SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

June 2026 - VOL.3

The News

IN THE NEWS THIS WEEK

Microsoft Confirms RoguePlanet Defender Zero-Day, Says Patch is in Development

Microsoft has formally disclosed that it's working to release a patch to address a Defender zero-day codenamed RoguePlanet.

The vulnerability has now been assigned the CVE identifier CVE-2026-50656 (CVSS score: 7.8), with the tech giant describing it as a privilege escalation flaw.

"Microsoft is aware of an elevation of privilege in the Microsoft Malware Protection Engine in Microsoft Defender, publicly referred to as 'RoguePlanet,'" the company said. "We are working to provide a high-quality security update that addresses this vulnerability."

The development comes nearly a week after a security researcher named Chaotic Eclipse (aka Nightmare-Eclipse) released RoguePlanet, calling the exploit a case of a race condition that grants attackers a shell with SYSTEM-level privileges.

READ MORE

OTHER NEWS HIGHLIGHTS

Malicious JetBrains Plugins Steal AI API Keys as Chrome Extensions Capture Chatbot Chats

CISA Warns of Actively Exploited Joomla JCE Flaw Allowing PHP Code Execution

Google Vertex AI SDK Flaw Let Attackers Hijack Model Uploads via Bucket Squatting

The News

TOP OF THE NEWS THIS WEEK

New Rokarolla Android Malware Steals PINs, SMS Codes, and Crypto Wallet Funds

Security researchers at Zimperium's zLabs have documented a new Android banking trojan, Rokarolla, that targets 217 banking and cryptocurrency apps and packs 137 remote commands.

Together, they give an operator near-total control of an infected phone: it lifts lock-screen PINs, reads and sends SMS, rewrites the clipboard to redirect crypto payments, and switches off Google Play Protect.

Rokarolla, named after its command-and-control servers, spreads through malicious websites posing as well-known apps such as TikTok and Chrome. The first thing a victim installs is a dropper that pretends to be Google Play Protect. It uses that disguise to get the payload installed and grab Accessibility access. Once the malware is running, one of its commands turns Play Protect off.

READ MORE

TOP RELATED ARTICLES

Attackers Exploit Three Fortinet FortiSandbox Flaws, One Patched Last Week

Cisco Releases Security Updates for Actively Exploited SD-WAN Manager Flaw

One-Click Microsoft 365 Copilot Flaw Could Have Let Attackers Steal Emails, Files, and MFA Codes

Geo-Politics

NEWS FROM AROUND THE WORLD

North Korean Hackers Are Turning Developer Tools Into Malware Delivery Channels

Cybersecurity researchers have flagged two malicious cyber campaigns that exhibit similarities with a persistent North Korean threat cluster known as Contagious Interview (aka Famous Chollima, HexagonalRodent, and Void Dokkaebi).

According to a report published by Proofpoint, the threat actor has been found orchestrating phishing campaigns using developer role recruitment or code review themes to target nearly 100 organizations in finance, cryptocurrency, education, technology, and several other sectors. The activity has been codenamed UNK_DeadDrop.

"The infection chain begins with emails containing links to actor-controlled GitHub repositories hosting malicious scripts that result in the execution of cross-platform malware for macOS, Linux, and Windows, including an open-source Go framework named Overlord," Proofpoint researchers Saher Naumaan and Carlos Rubio said.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Chinese Hackers Abused Google Workspace Rules to Steal Research and Defense Emails

---

Fake Microsoft Alerts Used to Deploy North Korean NarwhalRAT Malware

---

China-Linked SprySOCKS Backdoor Expands to Windows with Driver-Based Stealth

Breaches

SECURITY BREACHES THIS WEEK

iRhythm Confirms Data Stolen in Hack

iRhythm, a health company specializing in wearable cardiac monitoring technology, has been targeted in a cyberattack that resulted in the theft of information.

The data breach was disclosed by iRhythm, known for its Zio wearable ECG monitor, in a Monday filing with the SEC.

The company said it detected “unauthorized activity involving data maintained on certain third-party-hosted business applications” on June 8. iRhythm noted that the attack involved social engineering, but the targeted application has not been named.

A threat actor contacted the company on June 9, claiming to have stolen sensitive information, including proprietary data and patients’ protected health information. The hackers demanded a ransom to prevent the compromised files from being leaked.

iRhythm has been working with external cybersecurity experts to investigate the breach, and it has confirmed that some data has been stolen, but it has not said whether the threat actor’s description of the compromised data is accurate.

