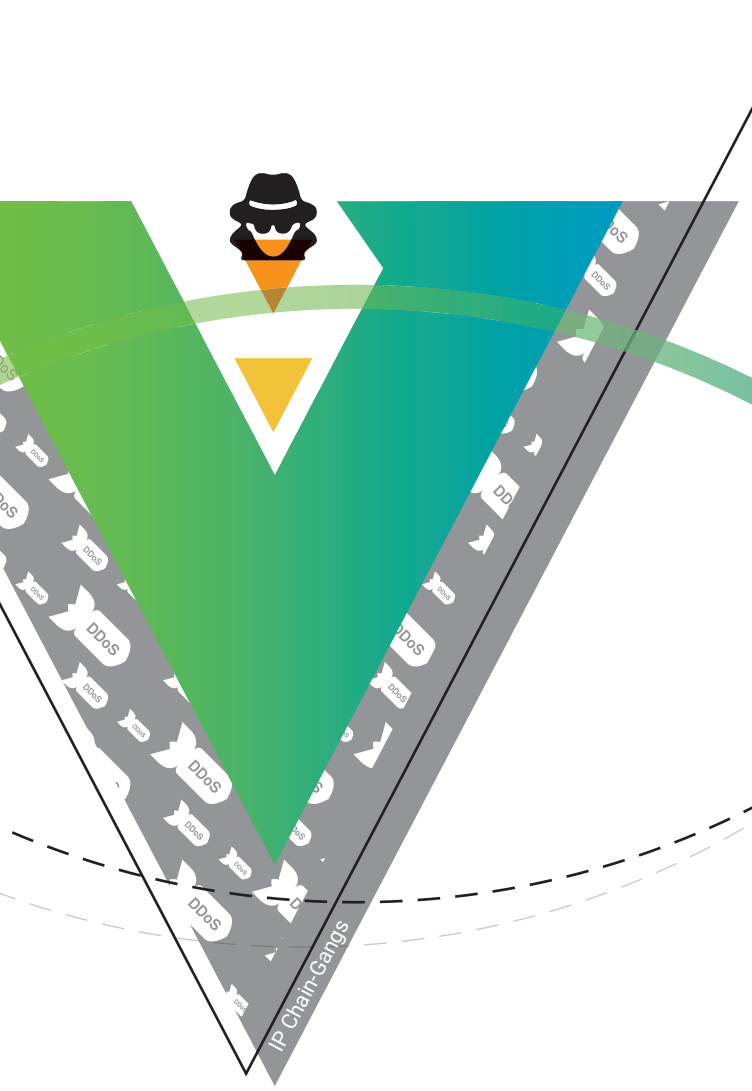


NSFOCUS

IP 团伙行为分析

作者：杨洪波，孙小冰，赵粮

NSFOCUS

2018.12

NSFOCUS

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。

在国内外设有 40 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，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，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安全运营等专业安全服务。

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。

特别声明

本报告分析所采用的数据完全匿名，不包含或泄露任何客户信息。如有任何问题或疑问，欢迎随时与作者联系。

IP 团伙行为分析

NSFOCUS

作者：杨洪波，孙小冰，赵粮

NSFOCUS

2018.12

目录

1 概述与执行摘要

在《绿盟科技 2018 年上半年网络安全观察》 报告中，我们注意到，“惯犯承担了约 40%的攻击事件，其中僵尸网络活动和 DDoS 攻击是惯犯们的主流攻击方式。”由于僵尸网络活动和 DDoS 攻击通常以协作方式从多个来源发起，因此多个惯犯以群体方式勾结“作案”就毫不奇怪了。我们将这样的群体称为“IP 团伙”（IP Chain-Gang）。在本报告中，我们基于绿盟科技自 2017 年以来所搜集的 DDoS 攻击数据，识别了多个 IP 团伙并研究了他们的团伙行为。

采用这种研究方法背后的逻辑是：既然各 IP 团伙均由某一个或一组攻击控制者控制，那么同一个团伙在不同的攻击中必然会表现出相似的行为。我们希望，通过研究团伙的历史行为给该团伙建立一个“团伙画像”，以便更准确地描述其背后的攻击控制者的行为方式、偏好的攻击方法和特征，以便更有效地防御这些团伙未来可能发起的攻击，防患于未然。

在本报告中，我们介绍了 IP 团伙的概念，对团伙行为进行了重点统计分析。根据分析，我们发现：

- 这些团伙成员虽然只占全部攻击者中的一小部分（2%），但却发起了相当大一部分（20%）的攻击；
- 20%的团伙对约 80%的团伙攻击流量负责；
- 反射攻击，特别是大流量攻击，是各团伙最青睐的攻击方法；
- 各团伙通常并未完全发挥其潜力，但是，了解它们的能力极限对于规划防御非常重要。

本报告是 IP 团伙主题系列中的开篇之作。在后续报告中，我们计划研究团伙成员如何进化与联系，以及如何基于此构建更有效的防御措施。

据我们所知，以团伙为单位对 DDoS 攻击进行研究在全球尚属首次。从这一全新角度来研究 DDoS 攻击，可以获得一些独特见解，有助于我们更好地检测、缓解、取证分析甚至预测 DDoS 攻击。

2 识别 IP 团伙

为识别 IP 团伙，我们首先分析了绿盟科技自 2017 年以来所搜集的 DDoS 攻击数据，并按步骤进行了下述操作（有关该团伙识别算法的更多信息，请参阅《检测 IP 团伙：组织有序的战略性僵尸》）：

a. 确定一次协同攻击中的攻击者并将其划归一组。这里，我们将协同攻击定义为针对某一目标在大约同一时间发起的攻击。由于这些攻击者协同工作，因此有理由相信他们被同一个攻击控制者控制。

b. 如果上一步中有两个组重叠或其行为非常“相似”，则将其合并为一个更大的组。重复此合并过程，直到不再存在重叠的组。在此过程中，用到了一套复杂的机器学习算法来确定“相似性”阈值。

c. 去掉组中的“偶然攻击者”（仅参与一小部分攻击的攻击者），提取每个攻击组的核心成员，得出我们所称的“IP 团伙”。

通过这一步骤，我们确定了 80 多个活跃的 IP 团伙。在本研究中，我们在算法中选择了相当严格的参数，因此，这些团伙中的所有成员都是实实在在的惯犯。每个惯犯都在我们的研究期间进行了多次攻击。因此，尽管这些团伙成员的数量仅占我们数据集中所有攻击者的 2%，但它们发起的攻击约占所有攻击的 20%。

