GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad 02 September, 2021

06 SEP 2021

Subject: **Advisory - Cyber Attacks on Pakistan's Critical Information Infrastructure (Advisory No. 60)**

M(Admin/HR)
A.S(Rev. Div.)
M(I.T)

1. Recently, it has been observed that massive drive of spear phishing emails are targeting Pakistan's **Critical Information Infrastructures (CII),** both in public and private sectors. Identified emails are titled in a way to attract receiver's attention (e.g) **"List of Pak Defense Personnel, DHA MULTAN Housing Scheme, Pegasus Project Global Investigation, Draft National Cyber Security Policy and titles relating Afghan situation.** Phishing emails (in certain cases) are being sent with Pakistan Armed Forces logos, to pretend as legit.

2. Attacks have been identified as targeted attacks **by hostile Cyber actors** for information gathering and system control. Such emails contain malicious **.doc** files to assist malware execution on targeted systems that may result in **malware distribution, data loss and identity theft** etc. An advisory is attached at **Annexure-A** to sensitize and urge all concerned to adopt recommended preventive measures.

3. Forwarded for information / dissemination to all concerned, please.

Major
(Imran Nazir)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

Project Director,
DHA Multan,
Multan Public School Road,
Near southern bypass,
Main Office DHA Multan.

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad

S4(BDT-I) forward to CIO of PRAL

Dy.No. 124731-R
ived in Chairman's Secti
06 SEP 2021

Sent to M(A/HR)/AS(Rev Div)

5. Director General (Tech), Dte Gen, ISI Islamabad
6. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

Annex-A

Advisory - Cyber Attacks on Pakistan's Critical Information Infrastructure (Advisory No. 60)

1. **Context.** Recently, it has been observed that massive drive of spear phishing emails are targeting Pakistan's **Critical Information Infrastructures (CII),** both in public and private sectors. Identified emails are titled in a way to attract receiver's attention (e.g) **"List of Pak Defense Personnel, DHA MULTAN Housing Scheme, Pegasus Project Global Investigation, Draft National Cyber Security Policy and titles relating Afghan situation.** Phishing emails (in certain cases) are being sent with Pakistan Armed Forces logos, to pretend as legit.

2. Attacks have been identified as targeted attacks **by hostile Cyber actors** for information gathering and system control. Such emails contain malicious **.doc** files to assist malware execution on targeted systems that may result in **malware distribution, data loss and identity theft** etc. Therefore, recommendations at **Para 5** must be adopted to for prevention against such attacks. **Organizations must evaluate their specific systems and may take additional safe guards to ensure protection of their network, system and data.**

3 **Summary of Malicious Emails**

a. **File Names.** List of Pak Defence Personnel, Pegasus_List.docm & DHA MULTAN Housing Scheme

b. **Sources of Malicious Emails.** The malicious email servers are run from USA and Lithuania with following email addresses:-

Ser.	Email Address
(1)	info@ispr.gov.pk
(2)	alert@ispr.gov.pk
(3)	latest_info@fbr.news
(4)	notice@fbr.news
(5)	alert@fbr.news
(6)	thenewsinernational@mailerservice.directory

4. **C&C Servers.** The C&C servers of above malicious emails are located in **USA** and **Lithaunia;** URL: Pirnaram.xyz & Parinari.xyz and IP address: **62.77.153.51** & **172.67.219.211.**

5. **Recommendations.** The **IP addresses (62.77.153.51 & 172.67.219.211)** and **URL** (Pirnaram.xyz & Parinari.xyz) must be blocked at Firewall and Email Server. Additionally following recommended measures must be adopted:-

a. **Microsoft Office**

(1) Disable macros. **Do not enable content** of macros.

(2) Warning signs appearing in word documents indicates malware execution thus **select "no"** to halt execution and report.

(3) **Disable "Update automatic links at open"** option in Word by going to File > Options > Advance> scroll to General and then remove tick box.

(4) **Disable Microsoft Equation Editor in Office from registry** to avoid attack.

(5) Microsoft executables including **Verclsid, Rund1ll32 Regsvr32, Regsvcs/Regasm, Odbcconf, MSiexec, Mshta, InstallUtil, CMSTP, Control Panel, Compiled HTML File** to be monitored as major malware executables and must be blacklisted.

b. **Email Server**

(1) For secure communication, **email server should be hosted on secure domains with valid / verified HTTPs SSL certificate.** SSL certificate can be obtained from trusted vendors like GoDaddy, GlobalSign or Verisign etc, moreover, free SSL certificates may also be obtained via certificate authorities like LetsEncrypt (letsencrypt.org) or ZeroSSL etc.

(2) **To combat against Spamming, Spoofing** and **Phishing,** enable **SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance)** in DNS record.

(3) Always verify and test the domain for above configuration **by checking via online websites like dmarcian.com (DMARC Inspector), dkimvalidator.com (DKIM Validator) and mail-tester.com (Spam Test). If email server doesn't qualifies the test then it shouldn't be deployed in production environment.**

(4) It is mandatory **to turn on STARTTLS on email servers** and **test it** after deployment and configuration via **https://www.checktls.com/TestReceiver (Online TLS Checker).** If any of the **test fails then email server shouldn't be deployment in production environment.**

(5) Restrict and secure use of command-line application and system administration tools like **Powershell.**

(6) **Phishing filter** on email application to avoid attacks.

c. **Internet / Email Users**

(1) All email attachments sent must be encrypted with password and password must be communicated through secure source.

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

(3) Google warns about malicious file / website so don't proceed on site and Install Anti-phishing toolbar.

(4) Identify spam message if it seems urgent, provide some gifts / shocking news or requires to spread it among others.

(5) Never open attachments from untrusted sources.

(6) Endpoint on which official email is being accessed / sent should be secured via well reputed, licensed and updated antivirus solution.

(7) Never forward your OTP (One time password) to anyone.

(8) Window defender and Firewall of system to be **on recommended settings.**

(9) **Never click on links** and **type the link** of known websites.

(10) Email addresses, passwords or sensitive information should never be entered on links.

(11) Do not forward, click or view link or photo sent on WhatsApp from unknown numbers.

(12) Requests for personal or financial information should be avoided and never entertained.

(13) Change password frequently and **never store passwords in browser.**

6. **Reporting of Suspicious Files / Emails.** Any Malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

asntisb2@cabinet.gov.pk

7. Forwarded for perusal and dissemination of information to all concerned and under command, please.