Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people
– Bruce Schneier

SCC Threat Pulse | NOV. | Vol.3

The News



Optimizely flaw allowed card-skimming code to reach customer sites

Optimizely confirmed that an unauthorised party abused a Web Experimentation signup flaw to impersonate users and insert malicious JavaScript into selected customer projects. The company says it closed the flaw, removed the code and found no customer-password theft.

The injected code targeted payment details entered directly into affected sites and cryptocurrency transactions. A trusted third-party web snippet can therefore become a visitor-side supply-chain risk even where the affected organisation's own network was not breached.

Defender focus: determine whether Web Experimentation was used during the exposure window, review browser-side telemetry and payment-page changes, enforce a restrictive content-security policy, and retain relevant web logs for investigation.

Read more ›

Other news highlights

NGINX HTTP/2 flaw may allow unauthenticated code execution in specific configurations.

PHP releases critical security fixes across all supported branches.

Updated ScreenConnect guidance urges customers to disable exposed extensions and update.

CISA adds exploited Puppet remote-code-execution flaw to KEV.

The News

Top of the news



N-central exploitation reaches patched servers as vendor ships another hotfix

Researchers reported cryptominer deployment on 21 N-central servers, including systems running the earlier Hotfix 2 release. N-able subsequently released Hotfix 3, which hardens agent and probe authentication, blocks legacy APIs permanently and requires customers to update agents and probes.

This is a material update to the MSP-management risk reported last week: attackers have demonstrated exploitation after an initial remediation release. Remote-management infrastructure deserves the same urgent incident-response treatment as an internet-facing identity or VPN appliance.

Defender focus: install N-central 2026.4 HF3, update all agents and probes, review server and agent logs for unauthorised scripts or miners, rotate exposed credentials and restrict management access.

Read more ›

Other news highlights

Red Hat Quay flaw may expose private container images.

Java4Shell exploitation attempt uses a Chrome-themed disguise.

WordPress Core update addresses 20 security vulnerabilities.

NCSC Ireland warns of unpatched vulnerabilities in Danfoss refrigeration controllers

Geo-Politics



SilentAir interception campaign exposes telecom signalling risk across regions

Enea reported that a newly named actor, SilentAir, used compromised telecom equipment to intercept calls and SMS two-factor-authentication messages, primarily against Taiwanese users. The researchers assess a state-level operator with high confidence but link the activity to China only with low confidence.

The campaign illustrates that identity assurance can fail upstream of the enterprise when an attacker can abuse mobile-network signalling. Organisations that still rely on SMS for privileged access should treat it as a weaker recovery channel, not as the highest assurance factor.

Defender focus: move privileged and high-risk users toward phishing-resistant authenticators, monitor mobile-number and recovery-factor changes, and alert on unusual enrolment or session-recovery activity.

Read more ›

Other news highlights

EggStreme campaign targets Philippine government organisations.

Gateway attacks deploy a backdoor and destructive wiper in geopolitically linked activity.

Hacktivist groups claim attacks against European ports and public bodies.

Breaches

Security Breaches this week



COLD RELIC reused stolen cloud data to breach a second US organisation

Google Threat Intelligence and Mandiant described a 2026 intrusion in which COLD RELIC used employee and relationship information stolen from an earlier US Google Workspace compromise to impersonate contacts and target a second organisation. Google attributes the group to Russian state interests.

The affected tenant's Super Admin credentials were combined with MFA push fatigue, then rogue MFA devices, passkeys and backup codes were used to preserve access. The actor also conducted tenant-wide data-export activity and deleted alerts to reduce visibility.

Defender focus: protect administrator accounts with phishing-resistant MFA, alert on new passkeys and Customer Takeout events, review changes to Alert Center notifications, and revoke attacker-enrolled authenticators during cloud-identity containment.

Read more ›

Other news highlights

Cursor links trojanised extension to a stolen supplier key

Malicious Microsoft Agent Framework packages steal cloud credentials

Vulnerabilities

Vulnerabilities & Exploits



THIS WEEK | CVE-2026-123890 | VMware vCenter Server
Broadcom disclosed a critical authentication-bypass vulnerability in Vmware Directory Service. An attacker with network access could bypass authentication and gain unauthorised access to vCenter. The vulnerability has reportedly been exploited as a zero-day to obtain administrator access and access virtual-machine data. Apply Broadcom’s fixed releases immediately; no workaround is available.

CVSS score: 9.8

THIS WEEK | F5 BIG-IP | six CVEs
F5 disclosed six unauthenticated data-plane flaws, each rated CVSS 9.8, that can crash traffic in specific iRule or APM configurations and may permit RCE. Affected systems require F5 engineering hotfixes; F5 lists no workaround. Review exposed virtual servers and install the applicable fixes.

CVSS score: 9.8

Last week’s recaps

CVE-2026-116606 and CVE-2026-111560
Barracuda Email Security Gateway

CVSS 9.3 / 8.6. Barracuda confirmed exploitation affecting a small number of organisations. The vulnerabilities can be chained to bypass authorisation and obtain root access where an affected administrative interface is reachable. Apply current security updates and restrict administrative access.

CVE-2026-125350
Google Chromium

CVSS 8.8. Google patched an actively exploited use-after-free vulnerability in Chromium’s XML component. Update Google Chrome and other affected Chromium-based browsers to vendor-fixed releases.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's 17 November OBSOFT profile identifies six resolved or data-destroyed leak-site entries and one pending entry. The group presents itself as a bug-bounty collective; All figures and victim claims are based on observed leak-site activity and remain independently unverified.

Target industries

The source estimates 122.65 TB across the six resolved entries, with individual claims from 508.6 GB to 45.2 TB. It has not confirmed an initial-access method, tooling or proof of data theft.

Target country

South Korea is the leading and only identified country in the six resolved entries. CyberXTron names Korean automotive, Senegalese banking and US healthcare targets in an announcement, but does not assign those claims to the resolved-country tally.

Top Group

OBSOFT claims an AI-driven operation, but CyberXTron found no technical evidence supporting that claim. Treat leak-site assertions as intelligence leads and validate any alleged victim impact through direct organisational or authority disclosures.

Top Threat Actors

OBSOFT

6 Resolved or data-destroyed entries
17 November Snapshot

1 Pending Entry
Source-recorded claim

122.65TB claimed
Across six resolved entries

Phishing

Phishing news this week



Fake freight portals target logistics identities and fuel-card credentials

Researchers reported fake FMCSA, DAT and TIMOCOM portals that impersonate carrier-verification, broker-onboarding and load-board services. The campaigns seek identity and fuel-card credentials, and may also deliver remote-access malware.

The lures exploit normal operational workflows in transport and logistics, where a fast response to a carrier, broker or compliance query can create pressure to trust a familiar-looking portal. Stolen credentials can expose dispatch, payment and fleet-management systems.

Defender focus: make access to operational portals conditional on verified bookmarks and phishing-resistant MFA, monitor new remote-control tooling, and require out-of-band validation before changing payment or carrier records.

Other news highlights

Calendar-invite phishing campaign steals active Google sessions

Fake Indian traffic fines deliver Android banking malware

Bank phishing campaign uses fake suspension pages to hinder takedowns

Trigram infostealer campaign uses recruitment and package-delivery lures

Read more ›