Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

North Korean Hackers Embed Malicious Code in Legitimate npm Packages

Date of Publication	Admiralty Code	TA Number
August 7, 2024	A1	TA2024300

Summary

Attack Discovered: July 2024
Attack Region: Worldwide
Threat Actor: Moonstone Sleet (aka Stressed Pungsan, Storm-1789)
Attack: The North Korea-linked threat actor group, known as "Stressed Pungsan," has been actively distributing malicious npm packages on the package registry. This campaign primarily targets Windows systems, achieving data exfiltration, credential theft, and lateral movement within compromised networks by infiltrating with malicious npm packages. The activities of "Stressed Pungsan" closely align with those of the MOONSTONE SLEET group.

Attack Regions

Attack Details

#1 North Korea-linked threat actor Stressed Pungsan continue to push malicious npm packages to the JavaScript package registry to infect Windows systems. "Stressed Pungsan" closely aligns with the threat actor known as MOONSTONE SLEET, sharing similar TTPs, malicious packages, and C2 infrastructure.

#2 These packages act as initial entry points for malware, enabling data exfiltration, credential theft, and lateral movement within targeted networks. Researchers identified a npm user named nagasiren978 who uploaded two malicious packages, "harthat-hash" and "harthat-api," which then downloaded additional malware from a suspected North Korean C2 server.

#3 The malicious npm package `harthat-api` mimics the legitimate `Hardhat` package by using a similar name. While the code is sourced from the reputable `node-config` repository, the malicious package modifies the `package.json` file to remove the preinstall script and renames the package to `config`. It also includes two additional files, `deference.js` and `pk.json`.

#4 The preinstall script executes the deference.js file, which generates a batch file that first checks for a Windows execution environment before proceeding with further execution. The threat actor uses `curl` to download a file named `Temp.b`, which is renamed to `package.db`, a Windows DLL. The script leverages the `rundll32.exe` executable to load and execute the DLL, bypassing system defenses by using this trusted system binary. After executing the payload, the script deletes the DLL file and replaces the `package.json` file, restoring the original content from the `node-config` project.

#5 An analysis of the discovered DLL revealed it to be incomplete and devoid of any malicious content. However, it did feature anti-debugging and anti-reverse engineering mechanisms, suggesting that the threat actors' final payload is still under development. Threat actors are increasingly using malicious npm packages to compromise targets. This tactic is on the rise, with attackers frequently embedding malicious code within seemingly legitimate packages that mimic existing content.

Recommendations

Vigilant Package Management: Ensure thorough scrutiny of all npm packages prior to installation to prevent introducing malicious code into your environment. Keep a vigilant eye on package installations for any suspicious behavior or anomalies that could indicate a security threat.

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.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0008 Lateral Movement	TA0010 Exfiltration	TA0011 Command and Control	T1189 Drive-by Compromise
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1036 Masquerading	T1218 System Binary Proxy Execution
T1218.011 Rundll32	T1070 Indicator Removal	T1070.004 File Deletion	T1574 Hijack Execution Flow
T1574.002 DLL Side-Loading	T1071 Application Layer Protocol	T1071.001 Web Protocols	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	142[.]111[.]77[.]196
SHA256	d2a74db6b9c900ad29a81432af72eee8ed4e22bf61055e7e8f7a5f1a33778277

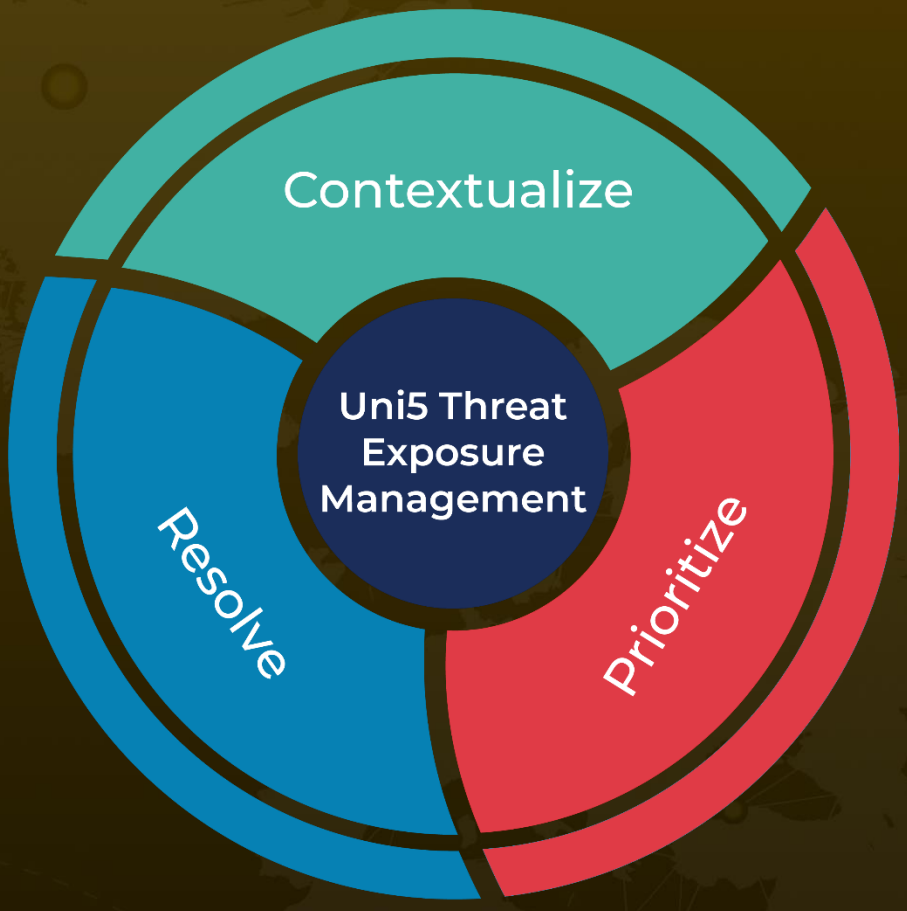
References

https://securitylabs.datadoghq.com/articles/stressed-pungsan-dprk-aligned-threat-actor-leverages-npm-for-initial-access/

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

August 7, 2024 • 7:30 AM

More at www.hivepro.com