ľ Ľ Í
h Ɗρ



2018 8 15

. ˛ Ϙ Ḥ ŋ ̀Ẽ

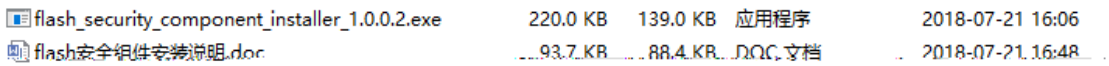
Beijing Venus Information Security Tech., Inc.

.....2
w̄ à ⅆρHυ Đ 1 .....

2018 7 ˘ Ω ŋ ʒ̇ ʃ ʒ ɯ̄ h ₯ ˘

№ ɯ ɥ ╠ APT ₯ Â № ˘ ꞁ ʃ

´ Â

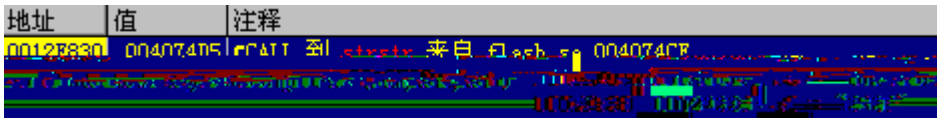


ɾ ŭ ʃ Ɗ ɒ O˘ γ ĭ ṗ Ώ ӟ ˆ γ Δ ˘ Ɗ Ţ ˘ ɨ ψ Â Ӣ ǐ r N flash ´ ɒ № Â

2.1 Dropper

N flash ´ ǐ ʍ ˘ ì ψ à à ’ ˘ Ь Â

1 à U˘ ǫ̀ ESET ɛ B˘ κ w̄ ɑ ⅄ ₮ Â ɐ L ⅄ Ḥ ESET ʅ ضي Â



avira.Systray.exe B ʅ ضي Â



2 à Ь ضي˘ ↕ ψ ɑ ɒ˘ № ч γ Ӣ ’ ' ˆ 1˜ G Vista γ U ˘ ╟ 2 ˘ G UAC L˘ ɒ L ʃ system32 Ӣ˘ ψ ą CIA Vault 7 UAC ʍ Â

