Malware Analysis [#1]- NanoCore Rat

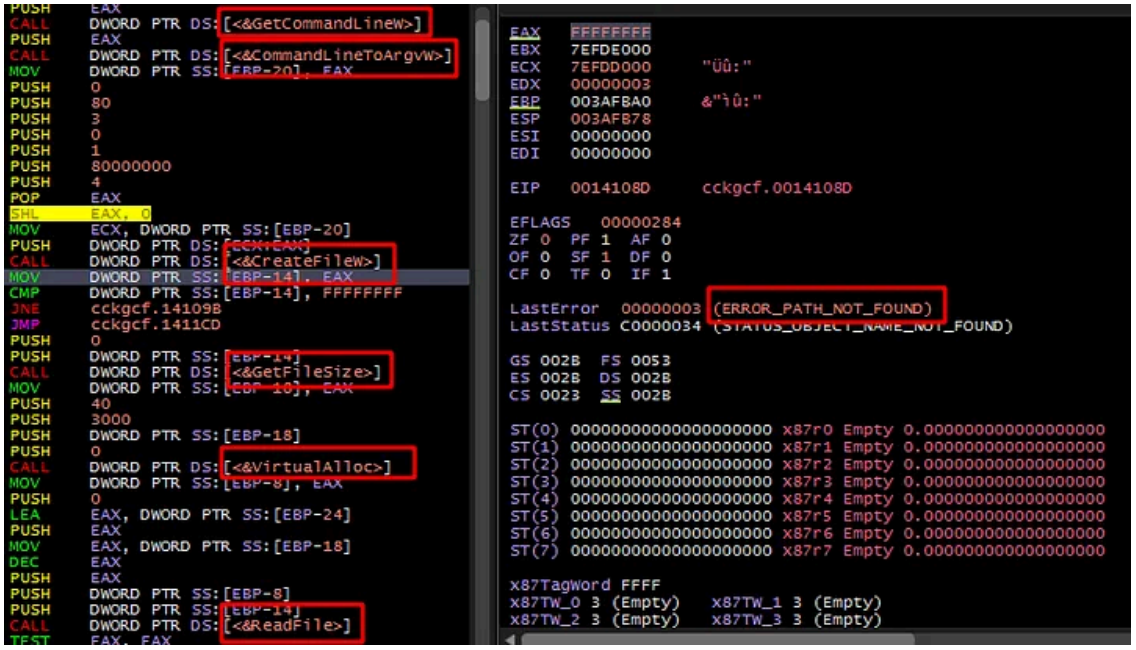
By 0xM3H51N

Published: 2022-09-09 · Archived: 2026-04-05 20:09:20 UTC

Dynamic Analysis of ccgkcf.exe:

As mentioned before when running this instance without any argument the process will exit and no action will be taken, but when adding the “**cmdkuqqy”** as an argument as we saw the installer did when creating a new process, the sample continue it’s work by opening the “**cmdkuqqy**” file get it’s size read it and decrypt it and at last handle the execution to the shell-code :

Press enter or click to view image in full size

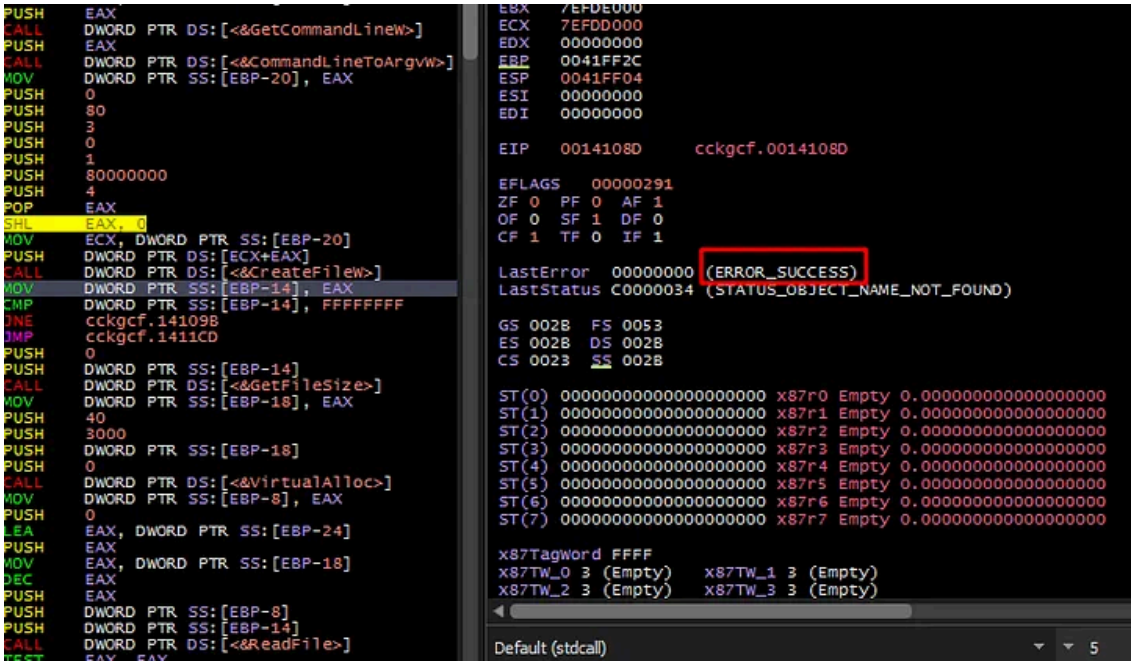


x64dbg: Error path not found

```
Command: init C:\<path>\cckgcf.exe, C:\<path>\cmdkuqqy
```

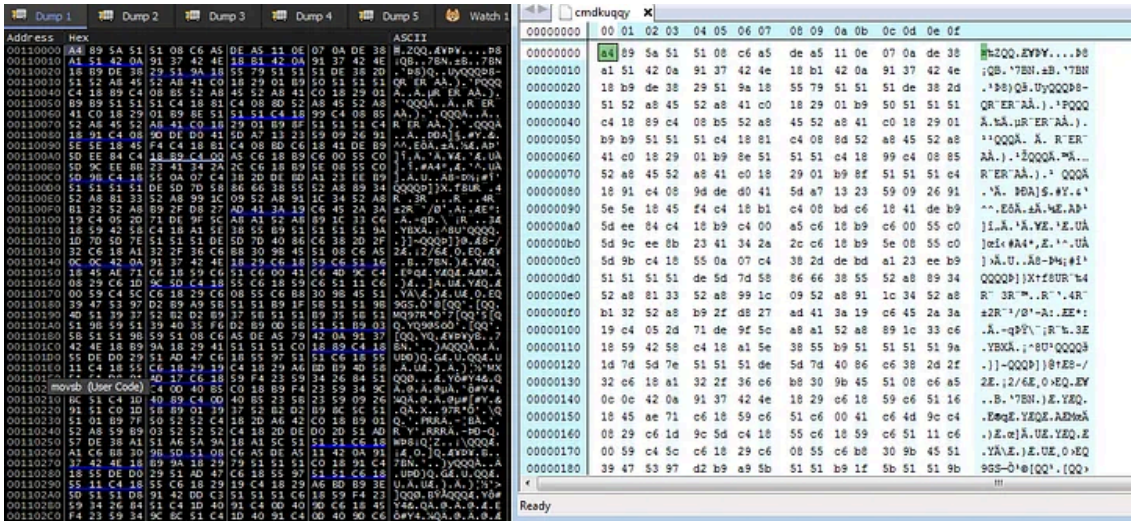
x64dbg: Command to add argument

Press enter or click to view image in full size



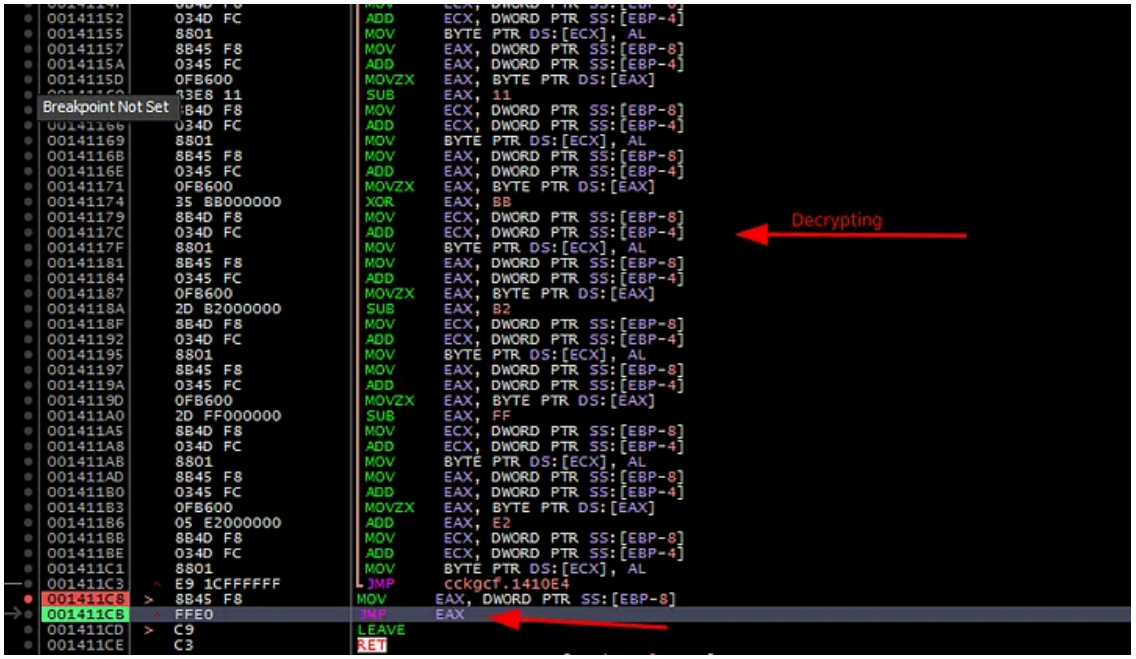
x64dbg: function succeed

Press enter or click to view image in full size



hex comparison

Press enter or click to view image in full size



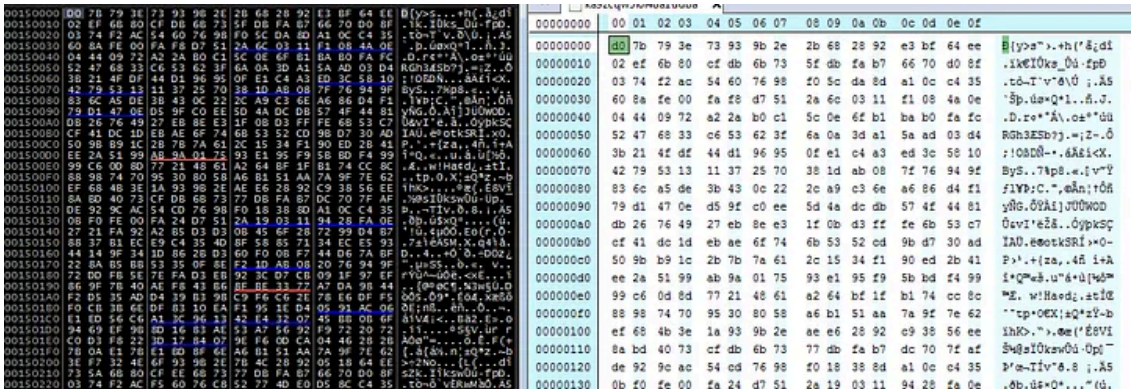
x64dbg: Jumping after decryption

The shell-code start by loading libraries and importing modules then it pushes the below names letter by letter to memory:

- ka9zcqw3l6l48a1uuba.
- ratotpvvsmo.exe.
- gswccl.
- hhtktvn.

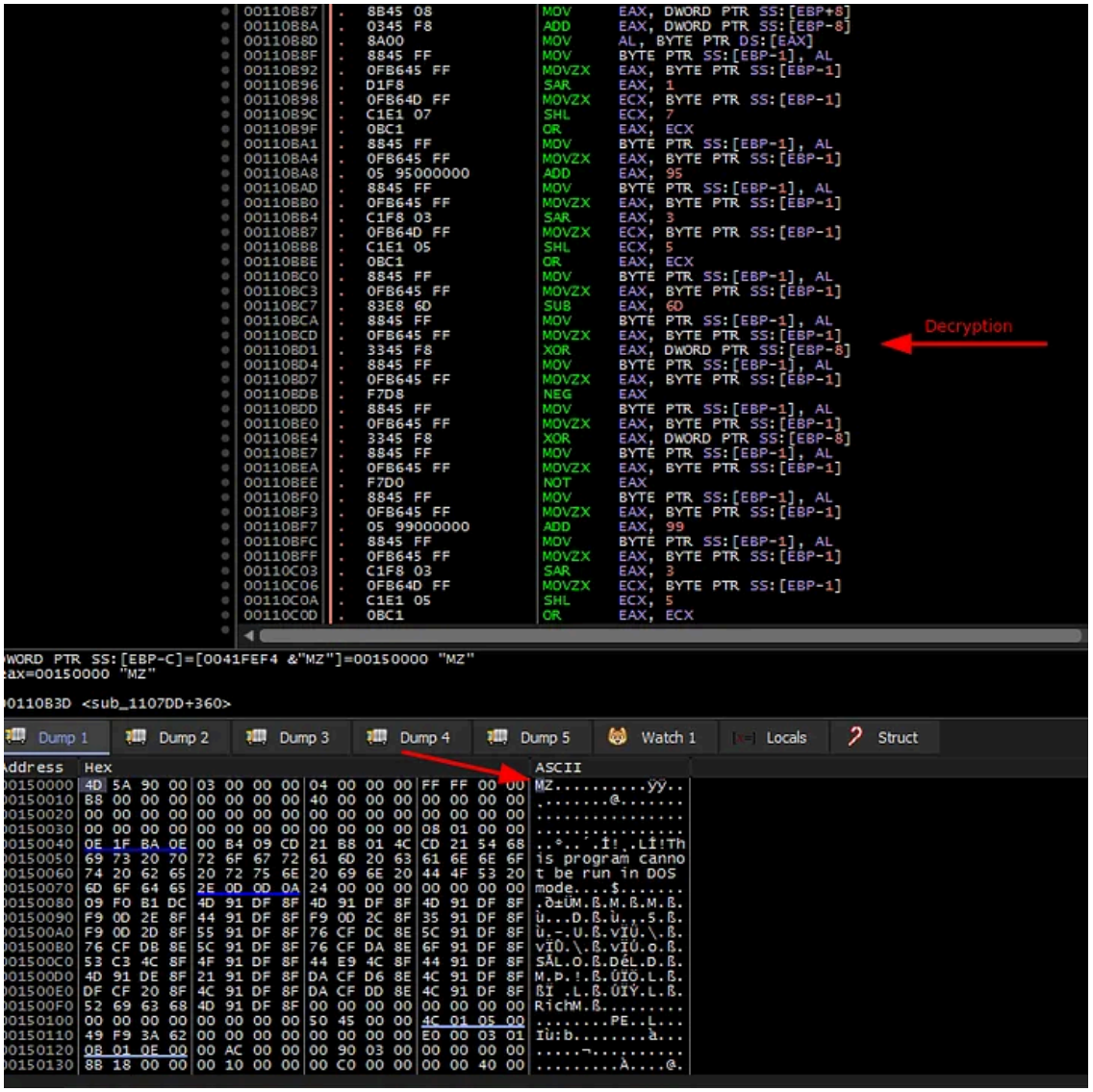
after that it opens “**ka9zcqw3l6l48a1uuba”** file from the %TEMP% folder to get handle of it then get the file size, allocate memory, read file and decrypt the data read from the file, so I dumped it to a file to be analyzed later:

Press enter or click to view image in full size



The buffer that receives the data read from file “**ka9zcqw3l6l48a1uuba**”

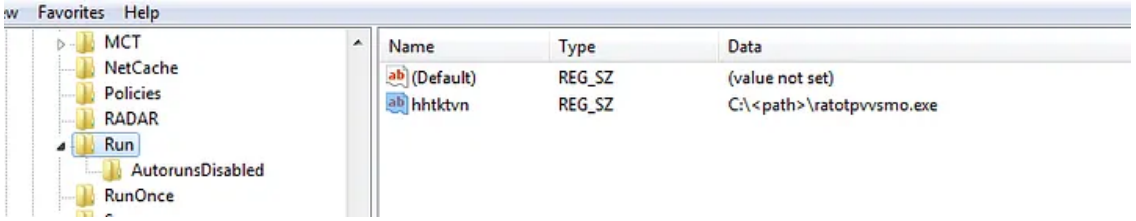
Press enter or click to view image in full size



x64dbg: After decrypting data

After that it creates a folder with name “**gswccl**” in “C:\<USER>\AppData\Roaming” and creates a file named “**ratotpvvsmo.exe**” in it and use this file as persistence technique by changing the auto run value in the registry “HKCU\SOFTWARE\Micorsoft\Windows\CurrentVersion\Run” with name “**hhtktvn**” :

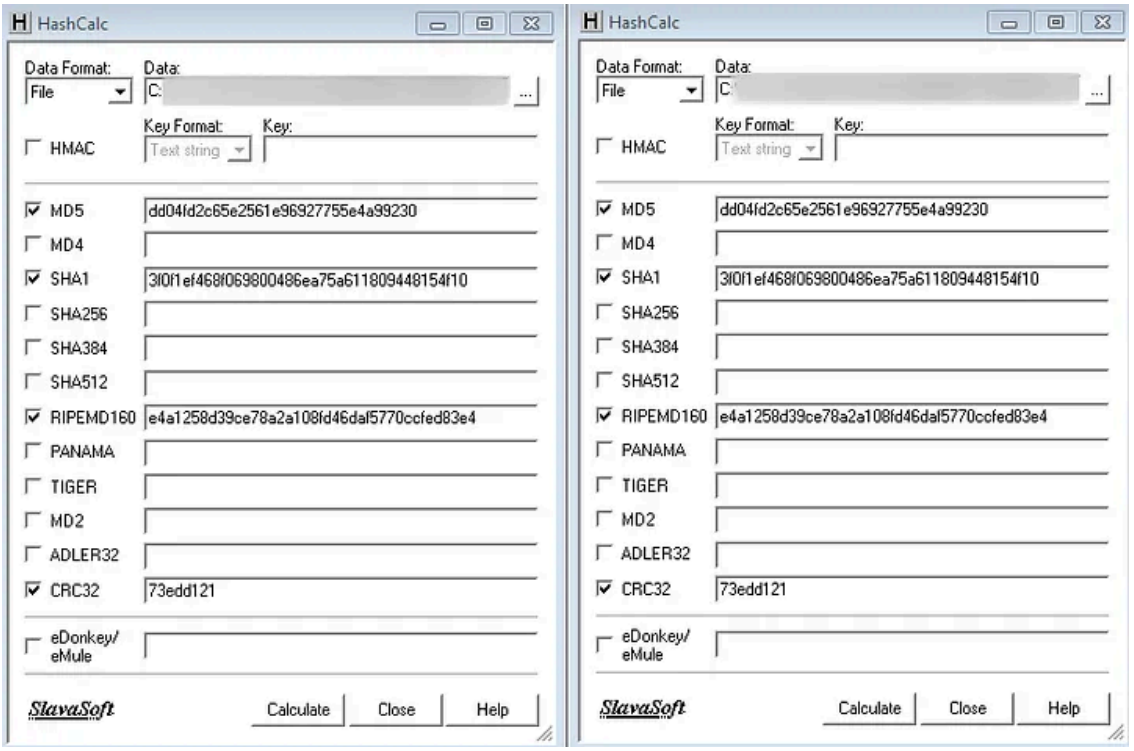
Press enter or click to view image in full size



Registry new value; path to executable was changed for the snapshot

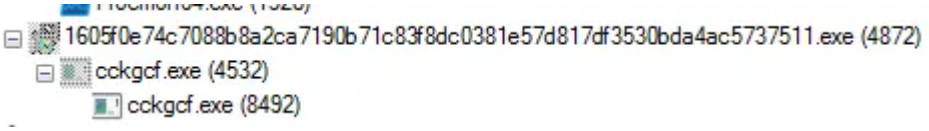
and by fast look at that “**ratotpvvsmo.exe”** we see that it is a copy of **“ccgkcf.exe” executable:**

Press enter or click to view image in full size



HashCalc: comparison for **ccgkcf.exe and ratotpvvsmo.exe**

Proceeding with the analysis we see that it create a new process with it's name and inject the code the was decrypted from the "**ka9zcqw3l6l48a1uuba**" file to it and exit the process



Procmon: process injection

What also worth to mention that it uses "Havens gate" technique which refer to far return, to switch to the 64bit mode, also It can be used as an anti reverse engineering technique for protecting the malware.

From Infosec Writeups: A lot is coming up in the Infosec every day that it's hard to keep up with. [Join our weekly newsletter](#) to get all the latest Infosec trends in the form of 5 articles, 4 Threads, 3 videos, 2 Github Repos and tools, and 1 job alert for FREE!

Source: https://medium.com/@M3HS1N/malware-analysis-nanocore-rat-6cae8c6df918