Goblin Panda continues to target Vietnam

medium.com/@Sebdraven/goblin-panda-continues-to-target-vietnam-bc2f0f56dcd6

Sebdraven May 2, 2019

Sebdraven

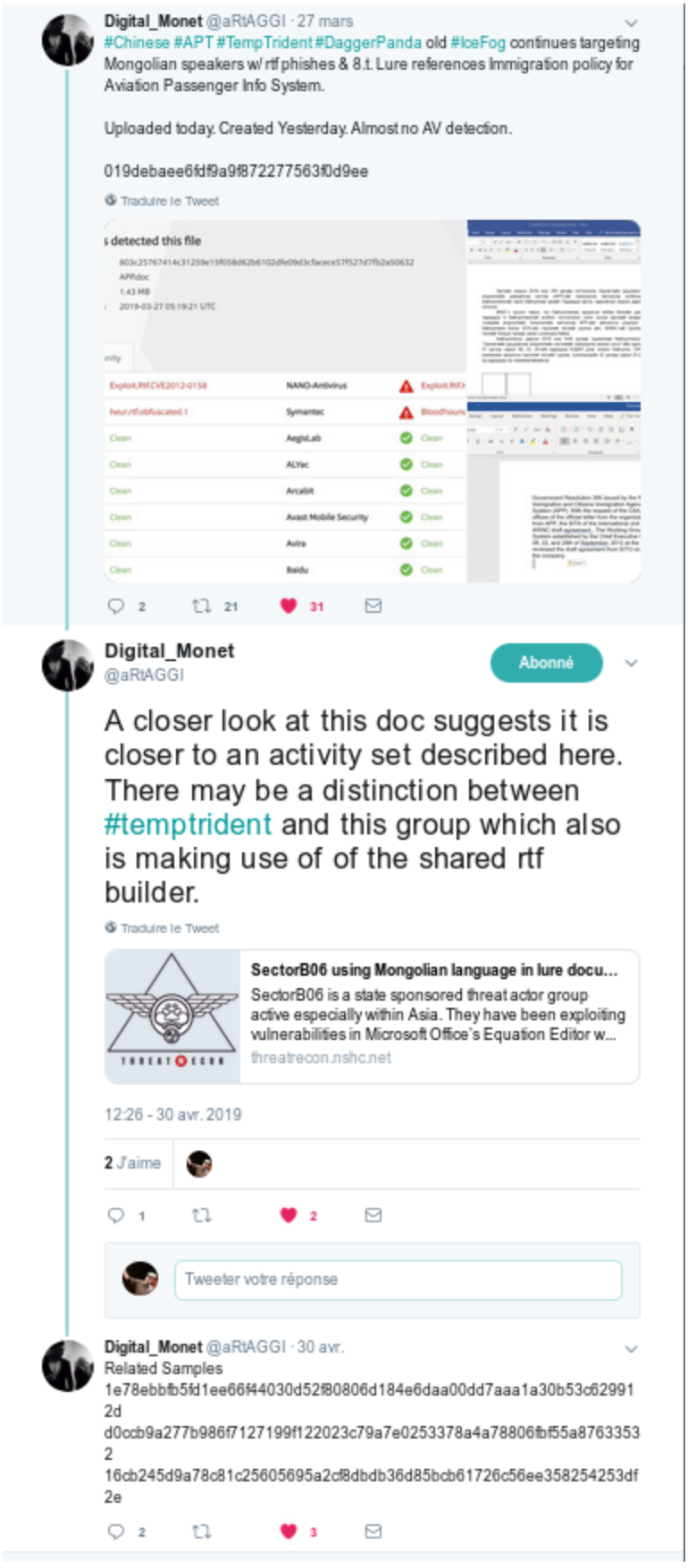
May 2, 2019

.

2 min read

Chinese actors have changed the rtf exploit following my different articles and Anomali article https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-apts-have-a-shared-supply-chain

But In march a researcher of Anomali @aRtAGGI made a link very interesting between Icefog and an article targeting Mongelian speaker https://threatrecon.nshc.net/2019/04/30/sectorb06-using-mongolian-language-in-lure-document/



I decide to reanalyze the RTF exploit. It's the same techniques, they have just change the XORing and the exploit body to bypass the yara rules which have been published.

After a new rule and retro hunting, I found a new RTF file 81f75839e6193212d71d771edea62430111482177cdc481f4688d82cd8a5fed6 exploiting the same RTF vulnerability CVE-2017–11882 and drops two files

C:\Users\admin\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\QcConsol.exe 9f3114e48dd0245467fd184bb9655a5208fa7d13e2fe06514d1f3d61ce8b8770

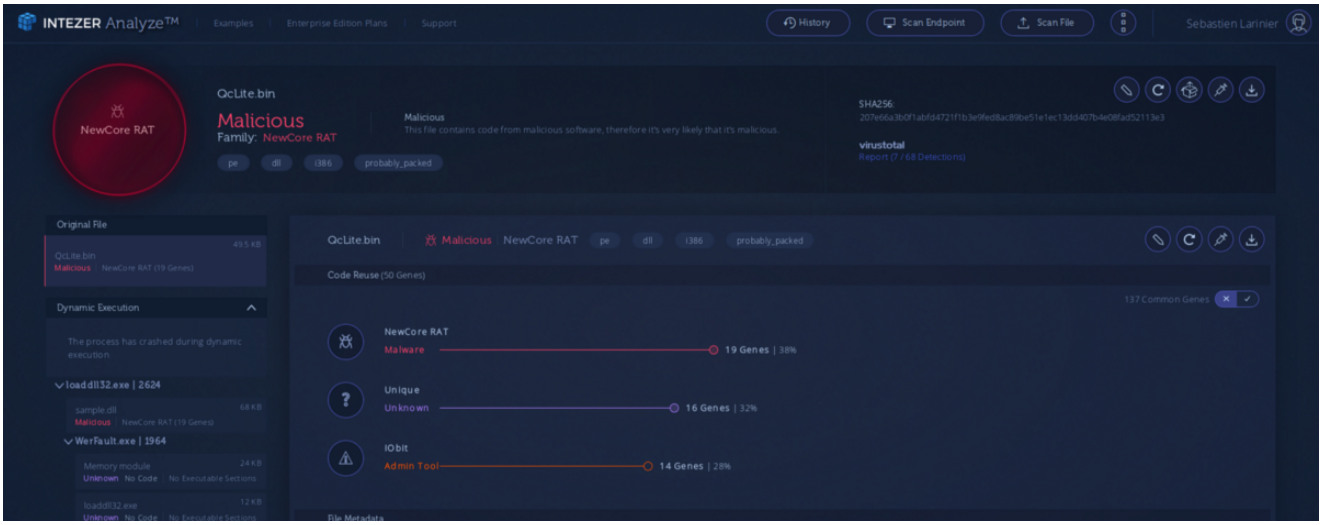
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\QcLite.dll 207e66a3b0f1abfd4721f1b3e9fed8ac89be51e1ec13dd407b4e08fad52113e3

The backdoor is the DLL and has as usual, the malware is executing using the side loading.

The dll is a variant of the newcoreRAT with many similarities with 05d0ad2bcc1c6e2752a231bc36d07a841f075a0a32a3a62abaafddbdafd72f62

5a592b92ffcbea75e458726cecc7f159b8f71c46b80de30bac2a48006ac1e1b3

5b652205b1c248e5d5fc0eb5f53c5754df829ed2479687d4f14c2e08fbf87e76



and the RTF is a spear phishing targeting Vietnamese people.

The malware seems to compile 11 Dec 2018 and the document has created in 2019:01:18.

The C2 of the backdoor is a old domain web.hcmuafgh.com but it's a new IP 193.29.56.62.

IOCs

81f75839e6193212d71d771edea62430111482177cdc481f4688d82cd8a5fed6

C:\Users\admin\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\QcLite.dll 207e66a3b0f1abfd4721f1b3e9fed8ac89be51e1ec13dd407b4e08fad52113e3 sha256 C:\Users\admin\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\QcConsol.exe

9f3114e48dd0245467fd184bb9655a5208fa7d13e2fe06514d1f3d61ce8b8770
web.hcmuafgh.com
193.29.56.62
http://web.hcmuafgh.com:4357/link?
url=maOVmKGmMDU1&enpl=OXcoVQ==&encd=XARIZTE=