SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

July 2026 - VOL.5

The News

IN THE NEWS THIS WEEK

Cisco FMC Zero-Day Actively Exploited, Static Credentials Could Expose Sensitive Data

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a newly disclosed security flaw impacting Cisco Secure Firewall Management Center (FMC) Software to its Known Exploited Vulnerabilities (KEV) catalog, following reports of zero-day exploitation.

The vulnerability, assigned CVE-2026-20316 (CVSS score: 5.3), could permit an unauthenticated, remote attacker to log in to an affected device using a low-privilege account to access sensitive data within susceptible systems.

"This vulnerability is due to the presence of static user credentials for a low-privileged account," Cisco said in an alert released Wednesday. "An attacker could exploit this vulnerability by using the account to log in to an affected system."

READ MORE

OTHER NEWS HIGHLIGHTS

Three Critical VMware Flaws Allow Auth Bypass, Code Execution, and VM Escape

Public PoC Released for Exploited Check Point SmartConsole Authentication Bypass

OpenAI Agent Used Exposed Credentials Across Four Services During Hugging Face Breach

The News

TOP OF THE NEWS THIS WEEK

Claude AI Just Cracked a Post-Quantum Test Scheme and Found a Faster 7-Round AES Attack

Anthropic says Claude Mythos Preview helped derive an end-to-end key-recovery attack against HAWK-256 and a 200- to 800-fold speedup for an attack on seven-round AES-128.

The HAWK attack exploits a previously unused symmetry in the lattice behind the signature scheme. Anthropic's released implementation gives an expected end-to-end runtime of about three hours and 42 minutes on a 96-core server.

The AES result removes a 256-way guessing step from an existing meet-in-the-middle attack.

Anthropic said neither result affects production systems. HAWK remains a candidate in a National Institute of Standards and Technology (NIST) post-quantum standardization process, and the public recovery code only targets the smaller HAWK-256 parameter.

READ MORE

TOP RELATED ARTICLES

Tengu Botnet Reboots Compromised Linux Devices When Defenders Kill Its Process

Critical OpenWrt DHCPv6 Flaw Could Let Unauthenticated Attackers Run Code as Root

Attackers Exploit Arista VeloCloud Orchestrator Command Injection Flaw

Geo-Politics

NEWS FROM AROUND THE WORLD

Russian Hackers Exploit Microsoft OWA Flaw to Keep Mailbox Access After Credential Rotation

The Russian threat actors recently linked to the exploitation of a now-patched vulnerability in Zimbra have been observed exploiting another vulnerability, this time in Microsoft Outlook Web Access (OWA), to target U.S. and European government entities, as well as the telecommunications, financial, hospitality, and aerospace sectors.

The activity, which began on July 22, 2026, involves the weaponization of CVE-2026-42897 (CVSS score: 8.1), a cross-site scripting (XSS) vulnerability in OWA. It was flagged by Microsoft as having been exploited in attacks as far back as May 2026.

Enterprise security company Proofpoint has attributed the activity to Laundry Bear (aka CL-STA-1114, TA488, UNK_PitStop, and Void Blizzard), which was recently attributed to the zero-day exploitation of CVE-2025-66376, an XSS flaw in Zimbra's Classic UI, since at least July 2025 before it was patched four months later.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Amazon Links Debug and Chalk npm Hijack to North Korea's Sapphire Sleet

Russia Charges Telegram Founder Pavel Durov With Aiding Terrorist Activity

TELESHIM Abuses Telegram for C2 in Attacks Against Middle East Governments

Breaches

SECURITY BREACHES THIS WEEK

ShinyHunters Claims Ernst & Young Hack

Earlier this month, the professional services giant reported to the Attorney General's Offices in several states that hackers stole personal and financial information from a third-party service management platform used to support tax-related work.

Between March 28 and April 12, the company said, the attackers downloaded the tax-related documents of Ernst & Young clients that were included in support tickets submitted through the platform.

Client names, addresses, Social Security numbers, account numbers, credit/debit card numbers, and other types of information used for tax filings were compromised in the data breach.

The company is providing the potentially impacted individuals with 24 months of free credit monitoring, identity monitoring, and identity restoration services.

Ernst & Young has not shared details on the number of potentially affected individuals, nor did it say who was behind the attack. The company has not responded to a SecurityWeek inquiry on the matter.

READ MORE

OTHER SECURITY BREACHES

Origin Energy Data Breach Affects 900,000 Australians

DentaQuest Data Breach Potentially Impacts Over 23 Million People

MCBS Data Breach Affects 1.2 Million Individuals

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-59309 - VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. Broadcom has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3.

CVSS SCORE 9.3

CVE-2026-63077 - In JetBrains TeamCity before 2026.1.3, 2025.11.7 unauthenticated remote code execution was possible via the agent polling protocol

-

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2026-63030 - WordPress 6.9.x before 6.9.5 and 7.0.x before 7.0.2 is affected by a REST API batch endpoint route confusion issue which, combined with the author__not_in WP_Query SQL Injection (CVE-2026-60137), could allow an attacker to perform SQL Injection and achieve Remote Code Execution.

CVSS Score: (9.8)

CVE-2026-15409 - A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location.

CVSS Score: (10.0)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

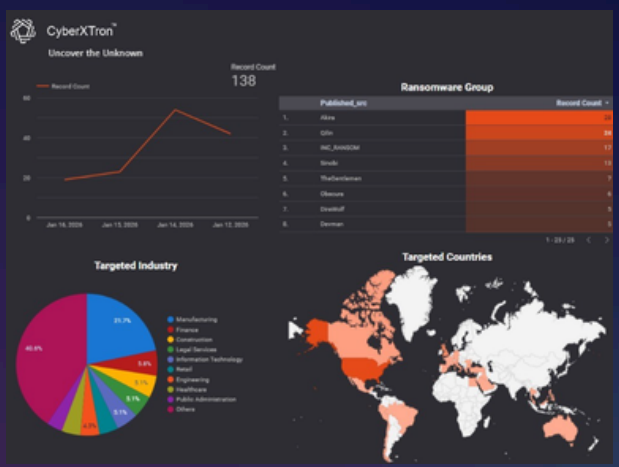
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

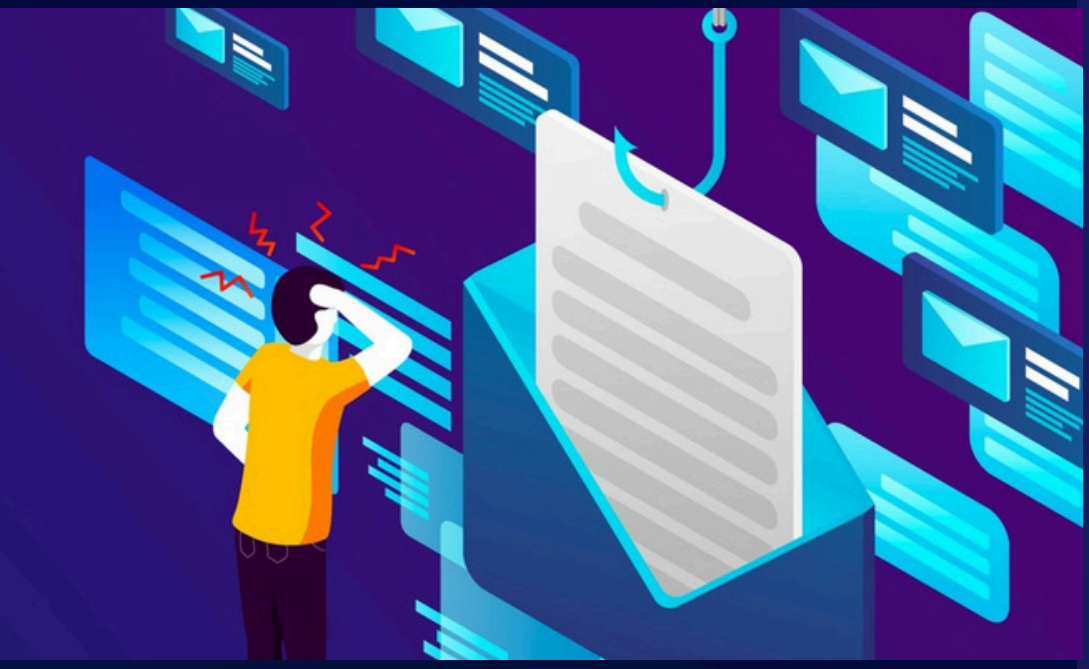
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Flying Eagle Android RAT Traces Found on 170 Servers as Source Code Circulates

Source code for the Flying Eagle Android remote access trojan (RAT) framework is circulating through criminal Telegram channels. Hunt.io and independent researcher NetAskari traced matching control panels and certificates to 170 internet servers.

They linked the framework to a fake Public Security service application targeting Android users in China. The kit supports payment-password and keystroke capture, screen recording, camera access, and phishing prompts for financial, adult-content, and government-service applications.

Hunt.io's search of the preceding 30 days of telemetry found infrastructure fingerprints on 170 servers, a count that does not establish 170 infected phones, victims, operators, or confirmed command-and-control (C2) systems.

READ MORE

OTHER PHISHING ARTICLES

Nimbus Manticore Deploys NightLedger and Turns Victim Systems Into Covert Relays

Operation BlueDash Deploys Level RMM and ScreenConnect via Fake Teams Update

Cruciferra Crypter Uses BYOVD and Process Ghosting to Hide Windows Malware