

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

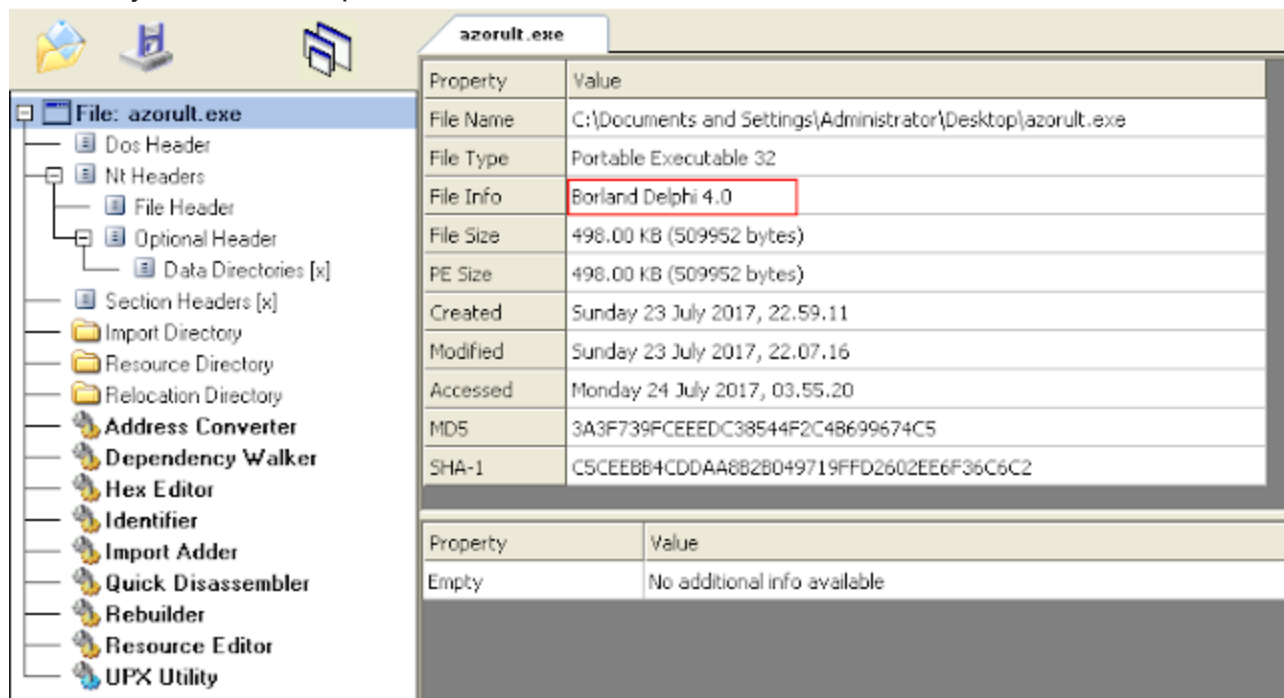
vkremez.com/2017/07/lets-learn-reversing-credential-and.html

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

Address	Hex dump	ASCII	Registers (FPU)
00404000	55	PUSH EBP	EAX: 0040E794 ASCII "as0d749sdad90u4065ca1"
00404001	56	MOV EBP, ESP	EAX: 00000000
00404002	58 10	MOV EAX, DWORD PTR SS:[EBP+10]	EAX: 00000000
00404003	59	PUSH EBX	EAX: 00000000
00404004	5B 01	MOV EBX, PTR SS:[EBP+1]	EAX: 00000000
00404005	5C	MOV EAX, EBX	EAX: 77F07060
00404006	5D	MOV EAX, 7F	ESP: 0012F200
00404007	5E	PUSH ESI	ESP: 0012F180
00404008	5F 00	MOV EAX, DWORD PTR SS:[EBP+0]	EAX: 00470000 azorult.00470000
00404009	5A	PUSH EAX	EIP: 0040400E azorult.0040400E
0040400A	58 00	MOV EAX, PTR SS:[EBP+0]	EAX: 00000000
0040400B	59	POP EBP	EAX: 00000000
0040400C	58	MOV EAX, ESP	EAX: 00000000
0040400D	58	MOV EAX, ESP	EAX: 00000000
0040400E	58	MOV EAX, ESP	EAX: 00000000
0040400F	58	MOV EAX, ESP	EAX: 00000000
00404010	58	MOV EAX, ESP	EAX: 00000000
00404011	58	MOV EAX, ESP	EAX: 00000000
00404012	58	MOV EAX, ESP	EAX: 00000000
00404013	58	MOV EAX, ESP	EAX: 00000000
00404014	58	MOV EAX, ESP	EAX: 00000000
00404015	58	MOV EAX, ESP	EAX: 00000000
00404016	58	MOV EAX, ESP	EAX: 00000000
00404017	58	MOV EAX, ESP	EAX: 00000000
00404018	58	MOV EAX, ESP	EAX: 00000000
00404019	58	MOV EAX, ESP	EAX: 00000000
0040401A	58	MOV EAX, ESP	EAX: 00000000
0040401B	58	MOV EAX, ESP	EAX: 00000000
0040401C	58	MOV EAX, ESP	EAX: 00000000
0040401D	58	MOV EAX, ESP	EAX: 00000000
0040401E	58	MOV EAX, ESP	EAX: 00000000
0040401F	58	MOV EAX, ESP	EAX: 00000000
00404020	58	MOV EAX, ESP	EAX: 00000000
00404021	58	MOV EAX, ESP	EAX: 00000000
00404022	58	MOV EAX, ESP	EAX: 00000000
00404023	58	MOV EAX, ESP	EAX: 00000000
00404024	58	MOV EAX, ESP	EAX: 00000000
00404025	58	MOV EAX, ESP	EAX: 00000000
00404026	58	MOV EAX, ESP	EAX: 00000000
00404027	58	MOV EAX, ESP	EAX: 00000000
00404028	58	MOV EAX, ESP	EAX: 00000000
00404029	58	MOV EAX, ESP	EAX: 00000000
0040402A	58	MOV EAX, ESP	EAX: 00000000
0040402B	58	MOV EAX, ESP	EAX: 00000000
0040402C	58	MOV EAX, ESP	EAX: 00000000
0040402D	58	MOV EAX, ESP	EAX: 00000000
0040402E	58	MOV EAX, ESP	EAX: 00000000
0040402F	58	MOV EAX, ESP	EAX: 00000000
00404030	58	MOV EAX, ESP	EAX: 00000000
00404031	58	MOV EAX, ESP	EAX: 00000000

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

Address	Hex dump	ASCII
0046E8F8	8D 48 F9 FF	CALL 004031EC
0046E8FB	8D 45 E0	LEA EAX, DWORD PTR SS:[EBP-20]
0046E8FE	A9 91 F9 FF	CALL 004079B0
0046E901	8D 45 E0	LEA EAX, DWORD PTR SS:[EBP-20]
0046E904	8D 55 E4	LEA EDI, DWORD PTR SS:[EBP-1C]
0046E907	E8 D2 80 F9 FF	CALL 004076E4
0046E90A	8D 4D E4	LEA ECX, DWORD PTR SS:[EBP-1C]
0046E90D	8D 45 E8	LEA EAX, DWORD PTR SS:[EBP-18]
0046E910	8B DCEF 46 00	MOV EDI, 46EFD0
0046E913	E8 36 48 F9 FF	CALL 00403458
0046E916	8D 45 F4	LEA EAX, DWORD PTR SS:[EBP-C]
0046E919	58	PUSH EAX
0046E91C	8D 55 E8	LEA EDI, DWORD PTR SS:[EBP-18]
0046E91F	B1 01	MOV CL, 1
0046E922	8D 45 F8	LEA EAX, DWORD PTR SS:[EBP-8]
0046E925	E8 D9 60 F9 FF	CALL 0040570C
0046E928	8D 45 F4	LEA EAX, DWORD PTR SS:[EBP-C]
0046E92B	58	PUSH EAX
0046E926	8D 55 F4	LEA EDI, DWORD PTR SS:[EBP-C]
0046E929	B8 ECEF 46 00	MOV EAX, 46EFD0
0046E92C	E8 0C 4E F9 FF	CALL 00403750
0046E92F	8D 50 04	ADD EAX, 4
0046E932
0046E935
0046E938
0046E93B
0046E93E
0046E941
0046E944
0046E947
0046E94A
0046E94D
0046E950
0046E953
0046E956
0046E959
0046E95C
0046E95F
0046E962
0046E965
0046E968
0046E96B
0046E96E
0046E971
0046E974
0046E977
0046E97A
0046E97D
0046E980
0046E983
0046E986
0046E989
0046E98C
0046E98F
0046E992
0046E995
0046E998
0046E99B
0046E99E
0046E9A1
0046E9A4
0046E9A7
0046E9AA
0046E9AD
0046E9B0
0046E9B3
0046E9B6
0046E9B9
0046E9BC
0046E9BF
0046E9C2
0046E9C5
0046E9C8
0046E9CB
0046E9CE
0046E9D1
0046E9D4
0046E9D7
0046E9DA
0046E9DD
0046E9E0
0046E9E3
0046E9E6
0046E9E9
0046E9EC
0046E9EF
0046E9F2
0046E9F5
0046E9F8
0046E9FB
0046E9FE
0046E901	41 44 45 39 37 43 41 2D 46 36 34 43 38 31 37 38	ADE97CA-F64C8173
0046E902	2D 31 44 32 36 43 32 37 3D 2D 42 30 34 30 41 42	-1D26C270-B040AB
0046E903	30 34 36 00 74 01 96 00 74 01 96 00 30 00 00 00	046.t03.t03.0...

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

0046E985	803E 00	CMO BYTE PTR DS:[ESI],0	
0046E988	74 1A	JE SHORT 0046E994	azorult.0046E988
0046E98A	E8 5D83FFFF	CALL 0046E98C	azorult.0046E98C
0046E98F	8D45 DC	LEA EAX, DWORD PTR SS:[EBP-24]	
0046E992	E8 2D779FFF	CALL 0046E9C4	azorult.0046E9C4
0046E997	8B45 DC	MOV EAX, DWORD PTR SS:[EBP-24]	
0046E99A	8A 0CF04620	MOV EDI, 46F08C	ASCII "Passwords.txt"
0046E99F	E8 64A4FFFF	CALL 0046E9B8	azorult.0046E9B8
0046E9A4	807E 01 00	CMO BYTE PTR DS:[ESI+1],0	
0046E9A8	74 1A	JE SHORT 0046E9C4	azorult.0046E9C4
0046E9AA	E8 210DFFFF	CALL 0046C6D8	azorult.0046C6D8
0046E9AF	8D45 D8	LEA EAX, DWORD PTR SS:[EBP-28]	
0046E9B2	E8 5D789FFF	CALL 0046E214	azorult.0046E214
0046E9B7	8B45 D8	MOV EAX, DWORD PTR SS:[EBP-28]	
0046E9BA	8A 24F04620	MOV EDI, 46F024	ASCII "CookieList.txt"
0046E9BF	E8 44A4FFFF	CALL 0046E9B8	azorult.0046E9B8
0046E9C4	807E 05 00	CMO BYTE PTR DS:[ESI+5],0	
0046E9C8	74 3E	JE SHORT 0046EA08	azorult.0046EA08
0046E9CA	68 38F04620	PUSH 46F038	
0046E9CF	FF76 00	PUSH DWORD PTR DS:[ESI+8]	
0046E9D2	68 38F04620	PUSH 46F038	
0046E9D7	8D45 D4	LEA EAX, DWORD PTR SS:[EBP-2C]	
0046E9DA	8A 03000000	MOV EDI, 3	
0046E9DF	E8 E4509FFF	CALL 004039C8	azorult.004039C8

AZORult's custom base64-like alphabet:

