

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	1
UK backs down in Apple privacy row, US says	2
Are High-Privilege NHIs Properly Protected?.....	3
Password Managers Vulnerable to Data Theft via Clickjacking	4
Acumen Cyber Threat Intelligence Digest – 22/08/2025, Week 33:.....	5

SC3 Daily Threat Summaries and Weekly Report



Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

This week's reports:



SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu
lletin-18-August-2025 lletin-19-August-2025 lletin-20-August-2025 lletin-21-August-2025 lletin-22-August-2025



ICO Scotland SC3-Weekly-vulnera
Guidance on MFA - bility-report-18-Aug



UK backs down in Apple privacy row, US says

The UK government has quietly backed away from a controversial demand that would have forced Apple to create a “back door” into its encrypted services—potentially giving authorities access to private data from users around the world, including Americans.

UK backs down in Apple privacy row, US says - BBC News

This demand was issued under the **Investigatory Powers Act** and targeted Apple’s **Advanced Data Protection (ADP)** feature, which encrypts user data so securely that even Apple can’t access it. To comply, Apple would have had to break its own encryption—something it flatly refused to do.

Instead, Apple pulled ADP from the UK market and launched a legal challenge, with a tribunal scheduled for early 2026. Now, according to a post by **US Director of National Intelligence Tulsi Gabbard**, the UK has dropped the demand. Apple hasn’t received formal confirmation yet, and the UK government remains tight-lipped, citing operational secrecy.

Privacy advocates are cautiously celebrating. Groups like **Liberty** and **Privacy International** had already filed legal actions against the UK government, warning that such powers could be abused to target politicians, activists, and minority groups. They argue that the mere existence of these powers poses a long-term risk.

The US and UK already have a **Data Access Agreement** for law enforcement cooperation, but this latest move was seen as overreach. Critics say it would have undermined global trust in encrypted services and set a dangerous precedent.

Action Point: Monitor Legal Developments – The UK’s Investigatory Powers Act still allows for future demands. Stay informed on any changes or tribunal outcomes.

Review Encryption Policies – Ensure your organisation’s use of end-to-end encryption aligns with legal frameworks in all operating regions.



Are High-Privilege NHIs Properly Protected?

In today's cloud-heavy environments, **Non-Human Identities (NHIs)**—like machine accounts, service principals, and API keys—are everywhere. They're the "tourists" in your system, and their credentials are the "passports" that grant access. But are these high-privilege NHIs being properly protected?

Main Article

The article highlights a growing concern: **many organisations overlook NHI security**, especially those with elevated access. These identities often have broad permissions and touch sensitive systems, making them prime targets for attackers. Without proper management, they can become major vulnerabilities.

Why NHI Management Matters

Poor NHI management can lead to:

- **Security gaps** that attackers exploit.
- **Compliance failures** due to lack of audit trails.
- **Operational inefficiencies** from manual secret handling.
- **Cost overruns** from unmanaged lifecycle processes.

The article compares securing NHIs to **guarding a fortress**—you need to protect both the identities and their credentials, monitor their activity, and manage their lifecycle from creation to decommissioning.

What Good NHI Management Looks Like

A solid NHI strategy includes:

- **Discovery** of all NHIs in your environment.
- **Classification** based on access and risk.
- **Threat detection** tied to usage patterns.
- **Remediation** for misconfigurations or exposed secrets.

You need **context-aware security intelligence** that understands how NHIs interact with your systems.

Action Point: Audit Your NHIs – Identify all machine identities, especially those with high privileges. Know what they access and how.

Implement Lifecycle Management – Track NHIs from creation to retirement. Automate secret rotation and decommissioning.

Use Centralized Governance Tools – Gain visibility and control over NHI permissions and usage.

Enforce Policy Compliance – Ensure NHIs meet regulatory standards with proper logging and access controls.

Educate Your Teams – Make sure developers and IT staff understand the risks and responsibilities tied to NHIs.

Stay Proactive – Monitor for anomalies and update your strategy regularly. NHI protection is not a one-time fix.



Password Managers Vulnerable to Data Theft via Clickjacking

A researcher has tested nearly a dozen password managers and found that they were all vulnerable to clickjacking attacks that could lead to the theft of highly sensitive data.

[Main Article](#)

The research was conducted by Marek Tóth and it was presented earlier this month at the DEF CON conference. The researcher has now also published a blog post detailing his findings.

The researcher targeted 1Password, Bitwarden, Dashlane, Enpass, Keeper, LastPass, LogMeOnce, NordPass, ProtonPass, RoboForm, and Apple's iCloud Passwords, specifically their associated browser extensions.

These browser extensions are very popular. An analysis by the researcher found that they have a total of nearly 40 million active installations, based on data from the official browser extension repositories for Chrome, Edge and Firefox.

Clickjacking is an attack technique in which the attacker tricks the targeted user into clicking on hidden elements on a web page. The attacker sets up a website that contains malicious buttons or other elements that are transparent and placed on top of harmless-looking elements on the page. When the victim visits the attacker's site and interacts with these harmless-looking elements, they are actually clicking on the malicious element, unknowingly carrying out dangerous actions.

Tóth showed how an attacker can use DOM-based extension clickjacking and the autofill functionality of password managers to exfiltrate sensitive data stored by these applications, including personal data, usernames and passwords, passkeys, and payment card information.

The [attacks demonstrated](#) by the researcher require 0-5 clicks from the victim, with a majority requiring only one click on a harmless-looking element on the page. The single-click attacks often involved exploitation of XSS or other vulnerabilities.

DOM, or Document Object Model, is an object tree created by the browser when it loads an HTML or XML web page. It enables JavaScript and other scripting languages to interact with and change the page, including hide elements, modify text, or add new content dynamically.

Action Point: "LastPass has implemented certain clickjacking safeguards, including a pop-up notification that appears before auto-filling credit cards and personal details on all sites, and we're committed to exploring ways to further protect users while continuing to preserve the experience our customers expect," Cox explained.

He added, "In the meantime, our [TIME] team encourages all users of password managers to remain vigilant, avoid interacting with suspicious overlays or pop-ups, and keep their LastPass extensions up to date."



Acumen Cyber Threat Intelligence Digest – 22/08/2025, Week 33:

The latest Cyber Threat Intelligence Digest highlights escalating exploitation of critical vulnerabilities and sophisticated phishing campaigns. Kaspersky reported that attackers are abusing CVE-2025-29824 to deliver the PipeMagic backdoor, a modular tool enabling credential theft, payload injection, and stealthy operations. The campaign, observed in Saudi Arabia and Brazil, spreads via trojanised ChatGPT apps, malicious help files, and DLL hijacking. Separately, Trustwave exposed EncryptHub's campaign blending social engineering with CVE-2025-26633 exploitation in Microsoft Management Console, using fake IT communications to trick victims into granting access. Fortinet also patched CVE-2025-52970 in FortiWeb, an authentication bypass vulnerability, though no active exploitation has been observed.

Main Article

Threat campaigns remain highly adaptive. Morphisec detailed phishing emails disguised as copyright claims delivering an updated Noodlophile Stealer via DLL side-loading, targeting Facebook business users worldwide. BleepingComputer tracked homoglyph-based phishing against Booking.com and Intuit, while Anurag highlighted fake voicemail alerts leading to Google credential theft through a convincing spoofed login flow.

General news saw UK telecom provider Colt report outages from a cyber incident, and Stock in the Channel disclose a ransomware attack with no data loss. Researchers also uncovered McDonald's app flaws enabling free rewards abuse and broader systemic weaknesses in its Design Hub platform, exposing sensitive corporate data.

Action Point - Remediation Actions: Following the information provided above, we recommend that the technologies mentioned be fully patched and updated. We also want to highlight and recommend applying the following patches where applicable:

- **CVE-2025-29824:** apply the latest Windows security updates addressing the CLFS (Common Log File System) driver. Restrict access to msbuild and other scriptable tools for non-developer users, monitor for suspicious use of msbuild.exe, and audit execution of .msh and .dll files from user directories. Implement application allowlisting and behavioural detection for named pipe communications and shellcode injection attempts. Investigate use of trojanised applications such as fake ChatGPT clients, and block their execution where possible.
- **CVE-2025-26633:** To mitigate the exploitation of this Microsoft Management Console (MMC) vulnerability, ensure all systems are patched with the latest security updates from Microsoft. Limit remote access privileges and educate staff on the risks of social engineering tactics such as impersonation via phone or Microsoft Teams. Monitor PowerShell execution logs for unusual .msc file activity and use endpoint detection tools to identify and block malicious payloads related to this vulnerability.
- **CVE-2025-52970:** Apply Fortinet's official patch for FortiWeb versions 7.0.0 through 7.6.3 to remediate this authentication bypass vulnerability. Organisations should upgrade to the fixed version as soon as possible and review access logs for signs of suspicious activity. Where patching is delayed, restrict access to FortiWeb management interfaces and limit exposure to trusted IP addresses.

All the best from all of us at HEFESTIS and look out for our next ThreatScape update next week.

SharePoint



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



[Cybershield Education MISP Stats \(Wednesday 27th Aug 2025\)](#)

Who is using the service 25 Organisations 68 Users What's new this update For the past month (28th July – 27th Aug) 1,815 published events 97,805 attributes marked for IDS 397 compromised suppliers 1,656 Critical/High CVEs 294 NCSC events 56 OSINT e...

Steve McIntosh

8/28/2025

8 views



Scottish
Cyber
Coordination
Centre

[SC3 weekly threat reports](#)

Action Point: Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

Steve McIntosh

8/28/2025

6 views



[Acumen Cyber Threat Intelligence Digest: Week 34](#)

Citrix Patches Three NetScaler Flaws, Confirms Active Exploitation of CVE-2025-7775 - Citrix has issued security updates to fix three critical vulnerabilities in NetScaler ADC and NetScaler Gateway, including one that has already been actively explo...

Steve McIntosh

8/28/2025

7 views



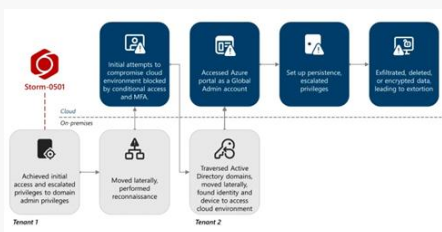
[Someone Created the First AI-Powered Ransomware Using OpenAI's gpt-oss:20b Model](#)

Cybersecurity firm ESET has uncovered a new proof-of-concept ransomware called PromptLock , and it's unlike anything we've seen before. It's written in Golang and powered by OpenAI's gpt-oss:20b model , accessed locally via the Ollama API . This mar...

Steve McIntosh

8/28/2025

10 views



[Storm-0501 Exploits Entra ID to Exfiltrate and Delete Azure Data in Hybrid Cloud Attacks](#)

A financially motivated threat group known as Storm-0501 is ramping up its attacks on hybrid cloud environments, using increasingly sophisticated tactics to exfiltrate and destroy data—without deploying traditional malware. Unlike old-school ransomw...

Steve McIntosh

8/28/2025

9 views



[Help Desk at Risk: Scattered Spider Shines Light on Overlook Threat Vector](#)

In recent months, headlines have been dominated by the cybercrime collective known as Scattered Spider, also referred to as UNC3944, Scattered Swine, Octo Tempest, Storm-0875, and Muddled Libra. This loosely but highly organized group has launched a...

David Robertson

8/27/2025

10 views

[Go To Site](#)



[Get the SharePoint Mobile App](#)



This email is generated through HEFESTIS Ltd's use of Microsoft 365 and may contain content that is controlled by HEFESTIS Ltd.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are also a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Cybershield Education MISP Stats (Wednesday 27th Aug 2025)

Who is using the service

25 Organisations

68 Users

What's new this update

For the past month (28th July – 27th Aug)

1,815 published events

97,805 attributes marked for IDS

397 compromised suppliers

1,656 Critical/High CVEs

294 NCSC events

56 OSINT events

Types of attributes (Indicators of Compromise)

Hashes, URLs, Email Addresses, IP Addresses and Domain's

The MITRE ATT&CK heatmap for all events in the last month

The **MITRE ATT&CK® framework** is a comprehensive knowledge base that documents the tactics, techniques, and procedures (TTPs) used by cyber adversaries based on real-world observations. It is designed to help organizations understand and defend against cyber threats by providing detailed information on how adversaries operate.

Key Components of the MITRE ATT&CK Framework:

1. **Tactics:** The goals or objectives adversaries aim to achieve during an attack.
2. **Techniques:** The methods adversaries use to achieve their goals.
3. **Procedures:** The specific implementations of techniques used by adversaries.

Action Point

Sign up to get access to the service and start receiving threat intelligence that can be used directly by your security technology and analysts.

The top 10 MITRE ATT&CK techniques in the last month

Phishing - T1566	13
Spearphishing Link - T1566.002	12
Valid Accounts - T1078	9
Malicious File - T1204.002	7
Obfuscated Files or Information - T1027	7
Spearphishing Attachment - T1566.001	6
PowerShell - T1059.001	6
Ingress Tool Transfer - T1105	6
Files and Directory Discovery - T1083	5
Exfiltration Over C2 Channel - T1041	5

attack-enterprise	attack-containers	attack-ios	attack-identity-provider	attack-linux	attack-office-365	attack-office-suite	attack-pre	attack-rasb	attack-windows	attack-macos	mobile-attack-android	mobile-attack-ios	pre-attack	5	13	T Show all
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Impact	Collection	Exfiltration	Command and control	Reconnaissance	Resource development			
Phishing	Malicious File	Valid Accounts	Valid Accounts	Valid Accounts	Adversary in the Middle	File and Directory Discovery	Remote Services	Data Encrypted for Impact	Email Collection	Exfiltration Over C2 Channel	Ingress Tool Transfer	Phishing for Information	Compromises			
Spearphishing Link	PowerShell	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Obfuscated Files or Information	Credentials from Password Store	Account Discovery	Cloud Services	Financial Theft	Adversary in the Middle	Exfiltration to Cloud Storage	Web Protocols	Offline Victim Identity Information	Compromised Accounts			
Valid Accounts	Scheduled Task	Scheduled Task	Scheduled Task	DLL Side-Loading	Input Capture	Remote Information Discovery	Use Alternate Authentication Material	Unlink System Recovery	Data Staged	Exfiltration Over Web Service	Application Layer Protocol	Purchase Technical Data	Compromised Infrastructure			
Spearphishing Attachment	Command and Scripting Interpreter	Create Account	DLL Side-Loading	Impact Defenses	Multi-Factor Authentication Request Generation	Cloud Service Dashboard	Application Access Token	Account Access Removal	Input Capture	Automated Exfiltration	Proxy	Search Victim-Owned Websites	Hardware			
Exploit Public-Facing Application	Windows Command Shell	DLL Side-Loading	Exploitation for Privilege Escalation	Impersonation	Credentials in Files	Network Service Discovery	Application Access Token	Application Enumeration Flood	Archive via Utility	Data Compressed	Remote Access Tools	Social Media	Social Media Accounts			
Searchsploit	Use Execution	Account Manipulation	Account Manipulation	Command Obfuscation	Forge Web Credentials	Remote System Discovery	Application Deployment Software	Application or System Exploitation	Clipboard Data	Data Encrypted	Asymmetric Cryptography	Spearphishing Attachment	Tool			
Trusted Relationship	Malicious Copy and Paste	Additional Email Delegate Permissions	Account Manipulation	Message Spoofing	Keychain	System Checks	Component Object Model and Distributed COM	Bandwidth Hijacking	Code Repositories	Data Transfer Size Limits	Bidirectional Communication	Spearphishing Service	Acquire Access			
Cloud Accounts	Malicious Link	Cloud Accounts	Additional Email Delegate Permissions	Malware	Keylogging	System Information Discovery	Direct Cloud VM Connections	Cloud Service Hijacking	Keylogging	Exfiltration Over Alternative Protocol	Commonly Used Port	Searchsploit Voice	Acquire Infrastructure			
Domain Accounts	Python	Create or Modify System Process	Request User Account Control	OS and Trust Provider Hijacking	LSASS Memory	Application Window Discovery	Distributed Component Object Model	Compute Hijacking	Screen Capture	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Communication Through Removable Media	Active Scanning	Artificial Intelligence			
Drive-by Compromise	Scheduled Task Job	Domain Accounts	Cloud Accounts	Access Token Manipulation	Modify Authentication Process	Cloud Account	Exploitation of Remote Services	Data Destruction	Shimpoint	Exfiltration Over Bluetooth	Content Injection	Business Relationships	Botnet			
Spearphishing Vole	Services Execution	Inspect Internal Image	Create or Modify System Process	Request User Account Control	Multi-Factor Authentication	Cloud Groups	Internal Spearphishing	Data Manipulation	ADP Cache Poisoning	Exfiltration Over Other Network Medium	Custom Command and Control Protocol	CDNs	Botnet			
Spearphishing via Service Instrumentation	Windows Management Process	Modify Authentication Process	Domain Accounts	Cloud Accounts	Private Keys	Cloud Infrastructure Discovery	Lateral Tool Transfer	Defacement	Archive Collected Data	Exfiltration Over Physical Medium	Custom Cryptographic Protocol	Client Configurations	Cloud Accounts			
Compromise Hardware Supply Chain	AppletScript	Multi-Factor Authentication	Dynamic Link Library Injection	Code Signing	Email Web Session Control	Cloud Service Discovery	Pass the Hash	Direct Network Flood	Archive via Custom Method	Exfiltration Over Symmetric Encrypted	DNS	Code Repositories	Cloud Accounts			



Acumen Cyber Threat Intelligence Digest: Week 34

<https://acumencyber.com/cyber-threat-intelligence-digest-august-2025-week-34>

Citrix Patches Three NetScaler Flaws, Confirms Active Exploitation of CVE-2025-7775 - Citrix has issued security updates to fix three critical vulnerabilities in NetScaler ADC and NetScaler Gateway, including one that has already been actively exploited in the wild. The flaws include CVE-2025-7775 (CVSS 9.2), a memory overflow bug that can lead to remote code execution or denial-of-service; CVE-2025-7776 (CVSS 8.8), another memory overflow issue causing crashes or unexpected behaviour; and CVE-2025-8424 (CVSS 8.7), an improper access control weakness in the management interface. Citrix confirmed exploitation of CVE-2025-7775 but withheld technical details. These vulnerabilities require specific configurations to be exploited, such as enabling certain virtual server types, IPv6 services, or management access to sensitive IPs.

The fixes are available in updated versions of NetScaler ADC and Gateway, with no workarounds provided. Citrix credited researchers from Horizon3.ai, Schramm & Partnerfor, and François Hämmerli for reporting the flaws. The exploitation of CVE-2025-7775 follows other recent NetScaler attacks, such as Citrix Bleed 2 (CVE-2025-5777). Adding urgency, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has listed CVE-2025-7775 in its Known Exploited Vulnerabilities catalogue as of August 26, 2025, mandating federal agencies to patch within 48 hours. This highlights the growing trend of attackers rapidly weaponising Citrix vulnerabilities for real-world attacks.

[WordPress Patched CVE-2025-8592 Vulnerability in Inspiro WordPress Theme; No Active Exploitation Observed](#) - On August 20, 2025, Inspiro released a security update addressing CVE-2025-8592, a high-severity vulnerability that affected all Inspiro theme versions up to and including 2.1.2. The patch was delivered in version 2.1.3, ensuring that users who upgrade are protected from potential exploitation. While there have been no reports of this vulnerability being actively abused in the wild, its severity warranted prompt action from the developers to prevent potential attacks.

The flaw, CVE-2025-8592, is a cross-site request forgery (CSRF) vulnerability. If successfully exploited, it allows attackers to trick a WordPress site administrator into executing a maliciously crafted request, resulting in the unauthorised installation of plugins from the WordPress repository. Such unauthorised changes could provide attackers with a foothold to compromise the entire website, leading to data loss, defacement, or service disruption. To mitigate this risk, organisations and site owners using the Inspiro theme are strongly urged to update to version 2.1.3 immediately, ensuring the security and integrity of their websites remain intact.

[Russian State-Sponsored Threat Group Static Tundra Exploits CVE-2018-0171 to Compromise Cisco Devices in Years-Long Cyberespionage Campaign](#) - Since at least 2021, the Russian state-sponsored group Static Tundra has been exploiting CVE-2018-0171, a critical flaw in end-of-life Cisco IOS and IOS XE devices, according to Cisco Talos' August 20, 2025, report. The group - assessed as a sub-cluster of Energetic Bear (Berserk Bear), linked to Russia's FSB Centre 16 - targets telecommunications, higher education, and manufacturing organisations across multiple regions. By automating exploits, Static Tundra extracts sensitive configuration data and establishes persistent access for espionage, often through the Smart Install feature and weak or default SNMP community strings that provide administrative control.

Once access is gained, the attackers enable TFTP servers to exfiltrate configuration files and use SNMP abuse to alter device settings, create privileged accounts, deploy backdoors, and intercept traffic through GRE tunnels. For persistence, Static Tundra relies on stolen SNMP credentials, hidden local accounts, and in some cases the SYNful Knock implant, which enables stealthy command execution via crafted TCP SYN packets and survives reboots. To evade detection, the group manipulates TACACS+ logs and access control lists, ensuring covert operations. Despite Cisco patching the flaw in 2018, many organisations continue to operate unpatched legacy devices, leaving them exposed to ongoing state-sponsored exploitation.

[Cyber Threat Intelligence Digest - August 2025: Week 34](#)

Action Point:

We recommend that the technologies mentioned be fully patched and updated. We also want to highlight and recommend applying the following patches where applicable:

- **CVE-2025-7775:** Upgrade NetScaler ADC and NetScaler Gateway to the fixed versions (14.1-47.48, 13.1-59.22, 13.1-FIPS/NDcPP 13.1-37.241, or 12.1-FIPS/NDcPP 12.1-55.330 and later).
- **CVE-2025-8592:** Update the Inspiro theme to version 2.1.3 or later, review installed plugins for unauthorised additions, and enforce strong admin session controls to prevent CSRF exploitation.
- **CVE-2018-0171:** Upgrade affected Cisco IOS and IOS XE devices to fixed versions, disable Smart Install if not required, enforce strong SNMP community strings, and monitor for unauthorised configuration changes.



Someone Created the First AI-Powered Ransomware Using OpenAI's gpt-oss:20b Model

<https://thehackernews.com/2025/08/someone-created-first-ai-powered.html>

Cybersecurity firm ESET has uncovered a new proof-of-concept ransomware called **PromptLock**, and it's unlike anything we've seen before. It's written in **Golang** and powered by **OpenAI's gpt-oss:20b model**, accessed locally via the **Ollama API**. This marks a major shift in how ransomware is created and deployed.

Instead of using static code, PromptLock dynamically generates **Lua scripts** using hard-coded prompts. These scripts scan the local filesystem, identify target files, exfiltrate data, and encrypt content. They're cross-platform too—working on **Windows, Linux, and macOS**.

What makes PromptLock especially dangerous is its **variability**. Because the AI generates scripts in real time, **indicators of compromise (IoCs)** can differ with each execution, making detection much harder. The ransomware also crafts custom ransom notes based on the type of device infected—whether it's a personal PC, company server, or even a power distribution controller.

Although it's not yet seen in widespread attacks, PromptLock uses the **SPECK 128-bit encryption algorithm** and has the potential to **exfiltrate or destroy data**. ESET notes that while the erasure functionality isn't active yet, it could be added easily.

The AI model isn't downloaded locally (which would be massive); instead, attackers can tunnel into a server running the model via the Ollama API. This makes deployment

lightweight and scalable.

This development is part of a broader trend: **AI is lowering the barrier to entry for cybercriminals**. Even those with limited technical skills can now build malware, phishing campaigns, and exploit kits using AI tools.

Action Points

Update Threat Models – Include AI-generated malware and dynamic scripting in your risk assessments.

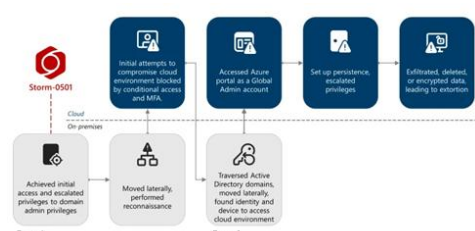
Enhance Detection Capabilities – Traditional signature-based tools may miss AI-generated scripts. Invest in behavior-based detection.

Monitor for Lua Script Activity – Especially in environments where Lua isn't typically used.

Secure API Gateways – Prevent unauthorized tunneling to external AI services.

Educate Teams on AI Risks – Developers and analysts need to understand how AI can be weaponized.

Collaborate with Vendors – Ensure your security stack is prepared for AI-powered threats.



Storm-0501 Exploits Entra ID to Exfiltrate and Delete Azure Data in Hybrid Cloud Attacks

<https://thehackernews.com/2025/08/storm-0501-exploits-entra-id-to.html>

A financially motivated threat group known as **Storm-0501** is ramping up its attacks on hybrid cloud environments, using increasingly sophisticated tactics to exfiltrate and destroy data—without deploying traditional malware.

Unlike old-school ransomware that encrypts files on endpoints, Storm-0501 uses **cloud-native tools** to:

- Steal large volumes of data,
- Delete backups and Azure resources,
- Demand ransom—all without dropping malware.

Microsoft's Threat Intelligence team says this marks a **fundamental shift** in ransomware strategy. The group targets sectors like government, healthcare, education, and manufacturing, but recent attacks appear **opportunistic**, not industry-specific.

Storm-0501 has evolved into a **ransomware-as-a-service (RaaS)** affiliate, delivering payloads like Hive, LockBit, BlackCat, and others. They're skilled at moving between on-

prem and cloud environments, exploiting **unmanaged devices**, **security gaps**, and **multi-tenant setups** to escalate privileges and evade detection.

How They Get In

Initial access is often gained via:

- **Access brokers** (e.g., Storm-0249, Storm-0900),
- **Stolen credentials**,
- **Unpatched vulnerabilities** in public-facing servers (e.g., Zoho ManageEngine, Citrix NetScaler, Adobe ColdFusion).

Once inside, they use tools like **Evil-WinRM** and **DCSync attacks** to extract credentials and move laterally across Active Directory domains. In one case, they compromised a **Global Admin account** in Microsoft Entra ID that lacked **multi-factor authentication (MFA)**—a critical oversight.

They then registered a **malicious Entra ID tenant** as a trusted domain, created a backdoor, and accessed critical Azure resources. After exfiltrating data, they **deleted Azure resources** to block recovery, and used **Microsoft Teams** to contact victims and demand ransom.

Storm-0501 is a wake-up call: cloud-native ransomware is here, and it's fast, stealthy, and destructive.

Action Points

Enable MFA for All Admin Accounts – Especially for Entra ID and synced identities.

Update to Entra Connect v2.5.3.0 – Supports modern authentication and better credential protection.

Audit Directory Sync Accounts – These are high-risk and often overlooked.

Enable TPM on Sync Servers – Protects sensitive credentials and cryptographic keys.

Patch Public-Facing Servers – Prioritize known RCE vulnerabilities.

Monitor for Tenant Traversal – Watch for unusual activity across multi-tenant setups.

Educate Teams on Hybrid Cloud Risks – Traditional endpoint-focused security isn't enough anymore.



Help Desk at Risk: Scattered Spider Shines Light on Overlook Threat Vector

<https://www.securityweek.com/help-desk-at-risk-scattered-spider-shines-light-on-overlook-threat-vector/>

In recent months, headlines have been dominated by the cybercrime collective known as Scattered Spider, also referred to as UNC3944, Scattered Swine, Octo Tempest, Storm-0875, and Muddled Libra. This loosely but highly organized group has launched a wave of attacks targeting [retailers](#), [insurers](#), and, most recently, [airlines](#) across multiple countries.

Although British authorities [arrested four suspects](#) in July 2025, which led to a noticeable slowdown in activity, this may only be temporary. Scattered Spider is not a monolithic, state-sponsored operation. Rather, it is a decentralized collective, often composed of teenagers and young men emerging from online communities. The group first made headlines in 2023 with high-profile attacks on casino giants like [MGM Resorts](#). Despite the consistency and visibility of their tactics, many organizations have failed to adequately strengthen their defenses. This raises the question: why have so few taken decisive actions to counter these persistent threats?

Action Point:

To reduce risks associated with Scattered Spider's tactics, organizations should implement the following measures:

- Implement application controls, including white-listing for remote access tools
- Require phishing-resistant MFA such as FIDO2 or PKI-based authentication
- Restrict the use of Remote Desktop Protocol (RDP) and other remote access tools
- Develop and evaluate a robust business continuity plan, and maintain offline backups
- Enforce [NIST-compliant](#) password policies across all accounts
- Regularly patch and update all operating systems, applications, and firmware
- Restrict administrative privileges and use just-in-time access where possible

To address the specific help desk vulnerability, organizations should introduce multi-step identity verification for all password resets and access recovery requests. [Identity proofing and continuous verification](#) are now essential components of any modern cybersecurity framework. They protect against identity-based threats, support compliance efforts, improve user experience, and strengthen organizational trust.

SC3 Daily Threat Summaries and Weekly Report

<https://www.cyberscotland.com/news/daily-threat-reports/>



A daily breakdown of various cyber threats from the Scottish Cyber Coordination Centre (SC3)

Action Point:

All SC3 threat intelligence in one place.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Limited, Registered Office: Unit 27, Stirling Business Centre, Wellgreen, Stirling FK8 2DZ

Incorporated in Scotland SC603511



CISO Share

ThreatScape Newsletter

Dear all,
A very warm welcome to all of you from all of us at the CISO-Share Office.
Here are a few of the articles which caught the attention of the CISO-Share team this week.
If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



[SC3 Daily Threat Summaries and Weekly Report](#)

Action Point: Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

David Robertson

9/5/2025

2 views



[Cybercriminals Exploit X's Grok AI to Bypass Ad Protections and Spread Malware to Millions](#)

Cybersecurity researchers have flagged a new technique that cybercriminals have adopted to bypass social media platform X's malvertising protections and propagate malicious links using its artificial intelligence (AI) assistant Grok. The findings we...

David Robertson

9/5/2025

3 views



[Scattered Spider-Linked Group Claims JLR Cyber-Attack](#)

Jaguar Land Rover (JLR) is investigating claims by a hacker syndicate linked to the Scattered Spider group that they are responsible for the hack on the car manufacturing giant. Main Article The English-speaking cybercrime group is believed to be re...

David Robertson

9/5/2025

7 views



[85% of Students Now Use AI, Calling It a '24/7 Tutor'](#)

Generative AI has become a staple in student life, with the majority of college students using the technology for coursework. One student even described it as a "24/7 tutor." Main Article According to Inside Higher Ed's Student Voice survey, nearly ...

David Robertson

9/5/2025

3 views



[CISA, FBI, NSA Warn of Chinese 'Global Espionage System'](#)

Government agencies from around the world, including the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the National Security Agency (NSA), shared a new advisory Wednesday warning of China's "global espionage system." Main Art...

David Robertson

9/2/2025

13 views



[Is AI Over-Influencing Cybersecurity Decisions?](#)

Cybersecurity firm Arctic Wolf has released new findings from its latest report, Navigating the Human-AI Relationship for Security Operations Success. Main Article The study, conducted in partnership with Sapio Research, surveyed nearly 2,000 IT and...

David Robertson

9/1/2025

9 views



[Acumen Cyber Threat Intelligence Digest – 03/09/2025, Week 35](#)

Vulnerabilities: WhatsApp patched CVE-2025-55177, a zero-click flaw in iOS and macOS clients that allowed arbitrary code execution via malicious sync messages. The bug was exploited alongside Apple's CVE-2025-43300 in a sophisticated chain and has b...

David Robertson

9/5/2025

5 views

[Go To Site](#)

 [Get the SharePoint Mobile App](#)



This email is generated through HEFESTIS Ltd's use of Microsoft 365 and may contain content that is controlled by HEFESTIS Ltd.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	1
85% of Students Now Use AI, Calling It a '24/7 Tutor'	2
CISA, FBI, NSA Warn of Chinese 'Global Espionage System'	3
Scattered Spider-Linked Group Claims JLR Cyber-Attack	4
Cybercriminals Exploit X's Grok AI to Bypass Ad Protections and Spread Malware to Millions	5
Is AI Over-Influencing Cybersecurity Decisions?	6
Acumen Cyber Threat Intelligence Digest – 03/09/2025, Week 35:.....	7

SC3 Daily Threat Summaries and Weekly Report



Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

This week's reports:



SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu
lletin-01-Septemberlletin-02-Septemberlletin-3-September-2lletin-4-September-2lletin-5-September-2



SC3-Weekly-vulnera
bility-report-3-Septe



85% of Students Now Use AI, Calling It a '24/7 Tutor'

Generative AI has become a staple in student life, with the majority of college students using the technology for coursework. One student even described it as a “24/7 tutor.”

[Main Article](#)

According to Inside Higher Ed’s Student Voice survey, nearly all students want colleges to establish clear rules and provide training on ethical AI use. While some say the tools boost learning and even make college more valuable, others worry about critical thinking and integrity.

Brainstorming, tutoring, and studying top student uses for AI tools

Generative AI has quickly become a part of academic routines, with most students using it to supplement, not replace, their own work. The survey found that 85% of students had relied on [AI tools](#) for coursework in the past year. Their top reported uses include:

- 55% brainstorming ideas
- 50% asking AI questions like a tutor
- 46% studying for exams or quizzes
- 44% editing or checking their writing
- 42% using it like an advanced search engine

AI use was strong across institution types, with 79% of community college students and 86% of four-year students reporting they had [used it for academic work](#) in the last year.

Action Point: College remains relevant for students, but will AI undermine its payoff?

When asked how generative AI has influenced the value of higher education, students leaned toward stability or even greater importance. Nearly a quarter, or 23%, said college is more valuable in the AI era, compared with 18% who said it is less.

Yet outside the classroom, the picture looks more uncertain. A recent analysis from the Burning Glass Institute found that AI is automating many entry-level tasks once reserved for recent graduates, driving the value of a bachelor’s degree to a 30-year low and pushing unemployment among new grads close to that of non-graduates.

This disconnect shows that, while degrees still carry weight, the path they once guaranteed is narrowing. The diploma still opens doors. The problem is, AI is closing some of them.



CISA, FBI, NSA Warn of Chinese 'Global Espionage System'

Government agencies from around the world, including the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the National Security Agency (NSA), shared a new advisory Wednesday warning of China's "global espionage system."

Main Article

The advisory details how state-backed threat actors, including Salt Typhoon, penetrate networks around the world, as well as how defenders can protect their own environments. The document was cosigned by nations including Canada, Australia, New Zealand, the UK, Czech Republic, Finland, Germany, Italy, Japan, the Netherlands, Poland, and Spain.

