SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

June 2026 - VOL.2

The News

IN THE NEWS THIS WEEK

Ivanti, Fortinet, and SAP Release Patches for Multiple Critical Vulnerabilities

Fortinet, Ivanti, and SAP have released security updates to address multiple critical security vulnerabilities that could result in arbitrary code execution and information disclosure.

The security flaw patched by Fortinet relates to a command injection vulnerability in FortiSandbox, FortiSandbox Cloud, and FortiSandbox PaaS WEB UI. It's tracked as CVE-2026-25089 (CVSS score: 9.1).

"An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiSandbox, FortiSandbox Cloud and FortiSandbox PaaS WEB UI may allow an unauthenticated attacker to execute unauthorized commands via specifically crafted HTTP requests," Fortinet said.

The issue impacts the following products and versions -

- FortiSandbox 5.0.0 through 5.0.5 (Upgrade to 5.0.6 or above)
- FortiSandbox 4.4.0 through 4.4.8 (Upgrade to 4.4.9 or above)
- FortiSandbox Cloud 5.0.4 through 5.0.5 (Upgrade to 5.0.6 or above)
- FortiSandbox PaaS 5.0.4 through 5.0.5 (Upgrade to 5.0.6 or above)

READ MORE

OTHER NEWS HIGHLIGHTS

Unpatched Langflow Flaw CVE-2026-5027 Exploited for Unauthenticated RCE

CISA Adds Cisco, Chrome, and Arista Flaws to KEV Catalog Amid Active Exploitation

---

Microsoft Restores Some GitHub Repos, Keeps Others Offline as Miasma Probe Continues

---

The News

TOP OF THE NEWS THIS WEEK

Microsoft Patches Record 206 Flaws, Including Three Zero-Days and Critical RCE Bugs

Microsoft on Tuesday released fixes for a record 206 security vulnerabilities impacting its software portfolio, including three flaws that have been publicly disclosed at the time of release.

Of the 206 flaws, 39 are rated Critical, and 167 are rated Important in severity. This includes 63 privilege escalation, 56 remote code execution, 30 information disclosure, 27 spoofing, 20 security feature bypass, seven denial-of-service, and three tampering vulnerabilities.

The patches also include two non-Microsoft CVEs, a privilege escalation vulnerability impacting Windows Kernel (CVE-2025-10263) and a UEFI Secure Boot security feature bypass (CVE-2026-8863). They are in addition to more than 350 security flaws that Google has addressed in Chromium, which is used in Microsoft's Edge browser.

Topping the list of fixes is CVE-2026-45657 (CVSS score: 9.8), a use-after-free flaw affecting Windows Kernel that could result in remote code execution.

READ MORE

TOP RELATED ARTICLES

Microsoft Defender RoguePlanet Zero-Day Grants SYSTEM Access on Updated Windows

ServiceNow Flaw Exploited to Gain Unauthorized Access to Customer Instances

GitHub to Disable npm Install Scripts by Default to Stop Supply Chain Attacks

Geo-Politics

NEWS FROM AROUND THE WORLD

China-Linked JDY Botnet Expands to 1,500+ Devices for Cyber Reconnaissance

Cybersecurity researchers have warned of a "resurgence and expansion" of JDY, a covert network associated with China-nexus state-sponsored threat actors.

"The JDY botnet comprises over 1,500 SOHO [small office and home office] and IoT devices and operates as a centrally controlled, high-performance scanner used to discover, fingerprint, and continuously map exposed services at scale," Lumen's Black Lotus Labs said in a report shared with The Hacker News.

JDY was first flagged as a cluster within another botnet codenamed KV-botnet in mid-December 2023. Primarily used for broader scanning against internet targets, the stealthy network comprising compromised SOHO routers, firewalls, and IoT devices has been put to use by Chinese hacking groups like Volt Typhoon.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

China used websites to target security-clearance holders, officials say

---

WinRAR Flaw Exploited by Russia-Aligned Groups to Deploy Stealers in Ukraine

---

Chinese, N. Korean Threat Groups Build on Asia-Pacific Success

Breaches

SECURITY BREACHES THIS WEEK

Hackers Leak DentaQuest Information Impacting 2.6 Million

The ShinyHunters extortion group has published over 230 gigabytes of data allegedly stolen from dental benefits administrator DentaQuest.

The threat actor listed DentaQuest on its Tor-based leak site last month, claiming negotiations with the company failed, and leaking a 234 GB archive containing allegedly stolen data. According to data breach notification website HaveIBeenPwned, which added the information to its database, the leak impacts roughly 2.6 million accounts.

The dataset includes names, addresses, email addresses, phone numbers, dates of birth, government-issued IDs, and health insurance information.

This week, DentaQuest confirmed falling victim to a cyberattack, saying it was working with external cybersecurity experts to determine the scope of the incident and what data might have been compromised.

