



The Dark Side of Open Source Productivity

Jamie Scott, Endor Labs
March 2, 2023



80% of code in modern apps is code
you didn't write

3.3M

OSS
Projects

47M

Versions

3.1T

Yearly
Downloads

33%


YoY Growth

What developers imagined



What developers got - "Dependency Hell"



 **Lars Kiesow** @larskiesow

They could have at last spent 5 min researching what they actually need instead of including just every dependency they could find... [#ocdaily](#)
[#dependencyhell](#) [#development](#)

```
[INFO]
[INFO]
[INFO] --- maven-dependency-plugin:3.0.2:analyze (default-cli) @ opencast-search ---
[WARNING] Unused declared dependencies found:
[WARNING] org.osgi.org.osgi.core:jar:5.0.0:provided
[WARNING] net.java.dev.jna:jna:jar:4.1.0:compile
[WARNING] org.apache.lucene:lucene-analyzers-common:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-codecs:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-core:jar:4.10.4:compile
[WARNING] org.apache.lucene:lucene-expressions:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-grouping:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-highlighter:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-join:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-memory:jar:4.10.4:runtime
[WARNING] org.apache.lucene:lucene-misc:jar:4.10.4:runtime
```

 **your friend kasra** @jc4p · Oct 26


i love making apps cause i love having to upgrade dependencies of dependencies that result in needing to upgrade my entire OS X

4 8


 **rossipedia** 🇺🇦 @rossipedia

Replying to @jc4p

dependency hell is a real place and we are all living there

 **hemloc** @hemloc_io · Oct 26

yet another day in **dependency hell**

 **Jaana Dogan** ヤナ ドガン 🌟 @rakyll · Oct 11

In tech, we need a "**Dependency removal engineer**" role.

87 374 3,329

 **Kelsey Hightower** 🌟 @kelseyhightower

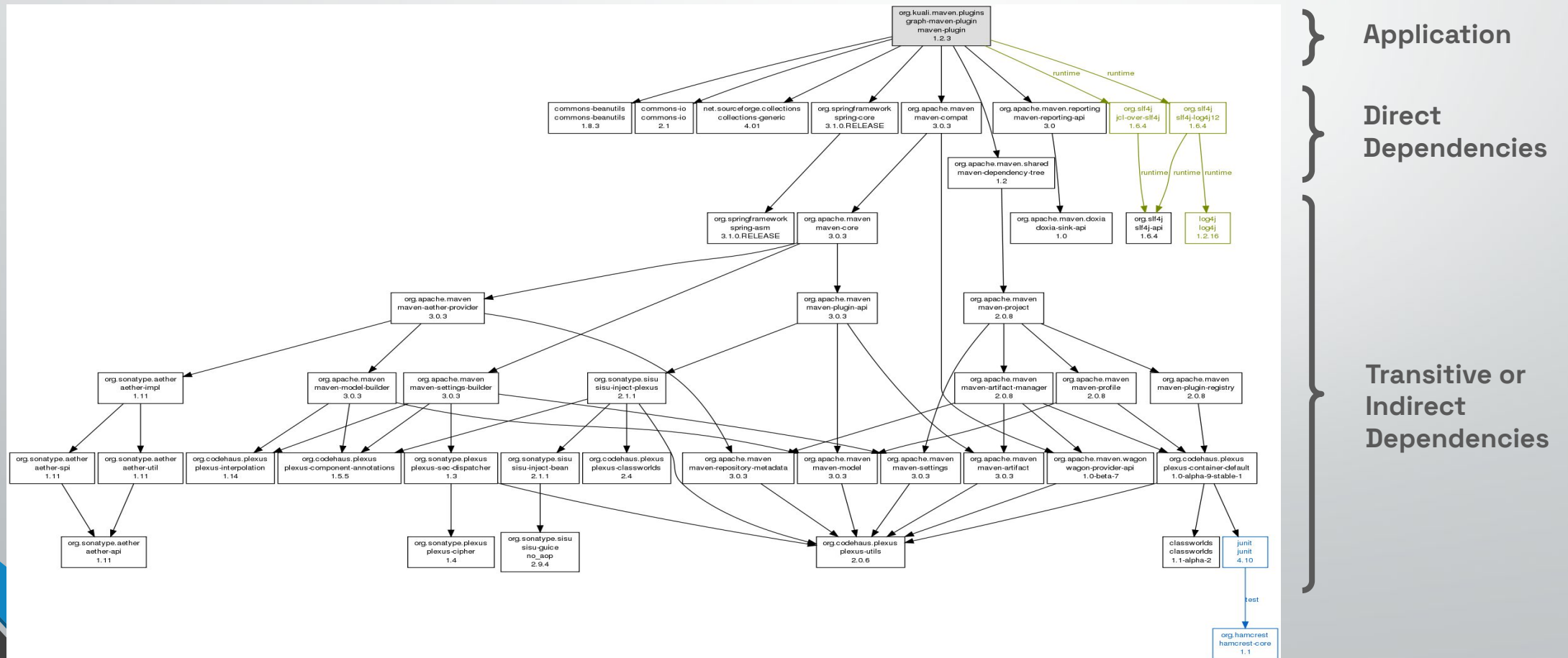
Given what we know about managing dependencies we are going to eventually run into problems around versioning and conflicts. Upgrading one dependency can break everything.

