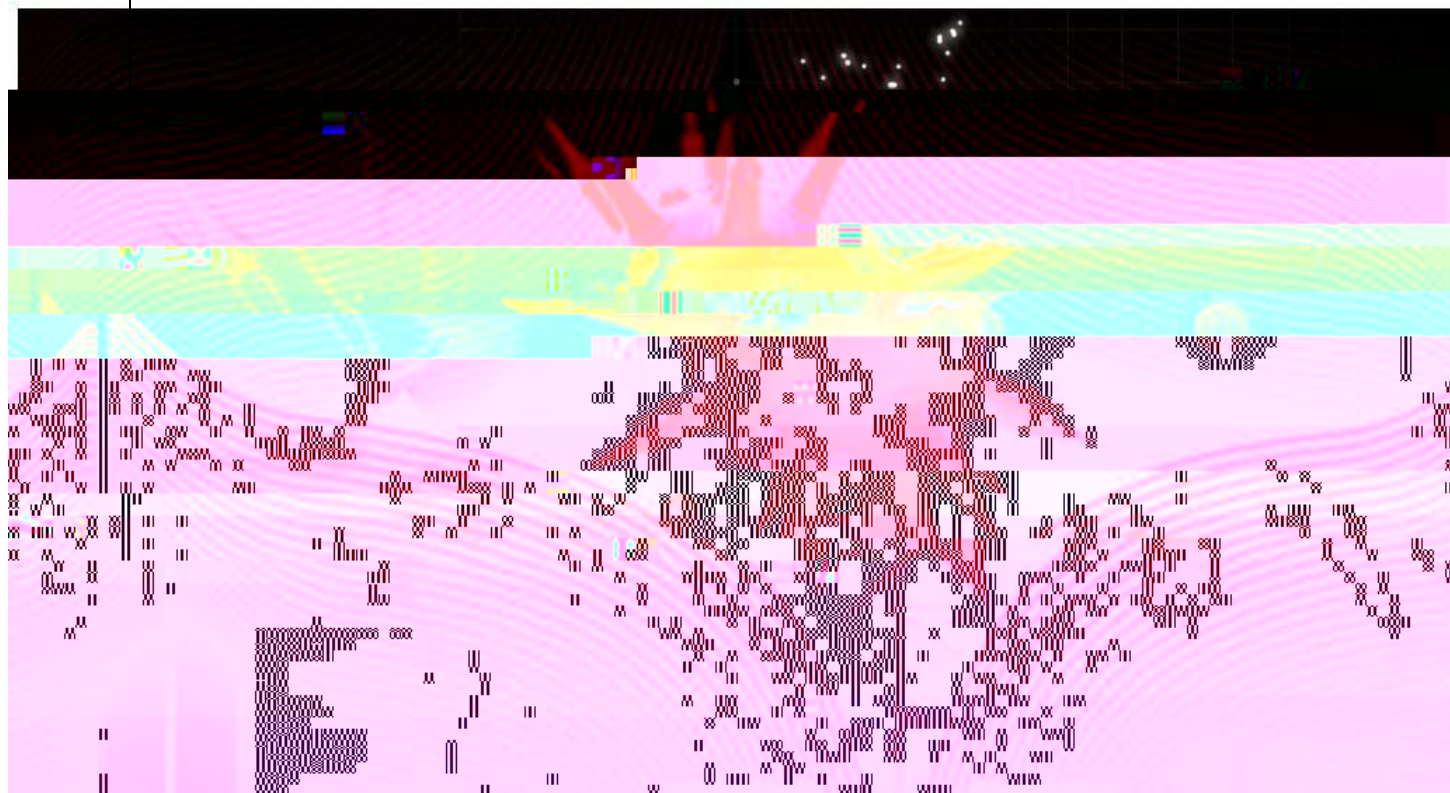


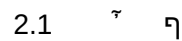


·	Др	Р	і	13.....	4
Н.					5
2.1	0x01.	№			5
2.2	0x02.	Shellcode №			9
2.3	0x03.	PE dump №			10
·					12
	APT	ао	γ		12
·		APT	ао		13
4.1		APT ^{ао}	=		13
4.2	Г	VenusEye	η		

2.1	τ η	5
2.2	$\mathcal{L}$ $\mathfrak{D}$ $\mathfrak{U}$	6
2.3	Δ TabStrip $\mathfrak{D}$	6
2.4	TabStrip $\mathfrak{D}$ ControlTipText	6
2.5	shellcode	7
2.6	$\mathbb{P}$ $\mathfrak{I}$	7
2.7	RtlMoveMemory shellcode.....	7
2.8	EnumCalendarInfoW $\mathbb{P}$	8
2.9	EnumCalendarInfo $\mathbb{P}$	8
2.10	EnumCalendarInfoW $\mathbb{P}$ shellcode $\mathfrak{b}$ $\mathbb{P}$ $\mathfrak{D}$ $\sim$	8
2.11	EnumCalendarInfoW $\mathbb{P}$ $\sim$ $\circ$ η	8
2.12	EnumCalendarInfoW $\mathbb{P}$ shellcode	9
2.13	Shellcode	10
2.14	C&C $\mathcal{L}$ $\mathfrak{D}$	11
3.1	$\mathbb{P}$	12
3.2	$\sim$	12

