DCRAT malware Evades SandBox that use Fake Internet by using the Google public DNS IP address....

Published: 2019-10-02 · Archived: 2026-04-05 22:05:31 UTC

In past few days, I saw a nice post by @James_inthe_box regarding DCRAT malware, that may do several thing base on the IOC strings he shared in that post. I fetch it today and I found a interesting technique it use to evade sandbox that using fake internet to spoof internet connection for malware analysis.
https://twitter.com/James_inthe_box/status/1178275531692756992?s=20

figure 3: The digital signature of daaca.exe

The Evasion Technique:

the obfuscated code start by decrypting the initial API it needs and also the google public host name to fetch the DNS information of it later.

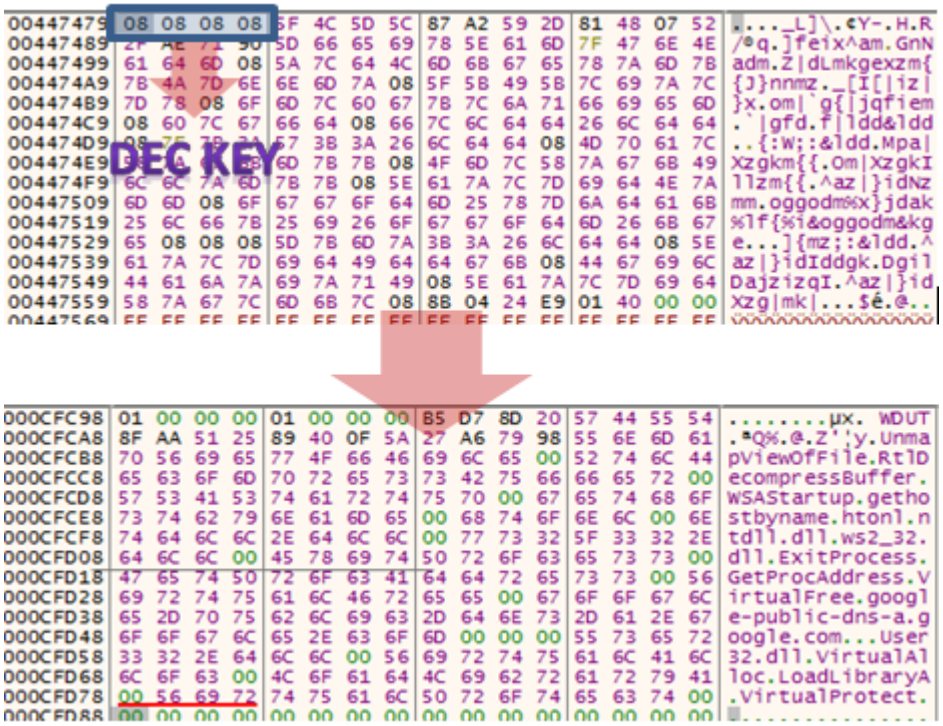

figure 4: initial API and the google public host name string

Then it will resolve all the API and do **gethostbyname** to the google public domain name *"google-public-dns-a.google.com"* to retrieve its DNS information and used the **h_addr_list** to decrypt the code that will decompress the DCloader and its .DLL component

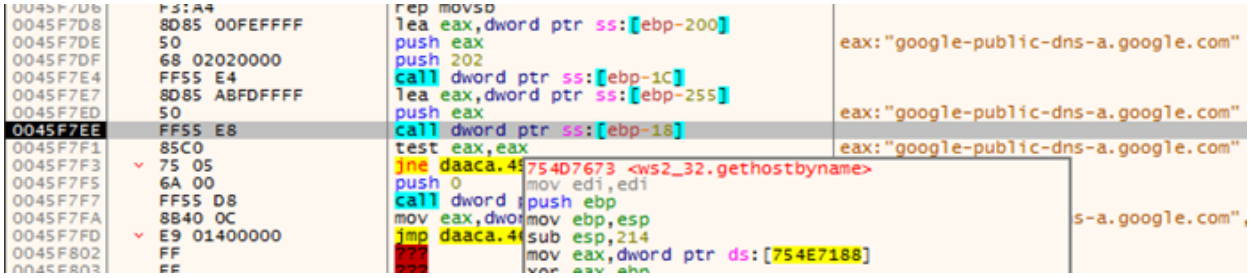

figure 5: retrieving DNS information to the google public dns domain name.

The decrypted code will load 2 Virtual Allocated memories to decompress its code using **RtlDecompressBuffer** Api.

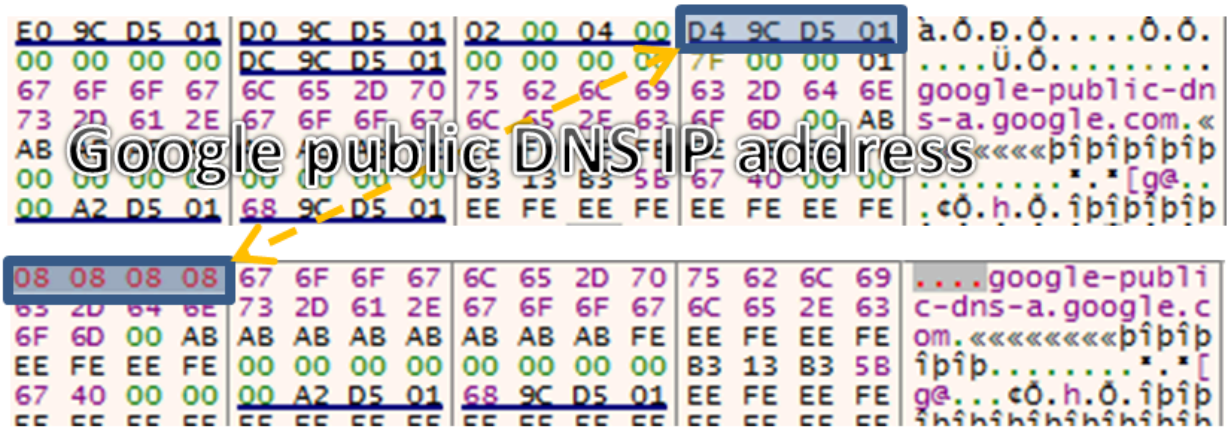

figure 6 : retrieving hostent of the google public DNS

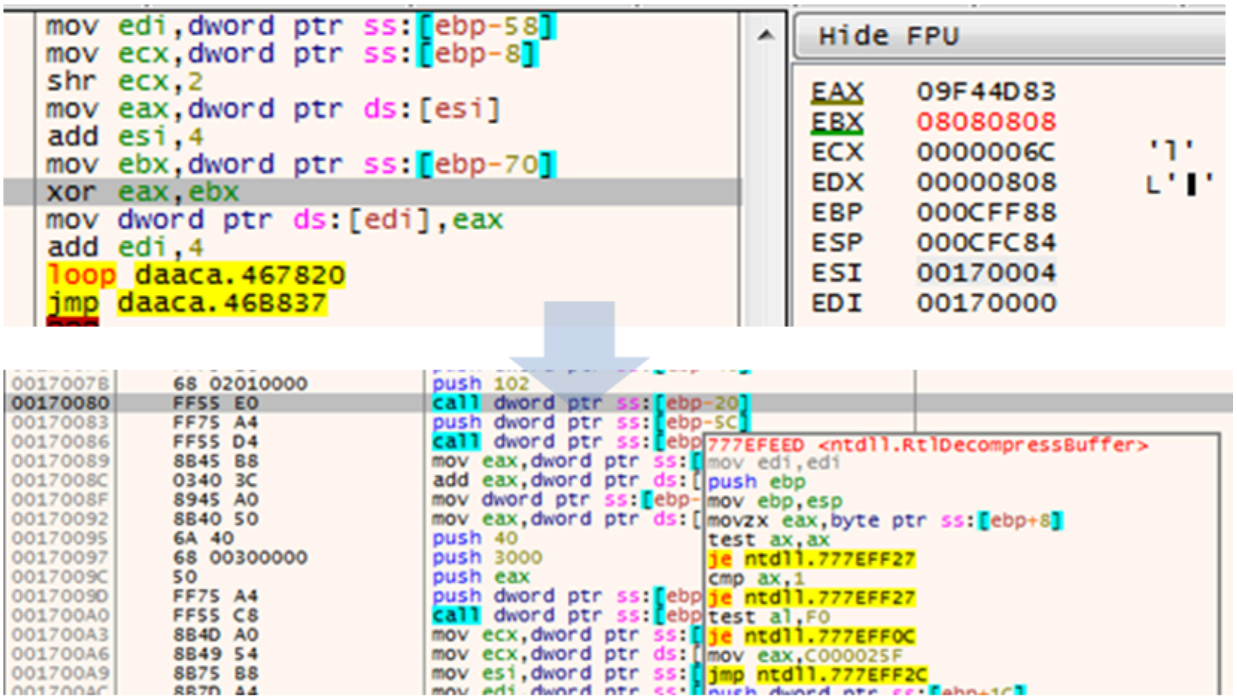

figure 7: decompressing the dcrat malware

The decrypted DCRAT consist of a loader and 2 .dll (32 bit & 64 bit) that will be injected to explorer.exe.

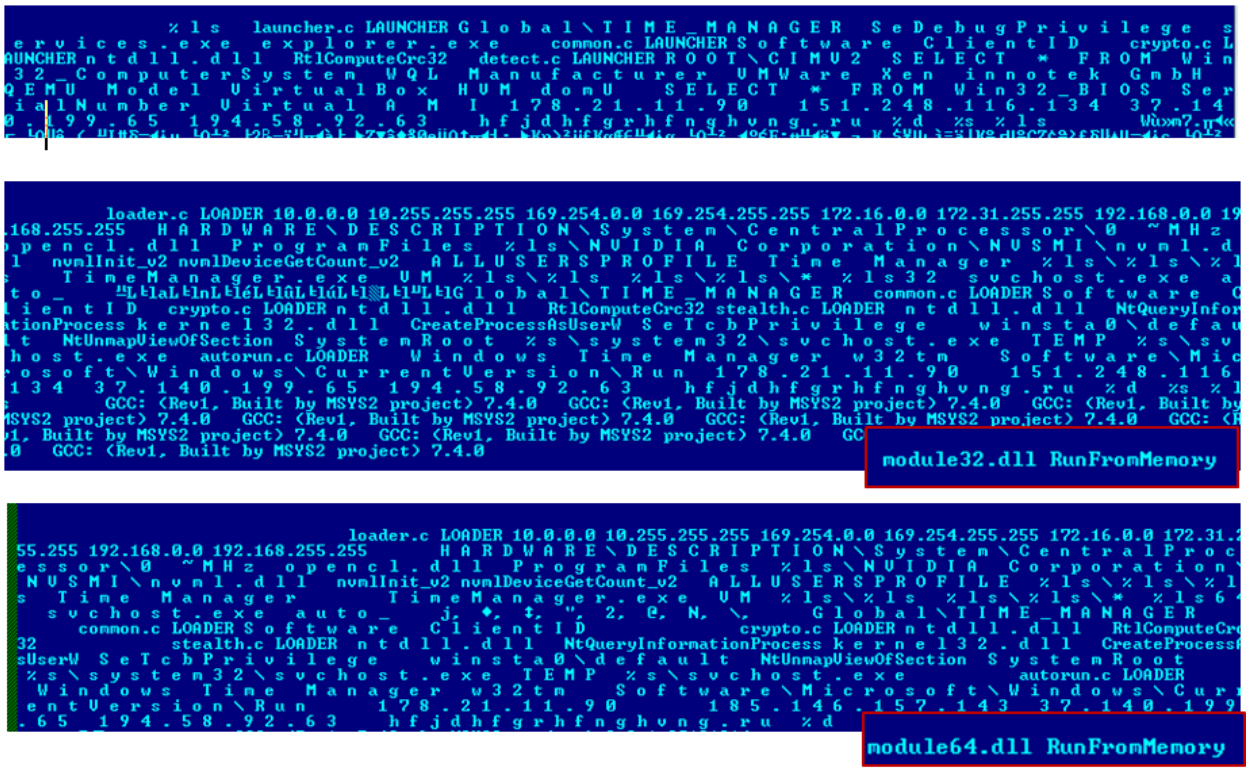

figure 8: DCRAT malware

Conclusion:

This malware show a simple way how to detect internet connection during its execution and also evading the sandbox that are using fake internet. I know that this trick is quite easy to overcome by malware analyst but good to know to improve automation and blackbox testing. :)

sha1:563d9f1b35b4898d16aff1dccd8969299f7ab8b7
md5: b478d340a787b85e086cc951d0696cb1

IOC and strings:

35840:%ls
35866:RGlobal\TIME_MANAGER
35908:SeDebugPrivilege
35942:services.exe
35968:explorer.exe
36012:RSoftware
36032:ClientID
36068:Rntdll.dll
36124:RROOT\CIMV2
36148:SELECT * FROM Win32_ComputerSystem
36218:WQL
36226:Manufacturer

36252:VMWare
36266:Xen
36274:innotek GmbH
36300:QEMU
36310:Model
36322:VirtualBox
36344:HVM domU
36364:SELECT * FROM Win32_BIOS
36414:SerialNumber
36440:Virtual
36456:A M I
36468:178.21.11.90
36496:151.248.116.134
36528:37.140.199.65
36556:194.58.92.63
36584:hfjdhfgrhfnghvng.ru
36634:%ls
105220:HARDWARE\DESCRIPTION\System\CentralProcessor\0
105314:~MHz
105324:opencl.dll
105346:ProgramFiles
105372:%ls\NVIDIA Corporation\NVSMI\nvml.dll
105484:ALLUSERSPROFILE
105516:Time Manager
105542:%ls\%ls\%ls
105568:TimeManager.exe
105606:%ls\%ls
105622:%ls\%ls*
105642:%ls32
105654:svchost.exe
105678:auto_
105724:Global\TIME_MANAGER
105778:RSoftware
105798:ClientID
105830:Rntdll.dll
105886:ntdll.dll
105930:skernel32.dll
105980:SeTcbPrivilege
106012:winsta0\default
106066:SystemRoot
106088:%s\system32\svchost.exe
106136:TEMP

106146:%s\svchost.exe
106196:Windows Time Manager
106238:w32tm
106252:Software\Microsoft\Windows\CurrentVersion\Run
106344:178.21.11.90
106372:151.248.116.134
106404:37.140.199.65
106432:194.58.92.63
106460:hfjdhfgrhfnghvng.ru
106510:%ls
183048:HARDWARE\DESCRIPTION\System\CentralProcessor\0
183142:~MHz
183152:opencl.dll
183174:ProgramFiles
183200:%ls\NVIDIA Corporation\NVSMI\nvml.dll
183312:ALLUSERSPROFILE
183344:%ls\%ls\%ls
183368:Time Manager
183400:TimeManager.exe
183438:%ls\%ls
183454:%ls\%ls*
183474:%ls64
183486:svchost.exe
183510:auto_
183560:Global\TIME_MANAGER
183622:RSoftware
183642:ClientID
183686:Rntdll.dll
183754:ntdll.dll
183798:skernel32.dll
183848:SeTcbPrivilege
183880:winsta0\default
183934:SystemRoot
183960:%s\system32\svchost.exe
184008:TEMP
184018:%s\svchost.exe
184080:Windows Time Manager
184122:w32tm
184136:Software\Microsoft\Windows\CurrentVersion\Run
184232:178.21.11.90
184264:185.146.157.143
184296:37.140.199.65

184324:194.58.92.63
184352:hfjdhfgrhfnghvng.ru
184402:%ls

Source: https://tccontre.blogspot.com/2019/10/dcrat-malware-evades-sandbox-that-use.html