unit42.paloaltonetworks.com /npm-supply-chain-attack/

"Shai-Hulud" Worm Compromises npm Ecosystem in Supply Chain Attack

Unit 42 ⋮ ⋮ 9/17/2025

Executive Summary

Palo Alto Networks Unit 42 is investigating an active and widespread software supply chain attack targeting the Node Package Manager (npm) ecosystem. A novel, self-replicating worm, which is currently being tracked as "Shai-Hulud," is responsible for the compromise of over 180 software packages.

This attack represents a significant evolution in supply chain threats, leveraging automated propagation to achieve scale. Unit 42 also assesses with moderate confidence that an LLM was used to generate the malicious bash script, based on inclusion of comments and emojis.

Palo Alto Networks customers are better protected from, and receive mitigations for aspects of this attack, through various products and services, including:

- Cortex Cloud
- Prisma Cloud
- Cortex XDR and XSIAM
- Advanced WildFire

The Unit 42 Incident Response team can also be engaged to help with a compromise or to provide a proactive assessment to lower your risk.

Related Unit 42 Topics **Supply Chain**, Credential Harvesting, **Phishing**, **JavaScript**

Background on npm Packages and the Supply Chain

The attack may originate from a credential-harvesting phishing campaign spoofing npm and asking developers to “update” their multi-factor authentication (MFA) login options. Once initial access was gained, the threat actor deployed a malicious payload that functions as a worm, initiating a multi-stage attack sequence. Based on the inclusion of comments and emojis in the bash script, Unit 42 assesses with moderate confidence the threat actor leveraged LLM to assist in writing the malicious code.

The malicious package versions contain a worm that executes a post-installation script. This malware scans the compromised environment for sensitive credentials, including:

- .npmrc files (for npm tokens)
- Environment variables and configuration files specifically targeting GitHub Personal Access Tokens (PATs) and API keys for cloud services like:
    - Amazon Web Services (AWS)
    - Google Cloud Platform (GCP)
    - Microsoft Azure

Harvested credentials are exfiltrated to an actor-controlled endpoint. The malware programmatically creates a new public GitHub repository named "Shai-Hulud" under the victim's account and commits the stolen secrets to it, exposing them publicly.

Using the stolen npm token, the malware authenticates to the npm registry as the compromised developer. It then identifies other packages maintained by that developer, injects malicious code into them, and publishes the new, compromised versions to the registry. This automated process allows the malware to spread exponentially without direct actor intervention.

Current Scope of the Attack

The scope of the compromise is extensive, impacting numerous packages, including the widely used @ctrl/tinycolor library, which receives millions of weekly downloads.

Credential theft from this campaign can lead directly to compromise of cloud services (such as AWS, Azure, GCP), leading to data theft from storage buckets, ransomware deployment, cryptomining or deletion of production environments. It may also lead to direct database theft and hijacking of third-party services for phishing. Additionally, stolen SSH keys can enable lateral movement within compromised networks.

Interim Guidance

1. Credential Rotation: Immediately rotate all developer credentials. This includes npm access tokens, GitHub PATs and SSH keys, and all programmatic access keys for cloud and third-party services. Assume that any secret present on a developer's machine may have been compromised.
2. Dependency Auditing: Conduct a thorough and immediate audit of all project dependencies. Use tools like npm audit to identify vulnerable package versions. Scrutinize your project's package-lock.json or

yarn.lock files to ensure you are not using any of the known-compromised packages. Remove or update affected dependencies immediately.

3. GitHub Account Security Review: All developers should review their GitHub accounts for unrecognized public repositories (specifically "Shai-Hulud"), suspicious commits or unexpected modifications to GitHub Actions workflows that could establish persistence.
4. Enforce MFA: Ensure that MFA is strictly enforced on all developer accounts, particularly for critical platforms like GitHub and npm, to prevent credential abuse.

Unit 42 Managed Threat Hunting Queries

```
// Description: Reports indicate only Linux+Mac is targeted due to an os.platform() check, ensure agent coverage on these devices

dataset = endpoints

| filter endpoint_status in (ENUM.CONNECTED, ENUM.DISCONNECTED)

| comp count() by platform
```

```
// Description: Check for connections to any webhook.site domains in raw NGFW URL logs. Optional filter for specific URI observed in use by threat actor.

dataset = panw_ngfw_url_raw

| filter lowercase(url_domain) contains "webhook.site"

| alter susp_uri = if(uri contains "bb8ca5f6-4175-45d2-b042-fc9ebb8170b7")

// Optional filter:

// | filter susp_uri = true

| fields url_domain, uri, susp_uri, *
```

```
// Description: Check for connections to any webhook.site domains in XDR telemetry. Optional filter for specific URI observed in use by threat actor.

dataset = xdr_data

| filter event_type = STORY

| filter lowercase(dst_action_external_hostname) contains "webhook.site" or lowercase(dns_query_name) contains "webhook.site"

| fields agent_hostname, dst_action_external_hostname, dns_query_name
```

```
// Description: Detect malicious YAML file

dataset = xdr_data

| filter event_type = FILE and action_file_name = "shai-hulud-workflow.yml" and agent_os_type in (ENUM.AGENT_OS_MAC, ENUM.AGENT_OS_LINUX)

| fields agent_hostname, actor_effective_username, action_file_name, action_file_path, actor_process_image_name, actor_process_command_line
```

```
// Description: Detects Trufflehog usage. Legitimate tool abused by threat actor for secrets discovery. False positives may occur if there is legitimate use.

dataset = xdr_data

| filter event_type = PROCESS and lowercase(action_process_image_command_line) contains "trufflehog"

| fields agent_hostname, actor_effective_username, actor_process_command_line, action_process_image_command_line
```

```
// Description: Detect malicious bundle.js file

config case_sensitive = false

| dataset = xdr_data

| filter event_type = FILE and action_file_sha256 =
"46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09"

| fields agent_hostname, action_file_name, action_file_path, event_type, event_sub_type,
actor_process_image_name, actor_process_command_line
```

Conclusion

The Shai-Hulud worm represents a significant escalation in the ongoing series of NPM attacks targeting the open-source community. This follows recent incidents such as the s1ngularity/Nx compromise, which involved credential theft and exposed private repositories, and a widespread NPM phishing campaign observed in September 2024.

Its self-replicating design is particularly notable, effectively combining credential harvesting with an automated dissemination mechanism that exploits maintainers' existing publishing rights to proliferate across the ecosystem. Furthermore, we have observed the integration of AI-generated content within the Shai-Hulud campaign, a development that follows the s1ngularity/Nx attack's explicit weaponization of AI command-line tools for reconnaissance. This signifies the ever-evolving threat from malicious actors exploiting AI for malicious activity, accelerating secret sprawl.

The consistent and refined nature of these attack methodologies underscores a growing threat to open-source software supply chains. These attacks are propagating at the speed of Continuous Integration and Continuous Delivery (CI/CD), which poses long-lasting and increasing security challenges for the entire ecosystem.

Palo Alto Networks has shared our findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Palo Alto Networks Product Protections and Detections for npm Packages Supply Chain Attacks

Palo Alto Networks customers can leverage a variety of product protections, services and updates designed to identify and defend against this threat.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107

Advanced WildFire

The Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of indicators associated with this threat.

Cortex XDR and XSIAM

Cortex XDR and XSIAM agents help protect against the threats described in this article. The agents prevent the execution of known malicious malware and may also prevent the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.

Cortex Cloud

Cortex Cloud published a detailed blog post describing how Cortex Cloud can be used for detecting and preventing supply chain attacks.

Prisma Cloud

Prisma Cloud can help detect the use of the malicious packages and recognize misconfigurations in the pipelines that might lead customers to use untested/unsanctioned OSS package versions. However, the scanner is designed for detection of vulnerabilities, license issues and operational risks, and not for detecting malicious code on new packages. It is important to investigate relevant CI/CD alerts and ensure your applications are not using unsanctioned versions of npm packages.

Indicators of Compromise

- 46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09
- b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777
- dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c
- 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db

- hxxps://webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7

Additional Resources

- Breakdown: Widespread npm Supply Chain Attack Puts Billions of Weekly Downloads at Risk – Palo Alto Networks