**Cyber Security Advisories**

**Date: 31 December 2024**

1. **TA-APT-2024-12-17-004**

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.

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

**IP:**

94.177.123.112

**Domain: -**

getsecurechat.com

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

1. **TA-PHI-2024-12-17-006**

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.

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

**Domains:**

certin.online

indian.army.be

www.pmjay.gov.in.crsor.live

pahchanindia.xyz

app.joinindianarmy.in

careerindianairforce.cdse.in

indianairforce.afcat.in

join.indian.navy.in

joinindianarmy.in

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

1. **TA-PHI-2024-12-17-007**

Dynamic Domain Name System (DDNS) domains are a type of DNS service that allows the automatic updating of a domain's DNS records in real time, typically associated with dynamic IP addresses. DDNS is commonly used for legitimate purposes, such as enabling remote access to devices with changing IPs, hosting servers on non-static networks, or maintaining connectivity for IoT devices. By leveraging DDNS domains, adversaries can dynamically change the IP addresses of their C2 servers while retaining the same domain name, making it harder for defenders to block or monitor their operations effectively. Organizations should monitor DDNS traffic closely and implement appropriate security measures to detect and block potential misuse.

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

Domains:

drdo.gov.in.aboutcase.nl

gov.in.aboutcase.nl

indianarmy.nic.in.aboutcase.nl

mod.gov.in.aboutcase.nl

nic.in.aboutcase.nl

\*.aboutcase.nl

\*.publicvm.com

\*.work.gd

IPs:-

199.59.243.227

103.215.216.35

5.189.221.41

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

1. **TA-MAW-2024-12-17-009**

It has been observed that threat actors are using PHPsert, a PHP-based web shell, in their cyber espionage campaign. PHPsert web shell uses various code obfuscation techniques, including XOR encoding, hexadecimal character representation, string concatenation, and randomized variable names for evading static analysis and detection.

**Capabilities of PHPsert:**

* Capability to retrieve the attacker-provided PHP code from attacker controlled server.
* Execute the payload downloaded from attacker controlled server.
* Keep changing its variant by doing minor differences in their implementation.

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

**IPs:**

185.76.78.117

**Hashes:**

2e2cf8a4a0e7decceb8e22536b13173479da0d13

3035d8846d7a9f309f2d24daba6ac33ad99524fc

399776991a094e1ee78b2a915bf4491e67c04ec7

3a688c844259822c51ceb3aea508303c4a654eb3

4d6947a19dd9a420c22fee39fac8b4df95a47569

63cea28d927f8e629377399fa08a9cb4fd0c6238

6549e50645bb1c02e4972651d335a75cb6d5aa74

83ca53c95705352ff60149b0b17a686956e23172

b2811cb4d0afe13d2722093039a72588c348dcfd

c0e03fce8f7f51e91da79f773aa870f0897b0ee2

cb6726fb3f7952ede04ed22d2c72389255991827

d57fa43944676c56e66f4b20ffa3d82048e354fd

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

1. **VA-2024-12-17-005**

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

File Name: Prominent Vulnerability List.pdf

SHA256: 9fdd98750bfbfd01f2aef77695c019a3d078dca365c4257e39832c3c57d824e8

1. **VA-2024-12-17-006**

Vulnerability in Siemens User Management Component (UMC)

A heap-based buffer overflow vulnerability has been discovered in Siemens User Management Component (UMC) which could allow an arbitrary code execution. Security updates and mitigation are available.

CVE ID: CVE-2024-49775 (Critical)

Vulnerability in TenderDocTransfer from Chunghwa Telecom

Chunghwa Telecom has released security updates to resolve reflected Cross-Site Scripting (XSS) vulnerability in the TenderDocTransfer application. The affected versions are TenderDocTransfer from version 0.41.151 to 0.41.156.

CVE ID: CVE-2024-12641 (Critical)

WordPress Security Update for Super Backup & Clone - Migrate WordPress Plugin

WordPress has released a security update to resolve arbitrary file uploads vulnerability in the Super Backup & Clone - Migrate WordPress plugin. The affected products are Super Backup & Clone - Migrate plugin, all versions up to, and including, 2.3.3.

CVE ID: CVE-2024-9290(Critical)

Vulnerability in Microsoft Update Catalog

An elevation of privilege vulnerability has been discovered in the Microsoft Update Catalog.

CVE ID: CVE-2024-49147 (Critical)

WordPress Security Update for Super Backup & Clone - Migrate Plugin

WordPress has released a security update to resolve arbitrary file uploads vulnerability in the Vayu Blocks – Gutenberg Blocks for WordPress & WooCommerce plugin. The affected products are Vayu Blocks – Gutenberg Blocks for WordPress & WooCommerce plugin, all versions up to, and including, 1.1.1.

CVE ID: CVE-2024-10124(Critical)

Vulnerability in Sign In With Google plugin for WordPress

An authentication bypass vulnerability has been discovered in the Sign In With Google plugin for WordPress. The affected products are Sign In With Google plugin for WordPress, all versions up to, and including, 1.8.0.

CVE ID : CVE-2024-11015 (Critical)

Microsoft Security Updates for Windows Lightweight Directory Access Protocol

Microsoft has released security updates to resolve the Remote Code Execution (RCE) Vulnerability in Windows Lightweight Directory Access Protocol (LDAP) affecting multiple Windows products.

CVE ID: CVE-2024-49112 (Critical)

Apple Security Updates for Multiple Products

Apple has released security updates for its multiple products.

Ivanti Security Updates for Multiple Products

Ivanti has released security updates for its multiple products.

Security Updates for Super Backup & Clone - Migrate for WordPress Plugin

WordPress has released security updates to resolve the Remote Code Execution vulnerability in Super Backup & Clone - Migrate for WordPress plugin. The affected versions are Super Backup & Clone - Migrate for WordPress plugin all versions up to, and including, 2.3.3.

CVE ID: CVE-2024-9290 (Critical)

1. **TA-MAW-2024-12-18-010**

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:

212.64.199.97

45.200.148.113

Domains:

something.catchat.us

q5f2k0evy7go2rax9m4g.ru

xg5kisn74mk2xi7gu55d.q5f2k0evy7go2rax9m4g.ru

Hashes:

045f548b113bf0d7d77fad1ac21b97bd81ec84f894b637bf9e4278a1239f75c5

0567baebbff7c5e8bc3363bf281e157fa78fc9d1ec1519ebe63a3f534d0806e8

06c20e10c1b2a1a497808bdb8ee09408704035be16e94f1223b2f5f1b6c7b43e

07436ba06220ede5338f7f770e7c6a660f11e3bbebba6c92d5988d5f512b4983

091e45adcd0fce24dbb46c211bd40a5c797ca84dec7f410badcb1e4f7d784152

09f78a23ffda93419e34c29e9a7262310e37d7ec26b7590119066fe0982de034

0b9223077fdb7111aff243fc6a4ab60aeffe84b204ef95d4b966b23903df6d72

110bf5dbc26ca732a7fb8243fe4fbc01901b00316740e3fd1233b873e43fee7e

164fb4af0b74ff37d983392a157a4d9b464391dee726dffcfc205c930a1b062f

19dec39778829e777ceb0ba83821dbb01a3bbd8a6b20f6f0fc9df1991677723d

1a698a7548e186155ad9802aa85952527bb0a1ab772462ee5b031de63f2f8aad

1ab64419388ff40eef0fb7ef31b218c60cd38d41e6295852b104ad2f4b20ce2b

1bfe2c9673f0822738a63826ba175d9dd54fa83c65f5bc4dadf1334612688e0f

1e5e6fe1899dedc11359d1ee2055fa800722439b7ee5b4fd806697ab8ad83f1d

23066de863b6b93a9f65f727c32c207928db26f058cec6d4c80d00a712cd029d

23db6425045ebe57c069ca61a25ad1efd8b0674fc67143adb271ddc25592d36f

2e54845a3bc6be86f083ea5a5a6d3f95c8c8f9fdbdad516be89d97a54664c25a

2fee0a938d98883e12a66ab95af6e8dbadf8c045a7ebc69dc87e19c56e67b9d5

36b38a7e807e19d2616365df513078b18803d512a0fad95d570334b402e39421

394cf6ad4a71182985a3bea2bb6f973d6cf58f8ce38937ccb5b4961e00ff6233

3cbfbfde21391f01128a4ed62cc49129f844676e0dd2ab375cfe82013f06375d

4023836f7a4a9d9f3e33d5d1423897633210b17fd0ec725473832ba94d42f6e0

44647af4a2e634cf0d9b74dde286fe5038902b99bb313e48ccbd0d5d491b2dc8

4802abc59f6a6fb19007440e97ab34e5623218a84f6f66e2fcd0162f32dde954

494ff34c3e791426bbc174cd05c59dfb0cffc88270c2165da118620b035dfcce

4a4d2cb9f318d3b31c134d7ddff8b0d02b00b023a8079d064c177bb7e760f9b2

504e07cf24bbd76a4cf1d66dfd1d380ecaf43c71c8414429be2aa32d4d20e3f9

5172dcf51fd501712a0b89b9ff4e63ede41754c63926a9ae6475f0a4763d0536

524eed0cc5e16a7d26efb46ce9d09641470c2db156d69558270f0c9de0271c2f

5b761a8a4e448721cd51b87c58fb74827e017e9d83decb8f0a4d63ee4e9406fe

5d43fac8e35286924e9f09294e51ed9967c282653014c7705d2f711023665d14

60551f72c86db8758cb06b3bbbd6c2413231c2b5906d3b65e53a2e22b04ecb4f

613885ab9cc5e5ad0b3182705e46288351eb92994b4a3789b04c41af138ae5f5

621f9c16c1532667d19506c0ed48b0dade15b6702908114f4450e6e7acbd5c08

64acfe57eae8113ebb6b082535800549dd85dbdbad267f36b2fbdd1c237ba254

6768b85900fee8d331086917837f2e9527ee24bad0db6e551adb85096cfe2d25

69e1453cd0cff9eb16ba3307a179e5718dc7a51ca8210798de480f34ed71f241

6b96dc9fbe7791cc5c0af51ca9b107ccfac66652fa65693251ce23beb772635f

784db5194f8b5a98cba51ceb1af187437c183b7fec992c9b03046a85cd026271

79aff9257684e0d819fceb02646d0a470511d7449c0f7a111cec5080ab3f728c

7c09fb46c4cf17bb73ec4584f1413497551fda002fc382b9a05f8e95695f6657

7ddcd50e0416e567d5ef8df927f7932324cddbb7991a46d30aadf0d224c422b1

82d117c59867ac2b0b9ba6ee61df2d82881562bc8504d5ca427de3a3544d56e8

86c5d2fca15bb5db93ae5dd24bf2cf2757fda1936914ba444c3dcf4851f4afa1

8736f6b7f08b204ade250ed7978dd764d647e894a12d926fdae6c038a2ed341f

96c9216dd3579351744f8303a135dcf1d056acd289aaa0b99c2d62de9549af31

96d159d5967e08d6ad007928993d21b462613139487cb5008c692fc2a7df6d9b

99f864c2627e28d2349ea0939bfc8d8ab87845924d7e7ae9b0f7c8883373b5db

9d225b858b47975fc3c30a5425b589897c235727dfead4cc0e2c261fae615bf3

9efbf31d6e27540eba5069725740b9eecc381a81f23cbfb80d0efeed7c839691

a0add01a6b30aecaf27a7426b12f0466db04bb3d59ef165b7cad48795463e32c

a77b2e4c2a1f4775efd8d3e6527812313b572e3a7538817ebbf36bef69138984

a79f9f82addda9680a8f94bcdaff5837cbc955f370de4f8dcdecc037e190a23b

bbb53c572a1a01eb7c910d59e362fa68d2b0a6e005065453b044bc22f80c6107

bf9811b55a00afb6e01158b6d6e37549ade7f80035a71060ed12f2bad594f575

c0c49288593828f5610e6be970b3e0415ea3583d2091f08240be1dabdb7940ba

c2495bf6bf55b3d2ad2a6a7db9c1256d003665048faca66893804232023c5870

c2b9b2283a0c7b5e0f8acd8b105337745e79e53c1fdf751209a0c0680376dfe2

c45ed30f4ba0d354b6ce670d234c4a3a194f4e21efbbbc2611ec88ab9c349a90

c551c9b232e01e120cea46d2276f3f92d5cfd492596eebf73fc6db9be119f27b

c8015ef983d37ddca9fb0fe3fa6031d10a8126d66d143e87231344abf477c637

c8986532f06833c7746e9cdfba244deae70ff32a54ced320c7c7db6c8a59e8c4

cae050d4ee9fd92bd816bd08f9f2d6a1e61be5137680b4fb844e037c4586e6ad

cb37af731170a48d758d889efed10d052d6330a1e3235f4c666587959bf064da

d1b2f197da658d907b5831fb47968b493bbdf66b7b517d20d7c5aee1c02159f9

d27b16c4a509ddc6daca9b0ed01690e23a43bf745360d149588a367e6967ecd3

d3225b7b294776a0bf960886e082f00ce32a06985b30fbb94d288e66074f305d

d44a882c31ec7c996cf327ac75602b8465e7f42ca4fae81cedd49b72ccd6b9e7

da3e6caf42495914f39617e44643a7e063e5dfac17e5733678a0cc0db7d4cde5

e0391b75c37e98876b3205fd5dbdb61fb412746eb468ad450423a11bdc5662c6

e4f31d795d55c395c53353935cac0a1d4e6ad474381dffc44ef137a8050178b8

e96ee81beeb479cde2fa9d0e0875bcec000bdf1b29665261da2520c2493a6135

eb52b30de09a45e5f476f759b879c4bf76d83408f98051862f32a49924e65a2a

f58a0e90af9096b654bc8c021b5aaf98c786e60213c50d68315e8811808dada4

f7d14865e3d08b88f92e42e7d50b2d48c129e36b41f41523ec66192967500423

fadfcd3251b69def51057b963361fe491a462ebc55fd4221d6a9b0abdd599ce6

fb76d3b27cf799ce57466693ae75dd2b0d0fc627d2dff55f518c6910f86d9bce

fcd8a6fc9e1bab10ffd2934270702658d9b5e93eb04c67f8583b174013a5799f

fce381cf7968ff6076c1748b44ecb7c004beacf34fcc3ad4105443eb1dc700f5

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

1. **TA-MAW-2024-12-18-011**

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:**

103.210.94.88

103.197.115.182

182.60.10.202

47.237.70.64

120.86.253.202

8.222.140.84

120.85.117.23

2.50.12.94

202.168.84.233

195.3.223.52

45.221.98.118

27.47.2.199

31.220.1.88

47.84.32.163

120.85.114.158

59.94.44.46

120.85.119.87

173.231.22.19

107.172.21.17

103.210.94.111

120.85.117.12

47.236.135.111

120.86.252.5

112.94.99.204

123.58.199.75

27.43.205.232

103.149.87.69

193.239.147.201

175.107.2.70

61.52.36.39

123.175.90.16

117.205.47.127

117.199.22.177

61.2.104.116

112.248.110.221

61.3.131.41

42.52.160.192

59.95.88.227

45.230.66.14

42.224.122.9

103.199.200.75

196.189.40.159

175.175.61.209

112.94.97.204

117.235.58.205

152.32.148.250

87.121.86.54

51.159.99.244

70.39.75.132

178.215.224.228

182.64.143.22

47.88.101.80

117.209.88.97

221.15.227.118

117.199.72.2

103.115.197.215

103.210.94.248

60.22.178.173

115.55.130.209

59.182.118.111

175.107.3.160

112.248.141.215

117.209.20.138

117.209.240.58

103.247.52.82

117.198.240.186

45.230.66.42

175.107.3.213

209.103.243.40

122.96.50.190

175.151.104.152

141.147.35.246

130.61.232.223

130.61.131.236

120.224.87.183

161.132.50.89

106.124.134.61

171.244.40.20

134.255.179.102

221.1.150.146

130.61.60.134

103.54.12.100

91.205.105.147

47.236.49.157

130.162.253.178

117.72.104.80

39.165.196.149

216.10.250.218

212.28.190.31

45.137.194.55

94.142.140.201

83.143.112.244

8.220.185.175

130.61.43.118

47.236.127.1

191.96.245.224

112.6.214.244

103.149.91.229

176.124.205.151

107.175.82.204

130.61.81.206

220.250.52.123

130.61.103.179

1.54.108.96

182.44.13.243

36.138.79.187

175.107.2.223

59.97.124.223

175.146.53.6

117.209.235.107

117.209.7.174

117.206.176.113

117.210.191.49

103.167.204.40

213.92.254.186

221.200.70.250

175.107.3.252

175.107.0.234

220.198.241.106

112.94.96.83

59.99.42.246

114.247.184.161

45.156.128.49

23.94.61.137

198.23.149.17

178.72.71.123

45.178.251.62

160.178.152.251

202.55.134.250

154.9.247.230

92.255.57.86

103.160.69.101

66.63.187.64

175.101.29.202

87.120.125.95

43.242.117.18

116.110.78.200

66.63.187.69

49.205.218.245

66.63.187.54

105.112.225.26

43.134.160.203

185.216.147.183

103.69.29.162

43.133.32.74

193.141.60.85

177.54.132.238

94.102.49.19

106.51.65.26

206.238.123.168

59.184.245.232

112.94.99.62

103.210.94.160

222.240.12.11

141.98.11.155

223.149.52.129

120.85.119.245

154.38.189.45

103.210.94.31

152.42.234.215

27.122.61.21

103.210.94.171

119.188.171.195

112.94.99.160

103.210.94.91

120.85.117.177

124.8.180.27

45.127.126.84

103.199.180.142

**URLs:-**

http://103.199.205.197

http://85.191.154.89:58207/

http://45.64.226.218:56563/

http://219.155.208.30:54535/

http://61.3.83.105:45679/

http://59.183.105.18:37779/

http://124.234.246.127:56111/

http://59.184.254.21:44702/

http://117.223.8.147:42491/

http://61.1.235.216:58198/

http://103.197.112.7:58394/

http://175.107.3.217:36559/

http://103.115.197.213:40128/

http://60.19.241.252:47610/

http://220.158.159.242:48076/

http://59.89.66.45:52945/

http://117.248.24.87:37089/

http://223.8.206.30:46634/

http://223.8.0.201:50494/

http://14.26.130.29:33473/

http://117.242.251.175:45610/

http://119.116.132.88:32799/

http://45.178.250.42:11282/

http://1.70.130.253:52837/

http://171.36.16.171:46233/

http://59.88.233.164:52375/

http://190.103.70.57:34328/

http://117.209.113.254:55581/

http://59.183.136.8:35727/

http://117.235.126.180:51380/

http://123.185.228.118:46192/

http://115.50.0.138:44819/

http://59.184.241.147:54387/

http://185.248.12.129:50915/

http://113.26.95.127:56656/

http://223.13.82.9:54296/

http://119.179.213.228:49140/

http://42.52.160.192:51132/

http://175.175.61.209:32936/

http://61.3.131.41:33761/

http://117.196.143.95:54868/

http://110.182.241.29:49224/

http://103.199.200.75:42541/

http://45.230.66.14:10907/

http://114.227.58.43:48102/

http://59.95.88.227:46190/

http://117.209.81.225:54036/

http://182.127.153.29:36000/

http://175.107.0.96:58504/

http://61.52.36.39:39274/

http://14.102.96.21:46406/

http://118.174.70.8:56365/

http://49.71.26.97:40725/

http://196.189.40.159:58416/

http://193.239.147.201/bins/x86

http://103.199.200.75:42541/Mozi.m

http://112.248.110.221:36534/Mozi.m

http://117.199.22.177:43993/Mozi.m

http://117.235.58.205:40253/Mozi.m

http://123.175.90.16:59515/Mozi.m

http://175.107.2.70:45557/Mozi.m

http://175.175.61.209:32936/Mozi.m

http://42.224.122.9:45981/Mozi.m

http://42.52.160.192:51132/Mozi.m

http://45.230.66.14:10907/Mozi.m

http://59.95.88.227:46190/Mozi.m

http://61.2.104.116:35156/Mozi.m

http://61.3.131.41:33761/Mozi.m

http://61.52.36.39:39274/Mozi.m

http://196.189.40.159:58416/Mozi.a

http://175.107.9.115:46376/

http://59.95.80.168:60878/

http://117.209.80.40:54496/

http://103.200.84.43:34731/

http://117.196.174.193:43789/

http://117.221.173.36:49502/

http://119.115.161.193:34127/

http://42.7.222.225:39408/

http://45.230.66.41:10482/

http://85.191.154.89:58207/

http://122.148.196.101:47796/

http://123.13.156.92:35455/

http://59.97.122.168:35881/

http://102.207.137.125:58327/

http://59.99.91.157:36464/

http://115.50.2.6:41988/

http://115.49.27.167:40973/

http://182.114.49.199:59729/

http://61.3.137.1:44543/

http://27.217.202.43:49938/

http://114.239.168.24:58268/

http://117.235.52.158:56836/

http://103.124.138.115:39000/

http://42.85.185.171:43391/

http://59.93.25.121:40701/

http://117.204.236.148:42968/

http://59.89.231.16:42179/

http://61.3.102.185:48687/

http://115.49.24.244:55918/

http://45.164.177.106:11394/

http://139.5.1.232:36839/

http://90.227.182.190:39883/

http://42.54.165.222:36568/

http://103.124.138.115:55672/

http://117.243.223.35:45640/

http://115.51.42.151:35798/

http://117.208.215.180:46116/

http://182.113.47.100:53102/

http://123.14.119.35:39921/

http://123.14.110.97:37640/

http://221.202.20.121:59035/

http://117.210.183.229:40792/

http://45.178.250.150:11774/

http://117.209.93.26:53392/

http://27.37.89.101:60631/

http://116.111.16.74:55643/

http://112.255.110.241:56312/

http://200.124.241.140:44184/

http://139.5.0.169:38902/

http://182.116.54.177:41916/

http://201.110.101.73:41816/

http://175.30.114.47:40590/

http://117.221.240.241:54529/

http://61.54.61.14:54441/

http://61.52.7.244:41361/

http://123.190.138.123:55847/

http://196.189.35.8:55844/

http://117.209.2.170:59843/

http://94.156.58.77:39015/

http://123.139.220.169:52607/

http://113.26.57.110:40200/

http://103.78.148.166:47328/

http://103.199.205.158:44866/

http://115.56.184.232:38492/

http://123.9.243.30:38933/

http://45.115.89.59:40860/

http://117.199.77.240:40683/

http://223.13.70.129:53818/

http://196.189.35.8:55844/

http://117.209.82.87:43196/

http://112.246.17.232:37114/

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

1. **TA-MAW-2024-12-20-012**

It has been observed that threat actors are actively targeting Critical Sector Entities with a malware variant known as AllaKore RAT. This malware has been used to steal sensitive information through a combination of malicious techniques and sophisticated spear-phishing campaigns, which aim to trick officials into executing infected attachments. Specifically, threat actor SideCopy is involved in deploying AllaKore RAT on targeted systems.

Key Characteristics 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Domains:-

microsoftstores.zapto.org

\*.zapto.org

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

1. **TA-APT-2024-12-20-004**

It has been observed that Spynote, a mobile Remote Access Trojan (RAT), primarily targeting Android devices, is designed to gain unauthorized control over infected devices, exfiltrate sensitive data, and spy on victims. The Spynote RAT is distributed via malicious apps, fake updates, or trojanized applications disguising itself as legitimate software to trick users into installation. Once installed, Spynote exploits device permissions to perform malicious activities, including stealing credentials, recording calls, capturing screenshots, activating cameras, and exfiltrating SMS and contact lists. It can also establish persistent Command and Control (C2) communication to execute attacker commands.

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

**IP:**

182.180.104.47

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

1. **VA-2024-12-20-007**

It has been observed that a critical vulnerability tracked as CVE-2024-53677 is being exploited by adversaries and affecting Apache Struts. Exploitation attempts using various malware families and techniques such as path traversal and authentication bypass are being used for exploitation. File upload parameters can be changed by an attacker to allow path traversal, which in certain cases may result in the uploading of a malicious file that can be used to carry out Remote Code Execution. The threat actor might also be able to upload random payloads to vulnerable systems, which they might then use to execute instructions, steal information, or download other payloads for further exploitation.

**AFFECTED VERSIONS:**

Struts 2.0.0 through Struts 2.3.37 (End of life)

Struts 2.5.0 through Struts 2.5.33 (End of Life)

Struts 6.0.0 through Struts 6.3.0.2

**Recommendations:**

* Organizations should prioritize patching as soon as possible.
* It is recommended to upgrade to Struts 6.4.0 or greater and use Action File Upload Interceptor to mitigate the risk of cyber attack.
* It is also advisable to migrate to the new file upload mechanism.

1. **TA-MAW-2024-12-20-013**

It has been observed that state-sponsored groups or cybercriminal organizations are targeting Critical Sector Entities through malware campaigns. This malware targets 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**IPs:**

115.61.168.143

103.238.227.183

115.61.169.139

103.238.225.248

182.114.110.170

116.206.178.67

**Domains:**

howtotopics.com

thelocaltribe.com

councilofwizards.com

goclamdep.net

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

1. **TA-MAW-2024-12-23-014**

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:**

120.85.117.100

120.85.114.70

111.253.50.94

1.163.200.249

220.198.241.242

111.249.4.177

122.96.50.175

185.157.247.35

64.49.14.19

193.239.147.201

26.99.153.102

27.43.206.145

103.210.94.9

120.86.253.105

24.132.249.139

175.182.131.54

123.58.199.75

123.241.186.26

95.214.55.74

157.231.51.20

31.220.1.88

113.199.116.100

122.97.138.130

27.43.207.20

103.210.94.104

103.210.94.96

103.245.236.146

36.150.108.230

147.139.212.194

113.247.176.239

27.122.61.254

61.152.143.73

27.43.206.45

152.42.234.215

103.149.87.69

123.241.41.211

117.209.46.126

112.94.98.68

143.92.61.57

27.157.169.233

212.192.241.72

120.85.116.42

103.199.180.147

120.85.117.155

181.214.173.76

175.107.37.51

27.47.1.7

27.43.207.217

103.199.200.84

**URLs:-**

http://59.91.97.185:48973/

http://45.164.177.109:10920/

http://59.95.91.121:37028/

http://123.11.78.221:47500/

http://45.164.177.132:11542/

http://113.222.147.100:34485/

http://117.216.66.68:51382/

http://61.1.245.134:45449/

http://115.63.10.145:51367/

http://117.242.252.255:55996/

http://178.141.79.50:44637/

http://45.230.66.47:10623/

http://115.49.235.149:55055/

http://59.96.254.48:42545/

http://102.33.6.151:57090/

http://117.251.163.55:37920/

http://117.223.11.77:50238/

http://42.224.196.3:54678/

http://45.164.177.75:10183/

http://117.192.233.45:39611/

http://190.109.227.93:50213/

http://103.124.138.115:52534/

http://45.164.177.124:10703/

http://59.99.221.81:55220/

http://61.0.187.100:60277/

http://45.164.177.1:11752/

http://182.120.165.247:50645/

http://117.247.24.88:34276/

http://59.184.250.110:36986/

http://220.158.159.12:40589/

http://117.199.30.15:48835/

http://139.5.1.241:39954/

http://42.231.89.181:49952/

http://42.248.174.2:55080/

http://125.44.211.8:48642/

http://117.253.164.136:56467/

http://45.164.177.20:10139/

http://102.33.40.70:53955/

http://117.209.25.224:52308/

http://102.207.137.125:37514/

http://103.210.101.55:34124/

http://125.46.197.226:36731/

http://182.88.164.173:50162/

http://223.8.239.68:34480/

http://182.124.26.222:50357/

http://59.93.202.15:39072/

http://27.215.126.55:40357/

http://119.116.84.19:58388/

http://175.107.1.108:51892/

http://103.200.85.40:58678/

http://59.184.242.196:53847/

http://59.89.64.109:33425/

http://175.107.3.69:58427/

http://139.5.10.56:39060/

http://220.158.159.125:39340/

http://222.141.154.46:58232/

http://123.14.17.24:34719/

http://45.164.177.170:10113/

http://220.152.181.6:59969/

http://85.191.154.37:57508/

http://123.175.25.67:56806/

http://61.0.8.210:41865/

http://117.209.237.71:54876/

http://123.175.66.48:44052/

http://45.164.177.118:10387/

http://27.215.52.137:45343/

http://27.217.174.252:39818/

http://119.179.198.21:48047/

http://119.180.54.225:38394/

http://117.210.186.43:37534/

http://123.12.84.141:44045/

http://182.116.23.124:49100/

http://61.3.143.3:59507/

http://182.127.113.79:36787/

http://220.158.159.38:48983/

http://42.234.57.238:49026/

http://42.228.106.8:32797/

http://42.58.208.16:48728/

http://123.149.78.240:48727/

http://45.230.66.29:11043/

http://117.248.63.132:53379/

http://160.238.95.229:35738/

http://175.107.0.225:53900/

http://123.14.106.155:52430/

http://117.199.181.150:34811/

http://103.210.93.28:46310/

http://117.209.9.20:38966/

http://59.178.67.250:53146/

http://123.14.252.199:53218/

http://110.182.172.94:54296/

http://118.172.51.231:54432/

http://175.162.36.215:35571/

http://114.228.129.17:55343/

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

1. **VA-2024-12-23-008**

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

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

**SHA256:** 37cdf3b4fc669227225b8882d8d0e80bfd05158268f0b90de1b919ce0a07b79a

1. **TA-PHI-2024-12-23-008**

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:**

sci-gov.info

assamrifles.gov.in.lazetoys.com

maharashtra.gov.in.studentemarks.in

rmc.gov.in.webstatarchive.com

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

1. **VA-2024-12-23-009**

A surge in password-spraying attacks has been observed which leads to user account lockouts and being denied VPN access. Adversaries have used password-spraying attacks for credential access. Password spraying is a type of brute force attack in which an adversary uses a single common password or a handful of common passwords to try to access many accounts on a network. Unlike traditional brute-force attacks, which typically try many passwords on a single account, a password-spraying attack spreads out the effort across multiple accounts using only a few (or even a single) password per account. This method is designed to avoid triggering account lockout mechanisms that are often in place to prevent too many failed login attempts on a single account.

1. **TA-RAN-2024-12-24-003**

It has been observed that there is an increase in RansomHub activity. RansomHub is a term associated with cybercrime & ransomware operations that refers to platforms, forums, or marketplaces used by cybercriminals to facilitate the buying, selling, or sharing of ransomware tools, stolen data and other illicit services related to ransomware attacks.

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.

New RansomHub tools and TTPs :

* KMS Auto: An open-source suite of tools (KMS Auto ++, KMS Auto Lite, and KMS Auto Net) developed to activate Microsoft Windows and Office for free. These tools are developed in .NET and can run on multiple operating systems.
* Supremo: A legitimate remote desktop software to establish remote access. The affiliates downloads Supremo following installation of Splashtop, another popular remote access software, likely to create multiple persistence mechanisms.
* Veeamp: A password stealer malware that targets the Veeam data backup and recovery application.

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

**Hashes (SHA-256)**

81f8fc4aef686dbc4e2b1f6b08fbac33bf877610c268564e9ecfbae1425d5e5c

4aab0c8d1dfa1b5164fcb3ecb6a837c030a24cc7a0103ba3ccdf77fabf083281

419a59355b6038ba17dbf4ed4f6961cd6535cffbe205ac31c7628e38a94405d9

9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732

18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88

7989888fc3aa7447bcf51615bd7cdc2e66e01e873a399d5947527156dd7b2595

10629b9bcb7da31ff8bc980e94f97dfc0dee9e9c72d6db75e98c65c7d5c73012

22236e6ecf21c772759cea279e38cddc3d9d0f053be6aabe5779c87eadd68b58

467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486

05f57f3a97eb990bcef3904c46d9d58a8e547c4eded64d23cb51c85249e6e47f

619c83c432e7efb7cdf9b98e31ee617275385b96297ca467ebf29c1ef9110877

6502364a11ffe1b4fcdf6a5f55dae190d244c2e9646c88b45cc3a4e210e1e575

ce162d2d3649a13a48510e79ef0046f9a194f9609c5ee0ee340766abe1d1b565

8ecea5e10fe8a23cae5b3a7a21706b5fdd6c3042f549d773d7e4d8cf13408032

b3eb283c2c18cbd61e2059f0aa1c52ecc395f3fe492196661018337e982bb1d5

7022e9b74a97d5f189bdfeb2bebf298b30b7f8e96f327f84c76fe12ce37a2ff3

237e7d8399a8730c5a658b46e6084947e1993da53f7242d41869a1b21bd7adc7

a96a0ba7998a6956c8073b6eff9306398cc03fb9866e4cabf0810a69bb2a43b2

7989888fc3aa7447bcf51615bd7cdc2e66e01e873a399d5947527156dd7b2595

d9ae52dbff8bdcd67c162870fb907ced97d6bb011a2a587f859638c38758f2fa

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

1. **TA-MAW-2024-12-24-015**

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:**

20.221.64.23

185.255.120.43

31.172.83.147

**Domains:**

stresser.pw

**Hashes:**

0020b9159b4ff44f4a6afb28107109627498e9245983a807b623adef72ae39c0

04e83cff983b48e6ed48f636a446e64135bcc582e684b8f1d04aa093ffed47bb

051193750ed32fd908511bf1d0fa5da3370442490177e9e2074e7d81a9fbfd69

0544cb52a924da780dfef5f1ad2c09932ab3a715e975c69528be6f46af9d3e74

05b92b97502325611eb11ed99e259c59b824c62806bcf558c645587ee0bec39b

0a7bb9f077ca659ceca726b3c5903f2d74c805beeb6c2996356629067157e8a9

1485900c30d5237868b631de0308b0089ad263808e4c820f9e46bd3802d4742a

14f8c462a12a94e86a17b9af2d81caa032d8bbd8f96ba2faba431bc8ef23f381

162304fdc1cd3d75fea554573ff5af4dff3e2b3364790faa76fb37caa86d0fd5

171cdbcf009ab1f14567331f9dec9bc5964979b95ede87f4a948be71bcc5a286

1760ef63d11e8bdf984c1291a0512261d079c932558f516039b2b0dd0d237dc1

1764b6cfd1498df572b16ae51695a762a7315c41fe5b6d992607704ab0d4e862

251b21fe4dbb1b55a5ba3bb4e9e9a0c8cf537ad05aefa1255c6b4aaacace5fc2

26967c9fdad5754def84215c37e4a5c14ad712441d9cf4461c98fa335d97e5b4

288fb765949d2d73542a6fda793ef2141bb3b78dd62e9ef29851970b1baa1cdb

299a7c514587e66965f5974eca4615d86bb1d11ec3fc0a343cc3a372853f8367

2f7138b5586d138742692b751a1392fdabd8b10d5716d8c47151ccd6bdff9c31

33dc056b0f01ec8c878617d649800c32d387ef0e73ace537894a86c42cb7ee6d

37edfff53329b5314b8731ddac1f7494a123ba5e6ed8055f4859cd6d08264fd2

38a9660cc6cc2e81a8e22634deefd8e37e1f4fccb987c60a8d126317e922bdf9

39f400cfe0158e9074f6b5778395b1a58286713547703942b64832ca61b17a86

3c63a335ba254e34f33457ef150541e8caa5abace4e63da688d149b699b823a3

3c7f1e0b01c900b5828447ad62a5b7827fbfffd967e311216abe614115f896ee

3dcb35f690db2ce8813c1c9da1afc2a3290d05982aad962d0decd16e22cbeda2

4de33c85ab2214bd48d0abf5f028708c04e6da105f2c0abdfa1af103819b965e

4f2127e4905cc911e63bd43e34dcd9ffc62fb286e003f4e00910b31974b36a69

585ebabd8ea102b183f5c9876b88a02ff6c3e73c84eac1eda697be522e4e7635

58c9957fd0051e0806f8b92ef24c0628b59fd9dfcc9b4e17dbd2fc2785c34148

59efbdb3ff151f47d53d618917a4006d53296af046b49afab7da9ea4bfc40bef

5e6dcfba7136639901b4997698d5ee6065089b283d86c0c5cb7f07ab99c1f0d5

60472e286fc9933a31b7500d8f2b4273138b328a35c87a33f7c1886c5e34dfce

619daaef476d6b309f1ee3ac9fafff964e9a4c1ad2e05f938c3a2cf4a917aaf7

68c27701dc21461780134ea4debadff91fd724a983521369922ae86cd703a15e

6b850932b63810e776d14567554bc859bb1164c7b8d13e47306a33b0e3e22763

6f16eacb53d3ec46cac764a5c6ff30cb3b781dd7a21b1c0da0d2004e5f143492

760f18c983a524296a30cfce0683bce5ae9fc58c3757169c5d2b4ca1dcded51c

772e82967c8e436e64cb8b31f582b7cb255b5a7f02df03ac2551aadfe2c287fe

7952b6f54d1ddfed2359245de196fb3d91e33e280349f566172d96897e54b04b

823317d0066434e2981c194baf91f3a0cbacd0abd14b4f0a5676852dd3c352c7

86b5a24e812fd73150b33420ee8bc77bd0bc4ee31a3ffb0211c070388b0bd1d9

8a0514952b4fb179dffdaa02c9e95d9edb157cf7a6d48c6dca82405676df5411

8d0b462f3a11db77ec4a28f8c4fbfa0eed1f10928749410ea1572983703d8f83

91c6db1a101cd083c457808cc956ca7621f1603705d5ea6d575f9d0e2d1b1d55

973d168d62d72d6aade3e517f01517af33db47ab3c98700cfeb92a0088ab601e

9ad73cf3a1ac2fa0676616b6c47f8458c0db4f12f0bee2ba635f9d2cb29637cc

9af537452e466b13d5f87960404e8837e2165fc4df896b6f367a43b0d53f02a7

a3eae8ee4664358f5549c9092d56c56b83eecd2fb0f77163f5badabcca1d8a82

a628f5d9287c5a589209c468af74831734fb17ad6cbd9b30f7d7b7ab1eb34fba

ab1ef31147431fff3f4bacf70b5844cdf8cfb9109ab35cc48cdf273bcd41801f

ab2673de475350cfc769f87bab300f542364173dd79123905cc3351dea70cc33

b1e6fcfe6b504e2907ed424a4d04ab0185f199e0fc26772ac3e9a7a11a99ad7c

b62882d995056971e0c6803a9b3192ec20c798346190cd1e74cae8bcc58cd91f

b995f0b8cac59259d9a4b9c6b3c0d986e98e74ac5b8f9906fe94778b46b65b63

bc5fb52da40145a1015a97f7969fe13cea6e42f467763caf3d5bbf686bad6547

c242559d38b05caebeec96c80a5a3b7aee7d849a6353fb60b02407e46bd94255

c7cd273f017e3cfe2e4dcfcfef6efac535a5fb7f8d1808be2ceb480cf2fe4361

cb7fa9a8dcef85d5c088d80d6e49d3ee9df0feda1dde95fe2b8f9b245f3d3e96

d548b5b92fd5b1afdb79d91b22d314c01cc5ec3ad4c2cf697673e746621167cb

e20ba7a96c963109ca9b41b8556ca8540de7baf5c26cde586f71416e2c4f9802

e271f4c6921bb64b7cfea367595d05c1becd3ce53743f439247810036a981b69

eccfa82d22890f31c64bda17558ee576c473abc0c61fac6f12d5c700c0c903fa

ee672367219bc4fe2a3dbde9765f2df28bfe4ada54e1623470c9aa81111ca1c6

f148ef3515d7cf4dce720b4abf4c3e15b83bfaee58cf387a4c25a0850ac10de0

f1f197e5826fb1dab05a107ddec7d1de7084178d1fc647d4149e1c1c832ae2f8

f7fb85b4f874b0545cd71b69e284457b78eb299e5d1ac7a868fc5a572ad824ad

fb48e310918593526b89a4354ed829932c63aeee6e4e2db6b3a25e306e858342

fe58b5ab6a62b7e84264dbd0ad42faed15d41407974dd6a09887d4470d3dac33

fea0959d65ea7100e7ce7b536138fa11bb44754b167a4377a2b117da70e422b1

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

1. **TA-MAW-2024-12-24-016**

It has been observed that HiatusRAT, a sophisticated Remote Access Trojan (RAT), is targeting outdated business-grade routers / network edge routers, IoT devices, particularly web cameras and DVRs. Its capabilities include remote control, passive traffic collection, executing remote control commands, covert Command and Control (C2) functions, converting infected devices into SOCKS5 proxies for adversaries.

State-sponsored threat actors are known to exploit compromised devices as part of anonymization or Operational Relay Box (ORB) networks. These covert infrastructures obscure the origin and destination of malicious traffic. Such mesh networks often consist of compromised devices or actor-controlled Virtual Private Servers (VPS), utilizing multiple hops between entry and exit points to complicate tracking and attribution efforts.

Impacts:

* Remote device takeover and control
* Unauthorized access to surveillance systems
* Potential network compromise
* Data exfiltration risks

Distribution Methods:

* Scanning campaigns targeting vulnerable IoT devices
* Exploitation of unpatched vulnerabilities
* Telnet access exploitation
* Brute force attacks using tools like Medusa

Capabilities:

* Remote device control and takeover
* Passive traffic collection
* Functions as covert C2 infrastructure
* Reconnaissance capabilities
* SOCK Proxy servers  / relay traffic systems

Attack Methods:

* Exploits multiple CVEs targeting IoT devices
* Uses publicly available tools (Ingram for scanning, Medusa for brute-forcing)
* Targets devices with telnet access
* Exploits weak vendor-supplied passwords

Indicators of Compromise (IOCs):

* Targeted TCP Ports: 23, 26, 554, 2323, 567, 5523, 8080, 9530, 56575
* Scanning tools: Ingram (webcam-scanning tool), Medusa (brute-force tool)
* Targeted devices: Xiongmai and Hikvision devices with telnet access

**Recommendations:**

* Limit and Isolate IoT Devices: Restrict or isolate vulnerable devices from the main network. Replace Unsupported / End of Life devices.
* Regular Patching and Updates: Apply firmware, OS, and software patches immediately. Remove unsupported devices.
* Strong Passwords: Avoid default passwords; use unique, complex passwords and enforce policies and Audit administrative accounts
* Multi-Factor Authentication: Implement wherever possible.
* Security Monitoring: Log network activity and set up alerts for unusual behavior.
* Network Segmentation: Segment networks to reduce risk and exposure and Scan and mediate unnecessary open ports

1. **TA-RAN-2024-12-26-004**

It has been observed that various ransomware groups, including BlackByte, Qilin, Embargo, DragonForce, Akira, Kassieka, and RansomHub, have been observed using Bring Your Own Vulnerable Driver (BYOVD) techniques for evading detection, maintaining persistence, and escalating privileges. In these attacks, cybercriminals identify signed drivers with known vulnerabilities, which are often available from online repositories like LoLDrivers.io. These compromised drivers are then deployed onto victim systems, either as part of a broader attack chain or bundled with malicious payloads, to exploit the vulnerabilities and gain elevated privileges on the targeted machines.

**Recent Attacks Utilizing BYOVD:**

* Kasseika: Exploited a vulnerable driver, viragt64.sys (part of the VirIT antivirus software), to disable security processes and facilitate the ransomware execution.
* Akira:  Abused the zamguard64.sys driver from Zemana Anti-Malware to disable EDR at the kernel level. Akira has evolved its tactics, focusing on data exfiltration while continuing to leverage BYOVD techniques.
* Qilin: Used the amsdk.sys driver (CVE-2024-1853) to terminate processes and evade security measures. This attack was part of the group’s double-extortion approach.
* BlackByte: Deployed a series of vulnerable drivers (RtCore64.sys, DBUtil\_2\_3.sys, zamguard64.sys, gdrv.sys) to bypass security defenses and facilitate encryption.
* RansomHub: Exploited a vulnerable driver through a new tool, EDRKillShifter, to disable security tools and escalate privileges before deploying ransomware.
* Embargo: Used Sysmon64.sys as part of an attack that leveraged safe mode and BYOVD techniques to disable EDR before ransomware deployment.

The increasing use of BYOVD techniques is concerning as it allows attackers to bypass even advanced defenses like Endpoint Detection and Response (EDR) tools. It enables them to:

* Gain kernel-level access: Exploiting vulnerable drivers enables attackers to perform privileged actions on a victim’s system, often undetected by traditional security tools.
* Disable security tools: Malicious drivers can disable critical processes related to security and defense mechanisms, leaving systems more vulnerable to additional attacks.
* Establish persistence: Once deployed, these vulnerable drivers can remain on systems, providing attackers with ongoing access.

**Recommendations:**

* Implement driver blocklisting tools: Utilize solutions such as the Microsoft Vulnerable Driver Blocklist to block the loading of known vulnerable drivers.
* Keep drivers updated: Ensure that all drivers, particularly those from vendors with known vulnerabilities, are regularly updated with the latest security patches.
* Enforce strict driver loading policies: Use tools like Microsoft Windows Defender Application Control (WDAC) to control and prevent the loading of unauthorized or unsigned drivers.
* Restrict driver installation permissions: Limit driver installation and updates to trusted administrative accounts to reduce the risk of unauthorized drivers being installed.
* Deploy advanced EDR solutions: Ensure your endpoint detection and response (EDR) solutions are capable of identifying and blocking attempts to exploit vulnerable drivers, even when they are signed.

1. **TA-PHI-2024-12-26-008**

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.email.gov.in.indiandefence.link

email.gov.in.indiandefence.link

\*.indiandefence.link

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

1. **TA-PHI-2024-12-30-009**

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 with their resolving IP's that are targeting Critical Sector Entities (CIIs).

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

**Domains:**

gov.in.cyou

nci.in

goov.in

gov.in.top

crsorgimygovin.in

email.gov.dvia.ev

mod.ggovin.com

gov.in.app

crsorgovin.org

crsorgimygovin.in

scigovin.com

print.govindia.in

electronicgovindia.net

thedigitizeindiagovin.com

**IPs:**

44.227.65.245

64.190.63.222

75.2.115.190

87.242.126.96

144.76.3.233

161.97.164.143

104.22.7.114

13.248.169.48

85.107.56.194

144.76.3.233

91.195.240.94

217.21.87.17

190.92.174.28

206.189.132.222

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

1. **TA-APT-2024-12-30-005**

Reference is made to earlier advisories on Mythic Malware - APT 36 Campaign.

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

**Common Features of Mythic Malware:**

* Persistence
* Remote access and data theft
* Modular architecture and customizable
* Stealth techniques to avoid detection by security software

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

**IP:**

170.64.175.56

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