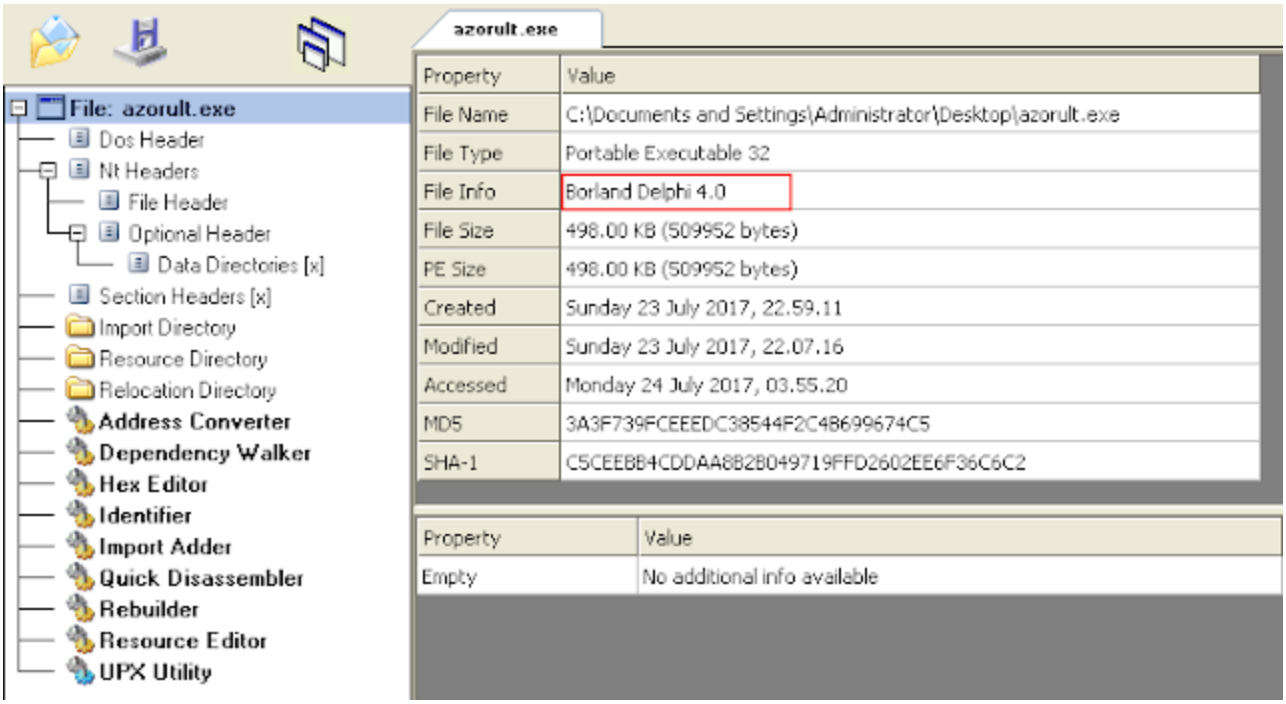
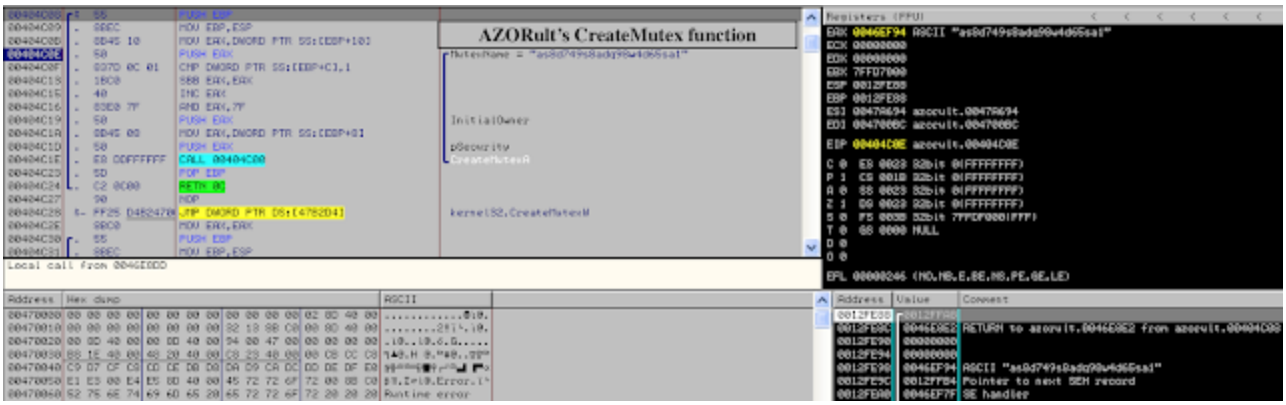
Let's Learn: Reversing Credential and Payment Card Information Stealer 'AZORult V2'

vkremez.com/2017/07/lets-learn-reversing-credential-and.html

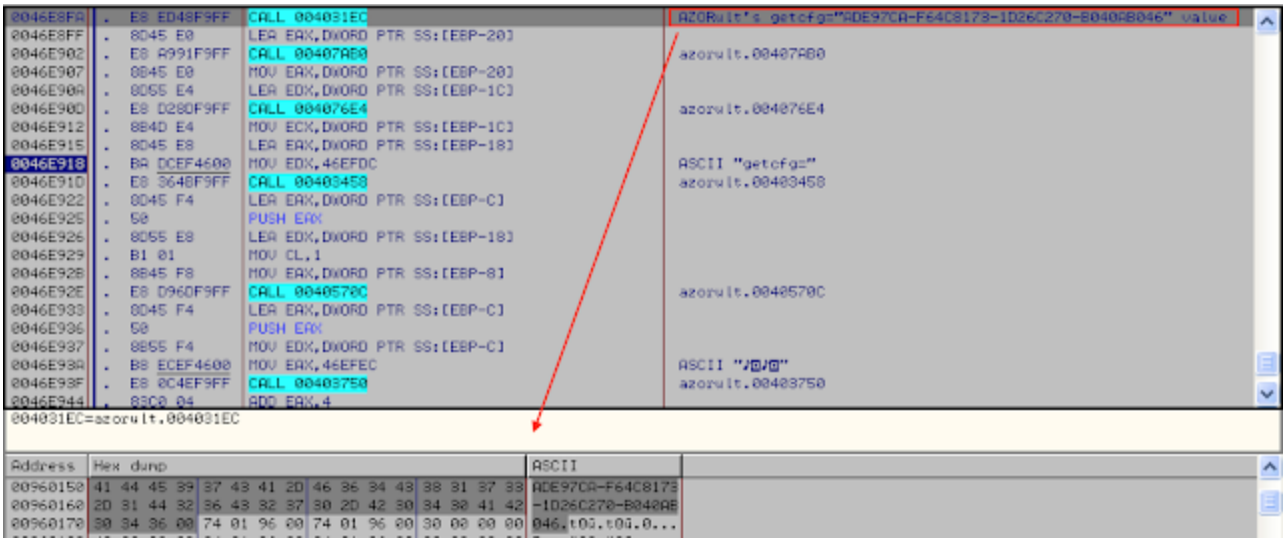
Goal: Reverse the second version of the popular credential and payment card information stealer “AZORult"
Original find: @DynamicAnalysis
Source: AU2_EXEsd.exe
Tool: OllyDBG, CFF Explorer



Brief overview: AZORult Version 2 Stealer, written in Borland Delphi collects informations, sends a report to the C2 server, then self-deletes. AZORult steals cookies, saved passwords, and saved credit card information from browsers. It also steals XMPP and Bitcoin wallet information Additionally, the malware is able to grab files from Desktop with specified extensions. It supports .bit domain communication.
Command-and-Control (C2) Server: parking-services[.]us/gate[.]php
Mutex: as8d749s8adq98w4d65sa1

