SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

July 2026 - VOL.4

The News

IN THE NEWS THIS WEEK

WP2Shell WordPress Vulnerabilities Exploited in the Wild

Two newly patched WordPress vulnerabilities are being exploited in the wild, with attacks beginning shortly after they came to light.

The vulnerabilities have been dubbed WP2Shell and they are officially tracked as CVE-2026-60137 and CVE-2026-63030.

According to Searchlight Cyber, whose researchers discovered the flaws, WordPress versions 6.9.0 through 6.9.4 and 7.0.0 through 7.0.1 are affected.

“The attack has no preconditions and can be exploited by an anonymous user in a stock install of WordPress with no plugins,” the security firm warned.

WordPress announced patches on Friday with the release of versions 6.9.5 and 7.0.2.

“Due to the severity, the WordPress.org team have enabled forced updates via the auto-update system for sites running affected versions,” WordPress developers said.

READ MORE

OTHER NEWS HIGHLIGHTS

Adobe Acrobat Extension Flaw Let Malicious Sites Read WhatsApp Web Data

Hackers Exploit Windmill Flaw to Read Arbitrary Server Files Without Authentication

Microsoft Azure DevOps MCP Flaw Lets Hidden PR Comments Hijack AI Review Agents

The News

TOP OF THE NEWS THIS WEEK

Ubuntu snap-confine Flaw Could Give Local Users Root on Default Desktop Installs

Cybersecurity researchers have disclosed details of a new local privilege escalation (LPE) vulnerability in snap-confine that an unprivileged user can trigger to obtain root access and gain complete control of a target environment.

The high-severity flaw, tracked as CVE-2026-8933 (CVSS score: 7.8), impacts default installations of Ubuntu Desktop 24.04, 25.10, and 26.04. The disclosure comes as 442 security flaws in Linux have been publicized over the past three days.

"The issue stems from a security hardening change that inadvertently introduced a race condition during sandbox initialization," Saeed Abbasi, head of Threat Research Unit (TRU) and director of product at Qualys, said.

Snap-confine is a program used internally by snapd to construct the execution environment for snap applications. Snapd is the background service or daemon that manages snap packages on Linux systems. Snaps are nothing but a software packaging format devised by Canonical that allows an application to run securely in an isolated sandbox across most Linux distributions.

READ MORE

TOP RELATED ARTICLES

Apple Fixes Hide My Email Bug That Exposed Real Addresses in Mail Logs

Check Point Patches Exploited SmartConsole Flaw Allowing Full Admin Access

OpenAI Says Its AI Models Escaped Sandbox, Targeted Hugging Face to Cheat Benchmark

Geo-Politics

NEWS FROM AROUND THE WORLD

Russian Intelligence Hacks IP Cameras to Spy on Military Logistics Across NATO States and Ukraine

At least one Russian intelligence service is systematically hijacking internet-connected security cameras across Europe and Ukraine, using the feeds to watch military transport routes, weapons shipments bound for Kyiv, and the locations of Ukrainian troops.

That is the finding of a cybersecurity advisory published July 10 by the AIVD and MIVD, the Netherlands' civilian and military intelligence services, which describe the operation as ongoing.

In Ukraine, the surveillance has not stayed passive. Camera access there has been "used in attempts to neutralise Ukrainian military personnel" and destroy their equipment, the services say, turning an exposed roadside or business camera into a targeting aid.

Across EU and NATO states, the services add, the same camera access is also collecting military intelligence that has nothing to do with the war.

Getting in is rarely the hard part. The operators scan the internet for exposed devices, fingerprint IP cameras by brand, and walk into the ones still running default passwords, obsolete firmware, and factory settings nobody changed.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Russian-Speaking Hacker Uses Google Gemini CLI to Control Botnet of Eight Dental Clinic PCs

Fake Coding Tests Deliver OtterCookie-Aligned Malware Hidden in SVG Flag Images

Armenia Detains Russian Tourist on U.S. Warrant for REvil Hacker, Lawyers Say Wrong Man

Breaches

SECURITY BREACHES THIS WEEK

Ransomware Group Threatening to Leak Data Stolen From Coca-Cola's Fairlife

The Anubis ransomware group has taken credit for the disruptive attack on Coca-Cola subsidiary Fairlife and is threatening to leak stolen data unless a ransom is paid.

Coca-Cola revealed last week that production at dairy company Fairlife had been suspended due to a ransomware attack. The full impact of the incident was still being assessed at the time of disclosure.

The Anubis group listed Coca-Cola and Fairlife on its leak website on July 20. The cybercriminals claimed to have "locked" servers – this likely means they have encrypted files – and exfiltrated 1 TB of "confidential data".

The hackers said they can help the company restore its systems within hours if it agrees to pay a ransom. Coca-Cola has been given a week to pay up, or the stolen data will be leaked.

READ MORE

OTHER SECURITY BREACHES

Suno, Paidwork Data Breaches Affect Tens of Millions of Accounts

Clover Health Investments Discloses Data Breach

Estée Lauder Discloses Impact From Oracle EBS Zero-Day Hack

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-63030 - WordPress 6.9.x before 6.9.5 and 7.0.x before 7.0.2 is affected by a REST API batch endpoint route confusion issue which, combined with the author__not_in WP_Query SQL Injection (CVE-2026-60137), could allow an attacker to perform SQL Injection and achieve Remote Code Execution.

CVSS SCORE 9.8

CVE-2026-15409 - A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location.

CVSS SCORE 10.0

LAST WEEKS RECAP

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)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

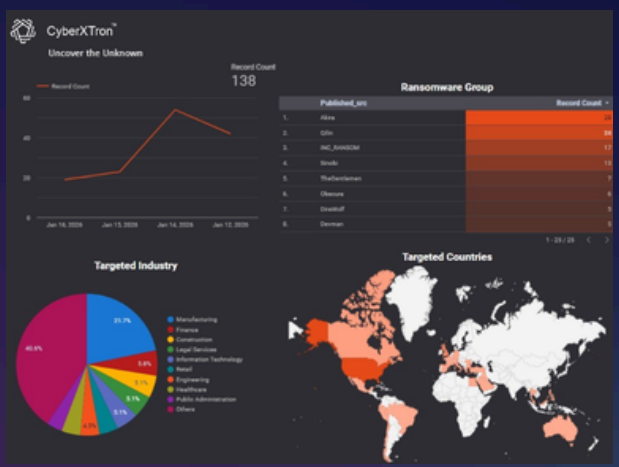
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

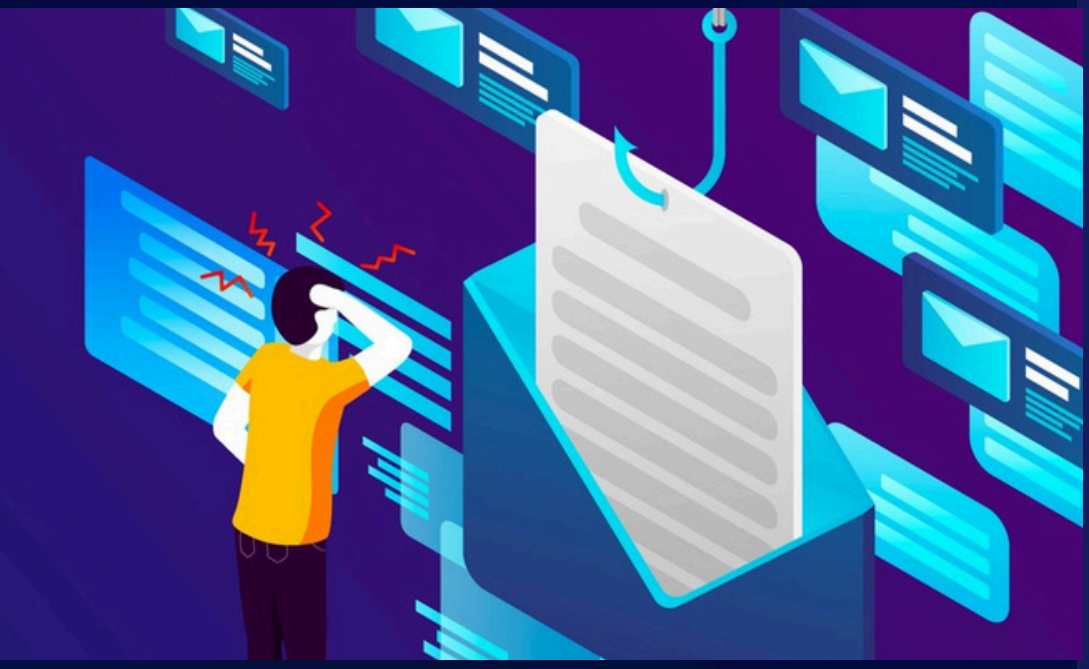
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Police Dismantle Kratos Phishing Kit Built to Steal Microsoft 365 Sessions and Bypass MFA

German and US law enforcement have taken down the core infrastructure of Kratos, described by German investigators as one of the world's most widely used criminal phishing kits, and Indonesian authorities arrested the man they say developed and ran it.

In a joint announcement on Monday, the Frankfurt public prosecutor's cybercrime unit (ZIT) and Germany's Federal Criminal Police Office (BKA) said they pulled more than 200 servers offline. Investigators estimate roughly 1,800 paying customers used Kratos to run about 15,000 phishing campaigns a month.

Kratos harvested more than passwords. The kit was designed to steal the session cookie along with the login, and that cookie is enough to walk past two-factor authentication into the account as the user, the BKA said.

READ MORE

OTHER PHISHING ARTICLES

FakeGit Campaign Uses 7,600 GitHub Repositories to Spread SmartLoader Malware

Exposed Server Reveals AI-Assisted Phishing Toolkit Behind WebDAV Malware Campaign

GoldenEyeDog Subgroup Linked to DigiCert Breach and Code-Signing Certificate Theft