



Dependency

Lodash

@typescript-eslintt5.x

react

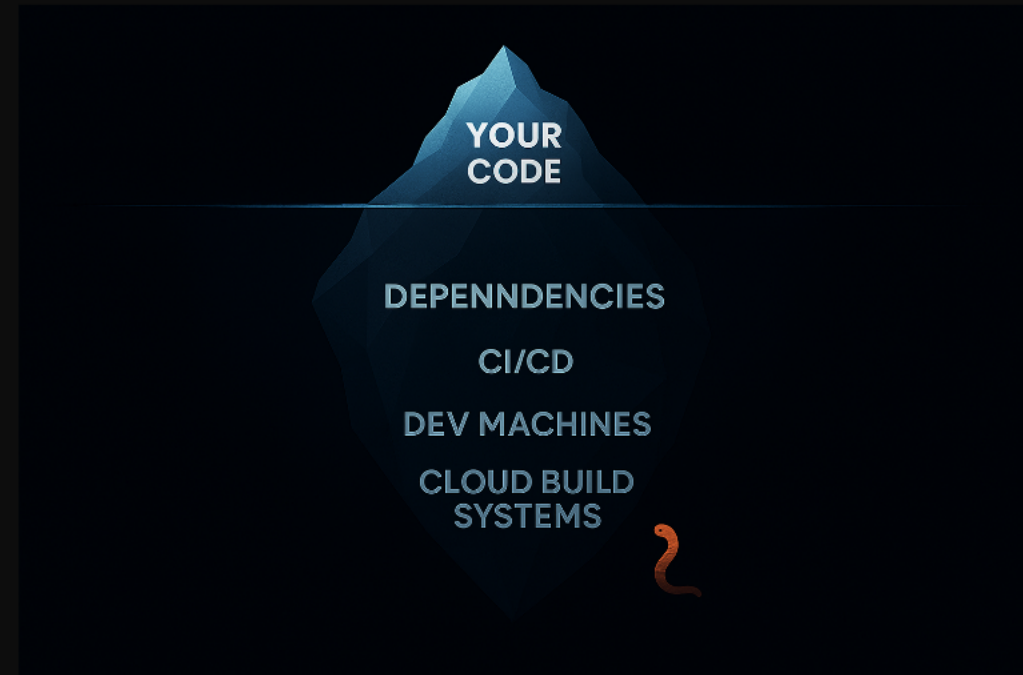
eslint-plugin-react 7.x

Your App is Made of Worms

What the Shai-Hulud Worm Teaches Us About Modern Application Security

Why you might be vulnerable

- Modern Apps aren't just code
- Traditional Security Tooling only protects part of the app
- Attackers Exploit Trust, not just bugs



What you should learn

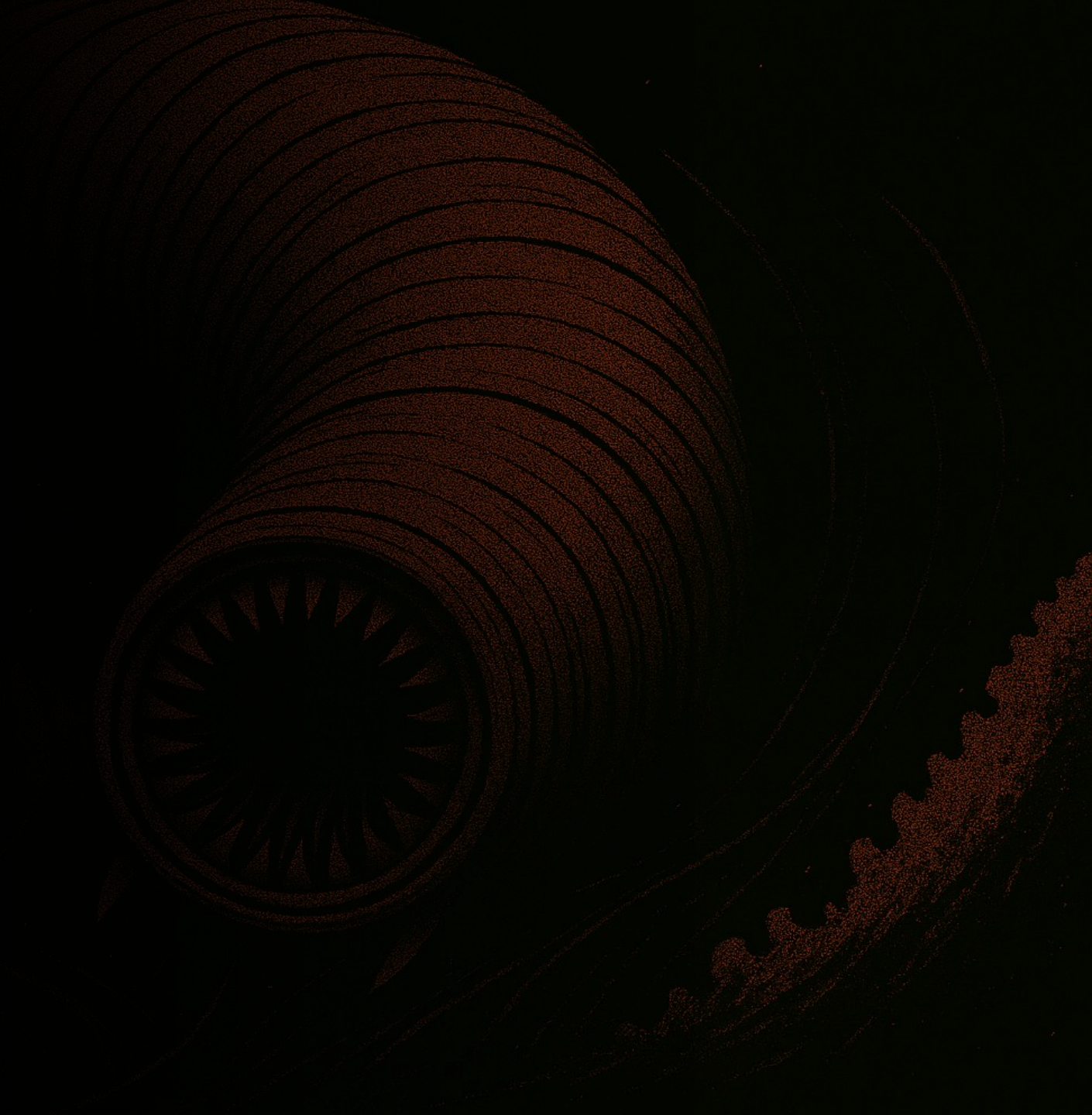
- How supply chain attacks spread in web ecosystems
- Why cloud and developer workflows increase exposure
- Practical lessons to reduce risk





The 2025 Shai-Hulud Worm: What Happened

- September 2025 – Initial Wave
- November 2025 – Shai-Hulud 2.0

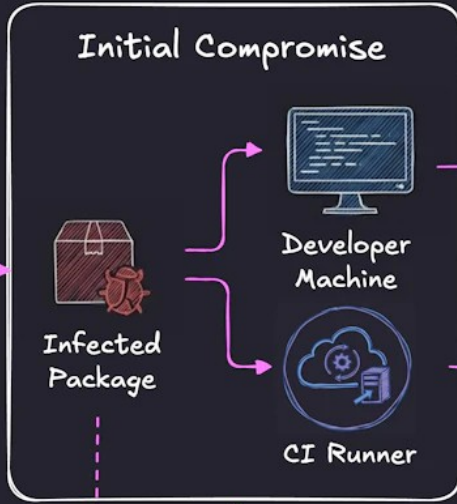


SHA1-HULUD 2.0: ONGOING SUPPLY CHAIN ATTACK

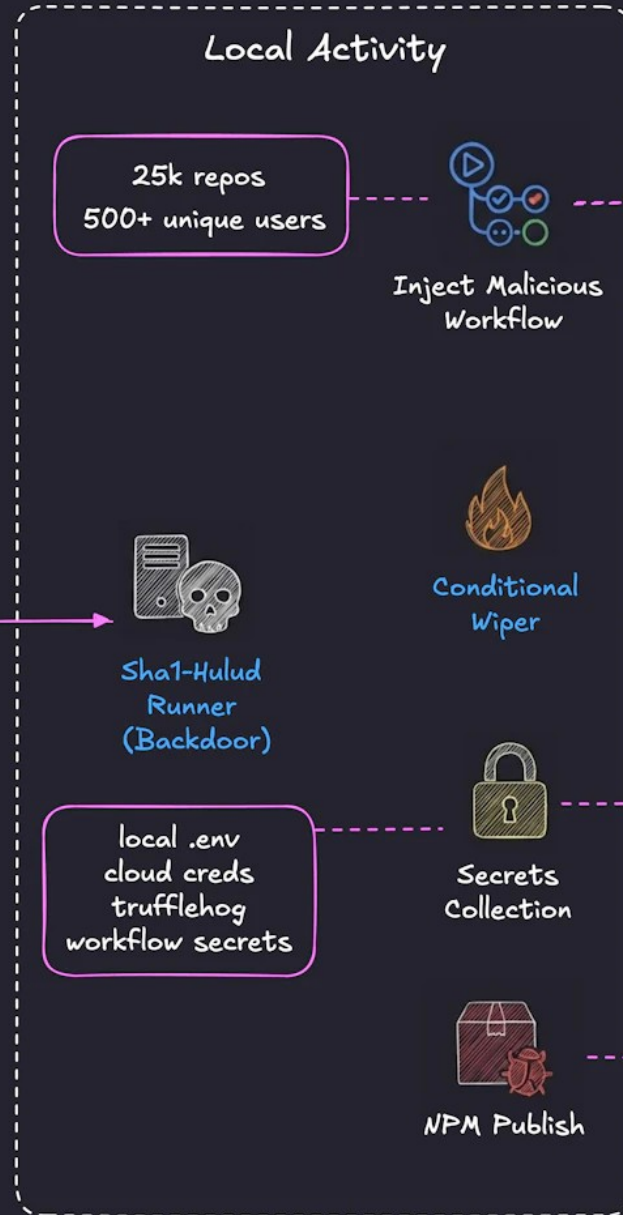
new techniques
in Sha1-Hulud 2.0



Attacker



500+ packages
100M+ monthly downloads

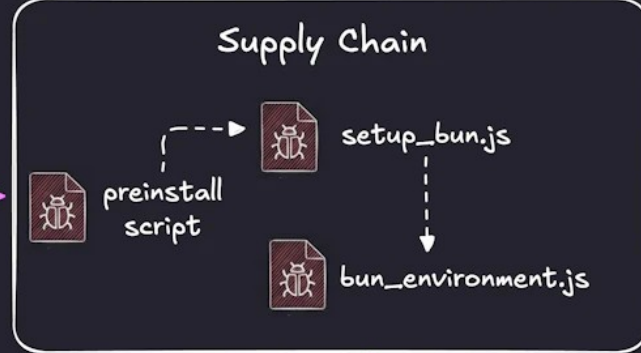


exfil & C2

GitHub keys
found

GitHub keys
not found

CI/CD Pipeline (GitHub Actions)



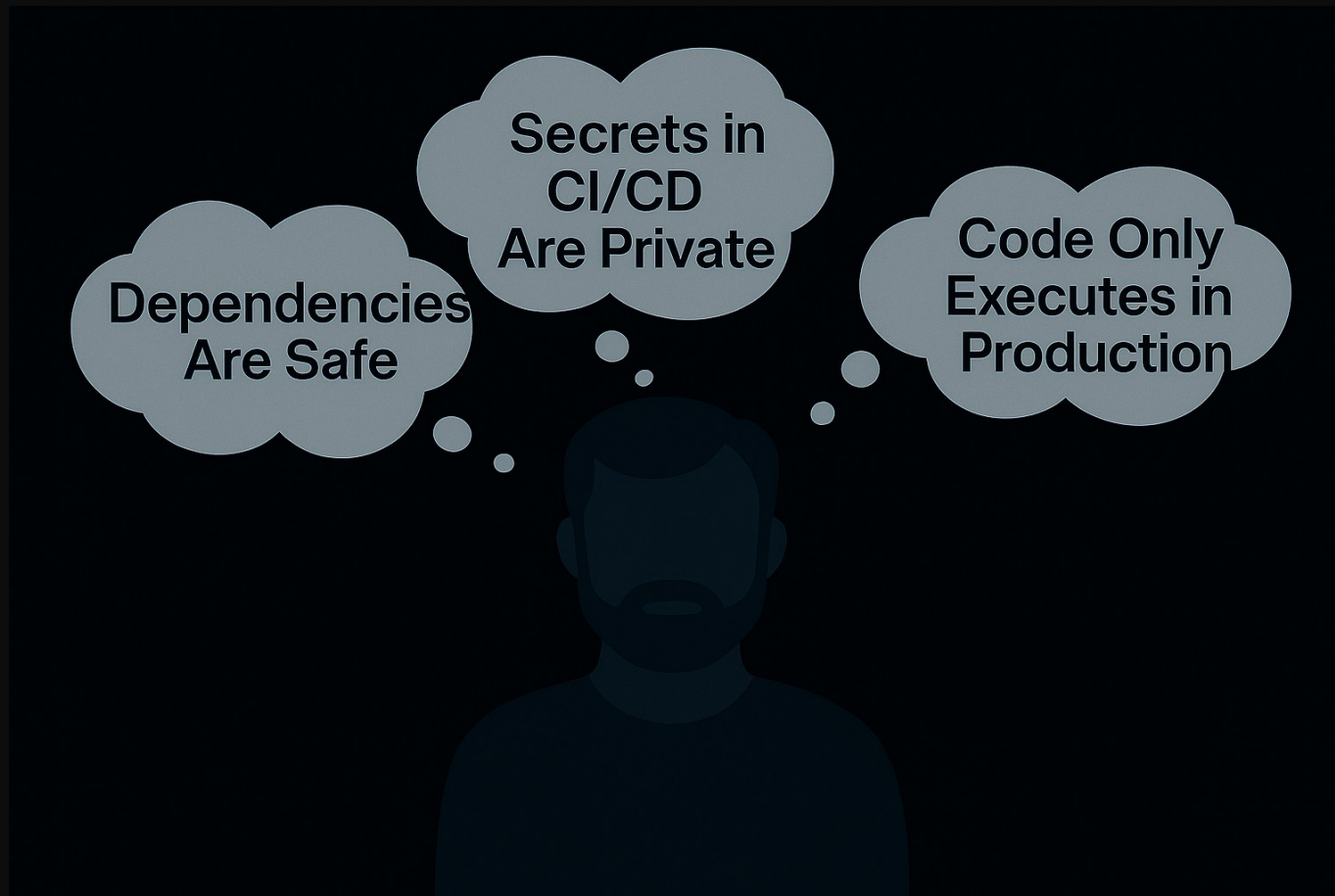
possible impact

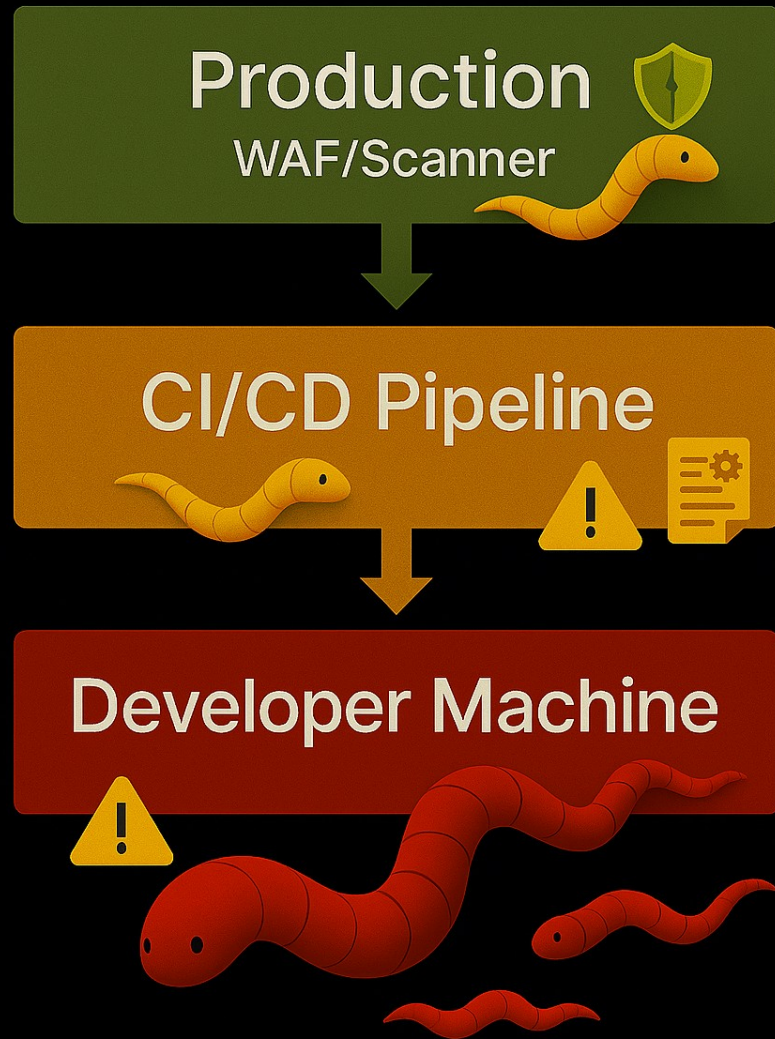
worm-like
propagation



The Real-World Impact

Broken Assumptions





Why Traditional Web Defenses Fail

- WAFs and Web Scanners Protect Only Production
 - Runtime Monitoring is Reactive, Not Preventive
 - Dependencies Are Trusted by Default
 - CI/CD Pipelines and Developer Workstations Are Blind Spots
-



The Hidden Attack Surface

- **Developer Machines**
- **CI/CD Pipelines**
- **Cloud Build Environments & Production**
- **Dependencies**

Your App = A Colony of Worms

- Each Dependency
= A Worm
- Trust Boundaries
= Fences That
Don't Exist
-

What You Can Do About It



Manage Dependencies
Carefully



Secure CI/CD & Build
Pipelines



Track and Audit Your Supply
Chain



Remember the Big Picture



Preventive Steps for Developers & Teams

- 🐛 **Pin Dependencies / Use Lockfiles**
- 🐛 **Vet Packages Before Installing**
- 🐛 **Limit Unnecessary Install Scripts**

CI/CD & Build Hygiene

- **Isolate Build Environments**
- **Remove Unnecessary Secrets from Pipelines**
- **Monitor Unexpected Network Calls During Builds**



Monitoring & Response

- Use SBOMs (Software Bill of Materials)
- Alert on Unexpected Dependency Changes or Credential Exfiltration
- Regularly Audit Build Logs





- **Your App = Ecosystem, Not Just Code**
- **Trust is the Real Attack Surface**
- **Small, Practical Steps Reduce Exposure**

Now What?

- 
- **Security Starts Early**
 - **Trust Carefully, Verify Often**
 - **Small Steps Make a Big Difference**