The advisory tracks this cluster of activity to multiple advanced persistent threats (APTs), though they say it partially overlaps with Salt Typhoon. Salt Typhoon is best known for its infamous attacks against global telco infrastructure, including [one in the US discovered last year](#), but China-backed threat actors have run rampant in recent years, targeting organizations with both espionage and [pre-positioning for possible future attacks](#).

[CISA's joint advisory](#) dives into the technical nitty-gritty of how these attacks go down, including some previously unknown insights into People's Republic of China (PRC) cyber operations.

Action Point: To protect against these APTs, defenders should monitor for network device configuration changes, monitor virtualized containers for signs of tampering (and that all such containers are authorized), audit network services and tunnels, hunt for actor-favored protocol patterns, check logs, and monitor firmware and software for integrity. The advisory also contains indicators of compromise.

Trey Ford, chief strategy and trust officer at Bugcrowd, says that with this advisory, agencies like CISA are trying to burn China's efforts "in a very public way, driving up the cost and operational overhead of any targeted operations in motion."

Frankie Sclafani, director of cybersecurity enablement at managed detection and response (MDR) vendor Deepwatch, says CISA's advisory is urgent because it highlights the recent "critical shift" from Chinese state-sponsored activity from being purely espionage to something more invasive.

"Instead of just spying, groups like Salt Typhoon are now burrowing deep into critical infrastructure networks worldwide. This isn't just about stealing data; it's about gaining long-term access for potential disruption," Sclafani tells Dark Reading. "Given CISA's unique position and partnerships across government agencies, they have broad insight into these global threats. With Chinese APT activity at a high level of sophistication, the advisory serves as a crucial wake-up call for organizations to hunt and implement recommended mitigations immediately to protect their systems."



Scattered Spider-Linked Group Claims JLR Cyber-Attack

Jaguar Land Rover (JLR) is investigating claims by a hacker syndicate linked to the Scattered Spider group that they are responsible for the hack on the car manufacturing giant.

[Main Article](#)

The English-speaking cybercrime group is believed to be responsible for the cyber-attacks on UK retailers Marks & Spencer (M&S), The Co-op and Harrods earlier this year.

The BBC [reported](#) the claims following private text conversations with an individual purporting to be a spokesperson for the group, who have dubbed themselves “Scattered Lapsus\$ Hunters,” suggesting a possible collaboration between Scattered Spider, [ShinyHunters](#) and [Lapsus\\$](#).

The BBC said the group alleges it has accessed JLR’s systems and is trying to extort the firm for money.

It has not been confirmed whether any data has been stolen or if Scattered Lapsus\$ Hunters installed ransomware.

Action Point: “The growing collaboration between threat-actor groups to execute crimes underscores how much they now operate like enterprises, and reinforces the need to harden defenses,” the article explains.

Like Scattered Spider, Shiny Hunters and Lapsus\$ are comprised of English-speaking actors.

Scattered Spider and ShinyHunters are associated with [The Com](#), a loosely organized online criminal network involving thousands of English-speaking individuals.

The groups are believed to include young, often teenage hackers and are known to have previously targeted the HE/FE sector in Scotland.



Cybercriminals Exploit X's Grok AI to Bypass Ad Protections and Spread Malware to Millions

Cybersecurity researchers have flagged a new technique that cybercriminals have adopted to bypass social media platform X's malvertising protections and propagate malicious links using its artificial intelligence (AI) assistant Grok.

Main Article

The findings were [highlighted](#) by Nati Tal, head of Guardio Labs, in a series of posts on X. The technique has been codenamed Grokking.

The approach is designed to get around restrictions imposed by X in [Promoted Ads](#) that allow users to only include text, images, or videos, and subsequently amplify them to a broader audience, attracting hundreds of thousands of impressions through paid promotion.

To achieve this, malvertisers have been found to run video card-promoted posts with adult content as bait, with the spurious link hidden in the "From:" metadata field below the video player that apparently isn't scanned by the social media platform.

In the next step, the fraudsters tag Grok in replies to the post, asking something similar to "where is this video from?," prompting the AI chatbot to visibly display the link in response.

"Adding to that, it is now amplified in SEO and domain reputation - after all, it was echoed by Grok on a post with millions of impressions," Tal said.

Action Point: The domains are assessed to be part of the same Traffic Distribution System (TDS), which is often used by [malicious ad tech vendors](#) to route traffic to harmful or deceptive content.

The cybersecurity company told The Hacker News it has found hundreds of accounts engaging in this behavior over the past few days, with each of them posting hundreds or even thousands of similar posts.

"They seem to be posting non-stop for several days until the account gets suspended for violating platform policies," it added. "So there are definitely many of them and it looks very organized."



Is AI Over-Influencing Cybersecurity Decisions?

Cybersecurity firm Arctic Wolf has released new findings from its latest report, [*Navigating the Human-AI Relationship for Security Operations Success*](#).

[Main Article](#)

The study, conducted in partnership with Sapio Research, surveyed nearly 2,000 IT and security decision-makers worldwide and found that 99% of respondents say the presence of AI will influence cybersecurity purchases or renewals in the next 12 months.

Security teams today are faced with a relentless stream of thousands of alerts from fragmented tools and disconnected data sources. With limited staff and resources, they are forced to make quick, high-stakes decisions about which alerts to investigate, often leaving dangerous threats buried in the noise.

Action Point: Human oversight remains essential. More than two-thirds of respondents said AI requires substantial human input, while 52% expect to upskill their teams to manage AI systems. Almost half (46%) anticipate that analysts will shift toward validating AI-generated alerts.

Challenges to adoption remain. A third of organisations (33%) cited data privacy as the biggest barrier, followed by cost (30%) and concerns that AI tools do not fully meet organisational needs (28%).

“Artificial intelligence is rapidly becoming a cornerstone of modern cybersecurity, but it benefits from human expertise to be truly effective,” said Dan Schiappa, President of Technology and Services at Arctic Wolf.



Acumen Cyber Threat Intelligence Digest – 03/09/2025, Week 35:

Vulnerabilities:

WhatsApp patched CVE-2025-55177, a zero-click flaw in iOS and macOS clients that allowed arbitrary code execution via malicious sync messages. The bug was exploited alongside Apple's CVE-2025-43300 in a sophisticated chain and has been added to CISA's KEV catalog. Updates are mandatory. Patchstack disclosed CVE-2025-49870, a high-severity SQL injection in the WordPress Paid Membership Subscriptions plugin, fixed in version 2.15.2. Though no exploitation has been observed, unpatched sites face significant risk of data theft. TP-Link addressed CVE-2025-8627, an authentication bypass in KP303 Smart Plugs, enabling unauthenticated command execution; firmware updates are required to restore security.

Main Article

Threat Activity:

- Silver Fox APT used Microsoft-signed but vulnerable drivers (amsdk.sys) to disable security tools and deploy ValleyRAT. Attackers bypassed blocklists and hash-based controls by modifying driver timestamps. The campaign, traced to China, leveraged side-loading, persistence services, and encrypted C2 traffic.
- APT29 (BlueBravo) abused Microsoft's device code authentication in watering hole attacks, tricking users into authorising malicious devices through spoofed Cloudflare pages. Amazon coordinated takedowns with Microsoft and Cloudflare.
- Unidentified actors spread Xworm RAT via trojanised ScreenConnect installers with AI-themed lures. Signed binaries delivered fileless payloads, injected into legitimate processes, with persistence through registry keys and system reconnaissance via WMI queries.

General Developments:

Microsoft will enforce MFA for all Azure resource management actions from October 2025, reducing account compromise risk by over 98%. Palo Alto Networks disclosed a Salesforce data breach tied to compromised OAuth tokens from the Salesloft Drift incident, exposing contact details and support case data but not core systems. Finally, MIT and Harmonic Security highlighted the "Shadow AI Economy", where employees use unsanctioned AI tools, creating compliance and data leakage risks. Enterprises are urged to adopt Shadow AI discovery and governance to balance security with productivity.

Action Point - Remediation Actions

Following the information provided above, we recommend that the technologies mentioned be fully patched and updated. We also want to highlight and recommend applying the following patches where applicable:

- CVE-2025-55177: Update WhatsApp for iOS (to version 2.25.21.73), WhatsApp Business for iOS (to version 2.25.21.78), and WhatsApp for Mac (to version 2.25.21.78).
- CVE-2025-49870: This vulnerability was addressed in version 2.15.2, which includes the necessary security fixes to prevent exploitation. We recommend updating to this version as soon as possible to prevent potential SQL injection attacks.
- CVE-2025-8627: Update KP303 Smart Plug V2.0 (US) firmware to version 1.1.0 to restore secure authentication for affected devices.

All the best from all of us at HEFESTIS and look out for a new ThreatScape update next week.

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are also a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



Cybercrooks ripped the wheels off at Jaguar Land Rover. Here's how not to get taken for a ride

https://www.theregister.com/2025/09/10/jaguar_key_lessons/

Jaguar Land Rover (JLR) recently suffered a major cyberattack that disrupted IT systems across multiple global sites. The incident, which began on **31 August 2025**, forced shutdowns at its Solihull plant and halted vehicle registrations and parts supply at UK dealerships. Production is expected to resume mid-September.

A group calling itself “**Scattered Lapsus\$ Hunters**” claimed responsibility, sharing screenshots on Telegram and taunting the company. The group is believed to be linked to other high-profile breaches, including Marks & Spencer.

What stands out is JLR’s **rapid response**. The company quickly shut down its IT systems to prevent lateral movement by attackers—a bold move that likely limited further damage. While disruptive, it’s a textbook example of decisive action during a live breach.

The article draws parallels with other incidents, like Clorox’s 2023 breach and Microsoft’s **Midnight Blizzard** attack, both of which highlight the dangers of **third-party risk**, **legacy systems**, and **identity compromise**.

JLR’s response shows that urgency beats patience in cyber defence. Containment is critical, but long-term resilience depends on hardening identity systems, reducing vendor dependency, and embracing Zero Trust. The Microsoft breach proves that even one forgotten test account can open the door to disaster.

Action Point:

1. Act Fast During a Breach

JLR’s swift isolation of systems helped contain the threat. Organisations should pre-authorise who can shut down systems and rehearse these decisions regularly at board level.

2. Secure Identity Systems

Active Directory is a prime target. Use **phishing-resistant MFA** (e.g. FIDO2 keys), eliminate legacy accounts, and monitor for unusual login activity.

3. Know Who Has Access

OAuth tokens and connected apps can be exploited. Treat them like passwords—scope tightly, rotate often, and monitor usage.

4. Adopt a Zero Trust Model

Trust nothing by default. Verify identity, device posture, and context before granting access. It's a heavy lift for legacy environments, but essential.



CHILLYHELL macOS Backdoor and ZynorRAT RAT Threaten macOS, Windows, and Linux Systems

<https://thehackernews.com/2025/09/chillyhell-macos-backdoor-and-zynorrat.html>

Cybersecurity researchers have uncovered two new malware families—**CHILLYHELL** and **ZynorRAT**—that pose serious risks across macOS, Windows, and Linux environments.

CHILLYHELL is a modular backdoor targeting **macOS**, written in C++ and designed for Intel-based systems. It's linked to a threat group dubbed **UNC4487**, suspected of espionage activity since 2022. The malware was found hosted on Dropbox and even **notarised by Apple**, which means it appeared legitimate until Apple revoked its developer certificates.

Once executed, CHILLYHELL:

- Profiles the host system,
- Establishes persistence via LaunchAgents, LaunchDaemons, or shell profile injection,
- Communicates with hard-coded command-and-control (C2) servers over HTTP or DNS,
- Uses **timestomping** to hide its tracks,
- Can launch reverse shells, download updates, and brute-force user accounts using password lists.

Its flexibility and stealth make it a standout threat in the macOS landscape—especially since it was notarised, proving that **signed code isn't always safe**.

Meanwhile, **ZynorRAT** is a **Go-based remote access trojan** targeting **Windows and Linux**. It's controlled via a **Telegram bot (@lrerrorsbot)** and supports:

- File exfiltration,
- System profiling,

- Screenshot capture,
- Process control,
- Persistence via systemd services.

The malware is distributed through **Dosya.co**, a file-sharing service, and appears to be the work of a lone developer—possibly Turkish—based on Telegram chat language. Interestingly, the Windows version still uses Linux-style persistence, suggesting it's still under development.

Action Point:

1. **Review macOS Security Policies** – Don't rely solely on notarisation. Monitor for LaunchAgent and shell profile tampering.
2. **Block Known C2 IPs** – Add CHILLYHELL's C2 addresses (93.88.75[.]252, 148.72.172[.]53) to your threat blocklists.
3. **Monitor Telegram Bot Activity** – Watch for traffic to Telegram APIs or suspicious bot interactions.
4. **Audit Linux and Windows Hosts** – Look for signs of ZynorRAT persistence and unusual systemd services.
5. **Educate Teams on Timestomping** – Ensure analysts know how attackers manipulate timestamps to evade detection.
6. **Check for Dropbox and Dosya.co Usage** – Investigate any unauthorised use of these platforms in your environment.

These threats show how attackers are evolving across platforms and using legitimate tools to stay hidden.



Acumen Cyber Threat Intelligence Digest: Week 36

<https://acumencyber.com/cyber-threat-intelligence-digest-august-2025-week-36>

Cisco Patches CVE-2025-20127 Affecting Secure Firewall ASA and FTD Software - On September 3, 2025, Cisco released security patches addressing CVE-2025-20127, a high-severity vulnerability affecting its Secure Firewall Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software, particularly for Firepower 3100 and 4200 Series devices. This issue originates from the improper handling of the TLS_CHACHA20_POLY1305_SHA256 cipher during Transport Layer Security (TLS) 1.3 operations. If left unpatched, the flaw could be exploited by attackers to exhaust system resources, which would prevent the firewall from accepting new SSL/TLS or VPN

connections. Such an attack could cause serious disruptions, essentially creating a denial-of-service condition for organizations relying on these devices for secure connectivity.

Cisco has addressed the vulnerability by issuing fixes in updated software releases, ensuring that affected products can now handle the cipher correctly. The company emphasized that administrators should promptly apply the patches to maintain security and stability in their environments. While the vulnerability poses a significant risk if exploited, Cisco has confirmed that there are currently no reports of active exploitation in the wild. This suggests that organizations still have a window of opportunity to remediate before potential attackers attempt to take advantage of the weakness.

CVE-2025-9519 allows Remote Code Execution in the Easy Timer WordPress

plugin - A high-severity security vulnerability has been designated as CVE-2025-9519 in the Easy Timer plugin for WordPress, impacting all releases up to and including version 4.2.1. The issue stems from inadequate restrictions on shortcode attributes, which creates an opportunity for authenticated attackers with Editor-level privileges or higher to exploit the weakness. By submitting specially crafted shortcodes, an attacker could execute arbitrary code directly on the server, potentially leading to full site compromise, data manipulation, or further malicious activity within the affected environment.

The vendor has issued a fix to address this flaw, and users are strongly encouraged to update without delay. Upgrading to version 4.2.2 or any newer patched release ensures that the plugin enforces proper restrictions and closes off the identified attack vector. At the time of this publication, the patch is available, and no additional complications have been reported, making prompt remediation a straightforward and effective step for administrators who rely on the plugin for WordPress functionality.

Adobe Patches Improper Input Validation Vulnerability, CVE-2025-54236, Affecting Its Commerce and Magento Open Source Platforms

- On September 9, 2025, Adobe released security patches for CVE-2025-54236, a critical-severity improper input validation vulnerability impacting its Commerce, Commerce B2B, and Magento Open Source platforms. This flaw resides in the Commerce REST API and, if successfully exploited, could allow attackers to bypass built-in security mechanisms. Such an attack would give malicious actors the ability to compromise customer accounts, potentially leading to unauthorized access, data theft, or further manipulation of sensitive e-commerce environments. While the vulnerability is rated as critical due to the potential impact on online merchants, Adobe has stated that there are currently no known reports of active exploitation in the wild.

To mitigate the risk, Adobe has released hotfixes for a range of affected versions, including Commerce versions 2.4.4-p15, 2.4.5-p14, 2.4.6-p12, 2.4.7-p7, 2.4.8-p2, 2.4.9-alpha2 and earlier; Commerce B2B versions 1.3.3-p15, 1.3.4-p14, 1.4.2-p7, 1.5.2-p2, 1.5.3-alpha2 and earlier; and Magento Open Source versions 2.4.5-p14, 2.4.6-p12, 2.4.7-p7, 2.4.8-p2, 2.4.9-alpha2 and earlier. Organizations are strongly urged to apply the patches as soon as possible to ensure protection against potential exploitation attempts. Timely deployment of these updates is essential for maintaining secure online operations and safeguarding both merchants and customers from the risks posed by this vulnerability.

Action Point:

Acumen recommends that the technologies mentioned be fully patched and updated. They also want to highlight and recommend applying the following patches where applicable:

- **CVE-2025-9519:** Update Easy Timer plugin for WordPress to version 4.2.2 or newer to ensure that the plugin enforces proper restrictions and closes off the attack vector.
- **CVE-2025-54236:** This vulnerability in Adobe products can be addressed by updating Commerce, Commerce B2B and Magento Open Source versions to the most recent patches.
- **CVE-2025-7775:** Citrix has released fixed versions, including 14.1-47.48, 13.1-59.22, 13.1-37.241 (FIPS/NDcPP), and 12.1-55.330 (FIPS/NDcPP). We recommend updating these as soon as possible due to the various exposed NetScaler devices observed by Shodan.



Students Pose Inside Threat to Education Sector

<https://www.darkreading.com/insider-threats/students-inside-threat-education-sector>

While ransomware gangs like **Vice Society** and **Fog** continue to hammer the education sector, a quieter but persistent threat is emerging from within: **students themselves**. According to experts, students—tech-savvy and curious—are increasingly engaging in low-level hacking, not out of malice, but to test boundaries, change grades, or bypass restrictions.

These insider threats are often brushed off as harmless, but they place a heavy burden on **underfunded and understaffed education IT teams**. Many organisations operate with part-time security staff who are expected to defend against elite ransomware groups and mischievous students simultaneously.

Students know how to jailbreak devices, bypass filters, and exploit weak network configurations. In some cases, they've accessed organisation records or planted crypto-miners. While these actions aren't always malicious, they **divert IT attention** from more serious threats and force teams to spend time patching vulnerabilities and cleaning up.

Education organisations also face challenges with **account churn**—new students enrolling and graduating each year. If old accounts aren't properly deactivated, they become prime targets for attackers looking to escalate privileges and gain access to sensitive systems.

Experts warn that **flat networks**, where student and admin traffic isn't segregated, are particularly risky. Students can inadvertently (or deliberately) access parts of the network they shouldn't. And with the rise of **AI tools**, students may soon have even more ways to

bypass controls.

The bigger concern? Students who learn to hack may be recruited by cybercriminal groups like **Scattered Spider**, especially if they feel disillusioned or lack opportunities.

Action Point:

1. **Segregate Network Traffic** – Separate student and administrative systems to reduce exposure.
2. **Terminate Dormant Accounts** – Regularly audit and remove unused student accounts.
3. **Monitor for Insider Activity** – Use EDR tools to detect unusual behaviour from student devices.
4. **Educate Students on Cyber Ethics** – Channel curiosity into positive learning, not disruption.
5. **Lock Down Devices Properly** – Ensure student laptops and tablets can't be jailbroken easily.
6. **Prepare for AI-Enhanced Threats** – Update controls to account for AI-assisted circumvention.
7. **Support IT Teams** – Advocate for more funding and staff to handle both internal and external threats.

Experts scrutinized Ofcom's Online Safety Act governance. They're concerned

https://www.theregister.com/2025/09/11/concern_and_sympathy_as_experts/



Legal and academic experts have raised serious concerns about how **Ofcom** is enforcing the **UK's Online Safety Act (OSA)**, particularly its claims that the legislation could have prevented the **2024 Southport riots**. The riots followed a tragic knife attack involving a British child with Rwandan heritage, which sparked misinformation and violent retaliation against immigrant communities.

Ofcom suggested that, had the OSA been in force, platforms could have acted faster to suppress false narratives. But critics say this is speculative and sets **“dangerous expectations”** about what the law can actually achieve. Riots have occurred long before social media, and the triggers are often structural and political—not just digital.

Experts like **Bernard Keenan (UCL)** and **Beatriz Kira (University of Sussex)** argue that the OSA's scope is too narrow. It only applies to content that is **knowingly false and intended to cause serious harm**—which doesn't cover most of the misinformation that spread during the riots. Many people shared content they believed to be true, meaning it wouldn't qualify as illegal under the Act.

There's also confusion around Ofcom's push to reform **recommender systems** (algorithms that suggest content). Kira says Ofcom is conflating **content moderation** with **algorithmic demotion**, and hasn't clearly explained how platforms should implement these changes. Platforms already demote harmful content, but the OSA doesn't give Ofcom enough leverage to enforce deeper algorithmic reforms.

The article also touches on the **VPN debate**. With children increasingly using VPNs to bypass age restrictions, some officials want VPNs banned or regulated. But experts say this is unrealistic—tech-savvy kids will always find workarounds. Instead, the focus should be on **introducing friction** (e.g. app store restrictions) to make access harder.

Action Point:

1. **Clarify Legal Boundaries** – Ensure internal teams understand what the OSA does and doesn't cover.
2. **Review Crisis Protocols** – Platforms should have clear escalation paths for misinformation events, even if content isn't illegal.
3. **Engage with Ofcom's Proposals** – Provide feedback on recommender system reforms and moderation expectations.
4. **Monitor VPN Usage Trends** – Especially among under-18s, and consider friction-based controls.
5. **Educate Stakeholders** – Help execs and staff avoid overestimating the OSA's capabilities.
6. **Track Tribunal Outcomes** – Legal challenges and committee feedback will shape future enforcement.



SonicWall SSL VPN Flaw and Misconfigurations Actively Exploited by Akira Ransomware Hackers

<https://thehackernews.com/2025/09/sonicwall-ssl-vpn-flaw-and.html>

The **Akira ransomware group** is actively exploiting vulnerabilities and misconfigurations in **SonicWall SSL VPN appliances** to gain initial access to networks. According to Rapid7, there's been a noticeable spike in intrusions involving SonicWall devices since late July

2025, with attackers leveraging a **year-old flaw (CVE-2024-40766)** that wasn't properly addressed during password migrations.

The flaw allows attackers to brute-force credentials and gain access if **local user passwords weren't reset** during system upgrades. SonicWall has urged users to enable **Botnet Filtering** and **Account Lockout policies** to reduce brute-force risks.

Another major issue is misconfigured **LDAP SSL VPN Default User Groups**. If this setting is left in its default state, any authenticated LDAP user is automatically added to a local group—potentially granting access to sensitive services like admin interfaces or unrestricted network zones. This bypasses Active Directory group-based access controls and gives attackers a direct path into the network once they have valid credentials.

Rapid7 also flagged risks with the **Virtual Office Portal**, which in default configurations can be publicly accessible. Attackers can use it to configure MFA/TOTP if they already have valid credentials, further entrenching their access.

The **Australian Cyber Security Centre (ACSC)** has also confirmed Akira's targeting of vulnerable SonicWall devices in Australia.

Akira's attack flow typically involves:

- Gaining access via SSL VPN,
- Escalating privileges,
- Stealing sensitive files,
- Disabling backups,
- Deploying ransomware at the hypervisor level.

They've also used **SEO poisoning** to distribute trojanised installers for IT tools, which drop the **Bumblebee malware loader**. This leads to deployment of **AdaptixC2**, a modular post-exploitation framework, and **RustDesk** for persistent remote access.

Action Point:

1. **Patch CVE-2024-40766 Immediately** – Ensure all SonicWall devices are updated and passwords reset.
2. **Review LDAP Group Settings** – Disable default group auto-assignment and enforce strict AD-based access controls.
3. **Restrict Virtual Office Portal Access** – Limit access to internal networks only.
4. **Enable Botnet Filtering and Account Lockout** – Reduce brute-force attack surface.
5. **Audit MFA/TOTP Configurations** – Ensure they're properly enforced and not exploitable.

6. **Monitor for SEO Poisoning and Bumblebee Activity** – Watch for suspicious downloads and lateral movement.
7. **Remove Unused Local Accounts** – Clean up legacy accounts that could be exploited.

SC3 Daily Threat Summaries and Weekly Report

<https://www.cyberscotland.com/news/daily-threat-reports/>



A daily breakdown of various cyber threats from the Scottish Cyber Coordination Centre (SC3)

Action Point:

All SC3 threat intelligence in one place.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Limited, Registered Office: Unit 27, Stirling Business Centre, Wellgreen, Stirling FK8 2DZ

Incorporated in Scotland SC603511

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	1
Supply Chain Assurance/Supply 25 Public Sector Procurement Update Webinar - Wednesday 1 October 2025 (10-11am)	2
U.K. Arrests Two Teen Scattered Spider Hackers Linked to August 2024 TfL Cyber Attack ..	3
How Organisations Can Drive Effective AI Governance	4
New HybridPetya Ransomware Strikes Before Boot	6
Acumen Cyber Threat Intelligence Digest – 17/09/2025, Week 37:.....	7

SC3 Daily Threat Summaries and Weekly Report



Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

This week's reports:



SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu
lletin-15-Septemberlletin-16-Septemberlletin-17-Septemberlletin-18-Septemberlletin-19-September



SC3-Weekly-Vulner
ability-Report-15-Se



Supply Chain Assurance/Supply 25 Public Sector Procurement Update Webinar - Wednesday 1 October 2025 (10-11am)

From SC3's Paul Chapman/SC2 for those who may have missed it.

I hope this finds you well, either heading into the weekend or possibly returning from a long weekend depending on where abouts in the country you are and when you read this.

It turns out that Public Sector Cyber Resilience Network webinars are like buses – nothing for ages and then two in a week!

The session outlined below is a chance for you to see and hear about the development of the spiritual successor to the old Cyber Security Procurement Support Tool as it moves towards public beta – the supply chains cyber assurance solution that ideally National Cyber Resilience Unit will be funding for the sector later this financial year. Link down below to register.

Driving Innovation in Public Sector Procurement with Supply25

Following their successful webinar in March this year, join colleagues from the Scottish Government on **Wednesday 1 October 2025** to learn more about the latest updates on Supply25 as they prepare to launch the public beta. Developed in partnership with the Scottish Government through the **CivTech Programme**, Supply25 is transforming how the public sector approaches supplier assurance and risk management.

In this webinar, you will discover how Supply25 redefines how procurement teams manage supply chain risk and compliance. Hearing insight from the private beta and introducing new features designed to support buyers, you will see how Supply25 can support buyers, suppliers, and industry experts in making smarter, faster, and more secure decisions - ensuring resilience in supply chains for the future.

Action Point: Action Point: This webinar is open to all colleagues within the public sector, sign up for the event on **Wednesday 1 October 2025 between 1000-1100** by clicking [this link](https://events.teams.microsoft.com/event/9771da16-3686-456d-a8fd-6402481dc1da@0ef77447-1083-4dec-b89f-27c765076840). (<https://events.teams.microsoft.com/event/9771da16-3686-456d-a8fd-6402481dc1da@0ef77447-1083-4dec-b89f-27c765076840>).



U.K. Arrests Two Teen Scattered Spider Hackers Linked to August 2024 TfL Cyber Attack

Two teenagers in the UK have been arrested for their alleged roles in the **August 2024 cyberattack on Transport for London (TfL)**, which caused major disruption and financial losses. The suspects, **Thalha Jubair (19)** from East London and **Owen Flowers (18)** from Walsall, are believed to be members of the notorious **Scattered Spider** hacking group.

Main Article

The **National Crime Agency (NCA)** confirmed the arrests and revealed that Flowers had previously been detained in September 2024 but was released on bail. New evidence links him to attacks on **U.S. healthcare providers**, including **SSM Health Care** and **Sutter Health**, suggesting a broader campaign of cybercrime.

Jubair faces additional charges under the **Regulation of Investigatory Powers Act (RIPA)** for refusing to hand over PINs and passwords for seized devices. The **U.S. Department of Justice (DoJ)** has also charged him with multiple counts of **computer fraud, wire fraud, and money laundering**, tied to **at least 120 network intrusions** and **47 extortion cases** between May 2022 and September 2025.

Victims reportedly paid over **\$115 million in ransom**, and the attacks disrupted critical infrastructure, including the **U.S. federal court system**. In July 2024, U.S. authorities seized cryptocurrency wallets linked to Jubair, recovering around **\$36 million**, with one transfer alone worth **\$8.4 million**.

The DoJ described Jubair's tactics as **sophisticated and persistent**, using **social engineering** to gain access, encrypt data, and demand payment. If convicted, he faces up to **95 years in prison**.

This case highlights the growing threat from **young, tech-savvy insiders** and the importance of **cross-border cooperation** in tackling cybercrime.

- **Action Point: Review Social Engineering Defences** – Scattered Spider is known for exploiting human trust. Reinforce training and simulate phishing attacks.
- **Audit Access Controls** – Ensure privileged access is tightly scoped and monitored, especially for critical infrastructure.
- **Monitor for Lateral Movement** – Use EDR and SIEM tools to detect unusual activity across systems.
- **Secure Cryptographic Assets** – Protect wallets and keys with hardware security modules and strict access policies.
- **Prepare for Legal Requests** – Be ready to comply with RIPA and similar laws requiring access to encrypted devices.

How Organisations Can Drive Effective AI Governance

SANS AI Security Guidelines – Control Categories	
Control Category	Description
Access Controls	Secure models, APIs, and datasets via least privilege, strong authentication, and encrypted access. Monitor for unauthorized use.
Data Controls	Protect training and augmentation data through sanitization, masking, lineage validation, and restricted access.
Deployment Strategies	Harden AI pipelines and infrastructure with sandboxing, model validation, CI/CD gating, and red teaming.
Inference Security	Prevent prompt injection and misuse with guardrails, I/O validation, limited functionality, and escalation paths.
Monitoring	Continuously log and monitor inputs, outputs, and behavior to detect drift, anomalies, and degradation.
Model Security	Apply version control, integrity checks, and anti-tamper protections to defend models from theft or manipulation

As artificial intelligence becomes embedded across business operations, organisations face a growing challenge: **how to govern AI use responsibly without stifling innovation**.

Traditional governance models—rigid policies and blanket bans—don't work in today's fast-moving AI landscape. Instead, organisations need **flexible, scalable frameworks** that evolve with technology and business needs.

Main Article

AI offers huge opportunities for efficiency, insight, and transformation. But it also introduces risks like **data leakage, shadow AI, and regulatory non-compliance**. The key is finding a governance approach that enables **safe adoption at scale**.

The article outlines three practical strategies for organisations:

1. Understand What's Really Happening

Banning tools like ChatGPT may seem like a quick fix, but it often drives usage underground. Instead, organisations should:

- Map out where and how AI is being used,
- Track platforms and tools in use,
- Understand how employees are integrating AI into workflows.

Tools like **AI Bills of Materials (AIBOMs)** and **model registries** help track data sources, model performance, and usage. Establishing **cross-functional AI governance committees**—including legal, HR, compliance, and business units—ensures shared responsibility and oversight.

2. Align Policies to Business Speed

Governance policies must be **living documents** that adapt to changing technologies, leadership priorities, and employee behaviours. Blanket bans often backfire, leading to shadow IT and unmanaged risk. Instead, policies should be:

- Practical and enforceable,
- Aligned with business goals,
- Reviewed regularly to stay relevant.

3. Make Governance Sustainable

The goal isn't to block AI—it's to **enable responsible use**. Provide secure, enterprise-grade AI tools and reward good behaviour. Use AI to **enhance security operations**, automate threat detection, and support analysts. Protect AI systems from adversarial threats using frameworks like the **SANS Secure AI Blueprint**.

Action Points:

1. "Build an **AI inventory** and track model usage across departments.
 2. Form a **cross-functional governance committee** to oversee AI strategy.
 3. Design **flexible policies** that evolve with business needs.
 4. Provide **secure, approved AI tools** to reduce shadow AI risks.
 5. Use AI in **security operations** to improve threat detection and response.
 6. Protect AI systems using **industry-standard security frameworks**.
-



New HybridPetya Ransomware Strikes Before Boot

HybridPetya is ransomware that bypasses UEFI Secure Boot to encrypt systems before they start.

Cybersecurity researchers have recently uncovered a novel ransomware strain, HybridPetya, that blends characteristics of the infamous Petya/NotPetya malware with advanced firmware-level

attack capabilities.

Main Article

This new threat leverages a vulnerability in the Unified Extensible Firmware Interface (UEFI) to bypass Secure Boot, placing modern systems at risk of compromise before their operating systems even load.

Technical overview

Cybersecurity firm [ESET](#) reported that [HybridPetya samples were first uploaded to VirusTotal](#). The ransomware encrypts the Master File Table (MFT) of NTFS partitions, rendering file systems inaccessible without the decryption key. Unlike its predecessors, HybridPetya installs a malicious EFI application on the EFI System Partition, allowing it to execute during system startup and evade conventional security tools.

The malware consists of two primary components:

- **Installer:** Deploys the payload and modifies bootloaders.
- **Bootkit:** Responsible for loading configuration data, initiating encryption, and displaying deceptive disk-check messages.

HybridPetya exploits [CVE-2024-7344](#), a remote code execution vulnerability in the *Howyar Reloader* UEFI application. By abusing a renamed binary (bootmgfw.efi) and a crafted file (cloak.dat), HybridPetya loads unsigned code without integrity checks, effectively bypassing UEFI Secure Boot

Microsoft addressed this vulnerability in its [January 2025 Patch Tuesday update](#), but unpatched systems remain vulnerable.

Action Point: Defensive recommendations

Security professionals recommend the following measures to mitigate HybridPetya's risk:

- Apply Microsoft's [January 2025 patch](#) and verify firmware updates via the Linux Vendor Firmware Service where applicable.
- Audit UEFI bootloaders for tampering and enforce strict Secure Boot policies.
- Monitor for unauthorized EFI applications or suspicious files (e.g., cloak.dat).
- Maintain offline backups and educate administrators about firmware threats.

HybridPetya shows the evolution of ransomware into firmware domains, eroding the boundary between traditional malware and pre-OS exploits.



Acumen Cyber Threat Intelligence Digest – 17/09/2025, Week 37:

Acumen cyber threat report.

Between September 9–11, 2025, multiple cybersecurity developments highlighted new vulnerabilities and threats.

Main Article

Vulnerabilities:

Sophos patched **CVE-2025-10159**, an authentication bypass flaw in AP6 Wireless Access Points, which could enable privilege escalation via management IPs. No exploitation has been reported. Researchers from ETH Zurich disclosed **VMscape (CVE-2025-40300)**, a proof-of-concept exploit affecting AMD Zen CPUs and older Intel processors in virtualized environments, enabling branch target injection attacks that risk theft of sensitive data like encryption keys. Meanwhile, the U.S. **CISA** issued eleven advisories covering sixteen vulnerabilities in Siemens, Schneider Electric, and Daikin products, ranging from buffer overflows to weak password recovery, with patches available.

Threats:

Trend Micro reported **EvilAI malware**, first observed in August 2025, masquerading as legitimate AI tools to infiltrate manufacturing, government, healthcare, and tech sectors in India, the U.S., and France. Delivered via trojanized apps and malvertising, it leverages AI-generated code, persistence mechanisms, and encrypted traffic to evade detection. Separately, AhnLab analyzed **CyberVolk ransomware**, active since 2024, which targets government and infrastructure in Japan, France, and the UK, aligning with Russian geopolitical interests. It employs dual encryption and Telegram-based operations. Palo Alto's Unit 42 revealed a **malvertising campaign abusing GitHub dangling commits** to distribute a trojanized GitHub Desktop client, affecting global sectors from tourism to retail.

General news:

The UK **ICO** warned of rising school cyberattacks driven by student hackers, while delays to the **Cyber Security and Resilience Bill** raised concerns amid recent disruptive incidents, including at Jaguar Land Rover. The **FBI** issued a flash warning on data theft campaigns by **Scattered Spider** and **ShinyHunters**, who are extorting Salesforce customers.

Trends:

Recorded Future observed heightened activity from ransomware groups including newly emerged Gentleman, Yurei, and Radar. Globally, trending threats involve groups like Lapsus\$, Kimsuky, and ShinyHunters, exploiting vulnerabilities such as **CVE-2025-6218**, **CVE-2025-7344**, and targeting firms like Tata Group and SK Telecom.

Action Point - Remediation Actions

- Following the information provided above, we recommend that the technologies mentioned be fully patched and updated. We also want to highlight and recommend applying the following patches where applicable:
- CVE-2025-10159: To prevent threat actors from exploiting CVE-2025-10159, we recommend organisations update AP6 Wireless Access Points to version 1.7.2563 (MR7).
- CVE-2025-40300: We recommend organisations apply the latest Linux kernel updates, which include optimised use of the Indirect Branch Prediction Barrier (IBPB) to flush branch predictor states on VMExit.
- CISA ICS: We recommend organisations apply the latest vendor patches for Siemens, Schneider Electric, and Daikin products to address the vulnerabilities.

All the best from all of us at [HEFESTIS](#) and look out for a new [ThreatScape](#) update next week.

SharePoint



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



[Acumen Cyber Threat Intelligence Digest: Week 38](#)

This week's digest highlights several critical vulnerabilities, active threat campaigns, and emerging risks that organisations should act on swiftly to protect their infrastructure and data. Key Vulnerabilities & Patches SolarWinds Web Help Desk (CV...

Steve McIntosh

9/25/2025



[SC3 weekly threat reports](#)

Action Point: Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

Steve McIntosh

9/25/2025



[Government considers financial support for JLR suppliers](#)

Jaguar Land Rover (JLR) is still reeling from a major cyberattack that forced it to shut down IT systems and suspend production across its UK factories. The disruption, which began at the end of August 2025, is costing the company an estimated £50 m...

Steve McIntosh

9/25/2025



[Airport Chaos Enters Third Day After Supply Chain Attack](#)

A suspected cyber-attack targeting a third-party software supplier has caused major flight cancellations and delays at several European airports over the weekend. Main Article London's Heathrow Airport and terminals in Brussels, Berlin and Dublin ar...

David Robertson

9/24/2025



[Critical Security Flaws Grow with AI Use, New Report Shows](#)

A sharp increase in hardware, API and network vulnerabilities is exposing organizations to new risks, according to Inside the Mind of a CISO 2025: Resilience in an AI-Accelerated World . Main Article The annual report from Bugcrowd, published on Sep...

David Robertson

9/24/2025



[Attacker Breakout Time Falls to 18 Minutes](#)

Threat actors are accelerating their attacks and adopting innovative new ways to circumvent endpoint detection mechanisms, according to a new report from ReliaQuest. Main Article The threat intelligence vendor claimed in its latest Threat Spotlight ...

David Robertson

9/24/2025



[GitHub Aims to Secure Supply Chain as NPM Hacks Ramp Up](#)

GitHub this week committed to a more secure NPM supply chain in the wake of a handful of attacks causing widespread compromise. Main Article npm, or Node Package Manager, is a critical tool in the JavaScript ecosystem that serves two main functions:...

David Robertson

9/24/2025

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are also a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



Acumen Cyber Threat Intelligence Digest: Week 38

<https://acumencyber.com/cyber-threat-intelligence-digest-september-2025-week-38>

This week's digest highlights several critical vulnerabilities, active threat campaigns, and emerging risks that organisations should act on swiftly to protect their infrastructure and data.

Key Vulnerabilities & Patches

1. **SolarWinds Web Help Desk (CVE-2025-26399)**
A critical remote code execution flaw affects versions 12.8.7 and earlier. Attackers could run malicious commands without authentication.
2. **Google Chrome (CVE-2025-10585)**
A type confusion bug in the V8 engine is being actively exploited. Other patched flaws include use-after-free and buffer overflow issues.
3. **GeoServer (CVE-2024-36401)**
Exploited by unknown actors to breach a US federal agency. Attackers used web shells, cron jobs, and privilege escalation tools like Dirty COW.

Threat Actor Activity

- **Lockbit 5.0 Ransomware**
New Linux and ESXi samples show advanced evasion tactics, including log rotation and kernel profiling.
- **SonicWall Cloud Backup Breach**
Attackers brute-forced access to encrypted firewall configuration files.
- **Nimbus Manticore (Iranian APT)**
Targeting European defence and telecom sectors using spearphishing and custom

malware (MiniJunk, MiniBrowse).

Sector-Wide Disruption

- **European Airports Hit by Ransomware**
A third-party attack on Collins Aerospace disrupted check-in systems at major airports including Heathrow, Brussels, and Berlin.
- **Jaguar Land Rover Shutdown Extended**
Cyberattack halts production, affecting 30,000+ staff and 150,000 supply chain jobs.

Action Point:

- Patch all listed vulnerabilities urgently.
- Audit cloud and VPN configurations for brute-force exposure.
- Monitor for ransomware and APT activity using updated IoCs.
- Strengthen third-party risk assessments and incident response plans.



Government considers financial support for JLR suppliers

<https://www.bbc.co.uk/news/articles/c62nv0xx32go>

Jaguar Land Rover (JLR) is still reeling from a **major cyberattack** that forced it to shut down IT systems and suspend production across its UK factories. The disruption, which began at the end of August 2025, is costing the company an estimated **£50 million per week** and has left thousands of workers and suppliers in limbo.

The UK government is now considering **financial support for JLR's suppliers**, particularly smaller firms that rely solely on JLR contracts.

Options include:

- **Government-backed loans** (though unpopular with suppliers),
- **Direct purchase and stockpiling of parts** to keep businesses afloat.

This would be the **first time government aid is offered due to a cyberattack**, highlighting how digital threats are now economic threats too.

JLR's production lines in Solihull, Wolverhampton, and Halewood remain offline until at least **1 October**, with some reports suggesting delays could stretch into November. The impact extends globally, affecting JLR's facilities in **Slovakia, China, and India**.

The attack has triggered concern across government and industry. Ministers, including the Business Secretary and Industry Minister, have visited affected sites and are working with JLR a

and suppliers to find solutions. The **Business and Trade Select Committee** is also gathering evidence from impacted firms.

The group claiming responsibility—**Scattered Lapsus\$ Hunters**—has also targeted other UK institutions like **Marks & Spencer** and **Co-op**, the latter reporting **£206 million in lost revenue** due to its own breach.

This incident shows that cyberattacks are no longer just IT problems—they're **operational, financial, and strategic risks**.

Action Point:

- **Review Cyber Resilience Plans** – Ensure business continuity strategies include cyberattack scenarios, especially for supply chain disruption.
- **Explore Contingency Procurement Models** – Consider how to maintain operations if key suppliers go offline.
- **Monitor Regulatory and Government Response** – Stay informed on potential support schemes and policy changes.



Airport Chaos Enters Third Day After Supply Chain Attack

<https://www.infosecurity-magazine.com/news/airport-chaos-third-day-supply/>

A suspected cyber-attack targeting a third-party software supplier has caused major flight cancellations and delays at several

European airports over the weekend.

London's Heathrow Airport and terminals in Brussels, Berlin and Dublin are among those that continue to be impacted by the incident.

US aerospace and defense giant RTX told the [BBC](#) that its Muse software was targeted by threat actors. The software helps airlines to digitally check in passengers, validate boarding passes and tag baggage – enabling them to share desks and gates rather than requiring their own.

As such, the outage forced some airlines at certain European airports to check in and board passengers by pen and paper.

Action Point:

“These attacks often strike through the supply chain, exploiting third-party platforms that are used by multiple airlines and airports at once,” she said.

"To build resilience, aviation companies must take a layered approach: rigorously patching and updating software to close vulnerabilities, continuously monitoring for unusual activity that could indicate an intrusion, and implementing clear, well-tested backup systems that ensure airports and airlines can keep operating even if critical digital tools are knocked offline."

Improved information-sharing between governments, airlines and technology providers is also vital to accelerate incident response across borders, Wilson argued.



Critical Security Flaws Grow with AI Use, New Report Shows

<https://www.infosecurity-magazine.com/news/critical-security-flaws-grow-ai-use/>

A sharp increase in hardware, API and network vulnerabilities is exposing organizations to new risks, according to *Inside the Mind of a CISO 2025: Resilience in an AI-Accelerated World*.

The annual report from Bugcrowd, [published on September 23](#), draws on hundreds of thousands of vulnerability data points gathered from global bug bounty and disclosure programs.

AI Expands the Attack Surface

The study finds that AI-assisted software development, while accelerating innovation, is also widening the attack surface.

Applications pushed through rapid release cycles often leave behind gaps in access control, data protection and hardware security. At the same time, attackers are exploiting overlooked entry points such as APIs.

"We are in a high-stakes innovation race, but with every AI advance, the security landscape becomes exponentially more complex," said Nick McKenzie, CISO of Bugcrowd.

"Attackers are exploiting this complexity, but still targeting foundational layers like hardware and APIs. No single CISO can win this race alone."

Action Point:

Randolph Barr, CISO at Cequence Security, highlighted a growing risk from AI-enabled impersonation: "This goes beyond phishing, it's targeted impersonation backed by research and AI."

He argued that layered security controls must move beyond blaming "human error" to detect and block these sophisticated attacks in real time.

The Bugcrowd report concludes that collective intelligence and continuous offensive testing will be essential to withstand escalating digital threats.



Attacker Breakout Time Falls to 18 Minutes

<https://www.infosecurity-magazine.com/news/attacker-breakout-time-falls-18/>

Threat actors are accelerating their attacks and adopting innovative new ways to circumvent endpoint detection mechanisms, according to a new report from ReliaQuest.

The threat intelligence vendor claimed in its latest *Threat Spotlight* report for the period June–August 2025 that average breakout time – the period from initial access to lateral movement – dropped to 18 minutes.

One attack from the Akira came in at just six minutes, way below the lowest breakout time recorded in 2024, of 27 minutes.

The figure keeps falling. In January, [ReliaQuest claimed](#) breakout time in 2024 was 22% shorter than the previous year. Once adversaries reach this stage, attacks become harder to detect and contain.

Threat actors are not just getting faster but also smarter, ReliaQuest warned. There's been a sharp rise in ransomware operations using the SMB file-sharing protocol for remote file encryption – from 20% to 29% of ransomware attacks.

“Using compromised credentials, attackers access shared files on a network via a single compromised host, often through unmanaged devices or VPNs,” the report noted. “By encrypting data remotely, they bypass endpoint protections entirely, operating quietly and efficiently within the network. This highlights a critical flaw in endpoint-focused defenses: Attacks don't stop at the endpoint, and neither should your defenses.”

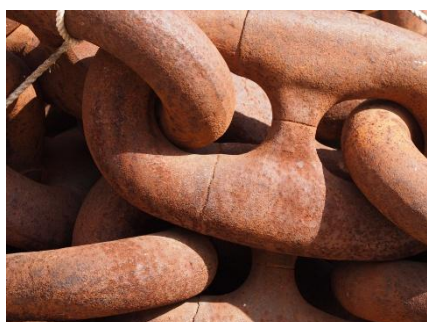
Action Point:

ReliaQuest also warned that drive-by-compromise remains the most popular tactic for initial access, accounting for 34% of incidents. That's versus 12% for spear phishing links and, remarkably, 12% for USB malware.

“USB-based malware is thriving because of weak policy enforcement and inconsistent endpoint controls. It's easy to overlook the dangers of plugging in unvetted USBs and attackers exploit this to infiltrate corporate networks,” the report noted.

It pointed to the Gamarue variant as particularly prevalent in the period.

“Gamarue hides its malicious Dynamic Link Libraries (DLLs) so well that most employees wouldn’t know they’re infected,” ReliaQuest [said](#). “The infection trigger – a malicious LNK file – disguises itself as a legitimate file already present on the USB, making it even harder to spot.”



GitHub Aims to Secure Supply Chain as NPM Hacks Ramp Up

<https://www.darkreading.com/application-security/github-secure-supply-chain-npm-hacks-ramp-up>

GitHub this week committed to a more secure NPM supply chain in the wake of a handful of attacks causing widespread compromise.

npm, or Node Package Manager, is a critical tool in the JavaScript ecosystem that serves two main functions:

- **Public Repository:** It acts as a repository for open-source JavaScript packages, allowing developers to share and manage reusable code libraries.
- **Command-Line Interface (CLI):** It provides a command-line interface for developers to interact with the npm registry, facilitating the installation and management of packages.

On Sept. 22, GitHub senior director of security research Xavier René-Corail published a blog post to GitHub addressing the surge in package registry-based attacks, specifically NPM packages. The post comes in the wake of two major supply chain attacks involving NPM packages this past month: the [self-replicating Shai-Hulud malware campaign](#) and a social engineering attack against [prolific developer Qix](#).

In the case of Shai-Hulud, an infostealing malware that embedded itself in poisoned malware packages and could steal secrets including NPM tokens, GitHub said the worm could have resulted in an endless stream of attacks if the security industry didn't take swift action. For its part, the company said it immediately removed more than 500 compromised packages and blocked new packages containing the malware's indicators of compromise.

In addition to these actions, GitHub said it would take steps to harden the NPM supply-chain and make package publication more secure.

Action Point:

"By enforcing modern 2FA and adopting granular, short-lived tokens, GitHub is raising the bar for attackers and closing off some of the paths that enabled incidents like the Qix

compromise and Shai-Hulud," McGuire says. "That said, no single change will fully prevent these types of attacks. Package registries are only one part of the open source software supply chain, and attackers are increasingly creative in finding ways to compromise popular projects."

SC3 Daily Threat Summaries and Weekly Report

<https://www.cyberscotland.com/news/daily-threat-reports/>



A daily breakdown of various cyber threats from the Scottish Cyber Coordination Centre (SC3)

Action Point:

All SC3 threat intelligence in one place.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Limited, Registered Office: Unit 27, Stirling Business Centre, Wellgreen, Stirling FK8 2DZ

Incorporated in Scotland SC603511

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	1
Cyber Security Awareness Month: NCSC Branded Materials	2
Member Article: AiTM event with IoC's	6
Chinese APT 'Phantom Taurus' Targeting Organizations With Net-Star Malware	9
'Trifacta' of Google Gemini Flaws Turn AI Into Attack Vehicle	10
Shutdown Threatens US Intel Sharing, Cyber Defense	11
Acumen Cyber Threat Intelligence Digest – 1/10/2025, Week 39:	12

SC3 Daily Threat Summaries and Weekly Report



Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

This week's reports:



SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu
lletin-30-Septemberlletin-1-October-202lletin-2-October-202lletin-3-October-202



SC3-Weekly-Vulner
ability-Report-30-Se



National Cyber
Security Centre
a part of GCHQ

Cyber Security Awareness Month: NCSC Branded Materials

Useful presentation from NCSC:

Presentation attached to this edition

Hi all,

We hope that you are doing well. We just wanted to share the attached NCSC External Partners Deck for Cyber Security Awareness Month, which your External or Internal Communications teams may wish to share through your organisation or partner networks.

The material is aimed at industry partners, and highlights some key NCSC resources we're promoting (to different types of organisations and employees) over Cyber Security Awareness Month, including:

- Cyber Essentials
- Cyber Action Toolkit
- Cyber Governance for Boards
- Early Warning
- Assured Services
- Top Tips for Staff

Thanks,

Sector Resilience

Action Point: Depending on the material you wish to share, this could be targeted at staff, suppliers or others in your sector. The campaign will be delivered through coordinated communications moments using social channels including LinkedIn, Instagram, Facebook, Bluesky, Threads and X.

For any terms and conditions please refer to the NCSC website ([Terms & conditions - NCSC.GOV.UK](#)), and for any queries around co-branding the assets please contact our External Affairs team (externalaffairs@ncsc.gov.uk).



Member Phishing Alert

A member has offered to share information on a phishing attack that they have recently experienced.

The phishing attempt started with a email chasing an invoice. Within the email body chain there was a fabricated reply from a genuine contact (employee A) saying this should be forwarded onto the accounts team with said team's email address embedded in the reply.

