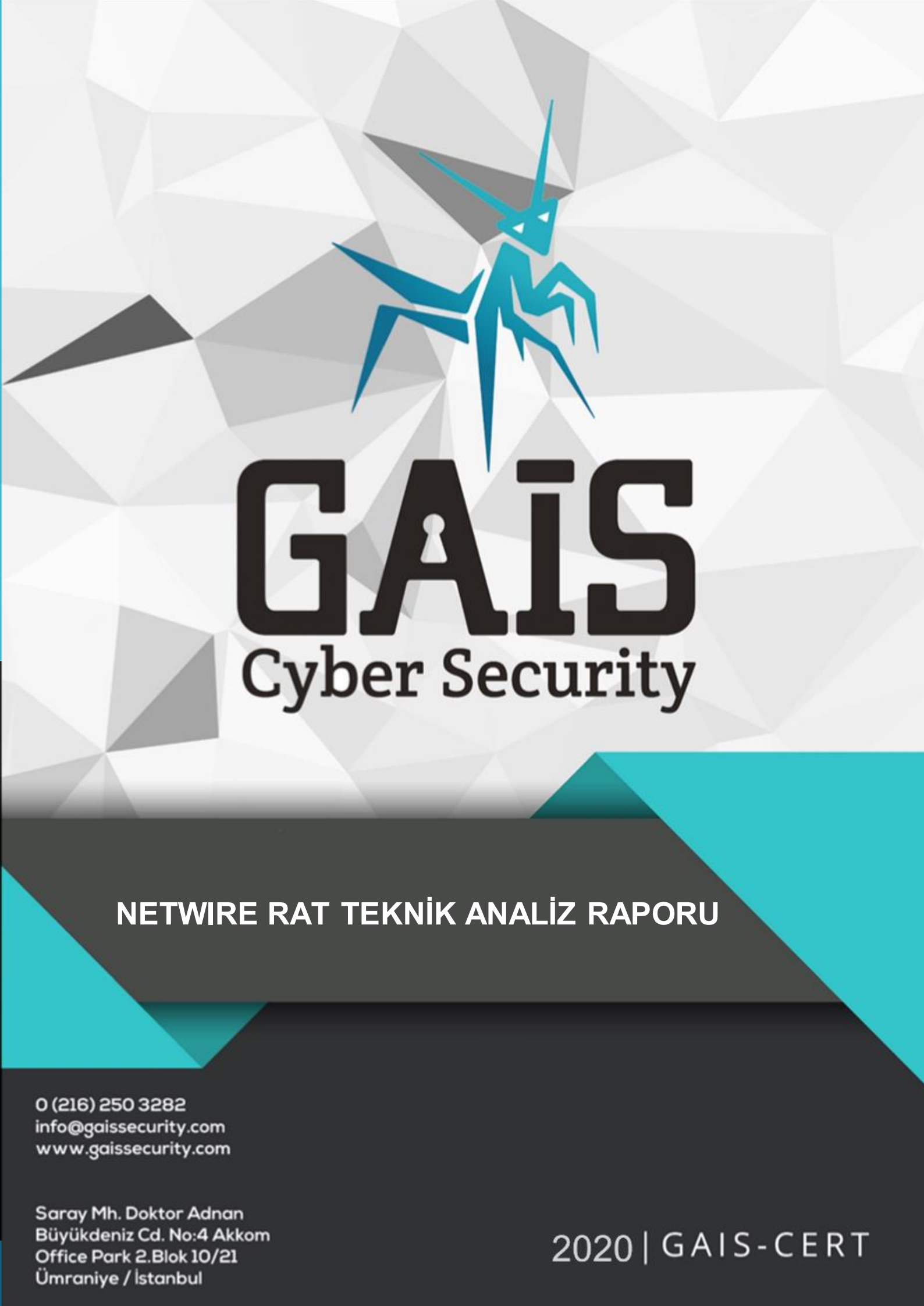


NETWIRE RAT TEKNİK ANALİZ RAPORU

0 (216) 250 3282
info@gaissecurity.com
www.gaissecurity.com

Saray Mh. Doktor Adnan
Büyükdeniz Cd. No:4 Akkom
Office Park 2.Blok 10/21
Ümraniye / İstanbul

2020 | GAIS-CERT

İÇİNDEKİLER

Remote Access Trojan türündeki NetWire zararlısına ait dosya yolları, registry kayıtları, tutulan loglar ve tüm indikatörler ile ilgili bilgiler ayrıntılı bir şekilde analiz edilip raporlanmıştır.

Giriş

RAT türündeki NetWire zararlısı, İran kökenli APT33 grubu tarafından yazılan uzaktan erişim aracıdır. İlk türevleri 2012 yılında ortaya çıkmıştır. Genel ilerleyişini Word makroları, mail phishing ve legal uygulamalar ile birlikte birleştirerek hedef sistemlere bulaşıp sistemi istismar etmektedir. İstismar edilen sistemler üzerinde çeşitli kötü amaçlı işlem gerçekleştirilebilir. Örnek olarak;

- Keylogger
- Uzaktan kontrol
- Çeşitli tarayıcılar üzerindeki verilere erişim sağlama
- Outlook içindeki hassas verilere erişme
- Clipboard üzerindeki verilere erişim

NetWire zararlısının 2012 yılından beri üretilen türevleri yeraltı hack topluluklarında ve darknet forumlarında 40 ile 140 dolar arasında Remote Administration Tool olarak satışa çıkarılmaktadır. Yapılan incelemede bu tip zararlının genelde banka vb. sistemleri hedef aldığı ortaya çıkmıştır. Windows, Linux, MacOS gibi birçok sisteme saldırabilir. En son aldığı güncelleme ile birlikte POS cihazlarına yönelik saldırılar gerçekleştirmesi çok dikkat çekmiştir.

Ön İzlenim

İncelenen bu versiyondaki NetWire zararlısı 13.05.2020 tarihinde ortaya çıkmıştır. Mail phishing yöntemi ve legal bir muhasebe uygulaması ile birleştirilerek yayılmayı sürdürmüştür. Zararlı dosyanın ilk adı “RFQ List 13052020” olarak adlandırılmıştır. Zararlının uzantısı .scr olup sisteme bu uzantı ile bulaşmaktadır. İsminden anlaşıldığı üzere bankalar ve şirketlerin muhasebe departmanını hedef almıştır. Dosya ismindeki “RFQ” fiyat teklif talebi anlamına gelip sondaki numaralar ise tarihi belirtmektedir. Örneğin: “13.05.2020”.

