The Shai-Hulud NPM Worm: When Supply Chains Bite Back

- Sept 2025
- The first self-propagating worm to hit npm
- The start of something new ...

Steve Poole

Independent Consultant, Advocate and Engineer

Steve Poole is a recognized Java Champion, Secure Development Expert, and DevOps leader, with extensive experience in building resilient and secure digital infrastructures.

Steve specializes in secure development practices, guiding organizations in integrating robust security into their DevOps pipelines, and enhancing software supply chain security.

Steve is passionate about helping developers become more security-conscious, sharing insights on proactive defense strategies and mitigating risks from sophisticated attacks like the Shai-Hulud NPM worm.

reflexframeworks.com
@spoole167

https://www.linkedin.com/in/noregressions/

September 2025: npm Meets Its First Worm

1

Popular Package Compromised

@ctrl/tinycolor targeted

2

CI Runners Infected

Automated builds execute malware

3

Secrets Harvested

Tokens and credentials stolen

4

Rapid Propagation

Dozens of packages, thousands of installs

How Shai-Hulud Operates

Package Install

npm install triggers

Postinstall Hook

Malicious script executes

Bundle.js Injection

Massive payload deployed

Forced Publish

Worm spreads further

- ### Entry Point

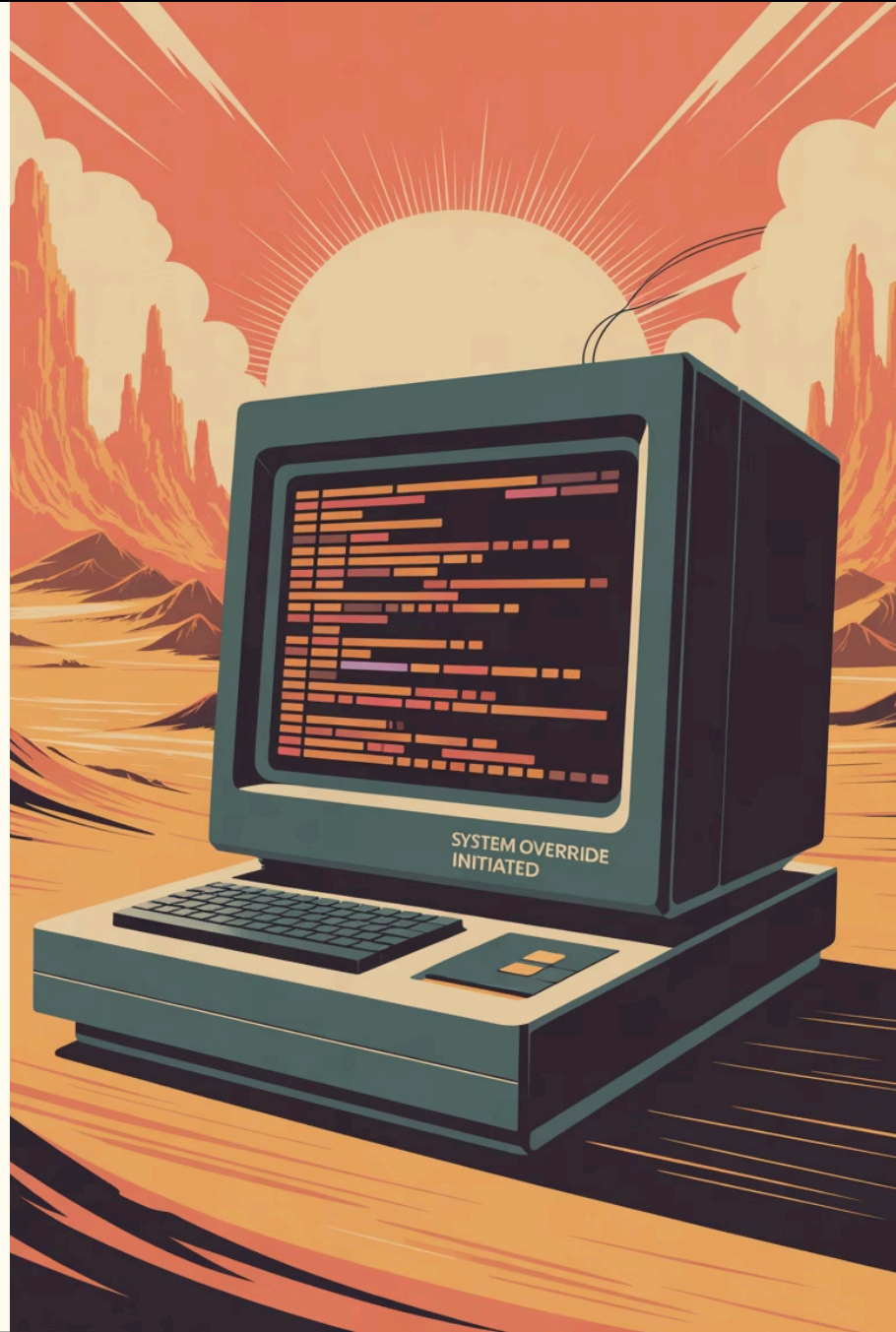
  Malicious code executed via **postinstall hooks** during package installation.

- ### Payload Delivery

  A massive malware payload was delivered by injecting into **bundle.js**.

- ### Automatic Propagation

  The worm achieved widespread **automatic propagation** through forced package publishing.



High-Value Targets

GitHub Tokens

Full repository access

npm Credentials

Package publishing rights

Cloud Keys

AWS, Azure, GCP access

Targeted Valuable Assets

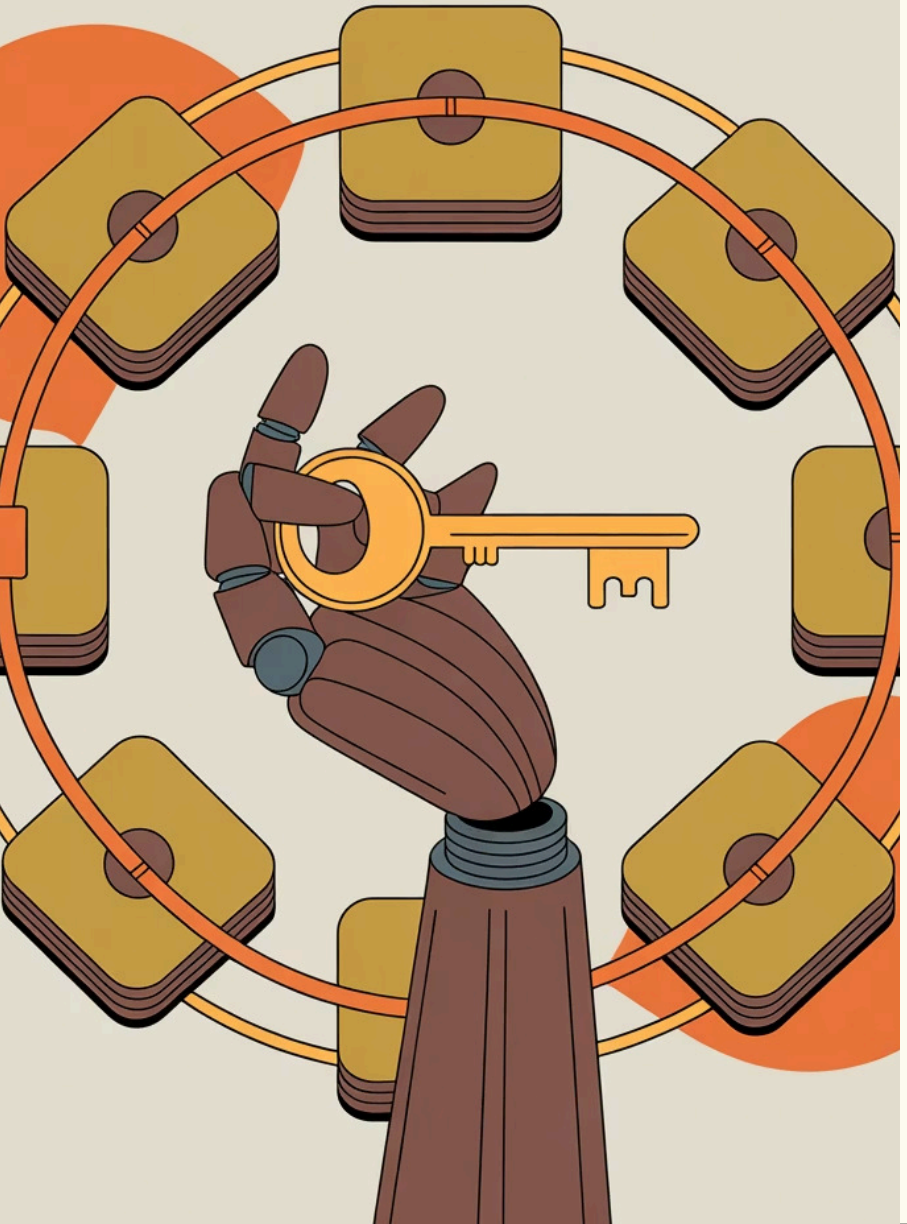
The worm specifically aimed for critical credentials like GitHub tokens, npm publishing rights, and cloud access keys (AWS, Azure, GCP).

Persistence via GitHub Actions

It injected malicious GitHub Actions workflows to maintain persistent access and control over compromised repositories.

Strategic, Not Random

Instead of random scanning, the attack was highly strategic, focusing on assets that provided maximum leverage for further propagation and impact.



CI/CD: The Perfect Storm

Always Connected

Continuous network access for builds

Credential Rich

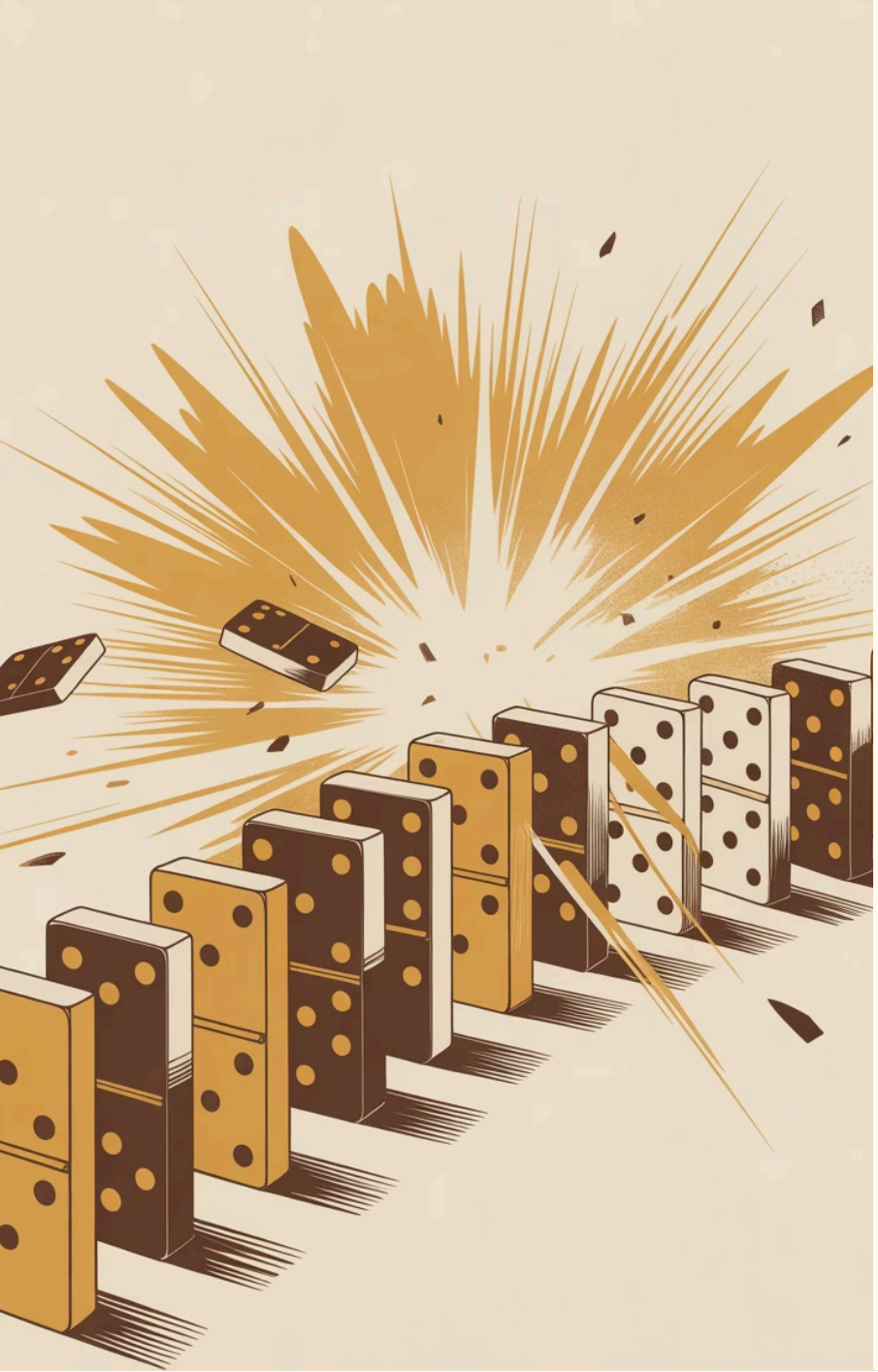
High-privilege tokens everywhere

Automated Trust

npm installs on every build

Ideal Worm Environment

These combined factors create a highly vulnerable and effective host for propagation.



The Domino Effect: Exponential Destruction

- Maintainer Compromised
- Credentials Stolen
- Packages Poisoned
- Worm Spreads

1 maintainer → 40+ packages → 1000s infected → 72 hours

Practical DevOps Controls

- [ ] **Lockfile Policies**
  Pin dependencies, block unexpected updates
- [ ] **SBOM Monitoring**
  Track what's actually in your builds
- [ ] **Short-lived Tokens**
  OIDC over long-lived credentials
- [ ] **Network Egress Control**
  Block unauthorized outbound connections

Warning Signs in Your Environment

1

Suspicious Repositories

New repos named 'Shai-Hulud'

2

Rogue Workflows

Unexpected GitHub Actions appearing

3

External Communications

Outbound calls to webhook.site

- Early detection saves time
- Monitor these patterns
- The next worm is coming

When Supply Chains Bite Back

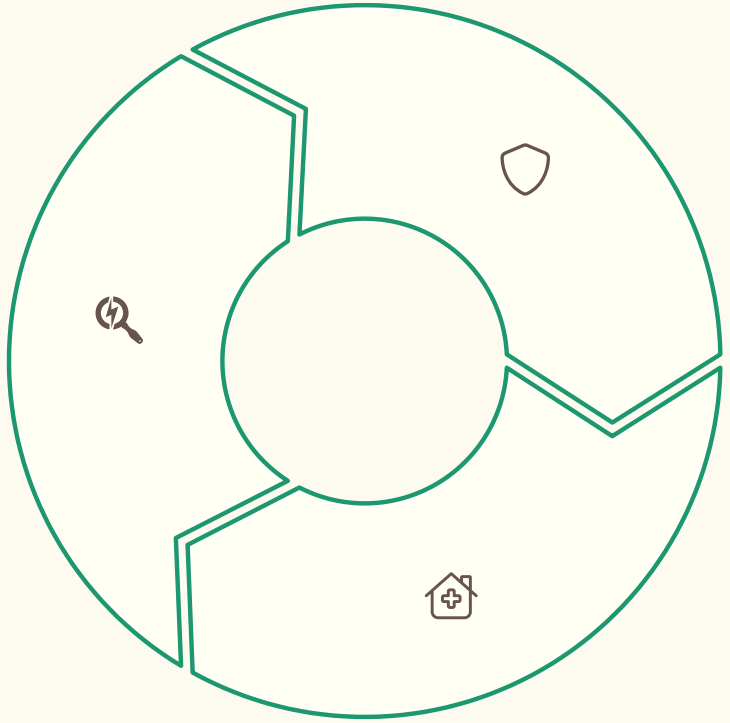
This marked a turning point: malware that propagates itself through our most trusted systems.

For DevOps teams, the pipeline is now the front line of defence.

Your Action Plan

Audit Dependencies

Know what's in your supply chain



Harden Pipelines

Implement security controls

Practice Response

Prepare for the next attack

- **The threat is growing:** Supply chain attacks are escalating, impacting businesses across all sectors.
- **Preparation is paramount:** Building robust defenses now is critical to protect your pipeline.
- **Act before it's too late:** Don't wait for the next breach; secure your systems today.

Learn how to make defending against software supply chain attacks second nature @

REFLEXFRAMEWORKS.COM

@spoole167

https://www.linkedin.com/in/noregressions/