NCA-280323-03	ADVISORY ON HUNDREDS OF BANKING APPS AT RISK FROM THE NEW NEXUS ANDROID TROJAN.

Overview

The new Nexus Android banking trojan is designed to operate stealthily, with the ability to hide from detection and evade security measures. A staggering variety of different banking and financial apps are susceptible to attack by this Trojan. The malware is being distributed through phishing pages disguised as legitimate websites called YouTube Vanced.

Impact

The trojan can intercept and steal sensitive data, including login credentials, credit card information, and other financial information, once it has been installed on your device. Additionally, it has the ability to intercept codes from the Google Authenticator app as well as two-factor authentication messages delivered by text. The banking malware can also delete text messages that have been received on an infected device and periodically update itself by pinging a command-and-control server that is under the control of cybercriminals.

Preventive Measures

- Avoid clicking on ads or unverified links.
- Avoid visiting or downloading apps from unauthorized websites.
- Ensure to install Antivirus software on device.

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

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