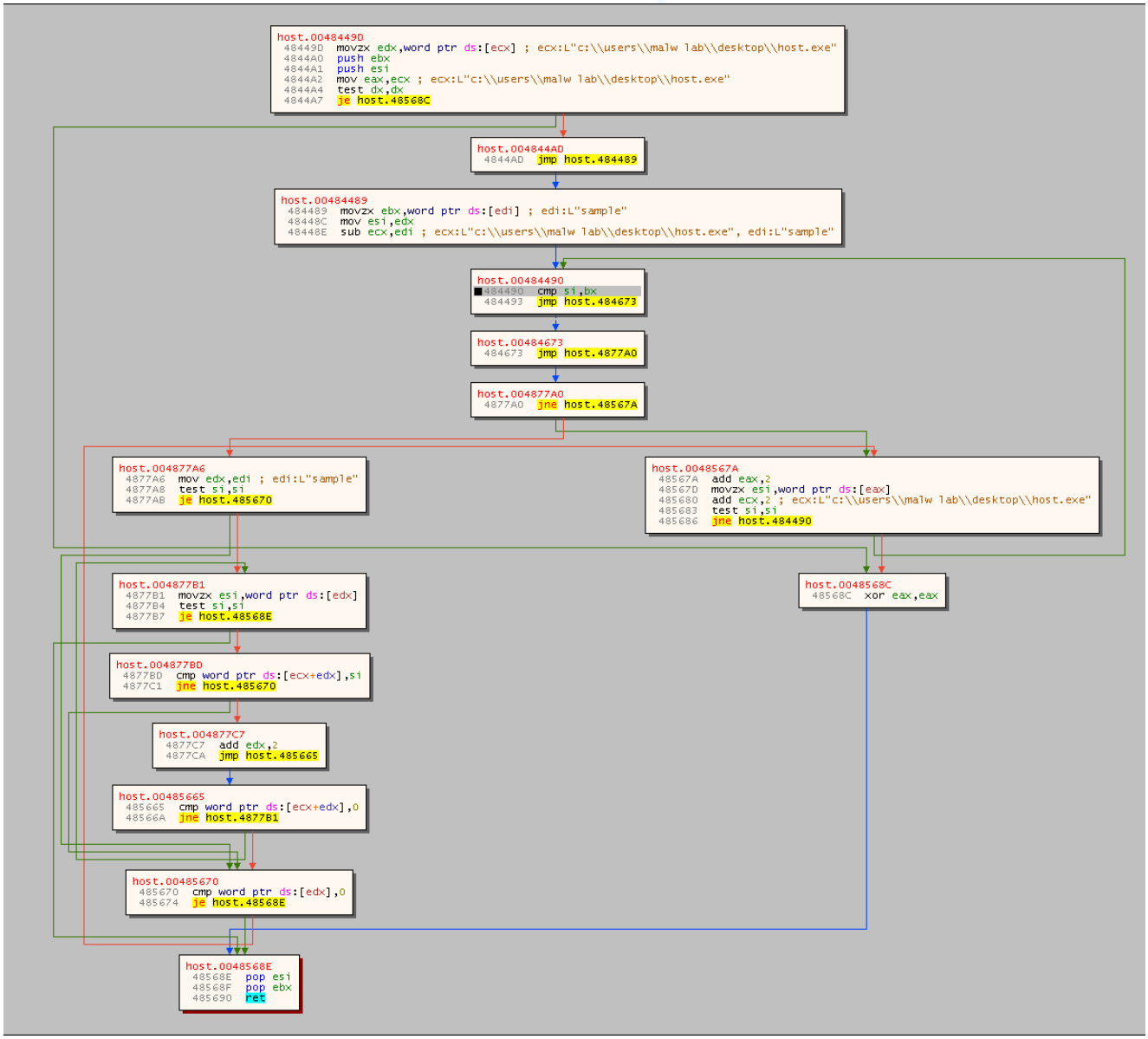
Borland Delphi 7 ile compile edilen zararlı Turbo Linker(2.25 Delphi) kullanılarak legal bir muhasebe uygulaması ile birleştirilmiştir.

Dosya Adı	RFQ List 13052020.src
MD5	72DD0F3D54F711E8F3C83A2F1B7CE6DC
SHA1	4022218FC6956E0BF458E3DA091733D9676D738A
SHA256	56CDF2F0ADFFCC195D95801F4F61DA727EDF5E6FE6BBBF0AC71462F733DF9DE9

İlk olarak şüphe çekmemesi için zararlı, karşımıza .scr uzantılı bir ekran koruyucu görünümünde çıkmaktadır. Bu .scr dosyası çalıştırıldığı zaman genelde kullanılan anti-debug yöntemleri dışında kendi farklı kontrollerinden geçer. Kullandığı bazı teknikler şunlardır;

- **Dosya yolu üzerinde analiz ortamını belirten anahtar kelime taraması**
  - Malware
  - Sample
  - Sandbox

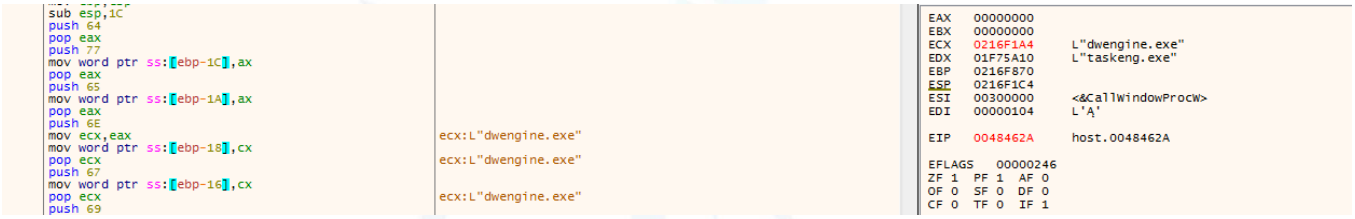
Bu anahtar kelimeleri dosya yolu ile karşılaştırarak eğer bu kelimelerden birisini içeriyor ise analiz ortamında olduğunu anlamaktadır.



