PURPOSE

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The National Cyber Security Centre is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

OVERVIEW

On 13 December 2020 SolarWinds disclosed a security advisory outlining recent malicious activity impacting SolarWinds Orion Platform resulting from a supply chain compromise. FireEye has published a report detailing the widespread campaign by a "highly evasive" actor gaining access to numerous public and private organizations around the world.

DETAILS

FireEye reports they have discovered a global intrusion campaign resulting from a supply chain compromise. Through trojanizing SolarWinds Orion Platform software updates, actors were successfully able to distribute malware. This campaign may have begun as early as Spring 2020 and FireEye reports it is currently ongoing. Post compromise activity leverages multiple techniques to evade detection and obscure their activity, which includes lateral movement and data theft. FireEye has provided a detailed analysis as well as opportunities for detection.

MITIGATION

SolarWinds has provided guidance on how to identify the version of Orion Platform organizations are using, and to check which hotfixes organizations have applied. If an organization cannot upgrade immediately, please follow the guidelines securing an Orion Platform instance.

An additional hotfix release, 2020.2.1 HF 2 is anticipated to be made available Tuesday, December 15, 2020. SolarWinds recommends that all customers update to release 2020.2.1 HF 2 once it is available, as the 2020.2.1 HF 2 release both replaces the compromised component and provides several additional security enhancements.

The following recommendations provided by FireEye are mitigation techniques that could be deployed as first steps to address the risk of trojanized SolarWinds software in an environment. The Cyber Centre encourages organizations review the below recommendations and action those based on an organization's own risk-based assessment.

Ensure that SolarWinds servers are isolated or contained until a further review and investigation is conducted. This should include blocking all Internet egress from SolarWinds servers.

If SolarWinds infrastructure is not isolated, consider taking the following steps:

- Restrict scope of connectivity to endpoints from SolarWinds servers, especially those that would be considered Tier 0 / crown jewel assets
- Restrict the scope of accounts that have local administrator privileged on SolarWinds servers.
- Block Internet egress from servers or other endpoints with SolarWinds software.
- Consider (at a minimum) changing passwords for accounts that have access to SolarWinds servers / infrastructure. Based upon further review / investigation, additional remediation measures may be required.
- If SolarWinds is used to managed networking infrastructure, consider conducting a review of network device configurations for unexpected or unauthorized modifications. Note, this is a proactive measure due to the scope of SolarWinds functionality, not based on investigative findings.

FireEye has further provided indicators to assist network defenders in the detection of malicious activity.

If malicious activity is discovered in an environment, FireEye recommends conducting a comprehensive investigation and designing and executing a remediation strategy driven by the investigative findings and details of the impacted environment.

INCIDENT REPORTING

Government and Business Entities are encouraged to report any suspected cybersecurity incidents to CERT-GH at the National Cyber Security Centre (NCSC). Once a report is received, CERT-GH will work with relevant institutions including Sectoral CERTs (NCA/Telecommunications Sector CERT, NITA/Government Sector CERT, BoG/Financial sector CERT), Criminal

Investigation Department (CID), Data Protection Commission (DPC) and other relevant institutions to provide appropriate response and mitigating measures. Contact CERT-GH through the following points of contacts to report incidents:

REFERENCES

SolarWinds Security Advisory
https://www.solarwinds.com/securityadvisory

Highly Evasive Attacker Leverages SolarWinds Supply Chain
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Sunburst_countermeasures
https://github.com/fireeye/sunburst_countermeasures

Determine which version of a SolarWinds Orion product I have installed
https://support.solarwinds.com/SuccessCenter/s/article/Determine-which-version-of-a-SolarWinds-Orion-product-I-have-installed?language=en_US

Verify hotfixes that have been installed
https://support.solarwinds.com/SuccessCenter/s/article/Verify-hotfixes-that-have-been-installed?language=en_US

Secure Configuration for the Orion Platform
https://www.solarwinds.com/-/media/solarwinds/swdcv2/landing-pages/trust-center/resources/secure-configuration-in-the-orion-platform.ashx?rev=32603e0c87d84085b081f99a33fe5f4d&hash=62A998B9753957D82BC0F07005D38368

Customer Guidance on Recent Nation-State Cyber Attacks

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/