

卜

乚

!



2018 8 15

Beijing Venus Information Security Tech., Inc.

.....

42
.....

2018 7

APT

山

W

flash_security_component_installer_1.0.0.2.exe	220.0 KB	139.0 KB	应用程序	2018-07-21 16:06
flash安全组件安装说明.doc	93.7 KB	88.4 KB	DOC 文档	2018-07-21 16:48

W

flash

W

2.1 Dropper

flash

4

4

W

14

ESET

W

ESET

W

[illegible]

avira.Sysstray.exe

W

地址	值	注释
0012ED24	0012ED74	UNICODE "winlogon.exe"
0012ED28	0012ED8C	
0012ED2C	003A8152	UNICODE "avrt.sys"

24

1

Vista

UAC

system32

CIA Vault 7

UAC

W

wusa.exe

W

2

PE

temp0 4 fake 4 acess 4 wrivt.exe

wrivt.exe

Vista

64

W

W

64exename	wrivt.exe	64
64loadpath7	system/msTracer.dll	



AfterInstallation	RemoveInstaller	flash
-------------------	-----------------	-------



COM IARPUinstallStringLauncher

UninstallString xcopy.exe msTracer.dll system32 山¹²

64 360tray.exe rstray.exe 4

qqpctray.exe UAC 山

rstray.exe 山 qqpctray.exe k Vista.exe 1 505.42 590.11 Items [0000

360tray.exe wrivt.exe 山 wrivt.exe

temp0山 Vista 64

9</MCID 53>> B3659 TC BT.1 1171



360tray.exe 4

rstray.exe 4 qqpctray.exe

WSearch

W



		Dropper		4			
		temp0	Loader				
		temp0	temp0	AV	access		
1	4	Dropper	DLL	temp0			
1	32	XP	temp0	system/srvlic.dll			
LanmanServer			LanmanServer	svchost.exe	srvsvc.dll		
srvsvc.dll		LoadLicensingLibrary		API	srvlic.dll		
74FF755E		mov		edi, offset aSrvlic_dll ; "srvlic.dll"			
74FF7563		push		edi ; wchar_t *			
74FF7564		mov		esi, eax			
74FF7566		call		ds:wcslen			
2	32	Window 7	temp0	system/msTracer.dll			
		WSearch	SearchProtocolHost.exe	msTracer.dll			



needmid

```
version.dll  temp0
```

fake

W

6 4 access

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\x

x	DisplayName
---	-------------

W

74

version.dll

W

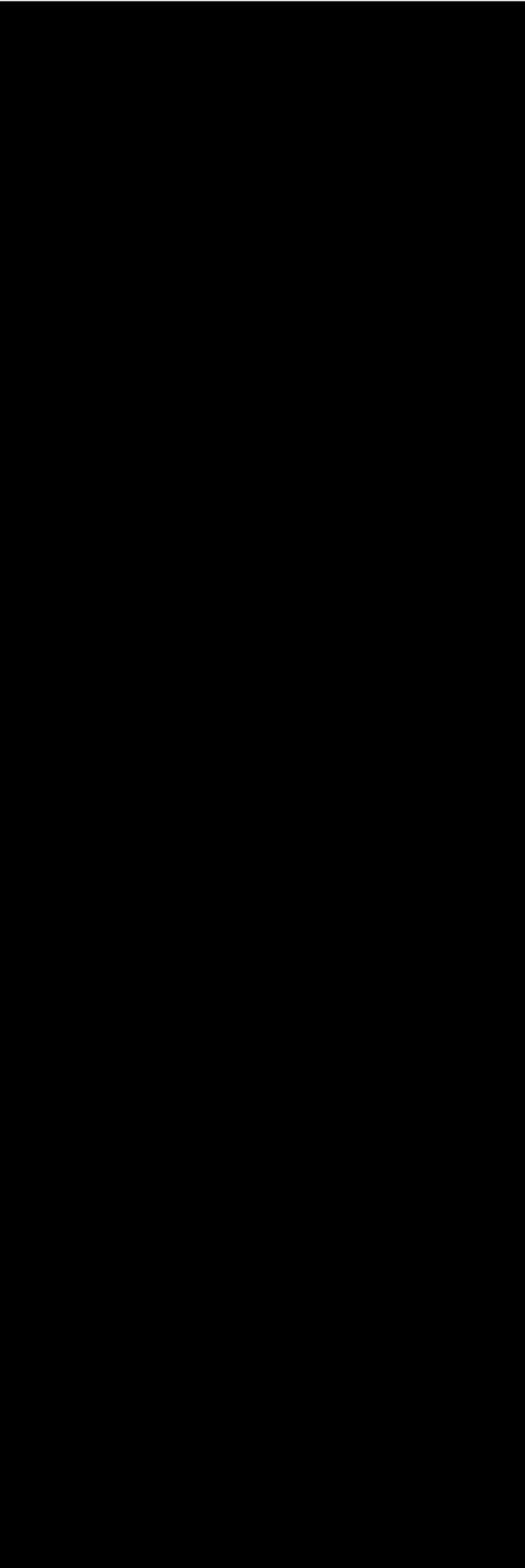
temp0

fake

W

access

version.dll 山



24 Vista System temp0





```
push    offset aSuccess ; "success"
push    [ebp+arg_4]      ; int
call    sub_10002444
or      [ebp+Src], 0FFFFFFFh
or      [ebp+var_4], 0FFFFFFFh
mov     esi, eax
lea     eax, [ebp+Src]
push    8                ; Size
push    eax              ; Src
push    esi              ; Dst
call    memcpy
add     esi, 8
push    offset aX86      ; "X86"
push    esi              ; int
call    sub_10002444
```

0	00	73	00	75	00	63	00	63	00	65	00	73	00	• success	00B7003C	07	00	00
F	FF	FF	FF	FF	FF	FF	03	00	00	00	58	00	00	s...tX	00B7003C	73	00	FF
5	00	00	00	00	00	00	00	00	00	00	00	00	00	86	00B7004C	38	00	30

ExecCmd_GetPlatformBits success X86

8 FF 山

```
lea     rdx, aSuccess    ; "success"
mov     rcx, rdi
call    sub_100027B4
lea     rdx, [rsp+38h+Src] ; Src
mov     r8d, 8           ; Size
mov     rcx, rax          ; Dst
mov     rbx, rax
mov     [rsp+38h+Src], 0FFFFFFFFFFFFFFFFh
call    memcpy
lea     rcx, [rbx+8]
lea     rdx, aX64        ; "X64"
call    sub_100027B4
```

64 Dropper 64 fake success X64山

C&C 32 64 山

SecretKey 0x5E2A5642 Magic(0xC7315A6B)

山 Magic(0xC7315A6B)

C&C 0xC7315A6B山



地址	十六进制	ASCII
42 56 2A 5E 3C 45 EF 4F	13 BB BB BB 00 00 BV** <跟换	00B70020 30 00 00 00
55 BB 65 BB 53 BB 0C BB 0C BB B8 B8	机运运管??柜	00B70030 0C BB FA BB
B8 B8 A4 BB BB BB F9 BB F6 BB 8A BB	父父父+换 耀斌	00B70040 B8 B8 B8 B8
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00B70050 7B 7B 7B 7B 00 00 00 00 00 00 00 00	

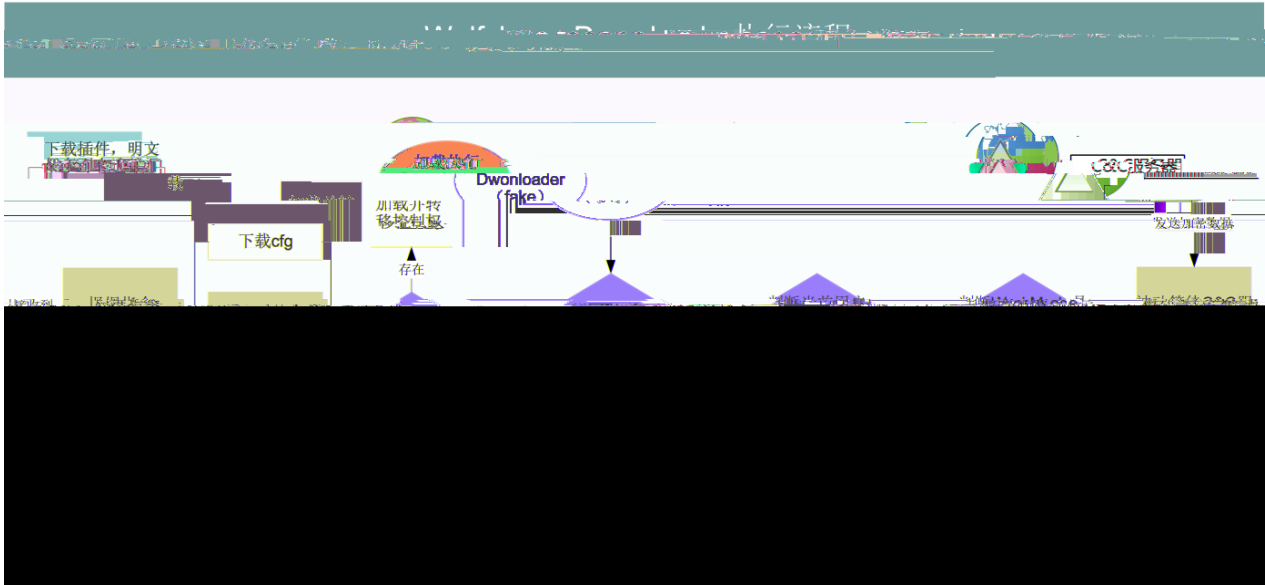
4 4 fake 6

OPcode1	OPcode2	
0134A6D30	0100B4627	
0C558B012	05047A6F4	cfg
022836D73	06F42E3C0	X86 or X64
03254BFD2	0 6FF39717	dll
0B4749FFF	0A7109782	
0DDD7303E	0CDF2E7F4	cfg

5 4 fake main

main fake 山 山

Donwloader 山



2.2.3

main





inter

dll

山 dll

4

山



Revinst

3.2

Loader temp0

series 4 mainpath 4 CommonAppData 4 System/ 4 Windows/

2014 2015 temp0

commonappdata/Windows CE/fake

fake 11 temp0 fake 11

2014 2015 temp0 access11

fake

loadpathxp 4loadpathxp 4loadpath7 4loadpath7 4loadpathsv 4loadpathsv 4
windows/explorer.exe 4SearchIndexer-1 4SearchIndexer-2 4WorkMode 4AddressList 4
ClientID 4 ControllerID 4 ControllerVersion 4 PluginCoder 4 Persistence 4
WorkingDirectory 4system/msTracer.dll 4windows/fixsst.dll 4system/srvlic.dll 4series 4
SpecialPlugin 4
SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\Restrict
edServices\Static\System11



```
1000943C a64loadpath7:
1000943C          unicode 0, <64loadpath7>
10009452          dd 13h
10009456 .aSystemMstracer+
          unicode 0, <64loadpath7>
          dd 13h
          unicode 0, <64loadpath7>
          dd 13h
          unicode 0, <64loadpath7>
          dd 13h
```

fake 2014 2015 fake cfg

0C558B012/5047A6F4 4 0DDD7303E/0CDF2E7F4

4

fake main ClientID 4 ControllerID fake

ClientID ClientBasicInformation

ControllerID C&C

	2014(fake)	2015(fake)	2017(fake)	main
ClientID				E5201314
ControllerID	20140410144726	20140410144726	20160224152828	20130628173338

ClientID 4 ControllerID

fake main C&C 4

Magic 0xC7315A6B

0xC7315A6B

GDATA

1. TooHash 1

W

fake

opcode

- TooHash 4

W

```

1 bool * __cdecl sub_1000311C(int a1, int a2, int Src, int a4)
2 {
3     if ( a1 == 0x134A6D30 && a2 == 0x100B4627 )
4         return sub_10002D44(Src, a4);
5     if ( a1 == 0x0C588012 && a2 == 0x5047A5F4 )
6         return sub_10002E61(Src, a4);
7     if ( a1 == 0x02100000 && a2 == 0x0F42F3C0 )
8         return sub_10002566(Src, a4);
9 }

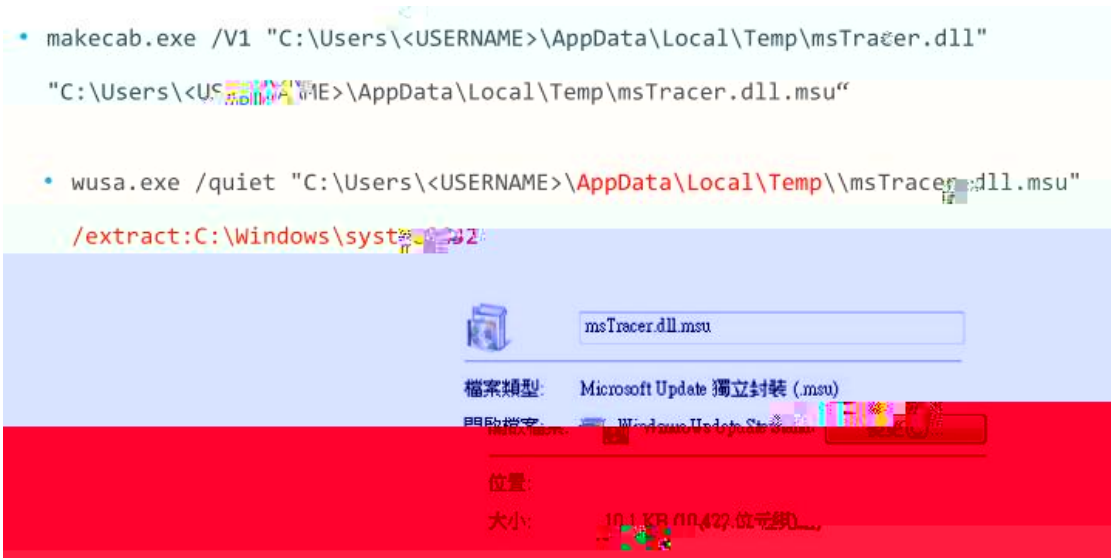
```

• **response**

MESSAGE_LEN[4]	MESSAGE[MESSAGE_LEN*2]	RETCODE[1]
----------------	------------------------	------------

UAC

W



I TooHash L

山

102 4 103 .xls

.doc

.xls

.xls

Wo.doc

4VenusEye

I TooHash L

山

山

APT

山

I

L 山

5

山

山



10d678deeaad0b45dea9bd70e21325da
a26ebe515cc6af6d05ad6d88c0257787
415027680047ed31fa5a84c94a46d582
31b6dbffc5f6d10e1fe7437626a7582b
40e916f03bbbc64921496e88d2d1d099
29daa2cffaf4e288388eb97da1f29a91
dd00fc9adaa3e20630dad5e5faaeff5
66a4bd97867c6364a3846654dfd37a24
095cf3f0ef7111d386bf7312186c7656
1366f1c75368964f8af247d2709e4889
6ec1db9872f6ca979649b4dab7bbe7fc
024883786ba706fe8c8a6354a355d30c

PDB

main

Z:\z_code\

- 1 <https://hitcon.org/2016/pacific/0composition/pdf/1202/1202%20R0%200930%20an%20intelligence-driven%20approach%20to%20cyber%20defense.pdf>
- 2 https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf