

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

MAY 2026 - VOL.1

The News

IN THE NEWS THIS WEEK



Researchers Uncover 73 Fake VS Code Extensions Delivering GlassWorm v2 Malware

Cybersecurity researchers have flagged dozens of Microsoft Visual Studio Code (VS Code) extensions on the Open VSX repository that are linked to a persistent information-stealing campaign dubbed GlassWorm.

The cluster of 73 extensions has been identified as cloned versions of their legitimate counterparts. Of these, six have been confirmed to be malicious, with the remaining acting as seemingly harmless sleeper packages to get users to download them and build trust, before their true intent is manifested through a subsequent update.

All the extensions were published at the start of the month. In total, more than 320 artifacts have been identified since December 21, 2025.

The disclosure comes as the threat actors behind the campaign are actively evolving their modus operandi, pivoting to sleeper packages and transitive dependencies to evade detection, while simultaneously using Zig-based droppers to deploy a secondary VSIX extension hosted on GitHub that can infect all integrated development environments (IDEs) on a developer's machine.

READ MORE >

OTHER NEWS HIGHLIGHTS

[Tropic Trooper Uses Trojanized SumatraPDF and GitHub to Deploy AdaptixC2](#)

[26 FakeWallet Apps Found on Apple App Store Targeting Crypto Seed Phrases](#)

[Feuding Ransomware Groups Leak Each Other's Data](#)

The News

TOP OF THE NEWS THIS WEEK



Firestarter malware survives Cisco firewall updates, security patches

Cybersecurity agencies in the U.S. and U.K. are warning about a custom malware called Firestarter persisting on Cisco Firepower and Secure Firewall devices running Adaptive Security Appliance (ASA) or Firepower Threat Defense (FTD) software.

The backdoor has been attributed to a threat actor that Cisco Talos tracks internally as UAT-4356, known for cyberespionage campaigns, including ArcaneDoor.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.K. National Cyber Security Center (NCSC) believe that the adversary obtained initial access by exploiting a missing authorization issue (CVE-2025-20333) and/or a buffer overflow bug (CVE-2025-20362).

The vendor “strongly recommends reimaging and upgrading the device using the fixed releases,” which covers both compromised and non-compromised cases. To determine a compromise, administrators should run the ‘show kernel process | include lina_cs’ command. For any resulting output, the device should be considered compromised.

[READ MORE >](#)

TOP RELATED ARTICLES

[UNC6692 Combines Social Engineering, Malware, Cloud Abuse](#)

[PyPI package with 1.1M monthly downloads hacked to push infostealer](#)

[New Python Backdoor Uses Tunneling Service to Steal Browser and Cloud Credentials](#)

Geo-Politics

NEWS FROM AROUND THE WORLD



China-Backed Hackers Are Industrializing Botnets

This week, the UK's National Cyber Security Centre (NCSC-UK), in concert with cybersecurity agencies in the US and other countries, warned of China-nexus threat actors increasingly using covert networks of compromised routers, IoT, and smart devices to facilitate attacks against US organizations.

Evidence suggests that Chinese information security companies are systematically creating and maintaining many of these botnets, which are often composed of small office and home office (SOHO) routers.

Chinese threat groups like Flax Typhoon and Volt Typhoon have then been using these networks to conduct reconnaissance, deliver and communicate with malware, and exfiltrate data in a "low-cost, low-risk, deniable way," the joint advisory noted.

"They can also be used for general deniable Internet browsing, allowing threat actors to research exploitation techniques, new TTPs, and their victims, without attribution," the agencies said. "Some covert networks are also used by legitimate customers to browse the Internet, making it challenging to attribute malicious activity."

READ MORE >

HIGHLIGHTS FROM AROUND THE WORLD

[North Korea's Lazarus Targets macOS Users via ClickFix](#)

[PhantomCore Exploits TrueConf Vulnerabilities to Breach Russian Networks](#)

[BlueNoroff Uses Fake Zoom Calls to Turn Victims Into Attack Lures](#)

Breaches

SECURITY BREACHES THIS WEEK



OTHER SECURITY BREACHES

[ShinyHunters claim they have cruise giant Carnival's booty as 7.5M emails surface](#)

[ADT confirms data breach after ShinyHunters leak threat](#)

[American utility firm Itron discloses breach of internal IT network](#)

Medtronic confirms breach after hackers claim 9 million records theft

Medical device giant Medtronic disclosed last week that hackers breached its network and accessed data in "certain corporate IT systems."

The confirmation comes after the infamous data extortion group 'ShinyHunters' claimed the intrusion and the theft of more than 9 million records from the company.

Medtronic is an international medical equipment giant with 90,000 employees and operations in 150 countries. It is the largest medical device maker in the world by revenue (\$33.5 billion) and also develops healthcare technologies and therapies.

Although Medtronic did not provide additional information about the attack or its perpetrators, threat actor ShinyHunters listed the company among its victims, stating that their breach resulted in the theft "over 9 million records containing PII [personally identifiable information]."

The threat actor also claims to have compromised "terabytes of internal corporate data" and pressured the company to pay under the threat of a leak.

[READ MORE >](#)

Vulnerabilities

VULNERABILITIES & EXPLOITS



CVE-2026-3854: Github Vulnerability allows an authenticated user to obtain remote code execution with a single "git push" command.

CVSS SCORE 8.8

CVE-2026-7333: Use after free in GPU in Chrome allows for sandbox escape via a crafted HTML page.

CVSS SCORE 9.6

LAST WEEKS RECAP

CVE-2026-40372 - Improper verification of cryptographic signature in ASP.NET Core allows an unauthorized attacker to elevate privileges over a network.
CVSS Score: (9.1)

CVE-2026-34197 - Improper Input Validation, Improper Control of _____ Generation of Code ('Code Injection'), vulnerability in Apache ActiveMQ
CVSS Score: (8.8)

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



Crime crew impersonates help desk, abuses Microsoft Teams to steal your data

A previously unknown threat group using tried-and-tested social engineering tactics - Microsoft Teams chat invitations and helpdesk staff impersonation - is also using custom malware in its data-stealing attacks, according to Google's Threat Intelligence Group.

The threat hunters say they spotted a "large email campaign" in late December 2025. The attack started by spamming target organizations with an overwhelming amount of email traffic. Then someone posing as helpdesk personnel would reach out via Microsoft Teams to offer help with the email volume.

The fake helpdesk worker prompts the user to click a link that supposedly installs a local patch that prevents email spamming. This directs victims to a landing page masquerading as a "Mailbox Repair Utility" complete with a "Health Check" button that, when clicked, prompts users to authenticate using their email and password, allowing the attackers to nab them.

The phishing page then performs a fake mailbox integrity check, which keeps the victim engaged while credentials and metadata are sent to an attacker-controlled Amazon S3 bucket and staged files continue downloading onto the user's machine.

[READ MORE >](#)

OTHER PHISHING ARTICLES

[Nearly half of UK businesses pwned last year as phishing keeps doing the job like it's 2005](#)

[NASA Employees Duped in Chinese Phishing Scheme Targeting U.S. Defense Software](#)

[Germany Suspects Russia Is Behind Signal Phishing That Targeted Top Officials](#)