Meduza

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

Ön Bakış

Gizemli bir aktör tarafından hazırlanan Meduza Stealer, Windows kullanıcılarını ve kuruluşlarını hedef alacak şekilde özel olarak tasarlanmıştır. Şu an için yalnızca belirli on ülke haricinde etkin olduğu bilinmektedir. Meduza Stealer'ın ana hedefi kapsamlı veri hırsızlığıdır. Kullanıcıların tarama etkinliklerini ele geçirerek tarayıcıyla ilgili çeşitli verileri toplar. Bu veriler, kritik oturum açma bilgilerinden değerli tarama geçmişi kayıtlarına ve özenle seçilmiş yer imlerine kadar geniş bir yelpazeyi kapsamaktadır. Kripto cüzdanı uzantıları, şifre yöneticisi ve iki faktörlü kimlik doğrulama uygulamaları dahil olmak üzere bu tehdide karşı savunmasızdır.

Bu kötü amaçlı yazılım;

- Web tarayıcılarına kaydedilen kimlik bilgilerine,
- Web tarayıcılarına kaydedilen kripto cüzdan bilgilerine,
- Web tarayıcılarına kaydedilen çerez bilgilerine,
- Şifre yöneticisi uygulamalarına,
- İki faktörlü kimlik doğrulama uygulamalarına,
- Kayıtlı Outlook hesaplarıyla ilgili bilgilere,
- Bilgisayardaki sistem bilgilerine,
- Bilgisayardaki bazı uygulamaların tuttuğu kimlik bilgilerine,
- Bilgisayar belgelerine,

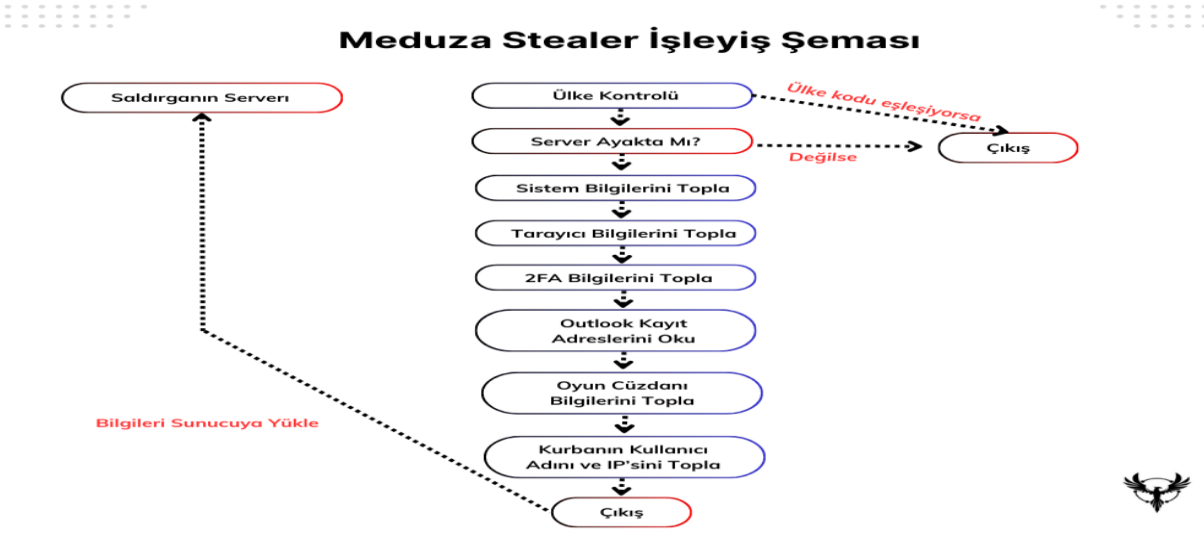
  Erişim sağlamaktadır.

Meduza.exe Analizi

Adı	meduza.exe
MD5	C6068C2C575E85EB94E2299FC05CBF64
SHA256	0d0a4622c58f3f17d16fb5cbd0aa5403bc614ca58847b4a725f432d202a55454
Dosya Türü	PE64 / EXE

Genel Bakış

Meduza Stealer, zararlı eylemlerine başlamadan önce bir anti-debug tekniği olarak **IsDebuggerPresent** API kullanılmıştır. Bunu yapmasındaki amaç analistin işini zorlaştırmaktır. Ardından **ülke kodlarını** ve **windows işletim sistemi sürümünü** kontrol etmektedir. Kontrollerin sağlanması durumunda asıl zararlı işlemlerin yapıldığı fonksiyonlar çağrılmaktadır. Zararlının amacı; sistem bilgilerinin, tarayıcı verilerinin, şifre yöneticisi ayrıntılarının, madencilikle ilgili kayıt defteri bilgilerinin ve yüklü uygulamalara ilişkin ayrıntılarının toplanmasını içermektedir. Bu detaylı bilgilerin tümü toplandıktan sonra paketlenmektedir. Saldırganın komuta kontrol sunucusuna yüklenmeye hazır hale gelmektedir. İşlemler tamamlandıktan sonra arka planda program kendini silerek zararlı eylemlerine son vermektedir.



Şekil 1 – Zararlının İşleyiş Şeması

Zararlının dil kontrolü yapılarak çalıştırılması engellenen ülkeler:

Rusya	Ermenistan	Belarus
Kazakistan	Özbekistan	Tacikistan
Moldova	Kırgızistan	Türkmenistan
Gürcistan		

Şekil 2 – Dil Kontrolü Yapılan Ülkeler Tablosu

Zararlının hedeflediği şifre yöneticileri ve iki faktörlü kimlik doğrulama uygulamaları:

GAuthAuthenticator	Authenticator	SafePal	Guarda
EOS Authenticator	BrowserPass	KeePassXC	1Password
Trezor Password Manager	Dashlane	Bitwarden	LastPass
Keeper	Nordpass	RoboFrom	Splikity
MYKI	Zoho Vault	Authy	

Şekil 3 – Zararlının Hedeflediği Şifre Yöneticileri ve İki faktörlü kimlik doğrulama Listesi

Zararlının hedeflediği masaüstü uygulamaları:

Discord	Telegram	Jaxx_Liberty

Şekil 4 – Zararlının Hedeflediği Masaüstü Uygulamalar Listesi

Zararlının hedeflediği tarayıcılar:

Microfost Edge	Mozilla Firefox	Pale Moon	Suhba	RockMelt
Google Chrome	Chromium	Amigo	QQBrowser	Vivaldi
CrytoTab Browser	TorBro Browser	Cent Browser	Opera	Brave Old
Chedot Browser	Torch	7Star	Tencent	OperaGX
Privacy Browser	Yandex Browser	360 Browser	Orbitum	Xpom
Comodo Dragon Epic	Opera Browser	SalamWeb	Kinza	Xvast
Nichrome	Slim Browser	Chromodo	Go Browser	Maxthon
Mail.Ru Atom	CocCoc Browser	Coowon		

Şekil 5 – Zararlının Hedeflediği Tarayıcılaın Listesi

Zararlının hedeflediği kripto cüzdanlar:

Electrum	Electrum-LTC	Exodus	ElektronCash	MultiDoge
Jaxx_Desktop_Old	Atomic	Binance	Coinomi	Monero
TronLink	MetaMask	Wasabi Wallet	Yoroi	DashCore
Niftywallet	Mathwallet	Coinbase	Guarda	EQUALWallet
JaxxLiberty	BitAppWallet	iWallet	Wombat	MeWCx
Guidwallet	RoninWallet	Neoline	CloverWallet	Liqualitywallet
Terra Station	Keplr	Sollet	AuroWallet	PolymeshWallet
ICONex	Harmony	Coin98	EVER Wallet	KardiaChain
Rabby	Phantom	BraveWallet	Atomic	Paliwallet
Boltx	Xdefiwallet	NamiWallet	MaiarDeFiWallet	Goby
Solflare	Cyanowallet	TezBox	Temple	
BinanceChainWallet	Blockstream Green	Daedalus	Waveskeepe	

Şekil 6 – Zararlının Hedeflediği Kripto Cüzdanların Listesi

Zararlının topladığı sistem ayrıntıları:

Sistem Bileşenleri Ayrıntıları	Bilgisayar Adı
CPU Detayları	Çalışma Yolu
Coğrafi Konum	GPU
Donanım Kimliği	Public IP
İşletim Sistemi Ayrıntıları	RAM Detayları
Ekran Çözünürlük Ayrıntıları	Ekran Görüntüsü
Zaman	Saat Dilimi

Şekil – 7 Zararlının Topladığı Sistem Ayrıntıları

Dinamik Analiz

Zararlı, herhangi bir zararlı aktivite göstermeden önce **IsProcessorFeaturePresent** API ile çalıştığı cihazın işletim sisteminin Windows 7 veya altı olup olmadığını kontrol etmektedir.

```
BOOL __fastcall sub_13F09CE8C(DWORD64 a1)
{
  DWORD64 retaddr; // [rsp+38h] [rbp+0h]
  DWORD64 v3; // [rsp+40h] [rbp+8h] BYREF

  v3 = a1;
  if ( IsProcessorFeaturePresent(0x17u) )
    __fastfail(2u);
  capture_previous_context(&ContextRecord);
  ContextRecord.Rip = retaddr;
  ContextRecord.Rsp = (DWORD64)&v3;
  qword_13F0DA790 = retaddr;
  ContextRecord.Rcx = v3;
  dword_13F0DA780 = -1073740791;
  dword_13F0DA784 = 1;
  dword_13F0DA798 = 1;
  unk_13F0DA7A0 = 2i64;
  return _raise_securityfailure((struct _EXCEPTION_POINTERS *)&ExceptionInfo);
}
```

Şekil 8 – İşletim Sistemi Sürüm Tespitinin Elde Edilmesi

Ardından zararlı, bilgisayara ait işlemci ve mimari bilgilerini elde etmektedir.

```
000000013FB3EC04  C5FE6F52 20          vmovdqu ymm2,yword ptr ds:[rdx+20]      rdx+20:L"OM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC"
000000013FB3EC09  C5FE6F5A 40          vmovdqu ymm3,yword ptr ds:[rdx+40]      rdx+40:L"D;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC"
000000013FB3EC0E  C5FE6F62 60          vmovdqu ymm4,yword ptr ds:[rdx+60]      rdx+60:L".JSE;.WSF;.WSH;.MSC"
000000013FB3EC13  C5FD7F09             vmovdqa yword ptr ds:[rcx],ymm1
000000013FB3EC17  C5FD7F51 20          vmovdqa yword ptr ds:[rcx+20],ymm2
000000013FB3EC1C  C5FD7F59 40          vmovdqa yword ptr ds:[rcx+40],ymm3      rcx+40:L"`1"
000000013FB3EC21  C5FD7F61 60          vmovdqa yword ptr ds:[rcx+60],ymm4
000000013FB3EC26  C5FE6F8A 80000000    vmovdqu ymm1,yword ptr ds:[rdx+80]      rdx+80:L"MSC"
000000013FB3EC2E  C5FE6F92 A0000000    vmovdqu ymm2,yword ptr ds:[rdx+A0]      rdx+A0:L"CHITECTURE=AMD64"
000000013FB3EC36  C5FE6F9A C0000000    vmovdqu ymm3,yword ptr ds:[rdx+C0]
000000013FB3EC3E  C5FE6FA2 E0000000    vmovdqu ymm4,yword ptr ds:[rdx+E0]      rdx+E0:L"IFIER=Intel64 Family 6 Model 165 Stepping 2, GenuineIntel"
000000013FB3EC46  C5FD7F89 80000000    vmovdqa yword ptr ds:[rcx+80],ymm1
000000013FB3EC4E  C5FD7F91 A0000000    vmovdqa yword ptr ds:[rcx+A0],ymm2
```

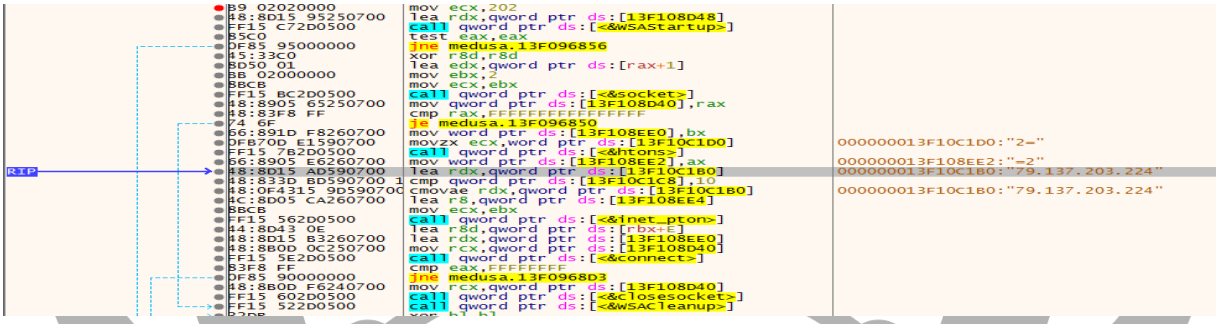
Şekil 9 – İşlemci ve Mimari Bilgilerini Elde Edilmesi

Meduza Stealer, bir makineye başarılı bir şekilde sızdığında gerçekleştirdiği ilk adım coğrafi konumu kontrol etmektir. Kurbanın coğrafi konumu hırsızın önceden tanımlanmış listesinde yer alıyorsa (Bkz. Şekil 2) zararlı yazılım çalışmamaktadır.

```
00000013FB2E761   74 1D          je medusa.13FB2E780
00000013FB2E763   48:8BD7        mov rdx,rdi                              rdx:"RU", rdi:"RU"
00000013FB2E766   48:8BCB        mov rcx,rbx                              rcx:"RU"
00000013FB2E769   E8 72070000    call <medusa.country_code_check_list>
00000013FB2E76E   48:83C3 20     add rbx,20
00000013FB2E772   48:895C24 30   mov qword ptr ss:[rsp+30],rbx            [rsp+30]:"RU"
00000013FB2E777   48:83C7 20     add rdi,20                               rdi:"RU"
00000013FB2E77B   48:3BFD        cmp rdi,rbp
00000013FB2E77E   75 E3          jne medusa.13FB2E763
00000013FB2E780   48:895C24 28   mov qword ptr ss:[rsp+28],rbx            [rsp+28]:"RU"
00000013FB2E785   48:8BD3        mov rdx,rbx                              rdx:"RU"
00000013FB2E788   48:8BCB        mov rcx,rbx                              rcx:"RU"
00000013FB2E78B   E8 60320000    call medusa.13FB319F0
```

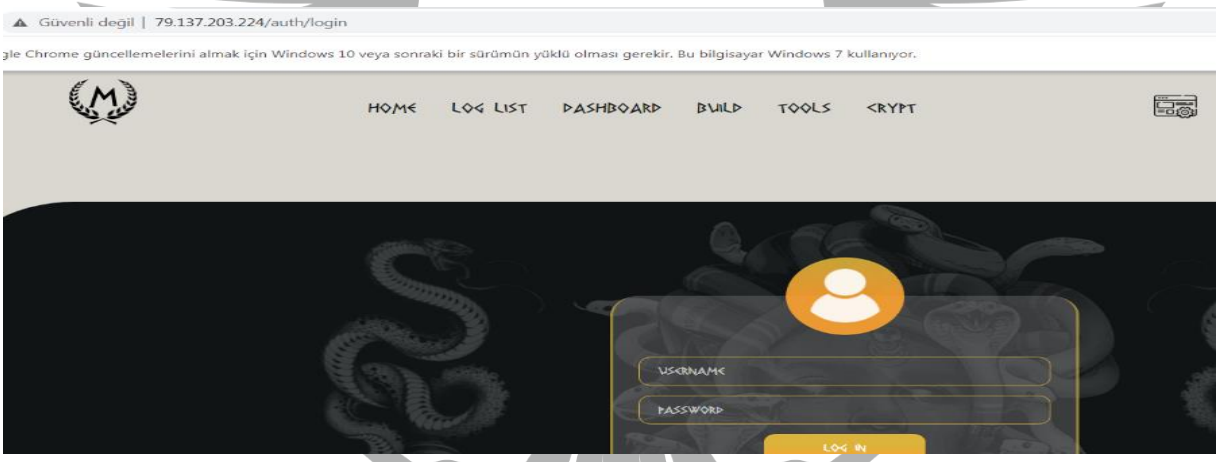
Şekil 10 – Ülke Kodlarına Bakılarak Hedef Ülke Kontrollerinin Elde Edilmesi

Zararlı Şekil 11'de sunucu kontrolü gerçekleştirmektedir. Sunucu ayakta ise kötü niyetli işlemlerine devam etmekte olup aksi durumda işlemlerine son vermektedir.



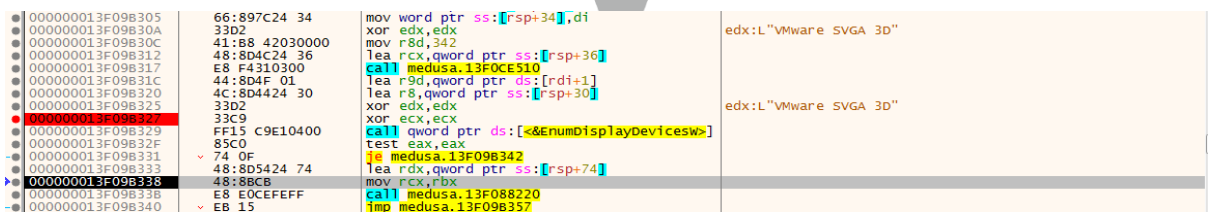
Şekil 11 – Zararlının İstek Attığı IP Adresine Yaptığı Bağlantının Elde Edilmesi

Takip edilen adreste panel isteği **/auth/login** dizinine yönlendirmektedir.



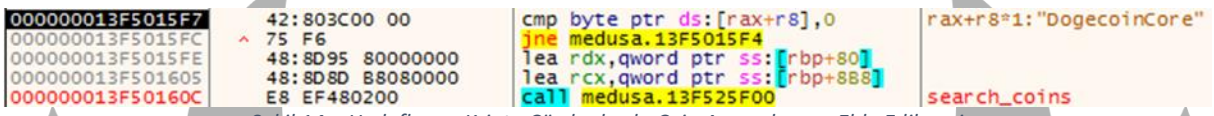
Şekil 12 – Zararlının İletişime Geçtiği Web Panel Adresinin Elde Edilmesi

Zararlı **EnumDisplayDevices** API ile geçerli oturumdaki görüntüleme aygıtları hakkında bilgi almaktadır.



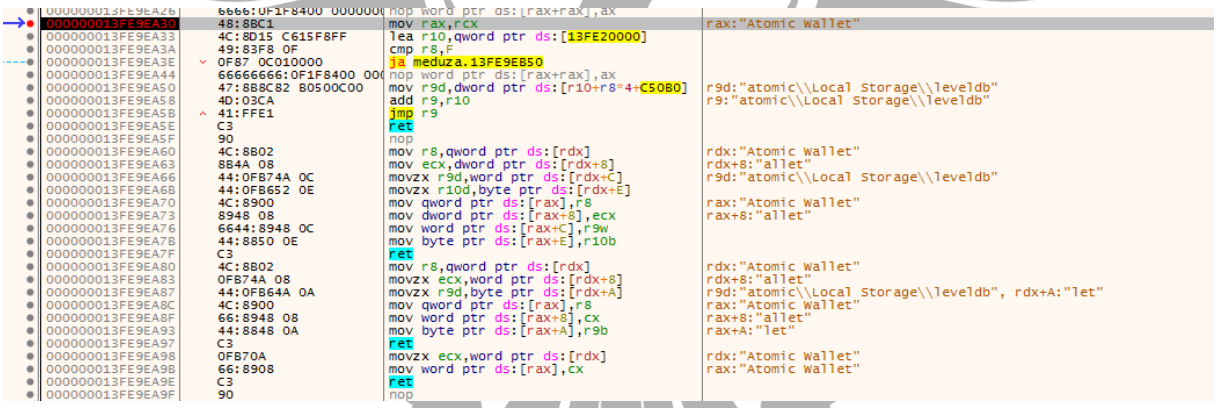
Şekil 13 – Görüntüleme Aygıtları Hakkında Bilgi Elde Edilmesi

Kripto varlıklarıyla ile ilgili zararlı ilk olarak sırasıyla tarayıcadaki eklenti ve cihazda donanımsal olarak bulunan hedef kripto cüzdanı belirlemektedir. İlgili hedef coin cüzdanda arandıktan sonra parametre olarak kripto para ismi, cüzdan ismi ve cüzdan ile ilgili dosyanın ismi verilmektedir.



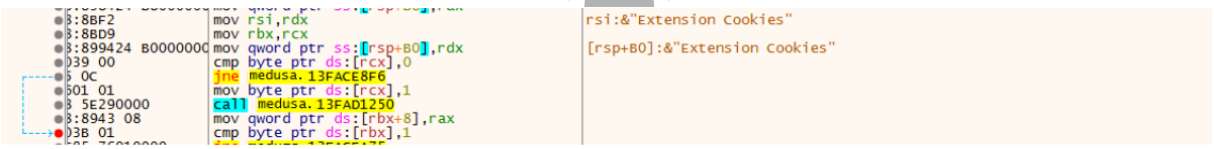
Şekil 14 – Hedeflenen Kripto Cüzdanlarda Coin Aramalarının Elde Edilmesi

CreateDirectoryA API ile crypto klasörünün içerisine coin ismiyle yeni bir klasör oluşturulur. **SHGetFolderPathA** API ile APPDATA klasörünün dizini alınmaktadır, **IstrcatA** ile sonuna cüzdan ismi dizin olarak eklenmektedir. Cüzdanın mutlak dizini elde edilmektedir. Cüzdan datalarının bulunduğu dizine gelmektedir. Kripto para ile ilgili veriler crypto klasörünün içine kopyalanmaktadır.



Şekil 15 – Zararlının Hedeflediği Kripto Cüzdanların Elde Edilmesi

Zararlı tarayıcıda bulunan tüm eklentilerin çerezlerini elde etmektedir.

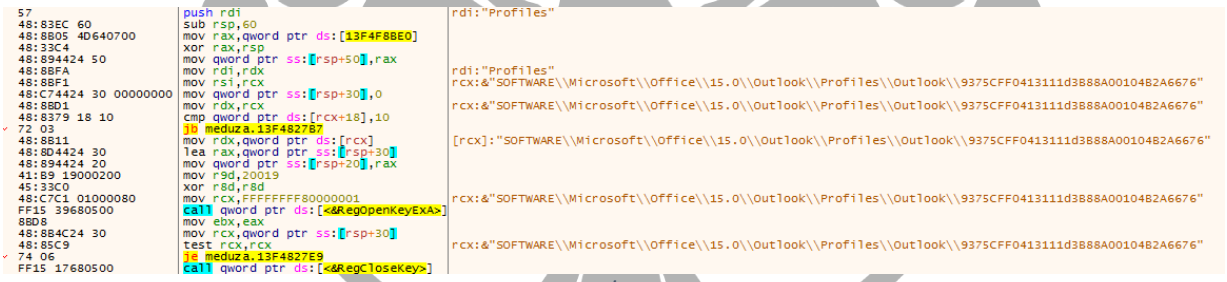


Şekil 16 – Tarayıcıda Bulunan Eklentilere Ait Çerezleri Elde Edilmesi

Buna ek olarak, zararlı Chrome tarayıcısında tutulan network çerezlerine erişmektedir.

Şekil 17 – Chrome'da Tutulan Network Çerezlerini Elde Edilmesi

Tarayıcı işlemleri tamamlandıktan sonra programın sıradaki hedefi Outlook verileridir. Bu aşamada zararlı, Windows Kayıt Defterindeki Outlook kayıt adreslerinde **RegOpenKeyExA** API ile **HKEY_CURENT_USER** için **KEY_READ** izni ile parametre olarak verilen registry dizinleri için handle almaya çalışmaktadır. ERROR_SUCCESS değeri return olursa **RegEnumValueA** API varsayılana ek olarak handle ve verilerin içine yazılacağı char array değişkeni verilerek çağrı yapılmaktadır. Bu çağrı while döngüsü içerisinde return değerinin değili olacak şekilde ayarlanmıştır. ERROR_SUCCESS değeri alındığı sürece çalışacaktır.

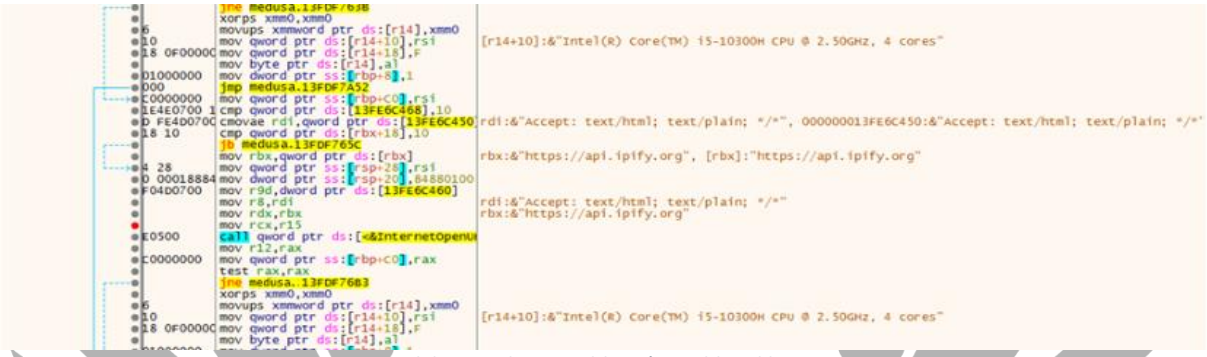


Şekil 18 – Zararlının Handleni Almak İstediği Kayıt Adresinin Elde Edilmesi

- SOFTWARE\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676
- SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676

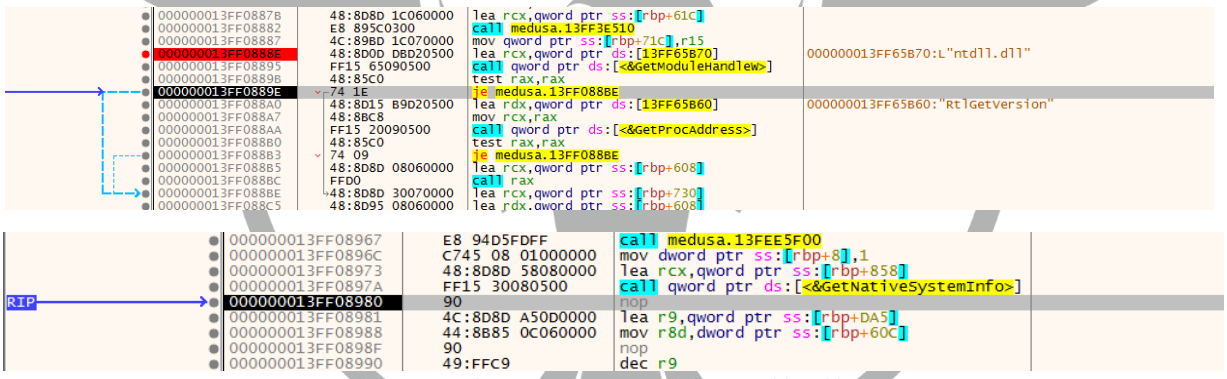
Şekil 19 – Zararlının Handleni Almak İstediği Kayıt Adresleri

Zararlı, kayıt adreslerini okuduktan sonra C2 sunucusu ile iletişime geçmektedir. Fakat bunun öncesinde **InternetOpenUrlA** API ile **api[.]ipify[.]org** adresine istek göndererek kurbanın public IP'sini döndürmektedir.



Şekil 20 – Cihazın Public IP'sini Elde Edilmesi

Zararlı, **RtlGetVersion** ve **GetNativeSystemInfo** API'lerini kullanarak yerel sistem ve sürüm bilgileri hakkındaki bilgileri alır.

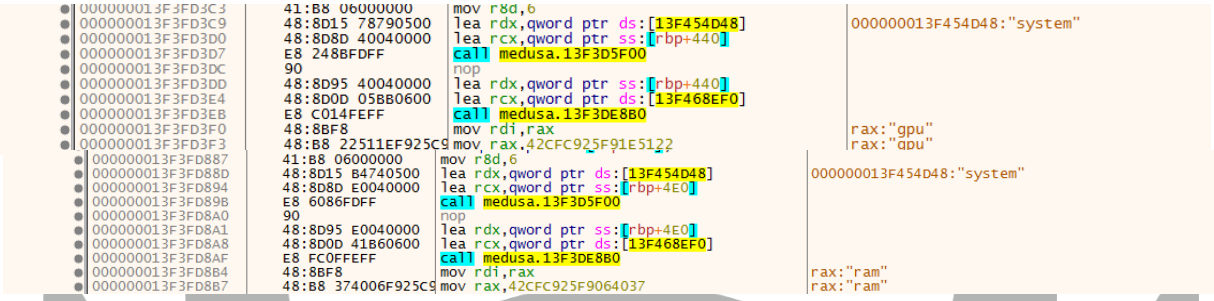


Şekil 21 – Yerel Sistem ve Sürüm Bilgilerinin Elde Edilmesi

Zararlı, **GetComputerName** API kullanarak kurbanın makinesinin ismini toplamaktadır.

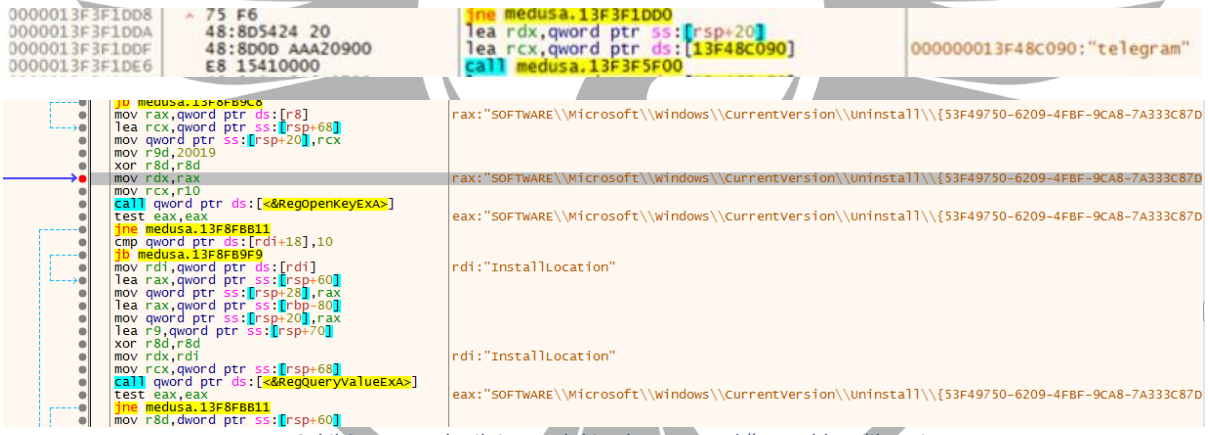
Şekil 22 – Kurban Cihazın İsminin Elde Edilmesi

Buna ek olarak, zararlının GPU, RAM ve Şekil-7'deki diğer sistem bilgilerini topladığı görülmektedir.



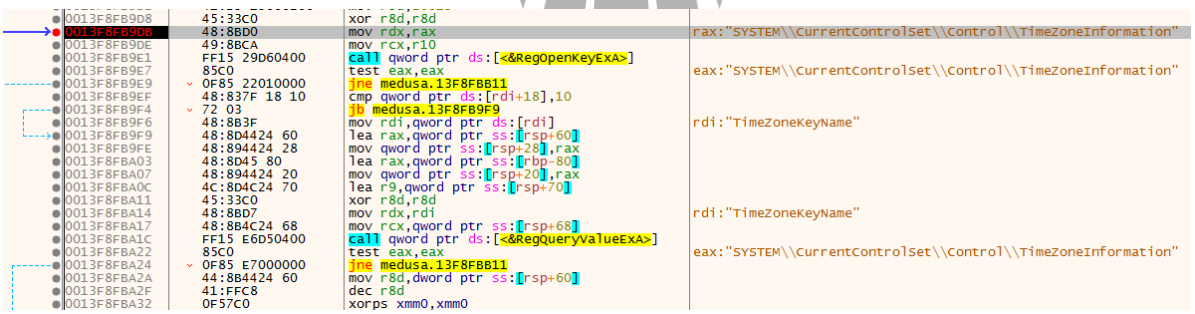
Şekil 23 – Zararlının Sistem Bilgilerinin Elde Edilmesi

Hedef bilgisayardaki Telegram uygulaması ve kayıt defteri anahtarını **InstallLocation** değeri aracılığıyla kontrol etmektedir.



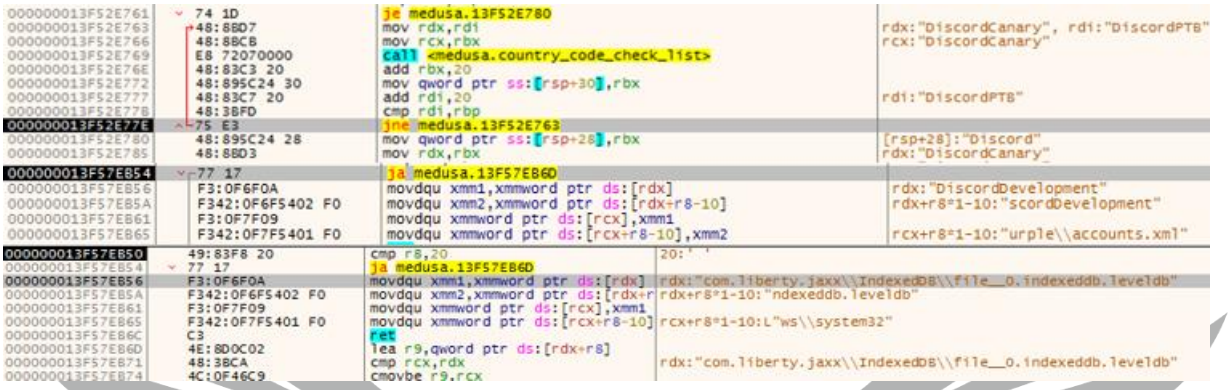
Şekil 24 – Zararlı Bilgisayardaki Telegram Varlığının Elde Edilmesi

Saat dilimi bilgileri, **SYSTEM\CurrentControlSet\Control\TimeZoneInformation** kayıt defteri anahtarına erişilerek ve **TimeZoneKeyName** API çağrılarak alınmaktadır.



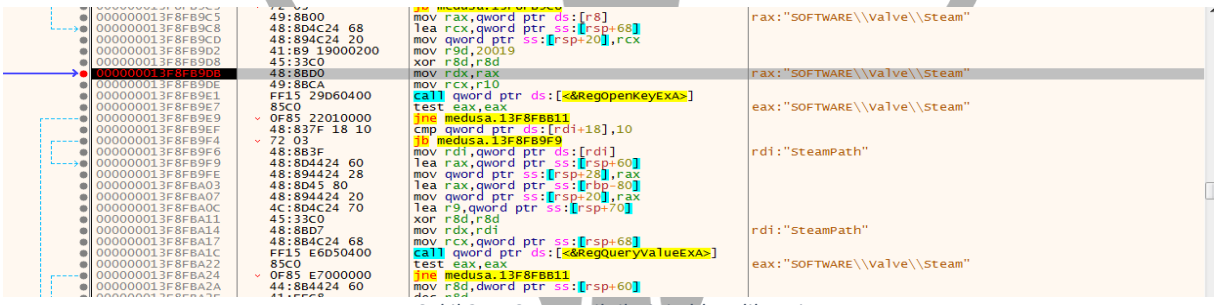
Şekil 25 – Zararlı Bilgisayardaki Saat Dilimi Bilgilerini Elde Edilmesi

Zararlı, Discord uygulamasına özel olarak çalışan bazı alt programlara ve discord kullanıcı hesaplarının tutulduğu **accounts.xml** dosyasına erişmeyi hedeflemektedir. Aynı zamanda, **liberty jaxx** cüzdanının masaüstü uygulamasına ait olan veritabanı dosyasına erişmek istemektedir.



Şekil 26 – Zararlının Erişmek İstediği Bazı Masaüstü Uygulamaların Elde Edilmesi

Zararlı, Steam istemci verilerini "**\SOFTWARE\Valve\Steam**" kayıt defteri anahtarını okuyarak almaktadır. Steam, Valve Corporation tarafından oluşturulan ve öncelikle video oyunları için kullanılan bir dijital dağıtım platformudur. Bu kayıt defteri anahtarı; kullanıcıya özel ayarları, oyun bilgilerini, oturum açma verilerini, oturum bilgilerini ve Steam istemcisiyle ilişkili diğer yapılandırma verilerini saklamaktadır.

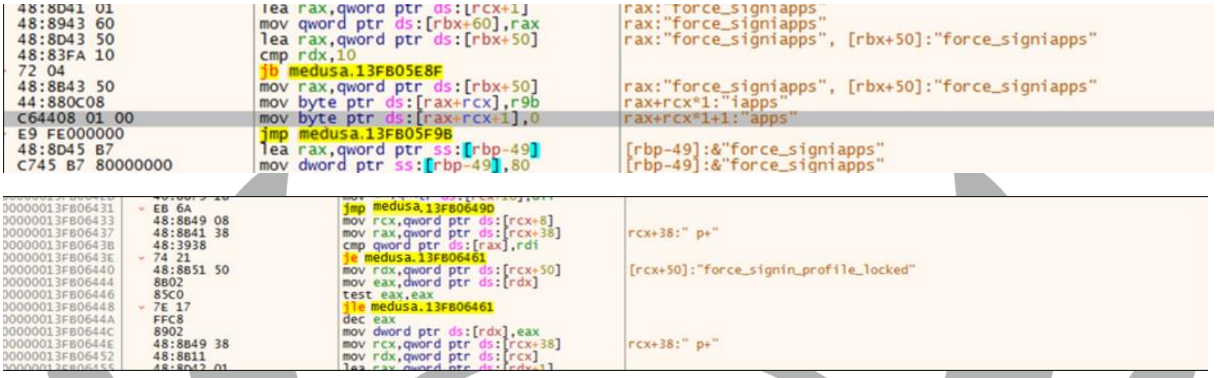


Şekil 27 – Steam Bilgilerini Elde Edilmesi

Devamında zararlı, Chrome tarayıcısındaki kullanıcıların profil fotoğraflarını toplamaktadır.

Şekil 28 – Zararlının Kullanıcı Profil Fotoğtaflarını Elde Etmesi

Zararlı, kilitlenmiş kullanıcı profillerinin bilgilerini elde etmeye çalışmaktadır.



Şekil 29 – Zararlının Kullancı Profillerini Elde Etmesi

Son olarak zararlı, **GetModuleFileNameA** API kullanılarak verilen yürütülebilir dosyanın konumunu almaktadır. Ardından **ShellExecuteA** API ile **komut istemcisini** açtıktan sonra Şekil 31'deki komutu çalıştırmaktadır.

Şekil 30 – Zararlının İşlemini Tamamladıktan Sonra Kendisini Silmesinin Elde Edilmesi

Aşağıdaki cmd scripti ile **Nul** komutu ekrana herhangi bir çıktı vermeden 1[.]1[.]1[.]1[.] IP adresine bir paket gönderir ve 3 saniye aralıklarla bir timeout oluşturmaktadır. 3 saniye sonra **Del** komutu çalışmaktadır. Komut çalıştıktan sonra zararlı kendisi silerek işlemlerine son vermektedir.

```
ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \"C:\\Users\\*\\Desktop\\medusa.exe"
```

Şekil 31 – Zararlının Kendisini Silerken Çalıştırdığı Komut

YARA Kuralı

```
rule Medusa {

        meta:

                description = "MedusaStealer"

        strings:

                $wallet1 = "\\Electrum\\wallets\\"

                $wallet2 = "\\atomic\\Local Storage\\leveldb\\"

                $wallet3 = "\\WalletWasabi\\Client\\Wallets\\"

                $wallet4 = "Coinomi\\Coinomi\\wallets"

                $wallet5 = "\\Exodus\\exodus.wallet\\"

                $wallet6 = "\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\"

                $wallet7 = "\\Metamask\\"

                $k1 = "SOFTWARE\\Microsoft\\Windows Messaging
Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676"

                $k2 = "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging
Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676"

                $x1 = "DiscordDevelopment\\accounts.xml"

                $x2 = "Ethereum\\keystore"

                $x3 = "User Data\\Extension Cookies"

                $x4 = "Web Data"

                $x5 = "Login Data"

                $x6 = "DiscordPTB"

                $x7 = "DiscordCanary"

                $ip = "79.137.203.224"
```

```
        $c1 = "Bitcoin"
        $c2 = "Ethereum"
        $c3 = "Armory"
        $c4 = "bytecoin"
        $c5 = "LiteCoin"
        $api1 = "EnumDisplayDevicesA"
        $api2 = "GdipCreateBitmapFromHBITMAP"
        $api3 = "GetUserDefaultLocaleName"
        $api4 = "CryptoMsgDllCNGExportKeyFree"
        $api5 = "GdipSaveImageToStream"
        $api6 = "InternetReadFile"
        $api7 = "WSAStartup"
        $api8 = "InternetOpenUrlA"
        $api9 = "HttpQueryInfoW"
        $api10 = "InternetQueryDataAvailable"
        $api11 = "IsDebuggerPresent"
    condition:
        all of them or
        4 of ($wallet*) and 3 of ($c*) or
        4 of ($wallet*) and 3 of ($api*) or
        2 of ($wallet*) and all of ($k*) and all of ($x*) and $ip
}
```

MITRE ATTACK TABLE

Collection	Execution	Discovery	Defense Evasion	Credential Access	C&C	Exfliration
Data from Local System (T1005)	**Windows Command Shell** (T1059.003)	**File and Directory Discovery** (T1083)	**Debugger Evasion** (T1622)	**Credentials from Web Browsers** (T1555.003)	**Standard Encoding** (T1132.001)	**Exfliration Over C2 Channel** (T1041)
		Query Registry (T1012)	**Deobfuscate/ Decode Filesor Information** (T1140)	**Steal Web Session Cookie** (T1539)		
		System Information Discovery (T1082)				

Çözüm Önerileri

1. Güncel bir antivirüs programı kullanılmalıdır.
2. Parolalar bilgisayar içerisinde açık metin şeklinde depolanmamalıdır.
3. Bilinmeyen uygulamalar kontrol edilmeden çalıştırılmamalıdır.
4. Kripto cüzdanlarında iki faktörlü kimlik doğrulaması kullanılmalıdır.
5. Soğuk cüzdan gibi daha güvenilir kripto para saklama yöntemleri tercih edilmelidir.
6. Bilinmeyen e-postaların ek dosyaları açılmamalıdır.
7. Güvenilir kaynaktan olmayan linklere tıklanmamalıdır.
8. Kullanılan uygulamalar güncel tutulmalıdır.

HAZIRLAYAN

Akif İnan Yiğit	LinkedIn
Halit Düzgün	LinkedIn
Mehmet Özen	LinkedIn
Ömer Faruk Berber	LinkedIn