# Revisiting Heaven's Gate with Lumma Stealer

**Prepared by: Vlad Pasca, Senior Malware &** 

**Threat Analyst** 



SecurityScorecard.com info@securityscorecard.com

Tower 49 12 E 49<sup>th</sup> Street Suite 15-001 New York, NY 10017 1.800.682.1707

# Table of contents

Table of contents Executive summary Analysis and findings Indicators of Compromise



# **Executive summary**

Lumma is a stealer that has been sold on hacker forums since August 2022. The malware steals information from web browsers, cryptocurrency wallets, 2FA extensions, and applications such as AnyDesk, FileZilla, KeePass, Steam, and Telegram. The process also gathers data about the infected machine, such as the installed applications, the username and computer name, the current hardware profile, the system default language, the screen resolution, the RAM amount, and the processor name and type. The malware employs the Heaven's Gate technique that enables a 32-bit process to execute 64-bit code by performing a call using segment selector 0x33. The stolen information is exfiltrated to the C2 server using multiple HTTP POST requests.

# **Analysis and findings**

SHA256: 199de8b727ceae96afb7c7560092c1d7a4dbe5a005c07ae20cffd9871da52b82

File name:	C:\Users\ Desktop\malware.exe	
Scan Scri	ipts Plugins Log	
Туре	: PE Size: 3449856 Entropy FLC S H	
Export	Import Resource Overlay LIET PE	
EntryPoint:	0059314d > ImageBase: 00400000	
NumberOfSe	ctions: 0003 > SizeOfImage: 005b4000	
packer	MPRESS(2.19)[-] ?	
linker	unknown(14.0)[EXE32,admin] ?	Options
	•	About
	Signatures 406 ms Scan	Exit

Using the "Detect It Easy" tool, we determined that the sample is packed with MPRESS:

### Figure 1

As we can see in figure 2, the code is decoded at runtime, and we need to find the point where to dump the unpacked executable:



Figure 2

The malware implements the API hashing technique that resolves the necessary APIs based on 4-byte hashes:



The ExpandEnvironmentStringsW API is utilized to obtain the path of the Google Chrome User Data directory, as shown in figure 5.

O04096CD 56     O04096CE FF 74 24 2C     O04096D2 FF 84 24 14 01 00	push esi push dword ptr ss: [esp+2C] push dword ptr ss: [esp+114]	x875W_C1 0 x875W_C0 0 x875W_E5 0 x875W_SF 0 x875W_P 0 x875W_U 0
exectarnal22 ExpandEnvironmentStringsWb (764745	(call eax	eax:Ex → Default (stdcall) → 5 • Unlock 1: [esp] 0287FF58 L"%localappdata%\\Google\\Chro
.MPRESS1:004096D9 malware.exe:\$96D9 #88D9	40)	2: [e5p+4] 028D05E0 3: [e5p+6] 0000104 4: [e5p+6] F65095E0 5: [e5p+10] 0000000
Ump 1 Ump 2 Ump 3 Ump 4	Dump 5 🛞 Watch 1 🛛 🖉 Struct	ODIEIDED         0287FF58         ["%localappdata%\\Google\\Chrome\\User Data"           0019FD24         028D05E0         0019FD24         0019FD24

Figure 5

The malicious binary determines if the current process is running under WOW64 via a function call to IsWow64Process2:

● 004282A0 ● 004282A3 ● 004282A6 ● 004282A6 ● 004282A6	FF 75 E0 FF 75 DC FF 75 9C FF D0	push dword ptr ss: [ebp-20] push dword ptr ss: [ebp-24] push dword ptr ss: [ebp-64] call eax	eax:15	0 0 x875W_ES 0 0 x875W_U 0
eax= <kernelbase.iswow64proc< td=""><td>cess2&gt; (76F09E70) exe:\$282A9 #2A4A9</td><td></td><td>&gt; Uctobit (stock) 1: [esp] FFFFFFF 2: [esp+4] 0019F820 4: [esp+6] 0019F820 4: [esp+c] 00000000 5: [esp+10] 00000000</td><td></td></kernelbase.iswow64proc<>	cess2> (76F09E70) exe:\$282A9 #2A4A9		> Uctobit (stock) 1: [esp] FFFFFFF 2: [esp+4] 0019F820 4: [esp+6] 0019F820 4: [esp+c] 00000000 5: [esp+10] 00000000	
Dump 1 Dump 2	Dump 3 👯 Dump 4 👯 Dun	np 5 🥮 Watch 1 [x= Locals 🎾 Struct	0019FAE0 FFFFFFF 0019FAF4 0019FB24 0019FAF8 0019FB20	

The malicious process opens the NTDLL.dll file in order to extract the syscall numbers that will be used at runtime (0x8000000 = **GENERIC\_READ**, 0x1 = **FILE\_SHARE\_READ**, 0x3 = **OPEN\_EXISTING**, 0x80 = **FILE\_ATTRIBUTE\_NORMAL**):

EIP 004E1153 87 34 24 004E1156 C3	xchg dword ptr ss:[esp],es1	(esp): → Default (stdcal)
dword ptr [esp]=[0019F56C <&CreateFilew>]= <kernel32.cre esi=B '\v' .MPRESS1:004E1153 malware.exe:\$E1153 #E0353</kernel32.cre 	ateFilew>	1: [E5P4] 0042A343 malware.0042A343 2: [E5P4] 0042B0 L°C:\\Windows\\System32\\nt: 3: [E5P4] 0000000 4: [E5P40] 00000001 5: [E5P44] 0000000
💷 Dump 1 🚛 Dump 2 🚛 Dump 3 🚛 Dump 4 🚛 Dump 5	🛞 Watch 1 🛛 🗱 Locals 🖉 Struct	0019F56C 76ACDDE0 kernel32.CreateFileW 0019F570 [0042A343 malware.0042A343
Address         Hex           76FE1000         1C         00         1E         0         00         DE         FE         76         28         00         2A         00         DE         FE         76         28         00         2A         00         DE         FE         76         12         00         20         DE         FE         76         12         00         20         00         FE         76         12         00         12         00         FE         76         13         00         20         00         FE         76         13         00         14         00         FE         76         12         00         12         00         FE         10         FE         10         10         10         10         10         10         10         10         10         10         10         10         10         10	ASCII       ASCII      ASCIV      ASCIV	0019F574 004520B0 L°C:\\Windows\\System32\\ntdll.dll" 0019F576 80000000 0019F550 00000001 0019F580 00000000 0019F584 00000003 0019F588 00000080



It retrieves the size of the specified DLL using GetFileSize:

	ret	> Default (stdcall)
.MPRESS1:0042157B malware.exe:\$2157B #2077B		2: [esp+8] 00000150 3: [esp+1] 0000000 4: [esp+10] FDB03A50 5: [esp+14] 00452DEC L"KernelBase.dll"
Ump 1 Ump 2 Ump 3 Ump 4 Ump 4	mp 5 🛞 Watch 1 💷 Locals 🦻 Struct	00195580 76ACE000 kernel32.GetFileSize 00195584 0042A358 return to malware.0042A358 from malware. 00195588 00000150

#### Figure 8

The ReadFile method is used to read data from the DLL:

EIP	0042A8	C3			ret				>	Def	ault (stdcall	)	▼ 5 \$	Unlock
.MPRESS1:00	042A81E malwa	are.exe:\$2A8	1E #29A1E							1: 2: 3: 4: 5:	[esp+4] [esp+8] [esp+C] [esp+10] [esp+14]	0042AFC8 malware.0 00000150 04890020 ] 001DD100 ] 00195684	D42AFC8	
Dump 1	Dump 2	Dump 3	💷 Dump 4	📖 Dump 5	👹 Watch 1	[x=] Locals	2 Struct	0	019F574 7 019F578 0	6ACE16	kernel 8 return	32.ReadFile to malware.0042AFG	8 from malu	vare.004
Address Ho 04890020 0 04890030 0 04890040 0	ex 0 00 00 00 00 0 00 00 00 00 0 00 00 00		0 00 00 00 0 00 00 00 0 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00	ASCII				019F57C (0 019F580 (0 019F584 (0 019F588 (0 019F58C (0	0000019 0489002 001DD10 0019F68	0 0 4 0			

#### Figure 9

The malicious activity is implemented using the Heaven's Gate technique. The segment selector 0x33 is utilized to transition to x64 mode and execute 64-bit code. As we can see below, the syscall 0x55 (NtCreateFile function) is used to open the Local State file:





Figure 11

NtQueryInformationFile is used to obtain the above file size:

🔄 SecurityScorecard

■ 0040102D 0040102E 00401030 00401030 0040103A 0040103A 0040103B 0040103B 0040103B 0040103B 00401040 00401040 00401040 00401045 00401045 00401045 00401045 00401045 00401045 00401045 00401051 00401051 00401055 004	55         58         53         52         51         51         51         51         51         51         51         51         54         51         54         54         54         54         54         54         54         54         54         54         55         55         55         55         57         52         52         51         54         54         54         54         54         54         54         54         54         54         54         54         54         54         54         55         10         54         55         10         54         55         10         54         55         10         56         10         10         10         10         10         10         10         10         10         10         10         10         10         10<	push ebp mov ebp,esp and esp,FFFFFF0 call far 35;malware.40103E mov esp,ebp pet trc ecx push edx push edx trc ecx push ecx push ecx push ecx push ecx trc ecx push ecx trc ecx push ecx trc ecx push est trc ecx trc ec	ebx:Ge	F0 IF1 IF1           astEtror 00000000 (ERROR_SUCCESS)           astStatus C0000034 (STATUS_0BJECT_NAME_NOT_FOU           S 0028 F5 0053           S 0028 JS 0028           S700 0000000000000000000000000000000000
• <			> De	fault (stdcall) 🔹 5 🖶 🗌 Unloc
0033:0040103E=0 .MPRESS1:00401033 malware.e	xe:\$1033 #233		1	[esp+6] 0000001 [esp+C] 00000005 [esp+10] 02CB1680 [esp+14] C1FDC799
Image: Doump 1         Image: Doump 2         Image:	Dump 3 500 Dump 4 500 Dump CB 02 38 16 CB 02 18 00 00 AB AB AB AB AB AB AB EE FE EE	S         Image: Second system         Struct           ASCII         ASCII         Image: Second system         Struct           FE         Second system         Struct         Struct	0019FA90 0019F8 0019FA94 004280 0019FA98 000000 0019FA92 000000 0019FA9C 000000 0019FA9C 000000	0 46 return to malware.00428D46 from malware.004 11 05 80 80

The malicious binary reads the file content by calling the NtReadFile method:

	0040102D	55	push ebp		
	0040102E	89 E5	mov ebp.esp		
	00401030	83 E4 F0	and esp. FFFFFF0		LastError 00000000 (ERROR_SUCCESS)
ETP	00401033	9A 3F 10 40 00 33 00	call far 33:malware, 40103E		LastStatus C0000034 (STATUS OBJECT NAME NOT FOUN
	0040103A	89 EC	mov esp.ebp		
	00401030	50	pop ebp		GS 0028 ES 0052
	00401030	63	rat		55 0020 PS 0020
	00401025	41	inc acy		ES 002B DS 002B
	00401035	52	nuch edv		CS 0023 SS 0028
	0040103P	54	push ecx		
	00401040	50	push edv		x87r0 00000000000000000 ST0 Empty 0.000000000
	00401041	52	inc eck		x87r1 000000000000000000 ST1 Empty 0.000000000
	00401042	74	THE ECA		x87r2 00000000000000000 ST2 Empty 0.000000000
	00401043	50	push eax		x87r3 00000000000000000 ST3 Empty 0.000000000
	00401044	41	Inc ecx		x87r4 0000000000000000 ST4 Empty 0.00000000
	00401045	51	push ecx		x8745 000000000000000000000000000000000000
	00401046	41	Inc ecx		x87FS 000000000000000000000000000000000000
	00401047	56	push est		x8/F6 000000000000000000000000000000000000
	00401048	41	Inc ecx		x87r7 000000000000000000 ST7 Empty 0.000000000
	00401049	57	push eat		
	0040104A	41	inc ecx		x87TagWord FFFF
	00401048	54	push esp		x87TW_0 3 (Empty) x87TW_1 3 (Empty)
	0040104C	41	Inc ecx		x87TW 2 3 (Empty) x87TW 3 3 (Empty)
	0040104D	53	push ebx	ebx:Ge	x87TW 4 3 (Empty) x87TW 5 3 (Empty)
	0040104E	41	Inc ecx		verte 6 2 (Empty) verte 7 2 (Empty)
	0040104F	55	push ebp		Korra_o S (Empty) Korra_r S (Empty)
	00401050	49	dec ecx		
	00401051	C7 C2 00 00 00 00	mov edx,0		x87Statusword 0000
	00401057	49	dec ecx		x87SW_B 0 x87SW_C3 0 x87SW_C2 0
	00401058	C7 C6 00 00 00 00	mov esi,0		x875W_C1 0 x875W_C0 0 x875W_E5 0
	0040105E	44	inc esp		x875W_SF 0 x875W_P 0 x875W_U 0
	0040105F	8B 55 10	mov edx, dword ptr ss:[ebp+10]		
	00401062	44	inc esp	V V	
	00404060	66 75 0C	Taran and shared and an endertailed		Default (stdcall) 🔻 5 💠 🗌 Unlock
	<			>	1: [ecn+4] 00420046 ma]ware 00420046
0033:0040103E=0	)				2: [esp+1] 00000006
					3: [esp+C] 00000009
					4: [eco+10] 02CC4ER0
.MPRESS1:004010	33 malware.ex	xe:\$1033 #233			5: [esp+14] C15DC700
					a. feabrard crineing
Dumo 1	Dumo 2	umo 3 IIII Dumo 4 IIII Dumo 5	Watch 1 Irali ocale Struct 001	9FA80 001	9FB60
e-e bump 1 e-e	bump z www.	tump 5 ere bump 4 ere bump 5		9FA84 004	28D46 return to malware.00428D46 from malware.004(
Address Hex			ASCII	9FA86 000	00000
02CC4EB0 50 01	00 00 00 00	00 00 00 00 00 00 00 00 00 00 00	00 P	9FA90 020	CAEBO
02CC4EC0 10 16	CB 02 B0 16 0	CB 02 E1 37 01 00 00 00 00 0	00EE. a7	9FA94 C1F	DC 7 9 9
02CC4ED0 00 00	00 00 AB AB	AB AB AB AB AB AB EE FE EE F	E ««««««««iþiþ	95498 866	40011

Figure 13

Finally, the file is closed via a function call to NtCloseFile:

StP         Column           0.040103A         0.040103A           0.040103C         0.040103D           0.040103D         0.040103D           0.040103D         0.040103D           0.040103D         0.040103D           0.040103D         0.040103D           0.040103D         0.040103D           0.0401042         0.0401042           0.0401044         0.0401044           0.0401044         0.0401044           0.0401044         0.0401044           0.0401044         0.0401044           0.0401045         0.0401045           0.0401046         0.0401045           0.0401045         0.0401045           0.0401045         0.0401045           0.0401045         0.0401045           0.0401050         0.0401055           0.0401055         0.0401055           0.0401055         0.0401055           0.0401055         0.0401055           0.0401055         0.0401055	9A         3E         10         40         00         33         00           89         EC         50         51         52         51         52         51         52         41         50         41         50         41         56         41         56         41         57         41         54         41         57         57         41         56         41         51         57         57         52         41         56         41         51         51         57         51         57         51         57         51         57         51         51         51         57         51         52         41         51         51         52         41         51         51         51         57         51         57         51         51         51         51         51         51         51         55         51         55         51         51         55         51 </th <th><pre>call fai 33:malware.40103E mov esp, ebp pop ebp ret fush ex push ex push ecx push ecx push ecx push ecx push ecx inc ecx push ecy push ecx push ecy pus</pre></th> <th>ebx:Ge</th> <th>LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOU GS 0028 FS 0053 ES 0028 DS 0028 CS 0023 <u>SS</u> 0028 X87r0 00000000000000000000000000000000000</th>	<pre>call fai 33:malware.40103E mov esp, ebp pop ebp ret fush ex push ex push ecx push ecx push ecx push ecx push ecx inc ecx push ecy push ecx push ecy pus</pre>	ebx:Ge	LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOU GS 0028 FS 0053 ES 0028 DS 0028 CS 0023 <u>SS</u> 0028 X87r0 00000000000000000000000000000000000
0033:0040103E=0           .MPRESS1:00401033 malware.e	xxe:\$1033 #233 Dump 3 ## Dump 4 ## Dump AB AB AB AB AB AB AB EE FE EE 90 00 08 90 F1 AE 2F D5 90	5         60         Watch 1         Ix=  Locals         20         Struct           ASCII         ASCII         FE         Bx_accescent prip         00         100	0019F850 666 0019F884 001 0019F888 004 0019F885 000 0019F890 000 0019F890 000	1: (esp-4) 0019FC64 2: (esp-4) 00428046 malware.00428D46 3: (esp-C) 0000000F 4: (esp-10) 00000001 5: [esp-14] 02C810A8 FG07E 9FC64 9FC64 9FC64 00001 80068

Figure 14

The "encrypted\_key" extracted from the Local State file is Base64-decoded using the CryptStringToBinaryA API (0x1 = **CRYPT\_STRING\_BASE64**):

	push edi push dword ptr ss: ebp-1C] push dword ptr ss: ebp-4C] push dword ptr ss: ebp-4C] push edi push edi push dword ptr ss: ebp-84]	[ebp-8 eax:Cr	xe/rm_b 3 (EmpLy) x8/rm_/ 3 (EmpLy) x8/5tatusword 0000 x8/5W_E 0 x8/5W_C3 0 x875W_C2 0 x8/5W_E 0 x8/5W_C3 0 x875W_E5 0 x8/5W_E 0 x8/5W_P 0 x8/5W_U 0 Default (stdcall) v 5 0 x8/5W_U 0 1 (esp)+1 00000000 1 (esp)+1 00000000 2 (esp+4) (esp+4) 00000000 2 (esp+4) (e
Image: Second	5 🛞 Watch 1   i=locals 🎾 Struct A [0, *, 0, *, 0, *, 0, *, 0, *] BA [0, *, 0, *, 0, *, 0, *] BA [0, *, 0, *, 0, *, 0, *] A [0, *, 0, *] (A [0, *]) (A [0, *])	0019FBFC 02CC7 0019FC00 00000 0019FC04 00000 0019FC08 02CF1 0019FC0C 0019F 0019FC10 00000 0019FC14 00000	7E8 "RF8BUEKBAAAAOIyd3wEVORGMegDAT8KX6wEAAADfM+ 001 A30 C28 000

#### Figure 15

The binary decrypts the resulting buffer and obtains a 32-byte AES key using CryptUnprotectData:

0040714E 89 0C 24 00407155 C7 44 24 14 00 00 00 00 00407155 FF D2 € 00407155 FF D2	mov dword ptr ss: esp],ecx mov dword ptr ss: espiid],o call edx	edx:crv Default (stdcall)
edx= <crypt32.cryptunprotectdata> (768958E0)</crypt32.cryptunprotectdata>		2: [esp+4] 00000000
		3: [esp+8] 00000000
.MPRESS1:00407159 malware.exe:\$7159 #6359		4: [esp+C] 00000000 5: [esp+10] 00000000
	(A)	0019F8FC 0019FC18
Ump 1 Ump 2 Ump 3 Ump 4 Ump 4	5 🐨 Watch 1 🛛 🖾 Locals 🖉 Struct	0019FC00 00000000
Address Hex	ASCII	0019FC04 0000000
0019FC18 06 01 00 00 18 26 CF 02 00 00 00 00 00 00 00 00	00ů	0019FC08 0000000
0019FC28 0B 01 00 00 E1 37 01 00 B0 16 CB 02 00 00 00	00 â7 E	0019FC10 00000000
0019FC38 00 00 00 00 A8 00 CB 02 D8 00 CB 02 50 01 00	00E.Ø.E.P	0019FC14 0019FC20

#### Figure 16

Lumma Stealer targets multiple Browser wallets, which are located in the "Google\Chrome\User Data\Default\Local Extension Settings\" directory. An example is shown in figure 17, which is looking for MetaMask:

0040102D 55	push ebp	1	CEO IEX XEX
0040102E 89 E5	mov ebp,esp		
00401030     83 E4 F0	and esp, FFFFFF0	_	LastError 00000000 (ERROR_SUCCESS)
00401033 9A 3E 10 40 00 33 00	Mov esp.ehp		Laststatus 0000000 (STATUS_SUCCESS)
• 0040103C 5D	pop ebp		GS 0028 ES 0053
e 0040103D C3	ret		ES 002B DS 002B
0040103E 41	inc ecx		CS 0023 SS 0028
0040103F 52	push edx		
e 00401040 51 e 00401041 52	push edx		x87r0 00000000000000000 STO Empty 0.00000000
00401042 41	inc ecx		x87r1 000000000000000000 ST1 Empty 0.00000000
00401043     50	push eax		x87r2 000000000000000000 ST2 Empty 0.00000000
00401044     41	inc ecx		x87r3 000000000000000000 ST3 Empty 0.00000000
• 00401045 <b>51</b>	push ecx		x8/F4 000000000000000000000000000000000000
e 00401046 41	nuch est		x87r6 000000000000000000000000000000000000
00401048 41	inc ecx		x87r7 000000000000000000 ST7 Empty 0.00000000
Ø 00401049 57	push edi		
0040104A     41	inc ecx		x87TagWord FFFF
• 0040104B 54	push esp		x87TW_0 3 (Empty) x87TW_1 3 (Empty)
0040104C 41     0040104D 52	INC ECX	aby: Ge	x87TW_2 3 (Empty) x87TW_3 3 (Empty)
e 0040104E 41	inc ecx	eux. de	x87TW_4 3 (Empty) x87TW_5 3 (Empty)
0040104F 55	push ebp		x87TW_6 3 (Empty) x87TW_7 3 (Empty)
00401050     49	dec ecx		water swalland oppo
• 00401051 C7 C2 00 00 00 00	mov edx,0		X8/Statusword 0000
e 00401057 49 e 00401058 C7 C6 00 00 00 00	dec ecx		x875W C1 0 x875W C0 0 x875W E5 0
e 0040105E 44	inc esp		x875W SE 0 x875W P 0 x875W U 0
0040105F 88 55 10	mov edx, dword ptr ss: [ebp+10]		
00401062 44	inc esp	~	
		>	Default (stdcall) The Source Unlock
00331-00401035=0			1: [esp+4] 0042BD46 malware.0042BD46
0033:00401032=0			2: [esp+8] 00000055
			4: [esp+t0] 02028080
.MPRESS1:00401033 malware.exe:\$1033 #233			5: [esp+14] C1FDC799
	0019	9E4E0 -0019	PF5D0
Ump 1 Ump 2 Ump 3 Ump 4 Ump 5	Watch 1 [x=] Locals 2 Struct 0019	9F4F4 0042	2BD46 return to malware.0042BD46 from malware.004
Address Hex	ASCII	9F4F8 0000	00055
02D2BB00 00 00 00 00 00 00 00 00 39 9C F2 4D 2E D6 00 18		9F4FC 0000	0000B
02D2BB10 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA		9E504 C1E	0799
02D2BB20 AB 00 00 00 00 00 00 00 00	««««««««««	9F508 8664	\$3AF9
02D2BB30 75 9C F2 01 2E D6 00 18 5C 00 3F 00 3F 00 5C 00	0019	9F50C 0000	0000A
02028850 5C 00 5C 00 5C 00 55 00 75 00 05 00 72 00 73 00	0019	9F510 02D2	2BD 80
02D2BB60 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00	D.a.t.a.\.L.O.C. 0015	9F514 0000	00000
02D2BB70 61 00 6C 00 5C 00 47 00 6F 00 6F 00 67 00 6C 00	a.l.\.G.o.o.g.l.	9E51C 9EE1	19201
02D2BB80 65 00 5C 00 43 00 68 00 72 00 6F 00 6D 00 65 00	e.\.C.n.r.o.m.e. 0019	9F520 0000	00055
02028840 74 00 61 00 55 00 44 00 65 00 66 00 61 00 75 00	T.a.\.D.e.f.a.u. 0019	9F524 8664	44F0E
02028880 6C 00 74 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00	1.t.\.L.o.c.a.1.	9F528 0019	9F638
02D2BBC0 20 00 45 00 78 00 74 00 65 00 6E 00 73 00 69 00	.E.x.t.e.n.s.i. 0015	9F52C 0019	7F5A0
02D2BBD0 6F 00 6E 00 20 00 53 00 65 00 74 00 74 00 69 00	0.nS.e.t.t.i. 0015	9F534 0000	0014C
02028860 66 00 67 00 73 00 5C 00 65 00 6A 00 62 00 61 00	n.g.s.\.e.j.b.a. 0019	9F538 0000	0000B
02028C00 68 00 6C 00 67 00 68 00 65 00 63 00 64 00 61 00	h.l.g.h.e.c.d.a.	9F53C 0019	0F63C
02D2BC10 6C 00 6D 00 65 00 65 00 65 00 61 00 6A 00 6E 00	1.m.e.e.e.a.j.n.	9F5 40 0000	00000 kernelbase Tswow64Process2
		71 7 T T T T OF C	267 V NEI HEINGSCI ISHUNDERI ULCSSE



The following Browser wallets and 2FA applications are targeted:

- aeachknmefphepccionboohckonoeemg (Coin98 Wallet)
- afbcbjpbpfadlkmhmclhkeeodmamcflc (Math Wallet)
- aiifbnbfobpmeekipheeijimdpnlpgpp (Station Wallet)
- amkmjjmmflddogmhpjloimipbofnfjih (Wombat)
- bcopgchhojmggmffilpImbdicgaihlkp (Hycon Lite Wallet)
- bhghoamapcdpbohphigoooaddinpkbai (Google Authenticator extension)
- blnieiiffboillknjnepogjhkgnoapac (EQUAL Wallet)
- cihmoadaighcejopammfbmddcmdekcje (Leaf Wallet)
- cjelfplplebdjjenllpjcblmjkfcffne (Jaxx Liberty)
- cnmamaachppnkjgnildpdmkaakejnhae (Auro Wallet)
- cphhlgmgameodnhkjdmkpanlelnlohao (NeoLine Wallet)
- dkdedlpgdmmkkfjabffeganieamfklkm (Cyano Wallet)
- dmkamcknogkgcdfhhbddcghachkejeap (Kepir Wallet)
- ejbalbakoplchlghecdalmeeeajnimhm (MetaMask)
- ffnbelfdoeiohenkjibnmadjiehjhajb (Yoroi Wallet)
- fhbohimaelbohpjbbldcngcnapndodjp (Binance Wallet)

# SecurityScorecard

- fhmfendgdocmcbmfikdcogofphimnkno (Sollet)
- fihkakfobkmkjojpchpfgcmhfjnmnfpi (BitApp Wallet)
- flpiciilemghbmfalicajoolhkkenfel (ICONex)
- fnjhmkhhmkbjkkabndcnnogagogbneec (Ronin Wallet)
- gaedmjdfmmahhbjefcbgaolhhanlaolb (Authy 2FA Authentication)
- hcflpincpppdclinealmandijcmnkbgn (KHC Wallet)
- hnfanknocfeofbddgcijnmhnfnkdnaad (Coinbase Wallet)
- hpglfhgfnhbgpjdenjgmdgoeiappafln (Guarda)
- ibnejdfjmmkpcnlpebklmnkoeoihofec (TronLink)
- ijmpgkjfkbfhoebgogflfebnmejmfbml (BitClip)
- ilgcnhelpchnceeipipijaljkblbcobl (GAuth Authenticator)
- imloifkgjagghnncjkhggdhalmcnfklk (Trezor Password Manager)
- infeboajgfhgbjpjbeppbkgnabfdkdaf (OneKey Legacy)
- jbdaocneiiinmjbjlgalhcelgbejmnid (Nifty Wallet)
- jojhfeoedkpkglbfimdfabpdfjaoolaf (Polymesh Wallet)
- kkpllkodjeloidieedojogacfhpaihoh (Enkrypt)
- klnaejjgbibmhlephnhpmaofohgkpgkd (ZilPay)
- kncchdigobghenbbaddojjnnaogfppfj (iWallet)
- kpfopkelmapcoipemfendmdcghnegimn (Liquality Wallet)
- lkcjlnjfpbikmcmbachjpdbijejflpcm (Steem Keychain)
- lodccjjbdhfakaekdiahmedfbieldgik (DappPlay)
- mnfifefkajgofkcjkemidiaecocnkjeh (TezBox)
- nanjmdknhkinifnkgdcggcfnhdaammmj (GuildWallet)
- nhnkbkgjikgcigadomkphalanndcapjk (CLV Wallet)
- nkbihfbeogaeaoehlefnkodbefgpgknn (MetaMask)
- nkddgncdjgjfcddamfgcmfnlhccnimig (Saturn Wallet)
- nknhiehlklippafakaeklbeglecifhad (Nabox Wallet)
- nlbmnnijcnlegkjjpcfjclmcfggfefdm (MEW CX)
- nlgbhdfgdhgbiamfdfmbikcdghidoadd (Byone)
- oeljdldpnmdbchonielidgobddffflal (EOS Authenticator)
- onofpnbbkehpmmoabgpcpmigafmmnjhl (Nash Extension)
- ookjlbkiijinhpmnjffcofjonbfbgaoc (Temple)

🔄 SecurityScorecard



The "Login Data" database containing login data such as usernames and passwords will also be exfiltrated by the stealer:



The malware organizes the database based on its name and the SQLite format:

004081AF         FF 74 24 08           004081AF         FF 74 24 08           004081AF         FF 74 24 08           004081B7         FF 74 24 08           002051B3         ES 59 1A 01 00           <	push dword ptr ss: [sp+1] push dword ptr ss: [sp+1] push dword ptr ss: [sp+1] push dword ptr ss: [sp+4] call malware.419CA9	csp+8         x875W_B 0         x875W_C3 0         x875W_C2 0           x875W_C1 0         x875W_C1 0         x875W_C2 0         x875W_C2 0           x875W_S5 0         x875W_S5 0         x875W_D 0         x875W_D 0           x875W_S5 0         x875W_D 0         x875W_D 0         0           y         Default (stdcall)         v 5 0         uhod           11:         [csp1 0129EF27C         c2:         [csp1 4]         020438C0 L"Chrome/Default/Login Data"
.MPRESS1:00408188 malware.exe:\$8188 #7388		3: [esp+8] 048E0060 "SQLite format 3" 4: [esp+C] 0000C000 5: [esp+10] 02D43BC0 L"Chrome/Default/Login Data
Dump 1         Dump 2         Dump 3         Dump 4           Address         Hex	Ump 5 😸 Watch 1 🛛 🖉 Struct	0019F264 0019FE70   0019FE70   0019FE80   020438C0 L "Chrome/Default/Login Data" 0019FC80   020438C0 L "Chrome/Default/Login Data" 0019FC84   048E0060   "SQLite format 3"

Multiple relevant strings are obfuscated by inserting the "edx765" string. An example of the decoding operation is displayed in figure 23.

	push malware, 452206 call malware, 424431	4522D6 > Default	:(stdcall) :sp] 004522D6 L"Logedx765in /	▼ 5 € Unlock Daedx765ta Foedx
.MPRESS1:004085DA malware.exe:\$85DA #77DA		3: e 4: e 5: e	sp+8] 00000000 sp+C] 00000000 sp+C] 7F0D2A3E	
am         am         am         am           Address         Hex         0.00         67.00         69.00         66.00         20.00         44.00           02D49960         040.00         06.00         67.00         69.00         66.00         20.00	ASCII 0.61.00 L.o.g.1.nD.a. 0.41.00 L.a. F.o.rA. 0.48 AB (.c. c.o. U., D. t	0039ECE0 004522D6 L"Loged	x765in Daedx765ta Foedx765r	Accedx765ount"

#### Figure 23

Another database called "Login Data For Account" is also targeted by the malware (see figure 24).

Image: Construction of the second s	00401050       52       put ebp Mede       put ebp Mede<	🕈 🗌 Unlock
## Dump 1         ## Dump 2         ## Dump 3         ## Dump 4         ## Dump 5         @ Watch 1         Ix=  Locals         > Struct         OD19F9F8         OO19F9F8         6667607E         OO19F9F8         6667607E         OO19F9F8         6667607E         OO19F9F8         6667607E         OO19F9F8         6667607E         OO19F9F8         6667607E         OO19F9F0         OO19F9F8         6667607E         OO19F9F0         OO19F9F0 <td>#Dump 2     ## Dump 3     ## Dump 4     ## Dump 5      ## Dump 5     ## Locals</td> <td>alware.0040</td>	#Dump 2     ## Dump 3     ## Dump 4     ## Dump 5      ## Dump 5     ## Locals	alware.0040

Figure 24

A Google Chrome database called "Web Data" will be exfiltrated as well:



The process opens and reads the Google Chrome cookies database, as highlighted below:

CONTRACT     CONTRACT	55         E5         F0           83         E4         F0           94         3E         L0         40         00         33         00           89         EC         SC         SC <td><pre>push ebp.esp and esp.FFFFFF0 call far 31:malware.40103E mov esp.ebp ret inc.eck push edx inc.eck push edx inc.eck push edx inc.eck push eck inc.eck push eck inc.eck push eck inc.eck push eck inc.eck push esp inc.eck push ebx inc.eck push ebx inc.eck inc.eck push ebx inc.eck inck inc.eck inc.eck inck inck in</pre></td> <td>ebx:G-</td> <td>LastError 00000000 (ERROR_SUCCESS) GS 0028 FS 0053 ES 0028 DS 0028 SS 0028 SS 0028 x87r0 00000000000000000000000000000000000</td>	<pre>push ebp.esp and esp.FFFFFF0 call far 31:malware.40103E mov esp.ebp ret inc.eck push edx inc.eck push edx inc.eck push edx inc.eck push eck inc.eck push eck inc.eck push eck inc.eck push eck inc.eck push esp inc.eck push ebx inc.eck push ebx inc.eck inc.eck push ebx inc.eck inck inc.eck inc.eck inck inck in</pre>	ebx:G-	LastError 00000000 (ERROR_SUCCESS) GS 0028 FS 0053 ES 0028 DS 0028 SS 0028 SS 0028 x87r0 00000000000000000000000000000000000
.MPRESS1:00401033 malware.	exe:\$1033 #233			4: [esp+10] 00428D46 malware.00428D46
Address         Hex           04910738         38         9C         F2         4F         62         D6           04910748         58         9C         F2         4F         62         D6           04910748         6F         00         72         00         58         00           04910758         69         00         65         00         73         00           04910768         00         00         00         00         00         00         00	Dump 3         ## Dump 4         ## Dum           09 18         4E 00 65 00         74 00 7           5C 00         43 00 6F 00 6F 00 6F         00 6F 00 6F           00 00 AB	p 5	00195920 FFFF 00195974 0000 00195976 6667 00195976 0019 00195A00 0001 00195A00 0000 00195A08 0000 00195A08 0000 00195A08 0000	FFFF 0008 607E FADC 18046 return to malware.00428D46 from malware.004 00055 90008 107C0

Figure 27

The local storage data can be found in the "Google\Chrome\User Data\Default\Local Storage\leveldb\" directory:



Figure 28

●         0040102D 0040102E ●         0040102D 0040102E           ●         0040103D 0040103C         0040103C           ●         0040103C         0040104C           ●         0040104C         0040104C           ●	55 89 E5 83 E4 F0 9A 3E 10 40 00 33 00 89 EC 50 C3 41 52 51 52 41 50 41 51 52 41 51 52 41 51 52 41 51 52 41 51 52 41 50 6 6 6 7 7 41 50 6 6 6 7 7 41 50 6 7 41 50 6 7 41 50 6 7 7 41 50 6 7 7 41 50 6 7 7 41 50 6 7 7 7 41 50 6 7 7 7 41 50 6 7 7 7 7 7 7 7 7 7 7 7 7 7	push ebp mov ebp,esp and esp,fFFFFF0 call far B3:malware.40103E mov esp,ebp pop ebp fee table function push ecx push ecx push ecx push ecx push ecx push ecx inc ecx push ecx inc ecx push ecx inc ecx push esp inc ecx push esp inc ecx push ebx inc ecx push ebx inc ecx push ebx inc ecx push esp inc ecx push esp	ebx:G-	LastError 00000000 (ERROR_SUCCESS) LastStatus 00000000 (STATUS_SUCCESS) GS 0028 FS 0053 ES 0028 DS 0028 CS 0023 <u>SS</u> 0028 X87r0 00000000000000000000000000000000000
The second			00195970 -0019	PEASO
Dump 1 Dump 2	Dump 3 👹 Dump 4 👹 Dump	5 😨 Watch 1 🛛 🕸 Locals 🎾 Struct	00195974 0042	28D46 return to malware.00428D46 from malware.004
Address Hex		ASCII	^ 0019F978 0000	00009
OT AD BA OD FO	AD BA OD FO AD BA OD FO AD	BA NOT TO TO TO TO TO	0019F980 0496	5D7F8

GetCurrentHwProfileA is utilized to obtain information about the current hardware profile (figure 30).

	FF DO	push esi call eax	eax:G	Default (stdcall)	▼ 5 \$ Unlock
eax= <advap132.getcurrenthwpr< td=""><td>ofileA&gt; (73A71D7</td><td>0)</td><td></td><td>1: [esp] 04975A30 2: [esp+4] 02C62198 3: [esp+8] 02D2B0E0 4: [esp+C] 00000000</td><td></td></advap132.getcurrenthwpr<>	ofileA> (73A71D7	0)		1: [esp] 04975A30 2: [esp+4] 02C62198 3: [esp+8] 02D2B0E0 4: [esp+C] 00000000	
MPRESSI:0041ASAS maiware.ex	C: \$1A5A5 #197A5		0019FE10 0497	5A30	

#### Figure 30

The data that will be exfiltrated contains the GUID string corresponding to the hardware profile, the "TRNGVa—stream" Lumma ID, and the targeted databases that were compressed:



Figure 31



WinHttpOpen is used to initialize the use of WinHTTP functions with the "TeslaBrowser/5.5" user agent (see figure 32).



#### Figure 32

The malicious binary performs a network connection to the "45.9.74.78" C2 server on port 80:

EIP	<ul> <li>0041B848</li> <li>0041B848</li> <li>0041B848</li> <li>0041B853</li> <li>0041B853</li> <li>0041B853</li> </ul>	6A 0 6A 5 F FF 7 FF 7 FF 7	0 5 08 5 C4 0		push 0 push 50 push dword p push dword p call eax	tr ss: ebp+ tr ss: ebp-	8] 3C]	 _	[ebp+: eax:W ~	x8 x8 x8 Defa	7SW_C1 0 7SW_SF 0 7SW_O 0	x875W_ x875W_ x875W_	CO 0 P 0 Z 0	x875W_E x875W_U x875W_D	<ul> <li>5</li> <li>0</li> <li>0</li> <li>0</li> </ul>	Unloc
eax= <winhtt< td=""><td>tp.WinHttpConr</td><td>nect&gt; (705</td><td>57110)</td><td></td><td></td><td></td><td></td><td></td><td></td><td>1: 2: 3: 4:</td><td>[esp] 0 [esp+4] [esp+8] [esp+C]</td><td>4D03788 004542D0 00000050 00000000</td><td>C L"4</td><td>5.9.74.78</td><td></td><td></td></winhtt<>	tp.WinHttpConr	nect> (705	57110)							1: 2: 3: 4:	[esp] 0 [esp+4] [esp+8] [esp+C]	4D03788 004542D0 00000050 00000000	C L"4	5.9.74.78		
.MPRESS1:00	J418855 malwar	e. exe: \$18	855 #1AD55													
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	💮 Watch 1	[x=] Locals	2 Struct	0019F	018 04D0 01C 0045	3788 42DC	L"45.9	.74.78"				
Address He	ex		~ ~ ~ ~ ~	00 00 00 00	ASCII			 0019F	0000	00050						

#### Figure 33

The WinHttpOpenRequest API is utilized to create an HTTP POST request to the "/c2sock" URI:

	88 40 88 83 EC 1C 0F 57 CO 9F 11 44 24 0C 88 55 0C 89 54 24 08 89 0C 24 C7 44 24 04 9C 42 45 00 FF 00 west> (70551440) xe:\$18893 #1AD93	<pre>mov ecx,dword ptr ss:[ebp-48] sub esp,iC xorps xmm0,xmm0 movups xmm0,rtr ss:[ebp+C] mov dword ptr ss:[ebp+C] mov dword ptr ss:[esp+6],edx mov dword ptr ss:[esp+6],edx mov dword ptr ss:[esp+6],edx mov dword ptr ss:[esp+6],edx</pre>	[ebp+i [esp+i [word eaxim ♥	x8/1w_0 5 (LmpLy)       x8/1w_/ 5 (LmpLy)         x875xL0.50000       x875w_C3 0 x875w_C2 0         x875w_0 0 x875w_C3 0 x875w_U 0       x875w_U 0         x875w_0 0 x875w_C 0 x875w_U 0       x875w_D 0         x875w_0 0 x875w_U 0 x875w_U 0       x875w_D 0         x875w_0 0 x875w_U 0 x875w_U 0       x875w_D 0         Default (stdcal)       ▼ 5 € _ Unicd         1:       [ssp] 02CAA0A8         1:       [ssp] 0453144 L''/C2Sock"         4:       [ssp-c]_00000000
💭 Dump 1 💭 Dump 2 💭 🕻	Dump 3 💭 Dump 4 💭 Dump 9	5 🛞 Watch 1 🛛 🕸 Locals 🖉 Struct	0019FD0C 02CA 0019FD10 0045	A0A8 429C L"POST"
Address         Hex           02C62130         40         00         00         00         00           02C62140         00         00         00         00         00         F0           02C62150         00         00         00         00         00         00         00	00 00 00 00 00 00 00 00 00 00 AD BA <u>98 FC C5 02</u> 0D FO AD 00 00 00 00 00 00 0D FO AD	ASCII 00 @	0019FD14 0045 0019FD18 0000 0019FD1C 0000 0019FD20 0000 0019FD24 0000	3144 L"/c2sock" 0000 0000 0000 0000

#### Figure 34

The stealer sets the time outs involved in the HTTP connections using WinHttpSetTimeouts (figure 35).

● 041882 041882 041882 041885 041885 89 0C 24 041885 89 0C 24 041885 89 0C 24 041885 89 0C 24	<pre>movaps xmm0,xmmvord ptr ds:[a48160] movups xmmvord ptr ss:[esp+4],xmm0 mov dhord ptr ss:[esp],ecx (a1) eax</pre>	0044E: eax:W	x875w_SF 0 x875w_P 0 x875w_U 0 x875w_O 0 x875w_Z 0 x875w_D 0 befault (stocal) ▼ 5 ⊡ Unlock
eax= <winhttp.winhttpsettimeouts> (7054D580)</winhttp.winhttpsettimeouts>			2: [esp+4] 000493E0 L"1-1-1"
.MPRESS1:0041BBC1 malware.exe:\$1BBC1 #1ADC1			3: [esp+8] 000493E0 L"1-1-1" 4: [esp+C] 000493E0 L"1-1-1"
💭 Dump 1 👹 Dump 2 👹 Dump 3 👹 Dump 4 👹 Dump 5	Watch 1  x=  Locals 2 Struct	19FD14 02 19FD18 00	CAA230 0493E0 L"1-1-1"
Address Hex	ASCII 001	19FD1C 00	0493E0 L"1-1-1"
000493E0 31 00 2D 00 31 00 2D 00 31 00 00 00 00 00 00 00	00 111	19FD24 00	00493E0 L"1-1-1"

#### Figure 35

The malware adds an HTTP request header via a function call to WinHttpAddRequestHeaders (0x20000000 = **WINHTTP\_ADDREQ\_FLAG\_ADD**):

ere-	<ul> <li>004188F6</li> <li>004188FB</li> <li>004188FE</li> <li>004188FE</li> <li>004188FE</li> <li>004185FE</li> <li>004185FE</li> </ul>	68 00 00 00 6A FF 56 FF 75 EC FF D0	20	push 2000000 push FFFFFFF push esi push dword pt call eax	tr ss:[ebp	-14]	esi: eax:		(87 SW_C (87 SW_S (87 SW_0 efault (st	1 0 F 0 dcall)	x87SW_C( x87SW_P x87SW_Z	0 0 0	x87SW_ES x87SW_U x87SW_D	0 0 0 5 🗘 Unloc
eax= <winht< td=""><td>041BC01 malwar</td><td>equestHeaders&gt; (70</td><td>052CE60)</td><td></td><td></td><td></td><td></td><td>234</td><td>: [esp : [esp : [esp</td><td>+4] 02 +8] FF +C] 20</td><td>CAASE0 FFFFFFF 0000000</td><td>L"Con</td><td>ntent-Type</td><td>: multipart/f</td></winht<>	041BC01 malwar	equestHeaders> (70	052CE60)					234	: [esp : [esp : [esp	+4] 02 +8] FF +C] 20	CAASE0 FFFFFFF 0000000	L"Con	ntent-Type	: multipart/f
Address   F	E Dump 2	Dump 3 🔛 Dump	4 💭 Dump 5	🛞 Watch 1 ASCII	[x=] Locals	Struct	 0019FD18 0019FD1C 0019FD20 0019FD24	02CAA2 02CAA5 FFFFFF	30 E0 L"C	onten	t-Type:	mult	ipart/form	n-data; bounda
02CAA5E0 4 02CAA5F0 5 02CAA600 6 02CAA600 6 02CAA620 6 02CAA630 6 02CAA630 6 02CAA640 3 02CAA650 3 02CAA650 3	III         0.0         GF         0.0         GE           .4         0.0         7.9         0.0         7.0           .6         0.0         7.4         0.0         6.9           .6         0.0         GF         0.0         7.2           .1         0.0         3.8         0.0         2.0           .1         0.0         7.2         0.0         7.9           .8         0.0         3.7         0.0         3.8           .8         0.0         3.7         0.0         3.1           .4         0.0         0.0         0.0         0.0	00         74         00         65         00         6E           00         65         00         3A         00         20           00         70         00         61         00         72           00         6D         00         2D         00         64           00         62         00         6E         00         75           00         3D         05         53         00         71           00         31         00         37         00         68           00         37         00         39         00         30	00         74         00         2D         00           00         6D         00         75         00           00         61         00         74         00           00         61         00         74         00           00         62         00         64         00           00         44         00         65         00           00         75         00         66         00           00         71         00         37         00	C.o.n.t.e.n T.y.p.e.: 1.t.i.p.a.r f.o.r.md a.;. b.o.u a.r.y.=.S.q 8.7.8.1.7.h 8.7.1.7.9.3	.t .m.u. .t./. .a.t. .n.d. .D.e. .u.f. .q.7.		D019FD28 D019FD2C D019FD30 D019FD34 D019FD38 D019FD3C D019FD40 D019FD44	E969C8 000000 010000 010100 000101 010100 0497FD 0497FD	1C 16 00 01 00 65 08 08					

WinHttpSendRequest is used to send the HTTP request to the C2 server, as highlighted in figure 37.

● 00413759 89 5C 24 18 00413750 88 7D 14 00413770 68 7C 24 14 00413774 0F 57 CO 00413777 0F 11 44 24 04 00413777 0F 11 44 24 04 00413777 FF DO	<pre>mov dword ptr ss:[esp+14] ebx mov edi dword ptr ss:[ebp-14] mov dword ptr ss:[esp+14],edi xorps xmmword ptr ss:[esp+4],xmm0 mov dword ptr ss:[esp],ecx call eax</pre>	eax:W Pef	87 StatusWord 0000 87 SW_B 0 x87 SW_C3 87 SW_C1 0 x87 SW_C0 87 SW_SF 0 x87 SW_P 87 SW_O 0 x87 SW_Z fault (stdcall)	0 x875w_C2 0 0 x875w_E5 0 0 x875w_U 0 0 x875w_D 0 • 10 unlock
<pre>ceax=<winhttp.winhttpsendrequest> (7053E1A0) .MPRESS1:0041877F malware.exe:\$1877F #1A97F</winhttp.winhttpsendrequest></pre>		> 1: 2: 3: 4:	[esp] 02CAA230 [esp+4] 00000000 [esp+8] 00000000 [esp+C] 00000000	
Image: Second state         Image: Second state	5	019FD0C 02CAA23 019FD10 0000000 019FD14 0000000 019FD18 0000000 019FD1C 0000000 019FD1C 0000000 019FD24 0000000	0 0 0 0 0 7 0	

#### Figure 37

The stolen information is exfiltrated by calling the WinHttpWriteData method:

<ul> <li>00418797</li> <li>FF 75 D0</li> <li>0041879A</li> <li>57</li> <li>00418798</li> <li>FF 75 10</li> <li>0041879E</li> <li>FF 75 EC</li> </ul>	push dword ptr ss: [ebp-30] push edi push dword ptr ss: [ebp+10] push dword ptr ss: [ebp-14]	x875W_C1         0         x875W_C0         0         x875W_E5         0           x875W_SF         0         x875W_P         0         x875W_U         0           x875W_O         0         x875W_Z         0         x875W_D         0
EIP 004187A1 FF D0	call eax eax:	Default (stdcall)
eax= <winhttp.winhttpwritedata> (7054D180) .MPRESS1:004187A1 malware.exe:\$187A1 #1A9A1</winhttp.winhttpwritedata>	· · · · · · · · · · · · · · · · · · ·	1: [esp] 02CAA30 2: [esp+4] 02C62198 3: [esp+8] 00041637 4: [esp+C]_0019FD28
Ump 1 Ump 2 Ump 3 Ump 4 Ump 5	Image: Watch 1         [x=] Locals         Image: Struct         Image: O019FD12         Image: O019FD12 </td <td>2CAA230 2C62198</td>	2CAA230 2C62198
Address Hex 02C62198 2D 2D 53 71 44 65 38 37 38 31 37 68 75 66 38 3	ASCII 0019FD20 0 0019FD24 0 0019FD24 0	0041637 0019FD28

#### Figure 38

The process waits to receive the response from the C2 server using the WinHttpReceiveResponse function:

EIP	• 0041B4D5 • 0041B4D7 • 0041B4DA	6A 00 FF 75 EC FF D0	push 0 push dword p call eax	tr ss:[ebp-14		eau	CI W ~	x87SW_0	0 x875w dcall)	_z (	) x875W_D	0
eax= <winht< td=""><td colspan="8">eax=<winhttp.winhttpreceiveresponse> (70557610) .MPRE5S1:004184DA malware.exe:\$184DA #1A6DA</winhttp.winhttpreceiveresponse></td><td>] 02CAA230 +4] 000000 +8] 000000 +C] 000000</td><td>00 00 16</td><td></td><td></td></winht<>	eax= <winhttp.winhttpreceiveresponse> (70557610) .MPRE5S1:004184DA malware.exe:\$184DA #1A6DA</winhttp.winhttpreceiveresponse>								] 02CAA230 +4] 000000 +8] 000000 +C] 000000	00 00 16		
Dump 1	💷 Dump 2 📖 I	Dump 3 🔛 Dump 4	📖 Dump 5 🛛 🍪 Watch 1	[x=] Locals	Struct	0019FD20 0019FD24	02CA	A230 0000				

#### Figure 39

Finally, the binary closes the HINTERNET handle using WinHttpCloseHandle:

	0041BSCD	FF 75 C4	push dword ptr ss:[ebp-3C]			
EIP	• 004188D0 <	FF DO	call eax	eax:w`	Default (stdcall)	▼ 5 🗘 Unlock
eax= <winhttp.< td=""><td>winHttpCloseHar</td><td>ndle&gt; (705338D0)</td><td></td><td></td><td>2: [esp+4] 00000000 3: [esp+8] 00000016</td><td></td></winhttp.<>	winHttpCloseHar	ndle> (705338D0)			2: [esp+4] 00000000 3: [esp+8] 00000016	
.MPRESS1:0041	BSDO malware.ex	<pre>ke:\$1B8D0 #1AAD0</pre>			4: [esp+C] 01000000	
in a second	mm_	- (II) - · · ·	am _ 00 (i)	0019FD24 040	03788	

Other browsers are also targeted (figure 41):

- Chromium
- Microsoft Edge
- Kometa
- Opera Stable
- Opera GX Stable
- Opera Neon
- Brave
- Comodo Dragon
- CocCoc Browser

	push ebp mov ebp,esp and esp,FFFFFF0 call far 39,malware.40103E mov esp,ebp pose pose push edx push esp push edx push esp push edx push edx push esp push edx push edx pus	CF 0 FF 1 FF 1 LastError 00000000 (ERROR_SUCCESS) LastError 0000007C (STATUS_MO_TOKEN) GS 0028 FS 0053 ES 0028 DS 0028 x87r0 00000000000000000 ST0 Empty 0.0000000 x87r2 000000000000000000 ST1 Empty 0.0000000 x87r2 0000000000000000000 ST2 Empty 0.0000000 x87r4 000000000000000000 ST3 Empty 0.0000000 x87r4 0000000000000000000 ST4 Empty 0.0000000 x87r4 00000000000000000000 ST5 Empty 0.0000000 x87r5 00000000000000000000 ST5 Empty 0.00000000 x87r6 00000000000000000000 ST5 Empty 0.00000000 x87r6 00000000000000000000 ST6 Empty 0.00000000 x87r6 0000000000000000000000 ST7 Empty 0.00000000 x87r6 0000000000000000000000 ST7 Empty 0.00000000 x87ragword FFFF x87Tm_3 3 (Empty) x87TM_3 3 (Empty) x87Tm_3 3 (Empty) x87TM_3 3 (Empty)
00441047 00401048 00401048 00401048 00401044 00401044 00401046 41 00401046 51 00401047 55 00401051 00401051 00401051 00401051 00401051 00401051 00401051 00401051 00401051 00401051 00401051 00401051 00401052 40 00401052 40 00401052 00000000000000000000000000000000000	Jush est inc ecx push est inc ecx push esp inc ecx push ebx dec ecx mov edx,0 dec ecx mov est,0 inc esp inc esp inc esp	AS7'€ 000000000000000000000000000000000000
.MPRESS1:00401033 malware.exe:\$1033 #233		4: [csp+10] 00428D46 malware.00428D46
### Dump 1         ### Dump 2         ### Dump 3         ### Dump 4         ### Dump 5           Address         Hex         00         90         02         00 <t< td=""><td>Wetch 1         Image: Amage and the ama</td><td>0000         0000000           000000008         00000008           00000008         0000008           0000008         0000008           0000008         0000008           0000008         0000008           0000008         0000008           000000000         0000000           00000000         0000000           00000000         0000000           00000000         0000000           9         91010000           9         9512301           00000005         3864470E           00197884         00197884</td></t<>	Wetch 1         Image: Amage and the ama	0000         0000000           000000008         00000008           00000008         0000008           0000008         0000008           0000008         0000008           0000008         0000008           0000008         0000008           000000000         0000000           00000000         0000000           00000000         0000000           00000000         0000000           9         91010000           9         9512301           00000005         3864470E           00197884         00197884

Figure 41

The stealer is looking for ".txt" files in the "C:\Users\<User>\" folder recursively:



Figure 42



Figure 43

The malware steals data from the following crypto wallets (see figure 44):

- Binance
- Electrum
- Ethereum
- Exodus
- Ledger Live
- Atomic
- Coinomi



0040102D         55           0040102D         89           0040102E         81           0040104E         85           0040104E         85           0040104E         85           0040104E         88           0040104E         88           0040104E         88           0040104E         88           0040104E         88           0040105E	push ebp mov ebp, esp and 40 00 33 00         push ebp and 40 00 33 00           10 40 00 33 00         mov esp, ebp pop ebp free ecc.         mov esp, ebp pop ebp free ecc.           11cs, eca.         mov esp, ebp pop ebp free ecc.         mov esp, ebp pop ebp free ecc.           11cs, eca.         mov esp, ebp push eck.         not push eck.           11cs, eca.         not push eck.         not push eck.           11cc, eca.         push eck.         not push eck.           11cc, eca.         push eck.         not push eck.           11cc, ecx.         push eck.         not push eck.           00 00 00 00         mov eck.         not mov eck.           10         mov eck.         not push eck.	d ptr ss:[ebp+10]	ebx:C	LastError 00000000 (ERROR_SUCCESS) LastStatus C00007C (STATUS_NO_TOKEN) 65 0028 F5 0053 E5 0028 D5 0028 X8770 000000000000000000 5T0 Empty 0.00000000 X8772 000000000000000000 5T1 Empty 0.00000000 X8772 000000000000000000 5T1 Empty 0.00000000 X8774 000000000000000000 5T1 Empty 0.00000000 X8774 0000000000000000000 5T1 Empty 0.00000000 X8774 00000000000000000000000000000000000
0033:0040103E=0				2: [esp+8] 00000055
				4: [esp+10] 05489668
.MPRESS1:00401033 malware.exe:\$1033	#233			
Image         Image <th< td=""><td>Dump 4         Ump 5         Watch 1           ASCII           00         <t< td=""><td>Itellocals         Struct         COLDEd 0013F4           0013F4         0013F4           0013F4         0013F4</td><td>80         0019           584         00421           585         00401           586         00401           587         00401           590         0548           594         8664           595         8664           596         00001           5A0         0548           594         8664           595         8664           596         00001           5A3         01011           5A4         00001           5A5         01019           5A6         0119           5B6         0019           5B7         0019           5C4         00000           5C4         00000           5C4         00019           5C4         00000           5C4         00000           5C5         00000</td><td>7760 8046 return to malware.00428046 from malware.004 8046 8046 8047 8048 8049 8049 8049 8049 8049 8049 8049</td></t<></td></th<>	Dump 4         Ump 5         Watch 1           ASCII           00 <t< td=""><td>Itellocals         Struct         COLDEd 0013F4           0013F4         0013F4           0013F4         0013F4</td><td>80         0019           584         00421           585         00401           586         00401           587         00401           590         0548           594         8664           595         8664           596         00001           5A0         0548           594         8664           595         8664           596         00001           5A3         01011           5A4         00001           5A5         01019           5A6         0119           5B6         0019           5B7         0019           5C4         00000           5C4         00000           5C4         00019           5C4         00000           5C4         00000           5C5         00000</td><td>7760 8046 return to malware.00428046 from malware.004 8046 8046 8047 8048 8049 8049 8049 8049 8049 8049 8049</td></t<>	Itellocals         Struct         COLDEd 0013F4           0013F4         0013F4           0013F4         0013F4	80         0019           584         00421           585         00401           586         00401           587         00401           590         0548           594         8664           595         8664           596         00001           5A0         0548           594         8664           595         8664           596         00001           5A3         01011           5A4         00001           5A5         01019           5A6         0119           5B6         0019           5B7         0019           5C4         00000           5C4         00000           5C4         00019           5C4         00000           5C4         00000           5C5         00000	7760 8046 return to malware.00428046 from malware.004 8046 8046 8047 8048 8049 8049 8049 8049 8049 8049 8049

