

Meduza

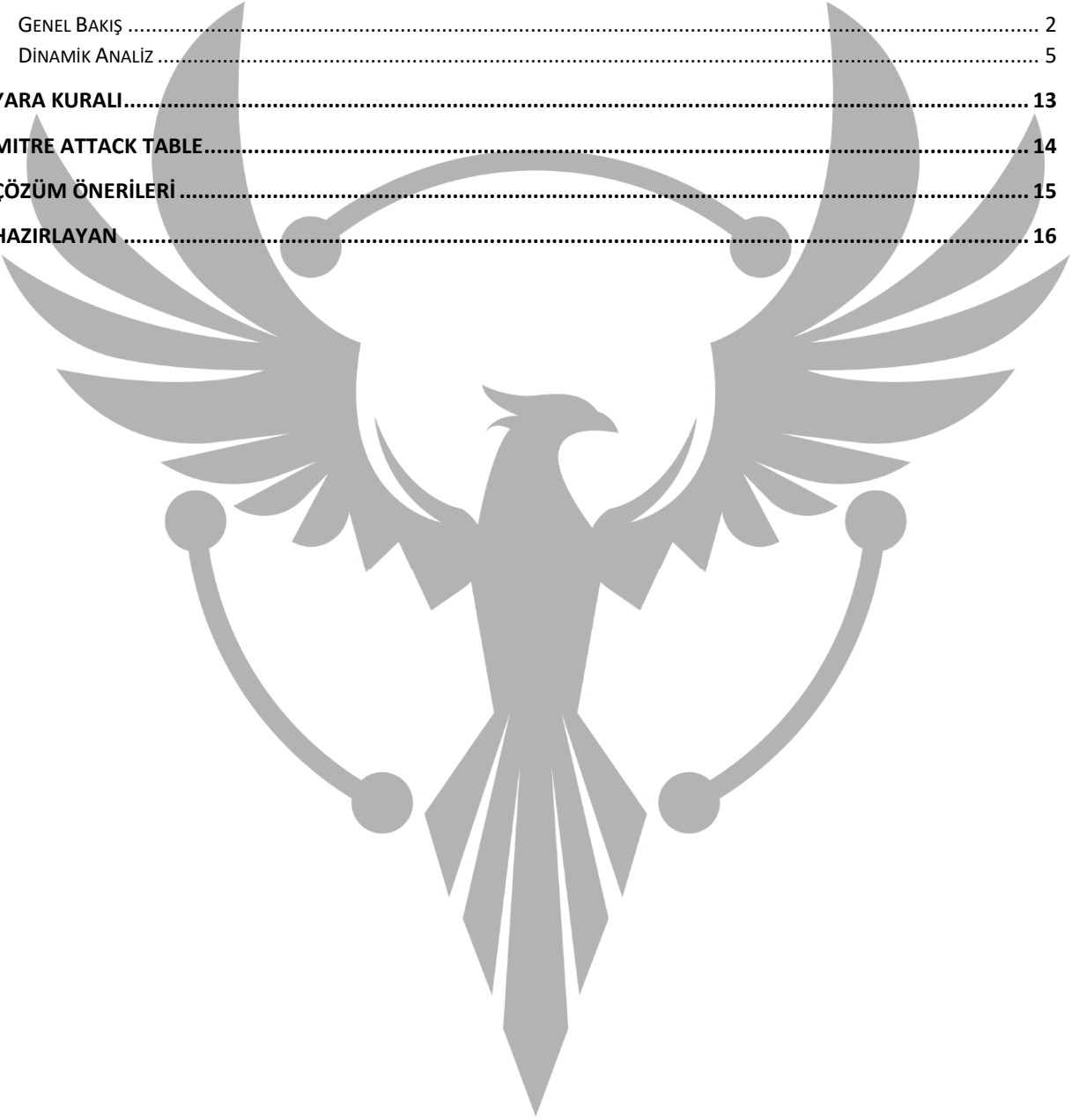
TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

ÖN BAKIŞ.....	1
MEDUZA.EXE ANALİZİ	2
GENEL BAKIŞ	2
DİNAMİK ANALİZ	5
YARA KURALI.....	13
MITRE ATTACK TABLE.....	14
ÇÖZÜM ÖNERİLERİ	15
HAZIRLAYAN	16



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,

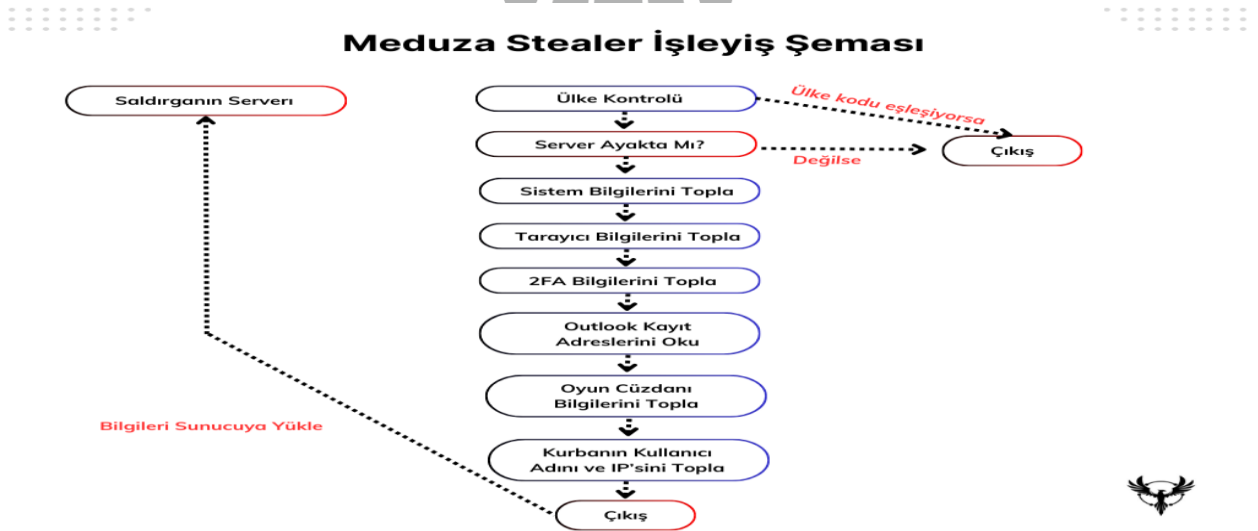
Erişim sağlamaktadır.

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. Zararlıının 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 – Zararlıının 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:

GAAuthenticator	Authenticator	SafePal	Guarda
EOS Authenticator	BrowserPass	KeePassXC	1Password
Trezor Password Manager	Dashlane	Bitwarden	LastPass
Keeper	Nordpass	RoboForm	Splicity
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 800L __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	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	rcx+40:L"1"
000000013FB3EC1C	C5FD7F59 40	vmovdqa yword ptr ds:[rcx+40],ymm3	rdx+80:L"MSC"
000000013FB3EC21	C5FD7F61 60	vmovdqa yword ptr ds:[rcx+60],ymm4	rdx+A0:L"CHITECTURE=AMD64"
000000013FB3EC26	C5FE6F8A 80000000	vmovdqu ymm1,yword ptr ds:[rdx+80]	rdx+E0:L"IFIER=Intel64 Family 6 Model 165 Stepping 2, GenuineIntel"
000000013FB3EC2E	C5FE6F92 A0000000	vmovdqu ymm2,yword ptr ds:[rdx+A0]	
000000013FB3EC36	C5FE6F9A C0000000	vmovdqu ymm3,yword ptr ds:[rdx+C0]	
000000013FB3EC3E	C5FE6FA2 E0000000	vmovdqu ymm4,yword ptr ds:[rdx+E0]	
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.

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	

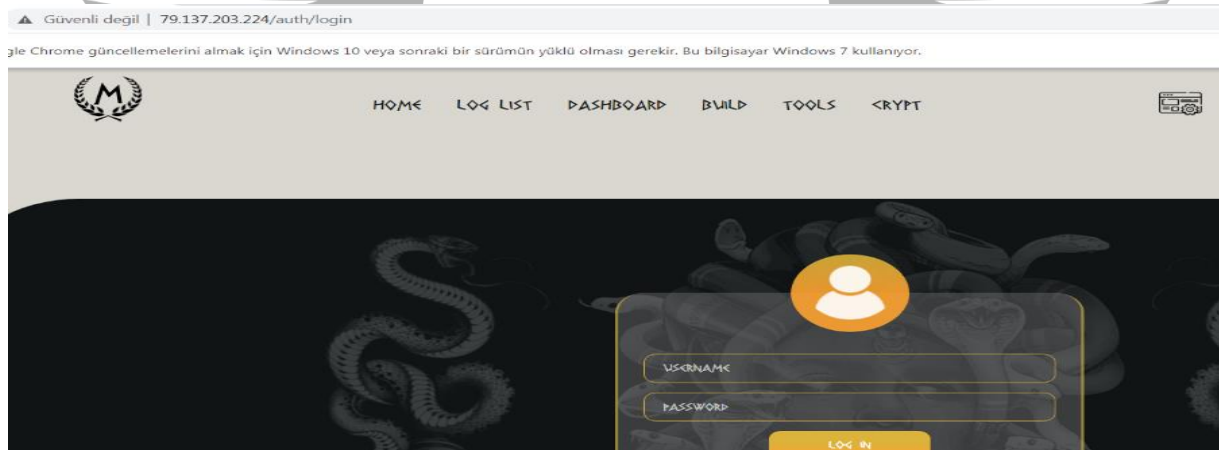
Şekil 10 – Ülke Kodlarına Bakılarak Hedef Ülke Kontrollerinin Elde Edilmesi

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

<pre> B9 02020000 mov ecx,202 E8:8D15 95250700 lea rdx,qword ptr ds:[13F108D48] FF15 C72D0500 call qword ptr ds:[<&WSAStartup>] E5C0 test eax,edx E8:85 95000000 jmp medusa.13F096856 E5:33C0 xor r8d,r8d E8:8D50 01 lea edx,qword ptr ds:[rax+1] E8:85C8 mov ebx,2 E8:85C8 call qword ptr ds:[<&sockets>] E8:8905 65250700 mov qword ptr ds:[13F108D40],rax E8:83F8 FF cmp rax,FFFFFFFFFFFFFFFF E4 6F jmp medusa.13F096856 E8:8D15 AD590700 mov word ptr ds:[13F108EE0],bx E8:833D BD590700 movzx ecx,word ptr ds:[13F10C1D0] E8:8905 E6260700 mov word ptr ds:[13F108EE2],ax E8:8D15 AD590700 lea rdx,qword ptr ds:[13F10C1B0] E8:833D BD590700 cmp qword ptr ds:[13F10C1F8],r10 E8:0F4315 9D590700 cmovae rdx,qword ptr ds:[13F10C1B0] E8:8D05 CA260700 lea r8,qword ptr ds:[13F108EE4] E8:85C8 mov ecx,ebx E8:85C8 call qword ptr ds:[<&inet_ptons>] E8:8D15 83260700 lea rdx,qword ptr ds:[rbx+1] E8:880D 0C250700 mov rcx,qword ptr ds:[13F108EE0] E8:85C8 call qword ptr ds:[<&connect>] E8:85C8 call qword ptr ds:[<&connect>] E8:85C8 jmp medusa.13F0968D3 E8:880D F6240700 mov rcx,qword ptr ds:[13F108D40] E8:85C8 call qword ptr ds:[<&close_socket>] E8:85C8 call qword ptr ds:[<&WSACleanup>] E8:85C8 jmp k1 k1 </pre>	<pre> 0000000013F10C1D0:"2-" 0000000013F108EE2:"2" 0000000013F10C1B0:"79.137.203.224" 0000000013F10C1B0:"79.137.203.224" </pre>
--	---

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.

