网络安全威胁态势分析 月报

2020 年 10 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 10 月份的新增漏洞呈下降趋势，新增高危漏洞 131 个，主要分布在 Microsoft、Google、Cisco、Apple、Adobe、Oracle、IBM、draytek、小米等厂商的主要产品中。

2020 年 10 月绿盟科技安全漏洞库共收录 747 个漏洞[1]，其中高危漏洞 131 个，微软高危漏洞 44 个。绿盟科技收录高危漏洞数量与前期相比呈下降趋势。

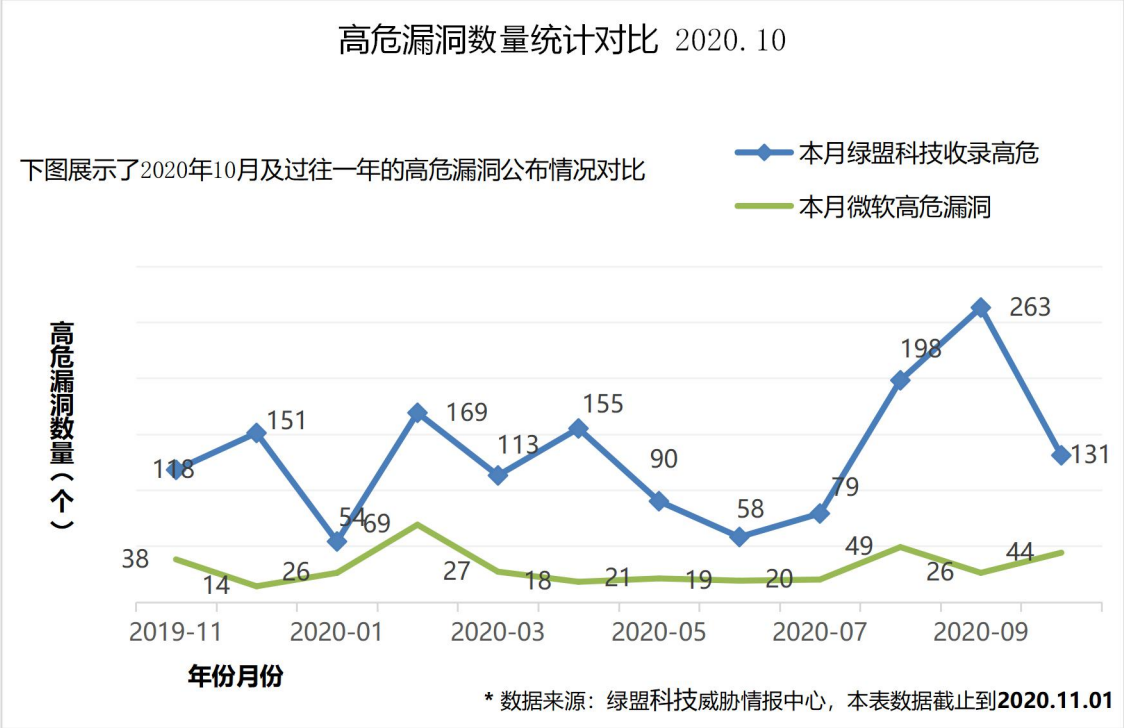

图 1.1 高危漏洞数量统计对比

1.2 恶意软件态势综述

2020 年 10 月份数据与 2020 年 1 至 10 月份数据中恶意软件各类型分布如下图所示。10 月份各恶意软件类型占比相比 2020 年全年情况有

[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。

所波动，后门与挖矿稍有下降，均占比 74%左右；蠕虫表现基本持平，木马活跃度有所下降。

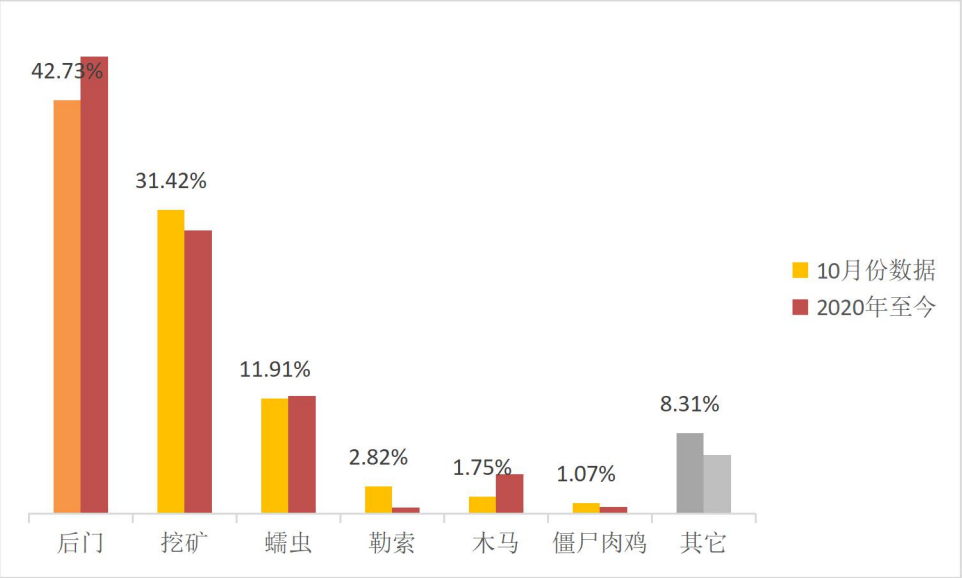

图 1.2 恶意软件类型

1.3 物联网安全态势综述

本月有 3 个值得重点关注的物联网安全事件：

（1）蓝牙出血：基于 Linux 物联网设备的“零点击”内核漏洞

（2）5G 打开潘多拉盒子：全球被感染物联网设备猛增 100%

本月漏洞平台 Exploit-DB 新增 22 个物联网漏洞利用，存在 4 个 RCE 类漏洞，大部分危害程度较低。

本月针对物联网设备的攻击数量趋于平稳。

1.4 DDOS 攻击态势综述

2020 年 10 月份，我们监控到 DDoS 攻击次数和攻击总流量相比上个月都有所减少。2020 年 10 月，攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 63%。从一天 24 小时攻击占比来看，0 点到 7 点为攻击高峰攻击。从每周中 DDoS 攻击活动的分布来看，主要集中在周二。2020

年 10 月份主要的攻击类型是 SYN 类型，占总攻击次数的 52%。从流量占比来看，SYN Flood 发起的攻击流量占比最高，占比 53%。根据 2020 年 10 月的 DDoS 攻击数据（国际 nta 数据）进行聚类分析，共发现 24 个团伙活跃。

1.5 僵尸网络及蜜罐态势综述

2020 年 10 月份僵尸网络活动主要由 DDoS 攻击构成，其中主要攻击来自知名 DOFLOO 木马家族。本月的 DDoS 攻击手段主要倾向于 CC_FLOOD，僵尸网络控制端主要托管于云服务厂商 DigitalOcean 及 Hotwinds，木马传播利用漏洞主要为 CVE-2017-17215,与往月差别不大。

蜜罐方面，2020 年 10 月份互联网攻击活动主要由恶意扫描构成，针对 80 端口的攻击呈现上升趋势，漏洞利用方面，CVE-2017-10271 漏洞利用占比较高。DDOS 反射攻击方面，DNS 服务上月攻击数据最多。上月捕获 8930024 次攻击事件，其中攻击次数最高的攻击事件针对目标为 109.174.127.6，持续时间达到 28 小时。

2. 漏洞态势

2.1 漏洞类型分析

在本月收录的 131 个高危漏洞中，包括命令执行、信息泄露、拒绝服务、未授权的信息修改等漏洞类型。具体数量如下图：

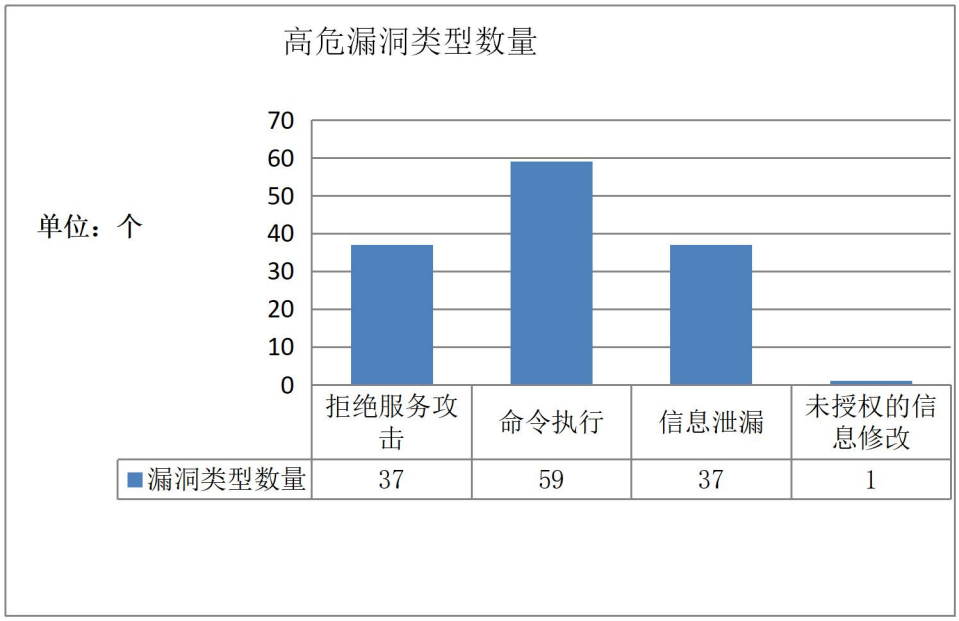

图 2.1 高危漏洞类型数量

2.2 漏洞分布分析

131 个高危漏洞主要分布在 Microsoft、Google、Cisco、Apple、Adobe、Oracle、IBM、draytek、小米等厂商的主要产品中。共涉及 18 个厂商，其中数量的分布如下：

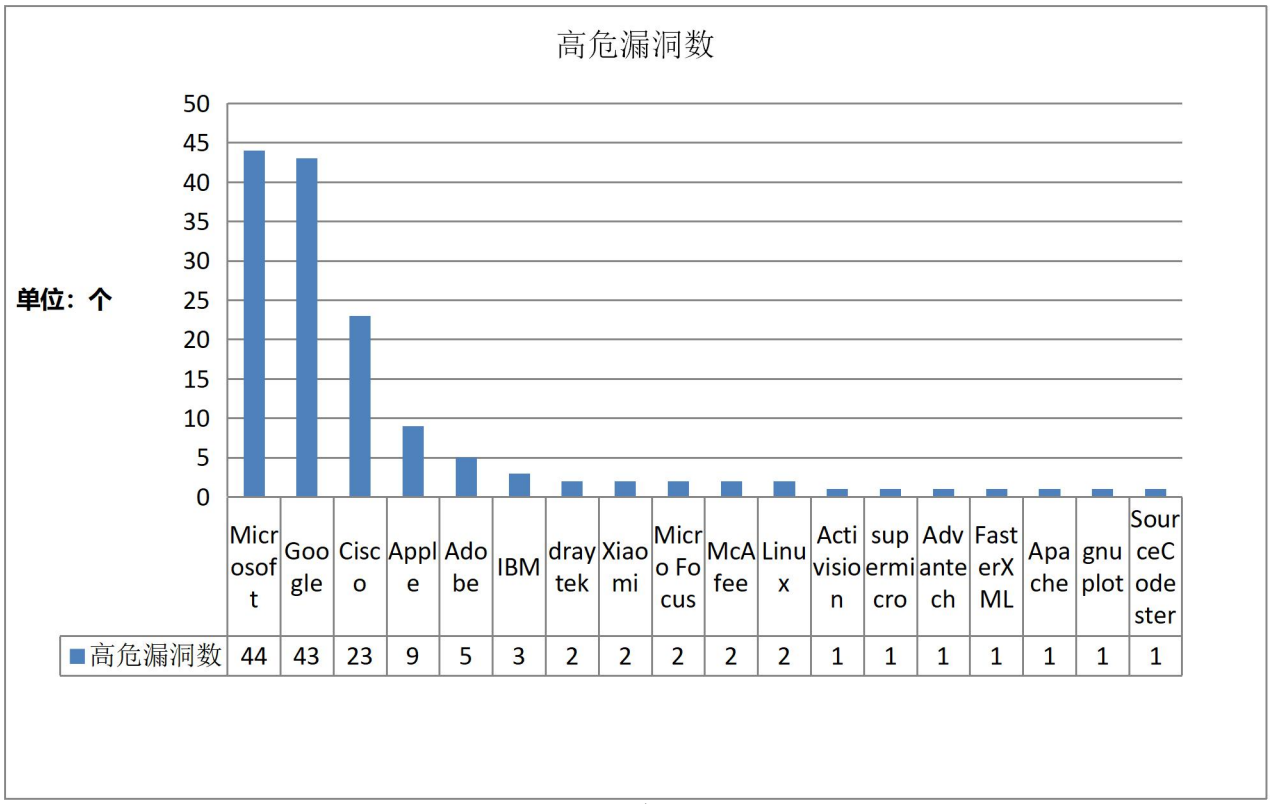

图 2.2 高危漏洞数目

其中微软相关的漏洞有 44 个，主要分布在 Microsoft Windows 操作系统、Visual Studio、Exchange Server、SharePoint Server、Edge 浏览器以及 Azure 等广泛使用的产品，其中包括命令执行、信息泄露以及拒绝服务等高危漏洞类型。

Google 相关的 43 个漏洞分布在 Chrome 浏览器以及 Android 系统中，Chrome 浏览器的漏洞主要包含缓冲区溢出、内存错误以及越界写入。

Cisco 相关的漏洞有 23 个，漏洞主要分布在运行 Cisco IOS 和 Cisco IOS XE 软件的 Cisco 设备以及网络接入点设备 APS 中。成功利用这些漏洞可以在受影响的系统中执行任意代码、拒绝服务、越界写入。

