

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

MAY 2026 - VOL.2

The News

IN THE NEWS THIS WEEK



OTHER NEWS HIGHLIGHTS

[NHS to close-source hundreds of GitHub repos over AI, security concerns](#)

[Backdoored PyTorch Lightning package drops credential stealer](#)

[ConsentFix v3 attacks target Azure with automated OAuth abuse](#)

Cisco Patches High-Severity Vulnerabilities in Enterprise Products

Cisco on Wednesday announced patches for multiple vulnerabilities across its enterprise products, including five high-severity bugs.

Two high-severity issues, tracked as CVE-2026-20034 and CVE-2026-20035, which could lead to server-side request forgery (SSRF) attacks, were resolved in Cisco Unity Connection.

Cisco addressed a high-severity defect (CVE-2026-20185) in the Simple Network Management Protocol (SNMP) subsystem of SG350 and SG350X switches that could be exploited to cause a denial-of-service (DoS) condition.

The Crosswork Network Controller (CNC) and Network Services Orchestrator (NSO) were found vulnerable to a high-severity DoS vulnerability tracked as CVE-2026-20188.

The fifth high-severity bug, tracked as CVE-2026-20167, was addressed in the web interface of IoT Field Network Director. Due to improper error handling, the weakness allows attackers to submit crafted input and cause the router to reload, leading to a DoS condition.

READ MORE >

The News

TOP OF THE NEWS THIS WEEK



Critical cPanel Vulnerability Weaponized to Target Government and MSP Networks

This week, an emergency update for WHM and cPanel was released to fix a critical authentication bypass flaw that allows attackers to access control panels.

WHM and cPanel are Linux-based web hosting control panels for server and website management. While WHM provides server-level control, cPanel provides administrator access to the website backend, webmail, and databases.

An unknown threat actor has been observed targeting government and military entities in Southeast Asia, alongside a smaller cluster of managed service providers (MSPs) and hosting providers in the Philippines, Laos, Canada, South Africa, and the U.S., by exploiting the recently disclosed vulnerability.

It's not yet known how many organizations have been impacted by the vulnerability, but security firm Rapid7 used Shodan to identify roughly 1.5 million internet-exposed cPanel instances.

READ MORE >

TOP RELATED ARTICLES

[Palo Alto Networks
firewall zero-day
exploited for nearly a
month](#)

[Linux cryptographic
code flaw offers fast
route to root](#)

[Government,
Scientific Entities Hit
via Daemon Tools
Supply Chain Attack](#)

Geo-Politics

NEWS FROM AROUND THE WORLD



China-Linked Hackers Target Asian Governments, NATO State, Journalists, and Activists

Cybersecurity researchers have disclosed details of a new China-aligned espionage campaign targeting government and defense sectors across South, East, and Southeast Asia, along with one European government belonging to NATO. Trend Micro has attributed the activity to a threat activity cluster it tracks under the temporary designation SHADOW-EARTH-053.

"The group exploits N-day vulnerabilities in internet-facing Microsoft Exchange and Internet Information Services (IIS) servers (e.g., ProxyLogon chain), then deploys web shells (Godzilla) for persistent access and stages ShadowPad implants via DLL sideloading of legitimate signed executables," security researchers Daniel Lunghi and Lucas Silva said in an analysis.

Targets of the campaigns include Pakistan, Thailand, Malaysia, India, Myanmar, Sri Lanka, and Taiwan. The lone European country that features in the threat actor's victimology footprint is Poland.

READ MORE >

HIGHLIGHTS FROM AROUND THE WORLD

[Microsoft's patch for a 0-day exploited by Russian spies fell short. Another Windows flaw is under attack](#)

[Iranian APT Intrusion Masquerades as Chaos Ransomware Attack](#)

[Silver Fox Springs Tax-Themed Attacks on Orgs in India, Russia](#)

Breaches

SECURITY BREACHES THIS WEEK



OTHER SECURITY BREACHES

[ShinyHunters claims dump puts 119K Vimeo emails in the wild](#)

[Instructure hacker claims data theft from 8,800 schools, universities](#)

[Real estate giant confirms vishing incident as ShinyHunters and Qilin both come knocking](#)

Trellix discloses data breach after source code repository hack

Cybersecurity firm Trellix disclosed a data breach after attackers gained access to "a portion" of its source code repository.

Trellix is a global cybersecurity company formed from the October 2021 merger of McAfee Enterprise and FireEye. It provides services to over 50,000 business and government customers worldwide, protecting more than 200 million endpoints.

At the moment, Trellix said it has yet to find evidence that the threat actors have exploited or altered the source code they accessed.

"Trellix recently identified unauthorized access to a portion of our source code repository. Upon learning of this matter, we immediately began working with leading forensic experts to resolve it," Trellix says.

"We have also notified law enforcement. Based on our investigation to date, we have found no evidence that our source code release or distribution process was affected, or that our source code has been exploited."

READ MORE >

Vulnerabilities

VULNERABILITIES & EXPLOITS



[CVE-2026-31431: Copy Fail vulnerability enables Linux root privilege escalation across cloud environments](#)

CVSS SCORE 7.8

[CVE-2026-0300: Unauthenticated user initiated Buffer Overflow Vulnerability in User-ID™ Authentication Portal \(PAN-OS\)](#)

CVSS SCORE 8.8

LAST WEEKS RECAP

[CVE-2026-3854: Github Vulnerability allows an authenticated user to obtain remote code execution with a single "git push" command.](#)
CVSS Score: (8.8)

[CVE-2026-7333: Use after free in GPU in Chrome allows for sandbox escape via a crafted HTML page.](#)
CVSS Score: (9.6)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS



TOP THREAT ACTORS

Qilin

Qilin is a ransomware-as-a-service operation linked to Russia, encrypting and stealing data for ransom. Active since October 2022, it has targeted organizations like The Big Issue and Yanfeng.

Akira

Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to \$42 million by April 2024.

Clop

Clop ransomware first emerged in 2019, when it became a prevalent threat to organizations and businesses. Clop ransomware encrypts the victims files and threatens to leak the confidential information if no ransom is paid.



OVERVIEW

A total of 138 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 21.7% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 76 affected entities.

TOP GROUP

The Akira was the most active, claiming 28 victims.



Dive into this interactive report to uncover hidden trends [HERE!](#)

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

Phishing

PHISHING NEWS THIS WEEK



OTHER PHISHING ARTICLES

[Researchers report Amazon SES abused in phishing to evade detection](#)

[Phishing Campaign Hits 80+ Orgs Using SimpleHelp and ScreenConnect RMM Tools](#)

[30,000 Facebook Accounts Hacked via Google AppSheet Phishing Campaign](#)

Microsoft Details Phishing Campaign Targeting 35,000 Users Across 26 Countries

Microsoft has disclosed details of a large-scale credential theft campaign that has leveraged a combination of code of conduct-themed lures and legitimate email services to direct users to attacker-controlled domains and steal authentication tokens. The multi-stage campaign, observed between April 14 and 16, 2026, targeted more than 35,000 users across over 13,000 organizations in 26 countries, with 92% of the targets located in the U.S.

"The lures in this campaign used polished, enterprise-style HTML templates with structured layouts and preemptive authenticity statements, making them appear more credible than typical phishing emails and increasing their plausibility as legitimate internal communications," the Microsoft Defender Security Research Team and Microsoft Threat Intelligence said.

"Because the messages contained accusations and repeated time-bound action prompts, the campaign created a sense of urgency and pressure to act."

The email messages used in the campaign employ lures related to code of conduct reviews, using display names like "Internal Regulatory COC," "Workforce Communications," and "Team Conduct Report." Subject lines associated with these emails include "Internal case log issued under conduct policy" and "Reminder: employer opened a non-compliance case log."

[READ MORE >](#)