LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Fileless Malware

09/10/2020

Report #: 202009101030

Agenda

- Executive Summary
- What is Fileless Malware
- What makes it different than other malware
- Tools, Techniques, and Procedures
- Case Studies
- Defending Against Fileless Malware
- Summary

Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Executive Summary

- Fileless malware: Anatomy and Differences
  - “a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove” (McAfee, 2020)

- Operates mainly in memory
  - Entry point for other malware

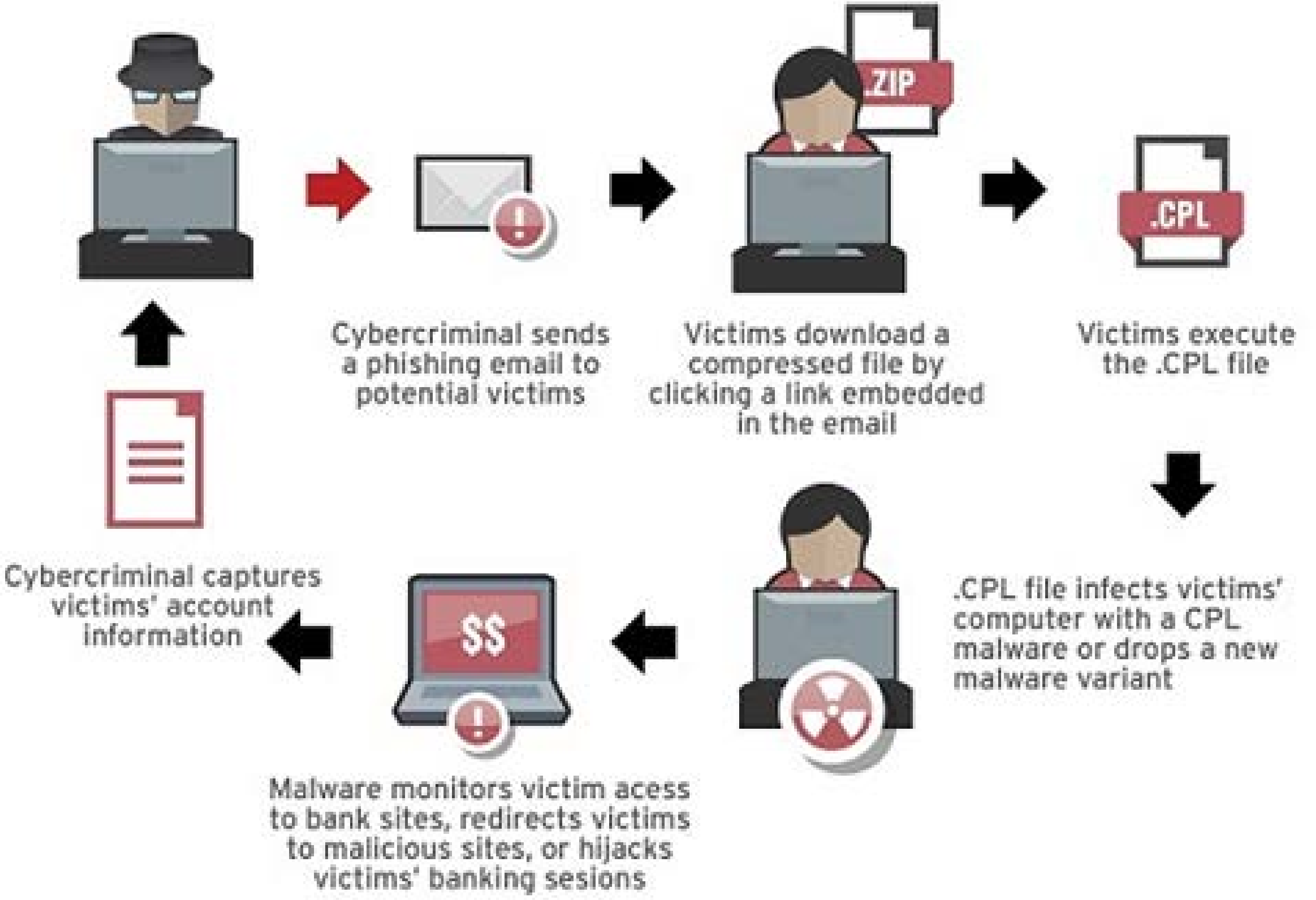
- Heavy use of
  - Social Engineering
  - PowerShell

The site ahead contains malware

Attackers currently on malware.testing.google.test might attempt t
programs on your Mac that steal or delete your information (for examp
passwords, messages and credit cards).

Photo credit Christiaan Colen

Anatomy of a Malware attack



Cybercriminal sends a phishing email to potential victims

Victims download a compressed file by clicking a link embedded in the email

Victims execute the .CPL file

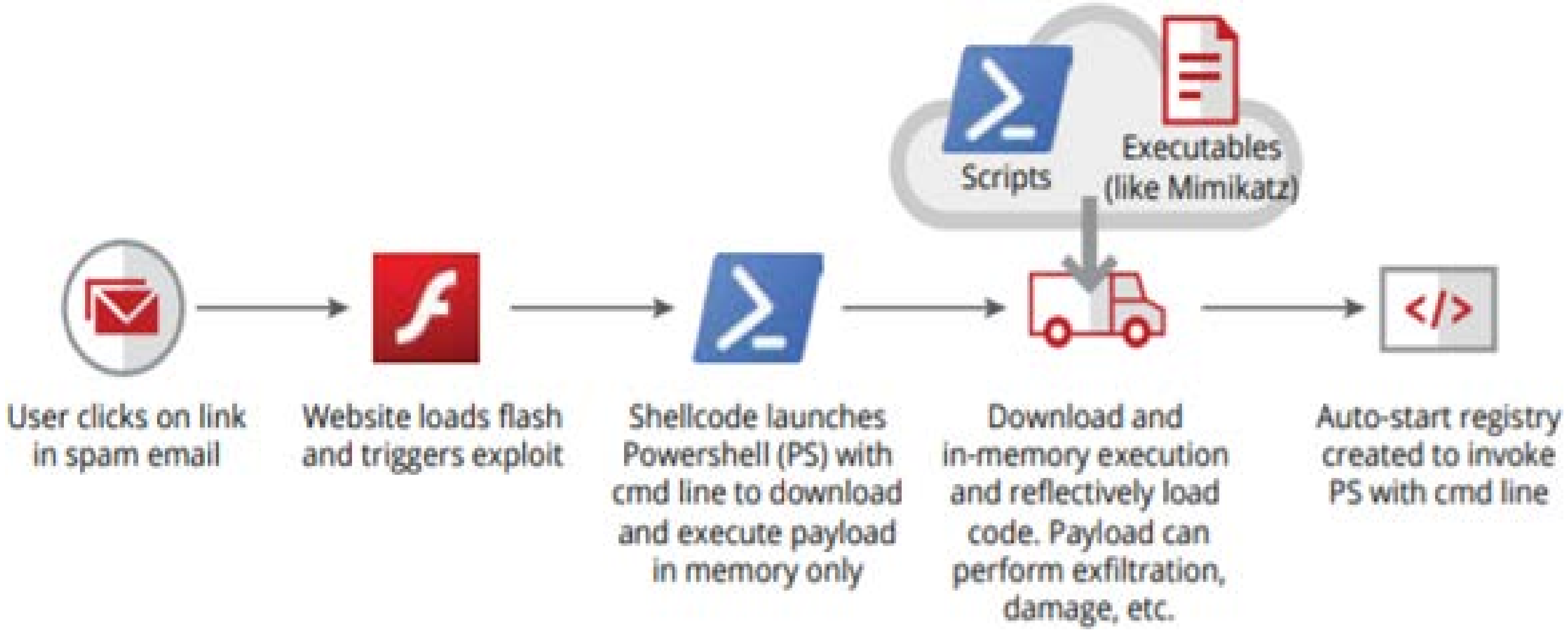
.CPL file infects victims' computer with a CPL malware or drops a new malware variant

