
CHINA TELECOM
NSFOCUS
201
HREAT REPORT
DD
胁报告


云堤
SECURITY

“ ”


NSFOCUS

2016 DDoS DDoS
2016 DDoS 22 18.6%
2015 50-100Gbps 2016 Q4
172.6% 300Gbps Q3 522.2% DDoS
DDoS

DDoS DDoS
DDoS DDoS
2016 DDoS

DDoS ,
, 2016 DDoS 2016
DDoS 2016 DDoS DDoS
2016 DDoS DDoS

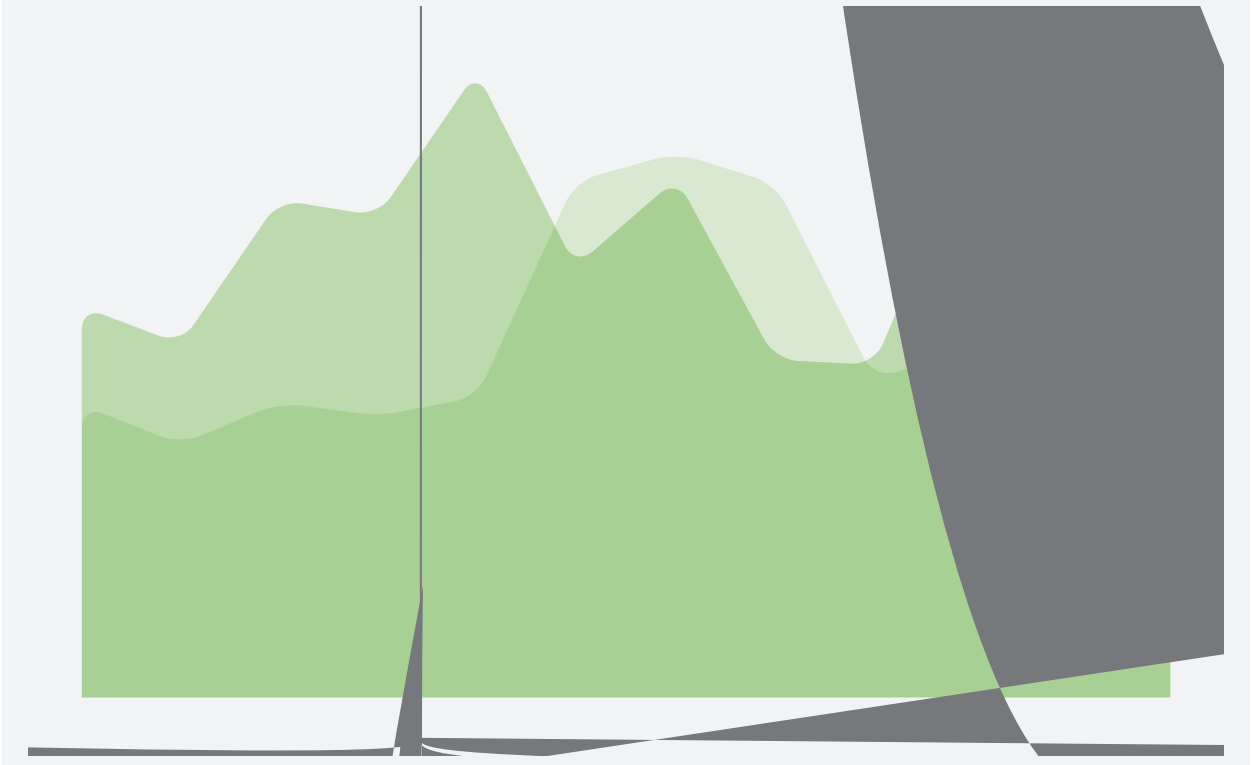
DDoS


2016 DD
D

DDoS

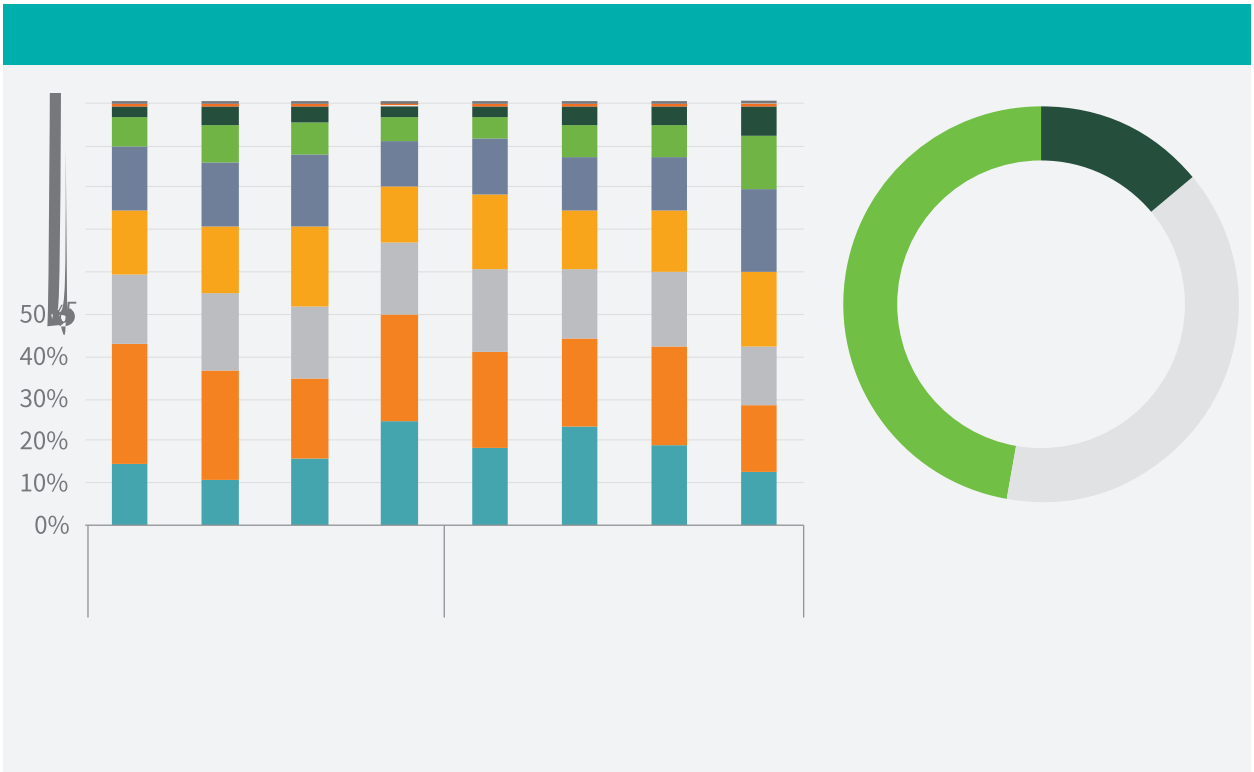
2016 DDoS 22 18.6% 1
15 36 TBytes 25%

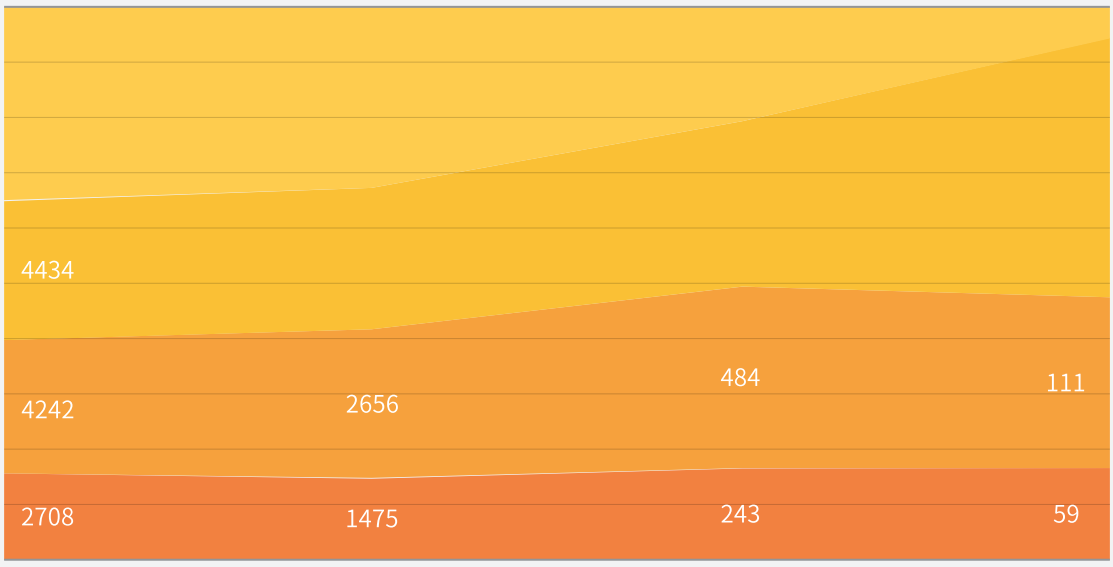
2016 DDoS
Mirai

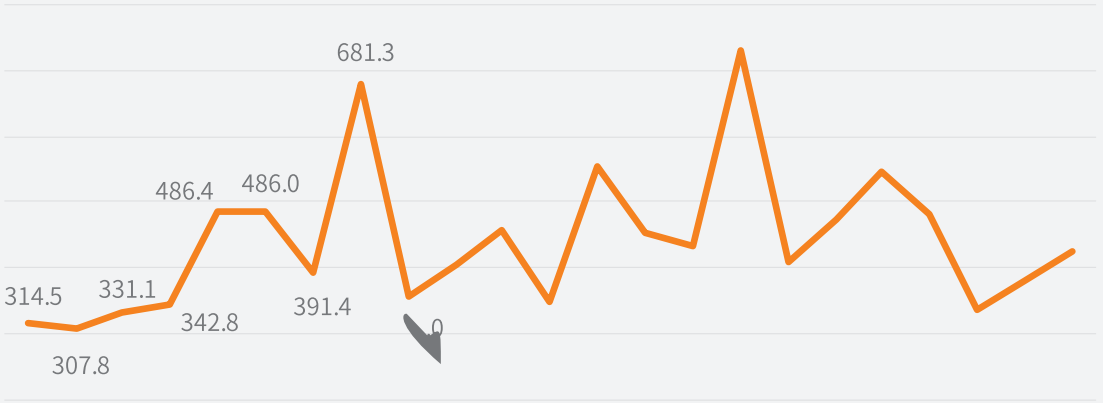


2016 5Gbps 39.1%
2 5-50Gbps 47.4% 0.2 50Gbps
13.5% 2.2

2016




4434
4242
2656
484
111
2708
1475
243
59

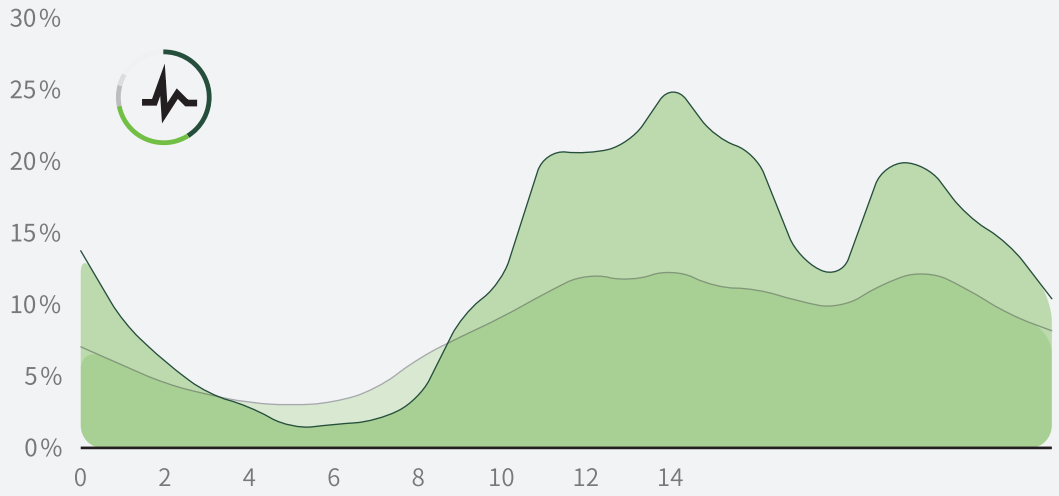

681.3
486.4
486.0
314.5
331.1
342.8
391.4
307.8
0

5Gbps 10-23

79.6% 100Gbps 10-23 82.5%

2 11-16

43.4% 14 19-20 13.3%



2016 30 DDoS 51.4%

5

2016

100Gbps

5

Gbps

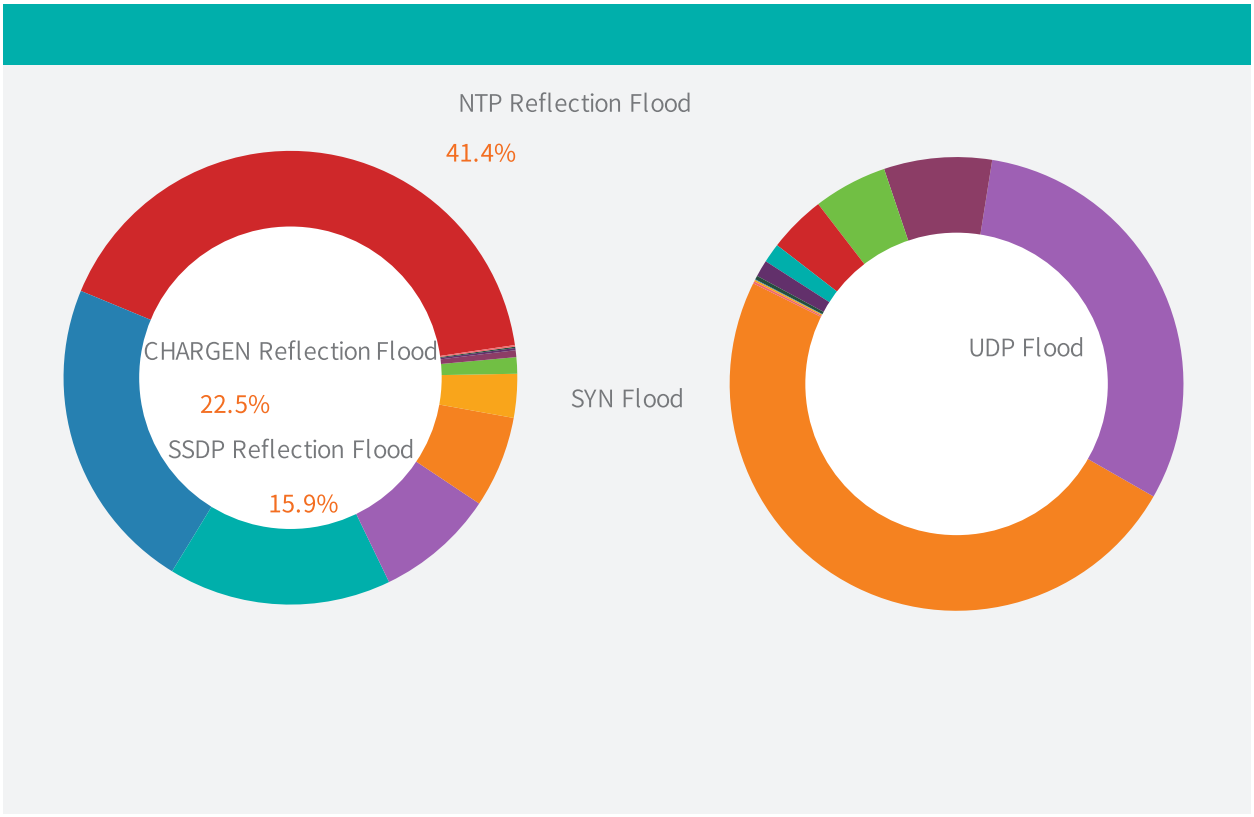
DDoS ATM

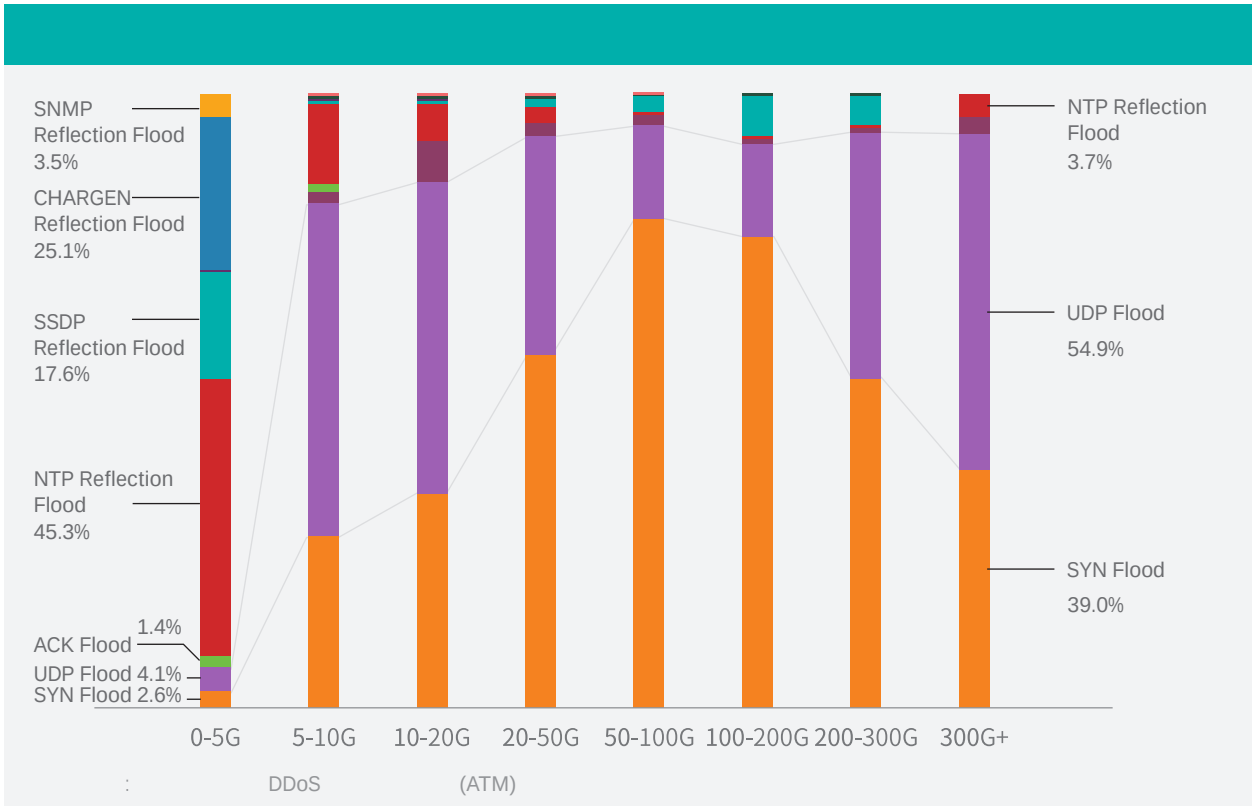
2016 Top 3 DDoS NTP CHARGEN SSDP 80%

IP

DDoS DDoS

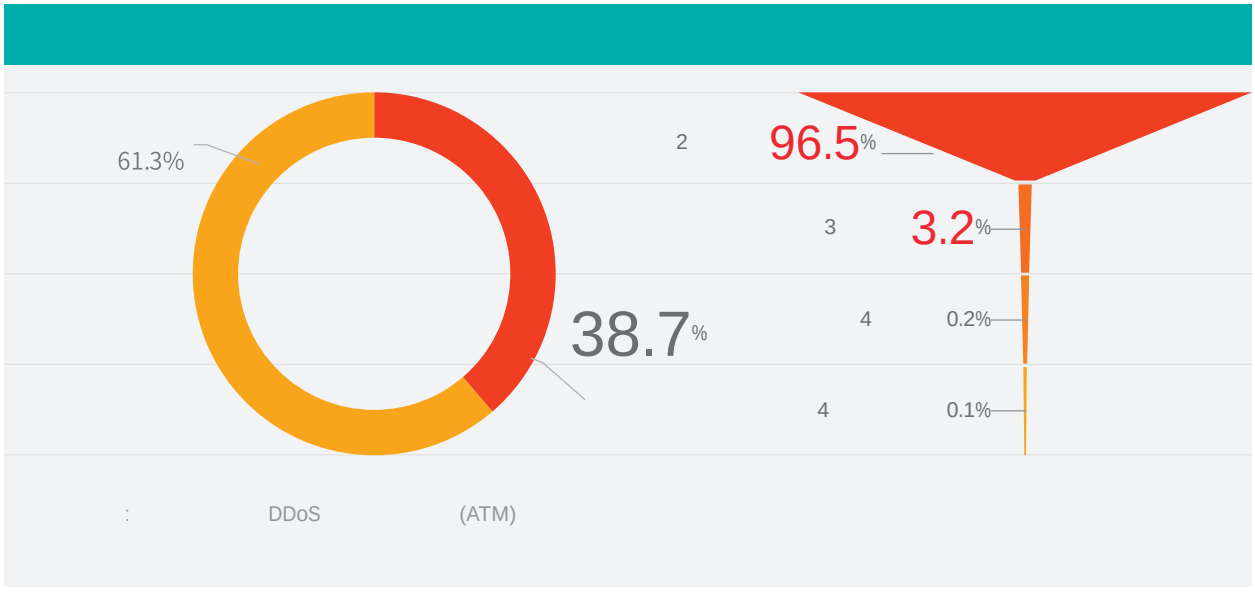
DDoS


NTP Reflection Flood
41.4%
CHARGEN Reflection Flood
22.5%
SSDP Reflection Flood
15.9%
SYN Flood
UDP Flood