0040510F	29C9	MOV EAX, EAX	Custom AZORult's alphabet based4-like alphabet
00405111	8945 F8	MOV DWORD PTR SS:[EBP-18], EAX	
00405114	8B45 FC	MOV EAX, DWORD PTR SS:[EBP-4]	
00405117	E8 F8E2FFFF	CALL 0040348C	azorult.0040348C
0040511C	85F8	TEST ESI, EAX	
0040511E	85F5	TEST ESI, ESI	
00405120	8F35 32000000	JL 00405188	azorult.00405188
00405126	C745 F4 0100	MOV DWORD PTR SS:[EBP-C], 1	
0040512D	8D45 EC	LEA EAX, DWORD PTR SS:[EBP-14]	
00405130	8B55 FC	MOV EDI, DWORD PTR SS:[EBP-4]	
00405133	8B4D F4	MOV ECX, DWORD PTR SS:[EBP-C]	
00405136	8D548A FF	MOV DL, BYTE PTR DS:[EDI+ECX-13]	
0040513A	E8 FDE1FFFF	CALL 0040333C	azorult.0040333C
0040513F	8B45 EC	MOV EAX, DWORD PTR SS:[EBP-14]	
00405142	8A F4514000	MOV EDI, 4051F4	
00405147	E8 34E6FFFF	CALL 00403750	ASCII "ST294LUM/56ckL0oq78Ezstvwuivz01NCP0RvSHIJK00VZabodefzDFHljn9+/"
0040514C	8B00	MOV EBX, EAX	azorult.00403750
0040514E	4B	DEC EBX	
0040514F	85D8	TEST EBX, EBX	
00405151	7C 65	JL SHORT 00405188	azorult.00405188
00405153	8B45 F8	MOV EAX, DWORD PTR SS:[EBP-18]	
00405156	C1E9 06	SHL EAX, 6	
00405159	8308	ADD EBX, EAX	
0040515B	895D F8	MOV DWORD PTR SS:[EBP-18], EBX	
0040515E	83C7 06	ADD EDI, 6	
00405161	83FF 06	CMO EDI, 6	
00405164	7C 48	JL SHORT 00405188	azorult.00405188
00405166	83EF 06	SUB EDI, 6	azorult.0040518E

Obtains Windows version via ProductName Registry value:

0040798C	53	PUSH EBX	AZORult obtains Windows version
00407990	81C4 F8DFFFF	ADD ESP, -208	
00407993	8BD8	MOV EBX, EAX	
00407995	C74424 04 00	MOV DWORD PTR SS:[ESP+4], 100	
0040799D	8BC3	MOV EAX, EBX	
0040799F	8A 38704000	MOV EDI, 407A98	
004079C4	E8 9FBEFFFF	CALL 00403960	azorult.00403960
004079C9	6A 00	PUSH 0	pDisposition = NULL
004079CB	8D4424 04	LEA EAX, DWORD PTR SS:[ESP+4]	pHandle
004079CF	50	PUSH EAX	pSecurity = NULL
004079D0	6A 00	PUSH 0	Access = KEY_READ
004079D2	68 19000200	PUSH 20019	Options = REG_OPTION_NON_VOLATILE
004079D7	6A 00	PUSH 0	Class = NULL
004079D9	6A 00	PUSH 0	Reserved = 0
004079DB	6A 00	PUSH 0	Subkey = "SOFTWARE\Microsoft\Windows NT\CurrentVersion"
004079DD	68 3C704000	PUSH 407A9C	hKey = HKEY_LOCAL_MACHINE
004079E2	68 02000000	PUSH 0000002	RegCreateKeyExW
004079E7	E8 A4D1FFFF	CALL 00404B90	azorult.00407A2A
004079EC	85C8	TEST EAX, EAX	
004079EE	75 3A	JNZ SHORT 00407A2A	
004079F0	8D4424 04	LEA EAX, DWORD PTR SS:[ESP+4]	pBufSize
004079F4	50	PUSH EAX	Buffer
004079F5	8D4424 0C	LEA EAX, DWORD PTR SS:[ESP+C]	pValueType = NULL
004079F9	50	PUSH EAX	Reserved = NULL
004079FA	6A 00	PUSH 0	ValueName = "ProductName"
004079FC	6A 00	PUSH 0	
004079FE	68 90704000	PUSH 407A98	hKey
00407A03	8B4424 14	MOV EAX, DWORD PTR SS:[ESP+14]	RegOpenKeyExW
00407A07	50	PUSH EAX	
00407A08	E8 B3D1FFFF	CALL 00404BC0	azorult.00407A21
00407A0D	85C8	TEST EAX, EAX	
00407A0F	75 10	JNZ SHORT 00407A21	
00407A11	8BC3	MOV EAX, EBX	
00407A13	8D5424 08	LEA EDI, DWORD PTR SS:[ESP+8]	
00407A17	B9 00010000	MOV ECX, 100	
00407A1C	E8 9B8FFFFF	CALL 0040396C	azorult.0040396C
00407A21	8B0424	MOV EAX, DWORD PTR SS:[ESP]	
00407A24	50	PUSH EAX	
00407A25	E8 SED1FFFF	CALL 00404B88	hKey
00407A2A	81C4 00020000	ADD ESP, 208	RegCloseKey
00407A30	5B	POP EBX	
00407A31	C3	RET	
00407A32	00	DB 00	
00407A33	00	DB 00	

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.

```
00407400 53          PUSH EBX
00407401 . 81C4 FCFDFF  ADD ESP,-204
00407402 . 8BD8       MOV EBX,EBX
00407403 . C78424 FF00 MOV DWORD PTR SS:[ESP],0FF
00407404 . 54        PUSH ESP
00407405 . 8D4424 00  LEA EAX,DMWORD PTR SS:[ESP+0]
00407406 . 50        PUSH EAX
00407407 . E8 B5D6FFFF CALL 0040839C
00407408 . 85C0       TEST EAX,EAX
00407409 .. 74 12     JE SHORT 004074D9
0040740A . 8BC3       MOV EAX,EBX
0040740B . 8D5424 04  LEA EDI,DMWORD PTR SS:[ESP+4]
0040740C . B9 00010000 MOV ECX,100
0040740D . E8 E5C4FFFF CALL 0040839C
0040740E .. EB 07     JMP SHORT 004074E0
0040740F > 8BC3       MOV EAX,EBX
00407410 . E8 4CC3FFFF CALL 0040838C
00407411 > 81C4 04020000 ADD ESP,204
00407412 . 5B        POP EBX
00407413 . C3        RETN
00407414 53          PUSH EBX
00407415 . 81C4 FCFDFF  ADD ESP,-204
00407416 . 8BD8       MOV EBX,EBX
00407417 . C78424 000100 MOV DWORD PTR SS:[ESP],100
00407418 . 54        PUSH ESP
00407419 . 8D4424 08  LEA EAX,DMWORD PTR SS:[ESP+8]
0040741A . 50        PUSH EAX
0040741B . E8 F5D7FFFF CALL 004084CF
0040741C . 85C0       TEST EAX,EAX
0040741D .. 74 12     JE SHORT 00407519
0040741E . 8BC3       MOV EAX,EBX
0040741F . 8D5424 04  LEA EDI,DMWORD PTR SS:[ESP+4]
00407420 . B9 00010000 MOV ECX,100
00407421 . E8 A5C4FFFF CALL 0040839C
00407422 .. EB 07     JMP SHORT 00407520
00407423 > 8BC3       MOV EAX,EBX
00407424 . E8 0CC3FFFF CALL 0040838C
00407425 > 81C4 04020000 ADD ESP,204
00407426 . 5B        POP EBX
00407427 . C3        RETN
```

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

```

00465D14 | . 8B C9514500 | MOV EAX,456100 | UNICODE ""LOCALAPPDATA\Google\Chrome\User Data\"
00465D19 | . E8 0614F9FF | CALL 00407124 | azorult.00407124
00465D1E | . 8B45 F0 | MOV EAX,DAWORD PTR SS:[EBP-10]
00465D21 | . 8040 F4 | LEA ECX,DAWORD PTR SS:[EBP-C]
00465D24 | . BA 14624500 | MOV EDI,466214 | UNICODE "GoogleChrome"
00465D29 | . E8 0EFDFFFF | CALL 0046598C | azorult.0046598C
00465D2E | . FF75 F4 | PUSH DAWORD PTR SS:[EBP-C]
00465D31 | . 68 34624500 | PUSH 466234 | UNICODE "jg"
00465D36 | . 8045 FC | LEA EAX,DAWORD PTR SS:[EBP-4]
00465D39 | . BA 03000000 | MOV EDI,3
00465D3E | . E8 0500F9FF | CALL 004039C8 | azorult.004039C8
00465D43 | . 8B55 FC | MOV EDI,DAWORD PTR SS:[EBP-4]
00465D46 | . 8BC3 | MOV EAX,EDI
00465D48 | . E8 A806F9FF | CALL 004039F8 | azorult.004039F8
00465D4D | . 8045 E8 | LEA EAX,DAWORD PTR SS:[EBP-10]
00465D50 | . 8B13 | MOV EDI,DAWORD PTR DS:[EBX]
00465D52 | . E8 010CF9FF | CALL 004039C8 | azorult.004039C8
00465D57 | . FF75 E8 | PUSH DAWORD PTR SS:[EBP-10]
00465D5A | . 8055 E8 | LEA EDI,DAWORD PTR SS:[EBP-20]
00465D5D | . 8B 48624500 | MOV EAX,466240 | UNICODE ""LOCALAPPDATA\Google\Chrome\SxS\User Data\"
00465D62 | . E8 8D13F9FF | CALL 00407124 | azorult.00407124
00465D67 | . 8B45 E8 | MOV EAX,DAWORD PTR SS:[EBP-20]
00465D6A | . 8040 E4 | LEA ECX,DAWORD PTR SS:[EBP-1C]
00465D6D | . BA 9C624500 | MOV EDI,46629C | UNICODE "GoogleChrome64"
00465D72 | . E8 45FDFFFF | CALL 0046598C | azorult.0046598C
00465D77 | . FF75 E4 | PUSH DAWORD PTR SS:[EBP-1C]
00465D7A | . 68 34624500 | PUSH 466234 | UNICODE "jg"
00465D7F | . 8045 EC | LEA EAX,DAWORD PTR SS:[EBP-14]
00465D82 | . BA 03000000 | MOV EDI,3
00465D87 | . E8 3C00F9FF | CALL 004039C8 | azorult.004039C8
00465D8C | . 8B55 EC | MOV EDI,DAWORD PTR SS:[EBP-14]
00465D8F | . 8BC3 | MOV EAX,EDI
00465D91 | . E8 4206F9FF | CALL 004039F8 | azorult.004039F8
00465D96 | . 8045 D8 | LEA EAX,DAWORD PTR SS:[EBP-20]
00465D99 | . 8B13 | MOV EDI,DAWORD PTR DS:[EBX]
00465D9B | . E8 380CF9FF | CALL 004039C8 | azorult.004039C8
00465DA0 | . FF75 D8 | PUSH DAWORD PTR SS:[EBP-20]
00465DA3 | . 8055 D8 | LEA EDI,DAWORD PTR SS:[EBP-30]
00465DA6 | . 8B C8624500 | MOV EAX,4662C0 | UNICODE ""LOCALAPPDATA\Xpon\User Data\"
00465DAB | . E8 7413F9FF | CALL 00407124 | azorult.00407124
00465DB0 | . 8B45 D8 | MOV EAX,DAWORD PTR SS:[EBP-30]
00465DB3 | . 8040 D4 | LEA ECX,DAWORD PTR SS:[EBP-2C]
00465DB6 | . BA 84634500 | MOV EDI,466304 | UNICODE "InternetMailRu"
00465DBB | . E8 FC00FFFF | CALL 0046598C | azorult.0046598C
00465DC0 | . FF75 D4 | PUSH DAWORD PTR SS:[EBP-2C]
00465DC3 | . 68 34624500 | PUSH 466234 | UNICODE "jg"
00465DC8 | . 8045 DC | LEA EAX,DAWORD PTR SS:[EBP-24]
00465DCE | . BA 03000000 | MOV EDI,3

```

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

- PsiPlus
- Psi
- Pidgin

Moreover, AZOrult also appear to collect 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.

The screenshot shows a debugger window with two main panes. The top pane displays assembly code with instructions like 'TEST EDI,EDI', 'JE SHORT 00403794', 'PUSH EDI', etc. A red box highlights the instruction 'JE SHORT 00403794'. The bottom pane shows a hex dump of memory, with columns for Address, Hex dump, and ASCII. A red arrow points from the highlighted instruction in the assembly pane to the hex dump entry at address 00968800, which contains the ASCII string '1..IS_G_COINS:'. A text box in the assembly pane reads 'AZORults grabs .txt and .dat files from Desktop'.

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:

The screenshot shows a debugger window with the following assembly code on the left and CPU registers on the right.

Address	Disassembly	Comment
004F216	xor eax, eax	
004F218	push ebp	
004F219	mov esp, ebp	
004F21E	push [ebp+00000000]	
004F221	lea ebx, [ebp+00000000]	
004F224	push ebx	
004F225	lea ebx, [ebp+00000000]	
004F227	push ebx	
004F230	push 0	
004F232	call 00404070	
004F237	lea ebx, [ebp+00000000]	
004F239	lea ebx, [ebp+00000000]	
004F23F	lea ebx, [ebp+00000000]	
004F240	push [ebp+00000000]	
004F241	push [ebp+00000000]	
004F242	push [ebp+00000000]	
004F243	push [ebp+00000000]	
004F244	push [ebp+00000000]	
004F245	push [ebp+00000000]	
004F246	push [ebp+00000000]	
004F247	push [ebp+00000000]	
004F248	push [ebp+00000000]	
004F249	push [ebp+00000000]	
004F24A	push [ebp+00000000]	
004F24B	push [ebp+00000000]	
004F24C	push [ebp+00000000]	
004F24D	push [ebp+00000000]	
004F24E	push [ebp+00000000]	
004F24F	push [ebp+00000000]	
004F250	push [ebp+00000000]	
004F251	push [ebp+00000000]	
004F252	push [ebp+00000000]	
004F253	push [ebp+00000000]	
004F254	push [ebp+00000000]	
004F255	push [ebp+00000000]	
004F256	push [ebp+00000000]	
004F257	push [ebp+00000000]	
004F258	push [ebp+00000000]	
004F259	push [ebp+00000000]	
004F25A	push [ebp+00000000]	
004F25B	push [ebp+00000000]	
004F25C	push [ebp+00000000]	
004F25D	push [ebp+00000000]	
004F25E	push [ebp+00000000]	
004F25F	push [ebp+00000000]	
004F260	push [ebp+00000000]	
004F261	push [ebp+00000000]	
004F262	push [ebp+00000000]	
004F263	push [ebp+00000000]	
004F264	push [ebp+00000000]	
004F265	push [ebp+00000000]	
004F266	push [ebp+00000000]	
004F267	push [ebp+00000000]	
004F268	push [ebp+00000000]	
004F269	push [ebp+00000000]	
004F26A	push [ebp+00000000]	
004F26B	push [ebp+00000000]	
004F26C	push [ebp+00000000]	
004F26D	push [ebp+00000000]	
004F26E	push [ebp+00000000]	
004F26F	push [ebp+00000000]	
004F270	push [ebp+00000000]	
004F271	push [ebp+00000000]	
004F272	push [ebp+00000000]	
004F273	push [ebp+00000000]	
004F274	push [ebp+00000000]	
004F275	push [ebp+00000000]	
004F276	push [ebp+00000000]	
004F277	push [ebp+00000000]	
004F278	push [ebp+00000000]	
004F279	push [ebp+00000000]	
004F27A	push [ebp+00000000]	
004F27B	push [ebp+00000000]	
004F27C	push [ebp+00000000]	
004F27D	push [ebp+00000000]	
004F27E	push [ebp+00000000]	
004F27F	push [ebp+00000000]	
004F280	push [ebp+00000000]	
004F281	push [ebp+00000000]	
004F282	push [ebp+00000000]	
004F283	push [ebp+00000000]	
004F284	push [ebp+00000000]	
004F285	push [ebp+00000000]	
004F286	push [ebp+00000000]	
004F287	push [ebp+00000000]	
004F288	push [ebp+00000000]	
004F289	push [ebp+00000000]	
004F28A	push [ebp+00000000]	
004F28B	push [ebp+00000000]	
004F28C	push [ebp+00000000]	
004F28D	push [ebp+00000000]	
004F28E	push [ebp+00000000]	
004F28F	push [ebp+00000000]	
004F290	push [ebp+00000000]	
004F291	push [ebp+00000000]	
004F292	push [ebp+00000000]	
004F293	push [ebp+00000000]	
004F294	push [ebp+00000000]	
004F295	push [ebp+00000000]	
004F296	push [ebp+00000000]	
004F297	push [ebp+00000000]	
004F298	push [ebp+00000000]	
004F299	push [ebp+00000000]	
004F29A	push [ebp+00000000]	
004F29B	push [ebp+00000000]	
004F29C	push [ebp+00000000]	
004F29D	push [ebp+00000000]	
004F29E	push [ebp+00000000]	
004F29F	push [ebp+00000000]	
004F2A0	push [ebp+00000000]	
004F2A1	push [ebp+00000000]	
004F2A2	push [ebp+00000000]	
004F2A3	push [ebp+00000000]	
004F2A4	push [ebp+00000000]	
004F2A5	push [ebp+00000000]	
004F2A6	push [ebp+00000000]	
004F2A7	push [ebp+00000000]	
004F2A8	push [ebp+00000000]	
004F2A9	push [ebp+00000000]	
004F2AA	push [ebp+00000000]	
004F2AB	push [ebp+00000000]	
004F2AC	push [ebp+00000000]	
004F2AD	push [ebp+00000000]	
004F2AE	push [ebp+00000000]	
004F2AF	push [ebp+00000000]	
004F2B0	push [ebp+00000000]	
004F2B1	push [ebp+00000000]	
004F2B2	push [ebp+00000000]	
004F2B3	push [ebp+00000000]	
004F2B4	push [ebp+00000000]	
004F2B5	push [ebp+00000000]	
004F2B6	push [ebp+00000000]	
004F2B7	push [ebp+00000000]	
004F2B8	push [ebp+00000000]	
004F2B9	push [ebp+00000000]	
004F2BA	push [ebp+00000000]	
004F2BB	push [ebp+00000000]	
004F2BC	push [ebp+00000000]	
004F2BD	push [ebp+00000000]	
004F2BE	push [ebp+00000000]	
004F2BF	push [ebp+00000000]	
004F2C0	push [ebp+00000000]	
004F2C1	push [ebp+00000000]	
004F2C2	push [ebp+00000000]	
004F2C3	push [ebp+00000000]	
004F2C4	push [ebp+00000000]	
004F2C5	push [ebp+00000000]	
004F2C6	push [ebp+00000000]	
004F2C7	push [ebp+00000000]	
004F2C8	push [ebp+00000000]	
004F2C9	push [ebp+00000000]	
004F2CA	push [ebp+00000000]	
004F2CB	push [ebp+00000000]	
004F2CC	push [ebp+00000000]	
004F2CD	push [ebp+00000000]	
004F2CE	push [ebp+00000000]	
004F2CF	push [ebp+00000000]	
004F2D0	push [ebp+00000000]	
004F2D1	push [ebp+00000000]	
004F2D2	push [ebp+00000000]	
004F2D3	push [ebp+00000000]	
004F2D4	push [ebp+00000000]	
004F2D5	push [ebp+00000000]	
004F2D6	push [ebp+00000000]	
004F2D7	push [ebp+00000000]	
004F2D8	push [ebp+00000000]	
004F2D9	push [ebp+00000000]	
004F2DA	push [ebp+00000000]	
004F2DB	push [ebp+00000000]	
004F2DC	push [ebp+00000000]	
004F2DD	push [ebp+00000000]	
004F2DE	push [ebp+00000000]	
004F2DF	push [ebp+00000000]	
004F2E0	push [ebp+00000000]	
004F2E1	push [ebp+00000000]	
004F2E2	push [ebp+00000000]	
004F2E3	push [ebp+00000000]	
004F2E4	push [ebp+00000000]	
004F2E5	push [ebp+00000000]	
004F2E6	push [ebp+00000000]	
004F2E7	push [ebp+00000000]	
004F2E8	push [ebp+00000000]	
004F2E9	push [ebp+00000000]	
004F2EA	push [ebp+00000000]	
004F2EB	push [ebp+00000000]	
004F2EC	push [ebp+00000000]	
004F2ED	push [ebp+00000000]	
004F2EE	push [ebp+00000000]	
004F2EF	push [ebp+00000000]	
004F2F0	push [ebp+00000000]	
004F2F1	push [ebp+00000000]	
004F2F2	push [ebp+00000000]	
004F2F3	push [ebp+00000000]	
004F2F4	push [ebp+00000000]	
004F2F5	push [ebp+00000000]	
004F2F6	push [ebp+00000000]	
004F2F7	push [ebp+00000000]	
004F2F8	push [ebp+00000000]	
004F2F9	push [ebp+00000000]	
004F2FA	push [ebp+00000000]	
004F2FB	push [ebp+00000000]	
004F2FC	push [ebp+00000000]	
004F2FD	push [ebp+00000000]	
004F2FE	push [ebp+00000000]	
004F2FF	push [ebp+00000000]	

The CPU registers window on the right shows the following values:

- EAX: 00000000
- ECX: 00000000
- EDX: 00000000
- EBX: 00000000
- ESP: 004F230
- EBP: 004F230
- ESI: 00000000
- EDI: 00000000
- EIP: 004F230
- EAX: 00000000
- ECX: 00000000
- EDX: 00000000
- EBX: 00000000
- ESP: 004F230
- EBP: 004F230
- ESI: 00000000
- EDI: 00000000
- EIP: 004F230