Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

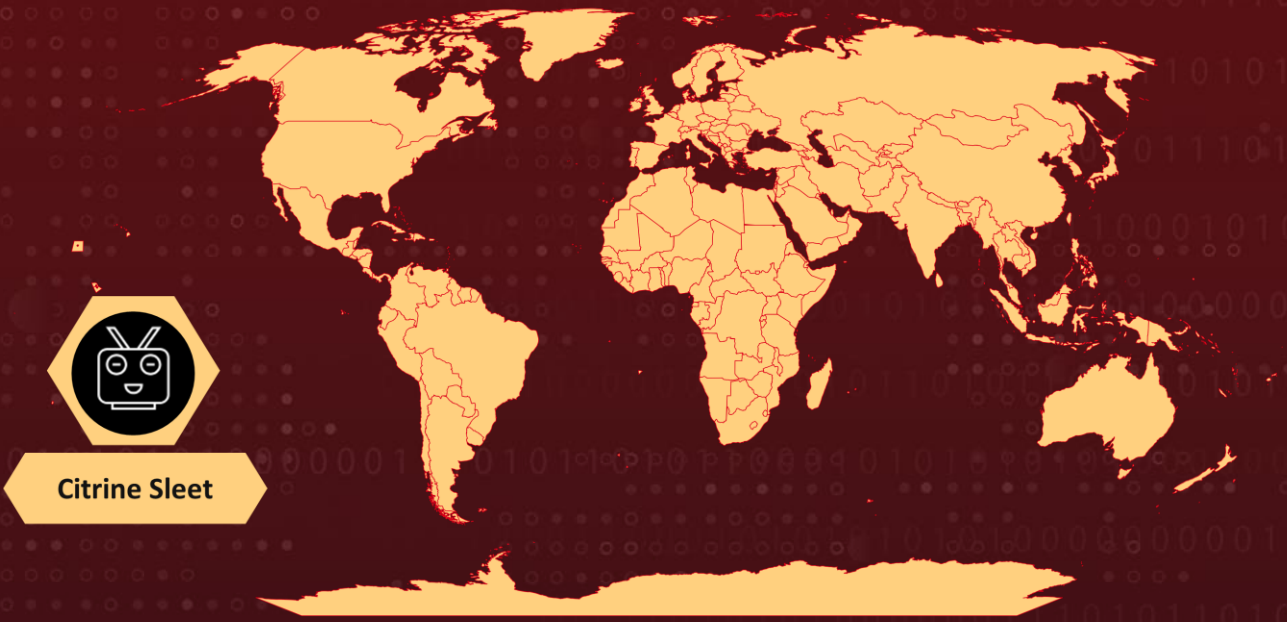
North Korean Hackers Exploit Chrome Zero-Day in Cryptocurrency Heists

Date of Publication	Admiralty Code	TA Number
September 3, 2024	A1	TA2024337

Summary

Attack Discovered: August 19, 2024
Attack Region: Worldwide
Targeted Industries: Cryptocurrency, Financial
Malware: FudModule
Actor: Citrine Sleet (aka Lazarus Group, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)
Attack: North Korean hackers have exploited a recently patched Google Chrome zero-day vulnerability (CVE-2024-7971) to deploy the FudModule rootkit. After gaining SYSTEM privileges using a Windows Kernel exploit, they were able to install the rootkit, allowing them to maintain persistent access to compromised systems.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-7971	Google Chromium V8 Type Confusion Vulnerability	Google Chrome, Microsoft Edge	✓	✓	✓

Attack Details

#1 The North Korean threat actor Citrine Sleet, also known as Lazarus, has been actively exploiting a zero-day vulnerability in Chromium, identified as CVE-2024-7971, to achieve remote code execution (RCE). Citrine Sleet primarily targets financial institutions, especially those involved in managing cryptocurrencies, to exploit this flaw for monetary gain. After leveraging CVE-2024-7971, Citrine Sleet uses a Windows Kernel exploit to escalate privileges to SYSTEM level, enabling the deployment of the FudModule rootkit and ensuring persistent access to compromised systems.

#2 Citrine Sleet commonly infects targets with its custom trojan malware, AppleJeus. This malware is engineered to gather the necessary information to seize control of victims' cryptocurrency assets. The FudModule rootkit has also been attributed to Citrine Sleet, suggesting a sharing of tools among North Korean cyber actors.

#3 CVE-2024-7971 is a type confusion vulnerability in the V8 JavaScript and WebAssembly engine. In a recent zero-day attack, Citrine Sleet followed the standard browser exploit chain stages, directing targets to a controlled domain. Although the method of luring targets to the site is unclear, social engineering is a known tactic of Citrine Sleet. Once a connection to the domain was made, the zero-day RCE exploit for CVE-2024-7971 was executed.

#4 After the RCE exploit successfully achieved code execution within the Chromium renderer's sandboxed environment, shellcode containing a Windows sandbox escape exploit and the FudModule rootkit was downloaded and loaded into memory. Upon a successful sandbox escape, the main FudModule rootkit executed in memory. This sophisticated rootkit employs direct kernel object manipulation (DKOM) techniques to bypass kernel security mechanisms. Operating exclusively from user mode, it performs kernel tampering using a read/write primitive, allowing deep manipulation of the operating system and maintaining covert persistence.

#5 FudModule is a highly advanced rootkit malware specifically designed to gain kernel access while avoiding detection. Threat actors use the FudModule data-only rootkit to achieve admin-to-kernel access on Windows systems. The Lazarus group has been deploying FudModule since at least October 2021. Organizations are strongly advised to implement the necessary security patches immediately to protect their systems against this sophisticated threat.

Recommendations

Update Chrome Immediately: Ensure your Chrome browser is updated to version 128.0.6613.84 (Linux) or 128.0.6613.84/.85 (Windows and macOS) or later. This version contains the patch for the CVE-2024-7971 vulnerability. You can update by navigating to Chrome Menu > Help > About Google Chrome, then letting the update process complete and clicking the 'Relaunch' button.

Remain Vigilant: Avoid clicking on suspicious links or visiting untrusted websites, as they may harbor malicious content. Be cautious when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0040** Impact	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1189** Drive-by Compromise	**T1566** Phishing	**T1014** Rootkit

T1036 Masquerading	T1068 Exploitation for Privilege Escalation	T1059 Command and Scripting Interpreter	T1176 Browser Extensions
T1553 Subvert Trust Controls	T1565 Data Manipulation		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	voyagorclub[.]space, weinsteinfrog[.]com

Patch Details

Update Google Chrome and Edge browser to latest version 128.0.6613.84 for Linux, 128.0.6613.84/.85 for Mac and Windows.

Link:
https://www.google.com/intl/en/chrome/?standalone=1

References

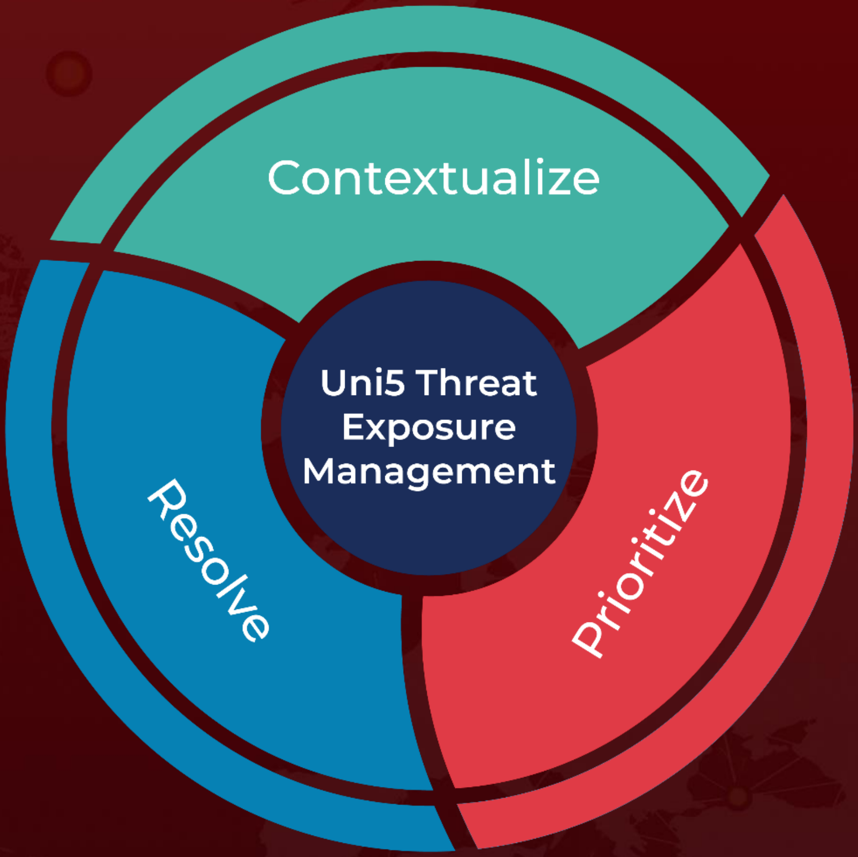
https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/

https://hivepro.com/threat-advisory/google-alerts-users-to-actively-exploited-chrome-zero-day-flaws/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 3, 2024 • 6:30 AM

More at www.hivepro.com