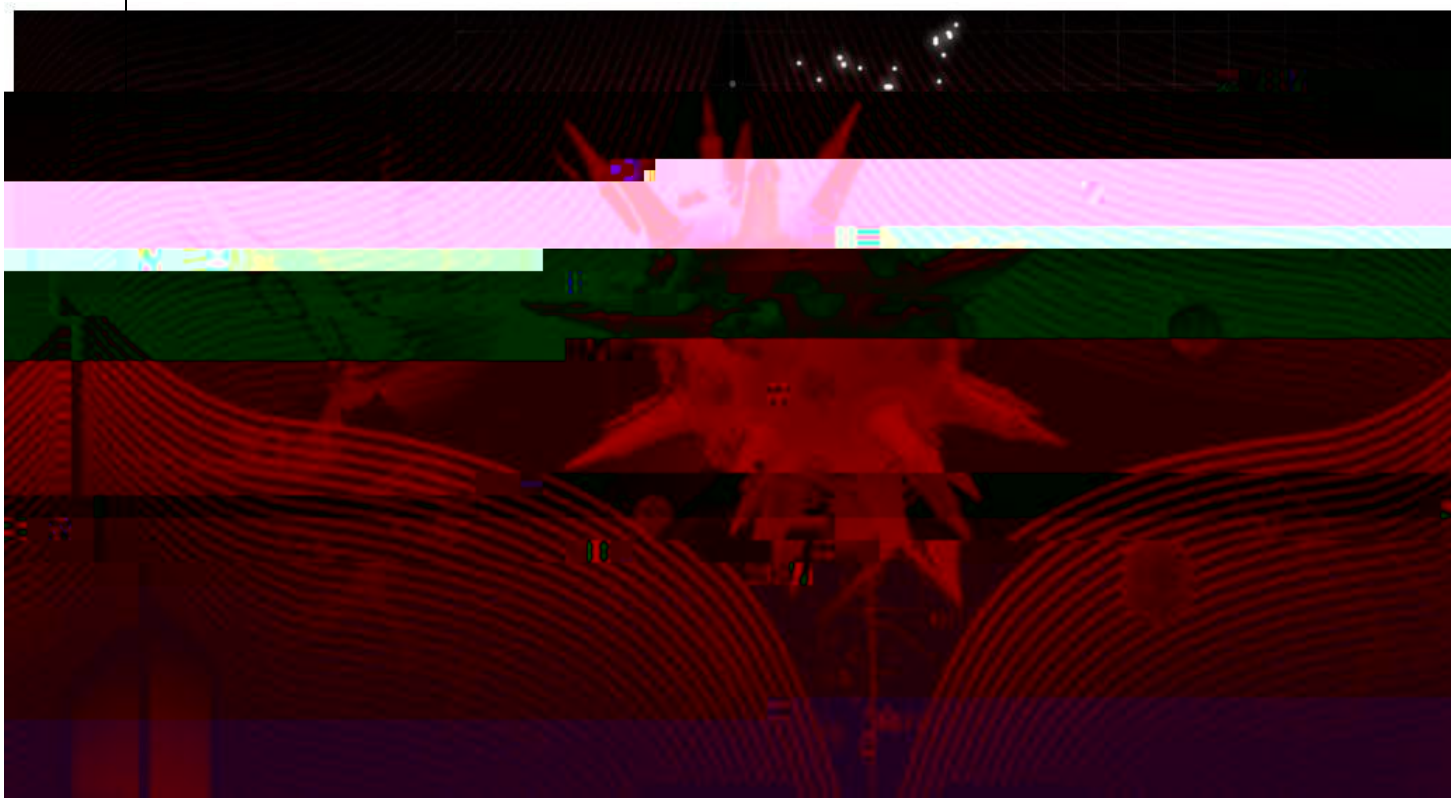


. Ⱡⱥ Ⱨ ΐ 13.....4

Ⱨ. غ .....5

2.1 0x01. ϥ № .....5

2.2 0x02. Shellcode № .....9

2.3 0x03. PE dump № .....10

. Ᵽ.....12

Ⱋ APT ᵒᵒ ج ˜ ٢ .....12

ضم. ˛ Ⱋ APT ᵒᵒ ج .....13

4.1 Ⱋ APTᵒᵒ ج ═ .....13

4.2 ˜ ɢ VenusEye ضخ ضخ ŋ ˜

يح 2.1 ˜ ๆ .....5
يح 2.2 ɾ ɒ ǚ .....6
يح 2.3 Δ TabStrip ɒ .....6
يح 2.4 TabStrip ɒ ControlTipText .....6
يح 2.5 shellcode .....7
يح 2.6 ₱ غ خي ض ǻ .....7
يح 2.7 RtlMoveMemory shellcode.....7
يح 2.8 EnumCalendarInfoW ₱ .....8
يح 2.9 EnumCalendarInfo ₱ .....8
يح 2.10 EnumCalendarInfoW ₱ shellcode ƀ عج ₱ ᴅ ˜ .....8
يح 2.11 EnumCalendarInfoW ₱ ˜ه ๆ .....8
يح 2.12 EnumCalendarInfoW ₱ shellcode .....9
يح 2.13 Shellcode .....10
يح 2.14 C&C عج ᒪ ɒ .....11
يح 3.1 ₱ يح .....12
يح 3.2 ˜ يح .....12

▪

Ǔ ↄ “ ” Ⅾρ Ƶ ´ ϼ ԋ U
ŋ ﻑ ǐ Ǔ “ ” Ⅾρ

№ Ǔ ╠ ﺽ ˆP
Ð

ϥ β ▯ ɾ TabStrip Ð Ǔ ४ shellcode
╠ ɾ ToggleButton Ð Ǔ ▯

₱ ▯ ↄ ₱ ₱
w ﻥ ﻥ Ḥ ₱ ╠ ă
³ ▯

G Y ו ∞ Ð “ ﻕ ”
ˆ Ǔ Ⅾρ G Ḥ ŋ ﺽ ŋ Ǔ
╠ ↄ ﻍ Ḥ G ﻥ ↕ ו ∞ G “
”

