网络安全威胁态势分析 年报

2020 年报

绿盟威胁情报中心

https://nti.nsfocus.com

目录

表格索引

插图索引

1. 网络安全态势综述

1.1 漏洞态势综述

2020 年绿盟科技安全漏洞库共收录 6397 个漏洞[1]，其中高危漏洞 1859 个，微软高危漏洞 395 个。漏洞数量按月进行统计，如图 1-1 所示。高危漏洞主要分布在 Microsoft、Adobe、Oracle、Cisco、Google、Apple、IBM、Mozilla、Moxa、Apple 等厂商的主要产品中。

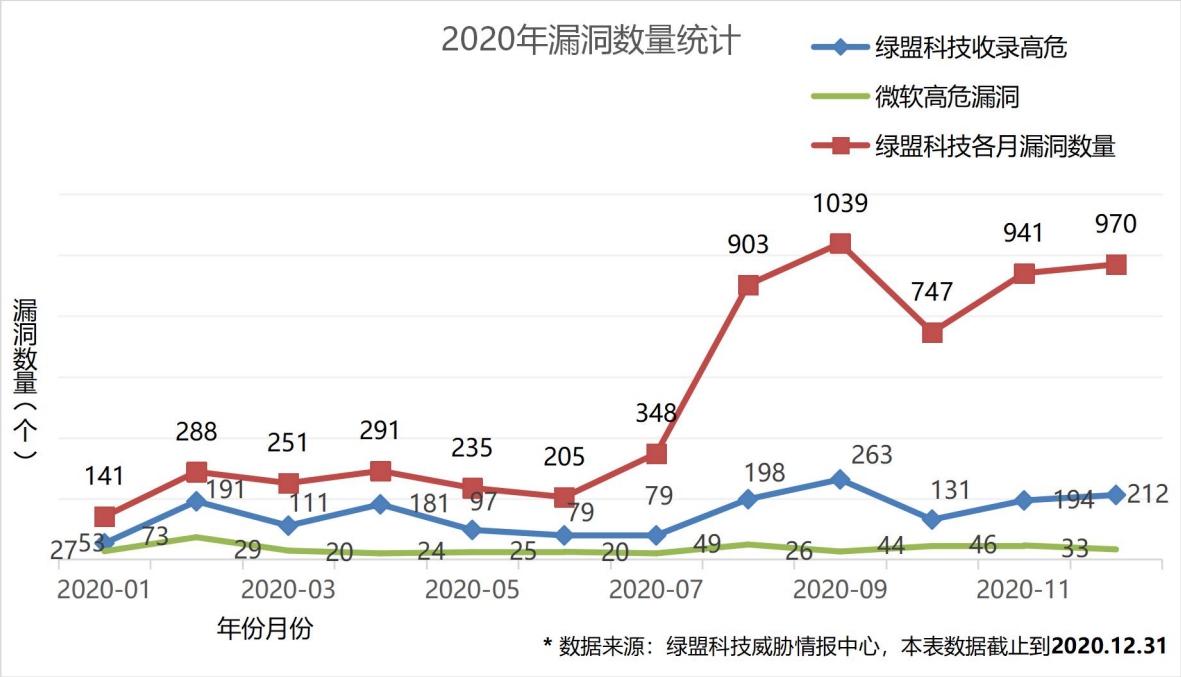

图 1-1 高危漏洞数量统计对比

1.2 恶意软件态势综述

2020 年数据中恶意软件各类型分布如下图所示。后门占比最高 45.96%，其次是挖矿和蠕虫，分别占比 29.42%和 12.55%。木马、勒索、僵尸肉鸡活跃度相对较低，总占比 5%左右。

[1] 绿盟科技漏洞库包含应用程序漏洞、安全产品漏洞、操作系统漏洞、数据库漏洞、网络设备漏洞等；

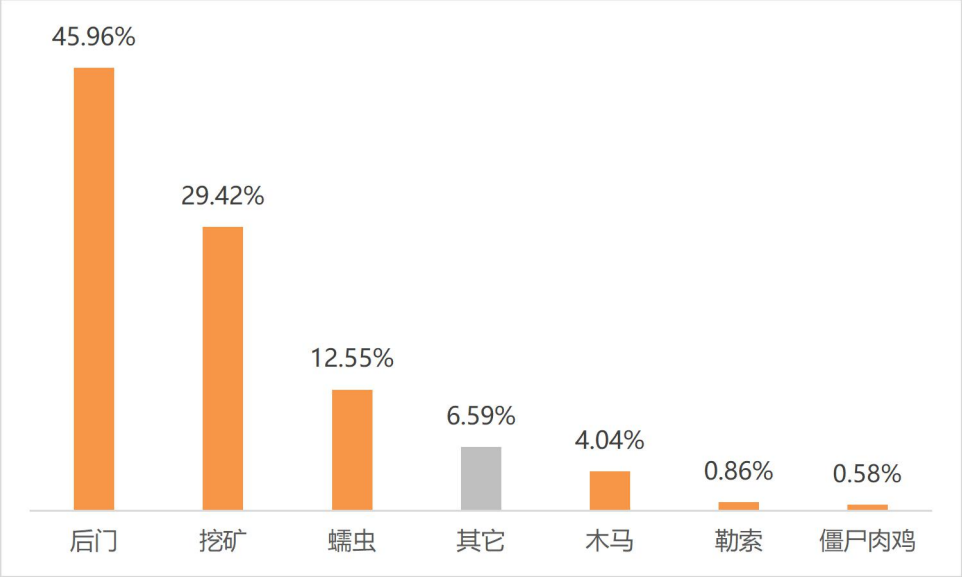

图 1-2 恶意软件类型

1.3 物联网安全态势综述

2020 全年有 9 个值得重点关注的物联网安全事件：

（1） Ripple20 0day 漏洞曝光，扫荡全球各行业数亿台联网设备

（2） 新的 OpenWrt RCE 漏洞曝光，影响数百万台网络设备一组工控蜜罐招来四个零日攻击

（3） CallStranger UPnP 漏洞曝光，影响数十亿台设备黑客利用 DrayTek 设备中的 0day 漏洞对企业网络发动攻击

（4） BadPower：让快速充电器变成手机电脑杀手

（5） 特斯拉废弃零件泄露隐私，谁为用户隐私买单？

（6） 智能门锁暗藏的物联网安全危机

（7） 蓝牙冒充攻击（BIAS），无线安全不可忽视

（8） DHDiscover：可放大近 200 倍的新型反射攻击

（9） 黑客伪造新冠病毒页面传播恶意软件

2020 全年，漏洞利用平台 Exploit-DB 共计出现 197 个物联网相关漏洞利用，以 Netgear 为首的网络设备厂商为主，我们认为出现这种现

象的原因，是网络设备的头部厂商通常出售的设备数量多，基数大，研究人员更关注其相关设备。漏洞利用的类型以 RCE 和 DoS 为主，其中 RCE 类漏洞数量最多，占总量的百分之三十五以上。

2020 年绿盟威胁捕获系统捕获到来自 200,470 个 IP 的 12,015,479 次访问请求日志。其中 68.1%的访问请求是对物联网漏洞进行利用的恶意攻击行为，在 56.76%的访问请求中我们识别到了可疑的 Linux 命令执行、Webshell 扫描、HTTP 代理探测等行为。

1.4 DDOS 攻击态势综述

2020 年，我们监控到 DDoS 攻击次数为 47 万次（event_id 为粒度），攻击总流量 6.6 万 TB 。攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 65%。从一天 24 小时攻击占比来看，11 点到 19 点为攻击高峰攻击。从每周中 DDoS 攻击活动的分布来看，周中（周二、周三、周四）最常被攻击。2020 年主要的攻击类型是 UDP 类型，占总攻击次数的 24%。从流量占比来看，UDP Flood 发起的攻击流量占比最高，占比 67%。全年活跃团伙 45 个。

1.5 僵尸网络及蜜罐态势综述

2020 年的 DDoS 僵尸网络活动中，主要攻击来自 Mirai、Gafgyt 和 Dofloo 等家族。

2020 年的 DDoS 攻击手段主要为 UDP flood、CC 和 TCP flood。

2020 年的僵尸网络控制端主要位于美国，而托管的云服务商中，Digital Ocean、OVH、ColorCrossing 和 Hostwinds 为其优先选项。

2020 检测到的 IoT DDoS 木马传播利用的各类漏洞种类超过了 140 种，其中 CVE-2017-17215（华为 HG532 路由器）、CVE-2014-8361

（Realtek rtl81xx SDK 远程代码执行漏洞）和 ThinkPHP 远程命令执行漏洞位居前列。

2. 漏洞态势

2.1 漏洞类型分析

2020 年收录的 1859 个高危漏洞中，包括输入验证错误、访问验证错误、来源验证错误、边界条件错误、设计错误、资源管理错误、权限错误、配置错误等 22 种漏洞类型。其中 TOP10 数量的漏洞类型如图 2-1 所示。

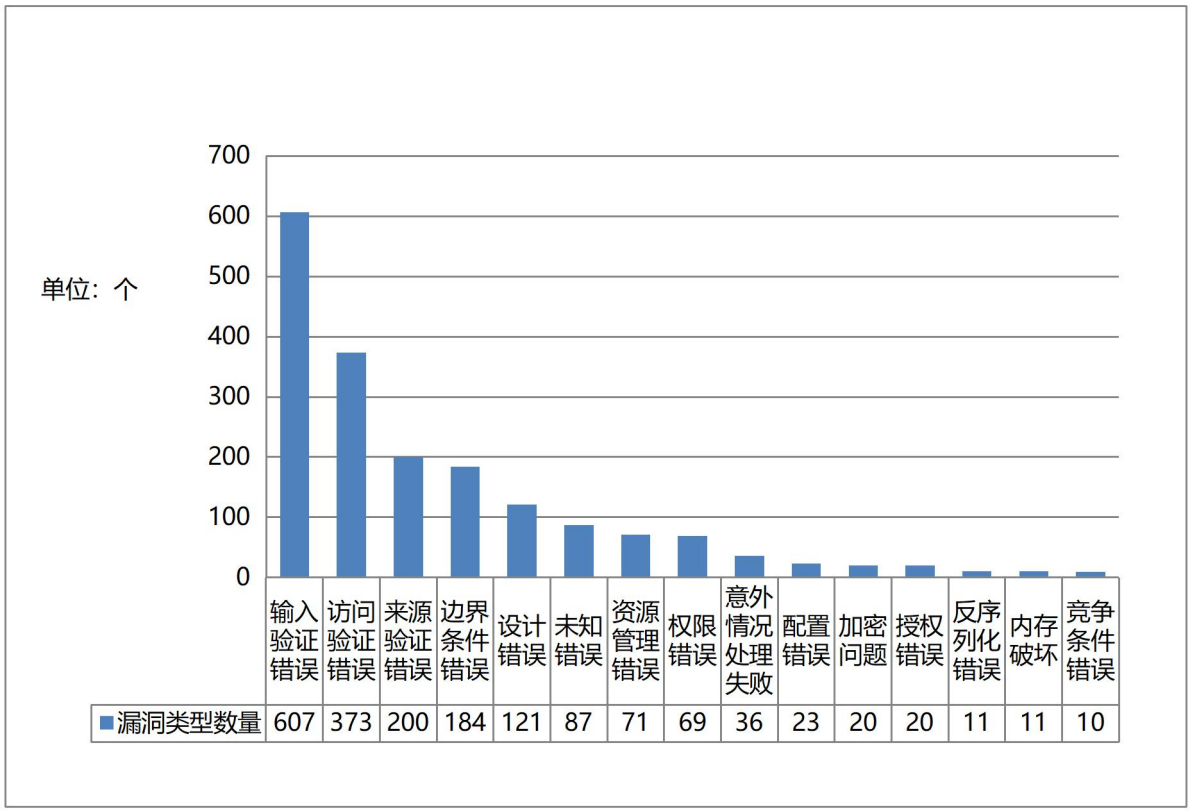

图 2-1 高危漏洞类型数量

2.2 漏洞分布分析

1859 个高危漏洞主要分布在 Microsoft、Adobe、Oracle、Cisco、Google、Apple、IBM、Mozilla、Moxa、Apple 等厂商的主要产品中，共涉及 296

个厂商，其中数量 TOP15 的分布如图 2-2 所示。

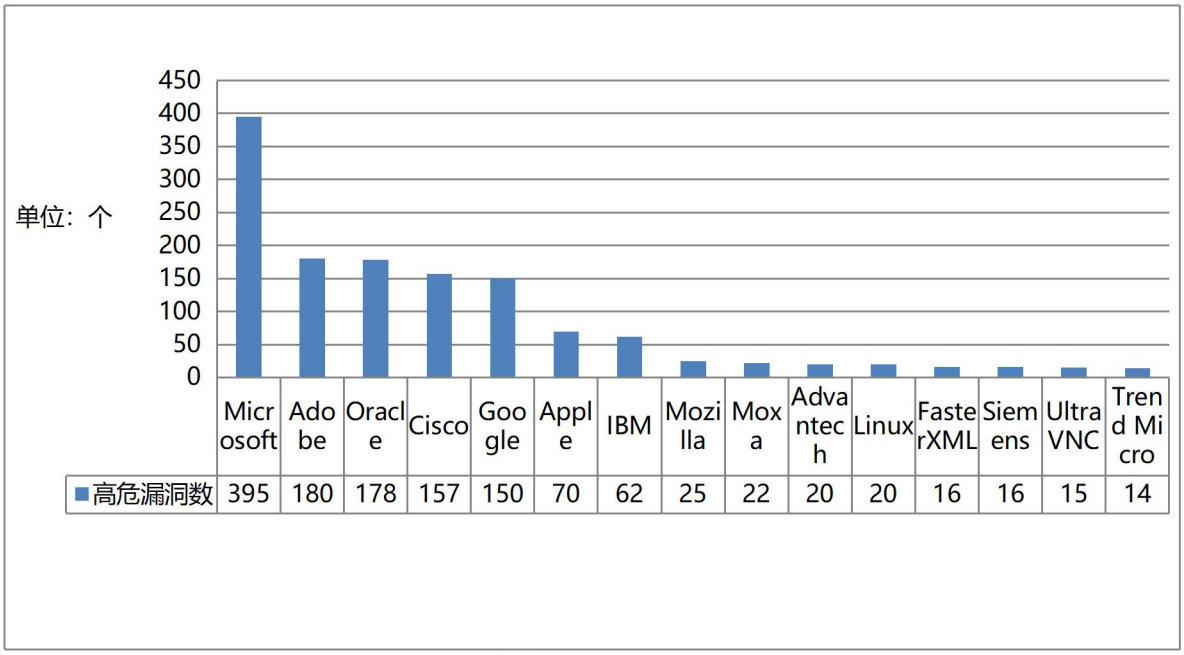

图 2-2 高危漏洞数目

其中 Microsoft 相关的漏洞有 184 个，主要分布在 Microsoft Windows、Microsoft Edge、Chakra Core、Internet Explorer、Microsoft Office、Exchange Server、SharePoint Server、Hyper-V、One Drive、Visual Studio Code 等广泛使用的产品。攻击者可利用这些漏洞执行任意代码、提升权限或造成信息泄露。

Adobe 的漏洞共 180 个，主要分布在 Adobe Acrobat Reader、Adobe Bridge、Adobe ColdFusion、Digital Editions、Adobe DNG SDK、Adobe Dreamweaver 以及 Adobe Flash Player 中。攻击者可利用这些漏洞执行任意代码。

Oracle 的漏洞有 178 个，主要集中于数据库服务器、应用服务器、协作套件、电子商务套件等的多个组件中，其中 Weblogic 的反序列化漏洞在业界备受关注。攻击者可利用这些漏洞执行任意代码、提升权限或造成信息泄露。

Cisco 的漏洞共 157 个，漏洞主要分布在 Cisco IOS XR 软件、Firepower 系统路由器、Nexus 系列交换机、Wireless IP、SD-WAN

vManage 软件等产品中。攻击者可利用这些漏洞执行任意代码、身份验证绕过、信息泄露、权限提升以及拒绝服务。

Google 的漏洞共 150 个，主要分布在 Chrome 浏览器、Android 系统、Android kernel 以及云平台总中。攻击者可利用这些漏洞执行任意代码、提升权限以及拒绝服务。

2.3 2020 年热点漏洞分析

（1） Oracle WebLogic Server 远程代码执行漏洞

CVE-2020-14882

NSFOCUS ID：50493

受影响版本

Oracle WebLogic Server 14.1.1.0.0

Oracle WebLogic Server 12.2.1.4.0

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 10.3.6.0.0

漏洞点评

Oracle Fusion Middleware 的 Oracle WebLogic Server 10.3.6.0.0、12.1.3.0.0、12.2.1.3.0、12.2.1.4.0 和 14.1.1.0.0 版本的 Console 组件存在远程代码执行漏洞。未经身份认证的攻击者可利用该漏洞通过 HTTP 访问网络而破坏 Oracle WebLogic Server 并对其进行接管。

（2） Microsoft Windows Server DNS Server 远程代码执行漏洞

CVE-2020-1350

NSFOCUS ID：47196

受影响版本

Microsoft Windows Server 2019

Microsoft Windows Server 2016

Microsoft Windows Server 2012

Microsoft Windows Server 2008

漏洞点评

Microsoft Windows DNS Server 中存在远程代码漏洞，该漏洞源于程序无法正确处理请求。攻击者可通过发送恶意的请求利用该漏洞在本地系统帐户的上下文中运行任意代码。

（3） Apache Kylin 远程命令执行漏洞

CVE-2020-1956

NSFOCUS ID：46860

受影响版本

Apache Group Kylin 2.3.0 – 2.3.2

Apache Group Kylin 2.4.0 – 2.4.1

Apache Group Kylin 2.5.0 – 2.5.2

Apache Group Kylin 2.6.0 – 2.6.5

Apache Group Kylin 3.0.0 – 3.0.1

Apache Group Kylin 3.0.0-alpha

Apache Group Kylin 3.0.0-alpha2

Apache Group Kylin 3.0.0-beta

漏洞点评

Apache Kylin 是 Apache 软件基金会的一款开源的、分布式的分析型数据仓库，主要提供 Hadoop/Spark 之上的 SQL 查询接口及多维分析（OLAP）能力，以支持超大规模数据。Kylin 某些版本中存在一些 restful API，可以将操作系统命令与用户输入的字符串连接起来，由于未对用户输入内容做合理校验，导致攻击者可以在未经验证的情况下执行任意系统命令。

（4） Apache Dubbo Provider 默认反序列化远程代码执行漏洞

CVE-2020-1948

NSFOCUS ID：46973

受影响版本

Apache Dubbo 2.6.0 <= Dubbo Version <= 2.6.

Apache Dubbo 2.7.0 <= Dubbo Version <= 2.7.

Apache Dubbo Dubbo <= 2.5.0

不受影响版本

Apache Dubbo Dubbo >= 2.7.7

漏洞点评

2020 年 6 月 23 日，Apache Dubbo 发布安全公告披露 Provider 默认反序列化导致的远程代码执行漏洞（CVE-2020-1948），攻击者可以发送带有无法识别的服务名或方法名及某些恶意参数负载的 RPC 请求，当恶意参数被反序列化时将导致代码执行。

（5） Apache Tomcat 文件包含漏洞

CVE-2020-1938

NSFOCUS ID：45940

受影响版本

Apache Group Tomcat 9 < 9.0.31

Apache Group Tomcat 8 < 8.5.51

Apache Group Tomcat 7 < 7.0.100

Apache Group Tomcat 6

不受影响版本

Apache Group Tomcat 9.0.31

Apache Group Tomcat 8.5.51

Apache Group Tomcat 7.0.100

漏洞点评

Apache Tomcat 由于 Tomcat AJP 协议存在缺陷，在实现上存在文件包含漏洞。攻击者利用该漏洞可通过构造特定参数，读取服务器 webapp 下的任意文件。若目标服务器同时存在文件上传功能，攻击者可进一步实现远程代码执行。

2.4 常见漏洞利用攻击趋势分析

2020 年监测到的漏洞利用告警共 106690288 次，基于漏洞利用的攻击排名 TOP10 如表 2-1 所示。其中 windows ms17-010 系列漏洞扫描攻击的告警最多，共 11716953 次。

表 2-1 2020 年漏洞利用告警 TOP10

漏洞信息	告警次数
windows ms17-010 系列漏洞扫描攻击	11716953
phpbb viewtopic.php topic_id 远程 sql 注入攻击	7415654
openssl sslv2 弱加密通信方式易受 drown 攻击(cve-2016-0800)	3468173
windows smb 远程代码执行漏洞(shadow brokers eternalblue)(cve-2017-0144)(ms17-010)	1971401
powerdns authoritative server dns tkey unknown record 拒绝服务漏洞(cve-2015-5311)	1848573
struts2 远程命令执行漏洞(s2-045)(s2-046)(cve-2017-5638)	877127
gnu bash 环境变量远程命令执行漏洞(cve-2014-6271)	805721
apache http server "mod_log_config"模块空 cookie 拒绝服务漏洞	699444
openswan 和 strongswan dpd 报文远程拒绝服务漏洞	649632
microsoft .net framework pe 加载器远程溢出漏洞（ms07-040）	544645

漏洞利用的攻击类型主要有扫描探测畸形攻击、CGI 攻击、扫描探测、溢出攻击、木马攻击等，攻击类型数量如表 2-2 所示。其中基于畸形攻击的告警数量最多，共 40022603 条。

表 2-2 2020 年漏洞利用攻击类型

攻击类型	告警数量
畸形攻击	40022603
CGI 攻击	14489934
木马攻击	14377066
扫描探测	13475318
其它攻击	12490187
溢出攻击	10881246
企业内部攻击	470314
暴力猜解	232821

事件监控	166412
蠕虫病毒	87381

漏洞利用的服务类型主要有 WWW、CGI 服务、SAMBA 协议、SSH、MISC 等，服务类型数量 TOP10 如表 2-3 所示。其中基于 CGI 的漏洞利用告警最多，共 35274114 条。

表 2-3 2020 年漏洞利用服务类型 TOP10

服务类型	告警数量
CGI	35274114
WWW	24858863
MISC	18357813
SAMBA	13168419
SSH	3003139
DNS	3002495
SUNRPC	558589
SMTP	490185
FTP	340142
SQL	254916

3. 恶意软件态势

3.1 后门

在信息安全领域，后门是指绕过安全控制而获取程序或系统访问权的方法。后门的最主要目的就是方便以后再次秘密进入或者控制系统。攻击者往往通过一些欺骗手段，诱使用户主动进行一些操作，比如下载或打开装有恶意代码的文件，用户在毫不知情的状况下在算机上创建了一个后门。或者攻击者在利用其它攻击方式攻陷一台主机后，在该主机上创建后门，这样既可以保证轻而易举的随时入侵又有很好隐蔽性，难以被发现。

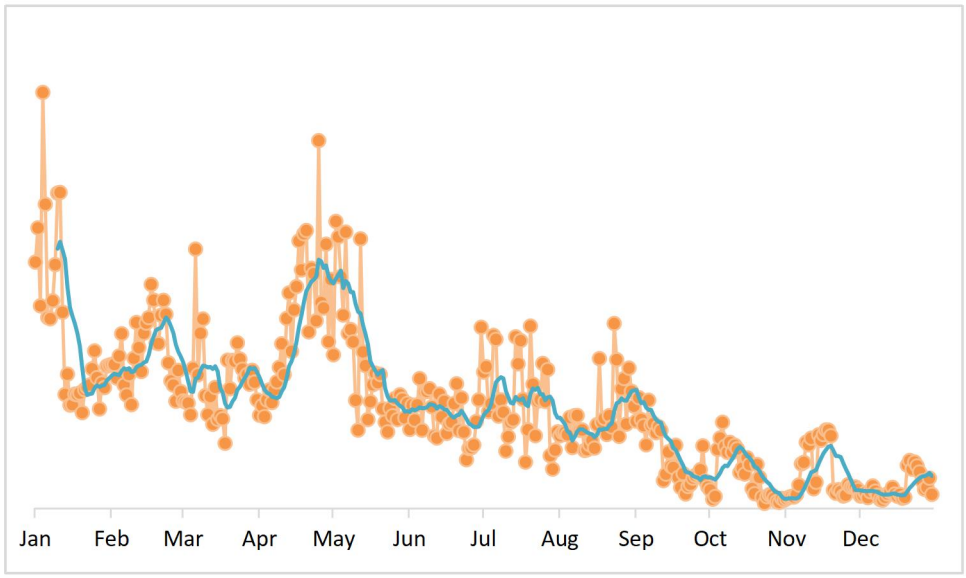

图 3-1 2020 年后门程序活动监测

从活跃趋势上来看，全年活跃度在五月份到达高峰，上半年活跃度较高且波动较大，下半年逐月下降，且趋于平稳。全年活跃度较高的后门程序为：

netcore / netis 路由器后门

早在 2014 年，国内电子厂商生产的 NetCore 系列路由器等设备被披露存在高权限后门。NetCore 漏洞的存在，使得攻击者可以通过此漏洞获取路由器 Root 权限，可完全控制受影响的产品。目前，很多互联网上还存在有该后门的路由器设备，而这些设备被国外物联网僵尸网络 Gafgyt 家族再次利用。

nssock2.dll 后门程序通信

NetSarang 的 Xmanager、Xshell、 Xftp、Xlpd 等产品的多个版本发布的 nssock2.dll 中存在的恶意代码。该后门会对一个域名发起请求，该域名还会向多个超长域名做渗出，且域名采用了 DGA 生成算法，通过 DNS 解析时渗出数据。并收集和上传主机信息到每月一个的 DGA 域名上，并保存服务器返回的配置信息。

3.2 挖矿

2017 年加密货币的价格持续飙升，在利益驱使下，传统勒索软件操纵者中很大一部分转向加密货币的挖掘。比特币、门罗币、以太坊等多种加密货币交易一度十分活跃。据不完全统计，目前全球有超过 1600 种加密货币，总市值超过 3400 亿美元。挖矿始终是攻击者变现的重要手段，短时间内并不会出现颓败现象。

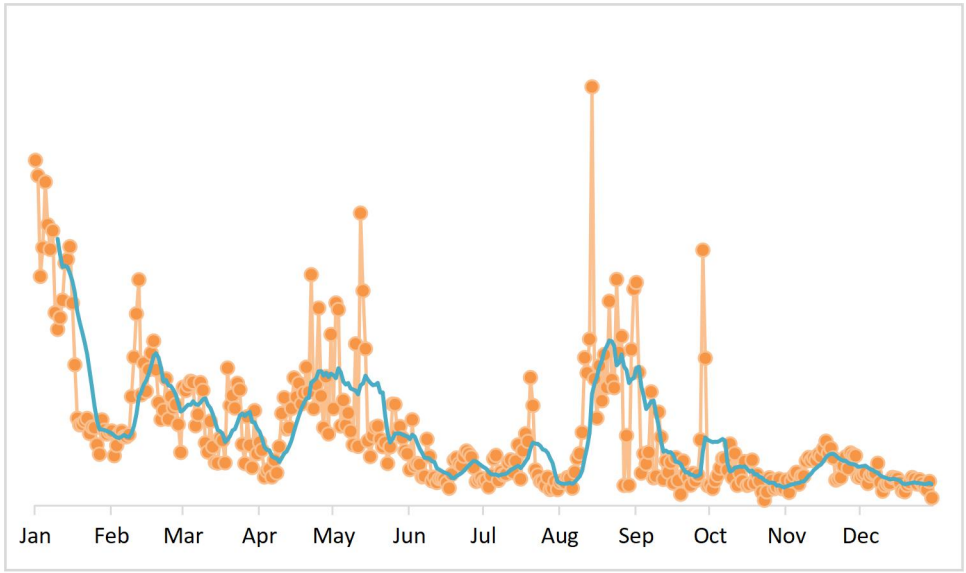

图 3-2 2020 挖矿程序活动监测

挖矿在一份月份活跃度到达峰值，后面持续下降，在五月份、九月份有所提升，年末到达最低谷且趋于平稳。全年活跃度较高的挖矿程序为：

Watchdogs 挖矿

Watchdogs 挖矿利用被感染 watchdogs 病毒的主机进行挖矿，该病毒通过 Redis 未授权访问漏洞及 ssh 弱口令进行突破植入，随后释放挖矿木马进行挖矿操作，并对内外网主机进行 redis 漏洞攻击及 ssh 暴力破解攻击，同时通过内外网扫描感染更多机器。

Wannamine

同样是永恒之蓝漏洞，2018 年，WannaMine 家族成为挖矿大军中的主力，上半年在所有检测到的挖矿活动中，占比超过了 70%，传播

速度令人咂舌。在攻击武器的选择上，永恒之蓝漏洞攻击被多数挖矿病毒家族所青睐。

3.3 蠕虫

蠕虫病毒是一种常见的计算机病毒，是无须计算机使用者干预即可运行的独立程序，它通过不停的获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。据长期观测，大部分蠕虫病毒最早发现时间距今都有 5 年以上， 可见这些蠕虫病毒繁衍、进化的能力以及在网络中彻底清除的难度。

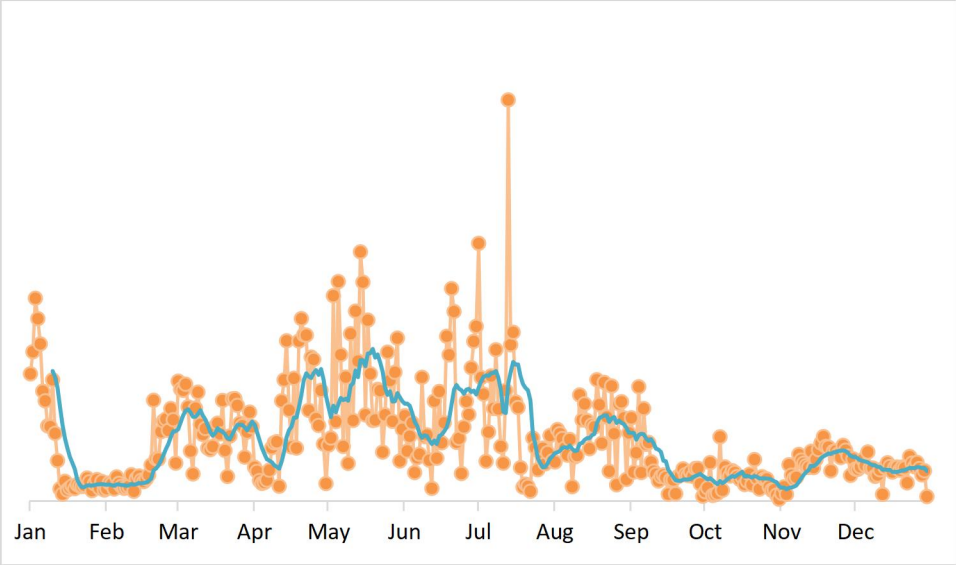

图 3-3 2020 年蠕虫活动监测

从全年数据来看，蠕虫程序 5 至 8 月份较为活跃，整体趋于平稳。全年活跃度较高的蠕虫程序为：

w32.faedevour

W32.Faedevour 活动次数远超排名前 5 的其他病毒。它在受感染的计算机中打开一个后门，窃取信息，接受远程攻击者的命令执行截图、下载文件、发送文件给攻击者等一系列操作，该蠕虫试图通网络驱动器和共享文件夹进行传播。

code red

“红色代码”病毒是 2001 年 7 月 15 日发现的一种网络蠕虫病毒，感染运行 Microsoft IIS Web 服务器的计算机。如果稍加改造，将是非常致命的病毒，红色代码三代病毒允许黑客拥有所攻破计算机的所有权限并为所欲为，可以盗走机密数据，严重威胁网络安全。

3.4 木马远控

木马的核心功能为信息窃取与其他复杂的远程控制。与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。而现实中病毒的分类往往没有统一的标准，木马病毒也可以拥有蠕虫特征。在此，我们以木马的核心功能作为简单的划分。

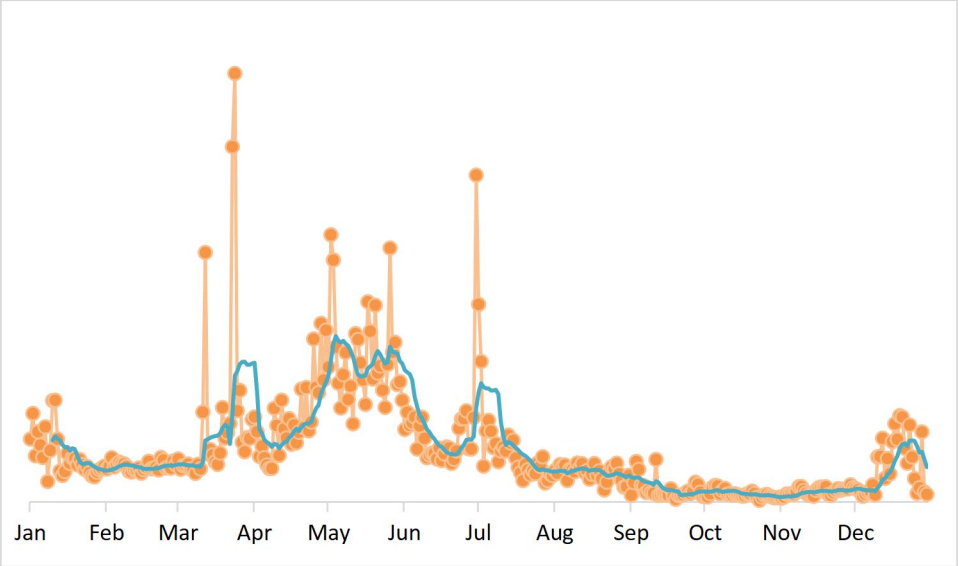

图 3-4 2020 年木马活动监测

从全年数据来看，木马程序活跃度上半年相对较高，且呈上升趋势，从七月份开始逐渐下降，至十二月起有一个小范围的升温。全年活跃度较高的木马程序为：

暗云木马

从 2015 年至今，暗云木马已感染数 以百万的计算机，并经过了几次的更新迭代，各变种也层出不穷，查而未绝。其中 Bootkit 木马是迄今为止最复杂的木马之一，其触角已发展到了黑色产业的方方面面。

驱动人生下载器木马

利用驱动人生升级通道进行下发并一直在不断更新。之前利用永恒之蓝漏洞扩散传播，木马在已感染主机上，通过下载更新文件，同时在利用永恒之蓝漏洞攻击后感染的机器上，植入最新版本的木马。以及后面在携带永恒之蓝漏洞的基础上新增暴力破解的功能，极大提高了木马的传播能力以及威胁范围。

3.5 勒索软件

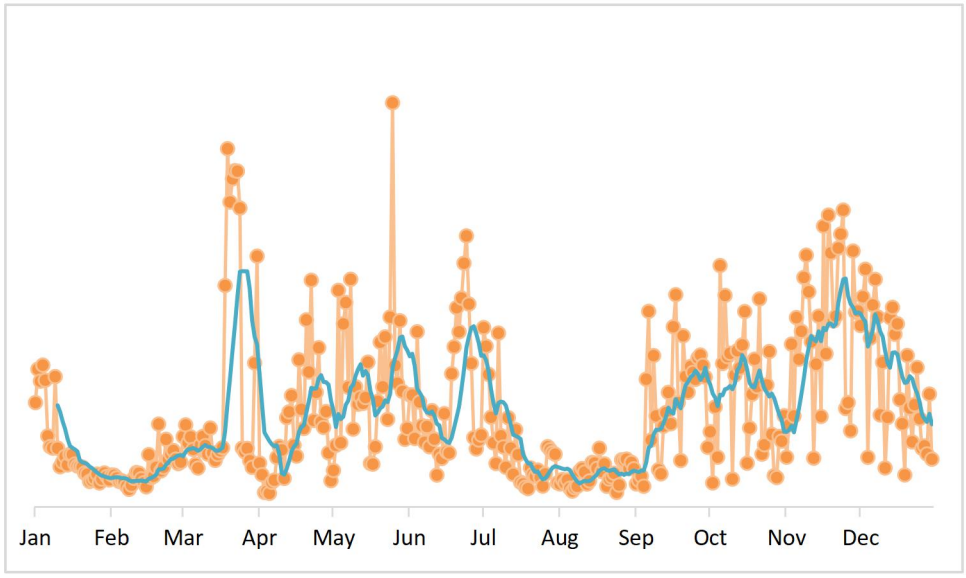

图 3-5 2020 年勒索软件活动监测

从全年的数据来看，4 月份活跃度激增后迅速下降，后面持续波动，八月份达到最低谷，年末又呈现较为活跃的状态。全年活跃度较高的勒索软件程序为：

Wannacry

2017 年 WannaCry 席卷全球，五个小时内，包括英国、俄罗斯、整个欧洲以及中国国内多地中招，最终影响国家高达 150 多个，经济

损失极其严重。虽然从 17 年 5 月份曝光至今已超过两年的时间，但利用永恒之蓝漏洞的攻击仍屡试不爽，这应当引起各行业从业者的重视。

trojan.cryptolocker.n 勒索软件

CryptoLocker 在 2013 年 9 月被首次发现，它可以感染大部分的 Windows 操作系统，包括：Windows XP、 Windows Vista、Windows 7、Windows 8。CryptoLocker 通常以邮件附件的方式进行传播，附件执行之后会对特定类型的文件进行加密，并弹出勒索窗体。

4. 物联网安全态势

4.1 2020 年重点物联网安全事件分析

（1）Ripple20 0day 漏洞曝光，扫荡全球各行业数亿台联网设备

以色列网络安全公司 JSOF 周二警告说，由于严重安全漏洞影响了 Treck TCP/IP 堆栈，全球数亿台（甚至更多）IoT 设备可能会受到远程攻击。这一漏洞影响各行各业，波及家用/消费设备、医疗保健、数据中心、企业、电信、石油、天然气、核能、交通运输以及许多其他关键基础架构。

Treck TCP / IP 是专门为嵌入式系统设计的高性能 TCP / IP 协议套件。JSOF 研究人员发现该产品共有 19 个 0day 漏洞，影响 Treck 网络协议的专有实现，因在 2020 年报道出来，所以将这一系列漏洞统称为“Ripple20”。

（2）新的 OpenWrt RCE 漏洞曝光，影响数百万台网络

ForAllSecure 软件公司的研究员 Guido Vranken 偶然间发现了一个基于 Linux 的开源操作系统 OpenWrt 的 RCE 漏洞，于 3 月 24 日在企业博客[2]中发布了该漏洞的技术详情和 PoC（漏洞编号为

CVE-2020-7982）。值得一提的是，该漏洞在 2017 年 2 月份就被引入代码，距今已有三年之久，在今年年初才上报给 OpenWrt 开发团队。根据 OpenWrt 项目团队发布的信息，受影响版本是 18.06.0 至 18.06.6、19.07.0 以及 LEDE 17.01.0 至 17.01.7 版本。

该漏洞存在于 OpenWrt 的 Opkg 包管理器中，由于包解析逻辑中的一个错误，包管理器忽略了嵌入在签名存储库索引中的 SHA-256 检验和，从而有效地绕过了已下载.ipk 工件的完整性检查，攻击者借助 Opkg 本身的 root 权限以及特制的.ipk 数据包，便可以注入任意恶意代码。

该漏洞利用的前提是，攻击者需要给 Web 服务器提供受损的软件包，并且拦截替换设备与 downloads.openwrt.org 之间的通信，或控制设备向 downloads.openwrt 发送的 DNS 查询。当在受害者系统上调用“opkg install ”安装命令时，在没有任何验证情况下，远程攻击者便可以利用该漏洞拦截目标设备的通信信息，欺骗用户安装恶意程序包或采用软件更新的方式来执行恶意代码，从而获取设备的完全控制权。

研究报告漏洞后，OpenWrt 就移除了包列表中 SHA-256 检验和的空格，这一定程度上可以缓解对用户带来的危险，但攻击者依然可以通过由 OpenWrt 维护者签名较旧的软件包列表进行相关操作。

OpenWRT 是一个高度模块化，高度自动化的嵌入式 Linux 系统，拥有强大的网络组件和扩展性，常常被用于工控设备、电话、小型机器人、智能家居、路由器以及 VoIP 设备，据不完全统计，该系统已被安装到全球上百万个物联网设备上。当这类严重 RCE 漏洞曝光后，设备用户应该以最快的速度升级官方发布的补丁，避免受到影响。

（3）CallStranger UPnP 漏洞曝光，影响数十亿台设备

2020 年 6 月 8 日，安全专家披露了一个名为“Call Stranger”[1]（漏洞编号为 CVE-2020-12695）的新型 UPnP 漏洞，该漏洞影响数十亿台

设备，已确认受影响的设备名单包括 Windows PC、Xbox One 以及华硕、贝尔金、博通、思科、戴尔、D-Link、华为、Netgear、三星、TP-Link、中兴等公司的电视和网络设备。该漏洞可能会被远程、未经认证的攻击者滥用、进行反射 DDoS 攻击、绕过安全系统进行内网渗透，以及内部端口扫描。

UPnP（Universal Plug and Play，UPnP）是一种包含多个协议（如 SSDP、SOAP 等）的网络协议簇，它允许联网设备，如个人电脑、打印机、互联网网关、Wi-Fi 接入点和移动设备无缝发现对方在网络上的存在，并建立功能性网络服务，用于数据共享、通信和娱乐。

2020 年 4 月 17 日之前生效的 UPnP 协议簇，SUBSCRIBE 函数中的 Callback 参数可以被攻击者控制，向互联网上可访问的任意目的地发送大量数据，导致反射攻击、数据外泄和其他意外的网络行为，影响暴露在互联网上的数百万设备和局域网内的数十亿设备，OCF（Open Connectivity Foundation）已经更新了 UPnP 规范来解决该问题。

传统的 UDP 类反射攻击通常利用传输层为 UDP、端口固定的服务（如 SSDP、NTP 等），但该漏洞造成反射攻击的 UPnP SOAP 服务传输层为 TCP，且暴露在互联网中的 SOAP 服务通常端口不固定，一旦僵尸网络利用该漏洞进行反射攻击，将给防护带来一定的困难。

遗憾的是，该漏洞是一个协议漏洞，这意味着厂商可能需要很长时间才能发布安全补丁。为了缓解该问题，厂商应在默认配置中禁用 UPnP SUBSCRIBE 功能，并禁用暴露在互联网上设备的 UPnP 协议。

尽管去年内，《绿盟科技 2019 物联网安全年报》[6]建议厂商和用户避免在互联网中暴露 UPnP 服务，但根据绿盟威胁情报中心显示，2020 年全球仍有近数百万台开启了 UPnP 服务的设备暴露在互联网中。研究人员认为，一旦相关漏洞被披露，僵尸网络可能很快就会加以利用并发起反射攻击，这种新型反射攻击，将给防护带来一定的困难。

诚然 UPnP 服务对方便设备间互联互通有极大帮助，但其过于庞大的协议簇，从设计到实现均可能存在各种缺陷，防止 UPnP 服务被黑客利用仍需 OCF、设备厂商、运营商和用户多方共同努力。

（4）BadPower：让快速充电器变成手机电脑杀手

2020 年 7 月 15 日，腾讯安全玄武实验室发布了一项命名为“BadPower”的重大安全问题研究报告[9]。报告指出，市面上现行大量快充终端设备存在安全问题，攻击者可通过改写快充设备的固件控制充电行为，造成被充电设备元器件烧毁，造成严重的后果。据保守估计，受“BadPower”影响的终端设备数量可能数以亿计。

具体的，腾讯玄武安全实验室对市面上 35 款支持快充技术的充电器、充电宝等产品进行了测试，发现其中 18 款存在安全问题。攻击者可利用特制设备、手机、笔记本等数字终端来入侵快充设备的固件，控制充电行为，使其向受电设备提供过高的功率，从而导致受电设备的元器件击穿、烧毁，还可能进一步给受电设备所在物理环境造成安全风险。攻击方式包括物理接触和非物理接触，有相当一部分攻击可以通过远程方式完成。在玄武实验室发现的 18 款存在 BadPower 问题的设备里，有 11 款设备可以通过数码终端进行无物理接触的攻击。腾讯安全玄武实验室已于 3 月 27 日将“BadPower”问题上报给国家主管机构 CNVD，同时也在积极和相关厂商一起推动行业采取积极措施消除 BadPower 问题。小米和 Anker 也对这次研究工作做出了贡献，另在未来上市的快充产品中也会加入安全检测环节。

BadPower 不是传统网络安全问题，虽然不会导致数据隐私泄露，但会给用户造成实实在在的财产损失，甚至更糟糕的情况。BadPower 再次提醒我们，随着信息技术的发展，数字世界和物理世界之间的界限正变得越来越模糊。之前我们知道工业控制系统、车联网系统的漏洞和威胁可能会影响物理世界，但这些似乎距离大多数人比较遥远，但是其

实像充电器这种人人都有、不起眼的小东西也可能打破数字世界和物理世界之间的结界。

（5）特斯拉废弃零件泄露隐私，谁为用户隐私买单？

在使用特斯拉车载信息娱乐服务前，用户必须输入详细的个人信息，存储这些信息的媒体控制单元或许正在成为用户隐私数据泄露的源头。2020 年 6 月，国外黑客发现，从废弃的特斯拉媒体控制单元（MCU）中，能够获取到之前设备所有者的隐私信息。

随着汽车智能化、网联化技术快速深入发展，汽车内车机、控制器甚至是车外未来的基础设施以及云端内个人隐私的数据会日益庞大，数据种类也会越来越多。这些数据带给我们安全驾驶以及出行便利的同时，隐私泄露的风险也在加大。除了软硬件、云端方面的技术防护手段之外，隐私防护也需要标准、法律、法规相配合，需要多方协同努力、长期研究。

（6）智能门锁暗藏的物联网安全危机

在物联网时代，智能门锁的普及率已经越来越高了，但智能门锁真的的安全吗？U-Tec UltraLoq 是众筹平台 Indiegogo 上的一款热门产品，现已在亚马逊等电商平台零售。这款锁拥有一些高级功能，包括指纹读取器、反窥视触摸屏，以及通过蓝牙和 WiFi 的 APP 端控制等。2020 年 8 月，Tripwire 的研究人员 Craig Young 发表了一篇博客，披露了其存在错误配置和其他安全问题，使得攻击者仅用一个 MAC 地址就可以窃取解锁令牌[10][11]。

除了提到的智能门锁，其实每天都有大量没有进行安全测试的物联网设备上市或上线，消费者必须意识到这个逐渐累积的风险。即使是门锁这样的关键安全系统，满足的网络安全规范和要求也很少，相关安全监管更少。正如我们在 Mirai 和其他物联网僵尸网络中所看到的那样，互联网上的各类智能设备，例如智能灯泡、智能冰箱、智能音箱、摄像

头等，在发生故障或被大规模劫持时也会造成严重破坏，并且目前的威胁或许只是冰山一角。

（7）蓝牙冒充攻击（BIAS），无线安全不可忽视

研究人员 Daniele Antonioli 于 2020 年 5 月披露了一个蓝牙协议栈漏洞，攻击者可以利用这个漏洞伪造并欺骗远程配对的蓝牙设备，其危害性影响数十亿蓝牙设备。

蓝牙协议被广泛应用于数十亿台设备中，其中包含了多种身份验证过程。两个蓝牙设备如果要建立加密连接，则必须使用密钥互相配对。在两个蓝牙设备成功配对之后，下一次它们就能够不经过配对过程而重新连接。BIAS 攻击就是利用了这个特性。

BIAS 是第一个被披露的与蓝牙身份验证、连接降级相关的安全问题。因为蓝牙连接的建立不需要用户交互，因此攻击非常隐蔽，危害性很大，尽管蓝牙 SIG 小组已经更新蓝牙核心规范来缓解这一漏洞，但用户仍需谨慎，并持续关注厂商是否推出固件或软件补丁等修复措施。

（8）DHDiscover：可放大近 200 倍的新型反射攻击

2020 年 3 月，腾讯发布了一篇关于某 DVR 被用于反射攻击的文章[4]。在该次攻击事件中，攻击者采用了一种新的 UDP 反射攻击方法，利用的是某视频监控厂商的设备发现服务（因其探测报文中包含 DHDiscover 字符串，因此，我们将其称之为 DHDiscover 服务）。本次攻击流量规模超过 50Gbps，反射源区域分布集中于美洲，亚洲，欧洲的众多国家和地区，尤其以韩国、巴西为重灾区。

反射攻击存在已久，随着防护能力的增强，攻击者的攻击手段也在发生变化，并将注意力放在了一些新的协议上。继去年的 WS-Discovery 反射攻击之后，DHDiscover 反射攻击成为今年出现的一种新的攻击方法。这两个协议都与设备发现有关，需要引起大家的重视。

（9）黑客伪造新冠病毒页面传播恶意软件

2020 年 3 月，研究人员发现有攻击者通过攻击 D-Link 与 Linksys 路由器的方式，劫持用户的网络访问并重定向至伪造的新冠病毒主题页面，通过虚假告示信息诱骗用户下载恶意软件。据发现者统计，截至 3 月 18 日，已经有逾 6000 人次下载了攻击者提供的恶意软件。

路由器是家庭用户与互联网之间的第一道防线，也是攻击者觊觎的首个风险点。修改路由器的默认管理密码，关闭路由器的对外暴露的服务端口，减少攻击面，可以有效缓解此类攻击。

4.2 2020 年新增物联网漏洞情况

2020 全年，漏洞利用平台 Exploit-DB 共计出现 197 个物联网相关漏洞利用，其中，Netgear、IBM、D-Link、Grandstream、Mikrotik 出现漏洞利用的数量位居前五，主要以网络设备厂商为主，同时也有大量厂商出现的漏洞利用数量仅为一个。我们认为，漏洞利用数量较多，并不能直接说明相应厂商的设备质量存在问题。造成这种现象的原因，是这些厂商出售的设备数量较多，研究人员更关注其相关产品。各厂商漏洞利用数量的分布如下所示：

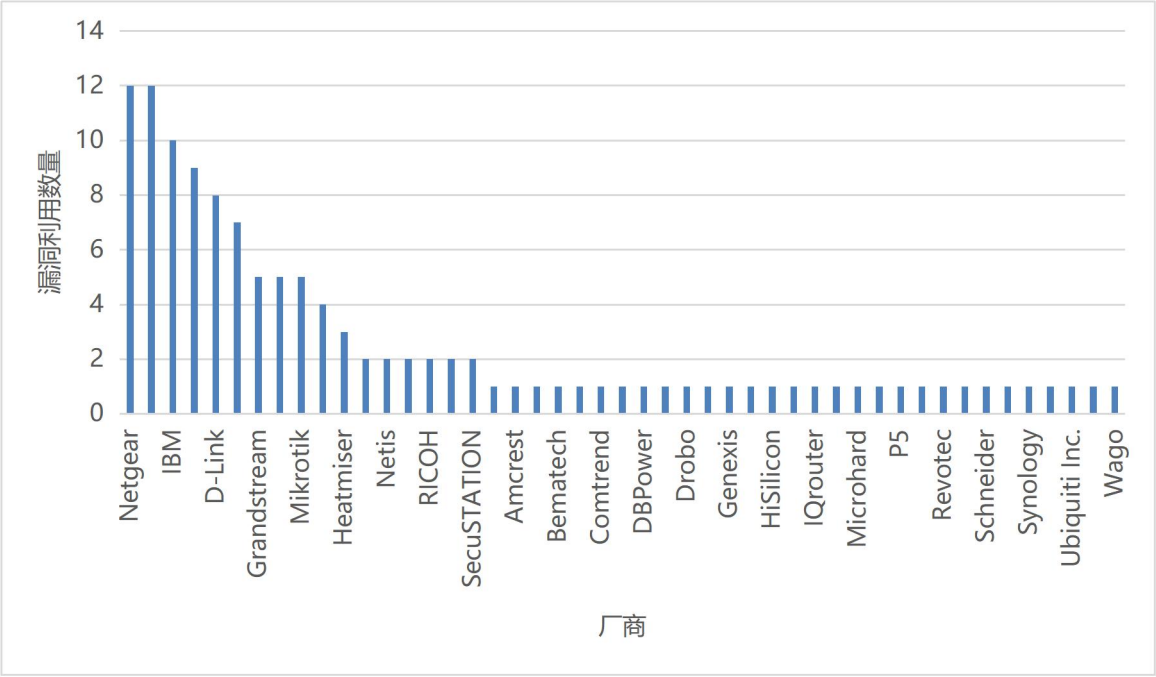

图 4-1 2020 年各厂商漏洞利用数量分布图

2020 年出现的漏洞利用，以 RCE 和 DoS 两类漏洞利用为主，其中 RCE 类漏洞数量最多，占总量的百分之三十五以上。RCE 漏洞危害严重且数量多，导致 Exploit-DB 公布 RCE 类漏洞成为僵尸网络热衷的武器。各类漏洞利用的分布图如下所示：

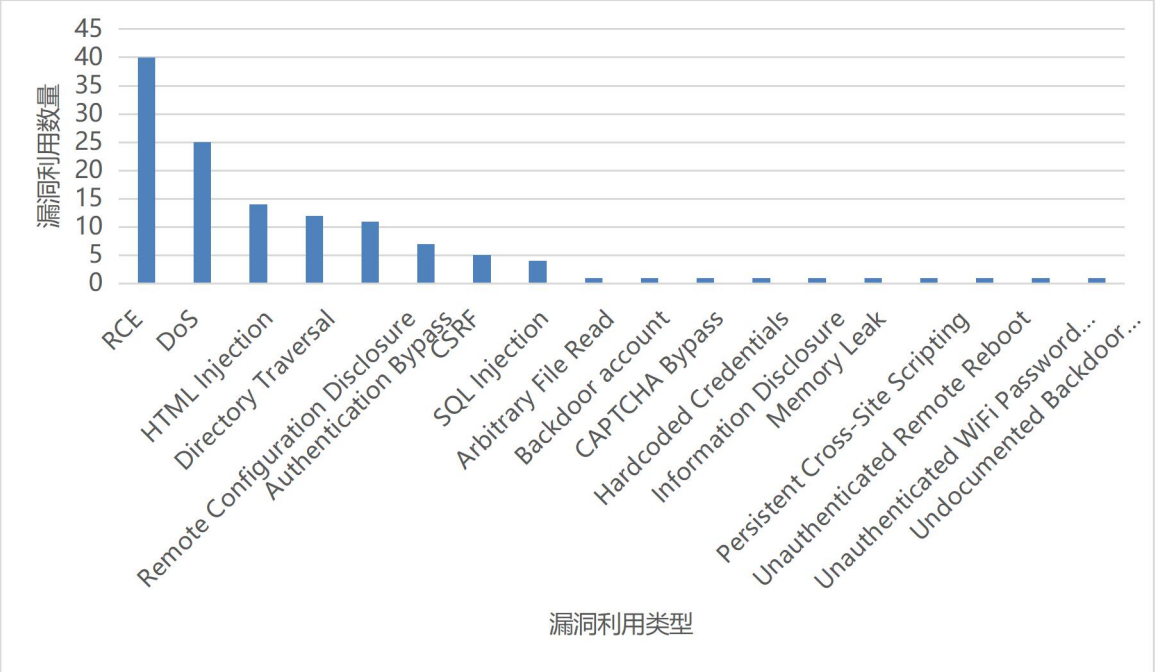

图 4-2 2020 年各类漏洞利用数量分布图

4.3 物联网漏洞利用情况

2020 年绿盟威胁捕获系统捕获到来自 200,470 个 IP 的 12,015,479 次访问请求日志。其中 68.1%的访问请求是对物联网漏洞进行利用的恶意攻击行为，在 56.76%的访问请求中我们识别到了可疑的 Linux 命令执行、Webshell 扫描、HTTP 代理探测等行为。

