UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00204

TANGLEBOT MALWARE GETS FULL ACCESS TO ANDROID

DATE ISSUED: 27th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new malware is spreading via SMS in the US and Canada with the false pretence of Covid-19 vaccine information and luring victims to a website where they are asked to install an Adobe Flash update then actually installs TangleBot is targeting Android users.

BREAKDOWN

In a similar fashion to the FluBot SMS malware which targeted victims in the UK and Europe and the CovidLock Android ransomware, attackers are preying on users fears using SMS as a new way of propagating their malware onto devices. Once installed, TangleBot is able to hide itself through many levels of obfuscation and the way it entangles itself in many device functions. This includes access to contacts, SMS and phone capabilities, call logs, internet access, location services, camera and microphone to enable data harvesting, spying, stalking, fraud and identity theft. It also creates an inventory of installed applications and is able to interact with a number of them or place overlay screens on top of them to harvest credentials. Detecting this type of malware and behaviour is extremely difficult so the best solution is to avoid infection in the first instance. There is no way to recover stolen data even if the user is able to detect the malware and remove it.

REMEDIATION STEPS

- Avoid clicking links in SMS messages. This should also apply to messages receive over social media or messaging applications – particularly if they are unexpected
- Read install prompts closely and be suspicious of websites requesting unexpected downloads.
- Only acquire applications from verified application stores such as Google Play

REFERENCES & RESOURCES

Threatpost https://threatpost.com/tanglebot-malware-device-functions/174999/
Heimdal Security https://heimdalsecurity.com/blog/us-canadian-android-mobile-users-targeted-by-tanglebot-malware/
CBS News https://www.cbsnews.com/news/tanglebot-android-malware-covid-19/