



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

The Strategic Framework for a Cyber Resilient Scotland 2025 - 2030 2

Malware Now Uses AI During Execution to Mutate and Collect Data, Google Warns 3

Hacker Conversations: Kunal Agarwal and the DNA of a Hacker 4

Ground zero: 5 things to do after discovering a cyberattack 5








Acumen Cyber Threat Intelligence Digest: Week 44 6

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
lletin-3-November-21
- 
SC3-Daily-threat-bu
lletin-4-November-21
- 
SC3-Daily-threat-bu
lletin-5-November-21
- 
SC3-Daily-Threat-Bu
lletin-06112025.pdf
- 
SC3-Daily-threat-bu
lletin-7-November-2
- 
SC3 - Monthly
Ransomware Reportability-Report-3-Nov
- 
SC3-Weekly-Vulner



The Strategic Framework for a Cyber Resilient Scotland 2025 - 2030

This framework is a refresh of the Strategic Framework for a Cyber Resilient Scotland 2021. In the face of an ever-changing cyber threat landscape, it will build on progress to date and address ongoing - and new - challenges.

Main Article

Scotland thrives by being a digitally secure and resilient nation.

Cyber Upskilling Funding: Public Sector

Are you a public sector organisation interested in upskilling your existing employees in Cyber Security qualifications at no cost to your business?

Funding Information

We are pleased to open applications for the fourth round of the **Public Sector Cyber Upskilling Fund**, funded by the **Scottish Government's National Cyber Resilience Unit**. This contributes towards the ambitions of *A Strategic Framework for a Cyber Resilient Scotland*.

The aim of the fund is to help public sector organisations improve the Cyber Security skills of their employees, which in turn will help to make the organisation more cyber resilient.

We want to support diversity and inclusivity in Scotland's public sector, and therefore encourage applications from learners who meet Equality, Diversity and Inclusion criteria.

As an employer you can claim up to £5,000 per learner (maximum of £7,000 per organisation) to pay for cyber skills training for your cyber/information security compliance professionals and internal auditors (or those who are performing those functions); simply fill out an application for the employees you would like to upskill including course or qualification details and costs.

Action Point: Organisations have the flexibility to choose any training provider they prefer – whether based in Scotland, elsewhere in the UK, or globally – as long as the training aligns with the Cyber Security qualifications you wish to deliver. This ensures you can select the provider that best meets the needs of your employees and organisation.

To be eligible, your organisation must be registered or based in Scotland, be recognised as a public sector organisation, and training must be secured by **31st March 2026**.

This is a quick and easy way to access skills funding for employees, nurturing your workforce and adding value to your organisation.

You can apply now for the fund [here](#).



Malware Now Uses AI During Execution to Mutate and Collect Data, Google Warns

Google's Threat Intelligence Group (GTIG) has seen several new and interesting ways in which malware has been leveraging artificial intelligence, going beyond its use for productivity gains.

Main Article

For some time now cybercriminals and state-sponsored threat actors have been leveraging AI to develop and enhance malware, plan attacks, and create social engineering lures.

The cybersecurity industry has also observed and demonstrated the potential for malware to utilize AI during execution.

For instance, the PromptLock ransomware, which made headlines a few months ago over its use of AI to generate scripts on the fly and perform various actions on compromised systems, is an experimental proof-of-concept developed by researchers.

However, Google researchers have come across several other pieces of malware that use AI during an attack. While some of them have been described as "experimental threats", such as PromptLock, others have been used in the wild.

Another experimental AI-powered malware seen by Google is PromptFlux, a dropper that can "regenerate" itself by rewriting its code and saving the new version in the Startup folder for persistence.

Action Point: "While adversaries are certainly trying to use mainstream AI platforms, guardrails have driven many to models available in the criminal underground," explained Billy Leonard, tech lead at Google Threat Intelligence Group. "Those tools are unrestricted, and can offer a significant advantage to the less advanced. There are several of these available now, and we expect they will lower the barrier to entry for many criminals."

In addition, nation-state actors linked to China, Iran and North Korea have continued to use Google's Gemini to enhance reconnaissance, data exfiltration, command and control systems, and other components of their operations.



Hacker Conversations: Kunal Agarwal and the DNA of a Hacker

Kunal Agarwal's cybersecurity journey takes him from the edge of Juvenile Hall to the founder and CEO of [dope.security](#).

Main Article

[Dope.security](#) provides a secure web gateway. It is designed to stop hackers making hay from websites. But its founder was, is, and will always be, a hacker.

Early days

"I was born and raised in California, but I started as a bit of a child hacker," he says. He was around nine years old, more than 20 years ago, and was at the age where he wanted to do things he shouldn't do or couldn't afford to do.

"It was a time of, hey, how do I watch this movie that I'm not allowed to go in and watch, and I can't go in and watch at home. So, I entered this world of wondering how to download a movie or a game for free."

This basic curiosity caused him to learn how emulators and ROMs work so that, if he could pirate a Nintendo game, he would be able to play it on a PC. It was the start of understanding technology.

It is worth interjecting that this behaviour is just a hop, skip and a jump from social engineering – a term that we usually limit to serious bad guys, but is really something everyone does in all aspects of daily living. Notice that the Agarwal child wanted to find ways to see movies and play games that he couldn't.

Action Point: If we assume that he is right, and that hacking is part of the hacker's DNA, then we can assume that the origin of hacking is an inescapable part of the hacker's nature. But that alone does not explain why we have different categories of hacker: black, white, grey, ethical, and nation-state. This comes from the hacker's environmental pressures pointing them in a specific direction. It implies a description of the hacker as a person driven by nature but shaped by nurture.



Ground zero: 5 things to do after discovering a cyberattack

Network defenders are feeling the heat. The number of data breaches [Verizon](#) investigated last year, as a share of overall incidents, was up 20 percentage points on the previous year. This need not be as catastrophic as it sounds, as long as teams are able to respond rapidly and decisively to intrusions. But those first minutes and hours are critical.

[Main Article](#)

Preparation is the key to effective incident response (IR). Although every organization (and incident) is different, you don't want to be making stuff up on the fly once the alarm bells have begun ringing. If everyone in the incident response team knows exactly what to do, there's more chance of a swift, satisfactory and low-cost resolution.

The need for speed

Once threat actors get inside your network, the clock is ticking. Whether they are after sensitive data to steal and ransom, or want to deploy ransomware or other malicious payloads, the key is to stop them before they're able to reach your crown jewels. This is becoming more challenging.

The [latest research](#) claims that adversaries progressed from initial access to lateral movement (aka "breakout time") 22% faster in 2024 than the previous year. The average breakout time was 48 minutes, although the fastest recorded attack was almost half that: just 27 minutes. Could you respond to a security breach in under half an hour?

Action Point: A strong post-incident culture treats every breach as a training exercise for the next one, improving defenses and decision-making under stress.

Beyond IT

It's not always possible to prevent a breach, but it is possible to minimize the damage. If your organization doesn't have the resources to monitor for threats 24/7, consider a managed detection and response (MDR) service from a trusted third party. Whatever happens, test your IR plan, and then test it again. Because successful incident response isn't just a matter for IT. It requires a number of stakeholders from across the organization and externally to work together in harmony. The kind of muscle memory you all need usually requires plenty of practice to develop.



Acumen Cyber Threat Intelligence Digest: Week 44

5th November 2025 - Threat Report

[Main Article](#)

Adobe has patched a critical “SessionReaper” flaw (CVE-2025-54236) in Adobe Commerce and Magento platforms after over **250 exploitation attempts** were detected in the wild. Around **62% of Magento stores remain unpatched**, leaving many still exposed. Meanwhile, **Kinsing** threat actors exploited **Apache ActiveMQ (CVE-2023-46604)** to deploy malware including **Cobalt Strike, Meterpreter, and XMRig** for crypto-mining and remote access. **Atlassian** also fixed a **high-severity path traversal bug (CVE-2025-22167)** in Jira Software and Service Management, though no active exploitation has been observed.

Kaspersky linked Italian spyware vendor **Memento Labs** to **Operation ForumTroll**, a Chrome (CVE-2025-2783) exploitation campaign targeting Russian and Belarusian organizations using **LeetAgent** and **Dante spyware**. Separately, **Koi Security** uncovered **PhantomRaven**, a supply-chain attack via **126 malicious npm packages** stealing GitHub and CI/CD credentials. **Varonis** identified a flaw in **Azure’s** app registration process that allowed the creation of fake Microsoft apps through Unicode manipulation.

In broader developments, a new **cybercrime alliance, “Scattered LAPSUS\$ Hunters,”** merges **Scattered Spider, LAPSUS\$, and ShinyHunters**, signaling a shift toward **extortion-as-a-service** models. A **Microsoft Azure outage** on 29 October disrupted major global sites, while researchers revealed a novel **AI cloaking attack** that feeds **false data to AI crawlers**, highlighting emerging risks at the intersection of cybersecurity and AI.

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-2025-22167:** This vulnerability can be remediated by updating to version 9.12.28, 10.3.12, 11.1.0
- **CVE-2025-54236:** This vulnerability can be remediated by installing the hotfix VULN-32437-2-4-X-patch from Adobe.
- **CVE-2023-46604:** Users are recommended to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue.

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.

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

11/14/2025

6 views

When Attacks Come Faster Than Patches: Why 2026 Will be the Year of Machine-Speed Security

Cybersecurity is entering a new era where attackers move at machine speed—and defenders are still stuck at human speed. Here's the reality: 50–61% of new vulnerabilities are exploited within 48 hours of disclosure . That's not weeks or days—it's hou...

Steve McIntosh

11/14/2025

5 views

What happens when employees take control of AI

A recent Moveworks study flips the usual narrative: AI isn't just a top-down initiative

anymore. It's employees—often non-technical ones—who are pushing AI into everyday workflows. What started as small experiments is now transforming entire operati...

Steve McIntosh

11/14/2025

3 views

Public Sector Cyber Resilience Network - Action Plan

This is an invite to hear more about the updated The Strategic Framework for a Cyber Resilient Scotland (launched last week), a chance to input to the development of the supporting action plan for the public sector that will be published early next ...

Steve McIntosh

11/12/2025

10 views

Acumen Cyber Threat Intelligence Digest: Week 45

Major Exploits Cisco ASA & FTD Firewalls : Two flaws (CVE-2025-20333 and CVE-2025-20362) are being hammered in DDoS attacks. These can lead to full device compromise and even endless reboot loops, knocking networks offline. Over 34,000 devices are s...

Steve McIntosh

11/12/2025

7 views

Two New Web Application Risk Categories Added to OWASP Top 10

The Open Web Application Security Project (OWASP) has released a revised version of its Top 10 list of critical risks to web applications, adding two new categories and reshuffling the overall list order. Main Article This 2025 release candidate, wh...

David Robertson

11/12/2025

13 views

Google Warns of AI-Driven Threat Escalation in 2026

The cybersecurity landscape is entering a defining moment as organizations prepare for a rapidly evolving threat environment in 2026. Main Article
According to Google Cloud's Cybersecurity Forecast 2026 report , threat actors are fully operationaliz...

David Robertson

11/12/2025

14 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.



When Attacks Come Faster Than Patches: Why 2026 Will be the Year of Machine-Speed Security

<https://thehackernews.com/2025/11/when-attacks-come-faster-than-patches.html>

Cybersecurity is entering a new era where attackers move at machine speed—and defenders are still stuck at human speed. Here's the reality: **50–61% of new vulnerabilities are exploited within 48 hours of disclosure**. That's not weeks or days—it's hours. Attackers have automated everything, and they're using AI to make it even faster.

The Race for Every CVE

- The moment a new vulnerability hits public databases, threat actors deploy automated scripts to scrape, analyse, and weaponise it.
- Exploit kits are packaged and shared across dark web forums within hours.
- Meanwhile, IT teams are still reading advisories, classifying severity, and queuing patches for the next cycle. That delay is the gap attackers exploit.

Why Attackers Win

- They operate on **volume, not precision**. Crashing 1,000 systems to compromise 100 is acceptable.
- They don't care about uptime or stability—defenders do.
- They invest heavily in automation and AI, treating offensive capability as a business priority.

The Defender's Dilemma

Quarterly or monthly patching cycles are dead. Awareness isn't the issue—execution speed is. Manual, ticket-based patching can't keep up. Every hour between disclosure and remediation is a risk window.

The Fix: Machine-Speed Defence

- **Automate patching and hardening:** Move from manual triage to policy-driven orchestration.

- **Controlled rollback:** Accept that occasional disruption is better than a full-scale breach.
- **Standardise and streamline:** Reduce manual steps, segment legacy systems, and eliminate bottlenecks in change management.

Automation isn't just about speed—it reduces burnout and error. Instead of chasing alerts, teams define rules once and let systems enforce them continuously.

Reality Check

Attackers are building fully automated pipelines, even using AI to develop exploits. They work 24/7, never tire, and don't care about consequences. If you're fighting a machine, you need a machine on your side.

