Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | OCT. | Vol.2

The News

In the news week



ClingSTUN turns exposed Linux and IoT devices into persistent proxies

FortiGuard Labs disclosed new research into ClingSTUN, a Linux backdoor exploiting unpatched internet-facing devices. It establishes persistence and turns infected hosts into remotely controlled proxy nodes.

The malware uses public STUN infrastructure to discover external IP addresses and ports and maintain NAT connectivity. Legitimate STUN servers should not be treated as attacker infrastructure solely because the malware uses them. Assess this traffic alongside suspicious processes and unexpected UDP connections.

The research describes multiple device families and architectures. This creates exposure for distributed sites, facilities, transport and engineering environments with unsupported routers or embedded systems.

Defender focus: inventory exposed devices, patch supported firmware, retire unsupported equipment, restrict remote management and investigate unexpected startup scripts or recurring UDP traffic.

Read more ›

Other news highlights

Firefox mitigation fix.

–

Meraki hardening release.

–

Atlassian file-access fix.

–

HFS exploitation reported (fix 13 Jul).

The News

Top of the news



ASOS confirms third-party platform breach and rogue notifications

ASOS confirmed that a third-party customer communication platform was compromised after users received unauthorised notifications. The company restricted access and engaged advisers and authorities.

ASOS said basic information such as names and contact details may have been accessed. It said it did not believe payment-card data or passwords were affected and that its website, app and operations remained available. The company did not confirm the attackers' separate Snowflake claim.

The incident illustrates how delegated access to notification and customer engagement services can provide a route to customers even when a retailer's main systems keep operating.

Defender focus: review supplier privileges, revoke affected service tokens, verify notification templates and delivery logs, and prepare trusted customer communications for unauthorised messages.

Read more ›

Other news highlights

Utility breach: 400,000 accounts.

–

Advantest breach update (incident Feb).

–

Fortra patches BoKS flaws.

–

Chrome 155 security fixes.

Geo-Politics

News from around the world



UK NCSC publishes disruption and recovery guidance for critical services

The UK National Cyber Security Centre released a consolidated framework for organisations facing highly disruptive cyber attacks. It stresses that recovery can take weeks or months and that impacts extend to services, supply chains, finance and reputation.

The guidance is especially relevant to transport, government, construction, facilities, energy and other operators with operational dependencies. It directs teams to prepare minimum-viable operations, test recovery, isolate backups, protect administrative access, segment networks and establish decision-making and communications arrangements before an incident.

Defender focus: use the guidance to test whether critical services can operate through loss of core IT, managed-service providers or cloud platforms.

Read more ›

Other news highlights

Iran-linked hacker extradited (attacks from 2013).

–

Qilin extradition update (incident Sep 2024).

–

US Senate backs cyber bill.

–

UK council red-team funding.

Breaches

Security Breaches this week



FBI attributes employee-data breach to third-party missed patch

The FBI said its review found that a security failure at a third-party-managed platform, after a contractor failed to apply an explicitly issued patch, led to a breach exposing personal information of thousands of bureau employees. Reuters sources identified the platform as Oracle PeopleSoft; the FBI did not publicly name the contractor or system.

The report is a reminder that a supplier-operated service can still become a material breach path. Defender focus: maintain an authoritative patch-status record for externally managed platforms, set escalation rules for missed critical patches, demand evidence of remediation, and rehearse identity-data breach response with suppliers.

Read more ›

Other news highlights

Denmark breach: 8.8m records.

–

Healthcare breaches affect 250,000.

–

Arizona court breach: over 1m affected.

–

Ploutus ATM-malware suspect arrested.

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-88779 | Citrix NetScaler ADC / Gateway
Memory overflow can cause denial of service when an appliance is configured as SAML Service Provider OR Identity Provider. Upgrade to the vendor's fixed build and review exposed SAML appliances.

CVSS score: 8.7

THIS WEEK | CVE-2026-76471 | Cisco NX-OS NX-API
Unauthenticated attackers can execute code as root or cause denial of service on affected NX-API-enabled Nexus switches. UCS 6300 exploitation requires credentials. Cisco reports no known malicious use. Upgrade; no workaround is available.

CVSS score: 9.8

Last weeks recaps

CVE-2026-87902
WordPress Core

CVSS 8.1. Path traversal can include a readable local PHP file and, under server/theme preconditions, lead to remote code execution. Last week's report recorded CISA KEV inclusion after exploitation evidence.

CVE-2026-94127
F5 BIG-IP APM

CVSS 9.8 (v3.1); 9.3 (v4). Heap overflow may permit unauthenticated remote code execution when an APM access policy and OAuth profile share a virtual server. Last week's report recorded active exploitation reported by F5.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's September recap claims 850 ransomware and extortion victims, down 27.0% from August. These are source claims and are not independently verified incident counts.

Target industries

CyberXTron records manufacturing (147), professional services (99), technology (95), finance (40), education (33), government and defence (28), and transportation (30). 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). These are source claims, not independently verified totals.

Top Group

TheGentlemen leads the report with 105 claimed September victims, followed by Qilin (74), Storm (37) and SafePay (32). Test recovery, third-party access and operational network segmentation.

Top Threat Actors

TheGentlemen

105 September victims

-

Qilin

74 September victims

_

Storm

37 September victims

Phishing

Phishing news this week



TA419 uses fake OneDrive flows to phish policy, legal and education targets

Proofpoint reported that TA419 used impersonation-led credential phishing against US think tanks, universities and legal-sector organisations. Initial emails invited recipients to join a fictitious AI-policy advisory effort; follow-up links used redirects, a fake OneDrive loading screen and a Browser-in-the-Browser adversary-in-the-middle phishing kit.

The chain targeted Microsoft 365 / Entra ID through the first-party OfficeHome application. The report frames the activity as espionage-focused, and the lures should be treated as an identity threat rather than an AI story.

Defender focus: deploy phishing-resistant, origin-bound authentication such as passkeys; verify unsolicited expert outreach through an independent channel; and monitor for unusual OAuth, redirect and cloud-session activity.

Read more ›

Other news highlights

Microsoft X account hijacked.

–

Fake Zoom installer carries backdoor.

MALFEX NPM malware: 40,000 downloads.

–

Google pauses OSS bug submissions.