

# Goblin Panda continues to target Vietnam

By Sebdraven

Published: 2019-05-02 · Archived: 2026-04-05 22:59:28 UTC



2 min read

May 2, 2019

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 Mongolian speaker <https://threatrecon.nshc.net/2019/04/30/sectorb06-using-mongolian-language-in-lure-document/>

**Digital\_Monet** @aRtAGGI · 27 mars

#Chinese #APT #TempTrident #DaggerPanda old #IceFog continues targeting Mongolian speakers w/ rtf phishing & 8.t. Lure references Immigration policy for Aviation Passenger Info System.

Uploaded today. Created Yesterday. Almost no AV detection.

019debaee6fd9a9872277563f0d9ee

Traduire le Tweet

detected this file

803257674143129b1505862b4102f6e903cface657f527f7b2460632

APFDoc  
1.43 MB  
2019-03-27 05:19:21 UTC

Exploit.Rtf.CVE2012-0158	NANO-Antivirus	Exploit.RTF
heuristic/Adware.Gen	Symantec	Bloodhound
Clean	AvastLab	Clean
Clean	ALYac	Clean
Clean	Avast	Clean
Clean	Avast Mobile Security	Clean
Clean	Avira	Clean
Clean	Baidu	Clean

2 21 31

---

**Digital\_Monet** @aRtAGGI

Abonné

A closer look at this doc suggests it is closer to an activity set described here. There may be a distinction between #tempt Trident and this group which also is making use of of the shared rtf builder.

Traduire le Tweet

**SectorB06 using Mongolian language in lure docu...**

SectorB06 is a state sponsored threat actor group active especially within Asia. They have been exploiting vulnerabilities in Microsoft Office's Equation Editor w...

threatrecon.nshc.net

12:26 - 30 avr. 2019

2 J'aime

1 2

Tweeter votre réponse

---

**Digital\_Monet** @aRtAGGI · 30 avr.

Related Samples

1e78ebbfb5fd1ee6644030d52f80806d184e6daa00dd7aaa1a30b53c629912d  
d00cb9a277b986f7127199f122023c79a7e0253378a4a78806fb55a87633532  
16cb245d9a78c81c25605695a2cd8dbdb36d85bcb61726c56ee358254253df2e

2 3

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.

## Get Sebdraven's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

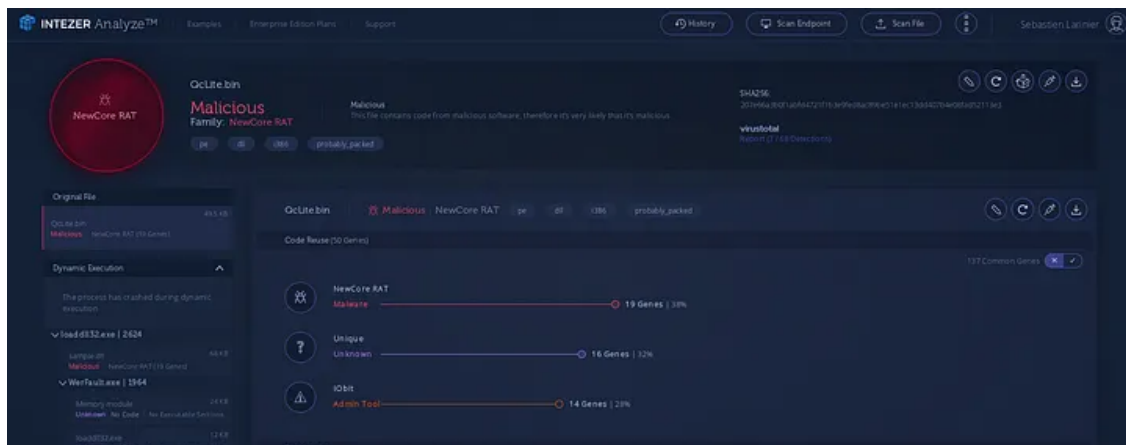
The dll is a variant of the newcoreRAT with many similarities with

05d0ad2bcc1c6e2752a231bc36d07a841f075a0a32a3a62abaafddbafdf72f62

5a592b92ffcbea75e458726cecc7f159b8f71c46b80de30bac2a48006ac1e1b3

5b652205b1c248e5d5fc0eb5f53c5754df829ed2479687d4f14c2e08fbf87e76

Press enter or click to view image in full size



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=>

---

Source: <https://medium.com/@Sebraven/goblin-panda-continues-to-target-vietnam-bc2f0f56dcd6>