JUNE 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!

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

Oyster, Kepavll, and BHO.BJ – Malware to Watch

Three lesser-known malware strains, Oyster, Kepavll, and BHO.BJ, are quietly infiltrating networks through outdated software, misleading ads, and fake installers. While they don't get as much attention as high-profile ransomware, they exploit the gaps defenders often overlook, like legacy tech and user habits.

Why This Matters *– Oyster has shown up in real ransomware attacks that hit U.S. airports. Kepavll operates in that murky space where tools don't look quite malicious enough to trigger alarms. BHO.BJ targets systems that organizations forgot they were still running. These kinds of threats slip through the cracks because they're not loud. Ignoring them is exactly what attackers count on. Read the full Threat Intelligence Report on the malware strains on Aspire's customer portal.*

Two-Year-Old Linux OverlayFS Privilege Escalation Vulnerability Exploited

Attackers are actively exploiting CVE-2023-0386, a high-severity vulnerability in the Linux kernel's OverlayFS subsystem, to escalate privileges from local user accounts directly to root. Exploitation involves abusing filesystem permissions to place malicious setuid binaries in writable locations, giving attackers complete administrative control.

Why This Matters *- This vulnerability may not be new, but attackers are actively abusing it now. It gives them an easy path to full root access on vulnerable systems. It's especially risky for organizations running containers or shared environments, where one compromised user can quickly escalate to total control. See Aspire's Emergency Flash Notice for more information.*

Citrix Bleed 2 Vulnerability Exploited – Attackers Hijacking NetScaler Sessions

Attackers are actively exploiting CVE-2025-5777 (CVSS 9.3), a critical memory-overread vulnerability dubbed "Citrix Bleed 2". Threat actors are hijacking user sessions and bypassing multi-factor authentication (MFA) on NetScaler ADC and Gateway. Immediate upgrade to patched versions and termination of active ICA and PCoIP sessions is highly recommended.

Why This Matters *- Attackers are now abusing Citrix Bleed 2 to hijack live NetScaler sessions and bypass MFA, without needing credentials. This gives them direct, privileged access into enterprise environments, often without detection. See Aspire's Emergency Flash Notice for further details.*

Cisco Unified CM Vulnerability Opens Door for Full System Takeover

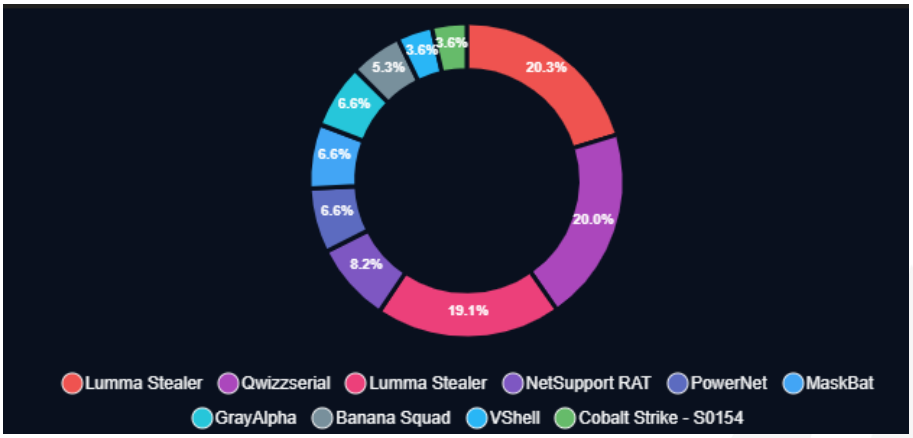
Cisco has publicized a critical vulnerability (CVE-2025-20309, CVSS 10) in certain versions of Cisco Unified Communications Manager (Unified CM) and Session Management Edition (SME). The flaw involves static, undeletable root credentials that could let a remote attacker take full control of the system. There are no workarounds. Users should patch immediately.

