The SolarWinds Attack — What Should a Business Do?

December 21, 2020

As if 2020 has not been bad enough, the world is now reacting to an unprecedented data security breach. Your company should convene its cybersecurity incident response team to survey the landscape, and determine whether you have been compromised.

While your IT professionals are hard at work searching for vulnerabilities and harm, executives and legal counsel must be prepared to assess risk and determine potential liabilities. You may need to notify regulators, customers, suppliers, insurers and data subjects. Even if you are not affected by the SolarWinds attack, you should take this opportunity to take stock of your cybersecurity protections.

What Happened? Hackers compromised a network management platform called Orion, made by SolarWinds. SolarWinds customers include more than 425 of the Fortune 500, the top 10 U.S. telecoms and government entities such as the Departments of the Treasury, Energy and Los Alamos National Laboratory. Of SolarWinds' 300,000 customers, 33,000 use the Orion suite, and 18,000 downloaded the malware used in the attack.

So What? In addition to jeopardizing national security interests, the attack puts the data and operations of countless enterprises at risk. The hackers, presumed to be members of the Russian SVR state espionage agency, have had access to victims' networks and data for at least nine months. They have planted malware that can monitor communications, extract data, shutdown or reboot systems, and otherwise disrupt business operations. The Cybersecurity & Infrastructure Security Agency (CISA) states the hack poses "a grave risk" to governments, critical infrastructure entities and the private sector.

How Did This Happen? This attack was made via the software supply chain, from malware called "SUNBURST" hidden in two normal SolarWinds Orion updates, each accompanied by a valid, signed Symantec certificate. The malicious updates occurred between March 2020 (version 2019.4 HF5) and June 2020 (version 2020.2.1 HF1). After a couple of weeks, the malware began to execute files and wreak havoc, which went undetected until security vendor FireEye disclosed the compromise of its system more than a week ago. The origin of the hackers' access to SolarWinds' software development build system is presently unknown.

What Should Businesses Do?

Block the Threat. Fortunately, the primary method of transmitting the malware appears to have been abated. Microsoft, FireEye and GoDaddy have turned the primary domain used in the SolarWinds backdoor (avsvmcloud[.]com) into a kill switch for the malware, so that it terminates itself and prevents further execution.

Keep Up to Date. Check the security advisories from SolarWinds, The SANS Institute and others. https://www.solarwinds.com/securityadvisory/faq and https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ CISA continues to update its Alert on the National Cyber Awareness System. https://us-cert.cisa.gov/ncas/alerts/aa20-352a

Revise your Security & Communication Plans. Assume the bad actors are observing your response, and adapt accordingly. CISA advises that you establish out-of-band communications guidance for staff and leadership; outline what "normal business" may be conducted on the suspect network; set out a call tree for critical contacts and decision making; and evaluate how you plan to communicate to stakeholders and media.

Investigate. This is a sophisticated attack, not easily found or remedied. Knowing whether you received the malware is critical, but only a starting point. Continued threat hunting and monitoring is vital. Outside forensics may be necessary. According to FireEye, the malware stops executing if it discovers it is being analyzed. It relies heavily on valid tokens for accounts, so you must focus on activity outside a user's normal duties. It is unlikely the hackers are still relying on the Orion privileges, so your indicators of compromise (IOCs) may now be entirely different. In some unfortunate cases, you may need to rebuild your entire network.

Check your Response Process. To determine the appropriate response to SolarWinds or any other compromise, company leadership, operations and IT need to be on the same page. Even if you use a network management system other than Orion, your Incident Response Team should use this opportunity to tabletop this incident, and consider how you would react. Assess the coverage, exclusions, retention amounts and deductibles of any cyberliability insurance. General Counsel and outside cybersecurity counsel play an integral part in determining next steps and protecting the integrity of decisions made.

Think Ahead. Going forward, governments and businesses are even more likely to integrate cybersecurity standards into all contracts, especially vendor contracts. Companies need to understand what those standards require, how to negotiate them and what happens if those measures are not met.

For help with your cybersecurity concerns or for more information, contact Tedrick Housh, Michael Cohen, one of the other attorneys on our Global Privacy, Cybersecurity & Data Protection team or your Lathrop

GPM attorney.