READ MORE

OTHER SECURITY BREACHES

Palo Alto Warns of Active Exploitation of PAN-OS GlobalProtect VPN Flaw

French Government Messaging Platform Breached by Mysterious ‘Misere’ Hacke

Ozempic Maker Novo Nordisk Says Hackers Breached IT Systems

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-0257 - Authentication bypass vulnerabilities in the GlobalProtect portal and gateway of Palo Alto Networks PAN-OS® software allow the attacker to bypass security restrictions and establish an unauthorized VPN connection,"

CVSS SCORE 7.8

CVE-2026-50656 - Microsoft Defender Elevation of Privilege Vulnerability

CVSS SCORE 7.8

LAST WEEKS RECAP

CVE-2026-5027 - Unpatched Langflow Flaw Exploited for Unauthenticated RCE

CVSS Score: (8.8)

CVE-2026-8863 - UEFI Secure Boot security feature bypass

CVSS Score: (6.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

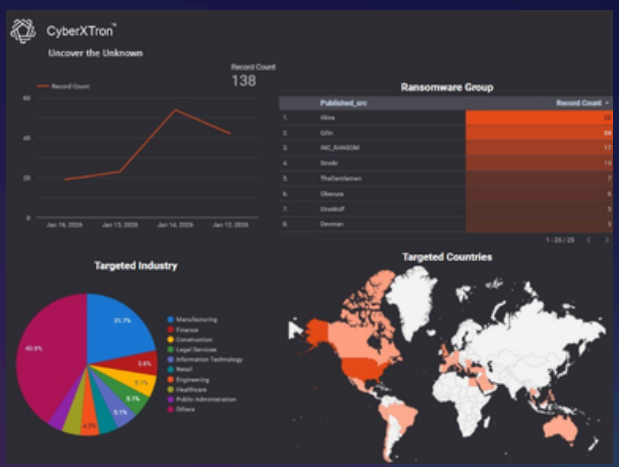
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

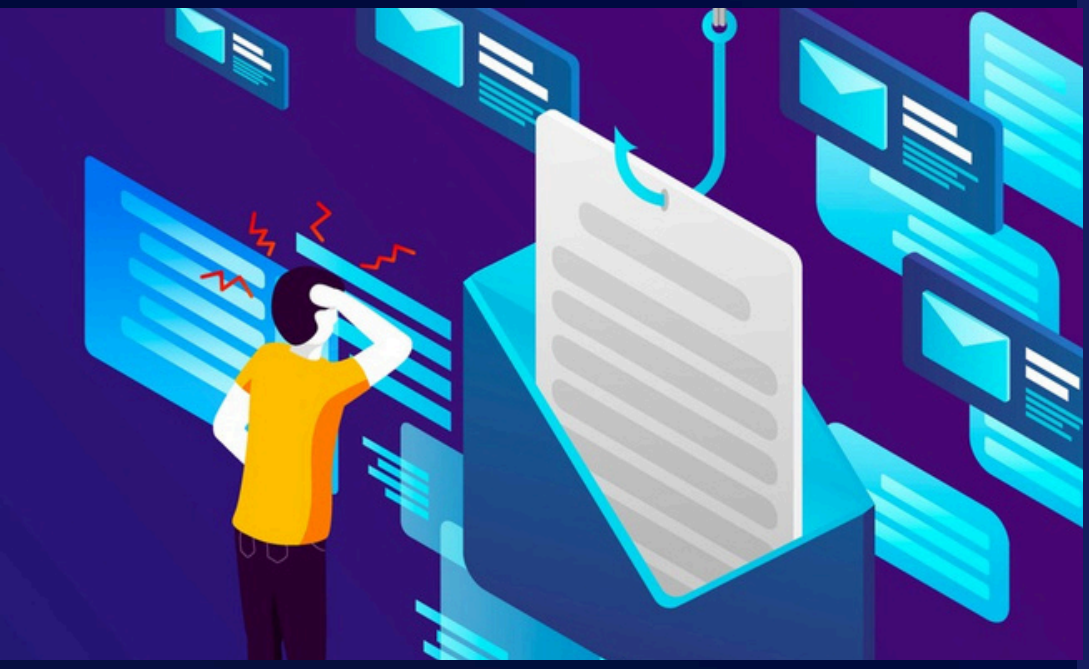
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

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 Sues Chinese Smishing Network Accused of Using Gemini AI in Phishing

Google on Friday said it's pursuing legal action against a Chinese cybercrime network, accusing it of using its Gemini artificial intelligence (AI) agent to send phishing text messages targeting Americans.

The network is said to be behind the development and management of a phishing-as-a-service (PhaaS) software kit called Outsider, per the tech giant.

"The operation weaponized Gemini to help generate fraudulent phishing pages and deploy massive SMS phishing ('smishing') attacks, often through text messages impersonating legitimate brands, alerting recipients of 'brokerage account issues' or insisting they are eligible for 'rewards through their mobile phone carrier,'" Google said.

"The texts prompt users to click a link leading to a fraudulent website that mimics trusted institutions to steal personal and financial information."

READ MORE

OTHER PHISHING ARTICLES

INTERPOL Operation Takes Down Sniper Dz Phishing Platform, Arrests Administrator

SpyCloud Report Finds Phishing Attacks Surge as Employee Data Is Exposed at 86% of Fortune 100 Companies

Google Sues Anonymous Cybercriminals Over Alleged Text Phishing Scams Fueled by AI