SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

June 2026 - VOL.4

The News

IN THE NEWS THIS WEEK

Cisco Catalyst SD-WAN Zero-Day CVE-2026-20245 Exploited to Gain Root Access

An unknown threat actor exploited a recently disclosed high-severity security flaw impacting Cisco Catalyst SD-WAN as a zero-day at least two months before it was publicly disclosed, according to new findings from Google-owned Mandiant.

The vulnerability, tracked as CVE-2026-20245 (CVSS score: 7.8), allows an authenticated, local attacker to execute arbitrary commands with elevated privileges by supplying a crafted file to the affected system by taking advantage of the device's insufficient validation of user-supplied input.

Earlier this month, Cisco acknowledged that it became aware of exploitation of this vulnerability, adding that a malicious actor must have netadmin privileges on an affected system to pull off a successful attack.

"Throughout the intrusion, to maintain operational security and avoid detection, the threat actor consistently employed anti-forensic techniques, selectively deleting and restoring system configuration files that were modified during their activities," Mandiant researchers Chester Sng, Pete Boonyakarn, and Logeswaran Nadarajan said.

READ MORE

OTHER NEWS HIGHLIGHTS

CISA Warns Critical Lantronix EDS5000 Flaw Is Being Actively Exploited

Cisco Unified CM Flaw Exploited After PoC Reveals File-Write Path to Root

Fake AI Agent Skill Passed Security Scans and Reportedly Reached 26,000 Agents

The News

TOP OF THE NEWS THIS WEEK

WhatsApp VBScript Campaign Uses Fake Documents to Install ManageEngine RMM Tool

Direct messages sent via WhatsApp are being used to distribute malicious Visual Basic Script (VBScript) files that lead to the installation of legitimate Remote Monitoring and Management (RMM) software.

Per findings from Kaspersky, the active campaign is targeting users of WhatsApp Desktop and WhatsApp Web across Malaysia, Brazil, India, Mexico, Singapore, the U.K., Spain, Taiwan, Australia, Russia, and Vietnam. The highest concentration of victims has been reported in Malaysia.

"The threat actor uses deceptive file names masquerading as business and financial documents to persuade recipients to download and execute the attachment," security researcher Fareed Radzi said. "Once executed, the VBScript initiates a multi-stage infection chain that ultimately results in the installation of legitimate Remote Monitoring and Management (RMM) software, enabling remote access to the victim's system."

It's suspected that the threat actor behind the operation managed to obtain surreptitious access to several WhatsApp accounts and then used them as a distribution vector for the VBScript files across their contacts. That said, exactly how these accounts are compromised is unclear.

READ MORE

TOP RELATED ARTICLES

OpenAI Expands Daybreak With GPT-5.5-Cyber to Help Defenders Patch Security Flaws

AryStinger Malware Infects 4,300 Legacy Routers to Build Reconnaissance Proxy Network

Hackers Exploit Gravity SMTP WordPress Plugin Bug to Expose API Keys

Geo-Politics

NEWS FROM AROUND THE WORLD

Canada's Spy Agency Used First-of-Its-Kind Warrant to Clean Botnet-Infected Devices

Canada's spy service got a judge's permission to reach into infected servers, home routers, and IoT gear sitting on Canadian soil and neutralize two foreign-run botnets.

The Federal Court released a public version of the ruling on June 15. It is the first time the Canadian Security Intelligence Service has used its threat reduction warrant powers this way.

The warrant let CSIS alter, degrade, and destroy botnet data on the infected machines and cut the devices loose from the networks.

The targets were Canada-based servers, small office and home office (SOHO) routers, and Internet of Things devices: Ring doorbells, security cameras, TVs, and other Wi-Fi-enabled appliances.

Justice Catherine Kane granted the warrant on May 1, 2024, renewed it that August, and issued the confidential reasons in February 2026. The warrant stayed out of public view for more than two years, until this month's redacted release.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

INTERPOL Warns Phishing, Ransomware, and AI Scams Are Rising Across Asia-Pacific

2026 FIFA World Cup Faces Surge in Cyber Threats

Russian Initial Access Broker Behind FortiBleed Campaign

Breaches

SECURITY BREACHES THIS WEEK

Canadian Electricity Provider London Hydro Discloses Data Breach

Canadian electricity provider London Hydro is investigating a data breach that potentially impacted the personal and account information of its customers.
London Hydro is a local distribution company serving the City of London, Ontario. It serves roughly 170,000 residential, institutional, commercial, and industrial customers.
On June 20, the electricity provider announced that hackers had broken into its systems and that customers' data was likely accessed.
"London Hydro and the appropriate authorities are currently investigating a data security incident which may have impacted a portion of personal information on some accounts," the company said.
The potentially affected data includes personal information such as names, addresses, email addresses, and phone numbers.
Account information, including account and billing numbers, service addresses, pricing plans, contract dates, and meter numbers and types, might have been impacted as well.

READ MORE

OTHER SECURITY BREACHES

Xsolis Data Breach Affects 1.4 Million Individuals

More Cybersecurity Firms Disclose Impact From Klue Hack

BeyondTrust, LastPass Impacted by Klue-Salesforce Incident

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-20245 - A vulnerability in the CLI of Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, and Cisco Catalyst SD-WAN Validator, formerly SD-WAN vBond

CVSS SCORE 7.8

CVE-2026-34908 - A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi OS devices to make unauthorized changes to the system.

CVSS SCORE 10.0

LAST WEEKS RECAP

CVE-2026-0257 - Authentication bypass vulnerabilities in the GlobalProtect portal and gateway of Palo Alto Networks PAN-OS® software allow the attacker to bypass security restrictions and establish an unauthorized VPN connection,"

CVSS Score: (7.8)

CVE-2026-50656 - Microsoft Defender Elevation of Privilege Vulnerability

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

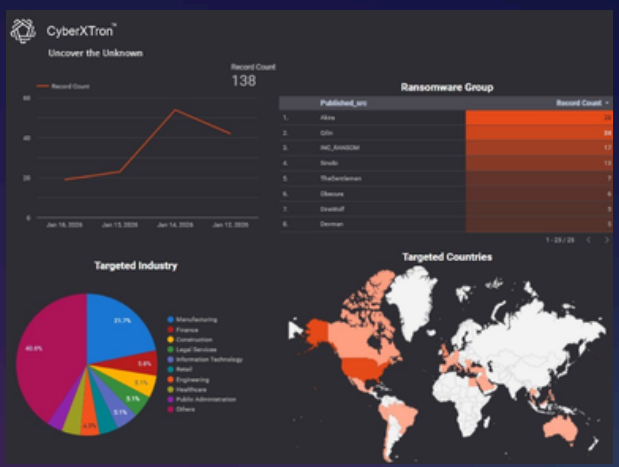
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

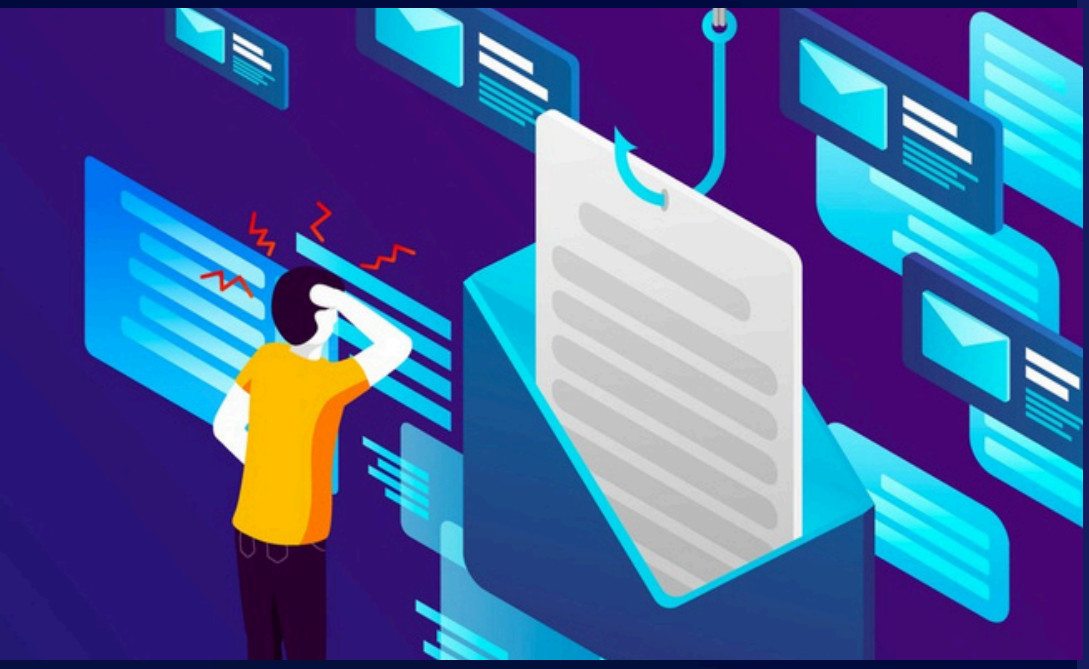
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Lookalike npm Package Hides a Multi-Stage Windows RAT

A malicious npm package has been caught impersonating one of the JavaScript ecosystem's most widely used build tools. The lookalike package hid a multi-stage Windows remote access trojan (RAT) in a supply chain attack on developer machines.

New analysis from JFrog detailed the package which was named postcss-minify-selector-parser. The moniker was intended to allow the package to pose as postcss-selector-parser, a hugely popular library with more than 150 million weekly downloads.

The illegitimate package was still available on the npm registry at the time of writing.

READ MORE

OTHER PHISHING ARTICLES

GTA 6 Scams Emerge as Pre-Orders Open

GentleKiller Framework Disables Victims' Security Software

Cybercrime Surges in APAC as Digitalization Takes Hold