From: Mr SANI ABHILASH CERT IN <cmtx.certin@meity.gov.in>
To: alert <alert_reply@cert-in.org.in>
Date: 19 Oct 2022, 05:04:17 PM
Subject: [CMTX-P-102022752] COBALT STRIKE ALERT 31 (TLP:RED)
Reply Reply To All Fwd Fwd As Attachment

HTML content follows

="" color:="" #000000"="">
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

[CMTX-P-102022752] COBALT STRIKE ALERT 31 (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-102022742] COBALT STRIKE ALERT 30 (TLP:RED)19.10.2022

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
165[.]22[.]252[.]28:2121 SG 14-10-2022
8[.]210[.]123[.]189:4443 HK 12-10-2022
103[.]239[.]30[.]98:9999 HK 12-10-2022
101[.]43[.]210[.]42:8443 CN 13-10-2022
39[.]105[.]31[.]193:50052, 443, 80 CN 12-10-2022
101[.]42[.]168[.]218:8443, 8080 CN 14-10-2022
42[.]192[.]2[.]200:4444, 443 CN 13-10-2022
49[.]235[.]95[.]50:8443, 87 CN 13-10-2022
81[.]68[.]136[.]117:8443, 443 CN 12-10-2022
121[.]5[.]233[.]126:6666, 8001 CN 14-10-2022
124[.]222[.]244[.]249:4455, 443, 50000 CN 14-10-2022
23[.]224[.]152[.]139:4433 US 12-10-2022
78[.]153[.]130[.]152:80, 8443 AT 12-10-2022
173[.]82[.]135[.]18:4443 US 14-10-2022
42[.]192[.]77[.]34:5555 CN 12-10-2022
124[.]221[.]81[.]252:9999 CN 12-10-2022
23[.]224[.]152[.]139:4433, 443 US 12-10-2022
78[.]153[.]130[.]152:8443, 80 AT 12-10-2022
47[.]103[.]71[.]63:81 CN 12-10-2022
1[.]116[.]156[.]226:8098, 8787 CN 14-10-2022
120[.]24[.]64[.]98:8443, 443 CN 13-10-2022
47[.]103[.]71[.]63:81, 3000 CN 12-10-2022
45[.]76[.]154[.]17:8443 SG 12-10-2022
107[.]148[.]14[.]42:2083 HK 13-10-2022
106[.]55[.]149[.]152:8099 CN 14-10-2022
39[.]102[.]50[.]219:5555 CN 16-10-2022
121[.]199[.]166[.]58:8888 CN 14-10-2022
124[.]223[.]93[.]144:8001 CN 12-10-2022
124[.]222[.]166[.]30:19443 CN 13-10-2022
45[.]76[.]154[.]17:8443, 443 SG 12-10-2022
43[.]142[.]138[.]251:8000 CN 12-10-2022
114[.]116[.]101[.]84:85 CN 12-10-2022
43[.]143[.]170[.]177:8443 CN 12-10-2022
43[.]142[.]138[.]251:8000, 8090, 9000, 8080 CN 16-10-2022
114[.]116[.]101[.]84:85, 443 CN 12-10-2022
178[.]18[.]255[.]124:445 DE 11-10-2022

