**Cyber Security Advisories**

**Date: 28 June 2024**

1. **CMTX-I-338062024: SideCopy - IOCs of Malware Campaign**

Following IOCs are associated with SideCopy malware campaign.

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

dipl.site

\*dipl.site

84.247.170.237

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

1. **CMTX-P062024605: PLUGX RAT ALERT 122**

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

172.247.109.146

180.178.47.20

180.178.47.18

202.144.192.46

2.58.14.121

180.178.47.19

180.178.47.22

192.248.191.48

180.178.47.21

180.178.47.20

202.144.192.46

202.144.192.46

180.178.47.21

180.178.47.19

180.178.47.19

202.144.192.46

172.247.109.146

180.178.47.18

180.178.47.20

180.178.47.22

180.178.47.18

172.247.109.146

180.178.47.18

180.178.47.22

172.247.109.146

180.178.47.18

180.178.47.22

180.178.47.18

180.178.47.20

172.111.233.43

180.178.47.19

180.178.47.21

180.178.47.21

180.178.47.21

180.178.47.18

149.104.1.160

180.178.47.19

180.178.47.20

96.43.101.229

180.178.47.22

180.178.47.20

172.247.109.146

180.178.47.22

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

1. **CMTX-P062024105: 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

202.181.26.17

158.247.199.18

149.28.149.7

103.85.25.16

158.247.199.18

158.247.199.18

202.181.26.17

139.84.163.18

202.181.26.17

202.181.26.17

202.181.26.17

158.247.199.18

202.181.26.17

158.247.199.18

202.181.26.17

202.181.26.17

202.181.26.17

103.85.25.16

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

1. **CMTX-P062024736: QuasarRAT Malware**

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

62.60.210.205

31.177.108.29

45.10.154.41

181.162.129.89

103.98.150.248

175.24.180.72

107.148.63.166

172.81.60.16

187.59.75.234

91.92.137.232

106.14.242.206

91.92.255.149

45.32.27.169

200.90.84.150

154.82.77.6

185.208.158.208

106.54.209.24

91.92.255.74

5.180.155.40

190.205.229.226

185.113.8.243

222.239.101.21

45.85.250.180

213.152.186.163

177.53.150.41

94.228.166.40

80.94.92.120

124.188.91.165

149.28.215.217

38.180.9.93

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

1. **CMTX-P062024045: Circulation of Phishing email contain links to counterfeit CERT-In websites**

ALERT BRIEF:

It has been reported that threat actors are currently circulating phishing emails with themes such as "Pakistan's Dark Secrets Revealed" and "Ex-Pak soldier exposes Honey Trapping plot." These malicious emails include links to counterfeit CERT-In websites hosting content related to these themes. In previous campaigns, similar tactics involved the use of fake websites impersonating reputable organizations to target users for purposes like malware deployment and credential theft. Therefore, organizations are strongly advised to remain vigilant against such deceptive practices.

Rcommendation:-

- - Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header). Block attachments of file types: [exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf].Ensure to scan all software downloaded from the Internet prior to executing. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).Before entering sensitive information on a website, check the URL for inconsistencies or suspicious elements. Ensure it uses HTTPS and matches the official domain.

- - Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent to prevent e-mail spoofing. This will prevent malicious mails to reach your corporate mailboxes. Always verify the sender's email address and domain. Be cautious of emails from unfamiliar or suspicious addresses.

- - Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known. Monitor users' web browsing habits; restrict access to sites with unfavourable content.

- - Promptly report any suspicious emails upon detection to incident@cert-in.org.in with detailed information like Sender's email address (including any spoofed or suspicious elements), Subject line of the email, Date and time of receipt and any attachments or links included in the email. Forward the mail as an attachment to preserve email headers and other critical metadata.

