BURR FORMAN LLP

What's a Company Do?

Articles / Publications
12.14.2020

Ransomware attacks have increased over the last several months, but the nation-state attacks identified over the last several days are causing people to take a harder look at their systems and what they can do to protect themselves.

Most businesses are aware of the possibility of a cyber-attack, and many even spend significant time and resources planning out how to respond to such attacks. Over the last several months, the increase in ransomware attacks and the increase in the size of the ransoms have heightened sensitivity to the issue across a variety of business markets. However, the nation-state attacks identified over the last several days are causing a lot of people to take a hard look at their systems and wonder what, if anything, they can do to protect themselves.

Yesterday, various sources throughout several government agencies confirmed that there had been successful hacks of their computer systems; the agencies impacted included the Treasury Department and the Department of Commerce. With the FBI and Department of Homeland Security continuing to investigate, it is possible -- and perhaps even likely -- that other targeted departments will be identified.

The Discovery of these attacks comes just days after FireEye, a large cybersecurity firm, announced it was the victim of a sophisticated attack believed to have been launched by hackers working in the direction of a foreign government. The hackers stole the hacking tools that FireEye uses to provide security assessments. Because FireEye's customer list includes many governmental entities as well as many global corporations, there is much speculation as to the scope of this attack.

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

What's a Company Do?

Investigations have revealed that both the FireEye attack and the government attacks were the result of malware, injected into the networks during a legitimate software update earlier this year. The legitimate software is Orion developed by SolarWinds, a software company based in Texas. According to SolarWinds' website, "Orion Platform is a comprehensive bandwidth performance management and fault management application that allows you to view the real-time statistics of your network directly from your web browser. " It is used by many businesses to monitor system performance and identify network problems.

SolarWinds acknowledged in a December 14th report to the SEC that the vulnerability was "inserted within the Orion products and existed in updates released between March and June 2020. . . . ". SolarWinds' CEO Kevin Thompson said, "We believe that this vulnerability is the result of a highly-sophisticated, targeted and manual supply chain attack by a nation-state."

In the same SEC report, SolarWinds reported that the malicious code was not present in SolarWinds' repository of the Orion source code. While there is speculation, there is not yet any confirmation of how the malware got into the software updates. SolarWinds has developed a fix for the vulnerability and made the new version available for download. It also expects to release a second fix on December 15, 2020.

For the system to be compromised, the vulnerability has to be present in the version of Orion installed on the system, and the vulnerability has to be activated. Because the vulnerability must be present and activated, not all Orion users are impacted. SolarWinds' SEC reports state that it "believes the actual number of [Orion] customers that may have had an installation of the Orion products that contained this vulnerability" is less than 18,000. SolarWinds has already notified approximately 33,000 of its customers who were active maintenance customers during the relevant time period of the issue.

If you use Orion in your business, the advice from the US Cybersecurity and Infrastructure Security Agency is to disconnect from the Orion system, review your network for signs of compromise, and assume further malware has been deployed to your systems. Should you discover any issues, Burr's cybersecurity team is available to help you assess your legal rights and obligations arising from the presence of the vulnerability, the activation of the vulnerability, or a data breach arising from the compromise of your systems. You may contact India Vincent or the Burr & Forman LLP attorney with whom you normally work for further assistance.