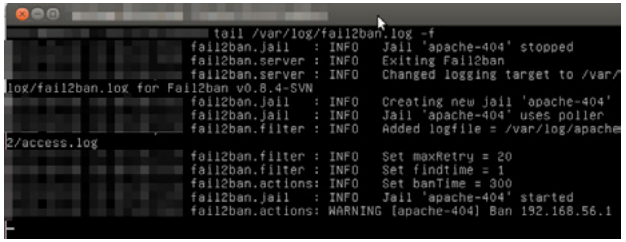
ขั้นต่อไป ให้ตรวจสอบว่า Apache ที่ท่านใช้งานอยู่ เก็บ Log (access log) ไว้ที่ใด (ในที่นี้สมมุติให้เป็น /etc/apache2/access.log) เมื่อทราบแล้ว ให้เพิ่มรายการนี้ในไฟล์ /etc/fail2ban/jail.conf และเช่นเดียวกับ สำหรับผู้ใช้งาน Linux Distribution อื่นที่ไม่ใช่ Debian หรือ Ubuntu ให้ตรวจสอบตำแหน่งที่เก็บไฟล์ jail.conf ของ Fail2ban จากคู่มือของ Distribution นั้นๆ

```
[apache-404]


enabled = true
port = http,https
filter = apache-404
logpath = /var/log/apache2/access.log
maxretry = 20
findtime = 1
bantime = 300
```

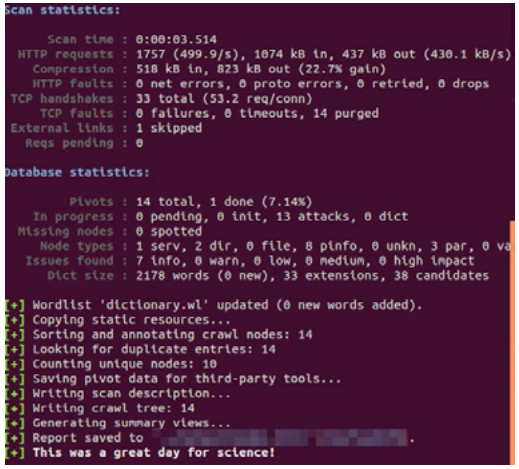
bantime คือช่วงเวลาที่จะให้ Fail2ban block การเข้าถึงจาก IP ที่ถูกตรวจพบว่าพยายามโจมตีระบบตามเงื่อนไขที่กำหนด โดยมีหน่วยเป็นวินาที หากกำหนดเป็นค่าติดลบ จะหมายถึงให้ Fail2ban ทำการ block IP นั้นๆ ตลอดไป และอย่าลืมว่า ตัวเลข 20 ครั้งต่อ 1 วินาทีเป็นการสมมุติขึ้น เพื่อให้เห็นได้ชัดเจนในการทดลอง ในชีวิตจริงอาจมีค่าที่ต่ำกว่านี้มาก เนื่องจากผู้ไม่ประสงค์ดีต้องการหลบหลีกการตรวจจับดังที่กล่าวไว้ข้างต้น

เมื่อกำหนดค่าให้ Fail2ban ตามตัวอย่างแล้ว ผู้เขียนก็จะมาลอง Scan ระบบด้วย Skipfish ดูอีกครั้ง ก็พบว่า Fail2ban สามารถตรวจพบการโจมตีตามเงื่อนไข คือมี 404 error จาก IP เดียวกัน 20 ครั้งต่อวินาที และทำการ block ได้สำเร็จ



รูปที่ 141 (28-2) แสดงการทำงานของ Fail2ban จาก Log ของโปรแกรม

และเมื่อมาดูในฝั่ง Skipfish ก็จะพบว่า การ Scan ถูก block ภายในเวลาประมาณ 3.5 วินาทีเท่านั้น



รูปที่ 142 (28-3) แสดงการทำงานของ Skipfish เมื่อทำการ Scan เครื่องแม่ข่ายที่ป้องกันไว้แล้ว

จากการทดลอง จะเห็นได้ว่า Fail2ban สามารถป้องกันการทำ Information gathering ด้วยวิธี URL scanning หรือ URL bruteforcing ได้ผลในระดับหนึ่ง แต่อย่างไรก็ตาม หากผู้ไม่ประสงค์ดีใช้รูปแบบการ Scan หรือ Probe วิธีอื่นๆ หรือในกรณีที่ของระบบที่มีช่องโหว่ที่รู้จักกันดีอยู่แล้ว ผู้ไม่ประสงค์ดีก็อาจจะทำการโจมตีได้โดย Fail2ban ไม่สามารถตรวจจับและป้องกันได้ นอกจากนี้ ระบบตรวจจับการโจมตีทุกชนิดย่อมมีโอกาสที่จะเกิดความผิดพลาดในลักษณะที่เรียกว่า False positive ได้ นั่นคือเป็นการใช้งานปกติที่ถูกเข้าใจผิดว่าเป็นการโจมตี และถูก block อย่างไม่ควรจะเป็น สำหรับตัวอย่างที่แสดงนี้อาจเกิดได้จากผู้พัฒนาเว็บไซต์ของท่านเอง ที่อาจสร้าง html page ที่มี dead link จำนวนมากโดยไม่รู้ตัว ทำให้ผู้ที่เข้ามาชมเว็บไซต์นั้นตามปกติถูก block เนื่องจากเกิด 404 error ขึ้นมากเกินค่าที่กำหนดโดยไม่ได้ตั้งใจ

และถึงแม้เมื่อท่านติดตั้ง Fail2ban ไปแล้วและได้ผลเป็นที่น่าพอใจ ท่านก็ควรที่จะพิจารณาการป้องกัน Web application ของท่านด้วยมาตรการอื่นๆ ด้วย ทั้งนี้อาศัยแนวคิดเรื่อง Defense-in-depth หรือ Layered defense ซึ่งผู้เขียนจะนำวิธีการป้องกันแบบอื่นๆ มาเสนอให้ท่านได้ทราบในโอกาสต่อไป

29 FLAME

ผู้เขียน: เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่: 8 มิ.ย. 2555
ปรับปรุงล่าสุด: 12 มิ.ย. 2555

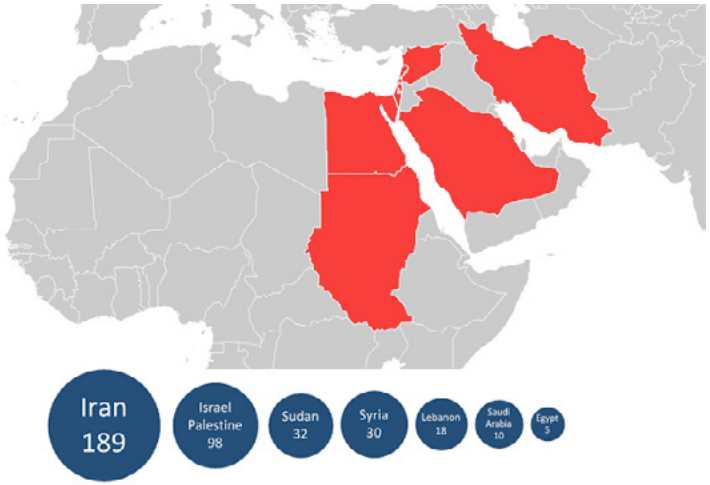
Discovery

เมื่อวันที่ 28 พ.ค. 2555 หน่วยงาน CERT ของประเทศอิหร่าน (MAHER) รายงานว่า ได้ค้นพบมัลแวร์ชนิดใหม่ที่มีเป้าหมายเพื่อโจมตีประเทศอิหร่าน โดยได้เรียกมัลแวร์ตัวนี้ว่า Flame ในเบื้องต้น ทาง MAHER ได้สันนิษฐานว่า Flame ถูกพัฒนาขึ้นโดยผู้พัฒนาทีมเดียวกับ Stuxnet และ Duqu

Flame ทำงานได้บน Windows XP, Vista และ 7 ใช้วิธีการแพร่กระจายผ่านทาง USB Drive และแพร่ผ่านระบบเครือข่าย (ซึ่งเป็นวิธีเดียวกันกับ Stuxnet) การทำงานหลักๆ ของ Flame คือขโมยข้อมูล Username และ Password, ลักลอบอัดเสียง, บันทึก Screenshot และลักลอบส่งข้อมูลออกไปให้ C&C Server ผ่านทางพอร์ต SSH และ HTTPS [29-1]

ศูนย์วิจัย CrySyS (Laboratory of Cryptography and System Security) จาก Budapest University of Technology and Economics เรียกมัลแวร์ตัวนี้ว่า Skywiper และได้ให้ข้อมูลเพิ่มเติมว่า ได้รับแจ้งเหตุการโจมตีด้วยมัลแวร์ดังกล่าวนี้จากหลายๆ ประเทศทั่วโลก ไม่ใช่แค่เฉพาะในตะวันออกกลางอย่างเดียว นอกจากนี้ยังได้ค้นพบวิธีที่ Skywiper ใช้ในการซ่อนตัวเองไม่ให้ถูกตรวจจับโดยโปรแกรมแอนตี้ไวรัส โดยการซ่อนโค้ดไว้ในไฟล์ .ocx และ .tmp ซึ่งโปรแกรมแอนตี้ไวรัสโดยส่วนใหญ่จะไม่สแกนไฟล์ 2 ชนิดนี้ [29-2] CrySyS รายงานว่า การพัฒนามัลแวร์ดังกล่าวนี้น่าจะได้รับการสนับสนุนด้านการเงินจากรัฐบาลหรือประเทศที่มีความต้องการที่จะใช้มัลแวร์ในการทำ Cyber Warfare (เอกสารของ CrySyS)

นักวิจัยจาก Kaspersky Lab ได้รายงานข้อมูลเพิ่มเติมว่า ประเทศที่ตกเป็นเป้าหมายของการโจมตี ได้แก่ อิหร่าน เลบานอน ซีเรีย อิสราเอล และประเทศอื่นๆ ในแถบตะวันออกกลาง ตามรูปที่ 143 (29-1)



รูปที่ 143 (29-1) ประเทศที่ตกเป็นเป้าหมายการโจมตีของ Flame (ที่มา: Securelist.com)

จากการวิเคราะห์ของ Kaspersky พบว่า Flame มีส่วนประกอบการทำงานหลายๆ ส่วนรวมอยู่ด้วยกัน เช่น Backdoor, Trojan รวมถึงส่วนที่เป็นการทำงานแบบ Worm ซึ่งใช้ในการแพร่กระจายตัวเองผ่านระบบเครือข่าย ทำให้ตัวมัลแวร์มีขนาดใหญ่ถึง 20 MB จึงยากต่อการวิเคราะห์

Kaspersky พบว่า ผู้สร้าง Flame ได้ปลอมแปลงวันเวลาที่สร้างไฟล์ เพื่อให้เกิดความยุ่งยากในการตรวจสอบ โดยวันเวลาที่สร้างไฟล์นั้นอาจจะเป็นไปได้ตั้งแต่ปี 1992, 1994, 1995 หรือปีอื่นๆ แต่โมดูลส่วนใหญ่ของมัลแวร์ถูกสร้างในปี 2011 และ 2012 จากการวิเคราะห์ของ Kaspersky คาดว่า Flame น่าจะถูกสร้างขึ้นในช่วงเดือนกุมภาพันธ์-มีนาคม ปี 2010 [29-3]

Symantec ได้รายงานการค้นพบมัลแวร์นี้ด้วยเช่นกัน และได้เรียกมัลแวร์ตัวนี้ว่า Flamer หลังจากที่ได้วิเคราะห์มัลแวร์ตัวนี้ ทำให้ทราบข้อมูลเพิ่มเติมว่า มีการโจมตีไปที่ยุโรปตะวันออกด้วย และยิ่งไปกว่านั้น Flamer นอกจากจะขโมยข้อมูลแล้ว ยังทำหน้าที่ขัดขวางการส่งออกน้ำมันของประเทศอิหร่าน โดยการ Shut down ระบบ Oil terminal ด้วย [29-4] [29-5]

Certificate

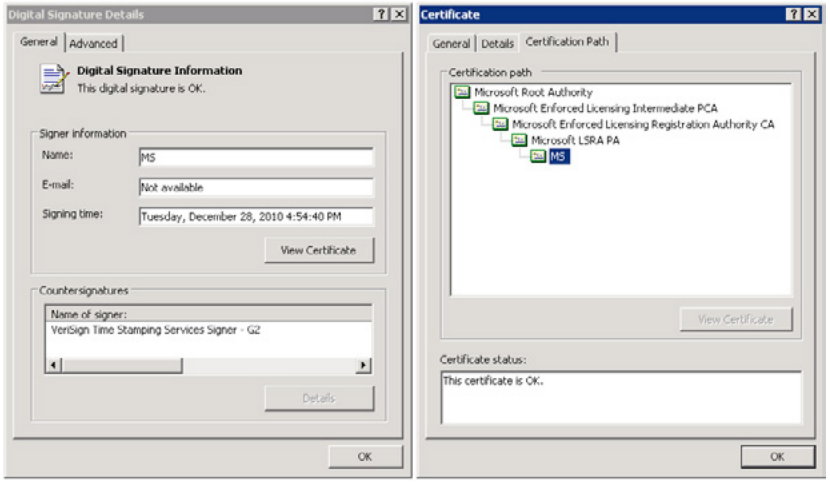
หลังจากที่มีการวิเคราะห์มัลแวร์โดยหน่วยงานต่างๆ เพื่อหาวิธีการทำงานและวิธีการเผยแพร่ ในวันที่ 3 มิ.ย. 2555 Microsoft ได้แจ้งเตือน Security Advisory หมายเลข 2718704 ว่าด้วยเรื่องของการปลอม Digital Certificate ของ Microsoft ซึ่ง Certificate ดังกล่าวนี้ถูกใช้ในการ Sign โค้ดของ Flame [29-6]

โค้ดของ Flame ถูก Sign โดย Microsoft Terminal Server Licensing Service ซึ่งเป็นระบบที่ใช้ในการยืนยันตัวตนในกรณีที่จะเข้าไปใช้งาน Remote Desktop Service ในองค์กร ระบบดังกล่าวนอกจากจะออก Certificate ได้แล้ว ยังสามารถ Sign โค้ดให้กับโปรแกรมได้ด้วย

ในเบื้องต้น Microsoft แจ้งว่า เหตุการณ์ดังกล่าวเกิดจากช่องโหว่ของ Cryptography algorithm รุ่นเก่า ซึ่งทำให้ผู้สร้างมัลแวร์สามารถ Sign โค้ดของโปรแกรมให้ดูเหมือนกับว่าโปรแกรมนั้นถูกพัฒนาและได้รับการรับรองจาก Microsoft แต่ในตอนนั้นยังไม่ได้ให้รายละเอียดเพิ่มเติมของช่องโหว่ดังกล่าว [29-7]

ผู้เชี่ยวชาญด้าน Security ได้วิเคราะห์ว่า ช่องโหว่ของการ Sign โค้ด เกิดจากการที่ Microsoft Certificate Authority (CA) ใช้อัลกอริทึม MD5 ในการ Sign Certificate ซึ่งอัลกอริทึมดังกล่าวมีปัญหาเรื่อง Hash Collision ทำให้แฮ็กเกอร์สามารถสร้าง Certificate ปลอมที่มี MD5 Hash ตรงกับ Hash ของ Microsoft แล้วส่งเข้ามายัง Terminal Server เพื่อให้ Sign โค้ดของ Flame โดยใช้ Certificate จริงของ Microsoft ได้ [29-8] [29-9]

Certificate ที่ถูกใช้ในการ Sign โค้ดของ Flame คือ Microsoft Enforced Licensing Intermediate PCA ซึ่งถูก Sign โดย Microsoft Root Authority และ Microsoft Enforced Licensing Registration Authority CA (SHA1) ซึ่งถูก Sign โดย Microsoft Root Certificate Authority [29-10] ตัวอย่าง Certificate ดังกล่าวเป็นดังรูปที่ 144 (29-2)



รูปที่ 144 (29-2) Certificate ของ Microsoft ที่ถูกใช้ใช้การ Sign โค้ดของ Flame (ที่มา: F-Secure)

Microsoft ได้ปิดความสามารถในการออก Certificate ผ่าน Terminal Server และได้เผยแพร่ Update หมายเลข **2718704** เพื่อ Revoke Certificate ดังกล่าว

ในวันที่ 6 มิ.ย. Microsoft ได้อธิบายรายละเอียดเพิ่มเติมของวิธีการที่ Flame ใช้ในการโจมตีระบบ Certificate ผู้ที่สนใจสามารถอ่านรายละเอียดเพิ่มเติมได้ที่ เว็บไซต์ Technet

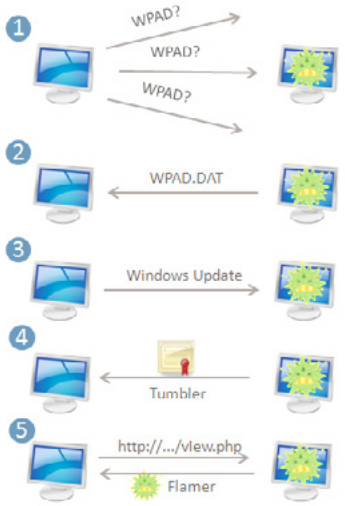
Windows Update

จุดประสงค์ที่แท้จริงของการ Sign โค้ดของมัลแวร์ด้วย Certificate ของ Microsoft คือการเผยแพร่มัลแวร์ผ่านระบบ Windows Update

เครื่องที่ติด Flame จะตั้งตัวเองเป็นเซิร์ฟเวอร์ Web Proxy Autodiscovery Protocol (WPAD) โดยปกติแล้ว เครื่องคอมพิวเตอร์ที่ใช้ Windows จะถูกตั้งค่า Proxy ให้เป็น Automatic proxy detection หลังจากที่เชื่อมต่อกับระบบเครือข่าย เครื่องดังกล่าวจะพยายามติดต่อกับเซิร์ฟเวอร์ wpad.DOMAINNAME (เช่น wpad.thaicert.or.th ในกรณีที่เครื่องดังกล่าวอยู่ในโดเมน thaicert.or.th) เพื่อตรวจสอบว่าเมื่อไหร่ที่ควรจะเชื่อมต่อ HTTP Proxy เพื่อใช้งาน Windows Update

เครื่องคอมพิวเตอร์ที่ติด Flame จะส่งไฟล์ wpad.dat เพื่อเป็นสัญญาณบอกเครื่องที่อยู่ในเครือข่ายเดียวกันว่าให้เชื่อมต่อ Proxy เพื่อใช้งาน Windows Update จากนั้นเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่าย จะเชื่อมต่อเข้ามายังเครื่องที่ติด Flame เพื่อดาวน์โหลดไฟล์ Windows Update

โดยปกติแล้วระบบ Windows Update จะมีการตรวจสอบ Signature ของไฟล์ที่จะนำมาอัพเดท เพื่อให้แน่ใจว่าเป็นไฟล์ที่มาจาก Microsoft จริงๆ และเนื่องจาก Flame ถูก Sign โดยใช้ Certificate ของ Microsoft จึงสามารถแพร่กระจายตัวเองผ่านระบบ Windows Update ได้ [29-11] [29-12] ขั้นตอนการทำงานของ Flame เป็นดังรูปที่ 145 (29-3)



รูปที่ 145 (29-3) การแพร่กระจายของ Flame ผ่านระบบ Windows Update (ที่มา: Symantec)

Suicide

ในวันที่ 4 มิ.ย. 2555 Kaspersky รายงานว่าเครื่อง C&C ของ Flame เป็นโดเมนที่จดทะเบียนโดยใช้ข้อมูลปลอม ซึ่งมีจำนวนกว่า 80 โดเมน และยังค้นพบเพิ่มเติมว่า Flame จะสุ่มดึงตัวอย่างข้อมูล 1 KB ออกจากไฟล์ PDF, Excel, Word ที่พบในเครื่อง จากนั้นจะบีบอัดแล้วส่งตัวอย่างข้อมูลที่ได้ไปให้ให้กับเครื่อง C&C เพื่อให้คนที่ควบคุมมัลแวร์อยู่วิเคราะห์ว่าจะเอาข้อมูลอะไรออกไปจากเครื่อง เหยื่อ [29-13]

หลังจากที่มีการค้นพบเครื่อง C&C ได้เพียง 2 วัน เครื่อง C&C บางส่วนก็ได้ส่งคำสั่ง “SUICIDE” เพื่อลบไฟล์ทุกไฟล์ของ Flame ออกจากเครื่องของเหยื่อ Symantec รายงานว่า คำสั่งลบดังกล่าวนี้เป็นการ “ลบโดยสมบูรณ์” (Completely Remove) เพราะคอมโพเนนต์ทั้งหมดของ Flame ที่อยู่ในเครื่องจะถูกลบทิ้งทันทีที่ได้รับคำสั่งนั้น [29-14]

Awareness

จากการใช้ช่องโหว่ของระบบ Windows Update เป็นช่องทางในการโจมตี ทำให้ผู้เชี่ยวชาญด้าน Security หลายฝ่ายออกมาแสดงความกังวลในเรื่องนี้ ด็อกเตอร์ Johannes B. Ullrich จาก SANS Technology Institute ได้มีข้อแนะนำในการใช้งาน Windows Update เช่น ติดตั้ง Update ผ่านการเชื่อมต่อที่เชื่อถือได้ (อินเทอร์เน็ตที่บ้านหรือที่ทำงาน) เท่านั้น ถึงแม้ว่าวิธีการดังกล่าวจะป้องกันการโจมตีแบบ Man-in-the-Middle ไม่ได้แบบ 100% ก็ตาม แต่ก็สามารถลดความเสี่ยงที่จะถูกโจมตีจากเทคนิคข้างต้นได้ อย่างไรก็ตาม หากจำเป็นที่จะต้องติดตั้ง Update ผ่านระบบเครือข่ายสาธารณะ ควรใช้การเชื่อมต่อผ่าน VPN [29-15]

What's next?

จากการพัฒนาของมัลแวร์ในช่วงปีที่ผ่านมา ไม่ว่าจะเป็น Stuxnet, Duqu จนมาถึง Flame มีสิ่งที่ตรงกันอย่างหนึ่งคือ มัลแวร์เหล่านี้ไม่ได้ถูกสร้างมาเพื่อให้เกิดความเสียหายต่อบุคคลทั่วไป แต่ถูกสร้างขึ้นมาโดยมีวัตถุประสงค์หลักเพื่อตั้งใจโจมตีหน่วยงานระดับประเทศ สิ่งดังกล่าวนี้แสดงให้เห็นว่า การทำสงครามในปัจจุบันนั้นได้เปลี่ยนรูปแบบจากยุทธวิธีทางการทหาร มาเป็นการทำสงครามผ่านโลกไซเบอร์แล้ว เพราะไม่ว่าจะเป็นการทำลายข้อมูล การสืบข่าว หรือแม้กระทั่งการส่งสายลับเข้าไปในฐานของศัตรูเพื่อขโมยความลับก็สามารถทำได้ด้วยการใช้มัลแวร์ทั้งสิ้น ดังนั้น จึงเป็นที่น่าสนใจอย่างยิ่งว่า ต่อจากนี้ การทำสงครามในโลกไซเบอร์จะเป็นไปในทิศทางใด เพื่อที่จะได้เรียนรู้และป้องกันภัยได้อย่างทันท่วงที

อ้างอิง

[29-1] http://www.certcc.ir/index.php?name=news&file=article&sid=1894
[29-2] http://nakedsecurity.sophos.com/2012/05/28/flame-malware-cyber-attack/
[29-3] http://www.securelist.com/en/blog?weblogid=208193522
[29-4] http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-

discreet-threat-targets-middle-east
[29-5] http://thehackernews.com/2012/05/flame-malware-21st-century-massive.html
[29-6] http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authority-signing-certificates-added-to-the-untrusted-certificate-store.aspx
[29-7] http://technet.microsoft.com/en-us/security/advisory/2718704
[29-8] http://www.h-online.com/security/news/item/Flame-worm-was-signed-by-forged-Microsoft-certificate-1594388.html
[29-9] http://searchsecurity.techtarget.com/news/2240151187/Microsoft-revokes-fraudulent-certificates-used-by-Flame-malware-toolkit
[29-10] https://www.f-secure.com/weblog/archives/00002377.html
[29-11] http://nakedsecurity.sophos.com/2012/06/04/flame-malware-used-man-in-the-middle-attack-against-windows-update/
[29-12] http://www.symantec.com/connect/blogs/w32flamer-microsoft-windows-update-man-middle
[29-13] http://arstechnica.com/security/2012/06/flame-espionage-malware-used-huge-network-to-steal-blueprints/
[29-14] http://www.symantec.com/connect/blogs/flamer-urgent-suicide
[29-15] http://isc.sans.edu/diary.html?storyid=13429

30 WEB APPLICATION SECURITY รายสะดวก #2

ผู้เขียน: ไพชยนต์ วิมุกตะนันทน์
วันที่เผยแพร่: ๒๒ มิถุนายน ๒๕๕๕
ปรับปรุงล่าสุด: ๒๒ มิถุนายน ๒๕๕๕

ครานี้ที่แล้วในบทความ Web Application Security รายสะดวก #1 ผู้เขียนได้กล่าวถึงการป้องกัน Web application ด้วยแนวคิด Defense-in-depth ซึ่งแนวคิดอันนี้ถือว่าเป็นแนวคิดที่นำไปใช้ได้กับการรักษาความมั่นคงปลอดภัยทุกชนิด สำหรับท่านผู้อ่านที่ยังไม่คุ้นเคยกับแนวคิดนี้ ก็ขออธิบายให้เข้าใจง่ายๆ ว่าเปรียบเทียบกับการป้องกันโจรเข้าบ้าน คงไม่มีใครติดกล้องวงจรปิดโดยไม่มีกุญแจประตู หรือเลี้ยงสุนัขโดยไม่มีรั้วบ้าน แต่มาตรการต่างๆ เหล่านี้ ต้องนำมาประกอบกันเพื่อเพิ่มความมั่นคงปลอดภัย การนำมาตรการป้องกันหลายๆ แบบมาใช้ร่วมกันแบบนี้ นอกจากจะช่วยให้ผู้ที่ไม่ประสงค์ดีไม่สามารถทำการได้สะดวกแล้ว ยังอาจทำให้ผู้ที่วางแผนจะบุกรุกหรือโจมตีเปลี่ยนใจไปโจมตีเป้าหมายที่มีการป้องกันน้อยกว่าแทน เนื่องจากมีความเสี่ยงน้อยกว่าก็เป็นได้

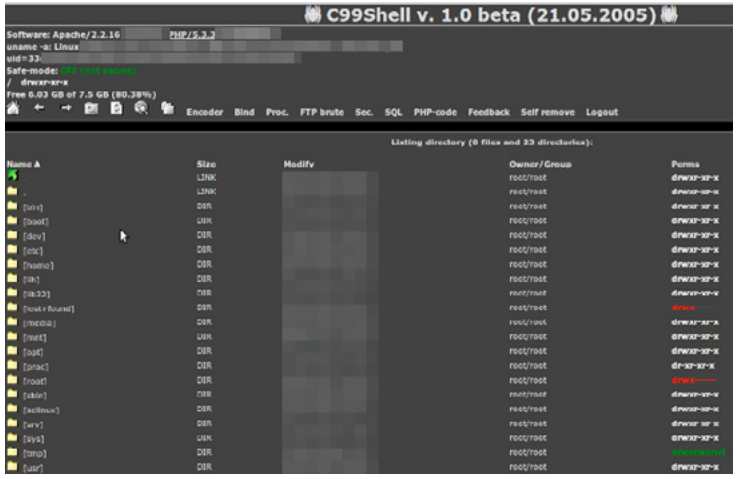
ถ้าพูดถึงการป้องกัน Web application ในแบบ Defense-in-depth แล้ว ตัวอย่างที่ผู้เขียนจะกล่าวถึงในครั้งนี้ก็คือการทำ chroot (Change root) หรือที่บางท่านที่คุ้นเคยกับระบบ FreeBSD อาจจะรู้จักในชื่อว่า Jail นั่นเอง วิธีการนี้ไม่ได้ใช้ป้องกันตัว Web application โดยตรง นั่นคือ หาก Web application มีช่องโหว่ การทำ chroot หรือ Jail ก็ไม่ได้ทำให้ช่องโหว่นั้นหมดไป แต่ทำให้ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์ (Exploit) จากช่องโหว่นั้นได้ยากขึ้น หรือใช้ได้อย่างไม่เต็มที่ ทำให้ลดโอกาสหรือลดความรุนแรงของความเสียหายจากการถูกโจมตีได้ระดับหนึ่ง

รูปแบบของการทำ chroot หรือ Jail ใน Web application นั้น มักจะทำกันที่ระดับของ Web server มากกว่าที่จะทำกันที่ Web application เป็นรายตัว โดยหลักการของ chroot คือการแยก Application ใดๆ (ในที่นี้คือ Web server) ให้ทำงานอยู่ในพื้นที่ Disk เฉพาะตัว ไม่ให้สามารถเข้าถึงพื้นที่ Disk ที่ใช้งานในระบบงานอื่นๆ ได้ ดังนั้นหาก Application ตัวนั้นเกิดความผิดพลาดในการทำงาน หรือถูกผู้ไม่ประสงค์ดีเข้าควบคุม Application นั้นก็จะไม่สามารถเข้าถึงไฟล์ระบบอื่นๆ หรือไฟล์ข้อมูลของระบบงานอื่นๆ ที่อยู่ในเครื่องเดียวกันได้ หลักการนี้เป็นหลักการเดียวกับหลักการ Sandbox ที่มีใช้ใน Web browser สมัย

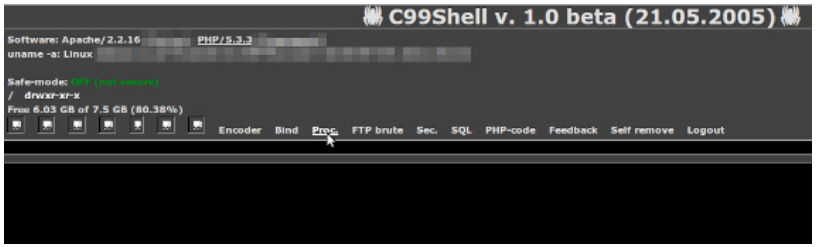
ใหม่บางตัว และมีใช้อยู่ในระบบ Android และ iOS ที่ใช้งานบนโทรศัพท์มือถือด้วย รูปแบบการทำงานของแต่ละระบบ ไม่ว่าจะเรียกว่า chroot, Jail หรือ Sandbox ก็ตาม ถึงแม้จะมีจุดประสงค์เดียวกัน แต่วิธีการทำงานอาจจะแตกต่างกันเล็กน้อย ในที่นี้จะขอกล่าวถึง chroot สำหรับ Apache web server ที่อยู่บนระบบปฏิบัติการ Linux เป็นหลัก เพื่อไม่ให้เกิดความสับสน

ในเมื่อเราจำเป็นต้องกำหนดพื้นที่เฉพาะที่ Application แต่ละตัวสามารถใช้งานได้ให้แยกกันอย่างเด็ดขาดแล้ว ใน Application ที่มีความซับซ้อนอย่าง Web server แล้วก็นับว่าเป็นเรื่องที่ยุ่งยากไม่น้อย ในอดีตที่ผ่านมาปัญหาสำคัญของการทำ chroot สำหรับ Web server ก็คือ Shared library และ System file ซึ่ง Web server จำเป็นต้องใช้ในการทำงาน เราจำเป็นต้อง Copy ส่วนประกอบต่างๆ เหล่านี้มาไว้ในพื้นที่ที่จะกำหนดให้เป็นพื้นที่เฉพาะของ Web server เสียก่อน บางครั้งรวมถึง Log file และ Temporary file ต่างๆ ที่ Web server จะต้องเขียนระหว่างการทำงานด้วย และจากที่ได้กล่าวไปข้างต้นว่า การ chroot หรือ Jail ไม่ใช่การป้องกัน Web application โดยตรง เมื่อพิจารณาจากความยุ่งยากของการดำเนินการแล้ว ผู้ดูแลระบบจำนวนไม่น้อยจึงอาจจะคิดว่า เป็นการลงทุนลงแรงที่ไม่ได้ผลดีเท่าที่ควร และอาจจะจัดอันดับเอาไว้เป็นสิ่งท้ายๆ ที่จะนำมาปฏิบัติ

แต่ความเป็นจริงแล้ว การ chroot จะเป็นประโยชน์มากในการลดผลกระทบ (Mitigate) ของการโจมตีบางรูปแบบ ที่ปกติจะมีอันตรายกับระบบอย่างมาก เช่น การโจมตีในรูปแบบ Command injection หรือการฝัง Shell ซึ่งผลลัพธ์ของการโจมตีประเภทนี้คือ การเข้าถึงระบบปฏิบัติการโดยตรง และมีสิทธิ์ในการเข้าถึงไฟล์ต่างๆ รวมถึงคำสั่งของระบบในลักษณะเช่นเดียวกับผู้ใช้คนหนึ่งในระบบ โดยอยู่ภายใต้สิทธิ์ (Privileges) ของ Web server ในกรณีนี้ หาก Web server นั้น ถูก chroot เอาไว้ ถึงแม้คำสั่งจะถูกส่งเข้ามาผ่านช่องโหว่ของ Web application ได้สำเร็จ แต่จะไม่สามารถมีผลกับระบบหรือ Application อื่นที่อยู่ในระบบนั้นได้ ตามภาพที่ 185 (30-1) และ 186 (30-2)



รูปที่ 146 (30-1) แสดง php shell เมื่อทำงานใน Apache ปกติ



รูปที่ 147 (30-2) แสดง php shell เมื่ออยู่ใน Apache ที่ถูก chroot

จากความแตกต่างของรูปที่ 146 (30-1) และ 147 (30-2) จะเห็นได้ว่า เมื่อ Web server (ในที่นี้คือ Apache) ถูก chroot แล้ว ต่อให้ถูกบุกรุกเข้ามาได้ ผู้ไม่ประสงค์ดีก็จะไม่สามารถเข้าถึงไฟล์ระบบหรือคำสั่งต่างๆ ได้เลย เว้นแต่ไฟล์ของ Web application และ Content ที่อยู่ใน Web server เท่านั้น เพราะพื้นที่ที่ระบบปฏิบัติการอนุญาตให้ Web server เข้าถึงได้มีแค่พื้นที่ที่ใช้เก็บ Content ของ Web server เท่านั้น

อย่างไรก็ตาม จุดอ่อนของ chroot ก็ยังมีอยู่ เช่นเดียวกับระบบป้องกันอื่นๆ ทุกชนิด ที่ไม่มีระบบใดสมบูรณ์พร้อมจนไม่สามารถทำลายได้ อันดับแรกคือ chroot จะสามารถป้องกันการเข้าถึงได้เฉพาะ Application ที่ไม่ได้มีสิทธิ์ root เท่านั้น กรณีนี้อาจจะไม่น่ากังวลนัก เนื่องจากในระบบปฏิบัติการสมัยใหม่มักจะกำหนดให้ Web server ทำงานในสิทธิ์ user ธรรมดาเท่านั้น (เว้นแต่ผู้ไม่ประสงค์ดีใช้เทคนิคขั้นสูง เช่น Privilege escalation ซึ่งจะกล่าวถึงในโอกาสหน้า) อีกข้อหนึ่งคือ chroot ไม่สามารถใช้ป้องกันการที่ผู้ไม่ประสงค์ดีจะทำลาย หรือดัดแปลงแก้ไข Web application ของท่าน ในกรณีนี้ ต้องเข้าใจก่อนว่า การโจมตีประเภท Command injection หรือการสั่งการผ่าน Shell ที่ถูกลักลอบฝังไว้ (รูปที่ 146 (30-1)) จะสามารถทำงานได้ตามสิทธิ์ของ Web server เท่านั้น ต่อให้เราจำกัดพื้นที่ที่ Web server สามารถเข้าถึงได้ด้วย chroot แล้วก็ตาม Web server ก็ยังจำเป็นต้องเข้าถึง Web application หรือ Content ต่างๆ เช่น รูปภาพ หรือข้อมูลที่ต้องการเผยแพร่ต่างๆ อยู่ดี ซึ่งก็ยังเป็นจุดที่ผู้ไม่ประสงค์ดีสามารถกระทำการมิดีมิร้ายแก่ระบบของท่าน ได้ นอกจากนี้ การโจมตีที่มีเป้าหมายเป็นข้อมูลใน Database อย่าง SQL Injection ก็ไม่สามารถป้องกันได้ด้วยวิธีนี้เช่นกัน

เมื่อทราบทั้ง ข้อดีและจุดอ่อนของ chroot แล้ว หากว่าท่านผู้อ่านต้องการนำไปทดลองทำดูบ้าง จะต้องทำอย่างไร? สำหรับท่านที่ใช้ Apache ตั้งแต่ version 2.2.10 ขึ้นไป ก็ค่อนข้างจะง่าย เพราะความสามารถ chroot นั้น ได้ถูกรวมมาอยู่ในตัวอยู่แล้ว สำหรับท่านที่ใช้ version เก่ากว่านี้ ก็มีทางเลือกอีก 2 ทางคือใช้ **mod_chroot** หรือใช้ **mod_security** ซึ่งจะไม่ขอพูดถึงในที่นี้

ขั้นตอนการ chroot ใน Apache version 2.2.10 ขึ้นไป จะมีขั้นตอนใหญ่ๆ ๔ ขั้น ดังนี้

1. กำหนดพื้นที่สำหรับทำเป็น root
2. แก้ไข Apache configuration
3. ย้าย Web application
4. ทดสอบการทำงาน

กำหนดพื้นที่สำหรับทำเป็น root

พื้นที่สำหรับเป็น root จะต้องเป็นพื้นที่ที่มีขนาดใหญ่เพียงพอสำหรับเก็บ Web application และข้อมูลทุกชนิดที่ต้องใช้กับ Web application เอง รวมถึงข้อมูลที่ต้องการเผยแพร่ผ่าน Web server ทั้งหมด ในที่นี้กำหนดให้เป็น /var/wwwroot

แก้ไข Apache configuration

เพิ่มบรรทัดดังต่อไปนี้ใน Apache configuration

ChrootDir /var/wwwroot

ย้าย Web application

เนื่องจากเมื่อ chroot แล้ว Apache จะไม่สามารถเข้าถึงสิ่งที่อยู่นอก root ได้เลย ดังนั้นจึงจำเป็นจะต้องย้าย Web application และ Content ต่างๆ เข้ามาอยู่ใน root ใหม่นี้ทั้งหมด เช่นถ้ามี Web application เดิม อยู่ที่ /var/www/application1 ก็ต้องย้าย Web application ดังกล่าวมาไว้เป็น /var/wwwroot/var/www/application1

ซึ่งอาจจะดูสับสนไม่น้อย แต่ก็เป็นการแลกกับการที่ไม่ต้องแก้ไข Configuration ของ Apache ให้มากจนเกินไปนัก ส่วนตำแหน่งที่เก็บ Log file และ SSL Key/Certificate ที่ใช้กับ Apache จะไม่ได้รับผลกระทบจากการทำ chroot แต่อย่างใด จึงไม่จำเป็นต้องแก้ไขใดๆ ทั้งสิ้น

ทดสอบการทำงาน

เพื่อให้แน่ใจว่า การ chroot เป็นไปอย่างสมบูรณ์ ไม่มีผลกระทบต่อการทำงาน จึงจำเป็นต้องทดลองใช้งานให้แน่ใจ โดยหลังจาก restart Apache แล้ว ให้ทดลองใช้งานพร้อมตรวจสอบ Log file ให้แน่ใจว่าไม่มี 404 not found หรือ Error ของ Web application เกิดขึ้นโดยไม่คาดคิด ซึ่งอาจหมายความว่าการย้าย Web application และ content ต่างๆ ยังไม่สมบูรณ์อย่างที่ควรจะเป็น

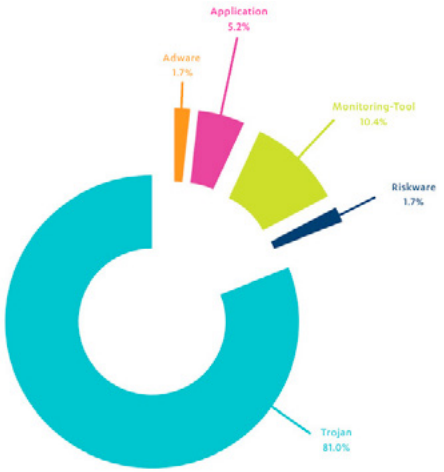
31 รู้ทันและป้องกัน MALWARE ในระบบปฏิบัติการ ANDROID ตอนที่ 2

ผู้เขียน: เสฏฐวุฒิ แสนนาม
วันที่เผยแพร่: 17 ส.ค. 2555
ปรับปรุงล่าสุด: 17 ส.ค. 2555

จากบทความ รู้ทันและป้องกัน Malware ในระบบปฏิบัติการ Android ผู้เขียนได้กล่าวถึงภัยคุกคามจาก Malware ในระบบปฏิบัติการ Android พร้อมทั้งแนะนำวิธีการตรวจสอบ Permission หรือสิทธิการทำงานของโปรแกรม และแนะนำวิธีการป้องกัน Malware ในเบื้องต้นไปแล้ว ในบทความตอนที่ 2 นี้จะกล่าวถึงช่องโหว่หรือวิธีการใหม่ๆ ที่ผู้สร้าง Malware นำมาใช้ในการโจมตี พร้อมทั้งเสนอแนวทางการป้องกันที่อาจช่วยได้

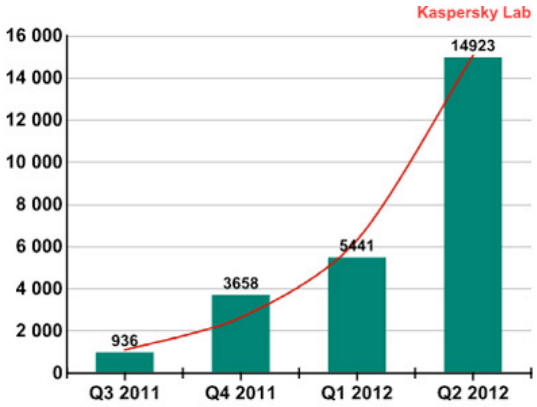
สถิติที่น่าสนใจเกี่ยวกับ Malware ในระบบปฏิบัติการ Android

จากข้อมูลใน Mobile Threat Report Q2 2012 ของ F-Secure [31-1] พบว่า Malware กว่า 64% มาจากศูนย์ซอฟต์แวร์ของผู้พัฒนาภายนอก (Third-party Android market) โดยประเภทของ Malware ที่พบมากที่สุดคือ Trojan ซึ่งคิดเป็น 81% ของจำนวน Malware ทั้งหมดที่พบในเดือนเมษายน - มิถุนายน 2555 ดังรูปที่ 148 (31-1) สถิติดังกล่าวแสดงให้เห็นว่า วิธีการแพร่กระจายของ Malware โดยส่วนใหญ่นั้นจะเป็นการหลอกลวงให้ผู้ใช้เป็นผู้ติดตั้งโปรแกรมอันตรายเข้าไปเอง



รูปที่ 148 (31-1) ประเภทของ Malware ที่พบในระบบปฏิบัติการ Android (ที่มา F-Secure)

และจากข้อมูลของ Kaspersky พบว่า จำนวน Malware ในระบบปฏิบัติการ Android ในเดือนเมษายน - มิถุนายน 2555 เพิ่มขึ้นเกือบ 3 เท่าของจำนวน Malware ในเดือนมกราคม - มีนาคม 2555 ดังรูปที่ 149 (31-2) [31-2]



รูปที่ 149 (31-2) สถิติการเพิ่มขึ้นของจำนวน Malware ในระบบปฏิบัติการ Android (ที่มา Net-Security)

ทางฝั่ง Android Market ที่ตอนนี้เปลี่ยนชื่อเป็น Google Play Store ถึงแม้ว่าทาง Google จะพัฒนาระบบ Bouncer ขึ้นมาเพื่อใช้ในการตรวจสอบความมั่นคงปลอดภัยของแอปพลิเคชันที่นักพัฒนาส่ง เข้ามาก่อนจะปล่อยให้ผู้ใช้ดาวน์โหลดจากศูนย์ซอฟต์แวร์แล้วก็ตาม [31-3] แต่นักวิจัยก็ยังค้นพบช่องโหว่ของระบบ

ดังกล่าว และได้ทดลองส่งแอปพลิเคชันที่มีโค้ดของ Malware เข้ามาใน Play Store แล้วพบว่าแอปพลิเคชันดังกล่าวสามารถผ่านเข้าสู่ Play Store ได้โดยไม่มีการแจ้งเตือนเรื่องความมั่นคงปลอดภัยแต่อย่างใด [31-4] ตัวอย่างการข้ามผ่านระบบ Bouncer ที่นักวิจัยใช้ เช่น การแบ่งส่วนโค้ดของ Malware ใส่ในแอปพลิเคชันที่อยู่ใน Play Store แล้วเก็บส่วนที่เหลือไว้ในเซิร์ฟเวอร์ภายนอก เมื่อผู้ใช้ติดตั้งแอปพลิเคชันดังกล่าวและเปิดใช้งาน แอปพลิเคชันนั้นก็จะไปดาวน์โหลดโค้ดส่วนที่เหลือมาจากเซิร์ฟเวอร์แล้วเริ่ม ทำงานตามคำสั่งอันตรายที่ถูกใส่ไว้ [31-5] ดังนั้น ถึงแม้ผู้ใช้จะดาวน์โหลดแอปพลิเคชันจาก Play Store ที่น่าจะเป็นศูนย์ซอฟต์แวร์ที่มีความน่าเชื่อถือที่สุดแล้วก็ถาม แต่ก็ยังไม่อาจมั่นใจว่าจะปลอดภัยจาก Malware ได้

ภัยคุกคามจาก Malware ในระบบปฏิบัติการ Android

Malware ในระบบปฏิบัติการ Android ได้ถูกพัฒนาไปมาก ข้อมูลด้านล่างนี้คือตัวอย่างวิธีการโจมตีแบบใหม่ที่ถูกค้นพบ

Man-in-the-Mobile

Man-in-the-Mobile (MitMo) เป็น 1 ในวิธีการโจมตีแบบ Man-in-the-Middle ซึ่งเป็นวิธีการที่ผู้ไม่หวังดีเข้ามาแทรกกลางในระหว่างการสนทนาเพื่อดักรับ ข้อมูลโดยไม่ให้ผู้ที่สนทนาอยู่รู้ตัว ซึ่งผู้ที่ดักรับข้อมูลได้นอกจากจะสามารถทราบข้อมูลทุกอย่างที่สนทนากันได้ แล้ว ยังอาจแก้ไขหรือปลอมแปลงข้อมูลที่รับส่งได้ด้วย เมื่อการโจมตีดังกล่าวมาอยู่ในอุปกรณ์พกพาจึงถูกเรียกว่า Man-in-the-Mobile

ตัวอย่าง Malware ที่โจมตีด้วยวิธีนี้ เช่น SPITMO (SpyEye in the mobile) ซึ่งจะหลอกให้ผู้ใช้ดาวน์โหลดแอปพลิเคชันมาติดตั้ง โดยภายในมีคำสั่งไม่พึงประสงค์ที่จะดัก OTP (One-time password) ซึ่งเป็นรหัสผ่านชั่วคราวที่ทางธนาคารจะส่ง SMS มาให้กับลูกค้าเพื่อใช้ในการเข้าสู่ระบบ ตัว Malware จะดักและส่งต่อ SMS ดังกล่าวไปให้กับผู้สร้าง Malware เพื่อสวมรอยเข้าสู่ระบบของธนาคารแทนผู้ใช้ตัวจริง [31-6]

Clickjacking

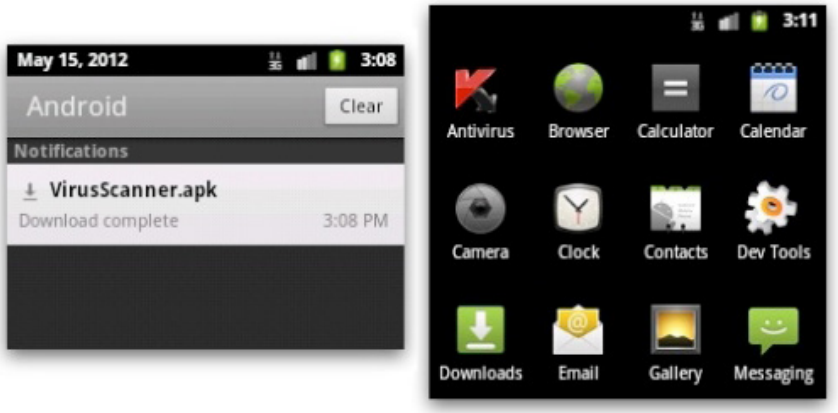
Clickjacking โดยปกติจะหมายถึงเว็บไซต์ที่ดูเหมือนเป็นเว็บไซต์ธรรมดาทั่วไป แต่หน้าเว็บนั้นถูกซ้อนทับโดยเนื้อหาที่มองไม่เห็น (Transparent Layer) โดยผู้ไม่หวังดีจะวางตำแหน่งของปุ่มหรือลิงก์ที่มีคำสั่งอันตรายไว้ซ้อนทับกับปุ่มหรือลิงก์ปกติ ทำให้เมื่อผู้ใช้คลิกที่ลิงก์ดังกล่าว ก็จะเป็นการสั่งให้คำสั่งอันตรายนั้นทำงานโดยไม่ได้ตั้งใจ [31-7]

ในระบบปฏิบัติการ Android นักวิจัยได้ทดลองสร้าง Malware ที่แสดงผล Transparent Layer ซ้อนทับไอคอนของแอปพลิเคชัน Browser ที่มากับระบบปฏิบัติการ โดยให้ไปเรียกแอปพลิเคชันอื่น เช่น แอปพลิเคชันที่บันทึกข้อมูลการใช้งานของผู้ใช้แล้วแอบส่งข้อมูลดังกล่าวไป ให้ผู้ไม่หวังดี เป็นต้น ตัวอย่างการโจมตีด้วยวิธีดังกล่าวสามารถดูได้จาก http://youtu.be/RxpMPrqnxC0 [31-8]

Antivirus ปลอม

จากปัญหาการแพร่ระบาดของ Malware ในระบบปฏิบัติการ Android จึงมีผู้พัฒนาซอฟต์แวร์ Antivirus ขึ้นมาเพื่อตรวจจับและกำจัด Malware ออกจากระบบ ผู้ไม่หวังดีอาศัยช่องทางนี้ในการโจมตีแบบ Social Engineering โดยการสร้างแอปพลิเคชัน Antivirus ปลอมขึ้นมาแล้วหลอกให้ผู้ใช้ดาวน์โหลดไปติดตั้ง [31-9] ตัวอย่างแอปพลิเคชัน Antivirus ปลอม เป็นดังรูปที่ 150 (31-3) อย่างไรก็ตาม แหล่งที่มาของซอฟต์แวร์ Antivirus ปลอมโดยส่วนใหญ่นั้นจะมาจากศูนย์ซอฟต์แวร์ภายนอก ยังไม่มีรายงานว่ามีแอปพลิเคชัน Antivirus ปลอมใน Play Store

สถิติการเพิ่มขึ้นของจำนวน Malware ในระบบปฏิบัติการ Android (ที่มา Net-Security)

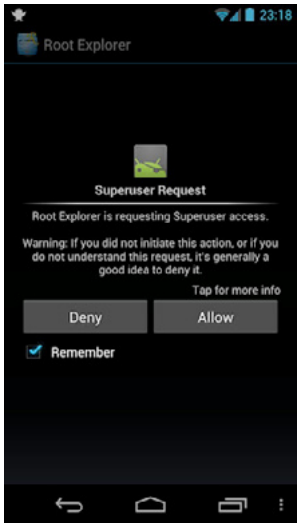


รูปที่ 150 (31-3) ตัวอย่างแอปพลิเคชัน Antivirus ปลอม (ที่มา nakedsecurity)

Root bypass

ในระบบปฏิบัติการ Linux จะมีบัญชีผู้ใช้ที่ชื่อ root เป็นผู้ใช้ที่มีสิทธิสูงสุดในระบบ สามารถแก้ไขการตั้งค่าของระบบรวมทั้งสามารถเข้าถึงหรือเปลี่ยนแปลงแก้ไขไฟล์ ของผู้ใช้ในระบบคนไหนก็ได้ เนื่องจากระบบปฏิบัติการ Android ถูกพัฒนาขึ้นโดยมีพื้นฐานมาจากระบบปฏิบัติการ Linux จึงมีบัญชีผู้ใช้ที่เป็น root อยู่ในระบบเช่นกัน ดังนั้นการ root ในระบบปฏิบัติการ Android จึงหมายถึงการประมวลผลแอปพลิเคชันใดๆ ก็ตามด้วยสิทธิของ root

การ root อุปกรณ์ที่ใช้งานระบบปฏิบัติการ Android นั้นจะมีขั้นตอนวิธีในการทำแตกต่างกันไป แต่โดยหลักแล้ว จะเป็นการนำไฟล์ไบนารีของคำสั่ง su (Super User) ไปไว้ในไดเรกทอรีที่เก็บคำสั่งของระบบ แล้วกำหนดสิทธิให้ไฟล์ su สามารถประมวลผลได้ จากนั้นติดตั้งแอปพลิเคชัน เช่น **Superuser** หรือ **SuperSU** ลงในระบบ เพื่อตรวจสอบสิทธิและกำหนดการอนุญาตให้โปรแกรมอื่นๆ สามารถประมวลผลผ่านคำสั่ง su โดยเมื่อติดตั้งโปรแกรมดังกล่าวลงในระบบ แล้วมีการเรียกใช้โปรแกรมที่ต้องการสิทธิของ root จะปรากฏหน้าต่างขึ้นมาเพื่อให้ผู้ใช้กดยืนยันการอนุญาตก่อน ดังรูปที่ 151 (31-4) [31-10]

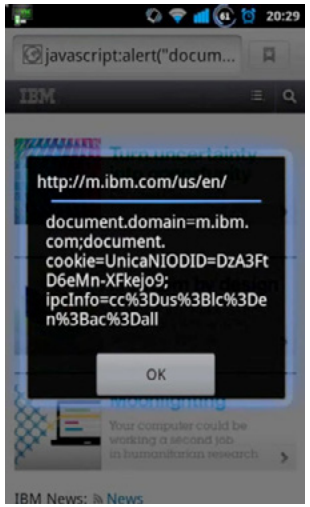


รูปที่ 151 (31-4) การขออนุญาตรันโปรแกรมโดยใช้สิทธิของ root (ที่มา Superuser)

ในระบบปฏิบัติการ Android เวอร์ชัน 3.0 และเวอร์ชัน 2.3.3 หรือเก่ากว่า จะมีช่องโหว่ CVE-2011-1823 ซึ่งช่องโหว่ดังกล่าวทำให้แอปพลิเคชันใดๆ ก็ตามสามารถประมวลผลคำสั่งอันตรายโดยใช้สิทธิของ root ได้ ช่องโหว่ดังกล่าวนี้ถูกเรียกในชื่อ Gingerbreak [31-11] Malware ตัวแรกที่โจมตีผ่านช่องโหว่ดังกล่าว คือ Gingermaster ซึ่งจะลักลอบเปิด Service ลับในเครื่องของผู้ใช้และส่งข้อมูลส่วนตัวออกไปให้กับผู้สร้าง Malware [31-12] Gingermaster สามารถทำงานภายใต้สิทธิของ root ได้โดยไม่ปรากฏหน้าต่างยืนยันการอนุญาต และเนื่องจากเป็นการโจมตีผ่านช่องโหว่ของระบบปฏิบัติการเอง ดังนั้นต่อให้ผู้ใช้ไม่ได้ root เครื่อง ก็จะถูกโจมตีได้เหมือนกับเครื่องที่ถูก root แล้วเช่นกัน

Drive-by-Download

โดยปกติแล้วแอปพลิเคชันในระบบปฏิบัติการ Android จะรันในโหมด Sandbox ซึ่งจะเป็นการทำงานแยกส่วนออกมาจากการทำงานของระบบปฏิบัติการตามปกติ เพื่อป้องกันไม่ให้แอปพลิเคชันใดๆ สามารถเข้าถึงหรือแก้ไขข้อมูลของแอปพลิเคชันอื่นได้ ในระบบปฏิบัติการ Android เวอร์ชัน 3.1 และเวอร์ชัน 2.3.4 หรือเก่ากว่า มีช่องโหว่ CVE-2011-2357 [31-13] ซึ่งเป็นข้อผิดพลาดในการโหลด URL ของแอปพลิเคชัน Browser โดยช่องโหว่ดังกล่าวนี้อนุญาตให้แอปพลิเคชันใดๆ สามารถข้ามผ่านระบบ Sandbox ของ Browser และส่ง JavaScript เข้ามาประมวลผลคำสั่งอันตรายได้ ตัวอย่างการโจมตีเป็นดังรูปที่ 152 (31-5)



รูปที่ 152 (31-5) ตัวอย่างการโจมตี Drive-by-Download ในระบบปฏิบัติการ Android (ที่มา IBMAppSecGrp)

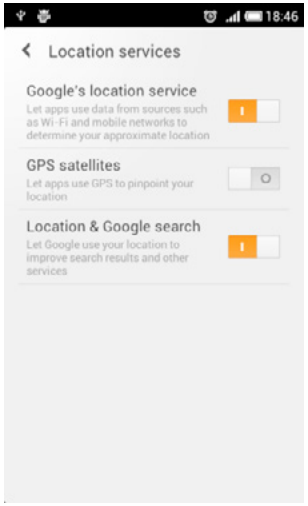
NFC

NFC หรือ Near field communication เป็นเทคโนโลยีการสื่อสารไร้สายระยะสั้น โดยมีระยะการใช้งานประมาณ 10 ซ.ม. นิยมใช้ในการชำระเงินโดยการแตะอุปกรณ์เข้ากับเครื่องรับชำระเงิน หรือแลกเปลี่ยนข้อมูลกับอุปกรณ์ที่อยู่ในระยะใกล้เคียงกัน [31-14] ในระบบปฏิบัติการ Android ตั้งแต่เวอร์ชัน 4.0 ขึ้นไป มีความสามารถชื่อ Android Beam ซึ่งใช้ความสามารถ NFC ในการส่งไฟล์ระหว่างอุปกรณ์ Android ด้วยกันได้ [31-15]

นักวิจัยค้นพบว่าสามารถโจมตีอุปกรณ์ที่ใช้งานระบบปฏิบัติการ Android ผ่านทาง NFC ได้ โดยการโจมตีดังกล่าวนี้ไม่ได้ใช้ช่องโหว่ของโพรโทคอล NFC แต่เป็นการโจมตีผ่านช่องโหว่ของ Browser (ดังที่อธิบายไปในหัวข้อก่อนหน้านี้) เนื่องจากหากนำอุปกรณ์ที่มีความสามารถ NFC ไปแตะเข้ากับ NFC Tag ที่มี URL ของเว็บไซต์อันตรายอยู่ ตัวระบบปฏิบัติการจะเปิด Browser ไปที่ URL นั้นโดยอัตโนมัติ ซึ่งอาจเป็นการดาวน์โหลด Malware หรืออาจเป็นการสั่งประมวลผลคำสั่งอันตรายผ่าน Browser ได้ ช่องโหว่ดังกล่าวนี้ถูกแก้ไขแล้วใน Android 4.0.2 โดยหากพบ NFC Tag ที่เป็น URL ระบบปฏิบัติการจะแสดงหน้าต่างเพื่อให้ผู้ใช้ยืนยันการเปิดเว็บไซต์ก่อนเสมอ [31-16]

A-GPS

ในการระบุตำแหน่งที่อยู่ โทรศัพท์มือถือ Smartphone โดยทั่วไปจะไม่ได้ใช้แค่ข้อมูลจาก GPS เพียงอย่างเดียว เนื่องจากการจับตำแหน่งจากดาวเทียมนั้นต้องใช้สัญญาณจากดาวเทียมอย่างน้อย 4 ดวง และต้องการการประมวลผลที่ค่อนข้างซับซ้อน ถ้าต้องการให้ได้ตำแหน่งที่แม่นยำจริงๆ นั้นอาจต้องใช้เวลาในการคำนวณถึง 12 นาที ดังนั้นจึงมีการใช้ข้อมูลจาก Wi-Fi หรือ Cellular Network จากผู้ให้บริการโทรศัพท์มือถือมาช่วยในการคำนวณตำแหน่งด้วย ซึ่งวิธีการดังกล่าวนี้เรียกว่า Assisted GPS หรือ A-GPS [31-17] ในระบบปฏิบัติการ Android ผู้ใช้สามารถเลือกวิธีการระบุตำแหน่งได้ในเมนู Location service โดยการเปิดใช้งาน A-GPS จะอยู่ที่ส่วน Google's location service และการเปิดใช้งาน GPS จากดาวเทียมจะอยู่ที่ส่วน GPS satelites ดังรูปที่ 153 (31-6)



รูปที่ 153 (31-6) การตั้งค่า Location Service

นักวิจัยได้ค้นพบว่าข้อมูลที่แลกเปลี่ยนกันระหว่างโทรศัพท์มือถือกับระบบ เครือข่ายนั้นไม่ได้ส่งผ่านช่องทางที่มั่นคงปลอดภัย ทำให้ผู้ไม่หวังดีสามารถส่งข้อมูล A-GPS ปลอม หรือข้อมูลอื่นๆ ที่อาจใช้ในการโจมตีได้ และการคำนวณพิกัดตำแหน่งนั้นไม่ได้ทำบนชิป GPS แต่ถูกคำนวณบน CPU ของตัวอุปกรณ์โดยตรง เนื่องจากมีความเร็วในการทำงานที่มากกว่า ดังนั้นผู้โจมตีจึงสามารถส่งคำสั่งอันตรายเข้าไปประมวลผลได้ โดยนักวิจัยได้ทดลองสร้าง Wi-Fi Network ที่ส่งข้อมูลไปกับ A-GPS ให้เปลี่ยนแปลงการตั้งค่าของอุปกรณ์ โดยตั้งค่าให้ทุกครั้งที่อุปกรณ์นั้นเชื่อมต่อ A-GPS ต้องส่งข้อมูลพิกัดตำแหน่งมาให้กับ Wi-Fi Network นี้ด้วย ทำให้นักวิจัยสามารถติดตามตำแหน่งของคนที่เคยเชื่อมต่อกับ Wi-Fi Network นี้ได้ [31-18]

การตรวจสอบและป้องกัน

การตรวจสอบช่องโหว่ในระบบปฏิบัติการ Android ที่ใช้อยู่ สามารถใช้โปรแกรมที่ทำขึ้นมาเพื่อตรวจสอบช่องโหว่โดยเฉพาะได้ เช่น โปรแกรม X-Ray for Android ดังรูปที่ 154 (31-7) โปรแกรมดังกล่าวนี้ถูกพัฒนาขึ้นโดยบริษัท Duo Security ซึ่งเป็นบริษัทที่พัฒนาซอฟต์แวร์ด้าน Two-Factor Authentication ผู้ใช้สามารถตรวจสอบข้อมูลเพิ่มเติมและดาวน์โหลดโปรแกรมดังกล่าวได้จากเว็บ ไซต์ http://www.xray.io/

รูปที่ 154 (31-7) โปรแกรม X-Ray for Android (ที่มา X-Ray)

