**Cyber Security Advisories**

**Date: 16 December 2024**

1. **TA-PHI-2024-12-04-001**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email contains a link email contains a link "https://mail-nics.online/" which is suspected to be mimicked/cloned page of a known website.

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

**URL:-**

https://mail-nics.online/

**Domain:-**

mail-nics.online

**IP:-**

104.21[.73.87

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

1. **TA-APT-2024-12-04-002**

It has been observed that APT 19, also known as Deep Panda, Codoso, C0d0so0, Bronze Firestone, Bronze Logan, Chlorine, Codoso, Group24, PeaceFrog, Pupa, Shell Crew and Sunshop Group is a state-sponsored threat group. Adversary uses tools such as EMPIRE and BEACON to facilitate their operations. APT 19 has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high-tech, education, manufacturing, and legal services, particularly focusing on espionage and intellectual property theft. In order to access shared files over SMB, APT19 uses strategies like lateral movement using legitimate accounts and sophisticated malware deployment, which frequently poses as legitimate software to avoid detection. The group has been linked to zero-day exploits used in wateringhole intrusions as well as direct spear-phishing activity. The group is associated with other threat actors like APT10 and APT33.

**IMPACTS:**

APT19 Uses CVE-2021-44228 (also known as "Log4Shell") in a Variety of Products to Install the COLDSTEEL Backdoor.

**DISTRIBUTION METHODS:**

APT 19 employs a variety of distribution methods to compromise targets, including:

* Spearphishing Emails: Sending emails with malicious attachments in RTF and XLSM formats
* Watering Hole Attacks: Compromising websites to infect visitors
* Strategic Web Compromises: Leveraging vulnerabilities in websites to redirect visitors to attacker-controlled infrastructure
* Drive-by Downloads: Infecting users' systems by exploiting vulnerabilities in browsers and plugins

**Recommendations:**

* Perform Regular Security Audits: Assess the security posture of your organization and identify potential vulnerabilities.
* Implement Network Segmentation: Isolate critical systems to limit the spread of an attack.
* Backup Data Regularly: Ensure that critical data is backed up and can be restored in case of a breach.
* Collaborate with Threat Intelligence Providers: Stay informed about the latest threats and share information with the cybersecurity community.

1. **TA-APT-2024-12-04-001**

It has been observed that 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IP:**

216.172.103.34

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

1. **TA-MAW-2024-12-04-001**

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:**

51.120.244.179

185.196.11.177

84.54.51.159

95.214.52.175

20.205.11.156

199.195.249.124

143.198.228.15

2.58.95.123

79.110.48.149

94.156.65.229

185.196.8.32

93.123.85.175

91.92.254.164

5.181.80.139

104.243.46.182

185.196.10.155

**Domains:**

stresser.pw

akenosec.xyz

cnc.changeme.com

report.changeme.com

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

1. **VA-2024-12-05-001**

Please find below link for the monthly CVE - KB Correlation list of Nov 2024 for your perusal and necessary action.

https://nciipc.gov.in/advisories/CVE/CVE-KB/2024/Nov.html

The list consists of 91 CVEs and their corresponding KBs for the month of Nov 2024

1. **TA-MAW-2024-12-06-002**

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

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

IP Addresses:

