**Cyber Security Advisories**

**Date: 15 November 2024**

1. **TA-MAW-2024-10-30-23**

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:

107.167.122.114

179.43.191.98

79.142.76.205

5.101.6.131

5.91.56.27

89.208.29.19

107.167.122.124

49.89.171.103

104.129.56.10

120.85.115.94

59.178.87.83

120.26.208.20

185.82.218.204

45.84.107.182

107.167.122.109

77.239.214.243

120.86.237.86

120.85.116.167

204.8.96.66

196.240.60.216

217.114.218.26

185.213.155.164

107.167.122.126

185.224.128.67

117.222.124.12

221.215.175.25

193.239.147.201

50.3.182.152

23.228.72.18

154.216.17.31

2.179.99.40

103.14.226.142

64.227.139.233

121.43.146.34

122.97.136.96

36.111.157.26

120.241.40.91

137.220.202.57

27.43.207.218

94.136.189.247

43.228.217.76

120.85.117.120

47.236.3.241

27.43.205.141

8.134.172.128

61.93.249.110

118.178.105.68

171.37.106.42

111.255.108.45

8.218.101.227

112.94.96.183

47.92.31.118

123.205.2.44

107.167.122.107

120.85.94.159

8.218.63.174

121.40.149.31

1.170.211.35

120.85.116.85

118.239.9.197

207.102.138.19

8.219.237.59

123.205.12.232

94.40.236.113

107.167.122.125

103.149.28.141

107.175.31.202

154.216.18.227

39.106.8.50

93.123.85.184

182.92.113.149

38.205.0.253

120.85.112.147

223.82.97.133

193.128.108.242

120.86.255.175

103.199.200.159

175.183.33.202

111.255.51.3

2.58.113.110

23.82.16.25

77.239.219.64

193.128.111.37

38.205.0.162

38.206.2.172

8.152.192.129

108.62.233.174

108.62.52.43

23.82.16.116

38.205.2.30

23.104.17.16

175.107.2.86

42.236.132.3

142.234.50.206

181.214.48.135

38.205.188.27

122.239.151.206

120.85.116.15

77.239.214.233

68.69.186.238

223.82.97.132

45.142.107.15

45.66.231.148

154.216.20.247

179.43.169.162

27.43.204.42

195.26.252.46

121.206.181.57

94.40.240.116

120.86.239.125

112.94.99.82

103.199.200.29

117.211.52.141

URLs: -

http://45.230.66.9:10848/

http://117.222.197.178:49978/

http://115.201.134.49:35065/

http://117.199.72.202:50951/

http://115.55.159.10:34845/

http://115.52.63.168:39638/

http://43.248.119.83:19490/

http://112.113.210.206:50750/

http://117.214.235.4:39648/

http://123.156.30.253:56120/

http://27.214.186.57:51191/

http://175.107.38.182:32992/

http://117.209.13.235:56628/

http://117.209.241.247:53558/

http://219.155.60.45:49860/

http://220.158.158.211:55822/

http://110.182.190.91:32828/

http://117.199.125.197:52745/

http://117.209.240.46:57913/

http://119.179.248.247:37950/

http://114.227.15.208:54255/

http://77.44.181.26:59618/

http://42.224.253.87:40099/

http://182.113.207.202:52314/

http://45.115.89.158:42978/

http://196.189.152.147:33694/

http://182.121.157.109:38387/

http://117.211.38.88:53315/

http://223.13.38.195:55297/

http://117.209.11.102:56038/

http://117.198.11.209:45523/

http://42.232.246.105:45874/

http://117.222.124.12:50940/

http://221.215.175.25:38681/

http://115.52.151.246:59819/

http://42.86.132.137:54371/

http://117.209.84.174:55485/

http://2.179.99.40:49092/

http://59.96.214.168:42569

http://117.209.89.111:60277

http://102.36.223.132:46156

http://60.212.193.179:60207

http://42.233.129.160:43167

http://103.203.72.132:45147

http://59.89.68.241:37554

http://120.61.204.146:59099

http://202.21.42.249:41111

http://175.107.2.165:43797

http://117.209.81.102:57897

http://112.248.0.159:49076

http://117.195.87.217:33063

http://61.53.75.254:59862

http://117.212.163.89:53689

http://45.230.66.47:11337

http://120.241.40.87:59897

http://42.231.42.96:37716

http://117.208.248.184:55332

http://182.117.68.14:49652

http://117.214.198.197:40883

http://223.10.65.199:42796

http://120.61.24.117:53387

http://117.209.1.159:57383

http://123.10.12.90:41950

http://117.219.122.74:48172

http://27.122.61.200:35962/

http://117.247.28.46:35622

http://27.122.61.232:32796

http://201.77.146.249:55211

http://139.5.11.235:51104

http://120.61.202.163:49929

http://117.209.34.154:36325

http://117.206.129.147:34961

http://117.203.180.142:58443

http://115.50.45.98:32917

http://177.163.242.113:54074/

http://222.140.184.128:36755/

http://59.182.208.225:37650/

http://117.211.42.24:37693/

http://105.158.123.43:35999/

http://117.235.35.213:51717/

http://27.37.78.234:46277/

http://223.151.73.246:39723/

http://39.87.12.22:57706/

http://117.209.124.166:51183/

http://117.254.102.237:42136/

http://116.231.166.217:43916/

http://117.208.222.101:43956/

http://117.253.2.55:37470/

http://103.167.204.27:57257/

http://27.122.61.62:48541/

http://59.99.195.121:42978/

http://59.95.93.214:54331/

http://42.6.82.152:45932/

http://222.141.39.216:44484/

http://220.158.159.226:55489/

http://220.158.158.188:37317/

http://219.156.63.73:49715/

http://120.60.233.111:53995/

http://117.235.60.87:32840/

http://117.222.119.123:42143/

http://117.209.9.198:47174/

http://117.209.47.147:56490/

http://117.209.23.169:36411/

http://117.206.88.49:55711/

http://115.48.144.169:41569/

