SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

March 2026 - VOL.3

The News

IN THE NEWS THIS WEEK

Apple Fixes WebKit Vulnerability Enabling Same-Origin Policy Bypass on iOS and macOS

Apple on Tuesday released its first round of Background Security Improvements to address a security flaw in WebKit that affects iOS, iPadOS, and macOS.

The vulnerability, tracked as CVE-2026-20643 (CVSS score: N/A), has been described as a cross-origin issue in WebKit's Navigation API that could be exploited to bypass the same-origin policy when processing maliciously crafted web content.

The flaw affects iOS 26.3.1, iPadOS 26.3.1, macOS 26.3.1, and macOS 26.3.2. It has been addressed with improved input validation in iOS 26.3.1 (a), iPadOS 26.3.1 (a), macOS 26.3.1 (a), and macOS 26.3.2 (a). Security researcher Thomas Espach has been credited with discovering and reporting the shortcoming.

Apple notes that Background Security Improvements are meant for delivering lightweight security releases for components such as the Safari browser, WebKit framework stack, and other system libraries through smaller, ongoing security patches rather than issuing them as part of larger software updates.

The feature is supported and enabled for future releases starting with iOS 26.1, iPadOS 26.1, and macOS 26. In cases where compatibility issues are discovered, the improvements may be temporarily removed and then enhanced in a subsequent software update, Apple adds.

READ MORE

OTHER NEWS HIGHLIGHTS

Veeam Patches 7 Critical Backup & Replication Flaws Allowing Remote Code Execution

Ubuntu CVE-2026-3888 Bug Lets Attackers Gain Root via systemd Cleanup Timing Exploit

9 Critical IP KVM Flaws Enable Unauthenticated Root Access Across Four Vendors

The News

TOP OF THE NEWS THIS WEEK

Cisco Firewall Vulnerability Exploited as Zero-Day in Interlock Ransomware Attacks

The vulnerability is tracked as CVE-2026-20131 and it affects the Secure Firewall Management Center (FMC) software. The availability of patches was announced on March 4, when Cisco patched dozens of other vulnerabilities in its FMC, ASA, and Secure FTD products.

CVE-2026-20131 impacts the web-based management interface of FMC software and it can be exploited by a remote, unauthenticated attacker to execute arbitrary Java code with root privileges.

Cisco noted at the time of disclosure that not exposing the FMC management interface to the internet reduces the vulnerability's attack surface.

READ MORE

TOP RELATED ARTICLES

'DarkSword' iOS Exploit Kit Used by State-Sponsored Hackers, Spyware Vendors

Researcher Discovers 4th WhatsApp View Once Bypass; Meta Won't Patch

Google Fixes Two Chrome Zero-Days Exploited in the Wild Affecting Skia and V8

Geo-Politics

NEWS FROM AROUND THE WORLD

EU Sanctions Companies in China, Iran for Cyberattacks

The European Council has imposed sanctions on three ostensibly private companies — two in China, one in Iran — for aiding and carrying out cyberattacks in European countries.

One of the two companies based in China, called Integrity Technology Group, is a mid-size publicly traded corporation. It was found to have regularly provided products that hackers used to compromise devices in Europe, not to mention the rest of the world. The European Council linked it to 65,000 compromised devices across six European Union (EU) countries between 2022 and 2023 alone.

The most notorious of the bunch, though, is Anxun Information Technology, better known to the West as "iSoon." ISoon is a hack-for-hire operation that has worked on behalf of China's government and military, though it purports to be a cybersecurity training company. In addition to the company itself, iSoon's two founders have also been sanctioned as individuals.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Breaches

SECURITY BREACHES THIS WEEK

Iranian Hackers Likely Used Malware-Stolen Credentials in Stryker Breach

The attack on Stryker, a major manufacturer of surgical equipment and orthopedic implants for hospitals worldwide, came to light on March 11, with the Iran-linked hacker group Handala immediately taking credit.

Handala, which is believed to be an anti-Israel hacktivist persona under the control of Iran's Ministry of Intelligence and Security (MOIS), claimed to have wiped more than 200,000 devices, forcing Stryker to shut down offices in dozens of countries. The hackers also claimed to have stolen a significant amount of data.

While some early reports indicated that the hackers used wiper malware in the attack — Handala has been known to use such malware — Stryker said it found no evidence of malware being deployed on its systems.

According to some reports, the attackers wiped systems by abusing Stryker's Microsoft Intune instance, which is used to remotely manage desktop and mobile endpoints and applications within the organization.

READ MORE

OTHER SECURITY BREACHES

Robotic Surgery Giant Intuitive Discloses Cyberattack

Oracle EBS Hack: Only 4 Corporate Giants Still Silent on Potential Impact

174 Vulnerabilities Targeted by RondoDox Botnet

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-20131 Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability

CVSS SCORE 10.0

CVE-2026-32746 Telnet: Critical vulnerability allows injecting malicious code from the network

CVSS SCORE 9.8

LAST WEEKS RECAP

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)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

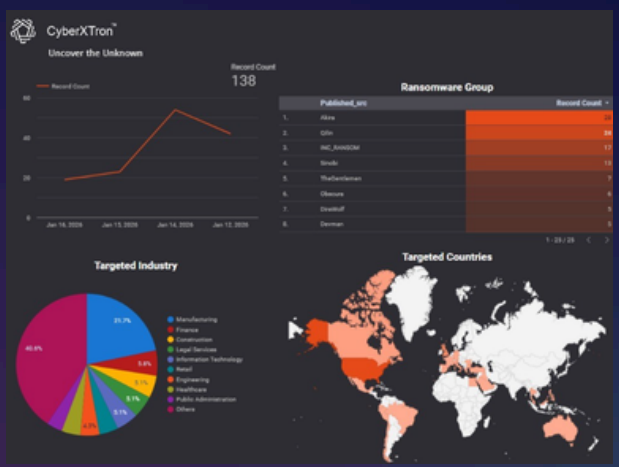
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

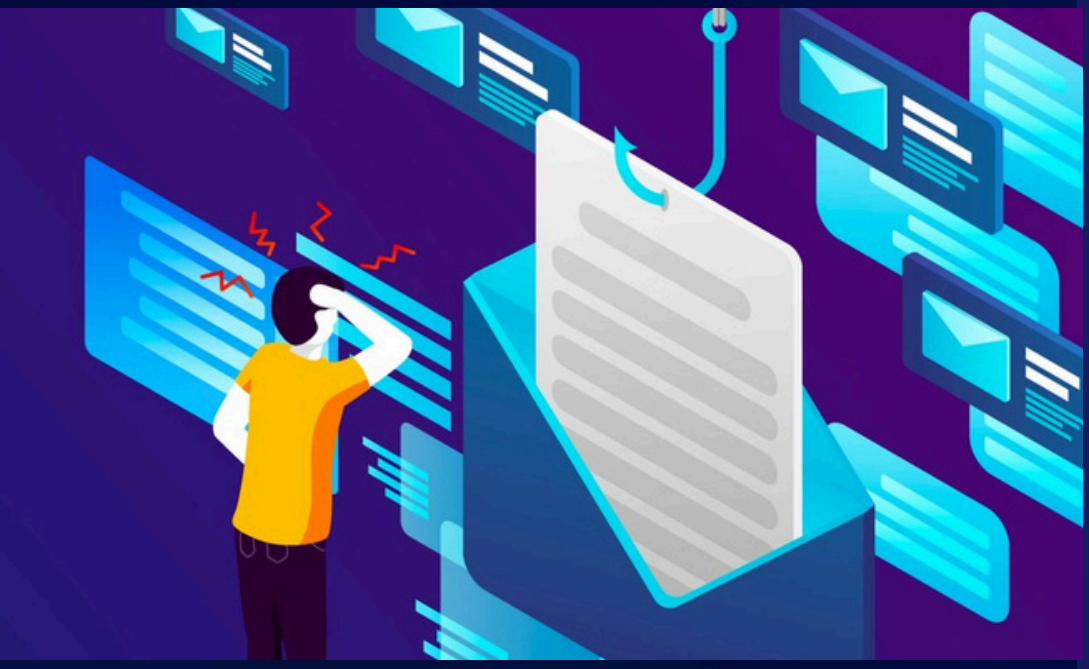
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Security Firm Executive Targeted in Sophisticated Phishing Attack

A C-level executive at Swedish exposure management and identity security firm Outpost24 was targeted in a sophisticated phishing attack, though the effort was unsuccessful, the company's subsidiary Specops Software reports.

Specops said the attack was identified early and blocked before it could compromise systems or impact users. However, the security firm has disclosed technical details to highlight its sophistication.

The attack, likely mounted with a recently identified phishing-as-a-service kit named Kratos, relied on a seven-step chain that leveraged layered infrastructure and legitimate services to evade detection and deceive the recipient.

The phishing message, impersonating financial services provider JP Morgan, appeared as if part of an existing email thread to increase its sense of legitimacy, and invited the recipient to review and sign a document.

READ MORE

OTHER PHISHING ARTICLES

Crypto Scam "ShieldGuard" Dismantled After Malware Discovery

Researchers Warn of Global Surge in Fake Shipment Tracking Scams

Companies House Web Glitch Exposes Corporate Details to Fraudsters