1. **CMTX-I-345062024: Malicious Domains - Spear-Phishing Campaign**

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

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

email.gov.in.parichay.online

email.gov.in.estbsec.in

email.estbsec.in

email.parichay.online

email.apsdelhicantt.in

email.emailnic-tech.email

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

Kindly take the required actions.

1. **CMTX-P062024065: Velvet ant Threat Actor**

ALERT BRIEF:

According to the reports, a new China linked threat actor group called "Velvet Ant" is active in the cyber threat landscape. The threat actor tried to exploit the vulnerable F5 BIG-IP (which is a network device widely used for load balancing and application delivery) to gain control over a system and maintain access (persistence) and also to exfilterate data. Threat group utilizes the backdoor PlugX (also known as Korplug) in espionage operations.

Toolset Used by Velvet Ant:

VELVETSTING: This tool is used for connecting to the threat actor's Command and Control (C&C) server and executing commands. It likely facilitates remote control and data exfiltration.

VELVETTAP: Designed for capturing network packets, this tool enables the threat actors to monitor and intercept network communications, potentially extracting sensitive information.

SAMRID: Identified as an open-source SOCKS proxy tunneller available on GitHub. This tool could be used by Velvet Ant to anonymize their network traffic or evade detection while maintaining communication with their infrastructure.

ESRDE: Similar to VELVETSTING but uses bash instead of csh (C shell). This tool likely serves a similar purpose in terms of command execution and control.

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

HASHES:

