2016 Q3 DDoS 态势报告

● 绿盟科技 DDoS 攻防研究实验室　NTI 绿盟威胁情报中心

多年来， 绿盟科技每天都在追踪全球 DDoS 攻击的风云变幻， 正如这浩瀚的宇宙，在无尽网络空间的深处，到底发生了什么？ Q3 DDoS 态势报告正从空间站发往地球……

更多链接…

目录

绿盟科技多年来持续追踪 DDoS 攻击态势，从监测的数据中，我们可以觉察一些规律。

在全球范围内看，近年来 DDoS 攻击多是 30 分钟以下的短时攻击，2016 年 3 季度短时攻击所占比重继续增长，达 56.6%; 攻击者仍旧很喜欢用混合式攻击，这类攻击占总攻击流量的 40.3%，以 NTP 反射和 UDP 混合最为常见；而反射类攻击相比传统的 botnet 攻击其攻击成本极低，且流量放大效果明显，我们监测到本季度有 90.5% 的攻击都采用了这种攻击形式。

但也有一些不寻常的情况出现……

40%

全球总 DDoS 攻击次数增加 40%

Q3 季度共检测到 71,416 次 DDoS 攻击，
比上个季度的 50,988 次增加 40%。

35 次

300G+ 超大流量 DDoS 攻击发生 35 次

Q3 季度 300Gbps 以上的超大流量攻击共发生 35 次，
相比 Q2 的 16 次增加 119%

19.4G

单次 DDoS 攻击平均峰值为 19.4G

Q3 季度平均攻击峰值为 19.4Gbps，比 Q2 的
16.7Gbps 有所上升。

572.6G

单次 DDoS 攻击最高峰值达 572.6G

Q3 季度单次攻击峰值最高达 572.6Gbps，相比 Q2 季度的 445.7Gbps 峰值有所上升，但仍然低于 Q1 季度的 615.1Gbps。

23 个

已独立发现 Mirai 僵尸网络主控端 23 个

其中最近更新的一个主控端是在 2016 年 10 月 13 日。最后一次查询结果显示，主控端主要分布在欧洲（荷兰、法国、波兰、乌克兰）、美国和日本。

440%

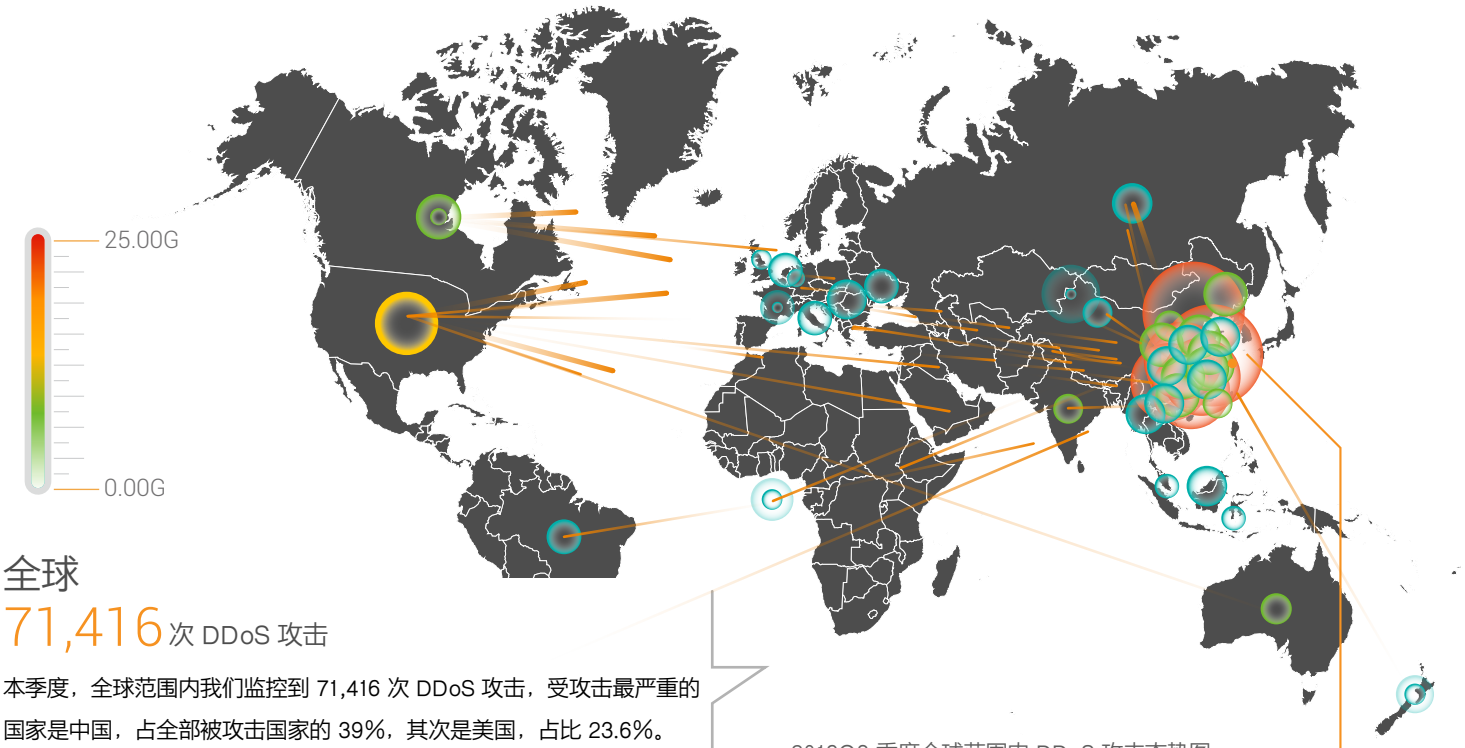
NTP Reflection 反射器数量增加 440%

Q3 季度全球范围内参与 DDoS 攻击的活跃反射器数量达 25,371 台，相比 Q2 数量增长了 440%。

150 万台

全球仅感染 Mirai 的物联网设备已经超过 150 万台

物联网设备成为黑客僵尸网络的新宠，截止到 10 月底仅感染 Mirai 的设备就已经达到 1,508,059 台，其僵尸网络在近期活动异常活跃，针对 23 端口的日扫描次数最高达 34 万次。



