SolarWinds: The CSO Perspective

Q&A WITH GAVIN REID, RECORDED FUTURE CSO

Information is still coming to light surrounding the SolarWinds breach, and we've received many questions from clients on the topic. Gavin Reid, CSO at Recorded Future, shares his thoughts on the evolving situation and actions he's taken.

The SolarWinds breach situation came to light because of FireEye's breach. How could a cybersecurity company like FireEye have been affected without noticing it?

Well the fact is, they DID notice it. There is a timing issue between breach and discovery, often referred to as "time to dwell." This attack persisted for way longer than anyone other than attackers would like. In this case, the attackers spread laterally using standard authentication methods and looked like normal authenticated users. We often spend a lot of time looking for compromised endpoints that try and escalate privileges and work their way up the stack, attempting to compromise something like an active directory server. This attack, once established, reversed that and started with complete authorized access – fewer organizations are well equipped to alert on authorized access. From Senator Mark Warner, Democrat of Virginia and the ranking member of the Senate Intelligence Committee: *"If FireEye had not come forward, I'm not sure we would be fully aware of it to this day."*

What was the first step you took as a CSO when the SolarWinds breach was announced?

The first step was to do a complete inventory, and by that, I mean an actual real scanning-based verification of what was on our network. I knew we did not formally use SolarWinds Orion internally; however, that does not mean someone could be running it informally in a lab. We are using Rumble.run for internal scanning. It is fast and accurate. I also verified with our Endpoint Detection and Response (EDR) agent to double check. Once I verified we were not running any of the impacted versions. I then searched for TTPs and IOCs to do a much more thorough investigation. To do that, organizations must have consolidated accurate, verified sources to easily access. These data sources allowed us to quickly protect our organization based on all of the available knowledge at the time. The information on this attack was growing hourly, so I also needed to ensure I had decent alerting for new TTPs & IOCs. With this new data, I could keep our investigation and protections as complete and as fresh as possible. Automation of alerting from a wide range of sources and IOC ingestion was a huge help. CISO's with dependable inventory scanning and IOC ingestion automation were much better off responding to this event. When we had a handle on what could loosely be called triage, we started a thorough review of potentially similar third-party risks — in particular, where we had a third party that had embedded infrastructure in our environment. What controls did we need or already have in place, and similarly, what alerting should something out-of-the expected happen? By then, we had some good TTPs from some of the original impacted organizations, FireEye and Microsoft, that gave us some very specific areas to look at and check for the affected services. We also applied the same methodology for any similar services we use. Of course, during all of this we were working with our clients to give them the same assistance.

It has been said that there was a multi-factor authentication (MFA) bypass involved. Can you discuss what that means? Should organizations not rely on MFA anymore?

No, not at all. That would be like saying someone broke into a safe, so therefore, we should never use safes anymore. MFA is one of the most important tools we have in the security arsenal. One area of MFA that should be obsolete though is SMS authorization as it is easily compromised. In this case, it looks like the attackers had direct API credentials to create tokens. If the attackers have administrative access to your back-end identity management or authentication, it is not surprising that they could make tokens to get around MFA. Microsoft released some excellent TTPs on this, and these are useful for alerting on whatever identity service or provider you may use:

- Tokens with configurations that deviate from the identity provider's configured behavior.
- Tokens without corresponding issuing logs at the identity provider.
- Tokens with MFA claims but without corresponding MFA activity logs at the identity provider.
- Tokens from IP addresses, agents, times, or for services that are anomalous for the requesting identity represented in the token.

The last one, in particular, should be part of an alerting program that is supported by advanced IDM functionality where appropriate, especially for any administrative type activity. Another thing: once a foot-hold was established they also started targeting accounts with extended access. Organizations that prepare for that eventuality with things like "red-forests," jump servers, and the like fared much better with this attack.

There has been discussion around the latest release from SolarWinds also containing portions of malicious code. How would you ensure the latest release is clean?

The vendor has released a lot of good information on how to check whether an organization is running the latest, clean version of SolarWinds Orion.

Could there be insider threats as well? How do you protect against that?

In this case, the attackers did not need access from an insider. However, we have seen insiders solicited to help breach organizations, and each attack an organization may face will be different.

Based on the fact that the threat actor had access to SolarWinds source code, do we anticipate they will likely exploit other vulnerabilities they find in the source code? Do you think this software is safe to use going forward?

I think it is a bit of a knee-jerk reaction to remove SolarWinds everywhere. I understand why people are doing it; they are under a lot of pressure to do so. For some of the organizations running SolarWinds, it may have been their only source of network telemetry. Now they have pulled it out and have no network visibility – leading to a worsening security posture. I believe that organizations should pay careful attention to any third-party software with administrative-level access to their infrastructure. Hopefully, this is a wake-up call for everyone: you need to prepare for and expect advanced security attacks.

Microsoft has also confirmed that it experienced a breach stemming from SolarWinds, stating that hackers were able to view source code, but did not have permissions to modify any code or systems. What takeaways or precautions should organizations be taking, given this breach?

Once the hackers had authenticated administrative access, no data was safe. Organizations need to prepare for precisely this sort of eventuality and ensure you have additional security controls, authentication, separation, and amazing visibility into events around high-value targets.

Do you see the SolarWinds breach changing how companies will approach cybersecurity in 2021? If so, how?

Recorded Future, like most other companies, will be paying careful attention to our identity providers and how they manage access. In particular, how do we limit risk if a credential gets compromised and get good notifications if something unexpected happens? We will also be putting any third-party services or software under the microscope and will be a lot more prescriptive on security controls and alerting.