SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

April 2026 - VOL.3

The News

IN THE NEWS THIS WEEK

April Patch Tuesday Fixes Critical Flaws Across SAP, Adobe, Microsoft, Fortinet, and More

A number of critical vulnerabilities impacting products from Adobe, Fortinet, Microsoft, and SAP have taken center stage in April's Patch Tuesday releases. Topping the list is an SQL injection vulnerability impacting SAP Business Planning and Consolidation and SAP Business Warehouse (CVE-2026-27681, CVSS score: 9.9) that could result in the execution of arbitrary database commands.

"The vulnerable ABAP program allows a low-privileged user to upload a file with arbitrary SQL statements that will then be executed," Onapsis said in an advisory. In a potential attack scenario, a bad actor could abuse the affected upload-related functionality to run malicious SQL against BW/BPC data stores, extract sensitive data, and delete or corrupt database content.

"Manipulated planning figures, broken reports, or deleted consolidation data can undermine close processes, executive reporting, and operational planning," Pathlock said. "In the wrong hands, this issue also creates a credible path to both stealthy data theft and overt business disruption."

READ MORE

OTHER NEWS HIGHLIGHTS

Adobe Patches Actively Exploited Acrobat Reader Flaw CVE-2026-34621

Google Rolls Out DBSC in Chrome 146 to Block Session Theft on Windows

Marimo RCE Flaw CVE-2026-39987 Exploited Within 10 Hours of Disclosure

The News

TOP OF THE NEWS THIS WEEK

Microsoft Issues Patches for SharePoint Zero-Day and 168 Other New Vulnerabilities

Microsoft on Tuesday released updates to address a record 169 security flaws across its product portfolio, including one vulnerability that has been actively exploited in the wild.

Of these 169 vulnerabilities, 157 are rated Important, eight are rated Critical, three are rated Moderate, and one is rated Low in severity. Ninety-three of the flaws are classified as privilege escalation, followed by 21 information disclosure, 21 remote code execution, 14 security feature bypass, 10 spoofing, and nine denial-of-service vulnerabilities.

Also included among the 169 flaws are four non-Microsoft issued CVEs impacting AMD (CVE-2023-20585), Node.js (CVE-2026-21637), Windows Secure Boot (CVE-2026-25250), and Git for Windows (CVE-2026-32631).

The updates are in addition to 78 vulnerabilities that have been addressed in its Chromium-based Edge browser since the update that was released last month.

READ MORE

TOP RELATED ARTICLES

Mirax Android RAT Turns Devices into SOCKS5 Proxies, Reaching 220,000 via Meta Ads

Google Adds Rust-Based DNS Parser into Pixel 10 Modem to Enhance Security

OpenAI Launches GPT-5.4-Cyber with Expanded Access for Security Teams

Geo-Politics

NEWS FROM AROUND THE WORLD

North Korea's APT37 Uses Facebook Social Engineering to Deliver RokRAT Malware

The North Korean hacking group tracked as APT37 (aka ScarCruft) has been attributed to a fresh multi-stage, social engineering campaign in which threat actors approached targets on Facebook and added them as friends on the social media platform, turning the trust-building exercise into a delivery channel for a remote access trojan called RokRAT.

"The threat actor used two Facebook accounts with their location set to Pyongyang and Pyongsong, North Korea, to identify and screen targets," the Genians Security Center (GSC) said in a technical breakdown of the campaign. "After building trust through friend requests, the actor moved the conversation to Messenger and used specific topics to lure targets as part of the initial social engineering stage of the attack."

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

UAC-0247 Targets Ukrainian Clinics and Government in Data-Theft Malware Campaign

Sweden Blames Pro-Russian Group for Cyberattack Last Year on Its Energy Infrastructure

6-Year Ransomware Campaign Targets Turkish Homes & SMBs

Breaches

SECURITY BREACHES THIS WEEK

Stryker warns of earnings fallout from March cyberattack

Stryker, the Michigan-based medtech provider, said in a regulatory filing that the March cyberattack that temporarily disrupted the company's manufacturing, ordering and shipping operations had a material impact on its first-quarter earnings.

The March 11 incident, which the Iran-backed threat group named Handala took responsibility for, was a wiper attack abusing the company's Microsoft Intune environment. The attackers wiped data from thousands of company devices and briefly disabled Stryker's electronic ordering systems.

The U.K.'s National Health Service issued an update in March noting that certain orders from Stryker in the days after the attack were impacted and an interim ordering system was set up.

READ MORE

OTHER SECURITY BREACHES

Europe's Largest Gym Chain Says Data Breach Impacts 1 Million Members

Hims Breach Exposes the Most Sensitive Kinds of PHI

Stolen Rockstar Games analytics data leaked by extortion gang

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-34621 - Successful exploitation of the flaw could allow an attacker to run malicious code on affected installations

CVSS SCORE 8.6

CVE-2026-34197 - is a remote code execution vulnerability in Apache ActiveMQ Classic that has been hiding in plain sight for 13 years

CVSS SCORE 8.8

LAST WEEKS RECAP

Fortinet FortiClient EMS Zero-Day: CVE-2026-35616 (Active Exploitation Underway)
CVSS Score: (9.8)

Docker CVE-2026-34040 Lets Attackers Bypass Authorization and Gain Host Access
CVSS Score: (8.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

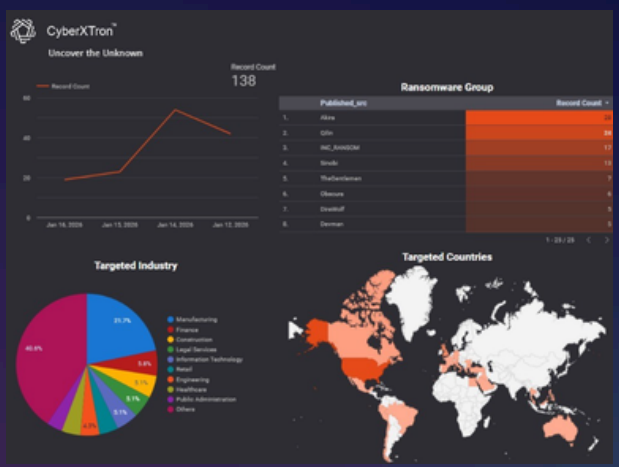
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

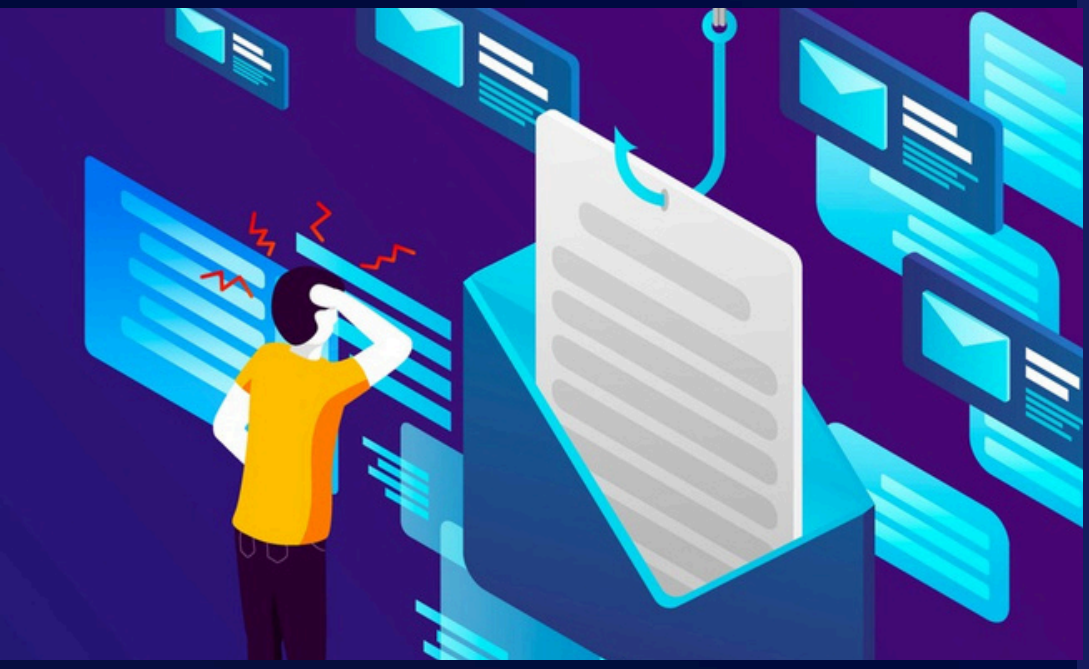
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



FBI and Indonesian Police Dismantle W3LL Phishing Network Behind $20M Fraud Attempts

The U.S. Federal Bureau of Investigation (FBI), in partnership with the Indonesian National Police, has dismantled the infrastructure associated with a global phishing operation that leveraged an off-the-shelf toolkit called W3LL to steal thousands of victims' account credentials and attempt more than $20 million in fraud.

In tandem, authorities detained the alleged developer, who has been identified as G.L, and seized key domains linked to the phishing scheme. "The takedown cuts off a major resource used by cybercriminals to gain unauthorized access to victims' accounts," the FBI said in a statement.

The W3LL phishing kit allowed criminals to mimic legitimate login pages to deceive victims into handing over their credentials, thus allowing the attackers to seize control of their accounts. The phishing kit was advertised for a fee of about $500.

READ MORE

OTHER PHISHING ARTICLES

n8n Webhooks Abused Since October 2025 to Deliver Malware via Phishing Emails

Newly Discovered PowMix Botnet Hits Czech Workers Using Randomized C2 Traffic

Microsoft adds Windows protections for malicious Remote Desktop files