The Urgent Need to Assess and Respond to Russian Supply Chain Attacks

December 22, 2020

Authors
Michael Vatis, Stewart A. Baker, Alan Cohn, Charles-Albert Helleputte, Paul R. Hurst, Jason M. Weinstein

Overview
According to media reports, Russian government hackers have penetrated the systems of thousands of companies across a variety of industries, as well numerous US government agencies. Moreover, what has been publicly reported may be only the tip of the iceberg in terms of both the scope of the attacks' victims and the attackers' methodologies. The most recent reporting also suggests that victim companies are not just those that would be of obvious interest to Russian intelligence services. Accordingly, all companies should assess whether they have been affected by this attack, what steps they need to take to remediate those effects, and what legal and contractual obligations they may have to notify government agencies, business partners, customers, and individuals.

Background
Hackers alleged to be working for the SVR, the Foreign Intelligence Service of the Russian Federation, have reportedly gained access to the networks of thousands of companies and federal government agencies, including the Departments of Commerce, Defense, Homeland Security, and Treasury.

The Russian hackers, also known as "Cozy Bear" and "Advanced Persistent Threat (APT) 29," were able to gain access to the networks of various organizations and agencies by breaking into SolarWinds, a technology company that has a large number of private companies and US government agencies as customers. The hackers then sent poisoned software updates to SolarWinds customers that used the company's Orion platform. Additionally, Microsoft has notified more than 40 of its customers that were victims of the same attack and that Microsoft said were "targeted more precisely and compromised through additional and sophisticated measures." In order to bypass cybersecurity systems undetected, the hackers used a counterfeit "token" to deceive service providers about the identity of the systems with which they were communicating.

Entities that reportedly used the compromised software include the US military; the Commerce, Defense, Energy, Justice, State, and Treasury Departments; the White House; NASA; the Federal Energy Regulatory Commission; the Centers for Disease Control and Prevention; the National Security Agency; leading telecommunications companies; utility companies; and technology companies. Entities that were affected by the compromise appear to be concentrated in the United States but also are located around the world, including in Canada, Mexico, Belgium, Spain, Britain, Israel and the United Arab Emirates.
The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) believes that the hacking began at least in March (with possible dry run attacks as early as October 2019) and is currently ongoing, as “removing this threat is highly complex and challenging for organizations.” At present, the extent of access and the information stolen is uncertain, and it is not clear what other actions the hackers have taken inside the networks they compromised. Moreover, CISA, Microsoft, and others have warned that the SolarWinds attack vector is likely just one of many that the hackers used to penetrate victim networks and to achieve system administrator access once inside. For the foreseeable future, there is likely to be a steady stream of revelations concerning additional victims of the attacks, additional software vulnerabilities exploited by the attackers, additional techniques used in carrying out the attacks, and even additional attackers.

**Questions**

The scope of the revelations thus far suggests that no company should consider itself to be immune from the effects of these attacks. Accordingly, companies should be undertaking at least the following actions now:

1. **All US companies** should be using the growing body of adversary signatures associated with the attack to examine their own systems to determine whether those systems have been compromised, assess the impact of any compromise, and take damage-control measures, including system remediation. Depending on what information has been breached, companies should determine whether they are required by law, regulation, or contract to notify individuals, regulators, or other businesses. The fact that the hackers appear to be interested primarily in nation-state intelligence gathering rather than the wholesale exploitation of personal information may mean that some state breach notification laws may not have been triggered. But a company cannot know that for sure without engaging in the necessary investigation and analysis to determine what information was accessed or acquired. In addition, contracts may require notification of a customer or business partner in circumstances that would not trigger a state breach notification requirement.

2. **US government contractors** should be determining whether their systems have been compromised, assessing whether any classified information or controlled unclassified information (e.g., sensitive, export-controlled, or proprietary data) that was developed or received in support of a government contract has been affected, accessed, or exfiltrated, and making any necessary disclosures to the US government agencies with which they maintain contracts. The threshold for disclosure by contractors generally is considerably lower than for breach notification of consumers, and the interest of the US government in this attacker’s victims is considerably higher, so it may be prudent to err on the side of disclosure in this channel. For defense contractors, this would include “rapidly reporting” within 72 hours of discovery of a cyber incident pursuant to the DFARS clause 252.204-7012.

3. **European companies** should similarly examine their own systems to determine whether they have been compromised, evaluate the impact of such a compromise, and implement damage-control measures, including system remediation. They should also assess notification and communication requirements under the General Data Protection Regulation (GDPR) and other EU cybersecurity incident frameworks they are subject to, such as the directive on the security of network and information system (NIS).

Steptoe’s Privacy and Cybersecurity lawyers have deep experience from both inside and outside government in responding to breaches, including national security breaches of this sort. We are well equipped to assist companies in performing the necessary investigations and impact assessments and analyzing any legal and contractual risks and obligations.

**Practices**

**Privacy & Cybersecurity**

**Government Contracts**