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

1. **TA-RAN-2024-11-04-001**

It has been observed that a new ransomware group dubbed “Interlock” has emerged, setting its sights on both Windows and FreeBSD operating systems. This multi-platform approach signals a concerning trend in the ransomware landscape, expanding the potential attack surface for organizations worldwide. Interlock targets FreeBSD as it’s widely utilized in servers and critical infrastructure. Adversaries can disrupt vital services, demand hefty ransoms, and coerce victims into paying.

Adversary's Windows variant utilizes a custom packer which employs various techniques to maintain a low profile, including clearing Windows event logs and self-deletion. Interlock clears multiple Windows event logs, including Application, Security, Setup, System, and Forwarded Events. With self-deletion enabled, it drops a DLL that eliminates the main binary using rundll32.exe.

Interlock ransomware appears to employ the increasingly common double-extortion tactic. After encrypting files and appending them with the “.interlock” extension, the adversary leaves a ransom note revealing that sensitive data has been stolen. Victims are then instructed to contact the threat actors via TOR to negotiate a ransom, with the threat of public data leaks adding pressure to comply.

Adversaries also use Microsoft’s Azure Storage Explorer and AzCopy to steal data from compromised networks and store it in Azure Blob storage. It is a relatively uncommon tactic among ransomware groups. This technique has only been seen in a few advanced ransomware actors, such as BianLian and Rhysida. Attackers are likely drawn to this method because Azure is a trusted enterprise-grade service widely adopted by organizations, making it less probable that data transfer attempts will be detected or blocked by corporate firewalls and security tools.

Recent intelligence indicates that the group has released both Windows and Linux versions of their ransomware, with malicious samples exhibiting capabilities like process enumeration, virtual machine detection, execution delay via the Sleep API function, and file encryption.

This group has demonstrated a focus on virtual environments, employing tactics to compromise systems and disrupt operations. Notably, INTERLOCK establishes Command and Control (C2) through a scheduled task using an anonymized network, which enhances its stealth and sophistication.

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

**IPs:**

195.201.21.34

159.223.46.184

**Domains:**

https://rvthereyet.com

https://apple-online.shop

**Hashes:(SHA 1)**

8a38825ee33980a27ab6970e090a30a46226f752

5cc81e0df62e0d68710e14b31e2270f2ec7ed166

1cb6a93e6d2d86d3479a1ea59f7d5b258f1c5c53

**Hashes:(SHA 256)**

7b9e12e3561285181634ab32015eb653ab5e5cfa157dd16cdd327104b258c332

c20baba26ebb596de14b403b9f78ddc3c13ce9870eea332476ac2c1dd582aa07

a4f0b68052e8da9a80b70407a92400c6a5def19717e0240ac608612476e1137e

5859c7402ae6b6a8a06d48e48bd5bfff49c63c41af4e73e0451c614219a25738

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

1. **TA-RAN-2024-11-04-002**

It has been observed that state-sponsored groups or cybercriminal organizations are using malware to target various sectors, including government (defence, external affairs etc.), finance, technology, and critical infrastructure. Its objectives range from espionage and data theft to sabotage and disruption.

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

**IP:**

65.20.73.88

Persistence (Registry entry): HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AutoLaunch

Malware dropped at location: %ProgramData%\AdobeAutoLaunch\

(the legitimate application name may change as the malicious file is being sideloaded

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

1. **TA-APT-2024-11-04-001**

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

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

**IP:**

35.88.139.137

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

1. **TA-PHI-2024-11-05-001**

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

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

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

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

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

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

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

IP Addresses

193.3.19.110

176.59.196.133

Domain

daslkjfhi2.xyz

URLs

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

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

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

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

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

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

https://redr.me/g3boil

https://redr.me/w0oimp

https://rb.gy/17xscr

https://cutt.ly/teznCIhy

HASHES (SHA256)

