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.

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**.

Annex-A

LIST OF KNOWN FAKE APPLICATIONS USED BY BITTER APT

Ser	Indicator of Compromise	APK/ Package Name
1.	6d3dcb9ad491628488feb9de6e092144	TrueIslam.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.folder.image
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

Annex-B

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)

Annex-C

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	Websistes 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		

Annwx-D

INDICATOR OF COMPROMISE

Ser	Indicator of Compromise	Description
1.	82.221.129[.]17	Shared hosting server with multiple suspicious and phishing sites
2.	185.27.134.139	Shared hosting server with multiple suspicious and phishing sites
3.	6d3dcb9ad491628488feb9de6e092144	TrueIslam.apk com.nightstar.islam
4.	ea3b4cde5ef86acfe2971345a2d57cc0	voicemail.apk display.Launcher
5.	cbb32c303d06aa4d2dba713936e70f5c	PrivateChat.apk droid.pixels
6.	ee85b2657ca5a1798b645d61e8f5080c	ImageViewer360.apk com.secureImages.viewer.SlideShow
7.	692ff450aec14aca235cd92e6c52a960	ImageView.apk com.folder.image
8.	de931e107d293303dd1ee7e4776d4ec7	com.android.display
9.	d7c21a239999e055ef9a08a0e6207552	SaimaEidPics.apk com.google.settings
10.	9edf73b04609e7c3dada1f1807c11a33	WhatsAppActivation.apk com.youtube.dwld
11.	f92ed513fb83e7418654c4ee2a89bed5	Secure.ImageViewer Image_Viewer.apk
12.	d20c6731e278a1d3202b4caa0902afa8	google.comgooglesettings Dawn News Official.apk
13.	b0d55ccc06573230f2f74b9e85b5a6c9	com.nightstar.phoneshield
14.	0e1db2219402ec254b150a4f6d8b0b02	eu.blitz.conversations
15.	4987f36c8c90ef2075e41f8a2964754f	tool.calculator
16.	68f0fb35fa7ad061b621a6b4c48155b2	com.picture.guard.view
17.	8aff67a6b4f3e398b912f8405beb5319	Bitter APKS
18.	448b8af1a6757aa5b827b382777ab3de	
19.	42c2d7aeb8a98df09c624a9605849927	
20.	1d2e23effc225880cadb7ee56dff25cf	
21.	82.221.129[.]18	Shared hosting server with multiple suspicious and phishing sites
22.	82.221.129[.]19	Shared hosting server with multiple suspicious and phishing sites

23.	94.156.175[.]61	Shared hosting server with multiple suspicious and phishing sites
24.	btappclientsvc[.]net	Malicious domain
25.	winmanagerservice[.]org	Malicious domain
26.	winmanagerservice[.]net	Malicious Domain
27.	v3solutions4all[.]com	Malicious Domain
28.	cdaxpropsvc[.]net	Malicious Domain
29.	wangluojiumingjingli[.]org	Malicious Domain
30.	mail.btappclientsvc.net	The mail server for the malicious domain btappclientsvc[.]net
31.	maill.catic.cn.accountvalidation.verifay.ysfts69887tgyu67tg6r.com.btappclientsvc.net	Phishing site mimicking the China National Aero-Technology Import & Export Corporation (CATIC)
32.	maill.ndrc.gov.cn.accountvalidation.verifay.vhj876uh786uy687.com.btappclientsvc.net	Phishing site mimicking the China National Development and Reform Commission (NDRC)
33.	mailll.mfa.gov.cn.accountvalidation.verifay.jk78huy688h67kjg7it8.com.btappclientsvc.net	Phishing site mimicking the China Ministry of Foreign Affairs
34.	mail.v3solutions4all.com	The mail server for the malicious domain v3solutions4all[.]org
35.	maill.catic.cn.accountverify.validation8u2745.v3solutions4all.com	Phishing site mimicking the China National Aero-Technology Import & Export Corporation (CATIC)
36.	maill.ceiec.cn.accountverify.validation7h8k97hnku0j.com.v3solutions4all.com	Phishing site mimicking the China National Electronics Import & Export Corporation (CEIEC)
37.	maill.mfa.gov.cn.accountverify.validationgyy837rgyud2378rry.com.v3solutions4all.com	Phishing site mimicking the Ministry of Foreign Affairs
38.	mail.winmanagerservice.org	The mail server for the malicious domain winmanagerservice[.]org
39.	maill.126.com.cn.accountvalidation.vj65rfy785ru76.com.winmanagerservice.org	Phishing site mimicking 126[.]com, is a popular email provide in China.
40.	maill.163.com.cn.accountvalidation.bh34567gh67.com.winmanagerservice.org	Phishing site mimicking 163[.]com, which is NetEase; an internet services company including email.