READ MORE

OTHER SECURITY BREACHES

University of Nottingham Confirms Breach After Hackers Leak Data

Meta Says 20,000 Instagram Accounts Hacked via AI Tool Abuse

174,000 Impacted by Lansing Community College Data Breach

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-5027 - Unpatched Langflow Flaw Exploited for Unauthenticated RCE

CVSS SCORE 8.8

CVE-2026-8863 - UEFI Secure Boot security feature bypass

CVSS SCORE 6.8

LAST WEEKS RECAP

CVE-2024-21182 - Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware

CVSS Score: (7.5)

CVE-2024-7593 - Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

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

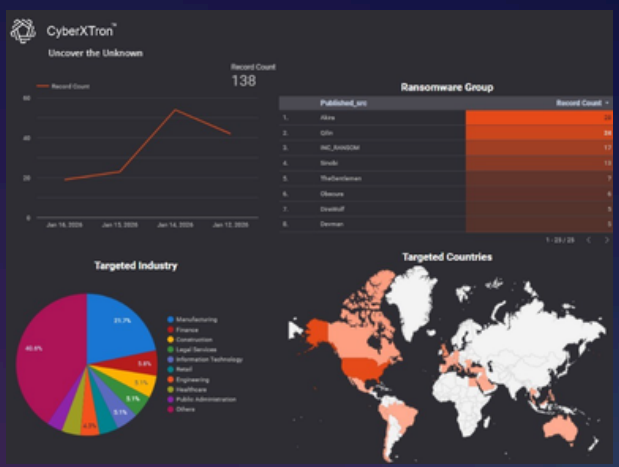
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

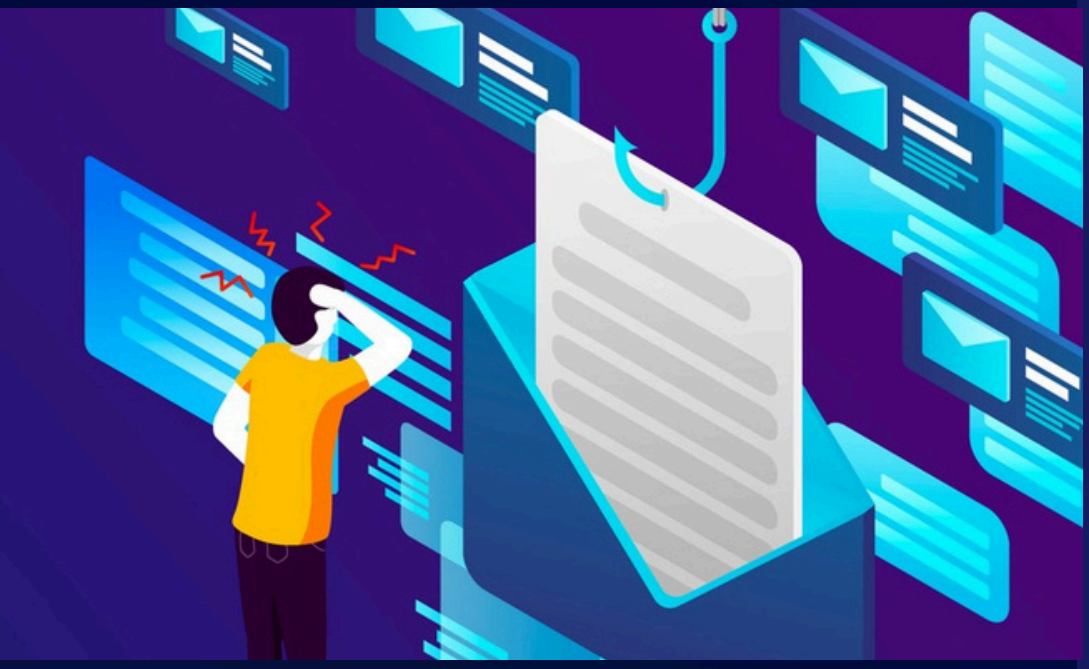
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Hades PyPI Attack: 19 Packages Poisoned to Auto-Run Bun Credential Stealer

The Miasma supply chain campaign has sparked a fresh attack wave called Hades, this time involving 37 malicious wheel artifacts across 19 packages in the Python Package Index (PyPI) registry, as the Mini Shai-Hulud-style attacks continue to be refined and splintered to target specific ecosystems.
"The compromised releases shipped a *-setup.pth file that attempts to execute automatically during Python startup, download the Bun JavaScript runtime, and run an obfuscated JavaScript payload named _index.js," Socket said in a new analysis.

READ MORE

OTHER PHISHING ARTICLES

Chrome V8 Zero-Day CVE-2026-11645 Exploited in the Wild - Patch Now

Instagram Account Hacks, Android Zero-Day, GitHub Worm and More

Meta Blocks NSO Group's New WhatsApp Phishing Attack, Files Contempt Order