FEBRUARY 2025

Welcome to our new CTI Threat Briefing! This monthly update is your go-to source for industry-specific threat intelligence tailored to Aspire's clientele. Each month, our briefing will dive into threat intelligence tailored to the specific industries within Aspire's customer base. From updates on threat actors to the latest malware trends, we'll dissect information to keep you informed.

Unless otherwise flagged all content is TLP:GREEN. If you are unfamiliar with the TLP protocol, please check this out: https://www.first.org/tlp/ . In short:

TLP:RED = Do not share with anyone
TLP:AMBER+STRICT = Limited to need to know within Aspire only.
TLP:AMBER = Limited to need to know.
TLP:GREEN = Limited to sharing within your community. This includes clients and others within the security community, but it is not for publishing publicly.
TLP:CLEAR = shout it from the rooftops!

SOC WINS

Aspire SOC Stops Active Exploitation of Apache Vulnerabilities

Aspire's Security Operations Center (SOC) successfully detected and contained an active cyberattack after threat actors exploited known critical Apache vulnerabilities on an external web server. The attackers quickly escalated to hands-on-keyboard activity, conducting system reconnaissance, user enumeration, and attempting to establish command-and-control (C2) communications.

However, Aspire's SOC analysts acted quickly, identifying the malicious activity in real time and neutralizing the threat before it could escalate further. This rapid response prevented unauthorized access and potential data exfiltration.

Why this Win Matters *- A fully exploited web server could have given attackers deep access to critical systems. They would have been able to gain control, move laterally, and eventually steal data. Aspire's quick containment of the breach shows the power of proactive monitoring and rapid incident response - making certain that threats are stopped before they become full-scale incidents.*

ASPIRE EMERGENCY FLASH NOTICES, THREAT INTELLIGENCE REPORTS, AND OTHER VULNERABILITIES TLP:CLEAR

Microsoft Outlook Vulnerability (CVE-2024-21413) Actively Exploited

A critical remote code execution (RCE) vulnerability in Microsoft Outlook (CVE-2024-21413) is being actively exploited, prompting an alert from CISA. The flaw, discovered by Check Point, allows attackers to bypass Office Protected View, opening malicious Office files in editing mode instead of read-only. Exploitation requires no user interaction - even previewing an email can trigger the attack. Threat actors use crafted file:// URLs to execute arbitrary code, steal NTLM credentials, and potentially gain full system control. Affected products include Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Outlook 2016, and Office 2019. Federal agencies have until February 27, 2025, to patch.

Why You Should Care *- This is a zero-click attack, meaning just previewing an email is enough to get compromised. Attackers can steal credentials, spread malware, or take full control of a system. Patching immediately is the only way to prevent this from being exploited. You can find guidance in Aspire's Emergency Flash Notice.*

Microsoft Patches Two Actively Exploited Zero-Day Vulnerabilities

Microsoft has patched two actively exploited zero-day vulnerabilities in Windows Ancillary Function Driver (AFD.sys) and Windows Storage, both of which allow attackers to escalate privileges and gain system control.

CVE-2025-21418 – A privilege escalation flaw in AFD.sys, which connects Windows applications to the internet. Attackers can use it to execute code with SYSTEM privileges, often paired with other exploits. It is unclear if Lazarus Group, known for similar attacks, is involved.

CVE-2025-21391 – A privilege escalation vulnerability in Windows Storage that allows attackers to delete targeted files, leading to system instability or service disruptions. This marks the first known case of this technique being used in the wild.

Why You Should Care *- These vulnerabilities give attackers full system control, allowing them to install malware or delete files. If left unpatched, any*

compromised system could be used as a launchpad for further attacks. Apply Microsoft's February 2025 updates as soon as possible. See Aspire's Emergency Flash Notice for more information.

Authentication Bypass in Palo Alto Networks PAN-OS

A serious authentication bypass vulnerability (CVE-2025-0108) in Palo Alto Networks PAN-OS is being actively exploited, allowing attackers to skip authentication and interact with PHP scripts on the firewall's management web interface. While remote code execution isn't possible, attackers can access sensitive firewall data and make unauthorized changes.