Why This Matters *- This vulnerability leaves a hidden backdoor wide open. There is no password guessing, no brute force, just instant root access via SSH. If you're running*

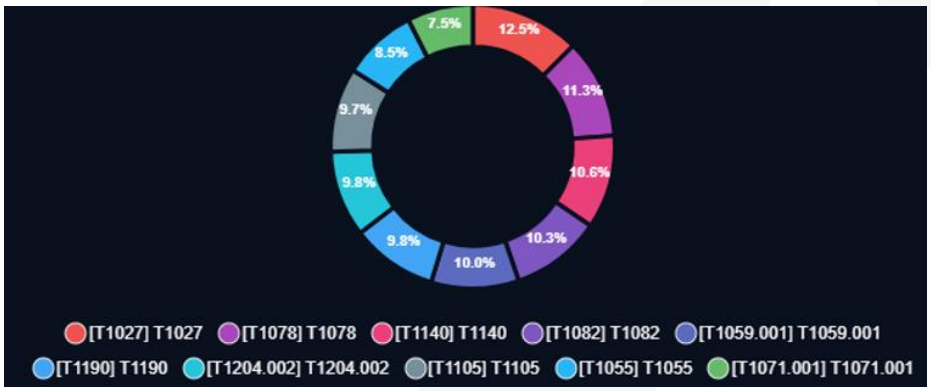
the affected Cisco Unified CM versions, attackers can take full control by only logging in. See Aspire's Emergency Flash Notice for further details.

INTELLIGENCE FOR JUNE 2025

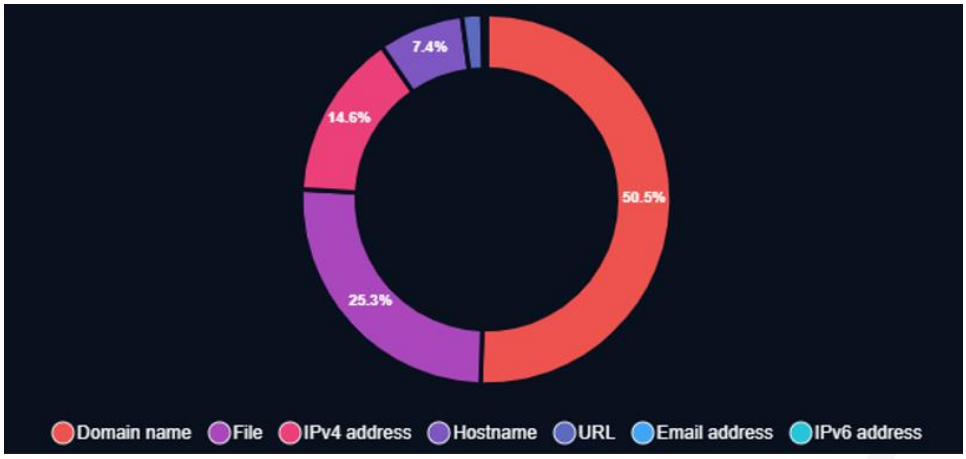
Top Threat Actors



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

Top Threat Actors for June 2025

Top Threat Actors June 2025

- **Government** – Void Blizzard, Earth Lamia, Proton66, Hazy Hawk, LapDogs, Sednit, Interlock Ransomware, TAG-110, Educated Manticore, Hive0131, TAG-140
- **Finance** – UNC5221, Earth Lamia, Proton66, China-nexus threat actors, Hazy Hawk, Hive0131, Void Dokkaebi, Danabot
- **Telecommunications** – Void Blizzard, UNC5221, China-nexus threat actors, LapDogs
- **Defense** – Void Blizzard, UNC5221, Sednit, Interlock Ransomware, TAG-110, TAG-140, Danabot

TOP MALWARE FOR JUNE 2025

Top Malware June 2025

- **Government** – PLUSDROP, GOREshell, DUSTTRAP, Crisis, NonRansomware, Ursnif – S0386
- **Finance** – Auto-Color, GOREshell, Brute Ratel, XMRig, Crisis, NonRansomware, Ursnif – S0386, Nimbo-C2
- **Defense** – Auto-Color, Crisis, NonRansomware, Ursnif – S0386
- **Technology** – PLUSDROP, Auto-Color, GOREshell, DUSTTRAP, XMRig, ShortLeash

Void Blizzard

- In June, threat actors continued to exploit trusted platforms. UNC6032 pushed fake AI websites through social media ads to deliver malware, while APT41 used Google Calendar as a command-and-control channel in a three-stage attack chain. Microsoft also flagged a new Russia-linked group, Void Blizzard, targeting government and critical sectors with low-complexity tactics like phishing and credential theft, proving that even basic methods can still lead to serious compromises.