91f6547bceddfb2f241570ac82c00de700e311e4a38dea60d8619638f1ed3520

d663b323d132a3c811bb53a48a686ea85c6bf8faeef3b48dfa93528be8f4133b

9a7a24b1c785b3c7c39f7e33e99897290165693dea1f46ed4f3c7919aef93928

75fa71e65344b61a80f0e598349b735912be39d04a7e2159748423bd860d3454

be852d7a59ba168d93eb975fbed652617046433e6fdc177d0087331f9a095f02

0acc25396ef78c00631c64df538678a323982115bafbfa7487a4370d4b4129ac

859c823eb3e7420e0db234ba224764faa62d391bddd25e9ad415b11d853741f9

9b9d2da73b510276d38d1698f3b87671958e338b40230e6a004ccaf3dcceb03b

b4d71b0ac0bc1495789501f9afce6f950b601a36c0836534294640f2db6b2f40

3a6a5b1d76dfcac5920e6e9163c08543304ba013425eb2c2e64071b15d26996e

bdf8a8c7f0298484dc95895dbddf367689ca361618453597129343838b94debb

7c9336afd7530576b6a0f2e978b36955e8f264fee429d810309ce157a4918aaa

c456747731141c2ea0f8e69f89193e8bb823da4667527fe90b614b97f1d425ae

55d6c4a95b5172ea47381ab66ea9ea37fa0afb53b9bb10a1d752ac4acc8f6cd4

527df166af23cd0d139ebad9d219f125137b5a7b619fa50e5e245ccaf8c0b7d6

4965f809b71ffb71fe8456d88dcd0a80a99fa6aa4ffd6ba96e1a1d810d41bbd0

b5aa86fd97624a317945d110541a07fc80b83dd960fbf16642720fc275d8f04f

9092cdd52109531f9f58c28bda25b0c3f82d9bd2d261ce5fcb0137873dbb0868

bcbc3184756a6cacfd5ca2b879708cfd015e84050c9b9ede096cfb70282f870c

febe116a87860e42bbcfd7c6e2c710446f33bdacc56e990f69493837c01f1059

7e118a6c4d6f162d8c6a53faf972bd3e675da7f9d0a0b67a1988b4e2102ebb53

cc48a02f06066a37c90d063b6d28ae17d9503e4ba6df69aef1b55b5fa5a5ff48

562974ea1325a88c916a55719fb9263eb6c710ba281fdee4ba7e9a98a3f4a5a8

92b2535373e55b16b6f3b2d134a1d5545e837d3c19fff4cead4e92558e302b6e

a9556cc05422cae960e36f76eeff7168b8e3cfeb16a20855a93d4f2ed4a65a8b

821d0cdc3e8a735976045ecb1afd1c0170bf39701d2da118b9533a45383a9ebe

436f35dc69bbe7cb8cf5430b52c3aedace099730245de57e004dc1f6531ae262

13f3c05cc348ecb47c4e86d1fb522fdf499a6fb23e0cc6370f4618137f055b04

3d9aaac0a8e5c7eadd79d8d5c16119d04f4e9db7107fc44a1e32a8746a1ec375

IPs

202.61.136.158

103.138.13.31

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

1. **CMTX-P062024028: RACCOON MALWARE**

ALERT BRIEF:

CERT-IN has been tracking prominent RATs/malware families. An uprise in activities associated with raccoon malware is reported. Raccoon is an info stealer malware available as a Malware as a Service. Raccoon malware has capability to check system settings, capture screenshots, collect basic information like OS version, IP and username and steal passwords and logins from a variety of browsers.

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

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

IPs

77.91.77.116

77.91.77.137

77.91.77.54

77.91.77.96

79.133.51.249

86.106.119.113

89.38.135.28

94.228.166.22

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

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

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

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

cbigovin.site

cbigovins.top

cbigovin.top

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

Kindly take the required actions.

1. **CMTX-I-338062024: SideCopy - IOCs of Malware Campaign**

The following IOCs are associated with Pakistan based SideCopy malware campaign:

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

190.2.131.195

http://checkip.dyndns.org/ (non-malicious as such, but used for

checking the public IP of the infected system)

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

Kindly take the required actions.

1. **CMTX-P062024055: CRITICAL VULNERABILITY (CVE-2024-30103) AFFECTING MICROSOFT OUTLOOK**

ALERT BRIEF:

CVE-2024-30103

CVSS-8.8

Affected Products: Microsoft Outlook, Microsoft Exchange Server, and Microsoft Office.

A critical-severity vulnerability, tracked as CVE-2024-30103 is affecting Microsoft Outlook. This zero-click remote code execution (RCE) flaw arises from Outlook's mishandling of specific email content. When a recipient opens a specially designed email containing malicious code, the exploit is triggered, allowing attackers to run arbitrary code potentially leading to unauthorized access, data theft, and system compromise.

Recommendations:

\* As vulnerability has its potential for exploitation by threat actors targeting Outlook clients, it is crucial to prioritize patching this vulnerability promptly to mitigate the risk of potential cyberattacks on company assets

References:-

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30103

https://ironscales.com/blog/zero-click-critical-microsoft-outlook-vulnerability.-what-you-need-to-know

1. **CMTX-I-021062024: Malicious Domains - Spear-Phishing Campaign**

The following malicious domain is associated with a spear-phishing campaign targeting government officials:

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

navygovin.000webhostapp.com

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

Kindly take the required actions.

1. **CMTX-P062024075: ACTIVE EXPLOITATION OF A CRITICAL VULNERABILITY (CVE-2024-28995) AFFECTING SOLAR WINDS SERV-U FILE TRANSFER SOFTWARE**

ALERT BRIEF:

CVE-2024-28995

CVSS-8.6

Associated Malware-CHAOS RAT

Affected Versions:

SolarWinds Serv-U 15.4.2 HF 1 and previous versions

Vulnerable Versions:

Serv-U FTP Server 15.4

Serv-U Gateway 15.4

Serv-U MFT Server 15.4, and

Serv-U File Server 15.4

A critical-severity vulnerability, tracked as CVE-2024-28995 is being actively exploited in the wild and affecting SolarWinds Serv-U file transfer software. The vulnerability is associated with a directory transversal bug that could allow attackers to read sensitive files on the host machine.

