SolarWinds says fewer than 100 customers were impacted by supply chain attack

therecord.media/solarwinds-says-fewer-than-100-customers-were-impacted-by-supply-chain-attack

May 8, 2021

Texas-based software firm SolarWinds downgraded the number of customers impacted by its 2020 supply chain attack from 18,000 to less than 100.

In an SEC filing on Friday, the company said that based on new information surfaced during its investigation, such as DNS traffic records, it now believes that while 18,000 of its 300,000 customers downloaded a version of its Orion software that was tainted with the Sunburst malware, the attackers activated the malware only on a handful of customers networks.

> We now estimate that the actual number of customers who were hacked through SUNBURST to be fewer than 100. […] This information is consistent with estimates provided by U.S. government entities and other researchers and consistent with the presumption the attack was highly targeted.
>
> *SolarWinds CEO Sudhakar Ramakrishna*

SolarWinds said that while it detected around 18,000 downloads of the tainted SolarWinds Orion app, many customers did not install the downloaded version, or the Orion update was installed in air-gapped networks where the malware couldn't connect to its command-and-control server, blocking any future attacks.

The company's CEO Sudhakar Ramakrishna said the company issued this update to correct media reports from last year that incorrectly suggested that 18,000 of its customers were hacked when, in reality, the attackers only went after a handful of selected targets, such as large companies and government organizations.

This was confirmed last month by the governments of several countries, including the Biden administration, who formally accused the Russian Foreign Intelligence Service (SVR) of orchestrating the SolarWinds supply chain attack as part of a targeted cyber-espionage campaign.

Investigation into the hacker's entry point is progressing

But the SEC document filed on Friday also provided additional insight into the company's internal investigation. One of the biggest mysteries that remains to be solved is how SVR hackers gained access to SolarWinds' internal network in the first place.

The Texas software company said it is still investigating this topic and has, in the meantime, narrowed down the entry point to three possibilities:

- Zero-day vulnerability in a third-party application or device;
- Brute-force attack, such as a password spray attack; or
- Social engineering, such as a targeted phishing attack.

SolarWinds also said that while they "don't know precisely when or how the threat actor first gained access to [their] environment," the company found new evidence that the threat actor compromised internal credentials and moved around its internal network and Microsoft Office 365 environment **for at least nine months** prior to initiating a so-called test run in October 2019, when they tested their ability to deploy malicious code inside the SolarWinds Orion app before launching the actual attack in March 2020.

In addition, SolarWinds said the SVR hackers also:

- The threat actor created and moved files that we believe contained source code for both Orion Platform software and non-Orion products. However, we are unable to determine the actual contents of those files.
- The threat actor created and moved additional files, including a file that may have contained data supporting our customer portal application. Although we're unable to determine the actual contents of the files, the information included in our customer portal databases does not contain highly sensitive personal information, such as credit card, Social Security, passport details, or bank account numbers, but contains other information such as customer name, email addresses, billing addresses, encrypted portal login credentials, IP addresses downloading any software and MAC addresses of the registered Orion servers.

- The threat actor accessed email accounts of certain personnel, some of which contained information related to current or former employees and customers. We are currently in the process of identifying all personal information contained in the emails of these accounts and expect to provide notices to any impacted individuals and other parties as appropriate.
- The threat actor moved files to a jump server, which we believe was intended to facilitate exfiltration of the files out of our environment.

SolarWinds said that it is still investigating the attack and its aftermath. The company is working with KPMG and CrowdStrike, and several government agencies.

Last month, the company revoked and issued a new digital code-signing certificate for its applications and also revamped its software build process to add post-build verification defenses.

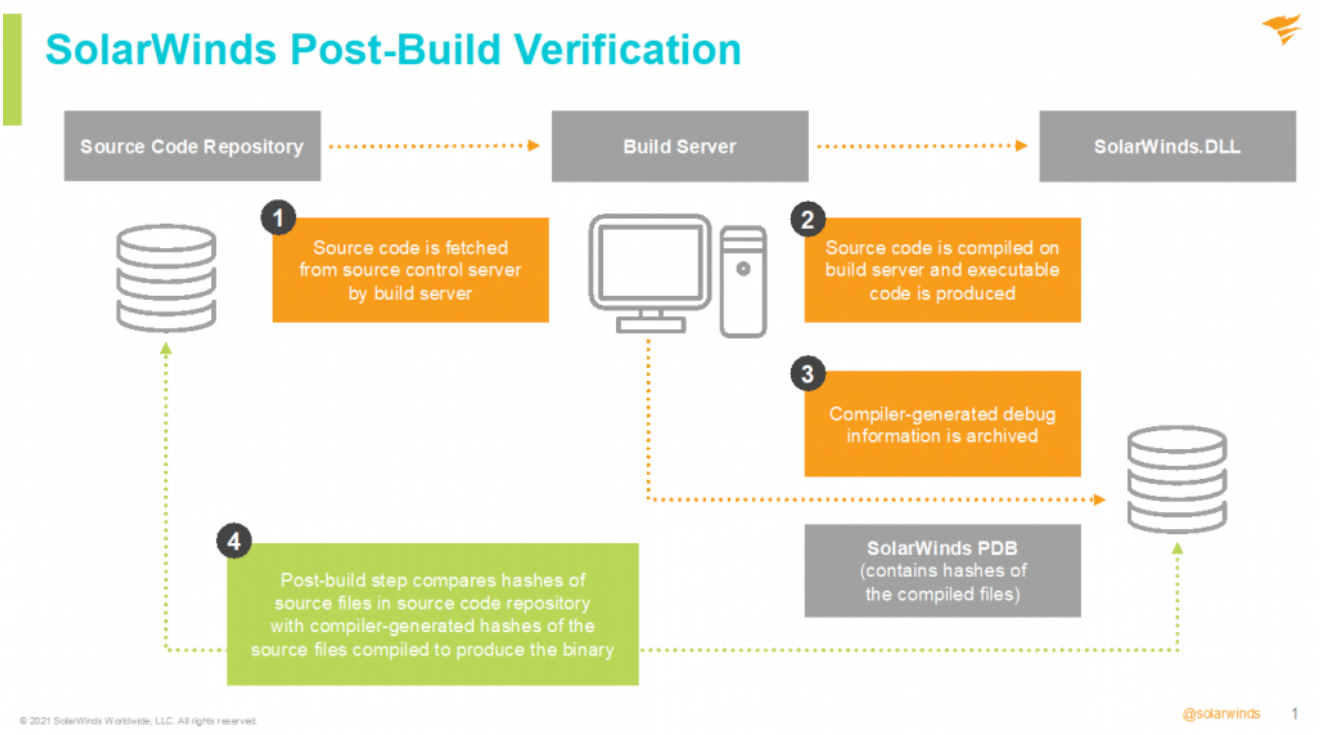

Image: SolarWinds LLC

Tags

- APT29
- Russia
- SEC
- SolarWinds
- supply chain attack
- SVR

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.