Tofsee

TEKNİK ANALİZ RAPORU

ZAYOTEM
ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

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.

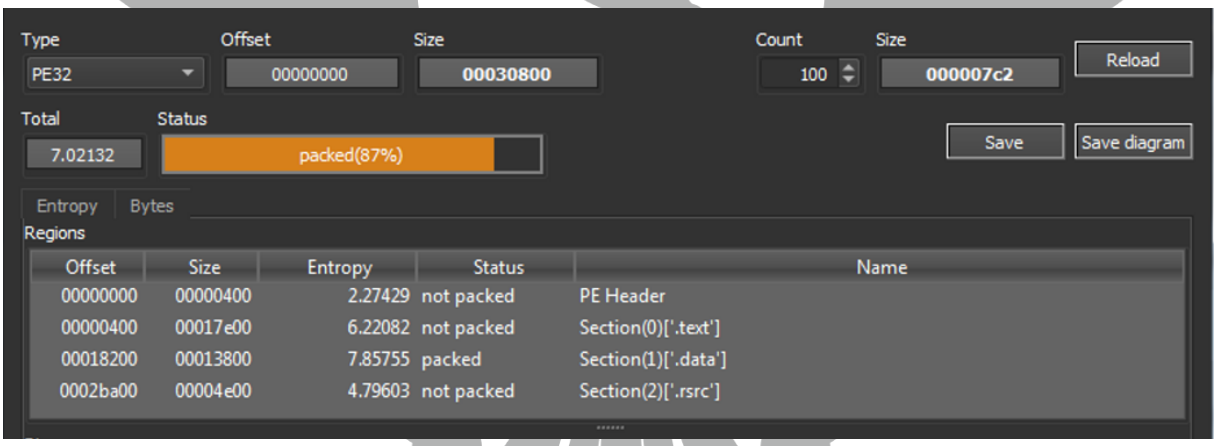
Tofsee, 2013 yılında ortaya çıktı ve o zamandan beri sürekli olarak güncellenerek geliştiriliyor. Özellikle Rusya ve Ukrayna gibi ülkelerde yoğun olarak kullanılmaktadır.

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	e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ffcc2ebc2fdf49
Dosya Türü	PE32 / EXE

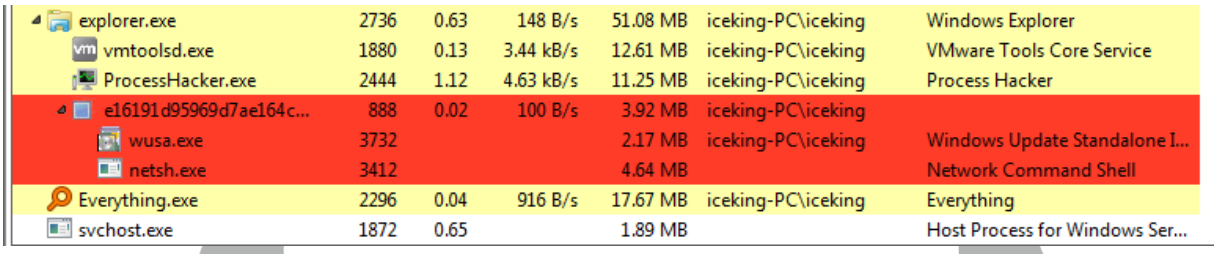
Statik Analiz



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
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.