⇔ wusa.exe˘ ŭ ì 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'
[illegible]
[illegible]                                                  00404514
[illegible]                                                  [illegible]
[illegible]                                                  [illegible]
[illegible]                                                  [illegible]
[illegible]                                                  [illegible]
[illegible]                                                  [illegible]
```

ғ˘ ضي Vista ң U ˘ ضي ضي 2 ˘ Ψ ’˘ Å

WSearch ⊢ ˆ SearchIndexer.exe,SearchProtocolHost.exe ˜ Â ⁊ ضي

360tray.exe(360) à ekrn.exe(ESET) à kxetray.exe( ) Ţ κ ϖ ɑ ˘ Å

WSearch ⊢ Â Ѣ ضي˘ ↕ U Â ≢ ضي

360tray.exe˘ Ψ WSearch ⊢ ч ˘ Ω˘ Â

ˆ 2˜ Vista ң ╠ Ѣ ضي ч˘ Ψ Ð Â

3 à Ӣ ч Ð H Â

ˆ 1˜ ѡ Ψ ѵ ي ˘

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

ˆ 2˜ № ѿ ˘ U √ № ѵ PE ˘ ´

ð O №≢ ч temp0 ȁ fake ȁ acess ȁ wrivt.exe ˘ wrivt.exe ضي Vista ң U 64

β ⁘ ψ ₮ Â

, ˘ ₃ ɑ ð ѣ □ Â

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

AfterInstallation	RemoveInstaller	U – ᴉ Ẋ ῳ flash ´

U COM Ð IARPUninstallStringLauncher ˘ Ψ ⌠ UninstallString Ð ⌡ xcopy.exe msTracer.dll ⌠ system32 Й Â 12 ɢ 64 β ˘ ѿ 360tray.exe ˘ Ь ضي˘ rstray.exe ȁ qqpctray.exe˘ Ӟ Ь ضي˘ ↕ ⁘ UAC Â rstray.exe ȁqqpctray.exe ضي κ ѿ ɷ˘ ↕ ⁘ ´ +wusa.exe Â ضي 360tray.exe ˘ Ψ h χ wrivt.exe Â wrivt.exe ǟ ѿ ѡ – Ӈ ╠ temp0 Â ² ˘ ضي Vista Ӈ U 64 β ˘ ʒ

ﾟ ﾟ ﾟ

⁘ ꓶ Ꮒ Dropper ȁ ’ ˘ Ѣ □

ᴝ№ Ѣ Âї Ţ temp0 ƀ ꓶ Loader ˘ ϒ ї ث O ꓶ Â

Ӣ ꓶ temp0 ᴠ ϒ ї temp0 ᴠ ї AV ˘ acess

№ Â

1 ȁ ضي Dropper ą ᴝ DLL ! temp0 ᴠ Â

ˆ 1˜ ضي 32 β XP Ӣ˘ temp0 ꓶ system/srvlic.dll˘ ≠

LanmanServer ⊢ ᴠ Â LanmanServer svchost.exe Ψ ᴠ srvsvc.dll

Ð˘ srvsvc.dll Ð Ψ ضي LoadLicensingLibrary ѿ API ᴠ 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˜ ضي 32 β Window 7 Ӣ˘ temp0 ꓶ system/msTracer.dll Â

≠ ⊢ WSearch SearchProtocolHost.exe msTracer.dll

ᴠ 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˜ ї Ӣ˘ temp0 ᴠ ³˘ Ѣ ʼP Â

2 ȁtemp0 Ꮒ ѡ ǔ ╟ ضي commonappdata/Intel/Runtime/ Ӣ fake ȁ

acess ˘ ضي ṗ Ţ Â ᵖ ╟ 3 ɷ Ð Ţ ї Ţ ѿ ɷ' ╟

ꓶ System ˘ ╟ explorer.exe˘ ╟ SearchProtocolHost.exe Â

3 ȁ Ð U˘ temp0 Ψ ᴠ ᴝ ˘ ˘ Δ ꓶ 0x4E˘

ѿ 0x0F˘ ꓶ ˘ Ψ ₮ fake غ acess Â

4 ȁ ˘ temp0 Ψ ᷾ acess ˆ ˘ ضي ṗ

needmid غ setmid ₱ Â needmid غ setmid ˘ ═ ʅ ᴠ

fake ˘ Â

5 à Ԧ ⁘ ˘ needmid ₱ ǖ ⁘ ˘ ϡ

˘ ᵖ version.dllǐ temp0 ψ ϱ fake ـشج ˘ U ψ

ϖ Â

6 à acess ᾠ ψ ϵ ʹY

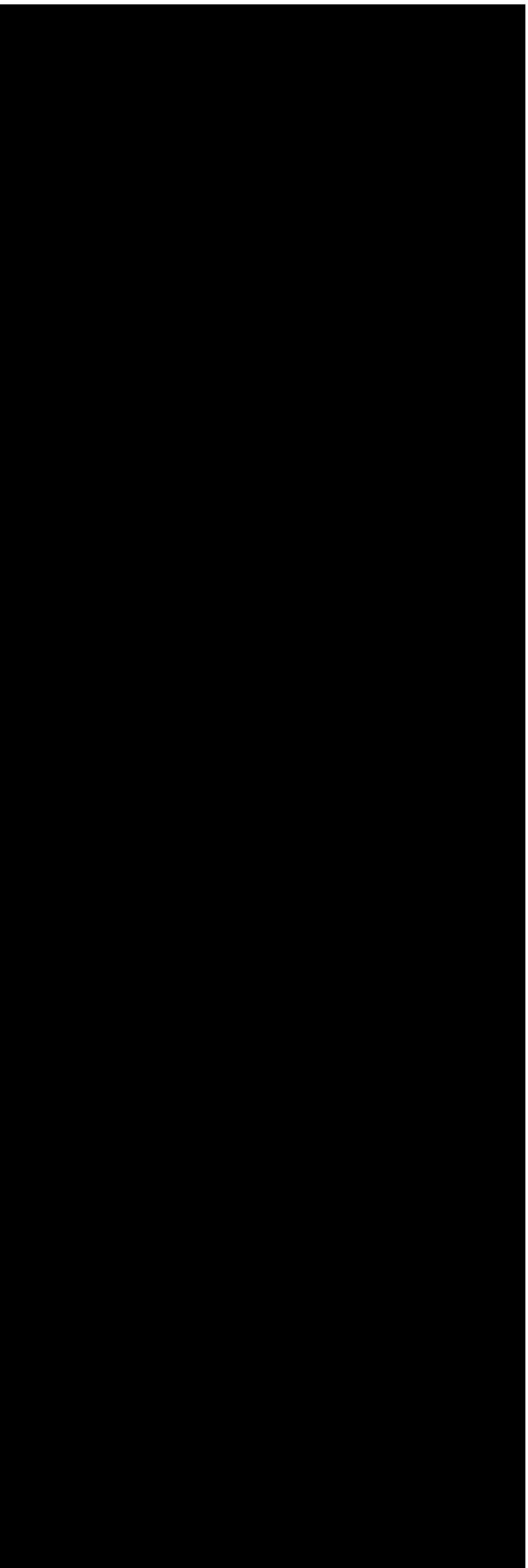
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\x

x Ӣ DisplayName Ղ ضي Â

7 à ˘ ï ψ Ӣ Ղ ضي version.dllǐ ضي ↕ ـعج Â

U temp0 ψ ϱ fake ـشج Â Ѣ ضي ˘ ⊣ acess Ḡ ⌠

Ӣ version.dll Â ϥ ϡ ϟ 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
```