Action Point:

- **Accelerate patching:** Adopt automated platforms for rapid, governed remediation.
- **Review policies:** Remove approval bottlenecks slowing critical updates.
- **Segment legacy systems:** Make them more automatable or isolate them.
- **Invest in orchestration tools:** Combine automation with rollback safeguards.
- **Shift mindset:** Prioritise speed over perfection—controlled risk beats compromise.
- **Prepare for AI-driven attacks:** Update detection and response strategies for machine-speed threats.



What happens when employees take control of AI

<https://www.helpnetsecurity.com/2025/11/14/moveworks-employee-led-ai-adoption-report/>

A recent Moveworks study flips the usual narrative: AI isn't just a top-down initiative anymore. It's employees—often non-technical ones—who are pushing AI into everyday workflows. What started as small experiments is now transforming entire operations.

What's Happening?

- **Ground-Up AI Adoption:** Staff closest to the work are spotting inefficiencies and using AI to fix them—without waiting for leadership approval. This means automation is spreading faster than governance can keep up.
- **Agentic AI in Action:** These systems don't just analyse—they execute. They're handling multi-step tasks like onboarding, IT support, and finance requests. About a

third of executives say AI has already reshaped major parts of their business.

- **New Roles Emerging:** Companies are creating positions like AI project coordinator, prompt writer, and automation manager. Leadership skills are shifting—knowing how to apply AI may matter more than traditional management experience.

The Cultural Shift

Executives admit they underestimated AI's impact. It's not just about cost savings anymore; it's about how work gets done. Measuring success now includes looking at collaboration, speed, and reduced friction. The future belongs to those who empower employees, not just deploy tools.

The Risk Factor

AI adoption is outpacing governance. Leaders need visibility into:

- Where AI is being used
- What data it touches
- Compliance and security implications

Security teams must pivot from blocking AI to enabling safe use. Partnering with employees who understand operational pain points can turn risk into opportunity.

Why It Matters

The question isn't "Will employees accept AI?"—they already have. The challenge is managing enthusiasm, experimentation, and risk. Training and communication around data handling, bias, and automation are just as critical as technical safeguards.

Action Point:

- **Map AI Usage:** Identify where employees are using AI and what data is involved.
 - **Update Governance:** Adapt risk frameworks to cover AI-driven workflows.
 - **Enable Secure Innovation:** Shift security posture from restriction to safe enablement.
 - **Invest in Skills:** Create roles for AI coordination and prompt engineering.
 - **Train & Communicate:** Build awareness around compliance, bias, and responsible automation.
 - **Measure Impact Differently:** Look beyond cost savings—focus on workflow improvements and employee empowerment.
-

Public Sector Cyber Resilience Network - Action Plan

This is an invite to hear more about the updated [The Strategic Framework for a Cyber Resilient Scotland](#) (launched last week), a chance to input to the development of the supporting action plan for the public sector that will be published early next year as well as catch up on any other Cyber Resilience Unit / Scottish Cyber Coordination Centre business, including the [Public Sector Cyber Upskilling Fund](#) (also launched last week) and the imminent Cyber Security and Resilience Bill.

You can register for the webinar from the link, this session isn't being recorded but the slides and significant points will be available afterwards for all to see.

<https://events.teams.microsoft.com/event/2cdf7a5d-c16f-49c5-88b9-9dec0ae14951%400ef77447-1083-4dec-b89f-27c765076840>

Action Point:

Sign up!



Acumen Cyber Threat Intelligence Digest: Week 45

<https://acumencyber.com/cyber-threat-intelligence-digest-november-2025-week-45>

Major Exploits

- **Cisco ASA & FTD Firewalls:** Two flaws (CVE-2025-20333 and CVE-2025-20362) are being hammered in DDoS attacks. These can lead to full device compromise and even endless reboot loops, knocking networks offline. Over **34,000 devices** are still exposed. If you haven't patched since September, you're in the danger zone.
- **WordPress Post SMTP Plugin:** CVE-2025-11833 lets attackers hijack admin accounts by exploiting email logs. Over **210,000 sites** remain vulnerable despite a patch being out since October.
- **Samsung Galaxy Devices:** CVE-2025-21042 is being used to deploy **LANDFALL spyware**, targeting Android 13–15. It's nasty—steals audio, messages, and files. Patch was released in April, but attackers are still active.

Emerging Threats

- **Supply Chain Attack via npm:** Seventeen malicious npm packages were found delivering Vidar infostealer. Over 2,000 downloads before removal. This is a wake-up call for developers—open-source ecosystems remain a big risk.
- **XWorm RAT via PNG Files:** A clever phishing campaign hides malware in PNGs, using PowerShell for in-memory execution. It's stealthy and persistent.
- **Hospitality Sector Phishing:** PureRAT malware is being deployed through fake Booking.com emails, compromising hotel admin accounts and leading to guest payment fraud.

Industry Trends

- UK mobile carriers are cracking down on spoofed numbers—expect better fraud prevention soon.
- Google warns of **AI-powered malware** that self-modifies mid-execution. This is the next frontier in evasion.
- Cyber insurance payouts in the UK surged **230%**, mostly due to ransomware. Insurance is not a substitute for strong security.

Action Points

1. **Patch immediately:**
 - Cisco ASA/FTD: Apply September and November advisories.
 - WordPress Post SMTP: Upgrade to v3.6.1 or later.
 - Samsung Galaxy: Ensure April 2025 security update is installed.
 2. **Audit npm dependencies:** Remove any suspicious packages and lock down your supply chain.
 3. **Strengthen phishing defences:** Train staff, enable MFA, and monitor for Booking.com-themed lures.
 4. **Prepare for AI-driven threats:** Review detection capabilities and consider behaviour-based monitoring.
 5. **Review cyber insurance:** Ensure coverage aligns with your risk profile, but don't rely on it alone.
-



Two New Web Application Risk Categories Added to OWASP Top 10

<https://www.securityweek.com/two-new-web-application-risk-categories-added-to-owasp-top-10/>

The Open Web Application Security Project (OWASP) has released a revised version of its Top 10 list of critical risks to web applications, adding two new categories and reshuffling the overall list order.

This 2025 release candidate, which is a near-final draft of the flagship OWASP Top 10 list, is open for comment until November 20.

Broken Access Control has maintained the leading position on the [2025 OWASP Top 10 list](#), after climbing there in 2021. The Broken Access Control category now incorporates server-side request forgery (SSRF), which was previously separate and tenth on the list.

Security Misconfiguration is now second on the list, up from fifth in the [2021 OWASP Top 10](#), followed by Software Supply Chain Failures, an expansion of Vulnerable and Outdated Components, which was previously sixth.

The expanded category includes “a broader scope of compromises occurring within or across the entire ecosystem of software dependencies, build systems, and distribution infrastructure,” OWASP notes, pointing out that it emerged as a top concern in the community survey.

Action Point:

“We plan to do additional data analysis as a supplement in the future. This significant increase in the number of CWEs necessitates changes to how the categories are structured,” OWASP notes.

However, the team used CVE data for Exploitability and (Technical) Impact, and calculated average exploit and impact scores by grouping CVEs with CVSS scores by CWE and looking at the percentage of applications that had CVSSv3 and CVSSv2 scores.

Due to the limits of automated testing, only eight categories have been selected from this data, which is considered incomplete. The other two categories come from the Top 10 community survey, in which practitioners vote for what they consider the highest risks.



Google Warns of AI-Driven Threat Escalation in 2026

<https://www.esecurityplanet.com/threats/google-warns-of-ai-driven-threat-escalation-in-2026>

The cybersecurity landscape is entering a defining moment as organizations prepare for a rapidly evolving threat environment in 2026.

According to Google Cloud's [Cybersecurity Forecast 2026 report](#), threat actors are fully operationalizing AI.

This [evolution](#) signals a paradigm shift in the global cyber threat ecosystem, demanding equally adaptive and intelligent defence strategies.

Google Cloud researchers report that adversaries have moved from using AI tools as occasional tactical aids to embedding them as foundational components of their operations. The normalization of AI-enabled attacks has dramatically increased both their speed and precision.

Where once human oversight limited scalability, automated [AI-driven attacks](#) can now identify vulnerabilities, craft deceptive messages, and execute breaches in minutes.

Action Point:

The report urges organizations to adopt proactive threat intelligence frameworks and multi-layered defence strategies.

This includes strengthening supply chain security, investing in real-time analytics, and cultivating a security culture that adapts as rapidly as adversaries innovate.

As the boundary between human and machine operations continues to blur, success in cybersecurity will depend on leveraging AI not only to respond but to anticipate.

Organizations must treat AI as both a potential threat vector and a powerful defensive ally.

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)

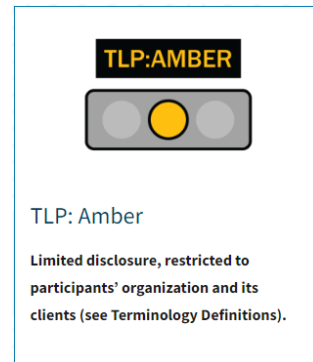
Action Point:

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



Threat Intelligence Priority Reporting (TIPR)

12 November 2025

Hello,

SC3 has been informed of a persistent Distributed Denial of Service (DDoS) attack against a Scottish public sector organisation and is sharing details to raise collective awareness across the community.

The organisation experienced the attack in the late evening of 10/11/25, with traffic volumes peaking at approximately 1,500 requests per second. Analysis confirmed this was not legitimate user activity.

Firewall logs identified multiple attack vectors originating from the following IP addresses:

- **179.43.173.12 (Switzerland)**
- **43.153.52.44 (United States)**

The organisation is continuing to monitor and mitigate the issue.

Please review these IOCs within your own environments and take any appropriate defensive measures. If you observe related activity or have additional intelligence, please get in touch

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
Gartner: 40% of Firms to Be Hit By Shadow AI Security Incidents	2
Chinese APT Infects Routers to Hijack Software Updates	3
Supply Chain Breaches Impact Almost All Firms Globally, BlueVoyant Reveals.....	4
WhatsApp Flaw Exposed 3.5 Billion User Accounts.....	5
Convenience culture is breaking personal security	6
Acumen Cyber Threat Intelligence Digest: Week 46	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-21-November-lletin-20-November-lletin-19-November-lletin-18-November-lletin-17-November-



SC3-Weekly-vulnera
bility-report-17-Nov



Gartner: 40% of Firms to Be Hit By Shadow AI Security Incidents

By 2030, more than 40% of global organizations will suffer security and compliance incidents due to the use of unauthorized AI tools, Gartner has predicted.

Main Article

The analyst said a survey of cybersecurity leaders earlier this year revealed that 69% have evidence or suspect that employees are using public generative AI (GenAI) at work.

It warned that such tools can increase the risk of IP loss, data exposure and other security and compliance issues. These should be well understood by now. As far back as 2023, Samsung was forced to ban the use of GenAI internally after staff shared source code and meeting notes with ChatGPT.

“To address these risks, CIOs should define clear enterprise-wide policies for AI tool usage, conduct regular audits for shadow AI activity and incorporate GenAI risk evaluation into their SaaS assessment processes,” said distinguished VP analyst Arun Chandrasekaran.

Gartner’s findings chime with several similar studies.

Action Point: “By establishing clear standards for reviewing and documenting AI-generated assets and tracking technical debt metrics in IT dashboards, enterprises can take proactive steps to prevent costly disruptions.”

The analyst also warned about ecosystem lock-in and the erosion of skills that could result from over-eager use of GenAI.

“To prevent the gradual loss of enterprise memory and capability, organizations should identify where human judgment and craftsmanship are essential, designing AI solutions to complement, not replace, these skills,” Chandrasekaran said.

He added that CIOs should prioritize open standards, open APIs and modular architectures when designing their AI stack, in order to avoid over-dependence on a single vendor.



Chinese APT Infects Routers to Hijack Software Updates

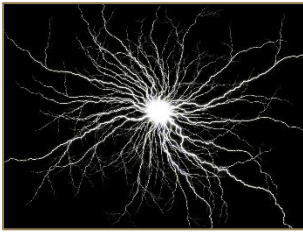
For more than half a decade now, a Chinese state-aligned threat actor has been spying on Chinese organizations by infecting their trusted software updates.

[Main Article](#)

When the [SolarWinds breach](#) was unearthed in 2020, it might have seemed like a uniquely devious event in cybersecurity history. But cyberattackers and cybersecurity researchers have been finding other, [novel ways of poisoning software updates](#) since then.

"PlushDaemon" is one such group that has quietly, for quite a while now, been taking its own approach to the update hijack. Like Chinese advanced persistent threats (APTs) often do, it infects organizations through their edge devices. But where most APTs use edge devices as initial entry points to deeper network compromise, researchers at ESET have found that PlushDaemon uses them in its own way. It hijacks network traffic using a specially designed implant, [re-routes legitimate software update requests](#) to its own infrastructure, and then serves victims malicious substitutes.

Action Point: "What we recommend defenders do," he says, "is be mindful of vulnerabilities in the devices that are in their networks, and to try to vet their credentials for vulnerabilities. That's it."



Supply Chain Breaches Impact Almost All Firms Globally, BlueVoyant Reveals

An overwhelming majority of organizations (97%) have been negatively impacted by [a supply chain breach](#), according to a new survey by BlueVoyant.

[Main Article](#)

This is a significant increase from 2024, when 81% of respondents to the same annual survey from the [third-party risk management](#) (TPRM) provider said they suffered from such an incident.

Sixty percent of respondents cite a lack of internal buy-in as a major obstacle, while communication with senior leadership is infrequent: only 24% brief executives monthly. Many programmes are still compliance-driven—only 16% focus primarily on reducing risk, with cyber-insurance and contractual demands being more common motivators.

Action Point: TPRM efforts also lack integration: even mature programmes are often siloed rather than part of broader enterprise risk strategies. Finally, organisations are growing their third-party networks faster than they can validate or remediate them, meaning added vendors may increase exposure faster than visibility or control can keep up.



WhatsApp Flaw Exposed 3.5 Billion User Accounts

Researchers uncovered a serious privacy flaw in WhatsApp that allowed them to **enumerate over 3.5 billion accounts worldwide**, including users in countries where the app is banned (China, Iran, Myanmar). The vulnerability was discovered by the University of Vienna and SBA Research and exploited WhatsApp's contact search mechanism.

[Main Article](#)

How the Flaw Worked

WhatsApp checks your phone's contacts to find other users. Researchers found they could abuse this process to send **unlimited queries**, confirming more than **100 million phone numbers per hour**. This allowed them to map active accounts across **245 countries**.

What Was Exposed

- **Phone numbers** and **public keys**.
- **Profile photos** (if set to public).
- **About Text** (sometimes revealing political, religious, or personal details).
- Metadata like **device OS**, **account age**, and **linked devices**. Even more worrying, **cryptographic keys were reused** in some cases, suggesting weaknesses in unofficial clients or fraudulent use.

The study also revealed:

- **2 million Chinese users** and **59 million Iranian users** active on WhatsApp despite bans.
- Nearly **half of the 500 million numbers leaked in Facebook's 2021 breach** are still active on WhatsApp.

Impact

Messages remain end-to-end encrypted, so content wasn't exposed. However, the ability to scrape personal data at scale poses huge privacy risks. Attackers could use this for profiling, phishing, or surveillance.

Meta's Response

Meta worked with researchers to patch the flaw and strengthen anti-scraping systems. The collected data was securely deleted, and there's **no evidence of malicious exploitation** so far.

A serious privacy flaw in WhatsApp let researchers map out 3.5 billion accounts and user phone numbers worldwide, thanks to a loophole in the app's system. The critical vulnerability, discovered by computer scientists at the University of Vienna and ...

Action Point:

- **Review Privacy Settings:**
 - Set profile photo and About Text to "Contacts Only" or "Nobody".
- **Educate Users:**
 - Warn about oversharing personal info in About Text.
- **Monitor for Enumeration Attacks:**
 - Implement rate-limiting and anomaly detection for API queries.
- **Audit Third-Party Clients:**
 - Block unofficial WhatsApp apps that may reuse cryptographic keys.



Convenience culture is breaking personal security

A new Bitdefender global survey reveals a worrying trend: scams are evolving faster than people can respond, thanks to AI. Over 70% of consumers encountered a scam in the past year, and 1 in 7 fell for one. AI-driven fraud is now mainstream, with 37% citing

deepfake audio/video as their top concern.

Main Article

AI Makes Scams Smarter

AI tools allow scammers to create convincing voices, videos, and personalised messages in seconds. They can mimic family members or colleagues, making it harder to spot fraud based on tone or wording. Even though people know the risks, habits haven't changed—and attackers are exploiting that.

Phones: The Weakest Link

- 53% of consumers do most transactions on mobile devices—banking, shopping, messaging, identity checks.
- Nearly half don't use any independent security tool on their phones.
- Reasons? Cost concerns and misplaced trust in built-in features. Older adults are especially likely to assume their device is “safe by default.” Unfortunately, attackers know this—and mobile-focused scams are rising fast.

Social Media: Scam Central

Social platforms have overtaken email, calls, and texts as the top scam channel. About one-third of respondents received a scam via social media. Oversharing is a big factor—66% post personal photos, videos, or life events. Younger users share more and are twice as likely to be scammed. Attackers harvest voice clips, travel photos, and relationship details to craft believable scripts or AI-generated imitations.

Convenience vs Security

People still reuse passwords, write them down, and only 25% use a password manager. Nearly half accept all cookies without checking settings. These shortcuts weaken privacy and make profiling easier. Victims of scams are even more likely to accept all cookies.

Trust and Fear

Consumers trust big tech (Google, Microsoft, Apple) more than platforms like TikTok or X—but still limit what data they share. Financial loss is the top fear (53%), followed by identity theft (17%). UK and Australia show the highest concern about financial attacks.

AI powered scams exploit weak mobile security, social media oversharing, and risky consumer habits worldwide.

Action Point:

- Educate users: Highlight AI-driven scam tactics and oversharing risks.
- Promote mobile security: Encourage installing reputable security apps.
- Push password hygiene: Advocate password managers and MFA.



Acumen Cyber Threat Intelligence Digest: Week 46

The latest Cyber Threat Intelligence Digest highlights significant vulnerability disclosures, active threat campaigns, and notable cybersecurity incidents across major vendors and global organisations. Cisco patched three flaws in its Catalyst Centre platform, including a high-severity privilege-escalation vulnerability (CVE-2025-20341) that could allow authenticated users to obtain administrator access. Two additional medium-severity issues—involving REST API command injection and unauthenticated cross-site scripting—were also remediated. Zyxel released firmware updates addressing two vulnerabilities affecting a wide array of its network devices, most notably CVE-2025-6599, an uncontrolled resource consumption flaw enabling Slowloris-style denial-of-service attacks. Mozilla issued patches for sixteen vulnerabilities in Firefox and ESR builds, fixing memory-corruption bugs, same-origin bypasses, sandbox escapes, and JIT issues, though none were known to be exploited.

Main Article

Several threat campaigns were observed. The Kraken ransomware group, linked to the HelloKitty cartel, continues global cross-platform attacks using SMB exploits for initial access, Cloudflared tunnels for persistence, SSHFS for exfiltration, and double-extortion tactics. Separately, threat actors deployed XWorm RAT through phishing emails containing obfuscated Visual Basic Script loaders that unpacked payloads in memory. Fortinet's FortiWeb was actively exploited via an unpatched path-traversal flaw enabling creation of unauthorized admin accounts.

In global cyber news, Anthropic revealed the first known large-scale AI-orchestrated espionage campaign by China-aligned GTG-1002, which used autonomous agents to conduct reconnaissance, exploitation, lateral movement, and data theft with minimal human oversight. Cloudflare also experienced widespread service outages due to internal maintenance issues, while Logitech disclosed a data breach linked to a third-party zero-day vulnerability amid related claims by the Clop ransomware group.

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-2025-20341/CVE-2025-20349/CVE-2025-20353:** These vulnerabilities can be remediated by upgrading Cisco Catalyst Centre to the most recent version.
- **CVE-2025-6599/CVE-2025-8693:** We recommend applying the latest firmware updates to prevent these devices being exploited.
- **CVE-2025-13012 to CVE-2025-13027:** Updating to Firefox 145 or ESR versions 140.5 or 115.30, to remediate all identified vulnerabilities and enhance the browsers posture.

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.



[Acumen Cyber Threat Intelligence Digest: Week 47](#)

Major Vulnerabilities WordPress W3 Total Cache Plugin (CVE-2025-9501) A critical command injection flaw lets attackers execute PHP payloads via malicious comments, enabling full remote code execution. A proof-of-concept exploit was released on 24 No...

Steve McIntosh

11/28/2025

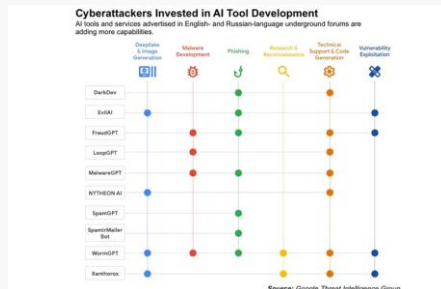


[SC3 weekly threat reports](#)

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

Steve McIntosh

11/28/2025

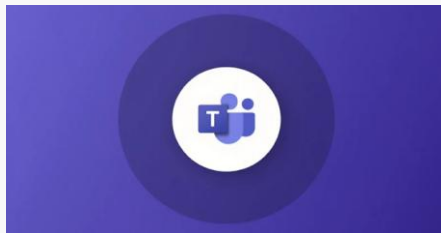


[How Malware Authors Are Incorporating LLMs to Evade Detection](#)

Cybercriminals are now experimenting with large language models (LLMs) like Google Gemini and Hugging Face to make malware more adaptive and harder to detect. Google's Threat Intelligence Group recently analysed five programs that show how attackers...

Steve McIntosh

11/28/2025



[MS Teams Guest Access Can Remove Defender Protection When Users Join External Tenants](#)

Cybersecurity researchers have flagged a serious issue in Microsoft Teams : the guest access feature can bypass Microsoft Defender for Office 365 protections when users join external tenants. This means your security controls don't apply once your u...

Steve McIntosh

11/28/2025



[Scottish council still rebuilding systems two years after ransomware attack](#)

Auditors remain concerned about the cyber resilience of a Scottish council as some systems are yet to be fully rebuilt following a ransomware attack in November 2023. Main Article The ransomware attack on Comhairle nan Eilean Siar, in Scotland's Wes...

David Robertson

11/28/2025



[Dartmouth College Confirms Data Theft in Oracle Hack](#)

Dartmouth College on Tuesday confirmed suffering a data breach after cybercriminals targeted its Oracle E-Business Suite (EBS) instance. Main Article The Ivy League research university said it uses Oracle EBS to manage its operations, and its EBS in...

David Robertson

11/27/2025

[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.



Acumen Cyber Threat Intelligence Digest: Week 47

<https://acumencyber.com/cyber-threat-intelligence-digest-november-2025-week-47>

Major Vulnerabilities

- **WordPress W3 Total Cache Plugin (CVE-2025-9501)**
A critical command injection flaw lets attackers execute PHP payloads via malicious comments, enabling full remote code execution. A proof-of-concept exploit was released on **24 Nov**.
Fix: Update to **v2.8.13 or later**, disable the plugin if patching isn't possible, and restrict comment functionality.
- **SonicWall Firewalls (CVE-2025-40601)**
Stack-based buffer overflow in Gen7 and Gen8 SonicOS could allow unauthenticated DoS attacks.
Fix: Upgrade Gen7 to **7.3.1-7013+** and Gen8 to **8.0.3-8011+**.
- **Cisco ISE & ISE-PIC**
Four flaws (three XSS, one info disclosure) affect versions 3.1–3.4. Exploitation could expose sensitive data or allow malicious code injection.
Fix: Apply patches for **3.2 Patch 8**, **3.3 Patch 8 (Dec)**, and **3.4 Patch 2/4**.

Active Threat Campaigns

- **ClickFix Campaign**
Fake Windows Update pages trick users into running commands that deploy LummaC2 and Rhadamanthys stealers via in-memory execution.
Tip: Train staff to avoid "Run box" prompts and enforce script-blocking policies.

- **DPRK “Contagious Interview”**

Targets AI and crypto professionals via fake job platforms. Victims paste weaponised commands during staged interviews, leading to full compromise.

Tip: Warn staff about unsolicited LinkedIn job offers and enforce endpoint controls.

- **TamperedChef Malvertising**

Global campaign using SEO and signed installers to deliver obfuscated JavaScript payloads. Targets healthcare, construction, and manufacturing sectors.

Tip: Block suspicious installers and monitor for scheduled tasks creating persistence.

General News

- UK councils hit by a cyber incident disrupting shared IT systems.
- Salesforce and Gainsight investigating API abuse from non-allowlisted IPs.
- UK MPs call for **software vendor liability**, mandatory breach reporting, and incentives for cyber resilience.

Action Points

1. **Patch immediately:**

- W3 Total Cache → v2.8.13+
- SonicWall → latest firmware
- Cisco ISE → latest patches

2. **Harden endpoints:**

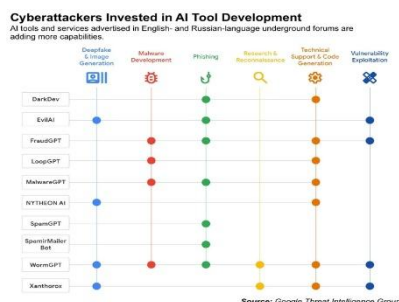
- Block PowerShell misuse and clipboard hijacking.

3. **Educate staff:**

- Warn about fake job interviews and Windows Update scams.

4. **Monitor malvertising:**

- Detect signed installers with short-lived certificates.
-



How Malware Authors Are Incorporating LLMs to Evade Detection

<https://www.darkreading.com/threat-intelligence/malware-authors-incorporate-llms-evade-detection>

Cybercriminals are now experimenting with **large language models (LLMs)** like Google Gemini and Hugging Face to make malware more adaptive and harder to detect. Google’s Threat Intelligence Group recently analysed five programs that show how attackers are using AI to rewrite code, generate commands, and

even automate attacks.

What's Happening?

