CYBERSECURITY BULLETIN

ISSUE 6

December 2020

WELCOME

Welcome to the sixth edition of GDS Cybersecurity bulletin.

The year 2020 has become exceptional in many ways, especially when it comes to the rise of cyber-attacks due to the Covid-19 pandemic. The latter provided an opportunity for attackers to hack IT infrastructures, taking advantage of the massive migration to remote work and the security gaps between the home and office networks. The cyber breach recorded during the final weeks of this challenging year that affected FireEye and SolarWinds shows a growing trend for sophisticated threats resulting into severe implications for the targeted entities.

So, what are the lessons learned? And what are the immediate actions following this targeted breach?

CONTENTS

SUMMARY

“This was a sniper round from somebody a mile away”, the words chosen by FireEye’s CEO to describe the SolarWinds hack. In a serious shift in cyber-attacks to a more complicated state driven threat, it has never been more important to start looking at security from a different perspective.

A closer look at the latest breaches and ways to mitigate them will be described in the next few pages.

"THE" DATA BREACH, SHOULD WE BE WORRIED?

In less than a week, two cyber security incidents were enough to prove that it is impossible to ensure total protection from hackers, if there were still doubts about that.

The first occurrence targeted FireEye and was revealed on the 8th of December 2020 in a blog post by FireEye's CEO, Kevin Mandia. The second occurrence was announced on the 13th of December 2020. The target this time was a software developed by SolarWinds.

FireEye is one of the top security firms with customers ranging from governments to major enterprises all over the world. By Mandia's own analysis, the attack was conducted by "a nation with top-tier offensive capabilities" with the attackers being "highly trained in operational security and executed with discipline and focus". "They used a novel combination of techniques not witnessed by us or our partners in the past" continues Mandia. The Washington Post reported that the attackers were the hacking arm of the Russian foreign intelligence service, the SVR, known as APT29 or Cozy Bear. The declared results of the attack were the stealing of FireEye's Red Team tools.

Figure-1: Kevin Mandia, CEO of the cybersecurity firm FireEye, testifies before the Senate Intelligence Committee in 2017. Mandia's company was the first to sound the alarm about the massive hack of government agencies and private companies on Dec.8.

SolarWinds' incident relied on a supply chain attack instead of attempting to have a go directly at the targets. SolarWinds lists all five US military branches as their customers as well as many governmental US organization such as the Pentagon, NASA and the Office of the US President. The incident was serious enough to elicit an emergency directive from CISA on the 13th of December ordering all federal agencies that use SolarWinds Orion (the source of the compromise) to "immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network". The Washington Post pointed fingers to APT29. FireEye, who are investigating the issue, have initially indirectly tied this to the hack that previously targeted them by saying that they "share certain common elements" while stopping short of confirming everyone's suspicions. It was later confirmed that SolarWinds' attack is what led to FireEye being compromised.

What do these complicated and far-reaching hacks mean closer to home?

- First, the Red Team tools stolen from FireEye will probably not constitute a major threat for well-prepared organizations. FireEye have been extremely transparent in their disclosure. They have published IOCs and methods to detect the use of their Red Team tools. In addition, if APT29 are skilled enough to execute such large-scale compromises of US federal agencies and one of the top security firms, this simply means that they do not really need those tools.

- Second, FireEye also stated that those tools do not include any zero-day exploits. This is a good thing. The immediate implication is that a properly functioning security defense (SIEM,

the player using these tools. Faced with hackers with the same level of focus and operational security knowledge as those who compromised FireEye would make the task of detecting a breach difficult. It is not about the tools, it is about how to use them.

- Third, there is always a way. Not in a positive sense. Some extremely high-value targets were eventually breached: the Natanz nuclear facilities in Iran, the US DNC, the Saudi Tasnee, the Ukrainian power grid (2015), the US power grid (2017), etc. The value of a target might not automatically translate into a well-protected target. However, when nation-sponsored groups are involved, with high discipline and resources to spare, a way-in is almost always found. No accumulation of tools, measures and procedures can prevent that. However, as seen in FireEye's case, a good security preparedness can lead to a quick detection of an intrusion followed by a proper, adequate response.

- Fourth, closed-source software is not the seal of approval for security that some might believe. Advocates of open-source software claim that the fact that code can be scrutinized improves security. While it does not close the debate of which model is more secure, SolarWinds' hack is a reminder to remain vigilant regardless of the adopted model.

We, at GDS, are continuously learning from such incidents. We have already notified our security customers about those incidents and the measures to be taken. We have also updated our security tools and platforms with the wealth of information released by FireEye and other, this will allow us to detect the offensive tools that has been stolen and the control servers used by the adversaries to conduct their attack.

ATTACK SCOPE

To date, several news about which companies were targeted by the latest attack have surfaced. The major ones were Microsoft & Cisco.
While investigating the first attack, Microsoft's research teams disclosed that different threat actor has installed malicious backdoors into the SolarWinds' software. On the other hand, Cisco claimed that although it doesn't use SolarWinds Orion for its enterprise network management or monitoring "we have identified and mitigated affected software in a small number of lab environments and a limited number of employee endpoints. We continue to investigate all aspects of this evolving situation with the highest priority."

