Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | OCT. | Vol.4

The News

In the news week



ConnectWise incident puts Microsoft 365 tenant access under scrutiny

ConnectWise disabled cloud services after unauthorised access to application identities associated with its Cloud Backup product. Researchers reported successful sign-ins to Microsoft 365 tenants, while ConnectWise said downstream impact remained under investigation.

The event matters to managed service providers and every organisation that grants third-party apps broad Exchange, SharePoint, Teams or Entra access. A trusted integration can create a cross-tenant path when its credentials are exposed.

Defender focus: identify affected app identities, review consent and privileged roles, hunt for persistence, rotate secrets and confirm backup and recovery options.

Read more ›

Other news highlights

UpdraftCentral key exposure used to backdoor WordPress sites.

–

Rank Math PRO compromise left a self-restoring backdoor.

–

OVHcloud CLI release files were swapped to steal secrets.

–

OpenCode Console incident may expose stored provider keys.

The News

Top of the news



Emergency PHP release addresses two remote-code-execution vulnerabilities

PHP released emergency updates for CVE-2026-109618 and CVE-2026-109619, two unauthenticated remote-code-execution vulnerabilities rated CVSS 9.2. Organisations running internet-facing PHP applications should identify affected services and move supported branches to their fixed releases.

The exposure reaches web applications, hosting environments and platforms that depend on PHP for application logic. Older end-of-life branches do not receive vendor fixes, making supported-version inventory and upgrade planning especially important.

Defender focus: update PHP, prioritise public-facing applications, validate deployment and package-manager versions, and review logs for unexpected requests or process activity.

Read more ›

Other news highlights

FortiSIEM public PoC enables unauthenticated RCE risk.

–

CISA KEV adds older Fortinet flaw after exploitation update.

–

Broadcom WPS flaw permits nearby root code execution.

–

Plex2Shell exploitation installs miners and proxy tooling.

Geo-Politics

News from around the world



ClickFix abuse of Siemens software turns trusted tooling into a RAT path

Siemens reported that attackers abused a DLL sideloading weakness in Software Center in ClickFix campaigns, using the legitimate signed application to execute a remote access trojan. The flaw has a fixed release.

Engineering, construction and industrial organisations frequently rely on specialised signed software, which can make trusted-tool abuse especially difficult to spot. This is a delivery and execution risk, not merely a user-awareness problem.

Defender focus: update Software Center, restrict user-writable DLL search paths, investigate msiexec-launched installers and alert on unusual signed-tool execution from user profiles.

Read more ›

Other news highlights

New ClickFix campaign abuses Windows finger.exe.

–

Qilin and INC exploit PAN-OS MFA-bypass flaw.

–

Malicious RubyGems packages target developer wallets.

–

LiteLLM compromise delivered a stealer and backdoor.

Breaches

Security Breaches this week



Targeted advertising infrastructure is linked to zero-click spyware delivery

Citizen Lab research described AdFection, in which targeted advertising infrastructure allegedly helped spyware operators identify and infect selected devices without a click. The evidence links the delivery path to Candiru activity while several aspects remain under investigation.

Government, media, critical-infrastructure and high-risk personnel should treat ad-tech exposure as part of their mobile and browser threat model. Routine web content can become a delivery route when an attacker has a capable exploit chain.

Defender focus: keep browsers and mobile devices supported, centralise telemetry, restrict high-risk ad exposure where appropriate and maintain a rapid escalation route for suspected targeted compromise.

Read more ›

Other news highlights

Pegasus infection confirmed on a Serbian leader's iPhone.

–

Autonomous agents reportedly targeted more than 1,200 sites.

–

Japan report tracks systemic data, API and ransomware exposure.

–

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-109618 and CVE-2026-109619 | PHP
PHP released emergency fixes for two unauthenticated RCE vulnerabilities (CVSS 9.2). Update supported branches to 8.5.12, 8.4.27, 8.3.36 or 8.2.35, and urgently assess exposed applications.

CVSS score: 9.2

THIS WEEK | Fortinet | CVE-2026-106173 and CVE-2025-61624
A public PoC demonstrates unauthenticated file write and possible RCE against FortiSIEM 7.5.0 (CVSS 9.4). Separately, CISA added the older CVE-2025-61624 Fortinet path-traversal flaw (CVSS 6.5) to KEV after evidence of exploitation. Upgrade FortiSIEM and assess affected Fortinet devices.

CVSS: 9.4 / 6.5

Last weeks recaps

CVE-2026-76519
Cisco Secure Email Gateway

CVSS 9.8. Cisco reported active exploitation of an unauthenticated arbitrary-file-write flaw in the AMP feature. Apply Cisco's fixed releases and inspect exposed appliances.

CVE-2026-0322
Palo Alto PAN-OS

CVSS 8.6. Palo Alto reported very limited exploitation of an authenticated management-interface RCE. Install the fixed release and keep management access internal.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's October-published Hyflock profile records 8 claimed leak-site victims. The source observed listings dated 9 September to 13 October; all victim, volume and capability claims need independent validation.

Target industries

The source describes claimed targets in manufacturing, chemicals, food and beverage, pharmaceuticals, telecommunications, accounting and government. It reports a double-extortion service with Windows, Linux/NAS and ESXi coverage.

Target country

India is the leading target country in the source with 2 claimed victims (25%). Other listed countries are Malaysia, Brazil, Saudi Arabia, Bangladesh, Ecuador and Turkiye with 1 each.

Top Group

CyberXTron reports roughly 13.5 TB of claimed data across six listings. The reported period is the observed listing range, not a global ransomware total; maintain offline backups and watch for exposed credentials and GPO change activity.

Top Threat Actors

Hyflock

8 claimed listings | Sep 9-Oct 13

-

No comparative actor total

Current source does not provide one

–

No comparative actor total

Current source does not provide one

Phishing

Phishing news this week



Microsoft-branded tech-support scam uses Help TDS and disposable hosting

Researchers documented a large Microsoft-impersonation operation using a malicious traffic-distribution system to route victims to fake alerts and remote-access tooling. The campaign relied on high-volume disposable hosting and rapidly changing infrastructure.

Technology, finance, legal and public-sector users remain attractive targets because remote-access fraud can become persistent intrusion or credential theft. The technique blends web redirection, fake system alerts and a persuasive phone call.

Defender focus: train users that legitimate support never requires an unsolicited call or pasted command, restrict unapproved remote tools and monitor for suspicious browser-to-remote-access execution chains.

Read more ›

Other news highlights

Hotel-sector lures use EtherHiding malware delivery.

–

Fake AI services distribute account and session stealers.

Hyflock lists eight claimed victims across seven countries.

–

No further qualifying phishing item found this week.