2016 38.7%

DDoS-for-Hire

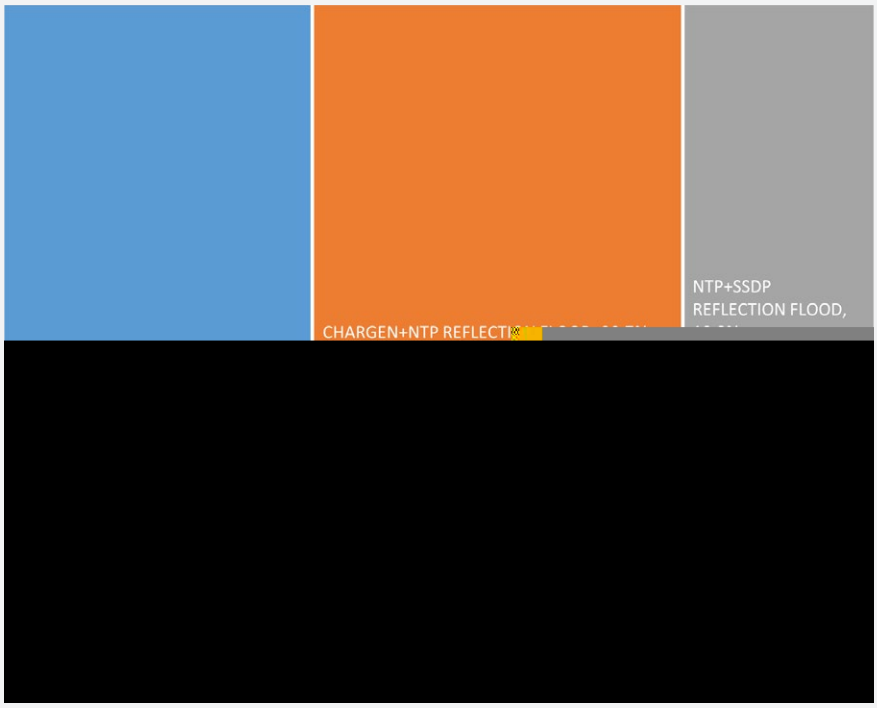


99.7%

SYN Flood UDP Flood

34.8% CHARGEN NTP

NTP SSDP UDP UDP



: DDoS (ATM)

2.3.1 2016

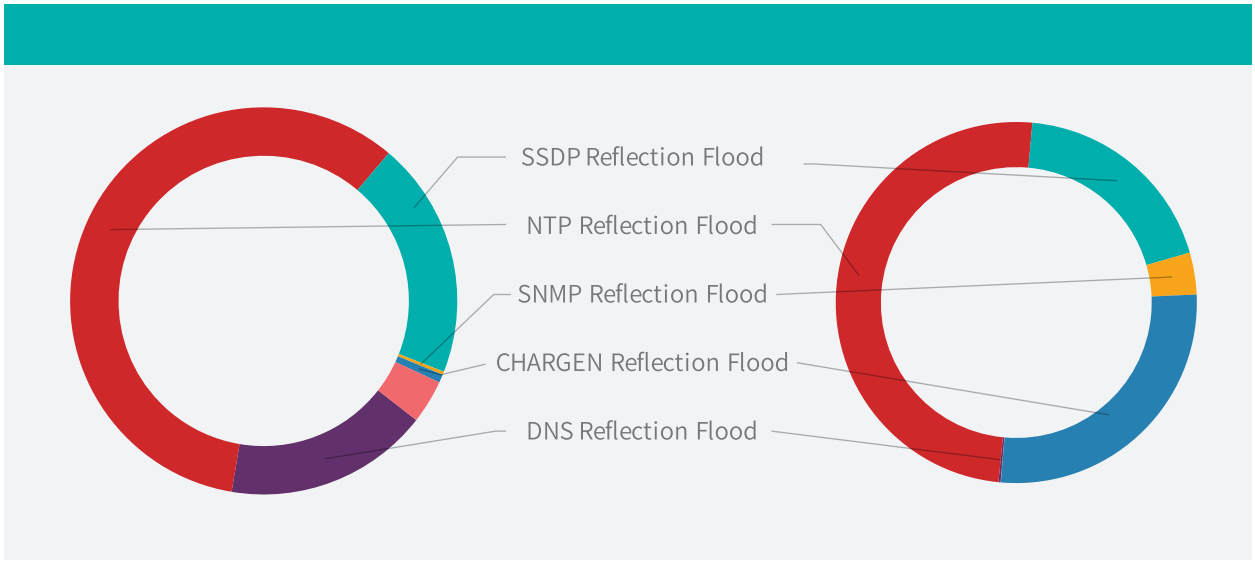
NTP Reflection Flood SSDP Reflection Flood

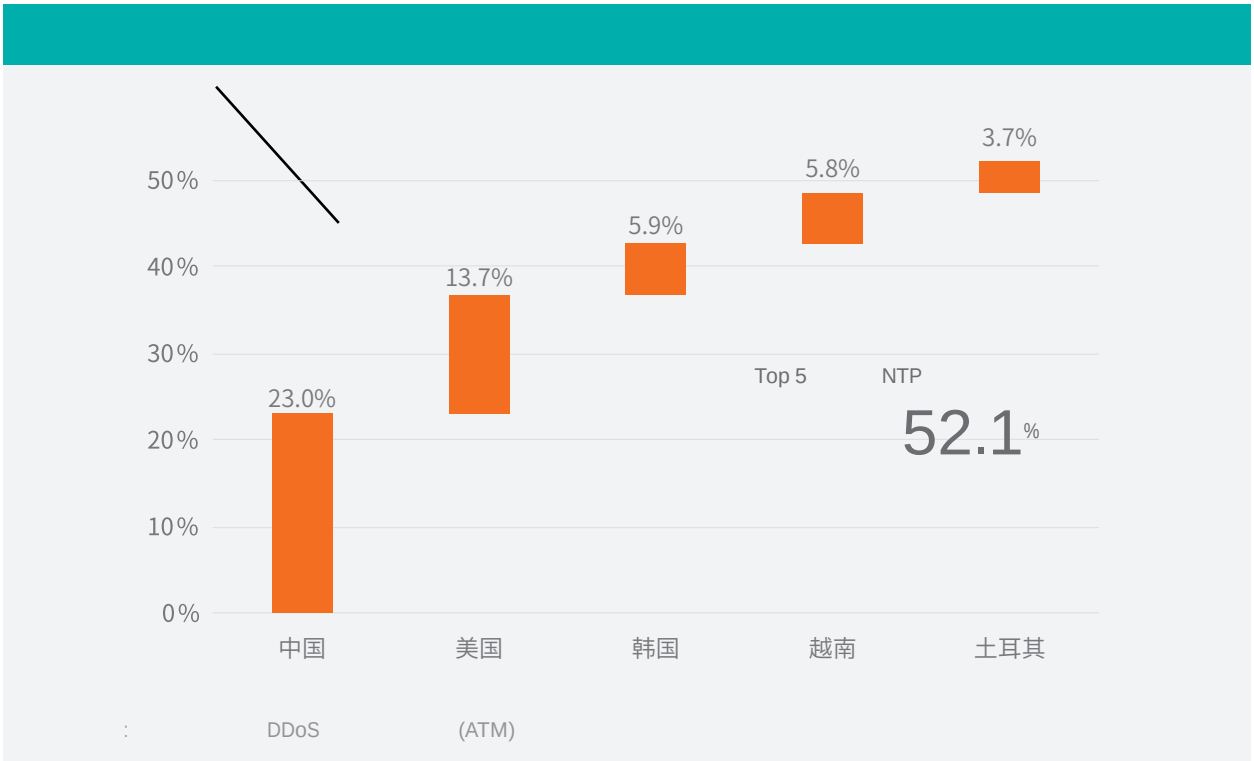
NTP Reflection Flood 58.5%

SSDP Reflection Flood DNS Reflection Flood 19.8% 17.1%

NTP Reflection Flood 49.8%

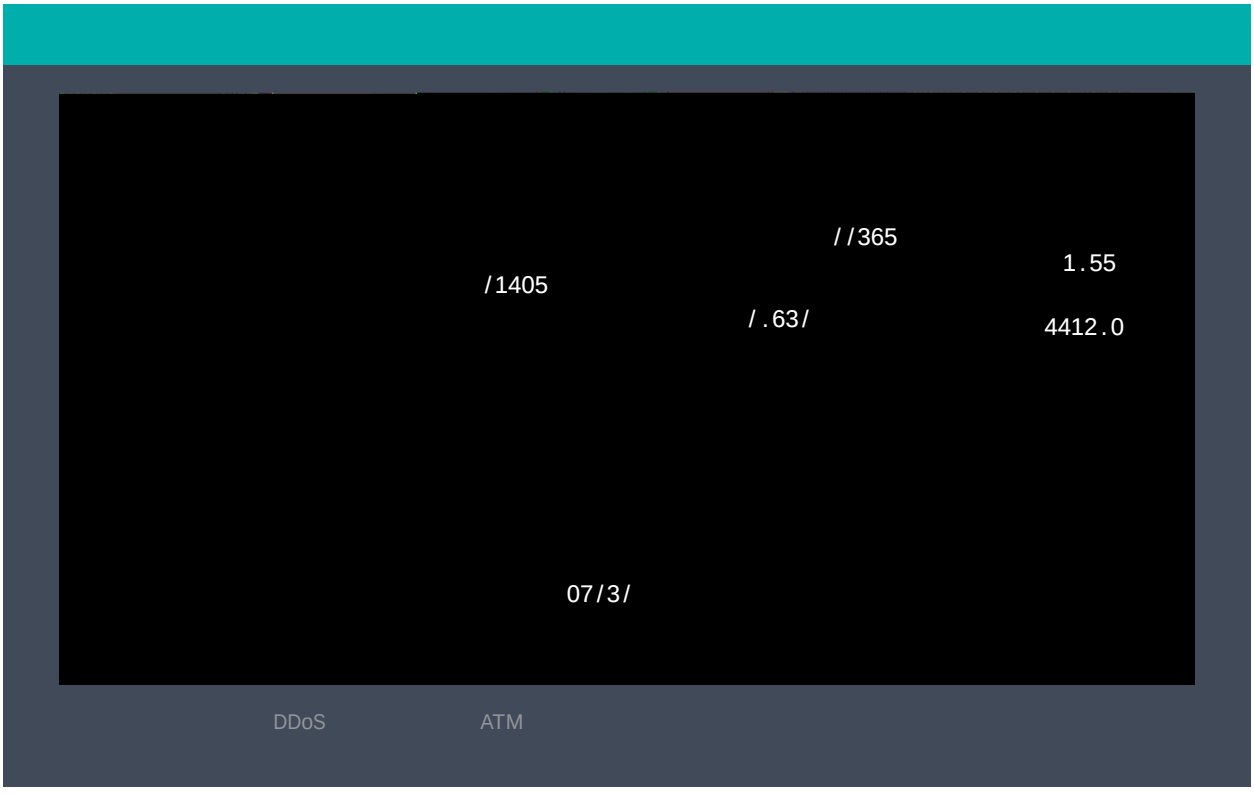
CHARGEN Reflection Flood SSDP Reflection Flood 27.1% 19.1%

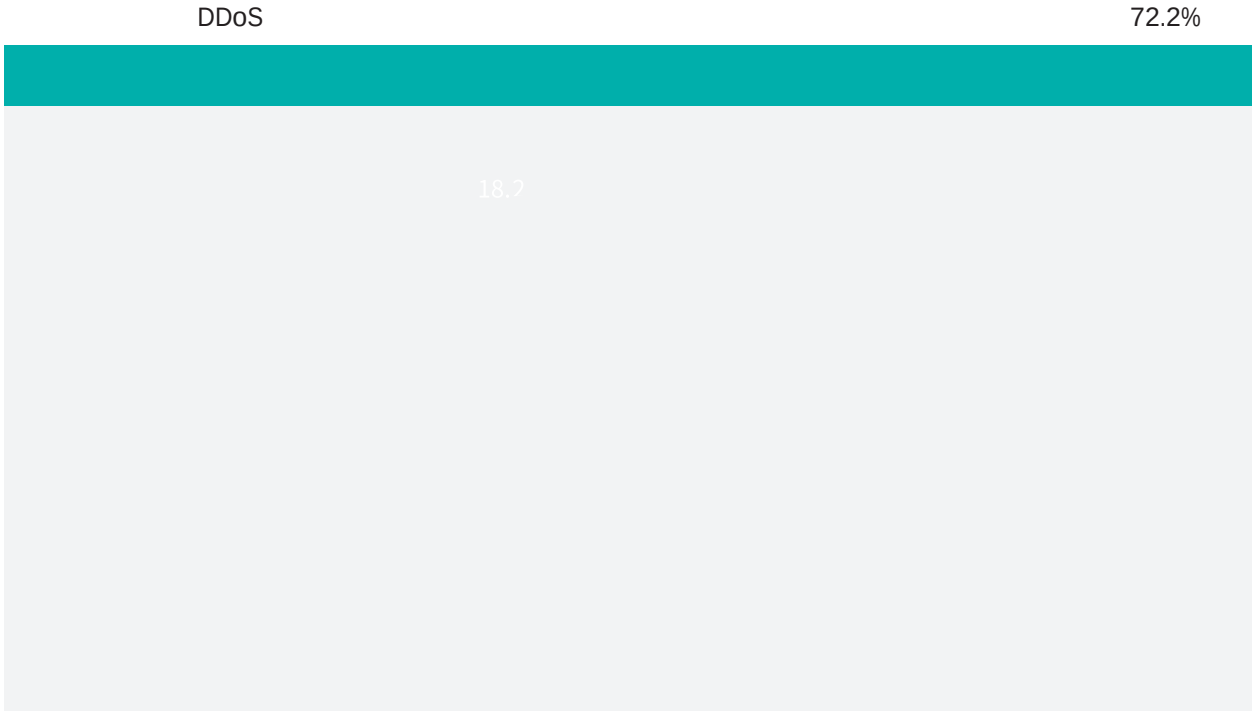

SSDP Reflection Flood
NTP Reflection Flood
SNMP Reflection Flood
CHARGEN Reflection Flood
DNS Reflection Flood

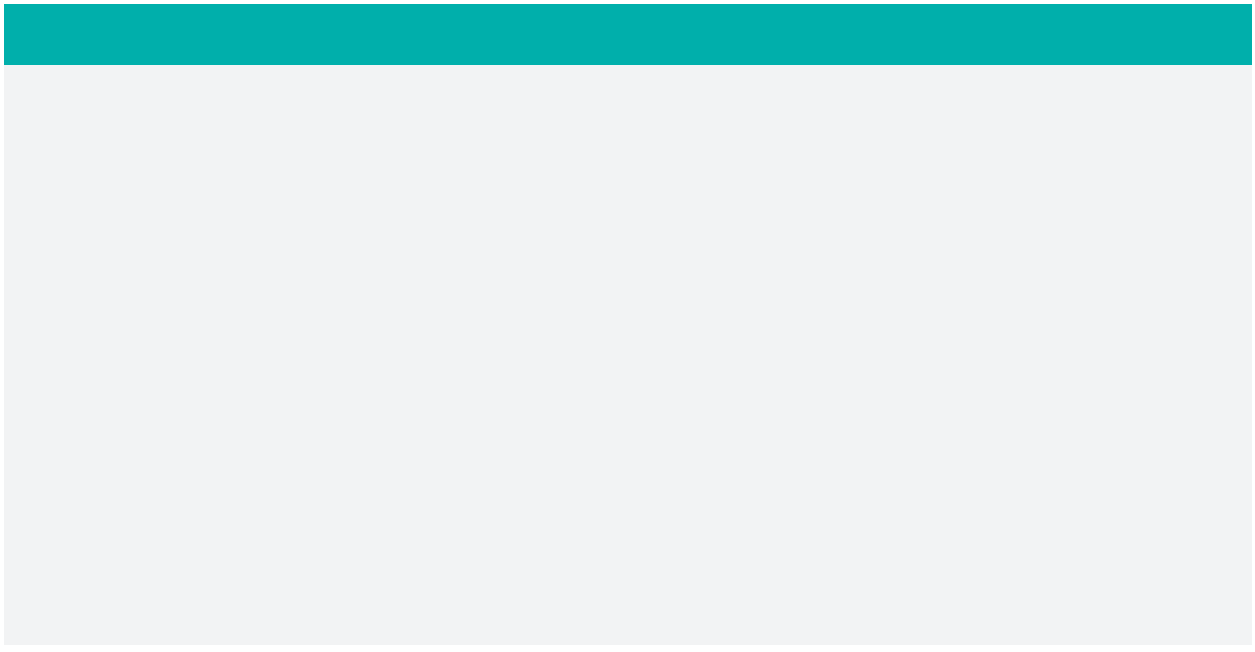


2016 SSDP 795,616

2016 Q4 SSDP SSDP




DDoS
72.2%
18.2

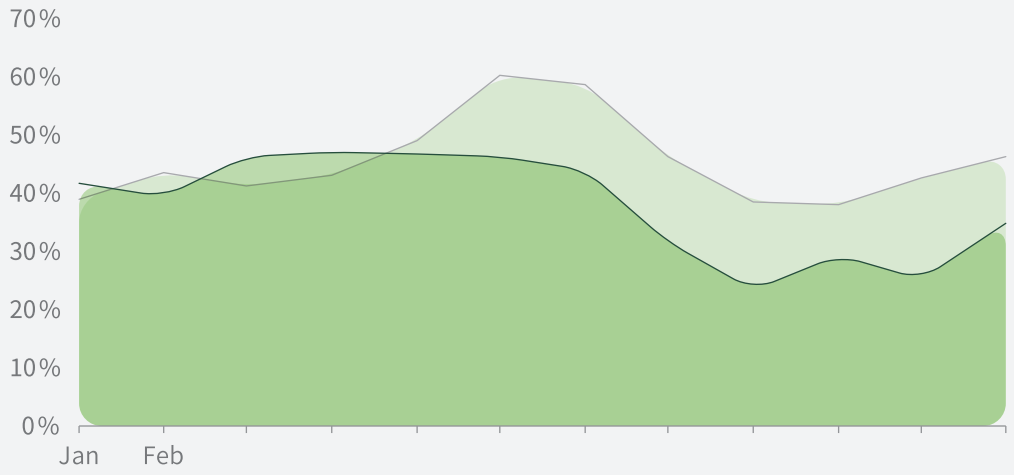


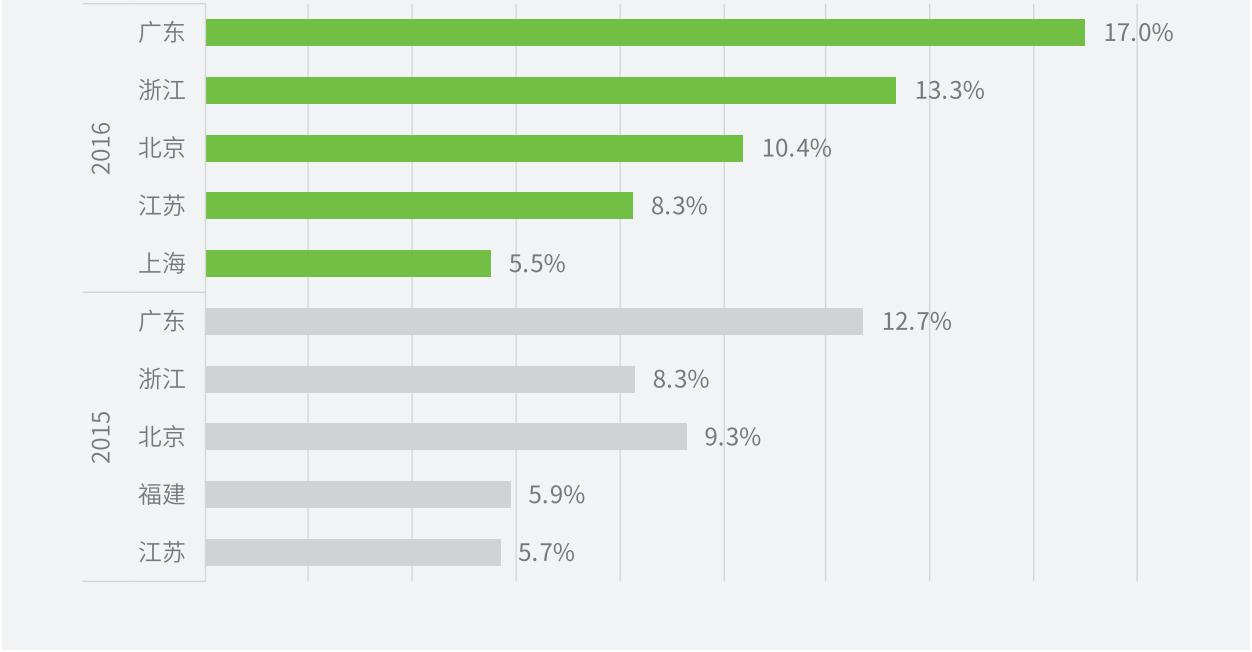
2015 2016 6

8-17 DDoS

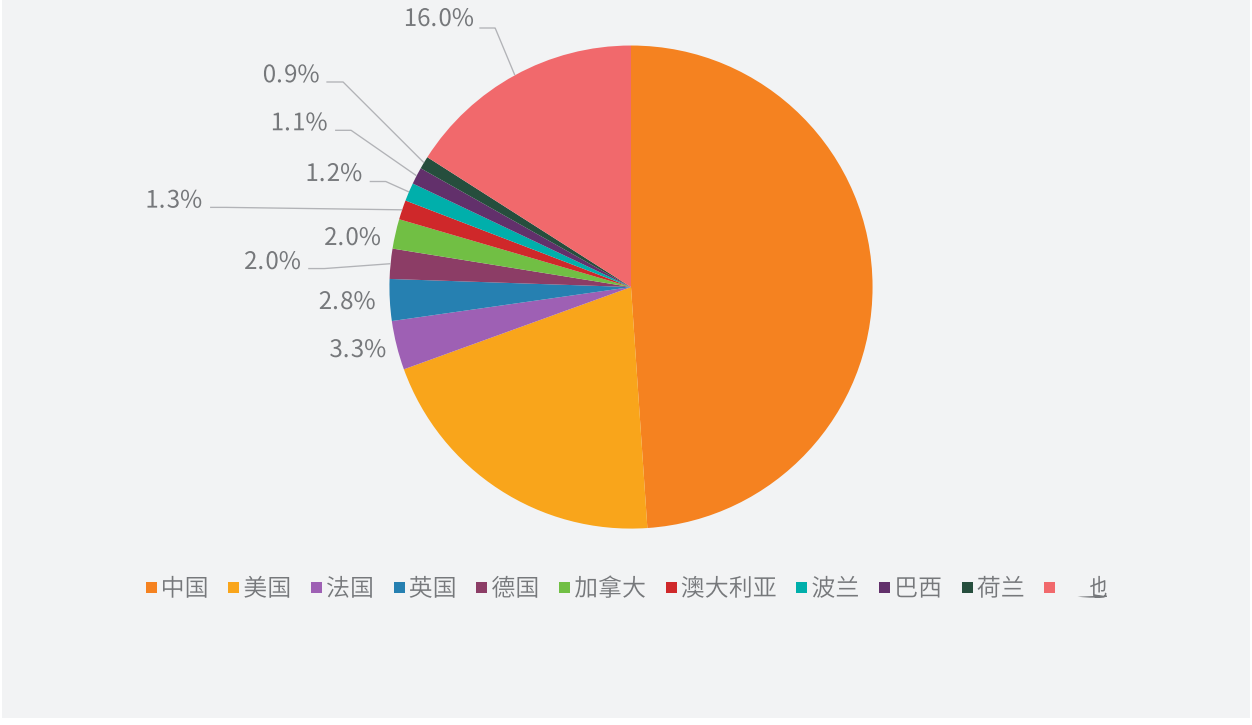
11 54.4% 18.7 2.4.1

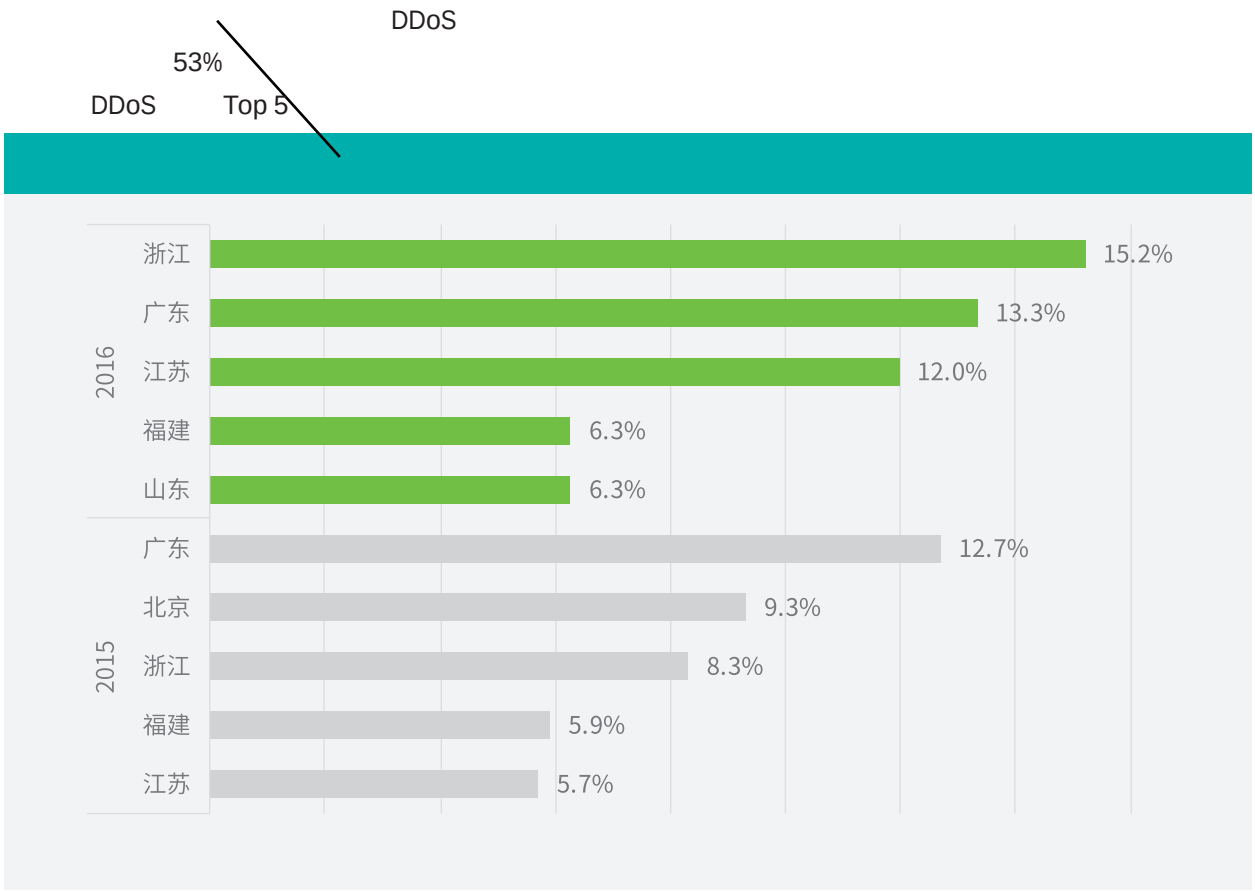
44.3%




2016
广东 17.0%
浙江 13.3%
北京 10.4%
江苏 8.3%
上海 5.5%
2015
广东 12.7%
浙江 8.3%
北京 9.3%
福建 5.9%
江苏 5.7%

48.9% 20.5%


16.0%
0.9%
1.1%
1.2%
1.3%
2.0%
2.0%
2.8%
3.3%
中国 美国 法国 英国 德国 加拿大 澳大利亚 波兰 巴西 荷兰 也

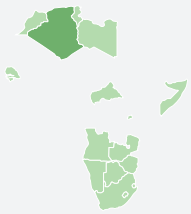

DDoS
53%
DDoS
Top 5
2016
浙江
15.2%
广东
13.3%
江苏
12.0%
福建
6.3%
山东
6.3%
2015
广东
12.7%
北京
9.3%
浙江
8.3%
福建
5.9%
江苏
5.7%

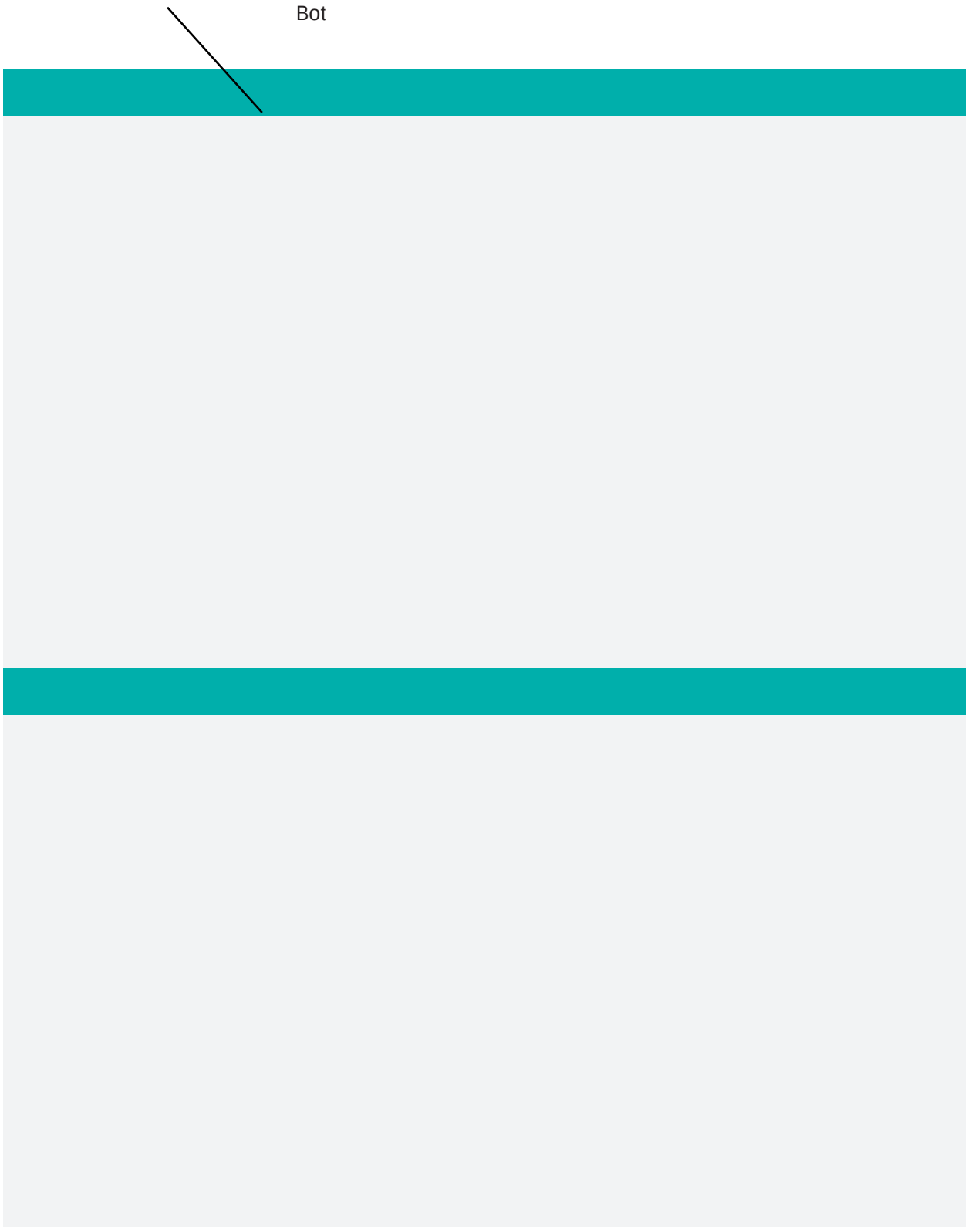
“ ”

“ ”

2016 BotMaster 120

Top 5 BotMaster 27%




Bot

Internet of Things IoT

2016 10

12

Lizardstresser Mirai Luabot DDoS

IoT Botnet Botnet

Bot PC Server

2016 10 “ ” 11 “ ”

DDoS

Mirai Mirai 57

2016

-	-	Report -	Report -		
g ng	23	re cing	48101	2016/5/28	
fu t.com	23	lu m	48101	2016/7/26	
la .cf	23	re ttenjoh.cf	48101	2015/11/16	
im	1367	yc	48202	2016/10/16	
lo g	23	dc cing	48101	2016/5/28	
sv u	23	ne me.ru	48101	2016/8/22	
sv u	23	sv u	48101	2016/8/22	
tv	23	tv	48101	2014/11/18	2016/6/13
fu k.com	23	fu com	53	2011/3/3	2016/4/14
ne gcandycane.cx	23	re candycane.cx	48101	2016/9/15	
he	23	sh	48202	2016/10/16	
hi ub	666	re ime.club	48101	2016/10/24	
ft yz	23	lis r.xyz	48101		
sc	23	sc	48101	2016/10/27	
cr ng	23	re cing	48101	2016/5/28	
ka t.xyz	23	re xyz	48101		
se us	23	re es.us	4810	2016/9/4	2016/9/4
lo	23	r.l	37065		
6 s.net	2047	e s.net	20470	1999/4/22	2016/5/26
ti	23	ti	4810	2004/11/18	2016/10/27
m e	23	re e	48101	2015/11/14	
b .xyz	23	ct net.xyz	48101		
cr com	23	lis s.com	48101	2016/11/8	2016/11/12
cr	23	re ow	48202		
au om	23	m n	48202	2016/11/16	2016/11/16
si	23	op th.us	4810	2016/9/4	2016/12/11
cr com	23	lo om	48101	2016/12/12	2016/12/12
al	23	tr s	48110		
cr	23	re	48101	2016/7/8	2016/7/26
cr	23	re net	48101	2001/6/29	2014/8/15
ur	23	ur	48101		

