A .NET rat targets Mongolia

sebdraven.medium.com/a-net-rat-target-mongolia-9c1439c39bc2

Sebdraven March 24, 2021

Sebdraven

Mar 23, 2021

.

4 min read

A new document royal road v7 installs a backdoor in .NET. a first executable is dropped \os03C2.tmp. This exe has many similarities with older campaigns using by Operation LagTime or Tonto Team.

Document

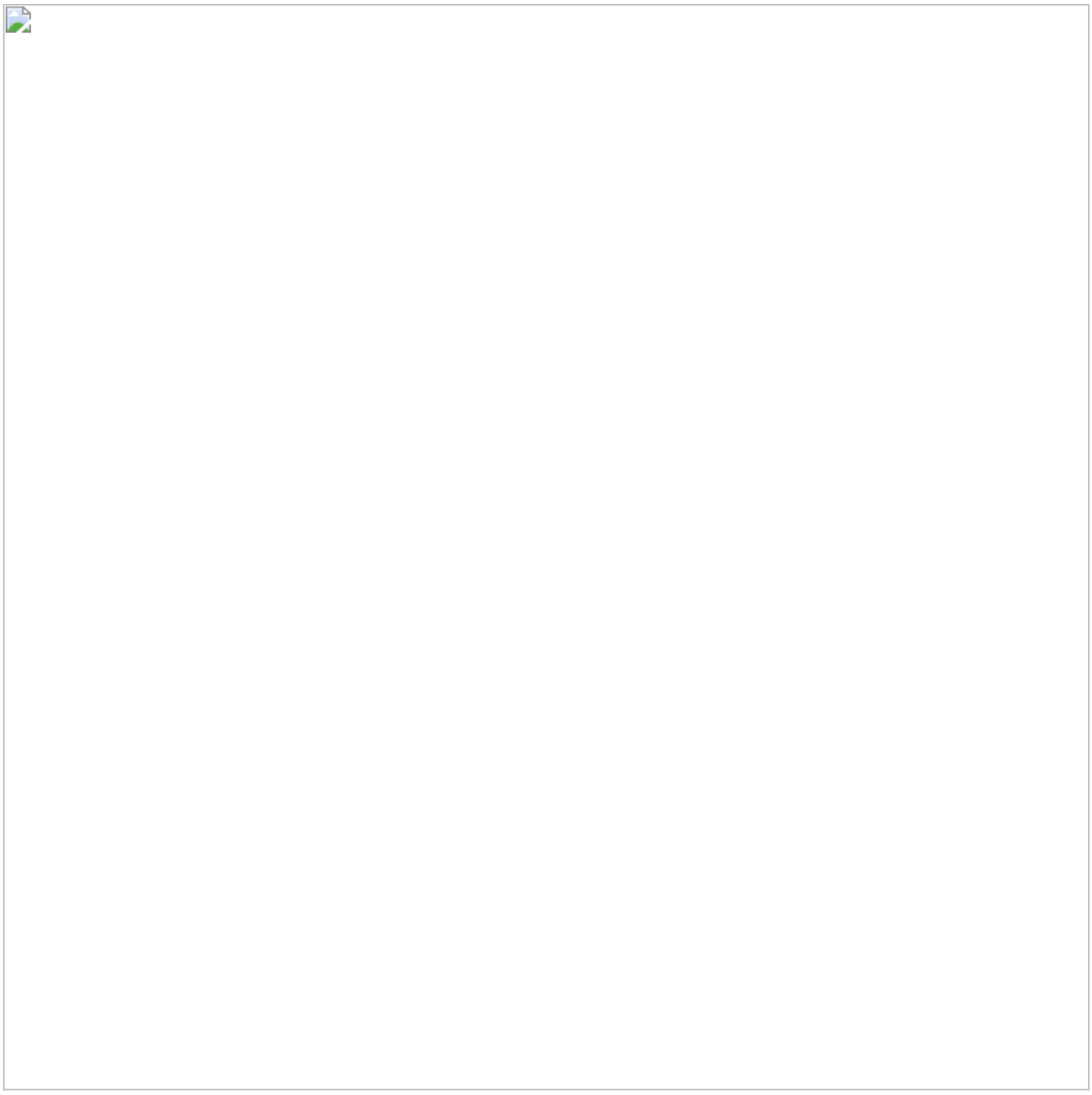
The decoy document is a document about infection of covid19 in Russia send to the Mongolia Authorities. The document is fake signed A. Amarsaikhan.

This technics was used by Operation LagTime and another APT Chinese.

Backdoor Analysis

The backdoor is installed C:\MSBuild\WindowsUpdate\S-1–2 and the name of file is csrss.exe like the legit process of Windows

