From: Mr SANI ABHILASH CERT IN <cmtx.certin@meity.gov.in>
Sent: 19 October 2022 12:41
To: alert reply <alert_reply@cert-in.org.in>
Subject: [CMTX-P102022426] APT41 recent activity, TLP: AMBER

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

Hash: SHA256

[CMTX-P102022426] APT41 recent activity, TLP: AMBER

META INFORMATION

Confidence- High

Risk- High

TLP: AMBER

Sector Targeted: Government

- ----------

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.

- ----------

ALERT BRIEF:

Aliases: Winnti Group, Barium, Bronze Atlas, Axiom, Blackfly and Wicked Panda

It has been reported that Chinese state-sponsored espionage group APT 41 is reportedly continuing stealing of proprietary information

from prolific entities under Operation CuckooBees. Recent cluster of activity tracked reflects that the notorious threat group is using

a new version of Spyder Loader, a sophisticated modular backdoor with capabilities to load AES-encrypted blobs to create wlbsctrl.dll a next-stage payload, implements ChaCha20 encryption algorithm and to escape detection cleans up created artifacts, overwrites the content of the dropped wlbsctrl.dll file before its deletion. Once gained access to the

target network, Winnti also deployed other post-exploitation tools that include Mimikatz and a trojanized zlib DLL module that can receive commands from a remote server or load arbitrary payloads.

- --- Additionally identified a new backdoor named DBoxAgent delivered via an ISO image that uses Dropbox as command and control server

to help distribute several payloads, including the KeyPlug malware.

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

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

HASHES

SHA256

904189ef4cec6ad4603918e63e0b2e477cb11503315ad3822437ee75920793f4

8dc38dcd26c62e93c81e7f4408b83ec4d2adfe9a06cfebef0de945b338ec3c8b

a9d967243678d31ba5027d1802fbc1606c10b7743d6d6851eddc32b9281eb2f6

be7f7955a296874f238da6ec5b63ffec995429ee1833e7fbcc294e36eeacbca4

DOMAIN

dash[.]lcmbk[.]com

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

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

RECOMMENDATIONS

- - - - Majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense.

- - - - Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints. Perform regular backup of all the critical information to minimize the loss.

- - - - Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent to prevent e-mail spoofing. This will prevent malicious mails to reach your corporate mailboxes.

- - - - Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header). Block attachments of file types: [exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf]. Ensure to scan all software downloaded from the Internet prior to executing.

- - - - Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known. Monitor users' web browsing habits; restrict access to sites with unfavourable content.

- - - - Monitor Connection attempts towards the listed Domains. Blocking the Domain is solely the recipient responsibility after diligently verifying them without impacting the operations.

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

CERT-IN Threat Intel Team

CERT-In

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

iQGzBAEBCAAdFiEE18QxKhH3psk73oSyMBJ44Xl9TXQFAmNPoe0ACgkQMBJ44Xl9

TXRCpwwAglD50ftuou8IuRmS6uz1MO3UfpR/HddajxGQAlmraHiqfhhg2MnpAGnm

bQNlF9xOmKdUOe+Qp0WtehXcojTrT44ZyHbsXZKidrHqQdGAk3p73lRo+fxrKNcg

DVMykQhnIMDK6YzXSUlm0rBmzaGQSRWSz1vFUjyZsogNLQSp3oNz07VSQBz8kbyA

d4kAlEFyekL5M8fcJoV8CVRZGbRI1aBTCHzV45PQtevE56f/6ekSGKgVZK45qR5d

Qk8GBDTQuC64TtttNydXlo6pXAUaUim3GY8kgQDRuXiX/DE943o8niBmmhVhwt0G

Rodjuuvi18a+ao91CCPrcBwJ30l3MyInJdEh6EXGYtNsmgaSjSR+lvcAH4DGGlQl

/ZpRo9oFv8Lv8XKM9iW2YY5oDQJ5MfWDg8xdCoisor1jmrRdGGt0V6LHrmmmLZDk

I/v17VBxstYha+NtmNeSrzbkN3X2PSum7opOdFEU8oYfZwTKNySgh0S5ZauV/DkK

a4JzZJcP

=nd9L

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