Recommendations:

\* As vulnerability has its potential for exploitation by threat actors targeting SolarWinds Serv-U file transfer software, it is crucial to prioritize patching this vulnerability promptly to mitigate the risk of potential cyberattacks on company assets

References:-

<https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995>

1. **CMTX-I-555062024: Mythic Malware - APT36 campaign**

Following IOCs 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>---------------

94.232.46.11

168-gov.info

node.hgxplayer.com

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

Kindly take the required actions.

1. **CMTX-P062024085: MYTHIC MALWARE**

ALERT BRIEF:

Mythic is a command-and-control (C2) framework used by threat actors for various malicious activities. The agents can perform tasks like executing commands, downloading files, and interacting with the user through an interactive shell. Mythic supports multiple communication profiles, including JSON and P2P connections. The framework is highly customizable and provides flexibility in designing and leveraging agents within the system. Recent updates to Mythic include features like interactive tasking, push C2 capabilities, dynamic file browsing, and database migrations.

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

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

IP Address

5.42.100.30

13.60.5.73

13.60.91.126

16.16.66.176

16.171.113.25

20.86.134.86

34.221.207.33

37.27.92.9

37.187.118.185

38.242.198.230

43.135.3.17

45.14.66.194

45.95.174.39

45.133.238.221

51.15.227.211

51.250.108.206

51.254.53.14

52.14.189.239

52.73.128.242

54.153.180.98

54.173.147.137

54.234.100.124

58.8.255.53

61.14.210.209

64.23.149.255

64.23.155.109

64.23.196.210

64.226.90.74

67.205.162.200

77.106.68.26

82.97.251.102

83.212.98.93

83.244.163.202

89.185.85.206

91.107.207.2

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

1. **CMTX-P062024105: Pantegana Malware**

ALERT BRIEF:

Pantegana is an open-source malware family written in Go that features a cross-platform payload client (Windows, Linux, OSX) and uses HTTPS for C2 communications. It supports file upload and download, system fingerprinting, and direct command-line interaction with infected hosts. Pantegana also supports obfuscation using the open-source obfuscator Garble. The Pantegana RAT uses a distinctive default certificate for its servers.

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

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

IP

119.28.107.67

154.92.19.225

198.98.62.227

205.185.126.208

209.141.41.176

209.141.46.83

43.130.237.18

205.185.126.208

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

1. **CMTX-P062024038: Agent Tesla Malware Alert**

Malware Alert Brief:

Agent Tesla usually spreads through phishing. However, the malware has a function which allows it to run automatically from a USB stick. At present, Agent Tesla is able to operate exclusively on Windows machines.

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

IP

203.161.184.34

89.45.67.2

153.92.8.115

86.96.202.167

153.92.8.107

61.19.247.49

203.175.9.22

203.161.184.34

45.252.248.26

213.189.52.181

79.172.209.125

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

1. **CMTX-P062024048: Amadey Malware Alert**

Malware Alert Brief:

Amadey is a simple Trojan bot. It is primarily used for collecting information on a victim's environment, though it can also deliver other malware.