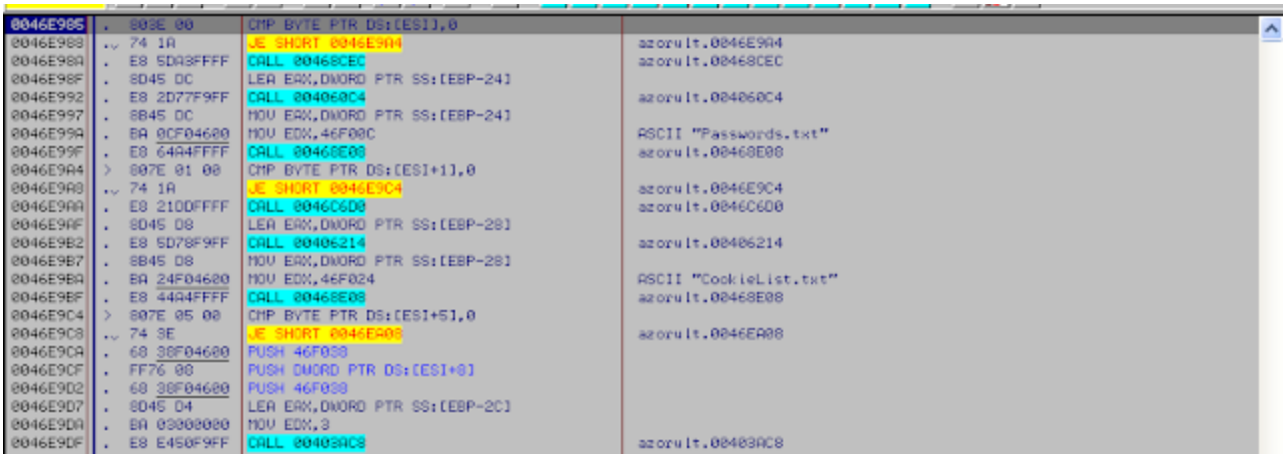


AZORult's getcfg=ADE97CA-F64C8173-1D26C270-B040AB046 value

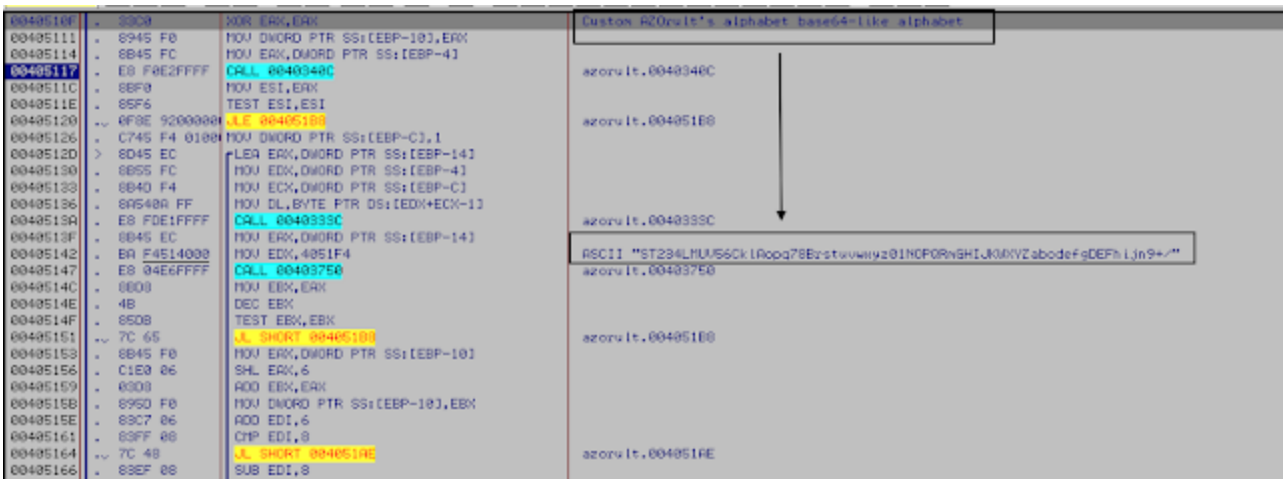


It encodes streams and separates the report information as follows:

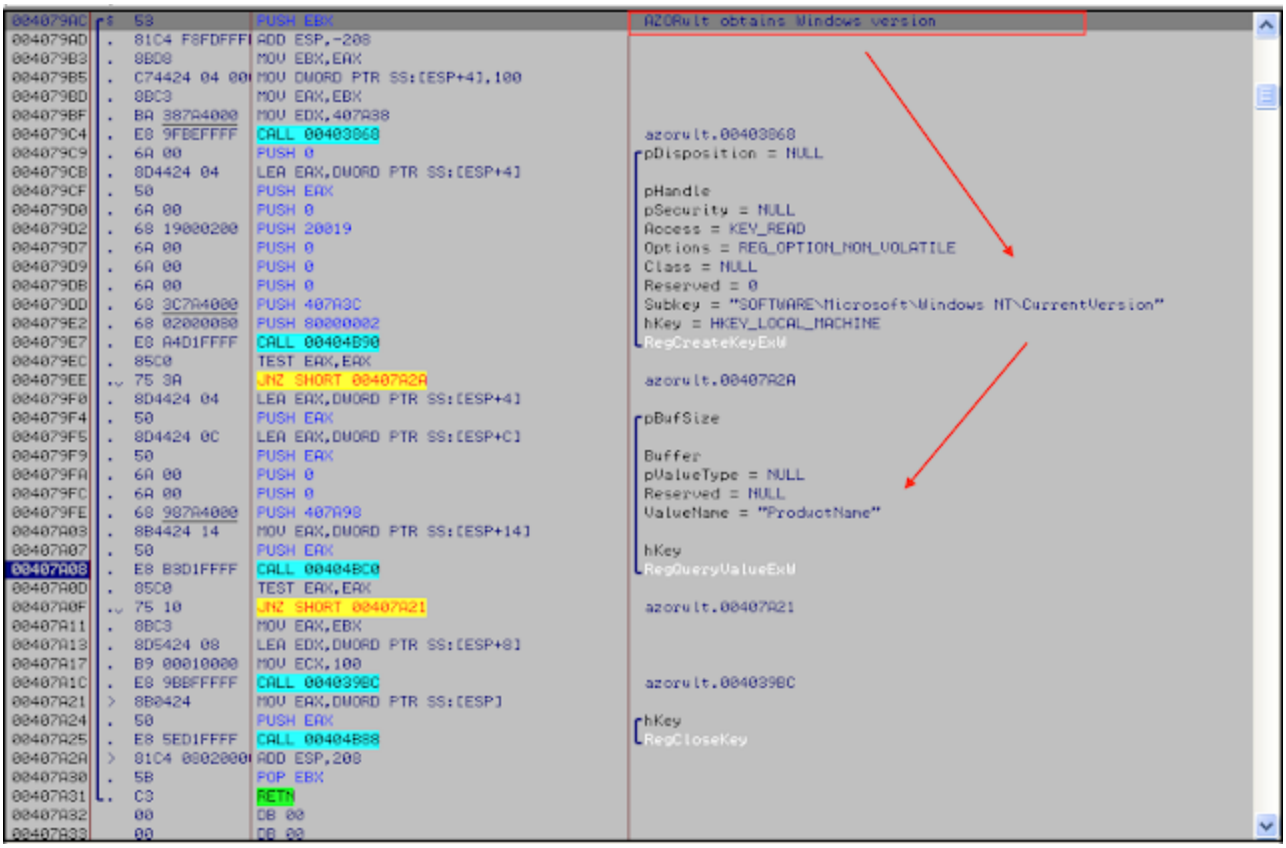
- Browsers\AutoComplete\<browser>_CC.txt
- Browsers\AutoComplete\<browser>__.default
- Browsers\Cookies\<browser>__.default.txt
- IP.txt
- Passwords.txt
- CookieList.txt
- SYSInfo.txt



AZORult's custom base64-like alphabet:



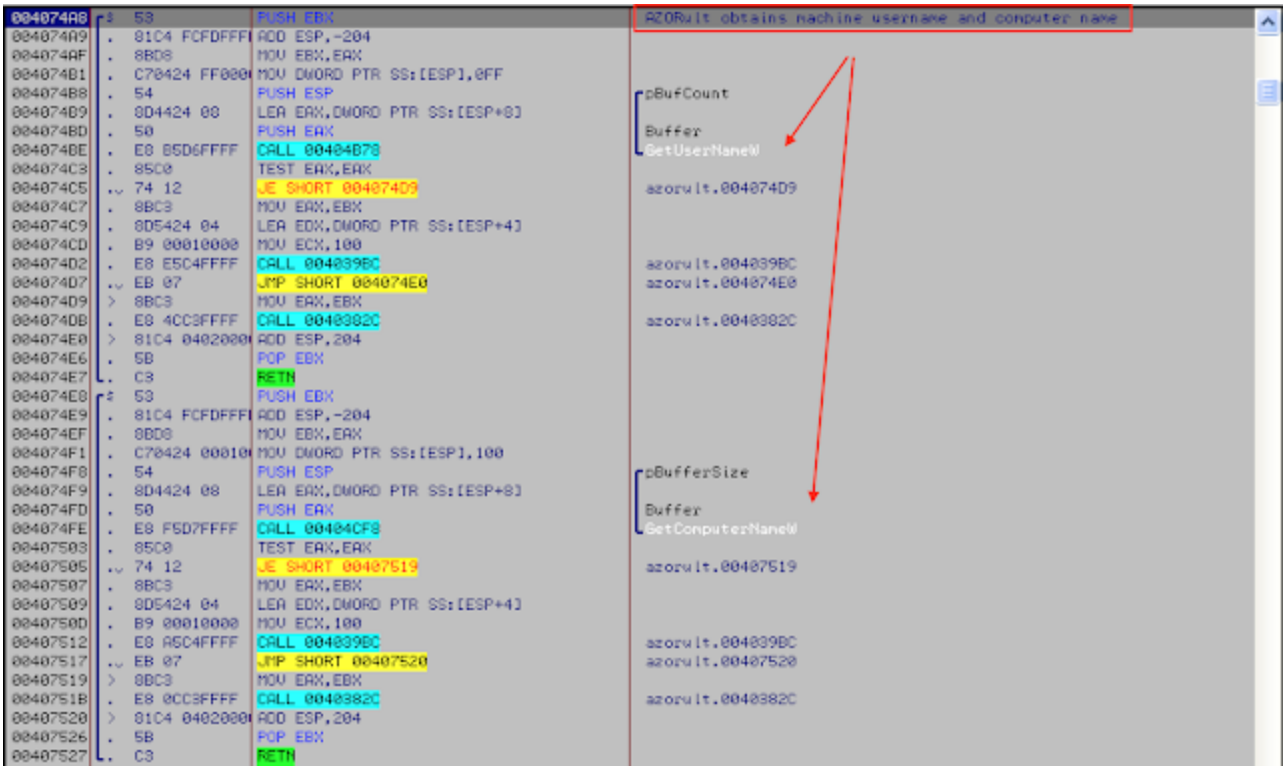
Obtains Windows version via ProductName Registry value:



The harvested SYSINFO victim information is in the following format:

- BIN:
- MachineID : -> SOFTWARE\Microsoft\Cryptography\MachineGuid
- EXE_PATH : <GetModuleFilename API >
- DLL_PATH : <GetModuleFilename API>
- Windows : - > SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName
- Comp(User) :
- CPU Model: -> HARDWARE\DESCRIPTION\System\CentralProcessor\0\ ProcessorNameString
- [System Process]
- [Programms]