<pre> 0000000013F09B305 66:897C24 34 mov word ptr ss:[rsp+34],di 0000000013F09B30A 33D2 xor edx,edx 0000000013F09B30C 41:B8 42030000 mov r8d,342 0000000013F09B312 E8:8D4C24 36 lea rcx,qword ptr ss:[rsp+36] 0000000013F09B317 E8:F4310300 call medusa.13F0CE510 0000000013F09B31C 44:8D4F 01 lea r9d,qword ptr ds:[rdi+1] 0000000013F09B320 4C:8D4424 30 lea r8,qword ptr ss:[rsp+30] 0000000013F09B325 33D2 xor edx,edx 0000000013F09B327 33C9 xor ecx,ecx 0000000013F09B329 FF15 C9E10400 call qword ptr ds:[<&EnumDisplayDevicesw>] 0000000013F09B32F 85C0 test eax,edx 0000000013F09B331 74 0F jmp medusa.13F09B342 0000000013F09B333 48:8D5424 74 lea rdx,qword ptr ss:[rsp+74] 0000000013F09B338 E8:88CB call medusa.13F088220 0000000013F09B33B E8:E0CEFEFF jmp medusa.13F09B357 0000000013F09B340 EB 15 </pre>	<pre> edx:L"VMware SVGA 3D" edx:L"VMware SVGA 3D" </pre>
--	--

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 80800000	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.

000000013FE9A30	48:8B11	mov rax,rcx	rax:"Atomic Wallet"
000000013FE9A33	4C:8D15 C615F8FF	lea r10,qword ptr ds:[13FE20000]	
000000013FE9A3A	49:83F8 0F	cmp r8,r8	
000000013FE9A3E	0F87 0C010000	ja medusa.13FE9E850	
000000013FE9A44	66666666:0F1F8400 00000000	nop word ptr ds:[rax+rax],ax	
000000013FE9A50	47:88C82 B0500C00	mov r9d,dword 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:8B02	mov r8,qword ptr ds:[rdx]	rdx:"Atomic Wallet"
000000013FE9A63	884A 08	mov ecx,dword 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:8B02	mov r8,qword ptr ds:[rdx]	rdx:"Atomic Wallet"
000000013FE9A83	0FB74A 08	movzx r9d,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 – Zararlının 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"
B39 00	cmp byte ptr ds:[rcx],0	
0C	jne medusa.13FACE8F6	
801 01	mov byte ptr ds:[rcx],1	
5E290000	call medusa.13FAD1250	
8:8943 08	mov qword ptr ds:[rbx+8],rax	
B3B 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.

```
0013F531601  E8 5AD30400      call medusa.13F57EA30
0013F531606  48 8B5424 20      mov rdx,qword ptr ss:[rsp+20]
0013F53160B  40 8BC6           mov r8,r14
0013F53160E  49 8BC6           mov rcx,r12
0013F5316E1  E8 4AD30400      call medusa.13F57EA30
0013F5316E6  33C0            xor eax,edx
0013F5316E8  6641 8907        mov word ptr ds:[r15],ax
0013F5316EC  48 893E          mov qword ptr ds:[r15],rdi
0013F5316F2  4C 8B6424 38      mov r12,qword ptr ss:[rsp+38]
0013F5316F7  48 8B7C24 40      mov rdi,qword ptr ss:[rsp+40]
0013F5316FC  48 8BAC24 80000000 mov rbp,qword ptr ss:[rsp+80]
0013F531704  4C 8B7424 30      mov r14,qword ptr ss:[rsp+30]
0013F531709  48 83C4 48        add rsp,48
0013F53170D  41 5F           pop r15
0013F53170F  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 varsayımla 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.

```
57      push rdi
48:83EC 60      sub rsp,60
48:8B05 40640700 mov rax,qword ptr ds:[13F4F68E0]
48:33C4      xor rax,rsp
48:894424 50      mov qword ptr ss:[rsp+50],rax
48:8BFA      mov rdi,rdx
48:8BF1      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      jb 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:B9 19000200 mov r9d,20019
45:33C0      xor r8d,r8d
48:C7C1 01000080 mov rcx,FFFFFFFF80000001
FF15 39680500 call qword ptr ds:[<4RegOpenKeyExA>]
8B08      mov ebx,eax
48:8B4C24 30      mov rcx,qword ptr ss:[rsp+30]
48:85C9      test rcx,rcx
74 06      je medusa.13F4827E9
FF15 17680500 call qword ptr ds:[<4RegCloseKey>]
```

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.

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 İsmi Elde Edilmesi

<pre> 000000013F3D3C3 000000013F3D3C9 000000013F3D3D0 000000013F3D3D7 000000013F3D3DC 000000013F3D3DD 000000013F3D3E4 000000013F3D3EB 000000013F3D3F0 000000013F3D3F3 000000013F3D887 000000013F3D88D 000000013F3D894 000000013F3D898 000000013F3D8A0 000000013F3D8A1 000000013F3D8A8 000000013F3D8AF 000000013F3D8B4 000000013F3D8B7 </pre>	<pre> 41:B8 06000000 mov r8d,6 48:8D15 78790500 lea rdx,qword ptr ds:[13F454D48] 48:8D8D 40040000 lea rcx,qword ptr ss:[rbp+440] E8 248BFDF5 call medusa.13F3D5F00 90 nop 48:8D95 40040000 lea rdx,qword ptr ss:[rbp+440] 48:8DD0 058B0600 lea rcx,qword ptr ds:[13F468EF0] E8 C014FEFF call medusa.13F3DE8B0 48:8BF8 mov rdi,rax 48:B8 2251EF925C9 mov rax,42CFC925F91E5122 41:B8 06000000 mov r8d,6 48:8D15 B4740500 lea rdx,qword ptr ds:[13F454D48] 48:8D8D E0040000 lea rcx,qword ptr ss:[rbp+4E0] E8 6086DFDF call medusa.13F3D5F00 90 nop 48:8D95 E0040000 lea rdx,qword ptr ss:[rbp+4E0] 48:8DD0 41B60600 lea rcx,qword ptr ds:[13F468EF0] E8 FC0FFEFF call medusa.13F3DE8B0 48:8BF8 mov rdi,rax 48:B8 37406F925C9 mov rax,42CFC925F9064037 </pre>	<pre> 000000013F454D48:"system" rax:"gpu" rax:"gpu" 000000013F454D48:"system" rax:"ram" rax:"ram" </pre>
--	--	---

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

0000013F3F1DD8 0000013F3F1DDA 0000013F3F1DDF 0000013F3F1DE6	* 75 F6 48:80542A 20 48:8D0D A2A20900 E8 15410000	<pre> jne medusa.13F3F1DD0 lea rcx,qword ptr ss:[rsp+20] lea rcx,qword ptr ss:[13F48C090] call medusa.13F3F5F00 </pre>	000000013F48C090:"telegram"
<pre> jnb medusa.13F8FB9B6 mov rax,qword ptr ds:[r8] lea rcx,qword ptr ss:[rsp+68] mov qword ptr ss:[rsp+20],rcx mov r9d,20019 xor r8d,r8d mov rdx,rax mov rcx,r10 call qword ptr ds:[<RegOpenKeyEx>] test eax,eax jne medusa.13F8FB9B11 cmp qword ptr ds:[rdi+18],10 jnb medusa.13F8FB9F99 mov rdi,qword ptr ds:[rdi] lea rax,qword ptr ss:[rsp+60] mov qword ptr ss:[rsp+20],rax lea rax,qword ptr ss:[rbp-80] mov qword ptr ss:[rsp+20],rax lea r9,qword ptr ss:[rsp+70] xor r8d,r8d mov rdx,rdi mov rcx,qword ptr ss:[rsp+68] call qword ptr ds:[<RegQueryValueEx>] test eax,eax jne medusa.13F8FB9B11 mov r8d,qword ptr ss:[rsp+60] </pre>	<pre> rax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D...} rax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D...} eax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D...} rdi:"InstallLocation" rdi:"InstallLocation" eax:"SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750-6209-4FBF-9CA8-7A333C87D...} </pre>		

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

0013F8FB9D8	45:33C0	xor r8d,r8d	
0013F8FB9D8	48:8800	mov rdx,rax	rax:"SYSTEM\\CurrentControlSet\\Control\\TimeZoneInformation"
0013F8FB9E1	49:98CA	mov rcx,r10	
0013F8FB9E1	4F15 29060400	call qword ptr ds:[<RegopenKeyEXA>]	
0013F8FB9E7	85C0	test eax,eax	eax:"SYSTEM\\CurrentControlSet\\Control\\TimeZoneInformation"
0013F8FB9E9	✓ 0F85 22010000	jne medusa.13F8FB811	
0013F8FB9EF	48:837F 18 10	cmp qword ptr ds:[rdi+18],10	
0013F8FB9F4	✓ 72 03	jb medusa.13F8FB9F9	rdi:"TimeZoneKeyName"
0013F8FB9F4	48:833F	mov rdi,qword ptr ds:[rdi]	
0013F8FB9F9	48:8D4424 60	lea rax,qword ptr ss:[rsp+60]	
0013F8FB9FE	48:894424 28	mov qword ptr ss:[rsp+28],rax	
0013F8FBA03	48:8D45 80	lea rax,qword ptr ss:[rbp-80]	
0013F8FBA07	48:894424 20	mov qword ptr ss:[rsp+20],rax	
0013F8FBA0C	4C:8D4C24 70	lea r9,qword ptr ss:[rsp+70]	
0013F8FBA11	45:33C0	xor r8d,r8d	
0013F8FBA14	48:8807	mov rdx,rdi	rdi:"TimeZoneKeyName"
0013F8FBA17	48:884C24 68	mov rcx,qword ptr ss:[rsp+68]	
0013F8FBA1C	4F15 6E050400	call qword ptr ds:[<RegQueryValueEXA>]	
0013F8FBA22	85C0	test eax,eax	eax:"SYSTEM\\CurrentControlSet\\Control\\TimeZoneInformation"
0013F8FBA24	✓ 0F85 E7000000	jne medusa.13F8FB811	
0013F8FBA2A	44:884424 60	mov r8d,qword ptr ss:[rsp+60]	
0013F8FBA2F	41:FFC8	dec r8d	
0013F8FBA37	0E57C0	xorps xmm0,xmm0	

10/

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	48:8807	mov rdx,rdi	rdx:"DiscordCanary", rdi:"DiscordPTB"
000000013F52E766	48:88C8	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"
000000013F52E778	48:38FD	cmp rdi,rbp	
000000013F52E77E	75 E3	jne medusa.13F52E763	
000000013F52E780	48:895C24 28	mov qword ptr ss:[rsp+28],rbx	[rsp+28]: "Discord"
000000013F52E785	48:88D3	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:"ndexeddb.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:"ws\\system32"
000000013F57E86C	C3	ret	
000000013F57E86D	4E:8D0C02	lea r9,qword ptr ds:[rdx+r8]	
000000013F57E871	48:38CA	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	49:8800	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	
000000013F8FB9DE	48:88D0	mov rdx,rcx	rax:"SOFTWARE\\Valve\\Steam"
000000013F8FB9E1	49:88CA	mov rcx,r10	
000000013F8FB9E1	FF15 29060400	call qword ptr ds:[<&RegOpenKeyExA>]	
000000013F8FB9E7	85C0	test eax,eax	eax:"SOFTWARE\\Valve\\Steam"
000000013F8FB9E9	✓ 0F85 22010000	jnz medusa.13F8FB9B1	
000000013F8FB9EF	48:837F 18 10	cmp qword ptr ds:[rdi+18],10	
000000013F8FB9F4	✓ 72 03	jb medusa.13F8FB9F9	rdi:"SteamPath"
000000013F8FB9F6	48:883F	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	48:88D7	mov rdx,rdi	
000000013F8FBA17	48:884C24 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	
000000013F8FBA24	✓ 0F85 E7000000	jnz medusa.13F8FB9B1	
000000013F8FBA2A	44:8B4424 60	mov r8q,dword ptr ss:[rsp+60]	