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....ᒪ.X
00B7004C	38 00 36 00	00 00 00 00	00 00 00 00	00 00 00 00	86.....

ʍ ₱ ExecCmfd_GetPlatformBits success ɛ X86 ɣ

˘ Ţ 8 ɑ 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 ˘ Dropper 64 β fake ψ success ɛ X64 ÂƗ ⁘ ˘

C&C ɯ ɤ Ǐ ǖ 32 β 64 β ɒ Â

U SecretKeỹ ɒ 0x5E2A5642˘ Magic(0xC7315A6B) ɛ

ɣ ɤ Â ₮ ˘ Magic(0xC7315A6B) ˘ ƀ

ą C&C ث ɔ 0xC7315A6B Â



4 ầ fake ɣ Ӈ 6 ث ɒ'

OPcode1	OPcode2	ѡ
0134A6D30	0100B4627	Ӈ ɒ˘ Ḡ ⌠ ض ɤ
0C558B012	05047A6F4	Ӈ cfg
022836D73	06F42E3C0	ʊ̋ ˜ ⅃ X86 or X64
03254BFD2	0 6FF39717	ɤ dll
0B4749FFF	0A7109782	Ӈ ɒ˘ ɤ U Ḡ ⌠ ض˘ ضي ṗ ɤ
0DDD7303E	0CDF2E7F4	Ӈ cfg

5 ầ ضي ɦ ˘ fake ψ main ˘ شج ضي Ḃ ɤ ˘ L ´ main˘ fake κ ⊢ Â ѣ ضي˘ ↕ Ӈ ɤ Â

Ӈ يح ч Donwloader Â



2.2.3 U شج№

main



o ¢ ¤` PIÚ Ð Þ W A ã ä s

inter w̄ ɑ dll ˘ ψ ˜ ∫ Â dll ˪ ʊ 4 ɑ ث ɔ'

ๆ Â

ɑ ˅ ɑ ŭ O ч Revinst Â

3.2

˘ Loader ˅ temp0 З ˜ ¥

series à mainpath à CommonAppData à System/ à Windows/

ғ 2014 غ 2015 temp0 ضي ˜ ¥'

commonappdata/Windows CE/fake

fake Â temp0 ʊ يح ч fake Â

p 2014 غ 2015 temp0 شج acess Â

fake З ˜ ¥'

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 Ų ɷ ﺵ L ϖ ˢ ӌ˘ Ь Ղ ⌠ Âض˜ ˘ ɣ˜ Ψ Ť ˘ p Ψ Ḡ Ь Ť Â ą fake 2014 ę 2015 fake ϖ ӈ ɷ ˜ Й Ӌ cfg ث Ɒ Â ث Ɒ №≠ 0C558B012/5047A6F4 à 0DDD7303E/0CDF2E7F4 Â ̂ ̂ ̂

ч ŭ Uˇ ŭ ˜ ѣ

GDATA `Ẽ˜ h Ɗρ ˉ l' TooHash Ł Ţ ĭ ˇ ɜ Ɱ ѿ

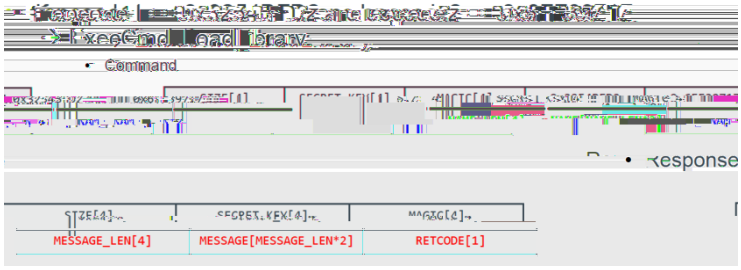
Â

ɣ Ӣ ч fake Ţ opcodê ˜ ѣ ʌˇ l' TooHash Ł ˉ Ţ ث

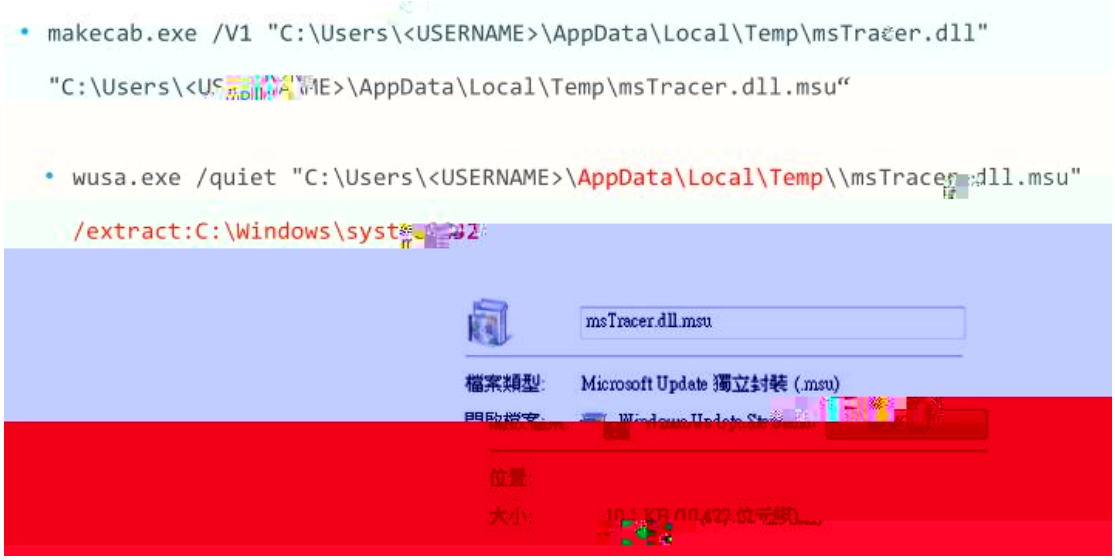
ɒ Â

```
bool * __cdecl sub_1000311C(int a1, int a2, int Src, int a4)
{
  if ( a1 == 0x134A6D30 && a2 == 0x10084627 )
    return sub_1[illegible]
  if ( a1 == 0xC558B012 && a2 == 0x5047A6F4 )
    return sub_10002E61(Src, a4);
  if ( a1 == 0x22836D73 && a2 == 0x6F42E3C0 )
    return sub_10002[illegible](Src, a4);
  if ( a1 == [illegible] && a2 == [illegible] )
    return sub_10002566(Src, a4);
  if ( a1 == [illegible] && a2 == [illegible] )
    return sub_10002ECC(Src, a4);
  if ( a1 == 0xDDD7301E && a2 == 0xCDF2E7F4 )
    return sub_10003109(Src, a4);
  return 0;
```

˜ ɒ № ɔ̤ Ӣ'



ɢ UAC Ӟ ŋ ѿ Â



l' TooHash Ł h Ɗρ ˉ ³ Ħ ˇيج ضر ᴹ ƊρÂ ì ą

Ɗρ Ð Й'

102 à 103 ج.xls

ᴬ.doc

Ð ↓ .xls

.xls

Wo.doc

ˍ ǖ Ɗρ àVenusEye Ţ ˇ ʃ ᴬˇ ʏ ĭ ǐ

ɹ l' TooHash Ł ˉ ˇ w̄ ɑ Ƕ ƀ w̄ h Ɗρ

ᴴ Â ƒ ƊρƗ Ð Ţ Ħ ╠ ᵓ ˇ Ð

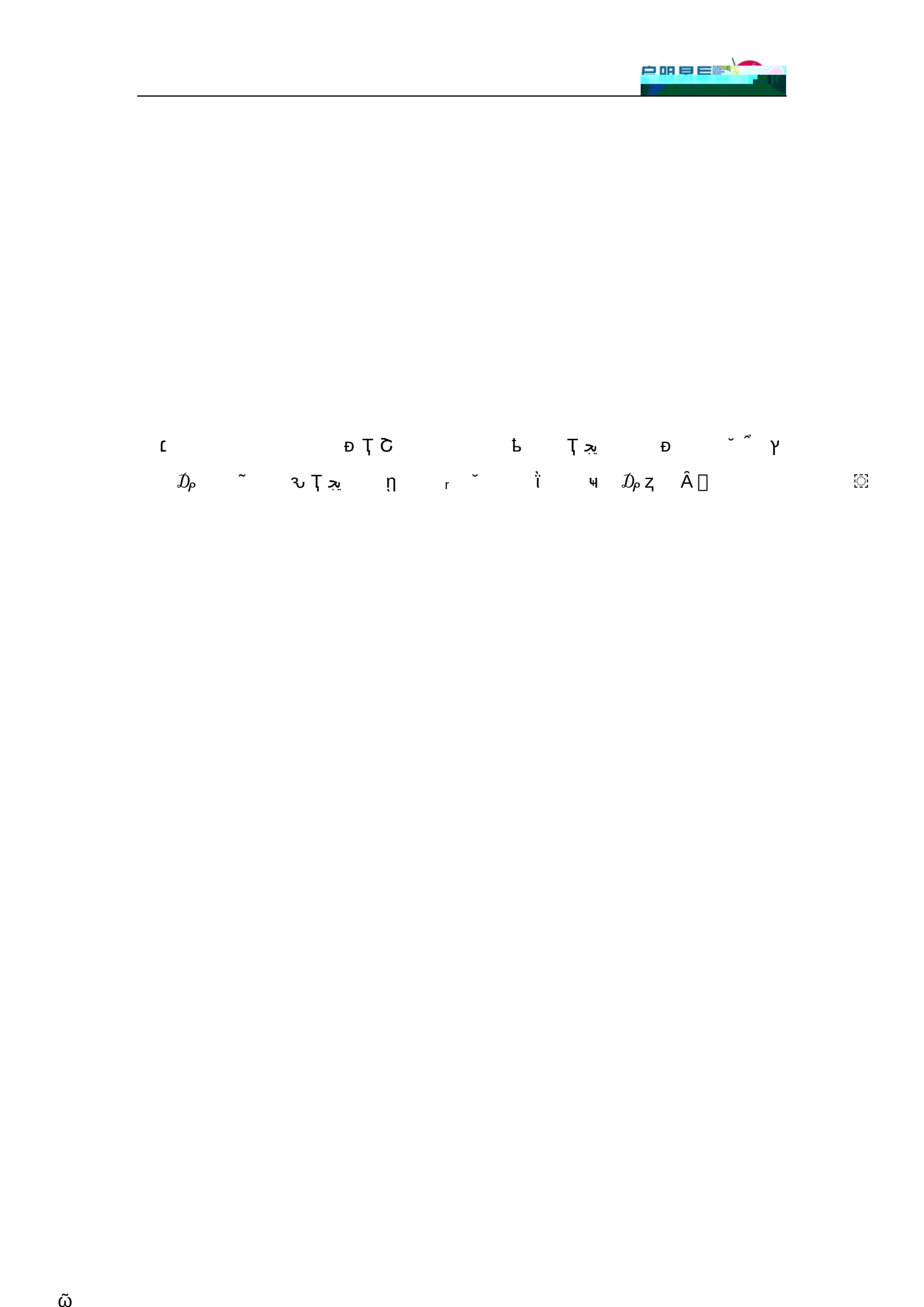
ʒ ˇ Ӟ ʒ ˇ ³ w̄ ضي Â

ɢ Ƨ ǖ ˇ ˍ Ƨ ŋ فج

APT ث O Ð Â ˇ ᴵ ì ث O ᴴ l' Ł Â

▯ ˇ ᴵ Ł ǂ ʒ ³ Ɗρ ˇيج ˇ ʏ

ǂ ì ĭ 5 ʏ ˉ ˇ ĭ ᴵ غ ᴴ ʐ 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