185.208.207.3

47.236.136.217

74.50.83.218

178.72.70.23

103.146.40.5

47.237.132.148

103.210.94.67

120.85.112.93

8.219.237.171

77.239.213.82

120.85.116.36

77.239.220.42

178.72.71.10

103.210.94.94

64.235.37.140

154.216.19.215

89.22.230.162

45.207.211.103

189.243.239.209

122.96.48.167

165.140.105.30

47.236.131.179

47.236.50.100

47.237.94.12

47.237.115.171

47.84.69.78

120.85.142.254

217.160.89.196

181.215.193.5

8.222.225.103

108.14.4.252

89.38.215.133

27.43.206.43

45.137.70.156

185.239.242.82

103.210.94.73

119.200.13.201

111.248.155.112

178.18.207.174

164.90.207.212

82.86.101.248

120.226.28.56

187.195.84.126

111.48.134.36

187.131.108.166

188.177.20.243

38.110.228.166

103.210.94.228

5.141.103.20

112.94.96.18

220.198.240.226

27.43.204.66

154.213.187.182

187.152.207.227

120.85.112.249

59.184.49.3

58.71.193.242

26.168.14.104

27.43.205.233

222.141.116.113

111.92.243.26

175.107.36.136

59.182.77.236

102.212.40.135

120.61.254.213

31.220.1.88

117.219.47.96

27.43.206.156

59.184.251.245

59.184.255.177

27.207.247.137

27.47.3.14

117.200.200.90

222.141.42.236

223.13.63.12

42.232.27.36

195.18.18.136

59.183.96.61

117.207.242.14

27.43.207.222

219.70.180.55

103.208.230.127

27.7.221.241

182.121.88.90

185.120.214.61

110.182.184.199

117.208.216.0

117.219.85.121

182.119.177.230

110.183.18.176

27.47.3.67

113.25.135.233

103.210.94.188

201.145.135.158

117.199.104.58

121.31.203.16

125.46.211.164

110.182.11.170

103.15.254.163

5.141.103.208

111.48.114.88

117.217.44.20

101.232.32.140

185.225.17.189

103.245.236.146

103.149.87.69

120.85.115.155

43.225.109.30

93.113.57.21

117.251.176.107

27.47.2.159

120.85.113.126

186.123.81.229

122.97.214.213

189.133.214.24

175.107.2.23

191.58.113.26

195.18.18.104

103.199.200.238

120.85.118.78

120.85.116.27

103.199.180.83

120.85.118.157

120.85.187.66

120.85.184.126

77.239.211.33

112.94.99.234

77.239.211.124

122.96.50.213

187.234.205.169

158.181.36.10

120.85.118.190

31.220.84.246

100.42.180.126

103.210.94.105

72.130.248.168

93.123.85.192

103.210.94.186

120.85.115.221

112.94.99.167

178.72.75.84

31.172.87.21

46.8.194.147

187.228.119.76

87.120.116.226

URLs:-

http://45.115.89.134:50723/

http://58.47.43.217:46945/

http://112.248.110.61:58962/

http://59.89.204.254:60618/

http://117.253.97.188:33443/

http://125.41.228.209:47067/

http://116.212.129.1:46583/

http://27.111.75.37:60458/

http://223.8.216.115:55024/

http://59.97.112.41:39702/

http://45.64.226.152:48399/

http://117.219.44.68:45838/

http://111.91.162.209:39595/

http://103.15.255.244:36209/

http://117.88.229.163:35816/

http://1.70.15.232:51817/

http://180.115.175.71:41772/

http://103.197.115.211:37712/

http://117.63.21.35:44023/

http://105.101.251.23:56754/

http://39.164.115.233:12548/

http://102.51.1.6:57308/

http://182.112.3.118:48924/

http://27.111.75.188:55828/

http://117.199.104.58:59982/

http://121.31.203.16:40498/

http://223.13.63.12:60514

http://110.183.18.176:49735

http://110.182.11.170:59331

http://101.232.32.140:58565

http://125.46.211.164:37250

http://103.15.254.163:37836

http://117.207.242.14:41242

http://117.199.104.58:59982

http://59.184.251.245:45198

http://59.184.255.177:45939

http://27.7.221.241:47456

http://103.208.230.127:48500

http://117.208.216.0:45734

http://117.219.85.121:49993

http://121.31.203.16:40498

http://113.25.135.233:49801

http://111.48.114.88:42472

http://182.121.88.90:47660

http://222.141.116.113:46934

http://59.182.77.236:32939

http://110.182.184.199:60302

http://175.107.36.136:36858

http://117.219.47.96:38486

http://42.232.27.36:52733

http://27.207.247.137:44172/

http://117.200.200.90:40285/

http://5.141.103.208:41315/

http://185.120.214.61:50444/

http://222.141.42.236:36895/

http://59.183.96.61:56769/

http://117.217.44.20:37772/

http://182.119.177.230:58616/

http://219.70.180.55:35848/

http://223.13.63.12:60514/

http://192.21.168.210:38377/

http://120.61.20.150:60502/

http://39.79.207.47:41359/

http://39.164.25.75:36142/

http://45.230.66.1:11507/

http://175.150.56.37:59953/

http://220.158.158.128:33151/

http://175.150.76.130:47330/

http://182.127.168.104:39374/

http://115.54.217.136:55924/

http://117.243.240.249:35264/

http://103.15.254.236:45457/

http://222.141.189.45:58843/

http://175.107.37.233:48015/

http://180.115.127.72:37173/

http://27.17.190.28:55621/

http://124.234.245.36:55451/

http://45.115.89.245:44790/

http://117.221.175.152:55750/

http://59.99.209.111:38732/

http://175.149.118.75:53206/

http://117.251.178.74:54718/

http://115.60.203.38:38909/

http://182.116.120.148:52627/

http://45.115.89.229:42217/

http://42.7.243.70:36245/

http://223.13.87.9:42151/

http://117.219.87.164:45292/

http://59.178.68.145:51330/

http://102.33.12.109:59088/

http://222.140.185.40:58761/

http://103.200.86.125:56423/

http://117.254.98.128:60485/

http://117.209.85.146:41434/

http://123.4.198.173:60974/

http://175.107.2.236:33019/

http://117.242.193.83:45410/

http://182.119.183.222:53914/

http://117.217.56.192:36481/

http://222.138.18.171:34736/

http://117.254.100.63:49099/

http://182.127.100.94:35101/

http://42.233.106.193:56273/

http://1.70.9.101:55138/

http://113.25.134.166:44971/

http://61.2.108.255:35284/

http://42.236.222.94:58825/

http://102.51.60.197:55386/

http://223.10.123.3:55888/

http://45.230.66.22:11793/

http://180.108.19.54:36809/

http://222.137.131.149:56197/

http://117.209.17.89:40450/

http://59.89.236.87:52218/

http://45.115.89.3:49911/

http://114.218.129.196:58087/

http://222.90.3.59:60370/

http://168.196.169.80:49316/

http://103.15.254.237:35685/

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

1. **TA-TAG-2024-12-06-001**

It has been observed that state-sponsored threat actors have increasingly targeted Indian government agencies/organisations with cyber-espionage campaigns, leveraging phishing, social engineering, and customs malware to steal sensitive information. These attacks often aim to compromise critical infrastructure and gain long-term access to systems for intelligence gathering.

**Common Features of Malware Deployed:**

* Phishing-Based Delivery: Malware is typically delivered through spear-phishing emails with malicious attachments or links.
* Data Exfiltration: Designed to steal documents, credentials, and other sensitive data.
* Persistence Mechanisms: Use of techniques like backdoors, scheduled tasks, autoruns to maintain long-term access.
* Camouflage: Malware disguised as legitimate files or applications to evade detection.
* Command & Control (C2) Communication: Use of Command and Control servers to receive instructions and exfiltrate data.

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

IPs:-

154.53.42.194

66.219.22.102

144.126.152.205

209.126.6.227

154.38.160.218

167.86.113.241

109.123.244.46

23.88.26.187

209.126.11.251

173.249.7.111

149.102.140.36

130.185.119.198

176.57.184.97

84.247.181.64

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

1. **TA-APT-2024-12-06-003**

It has been observed that 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

IP:

96.47.234.145

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

1. **TA-PHI-2024-12-06-002**

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 which are targeting Critical Sector Entities (CIIs).

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

**Domains:**

indianoil.cn

\*.in.services

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

1. **VA-2024-12-06-002**

**Vulnerability in Concert Ticket Ordering System**

A sql injection vulnerability has been discovered in code-projects Concert Ticket Ordering System 1.0.

CVE ID: CVE-2024-11970(Critical)

**Vulnerability in PHPGurukul Complaint Management System**

A sql injection vulnerability has been discovered in PHPGurukul Complaint Management system 1.0.

CVE ID: CVE-2024-11967 (Critical)

**Multiple Vulnerabilities in Ruijie's Reyee OS**

Multiple vulnerabilities have been discovered in Ruijie's Reyee OS. The affected versions are Reyee OS versions 2.206.x up to but not including 2.320.x.

CVE ID: CVE-2024-47547(Medium),CVE-2024-42494(Medium), CVE-2024-51727(Medium), CVE-2024-47043(High), CVE-2024-45722(High),CVE-2024-47791(High),CVE-2024-46874(High), CVE-2024-48874(Critical), CVE-2024-52324(Critical), CVE-2024-47146(Medium)

**Multiple Vulnerabilities in ICONICS, Mitsubishi Electric Equipments**

Multiple vulnerabilities have been discovered in ICONICS equipment, ICONICS Product Suite and Mitsubishi Electric equipment, Mitsubishi Electric MC Works64. The affected products are ICONICS Suite, including GENESIS64, Hyper Historian, AnalytiX & MobileHMI version 10.97.2, AlarmWorX Multimedia (AlarmWorX64 MMX) all versions prior to 10.97.3, MobileHMI all versions prior to 10.97.3, ICONICS Suite including GENESIS64, Hyper Historian, AnalytiX, and MobileHMI all versions prior to 10.97.3 and all versions of Mitsubishi Electric MC Works64.