9155795606fd3e5d0929cb83439e392447f00ff0f112cf172f65f78edccba172

393b1fdda7c4af084743c56c27585366567a8446c6438753d20b0b9ee3e72541

71c169992a8f98ef38b6ddcc22ca747944db6e047dc080523c1f54d1122dcc9f

f841f59e93bcad3d5ef5c4acceb799dc944a581c21dfa55faa76a7f84eb031bf

e70f33b5022f725663e4da47ce8196fdfb4c45460001a692172c147c4bbbeced

a444e147dd38ee76b4968f772ed67e0ed805de116137621e10acfa93781fe2c8

df1591e1619ad12efdd4c0df07dd26158b9a8b9c8ca06be885879322f7af2f4b

83e858a6a7dc299d6e141f81e1cb11a94c56ccc0853a946ceee2ad9a76a24a72

ae16a7225bcf3ff95e220934f5b99fcde623c389f80b0e48053b6f233884a20e

38f2d360dc5d0a3a3712936eab141017aa1a7c39d1fd3a2b51781e5c561e6bb8

74fb61dc7b6fb2d7793ab9eee02098886b2c451313da2c4ef8db478585c8a8d4

8bc22d5c0ffa3f83cab97c17bf2b1538cdcea956bcb33e13582551e5de423932

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

1. **TA-PHI-2024-11-05-002**

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

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

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

**Domains:**

delhipolice.gov.inh.no

meigov.info

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

1. **TA-APT-2024-11-05-002**

Reference is made to earlier advisories on the APT36.

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

**Common Features of Mythic Malware:**

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

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

**IP:**

64.188.25.79

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

1. **VA-2024-11-05-001**

**Vulnerability in langchain**

A SQL injection vulnerability has been discovered in the GraphCypherQAChain class of langchain-ai/langchainjs. The affected versions are GraphCypherQAChain class of langchain-ai/langchainjs version 0.2.5 and all versions with this class.

CVE ID: CVE-2024-7042 (Critical)

**Vulnerability in Meetup**

An authorization bypass vulnerability has been discovered in Meetup. The affected versions are Meetup: from n/a through 0.1.

CVE ID: CVE-2024-50483 (Critical)

**Multiple Vulnerabilities in Rockwell Automation FactoryTalk ThinManager Equipment**

Multiple vulnerabilities have been discovered in Rockwell Automation FactoryTalk ThinManager equipment. The affected versions are ThinManager: versions 11.2.0 to 11.2.9, versions 12.0.0 to 12.0.7, versions 12.1.0 to 12.1.8, versions 13.0.0 to 13.0.5, versions 13.1.0 to 13.1.3, versions 13.2.0 to 13.2.2, and version 14.0.0. The mitigation and workarounds are available.

CVE ID: CVE-2024-10386 (Critical), CVE-2024-10387 (High)

**Vulnerability in Crypto plugin for WordPress**

An authentication bypass vulnerability has been discovered in Crypto plugin for WordPress. The affected versions are Crypto plugin for WordPress up to and including, 2.15.

CVE ID: CVE-2024-9989 (Critical)

**Vulnerability in IBM**

A static credentials vulnerability has been discovered in IBM Flexible Service Processor. The affected versions are IBM Flexible Service Processor FW860.00 through FW860.B3, FW950.00 through FW950.C0, FW1030.00 through FW1030.61, FW1050.00 through FW1050.21, and FW1060.00 through FW1060.10. Security updates are available.

CVE ID: CVE-2024-45656 (Critical)

**Multiple Vulnerabilities in Siemens' Equipment InterMesh**

Multiple vulnerabilities have been discovered in several of Siemens' equipment- InterMesh. Siemens has released workarounds and mitigations to resolve these vulnerabilities.

CVE ID: CVE-2024-47901 (Critical), CVE-2024-47902 (High), CVE-2024-47903 (High), CVE-2024-47904 (High)

**Vulnerability in Delta Electronics' Equipment**

A deserialization of untrusted data vulnerability has been discovered in Delta Electronics' Equipment- InfraSuite Device Master. The affected versions are InfraSuite Device Master: Versions 1.0.12 and prior. Security updates are available.

CVE ID: CVE-2024-10456 (Critical)

**Vulnerability in Tongda**

A SQL injection vulnerability has been discovered in Tongda OA 2017. The affected versions are Tongda OA 2017 up to 11.10.

CVE ID: CVE-2024-10732 (Critical)

**Vulnerability in Tenda**

A stack-based buffer overflow vulnerability has been discovered in Tenda. The affected version is Tenda AC6 15.03.05.19.

CVE ID: CVE-2024-10698 (Critical)

**Vulnerability in Tenda**

A command injection vulnerability has been discovered in Tenda. The affected version is Tenda AC6 15.03.05.19.

CVE ID: CVE-2024-10697 (Critical)

**Vulnerability in LevelOne WBR-6012 Router**

A vulnerability has been discovered in LevelOne WBR-6012 router's web application that allows to change the administrator password and gain higher privileges without the current password. The affected version is LevelOne WBR-6012 router firmware version R0.40e6.

CVE ID: CVE-2024-33699 (Critical)

**Vulnerability in Tenda**

A stack-based buffer overflow vulnerability has been discovered in Tenda. The affected versions are Tenda AC1206 up to 20241027.

CVE: CVE-2024-10434 (Critical)

**Vulnerability in SECOM**

A vulnerability has been discovered in SECOM wireless router WRTM326 that does not properly validate a specific parameter and could execute arbitrary system commands by sending crafted requests.

CVE ID: CVE-2024-10119 (Critical)

**Vulnerability in AA-Team WZone**

A missing authorization vulnerability has been discovered in AA-Team WZone. The affected versions are WZone from n/a through 14.0.10.

CVE ID: CVE-2024-33545 (Critical)

1. **TA-PHI-2024-11-06-003**

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 has an attached

  PDF file  with themes "Letter Dated 05 November MoD.pdf" &" Letter Dated 05 November MEA.pdf" that contains a hyperlink https://email.gov.in.indianarmy.ml/service/home/?auth=co&id=29238&filename=INDIAN%20Armed%20Forces%20And%20Agencies%20Report&charset=UTF-8 with the title "View Document".

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

**IPs:**

176.123.0.55

93.157.106.19

146.70.142.134

**URLs:**

https://email.gov.in.indianarmy.ml/service/home/?auth=co&id=29238&filename=INDIAN%20Armed%20Forces%20And%20Agencies%20Report&charset=UTF-8

**Domain:**

indianarmy.ml

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

1. **TA-PHI-2024-11-06-004**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored 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:**

mail-desk.in

www.email.gov.in.indianarmy.pl

email.gov.in.indianarmy.pl

ail-gov.ink

auths.info

em.ail-gov.ink

email-g0v.online

aadhar-co.in

gov.in.nha.in

govscicourt.com

in.viewcerts.org

indian.airforce.life

indianarmy.ml

indianarmy.pl

joinindiannavy.com

loginmygov.info

mahagov.info

mail-panel.in

measgov.org

minfinfgov.info

mof-gov.info

nia-gov.info

orjinal.site

scigov.xyz

scigovcourt.com

sebi-gov.info

sebi-gov.io

sebigovin.sebi-gov.io

serviceonline.gov.in.viewcerts.org

adhar-ucl.auths.info

viewcert.life

ww25.indian.airforce.life

ww38.iwww.joinindiannavy.com

adhar.auths.info

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

1. **TA-RAN-2024-11-07-003**

It has been observed that Lynx ransomware encrypt victims' data and uses fork of Inc Ransomware in attacks. They retrieve system information and geolocation from the Windows registry and can modify registry settings to change system configurations. Their capabilities also include resizing volume shadow copies, encrypting files with with the “. LYNX” extension, and placing ransom notes in multiple directories.

**Impacts:**

* Delay data processing: It can delay execution using the Sleep API function.
* System Compromise: The malware can gain unauthorized access to systems for retrieving system time, deleting shadow copies and sending the ransom note to the printer.
* Stolen Credentials: The ransomware operators may use stolen credentials to breach targeted systems.

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

**Signatures:**

eaa0e773eb593b0046452f420b6db8a47178c09e6db0fa68f6a2d42c3f48e3bc

571f5de9dd0d509ed7e5242b9b7473c2b2cbb36ba64d38b32122a0a337d6cf8b

b378b7ef0f906358eec595777a50f9bb5cc7bb6635e0f031d65b818a26bdc4ee

ecbfea3e7869166dd418f15387bc33ce46f2c72168f571071916b5054d7f6e49

85699c7180ad77f2ede0b15862bb7b51ad9df0478ed394866ac7fa9362bf5683

64b249eb3ab5993e7bcf5c0130e5f31cbd79dabdcad97268042780726e68533f

508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef

7f104a3dfda3a7fbdd9b910d00b0169328c5d2facc10dc17b4378612ffa82d51

1754c9973bac8260412e5ec34bf5156f5bb157aa797f95ff4fc905439b74357a

d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6

05e4f234a0f177949f375a56b1a875c9ca3d2bee97a2cb73fc2708914416c5a9

fef674fce37d5de43a4d36e86b2c0851d738f110a0d48bae4b2dab4c6a2c373e

36e3c83e50a19ad1048dab7814f3922631990578aab0790401bc67dbcc90a72e

869d6ae8c0568e40086fd817766a503bfe130c805748e7880704985890aca947

ee1d8ac9fef147f0751000c38ca5d72feceeaae803049a2cd49dcce15223b720

f96ecd567d9a05a6adb33f07880eebf1d6a8709512302e363377065ca8f98f56

3156ee399296d55e56788b487701eb07fd5c49db04f80f5ab3dc5c4e3c071be0

fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced

11cfd8e84704194ff9c56780858e9bbb9e82ff1b958149d74c43969d06ea10bd

02472036db9ec498ae565b344f099263f3218ecb785282150e8565d5cac92461

e17c601551dfded76ab99a233957c5c4acf0229b46cd7fc2175ead7fe1e3d261

9ac550187c7c27a52c80e1c61def1d3d5e6dbae0e4eaeacf1a493908ffd3ec7d

ca9d2440850b730ba03b3a4f410760961d15eb87e55ec502908d2546cd6f598c

1a7c754ae1933338c740c807ec3dcf5e18e438356990761fdc2e75a2685ebf4a

a5925db043e3142e31f21bc18549eb7df289d7c938d56dffe3f5905af11ab97a

7ccea71dcec6042d83692ea9e1348f249b970af2d73c83af3f9d67c4434b2dd0

5a8883ad96a944593103f2f7f3a692ea3cde1ede71cf3de6750eb7a044a61486

463075274e328bd47d8092f4901e67f7fff6c5d972b5ffcf821d3c988797e8e3

82eb1910488657c78bef6879908526a2a2c6c31ab2f0517fcc5f3f6aa588b513

29a25e971dbb87d3adcee75693782d978a3ca9f64df0a59b015ca519a4026c49

63e0d4e861048f581c9e5c64b28a053eb0023d58eebf2b943868d5f68a67a8b7

a0ceb258924ef004fa4efeef4bc0a86012afdb858e855ed14f1bbd31ca2e42f5

c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef

**Email address:**

martina.lestariid1898@proton.me

**Domain:**

lynxblog.net

**URLs:**

http[:]//lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd.onion

http[:]//lynxbllrfr5262yvbgtqoyq76s7mpztcqkv6tjjxgpilpma7nyoeohyd.onion/disclosures

http[:]//lynxblogco7r37jt7p5wrmfxzqze7ghxw6rihzkqc455qluacwotciyd.onion

http[:]//lynxblogijy4jfoblgix2klxmkbgee4leoeuge7qt4fpfkj4zbi2sjyd.onion

http[:]//lynxblogmx3rbiwg3rpj4nds25hjsnrwkpxt5gaznetfikz4gz2csyad.onion

http[:]//lynxblogoxllth4b46cfwlop5pfj4s7dyv37yuy7qn2ftan6gd72hsad.onion

http[:]//lynxblogtwatfsrwj3oatpejwxk5bngqcd5f7s26iskagfu7ouaomjad.onion

http[:]//lynxblogxstgzsarfyk2pvhdv45igghb4zmthnzmsipzeoduruz3xwqd.onion

http[:]//lynxblogxutufossaeawlij3j3uikaloll5ko6grzhkwdclrjngrfoid.onion

http[:]//lynxch2k5xi35j7hlbmwl7d6u2oz4vp2wqp6qkwol624cod3d6iqiyqd.onion/login

http[:]//lynxchatbykq2vycvyrtjqb3yuj4ze2wvdubzr2u6b632trwvdbsgmyd.onion/login

http[:]//lynxchatde4spv5x6xlwxf47jdo7wtwwgikdoeroxamphu3e7tt5doqd.onion/login

http[:]//lynxchatdy3tgcuijsqofhssopcepirjfq2f4pvb5qd4un4dhqyxswqd.onion/login

http[:]//lynxchatdykpoelffqlvcbtry6o7gxk3rs2aiagh7ddz5yfttd6quxqd.onion/login

http[:]//lynxchatfw4rgsclp4567i4llkqjr2kltaumwwobxdik3qa2oorrknad.onion/login

http[:]//lynxchatly4zludmhmi75jrwhycnoqvkxb4prohxmyzf4euf5gjxroad.onion/login

http[:]//lynxchatohmppv6au67lloc2vs6chy7nya7dsu2hhs55mcjxp2joglad.onion/login

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

1. **TA-MAW-2024-11-08-001**

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:**

45.88.90.11

103.82.37.117

198.98.50.97

**Domains:**

shemale.free.nf

boats.dogmuncher.xyz

cnc.catfishes.es

**Hashes:**

01399d0721c5b3b5e43d9daee72cf8b19eeb23b09a669a7c15258f0444f92ee5

05a89b0467c8f768f47a57c48ef067f27bc621883fc2dbfef4381b70521a7e9f

09f2b8debd3211b290d618295c01df3a85c43ca3b0a71b5220e739c6c0e98fb2

14bac426f106b79590d024e1bca1f72357c82f88e969a54ad9d76b32e94cd6e4

1d073e160fd938a82458b744b6e2df5dbd7bdd8b5c72804f71e12cabae562081

223283d332a50819dc2ad0f7fb9631af5dff5d5e4c744da0a6c8de36be265b4f

258e79b35c65a7c391e9b5d1b670260883af14ae32713152405806c9c923081b

25c5703ce2d7284fc044cbb16fbb4ac0dd623d247f3a3486a7314720256d7e60

3d44b3229b54d6b4350d6cefa74ab395de71a4670510cca80cc2f3173c874e40

3eed1f07a55a6394c390b2d92a7dd4aefcbf7b1b015e02891772096986220468

3f7b2acff8720e4e33a9af7f00b425234476e677d8afdabcef73a1cb55e4b39f

40425b345479a89d1734852b7fb075006a0da5d4f393f815df8da366eda93126

4d2b2e7bd2a0da53e7c779d0efdaefde753d90555ede0a968d3cfafa656b162f

50f67750e35293cddf9ec0da8fe7871e75d015e6973528e4f3413a8fac03fda2

5177ff38042a39215c2cf515374c2507a39ba8e40cd2fc01e386ce5e6f36d806

53d803b671097ac85eb0cfa8808a286b07d45885cbd598ba5de48470efc26554

68eaf18820535496a2553fad6285bed07144c2a664794feb802c8a6cac2ab8b2

7b248c50d8ef5d466a2c0685a7e65a0b404220c781549de0a2f74921fa331c7b

7ffb510c4b364301754174dfe82d7db0e15888a9099ba13dc4e2a60cf8600bd1

81560aafd29554aac853512ac212968ff06dd6e24b87cc0c848d96ef901fa89d

867b12aca46413aeaa981633fe421e03b95e59b9c338453fac26540c4561e595

9b79fa745083c2c0631888da1038b1df2fdf24e93d498f572615d5946f293ecd

9d027676eedb49d2e191df82becf633516545ad8acaa018fdcdf4a87e87fba50

9df70eac532eaf8c9a6c1b0c1f899f618608ca07e95428c08f15f6f725b503d3

ad553f55800bb60c5af073ef25fa756bc1d6e9e436c3899fd04e9fc257a22822

b8b871926a4591d4cfe15f937170dc98b97f61e7587e99c7e3e6746eb622f277

bb2d21e50df175986035e9f30e8e12f0f5bfa4acf5da5b745de0f3a5c2b2e3b6

bbec1e6868b07633c0bc39b50a4bb108267df6b9ef36089ba57c041633fa70c8

bf83d027596b1edf53b11cf7f07d84b91f8a759e63f760f881dee1c427df37a3

c047cacc84db79b8be1518b068ca35aef31905163d89b018d597b9e16c2f9282

c16fe5263855cc1442fdb9c7ad057f715dd3182bbde709fee8d530952a5c1fd4

c285adacd823adb97ae109055e01353b6ecfa1e9f5fda85b574705aebe162473

c83c1d6a2c3ffa637619a359d7c05d19e2a8f7357abfb6181c2e5350a7161036

cbd16db4d21e03179885a51ad4aec18662f9db7571285fa59e67de2c6d5da5fe

cbe73fcbe63a12e35d26ef6fbedaf25bf446279437d15288e663d1ed83d7d1cf

d2938a29a2a4b5b2ca3e546ba63beca07acde93c9b63cb370a90a75b56363147

d3482df9f12b88000d90d26c4cd1e431d6bc035c65a263a507e0cebee16bb1f4

d6ebb854d897748e44d4b818aeed2ce2e7f6fdb87cdd868565215908046c40f3

e34daa3d2a59d2f5b79505e5124d5dbcab8d783d226b84618dbd17bd50cc1820

f3bb8c0fb1c089c25969b09bc26d9bc2307ca6e6061b8cede03635da800d2d61

f4b1da87f711e273f0e27242f5c5ada92260a3a950083038387317301dfca24e

face5aafe2a089c7f44e304febcb44ff3ad307f9168d62ee07659696237e94fd

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

1. **TA-TAG-2024-11-08-001**

It has been observed that threat actors TAG-110 aka UAC-0063 and Bluedelta, are an ongoing cyber-espionage campaign, targeting organizations in Central Asia, East Asia, and Europe.  Initial access is suspected to have come from malicious email attachments or exploitation of vulnerable web-facing services such as Rejetto HTTP File Server (HFS). Adversaries are  deploying the loader HATVIBE and the backdoor CHERRYSPY to conduct operations in this campaign. The other malicious malware that are used by adversaries are  STILLARCH, LOGPIE and Themida.

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

**IPs:-**

5.45.70.178

212.224.86.69

45.136.198.189

45.136.198.184

**Hahses:**

SHA-256:

332d9db35daa83c5ad226b9bf50e992713bc6a69c9ecd52a1223b81e992bc725

MD-5

d0c3b49e788600ff3967f784eb5de973

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

1. **VA-2024-11-08-002**

**Vulnerability in openimaj**

An XML External Entity (TTE) vulnerability has been discovered in Dmoz2CSV of openimaj. The affected version is Dmoz2CSV in openimaj v1.3.10.

CVE ID: CVE-2024-51136 (Critical)

**Vulnerability in Draytek Vigor3900**

An arbitrary command execution vulnerability has been discovered in Draytek Vigor3900. The affected version is Draytek Vigor3900 1.5.1.3.

