Government of India
National Critical Information Infrastructure Protection Centre
(A Unit of NTRO)

Date: 25 Nov 2019

Cyber Security Advisory: Phising Campaingn in CII

This data is to be considered as **TLP:AMBER**

Our trusted partner reported that, there is possible phishing campaign targeting Government Sector. Phishing is the fraudulent attempt to obtain usernames, passwords and other sensitive information by disguising as a trustworthy entity in an electronic communication Typically carried out by email spoofing or instant messaging.

IOCs :

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Suspected CnCs

203.119.214.124
CnCs found under this IP are as follows-
203.119.214.125
203.119.215.106
203.119.244.125
203.119.244.124
203.119.207.252
203.119.214.124
203.119.207.251
106.11.248.2
140.205.61.87
140.205.248.8
104.192.110.203
203.119.207.252
203.119.214.125
192.150.16.117
192.150.19.42
103.21.58.60

URL
[http://ns.adobe.com/xap/1.0/]
[http://ns.adobe.com/xap/1.0/]
[http://ns.adobe.com/xap/1.0/]
[http://ns.adobe.com/xap/1.0/]
[https://dhinakaransilkhouse.com/pictures/download.php]

filename=TT566842EFERYTE0_56790_usd.vbs;
MD5 94cfc6ba75d5681940502a103eab99be
SHA-1 2ddc811f223454fcd3149c5bee631bf27f38d717
SHA-256 633fd5fb253f7578a6c582f3402b9a357d5a109c34946e8234671b185a892db1
SSDEEP 6144:KyKwEiEytZ5oSk2G4F0FxLUfJnI+98JaKz:K7wEGtZAFxWn8zz
File type PDF Magic PDF document, version 1.4

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430