Malware Analysis without Sandbox

Nishant Ranjan | Regional Solutions Architect - SEA
Agenda

- Cyber Threat Landscape – *The World we live in*
- Sandbox Evasion proof points
- What Industry is doing!
- McAfee Approach
The World we live in – *Snapshot of last week*

**MONDAY**

UK Parliament Hit by Cyberattack, Up to 90 MPs' E-mail Accounts Hacked

Monday, June 26, 2017  ▶ Mohit Kumar

**FRIDAY**

Microsoft's Private Windows 10 Internal Builds and Partial Source Code Leaked Online

Friday, June 23, 2017  ▶ Mohit Kumar

**THURSDAY**

New GhostHook Attack Bypasses Windows 10 PatchGuard Protections

Thursday, June 22, 2017  ▶ Swati Khandelwal

Honda plant hit by WannaCry ransomware attack

Financial Times - 21 Jun 2017  
Honda has become the latest victim of the WannaCry cyberattack that crippled computer systems worldwide last month. The Japanese ...  
Cyber Attack At Honda Stops Production After WannaCry Worm Strikes

**WEDNESDAY**

Web Hosting Company Pays $1 Million to Ransomware Hackers to Get Files Back

Monday, June 19, 2017  ▶ Mohit Kumar
The World we live in – *Snapshot of last week*

**Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers**

Russian energy firms and Danish shipping company also hit by hackers

**Attack of 'ransomware' in the Spanish headquarters of two large multinationals**

The offices of DLA Piper and Mondelez in Spain are totally paralyzed: the firms have suffered this morning a computer attack that has crippled their entire computer system.
The World we live in – Spread of WannaCry

https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html
The World we live in – Where does Thailand stand

YoY rise in Cyber attack

ThaiCERT Incident Statistics 2017
Targeted Attack Lifecycle

**Prepare**
- Business-social-technical recon
- Probe the perimeter
- Test defenses

**Compromise**
- Package
- Deliver
- Exploit payload to establish foothold

**Maneuver**
- Establish interactive connection
- Escalate privileges
- Expand laterally

**Execute**
- Encrypt Files
- Demand Ransom
- Persist
Targeted Attack Lifecycle – Evasion Techniques

- Obfuscation
- Antimalware vendor network detection
- **Sandbox Evasion**

**Prepare**
- Packing file
- Anti-debugging
- Obfuscation
- Fake metadata

**Compromise**
- **Sandbox evasion**
- Code injection
- Bypass antimalware/user account control
- Self-deletion

**Maneuver**
- Network evasion
- Encryption
- Stealth
- TOR network

**Execute**

Rise in Sandbox Evasion

Anti-sandboxing has become more prominent because more businesses are using sandboxes to detect malware

Evasion Technique Use by Malware

- 23.3% Anti-sandbox
- 18.3% Code injection
- 16.1% Anti-debugging
- 21.2% Anti-monitoring
- 21.1% Anti-security tools

Rise in Sandbox Evasion

Anti-sandboxing has become more prominent because more businesses are using sandboxes to detect malware

Rise in Sandbox Evasion

**Locky Ransomware**
Uses command-line argument to evade automated sandbox analysis.

**Dridex banking Trojan**
Checks the value of the registry key
"HKLM\SYSTEM\ControlSet001\Services\Disk\Enum"

Rise in Sandbox Evasion

**Nymain downloader**
- Checks the date and do not execute after the end of the campaign.
- Checks whether the malware’s filename hash is on the system. If it is, an analysis could be underway.
- Check for a MAC address related to a virtual environment.
- Check the registry key HKLM\HARDWARE\Description\System\“SystemBiosVersion” to find the string “VBOX.”

**Necurs Trojan**

[Code snippet showing evasion techniques]

What Industry is doing!
Perform Analysis on EndPoint

Using the power of Machine Learning

Static Analysis (file type, resources, meta-data)
Fuzzy Hashing (identical byte or checksum sequences)
Import Address Hash (function calls, order of function calls)
Dynamic Analysis (file system, registry, network behaviors)
Memory Analysis (process or system memory analysis)
Unsupervised Machine Learning

How can we determine which dog falls into which breed?

We are given a large set of dogs of different breeds (Chihuahuas, Beagles, Dachshunds). We can use two features to distinguish them - their height and weight.
Similarity: Prototype-Based Clustering

Beagles

Dachshunds

Chihuahuas

Euclidean distance between two objects
Similarity: Classification-Based on Clustering

- Beagle
- Beagles
- Chihuahuas
- Dogs
- Dachshunds

Euclidean distance between two objects

Height

Weight
Leveraging Multiple Sources of Knowledge

- Identify a suspicious characteristic or activity
- The object is given a reputation and confidence level if existing signatures based methods don’t detect
- **Pre-execution:** Static file feature extraction (file type, import hash, entry point, resources, strings, packer and compiler details, compile time, APIs, section names)
- **Post-execution:** Behavioral features and memory analysis (behavioral sequence, process tree, file system, registry events, network communication events, mutex, strings from memory)

A hybrid approach provides the best classification rates!
Extracting Static Features

Ransomware: CTB-Locker (pre-execution)

- File type, resources, and strings
- Packer and compiler details
- Compile time, entry point
- Import address hash,
- Function calls and APIs
Extracting Behavioral Features
Ransomware: CTB-Locker (post-execution)

