

Tofsee

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN BAKIŞ	1
NIGHTSKYWALKER.EXE ANALİZİ	2
STATİK ANALİZ	2
DİNAMİK ANALİZ	3
STAGE 2 ANALİZİ	7
STATİK ANALİZ	7
DİNAMİK ANALİZ	8
YARA KURALI	13
MITRE ATTACK TABLE	14
ÇÖZÜM ÖNERİLERİ	14
HAZIRLAYAN	15

Ön Bakış

Tofsee, bir botnet olarak kullanılan bir kötü amaçlı yazılım ailesidir. Bu malware ailesi, spam e-postaları göndermek, kimlik avı saldırıları yapmak, kötü amaçlı yazılımlar indirmek ve kurbanların bilgisayarlarını diğer botnetlere katılmaya zorlamak gibi farklı amaçlar için kullanılabilir.

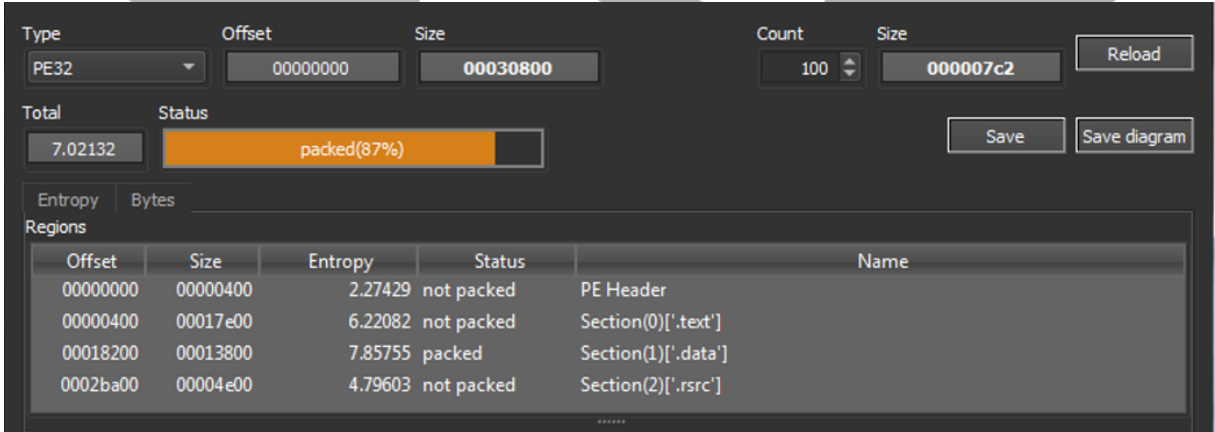
Tofsee, 2013 yılında ortaya çıktı ve o zamandan beri sürekli olarak güncellenerek geliştiriliyor. Özellikle Rusya ve Ukrayna gibi ülkelerde yoğun olarak kullanılmaktadır.

Tofsee malware ailesi, genellikle spam e-postalarının eklerinde veya zararlı bağlantılarla bulaşır. Bir kez kurbanın bilgisayarına yerleştirildiğinde, diğer kötü amaçlı yazılımlar indirmek ve diğer botnetlere bağlanmak gibi birçok farklı eylem gerçekleştirebilir.

nightskywalker.exe Analizi

Adı	nightskywalker.exe
MD5	e5d88e4a2497a5f8219482d64d3b501b
SHA256	e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ffcc2 ebc2fdf49
Dosya Türü	PE32 / EXE

Statik Analiz



Şekil 1- Zararlı dosyada paketleme işleminin gözlemlenmesi

Zararlının ilk bakışta paketlenmiş olduğu görülmektedir.

Dinamik Analiz

explorer.exe	2736	0.63	148 B/s	51.08 MB	iceking-PC\iceking	Windows Explorer
vm\vmtoolsd.exe	1880	0.13	3.44 kB/s	12.61 MB	iceking-PC\iceking	VMware Tools Core Service
ProcessHacker.exe	2444	1.12	4.63 kB/s	11.25 MB	iceking-PC\iceking	Process Hacker
e16191d95969d7ae164c...	888	0.02	100 B/s	3.92 MB	iceking-PC\iceking	
wusa.exe	3732			2.17 MB	iceking-PC\iceking	Windows Update Standalone I...
netsh.exe	3412			4.64 MB		Network Command Shell
Everything.exe	2296	0.04	916 B/s	17.67 MB	iceking-PC\iceking	Everything
svchost.exe	1872	0.65		1.89 MB		Host Process for Windows Ser...

Şekil 2-Zararlının Process Monitor ile incelenmesi

İlk etapda zararlının iki adet child process çalıştırdığı görülmektedir.

Kullanıcı Hesap Denetimi(UAC), bilgisayara izinsiz bir değişiklik yapılmasını engellemek için Windows işletim sisteminde kullanılmaktadır. "wusa.exe"(Windows Update Standalone Installer) otomatik yükseltme özelliği açık olan processlerden biridir. UAC iznine sahip olmadan kendisini yönetici olarak çalıştırma yetkisi vardır. Bu yetkiyi kötüye kullanarak wusa.exe içerisine zararlının enjekte olup yönetici yetkileri çalışması mümkün olmaktadır.

