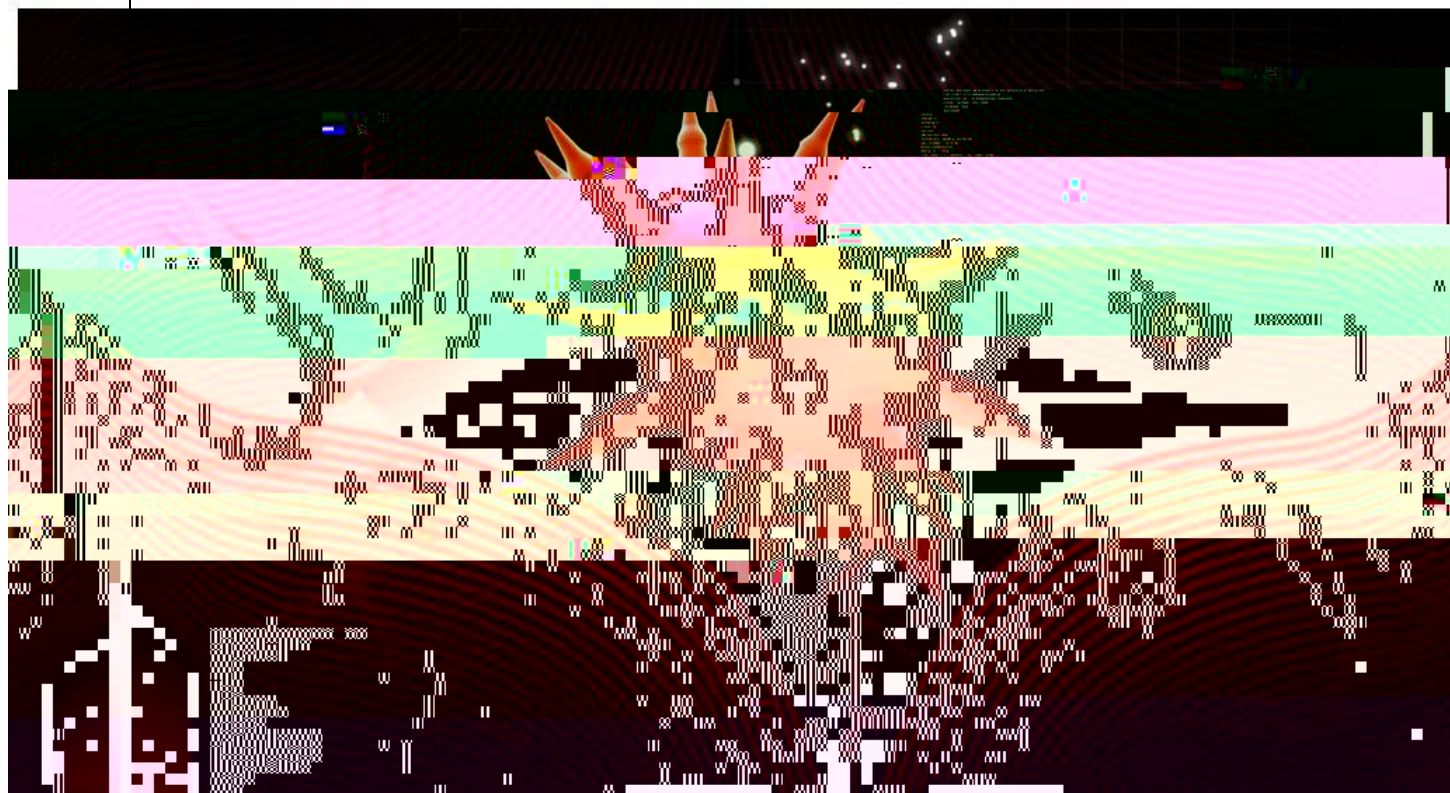




.	13.....	4
.		5
2.1 0x01.		5
2.2 0x02. Shellcode		9
2.3 0x03. PE dump		10
.		12
APT		12
.	APT	13
4.1 APT		13
4.2 VenusEye		

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



“ ”
“ ”

ToggleButton TabStrip shellcode

“ ”
“

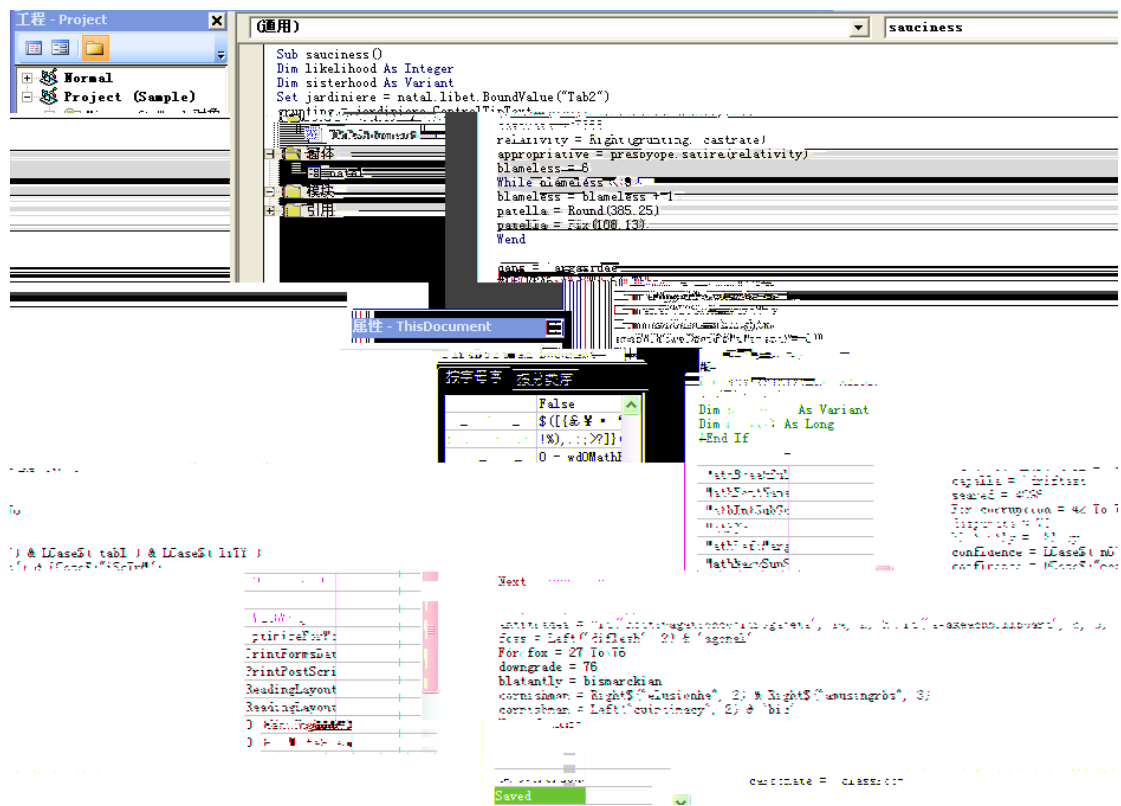
”

2016 11 08 15 00PM

sample.doc
MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

2.1 0x01.

