**Cyber Security Advisories**

**Date: 16 September 2024**

1. **CMTX-I-080092024: Malicious Domain used by Pakistan based Threat Actors**

ALERT BRIEF:

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>------

mail-wing.in

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

Network administrators may take required action against the above malicious domain.

1. **CMTX-P-3840920249: Agent Tesla Malware Alert**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

85.9.47.248

89.39.83.184

45.252.248.26

195.252.110.253

213.189.52.181

86.105.155.116

188.127.239.250

47.76.82.23

138.199.16.35

35.198.173.35

92.205.7.112

93.216.70.207

193.141.65.39

46.175.148.58

61.19.247.49

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

1. **CMTX-P-8850920249: Raccoon Malware Alert**

Raccoon Stealer is one of the most well-known and widely used information-stealing malware families. The malware steals data from applications, including login credentials, credit card information, browsing history, cookies, and cryptocurrency wallet accounts.

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

88.119.161.19

146.19.173.87

185.244.48.191

193.142.147.59

94.142.138.108

62.204.41.87

185.26.236.51

65.109.175.35

91.219.237.3

147.45.44.25

62.113.112.27

94.103.93.70

193.187.174.250

178.20.41.15

91.103.252.65

94.103.88.64

94.142.138.80

94.142.138.19

94.142.138.228

91.103.252.49

91.103.252.156

188.119.112.93

5.206.224.46

45.144.29.243

146.19.170.52

45.89.55.21

77.91.77.96

88.119.161.188

188.215.229.203

91.103.252.230

94.103.84.253

95.216.189.84

95.164.17.125

94.142.138.213

77.232.39.101

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

1. **CMTX-P-7690920249: Amadey Malware Alert**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

45.9.74.141

45.9.74.166

45.9.74.182

45.9.74.164

77.91.78.17

188.40.122.96

78.46.242.112

31.41.244.158

62.204.41.89

79.137.203.59

207.154.243.184

49.12.117.51

78.47.9.120

185.215.113.9

188.40.187.155

193.233.20.14

5.75.139.35

62.204.41.87

62.204.41.252

5.188.118.7

193.3.19.154

176.113.115.201

77.73.134.66

193.106.191.201

185.11.61.121

34.90.130.132

159.65.6.6

185.174.136.244

62.182.156.153

194.67.71.55

77.73.133.72

95.163.50.150

193.233.20.36

193.166.255.171

34.91.34.135

193.143.1.5

80.76.42.67

212.32.237.101

87.237.202.67

5.79.71.205

89.37.121.88

35.198.88.107

194.67.71.125

91.208.52.21

79.110.251.71

176.111.174.109

194.67.71.4

194.67.71.19

194.67.71.25

194.67.71.29

194.67.71.45

194.67.71.148

194.67.71.156

194.67.71.173

45.143.81.230

109.106.254.145

165.231.2.187

188.40.141.211

77.220.215.196

34.88.137.133

185.215.113.205

88.221.123.218

62.204.41.151

31.41.244.146

2.22.28.159

85.209.90.48

212.162.152.160

81.171.8.143

89.163.249.231

213.202.229.103

3.126.205.164

193.3.19.19

185.22.66.16

46.105.133.232

62.182.82.201

5.79.71.225

45.66.8.181

5.183.217.131

172.94.15.211

37.49.230.66

80.85.141.16

195.2.70.68

185.215.113.204

45.9.74.5

95.100.158.42

185.56.218.10

95.216.204.6

212.32.237.91

159.100.251.128

178.170.48.24

92.46.53.222

93.186.201.118

92.205.213.10

46.21.97.151

45.137.64.184

185.237.146.247

198.144.120.67

128.214.222.204

2.18.177.31

151.236.21.122

80.89.239.48

91.108.98.136

212.162.152.224

109.191.32.62

194.150.215.237

5.181.216.209

151.106.124.142

156.67.222.32

80.248.236.114

23.0.174.24

212.32.237.90

46.8.229.59

34.242.73.233

194.67.71.69

2.22.241.49

89.163.210.241

45.9.74.15

80.89.239.253

95.100.158.19

95.101.193.200

2.23.94.56

194.67.71.157

23.34.45.28

2.22.241.11

23.55.110.51

194.67.71.54

194.67.71.134

176.111.174.114

2.22.28.189

5.104.108.23

89.163.152.111

31.41.244.237

101.99.75.138

185.172.128.5

194.67.71.155

91.207.126.8

194.67.71.145

147.45.47.155

217.69.139.122

62.122.170.171

46.163.119.134

34.77.5.52

2.22.28.138

23.55.110.79

92.205.175.71

185.237.206.98

45.84.226.252

62.204.41.6

82.202.243.188

194.67.71.52

194.67.71.103

194.87.206.143

213.108.249.95

91.187.132.11

217.21.74.145

147.96.1.15

176.97.64.128

193.233.20.25

78.153.144.60

185.237.144.175

194.67.71.166

185.232.14.78

136.243.106.238

5.61.236.229

178.170.48.132

93.55.123.25

194.67.71.7

194.67.71.18

194.67.71.33

194.67.71.60

194.67.71.91

194.67.71.106

194.67.71.121

194.67.71.123

91.228.238.70

109.206.161.43

109.206.161.72

194.67.71.154

213.202.223.111

188.42.30.244

109.206.161.114

77.91.124.1

46.21.101.120

213.202.223.112

31.214.168.209

109.233.110.90

93.115.20.110

89.108.106.29

194.67.71.5

194.67.71.41

194.67.71.65

194.67.71.93

194.67.71.98

194.67.71.172

193.26.6.207

193.42.33.74

193.42.32.29

185.196.8.176

185.196.8.126

194.105.56.41

185.215.113.101

79.137.203.19

5.188.88.223

194.67.71.17

194.67.71.120

194.67.71.90

31.41.244.15

212.32.237.92

95.100.158.57

45.92.178.115

188.209.214.83

31.177.76.32

45.10.111.18

193.182.189.222

79.127.127.34

185.80.0.189

212.27.63.114

23.55.163.58

77.91.124.20

92.205.55.192

93.170.52.17

194.67.71.46

194.67.71.85

194.67.71.108

194.67.71.112

194.67.71.144

194.67.71.146

37.148.205.26

80.66.75.214

91.203.4.45

34.90.10.178

194.67.71.88

195.210.46.17

195.210.46.49

154.62.105.82

194.163.35.221

185.233.43.13

35.233.77.94

212.162.57.144

185.81.129.87

148.6.2.104

37.48.67.204

31.31.196.161

31.41.244.10

185.46.11.215

194.67.71.110

138.201.203.107

37.220.87.70

185.215.113.38

194.67.71.138

3.126.57.221

99.81.95.247

185.216.143.2

88.212.201.204

185.18.81.214

31.177.80.32

194.67.71.3

194.67.71.10

194.67.71.22

194.67.71.42

194.67.71.186

93.87.76.167

45.15.156.208

77.91.78.118

194.67.71.136

213.202.223.115

80.150.6.143

92.204.58.67

45.93.20.174

129.241.160.103

194.67.71.74

194.67.71.76

194.67.71.105

194.67.71.187

194.67.71.196

194.67.71.197

195.123.210.178

194.67.71.165

72.246.29.124

185.216.143.29

185.48.106.3

193.53.246.163

5.182.210.45

5.63.159.35

194.67.71.13

194.67.71.15

194.67.71.16

194.67.71.34

194.67.71.40

194.67.71.53

194.67.71.77

194.67.71.79

194.67.71.99

194.67.71.126

194.67.71.143

194.67.71.147

194.67.71.162

194.67.71.163

194.67.71.175

194.67.71.177

194.67.71.181

217.20.156.158

144.122.145.146

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

1. **CMTX-P-6350920249: Trickbot Malware Alert**

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

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

41.77.134.250

175.184.232.234

27.109.116.144

103.9.188.78

103.111.55.46

96.9.77.142

177.190.76.82

103.201.142.30

103.242.104.43

34.249.180.228

194.87.94.14

172.232.238.17

94.140.5.5

123.231.180.130

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

1. **CMTX-P-7980920249: Ursnif Malware Alert**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

