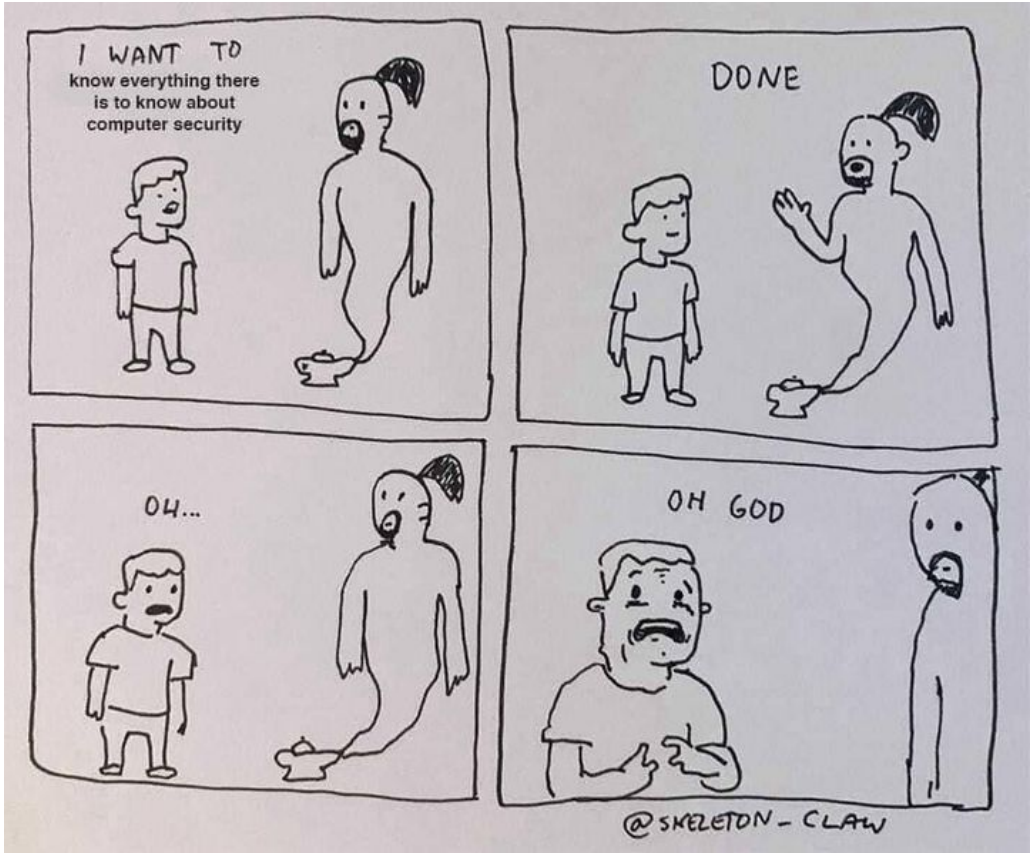
Ship Happens: The Stormy Seas of Supply Chain Security

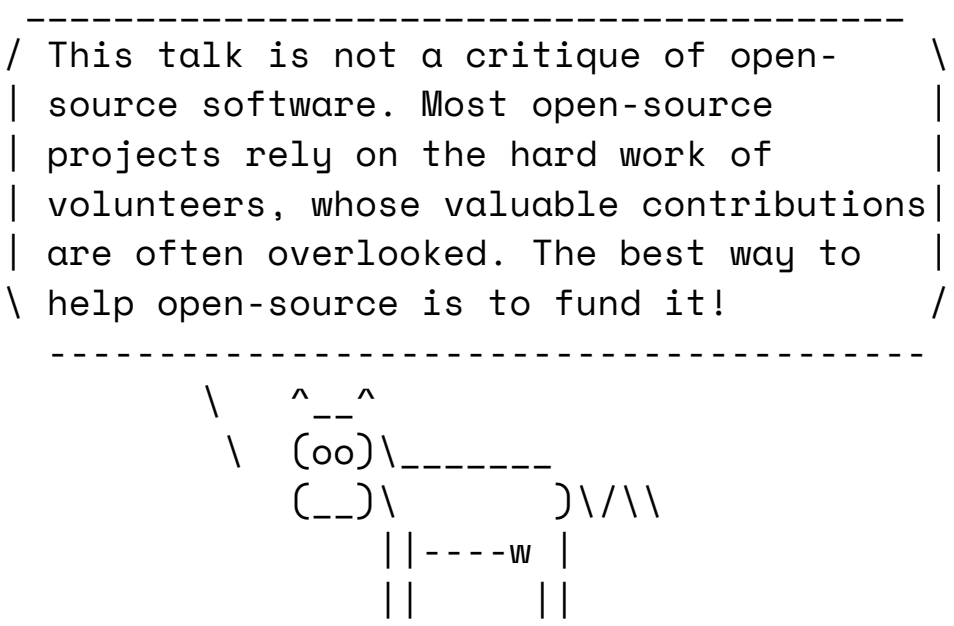
David Archer
Solution Architect, Endor Labs

Our voyage today

- Why talk about the software supply chain?
- What is a software supply chain?
- Why are they under attack?
- How software is built
- What can go wrong
- Securing your Source, Build, (Dependencies), Packages
- Resources
- Q & A

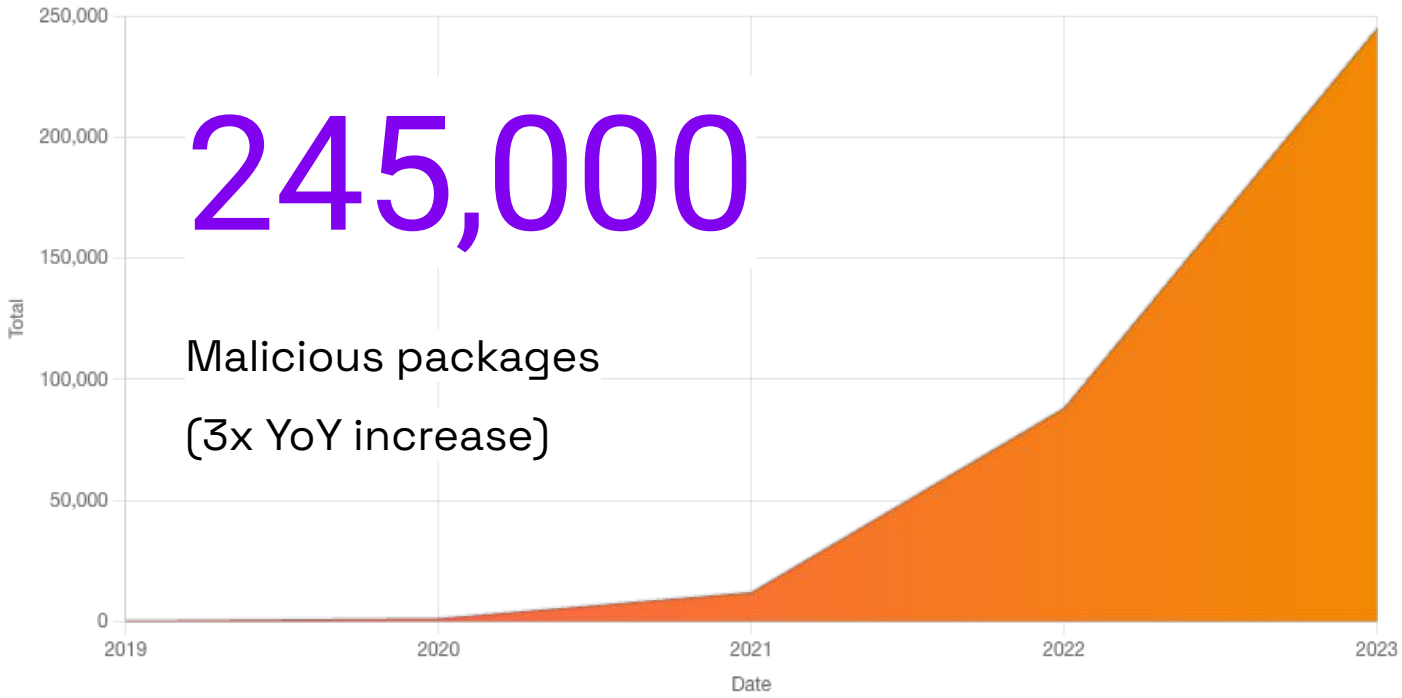


Before we set sail



Cowsay, courtesy of Tony Monroe

Why a talk about “software supply chain”?



solarwinds

Codecov

XZ

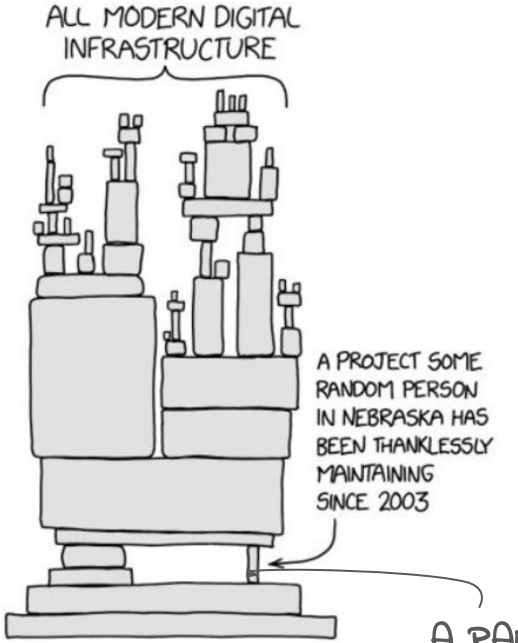
Log4Shell

Progress MOVEit

Kaseya

Sonatype SCSS Report 2023

Not all heroes wear capes



XKCD r/ProgrammerHumor

Why is this happening?

Technological Factors

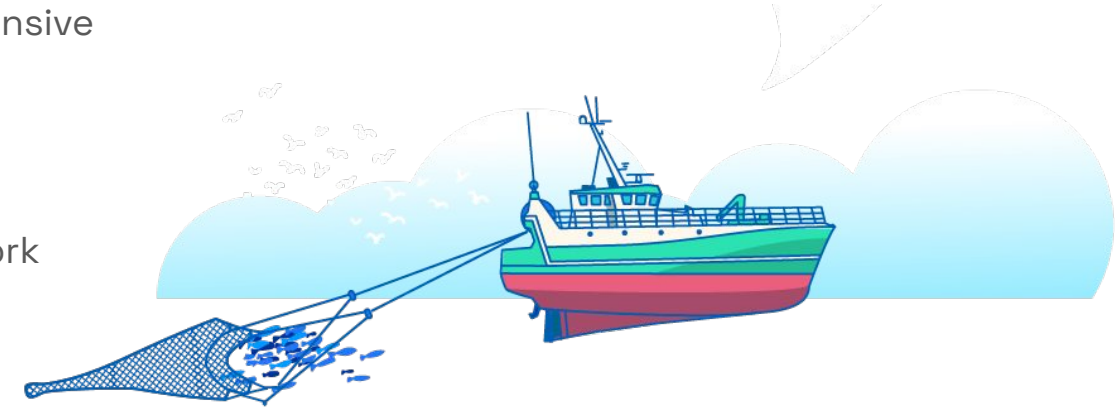
- Complex and interconnected supply chains
- Rapid adoption of open source
- Easy target?

Economic Factors

- Higher rewards
- Detection is difficult
- Many attacks are inexpensive

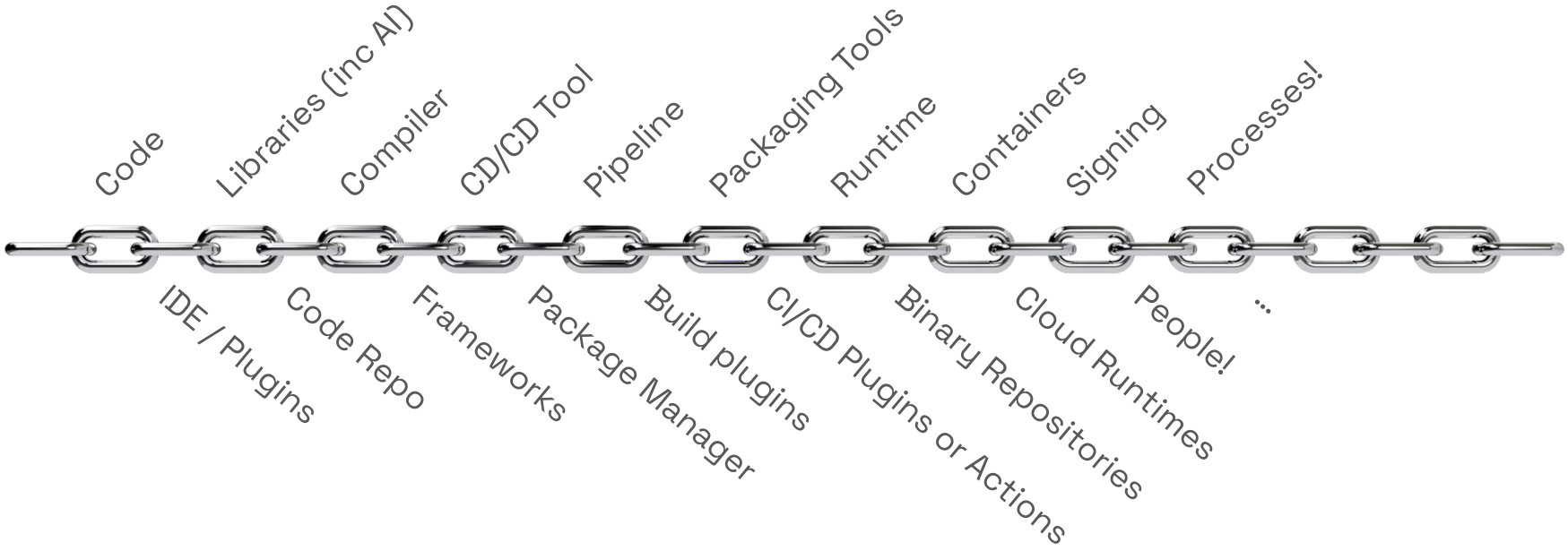
Human Factors

- “Trusting” mindset
- Rapid transition to remote work
- Pressure and burnout

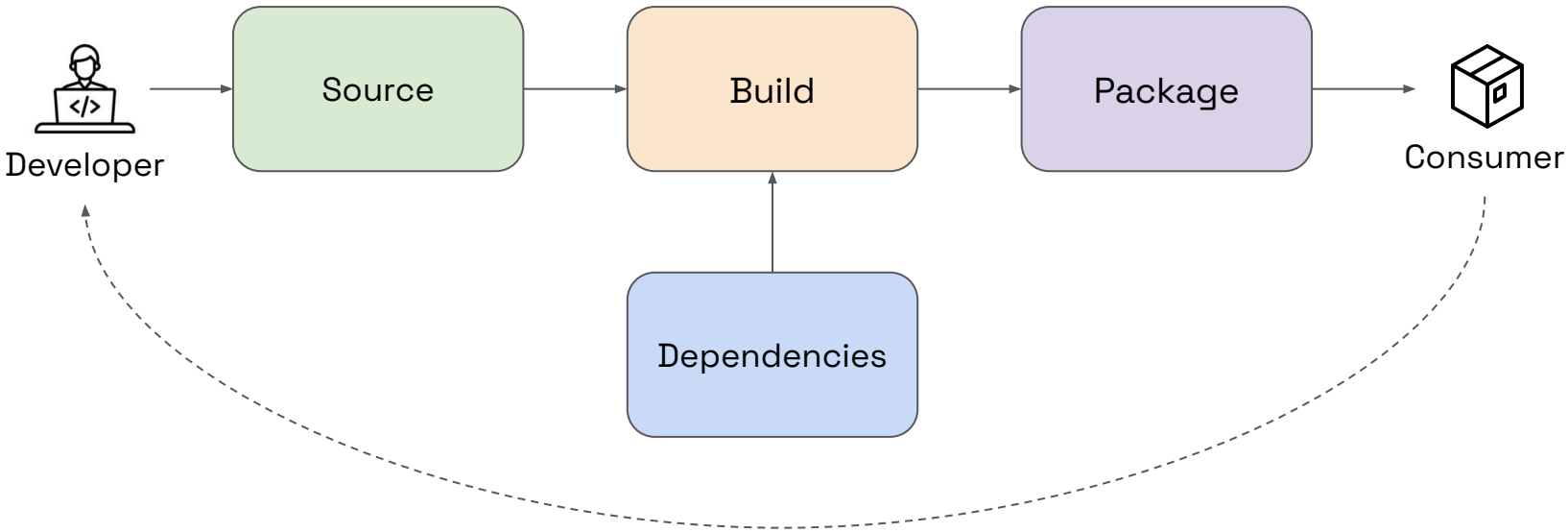


What is a software supply chain?

Anything used to deliver software to production



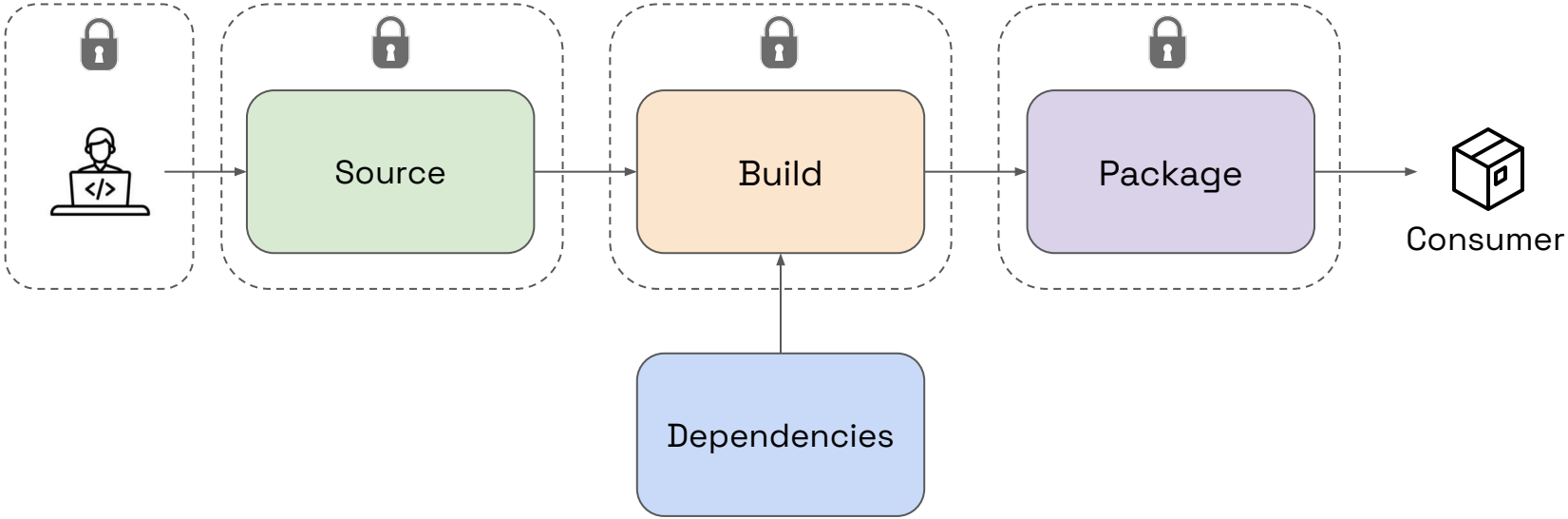
High level: How is software built?



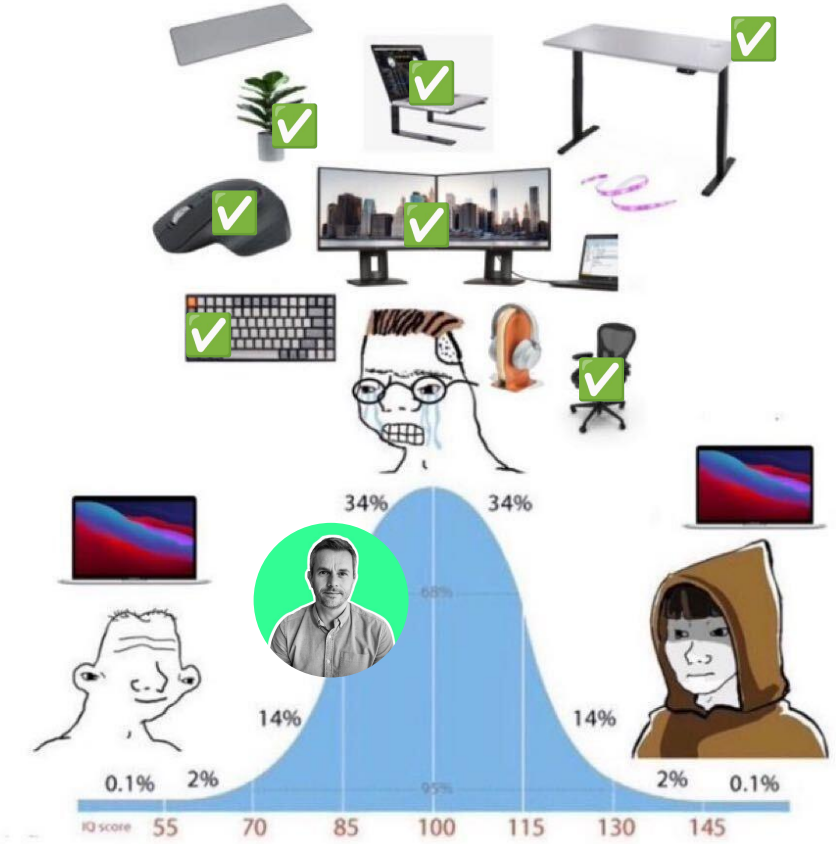
What's in your threat model?

Developer/ Workstation → IDE + plugins → Maven + plugins → Package Manager → Dependencies → Git Client → SCM Platform → CICD Platform → Maven + plugins → Package Manager → Dependencies → Linters → Javadoc → e2e Test Runner → Security Scanners → Binary Registry → Base Image → Docker Build → Container Registry → Consumer

Where are our trust boundaries?



Developers like shiny things!



Developers: navigating the risks

Threats

- Compromised device (malware)
- Credential theft/exposure
- Coding mistakes
- Malicious insider
- Social engineering
- Copy/paste!

Controls

- Access controls
- Endpoint protection
- Verify software integrity
- (SSC) Security training
- Commit signing
- SCA/*AST
- Web IDEs(!)
- **Code reviews**

CircleCI incident report for January 4, 2023 security incident

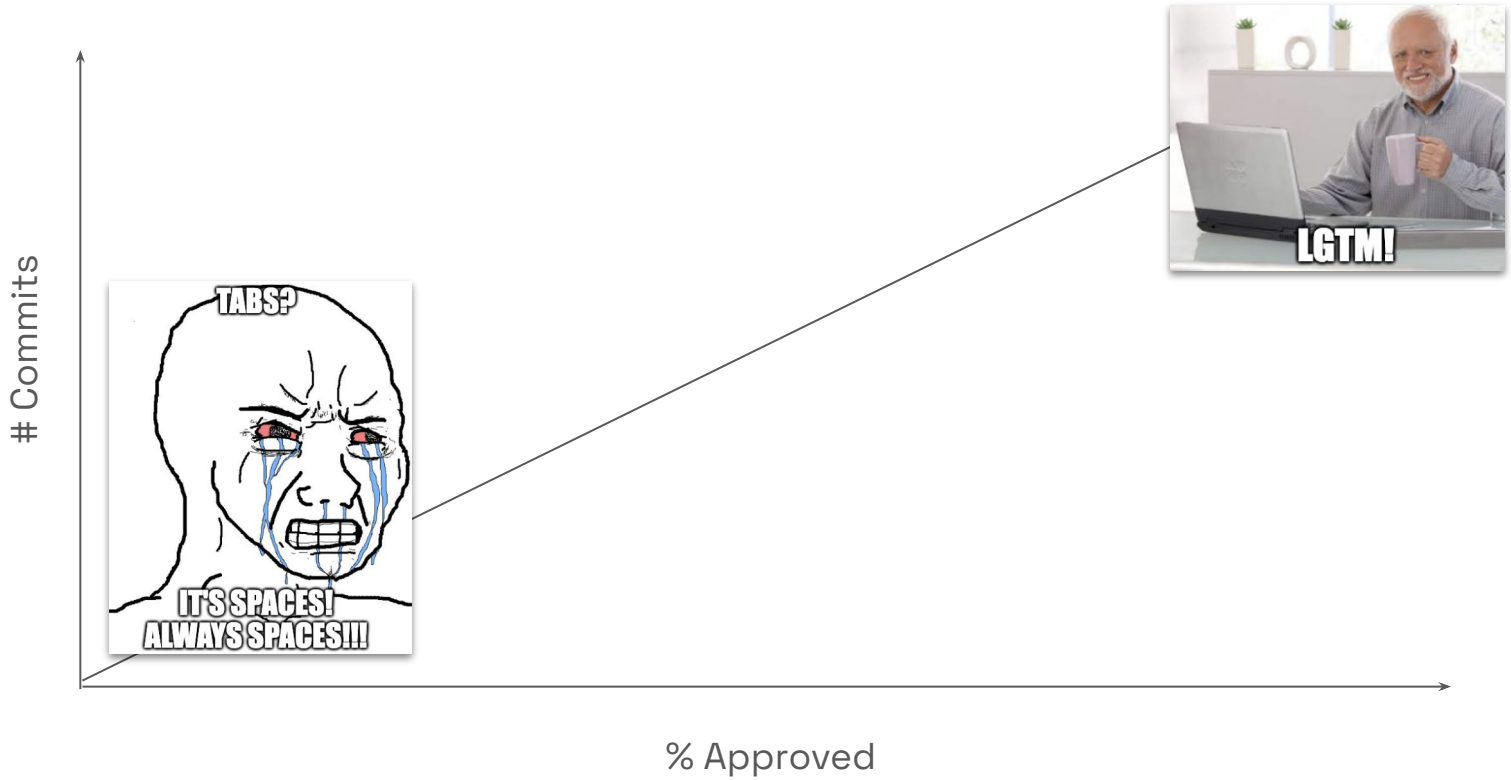
The Octopus Scanner Malware: Attacking the open source supply chain

Malicious VSCode extensions with millions of installs discovered

Cybercriminals pose as "helpful" Stack Overflow users to push malware

This Week in Malware - Over 70 packages discovered

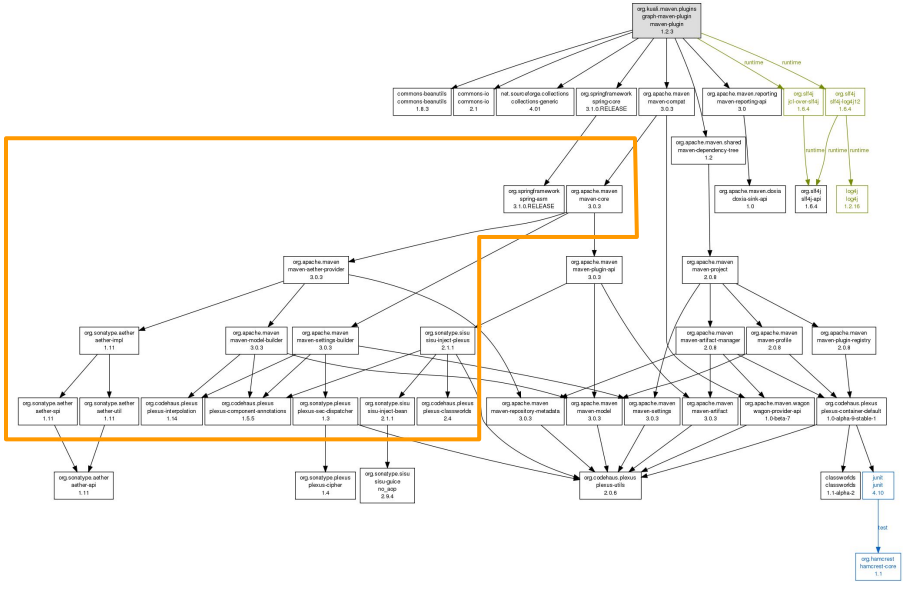
Code Reviews? Ain't Nobody Got Time for That!



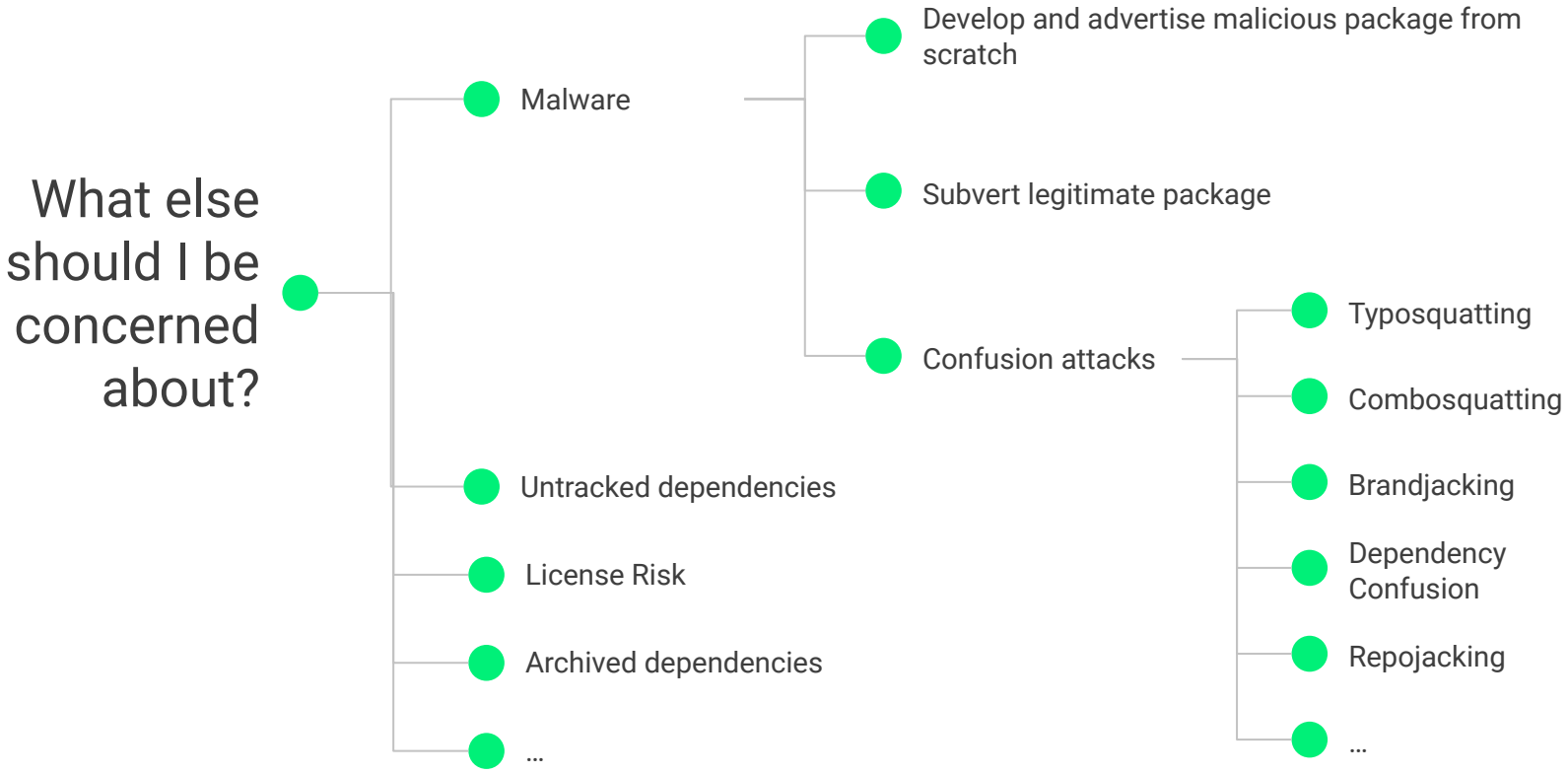
Charting dependency paths

95% of vulnerabilities are in transitive dependencies
(from the perspective of an application)

Program analysis techniques can determine reachability of vulnerable code

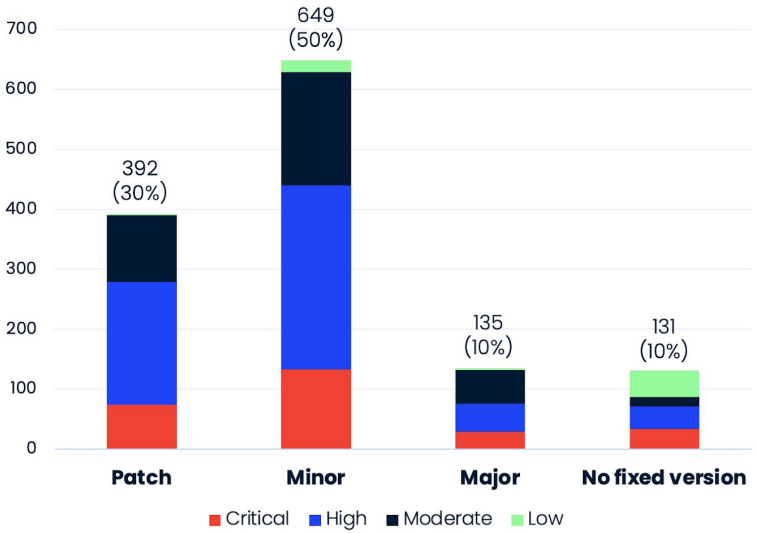


CVEs: Not the only sharks in the water!



See the Risk Explorer and Backstabber's Knife Collection for more!

Dependency bumps are harder than you think



Source: Moderne, June 2023

ELSEVIER

Journal of Systems and Software

Volume 183, January 2022, 111097

Can we trust tests to automate dependency updates? A case study of Java Projects ☆

Joseph Hejderup, Georgios Gousios

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.jss.2021.111097 Get rights and content

Under a Creative Commons license open access

Highlights

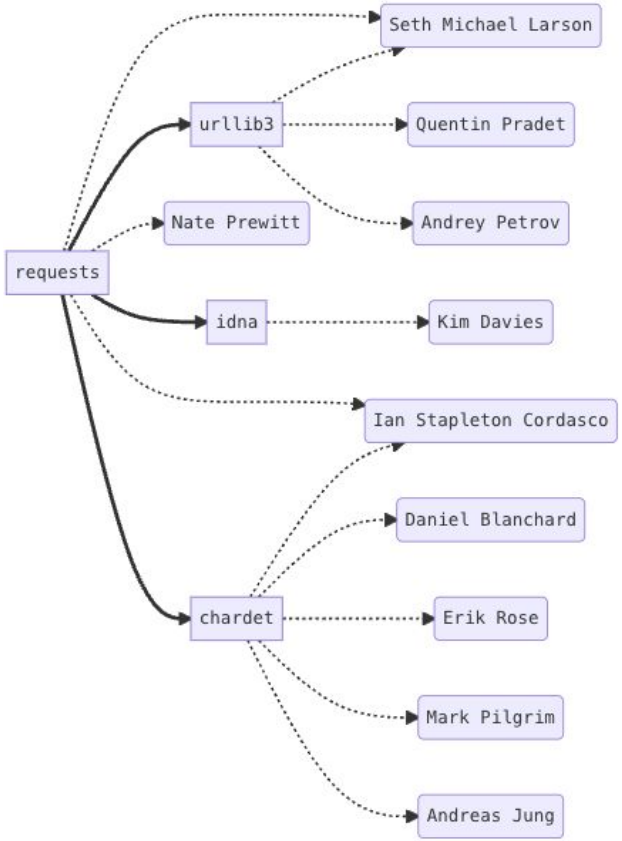
- Developers perceive tests as unreliable for automated dependency updating.
- Mutation testing reveal gaps in test coverage of dependencies.
- Static analysis can reduce gaps where tests are unable to reach in dependencies.
- Toolmakers should introduce an adequacy score for automated updating.
- Static analysis is useful and improves the reliability of automated updating.

https://www.sciencedirect.com/science/article/pii/S0164121221001941

Meet your new crew mates!

“The modern software supply chain is both miraculous and terrifying”

- Seth Michael Larson, core maintainer of urllib3



Dependencies you won’t find in your requirements.txt

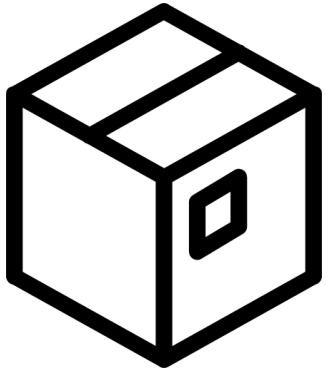
Smooth sailing with shipshape dependencies!

Is it secure?

- Unfixed vulnerabilities
- Potential Malware
- Calls sensitive APIs
- Obfuscated code
- Binaries in the repo

Does it meet your standards?

- Documentation
- % Test code in the repo
- Verified commits
- Major releases
- Automated builds



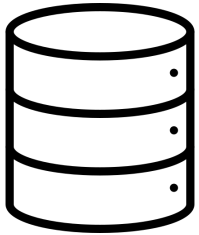
Is it popular?

- Is it forked
- Stars
- Subscribers
- Dependant projects
- Many downloads

Is it being well maintained?

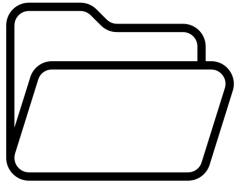
- Reputable contributors
- Regular commits
- Frequent releases
- Merged PRs
- Issues raised/closed

Securing your bounty



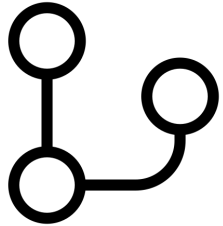
SCM Org

- Access Control
- Audit Logging
- Security Policies
- Integrations
- Verify organisation



Repo

- Secret scanning
- Multiple (but limited) admins
- Restrict visibility



Branch

- Branch protection
- Signed commits
- PR Checks
- Forced push restrictions
- Codeowner reviews

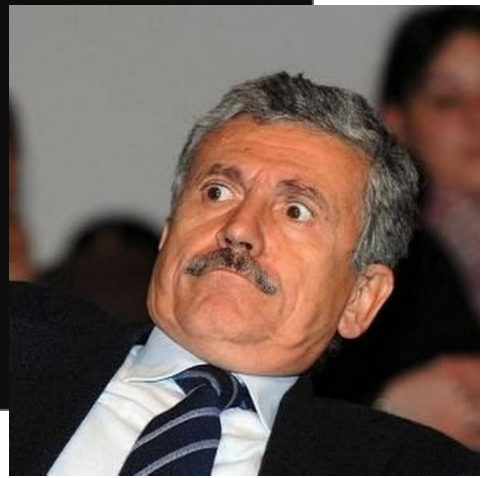
Review CIS Benchmark (GitHub/GitLab) for more details!

Beware: Untrusted tools can sink your ship

build
failed 2 weeks ago in 50s

Search logs

- Run actions/checkout@v4
- Setup JDK 17
- Obtaining access to your secrets, code and cloud environment
- Downloading a bunch of dependencies from around the world
- Running a few random GitHub actions that your developers chose
- Running this maven plugin that claims to make your code faster
- Run some linter that some dude in Birmingham wrote
- Saving the binary, good job y'all



Anchoring security: critical build controls

Pipeline/Workflow

- Secure secrets, duh
- Limit token scope
- Detect script injections
- Separate the build stage and isolate binaries
- Require run approval for all outside collaborators
- Don't run external scripts!

Actions/Plugins

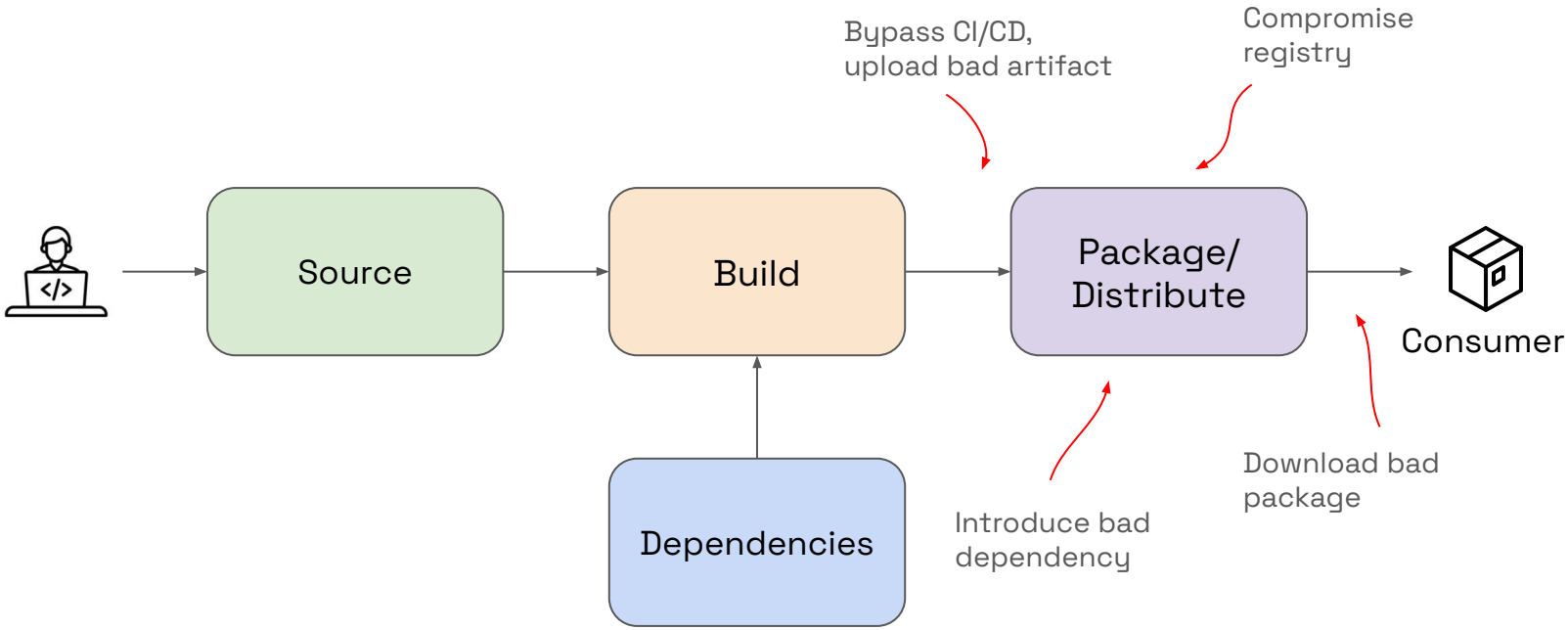
- **Gain visibility**!
- Pin to version hashes
- Understand the provenance
- Prevent PR approvals
- **Undertake code reviews** or consider limiting actions via a policy
- Fork actions

Build runners

- Use cloud-hosted runners if you can
- Don't run self-hosted runners for public repos
- Isolate self-hosted runners and limit network connections

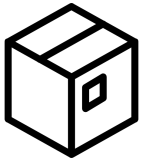

ALMOST.... THERE!

Sealing your cargo



Navigating integrity with artifact signing

Inputs



Package

+

Provenance
(commit, SBOM, pipeline)

Signing Provider

e.g. Sigstore or Endor Labs

Establish identity via OIDC

↓

Generate short-lived signing certificate

↓

Sign artifact digest

↓

Store signature, certificate and public key in immutable log

Verification

- ✓ Valid certificate
- ✓ Signature verified
- ✓ Timestamp matches validity
- ✓ Signature not revoked
- ✓ Provavance data matches

Frameworks/ Resources

Including:

- Supply Chain Threat Model
- Supply Chain Risks/Compromises
- Best Practices/Standards
- OWASP resources
- Hardening guides
- Free SSCS Developer training
- Tools/Utilities
- Blogs
- Research

Thank you!

ENDOR 💚 OWASP

Join us at Global AppSec Lisbon for Happy Hour drinks!