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

No. 1-5/2003 (NTISB-II) Islamabad 2 February, 2021

Subject: **Advisory – Prevention against Finger Command Exploitation (Advisory No. 2)**

1. Presently, attackers are utilizing Windows 10 native binaries and Windows built-in utilities to execute malicious payloads to **bypass / evade antimalware solutions**. One of such commands / utilities being abused by attackers is "**finger.exe**" being exploited by attackers for downloading maiicious payloads and exfiltrating data. Due to novelty of this technique, many antimalware solutions are unable to detect this tactic. Therefore, system / network administrators need to follow recommendations mentioned at para 3 to avoid intrusions.

2. **Technical Details**

a. **Attack Vectors. Phishing Emails** or **compromised Websites**

b. **Utility being Abused.**
Finger exe(C:\Windows\System32finger.exe

c. **Mode of Operation**

i. Attackers send phishing email with **macro** document.

ii. upon downloading and opening attachment macro gets executed

iii. Malicious macro is preprogrammed to download additional payload from its C&C server using **finger.exe** utility.

iv Data (including Word, PowerPoint, Excel, PDFs) is exfiltrated to C&C server using finger command.

d. **Anti-Virus Evasion.** Finger command is **whitelisted** and **digitally singed Microsoft Windows Operating System utility** and attackers are increasingly abusing Finger utility to **bypass automated defenses** like **firewalls** and **antivirus**.

03 FEB 2021
M(Admin) / HR
M(I.T)
A.S
(Review)
Chief (IT)
FBR eDOX No. 17124-R Received in Member (IT) Dated 4/2/2021
FBR eDOX No. 17124-R Received in Chairman's Secty. on 03 FEB 2021

e. Other Commonly abused Commands / Utilities. List of commands that can be abused by attackers for exploitation purposes is mentioned at link:

https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

3. Recommendations

a. System / Network Administrators

i. Windows commands / utilities not required by end-users **should be blacklisted for endpoint execution** like mshta.exe, bitsadmin.exe, finger.exe, cerrtutil.exe, cipher.exe and syskey.exe.

ii. **Block execution of scripts** with .vbs, .vbe, .hta, .js, .wsh, .wsf, .com, .pif., .ps1 extensions.

iii. **Blacklist / block outbound network connections** from winword.exe, notepad.exe, exploarer.exe, powershell.exe, bitsadmin.exe, mshta.exe, excel.exe and eqnedt32.exe.

iv. Centralized **monitoring of endpoint windows logs** must be performed to detect anomalous user behavior.

v. Regularly update antimalware solutions running on endpoints in enterprise environment as well as standalone systems.

vi Educate endusers regarding Cyber Security best practices and antimalware measures.

b. End-users

i **Regularly update reputed antiviruses** such as Kaspersky, Avira, Avast etc.

ii **Do not download attachments from emails or websites unless sure about the source.**

iii. Avoid downloading softwares from untrusted websites or torrents.

iv. Use Chrome or Firefox for browsing internet instead of internet explorer.

v. Make sure that web browser is up to date and no plugins other than adblock or adblock plus are enabled.

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

i. **asntisb2@cabinet.gov.pk**

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

Major
(Ch Usman Firdous)
Assistant Secretary (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-II, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad