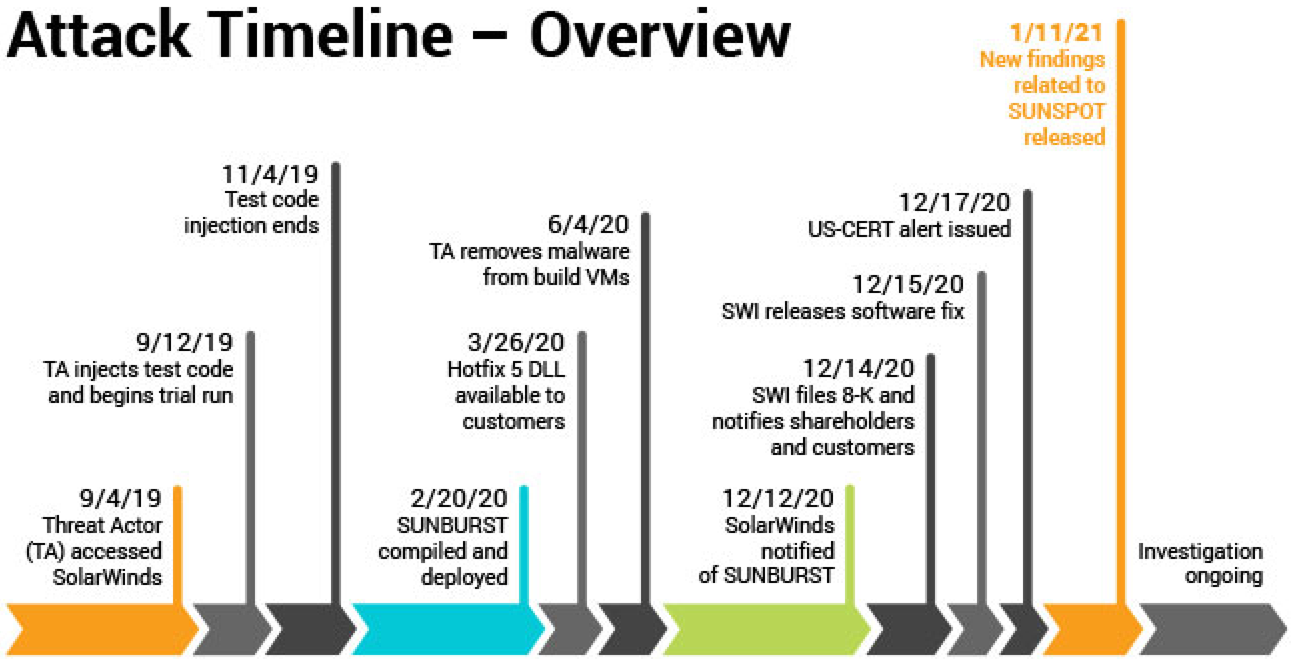
New Findings From Our Investigation of SUNBURST

orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

January 11, 2021

Since the cyberattack on our customers and SolarWinds, we have been working around the clock to support our customers. As we shared in our recent update, we are partnering with multiple industry-leading cybersecurity experts to strengthen our systems, further enhance our product development processes, and adapt the ways that we deliver powerful, affordable, and secure solutions to our customers. We are working with our counsel, DLA Piper, CrowdStrike, KPMG, and other industry experts to perform our root cause analysis of the attack. As part of that analysis, we are examining how the SUNBURST malicious code was inserted into our Orion Platform software and once inserted, how the code operated and remained undetected. Today we are providing an update on the investigation thus far and an important development we believe brings us closer to understanding how this serious attack was carried out. We believe we have found a highly sophisticated and novel malicious code injection source the perpetrators used to insert the SUNBURST malicious code into builds of our Orion Platform software. We recognize the software development and build process used by SolarWinds is common throughout the software industry, so we believe that sharing this information openly will help the industry guard against similar attacks in the future and create safer environments for customers. The security of our customers and our commitment to transparency continue to guide our work in these areas and going forward. **Highly sophisticated and complex malware designed to circumvent threat detection** As we and industry experts have noted previously, the SUNBURST attack appears to be one of the most complex and sophisticated cyberattacks in history. The U.S. government and many private-sector experts have stated the belief that a foreign nation-state conducted this intrusive operation as part of a widespread attack against America’s cyberinfrastructure. To date, our investigations have not independently verified the identity of the perpetrators. Analysis suggests that by managing the intrusion through multiple servers based in the United States and mimicking legitimate network traffic, the attackers were able to circumvent threat detection techniques employed by both SolarWinds, other private companies, and the federal government. The SUNBURST malicious code itself appears to have been designed to provide the perpetrators a way to enter a customer’s IT environment. If exploited, the perpetrators then had to avoid firewalls and other security controls within the customer’s environment. KPMG and CrowdStrike, working together with the SolarWinds team, have been able to locate the malicious code injection source. We have reverse-engineered the code responsible for the attack, enabling us to learn more about the tool that was developed and deployed into the build environment. This highly sophisticated and novel code was designed to inject the SUNBURST malicious code into the SolarWinds Orion Platform without arousing the suspicion of our software development and build teams. We encourage everyone to visit this blog post, authored by the CrowdStrike team, which provides additional details into these findings and other technical aspects of this attack, and contains valuable information intended to help the industry better understand attacks of this nature. As we discussed in our previous post, we hope that this event ushers in a new level of collaboration and information sharing within the technology industry to address and prevent similar attacks in the future. Our concern is that right now similar processes may exist in software development environments at other companies throughout the world. The severity and complexity of this attack has taught us that more effectively combatting similar attacks in the future will require an industry-wide approach as well as public-private partnerships that leverage the skills, insight, knowledge, and resources of all constituents. We want to be a part of that solution, which is why we are sharing this information with the broader community, and we will continue to share progress as we assimilate this information into our go-forward practices. **Our investigations to date** We are actively working with law enforcement, the intelligence community, governments, and industry colleagues in our and their investigations. As we recently disclosed, we even shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed in their research.


Attack Timeline – Overview
9/4/19
Threat Actor (TA) accessed SolarWinds
9/12/19
TA injects test code and begins trial run
11/4/19
Test code injection ends
2/20/20
SUNBURST compiled and deployed
3/26/20
Hotfix 5 DLL available to customers
6/4/20
TA removes malware from build VMs
12/12/20
SolarWinds notified of SUNBURST
12/14/20
SWI files 8-K and notifies shareholders and customers
12/15/20
SWI releases software fix
12/17/20
US-CERT alert issued
1/11/21
New findings related to SUNSPOT released
Investigation ongoing

All events, dates, and times approximate and subject to change; pending completed investigation.

- Our current timeline for this incident begins in September 2019, which is the earliest suspicious activity on our internal systems identified by our forensic teams in the course of their current investigations.
- The subsequent October 2019 version of the Orion Platform release appears to have contained modifications designed to test the perpetrators' ability to insert code into our builds
- An updated version of the malicious code injection source that inserted the SUNBURST malicious code into Orion Platform releases starting on February 20, 2020.
- The perpetrators remained undetected and removed the SUNBURST malicious code from our environment in June 2020. During that time, through to today, SolarWinds investigated various vulnerabilities in its Orion Platform. It remediated or initiated the process of remediating vulnerabilities, a regular process that continues today. However, until December 2020, the company did not identify any vulnerabilities as what we now know as SUNBURST.
- On December 12, 2020, we were informed of the cyberattack and moved swiftly to notify and protect our customers and to investigate the attack in collaboration law enforcement, intelligence and governments.

As part of our ongoing efforts to protect our customers and investigate the SUNBURST attack, we are reviewing historical and current customer inquiries that might contribute to a better understanding of the attack. To date, we have identified two previous customer support incidents during the timeline referenced above that, with the benefit of hindsight, we believe may be related to SUNBURST. We investigated the first in conjunction with our customer and two third-party security companies. At that time, we did not determine the root cause of the suspicious activity or identify the presence of the SUNBURST malicious code within our Orion Platform software. The second incident occurred in November, and similarly, we did not identify the presence of the SUNBURST malicious code. We are still investigating these incidents and are sharing information related to them with law enforcement to support investigation efforts. We will continue our investigations to help ensure our products and internal systems are secure and to provide information that we hope leads to the identification of the perpetrators and the prevention of these types of attacks in the future. We also plan to continue to share our broader findings with the industry at large in the hope that everyone is better able protect themselves and deliver more secure solutions to their customers. ** *This Blog Post contains "forward-looking" statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, including statements regarding SolarWinds' investigation into the recent SUNBURST 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