**Written Testimony of Sudhakar Ramakrishna**

**Chief Executive Office, SolarWinds Inc.**

**United States Senate Select Committee on Intelligence**

**February 23, 2021**

## Introduction

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for inviting SolarWinds to assist in your efforts surrounding the unprecedented nation state attack on SolarWinds, its users and the technology industry more broadly. We appreciate the opportunity to share our findings, lessons learned and our recommendations to promote the public-private information sharing, collaboration and support that we believe are necessary to protect us all against these types of operations in the future.

My name is Sudhakar Ramakrishna, I am the new President & CEO of SolarWinds. I joined SolarWinds on January 4th. Prior to SolarWinds, I was the CEO of Pulse Secure for over 5 years. Pulse Secure is a provider of secure and zero trust access solutions, and previously, I held executive roles at Citrix, Polycom, and Motorola, amongst others.

SolarWinds is a provider of IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the ability to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid deployments. We are a Texas-based company with over 3,000 employees in 17 countries around the world.

## SolarWinds' Commitment to Cooperation and Transparency

We sincerely appreciate your interest and assistance in helping us to address the many challenges that we and our users face because of this unprecedented nation state attack. While we understand that these challenges are much larger than SolarWinds, we recognize that we need to learn from this and share those lessons toward a greater solution. We are grateful for the opportunity to do so in font of this Committee and for the very valuable assistance we continue to receive from the FBI, CISA, and the Intelligence Community.

It is our goal to provide the Committee with information on our investigation, and critically, how we are applying what we've learned to incorporate systematic and systemic improvements to our environment and Software Development Life Cycle (SDLC) processes.

Our number one priority has been, and continues to be, to ensure that our users are safe and protected. To this end, our teams worked tirelessly to provide remediations to the affected product and accomplished that within 3 days of learning of the attack. We have also been very active in our user outreach and have dedicated significant resources to help users and partners across the public and private sectors.

We look forward to helping the Committee understand the attack and its implications, lessons we have learned as we have confronted it, and recommendations to help you and the Intelligence Community further protect U.S. cybersecurity.

## Nation State Level Program

At this stage in our investigation, while we cannot definitively attribute the attack to any particular nation state, our external investigation partners CrowdStrike, KPMG and others confirm that the tactics, techniques and procedures displayed in this attack mirror that of a nation state.

There are three aspects of the attacker's activities that highlight the sophistication of the campaign: first, the malware, dubbed SUNBURST, they injected into the Orion Product for further deployment in our users' networks. Second, the malware they used in our build process to inject the SUNBURST code into Orion's final software package. And third, their stealthy use of U.S.-based cloud services to innocuously interact with victim networks.

### *Code Inserted into Our Users' Environment - SUNBURST*

By way of background, SUNBURST is a malicious code that was injected by the threat actor(s) into specific versions of our Orion Software Platform which we released between March of 2020 and June of 2020. Based on our investigations, SUNBURST was not present in versions of our Orion Software Platform and related products which we released prior to March 2020, or after June 2020.

It is important to understand what the malicious SUNBURST code was designed to do and what was required for the malicious code to be utilized by the threat actor(s). The malicious code was designed in such a way that when the impacted versions of the Orion Software Platform were installed on a network, the malware tried to open a "back door" into the target network.

The back door only worked if the Orion Software Platform had access to the internet which is not required for the Orion Software Platform to operate. If a back door was indeed opened, the threat actor(s) had to take further steps to gain access to the victim's network, and then had to circumvent firewalls and other security defenses within a target's IT environment.

### *Code Inserted into our Environment - SUNSPOT*

Further, working together with our partners, we have been able to locate the malicious code injection source by reverse engineering the code utilized in the nation state attack. The malicious tool that was deployed into the build environment to inject the SUNBURST backdoor into the Orion Software Platform has been code named SUNSPOT and was designed to be injected without arousing the suspicion of our software development and build teams.

Our investigations have also revealed that the threat actor(s) conducted an extensive intelligence reconnaissance and offensive operation inside of our networks. The reconnaissance element of the operation existed throughout our environment for months. The overall intent of this operation appears to have been to influence updates to our Orion Software Platform through the utilization of SUNSPOT to distribute SUNBURST deliberately and maliciously to Orion users.

The creation of SUNSPOT and its involvement in this operation is an alarming development for the software development community. Because of the extreme potential significance of this malicious tool to the wider IT community, I instructed our investigative team to immediately brief the U.S. law enforcement and Intelligence Community, including CISA and the UK NCSC, and publish information publicly on the details surrounding SUNSPOT and SUNBURST. My reasoning for doing so was to raise awareness swiftly and expeditiously to help the IT community identify similar attacks and to help prevent another company from having SUNSPOT or similar code embedded into their development environment.

*Adversary Abuse of U.S. Cloud Infrastructure*

Our analysis, confirmed in our conversations with U.S. Government partners, also suggests that by managing the campaign through multiple servers based in the United States and mimicking legitimate network traffic, the attackers were able to circumvent threat detection techniques.

**Adversary Campaign Takeaways**

We believe that the entire software industry should be concerned about the nation state attack as the methodologies and approaches that the threat actor(s) used can be replicated to impact software and hardware products from any company, and these are not SolarWinds specific vulnerabilities. To this end, we are sharing our findings with the broader community of vendors, partners, and users so that together, we ensure the safety of our environments.

The breadth of the nation state attack is large, and the level of potential impact is growing. We believe this increases the urgency for a coordinated response by the United States government and the technology industry. We are committed to contributing our lessons and experiences, and believe this response should build on recommendations from the Cyberspace Solarium Commission and the Fiscal Year 2021 National Defense Authorization Act (NDAA):

1. *Improving Industry Government Supply Chain Security Collaboration*
   Building on CISA's Information Communications Technology Supply Chain Risk Management Task Force and consistent with Solarium Enabling Recommendations 4.6.1 (Increase Support to Supply Chain Risk Management Efforts) and NDAA Section 1713 (Establishment of an Integrated Cybersecurity Center), advocate for a public-private initiative to secure enterprise software and services by increasing threat sharing and fostering greater joint collaboration between private firms and governments stakeholders including CISA, FBI, DoD and ODNI.

2. *Improving Federal Government Cybersecurity Standards*
   Building on DOD's Cybersecurity Maturity Model Certification (CMMC) effort for Department of Defense contractors and continued security enhancements to the Federal Information Security Modernization Act (FISMA), support the creation of industry-wide security standards based on continuous risk monitoring and measurement for current and potential government contractors.

3. *Improving Incident Notification to the Government*
   Consistent with Enabling Recommendation 4.7.1 (Pass a National Breach Notification Law), empower organizations with the appropriate incentives and liability protections to share more information on attempted or successful breaches with government cybersecurity authorities. Indicators of compromise associated with those events shared with software vendors in an anonymized way enriches the understanding of prevailing threat actor techniques and target sets, enabling software providers to improve defenses and better protect users.

In summary, certain initial important findings and conclusions based on our experience are as follows:

1. Various third-party experts have concluded that this attack shows that when a sophisticated nation state applies its full arsenal of resources, it is difficult for any enterprise to defend against it.
2. The use of SUNSPOT to compromise software build environments has exposed a significant threat to the global software supply chain at large. It has become increasingly clear that the risk of its use is not isolated to SolarWinds.[1] The threat affects the global software supply chain in general, as evidenced by the recent identification of additional companies that have been subjected to similar attacks.[2] Third-party experts now have confirmed SolarWinds was only one of the many supply chain vectors used by the nation state adversary, and perhaps not the largest one.
3. As testimony from cybersecurity expert Dmitri Alperovitch to the House Homeland Security Committee last week demonstrates, facts now reveal that the description of this issue as the "SolarWinds attack" is a misnomer. CISA's Acting Director Brandon Wales echoed this sentiment in an interview with the Wall Street Journal. Our nation faces a persistent, determined effort by adversarial nation states to attack, compromise, and exploit the software supply chain and labeling as the SolarWinds attack improperly narrows the scope of the threat.
4. We believe for any solution to be effective; prescriptions must apply a "zero trust" presumption, access provided on a least privileged basis, and must take account of the breadth of the problem across the entire U.S. supply chain.
5. Every enterprise can learn from these events and strive to improve their security posture and re-double their efforts towards public-private partnerships.

## Protecting Our Users

Since becoming aware of the nation state attack, we have worked tirelessly to ensure that our products are free of malicious code, protecting our private and public sector users and enabling them to continue to use our products safely.

We promptly disclosed the attack and acted expeditiously to provide our users with information and remediation and mitigation measures, including upgrades to all impacted versions of the Orion Software Platform. We are also applying our lessons learned and implementing sustainable improvement initiatives.

We have formed a "Technology and Cybersecurity" committee of our board. Two current sitting members of our board, who are CIOs with significant cybersecurity experience, and I comprise the three-member committee. This committee has the responsibility to provide advice to management and oversight of our cybersecurity improvement initiatives.

[1] https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601.

[2] https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601.

## Implementing Lessons Learned

We are applying our knowledge to evolve SolarWinds into a company that is "Secure by Design." These efforts are focused on three primary areas[3]:

- Further securing our internal environment;
- Enhancing our product development environment; and
- Ensuring the security and integrity of the products we deliver.

Key steps to further securing our internal environment which we are prioritizing as a central part of our operational fabric as we move forward include:

- Deploying additional, robust threat protection and threat hunting software on all our network endpoints, including a critical focus on our development environments;
- Resetting credentials for all users in the corporate and product development domains, including resetting the credentials for all privileged accounts, and for all accounts used in building the Orion Software Platform and related products; and
- Consolidating remote and cloud access avenues for accessing the SolarWinds network and applications by enforcing multi-factor authentication.

Key steps to enhancing our product development environment include:

- Performing ongoing forensic analysis of our product development environments identifying root causes of the breach and taking remediation steps; and
- Evolving to parallel build systems and environments with stricter access controls and deploying mechanisms to allow for reproducible builds from multiple independent pipelines. This will further improve the integrity of our software beyond code-signing practices which have proven to be inadequate.

Key steps to ensuring the security and integrity of the software that we deliver to users include:

- Adding additional automated and manual checks to ensure that our compiled releases match our source code after the completion of the compile process;
- Re-signing all Orion Software Platform and related products, as well as all other SolarWinds products, with new digital certificates;
- Performing extensive penetration testing of the Orion Software Platform and related products to identify any potential issues which we will resolve with urgency;
- Leveraging third-party tools to expand the security analysis of the source code for the Orion Software Platform and related products;
- Implementing least privilege access controls, network segmentation, and additional MFA and encryption for our development environments; and
- Engaging with and funding ethical hacking from white hat communities to quickly identify, report, and remediate security issues across the entire SolarWinds portfolio.

[3] We have published the elements of these dimension in a blog: https://orangematter.solarwinds.com/2021/01/07/our-plan-for-a-safer-solarwinds-and-customer-community/.

Our collective efforts are guiding our journey to becoming an even safer and more secure company for our users and other stakeholders.

We have also added additional levels of security and review in our software build process and in other areas of our environment– through tools, processes, automation, and, where necessary, manual checks to ensure the integrity and security of all our products.

## Understanding the Impact of the Nation State Level Program

Federal and civilian users use a range of SolarWinds' approximately 100 products. When SolarWinds was notified about the cyber attack, we conservatively estimated the number of potentially impacted users.

Now, with the advantage of ongoing and in-depth investigations into the circumstances of the compromise, we are better positioned to provide more reliable estimates. Only three Orion Software Platform versions released between March and June 2020 were affected. The remediations provided by SolarWinds, together with the "kill switch" discovered and implemented by our colleagues, rendered the SUNBURST code inert in the three affected Orion Software Platform versions.

On December 30, the Cybersecurity and Infrastructure Security Agency (CISA) notified users that the National Security Agency had examined this version and verified that it "eliminates the previously identified malicious code." Beyond the affected versions of Orion, to date, investigators have not found SUNBURST or a similar cyber attack in SolarWinds' many non-Orion products and tools, or in the 16 non-affected Orion Software Platform versions.

## Conclusion

Based on the challenges posed by SUNSPOT and SUNBURST and considering SolarWinds' extensive array of responses and initiatives, we believe that we can contribute meaningfully to a national solution. To that end, we hope the Committee will engage with SolarWinds on an ongoing basis and accept our assistance in any way that may be helpful.

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for your leadership on the important topic of our nation's cybersecurity. We appreciate the opportunity to share our experience with you and some of the lessons we have learned. It is clear to me that we must work together to ensure the safety and stability of the digital ecosystem and I pledge to you SolarWinds' active participation and contributions. I look forward to your questions.