ľ Ŀ Í
h Ďρ

金睛 VenusEye

2018 8 15

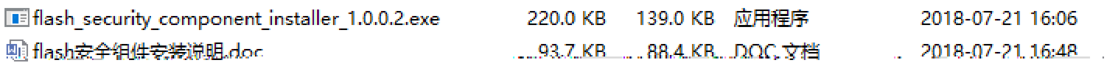
. ‹ Ω Ḥ ŋ Ȅ

Beijing Venus Information Security Tech., Inc.

2018 7 ˘ Ձ ῃ ﭬ ⌠ Ⴠ w̄ h 𝒟ρ ˘

№ Ҹ Ҥ ╠ APT 𝒟ρ Â № ˘ Ӏ ⌠

´ Â



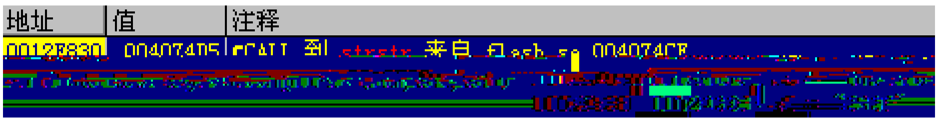
flash_security_component_installer_1.0.0.2.exe	220.0 KB	139.0 KB	应用程序	2018-07-21 16:06
flash安全组件安装说明.doc	93.7 KB	88.4 KB	DOC 文档	2018-07-21 16:48

ɾ ǘ ⌠ Ɗρ ɒ Oˇ ɣ ȋ̈ ṗ Ώ ӟ ˜ ɣ Δ ˇ Ɗρ Ț ˇ ғ Ψ Â Ӥ ȋ́ ᵣ ᴺ flash ´ Ð № Â

2.1 Dropper

ᴺ flash ´ ȋ́ ʬ ˇ ȉ Ψ à à ' ˇ ƅ Â

1 à Uˇ ῴ ESET ؏ ᴮˇ ĸ ŵ̈ ɷ ⩘ ₮ Â ɵ ᴸ ⩘ Ḥ ESET ʅ ض Â



地址	值	注释
0012E830	004074D5	CALL 到 strstr 来自 flash_se.004074CF

avira.Systray.exe ᴮ ʅ ض Â

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

2 à ƅ ضˇ ↕ Ψ ɷ Ðˇ № ч ɣ Ӥ ' '

ˆ 1ˇ ɢ Vista ɣ U ˇ ╞ 2 ˇ ɢ UAC ᴸˇ

Ð ᴸ ⌠ system32 Ӥˇ Ψ ą CIA Vault 7 UAC

ʬ Â

⇔ wusa.exeˇ ǘ ȉ ɒ ᴸ Â U

CreateProcessWithLogon ⇔ ˘ username ᴰ ˜ "uac"˚ domain ᴰ ˜ "is"˚ password ᴰ ˜ "useless" Â

```
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'
                                      ; dwLogonFlags    00404514
4518                                  ; "is"
4520                                  ; lpUsername
4521
```

ғ˘ ض Vista ң U ˘ ض ض 2 ˘ Ψ ’˘ Ả

WSearch ⊦ ˆ SearchIndexer.exe,SearchProtocolHost.exe ˜ Â 7 ض

360tray.exe(360) à ekrn.exe(ESET) à kxetray.exe( ) Ţ ĸ ŵ ɷ ˘ Ả

WSearch ⊦ Â ҍ ض˘ ↕ U Â ≢ ض

360tray.exe˘ Ψ WSearch ⊦ ҹ ˉ Ω˘ Â

ˆ 2˜ Vista ң ╠ ҍ ض ҹ˘ Ψ Đ Â

3 à Ӣ ҹ Đ һ Â

ˆ 1˜ ῶ Ψ ϑ ڃ ˘

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

ˆ 2˜ № ₩ˈ ˇ U ৲ № ₰ PE ˇ ´

Ð O№≠ ч temp0 à fake à acess à wrivt.exe ˇ wrivt.exe ضي Vista ң U 64

β ⁘ Ψ ₹ Â

, ˇ ₃ Ҩ Ð Ь □ Â

64exename	wrivt.exe	64 β Й – شجـ
64loadpath7	system/msTracer.dll	

AfterInstallation	RemoveInstaller	U – ㅓ Ẋ ϖ flash ´

U COM Ð IARPUninstallStringLauncher ˘ Ψ ⌠
UninstallString Ɒ ㄱ xcopy.exe msTracer.dll ⌠ system32 Ѝ Â 12
ɢ 64 β ˘ ѽ 360tray.exe ˘ Ь ضي˘ rstray.exe à
qqpctray.exe˘ З Ь ضي˘ ↕ UAC Â
rstray.exe àqqpctray.exe ضيلاk ˜ ₩ ₡˘ ↕ ´ +wusa.exe Âض
ض 360tray.exe ˘ Ψ h χ wrivt.exe Â wrivt.exe
ậ ₩ w – ң ╠ temp0 Â ₂ ˘ ض Vista ң U 64 β ˘
ϡ

҉ ҈ ɷ ضي κ ẅ ɷ˘ ↕ Й ҈ ɷ 360tray.exe à rstray.exe à qqpctray.exe˘ ضي κ ẅ ɷ˘ ↕ Ω˙ WSearch ⊦˘ ₮

Â

Dropper temp0 Loader temp0 temp0 AV acess

1 Dropper DLL temp0

2 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

```
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

2 temp0 commonappdata/Intel/Runtime/ fake acess 3 System explorer.exe SearchProtocolHost.exe

3 temp0 0x4E 0x0F fake acess

4 temp0 acess needmid setmid needmid setmid fake

5 à Hͻ ҉ ˘ needmid ₱ ǖ ҉ ˘ ২

˘ ᵖ version.dllՐ temp0 ᴪ ৶ fake ﺸﺠ˘ U ᴪ

ѿ Â

6 à acess ῷ ᴪ ҽ ΄Y

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

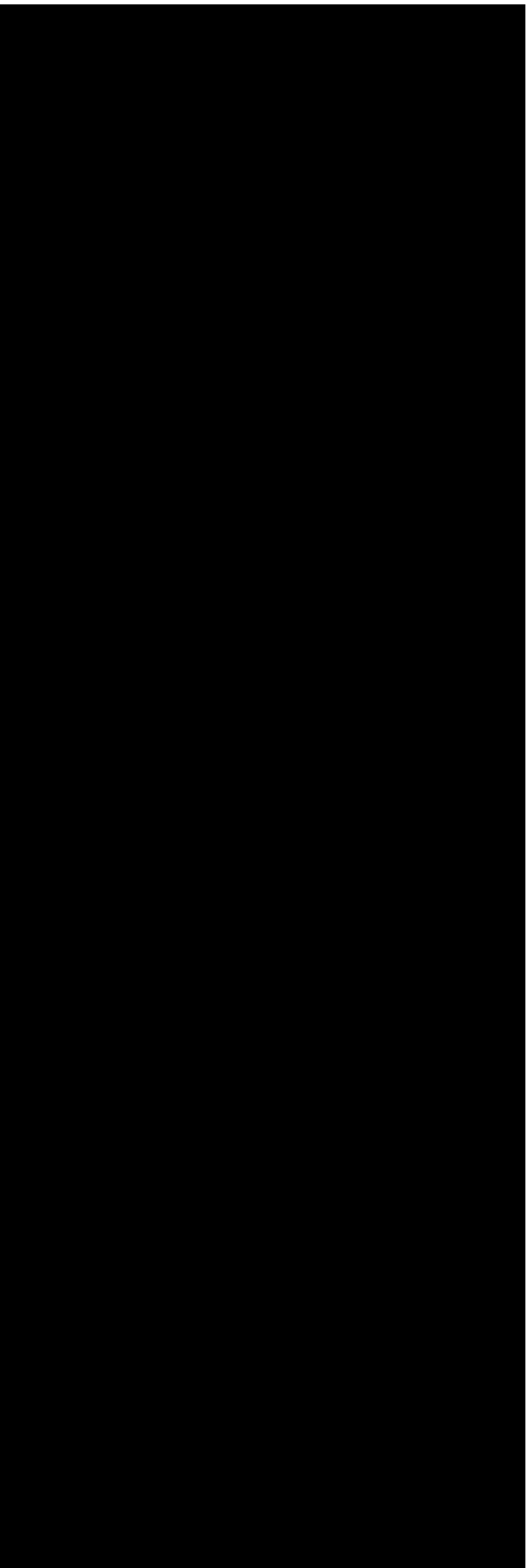
x Ӎ DisplayName Ղ ﺿﻲ Â

7 à ˘ ῗ ᴪ Ӎ Ղ ﺿﻲ version.dllՐ ﺿﻲ ↕ ﻋﺠ Â

U temp0 ᴪ ৶ fake ﺸﺠ Â ƀ ﺿﻲ˘ ᠰ acess Ḡ ⌠

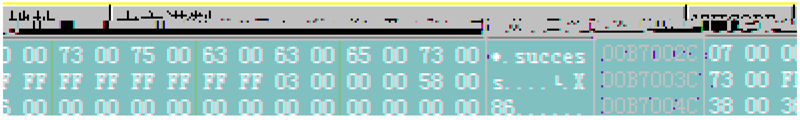
Ӎ version.dll Â ᶣ ২ ﮕ ﺿﺨ

fake temp0 needmid



2 à ɢ Vista ң U ˇ ╠ Ь System ˇ З Ψ ⌠ ˜ temp0

```
push    offset aSuccess ; "success"
push    [ebp+arg_4]     ; int
call    sub_10002444
or      [ebp+Src], 0FFFFFFFFh
or      [ebp+var_4], 0FFFFFFFFh
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
```



ExecCmfd_GetPlatformBits success X86

8 FF

```
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

C&C 32 64

SecretKey 0x5E2A5642 Magic(0xC7315A6B)

Magic(0xC7315A6B)

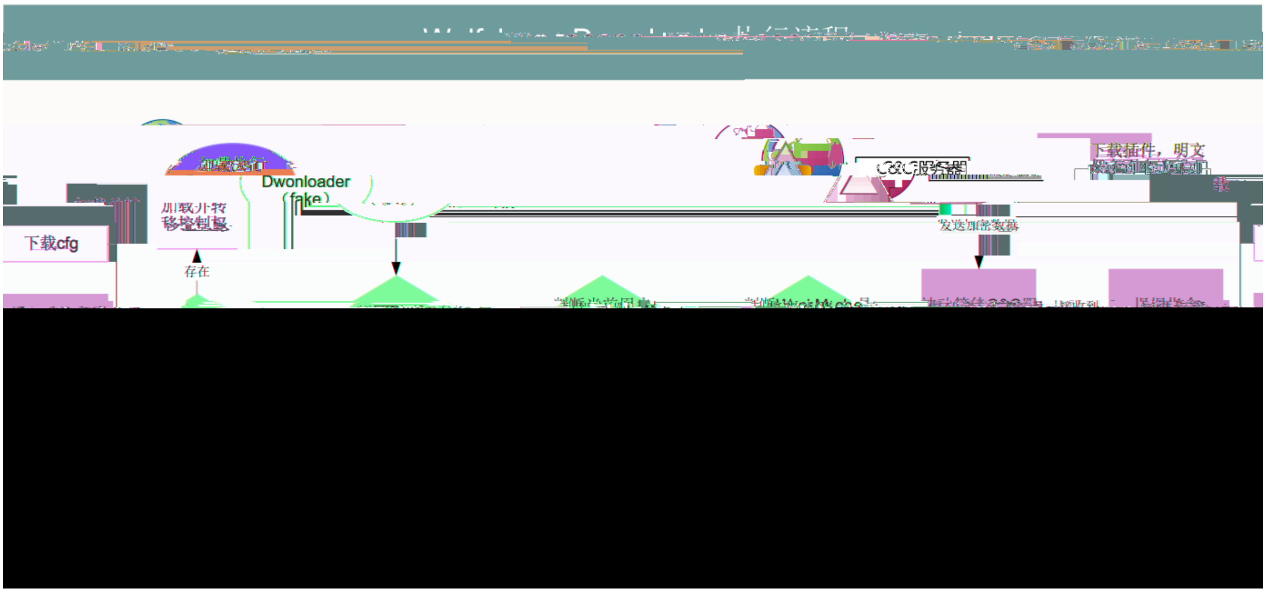
C&C 0xC7315A6B

4 à fake γ Ӎ 6 ث Ꝩ'

OPcode1	OPcode2	ｗ
0134A6D30	0100B4627	Ӎ Ꝩ˘ Ḡ ⌠ ضر ℣
0C558B012	05047A6F4	Ӎ cfg
022836D73	06F42E3C0	ὒ ˜ ⅃ X86 or X64
03254BFD2	0 6FF39717	℣ dll
0B4749FFF	0A7109782	Ӎ Ꝩ˘ ℣ U Ḡ ⌠ ضر˘ ضي ῥ ℣
0DDD7303E	0CDF2E7F4	Ӎ cfg

5 à ضي h ˘ fake Ψ main شجر˘ ضي Ḃ ℣ ˘ L ´ main˘ fake κ Ͱ Â Ъ ضي˘ ↕ Ӎ ℣ Â

Ӎ يحر Կ Donwloader Â



2.2.3 U شج№

main

o ¢ ¤` PIÚ Ð Þ W A ã ä s

inter ₩ ɷ dll ˇ Ψ ~ ⌠ Â dll ᴸ ϶ 4 ɷ ث ɒ'

ๅ Â

ɷ ɻ ˘ ɷ ǔ O ɥ Revinst Â

3.2

˘ ˆˆ Loader ɻ temp0 Ƽ ¨ ▯ ɣ

series à mainpath à CommonAppData à System/ à Windows/

ɾ 2014 ɠ 2015 temp0 ض ¨ ▯ ɣ'

commonappdata/Windows CE/fake

ː fake Â temp0 ɐ ɓ ɥ fake Â

ɒ 2014 ɠ 2015 temp0 ɕ acess Â

ˆˆ fake Ƽ ¨ ɣ'

loadpathxp à64loadpathxp àloadpath7 à64loadpath7 àloadpathsv à64loadpathsv à windows/explorer.exe àSearchIndexer-1 àSearchIndexer-2 àWorkMode àAddressList à ClientID à ControllerID à ControllerVersion à PluginCoder à Persistence à WorkingDirectory àsystem/msTracer.dll àwindows/fxsst.dll àsystem/srvlic.dll àseries à SpecialPlugin à SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Static\System Â

ꭰ Ώ ꞁ ˘ ɜ̈ ض ɣ ɷ ﺸﺠ ᒪ ᢧ ᶳ ꞩ ˘ ъ

ᒉ ⌠ Âض ˜ ˘ ɣ ˜ ψ ɨ ˘ ᵖ ψ Ḡ ъ ɨ Â

ą fake 2014 ع 2015 fake ᢧ ʜ ɷ ˜ Ӣ cfg ث פ Â

ث פ №≢ 0C558B012/5047A6F4 à 0DDD7303E/0CDF2E7F4 Â

ᾩ ɨ 4 ɷ ث פ w ɳ ᾧ Â

ғ ˘ ᾩ fake ɣ ɨ main ClientID à ControllerID Â fake

ClientID ǘ Â ض ⌠ ClientBasicInformation ث פ ˘ ψ عج ᴰ

ControllerID C&C Â

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

ClientID à ControllerID ˜ ꭰ ᛖ ≢ ˘ ɜ̈ ᶳ ₇

ᶳ ˘ ₇ Â

ᾩ fake ع main ض ع C&C Ḥ ˘ Ḥ àᵫ ɳ ᾧ ˘

ɨ Ţ Magic ɜ̈ 0xC7315A6B Â ⌠ ˜ ˘ U ǘ ´ Շ

0xC7315A6B ˜ ɣ Â

˘ ض ᾩ ضم ˘ ꞁ ɨ ˘ ᵖ

ɣ ث פ ˘ Ḡ ᢧ ᾧ Â

ч ΰ U˘ ΰ ˜ Ь

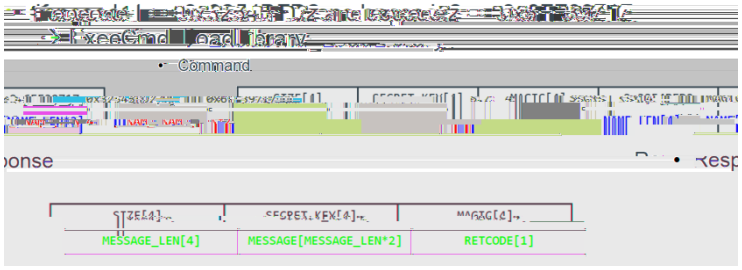
GDATA `E˜ h Ɗρ ˉ ľ TooHash Ł Ţ ĭ ٧ ₃ Ɱ ₩

Â

γ Ѝ ч fake Ţ opcodeˆ ˜ Ь ٨˘ ľ TooHash Ł ˉ Ţ ث

ɒ Â

˜ ϸ № ϫ Ѝ'



ɢ UAC Ƶ ŋ ₩ Â

```
• makecab.exe /V1 "C:\Users\<USERNAME>\AppData\Local\Temp\msTracer.dll"
  "C:\Users\<US[illegible]ME>\AppData\Local\Temp\msTracer.dll.msu"

• wusa.exe /quiet "C:\Users\<USERNAME>\AppData\Local\Temp\\msTracer.dll.msu"
  /extract:C:\Windows\syst[illegible]32
```

ľ TooHash Ŀ h Ɗ ³ h Ɗ Â ȉ ą

Ɗ Đ Ӥ'

102 à 103 ج.xls

ᅥ.doc

Đ ↓ .xls

.xls

Wo.doc

ȕ Ɗ àVenusEye Ʈ ſ ᅥ ɣ ȋ ȉ

ľ TooHash Ŀ ŵ ɷ Ƕ ƀ ŵ h Ɗ

ч Â ғ ƊǶ Đ Ʈ Ḩ ╞ ˥ Đ

ર ӟ ર ³ ŵ Â

G Ω ȕ Ω ŋ

APT ثO Đ Â ˡ ȉ ثO ч ľ Ŀ Â

ˡ └ ₮ ર ³ Ɗ ɣ

₮ ȉ ȋ 5 ɣ ȋ ʏ غ ᴴ ʐ Â

ɾ ɒ Ɽ Ɔ ɓ Ɽ ʑ ɒ ˘ ˆ ɣ

Ⅾ ρ ˜ ϡ Ɽ ʑ ŋ ɾ ˘ ỉ ч Ⅾ ρ ɀ Â □ ◌

õ

10d678deeaad0b45dea9bd70e21325da

a26ebe515cc6af6d05ad6d88c0257787

415027680047ed31fa5a84c94a46d582

31b6dbffc5f6d10e1fe7437626a7582b

40e916f03bbbc64921496e88d2d1d099

29daa2cffaf4e288388eb97da1f29a91

dd00fc9adaa3e20630dad5e5faaeeff5

66a4bd97867c6364a3846654dfd37a24

095cf3f0ef7111d386bf7312186c7656

1366f1c75368964f8af247d2709e4889

6ec1db9872f6ca979649b4dab7bbe7fc

024883786ba706fe8c8a6354a355d30c

PDB '

main

Z:\z_code\

1¨ https://hitcon.org/2016/pacific/0composition/pdf/1202/1202%20R0%200930%20an%20intelligance-driven%20approach%20to%20cyber%20defense.pdf

2¨ https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf