**Cyber Security Advisories**

**Date: 17 June 2024**

1. **CMTX-I-514052024: Threat Actors using Google Drive Based Services for Data Exfiltration**

Threat actors have been found abusing legitimate cloud based services such as Google drive, where the data on the compromised system is being exfiltrated. Hence, the network administrators are advised to monitor traffic towards domain: oauth2.googleapis.com and thereby identify the original process communicating. If the process is not legitimate/ user originated then kindly sanitize the system and network. IOCs associated with this malware campaign are as follows:

- ------------------------<SHA1 Hashes>-----------------------

549d80d0d2c3e2cf3ea530f37bfc0b9fe0cbd5f4

88fd8d71d879257b6cbf2bc12b6493771b26d8a0

60f1f06e4022f03569364e625f3db93524c16c9c

bae49f050b10aa68e67d147b0c5b9d7df8fb2ab5

0be52aa4bfd0acf26e5e06157a995bd343d5c2a0

- ---------------------- </SHA1 Hashes> ----------------------

Additional domains for other cloud/ API services to be MONITORED for malware exhibiting similar TTPs:

- ---------------<Domains>---------------

api.telegram.org

telegram.org

discord.com

discord.com/api/

api.slack.com

slack.com

api.dropboxapi.com

dropboxapi.com

api.dropbox.com

dropbox.com

- ---------------</Domains>--------------

1. **CMTX-I-200052024: CrimsonRAT - APT36 campaign**

Recent C&C server IP of CrimsonRAT malware used by Pakistan based threat actors to target government officials are as follows:

- ----------- <C&C IP> -----------

178.238.228.113

- ----------- </C&C IP> ----------

Kindly take the required actions.

1. **CMTX-I-040052024: SpyNote - APT36 Campaign**

Recent C&C server domains of SpyNote malware used by Pakistan based threat actors to target government officials are as follows:

- -----------<C&C Domains>-----------

server-chat1.chatindian.xyz

server-chat.chatindian.xyz

server.chatindian.xyz

\*.chatindian.xyz

- -----------</C&C Domains>----------

Kindly take the required actions.

1. **CMTX-P062024726: QuasarRAT Malware ALERT 54**

ALERT BRIEF:

Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely used by nation sponsored threat actors. Quasar RAT has capability of capturing screenshots, Key logger, gather System Information, remote Shell and Command execution, reversing proxy, Managing tasks and files, Configuring and building client executables.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP ADDRESSES

94.156.68.4

141.98.7.175

111.173.106.171

136.244.92.105

89.117.145.5

141.98.7.199

179.97.173.22

194.163.162.213

117.18.7.76

92.130.254.189

185.234.72.39

94.156.67.218

181.214.221.49

91.225.219.120

188.214.129.20

141.98.7.201

70.36.117.155

2.58.15.111

141.98.7.198

91.92.250.225

141.98.7.186

37.97.36.121

141.98.7.176

141.98.7.188

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P062024405: PLUGX RAT ALERT 120**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP Address

172.111.148.109

45.152.67.209

172.111.233.96

16.163.145.17

38.55.97.118

195.234.62.137

103.107.105.49

38.60.208.232

61.246.106.46

45.152.67.209

45.152.67.209

38.60.208.232

172.111.148.109

16.163.145.17

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P-062024015: Asylum Ambuscade Group**

Alert Brief:

Asylum Ambuscade is a cybercrime group engage in cyber espionage operations against government entities .The group used spear phishing emails to access the victim’s systems. The email contained attachments in the form of documents embedded with obfuscated Visual Basic Script (VBScript) and JavaScript files.

They have been observed using various tools such as SunSeed LUA script, WasabiSeed VBS and NODEBOT (JavaScript malware designed to bypass anti-virus software detections). with the help of SunSeed Asylum Ambuscade perform the following actions:

1. Deliver Cobalt Strike for post-compromise activities and an undisclosed remote access Trojan (RAT).

2. Take screenshots and log keystrokes, Gather the victim host and Active Directory information via Windows Management Instrumentation (WMI) queries.