- **LLMs in Malware Development:** Attackers use AI to:
 - Rewrite malicious code on the fly.
 - Generate unique commands for execution.
 - Automate exploitation and reconnaissance.
- Examples include:
 - **PROMPTFLUX:** VBScript malware that tries to rewrite its own source code using Gemini.
 - **PROMPTSTEAL:** Python tool querying Hugging Face API to analyse compromised systems.
 - **FRUITSHELL:** Reverse shell with hard-coded prompts to evade detection.
 - **QUIETVAULT:** Uses AI prompts to find and exfiltrate secrets.

Why It Matters

Generative AI gives skilled actors a framework similar to Metasploit or Cobalt Strike, while enabling less technical criminals to build sophisticated tools quickly. These techniques make malware **flexible and unpredictable**, but they also rely on external network access—meaning strong egress controls can still block them.

Current Reality

- Most samples are **prototypes**, not widespread yet.
- Many leave **execution artifacts** detectable by EDR tools.
- Attackers are learning to bypass AI safety guardrails by using pretexts like “capture-the-flag exercises” to trick LLMs into generating offensive code.

The Bigger Picture

This trend mirrors the **polymorphic malware era of the 1990s**, but now powered by AI. As defenders adopt AI for detection, attackers are doing the same to find vulnerabilities. The arms race is accelerating.

Action Points

1. **Monitor AI Service Traffic:**
 - Block or restrict access to external AI APIs from endpoints.
2. **Strengthen Egress Controls:**
 - Detect and block suspicious outbound connections.
3. **Enhance Detection:**
 - Use behaviour-based analytics and anomaly detection—not just signatures.
4. **Update Threat Models:**
 - Include AI-assisted malware and runtime code generation scenarios.
5. **Leverage AI Defensively:**
 - Deploy machine learning models to spot deviations from normal behaviour.

MS Teams Guest Access Can Remove Defender Protection When Users Join External Tenants

<https://thehackernews.com/2025/11/ms-teams-guest-access-can-remove.html>

Cybersecurity researchers have flagged a serious issue in **Microsoft Teams**: the **guest access feature** can bypass **Microsoft Defender for Office 365 protections** when users join external tenants. This means your security controls don't apply once your user steps into someone else's environment.

What's Happening?

- When a user accepts a **guest invitation** to another tenant, their security is governed by that tenant—not their home organisation.
- Attackers can exploit this by creating **malicious tenants** with minimal or no security (e.g., using low-cost Microsoft 365 licences without Defender).
- Once inside, the attacker can send phishing links or malware attachments without triggering Safe Links or Safe Attachments scans.

Why It's Dangerous

- The attack starts with an **email invite from Microsoft infrastructure**, which passes SPF, DKIM, and DMARC checks. Email security tools won't flag it.
- If the victim accepts, all communication happens in the attacker's tenant, outside your security boundary.
- Your organisation remains **completely unaware**—no alerts, no logs, no triggers.

Microsoft's New Feature

Microsoft is rolling out a Teams update that allows chatting with anyone via email—even non-Teams users. It's enabled by default and will be global by **January 2026**. While great for collaboration, it widens the attack surface.

Architectural Gap

Guest access \neq external access. External access still applies your policies; guest access does not. This is the **fundamental blind spot** attackers are exploiting.

Hypothetical Attack Chain

1. Attacker spins up a cheap Microsoft 365 tenant without Defender.
2. Sends Teams invite to target via email.
3. Victim accepts and becomes a guest in attacker's tenant.
4. Attacker sends phishing links or malware—no security scans apply.

Action Points

1. **Restrict B2B collaboration:**
 - Only allow guest invitations from trusted domains.
2. **Implement cross-tenant access controls:**

- Use Conditional Access and tenant restrictions.
- 3. **Disable external Teams invites if not needed:**
 - Set UseB2BInvitesToAddExternalUsers to false.
- 4. **Train users:**
 - Warn about unsolicited Teams invites from unknown sources.
- 5. **Monitor for anomalies:**
 - Track guest account activity and external tenant interactions.
- 6. **Review licensing strategy:**
 - Ensure Defender protections extend to collaboration scenarios.

Scottish council still rebuilding systems two years after ransomware attack

https://www.theregister.com/2025/11/27/western_isles_ransomware_council/



Auditors remain concerned about the cyber resilience of a Scottish council as some systems are yet to be fully rebuilt following a ransomware attack in November 2023.

The ransomware attack on Comhairle nan Eilean Siar, in Scotland's Western Isles, required "several" of its systems to be reconstructed, among other damage – especially to the authority's finance department.

Systems for housing benefits, council tax, and non-domestic rates remain unrestored, with their large data volumes slowing the digital renovation, the audit noted.

A [report](#) [PDF] on the attack, published by Scotland's Accounts Commission today, commended the Comhairle's swift response to the attack, but highlights various gaps that remain in its cybersecurity defences.

Action Point:

The Accounts Commission commended the authority for an appropriate response given its resources at the time. The council escalated the case to organizations like the central Scottish government and the NCSC, and followed its business continuity plan, even though it wasn't properly stress-tested for a scenario as serious as the ransomware attack it faced.

It also quickly identified that its HR/payroll system, ResourceLink, was the most critical system rendered inaccessible, and it worked quickly to restore functionality. Payroll was restored by the end of the month, so staff did not miss a pay check, and partial functionality was achieved by mid-December.

The authority engaged the right regulators and third parties, like UK cybersecurity biz NCC Group, to help with remediation efforts, and has made some progress in its recovery plan.



Dartmouth College Confirms Data Theft in Oracle Hack

<https://www.securityweek.com/dartmouth-college-confirms-data-theft-in-oracle-hack/>

Dartmouth College on Tuesday confirmed suffering a data breach after cybercriminals targeted its Oracle E-Business Suite (EBS) instance.

The Ivy League research university said it uses Oracle EBS to manage its operations, and its EBS instance was targeted in the recent zero-day attack between August 9 and August 12. Dartmouth College determined in late October that the attackers managed to exfiltrate files containing personal and financial information, including Social Security numbers.

The university told the Maine Attorney General that nearly 1,500 residents of the state are [impacted](#). In New Hampshire, authorities were told that [more than 31,000 people](#) are affected. The total number of affected people has not been disclosed.

The Cl0p ransomware group, which is the public-facing entity taking credit for the [Oracle EBS campaign](#), has been listing victims on its leak website.

Action Point:

[Canon](#) and [Mazda](#) confirmed to *SecurityWeek* in recent days that they have also been targeted in the Oracle campaign, but the carmaker said it found no evidence of data leakage.

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

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](#)

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

David Robertson

12/5/2025

6 views



[Cloudflare down: Internet stops working properly amid major outage](#)

Cloudflare has gone down, taking many other websites down with it. Visitors to a number of pages saw a “500 internet server error” warning, rather than the content they expected. Notably, that included Down Detector, a tracking website that shows ou...

David Robertson

12/5/2025

6 views



['Exploitation is imminent' as 39 percent of cloud environs have max-severity React hole](#)

A maximum-severity flaw in the widely used JavaScript library React, and several React-based frameworks including Next.js allows unauthenticated, remote attackers to execute malicious code on vulnerable instances. The flaw is easy to abuse, and mass...

David Robertson

12/5/2025

6 views



[Acumen: Cyber Threat Intelligence Digest: Week 48](#)

The latest Cyber Threat Intelligence Digest highlights key vulnerability disclosures, emerging malware, active phishing operations, and broader security developments. Major vendors issued critical

patches, including Apache's fix for CVE-2025-59789, ...

David Robertson

12/3/2025

8 views



[OpenAI User Data Exposed in Mixpanel Hack](#)

OpenAI is informing some users that they may be impacted by a recent data breach at product analytics and event-tracking solutions provider Mixpanel. Main Article Mixpanel disclosed the security incident on Thursday, saying that it was detected on N...

David Robertson

12/3/2025

7 views



[Chrome, Edge Extensions Caught Tracking Users, Creating Backdoors](#)

A threat actor has published over a hundred malicious extensions that can track and profile Chrome and Microsoft Edge users, and can also execute a payload on their systems, Koi Security reports. Main Article According to the company, the threat act...

David Robertson

12/3/2025

9 views



[Compromised account used to create fake organisation emails](#)

A member reported that a compromised student account was used to create 10 M365 groups via Teams. Each group was then assigned 100 email aliases in the same format as the student account but not valid. An Entra guest account was then created and lin...

Steve McIntosh

12/2/2025

16 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 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
'Exploitation is imminent' as 39 percent of cloud environs have max-severity React hole	2
OpenAI User Data Exposed in Mixpanel Hack.....	3
Chrome, Edge Extensions Caught Tracking Users, Creating Backdoors.....	4
Compromised account used to create fake organisation emails	5
Acumen Cyber Threat Intelligence Digest: Week 48	6

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-bulletin-1-December-2025



SC3-Daily-threat-bulletin-2-December-2025



SC3-Daily-threat-bulletin-3-December-2025



SC3-Daily-threat-bulletin-4-December-2025



SC3-Daily-threat-bulletin-5-December-2025



SC3-Weekly-vulnerability-report-1-December-2025



'Exploitation is imminent' as 39 percent of cloud environs have max-severity React hole

A maximum-severity flaw in the widely used JavaScript library React, and several React-based frameworks

including [Next.js](#) allows unauthenticated, remote attackers to execute malicious code on vulnerable instances. The flaw is easy to abuse, and mass exploitation is "imminent," according to security researchers.

[Main Article](#)

The React team [disclosed](#) the unauthenticated remote code execution (RCE) vulnerability in React Server Components on Wednesday. It's tracked as [CVE-2025-55182](#) and received a maximum 10.0 CVSS severity rating.

This is a big deal because much of the internet is built on React – one estimate suggests 39 percent of cloud environments are vulnerable to this flaw. This issue therefore deserves a prominent place on your to-do list.

The bug affects versions 19.0, 19.1.0, 19.1.1, and 19.2.0 of:

- [react-server-dom-webpack](#)
- [react-server-dom-parcel](#)
- [React-server-dom-turbopack](#)

It also affects the default configuration of several React frameworks and bundlers including [next](#), [react-router](#), [waku](#), [@parcel/rsc](#), [@vitejs/plugin-rsc](#), and [rwsdk](#).

Action Point: The project's maintainers say upgrading to versions [19.0.1](#), [19.1.2](#), and [19.2.1](#) fixes the flaw.



OpenAI User Data Exposed in Mixpanel Hack

OpenAI is informing some users that they may be impacted by a recent data breach at product analytics and event-tracking solutions provider Mixpanel.

[Main Article](#)

[Mixpanel](#) disclosed the security incident on Thursday, saying that it was detected on November 8. The company described it as a “smishing campaign” and noted that a “limited number of customers” are affected.

The company did not share any technical information on the intrusion, but pointed out that it secured affected accounts, rotated compromised credentials, revoked active sessions, reset employee passwords, and blocked malicious IPs in response to the incident.

While Maxpanel shared little information on the cyberattack, OpenAI, one of the affected customers, has provided more [details regarding impact](#).

The AI giant uses Mixpanel for web analytics, to help it understand product usage and improve the API product (platform.openai.com).

OpenAI said there was no unauthorized access to its own infrastructure and the data breach did not affect ChatGPT chat content, prompts, responses, or API usage data. OpenAI passwords, API keys, payment information, account credentials, and government IDs were not compromised.

“Users of ChatGPT and other products were not impacted,” OpenAI said.

However, the attacker did steal “a dataset containing limited customer identifiable information and analytics information”.

Action Point: Specifically, the hackers obtained user profile information associated with ‘platform.openai.com’, including name, email address, approximate location based on the user’s browser (such as city, state, and country), operating system and browser, organization or user ID, and referring website.

OpenAI warned that the compromised information could be useful to threat actors for phishing and social engineering attacks.

“As part of our security investigation, we removed Mixpanel from our production services, reviewed the affected datasets, and are working closely with Mixpanel and other partners to fully understand the incident and its scope. We are in the process of notifying impacted organizations, admins, and users directly. While we have found no evidence of any effect on systems or data outside Mixpanel’s environment, we continue to monitor closely for any signs of misuse,” OpenAI said.



Chrome, Edge Extensions Caught Tracking Users, Creating Backdoors

A threat actor has published over a hundred malicious extensions that can track and profile Chrome and Microsoft Edge users, and can also execute a payload on their systems, Koi Security reports.

Main Article

According to the company, the threat actor, tracked as [ShadyPanda](#), has been uploading seemingly innocuous extensions for roughly seven years, and weaponizing them after gaining users' trust.

The extensions have gathered over 4 million downloads and some of them remain available for download.

In 2023, as part of a campaign focused on affiliate fraud, ShadyPanda published 20 Chrome extensions under the name 'nuggetsno15', and 125 Edge extensions using the name 'Zhang'.

The extensions were designed to silently inject affiliate tracking codes every time the victim clicked on eBay, Amazon, or Booking.com links.

"Hidden commissions on every purchase. The extensions also deployed Google Analytics tracking to monetize browsing data – every website visit, search query, and click pattern logged and sold," Koi notes.

In early 2024, the threat actor changed tactics, publishing an extension posing as a tab productivity tool. Named Infinity V+, it redirected web searches through the browser hijacker trovi.com.

Additionally, ShadyPanda used malicious code to read victims' cookies and send the data to [nossldergoodting.com](#), creating unique identifiers without users' consent or knowledge. The code also captured users' input in the search box, profiling their interests in real time.

Action Point: One of these extensions, named WeTab New Tab Page, has over three million downloads. While posing as a productivity tool, it operates as a sophisticated surveillance platform, sending user data to 17 different domains, Koi says.

The cybersecurity firm says it linked the campaigns based on code similarities, overlapping infrastructure, and the observed obfuscation techniques, which have evolved over time.

A Google spokesperson has confirmed that the malicious extensions are not available on the Chrome Web Store.

Responding to a *SecurityWeek* inquiry, a Microsoft spokesperson said the company was not notified about the issue.

"We have removed all the extensions identified as malicious on Edge Add-on store. When we become aware of instances that violate our policies, we take appropriate action that includes, but is not limited to, the removal of prohibited content or termination of our publishing agreement," the company's representative said.



Compromised account used to create fake organisation emails

A member reported that a compromised student account was used to create 10 M365 groups via Teams. Each group was then assigned 100 email aliases in the same format as the student account but not valid.

An Entra guest account was then created and linked to an external gmail.com address and this email added to each group.

The groups can then be set to accept email from external senders to the fake student accounts with anything sent to these 1000 newly created addresses delivered to the gmail.com address.

These fake student email addresses could then be used to create accounts on external sites, used in phishing attempts and other scams.

Action Point:

You can create a script that searches for Unified (M365) Groups with

HiddenFromAddressListsEnabled not set to true

HiddenFromAddressListsEnabled set to true HiddenFromExchangeClientsEnabled set to true

Ensure that you have reviewed your Teams permissions and group creation controls.



Acumen Cyber Threat Intelligence Digest: Week 48

The latest Cyber Threat Intelligence Digest highlights key vulnerability disclosures, emerging malware, active phishing operations, and broader security developments. Major vendors issued critical patches, including Apache's fix for CVE-2025-59789, a stack-exhaustion flaw in bRPC triggered by deeply nested JSON, and IBM's patch for CVE-2024-45675, which allowed password-less administrative access to Informix Dynamic Server. Google's December 2025 Android Security Bulletin addressed 107 vulnerabilities, notably zero-days CVE-2025-48633 (information disclosure) and CVE-2025-48572 (privilege escalation), which may have seen limited targeted exploitation.

Main Article

New threats include GrokPy, malware distributed via Amadey that gathers system data, controls browsers through Chrome DevTools, performs OCR on screenshots, bypasses CAPTCHA using a Grok LLM, and creates automated Discord accounts. Phishing activity also intensified: a Calendly-themed campaign targets Google Workspace and Facebook Business accounts using staged lures, AiTM mechanisms, and Browser-in-the-Browser pop-ups. Another campaign linked to Scattered Lapsus\$ Hunters leverages over 40 spoofed Zendesk domains and fraudulent tickets to steal credentials and deploy malware, echoing infrastructure from prior Salesforce and Discord compromises.

General security news includes a data breach at UK ISP Brsk, with unverified claims of a 230,000-record leak, and a large-scale study revealing over 17,000 secrets exposed across GitLab Cloud repositories. Additionally, the ShadyPanda operation continues to infect millions through malicious Chrome and Edge extensions that evolved into spyware with remote-code-execution capabilities.

Threat-actor tracking shows new or rising activity for groups such as Black Shantrac Ransomware and XHJACK, while global trend analysis indicates spikes in reports related to groups like Beregini, MuddyWater, and INC Ransom, alongside newly prominent vulnerabilities and attack methods.

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-2025-59789:** This vulnerability can be remediated by updating the Apache bRPC to version 1.15.0.
- **CVE-2024-45675:** We recommend upgrading IBM Informix Dynamic Server to version 14.10.xC11W1.
- **CVE-2025-48633/ CVE-2025-48572:** These vulnerabilities can be addressed by updating to the newest version.

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.



[Researchers spot 700 percent increase in hypervisor ransomware attacks](#)

Researchers at Huntress have flagged a massive spike in ransomware attacks targeting hypervisors —the software layer that manages virtual machines. In the first half of 2025, hypervisors were involved in just 3% of ransomware incidents. Now, that fi...

Steve McIntosh

12/12/2025

2 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

12/12/2025

4 views



[Cybersecurity Performance Goals 2.0 \(CPG 2.0\)](#)

CISA's Cybersecurity Performance Goals 2.0 (CPG 2.0) are voluntary, high-impact practices designed to help organisations—big or small—strengthen their cyber resilience. They're not exhaustive, but they provide a baseline of priority actions that red...

Steve McIntosh

12/12/2025

5 views



[UK finally vows to look at 35-year-old Computer Misuse Act](#)

Portugal has just updated its cybersecurity law to protect researchers, and now the UK is under growing pressure to do the same. The Computer Misuse Act (CMA) , introduced in 1990, is widely seen as outdated and hostile to modern security research. ...

Steve McIntosh

12/12/2025

7 views



[North Korea-linked Actors Exploit React2Shell to Deploy New EtherRAT Malware](#)

Threat actors linked to North Korea are exploiting React2Shell (CVE-2025-55182) —a critical vulnerability in React Server Components—to deliver a new remote access trojan called EtherRAT . This marks a major escalation from opportunistic cryptominin...

Steve McIntosh

12/10/2025

13 views



[Microsoft Fixes Exploited Zero Day in Light Patch Tuesday](#)

Microsoft closed out 2025 with a lighter Patch Tuesday—just 57 vulnerabilities fixed , compared to the 163-patch monster in October. But don't relax too much: one of these flaws is already being exploited, and two others have public proof-of-concept...

Steve McIntosh

12/10/2025

13 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.

Researchers spot 700 percent increase in hypervisor ransomware attacks

https://www.theregister.com/2025/12/09/hypervisor_ransomware_attacks_increasing/



Researchers at Huntress have flagged a **massive spike in ransomware attacks targeting hypervisors**—the software layer that manages virtual machines. In the first half of 2025, hypervisors were involved in just 3% of ransomware incidents. Now, that figure has jumped to **25%**, a 700% increase. The main culprit? The **Akira ransomware group**, along with other threat actors, who are exploiting hypervisors to bypass traditional endpoint and network security.

Why hypervisors?

They're often under-protected. Attackers know that hypervisors control entire virtual infrastructures, so compromising them gives huge leverage. Plus, many hypervisors run proprietary OSs where defenders can't easily install tools like EDR, creating blind spots.

How attacks happen:

- Hackers compromise networks, steal credentials, and then target hypervisors.
- They use built-in tools (e.g., OpenSSL) to encrypt VM volumes—no need for custom ransomware binaries.
- Misuse of Hyper-V utilities to disable endpoint defences, tamper with virtual switches, and prep VMs for mass ransomware deployment.
- VMware and other platforms have already seen guest-to-host escape bugs exploited in the wild.

This trend is alarming because **hyperscale clouds rely on hypervisors**. A successful VM escape could have catastrophic consequences.

Bottom line: Hypervisors are now prime ransomware targets. Treat them as critical infrastructure—because attackers already do.

Action Point:

Revisit Security Basics:

- Enforce **multi-factor authentication (MFA)** and strong, complex passwords.
- Keep hypervisors **fully patched**—don't delay updates.

Hypervisor-Specific Defences:

- Enable settings that **allow only approved binaries** to run on hosts.
- Monitor hypervisor logs via **SIEM** for suspicious activity.

Credential Hygiene:

- Regularly audit and rotate admin credentials.
- Limit privileged access to hypervisor management tools.

Backup & Recovery:

- Ensure **robust backups** of VM volumes and hypervisor configurations.
- Test recovery plans—don't assume they'll work under pressure.

Stay Informed:

- Track advisories from vendors like VMware, Microsoft, and Nutanix.
- Watch for CISA alerts on hypervisor vulnerabilities.



Cybersecurity Performance Goals 2.0 (CPG 2.0)

<https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0>

CISA's **Cybersecurity Performance Goals 2.0 (CPG 2.0)** are voluntary, high-impact practices designed to help organisations—big or small—strengthen their cyber resilience. They're not exhaustive, but they provide a **baseline of priority actions** that reduce risk in measurable ways. Think of them as a practical roadmap for improving security without drowning in complexity.

Why CPG 2.0 Matters

- Developed using **CISA's operational data**, threat research, and industry feedback.
- Focused on **real-world threats** and **outcome-driven language**.
- Applicable across sectors, including critical infrastructure.

Core Areas and Key Practices

1. Govern

- Assign clear **cybersecurity responsibilities**.
- Maintain **incident response plans**.
- Implement **supply chain risk management** and vulnerability disclosure processes.
- Manage risks from **managed service providers**.

2. Identify

- Maintain an accurate **asset inventory**.
- Mitigate known vulnerabilities promptly.
- Validate cybersecurity controls independently.
- Document **network topology**.

3. Protect

- Change default passwords and enforce strong password policies.
- Implement **multi-factor authentication (MFA)**.
- Apply **least privilege principles** and separate admin accounts.
- Segment networks logically and physically.
- Provide regular **cybersecurity training**.
- Enable **email security**, strong encryption, and disable risky features like macros.
- Maintain **system backups**, change management, and hardware/software approval processes.

4. Detect

- Deploy **malicious code detection** tools.
- Identify adverse events quickly.

5. Respond

- Establish clear **incident communication and reporting procedures**.

6. Recover

- Plan and prepare for recovery after incidents.

Why It's Important

CPGs don't cover everything, but they capture **high-value practices** proven to reduce risk. They're a great starting point for organisations that need clarity on where to focus resources and align with the HEFESTIS pathway program.

Action Points

Assign accountability: Define roles for cybersecurity oversight and incident response.

Implement MFA and strong passwords: Make this non-negotiable.

Segment networks and enforce least privilege: Reduce lateral movement risk.

Train staff regularly: Human error is still the biggest vulnerability.

Enable email security and encryption: Protect against phishing and data leaks.

Maintain backups and change management: Ensure resilience and quick recovery.

Engage suppliers: Require vulnerability disclosure and security standards.

UK finally vows to look at 35-year-old Computer Misuse Act

https://www.theregister.com/2025/12/09/uk_computer_misuse_act/



Portugal has just updated its cybersecurity law to protect researchers, and now the UK is under growing pressure to do the same. The **Computer Misuse Act (CMA)**, introduced in 1990, is widely seen as outdated and hostile to modern security research. Even the UK government admits it's time for change.

What's Happening?

- **Portugal's Move:** Researchers acting “with the sole intention of identifying vulnerabilities” and reporting them for security improvement are now exempt from prosecution. Actions must be proportionate, non-disruptive, and not for financial gain (beyond professional remuneration).
- **UK Response:** Security Minister Dan Jarvis said the government is considering a “**statutory defence**” for researchers who meet certain safeguards. This follows decades of criticism from the infosec community.
- **Why It Matters:** The CMA was created before modern cybersecurity existed—long before bug bounty programs, vulnerability disclosure, or today's threat landscape. It criminalises good-faith testing, leaving researchers at risk of prosecution for doing their job.

Historic Context

The CMA was born after journalists Steve Gold and Robert Schifreen accessed the Duke of Edinburgh's BT Prestel account in the 1980s. They were prosecuted under forgery laws but later acquitted. The Act was meant to fill a legal gap—but now it's a barrier to security progress.

Current Challenges

- Researchers like Daniel Cuthbert have been convicted under CMA for benign actions, such as testing a tsunami donation site in 2004.
- UK cybercrime prosecutions have dropped 20%, but offences are at their highest since 2017—showing enforcement priorities are shifting.
- Industry leaders argue CMA reform is critical to support the UK's ambition to be “the safest place to live and do business online.”

What Reform Could Look Like

- Legal safe harbour for vulnerability research.
- Clear rules on proportionality, consent, and non-disruption.
- Alignment with global norms—Portugal's model could be a template.

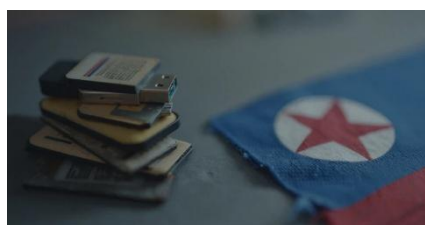
Action Points

Engage with Policy: Support initiatives like CyberUp's four principles for good-faith research.

Update Internal Policies: Define what constitutes authorised testing and disclosure.

Educate Researchers: Ensure teams understand current legal risks under CMA.

Prepare for Change: Align vulnerability management processes with expected legal updates.



North Korea-linked Actors Exploit React2Shell to Deploy New EtherRAT Malware

<https://thehackernews.com/2025/12/north-korea-linked-actors-exploit.html>

Threat actors linked to North Korea are exploiting **React2Shell (CVE-2025-55182)**—a critical vulnerability in React Server Components—to deliver a new remote access trojan called **EtherRAT**. This marks a major escalation from opportunistic cryptomining to **persistent, stealthy access** designed for long-term operations.

What Makes EtherRAT Dangerous

- **Ethereum Smart Contracts for C2:** EtherRAT uses **EtherHiding**, fetching its command-and-control (C2) URL from an Ethereum smart contract every five minutes.
- **Consensus Voting:** Queries nine public RPC endpoints and picks the majority response—making takedown nearly impossible.
- **Five Persistence Mechanisms:**
 - Systemd user service
 - XDG autostart entry
 - Cron jobs
 - .bashrc injection
 - Profile injection
- **Self-Updating Malware:** Sends its source code to an API, receives an obfuscated version, and overwrites itself—evading signature-based detection.

Attack Chain

1. Exploits **React2Shell (CVSS 10.0)** to run a Base64-encoded shell command.
2. Downloads a shell script via curl (with wget and python3 as fallbacks).
3. Installs **Node.js v20.10.0** from nodejs.org.

4. Deploys an encrypted blob and obfuscated JavaScript dropper.
5. Decrypts EtherRAT payload and executes it using Node.js.

Once active, EtherRAT polls its C2 every 500ms, executing any JavaScript response longer than 10 characters.

Links to Contagious Interview Campaign

This campaign targets blockchain and Web3 developers via **fake job interviews** on LinkedIn, Upwork, and Fiverr. Victims are tricked into running malicious code during coding tests.

Recent variants now abuse **VS Code tasks.json auto-run** to execute loader scripts when projects are opened, leading to BeaverTail and InvisibleFerret infections. Researchers found **13 versions** of this campaign across **27 GitHub accounts**, with DPRK actors shifting hosting to **Vercel**.

Action Points

Patch React2Shell immediately (CVE-2025-55182).

Audit npm and VS Code environments:

- Block auto-run tasks.json configurations.
- Scan for suspicious repos and scripts.

Restrict developer privileges:

- Enforce least privilege and endpoint monitoring.

Monitor Ethereum RPC traffic:

- Flag unusual smart contract queries.

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

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

Darren, Steve and I would like to wish you all a very restful and peaceful Christmas and New Year.

If, however you are unfortunate enough to experience a cyber incident and you would like HEFESTIS's help to respond and/or coordinate, PLEASE email us at ciso-office@hefestis.ac.uk.

And if you need to speak to one of the Team, in the first instance, please call the following mobile number (07565 217790), so that we can assess how best we can help and support you.

The CISO Office mailbox will be monitored over the period of our annual closure from 0900 to 1700, from Wednesday 24th December to Friday 2nd January, with reduced cover over the main holidays and at weekends.

If you need to call but there is no initial answer, please leave a voice message with a contact number and/or send a text message saying the same.

In the meantime, if you have any concern about, or need advice regarding reducing your attack surface over the festive period, please make contact with us.

Finally, thank you Everyone for your help and support in 2025, we hope 2026 will be just as much fun, if not more.

Take care and keep safe.

Best Wishes,

David, Steve, and Darren

At the CISO 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](#)

Please find SC3's daily threat summaries for this week for those who do not receive this information directly. Action Point: This week's reports: Cyber Resilience Early Warning (CREW) Notice 17 December 2025
Good morning, SC3 are aware of a supply c...

David Robertson

12/18/2025

16 views

[Think Like an Attacker: Cybersecurity Tips From a CISO](#)

Cybersecurity is a field that touches every aspect of modern life, from personal privacy to global business operations. In Dark Reading's latest episode, Etay Maor, chief security strategist at Cato Networks and professor at Boston College, shares h...

David Robertson

12/18/2025

9 views

[How Cyber Insurance MGAs Shape Policies for Evolving Cyber-Risks](#)

Managing general agents (MGAs) underwrite and administer insurance policies on behalf of insurance companies. Just as a broker serves as an intermediary between the buyer and the insurer, the MGA acts as an agent for the insurer. While the insurance...

David Robertson

12/18/2025

9 views

[Apple Patches Two Zero-Days Tied to Mysterious Exploited Chrome Flaw](#)

Apple has released macOS and iOS updates to patch dozens of vulnerabilities, including two zero-days that the tech giant says have been exploited in highly targeted attacks. Main Article According to Apple's advisories , the zero-days impact WebKit,...

David Robertson

12/17/2025

7 views

[In-the-Wild Exploitation of Fresh Fortinet Flaws Begins](#)

Threat actors have started exploiting two recent Fortinet vulnerabilities only days after patches were released, Arctic Wolf warns. Main Article The two flaws, tracked as CVE-2025-59718 and CVE-2025-59719 (CVSS score of 9.8), are described as improv...

David Robertson

12/17/2025

9 views

[Amazon: Russian Hackers Now Favour Misconfigurations in Critical Infrastructure Attacks](#)

Russian state-sponsored threat actors appear to be favoring misconfigurations over the exploitation of vulnerabilities for gaining access to the systems of targeted critical infrastructure organizations, according to Amazon's threat intelligence tea...

David Robertson

12/17/2025

8 views

[Acumen Cyber Threat Intelligence Digest:
Week 50](#)

The Week 50 Cyber Threat Intelligence Digest highlights significant vulnerabilities, active threat operations, and recommended remediation actions observed across the cyber landscape. A critical focus is on CVE-2025-55182 (“React2Shell”), a severe r...

David Robertson

12/18/2025

9 views

[Go To Site](#)

CISO-Share Office Weekly Newsletter

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

Darren, Steve and I would like to wish you all a very restful and peaceful Christmas and New Year.

If, however you are unfortunate enough to experience a cyber incident and you would like HEFESTIS's help to respond and/or coordinate, **PLEASE** email us at ciso-office@hefestis.ac.uk.

And if you need to speak to one of the Team, in the first instance, please call the following mobile number (**07565 217790**), so that we can assess how best we can help and support you.

The CISO Office mailbox will be monitored over the period of our annual closure from 0900 to 1700, from Wednesday 24th December to Friday 2nd January, with reduced cover over the main holidays and at weekends.

If you need to call but there is no initial answer, please leave a voice message with a contact number and/or send a text message saying the same.

In the meantime, if you have any concern about, or need advice regarding reducing your attack surface over the festive period, please make contact with us.

Finally, thank you Everyone for your help and support in 2025, we hope 2026 will be just as much fun, if not more.

Take care and keep safe.

Best Wishes,

David, Steve, and Darren
At the CISO 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	2
Amazon: Russian Hackers Now Favour Misconfigurations in Critical Infrastructure Attacks	3
Think Like an Attacker: Cybersecurity Tips From a CISO	8
How Cyber Insurance MGAs Shape Policies for Evolving Cyber-Risks	9
Apple Patches Two Zero-Days Tied to Mysterious Exploited Chrome Flaw	10
In-the-Wild Exploitation of Fresh Fortinet Flaws Begins	11
Acumen Cyber Threat Intelligence Digest: Week 50	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.

Cyber Resilience Early Warning (CREW) Notice: 17/12/2025

SC3 are aware of a supply chain attack against a public sector body. We are sharing the following IoCs with you for awareness or investigation at TLP Amber+Strict. Please do not share this information with any external parties.

Indicators of Compromise

File: rclone.exe (SHA256:
44959138b2c9b295d7d558e229f0b7495a5af446ab0fe472b8dc982b070e5a7b)

File: qtox.exe (SHA256:
23220603016067c7f1df18200007274c978549d28acb4faf687b2fcd7624dff3)

File: agent.exe: (SHA256:
8a96c8a800d5faf55acd259192166aa6c2ba1069b631f9cde90a079fabde420f)

Domain: g[.]api[.]mega[.]co[.]nz (Data exfiltration host)

IP: 66[.]203.125.13 (Data exfiltration host)

IP: 62[.]60.177.94 (C2)

IP: 130[.]43.175.10 (where malicious connections came from)

If your organisation is affected by the content of this CREW Notice, please reply to this email and provide details of the impact. Nil returns are not required

Kind regards

SC3 Incident Coordination, Scottish Cyber Co-ordination Centre, National Cyber Security & Resilience Division, Scottish Government

Tel 0300 244 9700

This email is issued as TLP Amber + Strict and is not for sharing outside your organisation. Please ensure this information is strictly limited to those within your organisation on a need-to-know basis.

TLP:Amber+Strict

When should it be used? Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organisation.

How should it be shared? Recipients may share TLP:AMBER+STRICT information only with members of their own organisation on a need-to-know basis to protect their organisation and prevent further harm.

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-December-lletin-16-December-lletin-17-December-lletin-18-December-lletin-19-December-



SC3-Weekly-Vulner
ability-Report-15-De



Amazon: Russian Hackers Now Favour Misconfigurations in Critical Infrastructure Attacks

Russian state-sponsored threat actors appear to be favouring misconfigurations over the exploitation of vulnerabilities for gaining access to the systems of targeted critical infrastructure organizations, according to Amazon's threat intelligence team.

Main Article

The malicious activity has been linked to the widely known Russian threat actor named [Sandworm](#), which has led Amazon's experts to conclude that the attacks are likely conducted by hackers associated with Russia's GRU military intelligence agency.

Amazon has also seen some infrastructure overlaps with hackers tracked by Bitdefender as [Curly COMrades](#), who may have been responsible for post-exploitation activities.

Over the past five years, Amazon has seen attacks aimed at energy organizations in Western nations, critical infrastructure in North America and Europe, and various types of organizations with cloud-hosted network infrastructure.

The tech giant has monitored the threat actors' attacks between 2021 and 2025, and up until this year they often achieved initial access through the exploitation of zero-day and n-day vulnerabilities.

Examples of vulnerabilities exploited between 2021 and 2024 include the WatchGuard flaw [CVE-2022-26318](#), Confluence flaws [CVE-2021-26084](#) and [CVE-2023-22518](#), and the Veeam product flaw [CVE-2023-27532](#).

Action Point: Here is a mitigation blueprint for Azure users to defend against those pesky Russian attacks - namely exploitation of misconfigured identity, networking, and management services rather than software vulnerabilities—and tailored for enterprise-scale Azure environments.

Executive Summary

For Azure enterprise environments, **misconfiguration defense equals identity, governance, and automation.**

The most effective controls are:

1. **Conditional Access + PIM everywhere**
2. **Private networking by default**
3. **Azure Policy deny rules**
4. **Centralized logging with Sentinel**
5. **IaC-driven deployments only**

These measures directly counter the attacker tradecraft described in the article by **removing opportunistic access paths, limiting blast radius, and detecting abuse early.**

1. Azure Identity (Primary Attack Surface)

Misconfiguration of identity and access controls is the highest-risk vector in Azure.

Required Controls

- **Enforce Conditional Access Everywhere**
 - Require MFA for *all* interactive users, especially:
 - Global Administrators
 - Privileged Role Administrators
 - Subscription Owners
 - Block legacy authentication protocols entirely.
- **Privileged Identity Management (PIM)**
 - Make all admin roles *Just-In-Time*.
 - Require approval and MFA for elevation.
 - Enforce time-bound role activation.
- **Eliminate Standing Privilege**
 - Remove permanent Global Admins.
 - Replace shared admin accounts with named identities.
- **Harden Service Principals & Managed Identities**
 - Rotate secrets regularly or eliminate them in favour of managed identities.
 - Scope permissions narrowly (no subscription-wide Contributor unless unavoidable).

Why: The campaign highlighted credential capture and replay against poorly protected access paths—Azure AD is the first line of defense.

2. Azure Networking & Edge Exposure

Threat actors favor **misconfigured ingress points** rather than exploiting zero-days.

Required Controls

- **Default-Deny Network Architecture**
 - NSGs: Explicitly block inbound traffic except required ports and sources.
 - Remove 0.0.0.0/0 rules wherever possible.
- **Restrict Management Access**
 - Disable public access to:
 - Azure VMs (RDP/SSH)
 - Azure SQL
 - Storage Accounts
 - Use:
 - Azure Bastion
 - Private Endpoints
 - VPN or ExpressRoute
- **Protect Edge Services**
 - Front all internet-facing services with:
 - Azure Application Gateway + WAF
 - Azure Front Door (with WAF)
- **Segmentation**
 - Separate:
 - Identity infrastructure
 - Management plane
 - Production workloads
 - OT/ICS or critical services

Why: The attackers exploited exposed or weakly protected edge infrastructure to gain persistent access.

3. Azure Resource Configuration Governance

Misconfiguration at scale requires **automated prevention**, not manual review.

Required Controls

- **Azure Policy (Mandatory)**
 - Deny policies for:
 - Public storage accounts
 - Public IPs on critical workloads
 - Non-approved VM images
 - Resources without diagnostic logging
 - Enforce tagging for ownership and environment.
- **Management Groups**
 - Apply security policy at the tenant root and cascade downward.
- **Infrastructure as Code (IaC)**
 - Require Terraform/Bicep/ARM for production changes.
 - Block portal-only deployments for critical subscriptions.
- **Azure Blueprints (or equivalent)**
 - Pre-package secure landing zones.

Why: The attack model assumes defenders rely on ad-hoc configuration and manual hardening—which does not scale.

4. Logging, Detection, and Misconfiguration Monitoring

Detection must focus on **configuration abuse**, not malware alone.

Required Controls

- **Centralized Logging**
 - Azure AD Sign-in Logs
 - Audit Logs
 - Activity Logs
 - NSG Flow Logs
 - Resource diagnostics
- **Microsoft Defender for Cloud**
 - Enable all relevant plans (Servers, Storage, App Services, Containers).
 - Actively remediate Secure Score findings.
- **Microsoft Sentinel**
 - Ingest Azure AD, Activity Logs, Defender alerts.
 - Enable analytics for:
 - Suspicious role assignment
 - Impossible travel
 - Excessive failed logins
 - Unusual API calls
- **Alert on Configuration Changes**
 - Monitor:
 - Role assignments
 - Network rule modifications
 - Public exposure changes

Why: These campaigns often remain “quiet” and look like normal admin activity unless explicitly monitored.

5. Azure Subscription & Tenant Hygiene

Required Controls

- **Limit Subscription Owners**
 - Maximum of 2–3 break-glass accounts.
- **Secure Break-Glass Accounts**
 - MFA excluded (intentionally) but:
 - Long, rotated passwords
 - Stored offline
 - Alert on use
- **Tenant-Wide Security Defaults**
 - Disable if using Conditional Access—but only after equivalent controls are in place.
- **Cross-Tenant Access Restrictions**
 - Explicitly define allowed B2B and cross-tenant trust settings.

6. Azure Backup, Recovery, and Resilience

Misconfiguration exploitation often precedes **destructive or disruptive actions**.

Required Controls

- **Immutable Backups**
 - Enable Azure Backup soft delete.
 - Restrict deletion permissions.
- **Recovery Vault Protection**
 - Separate backup admin roles from subscription admins.
- **Test Restoration**
 - Regularly validate recovery scenarios.

7. Operational Discipline

Required Controls

- **Configuration Drift Monitoring**
 - Compare live resources against IaC baselines.
 - **Red Team / Purple Team Exercises**
 - Explicitly test:
 - Public exposure
 - Role abuse
 - Conditional Access bypass attempts
 - **Change Management**
 - Enforce approvals for:
 - Network changes
 - Identity role changes
 - Public access enablement
-



Think Like an Attacker: Cybersecurity Tips From a CISO

Cybersecurity is a field that touches every aspect of modern life, from personal privacy to global business operations. In Dark Reading's latest episode, Etay Maor, chief security strategist at Cato Networks and professor at Boston College, shares his journey, expertise, and advice for those interested in entering this ever-evolving domain. With a career spanning decades, Maor's unique perspective highlights the many opportunities within cybersecurity and the importance of thinking like an attacker to build effective defenses.

Main Article

From hacking his school's database as a curious teenager to earning advanced degrees in computer science and counterterrorism, Maor's journey underscores the value of curiosity and hands-on learning. Today, Maor leverages his technical expertise and storytelling skills to educate students and professionals alike, emphasizing the need for diverse perspectives in tackling modern cyber threats. His work at Cato Networks and Boston College reflects his commitment to fostering innovation and collaboration in the field.

In this interview, Maor stresses that cybersecurity is not just a technical discipline but a multifaceted field that intersects with law, policy, marketing, and more. He encourages aspiring professionals to explore the wealth of resources available today, from online tutorials to artificial intelligence (AI) tools, and to embrace the industry's collaborative nature. Whether you're a technical expert or someone with a background in law or business, Maor believes there's a place for everyone in cybersecurity, as long as they are willing to learn, adapt, and think creatively.

Action Point:

EM: The main thing I'd like people to take away is not to be shy about trying and experimenting with different areas within cybersecurity. If you want to try hacking into systems, there's a wealth of information available — videos, tutorials, masterclasses, and even [AI chatbots](#) to help you figure things out.

If you're interested in thinking outside the box or understanding how an attacker might approach things, you can help organizations move beyond checklists and adopt more [forward-looking strategies](#).

Give it a try, and don't be afraid to approach cybersecurity professionals with questions. I'm sure they'll be happy to help.



How Cyber Insurance MGAs Shape Policies for Evolving Cyber-Risks

Managing general agents (MGAs) underwrite and administer insurance policies on behalf of insurance companies. Just as a broker serves as an intermediary between the buyer and the insurer, the MGA acts as an agent for the insurer. While the insurance companies ultimately carry the risk, they delegate to MGAs the work of designing coverage, assessing applicants, and setting terms. Some MGAs may even handle claims.

Main Article

"To anyone from the outside, they look like insurance companies, but they're actually not — they're intermediaries," explains Ben Beeson, founder and CEO of Galahad Risk Solutions, a cyber insurance brokerage. "They're an insurance vehicle that looks like an insurance company."

MGAs exist broadly across the insurance industry to help insurers enter areas of risk where they lack expertise. MGAs bring deep subject matter expertise to the underwriting process in areas such as cybersecurity, where there is a lack of longstanding actuarial data or standardization of how these specialized risk areas are measured and managed.

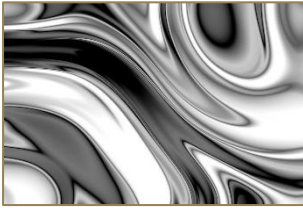
Action Point: Weighing the MGA Pros and Cons

Because they're insurance company intermediaries, MGAs rarely work directly for the insured. A company still needs a broker to help it navigate the options and find the best policy and terms. This is where the value of having a specialized cybersecurity insurance broker becomes apparent.

"The security tools offered by MGAs will have less relevance the bigger you are, but you may like the policy form and what it offers compared to a large insurance company," Beeson explains.

The MGA market typically underwrites businesses with up to \$1 billion in revenue, he adds. Larger companies may opt to work directly with insurance carriers for balance sheet protection, but midmarket companies can often go either way, depending on their specific needs.

"Maybe there's something specific you can't get from regular insurance companies that an MGA is offering," Beeson says. "Or maybe it's how cyber warfare is defined, or challenges around third-party risk and how to get coverage that covers your supply chain. If the brokers are doing their jobs, they'll know all of these details and understand the risk posture to help decide whether an MGA is the best fit."



Apple Patches Two Zero-Days Tied to Mysterious Exploited Chrome Flaw

Apple has released macOS and iOS updates to patch dozens of vulnerabilities, including two zero-days that the tech giant says have been exploited in highly targeted attacks.

[Main Article](#)

According to Apple's [advisories](#), the zero-days impact WebKit, the browser engine present in Safari, iOS, iPadOS, macOS, tvOS, watchOS, and visionOS.

One of the zero-days, CVE-2025-14174, has been described as a memory corruption issue, while the second, CVE-2025-43529, is a use-after-free bug. They can both be exploited using maliciously crafted web content to execute arbitrary code.

Apple announced patches for CVE-2025-14174 and CVE-2025-43529 with the release of [iOS and iPadOS 26.2](#), iOS and iPadOS 18.7.3, [macOS Tahoe 26.2](#), Safari 26.2 for macOS, tvOS 26.2, watchOS 26.2, and visionOS 26.2.

However, Apple's advisories clarify that the vulnerabilities have been exploited in "an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26".

Action Point: It appears Google and Apple have been coordinating the disclosure and patching of the vulnerability. According to Google's advisory, the issue came to light on December 5.

Google has not shared any information on attacks targeting Chrome users.

It's also worth noting that the Angle library is used by Chromium, and other Chromium-based browsers such as Edge, Opera, Vivaldi, and Brave are impacted as well.

Microsoft has already [updated Edge](#) to address CVE-2025-14174. [Vivaldi](#) has also been updated to patch the zero-day.



In-the-Wild Exploitation of Fresh Fortinet Flaws Begins

Threat actors have started exploiting two recent Fortinet vulnerabilities only days after patches were released, Arctic Wolf warns.

[Main Article](#)

The two flaws, tracked as CVE-2025-59718 and CVE-2025-59719 (CVSS score of 9.8), are described as improper verification of cryptographic signature issues impacting FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager.

[Fortinet rolled out fixes](#) for the two bugs on December 9, warning that they can be exploited via crafted SAML response messages to bypass the FortiCloud SSO login authentication. While disabled in default factory settings, SSO login authentication is enabled when an administrator registers a new device to FortiCare, unless they specifically disable the feature from the registration page.

Action Point: Administrators are advised to hunt for potential malicious activity and to reset credentials if any is discovered. Access to the firewall management interface should be restricted to trusted internal networks.

Patches for the exploited Fortinet vulnerabilities were included in FortiOS versions 7.6.4, 7.4.9, 7.2.12, and 7.0.18, FortiProxy versions 7.6.4, 7.4.11, 7.2.15, and 7.0.22, FortiSwitchManager versions 7.2.7 and 7.0.6, and FortiWeb versions 8.0.1, 7.6.5, and 7.4.10. Fortinet recommends disabling the 'Allow administrative login using FortiCloud SSO' feature to prevent exploitation.



Acumen Cyber Threat Intelligence Digest: Week 50

The Week 50 Cyber Threat Intelligence Digest highlights significant vulnerabilities, active threat operations, and recommended remediation actions observed across the cyber landscape. A critical focus is on CVE-2025-55182 ("React2Shell"), a severe remote code execution vulnerability in React Server Components. Active exploitation from 8 December was reported by Huntress, with threat actors scanning internet-facing Next.js systems and deploying diverse malware including cryptominers, backdoors, reverse proxies, and Sliver frameworks. Organisations using these components are urged to urgently patch and harden public applications.

Main Article

In addition, three PCI-SIG-disclosed vulnerabilities (CVE-2025-9612, CVE-2025-9613, CVE-2025-9614) affecting the PCIe IDE protocol were detailed. These flaws—impacting Intel Xeon and AMD EPYC platforms—could lead to information disclosure, privilege escalation, or denial of service if unmitigated. Although there were no reports of active exploitation at the time, vendors have issued engineering change notifications for mitigation.

Another high-severity disclosure involved CVE-2025-8351 in macOS Avast Antivirus, a heap-based overflow with potential local code execution or denial-of-service impact; organisations are advised to update to fixed releases promptly.

On the threat actor front, activity by China-linked "Ink Dragon" expanded into European government networks, leveraging ShadowPad IIS listeners and a new FinalDraft backdoor, while Russian state-linked Sandworm operations targeted misconfigured network edge devices to harvest credentials and sustain access across western critical infrastructure.

General cyber news included broader exploitation of React2Shell by multiple Chinese-aligned clusters, emergence of Cellik Android malware-as-a-service, and a confirmed cyberattack against the French Interior Ministry's email servers.

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-2025-55182 (React2Shell): This vulnerability can be addressed by updating React Server Components to a fixed version and remediating publicly exposed Next.js deployments.
- PCIe IDE Protocol Vulnerabilities (CVE-2025-9612, CVE-2025-9613, CVE-2025-9614): These issues can be mitigated by applying vendor-provided Engineering Change Notification updates for affected Intel Xeon and AMD EPYC systems and reviewing PCIe transaction handling configurations.
- CVE-2025-8351 (Avast macOS): This vulnerability can be remediated by updating Avast Antivirus on macOS to a fixed release that resolves the heap-based buffer overflow and out-of-bounds read issues.

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.



[Critical macOS Flaw Lets Attackers Bypass Apple Privacy Controls Without Consent](#)

A newly disclosed macOS vulnerability—CVE-2025-43530—poses a serious privacy and security risk by completely bypassing Apple's Transparency, Consent, and Control (TCC) system. TCC is supposed to be the gatekeeper that ensures apps can't access sen...

Steve McIntosh

1/9/2026

3 views



[Acumen Cyber Threat Intelligence Digest: Week 1 - 2026](#)

The biggest headline is around React2Shell (CVE-2025-55182) —a serious code-execution vulnerability affecting multiple versions of React Server Components. The disclosure happened in early December 2025, and within 24 hours, multiple China-nexus thr...

Steve McIntosh

1/8/2026

7 views



[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.

Steve McIntosh

1/8/2026

7 views



[900,000 Users Hit as Malicious Chrome Extensions Steal ChatGPT, DeepSeek Chats](#)

This article covers a major data-theft campaign involving malicious Chrome extensions that secretly harvested ChatGPT and DeepSeek conversations from more than 900,000 users . These extensions posed as harmless productivity tools, but once installed...

Steve McIntosh

1/8/2026

6 views



[CISA Flags Microsoft Office and HPE OneView Bugs as Actively Exploited](#)

CISA has added two newly highlighted security flaws—one in Microsoft Office PowerPoint and one in HPE OneView—to its Known Exploited Vulnerabilities (KEV) catalogue, meaning there's credible evidence that attackers are actively exploiting them. In s...

Steve McIntosh

1/8/2026

5 views



[Are criminals vibe coding malware? All signs point to yes](#)

The article digs into the rise of “vibe coding”—a trend where people (including cyber-criminals) increasingly use AI-assisted coding tools like Replit, Cursor, Claude, or similar platforms to generate software quickly. According to Palo Alto Networ...

Steve McIntosh

1/8/2026

7 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.



Critical macOS Flaw Lets Attackers Bypass Apple Privacy Controls Without Consent

<https://www.techrepublic.com/article/news-macos-flaw-apple-privacy-controls/>

A newly disclosed macOS vulnerability—**CVE-2025-43530**—poses a serious privacy and security risk by completely bypassing Apple's Transparency, Consent, and Control (TCC) system. TCC is supposed to be the gatekeeper that ensures apps can't access sensitive resources like the microphone, camera, documents, or AppleEvents without explicit user approval. This flaw lets attackers skip all of that silently.