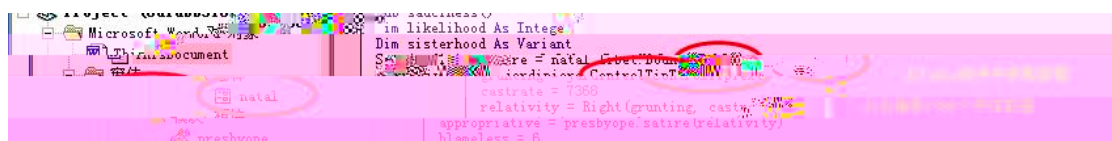
1



2.1

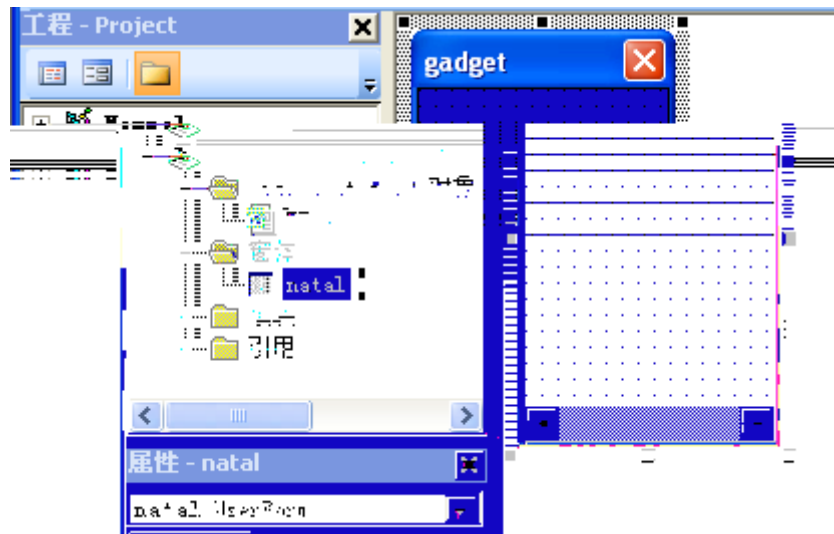
2

ControlTipText " natal " 7368 TabStrip 20161031_ ToggleButton



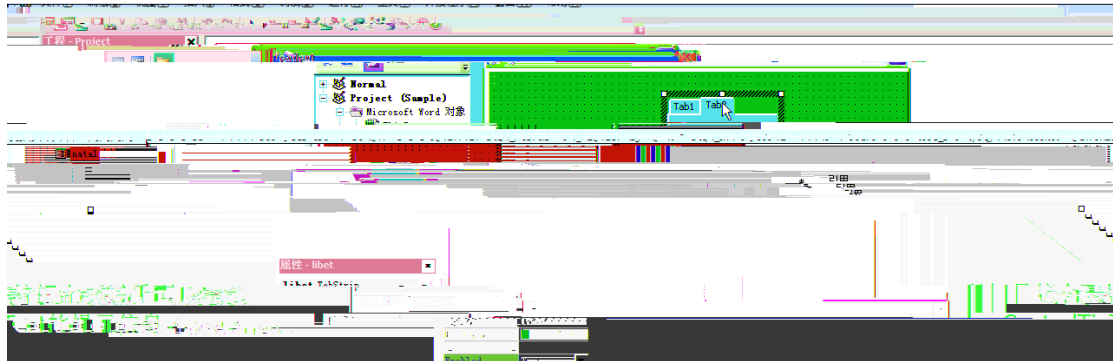
2.2

3 natal TabStrip



2.3 TabStrip

4 ControlTipText ControlTipText TabStrip TabStrip



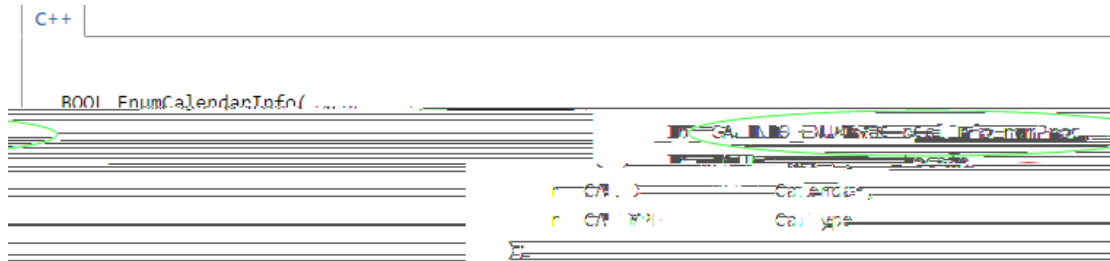
2.4 TabStrip ControlTipText

5 ControlTipText shellcode Shellcode

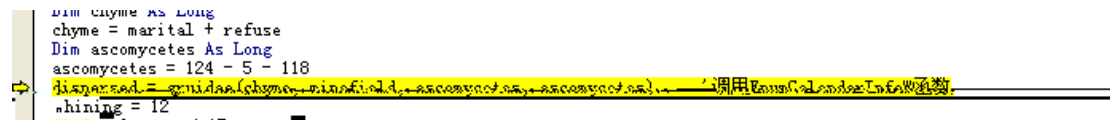
2.5 shellcode

6 RtlMoveMemory VirtualAllocEx

2.8 EnumCalendarInfoW

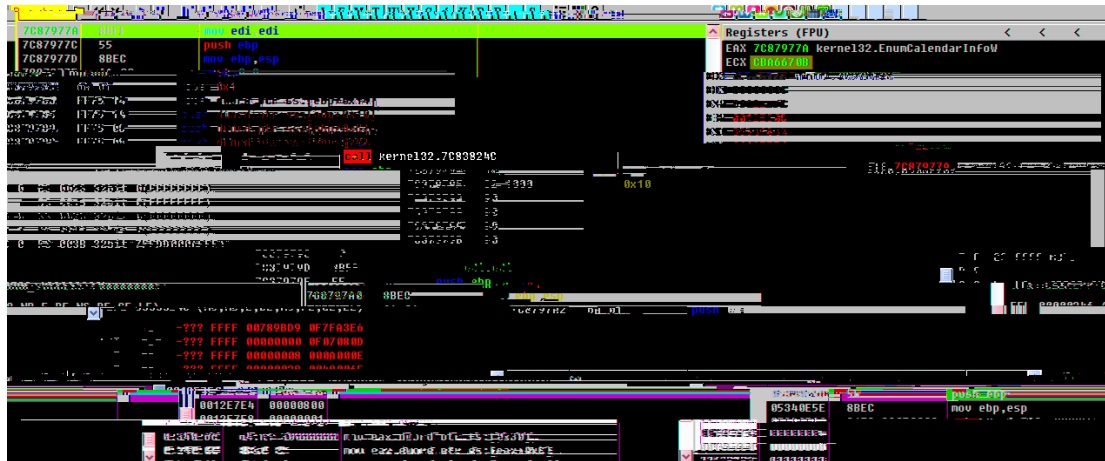


2.9 EnumCalendarInfo



2.10 EnumCalendarInfoW shellcode

9 EnumCalendarInfoW shellcode



2.11 EnumCalendarInfoW

2.12 EnumCalendarInfoW shellcode

2.2 0x02. Shellcode

Shellcode PE

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	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120100	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120110	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120120	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120130	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120140	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120150	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120160	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120170	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120180	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
05120190	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
051201A0	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
051201B0	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
051201C0	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
051201D0	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
051201E0	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A
051201F0	65	6F	65	3A	65	33	33	6D	6C	65	68	68	75 6C 65 3A	53336D6C656868756C653A

2.14 C&C

. mû

▪

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