CVE ID: CVE-2023-2650 (Low), CVE-2023-4807(Medium), CVE-2024-1182(High), CVE-2024-1573(Medium), CVE-2024-1574(Medium)

**Multiple Vulnerabilities in ETIC Telecom Remote Access Server**

Multiple vulnerabilities have been discovered in ETIC Telecom Remote Access Server (RAS). The affected products are ETIC Telecom RAS all versions prior to 4.5.0 and ETIC Telecom RAS all versions prior to 4.11.0.

CVE ID: CVE-2022-3703(High), CVE-2022-41607(Medium), CVE-2022-40981(Medium), CVE-2024-26155(Medium), CVE-2024-26154(Medium), CVE-2024-26157(Medium), CVE-2024-26156(Medium), CVE-2024-26153(High)

**Security Updates for  IBM Security Verify Access Appliance**

IBM has released security updates to resolve multiple security vulnerabilities in  IBM Security Verify Access Appliance. The affected versions are IBM Security Verify Access Appliance 10.0.0 through 10.0.8.

CVE ID:CVE-2024-49803(Critical), CVE-2024-49804(High), CVE-2024-49805(Critical), CVE-2024-49806(Critical)

**Vulnerability in Arduino**

A missing authentication vulnerability has been discovered in the Visual Studio Code extension for Arduino that allows to perform Remote Code Execution (RCE) through a network attack vector.

CVE ID: CVE-2024-43488 (Critical)

**Multiple Vulnerabilities in Kieback&Peter's Equipment**

Multiple vulnerabilities have been discovered in Kieback&Peter's Equipment- DDC4000 Series. Security updates are available.

CVE ID: CVE-2024-41717 (Critical), CVE-2024-43812 (High), CVE-2024-43698 (Critical)

**Vulnerability in HMS Networks' Equipment**

An insufficiently protected credential vulnerability has been discovered in HMS Networks' equipment- EWON FLEXY 202. The affected version is EWON FLEXY 202 firmware version 14.2s0.  Security updates are available.

CVE ID: CVE-2024-7755 (High)

**Multiple Vulnerabilities in Elvaco's Equipment**

Multiple vulnerabilities have been discovered in Elvaco's Equipment- M-Bus Metering Gateway CMe3100. Successful exploitation of these vulnerabilities could allow to perform Remote Code Execution (RCE), impersonate and send false information, or bypass authentication.

CVE ID: CVE-2024-49396 (High), CVE-2024-49397 (High), CVE-2024-49398 (Critical), CVE-2024-49399 (High)

**Vulnerability in Tiptel IP 286**

A directory traversal vulnerability has been discovered in Tiptel IP 286. The affected version is Tiptel IP 286 with firmware version 2.61.13.10.

CVE ID: CVE-2024-33109 (Critical)

**Vulnerability in Eliz Software Panel**

A plaintext storage of a password vulnerability has been discovered in Eliz Software Panel. The affected versions are Eliz Software Panel before v2.3.24.

CVE ID: CVE-2024-5960 (Critical)

**Vulnerability in TuomoKu**

An arbitrary code execution vulnerability has been discovered in TuomoKu SPx-GC. The affected versions are TuomoKu SPx-GC v.1.3.0 and before.

CVE ID: CVE-2024-44623 (Critical)

**Vulnerability in eladmin**

A Server Side Request Forgery (SSRF) vulnerability has been discovered in eladmin. The affected versions are eladmin v2.7 and before.

CVE ID: CVE-2024-44677 (Critical)

**Vulnerability in Tenda**

A stack based buffer overflow vulnerability has been discovered in Tenda. The affected version is Tenda FH1206 02.03.01.35.

CVE ID: CVE-2024-7707 (Critical)

**Vulnerability in LibreChat**

A vulnerability has been discovered in LibreChat that does not validate the normalized pathnames of images. The affected versions are LibreChat through 0.7.4-rc1.

CVE ID: CVE-2024-41704 (Critical)

**Vulnerability in LibreChat**

An incorrect access control vulnerability has been discovered in LibreChat. The affected versions are LibreChat through 0.7.4-rc1.

CVE ID: CVE-2024-41703 (Critical)

**Vulnerability in Apache CXF**

A Server Side Request Forgery (SSRF) vulnerability has been discovered in the WADL service description in versions of Apache CXF before 4.0.5, 3.6.4 and 3.5.9.

CVE ID: CVE-2024-29736 (Critical)

**Vulnerability in N-central Server**

An authentication bypass vulnerability has been discovered in N-central server. The affected versions are N-central prior to 2024.2.

CVE ID: CVE-2024-28200 (Critical)

**Vulnerability in Atmail**

A SQL injection vulnerability has been discovered in Atmail. The affected version is Atmail v6.6.0.

CVE ID: CVE-2024-24133 (Critical)

**Multiple Vulnerabilities in Several IBM Products**

Multiple vulnerabilities have been discovered in several IBM products. Security updates are available.

CVE ID: CVE-2022-41854(Medium), CVE-2022-25857(High), CVE-2022-38749(Low), CVE-2022-38749(Low), CVE-2022-38750(Low), CVE-2024-24790(Critical)

**Security Updates for Dell PowerScale OneFS**

Dell has released security update for PowerScale for multiple security vulnerabilities. These vulnerabilities could be exploited by malicious users to compromise the affected system.

CVE: CVE-2024-43102(Critical), CVE-2024-38477(High), CVE-2024-38474(Critical), CVE-2024-38475, CVE-2024-38473, CVE-2024-39573, CVE-2024-28849(Medium), CVE-2024-49602 (Medium) , CVE-2023-49582 (Medium) , CVE-2024-49603, CVE-2024-42426

1. **TA-RAN-2024-12-10-001**

It has been observed that state backed ransomware threat actors are targetting BFSI sector through digitally signed executable capable of disabling the end point detection tools and secure deletions post exploitation of the network. It is been observed that executable named "HRSword" been utilized in the attack having mentioned interdependent malicious files [hashes] :

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

**Hashes (MD-5)**

0F73B467FF03F9224C024F4EB3AECEDB

A3E617C32254E04828F3C7334FFEF74F

7AE9B68A55059D38E170E698CDA22CEE

98009F56C26AD1965F72C99C97B6E1A0

033C9F28ACADAAA32D947A4026020BEA

**Hashes (SHA-1)**

75ebd5bab5e2707d4533579a34d983b65af5ec7f

6c6b0aecb990083b0ae1834944c6e8e3cda7edc5

f0c3f1fd5fc95611f755b161b67d2057d73f0fb8

909fc9cc82a2779fa614b31fc48f78e185c3e357

48c62ced29bfbdf25b60c692c9b2b9396c895ee3

f4786406c9c4c139ff4b99b59e696673c46d5359

**Hashes (SHA-256)**

E705F69AFD97F343F3C1F2BC6027D30935A0BFD29FF025C563F6F8C1F9A7478E

B2B27D656D0C358DF31C3A911C5D56788F88DFA628A378591DEE0F20CAE5C5EE

0E408AED1ACF902A9F97ABF71CF0DD354024109C5D52A79054C421BE35D93549

00E9FFD2D752E93B8965E0F337808D4885FA8DBE2F6EDD5CD3BC06C364D200FB

90040340EE101CAC7831D7035230AC8AD4224D432E5636F34F13AA1C4A0C2041

B8BD7D55298617AB2620C83789D61A4CC4765E868BE706CE1C361C9C2603E421

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

1. **TA-PHI-2024-12-10-003**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The phishing email attachment is an archived file named  "Lr to MSQAA unit Call.rar" "D.O. letter on Def Sec Briefing Dated 09-12-24.rar". On extracting the archive, a suspicious file named "Lr to MSQAA unit Call.pdf.html" is found. The file extension, although appearing to be a PDF document, is actually an HTML file designed to execute malicious actions when opened.  On clicking, "Lr to MSQAA unit Call.pdf.html” file, its  redirects to  the link  'https://email.gov.in.mailindia.one/service/home/?auth=co&id=29238&filename=Lr%20to%20MSQAA%20%20Letter&charset=UTF-8' and  opens the phishing page of NIC login page and seeks for username and password.

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

**URL:-**

https://email.gov.in.mailindia.one/service/home/?auth=co&id=29238&filename=Lr%20to%20MSQAA%20%20Letter&charset=UTF-8

**Domain:-**

mailIndia.one

**IPs:-**

45.141.59.78

103.108.231.173

93.157.106.19

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

1. **TA-MAW-2024-12-10-003**

It has been observed that below given malicious IoCs are targeting Critical Sectors Entities.

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

IP Addresses:

85.239.34.134

157.119.205.57

87.120.116.225

Hashes:-

76FA5C4EB5A9D5BF310667ED3A266DD511B46168

ee4c39dec9dc54779e6fe40bc11b161dd74cc830

c14dd98df81c1bdfaaf16bf9f8804eb88e4c643ee55a7e5fdc21454dd88cab54

f3f3fc8827e4f914bab4474445c0517097ab77e495c1b394517dd0c12e76f248

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

1. **TA-MAW-2024-12-11-004**

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:**

85.209.17.110

154.216.16.98

64.235.45.196

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

1. **TA-PHI-2024-12-11-004**

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 which are targeting Critical Sector Entities (CIIs).

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

**Domains:**

www.centralgov.info

delhipolicegov.inh.no

mesgov.info

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

1. **TA-RAN-2024-12-11-002**

Reference is made to the Advisory No - TA-RAN-2024-12-10-001 with Subject Cyber Security Advisory: Ransomware Attack by Executing HRSword Tool dated 10 Dec 2024.

Please find below additional IOCs in this regard.

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

**Hashes (SHA-256)**

f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446

e705f69afd97f343f3c1f2bc6027d30935a0bfd29ff025c563f6f8c1f9a7478e

051795020363d8bd3494f15c69dff31d533ff42de92952d2619279c723b8e33a

ae8e0cab1786a619e0e0cb044209e5de7a6a30375dd88400c59551061f318a68

348a34d19c9ca09974bc4be7de699924322d1a5b89af354a7d4445689aa64d83

63929f07a47922510bb79e9d3cccd9cd74d79edd9c4e120b8951d311052800c8

c015c19dace973c46fd4be1785c1da85b48fe0313eb6f4e281904547030a405d

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

1. **TA-MAW-2024-12-11-006**

It has been observed that Dogcall RAT, also known as RokRat, is a sophisticated Remote Access Trojan (RAT) used by the APT37 group also known as Reaper, Inky Squid, RedEyes, ScarCruft. Adversary leverages social engineering techniques like spear-phishing to deploy malware. The malware employs multi-stage infection chains, often initiated via oversize Windows Shortcut (LNK) files disguised as legitimate documents or embedded within malicious Hangul Word Processor (HWP) files and utilizes legitimate cloud services for Command and Control (C2) purposes to evade detection. It has also been reported that it uses cloud storage APIs like pCloud, Dropbox, and Yandex, and is capable of capturing screenshots, logging keystrokes, and evading analysis with anti-virtual machine detections.

**Impacts:**

* Data Exfiltration: Stealing sensitive information such as login credentials, communication data, and browser data.
* Keylogging: Logging keystrokes to capture sensitive information
* Screen Capture: Capturing screenshots of the victim's machine
* Audio Capture: Recording audio from the victim's microphone
* File Manipulation: Downloading and uploading files on the victim's system
* Credential Harvesting: Stealing credentials stored in web browsers and Windows Credential Manager

**Mitigations:**

* Email Filtering: Implement robust email filtering to block phishing emails and malicious attachments.
* Endpoint Protection: Deploy advanced endpoint protection solutions with real-time threat detection and response capabilities.
* Regular Updates: Keep operating systems, applications, and antivirus software up to date to protect against known vulnerabilities.
* User Training: Conduct regular security awareness training for employees to recognize and report phishing attempts.
* Network Segmentation: Segment networks to limit the spread of malware and restrict access to sensitive data.

**Recommendations:**

* Monitor Network Traffic: Continuously monitor network traffic for unusual activity and signs of data exfiltration.
* Use Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security for accessing sensitive systems and data.
* Incident Response Plan: Develop and regularly update an incident response plan to quickly address and mitigate cyber threats.

