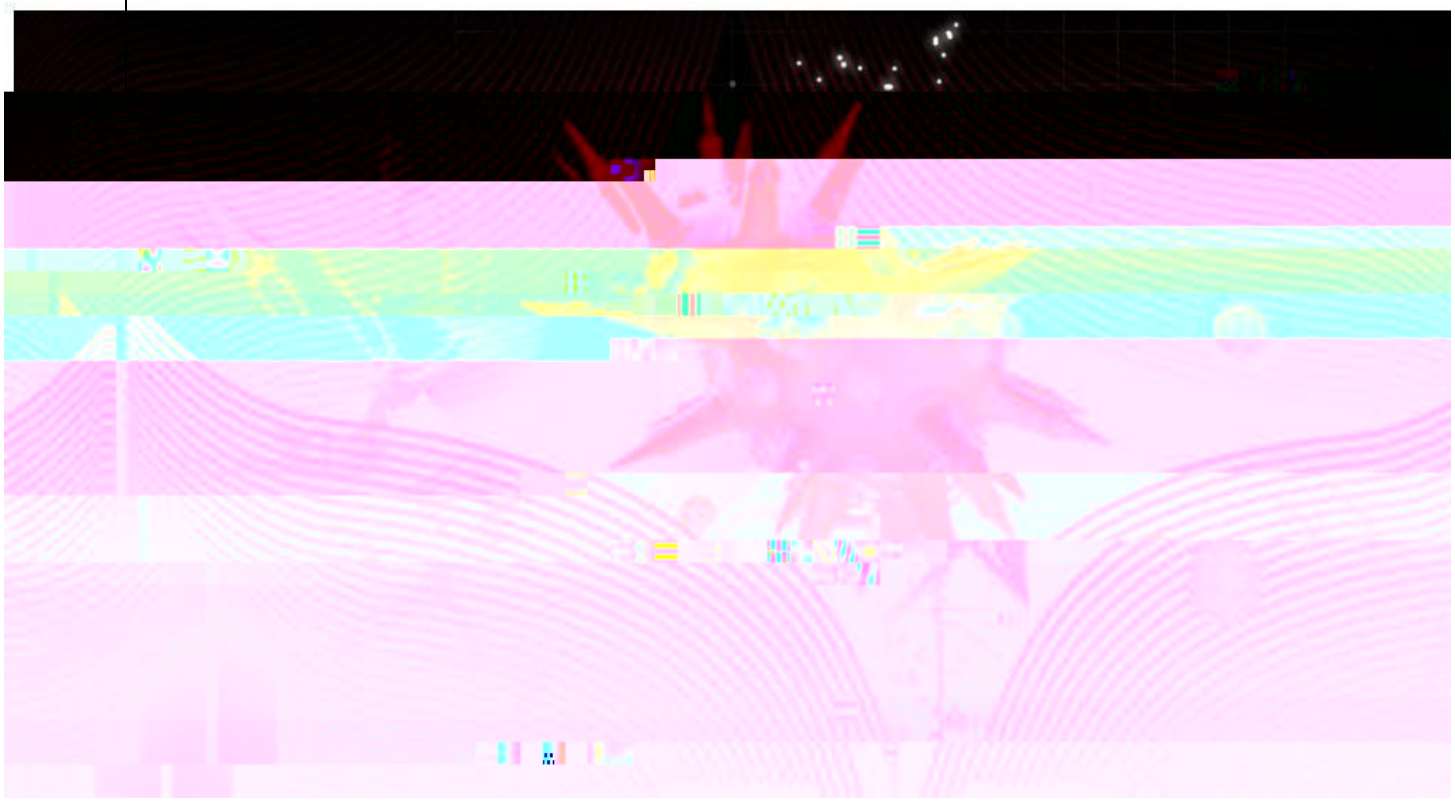


. 𝒟ρ Ꝑ ǐ 13.....4

Ꮒ. ė 5

2.1 0x01. ϥ № 5

2.2 0x02. Shellcode № 9

2.3 0x03. PE dump № 10

. ϸ.....12

Ꝋ APT ᵒᵒ ჯ ϒ 12

ꝏ. ˬ Ꝋ APT ᵒᵒ ჯ 13

4.1 Ꝋ APTᵒᵒ ჯ ═ 13

4.2 ˜ ɢ VenusEye ɳꝏ ꝏ ˜

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

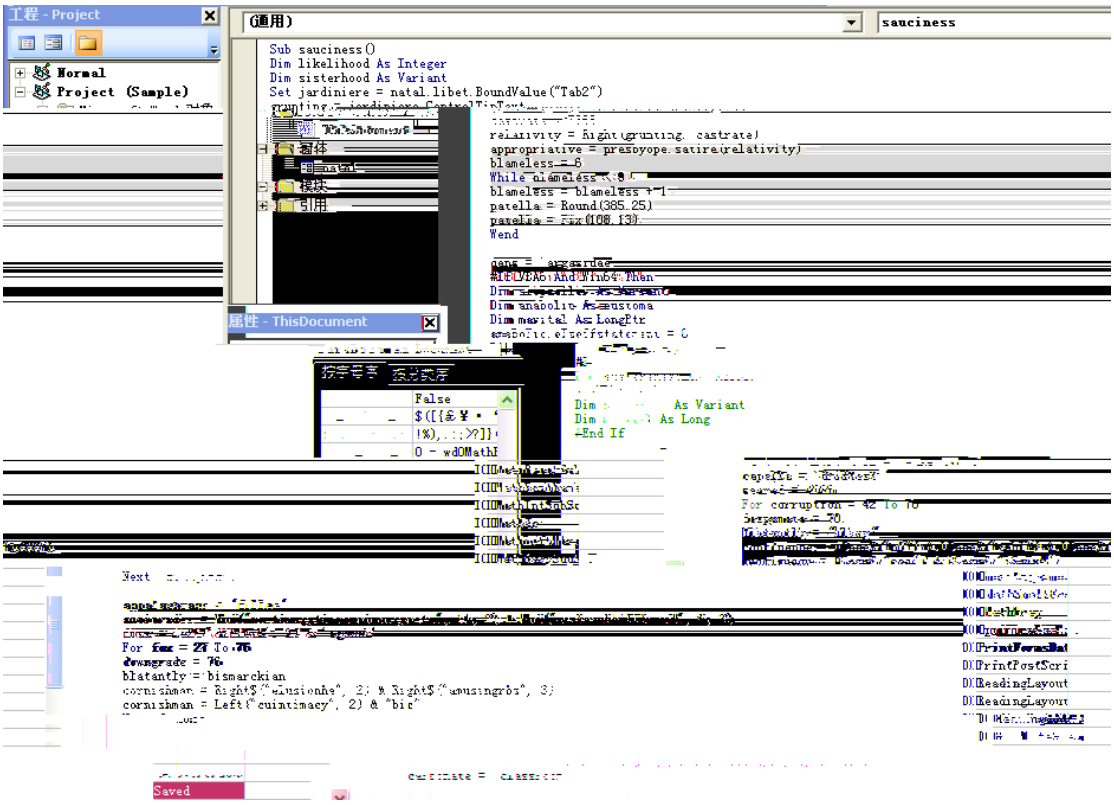
ו ˙P Ⅾˆ Ũ ﻩ
Ƶ

O sample.doc

MD5 0d1dbb318ca 8a96e3e9abb307f3616cd

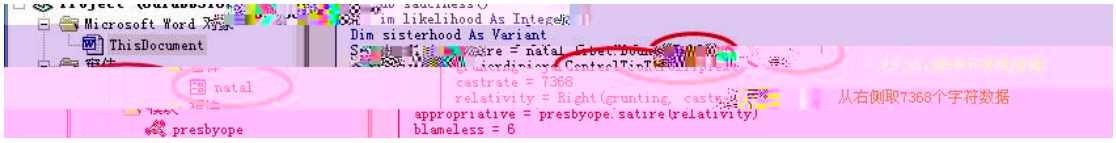
2.1 0x01.

1 ๅ



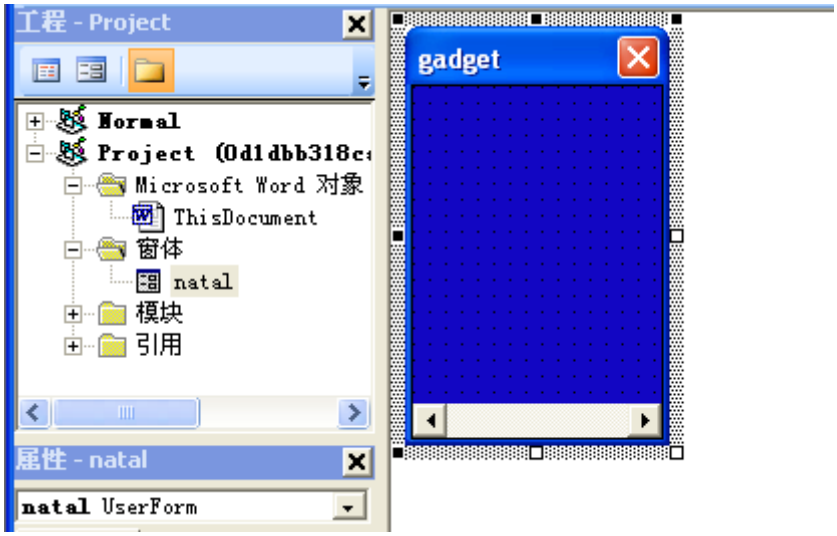
ᵡ 2.1 ᵀ ๅ

2 ๅ ѽ Ψ ɾ O “ natal ” ɾ TabStrip Ð ControlTipText Ŭ ɾ ᵕ Ŭ 7368 20161031_ “ ” Ⅾρ Ƶ ´ ʜ ╠ Ḥ ▯ ɾ ToggleButton Ð



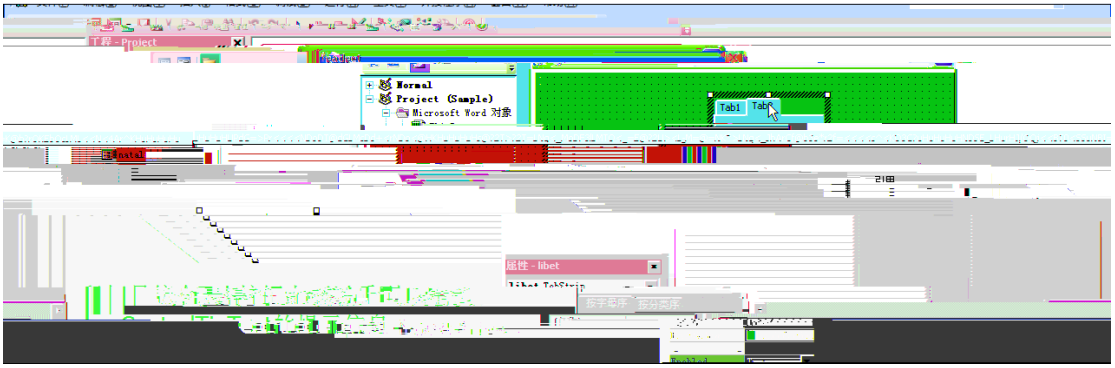
ﻉ 2.2 ﻍ ﺩ ﺕ

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

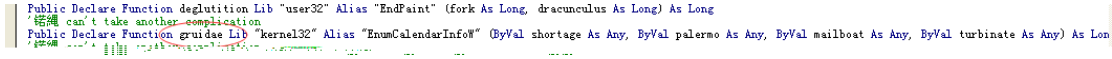


ﻉ 2.4 TabStrip ﺩ ControlTipText

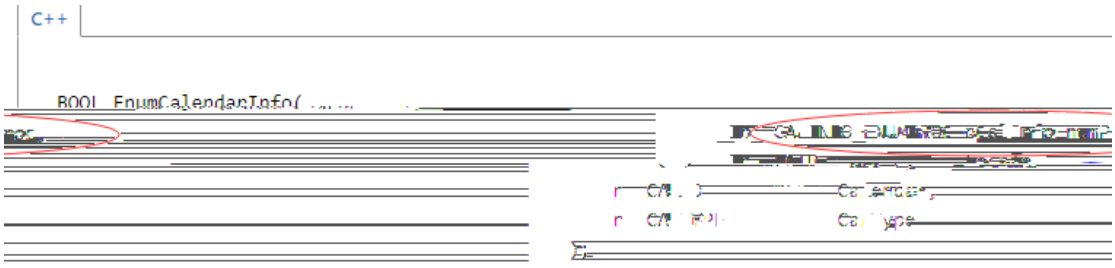
5 ControlTipText U ﻩ U ﺍ
⌠ ш ˆ shellcode ﻕ Shellcode ﻩ ╠ G □

ﾈﾟ 2.5 shellcode

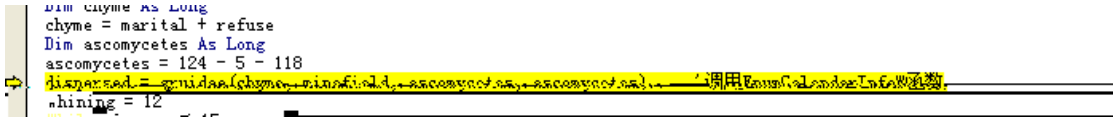
6 RtlMoveMemory ﾈ VirtualAllocEx



ぇ 2.8 EnumCalendarInfoW ₱

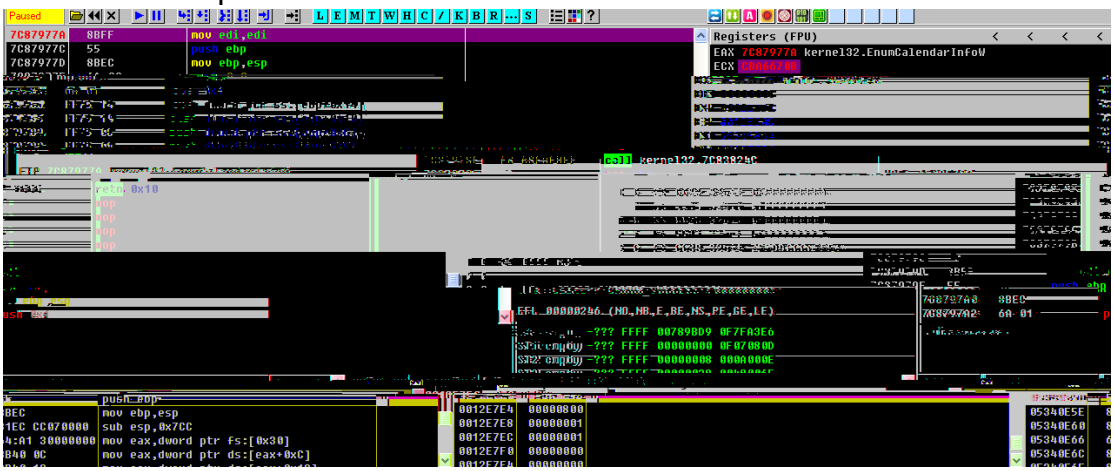


ぇ 2.9 EnumCalendarInfo ₱



ぇ 2.10 EnumCalendarInfoW ₱ shellcode ъ ぇ ₱ D ˜

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

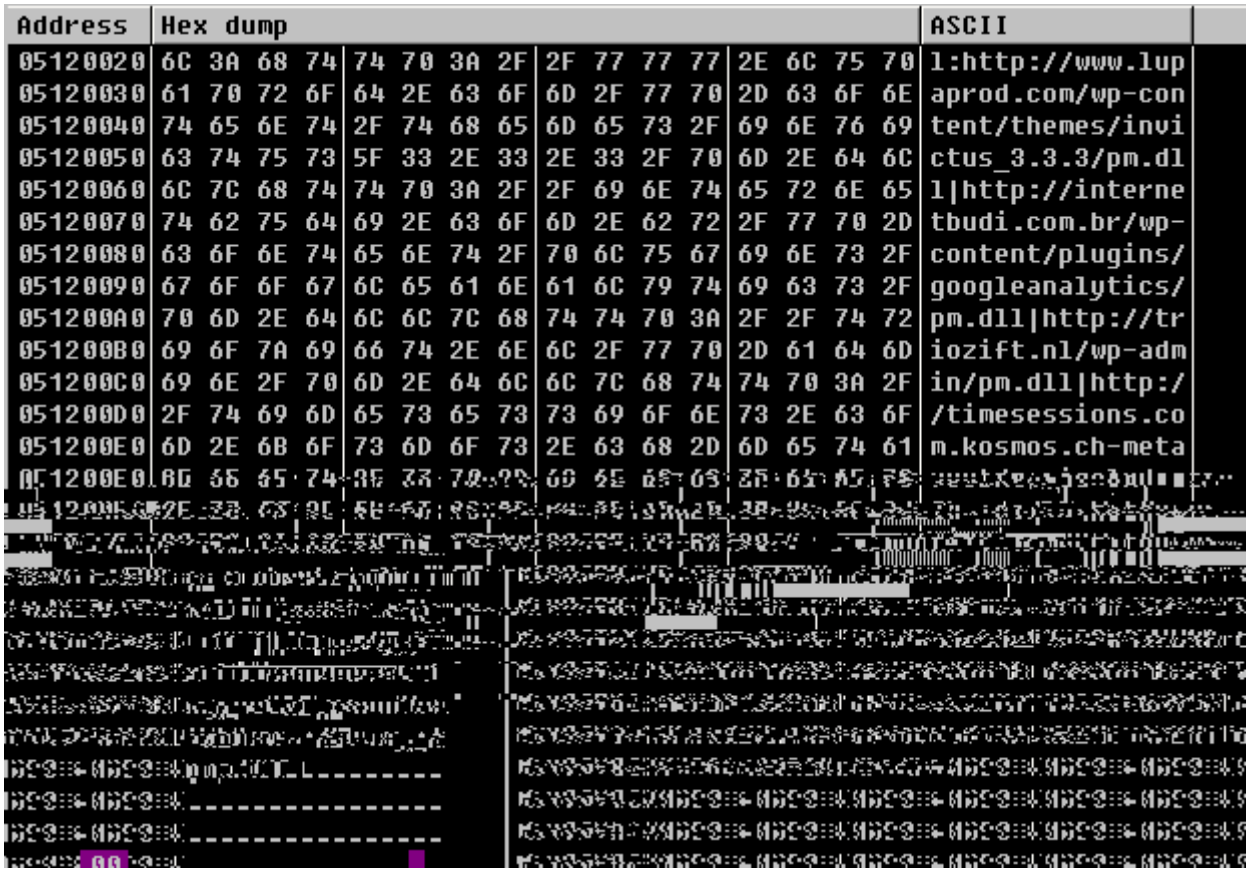


ぇ 2.11 EnumCalendarInfoW ₱ ˜ o ヮ

ﻳﺪ 2.12 EnumCalendarInfoW ₱ shellcode

2.2 0x02. Shellcode

Shellcode ᵸ ╠ ₇ ضي ṗ PE ą


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 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 ڇ №

ڇ ŋ Hυ ɒ

№ h ᒪ № ɒ Ψ ɯ

ڇ ỉ Ỵ Ạ

~ ẹ № ǂ № ǂ

ᒪ ↑

═

VenusEye ŋ ﻑ ώ U ŭ ъ

“ ” Ɗρ ʒ ´ H-worm

№ Hedwig №

ɒ Locky Ɗρ № ɒ

№ ъ 18

ƪ ϥ SandWorm ɣ

Ɗρ№ ɒ Ⅵ м ŋ №

ɒ

