Unanswered questions in the SolarWinds Orion hack

Kevin Reed
29 December 2020

On December 14, the IT infrastructure company SolarWinds confirmed that hackers had embedded malware into software updates for its flagship Orion platform and the malicious code had been pushed out to as many as 18,000 of its customers.

The hastily issued announcement from the Austin, Texas-based company said, "This attack was a very sophisticated supply chain attack, which refers to a disruption in a standard process resulting in a compromised result with a goal of being able to attack subsequent users of the software."

SolarWinds Orion is used widely by US government agencies and Fortune 500 corporations, as well as small to medium-sized companies, to perform basic information system and networking duties such as user accounts administration and performance monitoring, reporting and alerting. According to company marketing literature, Orion is sold as a "scalable architecture that reaches across your physical, virtualized, and cloud IT environments."

Once the software update containing the malware—now known as Sunburst or Solorigate—is installed on a host system, it creates a backdoor that reveals itself to the hackers after lying dormant for 12 to 14 days. SolarWinds said the Trojan-horse malicious code had been present in updates that were distributed between March and June of this year.

Reuters reported a day after the SolarWinds announcement that "the hackers have already parlayed their access into consequential breaches at the U.S. Treasury and Department of Commerce." The news agency said that "multiple criminals have offered to sell access to SolarWinds' computers through underground forums, according to two researchers who separately had access to those forums."

The US Cybersecurity Infrastructure Security Agency (CISA) of the Department of Homeland Security responded to news of the hack with an emergency directive that said, "Affected agencies shall immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network. Until such time as CISA directs affected entities to rebuild the Windows operating system and reinstall the SolarWinds software package, agencies are prohibited from (re)joining the Windows host OS to the enterprise domain."

While the information published about the Sunburst malware by SolarWinds and the CISA made reference to "threat actor activity" and that it "may have been conducted by an outside nation state," neither gave a specific national origin or a verified identity of the cyber attacker.

The corporate media sprang immediately into action to claim that Russia was responsible for the breach. On the same day that the SolarWinds acknowledgment was released, for example, the *New York Times* published an article entitled, "Scope of Russian hacking becomes clear: Multiple US Agencies were hit," co-authored by David Sanger.

For its part, the *Washington Post* published an article on December 14, "Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce," that included the following: "The Russian hackers, known by the nicknames APT29 or Cozy Bear, are part of that nation's foreign intelligence service, the SVR, and they breached email systems in some cases, said the people familiar with the intrusions, who spoke on the condition of anonymity because of the sensitivity of the matter."

Over the next several days, representatives of the US political establishment—both Democrats and Republicans—began repeating the assertion that the Russian government was behind the SolarWinds hack, some calling it an "act of war."

On December 16, Democratic Party Senate Minority Whip Dick Durbin of Illinois, told CNN, "This is virtually a declaration of war by Russia on the United States and we should take that seriously." Two days later, Marco Rubio, Republican Senator of Florida, tweeted, "The methods used to carry out the cyberhack are consistent with Russian cyber operations," and he told Fox News the attack was "almost, I would argue, an act of war, absolutely."

On December 19, during an interview with the right-wing talk radio host Mark Levin, Secretary of State Mike Pompeo—departing from the position of President Trump—said, "This was a very significant effort and I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity."

Both the corporate media and members of the US political establishment are making the assertion that Russia was responsible for the breach despite the lack of any evidence to

support their claims.

On the other hand, new details about the hack of the widely used SolarWinds Orion platform raise serious questions about the events of the past three weeks.

According to security experts and former employees, SolarWinds was extremely vulnerable to an intrusion like Sunburst—not only because of the widespread government and corporate use of its software—but for its own slipshod security practices.

The *New York Times* reported, for example: "The company did not have a chief information security officer, and internal emails shared with The New York Times showed that employees' passwords were leaking out on GitHub last year. Reuters earlier reported that a researcher informed the company last year that he had uncovered the password to SolarWinds' update mechanism — the vehicle through which 18,000 of its customers were compromised. The password was 'solarwinds123.' "

Meanwhile, Robert K. Knake, a senior Obama administration cybersecurity official, asked on Twitter, "I'm struggling with what the SolarWinds incident means for defending forward. How is this not a massive intelligence failure, particularly since we were supposedly all over Russian threat actors ahead of the election?" and "The IC [Intelligence Community] kept reporting that the Russians were targeting the election. That didn't happen but was the evidence that they were planted? Did NSA fall into a giant honeypot while the SVR [Russian intelligence agency] quietly pillaged the USG and industry?"

The truth is that the United States runs what is by far the world's most expansive and sophisticated cyberespionage operation. As revealed by former CIA office and National Security Agency (NSA) intelligence contractor Edward Snowden, there is well-documented factual evidence that the US government has engaged in warrantless surveillance of the public on a massive scale—with the PRISM and XKeyscore systems—and infiltrates and gathers intelligence on the computer systems of foreign entities through the Office of Tailored Access Operations of the NSA.

As was revealed by WikiLeaks in 2015, the US government tapped the phone calls of German Chancellor Angela Merkel and her closest advisers for years and spied on the staff of her predecessors Gerhard Schroeder and Helmut Kohl.

Last July, hackers breached security at Twitter and took control of dozens of high-profile accounts, including those of Joseph Biden, Barack Obama, Jeff Bezos and Bill Gates. During the Twitter hack, the intruders gained control of a control panel used by administrators at the micro-blogging social media platform to blacklist and censor content down to the level of specific users and their individual tweets.

Although two teenagers—one from Florida and the other from Massachusetts—were charged with breaching Twitter's security, one of them by pretending to work for the company's IT department, nothing has been said about the exposure of the blacklisting dashboard.

Lastly, the SolarWinds hack announcement was preceded by a report by the private cybersecurity and US intelligence consulting firm FireEye on December 8 that the firm was, "attacked by a highly sophisticated threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack."

CEO Kevin Mandia published a blog post that the hackers had used "a novel combination of techniques not witnessed by us or our partners in the past" to gain access to FireEye's "Red Team assessment tools that we use to test our customers' security." Although Mandia did not report precisely when FireEye's testing software had been compromised, he wrote that "we are proactively releasing methods and means to detect the use of our stolen Red Team tools."

Furthermore, Mandia added, "We have seen no evidence to date that any attacker has used the stolen Red Team tools" and "we have seen no evidence that the attacker exfiltrated data from our primary systems that store customer information from our incident response or consulting engagements, or the metadata collected by our products in our dynamic threat intelligence systems."

The FireEye CEO did not attribute the hack to any particular Advanced Persistent Threat actor or state sponsor, nor did he identify SolarWinds Orion platform as a potential target of the intrusion.

On that same day, the *Washington Post* published an article, based upon the FireEye disclosures, that "Russian spies" had "carried off another brazen hack" of the cybersecurity firm and stolen its Red Team tools. The *Post* report carefully stated, "though the firm did not attribute it to Russia's foreign intelligence service," the Russians were responsible "according to people familiar with the matter."

The next day, on December 9, the *New York Times* published an article about the FireEye hack that stated, "The Silicon Valley company said hackers—almost certainly Russian—made off with tools that could be used to mount new attacks around the world." Neither the *Post* nor the *Times* provided any specific facts or evidence connecting the FireEye hack to Russian intelligence agencies.