SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

July 2026 - VOL.2

The News

IN THE NEWS THIS WEEK

Unpatched Flaws Disclosed in Filesystem Bundled Into Millions of Embedded Devices

Security firm runZero has disclosed seven vulnerabilities in FatFs, a small filesystem library that lets a device read and write the FAT and exFAT formats used on USB drives and SD cards.

The flaws matter because FatFs is nearly everywhere. It ships inside the firmware that runs security cameras, drones, industrial controllers, hardware crypto wallets, and other devices built on real-time operating systems.

On the worst-affected systems, an attacker who gets a booby-trapped USB drive, SD card, or update file onto a device can corrupt its memory and run their own code.

Many embedded devices lack the memory protections found on phones and desktops, which is why runZero says "any physical access leads to a jailbreak." A public kiosk, a camera with an SD slot, an ATM, or a voting machine with a USB port should not hand over full control after a moment of physical access, but here it can.

READ MORE

OTHER NEWS HIGHLIGHTS

Zscaler ThreatLabz 2026 VPN Risk Report with Cybersecurity Insiders

SkillCloak Lets Malicious AI Agent Skills Evade Static Scanners with Self-Extracting Packing

Opera GX Flaw Let Malicious Sites Auto-Install Mods to Steal Data From Visited Pages

The News

TOP OF THE NEWS THIS WEEK

New Java-Based QuimaRAT MaaS Built to Run on Windows, Linux, and macOS

Cybersecurity researchers have flagged a novel Java-based remote access trojan (RAT) called QuimaRAT that's capable of targeting Windows, Linux, and macOS environments.

According to LevelBlue, the cross-platform malware is advertised under a malware-as-a-service (MaaS) model, costing anywhere between $150 for one month to $1,200 for lifetime access. Other subscription tiers include $300 for three months, $500 for six months, and $700 for twelve months.

"Built around a modular architecture, the RAT supports dynamic capability expansion through encrypted plugins that can be delivered, loaded, unloaded, and updated directly from its command-and-control (C2) infrastructure," the cybersecurity company said in an analysis of the malware.

The malware author also advertises a builder capable of generating multiple output formats, including JAR, EXE, APP, SH, BAT, and VBS, indicating an attempt to help prospective customers package the client tailored for different environments and delivery scenarios.

READ MORE

TOP RELATED ARTICLES

New TrojPix Attack Leaks Data From Air-Gapped Systems via Video Cable Emissions

Threat Actors Probe Gitea Docker Flaw CVE-2026-20896 13 Days After Disclosure

BeyondTrust Patches Critical Auth Bypass Flaws in Remote Support and PRA

Geo-Politics

NEWS FROM AROUND THE WORLD

Suspected China-Nexus Hackers Use Fake Indian Tax Filing Utility to Deploy DcRAT

A suspected China-nexus threat activity cluster has been observed targeting Indian taxpayers, tax professionals, and corporate finance teams to deliver a remote access trojan designed to steal sensitive data from compromised hosts.

The multi-stage campaign, codenamed Operation DragonReturn by Seqrite Labs, involves sending spear-phishing emails impersonating the Income Tax Department of India. It was first observed on May 18, 2026. The activity, per the cybersecurity company, coincides with the annual income tax filing season in the country.

"It is not opportunistic – the precision of the lure document, the use of real legal citations, bilingual content, and active payload rotation indicate a deliberate, resourced, and sustained threat operation focused exclusively on the Indian taxpayer ecosystem," security researchers Dixit Panchal and Soumen Burma said.

The end goal of the campaign is assessed to be the deployment of malware for financial gain or sensitive data theft.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

North Korean Hackers Publish 108 Malicious Packages and Extensions in PolinRider Campaign

North Korea-Linked npm Packages Mimic Rollup Polyfills to Steal Developer Secrets

Suspected China-Aligned Hackers Exploit Roundcube Flaws Against Universities

Breaches

SECURITY BREACHES THIS WEEK

Accenture Confirms Data Breach After Hacker Claims Source Code Theft

Professional services giant Accenture confirmed a data breach after a hacker claimed the theft of internal source code from the company.

The incident came to light this week, when a threat actor boasted on the hacker forum PwnForums about compromising Accenture and stealing 35 gigabytes of data.

According to the hacker, the information, including Azure access keys and tokens, configuration files, RSA and SSH keys, and source code, was exfiltrated from Accenture earlier this month.

The threat actor, who was trying to sell the allegedly stolen data, posted as proof-of-possession a screenshot depicting a private Azure DevOps repository apparently hosted on an accenture.com domain.

Responding to a SecurityWeek inquiry, Accenture confirmed the attack, but refrained from providing additional details on the matter.

“We are aware of this isolated matter, and we have remediated its source. There is no impact to Accenture operations and service delivery,” an Accenture spokesperson said.

READ MORE

OTHER SECURITY BREACHES

Cybercrime Medtronic Data Breach Impacts 3.8 Million People

Lone Attacker Uses AI to Breach AWS Cloud Environment in 72 Hours

CitrixBleed-ing Again? NetScaler Vulnerability Under Attack

Vulnerabilities

VULNERABILITIES & EXPLOITS

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

LAST WEEKS RECAP

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 ~~valid~~ation 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)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

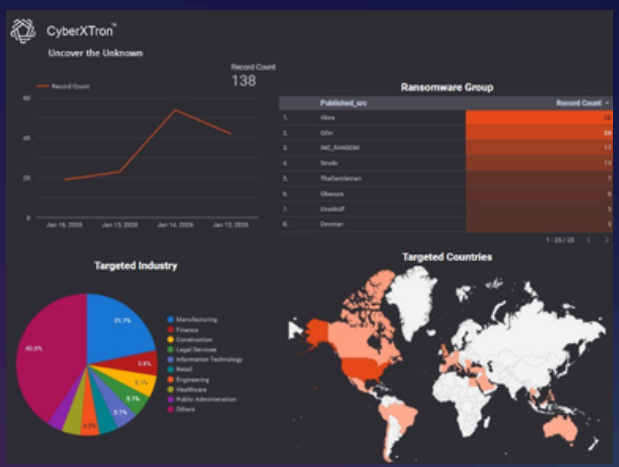
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

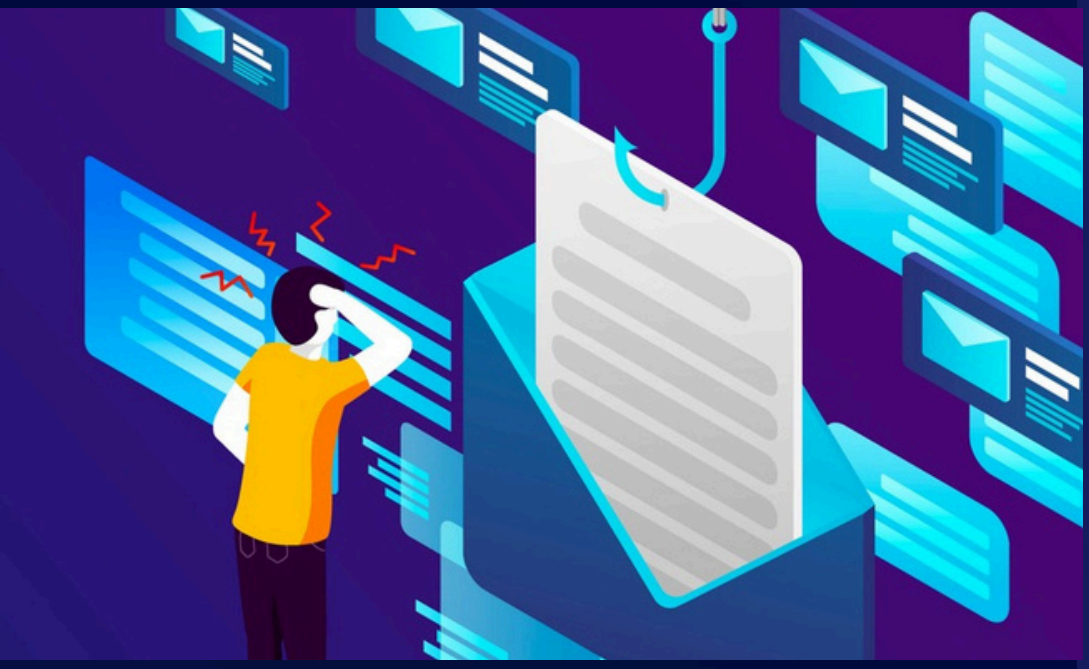
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



RedWing Android Spyware Sold as a Service on Telegram

A new Android spyware strain has been observed being rented out to criminals through Telegram, giving even low-skilled attackers the tools to hijack phones and steal banking credentials, researchers have found.

Zimperium's zLabs named the malware RedWing and described it as a polished malware-as-a-service (MaaS) operation with seller documentation, tutorial videos and a subscription model.

The firm linked it to Russian threat actors and said many of its samples currently slip past conventional security tools. What set RedWing apart was how easy it was to buy and deploy. A Telegram bot built and obfuscated the malicious APK for the customer, while a referral scheme offered discounts for spreading it further.

Operators could also generate fake app-store pages, mimicking Google Play, the Galaxy Store, AppGallery or Russia's RuStore, complete with bogus ratings and download counts to lure victims into installing it.

Once installed, RedWing walked the victim through a series of permission prompts dressed up as routine setup, coaxing them into granting the access it needed, including Android's accessibility service and control of the SMS inbox. From there, it could hide its own icon and run quietly in the background.

READ MORE

OTHER PHISHING ARTICLES

New Ghost Phishing Wave Is Breaking Traditional Email Security

SCMBANKER Malware Uses ClickFix Lures to Target Mexican Banking Users

DEBULL Tooling Abuses Microsoft Device-Code Flow to Target M365 Accounts