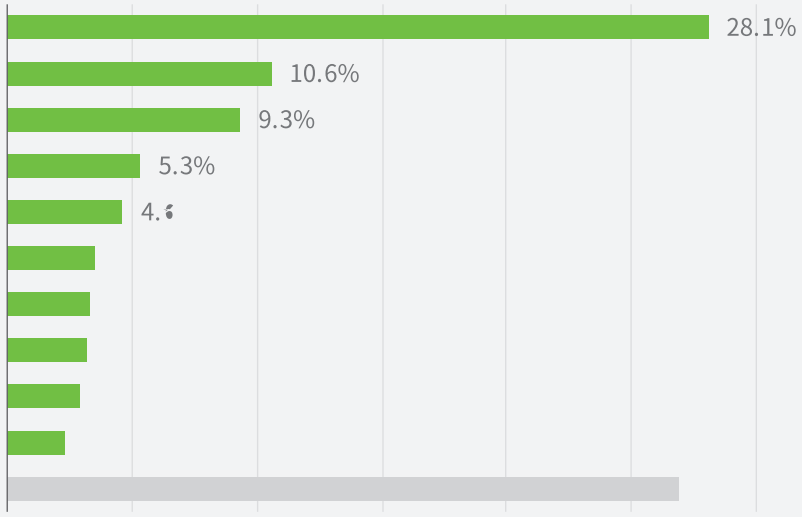
-	-	Report -	Report -		
ov[redacted]s.org	23	ov[redacted]s.org	48101	1998/11/22	
cr[redacted]	23	re[redacted]	44110	2015/3/4	2016/2/3
u[redacted]	23	bo[redacted]	48101	2001/8/10	2013/4/19
cr[redacted]	16741	re[redacted]	36637		
cr[redacted]ce	23	re[redacted]e	48101		
do[redacted]	23	co[redacted]e.ru	48101	2017/1/10	
w[redacted]lesixtodeath.top	23	do[redacted]todeath.top	48101	2016/11/28	
cr[redacted]	23	so[redacted]	48101	2016/7/9	
cz[redacted]	23	ha[redacted]b	47202	2017/1/14	
q5[redacted]x9m4g.ru	23	xg[redacted]'gu55d.q5f2k0evy7go2rax9m4g.ru	48101	2016/10/28	
ne[redacted]	23	re[redacted]g	48101	2016/3/25	
w[redacted].org	23	w[redacted].org	4810	2016/9/20	
ou[redacted]	23	re[redacted]	48101	2016/8/19	
qb[redacted]	23	w[redacted]xyz	48101		
cr[redacted]	443	re[redacted]m	10184	2017/1/24	
ba[redacted]om	23	rp[redacted]n	8000	2016/6/29	
w[redacted]g.ru	28610	w[redacted]ru	56817		
ne[redacted]ir		ne[redacted]ir	48101		2017/2/4
fla[redacted]	23	fla[redacted]	48101	2016/12/22	
cr[redacted]z	23	re[redacted]xyz	48101		
tra[redacted]	23	co[redacted]ru	48101	2017/2/11	
c.[redacted]	23	r.c[redacted]	48101		
nu[redacted]	23	nu[redacted]	48101		
br[redacted]	23	br[redacted]	48101	2017/2/17	
ba[redacted]n	23	rp[redacted]	8000	2017/2/15	2017/2/15
kr[redacted]wang	443	rd[redacted]ng	48101	2017/2/4	

DDoS

Mirai 200 Mirai

Bot Top 10

NTI


28.1%
10.6%
9.3%
5.3%
4.

2017 Mirai 2016 Q3 20 /

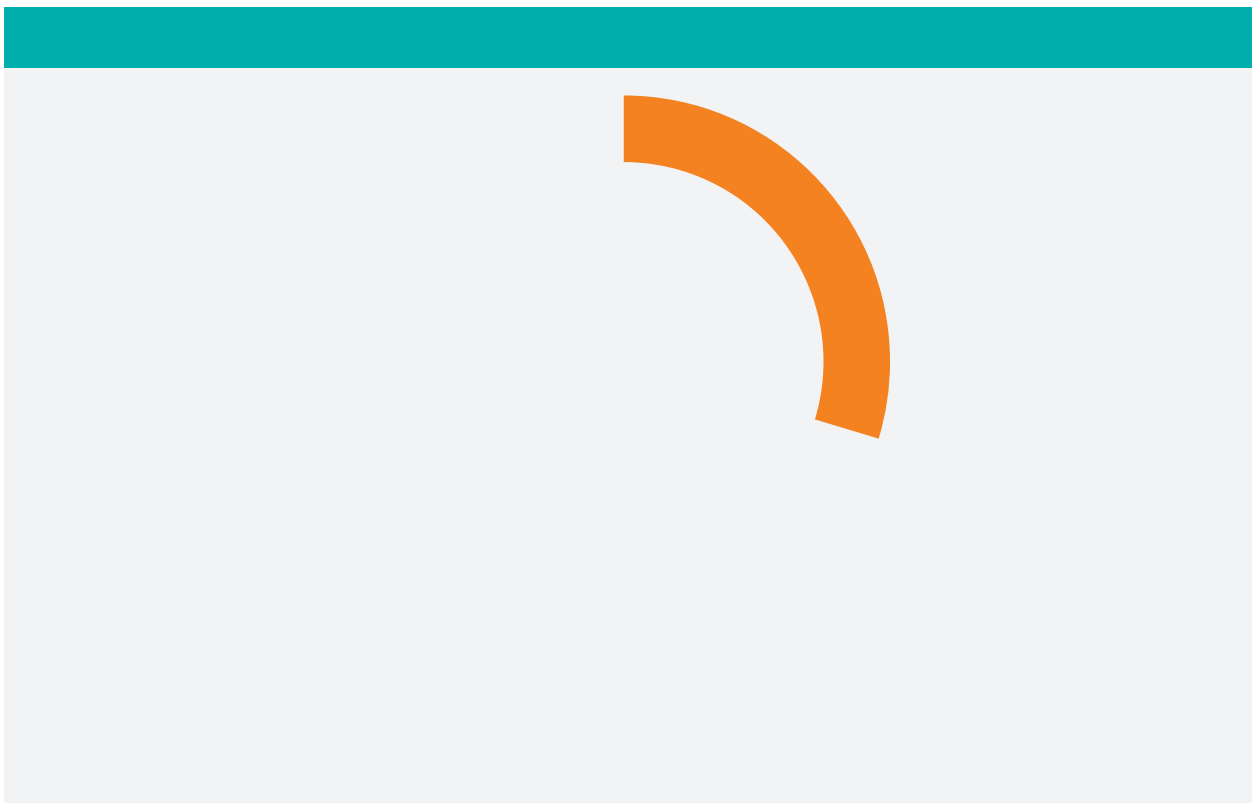
1. Mirai 2016

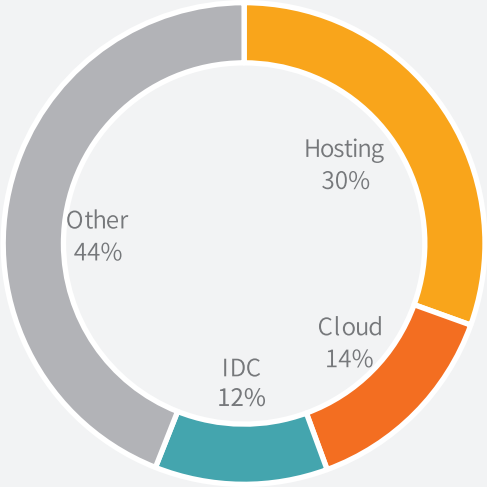
2. Mirai

Mirai AES.DoS Luabot Hajime DDoS

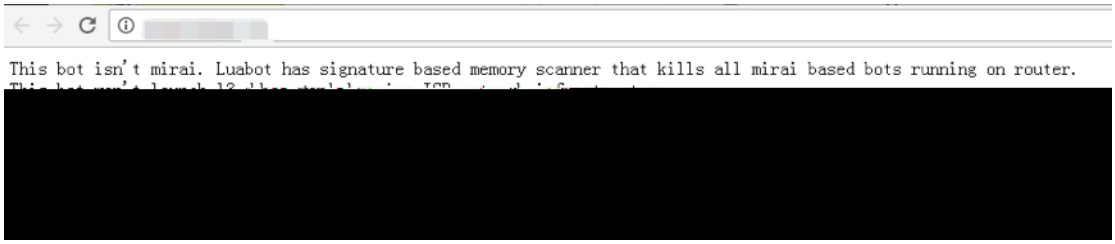
DDoS tfddos

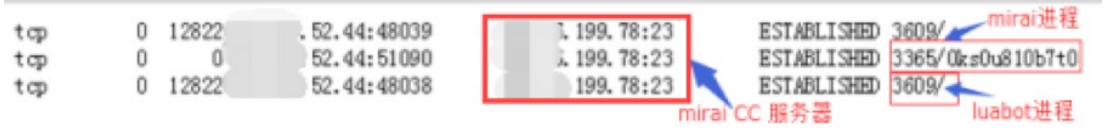
C&C 1000 76%




Hosting
30%
Cloud
14%
IDC
12%
Other
44%

DDoS


This bot isn't mirai. Luabot has signature based memory scanner that kills all mirai based bots running on router.


tcp 0 12822 52.44:48039 199.78:23 ESTABLISHED 3609/
tcp 0 0 52.44:51090 199.78:23 ESTABLISHED 3365/Oksou810b7t0
tcp 0 12822 52.44:48038 199.78:23 ESTABLISHED 3609/
mirai进程
mirai CC 服务器
luabot进程

DDoS

Gartner Inc. 2016 550 2020 208

2016

1. 2016 2 GSM GSMA, Group Special Mobile Association IoT
2. 2016 2 CSA, Cloud Security Alliance Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products
3. 2016 5 Web OWASP, Open Web Application Security Project
4. 2016 11 BITAG, Broadband Internet Technical Advisory Group Internet of Things (IoT) Broadband Internet Technical Advisory Group
5. 2016 12 IoT IoTs, IoT Security Foundation IoT Security Compliance Framework 1.0
6. 2016 12

1. 2016 10
2. 2016 11 DHS
3. 2016 3 “ ”
4. 2016 11

2016 9 20 KrebsonSecurity.com
Mirai 620Gbps DDoS vDOS Krebs
vDOS Krebs

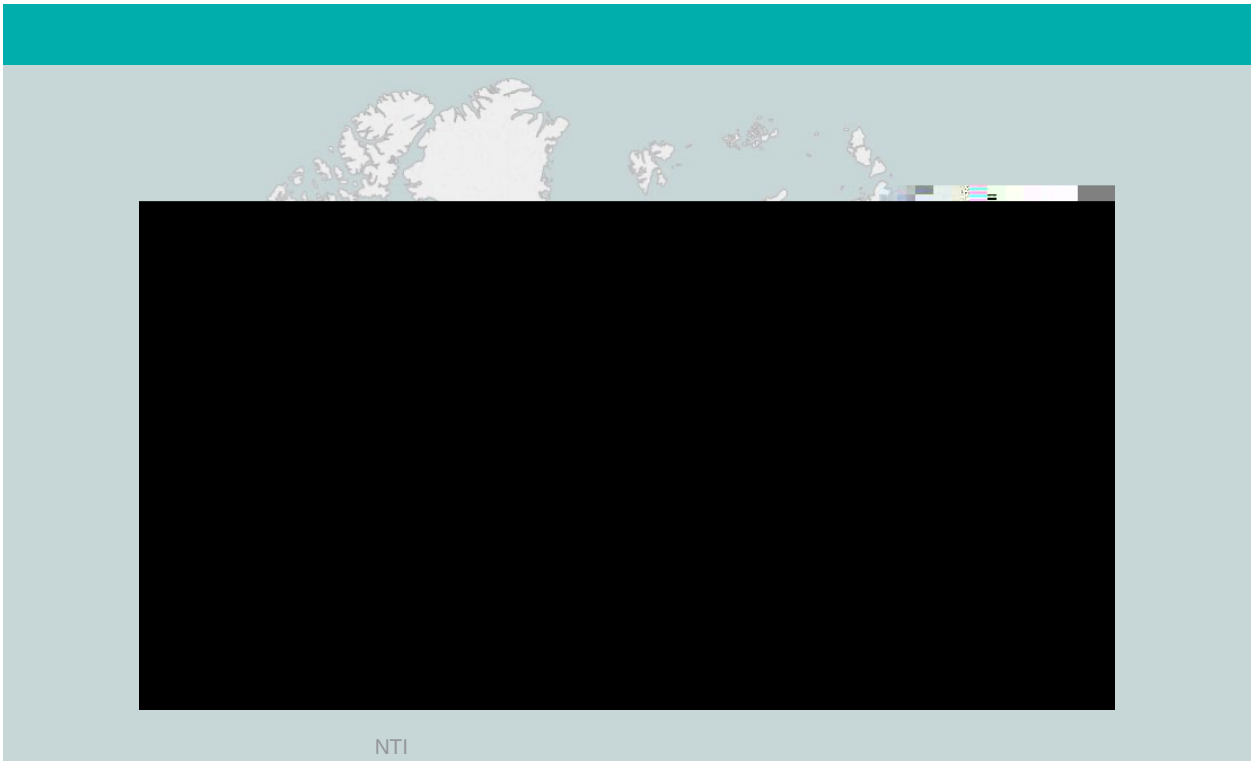
9 21 OVH CTO Octave Klaba Twitter 145,607
1Tbps DDoS 1.5Tbps DDoS
Krebs OVH Mirai OVH

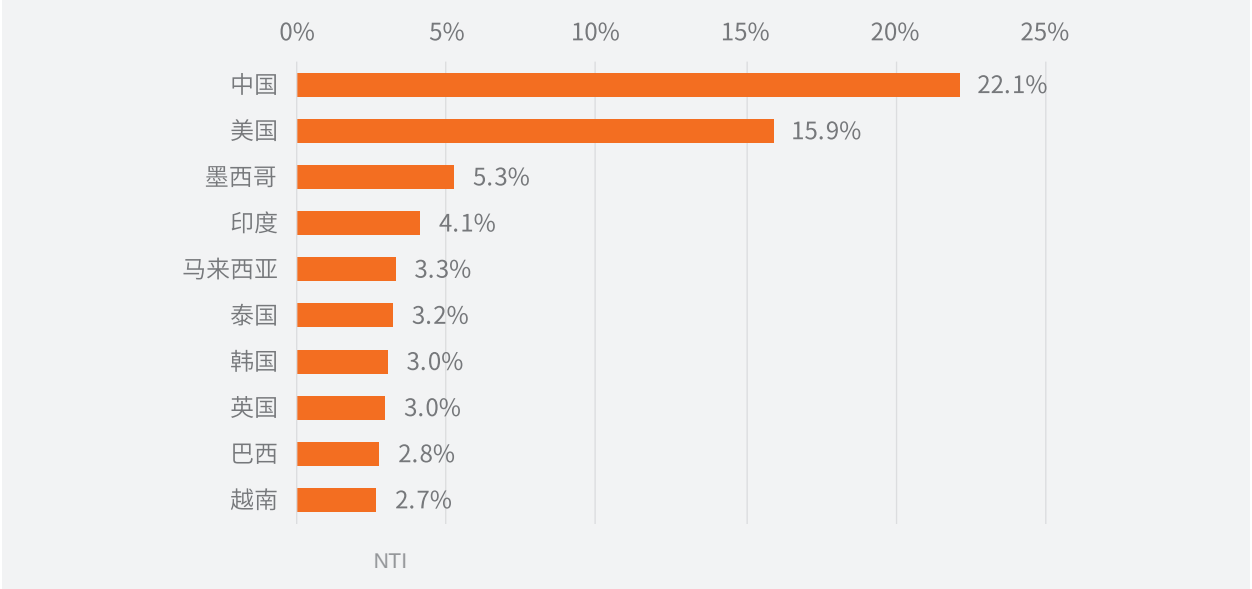
10 21 DNS DYN
DNS DynDNS DDoS Mirai
DynDNS GitHub Twitter Airbnb Reddit
DYN
“
”

11 90 2000

DDoS 2016 2016 Q3 DDoS
2016 Q3 300Gbp

2016



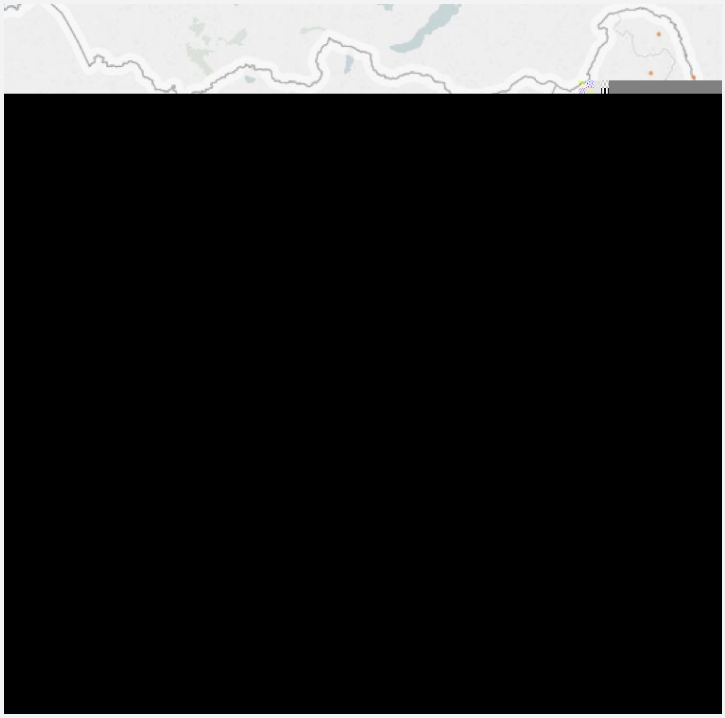


2016 50

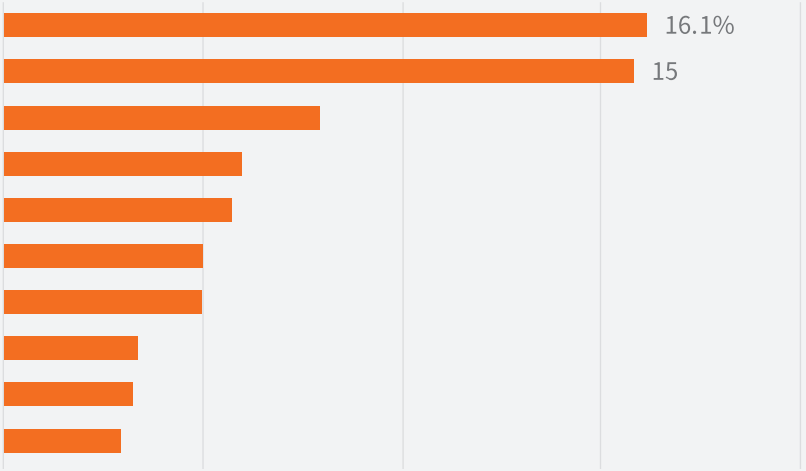
16.1%

TOP10 71.2% 28.8%

17



NTI



DDoS DDoS-For-Bitcoin Ransomeware Ransomware-for-Bitcoin DDoS DD4BC 140 DD4BC 10~200 Armada Collective Bitcoin DDoS

2016 3 “ Armada Collective ” 10~50 4600~2.3 1Tbps DDoS 10

DDoS-for-Bitcoin Armada Collective Proton Mail 20 DDoS Proton Mail

2017 Armada Collective DDoS 7~10 20-30 2 7 Tb DDoS 5 15 DDoS DDoS 2016 DDoS

Ransomware-as-a-service Ransomware-for-Bitcoin DDoS-as-a-service DDoS-for-Hire DDoS-for-BitcoinRxr 2016 “ ” FireCrypt DDoS DDoS Necurs Locky DDoS Necurs

