

2016Q1 DDoS 态势报告

Content

Content	2
内容摘要	2
特别声明	2
全球 DDoS 攻击事件	3
HSBC 网上银行遭大流量 DDoS 攻击	4
匿名者 (Anonymous) 抗议捕杀海豚活动	3
攻击 BBC 的黑客组织攻击美总统候选人官方网站	3
BTCC 受 DDoS 敲诈攻击	4
金融 DDoS 攻击事件	5
攻击时间分析	5
攻击源 IP 分析	7
攻击手段分析	8
新兴攻击手段	12
DDoS 攻击态势	8
分析方法	2
攻击类型分布	9
攻击事件分布	9
周趋势图	9
大流量攻击事件	10
攻击来源分布	10
攻击时间分布	10
攻击流量分布	11
攻击峰值趋势图	11
攻击流量的分布区间	11
DDoS 防护思想	12
特征+行为	错误!未定义书签。
过滤手段高级化	错误!未定义书签。
智能化防御技术	错误!未定义书签。
威胁情报	14
关于绿盟科技	15

内容摘要

DDoS 攻击是在众多网络攻击中一种简单有效并且具有很大危害性的攻击方式。它通过各种手段消耗网络带宽和系统资源，因而不能对正常用户进行服务，从而也实现拒绝正常用户的服务访问。对于线上产品和服务，造成的危害也是无法估计的。

本次报告中涉及的所有数据，来源于绿盟科技全球 DDoS 攻击态势感知系统和绿盟抗拒绝服务系统。

分析方法

本报告中流量数据分析基于 NetFlow 协议进行，是业界公认的一种统计方法，便于分析 DDoS 攻击流量构成、协议分布以及攻击行为。本报告对于攻击类型分布是从攻击协议流量占比进行分析；其他则是按照攻击事件的次数来进行统计分析。

本报告从 5 个方面进行阐述：先从攻击类型、攻击事件、攻击来源、攻击持续时间、攻击流量等对 DDoS 攻击进行统计分析；展示在第一季度绿盟抗拒绝服务系统的防护案例；介绍新兴的攻击手段，最后描述全球比较重大典型的 DDoS 攻击事件。

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。

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，请联系：

- 绿盟科技博客
- <http://blog.nsfocus.net/>
- 绿盟科技威胁响应中心微博
- <http://weibo.com/threatresponse>
- 绿盟科技微信号
- 搜索公众号 绿盟科技

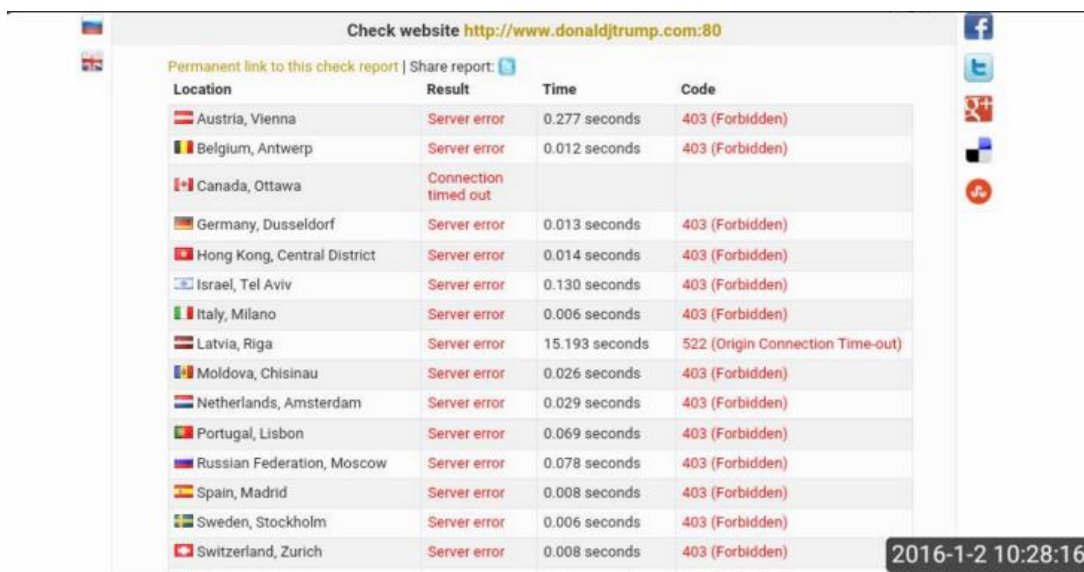
全球 DDoS 攻击事件

在 2016 年第一季度，全球范围内的 DDoS 攻击事件频发。从重大攻击事件分析，追逐利益仍然是黑客攻击的主要动机，“黑客主义”事件也在不断挑战政府的网站。

NWH (New World Hacking) 攻击美总统候选人网站事件

在 2015 年底，New World Hacking(NWH)对 BBC 网站发动了 602Gbps DDoS 攻击，在 2016 年 1 月 2 号这伙黑客组织故技重施，宣称对唐纳德·特朗普的官方竞选网站发动了网络攻击。这次攻击导致网站中断大约半个小时。

New World Hacktivists 在推特上公布了当时攻击数据统计报告：



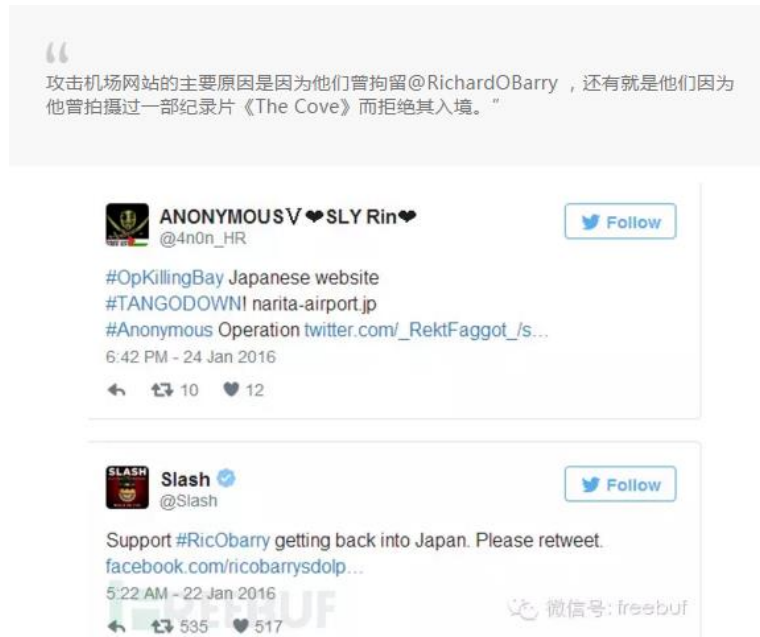
Location	Result	Time	Code
Austria, Vienna	Server error	0.277 seconds	403 (Forbidden)
Belgium, Antwerp	Server error	0.012 seconds	403 (Forbidden)
Canada, Ottawa	Connection timed out		
Germany, Dusseldorf	Server error	0.013 seconds	403 (Forbidden)
Hong Kong, Central District	Server error	0.014 seconds	403 (Forbidden)
Israel, Tel Aviv	Server error	0.130 seconds	403 (Forbidden)
Italy, Milano	Server error	0.006 seconds	403 (Forbidden)
Latvia, Riga	Server error	15.193 seconds	522 (Origin Connection Time-out)
Moldova, Chisinau	Server error	0.026 seconds	403 (Forbidden)
Netherlands, Amsterdam	Server error	0.029 seconds	403 (Forbidden)
Portugal, Lisbon	Server error	0.069 seconds	403 (Forbidden)
Russian Federation, Moscow	Server error	0.078 seconds	403 (Forbidden)
Spain, Madrid	Server error	0.008 seconds	403 (Forbidden)
Sweden, Stockholm	Server error	0.006 seconds	403 (Forbidden)
Switzerland, Zurich	Server error	0.008 seconds	403 (Forbidden)

 **New World Hackers** @NewWorldHacking · 1月2日
Statistics report on [donaldjtrump.com](http://www.donaldjtrump.com)
STILL #TangoDown by New World Hacking
#OpTrump #AnonFamily
1 hour test!

匿名者 (Anonymous) 攻击日成田机场网站事件

2016 年 1 月 24 号，黑客组织匿名者对日本成田国际机场官方网站发起 DDoS 攻击，并迫使其网站服务下线。据官方说明：此次攻击主要分为两种：要么大数据，大流量来压垮网络设备和服务器，要么有意制造大量无法完成的不完全请求来快速耗尽服务器资源，所以需要花掉相当多的时间恢复网站服务。

在这次攻击事件之后 HackRead 与该黑客组成成员一段对话：



英国 HSBC 网上银行遭大流量 DDoS 攻击事件

在 2016 年 1 月 29 日，英国的 HSBC 网上银行遭受大规模的 DDoS 攻击，攻击持续了数个小时，客户无法通过 Web 和 App 登陆网银，HSBC 也发表了被攻击声明。

HSBC internet banking came under a denial of service attack this morning, which affected personal banking websites in the UK.

HSBC has successfully defended against the attack, and customer transactions were not affected.

We are working hard to restore services, and normal service is now being resumed.

We apologise for any inconvenience this incident may have caused.

比特中国 BTCC 遭 DDoS 敲诈攻击事件

根据 BTCC (比特币中国) 官方微博透漏自 2015 年 12 月 19 日以来，陆续收到 DDoS 网络攻击。援引外媒报道在攻击之后 BTC 收到了来自匿名者的勒索信函，要求支付 1 比特币 (约合 2636.5 元) 的赎金，否则会发起更大规模的 DDoS 攻击。在 1 月 1 日，攻击者发动了 10Gbps 的攻击。攻击相比较强烈，导致了网站宕机。



中国金融机构遭 DDoS 攻击事件详解

由于金融行业是易受 DDoS 攻击之一，在第一季度中金融机构被集中攻击也是比较有影响力的事件。

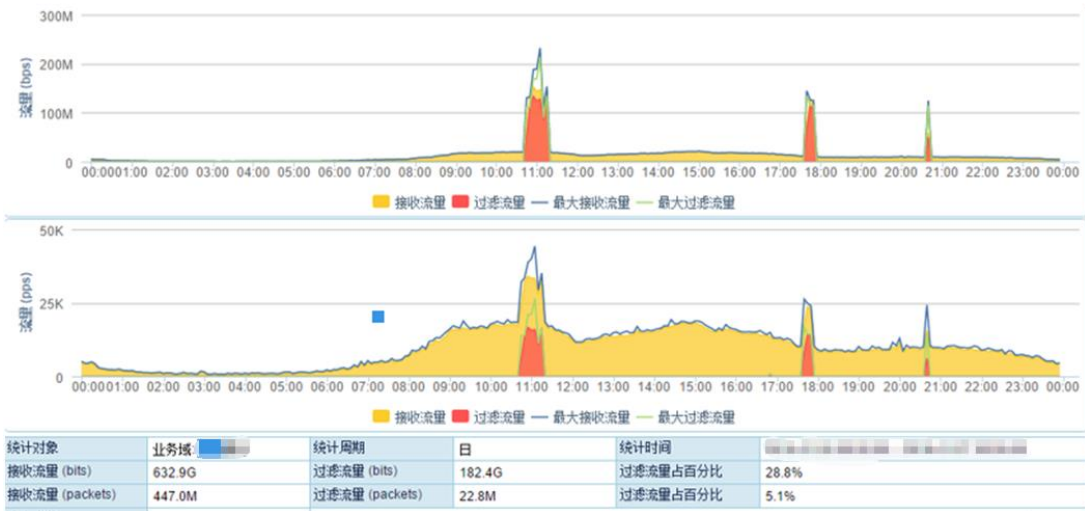
以下从攻击时间、攻击源以及攻击手段对此次事件进行阐述。

2016 年 1 月份，某清洗中心检测到多家金融机构遭受 DDoS 攻击，通过对几次攻击的时间、源 IP 地址以及攻击手段的汇总分析得出结论，此次针对某地区金融行业的攻击行动是同一个黑客组织所为。

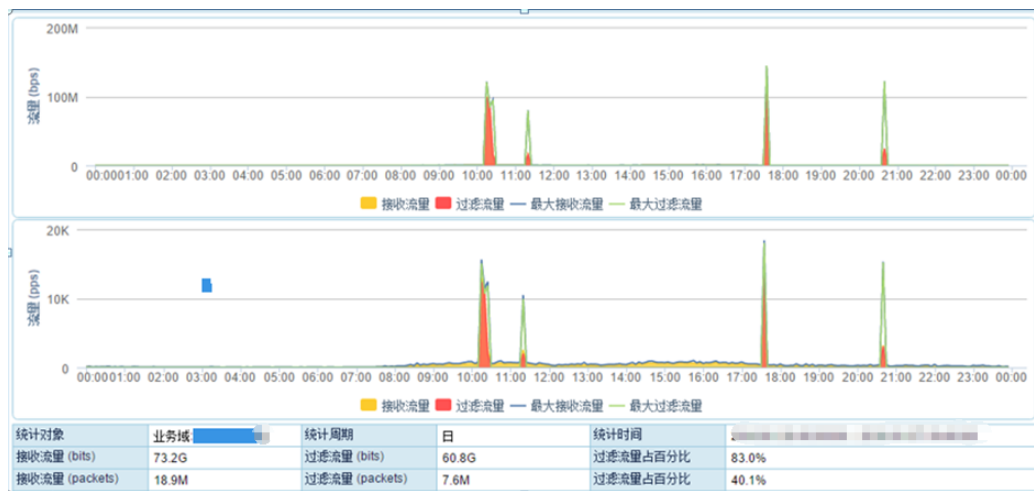
攻击时间分析

从攻击发生的时间来看，出现的多起攻击事件虽然目的客户不同，但是攻击发生的时间点是几乎重叠的。以下针对 2 个攻击分布的时间分析。

攻击时间 A：

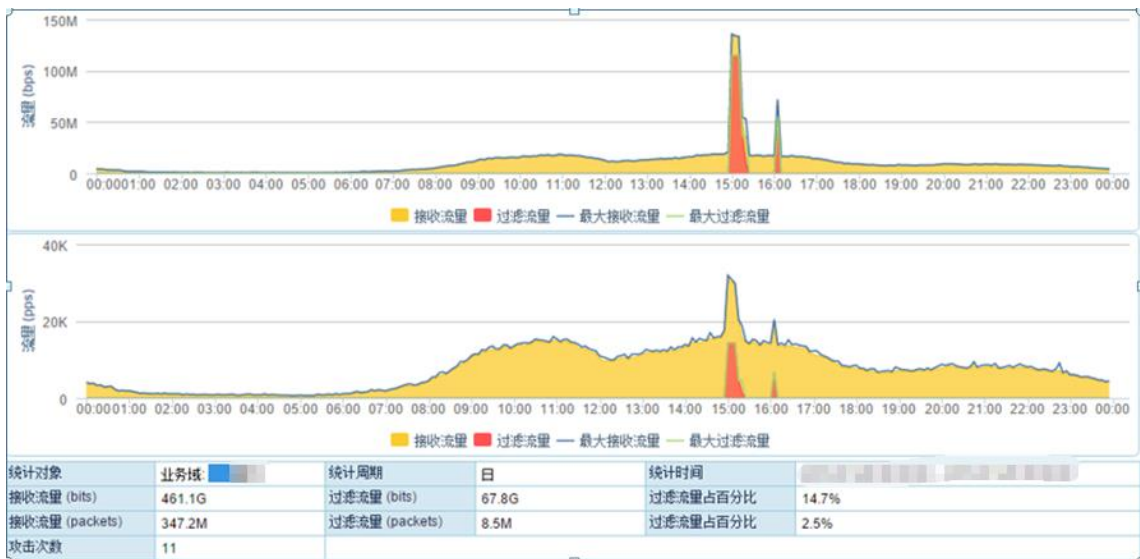


客户 1 受攻击时间



客户 2 受攻击时间

攻击时间 B :



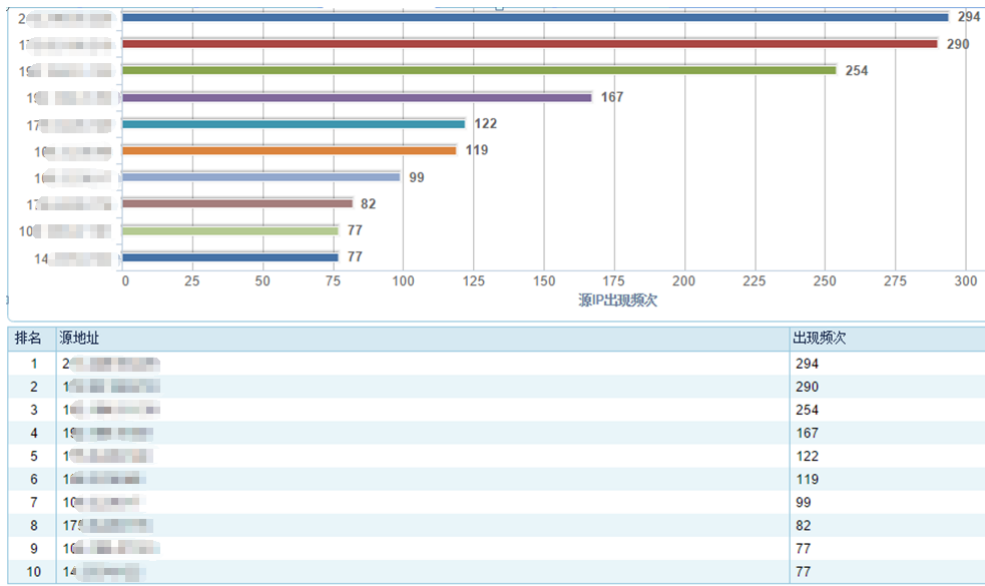
客户 1 受攻击时间



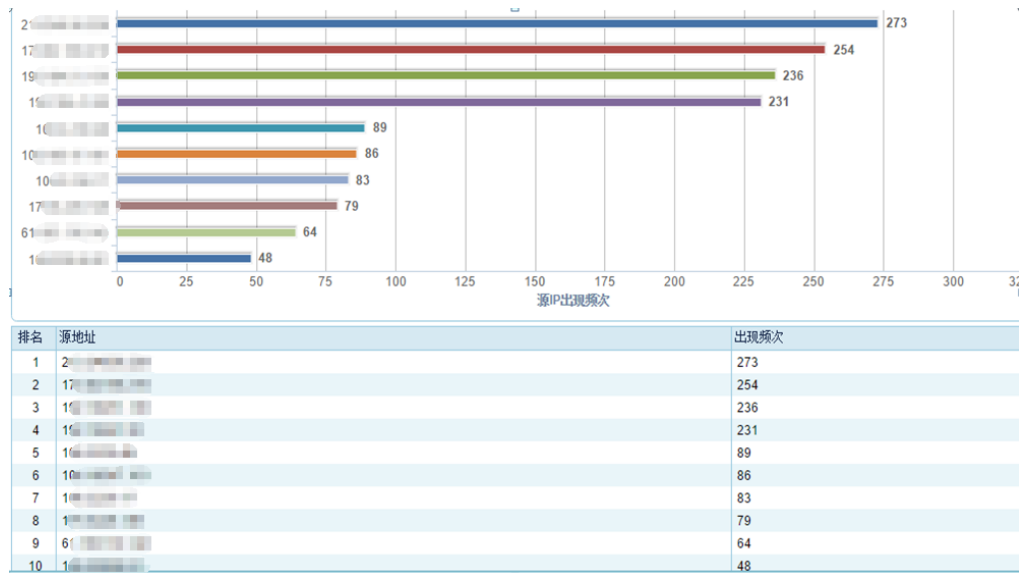
客户 2 受攻击时间

攻击源 IP 分析

从攻击源 IP 的分布来看，绿盟抗拒绝服务系统列举了 2 个攻击时间攻击流量的 Top 10 源 IP 地址中，过半来自海外。通过交叉对比我们发现，此次遭受攻击的数家金融企业都是受到这些源 IP 的攻击。



攻击时间 A 攻击源 IP 分布 Top10



攻击时间 B 攻击源 IP 分布 Top10

攻击手段分析

攻击手法上，此番大规模 DDoS 攻击所使用的攻击手段几乎完全相同，我们通过绿盟抗拒绝服务系统看到黑客通过发送大量 TCP 标志位无效的数据包造成 DDoS 攻击。

全球 DDoS 攻击态势

发现 1：从第一季度的攻击类型分布来看，攻击方式最多的还是占用系统资源的 SYN-FLOOD 以及占用带宽资源的 UDP-FLOOD 攻击。

发现 2：大流量攻击呈现增长趋势，在第一季度的最大攻击峰值达到 615Gbps。

发现 3：对第一季度攻击事件的分析中，30 分钟以内的攻击事件占到 55.95%，5-10G 小流量攻击事件约占 40%。

发现 4：受控攻击来源最多的国家是中国。

攻击类型演变为资源对抗

根据第一季度攻击类型的分布，攻击者使用最多的是 SYN、UDP 协议攻击，其中 SYN 占比最多；在 UDP 的攻击类型中，反射攻击应用也越来越多。顺延了 2015 年绿盟年度 DDoS 的报告中，SYN 和 UDP 的攻击类型占主要的趋势。由此，从攻击类型分布趋势看出，DDoS 攻击已经演变成一种资源的对抗战争，这种占用系统资源型攻击和带宽资源型攻击已经成为主要攻击手段。

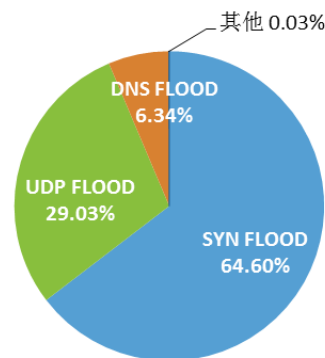


图3-1 攻击类型分布

攻击事件显著增加

周趋势图

从第一季度的攻击事件的趋势来看，在 3 月第二周和第三周攻击事件显著增加。

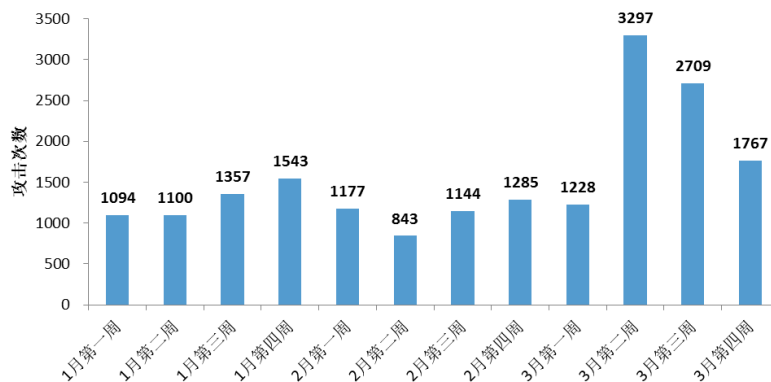


图3-2 攻击事件周趋势图

大流量攻击事件

在第一季度，攻击峰值超过 200Gbps 攻击次数达到 115 次，其中超过 300Gbps 的攻击 19 次，大流量攻击每月有增长趋势。

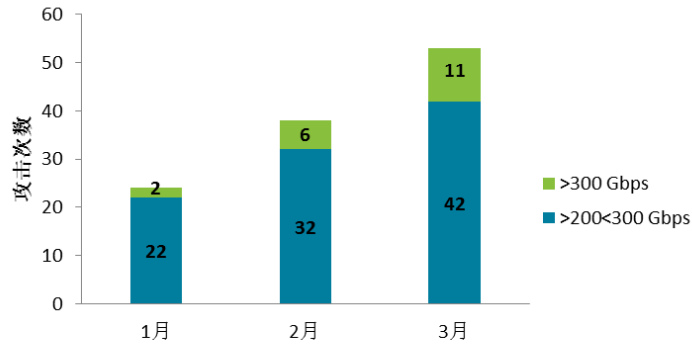


图3-3大流量攻击事件

攻击来源聚焦大国

在第一季度中，攻击来源最多的 Top5 国家，中国和美国是最主要的 2 个来源国家。

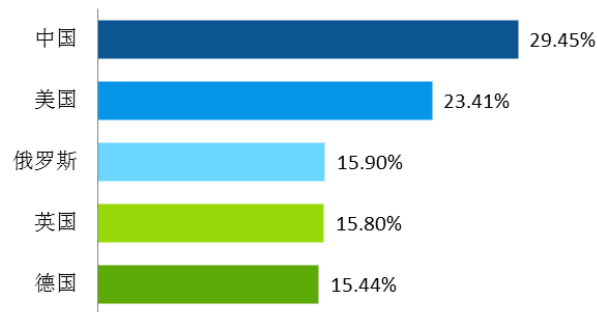


图3-4 攻击来源按国家分布

攻击时间整体缩短

在第一季度，攻击持续时间在 30 分钟以内的攻击事件占总数的 55.95%。说明攻击者更加倾向于短时间的攻击方式。

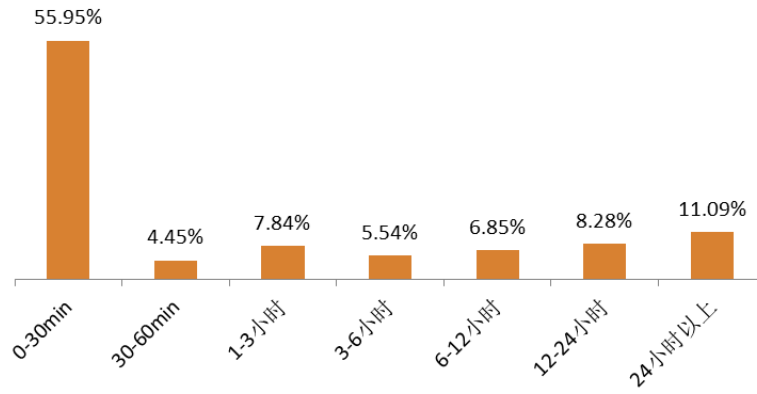


图3-5 DDoS攻击时间分布

攻击次数频繁，多为小流量

攻击峰值趋势图

在第一季度，最大攻击峰值为 615.1Gbps。

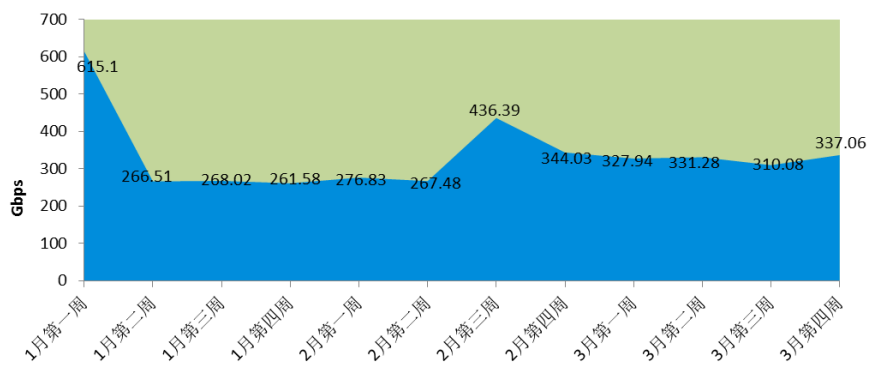


图3-6攻击峰值周趋势图

攻击流量的分布区间

统计第一季度不同攻击流量区间的攻击事件，可以看出 5G-10Gbps 流量的攻击事件最多，约占到 40%。

攻击者倾向于选择小流量的攻击方式。

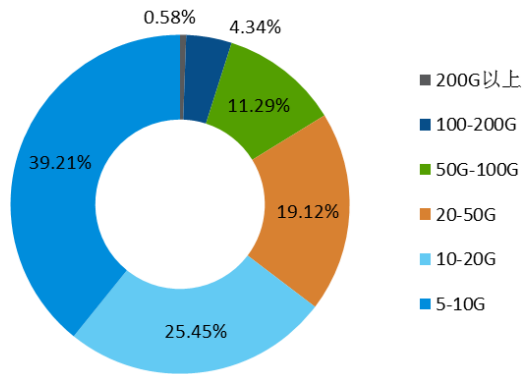


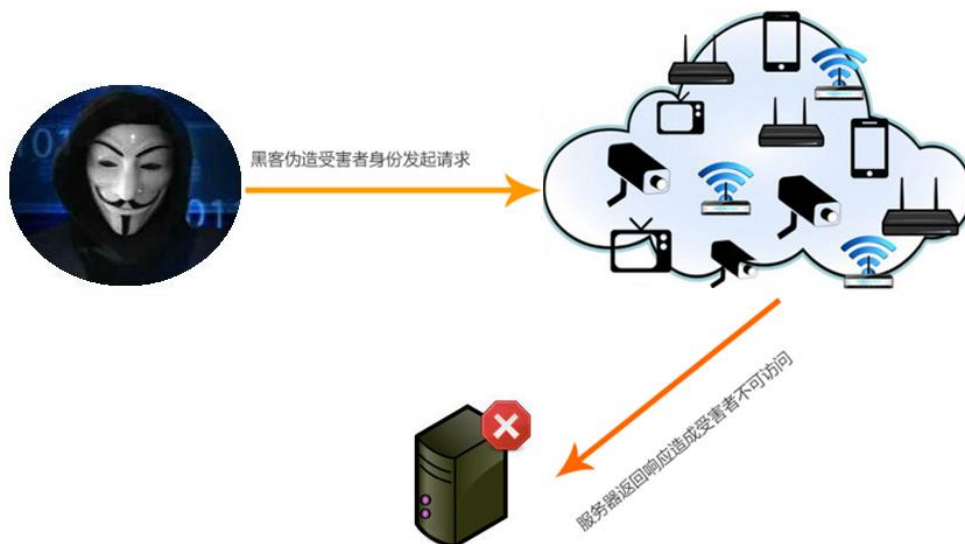
图3-7 流量攻击次数分布

新兴攻击手段

TFTP DDoS 反射放大攻击：

最近，爱丁堡龙比亚大学的研究人员已经发现 TFTP 服务器可以被利用为反射 DDoS 攻击。放大倍数能达到 60 倍，远高于许多其他协议。

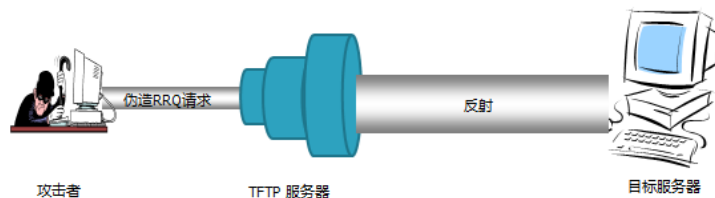
分布式反射攻击拒绝服务器攻击又称为 DRDoS 攻击 (Distributed Reflecion Denial of Service)，其原理是黑客伪造成被攻击者的 IP 地址，向互联网上大量开发特定服务器发起请求，接收到请求的那些主机根据源 IP 地址将相应数据包返回给受害者。如下图是典型的 DRDoS 过程：



典型的 DRDoS 过程

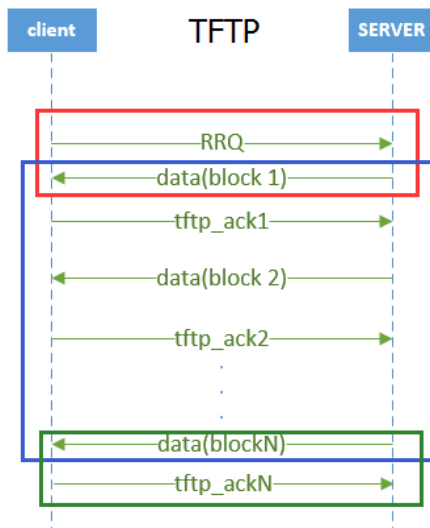
黑客往往会选择那些响应包远大于请求包的服务来利用，以较小的流量换取更大的流量，获得几倍甚至几十倍的放大效果。

TFTP 反射放大攻击分析，如下图：反射攻击示意图



反射攻击示意图

- (1) **为什么能反射**：由于 TFTP 是基于 UDP 传输的，所以只要伪造源向 TFTP 服务器发送请求，很容易进行反射。
- (2) **反射过程分析**：根据 TFTP 协议过程，TFTP 发起反射放大攻击，主要是靠第 1 个 RRQ 包，因为反射后的 data 包打到了目标服务器上，而且更换了端口（由 69 换成随机的），攻击者很难再伪造一个 ack 包给 TFTP 服务器以便让服务器发送下一个 data。



TFTP 协议过程

- (3) **反射放大倍数**：根据实验比如客户端发送一个 60 字节左右的 RRQ 请求报文，服务器回复的第 1 个 data 为 558 字节，放大倍数大概为 9 倍。因为反射的 data 包被打到目标服务器上，而目标服务器不会发送 ACK 包响应，所以 TFTP 就会利用他的重传机制，定时重传这个 558 字节的 data，直至超时，所以放大倍数应该是 $9*N$ ，放大倍数还是非常的可观。
- (4) **特点**：相对于其他的反射放大工具的区别在于，TFTP 的源端口可以是随机的，检测防护会更加的有难度。

DDoS 防护思想

从第一季度的 DDoS 的态势来看，DDoS 攻击仍然火热，攻击工具层出不穷，攻击事件也在频频发生。

由此，针对 DDoS 攻击的识别，以及在防护技术的发展上至少有以下 3 个方面的考虑：

1) 增强攻击行为识别，除了传统意义上的特征扫描和防护，需加大对攻击行为的跟踪，一方面以避免攻击者对于攻击环境的侦测，另一方面提高攻击识别率；

2) 增加过滤手段，包括基于威胁环境和正常业务环境的过滤技术，比如云端威胁 IP 信誉库，云端威胁指纹库，基于业务正常环境的“白”的过滤技术，如地理位置，业务端口，时间段等。

3) 智能化防御技术，在第一季度的报告看出，短时间攻击比重很大，为了提高防护的效率和效果，应该增加自学习、自动化技术，比如自学习用户业务环境，生成正常业务基线参数；感知设备攻击效果而自动化轮换防御算法等。

绿盟科技安全专家联合威胁响应中心的技术专家，对 2016 年第一季度 DDoS 态势进行了深入分析。

威胁情报



威胁情报的获取及响应都体现了防御能力的建设程度，威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报，并持续对匿名者攻击事件进行关注，保障客户业务的顺畅运行。

如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，可以随时通过在微博、微信中搜索 **绿盟科技** 联系我们，欢迎您的垂询！

关于绿盟科技



北京神州绿盟信息安全科技股份有限公司（简称**绿盟科技**）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。