

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

No. 1-5/2003 (NTISB-II)

Islamabad/4 April 2020

Subject: Prevention Against Indian APT Group- RattleSnake (Advisory No.5)

1. Background. The National Telecom & Information Technology Security Board (NTISB), working under the aegis of Cabinet Division has been mandated to ensure Telecommunication and Information Technology Security at National Level. To this end all Ministries and Departments are updated by NTISB about emerging threats in the field of Telecom and IT and necessary remedial measure are also suggested by issuing frequent advisories.

2. Introduction. Recently, a suspected APT (Advanced Persistent Threat) attack Group from India termed as Rattlesnake has resurfaced during COVID-19 crisis. This group utilizes modern payloads and spoofed emails to target defense / government departments of Pakistan, to gain persistent access and sensitive information. Currently, this group is using military based COVID-19 themed emails with malicious links for further information that redirects the user to download a zip file which contains a malicious Ink (shortcut) file. Downloading and clicking the shortcut file, opens a legitimate document in foreground and executes malicious code in background that gives unauthorized access to the hacker.

3. Summary of Malicious Email.

- a. Email Subject. Pak Army Deployed in Country in Fight Against Coronavirus.
- b. Fake Email ID. Health Regulations and Coordination.
- c. Spoofed Email Address. Information_4@nih.mail-ntp.net
- d. Download Package. Pak_Army_Deployed_in_Country_Fight_Against_Coronavirus.zip
- e. Antivirus Detection Rate Nil/55
- f. File Size. 2.76 KB
- g. File Extension. Ink (Malicious Shortcut File)
- h. Download Address. http://www.d01fa.net/images/F1130F2D/16364/11542/b1296f5f/Pak_Army_Deployed_in_Country_Fight_Against_Coronavirus.zip
- i. Classification. State Sponsored Rattlesnake APT Malware

FBR eDOX Dy.No. 6405-R
Received in Chairman's Sectt
on 15 APR 2020 3

M(A)

M(I.T)

A.S

(Rev. Div)

Chief (IT)

15 APR 2020

SS(IT-3)

j. Reference Links.

- (1) <https://mp.weixin.qq.com/s/CZrdsIzEs4iwIaTzJH7Ubg>
- (2) <https://s.tencent.com/research/report/479.html>
- (3) <https://it.rising.com.cn/dongtai/19658.html>

4. C&C Servers

Ser	URL address	IP address	Remarks
a.	http://www.d01fa.net	5.181.156.24	Dropper C2 server
b.	https://cloud-apt.net	185.225.19.96	Communication C2 server

5. Indicators of Compromise

- a. C:\ProgramData\fontFiles\05qUyR4.tmp
- b. C:\ProgramData\fontFiles\Duser.dll (Malicious DLL)
- c. C:\ProgramData\fontFiles\rekeywiz.exe (Legitimate EFS REKEY Wizard)
- d. C:\ProgramData\fontFiles\rekeywiz.exe.config
- e. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\font (Persistence Key)

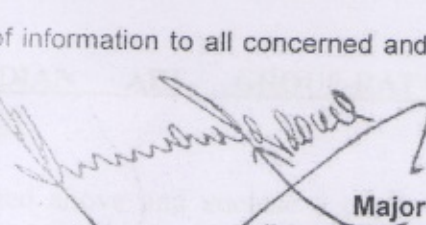
6. Capabilities of Malware

- a. Malware has capability to bypass antivirus and windows whitelisting.
- b. The malware is specially designed for targeted attacks and can stored document files, credentials, keys/SSL certificates and passwords.
- c. It can automatically execute itself on windows restart and every instance of this malware has extremely low detection rate.

7. Recommendations.

- a. Block execution of mshta.exe, wmic.exe, script.exe and wscript.exe on every system running in enterprise environment as this attack relies on free execution of mshta.exe
- b. Block execution of powershell encoded and malformed commands or block execution of windows powershell altogether.
- c. Implement strict Software Restriction Policies/Application Whitelisting to block executables running from %AppData%,*\StartMenu\Programs\Startup* and %TEMP% paths.
- d. Block execution of .hta, .vbs, .js, .jse scripts from enterprise environment.

- e. It is mandatory to enable 2 factor authentication on all your email accounts (Gmail, Yahoo, Hotmail etc), social media accounts (Facebook, Whatsapp etc) especially internet banking to prevent any sort of unauthorized access and financial loss.
- f. Regularly maintain and update antivirus solution from well reputed vendor like Kaspersky, AVAST, Avira etc.
8. Forwarded for perusal and dissemination of information to all concerned and under command, please.



Major
(Imran Nazir)
Assistant Secretary-I (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. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad