CYBERSECURITY BULLETIN

ISSUE 7

January 2021

WELCOME

Welcome to the seventh edition of GDS Cybersecurity bulletin.

"SolarWinds hack", possibly the biggest ever cybersecurity incident, directed against the US government and private companies, continues to expand in size and scope across other public and private sectors. Given the scale of the attack, all organizations must take swift action to assess their own exposure, re-evaluate their controls, security processes and mitigate their risks.

GDS' monitoring tools have detected several Lebanese organizations targeted by the malware and tools used in this attack. GDS SOC team can help assist and monitor your international traffic in case the IOCs cannot be implemented on your SIEM solution.

CONTENTS

SUMMARY

"The Sunburst attack appears to be one of the most complex and sophisticated cyberattacks in history" mentioned Sudhakar Ramakrishna the CEO of SolarWinds.

In this report, we will provide a general understanding for the attack path, lessons learned and the list of available IOCs to be added on your SIEM solution to determine your exposure to the attack.

SolarWinds Attack Supply Chain

New analysis results related to “SolarWinds hack” emerged last month, bringing up new information about this supply chain attack.

As stated by the cybersecurity firm Crowdstrike, a new malware named Sunspot was deployed in the network of SolarWinds in September 2019. This malware was used to replace the source code files inside “Orion” – a SolarWinds product deployed by 33,000 customers – with files that load the Sunburst malware previously discovered.
Sunburst malware executes commands with the ability to transfer files through DNS requests, execute files, profile the system, reboot the machine, and disable services.
This new finding will widen the footprint of the attack and no doubt leads to discovering more targeted victims that might be impacted by this initial entry backdoor.

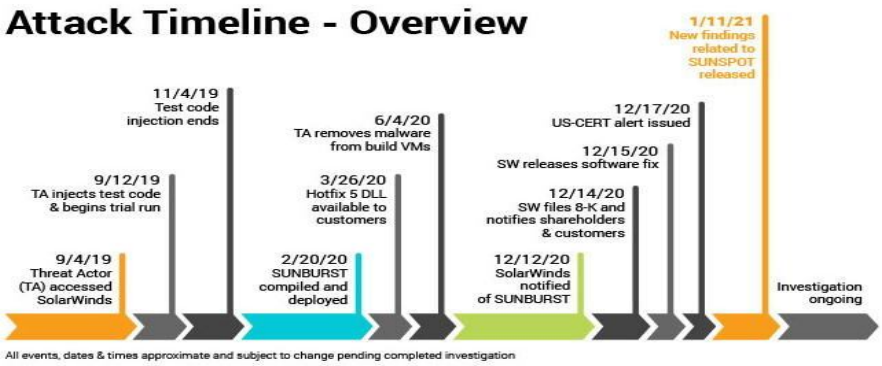

Figure 1: SolarWinds attack timeline - overview

An analysis of the Sunburst code by Kaspersky showed that it overlaps with the code of Kazuar malware strain, related to the Russian group Turla that is suspected as being a state-sponsored cyber-espionage outfit.
To avoid the attribution of the treat actor to any group, Kaspersky considered that SolarWinds ’hackers might be “using same coding ideas, buying the malware from the same coders, coders moving to different threat actors or simply a false flag to mislead the path of the analysts”.

Till date, all the security firms and researchers involved in the investigation are very cautious and they could not directly correlate SolarWinds hack to any cyber-attack group.

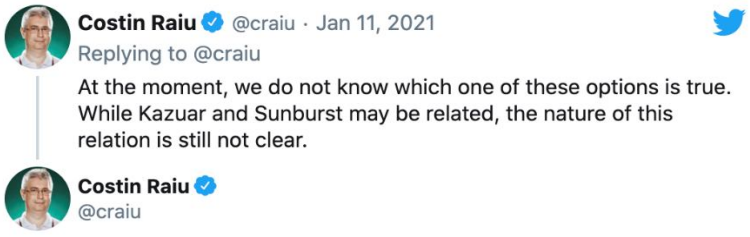

Figure 5: Costin Raiu, Director of Global Research and Analysis team at Kaspersky

The impact of this colossal hack is shown to be devastating. Till now, the reported victims included government, consulting, technology, and telecom firms in North America, Europe, Asia, and the

The top victims publicly announced are FireEye, Microsoft, Cisco, SAP, Intel, Deloitte, Nvidia, Fujistu, Amerisafe, Check Point, Digital Reach and Digital Sense, Belkin and Cox Communications.

Source: Third malware strain discovered in SolarWinds supply chain attack | ZDNet

Lessons Learned

Following this breach, enterprises should start assessing their overall security posture leading to enhancements in different areas.
So, what are the lessons learned and steps to be taken nearly?

- Most of the organizations have no visibility and control over the security practices implemented by their suppliers. In general, at the purchasing phase, the code of the product is not disclosed by the vendors and the customer's ability to perform proper assessment is practically difficult due to lack of expertise. Therefore, a new approach should be introduced at the purchasing level requiring an involvement from C-level executives, cybersecurity teams and other technical experts, not only to assess technically the product but also to perform a business risk and control management. Part of the points that can be tackled with the vendors at the purchasing phase are:
  - Request detailed and clear documentation regarding the best security practices applied on the code at the development level.
  - Validate their security practices by checking if the product is compliant with standards like ISO-27002 to reduce the risks.

  This approach will add complexity and delay to the purchasing process, but once the procedures are refined, it should become standardized and applied by all the enterprises.

- The initial detection of SolarWinds attack by the security firm FireEye was triggered by behavioural analysis rules and not through complex lateral movement or data exfiltration triggers.
  The analytic system of FireEye was able to detect an abnormal failed login attempt in correlation with other events such as user credentials, user location and others. This anomaly triggered an alert for their analysts to start investigating the abnormal behaviour.
  Given this fact, it is necessary to start implementing behavioural analytic technology within the security products using machine learning for data modelling, correlation, and analysis. Without such technology, this malicious login and all other associated activities would remain unknown and undisclosed. The lack of behavioural analytics in most enterprises today is considered as the most dangerous gap to be exploited by the hackers.
  GDS, through a dedicated team, is deploying artificial intelligence technology at different levels within the SOC and more specifically machine learning capabilities on AEGIS, GDS' managed SIEM platform.

- Nowadays, there are big challenges for an enterprise to identify that valuable data is being exfiltrated out its network and server endpoints, due to the huge amount of network traffic logs and to the tactics adopted by the hackers like obfuscation of the command-and-control IPs and encryption of the exfiltrated data. That said, most of the organizations must fine-tune their internal detection algorithms to consider for a possible malicious action from a trusted applications and zones and put more focus on the network management software.
  In addition, the traditional security best practices that are already implemented within big enterprises such as network segmentation, firewall perimeters policies preventing unwanted

users to access legitimate applications, are shown to be insufficient in preventing the occurrence of such attacks. This fact confirms that new security measures must be taken to reduce such high-profile software supply chain attacks.

Furthermore, new guidelines should be implemented to cover the above risks:

- Develop the security defences based on the principle that systems will be breached.
- Consider that cybersecurity is not only technology, but also processes and people.
- Implement security policies and procedures at all levels within an enterprise.

New IOCs For Sunspot

Tactics, Techniques and Procedures (TTPs)

- Persistence using scheduled tasks, triggered at boot time.
- Use of AES128-CBC to protect the targeted source code files and the backdoored source code file in the binary.
- Use of RC4 encryption with a hard-coded key to protect the log file entries.
- Log entries from different executions of the malware that are separated with a hard-coded value 32 78 A5 E7 1A 79 91 AC.
- Log file creation in the system temp directory C:\Windows\Temp\vmware-vmdmp.log masquerading as a legitimate VMWare log file.
- Detection of the targeted Visual Studio solution build by reading the virtual memory of MsBuild.exe processes, looking for the targeted solution filename.
- Access to the remote process arguments made via the remote process's PEB structure.
- Replacement of source code files during the build process, before compilation, by replacing file content with another version containing SUNBURST.
- Insertion of the backdoor code within #pragma statements disabling and restoring warnings, to prevent the backdoor code lines from appearing in build logs.
- Check of the MD5 hashes of the original source code and of the backdoored source code to ensure the tampering will not cause build errors.
- Attempt to open a non-existing mutex to detect when the malware operators want the backdoor to stop execution and safely exit.

Host Indicators of Attack

- Executables

Filename	SHA256 Hash	Build Time (UTC)
taskhostsvc.exe	c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168	2020-02-20 11:40:02

- Related Files

Description	SHA256 Hash
Backdoored Orion source code with SUNSPOT	0819db19be479122c1d48743e644070a8dc9a1c852df9a8c0dc2343e904da389

Description	SHA256 Hash
Backdoored Orion source code with SUNSPOT	0819db19be479122c1d48743e644070a8dc9a1c852df9a8c0dc2343e904da389

- File System

File Path	Description
C:\Windows\Temp\vmware-vmdmp.log	Encrypted log file

- Volatile Artifacts

Name	Type	Description
{12d61a41-4b74-7610-a4d8-3028d2f56395}	Mutex	Ensures a single implant instance
{56331e4d-76a3-0390-a7ee-567adf5836b7}	Mutex	Used to signal to the malware to safely exit

ATT&CK Framework

Tactic	Technique	Observable
Reconnaissance	**T1592.002** Gather Victim Host Information – Software	StellarParticle had an understanding of the Orion build chain before SUNSPOT was developed to tamper with it.
Resource Development	**T1587.001** Develop Capabilities – Malware	SUNSPOT was weaponized to specifically target the Orion build to replace one source code file and include the SUNBURST backdoor.
Persistence	**T1053.005** Scheduled Task	SUNSPOT is persisted in a scheduled task set to execute after the host has booted.
Defense Evasion	**T1140** Deobfuscate/Decode Information	The configuration in SUNSPOT is encrypted using AES128-CBC. It contains the replacement source code, the targeted Visual Studio solution file name, and targeted

Tactic	Technique	Observable
		source code file paths relative to the solution directory.
	T1027 Obfuscated Files or Information	The log file SUNSPOT writes is encrypted using RC4.
	T1480 Execution Guardrails	The replacement of source code is done only if the MD5 checksums of both the original source code file and backdoored replacement source code match hardcoded values.
	T1036 Masquerading	SUNSPOT masquerades as a legitimate Windows Binary and writes its logs in a fake VMWare log file.
Discovery	**T1057** Process Discovery	SUNSPOT monitors running processes looking for instances of MsBuild.exe.
Impact	**T1565.001** Data Manipulation Stored – Data Manipulation	Modification of the Orion source code to inject SUNBURST.

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.