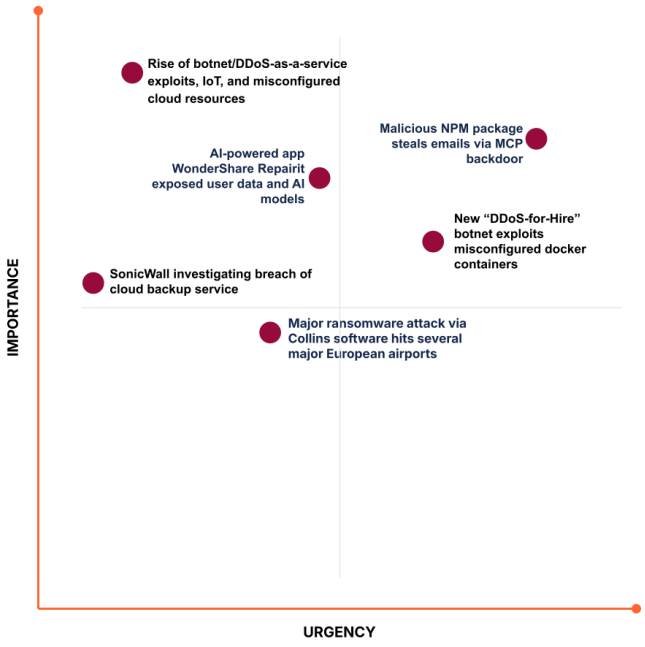
CLOUDFLARE

Cloudflare Cyber Briefing

October 3, 2025

Welcome to the Cloudflare Cyber Briefing from our Field CXO Team, helping leaders stay ahead in a fast-moving landscape of threats, technology shifts, and criminal tactics.

What you need to know:



AI cybersecurity

AI-powered app Wondershare Repairit exposes user data and AI models

Security researchers at Trend Micro have discovered two critical authentication bypass vulnerabilities in Wondershare Repairit, a data repair and photo editing

application. The vulnerabilities, CVE-2025-10643 (CVSS score: 9.1) and CVE-2025-10644 (CVSS score: 9.4), could allow an attacker to circumvent authentication, launch a supply chain attack, and execute arbitrary code on users' systems, via downloading malicious AI models the software offers for local editing purposes.

CISO's takeaway: As AI introduces threats like model tampering and data poisoning, CISOs must embed AI security into their strategies. At the same time, they must tackle ongoing risks from insecure coding, embedded credentials, and cloud misconfigurations. Championing DevSecOps, enforcing secrets management, and deploying strong cloud security posture management (CSPM) are essential to uphold least-privilege principles and strengthen resilience.

Source: The Hacker News *Read more →*

Malicious npm package steals emails via MCP backdoor

A malicious npm package, **"postmark-mcp,"** was discovered to have a backdoor that secretly stole user emails. The package, a Model Context Protocol (MCP) server, was downloaded approximately 1,500 times a week. Starting with version 1.0.16, the developer introduced a single line of code that copied every email processed by the server and sent it to their own personal server. This act of "impersonation" involved taking legitimate code, adding the malicious line, and publishing it under a name that appeared to be official. The flaw in the MCP ecosystem's trust model, where AI assistants can execute commands from these tools without security checks, was a key factor in this attack. It is estimated that thousands of emails, potentially containing sensitive information, were compromised daily. Even after the package was removed from the npm registry, the compromised versions remained active on users' machines.

CISO's takeaway: To counter risks from malicious third-party code and AI-driven tools, CISOs should adopt a layered defense strategy. This includes rigorous vetting with code analysis and publisher reviews before any third-party code is imported into the (S)DLC, enforcing least privilege in development and production, and monitoring for anomalous network activity. A dedicated incident response plan must also be in place — tested regularly to isolate compromised systems, remove malicious code, and ensure clear stakeholder communication.

Source: Koi Security *Read more →*

Cyber incidents

Major ransomware attack via Collins software hits several major European airports

A cyberattack on September 20, 2025, using ransomware, targeted Collins Aerospace's MUSE check-in software, causing significant disruptions at several major

European airports including London Heathrow, Brussels, and Berlin. The attack forced airport staff to switch to manual check-in processes, leading to widespread flight delays and cancellations.

CISO's takeaway: To address supply chain risks, CISOs should build resilience through strong third-party risk management — diversifying vendors, requiring verifiable security assurances, and monitoring supplier posture. Internally, they must harden ransomware defenses with employee training, rapid patching, and tested recovery plans. Contingency strategies should include manual backups and operational workarounds, while a coordinated incident response plan ensures clear communication with teams and the public to limit reputational damage.

Source: Reuters *Read more →*, AVSN *Read more →*

SonicWall investigating breach of cloud backup service

SonicWall is investigating a security incident where hackers used brute-force attacks to access the company's MySonicWall.com portal, gaining access to a small percentage (less than 5%) of backup firewall preference files. While the credentials within these files were encrypted, they also contained other information that could potentially be used to exploit the firewalls. The company has since terminated the unauthorized backup point and is working with law enforcement and cybersecurity firms to investigate the extent of the damage.

CISO's takeaway: To mitigate the risks associated with this type of attack, CISOs should prioritize credential management and security hygiene. This includes enforcing the use of strong, unique passwords and enabling multi-factor authentication (MFA) wherever possible. Organizations should also regularly review and update firewall configurations, and ensure that any cloud backup services used for critical infrastructure are properly secured and monitored for suspicious activity. Furthermore, it is essential to have a well-defined incident response plan in place to quickly address and remediate similar security breaches. This plan should include steps for identifying the scope of the attack, containing the threat, and communicating with affected stakeholders.