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

IP

185.196.10.188

5.42.65.80

188.40.122.96

78.46.242.112

62.182.156.153

207.154.243.184

79.137.203.59

103.91.187.97

185.215.113.35

31.41.244.158

79.137.203.19

185.172.128.19

185.153.197.14

193.233.20.14

5.42.64.33

185.18.245.58

91.189.114.21

134.0.116.60

62.204.41.89

188.49.167.201

194.93.26.201

185.215.113.204

190.224.203.37

119.204.11.2

130.204.29.121

186.101.193.110

185.215.113.14

116.58.10.60

60.246.120.127

152.231.127.144

187.212.234.245

154.144.253.197

148.230.249.9

189.61.54.32

196.188.120.80

187.152.17.215

189.163.91.64

189.189.237.188

217.219.131.81

187.199.128.51

181.123.219.23

218.152.239.123

62.150.232.50

183.100.39.16

190.220.21.28

186.233.231.45

93.118.137.82

213.172.74.157

185.215.113.205

5.42.64.44

5.42.66.29

95.86.30.3

200.45.93.45

84.252.15.104

91.139.220.31

190.145.136.42

103.27.74.23

151.233.51.166

63.143.98.185

109.175.29.39

188.237.2.116

188.40.187.155

220.125.3.190

212.112.110.243

190.147.128.172

190.159.30.35

102.189.94.209

78.89.199.216

111.90.147.73

189.165.174.71

62.204.41.252

211.119.84.111

211.119.84.112

200.63.106.141

178.134.214.182

195.85.218.100

211.171.233.129

211.181.24.132

131.255.215.165

181.52.122.51

181.128.122.163

190.28.110.209

201.184.36.53

190.13.174.94

41.152.179.82

201.119.104.185

211.168.53.110

186.182.55.44

175.145.157.179

58.151.148.90

123.213.233.131

189.195.132.134

201.110.217.30

93.103.167.123

116.58.10.59

89.23.103.42

123.140.161.243

190.176.87.110

200.114.83.251

186.145.236.93

190.147.2.86

102.189.16.24

89.249.221.146

189.181.21.63

62.204.41.87

210.182.29.70

211.40.39.251

187.134.55.166

175.119.10.231

196.189.156.245

211.202.224.10

220.82.134.210

189.146.249.153

190.156.239.49

49.44.53.44

95.158.162.200

211.171.233.126

179.152.58.121

190.159.138.51

187.199.138.76

125.7.253.10

102.189.75.13

45.9.74.141

45.9.74.166

45.9.74.182

45.9.74.164

49.12.117.51

34.90.130.132

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

1. **CMTX-P062024058: Emotet Malware**

Malware Alert Brief

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans.

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

IP

61.76.222.210

51.89.36.180

49.205.182.134

51.38.124.206

115.79.195.246

5.196.108.185

83.110.222.32

130.0.132.242

168.197.45.36

81.213.175.132

51.75.33.127

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

1. **CMTX-P062024068: Qbot Malware**

Malware Alert Brief:

Qbot (also known as QakBot) is a common trojan malware designed to steal passwords. Over time this malware has evolved from simple infostealer malware to an infostealer with a backdoor functionality. Qbot is primarily used by financially motivated actors.

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

IP

5.61.49.13

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

1. **CMTX-P062024078: RACCOON MALWARE**

ALERT BRIEF:

CERT-IN has been tracking prominent RATs/malware families. An uprise in activities associated with raccoon malware is reported. Raccoon is an info stealer malware available as a Malware as a Service. Raccoon malware has capability to check system settings, capture screenshots, collect basic information like OS version, IP and username and steal passwords and logins from a variety of browsers.

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

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

IP

193.142.147.59

77.91.77.96

178.20.41.15

185.244.48.191

88.119.161.19

146.19.173.87

77.91.77.137

94.142.138.108

77.91.77.54

5.42.64.7

94.142.138.49

91.92.242.162

94.142.138.49

5.42.64.13

77.91.77.116

94.142.138.108

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

1. **CMTX-P062024088: Redline malware**

Malware Alert Brief:

Redline malware is a recent malware written in C# with notable growth in 2021. It includes modules of stealing credentials and collecting information from the infected machine and the capability to download remote files

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

IP

185.172.128.33

94.156.67.67

194.26.232.43

147.45.47.93

185.215.113.67

5.42.65.63

4.185.27.237

91.92.249.24

89.23.100.222

43.155.163.53

65.108.20.226

45.140.147.183

13.60.40.107

185.237.165.67

135.181.135.172

89.23.97.100

5.189.138.247

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

1. **CMTX-P062024098: SocGholish malware**

Malware Alert Brief:

SocGholish uses social engineering to infect systems: it tricks users into running a malicious JavaScript payload that masquerades as a system or software update, such as a critical browser update.

