RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

MODUS OPERANDI OF THE LARGEST RUSSIAN CYBER-INTELLIGENCE OPERATION OF RECENT TIMES – ATTACK ON SOLARWINDS

GIORGI UZARASHVILI

161

EXPERT OPINION

RONDELI FOUNDATION

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

EXPERT OPINION

GIORGI UZARASHVILI

MODUS OPERANDI OF THE LARGEST RUSSIAN CYBER-INTELLIGENCE OPERATION OF RECENT TIMES – ATTACK ON SOLARWINDS

161

2021

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov

ISSN 1512-4835
ISBN

Introduction

The 2020 attack on SolarWinds is one of the largest cyber-intelligence campaigns in US history which inflicted significant damage on agencies such as the US Department of Defense (DoD), the Department of Homeland Security (DHS) and the Cybersecurity & Infrastructure Security Agency (CISA).[1] Incidentally, SolarWinds is a US-registered company that provides a wide range of IT-related services to the private and public sectors, including tools used for the remote management of the network's infrastructure.[2] Later, in April of this year, the attack was officially attributed to the Russian Foreign Intelligence Service (СВР - Служба Внешней Разведки). Its consequences were severe not only due to the fact that the attacker, with high probability, gained access to at least part of the information held by the above-mentioned US agencies, but also primarily for the demonstrative effect of this operation. In particular, the attacker demonstrated that no one is protected against Russian cyber-intelligence actors, including the agencies directly in charge of ensuring the information security of the national critical infrastructure throughout the country.

Consequently, the attack on SolarWinds negatively affected the US not only in terms of security, more specifically cyber security, but it also poses a significant challenge to its reputation. Namely, this incident questions whether or not US security forces have highly qualified personnel and appropriate technical equipment to protect significant information assets and prevent similar attacks. Moreover, there is a threat that this precedent will encourage similar actions by other hostile actors against the US in the future, primarily China and Iran.

As a result, the attack on SolarWinds should precipitate the beginning of a substantial upgrade process in the US cybersecurity system as the risk of recurring compromises is quite high if business processes in this sector are left unchanged.

With all of the above in mind, the Biden administration is most likely not going to limit itself to just sanctions, unlike the Trump administration that followed this route from 2016 when various sanctions (and only sanctions) were imposed on Russia's military intelligence service in late 2016. Thus, much tougher retaliatory measures from the current US high political leadership are expected,[3] also given the fact that the sanctions policy alone has hitherto not proven to be a deterrent against the Kremlin. Therefore, it is likely that this attack will go beyond the "ordinary security incident" and acquire the character of growing political tension.

This attack is also relevant for Georgia as our country is in the "operational coverage area" of SolarWinds and this geographical zone is serviced by the Kyiv office of the organization.[4] Thus, it is quite possible that some private or public institutions in Georgia are using a number of SolarWinds services. Otherwise, in the absence of a business contact, it is less likely that SolarWinds would have declared Georgia as an area of its commercial operation.

Even if we assume that legal entities or individuals in Georgia did not use the compromised service of SolarWinds, we can say with certain confidence that a significant part of them use other private commercial toolkits for the remote control of network infrastructure provided from different vendors. Therefore, it is quite possible to infiltrate their protected infrastructure with a method similar to that used against SolarWinds.

Overall, the findings of this Paper are relevant to any organization in Georgia that utilizes remote IT tools (both commercially contracted or in-house developed) for internal network or other infrastructure management.

Description of the Attack - Technical and Operational Details

In December 2020, the US-based private cybersecurity company, FireEye, detected an infection with Trojan malware embedded in a service provided by SolarWinds, a company registered in the same country. A malign Russian actor was the primary suspect in this case from the outset.[5] Later, in April 2021, the Foreign Intelligence Service of the Russian Federation was officially charged for the perpetration of this attack in April 2021. The main functionality of the attack was to embed malicious code in one of the services (products) of SolarWinds and the activation thereof in the target organizations. This compromised service of SolarWinds has been used by beneficiary organizations (approximately 18,000 public and private entities worldwide) for the remote management of network infrastructure.

There are five phases of the operational lifeline of the above-mentioned attack. These five phases were identified based on the results of a detailed study of published reports or other materials about this cyber offensive operation as well as a partial analysis of the infected .dll file conducted in a virtual environment (malware analytical tool – DnSpy launched through Virtual Box installed in the operational system of Windows 10x64).

Phase I

Initially, the attacker managed to penetrate the protected infrastructure of SolarWinds. As a result, a malign actor covertly infiltrated the communication process among programmers developing the SolarWinds Orion software update. It should be noted that following the common practice among professionals working on a particular software service, they divide the functions and separate the modules to be developed independently at a later time merging their developed codes with the software products of their fellow programmers mainly at the last stage of the development process.[6] The Russian Foreign Intelligence Service, namely, its cyber-intelligence group (APT 29), had intercepted this very process. Accordingly, a Russian cyber intel actor was also working in parallel on various malware code fragments that had to be built into the software update package along with the legitimate modules.

Access to the SolarWinds infrastructure was instrumental in realizing the attack, since the access to the internal infrastructure thereby allowed APT 29 to ensure the compatibility of its malicious code with other legitimate sections of the infected software update. As a result, the probability of APT 29's detection was minimized.

This stage is the most problematic part of our research as there is no credible information in the open sources about the method of penetration in the internal network infrastructure of SolarWinds on the part of the attacking actor. There are only versions that are not currently corroborated by any proper digital evidence whatsoever.

With this in mind, two primary versions emerge. According to the first, the company's internal network was compromised by an insider. The major circumstance supporting this narrative is related to the fact that

SolarWinds has offices in Eastern Europe where Russian special services have significant influence and enough operational resources to infiltrate various organizations.[7]

According to the second version speculated by the former CEO of the Company, a Russian cyber-intelligence actor penetrated SolarWinds by brute force using an intern’s simple password. [8] However, this version is problematic because its author did not present any factual evidence to substantiate his position, on the one hand, and if this version is validated, it will mainly confirm the systemic failure of the company’s information security management, on the other hand, as an intern should not have such high privileges to allow an attacker to access the most sensitive part of the inner informational assets if in case his/her credentials will be compromised.

Phase II

During this phase, the attacker intercepted a specific service of SolarWinds (Orion Platform) during the update process. As a result, malicious code was embedded in legitimate modules in such a way that it went unnoticed by the programmers working directly on the update package. One part of the malicious code which the attacker embedded in the legitimate code belonged to the StellarParticle group (unofficially called SUNPOST) which in turn was used to embed the backdoor in the software update package of SolarWinds Orion for gaining unauthorized access to the internal infrastructure of the beneficiaries of the platform.[9] Various cybersecurity companies refer to this by the code name SUNBURST.[10] The unnoticed cover-up of the malicious code was a cornerstone of the operational security for the attacking actor, since the whole operation would fail if it were detected at the beginning and the method of the attack would be easily exposed by the information security staff of the victim organization.[11]

Phase III

This phase of the SolarWinds attack involved the initial penetration in the target organization immediately after running the infected software update package by a specific beneficiary. The primary functionality of the malicious code built into this product, the so-called backdoor, was collecting information about the organization's internal infrastructure and sending it in a text format to the attacker. APT 29 launched an attack tailored to the internal specifics of the target organization based on the information it received which mainly contained data on the network infrastructure configuration of the infected organization. Consequently, the tactics and the methodology of further infection were different. The obtained data gave the malign actor an accurate picture about the so-called black holes of information security which was later exploited in order to establish additional access channels, alternative backdoors, with the infected organization. This approach of the Russian Foreign Intelligence Agency is of great importance in terms of the consistency and continuity of the attack. In particular, APT 29 sought to disguise the primary access channel as much as possible as a large-scale illegal extraction of information from the target organization posed a high risk of exposing intelligence activities. Accordingly, the intelligence actor rightly analyzed that if the primary access channel were to be uncovered, the attacker would be barred from the further exploitation of the malicious code embedded in the SolarWinds product itself.

Phase IV

In the fourth phase of the attack, APT 29 launched the most active and large-scale phase of the intelligence operation, involving the selection and extraction of operationally interesting data from the target organization. To this end, the attacker used a modified version of the famous Adversary Simulations and Red Team Operations Software - Cobalt Strike. As already mentioned above, Cobalt Strike belongs to the type of cyber exercise toolkit that has a number of complex and effective offensive functionalities required for large-scale and multi-stage penetration testing.[12] At the same time, the intelligence actor changed part of the functions of Cobalt Strike in accordance with its operational priorities in order to bypass the network and the internal information security configuration framework of the target organization.[13]

Phase V

In the final stages of the attack, the attacker began a so-called lateral movement within the organization with the main goal of gaining access to as many resources as possible within the victim organization while taking into account that running the SolarWinds Orion infected software update package in the system of victim organizations did not automatically provide additional access to the complete ICT infrastructure in most cases. This was mainly due to the internal network configuration and the strict separation of individual segments. Accordingly, one of the main tasks of the malign actor was to expand the area of attack as much as possible with the aim of also infecting the segment of information infrastructure that was not directly connected to the external network due to security requirements. In addition, one of the major priority directions of the lateral movement process was the installation of so-called Rootkit-type malware in the infected systems through which the attacker could maintain access to the target organizations even in the case of a complex upgrade of the compromised systems.

Attack Attribution

As already mentioned, the POTUS issued a statement on April 15, 2021 according to which the cyber-intelligence group of the Russian Federation Foreign Intelligence Service - the same APT 29 - was officially accused of perpetrating the attack on SolarWinds.[14] Following the announcement, the US special services released a joint assessment and recommendation document outlining the methods and techniques of infecting beneficiaries of the same software through the exploitation of the SolarWinds Orion Platform by the Foreign Intelligence Service as well as on the individual malware modules used in the process.[15]

Despite the publication of these types of data and technical advisories, there is still no public document based on respective evidence that would corroborate why the attack is particularly attributed to the Foreign Intelligence Service and not, for example, military intelligence which is better known in Western countries for its malicious cyber activities. Therefore, this paper will present some arguments and additional factual data aimed at further substantiating the implication of the Foreign Intelligence Service in the attack against SolarWinds.

To this end, the paper will identify the operational priorities and the goals of the Russian Special Services in the kinetic world in parallel to analyzing Russian APT actor’s tools and *modus operandi* in cyberspace. Otherwise, it would not be enough to accuse any specific intelligence service based on technical specifications only, given that in recent years a number of intelligence services (such as the Russian APT 29 TURLA Group) have been actively infecting other intelligence actors and exploiting their infrastructure so as to redirect traces towards an intermediary country in the case of an operational failure.[16]

Thus, the fact that this operation was of a purely intelligence type and did not possess the character of cyber sabotage or other active measures should be taken into account. This factor greatly reduces the possibility of the Russian GRU (Главное Разведывательное Управление) carrying out this operation as the analysis of the attacks organized by the Russian Military Intelligence shows that a specific cyber-intelligence operation is part of its so-called active measures and is intended for a short period in GRU’s case. In particular, once the GRU obtains the information it needs and it is the right time for the Kremlin to release this information, the Russian Military Intelligence usually publishes this type of data as a part of its “active measures” and, as a result, practically destroys its own intelligence platform.[17] Contrary to the GRU modus operandi as discussed above, the Operation was organized in a way to safely extract important information from the target institutions as long as possible and hence the continuity of this process was one of the primary goal during the whole operation.

In addition, it is also unlikely that the Russian Federal Security Service (Федеральная Служба Безопасности - ФСБ) is behind the operation, even though the FSB›s cyber-operations are largely oriented on intelligence gathering even despite the fact that the cyber intel group with the same classification as **APT 29 (TURLA Group)** is in direct contact with the FSB whose main operational focus is to conduct intelligence activities in cyberspace.[18]

However, with high probability the FSB would not have been able to carry out this operation due to the specificity of its targets and the different areas of operational coverage. In particular, the main geographical area for FSB operations is the continent of Europe and especially the countries of the former Soviet Union or the Soviet bloc and organizations, institutions or individuals located in these territories taking into account that the Kremlin considers these geographical areas as an extension of the Russian Federation, the so-called "Near Abroad" (ближнее зарубежье)[19] and tries to extend the FSB operational mandate thereto. This is also confirmed by the fact that the FSB has a significant military presence[20] on the territories occupied or annexed by Russia under the pretext of protecting its so-called borders and which gives it a sizable advantage over other special services of the Russian Federation.

Conclusion

The attack on SolarWinds is the largest and most damaging cyber-intelligence operation in US history hitherto known among the wider public. The operation was carried out in several phases with the key stage being the interception of the SolarWinds Orion Platform update package and embedding of malicious functional modules in its source code in such a way that it was overlooked by both SolarWinds programmers and information security managers. The attacker also evaded detection by the cybersecurity staff of SolarWinds beneficiaries who downloaded and launched the infected update package into their own systems. Such organizations were US national security agencies, including those structural units (such as the DHS CISA) primarily responsible for protecting critical US information systems.

Consequently, it is clear that the damage done by the attack on SolarWinds, along with the security dimension, has significant reputational losses. In particular, the Russian side tried to demonstrate that no one is "immune" to the offensive capability of the Kremlin's special services and, therefore, Russia can respond asymmetrically, including in cyberspace, in response to sanctions or other types of restrictive measures.

It is clear that the top political leadership of the US is also aware of these consequences which, in parallel with attributing the attack to the Russian Foreign Intelligence Service on April 15 of this year, also imposed sanctions on public and private institutions affiliated with the SVRAt the same time, it is expected that Washington's response will not be limited to sanctions alone as these instruments were proven to be ineffective when imposed on Russian military intelligence in 2016 for sufficiently deterring and preventing the Kremlin from conducting harmful activities in the cyber sphere. Consequently, senior US political officials repeatedly and directly hinted about responding with "painful measures" which most likely do not imply the sanctions policy alone. Accordingly, it is expected that the attack on SolarWinds as discussed in this paper will have a continuation in the near future and it may become a source of additional tension between the US and Russia.

References:

1. *Forbes*, “DHS, DOJ And DOD are All Customers of SolarWinds Orion - The Source of the Huge US Government Hack,” Accessible at: https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=65540ef925e6, last seen: 13/06/2021

2. SolarWinds: *We Make IT Look Easy,* Accessible at: https://www.solarwinds.com/company/home, last seen 13/06/2021

3. *New York Times*, “Preparing for Retaliation Against Russia, US Confronts Hacking by China,” Accessible at: https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html, last seen: 14/06/2021

4. SolarWinds, *SolarWinds Reseller Locator*; Accessible at: https://partner.solarwinds.com/reseller/find/, last seen: 14/06/2021

5. Office of Director of National Intelligence, *Joint State of US FBI, DHS CISA, DNI and NSA*, Accessible at: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2021/item/2176-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-the-office-of-the-director-of-national-intelligence-odni-and-the-national-security-agency-nsa, last seen: 14/06/2021

6. Microsoft, *Deep Dive into the Solorigate Second-stage Activation: From SUNBURST to TEARDROP and Raindrop*, Accessible at: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/, last seen: 15/06/2021

7. Endgadget, “SolarWinds Hack May Have Been Much Wider than First Thought”, Accessible at: https://www.engadget.com/russia-solarwinds-hack-broader-than-expected-211046098.html, last seen: 15/06/2021

8. CNN, “Former SolarWinds CEO Blames Intern for ‘solarwinds123’ Password Leak,” Accessible at: https://edition.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html, last seen: 15/06/2021

9. FireEye Threat Research, *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*, Accessible at: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html, last seen: 15/06/2021

10. *Ibid.,*

11. CrowdStrike, *SUNSPOT: An Implant in the Build Process;* Accessible at: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/, last seen: 15/06/2021

12. Cobalt Strike, *Cobalt Strike Features,* Accessible at: https://www.cobaltstrike.com/features, last seen: 15/06/2021

13. ZEDNET, “Microsoft: This is How the Sneaky SolarWinds Hackers Hid Their Onward Attacks for So Long,” Accessible at: https://www.zdnet.com/article/microsoft-this-is-how-the-sneaky-solarwinds-hackers-hid-their-onward-attacks-for-so-long/, last seen: 15/06/2021

14. US White House, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government,* Accessible at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/, last seen:15/06/2021

15. US FBI, DHS and DHS CISA, *Cybersecurity Advisory: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders*, Accessible at: https://us-cert.cisa.gov/ncas/alerts/aa21-116a, last seen: 15/06/2021

16. UK NCSC, *Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims*, Accessible at: https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims, last seen: 15/06/2021

17. One of the best demonstrations of this case is the publication of a set of emails discrediting Hillary Clinton during the US presidential election. Although the RF Military Intelligence Division could have maintained and developed covert access to the compromised accounts, it practically willingly uncovered the intelligence operation by utilizing the data obtained during the active measure. The situation was identical during the French presidential election when Russian military intelligence tried to aid an ultra-right-wing radical candidate, Marine Le Pen, by publishing various items of confidential information (general factual information about the attack is available at the following link: https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200).

18. Estonian Foreign Intelligence Service, *2018 Report,* pp. 57-60; Accessible at: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf, last seen: 15/06/2021

19. Atlantic Council, *Lubyanka Federation: How the FSB Determines the Politics and Economics of Russia,* Accessible at: https://www.atlanticcouncil.org/in-depth-research-reports/report/lubyanka-federation/, last seen: 16/06/2021

20. *EU Observer*, “10 Years on: Russia’s Occupation of Georgian Territory,” Accessible at: https://euobserver.com/opinion/142547, last seen: 16/06/2021; Nikolai Mitrokhin, *Infiltration, Instruction, Invasion: Russia’s War in the Donbass*, pp. 227-228, Accessible at: https://spps-jspps.autorenbetreuung.de/files/07-mitrokhin.pdf, last seen: 16/06/2021