3. Download and install hidden virtual network computing (hVNC). HVNC allowed Asylum Ambuscade to open a hidden instance in the form of a virtual desktop and control it covertly instead of taking over the victim's desktop.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASH

7fdb9a73b3f13dbd94d392132d896a5328daca59

ad8143de4fc609608d8925478fd8ea3cd9a37c5d

3e38d54cc55a48a3377a7e6a0800b09f2e281978

7f8742778fc848a6fbcffec9011b477402544171

557c5150a44f607ec4e7f4d0c0ed8ee6e9d12adf

7aa23e871e796f89c465537e6ece962412cda636

f85b82805c6204f34db0858e2f04da9f620a0277

441369397d0f8db755282739a05cb4cf52113c40

c98061592de61e34da280ab179465580947890de

384961e19624437eb4eb22b1bf45953d7147fb8f

d24a9c8a57c08d668f7d4a5b96fb7b5ba89d74c3

7db446b95d5198330b2b25e4ba6429c57942cfc9

5492061de582e71b2a5da046536d4150f6f497f1

57157c5d3c1bb3eb3e86b24b1f4240c867a5e94f

519e388182de055902c656b2d95ccf265a96ceab

29604997030752919ea42b6d6cee8d3ae28f527e

117ecfa95be19d5cf135a27aed786c98ec8ce50b

d5f8acad643ee8e1d33d184daea0c8ea8e7fd6f8

c554100c15ed3617ebfaab00c983ced5fec5db11

95edc096000c5b8da7c8f93867f736928ea32575

f2948c27f044fc6fb4849332657801f78c0f7d5e

ee1cfedd75cba9028904c759740725e855aa46b5

64f5ac9f0c6c12f2a48a1cb941847b0662734fbf

a9e3acfe029e3a80372c0bb6b7c500531d09edbe

62fa77daef21772d599f2dc17dbba0906b51f2d9

2b42fd41a1c8ac12221857dd2df93164a71b95d7

ac3afd14ad1aea9e77a84c84022b4022df1fc88b

7a78af75841c2a8d8a5929c214f08eb92739e9cb

5f67279c195f5e8a35a24cbea76e25bad6ab6e8e

Domain

snowzet.com

IP

91.92.246.117

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOCs END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-I-050152024: Malicious Domains used by APT Threat Actors**

In continuation to an earlier alerts CMTX-I-040152024, CMTX-I-050152024 dated 04th June, 2024 and 05th June, 2024 respectively additional malicious domains that are being used by APT threat actors are as follows:

- ----------<Malicious Domains>-----------

nicdsa.estttsec.in

nicgov.estttsec.in

indiangov.estttsec.in

rcilab.estttsec.in

iai.estttsec.in

server.estttsec.in

drdl-drdo.estttsec.in

bcci-gov.estttsec.in

drdl-drdo.estttsec.in

wind.estttsec.in

windows.estttsec.in

apsdigi.estttsec.in

csdindia-gov.sharesync.in

csdindia.sharesync.in

\*.sharesync.in

\*. estttsec.in

- ----------</Malicious Domains>-----------

1. **CMTX-I-040152024: Malicious Domains used by APT Threat Actors**

Following malicious domains are being used by APT threat actors to host malicious code/malware :

- -------<Malicious Domains>-------

basesoft.pcdapune.cloud

server.coordoffice.cloud

backup.eci-india.cloud

eci-india.cloud

mea-india.cloud

pcdapune.cloud

coordoffice.cloud

- -------</Malicious Domains>-------

1. **CMTX-I-050152024: Malicious Domains used by APT Threat Actors**

- ----------<Malicious Domains>-----------

bsnl.coordoffice.cloud

coordoffice.servefile.cloud

bsnl.servefile.cloud

backup.eci-india.cloud

winsoft.apsindia.cloud

adisharma.servefile.cloud

backup.servefile.cloud

lap2.timesofindia.cloud

lahp.timesofindia.cloud

backup.timesofindia.cloud

backup1.timesofindia.cloud

mea-india.winsoft.cloud

www.csdindia.cloud

nic1.csdindia.cloud

apply.csdindia.cloud

nic.csdindia.cloud

rcilab.awwa-gov.cloud

backup.awwa-gov.cloud

eci-india.windb.cloud

ipl.windb.cloud

\*.servefile.cloud

\*.eci-india.cloud

\*.timesofindia.cloud

\*.csdindia.cloud

\*.windb.cloud

\*.winsoft.cloud

\*.apsindia.cloud

\*.awwa-gov.cloud

\*.coordoffice.cloud

- -----------</Malicious Domains> -----------

1. **CMTX-I-050152024: Malicious Domains used by APT Threat Actors**

In continuation to an earlier alerts CMTX-I-040152024, CMTX-I-050152024 dated 04th June, 2024 and 05th June, 2024 respectively additional malicious domains that are being used by APT threat actors are as follows:

- ----------<Malicious Domains>-----------

nicdsa.estttsec.in

nicgov.estttsec.in

indiangov.estttsec.in

rcilab.estttsec.in

iai.estttsec.in

server.estttsec.in

drdl-drdo.estttsec.in

bcci-gov.estttsec.in

drdl-drdo.estttsec.in

wind.estttsec.in

windows.estttsec.in

apsdigi.estttsec.in

csdindia-gov.sharesync.in

csdindia.sharesync.in

\*.sharesync.in

\*. estttsec.in

- ----------</Malicious Domains>-----------

1. **CMTX-I-445062024: Mythic Malware - APT36 campaign**

Following IOCs (C2, malware hosting and malware deployment) are associated with Mythic Malware. This RAT is being used by the Pakistan based APT36 group to target Linux based systems in government offices.

- -----------------<IOCs>---------------

165.22.221.71

178.128.166.148

152.42.162.105

161.35.207.209

server.coordoffice.cloud

official-mail.in

iaf-coord.in

ftp.iaf-coord.in

infodesk-wing.in

- ----------------</IOCs>----------------

1. **CMTX-I-053062024: Recent IOCs of Chinese Malware Campaign**

Following domains are associated with China based malware campaign targeting government sector for espionage:

- ------------------------<IOCs>------------------------

docsgoogle.z7.web.core.windows.net

flaworkcomp.com

epsross.com

- ---------------------- </IOCs> ------------------------

1. **CMTX-I-004002024: Domains associated with ReverseRAT Malware**

Following domains have been found to be associated with ReverseRAT malware:

- --------------<Malicious Domains>-------------

0mn3d6yunkn0wn.com

22446688.duckdns.org

albert1.zapto.org

albert2.zapto.org

alt.epicip.info

axl24.dyndns-ip.com

axl24.no-ip.org

bcssecurecloud.com

bunny.no-ip.org

clone.epicip.info

cricket.bounceme.net

energtest.no-ip.info

givemeyourmoney.zapto.org

ihatepakistan.no-ip.info

iloveratss.no-ip.org

kinky82.zapto.org

m106072137032.v4.enabler.ne.jp

mdec.nelreports.net

mx4097sec.bcssecurecloud.com

newbiecss.no-ip.org

pivi.no-ip.biz

xegroups.com

- --------------</Malicious Domains>-------------

1. **CMTX-I-022062024: CrimsonRAT - APT36 campaign**

Recent C&C server IP of CrimsonRAT malware used by Pakistan based threat actors (APT36) to target government officials are as follows:

- ----------- <C&C IP> -----------

193.142.59.109

- ----------- </C&C IP> ----------

Kindly take the required actions.

1. **CMTX-P062024985: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP Address

141.95.127.48

38.60.217.160

139.59.90.69

141.95.127.48

141.95.127.48

38.60.217.160

139.59.90.69

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P062024995: SHADOWPAD Malware**

ALERT BRIEF:

Shadow pad, known as a Modular cyber-attack tool used by Chinese linked APT groups (APT41/Barium, APT10/Stone Panda, TONTO Team, APT27/Emissary Panda, APT15, Winnti Group, REDECHO)

A list of Indicators of compromise is provided below for your action side.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP Address

89.38.128.94

207.148.120.31

38.60.199.119

152.32.155.25

45.76.165.217

38.54.96.34

202.181.26.247

202.181.26.247

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P062024505: PLUGX RAT ALERT 121**

ALERT BRIEF:

PlugX RAT -reportedly used by Chinese State actors- a modular remote access trojan capable of uploading, downloading, and modifying files, keystroke logging, webcam control and accessing a remote cmd.exe shell. The RAT has a previous history of being known for its strong encryption, configuration and persistence techniques using side loading techniques for initial infection with Genuine and trusted executable. CERT-In has been communicating and sharing actionable threat intelligence.

A list of Indicators of compromise is provided below for yours action side.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP Address

156.59.183.241

47.243.198.15

52.77.42.172

194.124.33.235

110.173.49.212

172.111.233.12

216.118.234.158

202.144.192.146

154.219.2.142

45.92.70.108

38.89.72.192

156.59.183.241

45.92.70.108

154.219.2.142

52.77.42.172

154.219.2.142

156.59.183.241

45.92.70.108

52.77.42.172

47.243.198.15

47.243.198.15

156.59.183.241

202.144.192.146

47.243.198.15

47.243.198.15

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-P062024025: Cyber Espionage by Chinese Threat Actors**

ALERT BRIEF:

PREVIOUS REFERENCE:[CMTX-P032023116] Mustang Panda activity, TLP: AMBER (Dated 07/03/2023)