While much of the focus on SolarWinds's hack has been related to government departments, the number of private companies affected is likely to continue to grow. As reported by Forbes, Equifax and General Electric Co. are currently investigating to determine if they were affected.
An unconfirmed list of decoded domain names circulated on Twitter stated that Intel Corp. is possibly another victim of the attack amongst others. The list is yet

Figure-2: Tweet including the list of affected domains targeted in the latest attack.

"Analyzing Solorigate" that's how Microsoft started their blog on how they are preparing their Windows Defender to detect and protect from the attack. In their blog they stated that a malicious armed "DLL" file was responsible for the attack. They also added "The fact that the compromised file is digitally signed suggests the attackers were able to access the company's software development or distribution pipeline. Evidence suggests that as early as October 2019, these attackers have been testing their ability to insert code by adding empty classes. Therefore, insertion of malicious code into the SolarWinds.Orion.Core.BusinessLayer.dll likely occurred at an early stage, before the final stages of the software build, which would include digitally signing the compiled code. As a result, the DLL containing the malicious code is also digitally signed, which enhances its ability to run privileged actions and keep a low profile."

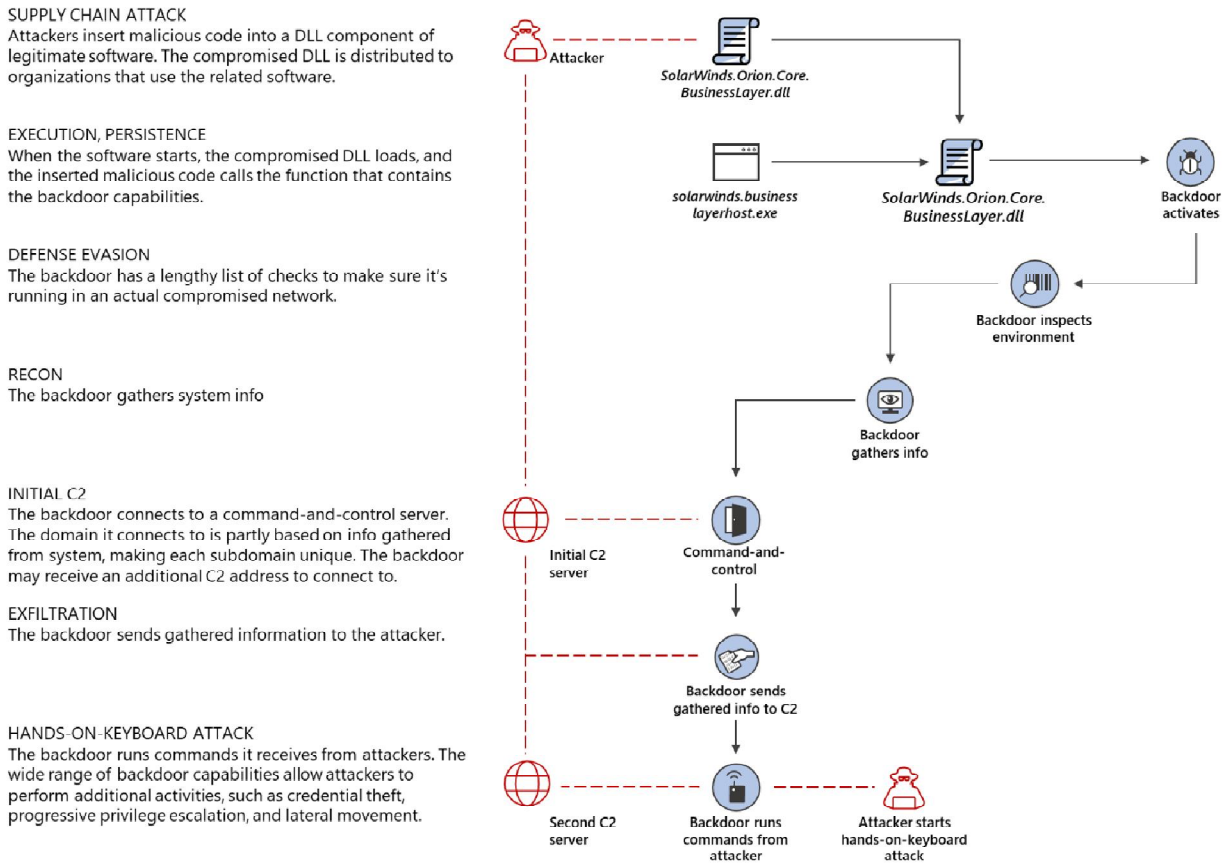

Figure-3: Solorigate malware infection chain

The chain shows how the attackers covertly infected dynamic libraries inside the SolarWinds' Orion platform then was automatically delivered to its customers within the update cycle.

Microsoft stated that "The challenge in detecting these kinds of attacks means organizations should focus on solutions that can look at different facets of network operations to detect ongoing attacks already inside the network, in addition to strong preventative protection." which confirm that looking at the attack from a single point of view won't be enough to determine if you are attacked or not. Multiple logs from different sources and endpoints on the network should be correlated together to give a broader picture of how it started and the current posture of the infiltration.

