2018 年活跃 DDoS 攻击团伙分析报告

国家计算机网络应急技术处理协调中心

2019 年 1 月

目 录

一、 报告摘要

CNCERT 针对多种主要用于发起 DDoS 攻击的僵尸网络家族进行抽样监测，并对 2018 年全年涉及的攻击资源和攻击团伙进行了多维分析，发现 C&C 控制端 IP 共 2108 个，总肉鸡 IP 数量为 140 万余台，受攻击目标 IP 数目 9 万余台，共发现攻击团伙 50 个，其中涉及活跃攻击团伙 16 个，共包含 358 个 C&C 控制端 IP，总共攻击约 3 万个目标 IP，在全年攻击目标中占比 31%。总体来看，利用这些僵尸网络家族进行 DDoS 攻击的特点主要有:

1. 从攻击目标规模和攻击事件数目来看，8 月份均为全年的最高峰。从控制的肉鸡规模来看，11 月份是全年的最高峰。

2. XorDDoS、Gafgyt、BillGates 这三种僵尸网络家族参与攻击事件最多。其中，XorDDoS 僵尸网络家族所控制的肉鸡规模最大，且持续时间最长；Gafgyt 僵尸网络家族总活跃 C&C 控制端 IP 数量最多，为 1096 个，而大部分 C&C 控制端只存活一个月，但由于其样本的主动感染特性，往往在出现数天后就能获得非常大的肉鸡规模。从攻击时间来看，XorDDoS 和 BillGates 僵尸网络家族在凌晨 2-10 时发起的攻击数量明显减少，疑似是需要由人工触发的攻击方式；Gafgyt 僵尸网络的攻击按时间分布较均匀，疑似是作为 DDoSaaS（DDoS as a service）对外提供服务。

3. 活跃攻击团伙中，规模最大的攻击团伙使用的僵尸网络由多个家族组成，而其他的团伙的家族特性相对比较单一。所有团伙的攻击目标数量占据全年总攻击目标数量的 36%，而规模最大的团伙的攻击目标数量占据了全年总攻击目标数的 23%。攻击团伙攻击的目标主要位于云主机厂商网段，行业主要覆盖游戏、博彩、色情等。单一团伙的长期攻击目标并无行业特性，仅在短期内受攻击任务影响会有短暂的行业特性。

在本报告中，一次 DDoS 攻击事件是指在经验攻击周期内，不同的攻击资源针对固定目标的单个 DDoS 攻击，攻击周期时长不超过 24 小时。如果相同的攻击目标被相同的攻击资源所攻击，但间隔为 24 小时或更多，则该事件被认为是两次攻击。此外，DDoS 攻击资源及攻击目标地址均指其 IP 地址，它们的地理位置由它的 IP 地址定位得到。DDoS 攻击团伙是指能利用一定规模的互联网攻击资源，在较长时间范围内活跃，同时期内利用攻击资源针对极相似的攻击目标集合进行攻击，其攻击资源在一定时间范围内固定，长时间会发生变化。同一攻击团伙所发起的系列 DDoS 攻击称为团伙性攻击。

二、 总体概况

2.1 攻击资源概况

从全年来看，利用僵尸网络发起 DDoS 攻击的事件数量，在年初呈现上涨趋势，在 8 月份开始下滑，如图 2.1 所示。C&C 控制端数量的月度统计趋势和 DDoS 攻击事件数量的月度统计趋势基本一致，同样是在 8 月份达到最大值后逐步回落，如图 2.2 所示。僵尸网络肉鸡数量发展趋势前期与 C&C 控制端类似，在年初呈现上涨趋势，在 8 月至 9 月期间有一定程度的下滑，但是 10 月之后肉鸡数量开始呈现大幅上涨趋势，说明在 10 月以后更少的 C&C 控制端控制了更多的肉鸡，出现了控制规模较大的控制端，如图 2.3 所示。受攻击目标的月度趋势与肉鸡基本一致，8 月达到了高峰，9 月有一定程度的下降，此后，受攻击目标的数量一直在中高位波动，如图 2.4 所示。

图 2.1 DDoS 攻击事件月度统计趋势

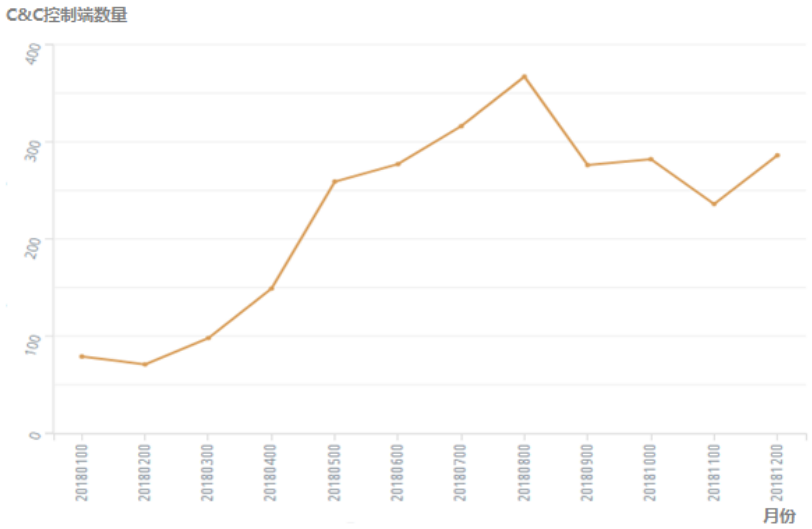

图 2.2 C&C 控制端月度统计趋势

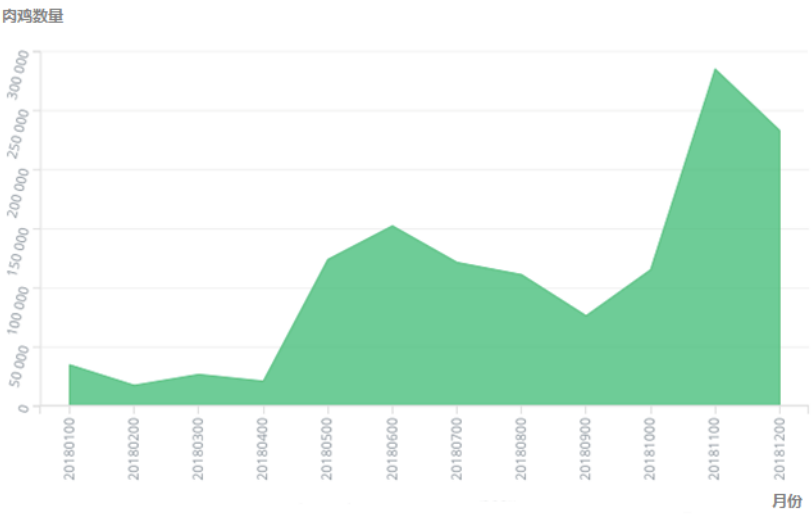

图 2.3 肉鸡月度统计趋势

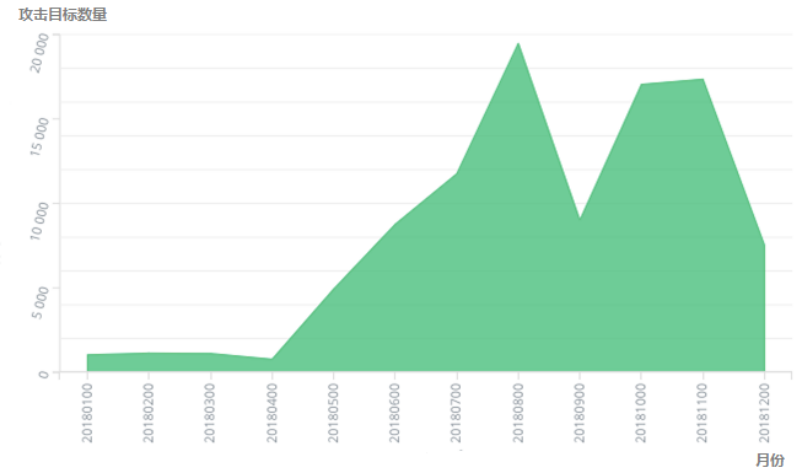

图 2.4 攻击目标月度统计趋势

2018 年全年涉及的攻击资源中，共发现 C&C 控制端 IP 共 2108 个，其中包含境内控制端占比 15.8%，境外控制端占比 84.2%，境内外的控制端按地理位置分布见图 2.5;总肉鸡 IP 数量为 140 万余台，其中境内肉鸡占比 90.6%，境外肉鸡占比 9.4%，境内外的肉鸡地址按地理位置分布见图 2.6；受攻击目标 IP 数目 9 万余台，其中境内受攻击目标占比 36.7%，境外受攻击目标占比 63.3%，境内外的受攻击目标按地理位置分布见图 2.7。综上可见，大量的境内肉鸡被境外控制端所利用，向境内外目标地址发起攻击。这些攻击目标所属行业主要分布在色情、博彩、文化体育和娱乐、运营商 IDC、金融、教育、国家机构等行业，如图 2.8 所示。

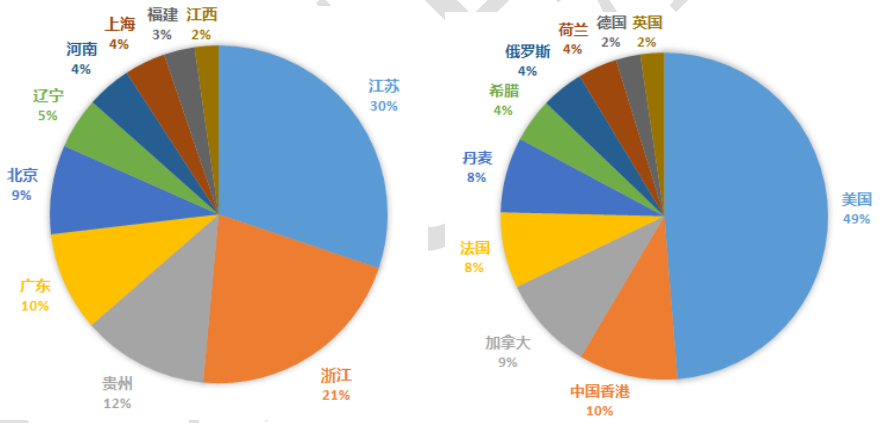

图 2.5 2018 年控制端地址数量 TOP10 国家或地区分布

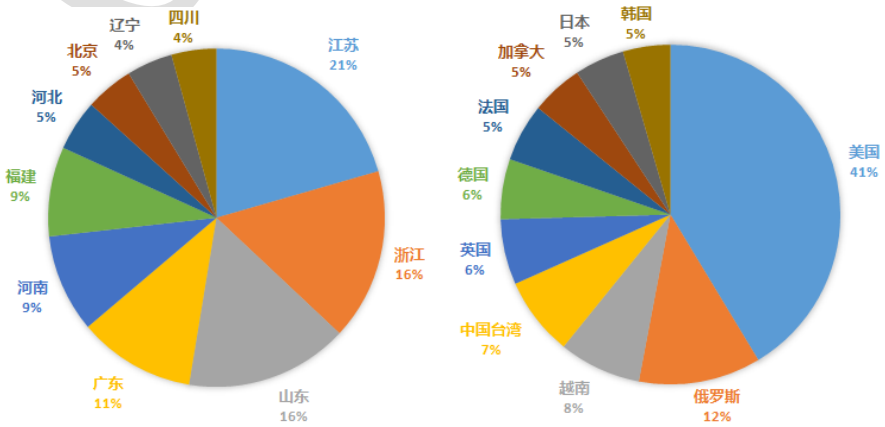

图 2.6 2018 年肉鸡地址数量 TOP10 国家或地区分布

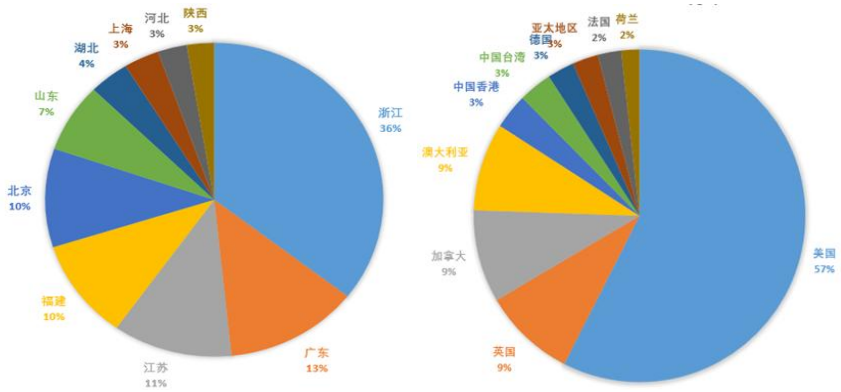

图 2.7 2018 年攻击目标地址数量 TOP10 国家或地区分布

图 2.8 攻击目标所属行业云图

2.2 活跃团伙概况

2018 年，CNCERT 共监测发现 50 个利用僵尸网络进行攻击的 DDoS 攻击团伙，攻击团伙的月度数量趋势如图 2.9 所示，与 C&C 控制端及攻击事件数量一样，在 8 月份达到最高峰。其中，活跃两个月及以上，且肉鸡数量较大的较活跃攻击团伙有 16 个，共包含 358 个 C&C，在全年 C&C 中占比 16%，总共攻击 2.8 万个目标，在全年攻击目标中占比 31%，其基本信息表见表 2.1。

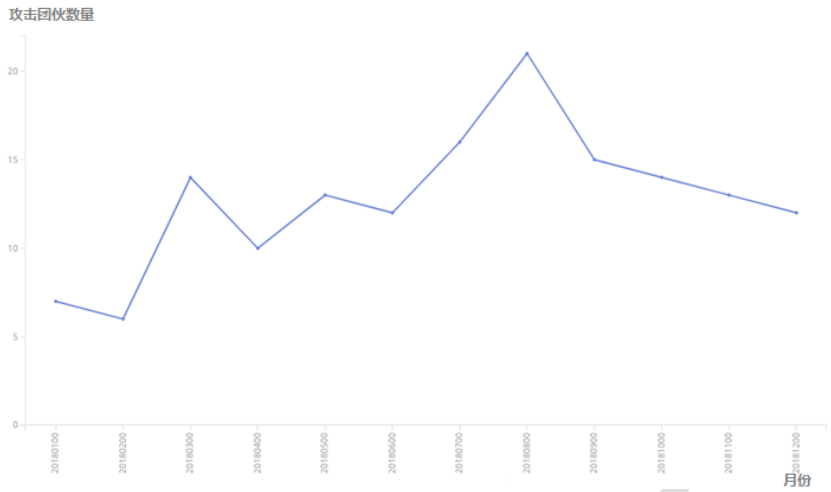

图 2.9 攻击团伙月度统计趋势

表 2.1 活跃攻击团伙基本信息表

团伙编号	最早活跃时间	最近活跃时间	活跃月份	C&C 数量	肉鸡数量	起止月份间隔	攻击目标数目
G1	20180101	20181231	12	283	571016	12	21324
G2	20180502	20181230	8	9	384	8	57
G3	20180308	20181104	2	2	462	8	2
G4	20180101	20180731	5	4	1779	7	185
G5	20180721	20181222	3	2	509	5	20
G6	20180606	20180925	2	2	543	4	74
G7	20180531	20180801	4	8	1426	2	369
G8	20180723	20180911	3	2	654	2	476
G9	20180511	20180712	3	9	13035	2	642
G10	20180708	20180905	3	2	699	2	87
G11	20180303	20180515	3	12	2921	2	47
G12	20180707	20180902	3	2	3243	2	380
G13	20180614	20180827	3	5	13290	2	5440
G14	20180109	20180225	2	2	639	2	142
G15	20180907	20181027	2	8	8358	2	4023
G16	20180802	20180816	1	74	10936	1	747

较活跃攻击团伙的 C&C 控制端和攻击目标总览如图 2.10 所示，图中的节点为 C&C 控制端及其攻击目标，C&C 控制端攻击过某攻击目标则连一条边，全年间它们的攻击关系自然地形成了力导向关系图。

从图中可以看出，代表不同攻击团伙的 16 个不同颜色的簇之间相互较为独立，同一攻击团伙的攻击目标非常集中，不同攻击团伙间的攻击目标重合度较小。

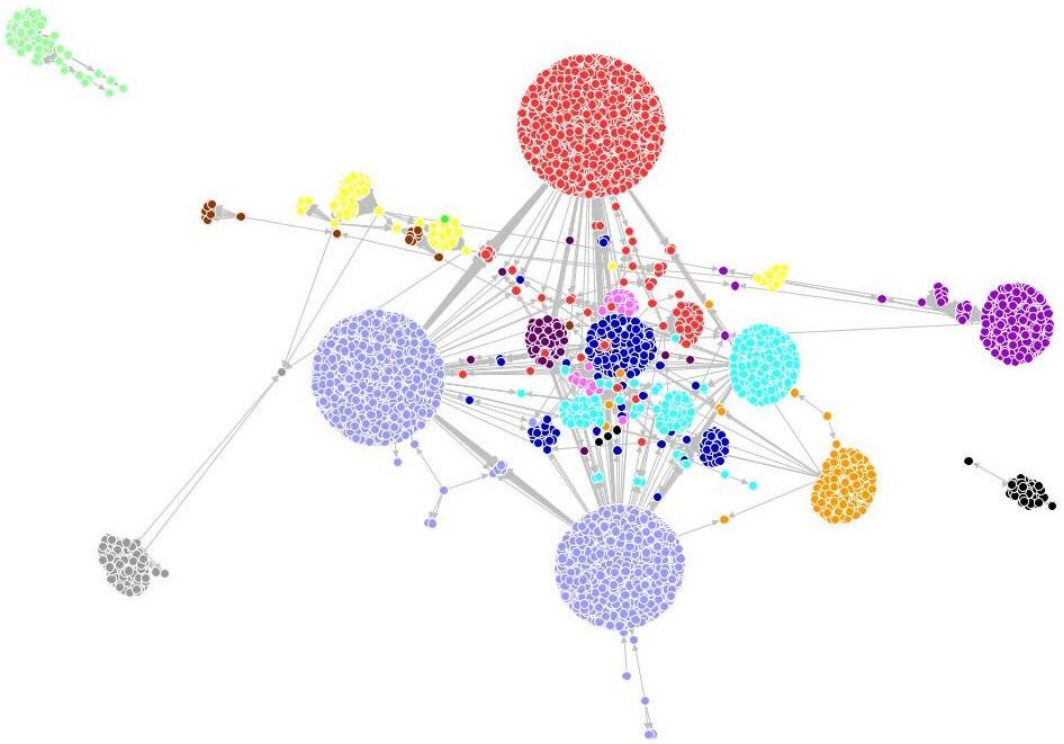

图 2.10 活跃攻击团伙总览（C&C 和攻击目标）

三、 重点僵尸网络家族攻击特点

3.1 XorDDoS 僵尸网络家族

XorDDoS 僵尸网络家族在全年共活跃 11 个月，在 2018 年 2 月份时曾短暂退出，家族总活跃 C&C 数量为 146 个，单个 C&C 攻击活跃时间最长持续 7 个月，C&C 控制端的月度数量分布如图 3.1 所示，其控制端数量在上半年大幅上升，在 6 月份达到高峰后逐步回落。该家族对僵尸网络的控制规模在上半年逐步攀升，在 7 月份达到小高峰后，

在 8-9 月份期间短暂回落后，在 10 月份重新扩大对僵尸网络的控制规模，并于 11 月份达到顶峰，当月单个 C&C 最高控制了 7 万个肉鸡，如图 3.2 所示；该家族攻击目标的月度分布如图 3.3 所示，全年的攻击目标数量呈现上升趋势；该家族每月涉及的攻击团伙数量趋势如图 3.4 所示，5-8 月的攻击团伙数量有一定下降，之后保持在 4 个以下的较稳定数量。

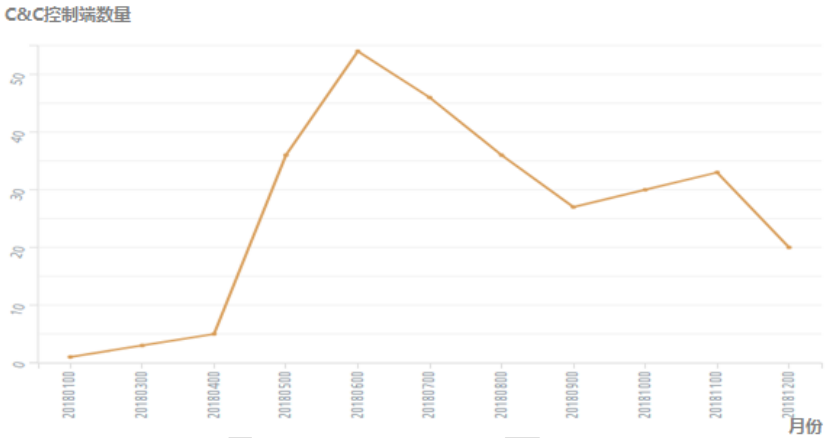

图 3.1 XorDDoS 僵尸网络家族 C&C 控制端月度数量分布

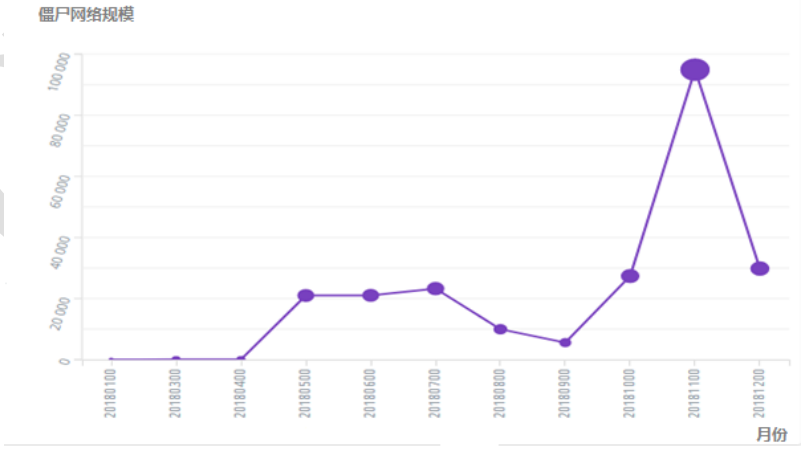

图 3.2 XorDDoS 僵尸网络家族控制规模月度分布

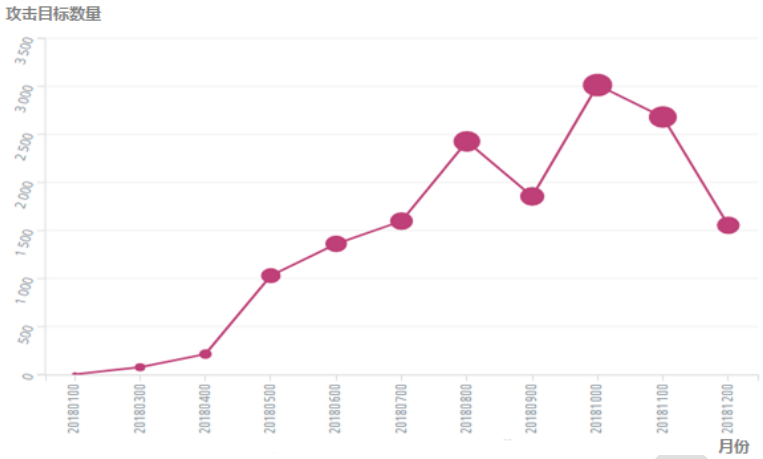

图 3.3 XorDDoS 僵尸网络家族的攻击目标月度分布

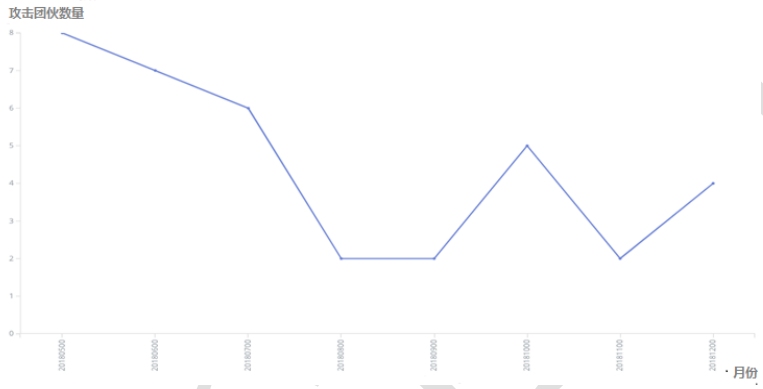

图 3.4 XorDDoS 僵尸网络家族月度涉及攻击团伙数量

从攻击发起时间分布来看，在凌晨 2 点到 10 点内，发起的攻击数量呈现明显下降，可能与作息时间相关，疑似是需要由人工触发的攻击方式。从攻击发起时间分布猜测，一方面，可能这是控制者的晚睡时间，另一方面也有可能是因为控制者的攻击目标在该时间段内都处于活跃低谷，没有攻击价值，如图 3.5 所示。

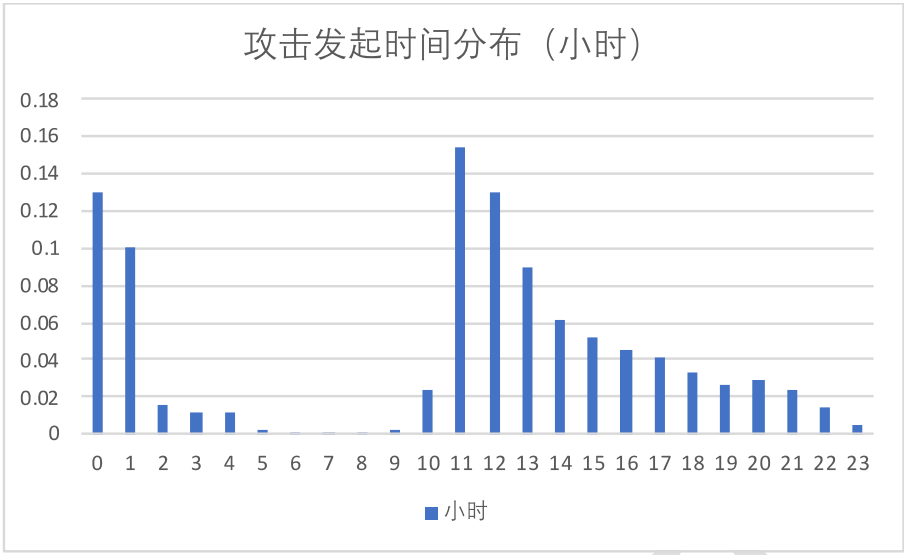

图 3.5 XorDDoS 僵尸网络家族攻击发起时间分布

XorDDoS 僵尸网络家族 C&C 控制端月活和日活情况如图 3.6 所示，月度攻击目标热度如图 3.7 所示。平均每个控制端活跃 2 个月，每个月平均活跃 11 天，每个月平均针对 209 个攻击目标发起攻击；其中有 7 个控制端的活跃月度超过 7 个月，且每个月的平均活跃天数超过 20 天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为 1662 个。

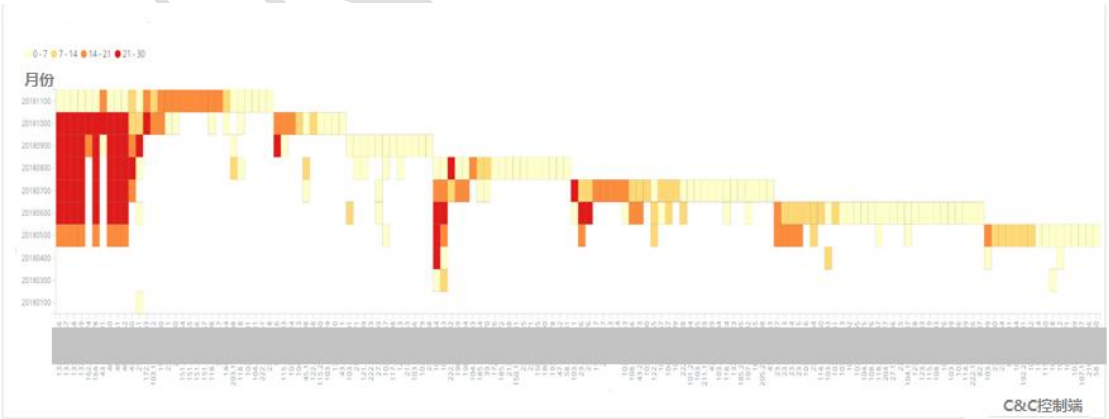

图 3.6 XorDDoS 僵尸网络家族 C&C 控制端月度日活跃热度

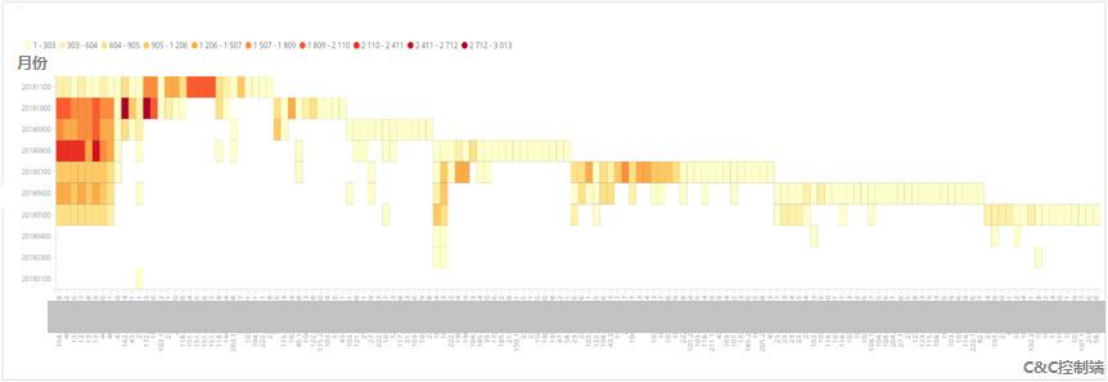

图 3.7 XorDDoS 僵尸网络家族 C&C 控制端月度攻击目标数量热度

XorDDoS 家族中规模最大的攻击团伙从 5 月份开始出现，全年总共连续出现 8 个月。该团伙的 C&C 控制端 IP 大多与某域名下的子域名相关，构成了本报告第四部分讨论的重要攻击团伙中的团伙 G1 的子团伙 G1-2。该子团伙与某 2014 年被发现的公开组织相关，该组织与游戏私服、色情、赌博等产业联系紧密。CNCERT 也对其进行了长期跟踪，监测发现该组织使用了大量包含特定字符串的恶意域名。CNCERT 于 2017 年溯源分析的数千起大流量攻击事件中，监测发现这些域名涉及了其中多起事件，且在 2017 年 8 月左右非常活跃，此后沉寂了半年多的时间，在 2018 年 5 月开始又重新活跃起来。对该子团伙的介绍详见 4.1.2 节。

3.2 Gafgyt 僵尸网络家族

Gafgyt 僵尸网络家族在全年 12 个月持续活跃，总活跃 C&C 控制端 IP 数量为 1096 个，超过总控制端的半数；单个 C&C 控制端存活时间最长为 8 个月，而其中仅有 133 个控制端 IP 存活时间超过一个月，大部分控制端 IP 只在一个月内存活。如图 3.8 所示，该家族的 C&C

控制端数量在上半年不断上升，并在 8 月份达到最高值后开始持续下滑；该家族对僵尸网络的控制规模在上半年呈现上升趋势，在 6-8 月份达到最高峰后，在 9 月份有一定下降，之后又缓慢上升，如图 3.9 所示，当月单个 C&C 最多控制了将近 7300 个肉鸡，平均单个 C&C 的肉鸡规模相对较小；利用该家族发起 DDoS 攻击的被攻击目标的月度分布如图 3.10 所示，10 月和 11 月的攻击目标数量呈现大幅上升趋势。

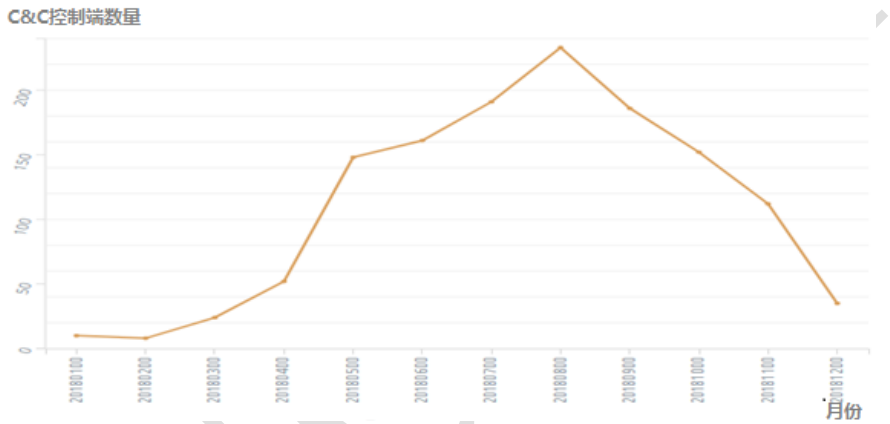

图 3.8 Gafgyt 僵尸网络家族 C&C 控制端月度数量分布

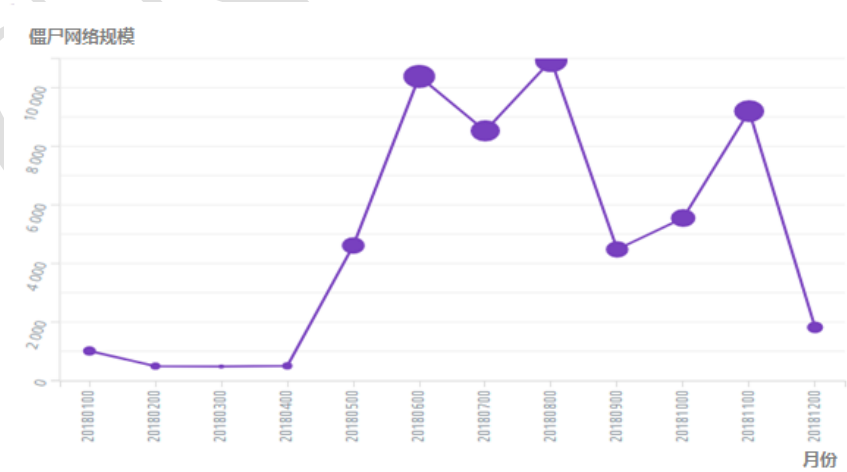

图 3.9 Gafgyt 僵尸网络家族控制规模月度分布

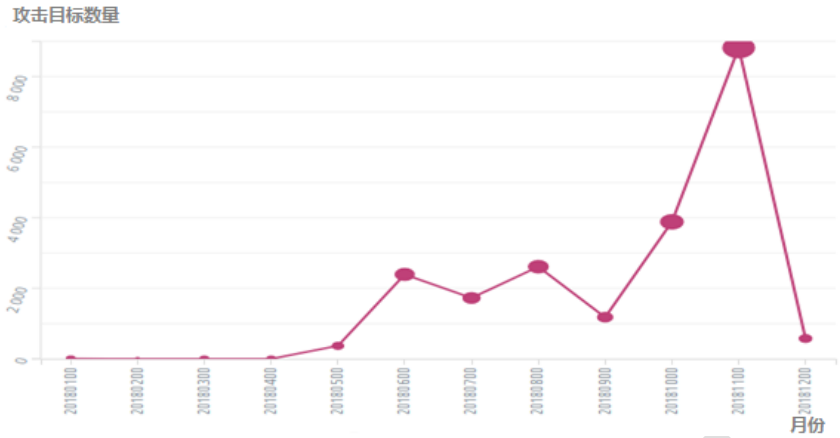

图 3.10 Gafgyt 僵尸网络家族的攻击目标月度分布

从图 3.11 的攻击发起时间分布来看，利用 Gafgyt 家族的攻击团伙，其攻击时间在全天分布相对较均匀，主要由于其为物联网僵尸网络，控制的肉鸡为常常 24 小时在线的物联网设备，且利用 Gafgyt 僵尸网络家族发起攻击，符合 DDoSaaS(DDoS as a Service)模式的服务特征。DDoSaaS 模式的僵尸网络是指提供租赁服务，即提供给没有僵尸资源和技术水平的用户一定时间内一定数量僵尸的使用权，并根据用户所需的规模、配置等参数的不同提供定制化的服务，加上自动支付平台的普及，用户们只要付款就可以即时获得一批佣兵式的攻击资源，这些因素正使得这一模式逐渐成为僵尸网络获利的主流。

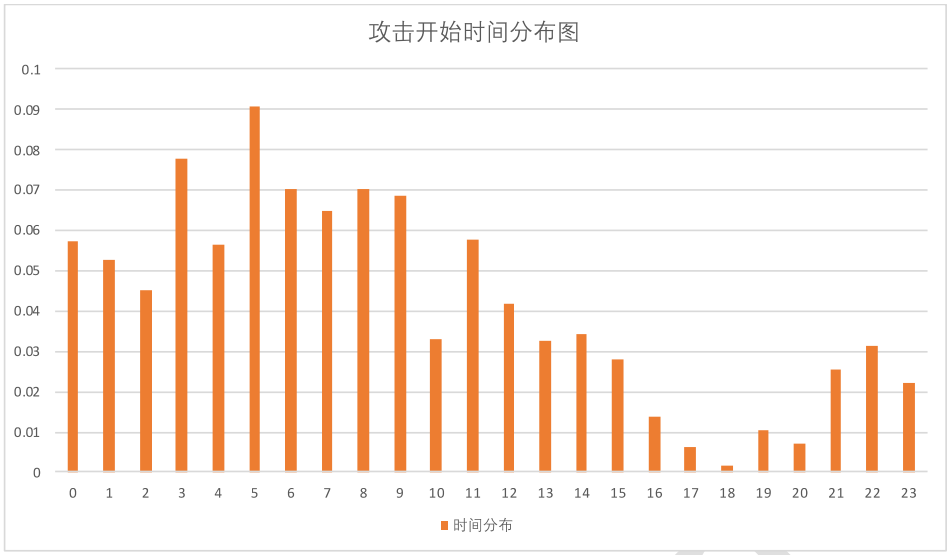

图 3.11 Gafgyt 僵尸网络家族攻击发起时间分布

从僵尸网络肉鸡规模上来看，使用 Gafgyt 家族的攻击团伙的特点是，每个月基本都会利用多个控制规模较大的 C&C 主机和其他控制规模较小的 C&C 主机共同攻击，并且 C&C 之间很少共同控制一批肉鸡，如图 3.12 所示。

