SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

July 2026 - VOL.3

The News

IN THE NEWS THIS WEEK

Firefox, Chrome, Adobe, and VMware Updates Fix Multiple Critical Security Flaws

Mozilla has released updates to address two critical flaws in Firefox for which it warned that exploit code has been published.

The vulnerabilities are listed below -

- CVE-2026-15718, an invalid pointer in the JavaScript: WebAssembly component
- CVE-2026-15719, a site isolation in the DOM: Navigation component

"We are aware that exploit code for this is public, however we are not aware of any attacks in the wild abusing this flaw," Mozilla said in an advisory. Both vulnerabilities have been addressed in Firefox version 152.0.6.

The release comes as Google shipped fixes for 15 security flaws, including two critical use-after-free bugs in Ozone (CVE-2026-15764 and CVE-2026-15765), a cross-platform abstraction layer that allows the browser to interact natively with various display servers and windowing systems. It supports Linux, ChromeOS, and Fuchsia.

READ MORE

OTHER NEWS HIGHLIGHTS

Zoom Patches Critical Windows Flaw That Could Enable Account Takeover

Cursor Flaw Lets Malicious Cloned Repositories Trigger Windows Code Execution

SAP Patches CVSS 9.9 NetWeaver ABAP Flaw That Could Expose or Modify Data

The News

TOP OF THE NEWS THIS WEEK

Researcher Drops New Windows Zero-Day PoC Hours After Microsoft Patch Tuesday

Security researcher Chaotic Eclipse (aka Nightmare-Eclipse) has released a new proof-of-concept (PoC) exploit called LegacyHive.

It has been described as a Windows User Profile Service arbitrary hive load elevation of privileges vulnerability. The Windows User Profile Service, also referred to as ProfSvc, is a core system component that manages user accounts and environments.

"The PoC requires another standard user credential and a third username (which can be an administrator account)," Chaotic Eclipse said. "If the PoC is successful, it will end up mounting the target user hive in the current user classes root."

The researcher said the exploit was stripped down to prevent public exploitation, adding the original exploit did not require additional user credentials and was not limited to the "usrclass.dat" hive.

"Any hive could be loaded using this vulnerability, but you would need some brain cells to make the PoC do it," the researcher noted.

READ MORE

TOP RELATED ARTICLES

Microsoft Patches Record 622 Flaws, Including Two Zero-Days Under Active Attack

Researchers Say Claude for Chrome Flaw Lets Rogue Extensions Trigger Gmail Reads

11 Old Microsoft-Signed Linux UEFI Shims Could Let Attackers Bypass Secure Boot

Geo-Politics

NEWS FROM AROUND THE WORLD

U.S. Sanctions First VPN Service and Malware Cryptor Seller Over Ransomware Support

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has designated two individuals and a VPN service provider for enabling ransomware actors' and other cybercriminals' malicious activities, including ransomware attacks against Americans.

The VPN, named First VPN Service (1VPNS), has been accused of offering its tools to ransomware groups, along with its 45-year-old Ukrainian administrator, Dmytro Rashevskyi. The department has also sanctioned Yegeniy Vladimirovich Silayev, a Belarusian national, for selling cryptors to help conceal ransomware and other malware as safe programs to avoid being detected by security tools.

First VPN was dismantled in May 2026 as part of a joint law enforcement operation by European and North American authorities for assisting criminal actors to obscure the origins of ransomware attacks, data theft, scanning, and denial-of-service attacks. The service had been operational since 2014, advertising that it neither keeps a log of users' identities or activities nor cooperates with law enforcement to tackle illegal activity originating from servers it rents to customers.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Russian cyber-attacks and destabilising activities: Council sanctions nine individuals and four entities

Three Russian Nationals and Two Companies Indicted for International Cybercrimes Resulting in More Than $62M in Victim Losses

North Korea Expands 'Hacking Control Tower' Behind 7.7 DDoS Attack and Kim Jong-nam Assassination

Breaches

SECURITY BREACHES THIS WEEK

Lidl discloses online shop breach after service provider hack

German discount supermarket chain Lidl notified customers in Germany, Belgium, and the Netherlands that attackers stole their personal information in a breach at a service provider.

Lidl, owned by Schwarz Group, the largest food retailer in Europe, has over 376,000 employees and operates 12,000 stores across Europe and the United States.

The discount giant notified affected customers of the incident over email last week and published separate notifications on its support websites in Belgium and the Netherlands.

As detailed in these alerts, the breach was discovered last week, with attackers stealing data from customers who used Lidl's online shop.

"Despite high IT security standards, unknown individuals briefly gained access to a separately stored file containing customer data, and part of the data was stolen from it. The online shop's system itself was not affected," the company said.

READ MORE

OTHER SECURITY BREACHES

Synopsys Finds No Evidence of Data Breach Amid Bosch Hack Claims

Centers Laboratory Data Breach Affects 540,000 Individuals

Police Disrupt a €140M Cyber Fraud Ring in Spain

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-44747 - SAP NetWeaver Application Server ABAP allows an authenticated attacker to leverage logical errors in memory management to cause a memory corruption that could lead to unauthorized data access, modification, or system unavailability.

CVSS SCORE 9.9

CVE-2026-55040 - Weak authentication in Microsoft Office SharePoint allows an unauthorized attacker to bypass a security feature over a network.

CVSS SCORE 9.1

LAST WEEKS RECAP

CVE-2026-55255 - Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.1, an Insecure Direct Object Reference (IDOR) vulnerability in /api/v1/responses endpoint allows an authenticated attacker to execute any flow belonging to another user by specifying the victim's flow ID in the request. This vulnerability is fixed in 1.9.1.

CVSS Score: (8.8)

CVE-2026-50656 - Microsoft is aware of an elevation of privilege in the Microsoft Malware Protection Engine

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

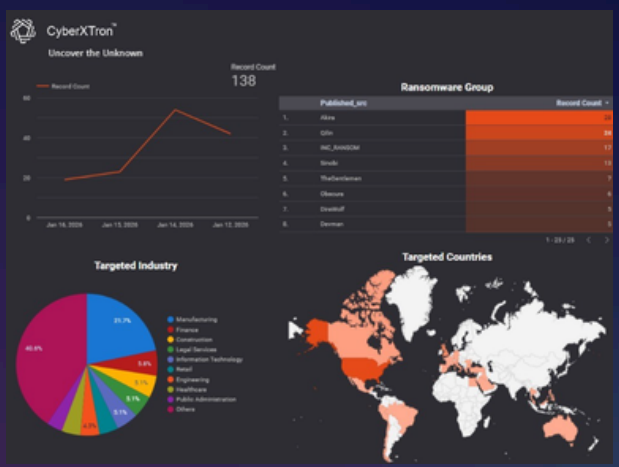
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

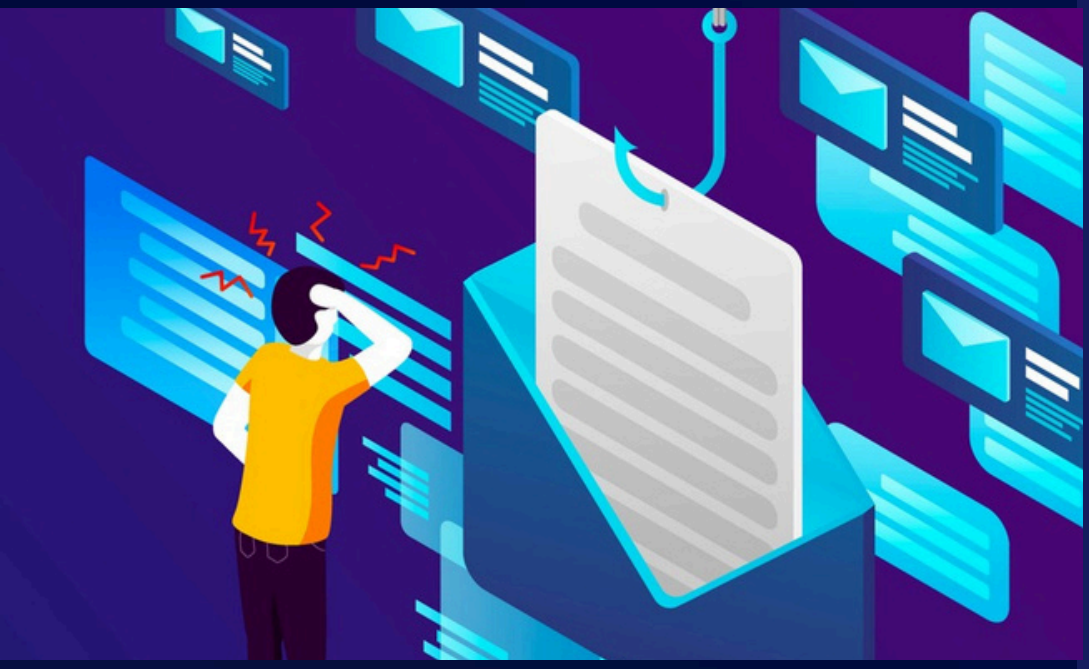
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Forg365 PhaaS Targets Microsoft 365 with Device Code and AitM Session Theft

A new phishing-as-a-service (PhaaS) operation called Forg365 is using a combination of device code phishing, adversary-in-the-middle (AitM) tactics, antibot evasion, artificial intelligence (AI)-assisted lure creation, and post-compromise mailbox operations targeting Microsoft 365 accounts.

Distributed via Telegram and costing $400 a month (or $3,800 per year), attack chains leverage phishing lures that make use of legitimate email delivery infrastructure, such as Amazon Simple Email Service (Amazon SES) and Twilio SendGrid, to imitate a redirection chain that blends into regular email traffic before it ends in Forg365-controlled domains.

"The panel exposes a mature operator workflow: accounts, links, invitations, OAuth app configuration, redirect links, SVG generation, campaign sending, SMTP profiles, SMTP rotation, AI email generation, token vaulting, account intelligence, keyword alerts, viewer links, and browser-extension support," ZeroBEC said.

READ MORE

OTHER PHISHING ARTICLES

Meta's New AI Image Tool Lets Others Use Your Public Instagram Photos in AI Images

CrashStealer macOS Malware Uses Notarized Dropper to Pass Gatekeeper Checks

OAuth Client ID Spoofing Lets Attackers Validate Stolen Microsoft Entra Credentials