从下图可以看出，整体来看，对物联网漏洞的攻击行为呈上升趋势。

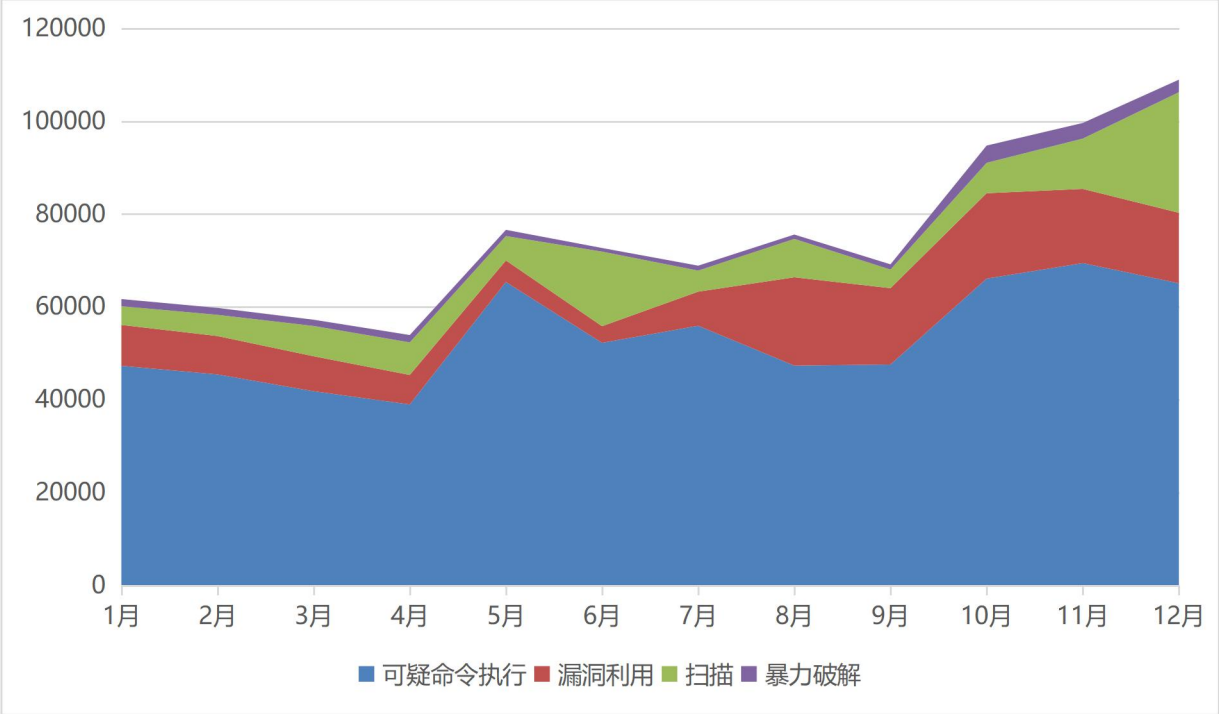

图 4-3 攻击源 IP 总量趋势

我们对物联网漏洞利用的情况进行统计，被利用最多的几个漏洞如下表所示。攻击者使用的漏洞大多在 Exploit-DB 有公开的漏洞利用脚本。

表 4-1 利用数量最多的 Top 10 漏洞

漏洞名称	CVE 或 Exploit-DB 编号	数量
MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution	edb-41471	2701714
D-Link Devices - HNAP SOAPAction-Header Command Execution	cve-2015-2051	1177796
AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities	edb-40500	499727
Eir D1000 Wireless Router - WAN Side Remote Command Injection	cve-2016-10372	170980
ZTE ZXV10 H108L Router with <= V1.0.01_WIND_A01 - RCE Root Exploit		78019
Realtek SDK - Miniigd UPnP SOAP Command Execution	cve-2014-8361	47853
Wireless IP Camera (P2P) WIFICAM - Remote Code Execution	cve-2017-8225	40293
Huawei Router HG532 - Arbitrary Command Execution	cve-2017-17215	29188
Multiple CCTV-DVR Vendors - Remote Code Execution	cve-2017-17215	18791
GPON Routers - Authentication Bypass / Command Injection	cve-2018-10562	15961

4.4 物联网威胁攻击源与攻击事件分析

对本年蜜罐日志中的 200,470 个源 IP 进行分析，其中 157,870 个 IP 发起过漏洞利用等恶意行为。从关联到恶意行为的 IP 分布在了 201 个国家和地区，从国家分布情况来看，中国最多，恶意 IP 数量占比达到了 27.92%。

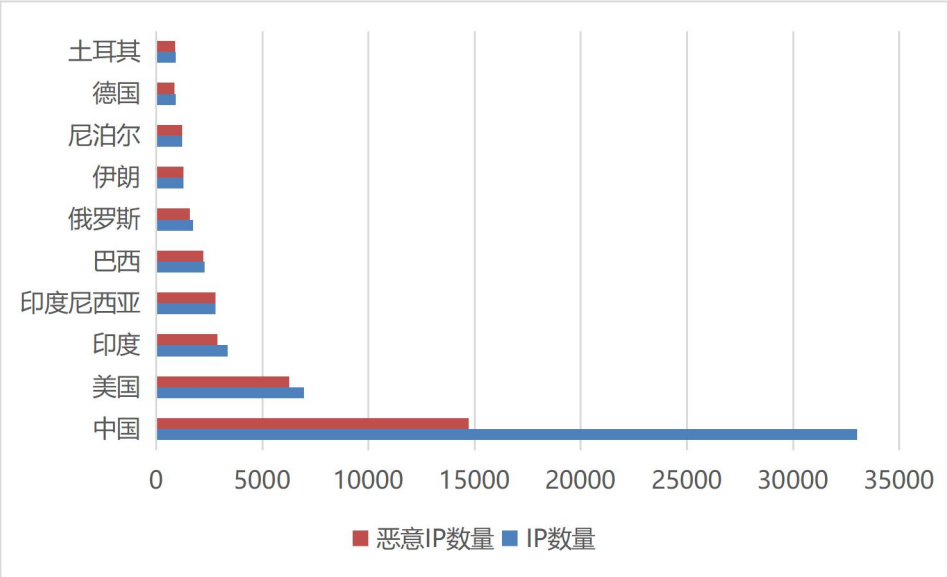

图 4-4 蜜罐的日志源 IP 的国家分布情况

我们对绿盟威胁捕获系统日志数据中的攻击事件进行了分析，这里我们将一天内一个独立 IP 的日志看作一次事件，事件的数量我们将以每月活跃 IP 为单位进行呈现。

2020 年总体趋势上，针对物联网设备的扫描与探测行为呈平稳趋势。

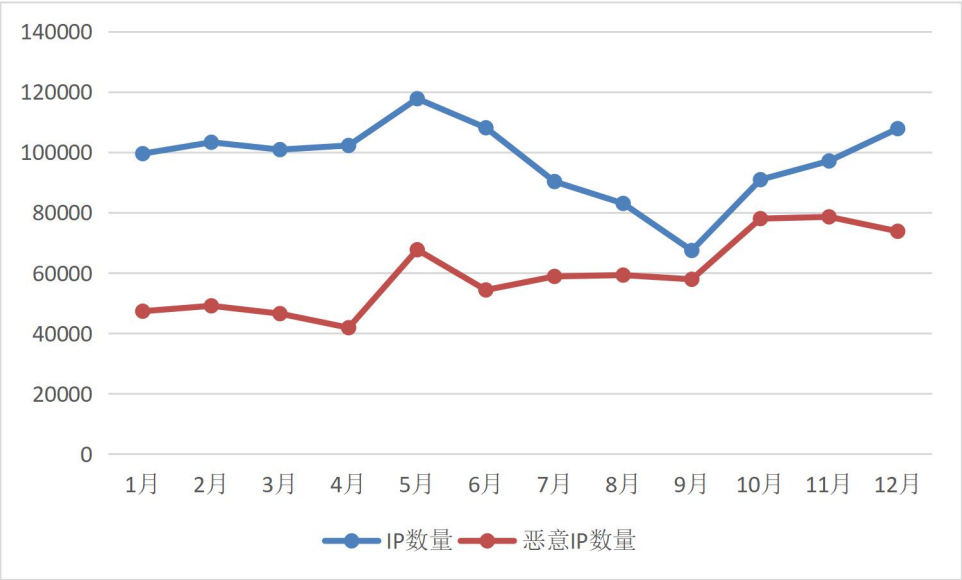

图 4-5 每日访问蜜罐的所有 IP、发送攻击请求 IP 的数量趋势

5. DDoS 攻击态势

5.1 DDoS 攻击流量与攻击次数

2020 年，我们监控到 DDoS 攻击次数为 47 万次（event_id 为粒度），攻击总流量 6.6 万 TB，详见下图。

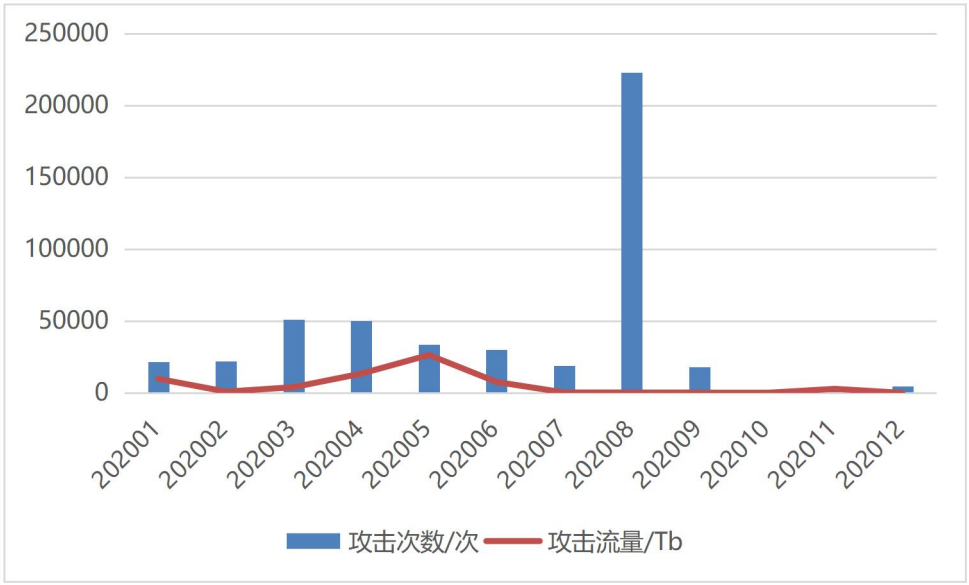

图 5-1 攻击次数与攻击流量

从各月来看，DDoS 攻击峰值在 100Gbps 以上的大流量攻击主要分布在 5 月份，占比 43%，DDoS 攻击峰值在 1G 以下的小流量攻击主要分布在 8 月份，占比 47%。

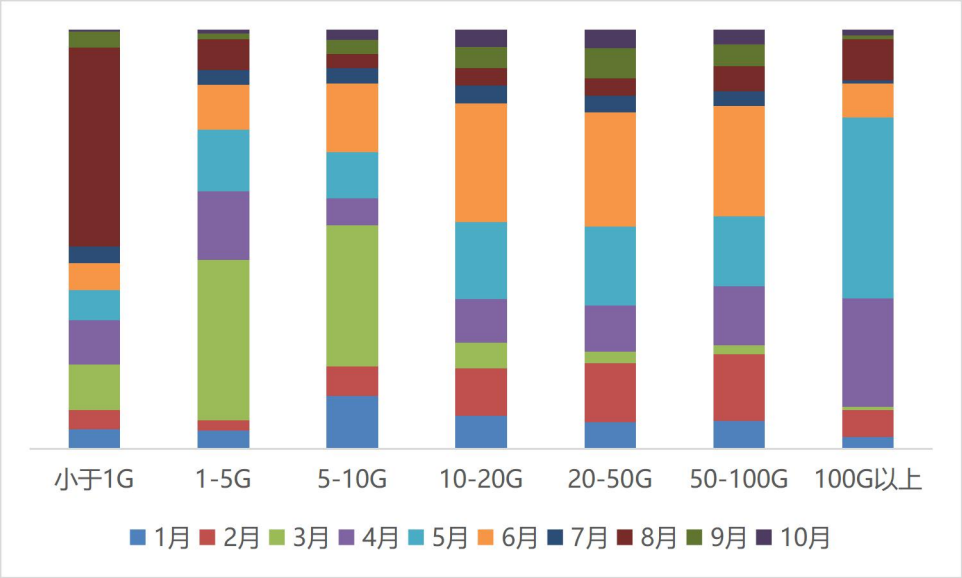

图 5-2 各类攻击规模各月份攻击次数占比

5.2 DDoS 攻击时间刻画

攻击持续时间占比

2020 年，攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 65%。这种短时攻击的高占比说明攻击者越来越重视攻击成本和效率，倾向于在短时间内，以极大的流量导致目标服务的用户掉线、延时和抖动。在长周期内，多次瞬时攻击能够严重影响目标服务质量，同时攻击成本得到有效控制。

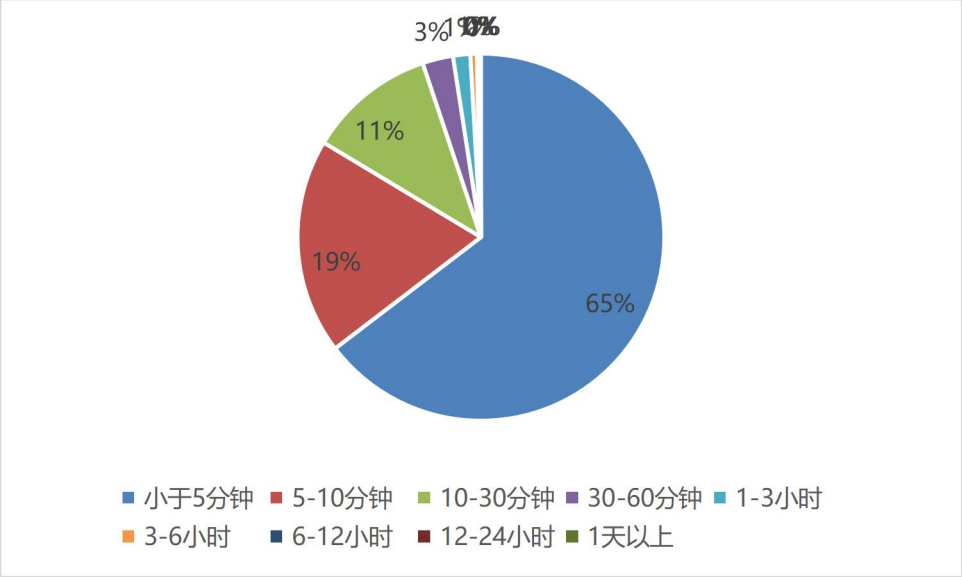

图 5-3 攻击持续时间占比

一天中 DDos 攻击活动分布

从一天 24 小时攻击占比来看，11 点到 19 点为攻击高峰攻击。

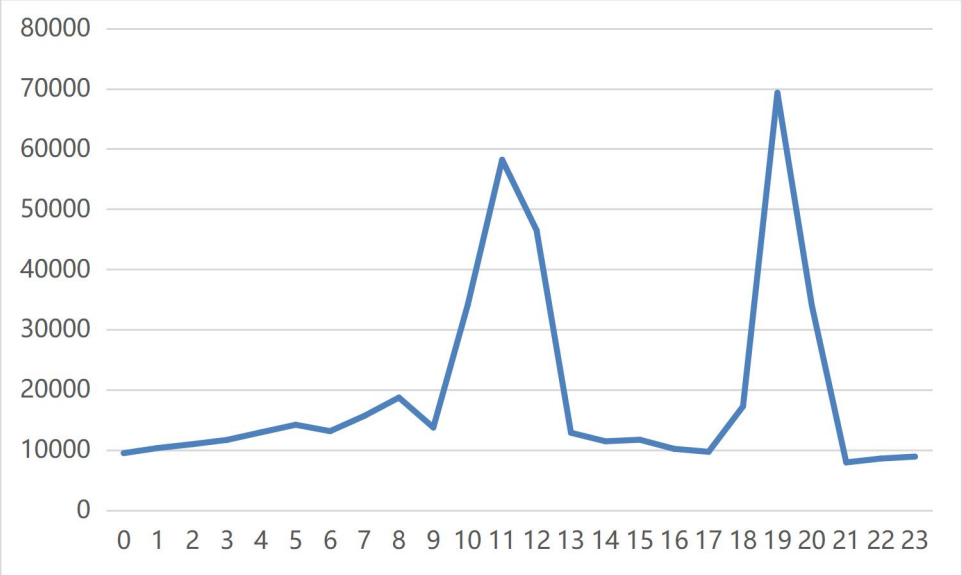

图 5-4 一天中 DDos 攻击活动分布

一周中 DDos 攻击活动分布

从每周中 DDoS 攻击活动的分布来看，周中（周二、周三、周四）最常被攻击。

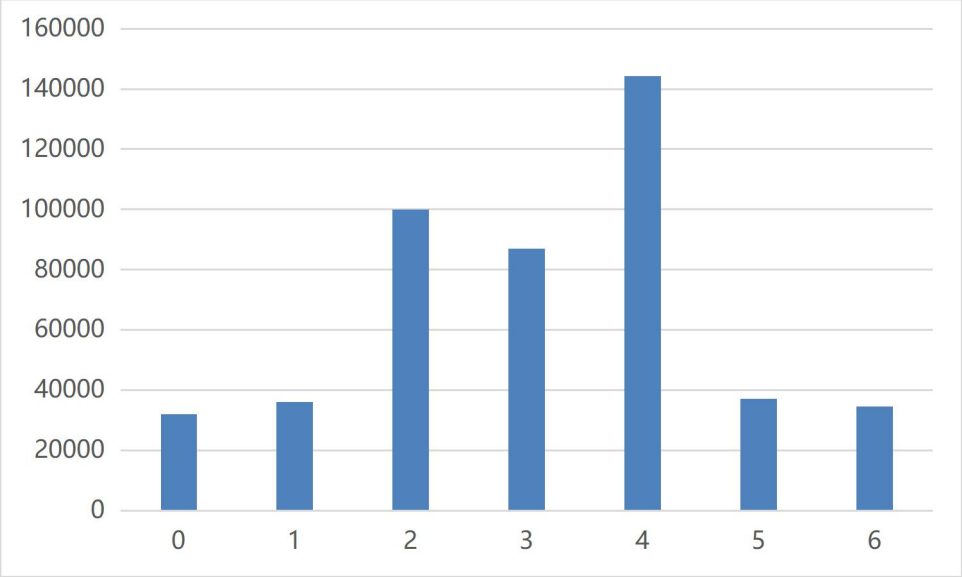

图 5-5 一周中 DDos 攻击活动分布

5.3 DDoS 攻击类型分析

2020 年，主要的攻击类型为 UDP Flood，SYN Flood，NTP Reflection Flood，这三大类攻击占了总攻击次数的 56%。UDP Flood 和 SYN Flood 依然是 DDoS 的主要攻击手法。值得关注的是，ACK Flood 由去年的攻击次数占比 14.9%减少至 2%，NTP Reflection Flood 取代了去年 ACK Flood 排名第三的位置。

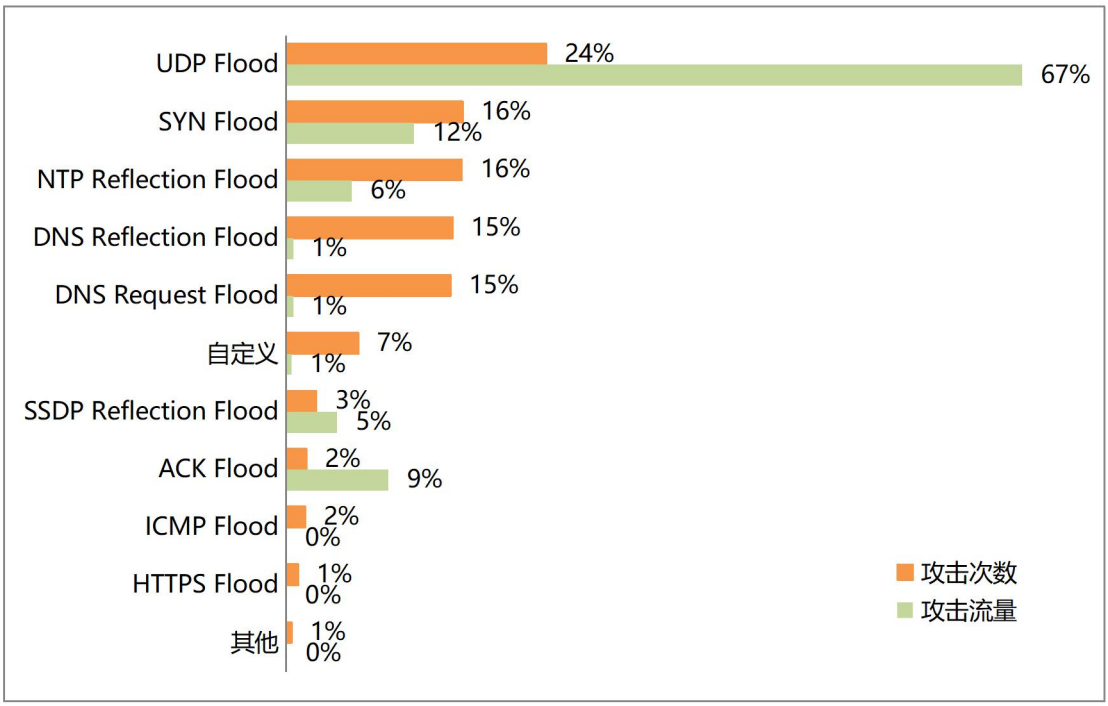

图 5-6 攻击类型的攻击次数分布

从混合型攻击事件来看，相比 2019 年，2020 年混合多种类型的 DDoS 攻击事件数量有所增加。在实际攻击过程中，攻击者混合使用多种方式组合探测以求最佳攻击方式，利用协议，系统的缺陷，尽其所能展开攻击，达到最完美的攻击效果。

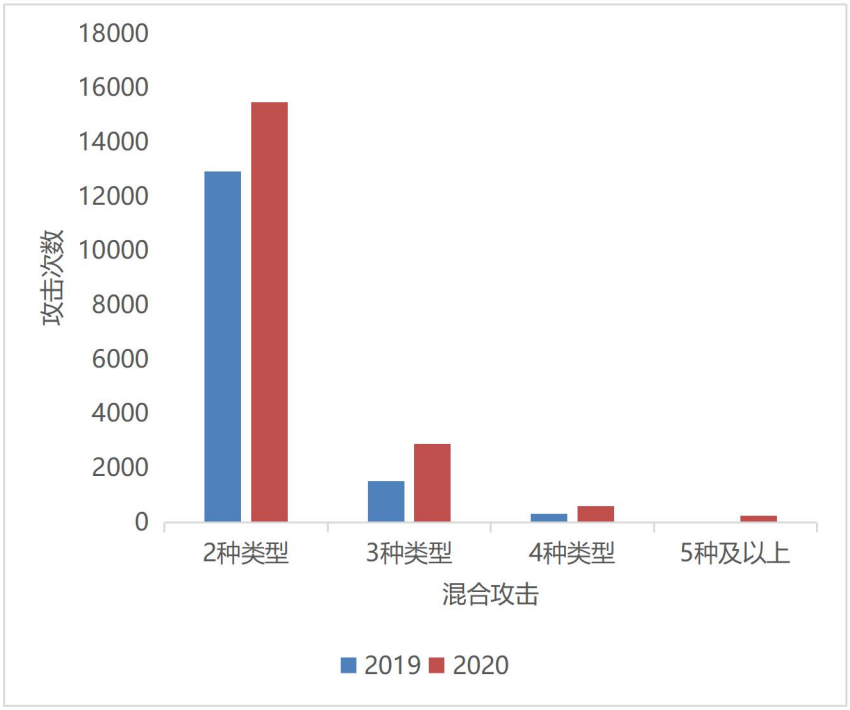

图 5-7 混合攻击分布

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM）

5.4 DDoS 团伙分析

团伙规模

2020 年共发现 45 个活跃团伙，团伙规模分布如下，大部分团伙规模都在 200 到 1 万之间。成员数量大于 1 万的大团伙有 4 个，其中规模最大的团伙成员数量高达 4.9 万个。

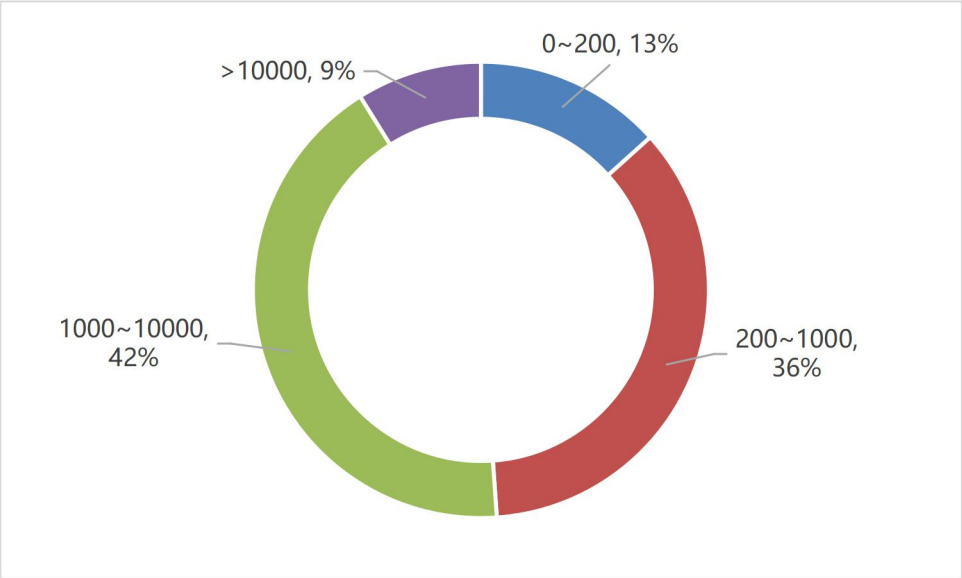

图 5-8 IP 团伙攻击源规模分布（每个区间代表团伙规模范围）

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM），绿盟黑洞云清洗、绿盟科技威胁情报中心

团伙攻击总流量

各团伙的流量分布如下，涵盖了来自同一团伙所有成员的全部攻击。单一团伙的攻击总流量最高达到 3624TB，这个最大攻击总流量是去年的两倍以上。

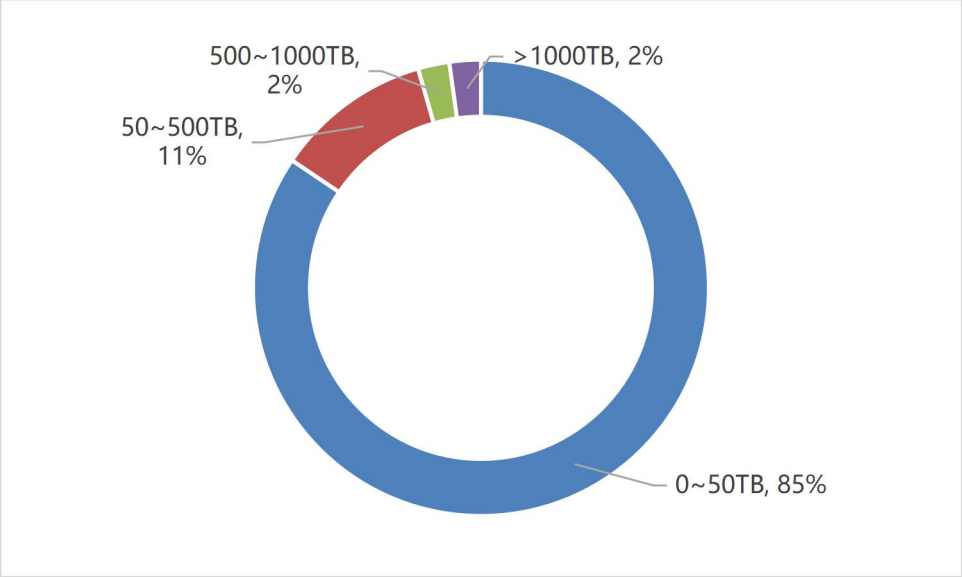

图 5-9 攻击总流量各区间团伙数量分布

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM），绿盟黑洞云清洗、绿盟科技威胁情报中心

团伙攻击资源类型

能够长期被操控的团伙攻击资源主要就是 IDC 和物联网设备，统计团伙所有攻击资源类型，占比最高的就是物联网设备，占比 31%。其中，占比最高的为 15%的摄像头、12%的路由器设备和 3%的网络电话。

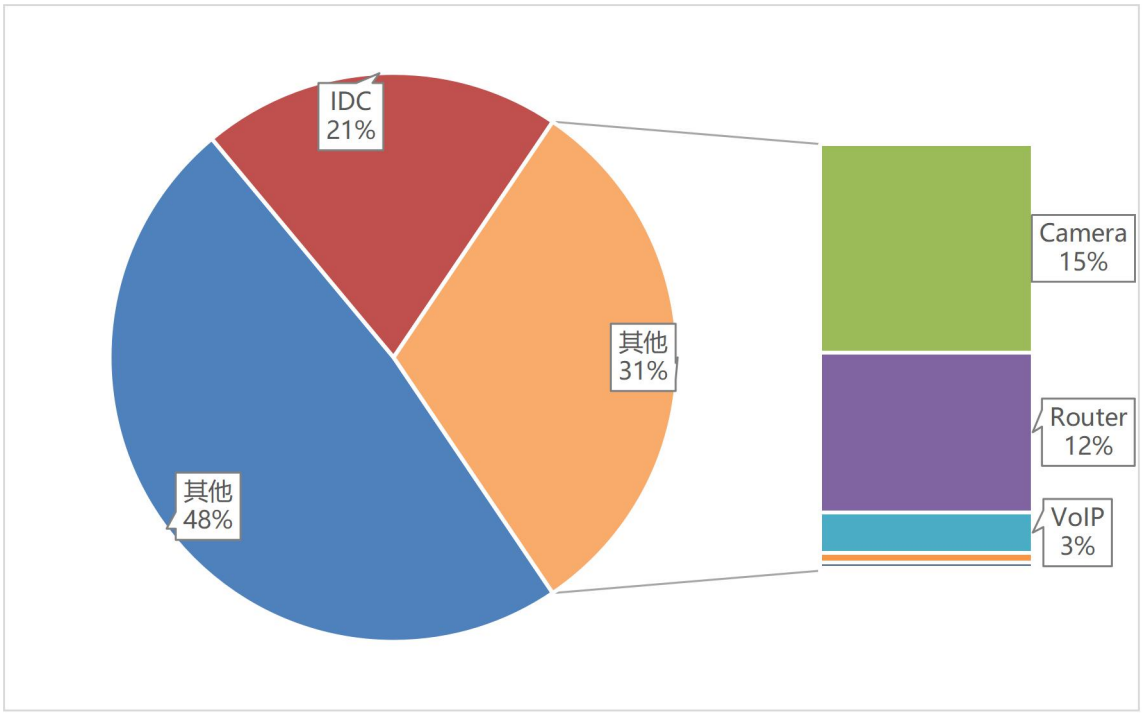

图 5-10 团伙攻击资源类型分布

数据来源：绿盟科技全球 DDoS 态势感知系统（ATM），绿盟黑洞云清洗、绿盟科技威胁情报中心

5.5 小节

2020 年，我们监控到 DDoS 攻击次数为 47 万次（event_id 为粒度），攻击总流量 6.6 万 TB 。攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 65%。从一天 24 小时攻击占比来看，11 点到 19 点为攻击高峰攻击。从每周中 DDoS 攻击活动的分布来看，周中（周二、周三、周四）最常被攻击。2020 年主要的攻击类型是 UDP 类型，占总攻击次数的 24%。从流量占比来看，UDP Flood 发起的攻击流量占比最高，占比 67%。全年活跃团伙 45 个。

6. 僵尸网络态势

6.1 DDoS 僵尸网络 2020 年攻击概览

2020 年的 DDoS 僵尸网络活动中，主要攻击来自 Mirai、Gafgyt 和 Dofloo 等家族。

2020 年的 DDoS 攻击手段主要为 UDP flood、CC 和 TCP flood。

2020 年的僵尸网络控制端主要位于美国，而托管的云服务商中，Digital Ocean、OVH、ColorCrossing 和 Hostwinds 为其优先选项。

2020 检测到的 IoT DDoS 木马传播利用的各类漏洞种类超过了 140 种，其中 CVE-2017-17215（华为 HG532 路由器）、CVE-2014-8361（Realtek rtl81xx SDK 远程代码执行漏洞）和 ThinkPHP 远程命令执行漏洞位居前列。

6.1.1 DDoS 攻击事件及家族分布

2020 年上半年总计监测到攻击指令逾 120 万条，包含攻击事件逾 19 万次，主要由 9 个家族构成，其攻击事件比重如下：

表 6-1 僵尸网络攻击事件及家族分布

Family	Attack Count	Percent
Mirai	105362	55.64%
Gafgyt	27718	14.64%
Yoyo	21369	11.28%
Sdbot	21052	11.12%
XorDDoS	7899	4.17%
Dofloo	4187	2.21%
Nitol	1373	0.73%
天罚 DDoS	383	0.20%
Tsunami	23	0.01%

攻击指令方面，攻击事件少的 Dofloo 位列第一，占比约 60%。这主要源于其在常在局部时段以高频率下发针对少数目标的攻击指令。

表 6-2 僵尸网络攻击事件及家族分布

Family	Attack Cmds Count	Percent
Dofloo	727045	60.389%
Mirai	200081	16.619%
SDBot	116934	9.713%
XorDDoS	53563	4.449%
Yoyo	44682	3.711%
Gafgyt	42541	3.533%
天罚 DDoS	14578	1.211%
Nitol	4497	0.374%
Tsunami	23	0.002%

2020 年较活跃家族的攻击事件月度趋势如下图所示：

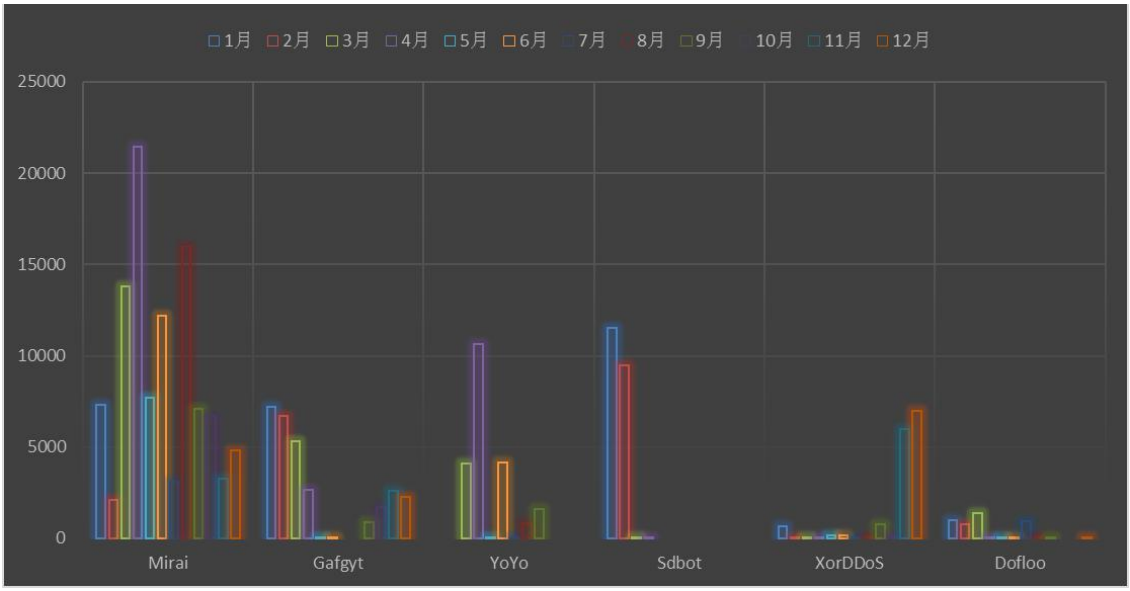

图 6-2 攻击事件趋势

（每个家族从左至右为 1~12 月数据）

可见，Mirai 全年保持活跃。Gafgyt 在年中有一段时间的沉寂期，此后一直未恢复之前的活跃度。YoYo 和 SDBot 只在特定月份活跃。XorDDoS 在年终迎来一波爆发。Dofloo 尽管指令数很多，活跃度高，但由于目标偏少，故而攻击事件较少。

