MARCH 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 Aids Prospective Client During Active Ransomware Attack

On the weekend of February 22–23, 2025, Aspire Technology Partners' Security Operations Center (SOC) team was contacted by a company that was not yet an official customer - but had been in discussions about becoming one. The organization had just discovered signs of a compromise. What followed was a real-time demonstration of Aspire's commitment responsiveness and customer-first values.

The compromise began the night of February 21st, when the potential customer's Network Security Engineer identified unauthorized activity in their domain. Threat actors had created a new domain admin account named "**support**", which was later used to access Domain Controllers and backup servers. It was also used to access zip files on a file server. The threat actors were also able to interact with the engineer's Remote Desktop Protocol (RDP) session even after the session was terminated, meaning the threat actor likely had live control of the system.

While on duty, SOC analyst, **Cathy Omanukwue**, detected the creation of a suspicious local admin account named "**veeamsupport"** on the client's backup server. Recognizing this as suspicious, Cathy acted immediately - isolating the server from the network within the hour. This decisive move protected the organization's only remaining backup server from further compromise, preserving their last line of recovery.

As soon as the rest of the SOC team caught wind of the breach, they jumped in - dropping everything over the weekend to help. After digging into the activity, they confirmed the Monti ransomware group was behind the attack.

Why this Win Matters *- Although the client wasn't under contract, Aspire's SOC treated the incident with urgency and focus. The team stepped in immediately to contain the threat and help stabilize the potential client's environment. The event showed just how valuable Aspire's SOC truly is and strengthened the trust that had already begun to form between the two teams. This incident also reinforced Aspire's core belief - when an organization is under threat, protecting their environment comes before paperwork.*

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

Microsoft Signed Driver Exploited in Ransomware Attacks

Threat actors are leveraging a zero-day vulnerability (CVE-2025-0289) in a Microsoft-signed driver from Paragon Software, using a Bring Your Own Vulnerable Driver (BYOVD) attack to escalate privileges and execute ransomware payloads. The BioNTdrv.sys driver, which is part of Paragon Partition Manager, has been actively exploited, even on systems where the software was never installed.

CERT Coordination Center issued an urgent advisory, warning that attackers are using this flaw to gain SYSTEM-level privileges before executing further malicious code. While Microsoft has blocked the vulnerable driver, multiple privilege escalation vulnerabilities remain in BioNTdrv.sys, making it a prime target for ransomware gangs looking to evade endpoint detection and response (EDR) solutions.

Why You Should Care *- Ransomware groups continue to weaponize signed drivers to evade security tools and escalate privileges, making traditional*

defenses less effective. Organizations must patch immediately, block vulnerable driver versions, and monitor for signs of privilege escalation activity.

Ingress Nightmare Vulnerabilities Allow Unauthenticated RCE in Ingress NGINY Controller

A set of high-severity flaws, known as IngressNightmare, affects the Ingress NGINX Controller for Kubernetes. Attackers could remotely execute code and access secrets across namespaces. Over 40% of internet-facing clusters may be impacted, including those used by Fortune 500 firms.

- CVEs (CVSS 9.8) – CVE-2025-24513, CVE-2025-24514, CVE-2025-1097, CVE-2025-1098, CVE-2025-1974
- Affected Products – Ingress NGINX Controller versions before 1.12.1, 1.11.5, 1.10.7

Why You Should Care *– Exploitation of these vulnerabilities can lead to full cluster compromise. See Aspire's Emergency Flash Notice for further details.*

Windows Zero Day Exploited in Cyber Espionage

A Windows zero-day flaw (ZDI-CAN-25373) has been actively exploited since 2017 by at least 11 state-backed groups from North Korea, Iran, Russia, and China. The vulnerability allows code execution via malicious shortcut (.lnk) files, allowing for data theft and cyber espionage. Microsoft does not plan to patch it immediately.

Why You Should Care *- All Windows versions are affected. Threat actors use this flaw to deploy malware and maintain persistent access. See Aspire's Emergency Flash Notice for details.*

Apache Tomcat Vulnerability Actively Exploited

A remote code execution vulnerability in Apache Tomcat (CVE-2025-24813, CVSS 9.8) was actively exploited just 30 hours after disclosure. Attackers used a PUT request to upload a malicious session file, then trigger execution via a crafted JSESSIONID. The flaw takes advantage of Tomcat's file-based session persistence and partial PUT handling.

Exploitation does not require authentication but depends on specific conditions - such as write access being enabled for the default servlet and the presence of a deserialization-capable library.

Why You Should Care *- Exploitation can result in full system compromise. Affected versions include Tomcat 9.x, 10.x, and 11.x. See Aspire's Emergency Flash Notice for details.*

VMware Zero-Day Vulnerabilities Exploited in the Wild

Broadcom released emergency patches for three VMware zero-day vulnerabilities (CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226) currently being exploited in the wild. The flaws impact ESXi, vSphere, Workstation, Fusion, Cloud Foundation, and Telco Cloud products.

Attackers with admin or root access to a VM can chain these flaws to escape the sandbox and run code on the host.

Why You Should Care *- These vulnerabilities are already being used in real-world attacks. Affected systems span multiple VMware platforms. See Aspire's Emergency Flash Notice for details.*

Google Zero-Day Exploited in Phishing Attacks

A zero-day vulnerability in Google Chrome (CVE-2025-2783) is being actively exploited in the wild. The flaw, caused by an incorrect handle in Mojo on Windows, allows for arbitrary code execution through drive-by compromise. Victims are typically lured through phishing emails - once the malicious link is clicked, code executes within the browser context of the logged-on user.

If the user has administrative privileges, attackers can install programs, steal or alter data, or create new accounts with full access.

Why You Should Care *- This zero-day affects Chrome versions prior to 134.0.6998.177/.178 for Windows. Google confirmed exploitation in the wild, with Kaspersky linking it to phishing-based delivery. Organizations should patch immediately, enforce least-privilege access, and monitor for suspicious browser behavior. See Google's Stable Channel for details.*

FBI Warns of File Converter Scam

The FBI Denver Field Office is warning about a growing scam where cybercriminals use free online file converter or downloader tools to spread malware. These sites perform as advertised, converting or combining files, but the resulting downloads may contain hidden malware that can lead to ransomware, identity theft, or data compromise.

These tools may also harvest sensitive information from uploaded files, including personal details, banking data, cryptocurrency wallet info, and login credentials. Victims often don't realize they've been compromised until significant damage has occurred.

Why You Should Care *- This scam is widespread and hard to detect. Avoid using free online converters from untrusted sources. Scan downloaded files with antivirus tools and educate users on the risks. If you are a victim, see the FBI's recommendations on next steps. Victims are also urged to report incidents to IC3.gov.*

SuperBlack Ransomware Exploits Two Fortinet Vulnerabilities

A new ransomware group called *Mora_001* is exploiting two Fortinet authentication bypass flaws (CVE-2024-55591 and CVE-2025-24472) to gain unauthorized access to firewall appliances and deploy a custom ransomware strain known as *SuperBlack*.

Although Fortinet initially claimed CVE-2025-24472 hadn't been exploited, Forescout researchers observed attacks using the flaw as early as February 2, 2025. Fortinet later updated its advisory to confirm active exploitation.

Attack Chain

The group exploits the vulnerabilities using WebSocket and HTTPS-based attacks to gain *super_admin* access. They then create persistent admin accounts (e.g., *forticloud-tech*, *fortigate-firewall*, *adnimistrator*) and configure automation tasks to restore them if removed. Lateral movement is carried out using stolen VPN credentials, WMIC, SSH, and TACACS+/RADIUS.

Before encrypting data, *Mora_001* exfiltrates sensitive information using a custom tool. After encryption, a ransom note is dropped, and a custom wiper called *WipeBlack* is used to erase the ransomware executable and hinder forensic efforts.

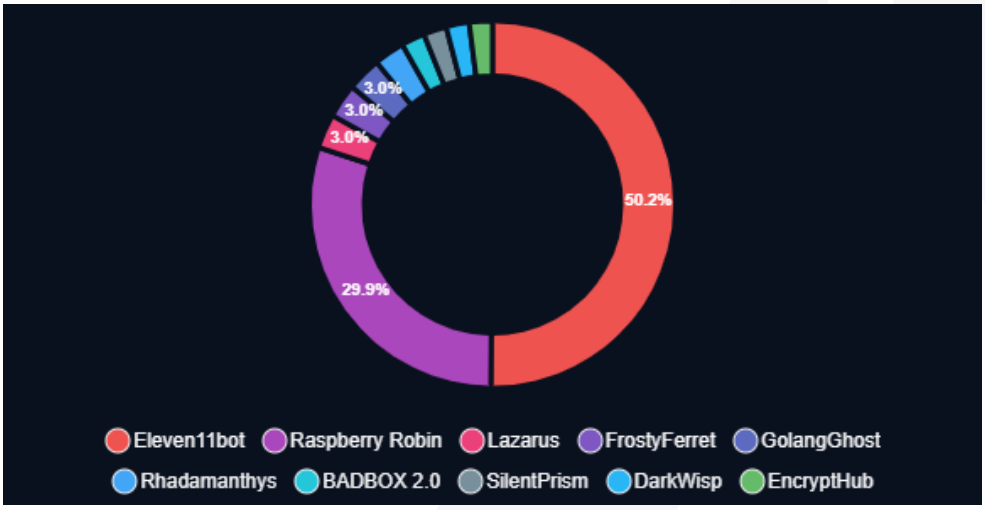
Ties to LockBit

Forescout found strong links between *SuperBlack* and LockBit. The encryptor is based on LockBit 3.0's leaked builder, featuring the same payload structure and encryption methods. The ransom note contains a TOX ID tied to LockBit, suggesting *Mora_001* may be a former affiliate or team member. Infrastructure overlaps and reuse of *WipeBlack*, also seen in other LockBit-connected campaigns, further support the link.

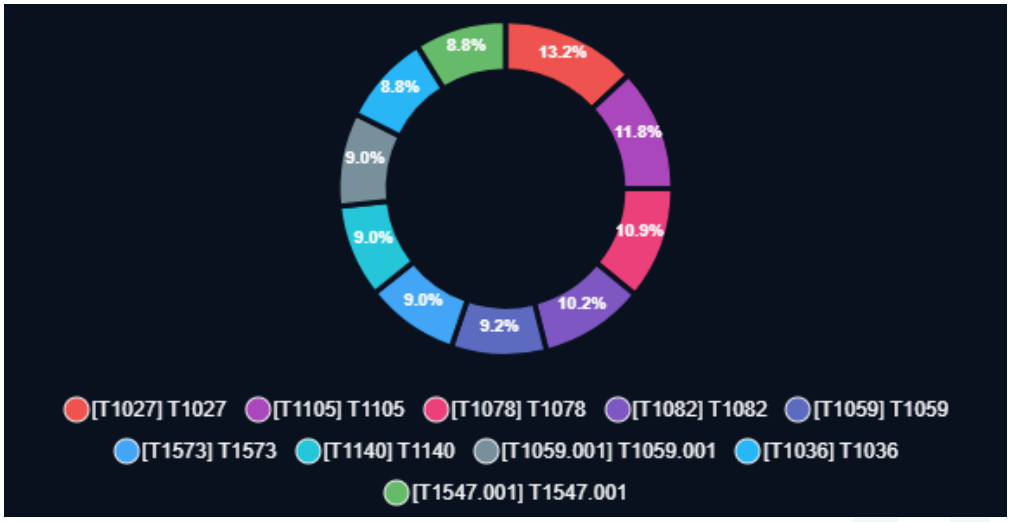
Why You Should Care *- SuperBlack is a concern because it's breaking in through Fortinet firewalls - your first line of defense. It doesn't just lock up files; it steals data, moves around your network, and covers its tracks. The group behind it moves fast and organizations need to be on guard when it comes to this ransomware group. For more details regarding SuperBlack ransomware please see the CTI team's Threat Intelligence Report.*

INTELLIGENCE FOR MARCH 2025

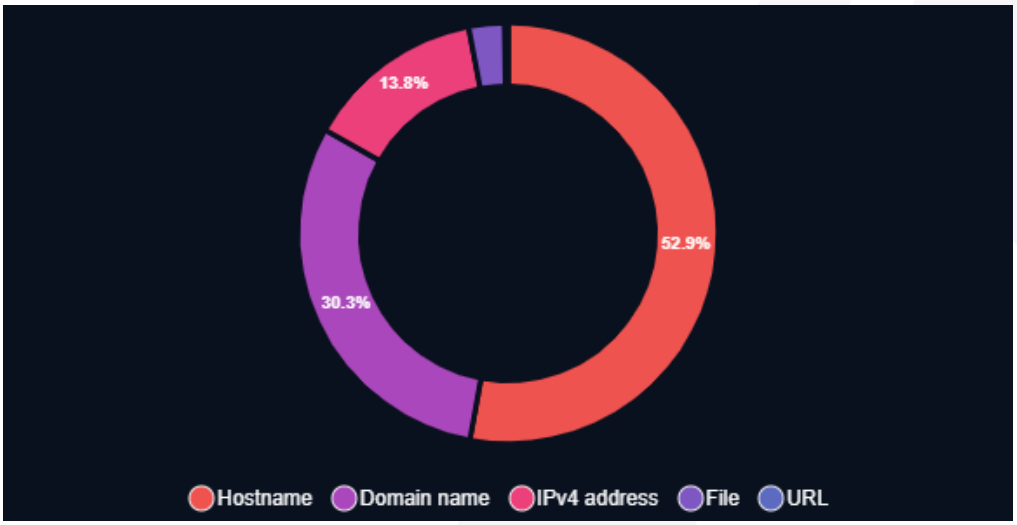
Top Threat Actors



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

TOP THREAT ACTORS FOR MARCH 2025

Top Threat Actors March 2025

- **Government** – PrintSteal, Head Mare and Twelve, Blind Eagle, ForumTroll, Water Gamayun, Paragon Solutions
- **Technology** – PrintSteal, UNC3886, Ransomhub, Lazarus, Desert Dexter, Crazy Evil
- **Defense** – Blind Eagle, UNC3886, Water Gamayun
- **Telecommunications** – UNC3886, REF8685

PrintSteal

- PrintSteal is a cybercriminal operation engaged in large-scale production and distribution of fraudulent Indian KYC documents, including Aadhaar and PAN cards. Operating since at least 2021, the group has utilized over 1,800 domains—about 600 currently active - to host fake platforms impersonating legitimate government services like the Common Service Centre (CSC) scheme. These websites employ illicit APIs to retrieve sensitive data, minimizing direct user input. The operation has reportedly generated significant revenue.

Blind Eagle (APT-C-36)

- Blind Eagle, also known as APT-C-36, is a South American threat actor active since at least 2018, primarily targeting entities in Colombia and other Latin American countries. The group employs spear-phishing emails to deliver various remote access trojans (RATs) like AsyncRAT and NjRAT, aiming at sectors including government, finance, and energy. Notably, Blind Eagle has exploited vulnerabilities such as CVE-2024-43451 to capture NTLMv2 hashes, facilitating unauthorized access and potential data theft.

UNC3886

- UNC3886 is a China-linked cyber espionage group known for exploiting zero-day vulnerabilities in network and virtualization technologies, including Fortinet and VMware products. The group has deployed custom malware and rootkits, such as variants of the TinyShell backdoor, to maintain persistent access and evade detection. Their operations often target systems lacking Endpoint Detection and Response (EDR) support.

Water Gamayun

- Water Gamayun, also known as EncryptHub and Larva-208, is a suspected Russian threat actor identified exploiting the MSC EvilTwin vulnerability (CVE-2025-26633) in the Microsoft Management Console framework. By manipulating .msc files and the MUIPath, they execute malicious code to establish persistence and exfiltrate sensitive data.

Top Malware for March 2025

Top Malware March 2025

- **Government** – ScreenConnect, Medusa, WhisperGate - S0689, PhantomJitter, Mispadu - S1122, RPipeCommander
- **Telecommunications** – ScreenConnect, Medusa, TINYSHELL, Lumma Stealer, Remcos, SEAELF, GOBRAT, BUSYBOX, Raspberry Robin
- **Defense** – Medusa, WhisperGate - S0689, Downloader Module, TINYSHELL, Remcos, SEAELF, GOBRAT, BUSYBOX, Raspberry Robin
- **Finance** – ScreenConnect, Mispadu - S1122

Medusa

- Medusa is a ransomware-as-a-service (RaaS) operation first identified in 2021. It has targeted over 300 victims across sectors such as healthcare, education, legal, insurance, technology, and manufacturing. The group uses phishing campaigns and exploits unpatched software vulnerabilities to infiltrate systems. Once inside, Medusa encrypts files and demands a ransom, often threatening to release sensitive data publicly, a tactic known as double extortion. Also, Medusa utilizes "living off the land" techniques, leveraging legitimate system tools to evade detection.

Lumma Stealer

- Lumma Stealer, also known as LummaC2, is an information-stealing malware written in C. Active since at least August 2022, it operates under a malware-as-a-service (MaaS) model. Lumma primarily targets sensitive data such as credentials, cryptocurrency wallets, and browser information. Recent campaigns have employed deceptive tactics like fake CAPTCHA verifications and malvertising to distribute the malware.

SeaElf

- SEAELF is an installer component associated with the MEDUSA rootkit, employed by the Chinese cyber espionage group UNC3886. This tool facilitates the deployment of the MEDUSA rootkit on compromised Linux systems, enabling unauthorized access and credential harvesting. SEAELF's role is pivotal in establishing persistence and facilitating further malicious activities within targeted networks.

SECURITY INCIDENTS

TMobile

T-Mobile has been ordered to pay $33 million in a SIM swapping case linked to the theft of cryptocurrency. The case was brought by investor Joseph “Josh” Jones, who lost over 1,500 bitcoin and 60,000 bitcoin cash (worth $38 million at the time) after an attacker gained control of his phone number. Despite having enhanced security measures, including an eight-digit PIN, the attacker was able to bypass protections, allegedly by exploiting internal access to T-Mobile’s systems.

The court ruled in favor of Jones, citing T-Mobile’s multiple security failures. The payout includes over $6.5 million in legal fees and interest. Lawyers for the plaintiff accused T-Mobile of attempting to hide the breach and obstruct the case, calling the company’s actions a threat to public trust. The case stresses long-standing concerns about SIM swapping and highlights the need for telecom providers to improve account security and prevent similar incidents in the future.

***Why You Should Care** - This case shows how weak telecom security can directly lead to major financial losses, even for accounts with extra protections. If attackers can bypass MFA by hijacking a phone number, it puts not just crypto wallets but bank accounts, email, and sensitive data at risk.*

Medusa Demands $100k to $15M in Ransom

Medusa ransomware has ramped up its activity in early 2025, with over 40 confirmed attacks in just the first two months of the year. Operating as a RaaS group, Medusa targets sectors like healthcare, education, legal, and manufacturing. Threat actors gain access using phishing emails and vulnerabilities in tools like ScreenConnect and Fortinet EMS. Once inside, they use legitimate tools such as AnyDesk and Advanced IP Scanner to maintain access and move laterally, often disabling endpoint protection along the way.

Medusa actors use double extortion (encrypting data while threatening to leak it) to pressure victims into paying ransoms that range from $100,000 to $15 million. The group's aggressive tactics and expanding list of victims have made it one of the most active ransomware threats this year.

Why You Should Care *- Medusa isn't just locking up files, it's stealing data and using it as leverage to force big payouts. If your organization relies on remote tools or hasn't patched recent vulnerabilities, you could already be at risk. The group moves fast and ignoring it could mean millions lost.*

SECURITY REPORTS

Uptick in Identity Based Attacks in 2024

A recent Cisco Talos report reveals that in 2024, identity-based attacks were responsible for 60% of cybersecurity incidents, affecting every stage of the attack lifecycle. Attackers frequently exploited valid credentials and native tools, with Active Directory targeted in 44% of these cases and cloud API compromises accounting for 20%. The primary motivations behind these identity-focused attacks included ransomware (50%), credential harvesting and resale (32%), espionage (10%), and financial fraud (8%).

The report also highlights significant weaknesses in MFA implementations, such as the absence of MFA on virtual private networks and vulnerabilities to MFA exhaustion attacks. Additionally, while the use of artificial intelligence by threat actors was limited in 2024, it was primarily used to enhance social engineering tactics and automate phishing campaigns. Looking ahead, the report expresses concern over the potential for AI systems themselves to become targets, especially as they are increasingly integrated into supply chain pipelines.

Why You Should Care *- Identity is now the front door for most attacks. If your organization isn't protecting credentials or enforcing strong, well-implemented MFA, you're giving attackers an easy way in. These intrusions are hard to spot and harder to stop because they look like normal user behavior. Failing to address identity security could lead to ransomware attacks and data theft.*

NOTABLE TTPS TLP:AMBER

Command and Control

- **Ingress Tool Transfer (T1105)** - Adversaries may transfer tools or files from external systems into a compromised environment. This can be achieved through command and control channels or alternative protocols like FTP. Once inside, these tools can facilitate further exploitation or lateral movement within the network.
    - **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**
        - **Network Traffic Analysis** – Monitor for anomalous data flows, such as unexpected file transfers from external sources or unusual protocols being used for data transfer.
        - **Process Monitoring** – Track the execution of utilities commonly used for downloading files, like certutil, PowerShell, curl, or wget, especially when they are used to access external resources.
        - **File Monitoring** – Observe the creation of new executable files in directories where such files are not typically added, which may indicate unauthorized tool transfers.

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.