MONTHLY THREAT BRIEF

October 2026



THIS MONTH IN CYBER

Key Developments shaping operational risk in October 2026

At a Glance

Firewalls and VPNs Stay Under Fire

Physical Systems Join the Blast Radius

AI Speeds Up Supply Chain Attacks

Backup Vendor Breach Exposed 2,200 Microsoft 365 Environments

Microsoft tied the ConnectWise Cloud Backup compromise to Storm-0940, a China-aligned group, and to ARTEX, an agentic AI testing framework used for recon, password spraying, and OAuth app abuse. Reported scale is over 2,200 tenants, and some attackers held privileged cloud access within hours.

What To Do

- Ask MSPs whether any tenant uses ConnectWise Cloud Backup
- Audit app credentials and role grants
- Review service principal sign-ins

North Korea Takes $6.3 Billion From Binance

Blockchain analysts at TRM Labs, Chainalysis, and Elliptic attribute the theft to TraderTraitor. Most of it left in about 20 minutes. Binance says it traced the start to a DevOps engineer's laptop, froze roughly $3 billion, and will cover the losses itself.

What To Do

- Treat engineer laptops as privileged infrastructure
- Require hardware-key approval on any large transfer path
- Pre-agree who can freeze assets, and how fast

Brief

French Supermarket Fridges Pushed to 50°C

Hackers reached remote-management software for refrigeration units at hundreds of stores, causing fires and spoiled food. Reporting points to a flaw in software from Danfoss. A second wave hit chains in early November.

FEC Pulls Its Filings Site

The Federal Election Commission took its electronic filing system offline on October 27 after a reported hacking attempt. The outage temporarily prevented political committees from submitting mandatory campaign finance disclosures just days before the midterm elections.

Hospital Diverts Patients, Quest Reports a Breach

A major New Mexico hospital closed clinics and diverted patients after a cyber incident disrupted operations. Quest Diagnostics also reported that some patient records were exposed.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Identity, Access, and Business Risk

Joint Advisory Details China-Linked Network Intrusion

The October 8 advisory ties Flax Typhoon activity to Integrity Technology Group. The chain runs from automated discovery with MicroScan to password spraying on Exchange and M365, mailbox collection, SoftEther VPN persistence, and DCSync. DOJ later seized infrastructure behind MicroScan and FishHub.

What To Do

- Sweep for old CVEs added to KEV on October 8
- Hunt SoftEther binaries named like Windows components
- Review directory replication events (4662)

A Leak Shows What Law Firms Are Paying to Extortionists

Leaked records expose payments to the Silent Ransom Group, also called Luna Moth, which has extorted millions from law firms. The playbook is plain: a call from "IT support," a push to install remote-access software, and sometimes a visitor in person.

What To Do

- Call the help desk back on a number you hold
- Permit only remote-access tools IT has signed off on
- Vet physical visitors at front desks

Device-Code Phishing Goes Commercial

The Wazza phishkit targets banking, government, and manufacturing in the US, using the device-code flow so a victim finishes a real Microsoft login for the attacker. It is now turning up in email compromise investigations.

What To Do

- Restrict device-code flow in conditional access
- Filter sign-ins by device-code protocol
- Block the kit's known domains

Developer Tools Became the Target

Researchers audited 15,465 public MCP servers, and 15.6% resolved to foreign infrastructure. A poisoned LiteLLM release sat on PyPI for 1 hour 44 minutes. The browsers inside VS Code, Cursor, Copilot, and Codex were broken too.

What To Do

- Pull skills and MCP servers from vetted sources only
- Rotate GitHub tokens, then check audit logs for odd branches

CONTINUED ON NEXT PAGE »

OPERATIONAL EXPOSURE

Infrastructure, Vulnerabilities, and Operational Risk

Fortinet Had a Rough Month

FortiBleed holds credentials for 86,644 devices in 194 countries, and the FBI says it's still active, with INC, Lynx, and Payload among the ransomware groups involved. FortiMail added an exploited zero-day with unauthenticated file writes, and FortiOS carried a PEERSTITCH payload.

What To Do

- Inventory every internet-exposed FortiGate
- Patch FortiMail to 7.6.7, 7.4.9, or 8.0.2
- Rotate credentials on exposed devices

Five More Edge Vendors Had Exploited Fixes

Citrix NetScaler (SAML zero-day, then reboot loops after the patch), Palo Alto PAN-OS (Qilin and INC bypassing MFA), SonicWall SMA 1000 (135 attempts after patching), BeyondTrust, and Arista VeloCloud all shipped fixes for exploited flaws. Ivanti and Fortinet make seven.

What To Do

- Get a written list of edge appliances each client runs
- Keep management interfaces off the internet
- Check KEV deadlines before the weekly meeting

PHP2Shell Reached Roughly 4 Million Servers

PHP released emergency fixes on October 21 for two critical RCE flaws already targeted by attackers. Two days later, PHP disclosed another unpatched RCE involving session upload progress. PHP 8.1 and older remain without fixes.

What To Do

- Move to 8.5.12, 8.4.27, 8.3.36, or 8.2.35
- Plan upgrades for end-of-life PHP
- Disable session upload progress for now

Ivanti Connect Secure Gets a Three-Bug Chain

Attackers chained three flaws for unauthenticated root, then used the appliance to enumerate Active Directory and read BitLocker recovery keys. A second KEV deadline lands November 13.

What To Do

- Confirm whether any Ivanti VPN is in service
- Patch to 25.1.1.3 or 22.8R2.6
- Hunt AD enumeration coming from the appliance

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

October 2026

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



Treat Vendor Access as Your Own Attack Surface

Recent supply chain incidents involving ConnectWise and other trusted services demonstrate how attackers can exploit vendor access to reach downstream customers. Inventory third-party applications, review their permissions in Microsoft 365 and other cloud environments, and remove unnecessary access.



Plan Your Response in Hours, Not Days

ARTEX demonstrated how quickly attackers can conduct reconnaissance and password spraying. Establish rapid escalation procedures, identify who can revoke compromised access, and test response plans to ensure security teams can contain threats before they spread.



Patch Internet-Facing Appliances in Days

Recent vulnerabilities affecting Fortinet, Ivanti, Citrix, Palo Alto, and other vendors highlight the risks of delayed patching. Prioritize actively exploited vulnerabilities, maintain an accurate asset inventory, and establish emergency patching procedures for exposed systems.



Plan for Cyber Events With Physical Consequences

Recent hospital disruptions and election filing outages demonstrate how cyber incidents can interrupt essential services. Identify critical operations, establish manual workarounds, and regularly test recovery procedures to minimize downtime and operational consequences.



Assume Trusted Software Can Be Turned Against You

Backup software, remote management, device-code logins, and developer plugins all did what they were built to do. The intrusion lived inside that trust, so monitor what trusted tools do, not just whether they are installed.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENCE SOURCES

PHP Discloses Another Remote Code Execution Vulnerability Following Emergency PHP2Shell Patches

Two days after the October 21 PHP2Shell fixes, PHP disclosed CVE-2026-115560, a third RCE that those updates do not cover. It only bites a narrow session configuration, and no exploitation is reported. The earlier two flaws are still being hit widely, so confirm those patches first, then check your exposure.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- Hundreds of Supermarkets in France Hit by 'Unprecedented' Cyberattack
- Hackers Used AI to Speed Up ConnectWise Cloud Backup Attack
- Microsoft Links Storm-0940 to ConnectWise Supply Chain Attack

Threat Intelligence & Activity

- FBI Seizes 7 Domains Linked to Flax Typhoon Hacking Tools
- North Korea Linked to $6.3 Billion Hack on Binance
- FBI Warns FortiBleed Remains Active After Amassing 86,644 Fortinet Device Credentials

Stay Connected

Follow us on social media for the latest updates: