The SolarWinds hack

Alston Jaudon

College of Engineering and Computer Science

University of Central Florida

CIS 3360: Security in Computing

Michael McAlpin

June 3, 2024

As technology becomes more advanced, the threat of cyberattacks becomes even more common. Using the Internet, we exchange information at an unbelievable rate when compared to the rest of history. Consequently, that information often ends up in the wrong hands; even worse, the exposure of that information can lead to the destruction of a person's life. Because of this, cybersecurity has never been more important. Even with all the precautions put in place, however, breaches can still occur due to the evolving nature of these cyberattacks. Recently, a company called SolarWinds was plagued by an attack in which hackers used a nearly undetectable strain of malware to get their hands on sensitive data. What followed was a year-long ordeal to discover just how these hackers gained access, as well as performing damage control for all the publicity this incident brought.

SolarWinds is an IT company that sells management tools to businesses looking to monitor their networks and infrastructure. They provide their services to many businesses around the world. Among their services is a commonly distributed tool called Orion, a software suite that acts as a performance monitor. Unfortunately, this would be the tool that the hackers used to gain a foothold on so many customer accounts. They targeted 3rd party software, in this case Orion, instead of SolarWinds directly in what is referred to as a supply chain attack. This works because 3rd party suppliers in the "supply chain" of a business generally have fewer security measures in place. Their malicious code, nicknamed "Sunburst", would then transmit data intermittently back to their own command-and-control server.

What makes this attack stand out from others is the amount of time it took to discover. It is suspected that the hackers gained access to Orion around September of 2019, but they didn't start deploying their malware until March of 2020. It would take until December for analysts at Mandiant, one of the leading firms in cybersecurity, to discover the source of the malware. In fact, the analysts at Mandiant joined the investigation because they too had been hacked. In an article by Wired, they describe the event as a golden SAML attack, where hackers use counterfeit authentication tokens to mimic an employee, thus giving themselves unlimited access to a company's servers. Of course, this was all derivative from the original injection of malware into the Orion software, which Mandiant realized they had been using.

The nature of how these hackers accessed the Orion files was almost unfeasible, and yet they pulled it off. Their process started before an Orion software update was even compiled by

using a backdoor injector tool. Hidden on Orion's build server, this tool would wait for Orion to compile and then quickly rewrite a duplicate file with the malicious Sunburst code in it. The tool then deleted itself, leaving no trace except for the tampered software update ready to be deployed. Because one of the developer's builds failed, they were able to obtain an image of every file contained on the system at that particular time; otherwise, they would've had no knowledge of the rogue injector tool and what it was doing. This posed a huge problem for the integrity of software development. The developers were using a build management service to help turn their source code into software. What they didn't have in that service was a second check to make sure what compiled was a match with their source code. In this paper-thin gap, it seems unnecessary to check for integrity, and yet, it's these opportunities hackers take to go unnoticed for so long. This breach has brought much needed attention to the software development process. Companies are more likely to include code integrity checks as well as segmented build environments where monitoring and anomaly detection tools are used more often.

It's clear that the hackers covered their tracks remarkably well, which points to the fact that this may not have been their first offensive. The main problem is that the identity of the attackers was never truly uncovered, though the evidence points to a certain group. Many analysts believe that this attack was performed by Russian operatives, more specifically their Foreign Intelligence Service (the SVR). Back in 2014, a group from the SVR nicknamed "Cozy Bear" infiltrated the White House's email and then the Democratic National Committee in 2015. It's highly speculated that this is the same group. Their goal for SolarWinds was most likely to conduct as much counterintelligence as they could, and they chose the perfect jumping point to do so; the Orion software had the most connections to customer networks. Their efforts gave them reach into local, state, and even federal agencies such as the Department of Homeland Security and the Department of Justice. At the federal level, we know the hackers were able to collect email, but they most likely got more than that. With the departments that were compromised, locations of US nuclear facilities and weapons, product and infrastructure plans, and non-public documents and employee details would all be up for grabs.

While many of the elements of this attack were still shrouded in mystery, cybersecurity companies were scrambling to reverse the effects of the spreading malware. In typical American

fashion, word of the breach quickly spread causing feelings of anger and fear in the SolarWinds shareholders, associated businesses, and even the general public. The first step was to disconnect from SolarWinds servers until an approved patch could be sent out. Employees at SolarWinds had to check and re-sign most of their products with a new digital certificate since the old one was now invalidated. Analysts noticed that the piece of Sunburst malware attempted to propagate by accessing different IP addresses. However, to remain discrete, it would terminate if attempting to resolve to an unwanted IP address. Knowing this, Microsoft and GoDaddy created a kill switch that always made the malware resolve to an unwanted IP address, effectively stopping it from traveling further. This was a huge success, but it didn't mean the malware was completely gone for good. There was the possibility that Sunburst had created secondary backdoors in the servers it had already visited. Monitoring these new intrusions is now a primary task in our government. President Biden even called for the creation of a Review Board that assesses cyber incidents. There were admittedly some simple mistakes leading to this breach. For example, the Orion servers were never configured with a firewall. These are mistakes that many businesses will learn from to ensure the confidentiality of their data.

We are now living in a world turned digital. It's easy to become the victim of social engineering plots simply because they are new and unexpected, and that's why it's so important for all of us to be educated on safe practices when we interact with technology. Incidents like the SolarWinds hack remind us that no piece of cyberspace is impenetrable. This does not mean that we should stop trying to protect our information, but rather, be more diligent in the areas of vulnerability. One way that businesses can prevent supply chain attacks is by making sure they have very secure connections to their suppliers; any weak link creates an opportunity for a hacker to sneak their malicious code in and create all sorts of problems. Cybersecurity used to be a reactive game where people with destructive intentions always got to make the first move. Now, proactive approaches are redefining the game, giving those who want to keep their information private the upper hand.

References

Saheed Oladimeji, S. M. K. (2023, November 3). *Solarwinds Hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Zetter, K. (2023, May 2). *The untold story of the boldest supply-chain Hack Ever*. Wired. https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/

What is a supply chain attack? - crowdstrike. crowdstrike.com. (2024, April 2). https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/