Poisoning the Well:
Software Supply Chain Attacks

Cheryl Biswas
06/23/2021

A diversity-driven conference committed to helping all underrepresented genders, sexualities, races and cultures in Information Security. The Diana Initiative features multiple speaker tracks, fully expanded villages with hands-on workshops, and a women-led Capture the Flag event.

July 16-17 2021 Virtual Conference

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

MARC ROGERS,
EXECUTIVE DIRECTOR OF CYBERSECURITY, OKTA

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 subvert the distribution system and push malicious updates
- T1195 in Mitre ATT&CK framework for initial access

> “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

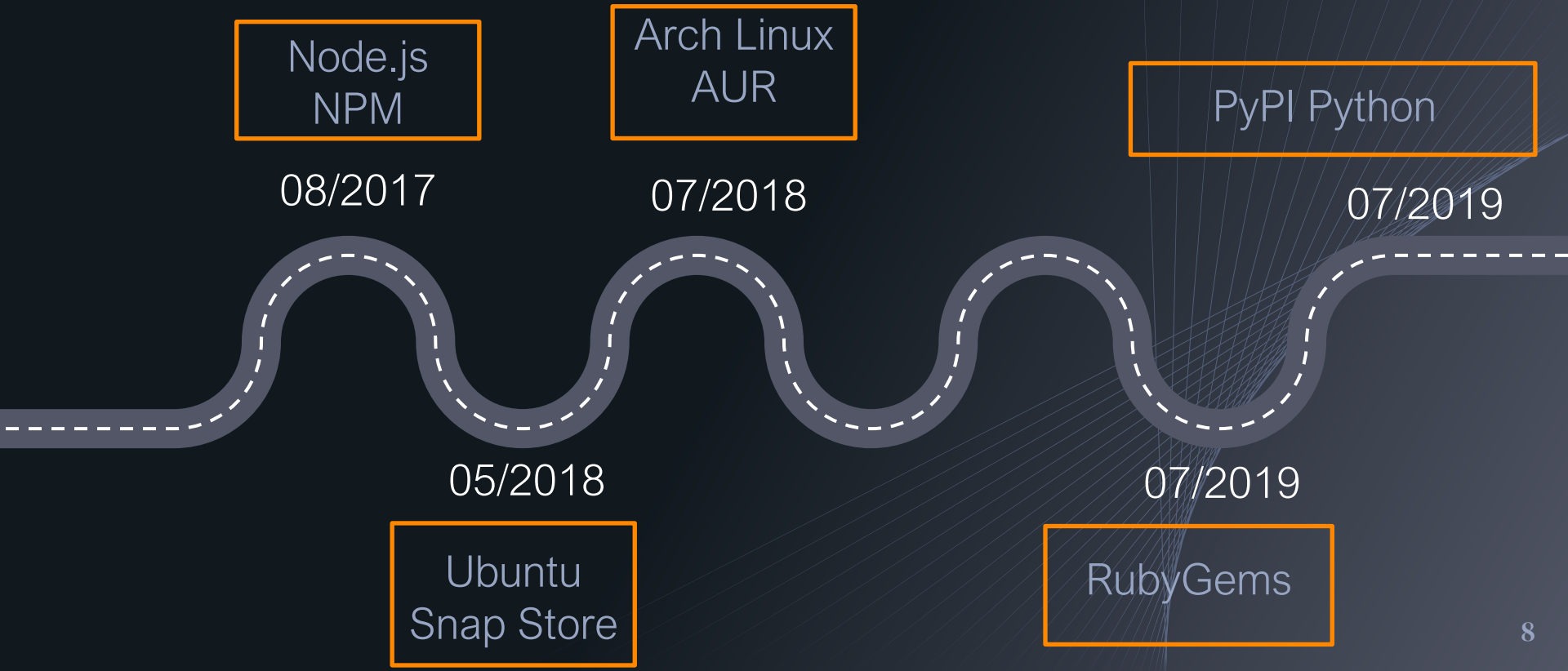
Who and Why

- State-sponsored threat actors
- Cyber espionage
- Hybridization attacks, augment conventional forces
- Incapacitate, disrupt, sabotage
- Key targets are business and enterprise
- Technology industry
- 27 attacks by nation state actors between 2017 and 2020

“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

Owning Open Source



> “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

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

> “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.”

> Several of the source code repositories also contained hard-coded credentials, which open the door to accessing other resources and expansion of the breach. It is a best practice to never commit code with hard-coded/plaintext credentials to your repositories.

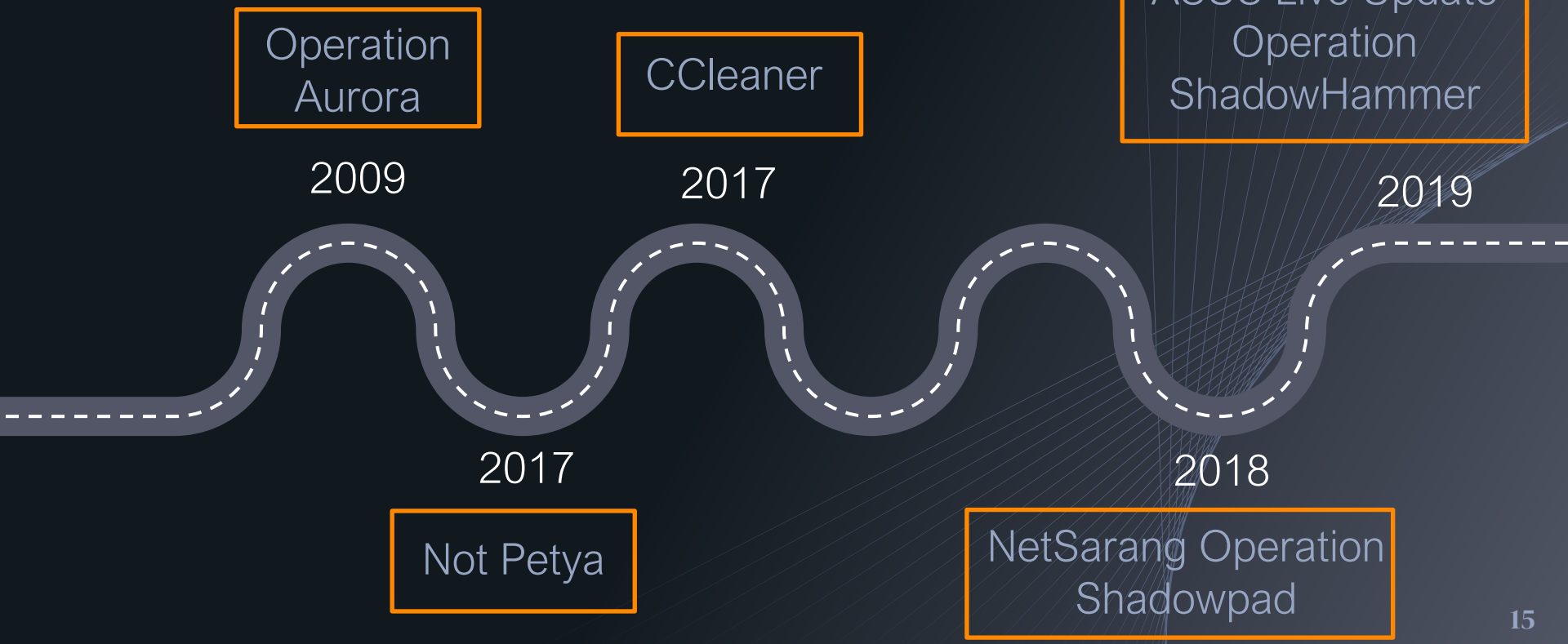
SEKHAR SARUKKAI, MCAFEE BLOG 07/31/2020


IT'S STUFF LIKE THIS
THAT GIVES ME TRUST ISSUES
memegenerator.net

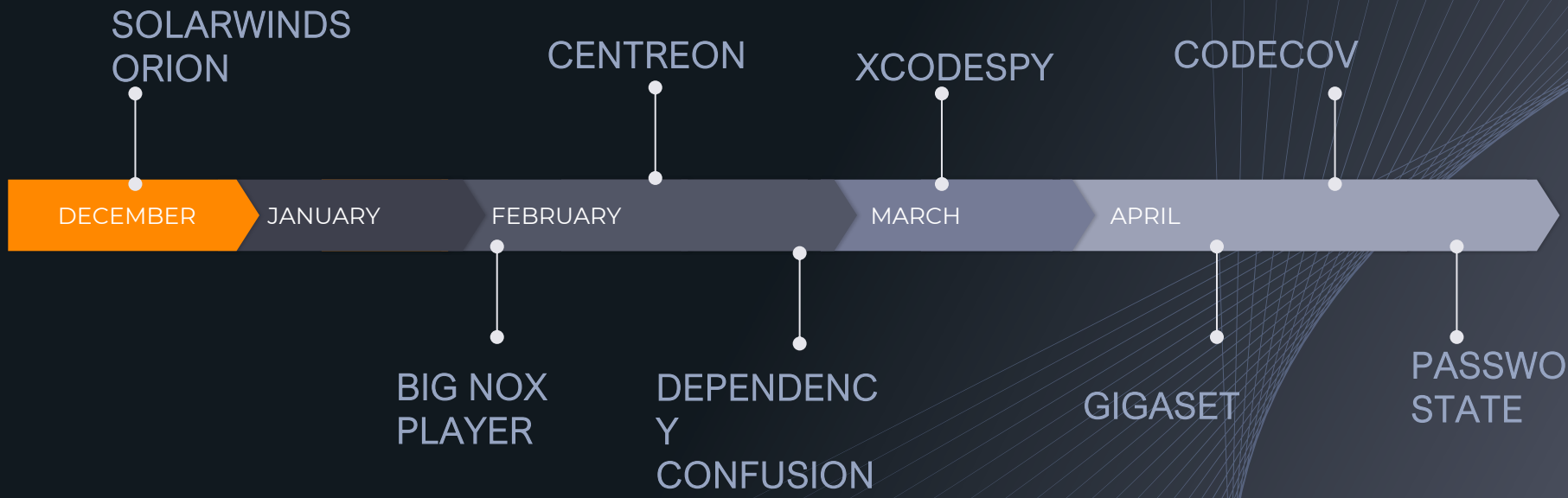
It’s Happened Before …

It will happen again

Timeline


Operation Aurora
2009
CCleaner
2017
ASUS Live Update Operation ShadowHammer
2019
2017
Not Petya
2018
NetSarang Operation Shadowpad

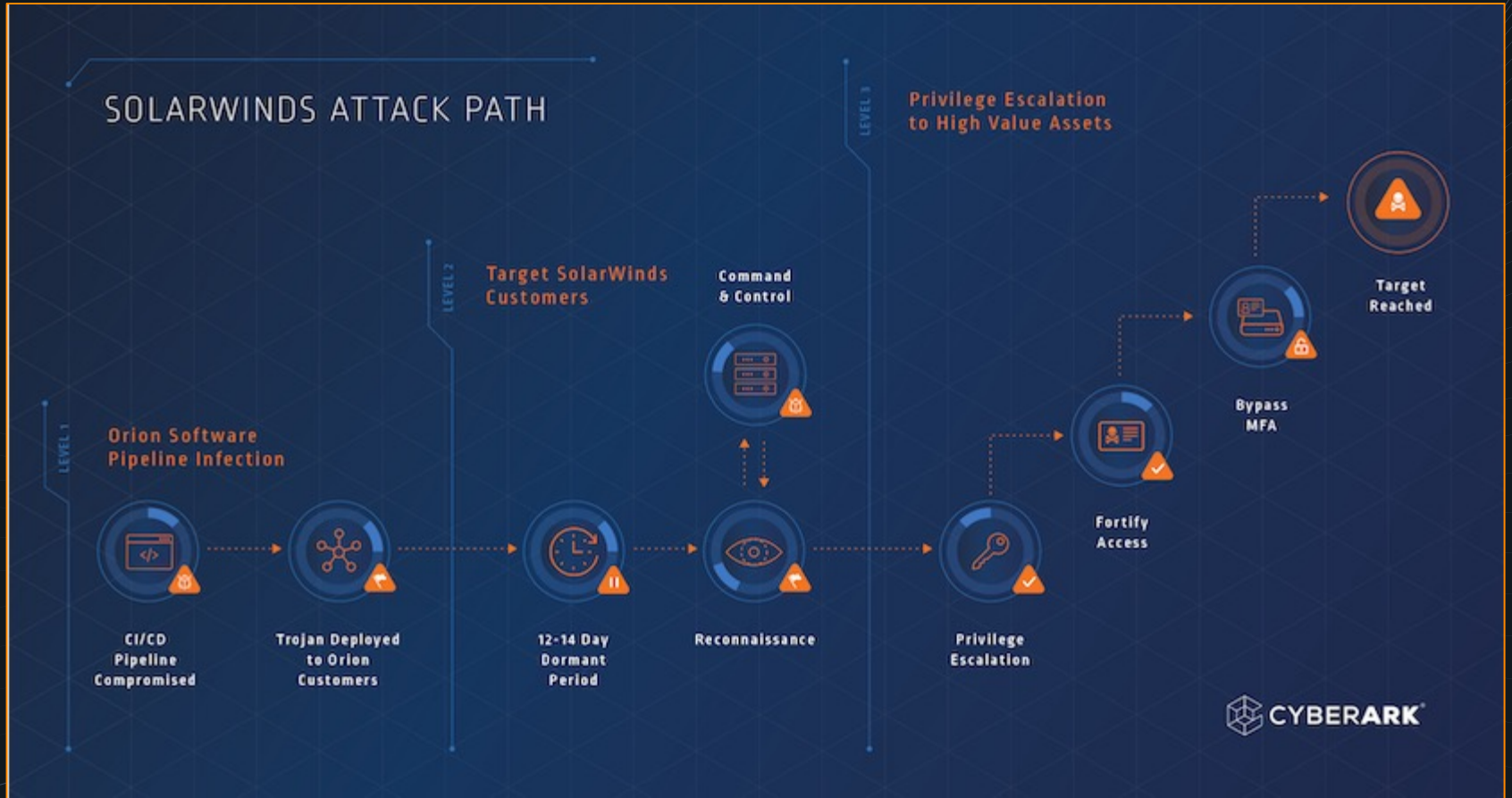
Timeline 2020 / 2021



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


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
Command & Control
Reconnaissance
LEVEL 3
Privilege Escalation to High Value Assets
Privilege Escalation
Fortify Access
Bypass MFA
Target Reached
CYBERARK

Dependency Confusion

- Targeted Apple, Microsoft, Tesla and 32 more
- Security researcher Alex Birsan devised and shared hypothesis PoC. It got copied
- Supply chain substitution attack:
  - Software installer script tricked into pulling malicious code file with the same name from public repository

XCodeSpy

- Targets iOS developers
- Installs backdoor on developer's computer
- Abuses the accepted norm of sharing projects online

Codecov

- 29,000 global enterprise customers including Proctor & Gamble, Royal Bank, Atlassian, GoDaddy
- Impacted development projects like Kubernetes, Ansible
- Impacted Twilio, Rapid7 and Mercari
- Attackers could extract credentials, tokens or keys passing through the CI environment

Now What Do We Do?

- Prompt communication, information sharing through mandatory reporting
- Code signing
- Make tech secure by default
- Set a level of international norms with clear penalties for attacks against critical infrastructure
- The executive order
- Sigstore

> The new exec 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

“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

Thank You!