NSFOCUS

2016Q2 DDoS 态势报告

据绿盟科技全球DDoS态势感知平台监控数据分析显示，Q2发生DDoS攻击事件有所下降，平均攻击峰值也有所降低，但攻击手段呈现复杂化，因此总体攻击态势依然严峻。

[点击下列标题跳转到对应章节↓↓↓]

更多链接…

全球攻击态势 50,988次 DDoS攻击

绿盟科技监控数据显示，Q2季度全球发生DDoS攻击达50,988次。

攻击流量趋势 单次攻击峰值 445.7G

Q2单一时间点攻击流量峰值1.8T，
单次攻击峰值445.7G，300G以上的攻击16次。

攻击时间趋势 单次攻击 387小时71TB

Q2平均攻击时长1.6小时，
单次攻击最长387小时，其总流量达71TB。

攻击类型趋势 62.1% 的反射攻击

从攻击次数占比看，Chargen 反射攻击占27.6%，
从攻击流量大小占比看，SYN为54.7%。

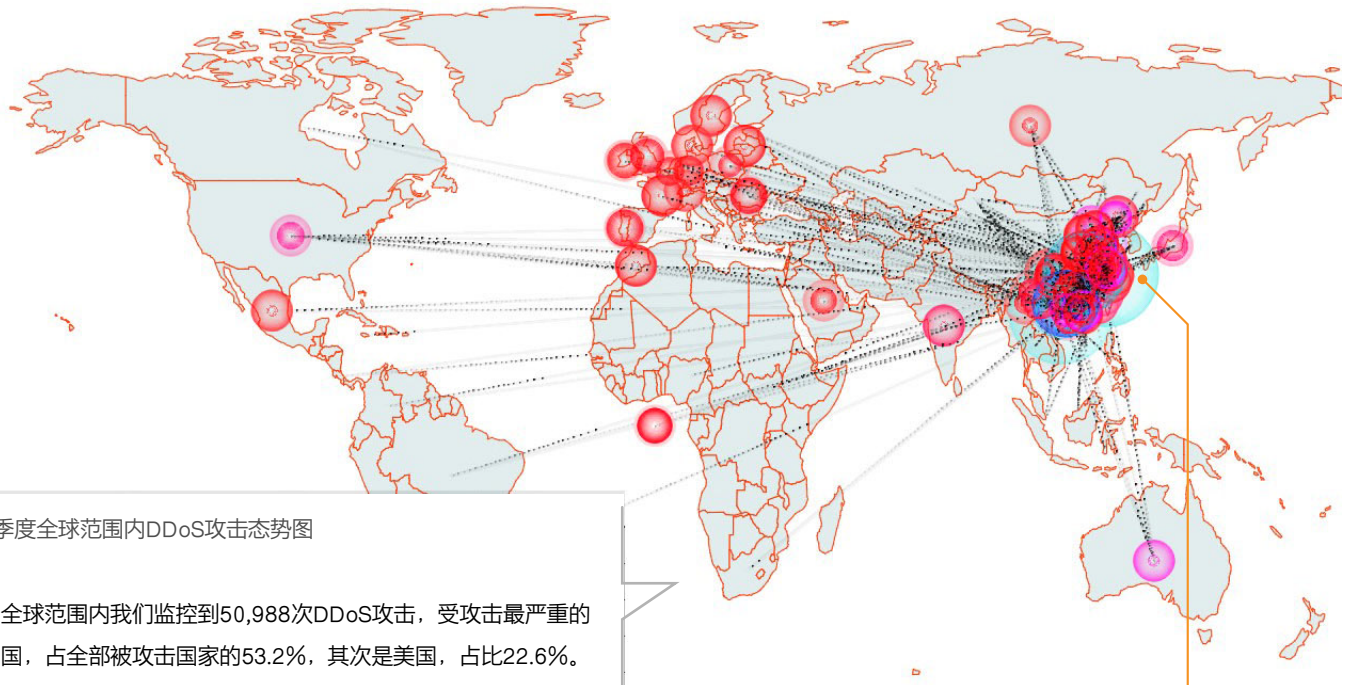
混合攻击趋势 33.7% 的混合攻击

从攻击流量大小占比看，混合攻击占总比的33.7%，
其中2-3种混合攻击占97.4%。

反射攻击趋势 365万 NTP反射器

从攻击次数占比看，Chargen反射攻击占所有反射类型的38.1%，从攻击流量大小占比看，NTP反射攻击占所有反射类型的36.1%。

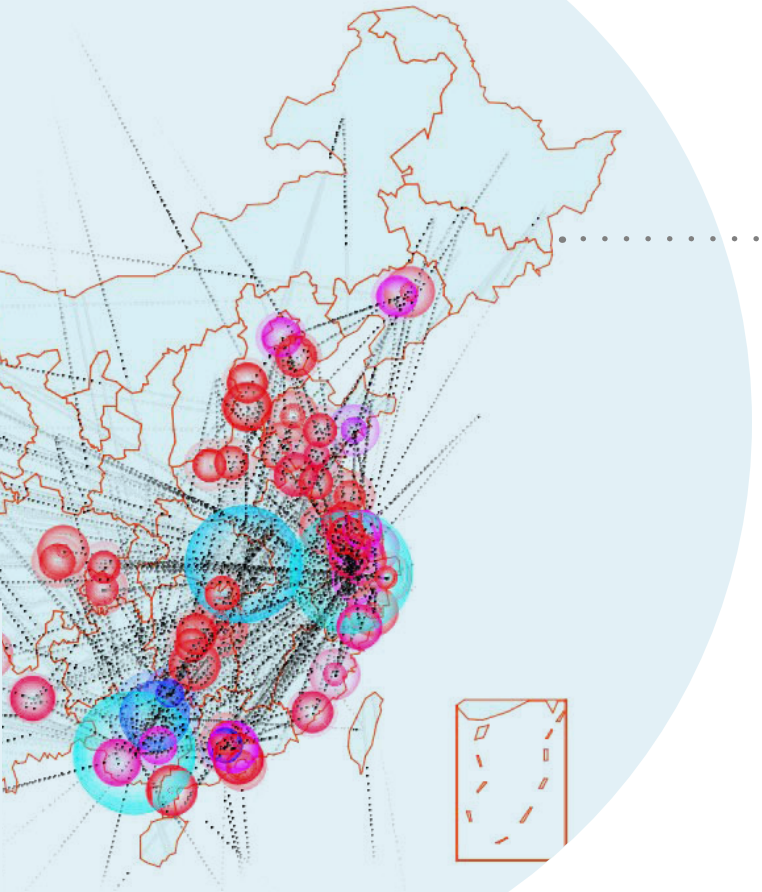
绿盟科技监控数据显示，Q2全球被DDoS攻击次数达到50,988次。



2016Q2季度全球范围内DDoS攻击态势图

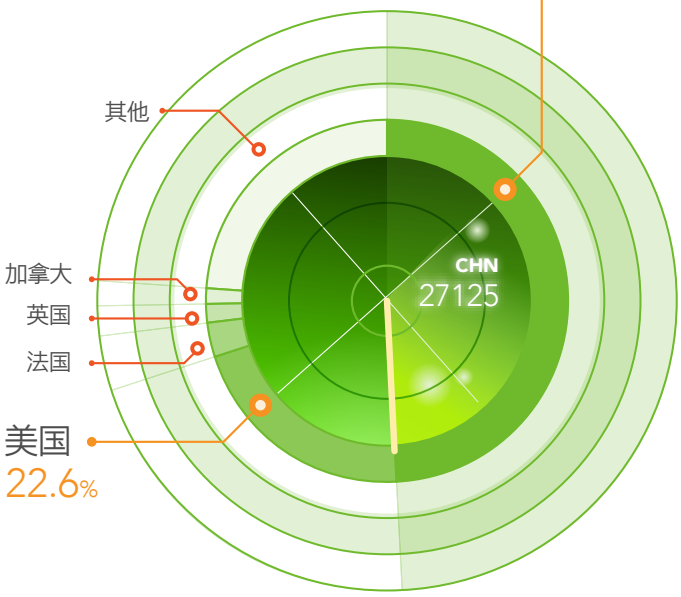
本季度，全球范围内我们监控到50,988次DDoS攻击，受攻击最严重的国家是中国，占全部被攻击国家的53.2%，其次是美国，占比22.6%。

中国
占全球被攻击国家 53.2%



本季度中国共发生27,125次DDoS攻击，受攻击最严重的地区是浙江、广西、广东、香港、江苏等东南沿海地区。

2016Q2季度中国范围内DDoS攻击态势图



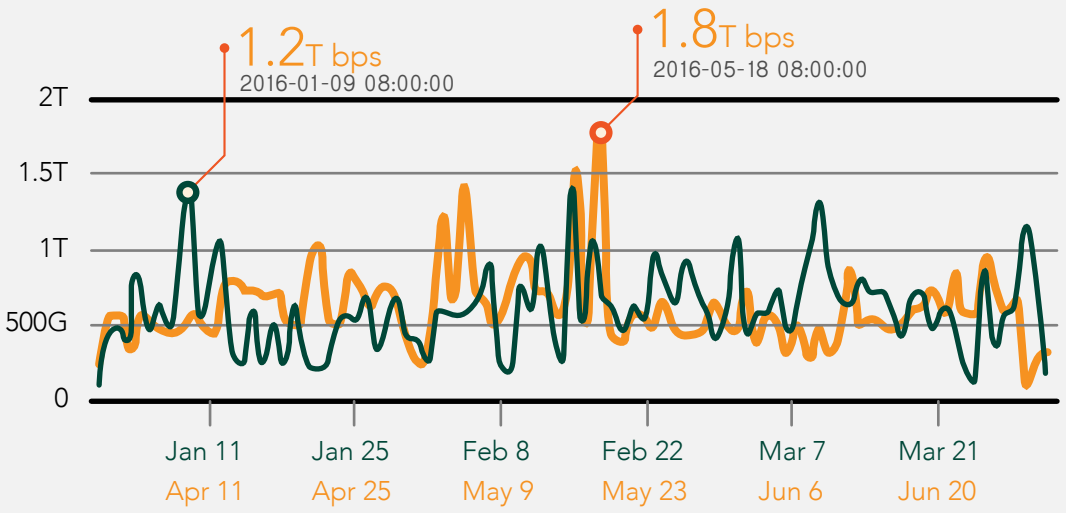
2016Q2季度全球被攻击国家按次数占比图

Q2单一时间点攻击流量峰值1.8T，单次攻击峰值445.7G，300G以上的攻击16次。

DDoS 攻击峰值

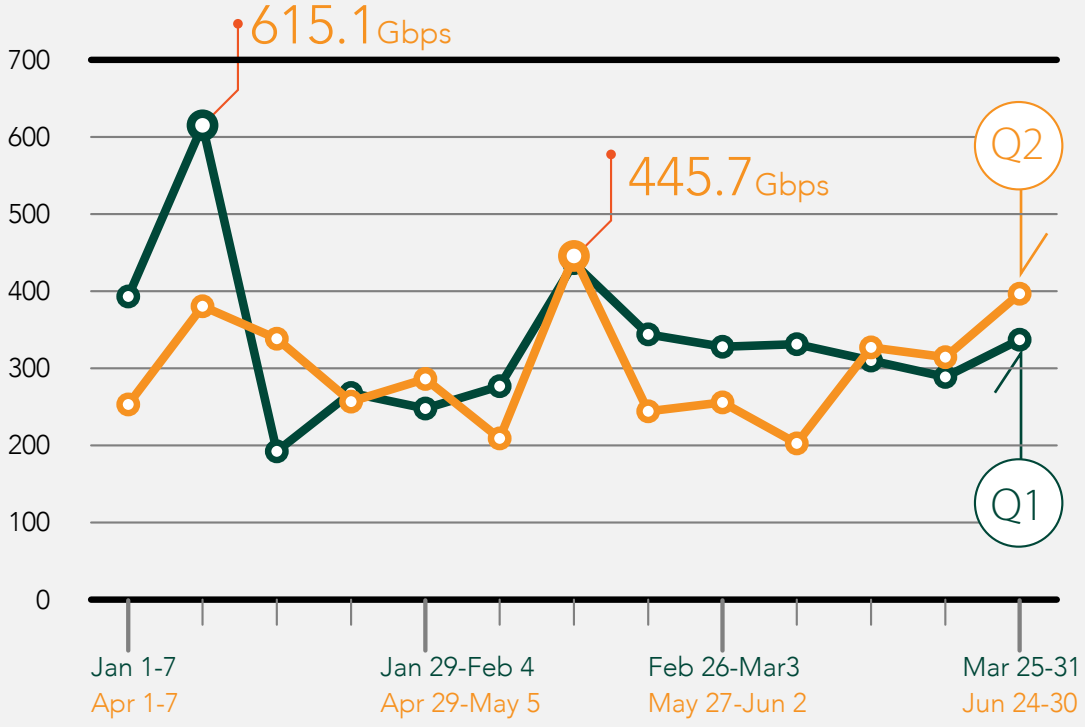
Q2季度的DDoS平均攻击峰值有所下降，Q2平均攻击峰值为16.7Gbps，相比Q1的27Gbps下降38.1%。

在2016年5月18日8点，观测到的总体攻击流量峰值达到 1.8Tbps，比Q1季度的1.2Tbps增长600Gbps。



2016Q1和Q2季度全球DDoS攻击累计总流量趋势图

本季度DDoS攻击单次最高峰值为445.7Gbps，相比Q1季度的615.1Gbps峰值有所下降。

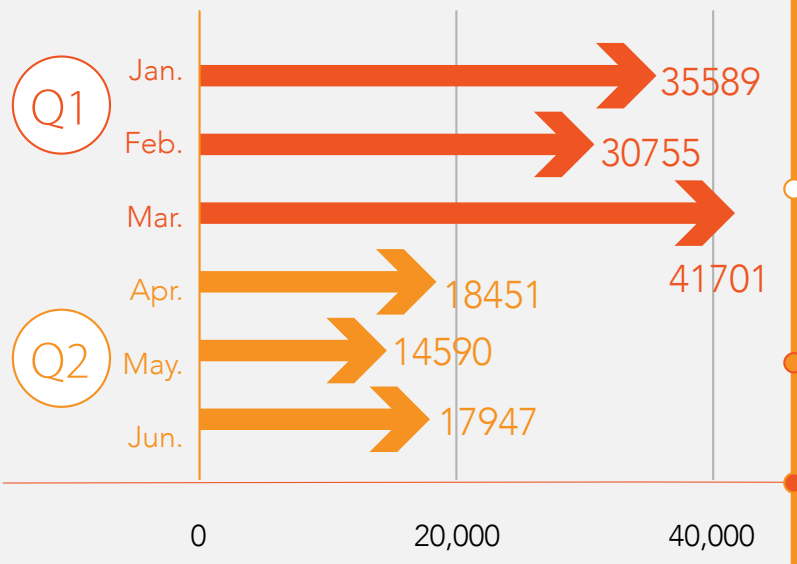


2016Q1和Q2季度单次DDoS攻击事件周峰值趋势对比图

本季度拥有最高攻击峰值的DDoS攻击发生在5月中旬，引人注意的不仅是该次DDoS攻击的高峰值，还有此次攻击是利用TCP（含SYN、RST ACK、RST、TCP Flag Misuse等）和 UDP流量发起的混合攻击，主要针对TCP和UDP 53端口，攻击高峰持续了将近一个小时。针对同一目标的DDoS攻击，从4月初就已经开始，断断续续直到6月底才彻底结束。除了上述混合攻击外，针对该目标，攻击者还多次采用了DNS Request Flood和UDP Flood 混合的脉冲攻击，脉冲波峰和波谷持续时间不断变换，有时半小时1次波峰，有时10分钟一次波峰，攻击者试图探测该目标流量处理能力的极限。

对这些攻击进行溯源分析，我们看到，攻击者轮流调用分布在全球范围约3万4千个僵尸主机发起DDoS攻击。该僵尸网络主要为Billgates botnet的一个变种，被控的主机大部分为带有高危漏洞或者弱口令的服务器，攻击峰值较大的肉鸡主要来自云端，另外少部分是被控制的网络监控摄像头。

DDoS 攻击次数

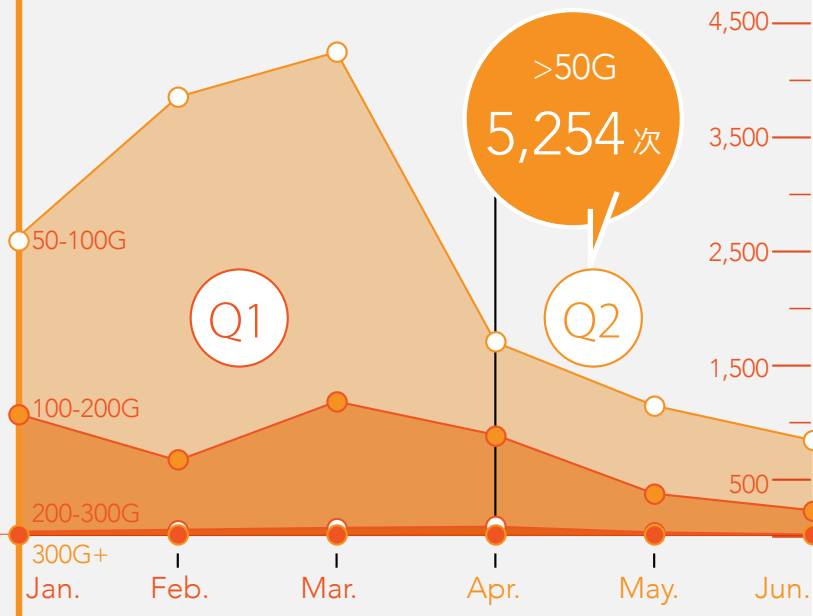


2016Q1 vs Q2 季度各月份DDoS攻击次数图

Q2季度发生的DDoS攻击总数相比Q1季度有所下降。

- 4月份共发生DDoS攻击18451次，相比3月份下降了55.8%。
- 5月份发生的DDoS攻击继续下降，相比前一个月下降20.9%，
- 6月份攻击有17947次，有所上升。

大流量 DDoS 攻击次数

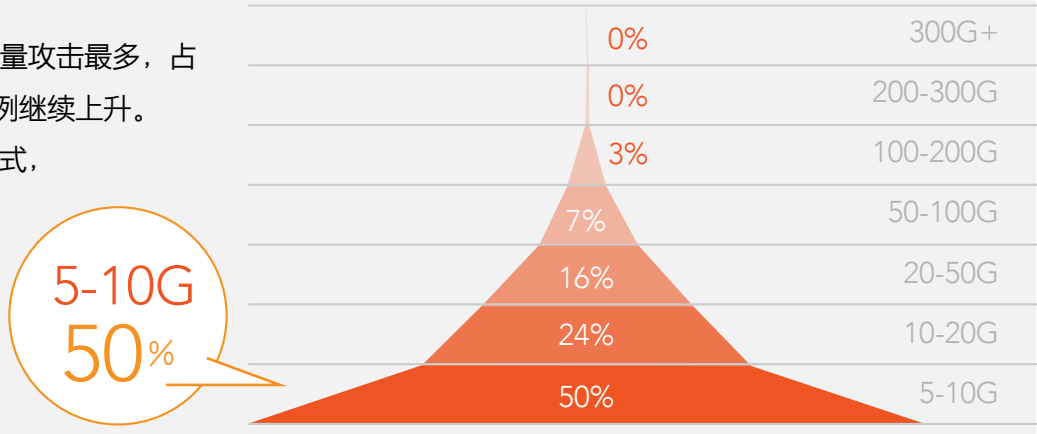


2016Q1和Q2季度各月份大流量（峰值>50Gbps）攻击次数图

Q2季度DDoS攻击峰值在50Gbps以上的大流量攻击共发生5254次，峰值在300Gbps以上的攻击共发生16次。

攻击流量各区间大小占比

Q2季度仍然是峰值在10Gbps以下的小流量攻击最多，占比达50%，相比Q1季度的40%其所占比例继续上升。可见攻击者越来越多地使用小流量攻击方式，只是攻击手段更加复杂。

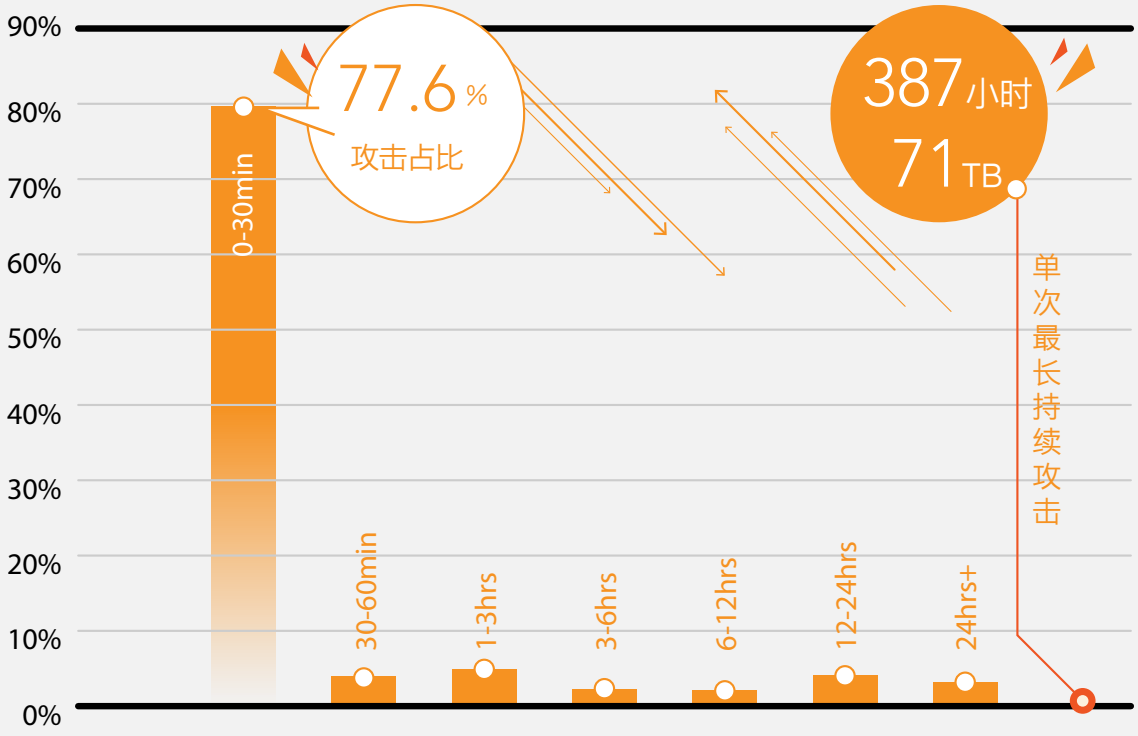


2016Q2季度攻击流量区间占比图

Q2平均攻击时长1.6小时，单次攻击最长387小时71T。

Q2季度平均攻击时长为1.6小时，攻击时长在30分钟以下的攻击继续增长，占总数的77.6%，比Q1季度增加21.6%。本季度攻击时长超过1天的攻击占总攻击次数的3.2%，比上一季度下降了8.7%。我们监控到最长的一次DDoS攻击持续了387小时，累计总攻击流量达71TBytes。

以上几点变化反映了Q2季度DDoS攻击更趋于短时攻击。其主要原因在于本季度反射攻击、混合攻击、脉冲攻击更加活跃，攻击者选择的攻击手段趋于复杂化，使用更短的时间就达到更好的攻击效果。

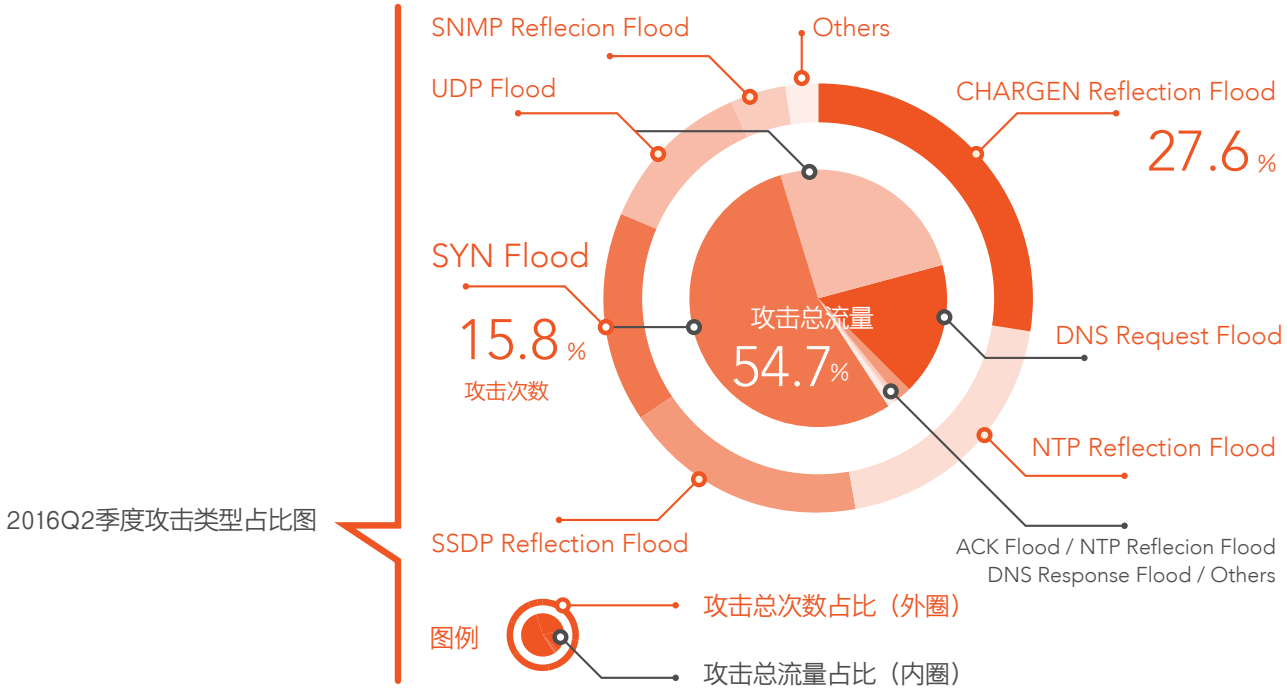


2016Q2季度攻击流量区间占比图

从攻击次数占比看，Chargen发生攻击为27.6%，从攻击流量占比来看，SYN为54.7%。

从攻击次数和攻击总流量占比来看，SYN Flood攻击依然在所有攻击类型中占比重较大，分别为15.8%、54.7%。另外，Q2季度各类型反射攻击比较活跃。

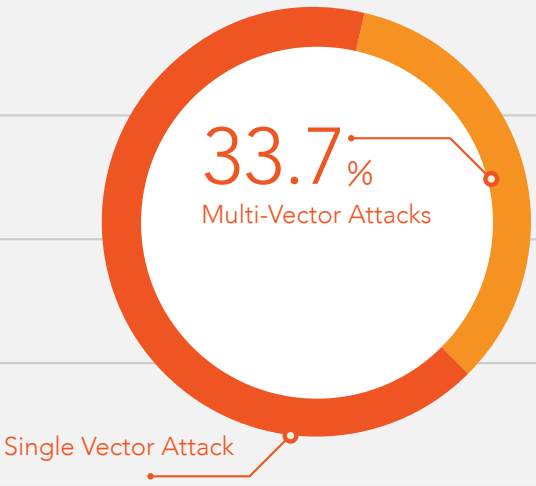
从攻击次数占比来看，Q2季度反射类型的攻击占总攻击次数的62.1%，其中NTP反射、CHARGEN反射、SSDP 反射攻击较多。



2016Q2季度攻击类型占比图

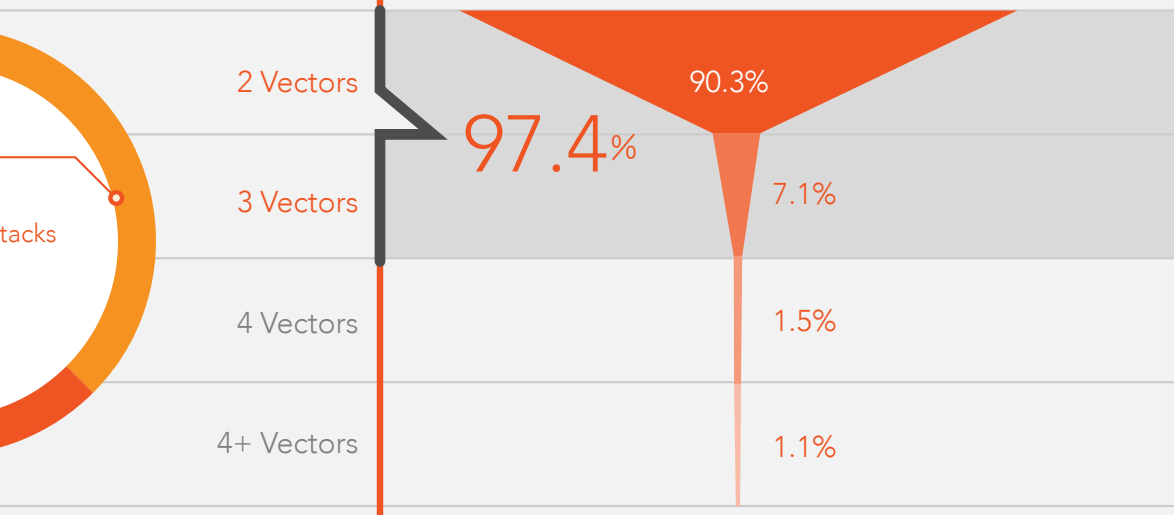
从流量来看，混合攻击占总比33.7%，其中2-3种混合攻击占97.4%。

Q2季度的DDoS攻击次数和大流量DDoS攻击事件相比Q1有所下降，但攻击手段更加复杂，我们观测到很多利用几种流量混合发起的攻击，这类攻击相比单类型攻击，对攻击目标网络破坏能力更强。从攻击总流量占比看，利用混合攻击手段发起的攻击流量占总类型分布的33.7%。



2016Q2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，统计其混合攻击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97.4%。



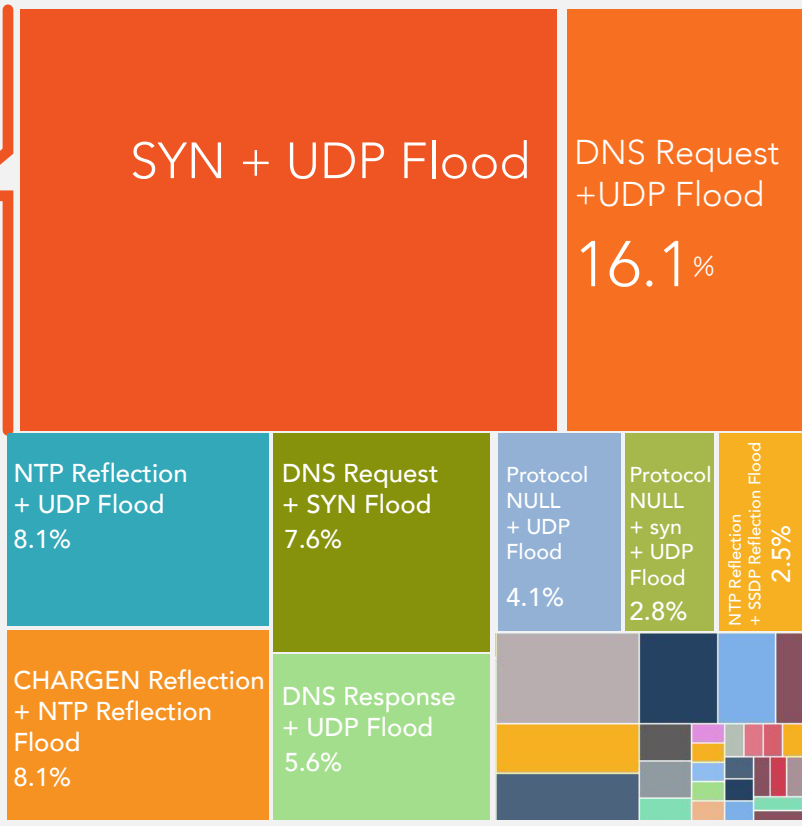
混合DDoS攻击种类数占比图

另外，对攻击者最常使用的混合类型做了统计，其占比如图所示。

36.1%
SYN+UDP

本季度最常见攻击混合类型为SYN Flood和UDP Flood攻击混合，占全部混合类型的36.1%。

另外发现较多使用反射攻击流量混合的情况，例如NTP Reflection Flood和UDP Flood混合，CHARGEN Reflection和NTP Reflection Flood混合，也有部分是NTP Reflection和SSDP Reflection Flood混合。
反射类型参与的混合攻击占全部混合种类的23%。

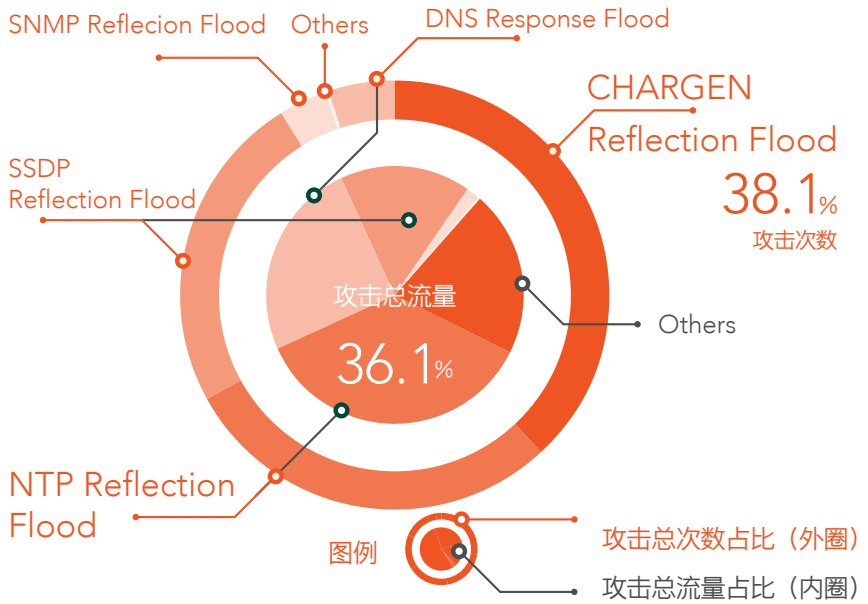


混合攻击按混合类型发生次数统计分布图

Q2季度反射类型攻击比较活跃，我们对各类反射攻击的次数和流量分别进行了统计。

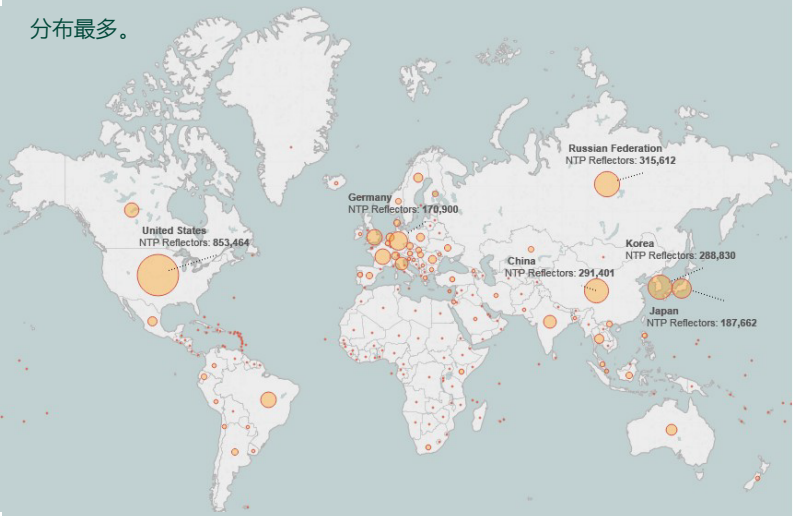
从攻击次数上看，本季度CHARGEN Reflection Flood攻击最为活跃，攻击次数占比38.1%，其次是NTP和SSDP Reflection Flood。

从攻击流量上来看，NTP Reflection Flood攻击流量占比最多，为36.1%，其次是DNS Reflection Flood攻击，攻击流量占比为24.8%。



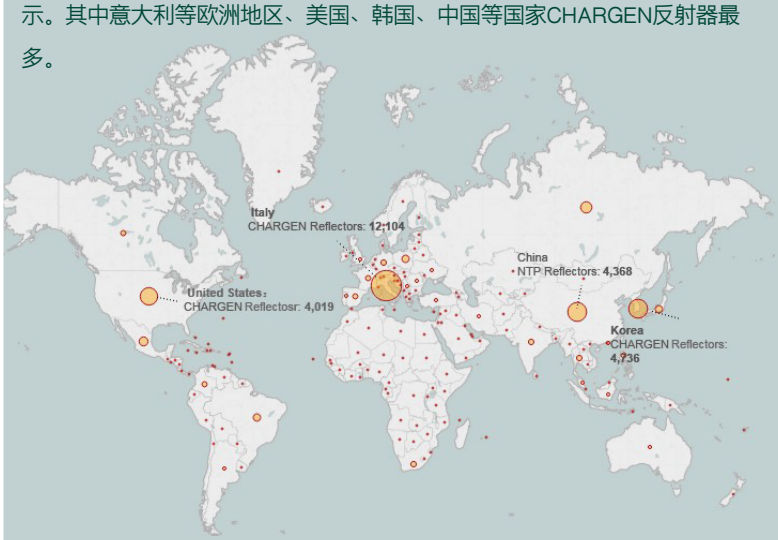
2016Q2季度各类反射攻击占比图

据我们最新统计，目前全球范围内NTP反射器累计达365万个，全球分布情况如下图所示，其中美、俄、中、韩、日，还有德国等欧洲地区NTP反射器分布最多。



2016Q2季度NTP反射器全球分布情况图

目前全球范围内CHARGEN反射器累计达3.8万个，全球分布情况如下图所示。其中意大利等欧洲地区、美国、韩国、中国等国家CHARGEN反射器最多。



2016Q2季度CHARGEN反射器全球分布情况图

本季度被利用来发起NTP Reflection Flood攻击的反射器分布情况如下图所示。

2016Q2季度被利用发起攻击的NTP反射器全球分布情况图

本季度被利用来发起CHARGEN Reflection Flood攻击的反射器分布情况如下图所示。

2016Q2季度被利用发起攻击的CHARGEN反射器全球分布情况图

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

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：绿盟科技全球DDoS态势感知平台

NSFOCUS