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

Date: 29 Nov 2019

Cyber Security Advisory: APT MUSTANG PANDA

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

Our trusted partner reported an ongoing malware campaign called “Mustang Panda” targeting public and private sectors. Attackers improved their campaign activities with unique Tactics, Techniques, and Procedures (TTPs). The TTPs in this campaign consist of the following:

- Use of zip file that contains a “.lnk” file.
- Utilization of double extension trick (sample.doc.lnk) to convince users to open the file.
- HTA (HTML Application) with VBScript embedded in the “.lnk” file
- VBScript drops payloads and opens a decoy document or PDF to the user.
- Usage of PlugX and Cobalt Strike payloads

Analyst’s Notes:
The “.lnk” files being utilized by Mustang Panda typically contain an embedded HTA script that, once executed, will drop and open the decoy document while the malicious activity of the payload runs in the background.

IoCs :

IP/Domain:
Web[.]officeproduces[.]com:8080
Download[.]officeproduces[.]com:443
update[.]olk4[.]com:53
hxxp://144[.]202[.]54[.]86/vkt2
hxxp://144[.]202[.]54[.]86/download/Mau2[.]hta
hxxp://144[.]202[.]54[.]86/download/Mau%20cam%20ket%20danh%20cho%20Chua%20D
ang%20vien[.]docx
hxxp://airdndvn[.]com/6CDC9F833C87FB661DBB9339
hxxp://www[.]wbemsystem[.]com/B2FC407BB86E8219/397A4853
web[.]officeproduces[.]com:8000/update?wd=1b1fe9aa
154[.]221[.]24[.]47/HaQ3
adobephotostage[.]com
olk4[.]com
apple-net[.]com
wbemsystem[.]com
yahoorealtors[.]com
infosecvn[.]com
airdndvn[.]com
officeproduces[.]com
web[.]adobephotostage[.]com
Up[.]officeproduces[.]com
We[.]officeproduces[.]com
geocities[.]jp
www[.]cab-sec[.]com

Hashes:
f80430864e7ac22b01cd8042215028e9e9a08cb053b59068a406971eb7d40860
988b01fe70e7c74b046c58207b5e1204bcdee34a035e73fbeb87202e925e92a7
ce1848033aa82f408201695f718fd82b8a1dd0d588332bc003c7abb6ce2664a2
10a0613fbc0b4ad0cc8ed2e4ca32386a489ee7a48b5ab5faa03c66b53b3ed1bd
bc2f69b138fd76ad52c63c0ce623b3c6800995eea849b3f5bcf3a9d76143106e
768ccfce5e2788dcae2b0ac0f01143cf13d65d74ceb03345924b8ac73a7fa1d9
62df273b977bc779860d0ad903f1c14ea8cb82ce79ddf15a194e4c300bbe0b29
b032fe5c0d44bc3376c980a089b38c90edb9ab65f98efbee3b2a01e7b3fbae31
d89a88edfb0108141e149db338044387af498e4b37d0b58c23b2365ff3ba557a
437416d9ef87da4f72b381c8306ca6d296dfdbd2cf83f4e85737f1f2b3f2e994
fb3e3d9671bb733fcecd6900def15b9a6b4f36b0a35bdc769b0a69bc5fb7e40d
161787d08f75adf61c58dcfdce34eaaf741626b3a9579ec14756ff7f658e3b51
c12319da450433229043b016ab9842a84d69ca0ba839bb72b0cb94c5f45179ec
1fc051343abfdb71da895783b4f42ca1a3f16ef026a5c3be2820d0194bee40b0
1cb8c0f87dca3906b6351eefb2a9a639f508d818b3f87ca14873101e95bd6d6b
e85ee3153d5cbd4ff8002a1053a820aa2e25db32ad24d4e8f3e12a3d4de5b3eb
777e36fcc5648fc6b528bc35391f756d87a649e97cfab9bff9d1292d0bfffd20

93ee92f9d417a6e1f87130b46d1edc546c2663cc1fdf375e3626b658b7cf75dd
147890b002ad1c58371aa7e9f2aefd07d50ae1d84febdbc7e0e45fa8925eefe7
131067d2b942176937e6e1e1fdda998d2a698be2084ea4ceacdc3b5e98182c65
2137e13f91c5a8f23327786535d5d0eef30f4e75e892d835c3313796a4b52945
0476ec8b4cb1b5dd368be52d9249f5b3cf6709b3141e9d02814c05f61cb90a91
e49aa226eb570b77e1aee8be606792f66a8af202898901d1acb4d6b4cde3d9c2
480522221226f0ccf801c98846ff405028b482bea10d6b221f7ac05c85874612
83daa6482a45076fba607cd4ee1016020a9690037534c4de6efca6946160ac04
2632a86067e0b05f705ae53ef6114a54ad3c3f697f7f32264344cd442000053e
89fdef30c14db09e4e82c561db4a35cbc039b95bdfa6340546f7ee54b887f59b
560297240bd14baec5a2131512b5562b273f791bababf7b8fbd8d9befaacab86
E585445A4B7257E4306758B288447DBF
6317D15863D31D1CCEF00552C30B9BE4
72838E5708FCFB90E83167F6A058AC2D
92E120B9A294532DE74613B9DEA26ECF
8F173A41FD6B11EC0768AF03A1126F2F
7F7FED2DD0A84660A39F893D8D030C00
2BC7298A57AE2B8AB5B4A7B53360EB5C
4D1EEEA3EDBA4847D6C3E68D8B731C86
4C451454E62F00C3D90EEEA841343BFF
868C5AD262C1AAD2ED22CAA82A5B2AFA
ACE387ECAA08719299E7CF5E89AC07E8
4213D982EE4D51AF943625FE7C9578BA
C55DC22EA69C1842079CFC030CAF667C
4579E202B2782C4D33711CC9FA05AC60
6565052707BA0930C4C8227814E029B7
31BBE446B62127FB5EDCBD5EF4E7B667
E82826B40D2F1AB2C10EB62A6B3738F7
FB271D3A5FFC0FAED0BA766D35B5D8C0
7AE80B778CB1328D1F541076C070A1F6
A55D2B4729A6D186FCAC2706C9003B5A
004F18E5F64E5C07AA639E542D8F6FF8
D38A944E49CE63408D8DCD20A4084A26
5EAAD2CA7A5CD25549BDB503034E73F4
FBA1643B9BE013A8580511E49EB5D079
125764F2AAD2F9D4D55CBFAEE889FBA7
73E084D0AFE665D4F064190753CF0F4F
CFCD54CE55913D566A6E6092009FC79C
0E8D8B01E3B11F1C2A51078AED07A3D2
27B3FA6DE306DF4CC092FBCE3D91ABA3
B1F8F6481E99922C678CC8ACD6F495D0
9295598E295D01BD6199625D7BC424EC
AD2B82ECF497D681DEFF4AB63C95AF7B
747B09E8ABF342F9E6D7BC3F1959EEC8
54F687BF537C8CAF6AC38AB3ABC68CA4
3E9BDA4FF1216AF7D2C29EE92C673DCC
D785CD7672D0CDBF0F3C92872E26971D
81C8ED13A3BFF4DEFC04C79B82FA2D84
456465EC5AE55B9D0AB20DBFFAA38C2E
A9573395D31BB540B14481DD23B3DE8C
B490554B61A2D75675C5F37250C578AA
E37655A4EB0C33747EB88DCF11D8034E
1B4D4779C855A5A249CAB6C1CCF8031B
9912EB641EABD640A476720C51F5E3AD
64E9E12B2496674CF359D41A81A6B2B0
A7AFBCCF69AC5711AC8348E6A231360F
CA2A23F3E304B0F309B67D9B5706BB98
F426B6062C959C46666E3389EBB945CC
FE71D6FCCE4A3DF89EAA96CC1D6C6E81
6ADEA1FF3A9CB50BD0CD1D206419C187
8B8E8C6B9AA0B873CA78F0AEFBBA11D3
A7B81A3E5730140E88CC83C1841C7DA4
8C48544C2A4E86778D5271AE01A34117
FBA9E5734D46AC6E46276D7F30CFA96B
98920B6CCC53701F47DC54F48E26F131
EBA57D89BC14708C0C0E9AE4A0E425AD
4BD45A1E9B441DC3CC67652C5E67766B
02129F8CF0688501EA803883AB21E1C9

Recommendations :

- Monitor Connection attempts towards the listed domains. 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. Maintain up-to-date antivirus signatures and engines.
- Ensure installation and usage of the latest version of PowerShell, with enhanced logging enabled script block logging and transcription enabled. Enabled code signing feature for all types of users in Power script.

Reference: CERT-In

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