จากข้อมูลที่นำเสนอไปข้างต้น จะเห็นได้ว่า การป้องกัน Malware โดยดูแค่ Permission ตอนติดตั้งแอปพลิเคชันนั้นคงจะไม่เพียงพอ เพราะผู้โจมตีต่างก็สรรหาวิธีการใหม่ๆ มาใช้อยู่เรื่อยๆ และการโจมตีบางอย่างก็เกิดขึ้นได้โดยที่ผู้ใช้แทบไม่รู้ตัวเลยด้วยซ้ำ ดังนั้น การป้องกันตัวที่ดีที่สุดควรเป็นการระวังในการใช้งานของตัวผู้ใช้เอง โดยเฉพาะการอัพเดทแอปพลิเคชันและระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุด และหมั่นติดตามข้อมูลข่าวสารเรื่องความมั่นคงปลอดภัยอยู่เสมอ

อ้างอิง

[31-1] http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf
[31-2] http://www.net-security.org/malware_news.php?id=2225
[31-3] http://googlemobile.blogspot.com/2012/02/android-and-security.html
[31-4] http://www.theregister.co.uk/2012/06/04/breaking_google_bouncer/
[31-5] http://www.symantec.com/connect/blogs/android-threat-trend-shows-criminals-are-thinking-outside-box
[31-6] http://www.net-security.org/malware_news.php?id=2183
[31-7] https://www.owasp.org/index.php/Clickjacking
[31-8] http://thehackernews.com/2012/07/android-clickjacking-rootkit.html
[31-9] http://nakedsecurity.sophos.com/2012/05/16/fake-anti-virus-disguises-used-by-android-malware/
[31-10] http://droidlessons.com/what-is-rooting-on-android-the-advantages-and-disadvantages/
[31-11] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1823
[31-12] http://nakedsecurity.sophos.com/2011/08/22/first-malware-using-android-gingerbreak-exploit/
[31-13] http://blog.watchfire.com/files/advisory-android-browser.pdf
[31-14] http://java.sun.com/developer/technicalArticles/javame/nfc/
[31-15] http://electronics.howstuffworks.com/android-beam.htm
[31-16] http://hexus.net/mobile/news/android/42933-android-nfc-walk-by-vulnerabilities-demonstrated/
[31-17] http://tech2.in.com/features/all/what-is-agps-how-does-it-work/115142
[31-18] http://www.technologyreview.com/news/428632/gps-weakness-could-enable-mass-smartphone-hacking/

32 PHISHING รูปแบบใหม่มากับ DATA URI

ผู้เขียน: ไพชยนต์ วิมุกตะนันทน์ และ พรพรหม ประภากิตติกุล
วันที่เผยแพร่: 7 ก.ย. 2555
ปรับปรุงล่าสุด: 7 ก.ย. 2555

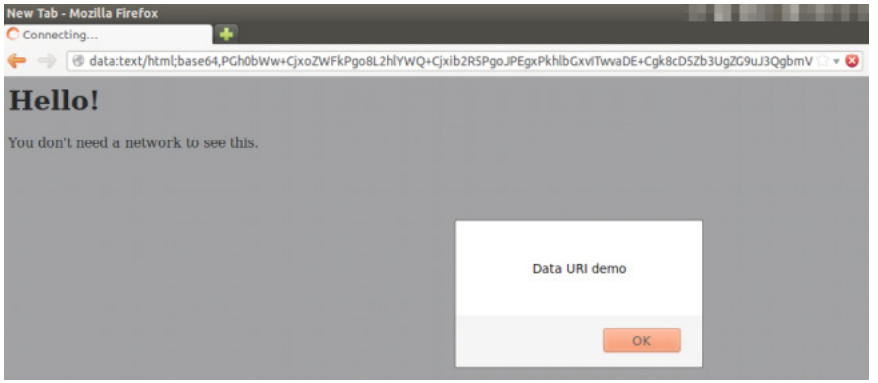
จากสถานการณ์รับแจ้งเหตุภัยคุกคามในปัจจุบัน พบว่าภัยคุกคามที่เกิดจาก Phishing ยังคงมาเป็นอันดับหนึ่งในประเทศไทย โดยการสร้างหน้าหลอกลวงให้เหยื่อหลงเชื่อกรอกข้อมูลสำคัญ และส่งข้อมูลกลับไปยังผู้โจมตีอีกครั้ง ซึ่งในกรณีดังกล่าวทางผู้สร้างเว็บเบราว์เซอร์ยอดนิยมทั้งหลาย ไม่ว่าจะเป็น Firefox, Chrome, Internet Explorer, Safari หรือ Opera ก็ล้วนแล้วแต่ไม่ได้นิ่งนอนใจ ซึ่งจะเห็นได้จากเว็บเบราว์เซอร์ชั้นนำเหล่านี้ได้มีการเพิ่มความสามารถในการตรวจจับ URL ของเว็บไซต์ที่ได้รับรายงานว่าเป็นหน้า Phishing และแจ้งให้ผู้ใช้ทราบก่อนที่จะเกิดการหลงเชื่อและป้อนข้อมูลสำคัญต่างๆ เข้าไป ดังที่เคยได้อธิบายถึงในบทความก่อนหน้านี้ (Web Browser กับการป้องกัน Phishing Website) ซึ่งผลลัพธ์ที่ได้จากแนวทางดังกล่าวก็นับว่าเป็นการป้องกันความเสียหายที่ได้ผลดีในระดับหนึ่ง

แต่ตามรายงานข่าวเมื่อวันที่ 29 สิงหาคม 2555 ที่ผ่านมา นักศึกษาจาก University of Oslo ประเทศนอร์เวย์ที่ชื่อ Henning Klevjer ได้นำเสนอแนวทางที่อาจนำไปสู่การโจมตีในลักษณะของ Phishing ในรูปแบบใหม่ [32-1] โดยมีการแสดงวิธีการฝัง HTML Code ของหน้า Phishing ลงใน URI โดยตรง และเมื่อมีการเปิดด้วยเว็บเบราว์เซอร์ก็จะทำให้เห็นหน้า Phishing ตาม HTML Code ที่ฝังลงไป เช่น URI ที่แสดงในรูปที่ 155 (32-1)

```
data:text/html;base64,PGh0bWw+CjxoZWFkPgo8L2hlYWQ+CjxibG2R5PgoJPEgxPkhlbGxvIFwvaDE+
Cgk8cD5Zb3UgZG9uJ3QgbmVlZCBhIG5ldHdvcmsgdG8gc2VlIHRoaXMuCgk8c2NyaXB0PgoJCWFs
ZXJ0KCJEYXRhIFVSSSBkZW1vIik7Cgk8L3NjcmlwdD4KPC9ib2R5Pgo8L2h0bWw+Cg==
```

รูปที่ 155 (32-1) ตัวอย่าง URI

เมื่อนำไปเปิดด้วยเว็บเบราว์เซอร์จะพบลักษณะดังรูปที่ 156 (32-2)



รูปที่ 156 (32-2) ตัวอย่างหน้าเว็บเพจที่เกิดจาก URI ในรูปที่ 155 (32-1)

ซึ่งสิ่งที่ทำให้ลักษณะการทำงานดังกล่าวแตกต่างจากการโจมตีด้วยเทคนิค Phishing ในลักษณะเดิมคือเว็บเบราว์เซอร์จะไม่ได้มีการติดต่อกับเว็บไซต์ใดเลยในการแสดงผลเว็บเพจนี้ โดยข้อมูลทั้งหมดไม่ว่าจะเป็น HTML Code หรือแม้แต่ Javascript เองก็สามารถถูกฝังเอาไว้ใน URI ข้างต้นได้ทั้งสิ้น ซึ่งเท่ากับว่าวิธีการที่เว็บเบราว์เซอร์ใช้ในการตรวจสอบหน้า Phishing ด้วย URL ก็จะไม่สามารถใช้ได้ผลอีกต่อไป

URI VS URL และภัยที่มากับ Data URI

ผู้ใช้หลายท่านคงได้ยินคำว่า URL กันมานานแล้ว บางท่านเมื่ออ่านบทความนี้ในตอนแรกอาจทำให้เกิดความสับสนเมื่อมีการพูดถึง URI โดยในหัวข้อนี้จะอธิบายความหมายของคำว่า URI และ URL เพื่อให้ผู้อ่านเกิดความเข้าใจถึงลักษณะการทำงานและแนวทางการโจมตีที่ได้ กล่าวไว้ในข้างต้น โดยมีรายละเอียดที่น่าสนใจดังต่อไปนี้

URI ย่อมาจาก Universal Resource Identifier เป็นมาตรฐานการอ้างอิงรูปแบบการเข้าถึงทรัพยากรต่างๆ เป็นมาตรฐานซึ่งดูแลกำกับโดยหน่วยงาน IANA มีลักษณะการเรียกใช้งานที่เรียกว่า Scheme โดยมี Scheme ที่กำหนดไว้เป็นมาตรฐาน [32-2] เช่น http, ftp, data เป็นต้น

URL (Uniform Resource Locator) ถือเป็นส่วนประกอบหนึ่งของ URI เป็นลักษณะของการระบุที่อยู่ของทรัพยากรบนเครือข่ายอินเทอร์เน็ต โดยมีรูปแบบการเรียกใช้คือ [scheme]://[domain:port/path] เช่น http://example.com หรือ ftp://example.com ซึ่งหมายถึงมีการเรียกใช้โพรโทคอลชื่อ HTTP และ FTP ในการเข้าถึงข้อมูลเว็บไซต์ชื่อ example.com

โดยจาก Scheme ของ URI ที่ได้มีการพูดถึงในบทความนี้คือ Data ซึ่งความจริงแล้วไม่ใช่สิ่งแปลกใหม่เนื่องจากความสามารถนี้ถูกระบุอยู่ใน RFC 2397 [32-3] ตั้งแต่ปี 1998 แล้ว และมีการนำมาใช้เป็นเวลานานพอสมควร โดยส่วนมากเป็นการใช้เพื่อแสดงรูปภาพขนาดเล็กๆ เช่น Bullet บนเว็บไซต์ โดยมีรูปแบบการใช้งานคือ data:[<mediatype>][;base64],<data> ดังตัวอย่างในรูปที่ 157 (32-3)

Pb29u0/\/\HNzxFtcuP+Cgfx0dPz8/Ppqajs7q4SFyfr6+vZV\/WJjupqb1g/\/\ow/\/\LuU/\/\PdYWCwsoX
d4xPJFRUpKskFFsXt0xvT09EZGr0DAq5OU0voAAP7+/t/f362u3X+Axm9wwQAAWzY2punp6eAAAD
s7qFlbtU5Qr/hgYPpvb/hcXE9PlPxubgsNmWdou2psv90AAP0AAP////8AACH5BAAAAAAALAAAAAA
QAAsAAAaFwJ/w1yv2TieEEsFg/B7QBwAAgeAkB5qNw/D5UOCIOFJRmBeKV0iFwZjeiQSFshJ5Epm
MR2a4gUglEy4EHQICJRoZDX1/gYOFAgMxiSx+gDGPhgMDLho5JnYNLDs6Fw58BjM6LQpkZWcLlw
GzsykIEDUSWFocFgW/Hx88S03FG8cwMDzLQQA7

รูปที่ 157 (32-3) ตัวอย่าง URI

ผลลัพธ์ของการแสดงผลบนเว็บเบราว์เซอร์จะแสดงรูปภาพธงชาติไทยขนาดเล็กทันที โดยไม่จำเป็นต้องมีไฟล์รูปภาพนี้อยู่ในเครื่องแม่ข่ายแต่อย่างใด ซึ่งลักษณะตัวอย่างดังที่กล่าวมานี้คงทำให้ผู้อ่านพอเข้าใจแล้วว่าเหตุใด เว็บเบราว์เซอร์จึงจะไม่สามารถตรวจสอบหน้า Phishing ที่เกิดจากการใช้งาน Data URI ได้

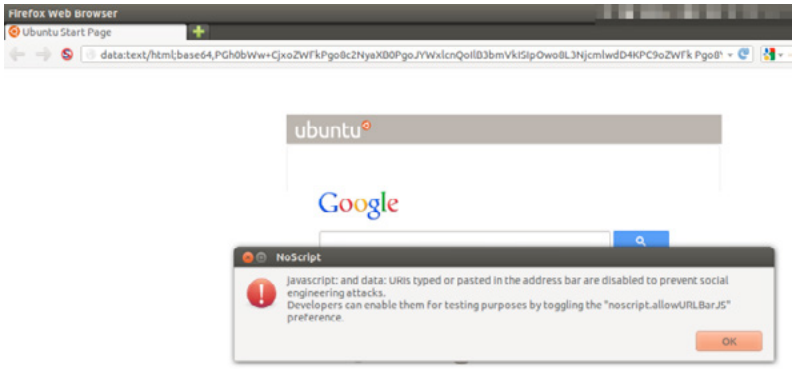
ข้อสังเกตการใช้งาน Data URI

พบว่าการใช้งาน Data URI ยังคงมีข้อจำกัดและลักษณะบางอย่าง ซึ่งอาจจะเป็นเหตุผลที่ในปัจจุบันนี้ยังไม่มีการใช้ Data URI ในการโจมตีในลักษณะ Phishing ก็ได้ โดยมีข้อมูลสนับสนุนได้แก่

1. ในช่อง Address bar ที่เป็นข้อมูล Data URI จะมีลักษณะที่ผิดปกติมาก โดยมีความยาวและไม่ได้ขึ้นต้นด้วย http:// เหมือนอย่างการเปิดเว็บไซต์อื่นทั่วๆไป ซึ่งอาจทำให้เหยื่อเกิดความสงสัยได้
2. การส่งข้อมูลที่หลอกลวงเหยื่อให้กรอกลงไปในหน้า Phishing นั้น ยังคงต้องอาศัยการรับข้อมูลของ Script ที่ต้องมีอยู่จริงบนอินเทอร์เน็ต นั่นหมายถึงใน Data URI ที่เปิดก็จะต้องมีข้อมูลในส่วนนี้อยู่ ซึ่งอาจถูกตรวจจับได้ด้วยกลไกการป้องกัน Phishing ของเว็บเบราว์เซอร์ต่อไป
3. มีการพบว่าเว็บเบราว์เซอร์ตระกูล Internet Explorer ซึ่งเป็นเว็บเบราว์เซอร์ที่ใช้กันแพร่หลายมากที่สุดตัวหนึ่ง ไม่สนับสนุนการใช้งาน Data URI ที่ฝังข้อมูล HTML Code แต่ยังคงสนับสนุนการใช้งานที่เป็นการแสดงข้อมูลประเภทรูปภาพเท่านั้น

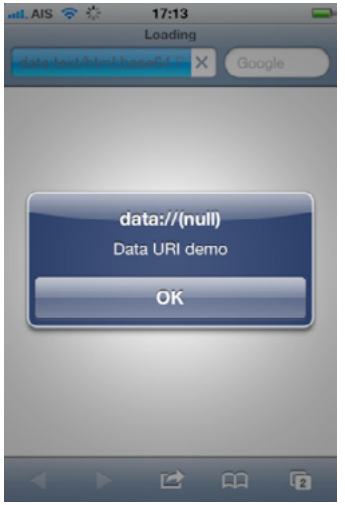
ข้อแนะนำในการป้องกันตนเอง

จากข้อสังเกตที่ได้กล่าวมาในข้างต้นผู้ใช้เว็บเบราว์เซอร์ Internet Explorer อาจจะสบายใจได้ในระดับหนึ่งเนื่องจากโปรแกรมดังกล่าวไม่สามารถทำงานกับ Data URI ได้ แต่สำหรับผู้ใช้ Firefox อาจจะสามารถป้องกันได้โดยการติดตั้ง Extension ที่ชื่อ NoScript ในการป้องกันการโจมตีแบบนี้ได้ โดย NoScript จะแสดงข้อความเตือนเมื่อผู้ใช้พยายามเข้าถึง Data URI ผ่านการ Click บน Link ซึ่งน่าจะเป็นสถานการณ์เดียวกันกับที่ผู้ใช้ได้รับอีเมล Phishing แต่จากการทดสอบพบว่าจะไม่เกิดผลถ้า Data URI นั้น เป็นส่วนหนึ่งของเว็บเพจอยู่แล้ว เช่นการใช้ Data URI แสดงรูปภาพ ดังรูปที่ 158 (32-4)