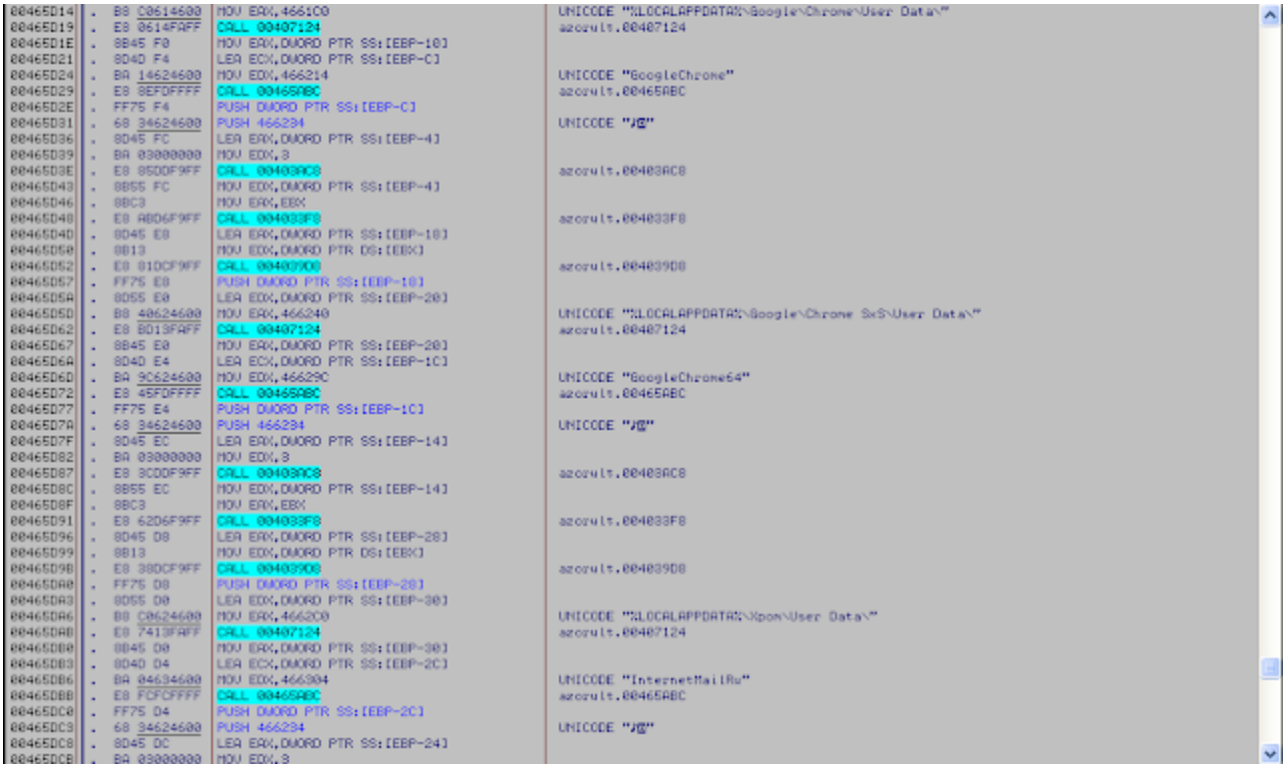
AZORult obtains the user and computer information via usual GetUserName and GetComputerName APIs.



The stealer targets the following applications for credential harvesting:

- Google Chrome (including x64)
- YandexBrowser
- Opera
- Firefox
- Orbitum
- Chromium

- Amigo
- Outlook
- FileZilla
- WinSCP
- Thunderbird
- 360Browser
- Vivaldi
- Bromium
- InternetMailRu
- Bromium
- Nichrome
- RockMelt
- Skype
- Steam



The stealer collects XMPP/Jabber credentials from the following apps:

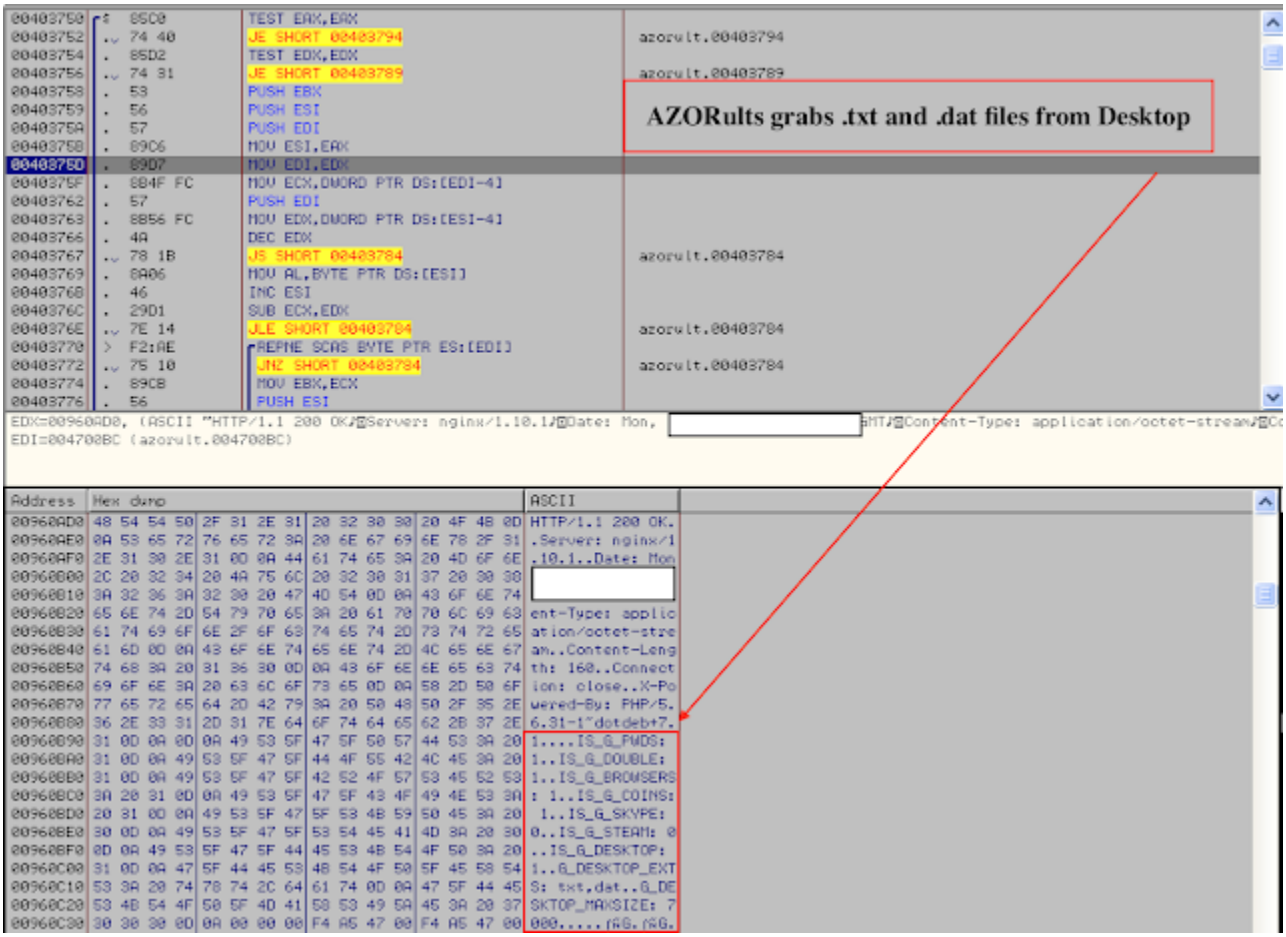
- PsiPlus
- Psi
- Pidgin

Moreover, AZOrult aslo appear to collet the following cryptocurrency files:

- wallet.dat
- \wallet.dat
- electrum.dat
- \electrum.dat

- .wallet
- \.wallet
- %APPDATA%\MultiBitHD
- mbhd.wallet.aes
- \MultiBitHD\
- \mbhd.wallet.aes
- \mbhd.checkpoints
- mbhd.checkpoints
- \mbhd.spvchain
- mbhd.spvchain
- \mbhd.yaml
- mbhd.yaml
- wallet_path
- Software\monero-project\monero-core
- \Monero\

Desktop file grabber of files with .txt & .dat extensions.



For example, here is AZORult's cookie/credit card grabber from Mozilla Firefox's Sqlite tables:

- SELECT host, path, isSecure, expiry, name, value FROM moz_cookies

- SELECT host_key, name, encrypted_value, value, path, secure, expires_utc FROM cookies
- SELECT host_key, name, name, value, path, secure, expires_utc FROM cookies
- SELECT fieldname, value FROM moz_formhistory
- SELECT name, value FROM autofill
- SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted value FROM credit_cards

Self-delete function: