SUNBURST Threat Analysis

What happened?

SolarWinds, an IT operations software vendor, was compromised and the software backdoored through a complex, intricate, and well-executed supply chain attack that was delivered to customers as early as March 2020. Leveraging the SolarWinds software update process allowed the adversaries to deliver the backdoor, labeled as "Sunburst," to about 18,000 organizations across the globe, sending the world reeling from the potential scale of the sweeping impact this breach will have for years to come.

While the group responsible for this breach has not been definitively attributed at this time, the United States government has stated this systemic attack was Russian in origin. It is our current understanding that two or more well-known Russian threat actors are coordinating this espionage campaign. Many of the known victims include some of the largest and most influential companies and government agencies in the United States, along with countless others across the globe. This begs the question as to how they were able to maintain undetected access to so many high-profile targets for such a substantial period of time.

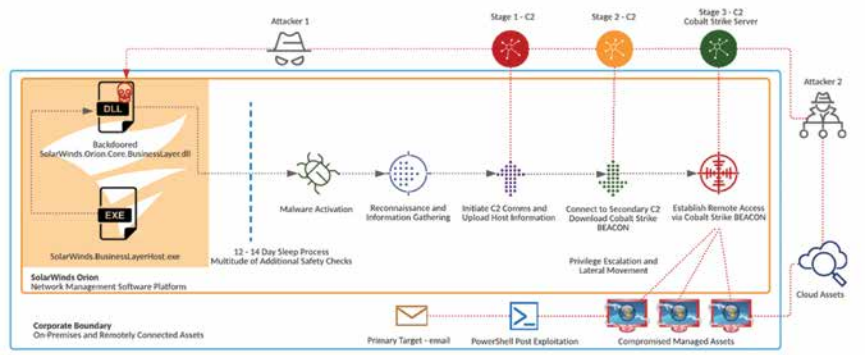

FIGURE 1: SUNBURST malware command and control (C2) process.

What is the impact?

The compromise of SolarWinds itself is uniquely impactful and will have a cascading impact across all industry verticals for months, if not years to come. SolarWinds Orion, the network management software solution that included the backdoor, is uniquely positioned to have access to administrative credentials and is consistently active, making it difficult to differentiate malicious post-exploitation behavior from legitimate and expected activity. This provides for the perfect environment for the adversary to embed themselves within the target organization and begin to conduct espionage operations focused on email and related data collection from cloud-hosted assets. This is compounded by the fact the SUNBURST malware includes a myriad of defense evasion techniques to further ensure the longevity of the operation.

The goal of this adversary is long-term persistence and monitoring, with a specific focus on espionage and data exfiltration. With the ever-expanding scope of this breach, VMware will continue to adapt preventions and detections.

What now?

All relevant watchlists and preventions are continually being updated across the VMware Carbon Black product line as we continue to learn more about the techniques, tactics and procedures involved. Please ensure that you have updated to the latest version of the sensor to ensure the most comprehensive protection and analytics.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2021 VMware, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 768860aq-flyr-sunburst-threat-anlys-uslet 2/21