**Cyber Security Advisories**

**Date: 17 October 2024**

1. **[CMTX-P102024075] Salt Typhoon Activity**

ALERT BRIEF:

Threat Actor Type: Nation State Sponsored APT group

Severity: High

Attack vectors: - Cyber spying (Cyber espionage)

Reports indicate that Chinese state-sponsored threat groups are actively targeting internet service providers (ISPs) as part of an ongoing cyberespionage campaign known as Salt Typhoon. These threat actors are infiltrating broadband infrastructure to establish persistent access, monitor communications, collect sensitive data, and set the stage for potential future attacks on critical infrastructure. The initial attack vector involves unauthorized access to ISP networks, possibly exploiting vulnerabilities in Cisco Systems routers. Once inside, the threat actors gather sensitive information, including users’ locations, billing details, and service usage data like call and text records. The tactics, techniques, and procedures (TTPs) associated with Salt Typhoon are similar to those used by Flax Typhoon and Volt Typhoon. The objective of threat actor is not only to collect intelligence but also to position themselves for potential future attacks on key infrastructures.

1. **[CMTX-I-401102024] Mythic Malware- APT36 campaign**

ALERT BRIEF:

Mythic is an advanced, customizable Command and Control (C2) framework primarily used by threat actors to control and manage malware operations. Mythic is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, MacOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents e.g. Apollo (Windows), Poseidon (Linux, MacOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

Recent C&C server of Mythic malware are as follows:

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

165.232.118.207

161.35.186.219

159.203.133.189

137.184.211.26

64.23.213.61

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

Network administrators may take required action against the above indicators of compromise (IOC).

1. **[CMTX-I-400102024] Malicious Domains used by Threat Actors**

- --------------------------<META INFORMATION>---------------

Confidence-High

Risk-High

TLP:AMBER-Limited disclosure, recipients can

only spread this on a need-to-know basis within

their organization and its clients.

- ---------------------------------------------------------------

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

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

mof-gov.info

scigovcourt.com

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

1. **[CMTX-P102024106] Blackout Ransomware**

Threat Campaign: Blackout Ransomware

The Blackout ransomware group operates an extortion blog on the dark web called "name-and-shame," where they list their victims. The blog is written entirely in English and can only be accessed via the Tor browser. While the specific tools, tactics, techniques, and procedures (TTPs) used by the Blackout ransomware group in their attacks remain unknown, a public sample linked to Blackout ransomware is available, with its indicators of compromise (IOCs) provided in the annexure.

Threat Type: Ransomware

Severity: High

- -----------------------------------------------------------------------------

Indicators of Compromise (IOCs):

HASHES:

ae121f28c05037d09f85f8b7ef9930f2d62c8f0e6e6a8d7ff092932ddbb1ad23

URL

black3gnkizshuynieigw6ejgpblb53mpasftzd6pydqpmq2vn2xf6yd.onion

- ----------------------------------------------------------------------------

1. **[CMTX-P102024024] INC Ransomware**

Threat Campaign: INC Ransomware

The INC Ransomware family, linked to the INC RANSOM threat actor group, has been targeting a variety of sectors. Initial access is often gained through first-stage malware loaders, such as Gootloader. This group employs double-extortion tactics, threatening to release stolen data if ransoms are not paid. The actors behind INC Ransomware exhibit capabilities like privilege escalation to carry out actions without detection, as well as lateral movement within networks using tools such as AnyDesk.

Threat Type: Ransomware

Severity: High

- ----------------------------------------------------------------------------------

Indicators of Compromise (IOCs):

HASHES:

c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef

d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6

508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef

36e3c83e50a19ad1048dab7814f3922631990578aab0790401bc67dbcc90a72e

fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced

869d6ae8c0568e40086fd817766a503bfe130c805748e7880704985890aca947

- ----------------------------------------------------------------------------------

1. **[CMTX-P-102024034]: Dark Crystal RAT (DC RAT)**

Threat Overview:

DarkCrystal RAT also known as DCRat is a commercial Russian backdoor which operates as a Malware-as-a-Service (MaaS). It has been associated with various malware families such as BlackMatter, Cerber, Cobalt Strike, Ficker Stealer, QakBot, REvil, and Ryuk. For its command and control communications, it uses SSL/TLS certificates. The malware allows threat actors to gain unauthorized access to infected systems and perform various malicious activities such as data theft and system control. It can steal information from the following sources like Browser cookies, Browser stored passwords ,Browser stored form content ,Browser history ,Stored credit cards (via Windows DPAPI & Chrome SQLite Database),Telegram, Discord tokens, keyloggers, etc.

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

Indicators of Compromise (IOCs):

IP:Port

217.15.160.54

159.65.235.56

179.13.4.37

8.217.140.110

194.32.149.186

91.92.254.46

217.15.160.54

179.13.4.37

185.213.25.37

124.221.231.247

51.89.253.9

103.147.185.18

12.187.175.72

45.135.232.38

27.124.45.77

95.179.246.167

103.75.190.47

192.197.113.223

144.91.127.15

51.77.103.216

4.233.193.26

195.33.238.38

123.249.104.74

76.66.229.229

12.202.180.114

45.77.179.49

43.199.93.110

27.124.45.70

8.217.88.225

117.72.74.85

91.92.254.114

171.251.30.8

42.113.255.207

91.92.247.210

217.195.197.55

107.189.171.137

201.191.100.200

188.166.240.231

121.5.112.136

129.204.197.19

1.14.126.22

83.147.38.162

136.244.80.89

103.142.146.12

193.233.203.181

207.246.99.14

195.33.238.39

154.12.47.158

103.243.26.65

4.248.59.179

8.137.98.17

185.117.90.153

209.126.4.168

154.12.93.14

103.186.108.212

42.192.132.36

147.185.221.20

202.162.109.198

54.39.83.175

124.220.49.140

141.223.48.24

20.90.89.160

59.27.223.225

119.91.157.193

46.246.6.13

78.135.83.58

46.246.82.7

121.199.58.53

121.196.235.124

103.17.185.70

203.104.42.92

107.167.92.76

111.230.96.32

94.156.65.202

4.178.137.16

154.216.19.100

76.66.229.226

121.41.177.111

110.41.40.124

182.188.47.2

101.99.92.203

94.124.192.220

39.105.61.159

185.146.88.217

176.96.138.247

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

HASH

2c898cc8d4ed2e67effe5362bf7951143563a965057110d6b803b983e7db3eb5

693e681c06e3b8f374bd5e25daa6c70d4947956f1aa5e1cb7a18f2da0844323f

763c1f21d22b7215d36e2dbd52d141d71d9e540c19f631f63f151c283b91f0d8

60665c8f8ff802fb116a4d761a812911a0cf209e5e56f48fdb566e94cc177c33

DOMAIN

cr87986.tw1.ru

1. **[CMTX-P102024044] Relay server Nodes used by Chinese actors**

A state-sponsored threat actor based in China has been observed using anonymization networks such as HiddenOrbit (RedRelay) and SuperJump, along with relay server nodes, to route their traffic and evade detection. The attackers leveraged active VPS nodes, compromised unpatched routers and IP cameras, to target internet-facing networks and security appliances of strategic interest. In this context, a list of relay server nodes actively used by the attackers has been compiled. The shared IP addresses are associated with small home and office (SoHo) routers and IP camera appliances. Additionally, IP profiling indicates that the attackers have specifically targeted unpatched CISCO RV340 VPN Router and Cyberoam devices.

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

1.22.207.35

1.22.255.28

103.104.73.40

103.111.234.44

103.112.85.196

103.12.195.20

103.121.118.42

103.142.115.26

103.145.168.212

103.147.249.126

103.160.240.4

103.167.72.8

103.205.127.2

103.228.222.248

103.231.44.98

103.233.92.146

103.252.145.75

103.255.180.132

103.48.199.2

103.56.225.96

103.74.198.34

103.77.125.2

103.79.11.233

103.88.236.92

103.98.85.217

106.201.238.202

106.51.28.209

106.51.80.140

111.118.241.130

111.92.41.85

111.93.32.162

114.143.16.250

114.143.225.198

115.124.115.20

115.242.180.154

115.242.230.194

115.243.243.178

115.244.173.102

115.244.251.158

116.75.150.113

117.200.73.248

117.203.228.18

117.203.243.38

117.208.59.67

117.236.96.228

117.239.186.65

117.254.83.105

122.160.144.182

122.160.65.240

122.166.211.60

122.169.116.104

122.176.122.172

122.179.137.207

122.187.153.10

122.252.253.10

124.123.96.106

136.232.96.74

139.167.50.178

14.142.99.222

14.143.224.59

14.194.176.228

14.194.242.66

14.98.98.62

150.107.210.172

150.129.131.150

152.58.92.127

183.82.101.212

183.82.111.42

183.82.98.176

202.134.205.103

202.88.227.94

202.88.254.69

203.112.154.29

203.123.38.174

43.225.163.33

45.115.168.80

47.247.64.156

49.204.234.232

49.36.137.120

49.36.192.43

49.43.251.100

59.144.105.74

59.93.37.55

59.95.102.36

61.2.142.145

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

1. **[CMTX-P-102024174] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is 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).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

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

45.67.34.151

139.180.193.182

202.181.27.211

216.238.121.119

216.238.68.75

45.32.144.227

64.176.6.27

38.60.198.62

202.61.87.139

207.246.106.76

155.138.195.85

95.179.240.31

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

1. **[CMTX-P-102024164] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

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

154.84.24.184

154.26.153.129

45.204.20.195

45.204.20.196

154.9.255.200

103.101.178.214

172.94.9.19

103.56.53.46

172.94.9.69

202.95.14.139

27.124.43.101

47.242.114.104

27.124.43.84

154.82.113.166

47.116.78.51

202.95.14.136

45.195.69.203

202.95.14.138

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

1. **[CMTX-I-500102024] Mythic Malware- APT36 campaign**

ythic is an advanced, customizable Command and Control (C2) framework primarily used by threat actors to control and manage malware operations. Mythic is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, MacOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents e.g. Apollo (Windows), Poseidon (Linux, MacOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

Recent C&C server of Mythic malware is as follows:

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

128.199.59.209

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

1. **[CMTX-I-502102024] Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

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

www.email.gov.in.igov.ink

www.email.gov.in.webiaf.link

email.gov.in.gov-in.mywire.org

mail.eoffice.ink

\*.igov.ink

\*.webiaf.link

\*.gov-in.mywire.org

\*.eoffice.ink

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

1. **[CMTX-P102024054] Relay server Nodes used by Chinese actors**

A state-sponsored threat actor based in China has been observed using anonymization networks such as HiddenOrbit (RedRelay) and SuperJump, along with relay server nodes, to route their traffic and evade detection. The attackers leveraged active VPS nodes, compromised unpatched routers and IP cameras, to target internet-facing networks and security appliances of strategic interest. In this context, a list of relay server nodes actively used by the attackers has been compiled. The shared IP addresses are associated with small home and office (SoHo) routers and IP camera appliances. Additionally, IP profiling indicates that the attackers have specifically targeted unpatched CISCO RV340 VPN Router and Cyberoam devices.

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

103.102.58.138

103.105.155.74

103.105.225.3

103.107.112.149

103.11.80.31

103.110.242.42

103.172.97.71

103.177.205.198

103.186.40.9

103.205.127.78

103.206.129.242

103.210.144.236

103.211.204.132

103.216.71.93

103.216.92.202

103.217.78.44

103.219.61.159

103.231.7.218

103.241.23.75

103.255.72.117

103.27.143.30

103.69.29.251

103.79.252.17

103.80.161.69

103.86.69.243

106.201.239.242

106.51.186.166

106.51.39.33

110.227.194.188

113.193.238.43

115.241.235.82

115.242.60.170

115.244.232.114

117.216.139.240

118.185.234.165

119.82.86.224

122.160.45.213

122.160.68.39

122.161.194.172

122.168.127.239

122.170.112.222

122.176.107.144

122.176.27.184

122.176.74.214

123.176.34.88

123.252.161.114

123.252.197.122

124.123.122.104

124.123.97.6

124.253.6.42

125.22.51.182

136.232.117.102

136.232.213.10

14.139.214.135

14.139.232.7

14.194.176.229

14.97.177.122

14.98.72.62

14.98.85.66

150.107.210.180

150.129.144.130

152.59.119.226

180.211.99.202

182.50.68.242

182.70.113.217

182.73.143.102

183.82.111.17

202.131.117.114

202.179.72.173

203.187.204.247

210.18.180.211

219.91.140.219

27.0.58.11

43.248.32.18

45.114.178.194

45.127.58.125

45.64.193.250

49.204.232.133

49.36.8.212

59.182.49.101

59.94.179.7

59.95.100.18

60.254.16.95

61.2.103.117

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

1. **[CMTX-P-102024064] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

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

45.32.124.105

104.233.173.53

63.141.237.208

45.32.149.253

137.220.183.79

103.125.219.228

103.21.90.202

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

1. **[CMTX-P-102024074] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is 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).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Impacts:

Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : Multi modular backdoor

3. Severity: High

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

154.205.134.232

141.164.49.53

149.28.28.9

45.76.191.59

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

1. **[CMTX-P-102024084] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

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

137.220.224.29

27.124.3.248

8.218.163.85

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

1. **[CMTX-I-301102024] Malicious Domains used by Threat Actors**

Threat Overview

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

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

sebi-gov.info

mahagov.info

gov.in.nha.in

ail-gov.ink

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

1. **[CMTX-I-302102024] CrimsonRAT- APT36 campaign**

Threat Overview

CrimsonRAT is a remote access trojan (RAT) primarily associated with APT36 (a.k.a. Transparent Tribe). It is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

Common Features of APT36 Threat Actor:

Spear-Phishing (highly targeted and convincing phishing emails to trick victims)

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

Recent C&C server IP of malware deployed by this threat actor is as follows:

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

152.105.206.128

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

1. **[CMTX-I-053102024] Mythic Malware- APT36 campaign**

Threat Overview

Mythic is an advanced, customizable Command and Control (C2) framework primarily used by threat actors to control and manage malware operations. Mythic is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, MacOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents e.g. Apollo (Windows), Poseidon (Linux, MacOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

Prevention Measures:

Be wary of unsolicited emails, especially those with attachments or links

Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.).

For Windows- Uncheck "Hide extensions for known file types" in File Explorer's Folder Options under the View tab to display file extensions

For Linux- ELF executables typically have no extension or use unconventional extensions. (check using 'file <file\_name>' command)

Principle of least privilege

Firewall and network security along with regular OS updates

Recent C&C server/IOCs of Mythic malware is as follows:

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

178.128.89.173 (malware hosting)

170.64.225.181

68.183.195.95

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

1. **[CMTX-I-053102024\_1] Mythic Malware- APT36 campaign**

Threat Overview

Mythic is an advanced, customizable Command and Control (C2) framework primarily used by threat actors to control and manage malware operations. Mythic is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, MacOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents e.g. Apollo (Windows), Poseidon (Linux, MacOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

Prevention Measures:

Be wary of unsolicited emails, especially those with attachments or links

Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.).

For Windows- Uncheck "Hide extensions for known file types" in File Explorer's Folder Options under the View tab to display file extensions

For Linux- ELF executables typically have no extension or use unconventional extensions. (check using 'file <file\_name>' command)

Principle of least privilege

Firewall and network security along with regular OS updates

With reference to the previous alert CMTX-I-053102024 dated 08/10/2024 additional IOCs of Mythic malware is as follows:

- -----------------< IOC>-------------

178.128.246.38 (malware hosting)

- -----------------</IOC>-------------

1. **[CMTX-P-102024034] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

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

2.58.15.48

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

1. **[CMTX-I-587102024] Malicious Domains used by Threat Actors**

Threat Overview

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

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

email-g0v.online

em.ail-gov.ink

\*.ail-gov.ink

\*.email-g0v.online

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

1. **[CMTX-P-502102024] Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

email-g0v.online

email-gov.ink

coord-dept.in

support-panel.in

ail-gov.ink

gov.in.nha.in

\*.ail-gov.ink

\*.email-g0v.online

www.email.gov.in.igov.ink

www.email.gov.in.webiaf.link

email.gov.in.gov-in.mywire.org

mail.eoffice.ink

\*.igov.ink

\*.webiaf.link

\*.gov-in.mywire.org

\*.eoffice.ink

1. **[CMTX-I-137102024] SideCopy Malware C&C Domain**

SideCopy is a Pakistan based, sophisticated threat actor known for deploying malware to target individuals and organizations, particularly India based. Named for its technique of mimicking other well-known attack patterns, SideCopy aims to steal sensitive information and conduct espionage. This group is particularly notable for its spear-phishing campaigns and the deployment of custom malware to compromise target systems.