43[.]226[.]73[.]184:8443 CN 11-10-2022
74[.]119[.]193[.]147:8443 HK 11-10-2022
175[.]27[.]168[.]123:8443 CN 13-10-2022
1[.]15[.]174[.]134:8443 CN 13-10-2022
82[.]156[.]2[.]25:8443 CN 13-10-2022
152[.]136[.]96[.]44:44309, 9999 CN 11-10-2022
104[.]238[.]186[.]59:8443 GB 11-10-2022
202[.]95[.]15[.]23:2086, 8333 HK 13-10-2022
104[.]233[.]163[.]244:8443 JP 13-10-2022
124[.]221[.]107[.]73:8443 CN 13-10-2022
170[.]178[.]221[.]75:80, 443 US 18-10-2022
152[.]136[.]232[.]171:8870 CN 11-10-2022
101[.]200[.]121[.]103:8438 CN 11-10-2022
149[.]129[.]72[.]37:8443 HK 11-10-2022
175[.]27[.]168[.]123:8443, 443 CN 13-10-2022
82[.]156[.]2[.]25:8443, 443, 80, 4431 CN 13-10-2022
150[.]158[.]198[.]163:8033 CN 11-10-2022
23[.]224[.]70[.]230:4433 US 11-10-2022
23[.]106[.]160[.]152:443 US 18-10-2022
23[.]106[.]215[.]115:443 US 18-10-2022
1[.]117[.]73[.]197:8443 CN 13-10-2022
88[.]214[.]27[.]53:4433 DE 11-10-2022
45[.]147[.]228[.]185:443 DE 18-10-2022
114[.]132[.]244[.]72:8099 CN 11-10-2022
174[.]138[.]21[.]86:80, 443 SG 18-10-2022
180[.]215[.]254[.]207:443 HK 18-10-2022
104[.]131[.]5[.]230:4433 US 11-10-2022
162[.]14[.]66[.]133:9090 CN 14-10-2022
45[.]204[.]1[.]25:8001 HK 14-10-2022
43[.]134[.]230[.]170:8443 SG 13-10-2022
47[.]93[.]9[.]242:82 CN 14-10-2022
124[.]71[.]131[.]11:8443 CN 11-10-2022
23[.]106[.]215[.]213:443 US 18-10-2022
23[.]83[.]133[.]104:443 US 18-10-2022
45[.]136[.]14[.]131:4433 HK 14-10-2022
43[.]138[.]110[.]50:666 CN 13-10-2022
124[.]70[.]180[.]245:8443 CN 11-10-2022
43[.]134[.]2[.]182:4444 SG 18-10-2022
23[.]224[.]70[.]230:4433, 443 US 11-10-2022
1[.]117[.]73[.]197:8443, 80, 443 CN 13-10-2022
88[.]214[.]27[.]53:4433, 443 DE 11-10-2022
114[.]132[.]244[.]72:8099, 80 CN 11-10-2022
45[.]153[.]240[.]56:443 DE 18-10-2022
78[.]128[.]112[.]98:443 BG 18-10-2022
8[.]210[.]143[.]49:8080 HK 18-10-2022
104[.]131[.]5[.]230:4433, 80, 443 US 11-10-2022
162[.]14[.]66[.]133:9090, 80 CN 14-10-2022
43[.]134[.]230[.]170:8443, 5000 SG 13-10-2022
182[.]110[.]23[.]81:8443 CN 11-10-2022
162[.]14[.]103[.]171:9999 CN 11-10-2022
121[.]5[.]150[.]180:8099 CN 11-10-2022
150[.]158[.]45[.]254:8443 CN 13-10-2022
1[.]116[.]123[.]104:8443 CN 13-10-2022
106[.]52[.]197[.]95:6666 CN 13-10-2022
150[.]158[.]45[.]254:8443, 10443 CN 13-10-2022
216[.]83[.]57[.]210:3260 HK 14-10-2022
84[.]32[.]188[.]232:444 NL 11-10-2022
139[.]224[.]198[.]190:9999, 9443 CN 11-10-2022
84[.]32[.]188[.]232:444, 443 NL 11-10-2022
139[.]224[.]198[.]190:9999, 9443, 4567 CN 11-10-2022
47[.]75[.]108[.]68:2022 HK 13-10-2022
82[.]156[.]76[.]210:8001 CN 11-10-2022
175[.]24[.]33[.]207:6666 CN 11-10-2022
47[.]75[.]108[.]68:2022, 443 HK 13-10-2022

175[.]24[.]33[.]207:6666, 8080 CN 11-10-2022
121[.]5[.]147[.]81:2087 CN 14-10-2022
1[.]15[.]232[.]225:2222 CN 13-10-2022
143[.]244[.]154[.]197:443 US 18-10-2022
164[.]155[.]64[.]43:8081 HK 18-10-2022
164[.]155[.]95[.]159:81 HK 18-10-2022
1[.]15[.]232[.]225:2222, 443, 801 CN 13-10-2022
47[.]242[.]110[.]140:4433 HK 13-10-2022
108[.]62[.]118[.]136:443 US 18-10-2022
112[.]121[.]173[.]228:8880 HK 18-10-2022
119[.]91[.]233[.]239:7777, 9999 CN 18-10-2022
124[.]223[.]86[.]128:80 CN 18-10-2022
139[.]224[.]17[.]133:80 CN 18-10-2022
142[.]44[.]211[.]35:443 CA 18-10-2022
168[.]100[.]11[.]84:80 NL 18-10-2022
190[.]123[.]44[.]225:443, 8080 PA 18-10-2022
45[.]147[.]230[.]195:443 DE 18-10-2022
89[.]207[.]129[.]48:4433 NL 18-10-2022
124[.]222[.]25[.]63:65533 CN 14-10-2022
47[.]100[.]180[.]123:3004 CN 13-10-2022
120[.]48[.]101[.]89:1181 CN 14-10-2022
182[.]108[.]63[.]24:8443 CN 13-10-2022

**********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

wsDVAwUBY0/eEzASeOF5fU10AQqx6QwAiytSYMdunCesiJMjUIfJmNw7IKNvm3wn
8pyT7pHq76u4RWXkrFAm75obrJn0WszPYXk29WzfkHpfxQUrdfiUPnjSPSzzp7nX
QGX8S84yYjdrI5b6UD8+wAj6DtFCIIxfmxLw1TVI2ravCjW5WA1uWfXvA7Fpjyrf
f8OVmZecDE+QIwyL74mnDod/pe7+Px95zv2zR1rGH7v4aRunO6lnEAWQHOHr64cD
fhANrqad8GQ1WibRwU8164plAggZnXVcJamvAYiOdiIsFeachvuYZUKos4uoZox4
pfSGVbqpx3ci3U0ej9ZPJ+kRYoPTFi6WZ/x1bffgxs3A7QwNsG2p+utBlZ4IMVve
JXBA3FsGj5oNKdy0VQK5DXTxW8eEwcYqcvpOqZYkF37FdSU5pv2XxQwtsb8xZ6oB
KTN1mAZep2cexsgvoT0laIAT0L47fsUBlz9E5Hg/CNWqu7aT5Pz92/+0VC4er+V8
ITAhdiV1etQi/zfPHQdl5a2mv+QhLr7x
=z2yi
-----END PGP SIGNATURE-----