Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

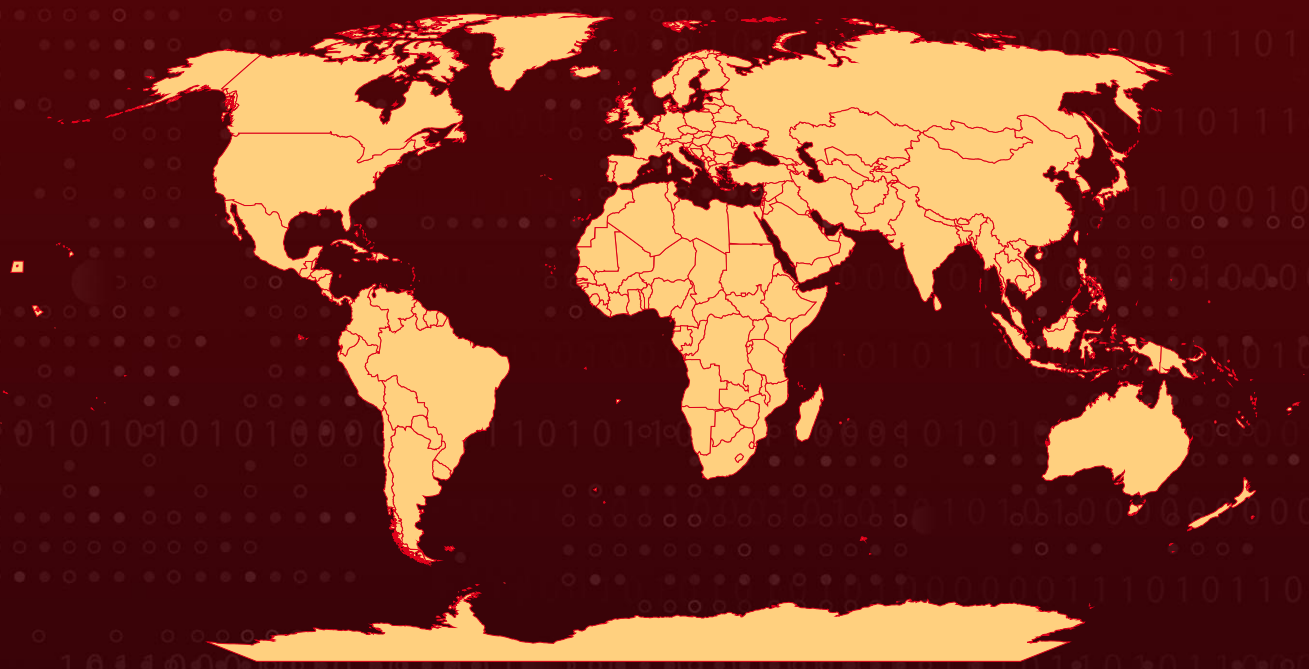
s1ngularity Nx Supply Chain Attack: AI-Driven Credential Theft & Mass Exposure

Date of Publication	Admiralty Code	TA Number
September 9, 2025	A1	TA2025274

Summary

First Seen: August 26, 2025
Targeted Countries: Worldwide
Targeted Platforms: npm ecosystem, GitHub repositories
Attack: The s1ngularity attack on the Nx supply chain exposed thousands of secrets and repositories by injecting malware into npm packages through a compromised GitHub Action. The malware harvested tokens, exfiltrated files, and even weaponized AI CLI tools to automate reconnaissance and data theft, making over 6,700 private repos public and leaking sensitive data from 1,700+ users. With many stolen tokens remaining valid for days, the incident highlights how AI-powered techniques are reshaping supply chain attacks and underscores the urgent need for stronger monitoring, artifact visibility, and defenses against AI-driven threats.

Attack Regions



Attack Details

#1

The s1ngularity attack was a large-scale supply chain compromise that targeted the Nx ecosystem in late August 2025. Attackers exploited a vulnerable GitHub Action to steal npm publishing tokens, which they used to inject malware into popular Nx package versions. Once installed, the malware collected environment variables, GitHub and npm tokens, and even leveraged local AI command-line tools to identify and exfiltrate sensitive files. The stolen data was published into public repositories under the attacker's naming scheme, creating widespread exposure.

#2

The attack unfolded in multiple phases. First, malicious packages were distributed through the compromised npm channel, impacting thousands of developers. Next, with stolen GitHub tokens, attackers flipped private repositories to public and renamed them to "s1ngularity-repository," exposing sensitive code and assets. Finally, a later stage of the campaign showed more focused targeting of individual organizations, with compromised accounts publishing sensitive repositories under the attacker's branding.

#3

The impact was significant, over 1,700 users had secrets exposed, with more than 20,000 files exfiltrated and at least 6,700 private repositories turned public. Many GitHub tokens remained valid for days after the leak, giving attackers extended access until a GitHub-led revocation effort reduced the risk. Some organizations faced severe exposure, with hundreds of repositories suddenly made visible to the public. This made the incident one of the most destructive recent supply chain compromises.

#4

What made this attack stand out was its use of AI-powered malware. The malicious code invoked local AI CLI tools with insecure flags (like --yolo and --trust-all-tools) to dynamically decide which files to steal, enabling more adaptive and evasive attacks. This blending of supply chain compromise with AI-assisted reconnaissance sets a worrying precedent for future threats.

Recommendations

Identify Exposure and Rotate Credentials: If you installed compromised Nx versions (nx 20.9.0–20.12.0, 21.5.0–21.8.0; @nx/enterprise-cloud 3.2.0; @nx/devkit 20.9.0, 21.5.0; @nx/workspace 20.9.0, 21.5.0; @nx/js 21.5.0; @nx/eslint 21.5.0; @nx/key 3.2.0; @nx/node 20.9.0, 21.5.0), treat your environment as compromised. Immediately revoke and rotate all GitHub tokens, npm tokens, SSH keys, API keys, and environment secrets. Check shell configs (.bashrc/.zshrc) for malicious modifications.

Remediation Steps if Compromised: Delete the node_modules folder, clear npm cache, and reinstall only safe versions after removing affected dependencies from lockfiles. Inspect and clean shell configs to remove injected shutdown commands. Delete suspicious files like /tmp/inventory.txt, and investigate any GitHub repositories named "s1ngularity-repository" for leaked results before removing them.

Audit GitHub Activity and Repositories: Review audit logs for sudden repository creations with "s1ngularity" naming, unexpected changes from private to public visibility, or abnormal GitHub Actions activity. Enable long-term log retention and feed logs into SIEM to improve monitoring and correlation. Treat any anomalies as indicators of compromise requiring immediate investigation.

Harden Supply Chain Security: Adopt npm Trusted Publishers to eliminate static publishing tokens and enforce least-privilege workflows in GitHub Actions. Pin both dependencies and GitHub Actions to known good versions or commit SHAs. Maintain Software Bills of Materials (SBOMs) for all projects to quickly track and assess exposure when incidents occur.

Build AI-Aware Defense Posture: Assume attackers will leverage AI-assisted reconnaissance; update threat models to account for adaptive and automated TTPs. Restrict installation and execution of unvetted AI CLI tools in developer environments. Train security teams to recognize AI-powered attack patterns, including exfiltration disguised as legitimate AI tool queries.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0010 Exfiltration
TA0005 Defense Evasion	TA0040 Impact	TA0006 Credential Access	TA0009 Collection
T1195 Supply Chain Compromise	T1059 Command and Scripting Interpreter	T1195.002 Compromise Software Supply Chain	T1036 Masquerading
T1027 Obfuscated Files or Information	T1586 Compromise Accounts	T1552.007 Container API	T1552.001 Credentials In Files
T1552 Unsecured Credentials	T1083 File and Directory Discovery	T1005 Data from Local System	T1567 Exfiltration Over Web Service
T1584 Compromise Infrastructure	T1204 User Execution	T1078 Valid Accounts	T1567.002 Exfiltration to Cloud Storage
T1518 Software Discovery	T1204.002 Malicious File	T1213 Data from Information Repositories	T1565 Data Manipulation
TA0007 Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
File name	/tmp/inventory[.]txt, /tmp/inventory[.]txt[.]bak
Ethereum Address	0xFc4a4858bafef54D1b1d7697bfb5c52F4c166976

References

https://socket.dev/blog/nx-packages-compromised

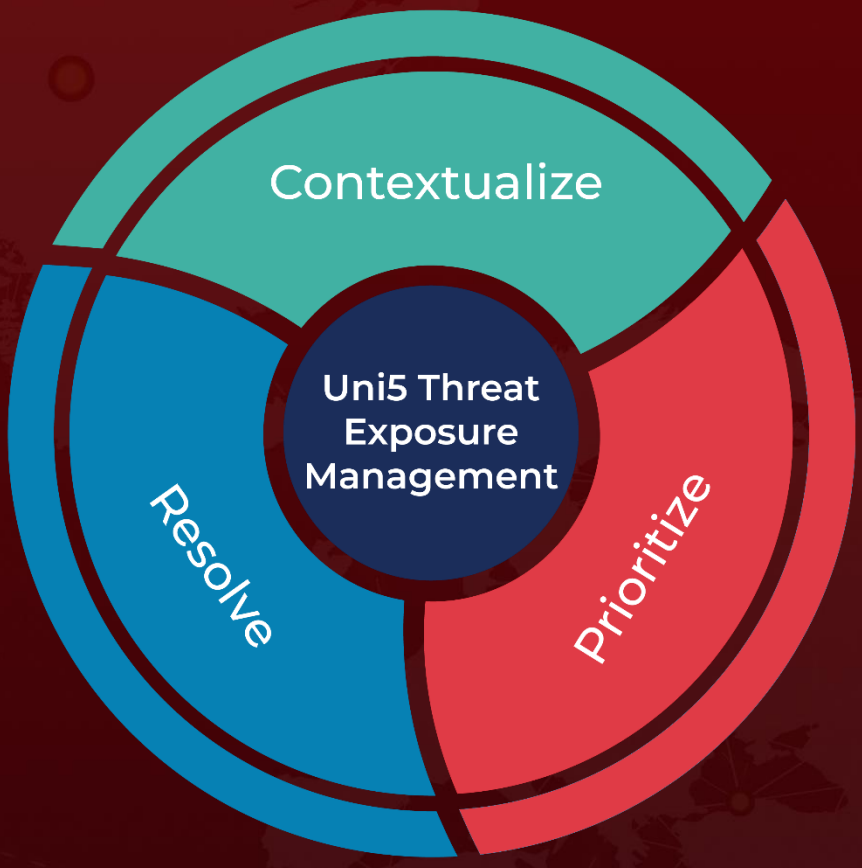
https://www.stepsecurity.io/blog/supply-chain-security-alert-popular-nx-build-system-package-compromised-with-data-stealing-malware

https://www.upwind.io/feed/npm-supply-chain-attack-massive-compromise-of-debug-chalk-and-16-other-packages

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

September 9, 2025 • 6:30 AM

More at www.hivepro.com