7:44 AM · Feb 26, 2018 · Twitter Web Client



Dependency 101

Software apps re-use (depend on) many other software components





Direct Dependencies

Transitive or Indirect Dependencies



OSS is more complex than you think

Wasted engineering cycles

Rather than developing features, engineers waste precious time chasing tons of false positives reported by current SCA tools.

Significant operational risk

Unvalidated, unused, outdated and unsupported dependencies impact application resilience, performance and security.

Emerging attack vectors

650% YoY increase in next-gen attacks that most organizations are unprepared to defend against with existing tools



Recent Incident: Gorilla

Risk is not always captured as a CVE

README.md

Gorilla Toolkit

⚠ The Gorilla Toolkit is now in archive-mode, and is no longer actively maintained. You can read more below.

We'll be putting the Gorilla project's repositories into "archive mode" by the end of 2022.

+10k weekly clones on
each package

Used in over
90K
repositories

18k GitHub
stars

Most popular
HTTP service
for Go

Where are we
using this
dependency?

What do we
replace it with?

Which
applications are
affected?

Are exposed to
security risk?



Recent Incident: PyTorch

Next-gen supply chain attack in an ML package

December 31, 2022

Compromised PyTorch-nightly dependency chain
between December 25th and December 30th, 2022.

17k forks

**Used in over
187K
repositories**

**61k GitHub
stars**

**Popular ML
framework by
Meta**

**Where are we
using this
dependency?**

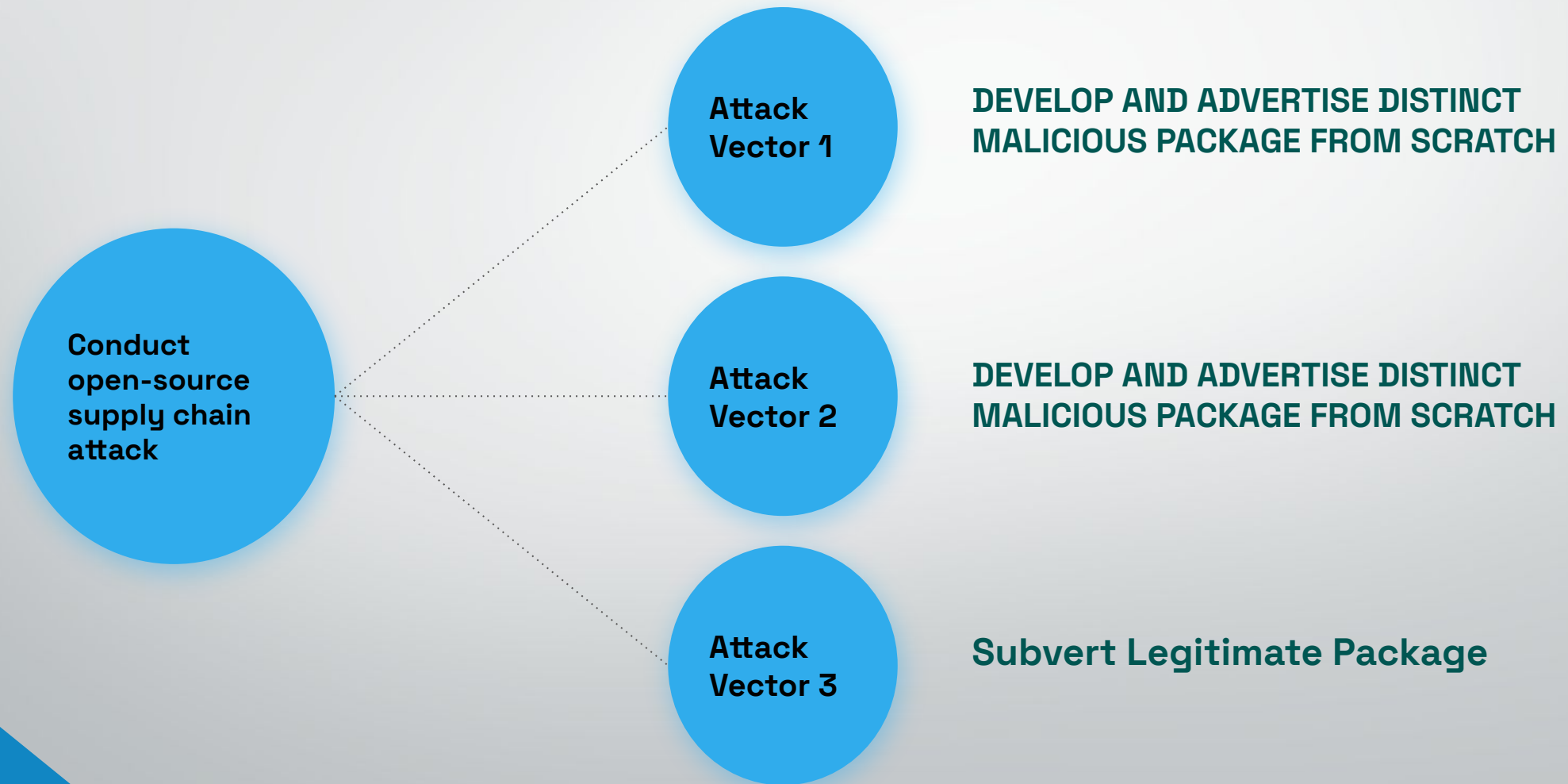
**What do we
replace it with?**

**Which
applications are
affected?**

**Are exposed to
security risk?**



A Taxonomy of Attacks



DEVELOP AND ADVERTISE DISTINCT MALICIOUS PACKAGE FROM SCRATCH



I need to get a job done!

I have just the thing!



Cool! This isn't suspicious at all!

DEVELOP AND ADVERTISE DISTINCT MALICIOUS PACKAGE FROM SCRATCH



SECURITY / SOFTWARE DEVELOPMENT

Npm Attackers Sneak a Backdoor into Node.js Deployments through Dependencies

May 8th, 2018 9:42am by [Lucian Constant](#)

17 Backdoored Docker Images Removed From Docker Hub

Inside the “Fallguys” Malware That Steals Your Browsing Data and Gaming IMs; Continued Attack on Open Source Software

September 02, 2020 By [Ax Sharma](#)

5 minute read time

June 13, 2018 02:40 PM

Python Packages Upload Your AWS Keys, env vars, Secrets to the Web

June 23, 2022 By [Ax Sharma](#)

5 minute read time

Create Name Confusion With Legitimate Package



Good ol' `urllib3-1.21.1.tar.gz`, just what
what I need!

Here you go, `urllib-1.21.1.tar.gz`!



Nice! Nothing weird here!

Create name confusion with legitimate package - Examples



PyPI Python repository hit by typosquatting sneak attack

Malicious Python Trojan Impersonates SentinelOne Security Client

A fully functional SentinelOne client is actually a Trojan horse that hides malicious code within; it was found lurking in the Python Package Index repository ecosystem.



Robert Lemos

Contributing Writer, Dark Reading

December 19, 2022

`crossenv` malware on the npm registry

On August 1, a user notified us [via Twitter](#) that a package with a name very similar to the popular cross-env package was sending environment variables from its installation context out to npm.hacktask.net. We reported this immediately and took action to remove the package. Further investigation led us to 40 packages in total.

A BEAUTIFUL FACTORY FOR MALICIOUS PACKAGES

@ Jossef Harush ✍ Co-authors Aviad Gershon and Tal Folkman 📅 March 28, 2022

🕒 Reading Time: 11 minutes

Update: IconBurst NPM software supply chain attack grabs data from apps and websites

Subvert Legitimate Package



I've been using this package for years! Time to update!

Here you go, just a regular update, don't think about it too much



Thanks! Wasn't going to!



Subvert legitimate package - Examples

Malicious code in the PureScript npm installer

12 Jul 2019

Backdoor Found in Themes and Plugins from AccessPress Themes

Updated on June 11, 2022 - Harald Eilertsen

Thousands of npm accounts use email addresses with expired domains

TECH / SECURITY

Open source developer corrupts widely-used libraries, affecting tons of projects

Dependency Confusion Demo



Actual footage of a cybersecurity job requirements list



How do we protect ourselves?

- [SG-001] Software Bill of Materials (SBOM)
- [SG-002] Patch Management
- [SG-003] Software Composition Analysis (SCA)
- [SG-005] Application Security Testing (AST)
- [SG-006] Runtime Application Self-Protection (RASP)
- [SG-010] Prevent Script Execution
- [SG-013] Use of Security, Quality and Health Metrics
- [SG-014] Code Isolation and Sandboxing
- [SG-023] Audit
- [SG-024] Security Assessment
- [SG-025] Vulnerability Assessment
- [SG-026] Penetration Testing
- [SG-036] Integrate Open Source Vulnerability scanners into CI/CD pipelines
- [SG-039] Establish vetting process for open-source components

- [SG-007] Code Signing
- [SG-008] Build Dependencies from Source
- [SG-037] Reproducible builds
- [SG-043] Integrity check of dependencies through cryptographic hashes

- [SG-007] Code Signing
- [SG-011] Typo Guard
- [SG-012] Typo Detection
- [SG-038] Preventive squatting

- [SG-009] Remove un-used Dependencies
- [SG-029] Version Pinning