December 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

Exploitation of Cleo File Transfer Software Vulnerabilities

Attackers are exploiting vulnerabilities in Cleo's file transfer software products—Harmony, VLTrader, and LexiCom—specifically CVE-2024-50623 and an unauthenticated host zero-day (CVE pending). CVE-2024-50623 allows unrestricted file uploads and downloads, allowing attackers to install malicious backdoor code on affected versions up to 5.8.0.23, with a patch released in October 2024 (v5.8.0.21) that proved ineffective. The zero-day flaw, affecting all versions including 5.8.0.21, exploits default Autorun directory settings, allowing attackers to execute arbitrary commands.

Why You Should Care *- These vulnerabilities can lead to unauthorized system access, data theft, and malicious alterations. Please see Aspire's Emergency Flash Notice for patch guidance.*

Cisco ASA Cross Site Scripting Vulnerability Exploited in the Wild

Cisco's CVE-2014-2120, a medium-severity cross-site scripting (XSS) vulnerability in the WebVPN login page of Cisco Adaptive Security Appliance (ASA) software, has been actively exploited as of November 2024. This flaw, which was initially disclosed in 2014, allows unauthenticated remote attackers to perform XSS attacks due to insufficient input validation. Attackers can exploit the vulnerability by tricking users into clicking a malicious link, leading to

unauthorized file uploads, code injection, and potential system compromise. The Androxgh0st botnet has been leveraging this and other vulnerabilities across various products.

Why You Should Care *- CVE-2014-2120 allows attackers to exploit insufficient input validation on the WebVPN login page, allowing for cross-site scripting (XSS) attacks. This could lead to unauthorized file uploads and malicious code insertion. Please see Aspire's Emergency Flash Notice for patch guidance.*

Actively Exploited Zero-Day in Windows CLFS Driver

Microsoft disclosed an actively exploited vulnerability in the Windows Common Log File System (CLFS) driver, tracked as CVE-2024-49138, as part of its December 2024 Patch Tuesday updates. This elevation of privilege flaw, with a CVSS score of 7.8, allows attackers to escalate privileges to SYSTEM level due to improper data validation in CLFS operations. While exploitation requires local access, it is low in complexity and does not need user interaction. Successful exploitation gives attackers complete control over affected systems. The vulnerability impacts a wide range of Windows operating systems, including Windows 10 (21H2 and later), Windows 11 (22H2), and Windows Server versions 2008 through 2022.

Why You Should Care *- Exploitation of CVE-2024-49138 is actively occurring and requires only local access. With no user interaction needed, attackers can easily gain full control, leading to potential data breaches and system compromise. See Aspire's Emergency Flash Notice for further details.*

Three Sophos Firewall Vulnerabilities

Sophos has resolved three vulnerabilities in its Sophos Firewall product that could allow attackers to perform remote code execution (RCE), SQL injection, and gain privileged SSH access. The issues include CVE-2024-12727, a pre-authentication SQL injection vulnerability potentially leading to RCE; CVE-2024-12728, a non-random SSH login passphrase that could permit unauthorized access; and CVE-2024-12729, a code injection vulnerability allowing authenticated users to execute arbitrary code and escalate privileges. These flaws affect Sophos Firewall version 21.0 GA and earlier, with limited exposure based on specific configurations.

Why You Should Care *- If the vulnerabilities in Sophos Firewall are exploited, attackers could execute arbitrary code remotely, leading to full system compromise. For patch guidance, please see Aspire's Emergency Flash Notice.*

Exploitation of Cleo File Transfer Software Vulnerabilities

Attackers are actively exploiting vulnerabilities in Cleo's file transfer software products—Harmony, VLTrader, and LexiCom—leading to unauthorized access, malicious file execution, and system compromise. These include CVE-2024-50623, an unrestricted file upload and download vulnerability allowing attackers to install backdoors, and an unauthenticated host zero-day that exploits default settings to execute arbitrary commands. While a patch for CVE-

2024-50623 was released in October 2024, it was ineffective.

Why You Should Care *- Exploitation of CVE-2024-50623 can lead to data theft, system compromise, and unauthorized changes to critical infrastructure. See Aspire's Emergency Flash notice for further details.*

Microsoft Update: Transition from AzureEdge.net Domains for .NET Developers

Microsoft is urging .NET developers to quickly update their applications and development pipelines to stop using the "azureedge.net" domains for installing .NET components due to the bankruptcy and imminent shutdown of CDN provider Edgio. The domains "dotnetcli.azureedge.net" and "dotnetbuilds.azureedge.net" will be unavailable in the coming months, potentially disrupting projects reliant on these services, including developers using .NET installers, GitHub Actions, Azure DevOps with custom pipelines, and Docker or script users referencing these domains.

As a result, Microsoft is transitioning to new CDN domains hosted by Edgio, Akamai, and Azure Front Door, with plans to consolidate the final distribution model in 2025. Developers are advised to update their code, scripts, and configurations to use builds.dotnet.microsoft.com instead, and CI/CD teams should ensure their workflows support these changes. Although the timing of this transition during the holiday season is challenging for IT teams, Microsoft has stated that it cannot simply continue using the old domains, despite owning them, in order to prevent future supply chain risks.

Why You Should Care *- Organizations relying on .NET components and development pipelines could face significant disruptions if they don't update their configurations before the "azureedge.net" domains go offline.*

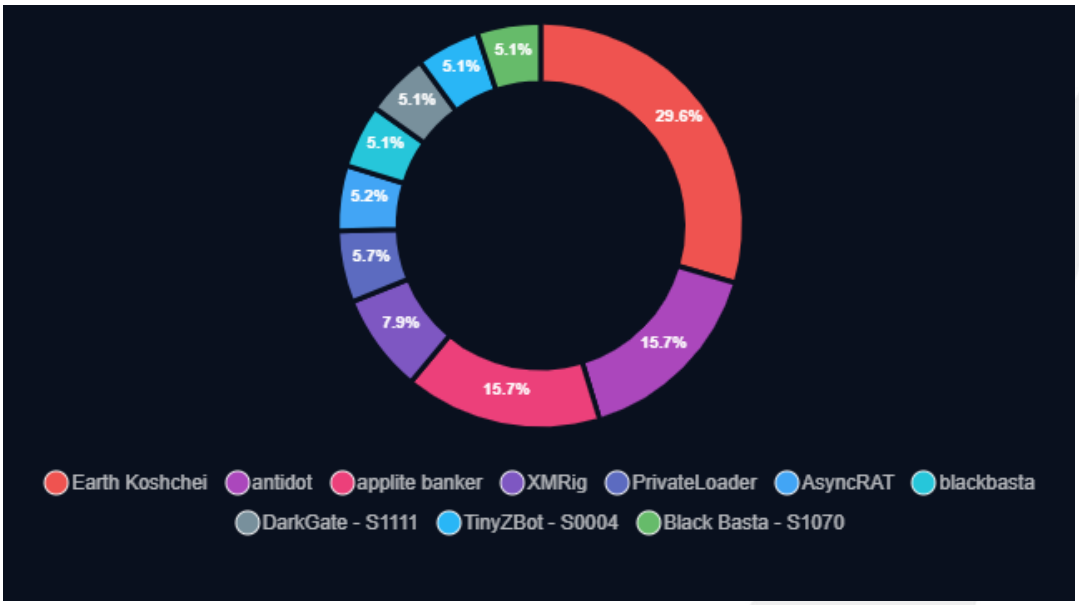
Rising Threat of Botnets Targeting Outdated D-Link Routers

Malware botnets, including Ficora and Capsaicin, have been targeting outdated D-Link routers in recent attacks. These devices, which include models such as DIR-645, DIR-806, GO-RT-AC750, and DIR-845L, are vulnerable due to outdated firmware or having reached end-of-life status. The botnets exploit known vulnerabilities such as CVE-2015-2051, CVE-2019-10891, CVE-2022-37056, and CVE-2024-33112 to gain initial access. Once compromised, the malware uses weaknesses in D-Link's management interface to execute commands, steal data, and potentially launch DDoS attacks. Ficora, a newer Mirai variant, spreads via brute force and shell scripts, while Capsaicin, linked to the Keksec group, infects devices through a downloader script.

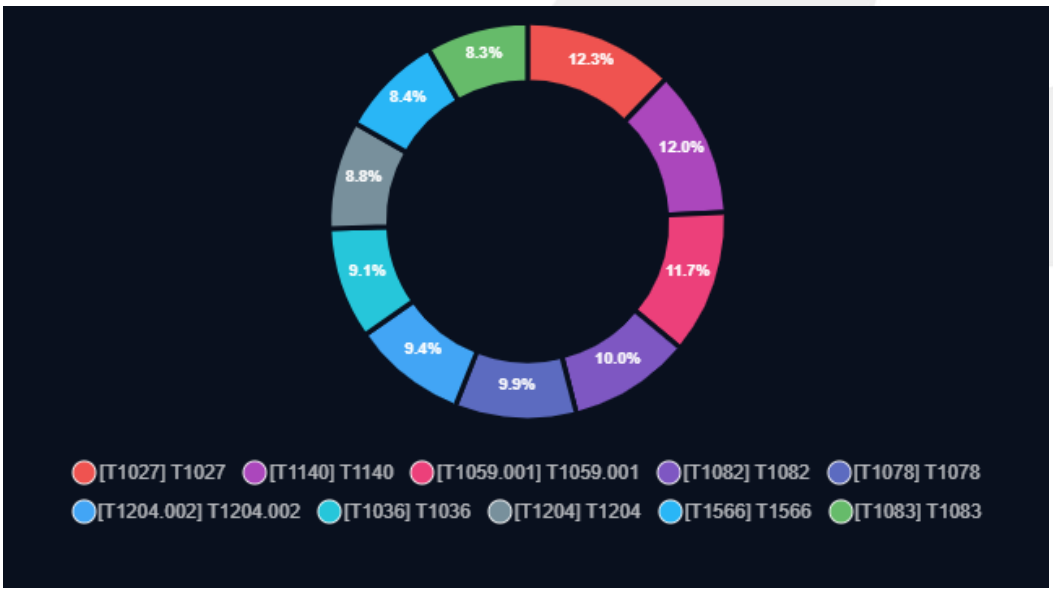
Why You Should Care *- These botnets can compromise outdated routers, leading to unauthorized access, data theft, and the potential for launching large-scale DDoS attacks. To defend against these attacks, organizations should ensure their devices are running the latest firmware or replace them if they no longer receive updates. Additionally, using strong, unique passwords and disabling unnecessary remote access can help reduce the risk of infection.*

Intelligence for December 2024

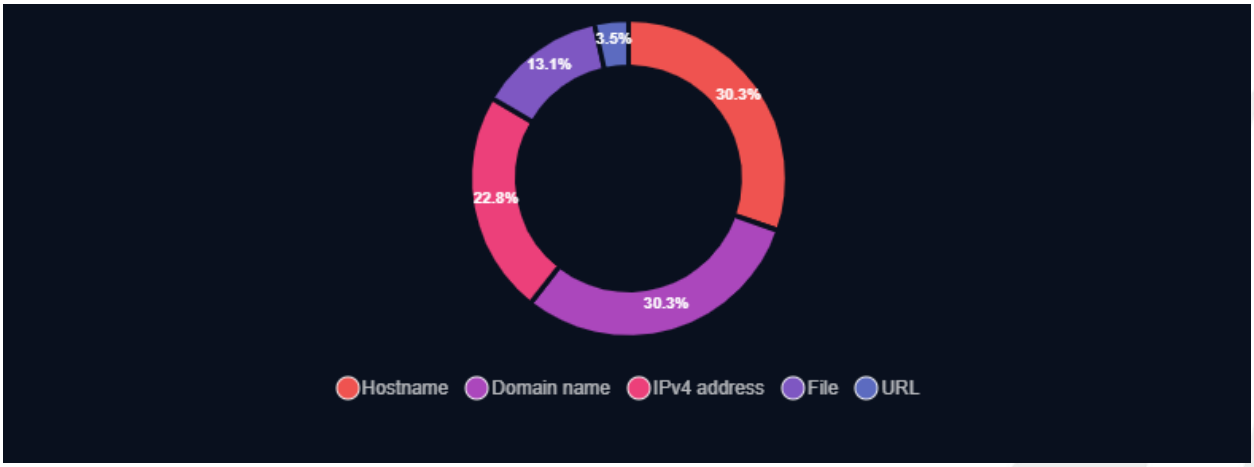
Top Threat Actors



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 manufacturing, information technology, human services, and healthcare sectors. Here is the latest research for those sectors.

Top Threat Actors for December 2024

Top Threat Actors December 2024

- **Manufacturing** – BlackBasta, BianLian, Kairos, Lynx, Howling Scorpius, ElDorado, 8Base, Nitrogen
- **Human Services** – BlackBasta, Akira, BianLian, SafePay, RansomHub, Lynx, Howling Scorpius, Play, Nitrogen
- **Information Technology** – BlackBasta, Akira, BianLian, RansomHub, Qilin, Kairos, Lynx, Play, ElDorado
- **Healthcare** – BlackBasta, Akira, BianLian, RansomHub, Qilin, Kairos, 8Base

BlackBasta

- The Black Basta ransomware group, linked to Storm-1811, has enhanced its tactics since October 2024 by using social engineering, phishing, and advanced payloads like Zbot and DarkGate. Their approach includes email bombing victims by signing them up for multiple mailing lists, followed by direct contact, often impersonating IT personnel via Microsoft Teams. Victims are urged to install legitimate remote access tools, which

attackers use to deploy malware, harvest credentials, and potentially bypass MFA. QR codes have also been introduced to redirect users to malicious sites. Black Basta's evolution, including the use of proprietary tools like KNOTWRAP and DAWNCRY, demonstrates a shift from botnet reliance to hybrid methods.

Howling Scorpius

- The Howling Scorpius ransomware group, initially observed in early 2023, operates the Akira ransomware-as-a-service (RaaS) platform and ranks among the most active ransomware groups globally. Using a double extortion strategy, the group targets small to medium-sized businesses across North America, Europe, and Australia in diverse sectors, including education, government, manufacturing, and technology.

  Operating both Windows and Linux encryptors, including ESXi variants, Howling Scorpius continually upgrades its tools, increasing the risk for targeted organizations. Its Tor-based leak site pressures victims by threatening to release stolen data, even if systems are restored without payment.

Safe Pay

- The SafePay ransomware group, which operates using a LockBit-based ransomware binary, has claimed 22 victims so far, as exposed by a Huntress report. This emerging cybercrime group was linked to two incidents in October 2024, affecting companies from different industries. Huntress was able to investigate and reverse-engineer SafePay's ransomware due to vulnerabilities in both the group's website and obfuscation techniques.

  SafePay's tactics mirror those of other well-known groups, including INC Ransomware and ALPHV/BlackCat, and involve using RDP for initial access, followed by file encryption and exfiltration. The group also leverages methods for privilege escalation and defense evasion, such as the use of a UAC bypass and manual manipulation of Windows Defender settings. Researchers recommend using specific detection rules for identifying SafePay's tactics, including monitoring unusual use of WinRAR and changes to security settings.

Top Malware for December 2024

Top Malware December 2024

- **Government** - Akira - S1129, MASOL RAT, SparrowDoor, GHOSTSPIDER, Owowa, SNAPPYBEE, TwoDash, Tavdig, ROAMINGMOUSE, UPPERCUT - S0275, BADNEWS - S0128
- **Technology** - Akira - S1129, MASOL RAT, SparrowDoor, GHOSTSPIDER, CrowDoor, ROAMINGMOUSE, UPPERCUT - S0275
- **Energy** - Owowa
- **Defense** - MiniPocket, TwoDash, Tavdig

Masol Rat/GhostSpider

- Since 2023, the Chinese APT group Earth Estries has been actively targeting critical sectors worldwide, focusing on industries like telecommunications and government entities across the US, Asia-Pacific, the Middle East, and South Africa. The group employs sophisticated tactics and a range of backdoors, including MASOL RAT and GHOSTSPIDER, to conduct long-term espionage. Earth Estries exploits public-facing server vulnerabilities to gain initial access and uses tools like living-off-the-land binaries and custom malware for lateral movement and sustained infiltration.

  GHOSTSPIDER, identified in Southeast Asian telecommunications companies, is a modular backdoor designed for targeted attacks, while MASOL RAT, discovered in Southeast Asian government networks, further enhances the group's cross-platform capabilities. Additionally, Earth Estries shares some TTPs with other Chinese APTs, such as FamousSparrow and GhostEmperor, although it remains unclear if they are directly connected. The group's tactics, including targeting vendor networks and using rootkits like DEMODEX, allowing them to maintain a long-term presence within compromised networks.

TwoDash

- Turla, a Russia-linked advanced persistent threat (APT) group, has been exploiting the infrastructure of a Pakistani hacking group, Storm-0156, since December 2022. This strategy, observed by Lumen Technologies' Black Lotus Labs and Microsoft, involves Turla infiltrating Storm-0156's command-and-control (C2) servers to conduct its own operations while remaining covert. By leveraging this access, Turla deployed custom malware families, including TwoDash, a bespoke downloader, and Statuezy, a trojan that logs clipboard data. This campaign primarily targeted Afghan government networks and Indian military institutions. TwoDash was used alongside other malware, such as MiniPocket, in a sophisticated operation that allowed Turla to further infiltrate the target networks without directly attacking them.

Tavdig

- Russian nation-state actor Secret Blizzard has been leveraging tools from other threat actors to conduct espionage activities, including using Amadey bot malware to deploy its custom Tavdig backdoor, which enables further access and installation of the KazuarV2 backdoor. In early 2024, Secret Blizzard used the Amadey bot, associated with cybercriminal group Storm-1919, to target Ukrainian military devices. The Tavdig backdoor, deployed through a PowerShell dropper, helped Secret Blizzard establish a foothold for deeper reconnaissance and persistence within compromised systems.

  Tavdig, specifically identified as Trojan:Win32/Tavdig.Crypt, was used to extract sensitive information and prepare devices for the KazuarV2 backdoor. Secret Blizzard's use of third-party malware shows their strategy of taking advantage of existing access. They focus on Ukrainian military devices and use advanced techniques to avoid detection, like encrypted survey tools and custom payloads to drop their malware.

Security Incidents

U.S Sanctions Chinese Company

The U.S. government has imposed sanctions on the Beijing-based Integrity Technology Group for supporting Flax Typhoon, a Chinese state-sponsored cyber group involved in large-scale botnet operations targeting American organizations and critical infrastructure. Active since at least 2021, Flax Typhoon exploits known vulnerabilities to infiltrate networks and maintain persistent access using legitimate remote access tools. Their botnet, which spans 260,000 devices including firewalls, routers, and IoT devices, has been linked to distributed denial-of-service (DDoS) attacks and malware distribution. The sanctions block Integrity Technology's U.S.-based assets and prohibit financial transactions involving the company.

***Why You Should care**: With a botnet of over 260,000 devices capable of launching DDoS attacks, infiltrating networks, and delivering malware, these operations threaten business continuity and data security.*

AT&T and Verizon

AT&T and Verizon have confirmed breaches in a widespread Chinese cyber-espionage campaign, attributed to the threat actor Salt Typhoon, targeting telecom carriers globally. Both companies stated that the attackers have been removed from their networks, with Verizon reporting no recent threat actor activity and AT&T noting limited incidents of foreign intelligence gathering and customer data exposure. T-Mobile also disclosed similar breaches but highlighted that its defenses prevented access to sensitive customer information. The campaign, which has affected nine U.S. telecommunications firms and carriers in numerous other countries, has prompted the U.S. government to consider banning China Telecom's operations and investigate TP-Link routers for potential national security risks.

U.S. Senator Ron Wyden has introduced the "Secure American Communications Act," a bill aimed at strengthening the cybersecurity of American telecommunications networks following breaches by Salt Typhoon. The proposed legislation mandates the Federal Communications Commission (FCC) to enforce binding cybersecurity rules, including annual vulnerability testing, timely patching, and independent compliance audits by telecom providers. Wyden criticized past regulatory leniency, which he claims allowed foreign hackers to exploit telecom systems, compromising calls, messages, and phone records. In response, FCC Chairwoman Jessica Rosenworcel pledged urgent action to bolster network security. Salt Typhoon, active since 2019, has breached multiple U.S. telecom carriers and remains a significant threat, with federal agencies advising encrypted communication to mitigate risks.

***Why You Should Care** - The Salt Typhoon breaches emphasize vulnerabilities in U.S. telecom networks, which serve as the backbone for critical infrastructure, businesses, and government operations. Hackers accessed sensitive data, including calls, messages, and phone records, increasing the risk of espionage and operational disruptions.*

Phishing Campaign Compromises 35 Chrome Extensions, Exposing Millions

A sophisticated phishing campaign has compromised at least 35 Google Chrome extensions, affecting approximately 2.6 million users by injecting malicious code to steal sensitive information. Hackers targeted extension developers through deceptive emails resembling official Google notifications, tricking them into granting OAuth permissions and bypassing multi-factor authentication. This allowed attackers to release tampered updates of popular extensions, including VPN tools, AI assistants, and productivity apps, which extracted session tokens, cookies, and credentials, particularly from Facebook Ads dashboards. Security researchers have linked the campaign to earlier phishing activity beginning in March 2024, with malicious payloads connecting to command-and-control servers for data exfiltration.

Why You Should Care *- Users are urged to uninstall or update affected extensions, reset credentials, and review permissions, while developers are advised to strengthen security practices against phishing attacks and conduct application checks.*

Notable TTPs TLP:AMBER

Defense Evasion

- **Deobfuscate/Decode Files or Information (T1140)** - Attackers may use obfuscated files or data to hide their activities, relying on malware tools or system utilities to decode or deobfuscate it. For example, they might use certutil to decode a remote access tool or the Windows copy /b command to reassemble binary fragments into malicious payloads. In some cases, they trick users into opening files or entering passwords to decrypt protected files.
    - **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**
        - **File Modification -** Monitor for unexpected changes made to files that could be attempts to hide intrusion artifacts. Suspicious file accesses, such as attempts to modify files that should not be altered, can indicate efforts to conceal evidence.
        - **Process Creation -** Monitor for the execution of processes that may be used to hide traces of an attack, such as common archive utilities (e.g., Zip and RAR tools), and correlate with other suspicious behaviors to reduce false positives from normal user or admin actions.
        - **Script Execution -** Monitor for attempts to run scripts on a system, especially if scripts are not typically used. Scripts executed outside of expected schedules or maintenance periods should be flagged for further analysis.

- **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.