"netsh.exe" bilgisayarın ağ yapılandırmasını değiştirmeye veya görüntülemeye yarayan bir programdır. Zararlının ağ ayarlarında değişiklik yapmış olabileceği görülmektedir.

```
lea eax,dword ptr ss:[ebp-4c]
push eax
call dword ptr ds:[&GetStartupInfoW]
push 40
push 20
pop esi
push esi
call e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
pop ecx
pop ecx
xor ecx,ecx
cmp eax,ecx
jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
or eax,FFFFFFFF
jmp e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
lea edx,dword ptr ds:[eax+800]
mov dword ptr ds:[593000],eax
mov dword ptr ds:[5930FC],esi
cmp eax,edx
jae e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
add eax,5
or dword ptr ds:[eax-5],FFFFFFFF
mov word ptr ds:[eax-1],A00
```

Şekil 3- GetStartupInfoW API'si kullanılarak bilgi toplanmaktadır

```
type="win32",version="1.0.0.0"C:\\Windows\\WinSxS\\manifests\\x86_microsoft.windows.is
olationautomation_6595b64144ccf1df_1.0.0.0_none_35d357a66c38ade4.manifest
```

Zararlı Şekil 3'de gösterilen API ile sistem ile alakalı bilgileri toplamaktadır.

●	0040DDEB	BB 0000FFFF	mov ebx,FFFF0000
●	0040DDF0	38C7	cmp eax,edi
--	0040DDF2	74 0D	je e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274
●	0040DDF4	85C3	test ebx,eax
--	0040DDF6	74 09	je e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274
●	0040DDF8	F7D0	not eax
●	0040DDFA	A3 8CB44200	mov dword ptr ds:[42B48C],eax
—	0040DDFF	EB 65	jmp e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274
→	0040DE01	56	push esi
●	0040DE02	8D45 F8	lea eax,dword ptr ss:[ebp-8]
●	0040DE05	50	push eax
●	0040DE06	FF15 90114000	call dword ptr ds:[<&GetSystemTimeAsFileTime>]
●	0040DE0C	8B75 FC	mov esi,dword ptr ss:[ebp-4]
●	0040DE0F	3375 F8	xor esi,dword ptr ss:[ebp-8]
●	0040DE12	FF15 A4104000	call dword ptr ds:[<&GetCurrentProcessId>]
●	0040DE18	33F0	xor esi,eax
●	0040DE1A	FF15 3C114000	call dword ptr ds:[<&GetCurrentThreadId>]
●	0040DE20	33F0	xor esi,eax
●	0040DE22	FF15 8C114000	call dword ptr ds:[<&GetTickCount>]
●	0040DE28	33F0	xor esi,eax
●	0040DE2A	8D45 F0	lea eax,dword ptr ss:[ebp-10]
●	0040DE2D	50	push eax
●	0040DE2E	FF15 88114000	call dword ptr ds:[<&QueryPerformanceCounter>]
●	0040DE34	8B45 F4	mov eax,dword ptr ss:[ebp-C]
●	0040DE37	3345 F0	xor eax,dword ptr ss:[ebp-10]
●	0040DE3A	33F0	xor esi,eax
●	0040DE3C	3BF7	cmp esi,edi
--	0040DE3E	75 07	jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274
—	0040DE40	BE 4FE640BB	mov esi,8B40E64F
—	0040DE45	EB 10	jmp e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274
→	0040DE47	85F3	test ebx,esi

Şekil 4- Sistem zamanı bilgileri toplamaktadır

Zararlı GetSystemTimeAsFileTime, GetCurrentProcessId, GetCurrentThreadId gibi API'ler kullanarak sistem zamanı bilgileri edinmektedir. O anki Process ve Thread Id'lerini edinmektedir.

push esi	esi:L"=:::=""
call dword ptr ds:[<&GetEnvironmentStringsW>]	esi:L"=:::="", eax:L"ComSpec=C:\\Windows\\system32\\cmd.exe"
mov esi,eax	esi:L"=:::=""
xor ecx,ecx	esi:L"=:::=""
cmp esi,ecx	esi:L"=:::=""
jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274	esi:L"=:::=""
xor eax,eax	esi:L"=:::=""
pop esi	esi:L"=:::=""
ret	esi:L"=:::=""
cmp word ptr ds:[esi],cx	esi:L"=:::=""
je e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274	esi:L"=:::=""
add eax,2	esi:L"=:::=""
cmp word ptr ds:[eax],cx	esi:L"=:::=""
jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274	esi:L"=:::=""
add eax,2	esi:L"=:::=""
cmp word ptr ds:[eax],cx	esi:L"=:::=""
jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274	esi:L"=:::=""
push ebx	esi:L"=:::=""
sub eax,esi	esi:L"=:::=""
lea ebx,dword ptr ds:[eax+2]	esi:L"=:::=""
push edi	esi:L"=:::=""
push ebx	esi:L"=:::=""
call e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274	esi:L"=:::=""
mov edi,eax	esi:L"=:::=""
pop ecx	esi:L"=:::=""
test edi,edi	esi:L"=:::=""
jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e90274	esi:L"=:::=""
push esi	esi:L"=:::=""
call dword ptr ds:[<&FreeEnvironmentStringsW>]	esi:L"=:::=""
mov eax,edi	esi:L"=:::=""
pop edi	esi:L"=:::=""
pop ebx	esi:L"=:::=""

Şekil 5- Sistemin bilgilerini toplamaktadır

GetEnvironmentStringsW API'si ile mevcut işlem için ortam değişken bilgilerini elde ettiği görülmektedir. Bu bilgiler kullanıcı, donanım ve ortam hakkında bilgi içeren hassas bilgilerden oluşmaktadır.

Zararlının topladığı bazı bilgiler aşağıdaki tabloda verilmiştir.

ALLUSERSPROFILE=C:\\ProgramData	NUMBER_OF_PROCESSORS=4
LOGONSERVER=\\\\ICEKING-PC	LOCALAPPDATA=C:\\Users\\user\\AppData\\Local
FP_NO_HOST_CHECK=NO	COMPUTERNAME=ICEKING-PC
OS=Windows_NT	PROCESSOR_ARCHITECTURE=x86
HOMEDRIVE=C:	ComSpec=C:\\Windows\\system32\\cmd.exe
TEMP=C:\\Users\\user\\AppData\\Local\\Temp	PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

Tablo 6- Zararlının edindiği bilgiler

```

00405195  5E                pop esi
00405196  81C4 84000000    add esp,84
0040519C  C3                ret
0040519D  FF35 048B5500    push dword ptr ds:[558B04]
004051A3  6A 00            push 0
004051A5  FF15 50104000    call dword ptr ds:[<&LocalAlloc>]
004051AB  A3 98585500      mov dword ptr ds:[558B98],eax
004051B0  C3                ret

```

Şekil 7- LocalAlloc kullanıldığı görülmektedir

Zararlı, **LocalAlloc** API'si kullanılarak yer ayırma işlemi yapmaktadır.

```

Hex
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ.....yy..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0E 1F BA 0E 00 84 09 CD 21 B8 01 4C CD 21 54 68  ..°..I!..LI!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.
F4 98 29 E0 80 F9 47 B3 80 F9 47 B3 80 F9 47 B3  ö.)à'ùg'ùg'ùg'
B9 81 D4 B3 85 F9 47 B3 80 F9 46 B3 A0 F9 47 B3  '.'ò*ùg'ùf'ùg'
B9 81 C4 B3 82 F9 47 B3 89 81 D5 B3 81 F9 47 B3  '.'A*ùg'.'ò±ùg'
B9 81 D2 B3 81 F9 47 B3 89 81 C3 B3 8A F9 47 B3  '.'ò±ùg'.'A°ùg'
B9 81 D3 B3 81 F9 47 B3 89 81 D6 B3 81 F9 47 B3  '.'ò±ùg'.'ò±ùg'
52 69 63 68 80 F9 47 B3 00 00 00 00 00 00 00 00  Rich'ùg'.....
00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  .....PE..L..
A0 DA 5B 4A 00 00 00 00 00 00 00 00 E0 00 02 21  ú[].....à.!

```

Şekil 7- Çıkarılan dosyanın hex kodu

Zararlı, ayrılan bu alana içerisinde paketlenmiş şekilde duran dosyayı yazmaktadır.

00405141	C705 49C74200 697274	mov dword ptr ds:[42C749],75747269	0042C749:"irtualProtect"
00405148	66:C705 4DC74200 616	mov word ptr ds:[42C74D],6C61	0042C74D:"alProtect"
00405154	C605 48C74200 56	mov byte ptr ds:[42C748],56	0042C748:"VirtualProtect", 56:'V'
00405158	66:C705 54C74200 637	mov word ptr ds:[42C754],7463	0042C754:"ct"
00405164	C605 56C74200 00	mov byte ptr ds:[42C756],0	0042C756:"Protect"
00405168	C705 4FC74200 50726F	mov dword ptr ds:[42C74F],746F7250	
00405175	FF15 4C104000	call dword ptr ds:[<&GetProcAddress>]	
0040517B	804C24 04	lea ecx,dword ptr ss:[esp+4]	

Şekil 9- GetProcAddress kullanılarak API çözümleme yapılmaktadır

Zararlı, API çözümleme(API Resolving) işlemi yapmaktadır. Gerekli tüm API'leri içeri aktarmaktansa sadece adını saklamaktadır. Çalışma zamanında dinamik bir şekilde GetProcAddress ile API'leri çözümlemektedir. Zararlı bu şekilde analizi zorlaştırmaktadır.

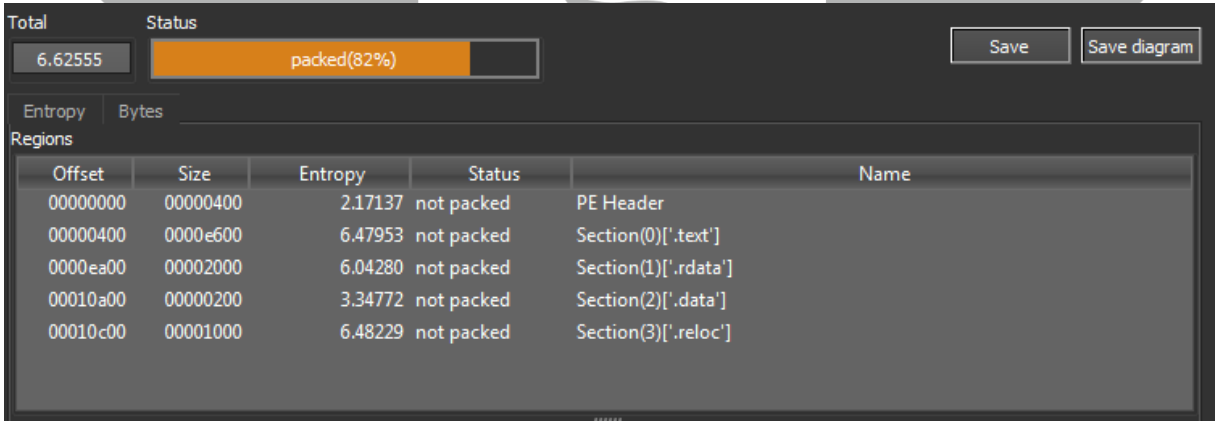
VirtualProtect API'sini kullanmak üzere bu çözümleme yapılmaktadır. Bulunduğu DLL GetProcAddress'e parametre olarak verildikten sonra dışarı aktarılan VirtualProtect API'sinin adresi döndürülmektedir. Bu şekilde çözümleme işlemi tamamlanmaktadır.

VirtualProtect API'si ile ayrılan bu alandaki dosyaya çalıştırma izni vermektedir. Daha sonra ayrılan alandaki dosya çalıştırılmaktadır.

Stage 2 Analizi

Adı	-
MD5	92E466525E810B79AE23EAC344A52027
SHA256	96baba74a907890b995f23c7db21568f7bfb5dbf417ed90ca311482b99702b72
Dosya Türü	PE32 / EXE

Statik Analiz



Şekil 10- Çıkarılan dosyada paketleme işlemi görülmemektedir.

Çıkarılan zararlı paketlenmiş değildir.

Dinamik Analiz

```

push esp
mov ebp,esp
mov eax,dword ptr ss:[ebp+8]
push edi
mov edi,dword ptr ss:[ebp+10]
mov cl,1
test edi,edi
jz 96baba74a907890b995f23c7db21568f7bf5db
push esi
mov esi,dword ptr ss:[ebp+C]
sub esi,eax
mov d1,byte ptr ds:[esi+eax]
xor d1,byte ptr ss:[ebp+14]
mov byte ptr ds:[eax],d1
add d1,byte ptr ss:[ebp+18]
neg cl
add byte ptr ss:[ebp+14],d1
inc eax
dec edi
jne 96baba74a907890b995f23c7db21568f7bf5db
pop esi
mov eax,dword ptr ss:[ebp+8]
pop edi
pop ebp
lea eax,dword ptr ds:[ecx+C]
lea edx,dword ptr ds:[eax-1]
mov dword ptr ds:[ecx],edx
test eax,edx
jne 96baba74a907890b995f23c7db21568f7bf5db
mov eax,dword ptr ds:[ecx]
movzx edx,byte ptr ds:[eax+1]
push esi
esi:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
[ebp+C]:\"C:\\Users\\i\ceking\\AppData\\Local\\Temp\\pfywtcjl.exe"
esi:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
eax:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
esi:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
eax:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
esi:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
eax:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto
esi:"cmd /C mkdir %s\r\ncmd /C move /Y \"%s\" %s\r\nsc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto

```

Şekil 11- CMD komutları gözükmemtedir

Zararlı, CMD komutlarını bir String içerisinde tutmaktadır. Tuttuğu bu String bir takım manipülasyonlar sonucu ayrı ayrı çalıştırılmaktadır.

```

cmd /C mkdir %s\r\n
cmd /C move /Y \"%s\" %s\r\n
sc create %s binPath= \"%s%s /d\\\"%s\\\" type= own start= auto DisplayName= \"wifi
support\"\\r\n
sc description %s \"wifi internet conection\"\\r\n
sc start %s\r\n\"

```

```

00FA9412 5A 00 push esi
00FA941C 56 8945 78 mov dword ptr ss:[ebp+78],eax
00FA9420 E8 055A0000 call 96baba74a907890b995f23c7db21568f7bf5db
00FA9425 83C4 0C add esp,C
00FA9428 837D 58 60 cmp dword ptr ss:[ebp+58],60
00FA942C 72 75 jz 96baba74a907890b995f23c7db21568f7bf5db
00FA942E 837D 7C 00 cmp dword ptr ss:[ebp+7C],0
00FA9432 74 6F jz 96baba74a907890b995f23c7db21568f7bf5db
00FA9434 E8 9008FFFF call 96baba74a907890b995f23c7db21568f7bf5db
00FA9439 50 push eax
00FA943A 8D85 A4FEFFFF lea eax,dword ptr ss:[ebp-15C]
00FA9440 50 push eax
00FA9441 E8 BASA0000 call 96baba74a907890b995f23c7db21568f7bf5db
00FA9446 53 push ebx
00FA9447 57 push edi
00FA944A 68 0C09FB00 push C
00FA944E 68 0C09FB00 push 96baba74a907890b995f23c7db21568f7bf5db
00FA9450 56 push esi
00FA9455 58 8D85 A4FEFFFF call 96baba74a907890b995f23c7db21568f7bf5db
00FA945E 50 push eax
00FA945F 50 push eax
00FA9462 E8 BC5A0000 call 96baba74a907890b995f23c7db21568f7bf5db
00FA9465 8D85 A4FEFFFF lea esp,24
00FA9466 50 lea eax,dword ptr ss:[ebp-15C]
00FA946C 53 push eax
00FA946D 57 push ebx
00FA946E 68 82000000 push edi
00FA9473 68 8209FB00 push 96baba74a907890b995f23c7db21568f7bf5db
00FA9478 56 push esi
00FA9479 E8 C690FFFF call 96baba74a907890b995f23c7db21568f7bf5db
esi:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
60:''
eax:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
eax:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
esi:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
eax:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
esi:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
eax:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
esi:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
eax:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=
esi:"netsh advfirewall firewall add rule name=\"Host-process for services of Windows\" dir=

```

Şekil 12- Windows Güvenlik Duvarına kural eklenmektedir

```
netsh advfirewall firewall add rule name="Host-process for services of Windows\" dir=in
action=allow program="\"%s\" enable=yes>nul\r\n
```

Zararlı, Windows Güvenlik Duvarı'na bir kural ekleyerek kendi trafiğine izin verir."Host-process for services of Windows" adıyla oluşturulan kural, gelen trafiğe izin vermektedir. Kuralın uygulanacağı program daha sonra "C:\\Users\\user\\AppData\\Local\\Temp\\pfywtcji.exe\" olarak belirlenir.

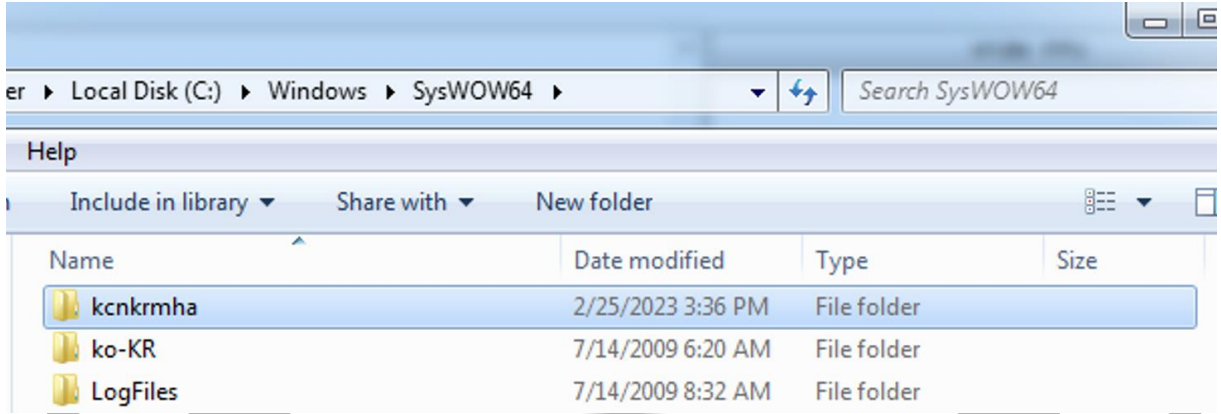
```
add esp,14
push eax
push dword ptr ss:[ebp+50]
call <&RegQueryValueExA>
test eax, eax
je 96baba74a907890b995f23c7db21568f7bfb5db
mov dword ptr ss:[ebp+78],3000
push dword ptr ss:[ebp+50]
call <&RegCloseKey>
mov esi,dword ptr ss:[ebp+78]
xor edi,edi
cmp dword ptr ss:[ebp+44],edi
jne 96baba74a907890b995f23c7db21568f7bfb5db
cmp dword ptr ss:[ebp+48],edi
je 96baba74a907890b995f23c7db21568f7bfb5db
cmp dword ptr ss:[ebp+5C],edi
jle 96baba74a907890b995f23c7db21568f7bfb5db
cmp dword ptr ss:[ebp+58],61
mov eax,dword ptr ss:[ebp+4C]
jg 96baba74a907890b995f23c7db21568f7bfb5db
cmp eax,1D0B
jb 96baba74a907890b995f23c7db21568f7bfb5db
push 800
lea eax,dword ptr ss:[ebp-195C]
push eax
lea eax,dword ptr ss:[ebp-95C]
push eax
call 96baba74a907890b995f23c7db21568f7bfb5db
add esp,C
test eax, eax
je 96baba74a907890b995f23c7db21568f7bfb5db
push eax
lea eax,dword ptr ss:[ebp+78]
push eax
lea eax,dword ptr ss:[ebp+5C]
push eax
lea eax,dword ptr ss:[ebp-195C]
push eax
call 96baba74a907890b995f23c7db21568f7bfb5db

eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
61:'a'
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
eax:"cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\ncmd /C move /Y \"C:\\Users\\iceking\\AppData\\Local\\Temp\\pfywtcji.exe\"
```

Şekil 13- Kendini sistem dosyalarına kopyalamaktadır

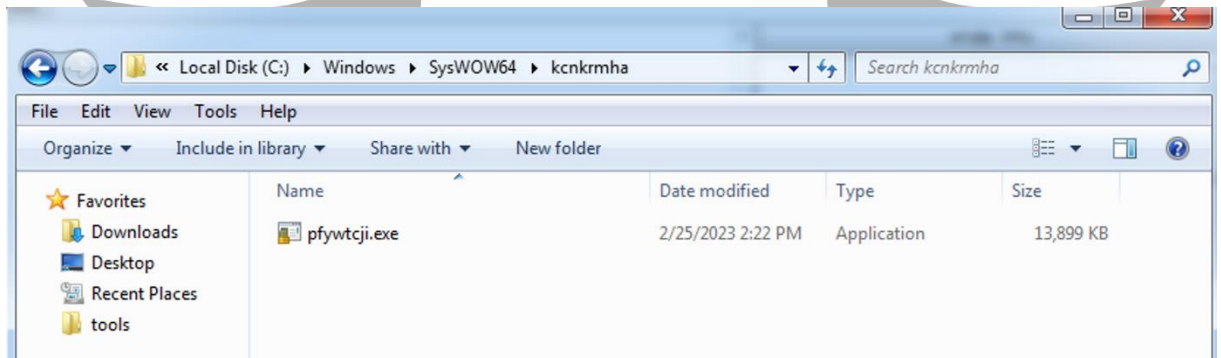
Dinamik oluşturulmuş komutlara değişken değerleri eklenmektedir. Değişken değerleri eklenmiş kodlar aşağıda verilmiştir.

```
cmd /C mkdir C:\\Windows\\SysWOW64\\kcnkrmha\\r\\n
cmd /C move /Y \"C:\\Users\\user\\AppData\\Local\\Temp\\pfywtcji.exe\"
C:\\Windows\\SysWOW64\\kcnkrmha\\r\\n
sc create kcnkrmha binPath= \"C:\\Windows\\SysWOW64\\kcnkrmha\\pfywtcji.exe
/d\\\"C:\\Users\\user\\Downloads\\96baba74a907890b995f23c7db21568f7bfb5dbf417ed90ca3
11482b99702b72.exe\\\" type= own start= auto DisplayName= \"wifi support\"\\r\n
sc description kcnkrmha \"wifi internet conection\"\\r\n
sc start kcnkrmha\\r\n
```



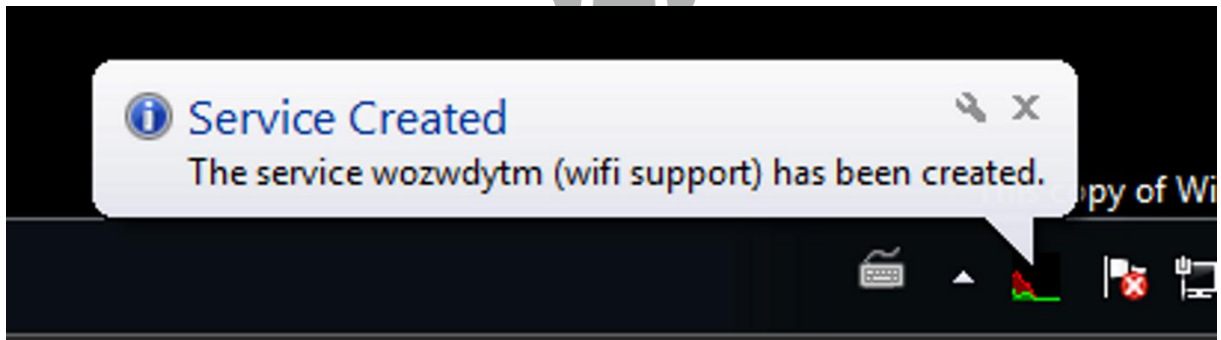
Şekil 8- SysWOW64 içinde oluşturulan dizin

Zararlı “C:\Windows\SysWOW64” içerisine bir dizin oluşturmaktadır.



Şekil 9- Oluşturulan dizinin içine taşınan zararlı

Zararlı, C:\Users\user\AppData\Local\Temp dizininde olan kötü amaçlı yazılım dosyasını C:\Windows\SysWOW64\kcnkrmha dizinine taşır.

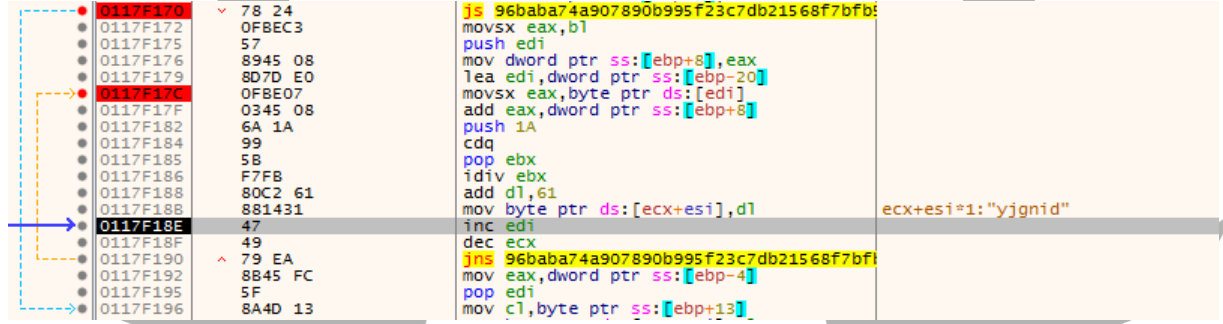


Şekil 10- “wifi support” ismiyle bir servis oluşturulmaktadır

Oluşturduğu klasör ismiyle bir servis oluşturmaktadır. Oluşturduğu servis kendisini “*wifi support*” ismiyle gizlemektedir.

Servisin içerisinde zararlı kendi yolunu verip sistem önyükleme zamanında kendisini otomatik çalıştırmaktadır. Ek olarak servise açıklama olarak “*wifi internet conection*” eklenmektedir.

Servis oluşturması bittikten sonra oluşturduğu servisi çalıştırmaktadır.



```
0117F170 78 24 js 96baba74a907890b995f23c7db21568f7bfb:
0117F172 0FBEC3 movsx eax,b1
0117F175 57 push edi
0117F176 8945 08 mov dword ptr ss:[ebp+8],eax
0117F179 807D E0 lea edi,dword ptr ss:[ebp-20]
0117F17C 0FBEO7 movsx eax,byte ptr ds:[edi]
0117F17F 0345 08 add eax,dword ptr ss:[ebp+8]
0117F182 6A 1A push 1A
0117F184 99 cdq
0117F185 5B pop ebx
0117F186 F7FB idiv ebx
0117F188 80C2 61 add dl,61
0117F188 881431 mov byte ptr ds:[ecx+esi],dl ecx+esi*1: "yjgnid"
0117F18E 47 inc edi
0117F18F 49 dec ecx
0117F190 79 EA jns 96baba74a907890b995f23c7db21568f7bfb:
0117F192 8B45 FC mov eax,dword ptr ss:[ebp-4]
0117F195 5F pop edi
0117F196 8A4D 13 mov cl,byte ptr ss:[ebp+13]
```

Şekil 11- İsimlerin rastgele olduğu yerlerden biri görülmektedir

Oluşturulan yedek dosyaların, servislerin, klasörlerin, güvenlik duvarı kurallarının isimleri rastgele bir şekilde oluşturulmaktadır.

```
.rdata:00F90490 asc_F90490 db ' ',0 ; DATA XREF: sub_F84699+7Afo
.rdata:00F90494 aRndChar_0 db '%RND_char',0 ; DATA XREF: sub_F84699+6Dfo
.rdata:00F9049E align 10h
.rdata:00F904A0 aQwertyuiopasdf_0 db 'qwertyuiopasdfghjklzxcvbnm',0 ; DATA XREF: sub_F84699+68fo
.rdata:00F904BB align 4
.rdata:00F904BC aRndChar db '%RND_CHAR',0 ; DATA XREF: sub_F84699+5Bfo
.rdata:00F904C6 align 4
.rdata:00F904C8 aQwertyuiopasdf db 'QWERTYUIOPASDFGHJKLZXCVBNM',0 ; DATA XREF: sub_F84699+56fo
.rdata:00F904C8 ; DATA XREF: sub_F84699+56fo
.rdata:00F904E3 align 4
.rdata:00F904E4 aRndHex_0 db '%RND_hex',0 ; DATA XREF: sub_F84699+46fo
.rdata:00F904ED align 10h
.rdata:00F904F0 a0123456789abcd_0 db '0123456789abcdef',0 ; DATA XREF: sub_F84699+41fo
.rdata:00F904F0 ; DATA XREF: sub_F84699+41fo
.rdata:00F90501 align 4
.rdata:00F90504 aRndHex db '%RND_HEX',0 ; DATA XREF: sub_F84699+34fo
.rdata:00F9050D align 10h
.rdata:00F90510 a0123456789abcd db '0123456789ABCDEF',0 ; DATA XREF: sub_F84699+2Ffo
.rdata:00F90510 ; sub_F8AEDD+27Cfo ...
.rdata:00F90521 align 4
.rdata:00F90524 aRndDigit db '%RND_DIGIT',0 ; DATA XREF: sub_F84699+22fo
.rdata:00F9052F align 10h
.rdata:00F90530 a0123456789 db '0123456789',0 ; DATA XREF: sub_F84699+1Dfo
.rdata:00F9053B align 4
.rdata:00F9053C aRndNum db '%RND_NUM',0 ; DATA XREF: sub_F84699+10fo
.rdata:00F90545 align 4
```

Şekil 18- İsimleri oluşturmakta kullanılan değişkenler

Bu deęişkenler isim oluřturma algoritmasında kullanılmaktadır. Rastgele isimler ile her alıřma anında farklı dosya ve servis ismi ile yakalanması zorlařmaktadır.

215	21.340430	192.168.224.152	185.251.89.37	TCP	54	49442 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
214	21.340390	185.251.89.37	192.168.224.152	TCP	60	443 → 49442 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
213	21.268024	192.168.224.152	185.251.89.37	TCP	66	49442 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
212	21.267462	192.168.224.2	192.168.224.152	DNS	92	Standard query response 0x1980 A svartalfheim.top A 185.251.89.37
211	21.021307	192.168.224.152	192.168.224.2	DNS	76	Standard query 0x1980 A svartalfheim.top
210	20.240553	192.168.224.152	192.168.224.2	NBNS	110	Refresh NB ICEKING-PC<00>
209	19.473822	80.66.75.4	192.168.224.152	TCP	442	[TCP Retransmission] 423 → 49246 [PSH, ACK] Seq=4381 Ack=1 Win=64240 Len=388
208	19.473806	80.66.75.4	192.168.224.152	TCP	1514	[TCP Retransmission] 423 → 49246 [ACK] Seq=2921 Ack=1 Win=64240 Len=1460
207	19.473806	80.66.75.4	192.168.224.152	TCP	1514	[TCP Retransmission] 423 → 49246 [ACK] Seq=1461 Ack=1 Win=64240 Len=1460
206	19.473806	80.66.75.4	192.168.224.152	TCP	1514	[TCP Retransmission] 423 → 49246 [ACK] Seq=1 Ack=1 Win=64240 Len=1460

Őekil 19- Network analizinde potansiyel C2 sunucusu

Aę trafiginde “svartalfheim[.]top” C2 sunucusu bulunmaktadır.

YARA Kuralı

```
import "hash"

rule tofsee {

  meta:

    author = "Berkay Dogan"

  strings:

    $a1 = "loader_id"

    $a2 = "hi_id"

    $a3 = "born_date"

    $b = "svartalfheim.top"

    $crypt1 = {33 D2 8B C6 F7 F1 81 F6 61 61 61 61 80 C2 61 0F B6 C2}

    $crypt2 = {32 55 14 88 10 8A D1 02 55 18 F6 D9 00 55 14}

  condition:

    hash.md5(0,filesize) == "92E466525E810B79AE23EAC344A52027"
    or $a* or $b or $crypt*

}
```


MITRE ATTACK TABLE

Reconnaissance	Execution	Persistence	Discovery	Privilege Escalation	Defense Evasion	C&C	Exfiltration
	T-1569 System Services	T-1547 Boot or Logon Autostart Execution	T-1082 System Information Discovery	T-1055 Process Injection	T-1027 Obfuscated Files or Information		
				T-1547 Boot or Logon Autostart Execution	T-1222 File and Directory Permissions Modification		
					T-1036 Creates files inside the user directory		

Çözüm Önerileri

1. İyi ve güncel bir antivirüs yazılımı kullanarak sistem güvenliğinizi artırabilirsiniz.
2. Güvenlik yazılımınızı ve işletim sisteminizi düzenli olarak güncelleyerek, bilinen saldırılara karşı savunmasını güçlendirebilirsiniz.
3. Kötü niyetli web sitelerine ve indirmelere maruz kalmamak için güvenilir web sitelerini kullanın ve indirmeleri güvenilir kaynaklardan yapın.
4. Önemli verilerinizi yedekleyerek, kötü amaçlı yazılımların neden olabileceği veri kaybı riskini azaltabilirsiniz.

HAZIRLAYAN

Berkay DOĐAN

<https://www.linkedin.com/in/berkay-dogan99/>

