Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

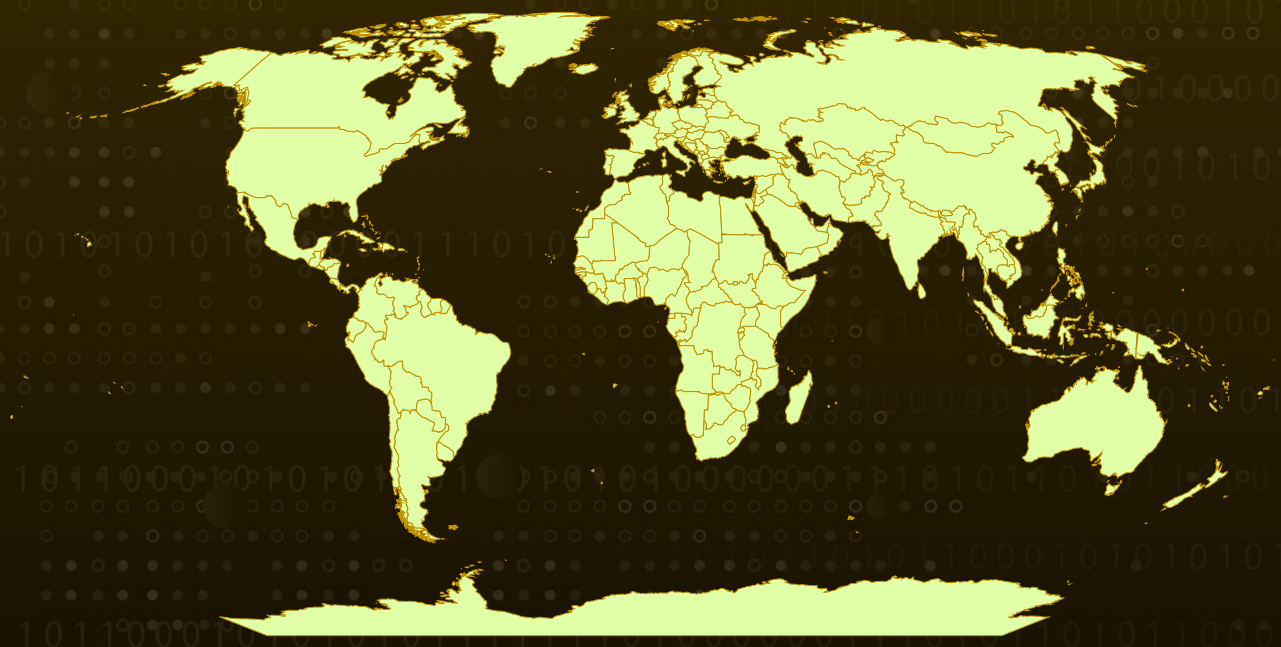
SleepyDuck: Trojan Nesting in the Open VSX Marketplace

Date of Publication	Admiralty Code	TA Number
November 6, 2025	A1	TA2025336

Summary

Attack Discovered: October 31, 2025
Targeted Countries: Worldwide
Malware: SleepyDuck
Affected Platform: Windows
Attack: A new threat called SleepyDuck has quietly infiltrated the Open VSX marketplace, disguising itself as a trusted Solidity extension to target developers. What seemed like a harmless coding tool quickly turned malicious after thousands of downloads, transforming into a stealthy remote access trojan. Once activated, it collects system data, evades sandbox detection, and communicates with its command server every few seconds. What makes SleepyDuck particularly dangerous is its clever use of the Ethereum blockchain to maintain control even if its main server goes offline, making it highly resilient and difficult to disrupt. This incident highlights a growing trend of supply chain attacks that exploit developer trust, proving that even familiar tools in coding environments can harbor hidden threats.

Attack Regions



Attack Details

#1 A newly discovered remote access trojan (RAT) named SleepyDuck has surfaced in the Open VSX IDE extension marketplace, masquerading as a legitimate Solidity extension. The malicious extension, juan-bianco.solidity-vlang, was initially released on October 31 as a seemingly safe tool but was quietly updated to version 0.0.8 on November 1, introducing malicious capabilities after it had already accumulated over 14,000 downloads. SleepyDuck stands out for its advanced sandbox evasion techniques and its use of an Ethereum smart contract that allows it to dynamically update its command-and-control (C2) server address if the original is taken down, ensuring persistent control.

#2 SleepyDuck activates whenever a user opens a new code editor window or selects a .sol (Solidity) file. It leverages the extension.js entry point, a commonly exploited mechanism, to disguise itself as a legitimate helper extension. However, its true purpose is revealed through an activation function that creates a lock file, ensuring the malware runs only once before executing a fake webpack.init() function containing malicious logic. Upon initialization, SleepyDuck performs four core operations: it determines the fastest Ethereum RPC provider, initializes itself, fetches an updated configuration, and begins communicating with its default C2 server at sleepyduck.xyz, polling every 30 seconds for instructions.

#3 During this setup process, SleepyDuck gathers sensitive system details, such as the hostname, username, MAC address, and timezone, which helps it evade detection in sandboxed environments. It then constructs a controlled JavaScript environment using vm.createContext(sandbox), allowing it to safely execute remote commands. The malware continuously exchanges data with the C2 serversending system details and awaiting further commands that may instruct it to download payloads, exfiltrate files, or perform system manipulations.

#4 To maintain resilience, SleepyDuck is equipped with a clever fallback mechanism that ensures continued communication even if its primary server goes offline. It embeds a reference to a smart contract on the Ethereum blockchain, which contains alternative RPC addresses and configuration data. If the C2 at is unavailable, the malware queries the contract, allowing it to update its command server, adjust polling intervals, or execute emergency commands across infected hosts. This use of blockchain-based infrastructure provides decentralized redundancy, making takedowns significantly more challenging.

#5 The sleepyduck.xyz domain was registered on November 1, 2025, a day after the associated Ethereum contract was deployed, indicating how rapidly the threat was put into motion. Analysts warn that despite SleepyDuck's sophisticated design, much of its code remains unobfuscated and unminified, suggesting it may still be in its early stagesand that similar threats could proliferate on Open VSX and Visual Studio marketplaces.

Recommendations

Verify Extensions Before Installing: Only download and install IDE extensions from trusted publishers with verified accounts. Always review the publisher's history, ratings, and download trends before adding any new tool, especially if it imitates popular extensions like Solidity helpers.

Audit and Remove Suspicious Extensions: If you've already installed the affected extension (juan-bianco.solidity-vlang), remove it immediately and run a full antivirus or endpoint security scan. Developers should also regularly review their installed extensions to ensure no unauthorized or unknown plugins are present.

Monitor for Unusual Activity: Watch for strange network traffic, especially outbound connections to unknown domains such as sleepyduck.xyz, and check for processes that launch unexpectedly when editing or opening files. Network monitoring tools or EDR solutions can help detect these anomalies early.

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
TA0011 Command and Control	**T1195** Supply Chain Compromise	**T1497** Virtualization/Sandbox Evasion	**T1082** System Information Discovery
T1027 Obfuscated Files or Information	**T1033** System Owner/User Discovery	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript
T1036 Masquerading	**T1071** Application Layer Protocol		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	sleepyduck[.]xyz
Ethereum address	0xDAfb81732db454DA238e9cFC9A9Fe5fb8e34c465

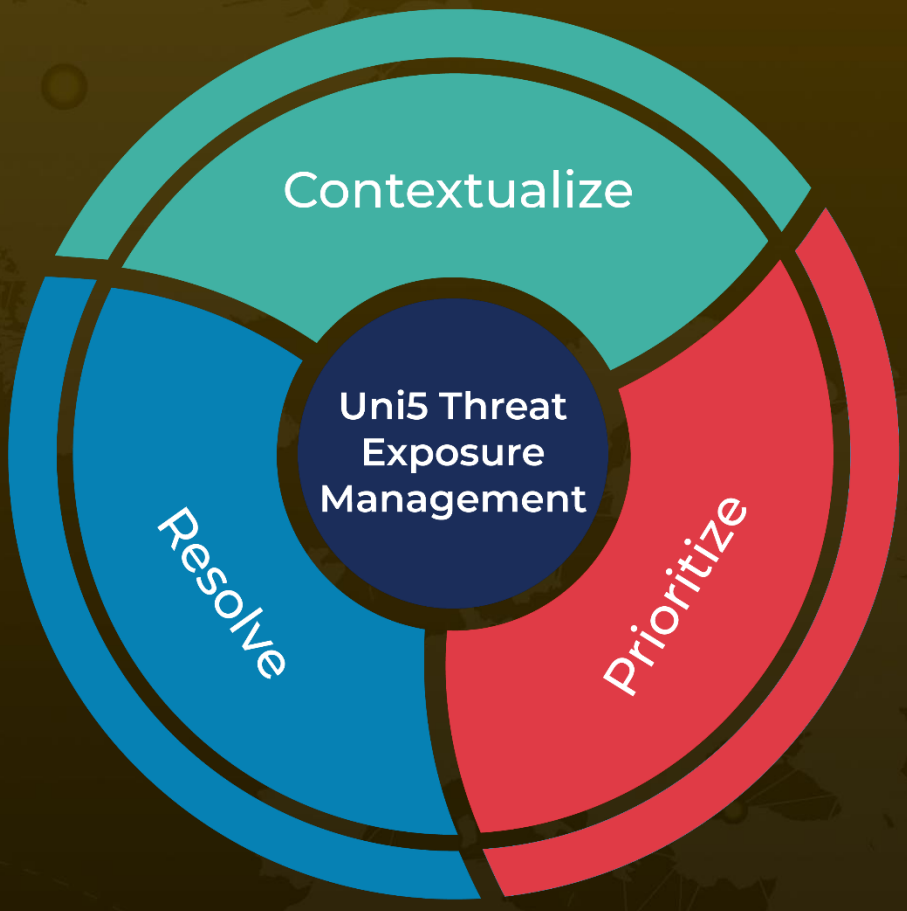
References

https://secureannex.com/blog/sleepyduck-malware/

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

November 6, 2025 • 4:00 AM

More at www.hivepro.com