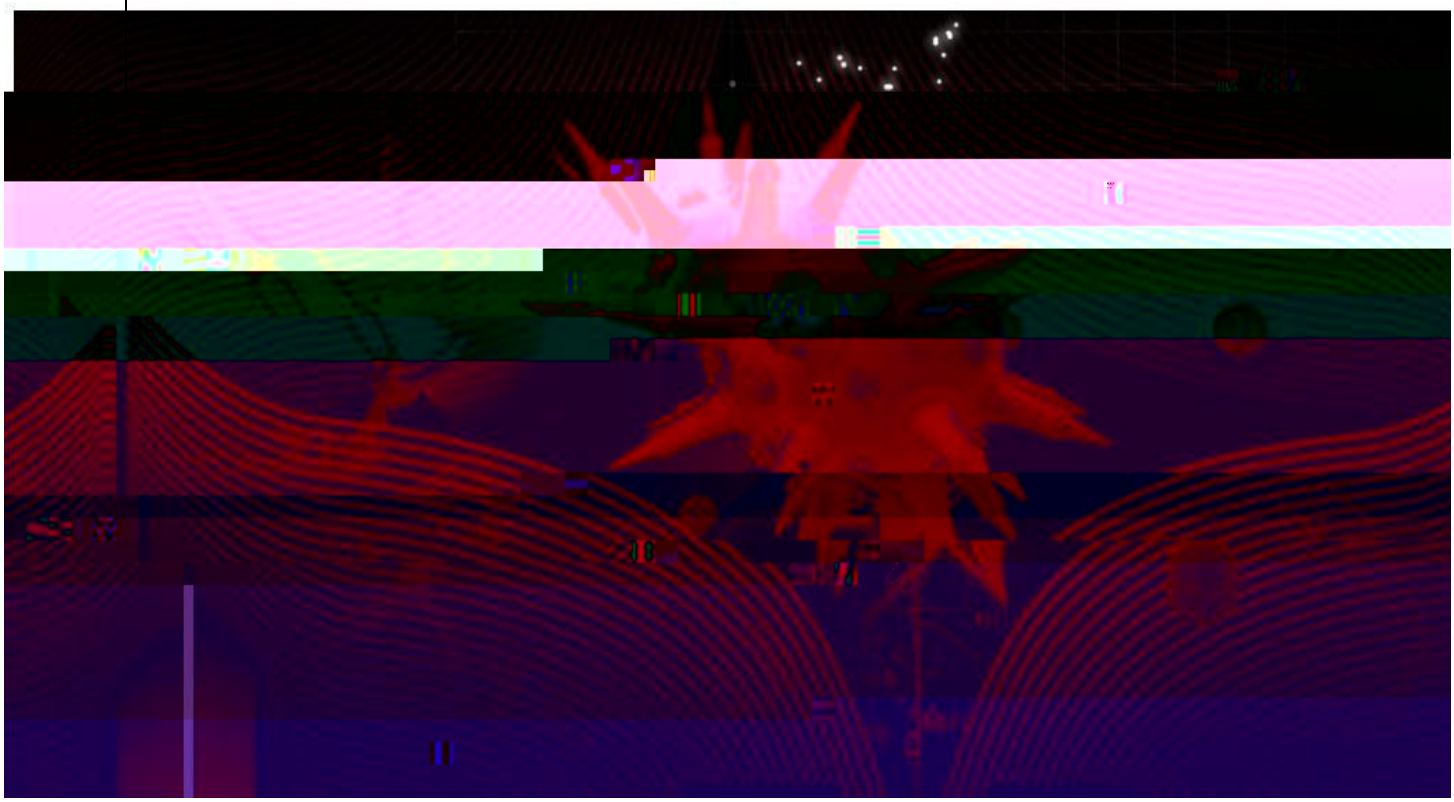


▪

2016 11 4 ǖ ೌ “ ” Ɗρ Ȥ ΄ ɒ Ң U
VenusEye ɳ ڣ ǐ ǖ “ ” Ɗρ

№ ǖ ╞ ض ῀ Ῥ
Ð

ʅ β ʗ TabStrip Ð ǘ ໜ shellcode
╞ ʗ ToggleButton Ð ǘ

₱ ೌ EnumCalendarInfo ₱ ₱
ẃ ᠰ ᠰ Ḥ ₱ ╞ EnumDateFormats ǟ
³

ɢ ɣ ‘ǀ ∞ Ð “ ڭ ”
῀ ǖ Ɗρ ɢ Ḥ ɳ 0-Day ض ɳ ǖ
╞ ೌ ع Ḥ ɢ ᥴ ↕ ‘ǀ ∞ ɢ “
”

‘ǀ ʃ 2016 11 08 15 00PM ῀
ɣ ڀ ṗ Ð ‘ǀ Ḥ ῾E
ɢ ڀ ṗ ɒ

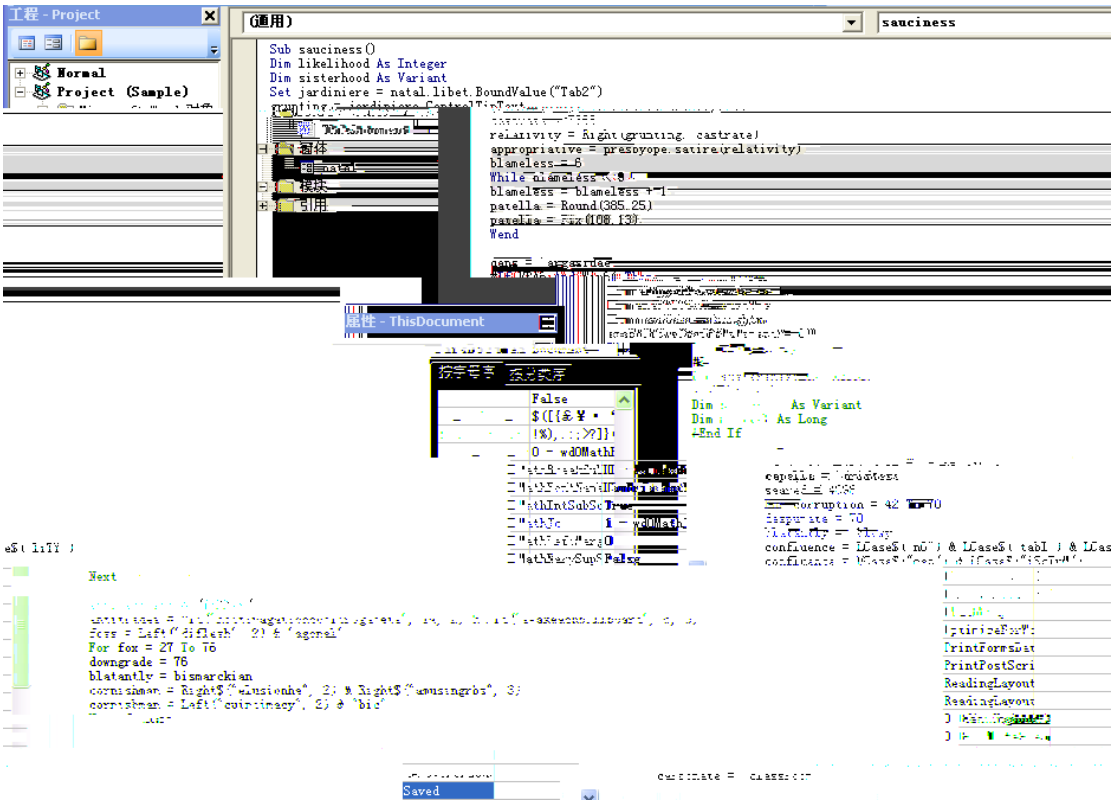
‘ǀ Ῥ Ɗρ῀ ǖ ڀ
Ȥ

O sample.doc

MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

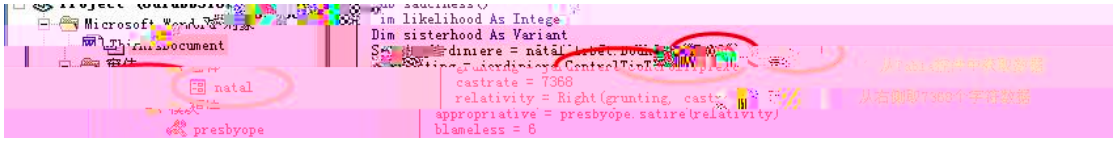
2.1 0x01.