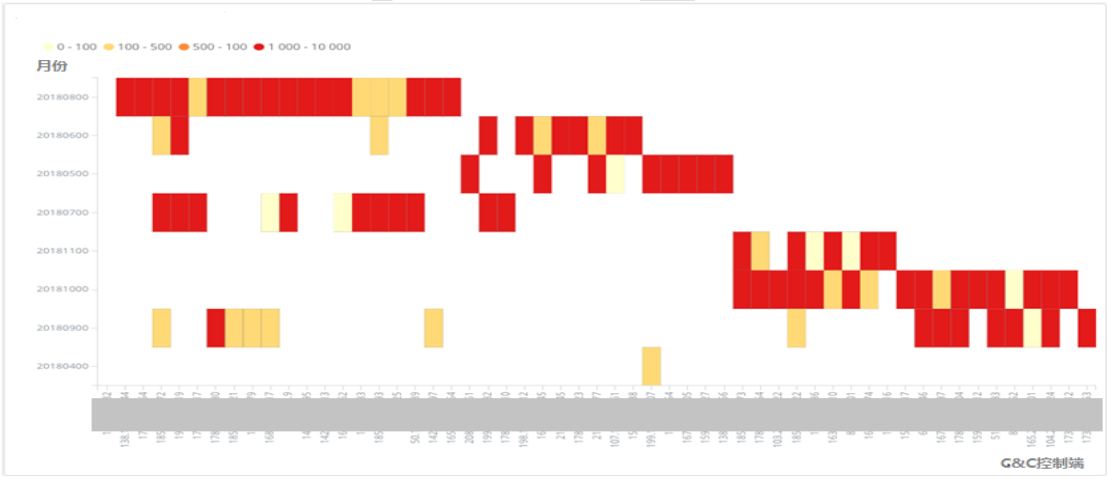

图 3.12 Gafgyt 家族的月度僵尸网络控制规模

Gafgyt 僵尸网络家族 C&C 控制端月活和日活情况如图 3.13 所示，月度攻击目标热度如图 3.14 所示。平均每个控制端活跃 1.3 个月，每个月平均活跃 3.44 天，每个月平均针对 29 个攻击目标发起攻击。

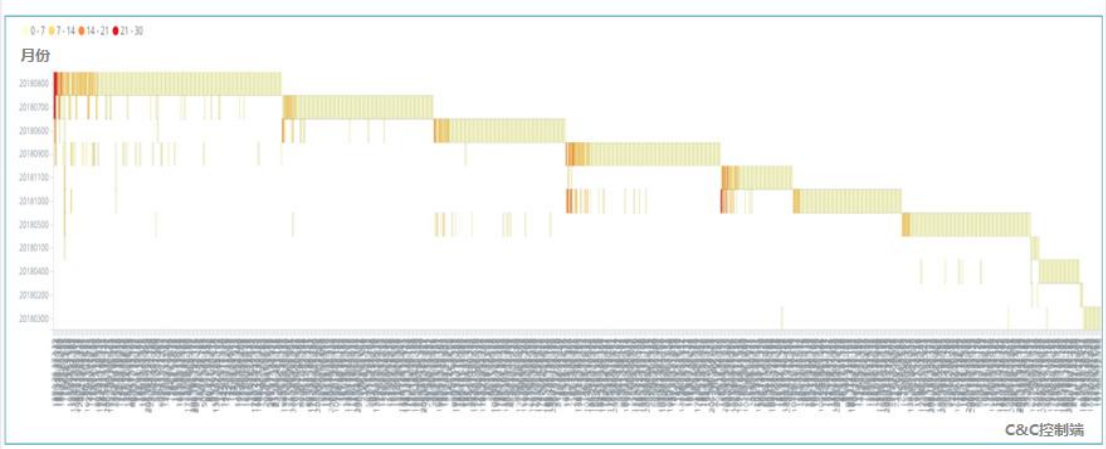

图 3.13 Gafgyt 僵尸网络家族 C&C 控制端月度日活跃热度

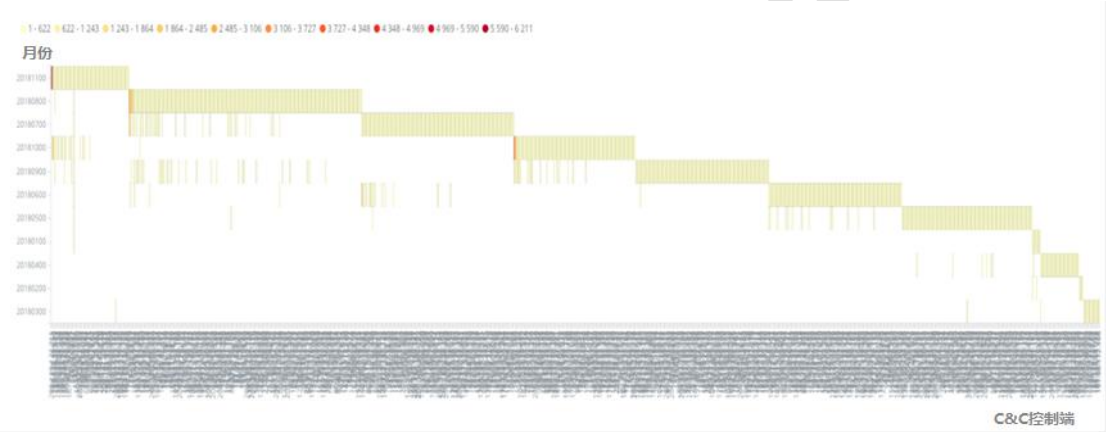

图 3.14 Gafgyt 僵尸网络家族 C&C 控制端月度攻击目标数量热度

3.3 BillGates 僵尸网络家族

BillGates 僵尸网络家族在全年 12 个月持续活跃，总活跃 C&C 控制端 IP 数量为 569 个,单个 C&C 存活时间最长为 11 个月,仅有 147 个 IP 存活时间超过一个月，而有 150 个 C&C 只出现一天。该家族的 C&C 数目全年保持较稳定的数量，在 10 月份达到全年最高峰，如图 3.15 所示。该家族对僵尸网络的控制规模在 5 月份达到顶峰，单个 C&C 最多控制 15010 个肉鸡，从 6 月份开始大幅下滑，在 8 月份逐渐缓慢扩大对僵尸网络的控制规模，并于 10 月份达到下半年的顶峰，

当月单个 C&C 最高控制了将近 5694 个肉鸡，仅全年最高峰的三分之一，如图 3.16 所示。利用该家族发起 DDoS 攻击的被攻击目标的月度分布如图 3.17 所示，全年的攻击目标数量呈现一定的波动上升趋势。

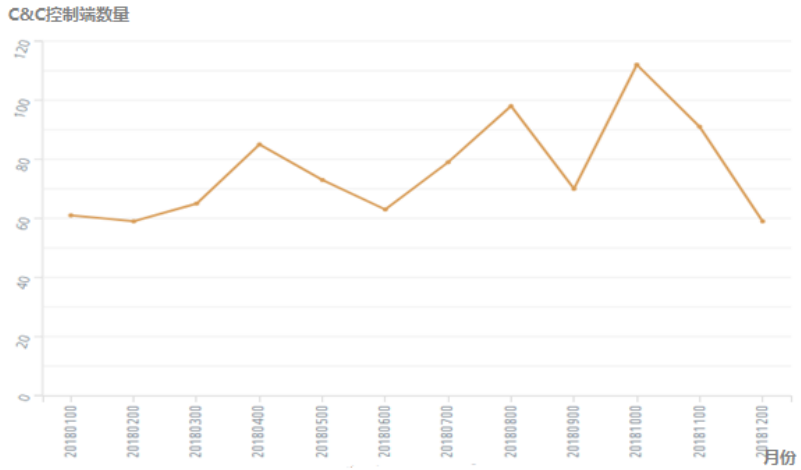

图 3.15 BillGates 僵尸网络家族 C&C 控制端月度数量分布

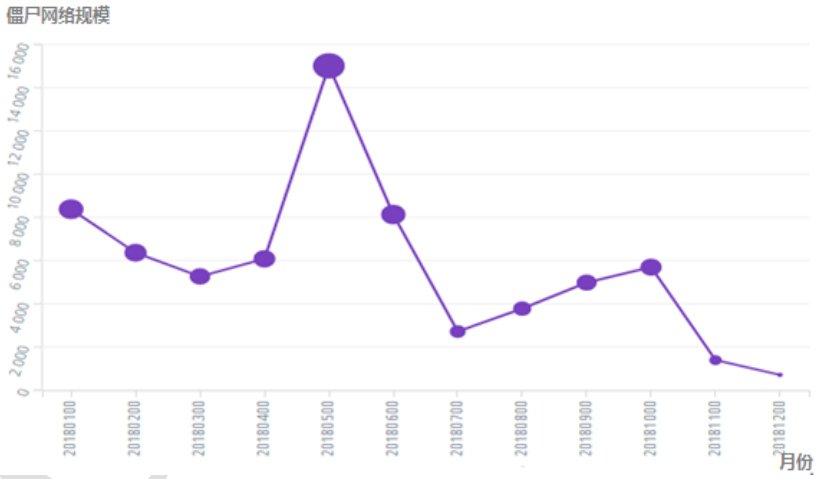

图 3.16 BillGates 僵尸网络家族控制规模月度分布

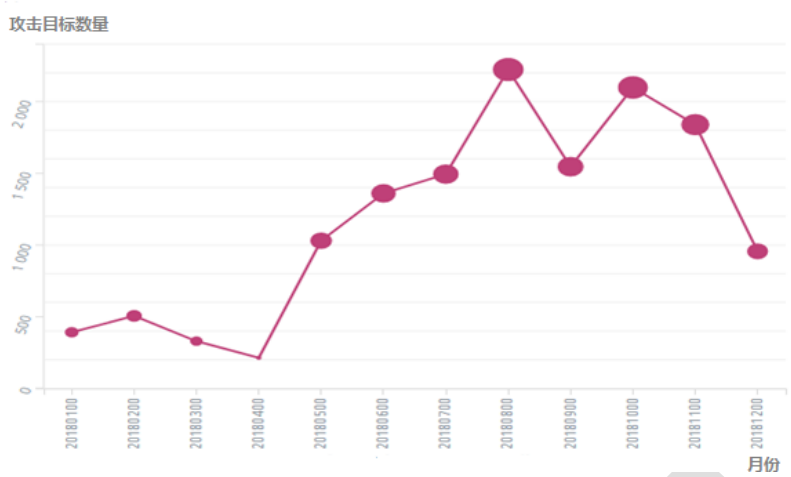

图 3.17 BillGates 僵尸网络家族的攻击目标月度分布

从攻击发起时间看，该家族与 XorDDoS 僵尸网络家族的情况极为相似，同样疑似是需要由人工触发的攻击方式。在凌晨 2 点到 10 点内，发起的攻击数量呈现明显下降，可能与作息时间相关，从攻击发起时间分布猜测，一方面，可能这是控制者的晚睡时间，另一方面也有可能是因为控制者的攻击目标在该时间段内都处于活跃低谷，没有攻击价值，如图 3.18 所示。

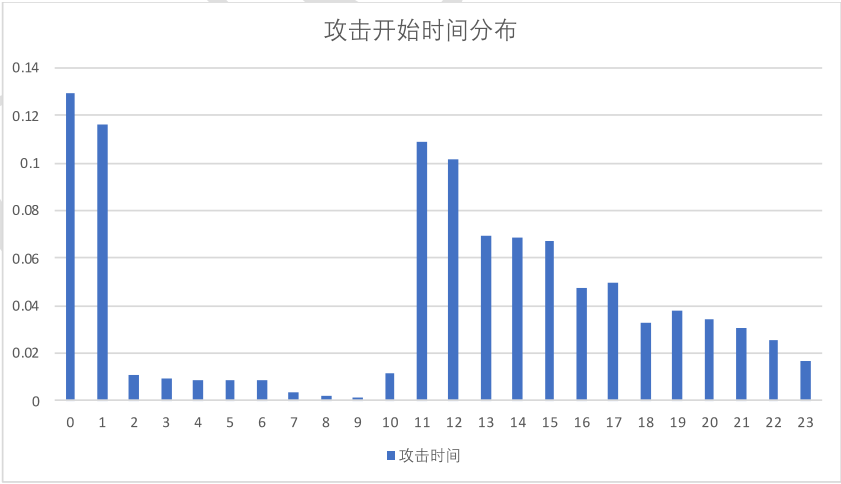

图 3.18 BillGates 僵尸网络家族攻击发起时间分布

BillGates 僵尸网络家族 C&C 控制端月活和日活情况如图 3.19 所示，月度攻击目标热度如图 3.20 所示。平均每个控制端活跃 1.6

个月，每个月平均活跃 5 天，每个月平均针对 96 攻击目标发起攻击；其中有 3 个控制端的活跃月度超过 7 个月，且每个月的平均活跃天数超过 18 天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为 974 个。

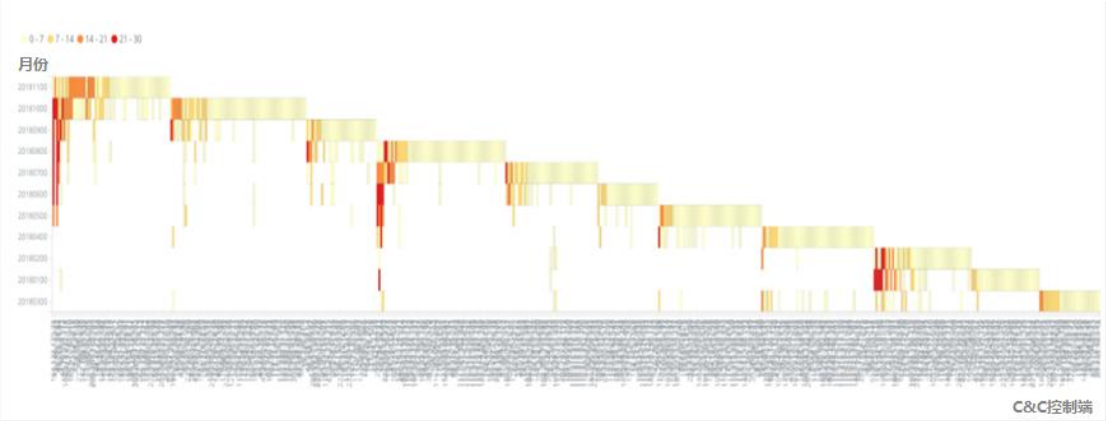

图 3.19 BillGates 僵尸网络家族 C&C 控制端月度日活跃热度

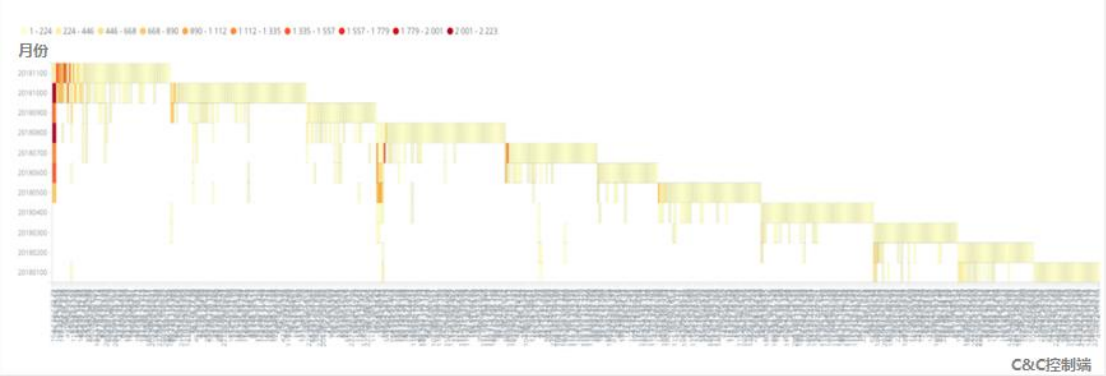

图 3.20 BillGates 僵尸网络家族 C&C 控制端月度攻击目标数量热度

四、 重点攻击团伙分析

4.1 团伙 G1：C&C 数量及肉鸡规模最大的攻击团伙

4.1.1 团伙 G1 总览

团伙 G1 在 2018 年全年持续活跃，共拥有 C&C 控制端 IP 数量 283 个，肉鸡规模超过 57 万，攻击目标超过 2 万个。该团伙能够利用多个僵尸网络家族发起攻击，XorDDoS 和 BillGates 家族的 C&C 控制端是该团伙的重点利用资源。该团伙的活跃 C&C 控制端数量在 4 月、5 月、6 月、12 月的数量最多，如图 4.1 所示；活跃僵尸网络肉鸡数量在 11 月、12 月的数量有大幅提升，如图 4.2 所示；攻击目标数量在 8 月、11 月的数量最多，如图 4.3 所示；攻击目标的地理归属主要位于我国境内，特别是浙江省、福建省和广东省，如图 4.4 所示。

图 4.1 团伙 G1 月度活跃 C&C 数量

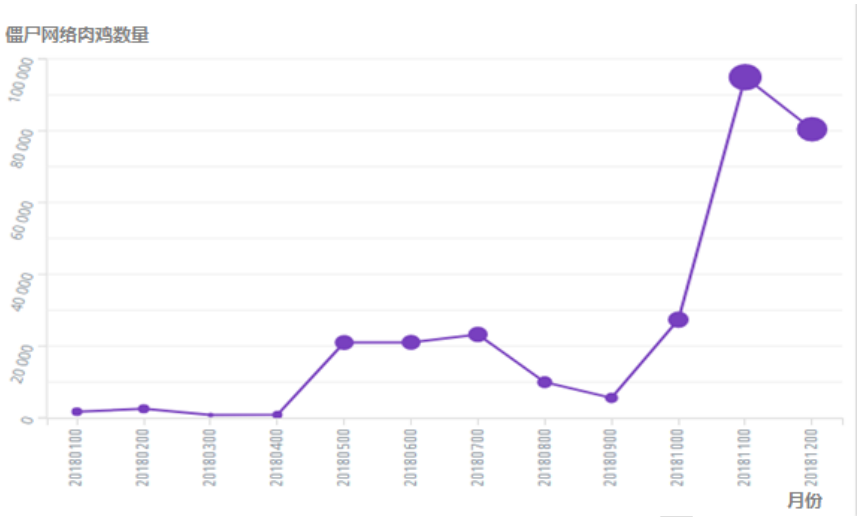

图 4.2 团伙 G1 月度活跃僵尸网络肉鸡数量

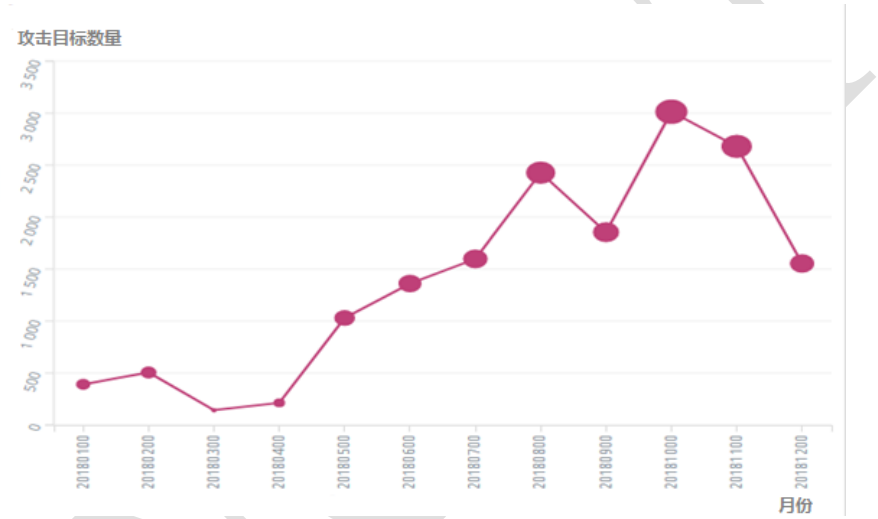

图 4.3 团伙 G1 的月度攻击目标数量

图 4.4 团伙 G1 的攻击目标归属国家和地区分布

团伙 G1 的 C&C 控制端月活和日活情况如图 4.5 所示，月度攻击目标热度如图 4.6 所示。图中可示，在 283 个 CC 控制端中，平均每

个控制端活跃 1.77 个月，每个月平均活跃 9.7 天，每个月平均针对 397 攻击目标发起攻击；其中有 7 个控制端的活跃月度超过 7 个月，且每个月的平均活跃天数超过 20 天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为 1099 个。

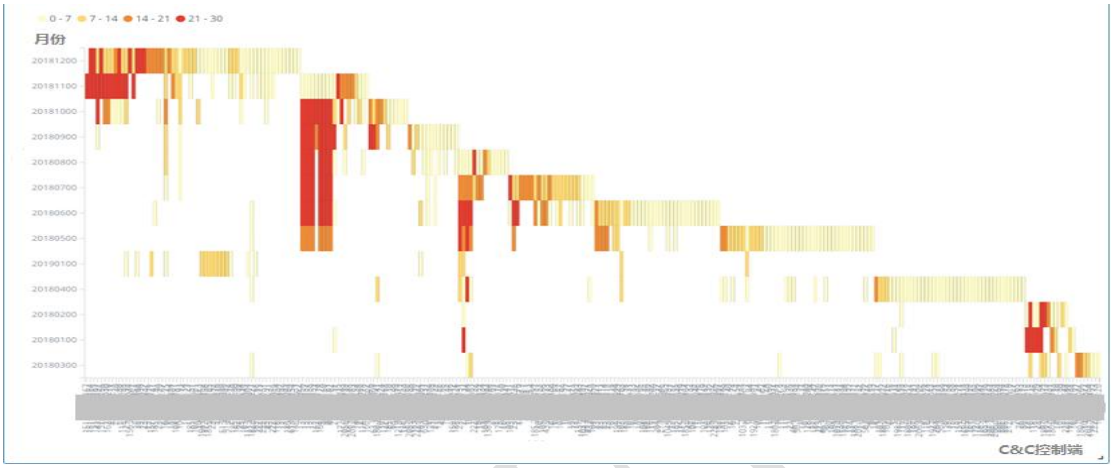

图 4.5 团伙 G1 的 C&C 控制端月度日活跃热度

图 4.6 团伙 G1 的 C&C 控制端月度攻击目标数量热度

团伙 G1 从其攻击发起时间看，符合 XorDDoS 和 Billgates 僵尸网络家族的攻击时间特性，在凌晨 2-10 点期间攻击数量有大幅的下降，在 11-12 点期间为攻击最高峰，如图 4.7 所示。

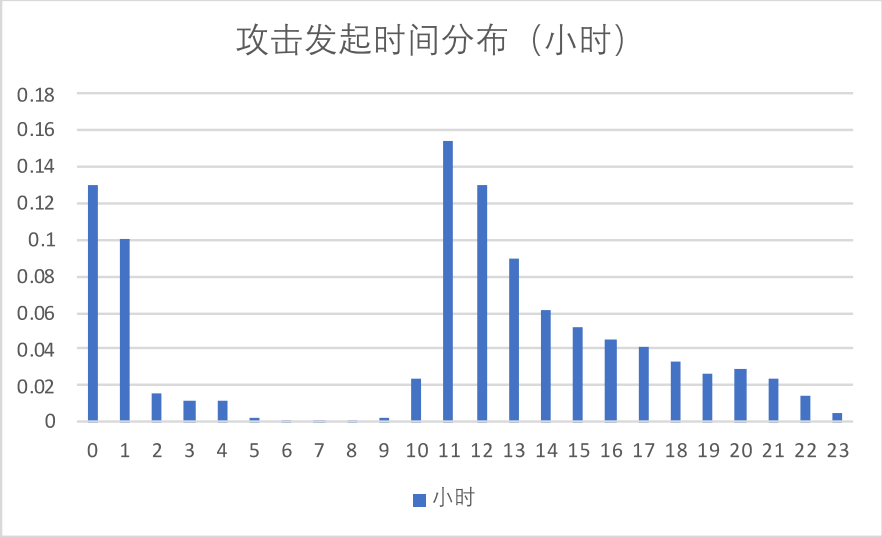

图 4.7 子团伙 G1-2 的攻击开始时间分布

团伙 G1 年度 C&C 和攻击目标的关系拓扑、以及 C&C 和肉鸡的关系拓扑如图 4.8 和图 4.9 所示，红色节点为控制端节点、紫色节点为攻击目标节点、黄色节点为肉鸡节点。从图中可以看到，攻击目标节点及肉鸡节点大量在各自的图的中间聚集，可以看出团伙使用的肉鸡资源和攻击目标具有非常强的重合性。

图 4.8 团伙 G1 年度 C&C 和攻击目标的关系拓扑（C&C 为红色，攻击目标为紫色）

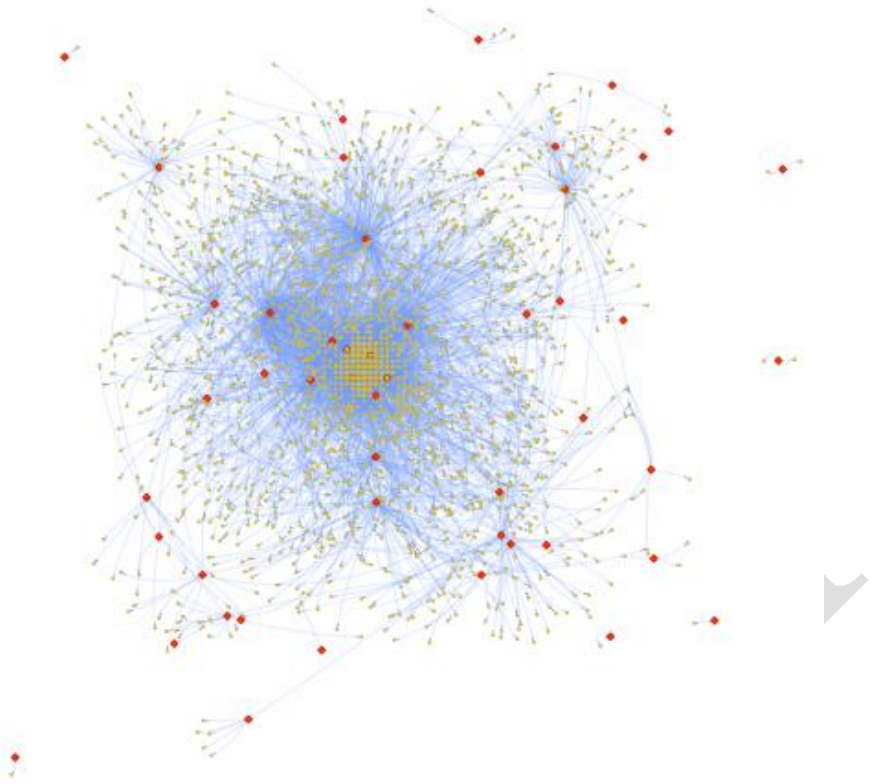

图 4.9 团伙 G1 的 C&C 和肉鸡的关系拓扑（C&C 为红色，肉鸡为黄色）

4.1.2 重要子团伙分析

团伙 G1 中，在各个月份出现的 C&C 控制端的攻击目标非常集中，但是它可以根据攻击资源的复用情况拆分成若干主要的子团伙，最重要的子团伙有以下三个:

一、 子团伙 G1-1

该子团伙在 3 月份首次出现，此后在每月均活跃，共包含了 23 个 C&C 控制端，主要利用 BillGates 僵尸网络发动攻击。该子团伙每个月的控制端平均在 1-7 个之间，如图 4.10 所示，其所利用的肉鸡

主要位于我国境内的北京、上海、浙江等省市，攻击目标主要位于我国境内的福建、广东、浙江等省市，如图 4.11 和图 4.12 所示。

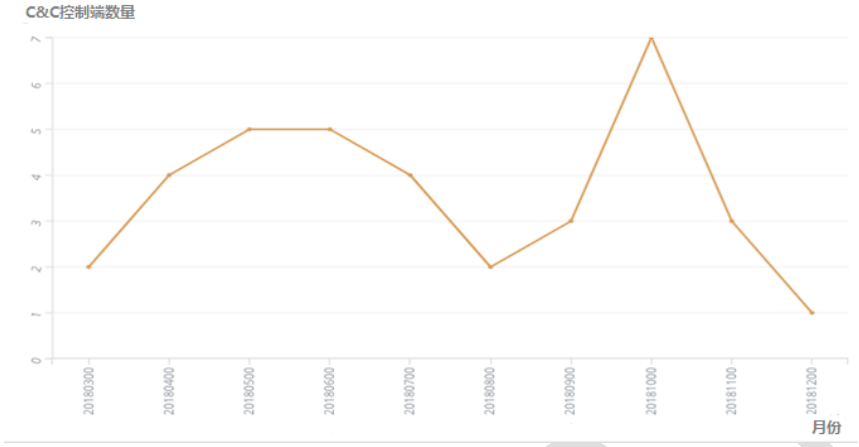

图 4.10 子团伙 G1-1 的月度活跃 C&C 数量

图 4.11 子团伙 G1-1 控制的肉鸡所属国家和地区分布

图 4.12 子团伙 G1-1 攻击目标所属国家和地区分布

二、 子团伙 G1-2

子团伙 G1-2 首次出现在 5 月，此后每月均活跃，共包含 13 个 C&C 控制端 IP，主要利用 XorDDoS 发动攻击。该子团伙的控制端数量

在 5-10 月保持在 8-9 个，在 11 月份增加为 12 个，随后在 12 月份下降为 5 个，如图 4.13 所示；同样，该子团伙僵尸网络肉鸡数量在 11 月份达到顶峰，当月肉鸡规模超过 7 万台，随后有一定程度的下降，如图 4.14 所示。该团伙的控制端绝大部分都位于法国，仅在 10 月份短暂切换到韩国的服务器 IP。从每月的攻击天数来看，该团伙基本每月都活跃 25 天以上。从攻击目标数目来看，该团伙的从 8 月份开始的攻击任务开始上升，如图 4.15 和图 4.16 所示。

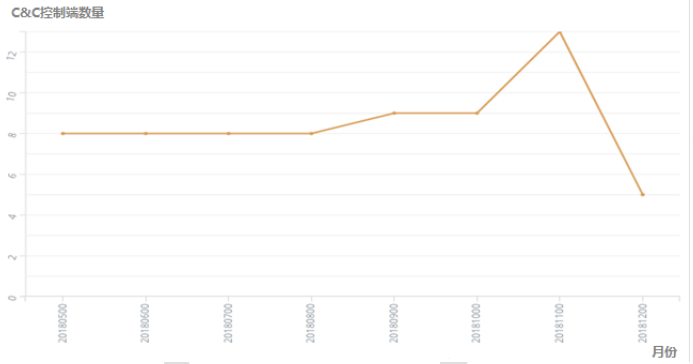

图 4.13 子团伙 G1-2 的月度活跃 C&C 数量

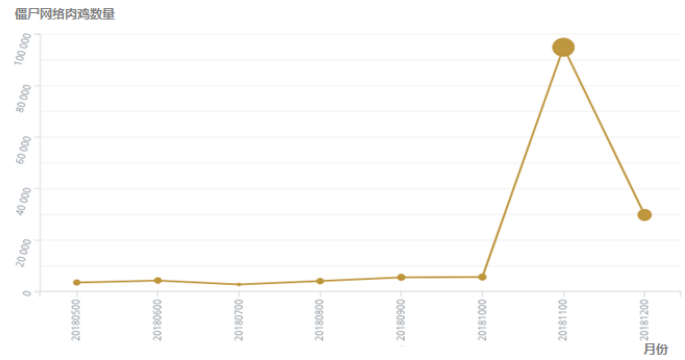

图 4.14 子团伙 G1-2 的月度活跃僵尸网络肉鸡数量

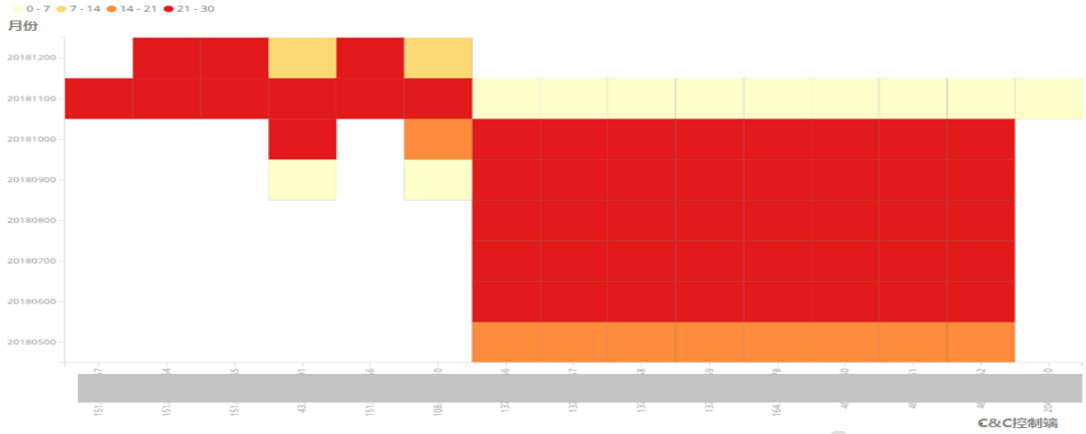

图 4.15 子团伙 G1-2 的月度活跃天数

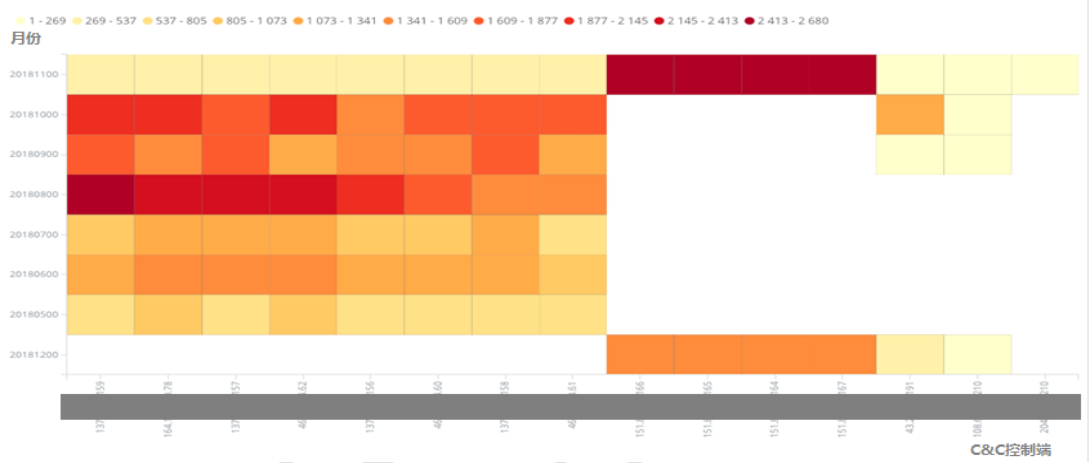

图 4.16 子团伙 G1-2 的月度攻击目标数目

子团伙 G1-2 所利用的肉鸡地址绝大部分是位于我国境内的江苏、广东、福建等省份，涉及大量的家用宽带用户，如图 4.17 所示；其攻击目标绝大部分都为 IDC 机房，主要包含位于杭州的阿里云服务器、位于福州和佛山电信/联通 IDC 机房、及位于北京的腾讯云服务器，如图 4.18 所示。

图 4.17 子团伙 G1-2 的肉鸡所属国家和地区分布

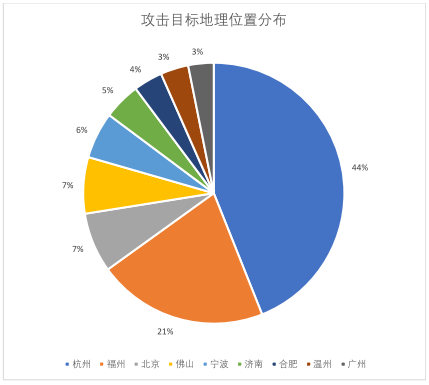

图 4.18 子团伙 G1-2 的攻击目标所属省份分布

从子团伙 10 月以前的肉鸡和 C&C 的关系见图 4.19，该团伙的每个 C&C 主要控制不同部分的肉鸡，仅有小部分肉鸡在一月内被多个 C&C 控制，然而在 11 月份，该团伙的大部分 C&C 都消亡，所有的肉鸡的控制权均转移至某特定网段的控制端 IP，如图 4.20 所示。

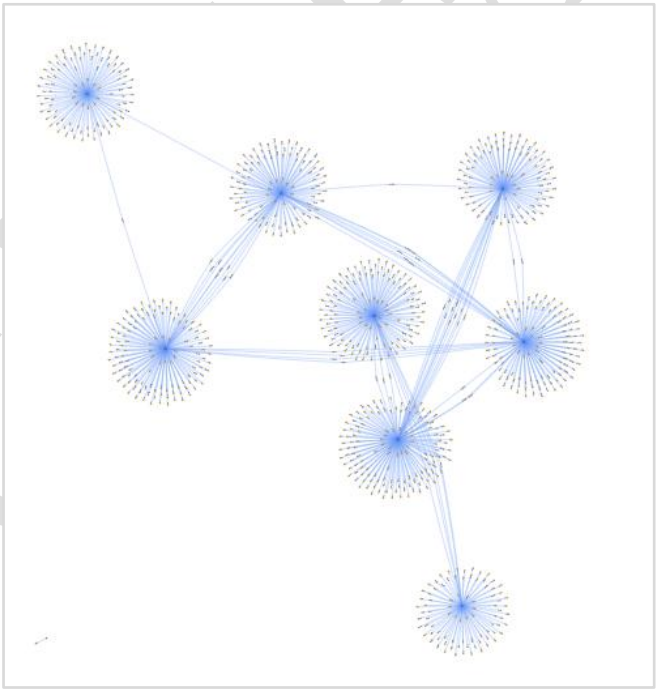

图 4.19 10 月以前子团伙 G1-2 的 C&C 与肉鸡的关系图

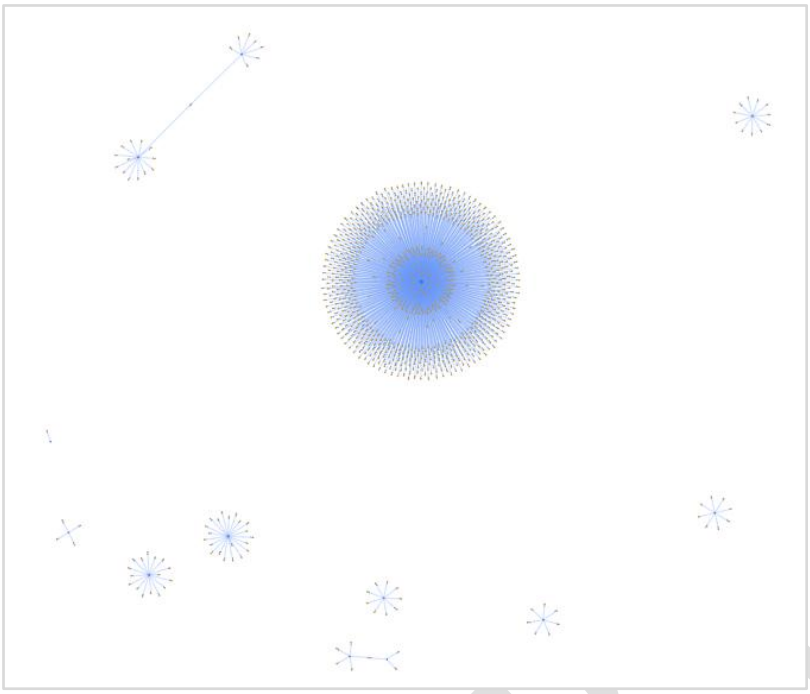

图 4.20 11 月份子团伙 G1-2 的 C&C 与肉鸡的关系图

子团伙 G1-2 的主要攻击目标主要为游戏行业和博彩业，仅在 11 月份攻击的游戏业相关 IP 达到 200 余个，关联域名 400 余个；博彩相关 IP 就达到 53 个，关联域名两百余个，攻击目标样例如图 4.21 所示。

博彩	色情	游戏外挂网站	游戏主页
			

图 4.21 子团伙 G1-2 的攻击目标样例

CNCERT 对该子团伙进行了长期跟踪，监测发现该子团伙使用了大量包含特定字符串的恶意域名。该子团伙与某 2014 年被发现的公开组织相关，该组织与游戏私服、色情、赌博等产业联系紧密。CNCERT

于 2017 年中心溯源分析的数千起大流量攻击事件中，监测发现这些域名涉及了其中多起事件，且在 2017 年 8 月左右非常活跃，此后沉寂了半年多的时间，在 2018 年 5 月开始又重新活跃起来。

三、 子团伙 G1-3

子团伙 G1-3 只在 6，7 月份活跃，共包含 6 个 C&C 控制端 IP，集中在境外某特定网段，主要利用 XorDDoS 僵尸网络发动攻击。该子团伙的主要攻击目标大量位于我国境内，如图 4.22 所示。

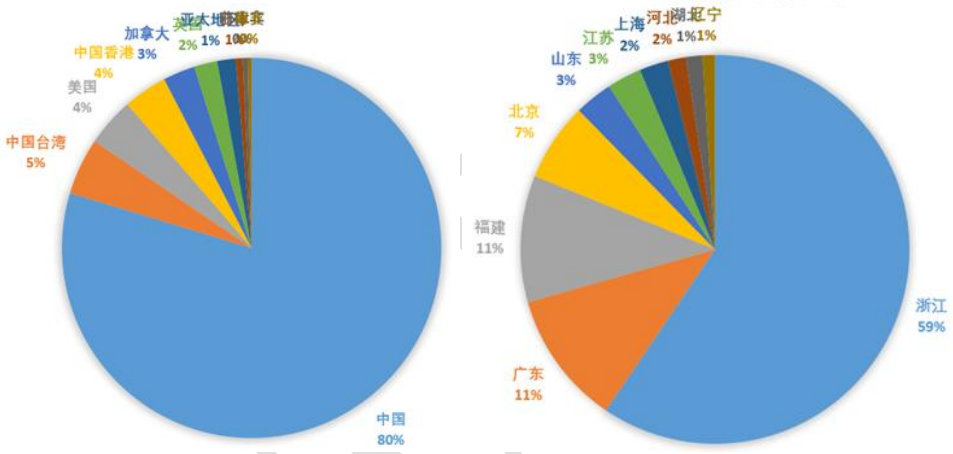

图 4.22 子团伙 G1-3 的攻击目标所属国家或地区 TOP10

4.2 团伙 G13：肉鸡规模第二大的攻击团伙

团伙 G13 全年的活跃时长为两个月，最初活跃时间为 2018 年 6 月，最近活跃时间为 2018 年 8 月，共包含 4 个 C&C 控制端，均位于我国境外，总共控制了 1.3 万台肉鸡，攻击目标总共 5440 个。该团伙所利用的肉鸡资源主要分布在我国境内，特别是江苏、广东、河南、浙江等省份，主要攻击目标为境外，特别是美国、加拿大、意大利等

国家的 VPS，如图 4.23 和图 4.24 所示。该团伙主要利用 Gafgyt 僵尸网络家族发动攻击。

图 4.23 团伙 G13 的肉鸡所属国家和地区分布

图 4.24 团伙 G13 的攻击目标所属国家和地区分布

团伙 G13 的 C&C 控制端月活和日活情况如图 4.25 所示，月度攻击目标热度如图 4.26 所示。在 5 个 CC 控制端中，平均每个控制端活跃 2 个月，每个月平均活跃 8 天，每个月平均针对 500 个攻击目标发起攻击；其中有 2 个控制端的活跃月度达到 3 个月，且每个月的平均活跃天数超过 15 天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为 1456 个。

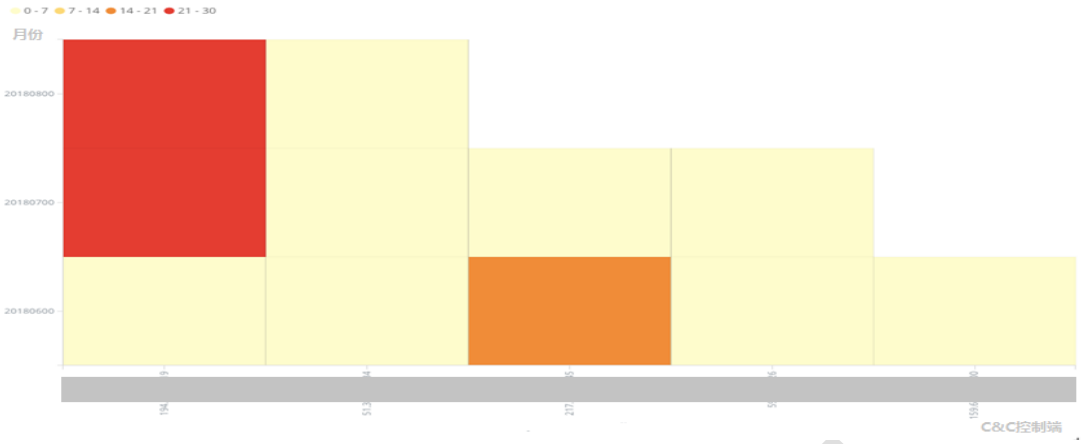

图 4.25 团伙 G13 的 C&C 控制端月度日活跃热度

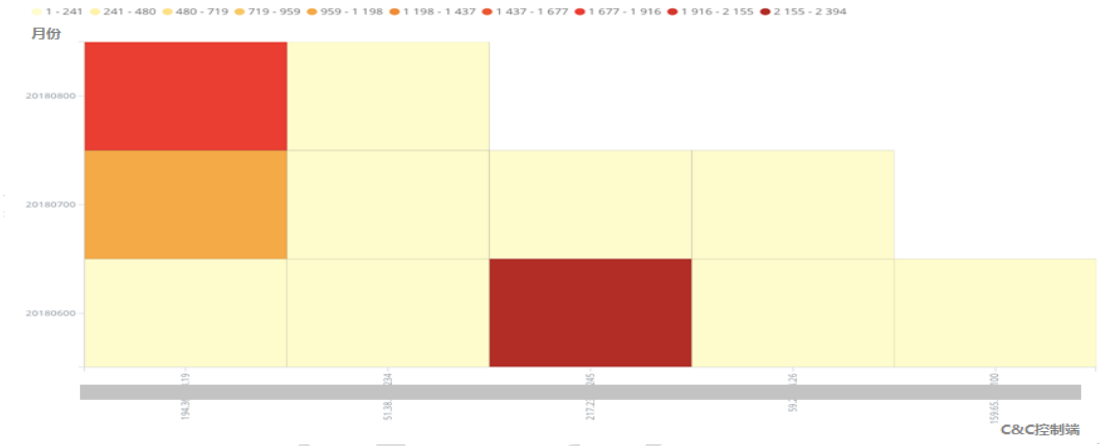

图 4.26 团伙 G13 的 C&C 控制端月度攻击目标数量热度

团伙 G13 的 C&C 和攻击目标的关系拓扑、以及 C&C 和肉鸡的关系拓扑如图 4.27 和图 4.28 所示，红色节点为控制端节点、紫色节点为攻击目标节点、黄色节点为肉鸡节点。从图中可以看到，攻击目标节点大量在图的中间聚集，可以看出团伙使用的攻击目标具有非常强的重合性，而团伙中每个 C&C 控制端所控制的肉鸡资源则围绕控制端节点分散开来，相对比较独立。

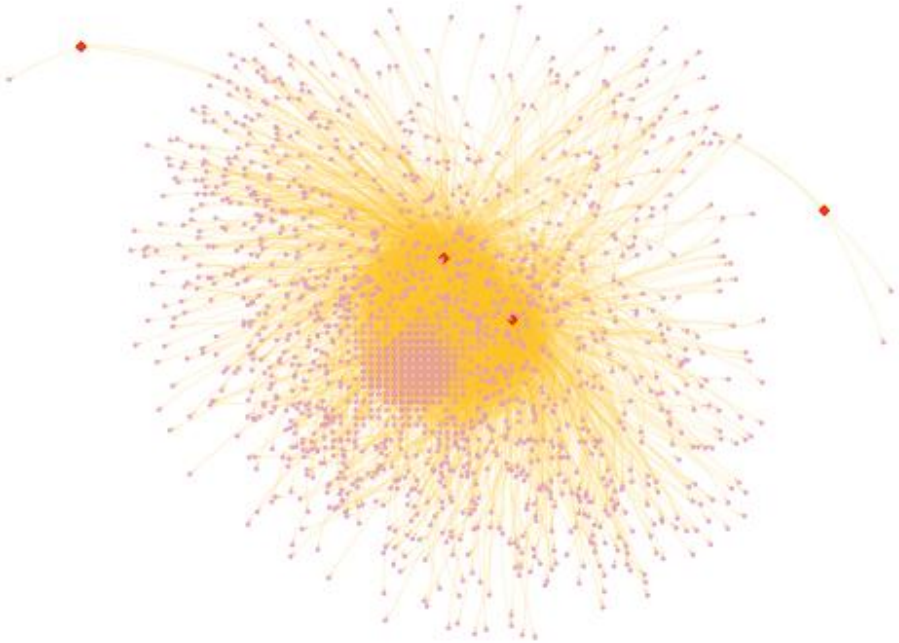

图 4.27 团伙 G13 年度 C&C 和攻击目标的关系拓扑（C&C 为红色，攻击目标为紫色）

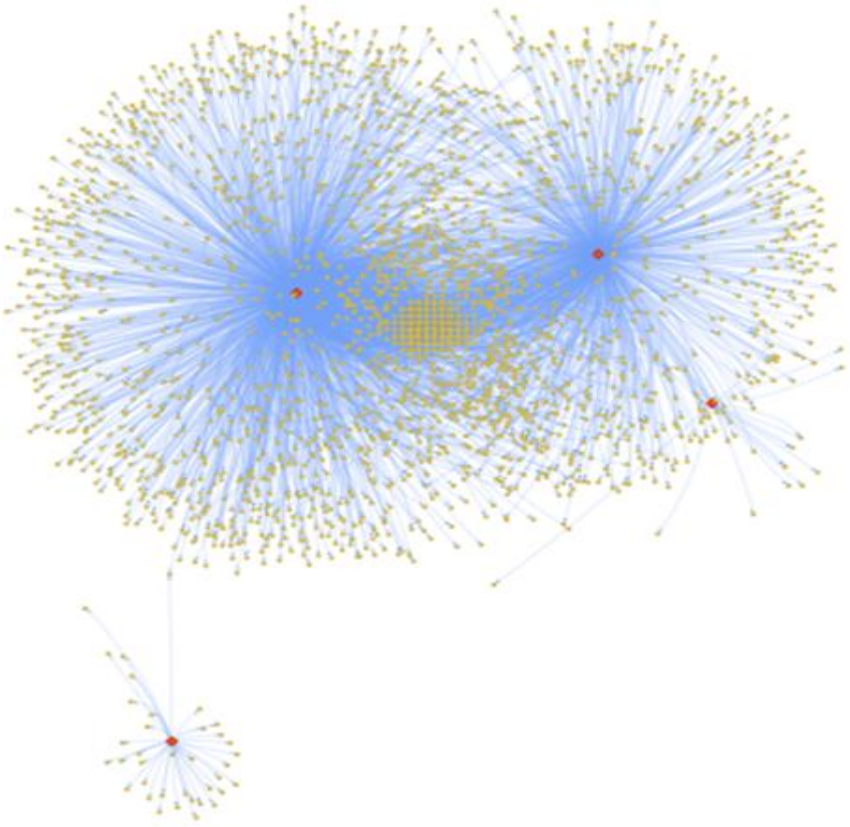

图 4.28 团伙 G13 的 C&C 和肉鸡的关系拓扑（C&C 为红色，肉鸡为黄色）

4.3 团伙 G9：肉鸡规模排名第三的团伙

团伙 G9 全年活跃时长为两个月，活跃时间从 2018 年 5 月 11 日到 2018 年 7 月 12 日，共包含 9 个 C&C 控制端，均归属美国、荷兰等境外国家，共控制 13035 个肉鸡，攻击目标为 642 个。该团伙主要利用 Gafgyt 僵尸网络家族发动攻击。该团伙所利用的大部分肉鸡资源都位于我国境内，主要位于北京、广东、浙江等省市，攻击的目标大量为我国福建省的电信 IDC 机房，还有许多境外的 IDC 机房，如图 4.29 和 4.30 所示。

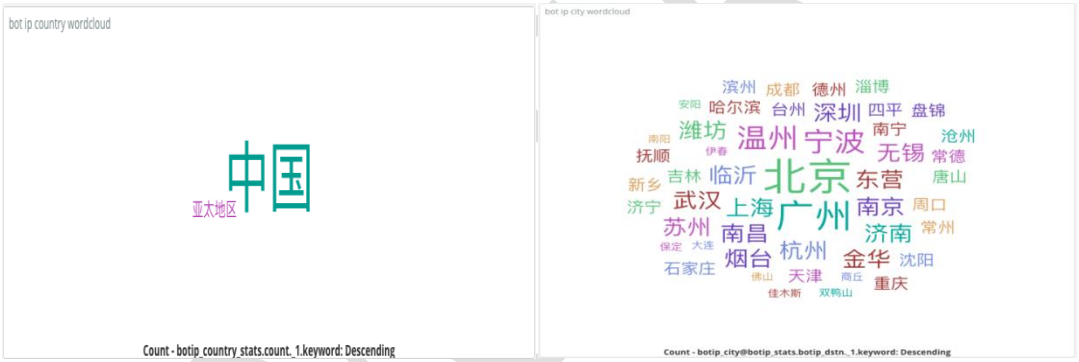

图 4.29 团伙 G9 利用的肉鸡资源所属国家或地区分布

图 4.30 团伙 G9 的攻击目标所属国家或地区分布

团伙 G9 的 C&C 控制端月活和日活情况如图 4.31 所示，月度攻击目标热度如图 4.32 所示。图中可示，在 9 个 CC 控制端中，平均每个

控制端活跃 1.5 个月，每个月平均活跃 2.57 天，每个月平均针对 47 攻击目标发起攻击；其中有 5 个控制端的活跃月度达到 2 个月，且每个月的平均活跃天数超过 3 天，这些控制端同时也是发起攻击最多的攻击源，平均每个月攻击的目标数量为 66 个。

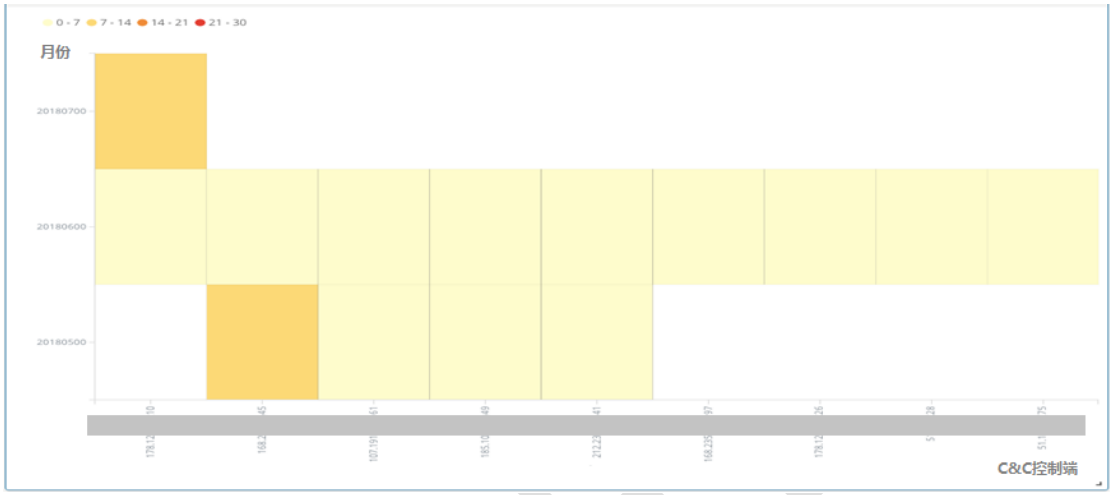

图 4.31 团伙 G9 的 C&C 控制端月度日活跃热度

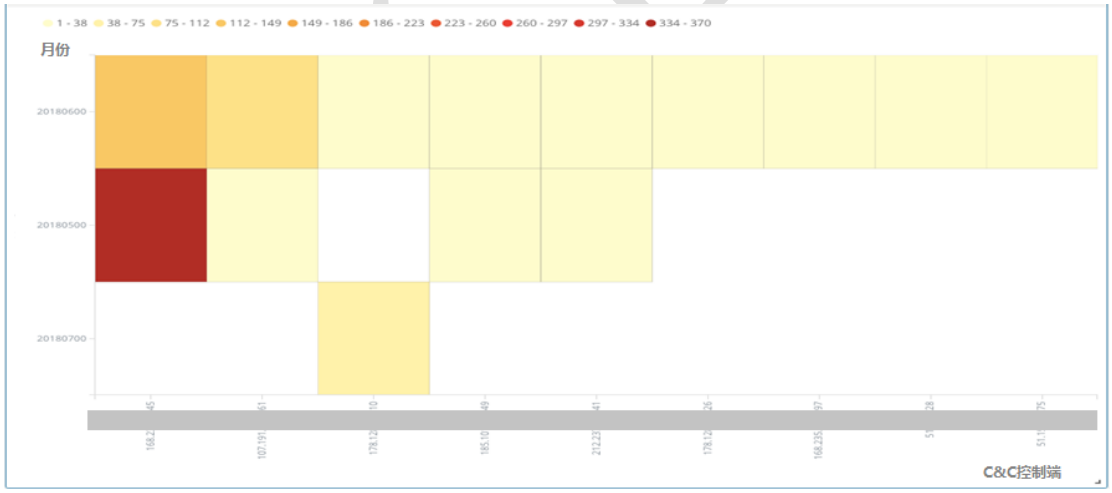

图 4.32 团伙 G9 的 C&C 控制端月度攻击目标数量热度

团伙 G9 的 C&C 和攻击目标的关系拓扑、以及 C&C 和肉鸡的关系拓扑如图 4.33 和图 4.34 所示，可以看出团伙 G9 的攻击目标具有一定的重合性，而团伙中每个 C&C 控制端所控制的肉鸡资源围绕控制端节点分散开来，相对较为独立。

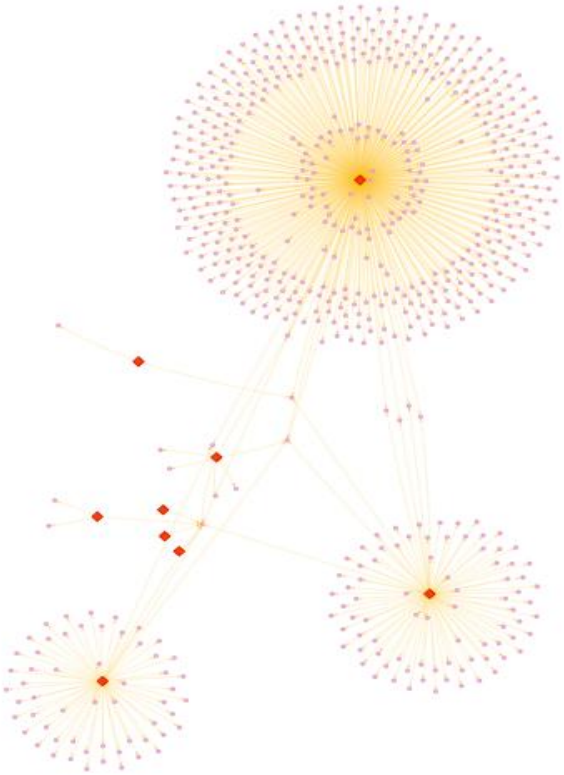

图 4.33 团伙 G9 的 C&C 控制端及攻击目标和的关系拓扑（C&C 为红色，攻击目标为紫色）

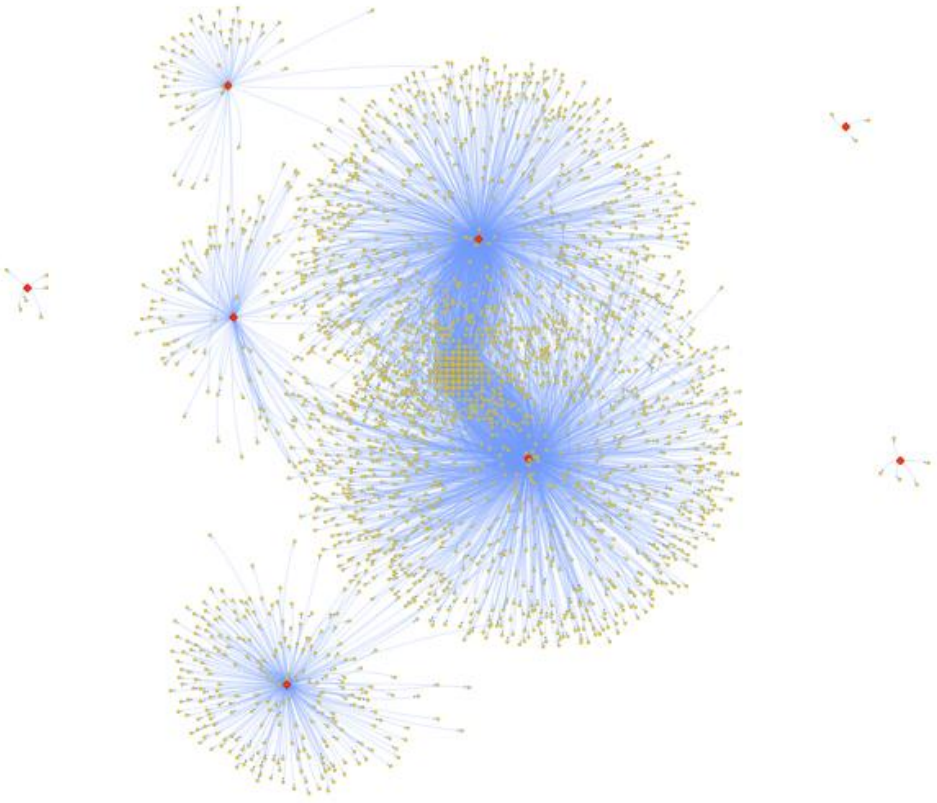

图 4.34 团伙 G9 的 C&C 和肉鸡的关系拓扑（C&C 为红色，肉鸡为黄色）

4.4 团伙 G16：利用 Gafgyt 僵尸网络家族的月度最大团伙

团伙 G16 全年只在 8 月份活跃了一个月，是 Gafgyt 僵尸网络家族中的控制端节点较为普遍的活跃形式，也是月度最大的团伙。只有一个 C&C 控制端是该团伙的核心控制端，如图 4.35 所示，图中最大的蓝色节点就是核心控制端，大部分攻击都由其所控制的肉鸡完成，其余的小部分攻击目标由多个 C&C 共同完成攻击。该团伙在 2018 年 8 月份控制了 1.1 万台肉鸡，由 74 个 C&C 共同控制。从该团伙攻击的目标 IP 相关域名来看，其主要攻击虚机主机运营商。

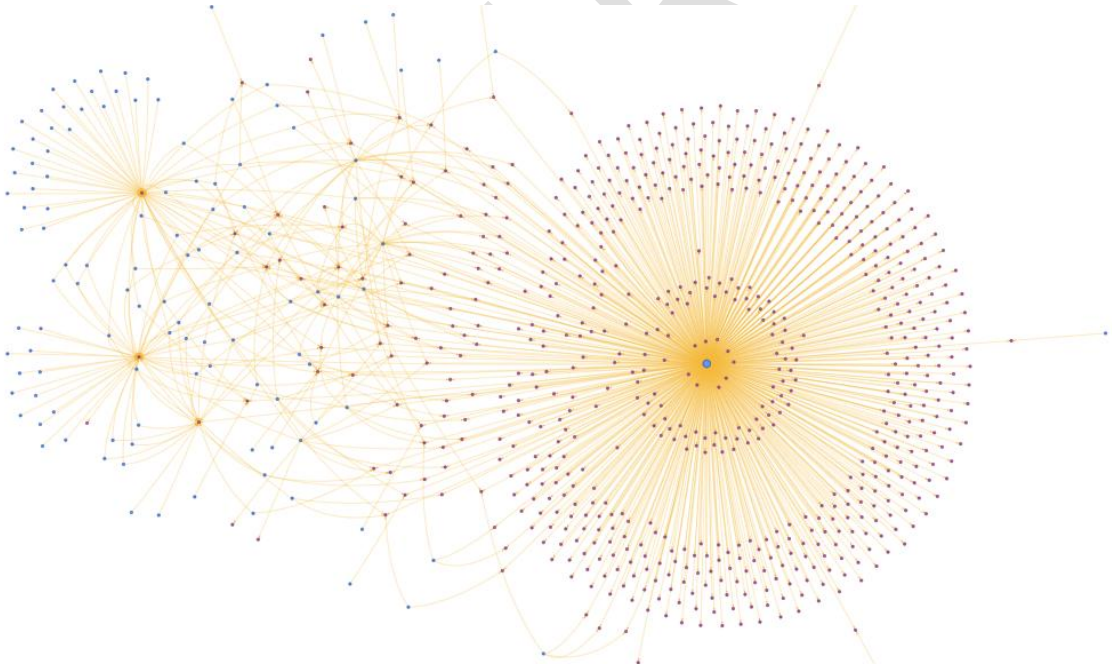

图 4.35 Gafgyt 家族的 C&C 中控制规模最大的团伙 G16（C&C 和攻击目标的关系）