7 minute read

Bad News Concerning SolarWinds Supply Chain Attack Will Continue to Unfold for Quite Some Time More

CYBERWATCH FINLAND

On Sunday, December 13, news broke out about the largest cyber operation of recent years against the U.S. government targets by an advanced persistent threat actor, APT29, associated with Foreign Intelligence Service of Russian Federation, also known as SVR (Служба внешней разведки Российской Федерации).[1] The original reporting shared details regarding the email systems of The U.S. Treasury Department and Commercial Department having been compromised, but as there has been more information coming out regarding the incident, the devastating size of the hack is slowly becoming revealed.

According to the sources, Russian operatives had successfully penetrated SolarWinds, an Austin, TX -based company offering their clients, among other products, also a widely used IT full stack management platform called Orion.[2] SolarWinds' customer base, which may also include users of other products than their Orion platform, included according to SolarWinds' website, more than 425 of the U.S. Fortune 500 companies, all U.S. telecommunications companies, all branches of the U.S. military, National Security Agency, and The Pentagon, to name a few.[3]

Once in, the Russian hackers proceeded to compromise a build server to have SolarWinds serve their customers a poisoned update of the Orion platform, including Russian injected malware. The distributed malware was later named SUNBURST by one of the compromised entities, FireEye.[4] The poisoned SolarWinds Orion platform update, which opened a backdoor to the target systems for access, and possibly also for insertion of additional tools for ensuring the foothold and continued access, was downloaded by the SolarWinds' customers more than 18,000 times.[5]

Nevertheless, it seems that the perpetrators were highly selective with their targeting.[6] This selective targeting sets the SolarWinds case apart from the NotPetya case associated with the GRU Sandworm team, where a destructive supply chain attack spread worldwide like a wildfire causing more than an estimated $10 billion in damages.[7] In addition to the government targets, one of the targets was an internationally well-known cybersecurity company, FireEye, which lost to the hackers tools they had been using in their penetration testing, or red teaming, activities.[8] This brazen targeting eventually led to the unfolding of the SolarWinds case, as FireEye investigators also detected other organizations had been targeted utilizing the same intrusion vector.[9]

According to some estimates, Russian operatives had initially penetrated the SolarWinds systems already back in October 2019 and made a test run with their chosen method of poisoning an update, but did not yet operationalize their access.[10] The operationalization took place according to the current understanding in March 2020, which has given Russian operatives possibly more than nine months of access to the targeted systems.[11]

To remedy the situation, Microsoft, itself a victim of SolarWinds hack, together with other industry partners, took over or sinkholed the domain used in command and control of the infected systems.[12] Such sinkholing was a continuation of similar operations conducted by Microsoft, where they had been crippling the perpetrators' operations by disrupting their command and control networks.[13]

In addition to the U.S. based companies, U.S. states, and governmental targets, such Departments of State and Homeland Security and National Nuclear Security Administration, according to Microsoft's analysis, targets residing across the globe, spanning from Canada to the United Kingdom and Belgium, have also been infected by SolarWinds poisoned update.[14] Similarly, organizations such as NATO have been investigating if they have been infected.[15]

It is not far-fetched to assume that similar investigations are taking place across the world. Governments and private organizations alike are scrambling to identify, if the SolarWinds hack has impacted them, and if there have been any malicious activities in their systems because of the hack.

As the hacks had a grave national security significance, also the United States Government scrambled into action. According to the reports, the National Security Council was summoned for a meeting on Saturday, December 12, to cover the hack.[16] Cybersecurity and Infrastructure Security Agency (CISA) issued a rare emergency directive on December 14, ordering the government organizations to disable the affected SolarWinds tool in their networks.

Following CISA directive, National Security Council announced on December 15 the establishment of Cyber Unified Coordination Group (UCG) to coordinate the whole-of-government response to the incident.[17] The USG announcement was followed by the joint statement by Federal Bureau of Investigations (FBI), CISA, and the Office of the Director of National Intelligence (ODNI) regarding their work on investigating the breach.[18] Throughout the process, both NSA and CISA have issued advisories and alerts to share technical information with the community fighting the breaches.[19]

There has also been information released about a second entity[20], which has been in the SolarWinds' systems, but if the situation is similar to the DNC case back in 2016 when GRU and SVR were in the same systems, or something else like two competing nations both having access to SolarWinds systems, it is too early to say for sure. Moreover, linked with SolarWinds investigation, authorities have warned that the perpetrators have also been using other means than just SolarWinds associated malware to access their targets, such flaws in VMWare and bypassing of multi-factor authentication.[21]

In addition to attribution conducted by commercial companies, Russian involvement in the SolarWinds hack has also been confirmed by the political figures in the U.S. For example, Secretary of State Mike Pompeo suggested Russia as the perpetrator in the SolarWinds case.[22] Similar statements have been made by senators Marco Rubio (R.) and Mitt Romney (R.) and by a number of politicians from the other side of the aisle.[23] According to the news sources, Biden transition team members have been pondering potential avenues for responding to the system penetrations, including new financial sanctions and potentially going even further.[24]

The current White House has not publicly made Kremlin accountable for the systems penetrations but has instead muddled the waters by suggesting that other players, such as China, may have been in play.[25]

At the time of the writing, the main goal for the SolarWinds hack, and the broad access it granted for the Russian intelligence, appears to have been to secure a foothold in selected systems for intelligence collection. While infuriating, and to some degree also embarrassing, the intelligence collection is a normal and, in many ways, also a necessary part of international affairs.

Nevertheless, at the same time, it is good to keep in mind that a foothold secured for intelligence collection could also be transformed into a platform for destructive operations. Intents may change as time passes, also changing the risk calculus of the victim. Thus, careful target analysis and the nature of targeted systems may reveal a lot of information about the perpetrators' intents. According to some, there have also been signs of critical infrastructure companies being affected by SolarWinds, but not necessarily been penetrated after the original infection. [26]

As more information is being revealed about the SolarWinds hack, there is a growing discussion in the expert community on potential impacts and additional motivations behind the hack. Other than intelligence collection, the listed motivations have included Russia building a deterrent against the U.S. cyber-attacks against targets in Russia, or Russian interests elsewhere. Moreover, it has been speculated that a foothold in the U.S. systems would have served as a bargaining chip, should the elections meddling prevention related activities by the U.S. authorities against Russian actors have become too painful to bear.

While some public outrage and follow-up actions are necessary for the optics and political purposes, it is improbable that outside of limited response such as sanctions, there will be any significant *public* retribution against Russia or their interests, in cyber or in other domains. Most of the response related actions will be concentrated on learning more about the Russian intents, their available resources for human operated missions, target prioritization processes, and their overall tradecraft. Furthermore, the focus is also put on the global breadth of the hack, what information got stolen during the time Russian operatives had access to the systems, trying to rid the systems from any remaining unauthorized parties, and learning how to defend better against similar attacks in future.

While the former U.S. government officials are trying to grasp the SolarWinds case's full ramifications, Kremlin has denied having anything to do with the hacks.[27] Nevertheless, on December 20, Putin congratulated his security services for the work well-done on a national day of celebration for the members of the country's security services while standing in front of SVR headquarters.[28] Meanwhile, the market reaction to the SolarWinds case was swift and painful. SolarWinds' stock is at the time of the writing trading around $16 price per share, one third less than just one month ago.

Sources:
[1] https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG
[2] https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html, https://www.solarwinds.com/orion-platform
[3] https://web.archive.org/web/20201214065921/, https://www.solarwinds.com/company/customers
[4] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[5] https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/
[6] https://arstechnica.com/information-technology/2020/12/only-an-elite-few-solarwinds-hack-victims-received-follow-on-attacks/
[7] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[8] https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[9] https://www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack
[10] https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
[11] https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/
[12] https://www.zdnet.com/article/microsoft-was-also-breached-in-recent-solarwinds-supply-chain-hack-report/, https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/
[13] See for example: https://www.darkreading.com/attacks-breaches/microsoft-sinkholes-6-fancy-bear-apt28-internet-domains/d/d-id/1332628
[14] https://www.bloomberg.com/news/articles/2020-12-17/u-s-states-were-also-hacked-in-suspected-russian-attack, https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855, https://www.npr.org/2020/12/18/947914979/microsoft-says-40-customers-hit-by-ongoing-hack-of-government-agencies
[15] https://www.bloomberg.com/news/articles/2020-12-14/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack
[16] https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG
[17] https://twitter.com/WHNSC/status/1338863139278913537
[18] https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure
[19] See for example: https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/, https://us-cert.cisa.gov/ncas/alerts/aa20-352a
[20] https://www.reuters.com/article/us-usa-cyber-solarwinds/second-hacking-team-was-targeting-solarwinds-at-time-of-big-breach-idINKBN28T0U1, https://www.zdnet.com/article/a-second-hacking-group-has-targeted-solarwinds-systems/
[21] https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/
[22] https://www.npr.org/2020/12/19/948318197/pompeo-russia-pretty-clearly-behind-massive-solarwinds-cyberattack
[23] https://www.forbes.com/sites/andrewsolender/2020/12/17/trump-takes-bipartisan-criticism-for-silence-on-massive-cyber-attack/
[24] https://www.reuters.com/article/usa-cyber-breach-biden/bidens-options-for-russian-hacking-punishment-sanctions-cyber-retaliation-idUSKBN28U0DV, https://www.reuters.com/article/usa-cyber-breach-idUSKBN28U0IK
[25] https://www.bloomberg.com/news/articles/2020-12-19/trump-downplays-massive-hack-floats-china-as-possible-culprit?srnd=cybersecurity
[26] For some related discussion, see for example: https://www.linkedin.com/feed/update/urn:li:activity:6745762156412776448/
[27] https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html, https://www.themoscowtimes.com/2020/12/21/russia-denies-role-in-us-cyber-attacks-a72426
[28] http://en.kremlin.ru/events/president/news