全球

71,416 次 DDoS 攻击

本季度，全球范围内我们监控到 71,416 次 DDoS 攻击，受攻击最严重的国家是中国，占全部被攻击国家的 39%，其次是美国，占比 23.6%。

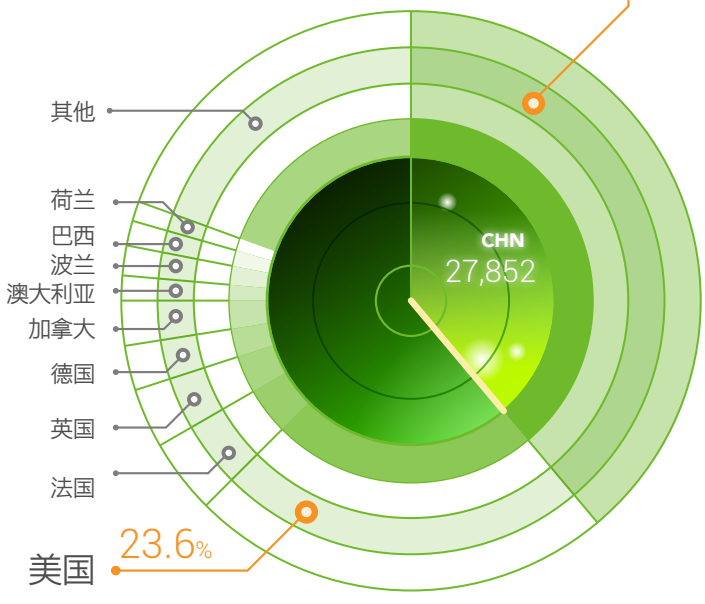
2016Q3 季度全球范围内 DDoS 攻击态势图

2016 Q3 季度中国范围内 DDoS 攻击态势图（局部）

中国

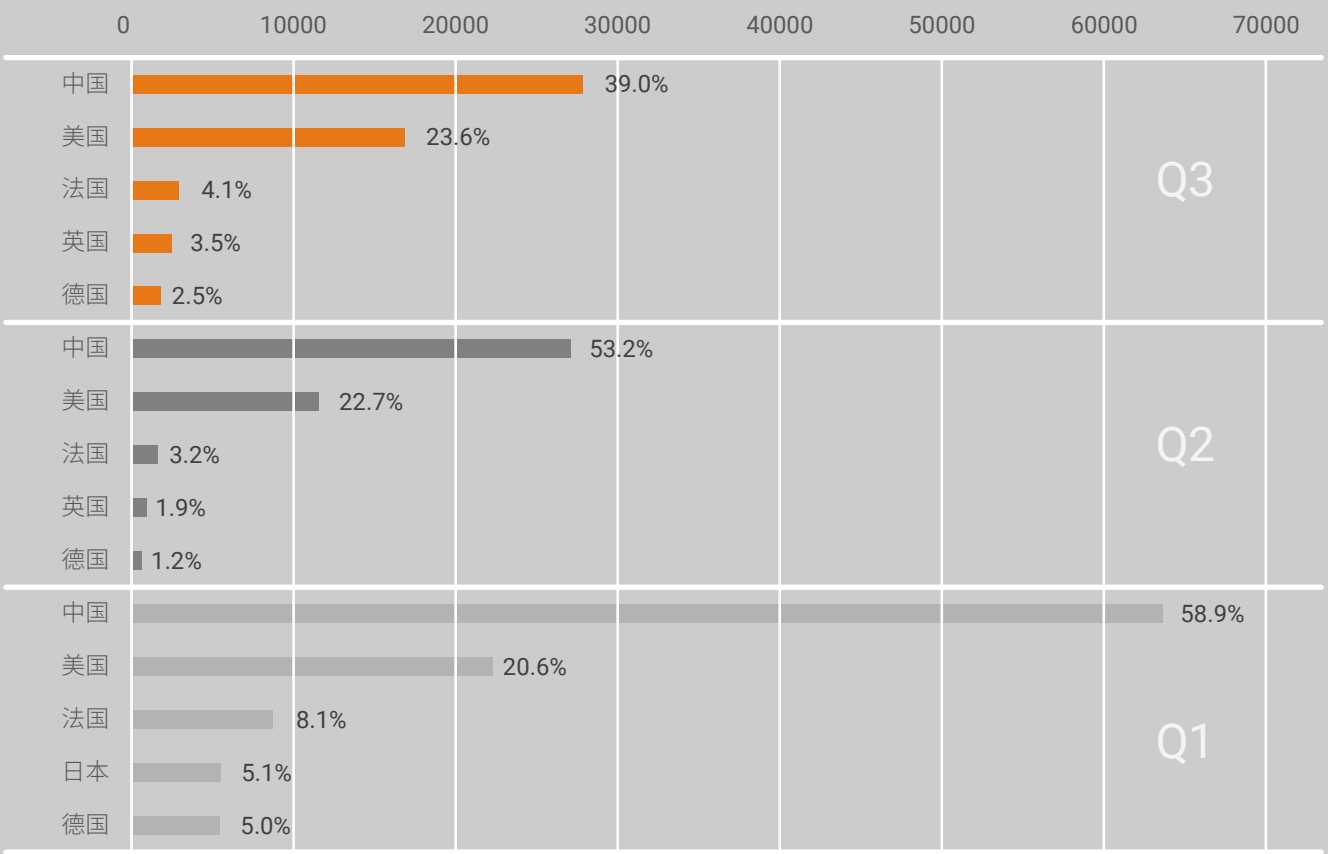
DDoS 被攻击次数占全球 **39%**

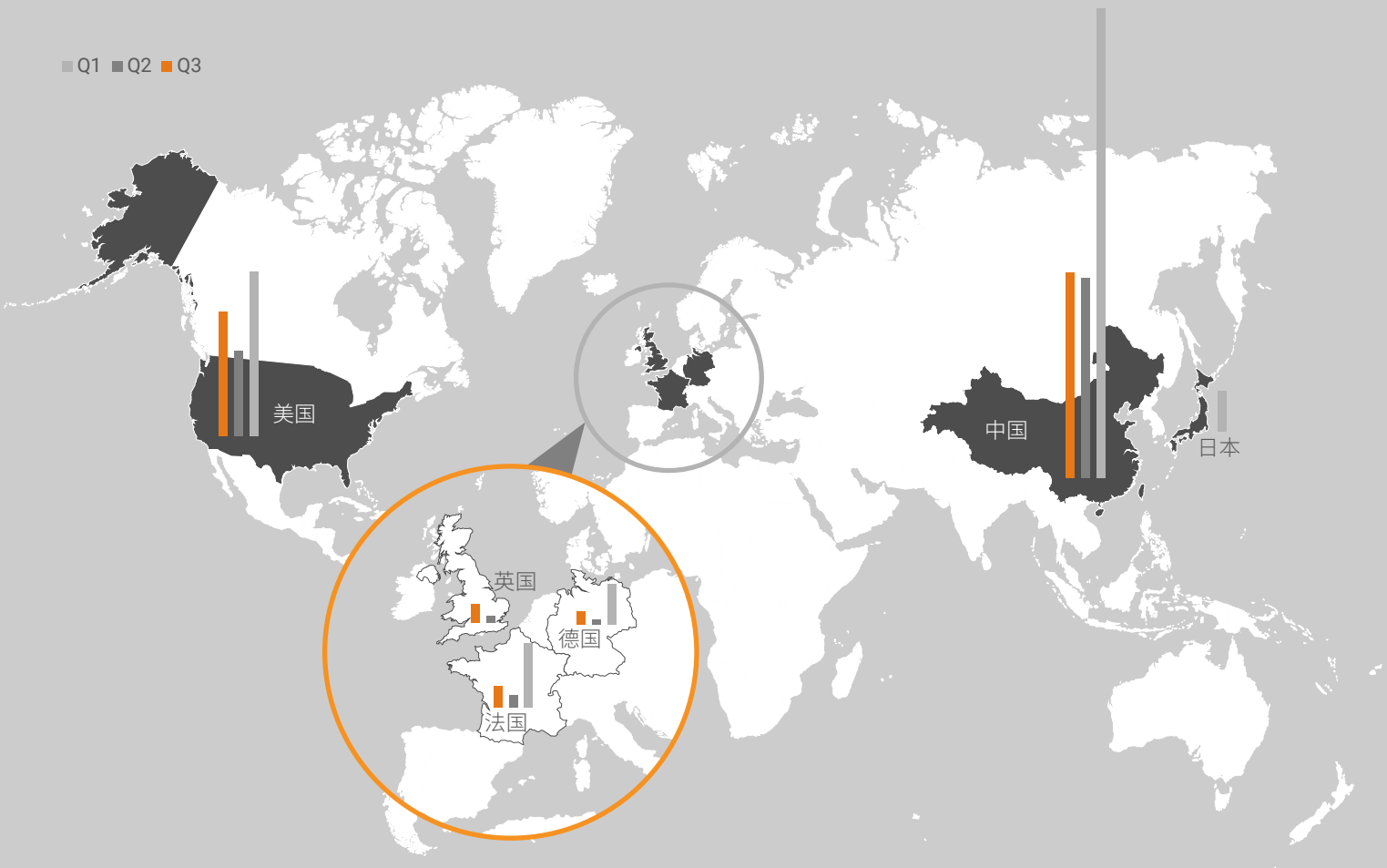
本季度中国共发生 27,852 次 DDoS 攻击，相比 Q1 和 Q2 季度，中国被攻击次数在全球各国家中所占比例有所下降，分别下降了 19.9%，14.2%。其中受攻击最严重的地区是浙江、广西、广东、北京、江苏等地区。



2016 Q3 季度全球被攻击国家 TOP10 按次数占比图

2016 Q1-Q3 季度全球被攻击国家 TOP5 按次数占比图



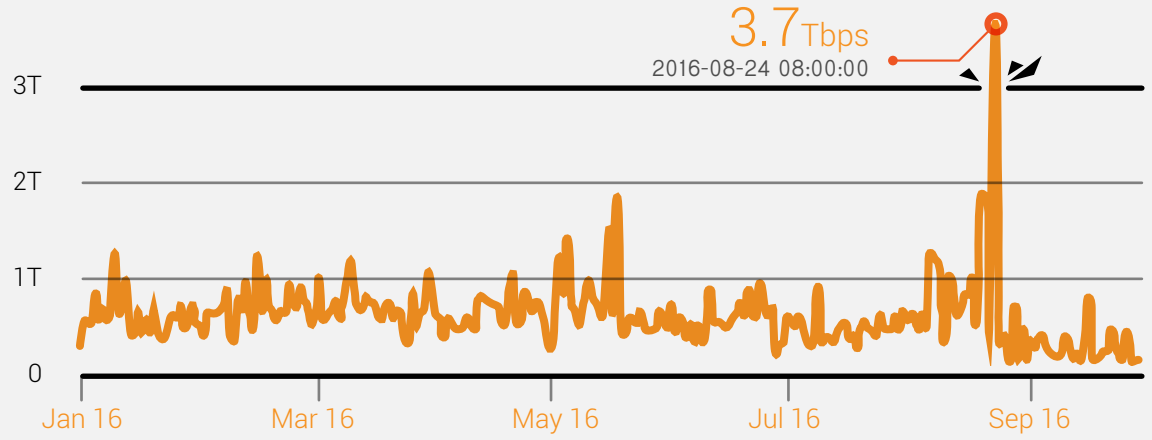


DDoS 攻击峰值

Q3 季度单次 DDoS 平均攻击峰值为 19.4Gbps，相比 Q2 的 16.7Gbps 上升 16.2%，比 Q1 的 28.2Gbps 减少 31.2%。

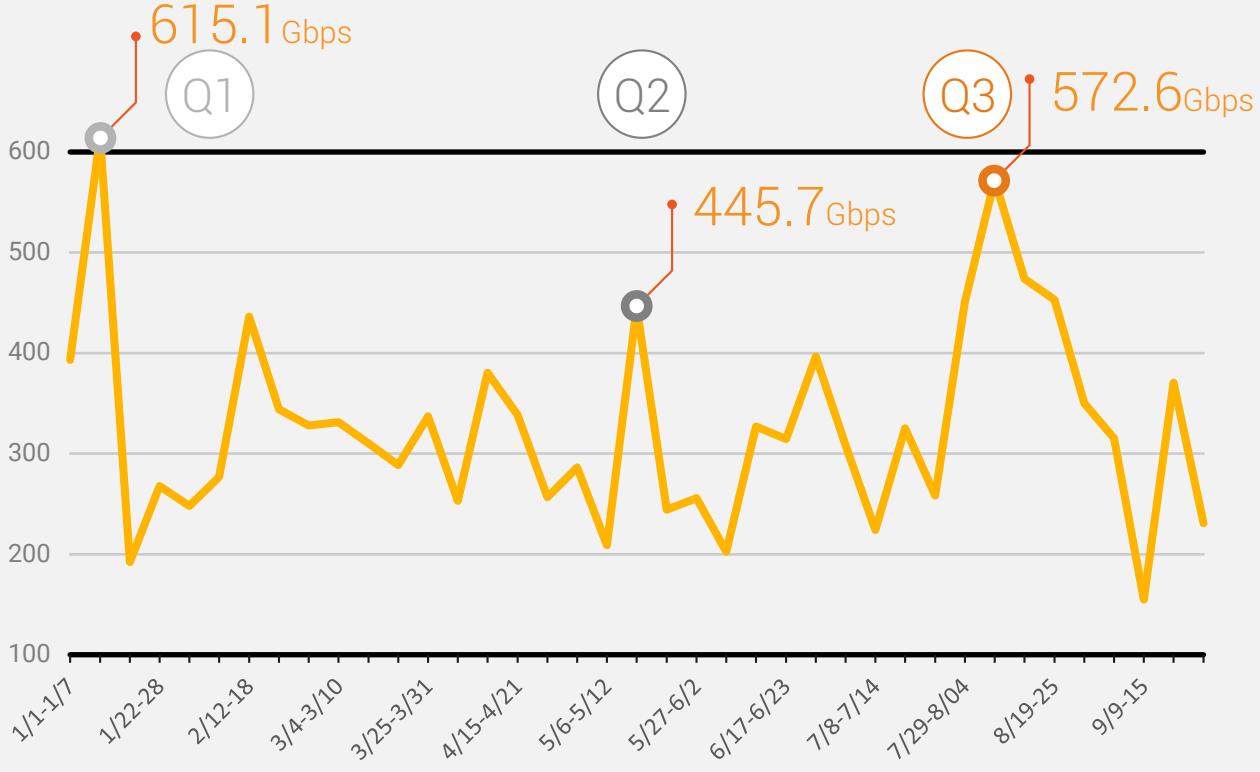
Q3 季度 DDoS 攻击累计流量的最高峰值为 3.7Tbps，比 Q2 季度的 1.8Tbps 增加 1.9Tbps，比 Q1 季度的 1.2Tbps 增长了 2.5Tbps。

2016 Q1-Q3 季度全球 DDoS 攻击累计总流量趋势图



本季度单次 DDoS 攻击最高峰值为 572.6Gbps，相比 Q2 季度的 445.7Gbps 峰值有所上升，但仍然低于 Q1 季度的 615.1Gbps。

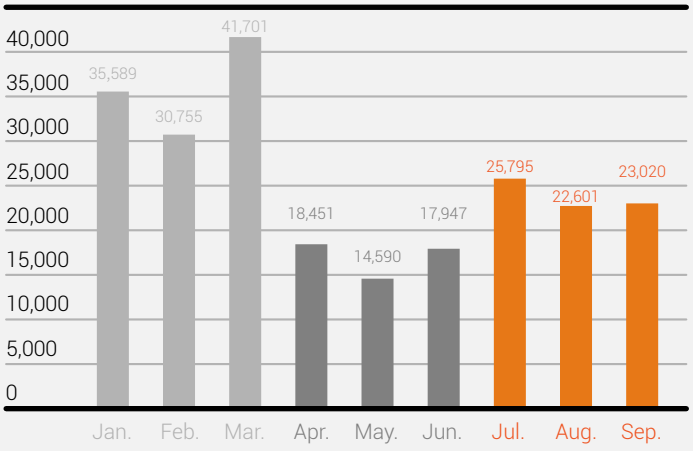
2016 Q1-Q3 季度单次 DDoS 攻击事件周峰值趋势图



我们对本季度攻击峰值较高的几个攻击事件进行溯源分析，发现除了几个是 NTP 和 SSDP 反射攻击外，其余的非反射攻击大都有网络摄像头、家庭路由器这些物联网设备的参与，且大部分流量的攻击特征符合 Mirai 的僵尸网络攻击特点。这也恰恰印证了我们在 10 月 14 日发布《2016 绿盟科技网络视频监控系统安全报告》中的观点，目前已经有大量物联网设备感染了如 Mirai、Luabot 等恶意僵尸网络程序，被用于扫描、DDoS 攻击等黑客活动。由于物联网设备普遍存在着各种安全问题，相比传统的 PC 机，黑客开始青睐于使用直接或者间接暴露于互联网上的物联网设备作为僵尸网络的被控肉鸡。可以预见，随着物联网技术的发展及各行业对其需求的不断扩大，成千上万的物联网设备正在以惊人的速度接入互联网，这一趋势将会更加明显。

DDoS 攻击次数

2016 Q1-Q3 季度各月份 DDoS 攻击次数图



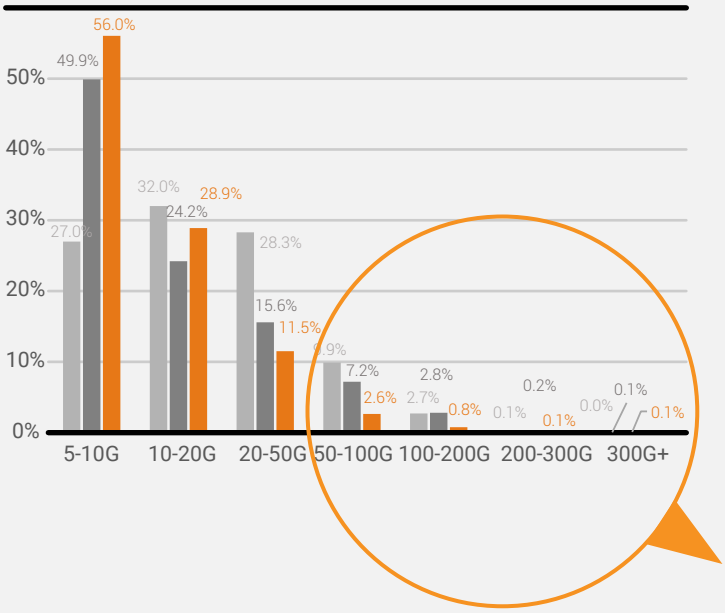
Q1 Q2 Q3

Q3 季度，我们监控到 DDoS 攻击 71,416 次，相比 Q2 季度的 50,988 次增加 40%，但仍然低于 Q1 季度的 108,045 次。

7 月份共发生 DDoS 攻击 25,795 次，比上个月增长了 43.7%。到 8 月份攻击有所下降，相比 7 月份减少 22.4%，9 月份发生攻击 23,020 次，与 8 月份持平。

攻击流量各区间分布情况

2016 Q1-Q3 季度攻击流量区间占比图



Q1 Q2 Q3

Q1 Q2 Q3

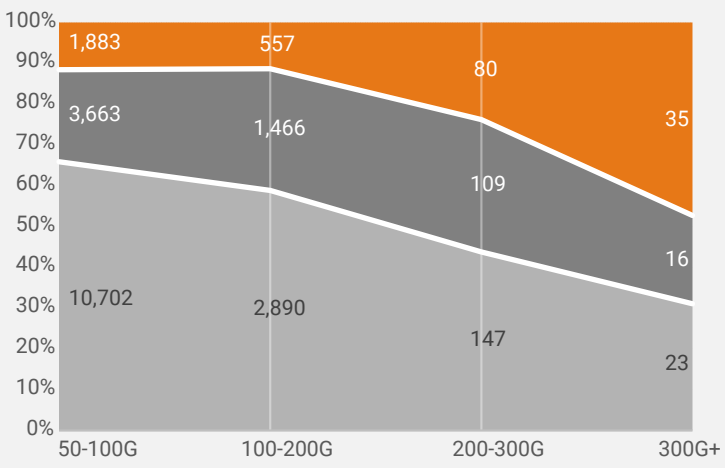
Q3 季度攻击峰值在 20Gbps 以下的小流量攻击相比 Q1、Q2 季度所占比例继续增加，其占比达整个 Q3 季度总攻击次数的 85%。

攻击峰值在 20-50G 的中型攻击占比 11.5%。峰值在 50-300Gbps 间的大流量攻击占比 3.5%，相比前两个季度的均明显下降。

大流量 DDoS 攻击趋势 Q3 季度峰值在 300Gbps 以上的超大型 DDoS 攻击共发生 35 次，相比前两个季度均有所增加。

峰值在 50Gbps 以上的大流量攻击共发生 2,555 次，相比 Q1 的 13,762 次，Q2 的 5,254 次，分别下降 81% 和 51%。

2016 Q1-Q3 季度大流量（峰值 >50Gbps）攻击次数图

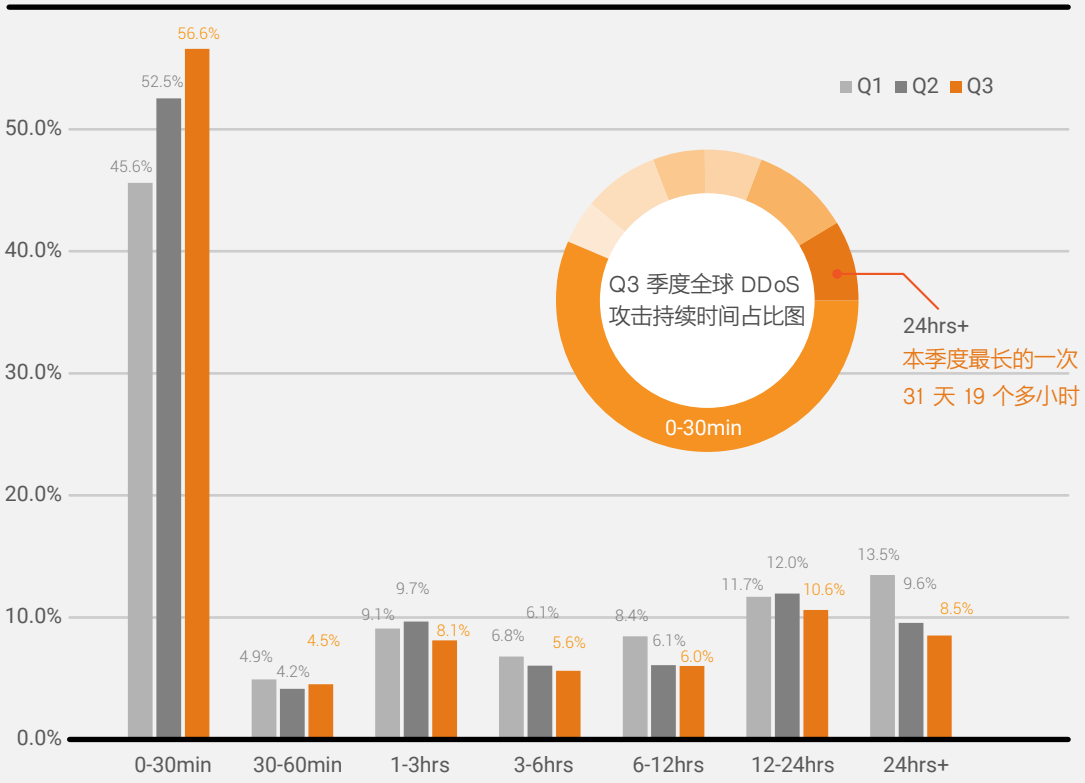


DDoS 攻击持续时间

本季度攻击时长在 30 分钟以下的攻击占总数的 56.6%，相比前两个季度继续上升。平均攻击时长为 7.2 小时，相比 Q2 季度的 8.1 小时略有下降 。攻击时长超过 1 天的攻击占总攻击次数的 8.5%，相比前两个季度继续下降。

我们监控到 Q3 最长的一次 DDoS 攻击持续了 31 天 19 个多小时（764 小时），累计总攻击流量达 17 TBytes。

2016 Q1-Q3 季度全球 DDoS 攻击持续时间占比图

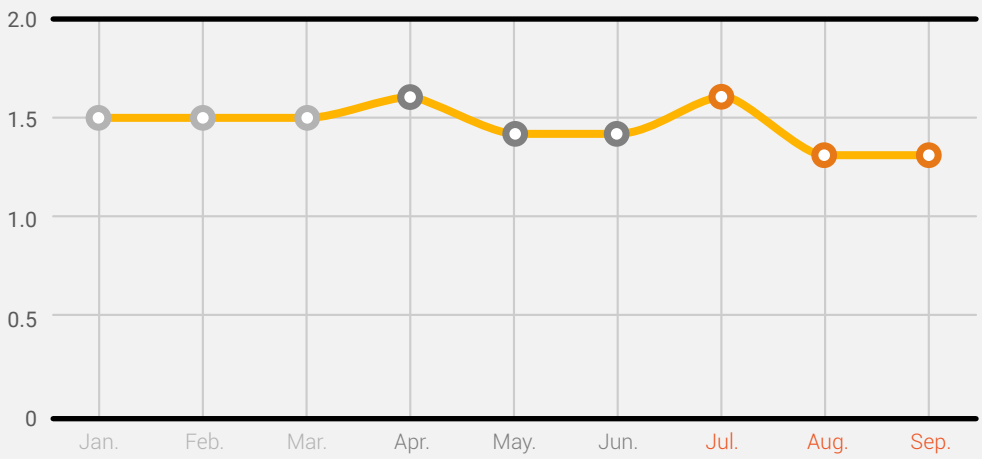


DDoS 重复攻击频次

Q3 季度单个 IP 平均被攻击次数与前两个季度相比略有下降，大概单个 IP 每个月平均被攻击 1.4 次，Q1 和 Q2 均是 1.5 次 / 月。

我们监控到某网络在 Q3 季度内被重复攻击达 30 次，攻击手段多是短时的 UDP Flood 和 NTP Reflection Flood 混合攻击。

2016 Q1-Q3 季度各月份单个 IP 平均被攻击频次

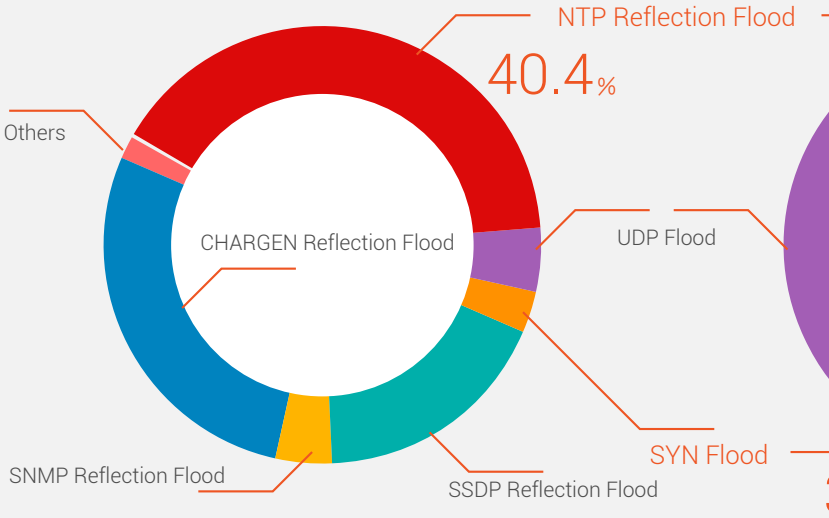


各攻击类型次数和流量占比

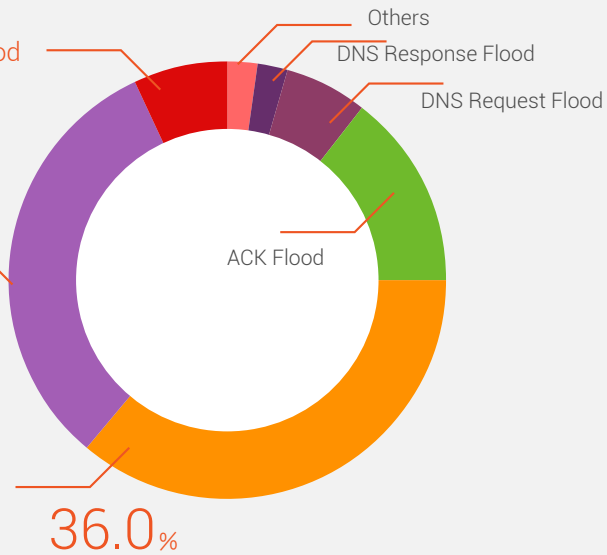
从攻击次数上看，Q3 反射攻击在总攻击次数上的占比达 90.5%，相比 Q2 季度增长了 20.6%。其中，NTP 反射攻击次数最多，占 40.4%，其次是 Chargen、SSDP、SNMP 反射攻击。

反射攻击的原理是攻击者伪造请求，将受害者 IP 地址作为请求源地址并将之发往互联网中大量存在协议漏洞的反射器，利用这些协议回应包字节数远大于请求包的特点，达到反射放大流量的效果，构成对目标网络的大流量 DDoS 攻击。由于不需要像传统僵尸网络那样对大量的攻击源进行事先感染和控制，因此发起此类大流量攻击的代价远远小于传统的 DDoS 攻击。目前已知流量放大倍数最高的反射攻击是 NTP 反射攻击，最大可放大至 556.9 倍。

2016 Q3 季度按攻击总次数统计类型占比图



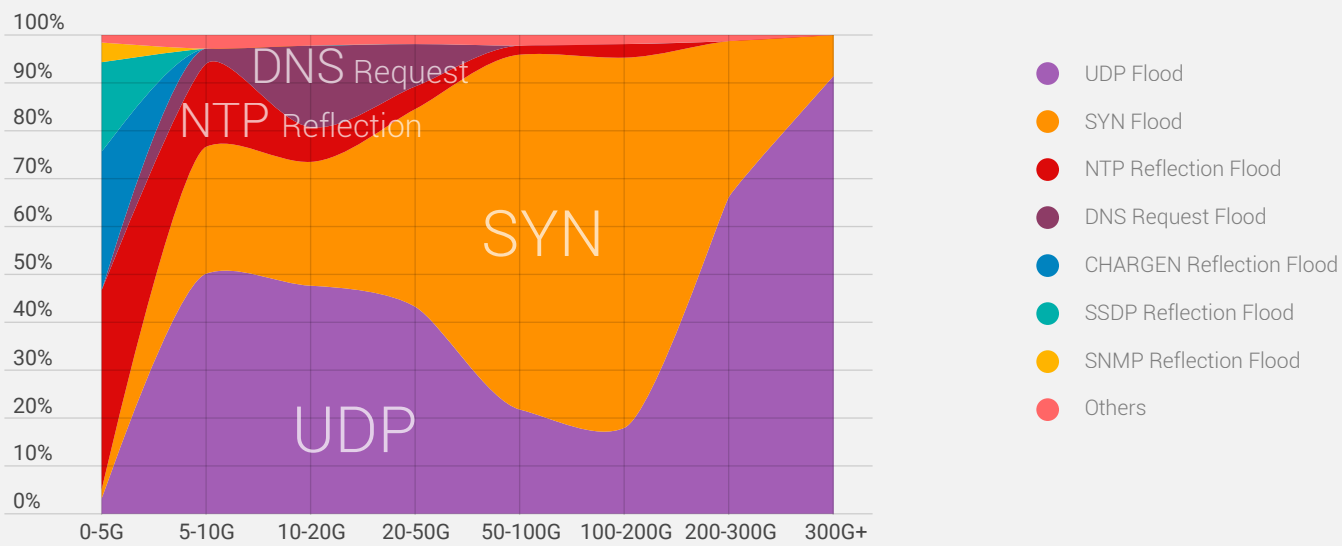
2016 Q3 季度按攻击总流量统计类型占比图



攻击类型各流量区间占比

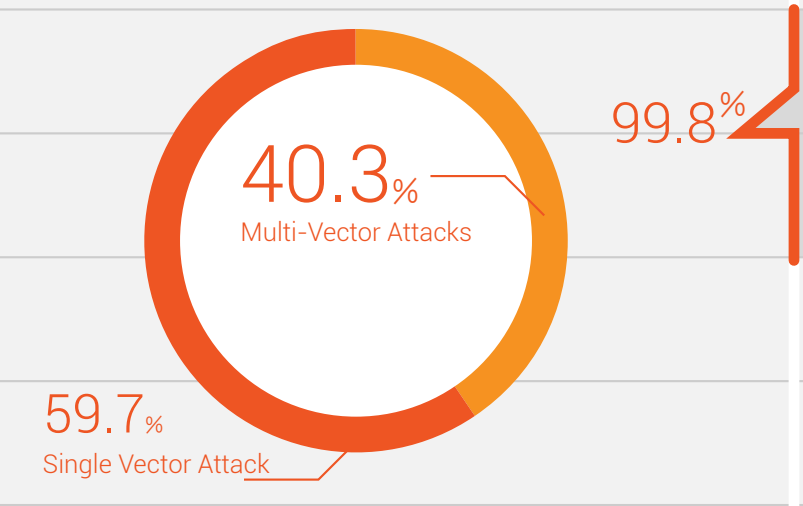
经分析，在不同的攻击峰值流量区间内，攻击协议类型表现出不同的分布特征。在 5G 以下的小流量攻击中 NTP Reflection Flood、CHARGEN Reflection Flood 等反射类攻击较多，峰值在 50-200G 的大型流量中以 SYN Flood 为主，峰值在 5-50G 中小型流量和 200G 以上的大型、超大型流量中以 UDP Flood 为主，SYN Flood 为辅。这表明，不同的攻击工具，或不同类型的僵尸网络，或不同攻击组织的攻击手段和攻击能力也不尽相同。

2016 Q3 季度按攻击类型各流量区间占比图



Q3 季度利用多种流量混合发起的攻击占全部攻击流量的 40.3%，相比 Q2 季度的 33.7% 继续增加，占比增长了 6.6%。

2016 Q3 季度混合与非混合攻击手段占比图



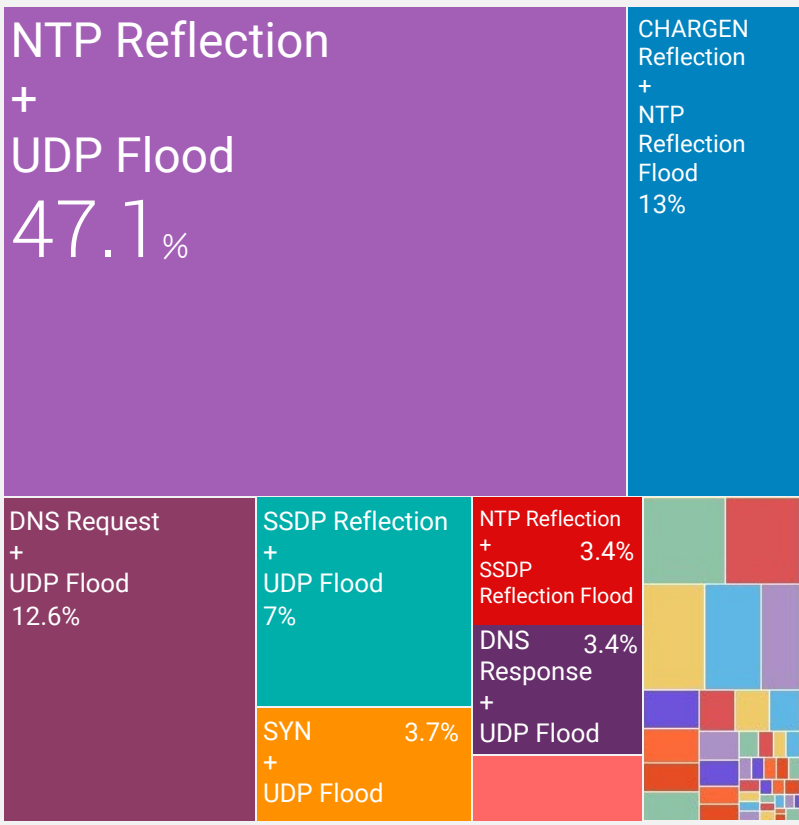
我们对使用混合攻击手段发起的攻击进行分析，统计其使用的种类数占比情况，如下图所示，发现混合攻击中 2 至 3 种攻击类型的混合较为常见，占总体分布的 99.8%。

混合 DDoS 攻击种类数占比图

47.1% 的攻击者常使用组合攻击形式
NTP Reflection Flood + UDP Flood

本季度最常见攻击混合类型为 NTP Reflection Flood 和 UDP Flood 攻击混合，占全部混合类型的 47.1%。使用反射攻击流量混合的攻击仍然占较大比例，如 CHARGEN Reflection 和 NTP Reflection Flood 混合，SSDP Reflection 和 UDP Flood 混合，NTP Reflection 和 SSDP Reflection 混合等。

混合攻击按混合类型发生次数统计分布图



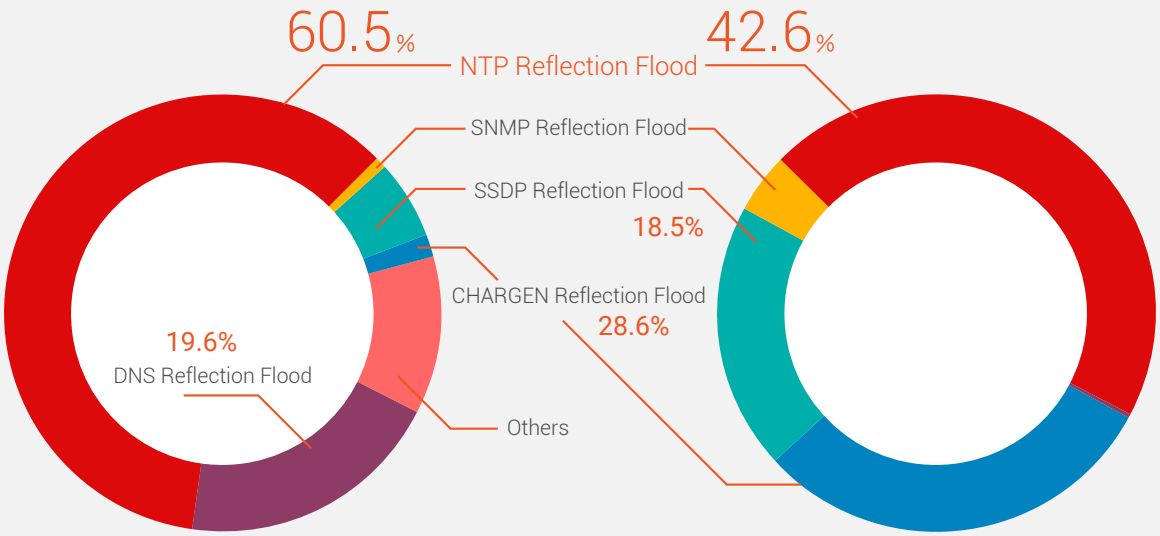
各类反射攻击占比

Q3 季度反射类型攻击仍然比较活跃，相比 Q2 季度大幅度增加，我们对本季度各类反射攻击的次数和流量占比情况分别进行了统计。

从攻击流量上来看，NTP Reflection Flood 攻击流量占比最多，为 60.5%，其占比比 Q2 季度增长了 24.4%。其次是 DNS 和 SSDP Reflection Flood 攻击，攻击流量占比分别为 19.6%， 5.9%，相比上一季度均有所下降。

从攻击次数上看，NTP Reflection Flood 在本季度超过 CHARGEN Reflection Flood 成为最活跃的反射攻击，其占比为 42.6%，比上一季度占比增加 13.6%。CHARGEN 和 SSDP Reflection Flood 占比都略有下降。

2016 Q3 季度各类反射攻击流量占比图



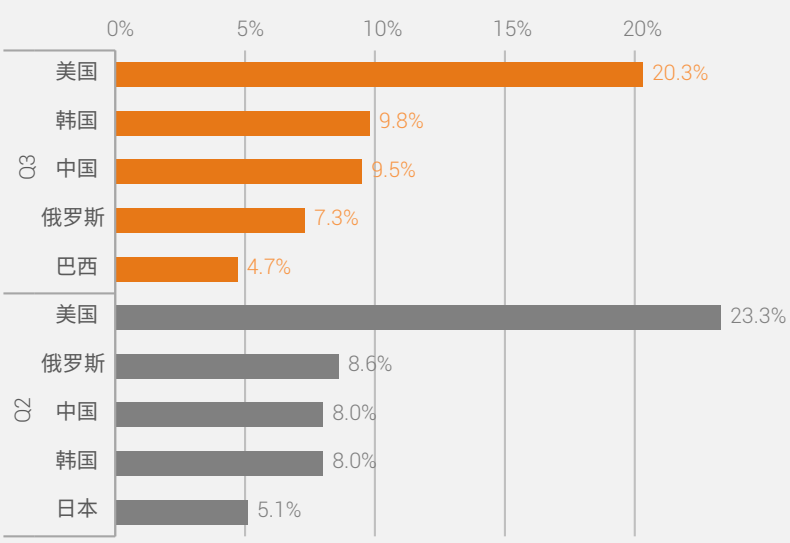
2016 Q3 季度各类反射攻击次数占比图

活跃 NTP 反射器全球分布

据我们最新统计，本季度被利用来发起 NTP Reflection Flood 攻击的反射器共 25,371 个，相比 Q2 季度数量增长了 440%。其全球分布情况如下图所示。其中，中国占比最多，其次是美国、越南、韩国和俄罗斯。相比 Q2 季度，越南和韩国两个国家的占比增多，超过了俄罗斯、日本和法国跻身 TOP5 国家行列。

2016 Q3 季度被利用发起攻击的 NTP 反射器全球分布情况图

2016 Q3 季度各类反射攻击次数占比图



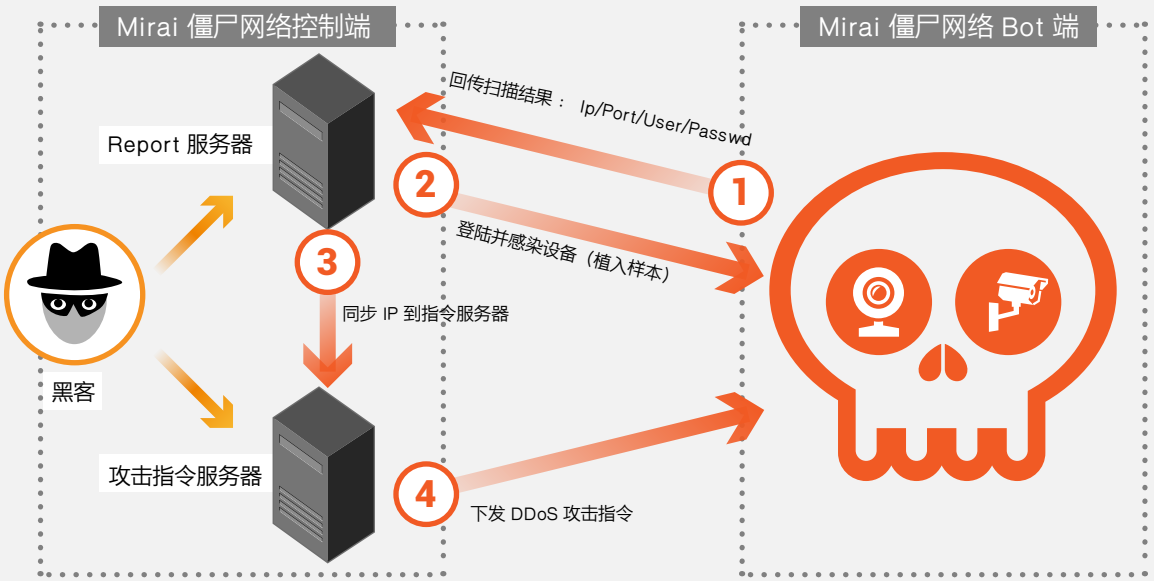
08 DDoS 攻击趋势： 基于物联网设备的僵尸网络

基于物联网设备的僵尸网络已经改变了全球DDoS攻击的趋势，它已经成为黑客DDoS工具的新宠，其拥有的潜在破坏能力已经不容小觑。下面我们将对物联网的僵尸网络情况，特别是Mirai的近况进行详细分析。

IoT 僵尸网络工作原理

我们以当前最活跃的 Mirai 僵尸网络为例，对僵尸网络主控端与 Bot 端的通信过程进行说明。不同的僵尸网络的主控端一般对应 2 类服务器，一类是用于向 Bot 客户端下发 DDoS 指令、扫描指令的，叫做指令服务器； 一个是用于接收各 Bot 端扫描结果并向上报的目标植入恶意程序的，叫 Report 服务器（一般也用于恶意样本存储）。两类服务器与 Bot 端的通信使用不同的端口。Mirai 僵尸网络各控制端和 Bot 端具体通信过程如下图所示。

Mirai 僵尸网络主控端和 Bot 端通信过程



Mirai 僵尸网络主控端分布情况

截止到 10 月底，我们独立监控到的基于 Mirai 的僵尸网络主控端有 23 个，如下表所示。包含指令服务器、Report 服务器及其使用的通信端口号，注册时间和更新时间。

Mirai 僵尸网络主控端列表

攻击指令服务器-地址	攻击指令服务器-端口	Report服务器-地址	Report服务器-端口	注册时间	更新时间
gay. .racing	23	repor ed.racing	48101	2016年5月28日	
fuckl rt.com	23	lu rt.com	48101	2016年7月26日	
laatr h.cf	23	rep joh.cf	48101	2015年11月16日	
im o.work	1367	your to.work	48202	2016年10月16日	
lol.d ed.racing	23	dong ed.racing	48101	2016年5月28日	
swi me.ru	23	new me.ru	48101	2016年8月22日	
swi me.ru	23	sv me.ru	48101	2016年8月22日	
tw. n.com	23	tw n.com	48101	2014年11月18日	2016年6月13日
fuck1.b k.com	23	fuck ook.com	53	2016年2月9日	2016年10月13日
network.santash ane.cx	23	report.santa cane.cx	48101	2016年9月15日	
hei to.work	23	she to.work	48202	2016年10月16日	
high e.club	666	report me.club	48101	2016年10月24日	
ftp.x er.xyz	23	listen.x ter.xyz	48101		
sdrf yy.top	23	sdrf syy.top	48101	2016年10月27日	
cnc.c ed.racing	23	report ed.racing	48101	2016年5月28日	
kankerc st.xyz	23	report. st.xyz	48101		
secur es.us	23	rep.s tes.us	4810	2016年9月4日	
load re.pw	23	r. ure.pw	37065		
6d77a s.net	2047	e98 tes.net	20470	1999年4月22日	2016年5月26日
q5f2k0 4g.ru	23	xg5kisn74mk 4g.ru	48101	2016年10月28日	
n rk.org	23	repo xrk.org	48101	2016年3月25日	
www.m m.org	23	www. am.org	4810	2016年9月20日	
ou an.ru	23	rep lan.ru	48101	2016年8月19日	

08 DDoS 攻击趋势： 基于物联网设备的僵尸网络

从这些服务器地址的注册时间或者更新时间来看，大部分都是在今年的 5 月份以后，尤其 7 月底至 10 月底最多，这段时间也恰巧是 Mirai 僵尸网络最活跃的时间。列表中的 santasbigcandycane.cx 是已泄露的 Mirai 源码中提到的主控端。

我们对这些僵尸网络进行了密切的监控，截止到本报告截稿时，表格中有部分控制端已经无法连上，但大部分依然比较活跃。推测由于近期 Mirai 的大流量 DDoS 攻击频现，各相关组织已经开始对其进行治理。

下图是我们监控到 q5f2k0exxxx.ru 这个僵尸网络的攻击指令，可以看到，其针对同一个目标在短时间段内分别发起了三次 DDoS 攻击，而且攻击手段在不断变化，分别是 GRE IP Flood、ACK stomp Flood、HTTP Flood 攻击，很可能攻击者是在试探目标网络的带宽承受及防御能力。

```
2016-11-03 17:04:10
duration:       600
attack ID:      6  [GRE IP flood]
target count:   1
targets:        5.      .120/32
opts count:     2
opts[0].key:    7   data length:    2
opts[1].key:    25  data length:    15

2016-11-03 17:14:11
duration:       30
attack ID:      5  [ACK stomp flood]
target count:   1
targets:        5.      120/32
opts count:     1
opts[0].key:    7   data length:    2

2016-11-03 17:15:11
duration:       30
attack ID:      10 [HTTP flood]
target count:   2
targets:        104.      .30/32 | 104.25.182.30/32
opts count:     3
opts[0].key:    7   data length:    2
opts[1].key:    8   data length:    12
opts[2].key:    24  data length:    4

2016-11-03 17:16:04
duration:       30
attack ID:      10 [HTTP flood]
target count:   1
targets:        5.      120/32
opts count:     3
opts[0].key:    7   data length:    2
opts[1].key:    8   data length:    12
opts[2].key:    24  data length:    4
```

Mirai 僵尸网络某主控端 DDoS 攻击指令

另外，这些主控端为了躲避检查，经常变换 IP，根据其最后一次使用的 IP 进行查询，其主控端主要分布在欧洲（荷兰、法国、波兰、乌克兰），美国和日本。

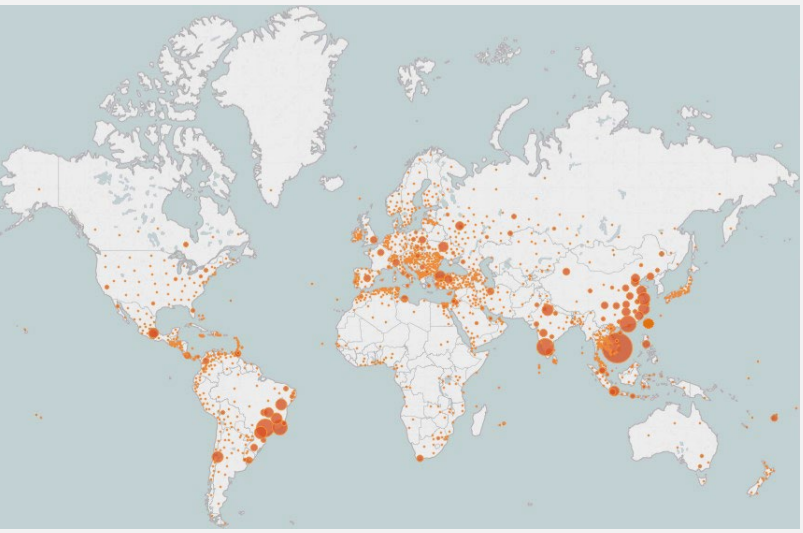
Mirai 僵尸网络 Bot 端分布

截止到 10 月底，我们统计到全球范围内仅感染 Mirai 的物联网设备的数量就已经达到 1,508,059 个，遍布全球的 209 个国家或地区。

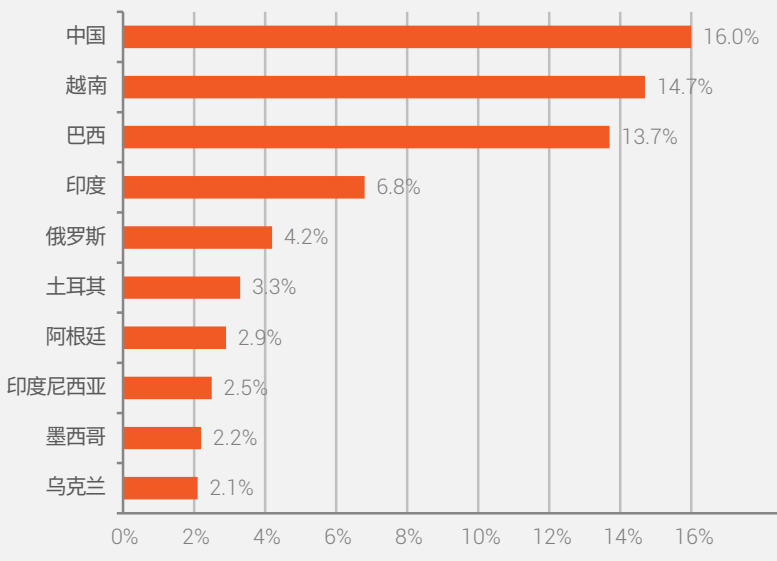
Mirai 僵尸网络 Bot 端全球分布情况如下图

Mirai Bot 端全球分布数量占比 Top 10 国家如下图所示，其中前 3 名是中国、越南、巴西，分别占全球总数的 16%、14.7% 和 13.7%。剩余国家分别是印度、俄罗斯、土耳其、阿根廷、印度尼西亚、墨西哥和乌克兰。这 10 个国家就占据了全球总数量的 68.4%。

Mirai 僵尸网络 Bot 端全球分布图



Mirai 僵尸网络 Bot 端全球分布国家 TOP10 占比



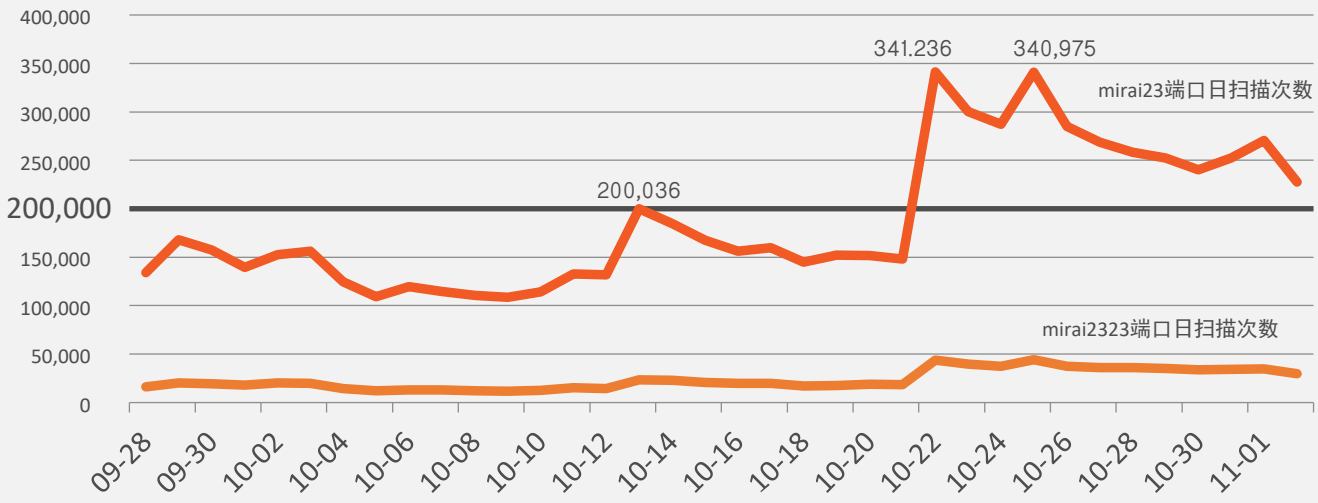
Mirai 全球扫描活动

2016 年 9 月底，Mirai 的作者公开了其源代码。经分析，Mirai 僵尸网络使用某固定特征对 23 和 2323 端口进行扫描，用于发现网络中新的感染目标。因此我们对其全球扫描的情况进行了监控。

下图是截取了近一个月内其每日扫描 23 和 2323 端口次数的情况（EST 时间）。10 月 21 日之前针对 23 端口的扫描大概在 15 万次 / 日左右，针对 2323 端口的扫描大概在 2 万次 / 日左右。到 10 月 22 日，针对 23 端口的扫描开始大幅度增加，最高达 34 万次 / 日，后面几天略有震荡，总体趋势在缓慢下降； 针对 2323 端口的扫描相比此前翻了一倍左右。推测 10 月 22 日扫描的骤增可能与 Dyn 将 21 日导致美国大范围断网的矛头指向 Mirai 有关，这次着实让 Mirai 又火了一把，因此更多的黑客开始利用 Mirai 建造自己的僵尸网络。

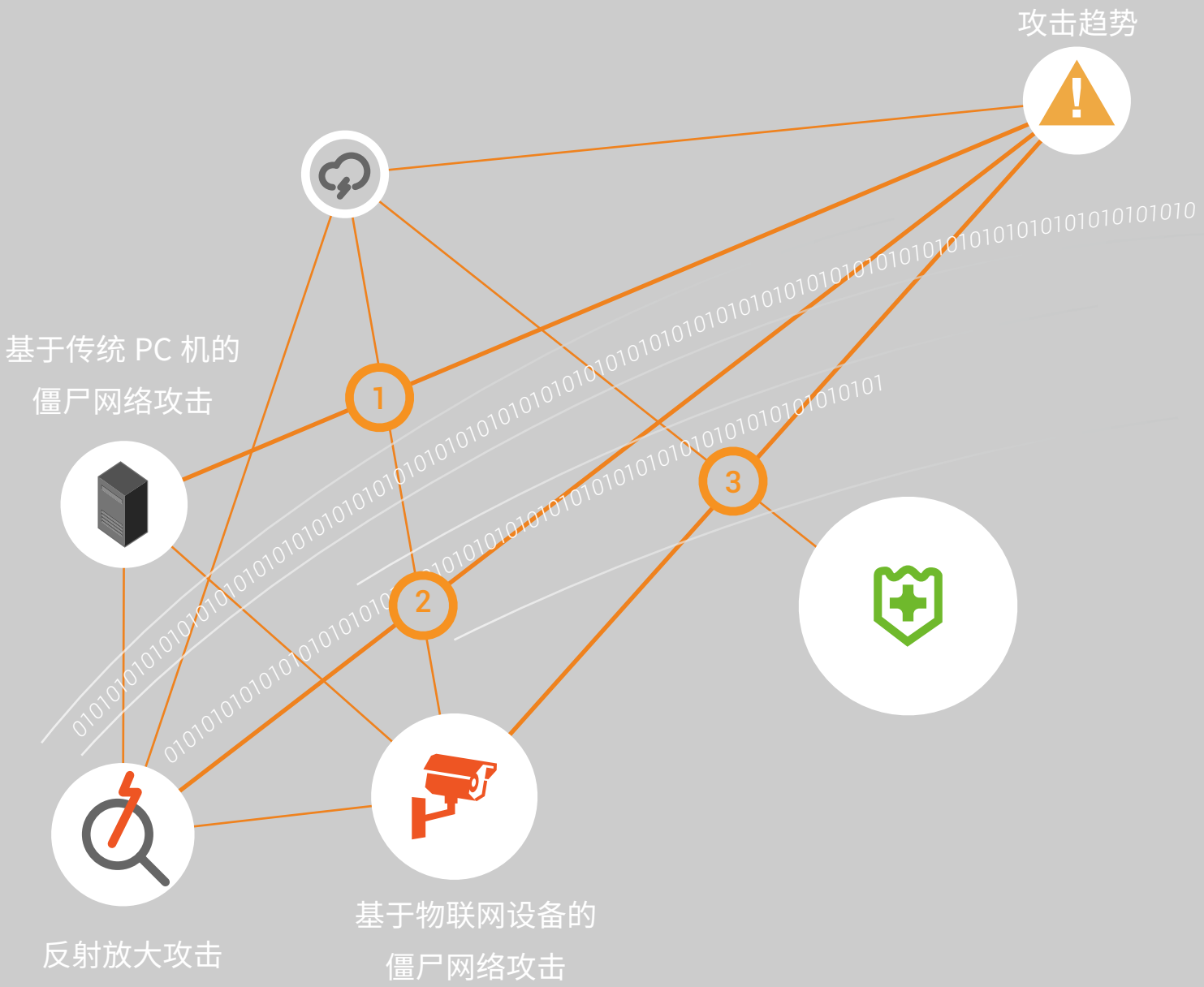
尽管后面其趋势略有降低，但始终都高于 10 月 22 日之前的日扫描次数。可看出，Mirai 僵尸网络在近一月内仍然比较活跃。可以预见到，随着全球大量物联网设备不断地接入互联网，感染 Mirai 或其变种的设备数量会继续飞速增长。

Mirai 僵尸网络 23 和 2323 端口日扫描次数图



正如之前的《2016 绿盟科技网络视频监控系统安全报告》中，我们所提到的，物联网的安全现状如不加以控制和改变，基于物联网的僵尸网络就会以惊人的速度扩张，届时将给全球的网络安全防护带来极大的挑战。

随着物联网的崛起及其现阶段暴露的各种安全问题， 全球 DDoS 攻击趋势正在发生巨大变化。从最初的基于传统 PC 机的僵尸网络攻击，到近两年兴起的反射放大攻击，到现在开始逐步转向基于各类物联网设备的僵尸网络攻击，这一变化过程反应了攻击者在利益的驱使下不断试图寻找低成本，高效率的攻击工具及攻击方式。我们也将持续追踪这些变化， 并及时发布预警和提供行之有效的防御机制，促进互联网生态环境健康、有序的发展，这也正是我们在一直不懈努力追求的目标。



特别声明

为避免客户数据泄露，所有数据在进行分析前都已经匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

相关链接

NSFOCUS 2016 Q1 DDoS 态势报告

NSFOCUS 2015 年度 DDoS 态势报告

NSFOCUS 2016 Q2 DDoS 态势报告

2016 绿盟科技网络视频监控系统安全报告

了解更多

绿盟科技威胁响应中心和 DDoS 攻防研究实验室持续关注 DDoS 攻击事件的进展，如果您需要了解更多信息，请访问：

- 绿盟科技官网 - 研究报告
- 绿盟科技博客 - 安全报告
- 绿盟科技威胁响应中心微博
- 绿盟科技微信公众号（扫描右边二维码）

绿盟科技官方微信

数据来源： 绿盟科技 DDoS 攻防研究实验室 NTI 绿盟威胁情报中心

NSFOCUS