Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

The News



Refrigeration attacks expose connected-control risk

New reporting describes attackers changing refrigeration settings at supermarkets in several European countries, causing spoilage and disruption. Danfoss said its controls were involved; investigators had not attributed the incidents or confirmed a link to the earlier French attacks.

The update matters to facilities, retail, logistics and engineering operators because remotely managed building and cooling controls can turn a network intrusion into a safety, stock and continuity event.

Defender focus: inventory internet-reachable controllers, restrict supplier remote access, patch supported firmware, and test safe manual operation for critical cooling and building systems.

Read more ›

Other news highlights

Chainstack reports production-system breach.

–

OpenSSH flaw allows password bypass on affected Alpine Linux systems.

–

Synology warns of NAS ransomware attacks.

–

Siemens IoT2050 flaw reported under active attack.

The News

Top of the news



APT29-linked watering-hole campaign hijacks web analytics to deliver mobile exploits

Sekoia reported a campaign attributed to APT29 that used compromised websites, lookalike domains and a supply-chain compromise of Plerdy SEO Tracker. Injected JavaScript profiled visitors before delivering platform-specific iOS or Android exploit chains.

CVE-2024-27834, one of the Apple vulnerabilities used in the exploit chain, has since been added to CISA's Known Exploited Vulnerabilities catalogue.

The campaign highlights the risk of third-party web components: a legitimate site can become an attack path without an organisation directly hosting malicious content. Government, media, policy and high-risk users merit particular attention.

Defender focus: inventory third-party scripts, use integrity controls where feasible, monitor changes to web assets, maintain supported mobile builds and preserve browser telemetry for targeted-compromise investigations.

Read more ›

Other news highlights

Rails fixes a critical Active Storage upload flaw.

–

Xen flaws allow a guest to reach other VM memory.

–

–

Teams help-desk impersonation led to AD CS abuse and data theft.

–

BITTER uses PapRAT in South Asian espionage campaign.

Geo-Politics



Ukraine and Russia report hacks of emergency alert apps

Ukraine and Russia said emergency notification apps were compromised and sent false warnings about air raids, chemical attacks and nuclear danger. Ukraine temporarily suspended its app while other public warning channels continued. Reuters could not verify who was responsible; Ukraine's air force blamed Russia, while Russia also reported a cyberattack on its emergency ministry app.

The incident shows how access to public alerting systems can create confusion during an active conflict and weaken confidence in emergency communications.

Defender focus: protect administrator accounts and publishing interfaces, verify alerts through independent channels, retain app and identity logs, and maintain tested fallback warning methods.

Read more ›

Other news highlights

Moldova probespossible foreign role in government attacks.

–

China-aligned hackers hijack Sogou search redirects.

–

Russian police report VasyGrek infrastructure action.

–

FBI attributes Binance theft to North Korea-linked actors.

Breaches

Security Breaches this week



Air Creebec reports a newly discovered breach of administrative systems

Canadian regional airline Air Creebec confirmed a cybersecurity breach of its administrative systems on 4 November. The company warned that personal files belonging to customers, current and former employees, and retirees may have been taken; some files may also contain operational, administrative or financial information about customers and partners.

Air Creebec says flight operations and aircraft systems were not compromised because they operate separately. Investigators are assessing the scope, and the company says affected people will be contacted directly.

Defender focus: review administrative-system access and exfiltration logs, invalidate exposed credentials, watch for targeted follow-on phishing, and verify separation between corporate IT and operational flight systems.

Read more ›

Other news highlights

Leaked LiteLLM key exposed GitHub token risk.

–

Trojanized Cursor extension carried SSH backdoor.

–

Microsoft 365 token replay affects organisations.

–

Alpine GitLab attempt exposed packaging caveat.

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-76418 | Cisco ASA and FTD
Cisco reports active exploitation of an unauthenticated SSL VPN flaw that can reload affected firewalls when secondary authentication is configured. Apply the fixed ASA or FTD release, restrict remote access and review tunnel-group settings.

CVSS score: 8.6

THIS WEEK | CVE-2026-28336 | SolarWinds Dameware
SolarWinds disclosed a command-injection flaw that can compromise the remotely controlled host; authentication is required. Upgrade Dameware 2026.3 and earlier to fixed version 2026.3.1.

CVSS score: 9.9

Last weeks recaps

CVE-2026-101767
Oracle E-Business Suite
CVSS 9.8. Oracle fixed an unauthenticated Application Object Library vulnerability affecting EBS 12.2.3-12.2.15; probing was reported. Apply Oracle's update and review EBS web-tier requests.

CVE-2026-48356
Adobe Commerce

CVSS 9.6. Adobe rated this dangerous-file-upload issue Critical; reporting linked PolyShell abuse to compromised stores. Install Adobe's update and investigate unexpected loader code.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's November-published October report claims 1,157 ransomware and cyber-extortion victims, a 36.1% increase from September. These are source claims, not independently verified incident totals.

Target industries

The source records manufacturing (163), professional services (130), healthcare (124), technology (120), transportation (79), education (60), financial services (44), and government and defence (30). All figures are source claims.

Target country

The United States is the source's leading target country with 402 claimed victims. Other leading countries: Germany (53), United Kingdom (37), Brazil (33), Italy (27), Canada (26), Spain (24) and Mexico (24).

Top Group

The monthly source identifies 84 countries and territories and 82 active groups. Validate named victim claims against direct organisation or authority disclosures before escalation; maintain isolated, tested recovery paths and tightly governed supplier access.

Top Threat Actors

N0n

149 October victims

TheGentlemen

143 October victims

Qilin

129October victims

Phishing

Phishing news this week



Stolen Entra and Azure DevOps credentials reach cloud tenants

Todyl's reported campaign update describes attackers using stolen Microsoft Entra ID application credentials and Azure DevOps identities to access Microsoft 365 and Azure environments, including managed service providers and their customers. The reporting records mailbox and file access in affected tenants.

The incident reinforces that non-human identities and developer credentials can become broad tenant access paths, especially where applications have powerful permissions or an MSP relationship expands the blast radius.

Defender focus: audit app registrations and service principals, rotate compromised secrets, constrain consent and role grants, review sign-ins and mailbox access, and investigate unusual Azure DevOps identity use across customer tenants.

Read more ›

Other news highlights

Google patchescritical Android RCE issue.

–

SonicWall GMS EoL flaws receive no patch.

SkyW4lker kit steals Microsoft 365 tokens via device codes.

–

Canada warns of help-desk vishing against legal and finance firms.