2018 年网站攻击态势及“攻击团伙”挖掘分析报告

国家计算机网络应急技术处理协调中心

2019 年 3 月

前言

国家互联网应急中心（以下简称 CNCERT/CC）持续对网站攻击进行抽样监测分析。在获取网站服务器权限后，攻击者往往会留有网站后门（webshell），用于持续保持对被攻击网站的权限。也就是说，网站后门的植入、连接操作往往说明攻击者具有长期控制服务器权限的可能性，尤为值得关注。**CNCERT/CC 尝试从攻击源和被攻击端的角度对网站后门连接进行各维度的态势统计分析，进而观察网站攻击的总体态势，并对其中可能存在的“攻击团伙”进行挖掘和刻画，进而以“攻击团伙”的全新视角来观察网站攻击中一些值得关注的有紧密联系的攻击资源集合。**

本报告中的“攻击团伙”指的是通过相对独占的网络资源（例如攻击 IP、代理 IP、特定攻击工具等），针对相同的目标进行长期或者规模化攻击的网络资源集合。在网站后门攻击事件中，考虑到网站后门的相对独占性，则可以认为是通过攻击 IP 以及网站后门的连接紧密程度（例如连接关系、连接频繁度等），挖掘而出的攻击 IP 及其掌握的网站后门链接的集合。通过对挖掘而出的重要团伙进行深入分析，CNCERT/CC 发现，这些值得关注的团伙往往由带有一定目的的个人、组织，掌握和使用，通过网站后门持续保持对网站服务器的权限，实现数据窃取、黑帽 SEO、网页篡改等可能的黑色产业意图。后续 CNCERT/CC 将对观测到的部分典型网站攻击团伙进行细致跟踪分析并对外进行陆续发布。

详细分析情况请见报告正文。

一、2018 年网站攻击统计态势

据 CNCERT/CC 抽样监测，2018 年各月抽样监测发现的网站后门链接个数分布情况如下图所示。可以发现，**2018 年 3-8 月期间，监测到的网站攻击活动较为活跃。**

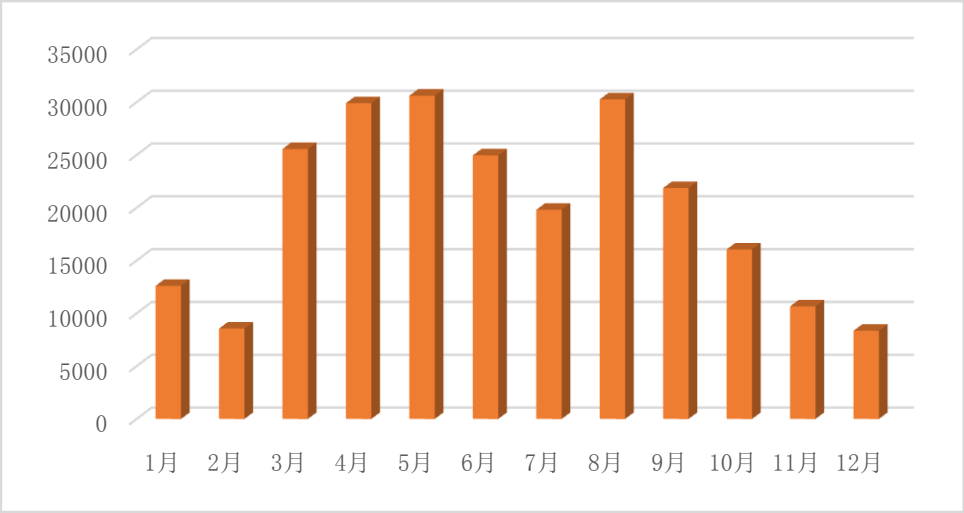

图 1.1 2018 年各月监测发现的网站后门链接个数

2018 年抽样监测到的网站后门脚本类型分布如下图所示，其中 **PHP 类型的网站后门数量最多**，占 66.7%；其次是 ASP 和 JSP 脚本类型的网站后门，分别占 24.2%、7.3%。

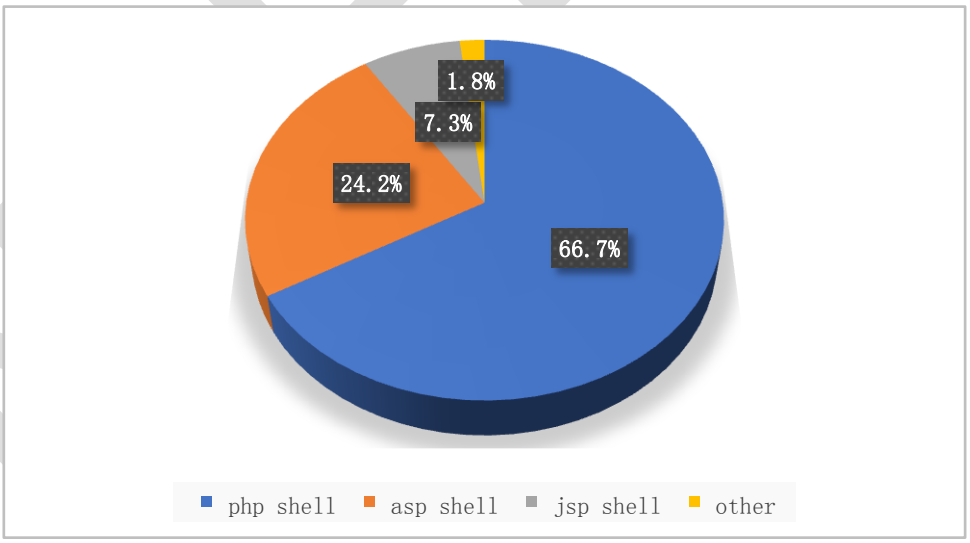

图 1.2 2018 年监测发现的网站后门按攻击脚本类型分布

网站后门全年统计态势如下图所示。可以看出，每月发起网站后门攻击的 IP 与受到网站后门攻击的服务器数量基本相近。每月监测发现的网站后门数量与受攻击域名数量基本与

攻击 IP 数/受攻击 IP 数呈正相关，且具有受攻击域名数量远小于网站后门数量的特点，**说明网站攻击者倾向于对同一个域名植入多个后门，用于保证持续获取网站权限。**

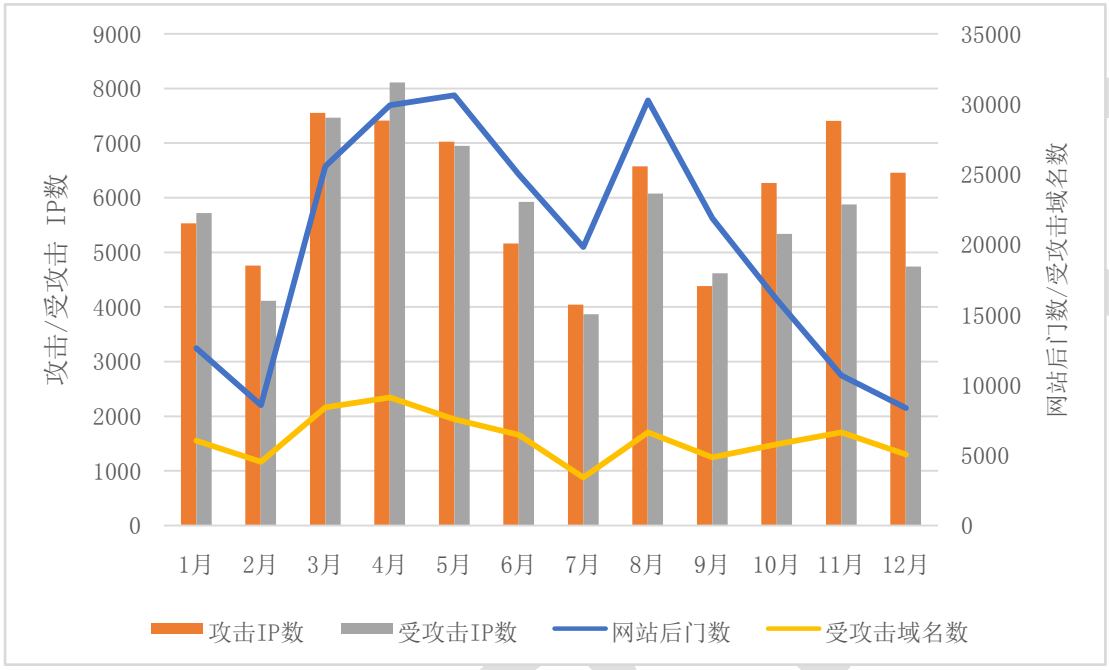

图 1.3 2018 年各月的网站攻击态势

1.1 攻击源分析

根据 CNCERT/CC 2018 年全年抽样监测，2018 年发起网站后门攻击的 IP 约有 5 万多个。分别统计各个攻击 IP 发起攻击的天数（详见下图）可知，94.5%的攻击 IP 活跃天数在 1-7 天内，**5.5%的攻击 IP 发起攻击的天数在 100 天及以上。这些活跃天数较长的惯犯攻击资源值得高度关注。**

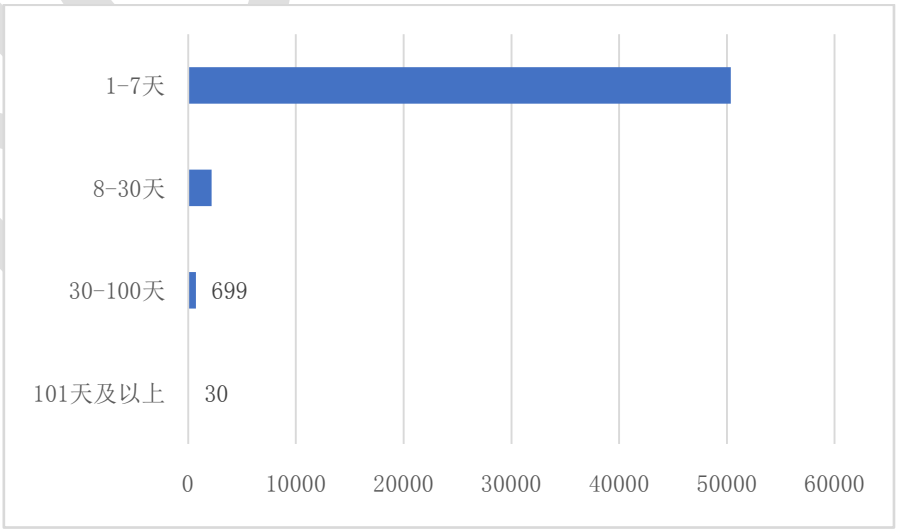

图 1.4 2018 年抽样监测发现攻击 IP 发起攻击天数分布

IP 归属地为境外的 2.7 万个攻击 IP 分别属于 133 个不同的国家/地区，拥有攻击 IP 数量最多的国家 Top 25 如下图所示。可知，**攻击 IP 中美国 IP 占比最多，约占所有境外攻击 IP 的 23.0%**；其次是中国香港、俄罗斯、尼日利亚、摩洛哥等境外国家和地区。

