BakerHostetler

A Risk-Based Approach to the SolarWinds Vulnerability Disclosures

On December 13, 2020, SolarWinds disclosed that an unknown attacker compromised its network and inserted malicious code (referred to as the Sunburst vulnerability) into software updates for the Orion platform. In what will likely become known as one of the most widespread and damaging cyber attacks in history, approximately 18,000 private and government organizations installed the malicious code as part of their usual patching process. But based on current information, the attacker – which was likely a Russian intelligence service – used the vulnerability to infiltrate only a small fraction of the organizations that installed the malicious code. Therefore, most will find no evidence of further compromise.

We recommend the following actions in response to this incident:

- For organizations that installed the malicious code, review the guidance below, eliminate the malicious code from your network, and complete a preliminary review for evidence of further compromise. Take additional action based on your organization's risk profile and the preliminary review results. Document your actions and follow new developments released by SolarWinds, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and other government agencies responding to the incident.
- For all organizations, consider whether additional third-party diligence is necessary to evaluate your service providers' potential exposure to the incident based on your risk profile and the third-party service providers you work with.

The SolarWinds Orion platform is a suite of products for monitoring and managing information technology infrastructure. For most organizations that use Orion, it is a foundation of their infrastructure with tentacles into systems across the network. Generally, servers running the platform are also connected to the Internet. This all makes Orion a perfect target for a supply-chain attack: an attacker that compromises the SolarWinds tool can use it to access a target's network and move to other systems with relatively little friction.

SolarWinds disclosed on December 13, 2020, that an attacker – widely believed to be the Russian SVR, a successor agency to the KGB responsible for spying outside Russia – compromised its network and inserted malicious code into the legitimate Orion code such that when organizations installed the compromised Orion updates, they also unwittingly installed the attacker's malicious code into their Orion servers. The security industry now refers to this malicious code as the Sunburst vulnerability, which opens a backdoor (unauthorized connection point) to compromised Orion servers. Upon install, which is the attack's first phase, the malicious code waits two weeks before attempting an outbound connection to the attacker's command-and-control (C2) server. The two-week delay evades security reviewers that may be looking for these unexpected connections. The initial connection merely notifies the attacker that a new victim is available for further compromise in the attack's second phase. In the second phase, the attacker sends instructions for the compromised server to communicate with additional C2 servers and pursue the attacker's other objectives (all of which are still not clear).

Following the Sunburst disclosure, SolarWinds released information about a second Orion vulnerability referred to as Supernova. Unlike Sunburst, the Supernova vulnerability is not introduced through the supply chain; instead, an attacker installs malware on an Orion server after it gains unauthorized access to the server through other means. Supernova is designed to appear to be a part of the Orion software.

We learn more about the attack's scope each day but based on current information we believe the attacker moved to the attack's second phase in only a relatively small number of organizations, for several reasons. First, the second phase is a manual process that consumes the attacker's time and resources and requires careful action to remain covert. Although well resourced, not even the SVR can manually exploit 18,000 organizations while maintaining the operational security necessary to avoid detection. Second, many organizations are unlikely to have information of interest to the Russian intelligence services. High-risk targets are U.S. government agencies, government and defense contractors, critical infrastructure organizations (including energy, financial, and healthcare), and private companies that are technology and security service providers to other companies (allowing the attacker to further exploit the supply chain). The attacker would waste its resources and unnecessarily increase detection risk by exploiting other targets. Third, information released by public and private intelligence services indicates the attacker may have compromised approximately 250 organizations in the attack's second phase. This all suggests organizations should take a risk-based approach to their response, guided by public information about the attack, each organization's own risk profile as a potential target of the Russian intelligence services, and results of the organization's preliminary review for evidence of compromise.

1. Get the background. In addition to the security advisory and FAQs on SolarWind's site, read CISA's alerts and continuing guidance on its Supply Chain Compromise page, including:
   - » CISA Activity Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector OrganizationsAlert AA20-352A – https://us-cert.cisa.gov/ncas/alerts/aa20-352a
   - » CISA Supplemental Guidance on Emergency Directive 21-01
   - » CISA updates Supplemental guidance on Emergency Directive 20-01 – note that as of December 30, 2020, the National Security Agency has now examined version 2020.2.1HF2 and verified that it eliminates the previously identified malicious code
2. Determine if you installed the versions of the Orion software identified as compromised, and patch or update accordingly. These are identified on the SolarWinds website along with a chart indicating the appropriate patching or updating path for particular versions of its software (https://www.solarwinds.com/securityadvisory). The site also provides a list of affected SolarWinds products. Consider rebuilding compromised systems.
3. Preserve evidence to support your forensic investigation. Before rebuilding or updating compromised Orion servers, obtain forensic images of these servers (and the servers' memory, if possible) to support a forensic investigation. Also consider preserving other security information and logging that may soon be overwritten. Merely identifying and updating compromised Orion software versions may not be sufficient remediation – most organizations that installed a malicious version should complete an initial review for signs of further compromise. As a starting point, use published indicators of compromise (IOCs) associated with the attack to identify potential evidence of further compromise. See, e.g., https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. The need for additional forensic review will depend on the results of that review and your organization's risk profile. Discuss an appropriate, risk-based response and investigation plan with your information security team and incident-response legal counsel.
4. Unfortunately, given the attacker's sophistication, the attacker may have already altered or obfuscated publicly disclosed IOCs or the attacker may have installed other malicious tools. Proactive threat hunting, monitoring, and additional logging may be appropriate for certain organizations, depending on the organization's risk profile. Again, discuss an appropriate, risk-based response and investigation plan with your information security team and incident-response legal counsel.
5. Document your actions as part of your organization's incident response process and risk management processes.

1. Prioritize review of third-party service providers that may use SolarWinds based on risk – if they have access to your systems or data, consider how such access might be used to impact your security or to expose sensitive data (e.g., customer or employee information) – and find out whether they installed the compromised Orion software. If so, find out whether they (a) disabled the software or applied the hot fix, (b) investigated whether the threat actor used the vulnerability to access the compromised systems, and (c) can tell you whether your systems or data were compromised as a result.
2. Document your actions as part of your organization's vendor management process.

This event reminds us that supply-chain attacks are some of the most difficult to prevent or detect. Organizations can minimize risk of supply-chain attacks through fundamental information security hygiene. Technical controls such as strong, zero-trust access control and aggressive monitoring can help mitigate scope and detect incidents when a supply-chain attack happens. And administrative controls such as third-party service provider diligence, security-conscious contracting requirements, and limiting third-party access to only that which is necessary can further limit damage.

Contacts

Theodore J. Kobus III
Chair
Digital Assets and Data Management Group
T +1.212.271.1504
tkobus@bakerlaw.com

Craig A. Hoffman
T +1.513.929.3491
cahoffman@bakerlaw.com

Andreas T. Kaltsounis
T +1.206.566.7080
akaltsounis@bakerlaw.com

Adam I. Cohen
T +1.212.589.4629
aicohen@bakerlaw.com

Toll Free 24-Hour
Data Breach Hotline
+1.855.217.5204

BTI CYBERSECURITY POWERHOUSE 2020
Leading Cybersecurity & Data Privacy Law Firm

RANKED IN Chambers GLOBAL 2020
Baker & Hostetler LLP
10 BakerHostetler attorneys were ranked in the 2020 edition of ***Chambers Global.***
4 firm rankings were earned in the USA in the areas of International Trade and Privacy and Data Security in the 2020 edition of ***Chambers Global.***

TOP RANKED Chambers USA 2020
Baker & Hostetler LLP
"Noted for its strength in litigation and defending regulatory investigations, and sought after for its wide-ranging compliance advice."
– ***Chambers USA*** 2020

ALM INTELLIGENCE PACESETTER
CYBERSECURITY **2020 – 2021**

bakerlaw.com

Recognized as one of the top firms for client service, BakerHostetler is a leading law firm that helps clients around the world address their most complex and critical business and regulatory issues. With six core practice groups – Business, Digital Assets and Data Management, Intellectual Property, Labor and Employment, Litigation, and Tax – the firm has nearly 1,000 lawyers located coast to coast. For more information, visit bakerlaw.com.

05.01.21.14.41_p03