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

Date: 28 Nov 2019

Cyber Security Advisory: APT Campaign

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

Our trusted partner has reported about an APT (Advanced Persistent Threat) campaign using phishing mails which carry malicious documents in the form of Doc, excel etc. The IoC's used by the threat actor behind this campaign is listed for your side.

IoCs :

IP/Domain
212.114.52.148
159.89.104.38
Live[.]supportoffline.pro
work-onine[.]info
en-content[.]com
play.funbook[.]pw
matissues[.]com
new.transportfun[.]pw

Hashes
6FF933099D61994FAB74DE4425D5ADA9
8E5B5F002BA6B04C75A7D5CEAA133569
AC060C11A52AEAF43A652EDC7AF2F725
0980896DBC627D2B2C8A47D75030CA0A
2642BE838B156DD1022DBD28F845E754
5885975A44ADF2E1ECCAB9399D00F2F1
402D0190AD9E12B2D3D1D8E564A563A8
E3159CC89A0AD8674048F02704E30D75
E2EBF241B54A5778B6DEF0E117E30714
9BCB3A443141416A3C57043BEE45EB11
81E766F61AB88BEC3FFCB53B817E1C51
20A199106999E018CCE1E283CA130241
0916D53F6BAD296B4B2DD27AEC4F5090
2D38A46D8A41EDC564E0826454C473C0
2B807B19474B46D0A5AB7BE8DFF26F6A
A737EF0FD22F2D98390320F626278349
30AAFF714CD0B07C35F567351AC6FF78
8F5D8A749B2C8BC9540E97F58BF05E21
0031498159AD6D526388EFE33045ED9E
4D8CA2D2AC2E70E1D57930DF0ECDDDAD
5D5116A96F7F2B2602ED9875F0F32DDF
9D479CEC86EA919694DAB765BBA9ABBD
9289D75F3386EC68B00CF433C812EB24
DE831BAB9684D35A5D5A1A379258CBC8
BEEB9E95B503B64FE8B57323A825CDB3
8FA0B9D8D0F9B794F3797C3EFDC106B5
0FC45004CF8D0A9941EB7F258AE342BB
2580426FA60CF63B954DDFFBEEEA812C
2EC9B8DD485AAE652EE388C081A03EF7
CA287C1C9AAA92102948ED92167EDC08
450252CD32A93054E793448B0592AD47
03B82F30DA08A283952C7D4A94976FCE
307434752D8187B94250CAB6C672764A
4DF1C80A43579650D3BFBA70BB0606C9
4FAEFD068173FFFA327223FD87E50FBB
3319F96FD20CBAC8B30BC55314C38AB5
0108A194E11A2D871F5571108087C05D
F3C25854EF4AA0439A4D67C59377A9ED
1AC48BEF4B90172FD8A6BEA01868428B
79D301C8C50F0FD47C5AD2439C118ECE
0606FC577BFA6766F5A75FD01F1AA81B
1505F2916E26893DF1705CEE58B15471
B8E5E01DD38A9BB04CCA8D3BFC9C7330
112D52594D2D981A2DB9BB5B0064EB5A
55F60E5420AB732B69E222FE6AD3F120
F1A94E75FFD6C27250D8FEADC2B19F53

A23A1E85D5B93FEBFEDEC5F114DC540A
56F0E9FF6DB534BB40499D74654B5C0B
B94EAC3BAA605D61BEB96D50E1D3747F
70B375214B30D4BC958F6DD12565A989
AE8FE7E35895608F630718632F1DB3E6
6992176E87E96A389DCA1CBE54D7E5A2
6ADE50F0C528129A8EE61A66AC23EA2D
338EAB92AB6CDE94D35267C993095FD4
7C95F63CB8A084ECE44D038453B88D5E
0DB8A723E8E8782EA93547D1C6D06D5E
561ADC55D8A9BF9D6966F7DD234D1E20
C9E58A0DACC8AAD78787E7127C366451
71B63F2539CACA874B4598DD83E02DA7
1ACEB72B9AB3C9E5F7DB5FF03C52A874
22CA3E5DACF65585C9A22ADB62B7DA86
EECC8A259DC8E1FC268FA598D6282AD7
1961EB941697113183567DCC8EA2137C
DFE36B2E312DCD78AFD93C5841C90866

Recommendations :

- Monitor Connection attempts towards the listed domains /IPs. The list may include compromised domains /IP resources as well.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution. Majority of the infection vectors are primarily introduced via phishing emails.
- Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Ensure that only signed script will execute in Power shell and practice “least privilege” of access.
- Enabled code signing feature for all types of users in Power script so that only signed script will execute in Power shell and practice “least privilege” of access.
- Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints.
- Segment the critical networks and vulnerable or hard to secure systems from the rest of the network intelligently to restrict the lateral movement.

Reference: CERT-In

Disclaimer:

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