The issue comes down to how macOS historically trusted certain accessibility services, especially **VoiceOver**, which is designed to support visually impaired users. VoiceOver and its related services (ScreenReader.framework and com.apple.scrod) effectively operate with elevated, system-level privileges—and Apple treated them as inherently trustworthy. Researchers uncovered **two key weaknesses** that, when chained together, break that trust model completely:

1. **macOS trusted Apple-signed binaries without verifying modification.**
Because validation relied on file location and signature alone, an attacker could inject a malicious dynamic library into one of these trusted system binaries and hijack its privileges. No admin rights needed.
2. **A classic Time-of-Check-Time-of-Use (TOCTOU) flaw.**
Attackers can modify a process *after* TCC checks have passed but *before* the process executes. That creates a tiny but exploitable window where malicious code can run with trusted privileges.

Once exploited, attackers can run arbitrary AppleScript, send AppleEvents to any application (including Finder), and silently access protected files, user data, and even microphone input—all without triggering the usual pop-ups or permission prompts. Since the attack doesn't require admin rights and can be executed locally, it's especially dangerous in shared-device environments, research labs, education settings, and any enterprise where initial access may be easy to achieve.

There's currently **no evidence of in-the-wild exploitation**, but **proof-of-concept code is already available**, which almost always accelerates threat-actor adoption.

Apple has issued a fix in **macOS 26.2**, but the article is clear: patching alone isn't enough. This is another example of the risks created when security models rely too heavily on implicit trust in privileged system components. Once that trust breaks, the privacy model collapses.

Action Point:

Patch immediately

- Upgrade all macOS devices to **macOS 26.2 or later**.

Audit accessibility & automation permissions

- Review VoiceOver, AppleScript, AppleEvents, and related entitlements.
- Restrict access to only approved applications.

Enforce least privilege on macOS endpoints

- Reduce local admin rights.
- Limit developer tools unless required.
- Block execution from user-writable locations.

Monitor for exploitation behaviours

- Unexpected AppleScript execution.
- Finder manipulation.
- Abnormal AppleEvent activity.
- dylib injection attempts.

Harden endpoint configuration

- Ensure Gatekeeper and System Integrity Protection (SIP) are enabled.
- Block unsigned or modified dynamic library loading.

Strengthen detection & response

- Centralise macOS logs.
- Conduct threat hunting for entitlement abuse.
- Rehearse incident response for local privilege-bypass scenarios.



Acumen Cyber Threat Intelligence Digest: Week 1 - 2026

<https://acumencyber.com/cyber-threat-intelligence-digest-january-2026-week-1>

The biggest headline is around **React2Shell (CVE-2025-55182)**—a serious code-execution vulnerability affecting multiple versions of React Server Components. The disclosure happened in early December 2025, and within 24 hours, multiple **China-nexus threat groups** (Earth Lamia, Jackpot Panda and others) were already exploiting it. Because the flaw is rooted in unsafe payload deserialisation, attackers can hit back-end systems by sending crafted HTTP requests. Patches exist, but the speed and scale of adoption means unpatched systems are highly exposed.

Two additional vulnerabilities are covered:

CVE-2025-55181 in Facebook's Proxygen library, which can cause infinite loops and memory exhaustion when handling huge payloads; and **CVE-2025-59789** in Apache bRPC, a critical stack-exhaustion bug triggered by deeply nested JSON. Neither is currently being exploited, but both are easy crash-vectors and must be patched quickly.

There's also a seasonal spike in **DocuSign-themed phishing** and fake **holiday loan scams**. These lure victims into entering corporate credentials or personal financial data using very realistic branding and third-party hosting services that make the attacks look legitimate. Forcepoint's analysis shows attackers exploiting services like Fastly, Glitch and Surge to make phishing flows harder to detect.

The supply-chain risk section describes **NeoShadow**, an npm campaign using typosquatted JavaScript packages uploaded in late December. These packages deliver multi-stage Windows backdoors using MSBuild, RuntimeBroker injection, Ethereum smart contracts to fetch C2 endpoints, and strong obfuscation techniques. A new variant found in January 2026 appears even harder to analyse, signalling ongoing refinement.

Beyond technical threats, the article also notes several major UK developments:

- The UK government has admitted that years of cyber policy have not worked and is resetting its nationwide strategy, including creating a Government Cyber Unit.
- Jaguar Land Rover revealed significant financial losses from its 2025 cyberattack, showing the long-tail business impact of major incidents.

Action Point:

Patch immediately:

- React Server Components (React2Shell) → upgrade to **19.0.1 / 19.1.2 / 19.2.1**
- Proxygen → **v2025.12.02.00+**
- Apache bRPC → **1.15.0+**

Hunt for exploitation:

- Look for suspicious React server-function traffic or malformed payloads.
- Monitor for npm typosquats and unexpected package updates.

Restrict supply chain exposure:

- Enforce package allowlists for npm.
- Review developer MFA and code-signing enforcement.

Strengthen phishing resilience:

- Warn users about DocuSign-themed and holiday-loan phishing.
- Block known malicious domains (Fastly/Glitch/Surge-hosted phishing pages).

Review resilience planning:

- Use Higham Lane School and JLR as reminders of operational exposure.
 - Validate incident response, especially for outage-heavy scenarios.
-



900,000 Users Hit as Malicious Chrome Extensions Steal ChatGPT, DeepSeek Chats

<https://www.techrepublic.com/article/news-900k-users-chrome-extensions-steal-chatgpt-deepseek-chats/>

This article covers a major data-theft campaign involving **malicious Chrome extensions** that secretly harvested ChatGPT and DeepSeek conversations from more than **900,000 users**. These extensions posed as harmless productivity tools, but once installed, they quietly turned into full-scale surveillance implants.

The attackers' trick was simple: they asked users for permission to collect "anonymous, non-identifiable analytics data." In reality, the extensions used Chrome's legitimate APIs to monitor browsing activity in real time. The key capability was the `chrome.tabs.onUpdated` API, which let the extensions watch for when users opened or interacted with AI chat platforms.

Once a user landed on ChatGPT or DeepSeek, the extension interacted directly with the page's DOM—meaning it scraped whatever the user could see. That included **full prompts, the AI's responses, and session metadata** that linked conversations back to individual users. Because the theft happened inside the browser, attackers didn't need exploits, man-in-the-middle interception, or fancy network techniques. The browser *was* the breach. Each infected browser got its own identifier so attackers could build detailed user profiles over time. Alongside AI chats, the extensions also collected the URLs of every open tab—giving attackers insight into internal systems, corporate dashboards, cloud consoles, and any sensitive web apps the victim visited.

Data was cached locally, bundled up into Base64-encoded chunks, and shipped off to attacker-controlled servers every 30 minutes. This drip-feed approach reduced suspicion while enabling large-scale harvesting.

The big takeaway is that this whole incident didn't rely on zero-days or high-end malware. The attackers simply abused Chrome's extension system and users' trust. Excessive permissions, vague consent wording, and weak extension governance created the perfect storm.

As AI tools become embedded in daily workflows, browser extensions are quietly becoming one of the most dangerous—and overlooked—attack surfaces. The article stresses that organisations need to treat browser extensions with the same seriousness as any other privileged software component.

Action Point:

Remove & investigate

- Immediately purge malicious extensions from all managed browsers.

- Audit endpoint telemetry to identify affected users and potential data loss.

Implement extension governance

- Enforce allowlists; block all unapproved extensions.
- Prevent sideloading and revalidate extensions when permissions change.

Manage browsers as corporate assets

- Use enterprise browser profiles to lock down installation rights.

Protect AI usage

- Apply DLP and logging to AI interactions.
- Limit sensitive data entered into AI tools.

Monitor for suspicious extension behaviour

- Watch for odd API usage and unexpected outbound traffic patterns.

Train users

- Educate staff about the risks of browser extensions—especially AI-related ones.



CISA Flags Microsoft Office and HPE OneView Bugs as Actively Exploited

<https://thehackernews.com/2026/01/cisa-flags-microsoft-office-and-hpe.html>

CISA has added two newly highlighted security flaws—one in Microsoft Office PowerPoint and one in HPE OneView—to its **Known Exploited Vulnerabilities (KEV)** catalogue, meaning there's credible evidence that attackers are actively exploiting them. In short: these aren't theoretical anymore. They're being used in real-world attacks, and organisations need to patch fast.

The first flaw, **CVE-2009-0556**, is actually an old PowerPoint vulnerability from 2009 with a CVSS 8.8 score. It allows attackers to run arbitrary code via memory corruption. Even though it's ancient, it's now being exploited again, which shows that legacy Office installations are still floating around in places where they really shouldn't be.

The second is much more severe: **CVE-2025-37164**, a CVSS 10.0 remote code execution flaw impacting **all versions** of HPE OneView prior to 11.00. A public proof-of-concept exploit landed at the end of December 2025, and once that happens, attackers don't need to do much work—they can simply tweak and deploy what's already available. HPE released patches and hotfixes for versions 5.20 through 10.00, but the exposure is huge because OneView is widely deployed in datacentres and often deeply integrated.

CISA has issued its usual directive: U.S. federal agencies must patch these by **28 January 2026**, but realistically every organisation should treat this as an urgent remediation

requirement, not a nice-to-have. Proof-of-concepts accelerate attacker adoption dramatically, and these vulnerabilities enable full remote code execution with minimal effort.

At present, the full details on who is exploiting these or how widespread the attacks are remain unclear. There are no public incident reports yet, but the combination of KEV listing + PoC availability is a clear red flag. If you run OneView and haven't patched, assume compromise is possible.

This situation underlines a recurring theme: older software and infrastructure tools remain high-value targets because patching them is often slow, risky, or operationally painful. Attackers know exactly where those gaps live.

Action Point:

Patch immediately:

- Upgrade HPE OneView to **v11.00 or later**.
- Ensure all Microsoft Office installations are fully up to date; remove unsupported versions.

Hunt for indicators:

- Review logs for suspicious activity around OneView management interfaces.
- Check for unexpected PowerPoint file execution or crashes.

Enforce asset hygiene:

- Decommission legacy Office installs—no exceptions.
- Validate that patching policies include infrastructure tools like OneView, not just endpoints.

Review network exposure:

- Ensure management interfaces like OneView aren't exposed to the internet.
- Apply MFA or IP restrictions where possible.

Are criminals vibe coding malware? All signs point to yes

https://www.theregister.com/2026/01/08/criminals_vibe_coding_malware/



The article digs into the rise of “*vibe coding*”—a trend where people (including cyber-criminals) increasingly use AI-assisted coding tools like Replit, Cursor, Claude, or similar platforms to generate software quickly. According to Palo Alto Networks’ Unit 42, there’s now *very likely* evidence that attackers are using these tools to build malware, including

writing API calls directly into the malicious code to ask LLMs how to create payloads, write phishing emails, or generate evasion techniques.

But here's the twist: AI generates mistakes. The same hallucinations and sloppy logic we see when AI writes legitimate code also show up in malicious code. Examples include bogus evasion techniques that don't actually work, or ransom notes saved as *readme.txt*—the sort of typo no seasoned operator would make. This creates a kind of “*security theatre*” where attacks *look* sophisticated but aren't actually functional.

However, defenders shouldn't get complacent. The speed and accessibility of AI tools means criminals can rapidly prototype and iterate. Meanwhile, many organisations are deep into AI adoption without applying basic security discipline. Only about half of the organisations Palo Alto works with have **any** limits on AI usage, and most have done no formal risk assessment. To address this growing risk, Palo Alto proposes the **SHIELD** framework for securing

AI-assisted coding. The acronym stands for:

- **Separation of Duties** – Restrict AI agents to dev/test environments; enforce access boundaries.
- **Human in the Loop** – Mandate human code review and PR approvals.
- **Input/Output Validation** – Sanitise prompts and validate outputs using techniques like SAST.
- **Enforce Security-Focused Helper Models** – Use AI specialised in security checks (secrets scanning, SAST, control verification).
- **Least Agency** – Give AI tools the minimum permissions necessary.
- **Defensive Technical Controls** – Controls around supply chain, execution management, and disable auto-execution by default.

The message is simple: AI coding tools bring speed, but without boundaries they introduce risk—fast.

Action Point:

Inventory & Risk Assess AI Tools

Identify which AI coding tools are in use; formally assess security, privacy, and data-handling risks.

Define Approved Tools

Allow *one* approved conversational LLM; firewall-block the rest.

Implement SHIELD Framework Controls

Particularly: least privilege, prompt sanitisation, SAST on all outputs, and human-in-the-loop reviews.

Create Policy for AI-Assisted Development

Include data boundaries, acceptable-use conditions, and restrictions for sensitive code.

Monitor for AI-generated Indicators

Look for artefacts like LLM watermarking or unusual code signatures indicating AI-generated malware.

Educate Developers and Security Teams

Focus on pitfalls of AI-generated code, especially hallucinations and security gaps.

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