Findings From Our Ongoing Investigations

orangematter.solarwinds.com/2021/02/03/findings-from-our-ongoing-investigations/

February 3, 2021

SolarWinds was one of a growing number of targets of a highly sophisticated, broad, and coordinated nation-state cyber operation that compromised multiple software and hardware companies. Along with our partners in industry and government, we believe other additional attack vectors unrelated to SolarWinds will continue to come to light over the coming weeks. This nation-state operation was a broad-based attack on the IT infrastructure on which we all rely. According to the Cybersecurity and Infrastructure Security Agency (CISA), other companies were compromised before the impacted versions of the Orion Platform were deployed to customers last year. Given its breadth, CISA's acting director, Brandon Wales, told the *Wall Street Journal* recently that "this campaign should not be thought of as the SolarWinds campaign." We've committed to sharing what we learn from this experience and continuing to fortify our systems as we work closely with our customers to protect their systems. This operation, however, highlights the need for enhanced collaboration within the industry to collectively improve how we prevent, manage, and remediate these kinds of threats and operations in the future. It also underscores the need for deeper public and private partnerships to create a more secure environment for everyone. As SolarWinds continues collaborating with private experts, law enforcement, and government agencies to investigate the attacks, we're exploring several potential theories about how the threat actors were able to enter and access our environment, and what actions the threat actors took once inside. Together with our third-party forensic investigators, we're pursuing numerous theories but currently believe the most likely attack vectors came through a compromise of

credentials and/or access through a third-party application via an at the time zero-day vulnerability. Investigations are still ongoing and given the sophistication of these attacks and the actions taken by the threat actors to manipulate our environment and remove evidence of their activities, combined with the large volumes of log and other data to analyze, our investigations will be ongoing for at least several more weeks, and possibly months. As we previously shared, FireEye contacted us December 12, 2020 regarding malicious code that was identified in the SolarWinds Orion Platform. Additionally, Microsoft notified us December 13, 2020 about a compromise related to our Office 365 environment. We've analyzed data from multiple systems and logs, including from our Office 365 and Azure tenants, along with logs from SolarWinds Security Event Manager, and our build environment platforms. As previously reported, this analysis has determined threat actors gained unauthorized access to our environment and conducted reconnaissance prior to the trial conducted on our Orion Platform software build in October 2019. We have not yet determined the exact date that the threat actors first gained unauthorized access to our environments. While we've confirmed suspicious activity related to our Office 365 environment, our investigation has not identified a specific vulnerability in Office 365 that would have allowed the threat actor to enter our environment through Office 365. We've confirmed that a SolarWinds email account was compromised and used to programmatically access accounts of targeted SolarWinds personnel in business and technical roles. By compromising credentials of SolarWinds employees, the threat actors were able to gain access to and exploit our Orion development environment. Research community investigations have highlighted these nation-state operators displayed determination, patience, extremely high operational security (OpSec), and advanced tactics, techniques, and procedures (TTPs). As part of our commitment to ensuring the industry has a more complete understanding of the increasingly sophisticated and organized threats, we're sharing these examples that come from the cybersecurity research community and our investigations:

- Variation and/or disabling of audit logs, timestamps, and other security measures;
- Manipulation of software builds through reusable automated processes and deployment of novel, sophisticated malware to effect exploitation and malicious goals;
- Modification through laundering of legitimate code from malicious code injection (SUNSPOT) and monitoring of disk space and activities before executing or creating files;
- Deletion of files and programs following use to avoid forensic discovery and masquerading of file names and activity to mimic legitimate applications and files;
- Variation of file names and other indicators across victims and within environments and active reconnaissance of victim environments and users for indicia of detection; and
- Automated dormancy periods of two weeks or more prior to activation, utilization of servers outside the monitoring authority of U.S. intelligence.

We are committed to sharing information openly in order to help the industry guard against similar attacks in the future and create safer environments for customers. For instance, given that software development and build processes are generally quite common throughout the industry, we promptly shared information about the novel malicious code injector

(SUNSPOT) we found so that other companies could check their software build environments and make any updates necessary to protect themselves. We published these details about the build manipulation activity in our January 11 blog post. Our partner CrowdStrike also published additional details related to this activity in a blog post published the same day. We continue to put a priority on our investigations to ensure we fully understand all elements of this sophisticated attack and can share our learnings with our customers and the broader community. We firmly believe the best way for the industry to prepare for and prevent attacks of these types in the future is to communicate openly and work together. ********** *This Blog Post contains "forward-looking" statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, as well as statements regarding SolarWinds' investigation into the recent SUBURST attack, the high-level timeline provided above and the company's findings to date, SolarWinds' understanding of the nature, source and duration of the attack and SolarWinds' plans to further investigate the attack, ensure our products and internal systems are secure and provide information regarding its findings. The information in this Blog Post is based on management's beliefs and assumptions and on information currently available to management, which may change as SolarWinds continues to address the vulnerability in its products, investigate the SUNBURST attack and related matters and as new or different information is discovered about these matters or generally. Forward-looking statements include all statements that are not historical facts and may be identified by terms such as "aim," "anticipate," "believe," "can," "could," "seek," "should," "feel," "expect," "will," "would," "plan," "intend," "estimate," "continue," "may," or similar expressions and the negatives of those terms. Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by the forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, (a) the discovery of new or different information regarding the SUNBURST attack and related security incidents or of additional vulnerabilities within, or attacks on, SolarWinds' products, services and systems, (b) the possibility that SolarWinds' mitigation and remediation efforts with respect to the SUNBURST attack and related security incidents may not be successful, (c) the possibility that customer, personnel or other data was exfiltrated as a result of the SUNBURST attack and related security incidents, (d) numerous financial, legal, reputational and other risks to SolarWinds related to the SUNBURST attack and related security incidents, including risks that the incidents may result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or vendor relationships and investor confidence, U.S. or foreign regulatory investigations and enforcement actions, litigation, indemnity obligations, damages for contractual breach, penalties for violation of applicable laws or regulations, significant costs for remediation and the incurrence of other liabilities, (e) risks that SolarWinds' insurance coverage, including coverage relating to certain security and privacy damages and claim expenses, may not be available or sufficient to compensate for all liabilities SolarWinds incurs related to these*

matters, (f) the possibility that SolarWinds' steps to secure its internal environment, improve its product development environment and ensure the security and integrity of the software that it delivers to customers may not be successful or sufficient to protect against threat actors or cyberattacks and (g) such other risks and uncertainties described more fully in documents filed with or furnished to the U.S. Securities and Exchange Commission by SolarWinds, including the risk factors discussed in SolarWinds' Annual Report on Form 10-K for the period ended December 31, 2019 filed on February 24, 2020, its Quarterly Report on Form 10-Q for the quarter ended March 31, 2020 filed on May 8, 2020, its Quarterly Report on Form 10-Q for the quarter ended June 30, 2020 filed on August 10, 2020 and its Quarterly Report on Form 10-Q for the quarter ended September 30, 2020 filed on November 5, 2020. All information provided in this Blog Post is as of the date hereof and SolarWinds undertakes no duty to update this information except as required by law.

Sudhakar Ramakrishna

Sudhakar Ramakrishna joined SolarWinds as President and Chief Executive Officer in January 2021. He is a global technology leader with nearly 25 years of experience…

Read more