29 September 2025

EMERGING THREATS

NPM - Shai-Hulud Worm

The "Shai-Hulud" worm represents a significant escalation in software supply chain attacks, particularly within the Node.js ecosystem. Discovered in mid-September 2025, this self-replicating malware has compromised over 500 npm packages, including widely used libraries such as @ctrl/tinycolor and several maintained by CrowdStrike. This worm's primary objective is to harvest developer credentials, such as GitHub Personal Access Tokens (PATs), npm tokens, and cloud service API keys, and exfiltrate them to attacker-controlled endpoints. Additionally, stolen credentials have been observed to be uploaded to public GitHub repositories named "Shai-Hulud," making them accessible to the public. The impact of this attack is significant, as it not only compromises individual developer environments but also exposes private repositories and organizational secrets, potentially leading to further exploitation.

THREAT SUMMARY

The "Shai-Hulud" worm represents a significant escalation in software supply chain attacks, particularly within the Node.js ecosystem. Discovered in mid-September 2025, this self-replicating malware has compromised over 500 npm packages, including widely used libraries such as @ctrl/tinycolor and several maintained by CrowdStrike. This worm's primary objective is to harvest developer credentials, such as GitHub Personal Access Tokens (PATs), npm tokens, and cloud service API keys, and exfiltrate them to attacker-controlled endpoints. Additionally, stolen credentials have been observed to be uploaded to public GitHub repositories named "Shai-Hulud," making them accessible to the public. The impact of this attack is significant, as it not only compromises individual developer environments but also exposes private repositories and organizational secrets, potentially leading to further exploitation.

SYNOPSIS

The Shai-Hulud worm operates by injecting malicious scripts into npm packages, which execute immediately upon installation. Once active, it scans the victim's environment for sensitive credentials, including npm tokens, GitHub Personal Access Tokens (PATs), and cloud service keys for AWS, GCP, and Azure. These credentials are then encoded and exfiltrated to attacker-controlled endpoints, as well as uploaded to a public GitHub repository named Shai-Hulud. The malware also deploys a malicious GitHub Actions workflow (shai-hulud-workflow.yml) that executes during CI/CD pipeline runs, enabling further exfiltration of secrets from compromised repositories and maintaining persistent access even after the initial infection.

In addition to credential theft, Shai-Hulud autonomously propagates by modifying the package.json files of all npm packages maintained by the victim, injecting its malicious script and republishing the packages to the npm registry. This self-replication mechanism allows the worm to spread to other developers and organizations using the infected packages. By combining automated propagation, persistent access through CI/CD workflows, and large-scale credential exfiltration, Shai-Hulud demonstrates a highly effective and dangerous supply-chain attack methodology that threatens the integrity of the npm ecosystem and exposes downstream organizations to potential compromise.

NPM - SHAI-HULUD WORM COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('c5d0f271-73cf-44a1-98ff-e6ed809d30e6'),touched:!t)

RELATED HUNT PACKAGES

BASE64 ENCODING WITH POTENTIAL EXFILTRATION

https://hunter.cyborgsecurity.io/research/hunt-package/d65c7ebb-08e9-4a23-b964-1041d3384d4a

USAGE OF CHMOD TO ENABLE EXECUTION - POTENTIAL PAYLOAD STAGING

https://hunter.cyborgsecurity.io/research/hunt-package/dfbdc565-a37c-472b-a4c7-6c0e5325b255

UNUSUAL SECRET SCANNING PROCESSES - TRUFFLEHOG ACTIVITY

https://hunter.cyborgsecurity.io/research/hunt-package/b6fba6ae-ffab-421b-9832-44b4c62e6fc7

SUSPICIOUS DNS REQUEST - GITHUB API

https://hunter.cyborgsecurity.io/research/hunt-package/8295dc2e-4cd4-425c-aecc-480617bc2c51

DOUBLE BASE64 ENCODING

https://hunter.cyborgsecurity.io/research/hunt-package/f5aec910-25b6-462c-982a-a4eb20fa7c91

MITRE CONTEXT

- Exploits Vulnerabilities:
  - CVE-2024-1709
  - CVE-2024-3400
  - CVE-2025-0282
  - CVE-2023-46747
  - CVE-2021-4436
- MITRE Tactic Names:
  - Defense Evasion
  - Credential Access
  - Discovery
  - Exfiltration
  - Collection
  - Execution
- MITRE Technique Names:
  - Automated Collection
  - Exfiltration Over C2 Channel
  - Command and Scripting Interpreter
  - Credentials in Files
  - Linux and Mac File and Directory Permissions Modification
  - Account Discovery
- MITRE Technique IDs:
  - T1041
  - T1222.002
  - T1119
  - T1087
  - T1081
  - T1059
- Threat Names:
  - Shai-Hulud

REFERENCES

1. https://www.trendmicro.com/en_us/research/25/i/npm-supply-chain-attack.html
2. https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem
3. https://unit42.paloaltonetworks.com/npm-supply-chain-attack/
4. https://www.blackduck.com/blog/npm-malware-attack-shai-hulud-threat.html