

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

17 NOV 2020

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

Islamabad 13 Nov 2020

Subject: Advisory – Prevention Against Cyber Espionage (Bitter APT) (Advisory No. 23)

1. Bitter APT is a sophisticated cyber threat actor likely been active since 2014, both in desktop and mobile malware campaigns. Cyber threat posed by Bitter APT is spreading through **fake websites** and **applications** that are targeting civ / army / defense / intelligence organizations as well as DAs abroad in a well-planned targeted manner. The medium used acts as benign, however, it performs malicious processes in background that compromise victim's machine. Details are as under: -

- a. First Seen / Reported. 2014.
- b. Sponsor Country / State. India (likely).
- c. Motivation. Espionage / Data Theft.
- d. Target Sector. Govt organizations / officials.
- e. Malware Types / Target OS. Windows and Android.

2. Infection Vector. The infection vector of Bitter APT has following 5x categories: -

- a. Fake applications (list attached at **Annex-A**).
- b. Active malware distribution sites / urls websites (**Annex-B**).
- c. List of Command & Control domains / urls (**Annex-C**).
- d. Indicator of compromise (IoCs) identified (**Annex-D**).
- e. List of **associated applications** on **Google Playstore** with malicious correspondent (signed with same certificate) with BitterRAT (**Annex-E**). These applications currently do not have **data exfiltration capabilities**, however, the **APT threat group can easily weaponize them by delivering an update**. Such techniques have already been used by the APT Group in past.

3. Recommendations. Visiting fake website or installation of malicious application can compromise the entire network of an organization with **ransomware**, **data leakage** or **privilege escalation** exploits. Following prevention measures are recommended: -

- a. Websites
 - 1) Install well reputed antiviruses such as Kaspersky, Avira, Avast etc.

M(A)
M(I.T)

A.S
(Rev. Div)

Chief (IT)

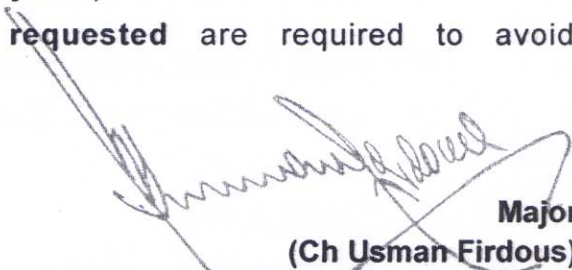
213045
Received in / Member (IT)
Date: 15/11/2020

2135245
Received in Chairman's Sect.

- 2) Regularly scan systems for software upgrades and security patches for Windows OS, Microsoft Office and all other on regular basis.
- 3) Check websites' URLs before entering any data and deploy web filter to block malicious websites (**Blocksi** extension filter for **Chrome**, **FoxFilter** for **Firefox**)

b. **Applications**

- (1) Regularly perform mobile phone updates.
- (2) **Uninstall** applications and software not in use.
- (3) Only required applications to be cautiously installed and used.
- (4) **Mobile security solutions COMODO app** etc to be installed along with other antivirus solutions and **data loss protection (DLP)** tools (**SolarWinds, CoSoSys** etc).
- (5) Ensure **Permissions requested** are required to avoid **privilege escalation**.


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

LIST OF KNOWN FAKE APPLICATIONS USED BY BITTER APT

Ser	Indicator of Compromise	APK/ Package Name
1.	6d3dcb9ad491628488feb9de6e092144	TruelIslam.apk com.nightstar.islam
2.	ea3b4cde5ef86acfe2971345a2d57cc0	voicemail.apk display.Launcher
3.	cbb32c303d06aa4d2dba713936e70f5c	PrivateChat.apk droid.pixels
4.	ee85b2657ca5a1798b645d61e8f5080c	ImageViewer360.apk com.secureImages.viewer.SlideShow
5.	692ff450aec14aca235cd92e6c52a960	ImageView.apk com.foldcr.imagec
6.	de931e107d293303dd1ee7e4776d4ec7	com.android.display
7.	d7c21a239999e055ef9a08a0e6207552	SaimaEidPics.apk com.google.settings
8.	9edf73b04609e7c3dada1f1807c11a33	WhatsAppActivation.apk com.youtube.dwld
9.	f92ed513fb83e7418654c4ee2a89bed5	Secure.ImageViewer Image_Viewer.apk
10.	d20c6731e278a1d3202b4caa0902afa8	google.comgooglesettings Dawn News Official.apk
11.	b0d55ccc06573230f2f74b9e85b5a6c9	com.nightstar.phoneshield
12.	0e1db2219402ec254b150a4f6d8b0b02	eu.blitz.conversations
13.	4987f36c8c90ef2075e41f8a2964754f	tool.calculator
14.	68f0fb35fa7ad061b621a6b4c48155b2	com.picture.guard.view

LIST OF ACTIVE MALWARE DISTRIBUTION SITES/ URLS

1. <http://www.gandharaart.org/images/IM/ImageViewer360.apk> (Android malware)
2. <http://spiceworld.rf.gd/Premium.php> (Android malware)
3. <http://www.gandharaart.org/news/lsasw> (Windows Malware)

LIST OF C&C DOMAINS/URLS

Ser	URL address	IP Address	Country
1.	flashnewsservice.org	94.46.187.223	UK
2.	blitzchatlog.ddns.net	23.83.133.67	US
3.	phoneshieldnet.com	Websites Currently Down	
4.	mypicks4u.com		
5.	playupdateapp.serveblog.net		
6.	btappclientsvc[.]net		
7.	v3solutions4all[.]com		
8.	cdaxpropsvc[.]net		
9.	http://blitzchatlog[.]ddns[.]net		
10.	http://techfront.com[.]cn		

