SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

May 2026 - VOL.5

The News

IN THE NEWS THIS WEEK

Microsoft Patches SharePoint RCE Flaw CVE-2026-45659 Across Server Versions

Microsoft has rolled out updates to fix a remote code execution vulnerability impacting SharePoint that could be exploited by bad actors in attacks without requiring any specialized conditions to be met.

The vulnerability, tracked as CVE-2026-45659, carries a CVSS score of 8.8. It has been assigned an important severity.

"Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network," Microsoft said in an advisory released last week.

Microsoft noted that the vulnerability could be triggered by any authenticated attacker, and that it does not require administrator or other elevated privileges.

READ MORE

OTHER NEWS HIGHLIGHTS

MFA Prompt Bombing: Why Your Second Factor Isn't Saving You

Claude Mythos AI Finds 10,000 High-Severity Flaws in Widely Used Software

Gitea Vulnerability Exposes Private Container Images without Authentication

The News

TOP OF THE NEWS THIS WEEK

Over 5,500 GitHub Repositories Infected in 'Megalodon' Supply Chain Attack

The campaign, dubbed Megalodon, relies on GitHub Actions workflows containing a payload designed to steal credentials, keys, tokens, and other secrets.

The workflows, SafeDep says, were injected through over 5,700 malicious commits pushed to the impacted repositories within a six-hour window, on May 18.

According to the cybersecurity firm, the attackers deployed two payloads as part of the attack. One was designed to add a new workflow that would be triggered on every push and pull request, and another that replaced existing workflows with specific triggers, creating dormant backdoors.

On infected machines, the malware would exfiltrate all CI environment variables, AWS credentials, GCP access tokens, Azure credentials, SSH private keys, Docker and Kubernetes configurations, API keys, database connection strings, GitHub Actions tokens, GitLab CI/CD tokens, and dozens of other types of secrets.

READ MORE

TOP RELATED ARTICLES

Grandoreiro Malware and BTMOB RAT Campaigns Target Windows and Android Users

KnowledgeDeliver LMS Flaw Exploited to Deploy Godzilla and Cobalt Strike

Ghost CMS CVE-2026-26980 Exploited to Hijack 700+ Sites for ClickFix Attacks

Geo-Politics

NEWS FROM AROUND THE WORLD

Iranian Hackers Deploy MiniFast and MiniJunk V2 via Phishing and SEO Poisoning

The Iranian state-sponsored threat actor known as Nimbus Manticore (aka Screening Serpens and UNC1549) has been attributed to a fresh campaign using lures impersonating organizations in the aviation and software sectors across the U.S., Europe, and the Middle East following the joint U.S.-Israeli military campaign against the country in late February 2026.

The activity, besides embracing previously undocumented techniques and enhanced capabilities, is characterized by the use of a new backdoor codenamed MiniFast (aka MiniUpdate) that appears to have been developed with assistance using artificial intelligence (AI), Check Point said in an analysis published last week.

Affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC), Nimbus Manticore is best known for targeting defense, aviation, and telecommunication sectors using career-themed phishing lures. These campaigns have also been codenamed the Iranian Dream Job, owing to tactical similarities with Operation Dream Job, a long-running threat cluster backed by North Korea.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Romanian Hacker Sentenced to Prison in US for Selling Access to State Network

Latin American Cybercriminals Hoover Up Government Data

China's Webworm Uses Discord, Microsoft Graphs to Hack EU Governments

Breaches

SECURITY BREACHES THIS WEEK

266,000 Affected by Data Breach at Radiology Associates of Richmond

According to the healthcare organization's incident notice, the data breach occurred on or about July 25, 2025, when hackers accessed its internal systems. RAR did not say when the intrusion was discovered, but said that it worked with external cybersecurity experts to contain the attack and investigate its scope. "After an extensive forensic investigation and manual document review, RAR's investigation concluded on or about April 6, 2026, that files containing protected health information pertaining to a limited number of individuals were acquired in an unauthorized manner as a result of the incident," the organization says.
On May 21, RAR started sending notification letters to the potentially impacted individuals. According to the organization's filing with the Maine Attorney General's Office, 266,183 people are receiving such letters.

READ MORE

OTHER SECURITY BREACHES

Lithuania Suspects Foreign Involvement in Data Leak of Over 600,000 National Register Entries

Oncology Institute Discloses Data Breach

185,000 Likely Impacted by 7-Eleven Data Breach

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-45659 - Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.

CVSS SCORE 8.8

CVE-2026-45498 - Microsoft Defender Denial of Service Vulnerability

CVSS SCORE 7.5

LAST WEEKS RECAP

CVE-2026-20223: Tracked as CVE-2026-20223 (CVSS score: 10.0), the vulnerability arises from insufficient validation and authentication when accessing REST API endpoints.
CVSS Score: (10.0)

CVE-2026-45585: Microsoft Releases Mitigation for YellowKey BitLocker Bypass CVE-2026-45585 Exploit
CVSS Score: (6.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

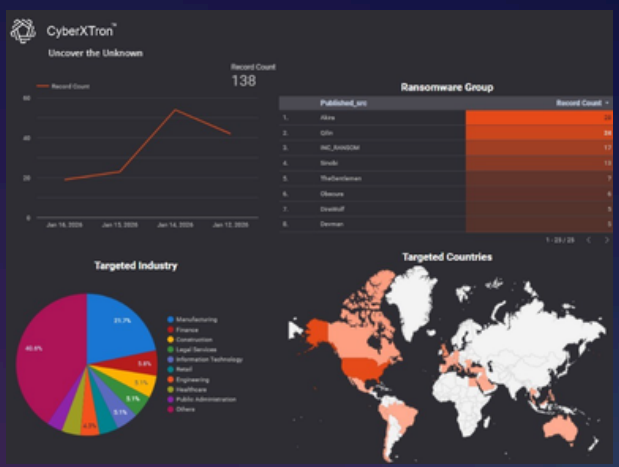
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

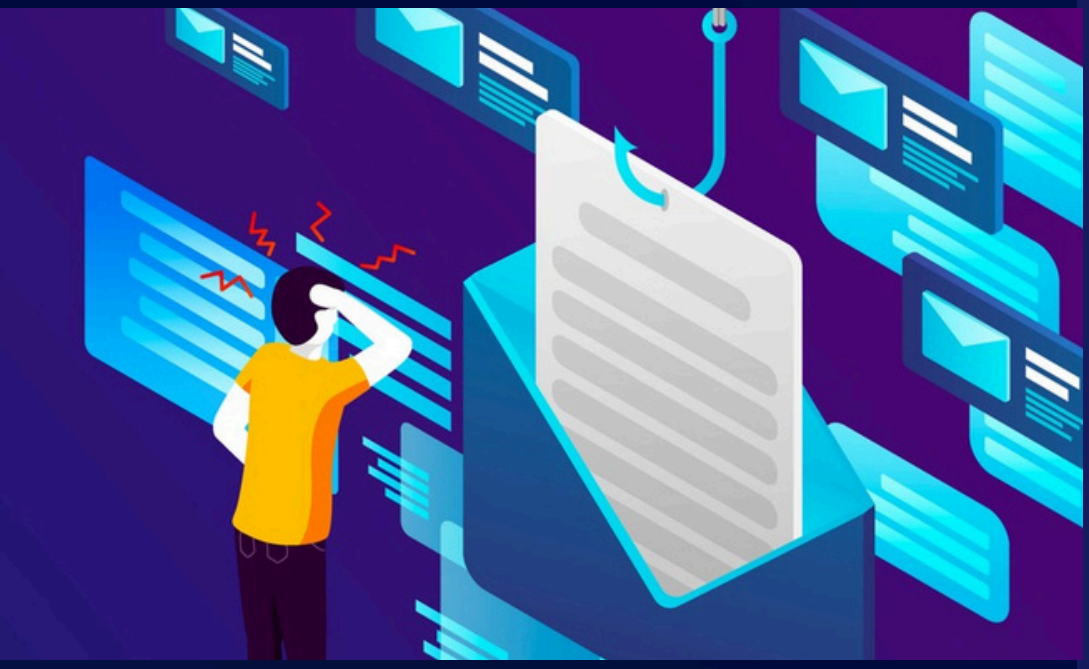
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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 warns of Kali365 phishing service targeting Microsoft 365 accounts

The FBI is warning about the Kali365 phishing-as-a-service platform (PhaaS) that is used to hijack Microsoft 365 accounts by abusing OAuth device code authentication to steal session tokens and bypass multi-factor authentication (MFA).

According to the FBI PSA, Kali365 first emerged in April 2026 and is distributed via Telegram channels for cybercriminals seeking an easier way to compromise Microsoft 365 accounts without stealing passwords or intercepting MFA codes.

The platform uses device code phishing, an increasingly popular method that abuses Microsoft's legitimate OAuth 2.0 Device Authorization grant flow to gain access to Microsoft Entra and Microsoft 365 accounts.

READ MORE

OTHER PHISHING ARTICLES

CERT-In Recommends 12-Hour Patching for Internet-Facing Flaws Amid AI-Assisted Attacks

FBI warns of in-person data theft attacks from extortion gang

Linux Flaws, Defender 0-Days, Router Botnets, and Supply Chain Chaos