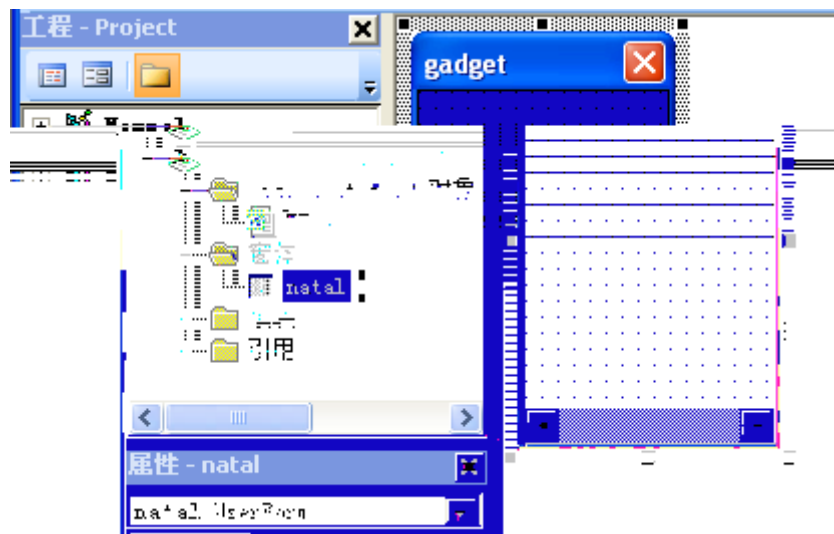
8a96e3e9abb307f3616cd

1 7

[illegible]

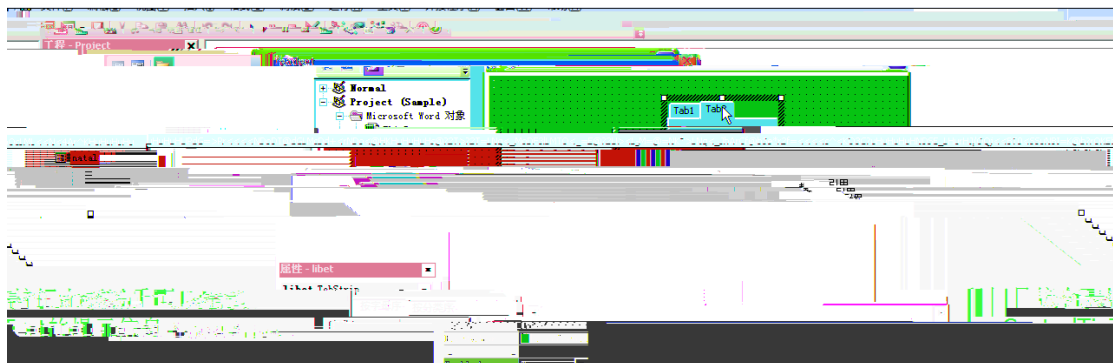
2.2 工 程 的 创 建

3 natal 工程 的 创建 和 添加 TabStrip 控件



2.3 添加 TabStrip 控件

4 在 natal 工程 中添加 ControlTipText 属性 和 添加 TabStrip 控件



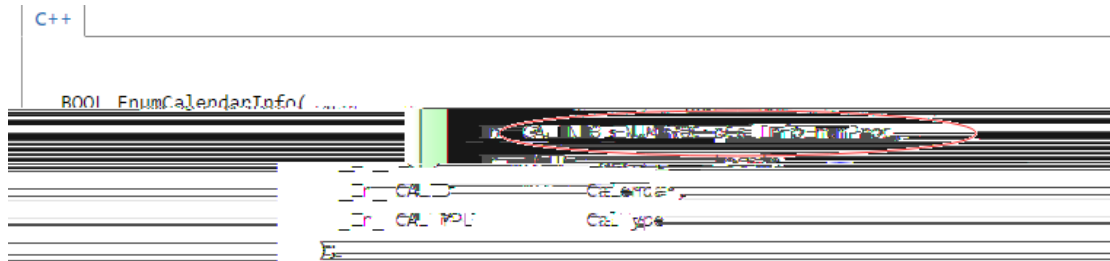
2.4 TabStrip 控件 的 属性 设置

5 ControlTipText 属性 的 设置 和 添加 Shellcode 控件

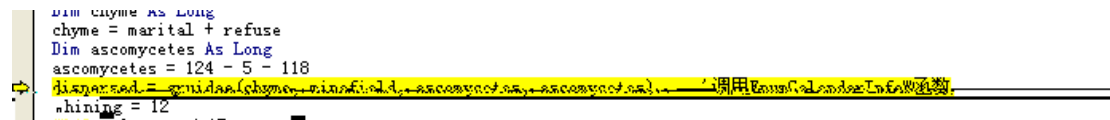
2.5 shellcode

6 RtlMoveMemory VirtualAllocEx

2.8 EnumCalendarInfoW

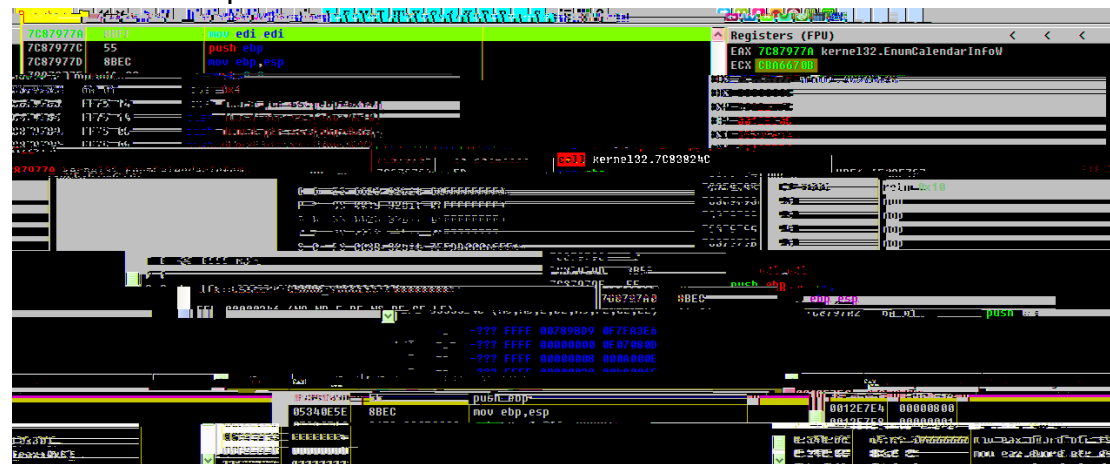


2.9 EnumCalendarInfo



2.10 EnumCalendarInfoW shellcode

9 a v | EnumCalendarInfoW ~ 3
shellcode 7



2.11 EnumCalendarInfoW ~ 0 7

2.2 0x02. Shellcode

Shellcode H ll 7 p PE a

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	05	1F	55	3B	05	33	39	0D	12	45	49	18	3F 62 65 38	
05120100	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120110	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120120	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120130	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120140	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120150	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120160	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120170	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120180	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120190	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051201A0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051201B0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051201C0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051201D0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051201E0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051201F0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120200	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120210	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120220	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120230	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120240	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120250	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120260	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120270	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120280	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120290	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051202A0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051202B0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051202C0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051202D0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051202E0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051202F0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120300	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120310	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120320	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120330	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120340	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120350	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120360	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120370	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120380	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120390	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051203A0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051203B0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051203C0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051203D0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051203E0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051203F0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120400	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120410	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120420	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120430	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120440	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120450	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120460	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120470	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120480	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
05120490	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051204A0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051204B0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051204C0	11	11	11	11	11	11	11	11	11	11	11	11	11 11 11 11	
051204D0	11	11	11	11	11	11	11	11	11	11	11			

. mû

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 $\mathfrak{A}$ $\mathfrak{G}$ $\mathfrak{M}$ $\mathfrak{V}$ $\mathfrak{N}$ $\mathfrak{D}$ $\mathfrak{I}$ $\mathfrak{V}$
 $\mathfrak{G}$ $\mathfrak{P}$ $\mathfrak{U}$ $\Leftrightarrow$ $\mathfrak{A}$ $\mathfrak{G}$ $\mathfrak{Z}$
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
 $\mathcal{D}_p \mathfrak{H} \mathfrak{D}$ $\mathfrak{A}$ $\sim$ 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
 $\mathcal{D}_p$



4.2 VenusEye

VenusEye η ∞ №

η Η ϑ

№ L № ψ ω

∞ ÿ ʘ A

~ № ƒ № ƒ

= L ↑

VenusEye η ̈́ ̈́ ̈́

“ ” Đ ρ z ´ H-worm

№ Hedwig №

Locky Đ ρ №

№ 3 18

γ SandWorm γ

Đ ρ № M M η №