87.106.18.141

64.120.88.229

18.141.10.107

133.125.38.187

13.251.16.150

91.195.240.85

156.146.44.17

156.146.44.18

156.146.44.16

156.146.45.183

34.242.73.233

3.126.57.221

99.81.95.247

3.126.205.164

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

1. **CMTX-P-4400920249: Redline Malware Alert**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

185.196.9.26

185.215.113.22

185.215.113.67

147.45.47.36

88.99.151.68

91.92.248.194

65.21.18.51

95.179.163.21

185.215.113.9

31.42.189.18

103.211.207.57

103.74.101.154

103.167.90.34

5.42.92.213

89.23.97.185

135.236.96.237

5.189.138.247

147.45.47.53

45.66.231.214

147.45.44.148

135.181.10.210

152.89.198.155

94.141.120.25

65.21.175.7

31.177.108.40

93.115.91.27

20.52.165.210

89.23.98.87

147.45.44.16

147.45.47.251

185.215.113.25

95.179.250.45

38.180.201.126

147.45.44.173

109.248.144.232

103.245.237.11

45.89.53.206

45.140.147.183

207.246.113.185

172.205.128.102

135.181.10.208

176.111.174.140

193.233.113.217

185.218.125.157

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

1. **CMTX-P-9850920249: SocGholish Malware Alert**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

185.216.114.10

77.245.56.14

31.220.15.143

103.249.111.96

45.130.201.24

92.53.96.139

217.160.0.215

192.46.231.103

93.190.41.79

195.24.68.25

217.160.0.220

217.160.0.246

45.130.201.23

185.187.241.36

185.26.122.54

103.181.142.39

5.101.115.147

92.204.68.47

145.239.23.7

49.245.96.145

213.186.33.16

27.254.141.224

35.215.148.34

119.59.103.1

171.245.245.214

164.52.214.211

92.205.49.95

45.43.183.213

117.54.114.102

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

1. **CMTX-P-1940920249: Emotet Malware Alert**

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

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

81.213.175.132

202.79.24.136

138.68.87.218

61.76.222.210

77.74.78.80

159.65.6.6

115.79.195.246

51.38.124.206

51.75.33.127

168.197.45.36

62.171.142.179

5.196.108.185

173.249.6.108

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

1. **CMTX-P-5170920249: Qbot Malware Alert**

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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

195.200.5.249

18.173.205.25

18.173.205.52

18.173.205.106

18.173.205.33

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

1. **CMTX-I-808092024: CrimsonRAT- APT36 campaign**

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

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 IP of malware deployed by this threat actor is as follows:

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

81.17.102.55

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

1. **CMTX-P092024025: SUPER JUMPER COVERT NETWORK**

Several Chinese state-sponsored threat groups use a private anonymization network or relay C2 network called as "SUPER JUMPER COVERT NETWORK" to obscure their malicious activities and make attribution & tracking more complicated.

SuperJump is associated with at least four distinct Chinese state-sponsored groups, including RedLima (APT15), RedKilo, TAG-104, and APT5.

This network comprises several hundred Virtual Private Server (VPS) nodes and some compromised devices, which facilitate the routing of threat actor traffic. These threat actor groups particularly using Super Jumper covert Network target internet-facing network and security appliances, conducting reconnaissance, exploitation activities and other cyber espionage operations. It also has overlapping characteristics with a network known as SPACEHOP, further emphasizing its role in supporting Chinese state-sponsored cyber activities.

Super Jump nodes have been configured in such a way that there is communication of C2 traffic for Chinese malwares like ShadowPad,PlugX etc.

The external operational infrastructure has been managed by the network and used to communicate with target networks.

Following activity has been observed by SuperJump network:

- -Relay ShadowPad and PlugX C2 traffic

- -Administer downstream operational infrastructure that is then used to interact with target networks

- -Direct reconnaissance and exploitation activity from SuperJump exit/egress nodes

- -Chinese threat actor group used SuperJump to exploit a zero-day Citrix NetScaler ADC vulnerability (CVE-2022-27518)

- - Some other malware families like ArcSilt ,ArcaneVoid etc are also associated with Super Jump Covert Network

1. **CMTX-I-053092024: Mythic Malware- APT36 campaign**

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 of Mythic malware is as follows:

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

206.189.134.185

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

1. **CMTX-I-443092024: Phishing Campaign Targeting Credentials via Telegram API**

CERT-In has observed a recently used phishing tactic, wherein the Pakistan based threat actors are sending phishing emails designed to capture user credentials. Once they obtain these credentials, they perform malicious activities by executing HTTP POST requests to the following URL:

Type: POST

URL: hXXps://api.telegram.org

The use of the Telegram API in this context suggests that the attackers are exfiltrating the stolen credentials or other sensitive data through Telegram. Telegram is a genuine application and is a popular messaging platform. Hence, this method allows them to quickly and covertly transfer data without raising immediate suspicion. Moreover, it is not required Telegram application to be installed in the victim machine for the data to be POST on the the URL.

Earlier also (CMTX-I-137032024 dated and CMTX-I-514052024 dated 31/05/2024) we had reported malware making use of popular messaging platforms for exfiltrating data on victim's machine.

Action Required:

- - Network administrators must monitor traffic to the URL mentioned above. Any POST requests to hXXps://api.telegram.org should be scrutinized to determine if they are legitimate or if they are related to this phishing/ malware activity.

- - If any unauthorized POST requests are detected, these should be investigated, and remedial measures should be taken.

1. **CMTX-P092024986: ToneShell Malware Campaign**

Please find additional IOC's of ToneShell Malware Campaign.

Indicators of Compromise (IOCs):

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

IP ADDRESSES:

43.246.209.139

45.115.236.142

45.115.236.143

103.27.109.52

103.27.109.206

103.43.16.65

137.220.251.44

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

1. **CMTX-I-445092024: Malicious Domain used by Pakistan based 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>------

section-mail.in

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

1. **CMTX-I-446092024: Phishing Campaign Targeting Credentials via Webex API**

Threat Overview

CERT-In has observed a recently used phishing tactic, wherein the threat actors are sending phishing emails designed to capture user credentials. Once they obtain these credentials, they submit it to the following URL using REST API:

URL: hXXps://webexapis.com

The use of the Webex API in this context suggests that the attackers are exfiltrating the stolen credentials or other sensitive data through Webex.Webex REST API allows developers to integrate various Webex functionalities such as Messaging,meeting and Device management.Hence, this method allows them to quickly and covertly transfer data without raising immediate suspicion. Moreover, it is not required Webex application to be installed in the victim machine for the data to be POST on the the URL.

Earlier also (CMTX-I-137032024 dated & CMTX-I-514052024 dated 31/05/2024 and CMTX-I-443092024 dated 04/09/2024) we had reported malware making use of popular messaging platforms for exfiltrating data on victim's machine.

Action Required:

- - - Network administrators must monitor traffic to the URL mentioned above. Any POST requests to hXXps://webexapis.com should be scrutinized to determine if they are legitimate or if they are related to this phishing/ malware activity.

- - - If any unauthorized POST requests are detected, these should be investigated, and remedial measures should be taken.

1. **CMTX-P-092024035: KTLVdoor Malware**

Threat Overview

Threat Campaign: KTLVdoor Malware

The Chinese threat actor "Earth Lusca" created a new multiplatform backdoor known as "KTLVdoor". The malware is written in Golang language and can run on Linux and Microsoft Windows platforms. It uses a lot of obfuscation techniques to disguise as genuine system utilities like Java and SSHD. Some of the capabilities of the malware include file manipulation, command execution,remote port scanning, renaming functions & packages with random strings, obfuscating embedded strings, and stripping symbols, to hinder reverse engineering and make samples more difficult to analyze.

The backdoor performs various functions on victim's machine:

• Creates an encrypted connection using AES-GCM between with its command-and-control (C2) server.

• Depending on the setup, uses several protocols for C2 connections, including HTTP, TCP, DNS, and Internet Control Message Protocol (ICMP).

• Compiles and transmits system data to the C2 server.

• Can execute commands, manipulate files, scan ports, set up proxies to route network traffic, and insert shellcode, among other activities.

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.

Threat Type: Backdoor

Severity: High

Mitigation and Recommendations:

1.Mandatory MFA Implementation: Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms. MFA adds an additional layer of security by requiring users to provide two or more verification methods before accessing accounts.