ו ⌠ 2016 11 08 15 00PM ˆ
Y ﺑ ρ Ð ו Ḥ `E
G ﺑ ρ ϼ

ו ˆP Ⅾˆρ Ǔ ﺑ
Ƶ

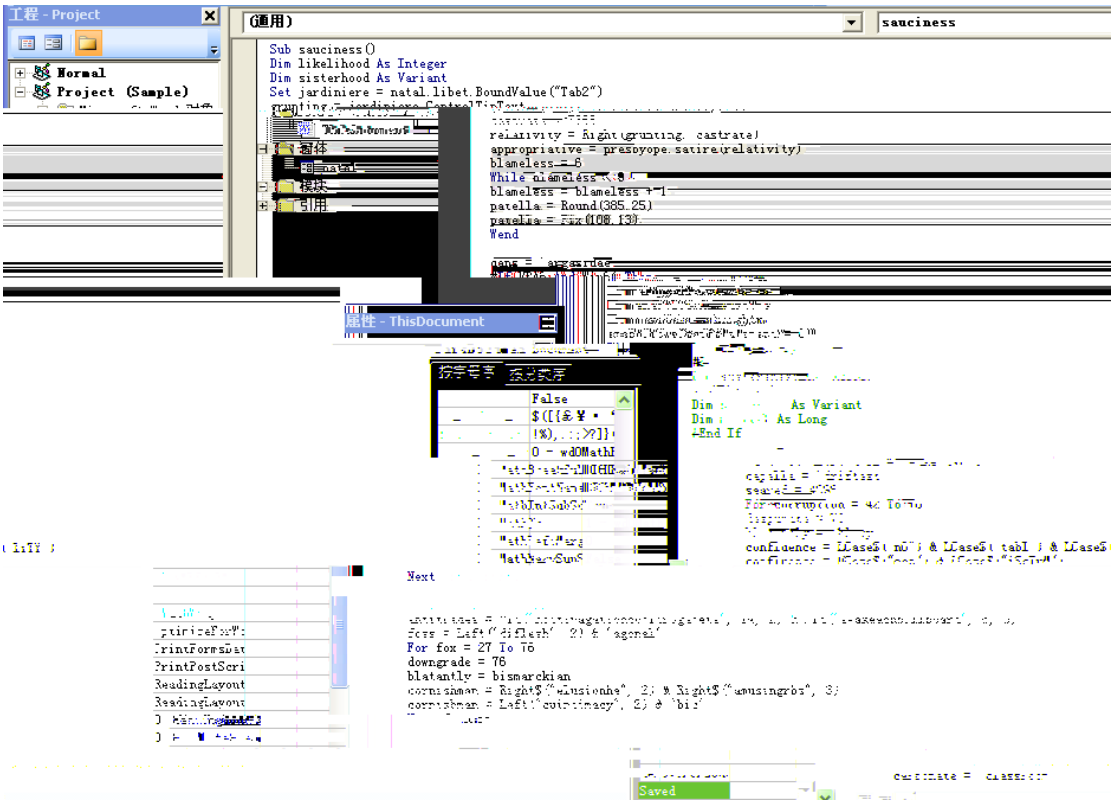
▪

O sample.doc

MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

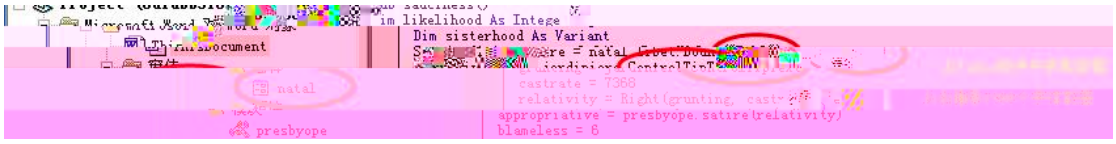
## 2.1 0x01.

1 ๆ



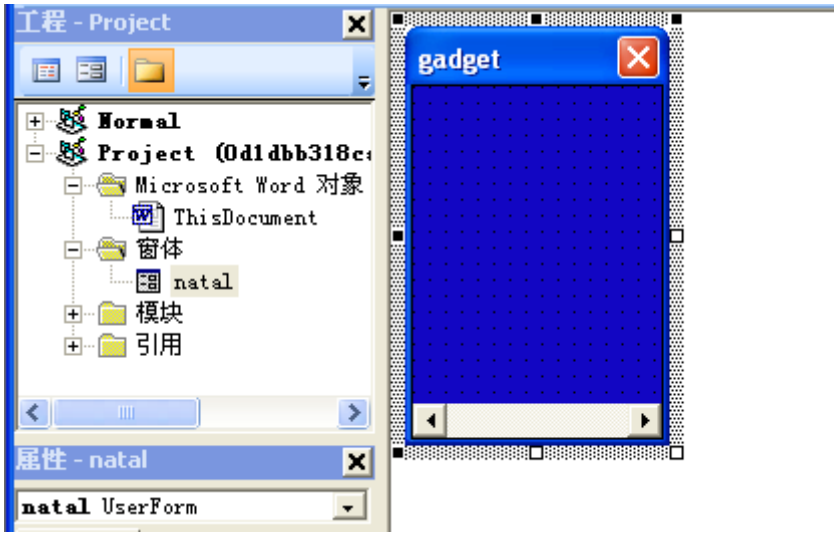

ϡ 2.1 ˜ ๆ

2 ๆ ᾠ ψ ɾ O “ natal ” ɾ TabStrip ᴅ ControlTipText ᴜ̆ ɾ ˚ ʊ ᴜ̆ 7368 20161031_ “ ” ᴅ ᴘ ᴢ ´ ʜ ╟ Ḥ ▯ ɾ ToggleButton ᴅ



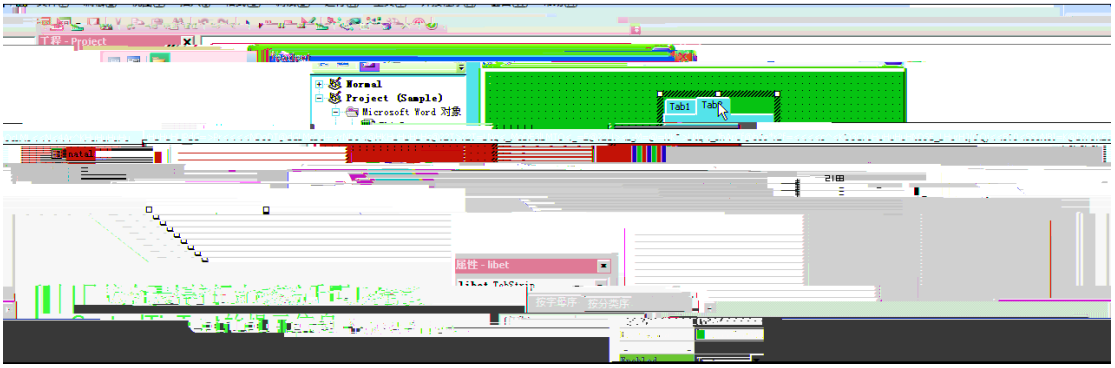
ﾒ 2.2 ﾋ ﾄ ﾜ

3 natal ｒ Δ ｒ TabStrip ﾄ.




ﾒ 2.3 Δ TabStrip ﾄ

4 d ﾘ ﾄ ضي ｒ TabStrip ﾄ ضي TabStrip ﾄ
ControlTipText ControlTipText ﾍ ﾔ Å ضي ﾄ
ﾇ ↑ Ḥ ﾍ ﾔ ﾄ Ḡ



ﾒ 2.4 TabStrip ﾄ ControlTipText

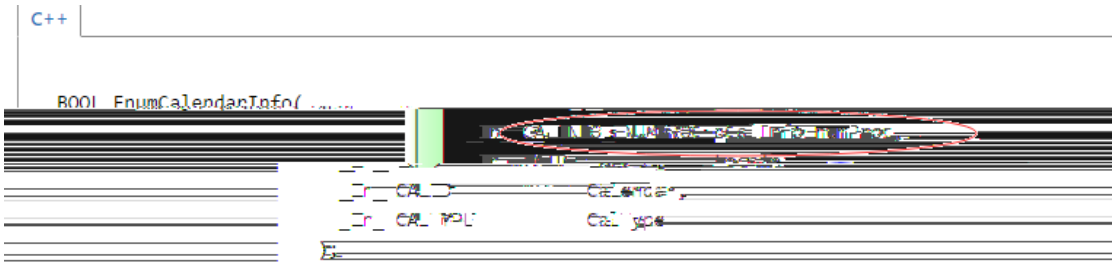
5 ControlTipText U Ḥ U ﾘ
ﾄ ﾠ ﾍ shellcode ﾗ Shellcode Ḥ ╠ G □

یہ 2.5 shellcode

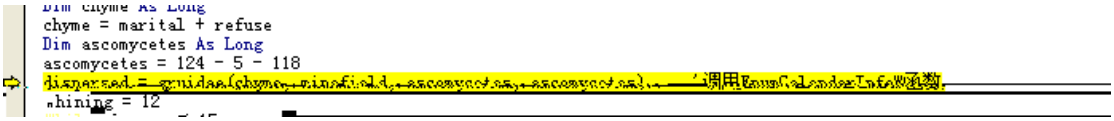
6 RtlMoveMemory غ VirtualAllocEx

[redacted]

ﾐ 2.8 EnumCalendarInfoW ₱

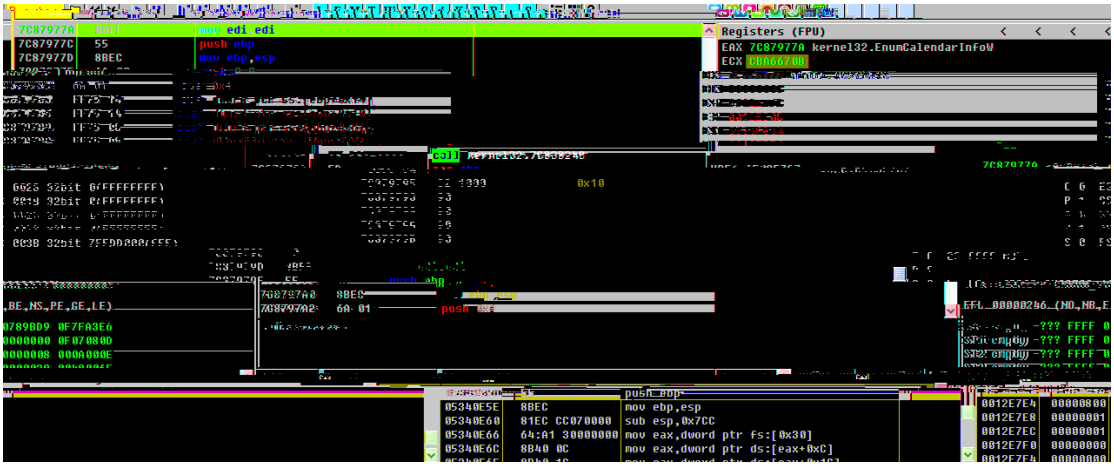



ﾐ 2.9 EnumCalendarInfo ₱




ﾐ 2.10 EnumCalendarInfoW ₱ shellcode ƀ ﾐ ₱ D ˜

9 ą ﾐ ﾐ ﾋ ﾃ EnumCalendarInfoW ₱ ˜ ﾐ shellcode ﾗ

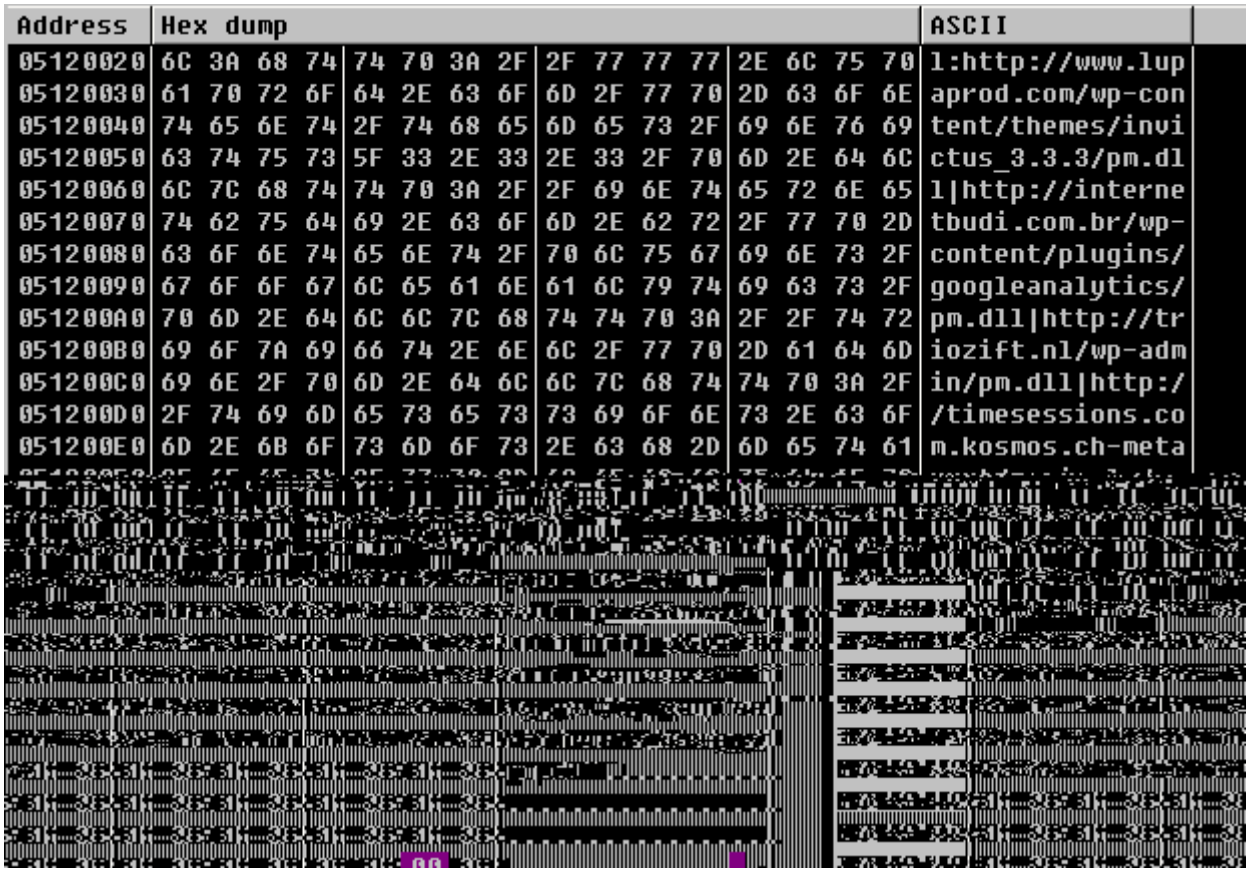



ﾐ 2.11 EnumCalendarInfoW ₱ ˜ o ﾗ

يح 2.12 EnumCalendarInfoW ₱ shellcode

## 2.2 0x02. Shellcode

Shellcode ӊ ╠ 7 ضي ṗ PE ą


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

2.14 C&C

.

# . APT

APT Ɗρ Ӈ ϒ Ӈ غج Ɗρ ΐ̣

D ɳ ~ ~ ~ ~ ~

ϒ̃ ɳ ϒ غج G ~ ϒ

~ ą ϙ غ Ɗρ ϟ Ɗρ

Ϙ APT ~ ج G ⅵ ⅵ № غ Ð ⅵ ⁚

G Ⓟ ΰ ⇔ ~ ج G Ζ

H-worm № APT Ɗρ ⅴ ~ ~ L ΰ ⅵ ~

Ɗρ APT Ɗρ Ҥ ~ ϒ Ϙ APT ~

ج ΰ 0-day ‰ β

## 4.1 APT

Ɗρ Ϙ APT ~ ج ~ ϒ

ƊρҤ Ð غ ~ ج ~ ϒ Ƨ Ɗρ Ð ضي

ϣ̃ ϙ ضي APT Ɗρ ~

Ϙ APT ~ ج ƀ ϙ ΐ

ɳ ~ ج ~ ´ ϙ Ɗρ ≢

~ 0-day ≠ Ϙ فج ΰ

↓ يج ρ̇ ϣ̈ ΐ̈ غ ˗ Ҥ

L خ ROP ≠ API Shell code

~ ϒ ₮ APT Ɗρ ▯ ~ ج ~ ⁚ ⊢ ΰ APT

Ɗρ يح




## 4.2 VenusEye

VenusEye ŋ ɟ̣ɟ̣ Ω ɟ̣ɟ̣ ˚˚ ɛ̣ №

˚˚ ɛ̣ ŋ Ɦ Ð

№ h ˡ № ɒ ψ ɯ

˚˚ ï ɣ̣ Ạ

˜ ɛ̣ № ǂ № ǂ

= ˡ ↑

VenusEye ŋ ɟ̣ɟ̣ ˙ ɷ̣ U ʊ̈ ʒ

“ ” Ɗ̣ρ ʐ ´ H-worm

№ Hedwig №

ɒ Locky Ɗ̣ρ № ɒ

№ ʒ 18

ʊ̣ ɿ SandWorm ɣ

Ɗ̣ρ№ ɒ ʍ ʍ ŋ №

ɒ

