Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

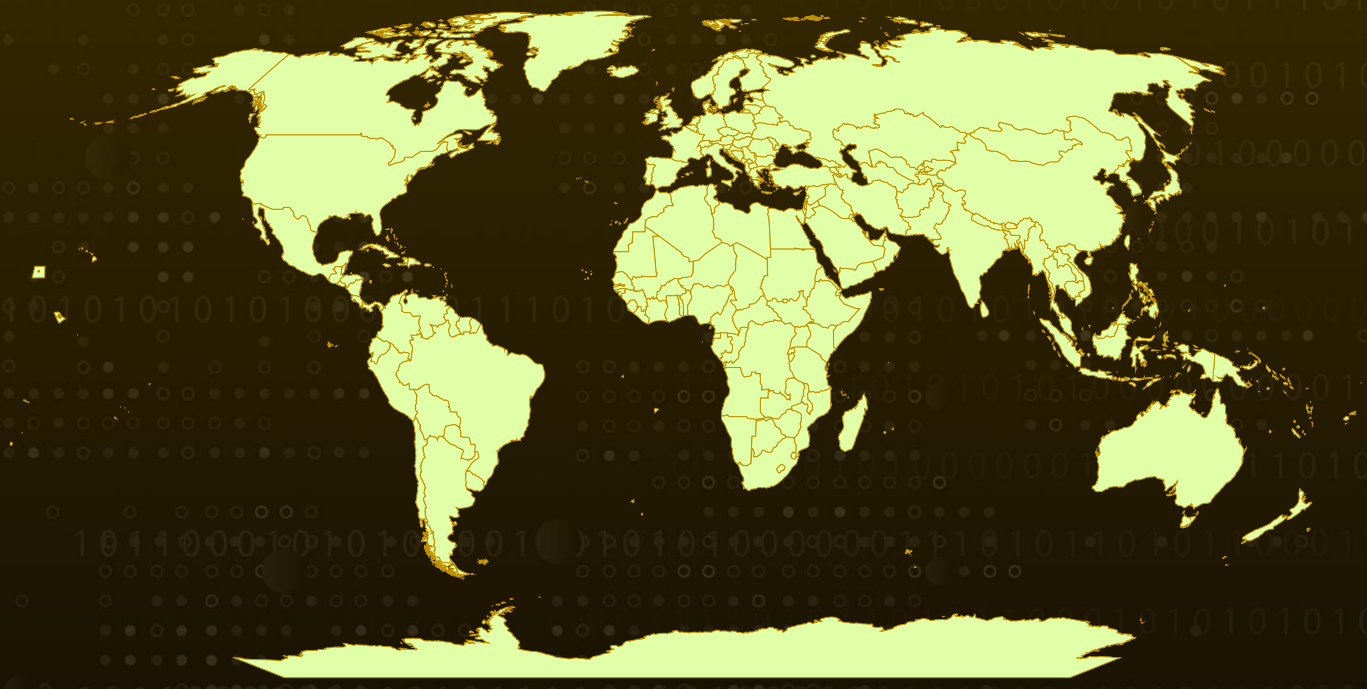
Quasar RAT Hidden in npm Package Targets Ethereum Developers

Date of Publication	Admiralty Code	TA Number
January 2, 2025	A1	TA2025001

Summary

First Seen: December 18, 2024
Targeted Countries: Worldwide
Malware: Quasar RAT
Targeted Industry: Cryptocurrency
Affected Platform: Windows
Attack: A malicious npm package “ethereumvulncontracthandler”, which disguises itself as a tool for detecting Ethereum smart contract vulnerabilities but actually deploys the Quasar Remote Access Trojan (RAT). This malware targets Windows systems, enabling attackers to perform activities like keystroke logging and credential harvesting. To mitigate risks, developers are urged to vet third-party packages and monitor network traffic for unusual activity. The incident emphasizes the need for robust security practices in software supply chains.

Attack Regions



Attack Details

#1

A malicious npm package named “ethereumvulncontracthandler”, which was discovered to be a disguise for the Quasar Remote Access Trojan (RAT). This package was introduced on December 18, 2024, under the alias "solidit-dev-416" and falsely claimed to help developers detect vulnerabilities in Ethereum smart contracts. However, upon installation, it executes a malicious script that targets Windows systems, posing a significant risk to developers in the Ethereum ecosystem.

#2

The Quasar RAT is a well-known tool used in various cybercrime campaigns for nearly a decade. It grants attackers remote access to infected machines, enabling them to perform a range of malicious activities such as keystroke logging, capturing screenshots, harvesting credentials, and exfiltrating files. This is particularly alarming for Ethereum developers who often handle sensitive financial information, making them attractive targets for cybercriminals.

#3

One of the notable aspects of this attack is the sophisticated obfuscation techniques employed by the threat actor. The malicious package uses layers of encoding, including Base64 and XOR, to hide its true purpose and evade detection by security tools. Additionally, the package includes checks to ensure it does not run in automated environments, which helps it avoid scrutiny during analysis and increases its chances of infecting targeted systems.

#4

Once installed, the Quasar RAT establishes persistence on the infected machine by modifying the Windows registry to ensure it runs at startup under the name client.exe. This allows the malware to maintain its presence even after system reboots, enabling continuous access for the attacker. The RAT communicates with a command-and-control server for further instructions and data exfiltration, making it a formidable threat.

Recommendations

Verify Package Sources: Only install dependencies from trusted and verified sources. Check for community reviews and recent activity on the repository. Prefer packages with a strong user base, regular updates, and active maintenance.

Use Dependency Scanning Tools: Employ tools like npm audit, or other security scanners to detect vulnerabilities and malicious code. Set up automated alerts for new vulnerabilities in dependencies to stay informed.

Minimize Permissions: Run development environments with restricted privileges to limit the impact of a potential compromise.

Monitor Network Traffic: Regularly monitor network traffic for unusual outbound connections that may indicate compromised systems. Implement IDS to detect and respond to suspicious activities in real-time.

Audit Dependencies: Regularly perform dependency audits using tools like npm audit or third-party scanners to identify vulnerabilities in packages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control	TA0005 Defense Evasion
TA0040 Impact	TA0010 Exfiltration	TA0006 Credential Access	TA0009 Collection
T1195.002 Compromise Software Supply Chain	T1059.007 JavaScript	T1036.005 Match Legitimate Name or Location	T1027 Obfuscated Files or Information
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1546.016 Installer Packages	T1105 Ingress Tool Transfer

T1547.001 Registry Run Keys / Startup Folder	T1113 Screen Capture	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1056.001 Keylogging	T1056 Input Capture	T1005 Data from Local System	T1070 Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9c3d53c7723bfdd037df85de4c26efcd5e6f4ad58cc24f7a38a774bf22de3876
URL	Hxxps[://]jujuju[.]lat/files/kk[.]cmd
Domain	captchacdn[.]com[:]7000
IPv4	154[.]216[.]17[.]47

References

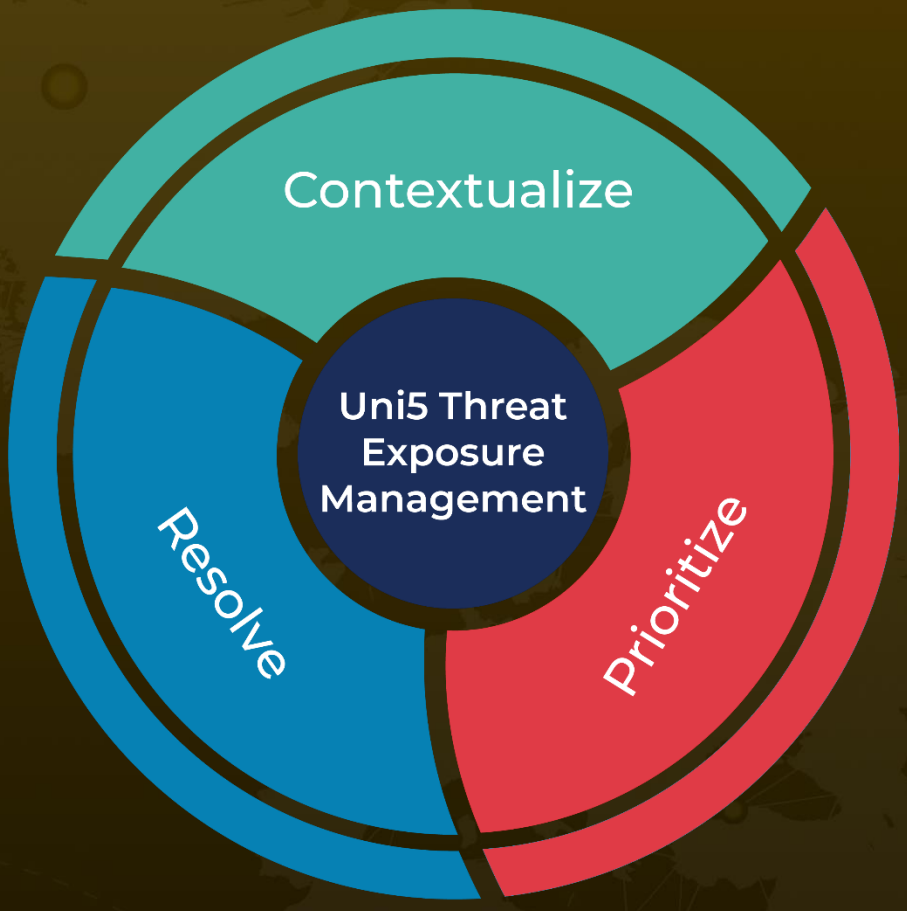
https://socket.dev/blog/quasar-rat-disguised-as-an-npm-package

https://www.hivepro.com/quasar-rat-utilizes-dll-side-loading-to-evade-detection/

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

January 2, 2025 • 11:00 PM

More at www.hivepro.com