The text files are compressed and exfiltrated using the same approach as before:

Address	He	ĸ			-								-				ASCII
055840F0	34	0D	0A	43	6F	6E	74	65	6E	74	2D	44	69	73	70	6F	4Content-Dispo
05584100	73	69	74	69	6F	6E	ЗA	20	66	6F	72	6D	2D	64	61	74	sition: form-dat
05584110	61	3B	20	6E	61	6D	65	3D	22	6C	69	64	22	0D	0A	0D	a; name="lid"
05584120	0A	54	52	4E	47	56	61	2D	2D	73	74	72	65	61	6D	0D	.TRNGVastream.
05584130	0A	2D	2D	53	71	44	65	38	37	38	31	37	68	75	66	38	SqDe87817huf8
05584140	37	31	37	39	33	71	37	34	0D	0A	43	6F	6E	74	65	6E	71793q74Conten
05584150	74	2D	44	69	73	70	6F	73	69	74	69	6F	6E	3A	20	66	t-Disposition: f
05584160	6F	72	6D	2D	64	61	74	61	3B	20	6E	61	GD	65	3D	22	orm-data; name="
05584170	66	69	6C	65	22	3B	20	66	69	6C	65	6E	61	6D	65	3D	file"; filename=
05584180	22	66	69	6C	65	22	0D	0A	43	6F	6E	74	65	6E	74	2D	"file"Content-
05584190	54	79	70	65	3A	20	61	74	74	61	63	68	6D	65	6E	74	Type: attachment
055841A0	2F	78	2D	6F	62	6A	65	63	74	0D	0A	0D	0A	50	4B	03	/x-objectPK.
055841B0	04	14	00	08	08	08	00	C5	3B	70	56	00	00	00	00	00	Â; pV
055841C0	00	00	00	00	00	00	00	27	00	04	00	49	6D	70	6F	72	Impor
055841D0	74	61	6E	74	20	46	69	6C	65	73	2F	50	72	6F	66	69	tant Files/Profi
055841E0	6C	65	2F	44	65	73	6B	74	6F	70	2F	62	6C	61	2E	74	le/Desktop/bla.t
055841F0	78	74	01	00	00	00	55	93	39	8E	1D	31	OC	44	73	03	xtU.91.Ds.
05584200	BE	C3	60	52	27	6A	AD	AD	CO	37	F9	89	D6	1B	18	F8	"A R'jA7ù.ÖØ
05584210	C7	F7	AB	61	OF	06	0A	88	A6	48	16	97	22	BB	FF	DB	C÷«a'H"»ÿÛ

# Figure 45

The stealer searches for ".conf" files in the AnyDesk directory:

00401022     00401022     00401022     00401022     00401022     00401022     00401022     00401022     00401032     00401032     00401032     00401032     00401041     00401041     00401041     00401043     00401044     00401044     00401044     00401044     00401044     00401044     00401044     00401044     00401045     00401045     00401045     00401045     00401051     0040105     004005     004005     0040105     0040105     0040105     0040105	55         63         E4         F0           94         3E         10         40         00         33         00           89         EC         50         52         52         52         52         52         52         52         52         52         51         52         51         52         51         52         51         52         51         52         51         52         51         52         51         52         51         52         51         51         52         51         51         52         51         51         51         51         51         51         53         54         55         54         55         55         55         55         55         55         55         55         52         52         52         52         52         54         55         54         55         54         55         54         55         54         55 <td>push ebp mov ebp.esp and esp.FFFFFF0 call far 33:malware.40103E mov esp.ebp pop ebp rec eck push eck push eck push eck push eck push eck push eck push eck push eck push esi inc eck push esi inc eck push ebp dec eck mov edx,0 dec eck mov esi,0 inc esp mov edx,dword ptr ss:[ebp+10] inc eck</td> <td>ebx: C</td> <td>LastStatus 0000000 (ERROR_SUCCESS) LastStatus 0000007 (STATUS_NO_TOKEN) GS 0028 FS 0053 ES 0028 DS 0028 CS 0028 SS 0028 x87r0 00000000000000000000000000000000000</td>	push ebp mov ebp.esp and esp.FFFFFF0 call far 33:malware.40103E mov esp.ebp pop ebp rec eck push eck push eck push eck push eck push eck push eck push eck push eck push esi inc eck push esi inc eck push ebp dec eck mov edx,0 dec eck mov esi,0 inc esp mov edx,dword ptr ss:[ebp+10] inc eck	ebx: C	LastStatus 0000000 (ERROR_SUCCESS) LastStatus 0000007 (STATUS_NO_TOKEN) GS 0028 FS 0053 ES 0028 DS 0028 CS 0028 SS 0028 x87r0 00000000000000000000000000000000000
0033:0040103E=0				1: [esp+4] 00428D46 malware.00428D46 2: [esp+8] 00000055
				3: [esp+C] 0000000B
.MPRESS1:00401033 malware.	exe:\$1033 #233			4: [esp+10] 04D1B5A0
Sill Dumo 1 Sill Dumo 2	0	n Martin Indiana () chart	0019F680 001	9F760
ere Dump 1 ere Dump 2 ere	Dump 5 8-8 Dump 4 8-9 Dum	p 5 Watch 1 M-1LOCals 2 Struct	0019F684 004	2BD46 return to malware.0042BD46 from malware.00
Address   Hex	55 00 72 00 65 00 72 00 73	ASCII	^ 0019F68C 000	0000B
04D18370 5C 00	SC 00 41 00 70 00 70	00 \	0019F690 04D	185A0
04D1B380 44 00 61 00 74 00	61 00 5C 00 52 00 6F 00 61	00 D.a.t.a.\.R.o.a.	0019F698 866	43AF9
04D18390 60 00 69 00 6E 00 04D183A0 44 00 65 00 73 00	67 00 SC 00 41 00 6E 00 75 6B 00 00 00 00 00 00 00 00 00	00 D.e.s.k	0019F69C 000	0000A
			- 00195510 040	TPE AD

The "recentservers.xml" and "sitemanager.xml" files found in the FileZilla directory will also be exfiltrated:

	push ebp mov ebp,esp and esp,FFFFFFO call far 35:malware.40103E mov esp,ebp pop ebp fee eex push edx push edx push edx inc ecx push eax inc ecx push esx inc ecx push esi	CF 0 FF 1 FF 1 LastError 0000000 (ERROR_SUCCESS) LastError 0000007C (STATUS_NO_TOKEN) GS 0028 FS 0053 ES 0028 DS 0028 X87r0 00000000000000000 ST0 Empty 0.0000000 X87r1 00000000000000000 ST1 Empty 0.0000000 X87r1 000000000000000000 ST1 Empty 0.0000000 X87r4 000000000000000000 ST1 Empty 0.0000000 X87r4 000000000000000000 ST2 Empty 0.0000000 X87r6 0000000000000000000 ST5 Empty 0.0000000 X87r6 0000000000000000000 ST6 Empty 0.0000000 X87r6 00000000000000000000 ST7 Empty 0.0000000
• 00401049 57 • 0040104A 41 • 0040104B 54 • 0040104C 41 • 0040104C 41 • 0040104C 51 • 0040104F 55 • 0040105F 49 • 00401057 49 • 00401057 49 • 00401058 C7 C6 00 00 00 • 00401058 44 • 00401035F 48 55 10 • 00401035F 48 55 10 • 00401035F 48 55 10 • 00401035F 48 55 10	push edi inc ecx push esp nuch ecx push ebp dec ecx mov edx,0 dec ecx mov edx,dword ptr ss:[ebp+10] inc esp	x87TagWord FFFF x87Tw_0 3 (Empty) x87Tw_1 3 (Empty) x87Tw_2 3 (Empty) x87Tw_3 3 (Empty) x87Tw_4 3 (Empty) x87Tw_5 3 (Empty) x87Tw_6 3 (Empty) x87Tw_5 3 (Empty) x87StatusWord 0000 x87Sw_5 0 x87Sw_C 0 x87Sw_C 0 x87Sw_5 0 x87Sw_C 0 x87Sw_U 0 befault (stdcal) Default (stdcal) ↓ 5 © Unloc
0033:0040103E=0 .MPRES51:00401033 malware.exe:\$1033 #233		2: [esp+8] 0000005 3: [esp+6] 0000005 4: [esp+10] 04CAB3E8
Image: Second system         Image: Se	Watch 1         Ix=ILocals         Struct         ODISIGS           ASCII         0019765         0019765         0019765           Q.C.:.U.S.e.r.S.         0019765         0019765         0019765           Q.A.T.A.R.o.A.         0019765         0019765         0019765           D.A.T.A.R.o.A.         0019765         0019765         0019765           D.A.T.A.R.o.A.         0019765         0019765         0019765	01-0019750 4 00428046 return to malware.00428046 from malware.00- 8 00000055 0 04CA8328 0 04CA8328 8 86643479 8 86643479 0 04CA8328 0 04CA8328

# Figure 47

The malicious binary searches for KeePass files (\*.kbdx) in the user profile directory. It locates the Steam folder and detects the "ssfn\*" files, as shown in the figure below.

0040102D     0040102E     0040102E     00401030     002000EE     0040103A	55 89 E5 83 E4 F0 9A 3E 10 40 00 33 00 89 EC	push ebp mov ebp,esp and esp,FFFFFFF call far 33:malware.40103E mov esp.ebp	LastError 00000000 (ERROR_SUCCESS) LastStatus C000007C (STATUS_NO_TOKEN)
0040103C 0040103D 0040103F 0040103F 0040103F 00401041 00401041 00401041 00401041 00401041 00401041 00401041 00401048 00401058 00401058 00401058 00400057 00000057 00000057 000000000000	00         CC           C3         41           52         51           52         51           51         51           41         51           41         51           52         51           53         51           54         53           53         54           55         44           55         40           67         62         00         00         00           67         65         10         44         88         55         10           44         44         44         44         44         44         44         45         44         45         44         44         44         44         45         44         44         44         44         44         44         44         44         44         44         45         44         44         44         45         44         45         45         44         44         45         45         45         45         45         45         45         45         45         45         45         45         45         46 <t< td=""><td><pre>mode cb; cbp mode cb; cbp fret ex push ecx push ecx push ecx push ecx push ecx push ecx push ecx push ecx push esi inc ecx push edx inc ecx inc ecx</pre></td><td>ebx:c GS 0028 FS 0053 ES 0028 DS 0028 CS 0023 <u>SS</u> 0028 x87r0 000000000000000000 ST0 Empty 0.00000 x87r1 000000000000000000 ST1 Empty 0.00000 x87r3 0000000000000000000 ST1 Empty 0.00000 x87r4 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87r5 0000000000000000000 ST5 Empty 0.00000 x87r5 0000000000000000000 ST5 Empty 0.00000 x87r4 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87TagWord FFFF x87Tw_0 3 (Empty) x87Tw_1 3 (Empty) x87Tx_4 3 (Empty) x87Tw_1 3 (Empty) x87Tx_6 0 0x87Sw_C1 0 x87Sw_C2 0 x87Sw_S1 0 x87Sw_C2 0 x87Sw_S2 0 x87Sw_S 0 x87Sw_P 0 x87Sw_L2 0 x87Sw_S 0 x87Sw_P 0 x87Sw_L0 x87Sw_S1 0 x87Sw_S1 0 x87Sw_S1 0</td></t<>	<pre>mode cb; cbp mode cb; cbp fret ex push ecx push ecx push ecx push ecx push ecx push ecx push ecx push ecx push esi inc ecx push edx inc ecx inc ecx</pre>	ebx:c GS 0028 FS 0053 ES 0028 DS 0028 CS 0023 <u>SS</u> 0028 x87r0 000000000000000000 ST0 Empty 0.00000 x87r1 000000000000000000 ST1 Empty 0.00000 x87r3 0000000000000000000 ST1 Empty 0.00000 x87r4 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87r5 0000000000000000000 ST5 Empty 0.00000 x87r5 0000000000000000000 ST5 Empty 0.00000 x87r4 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87r5 000000000000000000 ST5 Empty 0.00000 x87TagWord FFFF x87Tw_0 3 (Empty) x87Tw_1 3 (Empty) x87Tx_4 3 (Empty) x87Tw_1 3 (Empty) x87Tx_6 0 0x87Sw_C1 0 x87Sw_C2 0 x87Sw_S1 0 x87Sw_C2 0 x87Sw_S2 0 x87Sw_S 0 x87Sw_P 0 x87Sw_L2 0 x87Sw_S 0 x87Sw_P 0 x87Sw_L0 x87Sw_S1 0 x87Sw_S1 0 x87Sw_S1 0
0033:0040103E=0			1: [csp+4] 00428D46 malware.00428D46 2: [csp+4] 00000055 3: [csp+c] 00000008
.MPRESS1:00401033 malware.	exe:\$1033 #233		4: [esp+10] 05915C30
Image         Dump 1         Image         Dump 2         Image           Address         Hex         00000         00000         00000         00000         00000         00000         00000         00000         00000         00000         00000         00000         00000         0000000         000000         000000         000000         000000         000000         000000         000000         00000000         00000000         000000000         00000000         000000000         0000000000         000000000000000000000000000000000000	Dump 3         ∰ Dump 4         ∰ Dum           AD         BA         00	p 5         Image: Second	00195630         00197560           00197631         0028046           return to malware.00428046         from malware.           00197632         0000005           00197635         0000005           00197634         0000005           00197635         0000005           00197634         0000005           00197634         0000005           00197634         0000005           00197634         0000000           00197634         0000000           00197634         0000000           00197634         0000005           00197635         0000005           00197636         00197728           00197636         00197728           00197637         00197728           00197645         00197728           00197645         00197728           00197645         00197728           00197647         00197728           00197647         00197728           00197647         00197728           00197748         00197728           00197647         00197728

The process steals "\*s" files from Telegram Desktop:

Overvices         Observe of the serve
Std
0040133         89 EC         mov esp, ebp           0040133C         5D         pop ebp           0040133C         5D         pop ebp           0040133C         5D         pop ebp           0040133C         51         push ecx           00401031C         51         push ecx           00401032         51         push ecx           00401034         51         push ecx           00401034         51         push ecx           00401044         11c ecx         x87r0 00000000000000000000000000000000000
<ul> <li>             0040103C 0040103D 0040103D 0040103E 0040103E 0040103F 0040104D</li></ul>
004401392       C3       FEE         00401035       41       pin dxi         00401035       10       pin dxi         00401035       10       pin dxi         00401035       11       pin dxi         00401041       52       push dxi         00401042       11       inc ecx         00401043       50       push ecx         00401044       11       inc ecx         00401045       51       push ecx         00401046       41       inc ecx         00401046       54       push ecx         00401046       54       push ecx         00401046       54       push ecx         00401046       54       push ecx         00401047       54       push ecx         00401048       54       push ecx         00401046       53       push ecx         00401046       54       push ecx      <
00401036       41       Int etx       CS 0023 SS 0028         00401036       51       push etx       CS 0023 SS 0028         00401041       51       push etx       CS 0023 SS 0028         00401042       1nc etx       ST 0 0000000000000000000000000000000000
00401040         \$1         push eck           00401041         \$2         push eck           00401041         \$2         push eck           00401042         1nc ecx         \$770 0000000000000000000000000000000000
© 00401041         52         push edx         x8770         000000000000000000000000000000000000
<ul> <li>             00401042             41             (nc eck             00401043             50             00401043             50             00401044             41</li></ul>
<ul> <li>             00401043             50             00401044             41</li></ul>
00401044       41       Inc ecx       X87.5 000000000000000000000000000000000000
00401045       51       publick       x87r5       000000000000000000000000000000000000
00401047         56         push esi           00401048         1         inc ecx           00401048         1         inc ecx           00401049         57         push edi           00401044         1         inc ecx           00401045         41         inc ecx           00401046         41         inc ecx           00401046         53         push esp           00401046         53         push ebx           00401046         53         push ebx           00401047         55         push ebx           00401047         53         push ebx           00401047         54         inc ecx           00401048         54         push ebx           00401047         55         push ebp           00401047         55         push ebp           00401047         55         push ebp           00401049         54         cmpty)           00401049         55         push ebp           00401049         56         push ebp           00401049         57         push ebp           00401049         56         push ebp           00401049         57
<ul> <li>00401048</li> <li>41</li> <li>1nc ecx</li> <li>00401049</li> <li>57</li> <li>push edi</li> <li>00401044</li> <li>41</li> <li>1nc ecx</li> <li>00401048</li> <li>44</li> <li>1nc ecx</li> <li>00401046</li> <li>41</li> <li>1nc ecx</li> <li>00401046</li> <li>42</li> <li>1nc ecx</li> <li>00401046</li> <li>43</li> <li>1nc ecx</li> <li>1nc</li></ul>
0 00401049     57     push edi       0 00401043     11     inc ecx       0 00401045     54     push esp       0 00401046     11     inc ecx       0 00401046     53     push ebx       0 00401046     51     inc ecx       0 00401046     51     push ebp       0 00401046     53     push ebp       0 00401046     53     push ebp       0 00401046     54     inc ecx       0 00401046     55     push ebp       0 00401046     57     20 00 00 00       0 00401047     57     20 00 00 00       0 00401047     57     00 00 00
O040104A 41 1nc ecx     O040104B 54 push esp     O040104C 41 1nc ecx     O040104C 41 1nc ecx     O040104C 41 1nc ecx     O040104C 41 1nc ecx     O040104F 55 push ebp     O040104F 55 push ebp     O0401051 57 C2 C2 00 00 00 00 mov efx 0
00401045     54     push esp       0040104C     41     inc ecx       0040104C     53     push ebx       0040104C     55     push ebx       0040104C     55     push ebx       0040104C     55     push ebx       0040104C     55     push ebp       00401051     55     push ebp       00401051     57 C 20 00 00 00     00 000
00401040     53     push ebx     ebx: (     x87Tw_2 3 (Empty) x87Tw_3 3 (Empty)       00401040     53     push ebx     ebx: (     x87Tw_2 3 (Empty) x87Tw_3 3 (Empty)       0040104F     55     push ebp     x87Tw_4 3 (Empty) x87Tw_5 3 (Empty)       00401051     57     push ebp     x87Tw_6 3 (Empty) x87Tw_7 3 (Empty)
O040104E 41 inc eck     O040104F 55 push ebp     O0401051 57 C2 C2 00 00 00 00     O0401051 57 C2 C2 00 00 00 00     O0401051 57 C2 C2 00 00 00 00     O0 00 00 00     O00000     O00000     O00000     O00000     O00000     O0000     O000     O0000     O000     O0000     O000     O000     O000     O000     O000     O000     O000
0040104F 55 push ebp x87Tw_6 3 (Empty) x87Tw_7 3 (Empty)     00401050 49 dec ecx     00401051 C7 C2 00 00 00 mov dv 0     x87Tw 0 000     x87Tw 0 000
00401050 49 dec ecx     x87StatusWord 0000     x87StatusWord 0000
00401057 49 00 00 00 00 00 00 00 00 00 00 00 00 00
(0040105E 44 inc esp     (0040105E 44 inc esp
0040105F 88 55 10 mov edx,dword ptr ss:[ebp+10]
• 00401062 44 inc esp
● d Default (stdcall)
1: [csp+4] 00428D46 malware.00428D46
2: [esp+8] 00000055
3: [espt.] 000008
.MPRESS1:00401033 malware.exe:\$1033 #233
The Dump 1 The Dump 2 The Dump 3 The Dump 5 The Dump 5 Struct D019F660 D019F600 D019F600 D019F600 D019F600 D019F600 D019F600 D019F600 D019
Address Hex ASCII 0019568 00000055
05508C40 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 C.:.\U.s.e.r.s.
05508C50 5C 00 1 00 70 00 1 00 70 00 1 00 70 00 1 00 70 00 1 0 0 00 70 00 1 0 0 0 0
0550870 60 01 47 00 61 00 12 00 12 00 12 00 67 00 52 00 167 00 61 00 10 10 0 10 0 10 0 0 10 0 0 0 0
05508c80 65 00 67 00 72 00 61 00 60 00 20 00 44 00 65 00 e.g.r.a.mD.e.

# Figure 49

The binary steals Mozilla Firefox passwords, and the "key4.db" database found in the Profiles directory:

	55 89 E5 83 E4 F0 94 3E 10 40 00 33 00 89 EC 53 53 54 51 52 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 51 52 57 57 57 57 57 57 57 57 57 57	push ebp mov ebp.esp and esp.FFFFFF0 call far Brimalware.40103E mov esp.ebp peter inc ecx push edx push edx inc ecx push edx inc ecx push ecx inc ecx push esi inc ecx push exi inc ecx push exi inc ecx push esi inc ecx push exi inc exi push exi inc exi inc esp inc exi inc esp	ebx: C	LastError 00000000 (ERROR_SUCCESS) LastError 00000000 (ERROR_SUCCESS) LastError 00000000 (STATUS_NO_TOKEN) GS 0028 FS 0058 CS 0023 <u>SS</u> 0028 K370 00000000000000000000 ST0 Empty 0.00000000 K877 00000000000000000000 ST2 Empty 0.00000000 K877 0000000000000000000 ST2 Empty 0.00000000 K877 00000000000000000000 ST2 Empty 0.00000000 K877 00000000000000000000 ST2 Empty 0.00000000 K877 0000000000000000000 ST3 Empty 0.00000000 K877 0000000000000000000 ST3 Empty 0.00000000 K877 00000000000000000000 ST3 Empty 0.00000000 K877 0000000000000000000 ST3 Empty 0.00000000 K877 0000000000000000000 ST3 Empty 0.00000000 K877 000000000000000000000 ST3 Empty 0.00000000 K877 00000000000000000000 ST3 Empty 0.00000000 K877 00000000000000000000 ST3 Empty 0.00000000 K877 000000000000000000000 ST3 Empty 0.00000000 K877 000000000000000000000 ST3 Empty 0.00000000 K877 000000000000000000000 ST3 Empty 0.00000000 K877 0000000000000000000000 ST3 Empty 0.00000000 K877 0000000000000000000000 ST3 Empty 0.00000000 K875 0.00000000000000000000000 ST3 Empty 0.00000000 K875 0.000000000000000000000 ST3 Empty 0.00000000 K875 0.000000000000000000000000000 ST3 Empty 0.00000000 K875 0.0000000000000000000000000000000000 ST3 Empty 0.00000000 K875 0.00000000000000000000000000000000000
Etti Dumo 1 Etti Dumo 2 Etti	Dumo 2 Dumo 4 Dumo	E Match 1 [Vallacale 9 Struct	0019F7F0 0000	0000B
address         Hex           0551ADF8         30         9C         F2         443         F         6           0551ABF8         30         9C         F2         443         F         6           0551ABF8         64         00         61         00         74         00         05         51AE18         72         00         65         00         56         00         05         143         76         00         55         00         56         00         05         142         10 <t< td=""><td>3A         1A         25         00         61         00         70         00         70           51         00         25         00         52         00         52         00         60         00         60         00         60         66         00         61         00         50         00         62         00         61         00         50         00         50         00         25         00         50         00         73         00         00         00         AB           60         00         55         00         73         00         00         00         AB</td><td>ASCII 45000 2 100000 2 10000 2 10000 2 100000 2 100000 2 100000 2 100000 2 100000 2 100000 2 100000000</td><td>0019F7F4 6667 0019F7F6 00012 0019F7FC 0042 0019F804 0000 0019F804 0000 0019F808 0551 0019F808 0551</td><td>7607E 9F08 18046 from malware.00428D46 from malware.004 30055 30008 18840 32599</td></t<>	3A         1A         25         00         61         00         70         00         70           51         00         25         00         52         00         52         00         60         00         60         00         60         66         00         61         00         50         00         62         00         61         00         50         00         50         00         25         00         50         00         73         00         00         00         AB           60         00         55         00         73         00         00         00         AB	ASCII 45000 2 100000 2 10000 2 10000 2 100000 2 100000 2 100000 2 100000 2 100000 2 100000 2 100000000	0019F7F4 6667 0019F7F6 00012 0019F7FC 0042 0019F804 0000 0019F804 0000 0019F808 0551 0019F808 0551	7607E 9F08 18046 from malware.00428D46 from malware.004 30055 30008 18840 32599

The width and height of the screen of the primary display monitor are retrieved using GetSystemMetrics (0x0 = **SM\_CXSCREEN**, 0x1 = **SM\_CYSCREEN**):

eax= <user32.getsystemmetrics> (750 .MPRESS1:0042CC3B ma]ware.exe:\$200</user32.getsystemmetrics>	000000) 238 #28638	eaxis	Default (stdcall)         ▼         \$         ↓         Image: Construction of the state
	amM	. 6)	000000
		Figure 51	
0042CC4D 57 0042CC4E FF DC	push edi call eax	eaxit	Default (stdcall)
<pre>eax=<user32.getsystemmetrics> (75D .MPRESS1:0042CC4E malware.exe:\$2CC</user32.getsystemmetrics></pre>	08000) 4E #28E4E		1: [esp] 00000001 2: [esp+4] 02C50000 3: [esp+8] 7701FA0D ntdll.7701FA0D 4: [esp+C] 0551B0C8
	am am 20	. @) 0019F8DC 000	00001

## Figure 52

GetComputerNameA is utilized to extract the NetBIOS name of the local machine (see figure 53).

570	<ul> <li>0042CD42</li> <li>0042CD45</li> </ul>	FF 70	6 2C	push dword ptr push edi	ds:[esi+2	2C]			x83	SW_SF 0	x875W_P	1 x87SW_U	0
	<	FF DI		carr eax				>	Defa	ult (stdcall) [esp] 05	537A70	•	5 🗘 🗌 Unlock
eax= <kernel32.getcomputernamea> (76AA4280)</kernel32.getcomputernamea>								2: 3: 4:	[esp+4] [esp+8] [esp+C]	0019FDA4 02C50000 7701FA0D 1	ntdll.7701FA0D		
.MPRESS1:00	42CD46 maiware.	exe: \$2CL	046 #28F46										
Dump 1	Dump 2	Dump 3	Dump 4	Dump 5 💮 Watch 1	[x=] Locals	3 Struct	0019F8	D8 0553 DC 0019	B7A70 DFDA4				

#### Figure 53

The sample also obtains the username associated with the current thread:

EIP	● 0042CDA ● 0042CDA ● 0042CDA ● 0042CDA	B FF 76 57 F FF DO	30	P	ush dword p ush edi all eax	tr ds:[esi+	30]	eax:@	V Defa	7SW_SF 0 x875W_F	1 x875₩_U 0	Unlock
eax= <advapi32.getusernamea> (73A62CFO)         2           .MPRESS1:0042CDAF malware.exe:\$2CDAF #2BFAF         3</advapi32.getusernamea>							2: 3: 4:	[esp] 0553FA88 [esp+4] 0019FDA0 [esp+8] 02C50000 [esp+C] 7701FA0D	ntdll.7701FAOD			
Dump 1	Dump 2	Dump 3	🚛 Dump 4	Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	0019FBD8 05 0019FBDC 00	53FA88 19FDA0	3		

The malware retrieves the system default language by calling the GetSystemDefaultLocaleName API:

	<pre>0042D141 0042D142</pre>	53 57		oush ebx oush edi					×8	SW_SF 0	x875W_P	1 x875W_	U	
EIP	00420148	FF DO		call eax				eax: ¢	Defa	ult (stdcall)	519440		- 5	🗢 🗌 Unlod
eax= <kernel< th=""><th colspan="6">eax=<kernel32.getsystemdefaultlocalename> (76A77110) .MPRESS1:0042D143 malware.exe:\$2D143 #2C343</kernel32.getsystemdefaultlocalename></th><th></th><th>2: 3: 4:</th><th>[esp+4] [esp+8] [esp+C]</th><th>00000055 02C50000 7701FA0D</th><th>ntdll.7701FA</th><th>OD</th><th></th></kernel<>	eax= <kernel32.getsystemdefaultlocalename> (76A77110) .MPRESS1:0042D143 malware.exe:\$2D143 #2C343</kernel32.getsystemdefaultlocalename>							2: 3: 4:	[esp+4] [esp+8] [esp+C]	00000055 02C50000 7701FA0D	ntdll.7701FA	OD		
Dump 1	Dump 2	Dump 3 💭 Dum	np 4 📖 Dump 5	🛞 Watch 1	[x=] Locals	2 Struct	00195	055 000	19440	?				

#### Figure 55

The cpuid instruction is used to extract the processor name and type, as displayed in figure 56.

0042D1BB	B8 02 00 00 80	mov eax.80000002
0042D1C0	31 C9	xor ecx.ecx
ETP 0042D1C2	OF A2	COUSE
0042D1C4	89 07	mov dword ptr ds:[edi].eax
0042D1C6	89 5F 04	mov dword ptr ds:[edi+4].ebx
0042D1C9	89 4F 08	mov dword ptr ds:[edi+8].ecx
0042D1CC	89 57 OC	mov dword ptr ds:[edi+C].edx
0042D1CF	B8 03 00 00 80	mov eax.80000003
0042D1D4	B9 00 00 00 00	mov ecx.0
0042D1D9	OF A2	EDUSC .
0042D1DB	89 47 10	mov dword ptr ds:[edi+10].eax
0042D1DE	89 5F 14	mov dword ptr ds:[edi+14].ebx
0042D1E1	89 4F 18	mov dword ptr ds:[edi+18].ecx
0042D1E4	89 57 1C	mov dword ptr ds:[edi+1C].edx
0042D1E7	B8 04 00 00 80	mov eax.80000004
0042D1EC	31 C9	xor ecx.ecx
0042D1EE	OF A2	
0042D1F0	89 47 20	mov dword ptr ds:[edi+20].eax
0042D1F3	89 5F 24	mov dword ptr ds:[edi+24].ebx
0042D1F6	89 4F 28	mov dword ptr ds: [edi+28].ecx
0042D1F9	89 57 2C	mov dword ptr ds: [edi+2C], edx



GetPhysicallyInstalledSystemMemory is utilized to obtain the RAM amount that is installed on the computer:

EIP → 0042026E FF 76 24 00420263 FF D0 <	push dword ptr ds:[esi+24] call eax	eax:¢ v	Default (stdcall)	▼ 5 🗘 Unlock
<pre>eax=<kernel32.getphysicallyinstalledsystemmemory> (76A7 .MPRESS1:0042D2C1 malware.exe:\$2D2C1 #2C4C1</kernel32.getphysicallyinstalledsystemmemory></pre>	81C0)		2: [esp+4] 00000000 3: [esp+8] 0000000 4: [esp+C] 00001A8	
am am am	An A	0019FBDC 0019	FBEO	

#### Figure 57

Finally, the stealer exfiltrates an archive containing a file called "System.txt" that is shown in figure 58, and another one called "Software.txt" that contains the installed software.

LummaC2, Build 20233101
LID(Lumma ID): TRNGVastream
- PC:
- User:
- OS Version: Windows 10 (10.0.16299)
- HWID:
- Screen Resoluton: 1920x1080
- Language: en-US
- CPU Name:
- GPU: VMware SVGA 3D
- Physical Installed Memory: 2048MB

The process takes a screenshot and exfiltrates it as "Screen.png":

00421785     00421785     0042178     0042178     0042178     00421793     FF 74 24 08     00421793     FF 74 24 30     0042179     F7 74 24 30     0042179     FF 74 24 30     0042179     F7 74 24 30     004217     F7     F7 74 24 30     004217     F7     F7	push eax push word ptr ss:[esp+8] push malware.453364 push dword ptr ss:[esp+30] call malware.419CA9	45336	×875W_ ×875W_ ×875W_ Default (s	_B 0 x875w_C3 0 _C1 0 x875w_C0 0 _SF 0 x875w_P 1 _stdcall)	x875W_C2 0 x875W_ES 0 L x875W_U 0 ▼ 5 € Unlod
malware.00419CA9			2: [es	p+4] 0045336A L"S	creen.png"
.MPRESS1:00421797 malware.exe:\$21797 #20997			3: [es 4: [es	p+8] 06FA0020 p+C]_007E9036 mal	ware.007E9036
💭 Dump 1 💭 Dump 2 💭 Dump 3 💭 Dump 4 💭 Dump 5	🛞 Watch 1 🛛 🖉 Locals 🖉 Struct	019FE0C 00	019FE44	"Screen.png"	
Address   Hex	ASCII	019FE14 00	SFA0020		
06FA0020 42 4D 36 90 7E 00 00 00 00 36 00 00 02 8 0	00 BM6.~6(.	197210 00	760036 mg	alware.00720036	

Figure 59



# Indicators of Compromise

# SHA256

199de8b727ceae96afb7c7560092c1d7a4dbe5a005c07ae20cffd9871da52b82

# C2 server

45.9.74.78

# User agent

TeslaBrowser/5.5