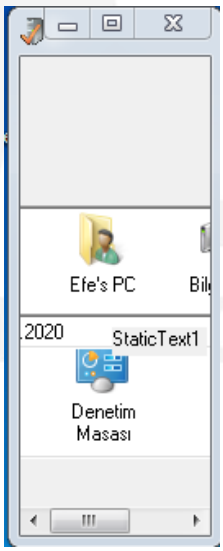
- **Çalışan processler arasında belirli anahtar kelimelerin taranması**
  - Bdwtxag.exe
  - Avgsvc.exe
  - Avgui.exe
  - Bdagent.exe
  - Avastsvc.exe

- Dwengine.exe
- Nissrv.exe
- Procmon.exe
- Ollydbg.exe
- Procmon64.exe
- Procexp64.exe
- Windbg.exe
- Avp.exe

Anti-virüs programları ve analiz araçlarına yönelik bir anahtar kelime taraması yapmaktadır.

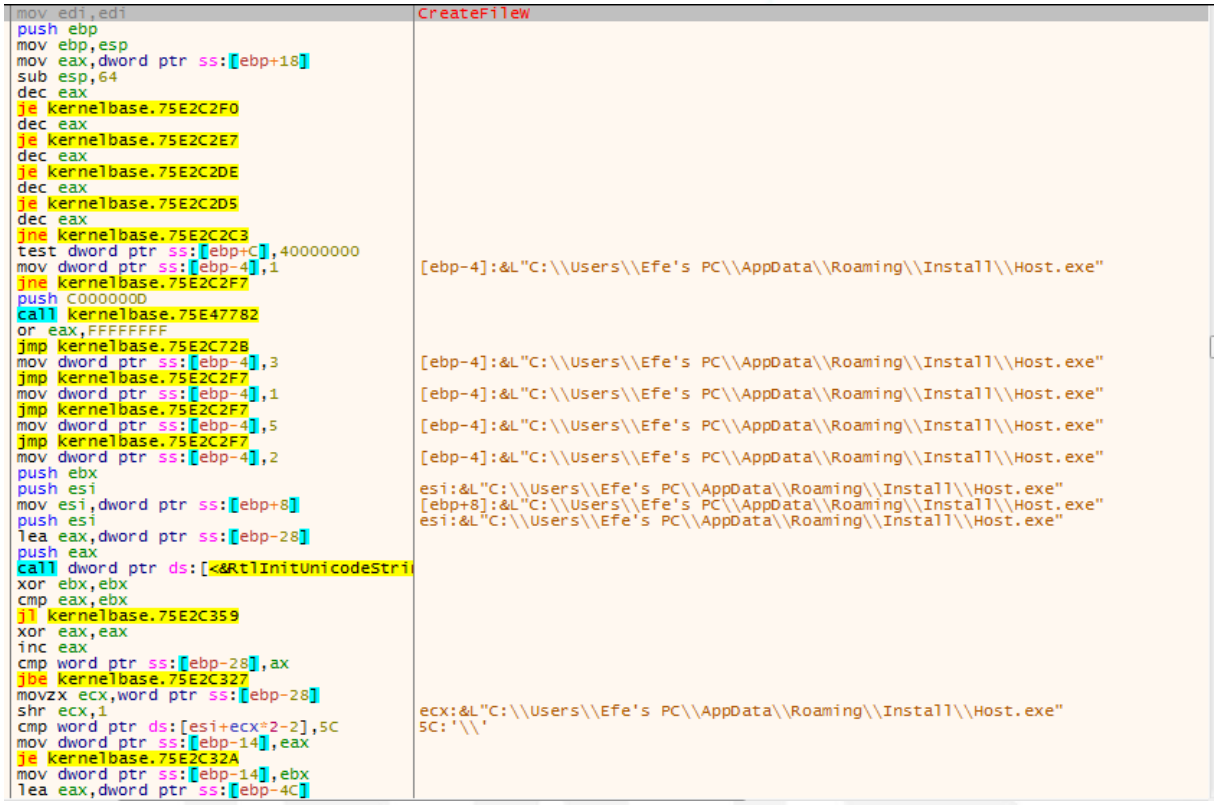


Belirli yerlerde anti-debug yöntemleri tetiklenirse, analizi şaşırtma amaçlı farklı bir legal uygulama açmaktadır. Bu uygulama basit bir dosya görüntülemeye yarayan ve içinde ufak bir ajandası olan muhasebe uygulaması gibi gözükmektedir.