WHAT CAN WE DO ABOUT IT?

"Prepare yourself, winter is coming" is a quote from "Ned Stark" from a famous series "Game of Thrones". He used the quote to galvanize his people to prepare for the leaner times he saw coming. Our winter will be in addition to the cold weather, a series of additional news that come to light mentioning new victims which will broader the attack scope till eventually one of us will be affected. Till then, we can start by implementing the guidance materials suggested by different vendors on our premises to prepare for what might be coming.

The first who published countermeasures where FireEye, which listed on their GitHub repository rules that can detect their stolen offensive tools. The list contains Snort, Yara, ClamAV & HXIOC rules. Additional information can be found on https://github.com/fireeye/red_team_tool_countermeasures

Talos Intelligence also prepared a list of IOCs to watch out for:

- Domains

  avsvmcloud[.]com (SUNBURST)
  panhardware[.]com (SUNBURST)
  incomeupdate[.]com (SUNBURST)
  websitetheme[.]com (SUNBURST)
  virtualdataserver[.]com (SUNBURST)
  thedoccloud[.]com (SUNBURST)
  globalnetworkissues[.]com (SUNBURST)
  virtualwebdata[.]com (SUNBURST)
  lcomputers[.]com (BEACON)
  webcodez[.]com (BEACON)
  infinitysoftwares[.]com (TEARDROP)
  zupertech[.]com (SUNBURST)
  databasegalore[.]com (SUNBURST)
  highdatabase[.]com (SUNBURST)
  freescanonline[.]com (SUNBURST)
  deftsecurity[.]com (SUNBURST)
  digitalcollege[.]org (SUNBURST)
  seobundlekit[.]com (SUNBURST)
  kubecloud[.]com (BEACON)
  solartrackingsystem[.]net (BEACON)
  ervsystem[.]com (TEARDROP)

- IP Addresses

  13.59.205[.]66 (SUNBURST)
  3.87.182[.]149 (BEACON)
  54.215.192[.]52 (SUNBURST)
  34.203.203[.]23 (SUNBURST)
  18.220.219[.]143 (SUNBURST)
  13.57.184[.]217 (SUNBURST)
  5.252.177[.]25 (SUNBURST)
  204.188.205[.]176 (SUNBURST)
  162.223.31[.]184 (BEACON)
  45.141.152[.]18 (BEACON)
  54.193.127[.]66 (SUNBURST)
  3.16.81[.]254 (SUNBURST)
  18.253.52[.]187 (SUNBURST)
  54.215.192[.]52 (SUNBURST)
  139.99.115[.]204 (SUNBURST)
  34.219.234[.]134 (BEACON)
  5.252.177[.]21 (SUNBURST)
  51.89.125[.]18 (SUNBURST)
  173.237.190[.]2 (BEACON)

- Hashes (SHA256)

  019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134 (SUNBURST)
  32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77 (SUNBURST)
  ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c (SUNBURST)
  c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77 (SUNBURST)
  c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 (SUPERNOVA)
  ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6 (SUNBURST)
  d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600 (SUNBURST)

dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b (SUNBURST)
1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c (TEARDROP)
b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07 (TEARDROP)
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589 (SUNBURST)
db9e63337dacf0c0f1baa06145fd5f1007002c63124f99180f520ac11d551420 (SUNBURST)
118189f90da3788362fe85eafa555298423e21ec37f147f3bf88c61d4cd46c51 (TEARDROP)
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed (SUNBURST)
abe22cf0d78836c3ea072daeaf4c5eeaf9c29b6feb597741651979fc8fbd2417 (SUNBURST)
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9 (SUNBURST)
2ade1ac8911ad6a23498230a5e119516db47f6e76687f804e2512cc9bcfda2b0 (SUNBURST)

Both CISA & DHS provided required actions and mitigations in their advisories:

1- Reimage system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1 and analyze for new user or service accounts.
2- Disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network.
3- Identify the existence of "SolarWinds.Orion.Core.BusinessLayer.dll" with a file hash of [b91ce2fa41029f6955bff20079468448] and "C:\WINDOWS\SysWOW64\netsetupsvc.dll".
4- Block all traffic to and from hosts where any version of SolarWinds Orion software has been installed.
5- Identify and remove threat-actor controlled accounts and persistence mechanisms.
6- Reset all credentials used by SolarWinds software and implement a rotation policy for these accounts. Require long and complex passwords.

To learn more about GDS and our security portfolio, visit https://www.gds.com.lb/security.php

Globalcom Data Services sal
Holcom Bldg., 4th floor
Corniche Al Nahr - Beirut - LEBANON
Tel: +961 - 1 - 59 52 59
info@gds.com.lb

About Globalcom Data Services sal

Operating since 1996, GDS is widely regarded as being one of the first Data Service Providers in Lebanon to bring modern and fast connectivity to the country. Always leading the way to the future for individuals and businesses, GDS has been continuously supporting new technologies for more than 20 years.
Building on its extensive network and security expertise, GDS provides a comprehensive security services portfolio. A team of security experts is available to assist customers with facing the complex security threats and cyber-attacks that might affect their business.