CVE ID: CVE-2024-51252 (Critical)

1. **TA-APT-2024-11-11-003**

Reference is made to earlier advisories on APT SideCopy.

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

**Common Features of SideCopy Malware:**

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

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

**IP:**

84.247.176.126

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

1. **TA-APT-2024-11-11-004**

Reference is made to earlier advisories on the APT36.

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

**Common Features of APT36 Threat Actor:**

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

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

**IP:**

64.227.134.248

83.171.248.67

143.110.179.176

38.54.84.83

84.247.135.235

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

1. **TA-PHI-2024-11-11-005**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored 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.attendance.in

gov.information.in

www.joinindianarmy.in

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

1. **TA-RAN-2024-11-11-004**

It has been observed that state-sponsored groups or cybercriminal organizations are using malware to target various sectors, including government (defence, external affairs etc.), finance, technology, and critical infrastructure. Its objectives range from espionage and data theft to sabotage and disruption.

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

* Phishing and Social Engineering: Attackers frequently use phishing emails or social engineering tactics to trick users into downloading malware or revealing sensitive information.
* Exploiting Vulnerabilities: Malware may exploit known software vulnerabilities to gain access to systems. This includes zero-day exploits that target unpatched software.
* Remote Access Trojans (RATs): Many Chinese malware variants include RATs, which allow attackers to control infected systems remotely, facilitating data exfiltration and further attacks.
* Command and Control (C2) Communication: Infected devices often communicate with C2 servers to receive instructions or send stolen data. This communication can be obfuscated to evade detection.
* Use of Malware Kits: Attackers may employ sophisticated malware kits, which simplify the creation of malware and the exploitation of vulnerabilities, making attacks more efficient.
* Fileless Malware: Some malware variants operate without writing files to disk, making detection more challenging. They reside in memory and execute scripts to carry out malicious activities.

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

**IP:**

139.84.142.11

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

1. **VA-2024-11-12-006**

**Google Released Security Updates for Chrome**

Google has released LTS-126  version 126.0.6478.257 Platform version 15886.82.0 for most ChromeOS devices to resolve multiple vulnerabilities.

CVE ID: CVE-2024-10487 (Critical), CVE-2024-10231 (High), CVE-2024-10229 (High), CVE-2024-9958 (Medium), CVE-2024-9963(Medium)

**Vulnerability in WordPress Relais 2FA plugin**

An authentication bypass vulnerability has been discovered in the WordPress Relais 2FA plugin. The affected versions are Relais 2FA plugin versions up to, and including, 1.0.

CVE ID: CVE-2024-10245 (Critical)

**WordPress Released Security Update for WP Membership plugin**

WordPress has released a security update to resolve arbitrary file uploads vulnerability in the WP Membership plugin. The affected versions are WP Membership plugin, all versions up to, and including, 1.6.2.

CVE ID: CVE-2024-10547 (Critical)

**WordPress Released Security Update for WPLMS Learning Management System**

WordPress has released a security update to resolve an arbitrary file read and deletion vulnerability in the WPLMS Learning Management System. The affected versions are WPLMS Learning Management System, all versions up to, and including, 4.962.

CVE ID: CVE-2024-10470 (Critical)

**Vulnerability in WordPress Debug Tool plugin**

An arbitrary file creation vulnerability has been discovered in the WordPress Debug Tool plugin. The affected versions are Debug Tool plugin, all versions up to, and including, 2.2.

CVE ID: CVE-2024-10586(Critical)

**WordPress Released Security Updates for WooCommerce Support Ticket System plugin**

WordPress has released security updates to resolve arbitrary file uploads and arbitrary file deletion vulnerabilities in the WooCommerce Support Ticket System plugin. The affected versions are WooCommerce Support Ticket System plugin, all versions up to, and including, 17.7.

CVE ID: CVE-2024-10627(Critical), CVE-2024-10625(Critical)

**WordPress Released Security Update for WordPress User Extra Fields plugin**

WordPress has released a security update to resolve arbitrary file uploads vulnerability in the WordPress User Extra Fields plugin. The affected versions are WordPress User Extra Fields plugin,all versions up to, and including, 16.5.

CVE ID: CVE-2024-10801(Critical)

**Vulnerabilities in WordPress CE21 Suite plugin**

Authentication bypass and information disclosure vulnerabilities have been discovered in the WordPress CE21 Suite plugin. The affected versions are CE21 Suite plugin, versions up to, and including, 2.2.0.

CVE ID: CVE-2024-10285(Critical), CVE-2024-10284(Critical)

**WordPress Released Security Update for RegistrationMagic – User Registration Plugin with Custom Registration Forms plugin**

WordPress has released a security update to resolve a privilege escalation vulnerability in the RegistrationMagic – User Registration Plugin with Custom Registration Forms plugin. The affected versions are WordPress User Extra Fields plugin, all versions up to, and including, 16.5.

CVE ID: CVE-2024-10508(Critical)

**WordPress Released Security Update for  Leopard - WordPress Offload Media plugin**

WordPress has released a security update to resolve a privilege escalation vulnerability in  Leopard - WordPress Offload Media plugin. The affected versions are  Leopard - WordPress Offload Media plugin, all versions up to, and including, 3.1.1.

CVE ID: CVE-2024-10589 (Critical)

**WordPress Released Security Update for Category Ajax Filter plugin**

WordPress has released a security update to resolve Local File Inclusion vulnerability vulnerability in the Category Ajax Filter plugin. The affected versions are Category Ajax Filter plugin, all versions up to, and including, 2.8.2.

CVE ID: CVE-2024-10871 (Critical)

1. **VA-2024-11-12-007**

Palo Alto Networks has released security updates to resolve a missing authentication vulnerability in its product Expedition. The affected versions are Expedition version from 1.2 before 1.2.92. This issue is fixed in Expedition 1.2.92 and all later versions. Expedition is a tool that helps with enrichment, tuning, and configuration migration. This problem puts credentials, configuration secrets, and other data that are imported into the Expedition at risk. This flaw might be used by an attacker to change the admin account password. To reset the password to the default values, an attacker would have to send a request to a certain endpoint. To exploit this vulnerability, specialized programming or coding is not necessary.

**Threat Type:** Vulnerability

**CVE-ID:** CVE-2024-5910

**CVSS** SCORE-9.3

**Severity:** Critical

**Impact:**

* Unauthorized Access: The Palo Alto Networks Expedition platform may allow attackers to access vital features without authorization.
* Admin Account Takeover: The flaw might enable attackers to gain control of the system by taking over admin accounts.
* Sensitive Data Exposure: Credentials, configuration secrets, and other private information uploaded into Expedition may be vulnerable to theft.
* Service Disruption: If this vulnerability is exploited, it may result in service interruptions that compromise the system's availability and integrity.
* Expanded Attack Surface:  The compromised system could be used as a launchpad for further attacks within the network, increasing the overall attack surface.

1. **TA-APT-2024-11-13-005**

Reference is made to earlier advisories on the APT36.

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.

It has been observed that APT36, also known as Transparent Tribe, is deploying ActionRAT (Remote Access Trojan) malware to compromise systems.

**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:**(ActionRAT Malware)

192.99.241.4

**IPs:**

198.46.177.73

212.8.240.221

104.144.198.105

178.238.229.192

181.215.47.169

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

1. **TA-PHI-2024-11-13-006**

It has been observed that numerous phishing domains/sub-domains have been registered by state-sponsored 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Domain:**

majhinaukri.co

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

1. **VA-2024-11-13-008**

**WordPress Released Security Update for WordPress User Extra Fields plugin**

WordPress has released a security update to resolve an arbitrary file deletion vulnerability in the WordPress User Extra Fields plugin. The affected versions are WordPress User Extra Fields plugin, all versions up to and including, 16.6.

CVE ID: CVE-2024-11150 (Critical)

**Microsoft Security Updates for Windows Kerberos**

Microsoft has released security updates to resolve the Remote Code Execution (RCE) vulnerability in Windows Kerberos affecting several Windows servers.

CVE ID: CVE-2024-43639 (Critical)

**Microsoft Security Updates for Azure CycleCloud Tool**

Microsoft has released security updates to resolve the Remote Code Execution (RCE) vulnerability in several versions of Azure CycleCloud tool.

CVE ID: CVE-2024-43602 (Critical)

**Microsoft Security Updates for .NET and Microsoft Visual Studio**

Microsoft has released security updates to resolve the Remote Code Execution (RCE) vulnerability in .NET and Microsoft Visual Studio. The affected products are .NET 9.0 installed on Linux, Windows & macOS and Microsoft Visual Studio 2022 versions 17.11, 17.10, 17.8 & 17.6.

CVE ID: CVE-2024-43498(Critical)

**Siemens Security Updates for SINEC INS**

Siemens has released security updates to resolve multiple vulnerabilities in SINEC INS. The affected versions are all versions of SINEC INS, before V1.0 SP2 Update 3.

CVE ID: CVE-2024-46890(Critical), CVE-2024-46888 (Critical)

**Siemens Security Updates for SINEC INS**

Siemens has released security updates to resolve deserialization vulnerability in TeleControl Server Basic. The affected version is TeleControl Server Basic V3.1.

CVE ID: CVE-2024-44102 (Critical)

**Microsoft Released November 2024 Security Updates**

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

**Adobe Security Updates**

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

CVE ID: CVE-2024-39397 (Critical)

**Subnet Solutions Security Updates for PowerSYSTEM Center**

Subnet Solutions has released security updates to resolve multiple vulnerabilities in its equipment PowerSYSTEM Center. The affected versions are PowerSYSTEM Center PSC 2020: v5.22.x and prior.

CVE ID: CVE-2024-45490( High), CVE-2024-45491(Critical), CVE-2024-45492(Critical)