Tele: 39282

Army Cyber Group
Dte Gen of Mil Ops
Signals Enclave
Rao Tula Ram Marg
New Delhi-110010

B/51080/ArCyGp/T-3

12 Jun 2023

AWES
Building No - 202
Shankar Vihar
New Delhi -110010

DISSEMINATION OF CYBER ALERT

1. Pl ref telecon between Col NR Maggo, (Retd), Dir, IT, AWES & OIC, CERT-Army on 12 Jun 2023.

2. It has recently come to lt that a phishing campaign has been launched targeting the parents of the children studying in Army Public Schools across the country. The parents are being contacted through Email, WhatsApp call and landline Nos to verify the student detls.

3. For the purpose of verification, a link is being shared over email/ WhatsApp/ message. On clicking the link, the user is directed to google drive which further downloads a file containing a malware capable of stealing imp info from a user's cmptr.

4. To sensitize the Army Public Schools about such campaign it is recom that all the Army Public Schools may pl be intimated to sensitize all parents that no such communication has been rendered by the school/ AWES.

5. A Cyber Alert on the ibid campaign is att herewith for your info and necessary action pl.

(S Anirudha Rao)
Lt Col
Staff Offr
for Offg Cdr

Encls. As above

Copy To:-

DGMO (MO-12)

COMPUTER EMERGENCY RESPONSE TEAM - ARMY (CERT-ARMY)
ARMY CYBER GROUP CYBER ALERT: 36-2023
E-Mail: certarmy@nic.in Tele: 39707 (Army) Fax: 26151531 (Civil)

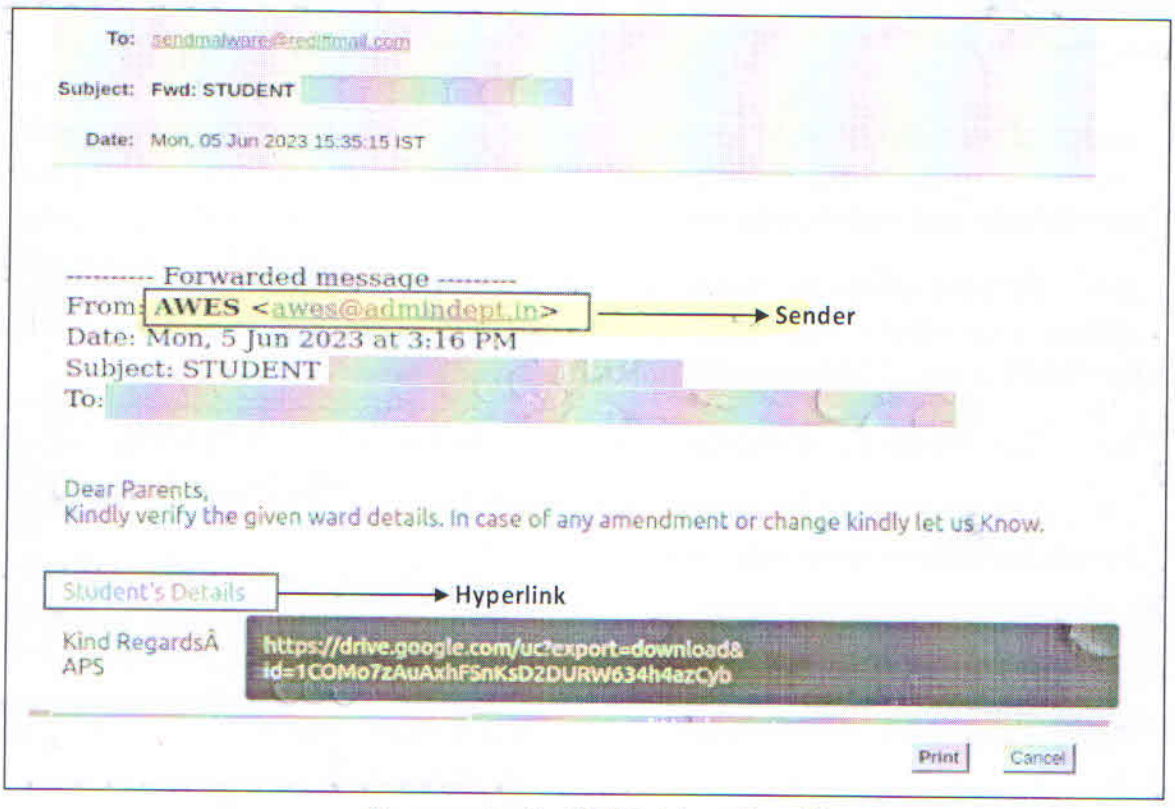
Campaign. Phishing Campaign Targeting Parents of Army School Students.

Background

1. A spear phishing attack has come to lt wherein a phishing email was promulgated by the threat actors to the parents of children studying in Army Public School to compromise the digital artefacts of IA pers. The email contains a hyperlink which is capable of downloading malicious executable file from google drive.

Modus Operandi

2. The threat actors appear to have obtained the name of children studying in various Army Public Schools and the email addresses of their parents. Further, a phishing email is being fwd to the parents on their official/personal email accounts from a fake email address named **AWES** (Email ID **awes@admindept.in**) having subject as '**STUDENT XXXXX <Student Name>**' with a hyperlink named '**Student's Details**'. Screenshot of the recd email is att below:-



Screenshot of Phishing Email

3. On accessing the hyperlink embedded with the email, a compressed file containing malicious file named **Student Details.exe** gets downloaded from google drive at url '**https://drive.google.com/uc?export=download&id=1COMo7zAuAxhFSnKsD2DURW634h4azCyb**'. The downloaded malicious file is capable of dropping the fwg files during execution:-

(a) circlex.exe

(b) Knowledge.dll

(c) detailsx.pdf - Fake PDF document

(d) myspace.zip - Compressed file contains Knowledge.dll (Malicious)

4. The said malicious file further triggers the dropped file named **circlex.exe** which makes necessary entry in 'Task Scheduler' for persistence and collects the computer details (cmptr name, OS details, IP addr, username etc) and uploads the collected info to its C2 server registered at IP addr **108.61.208.207**. The loc of said IP addr is **France**.

Recommendations

5. Fwg actions are recommended to be undertaken by users to contain the risks posed by the threat:-

(a) In case such email is recd, the same should be marked as spam and deleted. The email if recd should be fwd to CERT-Army at email ID **sendmalware@rediffmail.com**.

(b) Do not click on the hyperlink embedded with the email. If the link has been clicked and the file has been downloaded and accessed, users are advised to sanitize the cmptr with licensed and updated anti-virus tool imdtly.

(c) Keep all your sys updated with latest security patches and AV updates.

(d) The IP addr of C2 server **108.61.208.207** should be blocked at all cmptr/ perimeter security device (UTM/Firewall).

(e) Do not access emails from unknown contacts without verifying sender detls.

(f) This Cyber Alert may be disseminated to all serving pers through Rollcall/ Sainik Sammelan.

Conclusion

8. The threat actors are adopting various techniques to compromise the personal and official IT assets of def pers by means of sending various phishing mails using contemporary subjects. Users are advised to adhere to the recommendations listed above and also to the various best practices and advisories being regularly promulgated by Army Cyber Gp to ensure the security of pers/ official devices against these campaigns.

Sd/-x-x-x-x-x-x
(Abhishek Singh)
Lt Col
OIC CERT-Army
for Cdr

Case No: B/51084/ArCyGp/T-3

Dated: 08 Jun 2023

Distrs:-

All Brs/Dtes of IHQ of MoD Army (Coord)
All Comd/Corps HQ GS (IW)
All Comd/Corps HQ (Sigs)
All Comd/Corps HQ GS (Int)
All Div / Force HQ GS (Ops)
All Area HQ GS (Ops)
All Bde/ Sub Area GS

Internal

DG MI Dte
DGMO (MO -12) - For info pl.

Email

CERT-AF
CIRT-Navy
CERT-DCyA