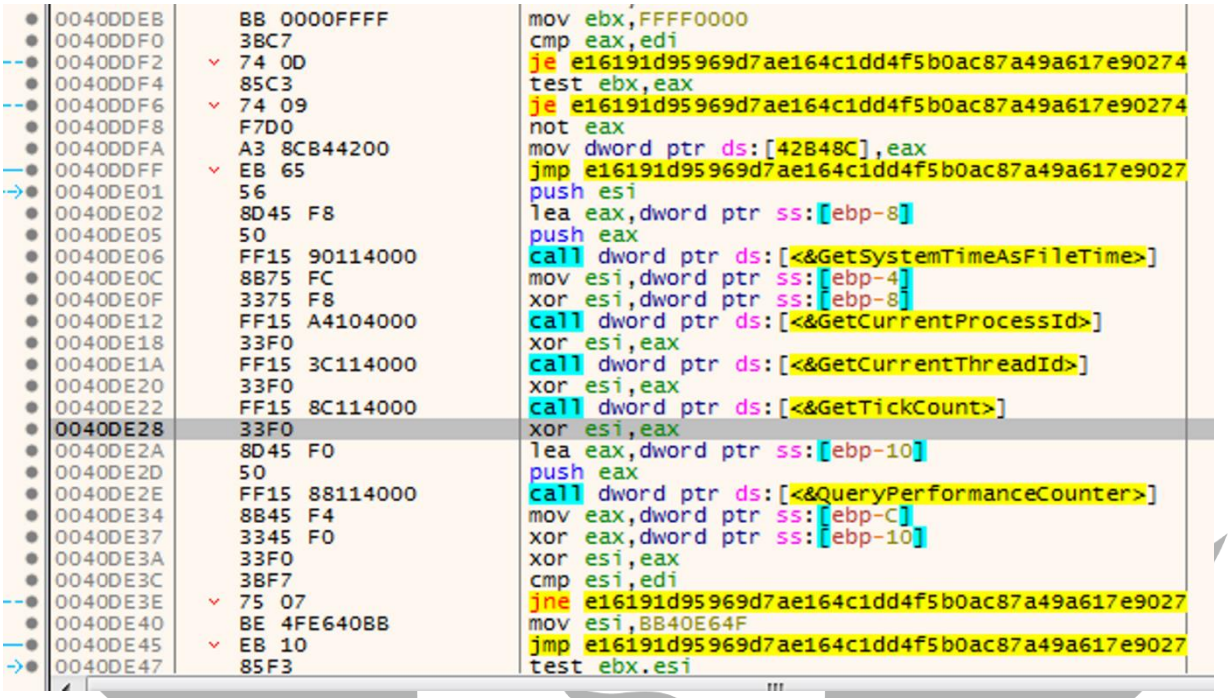
```
lea eax,dword ptr ss:[ebp-4C]
push eax
call dword ptr ds:[<&GetStartupInfoW>]
push 40
push 20
pop esi
push esi
call e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204f
pop ecx
pop ecx
xor ecx,ecx
cmp eax,ecx
jne e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
or eax,FFFFFFFF
jmp e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
lea edx,dword ptr ds:[eax+800]
mov dword ptr ds:[559D00],eax
mov dword ptr ds:[559CFC],esi
cmp eax,edx
jae e16191d95969d7ae164c1dd4f5b0ac87a49a617e902743d204ff
add eax,5
or dword ptr ds:[eax-5],FFFFFFFF
mov word ptr ds:[eax-1],A00
```

```
eax+800:L"\",type=\"win32\",version=\"1.0.0.0\"C:\\Windows\\WinSxS\\manifests\\x86_microsoft.wind
```

Şekil 3- GetStartupInfoW API'si kullanılarak bilgi toplanmaktadır

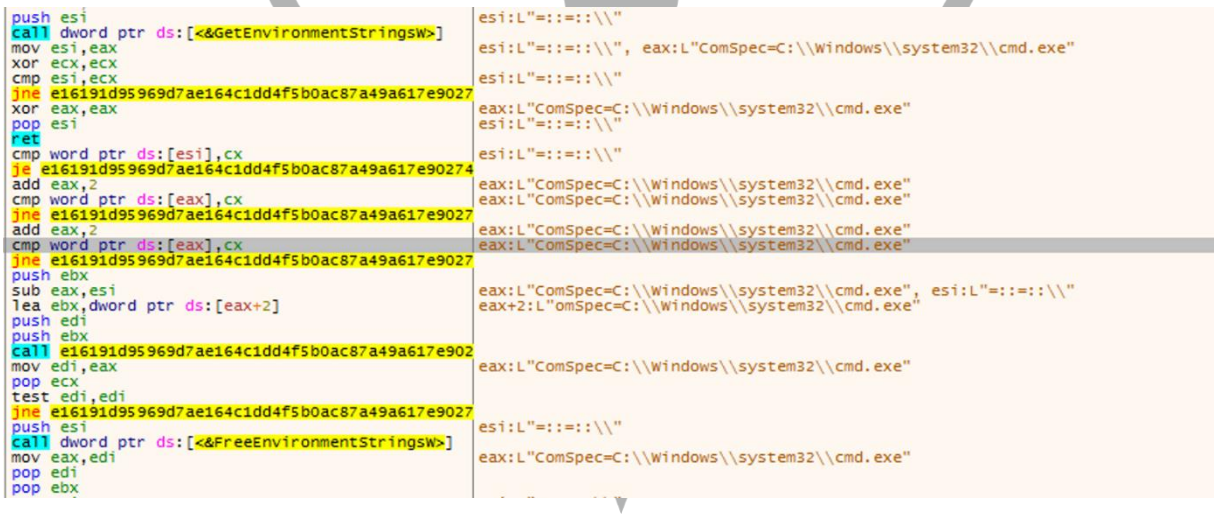
```
type=\"win32\",version=\"1.0.0.0\"C:\\Windows\\WinSxS\\manifests\\x86_microsoft.windows.isolationautomation_6595b64144ccf1df_1.0.0.0_none_35d357a66c38ade4.manifest
```

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



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.



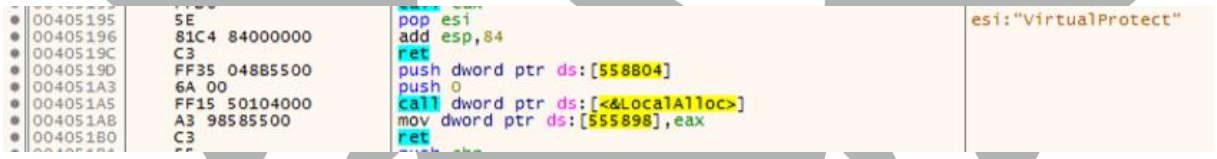
Şekil 5- Sistemin bilgilerini toplamaktadır

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.

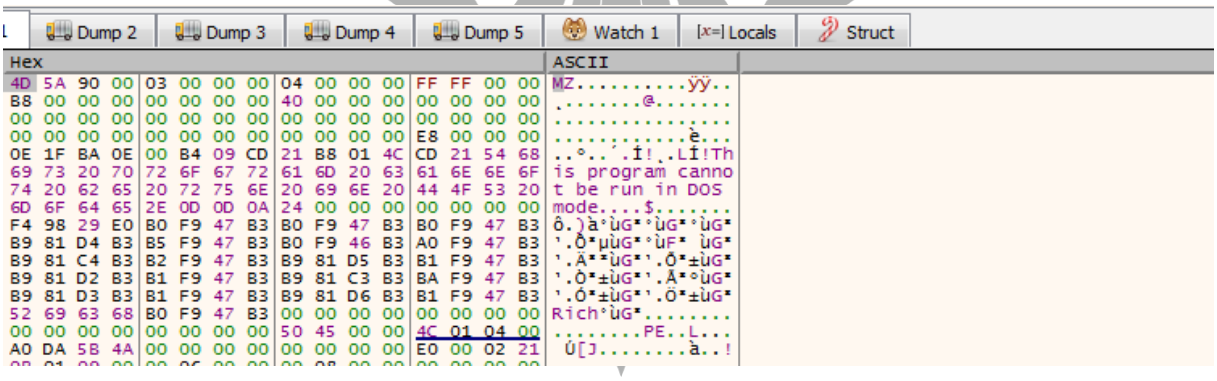
ALLUSERSPROFILE=C:\\ProgramData	NUMBER_OF_PROCESSORS=4
LOGONSERVER=\\\\ICEKING-PC	LOCALAPPDATA=C:\\Users\\user\\AppData\\Local
FP_NO_HOST_CHECK=NO	COMPUTERNAME=ICEKING-PC
OS=Windows_NT	PROCESSOR_ARCHITECTURE=x86
HOMEDRIVE=C:	ComSpec=C:\\Windows\\system32\\cmd.exe
TEMP=C:\\Users\\user\\AppData\\Local\\Temp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

Tablo 6- Zararlının edindiği bilgiler



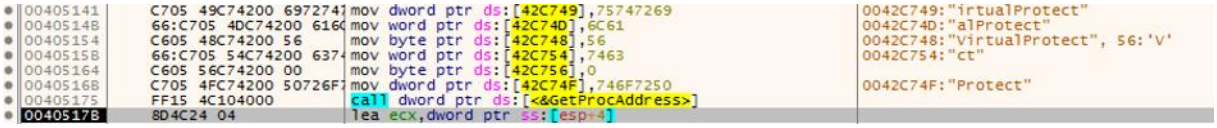
Şekil 7- LocalAlloc kullanıldığı görülmektedir

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



Şekil 7- Çıkarılan dosyanın hex kodu

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



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.

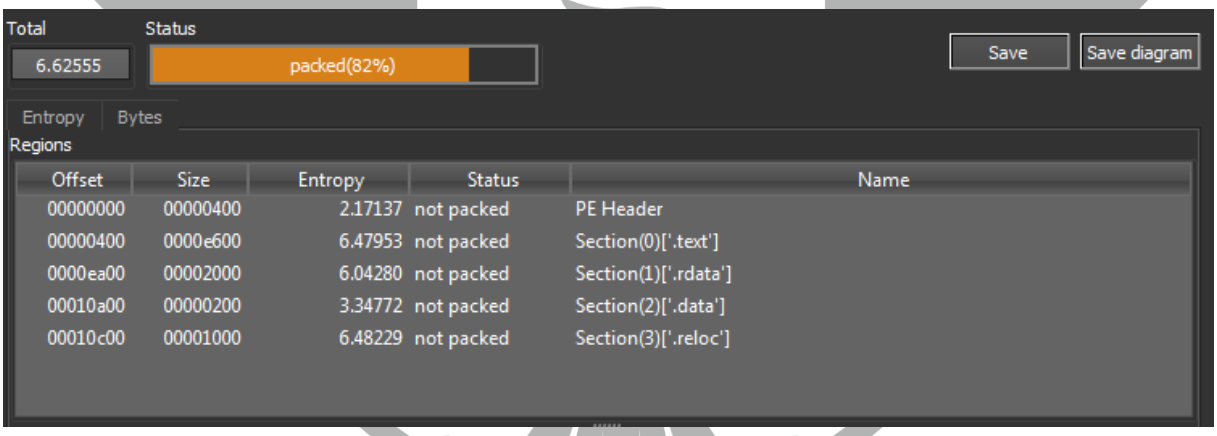
VirtualProtect API'sini kullanmak üzere bu çözümlenme yapılmaktadır. Bulunduğu DLL GetProcAddress'e parametre olarak verildikten sonra dışarı aktarılan VirtualProtect API'sinin adresi döndürülmektedir. Bu şekilde çözümleme işlemi tamamlanmaktadır.

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

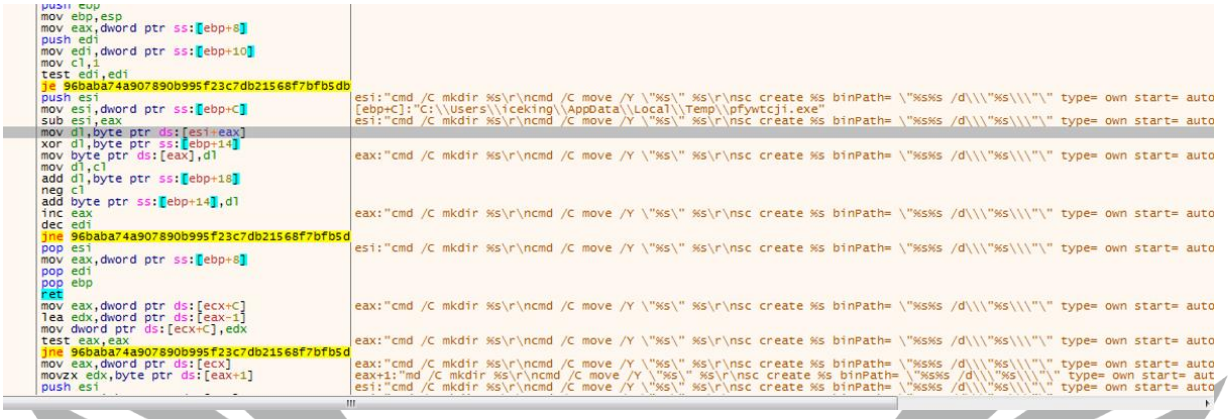
Statik Analiz



Şekil 10- Çıkarılan dosyada paketleme işlemi görülmemektedir.

Çıkarılan zararlı paketlenmiş değildir.

Dinamik Analiz



Şekil 11- CMD komutları gözükmektedir

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

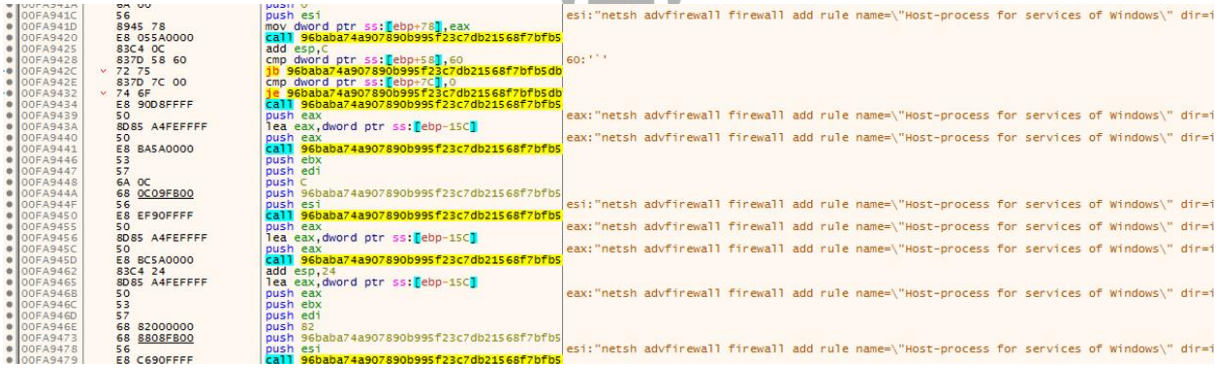
cmd /C mkdir %s\r\n

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

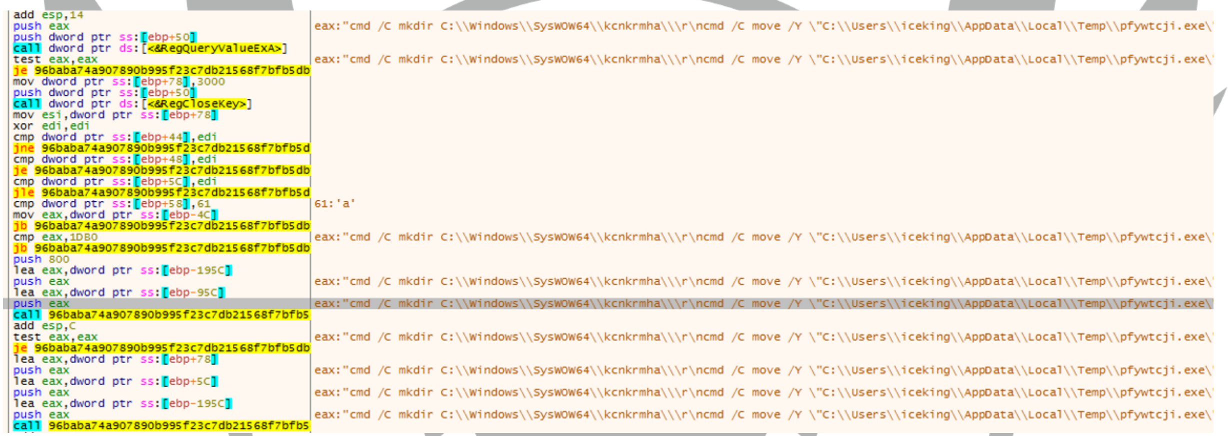
sc start %s\r\n”



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
```

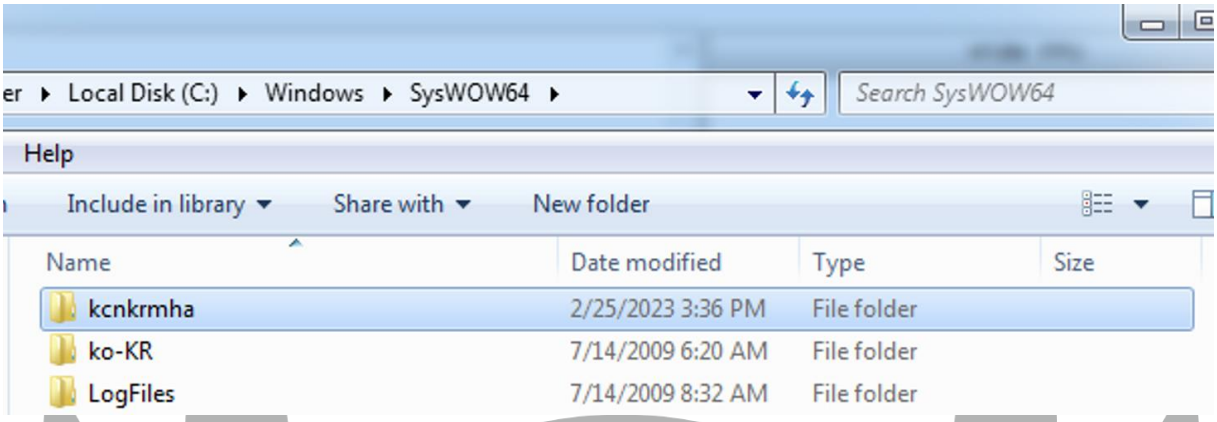
Zararlı, Windows Güvenlik Duvarı'na bir kural ekleyerek kendi trafiğine izin verir."Host-process for services of Windows" adıyla oluşturulan kural, gelen trafiğe izin vermektedir. Kuralın uygulanacağı program daha sonra ***"C:\\Users\\user\\AppData\\Local\\Temp\\pfywtcji.exe\"*** olarak belirlenir.



Şekil 13- Kendini sistem dosyalarına kopyalamaktadır

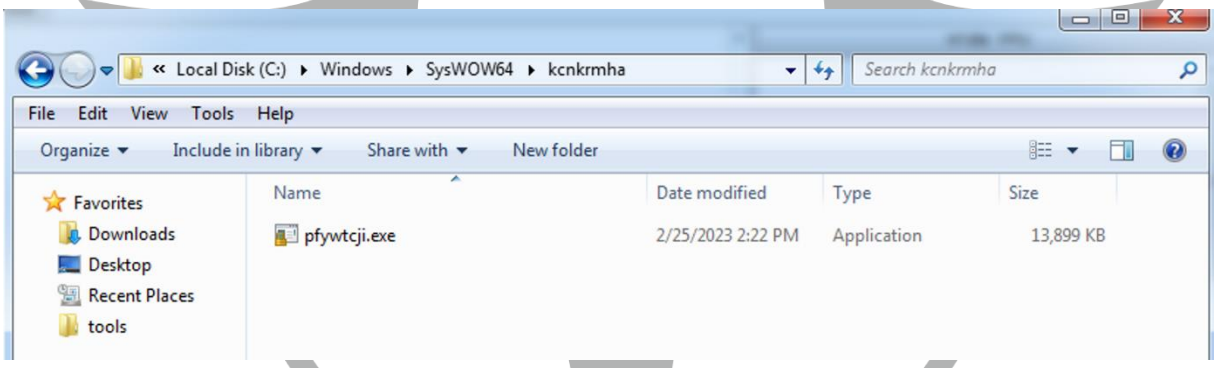
Dinamik oluşturulmuş komutlara değişken değerleri eklenmektedir. Değişken değerleri eklenmiş kodlar aşağıda verilmiştir.

```
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
```



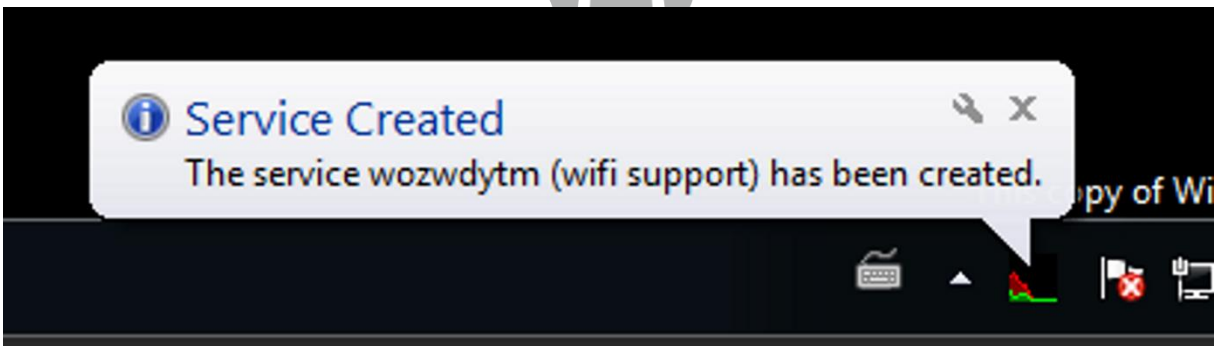
Şekil 8- SysWOW64 içinde oluşturulan dizin

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.

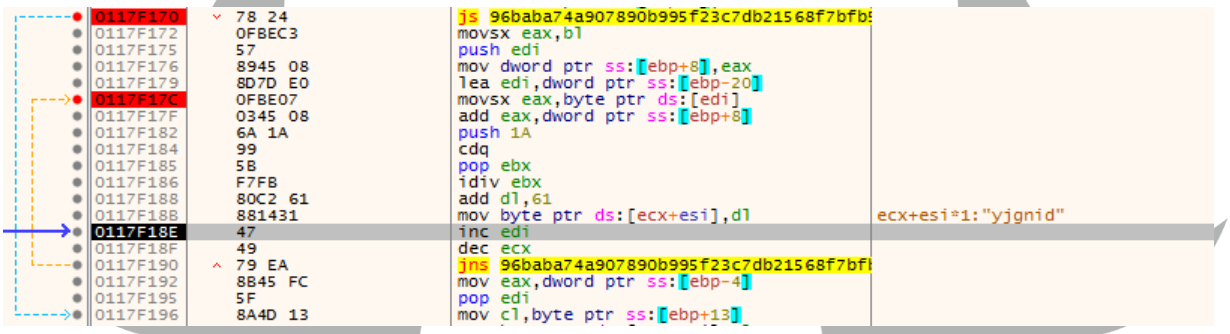


Şekil 10- "wifi support" ismiyle bir servis oluşturulmaktadır

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.



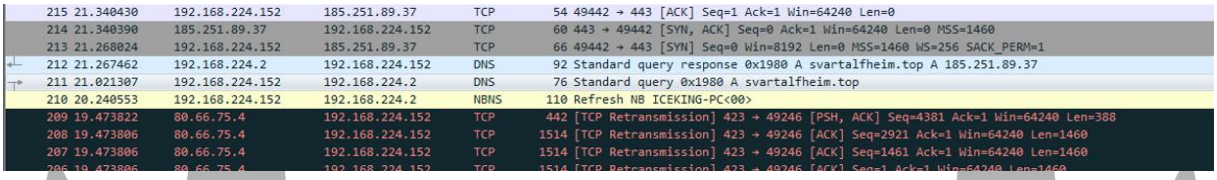
Şekil 11- İsimlerin rastgele oluştuğu yerlerden biri gözükmektedir

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

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

Şekil 18- İsimleri oluşturmakta kullanılan değişkenler

Bu değişkenler isim oluşturma algoritmasında kullanılmaktadır. Rastgele isimler ile her çalışma anında farklı dosya ve servis ismi ile yakalanması zorlaşmaktadır.



Şekil 19- Network analizinde potansiyel C2 sunucusu

Ağ trafiğinde “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	Exfliration
	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 DOĞAN

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