With a CVSS score of 9.1, this vulnerability is easy to exploit - it requires no special privileges, no user interaction, and only network access. Security researchers have observed attackers chaining it with CVE-2024-9474 to gain deeper access to unpatched PAN-OS web management interfaces. If your firewall's management interface is exposed to the internet or an untrusted network, you are at high risk and should patch immediately.

Why You Should Care *– If an attacker reaches your firewall, they control the gate to your network. They can steal sensitive data and alter security settings. If your firewall's management interface is publicly accessible, please see Aspire's Emergency Flash Notice for guidance.*

Salt Typhoon Exploits Cisco Vulnerabilities

Salt Typhoon, a nation-state threat actor, has been targeting U.S. telecommunications providers for at least three years, using stolen credentials and Cisco vulnerabilities to maintain persistent access to core infrastructure. The group has been moving undetected, collecting sensitive data, and exploiting unpatched Cisco devices to escalate privileges and execute commands. Researchers have observed multiple threat actors leveraging these flaws and all organizations with outdated Cisco systems are at risk.

Exploited Vulnerabilities

- CVE-2018-0171 (CVSS 9.8) – Remote code execution in Cisco IOS and IOS XE
- CVE-2023-20198 (CVSS 10) – Web UI privilege escalation in Cisco IOS XE
- CVE-2023-20273 (CVSS 10) – Another privilege escalation flaw in Cisco IOS XE
- CVE-2024-20399 (CVSS 6.0) – Command injection in Cisco NX-OS CLI

Why You Should Care *- Salt Typhoon isn't looking for quick wins; they're embedding themselves inside telecom networks for the long haul. If your Cisco devices aren't patched, they're an open door. Update and lock down access now. See Aspire's Emergency Flash Notice for more information.*

CISA Warns of RCE Vulnerability in CraftCMS

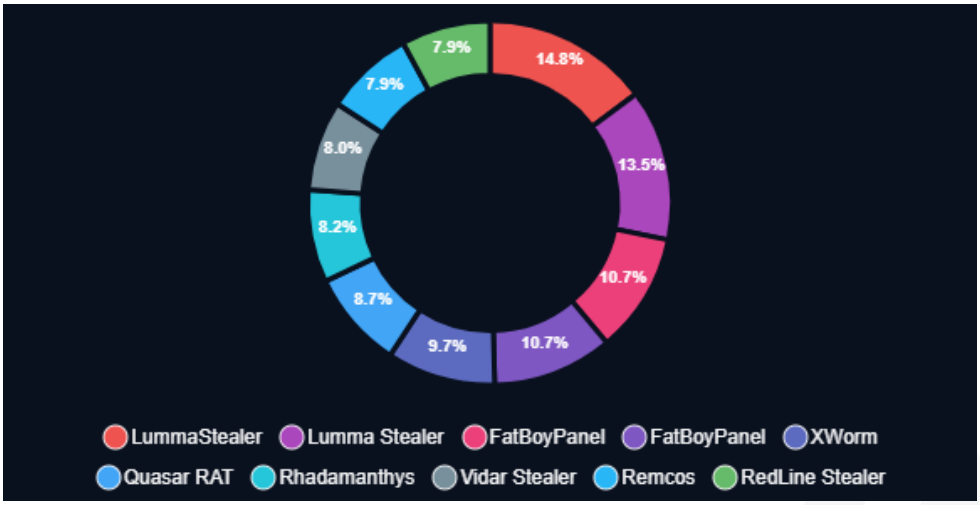
A remote code execution (RCE) vulnerability (CVE-2025-23209) has been discovered in Craft CMS versions 4 and 5, prompting CISA to add it to its Known Exploited Vulnerabilities (KEV) catalog. Exploiting this flaw isn't simple - attackers need the installation security key, which secures authentication tokens, session cookies, and database values. If obtained, they can decrypt sensitive data, forge authentication tokens, and execute malicious code remotely.

CISA has confirmed real-world exploitation, but details on who is behind the attacks remain unknown. The patch deadline is March 13, 2025, and admins should update to versions 5.5.8 or 4.13.8. Additionally, compromised installations should delete old security keys and generate new ones using the PHP craft setup/security-key command while ensuring previously encrypted data remains accessible.

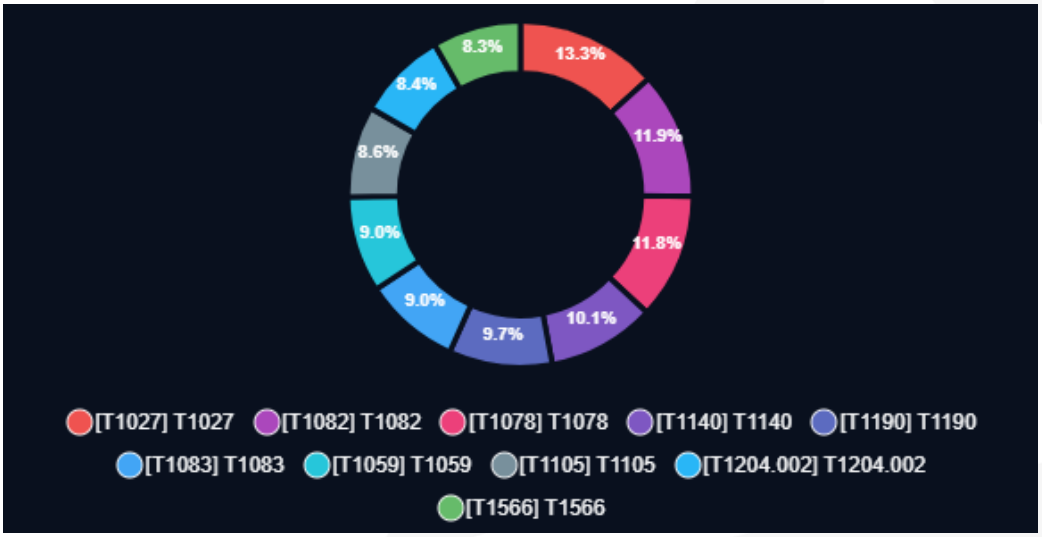
Why You Should Care*: A vulnerable CMS is an easy entry point for attackers. If compromised, threat actors can redirect users to phishing sites, inject malicious ads, or even drop malware on visitors' devices. See the* CraftCMS advisory for patch guidance.

INTELLIGENCE FOR FEBRUARY 2025

Top Threat Actors

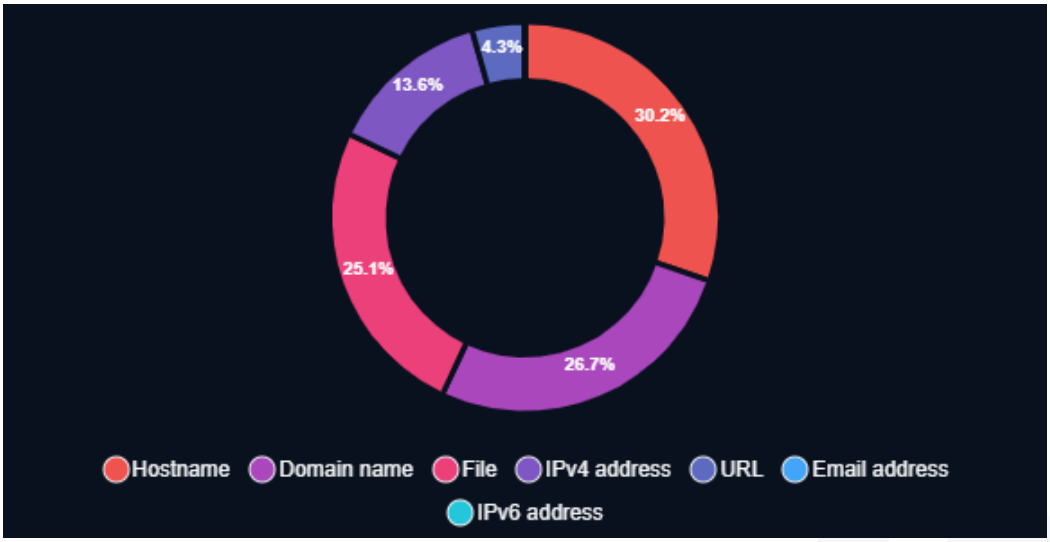


Top ATT&CK Techniques



Aspire Technology Partners
(732) 847-9600
www.aspiretransforms.com

Top Indicators by Type



Industry Specific Threat Actors & Malware

Over the past month, most attacks and malware activity we have observed in our collection focused on the government, technology, defense, and finance sectors. Here is the latest research for those sectors.

Top Threat Actors for February 2025

Top Threat Actors February 2025

- **Government** – Earth Koshchei, Howling Scorpius, Chinese-Speaking Group, Prometei, APT-C-48 (CNC), Paper Werewolf, Payroll Pirates, Lotus Blossom, Silent Lynx

- **Technology** – Earth Koshchei, Howling Scorpius, Chinese-Speaking Group, UNC5820, Prometei, FUNNULL
- **Finance** – UNC5820, Prometei, Paper Werewolf, Payroll Pirates, FUNNULL, Silent Lynx
- **Defense** – Earth Koshchei, Phorpiex, UNC5820, APT-C-48 (CNC)

Earth Koshchei

- Earth Koshchei, a suspected SVR-backed APT group, recently launched a large-scale rogue RDP campaign targeting government agencies, think tanks, researchers, and military organizations. Using spear-phishing emails, the attackers tricked victims into opening malicious RDP configuration files, which redirected their connections through a network of over 190 RDP relays. This setup allowed attackers to gain access to victim machines, potentially leading to data theft and malware installation.

  The campaign, which peaked on October 22, involved extensive infrastructure, including over 200 registered domains and multiple anonymization layers such as TOR, VPNs, and residential proxies to obfuscate activity and hinder attribution. Earth Koshchei has a history of adapting its tactics, often repurposing red team tools for espionage. Their use of rogue RDP techniques appears to be inspired by a previously published red team methodology, highlighting how APT groups leverage security research to refine their attacks. Organizations are advised to restrict outbound RDP connections and monitor for suspicious activity to mitigate the risk.

UNC5820

- Threat actor UNC5820 exploited a zero-day vulnerability (CVE-2024-47575) in FortiManager, affecting over 50 systems across multiple industries. Discovered by Fortinet and Mandiant, the attack began in June 2024 and continued through September, enabling unauthorized access and data theft. UNC5820 leveraged the flaw to extract configuration data, including details about managed Fortinet devices, usernames, and hashed passwords. Attackers connected to a remote server on port 541 and staged stolen data in a hidden archive before exfiltrating it via outbound traffic. In at least one instance, they registered their own device with the compromised FortiManager, suggesting an attempt to maintain long-term access. Security experts stress the urgency of applying Fortinet's October 24

patch, reviewing logs for suspicious activity, and implementing network segmentation.

Howling Scorpius (Akira)

- Akira ransomware saw a major surge in January and February, becoming the most active ransomware group and accounting for 13% of all recorded attacks, according to NCC Group. The group, linked to Storm-1567, has refined its tactics, achieving lightning-fast data exfiltration within just over two hours before deploying ransomware the following day. In a recent attack on a Latin American airline, Akira actors exploited an unpatched Veeam backup server using SSH, immediately extracting sensitive data before launching the ransomware. Their approach relies on legitimate tools like WinSCP for stealthy exfiltration, while also disabling antivirus protections and leveraging remote desktop software to spread across networks.

Top Malware for February 2025

Top Malware February 2025

- **Government** – Zegost, PowerTaskel
- **Technology** – Megazord, AndeLoader
- **Energy** – Zegost, SmokeLoader, DestroyRAT, Kaba, FatalRAT, RustBucket, PowerTaskel, Spark - S0543, Lynx, cd00r
- **Finance** – SmokeLoader, RustBucket, PowerTaskel, GoldKefu, GoldDigger

RustBucket

- The BlueNoroff APT group, a suspected sub-group of Lazarus, has been linked to a new macOS malware strain called RustBucket, which was discovered by Jamf Threat Labs. RustBucket operates in multiple stages, with an initial dropper disguised as an Internal PDF Viewer app that downloads additional payloads. The malware requires a specific malicious PDF to activate, at which point it decrypts hidden content, establishes contact with a command-and-control (C2) server, and downloads further malware components.

  The final stage, written in Rust, executes system reconnaissance and potentially more destructive actions. This campaign demonstrates BlueNoroff's ongoing

expansion into macOS environments, leveraging social engineering tactics and fake venture capital firm lures to target victims. Given the increasing sophistication of macOS malware, organizations are advised to enforce strict application security, block suspicious domains, and monitor for abnormal network activity to prevent unauthorized system access.

Cd00r

- The cd00r backdoor, originally an open-source proof-of-concept, has been repurposed by threat actors in a stealthy campaign targeting Juniper VPN gateways with a modified variant called J-Magic. This malware remained dormant until it detected a "magic packet", at which point it initiated a secondary challenge before establishing a reverse shell, giving attackers remote control over the device. Researchers from Lumen Technologies' Black Lotus Team linked J-Magic to previous malware like SeaSpy2, another cd00r-based backdoor that targeted Barracuda security appliances. While attribution remains unclear, similarities with prior attacks suggest a possible link to Chinese threat actors. Cd00r's passive, port-knocking technique makes it particularly stealthy, as it does not require persistent connections or listening services, allowing it to evade traditional security monitoring. Organizations relying on Juniper VPN gateways and other enterprise-grade networking equipment should monitor for unusual inbound traffic, restrict access to management interfaces, and apply firmware updates to mitigate the risk of similar backdoor deployments.

FatalRat

- A phishing campaign targeting industrial organizations across the Asia-Pacific (APAC) region has been delivering FatalRAT, using Chinese cloud services like myqcloud and Youdao Cloud Notes for attack infrastructure. The campaign relies on DLL side-loading to execute the malware stealthily while displaying decoy files to avoid suspicion. FatalRAT is highly capable, allowing attackers to log keystrokes, manipulate system functions, steal data, and install remote administration tools. The malware also performs extensive checks to evade virtual machines and sandbox environments. While attribution remains uncertain, researchers believe a Chinese-speaking threat actor may be responsible. Given FatalRAT's ability to spread across networks and manipulate devices, organizations should strengthen email security, restrict execution of unknown DLLs, and monitor network activity for suspicious connections to cloud services.

Lynx

- The Lynx ransomware operation has gained traction in early 2025, positioning itself as a highly organized Ransomware-as-a-Service (RaaS) platform with a

structured affiliate program. Built on the foundation of the INC ransomware, Lynx provides affiliates with an easy-to-use panel where they can customize attacks, generate ransomware samples, and manage data leaks. The group offers an 80% cut of ransom proceeds, making it an attractive option even for those with limited technical skills.

Lynx has targeted various industries, with recent breaches including Brown and Hurley, an Australian truck dealership, and Hunter Taubman Fischer & Li LLC, a U.S.-based law firm. The malware encrypts all files by default, steals sensitive data before encryption, and deletes recovery options to make restoration nearly impossible. It also utilizes credential dumping techniques, obfuscation, and Tor-based command-and-control (C2) infrastructure to evade detection.

Victims find their files renamed with a ".LYNX" extension, and a ransom note demanding payment via Tor. Given its cross-platform capabilities and aggressive expansion, organizations should implement strong access controls, regular backups, and advanced endpoint detection to defend against Lynx attacks.

SECURITY INCIDENTS

Qilin Ransomware Claims Lee Enterprises Attack

The Qilin ransomware group has claimed responsibility for the cyberattack on Lee Enterprises, which disrupted at least 75 newspapers across the U.S. in early February. The attackers encrypted files and stole 350 GB of data, including financial records, journalist payments, and internal documents. Qilin is now threatening to leak the stolen files on March 5 unless a ransom is paid, already sharing samples as proof.

Qilin, a Russia-linked Ransomware-as-a-Service (RaaS) group), has targeted nearly 300 organizations, including London hospitals. Many victims likely remain undisclosed as they opt to pay ransoms. The attack on Lee Enterprises reflects a growing trend of ransomware gangs targeting media companies, aiming to disrupt operations and extort payments through public data leaks.

***Why You Should Care**: Ransomware attacks on media organizations threaten not just operations but also confidential sources and public trust. The theft of sensitive data increases the risk of fraud, which could damage an organization's reputation.*

EncryptHub Compromises Over 600 Organizations in Global Attacks

The EncryptHub threat actor (Larva-208) has breached at least 618 organizations since June, using spear-phishing, SMS scams, and fake login pages to steal credentials. Victims were tricked into installing remote access tools like AnyDesk and TeamViewer, allowing attackers to move through networks undetected. From there, PowerShell scripts deployed infostealers that targeted cryptocurrency wallets, VPN configurations, password managers, and sensitive files. The group also used a custom PowerShell-based encryptor, suggesting a shift toward data extortion. Researchers believe EncryptHub sources its domains and phishing kits from a related group, Larva-148.

***Why You Should Care**: EncryptHub isn't relying on advanced exploits. They're tricking people into handing over access. Once they get in, they move fast, stealing credentials and locking up data. If security training and phishing defenses aren't in place, it's only a matter of time before they find their next target.*

Massive Botnet Exploits Basic Auth in Microsoft 365 Attacks

A botnet of over 130,000 compromised devices is password-spraying Microsoft 365 accounts, targeting Basic Authentication to bypass Multi-Factor Authentication (MFA) protections. Attackers are using credentials stolen by infostealer malware to automate login attempts at scale. Since Basic Auth does not trigger MFA, compromised accounts can be accessed undetected, often bypassing Conditional Access Policies. The botnet operates through command-and-control servers linked to China, using Hong Kong-based and U.S. hosting providers to proxy traffic and manage operations. Microsoft plans to deprecate Basic Auth by September 2025, but until then, it remains a prime target for attackers.

***Why You Should Care**: Attackers are exploiting outdated authentication settings that many companies haven't disabled. Once they break in, they can access email, steal data, and spread deeper into the network. Organizations should disable Basic Auth and monitor login attempts to thwart attacks.*

SECURITY REPORTS

Microsoft Disrupts Cybercrime Network Abusing Generative AI

Microsoft has identified and taken legal action against Storm-2139, a cybercrime group accused of modifying generative AI services for illegal purposes. The group's key

members, from Iran, the UK, Hong Kong, and Vietnam, allegedly scraped exposed credentials to bypass AI safeguards and resold access to malicious actors. These individuals enabled the generation of harmful synthetic content, including non-consensual images of public figures. Microsoft's Digital Crimes Unit (DCU) previously filed lawsuits against unknown participants but has now named four defendants and is working with law enforcement agencies worldwide. The crackdown has led to internal conflicts among cybercriminals, with members exposing each other online. In addition to legal action, Microsoft seized critical infrastructure, disrupting the group's operations and setting a precedent in the fight against AI abuse.

Why You Should Care *– Criminals exploiting AI-powered tools can manipulate public perception and spread misinformation. Without strict oversight, malicious actors can repurpose AI for fraud. Organizations must enforce strong security measures, and this means monitoring AI usage.*

Health Net and Centene Pay Over $11 Million for False Cybersecurity Certifications

Health Net Federal Services (HNFS) and its parent company, Centene Corporation, have agreed to pay $11.25 million to settle allegations that they falsely certified compliance with cybersecurity requirements in a Department of Defense (DoD) contract for the TRICARE health benefits program. The Justice Department accused HNFS of failing to properly scan for vulnerabilities, apply security patches, and address known cybersecurity risks between 2015 and 2018, despite reporting compliance in annual filings.

Federal investigators found that HNFS ignored internal and third-party audit findings, leaving sensitive information exposed to potential cyber threats. The Defense Criminal Investigative Service (DCIS) emphasized the importance of protecting TRICARE beneficiaries, stating that contractors who fail to meet cybersecurity standards will be held accountable.