Malware monitors victim acess to bank sites, redirects victims to malicious sites, or hijacks victims' banking sesions

Cybercriminal captures victims' account information

Trend Micro 2020

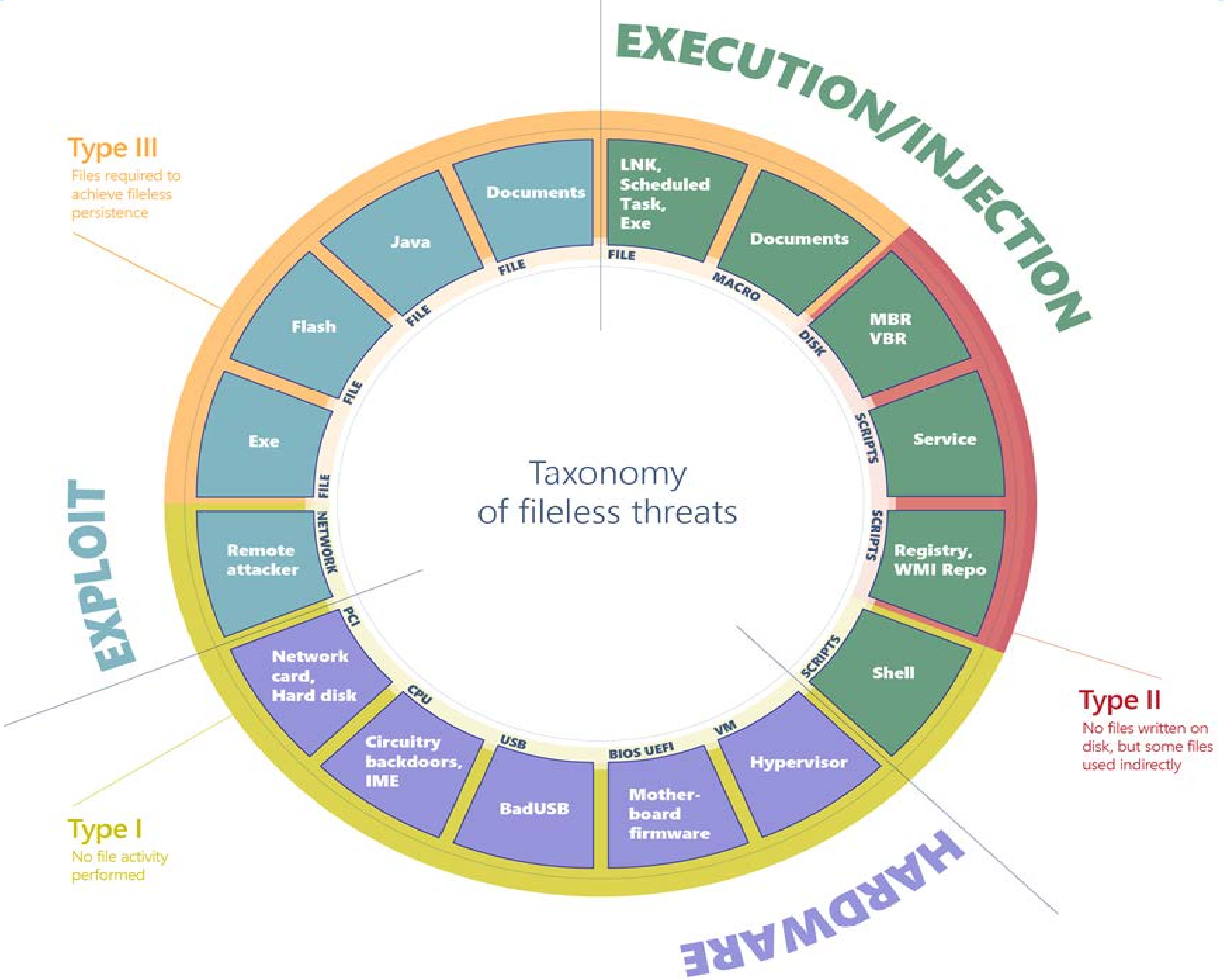
Why is Fileless Malware Different?



Scripts
Executables (like Mimikatz)
User clicks on link in spam email
Website loads flash and triggers exploit
Shellcode launches Powershell (PS) with cmd line to download and execute payload in memory only
Download and in-memory execution and reflectively load code. Payload can perform exfiltration, damage, etc.
Auto-start registry created to invoke PS with cmd line

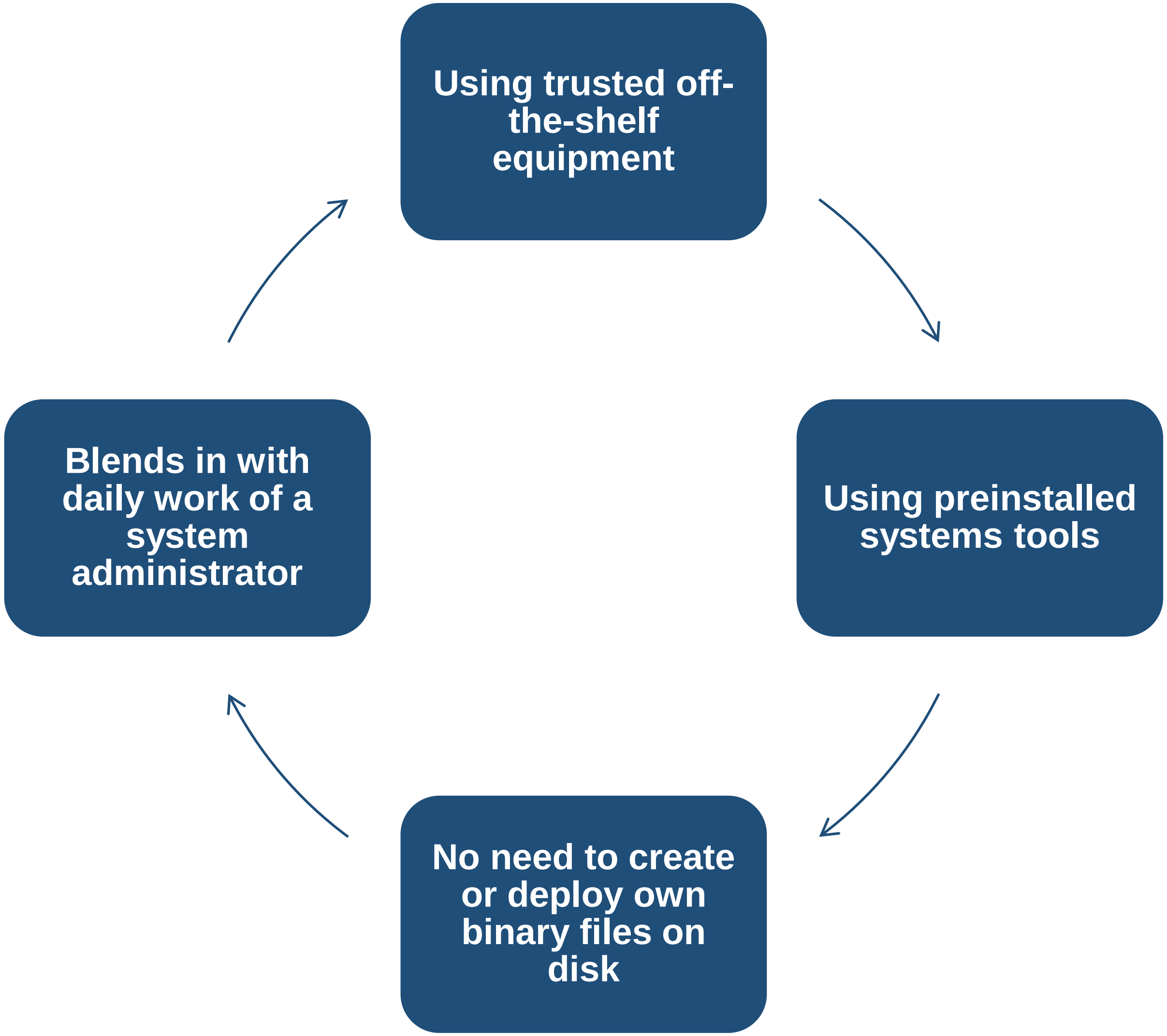
McAfee 2020

Types of Fileless Malware



Microsoft 2020

Living off the Land



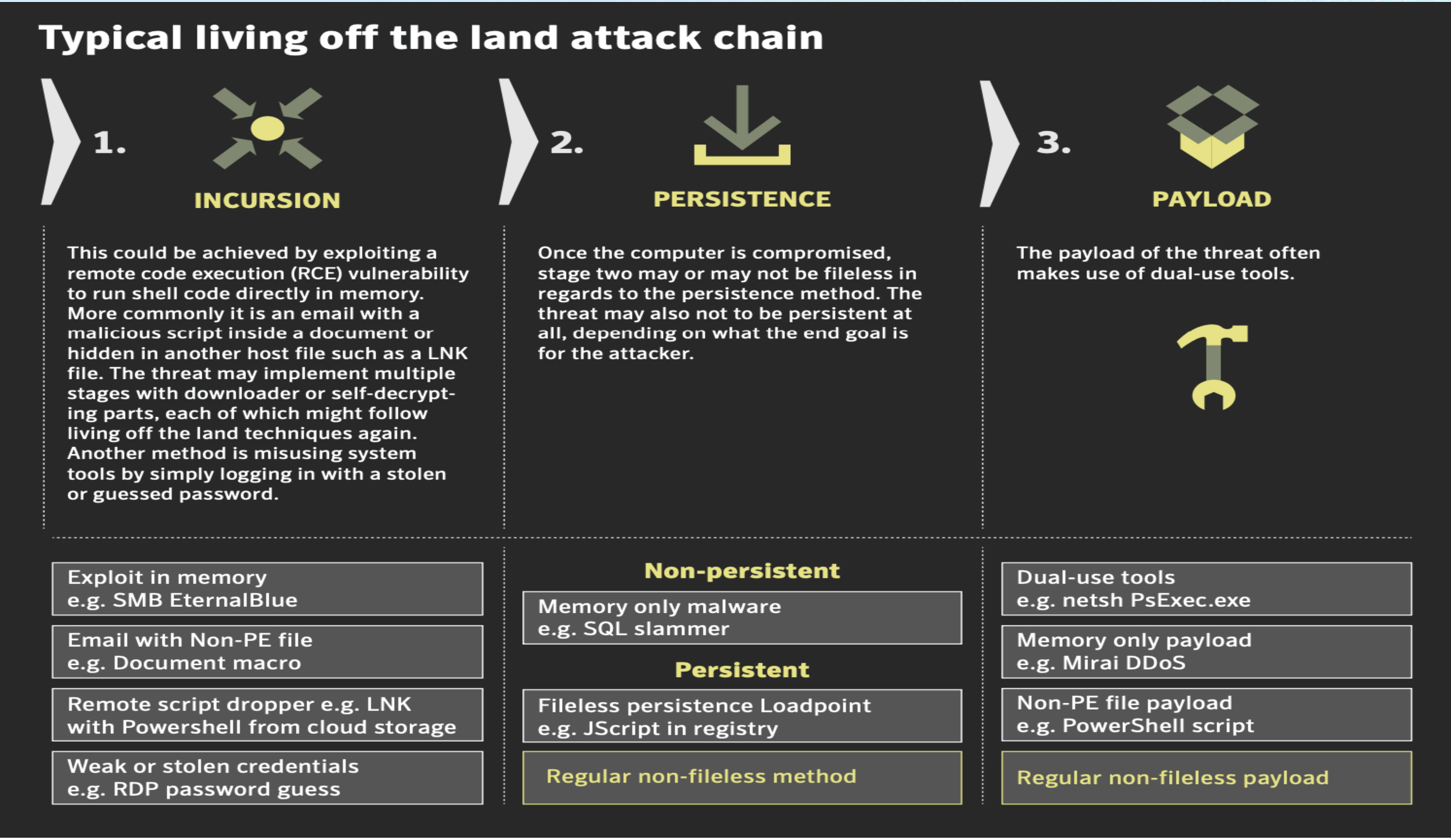
Using trusted off-the-shelf equipment

Using preinstalled systems tools

No need to create or deploy own binary files on disk

Blends in with daily work of a system administrator

Living Off the Land Attack Chain



Typical living off the land attack chain

1. INCURSION

This could be achieved by exploiting a remote code execution (RCE) vulnerability to run shell code directly in memory. More commonly it is an email with a malicious script inside a document or hidden in another host file such as a LNK file. The threat may implement multiple stages with downloader or self-decrypting parts, each of which might follow living off the land techniques again. Another method is misusing system tools by simply logging in with a stolen or guessed password.

- Exploit in memory
  e.g. SMB EternalBlue
- Email with Non-PE file
  e.g. Document macro
- Remote script dropper e.g. LNK with Powershell from cloud storage
- Weak or stolen credentials
  e.g. RDP password guess

2. PERSISTENCE

Once the computer is compromised, stage two may or may not be fileless in regards to the persistence method. The threat may also not to be persistent at all, depending on what the end goal is for the attacker.

Non-persistent

- Memory only malware
  e.g. SQL slammer

Persistent

- Fileless persistence Loadpoint
  e.g. JScript in registry
- Regular non-fileless method

3. PAYLOAD

The payload of the threat often makes use of dual-use tools.

- Dual-use tools
  e.g. netsh PsExec.exe
- Memory only payload
  e.g. Mirai DDoS
- Non-PE file payload
  e.g. PowerShell script
- Regular non-fileless payload

Wueest 2017

Fileless Attack Methods

Memory only threats

- These infections are not persistent. Restart will disinfect system
- Shellcode loads payload into memory without writing it to disk

Fileless persistence

- Windows Registry – Most popular fileless load point method is storing a script in the Windows registry
- Windows Management Instrumentation – Can stop process and execute scripts
- Group Policy Objects – Can be used to add a backdoor
- Scheduled Tasks – May be used to bypass User Account Controls

Dual-use tools

- Clean applications can be dual purposed by attacker
- Most system tools can be used in an unintended way

Non-Portable Executable (non-PE) file attacks

- Office documents with macros and scripts
- Involves a script and a legitimate tool
- Host system tool is a powerful scripting framework (PowerShell, WScript, CScript)

Fileless Attack Vectors

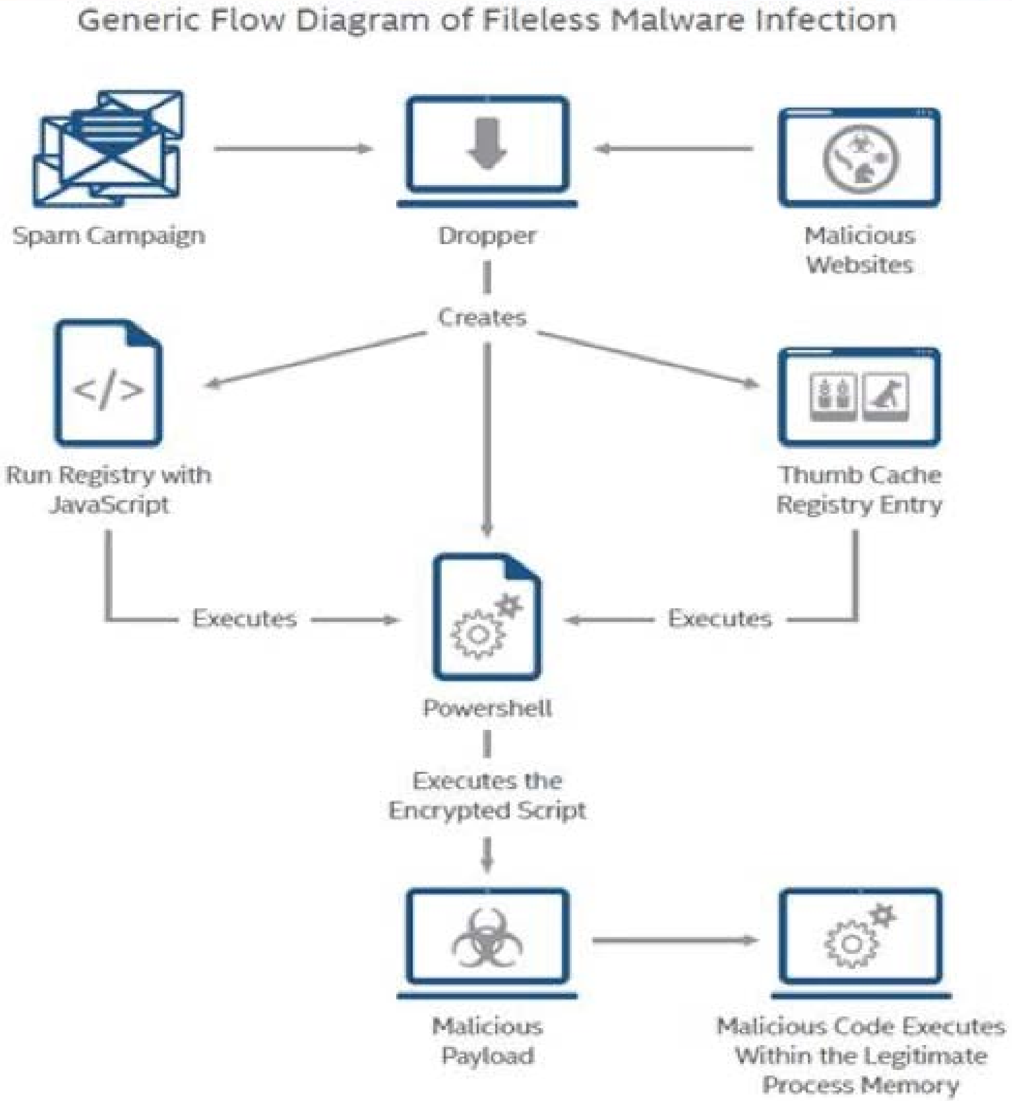
PowerShell

- Powerful interactive command-line interface and scripting environment in the Windows OS used to automate tasks
- May be used to download and run executables from the internet which can be executed in memory without touching disk
- PowerShell commands/scripts can be executed without directly invoking powershell.exe

Why Use PowerShell for Fileless Malware Attacks

- PowerShell is installed by default on Windows
- Sysadmins frequently use and trust PowerShell.
- PowerShell scripts are easy to obfuscate and can be difficult to detect in legacy security tools
- Has remote access capabilities by default, so can be used remotely by attackers

Fileless Attack Vectors


Generic Flow Diagram of Fileless Malware Infection
Spam Campaign
Dropper
Malicious Websites
Creates
Run Registry with JavaScript
Thumb Cache Registry Entry
Executes
Executes
Powershell
Executes the Encrypted Script
Malicious Payload
Malicious Code Executes Within the Legitimate Process Memory

McAfee 2017

Fileless Attack Vectors

Windows Management Instrumentation (WMI)

- Provides management of all Windows devices on a network
- Can be used to configure security settings like system properties, scheduling processes, user groups, or disabling error logs

Why Use WMI in a Fileless Malware Attack

- Installed by default on Windows OS
- WMI is frequently used and trusted by sysadmins
- WMI is given more credibility because every permanent WMI event subscription runs as SYSTEM
- Almost every OS action can trigger a WMI event, making it incredibly easy to use in combination with operating system actions

Fileless Attack Vectors

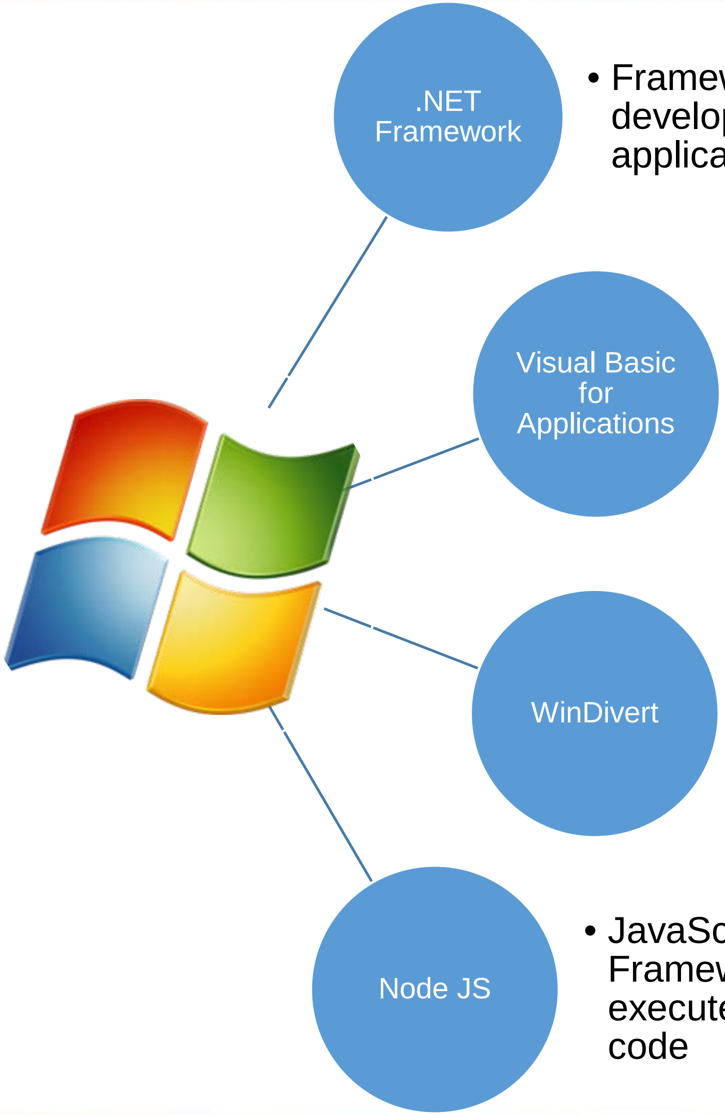
Metasploit Meterpreter

- Metasploit is a penetration testing framework used by attackers to connect to PowerShell on the victim's side
- Meterpreter is an attack payload within Metasploit

Why use Metasploit Meterpreter in a Malware Attack

- Meterpreter resides entirely in memory and writes nothing to disk
- No new process are created when Meterpreter injects itself into the compromised process and can migrate to other processes easily
- Uses encrypted communications by establishing a TLS/1.0 link
- Provides limited forensic evidence and impact on the victim machine

Fileless Attack Vectors



.NET Framework

- Framework to develop applications

Visual Basic for Applications

- VBA scripts are macros embedded in Word/Excel to automate tasks

WinDivert

- Network packet capture and manipulation utility

Node JS

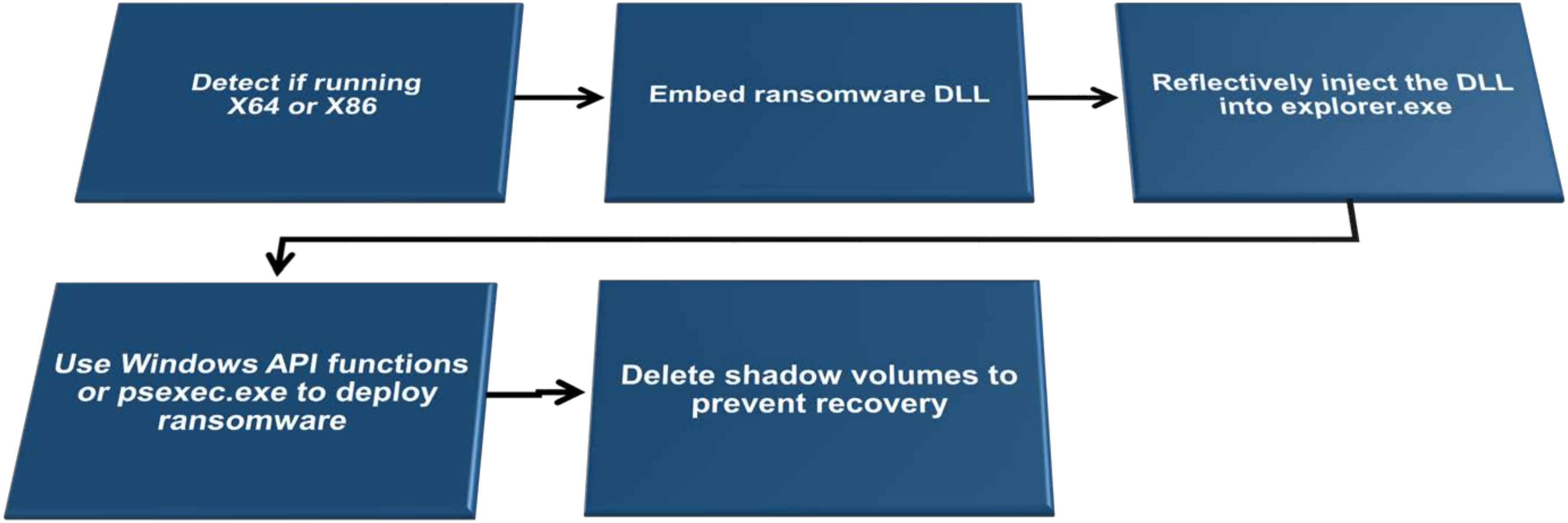
- JavaScript Framework to execute JavaScript code

Microsoft

Case Studies

Threat using Fileless Methods	Description
Netwalker **MITRE, 2020**	- Ransomware attack that uses fileless methods to gain access to systems - Exploited VPN vulnerabilities - Taken advantage of the COVID-19 pandemic - Collected over $25 million since March 2020
Nodorsok/Divergent	- Named Nodorsok by Microsoft and Divergent by Cisco Talos - Malware that employs advanced fileless techniques - Turns PCs into Proxies - Used for adware/click fraud - Reported last fall to have turned thousands of PCs into Zombie Proxies with malicious intent.
Not Petya **MITRE (2), 2020, McAfee (2), 2017**	- Not Petya emerged in June 2017 - Has infected organizations in several sectors, including finance, transportation, energy, commercial facilities, and healthcare causing $10 billion in damages worldwide - Infects computers Master Boot Records - Encrypts files without any way to decrypt wiping files from the infected machines

Case Studies: Netwalker TTPs



Detect if running X64 or X86

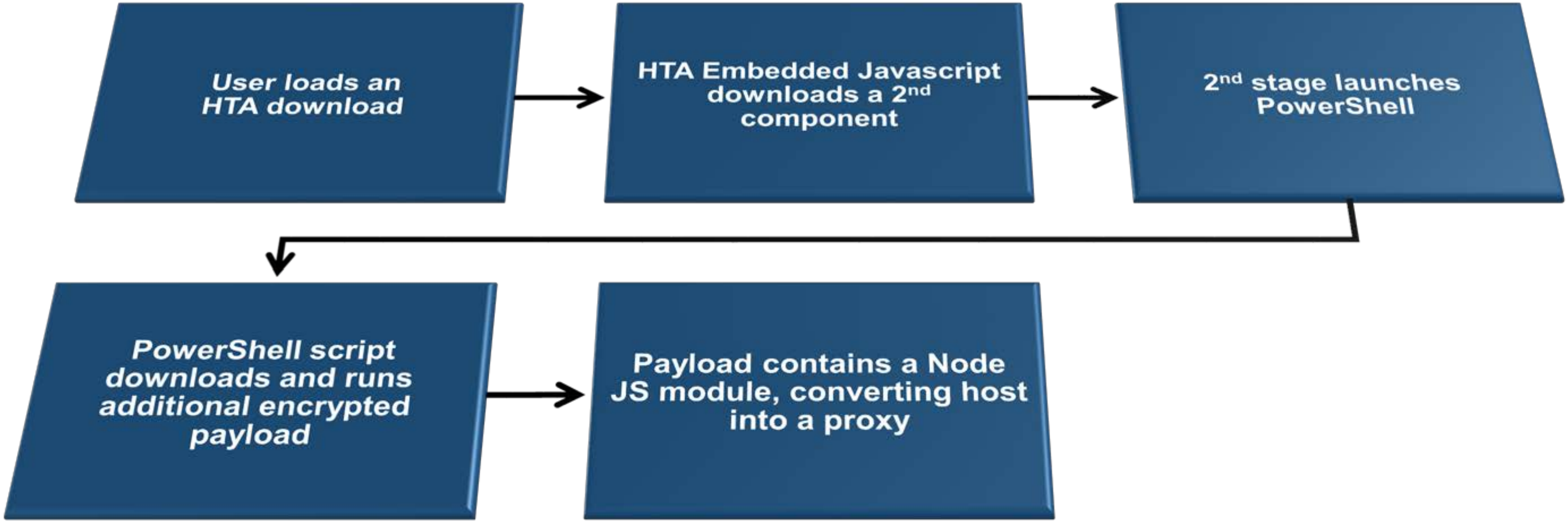
Embed ransomware DLL

Reflectively inject the DLL into explorer.exe

Use Windows API functions or psexec.exe to deploy ransomware

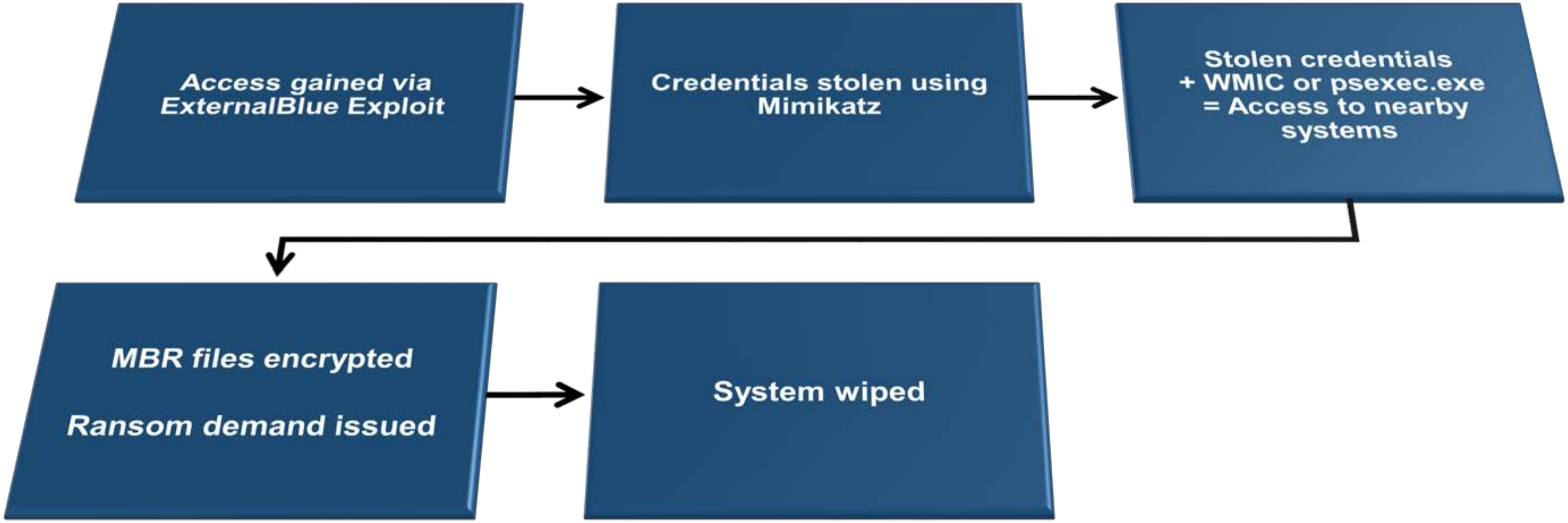
Delete shadow volumes to prevent recovery

Case Studies: Nordosok/Divergent TTPs



User loads an HTA download
HTA Embedded Javascript downloads a 2nd component
2nd stage launches PowerShell
PowerShell script downloads and runs additional encrypted payload
Payload contains a Node JS module, converting host into a proxy

Case Studies: Not Petya TTPs



Access gained via ExternalBlue Exploit

Credentials stolen using Mimikatz

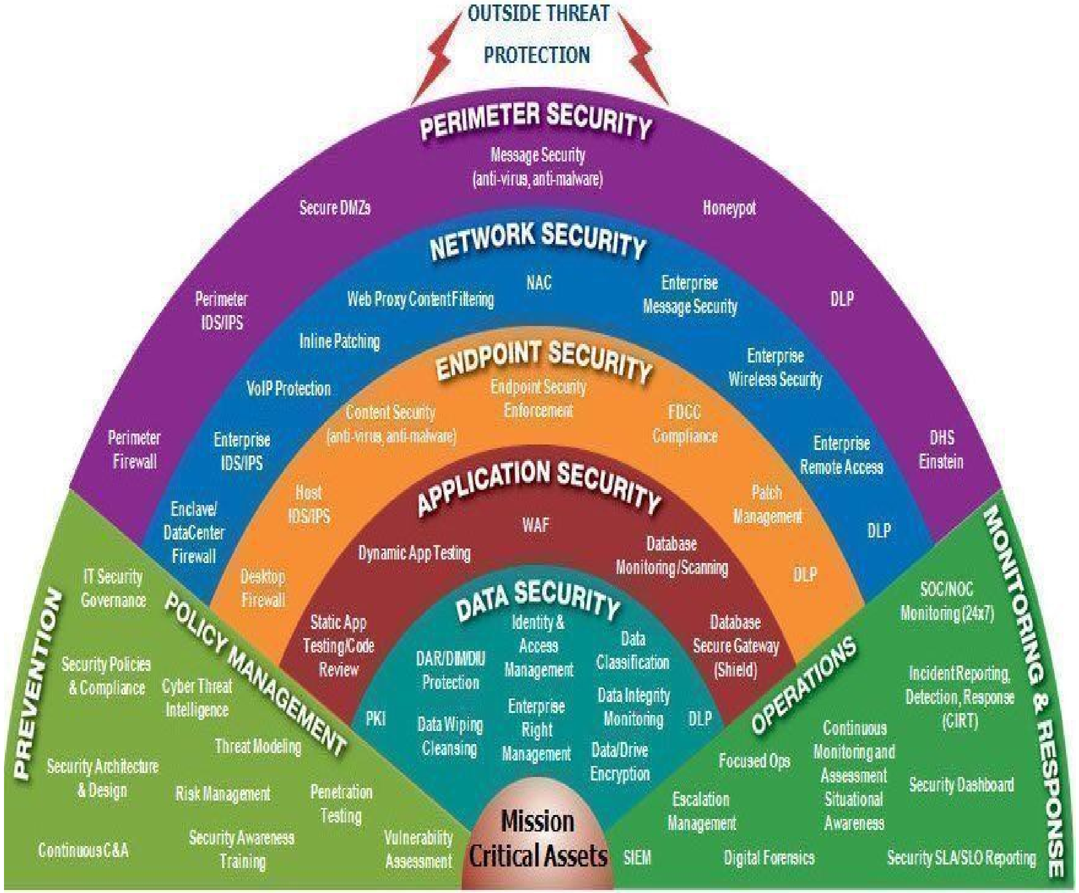
Stolen credentials
+ WMIC or psexec.exe
= Access to nearby systems

MBR files encrypted

Ransom demand issued

System wiped

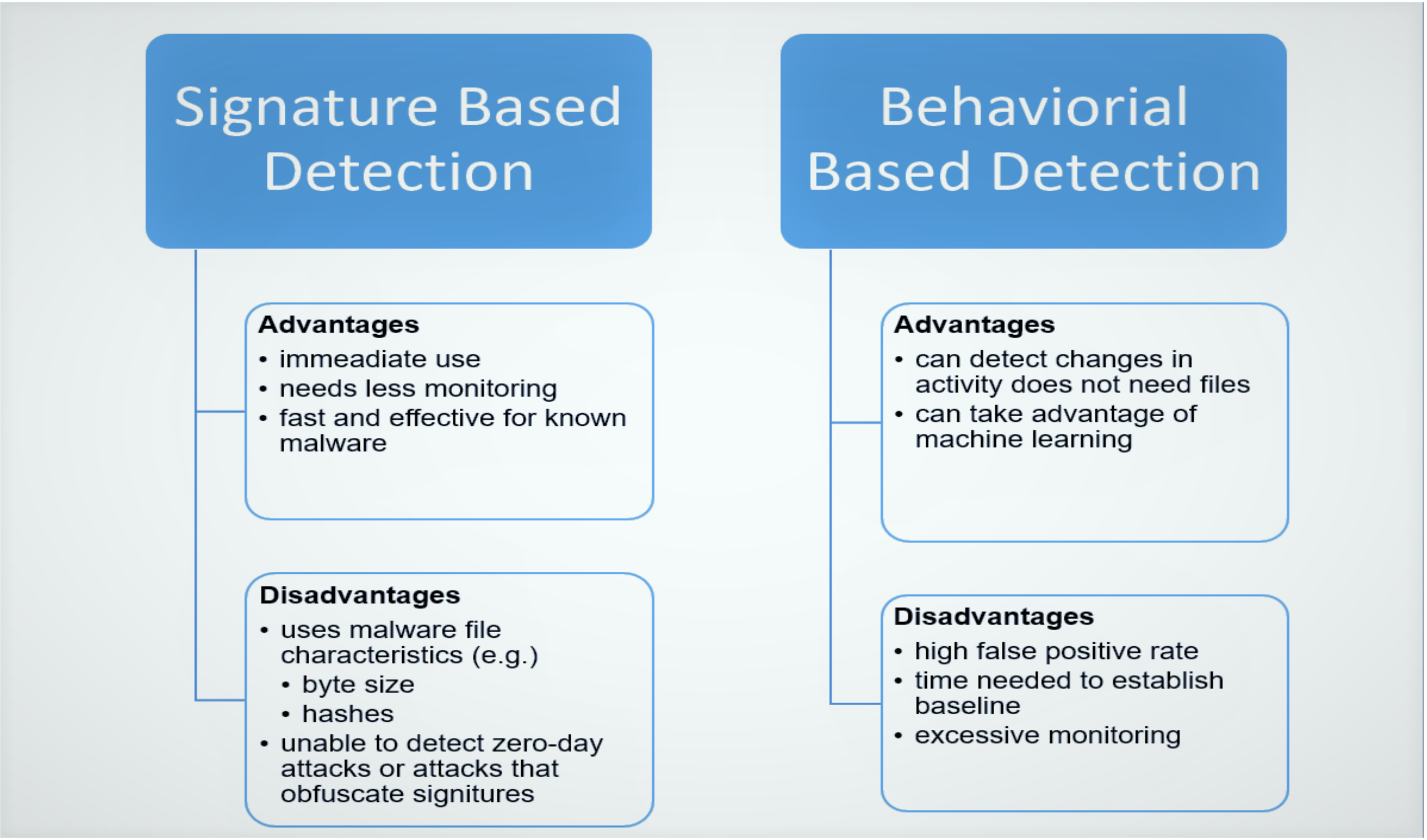
Defending Against Fileless Malware



Fisher 2018

- Practice strong cyber hygiene and defense in depth
- Train users to identify and guard against Social Engineering
- Instituting Least Privilege and Zero Trust Privilege
- Secure PowerShell use by taking advantage of its logging capability to monitor suspicious behavior.
- Use PowerShell commands such as Constrained Language Mode to secure systems from malicious code.
- Properly configure system components, apply updates and disable unused and outdated systems to block possible entry points.
- Never download and execute files from unfamiliar sources
- Use network detection and responses security solutions that utilize behavior monitoring

Defending Against Fileless Malware



Signature Based Detection

Advantages

- immeadiate use
- needs less monitoring
- fast and effective for known malware

Disadvantages

- uses malware file characteristics (e.g.)
  - byte size
  - hashes
- unable to detect zero-day attacks or attacks that obfuscate signitures

Behaviorial Based Detection

Advantages

- can detect changes in activity does not need files
- can take advantage of machine learning

Disadvantages

- high false positive rate
- time needed to establish baseline
- excessive monitoring

Summary

- Fileless Malware: Anatomy and Differences
- Attack Vectors: Social Engineering, PowerShell, Zero Day Vulnerabilities
- Mitigations include:
  - Improving cyber hygiene
  - Information security training for all important stakeholders
  - Updating systems (patching & securing configurations)
  - Disabling unused potential entry points

Reference Materials

References

- A Review on Fileless Malware Analysis Techniques. (2020, May). *International Journal of Engineering Research & Technology, 9*(5). doi: http://dx.doi.org/10.17577/IJERTV9IS050068
- Agency, C. a. (2018). *Petya Ransomware.* Retrieved August 2020, from https://us-cert.cisa.gov/ncas/alerts/TA17-181A
- Colen, C. (2016). [image] Chrome Malware Notification. Retrieved August 2020, from https://www.flickr.com/photos/christiaancolen/31229519675
- Fisher, M. (2018). [image] A Layered Defense. Retrieved August 2020, from Twitter: https://twitter.com/Fisher85M/status/1030976170181976064
- Green, A. (2020). What is Fileless Malware? PowerShell Exploited. Retrieved Aug 2020, from Varonis: https://www.varonis.com/blog/fileless-malware/
- Intelligence, T. (2019). Divergent: "Fileless" NodeJS Malware Burrows Deep Within the Host. Retrieved August 2020, from Talos Intelligence: https://blog.talosintelligence.com/2019/09/divergent-analysis.html
- Johansen, A. G. (2020). What is Fileless Malware and How Does it Work. Retrieved August 2020, from Norton.com: https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html
- Kaspersky. (2020). Fileless Threats Protection. Retrieved August 2020, from Kaspersky: https://www.kaspersky.com/enterprise-security/wiki-section/products/fileless-threats-protection
- Khandelwal, S. (2019). Microsoft Warns of a New Rare Fileless Malware Hijacking Windows Computers. Retrieved August 2020, from The Hacker News: https://thehackernews.com/2019/09/windows-fileless-malware-attack.html

References

- McAfee. (2017). DNSMessenger Revitalizes Fileless Malware, Uses Queries to Execute Attacks. Retrieved August 2020, from McAfee: https://www.mcafee.com/blogs/enterprise/dnsmessenger-revitalizes-fileless-malware-uses-dns-queries-execute-attacks/
- McAfee(2). (2017). New Variant of Petya Ransomware Spreading Like Wildfire. Retrieved August 2020, from McAfee: https://www.mcafee.com/blogs/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/
- McAfee. (2020). What Is Fileless Malware? Retrieved August 2020, from McAfee: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
- Mellen, A. (2019). Fileless Malware. Retrieved August 2020, from Cybereason: https://www.cybereason.com/blog/fileless-malware
- Microsoft. (2020). Documentation. Retrieved August 2020, from Microsoft: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/fileless-threats
- Microsoft Defender ATP Research Team. (2018). Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV. Retrieved August 2020, from Microsoft: https://www.microsoft.com/security/blog/2018/09/27/out-of-sight-but-not-invisible-defeating-fileless-malware-with-behavior-monitoring-amsi-and-next-gen-av/
- Microsoft Defender ATP Research Team. (2019). Bring your own LOLBin: Multi-stage, fileless Nodersok campaign delivers rare Node.js-based malware. Retrieved August 2020, from Microsoft: https://www.microsoft.com/security/blog/2019/09/26/bring-your-own-lolbin-multi-stage-fileless-nodersok-campaign-delivers-rare-node-js-based-malware/
- Microsoft. (n.d.). Licenses. Retrieved from Creative Commons: https://creativecommons.org/licenses/by-nc/3.0/

References

- MITRE. (2020). Netwalker. Retrieved August 2020, from MITRE ATT&CK: https://attack.mitre.org/software/S0457/
- MITRE (2). (2020). NotPetya. Retrieved August 2020, from MITRE ATT&CK: https://attack.mitre.org/software/S0368/
- National Cybersecurity and Communications Integration Center. (2017). Malware Initial Findings Report. Retrieved August 2020: https://us-cert.cisa.gov/sites/default/files/publications/MIFR-10130295.pdf
- Offensive Security. (2020). About the Metasploit Meterpreter. Retrieved August 2020, from Offensive Security: https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/
- Symantec. (2019). Living off the Land Turning Your Infrastructure Against You. Broadcom. https://docs.broadcom.com/docs/living-off-the-land-turning-your-infrastructure-against-you-en
- Team, S. S. (2019). Living off the Land: Attackers Leverage Legitimate Tools for Malicious Ends. Retrieved August 2020, from Symantec: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/living-land-legitimate-tools-malicious
- Trend Micro. (2020). Reflective Loading Runs Netwalker Fileless Ransomware. Retrieved August 2020, from Trend Micro: https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html
- Wueest, C. (2017). ISTR Living Off the Land and Fileless Attack Techniques. Retrieved August 2020, from Broadcom: https://docs.broadcom.com/doc/istr-living-off-the-land-and-fileless-attack-techniques-en
- Yaneza, J. (2014). Anatomy of a Control Panel Malware Attack, Part 2. Retrieved August 2020, from Trend Micro: https://blog.trendmicro.com/trendlabs-security-intelligence/anatomy-of-a-control-panel-malware-attack-part-2/

Questions

Questions

Upcoming Briefs

- 9/17 – Malsapam
- 9/24 – Netwalker Ransomware
- 10/15 - Side Channel Attacks
- 10/22 – Disinformation in the Healthcare Sector

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV