From: Mr SANI ABHILASH CERT IN <cmtx.certin@meity.gov.in>
Sent: 18 October 2022 10:23
To: alert <alert_reply@cert-in.org.in>
Subject: [CMTX-P-102022712] COBALT STRIKE ALERT 28 (TLP:RED)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

[CMTX-P-102022712] COBALT STRIKE ALERT 28 (TLP:RED)

META INFORMATION

Confidence- High

Risk- High

TLP- RED

- - - - - - - - - -

- - - - - - - - -

- - - - - - - -

- - - - - - -

- - - - - -

- - - - -

- - - -

- - -

- -

- ----------

- - - - - - - - - - -

NOTE FOR ACTION REPORT:

• CERT-IN requires observation/incident reports, if any, pertaining to

the shared alert i.e. SIEM alerts, specific positive hits, malware hashes,

threat hunting results in sanitized form within 6 hours to

cmtx.certin@meity.gov.in ONLY

• Compliance and after action reports and comments on audit observations, timings and quality of the alert contents, anomalies observed, false positives and any other comments can be sent as a Monthly Cumulative Summary Report.

• CERT-IN Threat Intelligence Platform recipients can share feedback anonymously in the form of IOCs/reports to the platform using TAXII INBOX functionality.

- - - - - - - - - -

- - - - - - - - -

- - - - - - - -

- - - - - - -

- - - - - -

- - - - -

- - - -

- - -

- -

- ----------

- - - - - - - - - - -

PREVIOUS ALERT REFRENCES:

[CMTX-P-102022702] COBALT STRIKE ALERT 27 (TLP:RED)17.10.2022

ALERT BRIEF:

CERT-IN has been tracking prominent RATs/malware families. An uprise in activities associated with Cobalt strike is reported.

OVERVIEW:

Attributed as a Commercially available framework Cobalt Strike supports Command and control communications over HTTP, HTTPS or DNS.

The framework has been a mainstay in cyberspace due to its advanced capabilities and is in use by Criminal groups and Nation state-sponsored actors.

CAPABILITIES:

- - - - - - - - - - - - Command Execution
- - - - - - - - - - - - Key Logging
- - - - - - - - - - - - File Transfer
- - - - - - - - - - - - Privilege Escalation
- - - - - - - - - - - - Port Scanning
- - - - - - - - - - - - Lateral Movement

A list of Indicators of compromise is provided below for your action side.

**********IOC START**********

IP:Ports Country Last seen

8[.]141[.]153[.]32:8099 CN 13-10-2022

138[.]68[.]229[.]86:8443 US 13-10-2022

178[.]62[.]204[.]22:443 NL 13-10-2022

8[.]210[.]84[.]140:6666 HK 12-10-2022

124[.]220[.]156[.]75:4430 CN 12-10-2022

49[.]7[.]131[.]69:5555 CN 12-10-2022

120[.]48[.]75[.]169:6666 CN 12-10-2022

120[.]48[.]116[.]48:8081 CN 12-10-2022

8[.]210[.]84[.]140:6666, 443 HK 12-10-2022

120[.]48[.]75[.]169:6666, 6667 CN 12-10-2022

47[.]100[.]100[.]12:2087 CN 12-10-2022

198[.]148[.]111[.]17:9999 US 12-10-2022

39[.]103[.]189[.]229:8443, 5555 CN 12-10-2022

36[.]27[.]214[.]150:4747 CN 14-10-2022

43[.]155[.]2[.]46:2086, 2096 HK 16-10-2022

8[.]142[.]92[.]17:7788, 8888 CN 16-10-2022

47[.]242[.]83[.]109:8143 HK 14-10-2022

42[.]202[.]144[.]230:8443 CN 12-10-2022

47[.]94[.]3[.]175:9113 CN 14-10-2022

45[.]32[.]64[.]150:8000, 8443 US 15-10-2022

107[.]182[.]18[.]111:4433 US 13-10-2022

23[.]227[.]203[.]100:8443 US 12-10-2022

43[.]138[.]150[.]21:8443 CN 12-10-2022

101[.]35[.]49[.]249:8443 CN 12-10-2022

170[.]178[.]217[.]162:8443 US 16-10-2022

124[.]221[.]119[.]2:8443, 9090 CN 12-10-2022

1[.]116[.]39[.]144:8443 CN 16-10-2022

47[.]98[.]253[.]9:8443 CN 12-10-2022

101[.]43[.]225[.]48:8888, 8443 CN 12-10-2022

47[.]244[.]167[.]171:801 HK 16-10-2022

43[.]142[.]49[.]253:8000 CN 16-10-2022

23[.]224[.]42[.]15:8443 US 13-10-2022

47[.]242[.]4[.]140:18443 HK 14-10-2022

101[.]43[.]85[.]51:8888 CN 12-10-2022

212[.]192[.]246[.]16:8443 NL 12-10-2022

81[.]69[.]39[.]123:8443 CN 12-10-2022

1[.]12[.]235[.]247:8000, 4434 CN 12-10-2022

124[.]223[.]164[.]205:5001 CN 12-10-2022

101[.]33[.]214[.]18:8000 CN 12-10-2022

161[.]97[.]161[.]77:8443 DE 12-10-2022

47[.]243[.]73[.]233:8443 HK 13-10-2022

92[.]38[.]135[.]188:8443 KR 12-10-2022

5[.]42[.]199[.]46:8443 RU 12-10-2022

120[.]53[.]235[.]205:8888 CN 12-10-2022

154[.]202[.]59[.]95:8443 HK 12-10-2022

160[.]124[.]103[.]87:8443 HK 12-10-2022

159[.]75[.]33[.]64:81 CN 12-10-2022

124[.]222[.]192[.]92:2086, 2096 CN 12-10-2022

43[.]128[.]130[.]160:8443 KR 13-10-2022

106[.]13[.]95[.]3:8443 CN 12-10-2022

59[.]63[.]224[.]101:8443 CN 12-10-2022

47[.]111[.]7[.]76:8888 CN 12-10-2022

124[.]223[.]10[.]130:8082 CN 12-10-2022

101[.]35[.]47[.]93:8443 CN 12-10-2022

120[.]53[.]233[.]231:9999, 8888 CN 12-10-2022

114[.]118[.]5[.]103:8443 CN 12-10-2022

42[.]192[.]21[.]181:8443 CN 12-10-2022

122[.]112[.]221[.]253:8443 CN 13-10-2022

154[.]204[.]57[.]111:8443 HK 13-10-2022

154[.]202[.]59[.]41:8443 HK 12-10-2022

209[.]133[.]211[.]242:9999 US 12-10-2022

112[.]196[.]204[.]233:8888 KR 12-10-2022

103[.]108[.]107[.]231:8443 MM 13-10-2022

143[.]198[.]13[.]212:8443 US 12-10-2022

119[.]29[.]89[.]253:8443 CN 13-10-2022

82[.]157[.]182[.]245:8088 CN 16-10-2022

119[.]3[.]134[.]252:81 CN 13-10-2022

158[.]247[.]203[.]139:3389 KR 13-10-2022

121[.]36[.]192[.]30:8443 CN 12-10-2022

154[.]209[.]228[.]14:8443 US 13-10-2022

82[.]157[.]245[.]205:4433 CN 15-10-2022

139[.]155[.]81[.]10:8443 CN 12-10-2022

43[.]138[.]66[.]231:8443 CN 12-10-2022

101[.]200[.]49[.]219:8443 CN 12-10-2022

47[.]103[.]157[.]82:50000, 8000 CN 12-10-2022

47[.]92[.]97[.]171:8443 CN 12-10-2022

120[.]132[.]81[.]238:8443 CN 13-10-2022

114[.]115[.]205[.]206:8888 CN 12-10-2022

103[.]253[.]43[.]230:8443 HK 12-10-2022

1[.]15[.]74[.]201:8443 CN 12-10-2022

124[.]222[.]100[.]22:8888, 9090 CN 15-10-2022

43[.]143[.]175[.]188:2096 CN 12-10-2022

110[.]42[.]190[.]201:8888 CN 13-10-2022

82[.]157[.]144[.]204:9999 CN 12-10-2022

121[.]5[.]130[.]73:6666 CN 12-10-2022

192[.]236[.]193[.]209:53 NL 12-10-2022

193[.]233[.]253[.]156:88 RU 13-10-2022

8[.]218[.]29[.]247:2083, 2087 HK 12-10-2022

118[.]25[.]12[.]11:6666 CN 13-10-2022

42[.]192[.]54[.]106:8443, 2082 CN 12-10-2022

47[.]103[.]13[.]224:9999 CN 12-10-2022

121[.]196[.]200[.]127:9999 CN 13-10-2022

47[.]242[.]83[.]75:81 HK 12-10-2022

144[.]34[.]170[.]124:8888 US 12-10-2022

**********IOC END**********

Please Note: The Above IOCs are also available in CERT-In Threat Intelligence Platform.

Recommendations:

- - - - - - - - - - -- Recommend to monitor connection towards the mentioned IP addresses.

- - - - - - - - - - -- The list may include compromised IP resources as well. Blocking the IPs is solely the recipient responsibility after diligently verifying them without impacting the operations.

- - - - - - - - - - -

- - - - - - - -

- - - - -

- - ----------ALERTEND----------

CERT-In Threat Intel Team

[PGP KEY ID 0x797D4D74]

[Link:https://keyserver.pgp.com/vkd/SubmitSearch.event?SearchCriteria=0x797

D4D74]

-----BEGIN PGP SIGNATURE-----

Version: Encryption Desktop 10.4.2 (Build 10531)

Charset: utf-8

wsDVAwUBY04vZTASeOF5fU10AQpDkwwAsIueIS9dUF25Bvu+b56Kz4Tf/JoiOH1C

L5lKTGQtlUYkUbFlq47vvNUblGpibUNQkySHWCB428sLoknL0YtxQAVZPT4WOY9s

5HyfAThLNKGaU5XmJ4OzsSt0HdERq252FqzWSap4MtYPc5DGX3r6TaI/njy+ynWK

BEnUu9c9tGCAeCMCdTtVPmAX29hJbS17LEpcj2PvJgz8K2G8u6dDbVNyLwiIofmB

INTQCEmnZU7ebweQQVQXk3PXBjWKEED8/YaLXDUOvbc39MSUErS3mqrAPMOiyrYG

WHm6lVZMX3glDhCrUlSwLV8Bqpq5XRMxiGZ7jQxHXYwAnHDCVBIVeBKXJQVItqz/

gSyocagWcP3w1GH4Z7Ys0QLPajCHYZqBABI/NCi5+JkJZEpjcTcn3WjAGE/mMKhB

kGpS0LyJGl+O/UZBqH5dfOFOBUUXB/7hnjsEU8crCf+ZUIEk5K8K2FEKdJUF2LYx

TAYWb/tKvZLsw+Kf4zaEh5LyMtCr2NK/

=94mD

-----END PGP SIGNATURE-----