

HiveForce Labs

THREAT ADVISORY

**ATTACK REPORT**

Lazarus Exploits Chrome Zero-Day in Fake DeFi Game Heist

Date of Publication

October 25, 2024

Admiralty Code

A1

TA Number

TA2024411

Summary

Attack Discovered: February 2024

Targeted Countries: Russia

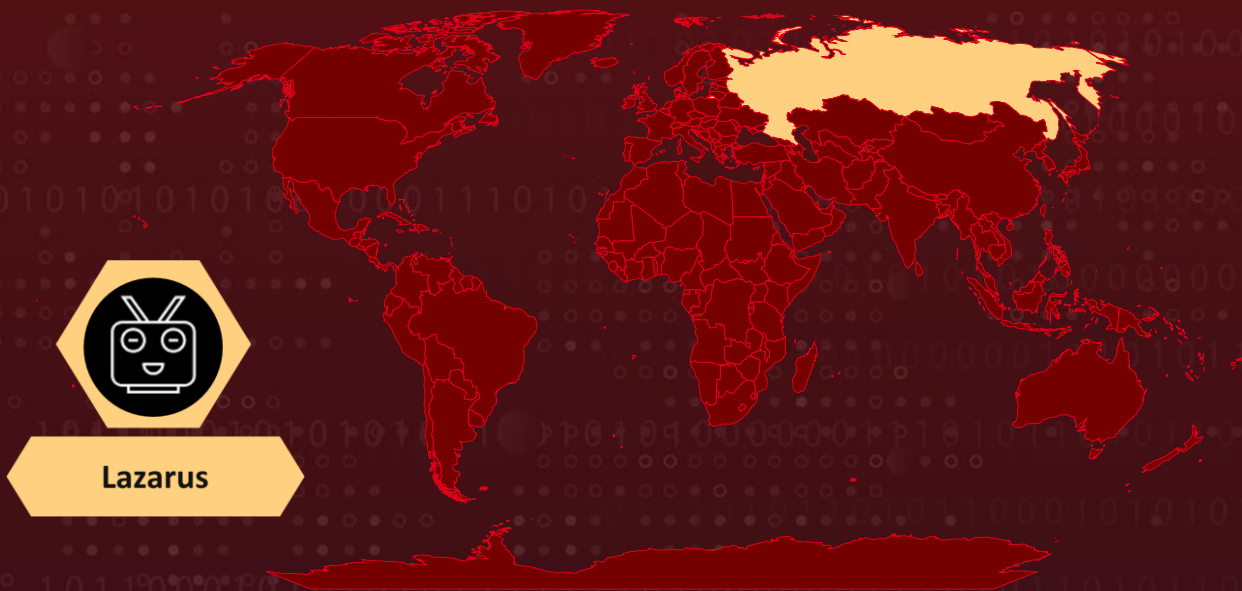
Targeted Industry: Cryptocurrency

Malware: Manuscript

Actor: Lazarus Group (aka UNC2970, 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, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)







Attack: The North Korean Lazarus hacking group has leveraged a Google Chrome zero-day vulnerability, identified as CVE-2024-4947, as part of a highly targeted campaign aimed at individuals in the cryptocurrency space. This exploitation was delivered through a fake decentralized finance (DeFi) game, designed to lure victims and compromise their systems. In one notable instance, the attackers targeted the personal computer of an unnamed Russian national, deploying the Manuscript backdoor to establish long-term access and facilitate further malicious activities.

🗡️ Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-4947	Google Chromium V8 Type Confusion Vulnerability	Google Chrome			
Unassigned	Google Chromium V8 SandBox Bypass Vulnerability	Google Chrome			

Attack Details

#1

The Lazarus APT group recently exploited a critical zero-day vulnerability in Google Chrome ([CVE-2024-4947](#)) to launch a deceptive attack on the cryptocurrency sector. Disguised as a decentralized finance (DeFi) game, the campaign specifically targeted influential individuals in the crypto space. A new variant of the "Manuscript" backdoor was discovered on the personal computer of an individual in Russia, marking an advanced social engineering effort.

#2

Lazarus has been employing Manuscript malware since years in various campaigns. Victims were directed to a malicious site that deployed an exploit aimed at Chrome's V8 Maglev JIT compiler, allowing the attackers to execute arbitrary code and gain extensive access to sensitive information on affected systems.

#3

In early 2024, researchers notified Google of the exploit's existence, allowing time for a patch before public disclosure. Meanwhile, Google blocked malicious domains associated with the campaign to prevent further exploitation.

#4

The attack method was highly complex. The threat actors used a TypeScript/React-based website containing obfuscated JavaScript, which exploited two vulnerabilities in Chrome. The first bypassed Chrome's memory protections, allowing memory manipulation from JavaScript, and the second broke through the V8 sandbox to achieve arbitrary code execution. The attackers used Irregexp, Chrome's regular expression interpreter, to extend control beyond V8's isolated memory space. This exploit allowed them to bypass traditional V8 sandboxing measures by accessing memory outside of standard boundaries, effectively creating an unrestricted path for shellcode execution.

#5

Lazarus cloned DeFiTankLand, creating a near-identical game, DeTankZone, by subtly altering assets and mechanics. They used targeted spear-phishing through social media and email to lure crypto influencers to try the supposed beta. The copy closely mirrored DeFiTankLand, even featuring cryptocurrency elements. Shortly after the campaign began, DeFiTankLand developers reported a breach in their cold wallet, suspecting an insider, though Lazarus is likely behind it.

#6

Lazarus's operation underscores the dangers of sophisticated APT actors and highlights the persistence of zero-day vulnerabilities in widely used software. This campaign shows Lazarus's adept use of both technical exploits and social engineering tactics, reinforcing the need for continued vigilance and timely security updates, especially in sectors like cryptocurrency.

Recommendations



Update Chrome Immediately: Ensure that all systems running Google Chrome are updated to version 125.0.6422.60/.61 for Windows and Mac, or 125.0.6422.60 for Linux. Promptly apply any security updates released by Google to stay protected against known vulnerabilities.



Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.



Strengthen Browser Security Configurations: Disable JIT (Just-In-Time) compilation where feasible and enable additional sandboxing features, particularly for high-risk users in sectors like finance.



Restrict Third-Party Applications and Plugins: Limit or restrict installation of unauthorized applications or browser plugins that can become vectors for exploits.



Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>TA0005</u> Defense Evasion	<u>TA0011</u> Command and Control	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities
<u>T1588.005</u> Exploits	<u>T1608</u> Stage Capabilities	<u>T1608.001</u> Upload Malware	<u>T1190</u> Exploit Public-Facing Application
<u>T1583</u> Acquire Infrastructure	<u>T1583.001</u> Domains	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.007</u> JavaScript
<u>T1566</u> Phishing	<u>T1566.002</u> Spearphishing Link	<u>T1204</u> User Execution	<u>T1204.001</u> Malicious Link
<u>T1132</u> Data Encoding	<u>T1132.001</u> Standard Encoding	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1036</u> Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	B2DC7AEC2C6D2FFA28219AC288E4750C, 8312E556C4EEC999204368D69BA91BF4
SHA1	E5DA4AB6366C5690DFD1BB386C7FE0C78F6ED54F, 7F28AD5EE9966410B15CA85B7FACB70088A17C5F
SHA256	7353AB9670133468081305BD442F7691CF2F2C1136F09D95084005 46C417833A, 59A37D7D2BF4CFFE31407EDD286A811D9600B68FE757829E30DA4 394AB65A4CC
Domains	detankzone[.]com, ccwaterfall[.]com

Patch Link

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

References

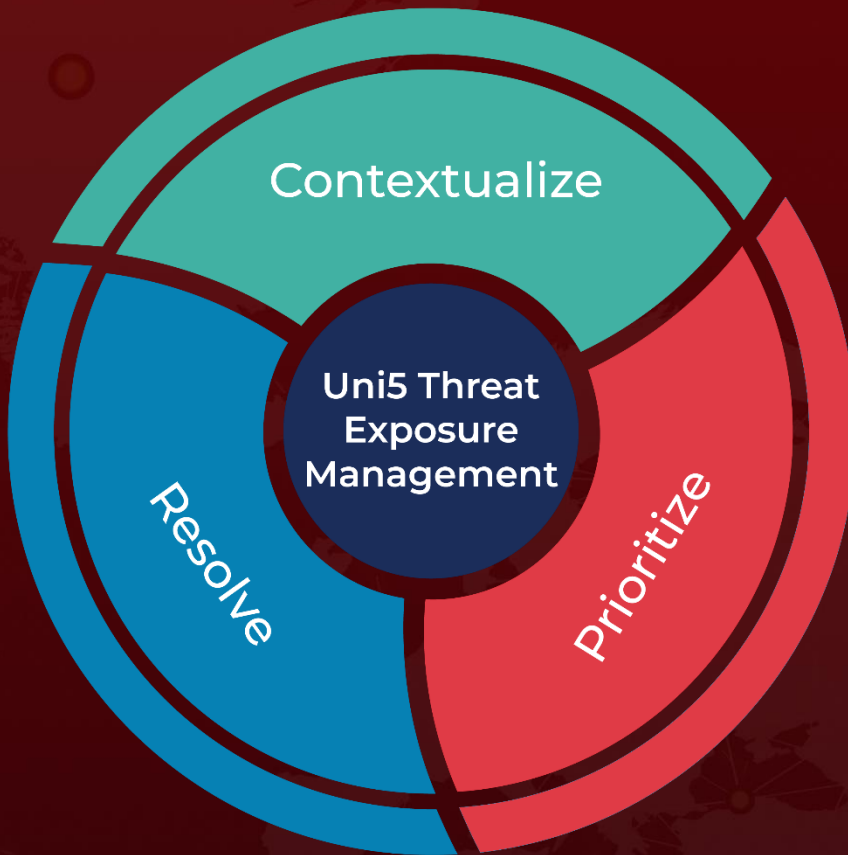
<https://securelist.com/lazarus-apt-steals-crypto-with-a-tank-game/114282/>

<https://www.hivepro.com/threat-advisory/yet-another-google-chrome-zero-day-exploited-in-the-wild/>

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

October 25, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com