应该注意的是，这些 IP 团伙的组成是动态变化的，原因是随着时间的推移，有的成员会离开（可能是因为系统所有者移除了恶意软件并修补了攻击控制者入侵系统所利用的安全漏洞），而同时又会有新成员加入（新系统被恶意软件感染并成为僵尸网络成员）。本报告中，我们将研究期间的团伙行为视为静态。在未来的研究中，我们将考虑动态性质。

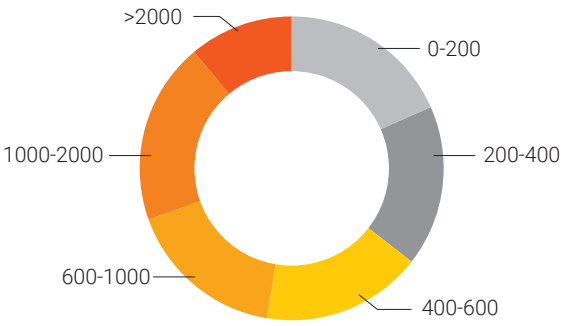
3 IP 团伙统计分析

在确定团伙之后，我们从几个不同的角度研究了各团伙的行为。除非另有说明，本节中提及的数字均为同一团伙中的所有成员的累计计数。

3.1 IP 团伙规模（成员数量）

下图展示了 IP 团伙规模的分布情况。大多数团伙成员数量不到 1000，但我们也发现有一个团伙成员数量超过 26,000。

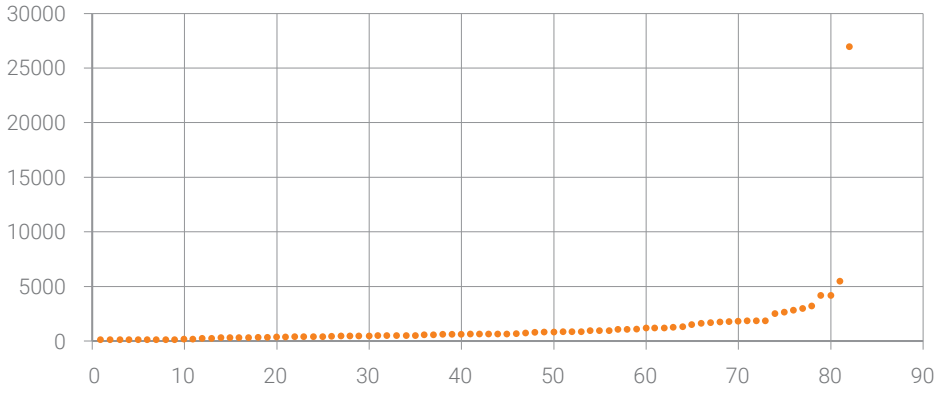
图 1 IP 团伙规模分布



IP团伙成员数量

下图展示了我们所识别的各 IP 团伙按规模大小的分布。图中的每个点代表一个团伙，共有 82 个团伙。

图 2 IP 团伙规模分布（每团伙）

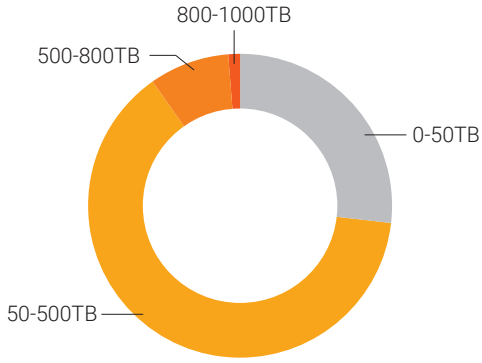


IP团伙成员数量分布

3.2 攻击总流量

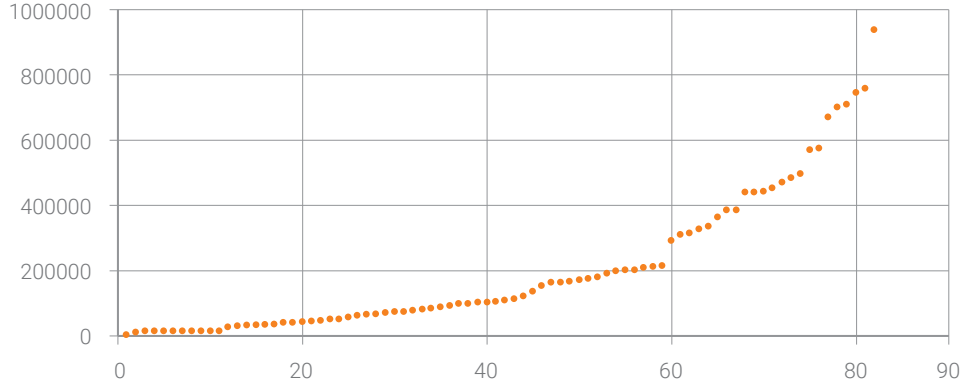
下图展示了各团伙的攻击总流量分布情况，涵盖了来自同一团伙所有成员的全部攻击。虽然不同团伙的攻击总流量看似存在巨大差异，但在我们研究期间，大多数团伙的攻击总流量都超过了 50TB。

图 3 攻击总流量分布



攻击总流量

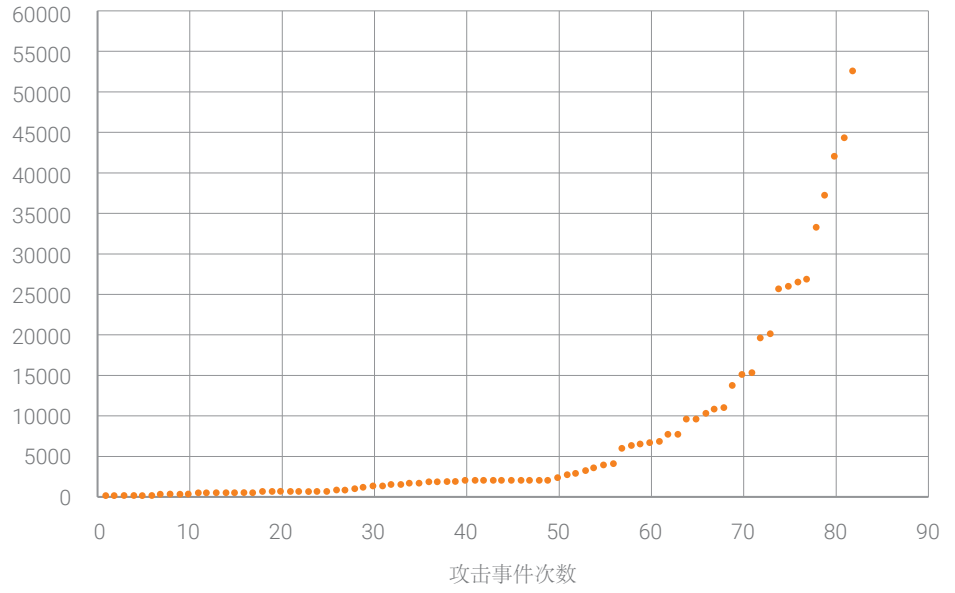
图 4 攻击总流量分布（每团伙）



3.3 攻击总次数

下图展示了各团伙按所发起 DDoS 攻击事件数量的分布。毫不意外，大约 20%的团伙发起了 80%的攻击。

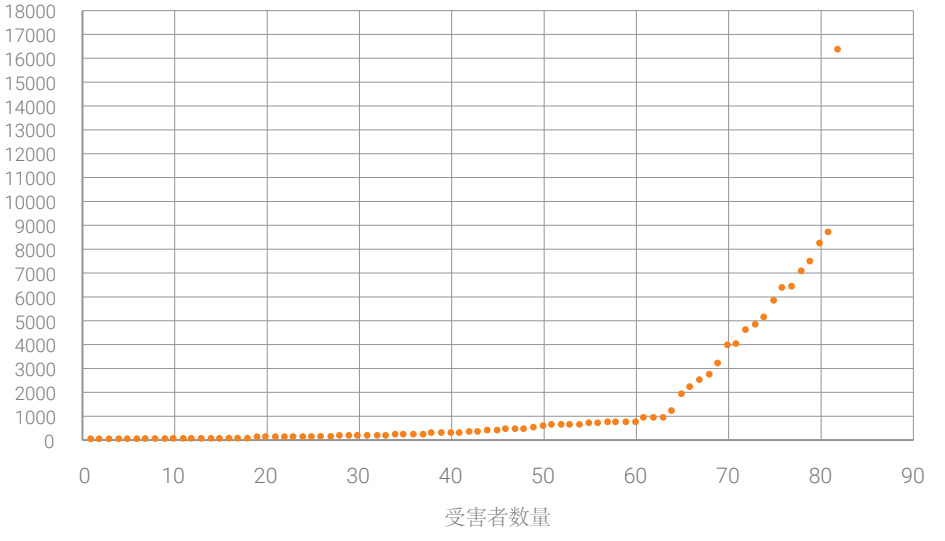
图 5 攻击总次数分布（每团伙）



3.4 团伙受害者数量

下图展示了各团伙按受害者数量的分布。我们看到，80%的团伙受害者不到 1000 个，但有一个团伙攻击了约 15%的目标。

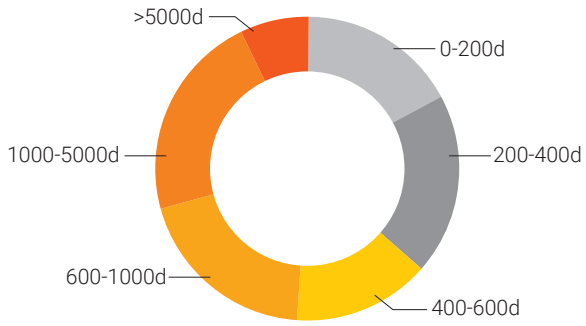
图 6 受害者数量分布（每团伙）



3.5 攻击总时长

下图展示了各团伙所有成员的总攻击时长的分布情况。有些团伙的总攻击时长高达 5000 多天，但多数团伙不到 1000 天。

图 7 总攻击时长



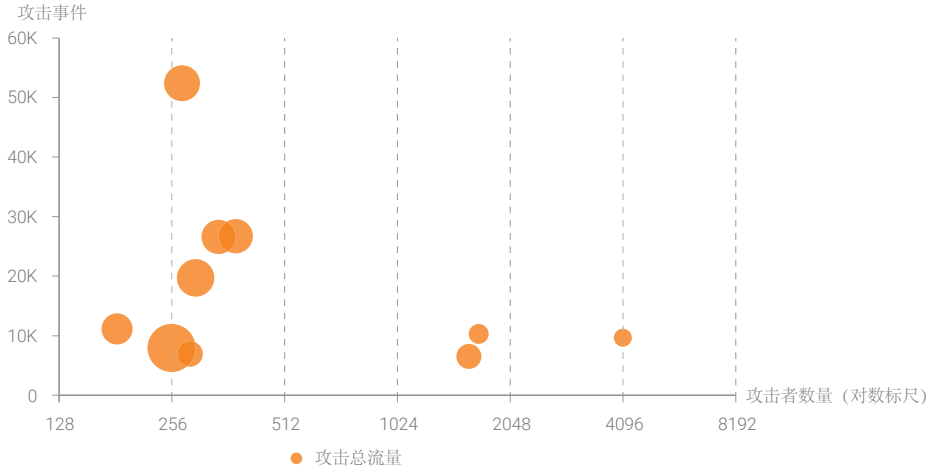
团伙攻击时长

3.6 团伙规模、攻击次数与攻击总流量比较

我们一般总感觉，较大的团伙会发动较多攻击，且产生的攻击总流量也较大，但事实并非如此。如下图所示，与更大规模的 IP 团伙相比，较少成员的团伙可能会发动次数更多、流量更高的攻击。

下图展示了按总攻击流量排名的前 10 个团伙，X 轴为 IP 团伙规模（对数标尺），Y 轴为攻击次数，攻击总流量以不同大小的橙色气泡表示。

图 8 团伙规模、攻击次数及攻击总流量对比



Top 10 IP团伙的攻击事件次数 – 攻击者数量 – 攻击总流量

如上图所示，气泡较大并不一定表示攻击者数量或攻击次数就多。具体来看，某拥有 274 名成员的团伙攻击频率极高（> 50K 次），超过了所有其他团伙。而最大的气泡（即攻击总流量最大）对应的团伙拥有较少成员（256），攻击次数也较少（<10K 次）。这说明，该特定团伙中的攻击者应该有更多带宽资源可以利用。

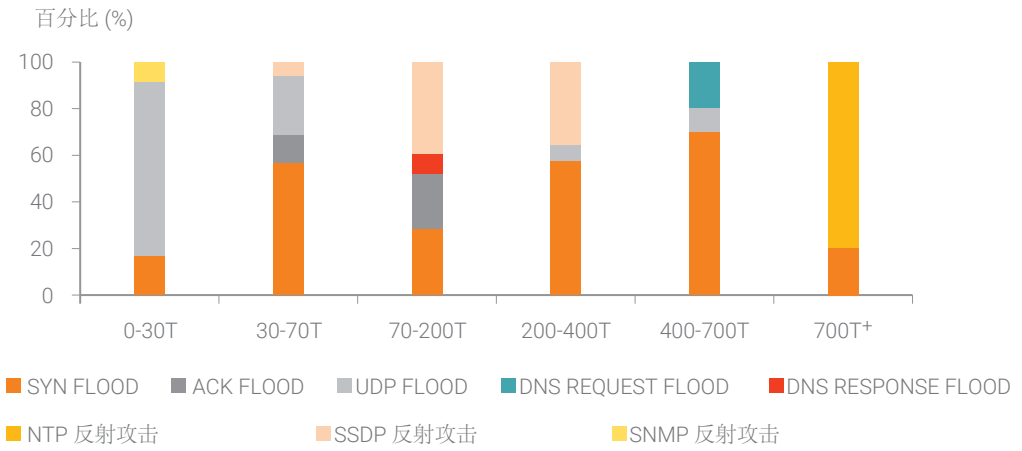
3.7 攻击类型（方法）

在研究 DDoS 攻击时，攻击方法的研究也很重要。不同的方法具有不同的特性，如产生的流量、实现和检测难度、系统依赖等。

3.7.1 攻击类型与攻击总流量

下图按攻击总流量区间展示了各种攻击的分布。

图 9 攻击类型与攻击总流量



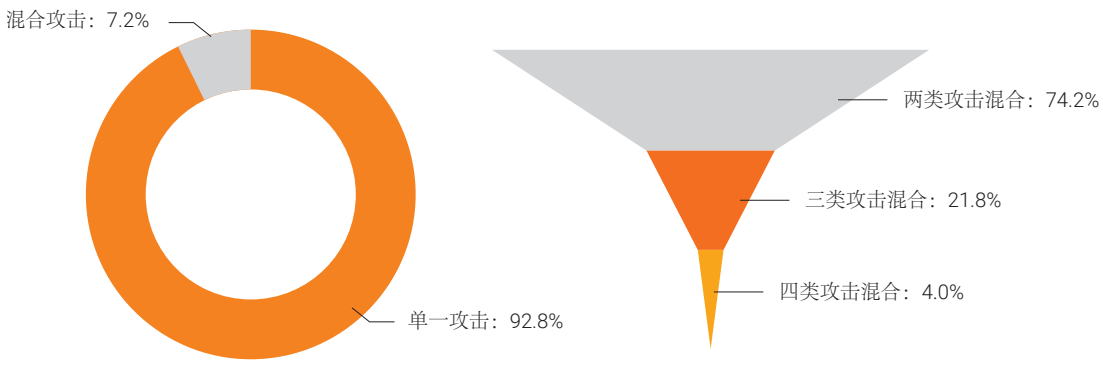
按攻击流量统计的IP团伙攻击类型

由于其出色的放大性能，NTP 反射攻击产生的流量在大流量攻击中占比最大，而 SYN Flood 攻击则最为普遍（很可能由于攻击方法简单）。这两种攻击再加上 UDP Flood 和 SSDP 反射攻击构成了最主要的攻击类型。

3.7.2 单一攻击与混合攻击

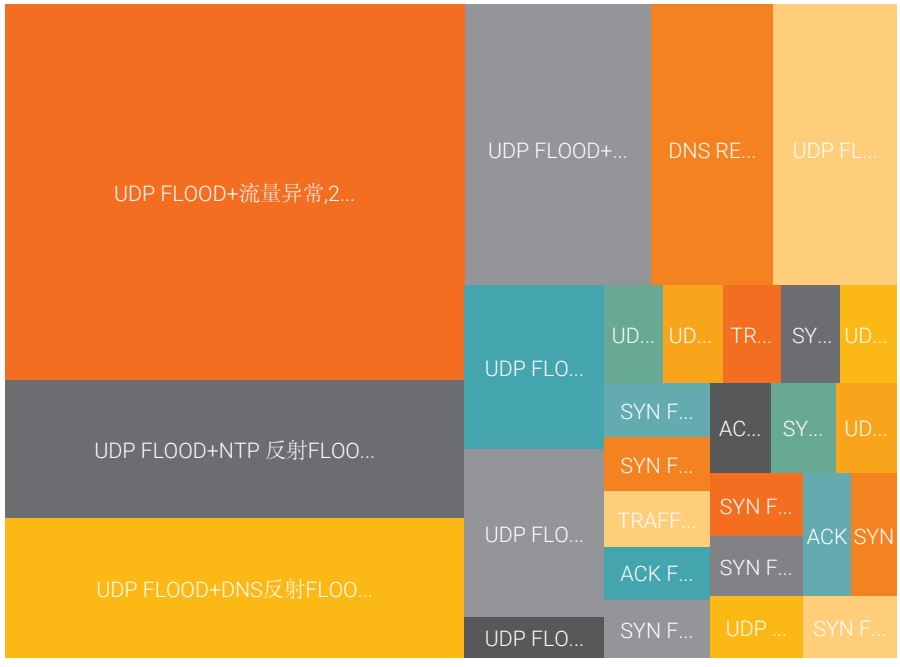
很多攻击团伙都有其青睐的攻击方法，透露出其背后的攻击控制者的技能和偏好。不过，我们观察到有些组织发动攻击时会采取多种攻击方法，有时甚至一起攻击中会涉及多种方法。下面两个图展示了某一团伙采用的攻击方法。

图 10 单一攻击与混合攻击（某一攻击团伙）



单一攻击与混合攻击

图 11 混合攻击中各种攻击方法的组合



混合攻击中各种攻击方法的常见组合

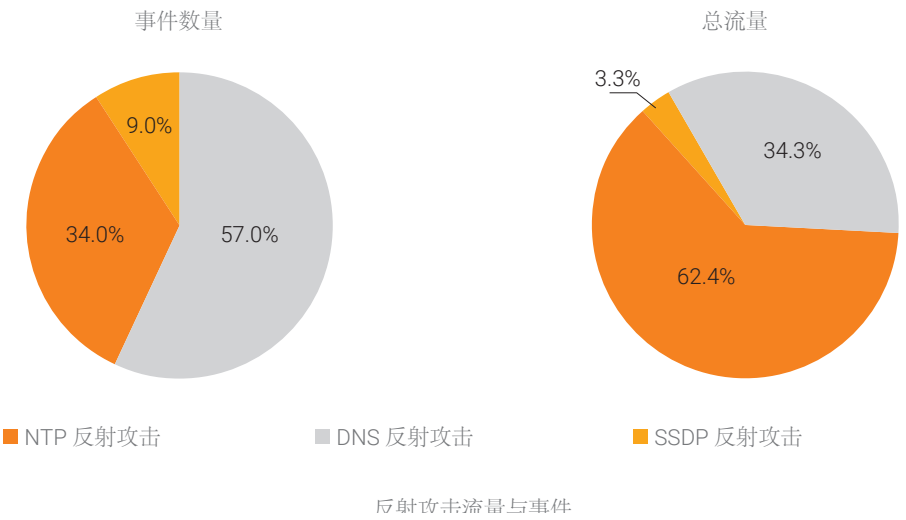
在图 10 中，我们看到该攻击团伙大多时候仅采用一种攻击方法发起攻击（93%），不过有时也会采取多种攻击方法对一个受害者发起协同性攻击。在混合攻击中，75% 的采取了两种攻击方法，4% 的采取了四种方法。

图 11 展示了混合攻击中各种攻击方法的组合。我们发现 UDP flood 攻击方法应用广泛。这不足为奇，因为 UDP flood 攻击是一种存在了很长时间的 DDoS 攻击方法，目前仍非常流行。

3.7.3 反射攻击流量与事件

我们发现各类反射型攻击方法正越来越多地出现在 DDoS 攻击中，尤其是大流量攻击。同时，我们发现有些攻击团伙会结合使用多种反射型攻击方法，如下图所示。

图 12 反射攻击流量与次数分布（某一攻击团伙）



反射攻击流量与事件

从攻击事件数量来看，DNS 反射攻击占比较大，占全部反射型攻击的 57%，其次是 NTP 反射攻击。从攻击流量来看，NTP 反射攻击占据主导地位，贡献了 62.5% 的流量，DNS 紧随其后。从触发较大流量的能力来看，NTP 反射攻击是一种更为强大的 DDoS 攻击。

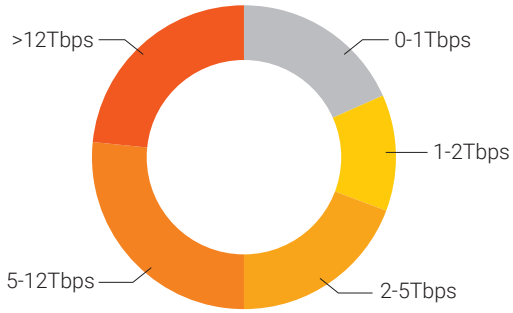
3.8 流量峰值

攻击团伙所产生的攻击流量峰值是我们研究的一个重要方面，因为它反映了攻击团伙对目标的最大攻击能力。在后面几节中，我们会介绍流量峰值的整体分布及随时间变化情况。

3.8.1 流量峰值的整体分布

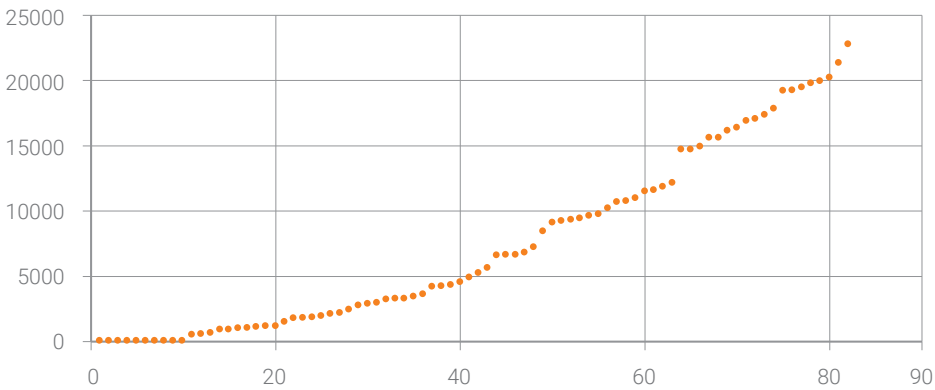
流量峰值（Tbps）是衡量某一团伙的攻击能力和恶意程度的关键参数。大多数 IP 团伙的流量峰值都超过了 2 Tbps。

图 13 IP 团伙的流量峰值分布



IP团伙峰值流量分布

图 14 流量峰值分布（每团伙）

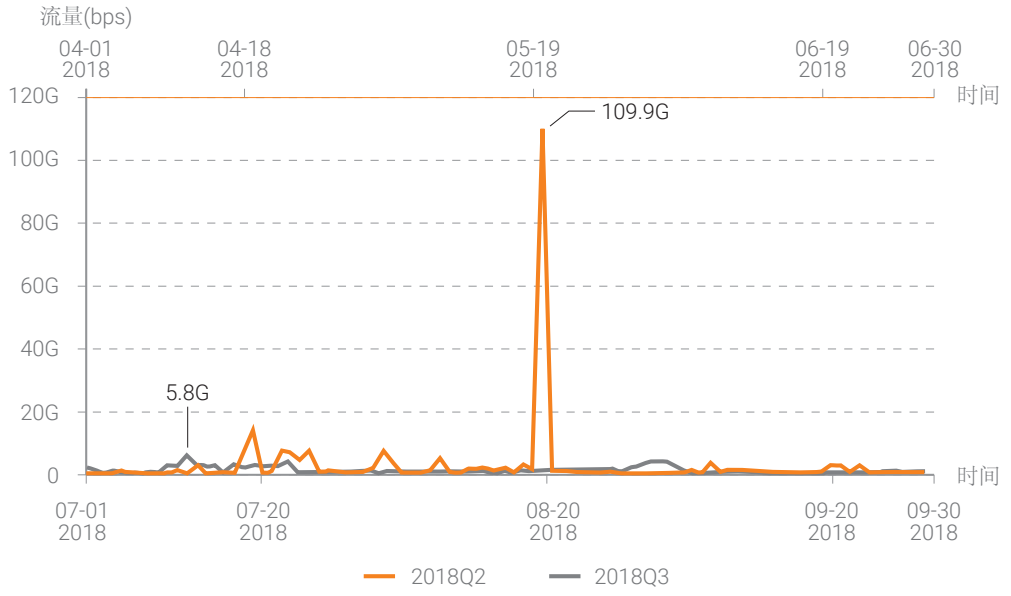


IP团伙的峰值流量分布 (Gbps)

3.8.2 单个团伙的攻击流量峰值

需要注意的是，攻击团伙的攻击流量并非总能达到其最大能力值。事实上，鉴于攻击控制者的业务需求和可用成员，大部分攻击的流量远低于其最大能力值。例如，下图对某个团伙的两个季度的流量峰值进行了对比。

图 15 单一攻击的流量峰值趋势（某一攻击团伙）

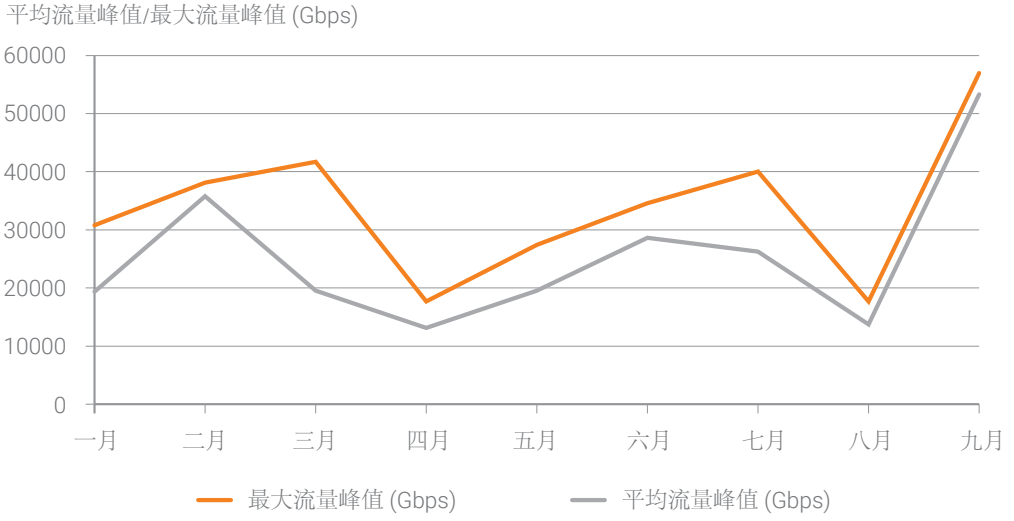


对该攻击团伙来说，攻击在 2018 年 5 月 20 日达到了流量峰值，而在其他月份流量不高。尽管该团伙的流量峰值趋势并不明显，但其最大流量峰值与日常峰值之间存在巨大差别。换句话说，若该团伙用尽浑身解数，会展示出强大的攻击能力。

3.8.3 十大攻击团伙

图 16 展示了 2018 年 1 月至 9 月期间十大攻击团伙的攻击流量峰值。我们将每个团伙的每日的平均 / 最大流量峰值进行累加，得到他们月度的平均 / 最大流量峰值。

图 16 十大攻击团伙的流量峰值



最大流量峰值和平均流量峰值代表了 IP 团伙的最大攻击能力和持续攻击能力。上图展示了 2018 年数月的攻击流量峰值高低起伏变化，反映了这些团伙的攻击活跃程度。

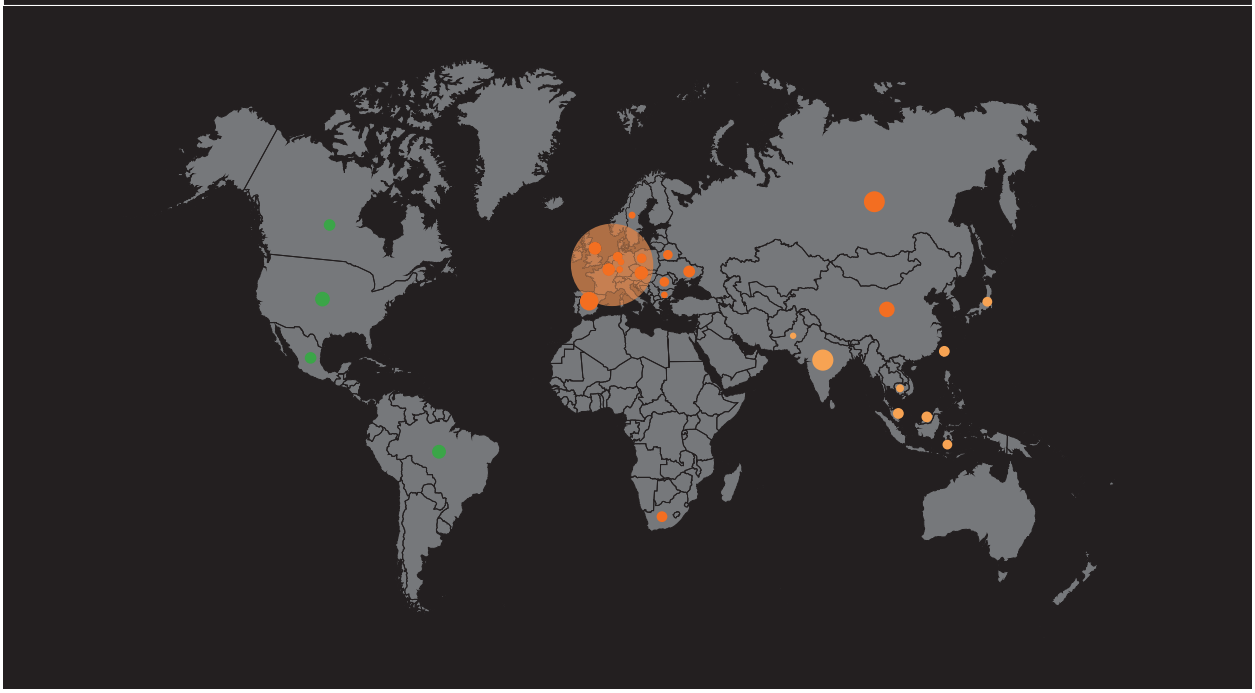
3.9 攻击者和受害者（不包括中国）的地理定位

从攻击者和受害者的地理定位信息能看出攻击发起的活跃地区及有价值的目标在哪。该地理定位信息不一定能暴露攻击控制者的具体位置，但至少可明确 DDoS 活动的热点地区。

由于我们的大部分传感器部署在中国，因此，我们的整体数据涉及的大部分攻击者和受害者均在中国境内。为展示中国以外的攻击活动，我们在本节仅用从部署在国外的传感器收集到的数据，对其中的地理位置进行了研究。

3.9.1 攻击者国家分布

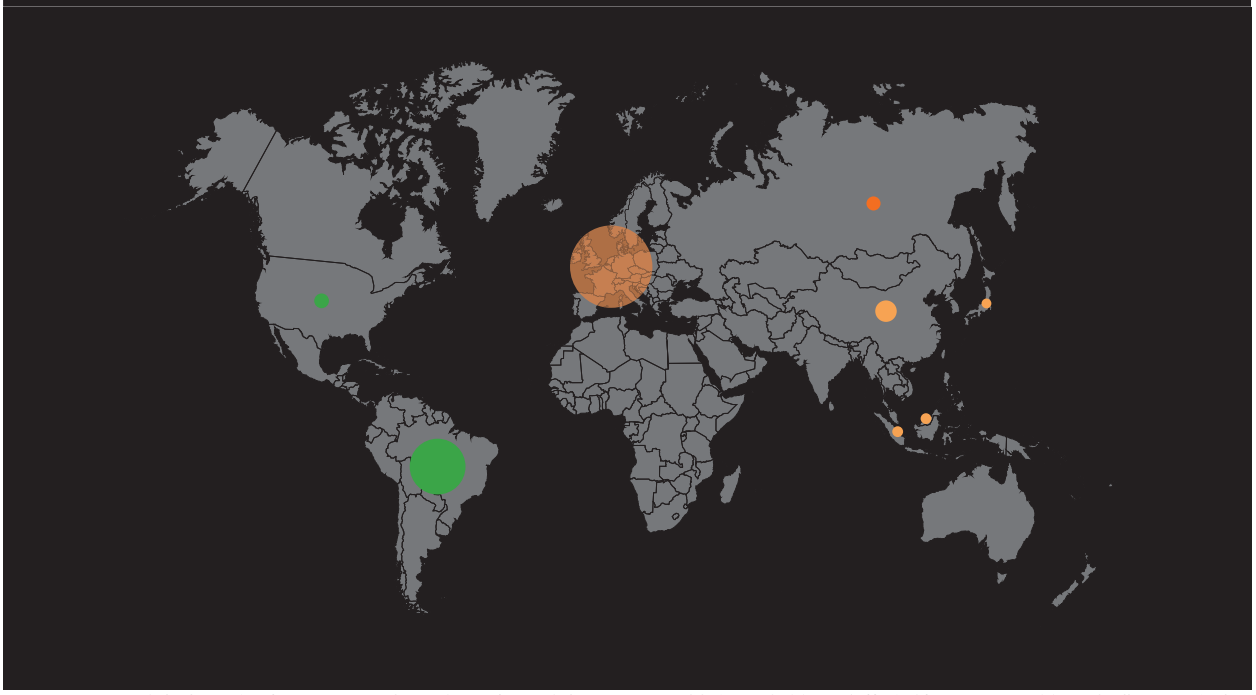
图 17 攻击源国家分布



从攻击者角度看，欧洲拥有最多的攻击源。此外，也有相当数量的攻击者位于亚洲和北美。

3.9.2 受害者国家分布

图 18 受害者国家分布

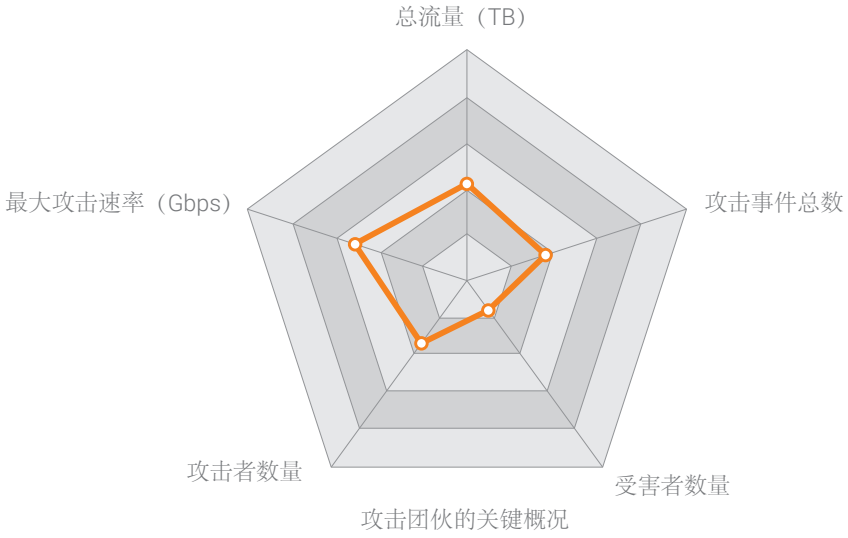


我们从以上受害者分布地图可以看出，欧洲地区受害最严重，其次是南美。除此之外，亚洲和美国也遭到了攻击。

4 IP 团伙画像模型

我们根据上文介绍的五个可量化特性绘制了以下雷达图：雷达图边缘的值为所有团伙的某个特性的最大值。该图的中心表示所有特性的 0 值，轴线上的每一格表示最大值的 20%。接下来，绘制雷达图上某一团伙的相对特性值，然后将各点连接起来就绘成了一幅针对这一团伙的整体概况图。

图 19 IP 团伙画像模型



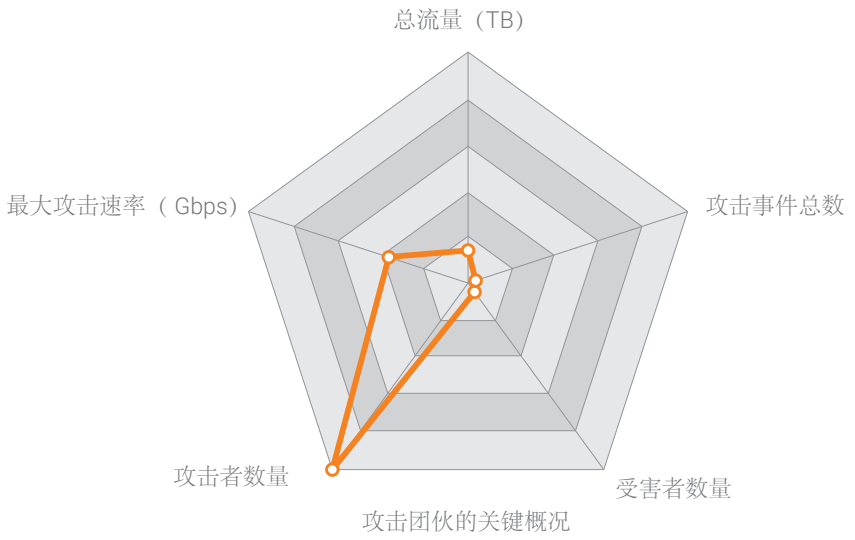
现在，我们可从多个角度分析某一 IP 团伙的不同特性，如攻击流量、事件数量、受害者数量、攻击 IP 数量和最大攻击速率。图 19 中橙色线条绘制的区域越大表示该团伙的攻击越多。这样，我们对这一团伙的攻击能力就有了一个粗略的认识。例如，相对而言，上图描绘的团伙虽涉及少量攻击者和受害者，但却生成了较大攻击流量和峰值。

在后面几节，我们会分析三个攻击团伙，每个团伙在不同特性中达到了最高值。

4.1 最大的攻击团伙

下图展示了我们发现的最大攻击团伙的画像图。从图中我们可以看出，该团伙的受害者和攻击次数均不多，但是其攻击峰值却较高，这可能是由于该团伙的成员基数庞大。

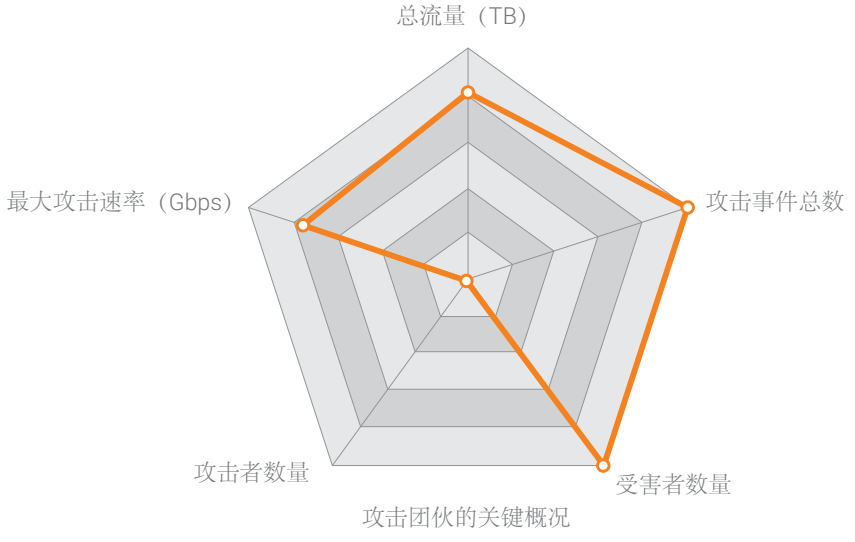
图 20 IP 团伙概要模型（最大团伙）



4.2 最活跃的攻击团伙

下图展示了攻击次数最多且受害者最多的攻击团伙。事实上，该团伙规模不大，但却能产生很大的攻击流量和流量峰值。可见，该团伙攻击性很强。

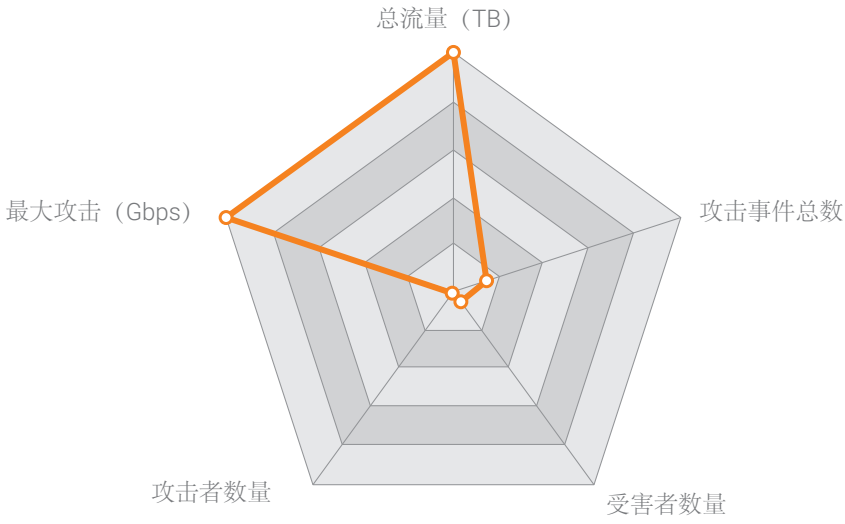
图 21 IP 团伙概要模型（最活跃的攻击团伙）



4.3 流量最大的攻击团伙

下图展示了攻击流量最大且流量峰值最高的攻击团伙。不过，该攻击团伙的规模相对较小，受害者和攻击次数也较少。我们推断该团伙的成员应该具备较大带宽的攻击管道。

图 22 IP 团伙概要模型（流量最大的团伙）



5 未来工作规划

在本文中，我们基于 IP 团伙概念从全新角度分析了网络攻击活动，旨在阐述攻击控制者掌控的攻击团伙是如何以协调一致方式来运作和发起攻击的。同时，我们展示了团伙画像模型，对这些攻击团伙进行分析和对比。

在后续工作中，我们计划追踪 IP 团伙的历史演进，分析其成员的内在联系，以便有助于预测这些团伙发起的攻击，并构建稳固有效的防御方法。

6 参考资料及致谢

6.1 参考资料

1. 绿盟科技 2018 年上半年网络安全观察，绿盟科技安全实验室， https://nsfocusglobal.com/2018-h1-cybersecurity-insights//
2. 检测 IP 团伙： 组织有序的战略性僵尸，赵天跃，邱晓峰（音译）， https://www.researchgate.net/publication/326162077_Detection_of_IP_Gangs_Strategically_Organized_Bots

6.2 致谢

以下同事在我们准备和分析数据以及编写和审校本文时给予了宝贵支持与帮助，在此表示由衷感谢：徐琳、薛梅、蔡铧宇、王渊、盖·罗斯费尔特（Guy Rosefelt）和张玲玲。

如有任何问题和意见，请联系 Xiaobing.sun@nsfocusglobal.com。

NSFOCUS

巨人背后的安全专家

www.nsfocusglobal.com