SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

March 2026 - VOL.2

The News

IN THE NEWS THIS WEEK

Microsoft Patches 84 Flaws in March Patch Tuesday, Including Two Public Zero-Days

Microsoft on Tuesday released patches for a set of 84 new security vulnerabilities affecting various software components, including two that have been listed as publicly known.

Of these, eight are rated Critical, and 76 are rated Important in severity. Forty-six of the patched vulnerabilities relate to privilege escalation, followed by 18 remote code execution, 10 information disclosure, four spoofing, four denial-of-service, and two security feature bypass flaws.

The fixes are in addition to 10 vulnerabilities that have been addressed in its Chromium-based Edge browser since the release of the February 2026 Patch Tuesday update.

READ MORE

OTHER NEWS HIGHLIGHTS

Apple Issues Security Updates for Older iOS Devices Targeted by Coruna WebKit Exploit

OpenAI Codex Security Scanned 1.2 Million Commits and Found 10,561 High-Severity Issues

Dozens of Vendors Patch Security Flaws Across Enterprise Software and Network Devices

The News

TOP OF THE NEWS THIS WEEK

Fortinet, Ivanti, Intel Patch High-Severity Vulnerabilities

Fortinet, Ivanti, and Intel on Tuesday rolled out security fixes for dozens of vulnerabilities, including high-severity bugs that could be exploited for arbitrary code execution, privilege escalation, or security protection bypasses.

Fortinet announced patches for 22 security defects across its products, including high-severity flaws in FortiWeb, FortiSwitchAXFixed, FortiManager, and FortiClientLinux.

The FortiWeb, FortiSwitchAXFixed, and FortiManager issues could be exploited by remote, unauthenticated attackers to bypass the authentication rate limit or execute unauthorized code or commands.

The FortiClientLinux weakness, described as a Symlink following vulnerability, could allow local attackers to escalate their privileges to root.

On Tuesday, Fortinet also addressed medium- and low-severity flaws that could lead to data tampering, security protection bypasses, arbitrary code execution, information disclosure, denial-of-service (DoS), arbitrary command execution, privilege escalation, or social engineering attacks.

Fortinet made no mention of any of these vulnerabilities being exploited in the wild.

READ MORE

TOP RELATED ARTICLES

CISA Flags Actively Exploited n8n RCE Bug as 24,700 Instances Remain Exposed

Anthropic Finds 22 Firefox Vulnerabilities Using Claude Opus 4.6 AI Model

Web Server Exploits and Mimikatz Used in Attacks Targeting Asian Critical Infrastructure

Geo-Politics

NEWS FROM AROUND THE WORLD

APT28 Uses BEARDSHELL and COVENANT Malware to Spy on Ukrainian Military

The Russian state-sponsored hacking group tracked as APT28 has been observed using a pair of implants dubbed BEARDSHELL and COVENANT to facilitate long-term surveillance of Ukrainian military personnel.

The two malware families have been put to use since April 2024, ESET said in a new report shared with The Hacker News.

APT28, also tracked as Blue Athena, BlueDelta, Fancy Bear, Fighting Ursa, Forest Blizzard (formerly Strontium), FROZENLAKE, Iron Twilight, ITG05, Pawn Storm, Sednit, Sofacy, and TA422, is a nation-state actor affiliated with Unit 26165 of the Russian Federation's military intelligence agency GRU.

The threat actor's malware arsenal consists of tools like BEARDSHELL and COVENANT, along with another program codenamed SLIMAGENT that's capable of logging keystrokes, capturing screenshots, and collecting clipboard data. SLIMAGENT was first publicly documented by the Computer Emergency Response Team of Ukraine (CERT-UA) in June 2025.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Middle East Conflict Highlights Cloud Resilience Gaps

Polyfill Supply Chain Attack Impacting 100k Sites Linked to North Korea

State-linked actors targeted US networks in lead-up to Iran war

Breaches

SECURITY BREACHES THIS WEEK

Michelin Confirms Data Breach Linked to Oracle EBS Attack

Tire giant Michelin has confirmed a data breach stemming from the massive cybercrime campaign that targeted organizations using Oracle's E-Business Suite (EBS) solution.

The ClOp ransomware and extortion group has taken credit for the EBS hacking campaign, which involved the exploitation of zero-day vulnerabilities to gain access to data stored by the targeted organizations in Oracle's enterprise management software.

It's worth noting that while ClOp serves as the public-facing extortion brand for the Oracle EBS campaign, cybersecurity researchers believe the operation was driven by a sophisticated cluster of threat actors, most notably FIN11.

More than 100 allegedly targeted organizations have been listed on the ClOp website.

One of them is tire maker Michelin, which has now confirmed for SecurityWeek that it was one of the impacted organizations.

READ MORE

OTHER SECURITY BREACHES

KadNap Malware Infects 14,000+ Edge Devices to Power Stealth Proxy Botnet

Chrome Extension Turns Malicious After Ownership Transfer, Enabling Code Injection and Data Theft

Medtech Firm Stryker Disrupted by Pro-Iran Hackers

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-27577 - Expression sandbox escape leading to remote code execution (RCE)

CVSS SCORE 9.4

CVE-2026-27493 - Unauthenticated expression evaluation via n8n's Form nodes

CVSS SCORE 9.5

LAST WEEKS RECAP

CVE-2026-20127 Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
CVSS Score: (10.0)

CVE-2026-3061: Out of bounds read in Google Chrome
CVSS Score: (9.1)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

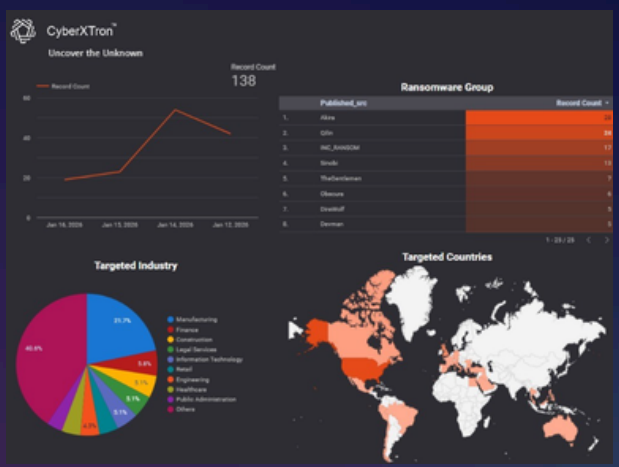
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

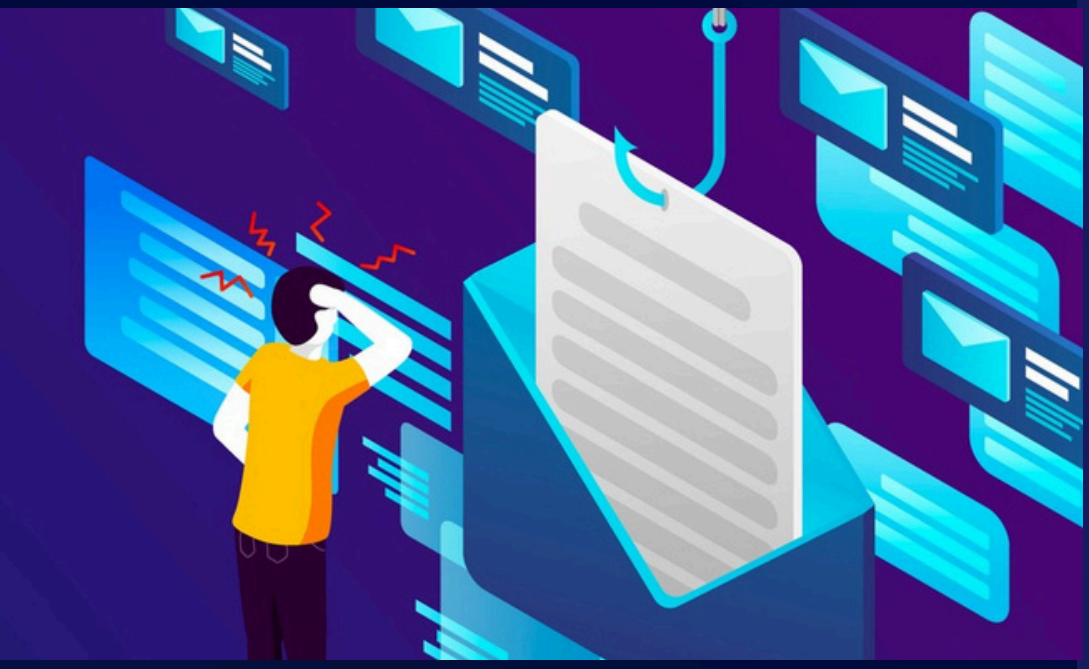
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Phishing Campaign Delivers BeatBanker Trojan To Spread Cryptocurrency Miner and RAT

A recent phishing campaign has been targeting Brazilian users through a trojanized version of the Red Alert rocket warning app.
This malware, named BeatBanker, masquerades as a legitimate application, spreading via a fake Google Play Store page and targeting devices with both a cryptocurrency miner and a banking Trojan.
This multi-layered attack campaign exploits public safety concerns, especially during times of geopolitical tension, making it an effective tool for cybercriminals.

READ MORE

OTHER PHISHING ARTICLES

Five Malicious Rust Crates and AI Bot Exploit CI/CD Pipelines to Steal Developer Secrets

Researchers Trick Perplexity's Comet AI Browser Into Phishing Scam in Under Four Minutes

Six Android Malware Families Target Pix Payments, Banking Apps, and Crypto Wallets