000000013F8FBA2E	44:8B4424 60	mov r8q,dword ptr ss:[rsp+60]	

Şekil 27 – Steam Bilgilerini Elde Edilmesi

Devamında zararlı, Chrome tarayıcısındaki kullanıcıların profil fotoğraflarını toplamaktadır.

0013FB06437	48:8841 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	48:8851 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	48:8849 38	mov rcx,qword ptr ds:[rcx+38]	rcx+38:" p+"
0013FB06452	48:8B11	mov rdx,qword ptr ds:[rcx]	
0013FB06455	48:8D47 01	lea rax,qword ptr ds:[rdx+1]	

Şekil 28 – Zararlının Kullanıcı Profil Fotoğraflarını Elde Etmesi

48:8D41 01 48:8943 60 48:8D43 50 48:83FA 10 72 04 48:8843 50 44:880C08 C64408 01 00 E9 FE000000 48:8D45 B7 C745 B7 80000000	lea eax,qword ptr ds:[rcx+1] mov qword ptr ds:[rbx+60],rax rax,qword ptr ds:[rbx+50] cmp rdx,10 jb medusa.13FB05E8F mov rax,qword ptr ds:[rbx+50] mov byte ptr ds:[rax+rcx],r9b mov byte ptr ds:[rax+rcx+1],0 jmp medusa.13FB05F9B lea rax,qword ptr ss:[rbp-49] mov dword ptr ss:[rbp-49],80	rax:force_signiapps rax:"force_signiapps" rax:"force_signiapps", [rbx+50]:"force_signiapps" rax:"force_signiapps", [rbx+50]:"force_signiapps" rax+rcx*1:"iapps" rax+rcx*1+1:"apps" [rbp-49]:&"force_signiapps" [rbp-49]:&"force_signiapps"
00000013FB06431 EB 6A 48:8849 08 00000013FB06437 48:8841 38 48:3938 74 21 00000013FB0643E 48:8851 50 00000013FB06444 8802 00000013FB06446 85C0 00000013FB06448 7E 17 00000013FB0644A FFC8 00000013FB0644C 8902 00000013FB0644E 48:8849 38 48:8811 48:8811 01	jmp medusa.13FB06490 mov rcx,qword ptr ds:[rcx+8] mov rax,qword ptr ds:[rcx+38] cmp qword ptr ds:[rax],rdi je medusa.13FB06461 mov rax,qword ptr ds:[rcx+50] mov eax,dword ptr ds:[rax] test eax,eax jne medusa.13FB06461 dec eax mov dword ptr ds:[rdx],eax mov rcx,qword ptr ds:[rcx+38] mov rdx,qword ptr ds:[rcx] lea rcx,qword ptr ds:[rcx+1]	rcx+38:" p+ " [rcx+50]:"force_signin_profile_locked" rcx+38:" p+ "

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

<pre> word ptr ss:[rbx+8] eax,qword ptr ss:[rbx] word ptr ss:[rbx+6] eax,xmmword ptr ss:[rbp+20] xmm0,xmmword ptr ss:[rbp+0] qword ptr ss:[rbp+10] word ptr ss:[rbp+2],edi qword ptr ss:[rbp+18],rdi cs,qword ptr ss:[rbp+20] ecx,ecx qword ptr ds:[&shellExecuteA] word ptr ss:[rbp+8],FFFFFFFF cs,qword ptr ss:[rbp+0] rdx:"open" RAX.13F739E34 dx cs,qword ptr ss:[rbp+0] rdx:"C:\Windows\medusa.exe" dx,1000 rdx:"open" RAX.13F739E2F dx,17 cs,qword ptr ds:[rcx-8] rdx:"open" dx,1C eax,FFFFFFFFFFFFFFFF RAX.13F739E73 medusa.13F77C86E xmm0,xmmword ptr ds:[13B7A7460] </pre>	<pre> RBX BEA6A25865589E80 RCX 0000000000000000 RDX 0000000000017E6C0 RBP 0000000000017E640 RSP 0000000000017E660 RSI D334266930864E43 RDI 00000000000000000 R8 0000000000017E680 R9 0000000000017E690 R10 0000000000017F70000 R11 00000000FFFFF0000 R12 00000000000000000 R13 00000000000000000 R14 000000000001D7120 R15 00000000000000000 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) </pre>
---	--

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.

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	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](#)

