" 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: 011-25665586, 2566589, 25665763 Fax: 011-25675030 email:cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security **Circular** Date: 12/07/2023

To

All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)

Sub: Advisory - Phishing Campaign by Cyber Threat actors .

Recently it has come to notice that a phishing URL 'https://drdo.gov.in.cyberdefenceexercise.cyou/cyberdefenceexercise.html' mimicking website of DRDO is in mass circulation since 03rd June 2023 within various sensitive government organisations including Defence establishments to harvest the NIC credentials of government officials under the pretext of Defence Cyber Exercise (DCX) through a compromised NIC email ID "mkjaiswal@ord.gov.in".

2. Additionally, some more such phishing campaigns are actively pursuing credential harvesting of Defence personnel under various pretexts which are shown in the table below:

S. No	Malicious Domain	IP Address
a.	cyberdefenceexercise.cyou	185.20.187.75 185.20.184.6 198.54.16.98
b.	aiapplication.chat	68.65.121.178
c.	vigilancedep.info	104.21.34.145
d.	kavachmail.in	104.21.64.80
e.	mod-info.xyz	68.65.121.153

3. The following compromised NIC email IDs were used to originate phishing campaigns:

S. No	Compromised email-ID
a.	manas.230192-cgo@gov.in
b.	coladm.afmc@nic.in
c.	msslakshmi.debel@gov.in
d.	jsns@dddpmod.gov.in
e.	Project75@navy.gov.in
f.	xanthopsia@nic.in

g.	olsbag@iaf.nic.in
h.	sao.33wg@iaf.nic.in
i.	devendra.k13@nic.in
j.	mkjaiswal@ord.gov.in
k.	captmaheshcmoudgil@gmail.com

4. In view of the above, the following actions are to be taken to contain spread of these campaigns:

   a. Block the suspicious URLs and the IPs mentioned in the table at para 2 at perimeter security devices.
   b. Sensitize all personnel under respective AOR regarding these phishing campaigns along with the modus operandi and advise them not to enter their NIC login credentials when redirected login page appears. Users to be also advised that any e-mail received from compromised IDs at para 3 above should not be opened.
   c. Forward any suspicious emails to DCyA email ID (soc.ids@gov.in) without clicking on any link/opening any attachments/enter credentials for analysis and further guidelines.
   d. Post forwarding to DCyA, delete phishing emails from the inbox and trash folders of all the recipients.

5. In view of the above, all the Controllers are advised to ensure strict compliance of the guidelines given above and disseminate these guidelines to all their sections and sub offices for strict compliance. Action taken report may please be forwarded to this office at the earliest.

Jt. CGDA (IT&S) has seen.

(Kamaljit Oberoi)
SAO (IT&S)