

启



启



E

E

启



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

2.1 Dropper

U

U

地址	值	注释
0012F830	004074D5	rCALL 到 strstr 来自 flash_se.004074CF

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

```
004044DD      mov     word ptr [ebp+Username], 'u'
004044E6      push   eax                ; lpProcessInformation
004044E7      lea   eax, [ebp+StartupInfo]
004044ED      push   eax                ; lpStartupInfo
004044EE      push   ebx                ; lpCurrentDirectory
004044EF      push   ebx                ; lpEnvironment
004044F0      push   ebx                ; dwCreationFlags
004044F1      push   ebx                ; lpCommandLine
004044F2      lea   eax, [ebp+Username]
004044F8      push   [ebp+lpApplicationName] ; lpApplicationName
004044FB      mov   word ptr [ebp+Username+2], 'a'
00404504      mov   word ptr [ebp+Username+4], 'c'
0040450D      mov   word ptr [ebp+Username+6], bx
00404514      push   LOGON_NETCREDENTIALS_ONLY ; dwLogonFlags
00404516      push   offset Password ; "useless"
0040451B      push   offset Domain ; "is"
00404520      push   eax                ; lpUsername
00404521      call  ds:CreateProcessWithLogonW
```

U

```
004012F1      push   RT_BITMAP
004012F3      push   110
004012F5      push   eax
004012F6      lea   eax, [ebp+var_194]
004012FC      push   eax
004012FD      call  loadcfqfromres
```

启



--	--	--	--

U

启



	S	
--	---	--

			E		U		U
		E		U		U	

U

U

				E		U		U
--	--	--	--	---	--	---	--	---

SS U S

E U

E U U

启



S

U

E

E

E

```
74FF755E      mov     edi, offset aSrvlic_dll ; "srvlic.dll"  
74FF7563      push   edi                ; wchar_t *  
74FF7564      mov     esi, eax  
74FF7566      call   ds:wcslen
```

U

U

```
push   offset aMstracer_dll ; "msTracer.dll"  
push   0Ch                ; int  
lea    ecx, [ebp+lpFilename]  
call   sub_100D135  
push   [ebp+lpFilename] ; lpLibFileName  
call   esi ; LoadLibraryW
```

3

temp0

S

U S

E

E

E

E

E SE

E

E

E

E

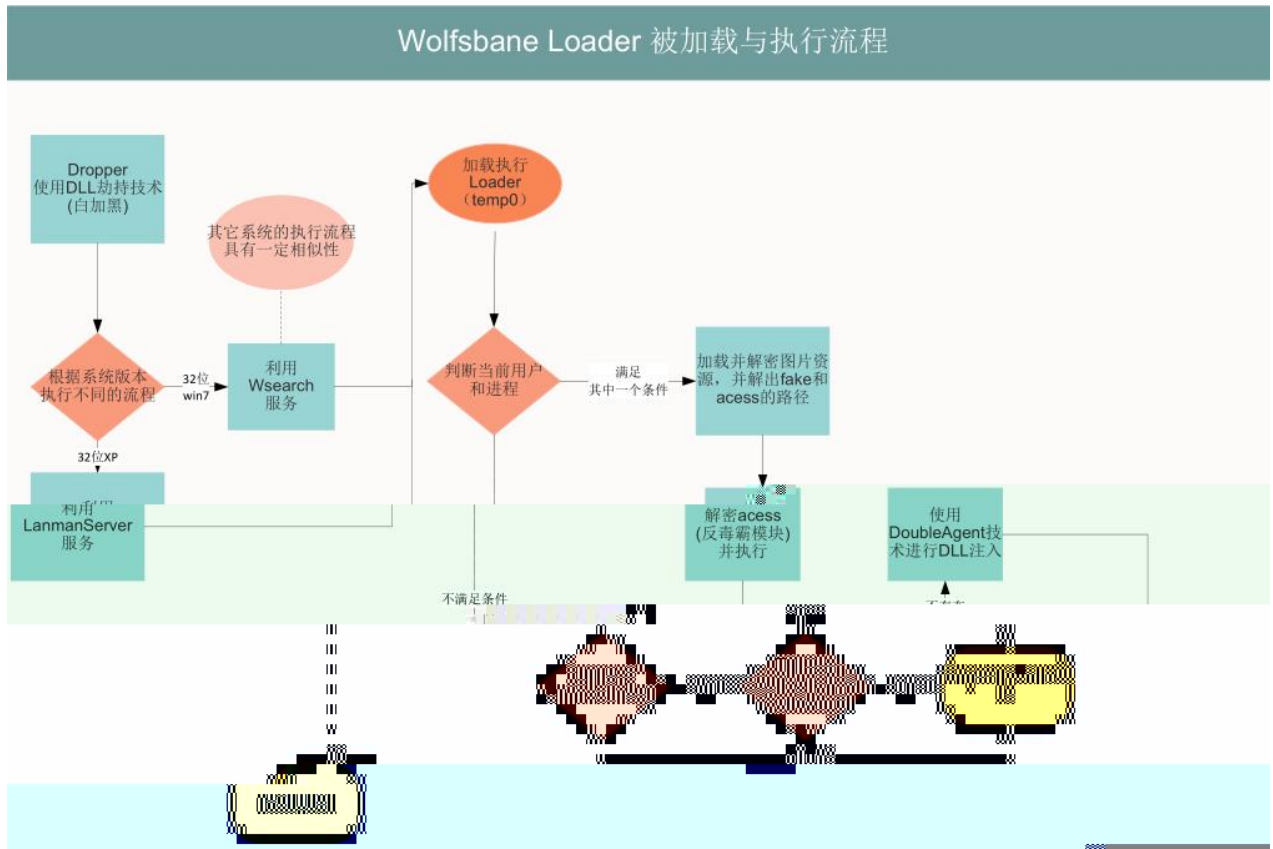
“HKEY_LOCAL_MACHINE U S

U

uniOnst.exe”

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
GlobalFlag	REG_SZ	0x100
VerifierDlls	REG_SZ	vfpod.dll
VerifierFlags	REG_DWORD	0x80000000 (2147483648)

地址	值	注释
0012F284	009C3107	CALL 到 WinExec 来自 009C3101
0012F288	0012F4A8	CmdLine = "c:\program files\kingsoft\kingsoft antivirus\uni0nst.exe"
0012F28C	00000000	ShowState = SW_HIDE



启



E

Data: 2000000006b1f21793f6e132228d5abfb50728ac9b89
[Length: 36]

00	0c	29	3c	a6	24	00	50	56	e7	13	5b	08	00	45	00
00	4c	00	21	00	00	80	06	ec	5d	3c	a9	01	56	c0	a8
4f	86	06	1a	04	1f	7e	60	52	99	a5	43	f2	fe	50	18
50	50	52	1c	00	00	00	00	00	00	00	00	00	00	00	00

地址	十六进制	ASCII
00B70020	06 B1 F2 17 6B 5A 31 C7 73 6D 83 22 C0 E3 42 6F	-彬kZ1莖m?楞Bo
00B70030	FC FF FF FF FF FF FF FF 00 00 00 00 00 00 00	?

E

10003147	>	3D 736D8322	CMP	EAX, 0x22836D73	loc_10003147
1000314C	>	75 08	JNZ	SHORT <loc_10003156>	
1000314E	.	81F9 C0E3426	CMP	ECX, 0x6F42E3C0	
10003154	>	74 58	JE	SHORT <ExecCmd_GetPlatformBits>	
10003156	>	3D D2BF5432	CMP	EAX, 0x3254BFD2	loc_10003156
1000315B	>	75 08	JNZ	SHORT <loc_10003165>	
1000315D	.	81F9 1797F36	CMP	ECX, 0x6FF39717	
10003163	>	74 3C	JE	SHORT <ExecCmd_LoadLibrary>	
10003165	>	3D FF9F74B4	CMP	EAX, 0xB4749FFF	loc_10003165
1000316A	>	75 08	JNZ	SHORT <loc_10003174>	
1000316C	.	81F9 829710A	CMP	ECX, 0xA7109782	
10003172	>	74 20	JE	SHORT <loc_10003194>	
10003174	>	3D 3E30D7DD	CMP	EAX, 0xDDD7303E	loc_10003174

```

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
    
```

地址	十六进制	UNICODE
00B7002C	07 00 00 00 73 00 75 00 63 00 63 00 65 00 73 00	+.succes
00B7003C	73 00 FF FF FF FF FF FF FF FF 03 00 00 00 58 00	s...X
00B7004C	38 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00	86.....

```

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
    
```

启



--	--	--

E

```
10089054 aServicecontext: ; DATA XREF: sub_100
10089054          unicode 0, <ServiceContext::ServiceTable>,0
1008908E          align 10h
10089090 aServiceFuncio: ; DATA XREF: sub_100
10089090          ; sub_10028580+31↑o
10089090          unicode 0, <Service::FunctionTableSection>,0
```

E
S
S
S E
S

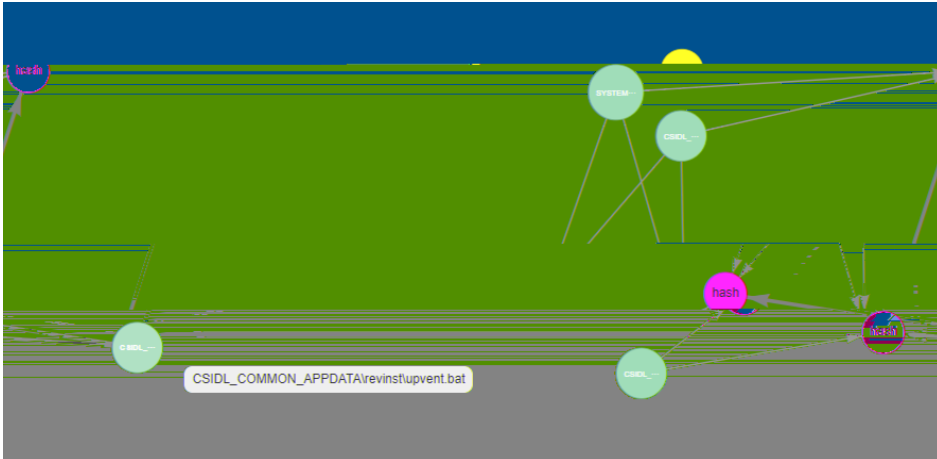
启



E

启





3.1



E

E

```

00403783      mov     [ebp+Str], '3'
00403789      mov     [ebp+var_36], '6'
0040378F      mov     [ebp+var_34], '0'
00403795      mov     [ebp+var_32], 't'
0040379B      mov     [ebp+var_30], 'r'
004037A1      mov     [ebp+var_2E], 'a'
004037A7      mov     [ebp+var_2C], 'y'
004037AD      mov     [ebp+var_2A], ' '
004037B3
004037B9
004037BF

```



```
1000943C a64loadpath7:  
1000943C          unicode 0, <64loadpath7>  
10009452          dd 13h  
10009456 aSystemMstracer:  
10009456          unicode 0, <system/msTracer.dll>  
1000947C          dd 0Ch  
10009480 a64loadpathsv:  
10009480          unicode 0, <64loadpathsv>  
10009498          dd 11h  
1000949C aWindowsFxsst_d:  
1000949C          unicode 0, <windows/fxsst.dll>
```

EEE E

E E

E

E

E				
E				

E E

E U

U

U

```
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 == 0x558B912 && a2 == 0x5047A674 )
6     return sub_10002E61(Src, a4);
7   if ( a1 == 0x2386078 && a2 == 0xbF42E368 )
8     return sub_1000251B(Src, a4);
9   if ( a1 == 0x3254BFD2 && a2 == 0x6FF39717 )
10    return sub_10002566(Src, a4);
11   if ( a1 == 0xB474BFFE && a2 == 0xA7109782 )
12    return sub_10002ECC(Src, a4);
13   if ( a1 == 0x0007301E && a2 == 0x0DF2E7F4 )
14    return sub_10003109(Src, a4);
15   return 0;
```

• If opcode1 == 0x3254BFD2 and opcode2 == 0x6FF39717

Request

0x3254BFD2	0x6FF39717	SIZE[4]	SECRET_KEY[4]	MAGIC[4]
------------	------------	---------	---------------	----------

Response

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

- makecab.exe /V1 "C:\Users\\AppData\Local\Temp\msTracer.dll"
"C:\Users\\AppData\Local\Temp\msTracer.dll.msu"
- wusa.exe /quiet "C:\Users\\AppData\Local\Temp\msTracer.dll.msu"
/extract:C:\Windows\system32



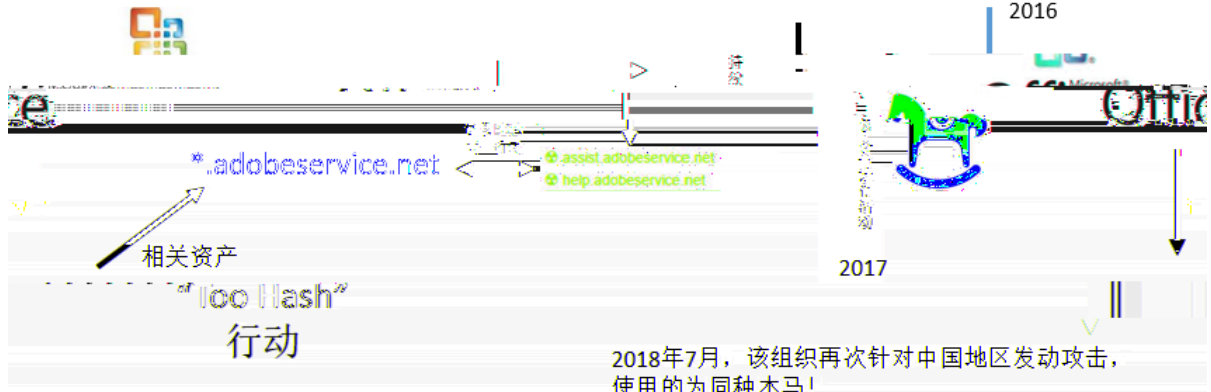
U

U

U

2013至2014年，该组织利用CVE-2012-0158构造含中文内容的恶意文档进行攻击活动

2016年，该组织使用了一种新的木马（家族名）并针对中国台湾进行攻击



U

IOC

E

S

S

S

S

S E

S E

S E E

S

启



S

E U

U