SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

June 2026 - VOL.1

The News

IN THE NEWS THIS WEEK

Microsoft 365 Android Apps Let Any App Steal Account Tokens via Leftover Debug Flag

A development flag left switched on in production builds of several Microsoft 365 Android apps disabled the check that limits account-token sharing to trusted Microsoft apps.

Any other app on the same phone could ask for the signed-in user's token and get it, then read email, open files, browse the calendar, and send messages as that user. No password, no login screen, no permission prompt.

Microsoft has patched it, and if you run Microsoft 365 apps on Android, update them.

The bug, which Enclave calls FlagLeft, hit Word, PowerPoint, Excel, Microsoft 365 Copilot, Microsoft Loop, and OneNote, six apps with billions of downloads between them. Teams shipped with the same flag set to false and were not affected, which Enclave reads as a slip rather than a design.

READ MORE

OTHER NEWS HIGHLIGHTS

One-Click GitHub Dev Attack Lets Attackers Steal Full GitHub OAuth Tokens

Unpatched Windows Search URI Vulnerability Lets Attackers Steal NTLMv2 Hashes

New HTTP/2 Bomb Vulnerability Allows Remote DoS on NGINX, Apache, IIS, Envoy & Cloudflare

The News

TOP OF THE NEWS THIS WEEK

Google June 2026 Android Update Patches 124 Flaws, One Actively Exploited

Google on Monday released patches for 124 security vulnerabilities impacting its Android operating system for the month of June 2026, including one high-severity flaw in the Framework component that has come under active exploitation.

Tracked as CVE-2025-48595 (CVSS score: 8.4), the security flaw has been described as a case of privilege escalation without requiring any user interaction. The vulnerability impacts devices running Android versions 14, 15, 16, and 16 QPR2 (Quarterly Platform Release 2).

"In multiple locations, there is a possible way to achieve code execution due to an integer overflow," according to a description of the vulnerability on CVE.org. "This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation."

READ MORE

TOP RELATED ARTICLES

Oracle WebLogic CVE-2024-21182 Added to KEV Catalog After Active Exploitation

OpenAI Codex Authentication Tokens Stolen in codexui-android npm Supply Chain Attack

PAN-OS GlobalProtect Authentication Bypass (CVE-2026-0257) Under Active Exploitation

Geo-Politics

NEWS FROM AROUND THE WORLD

Dutch Authorities Dismantle Botnet Linked to 17 Million Infected Devices

Dutch authorities have announced the takedown of a botnet that enslaved millions of infected devices, including computers, tablets, smartphones, and IoT devices, to carry out malicious attacks.

The bot network, per the Dutch Politie and the National Cyber Security Center (NCSC), consisted of at least 17 million infected devices. More than 200 servers located in the Netherlands acted as the platform's backend infrastructure.

According to a statement issued by the NCSC, police officials seized a subset of these servers from a hosting provider that provided the infrastructure. The provider is said to have subsequently taken the botnet offline following its use for criminal purposes.

Although the name of the botnet was not explicitly mentioned, local news outlet NL Times reported that the service in question was Asocks, a company that offers residential proxies. In April 2024, HUMAN's Satori Threat Intelligence team identified a campaign dubbed PROXYLIB that involved infecting Android devices with proxyware from LumiApps and Asocks.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Breaches

SECURITY BREACHES THIS WEEK

Carnival Data Breach Exposed 6 Million People

Cruise line operator Carnival Corporation is notifying approximately 6 million individuals that their personal information was stolen in a recent data breach. Carnival said the incident was identified on April 14, after hackers gained access to an employee's account via social engineering.

Using the compromised account, the attackers accessed certain company systems and exfiltrated files containing personal information.

"The company has been conducting a thorough and time-consuming analysis of the impacted files to determine what personal information they contained and to whom that information belongs," an incident notice on Carnival's website reads.

According to the company, the potentially impacted information varies by individual, but generally includes names, addresses, dates of birth, email addresses, phone numbers, and government-issued ID numbers.

On Wednesday, Carnival informed the Maine Attorney General's Office that 5,995,277 people were affected and that it was providing them with 24 months of free credit monitoring services.

READ MORE

OTHER SECURITY BREACHES

Charter Communications Data Breach Could Impact Nearly 5 Million

Critical Windows Netlogon Vulnerability in Attackers' Crosshairs

California Sues 23andMe, Alleging It Failed to Protect User Data in 2023 Breach

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-21182 - Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware

CVSS SCORE 7.5

CVE-2024-7593 - Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2026-45659 - Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.

CVSS Score: (8.8)

CVE-2026-45498 - Microsoft Defender Denial of Service Vulnerability

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

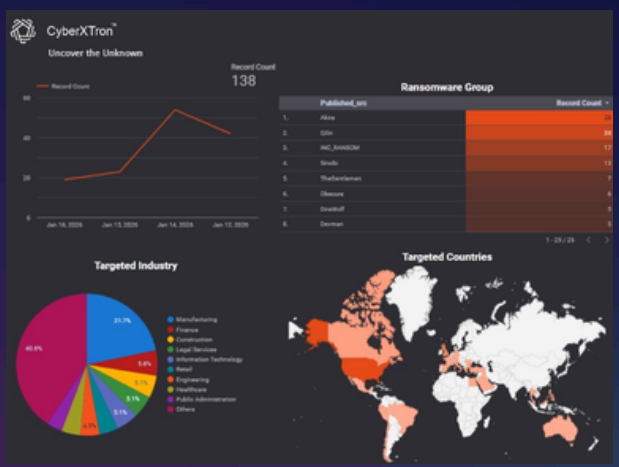
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

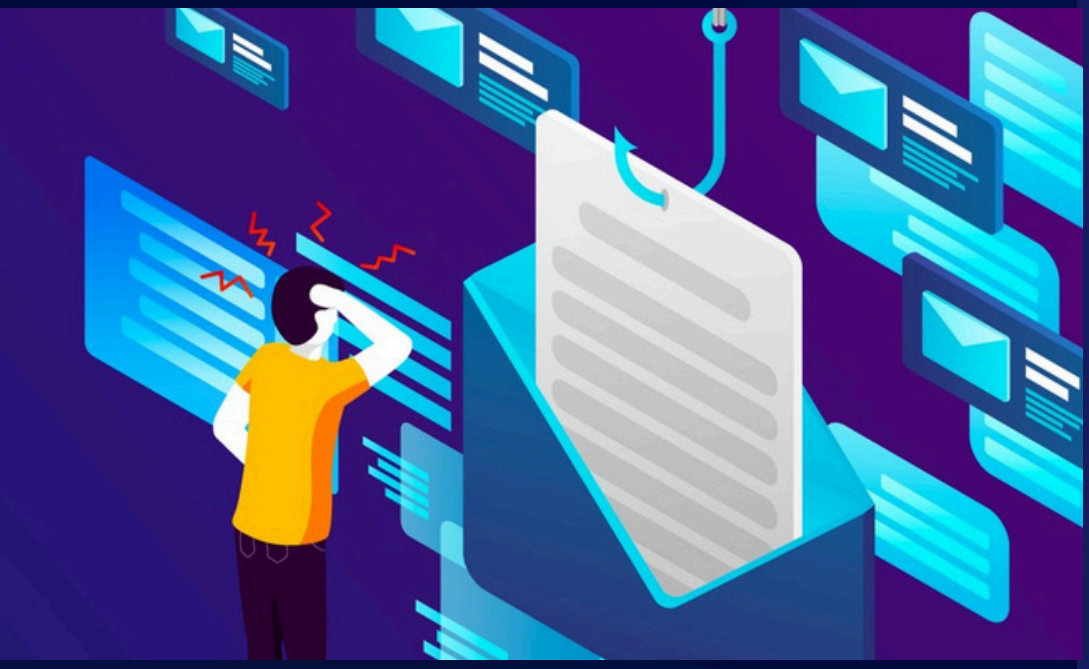
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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



Google DoubleClick Abused in New Malspam Campaign to Deliver DesckVB RAT

Cybersecurity researchers have flagged a new malspam campaign that makes use of Google's DoubleClick domain as a way to evade detection and ultimately deliver a remote access trojan (RAT) named DesckVB RAT.

"Before the victim ever reaches attacker-controlled infrastructure, the lure routes through DoubleClick, a legitimate Google-owned domain that many security tools are less likely to treat as suspicious," Huntress researchers Anna Pham and Adam Mooney said in a report shared with The Hacker News.

"From there, the victim is passed into a malspam kit that personalizes itself on the fly using the victim's email address, dynamically pulling in company branding and location details to make the page feel convincing without requiring the operators to handcraft a lure for each target."

READ MORE

OTHER PHISHING ARTICLES

ChatGPhish Vulnerability Turns ChatGPT Web Summaries Into a Phishing Surface

West Mercia Fraud & Scam bulletin June 2026

Keep getting calls from questionable numbers? Meet Scam Number Check