**Cyber Security Advisories**

**Date: 22-05-2024**

1. **CMTX-I-055042024 Mythic Malware - APT36 campaign**

Following IP is the C&C associated with Mythic Malware. This RAT could possibly be used by the Pakistan based threat actors under APT36 campaign to target Linux based systems in government offices.  
  
- -----------------<C&Cs>---------------  
109.48.0.110  
- ---------------</C&Cs>----------------  
  
Kindly take the required actions.

1. **CMTX-P042024285 Supershell Malware**

Supershell is a popular Chinese web based open-source command and control (C2) platform that supports multi-platform architecture client payloads (e.g. Windows, Linux, Android, FreeBSD).  Supershell is a versatile malware family leveraged by threat actors for unauthorized access to target entities. It provides a reverse secure shell (SSH) tunnel to obtain a fully interactive shell, remote system management, execute interactive scripts, and perform various remote operations using its fully interactive shell. Supershell has a range of functions and features including client management, client payload generation, file management, memory injection, obtains system information and the current user's username.

MITRE ATT&CK Enterprise Identifiers

T1021.004 (SSH)

T1059 (Command and Scripting Interpreter)

T1572 (Protocol Tunnelling)

T1059.003 (Windows Command Shell)

T1059.004 (UNIX Shell)

T1071.002 (File Transfer Protocols)

T1033 (System Owner/User Discovery)

T1082 (System Information Discovery)

T1571 (Non-Standard Port)

T1027.002 (Software Packing)

T1095 (Non-Application Layer Protocol)

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

Hashes

84a9748e5b11d4dd0c01ed4329339318abb70c0c8ed1885efa2f1307e625e333

9d8463696071372fc4526dadb73627c65de90379ef24fec8857d0f6f8b34e36d

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

1. **CMTX-P042024295 Multiple Security Flaws in Judge Zero**

ALERT BRIEF:

It has been reported that three critical security flaws (CVE-2024-28185 , CVE-2024-28189 , CVE-2024-29021) have been found in Judge0 (Judge Zero), which is an open-source online code execution system .These three critical flaws allow threat actors to perform a sandbox escape and obtain root permissions on the host machine to overwrite scripts on the system and gain code execution outside of the sandbox and on the Docker container running the submission job. The flaw lies in the Ruby script( "isolate\_job.rb,"), which is responsible for sandbox setup, running the code and execution of results.

The three vulnerabilities are as follows:

CVE-2024-28185 (CVSS score: 10.0)- Since the application is not looking out for symlink (symbolic links), therefore a threat actor can leverage to write to arbitrary files and gain code execution outside of the sandbox.

CVE-2024-28189 (CVSS score: 10.0)- The application uses the UNIX chown command on an untrusted file within the sandbox. An attacker can abuse this by creating a symbolic link (symlink) to a file outside the sandbox, allowing the attacker to run chown on arbitrary files outside of the sandbox

CVE-2024-29021 (CVSS score: 9.1)- If the threat actor has proper access to Judge0 API, then it allows them to obtain unsandboxed code execution as root on the target machine. This vulnerability is fixed in 1.13.1.

RECOMMENDATIONS:

\* If the organization is using a self hosted Judge0 instance, update to v1.13.1 or higher to be protected against these attacks.

1. **CMTX-P-042024345 Raccoon Stealer**

Malware Alert Brief:

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

77.221.151.21

88.119.161.188

5.42.64.13

148.113.9.132

88.119.161.188

5.42.64.8

195.2.80.198

146.19.173.72

46.226.162.32

94.142.138.227

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-042024325 SocGholish malware**

Malware Alert Brief:

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

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

119.13.110.128

94.74.81.25

49.0.200.240

124.243.147.143

119.13.103.16

124.243.133.194

124.243.135.236

124.243.150.185

159.138.87.228

159.138.107.49

190.92.207.126

190.92.209.68

190.92.212.240

110.238.111.178

119.13.100.146

124.243.137.156

124.243.150.210

159.138.111.76

110.238.110.240

49.0.206.247

94.74.91.100

110.238.109.69

110.238.110.49

110.238.110.173

110.238.111.143

114.119.191.138

119.8.160.152

119.8.174.80

119.8.189.12

119.13.106.164

159.138.96.117

159.138.98.152

190.92.199.115

190.92.202.240

190.92.218.78

119.8.182.13

124.243.135.66

159.138.110.8

49.0.202.170

94.74.86.10

114.119.173.19

119.8.163.174

119.8.184.79

124.243.132.91

124.243.135.114

124.243.138.34

124.243.144.175

124.243.148.114

124.243.150.207

159.138.84.3

159.138.102.121

190.92.199.75

190.92.201.44

190.92.202.17

190.92.205.141

190.92.206.5

190.92.209.6

110.238.108.75

119.13.103.43

124.243.134.32

124.243.134.100

124.243.133.152

94.74.88.121

124.243.133.84

124.243.133.174

159.138.86.86

190.92.209.33

190.92.209.184

119.8.191.240

190.92.221.166

92.205.215.210

110.238.105.241

119.13.100.213

190.92.209.78

111.59.4.88

213.239.204.39

216.24.213.76

103.251.2.17

49.0.202.9

49.0.203.90

94.74.81.247

94.74.86.81

94.74.87.150

94.74.89.166

94.74.90.18

110.238.104.11

110.238.104.149

110.238.111.118

114.119.175.21

114.119.183.63

119.8.180.239

119.13.100.118

119.13.102.48

119.13.104.159

124.243.134.156

124.243.134.178

124.243.134.238

124.243.136.184

124.243.138.123

124.243.138.211

124.243.138.234

124.243.139.136

124.243.148.133

124.243.150.61

146.190.108.97

159.138.96.146

159.138.105.87

159.138.111.129

159.138.122.45

190.92.198.2

190.92.198.120

190.92.208.167

190.92.209.117

190.92.210.30

190.92.216.77

190.92.219.69

154.118.228.212

119.13.102.196

159.138.103.220

190.92.204.0

124.243.151.132

190.92.216.94

119.13.108.89

190.92.200.145

49.0.200.202

49.0.202.25

49.0.207.93

94.74.84.50

110.238.104.205

110.238.106.48

110.238.110.188

119.8.180.20

119.8.186.126

119.13.101.155

119.13.111.116

124.243.132.85

124.243.134.105

124.243.134.214

124.243.136.43

124.243.137.68

124.243.147.133

159.138.98.91

159.138.102.200

159.138.123.188

190.92.201.11

190.92.201.147

190.92.202.236

190.92.206.249

110.238.104.161

124.243.136.12

94.74.92.178

140.206.235.85

41.77.19.22

49.0.204.2

49.0.204.77

49.0.204.143

49.0.205.7

49.0.205.155

49.0.206.9

49.0.206.16

94.74.82.84

94.74.85.36

94.74.86.73

94.74.90.33

110.238.107.187

110.238.109.93

110.238.109.217

114.119.172.216

114.119.173.218

114.119.174.88

114.119.174.224

119.8.162.110

119.8.189.202

119.13.101.211

119.13.111.86

124.243.132.146

124.243.133.39

124.243.133.248

124.243.134.126

124.243.135.130

124.243.135.189

124.243.144.216

124.243.151.1

124.243.151.209

159.138.84.146

159.138.96.79

159.138.97.145

159.138.99.105

159.138.103.36

159.138.105.142

159.138.105.174

159.138.108.179

159.138.108.228

159.138.109.164

159.138.110.195

159.138.121.137

172.70.142.250

172.70.188.79

190.92.202.169

190.92.203.43

190.92.205.226

190.92.206.161

190.92.211.238

190.92.213.201

190.92.216.150

190.92.218.81

190.92.219.57

190.92.219.153

159.138.105.133

190.92.216.205

119.13.104.114

94.74.83.173

94.74.88.87

110.238.107.76

110.238.109.250

124.243.134.180

124.243.136.249

124.243.147.61

124.243.148.161

124.243.151.237

159.138.105.125

159.138.109.192

190.92.201.101

190.92.212.116

190.92.214.209

145.239.23.7

49.0.204.117

94.74.95.244

124.243.146.76

49.0.200.89

49.0.205.171

94.74.80.56

94.74.81.63

94.74.82.64

94.74.85.211

94.74.91.67

94.74.94.92

101.44.160.205

110.238.110.36

110.238.111.43

114.119.180.127

114.119.187.162

119.8.182.195

119.8.186.12

119.13.100.35

119.13.102.112

119.13.107.86

119.13.111.241

124.243.133.99

124.243.133.175

124.243.134.232

124.243.135.98

124.243.136.24

124.243.145.23

124.243.146.203

124.243.148.115

159.138.97.57

159.138.99.74

159.138.106.135

159.138.110.189

159.138.121.61

190.92.200.8

190.92.202.5

190.92.202.87

190.92.203.86

190.92.211.194

190.92.213.52

190.92.213.155

190.92.215.15

45.80.187.8

110.238.106.18

110.238.108.53

124.243.132.24

124.243.136.201

94.74.88.198

119.13.105.88

124.243.136.109

124.243.148.208

124.243.150.81

159.138.110.35

190.92.201.38

190.92.204.96

190.92.208.153

45.130.201.28

180.235.151.162

36.134.147.75

140.206.235.102

89.14.187.124

157.90.253.188

213.239.200.253

213.180.203.227

103.186.24.27

118.67.200.222

43.255.154.45

95.217.109.26

43.252.215.139

103.130.212.57

101.44.250.84

101.91.148.219

121.40.79.79

77.75.78.169

5.75.225.67

167.235.192.35

172.68.194.213

81.17.122.33

103.18.245.175

89.248.172.115

5.188.210.91

83.97.73.239

109.106.253.151

114.119.131.232

114.119.158.149

27.254.33.86

150.107.31.64

202.29.39.5

2.58.45.2

103.127.198.180

210.211.125.205

18.139.252.83

161.97.165.247

8.218.249.47

39.148.73.216

101.44.250.177

101.91.134.204

172.69.150.245

212.117.30.221

5.255.231.200

95.108.213.132

31.187.75.89

114.119.148.27

163.44.198.43

178.128.103.253

122.155.167.53

167.172.65.95

171.244.51.61

43.139.114.241

101.44.251.170

112.18.35.225

123.249.99.231

124.220.52.114

140.206.235.116

172.71.218.15

51.159.37.51

163.172.74.29

49.12.150.117

94.130.138.211

103.11.153.223

212.126.107.236

185.93.165.224

178.128.110.101

5.188.210.80

45.32.100.163

47.128.31.1

49.0.207.20

119.13.100.156

124.243.138.37

124.243.139.76

159.138.97.137

159.138.98.180

172.70.147.44

190.92.200.155

190.92.212.251

103.20.96.219

77.246.105.178

15.206.135.123

180.102.134.69

222.79.104.23

62.122.184.194

103.162.50.12

45.130.201.32

58.49.233.126

117.151.148.121

118.123.105.85

119.41.194.190

121.227.91.153

172.68.243.78

51.159.37.33

94.31.89.212

144.76.67.110

103.47.135.89

45.128.160.157

3.1.18.74

47.128.20.208

114.119.181.215

119.13.100.91

119.13.110.84

124.243.136.227

159.138.82.138

159.138.86.210

159.138.96.240

159.138.97.11

163.44.198.62

172.68.242.19

190.92.199.100

190.92.207.3

190.92.216.34

27.254.68.45

27.254.81.20

125.27.83.162

203.170.129.26

116.100.217.251

87.123.37.22

103.50.163.40

43.252.237.98

91.224.60.25

174.138.27.156

84.232.4.97

192.36.109.123

116.111.101.10

111.172.249.49

117.151.145.243

114.119.129.34

178.128.99.103

101.36.106.134

115.231.78.10

108.162.227.7

58.211.23.183

123.6.49.47

123.244.131.43

162.158.134.61

135.181.213.219

103.47.135.77

84.38.188.16

92.51.2.233

43.243.118.228

47.128.25.89

47.128.30.218

89.233.105.89

118.194.250.113

165.154.51.221

185.196.0.16

27.76.197.91

116.106.108.172

116.107.191.107

116.118.98.26

171.233.176.105

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-042024375 Amadey Malware Alert**

