- “Death”

ADLab



1. 1
2. “ ” 2
2.1 “ ” 2
2.2 3
3. “DEATH” 5
4. “DEATH” 7
4.1 C&C .....

ADLab

- “ Death ”

ADL

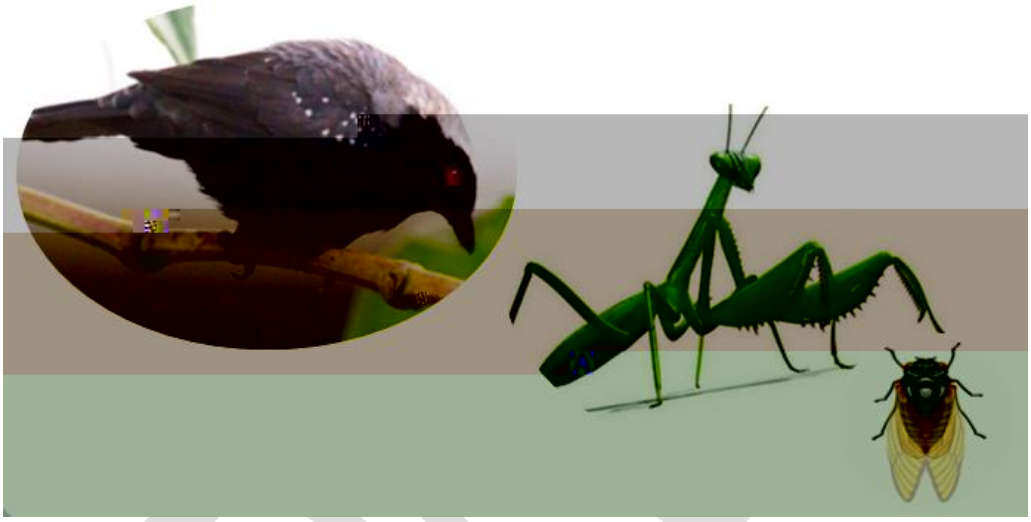
- “ Death ”

- “ Death ”

“ ”

“ ” “ ” “ ”

“ ”



2.1

2. 2

1

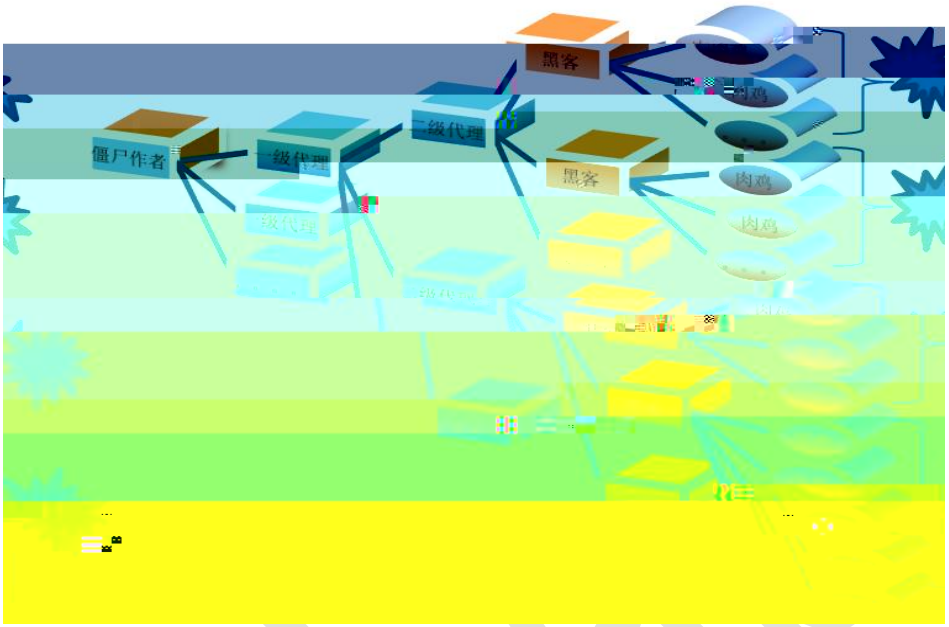
“ ”

(

)

- “ Death ”

ADLa



2.2

“ ”

“ ”

3. “ Death ”

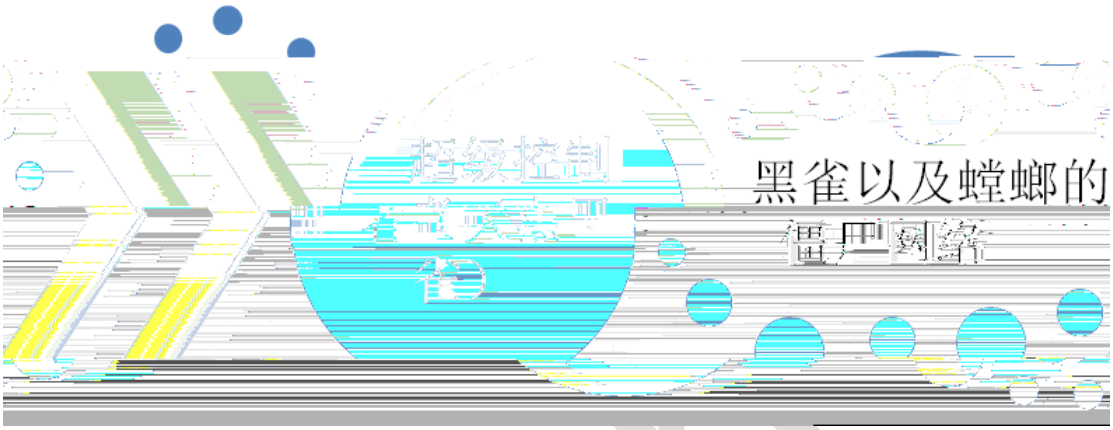
“ Death ” 2000

--

3.1

“ Death ”

- “ Death ”



3.1 ( )

C&C

“ Billgate ” DDoS

“ Death ”

ADLab

- “ Death ”

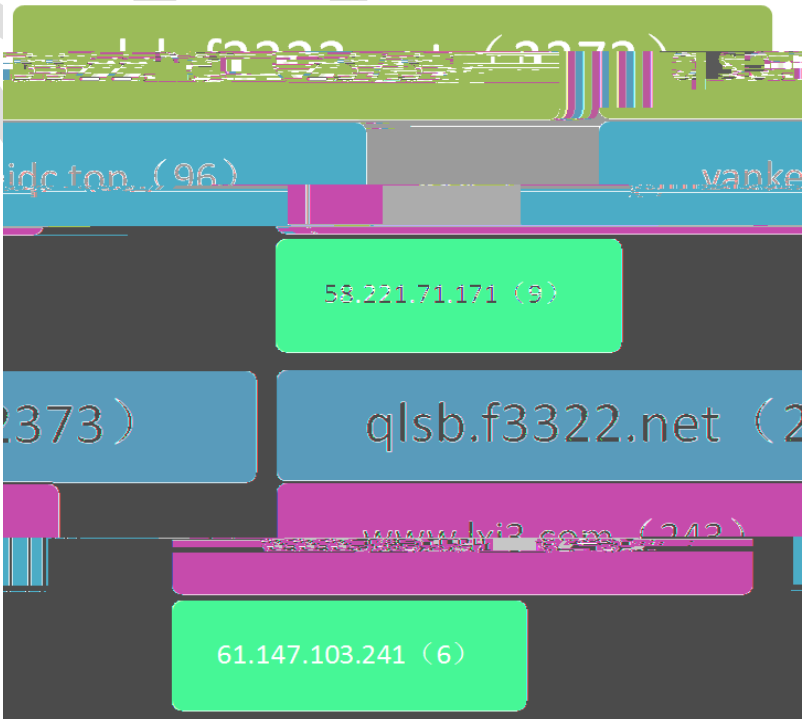
ADL

- “ Death ”

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

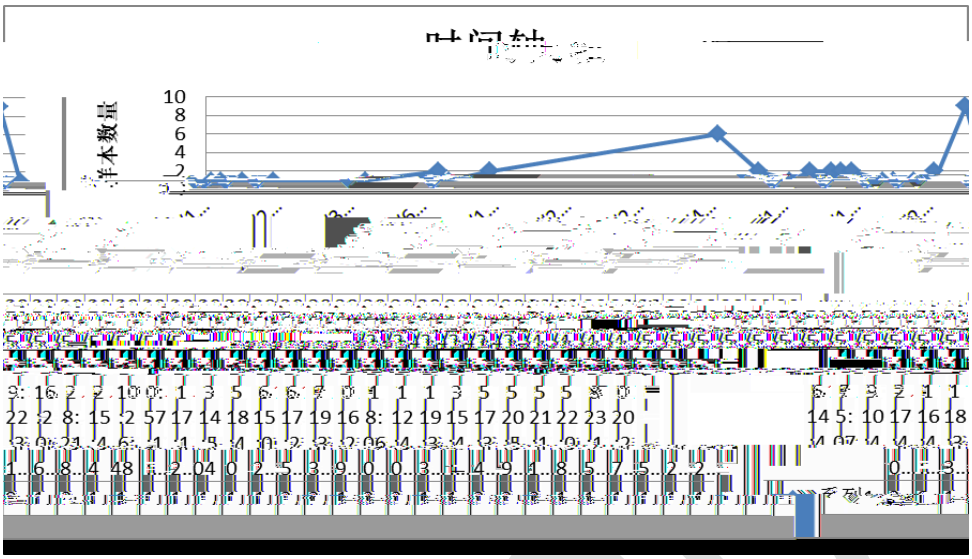
- “ Death ”

- “ Death ”

- “ Death ”

6344T8.69 1T8145 9.62Emage45 9.35 cT204955 9.04210.7e45BT217.21 454.68 cT223B9 47e4230.46549 7e4229.2367 47.4425 9.8013244 1BT296.275 34.77 3701.63 43.846.09

- “ Death ”



4.8 nb.cztlyy.com -

ADLab

- “ Death ”

460904531132AB1E67A12D5C068A04B0464BC460B11686. TET EMC / P MCID 08 BDC BT1 0 0 1 40.024 769.56 cm/ 15.2E752B43112D28056C112685 8

- “ Death ”

4. 7

2000

“ Billgate ”

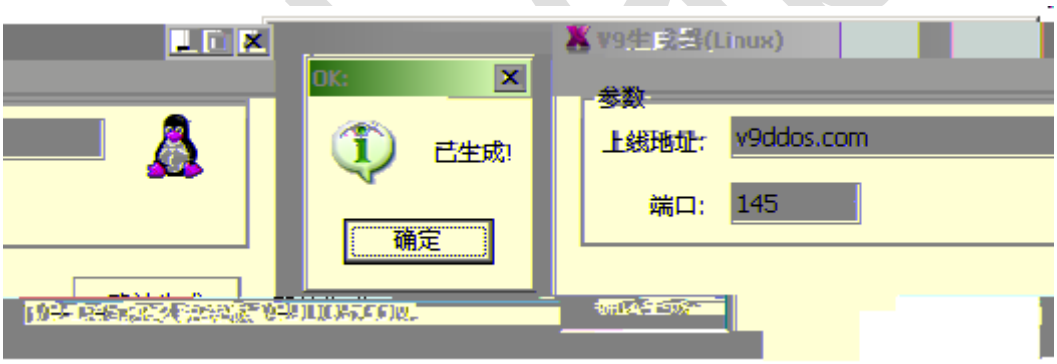
“ Billgate ” “ Death ”

“ Death ” “ Death ” “ Billgate ”

Manager ELF

“ Billgate ” (

) 4.10



4.10 “Billgate”

“ Billgate ” “ Death ” 4.11

- “ Death ”

4.8 “ DEATH ”

4.12

“ 4(eat)7(h]TJET EMC /P <MCID 92>BDC BT/F5 10.56 Tf1 0 0 1 113.1 442.94 Tm<0100072511111E26>TJET EMC /P

ADLab

AÐoY85..

- “ Death ”

- “ Death ”

2015 5 23 3

C&C qlsb.f3322net IP

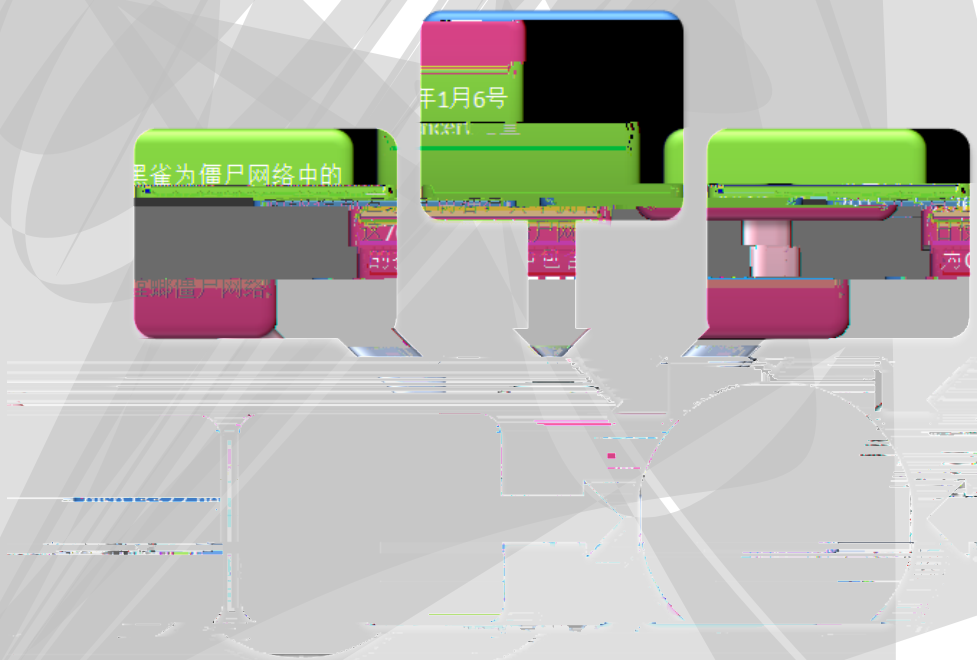
120.26.53.74

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	
0.0/14	2015-05-26 05:47:21	2015-06-12 00:00:00	120.26.53.74	CN	120.24.

C&C

5.5



- “ Death ”

5.3 Q

Q “ Death ”

ADLab

- “ Death ”



5.7 Q

C&C linux.yiqing.pw *

xionga DDoS

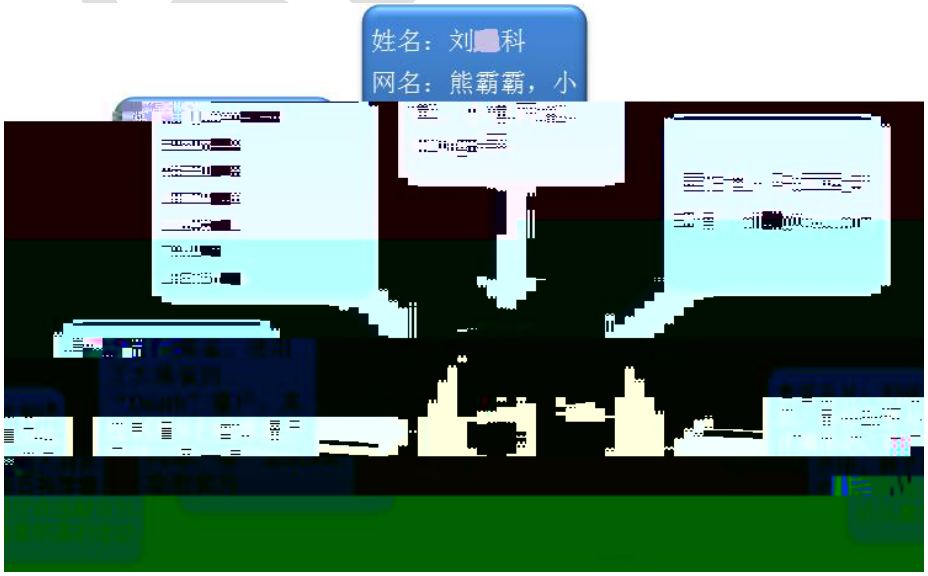
QQ 2013 Q

2016 3 4

DDoS

“ ”

“ ” 5.8



5.8 Q

- “ Death ”

- “ Death ”

- “ Death ”

- “ Death ”

- “ Death ”

ADL



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

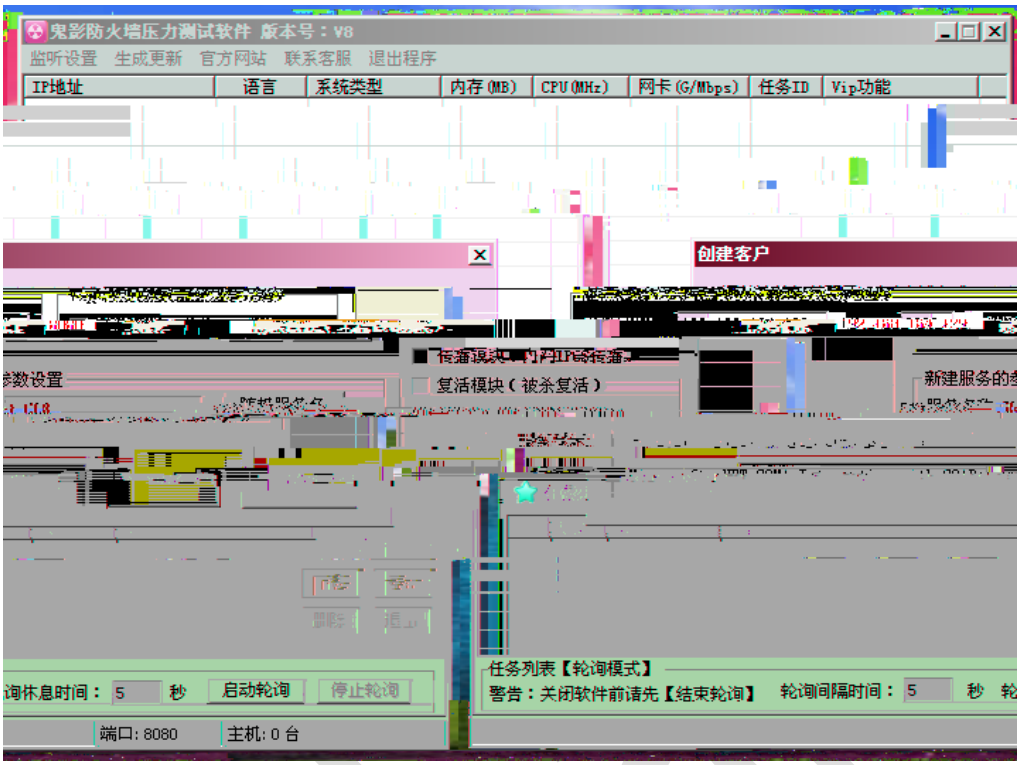
```
push    edi                 push    edi
push    180000              push    7200000
call    Sleep               call    ds:Sleep
```

6.8 C&C

- “ Death ”

- “ Death ”

- “ Death ”

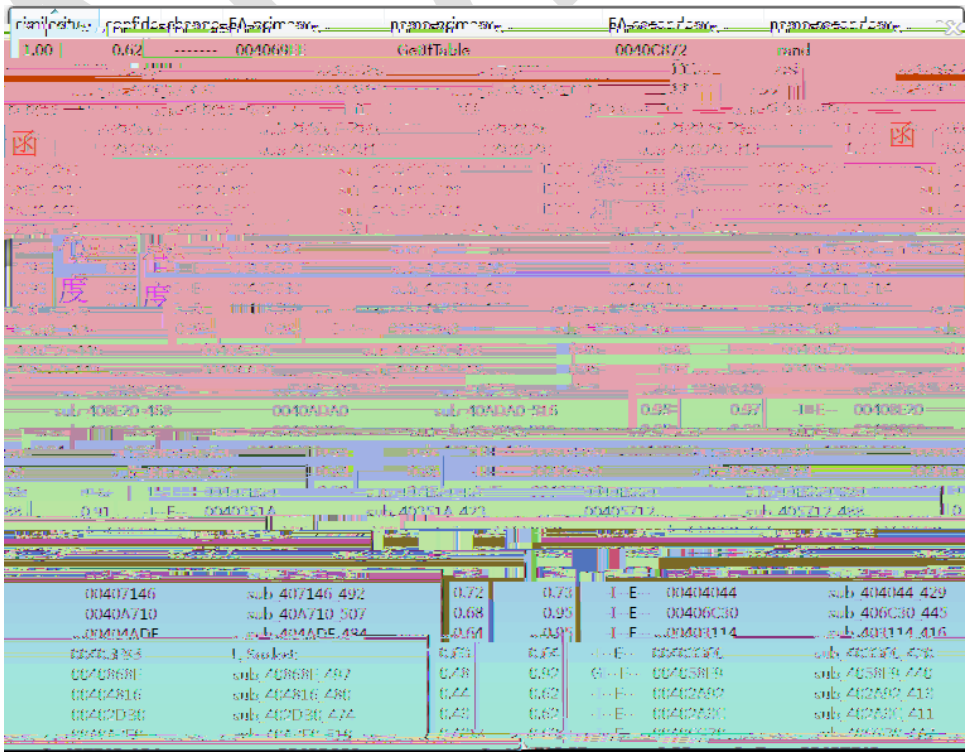


7.1 DDoS

IDA BinDiff “ Death ” Nitol DDoS

7.2 “ Death ” Nitol

API



7.2 Death Nitol

- “ Death ”

- “ Death ”

Nitol

IPC$

C&C Nitol “ Death ”

DDoS “ Death ”

DDoS v8 Nitol DDoS

“ Death ” DDoS

DDoS v8

“

“ Death ” Nitol Nitol

Nitol

ADLab

- “ Death ”



ADLab

- “ Death ”

C&C C&C C&C

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

“ Death ” C&C base64

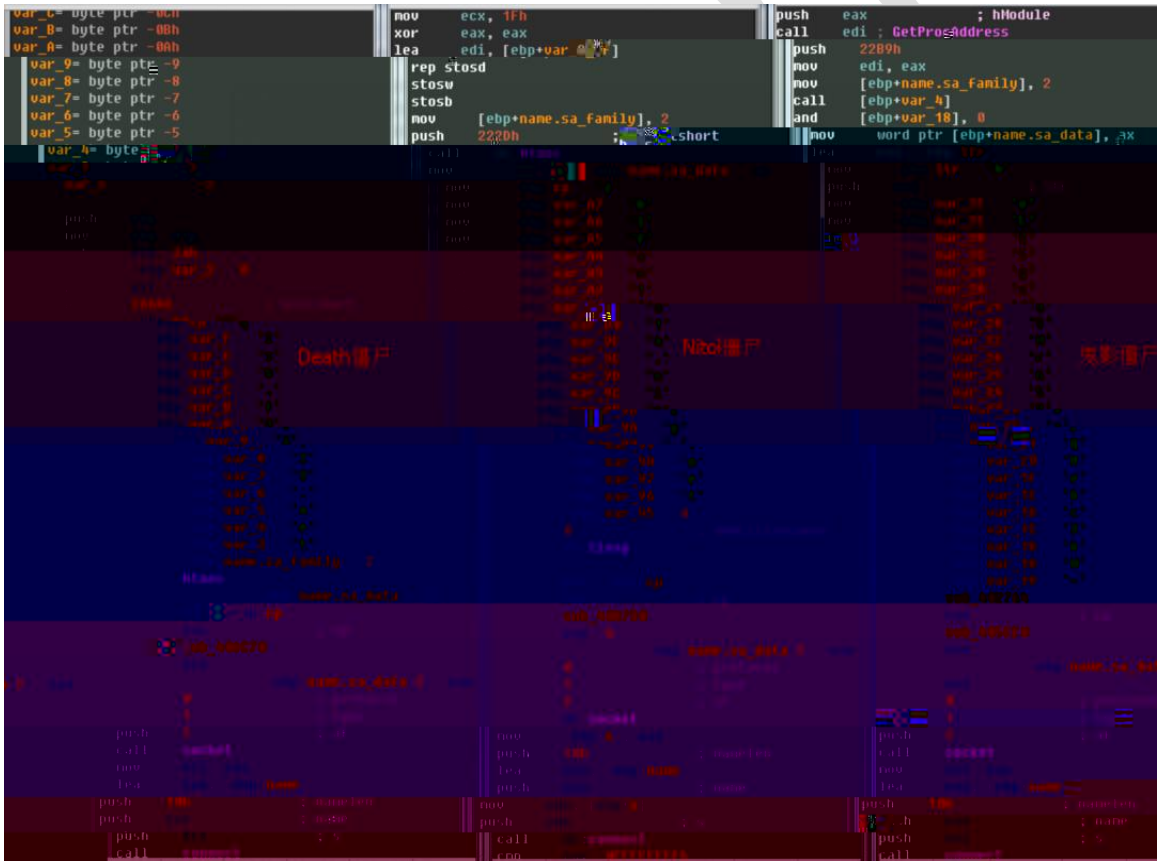
C&C C&C “ Death ”

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 ”