

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.

```

00447479 08 08 08 08 5F 4C 5D 5C 87 A2 59 2D 81 48 07 52 .....L]\.eY-.H.R
00447489 27 AE 71 90 5D 66 65 69 78 5E 61 6D 7F 47 6E 4E ./q.}feix^am.GnN
00447499 61 64 6D 08 5A 7C 64 4C 6D 68 67 65 78 7A 6D 78 adm.Z|dLmkgeXzm{
004474A9 78 4A 7D 6E 6E 6D 7A 08 5F 5B 49 5B 7C 69 7A 7C {J}nmz._[I[|iz|
004474B9 7D 78 08 6F 6D 7C 60 67 7B 7C 6A 71 66 69 65 6D }x.om|'g{|jqfiem
004474C9 08 60 7C 67 66 64 08 66 7C 6C 64 64 26 6C 64 64 .|gfd.f|ldd&ldd
004474D9 08 7E 7B 7A 67 3B 3A 26 6C 64 64 08 4D 70 61 7C ..{:w;:&ldd.Mpa|
004474E9 08 7E 7B 7A 67 3B 3A 26 6C 64 64 08 4D 70 61 7C Xzgm{|.Om|XzgmI
004474F9 6C 6C 7A 6D 78 7B 08 5E 61 7A 7C 7D 69 64 4E 7A llzm{|.^az|}idnz
00447509 6D 6D 08 6F 67 67 6F 64 6D 25 78 7D 6A 64 61 6B mm.oggodm{x}jdkz
00447519 25 6C 66 7B 25 69 26 6F 67 67 6F 64 6D 26 6B 67 %lf{%i&oggodm&kg
00447529 65 08 08 08 5D 7B 6D 7A 3B 3A 26 6C 64 64 08 5E e...}|mz;:&ldd.^
00447539 61 7A 7C 7D 69 64 49 64 64 67 6B 08 44 67 69 6C az|}idlddgk.Dgil
00447549 44 61 6A 7A 69 7A 71 49 08 5E 61 7A 7C 7D 69 64 DajzizqI.^az|}id
00447559 58 7A 67 7C 6D 6B 7C 08 8B 04 24 E9 01 40 00 00 Xzgm|mk|...se.@..
00447569 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```

↓

```

000CFC98 01 00 00 00 01 00 00 00 B5 D7 8D 20 57 44 55 54 .....µx. WDUT
000CFCAB 8F AA 51 25 89 40 0F 5A 27 A6 79 98 55 6E 6D 61 .*Q%.@.Z'|y.Unma
000CFCB8 70 56 69 65 77 4F 66 46 69 6C 65 00 52 74 6C 44 pviewOfFile.RtID
000CFC8 65 63 6F 6D 70 72 65 73 73 42 75 66 66 65 72 00 ecompressBuffer.
000CFC08 57 53 41 53 74 61 72 74 75 70 00 67 65 74 68 6F WSASStartup.getho
000CFC8 73 74 62 79 6E 61 6D 65 00 68 74 6F 6E 6C 00 6E stbyname.hton1.n
000CFCF8 74 64 6C 6C 2E 64 6C 6C 00 77 73 32 5F 33 32 2E tdll.dll.ws2_32.
000CFD08 64 64 6C 00 45 78 69 74 50 72 6F 63 65 73 73 00 dll.ExitProcess.
000CFD18 47 65 74 50 72 6F 63 41 64 64 72 65 73 73 00 56 GetProcAddress.V
000CFD28 69 72 74 75 61 6C 46 72 65 65 00 67 6F 6F 67 6C irtualFree.google
000CFD38 65 2D 70 75 62 6C 69 63 2D 64 6E 73 2D 61 2E 67 e-public-dns-a.g
000CFD48 6F 6F 67 6C 65 2E 63 6F 6D 00 00 00 55 73 65 72 oogle.com...User
000CFD58 33 32 2E 64 6C 6C 00 56 69 72 74 75 61 6C 41 6C 32.dll.VirtualAl
000CFD68 6C 6F 63 00 4C 6F 61 64 4C 69 62 72 61 72 79 41 loc.LoadLibraryA
000CFD78 00 56 69 72 74 75 61 6C 50 72 6F 74 65 63 74 00 .VirtualProtect.
000CFD88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

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

```

0045F7D6 F3:A4 rep movsd
0045F7D8 8D85 00FEFFFF lea eax,dword ptr ss:[ebp-200]
0045F7DE 50 push eax
0045F7DF 68 02020000 push 202
0045F7E4 FF55 E4 call dword ptr ss:[ebp-1C]
0045F7E7 8D85 ABDFFFFF lea eax,dword ptr ss:[ebp-255]
0045F7ED 50 push eax
0045F7EE FF55 E8 call dword ptr ss:[ebp-18]
0045F7F1 85C0 test eax,eax
0045F7F3 75 05 jne daaca.45754D7673 <ws2_32.gethostbyname>
0045F7F5 6A 00 push 0
0045F7F7 FF55 D8 call dword ptr ss:[ebp-18]
0045F7FA 8B40 0C mov eax,dword ptr ds:[754E7188]
0045F7FD E9 01400000 jmp daaca.45754D7673 <ws2_32.gethostbyname>
0045F802 FF var eax,ah
0045F803 FF

```

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.

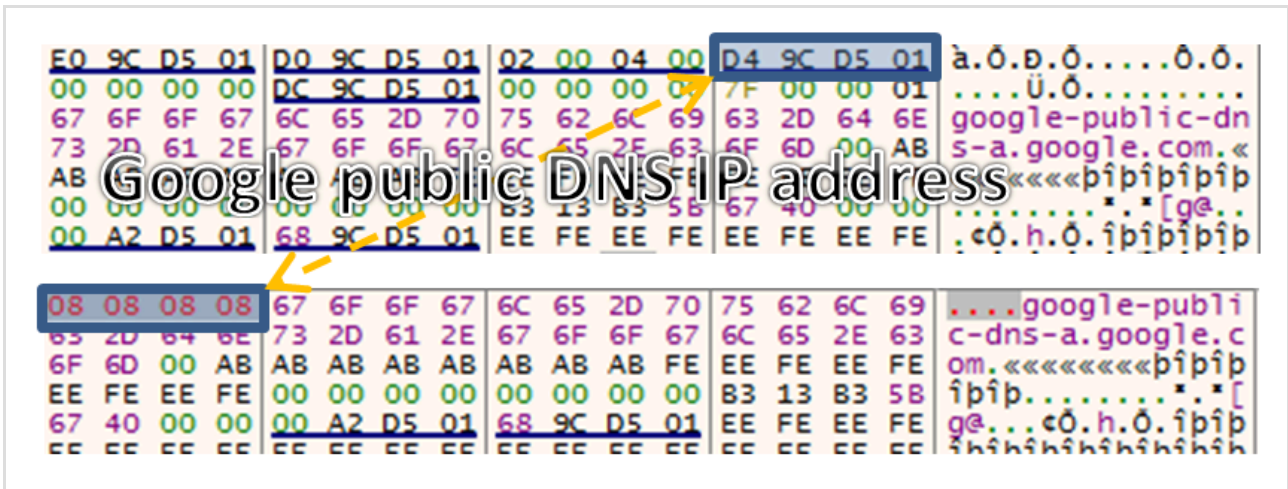


figure 6 : retrieving hostent of the google public DNS

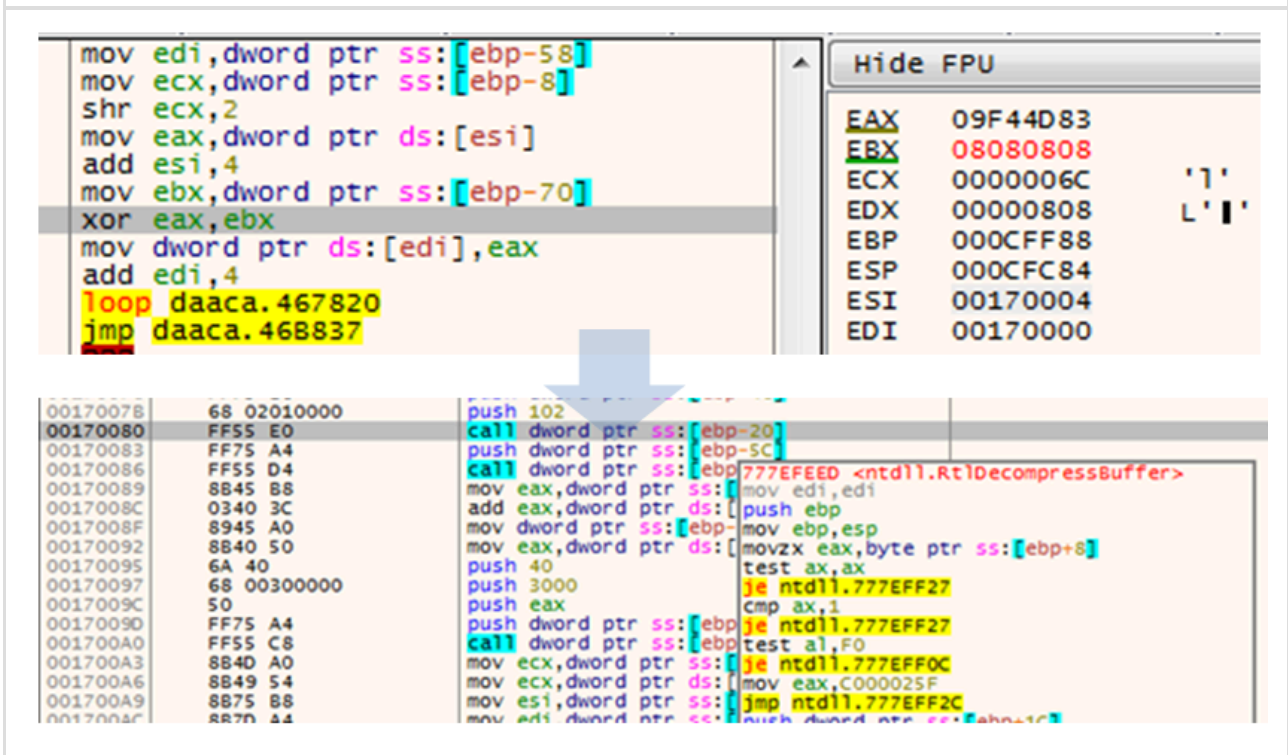


figure 7: decompressing the dcrat malware

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

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:hjdhfgrhfnghvng.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:hfjdhfgrhfngvhng.ru

184402:%ls

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