Department of Supervision, Central Office
Cyber Security & IT Risk (CSITE) Group

CONFIDENTIAL

Advisory 2_COVID-19 **Dated: March 23, 2020**

Supervised Entities (SEs) may please refer to the general guidance prescribed vide Advisory_COVID-19 dated March 13, 2020. In view of recent developments, it may be necessary for SEs to work with minimal strength and make provisions for key personnel to work from home/remote location. In doing so, SEs are advised to take necessary precautions to ensure that they meet their business continuity and cyber security objectives including the following:

i. Confidential/ sensitive data including customer data must be secured at all times. SEs may regulate the use of unconventional communication channels (such as mobile messaging applications) for official communication, considering the attendant data leak implications.
ii. All access to employees/ third-party personnel to the bank's IT systems must be secure.
iii. Detective systems/ mechanisms such as log monitoring/ Security Operations Centre, fraud risk (transaction) monitoring, performance monitoring, etc. must operate at the highest level of capabilities necessary to detect and alert abnormal events/ behaviour.
iv. Arrangements may be made to ensure incident response mechanisms possess adequate redundant capabilities by putting in place standby (even if off-site) incident response teams.
v. SEs may ensure that digital banking channels are adequately equipped to handle any increase in transaction volumes.
vi. Customers shall be adequately sensitised to exercise vigilance against social engineering attempts, particularly while undertaking digital banking transactions.

Securing Payment Ecosystem

vii. With reference to our earlier instructions on securing the payment ecosystem, SEs are advised to monitor all payment transactions, especially cross border transactions.

viii. SEs are urged to ensure that reconciliation process is robust across all payment systems and channels.

ix. In this connection, a reference is also invited to NPCI Advisory NPCI/2019-20/RMD 231 dated February 10, 2020 (addressed to all members of Rupay and NFS). SEs are advised to put in place necessary measures, as applicable, for all the cards issued.

CERT-In Threat Intel

x. Based on the threat intelligence received from CERT-In, it is gathered that threat actors are leveraging the COVID-19 pandemic for their own notorious gains. Details are given in the **Annex**.

xi. Many SEs would be already subscribing to the threat intelligence from Cert-In. SEs that are yet to subscribe to the threat intelligence from CERT-In are encouraged to subscribe directly. They may contact CERT-In on incident@cert-in.org.in for the same.

xii. SEs may take note of the TLP coding of the threat intelligence and use the content with strict confidentiality for securing their environment.

xiii. Some of the best practice and recommendations are:

a) The 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 defence.

b) Monitor Connection attempts towards the listed domains. The list may include compromised domains /IP resources as well. Blocking the domains/IPs is solely

the recipient responsibility after diligently verifying them without impacting the operations.

c) Allow remote access to the organization's network strictly with multi-factor authentication.

d) Systems having antivirus and a malware protection program on it and making sure they are always up to date with latest signatures.

e) Administrators applying strict application whitelisting, blocking unused ports, turning off unused services, and monitoring outgoing traffic to prevent infections from occurring.

f) Checking all services and devices for remote access for updates of firmware and security patches. Internet-facing open ports of remote-control services are a key target for attacks.

****

Annex

*************CERT-In –THREAT Intel********************
(TLP:Amber)

Onset of Coronavirus Themed Attacks: End of February 2020

Tactics and Attack Procedures Involved:

Strategies to lure victims the threat actors devise following new strategies to target victims with scams or malware campaigns:

- Using promotional codes
- Coronavirus Maps distributing instances of AZORult info stealer
- 'COVID19' as discount codes used by different hacking groups to promote their goods (malicious malware or exploit tools) for financial gain being sold over dark net

Malware Families Related to Covid-19:

- - AGENT TESLA
- - TRICKBOT
- - LOKIBOT
- - TRICKYMOUSE
- - VICIOUS PANDA CAMPAIGN
- - AZORULT
- - CRIMSON RAT
- - COVIDLOCK

A list of reported IOC's is listed for your perusal and action.

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

URLs:

hxxps://healing-yui223.com/cd[.]php
hxxps://www.schooluniformtrading[.]com[.]au/cdcgov/files/
hxxps://onthefx[.]com/cd[.]php
hxxps://urbanandruraldesign[.]com[.]au/cdcgov/files

hxxps://gocycle[.]com[.]au/cdcgov/files/
hxxps://185[.]234.73.125/wMB03o/Wx9u79.php
hxxps://45.128.134.14/C821al/vc2Tmy.php?
hxxp://198.23.200[.]241/~power13/.xoiaspxo/fre.php

IPs:

150[.]95[.]52[.]104
118[.]127[.]3[.]247
153[.]120[.]181[.]196
112[.]140[.]180[.]26
13[.]239[.]26[.]132
23[.]19[.]227[.]235
45[.]128[.]134[.]14
198[.]23[.]200[.]241
123[.]161[.]61[.]55
145[.]239[.]23[.]7
192[.]35[.]177[.]64
95[.]179[.]242[.]6
95[.]179[.]242[.]27
199[.]247[.]25[.]102
95[.]179[.]210[.]61
95[.]179[.]156[.]97
107[.]175[.]64[.]209
64[.]188[.]25[.]205

HASHES:

f92fecc6e4656652d66d1e63f29de8bfc09ea6537cf2c4dd01579dc909ba0113
3461B78384C000E3396589280A34D871C1DE3AE266334412202D4A6A85D02439
906eff4ac2f5244a59cc5e318469f2894f8ced406f1e0e48e964f90d1ff9fd88
1db31ada5f1ac2411ef33790244343946b741cd603745257a4612c5d2e6a4052
9aea43b22f214228caf4fc714f426c0a140b7dd70b010bf3778cd1c0ec440851
1545401f661f9326f5c604e1a025e811079ba4eace9d3830a05c5e4aa666803e
62dd16724874e0b05257118fb06427a6aeb839602bce52e6a139dc379f538bed
09400e30105b10cd484a2159e8496accd779045ac6775b351b80949a54e772df
5b12f8d817b5f98eb51ef675d5f31d3d1e34bf06befba424f08a5b28ce98d45a
3b701eac4e3a73aec109120c97102c17edf88a20d1883dd5eef6db60d52b8d92
d7f15f750cceeb9e28e412f278949f183f98aeb65fe99731b2340c8f1c008465
5187c9a84f5e69ba4b08538c3f5e7432e7b45ac84dec456ea07325ff5e94319a
ddb24e0a38ba9194fe299e351e54facb2cca9e6011db2f5242210284df91f900

c51658ed15a09e9d8759c9fbf24665d6f0101a19a2a147e06d58571d05266d0a
238fa49ed966cb746bffee3e7ca95b4a9db3bb0f897b8fd8ae560f9080749a82
e9621840e1bfaf16eaee37e2d1e9d1f0032158a09e638eaebff6d8626d47c95a
80392bebe21245128e3353eec7f499bdc5550e67501eceebf21985644d146768
215c72df44fe8e564d24f4d9930c27409e7f76e2045c67940cdcecdbdbd3b04f
69724a9bd8033bd16647bc9aea41d5fe9fb7f7a83c5d6fbfb439d21b7b9f53f6
679a8519587909f655bacea438168cbb4c03434aede9913d9a3a637c55a0eae7
9e12094c15f59d68ad17e5ed42ebb85e5b41f4258823b7b5c7472bdff21e6cee
e9766b6129d9e1d59b92c4313d704e8cdc1a9b38905021efcac334cdd451e617
1c98a36229b878bae15985c1ae0ff96e42f36fa06359323f205e18431d780a3b
c322d10ef3aa532d4625f1c2589eae0f723208db37a7c7e81e4f07e36c3a537e
3c756d761e89a0ea1216e2b7e57250ac76a80d5fe4f072e3b4b372e609ece74e
2a42f500d019a64970e1c63d48eefa27727f80fe0a5b13625e0e72a6ec98b968
751155c42e01837f0b17e3b8615be2a9189c997a
dde7dd81eb9527b7ef99ebeefa821b11581b98e0
fc9c38718e4d2c75a8ba894352fa2b3c9348c3d7
601a08e77ccb83ffcd4a3914286bb00e9b192cd6
27a029c864bb39910304d7ff2ca1396f22aa32a2
8b121bc5bd9382dfdf1431987a5131576321aefb
bf9ef96b9dc8bdbc6996491d8167a8e1e63283fe
fcf75e7cad45099bf977fe719a8a5fc245bd66b8
0bedd80bf62417760d25ce87dea0ce9a084c163c
5eee7a65ae5b5171bf29c329683aacc7eb99ee0c
3900054580bd4155b4b72ccf7144c6188987cd31
e7826f5d9a9b08e758224ef34e2212d7a8f1b728
a93ae61ce57db88be52593fc3f1565a442c34679
36e302e6751cc1a141d3a243ca19ec74bec9226a
080baf77c96ee71131b8ce4b057c126686c0c696
c945c9f4a56fd1057cac66fbc8b3e021974b1ec6
2426f9db2d962a444391aa3ddf75882faad0b67c
238a1d2be44b684f5fe848081ba4c3e6ff821917
05adf4a08f16776ee0b1c271713a7880
0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010
876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656
20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a
b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748

DOMAINS:

Postmaster[@]mallinckrodt[.]xyz
brentpaul403[@]yandex[.]ru
cdc-gov[.]org

cdcgov[.]org
insiderppe[.]cloudapp.net
kbfvzoboss.bid/alien/fre.php
cloud-security.ggpht[.]ml
dw.adyboh[.]com
wy.adyboh[.]com
feb.kkooppt[.]com
compdate.my03[.]com
jocoly.esvnpe[.]com
bmy.hqoohoa[.]com
bur.vueleslie[.]com
wind.windmilldrops[.]com

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