网络安全威胁态势分析 月报

2020 年 12 月

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

总体看十二月份的新增漏洞呈上升趋势，新增高危漏洞 212 个，主要分布在 Microsoft、Apple、Google、Cisco、Mozilla、IBM、Aruba Networks、SourceCodester 等厂商的主要产品中。

2020 年 12 月绿盟科技安全漏洞库共收录 970 个漏洞[1]，其中高危漏洞 212 个，微软高危漏洞 33 个。绿盟科技收录高危漏洞数量与前期相比呈上升趋势。

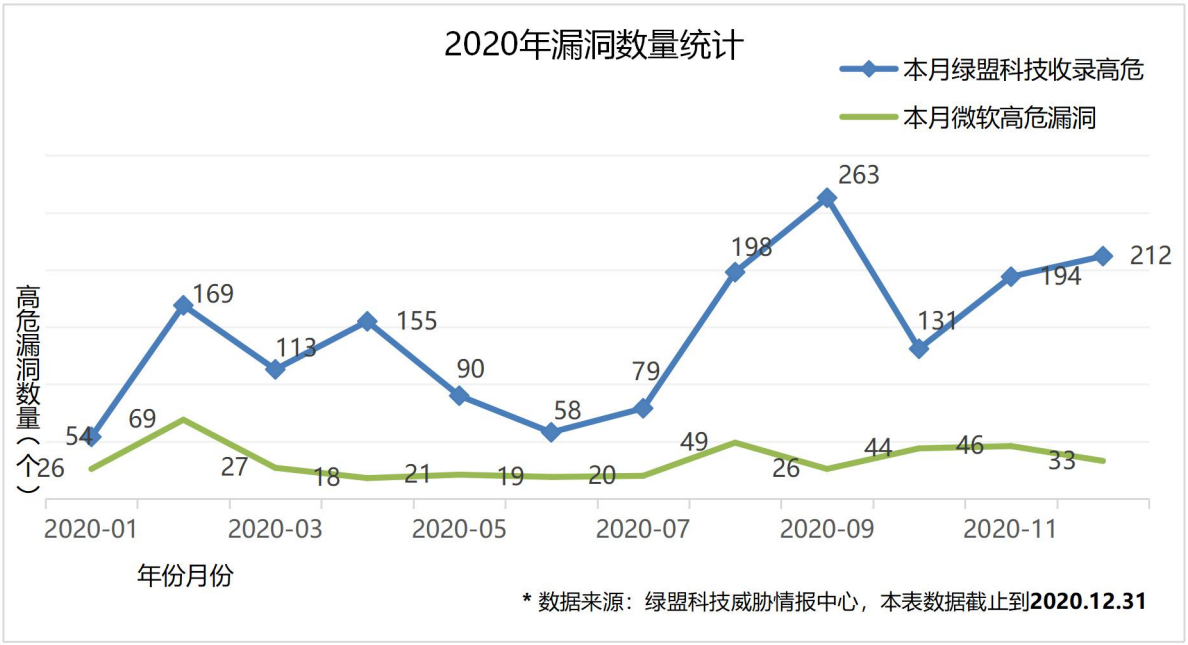

图 1-1 高危漏洞数量统计对比

1.2 恶意软件态势综述

2020 年 12 月份数据与 2020 年 1 至 12 月份数据中恶意软件各类型分布如下图所示。12 月份各恶意软件类型占比相比 2020 年全年情况有所波动，后门活动占比下降明显，挖矿活跃度较于全年有所降低，总占比 52%左右；此外，蠕虫，木马，勒索均表现相对活跃。

[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；

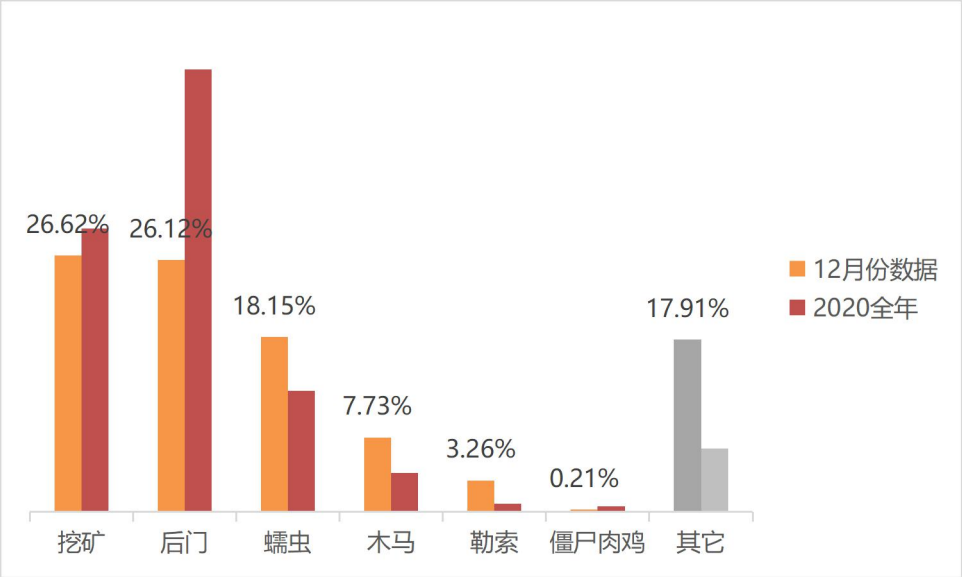

图 1-2 恶意软件类型

1.3 物联网安全态势综述

本月漏洞平台 Exploit-DB 新增 12 个物联网漏洞利用，存在 2 个 RCE 类漏洞，大部分危害程度较低。

本月有 3 个值得重点关注的物联网安全事件：

（1）Citrix 证实 NetScaler 的 ADC 正在受到 DDoS 攻击

（2）研究人员把 RAM 变成 WiFi 卡，从未联网的系统中窃取数据

（3）尽管修复了漏洞，但 Android 应用程序仍暴露了 1 亿用户的信息

本月蜜罐日志中的 66219 个源 IP 进行分析，其中 45757 个 IP 发起过漏洞利用等恶意行为，环比上月减少 5.14%。从关联到恶意行为的 IP 分布在了 174 个国家和地区，从国家分布情况来看，中国最多，占比达到了 32.14%。

1.4 DDOS 攻击态势综述

12 月我们监控到全球 DDoS 攻击次数为 34 万次（sip 为粒度），攻击总流量 25TB（数据来源：绿盟科技全球 DDoS 态势感知系统）。

攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 84%。从一天 24 小时攻击占比来看，凌晨 5 点为攻击高峰攻击。从每周中 DDoS 攻击活动的分布来看，周四最常被攻击。12 月份主要的攻击类型是 SYN Flood 类型，占总攻击次数的 67%。从流量占比来看，UDP Flood 发起的攻击流量占比最高，占比 27%。根据 2020 年 12 月的 DDoS 攻击数据进行聚类分析，共发现 3 个活跃团伙。

1.5 僵尸网络及蜜罐态势综述

在 2020 年 12 月份的 DDoS 僵尸网络活动中，监控到的攻击指令较 11 月有大幅度回升。XorDDoS 制造了最多的攻击事件，Dofloo 产生了最多的攻击指令。

12 月检测到的 DDoS 攻击手段主要为 CC、SYN flood 和 UDP flood。

12 月检测到的被用于托管僵尸网络控制端的已知云服务商/运营商中，位列前三的分别是 ColorCrossing、Maxko 和 Develapp。

12 月检测到的 IoT DDoS 木马传播利用的各类漏洞种类为 55 种，其中 CVE-2017-17215（华为 HG532 路由器）、CVE-2014-8361（Realtek SDK miniigd SOAP 服务远程代码执行）和 CVE-2018-10561（GPON 光纤路由器漏洞）位居前三。

2. 漏洞态势

2.1 漏洞类型分析

在本月收录的 212 个高危漏洞中，包括输入验证错误、访问验证错误、权限错误、资源管理错误、来源验证错误、边界条件错误等漏洞类型。具体数量如图 2-1 所示。

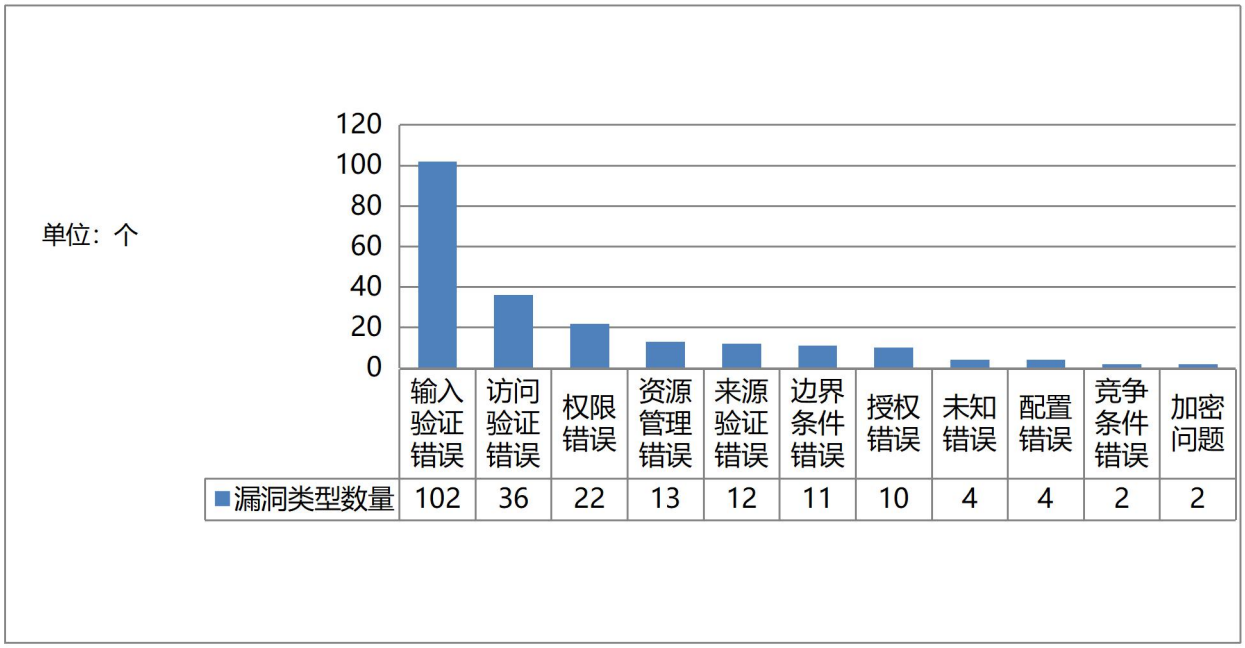

图 2-1 高危漏洞类型数量

2.2 漏洞分布分析

212 个高危漏洞主要分布在 Microsoft、Apple、Google、Cisco、Mozilla、IBM、Aruba Networks、SourceCodester 等厂商的主要产品中，共涉及 94 个厂商，其中数量 TOP15 的分布如图 2-2 所示。

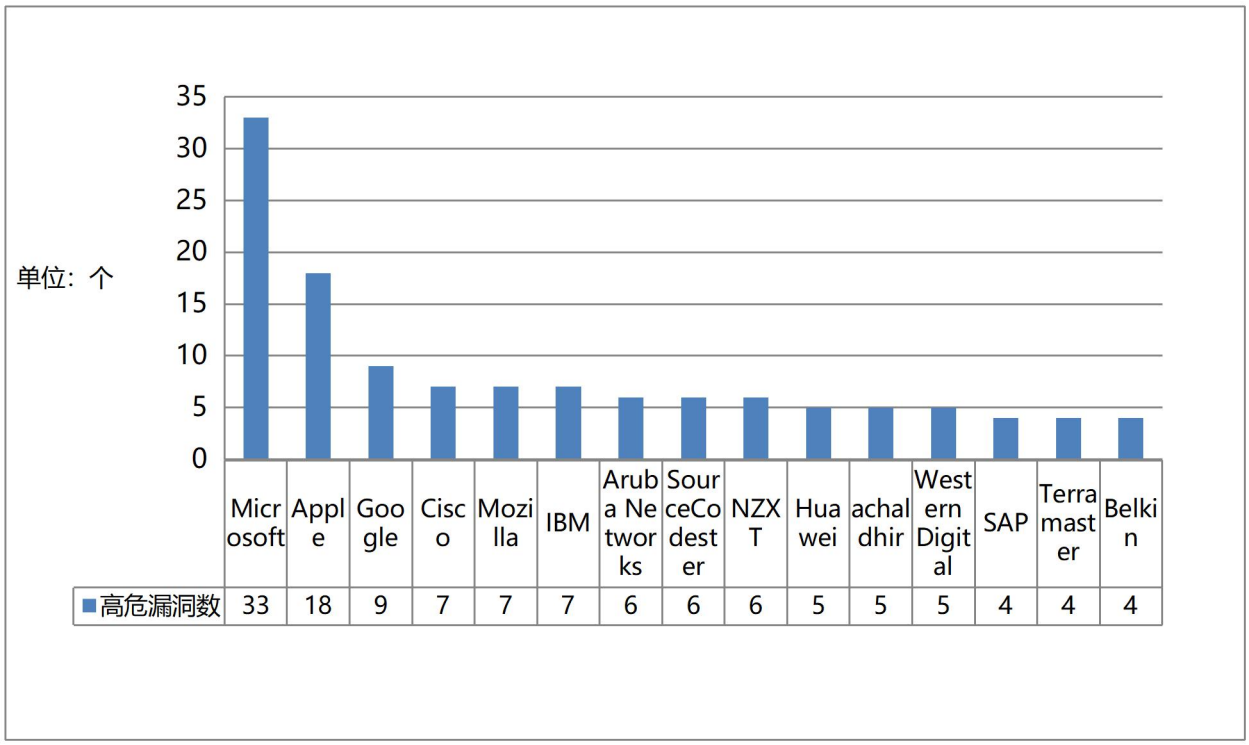

图 2-2 高危漏洞数目

其中微软相关的漏洞有 33 个，涉及 Windows 系统、Office、Exchange Server、Dynamics 365、Visual Studio Code TS-Lint 插件、Visual Studio 2019、SharePoint、Azure Sphere 等产品。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。

Apple 相关的漏洞有 18 个，主要分布在各个操作系统中，包含 macOS Catalina、iOS、iPadOS、tvOS、watchOS 等。攻击者可利用这些漏洞造成信息泄露、任意代码执行以及拒绝服务。