รูปที่ 158 (32-4) ตัวอย่างการแจ้งเตือน URI ผิดปกติ

และสำหรับเว็บเบราว์เซอร์อื่นๆ เช่น Chrome Safari หรือ Opera ก็ยังไม่ปรากฏว่ามีวิธีการป้องกันด้วยการโจมตีนี้แต่อย่างใด และจากการทดสอบด้วยเว็บเบราว์เซอร์บนโทรศัพท์มือถือที่เป็นระบบปฏิบัติการ Android และ iOS ก็พบว่าได้รับผลกระทบจากเรื่องนี้เช่นกัน และอาจรุนแรงกว่ากรณีที่ผู้ใช้ผ่านเครื่องคอมพิวเตอร์เนื่องจาก Address bar สำหรับโทรศัพท์มือถือค่อนข้างมีลักษณะการมองเห็นค่อนข้างจำกัดซึ่งอาจทำให้ สังเกตได้ยากขึ้นดังเช่นรูปที่ 159 (32-5)



รูปที่ 159 (32-5) ตัวอย่างการเปิด URI ในเบราว์เซอร์ Safari ในเครื่อง iPhone

ซึ่งในระหว่างนี้ผู้ใช้เองควรมีสติในการใช้งานอย่างระมัดระวังในการใช้งานจนกว่า จะมีวิธีป้องกันที่ดีกว่านี้ออกมา อย่างไรก็ตาม ไม่ว่าผู้อ่านจะใช้งานเว็บเบราว์เซอร์อะไร และมีระบบป้องกันหรือไม่ก็ตาม การใช้วิธีการสังเกต URL ที่ผิดปกติ หรือสอบถามกับทางสถาบันการเงินโดยตรงก่อนทุกครั้งที่มีความสงสัยเกี่ยวกับการทำธุรกรรมทางการเงิน ก็ย่อมเป็นแนวทางการป้องกันจากภัยของการโจมตีประเภท Phishing ที่ดีที่สุดในทุกกรณี

เอกสารอ้างอิง

[32-1] http://klevjers.com/papers/phishing.pdf

[32-2] http://www.iana.org/assignments/uri-schemes.html

[32-3] http://www.ietf.org/RFC/RFC2397.txt

33 PASSWORD, HASH และ RAINBOW TABLE

ผู้เขียน: ไพชยนต์ วิมุกตะนันทน์

วันที่เผยแพร่: 5 ตุลาคม 2555

ปรับปรุงล่าสุด: 5 ตุลาคม 2555

ในระยะนี้มีข่าวเกี่ยวกับองค์กรต่างๆ ทั้งของรัฐและเอกชนในต่างประเทศ ที่ถูกกลุ่มผู้ไม่ประสงค์ดีลักลอบขโมยข้อมูลออกมาอยู่บ่อยๆ ไม่ว่าจะด้วยเหตุผลทางการเมืองหรือเหตุผลอื่นๆ ก็ตาม แต่ทุกครั้งที่ข้อมูลในองค์กรเหล่านั้นหลุดออกมา สิ่งที่สูญเสียไปนอกจากข้อมูลที่เป็นความลับต่างๆ (รวมถึงความเชื่อมั่นที่มีต่อองค์กร) แล้ว บางครั้ง ข้อมูลส่วนบุคคล และรหัสผ่านของผู้ที่ใช้งานระบบสารสนเทศในองค์กรเหล่านั้นก็ถูกนำออกมาด้วย

ข้อมูลประเภทรหัสผ่านของบุคคลนั้น มีความสำคัญมากกว่าที่หลายคนคิด เพราะจากสถิติที่ผ่านมา พบว่าคนเรามักจะใช้รหัสผ่านซ้ำๆ กันในแต่ละระบบที่ตนเองใช้งาน เช่นผู้ใช้จำนวนไม่น้อยที่ใช้รหัสผ่านเดียวกันทั้งระบบอีเมล และ Web application ขององค์กร รวมถึงยังเอารหัสผ่านนี้ไปใช้กับอีเมลส่วนตัวด้วย [33-1] ทำให้เมื่อผู้ไม่ประสงค์ดีเจาะเอารหัสผ่านใน Web application ออกไปได้แล้ว ก็สามารถใช้รหัสผ่านนี้เพื่อเข้าถึงอีเมลของผู้ใช้คนนั้น ทั้งในองค์กรและอีเมลส่วนตัวได้อย่างสบาย

การเก็บรหัสผ่านในฐานข้อมูล หรือในไฟล์ข้อมูลก็ดี เป็นวิธีการปกติในการใช้งานรหัสผ่านของ Application ต่างๆ อยู่แล้ว ดังนั้นฐานข้อมูล หรือไฟล์ดังกล่าวนี้ จึงเปรียบเสมือนกุญแจเข้าสู่ระบบทั้งหมด ที่ผู้ดูแลระบบต้องคอยระมัดระวัง ไม่ให้ผู้ไม่ประสงค์ดีมาเอาออกไปได้ หรือถ้าเอาออกไปได้ก็ต้องนำไปใช้ประโยชน์ไม่ได้ ซึ่งในกรณีหลังนี้ ถ้าถามผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย ก็คงได้คำตอบว่า อย่าเก็บรหัสผ่านเอาไว้แบบ Plain text นั่นเอง

ถ้าไม่เก็บแบบ Plain text แล้วจะเก็บแบบใด ถ้าพูดถึงการเก็บข้อมูลให้เป็นความลับหลายคนคงนึกถึงการเข้ารหัสลับ (Encrypt) ซึ่งมีหลายรูปแบบด้วยกัน แต่การเก็บรหัสผ่านด้วยรหัสลับดูจะไม่เป็นวิธีที่ดีนัก เนื่องจากขึ้นชื่อว่าเป็นการเข้ารหัสลับแล้ว ก็ต้องมี Key ที่ใช้ถอดรหัสลับ (Decrypt) ซึ่งก็ไม่พ้นที่จะต้องเก็บเอาไว้ที่ใดที่หนึ่ง เช่นในตัว Application เอง ในกรณีนี้ ถ้าพิจารณาจากรูปแบบการโจมตีของผู้ไม่ประสงค์ดีที่ผ่านๆ มาแล้ว จะพบว่าส่วนมากผู้โจมตีจะสามารถเข้าถึงข้อมูลในเครื่อง Web server ได้ด้วย ดังนั้นนอกจาก

จะได้ข้อมูลที่มีการเข้ารหัสลับออกไปแล้ว ก็มักจะได้ Key ที่ส่วนมากจะซ่อนอยู่ในตัว Web application ออกไปด้วยเช่นกัน เปรียบเหมือนใช้ตู้เซฟอย่างดี แต่กลับวางกุญแจไว้บนโต๊ะข้างๆ กัน

Hashing

รูปแบบการเก็บรหัสผ่านที่นิยมใช้กันก็คือ การเก็บรหัสผ่านในรูปแบบของ Hash หรือชื่ออย่างเป็นทางการคือ Cryptographic Hash ความสามารถของ Hash คือ สร้าง “ข้อมูลแทนตัว” ของข้อมูลใดๆ ซึ่งในที่นี้คือรหัสผ่านนั่นเอง ข้อดีของ Hash ที่เหนือกว่าการเข้ารหัสลับก็คือค่า Hash หรือ “ข้อมูลแทนตัว” จะไม่สามารถถอดรหัส หรือกระทำการใดๆ เพื่อให้กลับออกมาเป็นค่าที่แท้จริงของข้อมูลนั้นๆ ได้ เช่นถ้าผู้ไม่ประสงค์ดี ได้ Hash ที่มีค่าเป็น 3fd7e602e98245a83eed414d798040e952e01cbee0979269d2a0150db-d37172030d6e8d6a2b1baaf23c2acfe1624d112b9fd6a7cd678b36e7aff411e9b09f0c7 ออกไปจากการเจาะระบบ ก็จะไม่สามารถทราบว่า รหัสผ่านที่แท้จริงคือ thisismysecretpassword เป็นอันขาด

ท่านผู้อ่านอาจจะสงสัยว่า ในเมื่อไม่มีทางที่จะ “ถอดรหัส” ค่า Hash ออกมาได้ ตัว Web application จะทราบได้อย่างไรว่าผู้ใช้งานป้อนรหัสผ่านเข้ามาถูกต้องแล้ว คำตอบก็คือ ตัว Web application ไม่จำเป็นต้องทราบว่ารหัสผ่านที่ถูกต้องคืออะไร ขอเพียงแค่เมื่อเอารหัสผ่านที่ผู้ใช้ป้อนเข้ามา ไปผ่าน Hash แบบเดียวกันกับที่ใช้กับรหัสผ่านที่เก็บในระบบ ถ้าผลที่ได้ออกมาตรงกับค่าที่เก็บเอาไว้ก็เป็นอันทราบได้แน่ว่ารหัสผ่านที่ผู้ใช้งานป้อนเข้ามานั้นถูกต้องแล้ว

Hash นั้นมีหลายแบบ ที่เป็นที่รู้จักกันมากที่สุดดูเหมือนจะเป็น MD5 ซึ่งมีข่าวใหญ่เมื่อหลายปีมาแล้วว่ามีผู้ Crack ได้สำเร็จ จนเกิดความวิตกกังวลไปทั่ว โดยเฉพาะผู้ที่ได้ยินข่าวมาโดยไม่ทราบรายละเอียดที่แท้จริง รายละเอียดของเรื่องนี้ก็คือ Hash ทุกชนิด มีข้อจำกัดอยู่อย่างหนึ่งคือการเกิด Collision หรือการซ้ำกันของค่า Hash ซึ่งถ้าลองพิจารณาดูแล้วจะเห็นว่าเรื่องนี้ไม่ใช่เรื่องแปลกเลย เนื่องจากคุณสมบัติของ “ข้อมูลแทนตัว” ที่ Hash สร้างขึ้นจะมีความยาวคงที่เสมอสำหรับ Hash แต่ละแบบ เช่นในกรณีของ MD5 จะมีขนาด 16 ไบต์ (128 บิต) ดังนั้นค่า MD5 ทั้งหมดในโลกนี้ที่จะมีได้คือ 256^16 หรือ 2^128 ค่าเท่านั้น ในขณะที่ข้อมูลที่ต้องการหาค่า Hash นั้นอาจเป็นข้อมูลอะไรก็ได้ ซึ่งย่อมมีความหลากหลายมากกว่า จำนวน 256^16 หรือ 2^128 แน่นอน จึงเป็นไปได้ที่จะพบว่ามีข้อมูลมากกว่า 1 ชุด ที่มีค่า Hash ตรงกัน และเช่นกัน สำหรับการใช้ Hash เก็บข้อมูลรหัสผ่าน ก็ย่อมมีโอกาสที่จะมีรหัสผ่านมากกว่า 1 ชุด ที่ให้ค่า Hash ออกมาตรงกันด้วย

ดูเหมือน Hash collision จะเป็นกฎธรรมชาติที่ไม่สามารถหลีกเลี่ยงได้ แต่ในกรณีของ MD5 จะมีความพิเศษมากขึ้นอีกขั้น เมื่อมีผู้ค้นพบวิธีการสร้างข้อมูลใดๆ ก็ตาม ให้มีค่า Hash ตรงกัน [33-2] จึงทำให้หน่วยงานด้านความมั่นคงปลอดภัยต่างๆ เช่น US-CERT ได้ระบุว่า MD5 เป็น Hash แบบที่มีความมั่นคงปลอดภัยไม่เพียงพอในปัจจุบัน [33-3] และควรหลีกเลี่ยงไปใช้การ Hash แบบอื่น ส่วน NIST ก็ได้แนะนำให้หน่วยงานรัฐบาลของสหรัฐฯ ใช้การ Hash แบบ SHA-2 [33-4] ซึ่งมีความยาวของค่า Hash ตั้งแต่ 28 ไบต์ (224 บิต) ขึ้นไปแทน

Hash cracking

อย่างไรก็ตาม การมีจุดอ่อนเรื่อง Hash collision ก็ยังไม่ใช่จุดอ่อนโดยตรงที่จะทำให้การเก็บรหัสผ่านด้วย MD5 ไม่มั่นคงปลอดภัย เพราะถึงแม้ผู้โจมตีจะได้รหัสผ่านที่ถูก Hash ด้วย MD5 เอาไว้ออกไป ก็ยังไม่สู้จะมีประโยชน์ต่อการใช้เข้าสู่ระบบนัก (ยกเว้นมีความผิดพลาดในการออกแบบ Application ซึ่งจะกล่าวถึงในโอกาสหน้า) ผู้โจมตีจำเป็นต้องหาทาง “ถอดรหัส” ของค่า Hash ออกมาให้เป็นรหัสผ่านได้เสียก่อน

ความจริงแล้ว Hash ไม่สามารถถอดรหัสได้ เนื่องจาก Hash ทุกชนิด ไม่ใช่การเข้ารหัส กระบวนการ Hash คือกระบวนการที่เรียกว่า “ฟังก์ชั่นทางเดียว” (One way function) ที่ไม่สามารถกระทำการย้อนกลับ (Reverse) ได้ ลองคิดถึงการนำข้อมูลขนาด 1 เทระไบต์ มา Hash ด้วย MD5 ซึ่งจะได้ 16 ไบต์เสมอ ถ้าสามารถหาวิธีแปลงข้อมูล 16 ไบต์กลับเป็น 1 เทระไบต์ ได้ก็เท่ากับว่า MD5 เป็นวิธีการบีบอัดข้อมูลที่ดีที่สุดในโลก

ดังนั้น การ “ถอดรหัส” ของ Hash ในความหมายที่เข้าใจกันทั่วไปก็หมายถึง การหาค่าตั้งต้นก่อนที่จะถูก Hash นั่นเอง ซึ่งวิธีการที่นิยมใช้กันก็คือ การใช้วิธีพยายามสุ่มรหัสผ่านที่เป็นไปได้ทีละค่า และนำไปผ่าน Hash แบบเดียวกับที่ใช้ Hash รหัสผ่านที่ได้มา แล้วเทียบกันจนกว่าจะพบค่าที่ตรงกัน ซึ่งอาจเรียกได้ว่าเป็นการ Bruteforce รูปแบบหนึ่ง ซึ่งถ้าหากรหัสผ่านมีความยาวหรือความซับซ้อนมาก กว่าจะสุ่มหารหัสผ่านที่ถูกต้องพบได้ก็ย่อมต้องใช้เวลานาน

การหาค่าตั้งต้นของ Hash จำเป็นต้องใช้ความสามารถของคอมพิวเตอร์ในการคำนวณค่า ซึ่งปัจจุบันนิยมใช้ GPU (Graphic Processing Unit) ของการ์ดแสดงผล (Display Adapter หรือ Display Card) มาคำนวณแทน เนื่องจากมีความสามารถในการคำนวณทางคณิตศาสตร์ดีกว่า CPU มาก และสามารถเพิ่มขยายความสามารถได้ด้วยการเพิ่มจำนวนการ์ดแสดงผลในเครื่อง คอมพิวเตอร์ ซึ่งสะดวกกว่าการเปลี่ยน CPU หรือเพิ่มจำนวน CPU