2.Enhanced Protection for Critical Accounts: Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security. This added layer of protection is crucial for safeguarding sensitive and high-privilege systems.

3.Comprehensive Password Policy: Establish and enforce a robust password policy across the organization. This policy should mandate that passwords include a minimum of 8 characters and incorporate a mix of uppercase and lowercase letters, numbers, and special characters. A strong password policy helps mitigate the risk of unauthorized access due to weak or easily guessable passwords.

4.Regular Password Resets: Implement a process for regular password resets enterprise-wide. This practice ensures that passwords are updated periodically, reducing the likelihood of compromised credentials remaining in use for extended periods.

5.Deploy Robust Anti-Malware and Virus Software: Ensure that all devices within the organization are equipped with strong, up-to-date anti-malware and antivirus software. Regularly update this software to protect against the latest threats. Effective anti-malware solutions can detect and block malicious software that attempts to install or execute on a device.

6.Block Malicious Sites and Links: Configure your anti-malware and antivirus software to prevent access to websites and online resources that are known to distribute malicious links or attachments. This proactive approach helps to safeguard users from inadvertently visiting harmful sites that could compromise device security.

7. Update IDS/IPS Signatures: Ensure your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have the latest signatures for KTLVdoor malware.

8. By enhancing logging, implementing continuous monitoring, and conducting systematic threat hunts on key organizational choke points, organizations can better detect and counteract advanced persistent threats such as KTLVdoor.

9. User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts. Promoting awareness can reduce the likelihood of successful infections.

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P-092024035]

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

Indicators of Compromise (IOCs):

HASHES:

d18019064e5903dcf7c29921c10a7a90176cccd55d9cf3ba1e3e9805c1364df1

c0b1deaa2598936c284684b50a652f98771a129e882f382ac011d5ab984fd132

18e2b7df374a838a57ebf3186b13a26e523cf964afde50b7ba765ed4d5509670

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

Tactics, Techniques, and Procedures (TTPs):

T1497.001 (System Checks)

T1082 (System Information Discovery)

T1497.001 (System Checks)

T1083 (File and Directory Discovery)

T1124 (System Time Discovery)

T1106 (Native API)

T1622 (Debugger Evasion)

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

1. **CMTX-P092024045: Cicada3301 Ransomware**

Threat Overview

Threat Campaign: Cicada3301 Ransomware

A new ransomware group called as "Cicada3301 Ransomware" is active in the cyber threat landscape and it operates as Ransomware-as-a-Service (RaaS). It uses double-extortion technique by encrypting files and threatening to leak sensitive data to compel victims into paying ransoms. The group uses Rust-based ransomware that has commonality with ALPHV ransomware, utilizing the ChaCha20 encryption algorithm while also leveraging a botnet called Brutus for credential brute-forcing. It uses legitimate tools to run programs remotely and encrypts files. The ransomware targets small to medium-sized businesses and takes advantage of vulnerabilities to gain initial access.

Impacts:

Threat Type : Ransomware

Severity: High

Affected Systems: Windows and Linux

Mitigation and Recommendations:

• It is strongly advised that downloading should be done only from reputable and official sources. Since programs obtained from third parties may include malware, all programs must be updated and activated using the features and tools supplied by authorized developers.

• It is also advised to exercise caution when browsing because dangerous and fraudulent content frequently looks innocent and real. It's important to handle incoming emails and other messages carefully. It is not advisable to open attachments or links included in suspicious or irrelevant emails since they may spread infection.

• Installing and maintaining an up-to-date reliable anti-virus program is crucial for user and device safety.

• Remove unnecessary access to administrative shares, particularly ADMIN$ and C$. If ADMIN$ and C$ are required for operational purposes, restrict access to only essential service or user accounts and continuously monitor for any unusual activity. Employ a host-based firewall to permit connections to administrative shares via SMB solely from a restricted group of administrator machines.

Preventive Measures:

• Anomaly Monitoring: Implement monitoring systems to detect unusual login activity or unauthorized access attempts that may indicate the use of stolen credentials.

• Password Management: Employ a trusted password manager to securely store and manage your passwords. These tools encrypt your passwords and sensitive data, increasing their security significantly compared to storing them in your browser. Also ensure that autofill and password saving features in your browser settings are disabled. This prevents your browser from automatically storing passwords as you enter them, reducing the risk of unauthorized access.

• User Education: Train users to recognize phishing attempts with context aware subjects and themes and mails particularly coming from trusted /compromised email accounts . Promoting awareness can reduce the likelihood of successful infections.

• Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

• Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively address malware infections and minimize damage.

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. A list of recent malware hashes are provided in Annexure.

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. Enable Two-Factor Authentication (2FA): Implement 2FA for all sensitive accounts, particularly for webmail, virtual private networks, and accounts that access critical systems to add an additional layer of security

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

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

Annexure

CERTIn-Threat Intelligence ID- [CMTX-P092024045]

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

Indicators of Compromise (IOCs):

HASH:

7b3022437b637c44f42741a92c7f7ed251845fd02dda642c0a47fde179bd984e

IP:

91.92.249.203

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

1. **CMTX-I-818092024: 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/Suspicious Domains>---------

drdo.gov.in.aboutcase.nl

usemembassymumbai-gov.info

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

Please note: Parent domain aboutcase.nl has already been covered via CMTX-I-501072024 dated 30/07/2024

As threat actors are creating several sub-domains for malicious parent domains on a regular basis, hence it is necessary to block the parent domain as well as all of its possible sub-domains beforehand. This could be done by blocking the parent domain as a wildcard domain '\*.aboutcase.nl', where \* corresponds to the wildcard.

Network administrators may take required action against the above malicious domains.

1. **CMTX-I-023092024: Mythic Malware- APT36 campaign**

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 of Mythic malware is as follows:

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

139.59.34.138

165.232.180.251

178.128.243.90

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

1. **CMTX-I-025092024: Mythic Malware- APT36 campaign**

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 of Mythic malware and its associated IPs are as follows:

- ------------< C&C and Associated IPs>---------

157.245.139.146

206.189.134.185

159.89.165.86

143.198.64.151

- ------------</C&C and Associated IPs>---------

1. **CMTX-I-025082024: Mythic Malware- APT36 campaign**

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 of Mythic malware are as follows:

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

138.68.134.123

170.64.132.144

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

1. **CMTX-P-092024045: 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.

Mitigation and Recommendations :

1. Patch Management: Regularly update and patch all software, operating systems, and applications to close vulnerabilities that malware could exploit.

2. Endpoint Protection: Utilize robust endpoint protection solutions, including antivirus and anti-malware tools, to detect and block known threats.

3. Network Segmentation: Divide your network into segments to limit the spread of malware. Ensure that critical systems and sensitive data are isolated from less secure network areas.

4. Access Controls: Implement strict access controls and adhere to the principle of least privilege, ensuring that users and systems have only the permissions they need.

5. Regular Backups: Maintain regular, secure backups of critical data and systems. Store backups offline or in a manner that prevents network access.

6. Security Awareness Training: Educate employees on cybersecurity best practices, including how to recognize phishing attempts and handle suspicious emails or attachments.

7. Intrusion Detection and Prevention: Implement intrusion detection and prevention systems (IDPS) to monitor network traffic and identify unusual or malicious activities.

8. Application Whitelisting: Use application whitelisting to ensure only approved applications can run on your systems, blocking unauthorized or potentially harmful software.

9. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address weaknesses in your security posture.

10. Threat Intelligence: Stay updated on emerging threats and vulnerabilities by subscribing to threat intelligence services for the latest information on new malware and attack techniques.

11. Incident Response Plan: Develop and regularly update an incident response plan to ensure a swift and effective response in the event of a security breach.

12. Monitoring and Logging: Implement comprehensive monitoring and logging practices to detect and analyze unusual activities that may indicate a breach.

13. 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].

14. 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.

15. 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.

16.Regularly monitor all outbound traffic, particularly traffic destined for newly registered domains or Dynamic DNS (DDNS) and Domain Generation Algorithms (DGA) domains.

17. Recommend to monitor DNS traffic to detect DNS tunneling such as Unusual DNS request/ response. Watch for anomalies like unusually large DNS queries or responses, an excessive number of DNS requests from a single source, or large amounts of data within DNS queries. or requests directed at unfamiliar or suspicious domains, as these can indicate potential tunneling activity.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-092024045

Indicators of Compromise (IOCs):

IP Addresses: Port:Last seen: Country Code

199.247.18.127

45.135.119.132

203.69.170.86

38.54.105.187

45.204.2.24

13.212.54.150

45.204.2.26

45.152.65.199

167.179.109.96

103.192.226.100

1.94.136.42

202.144.194.101

137.220.183.79

45.195.69.203

45.136.14.160

143.92.56.71

172.111.233.35

103.79.120.81

202.91.39.201

96.9.212.107

103.234.72.190

183.82.125.238

172.111.233.114

185.243.115.134

1. **CMTX-P-092024055: 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:

1. 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.

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

3. 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 : Multimodular backdoor

3. Severity: High

Distribution Methods:

• ShadowPad is often delivered through DLL sideloading techniques and exploits vulnerabilities in software such as Microsoft Office IME binary or Microsoft Exchange Server. It can also been distributed through supply-chain attacks

Mitigation and Recommendations :

1. Patch Management: Regularly update and patch all software, operating systems, and applications to close vulnerabilities that malware could exploit.

2. Endpoint Protection: Utilize robust endpoint protection solutions, including antivirus and anti-malware tools, to detect and block known threats.

3. Network Segmentation: Divide your network into segments to limit the spread of malware. Ensure that critical systems and sensitive data are isolated from less secure network areas.

4. Access Controls: Implement strict access controls and adhere to the principle of least privilege, ensuring that users and systems have only the permissions they need.

5. Regular Backups: Maintain regular, secure backups of critical data and systems. Store backups offline or in a manner that prevents network access.

6. Security Awareness Training: Educate employees on cybersecurity best practices, including how to recognize phishing attempts and handle suspicious emails or attachments.

7. Intrusion Detection and Prevention: Implement intrusion detection and prevention systems (IDPS) to monitor network traffic and identify unusual or malicious activities.

8. Application Whitelisting: Use application whitelisting to ensure only approved applications can run on your systems, blocking unauthorized or potentially harmful software.

9. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address weaknesses in your security posture.

10. Threat Intelligence: Stay updated on emerging threats and vulnerabilities by subscribing to threat intelligence services for the latest information on new malware and attack techniques.

11. Incident Response Plan: Develop and regularly update an incident response plan to ensure a swift and effective response in the event of a security breach.

12. Monitoring and Logging: Implement comprehensive monitoring and logging practices to detect and analyze unusual activities that may indicate a breach. Regularly monitor all outbound traffic, particularly traffic destined for newly registered domains or Dynamic DNS (DDNS) and Domain Generation Algorithms (DGA) domains.

13. Recommend to monitor DNS traffic to detect DNS tunneling such as Unusual DNS request/ response. Watch for anomalies like unusually large DNS queries or responses, an excessive number of DNS requests from a single source, or large amounts of data within DNS queries. or requests directed at unfamiliar or suspicious domains, as these can indicate potential tunneling activity.

Annexure

CERTIn-Threat Intelligence ID- CMTX-P-092024055

Indicators of Compromise (IOCs):

IP Addresses: Port

154.31.217.197

8.217.0.193

103.27.111.247

128.14.105.154

46.246.98.47

192.109.119.100

182.78.203.26

66.42.37.139

103.255.118.149

45.80.215.133

207.246.106.76

95.179.221.218

156.244.2.26

103.56.19.182

95.164.10.67

199.247.2.134

38.60.196.212

199.247.23.86

45.249.89.54

38.60.250.74

151.236.23.49

139.99.50.68

202.182.118.85

45.76.190.240

154.90.59.6

141.164.36.138

103.158.190.167

103.255.118.150

31.192.107.196

192.71.213.155

95.179.249.161

109.207.171.191

64.31.63.110

65.20.69.67

139.180.223.116

45.204.2.25

45.77.9.96

103.205.211.174

141.164.50.114

45.76.189.33

64.176.49.76

45.158.168.113

1. **CMTX-P092024996: Mallox Ransomware**

Threat Overview

Threat Campaign: Mallox Ransomware

Aliases: FARGO, TargetCompany, Tohnichi and Xollam

Mallox Ransomware is currently active in cyberspace and targeting unsecured Microsoft SQL Servers. The ransomware group also uses brute force technique to compromise publicly exposed MS SQL instances to infiltrate into the targeted network. After gaining access, the attackers use a command line and PowerShell to download the Mallox ransomware payload from a remote server. Like other prominent ransomware groups it also uses on double extortion technique and appends the extension ".mallox" to encrypted files.

Threat Type : Ransomware

Severity: High

Affected Systems: Windows and Linux

Mitigation and Recommendations:

Preventive Measures:

o Patch management: Regularly patch and update software and operating systems to the latest available versions.

o Comprehensive Password Policy: Establish and enforce a robust password policy across the organization. This policy should mandate that passwords include a minimum of 8 characters and incorporate a mix of uppercase and lowercase letters, numbers, and special characters. A strong password policy helps mitigate the risk of unauthorized access due to weak or easily guessable passwords.

o Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation] and unknown connections in the network traffic.

o Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

o Incident Response Plan: Develop and maintain an incident response plan to address malware infections quickly and effectively and minimize damage.

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

Indicators of Compromise (IOCs):

HASH:

9b772efb921de8f172f21125dd0e0ff7

79b60f8b5052a9d4cc0c92c2cdc47485

e713f05a62914496eef512a93a611622

3829a09bca120206883539eb33d55311

a8e214683307adaff39783dc656b398a

ac1a255e5c908f12ef68a45fc0043b16

b1b42fa300d8f43c6deb98754caf0934

3762f98a55f0ec19702f388fc0db74e2

6bd93817967cdb61e0d7951382390fa0

c494342b6c84f649dece4df2d3ff1031

16e708876c32ff56593ba00931e0fb67

d32a3478aad766be96f0cdbda1f10091

e98b3a8d2179e0bd0bebba42735d11b7

98c7f6b6ddf6a01adb25457e9a3c52b8

b13a1e9c7ef5a51f64a58bae9b508e62

URLs:

91.215.85.142%2FQWEwqdsvsf%2Fap.php

whyers.io%2FQWEwqdsvsf%2Fap.php

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

1. **CMTX-P092024106: BlackByte Ransomware**

Threat Overview

Threat Campaign: BlackByte Ransomware

BlackByte ransomware is a Ransomware-as-a-Service (RaaS) model where they rent out their ransomware to affiliates who can carry out intrusions into organizations and deploy it to encrypt files. The ransomware uses an obfuscated launcher to hide its nature on a target machine. Initial access is commonly achieved through exploiting vulnerabilities such as CVE-2024-37085 in VMware ESXi hypervisors or leveraging valid credentials purchased from Initial Access Brokers.The BlackByte uses different system commands to delete backups and shadow copies to thwart data recovery.

Threat Type : Ransomware

Severity: High

Mitigation and Recommendations:

Preventive Measures:

o Patch management: Regularly patch and update software and operating systems to the latest available versions.

o Comprehensive Password Policy: Establish and enforce a robust password policy across the organization. This policy should mandate that passwords include a minimum of 8 characters and incorporate a mix of uppercase and lowercase letters, numbers, and special characters. A strong password policy helps mitigate the risk of unauthorized access due to weak or easily guessable passwords.

o Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation] and unknown connections in the network traffic.

o Network Segmentation: Divide your network into segments to limit the spread of malware if an infection occurs, helping to contain and control the impact.

o Incident Response Plan: Develop and maintain an incident response plan to address malware infections quickly and effectively and minimize damage.

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

Indicators of Compromise (IOCs):

IP ADDRESSES:

185.93.6.31

45.9.148.114

109.206.243.59

185.225.73.244

DOMAINS:

Mega.co.nz

exe.mbt.tg

exe.mbt.th

exe.mbt.sb

myvisit.alteksecurity.org

URL's:

hxxp://gfs270n392.userstorage.mega.co.nz/ul/PCfY6R3GKGjIEQK2tzWLODSlhG-h5NbxGHdNAToANCzjKK8Z6kdCiqshxM6ctHDKpLU09-YobgYybaQkCnpwnw/4718592

hxxp://gfs262n303.userstorage.mega.co.nz/ul/f\_re9dP6f9G8GAJhd3p43aJnvHnw7rCHLumJV-MXDlaL2RaSQQrPH1BYStJHWy4JkPgJ13KczuiJoOl0iwjxDA/15204352

hxxp://gfs206n108.userstorage.mega.co.nz/ul/aX72PSSxERHKJwLdWCCOmsJQRioP7N6kcAltRRTbAgwGtNzcsdYa\_7HTb4ToVV\_HcVPORXotYAF5WqFAsmAOKA/15204352

hxxp://gfs208n174.userstorage.mega.co.nz/ul/z6nR8uTohiga4QeILJsXcAWlt05Vhu2XiDlne\_Qag-rgAmZkK2aZMvYrWC5FHRebBpMoxYZEEqSStHyvU6SnWQ/6815744

hxxp://gfs214n129.userstorage.mega.co.nz/ul/wVJUlrn9bMLekALaMZx\_o5FeK-U1oG9q4CWqHGNslUnVY2-BgJcEUxIJX9O4fXEWkt-x80LeAr7Jz9gXTCwzDA/2752512

hxxp://gfs204n140.userstorage.mega.co.nz/ul/\_Amu75VCTCu6BgIdFs8ZgHPyHqBFm5Cj8bV1xkM5QFt2T0x-9C\_KlHQAQ3kX4bzj8jgmyK9-dlbmx9ef6Y9JDw/1966080

hxxp://gfs206n171.userstorage.mega.co.nz/ul/9Y39ts0Mp6xtige0-wHhmMG74YgASgG1UhZYfzl\_fh8TN\_TQo1gSa92TNe\_HTBxvOTirA0yfouEE74-Y3Cy1Tw/81264640

hxxps://g.api.mega.co.nz

hxxps://g.api.mega.co.nz/cs?id=1674017543

hxxps://myvisit.alteksecurity.org/t

hxxps://temp.sh/szAyn/sys.exe

hxxp://45.9.148.114/forest.png

hxxp://185.93.6.31/mountain.png

HASHES:

47870de17eb7d1758d705b593ac75cce

c3ce2163fa601199380c21e22a653c0c

b020684717fe72dd398e0be5c2a36c809221f206

03011da0f7f2e04ddfc9b8d2356dc4cb

0f7e3c94b2d3df1722950ff472a06b3f96f65399

8d42417ef02e50249fb7f97fcbfbbb8b

c27e85de8db2f634db44baee4273bbeeb152435c

de9d361c8e00cf8fa1c1f96844a74cdc121809da

07a9b1fdfb383a2b1d0172802ce01033

351198e557151fa0f4eea2b3bb8771d180fa8432

4d2da36174633565f3dd5ed6dc5033c4

cd7034692d8f29f9146deb3641de7986

d63a7756bfdcd2be6c755bf288a92c8b

eed7357ab8d2fe31ea3dbcf3f9b7ec74

695e343b81a7b0208cbae33e11f7044c

296c51eb03e70808304b5f0e050f4f94

0c7b8da133799dd72d0dbe3ea012031e

a77899602387665cddb6a0f021184a2b

1473c91e9c0588f92928bed0ebf5e0f4

28b791746c97c0c04dcbfe0954e7173b

52b8ae74406e2f52fd81c8458647acd8

1785f4058c78ae3dd030808212ae3b04

b8e24e6436f6bed17757d011780e87b9

8dfa48e56fc3a6a2272771e708cdb4d2

4ce0bdd2d4303bf77611b8b34c7d2883

c010d1326689b95a3d8106f75003427c

ae6fbc60ba9c0f3a0fef72aeffcd3dc7

405cb8b1e55bb2a50f2ef3e7c2b28496

11e35160fc4efabd0a3bd7a7c6afc91b

659b77f88288b4874b5abe41ed36380d

151c6f04aeff0e00c54929f25328f6f7

959a7df5c465fcd963a641d87c18a565

5f40e1859053b70df9c0753d327f2cee

df7befc8cdc3c5434ef27cc669fb1e4b

51f2cf541f004d3c1fa8b0f94c89914a

d9e94f076d175ace80f211ea298fa46e

8320d9ec2eab7f5ff49186b2e630a15f

cea6be26d81a8ff3db0d9da666cd0f8f

31f818372fa07d1fd158c91510b6a077

a9cf6dce244ad9afd8ca92820b9c11b9

7139415fecd716bec6d38d2004176f5d

c13bf39e2f8bf49c9754de7fb1396a33

5c0a549ae45d9abe54ab662e53c484e2

ad29212716d0b074d976ad7e33b8f35f

d4aa276a7fbe8dcd858174eeacbb26ce

9344afc63753cd5e2ee0ff9aed43dc56

e2eb5b57a8765856be897b4f6dadca18

58e8043876f2f302fbc98d00c270778b

d2a15e76a4bfa7eb007a07fc8738edfb

e46bfbdf1031ea5a383040d0aa598d45

7c3782f1285f48d8c9a17be8db65b02d

2d8e4f38b36c334d0a32a7324832501d

23c893984e388278e7996b70f220aa28

5483da573c6a239f9a5d6e6552b307b0

1eee62ae28e6b20f4100ce4a02fedd94

a62d5c8ef4d626febfcd2c00898c6c27

03dc3de9d456453ea5ccc37fef77132e

72b9466693470b98ad6be6dd151e46e9

f6f11ad2cd2b0cf95ed42324876bee1d83e01775

13c6c472a1dfcb2cc03bd65a3f122e8230255821

c90f32fd0fd4eefe752b7b3f7ebfbc7bd9092b16

c2eaca8799d335954ef3d9a1867ec1b629ca4f1a

ff1b176f0885c730516e798aaa14cff694f34a3b

854e020efefbf393e04d897b6b0b83ef92fd2db8

b596dff6057ebde53c300fee089e0e5663ebeee1

597f9539014e3d0f350c069cd804aa71679486ae

84ed4ac411ee2757d7c80ac8ce7d02d805110afd

1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e

91f8592c7e8a3091273f0ccbfe34b2586c5998f7de63130050cb8ed36b4eec3e

4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e

5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103

3de8fe5cee8180e93697e4ddca87e721910b9dd922de849cab7b1b3a50e54a00

388163c9ec1458c779849db891e17efb16a941ca598c4c3ac3a50a77086beb69

8d2581e5cc6e6fdf17558afe025ff84d9023ea636aca74dee39900d8f523e912

ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f

3fb160e1770fafeedff2d77841bf02108c25cca4cb6d77e3fbf759077f356b70

0097b8722c8c0840e8c1a4dd579438344b3e6b4d630d17b0bbe9c55159f43142

aeb1b789395357e8cc8dbd313b95f624fc03e037984040cd7c1704775bfb4bd2

477382529659c3452020170d8150820210ab8cbdc6417a0f0ac86a793cd0d9b4

f361bafcc00b1423d24a7ea205264f5a0b96011e4928d9a91c2abc9911b433a1

20848d28414d4811b63b9645adb549eed0afbd6415d08b75b0a93fbf7cfbf21f

754ac79aca0cc1bcf46000ef6c4cbe8bebeb50dae60823a1e844647ac16b6867

4877ff7c3c2abd349646db1163814811e69b36374e289f5808cc794113ef55ae

9200167f75f207fca91448547c24685f30beb82e383deb39bb07c126f49d9613

d09de8044608823f95fdf8c12a6127c047bb04f896497b67d45d5baafe49c3b4

edc166b2e10484c409f69d8e34de501a8672fa632bf8bbcf06ba2377ffae6363

fd738a651e4d77d928155d1fdf228fb7b161fb40d3adf33a8971fd391694693c

989831eba5ea1767225690e41eb02a668a6f2d56dc1f6b783b20731192fe7422

da8ed9b1ba9999d2ec67a0580749a8d819f37598b4dc0ff7d4c18bf01ba4194e

118d2961babf42a31ee83cb3eb059de265a50327688d50faa66aaca99784afe8

01b857ab6a7870c73be225ae8f1fe118df45b28d76d47f07c6c4ddc15cc83091

3db5dc72a0774f6a5fdfb54981e7a883959b6a4965d0d2058b467e6d2d420baa

61c9df341f4a29b2f4e5e70a7639ef3c1822ee59d5ad14115903e384e6bcbdd3

088fc6c5e5140ab0c39e28fa043db70eb2ddb57b1ee5fb8380018d846f16ce8c

cf98bb777723cb50742cad3af0857e97d555e5478254f0018d44b4a796320f55

f3a9b486af5f694479f4b8ac218f0ffbd968e05a582265d4d2c8f5744eca556a

1226b7f3b25713772d56e27b8522bb5975af7cf8c63df5ae278dd24381564754

01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd

0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5

543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91

31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427

efc2125e628b116eb0c097c699e473a47a280dfcd3e02cada41bdf6969600b41

794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91

572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b

f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e

9103194d32a15ea9e8ede1c81960a5ba5d21213de55df52a6dac409f2e58bcfe

44a5e78fce5455579123af23665262b10165ac710a9f7538b764af76d7771550

94ce428f04f35e434dc9bd81e17fe506d8f81fe51ea40fca530f1f2ef00e2881

eb24370166021f9243fd98c0be7b22ab8cbc22147c15ecef8e75746eb484bb1a

1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad

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

1. **CMTX-I-020092024: Linux Malware C&C Domain and IP**

Linux based malware is often packaged in the Executable and Linkable Format (ELF), is designed to target and exploit vulnerabilities in Linux operating systems. ELF malware can range from basic trojans and worms to sophisticated rootkits and ransomware. It poses significant risks to servers, IoT devices, and other systems running Linux, often aiming to steal data, create botnets, or disrupt operations.

Common Features of Linux ELF Malware:

Data Theft

Botnet Creation

Remote Access

Persistence

Rootkits

Ransomware

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.). 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 domain and associated IP of this malware are as follows:

- ------------< C&C Domain and IP>---------

appsupport.my-router.de

zimbra-beta.info

45.142.155.117

45.142.155.113

- ------------</C&C Domain and IP>---------

1. **CMTX-P092024065: ACTIVE EXPLOITATION OF GEOSERVER VULNERABILITY (CVE-2024-36401)**

ALERT BRIEF:

According to the reports, a GeoServer (an open-source Java-based server for sharing and editing geospatial data) RCE Vulnerability tracked as CVE-2024-36401 is being actively exploited to deliver botnet malware, cryptocurrency miners, and a backdoor leveraging IT service providers, technology companies, and government entities. Weaponized exploit code for the same is publicly available. Some of the malwares being deployed are listed below:

1) GOREVERSE: GOREVERSE is a publicly available reverse shell backdoor written in GoLang language.It operates over Secure Shell (SSH) and is employed by the China based threat group UNC5174. The malware facilitates post-exploitation activities by establishing persistent connections with C2 servers, allowing attackers to issue commands and control compromised systems remotely.

2) SIDEWALK: The SideWalk malware family aka ScrambleCross/MOPSLED is a modular backdoor used primarily by the SparklingGoblin APT group. Its one of the capabilities include cross-platform capability with both Windows and Linux variants in active use. It uses ChaCha20 encryption and utilizes command-and-control (C2) infrastructure to execute various tasks. The malware shows code similarities with Specter RAT.

3) MIRAI VARIANT (JenX)- It was observed that a script downloaded a file named “sky”, thereafter, the script changed sky’s permissions to make it executable, and was run with the parameter “geo”, and then deleted it after execution. The sky file functions as the Mirai variant called JenX. It connects with the C2 domain to receive and execute commands, including launching brute-force attacks and distributed denial of service (DDoS) campaigns.

4) CONDI- Condi functions as a backdoor, enabling threat actors to control compromised systems, exfiltrate data, or deploy additional payloads. It was observed threat actors used a script to download multiple bot binaries related to Condi, later the script changed the binaries’ permissions to make them executable and run them. Condi connects with a C2 server to receive and execute commands, including launching various DDoS attacks.

5) CoinMiner- The CoinMiner malware family belongs to the XMRig variant. The malware's versatility allows it to operate alongside other threats like backdoors and ransomware, showcasing its dual function of financial gain and exploitation within compromised networks. CoinMiner exploited vulnerabilities like CVE-2020-14882 and CVE-2024-36401 to gain initial access to systems, often targeting poorly managed Linux SSH servers through credential stuffing and IP scanning techniques.

Threat Type: Vulnerability

Severity: High (CVSS SCORE:9.8)

Impact: This vulnerability can lead to executing arbitrary code.

Mitigation and Recommendations:

1) Patch and Update: Apply the latest security patches. Ensure that all systems

(Please note that simply applying patches for the CVE mentioned may not fully address the issue if your network was already compromised by these malwares while the device was still vulnerable. It is highly recommended to conduct further investigation into the use of stolen credentials to detect any attempts by the threat actors to gain access to other parts of the network)

2) Network Segmentation: Implement network segmentation to limit the spread of an attack and contain potential breaches within isolated segments.

3) Monitor and Detect: Enhance monitoring and detection capabilities to identify suspicious activities and potential exploitations. Regularly review logs for unusual access patterns.

4) Access Controls: Enforce strict access controls and least privilege principles to minimize the risk of unauthorized access and exploitation.

5) Incident Response: Develop and test incident response plans to ensure preparedness for ransomware and other cyber attack scenarios.

6) Threat Intelligence: Stay informed about emerging threats and vulnerabilities. Engage with threat intelligence services to receive timely updates and actionable information

7) Multi-Factor Authentication (MFA):

Mandatory MFA Implementation: Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms. MFA adds an additional layer of security by requiring users to provide two or more verification methods before accessing accounts.

Enhanced Protection for Critical Accounts: Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security. This added layer of protection is crucial for safeguarding sensitive and high-privilege systems.

8). Backup: Regularly back up important data and system configurations. This will help in recovery if an exploitation incident occurs.

Annexure:

CERTIn-Threat Intelligence ID- [CMTX-P092024065]

IOCs ASSOCIATED WITH (CVE-2024-36401):

IPs

181.214.58.14

47.253.46.11

188.214.27.50

209.146.124.181

95.85.93.196

188.214.27.50

HASH

7d052cffcf97b303d11c5d35fa9bc860155601cdea21e38447401571b35d2db1

b80e9466b7bb42959c29546b8c052e67fcaa0f591857617457d5d28348bd8860

d9e8b390f8e2e8a6c2308c723a6a812f59c055ecad4e9098a120e5c4c65d3905

79c9532fb6ef2742e207498bfe2b2ee09aa9773376ac0e56085083aab17b98be

5cc7e35254347f705422800bfb7fe29c6002e2537f6bac0ff996a720dfb5f48e

fabbb4611fb9df5d8f208d9353be0b73c3942fe78903da096cbfe2f47c9e3566

1588bee7db42495ba7e6e34d217e6b82c5ab93f27c1eea68435cbb9e7792f9be

e8b0f5a952f07c83c4d67809ac0715c7164d518323d8038542e84aab8456db43

3c73ebc7a85accc65c9ee5bf151f70b990e5a12f27a843ca21c0f9d9a10fd17d

9bf642a7e14f0a0b0a784f00a0d1cf590ac60ae5ae378d29d435519f4d9dbf2b

994b924b00fb56e12a6a987c4cdf65dd05a221c47b5fc0a7a2babf1f05c2ed38

c226744b40e8f5d2cf95b4fb2537ff00e222ecc2d24c5096ecfadb14b4a47f97

96cf27a66b629d2b19708c6887441a8422b40dc0e9e7c5c0f2212efe0b6b3323

b3a015b6650ec9800fa878ff9a5f732013806c8dcb0e7069515dae0dd380fda4

50b7e615b8cdc45486b6ed1c1c081c7a92c262edb84318fa864531dcab753f82

f7b97677b6387c1f02d429e98868bf6973a8dec14dfee2516a27e885d6b1c780

b60d7fb66caf103a04e81fb89dbb05111b4b0ef513f3769c8e0a8106ab01a075

a9e7b5284182d3881c865895ee6e0fb03273eec3dcbf4bfc82dd2b069245beae

c3101b0b74d76a95ba91b6cc4945657e928d2dac8fdf926ffbf09031d46e9186

b67ab1b9b66fdc2c4ed1689698a54a347c2bdd6eaff87039ae337675243670d8

83fb74bb852bbd722e6ebc4e249e49cb4bb4194493a26d62d4bfcdfca2998412

53994a35a57970dea48e97009f65ad045b69a83234b771b106446211376a6866

f3d3572ef96c9c59e137425ca6804e1b86b7f8b57210a3724d567017460774de

1af8e068aa7377f0055640af581a412aa9d7288c912a93dd0d739657af0079fb

1abd8cbd64d1d9c8d56b7ea6273ed62e1471f300fabc67dbc2416a48e2faf33d

addccd0ecb643251af2e79e878b19a8e9c8f1c87302e732ef057cdba821f4b30

d9dfe98b5fba09e17dbe29dfeb8deb7d777d4a3b0d670914691ed360b916116a

8d3440301bc94ed83cdafb69e4b0166d3a0020eb4f38e9fa159c2f13f14b2d29

a13a979f4ca57450528bb6cd7aa2bf47d2eea211053eb1a14b8c4a44fd661831

7194ec436231c2a383ffc7c75eef4f5b5a952c18fa176ffd0830667835a80533

20d97f144bf7b1662a13ac537715126b9b2f68eff46a4a09234743ae236f0177

d72e4cabffc84a31e50caf827b6e579cf6e4932e5cbc528a65a68728ba56b65b

5abf8a52d45f6d5970fab8d1dfd05b6ee7b0ef57df935f45761b89d3522fa592

24e80d66759b1c7a075aeb4fe0321eb6ac49eaf509089fd2882874ec6228d085

7355cc094f2e43e4dd7b8b698b559abe6d2d74cc48f5cfa464424314c6e41944

689504850db842365cd47eadd2d3d42888b9261e7d9e884f14bb7deeb21bb61d

762707f2c7fc4731c4c46ecb3364a4e7ace8984aa899cc57c624b342d3efa03f

4234eb5eb42fbe44d7163c4388d263b3fe57fb1e56bf56152ac352c3fd0beec0

373734730d8414d32883ebbd105c7a7c58397df995759c4e0bd367f2523d302d

d1d25730122f8bc125251832c6af03aedd705dfcc2d9eebcce4371c54bb84b39

3dce929b1c091abac3342788624f1ffa4be5d603eec4d7ab39b604694ac05d22

eb2f95bb2059a3690259f2c0d7537b3cad858869650b9c220d2d81e3720b6dde

2e0e324e36fafe71f5d2bcf521e6415dafbc3f1173ad77f1f3daa77bb581da5f

5d9eb83b4a6f2d49580e1658263eb972be336a2cad15a84561d17d59391191b0

75d7b6264f5a574bc75400c9d57282e9344d8b2df576ad2a36ab7e2575d5a395

e5e5122ba6d0b06f7ed8e57ab5324ae730970c0d23913f27b9ecc9094182c03d

275302d03a4378f1b852e6d783d3181c2899ae0e9ebad4c7160221320863c425

653a4ad0b00e59a01142f899b6aac9712cfb25063b5b9b2e7e3171f7f3a897ed

8fad39ec0671d9b401712ddbc1f24942b2ee2f4865b6ffcd2f019036e03cbade

c8b76b63644d2946fd0af72b48fa59f07a78e1f84464cff5e9b1ca4110e6113e

3928c5874249cc71b2d88e5c0c00989ac394238747bb7638897fc210531b4aab

c81d4770e812ddc883ead8ff41fd2e5a7d5bc8056521219ccf8784219d1bd819

bf56711bbe0b1dac3b1481d36e7ae2f312da5f404c554c2c45a01fe591b8464d

5c9722d3dc72dbeafec00256887867bad46d347a5fc797d57fc9e0fd317035d3

3369ddc627282eb38346e1a56118026dd3ccdb29b18ffff88ecf3663296ee6da

1. **CMTX-I-022092024: 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 Domains>---------

scigovin.com

scingov.com

scigov.online

supremecourtorder.in

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

1. **CMTX-I-404092024: Malicious Domains Associated with Macro Embedded Documents**

Macro-embedded documents are legitimate files (such as Word, Excel, or PowerPoint) contain macros (small programs) designed to automate tasks. However, cybercriminals often exploit this feature by embedding malicious macros in these documents to distribute malware. Once a user opens the document and enables the macro, the malicious code executes, potentially compromising the system.

How Macro Malware Works

Delivery: Malicious macro-embedded documents are typically distributed via phishing emails, often disguised as legitimate invoices, reports, or notifications.

Execution: Once the document is opened, the macro prompts the user to enable it. In some cases, it displays text that the content of the document won't get displayed until macros are enabled. If the user allows macros, the malware is executed.

Payload: The macro may download additional malware, such as trojans/ keyloggers/ ransomware or exploit vulnerabilities in the system.

Prevention Measures

Disable Macros by Default: Office software should be configured to disable macros by default, and macros should only be allowed from trusted sources.

Use Trusted Documents and Protected View: Files should be opened in "Protected View" by Microsoft Office, and macros should only be enabled in documents from verified, trusted sources.

Enable Macro Security Settings: Group Policy settings should be enforced to limit macro execution, such as enabling "Disable all macros except digitally signed macros."

User Awareness: Employees and users should be trained to recognize phishing emails and avoid enabling macros in unsolicited documents. The risks associated with macros should be communicated to users as a key defense.

Email Filtering: Advanced email filters should be used to block or quarantine emails containing macro-enabled documents (e.g., .docm, .xlsm) from untrusted senders.

Domains associated (malware hosting and C2) with recent macro based campaign targeting government officials are as follows:

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

sparklingpoints.info

craftscore.info

watchneed.info

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

1. **CMTX-I-500092024: 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 Domains>----------------

emailnic.org

email.gov.in.publications.ltd

www.email.gov.in.publications.ltd

email.gov.in.publications.tld.publications.ltd

www.email.gov.in.publications.tld.publications.ltd

\*.in.publications.ltd

\*.in.publications.tld.publications.ltd

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

As threat actors are creating several sub-domains for malicious parent domains on a regular basis, hence it is necessary to block the parent domain as well as all of its possible sub-domains beforehand. This could be done by blocking the parent domain as a wildcard domain '\*.phishing-domain.com', where \* corresponds to the wildcard.

1. **CMTX-I-514082024: 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.

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 IP of malware deployed by this threat actor is as follows:

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

31.220.74.247

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

1. **CMTX-P092024075: EARTH PRETA CAMPAIGN**

THREAT OVERVIEW:

1.Threat Campaign: EARTH PRETA CAMPAIGN

An Asia-Pacific (APAC) threat group named as "EARTH PRETA" is active in the cyber threat landscape. The campaign uses new tactics using new tools like FDMTP and PTSOCKET and updated malware variants. It also uses a new variant of the HIUPAN worm to spread PUBLOAD through removable drives alongside a fast-paced spearphishing campaign, wherein a malicious “.url” file attachment downloads DOWNBAIT malware, which executes decoy documents and PULLBAIT to load the CBROVER backdoor. CBROVER then installs PLUGX, which continues data collection and exfiltration.

HIUPAN- The PUBLOAD malware, which is a command tool for additional activities including data exfiltration and network spying, is largely distributed by this worm via portable disks. The most recent version of HIUPAN uses DLL side-loading with legitimate apps, namely CocCocUpdate.exe from CocCocBrowser, and is made to be easier to configure.

PUBLOAD- PUBLOAD collects system data and maps the network, compressing the gathered information and prepares it for exfiltration using tools like RAR. It also distributes other malware, such as PTSOCKET for file exfiltration and FDMTP for downloading more payloads.

FDMTP- It is a downloader tool that uses Duplex Message Transport Protocol (DMTP) to fetch and execute additional malware components.

PTSOCKET- It is a new exfiltration tool that transfers stolen files using TouchSocket over DMTP to support multi-threaded file transfers.

DOWNBAIT is a first-stage downloader malware that serves to retrieve and execute other malicious components, specifically PULLBAIT and CBROVER. It is characterized by its digital signature, which enhances its evasion capabilities against security measures.

PULLBAIT- PULLBAIT is a straightforward shellcode that serves as a downloader, enabling the execution of further malware payloads, including DOWNBAIT and CBROVER, which are part of a multi-stage infection chain linked to recent campaigns attributed to the Asia-Pacific threat group Earth Preta.

CBROVER- CBROVER is a backdoor malware that enables file downloads and remote shell execution, often functioning as a precursor to the PLUGX malware family.

CYBER IMPACTS:

1. Data Theft and Espionage: Nation State Spnsored APT groups often target intellectual property, trade secrets, and sensitive business information. This can lead to the theft of proprietary technology, research data, and confidential communications, impacting competitive advantage and business integrity.

2. Network Intrusion and Persistence: These actors employ sophisticated techniques to gain and maintain access to enterprise networks. They use advanced malware, spear-phishing, and other methods to infiltrate systems and remain undetected for long periods, which complicates detection and mitigation efforts.

3.Data Exfiltration and Manipulation: Once inside a network, APT actors can exfiltrate large volumes of data or manipulate data to disrupt business operations. This can result in misinformation, loss of data integrity, and long-term operational damage.

4. Compromise of Critical Infrastructure: Some APT groups target critical infrastructure components, which can have severe consequences. This might include disrupting industrial control systems, supply chains, or other essential services.

OPERATIONAL IMPACTS:

1. Operational Disruptions: Cyber intrusions can cause significant disruptions to normal business operations. This might include system outages, interruptions in service, or delays in production and delivery, all of which can impact overall business performance.

2. Operational Complexity and Resource Drain: The complexity of defending against APTs often requires significant resources, including specialized personnel and technology. This can strain existing resources and divert attention from other critical business functions.

3. Increased Security Costs: To defend against sophisticated APT threats, enterprises often need to invest heavily in advanced security measures, including threat detection systems, incident response capabilities, and regular security assessments.

4. Operational Complexity and Resource Drain: The complexity of defending against APTs often requires significant resources, including specialized personnel and technology. This can strain existing resources and divert attention from other critical business functions.

5. Strategic Disruption: In some cases, the exposure of strategic plans or sensitive negotiations can disrupt business strategies, partnerships, or market positioning

THREAT TYPE: Nation State Sponsored APT group

SEVERITY: High

ATTACK VECTORS Phishing,Virtualization/Sandbox Evasion, C&C Server,SpearPhishing Attachment

MITIGATIONS AND RECOMMENDATIONS:

1. Keep systems and products updated and patched as soon as possible after patches are released. Consider leveraging a centralized patch management system to automate and expedite the process.

2. Enforce multifactor authentication (MFA) for all users, without exception .

3. Immediately remove or isolate suspected compromised devices from the network.

4. Segment networks to limit or block lateral movement .

5. Implement strict password requirements, enforcing password complexity, changing passwords at a defined frequency, and performing regular account reviews to ensure compliance

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

Indicators of Compromise (IOCs):

IP ADDRESS

154.90.32.88

HASHES

565fa2992212c89bdec334c0fd318b3fd2c91707431fd8186016f11645925892

3278c06b5510edabb3318aa1892eb7e426e97946b86eea925965a46ba1725ebd

df0e16a29c9dffe2ff7b3d4c957af7459fd7e6fa8026d067202912b997773749

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

1. **CMTX-P092024116: EchoStrike tool**

ALERT BRIEF:

Reports indicate that a new Go-based tool called EchoStrike has been developed to create undetectable reverse shells and execute process injection on Windows systems. Users can customize their binaries with sophisticated persistence and encryption features through an interactive Python-based wizard. The tool also provides advanced options to modify the binary size and establish persistence through various methods, including altering the system registry, setting up a command autorun, creating scheduled tasks, or adding startup shortcuts on the target system.

1. **CMTX-092024085: Akira Ransomware Gang Exploiting SonicWall Vulnerability**

Threat Actor: Akira Ransomware Gang

Vulnerability: SonicWall Vulnerability CVE-2024-40766

Impact: Unauthorized access, data exfiltration, and system encryption leading to ransomware attacks.

Initial Access Vector-compromise of SSLVPN user accounts

Severity: Critical

Affected Systems: SonicWall firewalls SonicWall firewall devices across Gen 5, Gen 6, and some Gen 7 versions

Executive Summary:

The Akira Ransomware Gang, a prominent cybercriminal organization recognized for its advanced ransomware campaigns, has recently been detected exploiting SonicWall Vulnerability CVE-2024-40766. This vulnerability affects SonicWall firewall devices across Gen 5, Gen 6, and certain Gen 7 versions, with a CVSS score of 9.3, indicating a high-severity threat. Reports indicate that compromised accounts were local to the devices, lacked multi-factor authentication (MFA), and ran vulnerable firmware versions, which made them particularly susceptible to attack by the ransomware group.

Threat Actor Profile:

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

Mitigation Strategies:

1. Patch Management:

o Immediate Action: Apply the latest security patches provided by SonicWall for CVE-2024-40766

o It is recommended upgrading to the latest SonicOS version, resetting local SSL VPN passwords, enabling MFA, and restricting firewall management to trusted sources to mitigate risks.

o Long-Term: Regularly update all network security appliances and firmware to address newly discovered vulnerabilities.

2. Network Security:

o Segmentation: Implement network segmentation to limit the spread of ransomware within the organization.

o Monitoring: Enhance network monitoring to detect suspicious activities and potential exploitation attempts.

Recommendations:

1.Organizations using SonicWall devices should prioritize applying the security updates for CVE-2024-40766 and review their network security posture to ensure robust defenses against potential exploitation. Continuous monitoring and readiness to respond to ransomware incidents are crucial for minimizing damage and operational disruption.

2.For more information and updates, please consult SonicWall’s official advisory https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

1. **CMTX-P-1140920249: MacroPack-Generated Malicious Documents**

ALERT BRIEF:

A new wave of cyber threats has been identified involving the use of MacroPack,by threat actors to deliver sophisticated payloads such as Brute Ratel, Havoc, and PhantomCore. MacroPack is a highly versatile tool that enables cybercriminals to generate malicious macros, often embedded in seemingly benign documents like Word or Excel files. Once these documents are opened, the embedded macros execute, unleashing malware onto the victim's system. These tools are engineered to evade detection and compromise targeted systems, posing significant risks to organizations and individuals alike.

Technical Details:

Obfuscation Techniques: MacroPack-generated code includes function and variable renaming, removal of surplus space characters and comments, string encoding, and payload obfuscation. These techniques make it difficult to detect the malicious code using traditional file content signatures.

Payloads:

The documents deliver multiple payloads, including:

Brute Ratel: A C2 framework used for Red Teaming and adversary simulation.

Havoc: It is an open-source post-exploitation framework.

PhantomCore: A new variant of a remote access trojan.

Impact:

The use of MacroPack to generate malicious documents poses a significant threat to organizations. The advanced obfuscation techniques employed by MacroPack make it difficult to detect these documents using traditional security measures. Once executed, the payloads can exfiltrate sensitive information, execute arbitrary commands, and maintain persistent access to compromised systems.

1. **CMTX-P-2140920249: Loki backdoor**

ALERT BRIEF:

A new cyber threat has emerged in the form of the Loki backdoor, which is a private agent for the open-source Mythic framework.The Loki agent is a Mythic-compatible version of an agent for another framework called Havoc. It employs various techniques to complicate analysis, such as encrypting its memory image, indirectly calling system API functions.

Technical Details:

Loader and DLL Architecture: Loki is divided into a loader and a DLL, with the main functionality implemented in the DLL.

Obfuscation Techniques: The agent uses a modified djb2 hashing algorithm to obscure API functions and commands.

C2 Communication: Upon execution, the Loki loader sends encrypted system information to a C2 server, which responds with a DLL that is loaded into the device’s memory.

Impact:

The Loki backdoor poses a significant threat due to its advanced obfuscation techniques and ability to evade detection. It can exfiltrate sensitive information, execute arbitrary commands, and maintain persistent access to compromised systems.

1. **CMTX-I-525092024: 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 Domains>----------------

email-sec.in

email.gov.in.filesharing.breifcase.bharatdharti.xyz

\*.in.filesharing.breifcase.bharatdharti.xyz

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

As threat actors are creating several sub-domains for malicious parent domains on a regular basis, hence it is necessary to block the parent domain as well as all of its possible sub-domains beforehand. This could be done by blocking the parent domain as a wildcard domain '\*.phishing-domain.com', where \* corresponds to the wildcard.

Network administrators may take required action against the above malicious domains.