

“ हर काम देश के नाम ”

रक्षा लेखा महानियंत्रक



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



Phone: 011-25665586, 25665589, 25665763 Fax: 011-25675030 email: cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security

Circular

Date: 24/08/2022

To

**All PCsDA/CsDA/PCA(Fy)/PrIFA/IFA
(As per standard list)**

Subject : Cyber Security Alert : Whatsapp Squatting Campaign

Reference : HQrs office letter no. Mech/IT&S/810/Cyber security dated 18/02/2021

Please refer to the instructions issued vide this HQrs vide circular cited under reference regarding Fake Messaging App “WHSAPP.APK” embedded with malicious content.

2. Now, this HQrs have been received Inputs from MoD and credible Govt Agency that a new Squatting Campaign is being used by threat actors to target users and convince them to hand over their login credentials. Further, the malicious actors have registered via the following domain names - agendawhatsapp.com, whatsappagenda.com and whatsappo.com.

3. The above mentioned domain names would mislead user into believing them to be associated with popular chat application whatsapp. The site can be utilized for phishing consumer credentials, hosting malicious payloads, disinformation etc.


4. In continuation to the above instructions mentioned in referenced circular dated 18/02/2021 to all PCsDA/CsDA, All controllers officers are requested to issue necessary directions to all offices & staff, so that all get sensitized with and remain vigilant regarding alert for new Whatsapp Squatting Campaign and follow following directions.

- a. **Not to install malicious applications.**
- b. **Verify genuineness of any website by verifying the address displayed only in address bar of the browser.**
- c. **The correctness of domain name may be verified by a diligent search of the website on popular search engine like google, bing etc and only the correct web address may be stored in shortcuts of browser for easy retrieval/reference.**

5. Further, ensure that domain name squatting vectors be blocked in the perimeter security devices like firewalls and UTM's installed at their offices over internet.

6. It is directed to ensure strict compliance of the guidelines given above. Action taken report may please be forwarded to this office.

Jt. CGDA (IT&S) has seen.


(Bipin Das)
Sr. ACGDA(IT&S)