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

No. 1-5/2003 (NTISB-II) Islamabad 24 June, 2021

Subject: **Advisory- Prevention Against Cyber Espionage (Advisory No. 42)**

M(Admin)/HR)

M(I.T)

A.S(Rev.Div.)

1. Recently, a targeted malware is spreading through **email** with the subject **"Quotation_of_spare_parts"** among defence and civil organizations for information gathering and system control. These spoofed emails contain a malicious **".ink"** file which looks like a legitimate **PDF** file, but clicking on this link leads to malware execution in background. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned and adopt recommended preventive measures.

2. Forwarded for information and dissemination to all concerned, please.

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

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
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

CIO

Chief (I.T) / CIO
29/6
S(IT)

Annexure-A

PREVENTION AGAINST CYBER ESPIONAGE

1. Recently, a targeted malware is spreading through **email** with the subject **"Quotation_of_spare_parts"** among defence and civil organizations for information gathering and system control. These spoofed emails contain a malicious **".lnk"** file which looks like a legitimate **PDF** file, but clicking on this link leads to malware execution in background. Therefore, recommended measures at **Para4** must be adopted.

2. **Summary of Malicious Email.** Details attached at **Appex-I.**

3. **Capabilities of Malware**

   a. The malware deploys **HTTP RAT** to launch attack that can **easily bypass Firewalls** and gives **admin access** to target systems.

   b. The attacker can gain remote access of the system arid can execute additional payload.

   c. The malware uses various Microsoft certified executables including **certreq.exe, bitsadmin.exe** and **certutil.exe.**

   d. The attack involved **Windows certificates alterations** and **Task schedualers** to reside for persistence.

   e. The hackers may employ scripts to run through **Powershell.**

4. **Recommendations**

   a. Microsoft executables including **Verclsid, Rundll32, Regsvr32, Regsvcs / Regasm, Odbcconf, MSiexec, Mshta, InstallUtil, CMSTP, ControlPanel, Compiled HTML File** may be monitored as major malware executables. These executables may also be blacklisted, if not required.

   b. Restrict and ensure secure use of command-line application and system administration tools like Powershell.

   c. Be vigilant regarding redirected links on email etc and typing sensitive information online.

   d. Uninstall all not in use applications and software from system and personal phone.

   e. **Do not download attachments from emails unless you are sure about the source.**

   f. Window defender and Firewall of system to be configured on recommended settings

5. **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

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

Appex-I

Summary of Malicious Email

1. **File Name.** Quotation_of_spare_parts.lnk / cstc.pdf

2. **Antivirus Detection Rate.** Nil

3. **Dropped Files.**

   a. C:\Users\public**x.bat**

   b. C:\Programdata\Office\Hbs.exe

   c. C:\Programdata\Office\scvhost.exe

   d. C:\Windows\Tasks\googleupdater.exe

4. **Persistence.**

   a. Task schedualer is created with key HYS and value C:\Windows\Tasks\googleupdater.exe

      (1) Task schedualer is created with key **HostDriveCache Populate** and value C:\Programdata\Office\scvhost.exe

      (2) Task schedualer is created with key **HBSDriveCache Populate** and value C:\Programdata\Office\Hbs.exe

   b. **C&C Servers**

Ser	URL address	Country
(1)	151.236.29.186	Netherlands
(2)	45.138.172.233	Netherlands
(3)	23.106.124.107	Singapore