

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS
~~NEWS~~
PHISHING

MARCH 2026 - VOL.1

The News

IN THE NEWS THIS WEEK



Microsoft warns of AI agent risks in Cyber Pulse brief

Microsoft has launched Cyber Pulse, a digital briefing for business leaders. Its first edition focuses on the security and governance challenges emerging as organisations deploy AI agents at scale.

The briefing highlights growth in unsanctioned agents. It notes that some agents are approved by IT and others are not, and that this mix creates compliance and operational challenges.

The document links the spread of unsanctioned tools to workforce behaviour, citing a multinational survey of more than 1,700 data security professionals commissioned by Microsoft from Hypothesis Group. It found that 29% of employees have already used unsanctioned AI agents for work tasks.

The briefing points to security scenarios it says are already appearing in the field and in internal testing. Microsoft's Defender team recently identified a fraudulent campaign involving multiple actors using an AI attack technique it calls "memory poisoning", which it says manipulates an AI assistant's memory persistently and influences future responses.

READ MORE >

OTHER NEWS HIGHLIGHTS

[Attackers Relying More on AI, Inexpensive Components in Campaigns, HP Says](#)

[Bug in Google's Gemini AI Panel Opens Door to Hijacking](#)

[Critical OpenClaw Vulnerability Exposes AI Agent Risks](#)

The News

TOP OF THE NEWS THIS WEEK



Cisco warns of max severity Secure FMC flaws giving root access

Cisco has released security updates to patch two maximum-severity vulnerabilities in its Secure Firewall Management Center (FMC) software. Secure FMC is a web or SSH-based interface for admins to manage Cisco firewalls and configure application control, intrusion prevention, URL filtering, and advanced malware protection.

Both vulnerabilities can be exploited remotely by unauthenticated attackers: the authentication bypass flaw (CVE-2026-20079) allows attackers to gain root access to the underlying operating system, while the remote code execution (RCE) vulnerability (CVE-2026-20131) lets them execute arbitrary Java code as root on unpatched devices.

While they both affect Cisco Secure FMC Software, CVE-2026-20131 also affects Cisco Security Cloud Control (SCC) Firewall Management, a cloud-based security policy manager that simplifies policy across Cisco firewalls and other devices.

[READ MORE >](#)

TOP RELATED ARTICLES

[Coruna iOS Exploit Kit Uses 23 Exploits Across Five Chains Targeting iOS 13-17.2.1](#)

[Cisco flags more SD-WAN flaws as actively exploited in attacks](#)

[Fake Google Security site uses PWA app to steal credentials, MFA codes](#)

Geo-Politics

NEWS FROM AROUND THE WORLD



Iranian Strikes on Amazon Data Centers Highlight Industry's Vulnerability to Physical Disasters

Damage to three Amazon Web Services facilities in the Middle East from Iranian drone strikes highlights the rapid growth of data centers in the region, as well as the industry's vulnerability to conflict.

The company's cloud computing division, Amazon Web Services, said late Monday that two data centers in the United Arab Emirates were "directly struck" and another facility in Bahrain was also damaged after a drone landed nearby.

"These strikes have caused structural damage, disrupted power delivery to our infrastructure, and in some cases required fire suppression activities that resulted in additional water damage," AWS said in an [update](#) on its online dashboard.

The company advised customers using servers in the Middle East to migrate to other regions, and direct online traffic away from the UAE and Bahrain.

[READ MORE >](#)

HIGHLIGHTS FROM AROUND THE WORLD

[Hackers Weaponize Claude Code in Mexican Government Cyberattack](#)

[Expect Iran to Launch Cyber-Attacks Globally, Warns Google Head of Threat Intel](#)

[149 Hacktivist DDoS Attacks Hit 110 Organizations in 16 Countries After Middle East Conflict](#)

Breaches

SECURITY BREACHES THIS WEEK



OTHER SECURITY BREACHES

[Madison Square Garden Data Breach Confirmed Months After Hacker Attack](#)

[1.2 Million Affected by University of Hawaii Cancer Center Data Breach](#)

[Canadian Tire Data Breach Impacts 38 Million Accounts](#)

LexisNexis confirms data breach as hackers leak stolen files

American data analytics company LexisNexis Legal & Professional has confirmed to BleepingComputer that hackers breached its servers and accessed some customer and business information.

The company's data breach confirmation comes as a threat actor named FulcrumSec leaked 2GB of files on various underground forums and sites.

The threat actor says that on February 24 they gained access to the company's AWS infrastructure by exploiting the React2Shell vulnerability in an unpatched React frontend app.

READ MORE >

Vulnerabilities

VULNERABILITIES & EXPLOITS



[CVE-2026-21385: Qualcomm Multiple Chipsets Memory Corruption Vulnerability](#)

CVSS SCORE 7.8

[CVE-2026-20079: Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability](#)

CVSS SCORE 10.0

[CVE-2026-20131: Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability](#)

CVSS SCORE 10.0

LAST WEEKS RECAP

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

[CCVE-2026-3061: Out of bounds read in Google Chrome](#)
[CVSS Score: \(9.1\)](#)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS



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.



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

Phishing

PHISHING NEWS THIS WEEK



OTHER PHISHING ARTICLES

[LastPass Warns of New Phishing Campaign](#)

[Russian hackers deploy new malware in phishing campaign targeting Ukraine](#)

[Starkiller Phishing Suite Uses AitM Reverse Proxy to Bypass Multi-Factor Authentication](#)

Tycoon 2FA Phishing Platform Dismantled in Global Takedown

Tycoon 2FA is a subscription-based platform that enables threat actors to impersonate users, create phishing pages, and bypass multi-factor authentication (MFA). It has allowed malicious hackers to intercept authentication sessions and gain access to targeted email and cloud accounts without triggering alerts.

“Tycoon 2FA combined convincing phishing templates, realistic landing pages, and real-time capture of credentials and authentication codes into an easy-to-use package that scaled quickly. By lowering the technical barrier to entry, it allowed criminals with limited expertise to run sophisticated impersonation campaigns,” Microsoft said.

According to the tech giant, Tycoon 2FA accounted for roughly 62% of the phishing attempts it blocked last year. The platform had been used to send out tens of millions of phishing emails to 500,000 organizations every month.

“Despite extensive defenses, the service is linked to an estimated 96,000 distinct phishing victims worldwide since 2023, including more than 55,000 Microsoft customers,” Microsoft said.

READ MORE >