Actor behind Operation LagTime targets Russia

sebdraven.medium.com/actor-behind-operation-lagtime-targets-russia-f8c277dc52a9

Sebdraven November 25, 2020

Se bdrav

Sebdraven

Nov 25, 2020

.

2 min read

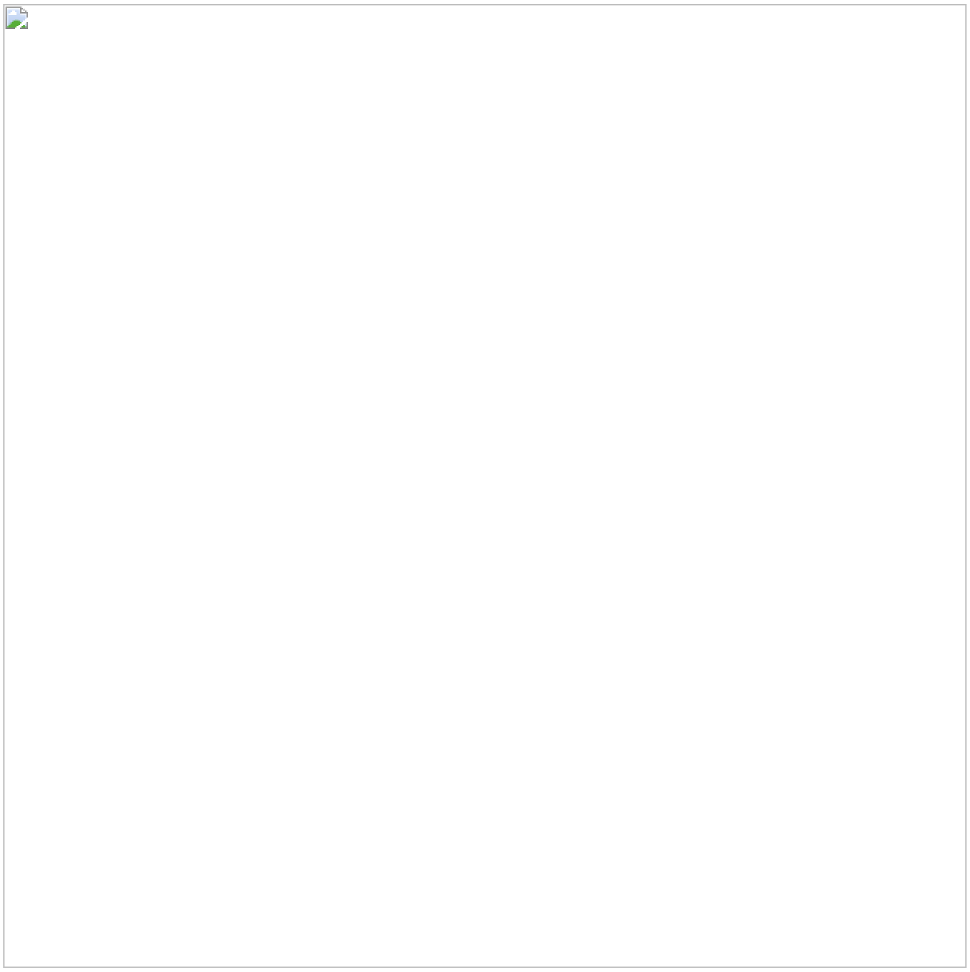
the file f5a78a155a219582db8959c3a96a1d91ed891801663b1cce0c599779773bc3f5 uses the version 7 of royal road document.

This file drops in memory a new backdoor rewriting the process EQNEDT32.EXE.

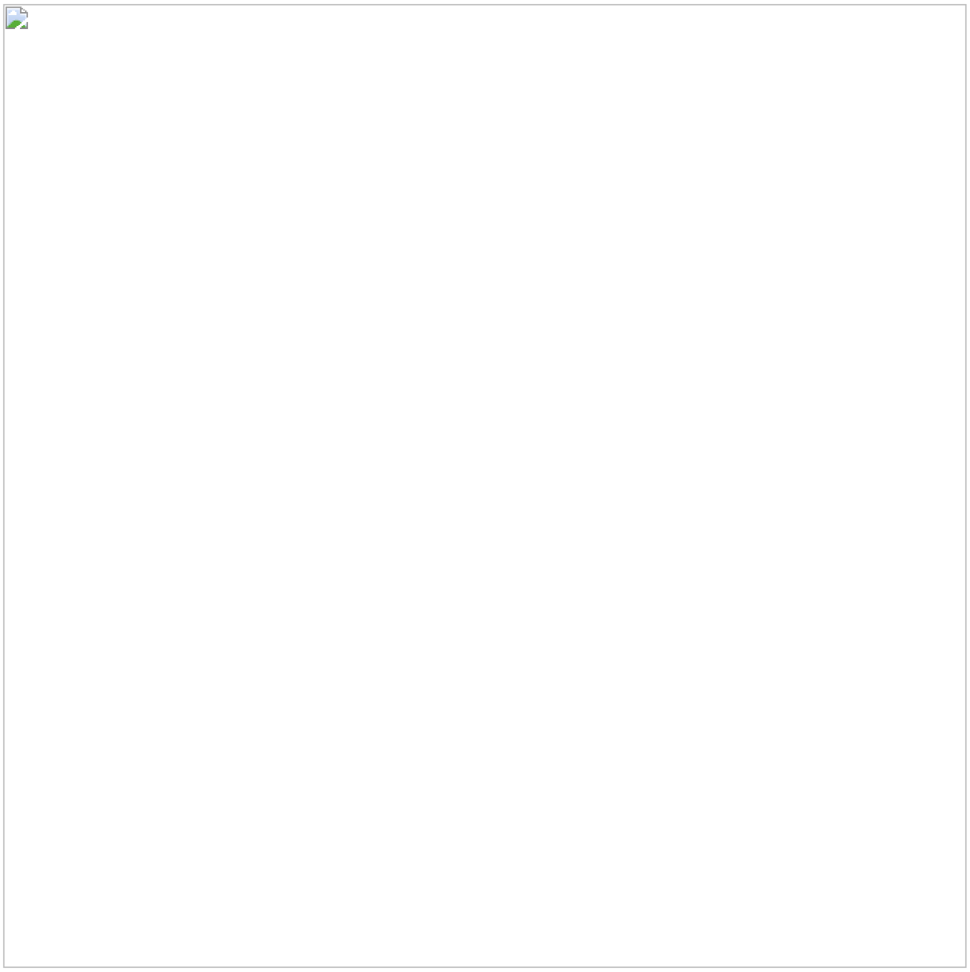
This document refers to the ceasefire between Armenia and Azerbaijan and seems to be send by the Mongolian authorities.

Analysis of the backdoor in memory

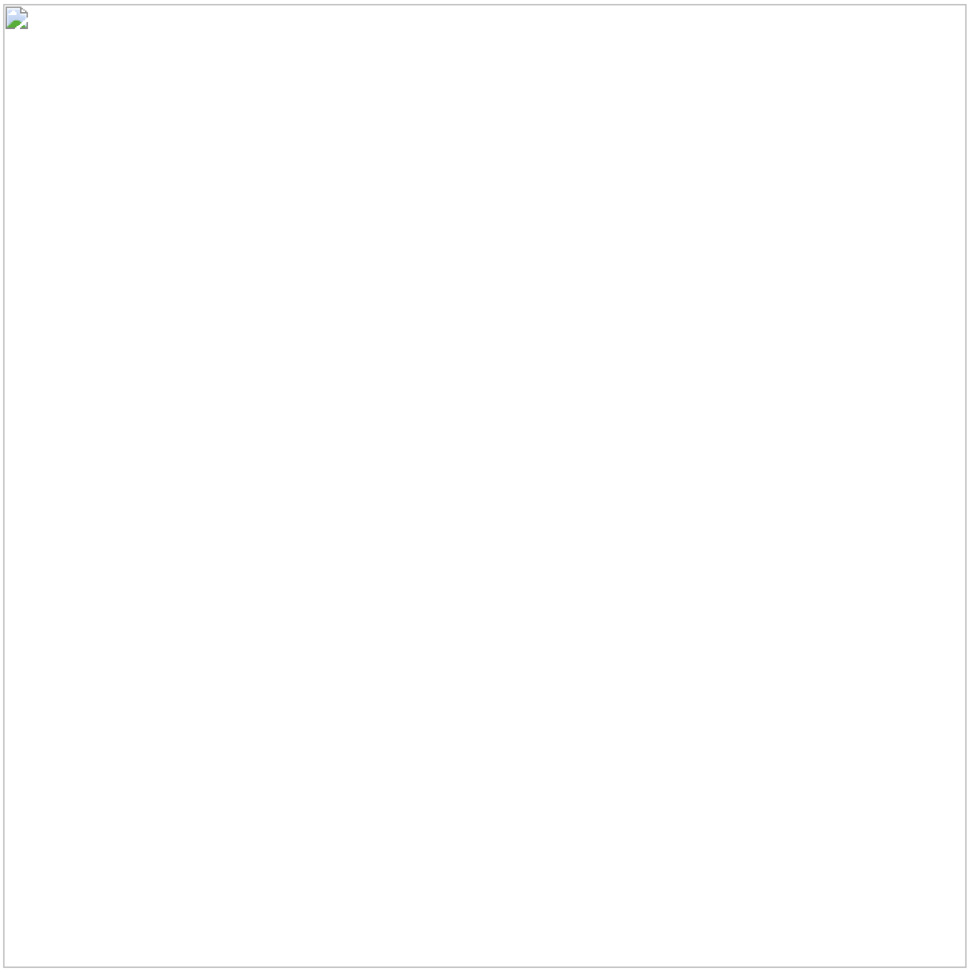
This backdoor is a state machine launching different threads. (function 00401640)



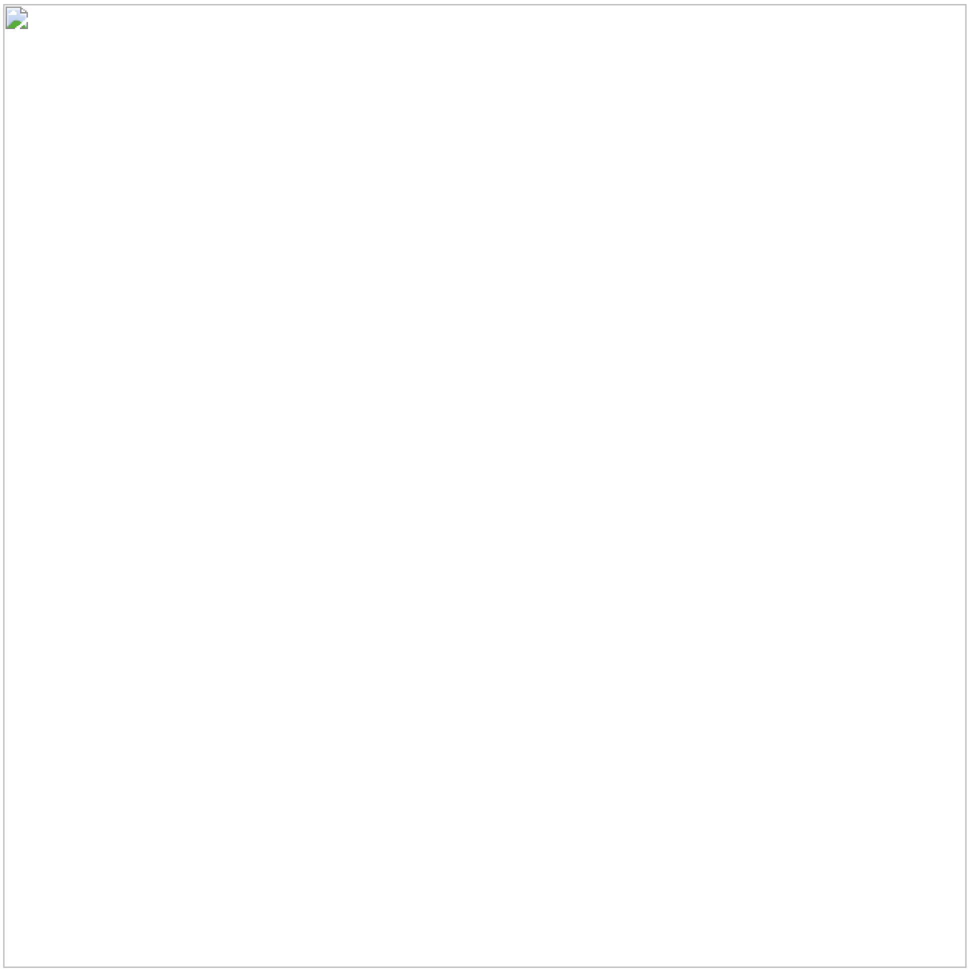
The backdoor checks the disk of the computer, the processes launched, the version of windows, the privileges of the user.



The malware tries many connections to the c2 in different functions:



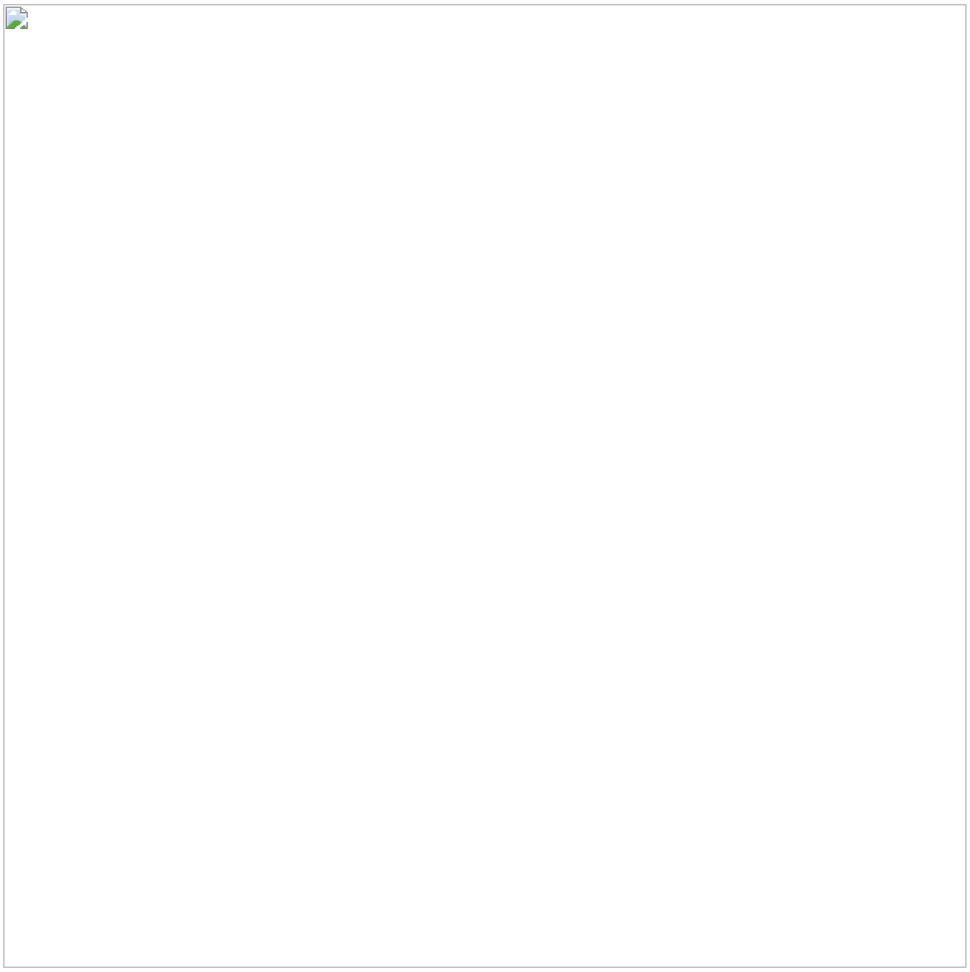
The domain of the c2 is in clear text in the malware



This backdoor is very simple to analyze. There are no packing and no obfuscation code.

Attribution

For Intezer, the similarity is high with the file 4c22eb33aa1d10511eaf8d13098e2687e44eaebc5af8112473e28acedac34be

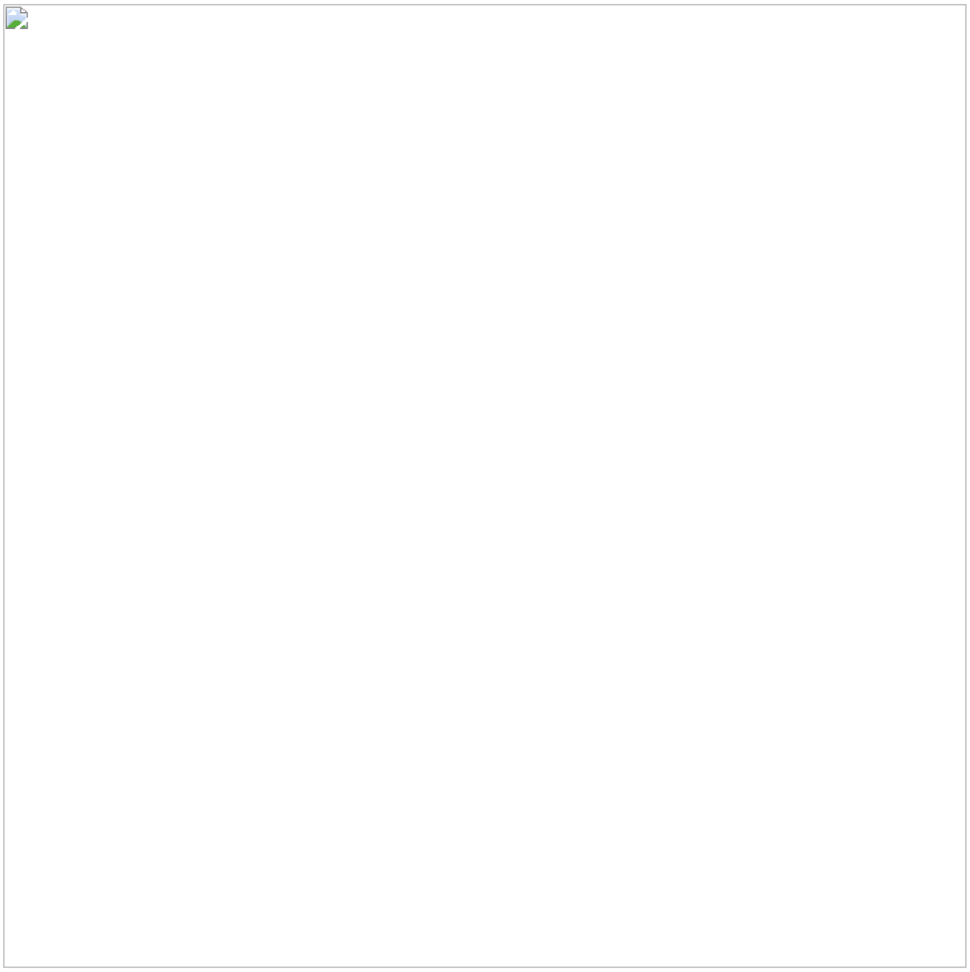


This malware was used in operation lagtime.
https://otx.alienvault.com/indicator/file/4c22eb33aa1d10511eaf8d13098e2687e44eaebc5af8112473e28acedac34bea

The IP of the C2 is 95.179.131.29 in operation LagTime.

So the campaign against russia is driven by the same threat actor of Operation LagTime IT

The configuration of the backdoor’s C2, 103.106.250.239 which is hosted in Malaysia, has changed in July 2020. This date seems to be the beginning of the operation.



IOCs

Rtf file

f5a78a155a219582db8959c3a96a1d91ed891801663b1cce0c599779773bc3f5
2d678cba2795d0339331125692e9a850a043a22f
ae1b4a5775aca501954076b8024b04ec

Network

custom.songuulcomiss.com
103.106.250.239

Backdoor:

46a9ca7d5364fbe5fd3d6ffb0f8d86e9a9e566708657e59ef8873d3ed536348d