November 2024

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!

Aspire Emergency Flash Notices, Threat Intelligence Reports, and other Vulnerabilities TLP:CLEAR

Cyber Threats Don't Take Holidays Off – Best Practices and an Aspire Case Study

It's the holiday season—a time for gathering with loved ones and shopping—but also a period of heightened vulnerability as threat actors exploit the busy time of year. Last year, Aspire mitigated a ransomware attack during Thanksgiving by responding to a customer incident. Attackers exploited a vulnerable Cisco ASA VPN, gained access using a compromised domain admin account, and moved laterally across the network, targeting critical systems. Aspire's swift response and proactive measures successfully disrupted the attack. For more details, see the Threat Intelligence Report in the customer portal.

Why You Should Care *- Cyberattacks increase during holidays due to reduced staffing and heightened risks. Proactively partnering with cybersecurity experts like Aspire Technology Partners can minimize the impact of such incidents, ensuring your organization is prepared for potential threats.*

Maximum Severity Command Injection Vulnerability Found in Cisco UWRB Access Points

In November, Cisco disclosed a critical command injection vulnerability (CVE-2024-20418, CVSS 10) in the web-based management interface of its Unified Industrial Wireless Software, which impacted Ultra-Reliable Wireless Backhaul (URWB) Access Points. The flaw allowed unauthenticated attackers to execute arbitrary commands with root privileges. Affected devices included Cisco Catalyst IW9165D, IW9165E, and IW9167E Access Points running vulnerable software versions or with URWB mode enabled, while other products like the Aironet and Catalyst 9100 Series were unaffected. If exploited, the vulnerability granted attackers root access, allowing them to steal data or monitor industrial networks, leading to significant downtime. Cisco urged users to review compatibility and memory requirements before applying the patch.

Why You Should Care *- If left unpatched, this vulnerability could give attackers full control over critical network devices, leading to operational disruption, data theft, and security breaches. Cisco has urged customers to patch devices as soon as possible to prevent exploitation. Cisco also urged users to review compatibility and memory requirements before applying the patch. See Aspire's Emergency Flash Notice for further details.*

Palo Alto Vulnerability Actively Exploited

CISA issued an alert for a critical vulnerability (CVE-2024-5910, CVSS 9.3) in Palo Alto Networks' Expedition migration tool, which was patched in July 2024 but was being exploited in November. The flaw, caused by missing authentication, allows attackers to reset admin passwords and access sensitive data. It affects versions below 1.2.92 and can be exploited via a simple request to an exposed endpoint. Other vulnerabilities in the tool include CVE-2024-9464 (authenticated command injection) and CVE-2024-9465 (unauthenticated SQL injection). CVE-2024-5910 can also be chained with CVE-2024-9464 for arbitrary command execution.

Why You Should Care *– CVE-2024-5910 allows attackers to reset admin passwords and access sensitive data, which is a significant risk. With active exploitation and a public proof-of-concept available, it's important to patch affected systems immediately. See Aspire's Emergency Flash Notice for further details.*

New Fileless Remcos RAT Malware via Excel Exploit

A November phishing campaign has been using Microsoft Excel files to deploy a fileless version of the Remcos RAT (Remote Access Trojan), exploiting CVE-2017-0199 (CVSS 7.8) in Microsoft Office and WordPad. This vulnerability allows attackers to execute arbitrary code via crafted Office documents, helping them gain unauthorized access, steal sensitive information, and maintain remote control. The malware evades detection using techniques like process hollowing and anti-debugging. Victims are lured through phishing emails containing a purchase order theme, triggering the exploit when an Excel attachment is opened. CVE-2017-0199 affects all Windows versions with vulnerable Office software.

Why You Should Care *– CVE-2017-0199 allows attackers to remotely control systems and steal sensitive data through a simple phishing email. As the exploit evades detection, it's important to patch vulnerable Office versions immediately. See Aspire's Emergency Flash Notice for further details.*

Windows Zero Day Vulnerability Exploited in the Wild

A critical NTLM Hash Disclosure spoofing vulnerability (CVE-2024-43451) was discovered in all supported Windows versions, exploited as a zero-day since at least April 2024. This flaw allows attackers to steal NTLMv2 hashes with minimal user interaction, enabling pass-the-hash attacks or plaintext password extraction. The vulnerability has been actively exploited in targeted campaigns, particularly against Ukrainian entities, delivering malware like SparkRAT and Redline Infostealer. It is triggered when a user interacts with a malicious URL file, leaking the victim's NTLMv2 hash to the attacker's remote server. Affected systems include Windows 7-11 and Windows Server 2008 and later.

Why You Should Care – *CVE-2024-43451 allows attackers to steal NTLMv2 hashes, allowing for unauthorized authentication and password extraction. With active exploitation in the wild, users should patch vulnerable systems immediately. See Aspire's Emergency Flash Notice for further details*.

VMware vCenter Server Updates Address Critical Vulnerabilities

VMware released updates addressing two critical vulnerabilities in VMware vCenter Server and VMware Cloud Foundation. CVE-2024-38812 (CVSS 9.8) is a heap-overflow vulnerability in the DCERPC protocol that could lead to remote code execution and full system compromise. CVE-2024-38813 (CVSS 7.5) is a privilege escalation flaw that could allow attackers to gain root-level access through network packet manipulation. Both vulnerabilities have been actively exploited in the wild, potentially resulting in unauthorized access, data breaches, and further system compromise.

Why You Should Care – *CVE-2024-38812 and CVE-2024-38813 allow attackers to remotely execute code and gain root access, compromising VMware vCenter Server systems. Given the active exploitation, it is critical to apply the patches immediately. See Aspire's Emergency Flash Notice for further details.*

Fortinet VPN Zero-Day Exploited in Active Malware Attacks

A zero-day vulnerability in Fortinet's FortiClient VPN client for Windows is being actively exploited by APT41 (BrazenBamboo) through its DEEPDATA malware framework. This flaw allows attackers to extract VPN credentials, including usernames, passwords, and server information, directly from system memory. The DEEPDATA framework is used for surveillance, credential theft, and data exfiltration, with plugins capable of extracting sensitive information from browsers, communication apps, and password managers. Affected systems include FortiClient VPN Client for Windows (latest analyzed version: v7.4.0), with no available patch since its discovery in July 2024.

Why You Should Care – *This vulnerability allows attackers to steal VPN credentials, allowing for unauthorized access and lateral movement within corporate networks. Until Fortinet issues a* *patch, organizations should apply recommended mitigations. See Aspire's Emergency Flash Notice for further details.*

Zero-Day Exploits in Palo Alto Networks Firewalls

Palo Alto Networks disclosed two zero-day vulnerabilities (CVE-2024-0012 and CVE-2024-9474) in its next-generation firewalls. CVE-2024-0012 (CVSS 9.3) is an authentication bypass flaw that allows attackers to access the management interface and gain administrative privileges without authentication. CVE-2024-9474 (CVSS 6.9) is a privilege escalation vulnerability enabling administrators to execute actions with root-level privileges. Exploitation of these vulnerabilities has led to malware deployment and unauthorized command execution on compromised systems, with reports of over 2,000 firewalls being breached.

Why You Should Care *- These vulnerabilities provide attackers with administrative control and the ability to escalate privileges, leading to potential widespread system compromise. Immediate patching is recommended. See Aspire's Emergency Flash Notice for further details.*

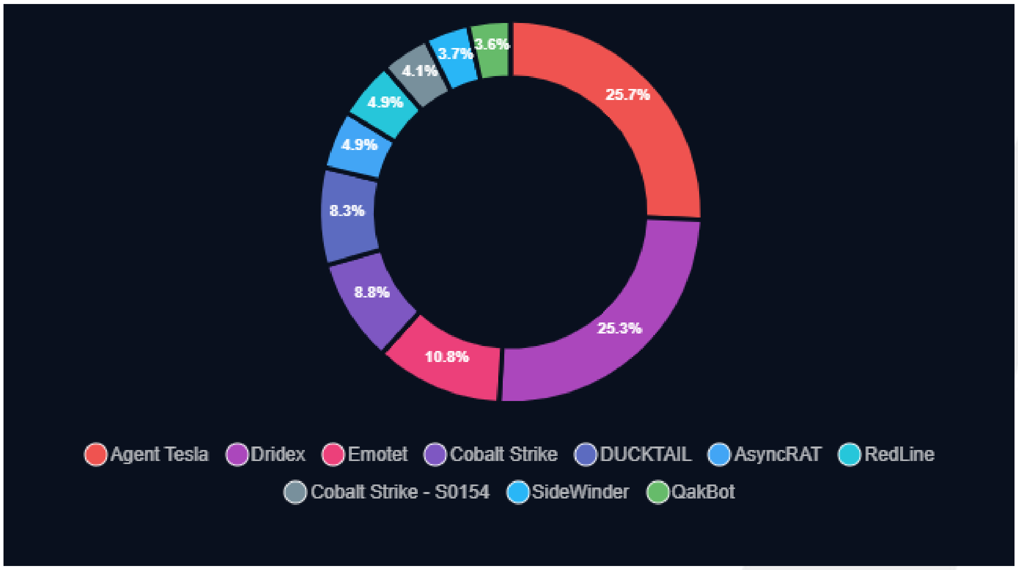
Microsoft Re-releases November 2024 Security Updates for Exchange

Microsoft has re-released the November 2024 Security Updates (SUs) for Exchange Server to address an issue in the original release (SUv1, KB5044062) that caused transport rules to stop functioning after a certain period. The updated version (SUv2, KB5049233) resolves this problem and introduces improved control over the X-MS-Exchange-P2FromRegexMatch header. All environments are advised to install SUv2, regardless of prior installation status or issues encountered with SUv1. Servers using Microsoft or Windows Update will automatically receive SUv2 in December 2024. Updated download links and additional guidance can be found in the original announcement and Exchange Health Checker tool.

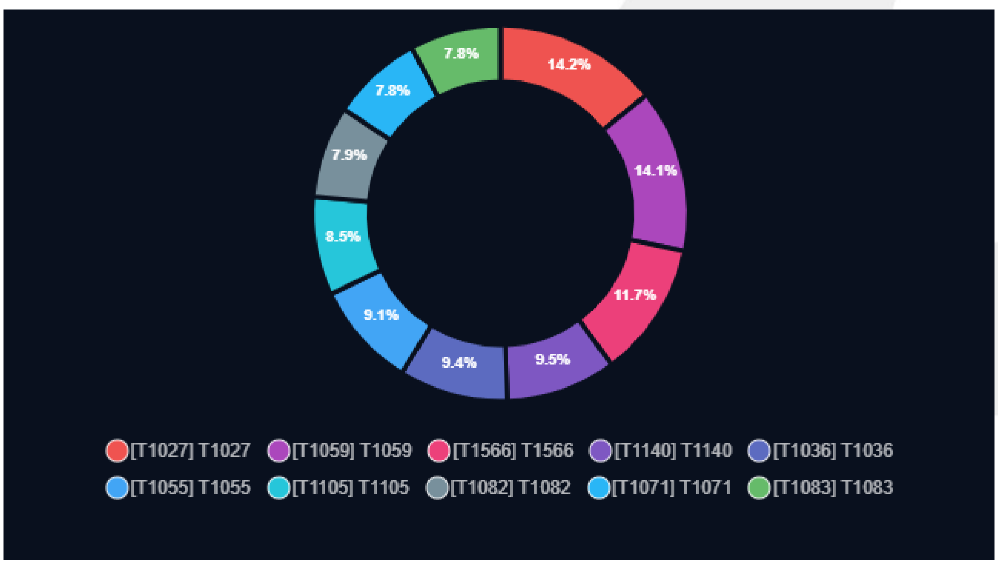
Why You Should Care *– SUv2 resolves critical transport rule issues and enhances functionality, making it vital for maintaining a secure and operational Exchange environment. For more details, see Microsoft's blog.*

Intelligence for November 2024

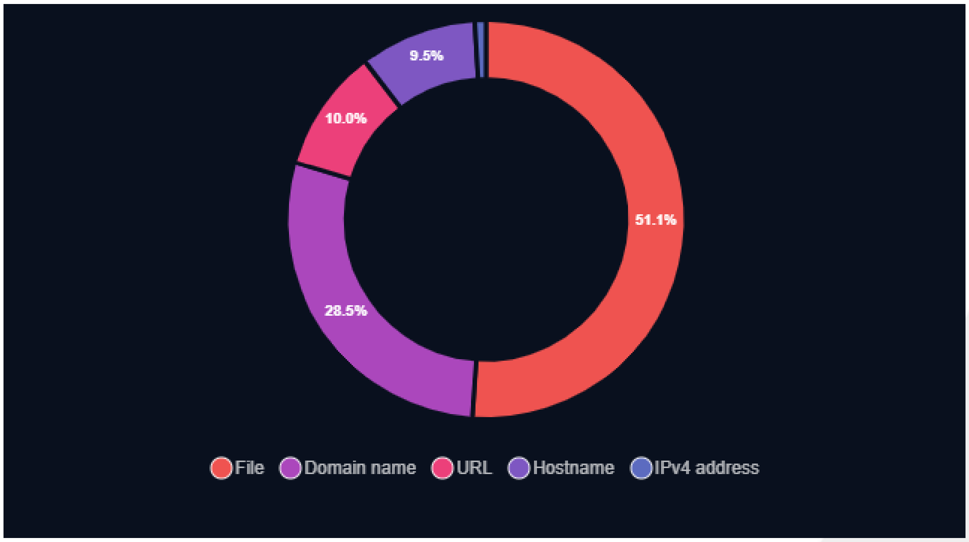
Top Threat Actors



Top ATT&CK Techniques



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, manufacturing, and finance sectors. Here is the latest research for those sectors.

Top Threat Actors for November 2024

Top Threat Actors November 2024

- **Government** - Targeted by UNC4841, Turla, Sponsoring Access, Iron Tiger, Crimson, Integrity Technology Group
- **Technology** - Targeted by UNC4841, Earth Krahang, Dark Angels, Dark Power, Lazarus Group, SloppyLemming, Integrity Technology Group, Rast gang, Flax Typhoon
- **Finance** - Targeted by Earth Krahang, Lazarus Group, Rast gang
- **Manufacturing** - Targeted by UNC4841, Earth Krahang, Sponsoring Access, Dark Angels, Dark Power, Twisted Panda, Rast gang, APT27

Crimson

- The Crimson Palace espionage campaign, carried out by three Chinese state-backed cyberespionage groups, has continued to target Southeast Asian governments, despite efforts to disrupt their activity. Sophos' recent report highlights ongoing attacks by the groups, Cluster Alpha, Cluster Bravo, and Cluster Charlie, which are tied to Chinese threat actors such as APT15 and APT41. Despite identifying and blocking some of their custom tools, the groups have adapted by using open-source tools and even a new malware called "Tattletale" to gather sensitive information.

Their activities have expanded across Southeast Asia, with attacks on at least 11 organizations, including government and public service entities. The campaign aims to steal data, maintain access to networks, and deliver malware to other targets. The groups are extremely persistent, evading security measures and leveraging compromised organizations for further attacks. These espionage efforts are seen as part of China's broader geopolitical strategy, particularly in light of tensions over the South China Sea.

Dark Angels

- The Dark Angels ransomware group, active since April 2022, is known for its sophisticated attacks targeting large corporations for significant ransom payments. Recently, researchers discovered the group has been targeting Windows, Linux, and ESXi systems using advanced techniques like phishing and exploiting vulnerabilities such as CVE-2023-22069. They use a double-extortion strategy, combining file encryption with data theft, and focus on high-value industries like healthcare and technology. Dark Angels operates independently, using modified Babuk, RTM Locker, and RagnarLocker variants for encryption, and exfiltrates massive amounts of data through their leak sites. Their selective targeting and stealthy lateral movement help maximize financial gains while avoiding detection.

APT27

- The Budworm APT group, also known as LuckyMouse or APT27, continues to evolve its toolset. In August 2023, the group targeted a Middle Eastern telecommunications organization and an Asian government using a previously unseen variant of its SysUpdate backdoor, SysUpdate DLL (inicore_v2.3.30.dll). Budworm deployed SysUpdate through DLL sideloading via the legitimate INISafeWebSSO application, a technique used by the group since 2018. SysUpdate offers various capabilities, including process management, file manipulation, and command execution. In addition to SysUpdate, the attackers used tools like AdFind, Curl, SecretsDump, and PasswordDumper for credential harvesting and network mapping. Budworm, active since at least 2013, continues to focus on intelligence-gathering campaigns targeting government, technology, and defense sectors.

Top Malware for November 2024

Top Malware November 2024

- **Government** - Targeted by RedLine Stealer, Hiloti, SolarPhantom, macOS.NotLockBit, CollectionRAT, ROGUEEYE, Pineflower, and Anunak
- **Technology** - Targeted by RedLine Stealer, Hiloti, SolarPhantom, macOS.NotLockBit, ROGUEEYE, DurianBeacon, AsyncRAT, Nimbo-C2, Lancefly, and Win.Worm.Coinminer
- **Finance** - Targeted by RedLine Stealer, Hiloti, ShadowPad - S0596, SolarPhantom, macOS.NotLockBit, CollectionRAT, Pineflower, Anunak, DurianBeacon, AsyncRAT, Lancefly, and Win.Worm.Coinminer
- **Manufacturing** - Targeted by RedLine Stealer, Hiloti, ShadowPad - S0596, SolarPhantom, Anunak, REPTILE, DurianBeacon, AsyncRAT, Nimbo-C2, Lancefly, and Win.Worm.Coinminer

RedLine Stealer

- ESET has released a detailed analysis of the RedLine Stealer malware empire following its dismantling in October by a Dutch-led operation with support from the FBI and UK's NCA. RedLine Stealer, one of the most widespread infostealers, harvested sensitive data such as cryptocurrency wallets, credit card details, and platform credentials. Sold as a subscription-based "turnkey infostealer solution," it was used by affiliates in campaigns posing as ChatGPT downloads or video game cheats. ESET identified over 1,000 unique IP addresses linked to its infrastructure, with most located in Germany, the Netherlands, and Russia. The malware's creator, Maxim Rudometov, has been identified and charged in the US.

NotLockBit

- NotLockBit is a ransomware family mimicking LockBit and is notable for being one of the first fully functional ransomware threats targeting macOS systems. Written in Go and distributed as an x86_64 binary, it can also target Windows systems. NotLockBit uses a double extortion model, exfiltrating data to an Amazon S3 bucket via hardcoded AWS credentials before encrypting files with RSA encryption, appending the ".abcd" extension, and issuing ransom demands. While mimicking LockBit's branding, researchers have found no affiliation between the two. Analysts consider NotLockBit an emerging threat to macOS and beyond.

Anunak

- The CARBANAK (aka ANUNAK) remote access trojan has resurfaced in a new campaign delivered via IDATLOADER (aka HIJACKLOADER), a malware loader gaining prominence in 2024. IDATLOADER, known for embedding payloads in PNG files using IDAT chunk steganography, has been used by a variety of threat actors, including ransomware groups. Kroll's analysis of an anomalous IDATLOADER sample revealed CARBANAK, a sophisticated malware associated with financially motivated APT groups such as FIN7 and Cobalt Gang. These groups have shifted focus over the years, from financial fraud to ransomware attacks targeting major industries. While CARBANAK's source code was leaked in 2019, Kroll assesses with high confidence that this activity is linked to the original operators, likely signaling a new campaign leveraging IDATLOADER for advanced attacks.

Security Incidents

T-Mobile Breach

This month, T-Mobile was breached by Salt Typhoon, a Chinese state-sponsored group, in a cyber-espionage campaign that targeted major U.S. telecoms, including AT&T and Verizon. Hackers exploited telecom vulnerabilities, accessed call records, unencrypted messages, and infiltrated systems used for law enforcement surveillance.

The breach, part of an eight-month campaign, highlighted weaknesses in the telecom sector, classified as critical infrastructure under U.S. law. Federal agencies investigated the incident, and T-Mobile worked to strengthen defenses through measures like zero-trust architecture and phishing-resistant authentication. Though T-Mobile reported no significant customer impact, the breach raised national security concerns, as high-ranking officials’ communications were compromised.

Amazon Breach

In November 2024, Amazon revealed a data breach involving a third-party property management vendor that exposed over 2.8 million lines of employee data, including work emails, phone numbers, and building locations. The breach stemmed from the MOVEit Transfer vulnerability, CVE-2023-34362, exploited since May 2023. Amazon assured that its core systems, including AWS, were unaffected, and customer data remained secure.

The cybercrime group "Nam3L3ss" claimed responsibility, posting the Amazon data online alongside information from 25 other organizations. The group, claiming access to over 250TB of stolen files, threatened further leaks. While ties to previous Cl0p ransomware attacks are suspected, researchers have yet to confirm Nam3L3ss’s affiliation or independence.

This breach highlights ongoing risks in supply chain security, as MOVEit-related attacks have impacted over 2,000 organizations and 62 million individuals. This breach is a reminder of the importance of managing vendor risks and demonstrates how even well-secured companies can be vulnerable to third-party exploits.

Notable TTPs TLP:AMBER

Execution

- **Command and Scripting Interpreter (T1059)** - Adversaries can exploit command and script interpreters, such as Unix Shell, PowerShell, Python, JavaScript, and Visual Basic, to execute commands, scripts, or binaries on systems. These interpreters are built into many platforms, including macOS, Linux, and Windows, and can be used by attackers to run arbitrary commands. Common methods of abuse include embedding malicious scripts in payloads delivered through lures or secondary downloads, executing commands through interactive terminals or shells, and utilizing remote services for remote execution.
- **Mitigations**
  - **Antivirus/Antimalware** - Antivirus can automatically quarantine suspicious files.
  - Audit - Regularly inventory systems for unauthorized command and scripting interpreters.
  - **Behavior Prevention on Endpoint** - Enable ASR rules on Windows 10 to block potentially harmful scripts from downloads.
  - **Code Signing** - Restrict execution to only signed scripts where possible.
  - **Disable or Remove Feature or Program** - Uninstall unnecessary or unused scripting interpreters and shells.
  - **Execution Prevention** - Use application control like PowerShell's Constrained Language mode to restrict dangerous commands.
  - **Limit Software Installation** - Prevent users from installing unneeded command or scripting interpreters.
  - **Privileged Account Management** - Limit PowerShell use to administrators and consider PowerShell JEA for remote sessions.
  - **Restrict Web-Based Content** - Use script-blocking extensions and adblockers to stop malicious scripts or ads from executing.
- **Detections**
  - **Command Execution** - Monitor command-line arguments for scripts that may indicate post-compromise behavior or suspicious activity.
  - **Module Load** - Track the loading of scripting modules like JScript.dll or vbscript.dll to detect potential script execution.
  - **Process Creation** - Monitor logs for processes linked to command-line or scripting activities, including unusual module loads.
  - **Process Metadata** - Capture data like environment variables or image names to identify abnormal process behavior, such as PowerShell downgrades.
  - **Script Execution** - Monitor for unusual script execution, especially on systems where scripts are uncommon, and capture scripts to assess intent.

Defense Evasion

- **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.