Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

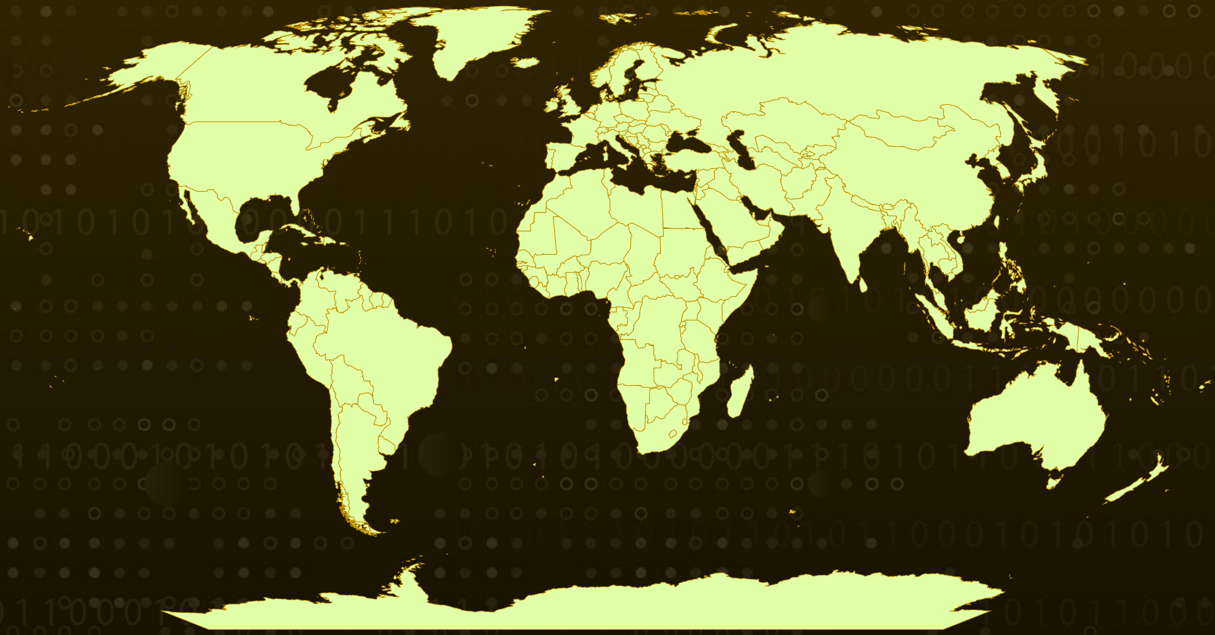
Malicious npm Packages Target WhatsApp Developers with Kill Switch

Date of Publication	Admiralty Code	TA Number
August 8, 2025	A1	TA2025243

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Targeted Industry: Developers
Attack: Two malicious npm packages, naya-flore and nvlore-hsc, have been uncovered targeting developers building WhatsApp integrations. Masquerading as legitimate socket libraries, these packages secretly contain a remote-controlled kill switch that wipes a developer's system if their phone number isn't found in a whitelist stored on a GitHub repository. When an unapproved number is detected, the package silently executes a destructive command that deletes all files. Although the code also includes functionality for device data exfiltration, it appears the attacker ultimately focused on system destruction. This incident marks a troubling shift in supply chain attacks, demonstrating a new level of precision where even niche developer communities are being deliberately and selectively targeted.

Attack Regions



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

Attack Details

#1 Two malicious npm packages, naya-flore and nvlore-hsc, have been discovered targeting developers building WhatsApp API integrations. Disguised as legitimate socket libraries, they were published by the npm user nayflore and have collectively received over 1,100 downloads. Beneath their seemingly harmless functionality, these packages hide a remote kill switch designed to wipe developers' systems. Their strategic use of familiar naming and coding patterns helped them evade suspicion and remain active on the npm registry.

#2 At the heart of the attack is a function named requestPairingCode, typically used during WhatsApp bot authentication. Once called, the function secretly contacts a GitHub-hosted database containing a list of whitelisted phone numbers, with the endpoint obfuscated using Base64 encoding. If the user’s phone number isn’t listed, the function executes a destructive rm -rf * command, erasing the system’s contents. This setup allows the attacker to maintain control over who is spared, enabling selective targeting based on phone number whitelisting.

#3 The packages also include a function named generateCreeds, designed to collect and exfiltrate device information to an external endpoint. Although this code is currently commented out, its full and functional implementation suggests the attacker originally intended to collect data but later narrowed the focus to system destruction. The infrastructure remains active, signaling potential future plans or adaptability in attack strategy. Additionally, naya-flore contains a hardcoded GitHub Personal Access Token, which doesn’t appear to serve a current malicious function but could point to either unfinished features or other avenues of compromise.

#4 To appear trustworthy, both packages mimic the behavior of genuine WhatsApp libraries, using familiar class names and function signatures to lower suspicion. This camouflage ensures that their malicious behavior is only triggered in targeted environments, specifically those not associated with "safe" phone numbers. The attacker has also released several other packages, such as noku-search, very-nay, naya-clone, node-smsk, and @veryflore/disc, which may appear harmless but warrant close scrutiny due to the actor’s malicious track record.

#5 This incident reflects a growing trend in highly targeted supply chain attacks aimed at niche developer communities. By tying the kill switch activation to phone numbers and hosting the control list on GitHub, the attacker demonstrates both technical sophistication and the ability to update targets dynamically without modifying the package itself. It’s a clear reminder that even small developer ecosystems can be in the crosshairs.

Recommendations

Review All Dependencies Carefully: Before using any npm package, especially ones related to WhatsApp or messaging APIs, take a moment to check what it does under the hood. Look for unexpected behaviors like file deletion commands, network requests, or obfuscated code.

Test in a Safe Environment First: Always test new or unfamiliar libraries in a sandbox or isolated development environment. This helps you catch anything suspicious, like unexpected system changes or data access without risking your actual machine or production data.

Avoid Blind Trust in Popularity: Don't assume a package is safe just because it has a few hundred or even a thousand downloads. Attackers often rely on small but strategic targeting, especially within niche developer communities.

Be Wary of Phone Number Usage: If a library asks for your phone number especially for bot authentication double-check what happens to that data. If it's being sent somewhere or used to trigger functionality, investigate further before proceeding.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0010 Exfiltration	**TA0040** Impact	**T1195** Supply Chain Compromise	**T1195.002** Compromise Software Supply Chain
T1027 Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript	**T1485** Data Destruction

T1041 Exfiltration Over C2 Channel	T1082 System Information Discovery	T1036 Masquerading	T1036.005 Match Legitimate Resource Name or Location

Indicators of Compromise (IOCs)

TYPE	VALUE
Malicious Packages	naya-flore, nvlore-hsc
URLs	hxxps[:]//api[.]verylinh[.]my[.]id/running, hxxps[:]//raw[.]githubusercontent[.]com/navaLinh/database/main/seska[.]json
Email	idzzcch@gmail[.]com
GitHub PAT	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

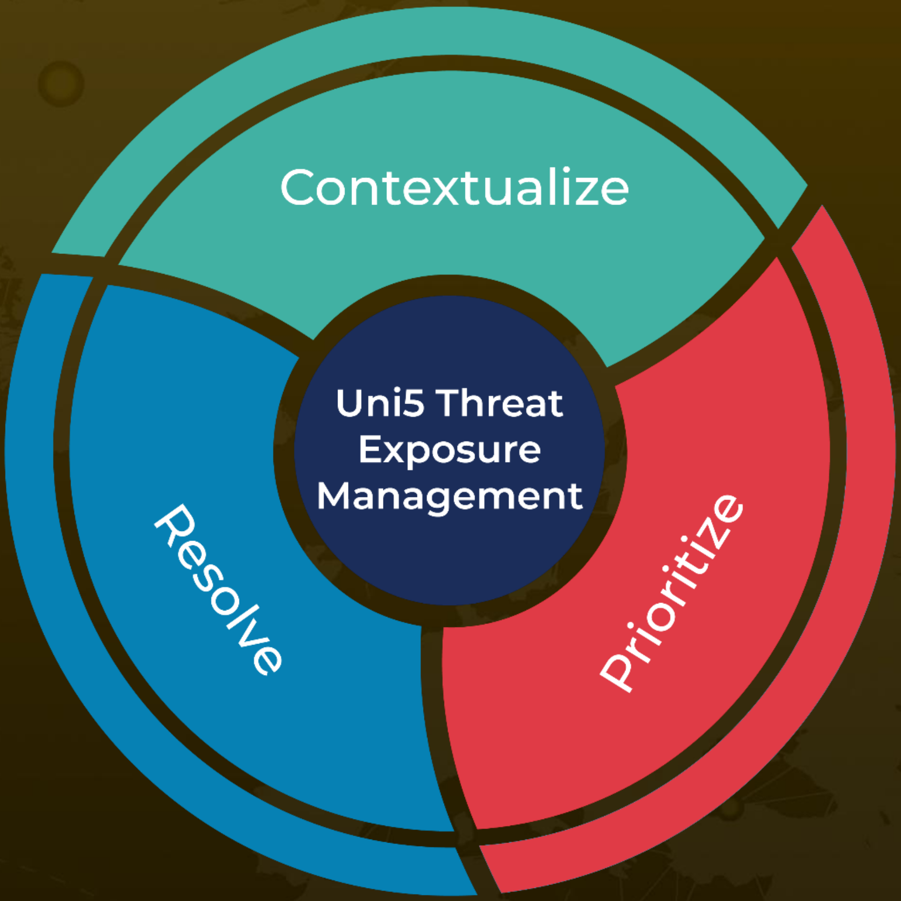
References

https://socket.dev/blog/malicious-npm-packages-target-whatsapp-developers-with-remote-kill-switch

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 8, 2025 • 5:40 AM

More at www.hivepro.com