Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | OCT. | Vol.5

The News

In the news week



Volt Typhoon's Silent Train shows sustained risk to edge and control-plane infrastructure

Lumen's Black Lotus Labs linked Volt Typhoon to a covert relay network used to support zero-day campaigns against management and orchestration systems. The network cycled through compromised SOHO, IoT and enterprise devices, then removed artefacts after operations.

The reported victim set includes telecommunications, government, defence, energy, water, transport, rail and aviation. The focus on management planes and downstream access makes this directly relevant to organisations that operate remote administration, SD-WAN or network-control services.

Defender focus: isolate management planes, restrict remote administration, patch and hunt on edge devices, and investigate short-lived chains of unusual SSH or proxy activity.

Read more ›

Other news highlights

CERT-UA warns of Dahua P2P camera takeovers.

–

Tailscale fixes SSH forwarding flaws.

–

FBI seizes Virtualine hosting domain.

–

Apple extends the CoreGraphics fix.

The News

Top of the news



Lazarus campaign abuses trusted South Korean security software to deliver malware

Kaspersky attributed Operation FlashHole to Lazarus after activity against South Korean construction, software and communications-equipment organisations. The campaign uses tailored lures and abuses trusted national security software to launch an in-memory malware chain. This shows how security software used for banking or government access can become an attractive delivery path when update and execution controls are weak. Construction and communications supply chains merit attention beyond the affected geography. Defender focus: inventory browser-integrated security software, apply vendor fixes, monitor signed-process DLL sideloading and review web filtering for tailored resume and portfolio lures.

Read more ›

Other news highlights

Keystone destroys inventory after key theft.

–

k0t campaign targets Fortinet and Palo Alto edge devices.

–

953 stores serve evasive JavaScript loaders.

–

Geo-Politics

News from around the world



GMO cloud breach links exposed desktop credentials to unauthorised FX trades

GMO confirmed unauthorised access and customer-data exfiltration from its Onamae.com Desktop Cloud service. A broker reported unauthorised trades using credentials believed to have been taken from affected hosted desktops; GMO shut down the service while its investigation continues.

The incident illustrates the compound risk where a hosted desktop provider can expose saved application credentials, customer data and downstream financial accounts. Claims about the intrusion path and attacker-posted material remain unverified unless confirmed by the company.

Defender focus: rotate credentials stored in affected virtual desktops, terminate sessions, review trading or financial-account activity, and separate privileged operations from general-purpose hosted environments.

Read more ›

Other news highlights

Moldova reports data extraction from government services.

–

ESET links Russian-aligned groups to a Ukraine wiper attack.

–

–

Breaches

Security Breaches this week



Gheist uses stolen GitHub tokens to exfiltrate secrets through Actions logs

Wiz tracked an automated campaign that uses stolen GitHub tokens to plant workflow files which encode repository and environment secrets into Actions logs, downloads the logs and deletes the runs. Wiz observed successful activity in private repositories and GitHub Enterprise environments.

A CI/CD compromise can expose deploy credentials, cloud roles and production secrets even where source code itself is not the main target. Public repository safeguards did not cover the private and enterprise cases reported by Wiz.

Defender focus: hunt for ci-sync branches and deleted workflow runs, revoke the tokens involved, rotate every reachable secret and review self-hosted runners for follow-on activity.

Read more ›

Other news highlights

ScarlettGroup reports five claimed extortion listings.

–

Capcom confirms exposure of 11.7 million account records.

–

Quest Diagnostics reports a current patient-record breach.

–

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-101767 | Oracle E-Business Suite
Oracle's October CPU fixes an unauthenticated HTTP vulnerability in Application Object Library (CVSS 9.8) affecting EBS 12.2.3-12.2.15. Reported probing followed quickly. Apply Oracle's update, restrict the EBS web tier and hunt for unexpected requests to the Thin Client Framework servlet.

CVSS score: 9.8

THIS WEEK | CVE-2026-48356 | Adobe Commerce and Magento
Adobe rates this unauthenticated dangerous-file-upload issue Critical (CVSS 9.6). Current reporting links active PolyShell abuse to compromised e-commerce stores. Install Adobe's security update, inspect CMS blocks and investigate unexpected loader code or outbound browser requests.

CVSS score: 9.6

Last weeks recaps

PHP2Shell RCE pair

CVE-2026-109618 and CVE-2026-109619, CVSS 9.2. PHP released emergency fixes for two unauthenticated RCE vulnerabilities. Update supported branches and assess exposed applications.

CVE-2026-106173
Fortinet FortiSIEM

CVSS 9.4. A public proof of concept raised the urgency of an unauthenticated file-write and possible RCE issue. Upgrade FortiSIEM and review exposed instances.

Ransomware

Weekly Ransomware Roundups



Top Threat Actors

ScarlettGroup

5 claimed listings | Oct 5-26

Overview

CyberXTron's October ScarlettGroup profile records 5 claimed leak-site listings. It describes a data-only extortion operation; every victim and capability assertion is a source claim, not independently verified.

Target industries

The profile says the group cross-posts each listing to criminal forums, with statuses for negotiation, leaked data or sale. No encryption, ransom note, ransom amount or initial-access method is confirmed.

Target country

The United States is the source's leading target country with 4 claimed victims. India has 1 claimed victim. The observed listing period runs from 5 October to the profile's 26 October update.

Top Group

Claimed targets span technology, professional services, government and defence, and education. Treat a listing as an extortion incident to validate, preserve logs and assess data exposure even when systems are not encrypted.

Phishing

Phishing news this week



Skyw4lker device-code phishing abuses legitimate Microsoft authentication flows

Research on the Skyw4lker kit shows business-themed documents routing targets through Google-hosted infrastructure and a Microsoft device-authorisation flow. The goal is not simply credential capture: a victim is manipulated into approving an attacker-initiated sign-in and granting access to resulting tokens.

Manufacturing, technology and healthcare organisations are among the reported targets. Valid-looking authentication events can hide the malicious context, making mail, browser, identity and cloud telemetry important to a full investigation.

Defender focus: limit device-code authorisation where appropriate, train staff to reject unsolicited codes, correlate document lures with sign-in events and revoke suspicious refresh tokens promptly.

Read more ›

Other news highlights

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

–

Operation CloudFire disrupts calendar-invite phishing domains.

–