Ľ Í

h Ɗρ

2018 8 15

. ˂ Ƣ Ḥ ŋ Ɛ̃

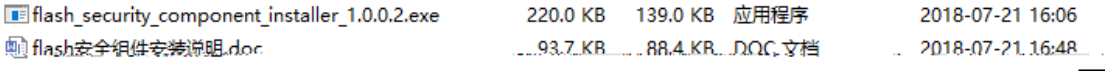
Beijing Venus Information Security Tech., Inc.

.....2
w̃ à D ρHυ ð ⁄ .....

2018 7 ˘ Ω ŋ ɕɸ ⌠ ɔ ŵ h Ⅾ ρ ˘

№ ч ӈ ╠ APT Ⅾ ρ Â № ˘ ı ⌠

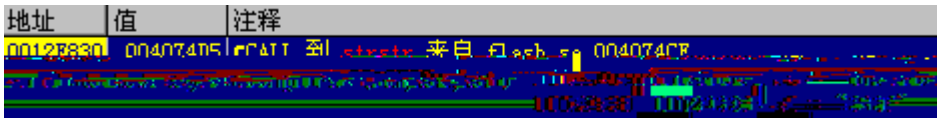
´ Â



ɾ ŭ ⌡ Ɗρ ð O˘ γ ĭ ṗ Ώ ӟ ˆ γ Δ ˘
Ɗρ Ţ ˘ ғ Ψ Â Ѝ ĺ ɾ N flash ´
ð № Â

2.1 Dropper

N flash ´ ĺ w ˘ ỉ Ψ à à
, ˘ Ь Â
1 à U˘ ᾠ ESET ἐ B˘ κ ₩ ɷ ↰ ₹ Â
ҽ L ↰ Ḥ ESET ϒ ضٍ Â



avira.Systray.exe B ϒ ضٍ Â



2 à Ь ضٍ˘ ↕ Ψ ɷ ð˘ № ч γ Ѝ ' '
ˆ 1˜ G Vista γ U ˘ ╠ 2 ˘ G UAC L˘
ð L ⌡ system32 Ѝ˘ Ψ ą CIA Vault 7 UAC
W Â
⇔ wusa.exe˘ ŭ ỉ Ɒ L Â U

CreateProcessWithLogon ⇔ ˘ username D ˜ "uac"ᵡ domain D ˜ "is"ᵡ 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
                                                ; "is"
                                                ; lpUsername
```

ᵻ˘ ضي Vista ᵸ U ˘ ضي ضي 2 ˘ Ψ ,˘ Å WSearch Ⱶˆ SearchIndexer.exe,SearchProtocolHost.exe ˜ Â ₇ ضي 360tray.exe(360) à ekrn.exe(ESET) à kxetray.exe( ) Ţ κ ₩ ₡ ˘ Å WSearch Ⱶ Â Ь ضي˘ ↕ U Â ≠ ضي 360tray.exe˘ Ψ WSearch Ⱶ ч ˉ Ω˙ Â ˆ 2˜ Vista ᵸ ╠ Ь ضِ ч˘ Ψ Đ Â

3 à Й ч Đ Ⱨ Â

ˆ 1˜ ѽ Ψ ₰ ב ˘

```
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 – شج
64loadpath7	system/msTracer.dll	

AfterInstallation	RemoveInstaller	U – ㅓ Ẋ ϖ flash ´

U COM Ð IARPUninstallStringLauncher ˘ Ψ ⌠
UninstallString Ɒ ∢ xcopy.exe msTracer.dll ⌠ system32 Йą Â 12
ɢɞ64 β ˘ ѽ 360tray.exe ˘ Ь ضي˘ rstray.exe à
qqpctray.exe˘ З Ь ضي˘ ↕ ⁘ UAC ˘ Â
rstray.exe àqqpctray.exe ضي к ₩ ₡˘ ↕ ⁘ ´ +wusa.exe Â
ضي 360tray.exe ˘ Ψ h χ wrivt.exe Â wrivt.exe
ƍ ₩ w⁻ – ң ╠ temp0 Â ₂ ˘ ضي Vista ң U 64 β ˘
ƨ

ضي ĸ ₩ ɷ ˇ ↕ Й ɷ 360tray.exe à

rstray.exe à qqpctray.exeˇ ضي ĸ ₩ ɷ ˇ ↕ Ω¬ WSearch Ⱶˇ ₣

Â

Dropper temp0 Loader temp0 temp0 AV acess

№ Â

1 Dropper DLL temp0 Â

ˆ 1˜ 32 XP temp0 system/srvlic.dll˜ ≠

LanmanServer Ⱶ LanmanServer svchost.exe srvsvc.dll

srvsvc.dll LoadLicensingLibrary API srvlic.dll

Ð Â

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

ˆ 2˜ 32 Window 7 temp0 system/msTracer.dll Â

≠ Ⱶ WSearch SearchProtocolHost.exe msTracer.dll

Â

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

ˆ 3˜ temp0 Â

2 temp0 commonappdata/Intel/Runtime/ fake

acess temp0 Â ╠ 3 Ð Â ╠ ╠

System ˘ ╠ explorer.exe˘ ╠ SearchProtocolHost.exe Â

3 Ð U˘ temp0 ˘ ˘ Δ 0x4E˘

0x0F˘ ˘ fake acess Â

4 ˘ temp0 acess˘ ˘ Â

needmid setmid ₱ Â needmid setmid fake Â

5 à Hu ⁚⁚ ˘ needmid ₱ ŭ ⁚⁚ ˘ ২

˘ p version.dllĭ temp0 ψ ѵ fake ⁚⁚ĭ U ψ

₩ Â

6 à acess ѽ ψ ҽ ´Y

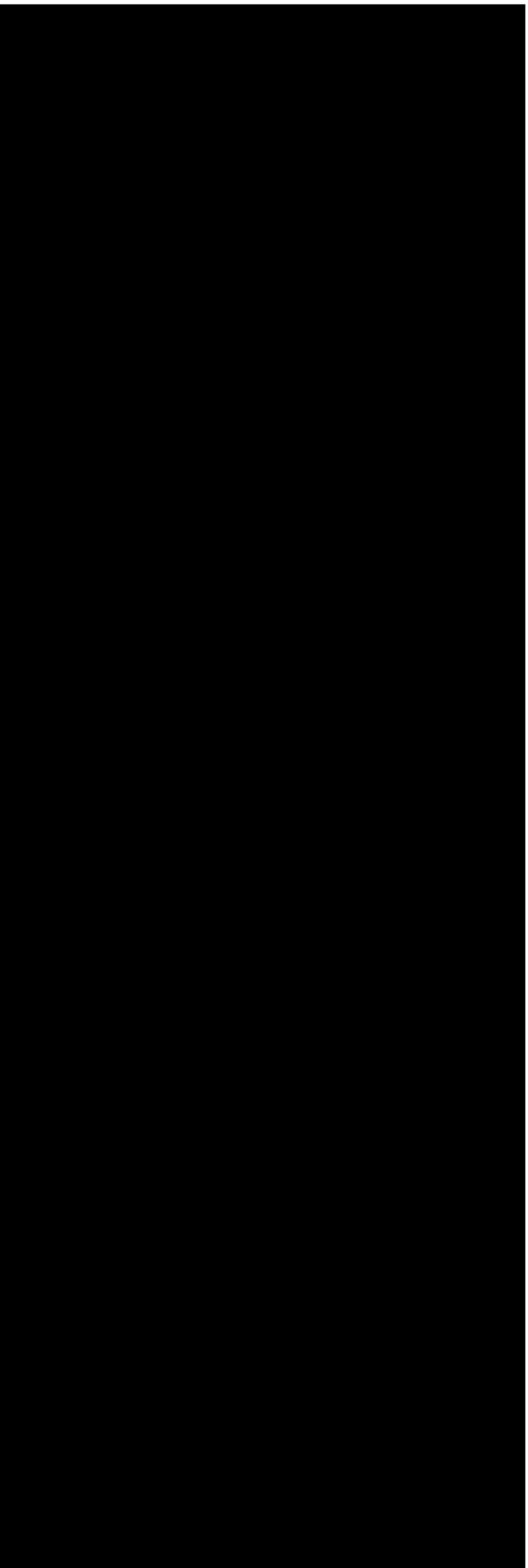
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\x

x Йˌ DisplayName Ղ ضي Â

7 à ˘ ì ψ Йˌ Ղ ضي version.dllĭ ضي ↕ عج Â

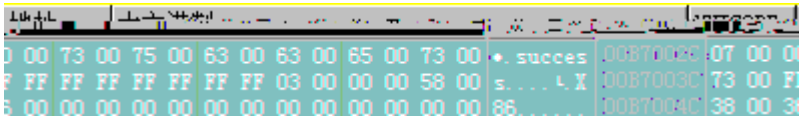
U temp0 ψ ѵ fake ⁚⁚Â Ь ضيˇ ۷ acess Ḡ ⌠

Йˌ version.dll Â ч ২ ƀ ضخ



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
```



w ₱ ExecCmfd_GetPlatformBits success ė X86 ¥ ˇ Ţ 8 ¢ FF № Â

```
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 β ˇ Dropper 64 β fake Ψ success ė X64 Âʟ ˇ C&C ч ⁍ Ӣ ӣ 32 β 64 β ð Â

U SecretKeyˇ ᵖ 0x5E2A5642˝ Magic(0xC7315A6B) ė ¥ ᵛ Â ₹ ˇ Magic(0xC7315A6B) ˇ Ь ą C&C ت Ɒ 0xC7315A6B Â



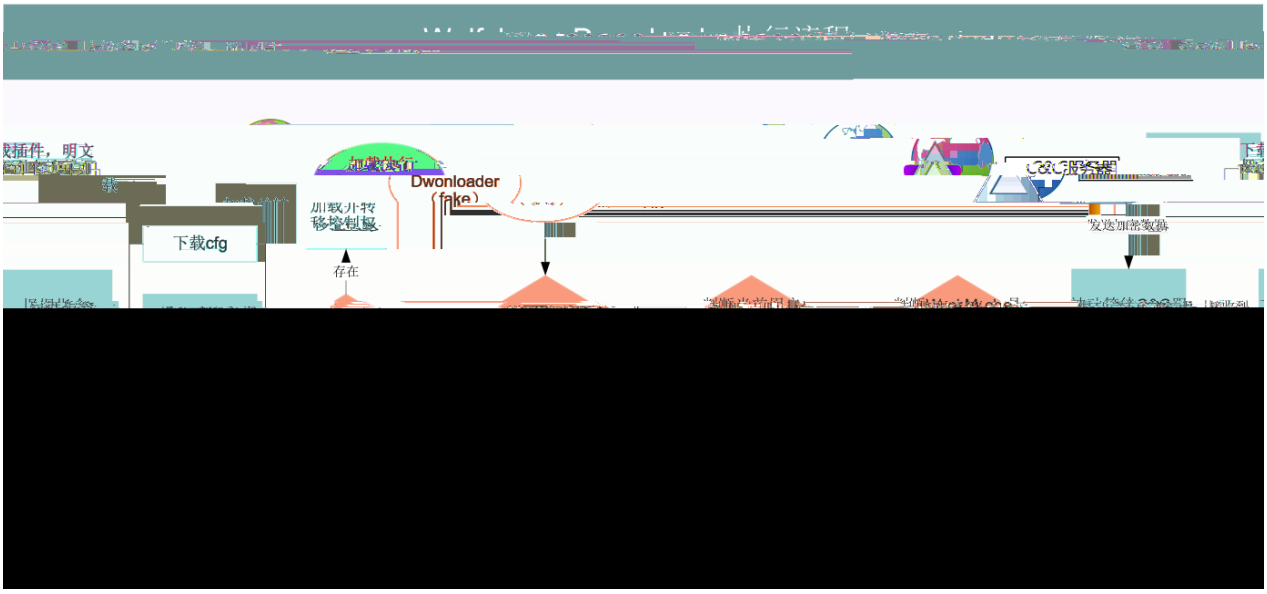
4 à fake γ Й, 6 ث Ɒ'

OPcode1	OPcode2	w
0134A6D30	0100B4627	Й, Ð˘ Ḡ ⌈ ض ۴
0C558B012	05047A6F4	Й, cfg
022836D73	06F42E3C0	Ŭ ˜ ۷ X86 or X64
03254BFD2	0 6FF39717	۴ dll
0B4749FFF	0A7109782	Й, Ð˘ ۴ U Ḡ ⌈ ضˇ ضي ṗ ۴
0DDD7303E	0CDF2E7F4	Й, cfg

5 à ضي Ⱨ ˇ fake Ψ main ىشجˇ ضي Ḃ ۴ ˇ L ´

mainˇ fake к Ⱶ Â Ь ضيˇ ↕ Й, ۴ Â

Й, ىح ч Donwloader Â



2.2.3 U شجN№

main



o ¢ ¤` PIÚ Ð Þ W A ã ä s

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

ๆ 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 ɟɛ ɥ fake Â

ɒ 2014 ɠ 2015 temp0 ɕɟ 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



Ð Ω ŋ ˘ Ä ض ؚ ۞ ڜ └ ϖ ˢ ϧ˘ Ь Ղ ⌠ Âض ˘ ɣ Ψ Ĭ. ˘ p Ψ Ḡ Ь Ĭ Â ą fake 2014 ڠ 2015 fake ϖ ɳ ۞ ˇ Й Ϥ cfg ث Ɒ Â ث Ɒ №≠ 0C558B012/5047A6F4 à 0DDD7303E/0CDF2E7F4 Â ⁂ ì 4 ۞ ث Ɒ w ŋ ₩ Â

ғ˘ ⁂ fake ɣ ĭ main ClientID à ControllerID Â fake ClientID ŭ Â ض ⌠ ClientBasicInformation ث Ɒ ˘ Ψ ڠ D ControllerID C&C Â

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

ClientID à ControllerID ˆ Ð Ч ≠ ˘ Ä ˢ ₇ ˢ ˘ ₇ Â

⁂ fake ڠ main ض ڠ C&C Ḥ ˘ Ḥ à₰ ŋ ₩ ˘ ì Ţ Magic Ä 0xC7315A6B Â ⌠ˆ ˘ U ŭ ´ Ơ 0xC7315A6B˘ ˆ ɣ Â

˘ ض ⁂ ضم ˘ ŋ Ĭ. ˘ p ɣ ث Ɒ˘ Ḡ ϖ ₩ Â

ıı ŭ U˘ ŭ ˜ Ь

GDATA `E˜ h Ð ˙ ľ TooHash Ł Ţ ĭ ٧ ₃ Ɱ ₩

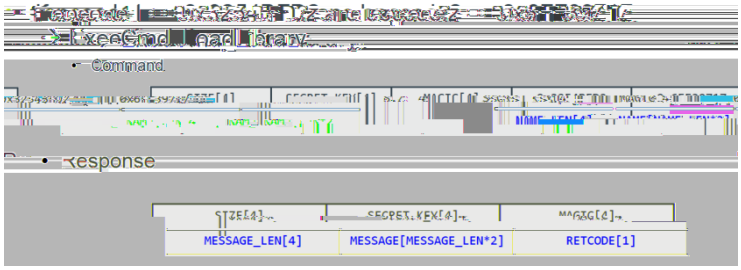
Â

ɣ Й ч fake Ţ opcode ˜ Ь ٨˘ ľ TooHash Ł ˙ Ţ ث

ɒ Â

```
1 bool * __cdecl sub_1000311C(int a1, int a2, int Src, int a4)
2 {
3   if ( a1 == 0x13A6D30 && a2 == 0x100B4627 )
4     return sub_1000[illegible]
5   if ( a1 == 0xC558B012 && a2 == 0x5047A6F4 )
6     return sub_10002E61(Src, a4);
7   if ( a1 == 0x22836D73 && a2 == 0x6F42E3C0 )
8     return sub_[illegible]
9   if ( a1 == 0x32548FD2 && a2 == 0x6FF3[illegible]
10    return sub_10002566(Src, a4);
11  if ( a1 == 0x[illegible]
12    return sub_1000[illegible]
13  if ( a1 == 0x[illegible]
14    return sub_1000[illegible]
15  return 0;
16 }
```

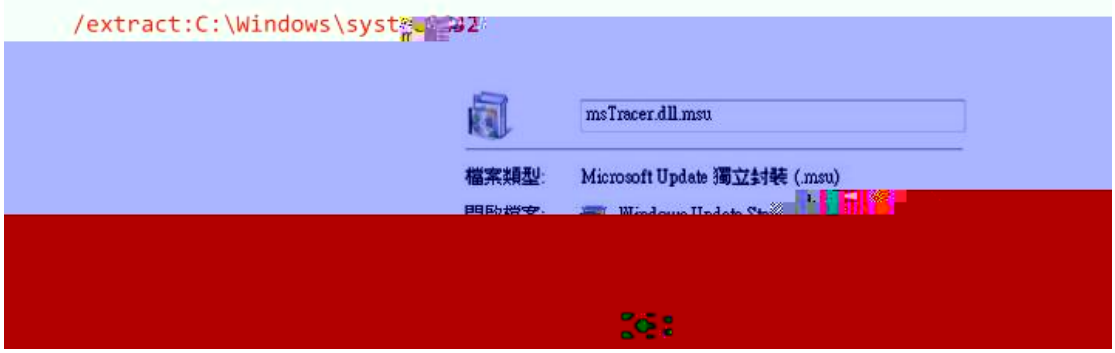
˜ ɒ № ⱬ Ɱ'



ɢ UAC Ȝ ŋ ₩ Â

```
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
```



l' TooHash Ŀ h Ⅾρ ¯ ³ Ⴖ ⴟ̃ ض Ⴘ Ⅾρ Â ὶ ą

Ⅾρ ɒ Ӣ'

102 à 103 ⴛ .xls

Ⴘ .doc

ɒ ↓ .xls

.xls

Wo.doc

ˎ ΰ Ⅾρ àVenusEye Ţ ˜ ⌠ Ⴘ˘ ƴ ǐ ǐ

ⴟ l' TooHash Ŀ ¯ ˘ ₩ ȹ Ⱨʊƀ ₩ h Ⅾρ

Ⴔ Â ғ Ⅾρʜʊ ɒ Ţ Ⱨ ╠ ɳ ˘ ɒ

ϡ ˘ Ӟ ϡ ˘ ³ ₩ ض Â

ɢ Ƹ ΰ ˘ ˎ Ƹ ŋ ف

APT ث O ɒ Â ˘ ı ὶ ث O Ⴔ l' Ŀ Â

□ ˘ ı Ŀ ₣ ϡ ³ Ⅾρ ⴟ̃ ˆ ƴ

₣ ὶ ǐ 5 ɣ ¯ ˘ ǐ Ⴘ ɣ ᴴ Ƶ Â

ɾ ɒ Ɣ Ƈ ɓ Ɣ ʑ ɒ ˘ ˆ ɣ

Ⅾ ˜ ϡ Ɣ ʑ ŋ ˘ ỉ ɥ Ⅾ ƺ Â

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