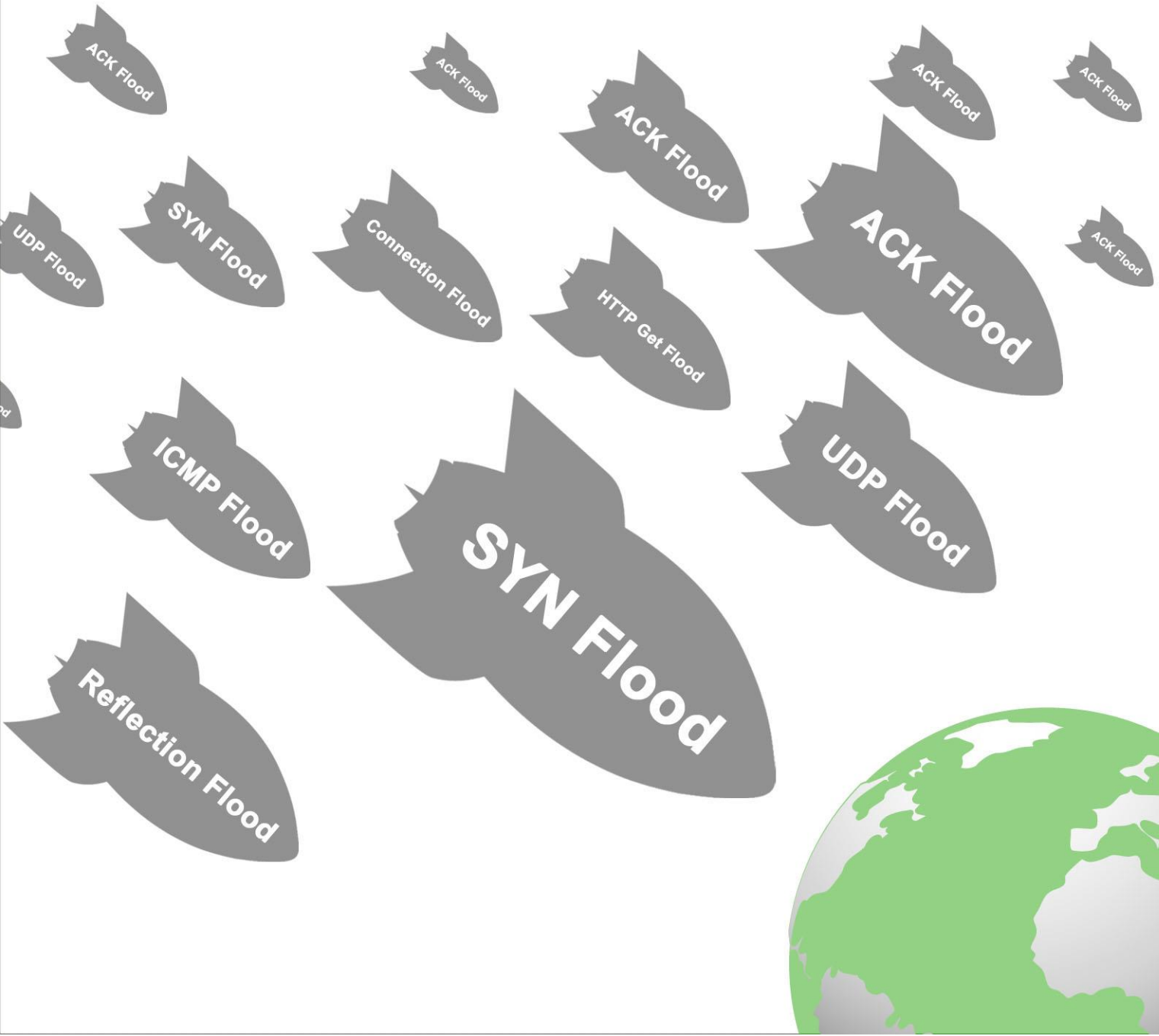
NSFOCUS

NSFOCUS
DDoS THREATS REPORT 2013 H1

2013H1绿盟科技DDoS威胁报告



执行摘要

多年来，绿盟科技致力于帮助客户实现业务的安全顺畅运行。每天，我们的防护产品和监测系统会发现数以千计的 DDoS（分布式拒绝服务）攻击在危害客户安全。为了向用户提供更多关于这类攻击的信息，绿盟科技威胁响应中心特别发布此报告。

2013 上半年，DDoS 攻击备受瞩目。黑客组织伊兹丁·哈桑网络战士向美国发起的挑战依然持续，许多知名银行因受到攻击而服务中断。反垃圾邮件组织 Spamhaus 受到的攻击，被认为是史上规模最大的 DDoS，流量达到了惊人的 300G。面对汹涌而来的数据洪流，没有谁敢说自己的防御系统万无一失。

大企业和大机构总是成为新闻头条。然而中小企业面对 DDoS 威胁时的境遇同样惨烈。上半年，九成以上的攻击发生在半小时之内，八成以上流量小于 50Mbps，三分之二的受害者遭受过不止一次攻击。攻击者反复采用时间短且流量小的 DDoS，可能只是因为这样可以用较小的成本来达成目的。

本报告从 DDoS 的概述、目标和方法角度对这一威胁进行了描述。其中的数据源自 90 次重大新闻报道和 168459 次攻击事件。所有数据在进行分析前都已经过匿名化处理，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报告中。

正文目录

图目录

DDoS 的攻击概述

2013 上半年 DDoS 事件和攻击频发。平均每两天，就会有一次重大 DDoS 事件被报道；而每两分钟，绿盟科技就会监测到一次 DDoS 攻击。攻击和重大事件在 4、5 月各自达到峰值。黑客行动主义是重大 DDoS 事件发生的主要原因，其次是商业犯罪和网络战。

观点 1：平均每两天发生一起重大 DDoS 攻击事件，每两分钟发生一次普通 DDoS 攻击事件

绿盟科技在 2013 上半年跟踪了新闻媒体报道的 90 次重大 DDoS 事件，平均每两天一次。同时，我们共监测到 168459 次 DDoS 攻击，平均每两分钟发生 1.29 次。其中重大事件在五月最多，而 DDoS 攻击则在四月达到峰值。

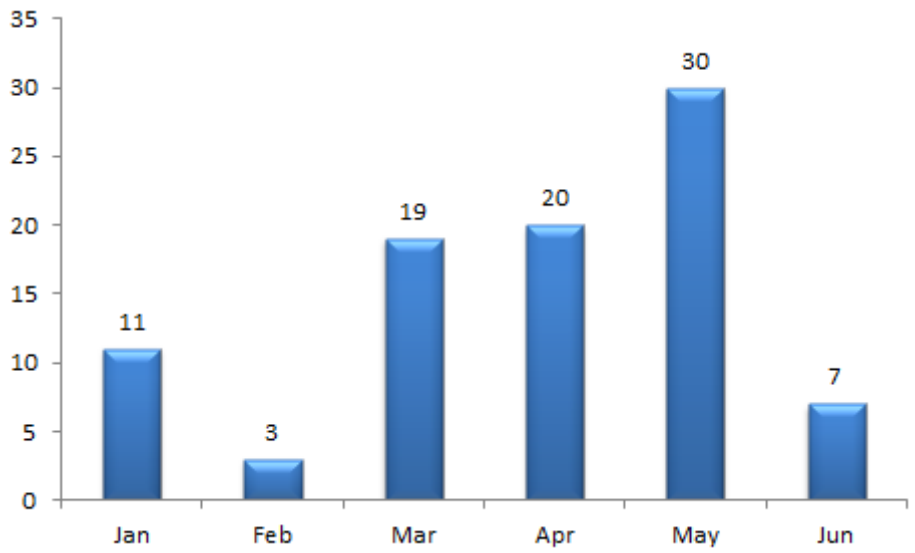


图 1　2013 上半年重大 DDoS 事件

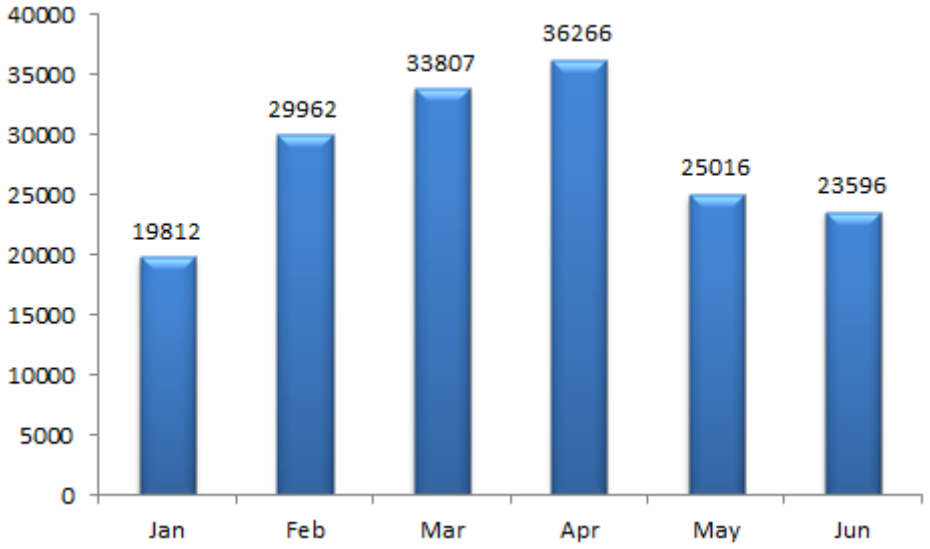


图 2　2013 上半年 DDoS 攻击

观点 2：黑客行动主义是重大 DDoS 事件发生的最主要原因，其次是商业犯罪和网络战

从绿盟科技跟踪的 90 次重大 DDoS 事件报道来看，黑客行动主义是发生重大 DDoS 事件的最主要原因。其次是商业犯罪和网络战。

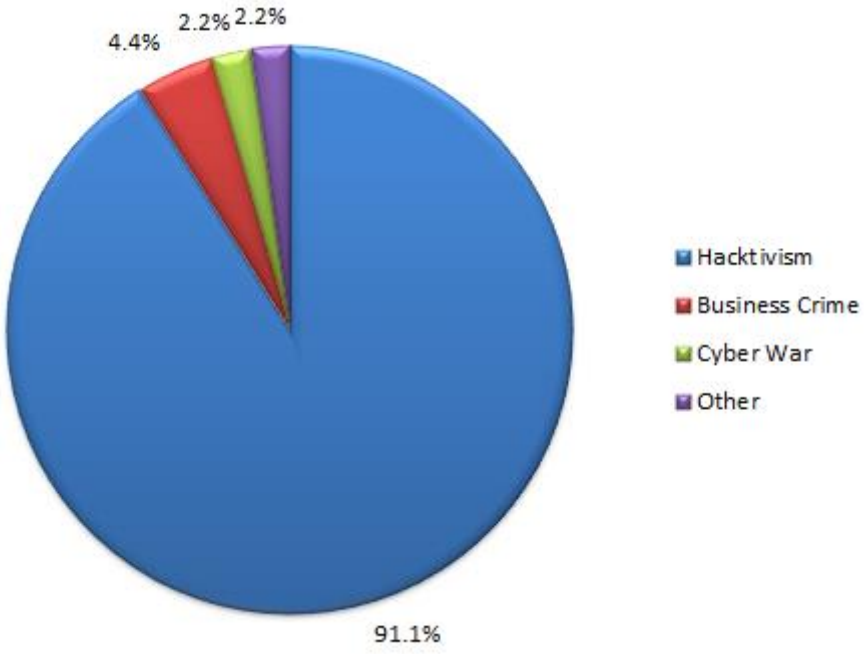


图 3　发生重大 DDoS 事件的原因

DDoS 的攻击对象

2013 上半年，DDoS 是安全界的焦点之一，主要原因是 Qassam 组织开展的“燕子行动”，美国银行业成为了这次行动的最大受害者。最受关注的事件中，被攻击者还包括一些政府和商业公司。此外，在绿盟科技监测的一般性攻击中，九成的对象位于中国。而三分之二的受害者遭遇了多次攻击。

事件 1：“燕子行动”(Operation Ababil)

2012 年 7 月，一个由美国人萨姆-巴西利(Sam Bacile)制作并导演的关于伊斯兰教先知穆罕默德的影片的预告片被放到 YouTube 上，引来了穆斯林世界的强烈抗议。同年 9 月 18 号，一群号称伊兹丁·哈桑网络战士（Cyber fighters of Izz ad-din Al-Qassam）在 pastebin 网站上发布公告，声明称其将美国银行和纽约交易所列为攻击目标，在 YouTube 上这部亵渎穆斯林先知的影片被移除之前，攻击将一直持续。从此，代号为“燕子行动”（Operation Ababil）的一系列针对美国金融机构的 DDoS 攻击事件拉开了序幕。“燕子行动”(Operation Ababil)这个代号引用自《可兰经》里的安拉派燕群去摧毁一队由也门国王派出攻击麦加的象群的故事。

到 2013 年 6 月为止，整个行动经历了三个阶段。第一阶段始于 2012 年 9 月 18 号，持续了 5 个星期；第二阶段从 2012 年 12 月 10 号开始，持续 7 个星期；第三阶段从 2013 年 3 月 5 日开始，持续 9 个星期，到 5 月 6 日停止。其中 2013 年上半年的行动如下图 4 所示。2013 年 7 月 23 日，第四阶段也已开始。

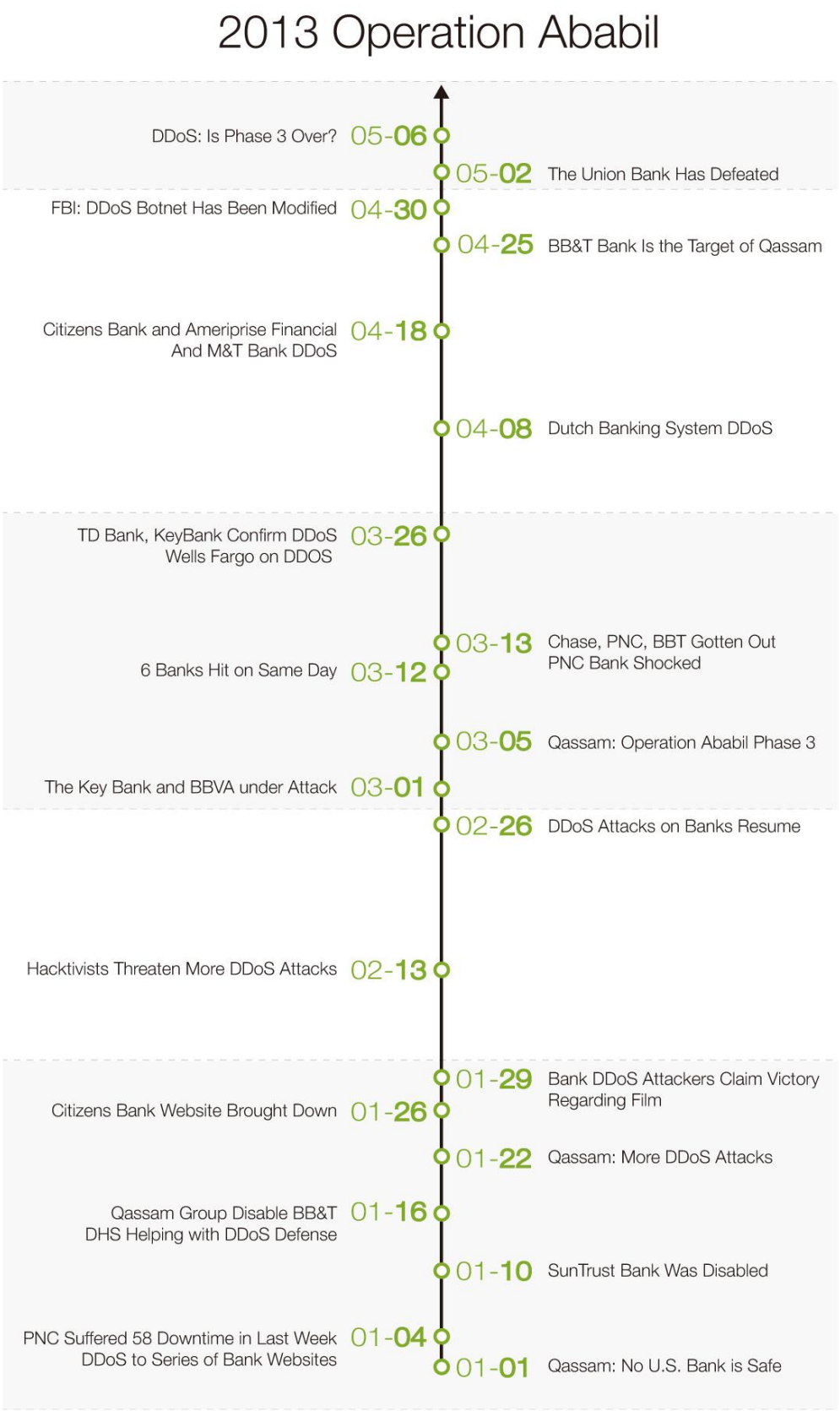

2013 Operation Ababil
DDoS: Is Phase 3 Over? 05-06
05-02 The Union Bank Has Defeated
FBI: DDoS Botnet Has Been Modified 04-30
04-25 BB&T Bank Is the Target of Qassam
Citizens Bank and Ameriprise Financial And M&T Bank DDoS 04-18
04-08 Dutch Banking System DDoS
TD Bank, KeyBank Confirm DDoS Wells Fargo on DDOS 03-26
03-13 Chase, PNC, BBT Gotten Out PNC Bank Shocked
6 Banks Hit on Same Day 03-12
03-05 Qassam: Operation Ababil Phase 3
The Key Bank and BBVA under Attack 03-01
02-26 DDoS Attacks on Banks Resume
Hacktivists Threaten More DDoS Attacks 02-13
01-29 Bank DDoS Attackers Claim Victory Regarding Film
Citizens Bank Website Brought Down 01-26
01-22 Qassam: More DDoS Attacks
Qassam Group Disable BB&T DHS Helping with DDoS Defense 01-16
01-10 SunTrust Bank Was Disabled
PNC Suffered 58 Downtime in Last Week DDoS to Series of Bank Websites 01-04
01-01 Qassam: No U.S. Bank is Safe

图 4　燕子行动时间线

在整个行动中，大多数美国金融机构的在线银行业务都遭受到了攻击，其中包括美国银行(Bank of America)、花旗集团(Citigroup)、富国银行(Wells Fargo)、美国合众银行(US Bancorp)、PNC 金融服务集团、第一资本(Capital One)、五三银行(Fifth Third Bank)、BB&T 银行和汇丰银行(HSBC)。DDoS 攻击对上述银行网站业务的连续性和可获得性造成了严重的影响，同时也对银行的声誉造成了不可估量的损失。由于事态的严重性，美国政府部门，包括国土安全部(DHS)、联邦调查局（FBI）以及金融监管机构，均参与了事件的调查和处理。

观点 3：银行、政府和商业公司是 DDoS 攻击的最大受害者

绿盟科技跟踪了上半年世界上较为重大的 90 次 DDoS 攻击事件，其中针对银行的事件共计 39 次，占 43%。造成这种现象的主要原因是黑客组织 Cyber fighters of Izz ad-din Al-Qassam，在从去年开始的燕子行动中，对美国银行业发动了持续数月的 DDoS 攻击。此外，针对政府 DDOS 攻击发生 26 次，占 29%；而针对商业企业的 19 次，占 21%。而非政府组织和网络服务提供商也是攻击目标。

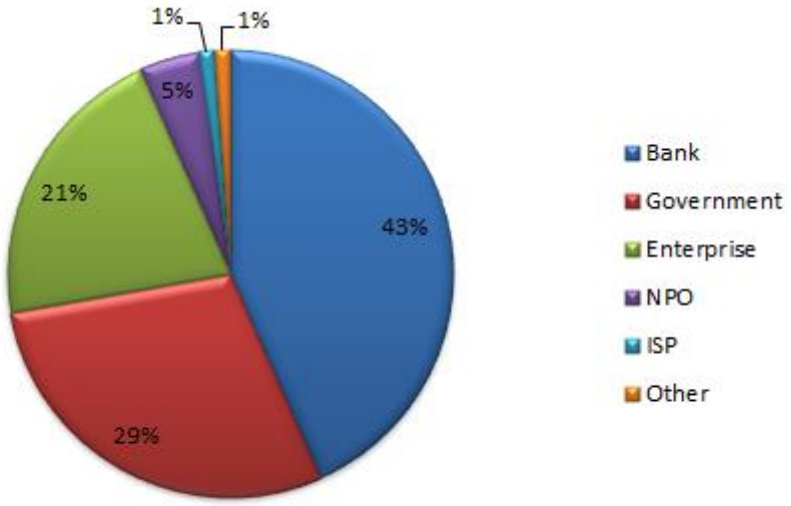


图 5　DDoS 攻击目标的行业分布

观点 4：中国依然是 DDoS 攻击的主要受害者，其次是美国、韩国等地

中国依然是 DDoS 攻击的主要受害者，占被攻击总数的 92.3%。其次是美国，占 5.8%。这一结果可能带有地域性，这是由于当前绿盟科技的大部分监测和防护业务在亚太地区，所以得到的数据也以这一区域为主。

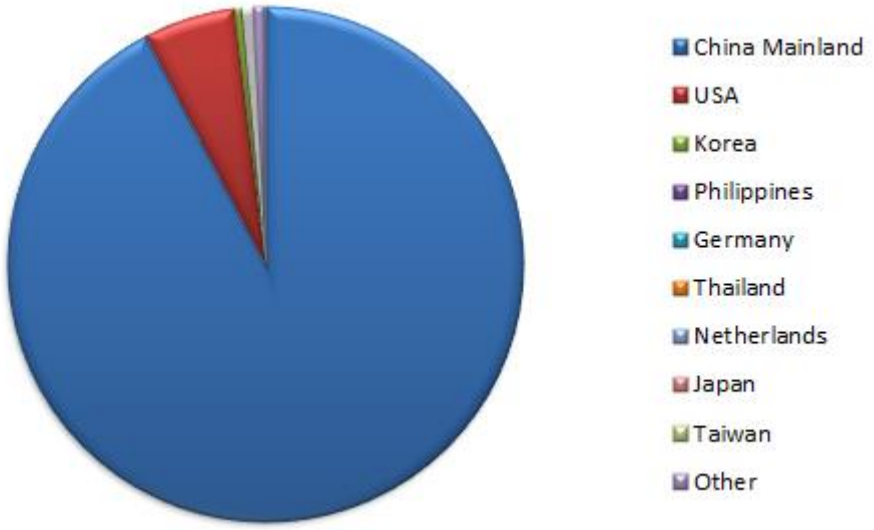


图 6　DDoS 攻击目标的地理分布

观点 5：三分之二的受害者遭遇多次攻击，6%在 10 次以上

攻击者往往会对同一目标发起多次攻击。2013 上半年，31.3%的受害者遭受了一次 DDoS 攻击，而 6.1%甚至遇到了 10 次以上。在 2012 全年内，有 50.7%的受害者遭受了一次 DDoS 攻击，5.2%遇到了 10 次以上。也就是说，去年只有一半受害者遭到了多次攻击，而今年上半年这一比例则达到了三分之二。很明显，攻击者现在更倾向于多次攻击同一目标，在 2013 下半年这一趋势还可能加强。产生这种现象的原因可能有两种：第一，攻击者进行 DDoS 攻击也需要考虑成本，例如租用僵尸网络，短期多次的攻击可以耗费较少的资金，而使效果看起来比较大；第二，一些没有防御能力的网站在受到攻击时不得不支付勒索金，消息传出后，自然成为其他攻击者的优先目标。

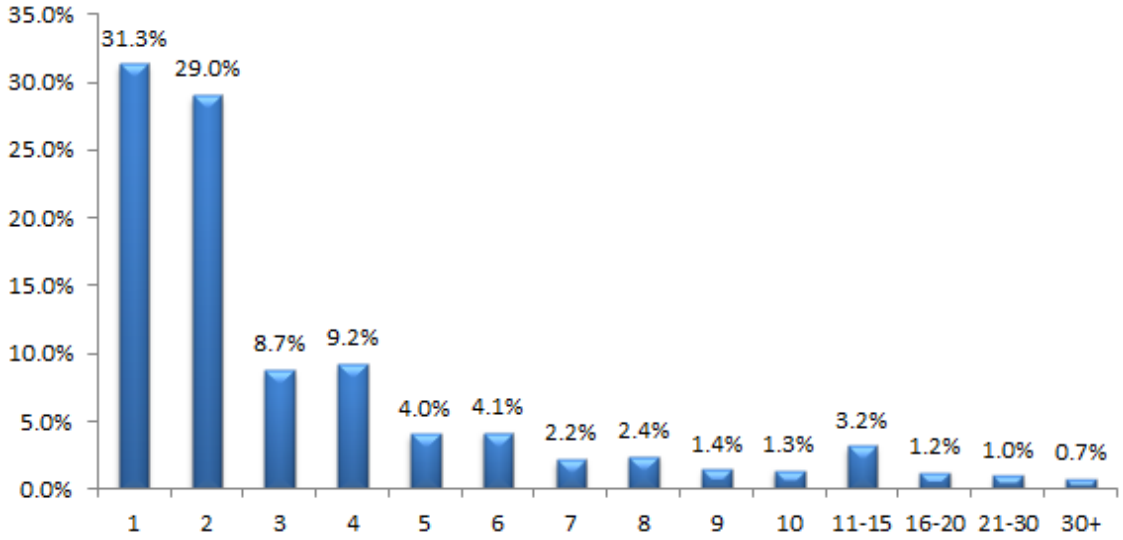


图 7　DDoS 的攻击频次

DDoS 的方法

2013 上半年，DDoS 攻击所采用的方式正在发生分化。一方面，攻击者不断追求更大的攻击流量。三月 Spamhaus 攻击事件被认为是史上最大规模的 DDoS 攻击，达到了惊人的 300G 攻击流量。另一方面，消耗应用资源的 DDoS 攻击大行其道，以 HTTP FLOOD 为代表，被攻击者广泛采用。这类攻击产生的流量和包速率并不大，破坏作用却同样显著。此外，混合攻击所占比重也越来越大，ICMP+TCP+UDP FLOOD 成为最常见的组合。

事件 2：史上最大规模的 DDoS 攻击

Spamhaus 是一家致力于反垃圾邮件的非盈利组织，总部在伦敦和日内瓦。Spamhaus 维护了一个巨大的垃圾邮件黑名单，这个黑名单被很多大学/研究机构、互联网提供商、军事机构和商业公司广泛使用。

从 2013 年 3 月 18 日起，Spamhaus 开始遭受 DDoS 攻击。攻击者通过僵尸网络和 DNS 反射技术进行攻击，攻击流量从 10G 不断增长，在 3 月 27 日达到惊人的 300G 攻击流量，被认为是互联网史上最大规模的 DDoS 攻击事件。

攻击者使用的主要攻击技术是 DNS 反射技术。从 2012 年开始，DNS 反射技术已经成为大规模第三层 DDoS 攻击的主要部分。DNS 反射攻击技术的基本方式是：向大量开放 DNS 解析器发送带有扩展字段 OPT RR（伪资源记录）的 DNS 查询请求，并将该 DNS 请求的源 IP 地址伪造成想要攻击的目标 IP 地址。开放 DNS 服务器在接收到请求后会对该请求进行解析查询，并将大范围域名查询的响应数据发送给攻击目标。由于请求数据比响应数据小得多，攻击者就可以利用该技术有效地放大其掌握的带宽资源和攻击流量。

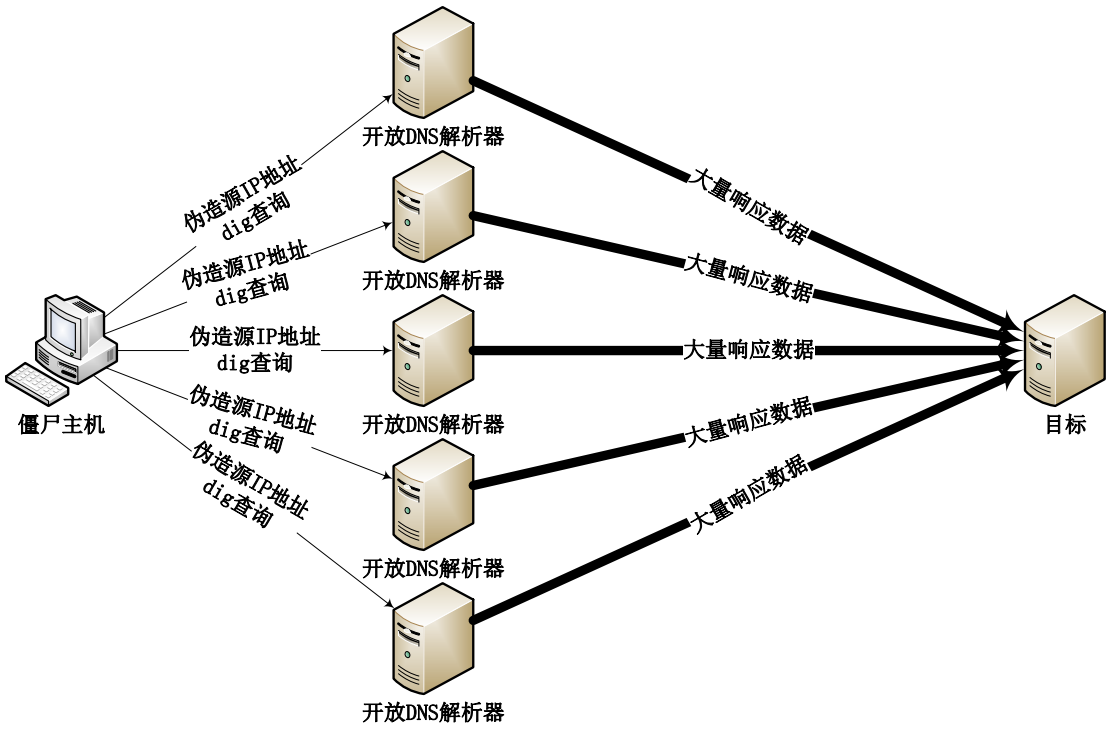


图 8　DNS 反射攻击

在本次事件中，攻击者向三万多个开放 DNS 服务器发送了对 ripe.net 域名的解析请求，并将源 IP 地址伪造成 Spamhaus 的 IP 地址，大量开放 DNS 服务器的响应数据产生了大约 300G 的攻击流量。DNS 请求数据的长度约为 36 字节，而响应数据的长度约为 3000 字节，这意味着利用 DNS 反射能够产生约 100 倍的放大效应，因此，攻击者只需要掌握和控制一个能够产生 3G 流量的僵尸网络，就能够进行这么大规模（300G）的攻击。除了 DNS 反射技术，攻击者还使用了 ACK 反射等其他技术进行攻击。

2013 年 7 月 25 日，互联网系统协会（ISC，Internet Systems Consortium）宣布，为了防御利用 DNS 发起的反射式 DDoS 攻击，最新版的 BIND 软件增加了响应速率限制（RRL，Response Rate Limiting）模块，并声称这会是缓解 DNS 反射攻击的最有效方法。

观点 6：TCP FLOOD 和 HTTP FLOOD 是最主要的 DDoS 攻击方式，两者占总数的四分之三

2013 上半年，我们共发现了 168459 次 DDoS 攻击，增长既来自攻击数量的增加，也由于观测范围的变大。其中 TCP FLOOD 占 38.7%，重新占据排行榜的首位；而 HTTP FLOOD 占总数

的 37.2%，与 2012 年相比下降 5.5%。DNS FLOOD 攻击则占 13.1%，依然是一种重要的攻击形式。这半年中，我们观测到 4.1%的 DDoS 采用了混合攻击的方式，成为一种新的普遍现象，所以我们将其单独列为一类。

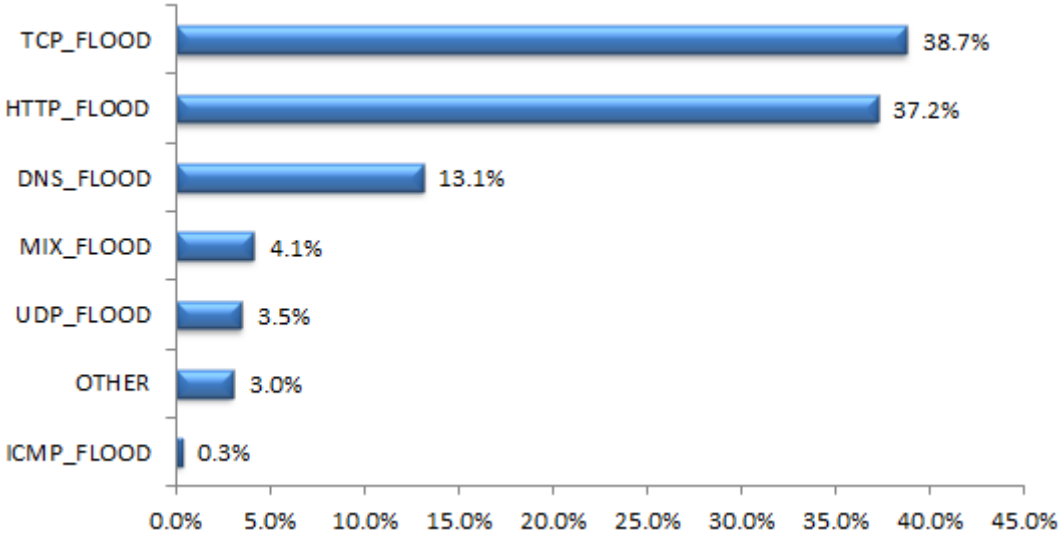


图 9　DDoS 攻击类型

观点 7：九成以上的 DDoS 攻击发生在半小时内，1.5%的攻击会持续一天以上

大部分 DDoS 攻击的持续时间并不长。三十分钟之内的攻击占到了 93.1%，与 2013 年的 93.2%基本持平。一个可能的猜测是攻击者的尝试性攻击在逐步减少。

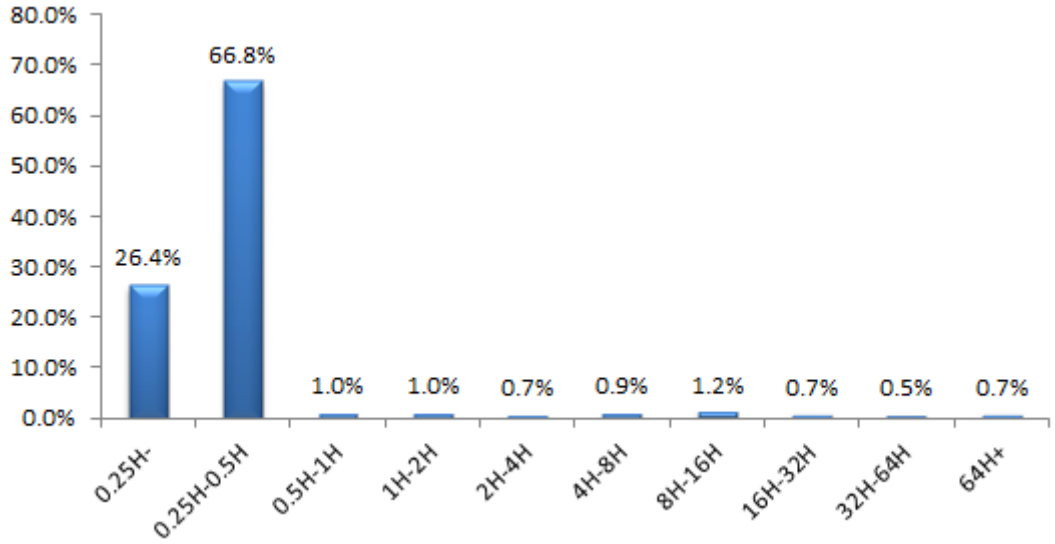


图 10　DDoS 的攻击持续时间

观点 8：峰值流量 50Mbps 以下的攻击占八成，包速率 0.2Mpps 以下的攻击占七成

在监测到的 DDoS 攻击中，流量 50Mbps 以下的占 80.1%，而 2G 以上的攻击只占 0.9%。近年来 HTTP FLOOD 攻击被攻击者大量采用，流量不再与攻击效果成正比，通过消耗应用资源而实现拒绝服务显然更有效率。

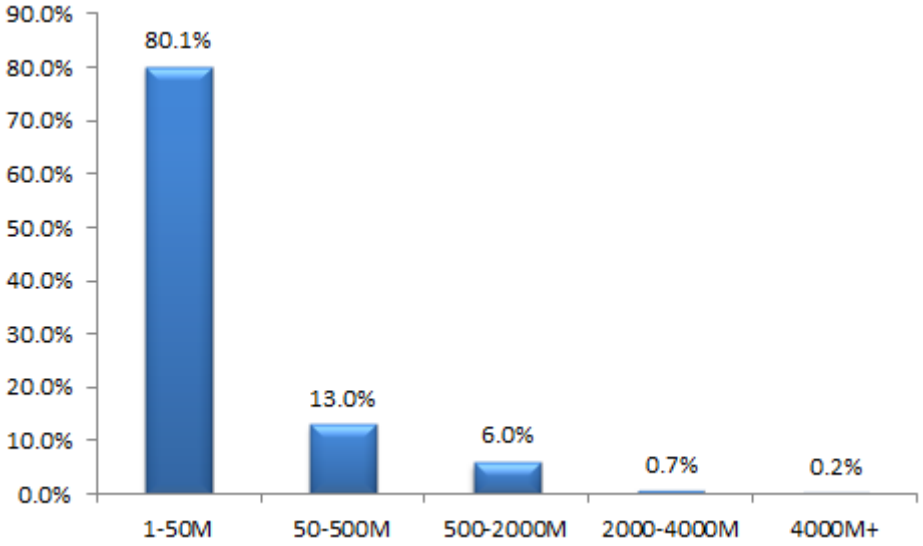


图 11　DDoS 攻击流量分布（bps）

此外，从每秒的峰值包速来看，69.1%攻击在 0.2M 以下。与流量的变化相比，包速率的范围更为集中，仅有 0.2%大于 3.2Mpps。

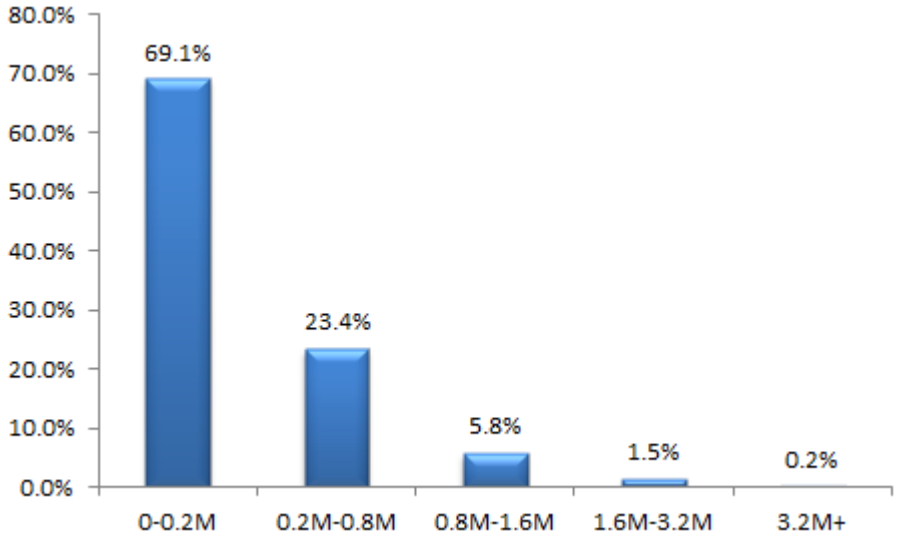


图 12　DDoS 攻击的包速率分布（pps）

观点 9：混合攻击所占比重逐步增加，其中一半是 ICMP+TCP+UDP FLOOD 的组合

2013 上半年绿盟科技监测到的 DDoS 混合攻击共计 6956 次，占攻击总数的 4.1%。对于其中的 6427 次，我们分析了其组成，并按照攻击使用的协议类型进行了分类。在这些混合攻击中，ICMP+TCP+UDP 的方式最为普遍，占总数的 50.6%；其次是前者再加入 DNS 的组合，占 18.5%；使用不同种类的 TCP FLOOD 进行组合攻击（例如 SYN FLOOD 和 ACK FLOOD）的占 9.8%。

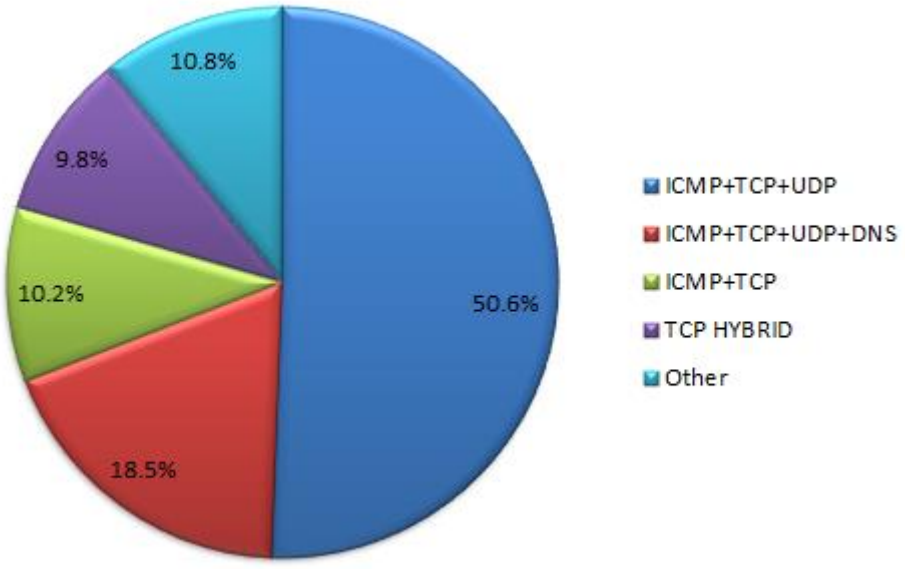


图 13　DDoS 混合攻击

结束语

同一现象，从不同角度看会有不同的理解。除本文中给出的观点之外，我们可以做一些可能合理的猜测。DDoS 攻击的数量在短期内不断起伏，长期来则处于持续增长的状态。媒体关注的事件往往是网络战和黑客行动主义，但更多的普通攻击单纯出于商业竞争或恶意勒索的目的。攻击者渐渐分为两类，一类专注于吸引眼球，一类则专注于赚钱，后者会越来越多地考虑“黑客经济学”的问题。受害者会发现，攻击给他们带来的单位时间损失，正变得越来越大。消耗应用资源的 DDoS，就符合这一目的，所以 HTTP FLOOD 大行其道。但传统的 TCP FLOOD 和 UDP FLOOD 也不会消失，当流量足够大时，任何信息系统都会难以应对。这场战争，您准备好了吗？

作者和贡献者

作者：

鲍旭华，绿盟科技 Email：baoxuhua@nsfocus.com
博士，绿盟科技战略研究部研究员，主要研究领域为信息安全事件分析、安全智能和态势感知。

洪海，绿盟科技 Email：honghai@nsfocus.com
绿盟科技安全研究部研究员，主要进行网络攻防和漏洞相关研究。

贡献者：

刘亚，绿盟科技 Email：liuya@nsfocus.com
曹志华，绿盟科技 Email：caozhihua@nsfocus.com
周志彬，绿盟科技 Email：zhouzhibin@nsfocus.com
王洋，绿盟科技 Email：wangyang2@nsfocus.com

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS