Lessons for Law Firms from the SolarWinds Breach

by Sharon D. Nelson, Esq. and John W. Simek

Perhaps classified as the worst data breach ever, the compromise of the SolarWinds Orion platform has impacted approximately 18,000 public and private sector customers according to Cyber Unified Coordination Group (UCG). The UCG also said that the Russian-backed Advanced Persistent Threat (APT) group is most likely responsible for the SolarWinds hack. As the investigation continues, we are learning more and more details about the attack and those impacted.

SolarWinds

So what is SolarWinds Orion and what is it used for? Essentially, SolarWinds Orion is a network monitoring and management tool. It is used by IT personnel to provide a single dashboard for administering various parts of the network to include the infrastructure and applications.

Discovery

In early December 2020, cybersecurity firm FireEye discovered that its own systems were compromised and attackers made off with FireEye's own tools for investigating breaches. While FireEye was investigating how their systems were pierced, it learned that there was a backdoor, known as Sunburst, within SolarWinds. We now know that the backdoor has existed for months and provided undetected access to thousands of systems.

So what led FireEye to even think they were compromised? Unlike a bomb threat, nobody called FireEye and said "Knock. Knock. I'm in your network." FireEye's CEO Kevin Mandia said the first clue to the massive attack was what is called a Severity-Zero Alert. "In this particular case, the event that got briefed to me and got us to escalate and declare this a full-blown incident was somebody was accessing our network just like we do, but they were doing it with a second registered device." They contacted the employee associated with the account and confirmed that they did not register a second phone. This is certainly a clear indication that the attacker already knew the employee's username and password. As Mandia further stated, "We had somebody bypassing our two-factor authentication by registering a new device and accessing our network just like our employees do, but it actually wasn't our employee." How many of us have systems in place to issue an alert for a second device being registered? Make that lesson one.

Impacted Entities

There are approximately 18,000 SolarWinds customers that have installed the Orion platform. We will discuss some of the impacted entities but not all of them. First, Microsoft was one of the high profile companies to be a victim of the SolarWinds hack. During its investigation, Microsoft discovered "… unusual activity with a small number of internal accounts and upon review, we discovered one account had been used to view source code in a number of source code repositories."

In addition to Microsoft, a joint statement issued by the FBI, CISA, ODNI and the NSA stated that only 10 government agencies were targeted by additional hacking activity. In other words, the cybercriminals used the SolarWinds backdoor as an entry point to the federal agencies. . One of those agencies was the US Department of Justice (DoJ). DoJ reported that around 3% (roughly 3,450 mailboxes) of the

department's Microsoft 365 mailboxes were potentially breached. This type of activity is not unusual when a system is compromised. The attacker will look to harvest additional information in order to compromise additional victims. Presumably, DoJ mailboxes would reveal some very valuable information.

Another impacted legal entity included the U.S. federal court system according to the Administrative Office (AO) of the U.S. Courts. "The AO is working with the Department of Homeland Security on a security audit relating to vulnerabilities in the Judiciary's Case Management/Electronic Case Files system (CM/ECF) that greatly risk compromising highly sensitive non-public documents stored on CM/ECF, particularly sealed filings." As readers know, the court document system supplies the publicly searchable PACER database. However, utilizing the SolarWinds backdoor would allow access to the sealed files, which may contain intellectual property, identities of confidential informants, trade secrets, or other highly sensitive information. The AO has instituted new procedures to protect highly sensitive court documents. It has suspended electronic uploads to CM/ECF and will accept documents in paper form or via a secure electronic device such as a flash drive. In addition, the files will be stored on a secure stand-alone computer system.

Lesson two – heighten security to protect confidential information.

Cloud Not Immune

Even if you use cloud services, you are not immune from attacks via the SolarWinds backdoor. Generally speaking, the cloud affords more protection than most firms can provide themselves. That is unless a human improperly configures cloud services, which is the number one cause of cloud data breaches. The SolarWinds Orion platform can also be used to manage cloud environments. This means that SolarWinds has administrator type access to many of the cloud services. It may also hold root Application Program Interface (API) keys for AWS (Amazon Web Services) or Microsoft Azure. This is particularly concerning as systems typically integrate with the cloud by using a service account, tokens or API.

Supply Chain Exposure

The hack of SolarWinds is termed a supply chain attack. This is not where the ultimate victim is attacked, but where a supplier or provider of services to the ultimate victim is compromised. The program code of SolarWinds Orion was compromised with undetectable backdoor access. As customers began installing updated Orion software, the backdoor came along and allowed access to the "end-user" victim. Without going into a lot of the propeller head technical details, the compromise of SolarWinds was extremely sophisticated with methods never seen before.

The risk of further supply chain attacks is real. Perhaps it is best summarized by Austin Berglas, global head of professional services at BlueVoyant. He said, "As technology advances and the world gets increasingly interconnected, these supply chain attacks will grow and become more effective, highlighting a critical vulnerability in all third-party relationships: the exploitation of trust." Lesson three – attack methods are constantly changing and supply chain attacks are likely to bedevil us for the foreseeable future.

Action Items

With such a sophisticated supply chain attack, how is the typical law firm supposed to protect itself and maintain the confidentiality of its client information? You can never be 100% secure, but there are some things you can do to help minimize your exposure.

If you are one of the 18,000 Orion customers, certainly install the updated version that removes the backdoor code and changes all the credentials for all users and services.

Consider installing endpoint detection and response (EDR) software on your computers for endpoint protection. EDR is a new class of protection and is not the same as anti-virus software. EDR solutions use artificial intelligence and machine learning to detect anomalies and non-normal computer/network activity. Monitoring network activity is also an important function. Consider installing an IDS (Intrusion Detection System) and IPS (Intrusion Prevention System). The Cisco Meraki product line is a very good affordable option for IDS/IPS functionality.

Logs, logs, logs. Have we mentioned logs? Make sure you have logging enabled wherever possible. Also, collect as much data as you can for as long a period as you can. Many compromises occurred months ago, so if you only have 30 days of logs, you will probably never know how you were compromised. Also, store the logs somewhere that is safe from deletion. Today, many attackers are deleting logs and backups after they have entered your network in order to make it harder to trace what happened and to impede recovery

Finally, CISA (Cybersecurity & Infrastructure Security Agency) has a webpage for tracking ongoing APT cyber activity. CISA also issued an alert (AA20-352A) concerning APT attacks with technical details for mitigation. The alert is accessible at https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

If there's a final lesson, it is that you cannot "set it and forget it" when it comes to cybersecurity. As threats evolve, your defenses must also evolve.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com