1. **TA-MAW-2024-12-11-005**

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

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

**IP Addresses:**

188.177.20.243

43.225.109.30

112.94.96.94

103.210.94.39

120.85.116.88

120.85.142.240

103.210.94.205

222.110.56.181

175.107.39.111

27.43.206.146

175.107.39.203

47.237.128.104

8.222.225.103

27.43.205.74

120.86.254.179

103.199.200.136

112.94.96.236

100.42.180.126

112.94.96.189

27.43.205.80

27.111.75.123

103.210.94.216

103.199.180.49

178.18.207.174

175.5.13.145

117.222.120.68

178.72.81.23

220.198.240.226

89.22.230.162

182.59.41.219

89.252.146.4

47.236.131.179

93.118.124.16

77.239.216.96

103.210.94.206

188.177.20.243

64.235.37.140

120.85.114.179

38.253.225.18

27.43.207.170

122.97.214.207

8.222.138.22

107.189.18.96

103.210.94.16

112.94.98.102

220.198.240.116

112.94.98.80

103.199.180.87

120.85.115.104

47.84.77.51

203.81.86.34

120.86.254.109

27.47.2.133

220.158.159.31

141.98.11.35

87.120.116.226

103.158.96.214

120.138.12.172

103.158.96.157

112.94.97.163

120.85.112.114

120.86.252.1

122.97.138.175

8.222.181.107

178.72.68.151

120.85.183.30

**URLs:-**

http://222.140.181.180:45405/

http://125.24.172.138:56365/

http://117.205.43.93:38341/

http://175.107.39.251:52532/

http://27.122.61.79:43503/

http://103.15.254.118:55927/

http://117.215.211.57:57167/

http://103.200.86.149:40223/

http://39.78.4.111:58869/

http://212.58.118.218:36714/

http://39.90.150.181:33827/

http://119.114.58.253:34998/

http://59.88.10.203:55289/

http://106.58.250.171:45183/

http://113.221.72.103:49198/

http://59.98.196.255:43798/

http://175.107.38.23:54934/

http://175.107.39.184:36584/

http://171.249.137.27:45283/

http://221.15.242.138:51577/

http://45.115.89.213:57799/

http://103.203.72.113:41261/

http://123.14.36.15:36350/

http://117.222.248.18:34815/

http://106.41.81.166:34178/

http://223.8.188.234:41919/

http://103.200.86.78:57417/

http://112.239.113.142:57108/

http://125.40.64.75:50831/

http://59.89.231.24:56305/

http://117.219.46.214:58396/

http://122.199.98.82:2698/

http://117.209.240.57:60624/

http://117.213.244.214:36854/

http://115.57.215.139:39893/

http://122.194.195.92:36704/

http://111.174.188.249:37045/

http://119.179.247.182:53628/

http://103.197.113.227:34909/

http://125.41.92.123:37172/

http://117.202.90.3:53360/

http://222.134.172.27:56647/

http://103.15.254.219:52817/

http://180.94.33.62:32950/

http://103.91.180.23:56218/

http://113.90.49.246:42840/

http://103.203.72.31:34097/

http://115.56.155.220:34875/

http://175.107.37.241:58175/

http://103.78.150.139:53204/

http://59.54.88.94:33031/

http://124.131.51.51:35913/

http://113.26.89.173:37265/

http://117.211.32.176:58418/

http://117.235.100.76:34204/

http://180.115.169.41:58464/

http://123.11.77.105:56575/

http://42.224.174.41:57136/

http://61.53.118.58:43341/

http://120.61.5.153:49976/

http://42.230.188.74:36245/

http://123.9.195.80:42724/

http://45.230.66.14:11301/

http://192.118.100.200:43686/

http://123.13.156.223:35455/

http://123.9.217.34:44406/

http://61.54.73.111:52432/

http://103.151.46.132:42105/

http://182.233.111.34:38409/

http://223.13.56.56:35346/

http://102.33.35.204:56861/

http://180.108.19.54:36809/

http://220.158.159.244:49915/

http://123.4.71.9:45225/

http://182.119.121.251:59015/

http://117.198.90.93:52486/

http://117.196.115.13:37744/

http://220.158.158.45:41495/

http://42.228.37.11:38421/

http://117.209.32.101:56776/

http://180.115.72.226:56592/

http://117.254.178.34:33378/

http://42.178.80.225:37180/

http://117.253.223.141:41589/

http://117.205.108.101:35980/

http://114.226.137.219:47800/

http://117.198.14.216:39433/

http://223.15.19.197:38241/

http://117.196.117.200:51566/

http://103.197.115.75:41592/

http://59.99.217.12:34380/

http://59.93.24.239:43135/

http://117.244.212.89:38120/

http://182.124.94.121:44667/

http://117.253.210.224:44321/

http://59.95.85.158:47263/

http://5.239.240.144:33960/

http://185.248.13.169:40075/

http://119.187.60.14:45788/

http://182.120.43.161:33021/

http://117.5.147.84:42372/

http://113.26.86.43:53408/

http://38.137.248.43:52511/

http://154.240.28.224:34754/

http://27.215.110.155:49773/

http://210.10.140.147:58165/

http://172.35.12.226:42398/

http://59.98.167.85:49371/

http://45.230.66.50:10525/

http://112.198.238.18:45624/

http://117.211.48.37:37644/

http://117.211.47.3:50975/

http://175.107.2.203:48894/

http://59.95.91.223:42926/

http://37.57.155.12:60982/

http://102.33.40.209:41024/

