Living off the Land (LOTL)

October 17, 2024

TLP:CLEAR, ID# *202410171300*

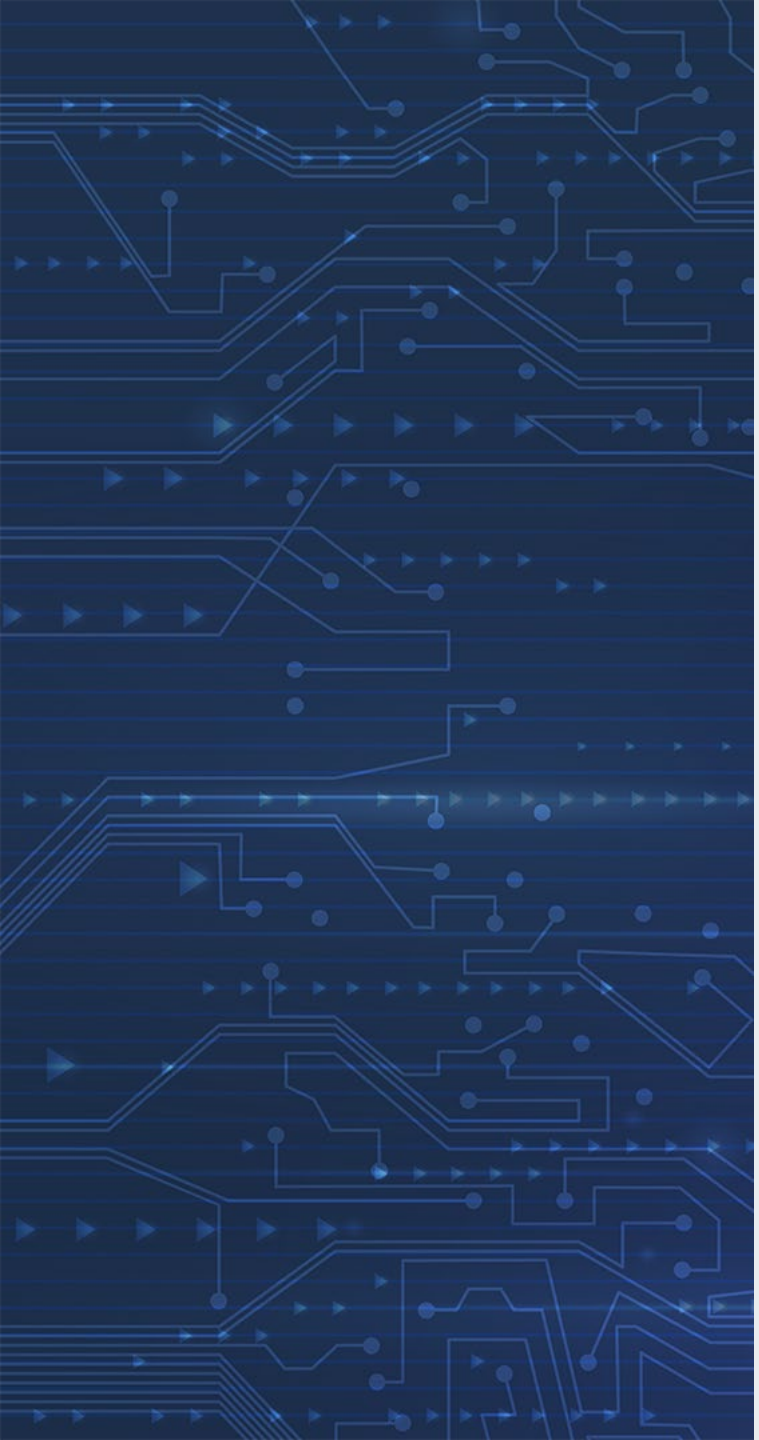
Agenda

- Living off the Land: An Introduction
- Understanding Living off the Land
- Preventing and Detecting Living off the Land Attacks

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



Living off the Land

An introduction

What is Living off the Land?

- In the physical world, “living off the land” means surviving only by the resources that can be harvested from the natural land.
- In the technology world, a Living off the Land (aka: LOLbins, LOTL) attack describes a cyberattack in which intruders use legitimate software and functions available in the system to perform malicious actions on it. Threat actors forage on the target system(s) for tools that they can use to achieve their goals.
- Attackers can bypass traditional security measures and disguise their actions as legitimate system processes by utilizing trusted tools.
- LOTL attacks are particularly effective against healthcare systems that rely on a wide range of trusted tools and technologies.

Source: CivilEats

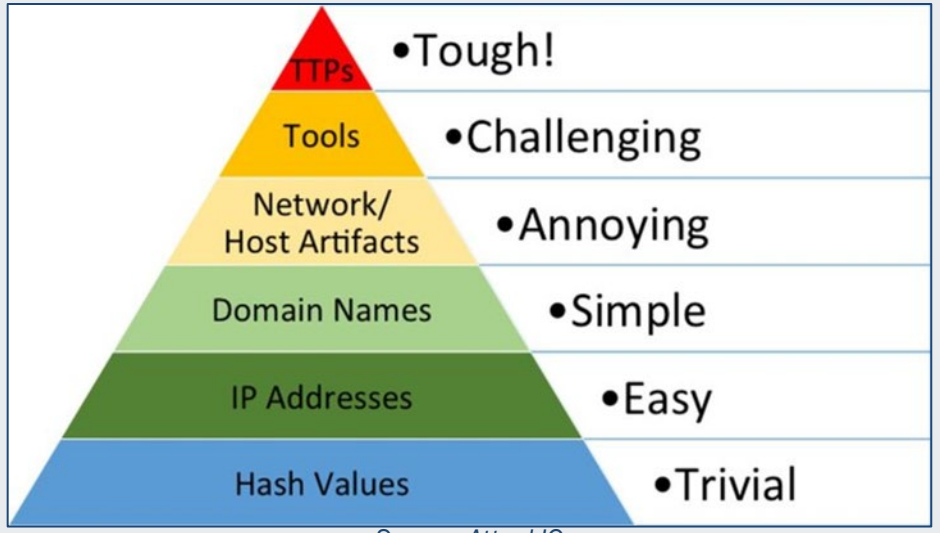
Source: Nucleon-Security

Why Do Threat Actors Utilize LOTL Attacks?