จากการทดลองด้วยโปรแกรม oclHashcat ซึ่งเป็นโปรแกรมที่ใช้หาค่าตั้งต้นของ Hash ด้วยการสุ่มค่าบนเครื่องคอมพิวเตอร์ที่ใช้ GPU ของ ATI รุ่น RADEON 5450 ซึ่งเป็น GPU รุ่นพื้นฐาน พบว่า สำหรับรหัสผ่านที่มีความยาว 6 ตัวอักษร และประกอบด้วยตัวอักษรทั้งตัวเล็กตัวใหญ่ สัญลักษณ์ และตัวเลข จะใช้เวลาไม่เกิน 1 ชั่วโมง ในการสุ่มค่าจนครบทุกค่าที่เป็นไปได้ใน Hash ชนิด MD5 นั่นหมายความว่า ถ้าผู้ใช้งานใช้รหัสผ่านที่มีความยาวเพียง 6 ตัวอักษรในระบบที่ใช้ Hash ชนิด MD5 ผู้โจมตีจะสามารถ “ถอดรหัส” ได้อย่างแน่นอนในเวลาไม่เกิน 1 ชั่วโมง แม้จะใช้เพียง GPU รุ่นพื้นฐานที่มีอายุร่วม 2 ปีแล้ว แต่ถ้าเพิ่มความยาวรหัสผ่านเป็น 8 และ 9 ตัวอักษร จะต้องใช้เวลามากขึ้นเป็นกว่า 300 วัน และกว่า 10 ปีตามลำดับ เพื่อสุ่มค่าจนครบทุกค่าที่เป็นไปได้ บน GPU ตัวเดิม

สำหรับตัวเลขของระยะเวลาตรงนี้คงต้องมีการอธิบายเพิ่มเติมเล็กน้อยว่า เป็นระยะเวลา “สูงสุด” ที่ต้องใช้ ซึ่งทั้งนี้ขึ้นอยู่กับรูปแบบการสุ่มค่าของโปรแกรม เช่นถ้ารหัสผ่านที่แท้จริงเป็น 000000001 และโปรแกรมเริ่มสุ่มตั้งแต่ 000000000 ก็คงทราบได้ทันทีว่าไม่ต้องรอถึง 10 ปีแน่นอน

ถ้ารหัสผ่านมีการเก็บด้วย Hash แบบอื่น เช่น SHA-1 หรือ SHA-2 ซึ่งใช้เวลาในการคำนวณมากกว่าระยะเวลาที่ใช้ในการหาค่าตั้งต้นก็ย่อมนานขึ้นไปอีก ดังนั้นแนวคิดของการใช้ Hash ที่คำนวณยากขึ้น (เช่น

SHA-2 ขนาด 512 บิต) ย่อมช่วยให้การ “ถอดรหัส” เป็นไปได้ยากขึ้น รวมถึงการใช้รหัสผ่านที่มีความยาวมากๆ เช่น 9 ตัวอักษรขึ้นไป หรือใช้ Salt ช่วย ในการเพิ่มความยาวของรหัสผ่านเข้าไปอีกชั้นหนึ่ง

Rainbow Table

ถึงแม้ GPU ระดับปานกลางที่สามารถคำนวณ Hash แบบ MD5 ได้ในระดับ 10 ล้าน Hash ต่อวินาที [33-5] จะราคาไม่แพงมากนัก แต่ก็ไม่ใช่ทุกคนที่จะมี GPU แบบนี้ใช้งาน จึงมีผู้คิดค้นวิธีที่สามารถนำผลลัพธ์จากการคำนวณ Hash มาใช้ซ้ำได้หลายๆ ครั้ง โดยไม่ต้องเสียเวลาคำนวณใหม่ หลักการคือเก็บค่ารหัสผ่านที่สุ่มขึ้นมา พร้อมกับค่า Hash ที่คำนวณออกมาได้เอาไว้ในไฟล์ โดยอาจแบ่งแยกตามความยาวของรหัสผ่านเพื่อให้ใช้งานได้ง่าย เวลานำมาใช้งานก็เพียงแค่เทียบค่า Hash ที่ต้องการหาค่าตั้งต้นมาเทียบกับค่าที่มีในไฟล์ วิธีนี้ก็จะใช้แค่ความสามารถในการค้นหาข้อมูลเท่านั้น ไม่จำเป็นต้องใช้ความสามารถในการคำนวณเลย ไฟล์ที่เก็บข้อมูล Hash และค่าตั้งต้นนี้เรียกว่า Rainbow Table

สำหรับผู้ที่มี GPU ดีๆ ใช้งาน อาจจะยอมเสียเวลาครั้งเดียวเพื่อสร้าง Hash ตามความยาว ความซับซ้อน และรูปแบบการ Hash ที่ต้องการออกมาเก็บเอาไว้ ส่วนครั้งต่อไปที่ต้องการใช้งานก็เอาไฟล์นี้ไปใช้ได้ทันที แต่ถ้าไม่มี GPU หรือไม่ต้องการเสียเวลาก็อาจใช้วิธีดาวน์โหลด Rainbow Table ที่มีผู้สร้างขึ้นมาเสร็จแล้ว และมีแจกจ่ายบนอินเตอร์เน็ตมาใช้งาน ซึ่ง Rainbow Table ที่มีแจกจ่ายนี้ ส่วนมากจะอยู่ในรูปแบบเฉพาะสำหรับโปรแกรม “ถอดรหัส” Hash แต่ละตัว เช่นไฟล์ชนิด .rti สำหรับโปรแกรม rcracki_mt [33-6] และแบ่งแยกตามชนิดของ Hash ความยาวของค่าตั้งต้น (ในที่นี้คือรหัสผ่าน) กับความซับซ้อนของรหัสผ่าน เช่น มีสัญลักษณ์พิเศษหรือไม่ เป็นต้น

ความเชื่ออย่างหนึ่งเกี่ยวกับ Rainbow Table ก็คือ มันสามารถ “ถอดรหัส” Hash ได้ทุกชนิด เรียกว่าการที่ผู้ไม่ประสงค์ดีได้ Hash ของรหัสผ่านไปนั้นก็เท่ากับได้รหัสผ่านไปโดยตรงนั่นเอง ความเชื่อนี้อาจจะไม่ผิดโดยสิ้นเชิง แต่อาจกล่าวได้ว่า ยังไม่ถูกต้องนัก เพราะการที่จะใช้ Rainbow Table ในการหารหัสผ่านที่ถูกต้องจาก Hash ใดๆ จะต้องใช้ Rainbow Table ที่สร้างขึ้นมาจาก Hash ที่ตรงกัน ความยาวรหัสผ่านตรงกัน (ไม่มากกว่าหรือน้อยกว่า) และมีความซับซ้อนระดับเดียวกันหรือมากกว่า ขั้นแรก ผู้ที่จะ “ถอดรหัส” Hash จะต้องรู้ว่าเป็น Hash ชนิดใด จากนั้นก็ต้องเดาความซับซ้อนของรหัสผ่าน ว่าต้องใช้ระดับใด ซึ่งในส่วนนี้อาจจะใช้วิธีเลือกความซับซ้อนที่สูงที่สุดเอาไว้ก่อนก็ได้ ส่วนสุดท้าย ที่ยากที่สุด คือ เดาความยาวของรหัสผ่าน เพราะอย่างที่ทราบแล้วว่า ค่า Hash จะมีค่าความยาวคงที่ ไม่ว่าจะมีค่าตั้งต้นขนาดเท่าไหร่ก็ตาม การพิจารณาความยาวของค่าตั้งต้นจากค่า Hash จึงเป็นไปได้ยาก ผู้ไม่ประสงค์ดีจะรู้ได้ว่า Rainbow Table ที่นำมาใช้มีความยาวของค่าตั้งต้นไม่ตรงกับรหัสผ่านที่ Hash เอาไว้ได้ก็ต่อเมื่อเสียเวลาลงมือไปแล้วเท่านั้น

นอกจากนี้ ในปัจจุบันก็ยังไม่ได้มีการสร้าง Rainbow Table ขึ้นมาสำหรับ Hash ทุกชนิด หรือทุกความยาวของรหัสผ่าน เพราะถึงแม้จะมี CPU หรือ GPU ที่มีความสามารถสูงๆ มากมาย แต่สำหรับ Hash ที่ต้องใช้พลังในการประมวลผลมาก เช่น SHA-2 ขนาด 256 บิตขึ้นไป รวมถึง Hash พื้นฐานเช่น MD5 เอง ในระดับความยาว 10 หรือ 12 ตัวอักษร หรือใช้ MD5 ซ้ำๆ หลายๆ ครั้ง ก็ยังจะต้องใช้เวลาในการสร้าง Rainbow Table มากจนไม่สามารถใช้ GPU ทั่วไปได้ ทำให้ยังไม่พบว่ามีการสร้าง Rainbow Table สำหรับ Hash ประเภทนี้ขึ้นมาแจกจ่ายเช่นกัน

Salting

จากที่กล่าวมาแล้วว่า รหัสผ่านยิ่งยาว ยิ่งต้องใช้เวลามากในการ “ถอดรหัส” แต่การบังคับให้ผู้ใช้งานระบบใดๆ สร้างรหัสผ่านขนาด 10 ตัวอักษรขึ้นไปก็อาจจะไม่เป็นการสะดวกแก่ผู้ใช้งานนัก วิธีการหนึ่งที่สามารถนำมาใช้เพิ่มความยาวให้กับรหัสผ่านโดยมีผลกระทบกับผู้ ใช้น้อยก็คือการเพิ่มข้อมูลที่สุ่มขึ้นมาจำนวนหนึ่งเข้าไปในรหัสผ่านที่ผู้ใช้ป้อนก่อนจะนำไป Hash ข้อมูลชุดที่เพิ่มขึ้นนี้เรียกว่า Salt ตัวอย่างเช่น เมื่อผู้ใช้งานตั้งค่ารหัสผ่านขึ้นมาเป็น “secretpassword” ซึ่งมีความยาว 14 ตัวอักษร ระบบจะสุ่มค่า Salt ขึ้นมาค่าหนึ่ง สมมุติให้เป็นค่า “fojgshU1” ซึ่งมีความยาว 8 ตัวอักษร ก่อนที่จะนำรหัสผ่านไปเก็บ ระบบจะนำรหัสผ่านกับ Salt มาต่อกัน แล้วจึงหา Hash ซึ่งจะเท่ากับ Hash นี้มีค่าตั้งต้นถึง 22 ตัวอักษร ซึ่งต้องใช้เวลาในการ “ถอดรหัส” นานกว่า Hash ของรหัสผ่านเดิมมาก ถึงแม้ว่าผู้ไม่ประสงค์ดีจะสามารถอ่านค่า Salt ของแต่ละรหัสผ่านได้โดยตรง (เนื่องจากปกติจะเก็บ Salt เป็น Plain Text) แต่ก็ไม่ได้ช่วยให้การสุ่มหารหัสผ่านที่ถูกต้องง่ายขึ้นแต่อย่างใด เพราะอุปสรรคของการ “ถอดรหัส” Hash อยู่ที่จำนวนครั้งที่ต้องคำนวณ Hash เป็นสำคัญ ในกรณีที่ให้รหัสผ่านเป็นตัวอักษรตัวเล็ก ตัวใหญ่ และตัวเลขเท่านั้น ซึ่งจะมีความเป็นไปได้ 62 แบบ จะเท่ากับว่า ถ้ารหัสผ่านยาว 14 ตัวอักษร ผู้ไม่ประสงค์ดีอาจต้อง Hash ถึง 62^14 ครั้ง ถึงจะได้ค่ารหัสผ่านที่ถูกต้อง แต่ถ้าเพิ่ม Salt เข้าไปอีก 8 ตัวอักษร จำนวนครั้งที่อาจต้องใช้จะมีถึง 62^22 ครั้ง ต่างกันถึง 218,340,105,584,896 เท่า ซึ่งเป็นเวลาที่เพิ่มขึ้นอย่างมหาศาลทีเดียว

Conclusion

1. ควรเก็บรหัสผ่านในรูปแบบ Hash เท่านั้น การเข้ารหัสลับ (Encyption) อาจไม่แตกต่างจากการเก็บรหัสผ่านเป็น Plain Text เมื่อถูกโจมตี
2. รหัสผ่านยิ่งยาว ยิ่งใช้เวลาในการ “ถอดรหัส” มาก
3. MD5 ยังเพียงพอที่จะใช้เก็บรหัสผ่าน ถ้าใช้ถูกวิธี แต่ก็ยังสู้ SHA-2 เมื่อใช้งานอย่างถูกวิธีเช่นกันไม่ได้
4. การใช้ Salt หรือ Hash ซ้ำๆ หลายๆ ครั้งช่วยเพิ่มความมั่นคงปลอดภัยได้
5. ที่ดีที่สุดคือ ระวังอย่าให้รหัสผ่านที่เก็บอยู่ ถูกเข้าถึงได้จากบุคคลภายนอก

อ้างอิง

[33-1] http://www.pcworld.com/article/161078/one_third_use_same_password.html

[33-2] http://www.win.tue.nl/hashclash/

[33-3] http://www.kb.cert.org/vuls/id/836068

[33-4] http://csrc.nist.gov/groups/ST/hash/policy.html

[33-5] http://majuric.org/software/cudamd5/

[33-6] http://www.freerainbowtables.com/en/download/

34 ข้อแนะนำในการใช้งานอินเทอร์เน็ตผ่านคอมพิวเตอร์สาธารณะ

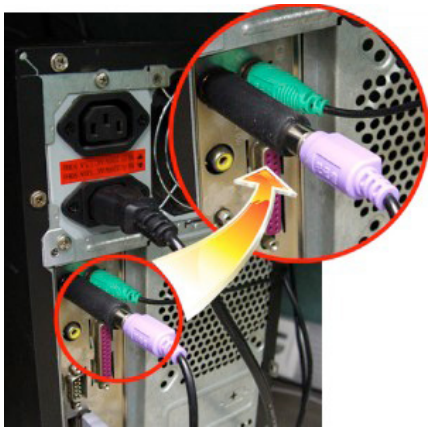
ผู้เขียน: เสฏฐวุฒิ แสนนาม

วันที่เผยแพร่: ๒๖ ต.ค. ๒๕๕๕
ปรับปรุงล่าสุด: ๒๖ ต.ค. ๒๕๕๕

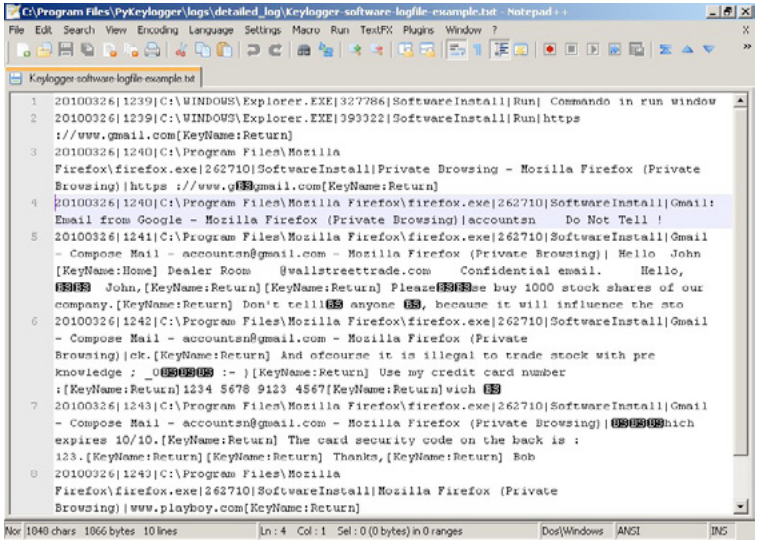
การใช้งานคอมพิวเตอร์สาธารณะนั้นมีความมั่นคงปลอดภัยต่ำ เพราะเราไม่อาจทราบได้ว่าเครื่องคอมพิวเตอร์ดังกล่าวนั้นได้ถูกผู้ไม่หวังดี ติดตั้งโปรแกรมอันตรายมาเพื่อดักรับข้อมูลหรือเปล่า หรือระบบที่เชื่อมต่ออยู่นั้นมีความมั่นคงปลอดภัยมากน้อยแค่ไหน อย่างไรก็ตาม ในบางสถานการณ์ เราอาจมีความจำเป็นที่จะต้องใช้งานอินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์สาธารณะ เพื่อเข้าถึงข้อมูลสำคัญ เช่น เช็คอีเมล หรือแก้ไขไฟล์เอกสาร เป็นต้น ดังนั้น เพื่อช่วยให้มีความมั่นคงปลอดภัยมากขึ้นในการใช้งานคอมพิวเตอร์สาธารณะ ข้อแนะนำต่างๆ เหล่านี้อาจช่วยในการปกป้องข้อมูลสำคัญจากผู้ไม่หวังดีได้

