Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

New Variant of RUSTBUCKET Malware Targeting Cryptocurrency Providers

Date of Publication	Admiralty Code	TA Number
July 06, 2023	A1	TA2023288

Summary

First appeared: May 11, 2023
Attack Region: Worldwide
Actor Name: Lazarus
Affected Platform: macOS
Malware: RUSTBUCKET
Targeted Industry: Cryptocurrency
Attack: The RUSTBUCKET malware family is actively developing, adding persistence capabilities, while the REF9135 operation by the DPRK targets cryptocurrency service providers.

Attack Regions

Lazarus
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

The RUSTBUCKET malware family is undergoing active development, incorporating new persistence capabilities and focusing on reducing its signature detection. This variant of RUSTBUCKET specifically targets macOS systems.

#2

The REF9135 cybercrime and espionage operation was attributed to the Lazarus Group operated by the Democratic People's Republic of North Korea (DPRK). The DPRK continues to engage in financially motivated attacks against cryptocurrency service providers.

#3

The execution flow of REF9135 is described in three stages. In Stage 1, an AppleScript is used to initiate the download of the Stage 2 binary from the command and control (C2) server. Stage 2 involves the execution of the downloaded binary, which communicates with the C2 server and prepares for the execution of Stage 3. In Stage 3, the malware gathers system information, establishes a connection to the C2 server, and waits for commands.

#4

Persistence mechanisms used by the updated RUSTBUCKET sample involve the creation of LaunchAgents and the copying of the malware's binary to specific paths. By adding a plist file and modifying launch configurations, the malware ensures its execution upon user login.

#5

This analysis connects the RUSTBUCKET campaign, previously attributed to the BlueNorOff group, with the Lazarus Group and the DPRK. The BlueNorOff group has a history of financially motivated attacks, with their most notable operation being the Bangladesh Bank cyber heist.

#6

The networking infrastructure of REF9135 involves multiple C2 domains, including starbucls[.]xyz, jaicvc[.]com, and crypto.hondchain[.]com. The campaign owners exhibit defense evasion techniques, such as monitoring their payload staging infrastructure and changing C2 domains to evade detection.

#7

The victimology of REF9135 points to a venture-backed cryptocurrency company operating in the European Union. This aligns with previous reports of BlueNorOff targeting organizations with access to significant amounts of cryptocurrency.

Recommendations

Utilize a robust endpoint protection solution and prevent RUSTBUCKET malware variants, providing real-time protection against known and unknown threats.

Apply strong access controls, including multi-factor authentication and privileged access management, and implement continuous monitoring to detect and respond to suspicious activities promptly, reducing the potential impact of REF9135 or similar threats.

Regularly train employees on security best practices, emphasizing the risks of phishing attacks and malicious downloads, to minimize the likelihood of falling victim to attacks by the Lazarus Group or other threat actors.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	**TA0011** Command and Control	**TA0005** Defense Evasion	**TA0002** Execution
TA0007 Discovery	**TA0001** Initial Access	**TA0009** Collection	**TA0008** Lateral Movement
TA0011 Command and Control	**T1071.001** Web Protocols	**T1071** Application Layer Protocol	**T1106** Native API
T1059 Command and Scripting Interpreter	**T1647** Plist File Modification	**T1547** Boot or Logon Autostart Execution	**T1082** System Information Discovery
T1218 System Binary Proxy Execution	**T1102** Web Service	**T1566** Phishing	**T1036** Masquerading
T1105 Ingress Tool Transfer	**T1204** User Execution		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a, 1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6, 9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747, 7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387, ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41, de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500, 4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16, fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69, 7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8
Domains	webhostwatto.work[.]gd, crypto.hondchain[.]com, starbucls[.]xyz, jaicvc[.]com, docsend.linkpc[.]net, companydeck[.]online
IPV4	104.168.167[.]88, 64.44.141[.]15

References

https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket

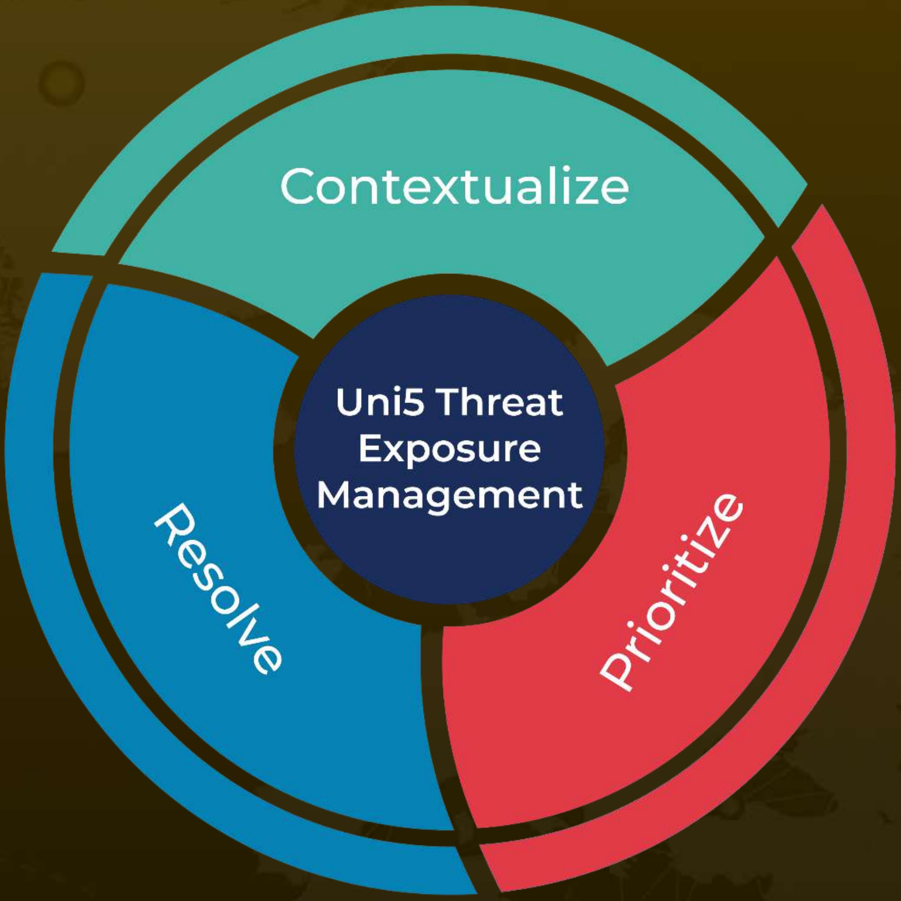
https://twitter.com/ESETresearch/status/1656385173968019456?s=20

https://www.hivepro.com/new-macos-malware-rustbucket-attributed-to-north-korean-group-bluenoroff/

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

July 06, 2023 • 00:30 AM

More at www.hivepro.com