Interlock Ransomware

- Interlock is a newer ransomware strain that targets both Windows and FreeBSD systems, encrypting files and appending “.interlock” to filenames. It’s often delivered through fake browser updates hosted on compromised sites and uses a social engineering tactic called “ClickFix” to get users to run malicious commands. The group behind it claims they’re forcing organizations to improve cybersecurity, but their actions (especially against healthcare) show otherwise.

Goreshell

- A recent campaign by China-backed threat actors involved the deployment of GoReShell malware as part of broader attacks targeting finance, government, and manufacturing sectors - along with an attempted hit on SentinelOne. GoReShell was used across both Windows and Linux systems to establish persistent remote access via reverse shells, allowing the attackers to quietly maintain footholds in compromised environments. The malware was delivered alongside ShadowPad and PurpleHaze, with DLL side-loading used to help evade detection on Windows.

Earth Lamia

- Earth Lamia, a China-linked APT group, continues to launch widespread attacks across industries including finance, government, IT, logistics, retail, and education. Their campaigns rely heavily on exploiting public-facing vulnerabilities in widely used platforms like Apache Struts, GitLab, WordPress, TeamCity, CyberPanel, Craft CMS, and most recently SAP NetWeaver (CVE-2025-31324). Fortinet and Trend Research have both reported consistent activity linked to this group, noting that Earth Lamia shifts targeting patterns over time. After gaining access, they deploy a modular .NET backdoor capable of loading plugins from their C2 server on demand. This makes detection and response more challenging.

Proton66

- Blind Eagle (also known as APT-C-36) has been observed leveraging the Russian bulletproof hosting service Proton66 to deliver phishing campaigns and remote access trojans (RATs) targeting Colombian banks. Trustwave linked a network of Proton66-hosted domains using dynamic DNS services like DuckDNS to distribute Visual Basic Script (VBS) loaders, which are used to silently deploy off-the-shelf RATs like AsyncRAT and Remcos. These phishing sites impersonated major banks such as Bancolombia and Davivienda to harvest credentials and install malware. Proton66's refusal to honor takedown requests gives threat actors like Blind Eagle a stable infrastructure to maintain persistent access and evade shutdown.

ShortLeash Backdoor

- The China-linked LapDogs campaign has been quietly compromising SOHO routers and IoT devices across the globe since 2023, using a custom backdoor called ShortLeash to maintain stealth access and persistence. SecurityScorecard researchers found that ShortLeash is deployed through Bash scripts on Linux systems, establishing covert command-and-control channels while disguising its traffic using fake TLS certificates. Some even spoof entities like the LAPD. This malware features multi-layer encryption, fake Nginx responses, and plugin-based functionality, allowing attackers to operate undetected for extended periods. Its use of compromised everyday devices, especially outdated routers, makes it particularly hard to spot and remove.

SECURITY INCIDENTS

Iran vs. The United States

As tensions escalate between the U.S. and Iran following recent military actions, federal agencies are urging critical infrastructure operators to be on heightened alert for potential cyber threats. A joint advisory from CISA, FBI, NSA, and DoD warns that although there's currently no evidence of a coordinated campaign, Iran has a track record of retaliating through cyberattacks, especially by exploiting well-known, unpatched vulnerabilities in internet-facing systems. Iran-affiliated actors often target weakly secured networks using tactics like password spraying and DDoS attacks, particularly when geopolitical tensions rise.

For the cybersecurity community, this is a moment to stay focused, not reactive. Overhyping the threat only amplifies Iran's psychological warfare objectives, but downplaying it risks exposure. Vigilance, patching, phishing-resistant MFA, and OT network isolation remain key as threat actors look for any opening during this unpredictable period.

Why This Matters *– Iran has a documented history of exploiting known weaknesses in U.S. infrastructure during geopolitical flare-ups, often causing major disruptions. With rising tensions, even uncoordinated attacks could escalate quickly. It's important to implement cyber security best practices now, instead of trying to react to a breach later.*

Cloudflare Outage

Google Cloud and Cloudflare issued public apologies following a major outage on June 12 that disrupted access to services like Spotify and Discord. The disruption stemmed from a Google Cloud policy update that triggered a crash loop in its API infrastructure, with recovery in some regions taking hours. Cloudflare's own outage was tied to its reliance on Google Cloud-backed storage for Workers KV, which experienced a 90% request failure rate during the incident. Both vendors emphasized their responsibility for managing third-party dependencies and outlined plans to boost system resilience, improve communication, and prevent future widespread disruptions.

