Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | OCT. | Vol.3

The News

In the news week



French supermarket attack exposes operational-technology risk

A large-scale cyberattack disrupted connected refrigeration systems at French retailers, warming fridges and freezers, spoiling food and causing fires. French authorities opened an investigation; Danfoss said affected systems used outdated firmware.

The incident shows how internet-reachable maintenance technology can translate directly into safety, service and supply-chain loss. Facilities, retail, logistics and engineering operators should treat remote-control systems as operational assets, not peripheral IT.

Defender focus: inventory remotely administered controllers, remove direct internet exposure, apply supported firmware, enforce vendor-access controls and test safe manual operation when supervisory systems fail.

Read more ›

Other news highlights

Microsoft October update: 1,413 flaws.

–

Docker fixes critical Hub access flaw.

–

SAP Cloud SDK OAuth credential risk.

–

GitLab fixes maximum-severity CI flaw.

The News

Top of the news



FBI and partners describe China-linked portal for stolen email access

The FBI and partner agencies said a China-linked group ran a portal that allowed third parties to access email stolen from organisations in Southeast Asia. The joint account identifies government, law enforcement, healthcare and other organisations among the targets.

The reporting highlights durable exposure from weak account controls, unpatched internet-facing systems and mailbox collection tooling. It also reinforces that compromised cloud identity can become a service offered to other actors.

Defender focus: enforce phishing-resistant MFA, review Microsoft 365 and Exchange sign-in and mailbox-audit activity, remove legacy authentication and rapidly investigate anomalous collection or forwarding rules.

Read more ›

Other news highlights

Another ShinyHunters suspect arrested.

–

Malicious GitHub Actions steal CI secrets.

–

AnyDesk Linux root exploit published.

–

Three teams hack patched Pixel 10s.

Geo-Politics

News from around the world



Flax Typhoon activity drives CISA action on five legacy flaws

CISA added five older vulnerabilities to its Known Exploited Vulnerabilities catalog following reported use by China-linked Flax Typhoon. The affected software includes products used in web, document and application environments.

The update is a reminder that exploitability, exposure and asset ownership matter more than a CVE's age. Legacy services and third-party software can retain real operational risk long after initial disclosure.

Defender focus: compare CISA KEV entries with internet-facing inventories, identify end-of-life software, apply available fixes or compensating controls, and verify that external suppliers own their patch deadlines.

Read more ›

Other news highlights

AhsayCBS exploits deploy XMRig miners.

–

ASHVEIN RAT targets Ukrainian government.

–

MatchBoil malware receives stealth update.

–

Preinstalled Android malware builds proxies.

Breaches

Security Breaches this week



Japan warns of data leaks tied to mobile APIs and exposed platforms

JPCERT/CC reported a rise in data leaks at Japanese organisations involving mobile-app API abuse and attacks on exposed systems, including business-intelligence and employee-management platforms. The alert does not attribute the incidents to one actor or method.

For technology, market-research, property and service organisations, mobile and internal-facing APIs often expose sensitive records when access checks are inconsistent across endpoints.

Defender focus: test authorisation on every API endpoint, block public access to management and analytics platforms, monitor unusual bulk queries and review application logs for the indicators shared by JPCERT/CC.

Read more ›

Other news highlights

Ransomware-recovery owner faces fraud charges.

–

Physical ransomware threats need caution.

–

Emperador claims 37 leak-site victims.

–

Luna Moth archive exposes extortion playbook.

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-96951 | Windows Shell
Microsoft confirms exploitation of a Windows Shell command-injection flaw that can bypass Mark of the Web protections after a user opens crafted content. Install the applicable Windows update and investigate suspicious files, links and downloads.

CVSS score: 8.8

THIS WEEK | CVE-2026-104935 | Ivanti Connect Secure
Ivanti reports limited exploitation of an authentication-bypass and remote-code-execution issue affecting Connect Secure before 25.1.3.0. Upgrade affected appliances immediately and conduct forensic review for compromise indicators.

CVSS score: 8.6

Last weeks recaps

CVE-2026-88779
Citrix NetScaler

CVSS 8.7. Memory overflow can cause denial of service when an appliance operates as a SAML Service Provider or Identity Provider. Apply Citrix's fixed build and review exposed SAML appliances.

CVE-2026-76471
Cisco NX-OS NX-API

CVSS 9.8. An unauthenticated attacker could execute code as root or cause denial of service on affected NX-API-enabled Nexus switches. Upgrade to Cisco's fixed software.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's October-published September report claims 850 ransomware and extortion victims, down 27.0% from August. These are source claims, not independently verified incident totals.

Target industries

The report records manufacturing (147), professional services (99), technology (95), finance (40), education (33), government and defence (28), and transportation (30). All figures are source claims.

Target country

The United States leads CyberXTron's September tally: 269 claimed victims (31.6%). Other leading countries: Germany (38), Brazil (31), Italy (28), Canada (27) and United Kingdom (26).

Top Group

The monthly source reports 91 countries and territories and 80 active groups. Assess named victim claims against direct organisation or authority disclosures before escalation; test recovery and supplier-access controls.

Top Threat Actors

TheGentlemen

105 September victims

-

Qilin

74 September victims

–

Storm

37 September victims

Phishing

Phishing news this week



North Korean phishing campaign targets Ukrainians for war intelligence

Dark Reading reported on a phishing campaign attributed to North Korean operators targeting Ukrainians for military and geopolitical information. The activity uses tailored social engineering to obtain access and intelligence rather than indiscriminate malware delivery.

The campaign is relevant to government, legal, education and policy organisations that receive unsolicited research, media or partnership requests. Identity compromise remains the central risk.

Defender focus: independently verify unsolicited outreach, use phishing-resistant MFA, protect cloud-session tokens, and monitor for unfamiliar OAuth grants, unusual sign-ins and mailbox-rule changes.

Read more ›

Other news highlights

Takedown disrupts Japanese phishing kits.

–

Google AitM kit relays MFA in real time.

Fake WatchGuard VPN site steals logins.

–

Secure Folder lure targets Microsoft accounts.