

- “Death”

ADLab



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

- “Death”

ADLab

- “Death”

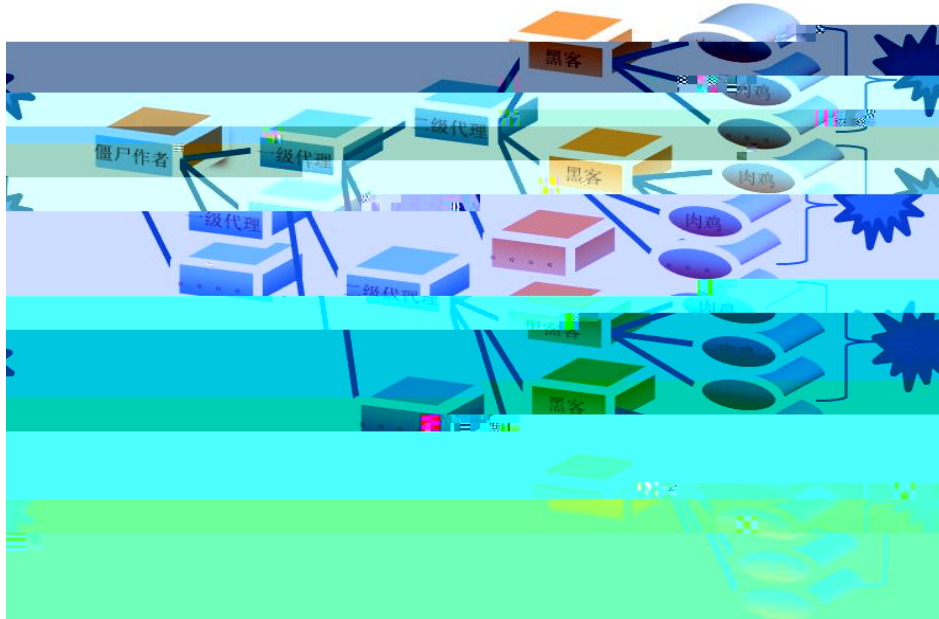


- “ Death ”



- “Death”





2.2

“

”

“

”

3. “Death”

“Death”

2000

--

3.1

“Death”



3.1 ()

C&C

“Billgate” DDoS

“Death”

- “Death”



ADL

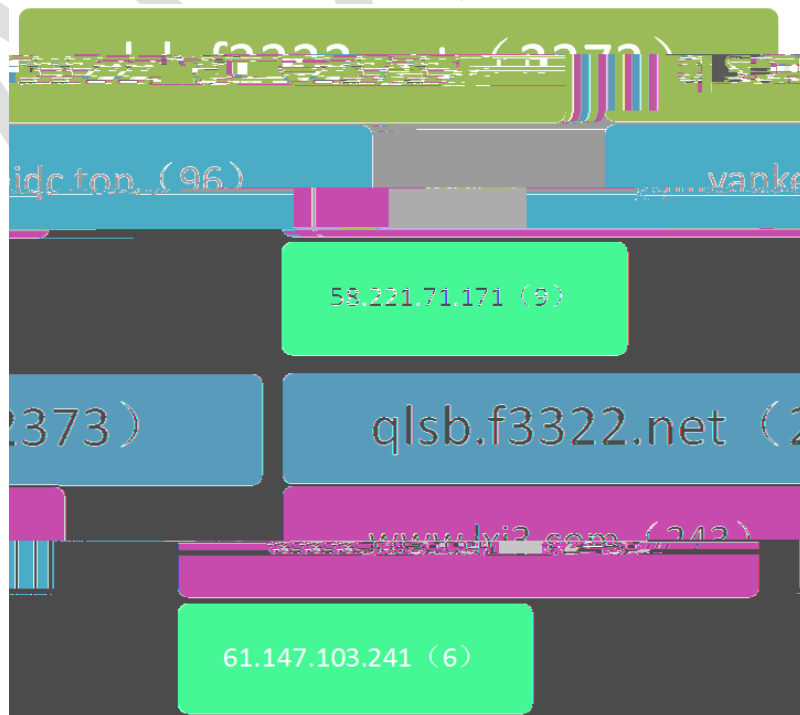
- “ Death ”



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



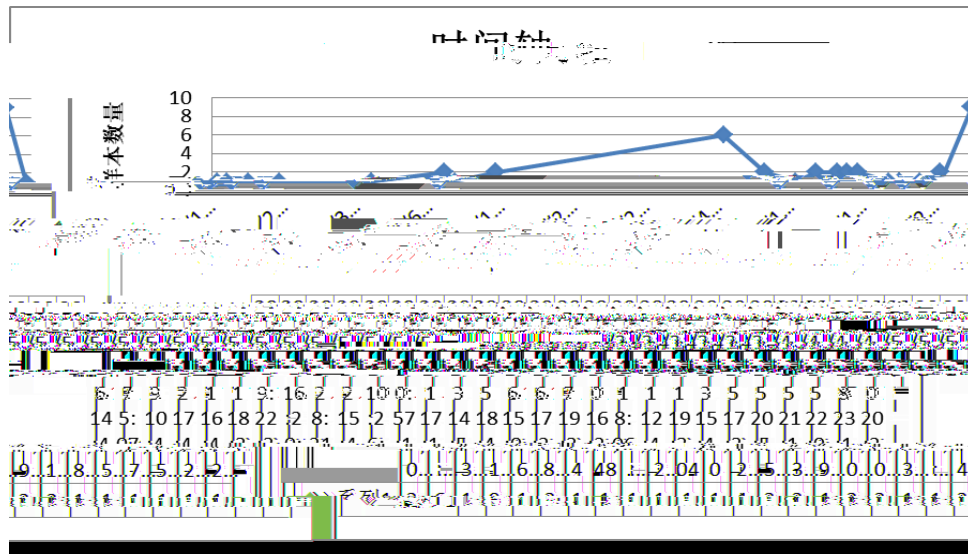
- “Death”



- “ Death ”

- “ Death ”





4.8 nb.cztlyy.com

- "Death"

- “Death”



- “Death”

4.7

2000

“Billgate”

“Billgate”

“Death”

“Death”

“Death”

“Billgate”

Manager

ELF

“Billgate”

(

)

4.10



4.10 “Billgate”

“Billgate”

“Death”

4.11

- “Death”

- “ Death ”



4. 8 “ DEATH ”

4.12

“ 4(eat)7(h)TET EMC /P MCID 92BDC BT/F5 10.56 Tf1 0 0 1 113.1 442.94 Tm010007251114E26TET EMC /P

ADLab

- “Death”



- “ Death ”

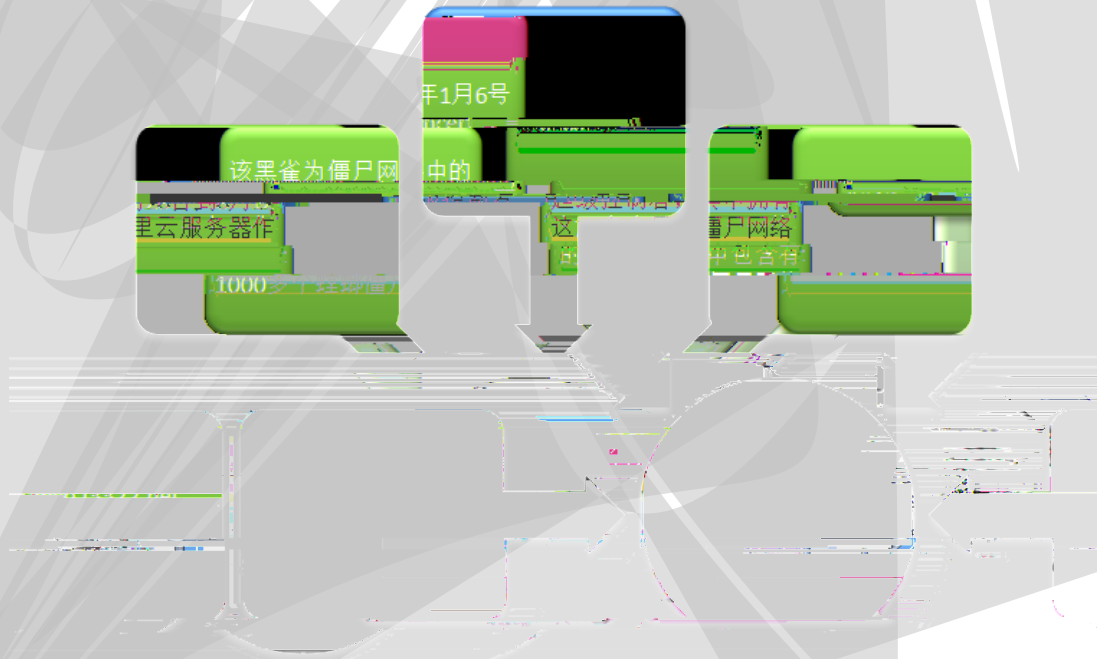


3

120.26.53.74

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
7.0/23	2015-06-15 10:00:00	2016-07-03 10:30:00	118.60.0.152	22.217A-1
0.0/14	2015-05-26 05:47:21	2015-06-12 00:00:00	120.26.53.74	CN

5.5



- “ Death ”

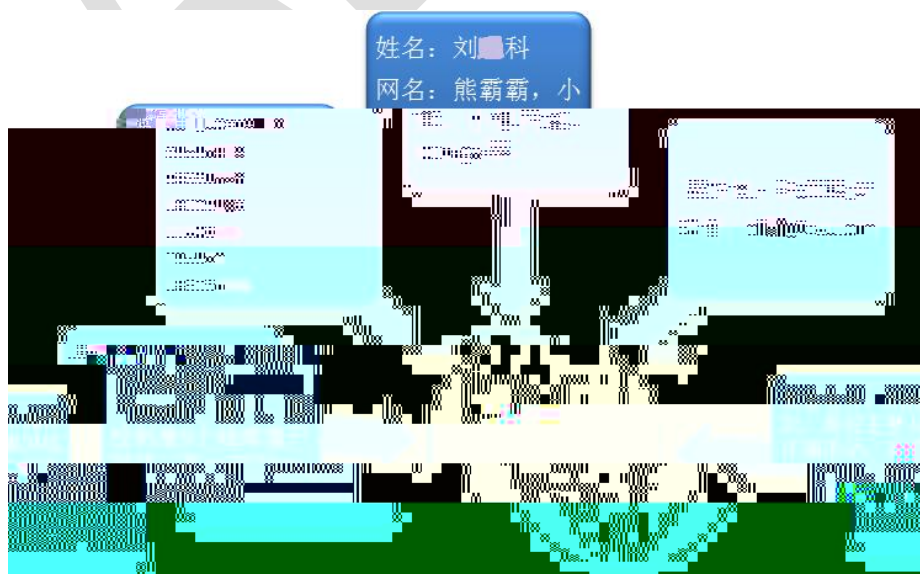
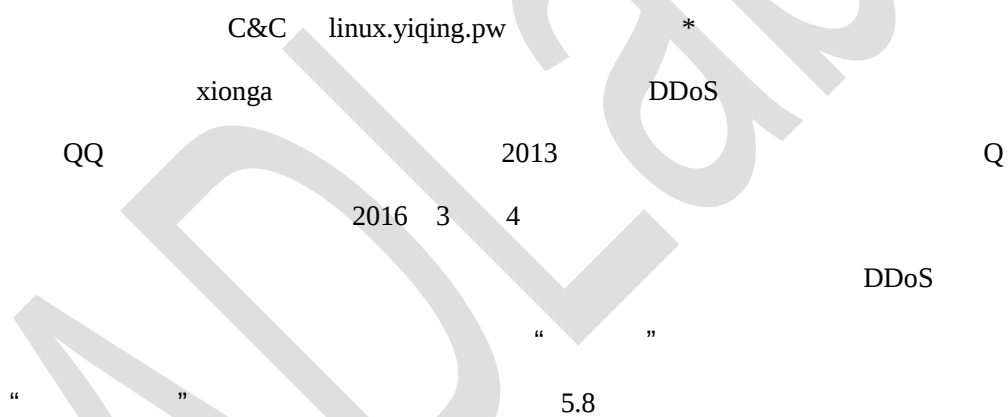
5.3 Q

Q “ Death ”

ADLab



5.7 Q



5.8 Q

- “ Death ”

- “Death”

- “Death”

- “ Death ”



- “Death”

ADLab

6.6

C&C

C&C

6.7 Q

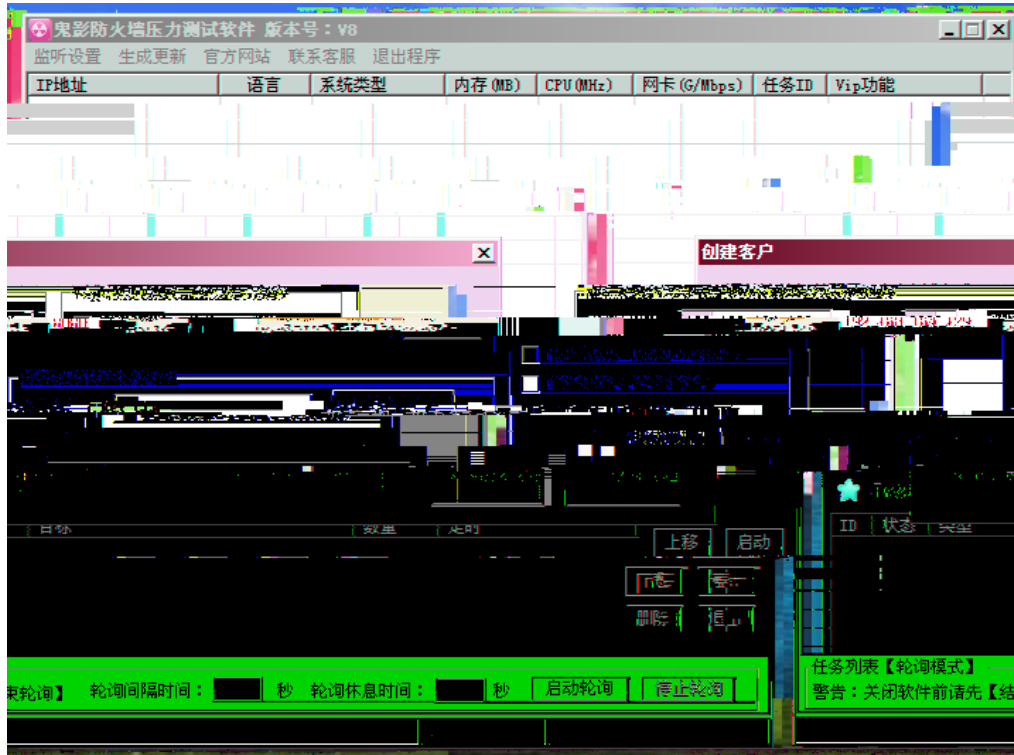
2

C&C

- “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

"

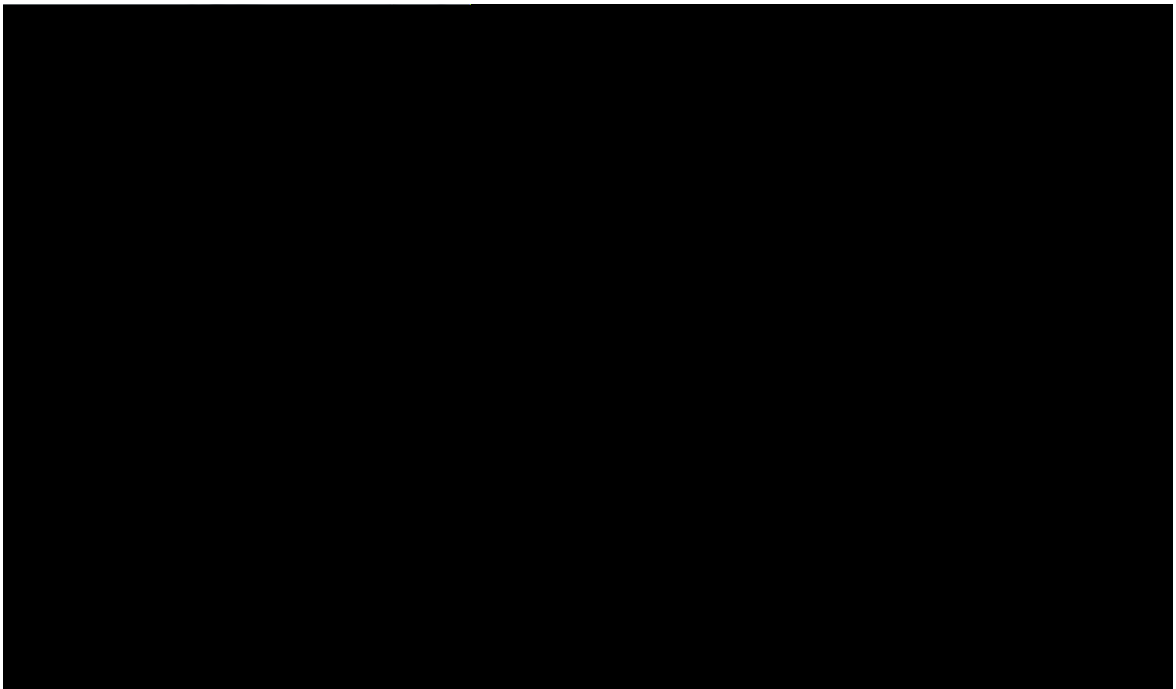
"Death "

Nitol

Nitol

Nitol

- “Death”



ADLab

- “Death”

AD

- “Death”