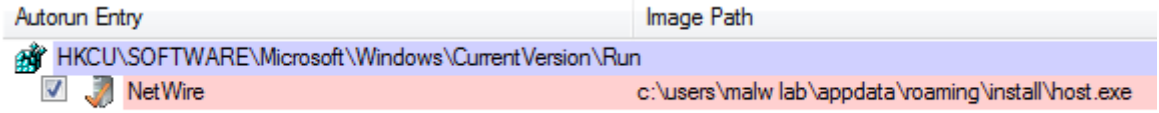


Bu anahtar kelimelere dayalı taramayı yaptıktan sonra eğer analiz ortamında değil ise kendisini **APPDATA** içine Host.exe olarak kopyalamakta ve başlangıca eklemektedir. Bundan sonra işlemleri Host.exe üzerinden yürütmektedir. Eğer bir analiz ortamında olduğunu tespit ederse sistem üzerinde hiçbir faaliyet göstermeden kendini sonlandırmaktadır.

RFQ List 13052020.src isimli ekran koruyucu dosyasının tek amacı **anti-debug** yöntemleri ile analiz ortamında olup olmadığını belirleme ve Host.exe'yi APPDATA üzerine kopyalayıp, başlangıca eklemektir. Bu işlemlerden sonra geri kalan kısım Host.exe tarafından yürütülecektir.



RAT türündeki NetWire zararlısı, kendisini AppData/Roaming/Install konumuna **Host.exe** adında kopyalamaktadır.

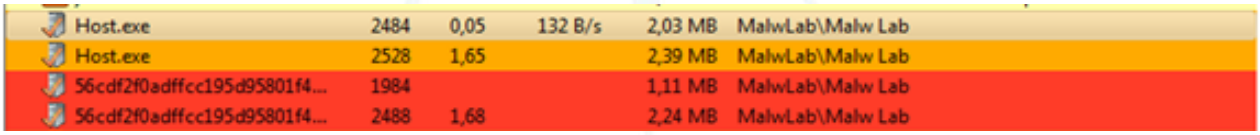


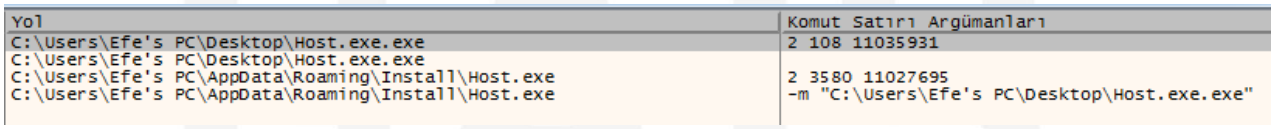
Ayrıca sistemde süreklilik sağlamak amacı ile kendisini kayıt defterinde sistem başlangıcına eklemektedir.

Host.exe Dosya Analizi

Dosya Adı	Host.exe
MD5	72DD0F3D54F711E8F3C83A2F1B7CE6DC
SHA1	4022218FC6956E0BF458E3DA091733D9676D738A
SHA256	56CDF2F0ADFFCC195D95801F4F61DA727EDF5E6FE6BBBF0AC71462F733DF9DE9

APPDATA üzerine kopyalanan Host.exe incelendiği zaman **RFQ List 13052020.src** isimli dosya ile aynı olduğu tespit edilebilmektedir. APPDATA dizinine içeriği farklı bir dosya olarak değil, tamamen aynı olarak kendisini kopyalamaktadır. Aynı dosya gibi gözükmesine rağmen RFQ List 13052020.src dosyasından farklı olarak çalışmaktadır. Bunun sebebi kendi dosya yolu ve adını kontrol etmekte olup bu dosya adı Host.exe ve dosya yolu APPDATA içinde ise farklı komutlarda çalışmaktadır. Farklı işlemler için, farklı parametreler ile çalışmaktadır.





Zararlı çalışmaya devam ettiğinde 4 farklı process ve 2 farklı parametre alarak devam etmektedir. Bu parametreler sayesinde aynı dosya farklı işlevler görmektedir.

APPDATA dizininde değil ve dosya adı Host.exe değil ise **-m** parametresi ile kendini başlatıp log tutma, bağlantı kurma gibi zararlı aktiviteleri gerçekleştirmektedir. Eğer zararlı uygulama APPDATA dizini üzerinde ve dosya adı Host.exe ise bu işlemleri parametre almadan gerçekleştirmektedir.

Diğer parametre ile çalıştığında ise log tutma ve bağlantı yapan zararlı uygulamanın kapanmaması gibi işlemleri sağlamaktadır.–m parametresi ile ya da APPDATA üzerinden direk olarak çalışmış ve programın çalışması durdurulmuş ise tekrar çalıştırılmaktadır.

Host.exe Davranış Analizi

APPDATA üzerinde çalışan Host.exe adındaki zararlı düzgün bir şekilde çalıştırıldığında kullandığı fonksiyon ve API'lar sayesinde çeşitli zararlı işlemler gerçekleştirmektedir. Bu işlemler arasında iki temel fonksiyon vardır.

Birinci fonksiyon sistem üzerinde elde edilen bilgilerin şifreli bir dosya oluşturarak LOG tutması işlemini gerçekleştirmektedir.

```
mov dword ptr ss:[ebp-4],1          [ebp-4]:L"C:\\Users\\Efe's PC\\AppData\\Roaming\\Logs\\19-05-2020"
jne kernelbase.75E2C2F7
push C000000D
call kernelbase.75E47782
or eax,FFFFFFFF
jmp kernelbase.75E2C72B
mov dword ptr ss:[ebp-4],3          [ebp-4]:L"C:\\Users\\Efe's PC\\AppData\\Roaming\\Logs\\19-05-2020"
jmp kernelbase.75E2C2F7
mov dword ptr ss:[ebp-4],1          [ebp-4]:L"C:\\Users\\Efe's PC\\AppData\\Roaming\\Logs\\19-05-2020"
jmp kernelbase.75E2C2F7
mov dword ptr ss:[ebp-4],5          [ebp-4]:L"C:\\Users\\Efe's PC\\AppData\\Roaming\\Logs\\19-05-2020"
jmp kernelbase.75E2C2F7
mov dword ptr ss:[ebp-4],2          [ebp-4]:L"C:\\Users\\Efe's PC\\AppData\\Roaming\\Logs\\19-05-2020"
push ebx
push esi
mov esi,dword ptr ss:[ebp+8]        [ebp+8]:L"C:\\Users\\Efe's PC\\AppData\\Roaming\\Logs\\19-05-2020"
push esi
lea eax,dword ptr ss:[ebp-28]
```

Log dosyası **AppData/Roaming/Logs/{TARİH}** şeklinde tutulmaktadır. Log dosyası içinde klavye tuş vuruşları, kopyalanan veriler gibi hassas veriler şifreli bir şekilde tutulmaktadır.

İkinci temel fonksiyon ise bu zararlının karşı taraf ile bağlantı kurarak önemli hassas verileri dışarı sızdırma görevini üstlenmektedir.

```
mov dword ptr ss:[esp+8],host.42310B    42310B:"HostId"
mov dword ptr ss:[esp+4],host.423112    423112:"SOFTWARE\\NetWire"
mov dword ptr ss:[esp],80000001
call host.410955
test al,al
jne host.40908E
lea edi,dword ptr ss:[esp+20]           [esp+20]:"194.5.97.76"
mov dword ptr ss:[esp+8],1
mov dword ptr ss:[esp+4],20             20:' '
mov dword ptr ss:[esp],edi
call host.408218
mov dword ptr ss:[esp+8],host.422580    422580:"HostId-sYKkGs"
mov dword ptr ss:[esp+4],host.423123    423123:"%Rand%"
mov dword ptr ss:[esp],0
call host.412876
test eax,eax                            eax:"194.5.97.76"
js host.4090BF
add eax,host.422580                     eax:"194.5.97.76", 422580:"HostId-sYKkGs"
mov dword ptr ss:[esp+4],6
mov dword ptr ss:[esp],eax
call host.4105BA
jmp host.4090BF
mov dword ptr ss:[esp+10],20            20:' '
mov dword ptr ss:[esp+C],ebx
mov dword ptr ss:[esp+8],host.42312A    42312A:"Install Date"
mov dword ptr ss:[esp+4],host.423112    423112:"SOFTWARE\\NetWire"
```