Motivation - Cyber Espionage

Aliases: Mustang Panda, BRONZE PRESIDENT, HoneyMyte, Vertigo Panda, Red Delta,

Temp.Hex, Twill Typhoon, TA416

It has been observed that Chinese threat actors targeted govt entities in cyber espionage operations. The initial attack vector starts by employing Microsoft Management Console Snap-in Control (.msc) files that runs a PowerShell command to download a Windows installer (MSI) file. The MSI filedrops a legitimate executable, a malicious loader DLL (written in Nim), and an encrypted payload. This leads to loading PlugX backdoor via DLL search order hijacking.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

HASHES

1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292

54549745868b27f5e533a99b3c10f29bc5504d01bd0792568f2ad1569625b1fd

d4b9f7c167bc69471baf9e18afd924cf9583b12eee0f088c98abfc55efd77617

288e79407daae7ae9483ef789d035d464cf878a611db453675ba1a2f6beb1a03

51d38688ae91d2f1dd91a042861073491989b2cbcd4a85ab6ff92948c2d1ddf9

e22618a90338feba0a109d029e25ebb95de8f3a472c9a208b1ca3c0dc68126cc

65f4208e7335b4a3c5f091a7801420b3e7b3fe5d774357dec2198200f369bc2a

8c9e1f17e82369d857e5bf3c41f0609b1e75fd5a4080634bc8ae7291ebe2186c

0c56d0b8780a7b3c50b6e79dab9cc36f726a65fd5baf6c49352d91084afaee6e

711d1e6a3045d7c81cd9e9b005e5571f4f3e31c1a7d387634b6826372fbdde75

DOMAINS:

buyinginfo.org

calgarycarfinancing.com

epsross.com

flaworkcomp.com

getupdates.net

indiinfo.com

inhller.com

iplanforamerica.com

lebohdc.com

londonisthereason.com

shreyaninfotech.com

truckingaccidentattorneyblog.com

versaillesinfo.com

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-I-025062024: Malicious Domains - Spear-Phishing Campaign**

Following malicious subdomain and the parent domain are associated with spear-phishing campaign targeting government officials:

- ----------------<Malicious Domain>----------------

cbigovin.top

mailgov.in.net

webmail.mailgov.in.net

mail.mailgov.in.net

- --------------</Malicious Domain>-----------------

Kindly take the required actions.

1. **CMTX-I-443062024: Malicious Domains - Spear-Phishing Campaign**

Following malicious subdomain and the parent domains are associated with spear-phishing campaign targeting government officials:

- ----------------<Malicious Domain>----------------

www.nia.gov.in.deputation.info

nia.gov.in.deputation.info

deputation.info

www.nia.gov.in.incidentreports.info

nia.gov.in.incidentreports.info

incidentreports.info

- --------------</Malicious Domain>-----------------

Kindly take the required actions.

1. **CMTX-I-080062024: SideCopy - C&C of Malware Campaign**

Following IOCs are associated with SideCopy malware campaign.

- ----------------------------- <IOCs> -------------------------

utkalsevasamitikanjurmarg.in (compromised domain)

defender.windowupdatecache.in

office.windowupdatecache.in

\*.windowupdatecache.in

- ---------------------------- </IOCs> -------------------------

Kindly take the required actions.

1. **CMTX-I-808062024: Malicious Domains - Spear-Phishing Campaign**

Following malicious domains are associated with spear-phishing campaign targeting government officials:

- --------<Malicious Domain>--------

adm-wing.in

branch-admin.in

coord-wing.in

- --------</Malicious Domain>-------

Kindly take the required actions.

1. **CMTX-I-543062024: Malicious Domains - Spear-Phishing Campaign**

The following sub-domain and parent domain are malicious and associated with spear-phishing campaign targeting government officials:

- --------<Malicious Domain>--------

email.niccert.site

niccert.site

- --------</Malicious Domain>-------

Kindly take the required actions.

1. **CMTX-P062024018: REDLINE STEALER MALWARE**

ALERT BRIEF:

RedLine Stealer is a .NET-based infostealer malware that is capable of harvesting information from browsers such as saved credentials,

autocomplete data and credit card information. It is also utilized in facilitating attacker to drop another payload or launch a hidden command shell on victims' machine.

A list of Indicators of compromise is provided below for the necessary action.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP

147.78.103.101

149.28.222.15

185.222.58.87

188.127.247.28

193.233.255.34

43.155.163.53

80.66.81.218

80.66.81.219

80.66.81.220

94.156.8.28

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*