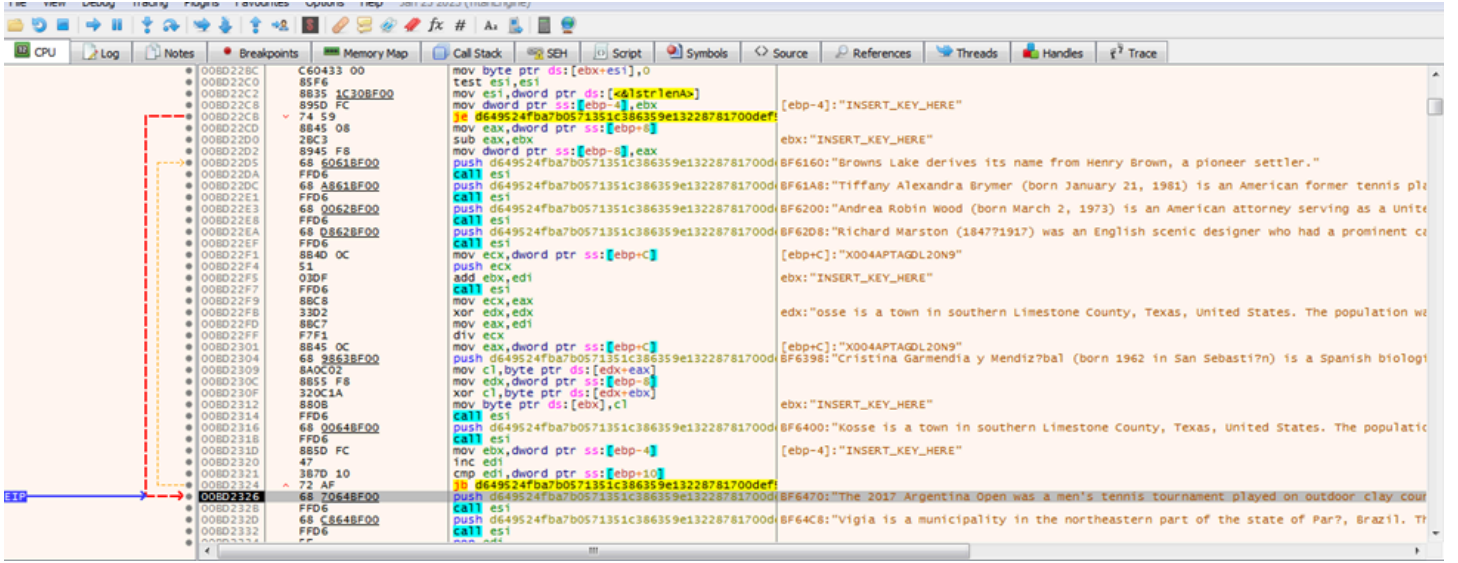


Ek Bilgiler/ Analist Notları



The screenshot shows a debugger window with assembly code on the left and string references on the right. The assembly code includes instructions like `mov byte ptr ds:[ebp+esi],0`, `test esi,esi`, `mov esi,dword ptr ds:[eax*lenA]`, `mov dword ptr ss:[ebp-4],ebx`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`, `mov eax,dword ptr ss:[ebp+0]`, `sub ebx,ebx`, `mov dword ptr ss:[ebp-8],eax`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`, `mov ecx,dword ptr ss:[ebp+c]`, `push ecx`, `add ebx,edi`, `call esi`, `mov ecx,ebx`, `xor edx,edx`, `mov eax,edi`, `div ecx`, `mov eax,dword ptr ss:[ebp+c]`, `push d649524fba7b0571351c386359e13228781700def`, `mov cl,byte ptr ds:[edx+eax]`, `mov edx,dword ptr ss:[ebp-4]`, `xor cl,byte ptr ds:[edx+ebx]`, `mov byte ptr ds:[ebx],cl`, `call esi`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`, `mov ebx,dword ptr ss:[ebp-4]`, `inc edi`, `cmp edi,dword ptr ss:[ebp+10]`, `call esi`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`, `push d649524fba7b0571351c386359e13228781700def`, `call esi`.

The string references on the right include: `[ebp-4]: "INSERT_KEY_HERE"`, `ebx: "INSERT_KEY_HERE"`, `BF6160: "Browns Lake derives its name from Henry Brown, a pioneer settler."`, `BF61A8: "Tiffany Alexandra Brymer (born January 21, 1981) is an American former tennis player"`, `BF6200: "Andrea Robin Wood (born March 2, 1973) is an American attorney serving as a United States"`, `BF62D8: "Richard Marston (1847-1917) was an English scenic designer who had a prominent career"`, `[ebp+c]: "X004APTAGDL20N9"`, `ebx: "INSERT_KEY_HERE"`, `[ebp+c]: "X004APTAGDL20N9"`, `BF6398: "Cristina Garmendia y Mendizabal (born 1962 in San Sebastian) is a Spanish biologist"`, `ebx: "INSERT_KEY_HERE"`, `BF6400: "Kosse is a town in southern Limestone County, Texas, United States. The population was 1,123,388"`, `[ebp-4]: "INSERT_KEY_HERE"`, `BF6470: "The 2017 Argentina Open was a men's tennis tournament played on outdoor clay courts"`, `BF64C8: "Vigia is a municipality in the northeastern part of the state of Parana, Brazil. The population was 1,123,388"`.

Stringler üzerinde gördüğümüz şifreli textlerin dinamikte çözüldüğünü görüyoruz. Stringlerin Windows API'ları çözdüğü gözlemlenmiştir.



The screenshot shows a debugger window with assembly code on the left and string references on the right. The assembly code includes instructions like `int3`, `push F`, `push d649524fba7b0571351c386359e13228781700def`, `call d649524fba7b0571351c386359e13228781700def`, `push E`, `push d649524fba7b0571351c386359e13228781700def`, `push d649524fba7b0571351c386359e13228781700def`, `mov dword ptr ds:[132F1F4],eax`, `call d649524fba7b0571351c386359e13228781700def`, `push C`, `push d649524fba7b0571351c386359e13228781700def`, `push d649524fba7b0571351c386359e13228781700def`, `mov dword ptr ds:[132F00C],eax`, `call d649524fba7b0571351c386359e13228781700def`, `push A`, `push d649524fba7b0571351c386359e13228781700def`, `push d649524fba7b0571351c386359e13228781700def`, `mov dword ptr ds:[132F468],eax`, `call d649524fba7b0571351c386359e13228781700def`, `push C`, `push d649524fba7b0571351c386359e13228781700def`, `push d649524fba7b0571351c386359e13228781700def`, `mov dword ptr ds:[132F400],eax`, `call d649524fba7b0571351c386359e13228781700def`, `add esp,48`, `push B`, `push d649524fba7b0571351c386359e13228781700def`, `push d649524fba7b0571351c386359e13228781700def`, `mov dword ptr ds:[132F138],eax`, `call d649524fba7b0571351c386359e13228781700def`, `push 5`, `push d649524fba7b0571351c386359e13228781700def`, `push d649524fba7b0571351c386359e13228781700def`, `mov dword ptr ds:[132F124],eax`, `call d649524fba7b0571351c386359e13228781700def`.

The string references on the right include: `383368: "X004APTAGDL20N9"`, `1123388: "MS2ANYR3Q6P@M0"`, `0132F1F4: "INSERT_KEY_HERE", eax: "GetUserNameA"`, `11233A8: "Q0B0812SI666"`, `0132F280: "GetProcAddress", eax: "GetUserNameA"`, `11233C8: "96MUN7FA"`, `11233D4: "UE9-V2"`, `0132F00C: "LoadLibraryA", eax: "GetUserNameA"`, `11233E0: "00305XFRK8"`, `0132F468: "IstrcatA", eax: "GetUserNameA"`, `11233F8: "USHKZ2J01VQ"`, `0132F4D0: "OpenEventA", eax: "GetUserNameA"`, `1123418: "XSD2RV65S1"`, `0132F138: "CreateEventA", eax: "GetUserNameA"`, `1123430: "M9BUX"`, `0132F124: "CloseHandle", eax: "GetUserNameA"`.

Farklı bir algoritma ile dynamic resolving işlemi yapılmaktadır.

003687A0	CC	int3		
003687A1	CC	int3		
003687A2	CC	int3		
003687A3	A1	mov eax, dword ptr ds:[590150]		eax:"screenshot.jpg"
003687A4	85C0	test eax, eax		eax:"screenshot.jpg"
003687A5	0F84	ja 0649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.3688CE		0057F434:"GetEnvironmentVariableA"
003687A6	8B00	mov ecx, dword ptr ds:[57F434]		eax:"screenshot.jpg"
003687A7	51	push ecx		eax:"screenshot.jpg"
003687A8	50	push eax		edx:"igla is a municipality in the northeastern part of the state o
003687A9	CALL	call dword ptr ds:[46getProcAddress]		eax:"screenshot.jpg"
003687AA	50	push eax		edx:"igla is a municipality in the northeastern part of the state o
003687AB	A3	mov dword ptr ds:[590150], eax		eax:"screenshot.jpg"
003687AC	51	push ecx		eax:"screenshot.jpg"
003687AD	50	push eax		0057F054:"GlobalLock"
003687AE	CALL	call dword ptr ds:[57F054]		edx:"igla is a municipality in the northeastern part of the state o
003687AF	51	push ecx		edx:"igla is a municipality in the northeastern part of the state o
003687B0	50	push eax		eax:"screenshot.jpg"
003687B1	A3	mov dword ptr ds:[59007C], eax		eax:"screenshot.jpg"
003687B2	CALL	call dword ptr ds:[46getProcAddress]		eax:"screenshot.jpg"
003687B3	50	push eax		eax:"screenshot.jpg"
003687B4	A3	mov dword ptr ds:[59018C], eax		edx:"igla is a municipality in the northeastern part of the state o
003687B5	51	push ecx		eax:"screenshot.jpg"
003687B6	50	push eax		edx:"igla is a municipality in the northeastern part of the state o
003687B7	CALL	call dword ptr ds:[46getProcAddress]		0057F084:"GlobalSize"
003687B8	50	push eax		edx:"igla is a municipality in the northeastern part of the state o
003687B9	A3	mov dword ptr ds:[590174], eax		edx:"igla is a municipality in the northeastern part of the state o
003687BA	CALL	call dword ptr ds:[46getProcAddress]		eax:"screenshot.jpg"
003687BB	50	push eax		eax:"screenshot.jpg"
003687BC	51	push ecx		eax:"screenshot.jpg"
003687BD	50	push eax		eax:"screenshot.jpg"
003687BE	51	push ecx		eax:"screenshot.jpg"
003687BF	50	push eax		eax:"screenshot.jpg"
003687C0	51	push ecx		eax:"screenshot.jpg"
003687C1	50	push eax		eax:"screenshot.jpg"
003687C2	51	push ecx		eax:"screenshot.jpg"
003687C3	50	push eax		eax:"screenshot.jpg"
003687C4	51	push ecx		eax:"screenshot.jpg"
003687C5	50	push eax		eax:"screenshot.jpg"
003687C6	51	push ecx		eax:"screenshot.jpg"
003687C7	50	push eax		eax:"screenshot.jpg"
003687C8	51	push ecx		eax:"screenshot.jpg"
003687C9	50	push eax		eax:"screenshot.jpg"
003687CA	51	push ecx		eax:"screenshot.jpg"
003687CB	50	push eax		eax:"screenshot.jpg"
003687CC	51	push ecx		eax:"screenshot.jpg"
003687CD	50	push eax		eax:"screenshot.jpg"
003687CE	51	push ecx		eax:"screenshot.jpg"
003687CF	50	push eax		eax:"screenshot.jpg"
003687D0	51	push ecx		eax:"screenshot.jpg"
003687D1	50	push eax		eax:"screenshot.jpg"
003687D2	51	push ecx		eax:"screenshot.jpg"
003687D3	50	push eax		eax:"screenshot.jpg"
003687D4	51	push ecx		eax:"screenshot.jpg"
003687D5	50	push eax		eax:"screenshot.jpg"
003687D6	51	push ecx		eax:"screenshot.jpg"
003687D7	50	push eax		eax:"screenshot.jpg"
003687D8	51	push ecx		eax:"screenshot.jpg"
003687D9	50	push eax		eax:"screenshot.jpg"
003687DA	51	push ecx		eax:"screenshot.jpg"
003687DB	50	push eax		eax:"screenshot.jpg"
003687DC	51	push ecx		eax:"screenshot.jpg"
003687DD	50	push eax		eax:"screenshot.jpg"
003687DE	51	push ecx		eax:"screenshot.jpg"
003687DF	50	push eax		eax:"screenshot.jpg"
003687E0	51	push ecx		eax:"screenshot.jpg"
003687E1	50	push eax		eax:"screenshot.jpg"
003687E2	51	push ecx		eax:"screenshot.jpg"
003687E3	50	push eax		eax:"screenshot.jpg"
003687E4	51	push ecx		eax:"screenshot.jpg"
003687E5	50	push eax		eax:"screenshot.jpg"
003687E6	51	push ecx		eax:"screenshot.jpg"
003687E7	50	push eax		eax:"screenshot.jpg"
003687E8	51	push ecx		eax:"screenshot.jpg"
003687E9	50	push eax		eax:"screenshot.jpg"
003687EA	51	push ecx		eax:"screenshot.jpg"
003687EB	50	push eax		eax:"screenshot.jpg"
003687EC	51	push ecx		eax:"screenshot.jpg"
003687ED	50	push eax		eax:"screenshot.jpg"
003687EE	51	push ecx		eax:"screenshot.jpg"
003687EF	50	push eax		eax:"screenshot.jpg"
003687F0	51	push ecx		eax:"screenshot.jpg"
003687F1	50	push eax		eax:"screenshot.jpg"
003687F2	51	push ecx		eax:"screenshot.jpg"
003687F3	50	push eax		eax:"screenshot.jpg"
003687F4	51	push ecx		eax:"screenshot.jpg"
003687F5	50	push eax		eax:"screenshot.jpg"
003687F6	51	push ecx		eax:"screenshot.jpg"
003687F7	50	push eax		eax:"screenshot.jpg"
003687F8	51	push ecx		eax:"screenshot.jpg"
003687F9	50	push eax		eax:"screenshot.jpg"
003687FA	51	push ecx		eax:"screenshot.jpg"
003687FB	50	push eax		eax:"screenshot.jpg"
003687FC	51	push ecx		eax:"screenshot.jpg"
003687FD	50	push eax		eax:"screenshot.jpg"
003687FE	51	push ecx		eax:"screenshot.jpg"
003687FF	50	push eax		eax:"screenshot.jpg"

GetProcAddress ile Dynamic resolving işlemi yapılmaktadır. API'ler çözümleniyor.

The screenshot shows Immunity Debugger with the following components:

- Assembly View:** Displays assembly instructions such as `push ecx`, `mov ecx, dword ptr ds:[ebp-1]`, and `call 0649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.129FDE0`. The `CALL` instruction is highlighted, indicating a dynamic resolution of a function pointer.
- Registers:** Shows the state of registers like `EAX`, `EBX`, `ECX`, `EDX`, `ESP`, `ESI`, `EDI`, and `EIP`. `EIP` is currently at `012A58A8`.
- Memory Dump:** Shows a hex dump of memory at address `012A58A8`, with the ASCII column displaying `return to 0649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.https`.
- Call Stack:** Shows the current call stack with frames for `GetCurrentProcessName` and `GetCurrentProcessName`.
- Command Line:** Shows the command `cmd.exe /c ...`.

Sistem bilgilerini çeken birçok fonksiyon mevcuttur. Sadece bilgisayar ve kullanıcı adını gösteren ekran görüntüsü iletilmiştir.

00175A36	05 00014000	add eax,400100	eax: "HTTP/1.1"
00175A3B	A1 88F13900	mov eax,dword ptr ds:[39F188]	eax: "HTTP/1.1"
00175A41	53	push ebx	
00175A42	53	push ebx	
00175A43	50	push ebx	eax: "HTTP/1.1"
00175A44	52	push edx	196978: "GET"
00175A45	68 78691900	push ds:d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.196978	
00175A4A	51	push ecx	
00175A50	FF15 94013800	CALL dword ptr ds:[&HttpOpenRequestA]	eax: "HTTP/1.1"
00175A53	3BF3	mov esi,ebx	
00175A55	OF84 F1000000	cmp esi,ebx	
00175A58	74 16	JL d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.175A54	
00175A5D	3BF8	cmp edi,ebx	
00175A5F	74 16	JL d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.175A75	
00175A66	6A 04	or dword ptr ss:[ebp-1C],10300	
00175A68	8D45 E4	lea eax,dword ptr ss:[ebp-1C]	
00175A6B	50	push eax	eax: "HTTP/1.1"
00175A6C	6A 1F	push 1F	
00175A6E	56	push esi	
00175A6F	FF15 68FF3A00	CALL dword ptr ds:[&InternetSetOptionA]	
00175A75	53	push ebx	
00175A76	53	push ebx	
00175A77	53	push ebx	
00175A78	53	push ebx	
00175A79	56	push esi	
00175A7A	FF15 28011800	CALL dword ptr ds:[&HttpSendRequestA]	
00175A80	53	push ebx	
00175A81	8D4D D0	lea ecx,dword ptr ss:[ebp-30]	
00175A84	51	push ecx	
00175A85	8D95 4CFEFFFF	lea edx,dword ptr ss:[ebp-184]	
00175A88	52	push edx	
00175A8C	6A 13	push 13	
00175A8E	56	push esi	
00175A8F	8BF8	mov edi,ebx	eax: "HTTP/1.1"
00175A91	C745 D0 00010000	mov dword ptr ss:[ebp-30],100	
00175A98	FF15 AC013800	CALL dword ptr ds:[&HttpQueryInfoA]	eax: "HTTP/1.1"
00175A9E	8BC0	test eax,ebx	
00175AA0	75 14	JNE d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.175A86	
00175AA2	8B75 08	mov esi,dword ptr ss:[ebp+8]	

Ndearn.xyz'ye istek atacak fakat Internet açık olmadığından KiUserExceptionDispatcher yakalıyor ve hata veriyor. O sebeple isteğin gideceği alanı nope'luyorum.

01035A51	8BF0	mov esi,ebx	
01035A53	3BF3	cmp esi,ebx	
01035A55	OF84 F1000000	JL d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.1035A4C	
01035A5B	3BF8	cmp edi,ebx	
01035A5D	74 16	JL d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.1035A75	
01035A66	6A 04	or dword ptr ss:[ebp-1C],10300	
01035A68	8D45 E4	lea eax,dword ptr ss:[ebp-1C]	
01035A6B	50	push eax	
01035A6C	6A 1F	push 1F	
01035A6E	56	push esi	
01035A75	FF15 68FF2601	CALL dword ptr ds:[&InternetSetOptionA]	
01035A76	53	push ebx	
01035A77	53	push ebx	
01035A78	53	push ebx	
01035A79	56	push esi	
01035A7A	90	nop	
01035A7B	90	nop	
01035A7C	90	nop	
01035A7D	90	nop	
01035A7E	90	nop	
01035A7F	90	nop	
01035A80	51	push ebx	
01035A81	8D4D D0	lea ecx,dword ptr ss:[ebp-30]	
01035A84	51	push ecx	
01035A85	8D95 4CFEFFFF	lea edx,dword ptr ss:[ebp-184]	
01035A88	52	push edx	
01035A8C	6A 13	push 13	
01035A8E	56	push esi	
01035A8F	8BF8	mov edi,ebx	
01035A91	C745 D0 00010000	mov dword ptr ss:[ebp-30],100	
01035A98	FF15 AC012701	CALL dword ptr ds:[&HttpQueryInfoA]	
01035AA0	75 14	JNE d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.1035A86	
01035AA2	8B75 08	mov esi,dword ptr ss:[ebp+8]	
01035AA4	68 7C490101	push d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.105697C	105697C: "ERROR"
01035AAA	8BC0	test eax,esi	
01035AAC	EB 4FA20000	JMP d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.103FD00	
01035AAD	EB 80000000	JMP d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.1035866	

010359C7	53	push ebx	
010359C8	53	push ebx	
010359C9	6A 01	push 1	
010359CB	8D4D 18	lea ecx,dword ptr ss:[ebp+18]	
010359CE	C645 FC 03	mov byte ptr ss:[ebp-4],3	
010359D2	EB C9A50000	JMP d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.103FFA0	
010359D7	50	push eax	
010359D8	FF15 6002701	CALL dword ptr ds:[&InternetOpenA]	
010359DE	8B15 38F3501	mov edx,dword ptr ds:[125F338]	0125F338: &"https"
010359E4	8BF0	mov esi,ebx	
010359E6	8B45 8C	mov eax,dword ptr ss:[ebp-74]	[ebp-74]: "https"
010359E9	52	push edx	
010359EA	50	push eax	
010359EB	8975 EC	mov dword ptr ss:[ebp-14],esi	
010359EE	33FF	xor edi,edi	
010359F0	FF15 3C012701	CALL dword ptr ds:[&StrCmpA]	
010359F6	85C0	test eax,ebx	
010359F8	75 03	JNE d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.10359FD	
010359FA	8D7B 01	lea edi,dword ptr ds:[ebx+1]	
010359FD	3BF3	cmp esi,ebx	
010359FF	OF84 58010000	JL d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.1035860	
01035A05	8B4D A0	mov ecx,dword ptr ss:[ebp-60]	
01035A08	8B55 98	mov edx,dword ptr ss:[ebp-68]	[ebp-68]: "steamcommunity.com"
01035A0B	53	push ebx	
01035A0C	53	push ebx	
01035A0D	6A 03	push 3	
01035A10	53	push ebx	
01035A11	51	push ecx	
01035A12	52	push edx	
01035A13	56	push esi	
01035A14	FF15 60012701	CALL dword ptr ds:[&InternetConnectA]	
01035A1A	8BC8	mov ecx,ebx	
01035A1C	894D D4	mov dword ptr ss:[ebp-2C],ecx	
01035A1F	3BCB	cmp ecx,ebx	
01035A21	OF84 32010000	JL d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2af66.1035859	
01035A27	8B55 B4	mov ecx,dword ptr ss:[ebp-4C]	[ebp-4C]: "/profiles/76561199662282318"
01035A2A	8BC7	mov eax,edi	
01035A2C	F7D8	neg eax	
01035A2E	1BC0	sbb eax,eax	
01035A30	53	push ebx	



STEAM

MAĞAZA TOPLULUK HAKKINDA DESTEK



iili <http://159.69.26.61> iili -

Seviye 0

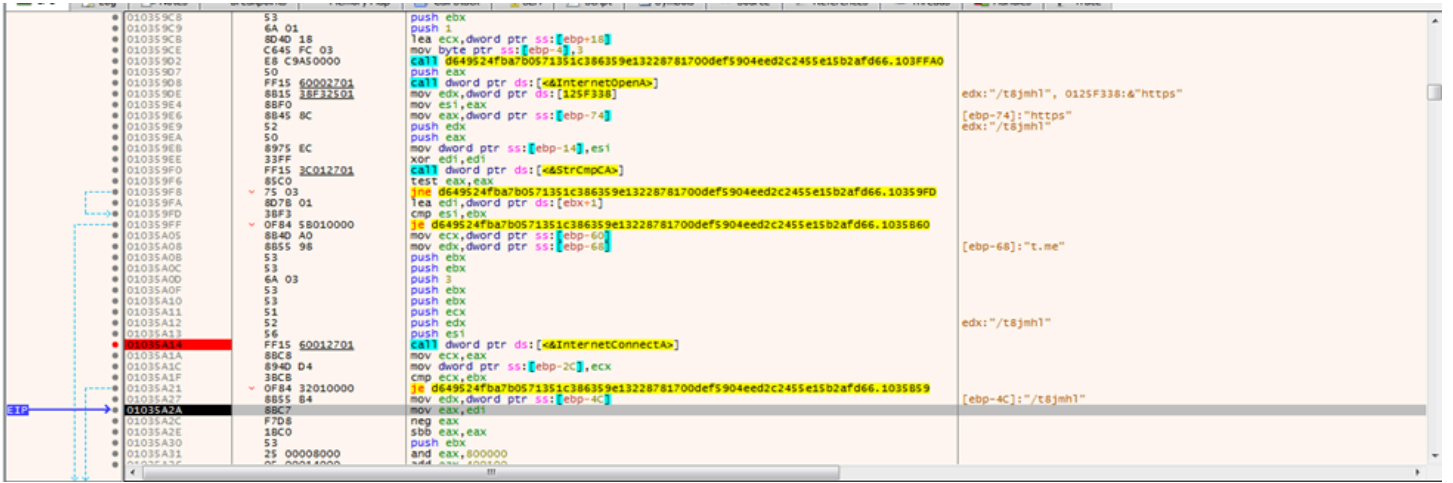
https://steamcommunity.com/profiles/76561199662282318 profilinde isim alanı iili http://159.69.26.61 iili şeklinde eklenmiştir. Dinamik analizde iili alanları ayrıştırdığı gözlemlenmiştir. (Kırmızı ile vurgulanmıştır.)

```
...rdata:0114E91D 00 00 00 align 10h
rdata:0114E920 68 74 74 70 73 3A 2F 2F 73 74+aHttPsSteamcomm db 'https://steamcommunity.com/profiles/76561199662282318',0
rdata:0114E920 65 61 6D 63 6F 6D 6D 75 6E 69+ ; DATA XREF: sub_112A790+8to
rdata:0114E956 00 00 align 4
rdata:0114E958 69 31 69 6C 00 aIiil db 'iili',0 ; DATA XREF: sub_112A7C0+8to
rdata:0114E95D 00 00 align 10h
rdata:0114E960 4D 6F 7A 69 6C 6C 61 2F 35 2E+aMozilla50Macin db 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
rdata:0114E960 30 28 4D 61 63 69 6E 74 6F+ ; DATA XREF: sub_112A7F0+8to
rdata:0114E960 73 68 3B 2D 49 6E 74 65 6C 20+db '22.0.0.0 Safari/537.36 OPR/108.0.0.0',0
rdata:0114E9E4 68 74 70 73 3A 2F 2F 74 2E+aHttPsTMeT8jml db 'https://t.me/t8jml',0
rdata:0114E9E4 6D 65 2F 74 38 6A 6D 68 6C 00 ; DATA XREF: sub_112A820+8to
rdata:0114E9F8 69 31 69 6C 00 aIiil_0 db 'iili',0 ; DATA XREF: sub_112A850+8to
rdata:0114E9FD 00 00 00 align 10h
rdata:0114EA00 4D 6F 7A 69 6C 6C 61 2F 35 2E+aMozilla50Macin_0 db 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
rdata:0114EA00 30 28 4D 61 63 69 6E 74 6F+ ; DATA XREF: sub_112A880+8to
rdata:0114EA00 73 68 3B 2D 49 6E 74 65 6C 20+db '22.0.0.0 Safari/537.36 OPR/108.0.0.0',0
rdata:0114EA84 68 74 70 73 3A 2F 2F 73 74+aHttPsSteamcomm_0 db 'https://steamcommunity.com/profiles/76561199662282318',0
```

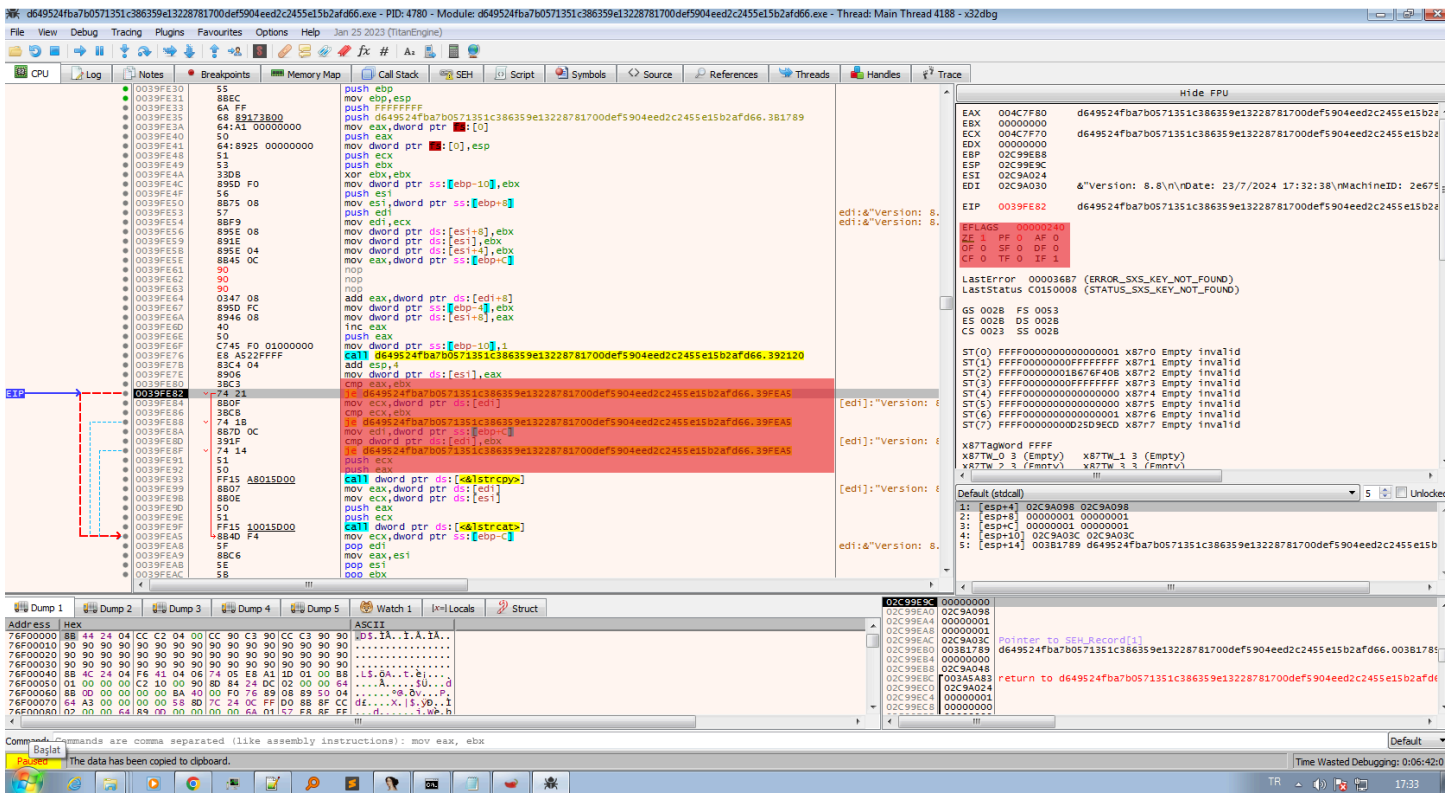
User Agent bilgileri de uygulamada depolanmaktadır.

Table with columns: Address, Displacement, Instruction, Comment. Contains memory dump data with user agent strings like 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.0.0 Safari/537.36 OPR/108.0.0.0' and other browser identifiers.

Farklı tarayıcıların vallet bilgileri de uygulama tarafından alınmaktadır.



Ek olarak "https://t.me/t8jmh1" adresine istek gitmektedir.



vurgulanan kısımda tarih kontrolü yapıyor. Zero flagi 1 yaparak kontrolden kurtulduk.

Uygulamanın komut istemini de açtığı görülmüşür ancak kullandığına dair bir bulgu bulunamamıştır.

Zararlı her çalıştığında farklı isimlerde .exe oluşturmaktadır.

BGCBGCAFII.exe	23.07.2024 14:59	Uygulama	0 KB
CAFBGDHCBA.exe	23.07.2024 15:04	Uygulama	0 KB
CBKJEGCBKK.exe	23.07.2024 15:05	Uygulama	0 KB
DGDBAKKJJK.exe	23.07.2024 15:05	Uygulama	0 KB
DGIJEGHDAE.exe	23.07.2024 14:43	Uygulama	0 KB
EGIDBFBFHJ.exe	23.07.2024 14:46	Uygulama	0 KB
KJJKFIIIJ.exe	23.07.2024 14:41	Uygulama	0 KB
KJKJEGIDB.exe	23.07.2024 14:54	Uygulama	0 KB



i1il http://159.69.26.61 i1li ↓

Level 0



i1il http://159.69.26.61 i1li

Level 0 | 0.3 years | Offline | Share

2024-04-01T09:36:40+00:00

Görüldüğü üzere Steam hesabı 1 Nisan 2024 tarihinde oluşturulmuş.

ndearn.xyz

whois information

Whois

DNS Records

Diagnostics

cache expires in 1 days, 0 hours, 0 minutes and 0 seconds

Registrar Info

Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com
Referral URL	https://www.godaddy.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientRenewProhibited https://icann.org/epp#clientRenewProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates

Expires On	2025-04-02
Registered On	2024-04-02
Updated On	0001-01-01

Site Status

Status Inactive

Server Type

Suggested Domains for ndearn.xyz

Ayrıca site durumu inaktif görünmekte. Ek olarak Wayback Machine vb. geçmişe dönük herhangi bir site içeriği tespit edilemediğinden zararlının analizini bitirmek durumunda kaldı.

Yara Kuralı

```
import "pe"
import "hash"
rule vidar_stealer
{
  meta:
    author = "takım8"
    description = "vidar stealer için yara kuralı"
    file_name =
      "d649524fba7b0571351c386359e13228781700def5904eed2c2455e15b2afd66.exe"

  strings:
    $mz = "MZ"

    $str1 = "X004APTAGDL20N9"
    $str2 = "SLWLVJLOZZGXL9FT3J17"
    $str3 = "passwords.txt"
    $str4 = "65 79 41 69 64 48 6C 77 49 6A 6F 67 49 6B 70 58 56 43 49 73 49 43 4A
68 62 47 63 69 4F 69 41 69 52 57 52 45 55 30 45 69 49 48 30"

    $sql1 = "SELECT target_path, tab_url from downloads"
    $sql2 = "SELECT service, encrypted_token FROM token_service"

  condition:
    filesize<=1MB and hash.md5(0,filesize)="baa9e1a92bab85279dca0aed641f1fa9"
and all of them and $mz at 0
}
```