Google 相关的漏洞有 9 个，漏洞主要分布在 Android、Android kernel 中，攻击者可利用这些漏洞提升权限、造成信息泄露或拒绝服务。

Cisco 相关的漏洞有 7 个，漏洞主要分布在 Cisco Security Manager、Cisco IoT Field Network Director、Cisco AsyncOS for the Secure Web Appliance、Cisco DNA Spaces Connector、Cisco WebEx Meetings、WebEx Meetings Server、SD-WAN vManage Software 等产品中。攻击者可利用这些漏洞执行任意代码、信息泄露以及拒绝服务。

Mozilla 相关的漏洞有 7 个，漏洞主要分布在 Firefox 浏览器、Thunderbird 邮件客户端中。攻击者可利用这些漏洞执行任意代码或拒绝服务。

IBM 的相关的漏洞有 7 个，漏洞主要分布在 IBM DB2 数据库管理系统、AIX 操作系统、Resilient SOAR、Connect：Direct for UNIX、Loopback 框架中。攻击者可利用这些漏洞执行任意代码、造成信息泄露或拒绝服务。

2.3 12 月热点漏洞分析

（1） Oracle WebLogic Server 信息泄露漏洞

CVE-2020-14557

NSFOCUS ID：51681

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
漏洞点评

Oracle WebLogic Server 的 Sample apps 组件存在信息泄露漏洞。未经身份认证的攻击者可利用该漏洞通过 HTTP 网络访问破坏 Oracle WebLogic Server，对 Oracle WebLogic Server 的关键数据或所有可访问数据进行未经授权访问、创建、删除和修改。

（2） TP-Link Archer A7 AC1750 任意代码执行漏洞
CVE-2020-28347
NSFOCUS ID：51482
受影响版本
TP-LINK Archer A7 AC1750 < 201029
漏洞点评

TP-Link Archer A7 AC1750 是中国普联（TP-Link）公司的一款无线路由器。TP-Link Archer A7 AC1750 201029 之前版本存在任意代码执行漏洞。远程攻击者可通过 slave_mac 参数利用该漏洞执行任意代码。

（3） Apache Struts 远程代码执行漏洞 S2-061
CVE-2020-17530
NSFOCUS ID：无
受影响版本：
Apache Struts 2.0.0 - 2.5.25
不受影响版本：
Apache Struts >= 2.5.26
漏洞点评

2020 年 12 月 8 日，Struts 官方发布安全通告，披露了一个远程代码执行漏洞 S2-061。该漏洞与 S2-059 类似，问题源于当开发人员使用

了 %{…} 语法进行强制 OGNL 解析时，某些特殊的 TAG 属性可能会被二次解析；攻击者可构造恶意的 OGNL 表达式触发漏洞，造成远程代码执行。

2.4 常见漏洞利用攻击趋势分析

12 月份监测的漏洞利用告警共 4348587 次，基于漏洞利用的攻击排名 TOP10 如表 2-1 所示。其中 apache http server "mod_log_config"模块空 cookie 拒绝服务漏洞的告警最多，共 666970 次。

表 2-1 12 月份漏洞利用告警 TOP10

漏洞信息	告警次数
apache http server "mod_log_config"模块空 cookie 拒绝服务漏洞	666970
windows ms17-010 系列漏洞扫描攻击	546276
openssl sslv2 弱加密通信方式易受 drown 攻击(cve-2016-0800)	276818
windows smb 远程代码执行漏洞(shadow brokers eternalblue)(ms17-010)	262986
gnu bash 环境变量远程命令执行漏洞(cve-2014-6271)	28371
struts2 远程命令执行漏洞(s2-045)(s2-046)(cve-2017-5638)	24049
netgear dgn1000b setup.cgi 远程命令注入漏洞	23999
busybox wget 缓冲区溢出(cve-2018-1000517)	23741
gpon home gateway 远程命令执行漏洞(cve-2018-10561,cve-2018-10562)	22192
poptop pptp read()参数负值远程缓冲区溢出攻击	19500

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 1793503 条。

表 2-2 12 月份漏洞利用攻击类型

攻击类型	告警数量
畸形攻击	1793503
CGI 攻击	761922
其它攻击	674413
扫描探测	627174

溢出攻击	428548
木马攻击	31040
事件监控	20197
企业内部攻击	14041
暴力猜解	2089
蠕虫病毒	10

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 WWW 的漏洞利用告警最多，共 1602338 条。

表 2-3 12 月份漏洞利用服务类型 TOP10

服务类型	告警数量
WWW	1602338
CGI	1341144
SAMBA	858255
SSH	277144
MISC	170037
DNS	46171
FTP	14711
SNMP	12076
Radius	8014
IMAP	4079

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。

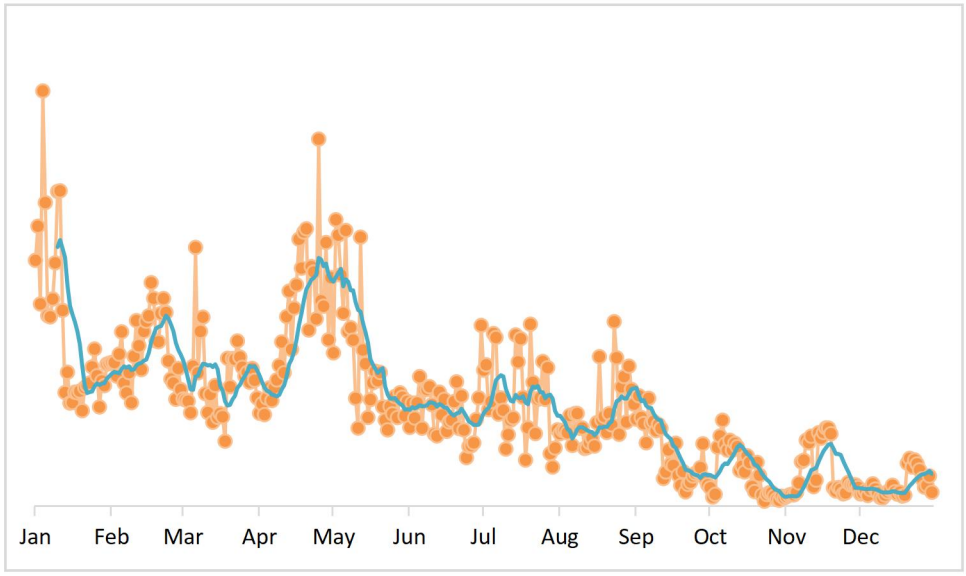

图 3-1 1 至 12 月份后门程序活动监测

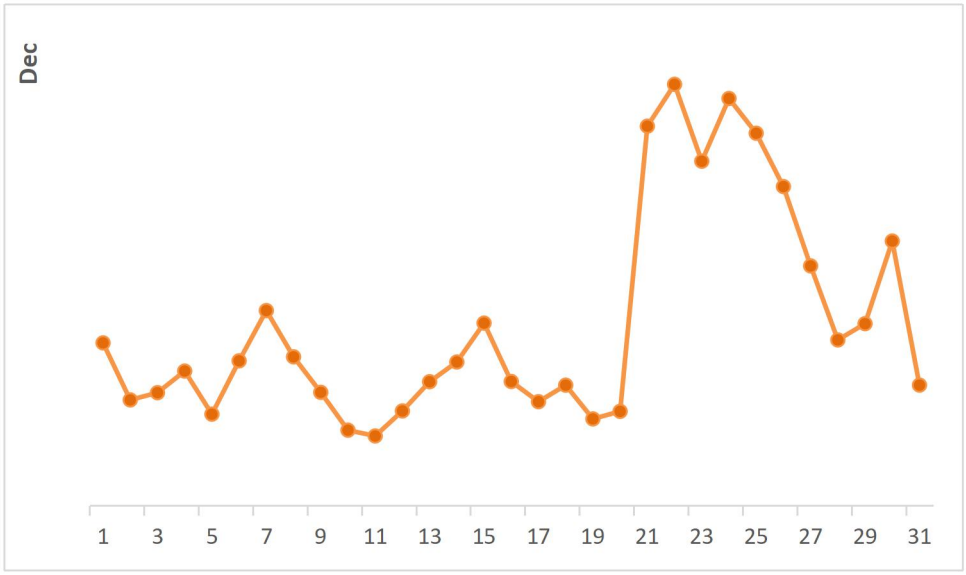

图 3-2 12 月份后门程序活动监测

从活跃趋势上来看，十二月份上半月活跃度较低且相对平稳，下半月活跃度波动较大，但整体活跃度不高。十二月份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。

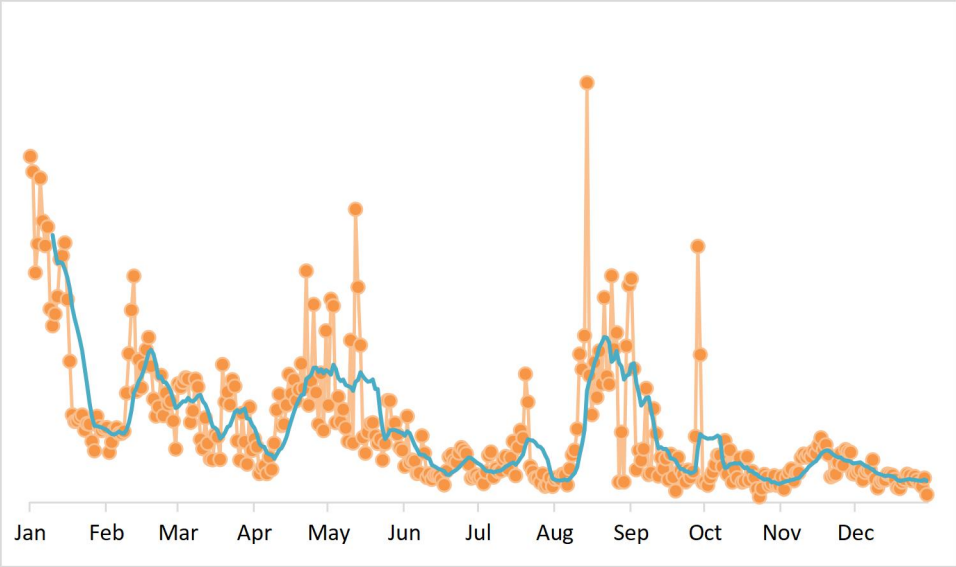

图 3-3 1 至 12 月份挖矿程序活动监测

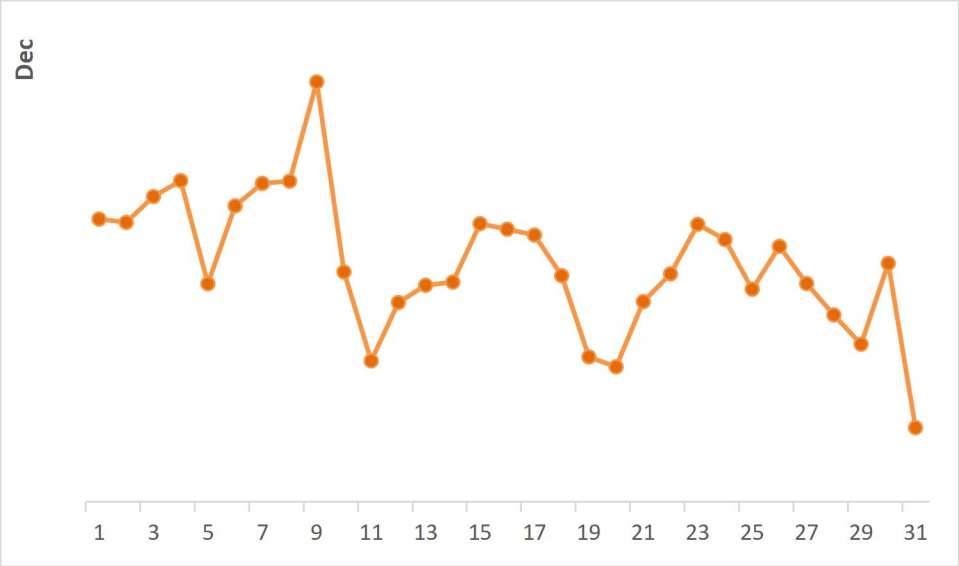

图 3-4 12 月份挖矿程序活动监测

十二月在全年的数据中表现的活跃度较低且相对平稳。十二月份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。

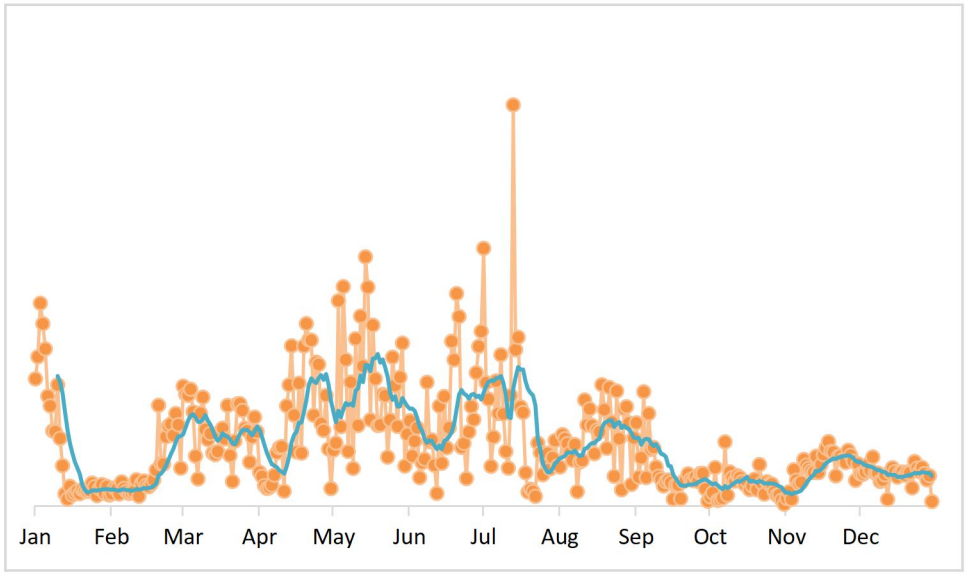

图 3-5 1 至 12 月份蠕虫活动监测

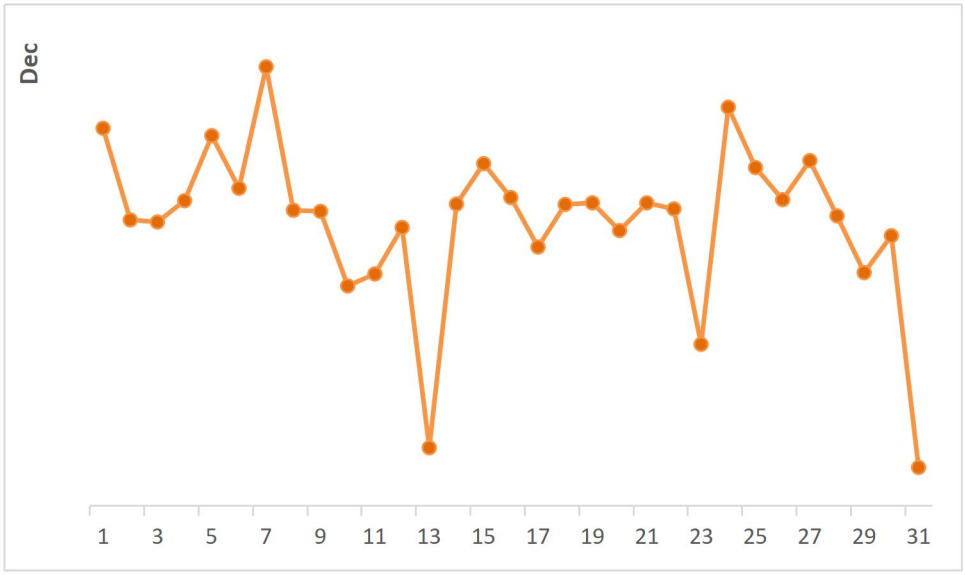

图 3-6 12 月份蠕虫活动监测

从全年数据来看，蠕虫程序活波动不大，整体区域平稳。十二月份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。

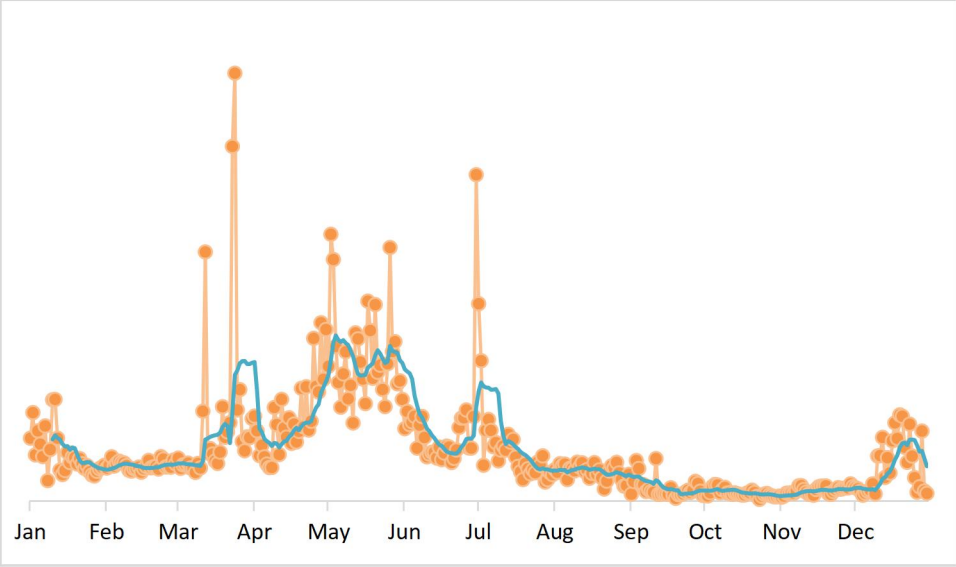

图 3-7 1 至 12 月份木马活动监测

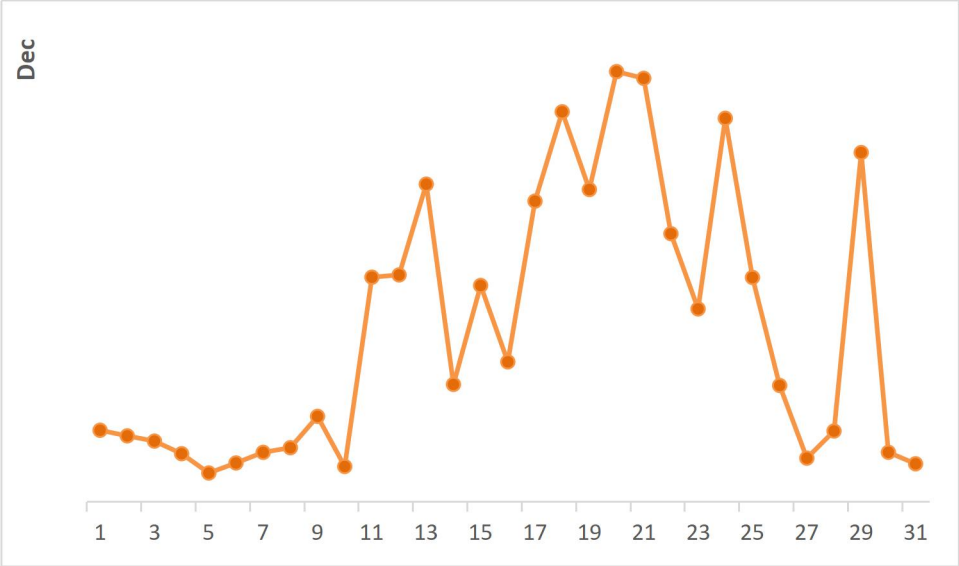

图 3-8 12 月份木马活动监测

从全年数据来看，木马程序活跃度从七月份开始逐渐下降，至十二月起有一个小范围的升温，十二月份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

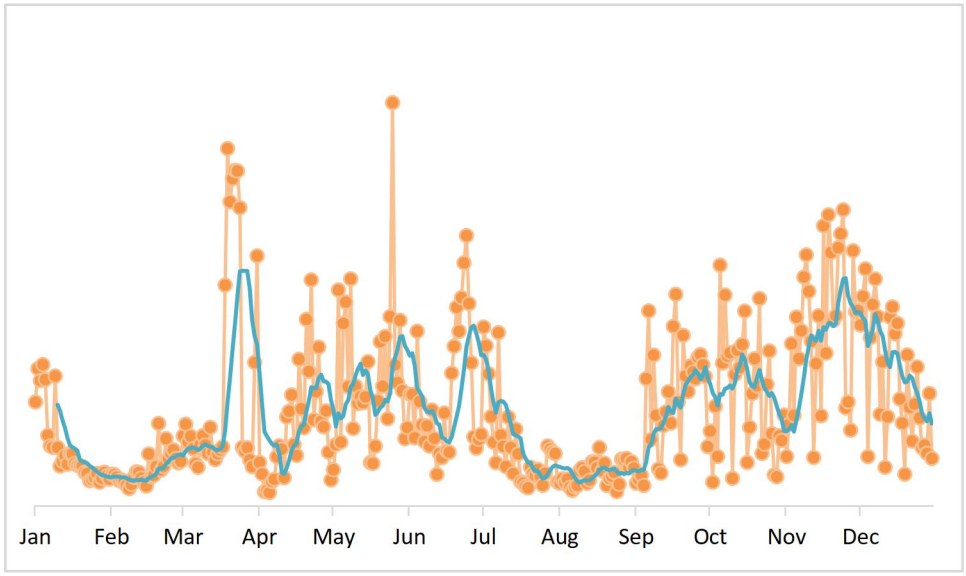

图 3-9 1 至 12 月份勒索软件活动监测

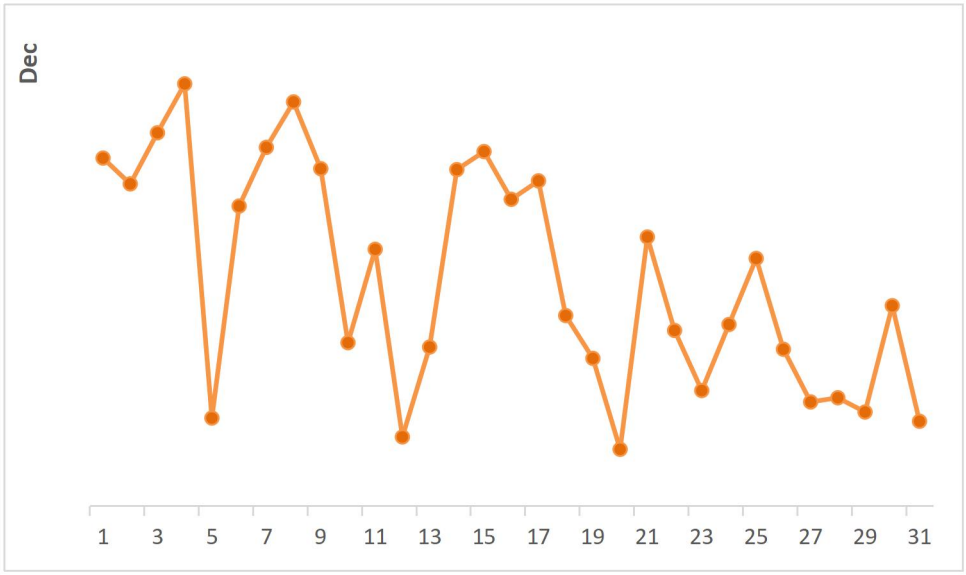

图 3-10 12 月份勒索软件活动监测

从全年的数据来看，十二月份勒索软件活动呈下降趋势，整个十二月份一直在波动，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 12 月重点物联网安全事件分析

（1）Citrix 证实 NetScaler 的 ADC 正在受到 DDoS 攻击

Citrix 于 2020 年 12 月 24 日证实，一种使用 DTLS 作为放大向量的持续 DDoS 攻击模式 正在影响启用了 EDT 的 CitrixApplicationDeliveryController （ADC）网络设备。数据报传输层安全性（ DTLS ）是一种通信协议，基于传输层安全性（ TLS ）协议，用于保护使用数据报传输的时延敏感的应用程序和服务。 该次攻击中，攻击者或僵尸程序可能会使 CitrixADCDTLS 网络吞吐量不堪重负，有可能导致出站带宽耗尽。

（2）研究人员把 RAM 变成 WiFi 卡，从未联网的系统中窃取数据

以色列一所大学的学者 2020 年 12 月 15 日发表了一项新的研究，详细介绍了一项技术，该技术可以将 RAM 卡转换成临时的 WIFI 发射器，并在没有 WiFi 的未联网的计算机内传输敏感数据。 该技术名为 AIR-FI，是以色列内盖夫本古里安大学研发部负责人 MordechaiGuri 发现的。 在过去的五年里，Guri 领导了数十个研究项目，通过非常规的方法从未联网的系统中窃取数据。

（3）尽管修复了漏洞，但 Android 应用程序仍暴露了 1 亿用户的信息

GOSMSPro 是一个 Android 即时消息应用程序，安装量超过 1 亿，尽管开发人员已经为修复数据泄漏背后的漏洞进行了将近两个星期的努力，但它仍在公开数百万用户的私人共享消息。该漏洞由 Trustwave 的研究人员三个月前发现并于 11 月 19 日公开披露，该漏洞使未经身份验证的攻击者可以不受限制地访问 GOSMSPro 用户私下共享的语音消息，视频和照片。

4.2 12 月新增物联网漏洞情况

2020 年 12 月，漏洞利用平台 Exploit-DB 新增 12 个物联网漏洞利用，其中两个远程命令执行漏洞。

表 4-1 2020 年 12 月新增物联网漏洞情况

EDB-ID	厂商	脆弱性类型	影响设备
49126	Intelbras	Authentication Bypass	Router RF 301K 1.1.2
49124	atx	Credential Disclosure	MiniCMTS200a Broadband Gateway 2.0
49110	Ruckus Networks	Remote Code Execution	BRAVIA Digital Signage 1.7.8
49187	Sony	System API Information Disclosure s	BRAVIA Digital Signage 1.7.8
49186	Sony	Unauthenticated Remote File Inclusion	iDS6 DSSPro Digital Signage System 6.2
48614	Eaton	Directory Traversal	Intelligent Power Manager 1.6
49266	ZEZNGGE	Authentication Bypass	Magic Home Pro 1.5.1
49262	Cisco Systems, Inc.	Path Traversal	ASA 9.14.1.10 and FTD 6.6.0.1
49256	Macally	Guest to Root Privilege Escalation	WIFISD2-2A82 2.000.010
49309	Sony	Code Execution	Playstation 4 < 7.02
49308	Sony	Code Execution	Playstation 4 < 7.02

49097	linksys	RCE	RE6500 1.0.11.001

物联网漏洞利用情况

本月绿盟威胁捕获系统捕获到来自 66219 个 IP 的 2494202 次访问请求日志。其中 69.1%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趋于平稳。

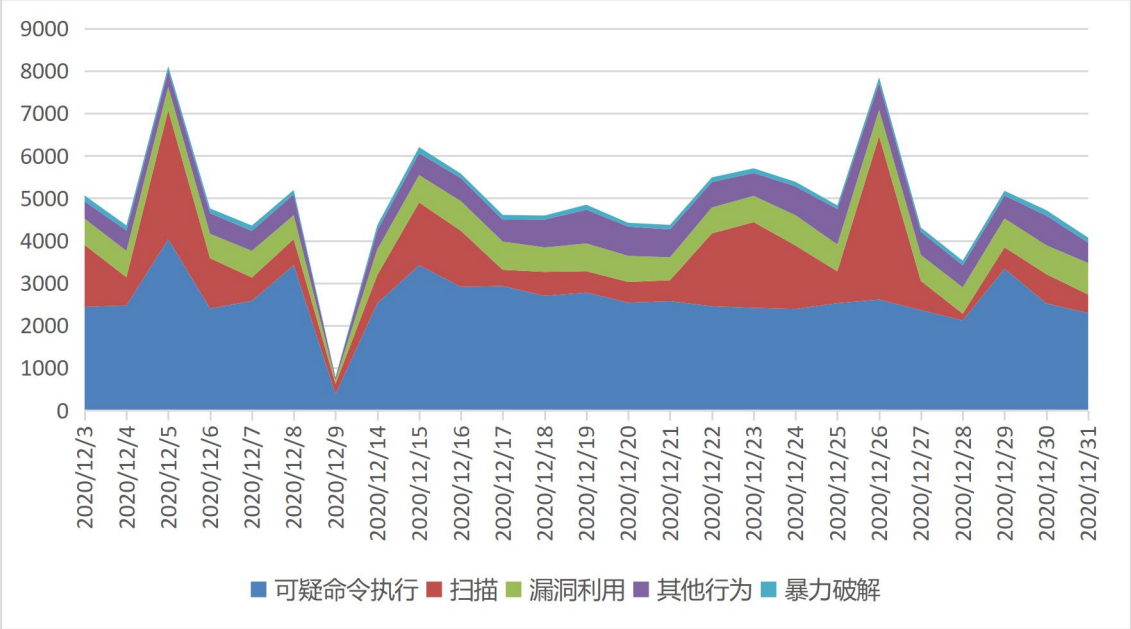

图 4-2 攻击源 IP 总量趋势

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 4-2 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 (Metasploit)	edb-41471	208302
AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities	edb-40500	128847
D-Link Devices - HNAP SOAPAction-Header Command Execution (Metasploit)	cve-2015-2051	32590

Eir D1000 Wireless Router - WAN Side Remote Command Injection (CVE-2016-10372)	cve-2016-10372	16521
Wireless IP Camera (P2P) WIFICAM - Remote Code Execution	cve-2017-8225	10573
CVE-2017-17215 - Huawei Router HG532 - Arbitrary Command Execution	cve-2017-17215	4756
Realtek SDK - Miniigd UPnP SOAP Command Execution (Metasploit) CVE-2014-8361	cve-2014-8361	2873
ThinkPHP 5.X - Remote Command Execution	edb-46150	1847
Multiple Vendors - Remote Configuration Disclosure	edb-48107	934
TVT NVMS 1000 - Directory Traversal	edb-48311	699

4.3 物联网威胁攻击源与攻击事件分析

对本月蜜罐日志中的 66219 个源 IP 进行分析，其中 45757 个 IP 发起过漏洞利用等恶意行为，环比上月减少 5.14%。从关联到恶意行为的 IP 分布在了 174 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 32.14%。

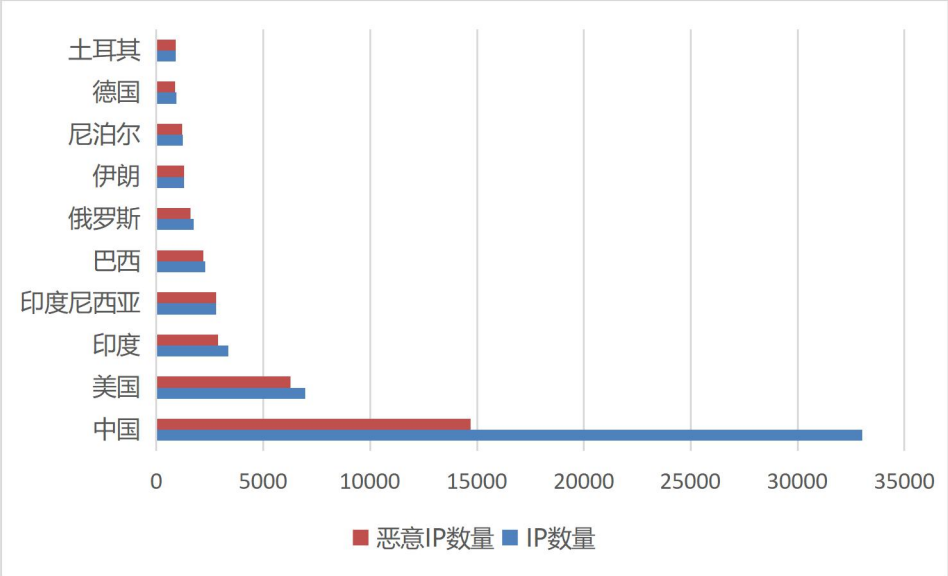

图 4-3 蜜罐的日志源 IP 的国家分布情况

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天每活跃 IP 为单位进行呈现。

12 月内总体趋势上，针对物联网设备的扫描与探测行为呈平稳趋势。

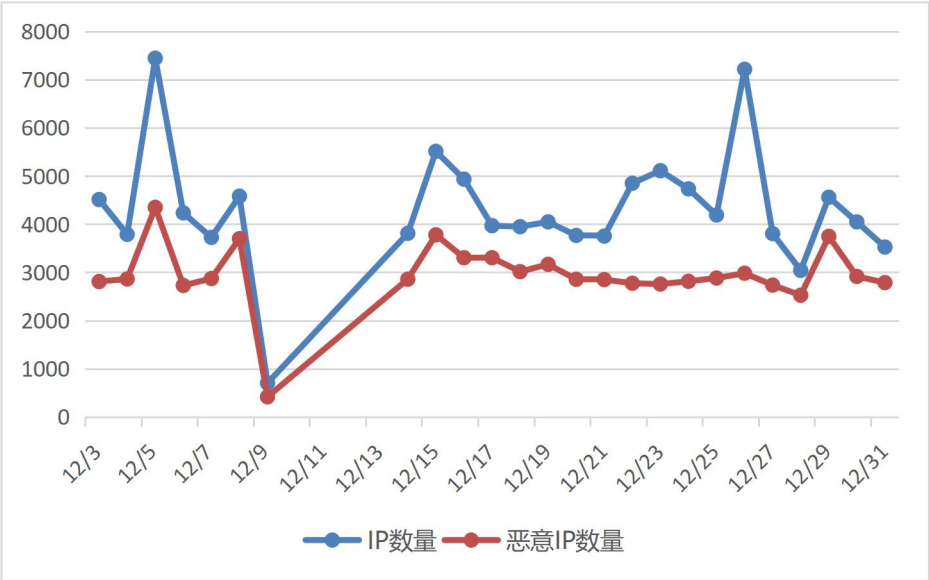

图 4-4 每日访问蜜罐的所有 IP、发送攻击请求 IP 的数量趋势

5. DDoS 攻击态势

5.1 DDoS 攻击流量与攻击次数

2020 年 12 月份，我们监控到国内 DDoS 攻击次数 1.33 万次，攻击总流量 2.963 万 TB（数据来源：中国电信云堤）。我们监控到全球 DDoS 攻击次数为 34 万次（sip 为粒度），攻击总流量 25TB（数据来源：绿盟科技全球 DDoS 态势感知系统），详见下图。

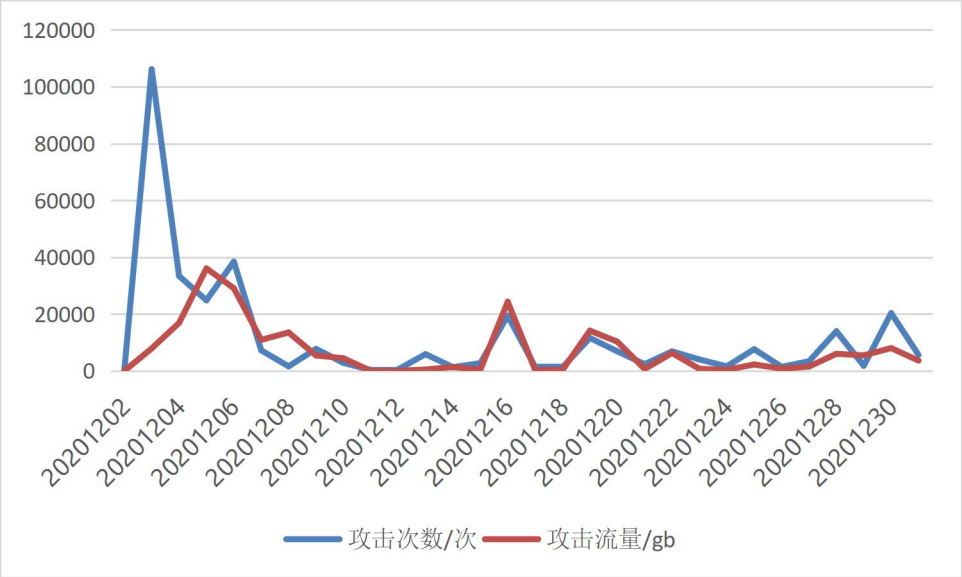

图 5-1 攻击流量与攻击次数

5.2 DDoS 攻击时间刻画

攻击持续时间占比

2020 年 12 月，攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 84%。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。

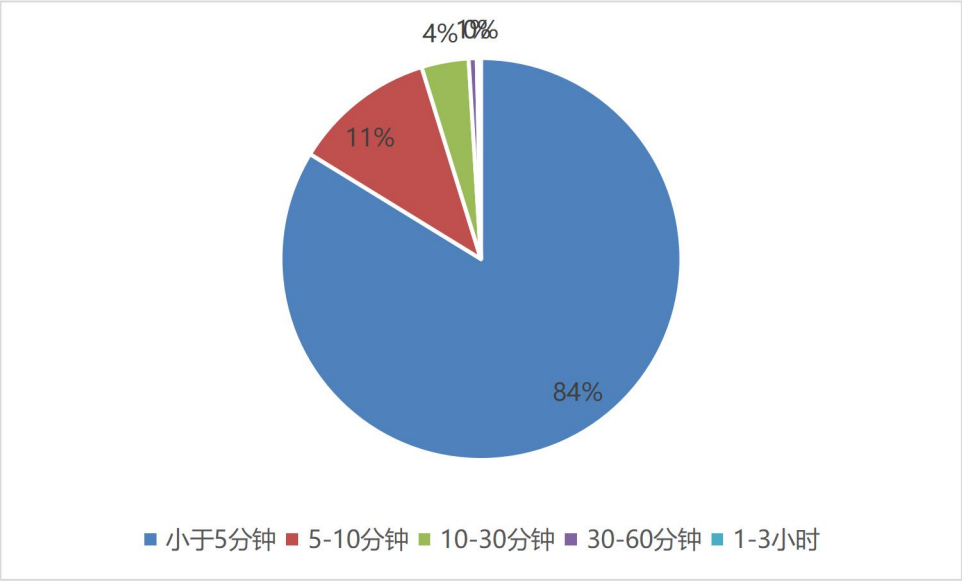

图 5-2 攻击持续时间占比

一天中 DDoS 攻击活动分布

从一天 24 小时攻击占比来看，凌晨 5 点为攻击高峰攻击。

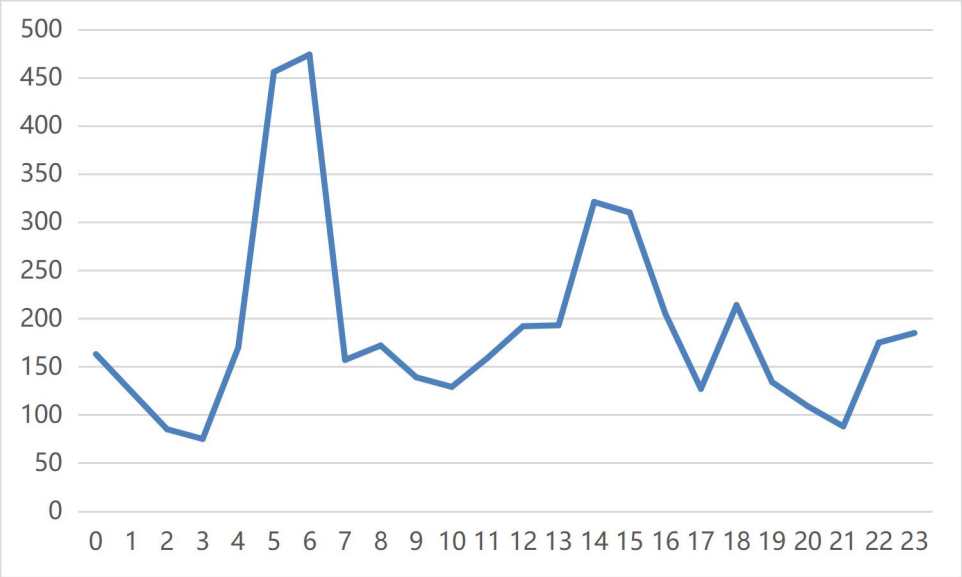

图 5-3 一天中 DDoS 攻击活动分布

一周中 DDoS 攻击活动分布

从每周中 DDoS 攻击活动的分布来看，周四最常被攻击。

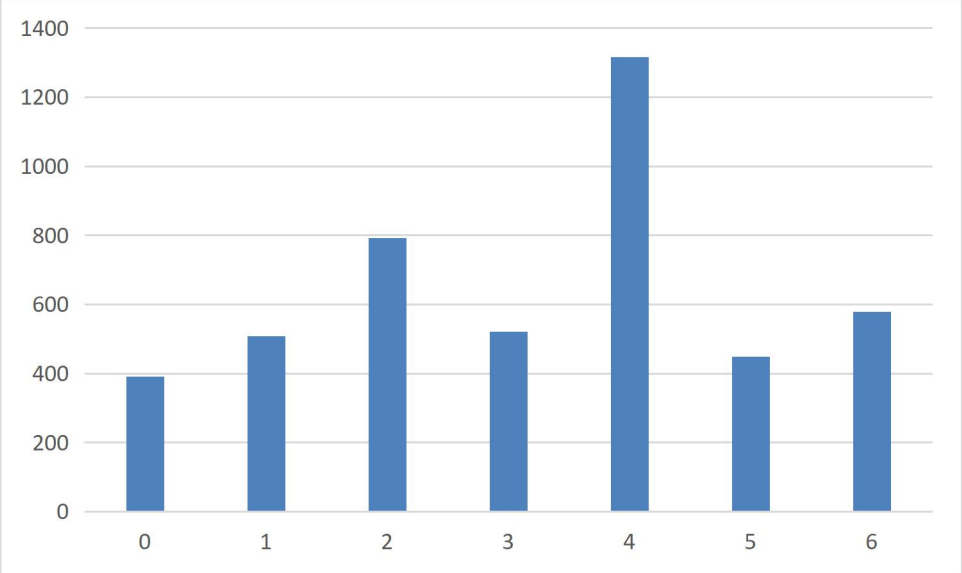

图 5-4 一周中 DDoS 攻击活动分布

5.3 DDoS 攻击类型分析

2020 年 12 月份主要的攻击类型是 SYN Flood 类型，占总攻击次数的 67%。从流量占比来看，UDP Flood 发起的攻击流量占比最高，占比 27%。

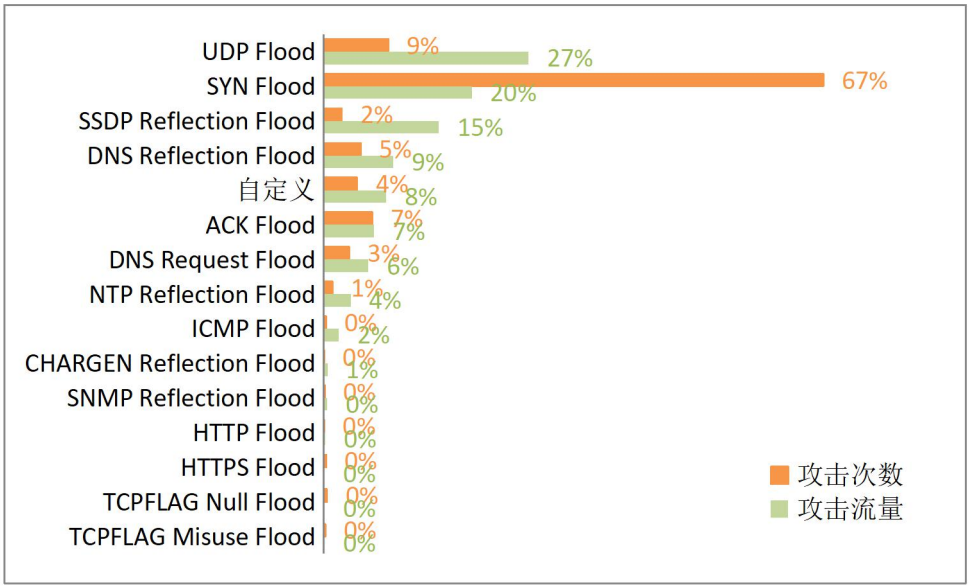

图 5-5 攻击类型分布

5.4 DDoS 团伙分析

团伙攻击是指通过相对独占的攻击资源，基于一定的攻击手法进行规模化攻击的行为。与其他大量由个体发起的普通攻击事件不同，团伙攻击行为往往带有典型的情报、经济等利益目标。因此形成基于网络数据的攻击团伙行为视角，掌握数据中的主要虚拟攻击团伙具有重要意义。根据 2020 年 12 月的 DDoS 攻击数据进行聚类分析，共发现 3 个活跃团伙。

表 5-1 12 月团伙概览

团伙编号团伙_DD	攻击源数量（核	攻击目标数量	攻击事件数量	活跃天数	最大bps	最大pps	攻击类型分布	攻击目标端口	攻击源端口	攻击源资产-传输层	攻击源资产-传输层	攻击源资产-开放服	攻击源资产-设备类

oS 场景	心实体）									端口	协议	务协议	型
cluster_DDoS@nta[oversea]_sipgang_20201201-20210101_1	353	98	240	16	99960000	9972	SSDP Reflection Flood（204，85.00%），NTP Reflection Flood（10，4.00%），SYN Flood（10，4.00%）		1900（23，10.00%）	1900（302，86.00%），554（70，20.00%），8000（39，11.00%）	UDP（313，89.00%），TCP（192，54.00%），SSL（11，3.00%）	UPNP（302，86.00%），HTTP（118，33.00%），RTSP（34，10.00%）	Camera（50，14.00%），Router(42，12.00%）
cluster_DDoS@nta[oversea]_sipgang_20201201-20210101_6	64	96	272	17	99720430	9999	NTP Reflection Flood（268，99.00%）	60067（15，6.00%），3890（15，6.00%），19295（14，5.00%）	123（117，43.00%）	123（60，94.00%），111（38，59.00%），22（34，53.00%）	UDP（61，95.00%），TCP（46，72.00%）	NTP（60，94.00%），PORTMAP（38，59.00%），SSH（34，53.00%）	

cluster_DDoS@nta[oversea]_sipgang_20201201-20210101_7	28	65	245	16	99525333	9999	NTP Reflection Flood（242，99.00%）	60067（17，7.00%），7143（17，7.00%），19295（17，7.00%）	123（111，45.00%）	123（28，100.00%），111（23，82.00%），53（23，82.00%）	UDP（28，100.00%），TCP（24，86.00%），SSL（11，39.00%）	NTP（28，100.00%），PORTMAP（23，82.00%），DNS（23，82.00%）	

规模最大团伙画像如下表，

表 5-2 规模最大团伙画像

团伙编号	**cluster_DDoS@nta[oversea]_sipgang_20201201-20210101_1**
攻击源数量（核心实体）	353
攻击目标数量	98
攻击事件数量	240
活跃天数	16
最大 **bps**	99960000
最大 **pps**	9972
攻击类型分布	SSDP Reflection Flood（204，85.00%），NTP Reflection Flood（10，4.00%），SYN Flood（10，4.00%）
攻击目标端口	
攻击源端口	1900（23，10.00%）
攻击源资产-传输层端口	1900（302，86.00%），554（70，20.00%），8000（39，11.00%）
攻击源资产-传输层协议	UDP（313，89.00%），TCP（192，54.00%），SSL（11，3.00%）
攻击源资产-开放服务协议	UPNP（302，86.00%），HTTP（118，33.00%），RTSP（34，10.00%）

攻击源资产-设备类型	Camera（50，14.00%），Router（42，12.00%）
攻击源资产-厂商	OpenBSD（10，3.00%）
攻击源资产-产品	
攻击源-国家	中国（321，91.00%）
攻击源-省	广东（56，16.00%），安徽（51，14.00%），河北（31，9.00%）
攻击源-城市	未知（15，4.00%），宣城（13，4.00%），亳州（10，3.00%）
攻击源-IDC 标签	其他（340，96.00%），IDC（13，4.00%）
攻击源-基站信息	其他（353，100.00%）
攻击源-机构	其他（353，100.00%）
攻击源-运营商	移动（317，90.00%）
攻击目标-国家	美国（60，61.00%），中国（27，28.00%）
攻击目标-省	香港（27，28.00%），弗吉尼亚州（20，20.00%），美国（18，18.00%）
攻击目标-城市	未知（51，52.00%），博伊顿（20，20.00%）
攻击目标-IDC 标签	IDC（97，99.00%）
攻击目标-基站信息	其他（98，100.00%）
攻击目标-机构	microsoft.com（85，24.00%）
攻击目标-运营商	其他（98，28.00%）
按天统计-事件数量	20201210（43，18.00%），20201212（35，15.00%），20201206（29，12.00%）
按天统计-攻击源数量	20201202（294，10.00%），20201205（291，10.00%），20201201（279，9.00%）
按天统计-攻击目标数量	20201206（16，15.00%），20201210（16，15.00%），20201209（13，12.00%）
详情-攻击源 IP	183.203.136.91（230，2.00%），183.223.159.81（91，1.00%），183.239.2.179（83，1.00%）
详情-攻击目标	52.152.96.90（1138，9.00%），20.62.154.40（977，8.00%），

IP	40.76.158.208（899，7.00%）
详情-攻击事件	3911870691631579382（949，8.00%），9012454234177669224（899，7.00%），8520242217896959146（633，5.00%）

5.5 小节

我们监控到全球 DDoS 攻击次数为 34 万次，攻击总流量 25TB。攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 84%。从一天 24 小时攻击占比来看，凌晨 5 点为攻击高峰攻击。从每周中 DDoS 攻击活动的分布来看，周四最常被攻击。12 月份主要的攻击类型是 SYN Flood 类型，占总攻击次数的 67%。从流量占比来看，UDP Flood 发起的攻击流量占比最高，占比 27%。根据 2020 年 12 月的 DDoS 攻击数据进行聚类分析，共发现 3 个活跃团伙。

6. 僵尸网络态势

6.1 DDoS 僵尸网络 12 月攻击概览

在 2020 年 12 月份的 DDoS 僵尸网络活动中，监控到的攻击指令较 11 月有大幅度回升。XorDDoS 制造了最多的攻击事件，Dofloo 产生了最多的攻击指令。

12 月检测到的 DDoS 攻击手段主要为 CC、SYN flood 和 UDP flood。

12 月检测到的被用于托管僵尸网络控制端的已知云服务商/运营商中，位列前三的分别是 ColorCrossing、Maxko 和 Develapp。

12 月检测到的 IoT DDoS 木马传播利用的各类漏洞种类为 55 种，其中 CVE-2017-17215（华为 HG532 路由器）、CVE-2014-8361（Realtek SDK miniigd SOAP 服务远程代码执行）和 CVE-2018-10561（GPON 光纤路由器漏洞）位居前三。

6.1.1 DDoS 攻击事件及家族分布

2020 年 12 月份检测到 DDoS 攻击指令为 148354 条，比 11 月增加近 3 倍，其中包含攻击事件数 14944，较 11 月有明显回升，共来自 7 个家族，其攻击比重如下：

表 6-1 僵尸网络攻击事件及家族分布

Family	Attack Events Count	Percent
XorDDoS	7002	46.85%
Mirai	4817	32.23%
Gafgyt	2263	15.14%
Nitol	845	5.65%
Dofloo	15	0.10%
Tsunami	1	0.01%
天罚 DDoS	1	0.01%

表 6-2 僵尸网络攻击指令及家族分布

Family	Attack Cmds Count	Percent
Dofloo	124183	83.71%
XorDDoS	9897	6.67%
Mirai	9086	6.12%
Gafgyt	3232	2.18%
Nitol	1877	1.27%
天罚 DDoS	78	0.05%
Tsunami	1	<0.01%

12 月检测到的攻击事件增长主要源于 XorDDoS 和 Mirai 家族指令数的增加。同时，由于 Dofloo 家族重新活跃，继续制造针对少数目标的高频攻击，使得 12 月份检测到的攻击指令数量大幅度提升，由上表可知 Dofloo 单个家族就产生了 80%以上的指令。Gafgyt 家族的事件数较 11 月有小幅度下降。其他家族攻击事件数相对较少。

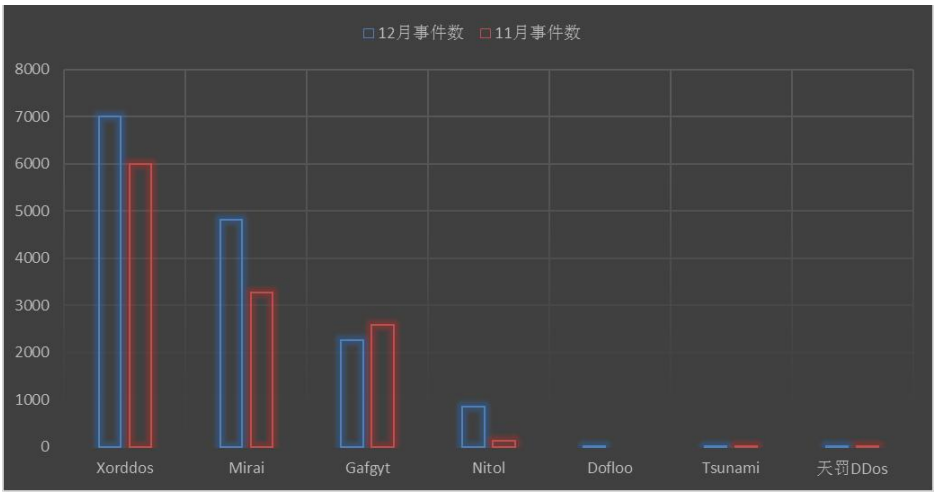

图 6-2 攻击事件趋势

以 10 分钟为超时上限，各家族连续攻击单个目标最长的持续时间靠前排名如下：

表 6-3 攻击最大连续下发指令时长

Family	Max Duration of Continuously Issued DDoS Cmd
Dofloo	**88 小时**
XorDDoS	**3.7 小时**
Mirai	**1.4 小时**
天罚 DDoS	**31 分钟**

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 6-4 攻击事件及家族比例

Family	Variant	Attack Count	Percent
XorDDoS	xorDDoS	4056	27.14%
	DDOS.XORDDOS.S0P0R0.LV	2946	19.71%
Mirai	mirai (变种流量在此处统一)	4817	32.23%
Gafgyt	gafgyt_left	2261	15.13%
	gafgyt_builds	2	0.01%
Nitol	DDOS.NITOL.S1P0R3.WV	520	3.48%
	DDOS.NITOL.S0P0R0.WO	323	2.16%
	DDOS.NITOL.S0P3R7.WV	2	0.01%
Dofloo	DDOS.DOFLOO.S0P0R0.LO	15	0.10%
Tsunami	DDOS.TSUNAMI.S0P0R1.IV	1	0.01%

天罚 DDoS	DDOS.TF.S0P0R0.LO	1	0.01%

XorDDoS 的两个变种制造了最多的攻击事件。而 Dofloo 本月重新开始活动，但因目标较少而导致事件数少。Gafgyt 和 Nitol 活跃变种数均较 11 月均较少了一个。其余家族情况与 11 月基本一致。

6.1.3 DDoS 攻击事件 C&C 分布

表 6-5 地理分布

Country	Count	Percent
美国	56	38.89%
德国	14	9.72%
荷兰	14	9.72%
匈牙利	8	5.56%
中国	8	5.56%
英国	7	4.86%
摩尔多瓦	7	4.86%
俄罗斯	7	4.86%
法国	6	4.17%
罗马尼亚	6	4.17%
奥地利	3	2.08%
加拿大	3	2.08%
保加利亚	1	0.69%
韩国	1	0.69%
爱尔兰	1	0.69%
伊朗	1	0.69%
印度	1	0.69%

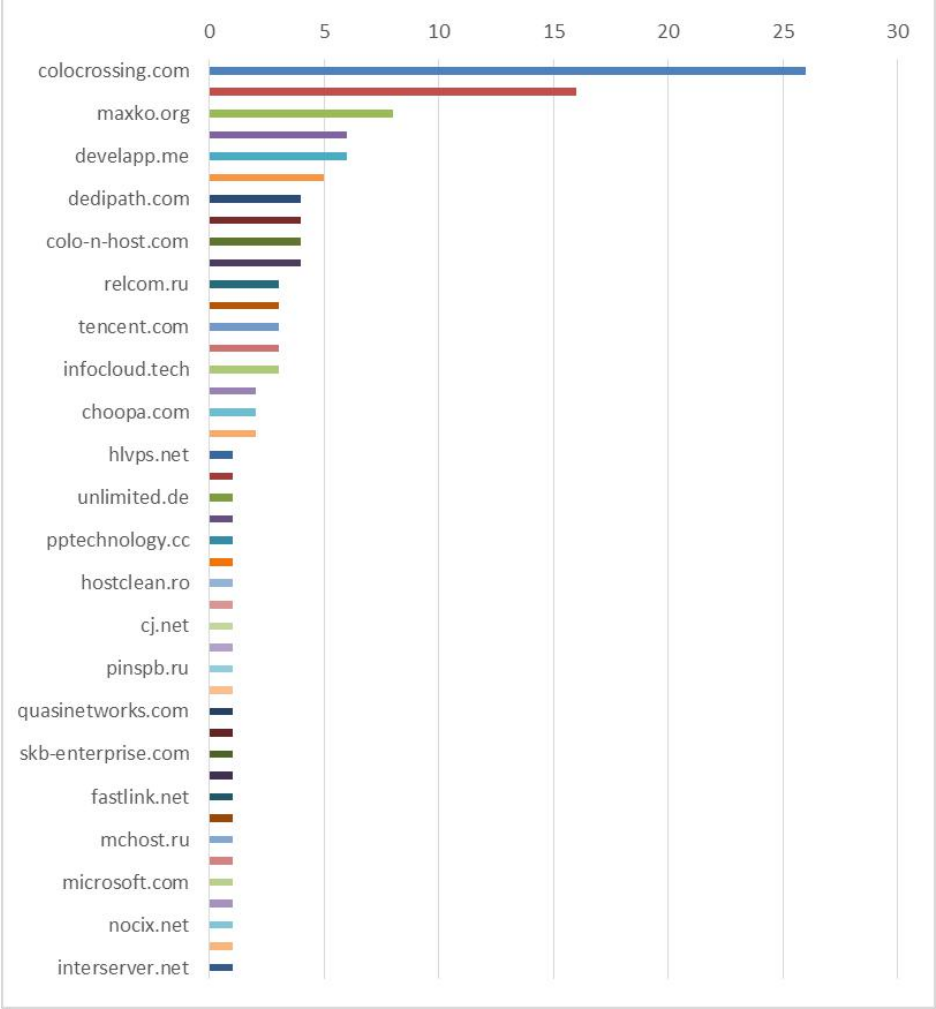

图 6-3 C&C 所属云服务及运营商分布

C&C 主要托管于云厂商，排名前三的分别是 ColorCrossing、Maxko 和 Develapp。此外有近 15 个分布在世界范围内的 C&C 暂无法判断出服务归属。

6.1.4 DDoS 攻击指令活跃度日级分布

Dofloo（红）呈现出超高活跃态势，并间歇性地出现局部活动峰值，且峰值不断升高，在月末达到最高点。其他家族的活跃度均不如 Dofloo。XorDDoS 的变种 xorDDoS（黄）在 4~6 日和 18~19 日分别出现峰值，其余时段较为相对沉寂，而另一变种 DDOS.XORDDOS.S0P0R0.LV（橘黄）呈现出类似的情况，仅在 1~3 日和 16~18 日期间较为活跃。Mirai（泥色）继续维持稳定的活跃度，虽然较低，但是覆盖了每一天。

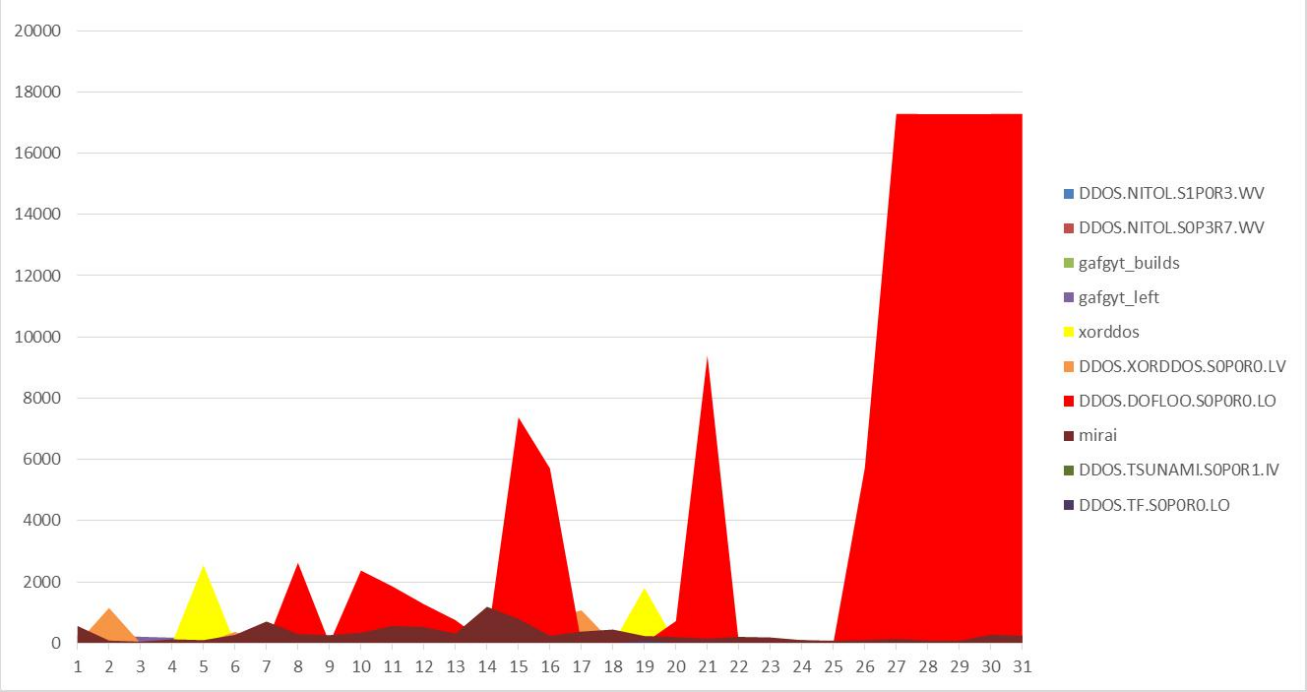

图 6-4 攻击指令活跃度日级分布

6.1.5 DDoS 攻击所使用 FLOOD 类型分布

表 6-6 攻击所使用 FLOOD 类型分布

Flood Type	Count (按次数统计)	Percent
CC	124183	83.57%
SYN flood	10638	7.16%
UDP flood	4423	2.98%
ACK flood	3193	2.15%
HTTP flood	2038	1.37%
混合类型	1701	1.14%
TCP flood	744	0.50%
DNS flood	725	0.49%
GRETH	575	0.39%
IP flood	336	0.23%
SMTP flood	40	0.03%

6.1.6 攻击使用 Linux/IoT 漏洞分布

表 6-7 攻击事件使用漏洞分布

Vulnerability	Count
CVE-2017-17215	876
CVE-2014-8361	384
Common_Shell_Command_Abuse	332
ZyXEL_P660HN_T_v1_ViewLog_asp_privilege_escalation	330
CVE-2018-10561	312
ThinkPHP_5_X_Remote_Command_Execution	309
JAWS_Webserver_unauthenticated_shell_command_execution	274
Eir_D1000_Wireless_Router_WAN_Side_Remote_Command_Injection	239
Netgear_DGN1000_1_1_00_48_Setup_cgi_Remote_Code_Execution	205
CVE-2015-2051	181
Vacron_NVR_RCE	145
CCTV-DVR Remote Code Execution	131
Linksys_E_series_Unauthenticated_Remote_Code_Execution	129
D_Link_OS_Command_Injection_via_UPnP_Interface	120
CVE-2016-6277	119
CVE_2017_17215_2	77
Netlink_GPON_Router_1_0_11_Remote_Code_Execution	39
CVE_2020_10173	27

D_Link_DSL_Devices_login_cgi_Remote_Command_Execution	23
Zeroshell_3_6_0_3_7_0_Net_Services_Remote_Code_Execution	18
Zyxel_P660HN_Remote_Command_Execution	15
CVE_2019_16920	8
CVE-2018-17173	8
CVE_2020_8218	8
unknown_exploit_ToolsCgi_moobot_20201103	8
CVE_2014_2321	6
wordpress_brute_force	4
CVE-2017-6884	3
NUUO_OS_Command_Injection_3	3
CVE-2014-9094	3
Symantec_Web_Gateway_5_0_2_8_Remote_Code_Execution	1

6.2 威胁捕获 12 月数据概览

蜜罐方面，2020 年 12 月份互联网攻击活动分为由恶意连接、DDoS 反射、暴力破解和漏洞利用构成。

恶意连接方面，针对 27015 和 111 端口的连接占比最多，其中前者达到 65%。

漏洞利用方面，针对 IP 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，占比高达 60%以上。

DDOS 反射攻击方面，upnp 占比继续增加，达到 55%。12 月共计捕获 DDoS 反射攻击事件超过 1005 万例，其中最长的持续时间高达 58 小时左右。

6.2.1 攻击总览

12 月份，公网威胁捕获系统共计捕获高低危攻击 257857967 次，恶意连接 65577500 次，占比 68.97%；漏洞利用 461027 次，占比 0.48%；暴力破解 18997931 次，占比 19.98%；DDoS 攻击 10050272 次，占比 10.57%；其中恶意连接占比最多。

后半部分我们将针对暴力破解，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。

12 月攻击类型占比情况如下：

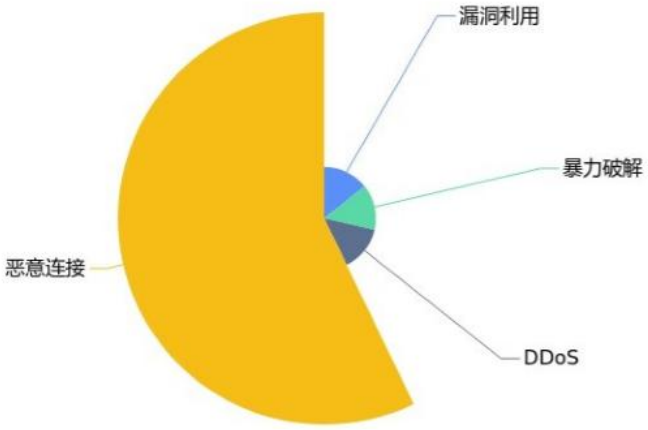

图 6-5 12 月攻击类型占比情况

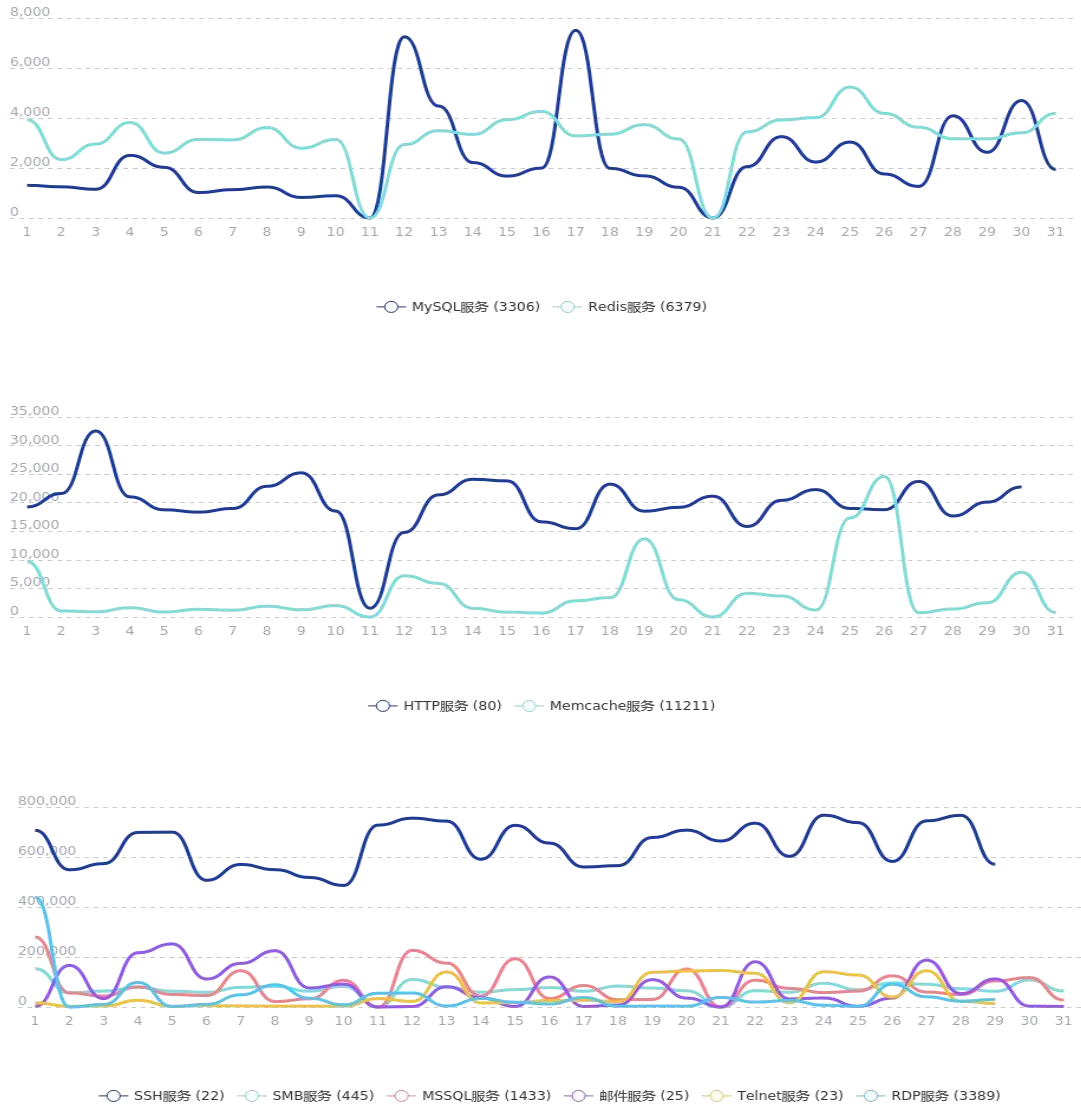

图 6-6 12 月高危端口攻击变化趋势

12 月漏洞利用排行榜如下：

表 6-8 12 月漏洞利用次数分布

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
EDBID40500	IpCameraNvrDvr	AvtechIpCameraNvrDvrDevice s	135496
Redis未授权访问漏洞	Redis	通用服务	101280
EDBID37171	Router	DLink	32456
EDBID40740	Router	EirD1000WirelessRouter	20298
EDBID43414	Router	HuaweiRouterHG532	5920
CVE201814847	Router	MikroTik	2869
CVE20148361	SDK	Realtek	2500
CVE20175638	struts2	通用服务	1367
CVE201710271	Weblogic	通用服务	1012

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。较 11 月相比，12 月出现较多针对 27015 端口的访问。该端口多见于游戏，可能涉及反射 DDoS 攻击。此外本月出现了部分针对 SUN 公司 RPC 端口 111 的访问，也是常见的渗透端口。

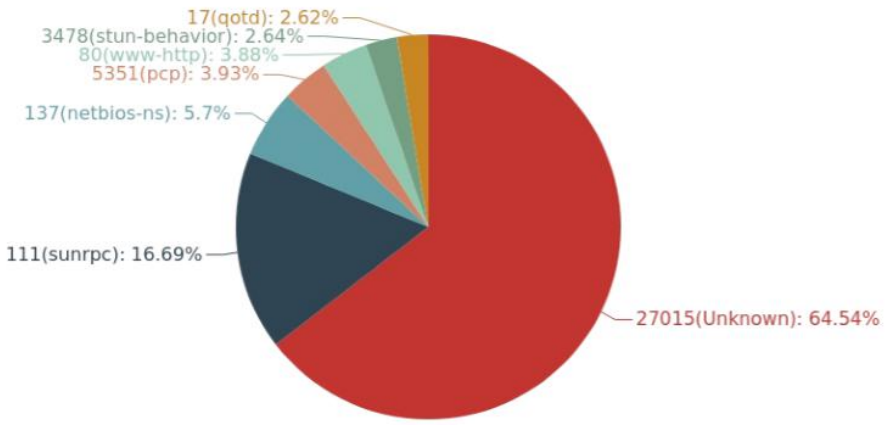

图 6-7 应用服务威胁趋势

6.2.2.2 暴力破解

上月共计捕获 162059334 次针对公网爆破攻击。其中用户名密码对共计捕获 168294 个。利用 TOP5 如下

表 6-9 用户名密码对利用次数

用户名	密码	利用次数
root	admin	8866828
root	1234	2922052
root	password	1549103
root	None	1140557
nproc	nproc	231437

表 6-10 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	8895550
1234	通用	过于简单	2959596
password	通用	一般	1623941
None	通用	过于简单	1155720
nproc	通用	过于简单	231437

登录尝试的前五个国家/地区为：

表 6-11 暴力破解排名前五国家

攻击国家	攻击次数
Netherlands	90967198
Panama	13050206
Moldova	13013791
Russian Federation	7089613
China	5514888

6.2.2.3 渗透行为

12 月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 6-12 常用命令

命令	入侵工具类型	使用次数
uname -a	外部命令	246975
cat /proc/cpuinfo | grep name | wc -l	外部命令	235673
cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}'	外部命令	235456
free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}'	外部命令	235405
which ls	外部命令	235345
ls -lh $(which ls)	外部命令	235345
crontab -l	外部命令	235285
uname -m	外部命令	235252
cat /proc/cpuinfo | grep model | grep name | wc -l	外部命令	235131
top	外部命令	235087
lscpu | grep Model	外部命令	234880
cd ~ && rm -rf .ssh && mkdir .ssh && echo "ssh-rsa AA AAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE 7VvAcwdli2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanU V9tJ2/9p7+vD0EpZ3Tz/+0kX34uAx1RV/75GVOmNx+9Eu WOnvNoaJe0QXxziIg9eLBHpgLMuakb5+BgTFB+rKJAw9 u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmPecjdySYMb6 6nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCG PK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujv cD9iUKQTTWYYjIIu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPK gAySVKPRK+oRw== mdrfckr">>.ssh/authorized_keys & & chmod -R go= ~/.ssh && cd ~	系统内置工具	232610
echo -e "\x6F\x6B"	系统内置工具	204499

表 6-13 攻击源 IP 前五 IP

攻击IP	攻击次数
5.188.86.165	7534912
5.188.86.168	6267874

5.188.86.207	5754539
5.188.86.178	5528585
5.188.86.206	5502871

攻击 IP 全球分布情况：

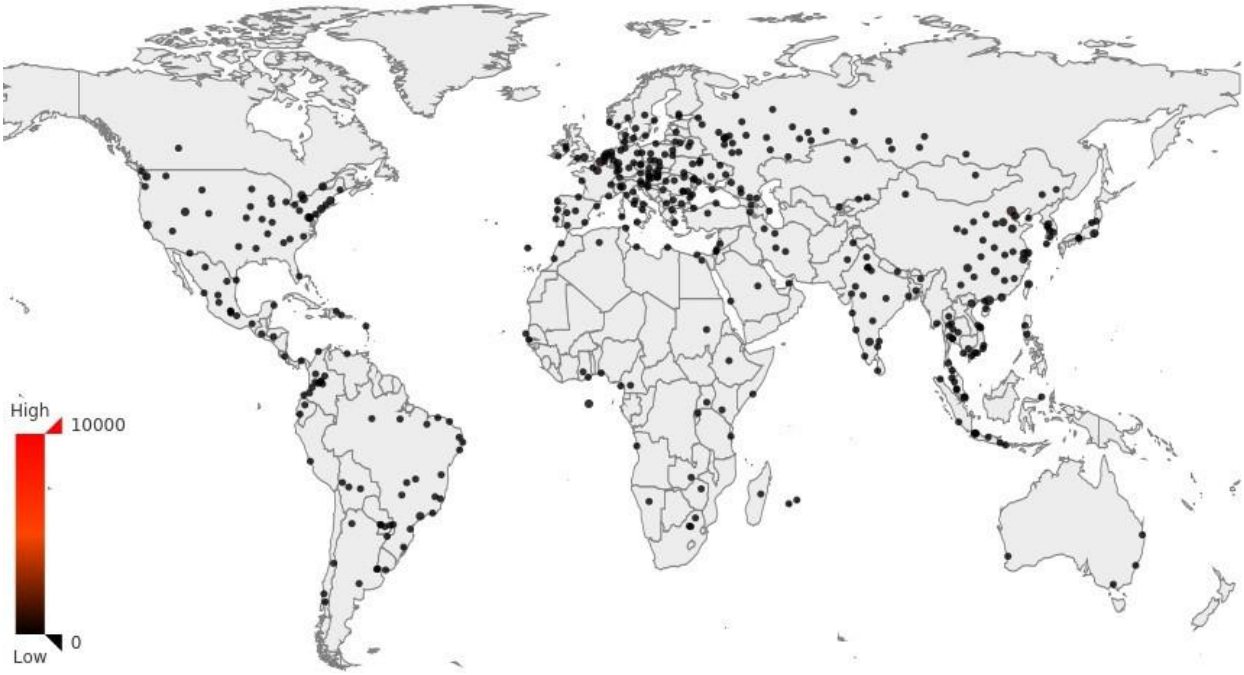

图 6-8 攻击 IP 全球分布

6.2.2.4 邮件攻击

12 月中我们在公网部署的邮件仿真服务捕获 2394893 封邮件，共计捕获 1222 个非重复来源攻击者 IP。涉及 284290 个受害目的邮箱。

表 6-14 攻击者针对目的邮箱

邮箱	使用次数
spameri@tiscali.it	291
1458070482@qq.com	63
check212014@gmail.com	59
anticarcel88@gmail.com	58
nedstark88@mail.com	58

表 6-15 攻击者针对邮件服务商

邮件服务商	使用次数
gmail.com	36720
yahoo.co.jp	31811
yahoo.com	18943
yahoo.com.tw	13552
hotmail.com	11996

6.2.2.5 应用程序漏洞利用

12 月共计在公网捕获 461027 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 42.90%。

最频繁的设备厂商为 MVPower，占比为 42.90%。

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。

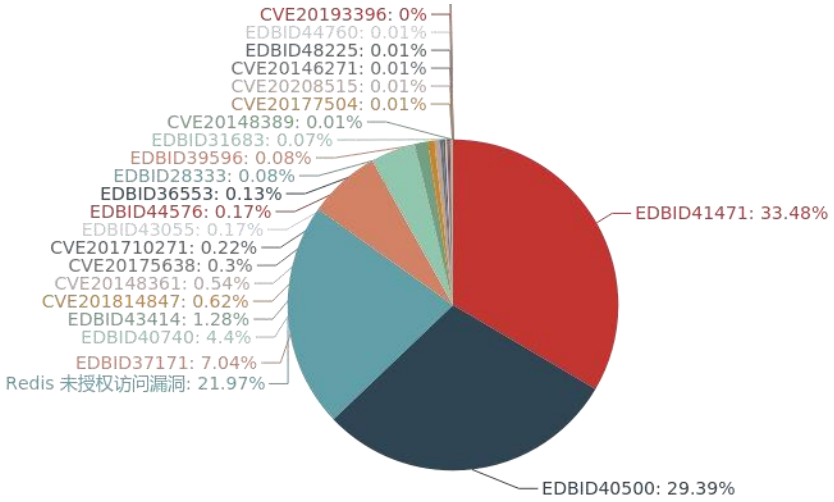

图 6-9 漏洞攻击及编号占比

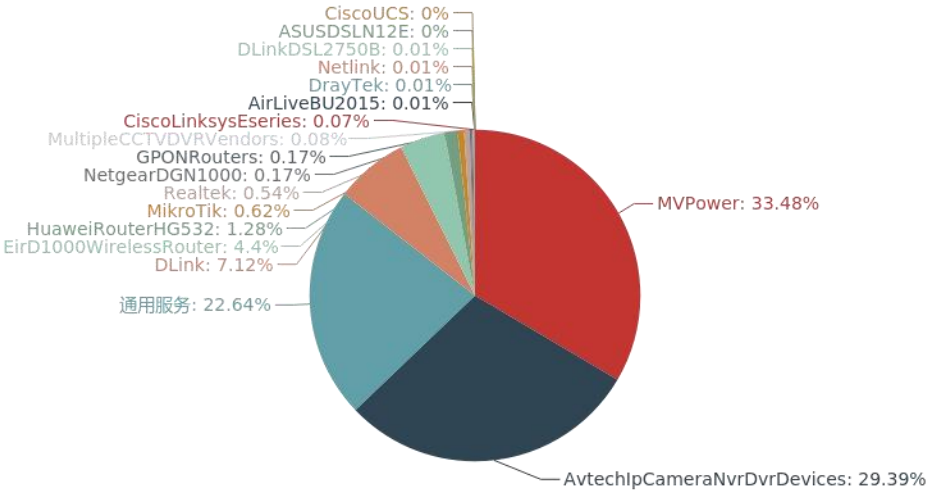

图 6-10 漏洞攻击针对厂商设备占比

数据库服务部分，捕获共计来源 IP 26943 个。Mysql 1954 个，MSsql 22071 个，redis 2918 个，非关系型数据库 2918 个。爆破利用用户名密码对 2842 个。来源客户端软件 5551 种。

表 6-16 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; 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;	199817
exec sp_dropextendedproc \'xp_cmdshell\';	98402
dbcc addextendedproc(\'xp_cmdshell\',\'xplog70.dll\')	98342
EXEC sp_configure \'show advanced options\', 1;RECONFIGURE;exec SP_CONFIGURE \'xp_cmdshell\', 1;RECONFIGURE;	98083
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\'	98014

表 6-17 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
ECS-T6-LARGE-2-	25814
YD-TJSJ	25453
BEYONDLIQUOR-PC	23869
CRM	15768
SERVER111	14094
WIN-CS57SS4GBC9	12966
EC2AMAZ-F03JIIO	12880
DT03565AC10	12735
iZs6ex5b44vc8dZ	12721

Web 服务部分，12 月共计捕获 15683257 次 WEB 攻击，涉及 92302 个攻击 IP， 6946 个来源 User Agent，26130 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 6-18 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	679255
Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/74.0. 3729.169 Safari/537.36	257163
Snickers-Avtech	118544
Python-urllib/2.7	94189
python-requests/2.6.0 CPython/2.7.5 Linux/3.10.01160.6.1.el7.x86_64	71969
Mozilla/5.0(Windows NT 6.1; WOW64;rv:66.0) Gecko/20100101 Firefox/66.0	67843
Mozilla/5.0 (compatible; CensysInspect/1.1; +https ://about.censys.io/)	48790
iLL-Avasatum	45266
python-requests/2.6.0 CPython/2.7.5 Linux/3.10.01062.1.1.el7.x86_64	36488
Update-Avtech	31327

表 6-19 攻击者最常使用的攻击路径

路径	访问次数
/	922348
/shell	297563
/ISAPI/Security/userCheck	114831
/snapshot.cgi	103159
/index.asp	68736
/cgi-bin/nobody/Search.cgi	68573
/nobody/ez.htm	67294
/cgi-bin/supervisor/CloudSetup.cgi	66924
/favicon.ico	66171
/login.html	50816

6.2.2.6 DDoS 反射攻击

12 月份捕获 10050272 次 DDoS 反射攻击事件，其中 upnp-57238 服务上月攻击利用最多。攻击次数最高的 DDoS 反射攻击事件受害 IP 为 183.131.206.48，持续时间达到 58.32 小时。与此同时，我们也捕获到了针对公网 1126699 个受害 IP 的 DDoS 反射攻击事件。

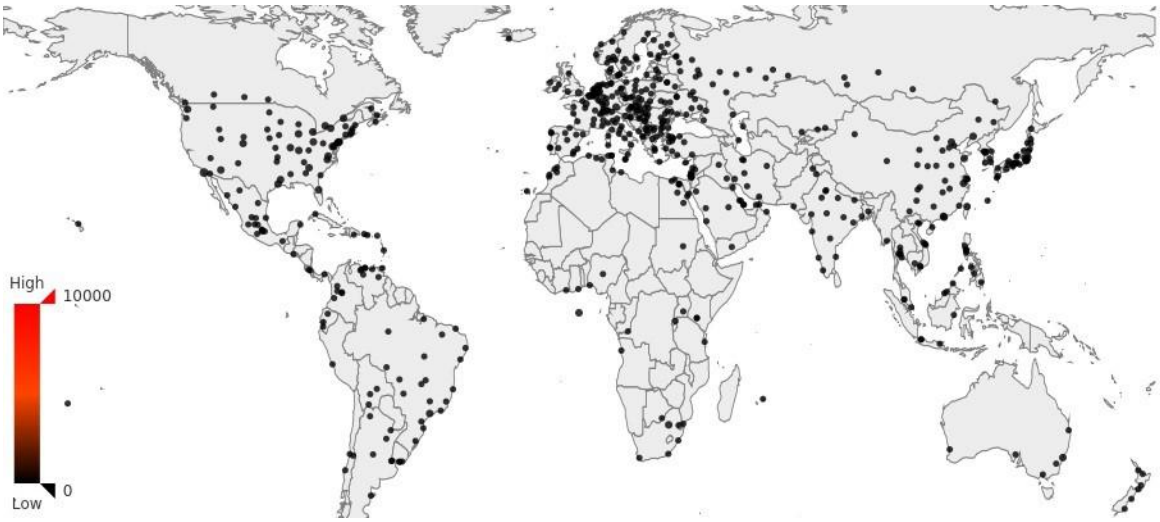

图 6-11 DDOS 反射攻击受害者分布

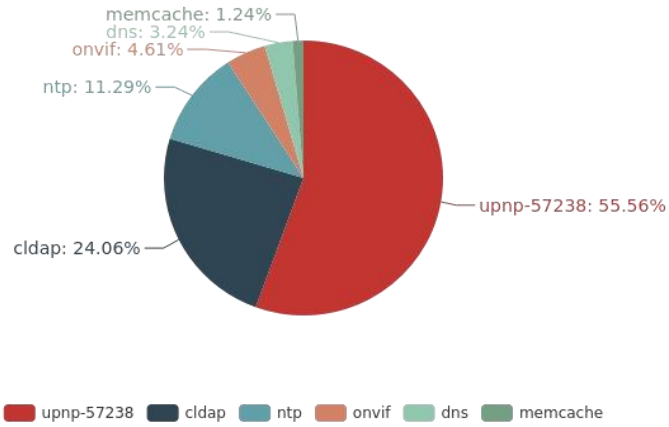

图 6-12 DDOS 反射攻击脆弱服务占比

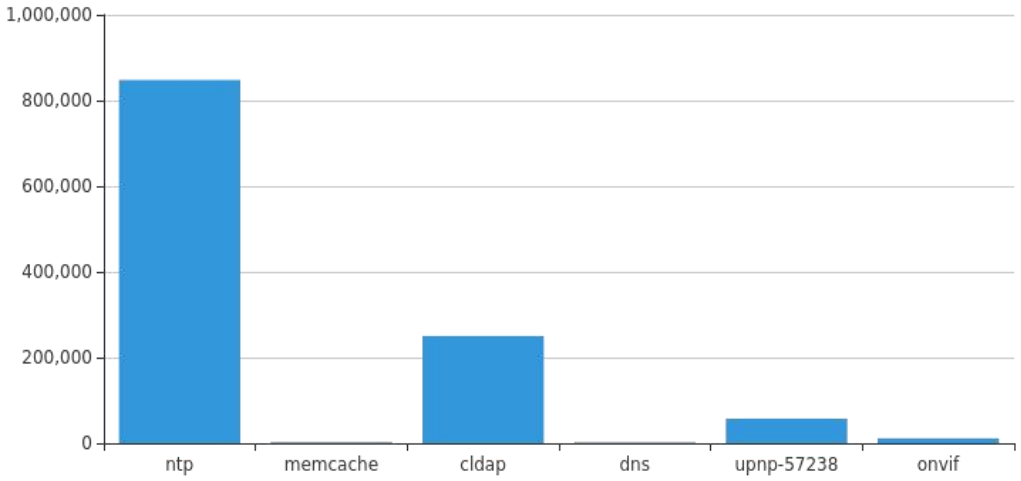

图 6-13 反射攻击对应反射源 IP 数目

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 12 月份的整体活跃情况较为平稳，活跃肉鸡总量增长至 18290 台，其中在中国的肉鸡最多，达到 8077 台，占比 44%。开放 22 端口的肉鸡数有 12953 台，占比接近所有肉鸡的 71%。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依然是 nproc-nproc。详细情况见下文。

6.2.3.1 活跃情况

通过对 12 月份每天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 6-13 所示，该挖矿僵尸网络在 12 月份的整体活跃情况较为平稳，在 12 月 28 日肉鸡数最高，达到 4374 台，12 月 25 日和 26 日数据存在问题，不作为参考。

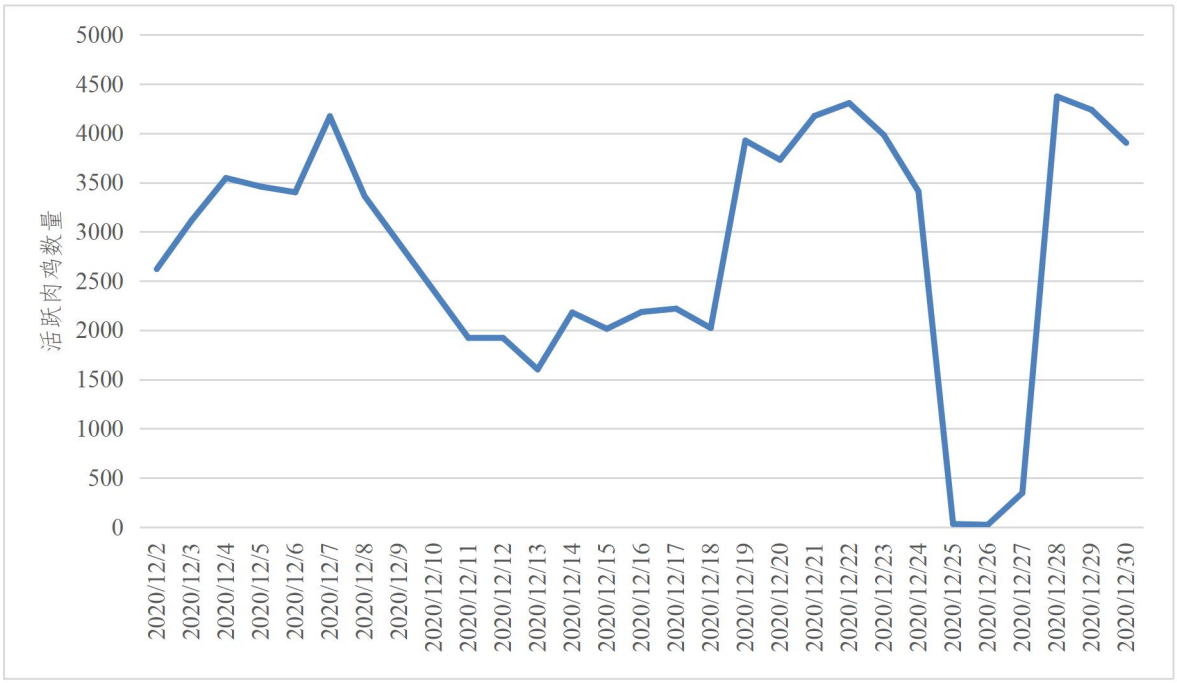

图 6-14 挖矿僵尸网络 12 月份活跃情况

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 6-14 所示，处于中国的肉鸡数最多，为 8077 台，占比 44%。

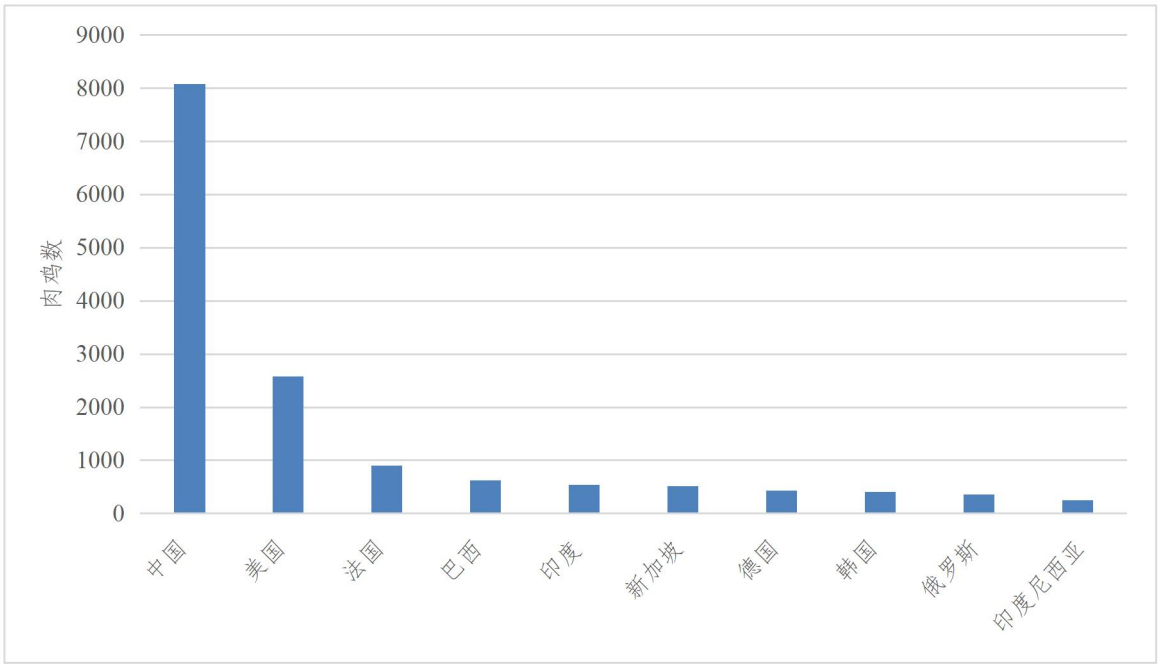

图 6-15 肉鸡国家数量 Top10

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 6-15 所示，这些肉鸡开放的端口前十名为：22、80、443、21、3306、3389、123、8080、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 71%。

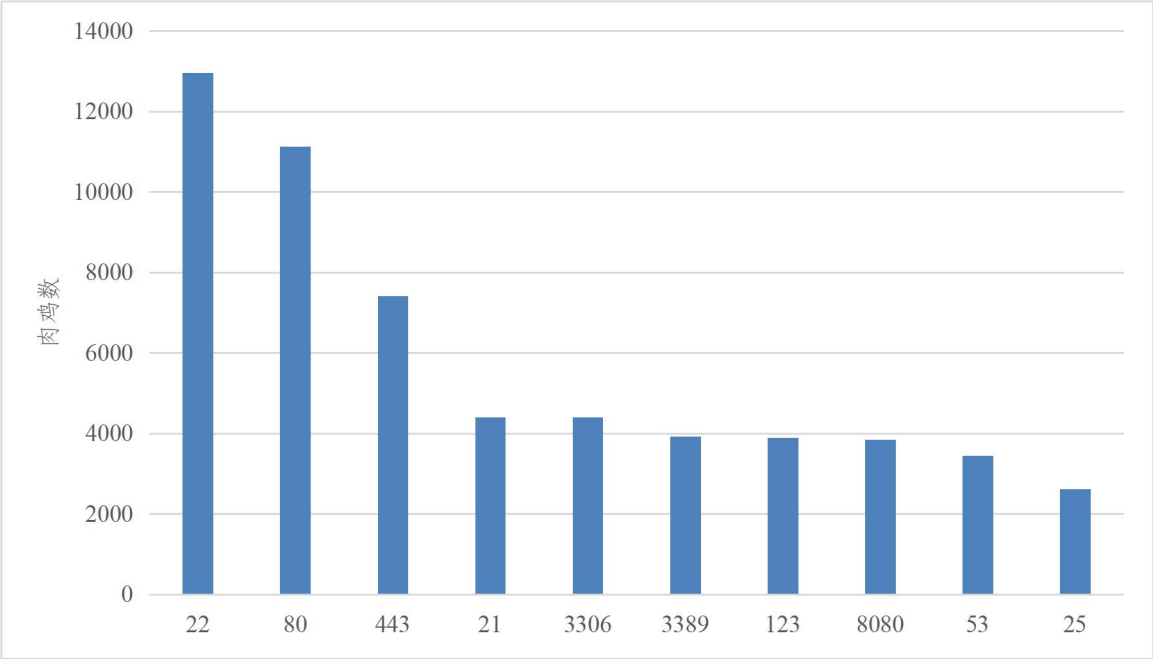

图 6-16 肉鸡开放端口数量 Top10

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 13%为物联网设备。如图 6-16 所示，这些物联网设备中 39%为摄像头，37%为路由器。

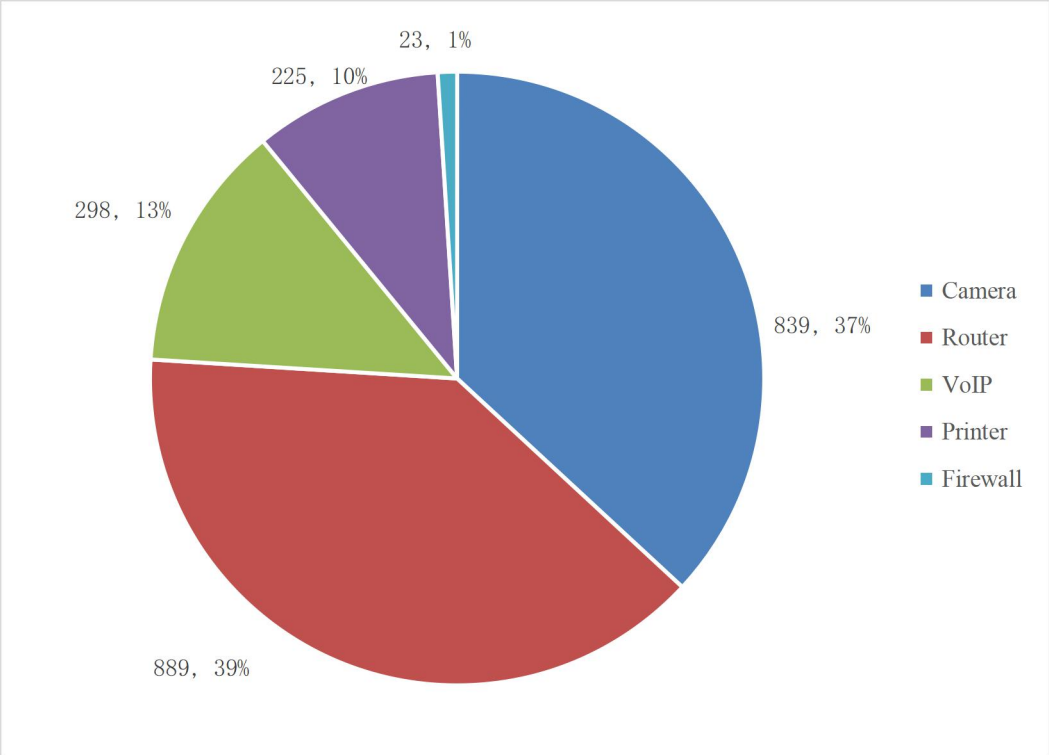

图 6-17 肉鸡设备类型分布

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 6-20 所示，该挖矿僵尸网络最常用的弱口令依然是 nproc-nproc。

表 6-20 暴力破解字典及使用次数

排名	账号-密码	使用次数
1	nproc-nproc	186452
2	m-m	213
3	yy-yy	212
4	guest-guest	211
5	vnc-vncpass	207

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

绿盟威胁情报中心(NTI)

绿盟威胁情报中心(NSFOCUS Threat Intelligence center, NTI)是绿盟科技为落实智慧安全2.0战略,促进网络空间安全生态建设和威胁情报应用,增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力,对全球网络安全威胁和态势进行持续观察和分析,以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容,推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品,为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力,帮助用户更好地了解和应对各类网络威胁。

www.nsfocus.com

总部:北京海淀区北洼路4号益泰大厦
绿盟科技(股票代码300369)

邮编:100089
电话:010-68438880
传真:010-68437328
邮箱:webadmin@nsfocus.com

绿盟科技官方微信