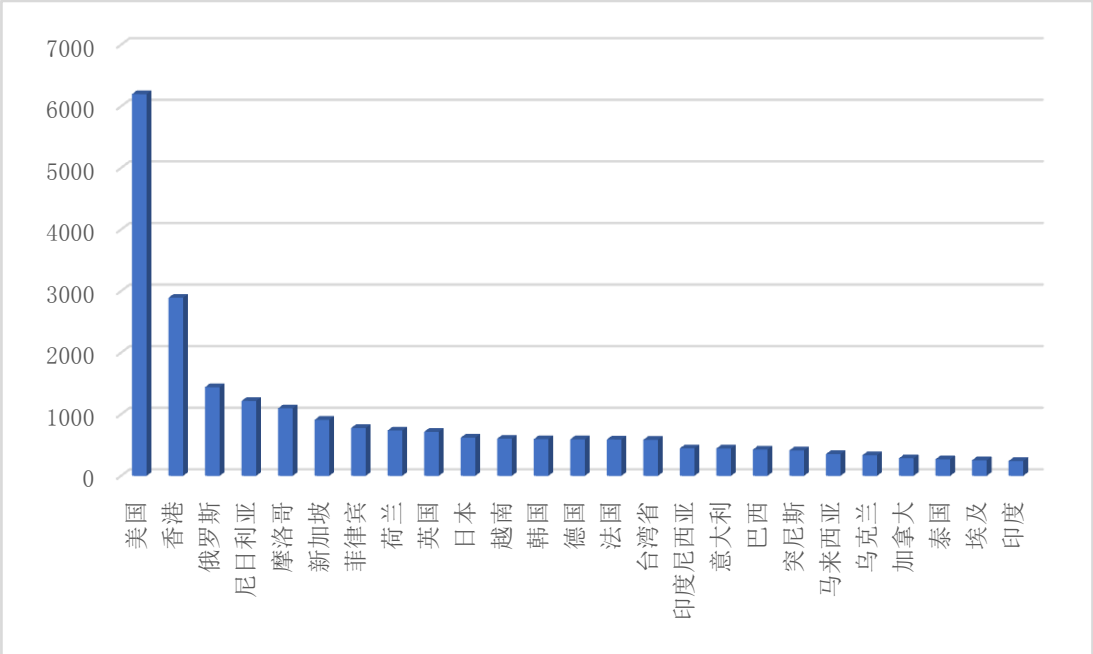

图 1.5　发起网站攻击的境外国家/地区的攻击 IP 个数（TOP 25）

根据 2018 年发起网站攻击的部分境外国家地区的攻击 IP 数量及其植入掌握的网站后门数量关系可知，大部分国家/地区均倾向于通过少量攻击资源发起大量攻击（即攻击 IP 数远小于其植入掌握的网站后门数），俄罗斯和尼日利亚例外。此外，美国和中国香港的攻击 IP 数和掌握的网站后门数量均远高于其他国家/地区。

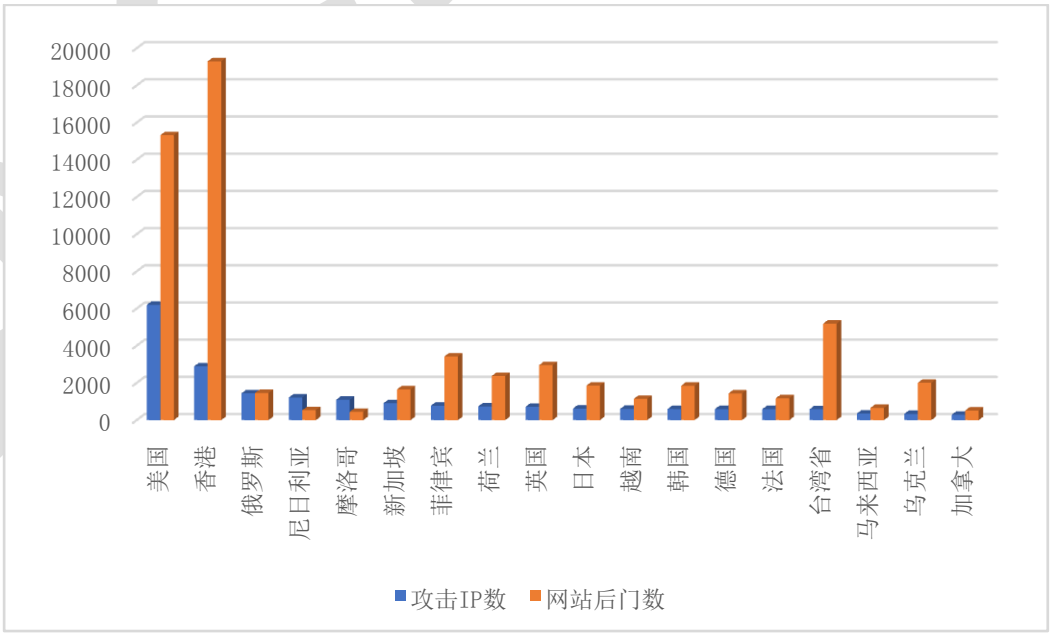

图 1.6　发起网站后门攻击的部分境外国家/地区的攻击 IP 数与网站后门数

1.2 被攻击端分析

根据 CNCERT/CC 抽样监测显示，2018 年受到网站后门攻击的服务器 IP 共有 4.5 万个，涉及的被攻击服务器端口约有 750 个。被攻击服务器端口按涉及网站后门个数的分布如下图所示。其中 80 端口的服务器被植入的网站后门个数最多，约占全年总网站后门个数的 94.6%；其次是 8080 端口，约占 1.4%。

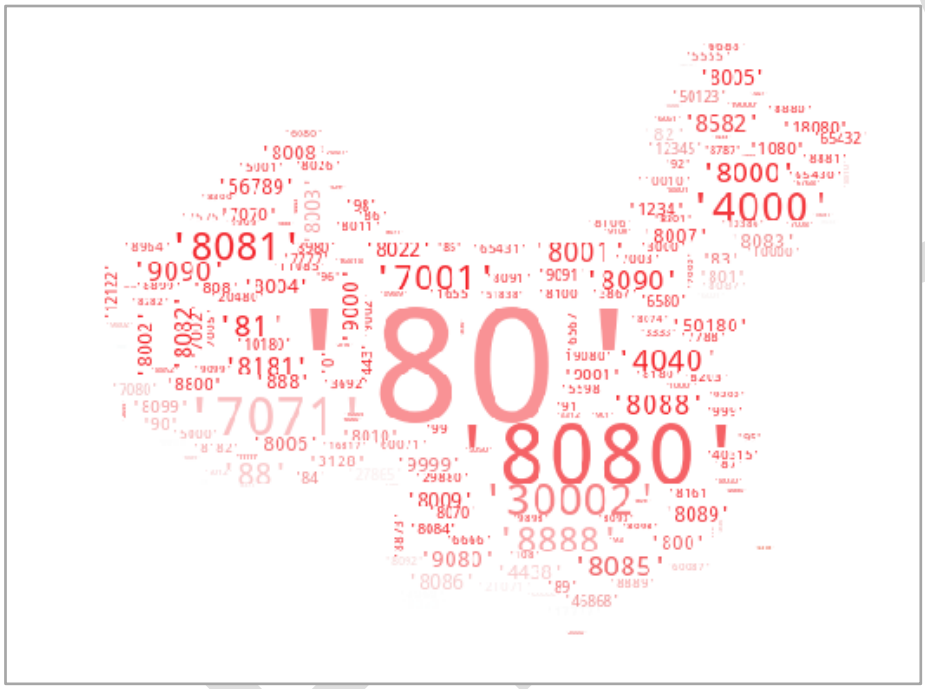

图 1.7 被攻击服务器端口按涉及网站后门个数分布

归属地在境内的被攻击服务器 IP 在我国的 31 个省市均有分布，按照省份统计受攻击 IP 数量，北京占比例最大，约 20.3%，其次是广东、浙江、山东等地区。

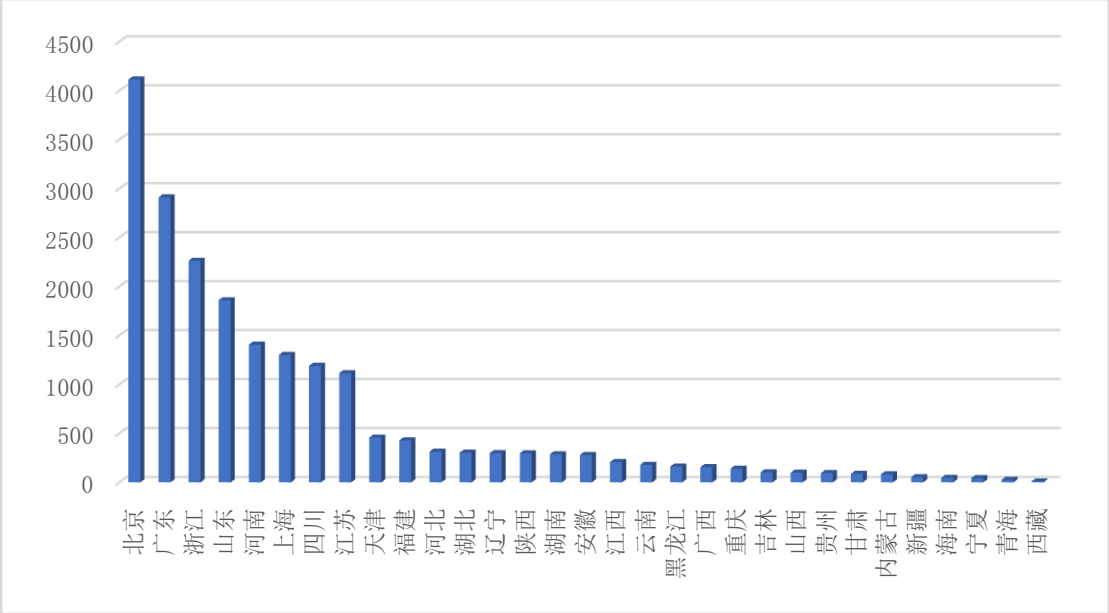

图 1.8 境内受到网站攻击的服务器 IP 数量按省份分布

二、2018 年挖掘发现的网站“攻击团伙”全年态势

CNCERT/CC 从全年观测视角发现，攻击活跃在 10 天以上的网站“攻击团伙”有 777 个，全年活跃的“攻击团伙”13 个，“攻击团伙”中使用过的攻击 IP 大于 100 的有 22 个，攻击网站数量超过 100 的“攻击团伙”有 61 个。

2.1 全年各月活跃的团伙数量分布

通过分析发现，**2018 年全年各月的活跃团伙数量最低位在年初（1 月与 2 月）和年底（12 月）；**上半年在 4 月份达到顶峰，当月活跃团伙数量达到 1049 个，在全年总团伙数量中占比 26%；下半年在 8 月份达到顶峰，当月活跃团伙数量达到 1083 个，在全年总团伙数量中占比 27%。

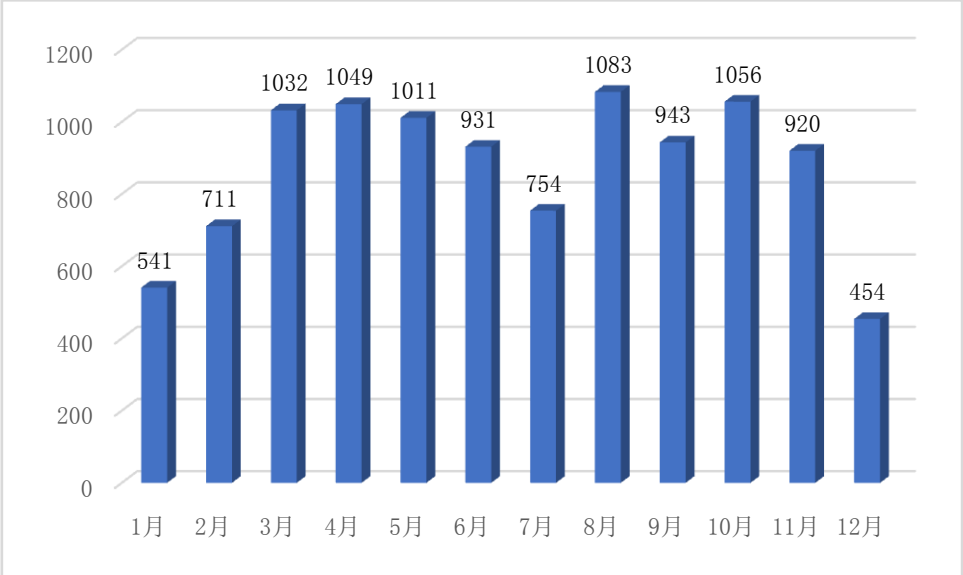

图 2.1 各月活跃团伙数量

在全年的团伙态势中，每月的活跃团伙数量和该团伙使用过的攻击 IP/掌握的网站后门/攻的击域名/攻击的服务器 IP 个数均呈现正相关性。

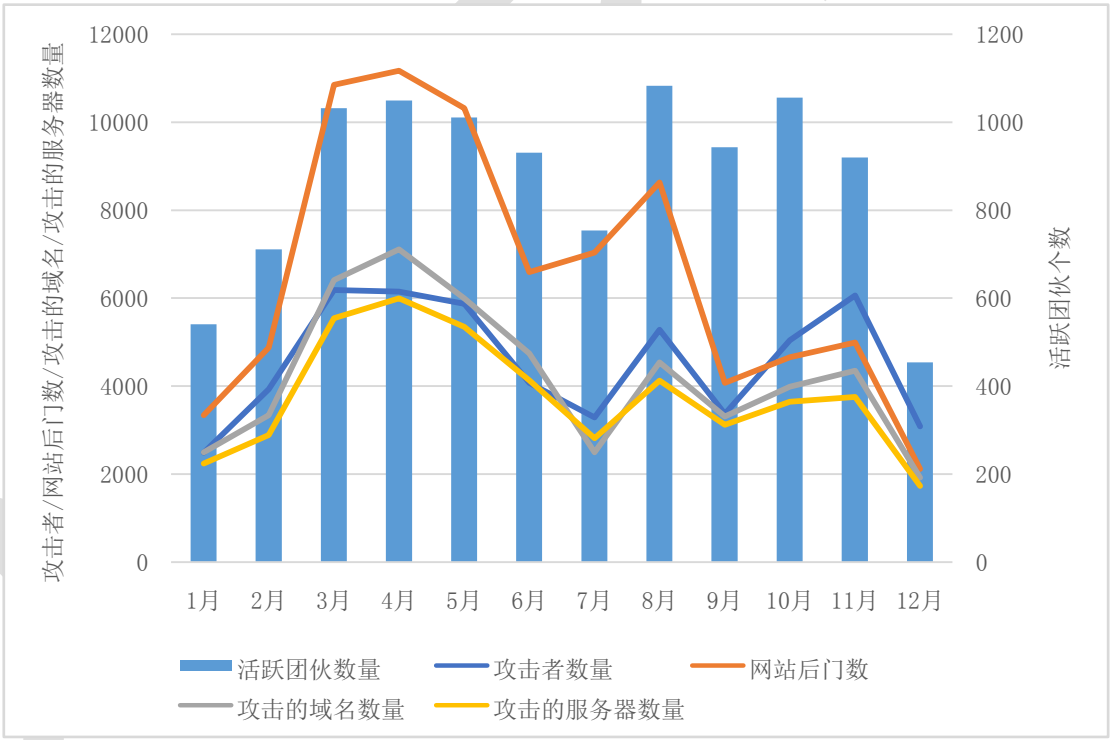

图 2.2 每月团伙的攻击资源及攻击目标的分布情况

2.2 活跃不同时间的团伙数量分布

从团伙的攻击活跃天数来看，团伙数量符合幂律分布。多数团伙的活跃天数较短，无法形成对被入侵网站服务器的持久化控制；**少量值得关注的团伙具有长时间持续攻击的特点，持续对其入侵的多个网站服务器实现长期控制。**

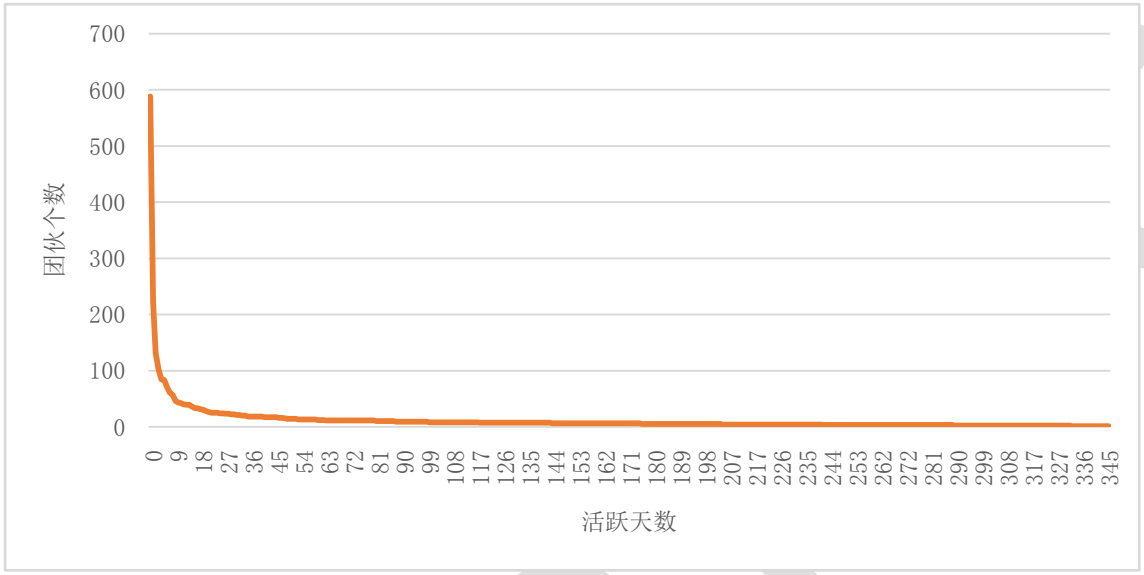

图 2.3 团伙个数按活跃天数分布

其中，活跃天数小于 10 天的团伙有 3227 个，占比 80.6%；**活跃天数在 10-100 天的攻击团伙 732 个，占比 18.3%；活跃天数大于 100 的团伙共有 45 个，占比 1%。**具体如下图所示：

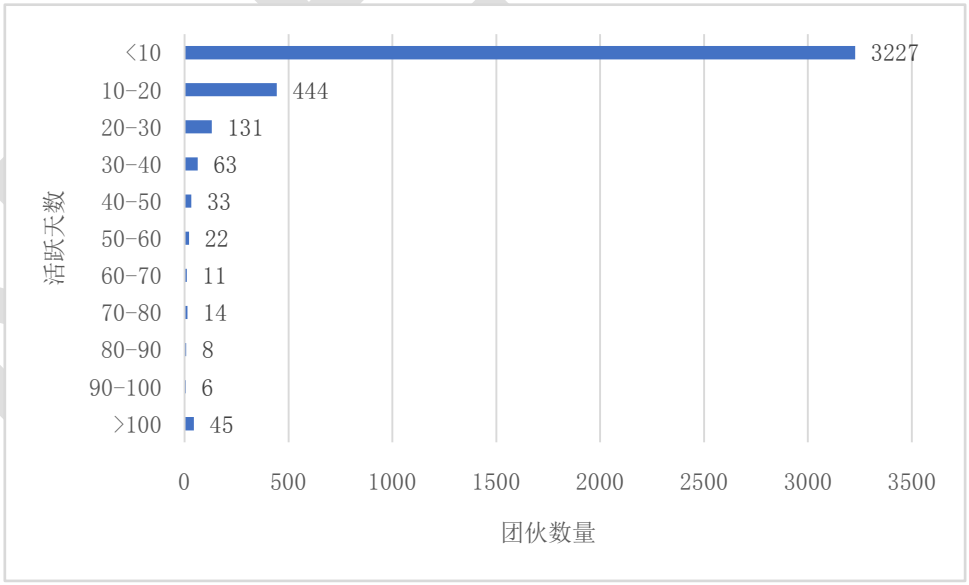

图 2.4 不同活跃天数的团伙数量

2.3 掌握不同攻击资源规模的团伙数量分布

大部分攻击团伙使用过的攻击资源（攻击 IP）较少，这些团伙或者攻击资源可能属于偶发性攻击，对网络空间的影响较少，而占用攻击资源较多的少部分攻击团伙则值得高度关注。

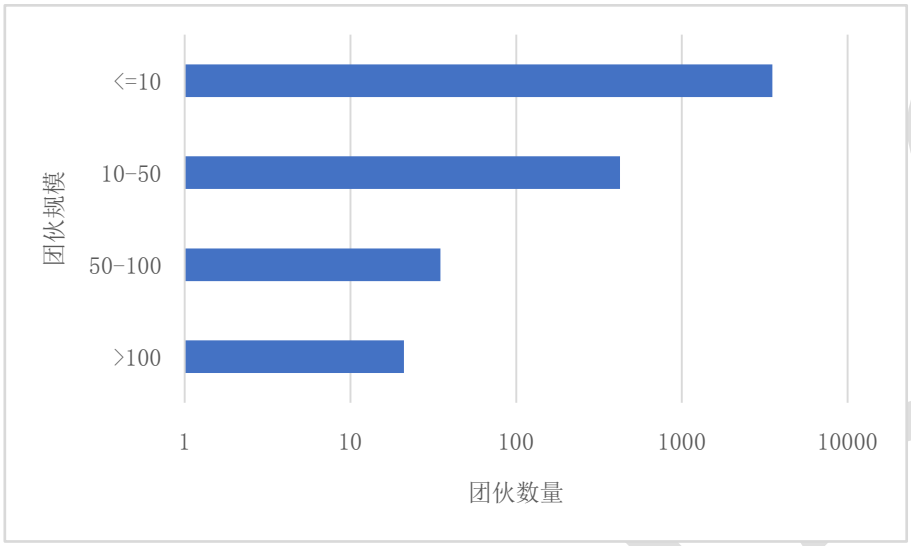

图 2.5 不同团伙规模下的团伙数量

2.4 进行不同操作的攻击团伙数量分布

在植入后门并对网站进行控制时，“获取目录树”和“读文件”几乎是必然使用到的操作，所以进行过此操作的团伙数量最多。排名第三的“删除文件或目录”多用来隐藏攻击者的入侵痕迹，排名第四的“命令执行”多用来对服务器进行进一步的提权，从此也可以窥见网站攻击者的常见攻击及隐藏手法。

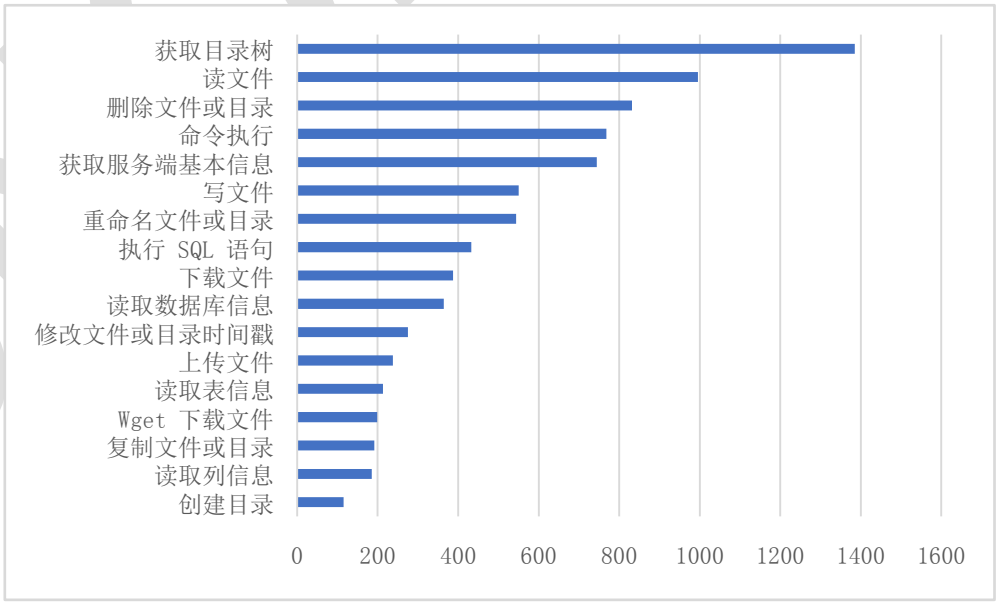

图 2.6 攻击团伙数量按进行过网站后门操作类型分布

2.5 攻击不同服务器数量的团伙数量分布

下图是攻击不同服务器数量的团伙数量分布，可以看出，大量团伙攻击的服务器数量较少（<=5），但也存在少量值得关注的团伙对大量服务器（>100）进行远程控制。

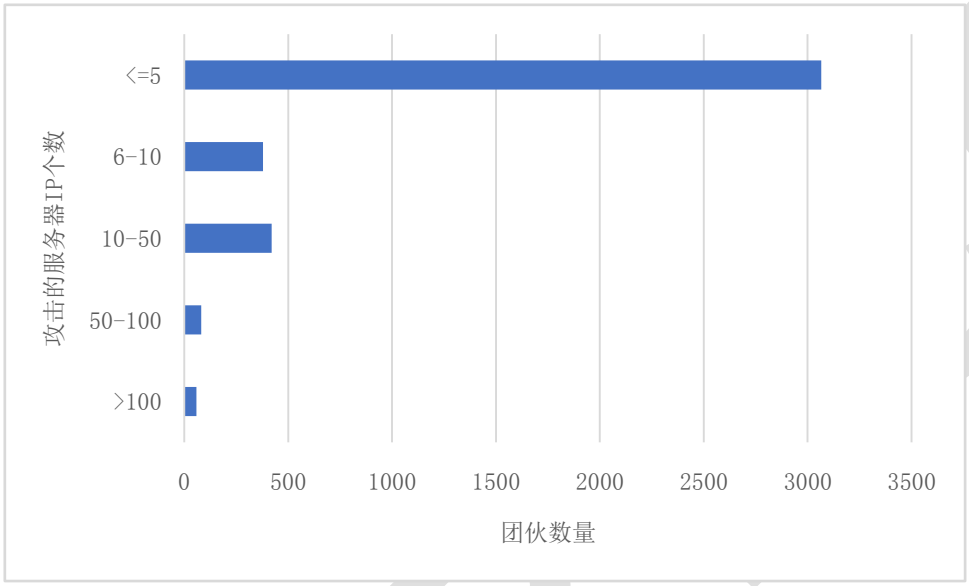

图 2.7 攻击不同服务器 IP 个数的团伙数量分布

下图是掌握不同网站后门个数的团伙数量分布，可以看出与上图的规律类似，大量团伙掌握的网站后门个数较少，部分值得高度关注的团伙掌握的网站后门数量较多。

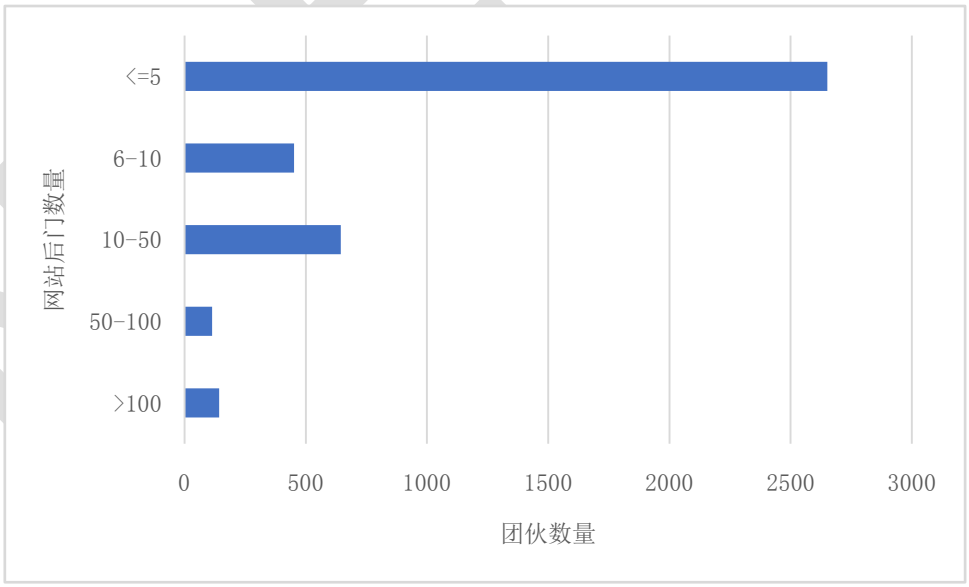

图 2.8 掌握不同网站后门个数的团伙数量分布

三、典型“攻击团伙”概览

在挖掘出各个“攻击团伙”之后，结合对“团伙”行为的监测和跟踪，可对各个团伙的攻击资源、手法、特点进行刻画分析。以下 CNCERT/CC 从不同维度挑选了三个典型团伙展开简单概述，**更加细致的跟踪分析将在后续陆续对外发布。**

在此之前 CNCERT/CC 从攻击资源以及被攻击目标的角度对攻击团伙进行了排名，具体如以下二图所示。根据两幅团伙攻击特点概要图可知，不同团伙的攻击特点具有较大差异。

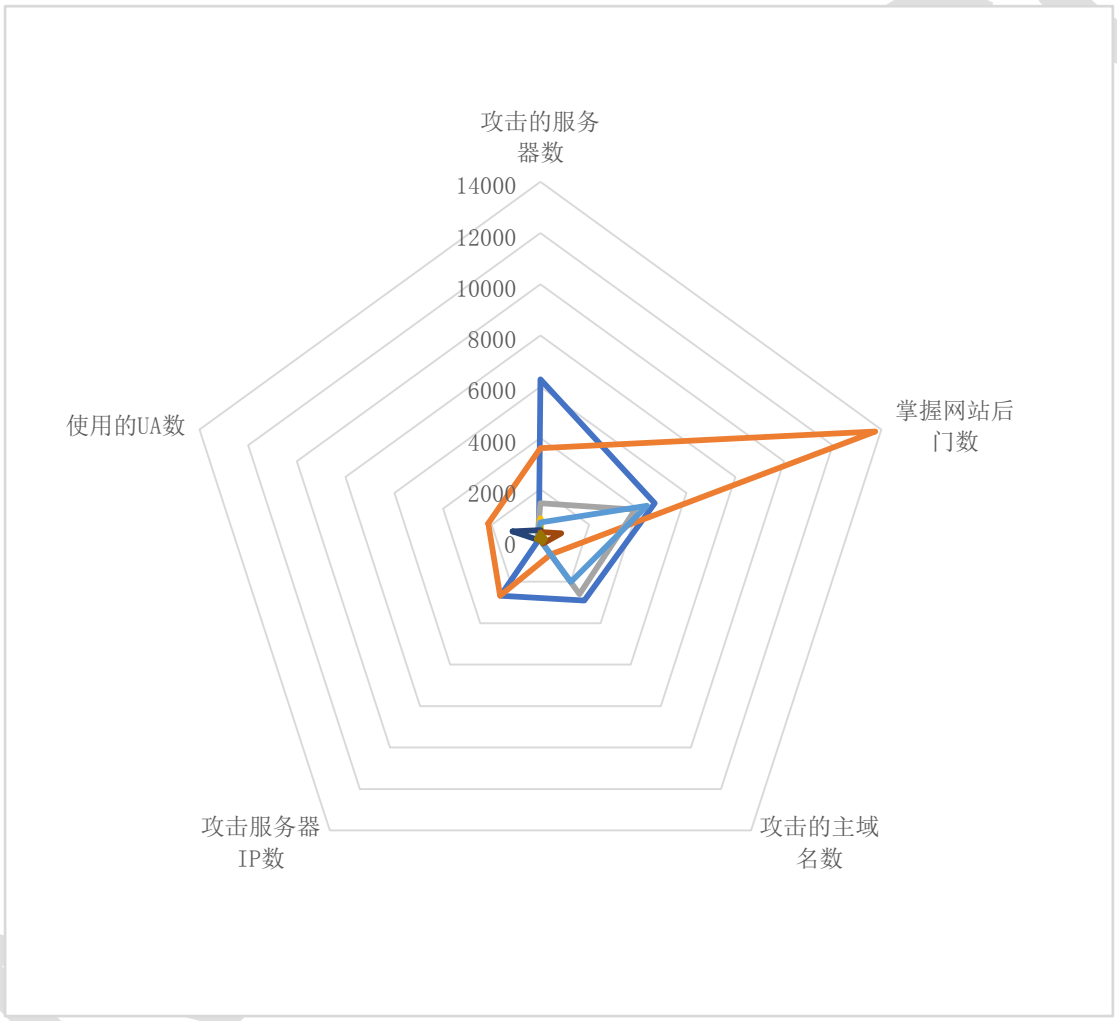

图 3.1 团伙规模（攻击 IP 个数）Top 10 的团伙攻击特点概要图

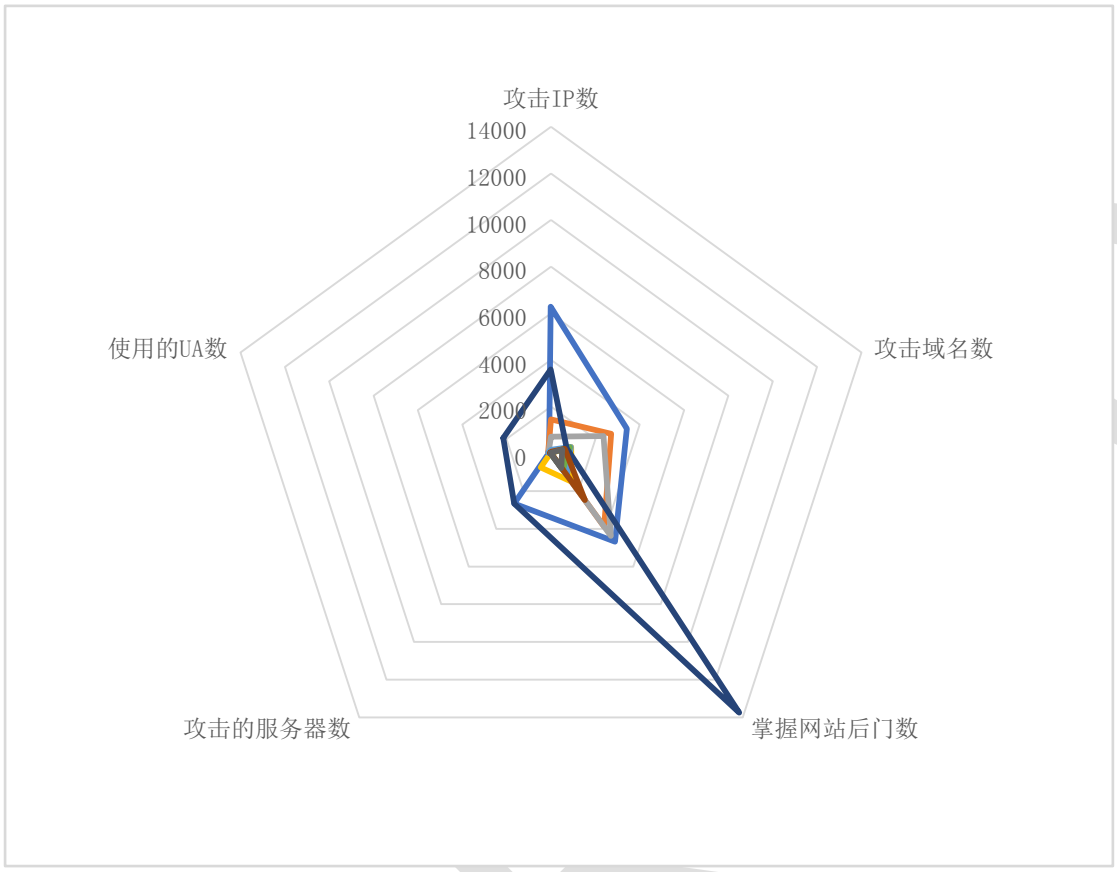

图 3.2 攻击的域名数量 Top 10 的团伙攻击特点概要图

3.1 GC_WEBATTACK_001：全年使用攻击资源最多的团伙

团伙总结：团伙 GC_WEBATTACK_001 全年使用过的攻击 IP 数量共 6283 个，为全年发现团伙中攻击资源最多的团伙，并且持续在全年各月活跃。在该团伙总共活跃的 260 天内，共攻击了 2668 个服务器，涉及 3425 个域名以及 4688 个网站后门。该团伙主要通过自动化工具对网站进行批量的扫描与控制，攻击 IP 主要来源于境外。

以下是该攻击团伙的攻击资源和攻击目标拓扑结构。可以看出，其中部分攻击 IP 所控制的网站后门较多，属于较为活跃的攻击资源。

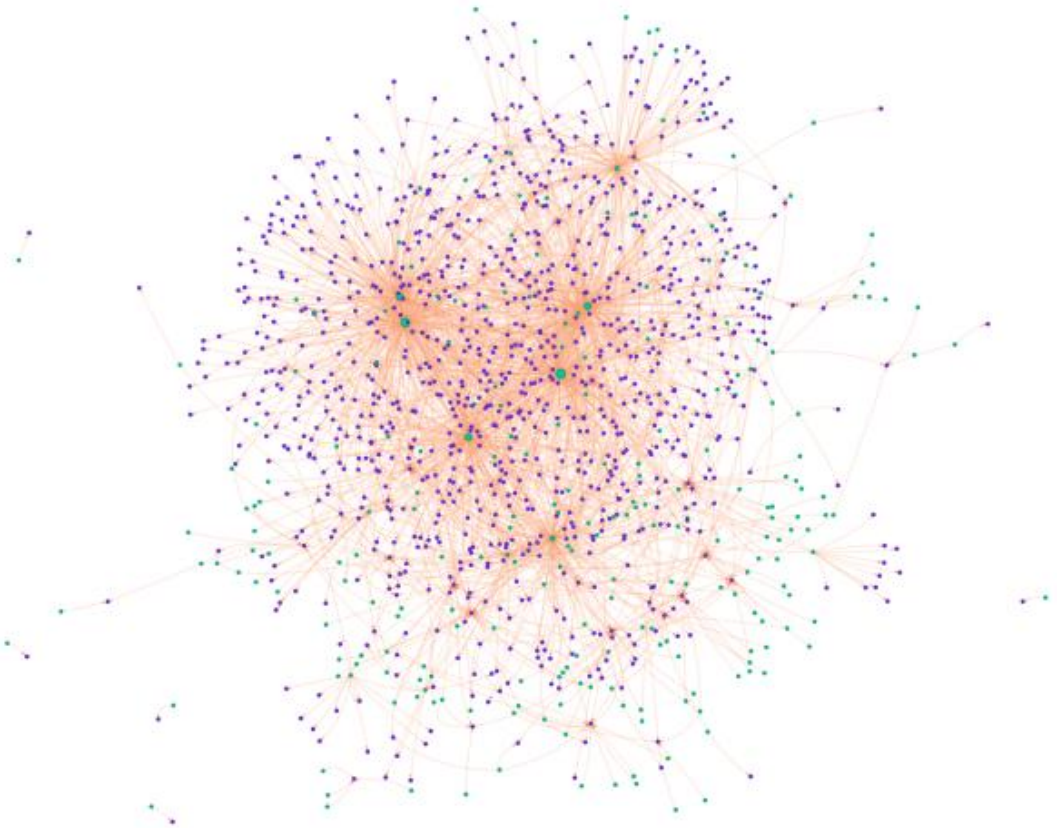

图 3.3 该团伙的攻击资源和攻击目标拓扑结构（受图片大小所限，只展示团伙的主要部分，绿色为攻击 IP，紫色为所连接的网站后门）

下图是该攻击团伙在 2018 年度每月的攻击概况。可以看出，2-5 月以及 10-12 月使用的攻击资源较多，并且攻击的网站服务器较多，其攻击行为较为活跃。

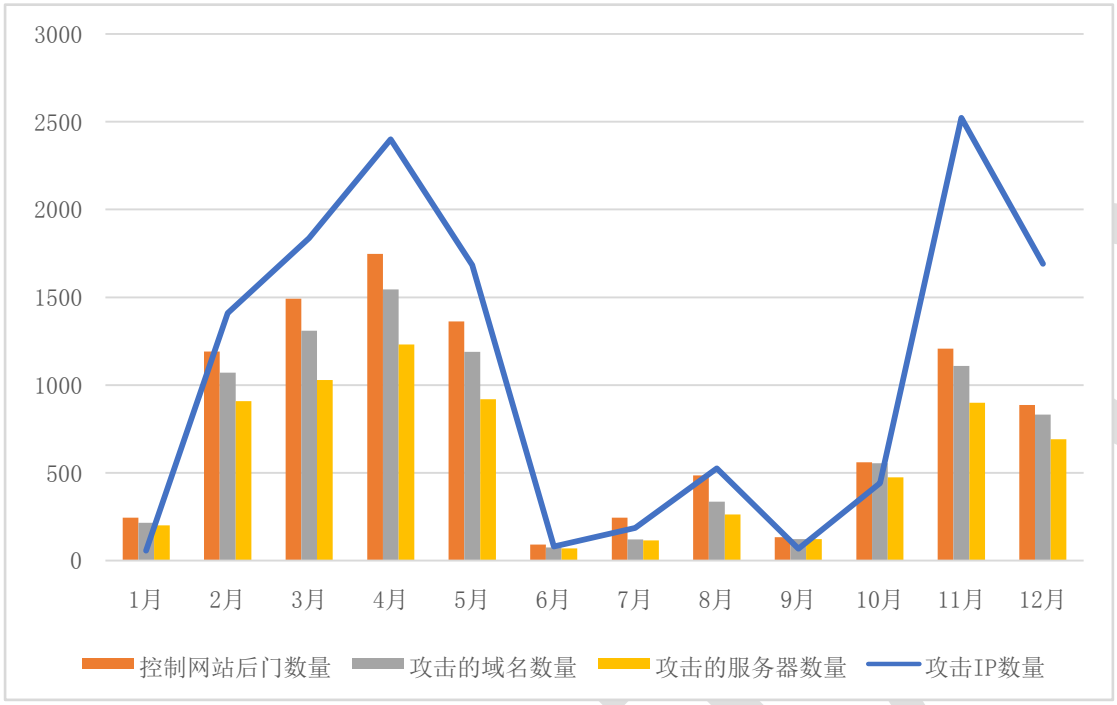

图 3.4　该团伙每月攻击资源和攻击目标情况

如下图所示，可以看出该团伙全天的活跃度比较平稳，说明该团伙的攻击自动化程度较高，推测是使用特定工具对目标网站自动植入后门并进行持续连接控制。

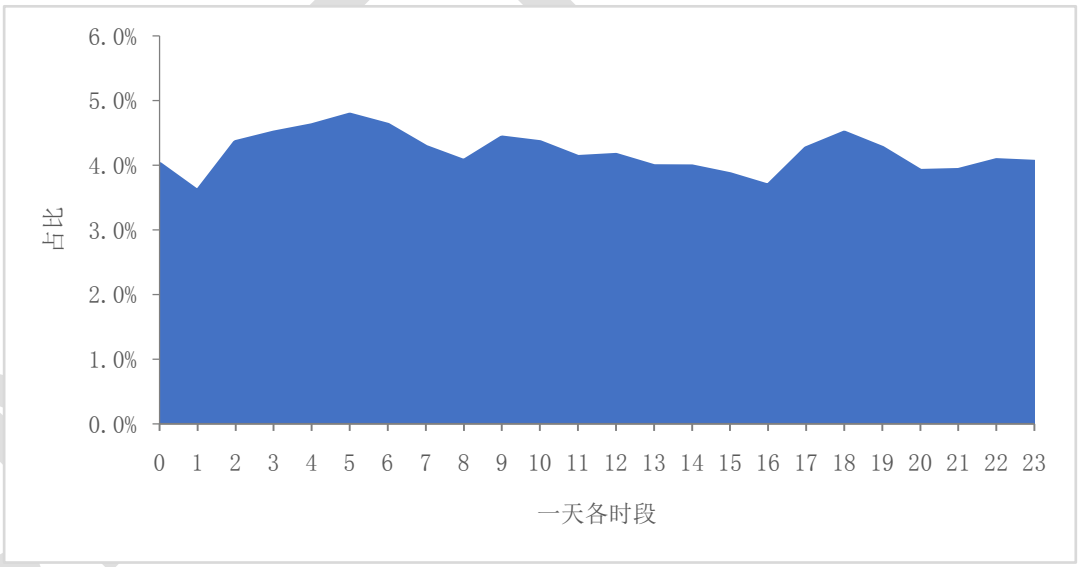

图 3.5　该团伙的活跃时段分布

该攻击团伙使用的攻击 IP 数量按境内外分布情况如下图所示，可以看出，该团伙使用的境外 IP 为主，占到了 6283 个攻击 IP 中的 80.3%。

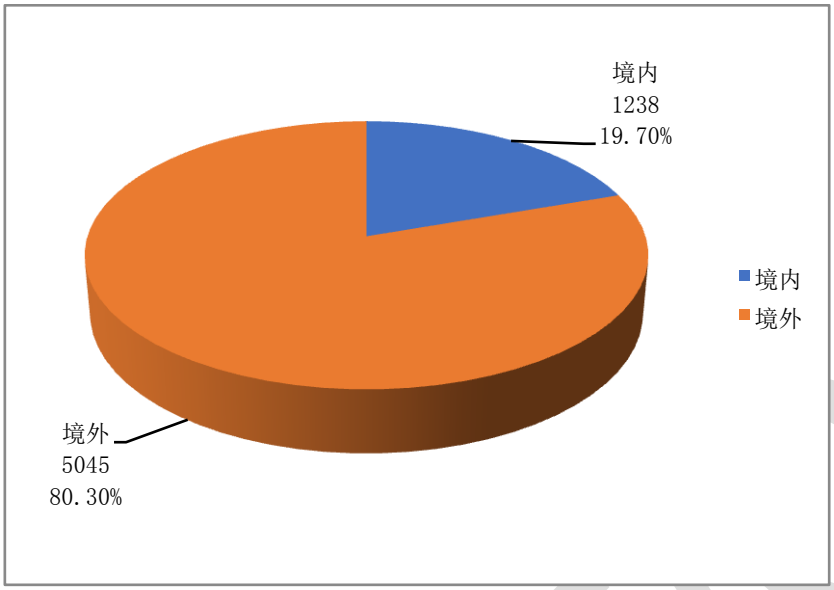

图 3.6 该团伙使用攻击 IP 的境内外分布

在 6283 个攻击 IP 中，3359 个攻击 IP 为 IDC 机房 IP，超过了一半以上，资源特点较为明显。

3.2 GC_WEBATTACK_002：攻击资源集中在境外某国的团伙

团伙总结：GC_WEBATTACK_002 使用的攻击 IP 有 319 个，全年 12 个月均有活跃，在其间断活跃的 102 天内，攻击了 174 个域名，涉及 157 个服务器 IP，植入和掌握网站后门 858 个，所攻击的网站类型主要集中在政府事业单位、企业网站、网贷和游戏网站等，种类繁多。该团伙的攻击 IP 绝大多数来自境外某国。

下图是该攻击团伙的攻击资源和攻击目标拓扑结构，可以看出其中的连接控制关系较为复杂。

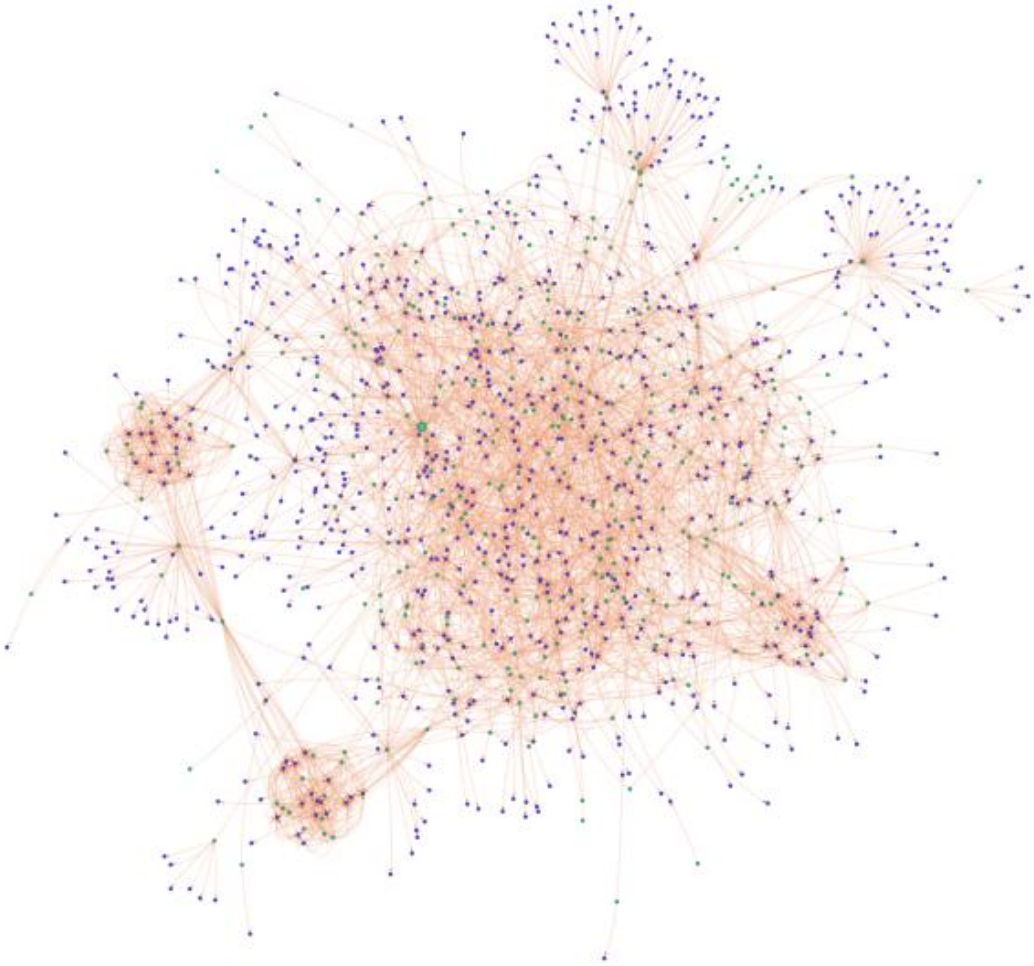

图 3.7 该团伙的攻击资源和攻击目标拓扑结构（受图片大小所限，只展示团伙的主要部分，绿色为攻击 IP，紫色为所连接的网站后门）

该攻击团伙在 2018 年全年控制的网站数量较为平均，但在 2018 年 5 月，7 月以及 8 月所控制的网站后门数量较多，且其中 7 月和 8 月使用过的攻击资源较多，具体如下所示。

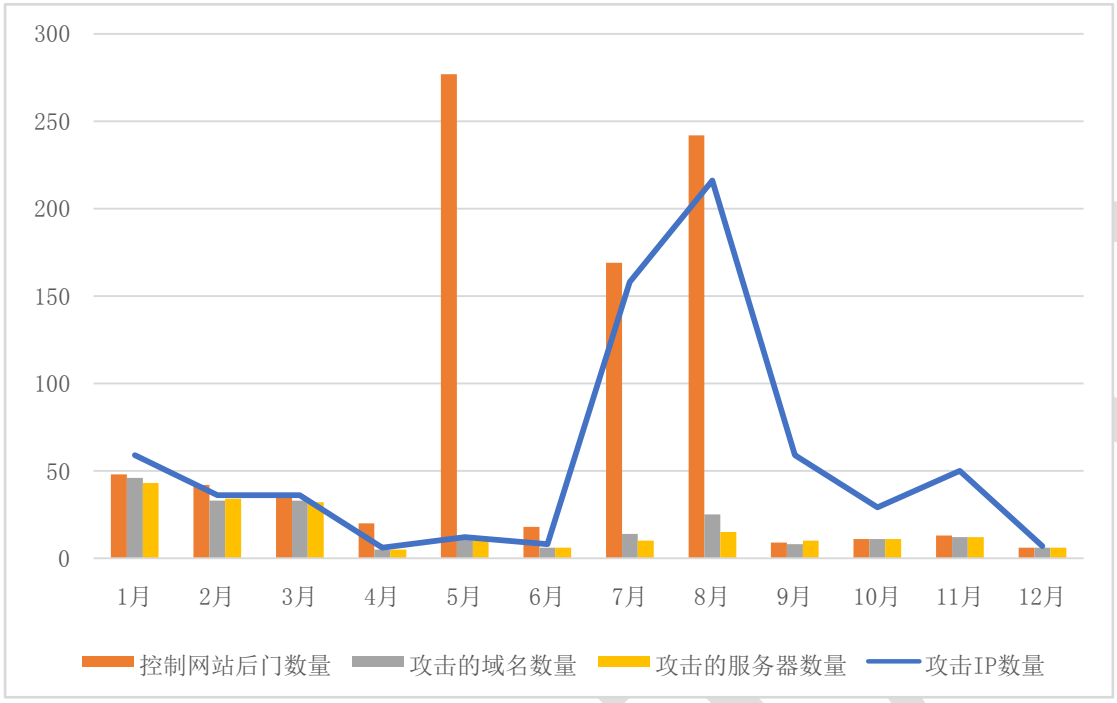

图 3.8 该团伙每月攻击资源和攻击目标情况

从该团伙的活跃时间段可以看出，在每日的凌晨 1 点，以及 9-15 点较为活跃。

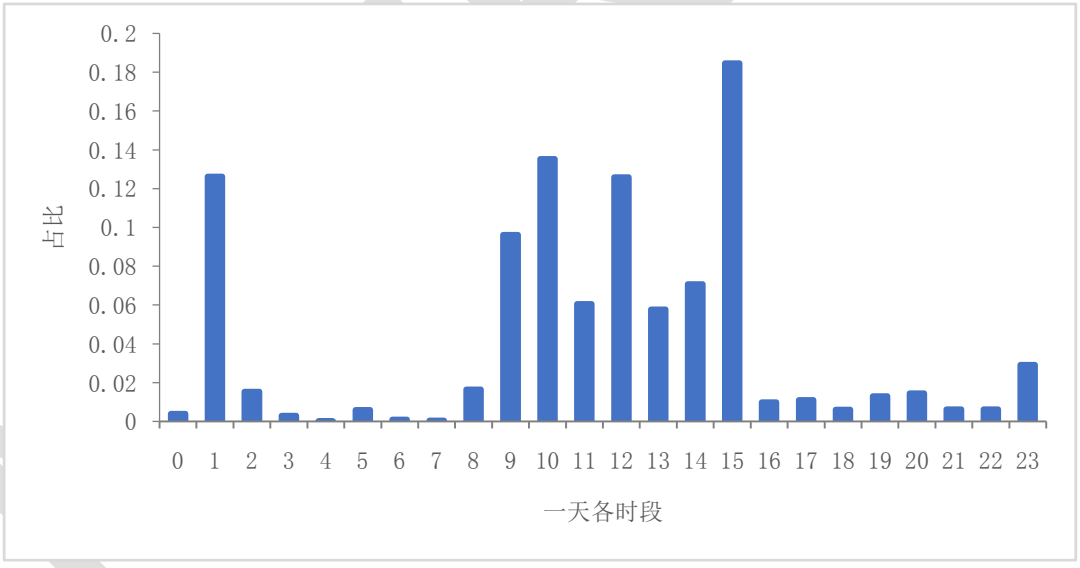

图 3.9 该团伙的活跃时段分布（以中国时区统计）

如下图所示，其攻击 IP 资源主要集中在境外某国。

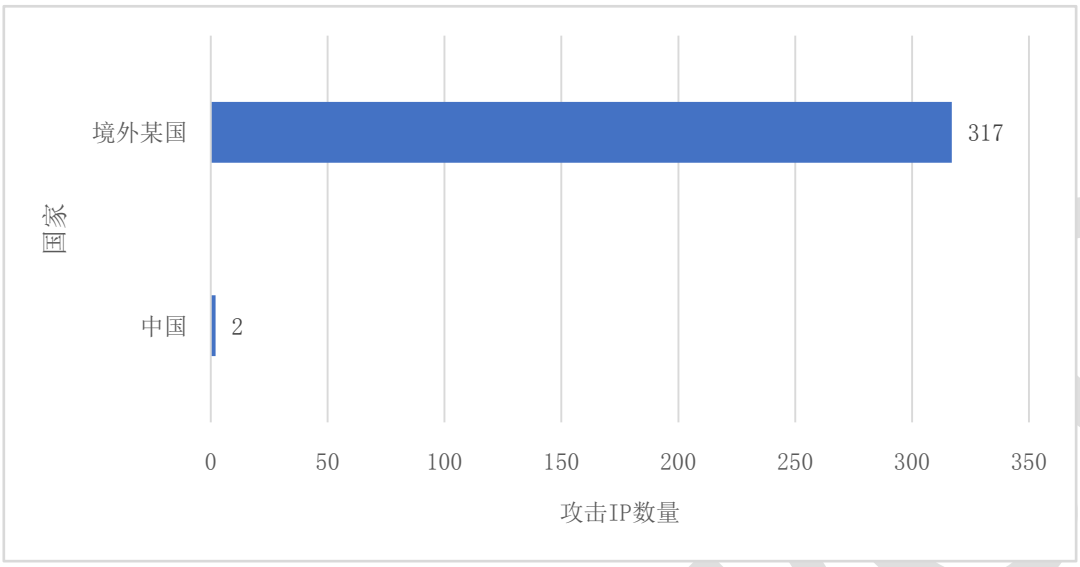

图 3.10 该团伙的攻击 IP 所属国家分布

其攻击的服务器 IP 主要集中在我国境内，按照 IP 的省份分布来看，主要集中在北京、河南等地。所攻击网站主要集中在政府事业单位、企业网站、网贷和游戏网站等类型。

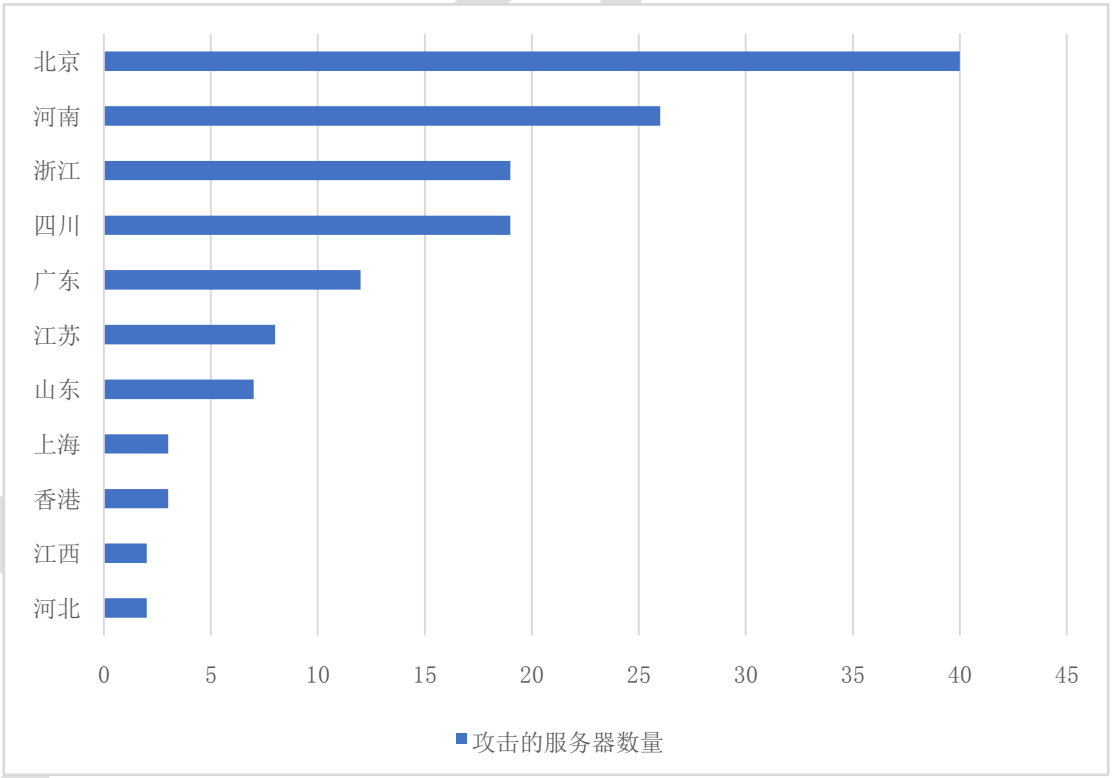

图 3.11 攻击境内网站服务器数量按省份 TOP10 分布

3.3 GC_WEBATTACK_003：某精准针对博彩网站的团伙

团伙总结：GC_WEBATTACK_003 的攻击 IP 数量为 61 个，通过抽样监测，仅观测到其攻击了 6 个网站域名。该团伙从 2018 年 1 月持续活跃到 8 月，其中 3 月份是活跃高峰期。该团伙的主要攻击目标为博彩网站，从其攻击动作来看，其攻击行为主要由窃取用户数据等黑产利益驱动。

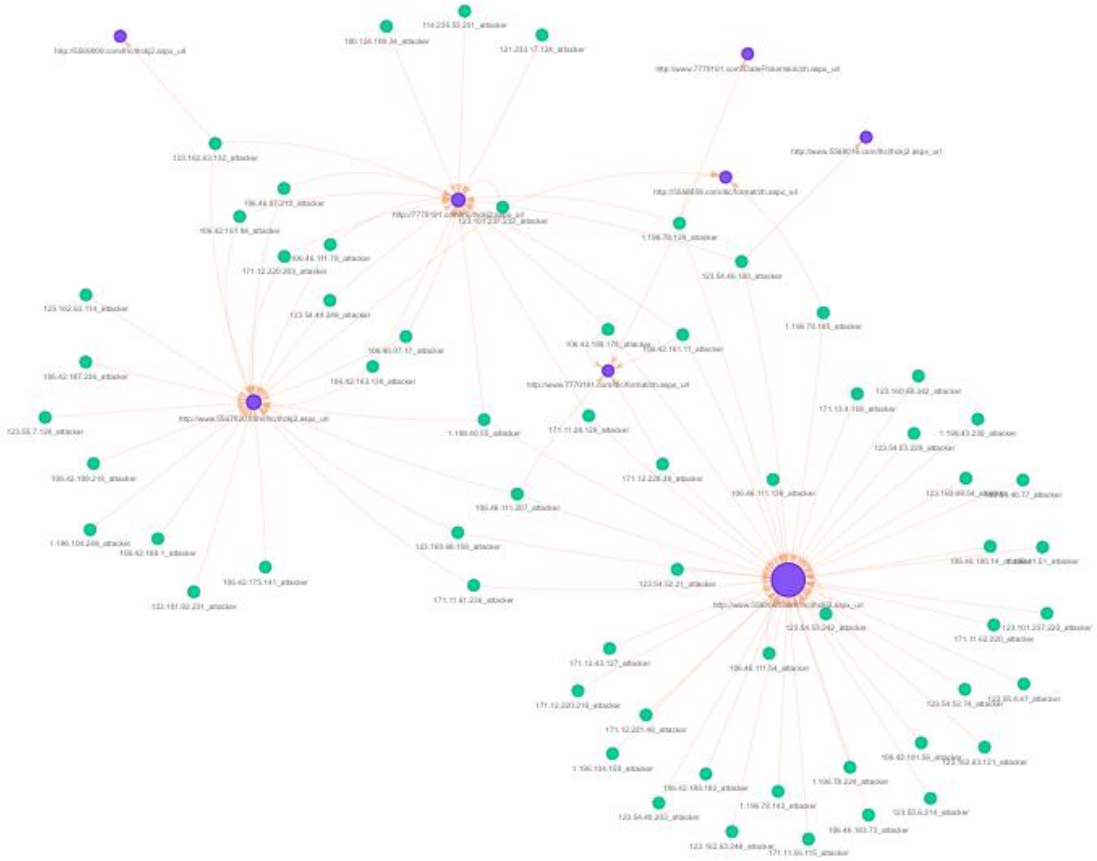

图 3.12 该团伙的攻击资源和攻击目标拓扑结构（受图片大小所限，只展示团伙的主要部分，绿色为攻击 IP，紫色为所连接的网站后门）

从该攻击团伙在 1-8 月的攻击行为来看，较为平稳。

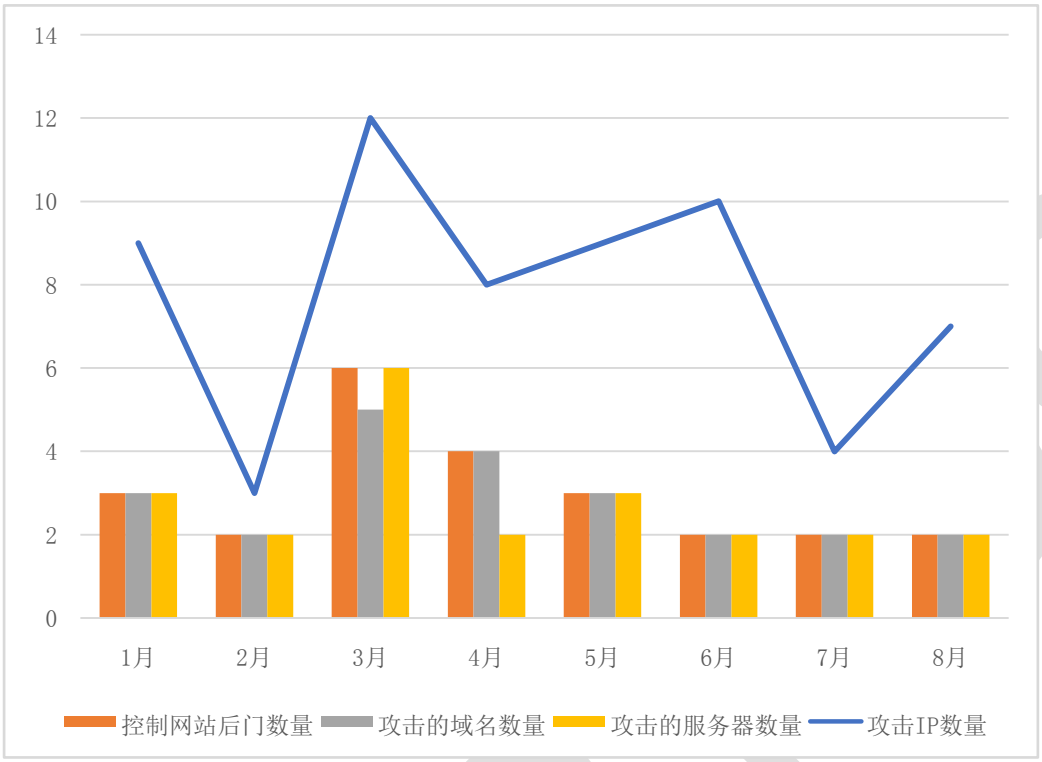

图 3.13 该团伙每月攻击资源和攻击目标情况

观察该团伙在一天 24 小时内的攻击行为占比，可以发现该攻击团伙从早上 10 点持续活跃至晚上 23 点，15 点-21 点为攻击团伙发起网站后门攻击的高峰期，占全天攻击的 80%。同时，活跃峰值在 20 点左右。

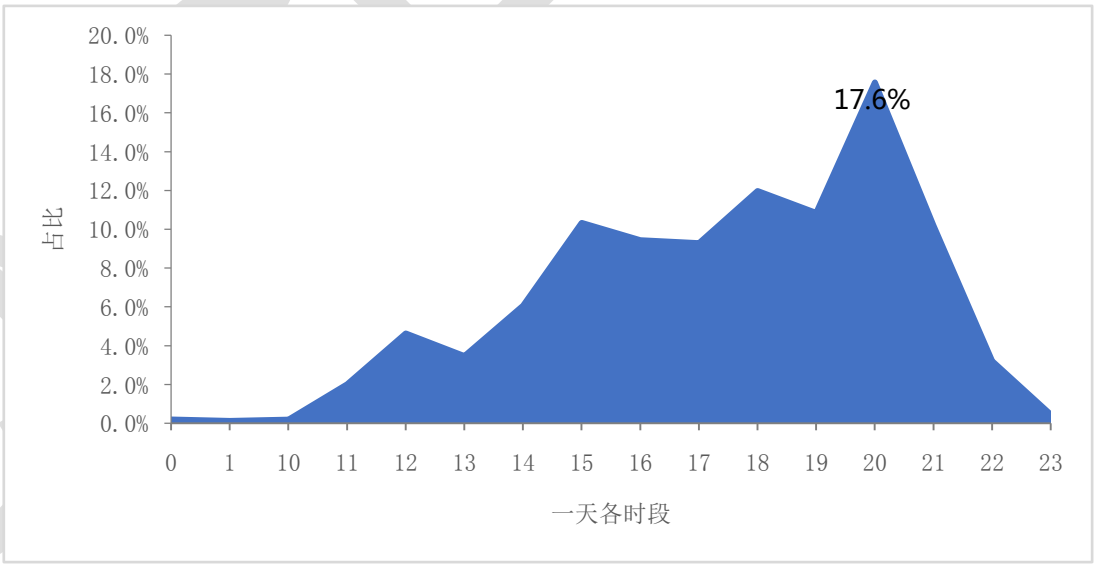

图 3.14 该团伙的活跃时段分布

该团伙攻击的目标服务器 IP 全部分布在中国香港，且全部为博彩网站。该攻击团伙对被攻击网站的操作属于典型的黑产利益驱动行为。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行，开展以互联网金融为代表的“互联网+”融合产业的相关安全监测工作。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2018 年，CNCERT 与 76 个国家和地区的 233 个组织建立了“CNCERT 国际合作伙伴”关系。