Malware Alert Brief:

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

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

143.233.226.2 Greece

45.88.6.140 Netherlands

80.89.239.253 Netherlands

213.202.223.111 Germany

23.211.175.131 Denmark

188.116.25.73 Netherlands

34.77.108.49 Belgium

89.163.140.92 Germany

212.204.112.209 Germany

111.118.212.223 India

195.210.46.25 Kazakhstan

185.34.52.14 Lithuania

31.136.56.198 Netherlands

147.32.80.105 Czechia

89.163.152.111 Germany

185.196.8.195 Switzerland

57.129.16.154 Germany

94.23.144.189 Netherlands

77.220.215.196 Netherlands

5.104.108.23 Germany

31.214.178.109 Spain

85.158.181.26 Austria

217.12.204.114 Ukraine

5.42.65.114 Russia

23.34.32.116 Denmark

82.192.82.228 Netherlands

176.123.3.81 Moldova

95.213.205.83 Russia

141.244.180.71 Austria

88.212.252.98 Russia

46.28.110.192 Czechia

104.81.74.13 Germany

104.95.184.201 Denmark

212.204.112.234 Germany

217.112.35.57 Russia

109.206.164.6 Netherlands

2.17.0.108 Denmark

195.197.95.175 Finland

5.104.107.111 Germany

89.163.225.9 Germany

89.163.225.77 Germany

93.186.197.159 Germany

129.233.217.55 Germany

212.18.29.11 Germany

212.204.112.237 Germany

213.202.223.112 Germany

34.91.10.214 Netherlands

45.88.6.142 Netherlands

78.41.204.29 Netherlands

95.215.205.165 Netherlands

154.41.249.22 Netherlands

213.163.82.22 Netherlands

85.9.63.132 Romania

89.108.83.57 Russia

93.190.206.138 Russia

109.248.203.81 Russia

194.158.225.52 Switzerland

185.215.113.204 Seychelles

45.156.23.186 Russia

37.48.94.74 Netherlands

185.56.218.10 Italy

103.21.58.236 India

185.22.66.15 Kazakhstan

185.215.113.205 Seychelles

5.75.139.35 Germany

212.32.237.91 Netherlands

103.173.227.99 Vietnam

5.35.7.129 Russia

103.191.76.170 Malaysia

140.78.3.68 Austria

140.78.3.82 Austria

140.78.3.83 Austria

31.47.253.138 Germany

89.163.155.199 Germany

92.205.64.125 Germany

104.87.211.38 Germany

152.53.20.60 Germany

103.21.59.165 India

185.221.175.56 Italy

154.62.105.80 Netherlands

154.62.105.95 Netherlands

154.62.105.121 Netherlands

185.104.29.66 Netherlands

185.244.217.174 Netherlands

194.187.99.214 Netherlands

212.162.153.12 Netherlands

89.40.33.95 Romania

87.236.16.203 Russia

109.248.237.223 Russia

185.173.94.221 Russia

87.197.140.141 Slovakia

91.201.63.141 Sweden

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-042024365 Emotet Malware**

Malware Alert Brief:

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

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

178.255.220.124

159.65.6.6

77.95.248.78

91.121.87.90

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-042024385 Agent Tesla Malware Alert**

Malware Alert Brief:

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

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

45.252.248.26

185.165.185.2

45.134.160.220

89.39.83.184

45.252.248.26

153.92.8.115

185.165.185.2

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-042024335 Redline malware**

Malware Alert Brief:

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

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

5.42.65.96

45.15.156.127

147.45.47.42

94.156.67.67

45.89.53.206

4.184.225.183

65.108.19.51

5.42.65.50

178.159.39.40

91.92.241.122

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

1. **CMTX-P-042024355 Qbot Malware**

Malware Alert Brief:

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

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

18.193.24.187

18.194.189.200

18.194.65.70

52.59.8.62

85.192.40.230

82.192.82.22

82.192.82.225

1. **CMTX-P-042024315 Trickbot malware**

Malware Alert Brief:

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

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

41.77.134.250

103.75.32.173

177.190.76.82

27.109.116.144

185.68.93.17

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P-042024305 Ursnif malware**

Malware Alert Brief:

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

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

37.228.132.107

31.177.80.32

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

RECOMMENDATIONS:

\* Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-I-144042024 QuestRAT Malware - APT36 campaign**

The gov.in domain (zpbeed.gov.in) is found to be compromised and hosting malware targeting government officials.  
  
- -------------------------------------------<IOCs>--------------------------------------  
Compromised domain: zpbeed.gov.in  
URL hosting malware: https://zpbeed.gov.in/circular?email=dprdefense@gmail.com  
c665b0b86a53e0b99a61617e551956e6988d8342 [SHA1  
d136178baa29a07fe0a61a43c34c8ec0b2b6e5e0 [SHA1  
- -----------------------------------------</IOCs>--------------------------------------  
  
The malware is a credential and document stealer which extract credentials in the various browsers, lists files in drives and thereafter exfiltrates them via SLACK API/ BOT  
  
Hence the following URLs needs to be monitored in the network:  
  
https://slack.com/api/chat.postMessage  
https://slack.com/api/files.upload  
https://hooks.slack.com/services

1. **CMTX-I-025052024 Malicious Domains - Spear-Phishing & Malware Hosting Campaign**

ith reference to alert CMTX-I-053042024 dated 30th April, 2024, additional domain observed is as follows:  
  
- ---------------<Malicious Domains>----------------  
cbigovoffice.in  
- -------------</Malicious Domains>-----------------

1. **CMTX-P052024015 VacBan Stealer**

ALERT BRIEF:

A new type of malware is active in cyber landscape which has evolved from a previous variant known as Creal Stealer. It exhibits both spyware and steal ware capabilities. The malware is primarily written in Python, making it versatile and capable of operating on various systems. The initial attack vector starts through phishing emails, malicious attachments, or downloads from compromised websites. The major capabilities of malware  include targeting  and extracting sensitive information from infected devices, such as login credentials and cryptocurrency wallet data, browser cookies, saved passwords etc., retrieve the version information of the machine’s operating system (OS), store collected data into text files (crpasswords.txt, crcookies.txt, crcreditcards.txt, crautofills.txt, crhistories.txt, and crbookmarks.txt) inside the Temp directory, drops a copy of itself inside the Startup folder for persistence, enumerate files and directories, delaying execution using the Windows API Sleep function and detect debuggers using the IsDebuggerPresent API function.

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

HASH

eef7738228a8044df536ff5424d2b4ca8dcf6f522ef8e3e0de644cc0e5abaa7b

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

Recommendations:-

• Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defence.

1. **CMTX-P052024975 PLUGX RAT ALERT 114**

ALERT BRIEF:

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

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

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

IP Address: Country Code

204.194.66.139:HK

103.108.67.136:HK

64.44.184.105:US

154.84.23.116:JP

104.233.161.173:JP

103.96.75.176:HK

54.249.202.142:JP

103.135.33.250:HK

103.146.231.2:HK

149.104.12.64:HK

13.115.129.191:JP

103.43.18.220:HK

45.76.213.19:JP

45.63.41.197:NL

43.135.48.48:HK

148.66.5.53:HK

45.76.110.175:JP

91.225.217.23:NO

35.77.99.82:JP

107.150.124.43:HK

34.92.77.165:HK

47.242.114.104:HK

45.32.148.180:FR

103.107.104.37:HK

45.83.236.105:HK

52.128.229.101:HK

61.4.112.186:HK

148.66.5.50:HK

203.69.170.86:TW

61.4.112.188:HK

208.85.16.182:ES

141.98.212.38:HK

103.127.125.218:KR

107.155.56.15:SG

103.142.9.135:HK

45.76.132.25:GB

152.32.243.122:KR

148.66.5.52:HK

208.72.153.162:US

107.155.56.87:SG

38.89.72.253:GB

194.124.33.123:CH

112.213.109.131:HK

72.18.215.38:US

152.32.211.67:HK

192.54.57.122:NL

149.28.130.206:SG

103.127.125.219:KR

112.213.109.141:HK

80.240.28.192:DE

103.218.243.167:HK

185.126.225.74:NL

167.179.109.96:JP

103.135.33.253:HK

103.135.33.251:HK

146.66.212.82:GB

185.235.242.10:RU

103.199.16.196:VN

104.233.160.81:JP

52.128.229.102:HK

103.79.120.74:HK

103.107.105.153:HK

101.99.94.142:BG

23.248.176.11:TW

5.255.88.185:NL

103.135.33.254:HK

16.162.255.7:HK

119.160.235.92:HK

148.66.5.54:HK

209.250.241.189:NL

64.7.198.130:RO

202.182.115.238:JP

112.121.161.109:HK

154.26.153.129:AU

64.176.59.90:JP

96.9.210.77:SG

107.173.63.250:US

13.115.194.155:JP

107.155.56.4:SG

155.138.203.78:US

134.122.129.154:HK

103.127.125.204:KR

64.44.57.14:US

103.135.33.252:HK

52.128.229.99:HK

119.160.235.91:HK

70.34.197.27:SE

38.60.199.103:SG

103.79.120.71:HK

43.135.32.151:HK

112.213.109.121:HK

103.127.125.225:KR

141.98.212.75:HK

216.238.113.209:BR

202.182.108.248:JP

103.107.105.253:HK

91.225.217.75:NO

52.128.229.98:HK

167.179.72.177:JP

34.92.57.130:HK

103.46.184.180:HK

203.86.233.102:HK

103.127.125.206:KR

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

1. **CMTX-P052024024 IOCs related to Chinese Threat Actor Campaign**

ALERT BRIEF:

A suspected Chinese state-sponsored activity using a custom backdoor [Shadowpad, PlugX and the offensive security tool [Cobalt strike is being observed. The group utilizes living-off-the-land (LOLBin) techniques, relying on legitimate software[Windows Remote Management (WinRM)  for lateral movement and operating system components to gain and maintain long-term access to victim networks, minimizing the use of traditional malware and maintain  persistence on compromised servers using tools such as China Chopper web shell.