- LOTL attacks are becoming more common. They tend to be more effective than traditional malware attacks, and this is because they are far more difficult to detect with legacy security tools, and they grant the attacker more time to escalate privileges, steal data, and set backdoors for future access.
- This type of attack takes advantage of scripting languages to execute malicious code directly in memory, bypassing traditional antivirus software that primarily scans files on disk, making it extremely challenging for security teams to detect and mitigate these attacks.

Why Do Threat Actors Utilize LOTL Attacks?, cont.

- **Fly Under the Radar/Avoid Detection**
  - Attackers may choose to fly under the radar of either prevention or detection technologies. Typically, prevention technologies will use a signature-based approach to detect and quarantine malicious processes. They may also use hash values or other indicators of comprise (IOCs) to detect a process.
  - See the Pyramid of Pain, which demonstrates that some indicators of compromise are more troubling to adversaries than others. This is because when those indicators are denied to an attacker, the loss of some will be more painful to them than the loss of others. So, while attackers can change IOCs relatively easily, using pre-existing software avoids the process being flagged as suspicious.
- **Use of Tools Already Embedded in Operating Systems**
  - Operating systems typically carry tooling for automation and scripting administrative activities. These tools will typically provide easy access to both local and domain-based configuration.
- **Tooling Can be Difficult to Develop and Distribute**
  - Typically, an attacker will scope out a target, but they may not know the entire environment the tools operate in, and it may be difficult, if not impossible, to test for every possible scenario. Using existing tools allows for a variety of operating systems and environments.



Source: AttackIQ

Living off the Land & Healthcare

- Healthcare organizations often operate in complex and decentralized environments with numerous interconnected systems, making maintaining consistent security measures across the entire network challenging.
- Due to limited resources and budget constraints, many healthcare organizations rely on outdated software, as it is difficult and costly to keep up with the constant updates and patches required to secure their systems effectively. Outdated software and unpatched vulnerabilities make healthcare entities easy targets for cybercriminals.
- Increasing digitization and interconnectivity of medical devices bring new avenues for attack, further increasing the risk to healthcare systems. While this connectivity brings numerous benefits, it also introduces potential vulnerabilities that attackers can exploit to gain control over these life-sustaining devices.

Understanding Living off the Land

An in-depth analysis

How Do Living off the Land Attacks Work?

- They typically involve the exploitation of scripting languages to download and execute malicious code without triggering any antivirus or intrusion detection systems.
- Attacks are often carried out in multiple stages, with attackers gaining an initial foothold in the system through spear phishing or exploiting vulnerabilities in the network.
- Once inside, they leverage existing tools and system features to traverse the network, gain access to sensitive data, exfiltrate it without detection, and/or establish persistent access for future attacks.
- Another method attackers employ is abusing legitimate system administration tools to move laterally across the network. By leveraging the trusted functionalities of these tools, attackers can explore the network, escalate privileges, and gain access to critical systems and data. This lateral movement allows them to continue their malicious activities undetected and persistently.
- Living off the Land attacks also often involve the use of fileless malware, which resides solely in memory and leaves no trace on the compromised system's hard drive (unlike traditional malware attacks, which leverage signature files to carry out the attack plan).

Different Types of Living off the Land Attacks

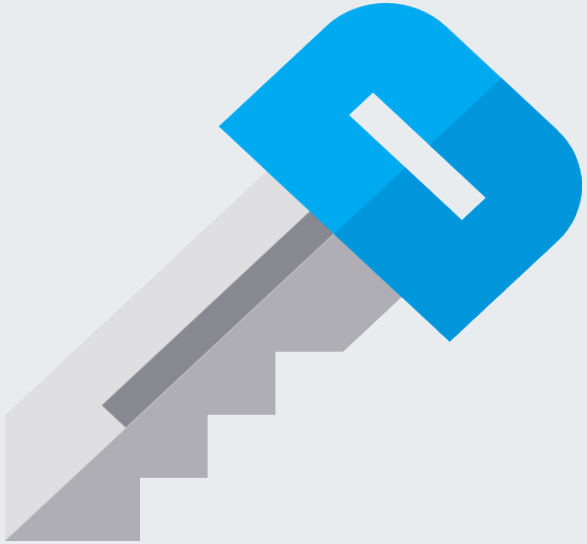
- Types of LOTL attacks to be aware of:
  - Binary Planting
  - Registry Run Keys
  - Fileless Malware
  - PowerShell-based Attacks
- Each attack poses a significant threat to organizations and individuals alike and requires proactive measures to prevent and detect.

Binary Planting

- Binary planting is a type of LOTL attack that is also known as Dynamic Link Libraries (DLL) hijacking, or DLL side-loading.
- Binary planting is a general term for an attack where the attacker places a binary file containing malicious code to a local or remote file system for a vulnerable application to load and execute. When an application tries to use the legitimate DLL, it unknowingly loads the malicious one instead, allowing the attacker to execute code on the victim's system.
- Ways this attack can occur:
  - Insecure access permissions on a local directory allows a local attacker to plant the malicious binary in a trusted location.
  - An application may be used for planting a malicious binary in another application's trusted location.
  - The application searches for a binary in untrusted locations, possibly on remote file systems.
- Particularly dangerous because it can be used to exploit applications that run with elevated privileges, such as system-level services and administrative tools.
- Detection can be difficult since it often appears like a legitimate process.

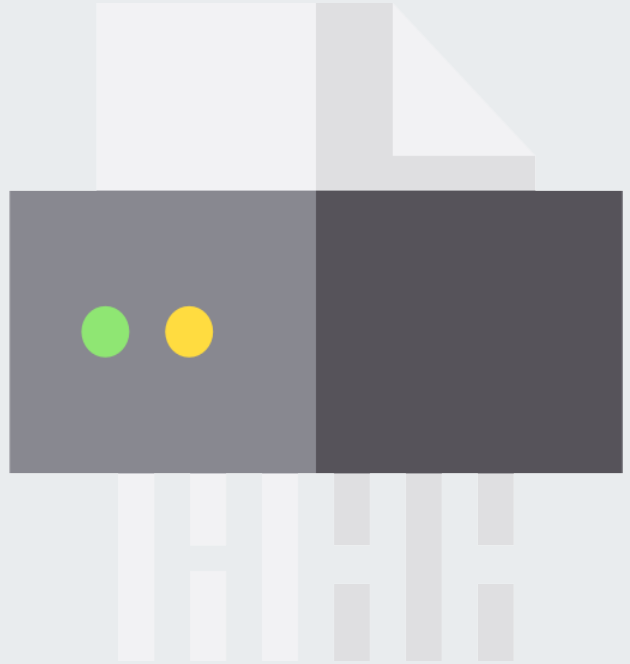
Registry Run Keys

- Registry run keys are a technique used by attackers to run their malicious code on a victim's system at startup.
- Threat actors may achieve persistence by adding a program to a startup folder or referencing it with a registry run key. Adding an entry to the run keys in the registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.
- It is a dangerous type of attack because threat actors can use these configuration locations to execute malware to maintain persistence through system reboots; can also allow the attacker to escalate privileges.
- **Masquerading**: A technique where an attacker makes the registry entries look as if they are associated with legitimate programs.



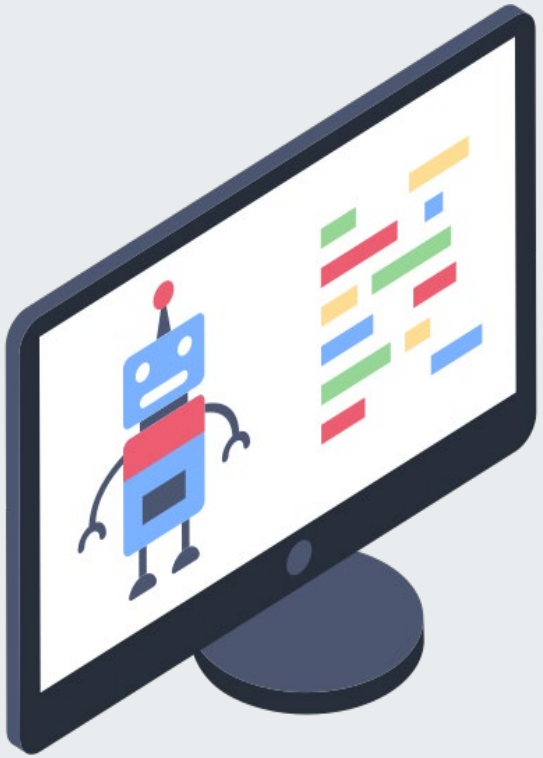
Fileless Malware

- LOTL attacks are often classified as fileless because they do not leave any artifacts behind, but fileless malware is also an advanced type of LOTL attack that bypasses traditional antivirus software by residing in the computer's memory instead of in the file system.
- The attackers use scripting languages such as PowerShell or Windows Management Instrumentation (WMI) to execute code directly in memory, and as a result, there is no file to scan, making it more difficult to detect.
- Can be used to steal sensitive data, install backdoors, or carry out various other malicious activities, and thus poses a significant threat to organizations that rely on traditional antivirus solutions.



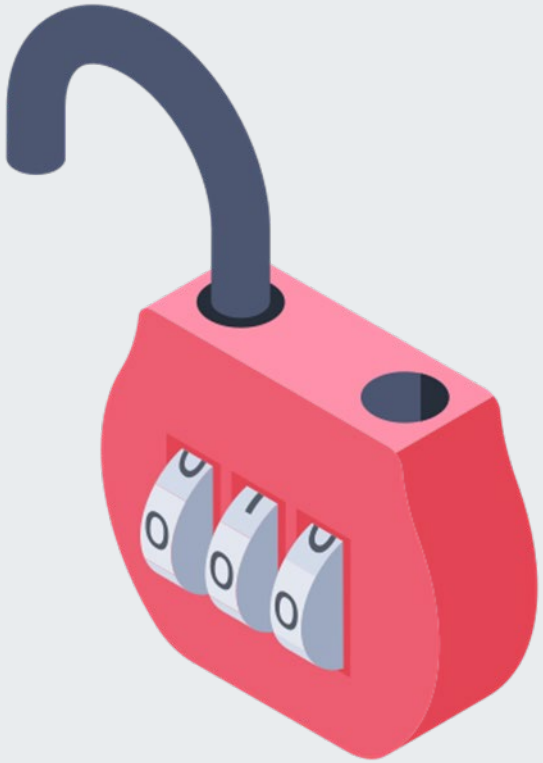
PowerShell-Based Attacks

- PowerShell-based attacks use Windows PowerShell, a powerful scripting language built into Windows, to execute malicious code.
- Attackers can use PowerShell to bypass traditional antivirus and other security measures by using PowerShell scripts to execute commands and run malware.
- This type of attack can be used to steal credentials, download additional malware, and spread throughout a network.
- Since PowerShell is a legitimate tool used by administrators, detection of this attack can be difficult, particularly if the attacker has gained privileges or access to an administrative account.



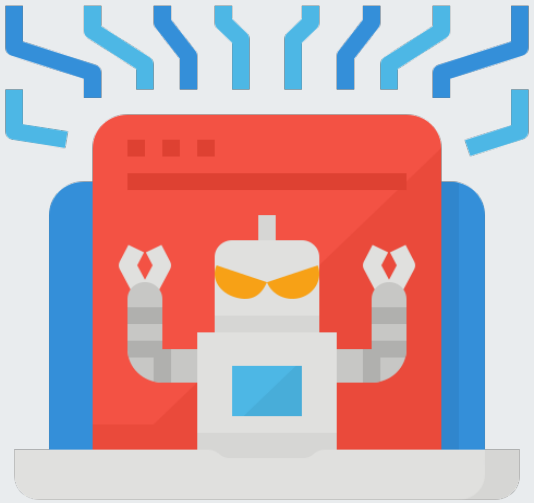
Obtaining Access

- Access can be accomplished in several ways:
  - Exploit Kits
  - Hijacked Native Tools
  - Registry Resident Malware
  - Memory-only Malware
  - Fileless Ransomware
  - Stolen Credentials



