SUBJECT: CYBER SECURITY ADVISORY - MALICIOUS SPEAR PHISHING EMAIL ATTACKERS (ADVISORY 13/2025)

Context. Reportedly, Indian threat actors are targeting government and defence departments for data acquisition via spear-phishing e-mails. In this regards, e-mails targeting specific users containing **malicious documents** have been identified. Details are as under:

2. **Modus Operandi**:

a. Malware propagated via spear phishing file names related to **Pahalgam Incident** (UpdateOnPahalgamAttackIIOK).

b. The malicious file had an extension of **.chm** (Complied HTML), which when clicked executes a hidden executable/ malicious file in background.

c. The malware after execution secretly collects data and images from device and further uploads to C&C (cyber espionage).

d. The documents contains screenshots of ARY, Duniya News, Channel 24, GTV, Express News etc. Details of malware are further elaborated in subsequent paragraphs.

3. **Technical/ Malware Details**:

a. **Malware File Name**. UpdateOnPahalgamAttachIIOJK(1-4).chm

b. **Hidden File/ Malware Name**. UpdateOnPahalgamAttachIIOJK.exe

c. **File Extension**. .chm (compiled HTML)

d. **Type of Malware**. Infostealer Trojan

e. **Infection Vector**. Email, WhatsApp Messages

f. **Detection**. Highly evasive (currently no known antivirus can detect this)

g. **Prevention**. Apply system hardening controls

h. **Command and Control (C2 server)**.

Rashid Mahmood
Secretary Revenue Div/Chairman FBR
01 July, 2025, 05:07:59 PM

M (IR-Ops)
M (IR-P)
M (Cus-Ops)
M (Cus-P)
M (Admn/HR)
M (IT)
M (PR)
M (Dl)
M (Legal)
M (Reforms)
M (L&A Custom)
M (Acc. & Audit)
Addl. Secy. Rev Div)
SA / SPS

DG(IT&DT)

02 JUL 2025
C(IT)

Fw'd, please.
3/7/25
Sec(IT) 4.1

Ser	IP Address	Port	Open Ports	Hosting Company	Location
(1)	151.236.21.48	8080	3386, 8080	M247 Europe (VPS Company)	France

i. **Capabilities of Malware**. Malware comprises of following capabilities:

(1) Querying of system information and account information including OS Name, OS Version, OS Manufacturer, OS Configuration etc.

(2) The malware has the capability to query all system directions, shared folders, Documents, Downloads, Desktop and system drive and look for PowerPoint, Document files, Word and PDF files.

(3) The consolidated information/ documents are uploaded to C2 server mentioned in para 3 (h) in systematic manner.

4. **User Advice**. Above in view, all users and administrators are advised to remain vigilant regarding phishing emails. Moreover, all administrators are advised to block above mentioned malicious domain/ URL at individual network firewalls. Cyber Security guidelines are attached as **Annex-A**.

5. For any query or reporting malware/ cyber incident, please forwarded the same on email address: falcon1947@proton.me.

6. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments for implementation.

Rashid Mahmood
Secretary Revenue Div/Chairman FBR
01 July , 2025, 07:02:59 PM

Annex-A

CYBER SECURITY BEST PRACTICES - PREVENTION AGAINST CYBER -ATTACKS

Guidelines for Smart Phone/ Internet & Email Security

a. **Be Aware of Phishing Attacks**

(1) Never open email attachments from unknown sources/ senders.

(2) If an email seems suspicious, just ignore it; even don't try to unsubscribe it by clicking unsubscribe link as it may allow hacker to access your emails data.

(3) Never open any attachment without anti-virus scan.

(4) If any suspicious email is received, immediately consult IT Administrator of your organization.

b. **Use Strong Passwords**

(1) To ensure email security, always use strong passwords employing combination of alphanumeric, special characters, upper and lower case letters.

(2) Avoid using general and easily guessable passwords e.g. DOB, Own/ family

names, vehicle registration number etc.

(3) Regularly change passwords.

c. **Use Two Factor Authentication**:

(1) In addition to strong passwords, also use two factor authentication e.g. OTP via call/ message, password reenter mechanism etc.

(2) Never share your One Time Password (OTP) with anyone.

d. **Avoid Email ID Exposure**:

(1) Avoid sharing email ID with unknown persons.

(2) Always confirm the identity of the individual to/ from whom email is being sent/ received.

(3) Avoid providing personal details in suspicious internet campaign.

(4) Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

(5) Never configure/ use official email on mobile phones.

e. **Always Send Password Protected Documents**

(1) All email attachments sent must be encrypted with password.

(2) Password must be communicated through a separate channel such as SMS, Call or WhatsApp message.

(3) Delete password from the sending channel (SMS, WhatsApp etc) once received /by the receiving party.

f. **Use Well Reputed and Licensed Anti-Virus**

(1) Endpoint (computer system or laptop) on which official email/ data is being accessed/ sent must be secured through reputed, licensed and updated antivirus/ anti-malware solution.

(2) Always keep system Firewalls activated and updated.

g. **Use Robust Paid Anti-Spam Filters**

(1) Use reputed Spam Filters.

Rashid Mahmood
Secretary Revenue Div/Chairman FBR
01 July 2021 05:07:59 PM

(2) Do not rely on Google/ Yahoo's Spam Filters as email attackers have become much sophisticated.

h. **Avoid Storing Data on Cloud Storage**

(1) Never store personal and official data on untrusted cloud storage.

(2) Avoid using online document converting tools (Word to PDF etc) with cloud based data storage technology.