SpiderOak

White Paper | November 2017

The Secure Application Updater.

Matthew Erickson

Dir. of Client Services and Technology
matt@spideroak-inc.com
+866.432.9888 x703

SpiderOak, Inc.

4741 Central St #324, Kansas City, MO 64112
+866.432.9888 | info@spideroak-inc.com

Protect your digital supply chain.

Supply chain attacks.

Digital supply chain attacks are becoming an increasingly common means of compromising an organization. Instead of making a direct attack on an organization's infrastructure, an adversary attacks the updates for software an organization depends on. This allows their attack payload to run internally without leaving any conventional trace of an attack. As software updates are commonly important for the continued secure operations of an organization, this type of attack is increasingly effective *(see figure 1 for example)*.

In all these cases, attacks can be mitigated by adding redundant points of trust to the process of creating and distributing

Supply chain attacks. (Continued)

software updates. If there is no single point of failure in the security chain, the cost of an attack can be made prohibitively expensive. A combination of effective technology and work process can be used to implement multiple independent authorities to approve a software release via cryptographic signatures, with more than one such signature required for acceptance of an update. A compromise of any one authority, or any tampering with the update itself, results in an invalid update. This ensures the software you mean to be running is the software you actually are running. Finally, with the advance of connected devices filling our lives, there's little to indicate a device may be compromised.

Protect your digital supply chain.

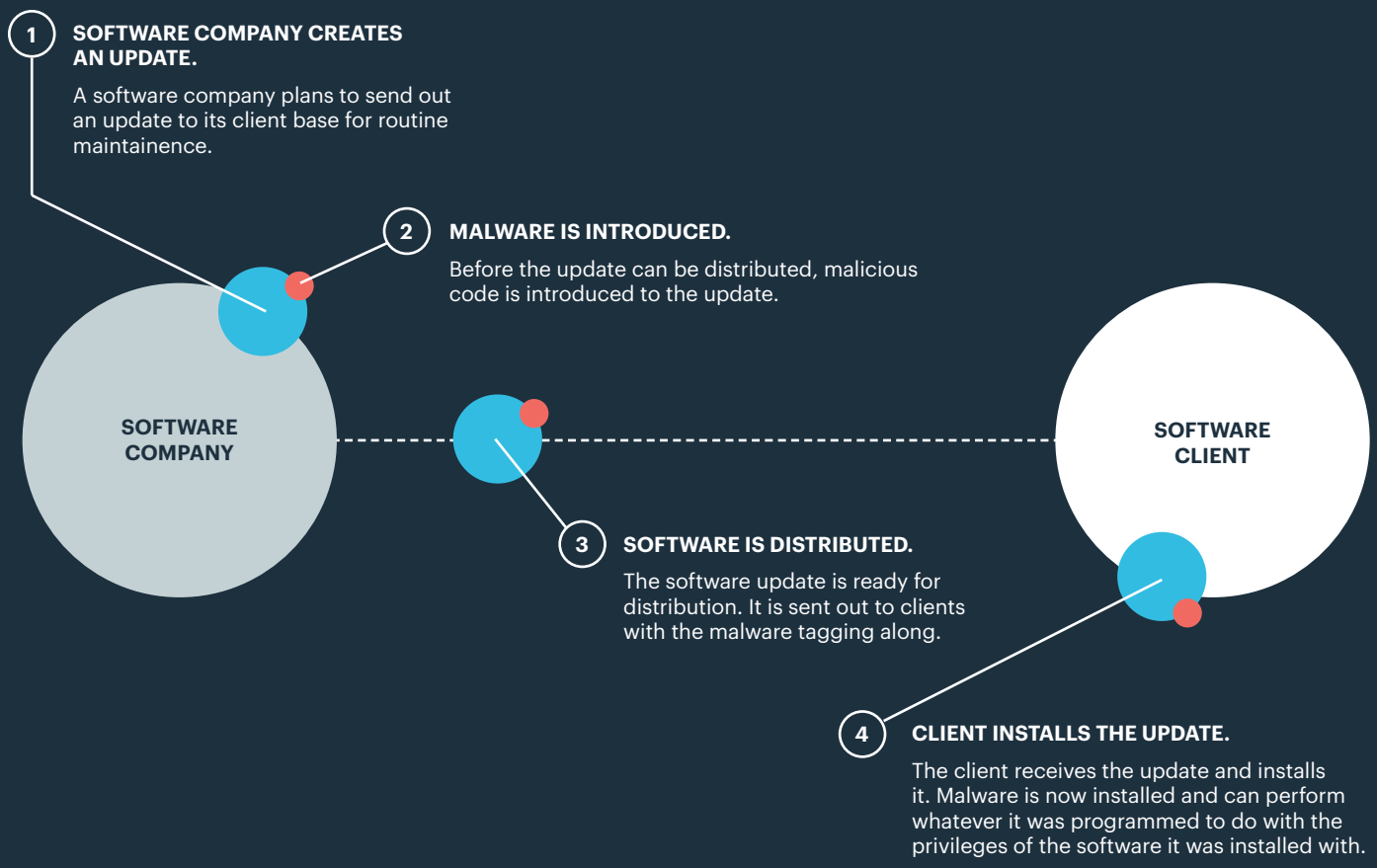
The SpiderOak Secure Application Updater, part of the SpiderOak Trusted Application Platform, provides a complete solution for producing and distributing secure software updates. It consists of an overall process around the production, audit, and release of updates, and is comprised of several components:

— Training and documentation on the creation of secure process around code review and update signatures.

— Software enabling the management of cryptographic keys and signing of update metadata.

— Software and documentation enabling the production of reproducible builds, essential for the review process.

Figure 1



The supply chain attack.

In this example, a software vendor crafts an update for its clients, but before the update can be distributed an attacker inserts malicious code that gets distributed along with the update. Other common attacks are attackers sending older versions with known vulnerabilities to be exploited, or silently blocking updates to correct known vulnerabilities in the existing software.

The Supply Chain Solution.

Decentralized Authority.

An organization making use of the Secure Application Updater will set up at least two authorities in the deployment process: a *Release Authority* and an *Integrity Authority*. The *Release Authority* is likely already in existence within an organization, and represents the person or group responsible for deciding exactly what source code is incorporated into a software release, producing the release, and signing it. This workflow will likely not change much within an organization adopting the SpiderOak Secure Application Updater.

The *Integrity Authority* is the second organization needed for the secure update process. This represents a team outside of

Decentralized Authority. (Continued)

the *Release Authority* with the following responsibilities:

— Reviewing the source code difference between the last release and this release, and ensuring that it matches the release notes without anything missing or added.

— Building the update themselves, and proving it has identical output compared to the *Release Authority*'s build.

Once the *Integrity Authority* has satisfied both of the above points, it will itself sign the update for release. An endpoint will not accept updates without valid signatures from all Authorities it knows about.

An organization may, at its choice, incorporate additional authorities in the review and signature process to provide dependable interlocks proving that updates pass various criteria. For example, an organization may include a *QA Authority* to signify the release has been shown to be free of defect. Additional authorities and their use is at the discretion of the organization making use of the Secure Application Updater.

Cryptographic key management.

Modern software update systems traditionally make use of the Public Key Infrastructure (PKI) to sign updates to protect against tampering. While this provides some protection, the PKI itself has been suffering an increasing amount of attacks. The compromise of any one key trusted by the client represents a failure of the security system; this is a key point on which the FLAME malware was able to infect target computers. SpiderOak provides tools to easily manage an independent keychain for each authority created to review and certify updates for release. These keys are not based on the public Certificate Authority infrastructure, but instead uniquely managed per authority. This eliminates attack through CA compromise or compromising the OS root CA list. Private keys are stored on Hardware Security Modules (HSMs), and the roots of trust for each keychain are intended to be kept in a physical safe (or other secure mechanism for infrequent access).

Reproducible builds.

If the software build system builds things reproducibly, the output of the build system is byte-for-byte identical for any given source code inputs. Most systems these days insert extra data into build output that prevents this from happening, such as file paths, timestamps, and build system information, none of which is required for actual operation of the software. Using reproducible builds, an organization can be sure that as long as multiple people all get the same output for the same source code, the built software accurately represents the source code. This is an essential part of the review process so an authority can be sure the updates they're releasing are the updates they mean to be releasing.

More information.

To learn more how to use the Secure Application Updater to enable complete control over your digital supply chain, reach out to us and we'll be happy to help you out.

Christopher Skinner

cskinner@spideroak-inc.com
+504.259.6700

Matthew Erickson

matt@spideroak-inc.com
+866.432.9888 x703