As the email chain looked to contain a response from a genuine person (employee A) from the member organisation, falsifying authenticity and the appearance of them being involved in the conversation, the finance contact replied. It was only when this reply came to the inbox of the genuine contact used (employee A) in the first email that they raised the alarm.

These types of attack where an email chain is used with valid organisational information, such as identities and email addresses are becoming more common. Details can be harvested from organisation sites, social media sites or previous breaches to give credence to fabricated conversations.

The anonymised text for the exchange is given below.

From: Paul Schwartz <pschwartz@tpmsupportdesk.com>

Sent: 29 September 2025 17:48

To: <genuine address of university accounts department>

Cc: paul@quantstrategies.org

Subject: Re: <university name> - Overdue Strategic Planning Services Invoice INV172573

Hi Accounting team

Following the request from <name of Principal> below, I am forwarding INV172573 for processing as directed.

Kindly note that this invoice is already overdue, and we would appreciate it if it could be processed at your earliest convenience. Please confirm receipt.

Paul Schwartz

Accounting | **QUANT CONSULTING LLC**

132 Bedford Avenue, 3rd Floor

Brooklyn, NY 11211

From: <name of Principal> <genuine email address from university>
Sent: Friday, September 26, 2025 04:31 PM
To: Paul Sternberg <paul@quantstrategies.org>
Cc: QUANT CONSULTING LLC Accounting <pschwartz@tpmsupportdesk.com>
Subject: <university name> Overdue Strategic Planning Services Invoice - INV172573

Paul,

I sincerely apologize for the delay in processing this payment; I had not seen your previous email until now. I have reviewed the invoice and everything is in order for payment.

To expedite the payment process and avoid any further delays please forward the invoice directly to our Accounting Department at <genuine email address of accounts department> for processing

I want to acknowledge the exceptional quality of work your team provided during our strategic planning initiative in June. The comprehensive market analysis and strategic roadmap have already begun to influence our decision-making processes, and the executive workshops were particularly valuable for our leadership team.

Thank you for your patience and professionalism.

Regards

<name of Principal>

From: Paul Sternberg <paul@quantstrategies.org>

Sent: Friday, September 26, 2025 10:31 AM

To: <name of Principal> <genuine email address from university>

Cc: QUANT CONSULTING LLC Accounting <pschwartz@tpmsupportdesk.com>

Subject: <university name> Overdue Strategic Planning Services Invoice - INV172573

Hi <name of Principal>,

I'm writing to follow up regarding the attached invoice issued for the recent strategic planning consultation services for Q2 provided to <university name>. As of today, the invoice remains outstanding and is now due.

Invoice Details:

Invoice Number: INV172573

Invoice Date: July 7th 2025

Amount Due: \$49,130

We kindly ask that payment be processed at your earliest convenience. Please note that, as the invoice is overdue, it may be subject to a late payment fee in accordance with our payment terms.

Thank you again for the opportunity to support your team. We truly value our partnership and look forward to continuing to work together.

Best Regards

Paul Sternberg

Chief Executive Officer

QUANT CONSULTING LLC

132 Bedford Avenue, 3rd Floor

Brooklyn, NY 11211

USA

*This email and any attachments are confidential and intended solely for the use of the named recipient(s). If you have received this email in error, please notify the sender immediately and permanently delete it from your system. Any unauthorized review, use, disclosure, copying, or distribution of this email is strictly prohibited. **QUANT CONSULTING LLC** accepts no liability for any errors or omissions in the content of this email that may have occurred during transmission.*

Action Point:

Ensure that users are aware that these attacks can happen and that any unexpected emails need to be treated with care and where necessary verified as part of business as usual processes.

Sharing information on attacks experienced give far greater protection and learning experiences for the community. Thanks to the member for sharing the details of this attack. HEFESTIS are always prepared to send on anonymised information regarding ongoing incidents, so please share what you can, it helps us all.



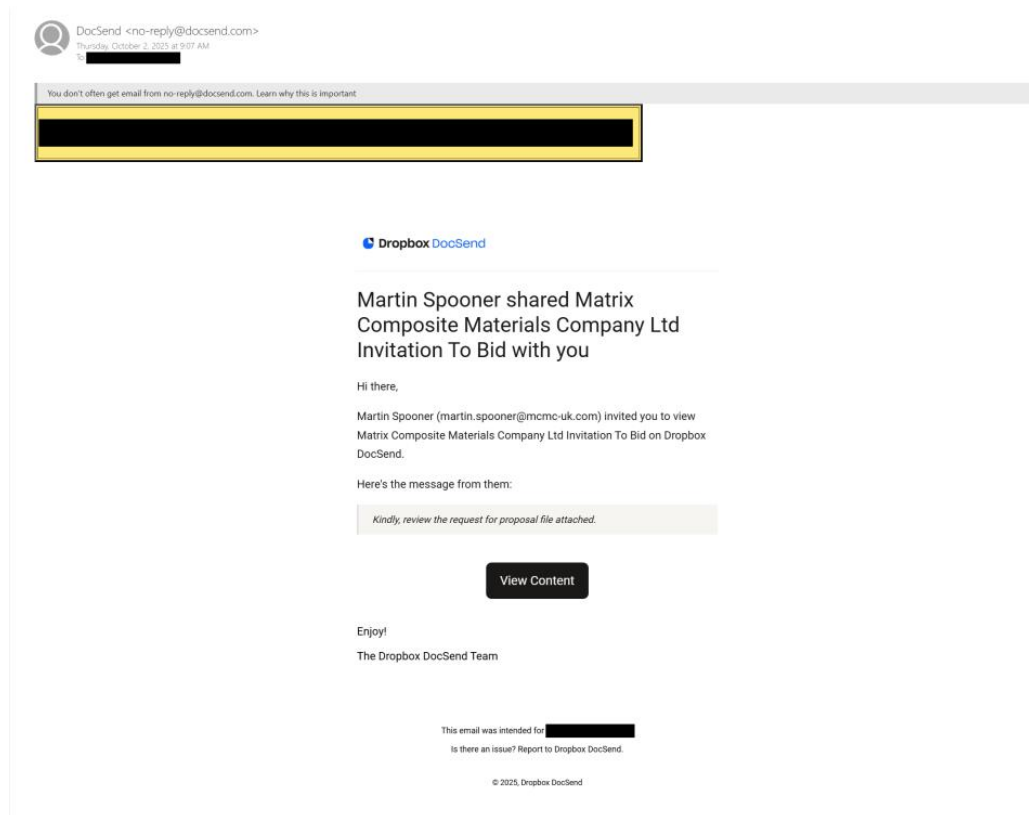
Member Article: AiTM event with IoC's

One of our members encountered and mitigated an adversary in the middle (AiTM) phishing attack this morning which a user clicked through and entered their credentials. Microsoft Defender Attack Disruption detected this and disabled the users account.

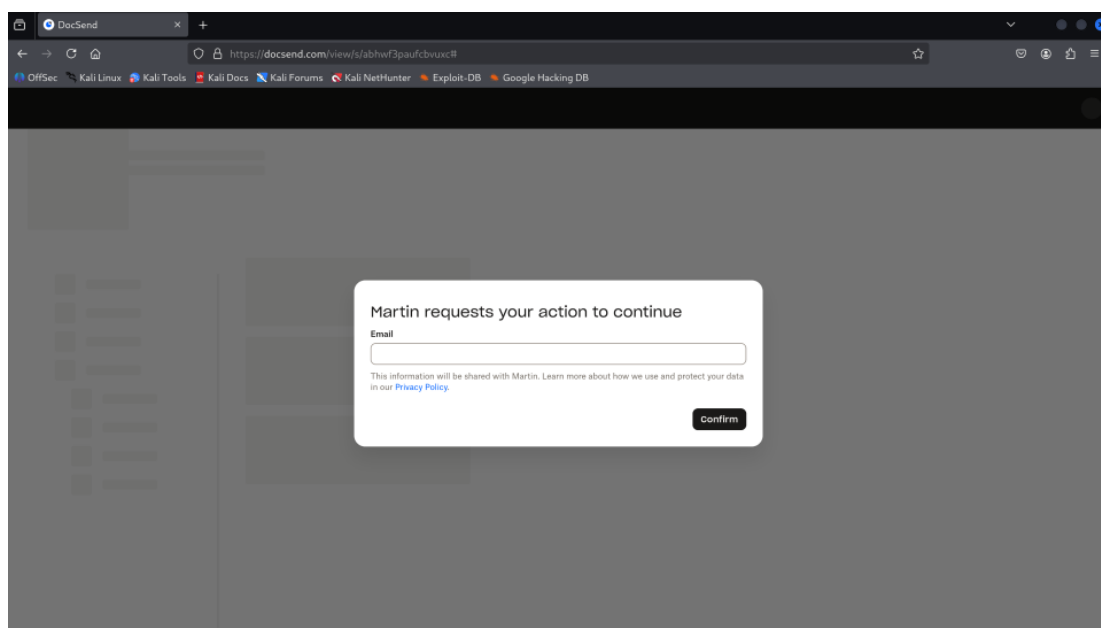
IOCs

Sender	no-reply@docsend.com
Subject (1)	Martin Spooner shared "Matrix Composite Materials Company Ltd Invitation To Bid" with you
Subject (2)	Please verify your email address to access this content
Time Received	02/10/2025 10:11 (1) and 10:12 (2)
Compromised Email Account	martin.spooner@mcmc-uk.com
Sign ins attempted from	68.64.184.139
	68.64.187.201

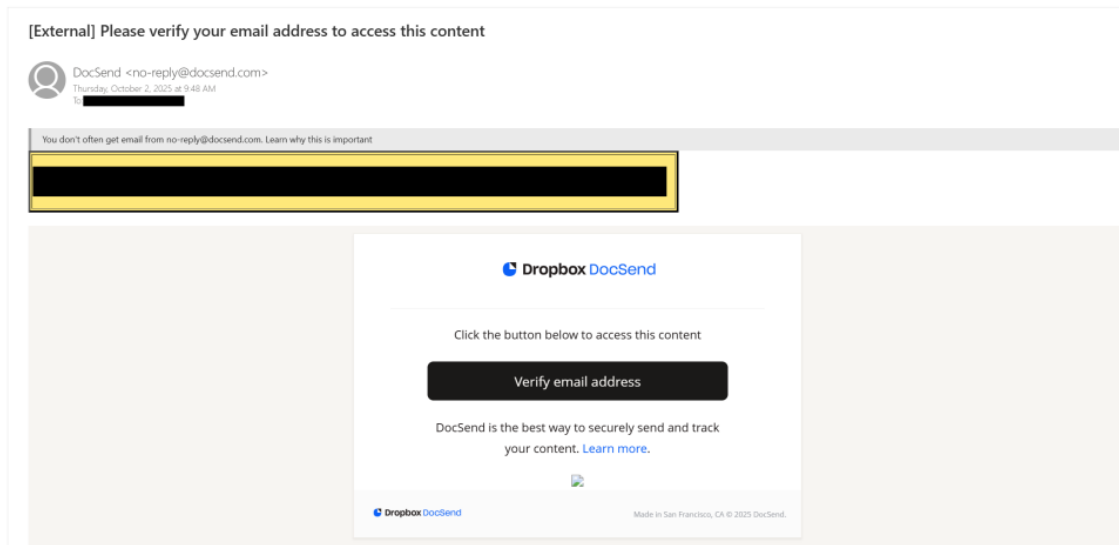
The initial email was a sharing link to a document from Dropbox DocSend



This opens a page to enter your email address



Which redirects to this page



Action Point: The link only works with the recipient address and has a session expiry because it couldn't be accessed using a disposable email account or by pulling the URL from Defender unfortunately.

The sender also sent out an apology to the user to say that their email account had been compromised so hopefully this has been resolved by the organisation now.



Chinese APT 'Phantom Taurus' Targeting Organizations With Net-Star Malware

Focused on espionage, the threat actor shares infrastructure with Chinese APTs, but uses different TTPs in attacks.

[Main Article](#)

A Chinese state-sponsored hacking group tracked as 'Phantom Taurus' has been targeting government and telecommunications organizations for espionage for more than two years, Palo Alto Networks reports.

Initially observed in 2023, the APT was only recently linked to Chinese hacking groups through shared infrastructure, as its tactics, techniques and procedures (TTPs) differ from those typically associated with threat actors operating out of China.

"These enable the group to conduct highly covert operations and maintain long-term access to critical targets," [says Palo Alto Networks](#).

The group, the cybersecurity firm explains, uses shared operational infrastructure exclusive to Chinese APTs, and targets high-value organizations (such as ministries of foreign affairs and embassies), in line with China's economic and geopolitical interests.

What sets Phantom Taurus apart, however, is the use of a different set of TTPs, some unique to the group, such as its Specter and Net-Star malware families, and the Ntospy malware. Tools typically used by Chinese hackers, such as China Chopper, the Potato suite, and Impacket, are also part of its inventory.

The APT has been observed targeting email servers to exfiltrate messages of interest, as well as directly targeting databases, in attacks against organizations in Africa, the Middle East, and Asia.

Action Point: It supports built-in commands to perform file system operations, access databases, execute arbitrary code, manage web shells, evade and bypass security solutions, load payloads directly in memory, and encrypt communication with the C&C.

The first malware loader, AssemblyExecuter V1, can execute other .NET assemblies in memory, allowing the attackers to dynamically load and execute additional code post-compromise.

AssemblyExecuter V2 has the same core purpose, but features enhanced evasion capabilities, with dedicated methods for bypassing Windows's Antimalware Scan Interface (AMSI) and Event Tracing for Windows (ETW) security mechanisms.

"We observed that the group takes an interest in diplomatic communications, defense-related intelligence and the operations of critical governmental ministries. The timing and scope of the group's operations frequently coincide with major global events and regional security affairs," Palo Alto Networks says.



'Trifecta' of Google Gemini Flaws Turn AI Into Attack Vehicle

Flaws in individual models of Google's AI suite created significant security and privacy risks for users, demonstrating the need for heightened defenses.

Main Article

Three flaws within separate models of [Google's Gemini](#) AI assistant suite exposed them to various injection attacks and data exfiltration, respectively, creating severe privacy risks for users, researchers have found. The flaws serve as a reminder that these models are not only targets for attackers, but also can be weaponized against users and thus require strict security parameters.

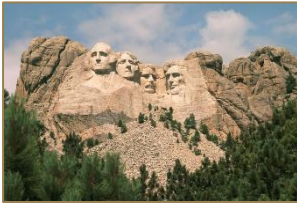
Researchers at Tenable discovered the flaws, which they dubbed the "[Gemini Trifecta](#)," in several products within Google's family of AI models — specifically Gemini Search Personalization, Gemini Cloud Assist, and the Gemini Browsing Tool, they revealed in a report published today.

Action Point:

As AI assistants like Google's Gemini become integral to how users interact with information, "defenders must treat AI integrations as [active attack surfaces](#) rather than passive tools," and put security parameters in place to protect their users, Matan says.

This can be done in a number of ways, such as "gaining visibility into all AI tools, authorized and unauthorized, regularly auditing logs and search histories for manipulation (specifically prompt injection attempts), as well as monitoring for unusual outbound requests that may indicate data exfiltration," he says.

It's also crucial for organizations to test AI services for resilience against prompt injection and implement layered defenses, including input sanitization and strict monitoring of tool executions, Matan adds.



Shutdown Threatens US Intel Sharing, Cyber Defense

Any prolonged US federal government shutdown could have wide-ranging consequences for the nation's cybersecurity posture, with the biggest immediate concern being a disruption in cyber threat intelligence sharing between the private sector and government.

Main Article

Other major concerns include the US Cybersecurity and Infrastructure Security Agency's (CISA) continued ability to execute its mission and potential exposures at federal agencies forced to release contractors and third parties on whom they currently rely for cybersecurity.

Action Point:

The shutdown, which began on Oct. 1 at 12:01 a.m., coincided with the lapsing of the Cybersecurity Information Sharing Act of 2015 (CISA 2015), after Congress failed to reauthorize the bill before its Sept. 30, 2025, sunset date.

CISA 2015 provided important legal protections for companies that shared threat data in good faith, shielding them from liability related to privacy or antitrust concerns. Security experts widely consider the statute vital for encouraging the voluntary exchange of cyber threat indicators such as malware signatures and attack patterns between the private sector and federal, state, and local governments.



Acumen Cyber Threat Intelligence Digest – 1/10/2025, Week 39:

The Cyber Threat Intelligence Digest highlights recent vulnerabilities, potential threats, and cyberattacks.

Main Article

Vulnerabilities:

VMware patched three high-severity flaws affecting vCenter and NSX products on September 29, 2025. These vulnerabilities (CVE-2025-41250, CVE-2025-41251, and CVE-2025-41252) involve email header manipulation, password recovery flaws, and username enumeration. Cisco patched a stack-based buffer overflow vulnerability (CVE-2025-20352) in its IOS and IOS XE software, which is actively being exploited, allowing attackers to trigger DoS or gain root access. Notepad++ also disclosed a command injection flaw (CVE-2025-56383) in version 8.8.3, with no active exploitation reported yet.

Potential Threats:

A malvertising campaign distributing trojanized Microsoft Teams installers was uncovered, delivering the Oyster backdoor via fraudulent installers signed with valid certificates. Additionally, a malicious npm package, "fezbox," uses QR code steganography to steal browser credentials. A fileless execution method using a 64-bit portable executable (PE) loader was also described, allowing malware to bypass endpoint detection.

