TECHHIVE SECURITY ADVISORY SERIES

Cybersecurity, News, Events and Threat Advisories

Volume 1 / Issue 1

TECH HIVE ADVISORY

Contact Us

+234 808 787 8783
contact@techhiveadvisory.org.ng
www. techhiveadvisory.org.ng

"Cybersecurity is becoming an integral part of business survival. The threat landscape is evolving, adversarial tactics and attacks are getting more sophisticated..."

Solarwinds Orion Threat (Solorigate)

Severity: High

What is the issue?

Upon download, Sunburst communicated with the hackers' malicious server to aid the identification of the victims. After that, the hackers chose the victims of interest, some of which included, Microsoft, FireEye, Cisco, United States Department of Homeland Security, etc.

This led to the compromise of the victims' assets both on cloud and on premises while also enabling the hackers to spy on the organization and access data. One of the lasting effects of this is that many threat actors will duplicate this type of supply chain attack due to its success rate.

A RECENT CYBER ATTACK TLDR

Threat actors secretly embedded a malicious code (Sunburst) in the update that Solarwinds pushed out for its Orion IT monitoring and management software. This compromised update was downloaded by over 18,000 organizations which included critical government agencies, thereby compromising some of these companies. See detailed information here.

What should you do?

- Use and implement least privilege access. This means that every user or module is given only privileges needed for the performance of their roles. Process for Privilege Access Management (PAM) should also be established
- Conduct periodic technical cybersecurity assessment (vulnerability assessment, penetration test, indicators of compromise assessment, threat hunting and intelligence etc.) using competent internal staff or third parties to conduct Penetration Test to discover vulnerabilities and its extents.
- Use Automated Threat Detection and Response solutions which helps to detect threat in real-time. Extend these to all endpoints, including critical infrastructure. See technical guidance for detecting Solorigate within your organizational network here.

Curated By: **Tojola Yusuf**
(@thetojolabilqis)
https://www.linkedin.com/in/tojola-yusuf-aciarb-b6640a152