T1053.005 (Scheduled Task)

T1059 (Command and Scripting Interpreter)

T1071.001 (Web Protocols)

T1105 (Ingress Tool Transfer)

T1203 (Exploitation for Client Execution)

T1480.001 (Environmental Keying)

T1547.009 (Shortcut Modification)

T1566.001 (Spear phishing Attachment)

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

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

43.132.211.81:9090

122.10.89.230:443

168.100.10.196:81, 80

43.132.211.81:9090, 8080, 443, 80

5.45.72.170:443

104.238.149.146:16330, 443, 5555, 80

45.121.51.124:9443, 443, 10443, 80

103.137.63.34:443, 10443, 80

38.147.190.206:443

129.204.168.253:443

194.250.22.161:8080

27.254.164.221:443

5.34.176.64:443, 53, 80

38.60.191.15:443

38.147.190.192:443, 80

103.118.40.21:9443, 443, 10443, 80

134.175.165.149:443

154.39.150.224:443

38.54.23.186:443

141.164.63.254:49998, 443, 5000

190.92.237.235:443

88.80.145.122:443

61.238.103.155:443

88.80.145.126:443

154.90.36.53:63535

119.235.250.146:63535

154.197.98.3:443, 53

135.181.173.66:443

139.180.154.192:80

129.204.234.170:443

106.55.57.85:443

176.119.150.92:443

64.7.199.4:81, 80

194.156.99.115:443, 8443

129.204.174.25:443

54.39.143.130:443

103.224.80.90:8443

45.77.244.106:80

203.23.128.34:63535

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

•    Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024656 GH0ST RAT Malware**

ALERT BRIEF:  
  
GH0ST is a backdoor written in C++ that communicates via a custom binary protocol over TCP or UDP. GH0ST RAT has capability of capturing screenshots, Key logger, remote Shell and Command execution, reversing proxy, file transfer and file management, features a packet signature at the start of each message that varies between samples.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
IP ADDRESSES: PORTS               Last Seen  
  
106.52.216.65:999    07-09-2023  
192.235.96.137:443    02-05-2024  
1.92.90.232:8000    11-04-2024  
109.190.79.33:80    10-11-2023  
94.191.187.105:443, 80    29-04-2024  
92.34.35.119:80    29-04-2024  
222.190.108.207:443    29-04-2024  
124.223.199.81:8808    01-05-2024  
27.25.156.47:8000    01-05-2024  
58.217.193.45:443    24-04-2023  
129.204.53.10:8081    24-01-2024  
  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.  
  
RECOMMENDATIONS  
  
- - - - - - - - - - - - - - - - - - - Recommend to monitor connection towards the mentioned IP addresses.  
- - - - - - - - - - - - - - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024985 PLUGX RAT ALERT 115**

ALERT BRIEF:

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

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

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

IP Address: Country Code

45.58.47.141:US

45.117.102.174:JP

52.128.229.100:HK

109.94.209.44:EE

82.117.255.176:RO

152.32.139.70:KR

45.128.153.36:DE

43.255.28.190:HK

149.28.23.65:JP

64.176.56.238:JP

148.66.5.51:HK

20.191.154.204:SG

156.59.39.101:TW

192.248.183.208:DE

45.82.31.235:KZ

141.164.59.106:KR

38.207.12.104:HK

38.207.12.125:HK

104.208.73.38:HK

38.207.29.137:HK

38.207.3.12:HK

180.178.35.50:HK

38.207.29.150:HK

38.207.12.108:HK

38.207.6.210:HK

110.173.53.162:HK

8.218.234.216:HK

38.207.6.204:HK

38.207.29.176:HK

38.207.6.222:HK

38.207.6.241:HK

38.207.12.96:HK

38.207.6.250:HK

38.207.29.182:HK

172.111.244.138:BE

38.207.6.236:HK

38.207.29.143:HK

180.178.35.53:HK

38.207.6.207:HK

38.207.3.53:HK

38.207.12.115:HK

38.207.6.237:HK

38.207.3.44:HK

103.31.181.41:KR

38.207.3.50:HK

38.207.29.134:HK

38.207.3.5:HK

141.164.63.254:KR

38.207.29.152:HK

180.178.35.52:HK

38.207.29.187:HK

38.207.6.216:HK

38.207.6.218:HK

38.207.6.211:HK

38.207.29.146:HK

38.207.3.40:HK

38.207.12.80:HK

38.207.29.136:HK

38.207.29.155:HK

38.207.12.69:HK

38.207.6.226:HK

38.207.12.103:HK

38.207.29.180:HK

38.207.3.48:HK

38.207.6.251:HK

38.207.12.78:HK

27.102.106.153:KR

38.207.3.39:HK

38.207.12.90:HK

38.207.29.161:HK

38.207.12.123:HK

38.207.3.26:HK

38.207.6.217:HK

180.178.35.54:HK

38.207.29.164:HK

38.207.12.88:HK

38.207.6.213:HK

156.245.13.12:HK

38.207.6.242:HK

38.207.29.141:HK

38.207.6.220:HK

38.207.6.209:HK

38.207.12.111:HK

38.207.3.59:HK

38.207.6.233:HK

38.207.3.51:HK

38.207.6.205:HK

38.207.29.168:HK

38.207.3.34:HK

38.207.6.212:HK

38.207.6.245:HK

38.207.29.139:HK

38.207.12.87:HK

38.207.12.121:HK

38.207.12.89:HK

38.207.3.38:HK

38.207.6.252:HK

38.207.12.118:HK

38.207.6.229:HK

38.207.29.174:HK

38.207.29.186:HK

38.207.6.228:HK

38.207.29.179:HK

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

Please Note: The Above IOCs are also available in CERT-In Threat

Intelligence Platform.

Recommendations:

 - Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024666 NJRAT Malware**

ALERT BRIEF:  
  
NJRAT is a .NET-based backdoor that uses a unique text-based protocol over TCP to communicate. The backdoor is capable of recording video, audio, screenshots, keystrokes, creating a reverse shell, transferring files, running files, stealing credentials, and spreading via USB drive. Malware has features to update its capability by getting plugins from a C2 server.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
IP ADDRESSES: PORTS              Last Seen     Country Code  
  
88.103.67.6:4567      01-04-2021    CZ  
163.25.88.112:3001      01-05-2024    TW  
91.139.9.30:4567      07-03-2019    CZ  
118.89.89.200:443      18-03-2024    CN  
213.226.247.114:4567      02-05-2024    CZ  
85.71.145.68:4567      02-05-2024    CZ  
121.130.106.72:6001      01-05-2024    KR  
193.165.145.150:4567      02-05-2024    CZ  
95.85.215.11:4567      02-05-2024    CZ  
74.217.12.45:7070      24-04-2023    US  
46.252.230.190:4567      02-05-2024    CZ  
213.155.225.9:4567      02-05-2024    CZ  
59.2.188.200:3000      02-05-2024    KR  
192.132.64.43:7070      24-04-2023    US  
90.179.181.196:4567      20-06-2016    CZ  
64.94.37.63:7070      24-04-2023    US  
185.15.144.94:4567      02-05-2024    CZ  
89.239.21.132:4567      02-05-2024    CZ  
90.177.24.27:4567      05-07-2017    CZ  
213.226.246.49:4567      02-05-2024    CZ  
36.189.24.2:6666      02-05-2024    CN  
185.22.237.120:4567      02-05-2024    CZ  
121.128.63.131:6001      01-05-2024    KR  
93.185.4.211:4567      02-05-2024    CZ  
185.15.144.111:4567      27-02-2017    CZ  
139.9.177.228:19802, 18602, 15002, 18202, 18802, 20002, 18402, 19002, 20202    02-05-2024    CN  
112.74.55.109:19202, 19402, 18602, 18202, 20002, 19002, 19802    30-04-2024    CN  
39.108.246.91:17402, 16402, 17602, 16202, 18202    30-04-2024    CN  
  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.  
  
RECOMMENDATIONS  
  
- - - - - - - - - - - - - - - - - - -- Recommend to monitor connection towards the mentioned IP addresses.  
- - - - - - - - - - - - - - - - - - -- The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024676 QuasarRAT Malware ALERT 50**

ALERT BRIEF:  
  
Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely used by nation sponsored threat actors. Quasar RAT has capability of capturing screenshots, Key logger, gather System Information, remote Shell and Command execution, reversing proxy, Managing tasks and files, Configuring and building client executables.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
IP ADDRESSES: PORTS               Last Seen      Country Code  
  
31.220.92.125:11    30-11-2023    DE  
185.196.10.80:4782    01-05-2024    IT  
45.144.30.147:4747, 4004    23-11-2023    RU  
64.112.85.37:4782    02-05-2024    US  
190.42.210.108:3333    02-05-2024    PE  
163.5.215.213:4782    02-05-2024    FR  
87.109.218.76:1337    02-05-2024    SA  
191.82.238.74:2000    02-05-2024    AR  
216.224.126.168:8899    05-01-2024    HK  
202.47.118.167:8080    17-03-2024    IN  
120.26.136.167:8088    12-02-2018    CN  
82.157.50.57:4782    14-07-2023    CN  
45.80.158.55:4782    02-05-2024    PL  
157.20.182.46:4782    30-04-2024    NL  
110.42.67.20:7707, 1337    29-04-2024    CN  
177.60.18.92:5000    02-05-2024    BR  
24.102.191.128:4782    01-05-2024    US  
62.60.165.76:10000    02-05-2024    IR  
45.32.69.159:4782    28-01-2024    US  
103.200.124.194:4782    02-05-2024    HK  
84.247.179.77:8080    02-05-2024    DE  
103.244.226.133:8086    02-05-2024    HK  
104.238.170.242:4782    06-10-2022    GB  
163.5.215.116:4782    02-05-2024    FR  
2.56.245.124:80    11-07-2019    DE  
64.176.220.24:7707, 8808, 6606, 4782    01-05-2024    US  
188.50.202.137:1337    29-04-2024    SA  
83.143.112.27:25565    02-05-2024    NL  
94.102.59.173:58943    13-01-2019    NL  
94.156.64.31:2404    26-04-2024    NL  
70.36.105.218:6868    02-05-2024    US  
126.120.141.1:4782    24-06-2018    JP  
110.42.102.204:7707, 1337    29-04-2024    CN  
158.247.236.255:443    02-05-2024    KR  
91.92.252.108:7000    02-05-2024    NL  
75.155.127.226:4782    02-05-2024    CA  
94.156.79.26:4001    02-05-2024    LT  
198.11.181.29:4000    02-05-2024    US  
1.40.168.142:1005    02-05-2024    AU  
121.184.1.234:443    02-05-2024    KR  
188.228.85.68:1337    02-05-2024    DK  
46.250.225.152:4782    02-05-2024    SG  
212.192.31.211:4782    07-04-2024    DE  
185.241.208.58:4782    02-05-2024    PL  
187.59.66.45:4782    02-05-2024    BR  
69.178.117.223:1604    02-05-2024    US  
86.105.212.230:4782    02-05-2024    FR  
5.189.159.115:8080    12-02-2023    DE  
192.144.128.196:1994    02-05-2024    CN  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.  
  
RECOMMENDATIONS  
  
- - - - - - - - - - - - - - - - - - - Recommend to monitor connection towards the mentioned IP addresses.  
- - - - - - - - - - - - - - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-I-053052024 CrimsonRAT - APT36 campaign**

Recent C&C server IP of AndroRAT malware used by Pakistan based APT36 threat actors to target defence and other government officials are as follows:

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

38.92.47.124

- ------------ </C&C IP -------------  
Kindly take the required actions.

1. **CMTX-P052024945 SHADOWPAD Malware**

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

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

IP Address: Country Code

139.99.50.68:SG

103.96.129.6:HK

38.54.29.176:GR

116.202.251.18:DE

151.236.23.49:ES

218.3.254.252:CN

45.63.124.252:JP

192.71.213.155:ES

64.176.8.105:CL

70.34.212.229:SE

95.179.242.107:DE

139.84.226.239:ZA

103.180.161.211:SG

38.54.79.251:PK

216.128.184.205:CA

64.176.47.234:JP

95.179.240.31:DE

185.81.115.126:NL

165.154.18.212:JP

103.27.111.214:HK

139.180.206.75:JP

45.32.151.219:FR

103.205.211.174:MY

45.32.184.230:NL

38.54.17.82:SG

141.164.35.65:KR

103.255.118.149:MY

185.167.61.85:DE

107.148.45.171:HK

64.176.42.10:JP

47.76.40.17:HK

38.60.134.143:FR

38.54.79.167:PK

38.60.249.194:DE

96.30.196.210:US

136.244.119.156:FR

64.176.169.137:IL

199.247.1.201:DE

154.12.26.93:HK

38.60.224.143:MX

45.77.170.42:SG

134.122.189.32:HK

216.83.40.84:HK

107.148.45.172:HK

107.148.45.174:HK

5.252.178.27:RO

38.60.216.102:FR

103.255.118.150:MY

199.247.10.114:FR

185.174.135.5:EE

185.81.114.132:NL

139.180.219.37:SG

38.60.249.246:DE

38.54.84.80:DE

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

•    Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024995 PLUGX RAT ALERT 116**

ALERT BRIEF:

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

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

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

IP Address: Country Code

38.207.29.185:HK

38.207.29.149:HK

152.32.204.39:JP

38.207.29.151:HK

38.207.3.28:HK

180.178.35.51:HK

38.207.6.200:HK

158.247.213.215:KR

38.207.3.19:HK

38.207.6.201:HK

38.207.12.74:HK

38.207.3.58:HK

38.207.12.66:HK

38.207.29.140:HK

38.207.12.82:HK

38.207.3.32:HK

38.207.6.231:HK

103.169.90.98:MY

156.234.62.148:KR

38.207.12.99:HK

38.207.29.160:HK

38.207.12.113:HK

38.207.3.13:HK

38.207.3.24:HK

156.245.13.9:HK

38.207.3.46:HK

156.245.13.5:HK

38.207.3.14:HK

38.207.29.147:HK

38.207.3.29:HK

38.207.12.122:HK

38.207.3.62:HK

38.207.12.67:HK

38.207.12.97:HK

38.207.29.173:HK

38.207.12.76:HK

38.207.12.93:HK

38.207.6.232:HK

38.207.3.27:HK

182.16.70.46:HK

154.84.24.184:JP

38.207.6.234:HK

38.207.6.224:HK

66.42.50.211:SG

38.207.29.167:HK

38.207.6.198:HK

38.207.3.10:HK

165.154.64.215:HK

38.207.3.55:HK

38.207.29.135:HK

38.207.6.253:HK

38.207.12.91:HK

38.207.3.57:HK

38.207.29.189:HK

38.207.12.84:HK

38.207.6.230:HK

38.207.6.202:HK

103.140.186.181:SG

38.207.3.31:HK

38.207.6.254:HK

38.207.6.199:HK

38.207.3.41:HK

38.207.29.145:HK

38.207.29.158:HK

38.207.12.105:HK

182.16.70.45:HK

38.207.12.70:HK

38.207.29.163:HK

38.207.6.248:HK

38.207.12.85:HK

38.207.29.184:HK

38.207.29.132:HK

38.207.3.22:HK

38.207.6.243:HK

38.207.6.227:HK

38.207.3.33:HK

103.140.186.39:SG

38.207.6.221:HK

38.207.29.144:HK

38.207.3.9:HK

182.16.70.42:HK

38.207.3.4:HK

38.207.12.117:HK

38.207.12.98:HK

182.16.70.44:HK

182.16.70.43:HK

38.207.12.120:HK

38.207.29.169:HK

38.207.12.110:HK

38.207.29.188:HK

38.207.29.178:HK

38.207.29.177:HK

38.207.12.86:HK

38.207.3.18:HK

38.207.12.72:HK

38.207.6.249:HK

38.207.12.73:HK

38.207.29.130:HK

38.207.3.37:HK

38.207.12.114:HK

38.207.12.75:HK

38.207.29.172:HK

38.207.3.49:HK

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

Please Note: The Above IOCs are also available in CERT-In Threat

Intelligence Platform.

Recommendations:

- Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-I-8080052024 Malicious Domains - Spear-Phishing & Malware Hosting Campaign**

Following domain and its subdomain are being used for spear-phishing/ host malware to target government officials:  
  
- ---------------<Malicious Domains>----------------  
mod.gov.in.reportdetails.info  
reportdetails.info  
- -------------</Malicious Domains>-----------------  
  
Kindly take the required actions.

1. **CMTX-P052024018 REDLINE STEALER MALWARE**

ALERT BRIEF:

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

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

MITRE ATT&CK Identifiers

T1059 (Command and Scripting Interpreter)

T1543 (Create or Modify System Process)

T1053 (Scheduled Task/Job)

T1027 (Obfuscated Files or Information)

T1003 (OS Credential Dumping)

T1055 (Process Injection)

T1140 (De obfuscate/Decode Files or Information)

T1547 (Boot or Logon Auto start Execution)

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

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

IP Ports    Country Code

108.166.181.182:4483,US

109.107.157.17:15866,NL

147.45.47.112:17752,DE

162.218.115.202:26392,US

163.5.160.27:51523,FR

176.123.161.158:1337,RU

185.172.128.70:3808,DE

185.215.113.117:30711,RU

185.222.58.99:55615,NL

195.133.44.41:2295,DE

23.111.173.50:8888,US

23.227.196.15:23461,US

45.137.22.150:55615,NL

5.42.92.179:18418,SE

91.92.240.220:81,NL

91.92.243.6:10425,NL

95.164.89.184:41653,DE

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

RECOMMENDATIONS

- - - - - - - Recommend to monitor connection towards the mentioned IP addresses.

- - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **[CMTX-P052024025 ArcaneDoor Activity**

ALERT BRIEF:

According to the reports, ArcaneDoor is a new cyber-espionage campaign which is suspected to be linked to Chinese hackers tracked as UAT4356 (aka Storm-1849). UAT4356 deploy two custom malwares i.e. "Line Runner" and "Line Dancer" to carry out their spying activities which help them in configuration modification, reconnaissance, network traffic capture/exfiltration and potentially lateral movement.

LINE DANCER- This implant is a memory-resident shellcode interpreter that enables adversaries to upload and execute arbitrary shellcode payloads.

LINE RUNNER- The threat actor maintains persistence using a backdoor called “Line Runner” on the compromised ASA (Adaptive Security Appliances) device using functionality related to a legacy capability that allowed for the pre-loading of VPN clients and plugins on the device.

There are two zero day vulnerabilities also that have been exploited by the hackers, tracked as CVE-2024-20353 and CVE-2024-20359.

CVE-2024-20353 (CVSS-8.6):

A Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.

CVE-2024-20359 (CVSS-6.0):

A 'Code Injection' vulnerability allows a remote, privileged attacker to escalate privileges. It is exploited in the wild, and exploit code is not publicly available.

MITRE ATT&CK Enterprise Identifiers:

Line Runner persistence mechanism (T1037)

The reboot action via CVE-2024-20353 (T1653)

Base64 obfuscation (T1140)

Hooking of the processHostScanReply() function (T0874)

Disabling syslog and tampering with AAA (T1562-001)

Injection of code into AAA and Crash Dump processes (T1055)

Execution of CLI commands (T1059)

Bypassing of the AAA mechanism (T1556)

Removal of files after execution (T1070-004)

HTTP interception for C2 communications (T1557)

HTTP C2 (T1071-001)

HTTP C2 one-way backdoor (T1102-003)

Data exfiltration over C2 (T1041)

Network sniffing (T1040)

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

IP Address

192.36.57.181

185.167.60.85

185.227.111.17

176.31.18.153

172.105.90.154

185.244.210.120

45.86.163.224

172.105.94.93

213.156.138.77

89.44.198.189

45.77.52.253

103.114.200.230

212.193.2.48

51.15.145.37

89.44.198.196

131.196.252.148

213.156.138.78

121.227.168.69

213.156.138.68

194.4.49.6

185.244.210.65

216.238.75.155

5.183.95.95

45.63.119.131

45.76.118.87

45.77.54.14

45.86.163.244

45.128.134.189

89.44.198.16

96.44.159.46

103.20.222.218

103.27.132.69

103.51.140.101

103.119.3.230

103.125.218.198

104.156.232.22

107.148.19.88

107.172.16.208

107.173.140.111

121.37.174.139

139.162.135.12

149.28.166.244

152.70.83.47

154.22.235.13

154.22.235.17

154.39.142.47

172.233.245.241

185.123.101.250

192.210.137.35

194.32.78.183

205.234.232.196

207.148.74.250

216.155.157.136

216.238.66.251

216.238.71.49

216.238.72.201

216.238.74.95

216.238.81.149

216.238.85.220

216.238.86.24

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

Recommendations:

\* Monitor the connection to/from their network perimeter devices to any of the IP addresses present in the IOC list provided above.

1. **CMTX-P052024028 RACCOON MALWARE**

ALERT BRIEF:

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

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

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

IPs: Ports: Country Code

31.172.87.216:80,DE

94.158.245.206:80,MD

5.181.156.17:80,MD

77.221.151.2:80,NL

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

Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.

Recommendations:

- - - - ------- Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient's responsibility after diligently verifying them without impacting the operations.

1. **CMTX-I-445052024 Android RAT - APT36 Campaign**

Following domains are malicious and being used as C&C/host malware (APK file) by Pakistan based APT36 threat actors. These malicious APK files are being circulated as legitimate apps to target government personnel.  
  
- ----------------<Malicious Domains> -----------------  
https://v2.androidstaticserve.com (C&C)  
https://cloudupnext.com (Hosting malware)  
- ---------------</Malicious Domains>------------------  
  
Kindly take the required actions.

1. **CMTX-P052024045 Two Critical Vulnerabilities (CVE-2024-21793 & CVE-2024-26026) Affecting F5 Next Central Manager**

ALERT BRIEF:

CVE-2024-21793

CVSS-7.5

CVE-2024-26026

CVSS-7.5

Two security vulnerabilities (CVE-2024-21793 & CVE-2024-26026) have been detected in F5 Next Central Manager, posing significant risks of exploitation by malicious actors. These vulnerabilities, once exploited, grant attackers unrestricted access to the system with administrative privileges, enabling them to establish accounts on any F5 assets managed by the Next Central Manager. These accounts remain concealed from the Central Manager due to a server-side request forgery (SSRF) vulnerability, which facilitates the invocation of an undocumented API for creating said accounts.

CVE-2024-21793 (CVSS-7.5)

An O Data injection vulnerability exists within the BIG-IP NEXT Central Manager’s API that could let attackers run harmful database commands even without logging in.

CVE-2024-26026 (CVSS-7.5)

An SQL injection vulnerability in BIG-IP Next Central Manager's API could allow an unauthenticated attacker to execute malicious SQL statements

Recommendations:-

• Prioritize patching these vulnerabilities promptly will help mitigate the risk of exploitation and enhance the company's overall cybersecurity posture.

1. **CMTX-P052024035 Active Exploitation of a critical vulnerability (CVE-2023-40000) Affecting LiteSpeed Cache plugin for WordPress**

ALERT BRIEF:

CVE-2023-40000

CVSS-8.3

It has been found that a critical vulnerability tracked as CVE-2023-40000 in the LiteSpeed Cache plugin for WordPress is actively being exploited by threat actors to create new admin users with the names wpsupp‑user and wp‑configuser. LiteSpeed Cache is a tool used on many WordPress websites to make them load faster. On successful exploitation of the vulnerability, hackers can take over the website, change its content, or even use it to spread malware.

AFFECTED VERSION- older than 5.7.0.1

Recommendations:-

• As there are high chances of attacker exploiting this vulnerability, prioritize patching the vulnerability and update it to latest version 6.2.0.1..

1. **CMTX-P052024955 SHADOWPAD Malware**

ALERT BRIEF:

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

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

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

IP Address: Port: Country Code: Last Seen

192.248.185.97:443:DE:07/05/2024

27.102.130.87:18080:KR:07/05/2024

45.158.168.113:18080:KR:07/05/2024

38.54.110.69:443:US:06/05/2024

95.179.220.73:443:FR:07/05/2024

146.196.80.175:6452:HK:07/05/2024

146.196.80.175:6452:HK:02/05/2024

95.179.220.73:443:FR:06/05/2024

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

•    Recommend to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024105 PLUGX RAT ALERT 117**

ALERT BRIEF:

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

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

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

IP Address: Port: Country Code: Last seen/ Scan Date

38.207.29.170:8443:HK:06/05/2024

38.207.6.247:8443:HK:06/05/2024

38.207.6.208:8443:HK:06/05/2024

38.207.29.148:8443:HK:06/05/2024

38.207.6.196:8443:HK:06/05/2024

38.207.6.238:8443:HK:06/05/2024

38.207.3.61:8443:HK:06/05/2024

38.207.3.60:8443:HK:06/05/2024

38.207.12.124:8443:HK:06/05/2024

103.40.11.218:80:SG:07/05/2024

38.207.12.102:8443:HK:06/05/2024

38.207.6.239:8443:HK:06/05/2024

38.207.12.71:8443:HK:06/05/2024

38.207.6.194:8443:HK:06/05/2024

38.207.29.142:8443:HK:06/05/2024

38.207.29.133:8443:HK:06/05/2024

38.207.3.45:8443:HK:06/05/2024

38.207.29.181:8443:HK:06/05/2024

38.207.3.7:8443:HK:06/05/2024

38.207.3.15:8443:HK:06/05/2024

38.207.29.138:8443:HK:06/05/2024

38.207.29.159:8443:HK:06/05/2024

38.207.3.30:8443:HK:06/05/2024

38.207.12.95:8443:HK:06/05/2024

38.207.12.106:8443:HK:06/05/2024

38.207.3.56:8443:HK:06/05/2024

38.207.3.17:8443:HK:06/05/2024

38.207.3.42:8443:HK:06/05/2024

38.207.6.215:8443:HK:06/05/2024

38.207.29.162:8443:HK:06/05/2024

38.207.29.157:8443:HK:06/05/2024

38.207.6.244:8443:HK:06/05/2024

38.207.12.116:8443:HK:06/05/2024

38.207.3.16:8443:HK:06/05/2024

38.207.29.165:8443:HK:06/05/2024

38.207.3.11:8443:HK:06/05/2024

38.207.6.195:8443:HK:06/05/2024

38.207.6.240:8443:HK:06/05/2024

38.207.3.25:8443:HK:06/05/2024

38.207.3.36:8443:HK:06/05/2024

38.207.3.52:8443:HK:06/05/2024

38.207.12.101:8443:HK:06/05/2024

38.207.3.2:8443:HK:06/05/2024

38.207.29.166:8443:HK:06/05/2024

38.207.12.94:8443:HK:06/05/2024

38.207.6.246:8443:HK:06/05/2024

38.207.12.119:8443:HK:06/05/2024

38.207.29.154:8443:HK:06/05/2024

38.207.12.68:8443:HK:06/05/2024

38.207.3.54:8443:HK:06/05/2024

38.207.6.203:8443:HK:06/05/2024

38.207.12.112:8443:HK:06/05/2024

38.207.6.219:8443:HK:06/05/2024

38.207.12.107:8443:HK:06/05/2024

38.207.29.171:8443:HK:06/05/2024

38.207.6.206:8443:HK:06/05/2024

38.207.6.214:8443:HK:06/05/2024

45.80.215.19:443:FR:06/05/2024

38.207.12.126:8443:HK:06/05/2024

38.207.6.235:8443:HK:06/05/2024

172.111.233.150:80:BE:07/05/2024

38.207.29.156:8443:HK:06/05/2024

38.207.6.197:8443:HK:06/05/2024

38.207.12.100:8443:HK:06/05/2024

38.207.6.223:8443:HK:06/05/2024

38.207.12.79:8443:HK:06/05/2024

38.207.29.175:8443:HK:06/05/2024

38.207.3.35:8443:HK:06/05/2024

38.207.3.23:8443:HK:06/05/2024

38.207.12.83:8443:HK:06/05/2024

38.207.3.21:8443:HK:06/05/2024

38.207.12.77:8443:HK:06/05/2024

38.207.12.81:8443:HK:06/05/2024

38.207.29.190:8443:HK:06/05/2024

38.207.3.6:8443:HK:06/05/2024

5.183.179.154:443:DE:07/05/2024

38.207.29.153:8443:HK:06/05/2024

38.207.6.225:8443:HK:06/05/2024

119.28.112.170:8443:SG:07/05/2024

38.207.3.47:8443:HK:06/05/2024

38.207.12.92:8443:HK:06/05/2024

38.207.12.109:8443:HK:06/05/2024

38.207.3.43:8443:HK:06/05/2024

38.207.3.8:8443:HK:06/05/2024

38.207.3.3:8443:HK:06/05/2024

38.207.6.246:8443:HK:01/05/2024

38.207.3.61:8443:HK:01/05/2024

38.207.3.20:8443:HK:01/05/2024

38.207.29.154:8443:HK:01/05/2024

38.207.6.219:8443:HK:01/05/2024

5.183.179.154:443:DE:01/05/2024

38.207.12.106:8443:HK:01/05/2024

38.207.3.23:8443:HK:01/05/2024

38.207.3.43:8443:HK:01/05/2024

38.207.3.21:8443:HK:01/05/2024

38.207.12.68:8443:HK:01/05/2024

38.207.12.116:8443:HK:01/05/2024

38.207.12.124:8443:HK:01/05/2024

38.207.3.45:8443:HK:01/05/2024

38.207.3.11:8443:HK:01/05/2024

38.207.12.83:8443:HK:01/05/2024

38.207.6.225:8443:HK:01/05/2024

38.207.12.107:8443:HK:01/05/2024

38.207.12.71:8443:HK:01/05/2024

38.207.29.153:8443:HK:01/05/2024

38.207.29.165:8443:HK:01/05/2024

38.207.3.36:8443:HK:01/05/2024

38.207.6.203:8443:HK:01/05/2024

38.207.3.3:8443:HK:01/05/2024

38.207.3.16:8443:HK:01/05/2024

38.207.3.42:8443:HK:01/05/2024

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

1. **CMTX-I-021052024 Android RAT - IOCs**

Recent C&C server IP of Android RAT/ Spynote malware are as follows:

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

64.188.24.72

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

Kindly take the required actions.

1. **CMTX-P-052024055 Black Basta Ransomware**

Alert Brief:

Black Basta ransomware group is again active in the cyber threat landscape. It gains initial access through phishing and exploiting vulnerabilities like ConnectWise, ZeroLogon, NoPac, and PrintNightmare. They follow a double-extortion approach, encrypting and stealing data. They’ve been seen using PowerShell to neutralize antivirus software and a tool named Backstab to undermine EDR systems. For lateral movement, they employ tools such as BITSAdmin, PsExec, and RDP. Victims are forced to pay the ransom, failing which their data is threatened to be published on the Black Basta TOR website. Recently, Black Basta actors targeted MDR clients with a phishing campaign, inundating them with spam and employing social engineering to gain remote access.

MITRE ATT&CK Enterprise Identifiers:

Phishing- T1566

Impair Defenses:Disable or ModifyTools- T1562.001

Command and Scripting Interpreter: PowerShell- T1059.001

Inhibit System Recovery- T1490

Data Encrypted for Impact- T1486

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

HASHES:

0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298

d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e

88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc

58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd

39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead

5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221

51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e

d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1

5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43

05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431

a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6

86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737

07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799

96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be

1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779

360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98

0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a

9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc

62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087

7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59

350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd

90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7

fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08

acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f

d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d

f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4

723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224

ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e

fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f

df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415

462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7

3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a

5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004

3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35

17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20

42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78

882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3

e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757

0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e

69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944

3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a

17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90

b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9

b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24

8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6

034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79

8C68B2A794BA3D148CAE91BDF9C8D357289752A94118B5558418A36D95A5A45F

b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24

3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc338058680407

808c96cb90b7de7792a827c6946ff48123802959635a23bf9d98478ae6a259f9

3a8fc07cadc08eeb8be342452636a754158403c3d4ebff379a4ae66f8298d9a6

4ac69411ed124da06ad66ee8bfbcea2f593b5b199a2c38496e1ee24f9d04f34a

819cb9bcf62be7666db5666a693524070b0df589c58309b067191b30480b0c3a

c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92121d4d6c3f0557ef9c881e0

d503090431fdd99c9df3451d9b73c5737c79eda6eb80c148b8dc71e84623401f

IPs:

66.249.66.18

95.181.173.227

207.126.152.242

72.14.196.50

72.14.196.192

72.14.196.2

72.14.196.226

46.161.27.151

207.126.152.242

185.219.221.136

64.176.219.106

5.78.115.67

46.8.16.77

185.7.214.79

185.220.100.240

107.189.30.69

5.183.130.92

185.220.101.149

188.130.218.39

188.130.137.181

46.8.10.134

155.138.246.122

80.239.207.200

183.181.86.147

34.149.120.3

104.21.40.72

34.250.161.149

88.198.198.90

151.101.130.159

35.244.153.44

35.212.86.55

34.251.163.236

34.160.81.203

34.149.36.179

104.21.26.145

83.243.40.10

35.227.194.51

35.190.31.54

34.120.190.48

116.203.186.178

34.160.17.71

DOMAINS:

childrensdolls.com

myfinancialexperts.com

limitedtoday.com

kekeoamigo.com

nebraska-lawyers.com

tomlawcenter.com

thesmartcloudusa.com

rasapool.net

artspathgroupe.net

specialdrills.com

thetrailbig.net

consulheartinc.com

otxcosmeticscare.com

otxcarecosmetics.com

artstrailman.com

ontexcare.com

trackgroup.net

businessprofessionalllc.com

securecloudmanage.com

oneblackwood.com

buygreenstudio.com

startupbuss.com

onedogsclub.com

wipresolutions.com

recentbeelive.com

trailcocompany.com

trailcosolutions.com

artstrailreviews.com

usaglobalnews.com

topglobaltv.com

startupmartec.net

technologgies.com

jenshol.com

simorten.com

investmentgblog.net

protectionek.com

airbusco.net

allcompanycenter.com

animalsfast.net

audsystemecll.net

auuditoe.com

bluenetworking.net

brendonline.com

businesforhome.com

caspercan.com

clearsystemwo.net

cloudworldst.net

constrtionfirst.com

erihudeg.com

garbagemoval.com

gartenlofti.com

getfnewsolutions.com

getfnewssolutions.com

investmendvisor.net

investmentrealtyhp.net

ionoslaba.com

jessvisser.com

karmafisker.com

kolinileas.com

maluisepaul.com

masterunix.net

monitor-websystem.net

monitorsystem.net

mytrailinvest.net

prettyanimals.net

reelsysmoona.net

seohomee.com

septcntr.com

softradar.net

startupbizaud.netn

startuptechnologyw.net

steamteamdev.net

stockinvestlab.net

taskthebox.net

trailgroupl.net

treeauwin.net

unitedfrom.com

unougn.com

wardeli.com

welausystem.net

wellsystemte.net

withclier.com

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

RECOMMENDATIONS:

\* Recommended to monitor connection towards the mentioned IP/Domain addresses.The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

\* Regularly update the operating system, applications, and security software. Patches often address known vulnerabilities that attackers exploit.

\* Enable MFA for critical services such as VPNs, remote desktop access, and email accounts. This adds an extra layer of security.

\* Isolate critical systems from less critical ones. Limit lateral movement for attackers within your network.

\* Educate employees about phishing techniques and safe online practices. Regular training can prevent social engineering attacks.

\* Regularly back up data to secure, offline locations. Test backups to ensure they are functional. Consider using immutable backups to prevent ransomware from affecting backups.

\* Limit user permissions to only what is necessary for their roles. Avoid unnecessary administrative privileges

\* Deploy endpoint security solutions that detect and block malicious activity. Use behavior-based detection to identify suspicious behavior.

Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.

1. **CMTX-I-636052024 Malicious Domains - Spear-Phishing Campaign**

Following malicious subdomain domain and the parent domain are associated with spear-phishing campaign targeting government officials:  
  
- ---------------<Malicious Domain>----------------  
email.niccs.online  
\*.niccs.online  
- -------------</Malicious Domain>-----------------  
  
Kindly take the required actions.

1. **CMTX-P052024038 Agent Tesla Malware Alert**

Malware Alert Brief:

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

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

103.92.235.178

203.175.9.22

86.96.202.167

45.252.248.26

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations..

1. **CMTX-P052024058 Emotet Malware**

Malware Alert Brief:

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

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

61.76.222.210 South Korea

51.89.36.180 Poland

202.79.24.136 Cambodia

115.79.195.246 Vietnam

81.213.175.132 Turkey

5.196.108.185 Netherlands

173.249.6.108 Germany

197.245.25.228 South Africa

77.74.78.80 Russia

130.0.132.242 Italy

49.205.182.134 India

173.212.214.235 Germany

51.75.33.127 Poland

51.159.23.217 France

51.38.124.206 Germany

91.121.87.90 France

83.110.223.58 United Arab Emirates

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024078 RACCOON MALWARE**

ALERT BRIEF:

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

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

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

94.142.138.49 Netherlands

193.142.147.59 Seychelles

94.142.138.108 Netherlands

88.119.161.188 India

185.244.48.191 Netherlands

5.42.64.13 Russia

195.20.16.155 Russia

94.142.138.228 Russia

146.19.173.87 Seychelles

172.86.75.59 Netherlands

178.20.41.15 Russia

91.103.252.65 Netherlands

77.221.151.21 Singapore

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

1. **CMTX-P052024088 Redline malware**

Malware Alert Brief:

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

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

185.215.113.67 Seychelles

185.172.128.33 Germany

5.42.65.96 Russia

94.156.67.67 Netherlands

89.23.97.100 Russia

89.23.100.222 Russia

65.108.20.226 Germany

135.181.11.35 Finland

91.92.248.129 Netherlands

15.165.134.129 Korea,  South

194.26.232.43 Netherlands

45.15.156.167 Netherlands

185.215.113.117 Seychelles

45.15.156.142 Netherlands

185.125.50.49 Russia

195.2.78.228 Russia

89.23.96.163 Russia

45.15.156.216 Netherlands

194.36.178.33 Singapore

195.20.16.134 Russia

95.164.89.184 Germany

91.92.249.24 Netherlands

45.89.53.206 Ukraine

65.108.19.51 Germany

91.92.249.182 Netherlands

147.45.47.42 Russia

109.120.178.235 Singapore

5.42.92.179 Sweden

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

1. **CMTX-P052024118 Ursnif malware**

Malware Alert Brief:

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

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

38.239.98.13 China

34.128.82.12 Indonesia

34.126.189.157 Singapore

34.143.166.163 Singapore

34.242.73.233 Ireland

3.126.57.221 Germany

99.81.95.247 Ireland

3.126.205.164 Germany

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

RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024108 Trickbot malware Alert**

Malware Alert Brief:

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

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

41.77.134.250 Mozambique

175.184.232.234 Indonesia

103.75.32.173 India

103.201.142.30 India

27.109.116.144 Cambodia

177.190.76.82 Brazil

196.41.57.46 Tanzania

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
RECOMMENDATIONS:  
  
Recommended to monitor connection towards the mentioned IP/Domain addresses.  
The list may include compromised Domain resources as well. Blocking the Domains is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024068 Qbot Malware**

Malware Alert Brief:

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

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

5.61.49.13 Netherlands

89.31.143.90 Germany

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

1. **CMTX-P052024048 Amadey Malware Alert**

Malware Alert Brief:

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

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

185.196.10.188 Switzerland

185.172.128.19 Germany

188.40.122.96 Germany

78.46.242.112 Germany

91.195.240.117 Germany

62.182.156.153 Russia

207.154.243.184 Germany

79.137.203.59 Germany

5.42.64.33 Austria

185.215.113.204 Seychelles

79.137.203.19 Germany

185.215.113.35 Seychelles

171.33.86.64 France

5.42.65.80 Russia

193.233.20.14 Russia

103.21.58.238 India

101.99.77.207 Malaysia

137.59.110.238 Malaysia

62.204.41.104 Russia

5.45.75.199 Netherlands

93.123.39.96 Bulgaria

134.0.116.60 Russia

176.97.64.128 Singapore

5.61.28.102 Iran

188.40.187.155 Germany

138.201.203.107 Germany

172.111.138.100 Thailand

202.45.144.21 Nepal

111.90.144.246 Malaysia

102.222.20.84 South Africa

103.145.36.52 India

185.215.113.38 Seychelles

62.204.41.252 Russia

216.10.241.193 India

23.251.131.105 Belgium

34.91.32.224 Netherlands

103.13.112.102 India

49.44.53.44 India

103.21.58.112 India

49.44.53.42 India

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

1. **CMTX-P052024098 SocGholish malware**

Malware Alert Brief:

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

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

77.245.56.14 Netherlands

101.44.249.115 China

101.44.249.154 China

101.44.162.229 Singapore

101.44.249.124 China

101.44.251.150 China

101.44.251.246 China

101.44.250.93 China

101.44.249.33 China

101.44.250.180 China

101.44.251.173 China

101.44.162.45 Singapore

101.44.163.232 Singapore

101.44.251.87 China

101.44.161.71 Singapore

101.44.248.87 China

101.44.248.91 China

101.44.251.49 China

101.44.249.242 China

101.44.249.224 China

101.44.162.166 Singapore

101.44.163.159 Singapore

101.44.160.20 Singapore

101.44.161.93 Singapore

101.44.250.84 China

101.44.248.250 China

101.44.250.46 China

101.44.161.51 Singapore

101.44.249.141 China

101.44.160.37 Singapore

195.24.68.25 Russia

101.44.249.85 China

185.216.114.10 Turkey

101.44.249.3 China

217.160.0.215 Germany

92.53.96.139 Russia

110.238.109.217 Singapore

124.243.136.201 Singapore

190.92.200.155 Singapore

178.128.62.153 Singapore

101.44.248.236 China

101.44.163.112 Singapore

101.44.160.205 Singapore

101.44.160.177 Singapore

101.44.250.35 China

101.44.251.37 China

101.44.160.189 Singapore

101.44.161.14 Singapore

101.44.162.16 Singapore

101.44.251.24 China

101.44.248.152 China

101.44.251.80 China

101.44.160.41 Singapore

101.44.162.130 Singapore

101.44.162.230 Singapore

101.44.160.128 Singapore

101.44.249.61 China

101.44.161.254 Singapore

101.44.249.92 China

101.44.161.77 Singapore

101.44.161.177 Singapore

101.44.160.158 Singapore

101.44.160.186 Singapore

101.44.161.205 Singapore

101.44.162.235 Singapore

101.44.250.106 China

103.212.98.210 China

31.220.15.143 Sweden

217.160.0.246 Germany

94.74.86.73 Singapore

159.138.105.142 Singapore

49.0.207.20 Singapore

190.92.216.34 Singapore

101.44.250.250 China

162.158.54.21 India

101.44.248.118 China

101.44.160.68 Singapore

101.44.250.212 China

101.44.250.140 China

101.44.251.174 China

101.44.248.7 China

101.44.250.19 China

101.44.250.230 China

101.44.251.103 China

101.44.160.204 Singapore

190.92.211.188 Singapore

190.92.216.77 Singapore

190.92.216.94 Singapore

119.13.100.35 Singapore

119.8.164.26 Singapore

124.243.138.168 Singapore

101.44.250.248 China

101.44.161.208 Singapore

119.13.100.165 Singapore

103.249.111.96 China

94.102.51.95 Netherlands

31.43.191.220 Azerbaijan

65.108.125.120 Finland

35.215.148.34 China

124.243.134.32 Singapore

159.138.99.105 Singapore

159.138.103.36 Singapore

190.92.205.226 Singapore

110.238.107.76 Singapore

168.76.20.229 South Africa

159.138.82.138 Singapore

136.243.220.209 Germany

119.8.189.192 Singapore

190.92.213.10 Singapore

94.74.82.64 Singapore

190.92.201.44 Singapore

119.13.101.155 Singapore

49.0.204.143 Singapore

159.138.109.164 Singapore

190.92.218.81 Singapore

124.243.134.180 Singapore

190.92.202.5 Singapore

124.243.148.208 Singapore

159.138.109.15 Singapore

190.92.216.156 Singapore

154.118.228.212 Tanzania

154.118.228.210 Tanzania

5.101.115.147 Estonia

119.13.108.89 Singapore

94.74.86.10 Singapore

124.243.132.91 Singapore

124.243.144.175 Singapore

119.13.103.43 Singapore

94.74.86.81 Singapore

159.138.103.220 Singapore

124.243.151.132 Singapore

119.13.101.211 Singapore

124.243.151.1 Singapore

159.138.105.174 Singapore

190.92.212.116 Singapore

94.74.85.211 Singapore

159.138.98.180 Singapore

124.243.138.37 Singapore

81.169.145.166 Germany

159.138.111.108 Singapore

147.236.231.12 Israel

49.0.204.165 Singapore

94.74.81.152 Singapore

119.13.105.238 Singapore

124.243.137.32 Singapore

124.243.139.173 Singapore

190.92.213.192 Singapore

190.92.221.220 Singapore

105.214.1.136 South Africa

93.157.28.30 Ukraine

110.238.110.49 Singapore

159.138.102.121 Singapore

119.13.102.196 Singapore

119.13.111.116 Singapore

124.243.133.99 Singapore

124.243.139.76 Singapore

49.0.205.1 Singapore

49.0.205.110 Singapore

94.74.84.205 Singapore

114.119.174.174 Singapore

124.243.135.231 Singapore

124.243.139.58 Singapore

159.138.96.119 Singapore

213.180.203.227 Russia

93.190.41.79 Ukraine

103.43.18.250 China

185.192.16.52 Qatar

5.255.231.107 Russia

87.250.224.238 Russia

103.164.81.98 Singapore

54.36.145.173 Spain

103.108.130.40 Indonesia

41.80.117.254 Kenya

171.238.63.87 Vietnam

209.35.167.131 Philippines

176.111.174.153 Russia

119.8.189.12 Singapore

190.92.208.167 Singapore

124.243.135.130 Singapore

145.239.23.7 Poland

119.13.100.91 Singapore

114.119.188.227 Singapore

101.91.134.135 China

156.146.45.236 China

94.74.86.0 Singapore

124.243.136.164 Singapore

103.130.219.128 Vietnam

119.13.110.128 Singapore

94.74.81.25 Singapore

49.0.200.240 Singapore

124.243.147.143 Singapore

119.13.103.16 Singapore

124.243.133.194 Singapore

124.243.135.236 Singapore

124.243.150.185 Singapore

159.138.87.228 Singapore

159.138.107.49 Singapore

190.92.207.126 Singapore

190.92.209.68 Singapore

190.92.212.240 Singapore

110.238.111.178 Singapore

119.13.100.146 Singapore

124.243.137.156 Singapore

124.243.150.210 Singapore

159.138.111.76 Singapore

110.238.110.240 Singapore

49.0.206.247 Singapore

94.74.91.100 Singapore

110.238.109.69 Singapore

110.238.110.173 Singapore

110.238.111.143 Singapore

114.119.191.138 Singapore

119.8.160.152 Singapore

119.8.174.80 Singapore

119.13.106.164 Singapore

159.138.96.117 Singapore

159.138.98.152 Singapore

190.92.199.115 Singapore

190.92.202.240 Singapore

190.92.218.78 Singapore

119.8.182.13 Singapore

124.243.135.66 Singapore

159.138.110.8 Singapore

49.0.202.170 Singapore

114.119.173.19 Singapore

119.8.163.174 Singapore

119.8.184.79 Singapore

124.243.135.114 Singapore

124.243.138.34 Singapore

124.243.148.114 Singapore

124.243.150.207 Singapore

159.138.84.3 Singapore

190.92.199.75 Singapore

190.92.202.17 Singapore

190.92.205.141 Singapore

190.92.206.5 Singapore

190.92.209.6 Singapore

110.238.108.75 Singapore

124.243.134.100 Singapore

124.243.133.152 Singapore

94.74.88.121 Singapore

124.243.133.84 Singapore

124.243.133.174 Singapore

159.138.86.86 Singapore

190.92.209.33 Singapore

190.92.209.184 Singapore

119.8.191.240 Singapore

190.92.221.166 Singapore

92.205.215.210 Germany

110.238.105.241 Singapore

119.13.100.213 Singapore

190.92.209.78 Singapore

111.59.4.88 China

213.239.204.39 Germany

216.24.213.76 Germany

103.251.2.17 Malaysia

49.0.202.9 Singapore

49.0.203.90 Singapore

94.74.81.247 Singapore

94.74.87.150 Singapore

94.74.89.166 Singapore

94.74.90.18 Singapore

110.238.104.11 Singapore

110.238.104.149 Singapore

110.238.111.118 Singapore

114.119.175.21 Singapore

114.119.183.63 Singapore

119.8.180.239 Singapore

119.13.100.118 Singapore

119.13.102.48 Singapore

119.13.104.159 Singapore

124.243.134.156 Singapore

124.243.134.178 Singapore

124.243.134.238 Singapore

124.243.136.184 Singapore

124.243.138.123 Singapore

124.243.138.211 Singapore

124.243.138.234 Singapore

124.243.139.136 Singapore

124.243.148.133 Singapore

124.243.150.61 Singapore

146.190.108.97 Singapore

159.138.96.146 Singapore

159.138.105.87 Singapore

159.138.111.129 Singapore

159.138.122.45 Singapore

190.92.198.2 Singapore

190.92.198.120 Singapore

190.92.209.117 Singapore

190.92.210.30 Singapore

190.92.219.69 Singapore

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

1. **CMTX-P052024686 QuasarRAT Malware ALERT 51**

ALERT BRIEF:

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

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

IP ADDRESSES: PORTS Last Seen Country Code

195.88.218.231:4782, 12-05-2024 US

95.179.245.127:4782, 8848,06-10-2022 DE

209.126.4.168:4782, 12-05-2024 US

114.132.87.123:4782, 10-05-2024 CN

94.156.79.113:4782, 12-05-2024 BG

101.33.253.250:4782, 12-05-2024 CN

103.253.73.222:118, 17-03-2024 TH

45.77.60.172:4782, 12-05-2024 FR

106.119.250.55:4782, 12-05-2024 CN

193.124.33.141:4782, 12-05-2024 RU

137.184.235.95:4782, 12-05-2024 US

185.161.208.116:4441, 12-05-2024 NL

93.123.85.108:4782, 04-05-2024 GB

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

1. **CMTX-I-200052024 Mythic Malware - APT36 campaign**

Following IP is the C&C associated with Mythic Malware. This RAT could possibly be used by the Pakistan based threat actors under APT36 campaign to target Linux based systems in government offices.

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

38.60.254.215

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

1. **CMTX-I-404052024 SideCopy - C&C of Malware Campaign**

Following IOCs are associated with SideCopy malware campaign.  
  
- ----------------------------- <IOCs> -------------------------  
64.188.27.144  
reviewassignment.online  
reviewassignment.in (compromised website)  
- ---------------------------- </IOCs> -------------------------

1. **CMTX-I-587052024 Malicious Domains - Spear-Phishings**

With reference to CMTX-I-053042024 dated 30/04/2024 and CMTX-I-025052024 dated 01/05/2024, additional domains associated with spear-phishing/malware hosting are as follows:

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

www.mod.gov.in.reportscases.info

\*.reportscases.info

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

Kindly take the required actions.

1. **CMTX-I-333052024 APT36 campaign**

Recent C&C server IP and domain of malware used by Pakistan based APT36 threat actors are as follows:  
  
- ------------------ <C&C> ----------------  
supplyprodaily.servehttp.com  
84.247.170.237  
- ----------------- </C&C>-----------------

1. **CMTX-I-400052024 Pakistan Based Malware Campaign**

Recent C&C server domains of malwares used by Pakistan based threat actors to target government officials are as follows:  
  
- ------------ <C&C Domains> ------------  
dns1.indianblog.xyz  
ur253.duckdns.org  
\*. indianblog.xyz  
- ----------- </C&C Domains>-------------  
  
If DDNS domain like duckdns.org, is not being accessed by your organization then the parent domain can be blocked.

Kindly take the required actions.

1. **CMTX-P052024965 SHADOWPAD Malware**

ALERT BRIEF:

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

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

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

IP Address: Port: Country Code:

118.194.251.224:8000:TH

45.125.12.239:8000, 443, 8443:HK

185.167.61.179:8081, 8080:DE

182.156.212.154:8443:IN

154.90.58.56:443:SG

45.125.12.239:8443:HK

185.167.61.179:8081:DE

165.227.179.19:8000:US

185.76.78.78:443:IT

182.74.183.226:8443:IN

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

1. **CMTX-P052024058 Emotet Malware**

Malware Alert Brief:

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

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

61.76.222.210 South Korea

51.89.36.180 Poland

202.79.24.136 Cambodia

115.79.195.246 Vietnam

81.213.175.132 Turkey

5.196.108.185 Netherlands

173.249.6.108 Germany

197.245.25.228 South Africa

77.74.78.80 Russia

130.0.132.242 Italy

49.205.182.134 India

173.212.214.235 Germany

51.75.33.127 Poland

51.159.23.217 France

51.38.124.206 Germany

91.121.87.90 France

83.110.223.58 United Arab Emirates

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

RECOMMENDATIONS:

Recommended to monitor connection towards the mentioned IP addresses. The list may include compromised IP resources as well. Blocking the IP is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024205 PLUGX RAT ALERT 118**

ALERT BRIEF:

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

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

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

IP Address: Port: Country Code

103.43.18.71:80, 443:HK

38.207.29.131:8443:HK

103.107.105.81:10082, 443, 5000:HK

139.84.139.205:8080:IN

139.180.222.28:443:SG

154.86.159.23:443:HK

38.207.29.183:8443:HK

103.85.24.165:80, 443, 53:JP

38.89.72.143:443:GB

52.198.183.214:80, 443:JP

103.56.18.101:443:HK

45.150.64.5:80:RU

52.198.183.214:80:JP

103.43.18.71:80:HK

103.85.24.165:80:JP

103.107.105.81:443:HK

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

1. **CMTX-P052024696 QuasarRAT Malware ALERT 52**

ALERT BRIEF:  
  
Quasar is a fast and light-weight publically available Windows remote administration tool coded in C# largely used by nation sponsored threat actors. Quasar RAT has capability of capturing screenshots, Key logger, gather System Information, remote Shell and Command execution, reversing proxy, Managing tasks and files, Configuring and building client executables.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC START\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
IP ADDRESSES: PORTS              Last Seen      Country Code  
  
108.165.179.33:442,    16-05-2024,    BR  
65.20.83.4:4782,    16-05-2024,    IN  
193.142.59.109:6546,    16-05-2024,    NL  
14.225.208.152:9999,    16-05-2024,    VN  
209.97.160.36:4782,    16-05-2024,    SG  
47.120.35.45:4782,    16-05-2024,    CN  
101.42.25.79:4782,    16-05-2024,    CN  
89.121.228.226:25565,    16-05-2024,    RO  
45.138.16.208:7000,    15-05-2024,    PL  
185.148.242.80:1337,    16-05-2024,    TR  
  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **CMTX-I-409052024 AllaKore RAT - APT36 campaign**

IOCs of AllaKore RAT malware used by Pakistan based APT36 threat actors are as follows:  
  
- -------------- <IOCs> ------------  
47.109.90.24  
120.78.74.120  
- ------------- </IOCs>------------  
  
Kindly take the required actions.

1. **CMTX-P052024706 GH0ST RAT Malware**

ALERT BRIEF:

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

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

IP ADDRESSES: PORTS, Country Code, Last Seen

149.210.102.111:443, GR , 17-05-2024

62.234.90.4:8000, CN, 14-05-2024

125.228.229.229:3456, TW, 16-05-2024

1. **CMTX-P052024128 REDLINE STEALER MALWARE**

ALERT BRIEF:

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

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

MITRE ATT&CK Identifiers

T1059 (Command and Scripting Interpreter)

T1543 (Create or Modify System Process)

T1053 (Scheduled Task/Job)

T1027 (Obfuscated Files or Information)

T1003 (OS Credential Dumping)

T1055 (Process Injection)

T1140 (De obfuscate/Decode Files or Information)

T1547 (Boot or Logon Auto start Execution)

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

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

IP Ports    Country Code

147.45.47.36:39849,DE

147.45.47.93:80,DE

185.216.70.15:65012,LT

185.29.10.215:15548,SE

80.66.81.134:80,RU

80.66.81.136:80,RU

80.66.81.137:80,RU

80.66.81.138:80,RU

80.66.81.2:80,RU

80.66.81.3:80,RU

80.66.89.146:80,RU

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

RECOMMENDATIONS

- - - - - - - Recommend to monitor connection towards the mentioned IP addresses.

- - - - - - - The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

1. **CMTX-P052024138 RACCOON MALWARE**

ALERT BRIEF:

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

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

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

IPs: Ports: Country Code

5.42.96.142:80,RU

77.221.151.82:80,NL

91.92.242.162:80,NL

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

1. **CMTX-I-304052024 Malicious Domains - Spear-Phishing**

With reference to CMTX-I-053042024 dated 30/04/2024, CMTX-I-025052024 dated 01/05/2024 and CMTX-I-587052024 dated 15/05/2024, additional domains associated with spear-phishing/malware hosting are as follows:  
  
- ----------------<Malicious Domain>----------------  
nia.gov.in.investigationreport.info  
\*.investigationreport.info  
- --------------</Malicious Domain>-----------------  
  
Kindly take the required actions.

1. **CMTX-P052024065 BlackTech Actor Activity**

ALERT BRIEF:

Aliases: Circuit Panda, Earth Hundun, HUAPI, Manga Taurus, Palmerworm, Red Djinn, and Temp.Overboard

Malwares Used :Waterbear RAT and Deuterbear RAT

According to the reports, a new China linked threat actor group called "BlackTech" is active in the cyber threat landscape. They use malwares named Waterbear (aka DBGPRINT) and Deuterbear to infect computers and steal information.

Deuterbear has advanced capabilities such as including support for shellcode plugins, avoiding handshakes for RAT operation, and using HTTPS for C&C communication, uses shellcode format, possesses anti-memory scanning, and shares a traffic key with its downloader unlike Waterbear.

MITRE ATT&CK Enterprise Identifiers:

Execution- T1129

Hijack Execution Flow: DLL Side-Loading-T1574.002

Boot or Logon Autostart Execution: Print Processors-T1547.012

Process Injection-T1055

Deobfuscate/Decode Files or Information-T1140

Execution Guardrails-T1480

Virtualization/Sandbox Evasion: Time Based Evasion-T1497.003

Debugger Evasion-T1622

File and Directory Discovery-T1083

System Network Configuration Discovery: Internet Connection Discovery-T1016.001

System Network Connections Discovery-T1049

Process Discovery-T1057

System Information Discovery-T1082

Query Registry-T1012

Remote Services: Windows Remote Management-T1021.006

Data from Local System-T1005

Exfiltration Over Command-and-Control Channel-T1041

Application Layer Protocol: Web Protocols-T1071.001

Encrypted Channel-T1573

Data Encoding: Non-Standard Encoding-T1132.002

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

HASHES:

88336746f2cf1034871c4ee334fae0d30c3eb101df6f3f1c94c777639293a031

609120ab45745bcfe8abc244ea1501ef563cb666abd9d730413c3986a76fb23d

3ecbca7bf2e4557e92595fe23872658bc3337e6f77a3aff02fb7b460272de7f4

d4b5127988fde3704193a30840e991dc745aea051d1551c7cb6f55853c8cb9da

974c407dd918ccba245da0fb9d5a68f123c78aacfa85cdaba2271d6ad81380ae

3d8512a513e5f94ce49a742ae3e4853775f05d7481b29bfacef4316d7ba3bde2

057a0e0f522cc217ba8754abbb67f8a667c0054fe0dcdaf01f4930d75cd667cc

31c76585ea703f96c95efab0778f599d8dc5c26eea5d155ce24f614e6bfe9e8c

DOMAINS:

quadrantbd.com

taishanlaw.com

bakhell.com

gelatosg.com

operatida.com

randaln.com

nestnewhome.com

dailteeau.com

lucashnancy.com

ccarden.com

availitond.com

gayionsd.com

rchitecture.org

operatida.com

centralizebd.com

There can be multiple subdomains for every domain mentioned above. Please monitor the same.

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

Recommendations:

\* Forbid the use of unused or unauthorized remote access tools. Implement technical controls to restrict access to these tools. Additionally, set up monitoring mechanisms to track the usage of approved tools and detect any unauthorized usage or suspicious activities.

\* Systems having an antivirus and a malware protection program on it and making sure they are always up to date. Systems and installed applications being fully patched and updated.

\* Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints. Perform regular backup of all the critical information to minimize the loss.

\* All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software.

1. **CMTX-P052024075 Zero Day Vulnerability in QNAP QTS**

ALERT BRIEF:

A stack buffer overflow zero day vulnerability tracked as CVE-2024-27130 is present in the "No\_Support\_ACL function" of share.cgi, which is part of the QNAP QTS operating system used in Network Attached Storage (NAS) devices. Once this flaw is exploited successfully, it can lead to remote code execution on the affected system if specific prerequisites are met. The vulnerability arises due to the unsafe use of the ‘strcpy’ function within the No\_Support\_ACL function.

In this case, the vulnerable function is accessed via the get\_file\_size request in the share.cgi script. When sharing media with external users, this function is invoked.

Recommendations:

• The vulnerability has the potential for Remote Code Execution (RCE) and is associated with a history of ransomware attacks targeting QNAP devices, it is strongly recommended to prioritize patching to mitigate the risk of exploitation by threat actors who may leverage it to launch cyber threats such as ransomware attacks or other malicious activities.

• Restricted access to the share.cgi script and other sensitive functions can help in avoiding unnecessary exploitation. NAS devices should be isolated from critical systems and their exposure to external networks should be limited.