File system, registry and network changes actions it begins encrypting files

- **Generates** a unique computer identifier
- **Surviving** reboot by moving itself into Appdata folder
- **Deactivate**: Shadow copies, Startup repair, Windows error recovery
- **Stops**: Windows Security Center, Defender, Update Service, Error reporting and BITS
- **Inject**: into explorer.exe, svchost.exe
- **Retrieve**: External IP-address
- **Starts encryption process**
What McAfee is doing

A Layered approach
McAfee® Endpoint Security Platform Threat Prevention

Layered Approach

- Whitelisting (Hash + Cert)
- Engine + DAT
- Global Threat Intelligence
- Threat Intelligence Exchange (Hash + Cert)
- Real Protect - Static
- Dynamic App Containment
- Real Protect - Behavioral

Adaptive Protection

Pre-Execution
Post-Execution
DAC – Dynamic Application Containment

1. Saves “Patient Zero”: Reduces or eliminates ability of greyware to make malicious changes to the endpoint (without requiring a security sandbox appliance).

2. Helps defeat “Sandbox-aware” malware: Since it happens on the endpoint (i.e. NOT a VM), malware is less-likely to detect the containment.

3. Dramatically speeds up the threat defense lifecycle: Detection occurs at the endpoint. Correction “not needed” since the malware is “already contained”, thus increasing IoC/IoA detection speed and stopping “infection” before it begins.

4. Enables crowd-sourcing of zero-day malware analysis: Enables McAfee to Crowd-Source 100,000,000++ endpoints for malware analysis in our cloud!
How “DAC” Containment Works...

1. Endpoint receives malware
2. Reputation Business Object provides reputation score
3. Based on score, ENS calls for Dynamic Application Containment (DAC)
4. Perform endpoint detections on behavior, access violations, memory scanning, etc. safely
5. RealProtect sends comparison results to endpoint to be acted upon
6. If dirty, report as such. If clean, allow object to run again.
Real Protect – *McAfee implementation of Machine Learning*

- Malware authors can change “how malware looks” (appearance, fingerprint, etc.)
- They seldom change all features of malware
- So if we perform Statistical Correlation on ALL the features of the malware, *static and behavioral*, then we should achieve invariant recognition
RealProtect Static Summary

Proactively Find Malware via Static-Analysis Machine Learning

Detects more “zero-day” malware on the endpoint, based on actual malware static file attributes, than any previous reactive signature-based method.
1. RealProtect Static gathers static properties (or features) from known-malware binaries on the backend

2. This information is fed to Machine-Learning ("ML") algorithms on the backend to create "RealProtect Static ML Models" of each malware binary type

- Multiple attributes, e.g.
- Compiler
- Language
- Size
- Linked DLLs
- Library References
- Etc.
- And many more...
3. On the endpoint, RealProtect Static can query either the local “ML Model” library or do a match lookup in the Cloud depending on the product solution.

4. If a match occurs, then RealProtect Static informs the endpoint solution of this fact and remediation will occur if needed.
Real Protect Static Technology Value Proposition

1. **Detects Zero-Day Malware Pre-Execution:** Detects obfuscated, polymorphic malware with static attribute analysis comparing to known malware.

2. **Works in Presence of Blocking Protection as well as Offline:** Improves detection in conjunction with use of Dynamic Application Containment or HIPS, Firewall, etc. or Offline.

3. **Faster Response + Reduced need for human analysis:** Analysis and match happen very quickly, ML-based system means this is extensible with very few resources.

4. **Requires very few resources on the Endpoint:** Both RAM and HDD/SSD requirements are very modest (a few MB).

5. **Reduces Endpoint Administrator Headaches:** Due to dramatic reduction in zero-day malware remediation.

**RealProtect Static = Detect malware on the endpoint based on analysis of static file attributes**
RealProtect Dynamic Technology

Unmask the Attack
Uncover the Hidden Malware

- Malware hides in the file system, but always performs malicious actions as a process.
- Therefore, if we analyze malware behavior, then we can match against known malware behaviors using an automated learning algorithm.
- This is one of the best ways to catch things like exploits or legitimate application misuse, which are hard to detect with static-only methods.
- RealProtect Dynamic is proactive protection through dynamic behavior analysis on the endpoint, comparing in the Cloud to known malware for a match.
How Real Protect Dynamic Detection Works...

1. Endpoint receives greyware. Based on intelligence scoring, Endpoint security product asks for a RealProtect assessment.

2. RealProtect allows process(es) to run and traces behaviors.

3. RealProtect sends behavior information to the Cloud for analysis.

4. RealProtect Cloud uses Machine Learning to compare behavior to known malware behavior(s).

5. RealProtect sends comparison results to endpoint for disposition.

6. If dirty, Endpoint asks RealProtect for remediation.
Classification with Real Protect

Graphic representation of clusters with samples which are similar
What Are We Showing Here?

RealProtect Behavioral Demonstration

1. Shows RealProtect Behavioral protecting against an instance of zero-day malware (Phishing attachment)

2. Demos how traditional signature-based scans would miss the malware, but RealProtect will detect and then remediate the threat in near real-time
Signature-based defenses don’t detect this zero-day malware

This is Process Explorer so we can see processes running
Let’s bring up ENS’ Control Panel...
We open the fake invoice...

Display of “Invoice” is a delaying tactic to give the malware time to create sub-processes...
However, with RealProtect running, we trace the behavior and send to Cloud for automatic classification. (all in the background) RealProtect matches it against known-malware and returns a conviction.
The Endpoint halts the process(es) and does an automatic remediation. All RealProtect actions taken are shown in the ENS event log. Endpoint is secure from the zero-day malware.