6.1.2 DDoS 攻击事件及家族变种构成

各家族变种在攻击事件中的比例如下：

表 6-3 攻击事件及家族比例

Family	Variant	Attack Count	Percent
Mirai	mirai（统一流量）	105362	55.64%
Gafgyt	gafgyt_builds	17756	9.38%
	gafgyt_left	9102	4.81%
	gafgyt_rebirth	767	0.41%
	gafgyt_demon	84	0.04%
	gafgyt_amnesia	9	<0.01%
YoYo	DDOS.YOYO.S0P0R0.WO	21369	11.28%
SDbot	DDOS.SDBOT.S0P0R0.WO	21052	11.12%
XorDDoS	DDOS.XORDDOS.S0P0R0.LV	4030	2.13%
	xorddos	3869	2.04%
Dofloo	DDOS.DOFLOO.S0P0R0.LO	4187	2.21%
Nitol	DDOS.NITOL.S1P0R3.WV	1159	0.61%

	DDOS.NITOL.S0P0R0.WO	110	0.06%
	servstart	56	0.03%
	DDOS.NITOL.S0P0R15.WV	28	0.01%
	DDOS.NITOL.S0P3R7.WV	20	0.01%
天罚 DDoS	DDOS.TF.S0P0R0.LO	383	0.20%
Tsunami	DDOS.TSUNAMI.S0P0R1.IV	23	0.01%

（Mirai 各变种因其流量无显著差异，故全部归为一类）

可见 Gafgyt 和 Nitol 变种相对较多。其中 gafgyt_builds 在 Gafgyt 变种中制造了最多的攻击事件，同时根据 gafgyt_amnesia 低下的事件数，可见不同变种的流行度有很大差异。NITOL.S1P0R3.WV 在 Nitol 变种中最为活跃，不过 Nitol 变种事件数加起来也远远少于 Mirai 和 Gafgyt。

6.1.3 DDoS 攻击事件 C&C 分布

表 6-4 地理分布

Country	Count	Percent
美国	624	39.32%
荷兰	211	13.30%
法国	114	7.18%
德国	108	6.81%
中国	95	5.99%
俄罗斯	68	4.28%
英国	54	3.40%
加拿大	51	3.21%
罗马尼亚	51	3.21%
摩尔多瓦	35	2.21%
波兰	24	1.51%
新加坡	15	0.95%
奥地利	14	0.88%
瑞士	12	0.76%
乌克兰	10	0.63%
卢森堡	9	0.57%
印度	9	0.57%
南非	9	0.57%
意大利	8	0.50%
保加利亚	8	0.50%
韩国	8	0.50%
伊朗	7	0.44%
巴西	7	0.44%
瑞典	6	0.38%
泰国	4	0.25%
澳大利亚	3	0.19%
越南	3	0.19%
土耳其	3	0.19%
捷克	2	0.13%

希腊	2	0.13%
芬兰	2	0.13%
立陶宛	2	0.13%
挪威	1	0.06%
葡萄牙	1	0.06%
西班牙	1	0.06%
丹麦	1	0.06%
日本	1	0.06%
马来西亚	1	0.06%
克罗地亚	1	0.06%
塞舌尔	1	0.06%
爱尔兰	1	0.06%

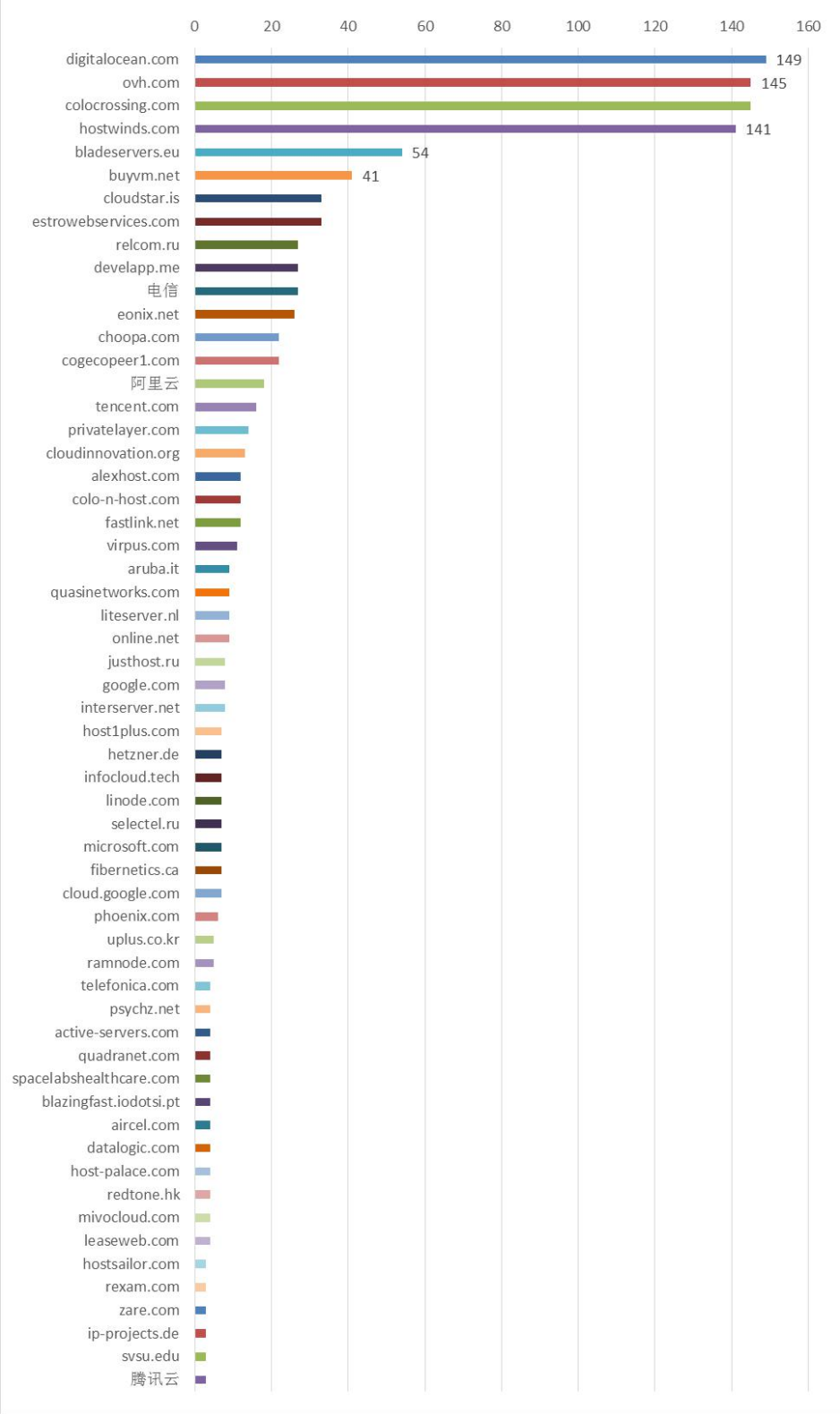

图 6-3 C&C 所属云服务及运营商分布

C&C 主要托管于云厂商，排名前四的分别是 Digital Ocean、OVH、ColorCrossing 和 Hostwinds。

6.1.4 DDoS 攻击指令活跃度日级分布

Dofloo（红）活跃度总体呈不连续态势，但在 1~3 月、8~9 月以及 12 月的局部时段异常活跃，尤其是在 12 月下旬达到最高峰且持续。Mirai（蓝）全年分布平均，在 7 月中下旬有明显的沉寂期，且 8 月后的活跃度明显不如之前。SDBot（橘黄）仅在 2 月上旬和 7 月初异常活跃，其余时间少见踪影。Yoyo（绿）在 3~7 月期间处于活跃期。XorDDoS（黄）在年底非常活跃，其余时间同样较为沉寂。剩余家族活跃度相对更低，已不见于图。

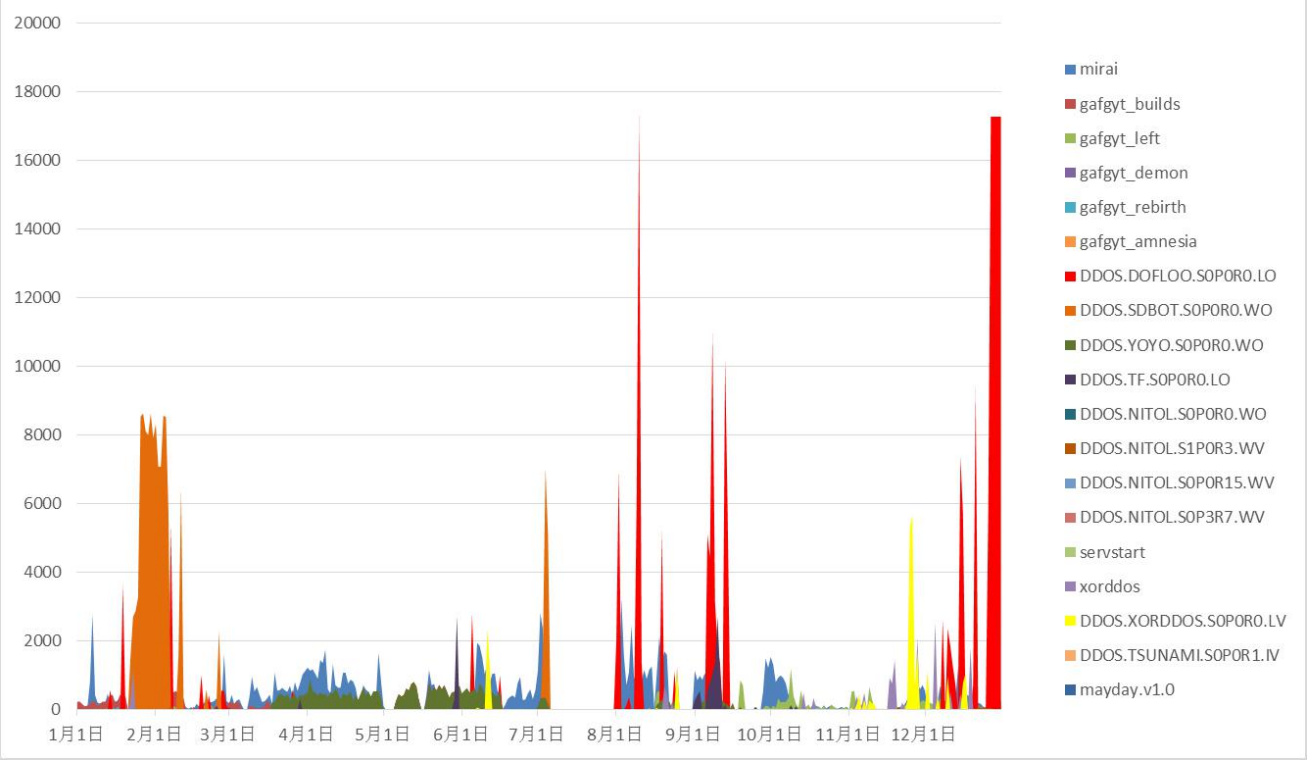

图 6-4 攻击指令活跃度日级分布

6.1.5 DDoS 攻击所使用 FLOOD 类型分布

表 6-5 攻击所使用 FLOOD 类型分布

Flood Type	Count (按次数统计)	Percent
UDP flood	523049	37.12%
CC	293349	20.82%
TCP Flood	253799	18.01%
SYN Flood	130945	9.29%
ACK Flood	54494	3.87%
混合类型	51832	3.68%
HTTP Flood	47096	3.34%
GRETH	15622	1.11%
COMPRESS Flood	15252	1.08%
DNS Flood	8747	0.62%
ICMP Flood	6570	0.47%
IP Flood	5961	0.42%
Proxy	2261	0.16%
不明类型	125	0.01%
SMTP Flood	120	0.01%

6.1.6 攻击使用的 Linux/IoT 漏洞分布

检测到的华为路由器漏洞使用率占比接近四分之一。其次分别是 Realtek rtl81xx SDK 远程代码执行漏洞和 ThinkPHP 远程命令执行漏洞。

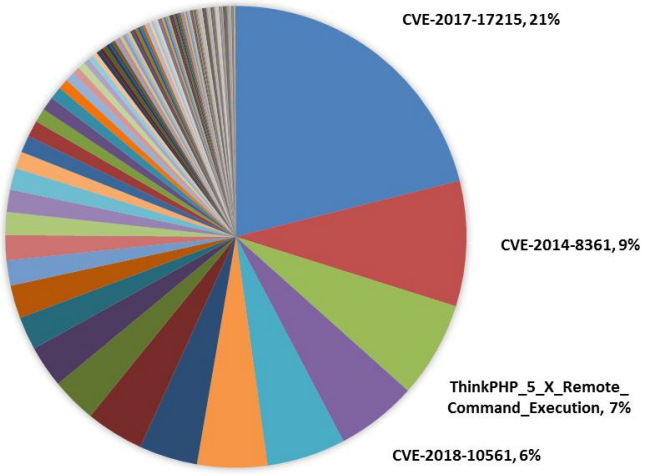

图 6-5 Linux/IoT 漏洞分布

下表显示了检测到的所有漏洞及使用次数。其中粗体表示 2020 年的新漏洞。

表 6-6 攻击事件使用漏洞分布

Vulnerability	Count
CVE-2017-17215	23078
CVE-2014-8361	9597
ThinkPHP_5_X_Remote_Command_Execution	7381
CVE-2018-10561	6213
ZyXEL_P660HN_T_v1_ViewLog_asp_privilege_escalation	6038
Linksys_E_series_Unauthenticated_Remote_Code_Execution	5368
CVE_2017_17215_2	4479
JAWS_Webserver_unauthenticated_shell_command_execution	4447
Common_Shell_Command_Abuse	3451
Eir_D1000_Wireless_Router_WAN_Side_Remote_Command_Injection	3221
CVE-2015-2051	2539
D_Link_DSL_Devices_login_cgi_Remote_Command_Execution	2536
Netlink_GPON_Router_1_0_11_Remote_Code_Execution	1930
CVE-2018-17173	1922
CVE_2020_10173	1754
CCTV-DVR Remote Code Execution	1703
Netgear_DGN1000_1_1_00_48_Setup_cgi_Remote_Code_Execution	1664
CVE-2016-6277	1309
Vacron_NVR_RCE	1308
Symantec_Web_Gateway_5_0_2_8_Remote_Code_Execution	1241
AVTECH_IP_Camera_NVR_DVR_Devices_Multiple_Vulnerabilities	1065
D_Link_OS_Command_Injection_via_UPnP_Interface	1063
Zyxel_P660HN_Remote_Command_Execution	966
CVE_2020_5722	785
CVE_2019_16920	730
CVE_2020_8515	570
unknown_exploit_ToolsCgi_moobot_20201103	554
CVE_2019_18396	454
CVE-2017-8221	413
CVE_2020_8218	354
Apache_Kylin_3_0_1_Command_Injection_Vulnerability	300

EnGenius_RCE	285
AVCON6_systems_management_platform_OGNL_Remote_Command_Execution	282
CVE_2013_5912	273
ACTi_ASOC_2200_Web_Configurator_2_6_Remote_Command_Execution	273
Fritz_Box_Webcm_Command_Injection	231
CVE-2014-9727	231
Edimax_Technology_EW_7438RPn_v3_Mini_1_27_Remote_Code_Execution	228
Fastweb_Fastgate_0_00_81_Remote_Code_Execution	228
CVE_2013_5948	228
DLink_and_TRENDnet_ncc2_service_multiple_vulnerabilities	220
vBulletin_5_6_2_widget_tabbedContainer_tab_panel_Remote_Code_Execution	213
Xfinity_Gateway_Remote_Code_Execution	203
CVE-2018-7841	203
CVE-2018-14933	203
Sar2HTML_Remote_Code_Execution	203
CVE-2018-15716	203
3Com_OfficeConnect_Code_Execution	195
CVE-2011-3587	195
CVE_2019_14931	182
CVE_2020_7209	174
Netis_WF2419_2_2_36123_Remote_Code_Execution	169
CVE-2014-9094	168
CVE-2017-6884	167
NUUO_OS_Command_Injection_3	167
CVE_2019_7276	150
CVE_2019_7405	150
TOTOLINK_Routers_Backdoor_Remote_Code_Execution	150
CVE_2019_16057	150
CVE_2018_13023	150
NETSYS_TOPSEC_DLink_internet_behaviour_management_device_RCE	150
ZTE_Remote_Command_Execution	150
CVE_2020_9054	150
CVE_2018_19276	150
CVE_2020_13782	143
CVE_2020_5902	141
Seowon_Slc_130_And_SLR_120S_Router_RCE	124
CVE_2017_5174	124
zero_day_2020_09_04	123
Netgear_R7000_Router_Remote_Code_Execution	122

CVE_2014_2321	117
Zeroshell_3_6_0_3_7_0_Net_Services_Remote_Code_Execution	110
Hootoo_HT_05_Remote_Code_Execution	105
ASUS_DSL_N12E_C1_1_1_2_3_345_Remote_Command_Execution	98
wordpress_brute_force	96
CVE_2019_7238	94
BEWARD_N100_H_264_VGA_IP_Camera_M2_1_6_Remote_Code_Execution	83
CVE-2007-3010	81
ZTE_ZXV10_H108L_Remote_Command_Execution	77
Seowonintech_Devices_Remote_Command_Execution	70
CVE_2020_10987	67
unknown_exploit_SetNet_20200930	64
CVE-2012-4869	54
CVE_2012_0262	53
Beckhoff_CX9020_CPU_Module_Remote_Code_Execution	53
Redmine_SCM_Repository_0_9_x_1_0_x_Arbitrary_Command_Execution	53
EyeLock_nano_NXT_3_5_Remote_Code_Execution	53
CVE-2018-11510	53
CVE_2005_2773	53
op5_7_1_9_Remote_Command_Execution	53
FLIR_Thermal_Camera_FC_S_PT_Command_Injection	53
CVE-2013-4861	53
CVE-2019-12989	53
Spreecommerce 0.60.1 - Arbitrary Command Execution	53
CVE_2006_4000	53
WePresent_WiPG_1000_Command_Injection	53
Gitorious_Arbitrary_Command_Execution	53
Dell_KACE_Systems_Management_Appliance_Unauthenticated_Remote_Code_Execution	53
HomeMatic_Zentrale_CCU2_Remote_Code_Execution	53
CVE-2005-2847	53
CVE-2009-2288	53
OpenDreamBox_2_0_0_Plugin_WebAdmin_Remote_Code_Execution	53
Iris_ID_IrisAccess_ICU_7000_2_Remote_Command_Execution	53
CVE_2003_0050	53
CVE_2017_16602	53
Dogfood_CRM_spell_php_Remote_Command_Execution	53
CVE-2019-17270	53
CVE-2011-5010	53

Belkin_Wemo_UPnP_Remote_Code_Execution	53
CVE-2015-2208	53
Linksys_WAG54G2_Web_Management_Console_Arbitrary_Command_Execution	53
CVE-2019-2725	53
Mitel_AWC_Command_Execution	53
CVE-2006-2237	53
CCBILL_CGI_ccbillx_c_whereami_cgi_Remote_Code_Execution	53
CVE-2019-3929	53
CVE-2018-6961	53
CVE-2005-0116	53
CVE-2013-5948	53
CVE-2008-3922	53
CVE-2010-5330	53
CVE-2013-5758	53
CVE_2014_3914	53
CVE_2019_16072	53
CVE-2017-5173	53
Sickbeard_0_1_Remote_Command_Injection	50
Avaya_Aura_Communication_Manager_5_2_Remote_Code_Execution	46
CVE_2019_6989	33
SAPIDO_RB_1732_Remote_Command_Execution	32
CVE_2017_6316	32
Zyxel_Secumanager_Pre_auth_RCE_with_chrooted_access	29
Joomla_Vemod_News_Mailer_1_0_SQL_Injection	28
CVE_2020_3657	21
CVE_2020_12109	19
CVE_2020_9484	19
CVE_2017_17105	19
CVE-2018-14417	11
CVE_2017_9841	11
CVE_2018_11776	10
Tea_LaTex_1_0_Remote_Code_Execution	10
CVE-2015-2280	10
xmlrpc_brute_force	4
ESCAM_IP_Camera_Remote_Code_Execution	3
AVTECH_Unauthenticated_Command_Injection	3
Fastweb_FASTGate_0_00_67_Remote_Code_Execution	2
CVE-2008-0149	1
D_Link_DCS_930L_Remote_Command_Execution	1

6.2 威胁捕获 2020 年数据概览

蜜罐方面，2020 年互联网攻击活动分别由恶意连接、DDoS 反射、暴力破解和漏洞利用构成。

恶意连接端口方面，针对 Chargen 端口的连接占比最多，达到 46%，可能涉及潜在 DDoS 攻击之前的扫描。

漏洞利用方面，针对 DVRTV 摄像头、Dlink 路由器、MVPower 摄像头和 Redis 的攻击最多，大部分是物联网设备。而 Mssql 则是受到攻击最多的数据库。

DDoS 反射攻击方面，DNS 占据近 33%，其次是 Cldap 和 Upnp。2020 年共计捕获 DDoS 反射攻击事件超过 6015 万例，其中最长的持续时间高达 86 小时左右。

6.2.1 攻击总览

2020 年，公网威胁捕获系统共计捕获高低危攻击 2207678439 次，恶意连接 958602783 次，占比 83.19%；漏洞利用 6678664 次，占比 0.58%；暴力破解 126838872 次，占比 11.01%；DDoS 攻击 60152423 次，占比 5.22%；其中恶意连接占比最多。

后半部分将针对暴力破解，渗透行为，邮件攻击，应用程序攻击，DDoS 反射攻击等典型攻击行为进行详细分析。

2020 年攻击类型占比情况如下：

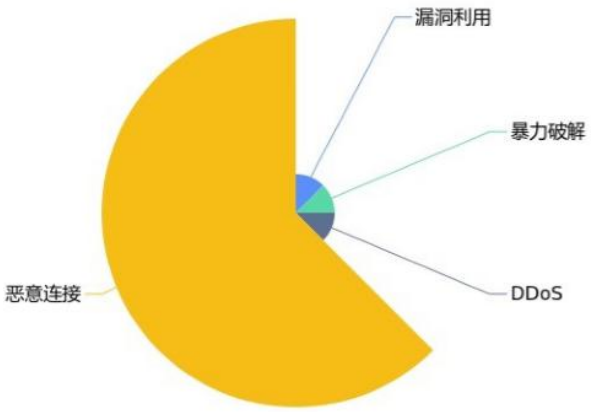

图 6-6 2020 年攻击类型占比情况

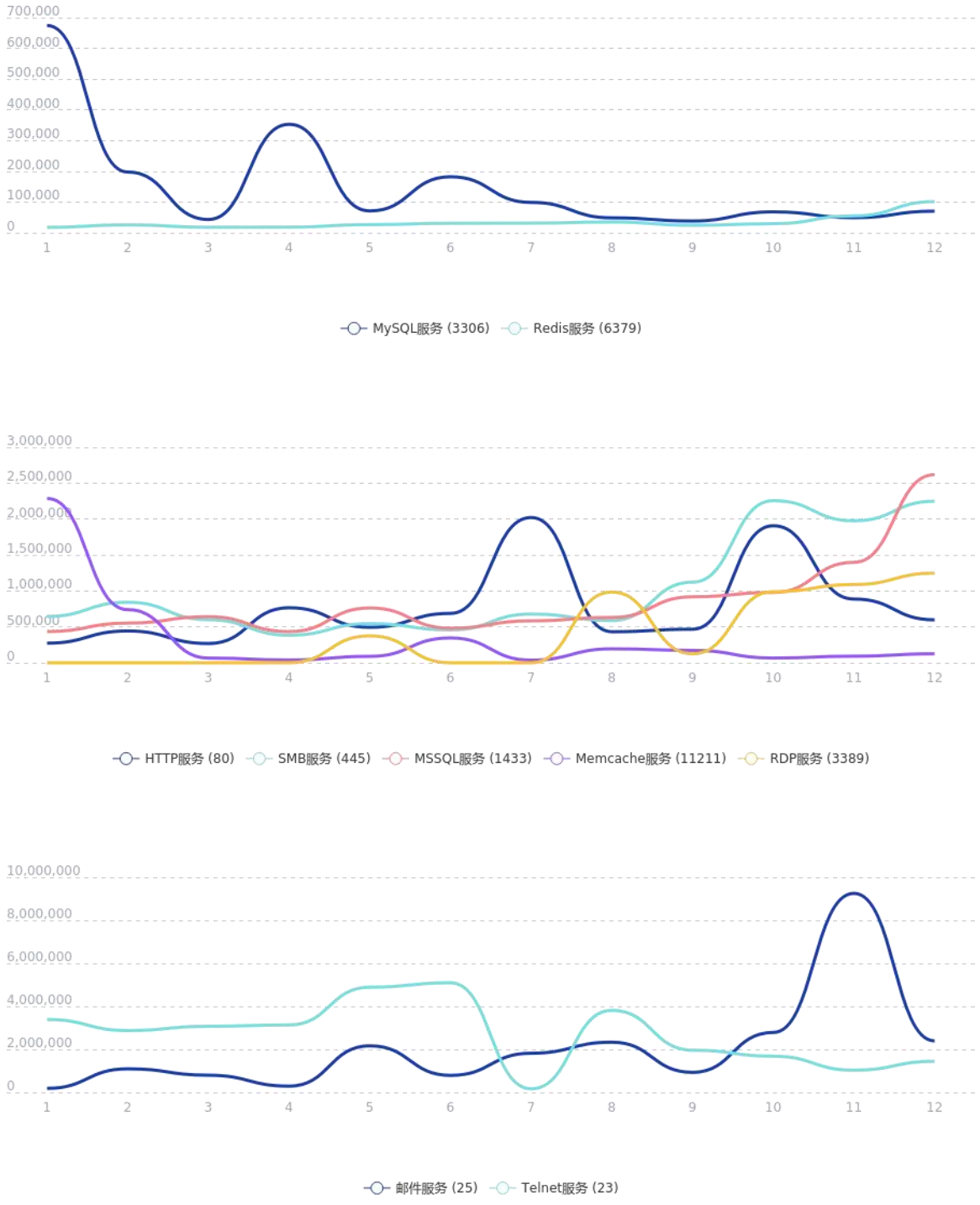

图 6-7 2020 年高危端口攻击变化趋势

2020 年漏洞利用排行榜如下：

表 6-7 2020 年漏洞利用次数分布

漏洞编号或名称	设备类型或服务类型	厂商或具体设备	利用次数
EDBID41471	DVRTV	MVPower	2153023
EDBID37171	Router	DLink	1348099
EDBID40500	IpCameraNvrDvr	AvtechIpCameraNvrDvrDevices	1013959
Redis未授权访问漏洞	Redis	通用服务	413292
EDBID36553	JBoss	通用服务	400472
CVE-2017-7504	JBoss	通用服务	370010
EDBID40740	Router	EirD1000WirelessRouter	209320
CVE-2014-8361	SDK	Realtek	169450
CVE-2017-5638	struts2	通用服务	154879
CVE-2019-3396	Confluence	通用服务	147967

6.2.2 典型攻击分析

6.2.2.1 全网威胁感知服务

应用服务威胁趋势统计如下。2020 年的端口访问以 Chargen 端口为主和 Ldap 端口为主。

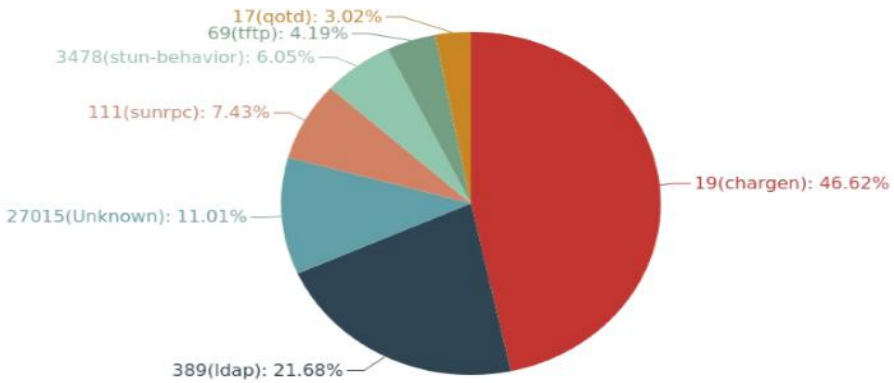

图 6-8 应用服务威胁趋势

6.2.2.2 暴力破解

2020 全年共计捕获 1024598775 次针对公网爆破攻击。其中用户名密码对共计捕获 1402384 个。

利用 TOP5 如下:

表 6-8 用户名密码对利用次数

用户名	密码	利用次数
root	admin	59262807
root	None	15911308
root	1234	8979711
root	password	3477284
nproc	nproc	2665479

表 6-9 攻击者使用的常用密码

密码	涉及设备	密码复杂度	利用次数
admin	通用	过于简单	59431020
None	通用	过于简单	16053832
1234	通用	过于简单	9104299
password	通用	一般	3617813
nproc	通用	过于简单	2665488

登录尝试的前五个国家/地区为:

表 6-10 暴力破解排名前五国家

攻击国家	攻击次数
Netherlands	522331928
Panama	67358009
Moldova	65120501
Russian Federation	52908121
China	26200158

6.2.2.3 渗透行为

2020 年中我们在公网部署的仿真服务捕获大量渗透行为，其中攻击者最常使用的命令如下：

表 6-11 常用命令

命令	入侵工具类型	使用次数
cat /proc/cpuinfo | grep name | wc -l	外部命令	2728641
uname -a	外部命令	2072867
cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}'	外部命令	2039853
free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}'	外部命令	2039187
ls -lh $(which ls)	外部命令	2038593

表 6-12 攻击源 IP 前五 IP

攻击IP	攻击次数
5.188.86.168	37345251
5.188.86.165	35895264
5.188.86.167	17490806
5.188.86.206	12385080
5.188.62.14	11842011

攻击 IP 全球分布情况：

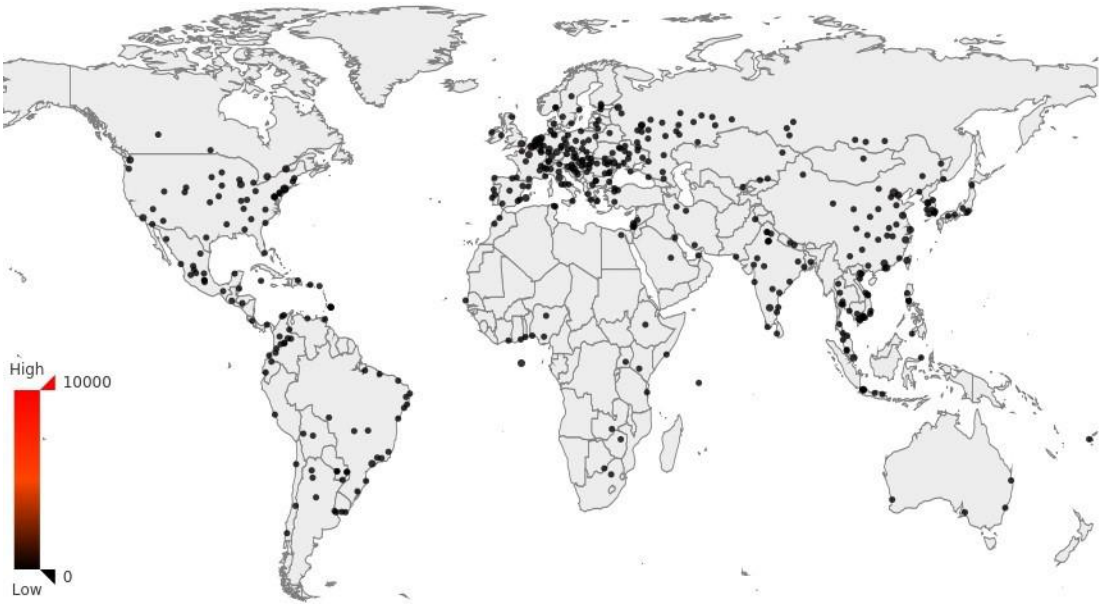

图 6-9 攻击 IP 全球分布

6.2.2.4 邮件攻击

2020 年中我们在公网部署的邮件仿真服务捕获 9251195 封邮件，共计捕获 2276 个非重复来源攻击者 IP。涉及 1424876 个受害目的邮箱。

表 6-13 攻击者针对目的邮箱

邮箱	使用次数
spameri@tiscali.it	8858
emeka@malatrade.com	2815
postmaster@khorasan.ac.ir	1938
berganza15000@yahoo.com	843
g.dan61@yahoo.ro	774

表 6-14 攻击者针对邮件服务商

邮件服务商	使用次数
hotmail.com	869238
yahoo.com	801965
gmail.com	785698
aol.com	319344
yahoo.co.jp	141532

6.2.2.5 应用程序漏洞利用

2020 年共计在公网捕获 6678664 次漏洞攻击行为。

最频繁利用的漏洞编号为 EDBID41471。

最频繁的设备类型为 DVRTV，占比为 34.36%。

最频繁的设备厂商为 MVPower，占比为 34.36%。

可以看出当前的漏洞攻击主要还是集中在物联网领域，值得重点关注。

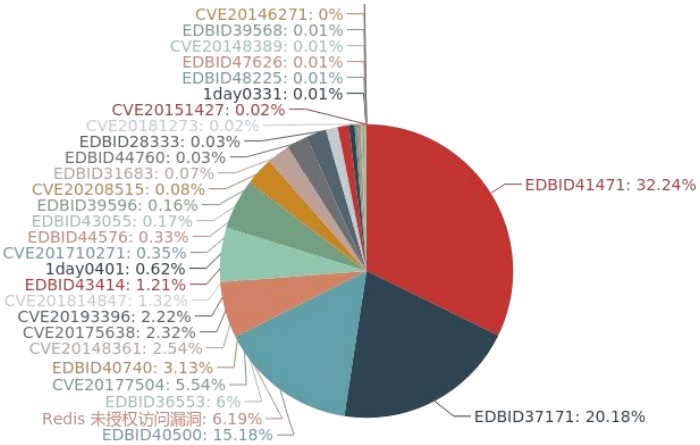

图 6-10 漏洞攻击及编号占比

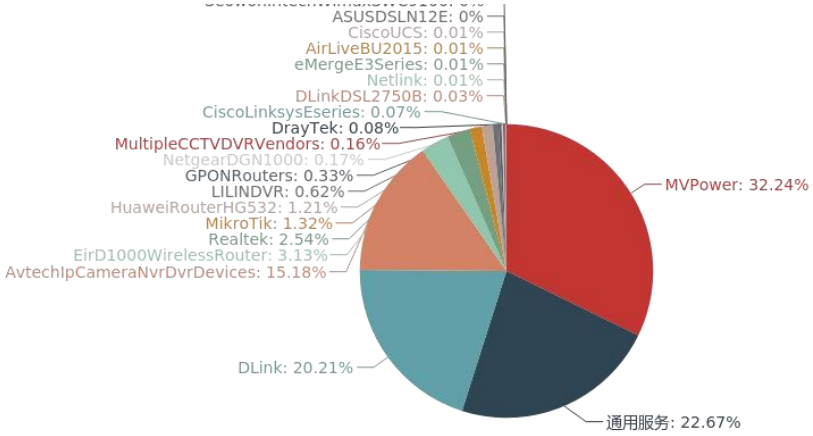

图 6-11 漏洞攻击针对厂商设备占比

数据库服务部分，捕获共计来源 IP 168920 个。Mysql 10984 个。MSsql 144245 个， redis 13691 个，非关系型数据库 13691 个。 爆破利用用户名密码对 11818 个。来源客户端软件 27360 种。

表 6-15 攻击者最常使用的数据库语句

数据库语句	使用次数
SET ARITHABORT ON; SET CONCAT_NULL_YIELDS_NULL ON; SET ANSI_NULLS ON;	534827

SET ANSI_NULL_DFLT_ON ON; SET ANSI_PADDING ON; SET ANSI_WARNINGS ON; SET ANSI_NULL_DFLT_ON ON; SET CURSOR_CLOSE_ON_COMMIT ON; SET QUOTED_IDENTIFIER ON; SET TEXTSIZE 2147483647;	
exec sp_dropextendedproc \'xp_cmdshell\';	261512
dbcc addextendedproc(\'xp_cmdshell\',\'xplog70.dll\')	260570
EXEC sp_configure \'show advanced options\', 1;RECONFIGURE;exec SP_CONFIGURE \'xp_cmdshell\', 1;RECONFIGURE;	259932
xp_cmdshell \'net user k8h3d k8d3j9SjfS7 /ADD && net localgroup administrators k8h3d /ADD&netsh advfirewall firewall add rule name=mssql dir=in action=allow protocol=TCP localport=1433&netsh advfirewall firewall add rule name=web dir=in action=allow protocol=TCP localport=80\'	259676

表 6-16 攻击者最常攻击的数据库客户端

客户端名称	使用次数
WIN-0SHU94IO5C3	42653
smcVfSZe	38732
SERVER	37305
WIN-T9AMIA64D5P	32085
zbxx01	27799
DESKTOP-0AAVQO1	26612
ECS-T6-LARGE-2-	25814
YD-TJSJ	25453
BEYONDLIQUOR-PC	23881
BILLINGDEPARTME	21279

Web服务部分，2020年共计捕获130284621次WEB攻击，涉及584135个攻击IP。41250个来源User Agent，395846个请求路径。

在捕获的WEB 攻击中，我们发现大部分的漏洞利用为物联网漏洞，由于物联网设备的脆弱性，针对物联网设备的攻击占比逐步上升。

表 6-17 攻击者最常使用的 User-Agent

User-Agent	使用次数
Mozilla/5.0 (Windows NT 5.1; rv:9.0.1) Gecko/20100101 Firefox/9.0.1	12609110
Mozilla/5.0(Windows NT 10.0; Win64; x64) Apple WebKit/537.36(KHTML,like Gecko) Chrome/74.0. 3729.169 Safari/537.36	1391157
Snickers-Avtech	1337087
Mozilla/5.0	1200876
Wget/1.12.1	1177053
python-requests/2.6.0 CPython/2.7.5 Linux/3.10.01127.13.1.el7.x86_64	1074896
python-requests/2.6.0 CPython/2.6.6 Linux/2.6.32754.25.1.el6.i686	828984
Mozilla/5.0(Windows NT 6.1; Win64; x64;rv:56.0) Gecko/20100101 Firefox/56.0	816071
Mozilla/5.0(Windows NT 10.0;Win64;x64;rv:76.0) Gecko/20100101 Firefox/76.0	764864
Mozilla/5.0(Windows NT 10.0;WOW64) AppleWe bKit/537.36(KHTML,like Gecko) Chrome/61.0.3163.100 Safari/537.36	527019

表 6-18 攻击者最常使用的攻击路径

路径	访问次数
/	10836911
/shell	3069125
/ws/v1/cluster/apps/index.asp	2099836
/HNAP1/	1438048
/videostream.cgi	1172289
/cgi-bin/nobody/index.asp	793606
/index.asp	637784
/cgi-bin/nobody/Search.cgi	582930
/_cat/indices	487401
/nobody/ez.htm	429196

6.2.2.6 DDoS 反射攻击

2020年捕获60152423次DDoS反射攻击事件，其中dns服务全年攻击

利用最多。

攻击次数最高的DDoS反射攻击事件受害IP为92.185.238.144，持续时间达到86.08小时。与此同时，我们也捕获到了针对公网10399351个受害IP的DDoS反射攻击事件。

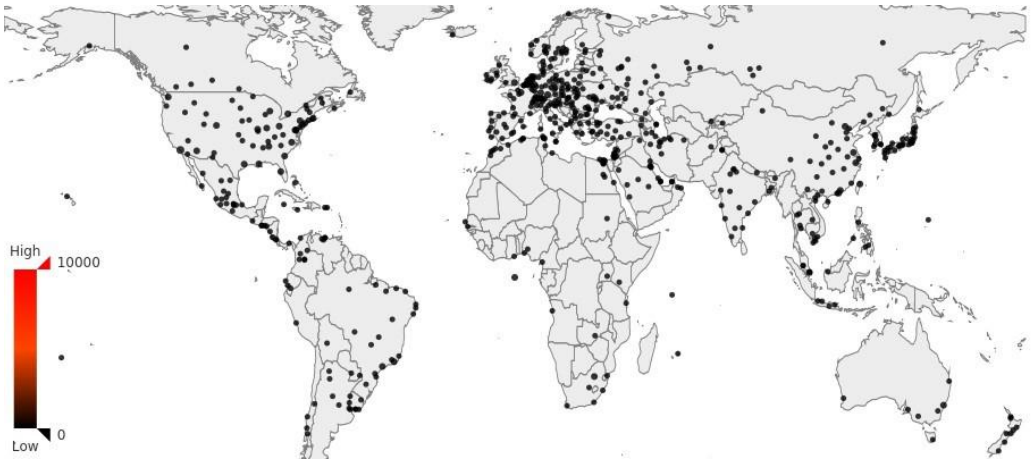

图 6-12 DDOS 反射攻击受害者分布

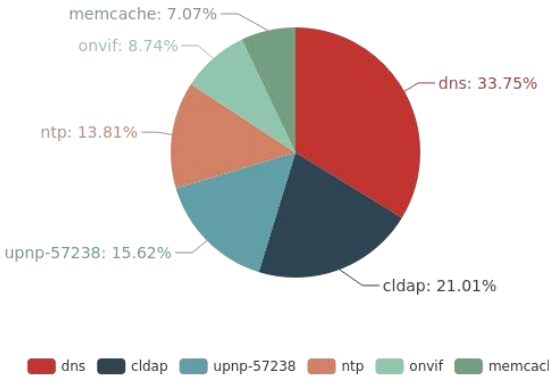

图 6-13 DDOS 反射攻击脆弱服务占比

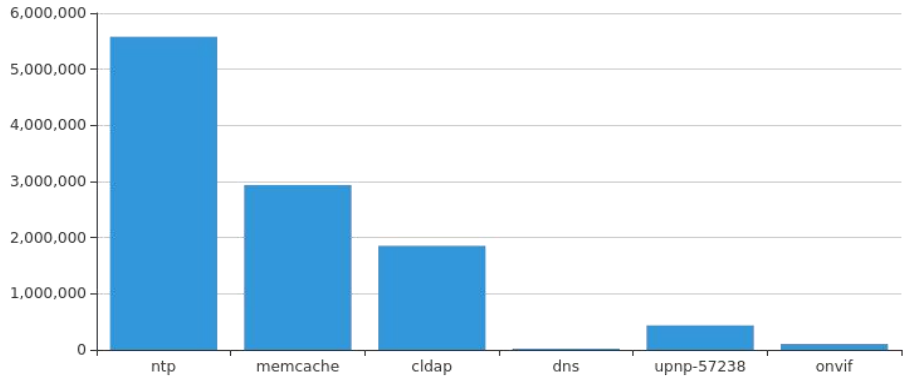

图 6-14 反射攻击对应反射源 IP 数目

6.2.3 挖矿僵尸网络态势

通过绿盟科技的威胁捕获系统，我们长期监测了一个面向门罗币挖矿的僵尸网络。该僵尸网络通过弱口令爆破入侵主机，以植入僵尸程序的方式获取控制权限，同时使用下载器下载并执行门罗币挖矿病毒脚本，实现恶意挖矿。

该挖矿僵尸网络在 2020 年的整体活跃情况呈增长趋势，活跃肉鸡总量达到 57038 台，其中在中国的肉鸡最多，达到 22472 台，占比 39%。开放 22 端口的肉鸡数有 22472 台，占比接近所有肉鸡的 25%。在已知的资产情报数据中，这些肉鸡的主要设备类型是路由器和摄像头。另外，该挖矿僵尸网络最常用的爆破弱口令是 nproc-nproc。详细情况见下文。

6.2.3.1 活跃情况

通过对 2020 年每月活跃的肉鸡数进行统计，可得到该挖矿僵尸网络的活跃情况。如图 6-14 所示，该挖矿僵尸网络在 2020 年的整体活跃情况呈增长趋势，在 11 月份肉鸡数最高，达到 18352 台。

图 6-15 挖矿僵尸网络 2020 年活跃情况

6.2.3.2 肉鸡国家分布情况

从地理位置维度对挖矿僵尸网络肉鸡进行分析，得到肉鸡国家数量 Top10。如图 6-15 所示，处于中国的肉鸡数最多，为 22472 台，占比 39%。

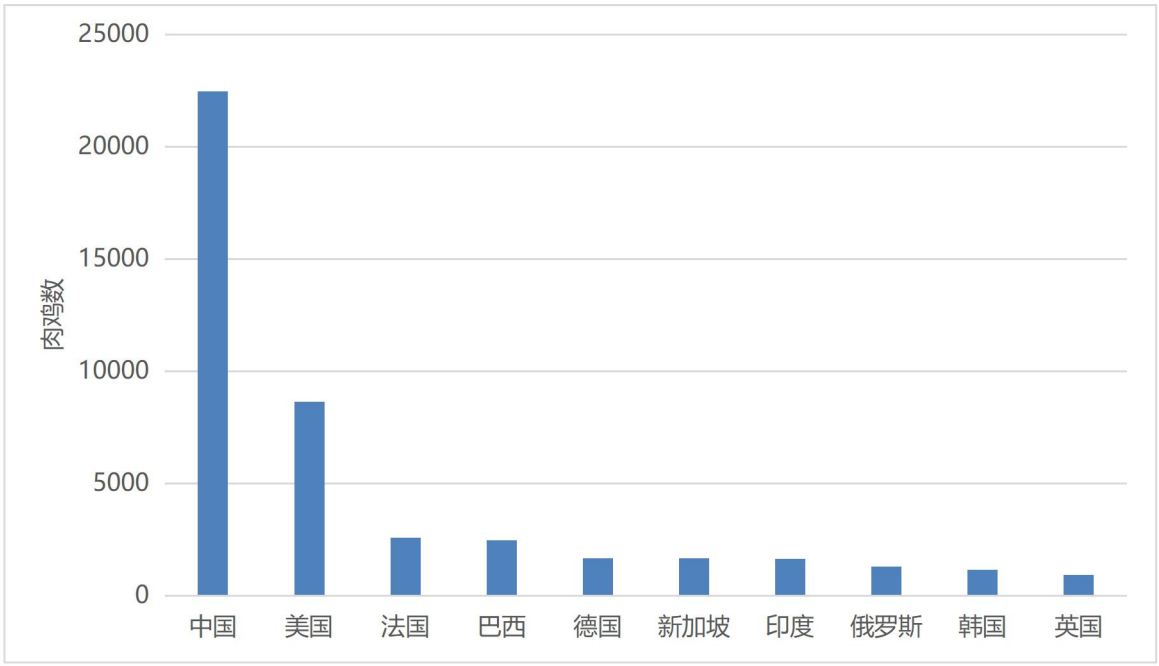

图 6-16 肉鸡国家数量 Top10

6.2.3.3 肉鸡开放端口分布

关注这些肉鸡的端口分布。如图 6-13 所示，这些肉鸡开放的端口前十名为：22、80、443、3306、21、8080、123、3389、53、25，开放的端口最多的是 22 端口，开放 22 端口的肉鸡占接近所有肉鸡的 25%。

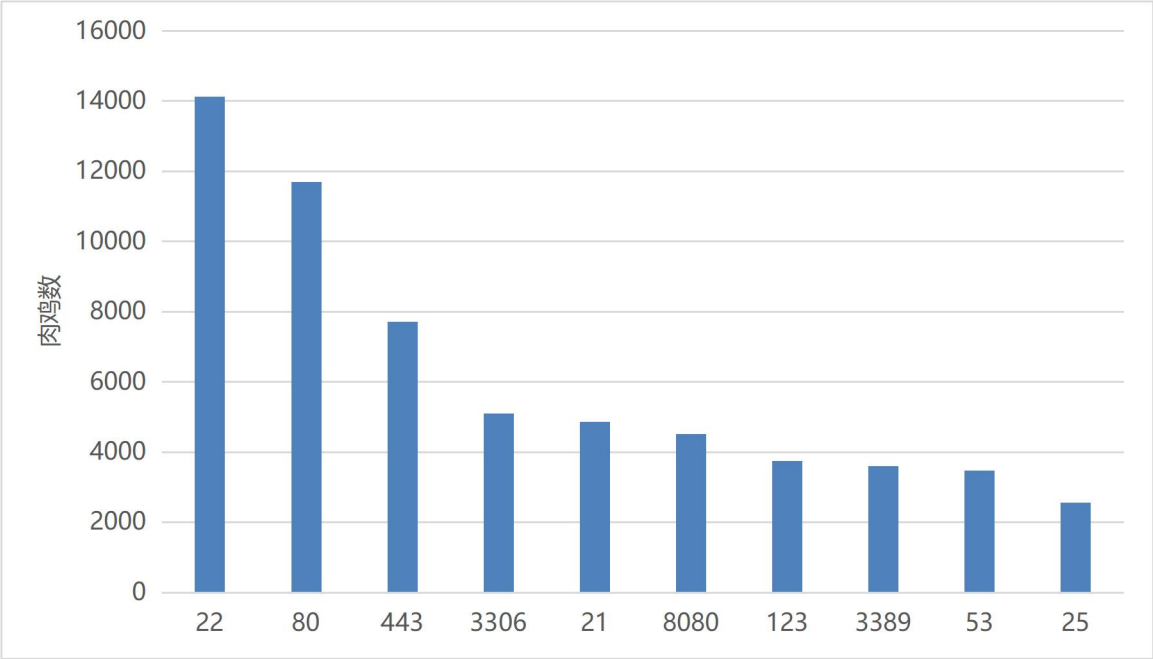

图 6-17 肉鸡开放端口数量 Top10

6.2.3.4 肉鸡设备类型分布

在已知的资产情报数据中，这些肉鸡有 12%为物联网设备。如图 6-17 所示，这些物联网设备中 35%为摄像头，34%为路由器。

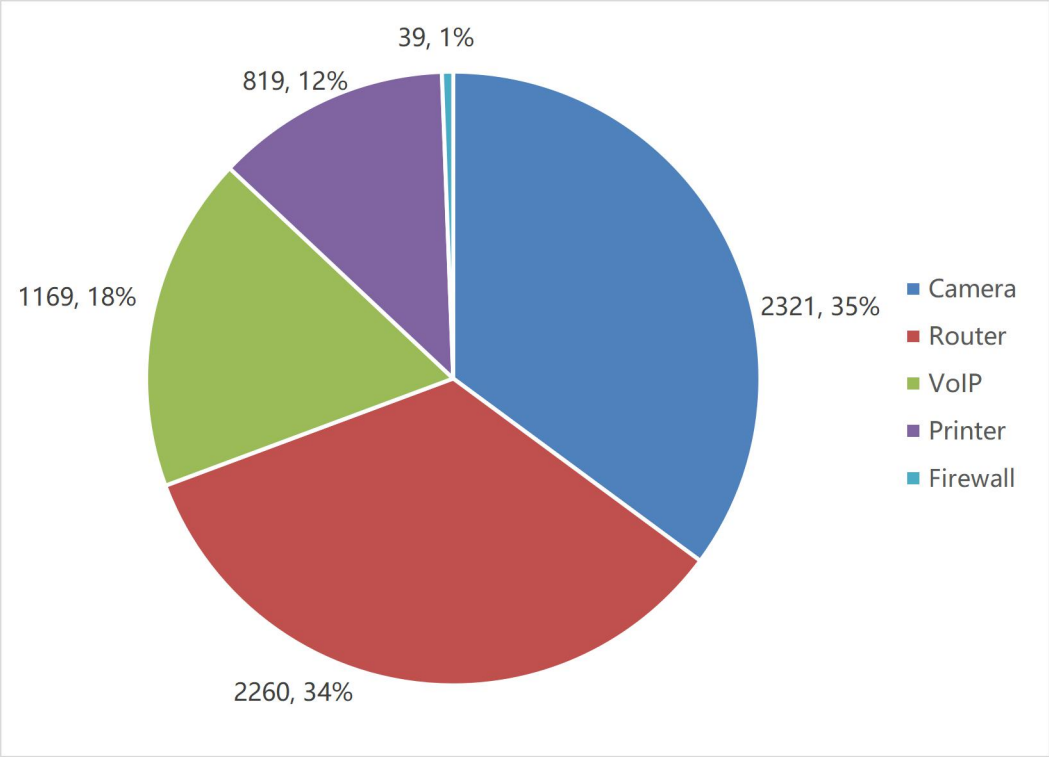

图 6-18 肉鸡设备类型分布

6.2.3.5 爆破弱口令情况

攻击者通过弱口令爆破攻击，未授权访问入侵主机。暴力破解字典 Top5 如表 6-18 所示，该挖矿僵尸网络最常用的弱口令是 nproc-nproc。

图 6-19 暴力破解字典及使用次数

排名	账号-密码	使用次数
1	nproc-nproc	452375
2	root-1QAZ2wsx	537
3	root-12345	517
4	guest-guest	510
5	root-p@ssw0rd	507

6.2.3.6 应对措施

我们发现大多数挖矿僵尸网络主要还是以端口扫描和弱口令爆破作为传播入口的，因此关键漏洞修复和弱口令入侵这些老生常谈的问题依然值得关注，在此我们重申几点注意事项：

（1） 重视 Telnet 等服务的弱口令问题，加强口令强度

（2） 配备必要的安全软硬件产品，保障系统安全

（3） 即时安装补丁和修复漏洞，避免漏洞利用

（4） 检查所有开放的服务端口，关闭不必要的端口