SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

July 2026 - VOL.1

The News

IN THE NEWS THIS WEEK

SharePoint RCE CVE-2026-45659 Added to CISA KEV After Active Exploitation

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added a high-severity flaw impacting Microsoft SharePoint Server to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.
The vulnerability, tracked as CVE-2026-45659 (CVSS score: 8.8), is a case of remote code execution arising from the deserialization of untrusted data. The issue was addressed by Microsoft in May 2026 for SharePoint Server Subscription Edition, SharePoint Server 2019, and SharePoint Enterprise Server 2016.
Microsoft noted that any authenticated attacker could trigger the vulnerability, and that it does not require admin or other elevated privileges. In a network-based attack, an authenticated attacker with a minimum of Site Member permissions (PR:L) could leverage it to execute code remotely on the SharePoint Server.

READ MORE

OTHER NEWS HIGHLIGHTS

Critical Cursor Flaws Could Let Prompt Injection Escape Sandbox and Run Commands

AI-Generated Browser Ransomware Abuses Chromium API on Windows, Linux, macOS, Android

Azure CLI Password Spray Hits at Least 78 Microsoft Accounts in 81M+ Attempts

The News

TOP OF THE NEWS THIS WEEK

Adobe Patches 7 CVSS 10.0 Flaws in ColdFusion and Campaign Classic

Adobe has released patches for multiple maximum-severity security flaws impacting Adobe ColdFusion and Adobe Campaign Classic.
The ColdFusion updates "resolves critical and important vulnerabilities that could lead to arbitrary code execution, privilege escalation, arbitrary file system read, and security feature bypass," Adobe said in an alert released Tuesday.
The issues have been addressed in ColdFusion 2023 Update 21 and ColdFusion 2025 Update 10. Security researchers Anirudh Anand, Matan Sandori, and 2Bsecure have been credited with discovering and reporting CVE-2026-48283, CVE-2026-48313, and CVE-2026-48307.

READ MORE

TOP RELATED ARTICLES

Citrix Patches Six NetScaler Flaws Allowing File Read and Denial-of-Service

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

Silent Swap Crypto Clipper Uses Fake Google Notes Extension to Replace Wallet Addresses

Geo-Politics

NEWS FROM AROUND THE WORLD

Ukraine Says Russian Intelligence Used Fake Support Texts to Steal Messaging Credentials

The Security Service of Ukraine (SSU) said it, together with the U.S. Federal Bureau of Investigation (FBI), uncovered a long-running campaign orchestrated by Russian intelligence services to break into the messaging accounts of government officials, military personnel, politicians, and activists in Ukraine, Europe, and the U.S.

The systematic cyber attacks aimed at stealing sensitive information from the victims, the agency added.

"The goal of these 'hacks' is to gain access to sensitive military, political, and economic information exchanged by users, as well as to steal their personal data," the agency warned in a post shared on Telegram.

To pull off the operation, the attackers send SMS messages that masquerade as the messaging platform's support bot and urge users to disclose their account credentials.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Breaches

SECURITY BREACHES THIS WEEK

Aflac Japan Data Breach Impacts 4.38 Million

The company's systems were hacked on June 15, and the attackers accessed them several times until June 25, when the data breach was discovered, Aflac said in a filing with the US Securities and Exchange Commission.

"Upon identifying the unlawful access, Aflac Japan promptly took steps designed to contain the incident and prevent further intrusion, including suspending certain systems," Aflac said.

The incident is limited to certain Aflac Japan systems and does not affect Aflac's systems related to the US business, the insurance giant told the SEC.

According to an FAQ published on Aflac Japan's website, at least five services have been disrupted as a result of the incident. For the time being, the company could not estimate when the affected services may be restored.

Aflac Japan says the attackers exfiltrated data from its policyholder portal, and that approximately 4.38 million customers and agents are likely affected.

READ MORE

OTHER SECURITY BREACHES

Nissan Employee Data Breached in Oracle PeopleSoft Hack

Insurance Regulators Group NAIC Hit in Oracle PeopleSoft Hack

More Klue Breach Victims Identified as Hackers Get Hacked

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-48276 - ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user.

CVSS SCORE 10.0

CVE-2026-8451 - Insufficient input validation in NetScaler ADC and NetScaler Gateway leading to memory overread if NetScaler ADC or NetScaler Gateway is configured as a SAML IDP

CVSS SCORE 7.5

LAST WEEKS RECAP

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: (7.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

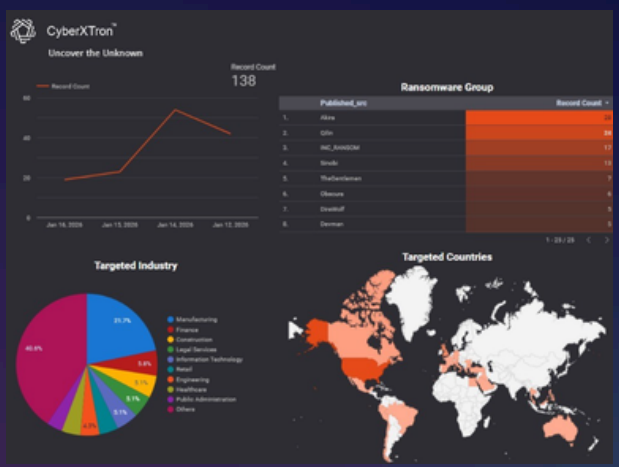
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

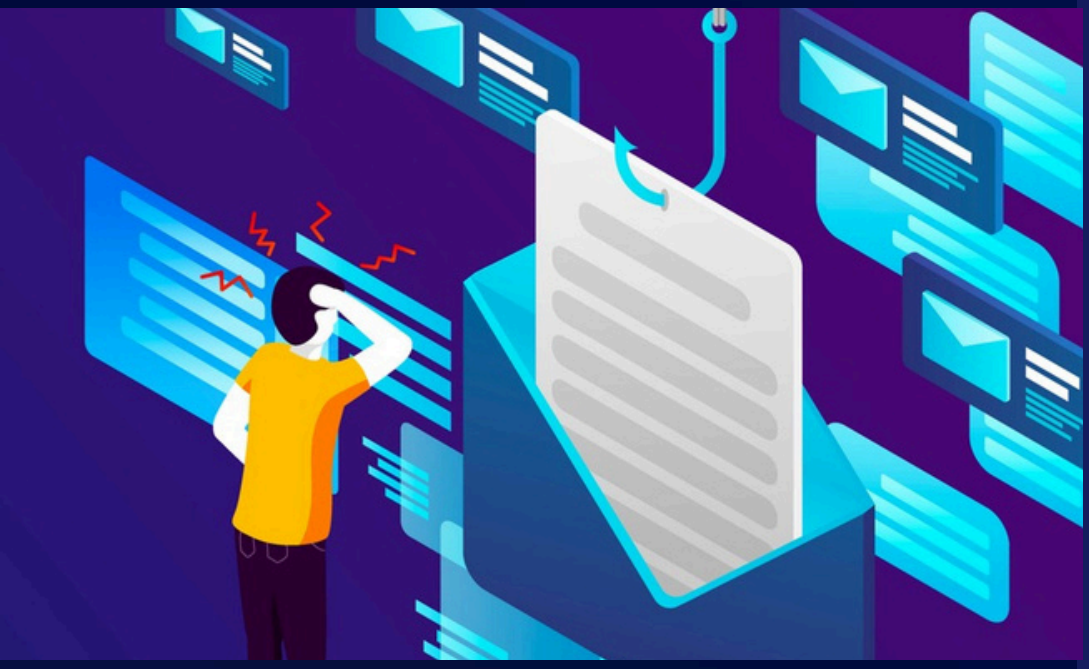
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Ousaban Banking Trojan Targets Iberian Bank Users with Fake PDF Lures

A Brazilian banking trojan called Ousaban is going after Windows users who bank in Spain and Portugal. Fortinet's FortiGuard Labs identified the campaign in May 2026.

It opens with a phishing PDF disguised as a corrupted file, checks that the visitor is really in Spain or Portugal, and hides its real payload inside an image.

The goal is the usual one: steal banking logins and take over accounts.

Ousaban sits quietly on a Windows PC and waits for the user to open a banking site. When a target bank loads, it can capture screenshots and keystrokes, tamper with the clipboard, show fake messages, and give the attacker remote control.

Together, those are the tools for hijacking a live banking session and taking over an account. Ousaban watches for more than two dozen banks across the two countries, among them Banco Santander, BBVA, CaixaBank, Bankinter, and Caixa Geral de Depósitos.

READ MORE

OTHER PHISHING ARTICLES

Phantom Squatting Uses AI-Hallucinated Domains for Phishing and Malware

VEIL#DROP Malware Chain Uses Blogger Platform to Deliver PureLogs Stealer

ConsentFix and ClickFix: How Microsoft 365 Accounts are Hijacked in 3 Seconds