



Software Supply Chain Attack



Overview

The cyberattacks on organizations that were made possible by exploiting a vulnerability in the Solarwinds Orion product are exemplary of a software supply chain attack, in which a backdoor was created in a network management software used by 18,000 organizations. The associated malware has the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. All traffic was made to look like typical network traffic for a management tool.

Lookout Analysis

Mobile apps could be susceptible to software supply chain attacks, particularly as many of the apps used by employees are not provided or vetted by IT. The cyberattacks enabled by Solarwinds exploit highlight the need to have visibility into everything that touches your corporate infrastructure - especially from third-party vendors.

In the context of mobile, it can be difficult to understand app permissions and how they access, handle, or transfer data on the device. Admins need a way to make informed decisions about whether they permit employees to use specific apps on their devices without invading their privacy.

In addition, it is critical to ensure app updates are performed securely by verifying app certificates to validate they are signed by the same developer as previous versions. It is recommended to always test an app software update from a third-party vendor in a sandbox environment to ensure it is safe for your employees.

Lookout detects app risks and ensures compliance

With the rich data from our mobile app risk assessments in the Lookout Security Graph, you are able to create app scoring customized to your organization's governance, risk and compliance requirements. We enable you to understand how apps interact with each other, the geo-location of IP addresses to which an app communicates, if an app has risky or malicious components, and whether the data transfer and storage are encrypted.

Lookout Mobile Risk and Compliance

Lookout Risk and Compliance provides full visibility into the mobile apps in your organization's fleet and enables you to implement organization-wide governance, risk and compliance policies. Lookout delivers a unique capability to provide mobile application risk assessment that gives the necessary insight into app permission and data access controls. The Lookout Security Graph has aggregated the insight from analyzing more than 125 million apps across nearly 200 million devices.

[Click here to learn more about Lookout Mobile Risk & Compliance](#)