रक्षा लेखा प्रधान नियंत्रक (मध्य कमान) 1 करियप्पा मार्ग,लखनऊ
छावनी-226002
Principal Controller of Defence Accounts (Central Command) 1 Cariappa Road, Lucknow Cantt.– 226002
कार्यालय फोन सं.-0522-2451084/कार्यालय फ़ैक्स सं-0522-2453038
Office Phone No.-0522-2451084/Office Fax No.-0522-2453038
E.Mail- cda-luck@nic.in

वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

Circular

No. IT&S/AN/174/Cyber Security/2023-24 Dated: 30.08.2023

To,

The Officer-in-Charge,
All sections of main Office
All Sub-Offices
Under PCDA(CC) Lucknow

Sub: Advisory on DOGERAT.

Ref: HQrs Office Circular No. Mech/IT&S/810/Cyber Security dated 24.08.2023

****

With reference to HQrs Office circular/advisory cited under reference, it is brought to notice that, 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.

All the Sub-Offices under PCDA (CC) Lucknow & All the sections of main Office are advised to strictly comply with the guidelines given in HQrs office circular for safeguarding against DOGERAT. A copy of the circular is attached for reference.

A compliance report may be forwarded to this office by 05/09/2023.

Encl: As above.

Sr. Accounts Officer
(IT & S)

Copy to:
The OI/C
OA Cell
} For uploading on website.

Sr. Accounts Officer
(IT & S)

" 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 Surendran)
Sr. AO(IDA (IT&S)