General News:

The Co-op retail chain lost \$275 million due to a cyberattack in April, impacting its food business. Harrods reported a second data breach within six months, affecting 430,000 customers, while Afghanistan experienced a nationwide internet blackout, disrupting essential services.

Threat Actor Trends:

Several threat actors showed new activity, including ransomware groups and cybercriminals using phishing, backdoor attacks, and exploits like CVE-2025-32463 and CVE-2025-41244. Remediation steps include patching the identified vulnerabilities in VMware, Cisco, and Notepad++.

Action Point - Remediation Actions

Following the information provided above, we recommend that the technologies mentioned be fully patched and updated. We also want to highlight and recommend applying the following patches where applicable:

- **CVE-2025-41250, CVE-2025-41251, CVE-2025-41252:** These vulnerabilities can be remediated by updating vCenter and NSX to the most recent version.
- **CVE-2025-20352:** We recommend updating SNMP versions v1, v2c, v3 and IOS and IOS XE to the most recent version to prevent this vulnerability from being exploited.
- **CVE-2025-56383:** There has not yet been a patch released for this CVE, we advise updating this once an update becomes available.

All the best from all of us at HEFESTIS and look out for a new ThreatScape update next week.



National Cyber
Security Centre
a part of GCHQ

CYBER SECURITY AWARENESS MONTH

EXTERNAL PARTNERS PACK

Index

- › [The Cyber context](#)
- › [Help for your business](#)
- › [Small businesses](#)
- › [Large businesses](#)
- › [Guidance for staff](#)
- › [Assets](#)

Throughout October, the National Cyber Security Centre will support Cyber Security Awareness Month by promoting practical, expert guidance to help UK businesses strengthen their cyber resilience and bolster their defences.

This year's global theme, *Secure Our World*, highlights the importance of taking action to protect against evolving cyber threats.

We're encouraging organisations to act now by using our trusted tools and services, including

- › Cyber Essentials
- › Cyber Action Toolkit
- › Cyber Governance for Boards
- › Early Warning
- › Assured Services

The campaign will be delivered through coordinated communications moments using social channels including LinkedIn, Instagram, Facebook, Bluesky, Threads and X.

We invite you to help amplify this campaign by sharing our messaging with your customers, stakeholders, and networks.

Cyber attacks are widespread and rising in sophistication

- 74% of large, 67% of medium and 42% of small businesses reported experiencing a cyber breach or attack¹ in the past year. Phishing remains the most common and disruptive threat, often requiring significant time and resource to investigate and manage. Businesses are increasingly aware of evolving tactics like AI impersonation, which are becoming more sophisticated and harder to detect.
- The financial cost can be severe. IBM's X-Force 2025 Threat Intelligence Index notes that the UK is the most targeted European country for cyber attacks in Europe². The recent cyber incident at Marks and Spencer has reportedly cost ~£300million.
- The NCSC's mission is to make the UK the safest place to live and work online so that everyone – whether at work or at home – can navigate the cyber landscape safely and with confidence. Our tools and NCSC-recognised industry services are available to support organisations of all sizes, in every sector.

How you can support Cyber Security Awareness Month

Social media

Share or comment on the NCSC's content. Use the suggested copy and hashtags provided in this pack.

Tag NCSC and use the hashtag:

#CyberMonth2025

Owned channels

Include a short article or message in newsletters, bulletins, or stakeholder updates.

Link to NCSC guidance and tools relevant to your audience.

Co-branding

If you would like to co-brand the assets with your own logo, please contact our External Affairs team:

externalaffairs@ncsc.gov.uk

How you can protect your business

Cyber Essentials:

www.ncsc.gov.uk/cyberessentials

For all organisations

92% fewer insurance claims, highlighting the real-world impact of these protections.

Cyber Essentials is a UK government-backed certification that proves your organisation is protected against the most common cyber threats.

Implementing just five key controls reduces risk, builds protection and gives stakeholders verified assurance that your organisation prioritises cyber security and meets the UK minimum standard for cyber security.

NCSC tools and services for small organisations

The Cyber Action Toolkit **Launching 14 October!**

The Cyber Action Toolkit is a free, personalised cyber security solution for sole traders to small organisations that turns cyber protection into simple, achievable steps for your business.

Just like you'd install a lock on your shop door, this toolkit helps you secure your business with straightforward actions tailored to your size and situation.

It guides you through building stronger cyber protection at your own pace, with built-in features that recognise your progress – providing a starting point to cyber security and a pathway towards Cyber Essentials certification.

NCSC tools and services for larger organisations

Cyber Governance for Boards

www.ncsc.gov.uk/cyber-governance-for-boards/overview

In partnership with DSIT, the NCSC created a Cyber Governance Training programme designed to empower boards to confidently implement the Cyber Governance Code of Practice. This training ensures boards are equipped to meet their cyber security responsibilities with clarity and confidence. The Cyber Governance Training aligns with the five core principles from the Cyber Governance Code of Practice. These are:

-  Risk Management
-  Strategy
-  People
-  Incident Planning, Response & Recovery
-  Assurance & Oversight

Each module takes around 20 minutes to complete and includes expected learning outcomes and links to relevant NCSC resources.

Early Warning

www.ncsc.gov.uk/section/active-cyber-defence/early-warning

For many organisations, the cost of network monitoring is prohibitive, and the specialist skills it requires often aren't available in-house. Early Warning is a free service designed to warn organisations of potential cyber attacks on their network, as soon as possible, potentially giving invaluable time to detect and stop a cyber incident before it escalates.

Assured Services

www.ncsc.gov.uk/section/products-services/assured-services

Our assured services help UK organisations find trusted cyber security providers, certified by the NCSC against strict technical standards. These experts can support you to prevent, detect, and respond to cyber threats.

Assets

[Click here to download all assets](#)

Assets within the pack

Social

- Statics in 1x1, 9x16, 16x9, 1920x1440
- Videos in 1x1, 9x16, 16x9, 1920x1440
- Headers for LinkedIn, X/Bluesky, SharePoint

Email

- Email header
- Signature static and video



You can find us on: [LinkedIn](#), [X \(Twitter\)](#), [Instagram](#), [Bluesky](#), [Facebook](#), [Threads](#)

Suggested Copy

Cyber threats are evolving, but so are the ways to protect against them. This #CyberMonth2025, explore @NCSC's guidance to help your organisation stay secure.
#SecureOurWorld

Learn how your organisation can improve its cyber resilience all #CyberMonth2025 with tools and advice shared by @ncsc throughout October
#SecureOurWorld

Cyber security is everyone's responsibility. This #CyberMonth2025, @NCSC is sharing tools and tips to help organisations and individuals build resilience together.
#SecureOurWorld

Wondering how to boost your organisation's cyber resilience? This #CyberMonth2025, @NCSC is sharing expert tips and tools all October long.
#SecureOurWorld



Social Media Timeline

Week	Dates	Theme	Key dates & Events
Week 1	1 – 5 Oct	#CyberMonth2025 Launch	1 Oct – Week 1 Launch post 3 Oct – NCSC 9th Birthday post
Week 2	6 – 12 Oct	Cyber Essentials	6 Oct – Week 2 Launch post
Week 3	13 – 19 Oct	Small business advice Annual Review	13 Oct – Week 3 launch post 14 Oct – Ada Lovelace Day (NCSC posting day before) 14 Oct – AR Launch In week: Cyber Action Toolkit
Week 4	20 – 26 Oct	Cyber Governance for Boards resources	20 Oct – Week 4 launch post
Week 5	27 – 31 Oct	Early Warning	27 Oct – Week 5 launch post 31 Oct – Final post

You can find us on: [LinkedIn](#), [X \(Twitter\)](#), [Instagram](#), [Bluesky](#), [Facebook](#), [Threads](#)

Internal Campaigns

If you wish to run internal awareness activity, refer your team to the [**NCSC guidance on Top Tips for Staff**](#) to help your staff keep your organisation safe.

You can link the training and use the key messages below to shape your own content:

- **Defence against phishing:** Recognise phishing attempts by looking out for urgency, authority, imitation and errors. Speak up if something feels suspicious, even if you've clicked.
- **Create strong passwords:** Create strong, unique passwords. Turn on two-factor authentication and prioritise protecting accounts that hold personal or financial information.
- **Secure your devices:** Keep devices locked with a PIN, password, or biometrics. Install updates promptly to fix known vulnerabilities. Be aware of your surroundings when working in public spaces and consider using a privacy screen.
- **Report incidents:** Report incidents quickly, even if you're unsure or think someone else will. Mistakes happen, and early reporting helps reduce harm. Flag security processes that don't work so they can be improved.

Thank You

For terms and conditions, please refer to the NCSC website:
[Terms & conditions – NCSC.GOV.UK](https://www.ncsc.gov.uk/terms-conditions)



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



[CL0P-Linked Hackers Breach Dozens of Organizations Through Oracle Software Flaw](#)

A newly discovered zero-day vulnerability in Oracle's E-Business Suite (EBS) —tracked as CVE-2025-61882 with a critical CVSS score of 9.8 —has been exploited by threat actors in a widespread campaign affecting dozens of organisations since August 20...

Steve McIntosh

10/10/2025

2 views



[New Microsoft Secure Future Initiative \(SFI\) patterns and practices: Practical guides to strengthen security](#)

Microsoft has released a new set of Secure Future Initiative (SFI) patterns and practices—designed to help organisations implement scalable, practical cybersecurity strategies based on real-world experience. These patterns are built by practitioners...

Steve McIntosh

10/10/2025

2 views



[Acumen Cyber Threat Intelligence Digest: Week 40](#)

This week's digest highlights several critical vulnerabilities, active threat campaigns, and emerging risks that organisations should address to strengthen resilience and reduce exposure. Key Vulnerabilities & Patches DrayTek Vigor Routers (CVE-2025...

Steve McIntosh

10/10/2025

3 views



[SC3 weekly threat reports](#)

Action Point: Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

Steve McIntosh

10/10/2025

4 views



[Employees regularly paste company secrets into ChatGPT](#)

A new report from cybersecurity firm LayerX reveals that employees are regularly pasting sensitive company data—including personally identifiable information (PII) and payment card data (PCI)—into generative AI tools like ChatGPT, often without pe...

Steve McIntosh

10/9/2025

5 views



[Too Authentic to be Synthetic: The Psychology Behind AI Voice Scams](#)

As AI-generated voices become indistinguishable from real ones, new research from Dr Neil Kirk at Abertay University reveals a troubling psychological vulnerability: people are more likely to trust voices that sound like their own. This means that r...

Steve McIntosh

10/9/2025

10 views

[Go To Site](#)

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are also a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



CL0P-Linked Hackers Breach Dozens of Organizations Through Oracle Software Flaw

<https://thehackernews.com/2025/10/cl0p-linked-hackers-breach-dozens-of.html>

A newly discovered zero-day vulnerability in **Oracle's E-Business Suite (EBS)**—tracked as **CVE-2025-61882** with a critical CVSS score of **9.8**—has been exploited by threat actors in a widespread campaign affecting **dozens of organisations** since August 2025.

The attacks, linked to tactics used by the **Cl0p ransomware group**, involve a sophisticated chain of exploits including:

- **Server-Side Request Forgery (SSRF)**
- **CRLF injection**
- **Authentication bypass**
- **XSL template injection**

These techniques allow attackers to gain **remote code execution** on Oracle EBS servers, set up reverse shells, and exfiltrate sensitive data. The campaign began with a **high-volume phishing email wave** targeting executives, using credentials bought from underground forums. Victims were told their Oracle EBS systems had been breached and were threatened with data leaks unless they paid a ransom.

Interestingly, while the Cl0p name was used, Google's Threat Intelligence Group (GTIG) and Mandiant suggest the actual malware and tooling—like **GOLDVEIN.JAVA**, **SAGELEAF**, and **SAGEWAVE**—may point to **FIN11**, a known cybercrime group. The attackers used Java-based payloads to install backdoors and execute reconnaissance commands from the EBS account **"applmgr"**.

Some of the exploit code was later leaked in a Telegram group linked to **Scattered LAPSUS\$ Hunters**, but attribution remains unclear.

Action Point:

- **Patch Oracle EBS Immediately**
Apply Oracle's latest security updates to close CVE-2025-61882 and related vulnerabilities.
 - **Audit EBS Configurations**
Review access controls, especially around the /OA_HTML/SyncServlet component and Template Preview functionality.
 - **Monitor for Suspicious Activity**
Look for signs of reverse shell activity, Java-based payloads, and unusual commands from the "applmgr" account.
-



New Microsoft Secure Future Initiative (SFI) patterns and practices: Practical guides to strengthen security

<https://www.microsoft.com/en-us/security/blog/2025/10/07/new-microsoft-secure-future-initiative-sfi-patterns-and-practices-practical-guides-to-strengthen-security/>

Microsoft has released a new set of **Secure Future Initiative (SFI)** patterns and practices—designed to help organisations implement **scalable, practical cybersecurity strategies** based on real-world experience. These patterns are built by practitioners, for practitioners, and reflect Microsoft's own internal security improvements.

The goal? To help organisations move beyond theory and adopt **repeatable, proven approaches** to common security challenges—whether it's protecting networks, securing cloud tenants, or locking down software pipelines.

What's Included in the Latest SFI Patterns

Microsoft's latest release includes six key patterns across three focus areas:

1. **Network Isolation**
Segment networks by default to contain breaches. Use per-service ACLs and isolated virtual networks to prevent lateral movement.
2. **Secure All Tenants and Resources**
Apply baseline security policies (MFA, Conditional Access) to every cloud tenant. Retire unused tenants to eliminate "shadow" environments.
3. **Higher Security for Entra ID Apps**
Remove unused apps, tighten permissions, and enforce strong authorisation to block identity-based attacks.
4. **Zero Trust for Source Code Access**
Require proof-of-presence MFA for critical code commits to prevent unauthorised

changes in the development pipeline.

5. **Protect the Software Supply Chain**

Standardise CI/CD pipelines, use internal package feeds, and automate scanning to prevent supply chain attacks.

6. **Centralise Access to Security Logs**

Improve incident response by standardising log collection and retention across multi-cloud environments.

Why It Matters for Organisations

These patterns are modular and extensible—like software design patterns—and can be adapted to different environments. Each one includes:

- A clear problem statement,
- Microsoft's internal solution,
- Practical guidance for implementation,
- Implications and trade-offs.

This structure helps organisations **understand, apply, and evolve** their security practices with confidence.

Action Point:

- Review the SFI library and identify patterns relevant to your environment.
- Form cross-functional teams to implement selected patterns.
- Retire unused cloud tenants and enforce MFA across all identities.
- Lock down CI/CD pipelines and source code access.
- Centralise log collection for better visibility and faster investigations.

Microsoft's SFI patterns offer a **roadmap to secure-by-design operations**.



Acumen Cyber Threat Intelligence Digest: Week 40

<https://acumencyber.com/cyber-threat-intelligence-digest-october-2025-week-40>

This week's digest highlights several critical vulnerabilities, active threat campaigns, and emerging risks that organisations should address to strengthen resilience and reduce exposure.

Key Vulnerabilities & Patches

1. **DrayTek Vigor Routers (CVE-2025-10547)**

A flaw in DrayOS could allow remote code execution via crafted HTTP/HTTPS requests.

Action: Patch immediately and disable remote WebUI/SSL VPN access or apply ACLs to reduce WAN risk.

2. **Redis Lua Scripting (CVE-2025-49844)**

A critical use-after-free vulnerability dubbed “RediShell” could allow attackers to escape the Lua sandbox and execute arbitrary code.

Action: Update Redis to the latest version across all environments.

3. **NVIDIA CUDA Toolkit & Adobe Acrobat Reader**

Cisco Talos disclosed multiple vulnerabilities, including buffer overflows and memory corruption issues.

Action: Apply September 2025 patches from NVIDIA and Adobe.

Active Threat Campaigns

- **UAT-8099 (China-linked)**

Targeting universities and telecoms via compromised Microsoft IIS servers. Tactics include SEO fraud, credential theft, and persistent access using BadIIS malware.

Action: Audit IIS servers, restrict file uploads, and monitor for web shell activity.

- **XiebroC2 & JuicyPotato on MS-SQL Servers**

Attackers are brute-forcing weak credentials, escalating privileges, and deploying remote-control frameworks.

Action: Enforce strong passwords, monitor for JuicyPotato usage, and block outbound traffic to known C2 IPs.

- **Android Spyware in UAE**

Fake Signal and ToTok apps are stealing data via phishing sites and unofficial app stores.

Action: Educate users, restrict APK sideloading, and monitor mobile device activity.

General News

- **Jaguar Land Rover Restarting Production**

Following a cyberattack, JLR is launching a supplier financing scheme to support recovery.

Action: Review supply chain cyber resilience and contingency plans.

- **Discord & Renault UK Third-Party Breaches**

Sensitive customer data exposed due to breaches at external service providers.

Action: Reassess third-party risk management and data sharing practices.

Action Point:

- Patch all listed vulnerabilities urgently.
- Audit exposed services and enforce strong access controls.
- Monitor for malware and C2 activity using updated IoCs.
- Strengthen third-party oversight and incident response coordination.

Employees regularly paste company secrets into ChatGPT

https://www.theregister.com/2025/10/07/gen_ai_shadow_it_secrets/



A new report from cybersecurity firm **LayerX** reveals that employees are regularly pasting sensitive company data—including **personally identifiable information (PII)** and **payment card data (PCI)**—into generative AI tools like **ChatGPT**, often without permission or oversight.

