Azadi Ka Amrit Mahotsav

कार्यालय रक्षा लेखा नियंत्रक (सेना)

Office of Controller of Defence Account (Army)
बेल्वेडियर परिसर, आयुध पथ, मेरठ छावनी - 250001
Belvedere Complex, Ayudh Path, Meerut Cantt-250001
Email : cdaedp.dad@hub.nic.in

No. IT&S/712/Gen Corres. Through Website Dated: 30/05/2023

To,

The Officer In-Charge
1. All sections of Main Office
2. All sub-offices

Subject: Phishing malware attachment.

HQrs office letter no. **Mech/IT&S/810/Cybersecurity** dated 22.05.2023 and even no. dated 17.05.2023 on the above mentioned subject is hereby circulated for necessary action and strict compliance please.

Encls: As above.

– Sd –
SAO (IT&S)

Copy to:

IT&S –III: For uploading the circular on website.

SAO (IT&S)

कार्यालय रक्षा लेखा महानियंत्रक
उलान बटार रोड, पालम, दिल्ली छावनी-110010
O/o The Controller General Of Defence Accounts
Ulan Batar Road, Palam, Delhi Cantt.- 110010
Phone: 01125665761,762 email: cgdanewdelhi@nic.in

4778
22/05/23

(सू.प्रो.एवं प्र विंग)

No. Mech/IT & S/810/Cybersecurity

Date: 22/05/2023

To,

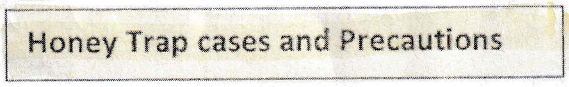
All PCsDA/CDAs/PIFAs/IFAs

For circulation & compliance
(B) 24/5
GO (EDP)

Subject: Phishing Malware attachment.

It has been observed that mails with following attachment are being received in NIC mail **(copy enclosed)**.

DO NOT CLICK ON THIS LINK


Honey Trap cases and Precautions

These mails are spoofed and sent to steal your e-mail ID & password. Please stay away from such type of mails and do not open the link given or share it with anyone else. In case if any individual has opened the above mentioned link, then it is advised to follow following instructions:-

i. Password must be reset immediately/changed on regular basis to prevent happening of such security incidents.
ii. Systems must be formatted to make it safe for future use.
iii. Any occurrence regarding the breach of security may be informed on urgent basis.
iv. Password for KAVACH application must be reset/ changed immediately on regular basis to prevent happening of such security incidents.

SAO (IT)

Email

Honey Trap Case and Precautions

From : Shri Hemant Jain, DEO Odisha Circle, Bhubaneshwar <deobhub-stats@nic.in>

Mon, May 08, 2023 04:26 PM

1 attachment

Subject : Honey Trap Case and Precautions

To : oiccomnetcen-navy@gov.in, CPMG Orissa Circle <cpmg_ori@indiapost.gov.in>, ORSAC <orsac.od@nic.in>, Cmde Hemant Padbidri <dawfs@navy.gov.in>, SRIRAM PADHI <civil-sed.koraput@hal-india.co.in>, Ishan Pande <msaseychelles@navy.gov.in>, ANKIT PANDEY <ankitpandey.dad@hub.nic.in>, Gyanendra Pandey <aogphqsambalpur.ncc@nccindia.nic.in>, Rambalak Paswan <chti1059@nic.in>, Amit Kumar Mishra DDG Lands II <ddglands2-dgde@nic.in>

Reply To : Shri Hemant Jain, DEO Odisha Circle, Bhubaneshwar <deobhub-stats@nic.in>

Respected Sir/ Madam,

1. **Dir Pradeep Kurulkar** of DRDO was arrested for sharing sensitive information with Pakistan Intelligence agency.

2. MoD has published a case study containing mobile nos used by Pakistani intelligence operatives to lure and honey trap Indian Officials.

3. Please view the case study and report any unusual activity.

Honey Trap Case and Precautions → Don't click here

- Instruct all to follow instructions.

--

भवदीय,

रक्षा सम्पदा अधिकारी.
ओड़ीशा मण्डल,
प्लॉट नो। 163, प्राची एनक्लव,
चन्द्रसेखरपुर, भूबनेश्वर,
ओड़ीशा- 751016.

3

भारत सरकार **Government of India**
रक्षा मंत्रालय **Ministry of Defence**
कार्यालय रक्षा लेखा महानियंत्रक
Office of the Controller General of Defence Accounts
उलान बटार रोड, पालम, दिल्ली छावनी-110010
Ulan Batar Road, Palam, Delhi Cantt – 110010
E-mail:cgdanewdelhi@nic.in
(IT & S Wing)

IT&S & OA cell for circulation in all sections & sub offices

CIRCULAR

No. Mech/IT & S/810/CyberSecurity

Dated :17/05/2023

To

All PCsDA /CDAs/PCA(Fys)/Pr.IFAs/IFAS

Subject: Advisory-A new wave of cyber attacks on Indian IT Infrastructure-China bsed threat actors.

It has been observed recently, that cyber threat actors are targeting prominent Indian organisations like AIIMs, ICMR, UIDAI etc. The TTPs (Tactics, technique & procedures) & IOCs are associated with Chinese threat actors. Further, investigation revealed that a new wave of cyber-attack campaign beginning around February, 2023 in which again systems of AIIMs, ICMR & UIDAI were targeted with similar type of malware (PlugX/Korplug) associated with Chinese threat actors.

2. Unique to this campaign is the usage of storage devices (pen drive) to compromise the systems and propagate the malware to other computers in the organisation. Based on the cyber incident report, it is observed that count of compromised computers in this case is far more than observed earlier as count of compromised computers is based on IP addresses & IP addresses are of routers which are connected with multiple computers.

3. Modus Operandi of the cyber-attack indicates involvement of Chinese threat actors who carry out cyber-attacks for data exfiltration & espionage. This malware infection is likely to increase in government organisations as there is no antivirus capable of detecting these malicious files. The list of IOCs (Indicators of Compromise) associated with this malware campaign is enclosed as Annexure.

Accordingly, it is requested that adequate protections may be put in place on IT systems at organisational level, in order to mitigate the cyber threats as mentioned above.

Enclosure: Annexure

Neeraj S

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

Annexure

Indicators of Compromise(IOCs)

1. Pen Drive

	Location	File/Folder Name	Remarks
	Root of pen drive e.g. E:/G:/ etc.	➢ Repository ➢ **KINGSTON.scr** or<volume name of the pen drive.scr> ➢ SmadEngine.dll ➢ Kaspersky ➢ Kaspersky/Usb drive/2.0 ➢ Kaspersky Usb Drive 2.0/crash handler.dll ➢ Kaspersky/Usb drive/2.0 ➢ ShellselDb.dat ➢ Kaspersky/Usb drive/2.0 Smad Protect32.exe ➢ Kaspersky/Usb drive/2.0/SmadEngine.dll ➢ Kaspersky/Usb drive/2.0/steam_monitor	The malicious file**<volume name of pen drive> will have different** nomenclature as per the volume name of the infected pen drive

2. Infected Computers:

S.No.	Location	File/Folder Name	Remarks
1.	C://Users/Public/Public Documents/Aquarius	crashhandler.dll gup.exe libcurl.dll Shellsel.Db.dat SmadavProtect32.exe SmadEngine.dll Steam_monitor.exe	A malicious folder by the name of Aquarius gets created comprising 7 malicious files
2.	C://Users/Public/Libraries/ Function	(i) IDMgetAll.dll (ii) Idmvs.dll	
3.	C://Users/Public/Libraries/ Function 1	LJHZRSPVLFMEWGNMYI	It has been observed that similar gibberish file names across infected computers
4.	C://Users/Public/Libraries/ pc_1	QZPDYHLSJA	
5.	C://Users/Public/Public Libraries/reg_1	DNPRNXDRLYKYWZVK	

3. Malicious IP Addresses

S.No.	IP address	Location	Remarks
1.	103.164.203.164	Malaysia	
2.	45.64.184.248	Thailand	