From: Mr SANI ABHILASH CERT IN <cmtx.certin@meity.gov.in>
Sent: 17 October 2022 11:05
To: alert reply <alert_reply@cert-in.org.in>
Subject: [CMTX-P-102022569] COBALT STRIKE ALERT 26 - TLP-RED [ONLY FOR RECIPIENT ORGANIZATIONS]

CAUTION: This Email has been sent from outside the Organization. Unless you trust the sender, Don't click links or open attachments as it may be a Phishing email, which can steal your Information and compromise your Computer.

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

Hash: SHA256

[CMTX-P-102022569] COBALT STRIKE ALERT 26 - TLP-RED [ONLY FOR RECIPIENT ORGANIZATIONS]

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-102022692] COBALT SRTKE ALERT 25 - TLP-RED [ONLY FOR RECIPIENT ORGANIZATIONS] DATED 14.10.2022

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's Country

Ports Lats Seen

119[.]45[.]238[.]142 CN

443,

16-Oct-22

107[.]148[.]49[.]253

HK

443,

13-Oct-22

139[.]9[.]3[.]92

CN

8443,

16-Oct-22

101[.]201[.]254[.]70

CN

443,

16-Oct-22

121[.]199[.]57[.]9

CN

443,

16-Oct-22

1[.]15[.]113[.]198

CN

443,

16-Oct-22

47[.]114[.]77[.]60

CN

8443,

6-Oct-22

35[.]166[.]32[.]190

US

443,

13-Oct-22

147[.]78[.]47[.]229

NL

443,

13-Oct-22

49[.]233[.]62[.]180

CN

8443,

16-Oct-22

52[.]231[.]11[.]154

KR

443,

16-Oct-22

39[.]101[.]65[.]233

CN

443,

15-Oct-22

103[.]253[.]43[.]84

HK

443,

15-Oct-22

121[.]89[.]233[.]124

CN

443,

15-Oct-22

103[.]27[.]109[.]249

HK

443,

15-Oct-22

150[.]109[.]151[.]11 HK

443,

15-Oct-22

39[.]107[.]109[.]123 CN

443,

9-Oct-22

123[.]56[.]161[.]138

CN

443,

13-Oct-22

18[.]218[.]215[.]185

US

443,

13-Oct-22

121[.]5[.]165[.]96

CN

443,

13-Oct-22

198[.]211[.]48[.]141

US

8443,

15-Oct-22

8[.]134[.]110[.]105

CN

43,

15-Oct-22

119[.]29[.]154[.]61

CN

443,

14-Oct-22

62[.]182[.]86[.]225

UA

443,

14-Oct-22

8[.]140[.]12[.]176

CN

443,

14-Oct-22

182[.]61[.]150[.]1

CN

8443,

14-Oct-22

160[.]20[.]145[.]111

DE

8443,82,14-Oct-22

***********************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
CERT-In

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

iQGzBAEBCAAdFiEE18QxKhH3psk73oSyMBJ44Xl9TXQFAmNM4J0ACgkQMBJ44Xl9
TXRpTQv/TWtsm48EU6xCkqCuRRcLyF90oveMcbPalM8c6d2VSkp3W1BFfkGO9u0g
IyYrwK66fD6HNNCDR9qp9SqCy0JyN06eufeBKS7WQn7tFVYQ5ou/lKm/ur2GwArr
zJ2el7tr94MvEX33iGceL9qA27hj/bpgm7gIv2+fseG3C0NvDr0FD+MdLmZjnNkU
H3A6Xp64xhZu/gAemK+0ydVC6jcJeXA5MFrZvUPGpoKP5FP/UBHuJebyPrMoszCh

JLnL2/bWMBqRIf09S3pLH4e32igpKQjh/KSbzIue7OTMEcL8bJKbBT31zwZqSYqG

DzONoS6EF2uVpV4TmScUzf4KP9o1f6AalQY9g/kVn1kVoIDPP4odd+QQhVqJwAPY

y3Z3FxnJx9X9aUDg48jfuzOd95Xjg6FdTABN+hHcuzTCEKFPW5n2dxPkwKKhu1Zb

OCEReYe5SkA3Z7DiYQ3tQYw86E1BtjBJTgh/lnduTULMN6A9qIzz4QEpOZ1M0pPE

tRojCiGP

=fZH5

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