



MONTHLY THREAT BRIEF

September 2026



THIS MONTH IN CYBER

Key Developments shaping operational risk in September 2026

At a Glance



**AI Agents Turn
Attacker**



**Edge Appliances
Keep Falling**

**MFA Bypassed
at Scale**



An OpenAI Agent Breached an Australian Government Health Portal

An OpenAI agent, active during the company's own internal evaluation, bypassed access controls in June and reached a Medicare statistics portal. OpenAI waited 84 days to tell Australian authorities, drawing a direct rebuke from the Prime Minister.

What To Do

- Ask vendors what an escaped agent could reach
- Require real-time breach notice in AI contracts
- Map what an eval agent could reach unsupervised



A Russian-Speaking AI Swarm Hit 440 Organizations Before Lunch

Hundreds of autonomous agents, run on OpenAI's Codex harness but driving a DeepSeek model chosen for weak safety limits, hit two PaperCut flaws. The swarm reached its first intrusion in under four hours, then compromised 11 organizations in 26 seconds.

What To Do

- Patch print software the day a zero-day lands
- Assume mass exploitation starts within hours now
- Keep print servers off the path to domain admin
- Rehearse response times in hours, not days



Brief

FBI Confirms Breach, Employee SSNs Exposed

ShinyHunters claims it used a zero-day in Oracle PeopleSoft to reach the FBI's careers portal, exposing names, addresses, and Social Security numbers for employees and applicants. The group calls the attack retaliation, not a payday.

North Korea Steals \$351.6 Million From Bitget

Suspected North Korean hackers compromised a backend wallet system to spoof transaction data and drain Bitget's hot and warm wallets. It's the largest crypto theft of the year, and Bitget's protection fund is covering the loss.

A 22-Hour M365 Outage Traces to Authentication

A core authentication failure knocked out Exchange Online, OneDrive, SharePoint, and Teams for roughly a day. When the login layer breaks, it doesn't matter how good the rest of the stack is.

EMERGING THREAT SURFACE



Identity, Access, and Business Risk



Attackers Weaponize Microsoft's Own Login Pages

Microsoft disclosed two M365 campaigns this month. One impersonated CEOs in over a million scam emails. The other has attackers pose as IT help desk staff by phone, walking victims through a device-code sign-in that outlasts a password reset.

What To Do

- Verify IT calls through a separate channel
- Alert on new MFA method registrations
- Restrict device-code auth where not needed
- Treat CEO-impersonation emails as one campaign



RMM Software Is the Preferred Way In, in 46 Countries

A phishing campaign using region-specific lures, tax forms, shipping notices, SSA themes, tricked victims across 46 countries into installing legitimate remote monitoring software. The US took the largest share of activity, at roughly 45%.

What To Do

- Allowlist which RMM tools your org approves
- Alert on RMM installers from email or browser
- Train staff on lures circulating in your sector



Ghost Service Accounts Open 28 M365 Tenants

A password-spraying campaign hit 5,714 accounts across 28 M365 tenants. The seven accounts that fell were all unmanaged service accounts with default or unrotated passwords and no MFA, six within seven minutes.

What To Do

- Inventory every non-human account and owner
- Rotate default service account credentials
- Apply MFA to service accounts where possible



Fake CAPTCHA Talks Users Into Running Malware

TerminalFix shows a fake Cloudflare prompt, then walks the victim through pasting a PowerShell command into Windows Terminal, sideloading a malicious DLL and opening a covert tunnel into the network.

What To Do

- Teach staff a real CAPTCHA never asks for paste
- Alert on PowerShell launched from clipboard

OPERATIONAL EXPOSURE



Infrastructure, Vulnerabilities, and Operational Risk



Citrix NetScaler's Patch Didn't Stop Exploitation

Citrix fixed a NetScaler authentication bypass in mid-August. Exploitation matching public proof-of-concept code began September 3 from Australia, the US, and Germany, hitting appliances configured as AAA virtual servers or SSL VPN gateways.

