ActiveState

ActiveState Platform's Secure Build Service

With a **650% increase** in supply chain attacks in 2020, securing your open source supply chain has never been more important. A common point of compromise for supply chain cyber attacks is the build environment, which is rarely as secure as the production environment. Compromising a build can allow hackers to inject malicious code into a patch, update or release that can potentially compromise tens of thousands of downstream customers that do nothing more than install software from their trusted vendor.

The ActiveState Platform provides a turnkey, end-to-end supply chain security solution that includes a secure build service. ActiveState imports source code vetted for licensing and maintainability, and then uses it to securely build the Python, Perl and Tcl packages your developers require. It fits with your existing development processes so you can ensure the security and integrity of the applications, services and updates you produce just by signing up.

The Weakest Link in the Software Supply Chain

The supply chain of most software vendors is extremely complex, spanning both public and private code repositories, open source tooling, point solutions from multiple vendors, and so on – all the processes, products and services used in the production of software. But of course, your supply chain is only as secure as its weakest link.

Recent attacks on **SolarWinds and Codecov** show that the build service is one of the key weak links bad actors are currently targeting. In the case of Codecov, attackers were able to obtain valid credentials from a poorly built container image, and then use them to compromise a bash script used by Codecov customers to upload their code. Once the customers downloaded and executed this script, the attackers were able to exfiltrate data from Codecov's customers.

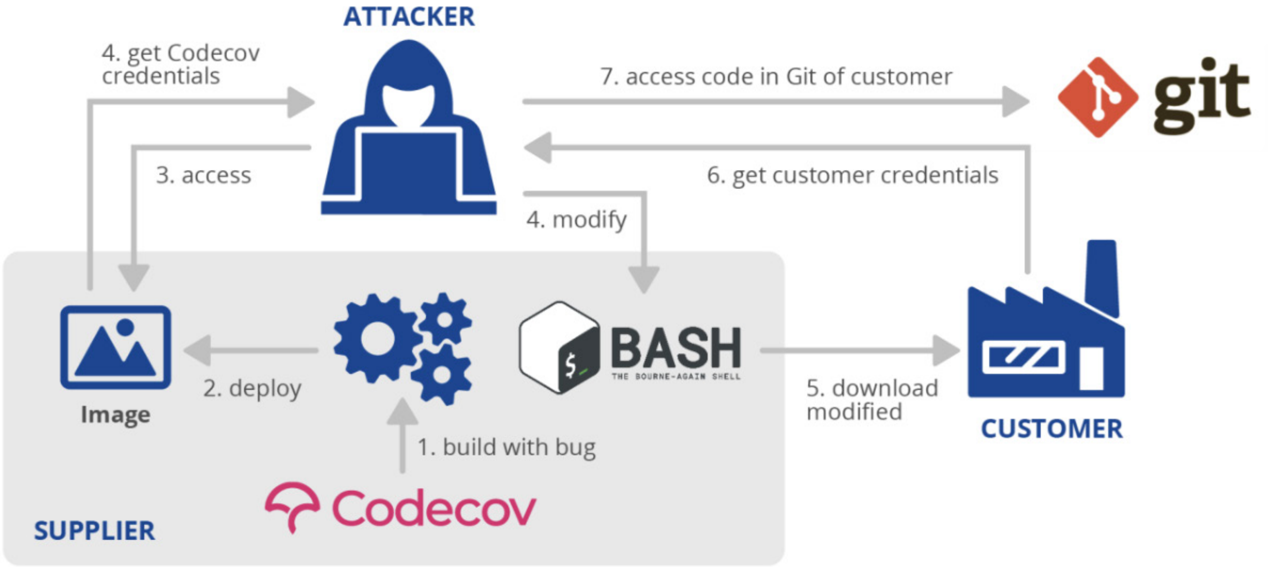

Image sourced from **ENISA Threat Landscape**

Securing the Build Service

Supply chain security starts with ensuring the security and integrity of the code you import. For example, in the case of open source components, best practices advocate importing only source code rather than prebuilt packages, especially if those prebuilt packages have not been signed by a trusted vendor. While some vendors provide signed components, most open source repositories do not sign their packages at this time.

The ActiveState Platform implements a number of controls to ensure the integrity and security of the build process, including:

- **Secure Build Service** - ActiveState's build service is just that: a dedicated service that runs on a minimal set of predefined, locked down resources rather than a developer's desktop or other arbitrary system that can offer a larger attack surface to hackers.
- **Scripted Builds** - build scripts cannot be accessed and modified within the build service, preventing exploits.
- **Ephemeral, Isolated Build Steps** - every step in a build process executes in its own container, which is discarded at the completion of each step. In other words, containers are purpose-built to perform a single function, reducing the potential for compromise.
- **Hermetic Environments** - containers have no internet access, preventing (for example) dynamic packages from including remote resources.

The result is a verifiably reproducible build, where not only do the same inputs produce the same outputs every time, but whose provenance can also be verified by tracing each component back to its original source.

ActiveState Platform: Turnkey Supply Chain Security

The ActiveState Platform provides software vendors a turnkey, supply chain security service that's quick to implement, easy to use and highly automated. Rather than cobbling together custom code and a number of point solutions from multiple vendors, the ActiveState Platform can provide an out-of-the-box, end-to-end solution saving organizations considerable time, resources and money.

ActiveState is the de-facto standard for millions of developers around the world who have been using our commercially-backed, secure open source language distributions for over 20 years. With the ActiveState Platform, developers can now automatically build their own Python, Perl or Tcl Environments for Windows, Linux or Mac—all without requiring language or operating system expertise.

You can try the ActiveState Platform by signing up for a free account at
platform.activestate.com

NORTHROP GRUMMAN NASA Honeywell GE Aviation

ActiveState

www.activestate.com

Toll-free in NA: 1-866.631.4581

solutions@activestate.com

Get a Demo

Contact Sales