Source: Cybersecurity Dive *Read more →*

Cyber insights

Rise of botnet / DDoS-as-a-service exploits, IoT, and misconfigured cloud resources

Distributed denial-of-service (DDoS) attacks have seen an unprecedented surge in the first quarter of 2025, with a 358% year-over-year increase. Hyper-volumetric attacks, exceeding 1 Terabit per second (Tbps), are now a daily occurrence. Ransom

DDoS (RDDoS) is also on the rise, with a 78% increase in reported extortion attempts in the last quarter of 2024. These attacks are no longer just a nuisance; they pose a strategic business risk, often used as a smokescreen for more severe threats like data theft and ransomware. The increasing sophistication of these attacks, including stealthy application-layer (L7) attacks that mimic legitimate user behavior, renders traditional on-premises defense mechanisms obsolete.

CISO's takeaway: The exponential growth and evolving nature of DDoS attacks demand a fundamental shift in defensive strategies. CISOs must recognize that legacy on-premises solutions are no longer adequate and can be a liability. The key to effective defense is a multi-layered, cloud-based, and automated mitigation strategy. This approach should combine robust network-layer and application-layer defenses capable of handling both brute-force volumetric floods and sophisticated low-and-slow attacks. Organizations should also focus on building a resilient infrastructure that can absorb large-scale attacks while maintaining service availability. Finally, a comprehensive incident response plan, including clear communication protocols and procedures for dealing with ransom demands, is crucial for minimizing the impact of a successful DDoS attack.

Source: TechRadar *Read More →*, DeepStrike *Read more →*

New "DDoS-for-hire" botnet exploits misconfigured docker containers

A new "DDoS-for-hire" service, dubbed ShadowV2, has emerged, leveraging misconfigured Docker containers on Amazon Web Services (AWS) to launch powerful distributed denial-of-service (DDoS) attacks. The botnet, first detected in June 2025, utilizes a sophisticated attack toolkit and a Python-based command-and-control (C2) framework hosted on GitHub Codespaces. The attackers breach Docker daemons, primarily on AWS EC2 instances, and deploy a Go-based remote access trojan (RAT) to gain control of the compromised systems. ShadowV2's attack methods are particularly concerning, as they include the ability to bypass Cloudflare's "under attack mode" and execute HTTP/2 Rapid Reset attacks. The botnet's infrastructure is hidden behind Cloudflare, and its user interface suggests it is being offered as a commercial service.

CISO's takeaway: The emergence of the ShadowV2 botnet highlights the critical importance of robust cloud security posture management, with a specific focus on securing containerized environments like Docker on AWS. CISOs must ensure that their organizations have implemented strict security controls, conduct regular security audits, and continuously monitor their cloud infrastructure to identify and remediate misconfigurations before they can be exploited. The sophistication of this "DDoS-for-hire" service, with its advanced evasion techniques, underscores the need for a multi-layered defense strategy. This should include not only preventative measures but also advanced DDoS mitigation services and a well-rehearsed incident response plan to

ensure a swift and effective response to such attacks. The "as-a-service" nature of this threat means that even less sophisticated actors can now launch powerful attacks, making a proactive defense and a strong security culture within the organization more important than ever.

Source: The Hacker News *Read more →*

Cloudflare insights

Cloudflare continuously enhances our security capabilities to address the very threats discussed above. Here's how our products and recent improvements provide tangible solutions:

Giving users choice with Cloudflare's new Content Signals Policy

- There are companies that scrape vast troves of data from the Internet every day. There is a real cost to website operators to serve these data scrapers, in particular when they receive no compensation in return — we are experiencing a classic free-rider problem. This is only going to get worse: we expect bot traffic to exceed human traffic on the Internet by the end of 2029, and by 2031, we anticipate that bot activity alone will surpass the sum of current Internet traffic.
- The Content Signals Policy integrates into website operators' robots.txt files. It is human-readable text following the # symbol to designate it as a comment. This policy defines three content signals — search, ai-input, and ai-train — and their relevance to crawlers.
- If you already know how to configure your robots.txt file, deploying content signals is as simple as adding the Content Signals Policy above and then defining your preferences via a content signal.

An AI Index for all our customers

- Cloudflare will soon automatically create an AI-optimized search index for your domain, and expose a set of ready-to-use standard APIs and tools including an MCP server, LLMs.txt, and a search API. For AI builders, Cloudflare will offer a new way to discover and retrieve web content.

Regional traffic and Certificate Transparency (CT) insights on Cloudflare Radar

- We're now leveraging our internal LLM, Cloudy, to generate automated summaries within our Cloudflare Email Security product, helping SOC teams better understand what's happening within flagged messages.

Cloudflare just got faster and more secure, powered by Rust

- We've replaced the original core system in Cloudflare with a new modular Rust-based proxy, replacing NGINX. It's not only substantially faster for all our customers, it's also more secure, and lets us ship new products quicker than ever before.

Cloudflare Introduces NET Dollar to Support a New Business Model for the AI-Driven Internet

- We've announced plans to introduce NET Dollar, a new US dollar-backed stablecoin that will enable instant, secure transactions for the agentic web. NET Dollar will help power a new business model for the Internet that rewards originality, sustains creativity, and enables innovation in an AI-driven world.

In case you missed it...

Uncover the signal from the noise and focus on today's most important cybersecurity trends via our Security Signal series.

Security Signal

Each episode of the Security Signal podcast translates cybersecurity complexities into actionable intelligence for executives at the helm.

Episode 2 Security Signal: Adversarial AI

Read the full 2025 Cloudflare Signals Report: Resilience at Scale.

Find more resources from the CXO team here:

- **James Todd, Field CTO:** Quantum threats are real — is your security ready?
- **Khalid Kark, Field CIO:** Reimagining cyber resilience
- **Christian Reilly, Field CTO:** AI 'Gold Rush' Demands Calculated Security Approaches