SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

February 2026 - VOL.3

The News

IN THE NEWS THIS WEEK

Dell RecoverPoint for VMs Zero-Day CVE-2026-22769 Exploited Since Mid-2024

A maximum severity security vulnerability in Dell RecoverPoint for Virtual Machines has been exploited as a zero-day by a suspected China-nexus threat cluster dubbed UNC6201 since mid-2024, according to a new report from Google Mandiant and Google Threat Intelligence Group (GTIG).

The activity involves the exploitation of CVE-2026-22769 (CVSS score: 10.0), a case of hard-coded credentials affecting versions prior to 6.0.3.1 HF1. Other products, including RecoverPoint Classic, are not vulnerable to the flaw.

"This is considered critical as an unauthenticated remote attacker with knowledge of the hardcoded credential could potentially exploit this vulnerability, leading to unauthorized access to the underlying operating system and root-level persistence," Dell said in a bulletin released Tuesday.

READ MORE

OTHER NEWS HIGHLIGHTS

Notepad++ Fixes Hijacked Update Mechanism Used to Deliver Targeted Malware

Researchers Show Copilot and Grok Can Be Abused as Malware C2 Proxies

SmartLoader Attack Uses Trojanized Oura MCP Server to Deploy StealC Infostealer

The News

TOP OF THE NEWS THIS WEEK

Microsoft Patches CVE-2026-26119 Privilege Escalation in Windows Admin Center

Microsoft has disclosed a now-patched security flaw in Windows Admin Center that could allow an attacker to escalate their privileges.

Windows Admin Center is a locally deployed, browser-based management tool set that lets users manage their Windows Clients, Servers, and Clusters without the need for connecting to the cloud.

The high-severity vulnerability, tracked as CVE-2026-26119, carries a CVSS score of 8.8 out of a maximum of 10.0

"Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges over a network," Microsoft said in an advisory released on February 17, 2026. "The attacker would gain the rights of the user that is running the affected application."

READ MORE

TOP RELATED ARTICLES

PromptSpy Android Malware Abuses Gemini AI to Automate Recent-Apps Persistence

Fake IPTV Apps Spread Massiv Android Malware Targeting Mobile Banking Users

Critical Flaws Found in Four VS Code Extensions with Over 125 Million Installs

Geo-Politics

NEWS FROM AROUND THE WORLD

Fake shops target Winter Olympics 2026 fans

In roughly the past week alone, we've identified nearly 20 lookalike domains designed to imitate the official Olympic merchandise store. These aren't crude copies thrown together overnight. The sites use the same polished storefront template, complete with promotional videos and background music designed to mirror the official shop.olympics.com experience. The layout and product pages are the same—the only thing that changes is the domain name. At a quick glance, most people wouldn't notice anything unusual.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

INTERPOL Operation Red Card 2.0 Arrests 651 in African Cybercrime Crackdown

---

CRESCENTHARVEST Campaign Targets Iran Protest Supporters With RAT Malware

---

Citizen Lab Finds Cellebrite Tool Used on Kenyan Activist's Phone in Police Custody

Breaches

SECURITY BREACHES THIS WEEK

New AI Data Leaks—More Than 1 Billion IDs And Photos Exposed

Updated February 19 with details of a second AI-related data leak, this one adding 2 million photos and videos to the 1 billion IDs, email and phone numbers already exposed by an AI-powered identity verification service.

Cybersecurity researchers have confirmed they discovered a massive “treasure trove” of unsecured data, with information on individuals from 26 countries, including, at the top of the list, the U.S., which appears to be linked to an AI-powered identity verification service. Totalling almost a terabyte of data and 1 billion records, the exposed information included national IDs, full names, addresses, phone numbers, and email.

Just when you think things couldn’t get any worse, those same researchers have now disclosed yet another AI-related data leak. This time impacting users of an Android app that deploys AI to provide “cinematic makeovers” for selfies. While not in quite the same league as the first, that will be cold comfort if your photos and videos were among the 2 million left exposed.

READ MORE

OTHER SECURITY BREACHES

Another bombshell in France: hacker pilfers data from 1.2 million bank accounts

German Rail Giant Deutsche Bahn Hit by Large-Scale DDoS Attack

Hackers Offer to Sell Millions of Eurail User Records

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-26119 Privilege Escalation in Windows Admin Center

CVSS SCORE 8.8

CVE-2026-22769 Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability

CVSS SCORE 10.0

LAST WEEKS RECAP

CVE-2026-1731: Critical Unauthenticated Remote Code Execution in BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)
CVSS Score: (9.9)

CVE-2026-1357: WordPress plugin with 900k installs vulnerable to critical RCE flaw
CVSS Score: (9.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

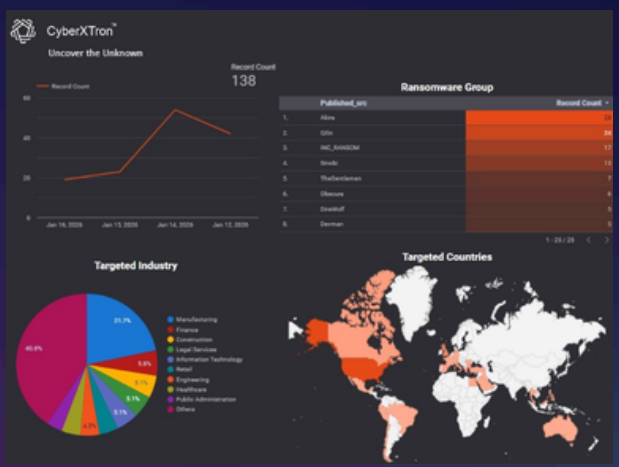
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

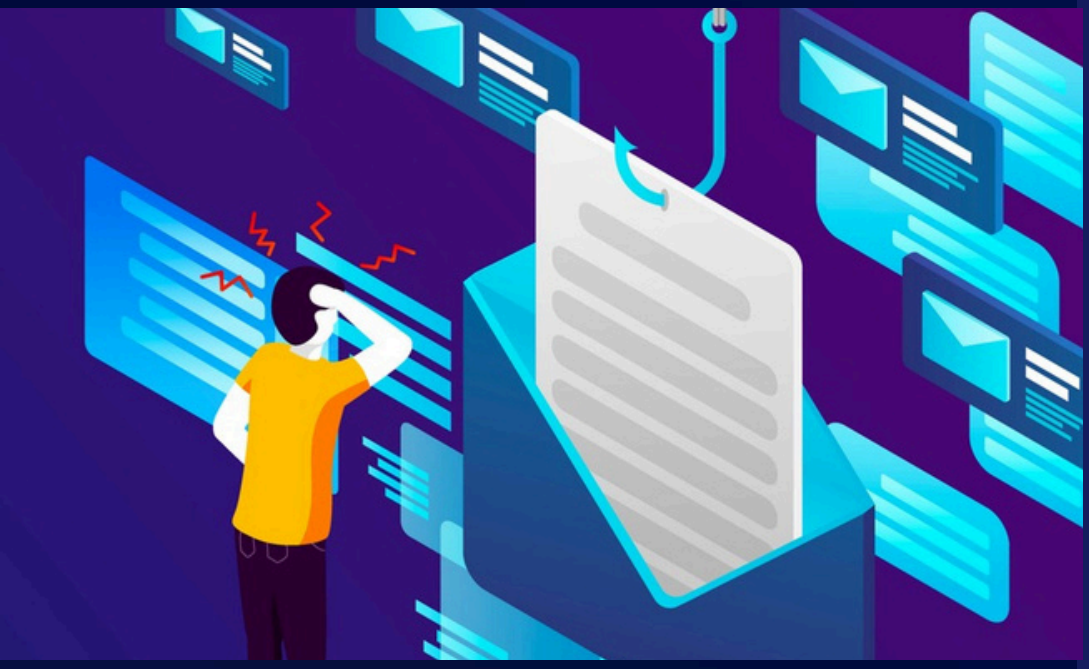
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Hackers target Microsoft Entra accounts in device code vishing attacks

Threat actors are targeting technology, manufacturing, and financial organizations in campaigns that combine device code phishing and voice phishing (vishing) to abuse the OAuth 2.0 Device Authorization flow and compromise Microsoft Entra accounts.
Unlike previous attacks that utilized malicious OAuth applications to compromise accounts, these campaigns instead leverage legitimate Microsoft OAuth client IDs and the device authorization flow to trick victims into authenticating.
This provides attackers with valid authentication tokens that can be used to access the victim's account without relying on regular phishing sites that steal passwords or intercept multi-factor authentication codes.

READ MORE

OTHER PHISHING ARTICLES

Nigerian man gets eight years in prison for hacking tax firms

Microsoft: Anti-phishing rules mistakenly blocked emails, Teams messages

Snail mail letters target Trezor and Ledger users in crypto-theft attacks