DDoS DDoS DDoS 25% 30% DDoS

2016 8 5 -21 Anonymous OlympicHacking

DDoS

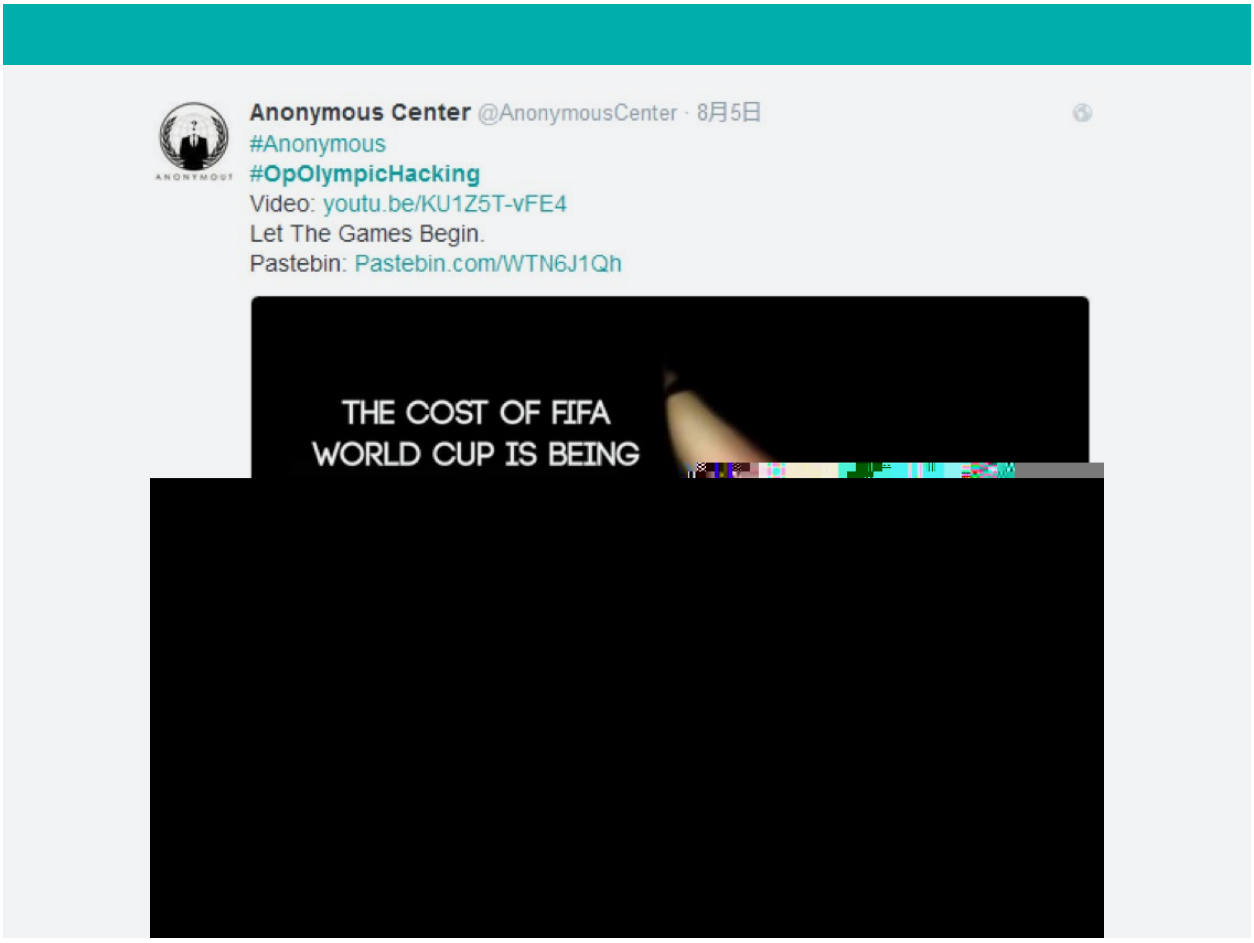
540Gbps 500Gbps Anonymous DDoS opolympddos

Windows LizardStresser Mirai

DNS NTP CHARGEN SSDP GRE Flood DDoS

DDoS

DDoS



DDoS

DDoS

1 - 5

DDoS-for-Hire DDoS

DDoS

1

Anonymous 4 1

trumptowerny.com 12 DDoS Anonymous

11 Mirai

30s HTTP layer7

2 11 IoT

Mirai DDoS

DDoS 500Gbps

Mirai Mirai

“ ”

3 DDoS

2016 5 Anonymous BannedOffline GhostSquadHackers

DDoS

4 5 DDoS

2016 11 5 DDoS 1

12 SYN Flood HTTP/HTTPS Flood 66

web web

Mirai 30

5 DDoS 2000

2016 4 Lizard Squad DDoS

“ Poodle Corp ”

DDoS 8 3 9 1

2000

6 DDoS

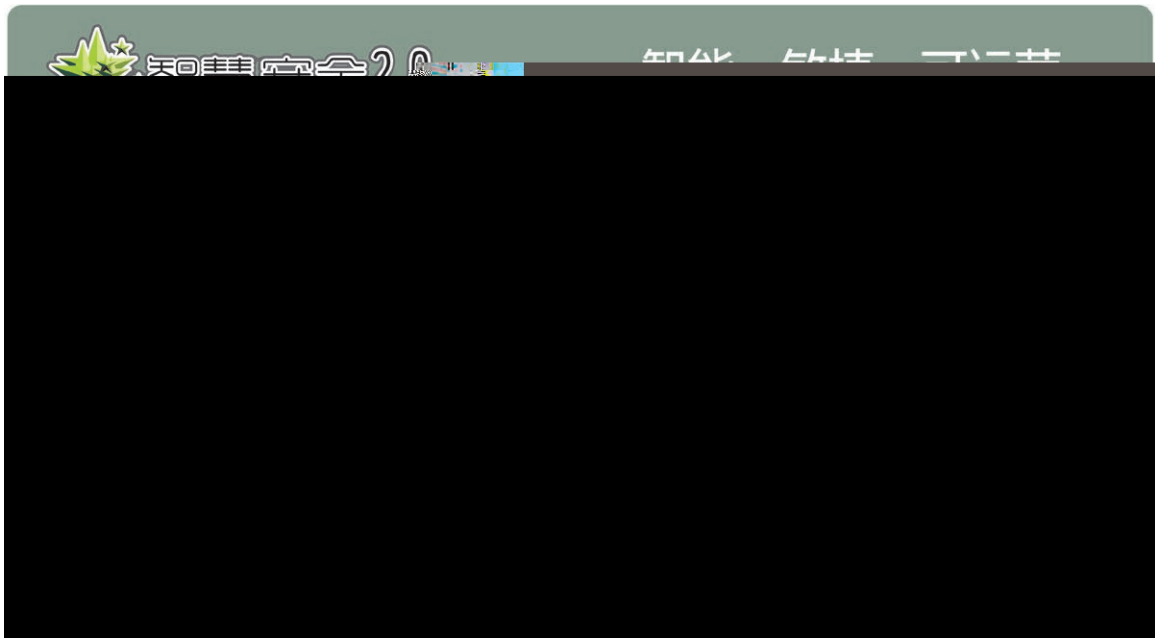
2016 12 DDoS 325.9Gbps DDoS

10Gbps 3 325.9Gbps

19

2015 “ ”

2.0



D 2016

		API IOS/Android

DDoS

Tbps

302 JS

DDoS D NTI

IP Botnet IP Bot

ADS

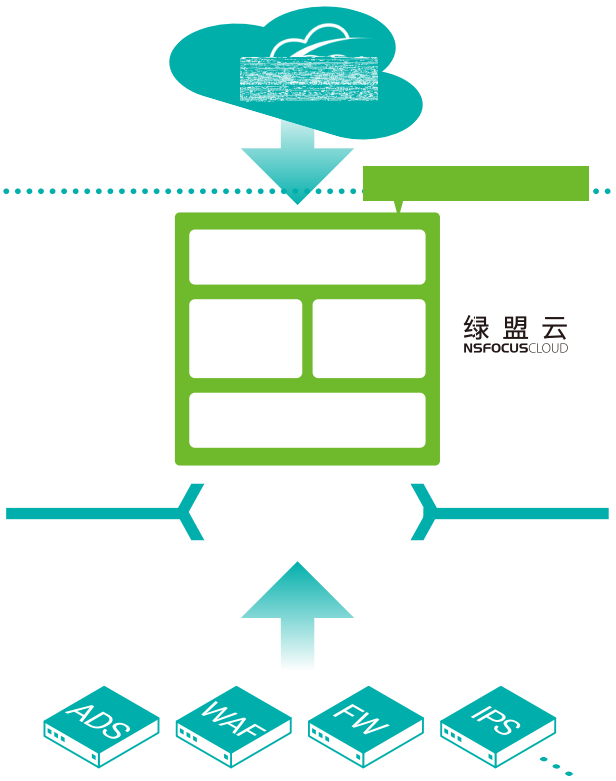
feed

DDoS DDoS

IT DDoS

/ “ ” “ ”

“ ” +



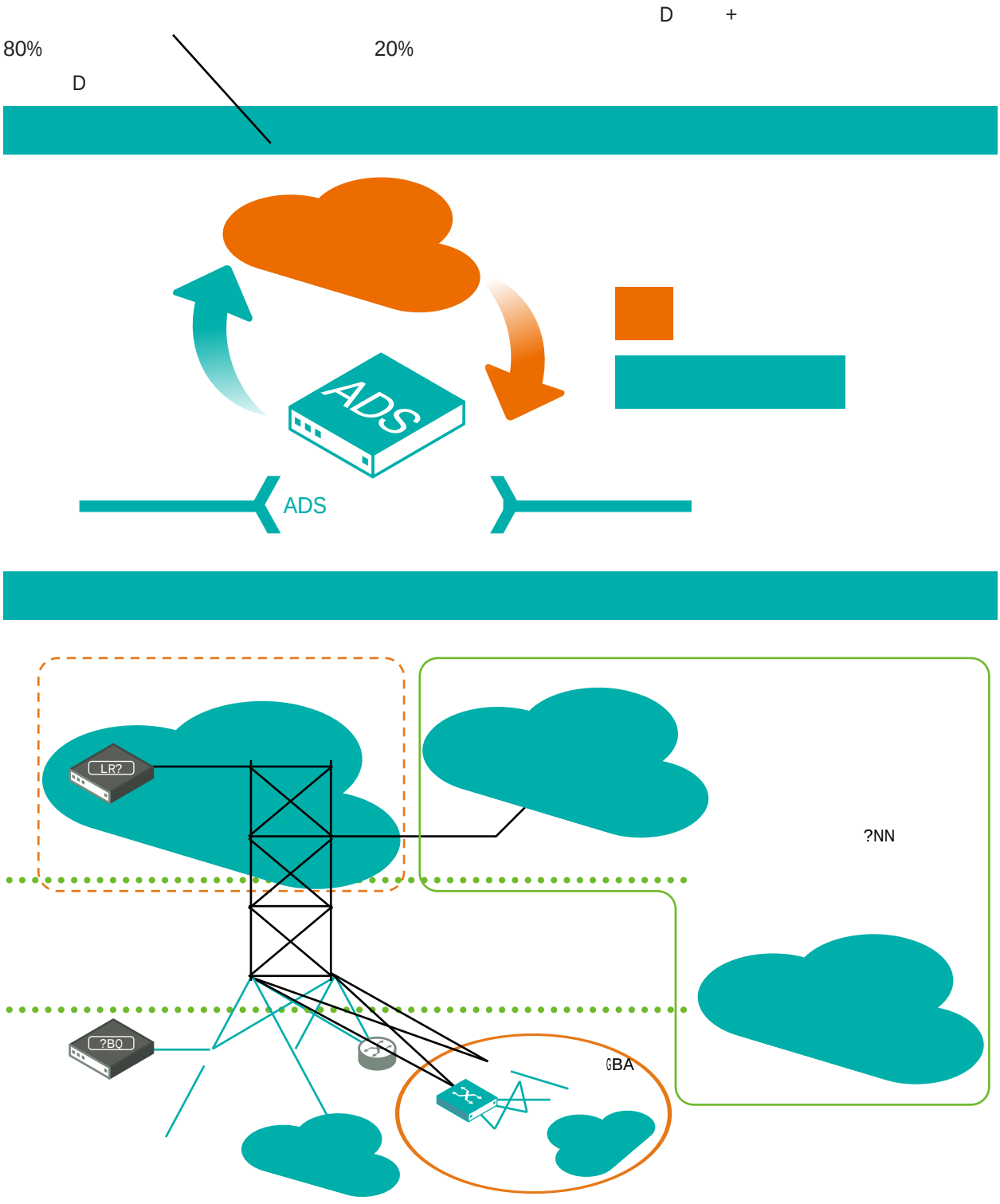
1.

2.

DDoS

3.

DDoS


D +
80%
20%
D
ADS
ADS
LR?
?NN
?BQ
GBA

D

1.
2.
3.
4. + D
5. 300Gbps DDoS

D

2016 DDoS Threat Report