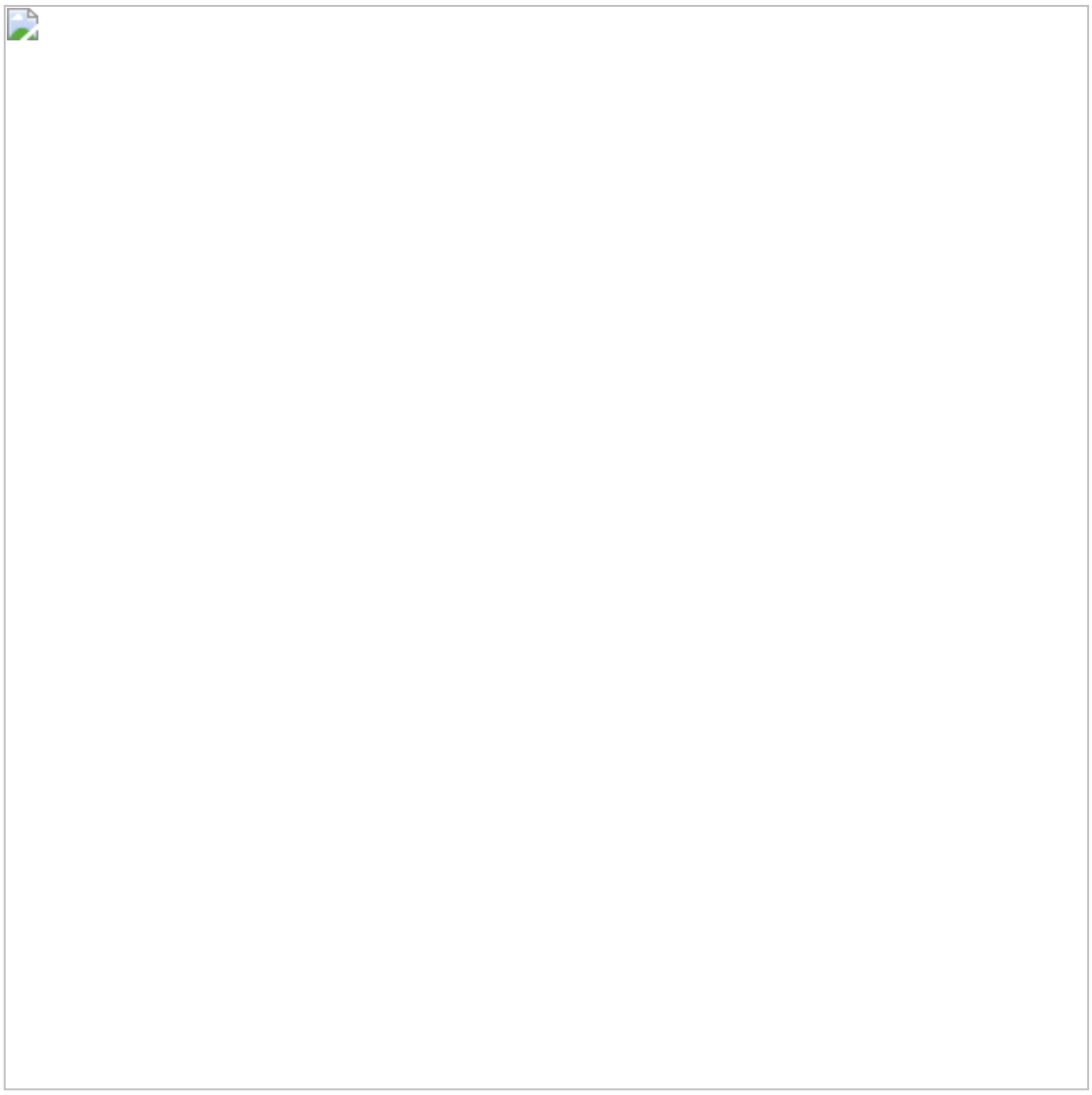
The configuration of the backdoor is stored in a ressource .NET.



The content of the XML file is encrypted with the AES algorithm. The key is hardcoded in the class Main_Form in the private method Main_Form_Load.

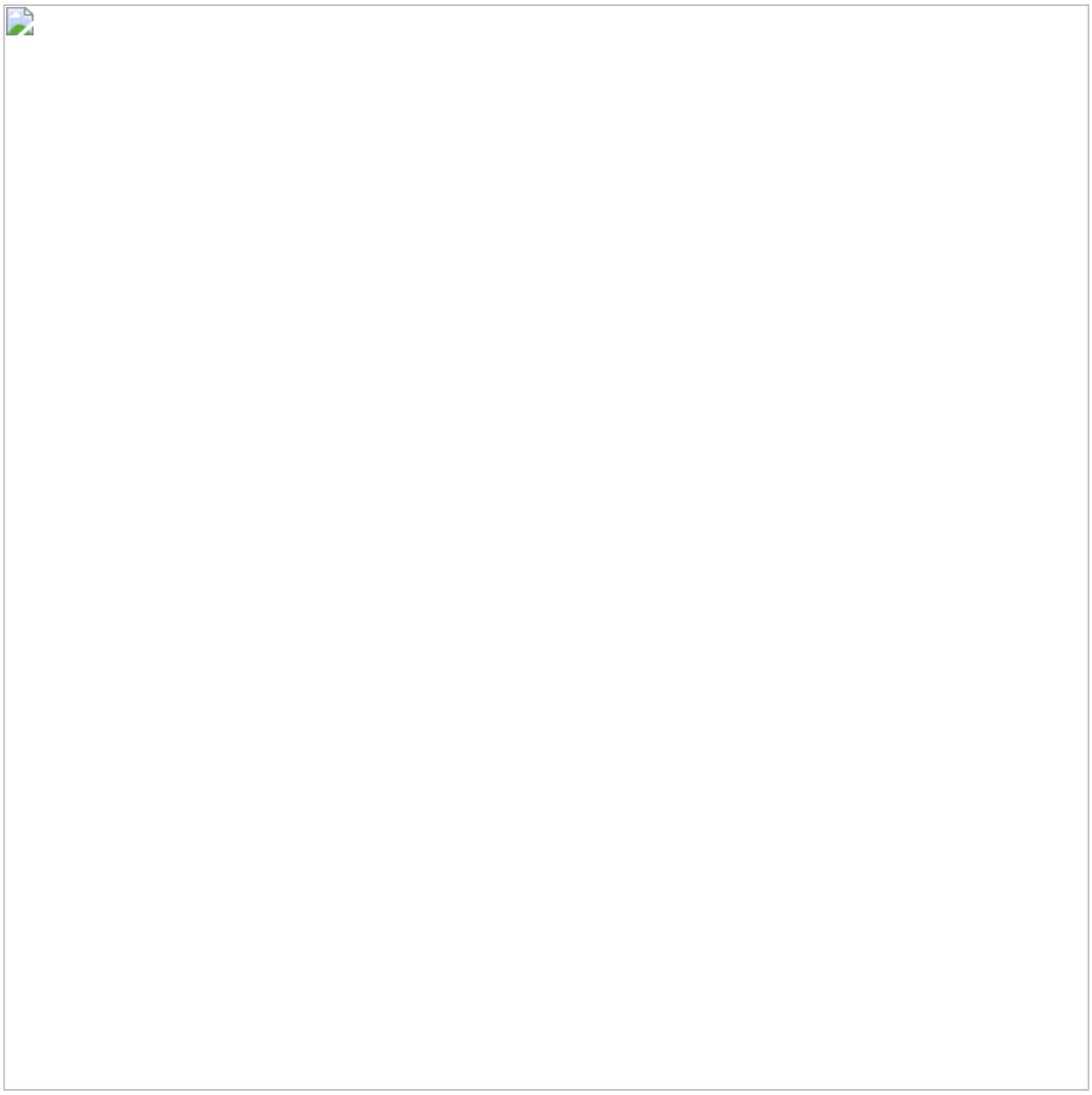
```
byte[] crypt_key = new byte[]
{
230,
23,
63,
211,
96,
49,
120,
48,
182,
11,
49,
173,
233,
114,
123,
61,
230,
23,
63,
211,
96,
49,
120,
48,
182,
11,
49,
173,
233,
114,
123,
61
};
```

The xml file is decrypted :

