GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad 12 January, 2021

Subject: **Advisory – SolarWinds Cyber Attack (Advisory No. 1)**

1. **SolarWinds Cyber Attack** made headlines after **FireEye** announced that its internal network was hacked using a malware-infected version of **SolarWinds Orion**. Hackers gained access to **FireEye RedTeam tools** and hacked VMware products. Attacks caused havoc in global cybersecurity industry as **critical US government agencies** were also affected. Microsoft has outline **attack methods, malware stains** and **mitigation strategies** but full extent of the attack remains unknown.

2. **Affected Institutes-Worldwide.** SolarWinds customers are based in USA, Canada, Mexico, Belgium, Spain, UK, Isreal and UAE. The affected organizations include IT industry, government department, think-tanks and NGOs. Major affected USA institutes include the following: -

Ser	Institute
a.	Energy Department and national Nuclear Security administration
b.	FireEye
c.	US Treasury Department
d.	US Department of Commerce's National telecommunication and Information Administration (NTIA)
e.	Department of Health, National Institute of Health (NIH)
f.	Cybersecurity and Infrastructure Agency (CISA)
g.	Department of Homeland Security (DHS)
h.	US Department of State

3. **Attacker's Details.** Adversary is believed to be **APT29 & Cozy Bear**. The group has been associated with **Russian Intelligence** and best known for carrying out 2016 hack against the **Democratic National Committee (DNC)**. FireEye has not confirmed the **APT29** attribution, however, attributed the group with a neutral codename **(UNC2452)**.

4. **Product Details – Orion.** Orion is a software platform for centralized monitoring and management usually employed in large networks to keep track of all IT resources such as servers, workstations, mobiles and IoT devices.

5. **Infection Details**

a. **MD5 Hash.** B91ce2fa4102f6955bff20079468448

b. **Indicators of Compromise**

i. [C:\WINDOWS/SysWOW64\netsetupsvc.dll]

ii. SolarWinds.Orion.Core.BusinessLayer.dll

c. **Malware Name.** The malware is named as SUNBURST by FireEye and Solorigate by Microsoft.

d. **News Source.** Attached at **Appex-I (Appex-I to Appex-IV)**

e. **Affected Orion Products.** Attach at **Appex-II**

f. **Yara Rules.** Attached at **Appex-III**

g. **Techniques used by the Attackers**

i. It was a supply chain attack where attackers compromised a server used to build updates for the SolarWinds Orion Platform followed by inserting backdoor malware into the product called Solorigate by Microsoft SUNBURST by FireEye.

ii. Post compromise activity leverages multiple techniques to evade detection and obscure their activity. **SolarWinds.Orion.Core.BusinessLayer.dll** is a **SolarWinds' digitally-signed** component of the Orion software framework that communicates via **HTTP to thirty party servers**.

iii. Attacker used **Compromied DLL** file associated with the Orion infrastructure management platform, allowing hands-on keyboard attack.

iv. **C&C Server**. Attached at **Appex-IV**

v. **Mitigation Steps Performed by Microsoft**

a. Removed the digital certificates the Trojaned files used.

b. Update Microsoft by Microsoft **Windows Defender** and **action for Solorigate** from **alert to Quarantine.**

6. **Capabilities of Malware.**

a. The update file is standard **Windows installer patch file** including the trojanized **SolarWinds.Orion.Core.BusinessLayer.dll**. The malicious DLL will be loaded by legitimate **SolarWinds.BusinessLayerHot.exe/SolarWinds.BusinessLayer hostx64.exe** (depending on system configuration). After period of up to two weeks, the malware will attempt to resolve a subdomain of **avsmclod[.]com** and hc C2 traffic malicious domains **mimic normal solarWinds API communications**.

b. Attacker can perform following activities on victim's machine: -

i. Remote access into the victim's environment.

ii. Transfer / execute files profile the system, reboot the machine, disable system services and deliver second -state payloads.

iii. Check whether HKU\SOFTWARE\Microsoft\CTF exists.

iv. Use multiple obfuscated blocklists to identity forensic and anti-virus tools running as processes, services and drivers.

v. Gather info on Registry, obfuscated Files/Information, FileDeletion, Ingress Tool Transfer, process/File/Directory and Windows Services.

c. **Light Malware Footprint.** Using limited malware to accomplish the mission while avoiding detection.

d. **Prioritization of Stealth.** The Malware is capable to go the significant lengths to observe and blend into normal network activity.

e. **High OPSEC.** The malware patiently conducts reconnaissance, consistently covering their tracks and using difficult to attribute tools.

f. **The malware masquerades its network traffic as the Orion improvement Program (OIP) protocol and stores**

reconnaissance results within legitimate plugin configuration files allowing it to blend with legitimate SolarWinds activity.

7. **Recommendations**

a. Regularly update reputed antiviruses such as Kaspersky, Avira, Avast etc and scan system regularly.

b. Sys admins must deploy FireEye published detection rules on respective servers (https://github.com/fireeye/sunburst countermeasures).

c. Upgrade cyber security procedures and develop cyber resources.

d. affected organizations (those using SolarWinds Orion and VMWare products) must immediately **disconnect or shutdown SolarWinds Orion products (versions 2019.4) from their network.**

e. **Block all traffic** to and from hosts (external to the enterprise) where any version of SolarWinds Orion software has been installed.

f. Endpoint protection systems must be placed in business environments.

g. Ensure that **Microsoft Defender** is operational as it is equipped to block malicious SolarWinds DLL.

h. Window defender and Firewall of system should be kept on recommended settings.

i. **Do not download attachments from emails unless you are sure about the source.**

j. **SolarWinds Servers**

i. ensure that SolarWinds servers are kept **isolated** / contained until a further **review** and **investigation** is conducted blocking all Internet egress.

ii. Restrict **Scope of connectivity to endpoints from SolarWinds servers** especially those considered as Tier 0 / crown jewel assets of SolarWinds servers.

iii. Restrict the **scope of accounts that have local administrator privileges** on SolarWinds servers.

iv. Consider changing passwords for accounts that have access to SolarWinds servers / infrastructure.

v. If SolarWinds is used to managed networking infrastructure, consider conducting a review of network device configurations. This is a proactive measure due to the scope of SolarWinds functionality, not base on investigative findings.

8. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for further analysis and suggesting mitigation measures:-

i. **asntisb2@cabinet.gov.pk**

9. Forwarded for perusal and dissemination of information to all concerned and under command, please.

Major
(Ch Usman Firdous)
Assistant Secretary (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

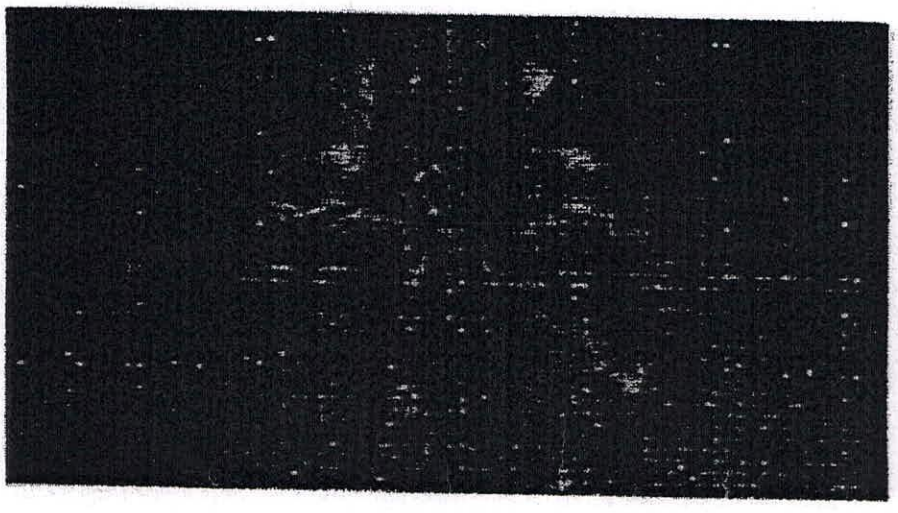
Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-II, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad

Appex-I

Microsoft has discovered yet more SolarWinds malware

The SolarWinds fallout continues as Microsoft reveals more



Appex-II

AFFECTED PRODUCTS

1. Known affected products include **Orion Platform versions 2019.4 HF 5,2020.2** with no hotfix installed or with **2020.2 HF 1**, including: -

a. Application Centric Monitor (ACM)
b. Database Performance Analyzer Integration Module* (DPAIM*)
c. Enterprise Operations Console (EOC)
d. High Availability (HA)
e. IP Address Manager (IPAM)
f. Log Analzyer (LA)
g. Network Automation Manager (NAM)
h. Network Configuration Manager (NCM)
i. Network Operations Manager (NOM)
j. User Device tracker (UDT)
k. Network Performance Monitor (NPM)
l. NetFlow Traffic Analzyer (NTA)
m. Server & Application Monitor (SAM)
n. Server Configuration Monitor (SCM)
o. Storage Resource Monitor (SRM)
p. Virtualization Manager (VMAN)
q. VoIP & Network Quality Manager (VNQM)
r. Web Performance Monitor (WPM)

2. Orion update versions released between **March 2020** and **June 2020** are infected: -

a. Orion Platform 2019.4 HF5, version 2019.4.5200.9083
b. Orion Platform 2020.2RC1, version 2020.2.100.12219
c. Orion Platform 2020.2RC2, version 2020.2.5200.12394
d. Orion Platform 2020.2, 2020.2 HF1, version 2020.2.5300.12432

3. Update affected systems to the latest version as soon as possible according to VMware's instructions at **(Reference Number KB81754)**. Review and harden configurations. The vulnerability affects the following products: -

a. VMware Access(R)3 20.01 and 20.10 on Linux(R)4
b. VMware vIDM(R)5 3.3.1,3.3.2 and 3.3.3 on Linux
c. VMware vIDM Connector 3.3.1, 3.3.2, 3.3.3, 19.03
d. VMware Cloud Foundations(R)6 4.x
e. VMware vRealize Suite Lifecycle Manager(R)7 8.x

Appex-III

SIGNATURES AND RULES

1. FireEye has provided two Yara rules to detect TEARDROP. Defenders should look for the following alerts from FireEye HX: MalwareGuard and WindowsDefender. Rules that helps to block some of the known domains and malicious traffic: -

   a. Rule 1010669 – Identified Malicious Domain – SolarWinds
   b. Rule 1010675 – Identified HTTP Backdoor Win32.Beaconsolar.A Runtime Detection
   c. Rule 1010676 – Identified HTTP Trojan.MSIL.Sunbrst.A traffic request
   d. Rule 1010691 – Solarwinds Orion Remote Code Execution vulnerability (CVE-2020-14005)
   e. Rule 1010693 – Identified HTTP Trojan.MSIL.Sunburst.A Traffic Request -1

2. Deep Discovery Inspector (DDI) rule has been released for this threat in the latest pattern: -

   a. 4491: DNS_SUNBURST_RESPONSE_SB
   b. 4492: HTTP_SUPERNOVA_WEBSHELL_RESPONSE

Appex-IV

MALICIOUS COMMUNICATING SERVERS

1. Deftsecurity.com
2. Highdatabase.com
3. Incomeupdate.com
4. Panhardware.com
5. Thedoccloud.com
6. Zupertech.co,
7. Seobundlekit.com
8. Solartrackingsystem.net
9. Freescanonline.com
10. Kubecloud.com
11. Thedoccloud.com
12. Globalnetworkissuses.com
13. Digitalcollege.org
14. Lcomputers.com
15. Webcodez.com
16. Virtualwebdata.com
17. Databasegalore.com
18. Avsvmcloud.com