

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

MAY 2026 - VOL.3

The News

IN THE NEWS THIS WEEK



Microsoft May 2026 Patch Tuesday fixes 120 flaws, no zero-days

This Patch Tuesday addresses 17 "Critical" vulnerabilities, 14 of which are remote code execution, 2 are elevation of privilege, and 1 is an information disclosure flaw.

Microsoft has not disclosed any zero-day vulnerabilities in this month's Patch Tuesday. However, there are some vulnerabilities fixed today that IT and security admins should be aware of.

As part of today's updates, Microsoft has fixed numerous vulnerabilities in Microsoft Office, Word, and Excel that could lead to remote code execution.

These flaws are exploited by opening malicious files, which can result in remote code execution. As many of these can be exploited via the preview pane, it is strongly advised to update Microsoft Office as soon as possible, especially if they commonly receive attachments.

READ MORE >

OTHER NEWS HIGHLIGHTS

[After Replacing TeamPCP Malware, 'PCPJack' Steals Cloud Secrets](#)

[Adobe Patches 52 Vulnerabilities in 10 Products](#)

[Chipmaker Patch Tuesday: Intel and AMD Patch 70 Vulnerabilities](#)

The News

TOP OF THE NEWS THIS WEEK



GemStuffer Abuses 150+ RubyGems to Exfiltrate Scraped U.K. Council Portal Data

Cybersecurity researchers are calling attention to a new campaign dubbed GemStuffer that has targeted the RubyGems repository with more than 150 gems that use the registry as a data exfiltration channel rather than for malware distribution.

"The packages do not appear designed for mass developer compromise," Socket said. "Many have little or no download activity, and the payloads are repetitive, noisy, and unusually self-contained."

"Instead, the scripts fetch pages from U.K. local government democratic services portals, package the collected responses into valid .gem archives, and publish those gems back to RubyGems using hardcoded API keys."

At a high level, the campaign abuses RubyGems as a place to stage the scraped council content. It does this by fetching hard-coded U.K. council portal URLs, packaging the HTTP responses into valid .gem archives, and publishing those archives to RubyGems using embedded registry credentials.

[READ MORE >](#)

TOP RELATED ARTICLES

[Fake OpenAI Privacy Filter Repo Hits #1 on Hugging Face, Draws 244K Downloads](#)

[Hackers Used AI to Develop First Known Zero-Day 2FA Bypass for Mass Exploitation](#)

[Fortinet warns of critical RCE flaws in FortiSandbox and FortiAuthenticator](#)

Geo-Politics

NEWS FROM AROUND THE WORLD



Palo Alto Zero-Day Exploited in Campaign Bearing Hallmarks of Chinese State Hacking

In an advisory published on May 6, Palo Alto Networks informed customers about CVE-2026-0300, a vulnerability affecting the User-ID Authentication Portal of PA and VM series firewalls. The company said the flaw, which allows unauthenticated remote code execution with root privileges, had been exploited as a zero-day.

According to the company, a “likely state-sponsored” threat group tracked as CL-STA-1132 was behind the attack. First exploitation attempts were observed on April 9, but were unsuccessful. The vulnerability was successfully leveraged one week later for remote code execution and Nginx worker process shellcode injection.

The attackers deployed the open source Earthworm and ReverseSocks5 tools. The former is a network tunneling tool that enables attackers to establish a covert communications channel, while the latter allows them to bypass firewalls and NAT.

Both tools have predominantly been used by Chinese APT groups, including Volt Typhoon and APT41. Log destruction has also often been observed during attacks attributed to Chinese threat actors.

[READ MORE >](#)

HIGHLIGHTS FROM AROUND THE WORLD

[Iranian hackers targeted major South Korean electronics maker](#)

[Chinese APTs Expand Targets, Update Backdoors in Recent Campaigns](#)

[Polish Security Agency Reports ICS Breaches at Five Water Treatment Plants](#)

Breaches

SECURITY BREACHES THIS WEEK



OTHER SECURITY BREACHES

[Zara data breach exposed personal information of 197,000 people](#)

[Skoda Data Breach Hits Online Shop Customers](#)

[US bank reports itself after slinging customer data at 'unauthorized AI app'](#)

Double Canvas breach acknowledged as ShinyHunters sets new pay-or-leak deadline

Ed-tech giant Instructure confirmed two rounds of unauthorized activity affecting its online learning platform Canvas within two weeks as data-theft-and-extortion crew ShinyHunters threatened to leak data it claims belongs to more than 275 million students, teachers, and staff tied to nearly 9,000 schools worldwide.

And it finally broke its silence on Monday about what happened, admitting not one but two intrusions after criminals exploited a security vulnerability in its Free-for-Teacher learning system, and saying the data thieves stole information including usernames, email addresses, course names, enrolment information, and messages.

ShinyHunters claims it stole 3.65 TB of data, including about 275 million records from about 8,800 schools including Harvard, Columbia, Rutgers, Georgetown, and Stanford universities. After moving the pay-or-leak deadline multiple times, ShinyHunters set a final deadline of end-of-day May 12 for individual institutions to contact them directly to negotiate payment - or the group will publish the full dataset.

READ MORE >

Vulnerabilities

VULNERABILITIES & EXPLOITS



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

LAST WEEKS RECAP

CVE-2026-31431: Copy Fail vulnerability enables Linux root privilege escalation across cloud environments
CVSS Score: (7.8)

CVE-2026-0300: Unauthenticated user initiated Buffer Overflow Vulnerability in User-ID™ Authentication Portal (PAN-OS).
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



OTHER PHISHING ARTICLES

[New VENOM phishing attacks steal senior executives' Microsoft logins](#)

[KongTuke hackers now use Microsoft Teams for corporate breaches](#)

[Hackers abuse Google ads, Claude.ai chats to push Mac malware](#)

Over 500 Organizations Hit in Years-Long Phishing Campaign

A phishing campaign that has been ongoing for more than four years has made hundreds of victims across multiple industries, SOCRadar reports.

Dubbed Operation HookedWing, the campaign was first documented in 2022 but has sustained activity and adapted its infrastructure while keeping core patterns largely unchanged.

Between 2022 and 2024, Operation HookedWing used GitHub domains with English content and compromised servers as infrastructure, and the attacks mainly featured Microsoft and Outlook themes. In 2024 and 2025, the threat actor expanded its targeting with French content, continuing to use GitHub, compromised servers, and previously observed phishing themes.

Starting in 2025, the threat actor has expanded both the active infrastructure and lures, obfuscating GitHub domain naming, adding more themes, and deploying additional landing pages.

Operation HookedWing relies on phishing emails impersonating human resources or colleagues, or posing as notifications. The messages have a simple structure and are designed to convey authority and urgency without raising suspicion.

READ MORE >