อันตรายจากการใช้งานคอมพิวเตอร์สาธารณะ

Keylogger คือฮาร์ดแวร์หรือซอฟต์แวร์ที่ทำหน้าที่บันทึกการกดปุ่มบน Keyboard ทำให้รู้ว่าผู้ที่ใช้งานคอมพิวเตอร์เครื่องนั้นพิมพ์ข้อความอะไรลงไปบ้าง [34-1] ซึ่งหาก Keylogger ถูกติดตั้งในเครื่องคอมพิวเตอร์สาธารณะ ผู้ไม่หวังดีก็สามารถได้ข้อมูลสำคัญๆ ของผู้ที่ใช้งานเครื่องนั้น เช่น Username หรือ Passsword ไปได้อย่างง่ายดาย ตัวอย่าง Keylogger เป็นดังรูปที่ 160 (34-1) และ 161 (34-2)



รูปที่ 160 (34-1) ตัวอย่าง Hardware Keylogger (ที่มา Wikipedia)



รูปที่ 161 (34-2) ตัวอย่างข้อมูลที่บันทึกโดยใช้ Software Keylogger (ที่มา Wikipedia)

Spyware เป็นซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อขโมยข้อมูลของผู้ใช้ ไม่ว่าจะเป็นข้อมูลการใช้งานอินเทอร์เน็ต ข้อมูลการตั้งค่าของเครื่อง แอบถ่ายภาพหน้าจอ หรือแม้กระทั่งแอบบันทึกเสียง เป็นต้น [2] Spyware อาจถูกติดตั้งมาในเครื่องแบบตั้งใจหรือไม่ตั้งใจก็ได้ เนื่องจากโปรแกรมที่แจกให้ผู้ใช้ดาวน์โหลดไปใช้งานได้ฟรีมีผู้พัฒนาบางราย แอบใส่ Spyware เข้ามาเพื่อเก็บข้อมูลพฤติกรรมของผู้ใช้ไว้ด้วย โปรแกรม Keylogger นั้นก็ถือว่าเป็น Spyware รูปแบบหนึ่ง

Shoulder surfing คอมพิวเตอร์บางเครื่องอาจไม่มีโปรแกรมอันตรายติดตั้งอยู่ แต่ถูกจัดวางไว้ในที่ที่คนสามารถเดินผ่านไปมาและมองเห็นสิ่งที่อยู่บนจอได้ง่าย ทำให้การยืนอยู่ด้านหลังเพื่อแอบมองรหัสผ่านนั้นสามารถทำได้ง่าย รวมไปถึงการแอบมองสิ่งที่ปรากฏอยู่บนหน้าจอจากระยะไกลนั้นก็อาจทำได้ง่าย เช่นกัน

Sniffer คือการดักรับข้อมูลที่ส่งผ่านระบบเครือข่าย หากเราเข้าเว็บไซต์ที่ใช้การเชื่อมต่อแบบ HTTP ซึ่งไม่มีการเข้ารหัสลับข้อมูลที่รับส่ง ก็อาจถูกผู้ไม่หวังดีขโมยข้อมูลสำคัญไปได้

ข้อแนะนำในการใช้งาน

เลือกใช้เครื่องที่ไม่มีคนเดินผ่านไปมาบ่อย เพื่อป้องกันการทำ Shoulder surfing และไม่ควรเลือกเครื่องที่วางอยู่ในตำแหน่งที่มีวัตถุสามารถสะท้อนแสงจากหน้า จอได้ เช่น โลหะ หรือ กระจก

ตรวจสอบ Keylogger แบบ Hardware โดยสังเกตที่สายต่อระหว่าง Keyboard กับช่องเสียบที่อยู่ด้านหลังเครื่องคอมพิวเตอร์ หากพบว่ามีอุปกรณ์แปลกๆ ถูกเสียบอยู่ อาจเป็น Keylogger ไม่ควรใช้เครื่องนั้น

บู๊ตเครื่องโดยใช้ Bootable CD หรือ Bootable USB หากเครื่องคอมพิวเตอร์สามารถบู๊ตจาก Bootable CD หรือ Bootable USB ได้ (เช่น Linux Live CD) การบู๊ตเครื่องด้วยวิธีดังกล่าวก็สามารถช่วยป้องกันอันตรายจากซอฟต์แวร์ไม่ พึงประสงค์ที่อาจถูกติดตั้งอยู่ในเครื่องดังกล่าวได้ อย่างไรก็ตาม วิธีดังกล่าวนี้อาจไม่สามารถใช้งานได้กับเครื่องคอมพิวเตอร์สาธารณะทุกเครื่อง เนื่องจากเครื่องดังกล่าวจำเป็นต้องมีการตั้งค่าการเชื่อมต่อกับเครือข่าย หรือตั้งค่าการเชื่อมต่อกับอุปกรณ์อื่นๆ ในระบบ ซึ่งการบู๊ตจาก Bootable CD หรือ Bootable USB อาจจะไม่มีข้อมูลการตั้งค่าในส่วนนี้ ทำให้ไม่สามารถเข้าใช้งานระบบเครือข่ายหรืออุปกรณ์อื่นๆ ได้ อย่างไรก็ตาม วิธีนี้เราจำเป็นต้องมีแผ่น Bootable CD หรือพก Bootable USB ติดตัวไปด้วย

ตรวจสอบ Software Keylogger และ Spyware ถ้าเครื่องที่ใช้งานมีโปรแกรมประเภท Antivirus หรือ Antispyware ติดตั้งอยู่ ก่อนใช้งาน ควรอัพเดทฐานข้อมูลของโปรแกรมและสแกนไฟล์ในเครื่องเพื่อตรวจสอบและกำจัด โปรแกรมไม่พึงประสงค์ โดยเฉพาะ Keylogger และ Spyware อย่างไรก็ตาม ถึงจะสแกนแล้วและไม่พบโปรแกรมอันตรายดังกล่าว ก็ควรใช้โปรแกรมประเภท On-Screen Keyboard ในการพิมพ์ Username และ Password ในหน้าเว็บไซต์ เพราะโปรแกรม Keylogger โดยส่วนใหญ่จะไม่สามารถดักจับข้อมูลที่พิมพ์จาก On-Screen Keyboard ได้ ตัวอย่างโปรแกรม On-Screen Keyboard เป็นดังรูปที่ 162 (34-3)

รูปที่ 162 (34-3) โปรแกรม On-Screen Keyboard ใน Windows 7 (ที่มา Microsoft)

ใช้ Portable Software เนื่องจาก Portable Software เป็นซอฟต์แวร์ที่สามารถเรียกใช้งานได้ทันที โดยไม่จำเป็นต้องติดตั้งลงในเครื่อง และโดยส่วนใหญ่จะนิยมเรียกใช้งานผ่าน USB Drive ซึ่งมีข้อดีคือข้อมูลการทำงานต่างๆ ของโปรแกรมนั้นจะถูกเก็บบันทึกลงในตัว USB Drive เอง ทำให้ปลอดภัยต่อการที่ข้อมูลรั่วไหลเนื่องจากการ Cache ข้อมูลเก็บไว้ในเครื่องได้ [34-3] ปัจจุบันมีผู้นำโปรแกรมประเภท Freeware หรือ Open Source มาพัฒนาให้เป็นแบบ Portable เพื่อให้ผู้ใช้ดาวน์โหลดไปใช้งานได้สะดวก เช่น เว็บไซต์ PortableApps.com เป็นต้น ซึ่งมีโปรแกรมที่จำเป็นสำหรับการใช้งานอินเทอร์เน็ต เช่น Browser, Instant Messenger, VoIP รวมอยู่ด้วย

ใช้งานเบราว์เซอร์ในโหมด Private Browsing หากจำเป็นต้องใช้งานเบราว์เซอร์ที่ติดตั้งอยู่ในเครื่อง ควรใช้งานเบราว์เซอร์ดังกล่าวในโหมด Private Browsing ซึ่งจะเป็นการตั้งค่าให้เบราว์เซอร์ไม่เก็บข้อมูลการใช้งานอินเทอร์เน็ต เช่น Cache, History, หรือ Cookie ไว้ในเครื่อง [34-4] ปัจจุบันโปรแกรมเบราวเซอร์โดยส่วนใหญ่มีความสามารถ Private Browsing มาด้วยอยู่แล้ว เพียงแต่จะใช้ชื่อแตกต่างกันไปในแต่ละโปรแกรม โดยที่

- Internet Explorer ใช้ชื่อ **InPrivate Browsing**
- Mozilla Firefox ใช้ชื่อ **Private Browsing**
- Google Chrome ใช้ชื่อ **Incognito mode**
- Opera ใช้ชื่อ **Private browsing**
- Safari ใช้ชื่อ **Private Browsing**

อย่างไรก็ตาม การทำงานของ Private Browsing นั้นเป็นแค่การลบไฟล์ทิ้งหลังจากที่ผู้ใช้ปิดแท็บหรือปิดโปรแกรมเบราว์เซอร์ เท่านั้น ผู้ไม่หวังดีอาจใช้โปรแกรมกู้ข้อมูลที่ถูกลบไปแล้วขึ้นมาดูได้ [34-5] [34-6]

ปิด Add-on ในเบราว์เซอร์ ถึงแม้ว่า Add-on ในเบราว์เซอร์นั้นจะมีประโยชน์ในการช่วยอำนวยความสะดวกและเพิ่มความสามารถใน การทำงานให้กับเบราว์เซอร์ แต่บาง Add-on อาจมีช่องโหว่เรื่องความมั่นคงปลอดภัย และบาง Add-on อาจทำหน้าที่เป็น Man-in-the-Browser คอยดักจับข้อมูลที่รับส่ง รวมถึงอาจแก้ไขหน้าเว็บไซต์ให้แสดงผลเว็บไซต์หลอกลวงได้ ดังนั้นเพื่อความมั่นคงปลอดภัยควรปิด Add-on ทั้งหมดในเบราว์เซอร์ หรือเลือกเปิดใช้งานเฉพาะ Add-on ที่จำเป็นเท่านั้น

ใช้การเชื่อมต่อผ่าน HTTPS การใช้งานเว็บไซต์ผ่านโพรโทคอล HTTPS ช่วยป้องกันไม่ให้ผู้ไม่หวังดีสามารถแกะข้อมูลสำคัญจากการดักรับข้อมูลได้ ดังที่เคยได้มีการอธิบายไปแล้วในบทความ วันนี้คุณใช้ HTTPS หรือยัง ดังนั้นหากเว็บไซต์ที่เข้าใช้งานรองรับการเชื่อมต่อแต่ HTTPS ก็ควรเปิดใช้งานทุกครั้ง

ใช้การยืนยันตัวตนแบบ 2 ขั้นตอน (Two-factor Authentication) ซึ่งจะเป็นการใช้ข้อมูลอีกส่วนร่วมกับรหัสผ่าน เพื่อใช้ในการเข้าสู่ระบบ ซึ่งโดยปกติแล้วจะเป็นการส่ง SMS บอกรหัสอีกชุดเข้ามายังโทรศัพท์มือถือที่ลงทะเบียนไว้กับบัญชีผู้ใช้นั้นๆ วิธีการตั้งค่าการใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอนสำหรับ Gmail และ Hotmail ได้มีการอธิบายไปแล้วในบทความ ป้องกันบัญชีผู้ใช้ Gmail / Hotmail จากการถูกแฮ็กด้วยวิธีง่ายๆ สำหรับบริการอื่นๆ สามารถศึกษาได้เว็บไซต์ของผู้ให้บริการนั้นๆ (ถ้ามี) [34-7]

ไม่บันทึกไฟล์ข้อมูลสำคัญลงในเครื่อง เพราะอาจเสี่ยงต่อการข้อมูลรั่วไหล เนื่องจากถึงแม้จะลบไฟล์ไปแล้ว แต่ผู้ไม่หวังก็ดีอาจใช้โปรแกรมกู้คืนไฟล์ที่ถูกลบไปแล้วได้ หากจำเป็นต้องบันทึกไฟล์ที่เป็นข้อมูลสำคัญเพื่อเปิดอ่านหรือแก้ไข ควรบันทึกลงในสื่อบันทึกข้อมูลภายนอก เช่น USB Drive

Logout ออกจากเว็บไซต์ทุกครั้งหลังใช้งาน เนื่องจากในบางเว็บไซต์จะมีการตั้งค่าให้จำสถานะของผู้ใช้ไว้ว่ากำลัง Login อยู่ ซึ่งถึงแม้จะปิดเบราว์เซอร์ไปแล้ว แต่หากเปิดเบราว์เซอร์แล้วเข้าเว็บไซต์นั้นใหม่ ก็จะยังคงสถานะเป็น Login อยู่ ดังนั้นเมื่อใช้งานเว็บไซต์ต่างๆ เสร็จเรียบร้อยแล้ว ควร Logout ทุดครั้ง เพื่อป้องกันการสวมรอยเข้าใช้งาน

Restart เครื่องหลังใช้งาน เนื่องจากในการใช้งานคอมพิวเตอร์ จะมีการเก็บข้อมูลไว้ใน RAM เพื่อใช้ในการประมวลผล ซึ่งหากเครื่องนั้นมี RAM น้อย เครื่องก็จะเอาข้อมูลส่วนที่เกินมาเก็บไว้ในฮาร์ดดิสก์ ซึ่งเรียกว่า Virtual Memory, Pagefile หรือ Swap ซึ่งถึงแม้จะปิดโปรแกรมไปแล้วก็ยังอาจมีข้อมูลสำคัญหลงเหลืออยู่ภายใน RAM หรือใน Virtual Memory ได้ การ Restart เครื่องจะเป็นการเคลียร์ข้อมูลที่อยู่ในส่วนนี้ออกไป [34-8]

ไม่ใช้งานธนาคารออนไลน์หรือทำธุรกรรมที่เกี่ยวข้องกับการเงิน เนื่องจากทั้งเครื่องคอมพิวเตอร์สาธารณะและเครือข่ายที่เชื่อมต่ออยู่นั้น ไม่สามารถแน่ใจในความมั่นคงปลอดภัยได้ เพื่อความไม่ประมาทจึงไม่ควรเข้าใช้งานเว็บไซต์ที่เกี่ยวข้องกับการทำธุรกรรมทางการเงิน

รีบเปลี่ยนรหัสผ่านทันทีที่สามารถทำได้ เพื่อเป็นการป้องกันในกรณีที่รหัสผ่านหลุดออกไป

ข้อแนะนำที่กล่าวถึงข้างต้นนี้สามารถช่วยให้การใช้งานอินเทอร์เน็ตผ่านคอมพิวเตอร์สาธารณะมีความมั่นคงปลอดภัยเพิ่มขึ้นได้ แต่อาจช่วยได้ในระดับหนึ่งเท่านั้น ผู้ใช้งานควรใช้ด้วยความระมัดระวัง และพึงระลึกไว้เสมอว่า การกระทำธุรกรรมต่างๆ โดยใช้คอมพิวเตอร์สาธารณะนั้นมีความเสี่ยงเสมอ

อ้างอิง

[34-1] http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1

[34-2] http://searchsecurity.techtarget.com/definition/spyware

[34-3] http://portableapps.com/about/what_is_a_portable_app

[34-4] http://www.howtogeek.com/117776/htg-explains-how-private-browsing-works-and-why-it-doesnt-offer-complete-privacy/

[34-5] http://www.techrepublic.com/blog/security/how-do-new-private-browsing-capabilities-affect-forensics/654

[34-6] http://www.ehow.com/info_12229669_recovery-private-browsing-cache-firefox.html

[34-7] http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two+factor-authentication-right-now

[34-8] http://support.microsoft.com/kb/314834

จัดพิมพ์และเผยแพร่โดย
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 เลขที่ 120 หมู่ 3อาคารรัฐประศาสนภักดี
(อาคาร B) ชั้น 7 ถ.แจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

เว็บไซต์ไทยเซิร์ต www.thaicert.or.th
เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) www.etda.or.th
เว็บไซต์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร www.mict.go.th