From: Mr SANI ABHILASH CERT IN <cmtx.certin@meity.gov.in>
Sent: 19 October 2022 09:41
To: alert <alert_reply@cert-in.org.in>
Subject: [CMTX-P-102022742] COBALT STRIKE ALERT 30 (TLP:RED)

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

Hash: SHA512

[CMTX-P-102022742] COBALT STRIKE ALERT 30 (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-102022732] COBALT STRIKE ALERT 29 (TLP:RED)18.10.2022

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[.]210[.]154[.]177:8443

HK 13-10-2022

43[.]138[.]27[.]53:8888

CN 14-10-2022

47[.]100[.]37[.]216:8888

CN 13-10-2022

123[.]60[.]47[.]130:6666

CN 15-10-2022

118[.]25[.]158[.]13:8088

CN 13-10-2022

42[.]192[.]155[.]199:6666

CN 13-10-2022

114[.]115[.]178[.]24:6666

CN 14-10-2022

91[.]208[.]236[.]103:8088

HK 13-10-2022

92[.]255[.]85[.]143:81, 83

RU 13-10-2022

101[.]200[.]233[.]32:8443

CN 13-10-2022

114[.]116[.]20[.]5:6668

CN 14-10-2022

150[.]158[.]78[.]254:8443

CN 13-10-2022

82[.]157[.]69[.]100:2083

CN 14-10-2022

116[.]62[.]122[.]85:6666

CN 13-10-2022

146[.]56[.]109[.]12:6666

KR 14-10-2022

101[.]35[.]151[.]156:8443

CN 13-10-2022

39[.]96[.]57[.]233:8443

CN 13-10-2022

124[.]221[.]195[.]114:8888

CN 13-10-2022

103[.]6[.]169[.]44:81

SG 13-10-2022

45[.]32[.]74[.]18:8443

US 13-10-2022

79[.]137[.]199[.]143:8443

NL 16-10-2022

104[.]238[.]148[.]4:8888

JP 13-10-2022

106[.]12[.]108[.]122:6666

CN 13-10-2022

152[.]67[.]117[.]125:8000

AU 13-10-2022

118[.]195[.]227[.]9:81

CN 13-10-2022

101[.]34[.]42[.]189:8888

CN 13-10-2022

159[.]75[.]98[.]80:8443

CN 13-10-2022

61[.]177[.]56[.]27:8888

CN 13-10-2022

43[.]138[.]243[.]184:8000

CN 13-10-2022

39[.]105[.]110[.]247:8099

CN 12-10-2022

45[.]89[.]103[.]240:8888

US 14-10-2022

124[.]223[.]204[.]198:88, 5555

CN 13-10-2022

47[.]104[.]212[.]159:8888

CN 13-10-2022

104[.]243[.]21[.]60:8888

US 13-10-2022

43[.]154[.]14[.]120:60001

HK 14-10-2022

120[.]24[.]213[.]238:8888

CN 13-10-2022

42[.]193[.]108[.]39:8023

CN 13-10-2022

175[.]178[.]217[.]18:9999

CN 13-10-2022

8[.]140[.]37[.]238:9999

CN 13-10-2022

114[.]115[.]235[.]249:81

CN 13-10-2022

124[.]222[.]131[.]194:9999, 5555

CN 13-10-2022

114[.]116[.]40[.]60:666

CN 14-10-2022

103[.]6[.]169[.]28:81

SG 13-10-2022

43[.]142[.]181[.]122:8888

CN 13-10-2022

1[.]116[.]4[.]48:8443

CN 13-10-2022

121[.]36[.]148[.]12:4433, 3389

CN 12-10-2022

1[.]117[.]89[.]216:9010, 9009

CN 14-10-2022

120[.]24[.]63[.]15:8443

CN 13-10-2022

211[.]149[.]234[.]225:8088

CN 14-10-2022

124[.]221[.]184[.]239:18080

CN 14-10-2022

103[.]45[.]69[.]222:8888

HK 13-10-2022

114[.]115[.]141[.]15:4431

CN 13-10-2022

45[.]32[.]64[.]150:8000, 8443, 80

US 13-10-2022

43[.]138[.]150[.]21:8443, 80, 443

CN 13-10-2022

5[.]42[.]199[.]46:8443, 53

RU 13-10-2022

120[.]53[.]235[.]205:8888, 443, 80

CN 13-10-2022

160[.]124[.]103[.]87:8443, 443

HK 13-10-2022

159[.]75[.]33[.]64:81, 80, 443

CN 13-10-2022

43[.]128[.]130[.]160:8443, 443

KR 13-10-2022

106[.]13[.]95[.]3:8443, 443

CN 13-10-2022

59[.]63[.]224[.]101:8443, 443

CN 13-10-2022

47[.]111[.]7[.]76:8888, 443

CN 13-10-2022

124[.]223[.]10[.]130:8082, 443, 8806

CN 13-10-2022

101[.]35[.]47[.]93:8443, 80, 443

CN 13-10-2022

120[.]53[.]233[.]231:9999, 8888, 443, 80

CN 13-10-2022

114[.]118[.]5[.]103:8443, 443

CN 13-10-2022

42[.]192[.]21[.]181:8443, 443, 80

CN 13-10-2022

154[.]204[.]57[.]111:8443, 443

HK 13-10-2022

209[.]133[.]211[.]242:9999, 443

US 13-10-2022

112[.]196[.]204[.]233:8888, 443, 80

KR 13-10-2022

119[.]3[.]134[.]252:81, 443

CN 13-10-2022

47[.]92[.]97[.]171:8443, 443

CN 13-10-2022

1[.]15[.]74[.]201:8443, 80, 443, 8080, 9443

CN 12-10-2022

42[.]192[.]54[.]106:8443, 2082, 80, 2083

CN 13-10-2022

47[.]100[.]37[.]216:8888, 80

CN 13-10-2022

92[.]255[.]85[.]143:81, 83, 84

RU 13-10-2022

101[.]200[.]233[.]32:8443, 9998

CN 13-10-2022

159[.]75[.]98[.]80:8443, 443

CN 13-10-2022

124[.]223[.]204[.]198:88, 5555, 80

CN 13-10-2022

43[.]142[.]181[.]122:8888, 80

CN 13-10-2022

1[.]117[.]89[.]216:9010, 9009, 80

CN 14-10-2022

119[.]91[.]22[.]81:8443

CN 14-10-2022

39[.]105[.]31[.]193:50052

CN 12-10-2022

43[.]138[.]73[.]164:8443

CN 12-10-2022

101[.]42[.]168[.]218:8443

CN 14-10-2022

42[.]192[.]2[.]200:4444

CN 13-10-2022

218[.]29[.]106[.]204:8000

CN 14-10-2022

49[.]235[.]95[.]50:8443

CN 13-10-2022

118[.]195[.]144[.]147:8090, 4443

CN 12-10-2022

81[.]68[.]136[.]117:8443

CN 12-10-2022

121[.]5[.]233[.]126:6666

CN 14-10-2022

119[.]91[.]205[.]225:8443

CN 13-10-2022

106[.]75[.]230[.]14:8443

CN 12-10-2022

124[.]222[.]47[.]89:49999

CN 14-10-2022

115[.]159[.]50[.]67:60001

CN 14-10-2022

139[.]196[.]110[.]126:6666

CN 13-10-2022

124[.]222[.]248[.]86:22222

CN 14-10-2022

139[.]224[.]227[.]232:9999

CN 13-10-2022

1[.]117[.]247[.]128:9000

CN 12-10-2022

124[.]222[.]244[.]249:4455

CN 14-10-2022

43[.]143[.]1[.]35:5555

CN 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

wsDVAwUBY0931jASeOF5fU10AQo6WgwAiKGYfBSWpjF0VsGVzkqQB/uvovbGCaVk

qcmRcpVBgpE+Hds64rcJu5EMzPubd9apu5TwkDmbw28lnWOvjyhqApXEcHaw8GbK

rNYjPnx45PUH78hofzVAyqRWq/8cP/CqImJyO7GjA9QllNgYyz+OmGEUxZXpsSsT

LZQq26sFWhz6AAv5/CllERLoKjodHDEyklMccIrRnfBRQd8T9nGWXxvid9zq0c9J

h/cQl26OzQzJLEnV7t0L+fLUlBaFHZtOsgD3csy7gaQg+Smmmu2y2IxpsOibhrFF

wpPfV1IrbI2w4tbGgMrX6FG0jHldJvRpl/uvDiKDt3U9Vnlqewa2iWhQTpbOi5h3

tp+Pl5EWQwiDcxGgpJGFDn+neYGyFsjN8fqCg4YHL5L4hOMrWAutYW3+VMsJ2tYh

F4GuCzO0HYwQ3XBbsX6EcbNkWO4X47czBtXXHmhStnbyyxwsKbPTNvnbvapaUUHw

iq1zXsiPJ26GjzUp2NfeWN3yF0LRe5dY

=ZXej

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