Why You Should Care *– If federal contractors cut corners on cybersecurity, the consequences go beyond contract breaches - they put sensitive government data at risk. Organizations handling protected information must take security obligations seriously or risk major financial and legal repercussions.*

NOTABLE TTPS TLP:AMBER

Defense Evasion

- **System Information Discovery (T1082)** - Adversaries may gather detailed system and hardware information, including OS version, patches, and architecture, to tailor their attacks. Tools like Systeminfo on Windows, systemsetup on macOS, and df -aH for disk details help extract this data. On network devices, attackers may use CLI commands like show version for system insights. In cloud environments, APIs from AWS, GCP, and Azure can reveal virtual machine details, aiding reconnaissance and payload development.
    - **Mitigations**
        - According to MITRE, this type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
    - **Detections**
        - **Command Execution** - Track executed commands and arguments that seek detailed system and hardware information, such as OS version, patches, and architecture. For network devices, review AAA logs for commands run by unauthorized or unexpected users.
        - **OS API Execution** - Monitor API calls that attempt to retrieve system and hardware details, such as OS version, patches, and architecture. Remote access tools may use Windows APIs to gather this data, while system management utilities like WMI and PowerShell can also be leveraged. In cloud environments, native logging can help detect access to APIs and dashboards containing system information, though normal administrative activity may generate similar logs.
        - **Process Creation** - Track newly launched processes that attempt to gather system and hardware details, including OS version, patches, hotfixes, service packs, and architecture.

Discovery

- **Obfuscated Files or Information (T1027)** - Adversaries use encryption, encoding, and obfuscation to hide payloads and executable files, making them harder to detect. These methods, including compressing or splitting files, are employed to bypass defenses and may require user actions like entering passwords to execute. Malicious files can be reassembled or revealed only when triggered. Command obfuscation also disguises malicious commands, using environment variables or platform-specific features to evade detection.
    - **Mitigations**

- **Antivirus/Antimalware** - Use antivirus software to automatically detect and quarantine suspicious files. On Windows 10+, consider enabling the Antimalware Scan Interface (AMSI) to analyze commands after they are processed or interpreted.
- **Audit** - Regularly review common fileless storage locations, such as the Registry or WMI repository, to detect potentially abnormal or malicious data.
- **Behavior Prevention on Endpoint** - Enable Attack Surface Reduction (ASR) rules on Windows 10+ to prevent the execution of potentially obfuscated payloads.
- **User Training** - Limit access to software deployment systems to authorized personnel and ensure only a controlled number of ingress points for deploying new software.

Detections

- **Application Log Content** - Monitor application logs for alerts triggered by antivirus or other security tools when a malicious tool is detected. Treat initial detections as a potential indication of a larger intrusion and investigate further for unrecognized activity.
- **Command Execution** - Track executed commands and arguments for signs of obfuscation, such as unusual escape characters or variations in argument syntax related to encoding.
- **File Creation** - Detecting file obfuscation can be challenging unless specific artifacts are left behind that can be identified through signatures. If obfuscation detection isn't possible, focus on identifying the malicious activity that created or modified the obfuscated file.
- **File Metadata** - Monitor file metadata, such as name, content (e.g., signatures or headers), user/owner, and permissions, to identify potential obfuscation based on specific file attributes.
- **Module Load** - Monitor module loads, especially those not included in import tables, as they may indicate obfuscated code. Dynamic malware analysis can also reveal signs of obfuscation.
- **OS API Execution** - Analyze calls to functions like GetProcAddress(), which may be associated with malicious code obfuscation.
- **Process Creation** - Track new processes that attempt to obfuscate or encrypt files to make them harder to discover or analyze, both on the system and in transit.
- **Script Execution** - Monitor executed scripts for signs of obfuscation, such as unusual command syntax or encoded/unreadable character blobs.

- **Windows Registry Key Creation** - Watch for the creation of Registry keys that may store malicious data, like commands or payloads.

CONTRIBUTOR(S)

Portia Cole

About Aspire

Aspire is a professional technology services firm specializing in the delivery of digital infrastructure solutions and managed services designed specifically to achieve our clients' business goals. We believe technology sits at the heart of every enterprise strategy. Our team takes time to understand your business initiatives and align technology solutions to drive the organization forward. Aspire's outcome-driven approach accelerates your journey by combining secure digital infrastructure, world-class design and implementation expertise, and managed services – all centered around transforming today's multi-cloud architectures into enablers of business value. Headquartered in Eatontown, New Jersey, Aspire is focused on serving the tri-state, mid-Atlantic, and New England regions with local operations in Mount Laurel, NJ; Conshohocken, PA; Albany and White Plains, NY; and Cambridge, MA.