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

No. 1-5/2003 (NTISB-II) Islamabad 13 August, 2021

Subject: **Cyber Security Advisory – Netwire RAT (Remote Access Trojan) (Advisory No. 53)**

1. Recently, a spear phishing campaign is targeting a wide range of government organizations in Pakistan using netwire RAT (Remote Access Trojan) malware. The combination of spear phishing and the use of information stealing RAT makes it a sophisticated attack vector. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned to take recommended corrective measures.

2. Forwarded for information / dissemination to concerned, please.

17 AUG 2021
M(Admin/HR) e10
M(I.T)
A.S (Rev. Div.)

Major
~~(Imran Nazir)~~
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

Chief (IT)/CBD
23/8
S(IT)

FBR eDOX Dy.No
Received in Chairman's Secttt
17 AUG 2021

Annex-A

Cyber Security Advisory – Netwire RAT (Remote Access Trojan) (Advisory No. 53)

1. Recently, a spear phishing campaign is targeting a wide range of government organizations in Pakistan using Netwire RAT (Remote Access Trojan) malware. The combination of spear phishing and use of information stealing RAT makes it a sophisticated attack vector. Therefore, recommendations given at **Para 3** must be adhered to prevent against the ongoing attack campaign.

2. **Technical Details.** Attached at **Appex-I.**

3. **Recommendations**

   a. **For System / Network Administrators**

      (1) Windows commands / utilities not required by endusers **should be blacklisted for endpoint execution** like mshta.exe, bitsadmin.exe, finger.exe, certutil.exe, cipher.exe and syskey.exe

      (2) **Block execution of scripts** with .vbs, .vbe, .hta, .js, .wsh, wsf, .com, .pif, .ps1 extensions as this attack relies upon free execution of scripts and powershell.

      (3) **Blacklist / Block outbound network connections** from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, mshta.exe, excel.exe and egnedt32.exe.

      (4) Centralized **monitoring of endpoint windows logs** must be performed to detect anomalous user behavior

      (5) Regularly update antimalware solutions running on endpoints in enterprise environment as well as standalone systems.

      (6) Educate endusers regarding cyber security best practices and antimalware measures

   b. **For Endusers.**

      (1) **Regularly update well reputed antiviruses** such as Kaspersky, Avira, Avast etc. and scan system regularly.

      (2) **Do not download attachments from emails or websites unless you are sure about the source.**

      (3) Avoid downloading softwares from untrusted websites or torrents

      (4) Use chrome / firefox for browsing internet instead of internet explorer

      (5) Make sure that web browser is up to date and no plugins other than adblock or adblock plus is enabled

4. **Reporting of Cyber Security issues / Queries.** For reporting malware or any other query / issues regarding Cyber Security, details may please be forwarded to this organization on the following email address: -

asntisb2@cabinet.gov.pk

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

Appex-I

TECHNICAL DETAILS - NETWIRE MALWARE

Attack Vectors. Phishing Emails and RAT (Remote Access Trojan)

Utility Abused. Powershell + VBS based scripts

Attack Cycle

a. Attackers send phishing email with macro document or with a known exploit.
b. Upon downloading and opening attachment, macro / exploit gets executed.
c. Malicious macro / exploit is preprogrammed to download additional payload from its C&C server or compromised website using powershell .vbs based script.
d. Data (including word, PowerPoint, excel, pdfs) is exfiltrated to C&C server.

Netwire Features

a. Includes taking screenshots
b. Keylogging
c. Stealing browser logs
d. Clipboard data
e. File harvesting, the theft of OS information, and the ability to download and execute additional malware.