
启明星辰公司-金睛安全研究团队



目 录

背景

一、攻击事件还原

1.1 攻击过程分析



1.2 载荷分析

 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

二、攻击样本分析

2.1 主 Dropper 分析

地址	值	注释
0012F830	004074D5	CALL 到 strstr 来自 flash_se.004074CF
0012F834	0012FB54	s1 = "IDA Pro v6.8 and Hex-Rays Decompiler (ARM,x64,x86)"
0012F838	0012FEEC	s2 = "ESET"

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

```

```

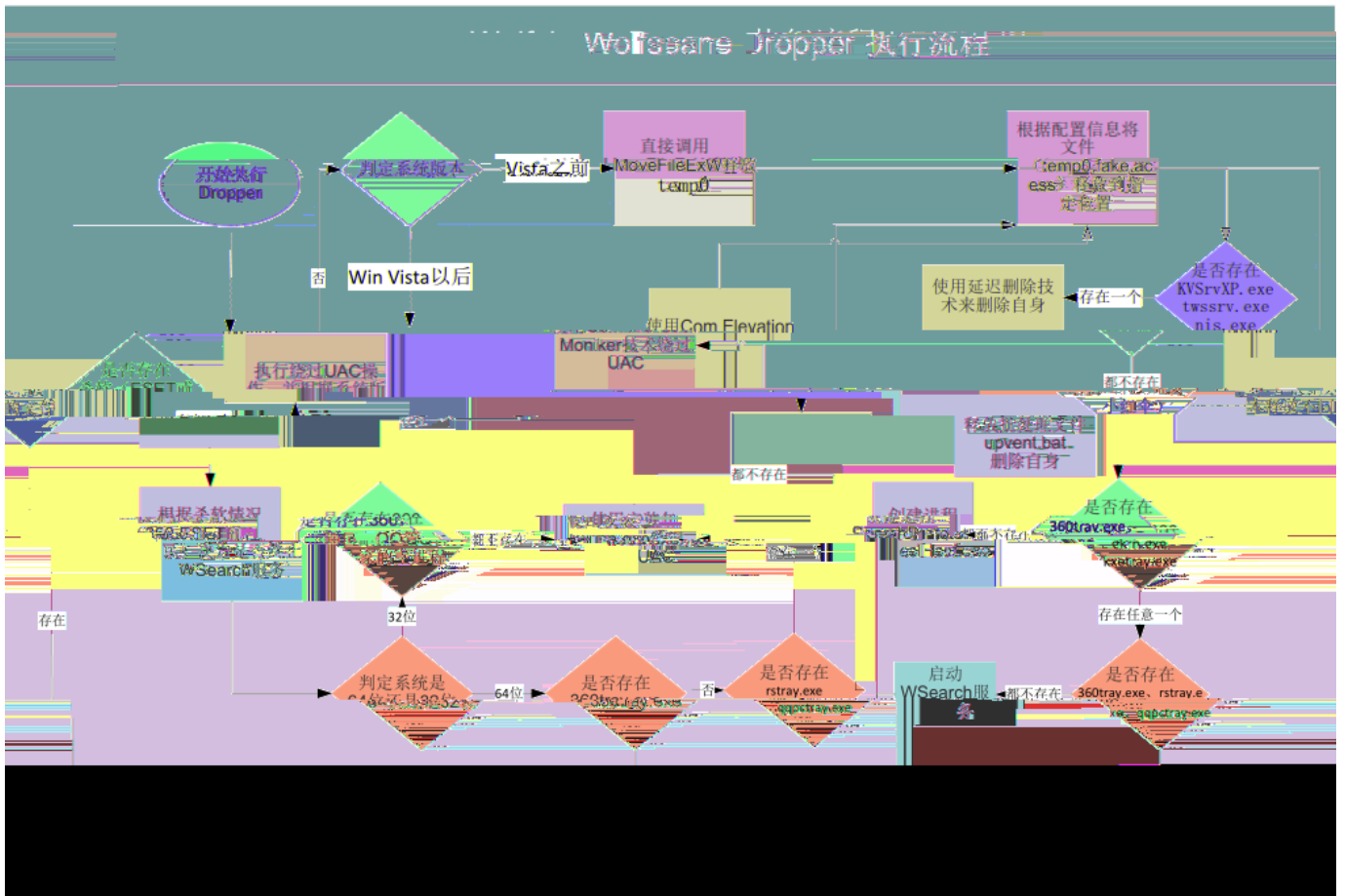
004012F1      push    RT_BITMAP
004012F3      push    110
004012F5      push    eax
004012F6      lea     eax, [ebp+var_194]
004012FC      push    eax
004012FD      call    loadcfqfromres

```


--	--	--

--

--



2.2 释放文件分析


```

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

```

```

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

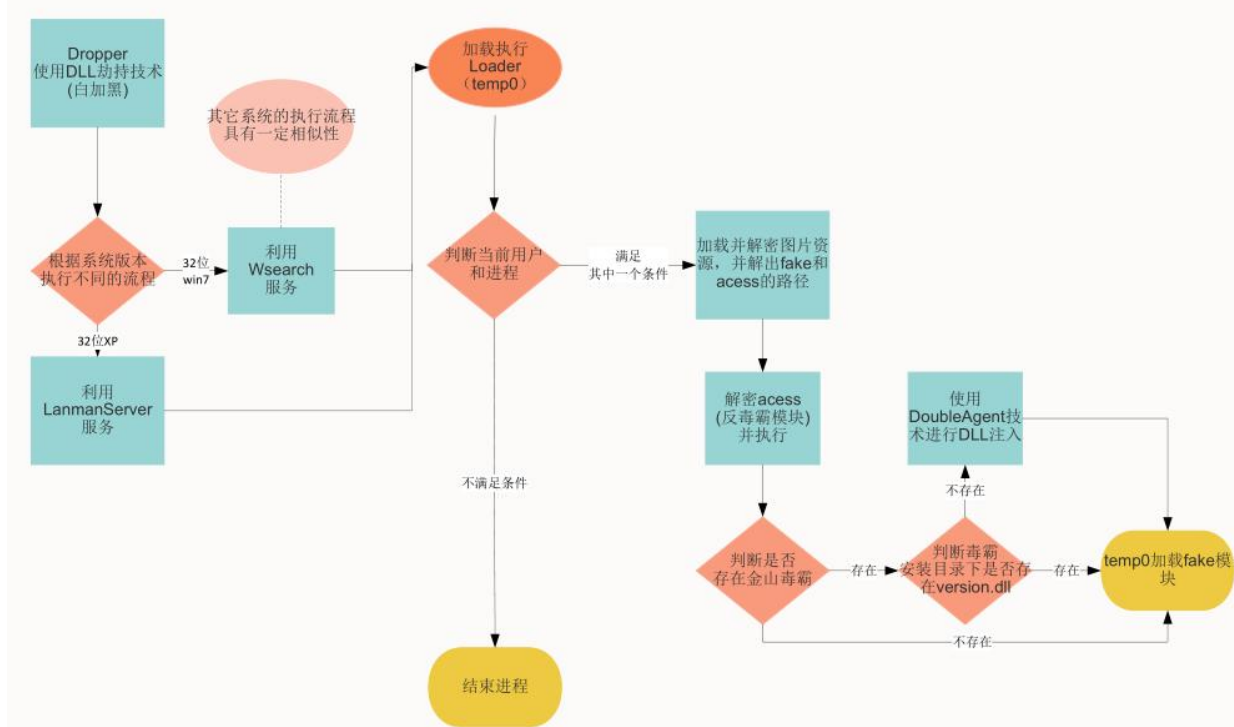
“HKEY_LOCAL_MACHINE

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\uniOnst.exe"
0012F28C	00000000	ShowState = SW_HIDE

Wolfsbane Loader 被加载与执行流程



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
fc	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1kZ1莖m?楞Bo
00B70030	FC FF FF FF FF FF FF FF 00 00 00 00 00 00 00	?

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, 0xDD07303E	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

```

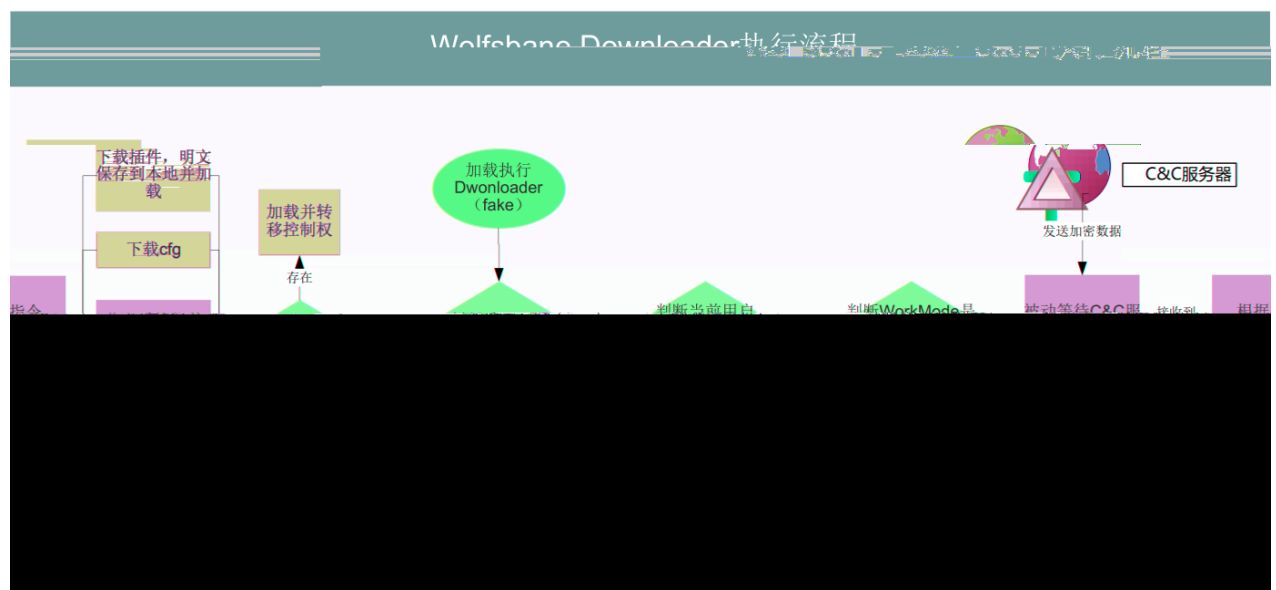
地址	十六进制	UNICODE
00B7002C	07 00 00 00 73 00 75 00 63 00 63 00 65 00 73 00	•. succes
00B7003C	73 00 FF FF FF FF FF FF FF FF 03 00 00 00 58 00	s. . . . 4. X
00B7004C	38 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00	86.

```

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

```

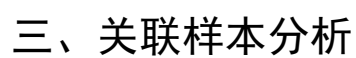
地址	十六进制	ASCII
00B70020	30 00 00 00 42 56 2A 5E 3C 45 EF 4F 13 BB BB BB	0...BV**^<E换
00B70030	0C BB FA BB 65 BB 65 BB 53 BB 0C BB 0C BB B8 B8	.机透透符??恒
00B70040	B8 B8 B8 B8 B8 B8 A4 BB BB BB F9 BB F6 BB 8A BB	父父父母换 曜斌
00B70050	BB BB BB BB 00 00 00 00 00 00 00 00 00 00 00 00	换换.....

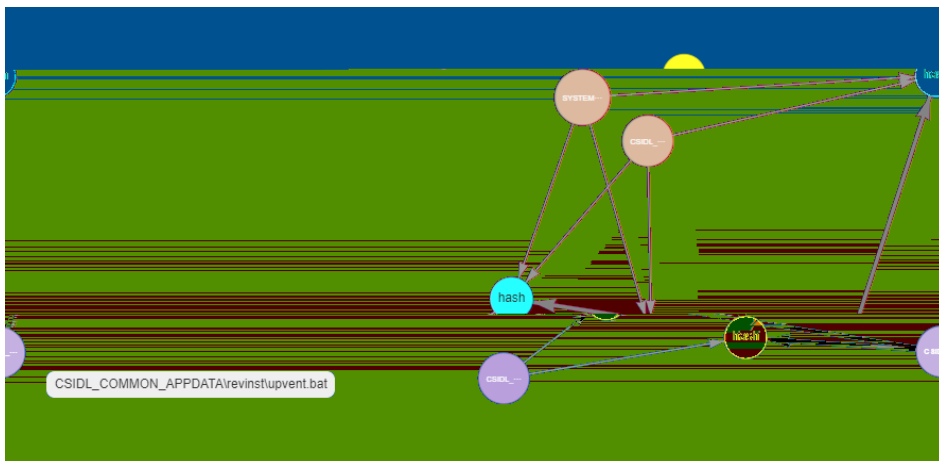


[illegible]

- utility
- io
- inter
- FxCoder

CreateFileService
ClientStatusService
BasicInformationService
ListFileService
ListFileRecursiveService
OpenFileService
CloseFileService
DeleteFileService
FileSizeService





3.1 配置信息比较



c

```

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], ' '
004037B8      mov     [ebp+var_28], ' '
004037B9      mov     [ebp+var_26], ' '
004037BF      mov     [ebp+var_24], ' '
    
```

c

3.2 释放文件比较

```

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>

```


四、溯源分析

```

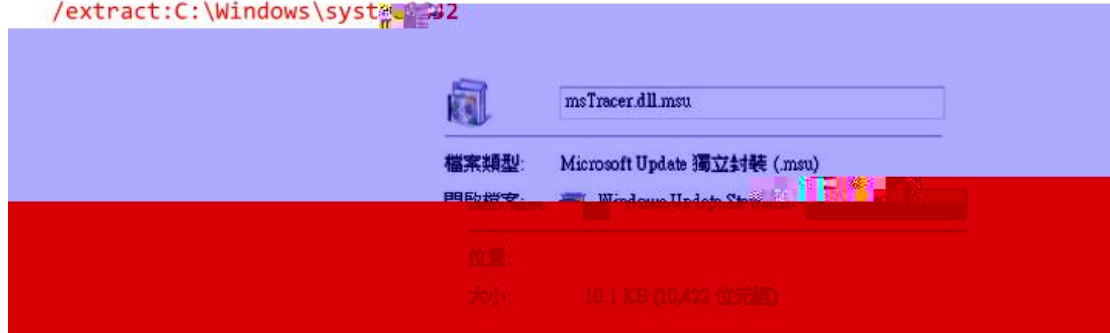
1 bool *__cdecl sub_1000311C(int a1, int a2, int Src, int a4)
2 {
3     if ( a1 == 0x13406D30 && a2 == 0x10004627 )
4         return sub_10002D44(Src, a4);
5     if ( a1 == 0xC5B8912 && a2 == 0x504785F4 )
6         return sub_10002E61(Src, a4);
7     if ( a1 == 0x21816073 && a2 == 0xA642E310 )
8         return sub_1000251B(Src, a4);
9     if ( a1 == 0x1254BFD2 && a2 == 0x6FF39717 )
10        return sub_10002566(Src, a4);
11     if ( a1 == 0xB474B6FE && a2 == 0xA71997B2 )
12        return sub_10002ECC(Src, a4);
13     if ( a1 == 0xD007391E && a2 == 0xDE2E7F4 )
14        return sub_10003109(Src, a4);
15     return 0;
16 }

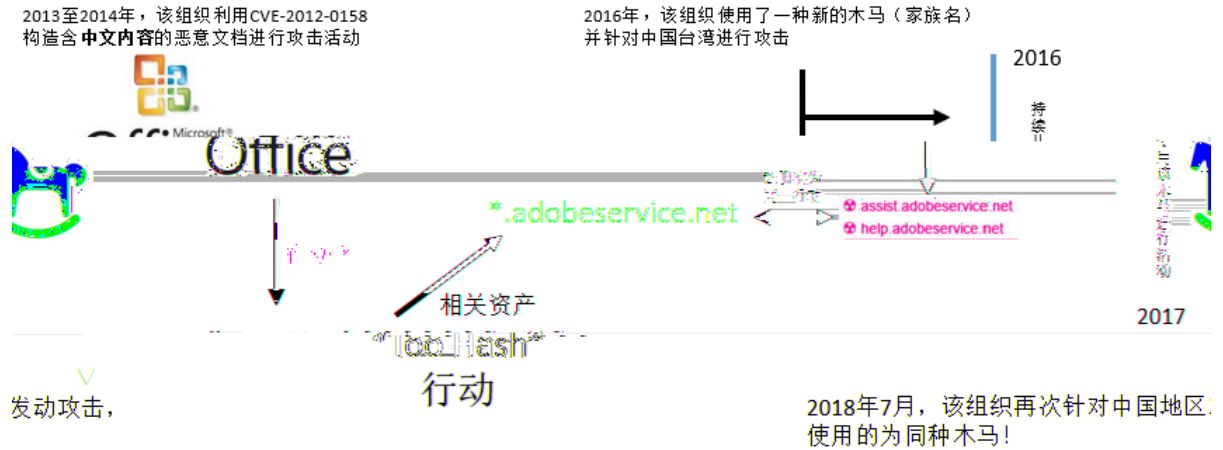
```

- If opcode1 == 0x3254BFD2 and opcode2 == 0x6FF39717
→ ExecCmd_LoadLibrary

• Command				
SIZE[4]	SECRET KEY[4]	MAGIC[4]	0x3254BFD2	0x6FF39717
• Response				
SECRET_KEY[4]	MAGIC[4]	SIZE[4]		
MESSAGE[MESSAGE_LEN*2]	RETCODE[1]	MESSAGE_LEN[4]		

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





五、总结

六、IOC

七、参考
