



कार्यालय ,रक्षा लेखा नियंत्रक, नं. 1,स्टाफ रोड, सिकंदराबाद  
Office of the Controller Of Defence Accounts  
No.1 Staff Road, Secunderabad-500 009  
(Tele/Fax:040-27843385-407 Fax: 040-27810499)  
Email id: secdedpcda.dad@nic.in



परिपत्र / CIRCULAR

सं./NO.ITS/5805/Gen.Corr/CyberSecurity

दिनांक/Date: 22.05.2023

सेवा में/To

प्रभारी अधिकारी/The Officer in Charge

1. वे.ले.का. (अ.श्रे) ई.एम.ई., सिकंदराबाद / PAO (Ors) EME, Secunderabad
2. वे.ले.का. (अ.श्रे), से.आ.कोर, सिकंदराबाद / PAO(Ors) AOC, Secunderbad
3. क्षे,ले.का. (थलसेना), विशाखापट्टणम /AAO (Army), Visakhapatnma
4. सिकंदराबाद/विशाखापट्टणम/सूर्यलंका और यदुदुमैलारम स्थित उप-कार्यालय  
All Sub offices, Secunderabad / Visakhapatnam / Suryalanka and Eddumailaram
5. मुख्य कार्यालय के सभी अनुभाग (स्थानीय) / All Sections, Main Office, Local.

विषय: उपदेशिका - भारतीय सूचना प्रौद्योगिकी आधारभूत संरचना पर साइबर हमले की नई लहर - चीन आधारित खतरे के सूचक ।

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

संदर्भ: मुख्यालय कार्यालय का दिनांक 19.05.2023 का पत्रांक Mech/IT&S/810/Cyber Security.

Ref: HQrs letter No. Mech/IT&S/810/Cyber Security dated 19.05.2023.

\*\*\*\*\*

उक्त विषय पर मुख्यालय कार्यालय के उपरोक्त पत्र की एक प्रति सूचना एवं अनुपालन हेतु संलग्न है ।

A copy of HQrs letter referred above on the subject is enclosed for information and compliance.

संलग्न: उपरोक्तानुसार

Encl: As above.

*Handwritten signature and date: 22/5/2023*

(के. गोपीचंद)

लेखा अधिकारी (आई.टी.)

प्रतिलिपि/Copy to:-

प्रभारी लेखा अधिकारी, आई.टी. अनु.

AO I/c , IT Section, Local

: र.ले.नि. की वेबसाइट पर पत्र/परिपत्र अपलोड करने के अनुरोध के साथ।

: with a request to upload this letter/circular in CDA's website.

*Handwritten signature*

(के. गोपीचंद)

लेखा अधिकारी (आई.टी.)



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)



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 based threat actors.**

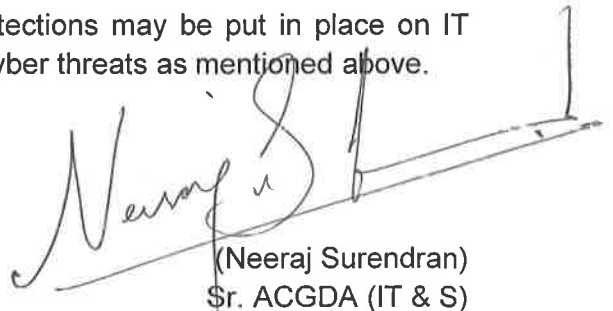
It has been observed recently, that cyber threat actors are targeting prominent Indian organisations like AIIMs, ICMR, UIDAI etc. The TTPs (Tactics, technique & procedures) & IOCs are associated with Chinese threat actors. Further, investigation revealed that a new wave of cyber-attack campaign beginning 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)

## Indicators of Compromise(IOCs)

### 1. Pen Drive

	Location	File/Folder Name	Remarks
	Root of pen drive e.g. E:/G:/ etc.	<ul style="list-style-type: none"> <li>➤ Repository</li> <li>➤ <b>KINGSTON.scr</b> or&lt;volume name of the pen drive.scr&gt;</li> <li>➤ SmadEngine.dll</li> <li>➤ Kaspersky</li> <li>➤ Kaspersky/Usb drive/2.0</li> <li>➤ Kaspersky Usb Drive 2.0/crash handler.dll</li> <li>➤ Kaspersky/Usb drive/2.0</li> <li>➤ ShellseIDb.dat</li> <li>➤ Kaspersky/Usb drive/2.0 Smad Protect32.exe</li> <li>➤ Kaspersky/Usb drive/2.0/SmadEngine.dll</li> <li>➤ Kaspersky/Usb drive/2.0/steam_monitor</li> </ul>	The malicious file< <b>volume name of pen drive</b> > will have <b>different</b> 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 ShellseIDb.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	