41.	maill.catic.cn.accountverify.validation567fg57f58g6.com.winmanagerservice.org	Phishing site mimicking the China National Aero-Technology Import & Export Corporation (CATIC)
42.	maill.mfa.gov.cn.accountverify.validation8u77654.winmanagerservice.org	Phishing site mimicking the Ministry of Foreign Affairs
43.	maill.polyauction.com.accountvalidation.security.jjh98iukhuj78.com.winmanagerservice.org	Phishing site mimicking the Poly Auction House. Beijing Poly International Auction, a subsidiary of Poly Culture Group Corp Ltd., is China's largest state-owned auction house and holds the highest auction transaction volume of Chinese art in the world.
44.	maill.mfa.gov.cn.accountverify.validation8u77654.winmanagerservice[.]org	Phishing site mimicking the Ministry of Foreign Affairs
45.	webmail.avic.com.accountverify.validation8u7329.jsbchk82056.nxjkgdgf34523.fghe5103.ncdjkbfkjh5674e.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd75894t5.njfg87543.kdjsdkj7564.jdchjsdy.rthfgyerty86.wangluojiumingjingli.org	Phishing site mimicking the Aviation Industry Corporation of China (AVIC)
46.	webmail.mofcom.gov.cn.accountverify.validation8u2904.jsbchkufd546.nxjkgdgfhh345s.fghese4.ncdjkbfkjh244e.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd75894t5.njfg87543.kdjsdkj7564.jdchjsdy.rthfgyerty33.wangluojiumingjingli.org	Phishing site mimicking the Ministry of Commerce (MOFCOM)
47.	maill.sasac.gov.cn.accountverify.validation8u6453.jsbch876452.nxjkgdg096574.fghe5392.ncdjkbfkj873e65.nckjdbcj86hty1.cdjcksdcuh57hgy43.njkd8766532.njfg73452.kdjsdkj7564.jdchjsdy.rthfgyert231.winmanagerservice[.]net.	Phishing site mimicking the State-owned Assets Supervision and Administration Commission of the State Council (SASAC)
48.	maill.catic.cn.accountvalidation.verifay783g677	Phishing site mimicking the China National Aero-Technology Import & Export Corporation (CATIC)

	hui.com.cdaxpropsvc.net	
49.	maill.cgwic.com.accountvalidation.verifay765hgy87.com.cdaxpropsvc.net	Phishing site mimicking the China Great Wall Industry Corporation(CGWIC)
50.	maill.cnnc.com.cn.accountvalidation.verifay2367bdg56.com.cdaxpropsvc.net	Phishing site mimicking the China National Nuclear Corporation (CNNC)
51.	maill.czec.com.cn.accountvalidation.verifay728gh4dgy6378et6.com.cdaxpropsvc.net	Phishing site mimicking the China Zhongyuan Engineering Corp (CZEC)
52.	maill.163.com.accountvalidation.verifay768ht7u6h.com.cdaxpropsvc.net	Phishing site mimicking 163[.]com, which is NetEase; an internet services company in China including email.
53.	325ece940de9fb486ef83b680ad00d385b64e435923d1bbc19cbcf33e220c2a2	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain btappclientsvc[.]net
54.	6a10a699f0ef084f5070968ae3cc35075990778bf82dca7e0477eeaebbee4eb1	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain winmanagerservice[.]org
55.	5538badac0221b42f457920802b23ebd8ccf2c64b1fb827cd6458a7f9de2c6de	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain winmanagerservice[.]org
56.	940a1bd16be51cd264ee7e315841b8aa0b0b86d3392d4d08ca00151f01a5cd28	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain v3solutions4all[.]com
57.	823f85eb6d3465145bb34e570b870e39001c4ec61f7ca325f88a23edee75654f	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain v3solutions4all[.]com
58.	f456f2a2802242e1404ef9a586366820c4bd7f7f3b113209d56fc34dee2d75bf	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain v3solutions4all[.]com
59.	7bc4f48a4345f4a47dabbf686a714d3e4c9af9d9f26e73ca873f54a4f164b732	Serial number for Let's Encrypt SSL/TLS Certificate installed on the malicious server used to target the government of China - sites ending in domain v3solutions4all[.]com
60.	techslogonserver[a]gmail[.]com	Registrant details: Yadavan Krishnan, LogonServer Technologies, +91.9994984807, 2/136, Sendraya Gownder Street Alagapuram Salem Tamil Nadu 636016 IN

Annex- E

LIST OF ASSOCIATED APPLICATION GOOGLE PLAYSTORE

Ser	Application	APK/ Package Name
1.	CalendarSlide	com.picture.guard.view
2.	ZeroCross	eu.blitz.conversation
3.	AlarmClockSlide	com.clocknews.update
4.	CalculatorTool	Tool.calculator