SCC | DIGITAL

# THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

February 2026 - VOL.1

# The News

## IN THE NEWS THIS WEEK

### Cisco, F5 Patch High-Severity Vulnerabilities

Cisco and F5 this week released patches for multiple vulnerabilities across their products, including high-severity issues leading to denial-of-service (DoS) conditions, command execution, and privilege escalation.

Cisco rolled out fixes for five security defects, including two high-severity bugs in TelePresence Collaboration Endpoint (CE) and RoomOS software, and Meeting Management.

The first, tracked as CVE-2026-20119, can be exploited remotely without authentication or user interaction to cause a DoS condition by sending a crafted meeting invitation to a vulnerable appliance.

Cisco fixed the flaw in TelePresence CE Software and RoomOS software versions 11.27.5.0 and 11.32.3.0.

The second vulnerability, tracked as CVE-2026-20098 and resolved in Meeting Management version 3.12.1 MR, exists because the web management interface fails to properly validate user input, allowing authenticated attackers to send crafted requests.

Successful exploitation of the bug allows attackers with at least the role of video operator to upload arbitrary files, including system files processed by the root account, thus leading to command execution with root privileges.



READ MORE

## OTHER NEWS HIGHLIGHTS

Microsoft Develops Scanner to Detect Backdoors in Open-Weight Large Language Models

Microsoft Warns Python Infostealers Target macOS via Fake Ads and Installers

Docker Fixes Critical Ask Gordon AI Flaw Allowing Code Execution via Image Metadata

# The News

## TOP OF THE NEWS THIS WEEK


### Critical n8n Flaw CVE-2026-25049 Enables System Command Execution via Malicious Workflows

A new, critical security vulnerability has been disclosed in the n8n workflow automation platform that, if successfully exploited, could result in the execution of arbitrary system commands.

The flaw, tracked as CVE-2026-25049 (CVSS score: 9.4), is the result of inadequate sanitization that bypasses safeguards put in place to address CVE-2025-68613 (CVSS score: 9.9), another critical defect that was patched by n8n in December 2025.

"Additional exploits in the expression evaluation of n8n have been identified and patched following CVE-2025-68613," n8n's maintainers said in an advisory released Wednesday.

"An authenticated user with permission to create or modify workflows could abuse crafted expressions in workflow parameters to trigger unintended system command execution on the host running n8n."

READ MORE



## TOP RELATED ARTICLES

CISA Adds Actively Exploited SolarWinds Web Help Desk RCE to KEV Catalog

Hackers Exploit Metro4Shell RCE Flaw in React Native CLI npm Package

APT28 Uses Microsoft Office CVE-2026-21509 in Espionage-Focused Malware Attacks

# Geo-Politics

## NEWS FROM AROUND THE WORLD


### China-Linked Amaranth-Dragon Exploits WinRAR Flaw in Espionage Campaigns

Threat actors affiliated with China have been attributed to a fresh set of cyber espionage campaigns targeting government and law enforcement agencies across Southeast Asia throughout 2025.

Check Point Research is tracking the previously undocumented activity cluster under the moniker Amaranth-Dragon, which it said shares links to the APT 41 ecosystem. Targeted countries include Cambodia, Thailand, Laos, Indonesia, Singapore, and the Philippines.

"Many of the campaigns were timed to coincide with sensitive local political developments, official government decisions, or regional security events. Attack chains mounted by the adversary have been found to abuse CVE-2025-8088, a now-patched security flaw impacting RARLAB WinRAR that allows for arbitrary code execution when specially crafted archives are opened by targets.

READ MORE

## HIGHLIGHTS FROM AROUND THE WORLD

Notepad++ Hosting Breach Attributed to China-Linked Lotus Blossom Hacking Group

Iran-Linked RedKitten Cyber Campaign Targets Human Rights NGOs and Activists

China-Linked UAT-8099 Targets IIS Servers in Asia with BadIIS SEO Malware

# Breaches

## SECURITY BREACHES THIS WEEK


### Harvard, UPenn Data Leaked in ShinyHunters Shakedown

Cyber extortion group ShinyHunters claimed responsibility Wednesday for late 2025 attacks against Harvard University and the University of Pennsylvania, publishing on a darkweb leak site what they claimed were more than 2 million records stolen from the two Ivy League schools. Threat intelligence firm Hudson Rock, which reviewed the leaked Harvard data, said it includes admissions and fundraising information, and details such as "top donors," as well as spouses, widows, parents, current students and family members who are prospective students. This serves not only as a "social graph" revealing "wealth bands" and details of "domestic intimacy," the firm said.

Leaked Harvard data includes "high-value target" fundraising details, listing Facebook founder Mark Zuckerberg as a $604 million contributor, alongside his home address and private email address. Other big donors include former New York City Mayor Michael Bloomberg, at $422 million and Microsoft co-founder Steve Ballmer at $102 million, Hudson Rock said. Leaked notes detail a "Bill Gates Top Prospect Strategy Meeting" in January 2023, with nine named attendees, aimed at getting him to donate more money to the university's programs.

The leak includes multiple legal documents, including a 2019 agreement signed by billionaire Bill Ackman, for his Pershing Square Foundation to pay $200,000 annually for 25 years in support of the university economics department's Foundations of Human Behavior Initiative

READ MORE

## OTHER SECURITY BREACHES

Big Breach or Smooth Sailing? Mexican Gov't Faces Leak Allegations

Coinbase confirms insider breach linked to leaked support tool screenshots

Iron Mountain: Data breach mostly limited to marketing materials

# Vulnerabilities

## VULNERABILITIES & EXPLOITS

CVE-2026-20119 - Cisco TelePresence Collaboration Endpoint Software and RoomOS Software Denial of Service Vulnerability

**CVSS SCORE 7.5**

CVE-2026-25049 - Critical n8n Flaw CVE-2026-25049 Enables System Command Execution via Malicious Workflows

**CVSS SCORE 9.8**

## LAST WEEKS RECAP

CVE-2026-24061 - telnetd in GNU Inetutils through 2.7 allows remote authentication bypass via a "-f root" value for the USER environment variable.
CVSS Score: (9.8)

CVE-2026-21509 - Reliance on untrusted inputs in a security decision in Microsoft Office allows an unauthorized attacker to bypass a security feature locally.
CVSS Score: (7.8)

# Ransomware

## WEEKLY RANSOMWARE ROUNDUPS

### OVERVIEW

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

### TARGET INDUSTRIES

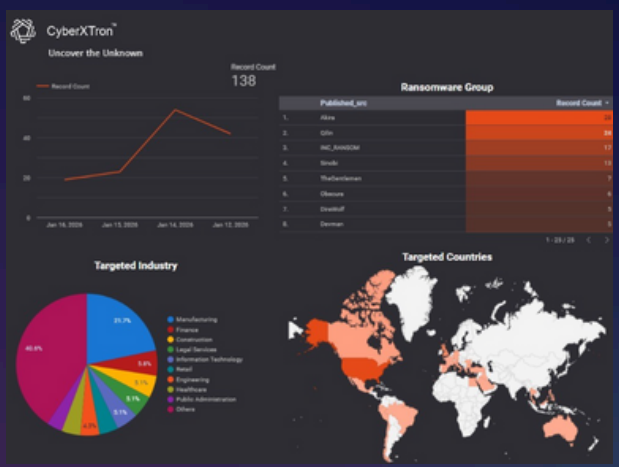
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

### 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

## 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**

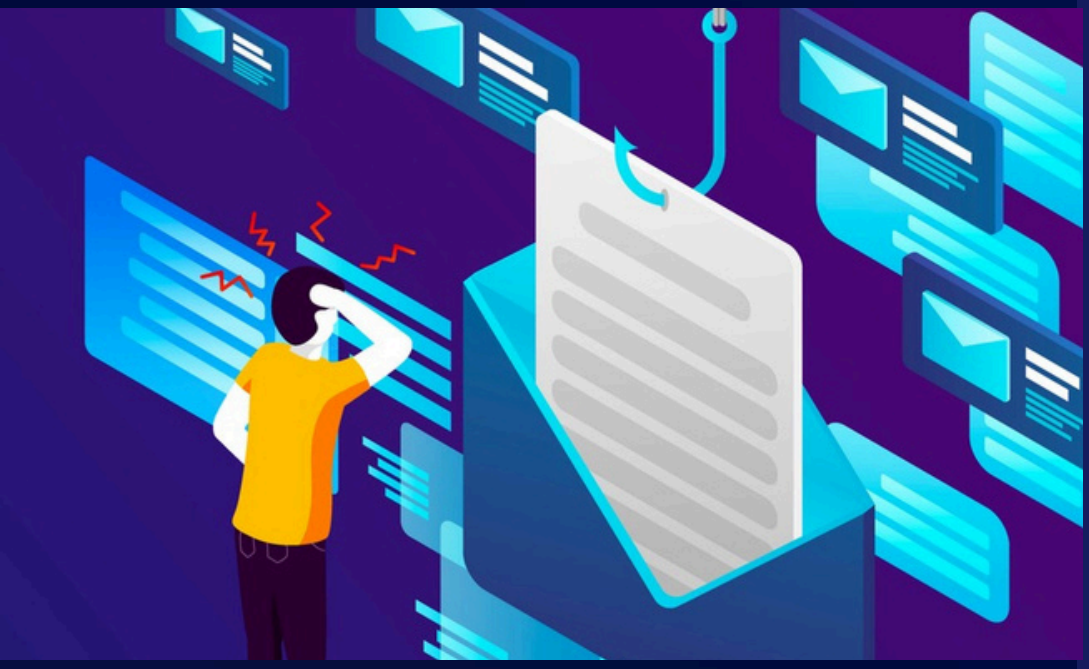
**Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.**

**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.**

# Phishing

## PHISHING NEWS THIS WEEK



### Cloud storage payment scam floods inboxes with fake renewals

Over the past few months, a large-scale cloud storage subscription scam campaign has been targeting users worldwide with repeated emails falsely warning recipients that their photos, files, and accounts are about to be blocked or deleted due to an alleged payment failure.
Based on numerous emails seen by BleepingComputer, the campaign has escalated over the past few months, with people receiving multiple versions of the scam each day, all appearing to be sent by the same scammers.
While the email text, the messages all attempt to create a sense of urgency by claiming a payment problem or storage issue must be resolved immediately, or people's files will be deleted or blocked.

READ MORE

## OTHER PHISHING ARTICLES

New Password-Stealing Phishing Campaign Targets Corporate Dropbox Credentials

AI-Enabled Voice and Virtual Meeting Fraud Surges 1000%+

AI Drives Doubling of Phishing Attacks in a Year