NCA-070322-06	ADVISORY ON SHARKBOT MALWARE AFFECTING ANDROID DEVICES

Overview

Sharkbot, is a malware that is designed to steal credentials and banking information from android devices. This malware works by taking advantage of accessibility features and it has managed to evade Google Play Store's security measures by using dropper apps. A dropper app is a trojan program that carries malicious code with it, to drop into a target device.

Impact

Sharkbot lures victims to enter their credentials in windows that mimic benign credential input forms. When the user enters credentials in these windows, the compromised data is sent to a malicious server.
Sharkbot also has the ability to send SMS messages, uninstall applications, send the device's contact list to a command and control server, disable battery optimization so as to enable it run in the background, imitate the user's actions (such as swipe over the screen, button presses, clicks and gestures), auto reply to notifications from Facebook Messenger and WhatsApp to distribute a phishing link which direct users to download dropper applications posing as antivirus apps, thus propagating the malware in a worm-like fashion.

Technical Details

Sharkbot uses Automatic Transfer Systems (ATS) to carry out unlawful transactions without the need for a live operator. The ATS characteristics allow the malware to get a list of events to replicate, which it then uses to make unauthorized transactions and install additional dangerous programs and carry out other malicious actions.
Sharkbot has several dropper applications that pose as antivirus apps to evade security barriers. Below, is a list of the harmful applications:

- Antivirus, Super Cleaner
- Atom Clean-Booster, Antivirus
- Alpha Antivirus, Cleaner
- Powerful Cleaner, Antivirus
- Center Security – Antivirus

Preventive Measures

Although these apps have been removed from the Google Play Store, Android device users should be cautious and always make research on every app before downloading. To further stay protected, ensure to carry out the following measures as presented below:

- Immediately delete such apps from device if already installed.
- Install known antivirus and anti-malware apps on devices.
- Run regular scans to detect threats.
- Do not download apps from unofficial marketplace or unknown sources.
- Do not download attachments or open links from unknown sources.

For further enquiries, please contact CERRT.NG through the following channels:

E-mail: cerrt@nitda.gov.ng
Phone:+2348178774580
Web: www.cerrt.ng