"हिंदी भाषा राष्ट्र निर्माण में सहायक है"

रक्षा लेखा प्रधान नियंत्रक) मध्य कमान (1 करियप्पा मार्ग, लखनऊ
छावनी226002-
Principal Controller of Defence Accounts (Central Command)
1 Cariappa Road, Lucknow Cantt.– 226002
कार्यालय फोन सं2453038-0522-कार्यालय फ़ैक्स सं/2451084-0522-.
Office Phone No.-0522-2451084/Office Fax No.-0522-
2453038
E.Mail- cda-luck@nic.in

Circular

No: EDP/AN/174/Cyber Security/2023-24 D te: 25 /05/2023

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

Sub : Advisory-A new wave of cyber attacks on Indian IT infrastructure-China based threat actors.

Ref : HQrs office letter No. Mech/IT&S/810/CyberSecurity dated 17.05.2023

****

With reference to HQrs office letter mentioned under reference, an advisory is issued regarding A new wave of cyber attacks on Indian IT infrastructure-China based threat actors.

It is requested that adequate protections may be put in place ,as mentioned in the circular, on IT systems at organizational level, in order to mitigate the cyber threats. A copy of circular is attached for reference.

Encl: As above

Sd-
Sr.AO (IT&S)

Copy to : OA Cell (Local) } For Website Upload

प्रमोद
Sr.AO (IT&S)

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

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 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	