http://175.107.36.96:54636/

http://219.157.34.90:44959/

http://117.248.16.174:33516/

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

1. **TA-MAW-2024-12-12-007**

It has been observed that PowerSCP Stealer is a PowerShell-based credential stealer specifically targeting Windows systems. Upon execution, PowerSCP Stealer downloads SSH/Utility Download, creates SSH key pair and sets the SSH Key Access Control. The malware also performs port scanning, port selection, creates persistence and exfiltration of  data from victim machine. Stealer exploits the Secure Copy Protocol (SCP) for data exfiltration and uses deceptive password prompts to collect valid windows login credentials. Stealer validates the credentials before sending them to its command-and-control (C2) server. This validation ensures that only verified credentials are exfiltrated, enhancing its utility for further malicious activities like second-stage malware deployment or credential broker transactions.

**Impacts:**

* Credential Theft: Successful credential exfiltration can lead to unauthorized access to sensitive systems.
* System Compromise: The malware can facilitate further attacks, including secondary malware deployment.
* Data Breach: Organizations may face data breaches that can damage their reputation and financial standing.

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

**IPs:**

185.255.178.85

**Hashes:**

7ff6e1696b4e9a247041e9d1b37120c7ef0671eb69b832d0c19fefc1088d53e2

facd14a7014e3a7d87955ed0be09e11df31d107ec58b7b53f6d7dae1b4a85cd4

2d046eb280238dfa5fbe15d0c3e0dfbde38bfcec7ee8b8b51e9887c840009842

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

1. **TA-MAW-2024-12-13-008**

t has been observed that threat actors are exploiting the public MQTT broker- "broker.hivemq.com" for data exfiltration from compromised systems. This domain is intended as a test environment for developers and IoT enthusiasts to experiment with MQTT protocol for messaging. But malicious actors are leveraging it as a covert channel for unauthorized data transfers.

Additional domains for other cloud/ API services to be MONITORED for malware exhibiting similar TTPs:

api.telegram.org

telegram.org

discord.com

discord.com/api/

api.slack.com

slack.com

api.dropboxapi.com

dropboxapi.com

api.dropbox.com

dropbox.com

Note: The above domains are legitimate, if the services of these domains are used then blocking may disrupt specific organizational operations. Hence, these domains need to be monitored at network perimeter level and the source process must be identified accordingly.

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

**Hashes (SHA1):-**

998f8ebecf89612d486522f168cc8f8ba67bdd7c

6f1a8ab4a2ab6d00fed67ef802573bd9635363c3

b7751a4a1d595df34783ad22898e0c28fccb2886

ccce17e5e24daa3e07167c16eb8f1fdc0b843ca7

70a4fc6db6b65c300cc45abea681f06d9daeb18f

fce13fed9387035f72c9bd9346a0501c57ec463e

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

1. **TA-PHI-2024-12-13-005**

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 which are targeting Critical Sector Entities (CIIs).

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

**Domains:**

www.the-night-of-travestie.de (currently resolving to 89.107.186.220)

indianairforce.website

www.indianairforce.nia.in

rbi-gov.info

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

1. **VA-2024-12-13-004**

It has been observed that a critical vulnerability, CVE-2024-50623, classified as "Unrestricted Upload of File with Dangerous Type", has been discovered in Cleo's file transfer products, including Cleo Harmony, VLTrader, and LexiCom. This vulnerability allows unauthenticated Remote Code Execution (RCE) due to the lack of restrictions on file uploads. Adversaries are exploiting this weakness to upload malicious files to the autoruns / subdirectory of the affected program, enabling them to automatically execute their payloads. The exploitation of this vulnerability has been linked to several malware families, including Safepay and Termite Ransomware.

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

Malicious File Location (check installation directory of Harmony/VLTrader/Lexico)

Cleo####.jar (ex: cleo.5264.jar/cleo.6597.jar etc)

hosts/main.xml file or a hosts/60282967-dc91-40ef-a34c-38e992509c2c.xml

**IP Address:**

185.181.230.115

80.67.5.133

5.181.158.25

185.162.128.133

184.107.3.70

195.123.224.8

184.107.3.196

176.123.5.126

5.149.249.226

185.181.230.103

209.127.12.38

181.214.147.164

192.119.99.42

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