Common Features of SideCopy Threat Actor:

Spear-Phishing (highly targeted and convincing phishing emails to trick victims)

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

Prevention Measures:

Be wary of unsolicited emails, especially those with attachments or links

Monitoring and logging to detect unusual activities indicating a compromise

Multi-Factor Authentication (MFA) for emails

Encrypt sensitive data to protect it in case of exfiltration

Recent C&C server Domain of malware deployed by this threat actor is as follows:

- ----------- < C&C Domain>----------

amazonindia-in.hopto.org

- ----------- </C&C Domain>----------

1. **[CMTX-P102024094] Relay server Nodes used by Chinese actors**

Threat Overview

A state-sponsored threat actor based in China has been observed using anonymization networks such as HiddenOrbit (RedRelay) and SuperJump, along with relay server nodes, to route their traffic and evade detection. The attackers leveraged active VPS nodes, compromised unpatched routers and IP cameras, to target internet-facing networks and security appliances of strategic interest. In this context, a list of relay server nodes actively used by the attackers has been compiled. The shared IP addresses are associated with small home and office (SoHo) routers and IP camera appliances. Additionally, IP profiling indicates that the attackers have specifically targeted unpatched CISCO RV340 VPN Router and Cyberoam devices.

Indicators of Compromise (IOCs):

IP ADDRESSES

1.22.170.53

103.122.228.8

103.152.199.52

103.158.45.20

103.160.207.197

103.167.72.243

103.173.137.46

103.203.172.13

103.211.36.166

103.217.78.206

103.234.137.78

103.250.163.73

103.251.212.66

103.44.53.68

103.57.134.194

103.6.187.253

103.68.176.234

103.70.204.34

103.80.248.80

103.83.255.26

106.222.211.33

106.51.248.38

110.226.124.120

111.92.61.45

111.92.62.28

111.92.63.150

112.196.118.123

113.193.24.157

114.79.149.98

115.166.142.186

117.203.231.133

117.205.64.66

117.206.175.61

117.219.9.234

117.247.19.61

117.247.91.66

117.248.250.212

117.251.18.141

122.162.145.183

122.169.42.89

122.170.0.244

122.176.27.18

123.63.241.133

125.18.175.130

136.232.180.174

139.167.52.54

14.139.252.99

14.194.23.211

150.129.144.137

150.129.55.35

171.50.247.73

178.248.117.54

182.73.212.26

182.74.138.66

182.75.24.234

183.177.126.127

183.83.219.9

202.131.109.90

202.164.156.15

202.53.94.58

202.83.28.9

219.65.55.162

223.233.76.55

223.29.205.154

43.224.9.71

43.228.113.110

45.114.192.44

45.126.169.138

49.206.114.232

49.207.13.46

49.249.59.42

49.43.89.182

59.145.197.194

59.92.127.214

61.247.228.253

1. **[CMTX-P102024104] RCRU64 Ransomware**

Threat Overview

Recent reports indicate a new ransomware campaign linked to RCRU64 threat actors. The initial access was likely obtained through Remote Desktop Protocol (RDP) on a public-facing server that lacked multi-factor authentication (MFA). Once inside, the attackers extracted credentials and encrypted files using a mix of open-source and custom tools, including fgdump, pwdump, Mimikatz, Advanced Port Scanner, and IObit Unlocker. They also left a ransom note instructing victims to reach out via email or Telegram.

Threat Type: Ransomware

Severity: High

- ------------------------------------------------------------------------------------------

Indicators of Compromise (IOCs):

IPs:

185.147.34.53:3586

190.93.96.6

190.93.96.29

190.93.96.30

187.116.73.31

HASHES

910dddb239ca9c7e153948ac3b076b088388de967ac55b2eb24a9a368a65bcbe

152c9b5e3265c889e66b77ae4f28578764ad886b9251620f1ddb9a74baa2c6a3

3fd192c206cac90463b7d363f42ef6b018f78a891d6a1e721e511d99f5bf3474

f14288bb71c91e7668b8d90200ed26f447d2037551e2467750ef1b9bd5861c4d

f80e1fd9f825c4c6939026a729cc411a1c71a48b9b9db9dbcef6d692a33e5c52

d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb

a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86

5fe00ded2d8fd701b7591f16248249d31e44f9adbda9f750d61fb5a0c3208f16

dc10d206da45be84f7101ae3053651d30859ec6636d81f000932fa215cc44d08

fcc7210cb356c413d47a60136e078528b2a6fe174755bf1c20aa87184e13dd09

eaa9dc1c9dc8620549fee54d81399488292349d2c8767b58b7d0396564fb43e7

3b3a3fe2eb5ef289fb58eee0f18b7240c375bc0d7af6ade747cfc865fa050d94

d31d8ff5a63702f23f068acf4b2d421396ca04a1c38375759ea45814054c3702

cbc19cb2308cf0aea7e99ba1fb5ed6f6dc46087aa011764ba65bdb1d96116ca2

ed7aabbbb1a98a769c2fa98fcface15667f31c17c7628dd781a4c812562ca7b2

0ebf9d3800f5ca5ba4792c1f7df8f06dbbf49fe698e873f161fa8b21e6307207

c5b30127f55ab4ff701b5772f3c668b98cdf6f7c426e65cc800e57c908b7f2cf

9368d4db4f743d3a97f8893c28e1157ed8ba82eb8d798b945de0f70c741d94f3

10eff0aa2b81ddcad196a560d843725452d344826185f2c4dd32c39fef0b142d

3f9d0c297e903a2200b78f8a87904934e1e1f0cd5fbef2194b0b6435361ed2ef

35f92e7543dfb8f05f512958c804787fa72ec23987c323b087bb38f53848bbcc

5c428f3ab071e48f70bf4e7ef1d8c377fd954c92dcac08f37eb9a42ce499442d

6612cf82da05701ed9262f598724a9435b015890a79aa0e928c53e4e6702bf08

67f0f6bfd582388917adcbfb294901f37e3979455880065220dcda03c7dd8f1a

6a180ebb123cc8970249ff9cc4496cd811b4d5d6a7356709c65cac188e3f742b

a2bb1178b6d17512f2606ad01cdc245ea52e91d17f6740d7dfdbef3a76e19c77

c3d7188add8892823fa6169f4ba3523b43e4cba6c9fff6931b3c482d077137c9

e928295cc90b8a0aac825a86f21e99b92f1c8665085c6e4cc3fc88cc63958e68

fe0383f9fa9df8b28729104c896eebc79dad0e9fc6f68612868385467e18fbc8

579d655b75afd6bf62b6740169eaef1238af4d2d47458ea3b3da36f3784a14a7

8f7192dee21820e55e051de6046b5dbce24819a95defe818d858e9cd3d242a17

4d3f38f349153ff936290ec069673026961973c49d883fc1186a925698d6a99a

Email addresses

Evo.team1992@gmail.com

Backshow@my.com

Captiial@gmail.com

Exploit2@cock.li

Anabellabackup@protonmail.com

decrypt\_.files@mailfence.com

Leoxrinse234@mailfence.com

Backonline@cock.li

Insomnia1441@gmail.com

Decvvv110@gmail.com

Wanhedaa@zohomail.eu

Dontcrylol@mailfence.com

Silolopi736@gmail.com

Kilook200@gmail.com

Dr.file2022@gmail.com

Pm24@tuta.io

Unknownsupport@mailfence.com

Redem.mikhail17662@gmail.com

Ez.microbe@zohomail.eu

Help.File@zohomail.eu

Qetsiyah@zohomail.com

Sc.computer1992@Gmail.com

Ross.dec1966@gmail.com

MrLetMeOpen@tutamail.com

HellCity@Tuta.io

Cryhelp45@gmail.com

Rdpdik6@gmail.com

Vansu@mailfence.com

Yuzuke@Tuta.io

Dec.717team@gmail.com

Lohikol22@gmail.com

Xinof2@skiff.com

Unlockingrdp3@gmail.com

Letmekey.me@gmail.com

Ransomwarebit@gmail.com

Jounypaulo@mail.ee

Helpadmin@mail.ee

- ------------------------------------------------------------------------------------------

1. **[CMTX-I-025102024] Malicious Domains used by Threat Actors**

Threat Overview

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

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

sebigovin.sebi-gov.io

sebi-gov.io

\*.sebi-gov.io

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

1. **[CMTX-I-021102024] Malicious Domains used by Threat Actors**

Threat Overview

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

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

adhar.auths.info

adhar-ucl.auths.info

cpanel.adhar.auths.info

cpanel.adhar-ucl.auths.info

new.auths.info

cpcalendars.adhar.auths.info

cpcalendars.adhar-ucl.auths.info

cpcalendars.new.auths.info

cpcontacts.auths.info

cpcontacts.adhar.auths.info

cpcontacts.adhar-ucl.auths.info

cpcontacts.new.auths.info

crsorgi.gov.in.web.index.php.auths.info

dc.crsorgi.gov.in.auths.info

webdisk.adhar-ucl.auths.info

webdisk.new.auths.info

webmail.adhar.auths.info

webmail.adhar-ucl.auths.info

webmail.new.auths.info

whm.auths.info

whm.adhar.auths.info

whm.adhar-ucl.auths.info

whm.new.auths.info

www.auths.info

www.adhar.auths.info

www.adhar-ucl.auths.info

www.crsorgi.gov.in.web.index.php.auths.info

www.dc.crsorgi.gov.in.auths.info

www.new.auths.info

mail-desk.in

minfinfgov.info

\*.auths.info

\*.mail-desk.in

\*.minfinfgov.info

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

1. **[CMTX-P-102024015]: Critical Alert: MYTHIC Malware Campaign**

Threat Overview

1. Threat Campaign: Mythic Malware Campaign

Mythic Malware is a sophisticated piece of software used by cyber actors (observed several campaigns from Pakistan based threat actors) to conduct various types of cyberattacks. This malware is designed to infiltrate systems, exfiltrate sensitive information, and maintain persistent access. It operates by exploiting vulnerabilities in software or operating systems to install itself covertly. Once installed, Mythic Malware can perform actions such as capturing keystrokes, accessing files, and sending data back to the attackers. Its use is primarily focused on espionage and data theft, making it a significant tool in cyber intelligence operations.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : A cross-platform, post-exploit, red teaming framework

3. Severity: High

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

152.42.198.168

165.232.118.207

170.64.175.56

164.92.179.221

152.42.198.168

139.59.109.136

142.93.74.10

159.223.0.196

161.35.186.219

164.90.177.232

159.203.133.189

165.232.118.207

147.182.150.146

137.184.67.135

170.64.175.56

157.245.146.223

164.92.179.221

134.209.101.248

14.225.254.224

14.225.255.32

14.225.255.166

18.191.106.202

52.53.207.84

86.38.247.225

35.153.232.88

3.68.92.103

178.128.92.166

159.223.0.196

149.248.4.114

194.171.96.118

57.155.2.68

52.128.230.46

34.31.178.96

194.87.85.8

35.200.161.35

43.135.3.17

14.225.254.224

195.158.82.221

216.128.129.3

95.164.22.13

45.77.151.211

193.201.126.69

195.208.174.240

14.225.217.103

149.210.143.97

185.158.94.217

172.211.232.90

47.83.23.246

104.143.38.196

149.248.56.154

95.164.19.54

162.212.154.121

3.15.21.172

20.115.66.63

139.84.149.212

14.225.217.7

54.218.90.249

45.77.151.211

14.225.217.205

46.8.237.247

138.197.156.131

88.90.159.162

35.196.90.200

160.238.36.36

64.176.214.38

121.127.33.25

51.15.227.211

51.254.53.14

64.226.91.107

78.141.204.24

14.225.255.166

54.247.71.250

165.232.118.207

52.232.197.207

159.203.133.189

152.42.198.168

18.234.143.128

195.189.96.70

139.59.109.136

35.204.187.119

64.23.213.61

52.25.188.122

45.133.238.221

139.84.195.78

45.133.238.221

20.115.73.1

92.222.217.152

162.120.71.226

89.31.122.21

202.61.137.238

3.227.184.192

74.249.9.163

20.229.189.122

185.158.94.217

13.245.162.103

66.70.202.83

207.180.224.247

88.90.159.162

20.185.50.39

54.218.90.249

66.42.40.228

172.105.27.15

172.201.107.88

149.104.26.229

81.208.161.44

34.219.143.252

81.208.161.44

34.171.84.82

170.64.234.99

20.51.254.237

51.178.137.204

43.134.38.211

143.244.171.63

14.225.217.7

52.128.230.42

89.221.225.227

50.18.43.35

44.224.147.7

209.38.45.156

14.225.217.103

147.182.150.146

45.145.229.103

139.84.195.78

35.177.104.235

51.144.104.92

14.225.217.205

95.111.236.195

51.144.103.170

40.69.91.248

161.35.186.219

137.184.211.26

45.92.9.144

51.144.105.221

3.16.25.250

216.225.205.4

51.254.53.14

193.149.129.107

34.95.22.12

172.232.190.135

51.145.156.236

172.105.27.15

165.232.118.207

35.200.161.35

145.131.8.169

149.248.59.104

45.76.234.154

20.92.252.75

52.128.230.44

154.38.167.90

78.141.204.24

188.166.121.117

192.109.241.19

64.176.214.38

107.175.0.167

3.133.126.43

198.7.121.101

64.23.184.118

20.115.66.63

84.32.131.58

46.8.237.247

164.90.158.199

142.93.74.10

172.232.190.135

20.92.252.75

51.15.227.211

54.160.134.78

145.131.8.169

89.44.199.196

170.64.175.56

94.232.43.221

64.23.155.109

64.226.91.107

149.248.56.154

195.230.23.91

86.38.247.225

47.237.20.201

45.145.229.103

13.66.164.102

107.175.0.167

54.158.206.132

164.90.158.199

149.28.83.179

14.225.255.32

217.28.130.27

149.248.59.104

136.244.109.139

47.245.14.36

8.210.9.166

13.58.109.128

164.92.179.221

20.51.254.237

170.64.234.99

45.32.113.133

121.43.166.96

52.128.230.43

51.145.154.243

144.202.72.130

193.201.126.69

52.128.230.45

35.87.210.123

172.210.77.31

46.166.165.95

18.133.77.74

129.211.212.43

45.32.113.133

43.135.3.17

152.42.198.168

142.93.74.10

159.223.0.196

159.203.133.189

147.182.150.146

159.89.1.205

161.35.186.219

68.183.195.95

14.225.254.224

51.178.137.204

163.172.171.199

198.255.103.64

14.225.255.166

14.225.255.32

172.235.56.104

83.244.163.202

14.225.217.103

14.225.217.7

185.158.94.217

172.105.27.15

145.131.8.169

170.64.234.99

107.175.0.167

172.232.190.135

34.68.58.67

45.133.238.221

185.43.4.70

143.198.70.94

81.208.161.44

45.145.229.103

158.101.188.29

37.187.118.185

64.226.91.107

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

1. **[CMTX-I-069102024] Malicious Domains used by Threat Actors**

Threat Overview

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

Prevention Measures:

>> Network administrator should implement email authentication protocols like SPF, DKIM, and DMARC to help detect and prevent email spoofing.

>> Inculcate the practice of verifying domain names and URLs before clicking on links, especially in emails.

>> Regular training sessions to raise awareness about the tactics used by attackers, such as typo-squatting and spear-phishing.

>> Implement Multi-Factor Authentication to add a layer of security.

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

aadhar-co.in

dc.crsorgi.gov.in.orjinal.site

gov.in.orjinal.site

crsorgi.gov.in.orjinal.site

documents.nia-gov.info

doh.nia-gov.info

dns.nia-gov.info

downloads.nia-gov.info

indiapotsgov.ink

orjinal.site

ucl.gov.in.aadhar-co.in

www.nia-gov.info

www.ucl.gov.in.aadhar-co.in

\*.aadhar-co.in

\*.nia-gov.info

\*.orjinal.site

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

1. **[CMTX-P102024114] Relay server Nodes used by Chinese actors**

A state-sponsored threat actor based in China has been observed using anonymization networks such as HiddenOrbit (RedRelay) and SuperJump, along with relay server nodes, to route their traffic and evade detection. The attackers leveraged active VPS nodes, compromised unpatched routers and IP cameras, to target internet-facing networks and security appliances of strategic interest. In this context, a list of relay server nodes actively used by the attackers has been compiled. The shared IP addresses are associated with small home and office (SoHo) routers and IP camera appliances. Additionally, IP profiling indicates that the attackers have specifically targeted unpatched CISCO RV340 VPN Router and Cyberoam devices.

Indicators of Compromise (IOCs):

- ---------------------------------------------------------------------------------

IP ADDRESSES

1.22.26.139

103.100.78.179

103.112.85.150

103.112.86.79

103.120.130.114

103.121.74.152

103.132.243.76

103.133.29.237

103.134.44.218

103.139.171.239

103.172.83.86

103.211.188.136

103.211.39.12

103.243.185.35

103.246.42.21

103.250.153.3

103.255.72.76

103.68.19.19

103.69.28.89

103.71.16.84

103.74.198.17

103.77.45.221

103.98.62.178

110.226.180.117

110.226.181.104

111.118.248.186

111.90.169.45

114.143.200.163

114.143.246.118

115.114.98.21

115.246.93.83

116.68.119.112

117.211.9.83

117.220.157.193

117.241.79.133

117.247.229.196

117.247.80.106

122.169.40.115

122.170.108.109

122.176.88.156

122.185.43.6

123.255.249.118

125.21.1.10

150.129.144.147

150.129.204.30

152.52.57.20

183.182.87.54

183.82.7.139

183.82.8.250

202.140.130.239

202.88.234.152

203.109.115.142

210.212.217.34

43.231.255.193

43.242.120.58

47.247.76.98

49.205.169.56

49.207.10.156

59.144.124.128

59.90.28.227

59.92.234.61

61.2.142.31

61.2.229.53

61.247.228.193

61.95.146.142

61.95.221.243

- ----------------------------------------------------------------------------------------

1. **[CMTX-P-102024124] SHADOWPAD (POISONPLUG) Malware Campaign**

Threat Overview

1. Threat Campaign: SHADOWPAD (POISONPLUG) Malware Campaign

ShadowPad is a sophisticated malware family that continues to be actively used by threat actors for espionage purposes. Its ability to evade detection and maintain persistence makes it a significant threat to targeted organizations. It is 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).

The malware has plug-in capabilities along with some other capabilities like self-destruction,can persist registry entries or services, and forward network connections. Social media sites have been used by POISONPLUG to host encoded command and control (C&C) orders.

It is designed to run in two stages; The first stage is a shellcode and second stage acts as an orchestrator for modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

Impacts:

Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : Multi modular backdoor

3. Severity: High

Indicators of Compromise (IOCs):

IP Addresses :Port

38.60.211.116

185.177.73.182

91.149.240.153

139.84.214.241

1. **[CMTX-P-102024134] PlugX Malware Campaign**

Threat Overview

1. Threat Campaign: PLUGX Malware Campaign

PlugX is a Remote Access Trojan (RAT), also known as SOGU, Korplug and Destroy RAT usually written in C. It is widely used by Chinese state-sponsored threat actors. This malware acts as a backdoor, allowing full control over the victim’s machine. Its notable features include the ability to execute commands on the affected machine to perform keylogging, capture screen activity, manage processes and services, etc. Its network protocol can vary between samples, potentially using HTTP, HTTPS, a custom binary protocol over TCP or UDP, and ICMP to communicate with the server. PlugX broadcasts UDP signals to devices on the same subnet as the victim and listens for responses to establish connections with other bots on the local network. 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.

Impacts:

o Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.

o System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.

o Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

2. Threat Type : MALWARE

3. Severity: High

Distribution Methods

• PlugX can also be delivered via phishing emails with malicious attachments, such as Windows shortcut (LNK) files and RAR archives. It employs techniques like DLL sideloading, DLL search order hijacking, and PowerShell commands for execution. Additionally, it can also spread through USB devices in a worm-like manner.

Indicators of Compromise (IOCs):

IP Addresses: Port

172.111.150.26

149.28.141.2

1. **[CMTX-I-080102024] Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

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

mail-panel.in

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

1. **[CMTX-102024025]- ACTIVE EXPLOITATION OF VEEAM VULNERABILITY (CVE-2024-40711) TO DEPLOY AKIRA AND FOG RANSOMWARE**

It has been reported that the threat actors are exploiting a critical deserialization vulnerability (CVE-2024-40711) in Veeam Backup & Replication (VBR) servers to deploy Akira & Fog ransomware to gain remote code execution and also leveraging compromised VPN credentials. For successful exploitation of the vulnerability, the attackers managed to create a local account “point” with administrative privileges to compromise VPN gateways without multifactor authentication and were running outdated software versions.

In the Fog ransomware incident, the attacker deployed it to an unprotected Hyper-V server, then used the utility rclone to exfiltrate data.

Fog ransomware has emerged as a significant cyber threat since its first identification in May 2024, targeting both Windows and Linux systems, affecting various sectors. The malware exploits compromised VPN credentials and critical vulnerabilities to gain initial access by creating local accounts with administrative privileges. Once inside a network, attackers utilize pass-the-hash techniques for lateral movement, often deploying the ransomware on unprotected Hyper-V servers.

The Akira ransomware gang, which emerged in March 2023, has rapidly established itself as a major cybersecurity threat. It is suspected that Akira has links to the defunct Conti ransomware gang. Operating under a ransomware-as-a-service (RaaS) model, Akira collaborates with other cybercriminals to carry out attacks. They utilize double extortion tactics by first stealing sensitive data, then encrypting it, and demanding two separate ransoms: one for decryption and another to prevent the public release of the stolen data. Initial access is frequently gained through compromised credentials.

Response Actions:

1. Disconnect Affected Systems: Immediately disconnect the infected system from the network to prevent further spread of the malware. Immediately address any signs of unauthorized access by changing passwords, reviewing access logs, and securing compromised accounts.

2. Remove Malicious Files: Use an antivirus or anti-malware tool to scan and remove malicious files. Most security software will allow you to perform a full system scan, identifying and quarantining or deleting threats.

3. Update Antivirus Definitions: Ensure your antivirus software is updated with the latest virus definitions. This can usually be done through the software's update function or by downloading the latest definitions from the vendor’s website.

4. Apply Security Updates: Ensure all systems and software are updated with the latest security patches to close any vulnerabilities exploited by the malware.