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

IP

85.117.32.82

35.215.148.34

77.75.78.166

77.245.56.14

101.44.160.204

103.43.18.114

101.44.162.117

195.24.68.25

128.199.167.175

185.216.114.10

37.57.218.243

47.128.124.211

5.101.115.147

103.153.68.122

89.22.232.186

93.159.230.87

213.219.247.125

138.199.24.24

174.138.28.229

47.128.60.130

47.128.114.149

47.128.118.29

47.128.38.86

47.128.116.139

47.128.122.244

47.128.52.238

47.128.16.47

47.128.16.65

47.128.17.108

47.128.18.185

47.128.19.9

47.128.19.23

47.128.19.65

47.128.21.235

47.128.23.9

47.128.23.96

47.128.23.212

47.128.24.36

47.128.27.19

47.128.28.119

47.128.28.236

47.128.29.77

47.128.29.130

47.128.29.208

47.128.30.132

47.128.31.138

47.128.31.204

47.128.33.20

47.128.34.108

47.128.34.205

47.128.36.39

47.128.36.98

47.128.37.165

47.128.38.15

47.128.38.88

47.128.38.167

47.128.38.246

47.128.39.155

47.128.39.246

47.128.40.110

47.128.40.218

47.128.40.225

47.128.41.232

47.128.42.103

47.128.42.215

47.128.43.104

47.128.43.136

47.128.43.244

47.128.44.30

47.128.44.128

47.128.45.185

47.128.46.53

47.128.46.120

47.128.47.84

47.128.49.102

47.128.50.178

47.128.51.87

47.128.51.208

47.128.52.128

47.128.52.172

47.128.53.17

47.128.53.162

47.128.53.252

47.128.54.100

47.128.54.210

47.128.55.206

47.128.55.247

47.128.56.8

47.128.56.102

47.128.56.131

47.128.56.203

47.128.57.217

47.128.58.38

47.128.59.252

47.128.59.253

47.128.60.4

47.128.60.92

47.128.60.144

47.128.60.216

47.128.62.49

47.128.97.16

47.128.97.186

47.128.98.185

47.128.109.77

47.128.110.10

47.128.110.180

47.128.110.192

47.128.110.232

47.128.111.74

47.128.112.83

47.128.112.137

47.128.113.16

47.128.113.90

47.128.113.223

47.128.114.20

47.128.114.179

47.128.114.190

47.128.116.168

47.128.116.220

47.128.118.5

47.128.118.88

47.128.119.0

47.128.120.10

47.128.120.66

47.128.122.145

47.128.123.70

47.128.123.80

47.128.123.146

47.128.123.174

47.128.125.104

47.128.127.17

47.128.127.19

47.128.127.151

47.128.127.200

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

1. **CMTX-P062024108: Trickbot malware**

Malware Alert Brief:

Trickbot is a highly modular malware, capable of performing a number of actions on a network such as stealing information or dropping ransomware.

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

IP

41.77.134.250

175.184.232.234

27.109.116.144

103.201.142.30

177.190.76.82

96.9.77.142

196.41.57.46

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

1. **CMTX-P062024118: Ursnif malware**

Malware Alert Brief:

Ursnif (also known as Gozi) is identified as a Banking Trojan, but its variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.

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

IP

13.251.16.150

18.143.155.63

18.141.10.107

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

1. **CMTX-P-062024115: DEPLOYMENT OF CL0P RANSOMWARE VARIANT BY FIN7 CYBERCRIMINAL GROUP**

Alert Brief:

ALIASES- GOLD NIAGARA, ITG14, Carbon Spider, ELBRUS, and Sangria Tempest

MOTIVATION-FINANCIAL GAIN

FIN7 is a Russian cyber criminal group which has been active in the cyber threat landscape targeting various organizations like retail and hospitality, along with manufacturing, transportation, insurance, and defense. The group executes ransomware attacks and extortion techniques to infiltrate corporate networks and payment systems using ransomware-as-a-service (RaaS) platforms for their campaigns, such as REvil, CL0P, DarkSide, and BlackMatter.

It has been reported that FIN7 is deploying CL0P ransomware variant in various industries like information management services, environmental service, legal services, manufacturing, transportation, education, medical and construction.

CL0P encrypts files and demands ransoms for decryption.

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

CL0P mutex

Kdfjs8293rjfsiyjiooiufoiewkfewjfoiewjrkiew

sdlkfjlkOFKJSLDdfjewklfw

IPs

185.72.8.147

166.1.190.48

23.133.88.226:443

URL

https[://]file.io/M9ofMokBC1TN

PowerShell script

2e6437b94564f1f3af504d69c77032bcf7a5423ae54a77eeb19b419350cf7f9a

dfa275a27ea43ccb5de9eecae6772077e65d8161ff4d037311d900cb7db7dbd8

7aea1b69ac949463ebbd901d5acf7187601085c33e3ad0e5dd1e6bf7347f3fb1

669fe9c12f0675743d18bd850a56eda7d0f616c71af9bb72f983247d8d18c6af

CL0P ransomware

1a362eea7a10cfe618d5934e35417c523b7fee22baeafd11862891c57efab217

005d2657a857adbc60d8811f8e256108550d0b79f3e95bb7ac1a0913867906f1

cd58a6837e4b5f1092eedfc3420d47812e6f347ba63ceefa2e6c451591cec94d

53a0517cb73c05729671aa3dcd2947eaeb3997378000f69b47c5a0d231bea53e

611be49c0bcff3044256c48ac721b69139dc844f3d722003757e76e2d4e67887

e786319a2a0eadc9b1da675a5f494abee902a2db472c1e72578a736c3332913e

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

1. **CMTX-P06024125: SparkRAT Malware**

ALERT BRIEF:

Spark RAT is an open source cross-platform remote access Trojan (RAT) written in Golang and frequently updated by its developer. Spark RAT is capable of evading detection by checking for virtual machines and debuggers on the compromised machine. The malware is typically delivered through the download and execution of batch files or LOLBins. It is used by threat actors due to its multi-platform capabilities and frequent updates. The most recent events involving Spark RAT include its deployment by Chinese-speaking threat actors.

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

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

IP

154.201.90.77

211.155.101.2

77.83.172.47

154.198.245.48

120.220.61.6

120.79.42.98

103.108.41.146

63.250.53.103

66.85.92.25

1.94.11.195

72.5.43.90

37.1.213.121

175.178.126.203

106.54.232.49

101.35.198.64

1.15.135.238

38.54.94.13

140.238.9.202

149.28.150.214

67.217.62.106

208.87.201.17

47.105.208.58

146.56.211.186

8.138.23.74

138.68.44.59

38.207.176.157

120.79.97.24

3.145.94.208

47.97.185.22

27.124.40.175

139.180.180.177

178.173.248.30

103.26.10.104

117.18.3.242

117.50.76.61

103.26.10.104

103.108.41.147

116.63.145.255

46.3.106.120

137.184.68.203

46.3.106.121

198.44.237.37

118.190.161.229

34.92.25.154

121.4.140.182

38.154.74.20

68.168.211.94

47.96.129.195

46.3.106.165

147.45.44.29

47.236.43.52

27.124.40.169

110.42.250.96

46.3.106.171

83.221.206.30

46.3.106.171

178.173.249.62

47.106.152.139

58.37.83.7

8.210.81.164

178.173.249.62

38.54.94.13

27.124.40.170

43.155.16.246

84.32.214.103

116.62.145.180

103.118.41.11

139.84.138.232

195.158.250.189

103.108.41.148

116.198.34.133

195.201.158.117

46.3.106.165

8.138.133.205

178.173.248.30

103.118.41.11

178.173.249.204

2.15.253.35

HASH

b8cab11421eb4731c16cf3c34ca2b3f2a758d 5e112f877b90a18b3e146c8add0

ec45da0ca70a9b71652cc95d51665f7ad5682 94bd5652c395a119bccd613e9b4

23efecc03506a9428175546a4b7d40c8a943c 252110e83dec132c6a5db8c4dd6

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

1. **CMTX-I-911062024: Malicious Domains - Spear-Phishing Campaign**

The following malicious domain is associated with a spear-phishing campaign targeting government officials:

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

cbigovins.site

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

Kindly take the required actions.

1. **CMTX-I-389062024: IOCs of Pakistan based Malware Campaign**

The following IOCs are associated with Pakistan based malware campaign:

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

swachbharat.xyz

207.244.239.158

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

Kindly take the required actions.

1. **CMTX-P062024135: MYTHIC MALWARE**

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

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

IPs

93.127.197.83

95.111.236.195

95.164.19.54

95.164.22.13

129.226.154.137

137.184.39.229

137.184.67.135

138.197.156.131

139.59.109.136

142.93.74.10

143.110.176.131

144.202.12.174

145.131.8.169

149.104.26.229

152.42.162.105

152.42.198.168

152.42.245.111

154.38.167.90

158.247.250.154

159.89.191.115

159.223.0.196

161.35.207.209

164.90.158.199

168.100.8.115

172.86.75.53

172.94.53.132

172.104.153.104

172.174.105.127

178.128.92.166

185.16.43.59

185.158.94.217

193.201.126.69

201.243.95.21

217.6.46.91

217.12.200.158

217.79.255.137

38.54.63.8

94.232.46.11

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

1. **CMTX-I-433062024: Malicious Domains - Spear-Phishing Campaign**

The following malicious domain and its associated IP are linked with a spear-phishing/malware hosting campaign by Pakistan based threat-actors to target government officials:

- ---------<Malicious Domain and Associated IP>--------

cert-in.org.in.honeytrap.online

78.40.117.207

- ---------</Malicious Domain and Associated IP>-------

Kindly take the required actions.

1. **CMTX-P062024746: GH0ST RAT Malware**

ALERT BRIEF:

GH0ST is a backdoor written in C++ that communicates via a custom binary protocol over TCP or UDP. GH0ST RAT has capability of capturing screenshots, Key logger, remote Shell and Command execution, reversing proxy, file transfer and file management, features a packet signature at the start of each message that varies between samples.

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

IP ADDRESSES

70.28.194.62

47.115.207.251

45.207.47.172

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

1. **CMTX-P062024756: QuasarRAT Malware ALERT 56**

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

119.45.53.199

91.92.250.148

128.199.96.24

91.92.243.74

91.182.38.39

89.169.55.95

194.156.98.99

124.71.225.72

191.93.112.233

162.14.109.249

95.179.242.32

45.63.16.30

192.121.102.103

203.23.128.30

41.216.183.47

185.208.158.136

43.135.119.209

91.92.242.187

195.26.243.241

142.127.78.224

181.162.151.240

188.50.164.181

202.146.223.26

194.187.251.163

14.35.42.91

78.70.235.238

94.156.64.24

194.238.29.238

87.109.205.118

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

1. **CMTX-I-090062024: Malicious Domains used by Pakistan based Threat Actors**

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

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

cgdaoffice.cordoffice.cloud

gangaram-hospital.cordoffice.cloud

\*.cgdaoffice.cloud

\*.cordoffice.cloud

\*.npcil-nic.cloud

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

1. **CMTX-I-514062024: IOCs of APT36 Malware campaign**

Following are the IOCs being used by Pakistan based APT36 threat actors for their malware campaign targeting government officials:

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

dummy.ggovin.com

detention.codewallah.in

mod.ggovin.com

\*.codewallah.in

\*.ggovin.com

zpbeed.gov.in (compromised domain)

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