Ayrıca zararlı bu iki ana fonksiyon dışında aşağıdaki zararlı işlemleri de yapmaktadır;

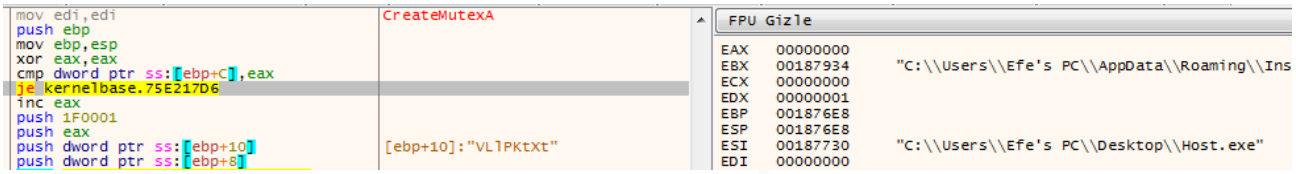
- Windows kayıt defteri içinde tarama yapma,
- Sistemde bulunan monitörler için tarama yapma,
- Başka bir çalıştırılabilir dosyayı çalıştırma,
- Sistem üzerinde herhangi bir komut çalıştırma,
- Sistem üzerinde bulunan dizin ve dosyalar arasında tarama yapma,
- Kullanıcı Mail bilgilerini elde etme,
- Kullanıcının tarayıcıdaki hassas verilerini elde etme.

```
%s\BraveSoftware\Brave-Browser\User Data\Default\Login Data
%s\BraveSoftware\Brave-Browser\User Data\Local State
SOFTWARE\
SOFTWARE\NetWire
Software\Microsoft\Internet Explorer\IntelliForms\Storage2
Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

Kayıt defterini okuyarak kullanıcın **Outlook** üzerindeki hassas verilerini elde edebilmektedir. Aynı şekilde kayıt defteri sayesinde **Shell Folders** da tutulan sistemdeki kök dizinlerinin bilgisini elde etmektedir.

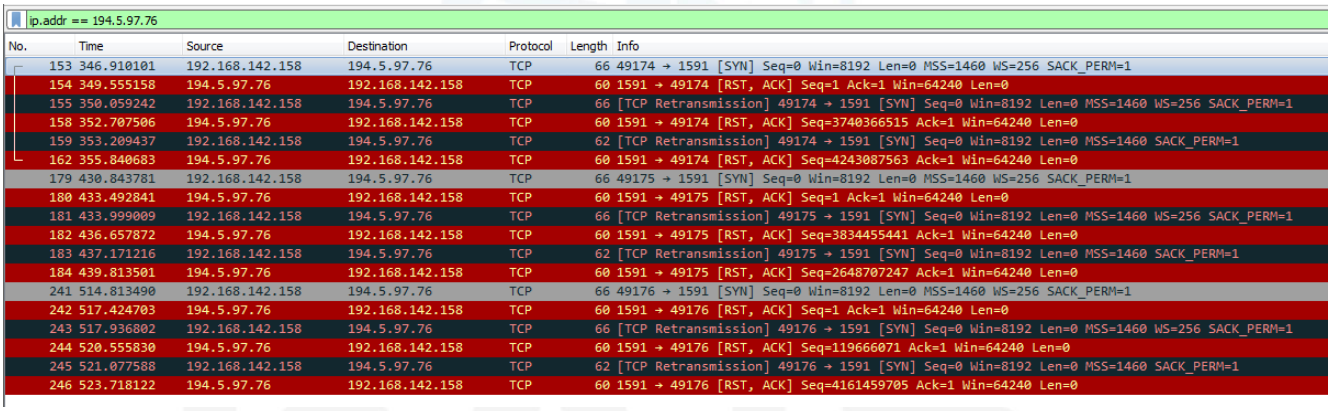
0002295D	%s\Google\Chrome\User Data\Default\Login Data
0002298B	%s\Google\Chrome\User Data\Local State
000229B2	%6\PI0WI4QI\u6d0 aC5C\ad8CQi5\mWn4R aC5C
000229DB	%s\Chromium\User Data\Default\Login Data
00022A04	%s\Chromium\User Data\Local State
00022A26	%6\PWIWSW\a0CnWR\u6d0 aC5C\ad8CQi5\mWn4R aC5C
00022A54	%s\Comodo\Dragon\User Data\Default\Login Data
00022A82	%s\Comodo\Dragon\User Data\Local State
00022AA9	%6\vCRSdf\vCRSdfc0Wg6d0\u6d0 aC5C\ad8CQi5\mWn4R aC5C
00022ADE	%s\Yandex\YandexBrowser\User Data\Default\Login Data
00022B13	%s\Yandex\YandexBrowser\User Data\Local State
00022B41	%s\BraveSoftware\Brave-Browser\User Data\Default\Login Data
00022B7D	%s\BraveSoftware\Brave-Browser\User Data\Local State
00022BB2	%s\360Chrome\Chrome\User Data\Default\Login Data
00022BE6	Chrome\Chrome\User Data\Default\Login Data
00022C11	%s\360Chrome\Chrome\User Data\Local State

Çeşitli tarayıcılarda tutulan kullanıcının giriş verileri, tarayıcı geçmişi gibi hassas verileri de C&C sunucularına sızdırmaktadır.



Zararlı ayrıca, sistem üzerinde "**VLlPKtXt**" adında mutex nesnesi oluşturmaktadır.

Network Analizi



C&C sunucusu olan **194[.]5.97[.]76** IP adresine RAT türündeki NetWire zararlısı sürekli olarak 1591 portuna bağlantı isteği yollamaktadır. Fakat port kapalı olduğu için C&C sunucusundan sürekli **RST** bayrağı dönmektedir.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
Host.exe	3516	TCP	malwlab.localdomain	49163	194.5.97.76	1591	SYN_SENT
lsass.exe	536	TCP	MalwLab	49157	MalwLab	0	LISTENING

Çözüm Önerileri

- Sistemlerde güncel, güvenilir bir antivirüs yazılımın kullanılması,
- Gelen maillerin özenle okunması, içinde bulunan eklerin taramadan geçirilmeden açılmaması,
- Spam maillerin dikkate alınmaması,
- İnternet üzerinde dolaşım yaparken phishing içeriklere dikkat edilmesi,
- İşletim sisteminde bulunan en son güncellemelerin yüklü olması,
- Sistem üzerindeki çalışan processlerin yaptığı işlemler ve ağ hareketlerinin izlenmesi
- Ağ üzerinde zararlı bağlantı kuran, IP adresleri, domainler ve C&C sunucularının adreslerinin filtrelenmesi gibi üretilen çözümler, RAT türündeki NetWire zararlısının sisteme bulaşmasını ve zarar vermesini engelleyebilmektedir.

YARA Kuralı

```
import "hash"
rule NetWire: RAT
{
    meta:
        description = "Netwire Banking Trojan"
        version = "NetWire v2.1 R5"
        first_date = "13.05.2020"
        report_date = "08.03.2020"
        file_name = "Host.exe"

    strings:
        $s1 = "P.rsrc" fullword
        $s2 = "P.reloc" fullword
        $s3 = "WWWWWWWW$.c" fullword
        $s4 = ".db2" fullword
        $s5 = "3XE4PMyW7kL2Pql3uCjp08vl8TUiLn3TlnCLUEnixJNRsbhpjQCO" fullword
        $s6 = "Host is down." fullword
        $s7 = "No route to host." fullword
        $s8 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuwxyz0123456789+/" fullword
        $s9 = "rfDesktop" fullword
        $s10="SOFTWARE\\Borland\\Delphi\\RTL" fullword
        $s11="Software\\Borland\\Delphi\\Locales" fullword
        $12="Software\\Borland\\Locales" fullword

    condition:
        hash.md5(0,filesize) == "72dd0f3d54f711e8f3c83a2f1b7ce6dc" or all of them
}
```