



# SIGNED, SEALED, DELIVERED:

## ABUSING TRUST IN SOFTWARE SUPPLY CHAIN ATTACKS

# WHOAMI

---


- ❖ Threat Intel Analyst with a Bank
- ❖ Founding member of The Diana Initiative, supporting diversity and equality in tech
- ❖ Member of C3X College Student Cyber simulation
- ❖ Specialized honours degree, Political Science
- ❖ ITIL
  
- ❖ DISCLAIMER: The views expressed here today are mine alone and not those of my employer

# AGENDA

---

- ❖ Software Supply Chain Attacks
- ❖ Code Dependencies
- ❖ Mistakes and Misconfigurations
- ❖ It's Happened Before
- ❖ Adversarial Inclinations
- ❖ Lessons Learned – Apply Now



The background is a dark blue gradient. In the corners, there are white line-art graphics resembling circuit boards or neural networks, with lines connecting to small circles.

**AS LONG AS YOU CAN OWN THE  
PEOPLE YOU CAN OWN THE  
WORLD.”**

**MARC ROGERS,  
EXECUTIVE DIRECTOR OF CYBERSECURITY, OKTA**



# SOFTWARE SUPPLY CHAIN ATTACKS

Abuse of trust

# THE ABUSE OF TRUST

---

- ❖ Compromise at the source
- ❖ Insertion of malicious code into legitimate software and distributed en masse
- ❖ The compromise of a single trusted source by adversaries to control the distribution system and deliver malicious updates
- ❖ Incapacitate, disrupt, sabotage
- ❖ T1195 in Mitre ATT&CK framework for initial access

# WHO AND WHY

---

- ❖ State-sponsored threat actors
- ❖ Cyber espionage and cybercrime
- ❖ Key targets are technology, business and enterprise
- ❖ China, China China
- ❖ 27 attacks by nation state actors between 2017 and 2020

# TIMELINE

Operation  
Aurora

2009

CCleaner

2017

ASUS Live Update  
Operation  
ShadowHammer

2019

2017

Not Petya

2018

NetSarang Operation<sup>8</sup>  
Shadowpad



# OPERATION AURORA 2009

---

- ❖ State-sponsored threat actors APT17/Elderwood
- ❖ Targets were major tech companies: Google, Adobe, Akamai, Juniper networks
- ❖ Goal: access and modify source code repositories
- ❖ Exploited 0days Internet Explorer and Perforce vulnerabilities
- ❖ “The SCMs were wide open ... No one ever thought about securing them” Dmitri Alperovitch, McAfee

# NOTPETYA 2017

---

- ❖ Russian State-sponsored threat actors “Sandworm”
- ❖ Compromised M.E.Doc accounting software Ukraine
- ❖ Sandworm detonated “logic bombs” in Ukrainian governmental organizations and companies
- ❖ Linkos Group pushed M.E. Doc updates
- ❖ Sandworm hijacked update servers, backdoor access
- ❖ NotPetya: destructive cyberweapon. Eternal Blue & Mimikatz
- ❖ Global collateral damage \$10 billion

# SHADOWHAMMER 2019

---

- ❖ Chinese state-sponsored threat actors APT17/Barium
- ❖ ASUS Live Update Utility
- ❖ Pre-installed to update BIOS, UEFI, drivers etc. TRUST
- ❖ Swift and Silent: sabotaged developer tools to modify old version of Live Update
- ❖ Undetected: Signed certificates, stored on official server
- ❖ Pushed out to over 1,000,000 laptops for remote control

Supply chain attacks are scary ... because they make it clear you're trusting a whole ecology. **You're trusting every vendor whose code is on your machine and you're trusting every vendor's vendor"**

NICK WEAVER, SECURITY RESEARCHER, UC BERKELY  
INTERNATIONAL COMPUTER SCIENCE INSTITUTE

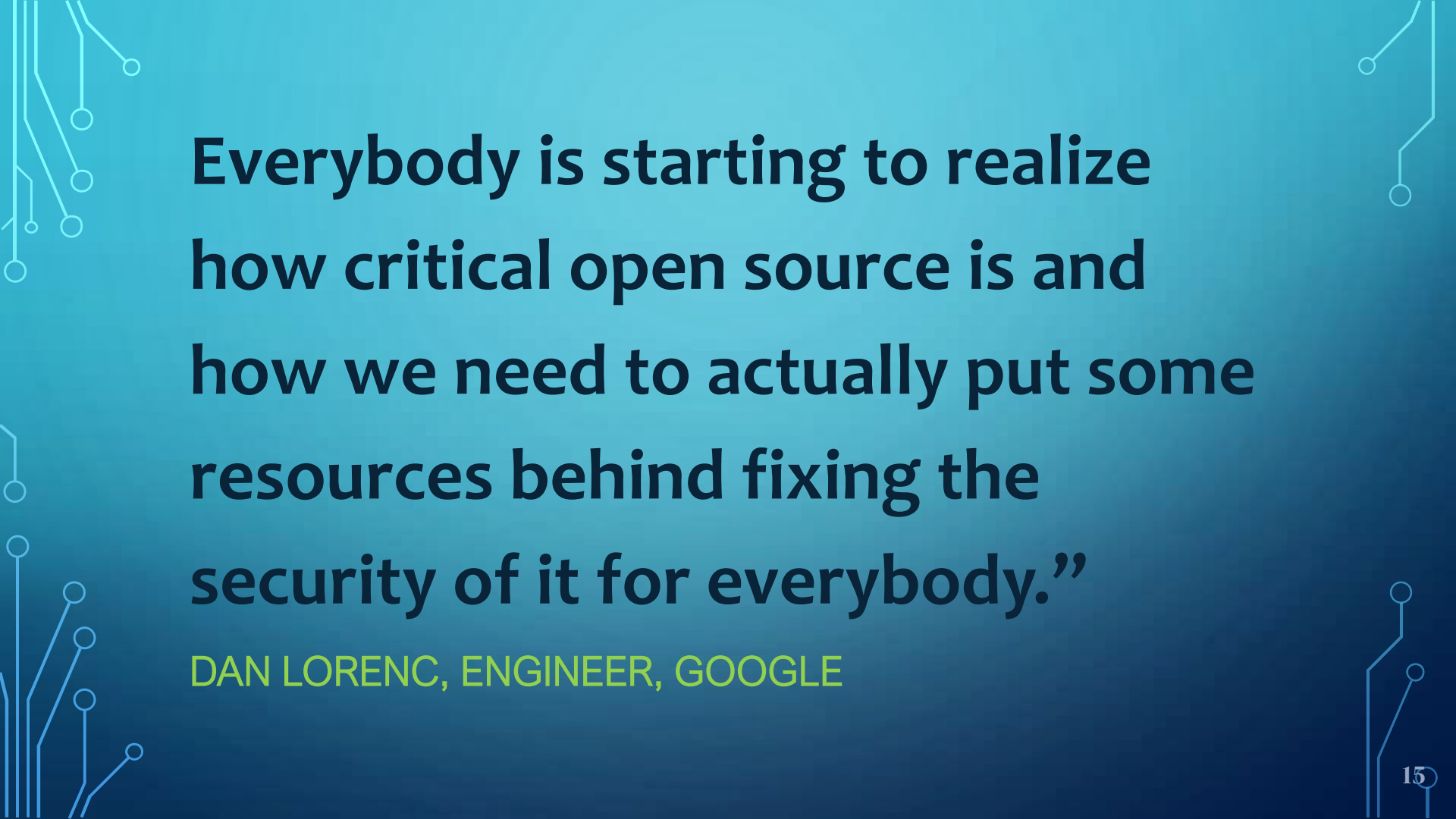
**IT'S STUFF LIKE THIS**

**THAT GIVES ME TRUST ISSUES**



# CODE DEPENDENCIES

The rise of Open Source and CI/CD pipelines

The slide features a teal-to-blue gradient background. In the corners, there are decorative white circuit-like lines with small circles at the end, resembling a PCB layout. The main text is centered and reads: 

**Everybody is starting to realize how critical open source is and how we need to actually put some resources behind fixing the security of it for everybody.”**

**DAN LORENC, ENGINEER, GOOGLE**

# CODE BREAKDOWN

---

- ❖ Average app has 118 open source libraries
- ❖ Average library 2.6 years old
- ❖ Average Java app has 50 open source vulnerabilities
- ❖ 99% of organization have 1 or more high-risk Java licences
- ❖ False positivity rates using legacy SCA tools:  
Java 23%    .NET 13%    Node 69%

<https://www.contrastsecurity.com/hubfs/DocumentsPDF/2021-Contrast-Labs-Open-Source-Security-Report.pdf>





## WHAT YOU WRITE<sup>12</sup>

- 60% release code multiple times per day; 80% do so multiple times per week
- 79% still under pressure for more speed
- 55% skip security processes to meet SDLC deadlines
- Less than 50% of application security integrated with CI/CD tools



## WHAT YOU BUILD WITH

- Developers have access to literally 1,000+ software development tools
- Work-from-home environments create greater security risks for thousands of pieces of software running with high privilege



## WHAT YOU BUY

- SaaS market to grow 25% by 2022<sup>13</sup>
- 70% indicate *"uninformed or misleading claims about security"* in a SaaS solution were cause of dissatisfaction<sup>14</sup>
- 95% of businesses host sensitive data in SaaS solutions<sup>15</sup>



## WHAT YOU USE

- 90% of applications rely on third-party libraries that comprise up to 70% of code<sup>16</sup>
- Applications on GitHub have an average of 200 dependencies<sup>17</sup>
- 73% of applications have a vulnerability traceable to third-party code

“Given recent vulnerability exposures and attacks of the software supply chain, **it is imperative that organizations pay much closer attention to the open-source code used in their applications.** There are significant risks in open-source libraries, but **identifying and remediating the ones that matter requires a different approach, one that provides a comprehensive picture of active and inactive libraries and classes, library age, vulnerabilities, and licensing issues. Legacy SCA and application security tools simply do not provide the level of accuracy and observability required**—especially when the C-suite and boards of directors are pressing for greater business acceleration.”

CONTRAST LABS OPEN SOURCE SECURITY REPORT 2021

# PWNING OPEN SOURCE

Node.js  
npm

08/2017

Arch Linux  
AUR

07/2018

PyPI Python

07/2019

05/2018

Ubuntu  
Snap Store

11/2018

Event-Stream  
npm

07/2019

RubyGems



# MISTAKES & MISCONFIGURATIONS

Oops I did it again

# CI/CD

---

- ❖ Continuous Integration and Continuous Delivery
- ❖ It's a DevOps best practice
- ❖ Good things: Collaboration, Software quality, Speed, Consistency
- ❖ Platforms: Jenkins, TeamCity, GitLab, CircleCI, Bamboo

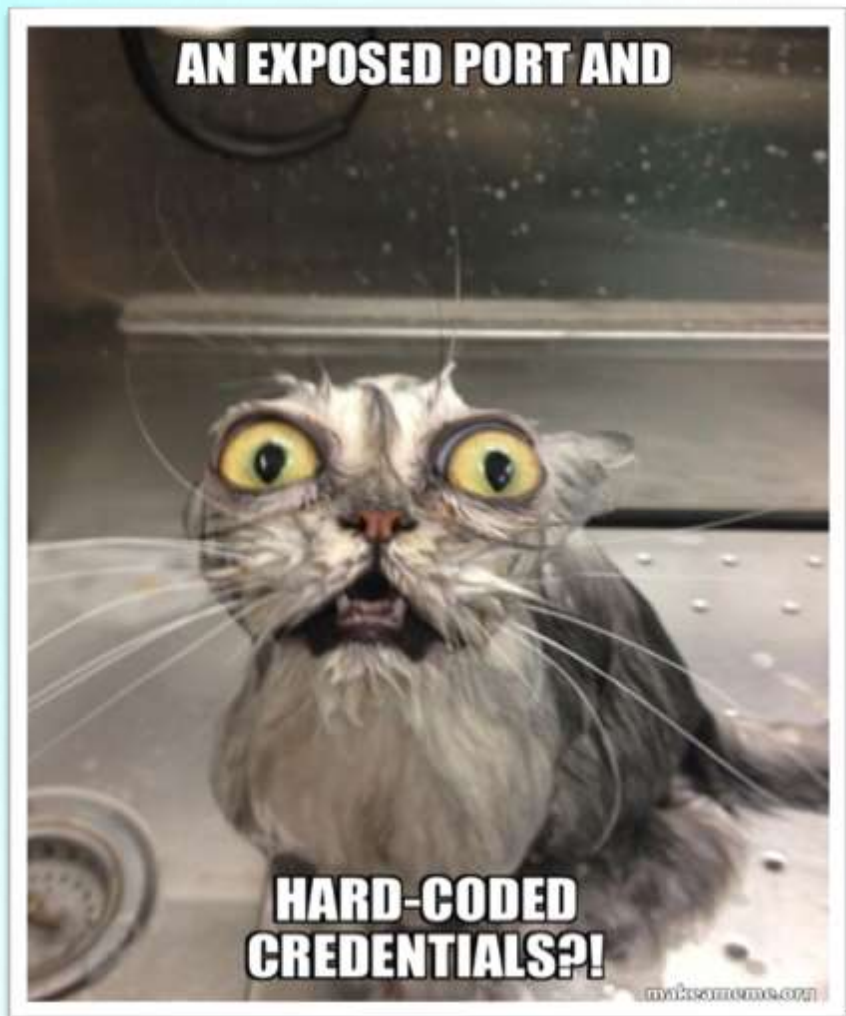
*MISTAKES WILL BE MADE*


# SONARQUBE 11/2020

---

- ❖ Open-source platform for automated code quality auditing and static analysis
- ❖ Vulnerable instances targeted multiple times
- ❖ Scanned online for exposed ports
- ❖ Access source code repos to exfil data and source code
- ❖ Default admin credentials hard-coded



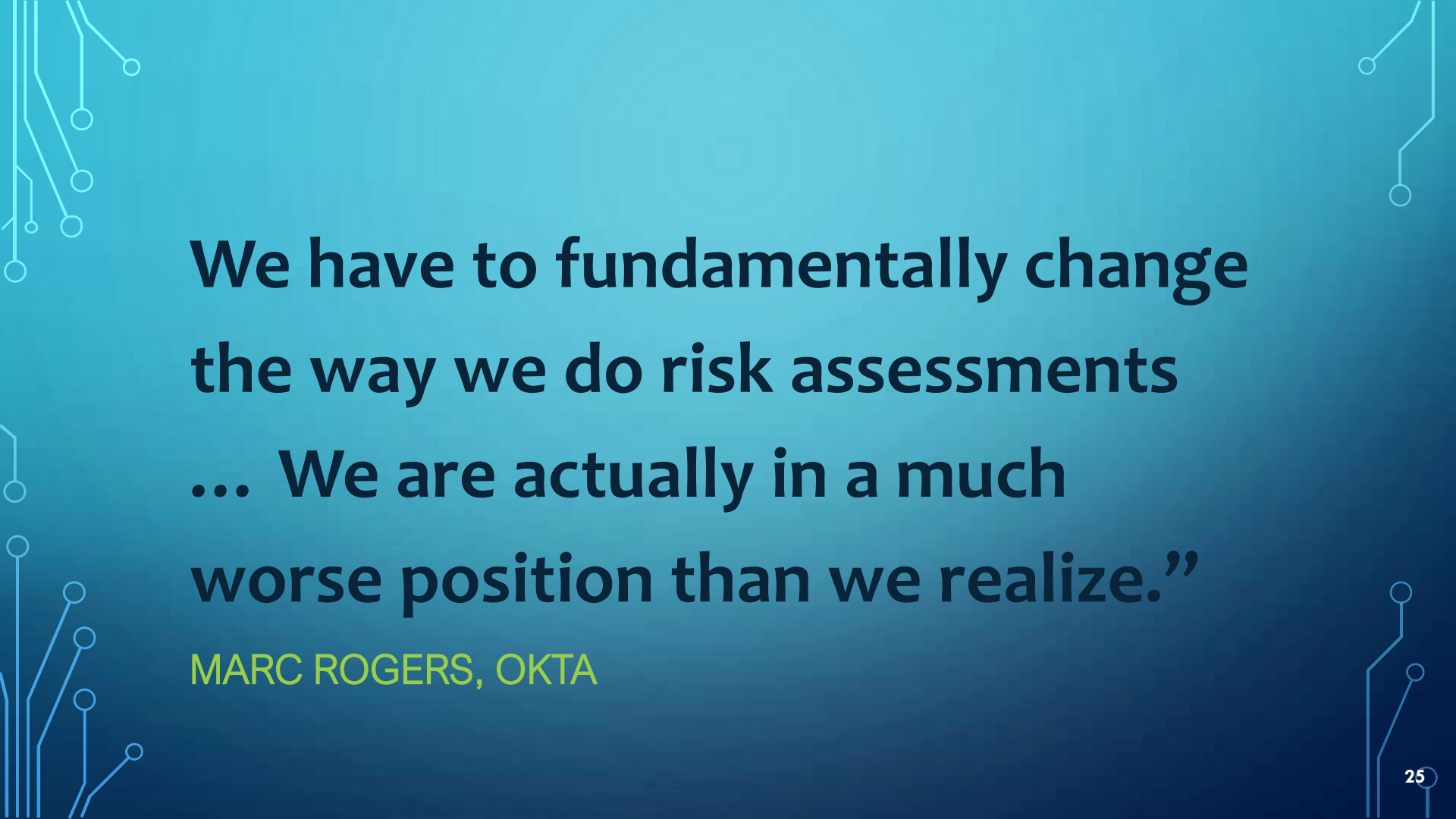


The slide features a dark blue background with white circuit-like lines in the corners. The lines consist of vertical and horizontal segments connected by small circles, resembling a printed circuit board layout. These lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Mistakes like misconfiguration and accidental credential exposure will happen in the development process, which is where InfoSec teams need to step in. Auditing infrastructure code both prior to deployment and continuously in production is essential for companies practicing DevOps and CI/CD.”

***MISTAKES WILL BE MADE***



The slide features a blue gradient background with white circuit-like lines in the corners. The main text is centered and reads: 

**We have to fundamentally change  
the way we do risk assessments  
... We are actually in a much  
worse position than we realize.”**

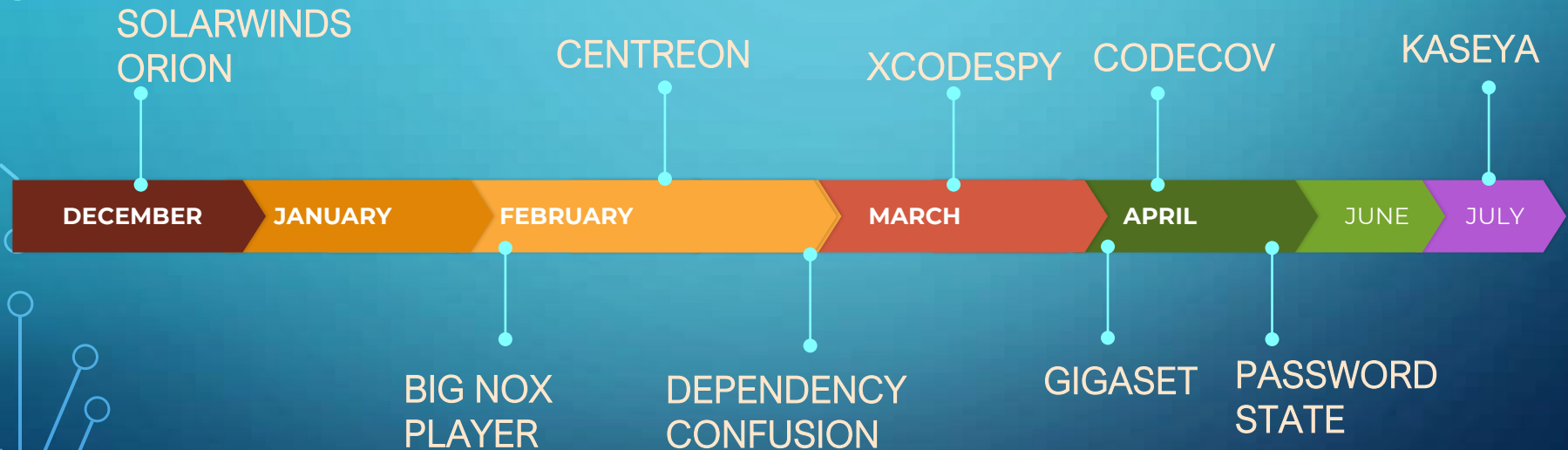
**MARC ROGERS, OKTA**



# IT'S HAPPENED BEFORE

It will happen again

# TIMELINE 2020 / 2021



# ATTACKS

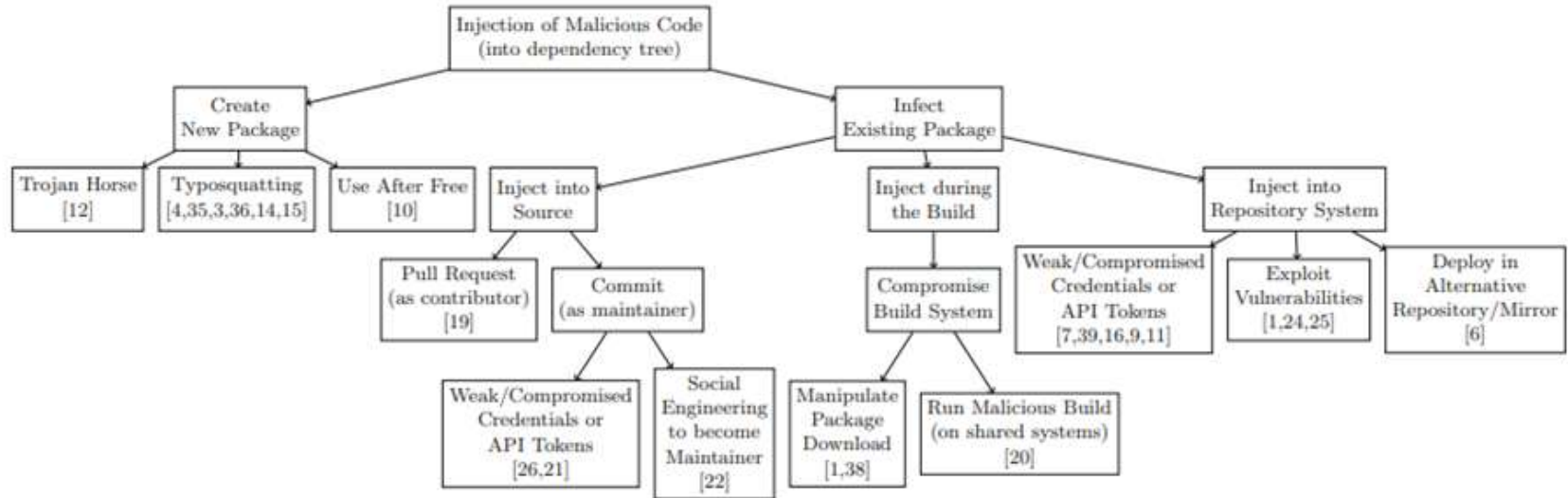
---

- ❖ Vendor Compromise
- ❖ Exploiting Third Party Applications
- ❖ Exploiting Open-Source Libraries
- ❖ Dependency Confusion
- ❖ Hostile Take-Over



<https://www.imperva.com/blog/5-ways-your-software-supply-chain-is-out-to-get-you-part-1-vendor-compromise/>

# PLAN OF ATTACK



**Fig. 2.** Attack tree to inject malicious code into dependency trees.

Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks

[https://link.springer.com/content/pdf/10.1007%2F978-3-030-52683-2\\_2.pdf](https://link.springer.com/content/pdf/10.1007%2F978-3-030-52683-2_2.pdf)

# SOLARWINDS

---

- ❖ SolarWinds Orion IT monitoring and management software
- ❖ Automated updates to 18,000 customers were compromised
- ❖ A small, highly selected number received further tailored malware attacks

# SOLARWINDS ATTACK PATH

LEVEL 1

Orion Software Pipeline Infection



CI/CD Pipeline Compromised



Trojan Deployed to Orion Customers

LEVEL 2

Target SolarWinds Customers



12-14 Day Dormant Period



Reconnaissance

Command & Control



LEVEL 3

Privilege Escalation to High Value Assets



Privilege Escalation



Fortify Access



Bypass MFA



Target Reached

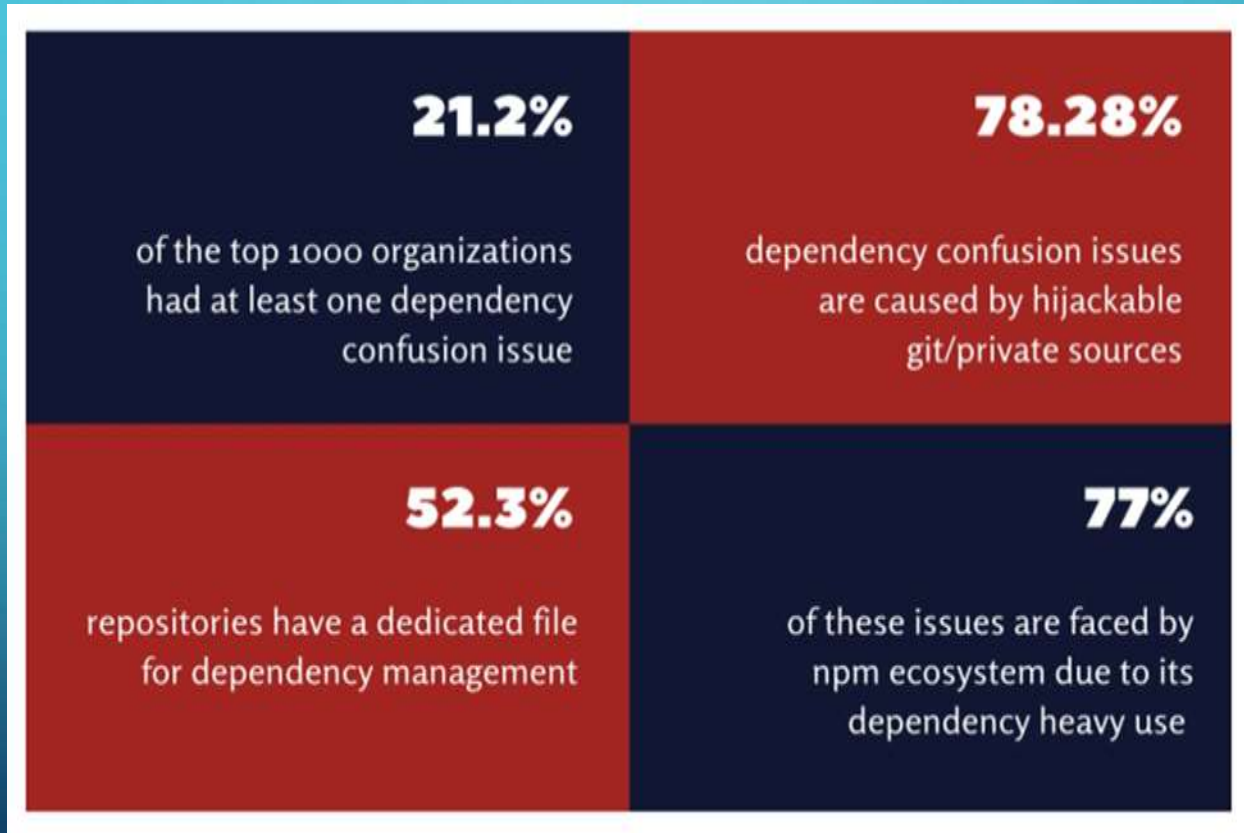
# DEPENDENCY CONFUSION

---

- ❖ Alex Birsan, security researcher
- ❖ Supply chain substitution attack hypothesis PoC
- ❖ Trick software installer script
- ❖ Pull malicious code **with the same name** from public repo not internal repo
- ❖ Targeted Apple, Microsoft, Tesla and 32 more
- ❖ Existing dependency scanners can't detect if a dependency executes malicious code



# Dependency Confusion Study



# XCODESPY

---

- ❖ New malware targets iOS developers
- ❖ Installs backdoor on developer's computer
- ❖ Attackers use legit development environment by Apple
- ❖ Victims tricked into adding online project to their app
- ❖ Targets shared sites and repositories
- ❖ Abuses the accepted norm of sharing projects online

*Abuse of trust*

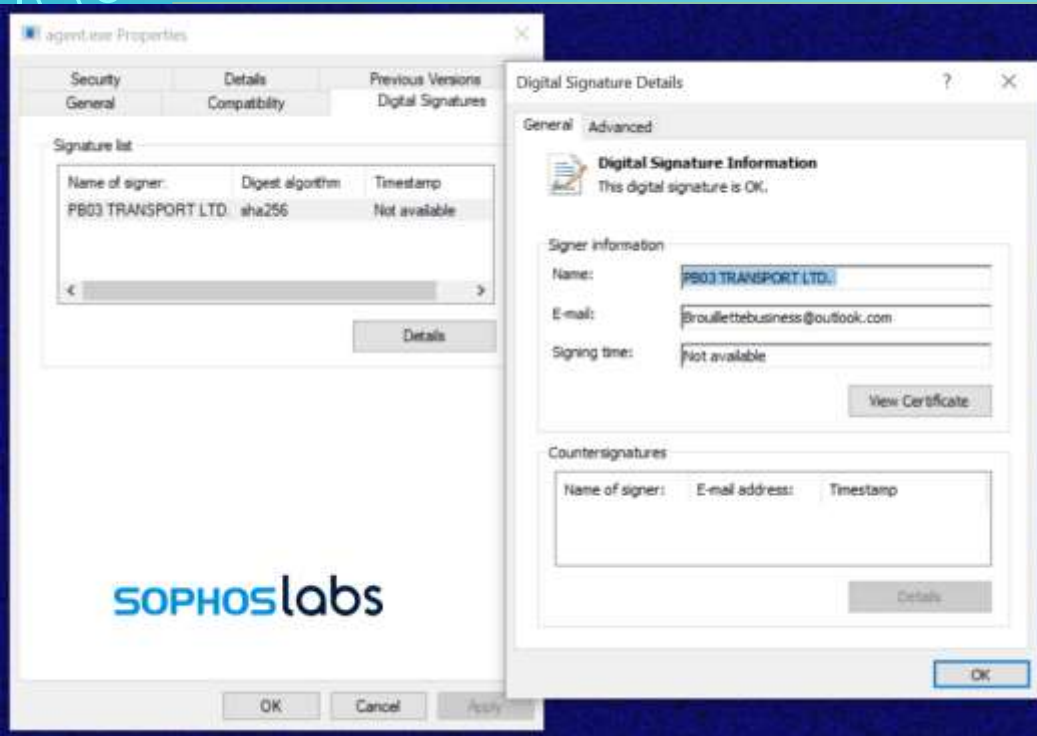
# CODECOV

---

- ❖ Online platform hosting code testing reports & stats
- ❖ 29,000 global enterprise customers
- ❖ Supply chain attack late January 2021 reported April 1
- ❖ Error in process creating Codecov Docker image
- ❖ Extract credentials that protect modification of Bash Uploader script
- ❖ Modify script to send customer deets to outside server
- ❖ Extract credentials, tokens or keys passing through the CI environment

# KASEYA

"it has a high level of trust on customer devices. By infiltrating the VSA Server, any attached client will perform whatever task the VSA Server requests without question. This is likely one of the reasons why Kaseya was targeted."



<https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers>

# KASEYA VSA AGENT HOT-FIX

---

- ❖ Automated malicious software update pushed via VSA
- ❖ 0days exploited in VSA used against MSPs
- ❖ Authentication bypass vulnerability leveraged in VSA web interface
- ❖ Uploaded malicious payload
- ❖ SQL injection to execute commands
- ❖ Attempt to disable MS Defender with signed certificate
- ❖ **TRUST ISSUES:** anti-malware software exclusions for Kaseya



# ADVERSARIAL INCLINATIONS

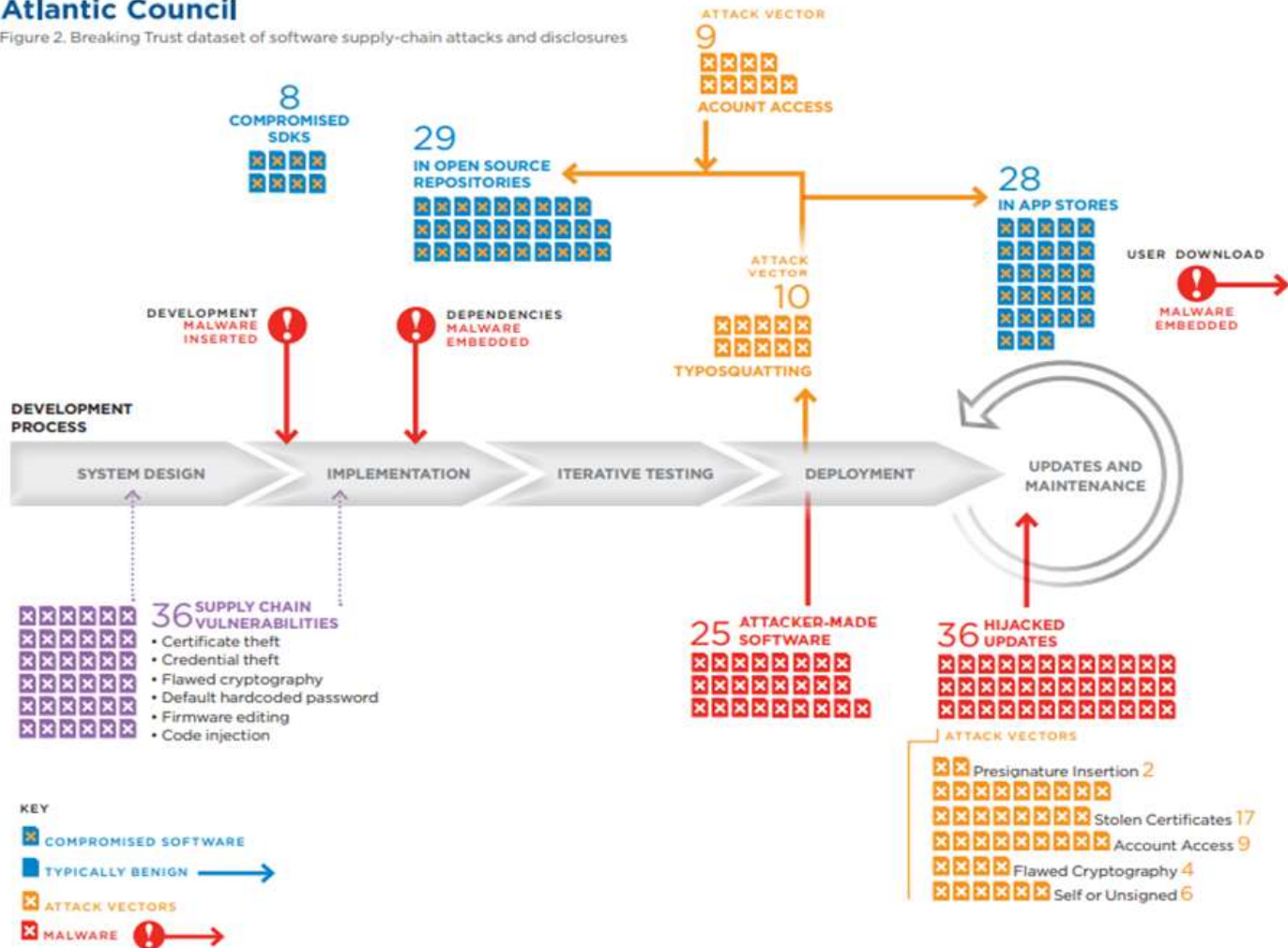
If you give an APT a cookie or a cert ...

A close-up, high-angle shot of Morpheus from the movie The Matrix. He is bald, has a serious expression, and is wearing his signature black sunglasses. The background is a blurred, dark interior. The text is overlaid in a bold, white, sans-serif font with a black outline.

**WHAT IF I TOLD YOU**

**THAT CHINA, NOT RUSSIA, HAS HISTORICALLY BEEN THE  
LEADING NATION-STATE SOURCE OF TECHNOLOGY SUPPLY CHAIN ATTACKS?**

Figure 2. Breaking Trust dataset of software supply-chain attacks and disclosures





# CHINA! CHINA! CHINA!

Kingslayer

CCleaner

2017

ASUS Live Update  
Operation  
ShadowHammer

2019

Able  
Desktop

2020

SITA

2021

2009

Operation  
Aurora

2017

NetSarang Operation  
Shadowpad

2020

SignSight

2020

GoldenSpy

41

# 2017 CCLEANER

---

- ❖ APT17 Axiom Group
- ❖ Intrusion to alter source code of product widely downloaded
- ❖ Initial access involved reused credentials and TeamViewer
- ❖ Compromised version came with signed certificates from the software vendor



# 2017 CCLEANER

---

- ❖ **Reconnaissance:** Gather victim information: host, identity, network, org. Possibly scanning. Search victim-owned websites
- ❖ **Initial compromise:** access unattended workstation of Ccleaner developer connected to Piriform network via TeamViewer remote. Credential reuse.
- ❖ Deliver malware using VBScript
- ❖ **Weaponization:** Developed malicious version of CCleaner
- ❖ **Delivery:** Use RDP to open backdoor on second unattended connected computer. Drop binary and malicious payload of 2<sup>nd</sup> stage malware. Deliver to 40 Ccleaner users

# 2017 CCLEANER

---

- ❖ **Delivery:** Compiled customized version of ShadowPad backdoor to allow further malicious downloads and data theft to prepare for third stage
- ❖ Installed 3<sup>rd</sup> stage payload
- ❖ **Exploitation:** infiltrate other computers via keylogger installed on compromised systems to steal credentials. Login using admin privileges through RDP
- ❖ **Installation:** Replaced original version of Ccleaner on the official website with the backdoored version. Distributed to millions
- ❖ **C&C:** send stolen data back
- ❖ **Action on Objectives:** possible data theft for espionage purposes

# 2017 SHADOWPAD

---

- ❖ Targeted Netsarang server software management platform
- ❖ Backdoor attack to allow downloads or data theft
- ❖ Malicious module hidden in a code library made suspect DNS requests
- ❖ Full backdoor for system compromise would be sent
- ❖ Similar tactics used by Chinese APTs Winnti and PlugX

# 2019 SHADOWHAMMER

---

- ❖ APT17 Barium
- ❖ Targeted ASUS Live Update Utility
- ❖ Pre-installed, used to auto-update BIOS, UEFI, drivers and applications
- ❖ Backdoor attack
- ❖ Modified older version of Asus Live Update software for distribution: signed, sealed, delivered

# 2020 ABLE DESKTOP

---

- ❖ Compromised Able Desktop chat software used by Mongolian government agencies
- ❖ Hijacked updates of software supply chain
- ❖ Targets private sector and government users in Mongolia
- ❖ APT group LuckyMouse

# 2020 SIGN SIGHT

---

- ❖ Targeted Vietnam Government Certification Authority
- ❖ Compromised agency's digital signature toolkit to install backdoor on target systems
- ❖ Modified software installers hosted on the government certification site
- ❖ Spyware tool "PhantomNet"
- ❖ Possibly TA428, espionage





# 2020 GOLDENSPY

---

- ❖ Targets businesses, notably Western, setting up in China
- ❖ Required tax payment software issued by local banks
- ❖ Produced by Golden Tax Department, Aisino Corporation
- ❖ Installs backdoor through GoldenSpy malware embedded in tax software.
- ❖ Persistent: Removal of tax software does not remove GoldenSpy
- ❖ System level privileges. Upload and execute any software
- ❖ Connected to C&C distinct from the tax software network



# LESSONS LEARNED

*Apply now*

**The new Executive Order is a great step forward but will take effort to understand all their dependencies and the vendors they use and the dependencies they bring**

**ROYAL HANSEN, VP SECURITY, GOOGLE**



**YOU GET DEPENDENCIES! YOU GET  
DEPENDENCIES!**



**AND YOU GET DEPENDENCIES!**

makeameme.org

# NOW WHAT DO WE DO?

---

- ❖ Prompt communication, information sharing through mandatory reporting
- ❖ Code signing
- ❖ Make tech secure by default
- ❖ SBOMs for all the things
- ❖ Set a level of international norms with clear penalties for attacks against critical infrastructure
- ❖ The new Executive Order

# TAKEAWAYS

---

- ❖ Pay more attention to the open-source code you use
- ❖ Change what we've been doing to identify and remediate risks
- ❖ Move on from legacy security and SCA tools
- ❖ Sigstore
- ❖ Package Hunter

*WE NEED TO LEVEL UP*



# SIGSTORE

❖ [https://sigstore.dev/what\\_is\\_sigstore/](https://sigstore.dev/what_is_sigstore/)

The screenshot shows the sigstore website with a news article titled "GitHub hacked, millions of projects at risk of being modified or deleted". Below the article is a diagram illustrating supply chain risks. The diagram shows a flow from Developers to Build systems (CI, Compilers), then to Code reviewers, and finally to Consumers. A red virus icon is shown infecting the flow between Build systems and Code reviewers. A list of risks is provided on the left side of the diagram.

- Replay / freeze attacks
- Compromised keys
- SSO Compromise
- Malicious hashes
- Compromise of build systems
- Easy reconnaissance (open configuration)

The diagram also includes icons for various components: Developers, Build systems (CI, Compilers), Code reviewers, package, Artifact (container,), Code Dependency, and Consumers.

# PACKAGE HUNTER

<https://gitlab.com/gitlab-org/security-products/package-hunter/-/blob/main/README.md#installation>





**Your chain is only as good as its weakest link and there are more ways to abuse the chain of trust than people realize.”**

**MARC ROGERS, OKTA**

**<https://risky.biz/soapbox51/>**



# THANK YOU!

Twitter: @3ncr1pt3d

Blog: [whitehatcheryl.wordpress.com](http://whitehatcheryl.wordpress.com)