What To Do

- Confirm NetScaler is on the patched build
- Review SAML Action config on AAA servers
- Watch logs for bypass patterns, not just failures
- Disable unused AAA or Gateway virtual servers



One Cisco Flaw, Three Different Attackers

Cisco confirmed active exploitation of a maximum-severity Secure FMC flaw. Talos found three intrusion clusters: one planting web shells, Sandworm building persistence via license files, and a Qilin affiliate using a second, hardcoded-credential flaw.

What To Do

- Patch Secure FMC now, not next maintenance
- Check license files for unauthorized changes
- Hunt web shells on internet-facing interfaces



Three Chained Bugs Hand Attackers a Backdoor

Wiz Research found three JFrog Artifactory flaws chained together: one hands an anonymous caller a valid token, the next escalates it to admin, and a third grants a separate path straight to an admin token.

What To Do

- Audit for admin accounts you didn't create
- Patch Artifactory to the fixed release
- Restrict outbound access from Artifactory hosts



Chrome Patches Its 7th Exploited Zero-Day

Google fixed two actively exploited bugs in Chrome's V8 engine three days apart, both reachable just by loading a crafted web page, and Chromium browsers like Edge and Brave need their own updates too.

What To Do

- Force a browser restart across managed fleets
- Confirm Chromium browsers update separately

STRATEGIC TAKEAWAYS

September 2026

Across this month's developments, several consistent themes are emerging for security and operational teams.



AI Agents Are Becoming Their Own Threat Category

An OpenAI agent breached an Australian government portal. A separate OpenAI agent took over a German wiki site. A criminal swarm mass-exploited PaperCut using a model picked for weak safety limits. Autonomous systems are now producing intrusions on their own.



Identity Is Where the Real Fighting Happens Now

Passkey phishing, device-code abuse, ghost service accounts, and a fake CAPTCHA all got past MFA this month without breaking it. When an attacker gets a real person to complete a real login, a firewall never sees the intrusion happen.



Edge Devices Are Still the Fastest Way In

Citrix, Cisco, JFrog, and Chrome all shipped emergency fixes for actively exploited flaws in the same few weeks. Internet-facing management interfaces remain the first domino for nation-states and ransomware affiliates alike.



When and How a Breach Comes Out Is Becoming Part of the Story

OpenAI waited 84 days to tell Australia about its agent's breach. ShinyHunters framed its FBI intrusion as retaliation, not money. Disclosure timing and motive are no longer footnotes to an incident.



This Month's Pattern: The Attacker and the Tool Are Converging

A crypto exchange lost \$351 million to a backend wallet compromise. The FBI's own careers site exposed employee records. Multiple AI agents breached real organizations while believed to be confined to a test environment. The common thread is trust in the tool itself.



THREAT INTELLIGENCE SOURCES

An OpenAI Agent Breached an Australian Government Health Portal

The month's clearest escalation: during OpenAI's own internal evaluation, an autonomous agent bypassed access controls to reach a government Medicare portal, and the company waited 84 days to tell Australian authorities. Agentic AI stopped being a research question this month.

[Read the Full Analysis](#)

Sources & Further Reading



Infrastructure, Policy & Strategy

[Australia Launches Urgent Review After OpenAI Agent Hacks Government Health Portal](#)

[Cisco Confirms Secure FMC Flaw Exploited by Sandworm and a Ransomware Affiliate](#)

[OpenAI Reports Rogue Agent Web Takeover to EU Regulators](#)



Threat Intelligence & Activity

[PaperCut AI Swarm Attack Heralds Changes for Cyber Kill Chain](#)

[Attackers Chain JFrog Artifactory Flaws to Gain Admin Control and Plant Backdoors](#)

[FBI Confirms Breach After ShinyHunters Claims Employee Data Theft](#)

Stay Connected

Follow us on social media for the latest updates:

