ActiveState

Eliminating Open Source Supply Chain Threats

How to Avoid Becoming the Next SolarWinds

ActiveState

Introductions

Nicole Schwartz

Security Product Manager
ActiveState

Dana Crane

Product Marketing Mgr
ActiveState

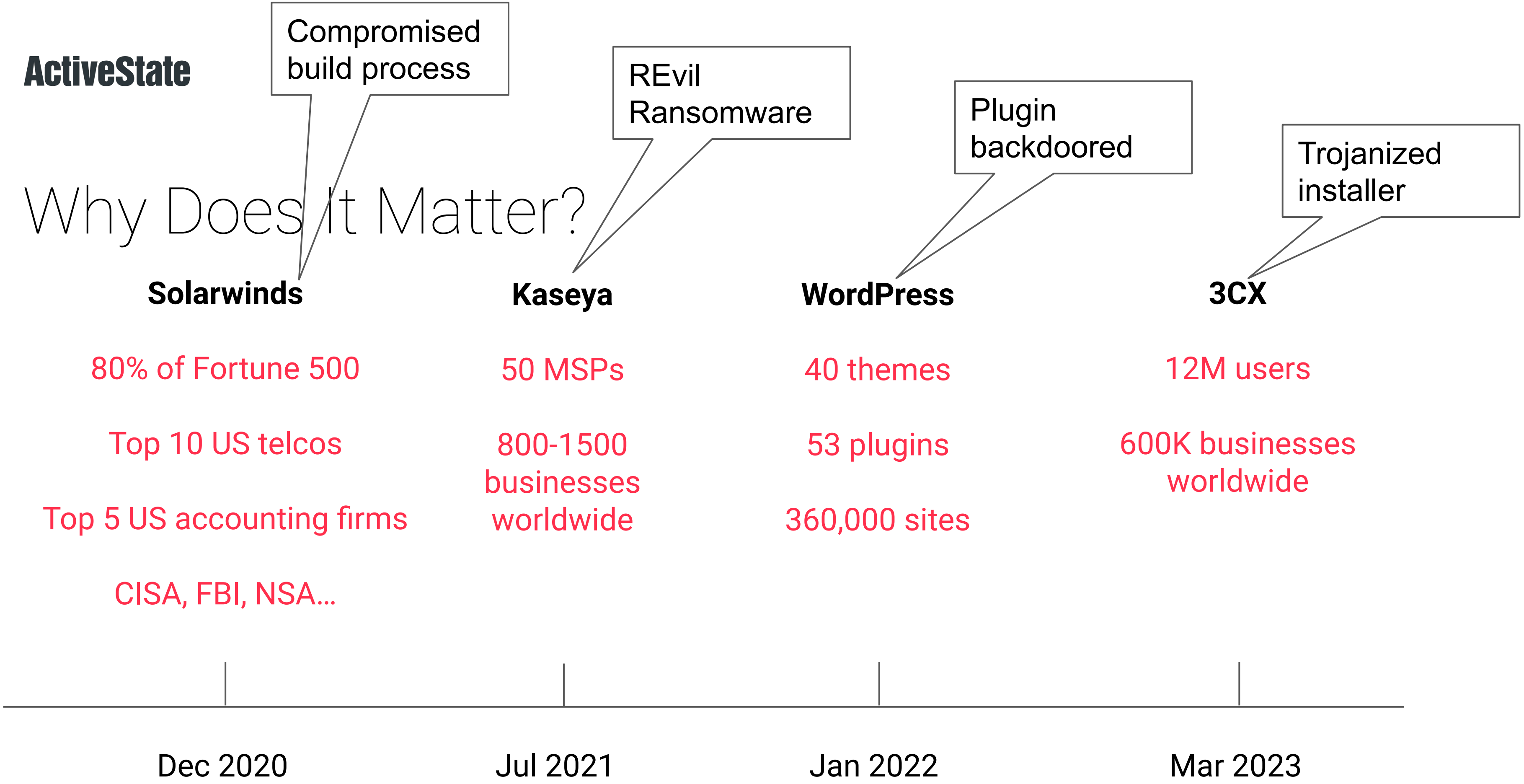
Housekeeping

- We will host polls throughout the webinar
- We will be emailing everyone the slides after the webinar
- Submit your questions in the Q&A tab and we will answer at the end

Our Mission

- Purpose
  - Create technology that just works: open source software that’s easy and safe for Enterprises and open source communities.
- What We Deliver
  - A secure open source software supply chain for the modern enterprise

Why Does It Matter?



Compromised build process

Solarwinds

80% of Fortune 500

Top 10 US telcos

Top 5 US accounting firms

CISA, FBI, NSA…

Dec 2020

REvil Ransomware

Kaseya

50 MSPs

800-1500 businesses worldwide

Jul 2021

Plugin backdoored

WordPress

40 themes

53 plugins

360,000 sites

Jan 2022

Trojanized installer

3CX

12M users

600K businesses worldwide

Mar 2023

What are Software Supply Chain Threats?

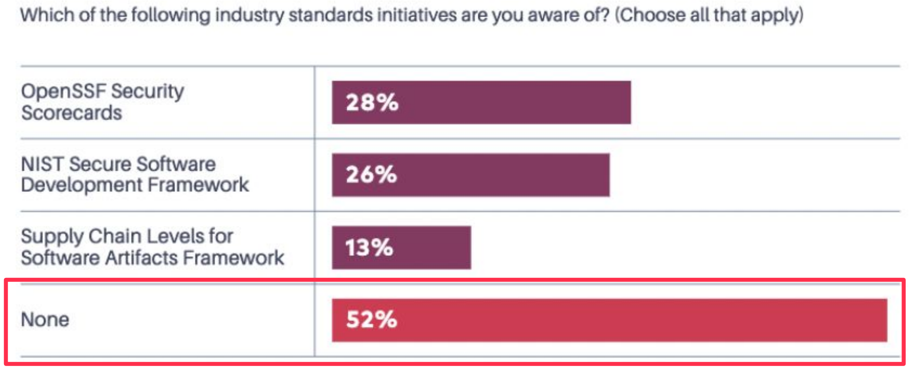
- Should we just be focused on open source vulnerabilities?
- Is it just open source code I need to worry about?
- My non-prod environments are fine, though, right?

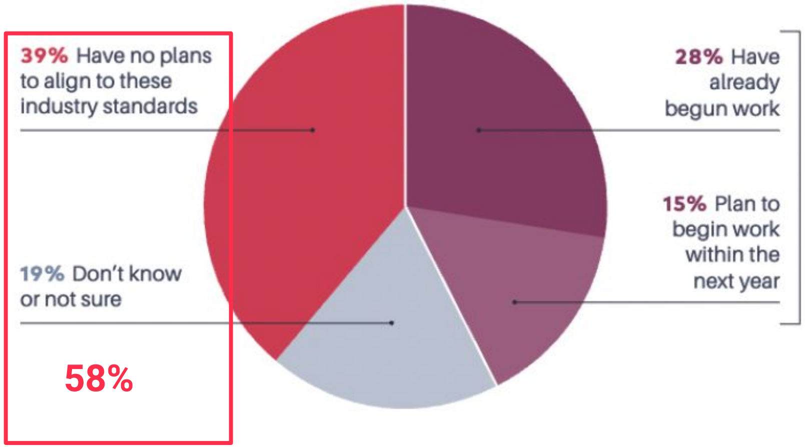
Carrots vs Sticks

- Supply Chain Security as market advantage
- Limiting ransomware attacks

- Executive Order 14028
  - June 11 - Agencies shall collect attestation letters for “critical software”
  - Sept 13 - Agencies shall collect attestation letters for all software
- Pending legislation worldwide
- US Proposal for Litigation

Open Source Maintainers to the Rescue?





Source: 2023 Tidelift State of the Open Source Maintainer Report

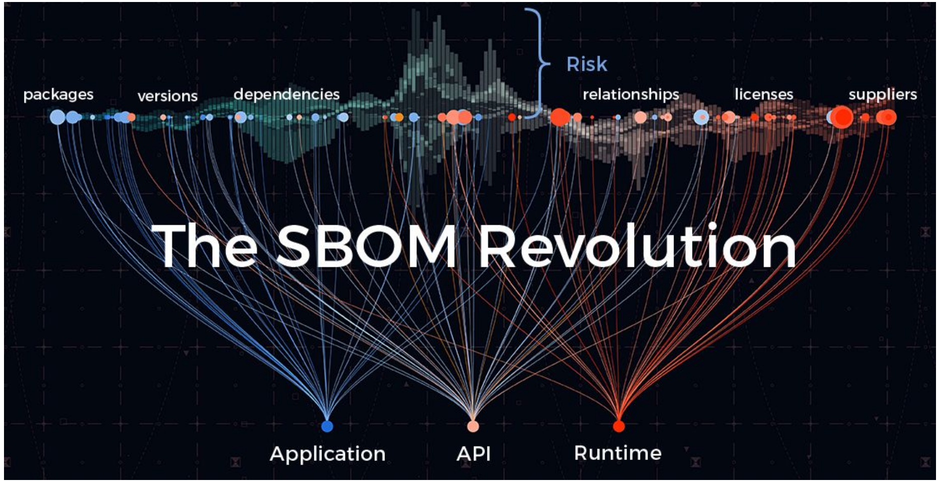
Poll: Have You Heard of These Standards?

Check all that apply:

- Yes, we are familiar with OSSF Scorecards
- Yes, we are familiar with NIST SSDF
- Yes, we are familiar with SLSA
- We are planning to implement/have implemented Scorecards
- We are planning to implement/have implemented SSDF
- We are planning to implement/have implemented SLSA

Step 1 - Get Visibility into Your Supply Chain

- Software Bill of Materials (SBOMs)
- Software Composition Analysis (SCA) tools/capabilities



Step 2 - Supply Chain Security Best Practices

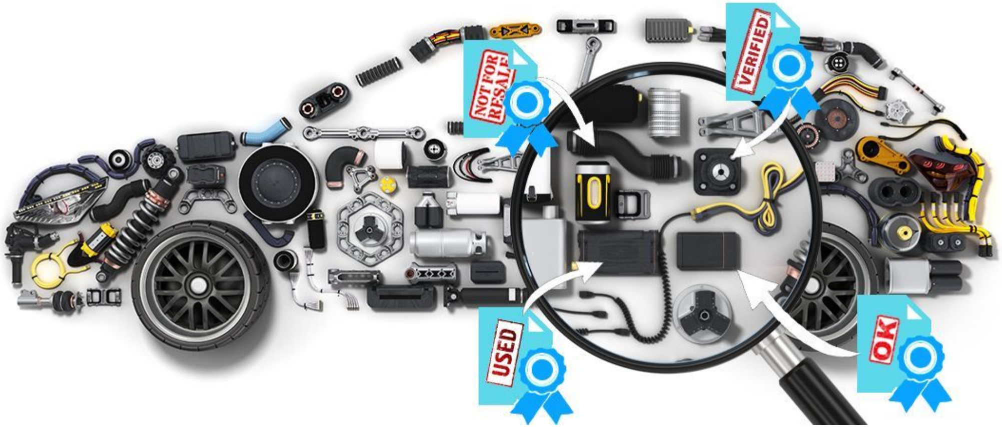
SLSA (Supply-chain Levels for Software Artifacts):

- Import process for third-party/ open source code
- Build process for software artifacts

1
2
3
4
Build
SLSA
Source
Deps
Supply chain Levels
for Software Artifacts

Step 3 - Enforcing Supply Chain Integrity

- Signed artifacts
- Software Attestations



Poll: Your Best Practices

How many of the following best practices does your organization implement? Select all that apply:

- We have a vetting process for imported code
- We build all open source packages from source code
- We create SBOMs
- We create Attestations
- We sign all our artifacts

ActiveState

ActiveState Platform Demo

ActiveState

Q&A

ActiveState

Next Steps

Schedule a demo with our product experts:
https://www.activestate.com/solutions/contact-sales/

Take our Supply Chain Security Survey & find out how you rate:
https://www.surveymonkey.com/r/BNGZPH6

Try the ActiveState Platform for free:
https://platform.activestate.com/