Why This Matters *- The outage exposed how deeply organizations rely on cloud infrastructure providers, and how a single failure (whether internal or through a third-party dependency) can ripple across multiple industries and popular platforms. It also*

reinforces the need for better resiliency planning and dependency management, especially as more businesses move toward cloud-native operations.

80,000 Entra ID Accounts Targeted by Password Spraying Campaign

Hackers using the TeamFiltration red team tool have targeted over 80,000 Microsoft Entra ID accounts since December 2024, focusing on cloud-based identity systems across hundreds of organizations. The attacker, tracked as UNK_SneakyStrike, used password-spraying tactics (especially aggressive during early January) to compromise accounts. The threat actor leveraged AWS infrastructure, Microsoft Teams APIs, and a Office 365 account to enumerate users and bypass defenses. Researchers at Proofpoint linked the campaign to TeamFiltration based on unique technical markers, including rare user agents and embedded outdated code from known security tools.

Why This Matters *- Identity-based attacks continue to succeed because many organizations still lack basic controls like MFA and conditional access. If threat actors are refining their tooling and exploiting public cloud services, defenders need to start strengthening their identity hygiene and detecting lateral movement early.*

Episource Data Breach Exposes Health Records of Over 5 Million U.S. Patients

Episource, a U.S.-based healthcare technology firm, confirmed a data breach that compromised the personal and medical information of over 5.4 million individuals. The breach occurred between January 27 and February 6, 2025, when attackers accessed and exfiltrated data from the company's systems.

Exposed data includes names, addresses, Social Security numbers, insurance and Medicaid details, and medical records, though no financial data was involved. The incident was discovered in early February, but the breach was officially reported to federal authorities in June. Episource has been notifying impacted individuals on behalf of its clients since April, advising them to stay alert for fraud and identity theft.

Why This Matters *- Healthcare data breaches carry long-term consequences, as medical and personal information is highly sensitive and difficult to change. With millions affected, this breach shows the growing risk of outsourcing data to third-party vendors in the healthcare sector.*

SECURITY REPORTS

OpenAI Uncovers Global Abuse of Language Models in Cyber Operations

OpenAI's June 2025 report reveals how cybercriminals are increasingly misusing AI to power attacks on cloud infrastructure, manipulate public discourse, and scale social engineering. The company detailed operations where large language models were used to generate fake résumés, bypass endpoint protections, automate phishing, and deploy tailored propaganda across platforms like TikTok and Telegram. Threat actors linked to North Korea, Russia, China, and Cambodia were observed leveraging ChatGPT to develop malware, target U.S. defense networks, and run influence and scam campaigns. OpenAI says its defensive approach combines AI-driven detection with manual review, while coordinating with cloud vendors and security partners to shut down abusive use.

Why This Matters *- Threat actors are now using AI not just to boost attack volume but to improve believability and speed. As adversaries incorporate LLMs, defenders will need to rethink traditional detection strategies and invest in AI-assisted defense to keep up.*

Notable TTPs TLP:AMBER

Discovery

- **System Information Discovery (T1082)** - Adversaries gather system details like OS version, patches, architecture, and disk space to guide their next steps. Tools like systeminfo (Windows), systemsetup (macOS), and df -aH (Unix) help extract this data. On network devices and ESXi servers, commands like show version and esxcli are used. In cloud environments (AWS, Azure, GCP), attackers may use APIs to access virtual machine info. This data helps shape payloads, avoid detection, and decide whether to escalate the attack.
    - **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** – Watch for command-line activity that gathers detailed system or hardware information—such as OS

version, patch levels, service packs, or system architecture. On network gear, review AAA logs for unusual or unauthorized command use. For ESXi hosts, check /var/log/shell.log for discovery-related commands that could indicate reconnaissance.

- **OS API Execution** – Track API activity that queries detailed system and hardware information—like OS version, patch status, service packs, or architecture. Some remote access tools pull this data directly through Windows APIs. Others may use system utilities like PowerShell or WMI. In cloud environments, check native logs for access to APIs or dashboards that reveal system details. Keep in mind that some of this activity may be legitimate, depending on how the system is used.
- **Process Creation** – Watch for newly launched processes that try to collect system or hardware details such as OS version, patch levels, service packs, or system architecture.

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
CTI Threat Researcher

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.