The study found that:

- **45% of enterprise employees** use generative AI tools.
- **77% of those users** paste data into chatbot queries.
- **22% of those pastes** contain PII or PCI data.
- **82% of pastes** come from **unmanaged personal accounts**, creating a major blind spot for organisations.

This means sensitive data is being shared with external platforms, often outside corporate control, raising serious **compliance, privacy, and geopolitical risks**—especially when tools like **Chinese AI models** are involved.

LayerX also found that **40% of file uploads** to AI platforms contain sensitive data, with **39% of those uploads** coming from non-corporate accounts. The issue isn't limited to AI—shadow IT is rampant across chat apps, video conferencing, and CRM platforms.

Interestingly, while ChatGPT dominates enterprise AI usage (used by **over 90% of AI users**), Microsoft Copilot adoption is low—just **2–3%**, despite being integrated into Microsoft 365. This suggests employees prefer tools they're familiar with, even if they're not officially sanctioned. This isn't just an IT issue—it's a **cross-functional governance challenge**.

Action Point:

- **Implement Single Sign-On (SSO)** – Enforce SSO across all critical apps to gain visibility into data flows and reduce shadow IT.
- **Monitor Browser-Based AI Use** – Use enterprise browser extensions or DLP tools to track AI interactions and uploads.

- **Educate Employees on AI Risks** – Run awareness campaigns about the dangers of pasting sensitive data into public AI tools.
- **Establish Clear AI Usage Policies** – Define what's allowed, what's not, and which tools are approved for use.
- **Audit Shadow IT Activity** – Regularly review usage of non-corporate accounts across AI, chat, and productivity platforms.
- **Engage Compliance and Legal Teams** – Ensure AI usage aligns with GDPR, PCI-DSS, and other regulatory frameworks.



Too Authentic to be Synthetic: The Psychology Behind AI Voice Scams

<https://www.digit.fyi/psychology-behind-ai-voice-scams/>

As AI-generated voices become indistinguishable from real ones, new research from **Dr Neil Kirk at Abertay University** reveals a troubling psychological vulnerability: people are more likely to trust voices that sound like their own. This means that **regional accents**, once a barrier to voice tech, are now a **tool for deception**.

Kirk's study shows that when people hear AI-enhanced voices mimicking local dialects—like Dundonian Scots—they instinctively assume the voice is human. This “**default-to-human**” bias is deeply rooted and hard to override, making it easier for scammers to bypass scepticism and impersonate trusted sources like banks, family members, or government services.

Unlike targeted voice cloning scams that require training on specific individuals, this new threat is **scalable and low-cost**. With tools like **ElevenLabs**, fraudsters can generate convincing synthetic voices using just a few seconds of audio. The result? Mass-market scams that feel personal and local.

A survey by **Starling Bank** found that while a quarter of UK adults have been targeted by AI voice scams, nearly half didn't even know this type of fraud existed. That's a huge awareness gap—and a growing risk.

Why Traditional Training Isn't Enough

Kirk's research also challenges the effectiveness of current security awareness training. Teaching people to spot deepfakes only improved detection by **3%**. Instead, Kirk found that **nudging people's assumptions**—by simply telling them AI can mimic local accents—**doubled recognition rates**.

This suggests that the solution isn't technical—it's **psychological**. Organisations need to shift how people think about AI, not just how they spot it. This isn't just a tech problem—it's a human one.

Action Point:

1. **Update Staff Awareness Campaigns** – Focus on changing assumptions, not just spotting fakes. Use nudges to highlight how realistic AI voices can sound.
2. **Review Voice Authentication Protocols** – Consider multi-factor verification for voice-based interactions.
3. **Monitor for Regional Accent Exploits** – Be alert to scams using local dialects to build trust.
4. **Educate students** – Let them know AI voice scams exist and how to respond.

SC3 Daily Threat Summaries and Weekly Report

<https://www.cyberscotland.com/news/daily-threat-reports/>



A daily breakdown of various cyber threats from the Scottish Cyber Coordination Centre (SC3)

Action Point:

All SC3 threat intelligence in one place.

All the best from all of us at **HEFESTIS** and look out for our next **Threatscape** update next week.

HEFESTIS Limited, Registered Office: Unit 27, Stirling Business Centre, Wellgreen, Stirling FK8 2DZ

Incorporated in Scotland SC603511

CISO-Share Office Weekly Newsletter

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.

Table of Contents

CISO-Share Office Weekly Newsletter	1
SC3 Daily Threat Summaries and Weekly Report	1
‘A Call to Arms’ as UK Faces 50% Surge in Major Cyberattacks.....	2
Banking Scams Up 65% Globally in Past Year	3
Cyberattackers Target LastPass, Top Password Managers.....	4
Microsoft Revokes Over 200 Certificates to Disrupt Ransomware Campaign	5
Data BreachesF5 Hack: Attack Linked to China, BIG-IP Flaws Patched, Governments Issue Alerts	6
Acumen Cyber Threat Intelligence Digest – 15/10/2025, Week 41:.....	7

SC3 Daily Threat Summaries and Weekly Report



Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

This week's reports:



SC3-Daily-threat-bu SC3-Daily-Threat-BuSC3-Daily-threat-bu SC3-Daily-threat-bu SC3-Daily-threat-bu
lletin-13-October-20lletin-14-October-20lletin-15-October-20lletin-16-October-20lletin-17-October-20



SC3-Weekly-Vulner
ability-Report-13-Oc



'A Call to Arms' as UK Faces 50% Surge in Major Cyberattacks

Cyberattacks are on the rise in the UK, according to the National Cyber Security Centre (NCSC), the UK's technical authority for cybersecurity.

[Main Article](#)

In its Annual Review, published on Tuesday, the security agency states that the UK has experienced a 50% increase in "highly significant" cyberattacks over the past year. Officials attributed the surge to the UK's increasing dependence on digital systems and a sharp increase in ransomware activity targeting organisations for financial gain.

Figures from the NCSC [annual review](#) revealed dramatic insights into the state of the UK's cybersecurity, including that it is experiencing the highest level of malicious digital activity recorded in nearly a decade, as the organization faces a new nationally significant cyber incident roughly every other day.

More bad actors than Hollywood

According to the report, the primary threats to security causing the 50% spike are state-sponsored actors from China, Iran, North Korea, and Russia, and underscored Russia's role in inspiring informal "hacktivist" groups that have launched disruptive attacks on the UK, the US, and other European and NATO countries.

Action Point: London calling

The UK government responded by issuing a "call to arms" to organizations, urging them to strengthen their cyber defenses and create contingency plans in the eventuality that their IT infrastructure is impacted.

"Cybersecurity is now a matter of business survival and national resilience," stated Richard Horne, the NCSC's chief executive, in a speech delivered at the Annual Review 2025 launch event on October 14 at NCSC headquarters in London.

Senior ministers, including Chancellor Rachel Reeves and Security Minister Dan Jarvis, have stressed to business leaders that cyber-resilience must be treated as a board-level responsibility.

"Cybercrime is a serious threat to the security of our economy, businesses, and people's livelihoods," said Jarvis. "While we work round the clock to counter threats and provide support to businesses of all sizes – we cannot do it alone."

The NCSC also warns of the growing role of artificial intelligence in cybercrime, predicting that AI-enhanced attacks will "almost certainly pose cyber-resilience challenges to 2027 and beyond."



Banking Scams Up 65% Globally in Past Year

A new report from BioCatch, a behavioral biometrics company specializing in financial crime prevention, reveals a dramatic global surge in scams — up 65% over the past year.

[Main Article](#)

Drawing data from financial institutions serving nearly 350 million consumers across five continents, the report highlights explosive growth in multiple scam types. Voice phishing (vishing) attempts doubled, romance scams rose by 63%, and investment scams climbed 42%. Meanwhile, SMS-based phishing skyrocketed — increasing tenfold year over year.

“While these numbers are staggering, they probably won’t surprise anyone,” BioCatch Director of Global Fraud Intelligence Tom Peacock said. “Fraud and anti-money laundering team leaders at the world’s largest banks fight through this scamming onslaught every single day, while the rest of us have undoubtedly noticed a marked surge in scammy text messages, emails, phone calls, and social posts.”

The exploited

According to the [report](#), purchase scams remain the most common form of fraud globally, with a 14% increase in attempts this year.

Action Point: “These aren’t backroom operations or something happening in the shadows,” Operation Shamrock Founder Erin West said. “Entire cities are now dedicated to scams, operating openly, protected, and expanding. They’re boomtowns, but instead of producing goods, their industry is fraud.”

Despite the grim findings, there is one bright spot: BioCatch customers reported a 15% decline in impersonation scams, which the company attributes to wider adoption of behavioral intelligence tools. In July, BioCatch launched Scams360, a platform designed to help banks detect and prevent complex social engineering schemes such as romance, investment, and business email compromise scams.



Cyberattackers Target LastPass, Top Password Managers

Major password managers are being impersonated in a spate of recent phishing attacks, including LastPass, Bitwarden, and 1Password, and enterprise users should be on notice. In a three-week span, all of them have been dealing with impersonation attacks by threat actors trying to con users into handing over their master password — and with it, troves of sensitive credentials.

Main Article

Password management vendors have long been among hackers' favorite brands to impersonate, for good reason. Users need to have complete trust in their password managers — after all, nobody would store all of their credentials for all of their accounts in an app they didn't have total confidence in. Phishers try to exploit that trust.

Action Point: "LastPass offers configurations that introduce friction into the authentication process to thwart attacker activity even if they do obtain valid customer credentials," says Alex Cox, director of the Threat Intelligence, Mitigation, Escalation (TIME) team at LastPass. Employees have the option to utilize a variety of multifactor authentication (MFA) protections, including passkeys and hardware tokens, and app alerts can block account logins from unrecognized locations.



Microsoft Revokes Over 200 Certificates to Disrupt Ransomware Campaign

Vanilla Tempest, also known as Vice Spider and [Vice Society](#), has been around since at least 2021, mainly known for its ransomware attacks on the education and healthcare sectors.

[Main Article](#)

Vice Society had its own leak website until 2023, disappearing at around the time when the notorious [Rhysida](#) ransomware emerged. The threat group has been known to deploy various file encryptors in its attacks, including BlackCat, Quantum Locker, and Zeppelin, but recently it has mainly used Rhysida ransomware.

Microsoft said it [disrupted a Vanilla Tempest campaign](#) in early October by revoking more than 200 certificates used by the cybercriminals to sign their malware.

According to the tech giant, the hackers signed fake Microsoft Teams setup files designed to install a backdoor named Oyster, which in turn would enable them to deploy Rhysida ransomware.

The fake Teams installers were delivered through websites hosted on domains such as 'teams-download.buzz' and 'teams-install.run'. Victims were likely lured to these sites through SEO poisoning.

When victims ran the fake Teams setup files, they executed a loader that downloaded a signed version of the Oyster backdoor, which has been used by Vanilla Tempest since at least June 2025. The cybercriminals started signing the backdoor in early September.

Action Point: Microsoft's actions make the malware distributed by Vanilla Tempest easier to detect and block, and the immediate impact on the cybercrime operation may be significant, but the threat actors will likely re-arm with new certificates and slightly modified tactics.



Data Breaches F5 Hack: Attack Linked to China, BIG-IP Flaws Patched, Governments Issue Alerts

More information has come to light on the cyberattack disclosed on Wednesday by security and application delivery solutions provider F5.

Main Article

[F5 blamed the attack](#) on an unspecified nation-state threat actor. Immediately after the news broke, [SecurityWeek](#) reported that the attack profile points to China as the potential threat actor.

Chinese hackers are known to [target BIG-IP appliances](#). In addition, Google reported recently that Chinese cyberspies had targeted SaaS and technology companies in an effort to obtain valuable data, including source code that could be analyzed in search for zero-day vulnerabilities. The attack involved a piece of malware named [Brickstorm](#).

Although it has not publicly said so, F5 also believes China is behind the attack, according to a report by [Bloomberg](#). The publication also reported that F5 has been providing customers a threat hunting guide focusing on the Brickstorm malware.

F5 customers have been told that the hackers dwelled in the company's network for at least 12 months, which is in line with Google's recent Brickstorm report, which stated that the Chinese cyberspies had lurked in victims' networks, on average, for nearly 400 days.

Google Threat Intelligence Group and Mandiant linked the Brickstorm attack to a threat actor tracked as UNC5221.

Mandiant and CrowdStrike have been called in to assist F5 with investigating the incident and securing its systems.

F5 said the hackers, whose presence was discovered on its systems on August 9, had accessed and exfiltrated some files, including source code of its BIG-IP flagship platform and information on undisclosed vulnerabilities.

Action Point: "The threat actor's access to F5's proprietary source code could provide that threat actor with a technical advantage to exploit F5 devices and software," CISA said. "The threat actor's access could enable the ability to conduct static and dynamic analysis for identification of logical flaws and zero-day vulnerabilities as well as the ability to develop targeted exploits."

The UK's National Cyber Security Centre (NCSC) issued similar [recommendations](#), noting, "Successful exploitation of the impacted F5 products could enable a threat actor to access embedded credentials and API keys, move laterally within an organisation's network, exfiltrate data, and establish persistent system access."



Acumen Cyber Threat Intelligence Digest – 15/10/2025, Week 41:

[Main Article](#)

Significant active exploitation and diverse threat activity mark this intelligence digest. Wordfence disclosed on 7 October 2025 active exploitation of CVE-2025-5947 in the Service Finder Bookings plugin (≤ 6.0), which permits unauthenticated account takeover and admin impersonation via a crafted `original_user_id` cookie; Aonetheme released v6.1 on 17 July 2025 but many instances remain unpatched and Wordfence blocked over 13,800 attempts.

Researcher David Leadbeater published analysis of OpenSSH ProxyCommand control-character injection (CVE-2025-61984), fixed in OpenSSH 10.1 (6 October 2025), where injected newlines in usernames can break shell parsing and run commands.

Rapid7 and CISA reported active exploitation of Cisco ASA/FTD missing authorization (CVE-2025-20362) enabling WebVPN file-upload traversal and buffer overflow, linked to RayInitiator and LINE VIPER deployments. CLOP exploited Oracle E-Business Suite zero-day CVE-2025-61882 for extortion and data theft, using XSL/DB templates and in-memory Java payloads. macOS ZuRu backdoor resurfaced via a trojanized Termius bundle, now using an embedded helper binary loader.

TA585 ran ClickFix and GitHub-themed phishing to deliver stealers (LummaC2, Rhadamanthys, MonsterV2). UK reported a record surge in nationally significant incidents; Ukraine advanced creation of a Cyber Force.

Ongoing campaigns show credential theft, targeted extortion, and sophisticated persistence techniques. Defenders should prioritise patching, monitoring, and incident response preparedness immediately now.

Action Point: Remediation Actions

Following the information provided above, we recommend that the technologies mentioned be fully patched and updated. We also want to highlight and recommend applying the following patches where applicable:

- **CVE-2025-5947:** Updating the associated Wordpress plugin to the latest available version will help mitigate this risk.
- **CVE-2025-61984:** Updating to the newly released OpenSSH 10.1, which rejects control characters in usernames can mitigate this vulnerability.
- **CVE-2025-20362:** Applying Cisco's recommended vendor patches, added to KEV in September 2025 can help mitigate this risk.

All the best from all of us at HEFESTIS and look out for a new ThreatScape update next week.



CISO Share

Threatscape

A very warm welcome to all of you from all of us at the CISO-Share Office.

Here are a few of the articles which caught the attention of the CISO-Share team this week.

If you have any questions or comments, please feel free to contact us via CISO-Office@hefestis.ac.uk.



[The Best End User Security Awareness Programs Aren't About Awareness Anymore](#)

Most cyberattacks today target people, not just systems. Whether it's phishing emails or social engineering, attackers are exploiting human behaviour. Experts argue that we need to move from "security awareness" to human risk management . It's not e...

Steve McIntosh

10/24/2025



[The Unkillable Threat: How Attackers Turned Blockchain Into Bulletproof Malware Infrastructure](#)

Cyber attackers have found a terrifyingly effective new tool: the blockchain. Originally designed to promote trust and transparency, blockchain's core features— decentralisation, immutability, and global access —are now being exploited to create mal...

Steve McIntosh

10/23/2025



[Acumen Cyber Threat Intelligence Digest: Week 42](#)

This week's digest highlights several vulnerabilities and threat campaigns that could impact universities and colleges—especially those with open-source tools, remote access services, and developer environments. Key Vulnerabilities to Patch ConnectW...

Steve McIntosh

10/23/2025



[SC3 weekly threat reports](#)

Action Point: Please find SC3's daily threat summaries for this week for those who do not receive this information directly.

Steve McIntosh

10/23/2025



[Hundreds of Misplaced Devices Put University Data at Risk](#)

A recent investigation has revealed that nearly 700 laptops, tablets, and phones have been lost or stolen across Russell Group universities in the past three years. The data, obtained via FOI and analysed by Parliament Street Think Tank, highlights ...

Steve McIntosh

10/22/2025



[Researchers Sound Alarm as LAPSUS\\$ Launch 'Extortion-as-a-Service'](#)

Cybersecurity researchers at Palo Alto Networks' Unit 42 have uncovered new developments linked to the Scattered LAPSUS\$ Hunters group—one of the most disruptive cybercriminal syndicates operating today. The group is now pivoting to a new model: Ext...

Steve McIntosh

10/22/2025

[Go To Site](#)

 [Get the SharePoint Mobile App](#)



This email is generated through HEFESTIS Ltd's use of Microsoft 365 and may contain content that is controlled by HEFESTIS Ltd.