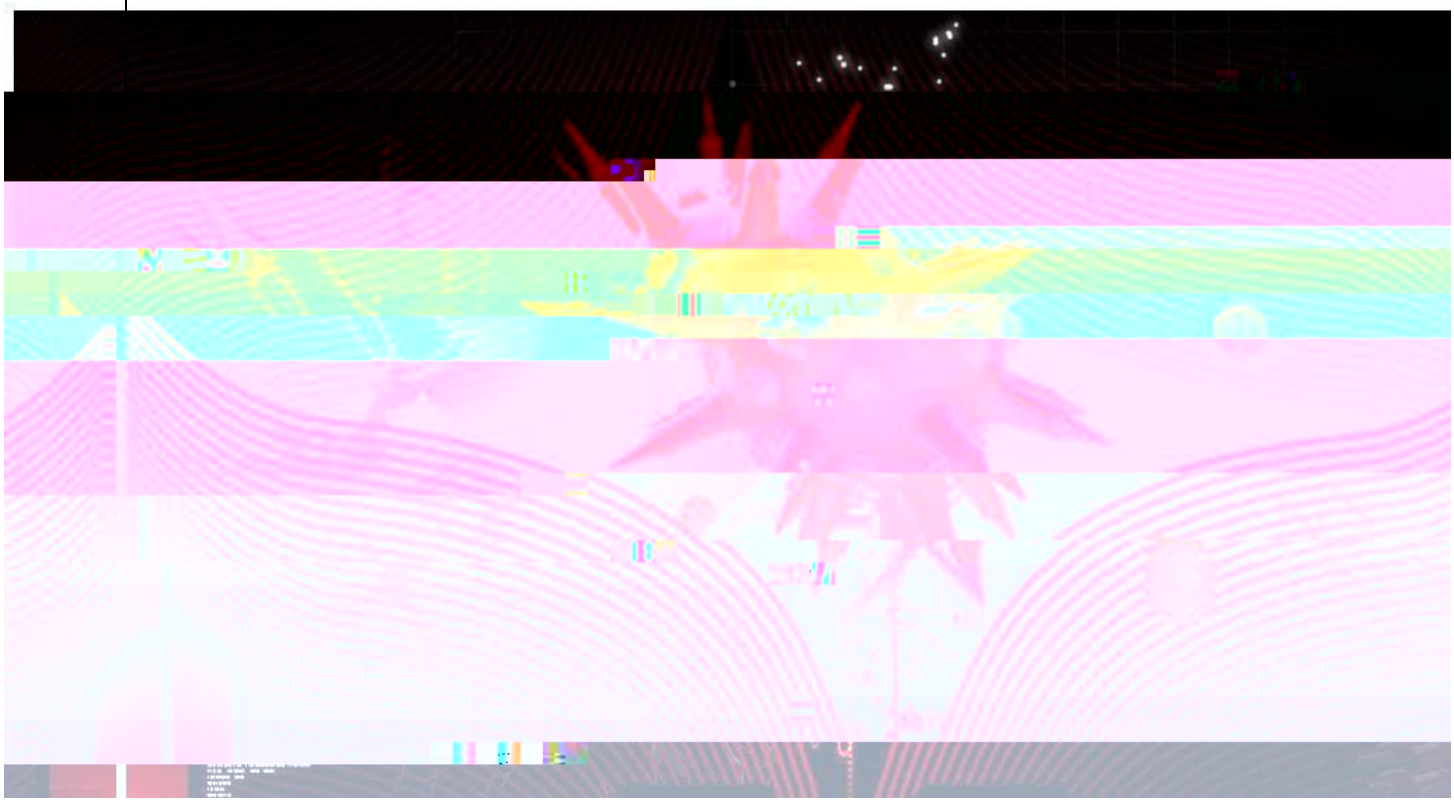


. 𝒟ρ Ꝑ ǐ 13.....4

Ꮒ. ė 5

2.1 0x01. ϥ № 5

2.2 0x02. Shellcode № 9

2.3 0x03. PE dump № 10

. ϸ.....12

Ꝋ APT ̊̊ ڃ̃ ץ 12

ᵯ. ̇ Ꝋ APT ̊̊ ڃ 13

4.1 Ꝋ APT̊̊ ڃ ═ 13

4.2 ̃ ɢ VenusEye ŋ ض ض ̃

ﻱ 2.1 ˜ ๆ 5
ﻱ 2.2 ɾ ɒ ษ๊ 6
ﻱ 2.3 Δ TabStrip ɒ 6
ﻱ 2.4 TabStrip ɒ ControlTipText 6
ﻱ 2.5 shellcode 7
ﻱ 2.6 ₱ غ خي ض أ 7
ﻱ 2.7 RtlMoveMemory shellcode.....7
ﻱ 2.8 EnumCalendarInfoW ₱ 8
ﻱ 2.9 EnumCalendarInfo ₱ 8
ﻱ 2.10 EnumCalendarInfoW ₱ shellcode ზ ﻍ ₱ ᴅ ˜ 8
ﻱ 2.11 EnumCalendarInfoW ₱ ˜ₒ ๆ 8
ﻱ 2.12 EnumCalendarInfoW ₱ shellcode 9
ﻱ 2.13 Shellcode 10
ﻱ 2.14 C&C ﻍ ㄴ ɒ 11
ﻱ 3.1 ₱ ﻱ 12
ﻱ 3.2 ˜ ﻱ 12

▪

2016 11 4 Ũ ২ “ ” Ⅾρ Ƶ ´ ϸ ԋ U
VenusEye ŋ ﻑ ǐ Ũ “ ” Ⅾρ

№ Ũ ╠ ﺽ □ ˆ ˙P
Ð

ϖ β □ ɾ TabStrip Ð Ǔ ४ shellcode
╠ ɾ ToggleButton Ð Ǔ □

₱ □ ২ EnumCalendarInfo ₱ ₱
w ሃ ሃ Ḥ ₱ ╠ EnumDateFormats ă
³ □

ɢ Ƴ ו ∞ Ð “ ﺝ ”
ˆ Ũ Ⅾρ ɢ Ḥ ŋ 0-Day ﺽ ŋ Ũ
╠ ২ ﻍ Ḥ ɢ ﾉ ↕ ו ∞ ɢ “
”

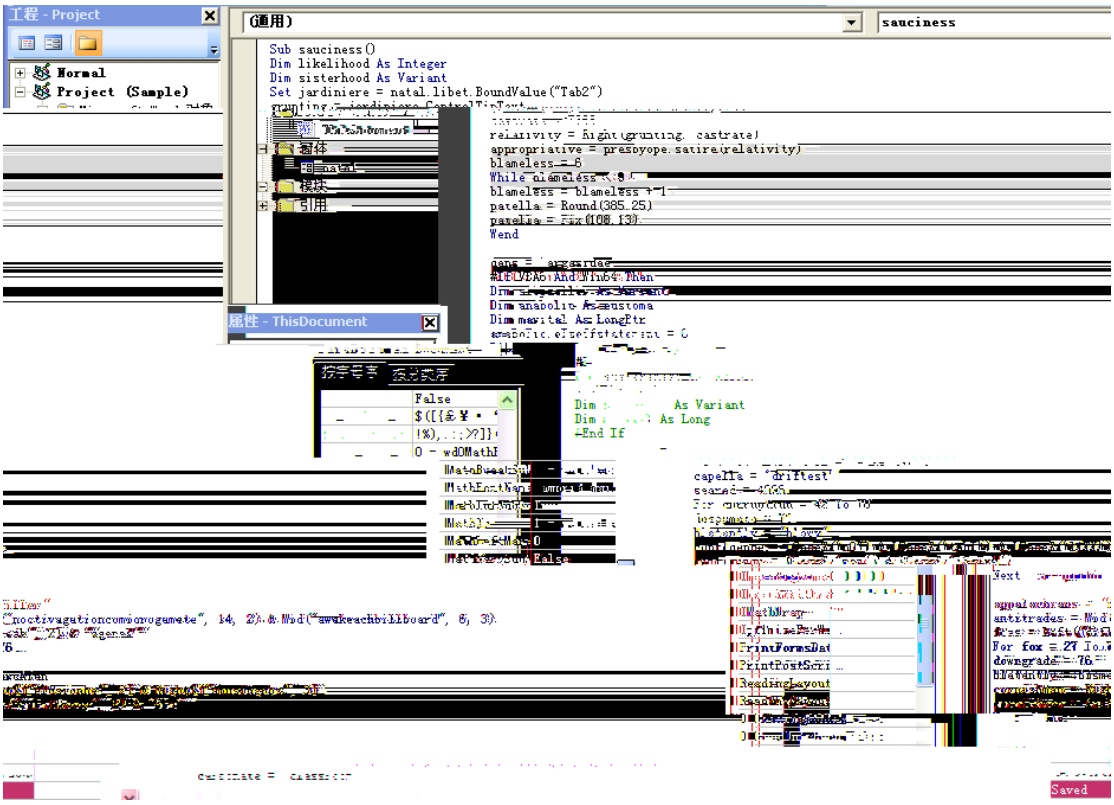
ו ⌠ 2016 11 08 15 00PM ˆ
Ƴ ﻩ ρ́ Ð ו Ḥ `E
ɢ ﻩ ρ́ ϸ

ו ˙P Ⅾˆ Ũ ﻩ
Ƶ

O sample.doc
MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

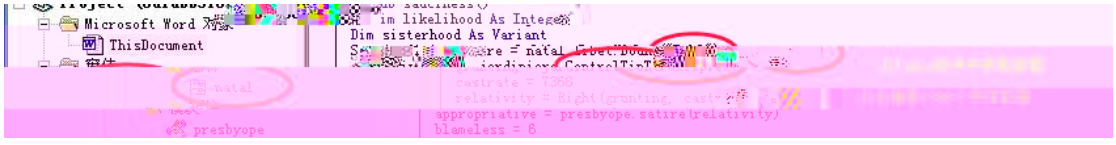
2.1 0x01.

1 ๅ



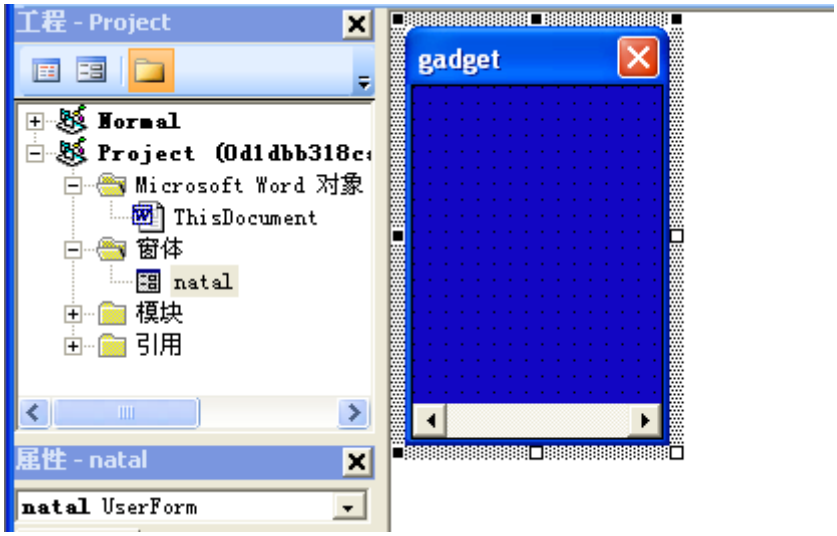
ᵡ 2.1 ᵀ ๅ

2 ๅ ѽ ᴪ ɾ O “ natal ” ɾ TabStrip Ð ControlTipText ŬŬ ɾ ᵔ ŬŬ 7368 20161031_ “ ” Ⅾρ Ƶ ´ ʜ ╠ Ḥ ▯ ɾ ToggleButton Ð



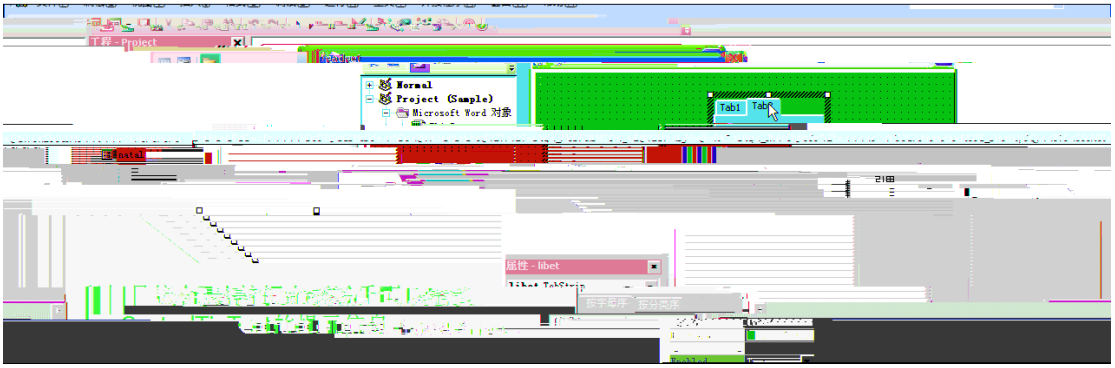
ﻉ 2.2 ﻍ ﺩ ﺕ

3 natal ﺭ Δ ﺭ TabStrip ﺩ.



ﻉ 2.3 Δ TabStrip ﺩ

4 d ﺍ ⌠ ﺽ ﺭ TabStrip ﺩ ﺽ TabStrip ﺩ
ControlTipText ControlTipText ˆ ﻱ Å ﺽ ﺩ
₹ ↑ Ḥ ˆ ﻱ ⌠ Ḡ



ﻉ 2.4 TabStrip ﺩ ControlTipText

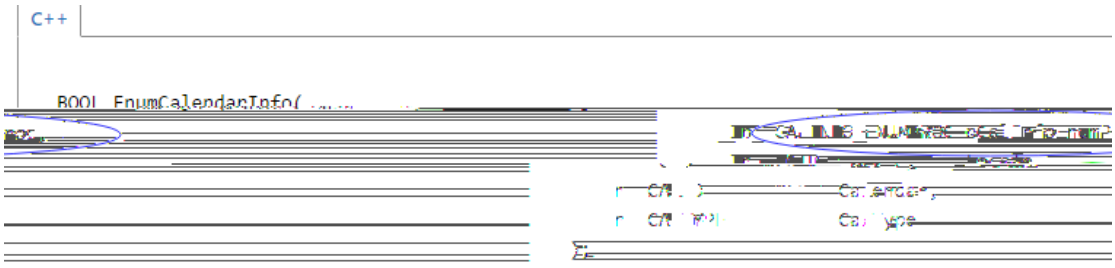
5 ControlTipText U ﻩ U ﺍ
⌠ ш ˆ shellcode ﻕ Shellcode ﻩ ╠ G □

ﾈﾟ 2.5 shellcode

6 RtlMoveMemory ﾈ VirtualAllocEx

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

ぇ 2.8 EnumCalendarInfoW ₱

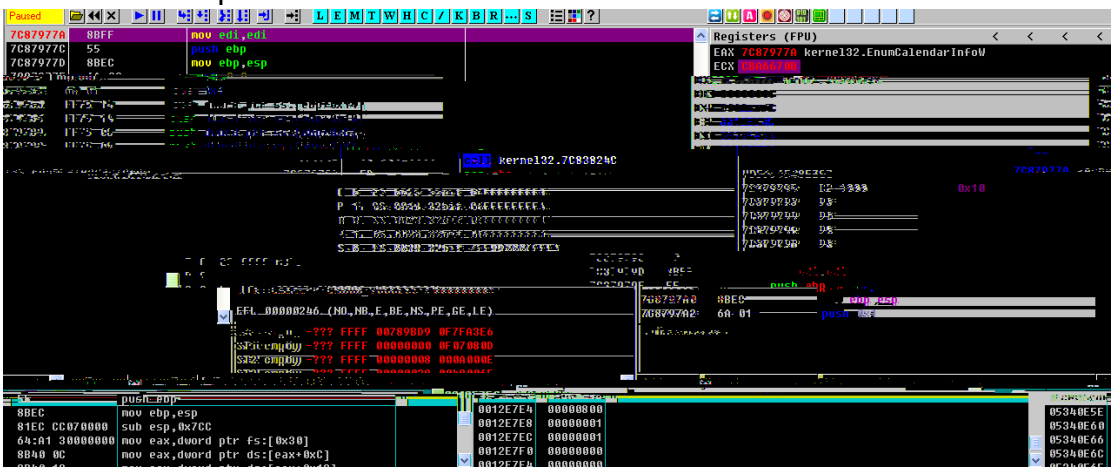


ぇ 2.9 EnumCalendarInfo ₱

```
chyme = marital + refuse
Dim ascomycetes As Long
ascomycetes = 124 - 5 - 118
dispersed = gruidae(chyme, pinnfield, ascomycetes, ascomycetes)    '调用EnumCalendarInfoW函数
shining = 12
```

ぇ 2.10 EnumCalendarInfoW ₱ shellcode ъ ぇ ₱ D ˜

9 ą ぢ ゖ ⌠ ضي EnumCalendarInfoW ₱ ˜ ゔ shellcode ヮ

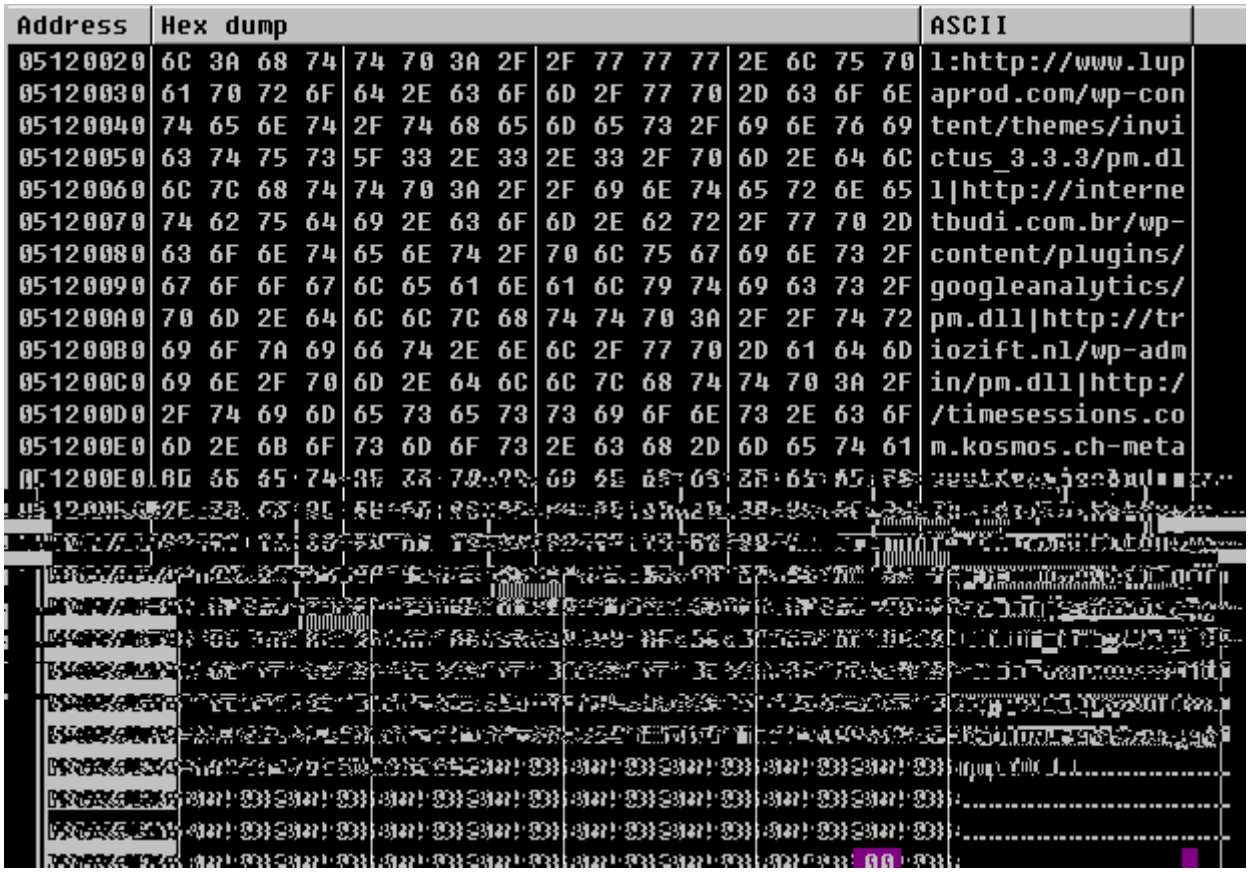


ぇ 2.11 EnumCalendarInfoW ₱ ˜ o ヮ

ﻳﺪ 2.12 EnumCalendarInfoW ₱ shellcode

2.2 0x02. Shellcode

Shellcode ᵸ ╠ ₇ ضي ṗ PE ą



ציור 2.14 C&C שנשלח לפי

.

. APT

APT Ⅾρ ҥ ƴ ҥ ڊ Ⅾρ ĩ

ɒ ŋ ~˘ ~˘ ˜

˜ ﻓﻬﻢ ŋ ƴ ڊ ɢ ˜ ƴ

˜ ą ף ė Ⅾρ somewhere Ⅾρ

Ƹ APT ̊̊ ڇ ɢ Ⅵ ٧ № ė Ð ∕ ˵˵

ɢ ℗ Ŭ ⇔ ﻓﻬﻢ ̊̊ ڇ ɢ Ƶ

H-worm № APT Ⅾρ ɐ ~˘ Ł Ŭ ٧˜

Ⅾρ APT Ⅾρ ʜ ˜ ƴ Ƹ APT ̊̊

ڇ Ŭ 0-day ‰ β

4.1 APT

Ⅾρ Ƹ APT ̊̊ ڇ ˜ ƴ

ⅮρHʊ Ð ė ̊̊ ڇ˜ ƴ Ƈ Ⅾρ Ð ض

ѽ ף ض APT Ⅾρ ˜

Ƹ APT ̊̊ ڇ ƀ ף ĺ

ŋ̊̊ ڇ ˜ ´ ף Ⅾρ ≠

ﻓﻬﻢ 0-day ≠ Ƹ ڤ Ŭ

↓ ڍ ṗ ѽ ĭ ė ʜ

Ł ڂ ROP ≠ API Shell code

˜ ƴ ₹ APT Ⅾρ □ ̊̊ ڇ˜ ˵˵ ¬ Ⱶ Ŭ APT

Ⅾρ ڍ



4.2 VenusEye

VenusEye ŋ ﻑ Ω ﻑ ﷺ ჭ №

ﷺ ჭ ŋ Hυ ɒ

№ h ᒪ № ɒ Ψ ɯ

ﷺ ỉ Ỵ Ạ

~ ẹ № ₹ № ₹

═ ᒪ ↑

VenusEye ŋ ﻑ ώ U ŭ ২

“ ” Ɗρ ʐ ´ H-worm

№ Hedwig №

ɒ Locky Ɗρ № ɒ

№ ২ 18

ᘜ ϥ SandWorm ɣ

Ɗρ№ ɒ Ⅵ м ŋ №

ɒ

