CRAN
Communications Regulatory Authority of Namibia

Physical Address: Communications House, No.56 Robert Mugabe Avenue, Windhoek, Namibia
Postal Address: Private Bag 13309, Windhoek, Namibia **Tel:** +264 61 222 666 **Fax:** +264 61 222 790
Email: cran@cran.na **Fax2Email:** +264 088 642 748 **Website:** www.cran.na

CYBER SECURITY ALERT

ADVISORY BY THE COMMUNICATION REGULATORY AUTHORITY OF NAMIBIA ON THE "SOLARWINDS ORION SUPPLY – CHAIN ATTACK"

The Communication Regulatory Authority of Namibia (CRAN) through the AfricaCERT, wishes to issue an advisory on Solarwinds Orion supply – chain attack malwares namely:

FireEye: SUNBURST
Microsoft: Solarigate

This follows a growing global concern and trend that shows, cyber criminals exploiting the vulnerability within the supply chains through a malicious software update of the SolarWinds Orion Platform – i.e. a supply chain attack[1], to hit their targets.

SolarWinds Orion Supply Chain Compromise

SolarWinds Orion is an enterprise network management software suite that includes performance and application monitoring and network configuration management along with several different types of analyzing tools. SolarWinds Orion is used to monitor and manage on-premise and hosted infrastructures. To provide SolarWinds Orion with the necessary visibility into this diverse set of technologies.

The threat actor has been observed leveraging a software supply chain compromise of SolarWinds Orion products[2]. The adversary added a malicious version of the binary solarwinds.orion.core.businesslayer.dll into the SolarWinds software lifecycle, which was then signed by the legitimate SolarWinds code signing certificate. This binary, once installed, calls out to a victim-specific avsvmcloud(.)com domain using a protocol designed to mimic legitimate

[1] https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html
[2] https://www.solarwinds.com/securityadvisory

SolarWinds protocol traffic. After the initial check-in, the adversary can use the Domain Name System (DNS) response to selectively send back new domains or IP addresses for interactive command and control (C2) traffic. Consequently, entities that observe traffic from their SolarWinds Orion devices to avsvmcloud(.)com, should not immediately conclude that the adversary leveraged the SolarWinds Orion backdoor. Instead, additional investigation is needed into whether the SolarWinds Orion device engaged in further unexplained communications. If additional Canonical Name record (CNAME) resolutions associated with the avsvmcloud(.)com domain are observed, possible additional adversary action leveraging the back door has occurred.

Though Namibia has not been adversely affected by such attacks as at now, the trend depicts a serious concern in cybercrime and thus government agencies, critical infrastructure entities i.e Telecommunications and Broadcasting service licensees as well as private sector organizations, are advised to take the necessary precaution.

The Authority is therefore advising all government agencies, critical infrastructure entities i.e Telecommunications and Broadcasting service licensees, as well as private sector organizations who might be using the SolarWinds Orion Software, that:-

a. A patch (hotfix) has been made available by SolarWinds on 15 December and is now available in the SolarWinds Customer Portal at https://customerportal.solarwinds.com/ ; and
b. The malicious binaries can detected and removed by Microsoft Defender if the operating systems are updated.

Issued by:

COMMUNICATIONS REGULATORY AUTHORITY OF NAMIBIA
PRIVATE BAG 13309
WINDHOEK NAMIBIA

JOCHEN TRAUT
ACTING CHIEF EXECUTIVE OFFICER