

NUKESPED TEKNİK ANALİZİ



İÇİNDEKİLER

GİRİŞ	3
Yüklediği DLL'ler	4
API Obfuscation	4
API Obfuscation	6
API Hammering.....	7
Sistem Bilgisi Alma	9
Bağlantı Kurduğu Adresler.....	11
Mitre Att&ck Tablosu.....	16
Çözüm Önerileri	18

GİRİŞ

Lazarus Apt grubuna ait NukeSped zararlı yazılımı, bir uzaktan erişim Truva atı olan (RAT-Remote Access Trojan) bu kötü yazılım örnekleri , 32 bit sistemler için derlendiği için birden fazla özelliği paylaştığını ortaya koymaktadır. Ayrıca, analizleri engellemek için şifreli dizeler içermektedirler. Kötü amaçlı yazılım, işlevleri dinamik olarak çözmektedir. Ayrıca, işe aktarma tablosunun kısa olduğu ve az sayıda ortak DLL ve işlevi işe aktardığı bulunmaktadır.

Birçok Kuzey Kore hacker grubu tarafından yazılan ve bu gruplardan en bilineni olan Lazarus'a kod kullanımıyla birlikte bağladılar ve bu bağlantıyı güçlendirdiler. Kötü amaçlı yazılımın temel işlevi, saldırganlara virüslü ana bilgisayarın uzaktan yönetimine izin vermektir. Sistem içerisinde analizi zorlaştırırken her API ismini şifrelemekte olup bunları API hammering yöntemiyle hafızasını doldururken Sandboxlarda analizini engellemektedir.

Dosya İsmi	n5JNGFT14Q.exe
MD5	fdc66cdabd46bc3b26aba4e59943726b
SHA1	c341002cc5f9214cc8fd71e633efef673267d1fd
SHA256	5c2f339362d0cd8e5a8e3105c9c56971087bea2701ea3b7324771b0ea2c26c6c
İlk Görüldüğü Tarih	20.06.2021 10:36:59 UTC

Yüklediği DLL'ler

Zararlı yazılım öncelikle aşağıdaki dll'leri sisteme yüklemekte. Gerekli yüklemeyi yaptıktan sonra bütün API'ları kontrol edip gerekli API'ları encrypt işlemi yaparak kendi hafızasına yazmaktadır.

user32.dll	kernel32.dll	ntdll.dll
winsx.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

Zararlı yazılım **GetModuleHandleW** API ile belirtilen modüle handle alıp içerisinden API çağırmakta olup API'ları kontrol etmektedir. Ardından **GetProcAddress** yardımıyla API isimlerini hafızaya yazmaktadır.

000000013F11ACFC	48:83	push rbx	
000000013F11AD01	48:83EC 20	sub rsp,20	
000000013F11AD02	48:8D0D FFD20000	lea rcx,qword ptr ds:[13F128008]	000000013F128008:"kerne32.dll"
000000013F11AD09	FF15 99C40000	call qword ptr ds:[<&GetModuleHandleW]	
000000013F11AD0F	48:8D15 12D30000	lea rdx,qword ptr ds:[13F128028]	000000013F128028:"F1sA11oc"
000000013F11AD16	48:89C8	mov rcx,rcx	
000000013F11AD19	48:8D08	mov rbx,rcx	
000000013F11AD1C	FF15 5EC30000	call qword ptr ds:[<&GetProcAddress]	
000000013F11AD22	48:8D15 0FD30000	lea rdx,qword ptr ds:[13F128038]	000000013F128038:"F1sFree"
000000013F11AD29	48:89C8	mov rcx,rbx	
000000013F11AD2C	48:3305 CD720100	xor rcx,qword ptr ds:[13F132000]	
000000013F11AD33	48:8905 26A80100	mov qword ptr ds:[13F135560],rcx	
000000013F11AD3A	FF15 40C30000	call qword ptr ds:[<&GetProcAddress]	
000000013F11AD40	48:8D15 F9D20000	lea rdx,qword ptr ds:[13F128040]	000000013F128040:"F1sGetValue"
000000013F11AD47	48:3305 82720100	xor rcx,qword ptr ds:[13F132000]	
000000013F11AD4E	48:89C8	mov rcx,rbx	
000000013F11AD51	48:8905 10A80100	mov qword ptr ds:[13F135568],rcx	
000000013F11AD58	FF15 22C30000	call qword ptr ds:[<&GetProcAddress]	
000000013F11AD5E	48:8D15 EBD20000	lea rdx,qword ptr ds:[13F128050]	000000013F128050:"F1sSetValue"
000000013F11AD65	48:3305 94720100	xor rcx,qword ptr ds:[13F132000]	
000000013F11AD6C	48:89C8	mov rcx,rbx	
000000013F11AD6F	48:8905 FAA70100	mov qword ptr ds:[13F135570],rcx	
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 rcx,qword ptr ds:[13F132000]	
000000013F11AD8A	48:89C8	mov rcx,rbx	
000000013F11AD8D	48:8905 E4A70100	mov qword ptr ds:[13F135578],rcx	
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 rcx,qword ptr ds:[13F132000]	
000000013F11ADA8	48:89C8	mov rcx,rbx	
000000013F11ADA8	48:8905 CEA70100	mov qword ptr ds:[13F135580],rcx	
000000013F11ADB2	FF15 C8C20000	call qword ptr ds:[<&GetProcAddress]	
000000013F11ADB8	48:8D15 D1D20000	lea rdx,qword ptr ds:[13F128090]	000000013F128090:"CreateSemaphoreEXW"
000000013F11ADB8	48:3305 3A720100	xor rcx,qword ptr ds:[13F132000]	
000000013F11ADC6	48:89C8	mov rcx,rbx	
000000013F11ADC9	48:8905 88A70100	mov qword ptr ds:[13F135588],rcx	
000000013F11ADD0	FF15 AAC20000	call qword ptr ds:[<&GetProcAddress]	
000000013F11ADD6	48:8D15 CBD20000	lea rdx,qword ptr ds:[13F1280A8]	000000013F1280A8:"SetThreadStackGuarantee"
000000013F11ADD0	48:3305 1C720100	xor rcx,qword ptr ds:[13F132000]	
000000013F11ADE4	48:89C8	mov rcx,rbx	
000000013F11ADE7	48:8905 A2A70100	mov qword ptr ds:[13F135590],rcx	
000000013F11ADEE	FF15 8CC20000	call qword ptr ds:[<&GetProcAddress]	
000000013F11ADF4	48:8D15 C5D20000	lea rdx,qword ptr ds:[13F1280C0]	000000013F1280C0:"CreateThreadPoolTimer"
000000013F11ADF8	48:3305 5E720100	xor rcx,qword ptr ds:[13F132000]	

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      48:8BC8     mov     rcx,rbx
000000013F5F41AE      E8:82F5FFFF call    apt.13F5F3790
000000013F5F41B1      48:8BC8     mov     rcx,rbx
000000013F5F41B4      FF15 D12E0100 call   qword ptr ds:[<&LoadLibraryA]
000000013F5F41B7      48:8BC8     mov     rcx,rbx
000000013F5F41BA      48:8BF8     mov     rdi,rbx
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 jg     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 63A80100 lea    rcx,qword ptr ds:[13F60ED40]
000000013F5F41DD      8975 30     mov     dword ptr ss:[rbp+30],esi
000000013F5F41E5      E8 2BF5FFFF call    apt.13F5F4010
000000013F5F41E8      48:8BC8     mov     edx,dword ptr ss:[rbp+30]
000000013F5F41EB      48:8BC8     mov     rcx,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,rbx
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      48:8D0D 44A80100 lea    rcx,qword ptr ds:[13F60ED60]
000000013F5F421C      8975 30     mov     dword ptr ss:[rbp+30],esi
000000013F5F421F      E8 ECFDFFFF call    apt.13F5F4010
000000013F5F4224      48:8BC8     mov     edx,dword ptr ss:[rbp+30]
000000013F5F4227      48:8BC8     mov     rcx,rbx
000000013F5F422A      48:8BD8     mov     rbx,rbx
000000013F5F422D      E8 5E15FFFF 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,rbx
000000013F5F4241      48:8905 B8120200 mov     qword ptr ds:[<&LoadLibraryA],rax
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 25A80100 lea    rcx,qword ptr ds:[13F60ED80]
000000013F5F4258      8975 30     mov     dword ptr ss:[rbp+30],esi
000000013F5F425E      E8 AD15FFFF call    apt.13F5F4010
000000013F5F4263      8B55 30     mov     edx,dword ptr ss:[rbp+30]
000000013F5F4266      48:8BC8     mov     rcx,rbx

```

Tüm API'ları şifreleyip eşleşen API'ları tek tek çağırılmaktadır. Zararlı yazılım **GetProcAddress** ile çağırıldığı API'ları kendi hafızasına yüklemektedir.

```

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,rbx
000000013F5F4241      48:8905 B8120200 mov     qword ptr ds:[<&LoadLibraryA],rax
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 25A80100 lea    rcx,qword ptr ds:[13F60ED80]
000000013F5F4258      8975 30     mov     dword ptr ss:[rbp+30],esi
000000013F5F425E      E8 AD15FFFF call    apt.13F5F4010
000000013F5F4263      8B55 30     mov     edx,dword ptr ss:[rbp+30]
000000013F5F4266      48:8BC8     mov     rcx,rbx
000000013F5F4269      48:8BD8     mov     rbx,rbx
000000013F5F426C      E8 1F15FFFF call    apt.13F5F3790
000000013F5F4271      48:8BD3     mov     rdx,rbx
000000013F5F4274      48:8BCF     mov     rcx,rDI
000000013F5F4277      FF15 83110200 call   qword ptr ds:[<&GetProcAddress]
000000013F5F427D      48:8BC8     mov     rcx,rbx
000000013F5F4280      48:8905 59110200 mov     qword ptr ds:[<&GetProcAddress],rax
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 06A80100 lea    rcx,qword ptr ds:[13F60EDA0]
000000013F5F429A      8975 30     mov     dword ptr ss:[rbp+30],esi
000000013F5F429D      E8 6E15FFFF call    apt.13F5F4010
000000013F5F42A1      8B55 30     mov     edx,dword ptr ss:[rbp+30]
000000013F5F42A5      48:8BC8     mov     rcx,rbx
000000013F5F42A8      48:8BD8     mov     rbx,rbx
000000013F5F42AB      E8 0FA5FFFF call    apt.13F5F3790
000000013F5F42B0      48:8BD3     mov     rdx,rbx
000000013F5F42B3      48:8BCF     mov     rcx,rDI
000000013F5F42B6      FF15 74110200 call   qword ptr ds:[<&GetProcAddress]
000000013F5F42BC      48:8BC8     mov     rcx,rbx
000000013F5F42BF      48:8905 B2110200 mov     qword ptr ds:[<&ole32.dll],rax
000000013F5F42C6      E8 55100000 call    apt.13F5F5320
000000013F5F42CB      4C:8D45 30   lea    r8,qword ptr ss:[rbp+30]
000000013F5F42D0      8D56 10     lea    edx,qword ptr ds:[rsi+10]
000000013F5F42D2      48:8D0D E7AA0100 lea    rcx,qword ptr ds:[13F60EDC0]
000000013F5F42D9      8975 30     mov     dword ptr ss:[rbp+30],esi
000000013F5F42DC      E8 2FD5FFFF call    apt.13F5F4010
000000013F5F42E1      8B55 30     mov     edx,dword ptr ss:[rbp+30]
000000013F5F42E4      48:8BC8     mov     rcx,rbx
000000013F5F42E7      48:8BD8     mov     rbx,rbx
000000013F5F42EA      E8 1A15FFFF call    apt.13F5F3790
000000013F5F42EF      48:8BD3     mov     rdx,rbx
000000013F5F42F2      48:8BCF     mov     rcx,rDI
000000013F5F42F5      FF15 35110200 call   qword ptr ds:[<&GetProcAddress]
000000013F5F42FB      48:8BC8     mov     rcx,rbx

```


API Obfuscation

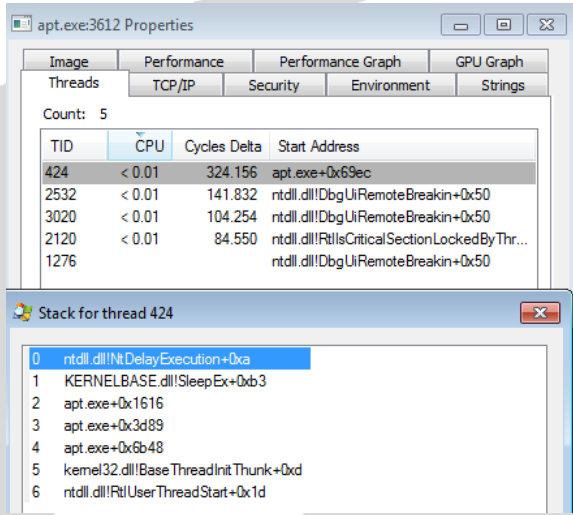
00000013F724C40	48:8BC8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
00000013F724C50	48:8BF8	mov rdi,rax	
00000013F724C53	ES:C060000	call apt.13F725320	
00000013F724C58	48:85FF	test rdi,rdi	
00000013F724C5B	OF84 E000000	je apt.13F724041	
00000013F724C61	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
00000013F724C65	48:8D0D 44A50100	lea rcx,qword ptr ds:[13F73F180]	rcx:"PeekMessage", 00000013F73F180:"11q2o2RU5RVRVH3J"
00000013F724C6C	BA 10000000	mov edx,10	
00000013F724C71	8975 30	mov dword ptr ss:[rbp+30],esi	
00000013F724C74	ES:97F3FFFF	call apt.13F724010	
00000013F724C79	8B55 30	mov edx,dword ptr ss:[rbp+30]	
00000013F724C7C	48:8BC8	mov rcx,rax	rcx:"PeekMessage"
00000013F724C7F	48:8BD8	mov rdx,rbx	rbx:"PeekMessage"
00000013F724C82	ES:09E8FFFF	call apt.13F723790	
00000013F724C87	48:8BD3	mov rdx,rbx	rbx:"PeekMessage"
00000013F724C8A	48:8BCF	mov rcx,rdi	rcx:"PeekMessage"
00000013F724C8D	FF15 90070200	call qword ptr ds:[&GetProcAddress]	
00000013F724C93	48:8BC8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
00000013F724C96	48:8905 B3070200	mov qword ptr ds:[13F745450],rax	
00000013F724C9D	E8 7E060000	call apt.13F725320	
00000013F724CA2	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
00000013F724CA6	48:8D0D 23A50100	lea rcx,qword ptr ds:[13F73F1D0]	rcx:"jky2uhoBuANYvw==", 00000013F20F1D0:"j02yp1pd9xNRnn3tg1WdQ=="
00000013F724CAD	BA 18000000	mov edx,18	
00000013F724CB2	8975 30	mov dword ptr ss:[rbp+30],esi	
00000013F724CB5	ES:56F3FFFF	call apt.13F724010	
00000013F724CBA	8B55 30	mov edx,dword ptr ss:[rbp+30]	
00000013F724CB8	48:8BC8	mov rcx,rax	rcx:"PeekMessage"
00000013F724CC0	48:8BD8	mov rdx,rbx	rbx:"PeekMessage"
00000013F724CC3	ES:C8EAF8FF	call apt.13F723790	
00000013F724CC8	48:8BD3	mov rdx,rbx	rbx:"PeekMessage"
00000013F724CCB	48:8BCF	mov rcx,rdi	rcx:"PeekMessage"
00000013F724CD0	FF15 5C070200	call qword ptr ds:[&GetProcAddress]	
00000013F724CD4	48:8BC8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
00000013F724CD7	48:8905 52080200	mov qword ptr ds:[13F745530],rax	
00000013F724CDE	E8 3D060000	call apt.13F725320	
00000013F724CE3	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
00000013F724CE7	48:8D0D 02A50100	lea rcx,qword ptr ds:[13F73F1F0]	rcx:"PeekMessage", 00000013F73F1F0:"n1aguEhF9Q95tmvtkFUur=="
00000013F724CEE	BA 18000000	mov edx,18	
00000013F724CF3	8975 30	mov dword ptr ss:[rbp+30],esi	
00000013F724CF6	ES:15F3FFFF	call apt.13F724010	
00000013F724CFB	8B55 30	mov edx,dword ptr ss:[rbp+30]	
00000013F724CFE	48:8BC8	mov rcx,rax	rcx:"PeekMessage"
00000013F724D01	48:8BD8	mov rdx,rbx	rbx:"PeekMessage"
00000013F724D04	ES:87EAF8FF	call apt.13F723790	
00000013F724D09	48:8BD3	mov rdx,rbx	rbx:"PeekMessage"
00000013F724D0C	48:8BCF	mov rcx,rdi	rcx:"PeekMessage"
00000013F724D0F	FF15 18070200	call qword ptr ds:[&GetProcAddress]	
00000013F724D15	48:8BC8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"

Şifrelediği API'ları hafızadan çağırıp kontrol ettikten sonra çözümleme işlemi yaparak tekrardan hafızasındaki listeye karşılaştırıp. Eğer kontrol edilen API doğru ise çözümlediği API'ları **GetProcAddress** API ile kendi hafızasına yüklemektedir.

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:[13F2DE020]	00000013F2DE020:"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 rdx,rbx	
013F2C41A9	E8 E2F5FFFF	call apt.13F2C3790	
013F2C41AE	48:8BCB	mov rcx,rbx	
013F2C41B1	FF15 D12E0100	call qword ptr ds:[&LoadLibraryA]	
013F2C41B7	48:8BC8	mov rcx,rbx	
013F2C41BA	48:8BF8	mov rdi,rbx	
013F2C41BD	E8 5E110000	call apt.13F2C5320	
013F2C41C2	44:8D76 01	lea r14,qword ptr ds:[rsi+1]	
013F2C41C6	48:85FF	test rdi,rdi	
013F2C41C9	OF84 4F0A0000	je apt.13F2C4C1E	
013F2C41CF	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
013F2C41D3	8D56 14	lea rcx,qword ptr ds:[rsi+14]	
013F2C41D6	48:8D0D 63AB0100	lea rcx,qword ptr ds:[13F2DE040]	00000013F2DE040:"nFqnmFte9SZQt2r7gk8="
013F2C41DD	8975 30	mov dword ptr ss:[rbp+30],esi	
013F2C41E0	E8 28FEFFFF	call apt.13F2C4010	
013F2C41E5	8B55 30	mov edx,dword ptr ss:[rbp+30]	
013F2C41E8	48:8BC8	mov rcx,rax	
013F2C41EB	48:8BD8	mov rdx,rbx	
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

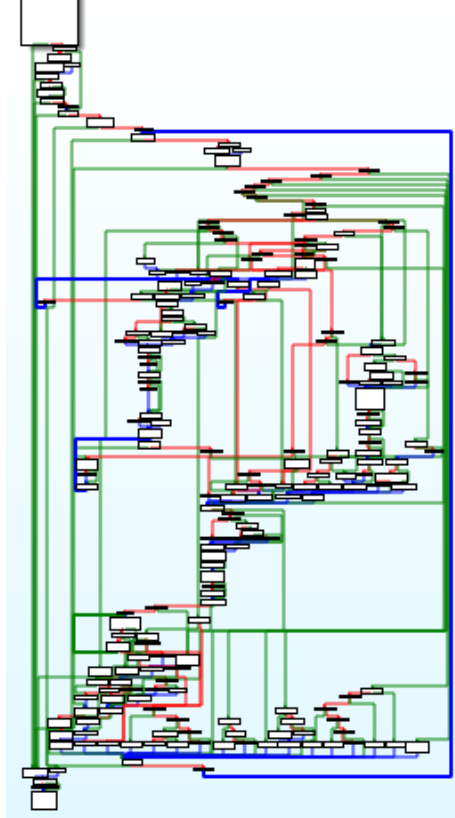
API hammering yöntemiyle birlikte zararlı yazılım kendisini oldukça fazla döngüye sokmaktadır ve ardından alanı çok fazla sayıda gereksiz bilgi ile doldurup sistemi yavaşlatmakta ve çağrı sürecini geciktirmektedir. Bu yöntem sayesinde Sandboxlarda zararlı kod analizi yaptırmamaktadır. Ve bu aşırı yüklenme ise sistem de DelayExecution hatası vermektedir.



Bu zararlı yazılımda verilebilecek belli başlı API hammering kullanılan API'lar:

GetProcAddress, LoadLibraryA, GetModuleHandleW.

Bu API'ları kullanarak sistem üzerinde yoğunluk ve gecikme oluşturup Sandboxlarda bu zararlı kodun çalışmasını engellemektedir.



Mutex Oluşturma

Assembly code snippet showing mutex creation logic:

```

mov qword ptr [rsp+10],rdx
mov qword ptr ss:[rsp+10],r9
push rbp
push rdi
sub rsp,50
and qword ptr ss:[rbp-30],0
mov rdi,rdx
xor edx,edx
mov rdx,rcx
lea rcx,qword ptr ss:[rbp-28]
lea r8d,qword ptr ss:[rdx+28]
call apt.13F497D00
test rdi,rdi
jnz apt.13F4952C0
call apt.13F497C7C
mov qword ptr [rax],i6
call apt.13F49623C
or eax,FFFFFFFF
jnz apt.13F495318
test rdx,rdx
jz apt.13F4952B8
lea r9,qword ptr ss:[rbp+30]
lea rcx,qword ptr ss:[rbp+30]
xor rdi,r8d
mov rdx,r8d
mov dword ptr ss:[rbp-28],7FFFFFFF
mov dword ptr ss:[rbp-30],42
mov qword ptr ss:[rbp+20],rbx
mov qword ptr ss:[rbp+30],rbx
call apt.13F4970C0
dec dword ptr ss:[rbp-28]
mov edx,edx
jz apt.13F495308
mov rcx,qword ptr ss:[rbp+30]
mov byte ptr ds:[rcx],0
jnz apt.13F495316
lea rdx,qword ptr ss:[rbp+30]
xor ecx,ecx
call apt.13F496E98
mov ecx,edx
add rsp,50
ret
    
```

Zararlı yazılım Microsoft32 adı altında bir adet mutex oluşturmakta ve bu mutex bilgisini şifreli şekilde hafızaya yazmaktadır.

Assembly code snippet showing mutex creation logic:

```

xor rax,rsip
mov qword ptr [rsp+1E0],rax
lea r9,qword ptr [13FFDE450]
xor edx,edx
xor ecx,ecx
call qword ptr ds:[<<CreateMutexA>]
call qword ptr ds:[<<GetLastError>]
cmp eax,8
jnz apt.13FFC1361
xor edx,edx
mov rcx,qword ptr ss:[rsp+1E0]
xor rcx,rsip
call apt.13FFC5260
add rsp,1F8
ret
call apt.13FFC4160
lea rcx,qword ptr [rcp+40]
    
```


Sistem Bilgisi Alma

Zararlı yazılım kullandığı bilgisayarın wi-fi bağdaştırıcısının model numarasını almakta ve kendi sistemi içerisine yazmaktadır.

Debugger window showing assembly code and hex dump. The assembly code includes instructions like `mov qword ptr ss:[rsp+68],rcx`, `rdi: \"9cx\", rdx: \"9cx\"`, and `call apt.13F2C7024`. The hex dump shows memory addresses from 00000000393E18 to 00000000393F28 with corresponding hex values and ASCII characters.

Giriş profilleri, girilen giriş dilinin ve girildiği klavyenin dilini ve bölgesinin otomatik olarak tanımlamasına yardımcı olmaktadır.

Debugger window showing assembly code and hex dump. The assembly code includes instructions like `xor r10,rci`, `mov ecx,r9d`, and `and edx,7f8`. The hex dump shows memory addresses from 00000000423E18 to 00000000423E40 with corresponding hex values and ASCII characters.

Event Altında Thread Başlatma

Zararlı yazılım “Global\\BFE_Notify_Event_{6585def3-da73-4483-a4ea-dd858969ee5f}” olay yürütme konfigürasyonu altında kontrol edip çalıştıracak olduğu thread’i bu komut satırı altından çalıştırmaktadır. Bu sayede analizini yapmayı zorlaştırmaktadır.

```
000007FEFABD3545 85C0 test eax, eax
000007FEFABD3547 0F85 31700000 jmp fwpuc1nt.7FEFABD457E
000007FEFABD354D 48:837C24 58 00 cmp qword ptr esi:[rsp+58], 0
000007FEFABD3553 0F85 89210000 jmp fwpuc1nt.7FEFABD56E4
000007FEFABD3559 4C:8D47 10 lea rsi, qword ptr ds:[rdi+10]
000007FEFABD355D 48:8D0D 34D00300 lea rcx, qword ptr ds:[7FEFAC10598]
000007FEFABD3564 3302 xor edx, edx
000007FEFABD3566 E8 8D000000 call fwpuc1nt.7FEFABD3628
000007FEFABD3568 48:8B08 mov rax, rax
000007FEFABD356E 48:85C0 test rax, rax
000007FEFABD3571 75 3A jmp fwpuc1nt.7FEFABD35AD
000007FEFABD3573 48:8D4F 20 lea rcx, qword ptr ds:[rdi+20]
000007FEFABD3577 E8 74DEFFFF call fwpuc1nt.7FEFABD13F0
000007FEFABD357F 48:8B08 mov rax, rax
000007FEFABD357F 48:85C0 test rax, rax
000007FEFABD3582 75 29 jmp fwpuc1nt.7FEFABD35AD
000007FEFABD3584 40:886F 50 mov byte ptr ds:[rdi+50], bl
000007FEFABD3588 4C:88424 68 mov r8, qword ptr esi:[rsp+68]
000007FEFABD358D 3302 xor edx, edx
000007FEFABD358F B9 00001000 mov ecx, 100000
000007FEFABD3594 FF15 86C0200 call qword ptr ds:[&OpenEventW]
000007FEFABD3594 48:8947 58 mov qword ptr ds:[rdi+58], rax
000007FEFABD359E 48:85C3 cmp rax, 0
000007FEFABD35A1 0F84 F96F0000 jmp fwpuc1nt.7FEFABD45A0
000007FEFABD35A7 49:89C24 mov qword ptr ds:[rdi], rdi
000007FEFABD35AB EB 00 jmp fwpuc1nt.7FEFABD35AD
000007FEFABD35AD 48:85F6 test rsi, rsi
000007FEFABD35B0 74 09 je fwpuc1nt.7FEFABD35BB
000007FEFABD35B2 48:8D4E 10 lea rcx, qword ptr ds:[rsi+10]
000007FEFABD35B6 E8 5DAFFFF call fwpuc1nt.7FEFABD20A0
000007FEFABD35B8 48:8D8C24 90000000 lea rcx, qword ptr esi:[rsp+90]
000007FEFABD35BC E8 48DAFFFF call fwpuc1nt.7FEFABD1010
000007FEFABD35C0 48:85C9 mov rcx, qword ptr esi:[rsp+90]
000007FEFABD35C0 48:85C9 test rcx, rcx
000007FEFABD35C4 48:85D8 jmp fwpuc1nt.7FEFABD5739
000007FEFABD35D9 48:8B08 mov rax, rax
000007FEFABD35DF 0F85 63210000 jmp fwpuc1nt.7FEFABD45D0
000007FEFABD35E4 48:85C0 mov rax, qword ptr esi:[rsp+68]
000007FEFABD35E4 48:898424 B0000000 mov qword ptr esi:[rsp+80], rax
000007FEFABD35E8 74 00 test rax, rax
000007FEFABD35E8 48:85C0 test rax, rax
000007FEFABD35F1 48:8D8C24 B0000000 lea rcx, qword ptr esi:[rsp+80]
000007FEFABD35F9 E8 12DAFFFF call fwpuc1nt.7FEFABD1010
000007FEFABD35FE 48:85DB test rax, rax
000007FEFABD3601 0F85 196E0000 jmp fwpuc1nt.7FEFABD45E4
```

Bağlantı Kurduğu Adresler

000000013F3713A9	4C:898424 F0010000	mov qword ptr [rsp+1F0],r14	
000000013F3713B1	E8 4A690000	call apt:13F377D00	
000000013F3713B5	48:8000 A33A0200	lea rcx,qword ptr ds:[13F394E60]	
000000013F3713B8	3302	xor edx,edx	
000000013F3713BF	41:58 04010000	mov r8d,104	
000000013F3713C5	E8 36690000	call apt:13F377D00	
000000013F3713CA	48:8000 9F380200	lea rcx,qword ptr ds:[13F394F70]	
000000013F3713D1	3302	xor edx,edx	
000000013F3713D3	41:58 04010000	mov r8d,104	
000000013F3713D9	E8 22690000	call apt:13F377D00	
000000013F3713DE	48:8010 8B3E0200	lea rcx,qword ptr ds:[13F3952A0]	
000000013F3713E5	3302	xor edx,edx	
000000013F3713E7	48:8BC8	mov rcx,rbx	
000000013F3713E9	41:58 04010000	mov r8d,104	
000000013F3713F0	E8 0B690000	call apt:13F377D00	
000000013F3713F5	33E0	xor ebp,ebp	
000000013F3713F7	4C:8D4424 30	lea rcx,qword ptr [rsp+30]	
000000013F3713FC	48:8000 5DD00100	lea rcx,qword ptr [13F38E460]	000000013F38E460: "BYR+jw2012ytc6b5Yv2Fe6wK1b7BuvROGh81p7KpQvBYntap7Vxw0R54K2n1W4E
000000013F371403	401400	lea rcx,qword ptr [ebp+44]	
000000013F371406	896C24 30	mov dword ptr [rsp+30],ebp	
000000013F37140A	E8 012C0000	call apt:13F374010	
000000013F37140F	48:884424 30	lea rcx,qword ptr [13F38E460]	
000000013F371414	48:88D0	mov rdx,rcx	
000000013F371417	48:8BC8	mov rcx,rcx	
000000013F37141A	4C:8BF0	mov r14,rcx	
000000013F37141D	E8 7E290000	call apt:13F3730A0	
000000013F371422	4C:8D4424 30	lea rcx,qword ptr [rsp+30]	
000000013F371427	8D55 44	lea rcx,qword ptr [rbp+44]	
000000013F37142A	48:8000 7FD00100	lea rcx,qword ptr [13F38E480]	000000013F38E480: "BYR+jw2012ytc6b5YSmVcStA/1FPn+FITXwYh01J10GFw5135QnuZ3JVPg/wA8i
000000013F371431	E8 0A2B0000	call apt:13F374010	
000000013F371436	48:884424 30	mov r8d,qword ptr [rsp+30]	
000000013F371438	48:8BC8	mov rcx,rcx	
000000013F37143E	48:8BC8	mov rcx,rcx	
000000013F371441	48:8BF0	mov r14,rcx	
000000013F371444	E8 37290000	call apt:13F3730A0	
000000013F371449	4C:8D4424 30	lea rcx,qword ptr [rsp+30]	
000000013F37144E	8D55 44	lea rcx,qword ptr [rbp+44]	
000000013F371451	48:8000 58D00100	lea rcx,qword ptr [13F38E480]	000000013F38E480: "BYR+jw2012ytc6b5YSmVcStA/1FPn+FITXwYh01J10GFw5135QnuZ3JVPg/wA8i
000000013F371458	E8 832B0000	call apt:13F374010	
000000013F371460	48:8000 7FD00100	lea rcx,qword ptr [rsp+30]	
000000013F371462	48:8BD0	mov rdx,rcx	
000000013F371465	48:8BC8	mov rcx,rcx	
000000013F371468	48:8BC8	mov rcx,rcx	

FCX=FFFFFFFF
qword ptr [000000013F38E460 "BYR+jw2012ytc6b5Yv2Fe6wK1b7BuvROGh81p7KpQvBYntap7Vxw0R54K2n1W4EUB="]-F32776A2B525962
.text:000000013F3713FC apt.exe:13FC #7FC

Encrypted halde tuttuğu URL bilgisini dinamik olarak çözümlenmektedir. Çözümlemiş URL bilgisi; **"mail[.]sisnet[.]co[.]kr/jsp/user/sms/sms_rcv_jsp"** çözümlendiği adrese bağlantı kurmaktadır. Bağlantı kurduktan sonra ise sistem üzerinde port açıp dinlemektedir.

000000013FDA3DAE	41:83 84	mov r11b,84	
000000013FDA3DB1	98 43902157	mov eax,57219043	
000000013FDA3DB6	41:89 C2A2A909	mov r9d,349AC2	
000000013FDA3DBC	40:85C0	test r8,r8	
000000013FDA3DBF	7E 7F	jmp apt:13FDA3E40	
000000013FDA3DC1	48:28DA	sub rdx,rdx	
000000013FDA3DC4	0F1F40 00	nop dword ptr ds:[rax],eax	
000000013FDA3DC8	48:8000 00000000	nop dword ptr ds:[rax+ax],eax	
000000013FDA3DD0	42:0F80C13	movzx ecx,byte ptr ds:[rbx+r10]	
000000013FDA3DD5	0F86D0	movzx edx,al	
000000013FDA3DE0	40:8052 01	lea r10,qword ptr ds:[r10+1]	
000000013FDA3DE3	41:32D3	xor dl,r11b	
000000013FDA3DE7	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	0F85C8	movzx ecx,al	
000000013FDA3DF0	41:32CB	and cl,r11b	
000000013FDA3DF4	44:0F86DA	movzx r11d,dl	
000000013FDA3E00	42:0F804C0 00000000	lea edx,qword ptr ds:[r9 8]	
000000013FDA3E03	41:33D1	xor edx,r9d	
000000013FDA3E06	44:32D9	mov r11b,cl	
000000013FDA3E09	41:88C9	mov ecx,r9d	
000000013FDA3E12	81E2 F8070000	and edx,r78	
000000013FDA3E15	C1E9 08	shr ecx,8	
000000013FDA3E18	C1E2 14	shl edx,14	
000000013FDA3E1B	44:8BCA	mov r9d,edx	
000000013FDA3E1D	801400	lea edx,qword ptr ds:[rax+rax]	
000000013FDA3E20	33D0	xor edx,edx	
000000013FDA3E22	44:08C9	or r9d,ecx	
000000013FDA3E25	C1E2 04	shl edx,4	
000000013FDA3E28	C1E1 07	shr ecx,7	
000000013FDA3E2A	83E2 80	xor edx,edx	
000000013FDA3E2D	33D1	and edx,FFFFFFF80	
000000013FDA3E30	88C8	mov ecx,ecx	
000000013FDA3E33	C1E2 11	shl edx,11	
000000013FDA3E36	C1E9 08	shr ecx,8	
000000013FDA3E39	88C2	mov eax,edx	
000000013FDA3E3B	08C1	or eax,ecx	
000000013FDA3E3E	49:FFC8	dec r8	
000000013FDA3E40	75 90	jmp apt:13FDA3D00	

edx=48 "H"
qword ptr [r9*8]=[92A27258]-???
.text:000000013FDA3DF8 apt.exe:3DF8 #31F8

Dokum1	Dokum2	Dokum3	Dokum4	Dokum5	İzle 1	[*] Yerel Değişkenler	Yapı	000000000016F718	00000000
Adres	hex	ASCII						000000000016F718	00000000
000000000022ADCO	60 00 33 00 32 00 5C 00 66 00 77 00 70 00 75 00	m.3.2.\.f.w.p.u.						000000000016F718	00000000
000000000022ADDB	63 00 6C 00 6E 00 74 00 2E 00 64 00 6C 00 6C 00	C.l.m.t...d.l.l.						000000000016F718	00000000
000000000022ADE0	00 00 00 00 00 00 00 00 FC 06 03 33 F7 00 00 88ü..3... ..						000000000016F718	00000000
000000000022ADFO	68 74 74 70 3A 2F 2F 6D 63 69 6C 2E 73 69 73 6E	http://mail.sisnet						000000000016F718	00000000
000000000022AE00	65 74 2E 63 6F 2E 68 72 2F 6A 73 70 2E 75 73 6E	et.co.kr/jsp/use						000000000016F718	00000000
000000000022AE10	72 2F 73 6D 73 2F 73 6D 73 5F 72 65 63 76 2E 6A	r/sms/sms_rcv_j						000000000016F718	00000000
000000000022AE20	70 00 00 00 00 00 00 00 00 00 64 00 6C 00 8C 00	sp...n.f...d.l.l.						000000000016F718	00000000
000000000022AE30	00 00 00 00 00 00 00 00 C1 06 03 33 F7 00 00 88ü..3... ..						000000000016F718	00000000
000000000022AE40	68 74 74 70 3A 2F 2F 6D 63 69 6C 2E 73 69 73 6E	http://mail.neoc						000000000016F718	00000000
000000000022AE50	79 6F 6E 2E 63 6F 6D 2F 6A 73 70 2F 75 73 65 72	yon.com/jsp/user						000000000016F718	00000000
000000000022AE60	2F 73 6D 73 2F 73 6D 73 5F 72 65 63 76 2E 6A 73	/sms/sms_rcv_js						000000000016F718	00000000
000000000022AE70	70 00 00 00 00 00 00 00 00 00 00 00 00 00 00	p.....						000000000016F718	00000000
000000000022AE80	00 00 00 00 00 00 00 CA 06 03 33 F7 00 00 88ü..3... ..						000000000016F718	00000000
000000000022AE90	68 74 74 70 3A 2F 8B 6C AD E9 BE 58 4A 68 C2 E6	http://1.6XV3kA						000000000016F718	00000000
000000000022AEA0	00 3F 05 F3 CD 78 52 13 5F 06 21 6F E8 94 E1 D705B	...e...&						000000000016F718	00000000
000000000022AEB0	85 C2 C8 B7 B1 09 EE CF 32 55 3C 6F 03 C6 9A	.AE.a.İZUk0b.Ä.						000000000016F718	01000000
000000000022AEC0	12 00 00 00 00 00 00 00 00 00 00 00 00 00 00I..3... ..						000000000016F718	00000000
000000000022AED0	00 00 00 00 00 00 00 CF 06 03 33 F7 00 00 80I..3... ..						000000000016F718	00000000

Bağlantı Kurduğu Adresler

Encrypted adrese (“mail[.]sisnet[.]co[.]kr”) bağlantı kurmakta ve bir süre sonra bağlantıyı sonlandırmaktadır.

```
000007FEFCA1C2A 894424 50 mov dword ptr [rsp+50],eax
000007FEFCA1C2E EB 00 jmp dnsapi.7FEFCA1C30
000007FEFCA1C32 3BF8 mov edi,ebx
000007FEFCA1C38 4C8D25 D9950400 lea r12,qword ptr ds:[7FEFCA9B218]
000007FEFCA1C3F EB 00 jmp dnsapi.7FEFCA1C41
000007FEFCA1C43 OF85 CC6E0100 jmp dnsapi.7FEFCA68B15
000007FEFCA1C49 81FE 7B260000 cmp esi,267B
000007FEFCA1C4F OF84 D5C20100 jmp dnsapi.7FEFCA6DF33
000007FEFCA1C55 4884424 60 mov rax,qword ptr ss:[rsp+60]
000007FEFCA1C5D OF84 F5060000 cmp rax,rbx
000007FEFCA1C63 488BF8 mov rdi,rbx
000007FEFCA1C66 4C8B00 A7950400 mov r12,qword ptr ds:[rax+8]
000007FEFCA1C71 488D15 A0950400 mov rcx,qword ptr ds:[7FEFCA9B218]
000007FEFCA1C78 483BCA lea rdx,qword ptr ds:[7FEFCA9B218]
000007FEFCA1C7D 74 0B jmp dnsapi.7FEFCA1C88
000007FEFCA1C80 OFB461 1C 0A bt dword ptr ds:[rcx-1C],A
000007FEFCA1C88 483BF8 cmp rdi,rbx
000007FEFCA1C8B 74 1B jmp dnsapi.7FEFCA1CA8
000007FEFCA1C8D 4839F 08 cmp qword ptr ds:[rdi+8],rbx
000007FEFCA1C91 OF84 90F9FFF mov r12,qword ptr ds:[rdi+8]
000007FEFCA1C97 4C8B87 08 mov rdi,qword ptr ds:[rdi]
000007FEFCA1C9E 483BF8 cmp rdi,rbx
000007FEFCA1CA1 75 EA jmp dnsapi.7FEFCA1C8D
000007FEFCA1CA3 4884424 60 mov rax,qword ptr ss:[rsp+60]
000007FEFCA1CA8 488BC8 mov rcx,rax
000007FEFCA1CAB 483BC3 cmp rax,rbx
000007FEFCA1CB3 74 12 jmp dnsapi.7FEFCA1CC2
000007FEFCA1CB8 8B51 14 mov edx,qword ptr ds:[rcx+14]
000007FEFCA1CB9 83E3 03 and edx,r14
000007FEFCA1CBF 413B06 cmp edi,r14
000007FEFCA1CC2 OF85 1A0C0000 jmp dnsapi.7FEFCA28D9
000007FEFCA1CCF 448BF3 mov r14,ebx
000007FEFCA1CC8 443BF3 cmp r14,ebx
000007FEFCA1CC5 OF85 D5C20100 jmp dnsapi.7FEFCA6DFA0
000007FEFCA1CCB B9 3D250000 mov ecx,25D
000007FEFCA1CD0 4C8B8C24 E8000000 mov r15,qword ptr ss:[rsp+E6]
000007FEFCA1CD8 498907 mov qword ptr ds:[r15],rax
000007FEFCA1CDB E9 3C010000 jmp dnsapi.7FEFCA1E1C
000007FEFCA1CE0 90 nop
```

Bu adrese bağlantı kurmakta sonra ise tekrardan kullandığı sitenin url kısmını encrypt edip hafızasına yazmaktadır.

Tekrardan başka bir “mail[.]neocyon[.]com/jsp/user/sms/sms_recv.jsp” uzantısına bağlantı kurup dinlemekte ve kendi URL adresini encrypt edip hafızasına yazmaktadır.

```
000000013F15141D E8 7E290000 call apt.13F153DA0
000000013F151422 4C8D4424 30 lea r8,qword ptr ss:[rsp+30]
000000013F151427 8D55 44 lea edx,qword ptr ss:[rbp+44]
000000013F15142A 488D00 7FD00100 lea rcx,qword ptr ds:[13F16E4B0]
000000013F151431 E8 DA280000 call apt.13F154030
000000013F151436 448B4424 30 mov r8d,dword ptr ss:[rsp+30]
000000013F15143B 488B00 mov rdx,rax
000000013F15143E 488BC8 mov rcx,rax
000000013F151441 488BF0 mov rsi,rax
000000013F151444 E8 57290000 call apt.13F153DA0
000000013F151449 4C8D4424 30 lea r8,qword ptr ss:[rsp+30]
000000013F15144E 8D55 44 lea edx,qword ptr ss:[rbp+44]
000000013F151451 488D00 58D00100 lea rcx,qword ptr ds:[13F16E4B0]
000000013F151458 E8 B3280000 call apt.13F154030
000000013F15145D 448B4424 30 mov r8d,dword ptr ss:[rsp+30]
000000013F151462 488B00 mov rdx,rax
000000013F151465 488BC8 mov rcx,rax
000000013F151468 488BF0 mov rdi,rax
000000013F15146B E8 30290000 call apt.13F153DA0
000000013F151470 4C8D005 F93A0200 lea r8,qword ptr ds:[13F174F70]
000000013F151477 498B06 mov rdx,r14
000000013F15147A 4D2BC6 sub r8,r14
000000013F15147D OF8F00 movzx ecx,byte ptr ds:[rax],eax
000000013F151483 488D52 01 lea rdx,qword ptr ds:[rdx]
000000013F151487 418B4C10 FF mov byte ptr ds:[r8+rdx-1],cl
000000013F15148C 84C9 test cl,cl
000000013F15148E 75 F0 jmp apt.13F151480
000000013F151491 488B8E mov rcx,r15
000000013F151493 4882BE sub rbx,r15
000000013F151496 666E0F1F8400 00000000 nop word ptr ds:[rax+rax],ax
000000013F1514A0 OF8601 movzx eax,byte ptr ds:[rcx]
000000013F1514A3 488D49 01 lea rcx,qword ptr ds:[rcx]
000000013F1514A7 88440B FF mov byte ptr ds:[rbx+rcx-1],al
000000013F1514AB 84C0 test al,al
000000013F1514AD 75 F1 jmp apt.13F1514A0
000000013F1514AF 488B9C24 00020000 mov rbx,qword ptr ss:[rsp+200]
000000013F1514B7 4C8D005 C2380200 lea r8,qword ptr ds:[13F175080]
000000013F1514BE 488BC7 mov rax,r15
000000013F1514C1 4C2BC7 sub r8,r15
000000013F1514C4 0F1F40 00 nop dword ptr ds:[rax],eax
000000013F1514C8 0F8F8400 00000000 movzx edx,byte ptr ds:[rax]
000000013F1514D0 0F8610 lea rax,qword ptr ds:[rax-1]
000000013F1514D3 488D40 01 mov byte ptr ds:[r8+rax-1],dl
000000013F1514D7 418B4C10 FF mov byte ptr ds:[r8+rax-1],dl
```

Bağlantı Kurduğu Adresler

Zararlı yazılım “mail[.]sisnet[.]co[.]kr” adresine bağlantı kurduktan sonra server ile bağlantı kurduğunu onaylamak için sistem üzerinden **HTTP/1.1 200** kodu gönderip bağlantıyı kurduğuna dair onay kodu göndermektedir.

```
000000013FF01C3A 48:33CC xor rcx,rsip
000000013FF01C3D E8 1E360000 call apt.13FF05260
000000013FF01C42 4C:8D9C24 80010000 lea r11,qword ptr ds:[rsp+180]
000000013FF01C44 49:8B58 38 mov r8b,qword ptr ds:[r11+38]
000000013FF01C4E 49:8B73 40 mov r9b,qword ptr ds:[r11+40]
000000013FF01C52 49:8B7B 48 mov rdb,qword ptr ds:[r11+48]
000000013FF01C56 49:8BE3 mov r5p,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
000000013FF01C7B 00:00000000 mov rax,qword ptr ds:[13FF22000]
000000013FF01C7D 48:33C4 xor rax,rsip
000000013FF01C7F 00:00000000 mov qword ptr ss:[rsp+460],rax
000000013FF01C82 00:00000000 mov eax,dword ptr ds:[13FF1E798]
000000013FF01C84 F2:0F1005 F0CA0100 movsd xmm0,qword ptr ds:[13FF1E790]
000000013FF01C86 00:00000000 mov r12,qword ptr ss:[rsp+400]
000000013FF01C88 00:00000000 mov dword ptr ss:[rsp+38],eax
000000013FF01C8A 00:00000000 movzx eax,byte ptr ds:[13FF1E79C]
000000013FF01C8C F2:0F114424 30 movsd qword ptr ss:[rsp+30],xmm0
000000013FF01C8E 00:00000000 movups xmm0,xmmword ptr ds:[13FF1E7A0]
000000013FF01C90 884424 3C mov byte ptr ss:[rsp+3c],al
000000013FF01C92 8B05 E8CA0100 mov eax,dword ptr ds:[13FF1E780]
000000013FF01C94 8B05 E8CA0100 mov eax,dword ptr ds:[13FF1E780]
000000013FF01C96 8B05 E8CA0100 mov eax,dword ptr ds:[13FF1E780]
```

Bağlantı kurduktan sonra ise her bağlantıya eşsiz birer cookie session id ataması yapmaktadır.

```
000000013F42E202 48:8BCB mov rcx,rbx
000000013F42E205 83F8 FF cmp eax,FFFFFFFF
000000013F42E208 00:00000000 je apt.13F42308E
000000013F42E20E 45:33C9 xor r9d,r9d
000000013F42E211 44:8BC6 mov r8d,esi
000000013F42E214 48:8B07 mov rdx,rdi
000000013F42E217 FF15 E3250200 call qword ptr ds:[k&send>]
000000013F42E21D 83F8 FF cmp eax,FFFFFFFF
000000013F42E220 00:00000000 je apt.13F42308E
000000013F42E226 48:84424 51 lea rcx,qword ptr ss:[rsp+51]
000000013F42E228 33D2 xor edx,edx
000000013F42E22D 41:8B FF030000 mov r8d,3FF
000000013F42E233 C64424 50 00 mov byte ptr ss:[rsp+50],0
000000013F42E238 E8 C34E0000 call apt.13F427000
000000013F42E23D 33C0 xor eax,eax
000000013F42E23F 48:8D5424 50 lea rdx,qword ptr ss:[rsp+50]
000000013F42E244 45:33C9 xor r9d,r9d
000000013F42E247 41:8B FF030000 mov r8d,3FF
000000013F42E24D 48:8BCB mov rcx,rbx
000000013F42E250 894424 30 mov dword ptr ss:[rsp+30],eax
000000013F42E254 894424 34 mov dword ptr ss:[rsp+34],eax
000000013F42E258 FF15 AA250200 call qword ptr ds:[k&recv>]
000000013F42E25E 8BF8 mov edi,eax
000000013F42E260 8D48 01 lea ecx,qword ptr ds:[rax+1]
000000013F42E263 83F9 01 cmp ecx,1
000000013F42E266 00:00000000 je apt.13F42308E
000000013F42E26C 48:8D08 51030000 lea rcx,qword ptr ss:[rbp+351]
000000013F42E273 33D2 xor edx,edx
000000013F42E275 41:8B FF030000 mov r8d,3FF
000000013F42E27B C685 50030000 00 mov byte ptr ss:[rbp+350],0
000000013F42E282 E8 794E0000 call apt.13F427000
000000013F42E287 48:8D4424 30 lea rax,qword ptr ss:[rsp+30]
000000013F42E28C 4C:8D4C24 34 lea r9,qword ptr ss:[rsp+34]
000000013F42E291 4C:8D85 50030000 lea r8,qword ptr ss:[rbp+350]
000000013F42E298 48:8D4C24 50 lea rcx,qword ptr ss:[rsp+50]
000000013F42E29D 8B07 mov edx,edi
000000013F42E29F 48:894424 20 mov qword ptr ss:[rsp+20],rax
000000013F42E2A4 E8 C7EDFFFF call apt.13F421C70
000000013F42E2A9 85C0 test eax,eax
000000013F42E2AB 00:00000000 je apt.13F42308E
000000013F42E2B1 4C:89BC24 60080000 mov qword ptr ss:[rsp+860],r15
000000013F42E2B9 44:8B7C24 30 mov r15d,dword ptr ss:[rsp+30]
000000013F42E2BE 45:85FF test r15d,r15d
000000013F42E2C1 75 12 jne apt.13F422E05
000000013F42E2C3 48:8BCB mov rcx,rbx
```


Bağlantı Kurduğu Adresler

Zararlı yazılım bağlantı kurduktan sonra **307** hatası verdirip yani internet sağlayıcısının taramasından kaçıp kendi sitesine yönlendirme yaptırmaktadır. Böylece daha kolay şekilde kendi yaptıkları mail sitesine hata vermeden gitmektedir.

```
00000013F0F2EB7 48:804424 30 1ea rax,qword ptr ss:[rsp+30]
00000013F0F2EB8 4C:804C24 34 1ea r9,qword ptr ss:[rsp+34]
00000013F0F2EB9 4C:8065 50030000 1ea r8,qword ptr ss:[rsp+38]
00000013F0F2E98 48:804C24 50 1ea rcx,qword ptr ss:[rsp+50]
00000013F0F2E9D 8807 mov edx,edi
00000013F0F2E9F 48:894424 20 mov qword ptr ss:[rsp+20],rax
00000013F0F2EA4 C011 apt.13F0F5C70
00000013F0F2EA9 85C0 test eax,ecx
00000013F0F2EAB 0F84 DA010000 jle apt.13F0F3088
00000013F0F2EB1 4C:898C24 60080000 mov qword ptr ss:[rsp+80],r15
00000013F0F2EB9 44:887C24 30 mov r15d,qword ptr ss:[rsp+30]
00000013F0F2EBE 45:85FF test r15d,r15d
00000013F0F2EC1 75 12 jnb apt.13F0F2E85
00000013F0F2EC3 48:89CB mov rcx,rbx
00000013F0F2EC6 FF15 2C250200 call qword ptr ds:[&closesockets]
00000013F0F2EC8 41:8047 32 1ea eax,qword ptr ds:[r15+2]
00000013F0F2ED0 4E 90000000 jmp apt.13F0F2F65
00000013F0F2ED5 887C24 34 mov edi,qword ptr ss:[rsp+34]
00000013F0F2ED9 41:38FF cmp edi,r15d
00000013F0F2EDC 75 2F jne apt.13F0F2F00
00000013F0F2EDE 48:8080 50030000 1ea rcx,qword ptr ss:[rbp+350]
00000013F0F2EE5 8807 mov edx,edi
00000013F0F2EE7 E8 44F6FFFF call apt.13F0F2530
00000013F0F2EE8 48:89CB mov rcx,rbx
00000013F0F2EEF 85C0 test eax,ecx
00000013F0F2EF1 74 00 jle apt.13F0F2F00
00000013F0F2EF3 FF15 FF240200 call qword ptr ds:[&closesockets]
00000013F0F2EF9 B8 C8000000 mov eax,c8
00000013F0F2EFE EB 65 jnb apt.13F0F2F65
00000013F0F2F00 FF15 F2240200 call qword ptr ds:[&closesockets]
00000013F0F2F06 B8 64000000 mov eax,64
00000013F0F2F08 EB 58 jnb apt.13F0F2F65
00000013F0F2F0D 41:81FF 0000A000 jmp apt.13F0F2F23
00000013F0F2F14 72 00 jle apt.13F0F2F23
00000013F0F2F19 FF15 D9240200 call qword ptr ds:[&closesockets]
00000013F0F2F1F 33C0 xor eax,ebx
00000013F0F2F21 EB 42 jnb apt.13F0F2F65
00000013F0F2F23 4C:894424 A8080000 mov qword ptr ss:[rsp+8A8],r12
00000013F0F2F28 45:8067 01 1ea r12d,qword ptr ds:[r15+1]
00000013F0F2F2F 4C:898424 68080000 mov qword ptr ss:[rsp+868],r14
00000013F0F2F37 41:89CC mov ecx,r12d
00000013F0F2F3A 41:38F4 cmp esi,r12d
00000013F0F2F3D E8 1E240000 call apt.13F0F5360
00000013F0F2C13 4C:8980 mov r15,rcx
4

```

rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?"

rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?"

64:'d'

rcx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?"

[rsp+8A8]:"/jsp/user/sms/sms_rcv.jsp"

ecx:"HTTP/1.1 307 Temporary Redirect\r\nLocation: http://88.255.216.16/landpage?"

cx=0000000002FE5F0 "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_rcv.jsp\r\nConnection: close\r\n\r\n"

bx=134 L'3'

text:00000013F0F2EC3 apt.exe:\$2EC3 #22C3

Network Analizi

İnternet sitelerine bağlantı kurduktan sonra ise **119[.]192[.]146[.]185** numaralı ip adresinin 80. portuna uzaktan erişimle bağlantı sağlamaktadır.

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

Backdoor türünde bir zararlı yazılım olduğundan dolayı belirlenen ip adresinden komut beklediği için sürekli olarak bağlantı kurup bağlantıyı sonlandırmaktadır.

TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Pack
[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		epnmap		0	LISTENING			
svchost.exe	688	TCPV6		epnmap		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 Tablosu

Yürütme	Kalıcılık	Ayrıcalık Yükseltme	Savunmadan Kaçma	Keşif	Toplamak	Komuta ve Kontrol
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 Security 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 Kuralı

```
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+OiJIOGFwsi3sQnuzzJVPG/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
}
```

Çözüm Önerileri

Backdoor türündeki Apt NukeSped zararlısından korunmanın yolları bulunmaktadır:

- Sistemlerde güncel, güvenilir bir anti-virüs yazılımının kullanılması,
- Gelen maillere özenle dikkat edilmesi, eklerin analiz edilmeden bilinçsizce açılmaması,
- Spam maillerin dikkate alınmaması,
- Açılacak olan uygulamaların yönetici iznini manuel olarak yetkilendirme yaparken dikkat edilmesi,
- Mutex nesnelerinin sistem üzerinde oluşturulması gibi çözümler,

Backdoor türündeki Apt NukeSped zararlısının sisteme bulaşmasını engelleyebilmektedir.

BUĐRA KÖSE

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