रक्षा लेखा नियंत्रक (सेना)

Controller of Defence Accounts(Army)

बेल्वेडियर परिसर, आयुध पथ, मेरठ छावनी– 250001

Belvedere Complex, Ayudh Path, Meerut Cantt-250001

Through Website

No. IT&S/III/Cyber Security/2023 Date: 30/08/2023

To

All sections of Main Office
All sub offices under the aegis of CDA (Army) Meerut

Sub: Advisory regarding DogeRAT malware.

"Malware" or malicious software refers to any intrusive software developed by cyber criminals to steal data and damage/destroy computer systems. One such malware is **DogeRAT** (Remote Access Trojan) for Android smartphones, that is being distributed via social media and various messaging platforms under the guise of legitimate applications like Opera Mini, OpenAI Chat GPT, Youtube Premium, etc.

In order to caution all individuals against DogeRAT and to encourage safe cyber behavior while using smartphones, copy of the advisory issued by HQrs Office vide letter No. Mech/IT&S/810/Cyber Security/Misc dated 24.08.2023 is forwarded herewith for due cognizance and compliance.

This is issued with the approval of GO (IT&S).

Encl: As stated above.

NAVEEN PRAKASH, SAO(IT&S)-NAVEENP, IT&S-ARMY
Accounts Officer

“ हर काम देश के नाम”

रक्षा लेखा महानियंत्रक

उलान बटाररोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts
Ulan Batar Road, Palam, Delhi Cantt.- 110010
(IT&S Wing)

Phone: 011-25665588 Fax: 011-25675030 email:cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security/Misc **Circular** Date: 24/08/2023

To

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)
(through DAD WAN/email)

Sub: Advisory on DOGERAT .

An open source Remote Access Trojan (RAT) called DogeRAT has been detected that targets Android users primarily located in India as part of a sophisticated malware campaign. The malware is distributed via social media and messaging platforms under guise of legitimate applications like Opera Mini, OpenAI Chat GPT and premium versions of Youtube, Netflix and Instagram.

Analysis/Impact:

2. Once installed on a victim’s device, the malware gains unauthorized access to sensitive data including contacts, messages and banking credentials.

3. It can also take control of the infected device, enabling malicious actions such as sending spam messages, making unauthorized payments, modifying files and even remotely capturing photos through the device’s cameras.

4. It has additional capabilities such as taking screenshots, stealing images, capturing clipboard content and logging keystrokes.

5. The malware is capable of tracking device location, recording the microphone retrieving contact lists, accessing call, SMS, clipboard and notification logs, viewing installed applications, downloading and uploading files, viewing connectivity status and executing additional commands from the C2 server.

6. In a recent incident, a cybercriminal group was observed using Telegram to circulate fake Youtube, ChatGPT, Opera Mini and Instagram among other popular apps with DogeRAT (Remote Access Trojan) malware targeting naïve smartphone user.

Recommendations/Safeguards:

7. Never install apps from unknown third party app stores or any website. Always download them from Google Play store/Apple app store/Windows store.

8. Never reply or click URL links on messages or emails sent from unknown senders.

9. Always ignore messages with URL link to download any app.

10. It is advisable to keep smartphones updated with the latest software and security patches released by the device maker.

11. It is a good practice to install an antivirus app from prominent publishers such as Kaspersky, AVG, McAfee and CloudSek.

12. In view of the above, all the Controllers are advised to ensure compliance of the guidelines given above and disseminate these guidelines to all their sections and sub offices for strict compliance.

Neeraj

(Neeraj Surendran)
Sr. ACGDA (IT&S)