5. Implement 2FA for all sensitive accounts, particularly for webmail, virtual private networks (VPN), and accounts that access critical systems to add an additional layer of security. Also, update/replace out-of-support VPNs

6. Periodic Backups and restoration tests to check the restoration integrity.

7. The reference link provided below is a one-stop resource to help organizations reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover, including step-by-step approaches to address potential attacks:

[https://www.cisa.gov/resources-tools/resources/stopransomware-guide]https://www.cisa.gov/resources-tools/resources/stopransomware-guide

1. **[CMTX-I-808102024] Recent IOCs of Chinese Malware Campaign**

Chinese-based malware is often linked to state-sponsored groups or cybercriminal organizations operating from China. This malware can target various sectors, including government (defence, external affairs etc.), finance, technology, and critical infrastructure. Its objectives range from espionage and data theft to sabotage and disruption.

Recent IOCs associated with such campaign are as follows:

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

formainservercheap.com

currently resolving to 188.208.141.218

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

1. **[CMTX-102024025]- ACTIVE EXPLOITATION OF VEEAM VULNERABILITY (CVE-2024-40711) TO DEPLOY AKIRA AND FOG RANSOMWARE**

CVE-2024-40711 is a vulnerability in Veeam's software related to deserialization issues, potentially enabling attackers to execute arbitrary code. Such vulnerabilities usually occur when an application deserializes untrusted data, creating security risks if that data can be tampered with. It is being reported that different ransomware operators and threat actors are exploiting this vulnerability.

Impact: If exploited, the vulnerability could lead to unauthorized access or control over the affected system.

Affected Version:  Veeam Backup & Replication 12.1.2.172, 12.1.1.56 and earlier

1. **[CMTX-P102024035] ACTIVE EXPLOITATION OF IVANTI CLOUD SERVICE APPLIANCE(CSA)FLAWS BY NATION STATE ADVERSARY**

ALERT BRIEF:

It has been reported that a suspected nation-state adversary is exploiting three zero days to gain unauthenticated access to the CSA, enumerate users configured in the appliance, and attempt to access the credentials of those users.

Threat actors were observed exploiting and chaining these zero-day vulnerabilities to gain initial access and establish beachhead accessto to a victim’s network.

The Three vulnerabilities are as follows:

1). CVE-2024-8190 (CVSS score: 7.2) -

An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that, when exploited, allows a remote, privileged attacker to obtain unauthorized access.

This vulnerability is exploited in the wild, and weaponized code is publicly available.

A command injection flaw in the resource /gsb/DateTimeTab.php

2). CVE-2024-8963 (CVSS score: 9.4) -

An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that, when exploited, allows a remote attacker to obtain unauthorized access.

This vulnerability is exploited in the wild, and exploit code is not publicly available.

A path traversal vulnerability on the resource /client/index.php

3). CVE-2024-9380 (CVSS score: 7.2) -

An Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability exists that, when exploited, allows a remote, privileged attacker to execute arbitrary code.

This vulnerability is exploited in the wild, and exploit code is not publicly available.

An authenticated command injection vulnerability affecting the resource reports.php

Threat Type: Vulnerability

IOCs ASSOCIATED WITH ABOVE THREE VULNERABILITIES:

IPs

DOMAINS:

apiv5.serverbks.xyz

189f31ed7d.ipv6.bypass.eu.org

iowxuintgredogzgblrsmr2cx2e471bor.oast.fun

o.lencr.org

c67f045c2f.ipv6.1433.eu.org

URL:

[http://temp.sh/khkzg/DateTimeTab.php]http://temp.sh/khkzg/DateTimeTab.php

[http://temp.sh/vQuoW/reports.php]http://temp.sh/vQuoW/reports.php

[http://l8u6aolk4ejfsl9zeq6321zvwm2eq3.burpcollaborator.net]http://l8u6aolk4ejfsl9zeq6321zvwm2eq3.burpcollaborator.net

IPs:

54.77.139.23

34.250.195.30

216.131.75.52

24.166.100.255

67.217.228.92

69.49.88.235

45.61.136.189

3.248.33.252

38.207.159.76

193.189.100.197

23.236.66.97

74.62.81.162

206.189.156.69

51.91.79.17

156.234.193.18

208.105.190.170

1. **[CMTX-I-443102024] SideCopy Malware C&C IP**

SideCopy is a Pakistan based, sophisticated threat actor known for deploying malware to target individuals and organizations, particularly India based. Named for its technique of mimicking other well-known attack patterns, SideCopy aims to steal sensitive information and conduct espionage. This group is particularly notable for its spear-phishing campaigns and the deployment of custom malware to compromise target systems.

Recent Command and Control (C&C/ C2) IP of malware deployed by this threat actor is as follows:

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

173.249.18.251

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

1. **[CMTX-I-665102024] Malicious Domains used for Phishing**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

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

postngov.ink

indiapiost.top

postn.ink

postigov.top

postgovi.top

dhli.ink

dhlc.ink

indiaposttgovin.top

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

1. **[CMTX-I-389102024] Malicious Domains used by Threat Actors**

Malicious domains are websites created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, and email-based fraud.

>> Spear-phishing targets individuals by sending emails with links to malicious domains that mimic legitimate sites. Victims are tricked into providing sensitive information, like login credentials, which attackers steal.

>> Malicious domains can also be used to distribute malware. Attackers may set up a website that appears legitimate but secretly hosts harmful software.

>> Typo-squatting involves registering misspelled domains (e.g., g0v.in for gov.in) to trick users into believing they're on a legitimate site. Attackers use these domains in email-based attacks to send fraudulent messages that appear trustworthy.

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

fcsupgovin.in

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