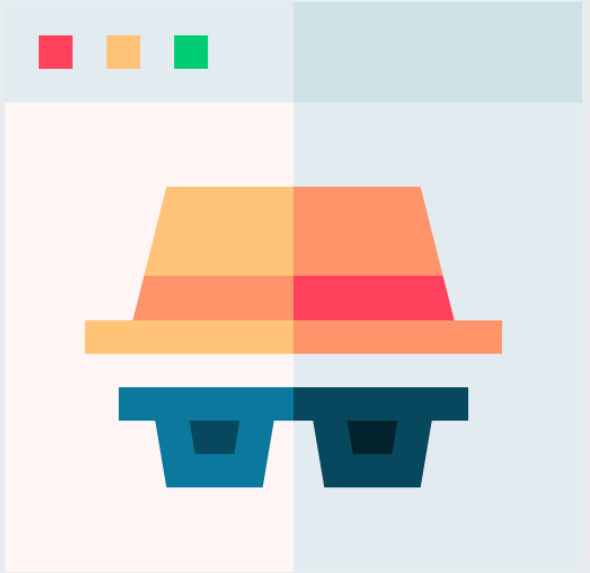
Exploit Kits

- **Exploits:** Pieces of code, sequences of commands, or collections of data
- **Exploit Kits:** Collections of exploits
- Adversaries use these tools to take advantage of vulnerabilities that are known to exist in an operating system or an installed application.
- Exploits are an efficient way to launch a fileless malware attack because they can be injected directly into memory without requiring anything to be written to disk.
- An exploit begins in the same way, regardless of whether the attack is fileless or uses traditional malware. Typically, a victim is lured through a phishing email or through social engineering. The exploit kit usually includes exploits for several vulnerabilities and a management console that the attacker can use to control the system.



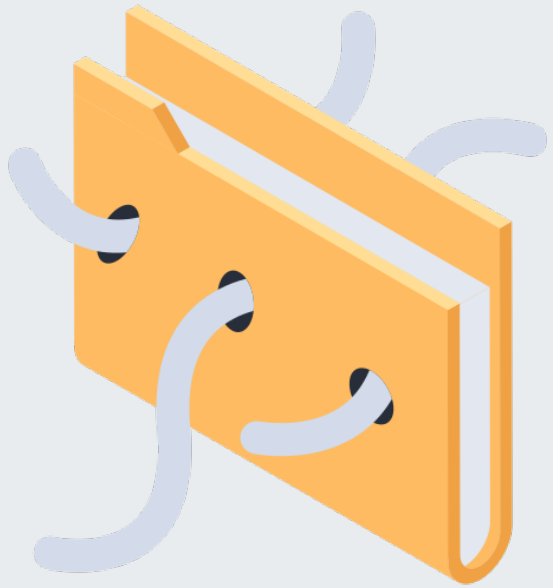
Hijacked Native or Dual-Use Tools

- In LOTL attacks, adversaries commonly hijack legitimate tools to escalate privileges, access different systems and networks, steal or encrypt data, install malware, set backdoor access points, or otherwise advance the attack path.
- Examples of native or dual-use tools:
  - File transfer protocol (FTP) clients or system functions, such as PsExec.
  - Forensic tools, such as the password extracting tool Mimikatz.
  - PowerShell, a script-launching framework that offers broad functionality for Windows device administration.
  - WMI, an interface for access to various Windows components.



Registry Resident Malware

- Registry resident malware is malware that installs itself in the Windows registry to remain persistent while evading detection.
- Windows systems are infected using a dropper program that downloads a malicious file. This malicious file remains active on the targeted system, which makes it vulnerable to detection by antivirus software. Fileless malware may also use a dropper program, but it does not download a malicious file. Instead, the dropper program itself writes malicious code straight into the Windows registry. The malicious code can be programmed to launch every time the OS is launched, and there is no malicious file to be discovered,
- The oldest variant of this type of attack is Poweliks, but there are many others, such as Kovter and GootKit.

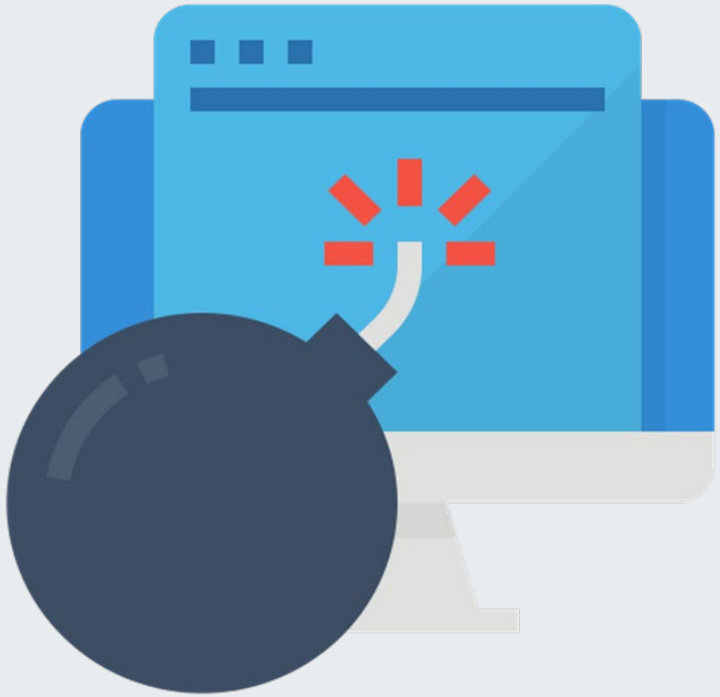


Memory-Only Malware

- Memory-only malware resides only in memory.
- Example of memory-only malware: Duqu
  - Discovered on September 1, 2011, but could have been deployed as early as December 2010.
  - A type of malware able to steal sensitive information.
  - Duqu 2.0, the most recent version of Duqu, has two versions, one of which has a backdoor that allows the adversary to gain a foothold in an organization. It also offers additional features such as reconnaissance, lateral movement, and data exfiltration.

Fileless Ransomware

- Adversaries do not limit themselves to one type of attack. They use any technology that will help them achieve their goal.
- Ransomware attackers are using fileless techniques to embed malicious code in documents using native scripting languages, such as macros, or to write the malicious code directly into memory with an exploit.
- The ransomware then hijacks native tools like PowerShell to encrypt hostage files without ever having written a line to disk.



Stolen Credentials

- Attackers may commence a LOTL attack utilizing stolen credentials so they can access their target under the guise of a legitimate user.
- Once inside, the attacker can use native tools such as WMI or PowerShell to conduct their attack.
- They can establish persistence by hiding code in the registry or the kernel, or by creating user accounts that grant them access to any system of their choosing.

Legitimate Tools Utilized by Cybercriminals in LOTL Attacks

- Tools commonly used by attackers in LOTL attacks:
  - PowerShell
  - Metasploit Framework
  - Mimikatz
  - Nmap
  - CobaltStrike
  - Wireshark
  - Aircrack-ng
  - John the Ripper
  - Hashcat
- These tools provide a wide range of capabilities, including network scanning, remote execution, password cracking, and exploitation of vulnerabilities.
- They are often used in combination to gather information, gain access to systems, and maintain persistence on the target network.

PowerShell

- PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework.
- Runs on Windows, Linux, and macOS.
- Often used in Living off the Land attacks to execute commands on the target system and automate various tasks.
- Attackers can use PowerShell to download and execute malicious code, bypass security controls, and evade detection.

Source: Microsoft

Metasploit Framework

- Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.
- Contains a suite of tools that can be used to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.
- Metasploit is used by cybersecurity professionals for penetration testing and exploitation of vulnerabilities; it is used for the same reasons in a LOTL attack.
- It provides a range of modules that can be used to identify and exploit weaknesses in systems, including remote code execution and privilege escalation.

Source: LinkedIn

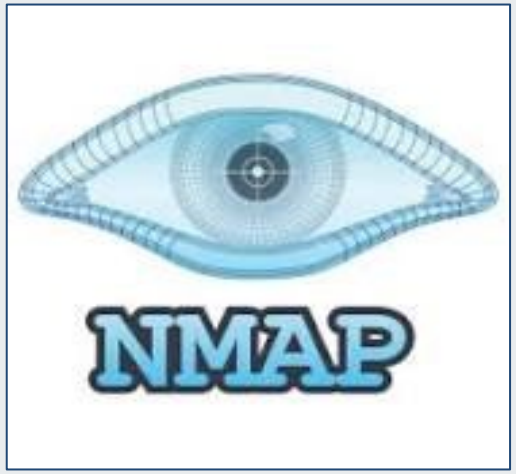
Mimikatz

- One of the most widely used and downloaded threat actor tools of the past 20 years; any cybersecurity professional tasked with protecting Windows networks needs to pay close attention to the latest Mimikatz developments to understand how hackers will manipulate the tool to infiltrate networks.
- Mimikatz is an open-source application that allows users to view and save authentication credentials, such as Kerberos tickets.
- Pentesters use Mimikatz to detect and exploit vulnerabilities in an organization's network so they can be fixed, but it is also a powerful hacking tool used in LOTL attacks for extracting plaintext passwords, hashes, and other sensitive information from the Windows operating system.
- Attackers can use Mimikatz to obtain credentials and gain access to other systems on the network, because in most cases, endpoint protection software and antivirus systems will not detect or delete the attack.

Source: Varonis

Nmap

- Nmap—short for Network Mapper—is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.
- Allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.
- When it comes to LOTL attacks, Nmap is used to map the network and to identify open ports, services, and vulnerabilities on target systems; can be used to gather information about the network topology, identify potential attack vectors, and fingerprint operating systems and applications.



Source: Nmap

Cobalt Strike

- Cobalt Strike is an adversary simulation software designed to test IT infrastructure for resilience against advanced cyberattacks; emulates realistic threats in live attacks, enabling organizations to assess their vulnerabilities and better protect themselves.
- Features of Cobalt Strike:
  - **Covert Communication:** Can be customized to use specific ports, protocols, HTTP headers, and encryption methods, allowing its traffic to blend in with regular traffic or mimic a particular application. This is due to its malleable command and control (C2), which allows the technology to move covertly undetected.
  - **Attack Packages:** Provides social engineering attacks that grant network access and can create and spread various types of malware upon infiltration.
  - **Beacon Configuration:** A remote agent known as a beacon is deployed with Cobalt Strike, and it can execute malicious code and provide a more significant foothold on a network.
  - **Post-Exploitation Modules:** A wide range of post-exploitation modules can gather information, escalate privileges, and maintain persistence within a system.
  - **Custom Scripts:** Creates custom scripts in various languages, including PowerShell, Python, C#, Bash, Java, VBA, and Ruby, which can help extend its capabilities.
- When it comes to LOTL attacks, Cobalt Strike is a tool that is often used to simulate advanced persistent threats (APTs) and conduct red team assessments.

Source: Pentest Partners

Wireshark

- Wireshark is a widely used, open-source network analyzer that can capture and display real-time details of network traffic; particularly useful for troubleshooting network issues, analyzing network protocols, and ensuring network security.
- Popular with healthcare entities, academic institutions, government agencies, corporations, and nonprofits, Wireshark is one such tool that can offer an in-depth view into network activities, diagnose network performance issues, or identify potential security threats.
- Attackers using Wireshark for Living off the Land are utilizing it for the same information; can be used to identify communication patterns, identify vulnerable services, and extract sensitive information from network packets.

Source: Wireshark

Aircrack-ng

- Aircrack-ng is a software suite for analyzing and hacking WiFi networks.
- Its functionality includes:
  - Monitoring through packet capture and export of data to text files.
  - Attacking through reauthentication or fake access points.
  - Testing by checking WiFi cards and driver capabilities.
  - Cracking various security standards, such as WEP and WPA PSK (WPA 1 and 2).
- Aircrack-ng is a suite of tools used in LOTL attacks for testing and cracking wireless network security; can be used to capture packets, perform brute-force attacks, and crack encryption keys to gain unauthorized access to wireless networks.

Source: Aircrack-ng

John the Ripper

- First released in 1996, John the Ripper is a password cracking tool originally produced for UNIX-based systems; designed to test password strength, brute-force encrypted passwords, and crack passwords via dictionary attacks.
- The tool comes in both GNU-licensed and proprietary versions. The pro version is designed for use by professional pen testers, has additional features such as multilingual wordlists, performance optimizations, and 64-bit architecture support.
- Some of the key features of the tool include offering multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the too, making it a password cracking tool of choice for beginners and professionals alike.
- John the Ripper is a password cracking tool used in LOTL attacks for testing password strength and cracking password hashes; supports a range of hash types and can be used to identify weak or vulnerable passwords.

Source: John the Ripper

Hashcat

- Hashcat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying; readily available for download on all major operating systems,
- When used for benign purposes, such as in penetration testing one's own infrastructure, it can reveal compromised or easy-to-guess credentials.
- Hackers use Hashcat to automate attacks against passwords and other shared secrets.
- Gives the user the ability to brute-force credential stores using known hashes, to conduct dictionary attacks and rainbow tables, and to reverse engineer readable information on user behavior into hashed-password combination attacks.
- It supports a wide range of hashing algorithms and can be used for brute-force attacks, dictionary attacks, and rule-based attacks to crack passwords and gain unauthorized access to systems and accounts.

Source: Hashcat

Recent Incidents in the Healthcare Sector

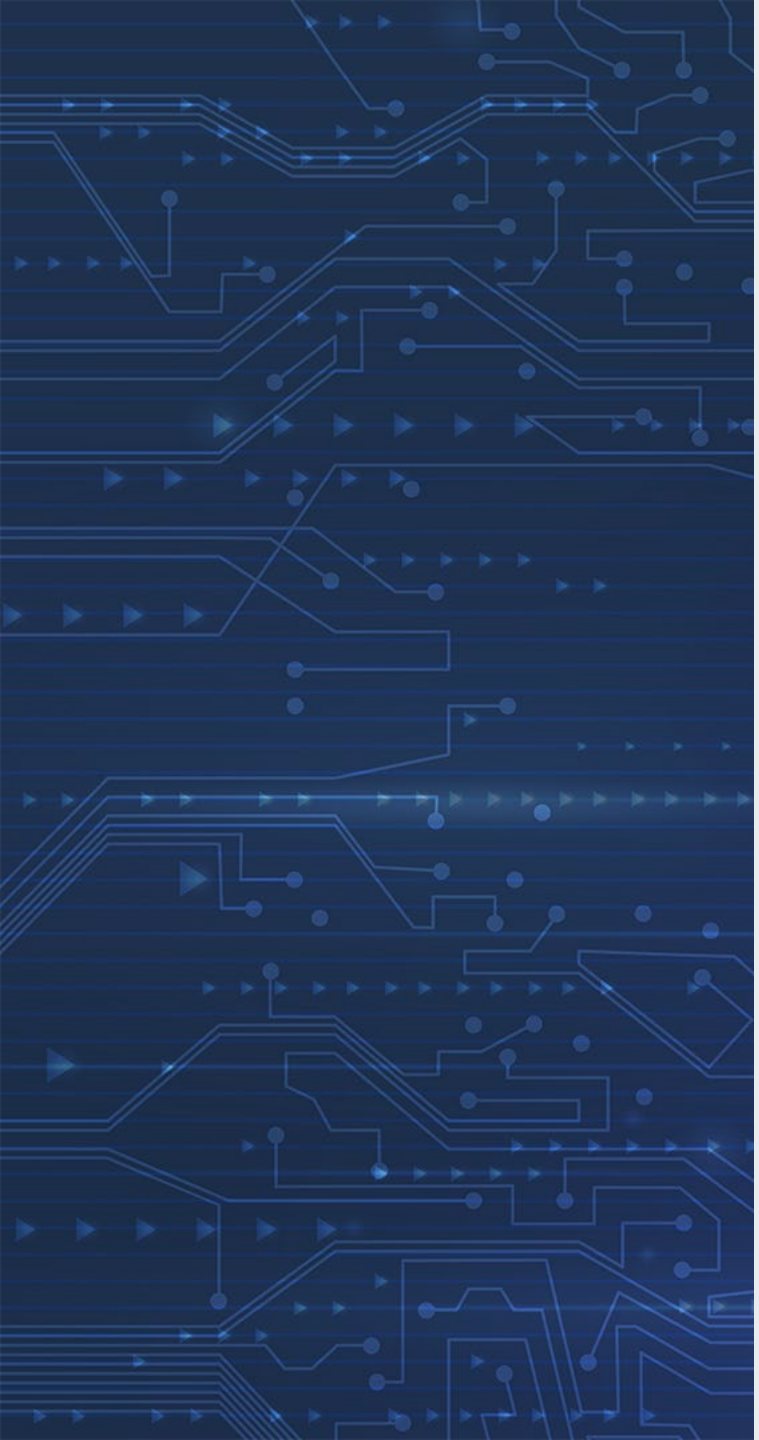
A healthcare institute is attacked

- In 2020, a ransomware group known as NetWalker utilized LOTL to target a California healthcare institute, encrypting critical files and demanding a ransom payment.
- The attack disrupted the healthcare entity's medical services, forcing them to divert patients to other hospitals and causing delays in critical treatments.

Recent Incidents in the Healthcare Sector, cont.

A 2024 report from the FBI & HHS regarding LOTL attacks observed against the U.S. HPH

- Threat actors gained initial access to employees' email accounts, and from there pivoted to target login information related to the processing of reimbursement payments to insurance companies or similar entities.
- To gain initial access to victim networks, the threat actor acquired credentials through social engineering or phishing. In some instances, the threat actor called an organization's IT Help Desk posing as an employee of the organization, and triggered a password reset for the targeted employee's account. In other instances, by manipulating the IT Help Desk employees, the threat actor was able to bypass MFA. In another instance, the threat actors registered a phishing domain that varied by one character from the target organization's true domain and targeted the organization's CFO.
- The threat actors often had PII of the impersonated employee, obtained from data breaches, enabling the threat actor to confirm the targeted employees' identity over the phone. If a social engineering attempt was successful, the threat actor then logged onto the victim account and attempted to use LOTL techniques. Threat actors were able to amend forms to make ACH changes to patients' accounts which enabled the diversion of legitimate payments to U.S. bank accounts controlled by the actors, followed by a second transfer of funds to overseas accounts.
- Report: Social Engineering Tactics Targeting Healthcare & Public Health Entities and Providers



Preventing and Detecting Living off the Land Attacks

Prevention is Mitigation

- Four actions to take to building a robust cybersecurity framework capable of handling Living off the Land attacks:
  - Training & Awareness
  - Limiting Access
  - Prioritize Visibility/Monitoring
    - User
    - Network
  - Collaboration & Reporting

Training & Awareness and Limiting Access

Training & Awareness

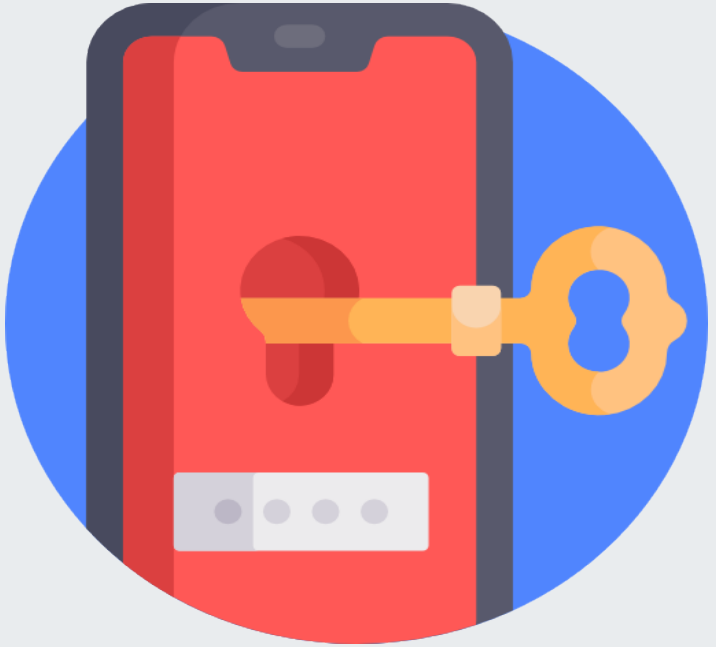
- Healthcare organizations must also focus on long-term strategies to protect their systems. A key aspect of this is fostering a cybersecurity culture from top to bottom within the organization—this means an ongoing staff training and awareness program to educate employees about the latest threats and best practices for protecting sensitive data.

Limiting Access

- **Limit the Use of Scripting Languages:** LOTL attacks rely on the use of scripting languages to execute malicious code, limiting the use of scripting languages or implementing strict controls can reduce the risk of these attacks.
- **Implement Least-privilege Access Controls:** Limiting access to sensitive data and resources can help reduce the risk of LOTL attacks and can help ensure that users only have access to the data and resources they need to perform their job functions
- **Adopt Zero-Trust Architecture:** In a zero-trust architecture, no entity is automatically trusted. Instead, every access request is thoroughly verified before granting access.

Prioritize Visibility/Monitoring

- Relying solely on preventative technologies is insufficient against threats that use legitimate tools.
- Visibility into all activities across the entire infrastructure is necessary to identify and mitigate such threats.
- Organizations must prioritize the implementation and ongoing improvement of a comprehensive threat detection, investigation, and response process; this ensures comprehensive visibility across the entire digital landscape of an organization encompassing network traffic, endpoint behavior, and user activity.
- By actively monitoring these facets, security teams can detect anomalies that deviate from normal operations, which are often indicative of LOTL attacks.



Prioritize Visibility/Monitoring: User

- **Leverage User & Entity Behavioral Analytics Tools:** These tools can analyze and create a baseline of typical user and entity activities over a period, providing a basis for deviations from normal behavior. These tools should also include account monitoring, as account monitoring and management controls can detect and prevent unauthorized activities by providing full visibility into work environments.
- **Indicators of Attack (IOAs):** One of the most effective ways to reduce the risk of LOTL attacks is by relying on indicators of attack (IOAs). IOAs include signs such as code execution, lateral movements and actions that seem to be intended to cloak the intruder's true intent. It does not matter whether the action was initiated from a file on the hard drive or from a fileless technique. What matters is the action performed, how it relates to other actions, its position in a sequence, and its dependent actions. These indicators reveal the true intentions and goals behind their behaviors and the events around them.

Prioritize Visibility/Monitoring: Network

- **Enable Comprehensive Logging:** Granular logging mechanisms are designed to meticulously track the usage of LOTL tools, including those embedded within operating systems. By enabling extended logging features, organizations can gather detailed insights into the execution patterns and command sequences of these tools, offering a clearer picture of potentially malicious activities. This level of logging provides a rich dataset from which security teams can identify unusual patterns, supporting the swift identification and mitigation of threats posed by sophisticated attackers.
- **Continual Review of Detections:** Fine tuning of detection capabilities based on environment and risk appetite is an important element of protecting against ever evolving threats and increasingly stealthy tactics.
- **Application Inventory:** Application inventory proactively identifies outdated and unpatched applications and operating systems so one can securely manage all the applications in an environment and ensure no hidden systems operate behind the scenes. Streamlining application inventory with an IT hygiene solution solves security and cost problems simultaneously. It also optimizes software configuration.
- **Update Software Regularly:** Regular software updates can patch vulnerabilities that could be exploited by LOTL attacks.
- **Implement Strong User Authentication:** Strong user authentication measures, such as multi-factor authentication, can help prevent unauthorized access to sensitive data and resources. It adds an extra layer of security by requiring users to provide multiple forms of identification before accessing critical systems and data, which can significantly reduce the risk of unauthorized access and data breaches.
- **Conduct Regular Assessments:** Regular security audits and penetration testing are also essential for identifying and addressing weaknesses in the network. This proactive approach helps ensure that security measures are up to date and effective in defending against evolving cyber threats.

Collaboration & Reporting

- Collaboration among healthcare organizations is crucial in the fight against Living off the Land attacks.
- By sharing information and experiences, healthcare organizations can collectively strengthen their defenses and stay ahead of evolving attack techniques.
- Additionally, adherence to industry standards and frameworks, such as the Health Insurance Portability and Accountability Act (HIPAA), can greatly improve system protection by providing a baseline for security practices.

Report to the FBI's IC3

Recovering from Living off the Land Attacks

- If a compromise is suspected, disconnect suspected compromised devices from the internet, isolate it from other devices, and report the event to the IT department.
- Since Living off the Land attacks take advantage of tools already on a target system, such attacks can evade detection for weeks or months, making recovering from these events extremely complex and time intensive.
- Organizations that suspect they may be the victim of such an attack should assess their network to determine if the organization has been breached, and where in the attack journey they may be. During their assessment, an organization should review current and historical events to identify signs of historical attacks, such as suspicious registry keys and suspicious output files, as well as identifying active threats.
- Many sophisticated adversaries spend months or years in their victims' networks without being detected, and a comprehensive historical analysis is critical to identifying if this has occurred.
- If an assessment reveals that an attack has occurred or is still in progress, the organization should work to contain the damage, recover and repair affected systems and harden the network for the future.

Resources

- NSA Joins Allies in Releasing Best Practices for Event Logging
  - Best practices for event logging and threat detection
- PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure
- The Current Threat Landscape of Healthcare

Reference Materials

References

- Aircrack-ng," Aircrack-ng. n.d. https://www.aircrack-ng.org/.
- "Aircrack-ng," Bugcrowd. N.d. https://www.bugcrowd.com/glossary/aircrack-ng/.
- "Binary Planting," OWASP. N.d. https://owasp.org/www-community/attacks/Binary_planting.
- "Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder," Mitre At&ck. 23 January 2020. https://attack.mitre.org/techniques/T1547/001/.
- Buckbee, Michael. "What is Mimikatz? The Beginner's Guide," Varonis. 23 March 2023. https://www.varonis.com/blog/what-is-mimikatz.
- "Cobalt Strike," BlackBerry. N.d. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/cobalt-strike#:~:text=Cobalt%20Strike%20is%20an%20adversary,vulnerabilities%20and%20better%20protect%20themselves.
- "Cobalt Strike: Walkthrough for Red Teamers," Pentest Partners. N.d. https://www.pentestpartners.com/security-blog/cobalt-strike-walkthrough-for-red-teamers/.
- "Combatting Cyber Threat Actors Perpetrating Living Off the Land Intrusions," NSA. 7 February 2024. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combatting-cyber-threat-actors-perpetrating-living-off-the-land-intrusions/
- Ellis, Steve. "Cyber Attacks - The Rise of Living off the Land Attacks," Office1. 20 September 2019. https://www.office1.com/blog/cyber-attacks-the-rise-of-living-off-the-land-attacks.

- Guisnet, Sebastien. “Living Off the Land or Fileless Attacks,” Nucleon. 27 March 2020. https://nucleon-security.com/security-insights/living-off-the-land-filleless-attacks/.
- Hanna, Katie Terrell. “Wireshark, TechTarget. January 2024. https://www.techtarget.com/whatis/definition/Wireshark.
- “Hashcat,” Hashcat. n.d. www.hashcat.net.
- “Hashcat,” Hypr. N.d. https://www.hypr.com/security-encyclopedia/hashcat.
- Hay, Mark E. “Interest in Foraging Is Booming. Here’s How to Do it Right,” Civil Eats. 9 July 2020. https://civileats.com/2020/07/09/interest-in-foraging-is-booming-heres-how-to-do-it-right/.
- Hollister, Andrew. “What Are Living Off the Land Attacks?,” Log Rhythm. 20 May 2024. https://logrhythm.com/blog/what-are-living-off-the-land-attacks/.
- Hollister, Andrew. “Living Off The Land Attacks: The Stealthy Threat Lurking In Cyberspace,” Forbes. 22 May 2024. https://www.forbes.com/sites/forbestechcouncil/2024/03/22/living-off-the-land-attacks-the-stealthy-threat-lurking-in-cyberspace/.

- “Identifying and Mitigating Living Off the Land Techniques,” CISA. 7 February 2024. https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques.
- “Introduction to Netcat,” GeeksforGeeks. 25 April 2023. https://www.geeksforgeeks.org/introduction-to-netcat/.
- IronNet. “What are “living off the land” attacks?,” Security Boulevard. 29 September 2020. https://securityboulevard.com/2020/09/what-are-living-off-the-land-attacks/.
- “John the Ripper,” John the Ripper. N.d. https://www.openwall.com/john/
- Lenaerts-Bergmans, Bart. “WHAT ARELIVING OFF THE LAND (LOTL) ATTACKS?,” CrowdStrike. 22 February 2023. https://www.crowdstrike.com/cybersecurity-101/living-off-the-land-attacks-lotl/.
- “Living off the Land (LotL) attack,” Kaspersky. N.d. https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/.
- “Living Off the Land (LOTL) Attacks,” Xcitium. N.d. https://www.xcitium.com/living-off-the-land-attacks/.
- “Living-Off-the-Land (LOTL) Attacks: Everything You Need to Know,” Kite Works. N.d. https://www.kiteworks.com/risk-compliance-glossary/living-off-the-land-attacks/.

- “Metasploit Framework,” Rapid 7. N.d. https://docs.rapid7.com/metasploit/msf-overview/.
- Miller, Christina. “Throwback attack: Duqu, one of the most skilled, mysterious and powerful APT groups,” Industrial Cybersecurity Pulse. 10 February 2022. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-duqu-one-of-the-most-skilled-mysterious-and-powerful-apt-groups/.
- Mutiso, Joel. “Metasploit Framework Explained: Understanding its Architecture and Components,” LinkedIn. 29 May 2024. https://www.linkedin.com/pulse/metasploit-framework-explained-understanding-its-joel-mutiso-yvihf.
- “Nmap,” Nmap. N.d. https://nmap.org/.
- “Powershell Documentation,” Microsoft. N.d. https://learn.microsoft.com/en-us/powershell/.
- Sharma, Ax. “John the Ripper explained: An essential password cracker for your hacker toolkit,” CSOOnline. 1 July 2020. https://www.csoonline.com/article/569533/john-the-ripper-explained-an-essential-password-cracker-for-your-hacker-toolkit.html.

- Shivanandhan, Manish. “What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time,” FreeCodeCamp. 2 October 2020. https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/.
- “Social Engineering Tactics Targeting Healthcare & Public Health Entities and Providers,” FBI. 24 June 2024. https://www.ic3.gov/Media/News/2024/240624.pdf.
- “Understanding ‘Living off the Land’ Attacks and Protecting Healthcare Systems,” Blue Goat Cyber. N.d. https://bluegoatcyber.com/blog/understanding-living-off-the-land-attacks-and-protecting-healthcare-systems/.
- “What is PowerShell?,” Microsoft. 7 March 2024. https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4.
- “What is the Pyramid of Pain?,” AttackIQ. N.d. https://www.attackiq.com/glossary/pyramid-of-pain/.
- “Wireshark,” Wireshark. N.d. https://www.wireshark.org/.

Questions

FAQ

Upcoming Brief

- November 14 – Phishing Attacks: Spoofing URLs with Cyrillic Characters

Product Evaluations

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

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

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. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

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

Threat Briefings

Presentations that provide 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.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV