

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

MAY 2026 - VOL.4

The News

IN THE NEWS THIS WEEK



Microsoft Warns of Two Actively Exploited Defender Vulnerabilities

Microsoft has disclosed that a privilege escalation and a denial-of-service flaw in Defender has come under active exploitation in the wild.

The former, tracked as [CVE-2026-41091](#), is rated 7.8 on the CVSS scoring system. Successful exploitation of the flaw could allow an attacker to gain SYSTEM privileges.

"Improper link resolution before file access ('link following') in Microsoft Defender allows an authorized attacker to elevate privileges locally," Microsoft said in an advisory.

The second vulnerability under exploitation is [CVE-2026-45498](#) (CVSS score: 4.0), a denial-of-service bug impacting Defender. The two vulnerabilities have been addressed in Microsoft Defender Antimalware Platform versions 1.1.26040.8 and 4.18.26040.7, respectively.

READ MORE >

OTHER NEWS HIGHLIGHTS

[GitHub Breached — Employee Device Hack Led to Exfiltration of 3,800+ Internal Repos](#)

[The New Phishing Click: How OAuth Consent Bypasses MFA](#)

[Google accidentally exposed details of unfixed Chromium flaw](#)

The News

TOP OF THE NEWS THIS WEEK



Microsoft's Retired IE Tool MSHTA Now Being Used in Fileless Malware Attacks

An old Windows tool called MSHTA is being exploited by hackers to infect systems with malware, reveals the latest research from Bitdefender. Reportedly, this tool, which was created to work with Internet Explorer (IE), still remains active by default on Windows computers despite IE's retirement in 2022, mainly to help run older software smoothly.

Bitdefender's research, shared with Hackread.com, highlights that threat actors are actively abusing it as a Living-off-the-Land binary (LOLBIN), enabling them to carry out [fileless attacks](#). They can execute malicious

VBScript and JavaScript code directly in the computer's memory and ensure that it appears as legitimate administrative tasks.

These fileless attack chains rely on common social engineering tricks like [ClickFix](#) scams and fake software downloads. Such as, in one campaign, fake Google ads for Claude Code were used to lure victims, and in another, attackers bundled malware into pirated downloads of the movie One Battle After Another.

Typically, attackers force MSHTA to run a hidden command shell, checking specific IP addresses to execute malicious packages via Microsoft Installer.

[READ MORE >](#)

PAGE TWO | TOP OF THE NEWS THIS WEEK

TOP RELATED ARTICLES

[Apple blocked over \\$11 billion in App Store fraud in 6 years](#)

[Max severity Cisco Secure Workload flaw gives Site Admin privileges](#)

[Police seize "First VPN" service used in ransomware, data theft attacks](#)

Geo-Politics

NEWS FROM AROUND THE WORLD



Ukraine identifies infostealer operator tied to 28,000 stolen accounts

The Ukrainian cyberpolice, working in conjunction with U.S. law enforcement, has identified an 18-year-old man from Odesa suspected of running an infostealer malware operation targeting users of an online store in California.

According to the Ukrainian police, the threat actor used information-stealing malware between 2024 and 2025 to infect users' devices and steal browser sessions and account credentials.

The attacks linked to the young hacker impacted 28,000 customer accounts, of which the cybercriminals used 5,800 to make unauthorized purchases totaling about \$721,000. The malicious operation caused \$250,000 in direct losses, including chargebacks.

Infostealers are a popular type of malware that harvests sensitive data, including passwords, browser cookies, session tokens, crypto wallets, and payment information, from infected devices and sends it to cybercriminals for account theft, fraud, and resale.

[READ MORE >](#)

HIGHLIGHTS FROM AROUND THE WORLD

[INTERPOL Operation Ramz Disrupts MENA Cybercrime Networks with 201 Arrests](#)

[Showboat Linux Malware Hits Middle East Telecom with SOCKS5 Proxy Backdoor](#)

[China's Webworm Uses Discord, Microsoft Graphs to Hack EU Governments](#)

Breaches

SECURITY BREACHES THIS WEEK



OTHER SECURITY BREACHES

[Hacker Selling 340 Million OnlyFans User Records Built From Old Breaches](#)

[Verizon DBIR: AI Helped Hackers Exploit Vulnerabilities in 31% of Recent Breaches](#)

[Hackers Actively Exploit 'Nginx Rift' Vulnerability Affecting NGINX, F5 Products](#)

GitHub investigates internal repositories breach claimed by TeamPCP

GitHub is investigating a breach of its internal repositories after the TeamPCP hacker group claimed to have accessed approximately 4,000 repositories containing private code.

GitHub's cloud-based development platform is used by more than 4 million organizations (including 90% of the Fortune 100) and over 180 million developers who contribute to more than 420 million code repositories.

The company has yet to share more information about the investigation, but said it currently has no evidence that customer data stored outside its internal repositories has been affected.

"We are investigating unauthorized access to GitHub's internal repositories," GitHub told BleepingComputer when asked for further details.

"While we currently have no evidence of impact to customer information stored outside of GitHub's internal repositories (such as our customers' enterprises, organizations, and repositories), we are closely monitoring our infrastructure for follow-on activity."

[READ MORE >](#)

Vulnerabilities

VULNERABILITIES & EXPLOITS



[CVE-2026-20223: Tracked as CVE-2026-20223 \(CVSS score: 10.0\), the vulnerability arises from insufficient validation and authentication when accessing REST API endpoints.](#)

CVSS SCORE 10.0

[CVE-2026-45585: Microsoft Releases Mitigation for YellowKey BitLocker Bypass CVE-2026-45585 Exploit](#)

CVSS SCORE 6.8

LAST WEEKS RECAP

[CVE-2026-42945: NGINX buffer overflow allows attackers to achieve remote code execution or DoS](#)

CVSS Score: (8.1)

[CVE-2026-40361: Zero click use-after-free bug can be exploited for remote code execution against Microsoft Outlook users](#)
CVSS Score: (8.4)

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



Phishing Campaign Exploits Google AppSheets to Target Facebook Accounts

Researchers at Guardo Labs are tracking a major phishing campaign that abused Google AppSheet as a relay to send phishing emails. The researchers identified more than 30,000 Facebook accounts that were compromised by this campaign. Since the emails are sent from Google's legitimate infrastructure, they're much more likely to land in users' inboxes.

"Email phishing used to rely on spoofing, shady SMTP infrastructure, and just enough broken authentication to slip through the cracks," the researchers write. "This case starts from the opposite premise: the email is real, the authentication is clean, and the delivery comes through Google's own AppSheet, the no-code app builder's notification system."

In the campaign observed by Guardio, the attackers are using AppSheet notifications to send phony alerts informing users that their Facebook Business accounts will be permanently disabled for copyright violations unless they submit an appeal. The link in the email leads to a convincingly spoofed Facebook login page designed to harvest credentials and personal information.

READ MORE >

OTHER PHISHING ARTICLES

[Warning: Phishing Attacks Are Abusing the Kuse AI App](#)

[Robinhood Glitch Allowed Attackers to Send Phishing Emails to Customers](#)

[Report: The Tycoon 2FA Phishing Kit Has Evolved](#)