ActiveState

Breaking Cybersecurity Bad Habits

Without Breaking the Bank

A DevOps Perspective

Introductions

Pablo Bleck
Team Lead
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

ActiveState

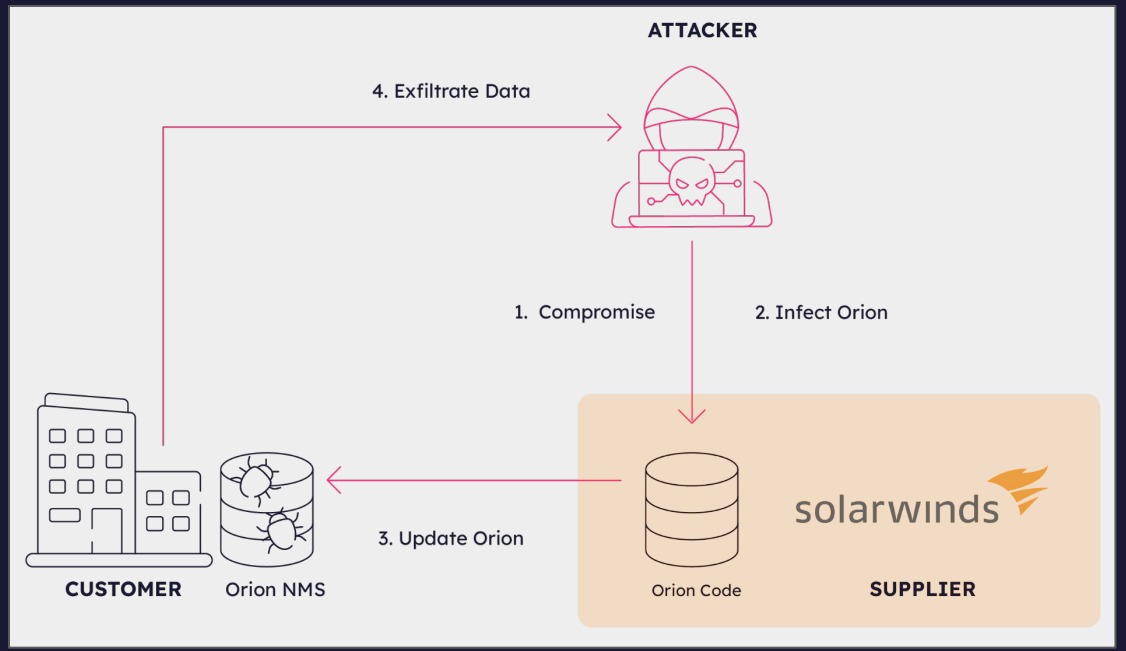
US Gov Carrots & Sticks

US Gov Software Supply Chain Attacks

Target	Multiple Gov Agencies	Colonial Pipeline	U.S. Merit Systems Protection Board	DoE, HHS, and more
Vector	Solarwinds	Ransomware	Log4j exploit	MOVEit exploit
Date	Dec 2020	May 2021	Nov 2022	June 2023

Solarwinds – December 2020

The real value of signed code is the establishment of trust, which is why this hack was so pernicious: it effectively undermined trust in signed software.



Regulations

Carrots:

- Jan 2021 - EO 14028 & M-22-18 encourage vendors to secure their software supply chain
- March 2022 - NIST releases the Secure Software Development Framework (SSDF)
- Sept 2022 - The federal government's Enduring Security Framework (ESF) working panel releases the "Securing the Software Supply Chain" report

Sticks:

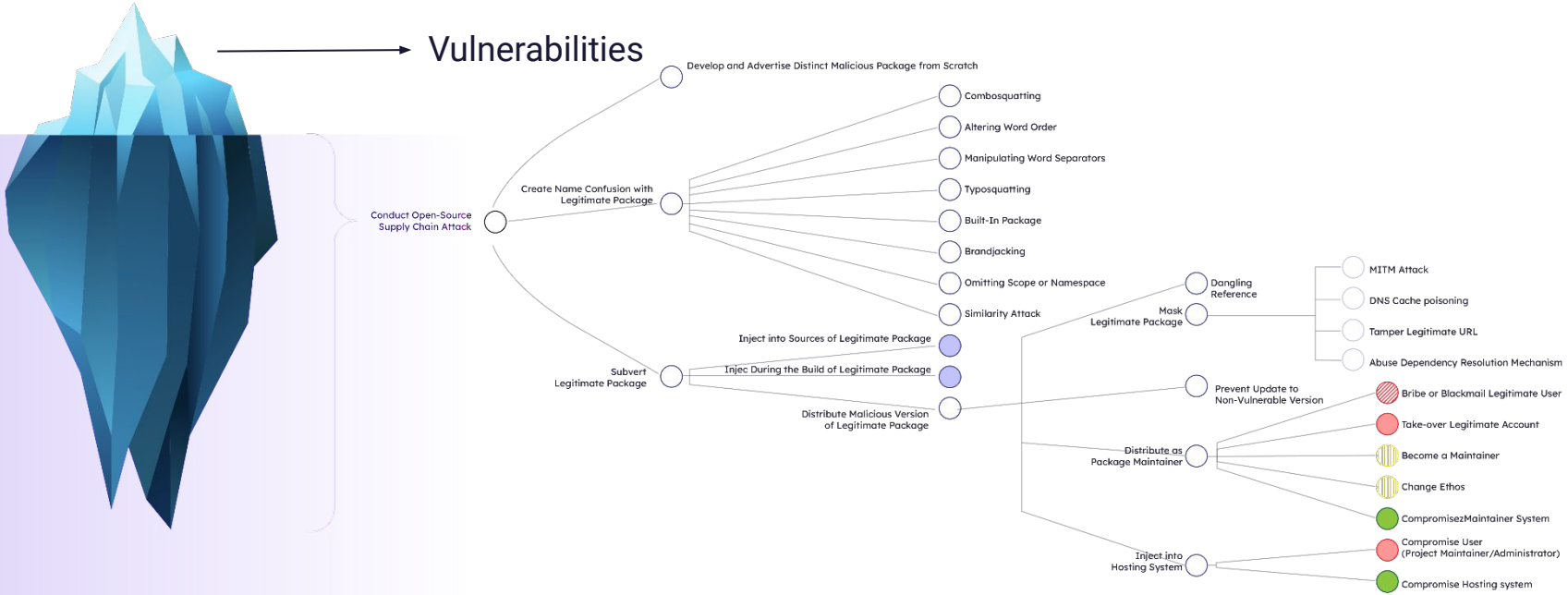
- March 2023 - National Cybersecurity Strategy 2023 proposes limiting software vendors' ability to contractually disclaim liability for poor software security
- Dec 2023 - The US Securities and Exchange Commission (SEC) Cybersecurity Disclosure Rules

Explosion of Supply Chain Attacks

Source: Sonatype

ActiveState

Vulnerabilities vs Supply Chain Threats



Source: SAP Supply Chain Risk Explorer

Litigations

- SolarWinds and its Information Security executive sued for their lax cybersecurity practices.
- Penn State University sued for falsifying security compliance reports.

  Similar cases have already resulted in over $2.2B in fines to date

- SEC rules mandate documenting -- and adhering to -- cybersecurity practices.

  The first case is First American Financial Corporation (FAFC) for deficient disclosure controls and procedures related to cybersecurity risks.

Poll

Are you aware of these regulations / best practices?

Check all that apply:

- EO14028
- NIST SSDF
- National Cybersecurity Strategy
- SEC Guidelines
- None of them

ActiveState

How Wall Street Works

ActiveState

Segregation of Duties - Big Financial Institutions

Security Architecture

Operations

Change management (Change the Bank/Keep the Bank)

Network Operations

Technology Risks

Modus Operandi

Highly in house development for increased controls

+ Much higher level of controls
+ Tighter integration with internal systems
+ Higher level of trust
- Slow change adoption
- Often efforts to reinvent the wheel/in house competing tech
- Lots of red-tape
- Frustration

ActiveState

Cybersecurity Bad Habits

Starting Unsecure

- **2023** – 2.1B open source packages are downloaded with known vulnerabilities
- **2022** – 2.1B open source packages are downloaded with known vulnerabilities

Never Updating the Codebase

> 79% of codebases are rarely updated once created
>
> -Veracode

Downloading Prebuilt Binaries

Despite the fact that:

- No details are provided about how the binary was built, or where its source code originated.
- Must blindly trust the author, as well as the authors of all the include dependencies.
- Precompiled binaries are difficult to scan in order to ensure they haven’t been compromised.

Poll

Does your company have any of these bad habits?

Check all that apply:

- Starting with an unsecure codebase
- Working with outdated codebases
- Downloading prebuilt components from open source repos
- We have no bad habits

Where does ActiveState fit in?

ActiveState Solutions

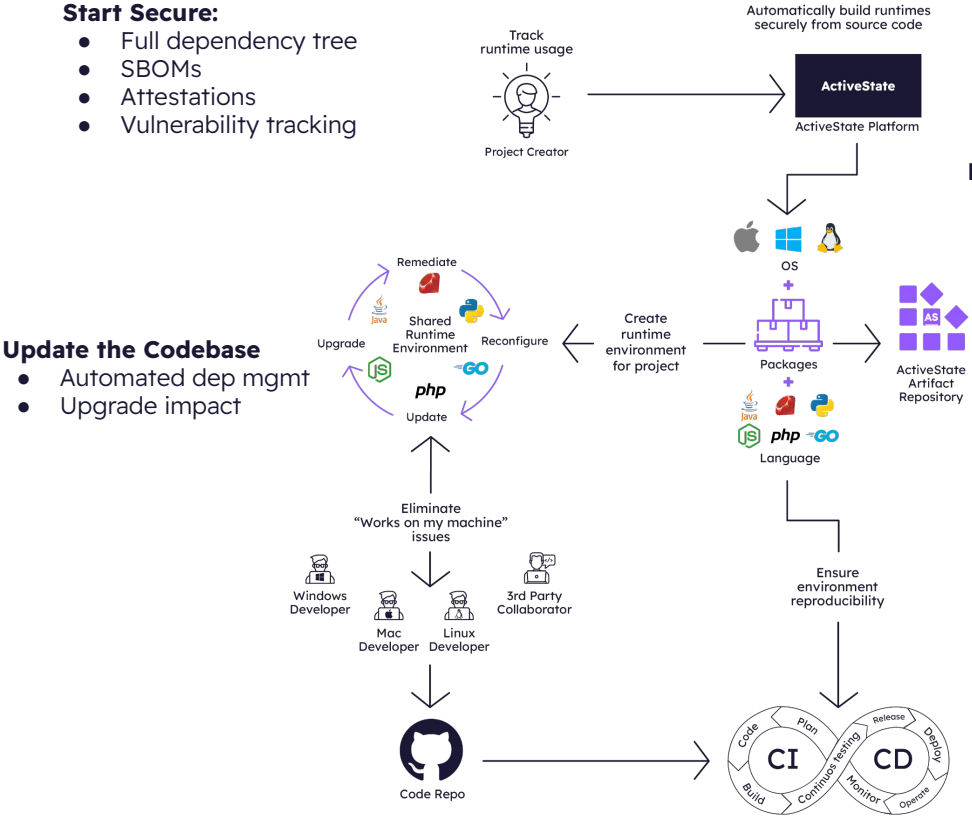
- State Tool vs Wall Street's internal tools for package management
- Integrating with Wall Street's existing systems (eg., Workday & Archive360)
- Package management that highlights vulnerabilities BEFORE you create your initial codebase
- Automated builds of dependencies from source code
- Automated dependency management when updating

ActiveState Platform

Start Secure:
- Full dependency tree
- SBOMs
- Attestations
- Vulnerability tracking

Update the Codebase
- Automated dep mgmt
- Upgrade impact

Build From Source
- Automated dependency vendoring
- SLSA build level 3
- Reproducible builds



ActiveState

ActiveState Platform Demo

Q&A

Next Steps

Schedule a discussion to get an assessment:

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/