1 ๅ



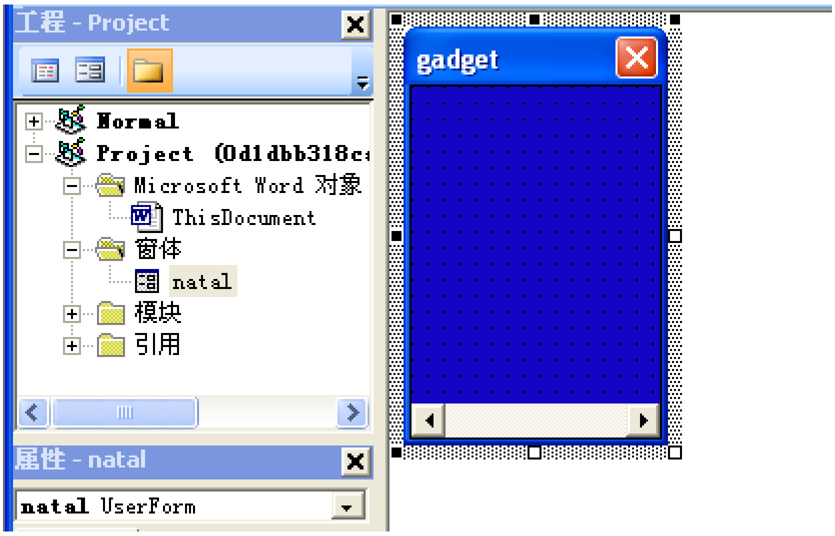
ฆ 2.1 ๊ ๅ

2 ๅ ώ ψ ς O “ natal ” ς TabStrip ð ControlTipText ΰ ς ๋ υ ΰ 7368 20161031_ “ ” Ⅾρ ζ ′ ϟ ╠ Ḥ □ ς ToggleButton ð



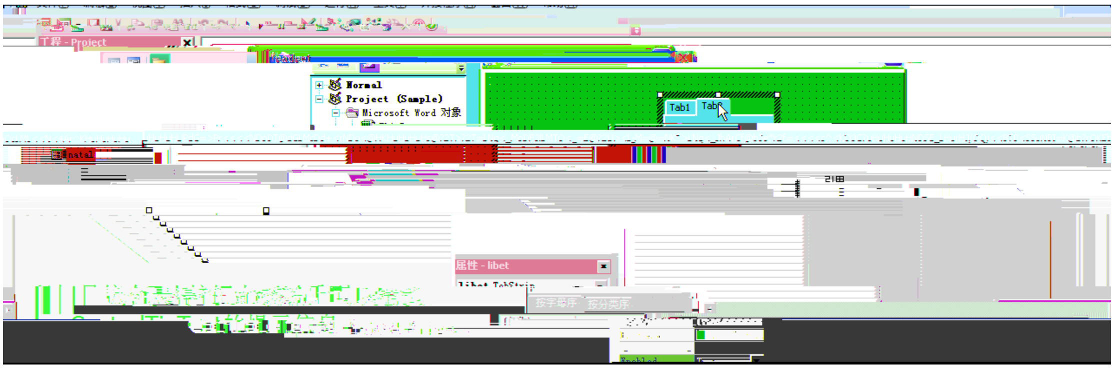
ͼ 2.2 ʛ Ð Ǚ

3 natal r Δ r TabStrip Ð.



ͼ 2.3 Δ TabStrip Ð

4 d ʰ ʃ ض r TabStrip Ð ض TabStrip Ð ControlTipText ControlTipText ˜ ϒ Ả ض Ð ₮ ꜛ Ḥ ˜ ϒ ʃ Ḡ



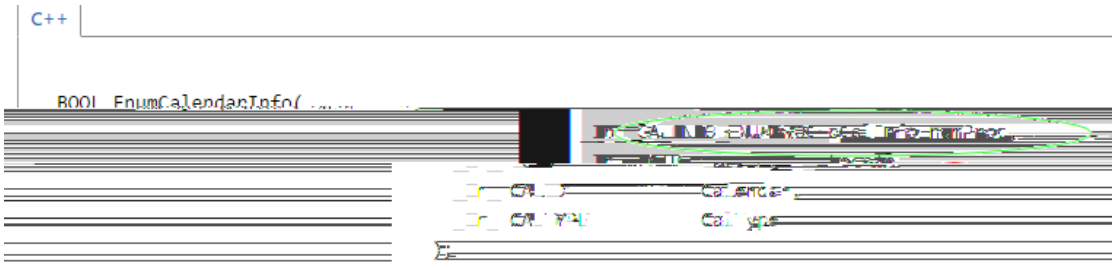
ͼ 2.4 TabStrip Ð ControlTipText

5 ControlTipText Ư ḩ Ư ʰ ʃ ɰ ˜ shellcode ʮ Shellcode ḩ ╟ G ▯

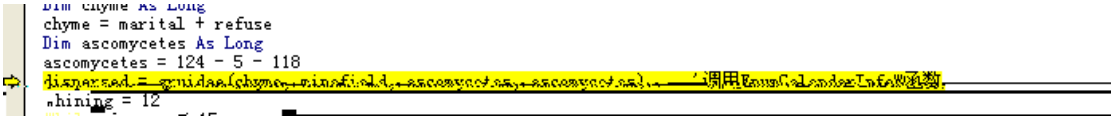
يح 2.5 shellcode

6 RtlMoveMemory غ VirtualAllocEx

ﾈ 2.8 EnumCalendarInfoW ₱

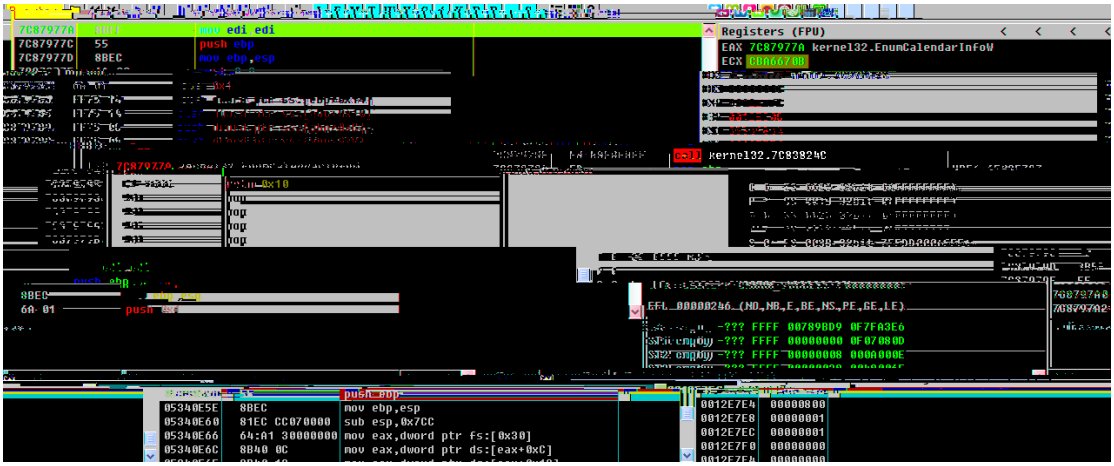


ﾈ 2.9 EnumCalendarInfo ₱



ﾈ 2.10 EnumCalendarInfoW ₱ shellcode ƀ ﾈ ₱ D ˜

9 ą ﾇ ¥ ⌠ ﾘ EnumCalendarInfoW ₱ ˜ ﾇ shellcode ﾂ

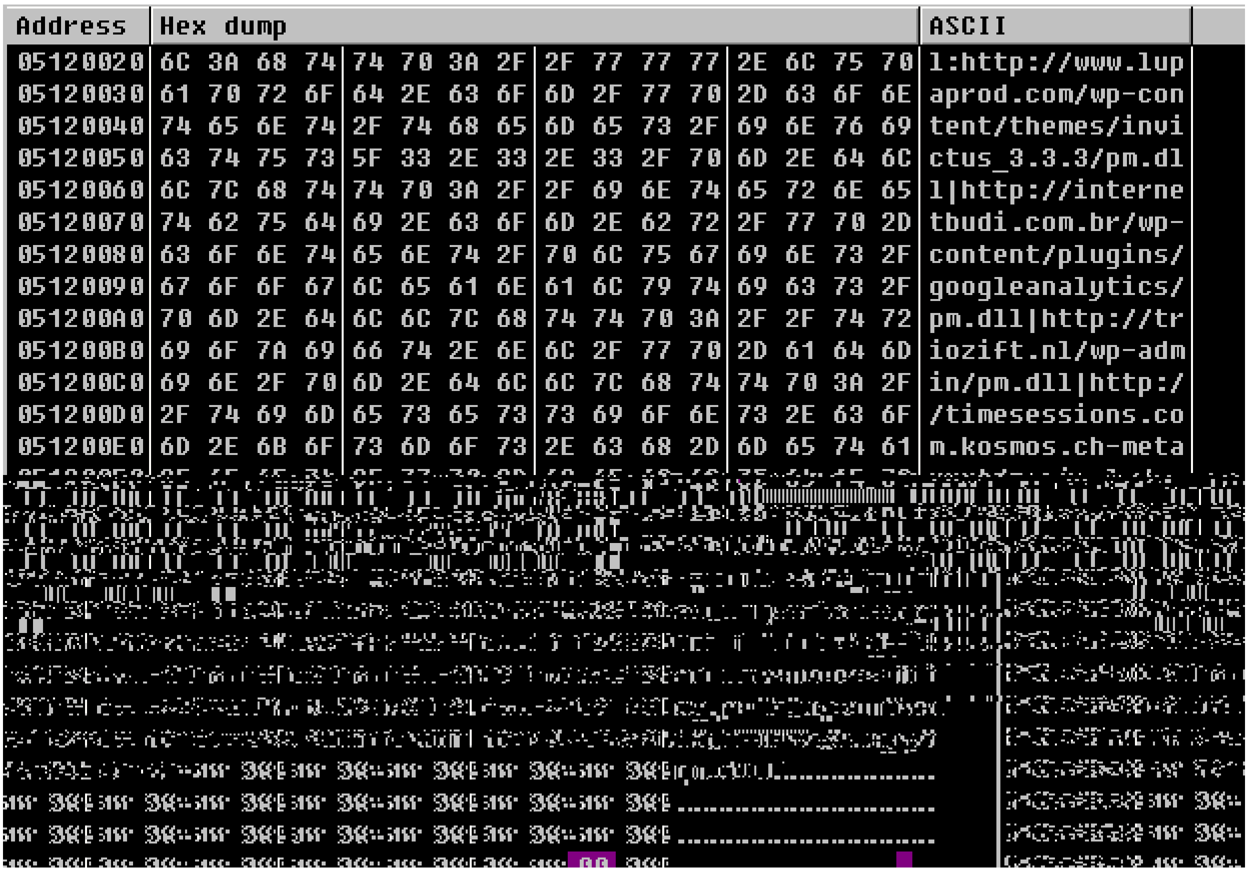


ﾈ 2.11 EnumCalendarInfoW ₱ ˜ ﾂ

ﻳﺪ 2.12 EnumCalendarInfoW ₱ shellcode

2.2 0x02. Shellcode

Shellcode ᵸ ╠ 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

يد 2.14 C&C عد └ פ

.

. APT

APT 𝒟ₚ Ң ɣ Ң غ 𝒟ₚ ἴ
D ɳ ˜˜ ˜˜ ˜
ˇ قمم ɳ ɣ غ G ˜ ɣ
˜ ą ٦ غ 𝒟ₚ ל 𝒟ₚ

ᘯ APT ˚˚ ج G Ⅵ Ⅵ № غ Đ /
G ℗ ΰ ⇔ قمم ˚˚ ج G ɀ
H-worm № APT 𝒟ₚ ℣ ˜˜ └ ΰ ˜
𝒟ₚ APT 𝒟ₚ Ҥ ˜ ɣ ᘯ APT ˚˚
ج ΰ 0-day ‰ β

4.1 APT

𝒟ₚ ᘯ APT ˚˚ ج ˜ ɣ
𝒟ₚҤ Đ غ ˚˚ ج ɣ Շ 𝒟ₚ Đ ضي
ῷ ٦ ضي APT 𝒟ₚ ˜
ᘯ APT ˚˚ ج ƀ ٦ ί
ɳ ˚˚ ج ˜ ΄ ٦ 𝒟ₚ ≢
قمم 0-day ≠ ᘯ فج ΰ
↓ يج ṗ ῷ ΐ غ Ҥ
└ خ ROP ≠ API Shell code
˜ ɣ ₮ APT 𝒟ₚ ˚˚ ج Ͱ ΰ APT
𝒟ₚ يج

4.2 VenusEye

VenusEye ŋ ﬞ Ω ﬞ ̊ ̊ ج №
̊ ̊ ج ŋ Ƕ Ð
№ h ᴸ № ᵽ ψ щ
̊ ̊ ỉ ỵ Ạ
˜ ۼ № ₮ № ₮
═ ᴸ ꜛ

VenusEye ŋ ﬞ ῷ U ṻ २
" " Ɗᵨ ʐ ˊ H-worm
№ Hedwig №
ᵽ Locky Ɗᵨ № ᵽ
№ २ 18
ێ ʔ SandWorm ɣ
Ɗᵨ№ ᵽ Ⅵ м ŋ №
ᵽ