PTA CERT for Telecom Sector

Security Advisory-No: Ext:01/10-25

05, Oct 2018

Threat Classification: Malware

Overview: A cyber-attack has been identified targeting Pakistani nationals' especially private firms doing contracts with Pakistan Defense Forces.

Attack Methodology:

- Target individual receives a call from an unknown Pakistani number claiming to be a Pakistani government official/ Pakistan Armed Forces. Caller Officer Requests for details on defence related products being developed and provided to defence organizations.
- The caller (attacker) also refers to ongoing products provided by the firms to Pakistan defence organizations to establish credibility.
- Following initial telephonic conversation (on GSM and WhatsApp) emails containing malicious link are sent to the target.
- Downloading and opening the file from email executes the malware in the background and the system is compromised/hacked.
- Attackers are using fake domain names similar to existing official domains/ websites owned by Government Institutes to convince the recipient that the emails are sent by the actual government departments.

  Following are the observed fake domains:

  - **fbrgov.com**
  - **moitgovpk.com**
  - **fpmadgovpk.com**

Summary of Malicious Email:

- Subject: Malfunctioning of TI Sight TK 69
- Sender's Email: fatehgeeiani@gmail.com
- Malicious Link: http://sharefile.site
- Downloaded Document(s): sharedfile.coc
- Document Signature (MD5): 47E52A73F000CD0F3863A9CD17981F95

Technical Analysis of Malware:

a) **Exploit:** Attacker has used vulnerability in Microsoft Word (CVE-2017-8570) to Target the victim.

b) **Capabilities of Malware:** The malware uploads data including documents and files to C&C Server.

c) **Anti-Virus Detection**: The malware "winc.exe" is not detected by major Anti-Virus software.

(1) Detection Rate. 0/67

(2) Detection Percentage. 0

d) **Malicious Domains/ IPs:**

Ser #	Malicious URL	IP Address	Hosting Country
(1)	https://sharefile.site	**23.95.9.107**	United States
(2)	C&C Server	**193.22.98.226**	Ukraine

Indicators of Compromise:

a) **Created Files:** Malware drops 3 x files at location "**VoAppDatalLocallTemp".** following are the details:

i. "**winc.exe",** a malicious executable file with signature (MD5): **25d3508a5e887cfd7343e798d839ad5a.**

ii. "**LS4TJPBOIVOOY3A.sct",** a script used to run the executable.

iii. "**decoy.doc",** a blank document.

b) **Created processes:** Malware runs as "**winc.exe**" (32 Bit Application) and has a size of 6.4MB.

c) **Persistence:** The malware creates a file **"Win Setting Loader"** in windows startup folder.

Mitigation Methods:

Following mitigation measures are suggested:

a) Kill process "winc.exe" using Windows Task Manager.

b) Delete the following dropped files.

i. **"%AppData1Local1Templwinc.exe"**

ii. **"%AppDatMLocallTemplLS4TJPB01V00Y3A.sct"**

iii. **"1AppDatalRoaming1Microsoft1Windows1Start Menu1Programs1Startup1Win Setting Loader"**

c) Implement filters at the email gateway to filter out email with known indicators and block suspicious IP addresses at the firewall.

d) Formulate a policy regarding suspicious emails so that all suspicious emails should be reported to the security or IT department.

e) Provide employees basic cyber security awareness training.

Recommendations:

a) The following C&C Servers must be blocked in firewall of own network.

- https://sharefile.site
- 23.95.9.107
- 193.22.98.226

b) Do not respond to such fake telephone calls and avoid sharing details of products supplied to Pakistan Defence Forces.

c) Install and update licensed and well reputed ant viruses such as Kaspersky, Avira, Avast etc.

d) If any indicators of compromise found in the system, then disconnect the computer from the internet and re-install OS.

e) Update all software including windows OS, Microsoft Office etc.

f) Do not download attachments from emails unless you are sure about the source.

g) Discard emails received from ambiguous / fake domains, mentioned above.

h) In case of any incident, please report to this office.