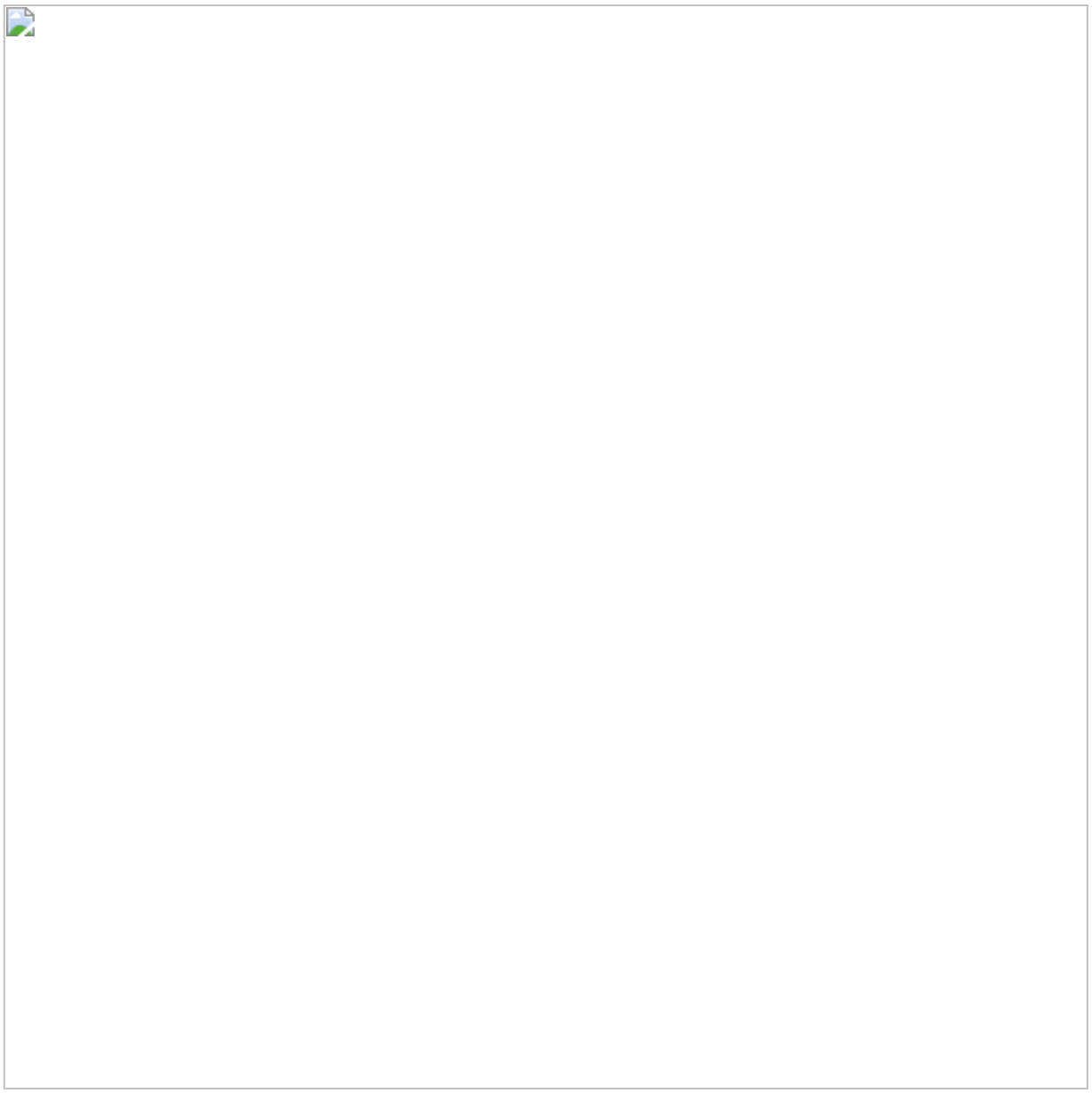


A session key is created and used for encrypting all data found by the backdoor and send to C2.

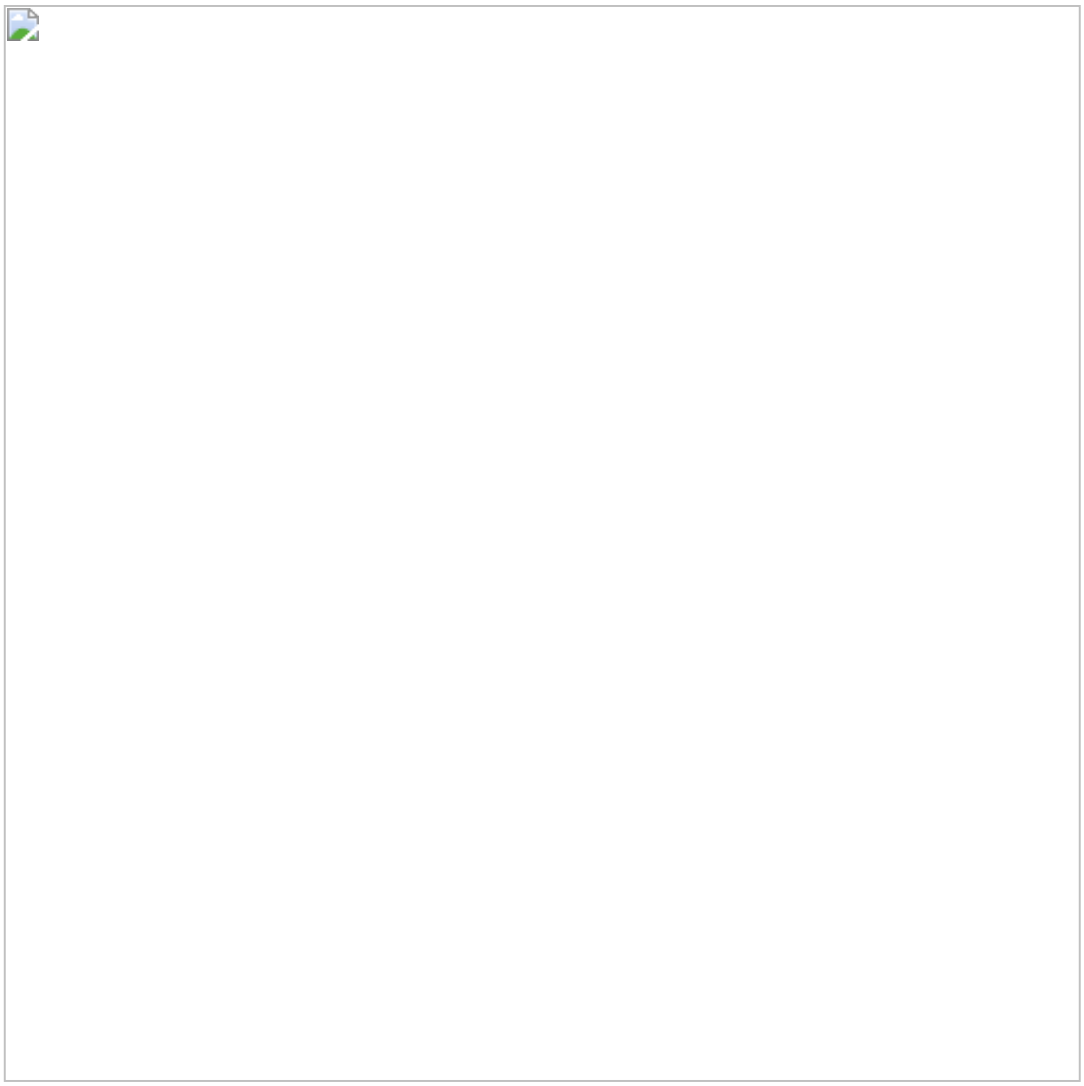
A mutant is created with the information of the configuration:

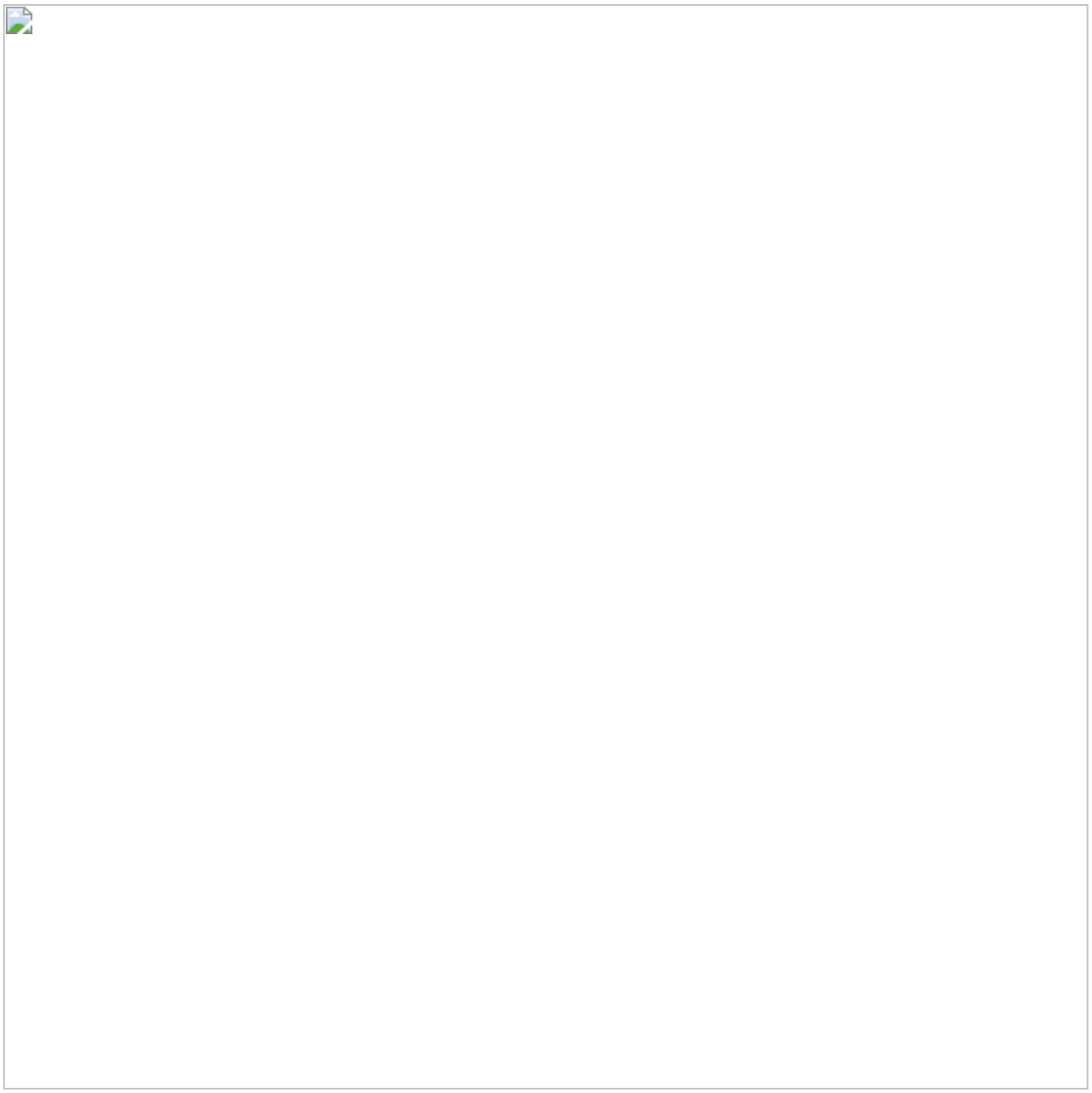


And the persistence is the run keys with a check of the privileges:



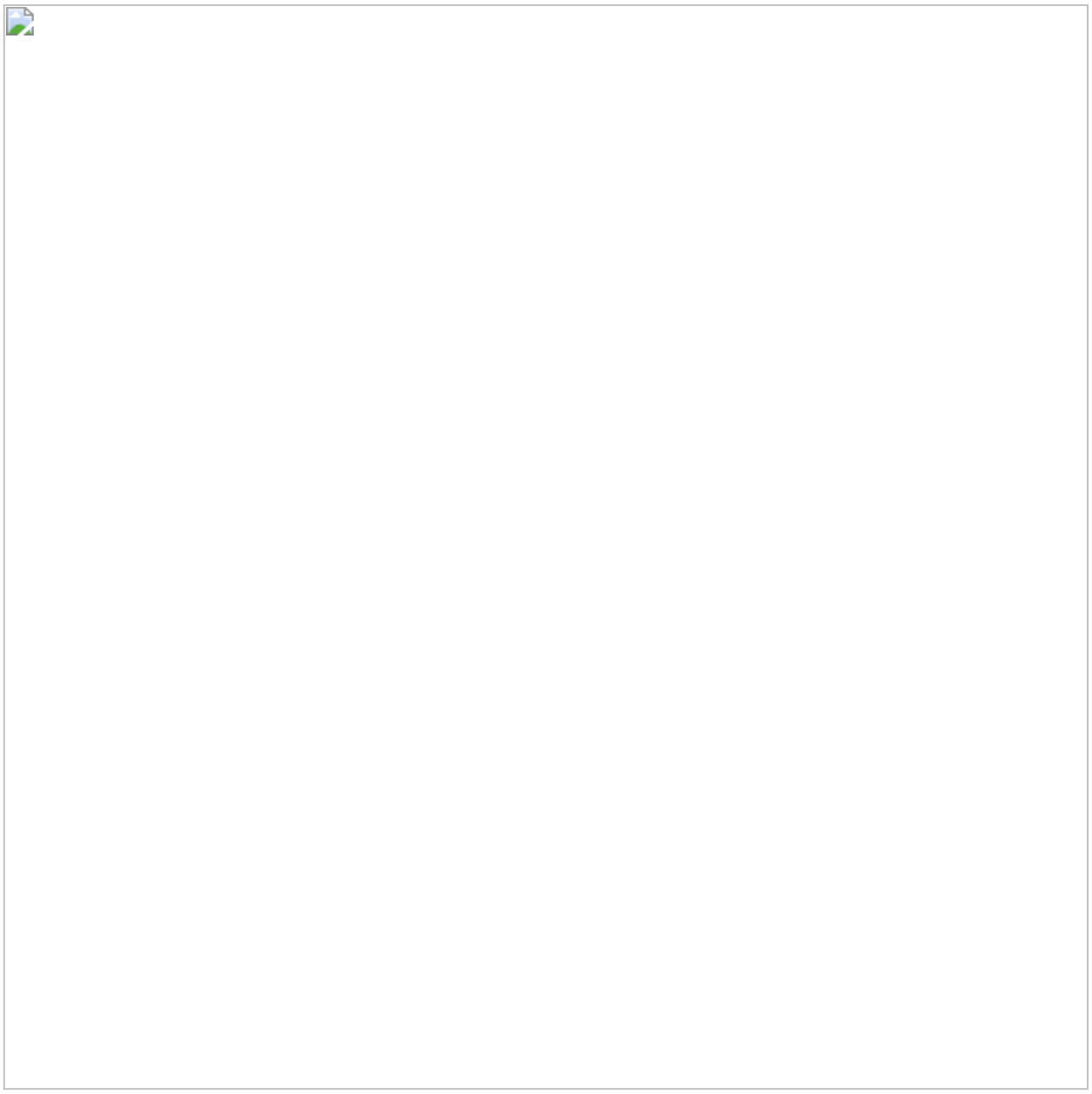
A connection to the c2 is done in a thread with the method Post_Online_Message. The messages are encrypted with the BasicKey hardcoded in the code: 8A5AE1329F9CD824EE915FE14328D267



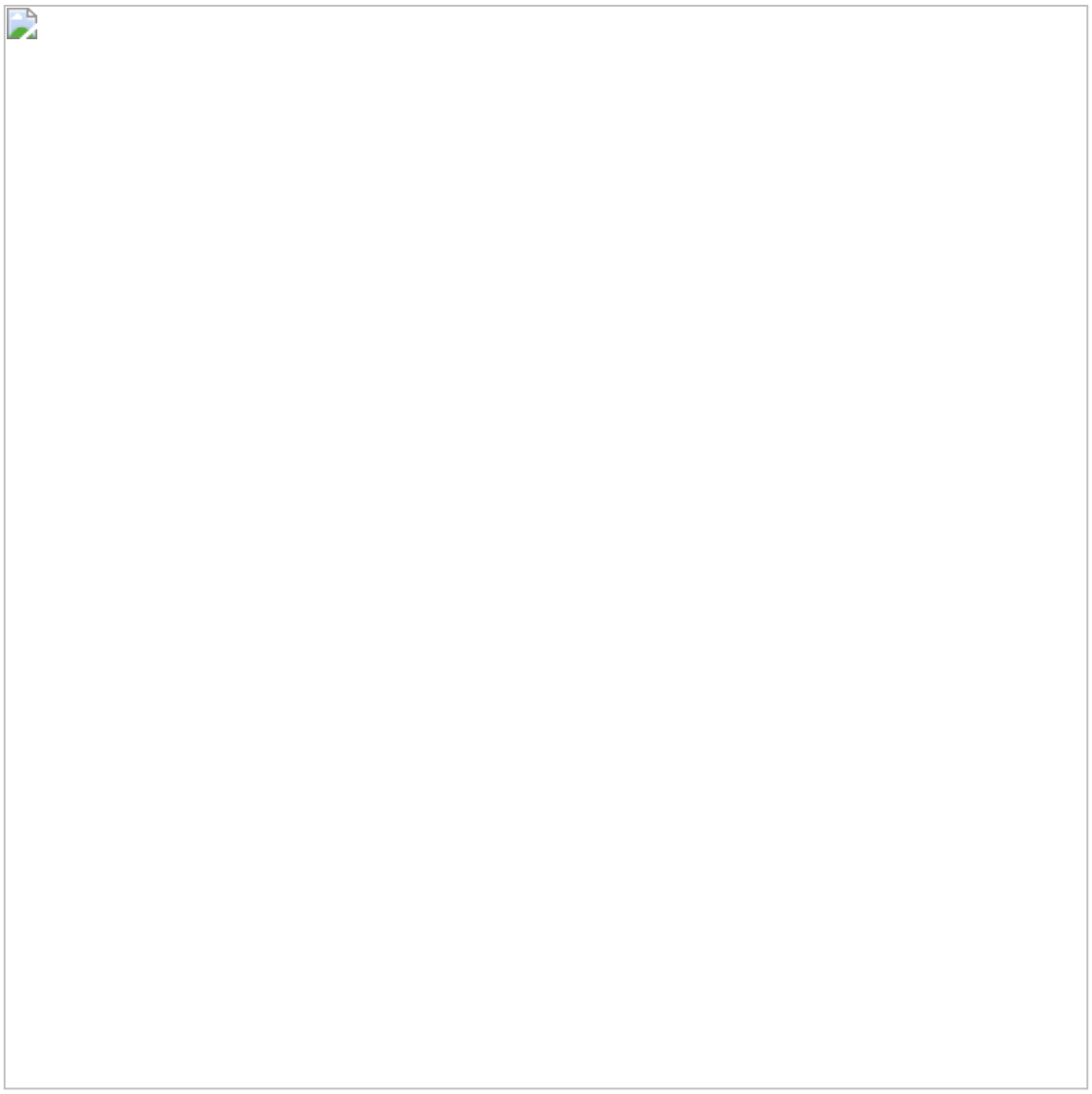


The first information are sent in the setting of the compromise computer with the method Get_ComputerInfo.

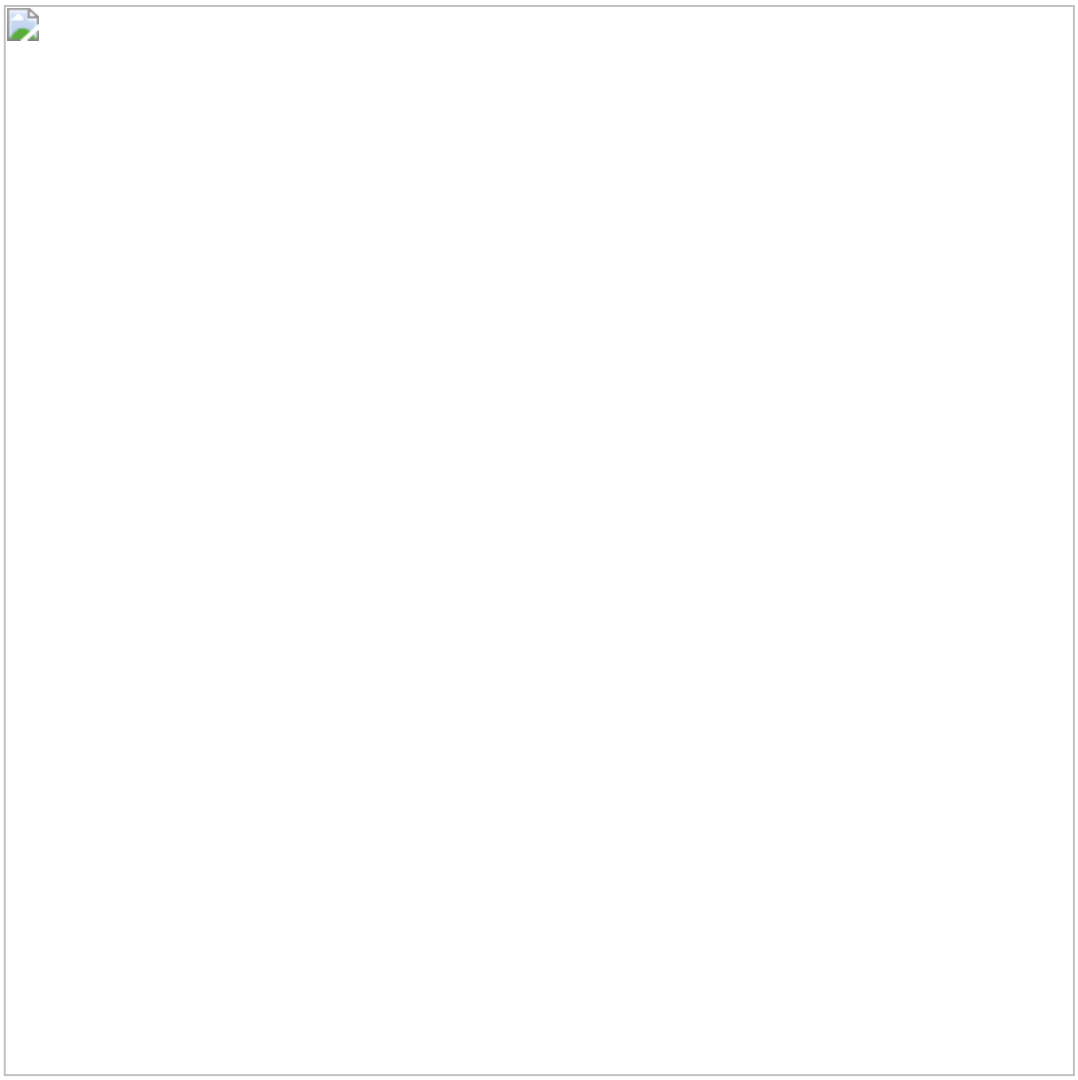
The disk are listed, the kind of operating system, the processor information, the memory ram. These information are collecting by using WMI and the IP of the computer.



After that, the backoor waits orders in another thread with the method Get_Server_Order.



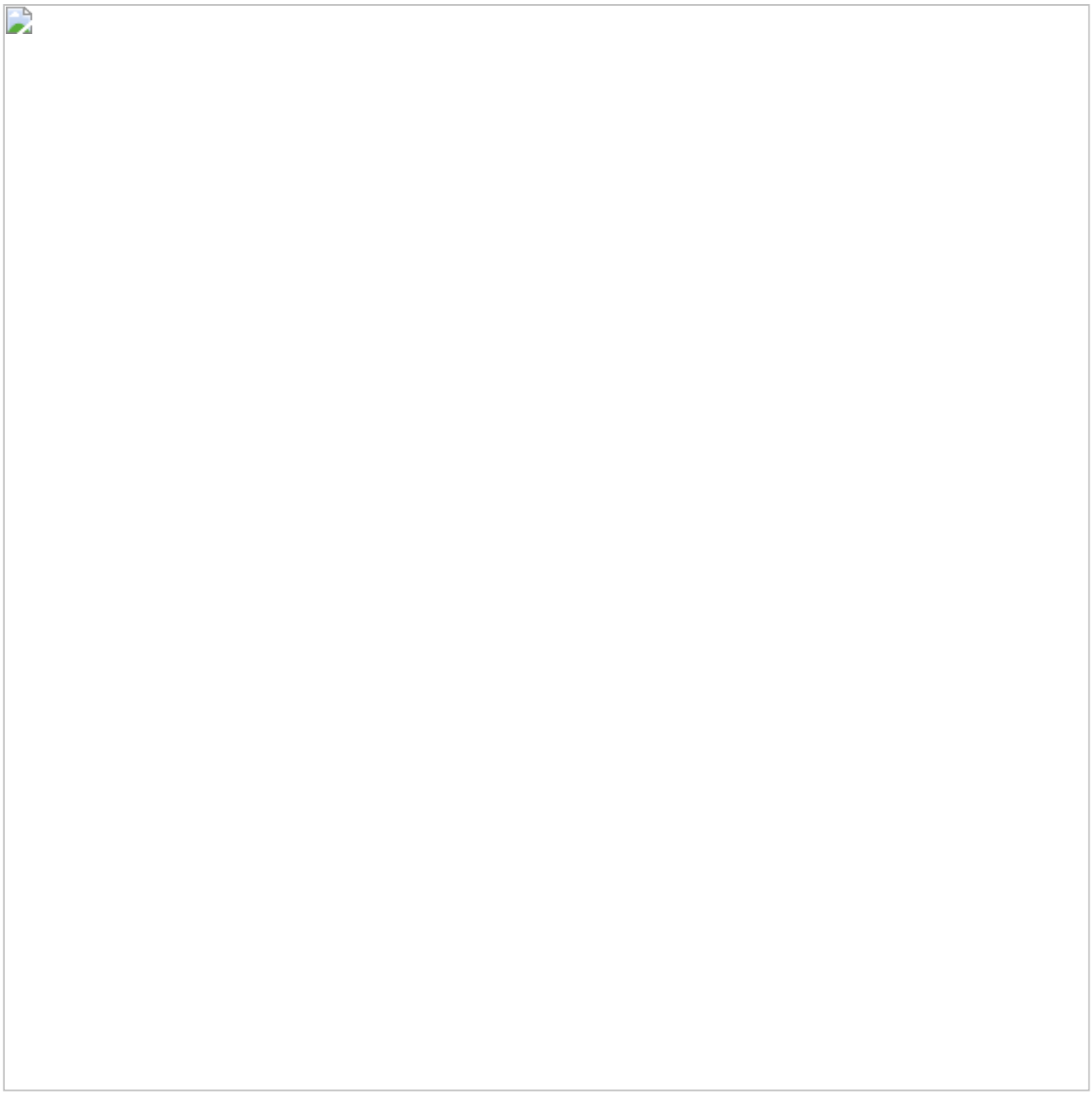
All orders are decrypted with the same BasicKey



And the method Order_Catcher launch the different orders:

the order is Getdir, $GetDisk, GetFileList, Checksum, DeleteFile, DeleteFolder, RenameFolder, RenameFile, RunHide, Upload, Download, ActiveDos, ExecuteCommand, Disconnect, Trans (to transfert data), Uninstall

Each order has a method with the same name:



Threat Intelligence

Many TTPs are similar to another groups like TA428 (Operation LagTime) or Tonto. So this backdoor can be developped by APT Chinese Group.

A new technic is to use .NET. There is different example with .Net plugx loader or tool to install the different payload like RedDelta. Chinese State-Sponsored Group ‘RedDelta’ Targets the Vatican and Catholic Organizations (recordedfuture.com)

In this case, there is not a side loading then many operations driven by APT chinese.

IOCs:

c2 185.82.218.40

RTF: 1120275dc25bc9a7b3e078138c7240fbf26c91890d829e51d9fa837fe90237ed

Dropped executable file
C:\Users\admin\AppData\Local\Temp\os03C2.tmp
2b038ad9bfb8c3f40e95e38b572bdf536d9fd2e7dd5cc0c66fbd0bdc1ed89fde
C:\MSBuild\WindowsUpdate\S-1–2\cssrs.exe
08be2c7239acb9557454088bba877a245c8ef9b0e9eb389c65a98e1c752c5709

c2: 185.82.218.40

Yara rule:

```
rule backdoor_net{
meta:
description= “Backdoor targets Mongolia”
author= “@sebdraven”
date = “2020–03–23”
tlp = “white”
strings:
$s1=”RunHide”
$s2=”Token”
$s3=”BasicKey”
$s4=”SessionKey”
$s5=”AdminKeyMD5"
$s6=”Aes256"
$s7=”Order_Catcher”
$s8=”Get_ComputerInfo”
$s9=”TransData”
condition:
all of them
}
```