

THREATLABZ REPORT

Encrypted attack predictions you need to know for 2025

New research and insights into threats hiding within HTTPS

Download Now

zscaler

CISA and FBI Raise Alerts on Exploited Flaws and Expanding HiatusRAT Campaign

Dec 17, 2024

Ravie Lakshmanan

Network Security / IoT Security



The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday **added** two security flaws to its Known Exploited Vulnerabilities (**KEV**) catalog, citing evidence of active exploitation in the wild.

The list of flaws is below -

- CVE-2024-20767** (CVSS score: 7.4) - Adobe ColdFusion contains an improper access control vulnerability that could allow an attacker to access or modify restricted files via an internet-exposed admin panel (Patched by Adobe in **March 2024**)
- CVE-2024-35250** (CVSS score: 7.8) - Microsoft Windows Kernel-Mode Driver contains an untrusted pointer dereference vulnerability that allows a local attacker to escalate privileges (Patched by Microsoft in **June 2024**)

Taiwanese cybersecurity company DEVCORE, which discovered and reported CVE-2024-35250, **shared** additional technical details in August 2024, stating it's rooted in the Microsoft Kernel Streaming Service (MSKSSRV).

CIS

Center for Internet Security

CIS SecureSuite

Make your cyber defense **strong**.
Make it **reasonable**.

GET STARTED

Defending against USB drive attacks with Wazuh

THN Weekly R

Zero-Day Exploits and Crypto Heists

Defending against attacks with Wazuh

THN Weekly R

\$1.5B Crypto Heist, Apple's Data Dilemma

THN Weekly R

Secrets Stolen, W

New Crypto Scam

THN Weekly R

Attacks, Old Trick

The Fastest Way to Secure Your Cloud

Show More

Popular Resources

Test Your Team's with Real-World C Simulations

[Report] The Top DevSecOps Pros

zscaler

Traditional Firewalls Are Obsolete in the AI Era

Stay Ahead with Zero Trust + AI360

LEARN MORE

There are currently no details on how the shortcomings are being weaponized in real-world attacks, although proof-of-concept (PoC) exploits for **both** of **them** exist in the public domain.

In light of active exploitation, Federal Civilian Executive Branch (FCEB) agencies are recommended to apply the necessary remediation by January 6, 2025, to secure their networks.

FBI Warns of HiatusRAT Targeting Web Cameras and DVRs

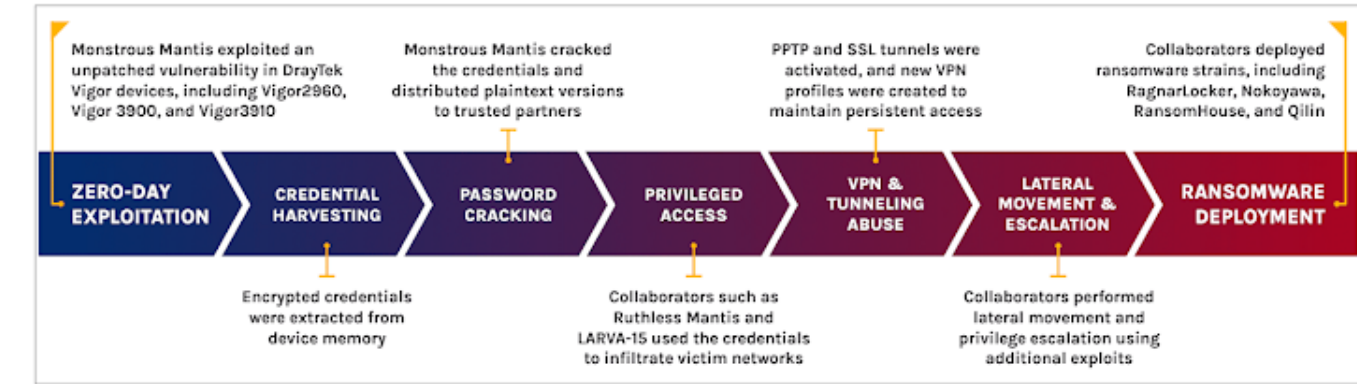
The development follows an alert from the Federal Bureau of Investigation (FBI) about **HiatusRAT** campaigns expanding beyond network edge devices like routers to scan Internet of Things (IoT) devices from Hikvision, D-Link, and Dahua located in the U.S., Australia, Canada, New Zealand, and the United Kingdom.

"The actors scanned web cameras and DVRs for vulnerabilities including **CVE-2017-7921**, **CVE-2018-9995**, **CVE-2020-25078**, **CVE-2021-33044**, **CVE-2021-36260**, and weak vendor-supplied passwords," the FBI **said**. "Many of these vulnerabilities have not yet been mitigated by the vendors."

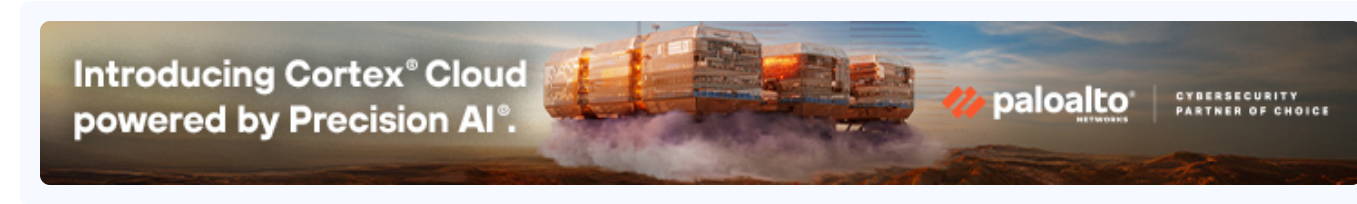
The malicious activity, observed in March 2024, involved the use of open-source utilities called **Ingram** and **Medusa** for scanning and brute-force authentication cracking.

DrayTek Routers Exploited in Ransomware Campaign

The warnings also come as Forescout Vedere Labs, with intelligence shared by PRODAFT, revealed last week that threat actors have exploited security flaws in DrayTek routers to target over 20,000 DrayTek Vigor devices as part of a coordinated ransomware campaign between August and September 2023.



"The operation exploited a suspected zero-day vulnerability, enabling attackers to infiltrate networks, steal credentials, and deploy ransomware," the company **said**, adding the campaign "involved three distinct threat actors – Monstrous Mantis (Ragnar Locker), Ruthless Mantis (PTI-288) and LARVA-15 (**Wazawaka**) – who followed a structured and efficient workflow."



Monstrous Mantis is believed to have identified and exploited the vulnerability and systematically harvested credentials, which were then cracked and shared with trusted partners like Ruthless Mantis and LARVA-15.

The attacks ultimately allowed the collaborators to conduct post-exploitation activities, including lateral movement and privilege escalation, ultimately leading to the deployment of different ransomware families such as RagnarLocker, Nokoyawa, RansomHouse, and Qilin.

— Trending News



⚡ THN Weekly Roundup: Zero-Day Exploits and Crypto Heists



Defending against USB drive attacks with Wazuh



⚡ THN Weekly Roundup: \$1.5B Crypto Heist, Apple's Data Dilemma



⚡ THN Weekly Roundup: Secrets Stolen, Wazuh New Crypto Scams



⚡ THN Weekly Roundup: Ransomware Attacks, Old Tricks

— Popular Resources



Test Your Team's Skills with Real-World CTF Simulations



[Report] The Top 10 DevSecOps Pros and Cons

"Monstrous Mantis withheld the exploit itself, retaining exclusive control over the initial access phase," the company said. "This calculated structure allowed them to profit indirectly, as ransomware operators who successfully monetized their intrusions were obliged to share a percentage of their proceeds."

Ruthless Mantis is estimated to have successfully compromised at least 337 organizations, mainly located in the U.K. and the Netherlands, with LARVA-15 acting as an initial access broker (IAB) by selling the access it gained from Monstrous Mantis to other threat actors.

It's suspected that the attacks made use of a then zero-day exploit in DrayTek devices, as evidenced by the discovery of [22 new vulnerabilities](#) that share root causes similar to [CVE-2020-8515](#) and [CVE-2024-41592](#).

"The recurrence of such vulnerabilities within the same codebase suggests a lack of thorough root cause analysis, variant hunting and systematic code reviews by the vendor following each vulnerability disclosure," Forescout noted.

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.

 [Tweet](#)

 [Share](#)

 [Share](#)

 [Share](#)

Trending News



THN Weekly Ransomware Report: Zero-Day Exploits and Crypto Heists



Defending against USB drive attacks with Wazuh



THN Weekly Ransomware Report: \$1.5B Crypto Heist and Apple's Data Dilemma



THN Weekly Ransomware Report: Secrets Stolen, Wazuh New Crypto Scams



THN Weekly Ransomware Report: Attacks, Old Tricks

Popular Resources

CYBERSECURITY WEBINARS

Secure Smarter, Not Harder

Learn How ASPM Combines Code and Runtime for Real-Time Protection

Keep your apps safe with ASPM—a simple tool that brings code and live data together for easy security.

Secure Your Webinar Access

Stop Identity Attacks in Their Tracks

Fed Up With Cyber Attacks? Discover the Simple Way to Block Identity Threats

Stop cyberattacks before they start—discover a simple, secure solution to eliminate identity threats in our exclusive webinar.

Watch This Now

Breaking News



Alleged Israeli LockBit Developer Rostislav Panev Extradited to U.S. for Cybercrime Charge...

A 51-year-old dual Russian and Israeli national who is alleged to be a developer of the LockBit ra.....



GSMA Confirms End-to-End Encryption for RCS, Enabling Secure Cross-Platform Messaging...

The GSM Association (GSMA) has formally announced support for end-to-end encryption (E2EE) for sec.....



Live Ransomware Demo: See How Hackers Breach Networks and Demand a Ransom...

Cyber threats evolve daily. In this live webinar, learn exactly how ransomware attacks unfold—from



Why Most Microsegmentation Projects Fail—And How Andelyn Biosciences Got It Right...

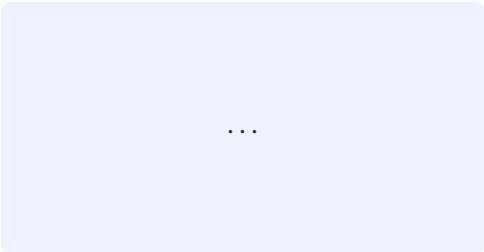
Most microsegmentation projects fail before they even get off the ground—too complex, too slow, too.....

Cybersecurity Resources



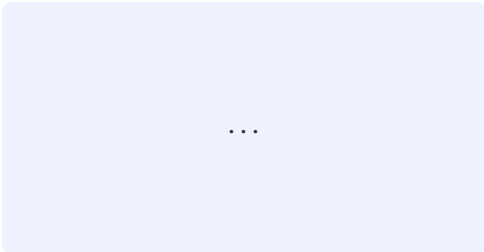
Choosing the Right Runtime Sensor

Wiz's new Runtime Buyer's Guide highlights the key features for securing your cloud-native environments like containers, Kubernetes, and serverless architectures.



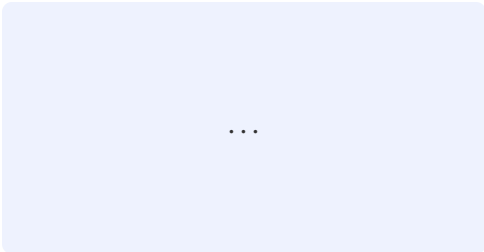
Want To Excel in Cybersecurity Risk Management?

Learn cybersecurity risk management from the experts. Attend our webinar on March 26.



Uplevel your Cybersecurity Skills at SANS Security West 2025 in San Diego on May 5

Cutting edge, expert-led training to boost your career. Train in-person to get a \$3,240 cyber-pro pass!



Stop Playing Defense Games Their Way

Companies spend billions of dollars on Firewalls and intrusion detection systems, yet continue to risk breaches.



Defending against USB drive attacks with Wazuh

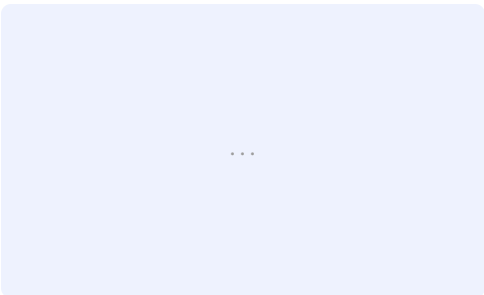


THN Weekly Roundup: \$1.5B Crypto Heist, Apple's Data Dilemma



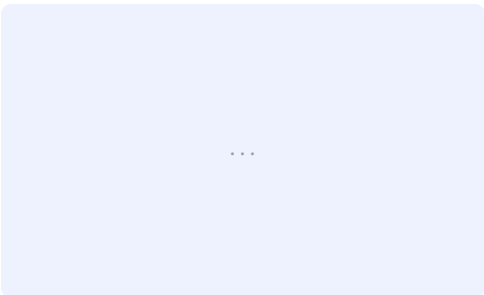
THN Weekly Roundup: Secrets Stolen, WikiLeaks New Crypto Scams

— Expert Insights / Videos Articles



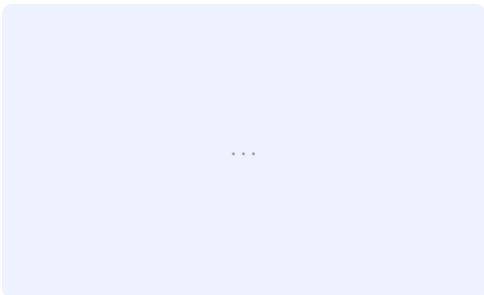
CTM360 Uncovers a Large-Scale Fake Play Store Scam Targeting Global Users: PlayPraetor Trojan

📅 March 10, 2025 [Read →](#)



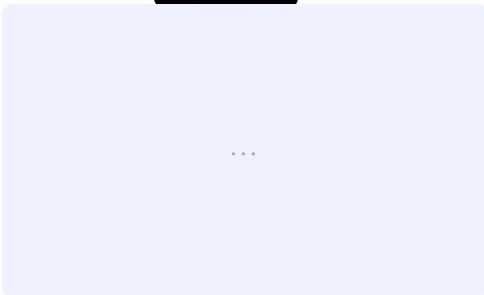
Identity Attacks: Prevention isn't Enough

📅 March 10, 2025 [Read →](#)



Why Now is the Time to Adopt a Threat-Led Approach to Vulnerability Management

📅 March 3, 2025 [Read →](#)



Why Aggregating Your Asset Inventory Leads to Better Security

📅 March 3, 2025 [Read →](#)



Test Your Team's Skills with Real-World CTF Simulations



[Report] The Top DevSecOps Pros

Get Latest News in Your Inbox

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders – all for free.

>

Connect with us!



922,500 Followers



625,000 Followers



23,100 Subscribers



145,000 Followers



1,890,500 Followers



143,200 Subscribers

Company

- About THN
- Advertise with us
- Contact

Pages

- Webinars
- Privacy Policy

RSS Feeds

Contact Us