Apple 相关的漏洞有 9 个，主要分布在各个操作系统中，包含 macOS Catalina、iOS、iPadOS、tvOS、watchOS 等。

2.3 10 月热点漏洞分析

（1） Microsoft Windows TCP/IP 远程代码执行漏洞

CVE-2020-16898

NSFOCUS ID：49927

受影响版本

Microsoft Windows 10 Version 2004

Microsoft Windows 10 Version 1909

Microsoft Windows 10 Version 1903

Microsoft Windows 10 Version 1809

Microsoft Windows 10 Version 1803

Microsoft Windows 10 Version 1709

Microsoft Windows Server version 2004 (Server Core Inst

Microsoft Windows Server version 1909 (Server Core Inst

Microsoft Windows Server version 1903 (Server Core Inst

Microsoft Windows Server 2019 (Server Core Installation

Microsoft Windows Server 2019

漏洞点评

Windows TCP/IP 存在远程代码执行漏洞。该漏洞源于程序未对 ICMPv6 路由器广告数据包进行正确处理。攻击者可以借助特制 ICMPv6 路由器广告数据包利用该漏洞实现远程代码执行。

（2） Cisco IOS XE 任意代码执行漏洞

CVE-2020-3423

NSFOCUS ID：49356

受影响版本

Cisco Cloud Services Router 1000V Series

Cisco 4000 Series Integrated Services Routers

Cisco ASR 1000 Series Aggregation Services Routers

Cisco Integrated Services Virtual Routers

漏洞点评

Cisco IOS XE Software 中 Lua 解释器的实现存在任意代码执行漏洞。该漏洞源于程序在用户提供的 Lua 脚本的上下文中未对 Lua 函数调用进行正确限制。经过身份认证的本地攻击者可通过提交恶意的 Lua 脚本利用该漏洞在受影响设备的基础 Linux 操作系统（OS）上以 root 特权执行任意代码。

（3） Apache ActiveMQ 任意代码执行漏洞

CVE-2020-11998

NSFOCUS ID：49920

受影响版本：

Apache ActiveMQ 5.15.13

漏洞点评

Apache ActiveMQ 5.15.13 版本存在任意代码执行漏洞。该漏洞源于 RMIConnectorServer 函数未对输入进行正确验证。攻击者可利用该漏洞使 Java 应用程序在系统上执行任意代码。

2.4 常见漏洞利用攻击趋势分析

10 月份监测的告警共 68142729 次，基于漏洞利用的攻击排名 TOP10 如表 2-1 所示。其中 NTP ntpd monlist Query Reflection 拒绝服务漏洞(CVE-2013-5211)的告警最多，共 3253335 次。

表 2.1 10 月份漏洞利用告警 TOP10

漏洞告警信息	告警次数
NTP ntpd monlist Query Reflection 拒绝服务漏洞(CVE-2013-5211),	3253335
OpenSSl SSLv2 弱加密通信方式易受 DROWN 攻击(CVE-2016-0800)	176944
Windows SMB 远程代码执行漏洞(Shadow Brokers EternalBlue) (CVE-2017-0144)(MS17-010)	85571
ThinkPHP 5.x 远程命令执行漏洞	83812
Apache php 文件后缀解析漏洞	46544
Netgear DGN1000B setup.cgi 远程命令注入漏洞	30520
Apache Shiro RememberMe 反序列化漏洞(CVE-2016-4437)	27163
PHPUnit 远程代码执行漏洞(CVE-2017-9841)	25584
GPON Home Gateway 远程命令执行漏洞 (CVE-2018-10561/CVE-2018-10562)	22108
D-Link Routers 操作系统命令注入漏洞(CVE-2015-2051)	22007

从漏洞类型来看，主要以拒绝服务、弱加密通信、反序列化以及远程代码执行为主。

从漏洞分布来看，主要有包含协议类型的 NTP 协议、SSLv2 协议以及 SMB 协议，框架类的 ThinkPHP、Web 服务器程序 Apache，PHP 的单元测试 PHPUnit，除此之外还监测到了 3 个工业物联网的漏洞利用，涉及 Netgear DGN1000B 无线路由器、GPON 家用光纤路由器以及 D-Link 路由器。

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。

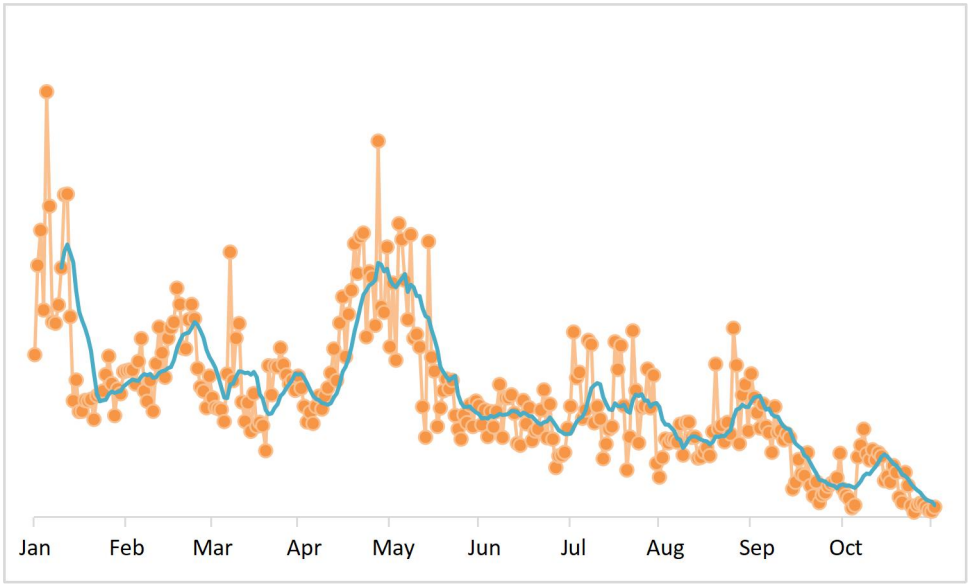

图 3.1 1 至 10 月份后门程序活动监测

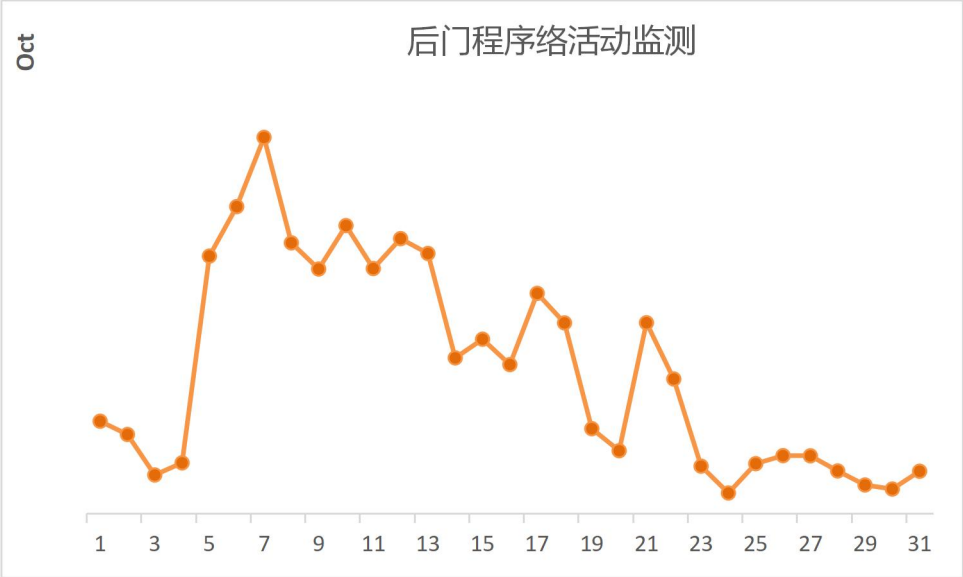

图 3.2 10 月份后门程序活动监测

从活跃趋势上来看，十月份月初活跃度有一个小的提升，整体呈下降趋势。十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。

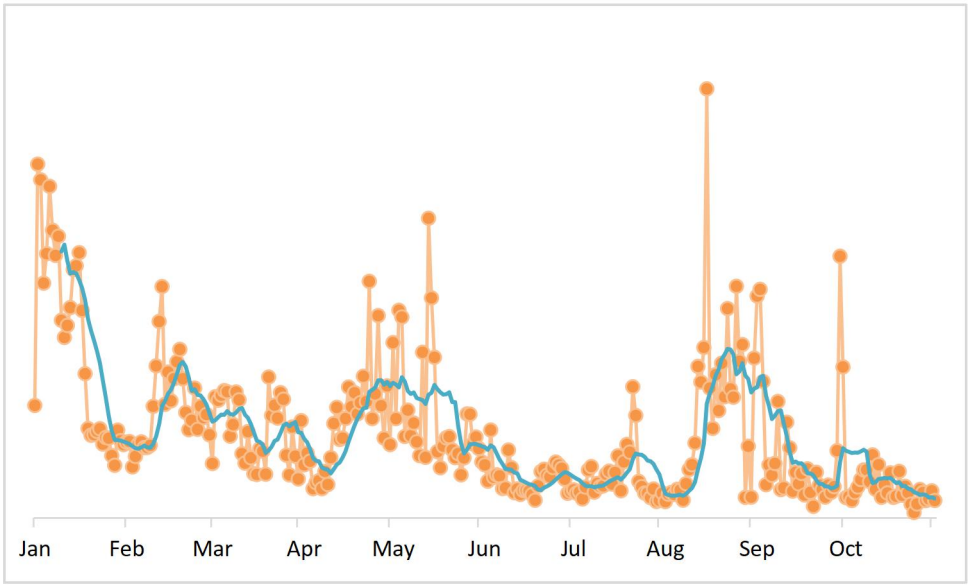

图 3.3 1 至 10 月份挖矿程序活动监测

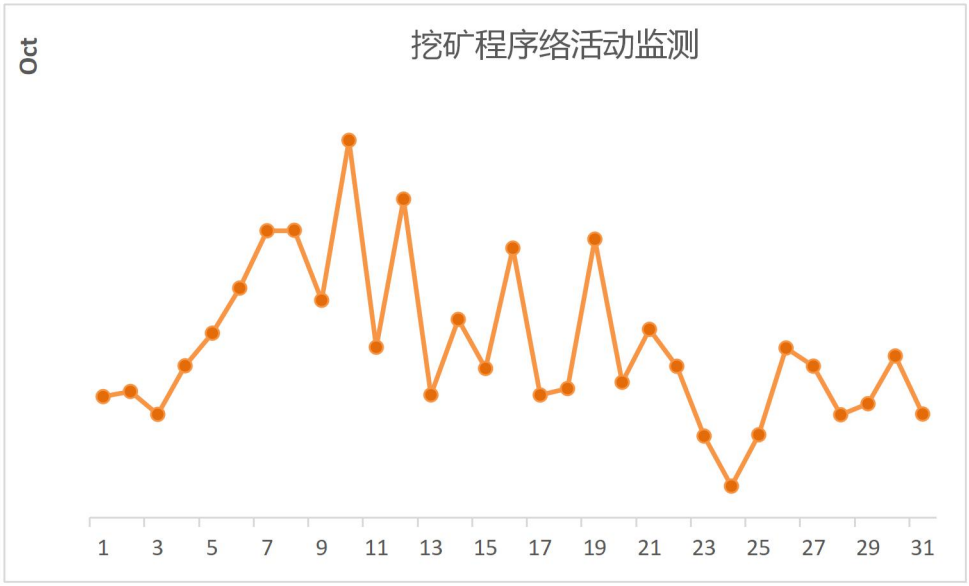

图 3.4 10 月份挖矿程序活动监测

相较于九月份波动不大，整体活跃度较低。十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。

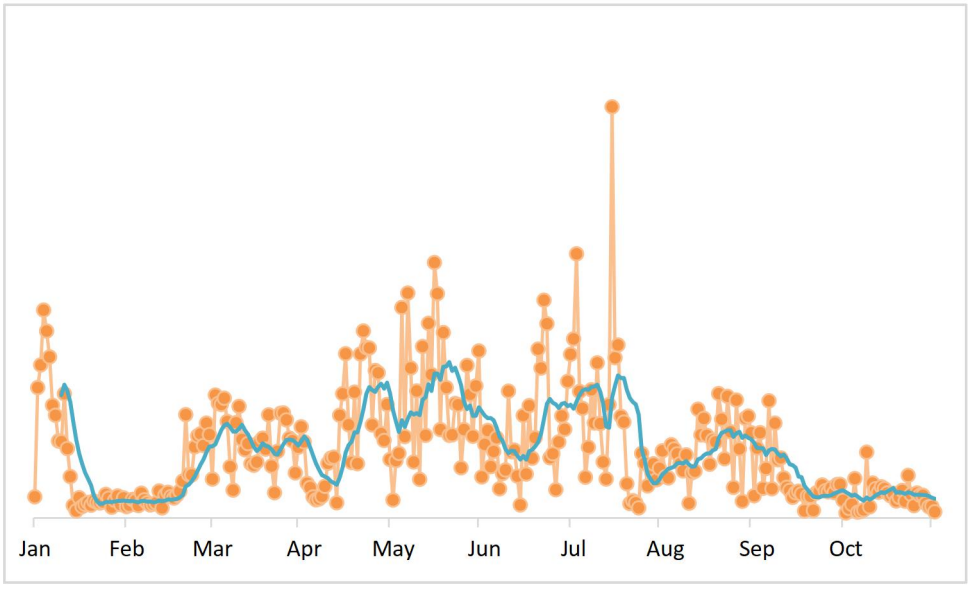

图 3.5 1 至 10 月份蠕虫活动监测

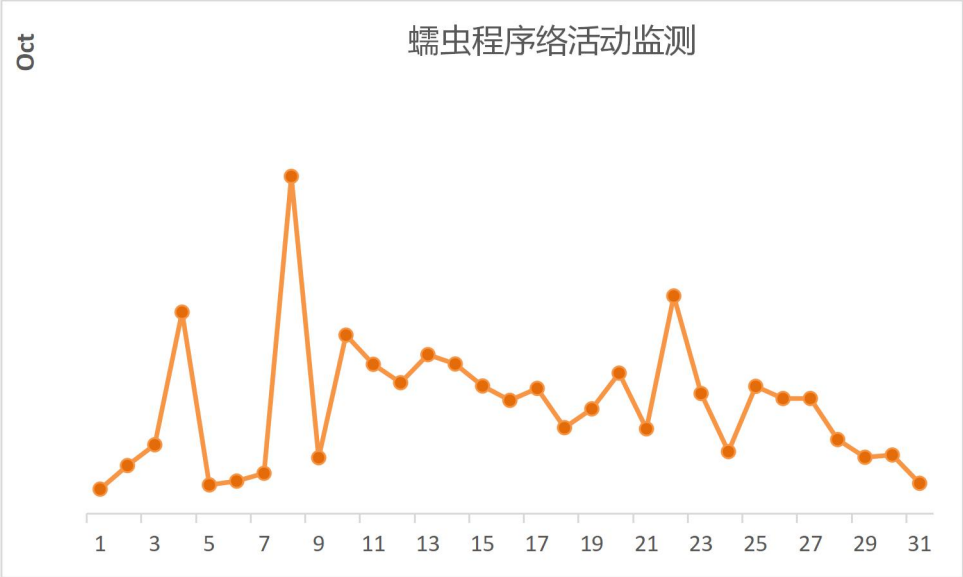

图 3.6 10 月份蠕虫活动监测

从全年数据来看，蠕虫程序活波动不大，几乎与二月份持平，处于全年较低水平。十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。

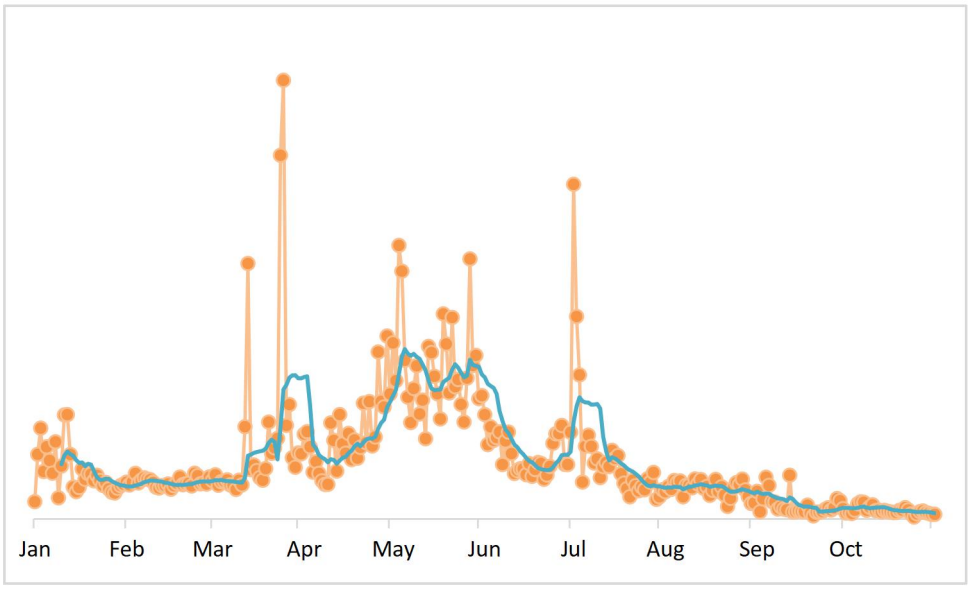

图 3.7 1 至 10 月份木马活动监测

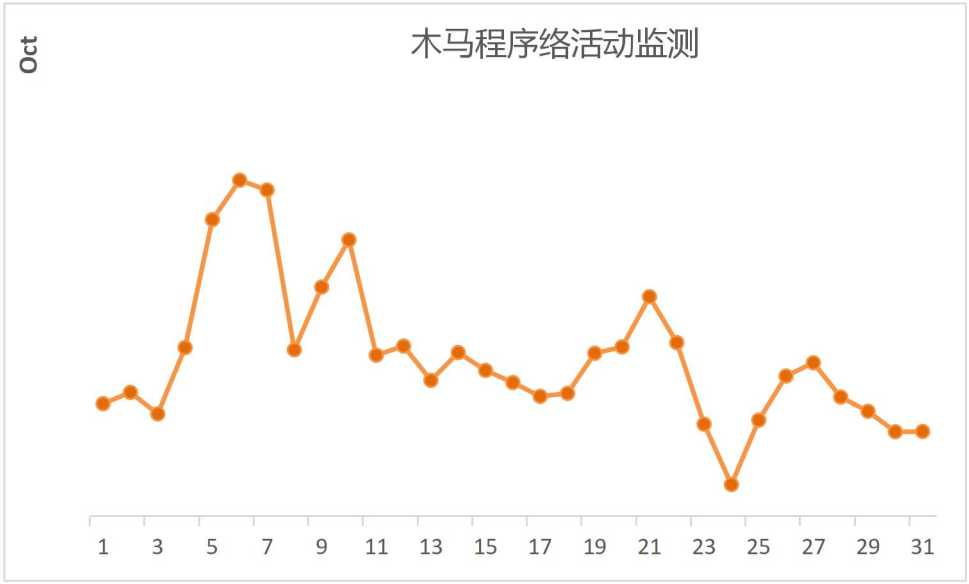

图 3.8 10 月份木马活动监测

从全年数据来看，木马程序活跃度从七月份开始逐渐下降，十月份整体呈下降趋势且波动范围不大，十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

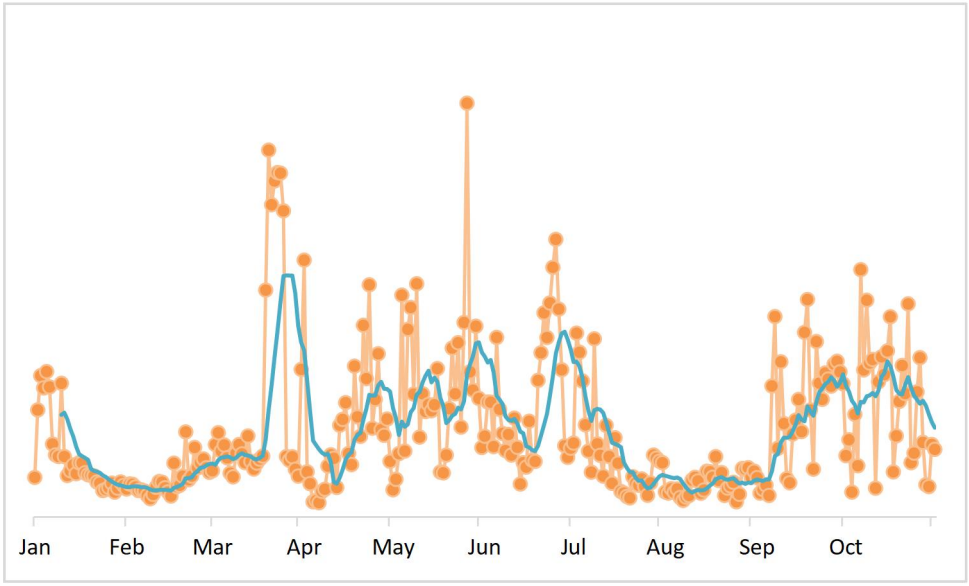

图 3.9 1 至 10 月份勒索软件活动监测

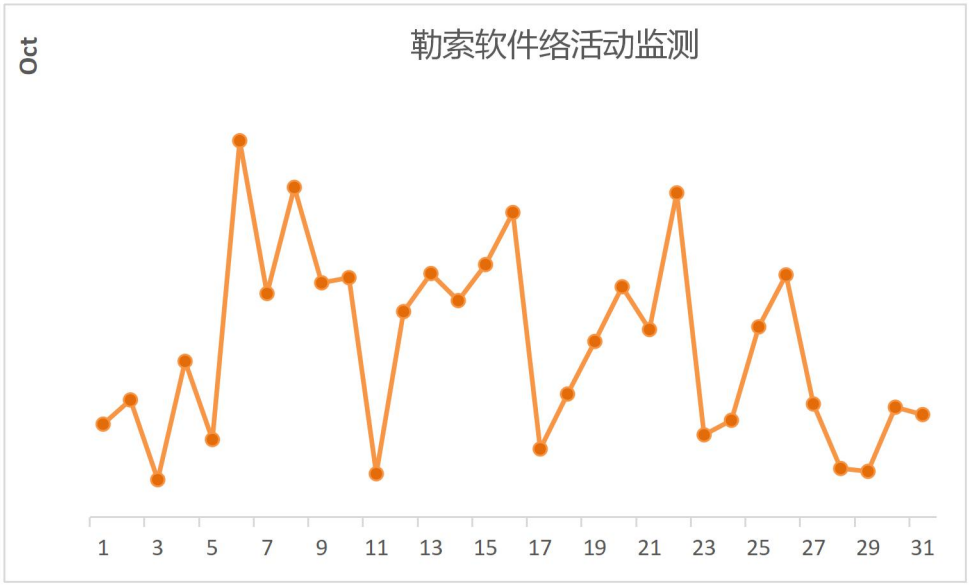

图 3.10 10 月份勒索软件活动监测

从全年的数据来看，十月份勒索软件活动呈上升趋势，整个十月份一直在波动，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 10 月重点物联网安全事件分析

（1）蓝牙出血：基于 Linux 物联网设备的“零点击”内核漏洞

Google 和英特尔警告说，Linux 蓝牙协议栈 BlueZ 发现一个高危漏洞，该协议栈为基于 Linux 的物联网（IoT）设备提供核心蓝牙层和协议的支持。

根据 Google 的说法，此漏洞影响支持 BlueZ 的 5.9 之前的 Linux 内核版本的用户。BlueZ 是根据 GNU 通用公共许可（GPL）发行的一个开源项目，具有 BlueZ 内核，该内核从 2.4.6 版本开始就已成为正式 Linux 内核的一部分。

该漏洞被 Google 称为“血牙”，可以由未经身份验证的本地攻击者通过特定输入进行“零点击”攻击，从而在目标设备上提升权限。

根据 Google 在 Github 上发布的一篇文章：

一个远程攻击者只需知道受害者的蓝牙地址就可以发送恶意的 l2cap （逻辑链路控制和适配层协议）数据包，实施拒绝服务攻击或带有内核特权的任意代码执行，恶意蓝牙芯片也可以触发此漏洞。

该漏洞（CVE-2020-12351）的 CVSS 评分为 8.3，属于较为严重的漏洞。它特别是源于 net/bluetooth/l2cap_core.c 中基于堆的类型混淆。类型混淆漏洞是一个特定的漏洞，可能导致超出范围的内存访问，并可能导致攻击者可以利用的代码执行或组件崩溃。在这种情况下，问题在于 Linux 内核中的 BlueZ 实现中没有对用户提供的输入进行验证。

（2）5G 打开潘多拉盒子：全球被感染物联网设备猛增 100%

根据诺基亚发布的最新《2020 年威胁情报报告》，过去一年来，全球受感染的物联网（IoT）设备的数量猛增了 100%。该报告根据服务提供商使用其 NetGuard Endpoint Security 工具处理的数据编制而成的。

报告显示，受感染的物联网设备现在占总数的近三分之一（32.7%），大大高于 2019 年报告中的 16.2%。

诺基亚认为，联网设备的感染率很大程度上取决于设备在互联网上的可见性。

“在为设备定期分配面向公众的互联网 IP 地址的网络中，我们发现 IoT 感染率很高。在使用运营商级 NAT 的网络中，由于网络扫描看不到易受攻击的设备，因此感染率大大降低了。”

“随着 5G 的实施，预计不仅物联网设备的数量将急剧增加，而且直接从互联网访问的物联网设备的份额也将增加。”

诺基亚警告说，5G 的其他方面也将给电信公司带来重大的新安全挑战：特别是网络功能虚拟化（NFV）和软件定义的网络（SDN）。

4.2 10 月新增物联网漏洞情况

2020 年 10 月，漏洞利用平台 Exploit-DB 新增 22 个物联网漏洞利用。

表 4.1 2020 年 10 月新增物联网漏洞情况

EDB-ID	厂商	脆弱性类型	影响设备
48835	Mida Solutions	Remote Code Execution	Mida eFramework 2.8.9
48857	Karel	Directory Traversal	Karel IP Phone IP1211
48847	SpinetiX	Username Enumeration	SpinetiX Fusion Digital Signage 3.4.8
48846	SpinetiX	CSRF	SpinetiX Fusion Digital Signage 3.4.8
48845	SpinetiX	Database Backup Disclosure	SpinetiX Fusion Digital Signage 3.4.8
48844	BrightSign LLC	File Delete Path Traversal	BrightSign Digital Signage Diagnostic Web Server 8.2.26
48843	BrightSign LLC	Server-Side Request Forgery	BrightSign Digital Signage Diagnostic Web Server 8.2.26
48842	Sony	Remote Stack Buffer Overflow	Sony IPELA Network Camera 1.82.01
48871	Cisco Systems, Inc.	Path Traversal	Cisco ASA and FTD 9.6.4.42
48863	D-Link	Denial of Service	D-Link DSR-250N 3.12
48908	Comtrend Corporation	Persistent XSS	Comtrend AR-5387un router
48903	Hisilicon	Unauthenticated RTSP buffer overflow (DoS)	HiSilicon Video Encoders
48902	Hisilicon	Full admin access via backdoor password	HiSilicon Video Encoders
48901	HiSilicon	RCE via unauthenticated upload of malicious firmware	HiSilicon video encoders
48900	HiSilicon	RCE via unauthenticated command injection	HiSilicon Video Encoders
48899	HiSilicon	Unauthenticated	HiSilicon Video Encoders

		file disclosure via path traversal	
48952	ReQuest	Remote Code Execution	ReQuest Serious Play F3 Media Server 7.0.3
48951	ReQuest	Remote Denial of Service	ReQuest Serious Play F3 Media Server 7.0.3
48950	ReQuest	Debug Log Disclosure	ReQuest Serious Play F3 Media Server 7.0.3
48949	ReQuest	Directory Traversal File Disclosure	ReQuest Serious Play Media Player 3.0
48948	GX Group	XSS	Genexis Platinum-4410
48958	Embedthis Software LLC	Digest Authentication Capture Replay Nonce Reuse	GoAhead Web Server 5.1.1

4.3 物联网漏洞利用情况

本月绿盟威胁捕获系统捕获到来自 54355 个 IP 的 3545149 次访问请求日志。其中 36.50%的访问请求是对物联网漏洞进行利用的恶意攻击行为，在 54.93%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。

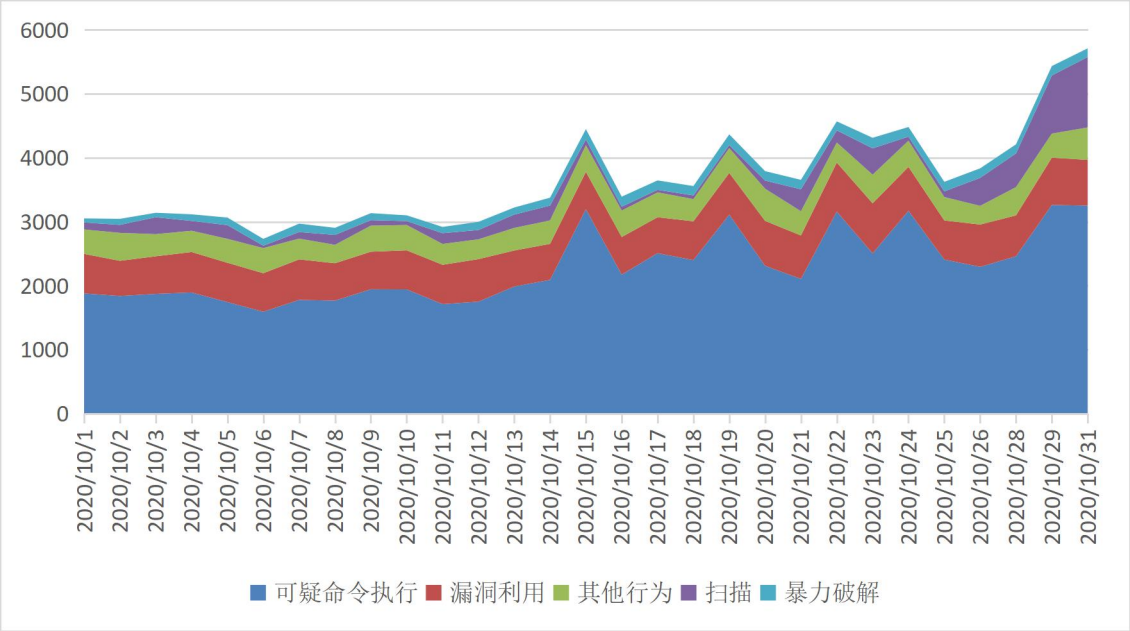

图 4.2 攻击源 IP 总量趋势

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
Sony IP Camera Scan(possibly related to CVE-2018-3937/3938)		718509
MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution (Metasploit)	edb-41471	242286
AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities	edb-40500	113834
D-Link Devices - HNAP SOAPAction-Header Command Execution (Metasploit)	cve-2015-2051	86896
Eir D1000 Wireless Router - WAN Side Remote Command Injection (CVE-2016-10372)	cve-2016-10372	22207
Multiple CCTV-DVR Vendors - Remote Code Execution	edb-39596	18791
九安摄像头扫描		18491
GPON Routers - Authentication Bypass / Command Injection CVE-2018-10561 / CVE-2018-10562	cve-2018-10562	6699
CVE-2017-17215 - Huawei Router HG532 - Arbitrary Command Execution	cve-2017-17215	5852
Realtek SDK - Miniigd UPnP SOAP Command Execution (Metasploit) CVE-2014-8361	cve-2014-8361	4769

4.4 物联网威胁攻击源与攻击事件分析

对本月蜜罐日志中的 54355 个源 IP 进行分析，其中 46671 个 IP 发起过漏洞利用等恶意行为，环比上月增加 50.28%。从关联到恶意行为的 IP 分布在了 178 个国家和地区，从国家分布情况来看，中国最多，占比达到了 29.46%。

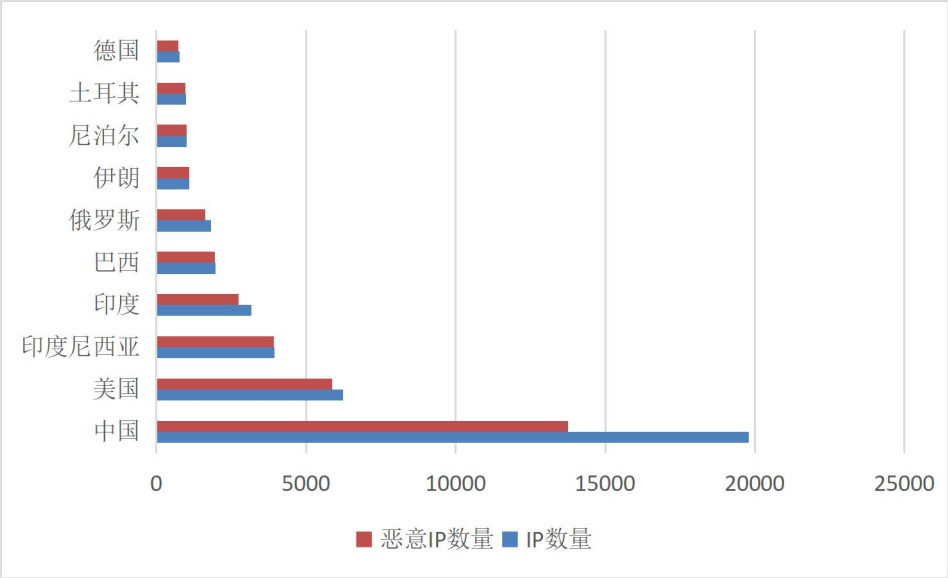

图 4.3 蜜罐的日志源 IP 的国家分布情况

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。

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。

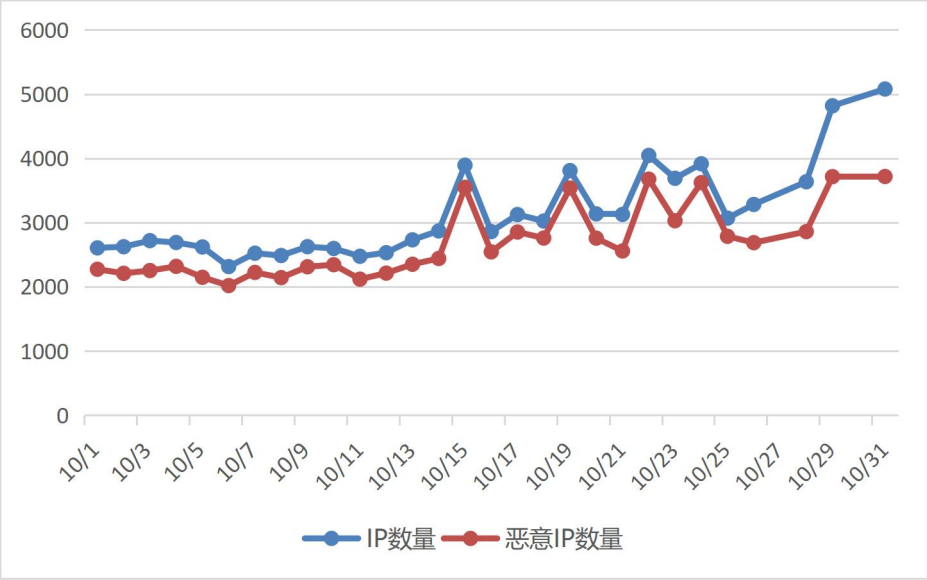

图 4.4 每日访问蜜罐的所有 IP、发送攻击请求 IP 的数量趋势

5. DDoS 攻击态势

5.1 DDoS 攻击流量与攻击次数

2020 年 10 月份，我们监控到 DDoS 攻击次数为 1843 次（event_id 为粒度），攻击总流量 393Tb，详见下图。

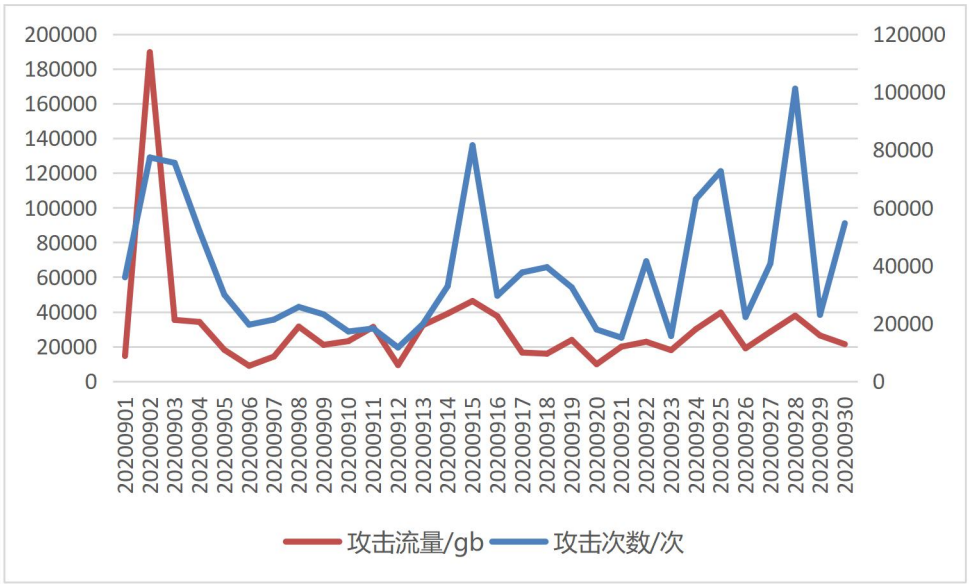

图 5.1 攻击流量与攻击次数

5.2 DDoS 攻击时间刻画

攻击持续时间占比

2020 年 10 月，攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 63%。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。

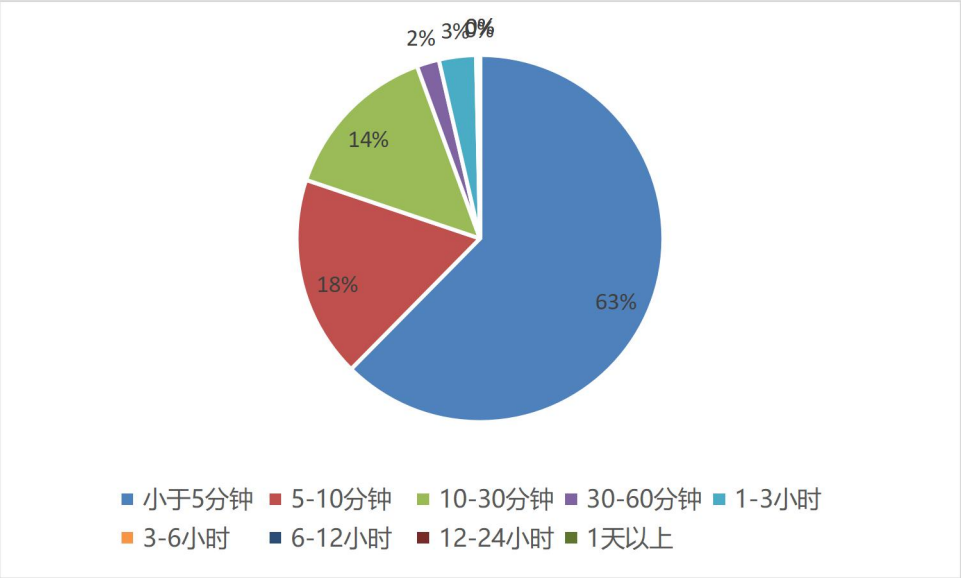

图 5.2 攻击持续时间占比

一天中 DDos 攻击活动分布

从一天 24 小时攻击占比来看，0 点到 7 点为攻击高峰攻击。

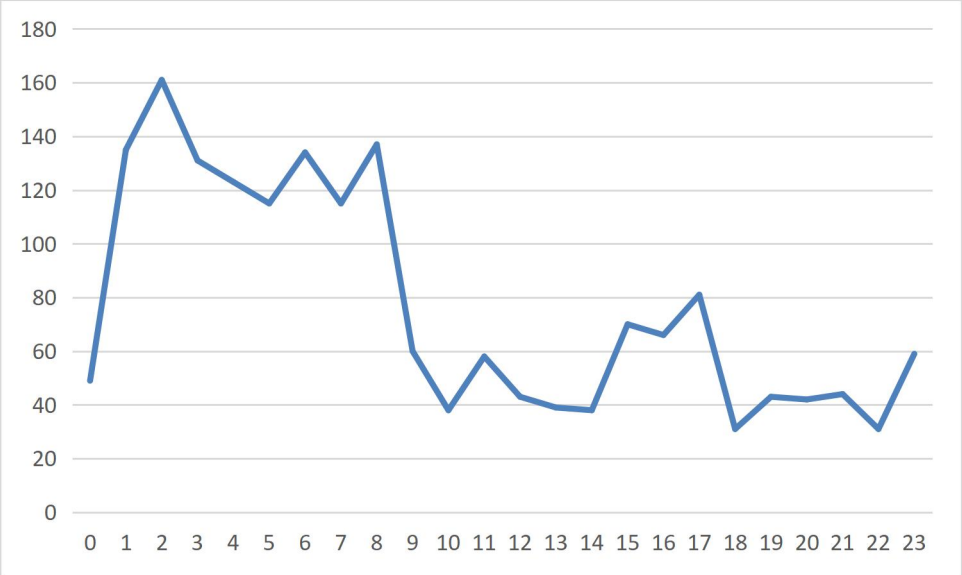

图 5.3 一天中 DDos 攻击活动分布

一周中 DDos 攻击活动分布

从每周中 DDoS 攻击活动的分布来看，周二最常被攻击。

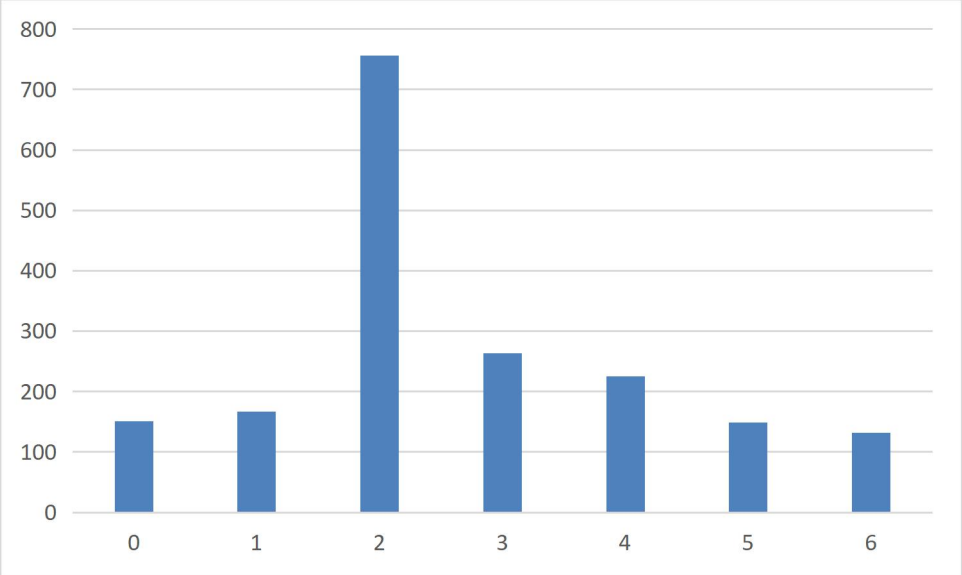

图 5.4 一周中 DDos 攻击活动分布

5.3 DDoS 攻击类型分析

2020 年 10 月份主要的攻击类型是 SYN 类型，占总攻击次数的 52%。从流量占比来看，SYN Flood 发起的攻击流量占比最高，占比 53%。

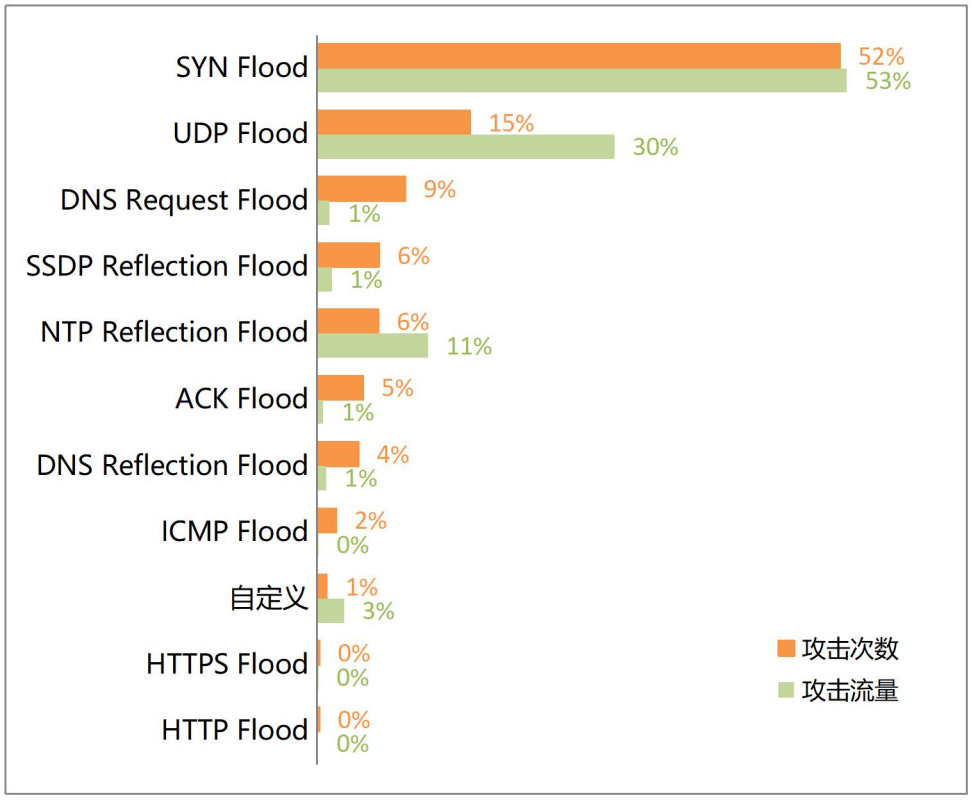

图 5.5 攻击类型分布

5.4 10 月份 DDoS 肉鸡团伙分析

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 10 月的 DDoS 攻击数据（国际 nta 数据）进行聚类分析，共发现 24 个团伙活跃。

团伙编号	攻击源数量（核心实体）	攻击目标数量	攻击事件数量	活跃天数	最大bps	最大pps
cluster_ddos@nta[oversea]_sipgang_20201001-202001101_1	11826	572	5682	37	9997516	99942
cluster_ddos@nta[oversea]_sipgang_20201001-202001101_5	781	13	448	9	99955507	999424
cluster_ddos@nta[oversea]_sipgang_20201001-202001101_6	435	629	4396	36	9997690666	99833
cluster_ddos@nta[oversea]_sipgang_20201001-202001101_7	372	175	1392	22	99973333	99833
cluster_ddos@nta[oversea]_sipgang_20201001-202001101_8	334	44	7158	18	9987686	99942

图 5.6 团伙规模 top5 概览

规模最大团伙画像如下表，

表 5.1 团伙 Gang10 月画像

团伙编号	cluster_ddos@nta[oversea]_sipgang_20201001-202001101_1
攻击源数量(核心实体)	11826
攻击目标数量	572
攻击事件数量	5682
活跃天数	37
最大 bps	9997516
最大 pps	99942
攻击类型分布	SYN Flood（3591，63.00%），HTTPS Flood（603，11.00%），UDP Flood（512，9.00%）
攻击目标端口	80（2292，40.00%），443（1073，19.00%），0（171，3.00%）
攻击源端口	1900（353，6.00%），0（159，3.00%），389（115，2.00%）
攻击源资产-传输层端口	80（5810，49.00%），443（5034，43.00%），22（4376，37.00%）
攻击源资产-传输层协议	TCP（9785，83.00%），UDP（7012，59.00%），SSL（4854，41.00%）
攻击源资产-开放	HTTP（7350，62.00%），HTTPS（5153，44.00%），SSH（3978，34.00%）

服务协议	
攻击源资产-设备类型	Router（2027，17.00%），Camera（1507，13.00%），VoIP（117，1.00%）
攻击源资产-厂商	OpenBSD（2246，19.00%），Apache（2240，19.00%），nginx（1277，11.00%）
攻击源资产-产品	
攻击源-国家	中国（2354，20.00%），美国（1785，15.00%），越南（1075，9.00%）
攻击源-省	香港（402，3.00%），加利福尼亚州（390，3.00%），胡志明市（329，3.00%）
攻击源-城市	未知（6340，54.00%），都柏林（240，2.00%），洛杉矶（199，2.00%）
攻击源-IDC 标签	其他（8560，72.00%），IDC（3265，28.00%）
攻击源-基站信息	其他（11820，100.00%）
攻击源-机构	其他（11274，95.00%），netserv.ro（10，0.00%）
攻击源-运营商	移动（1313，11.00%），其他（1203，10.00%），vnpt.vn（758，6.00%）
攻击目标-国家	美国（165，29.00%），中国（137，24.00%），阿联酋（69，12.00%）
攻击目标-省	香港（126，22.00%），爱荷华州（52，9.00%），阿布扎比（51，9.00%）
攻击目标-城市	未知（238，42.00%），得梅因（52，9.00%），博伊顿（50，9.00%）
攻击目标-IDC 标签	IDC（545，95.00%），其他（27，5.00%）
攻击目标-基站信息	其他（572，100.00%）
攻击目标-机构	microsoft.com（431，4.00%），zenlayer.com（36，0.00%），kirinnetworks.com（35，0.00%）
攻击目标-运营商	其他（571，5.00%）
按天统计-事件数量	20200807（680，12.00%），20200716（338，6.00%），20200821（303，5.00%）

按天统计-攻击源数量	20200716（2704，6.00%），20200726（2647，6.00%），20200722（2516，6.00%）
按天统计-攻击目标数量	20200820（45，5.00%），20200726（41，4.00%），20200723（39，4.00%）
详情-攻击源 IP	47.240.91.102（4396，2.00%），47.244.191.228（2578，1.00%），103.13.229.143（1381，1.00%）
详情-攻击目标 IP	128.1.217.251（21926，9.00%），128.1.217.245（14631，6.00%），128.1.217.253（13878，6.00%）
详情-攻击事件	2614270955193421427（9387，4.00%），8299811766094563558（6694，3.00%），4410366264227284039（6063，3.00%）

5.5 小结

2020 年 10 月份，我们监控到 DDoS 攻击次数为 1843 次（event_id 为粒度），攻击总流量 393Tb 。2020 年 10 月，攻击时长在 5 分钟以内的 DDoS 攻击占了全部攻击的 63%。从一天 24 小时攻击占比来看，0 点到 7 点为攻击高峰攻击。从每周中 DDoS 攻击活动的分布来看，周二最常被攻击。2020 年 10 月份主要的攻击类型是 SYN 类型，占总攻击次数的 52%。从流量占比来看，SYN Flood 发起的攻击流量占比最高，占比 53%。根据 2020 年 10 月的 DDoS 攻击数据（国际 nta 数据）进行聚类分析，共发现 24 个团伙活跃。

6. 僵尸网络态势

6.1 DDoS 僵尸网络 10 月攻击概览

在 2020 年 10 月份的 DDoS 僵尸网络活动中，监控到的攻击事件数较 9 月有所下降。Mirai 依然占据事件数首位，而 Gafgyt 有所回升，而之前一直活跃的 Dofloo 和 SDBot 则暂时销声匿迹。

10 月检测到的 DDoS 攻击手段主要为 UDP flood 和 ACK flood。

10 月检测到的被用于托管僵尸网络控制端的已知云服务商/运营商以 ColorCrossing、Digital Ocean 和 OVH 为主。

10 月检测到的 IoT 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）、ThinkPHP 远程命令执行漏洞和 CVE-2018-10561（GPON 光纤路由器身份认证绕过漏洞）位居前 3。

6.1.1 DDoS 攻击事件及家族分布

2020 年 10 月份检测到 DDoS 攻击指令 17745 条，其中包含攻击事件数 8570，来自 5 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 Count	Percent
Mirai	6650	77.60%
Gafgyt	1729	20.18%
XorDDoS	127	1.47%
Nitol	53	0.62%
天罚 DDoS	11	0.13%

2020 年 10 月检测到的攻击事件相比 2020 月 9 月下降了 18%，这主要源于 DDoS 指令数的整体下降。Gafgyt 家族的事件数有一定回升，但 Dofloo、SDBot 和 Yoyo 等之前较为活跃的家族在 10 月并未监测出现活动迹象。

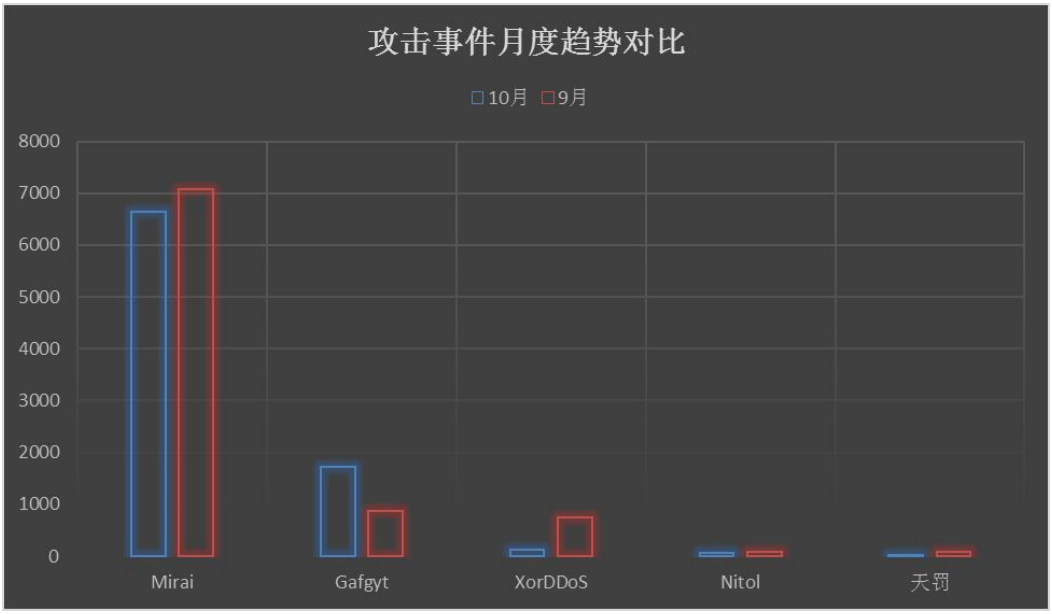

图 6.2 攻击事件趋势

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 6.2 攻击最大连续下发指令时长

Family	Max Duration of Continuously Issued DDoS Cmd
XorDDoS	3 小时
Mirai	44 分钟
Gafgyt	33 分钟
Nitol	13 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 6.3 攻击事件及家族比例

Family	Variant	Attack Count	Percent
Mirai	mirai	6650	77.60%
Gafgyt	gafgyt_left	1702	19.86%
	gafgyt_demon	17	0.20%
	gafgyt_builds	10	0.12%
XorDDoS	xorddos	127	1.48%
Nitol	DDOS.NITOL.S1P0R3.WV	42	0.49%
	DDOS.NITOL.S0P0R0.WO	8	0.09%
	DDOS.NITOL.S0P0R15.WV	2	0.02%
	DDOS.NITOL.S0P3R7.WV	1	0.01%

天罚 DDoS	DDOS.TF.S0P0R0.LO	11	0.13%

9 月份消失的 Gafgyt 变种 gafgyt_demon 在 10 月开始活动，而 gafgyt_rebirth 消失。而 Nitol 变种 DDOS.NITOL.S0P0R15.WV 重新出现轻微活动迹象。

6.1.3 DDoS 攻击事件 C&C 分布

表 6.4 地理分布

Country	Count	Percent
美国	55	38.19%
欧洲地区（未知）	21	14.58%
德国	11	7.64%
中国	8	5.56%
法国	7	4.86%
英国	7	4.86%
摩尔多瓦	7	4.86%
荷兰	7	4.86%
俄罗斯	6	4.17%
罗马尼亚	5	3.47%
奥地利	3	2.08%
加拿大	3	2.08%
爱尔兰	1	0.69%
韩国	1	0.69%
印度	1	0.69%
保加利亚	1	0.69%

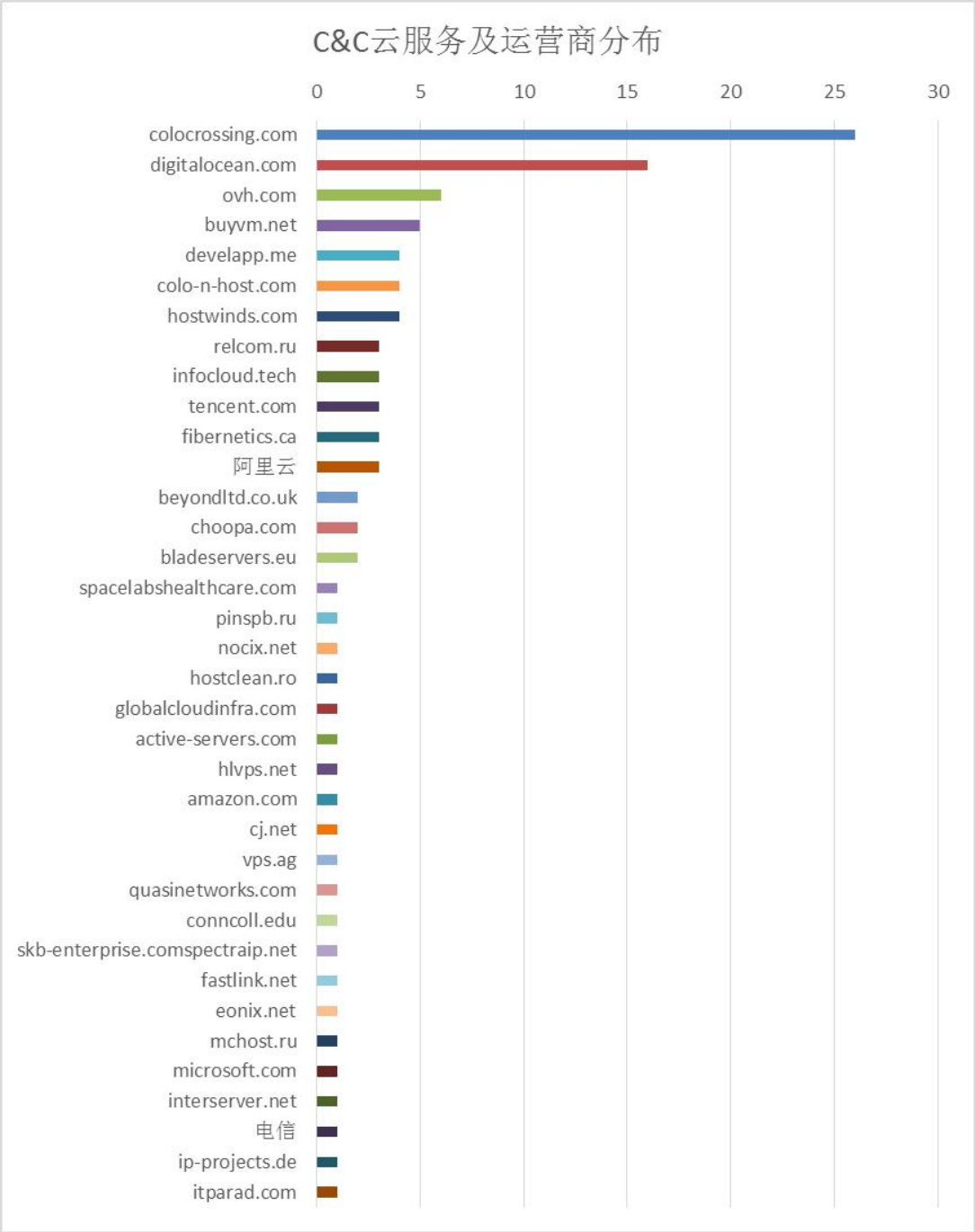

图 6.3 C&C 所属云服务及运营商分布

C&C 主要托管于云厂商，排名前三的分别是 ColorCrossing、Digital Ocean 和 OVH。此外有近 38 个分布在欧洲的 C&C 暂无法判断出归属。

6.1.4 DDoS 攻击指令活跃度日级分布

Mirai 总体（红）依旧保持着连续的活跃度，并承接 9 月底的上升趋势，在 10 月初达到高峰值，而其余时间较为平稳；其次是 gafgyt_left

（黄），在 8~15 日出现两次峰值；XorDDoS（棕）在 13~19 日期间出现了与 gafgyt_left 类似的情况。而天罚 DDoS（黑）在 8~12 内也发生过类似的涨幅。

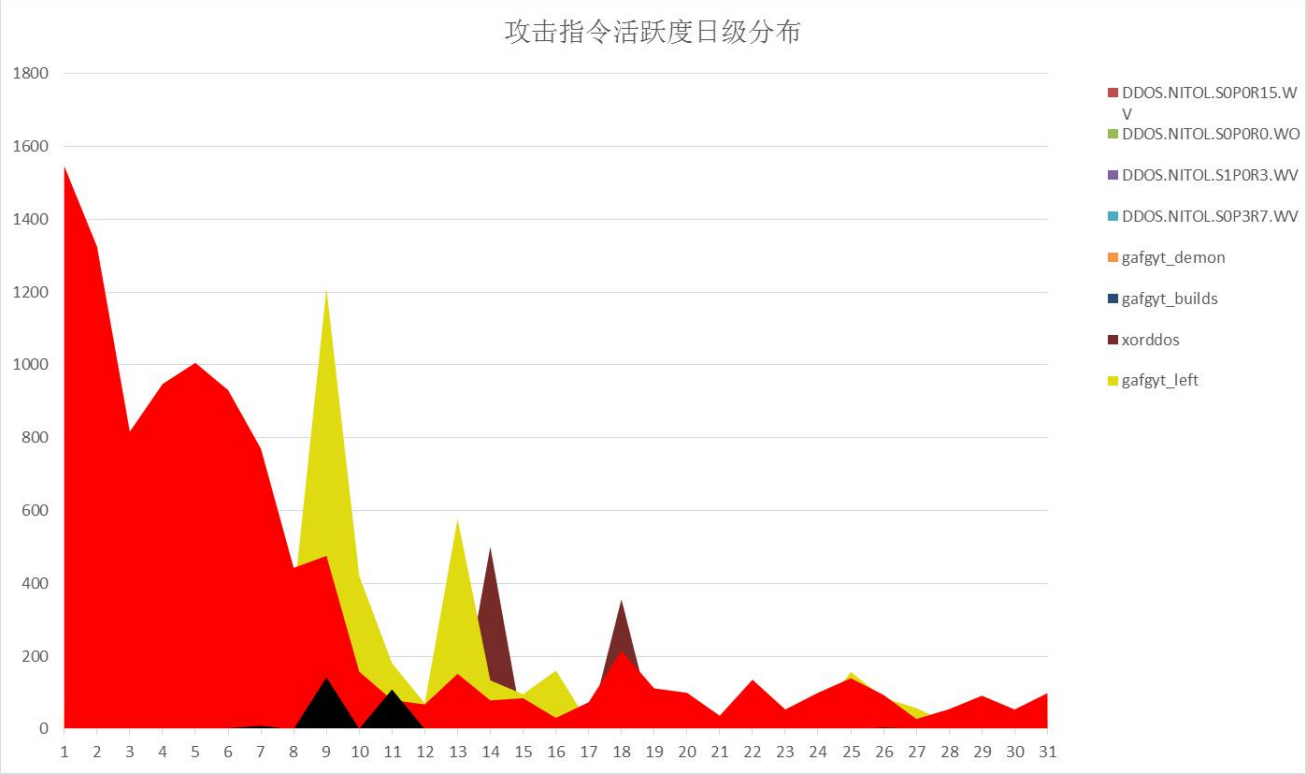

图 6.4 攻击指令活跃度日级分布

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	8226	48.35%
ACK flood	4068	23.91%
SYN flood	1660	9.76%
混合类型	1084	6.37%
HTTP flood	724	4.26%
TCP flood	557	3.27%
DNS flood	339	1.99%
GRETH	190	1.12%
IP flood	164	0.96%
SMTP flood	2	0.01%

6.1.6 攻击事件使用 Linux/IoT 漏洞分布

新增漏洞为 CVE_2017_9841、CVE_2020_8218 和 CVE_2020_3657。此外，还出现了 Mirai 变种 Moobot 利用不明潜在漏洞的情况。

Vulnerability	Count
CVE-2017-17215	2710
ThinkPHP_5_X_Remote_Command_Execution	1091
CVE-2018-10561	864
CVE-2014-8361	684
Common_Shell_Command_Abuse	617
ZyXEL_P660HN_T_v1_ViewLog_asp_privilege_escalation	581
JAWS_Webserver_unauthenticated_shell_command_execution	436
CVE-2015-2051	427
CCTV-DVR Remote Code Execution	403
D_Link_DSL_Devices_login_cgi_Remote_Command_Execution	397
Linksys_E_series_Unauthenticated_Remote_Code_Execution	349
CVE_2017_17215_2	325
Eir_D1000_Wireless_Router_WAN_Side_Remote_Command_Injection	304
unknown_exploit_ToolsCgi_moobot_20201103	295
CVE-2018-17173	291
Netgear_DGN1000_1_1_00_48_Setup_cgi_Remote_Code_Execution	279
CVE_2019_16920	250
CVE-2016-6277	160
Vacron_NVR_RCE	151
D_Link_OS_Command_Injection_via_UPnP_Interface	144
Netlink_GPON_Router_1_0_11_Remote_Code_Execution	131
CVE_2020_8218	96
CVE_2020_10173	46
CVE_2020_3657	21
vBulletin_5_6_2_widget_tabbedContainer_tab_panel_Remote_Code_Execution	20
Zyxel_P660HN_Remote_Command_Execution	17
CVE_2019_18396	14
CVE_2020_8515	11
CVE_2017_9841	11
NUUO_OS_Command_Injection_3	10
CVE-2017-6884	10
CVE-2014-9094	10

CVE_2014_2321	9
CVE_2017_5174	8
Seowon_Slc_130_And_SLR_120S_Router_RCE	8
zero_day_2020_09_04	8
CVE_2013_5948	7
Fastweb_Fastgate_0_00_81_Remote_Code_Execution	7
CVE_2020_5722	7
CVE_2019_6989	7
CVE_2020_7209	7
CVE_2013_5912	7
unknown_exploit_SetNet_20200930	7
CVE_2020_13782	7
EnGenius_RCE	7
CVE-2017-8221	7
AVCON6_systems_management_platform_OGNL_Remote_Command_Execution	7
DLink_and_TRENDnet_ncc2_service_multiple_vulnerabilities	7
Edimax_Technology_EW_7438RPn_v3_Mini_1_27_Remote_Code_Execution	7
Apache_Kylin_3_0_1_Command_Injection_Vulnerability	7
ACTi_ASOC_2200_Web_Configurator_2_6_Remote_Command_Execution	7
CVE_2020_12109	6
AVTECH_IP_Camera_NVR_DVR_Devices_Multiple_Vulnerabilities	2
wordpress_brute_force	2
Symantec_Web_Gateway_5_0_2_8_Remote_Code_Execution	2

表 6.6 攻击事件使用漏洞分布

6.2 威胁捕获 10 月数据概览

蜜罐方面，2020 年 10 月份互联网攻击活动主要由恶意扫描构成，其中针对低端口 19 的扫描占到绝大多数。漏洞利用方面，针对 AVTECH IP 摄像头、MVPower 摄像头、Dlink 路由器和 Redis 的攻击最多。弱口令登录主要来自荷兰、巴拿马和摩尔多瓦。DDOS 反射攻击方面，dns 占据近 50%。10 月共计捕获 DDoS 反射攻击事件超过 568 万例，其中最长的持续时间高达 50 小时左右。

6.2.1 攻击总览

在 10 月统计的 318006325 条数据中，共发现恶意连接 159423744 次，占比 98.67%；漏洞利用 457535 次，占比 0.28%；暴力破解 1697147 次，占比 1.05%；其中恶意连接占比最多。本月捕获 14 个平台恶意样本，其中 emotet 恶意家族占比最大，达到 46.05%。达到 55.28 %。

6.2.2 10 月攻击类型占比情况

图 6.5 10 月攻击类型占比情况

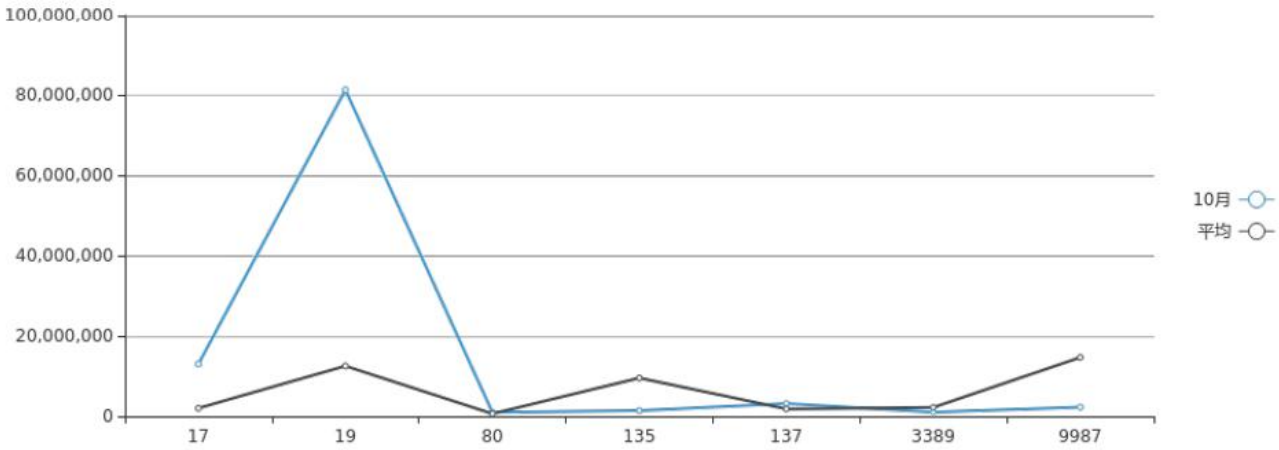

图 6.6 10 月高危端口攻击变化趋势

6.2.3 10 月漏洞利用排行榜

表 6.7 10 月漏洞利用次数分布

利用漏洞	利用次数
vul_EDB_ID_40500_HTTP_IpCameraNvrDvr_AvtechIpCameraNvrDvrDevices	138690
vul_EDB_ID_41471_HTTP_DVRTV_MVPower	93776
vul_EDB_ID_37171_HTTP_router_DLink	78194
redis未授权访问漏洞	29490
vul_CVE_2018_14847_HTTP_router_MikroTik	29135
vul_EDB_ID_40740_HTTP_Router_EirD1000WirelessRouter	24224
vul_CVE_2017_5638_HTTP_struts2_common	14314
vul_EDB_ID_44576_HTTP_router_GPONRouters	10163
vul_EDB_ID_36553_HTTP_JBoss_common	9661
vul_EDB_ID_39596_HTTP_CCTVDVR_MultipleCCTVDVRVendors	9017
vul_EDB_ID_43414_HTTP_router_HuaweiRouterHG532	6102
vul_CVE_2017_7504_HTTP_JBoss_common	5001
vul_CVE_2014_8361_HTTP_SDK_Realtek	3077
vul_CVE_2019_3396_HTTP_Confluence_common	2075
vul_CVE_2017_10271_HTTP_Weblogic_common	1519
vul_EDB_ID_43055_HTTP_router_NetgearDGN1000	869
vul_EDB_ID_31683_HTTP_router_CiscoLinksysEseries	711
vul_CVE_2018_1273_HTTP_Spring_common	709
vul_EDB_ID_28333_HTTP_router_DLink	419
vul_1day0401_HTTP_dvr_LILINDVR	187
vul_CVE_2020_8515_HTTP_Vigor_DrayTek	74

vul_EDB_ID_45135_HTTP_router_ASUSDSLN12E	52
vul_EDB_ID_44760_HTTP_router_DLinkDSL2750B	42
vul_EDB_ID_48225_HTTP_GPONRouter_Netlink	16
vul_EDB_ID_39568_HTTP_ucs_CiscoUCS	10
vul_CVE_2014_6271_HTTP_GNUBash_common	8

6.2.4 全网威胁感知服务

应用服务威胁趋势统计如下。较 9 月相比，10 月出现明显变化，针对低端口 19 的访问占到近 60%，疑似 Chargen DDoS 活动。

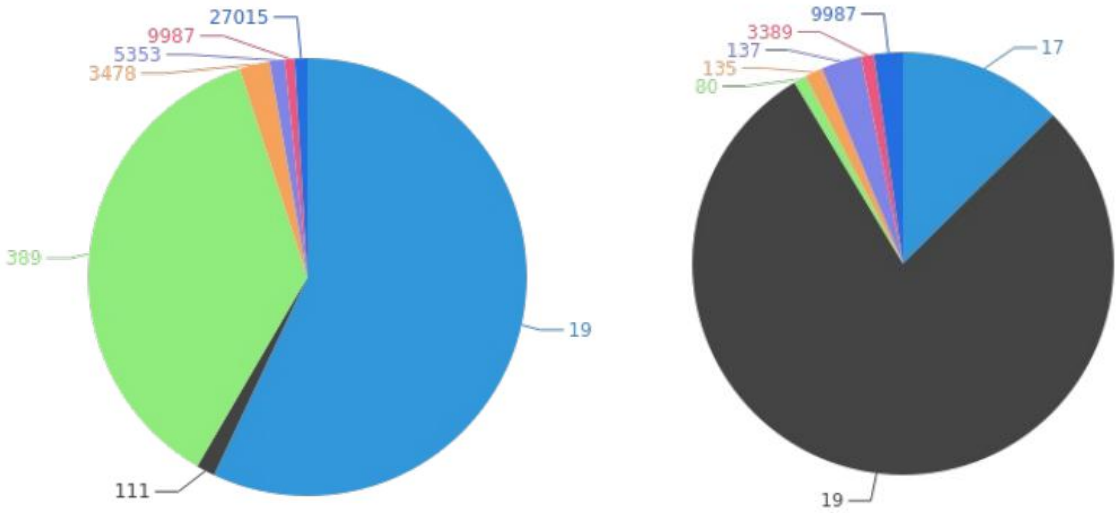

图 6.7 应用服务威胁趋势

6.2.4.2 暴力破解

上月共计捕获 137577917 条数据。其中用户名密码对共计捕获 118492 个。利用 TOP5 如下

表 6.8 用户名密码对利用次数

用户名密码对	利用次数
root_admin	6925644
root_None	1765399
root_1234	1729965
nproc_nproc	517855

root_password	345314

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	6939868
None	通用	过于简单	1782015
1234	通用	过于简单	1753877
nproc	通用	过于简单	517864
password	通用	一般	374062

其中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	70128184
Panama	14716678
Moldova	8350695
Russian Federation	6678294
China	5762604

6.2.4.3 入侵行为

威胁捕获系统中外部攻击者使用的最常用命令

表 6.11 常用命令

命令	入侵工具类型	使用次数
uname -a	外部命令	534585
cat /proc/cpuinfo | grep name | wc -l	外部命令	528450
cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}'	外部命令	527863
free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}'	外部命令	527671
ls -lh $(which ls)	外部命令	527508

表 6.12 攻击次数排名前五攻击 IP

攻击IP	攻击次数
5.188.86.165	5760981
5.188.86.168	5329767
45.227.255.207	5287364
5.188.86.206	4152612
5.188.86.167	4053852

攻击 IP 全球分布情况

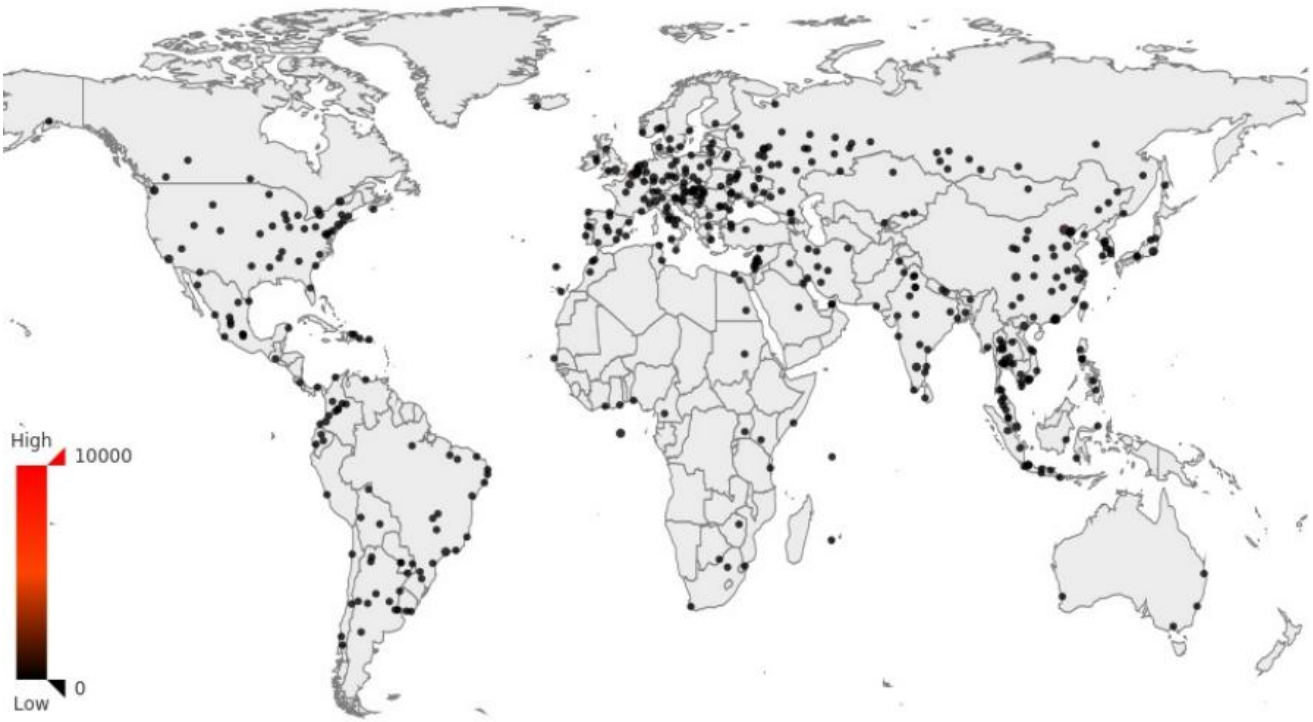

图 6.8 攻击 IP 全球分布

捕获 33869 个样本，涉及 45 个家族，43 个下载地址。恶意样本家族占比：

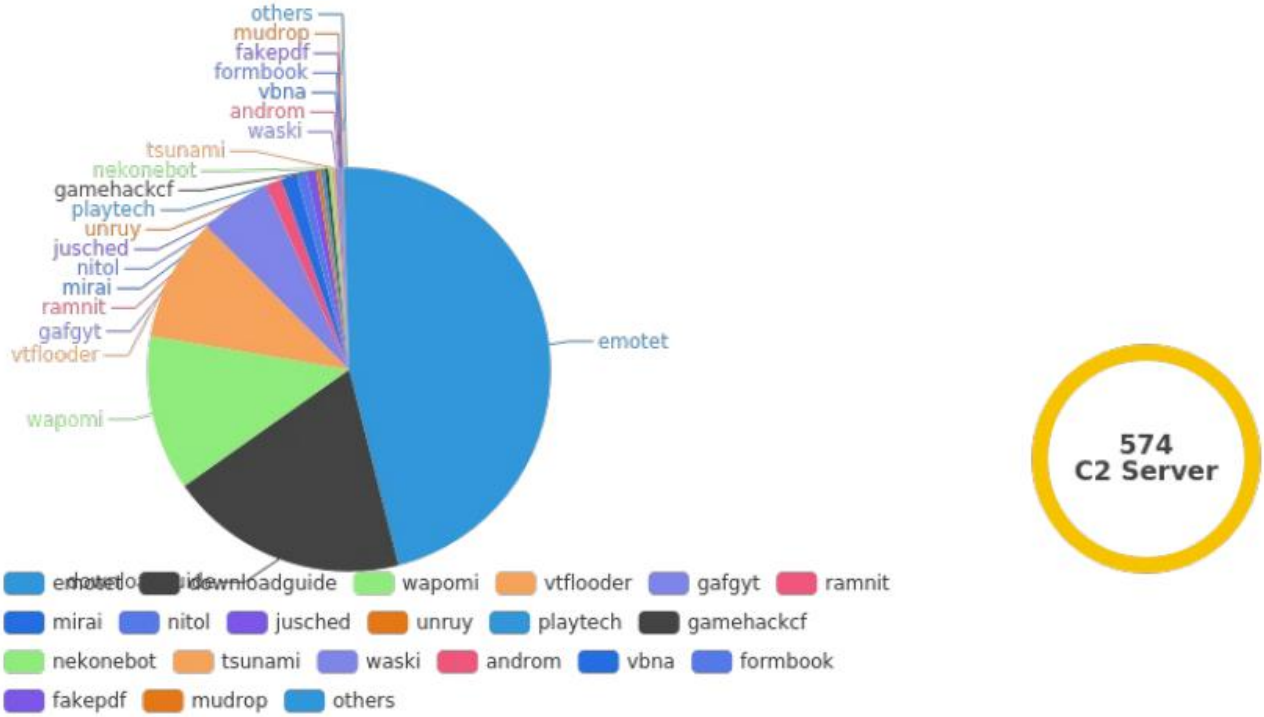

图 6.8 捕获样本涉及家族与 C2 分布

6.2.4.4 邮件攻击

10 月中我们共计捕获 1620 封邮件，其中垃圾邮件 793 封，钓鱼邮件 827 封。共计捕获 2635 个非重复来源 IP。涉及 434114 个目的邮箱。

邮箱	使用次数
spameri@tiscali.it	732
berganza15000@yahoo.com	190
susssinnicc4@yahoo.com	190
susssinnicc3@yahoo.com	153
susssinnicc5@yahoo.com	153

表 6.13 攻击者针对目的邮箱

表 6.14 攻击者针对邮件服务商

邮件服务商	使用次数
gmail.com	120899
yahoo.com	59420
hotmail.com	29813
yahoo.com.tw	18095
aol.com	13881

6.2.4.5 应用程序漏洞利用

10 月共计捕获 1076589 条数据，其中漏洞利用 72835 条。

6.2.4.5.1 数据库服务部分

捕获共计来源 IP 1076589 个。 Mysql1231 个，MS sql 17704 个，redis 1494 个，非关系型数据库 1494 个。 爆破利用用户名密码对 826 个。来源客户端软件 5188 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; SET ANSI_NULL_DFLT_ON ON;	35561

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\';	17047
dbcc addextendedproc(\'xp_cmdshell\',\'xplog70.dll\')	17021
EXEC sp_configure \'show advanced options\', 1;RECONFIGURE;exec SP_CONFIGURE \'xp_cmdshell\', 1;RECONFIGURE;	17011
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\'	16999

6.2.4.5.2 Web 服务部分

10 月共计捕获捕获 14580575 条数据，涉及 74442 个来源 IP。8648 个来源 User Agent。58608 个请求路径，涉及 12 种服务。

6.2.5 DDOS 反射攻击

DDOS 反射攻击，dns 服务上月攻击数据最多。所有服务捕获 5682447 次攻击事件，其中攻击次数最高的攻击事件针对目标为 45.205.9.39，持续时间达到 49.41 小时。

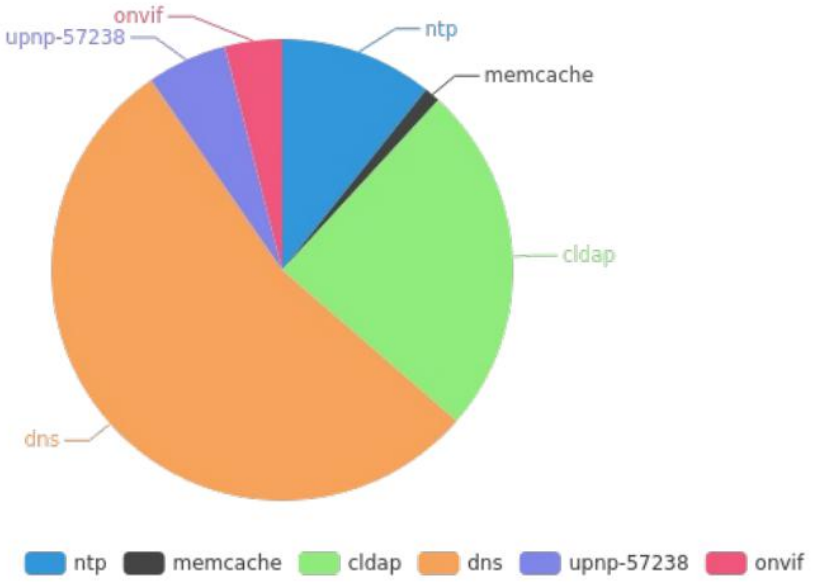

图 6.9 DDOS 反射攻击使用频率

反射攻击对应反射源 IP 数目

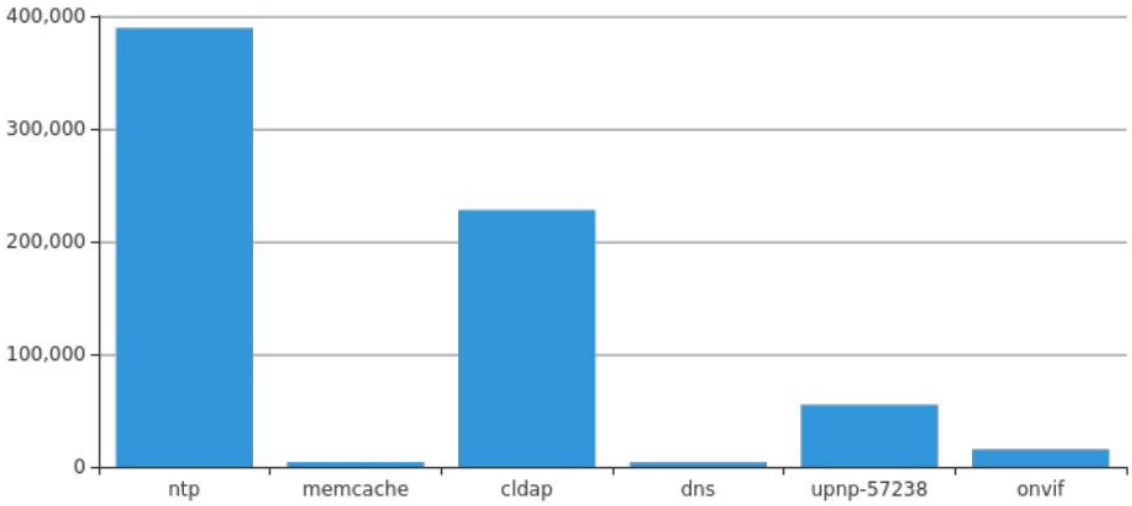

图 6.10 反射攻击对应反射源 IP 数目

6.2.6 物联网服务

IOT 服务共计捕获 1037005 个攻击 Payload，其中涉及了 20 个设备，3 个服务。捕获 74442 个攻击 IP，来源于 183 个国家和地区 IP。其中：

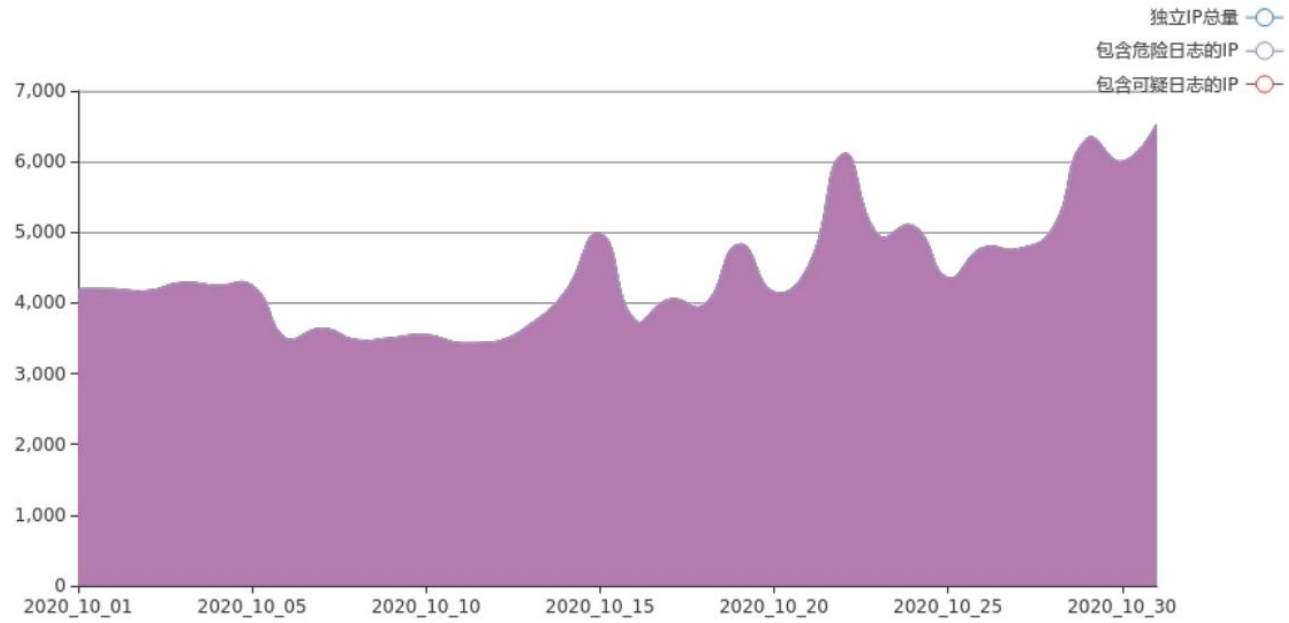

图 6.11 IP 数量趋势

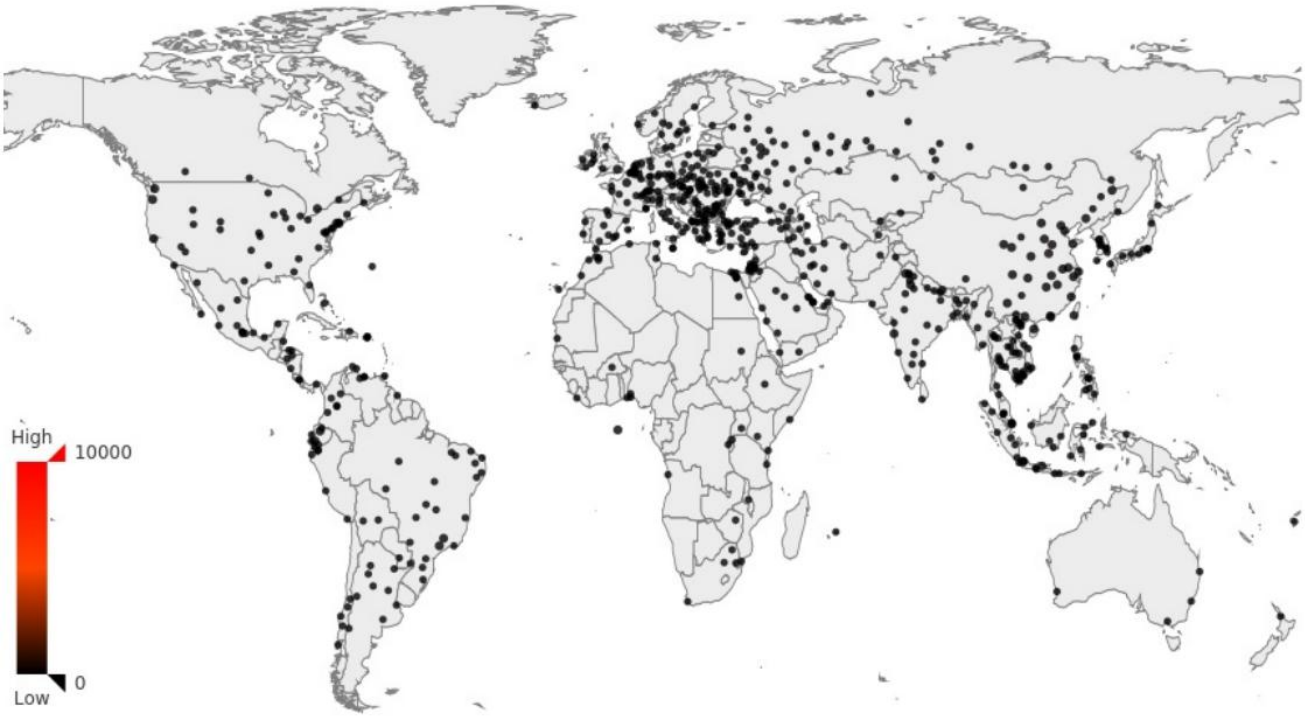

图 6.12 攻击 IP 全球分布情况

6.2.7 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10月份的整体活跃情况呈上升趋势，活跃肉鸡总量增长至17654台，其中在中国的肉鸡最多，达到7290台，占比41%。开放22端口的肉鸡数有13418台，占比接近所有肉鸡的 76%。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。

6.2.7.1 活跃情况

通过对10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 6-11 所示，该挖矿僵尸网络在10月份的整体活跃情况呈上升趋势，在10月26日肉鸡数最高，达到4252台。

图 6.13 挖矿僵尸网络 10 月份活跃情况

6.2.7.2 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 6-12 所示，处于中国的肉鸡数最多，为 7290 台，占比 41%。

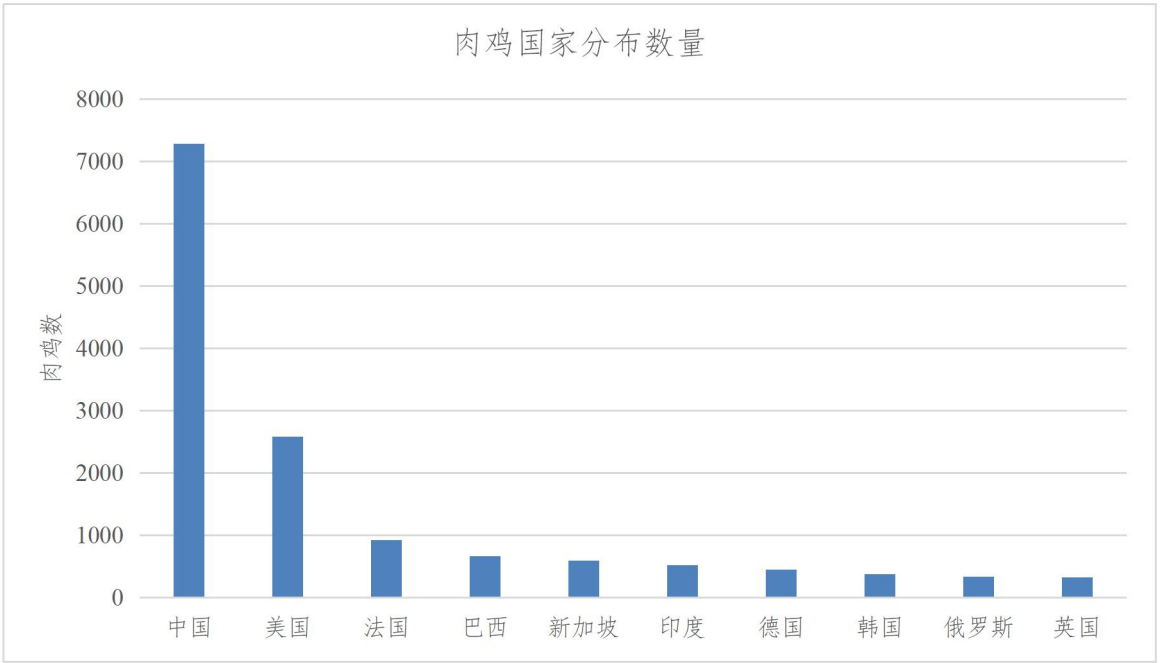

图 6.14 肉鸡国家数量 Top10

6.2.7.3 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、3389、123、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 76%。

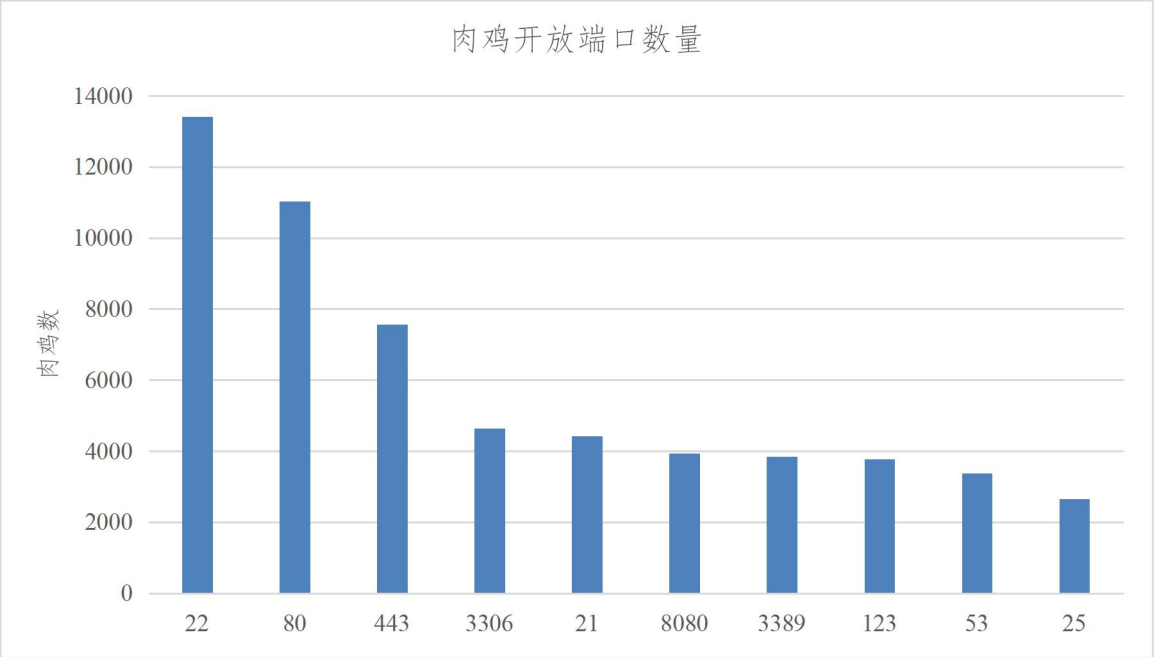

图 6.15 肉鸡开放端口数量 Top10

6.2.7.4 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 6-14 所示，这些物联网设备中 37%为摄像头，34%为路由器。

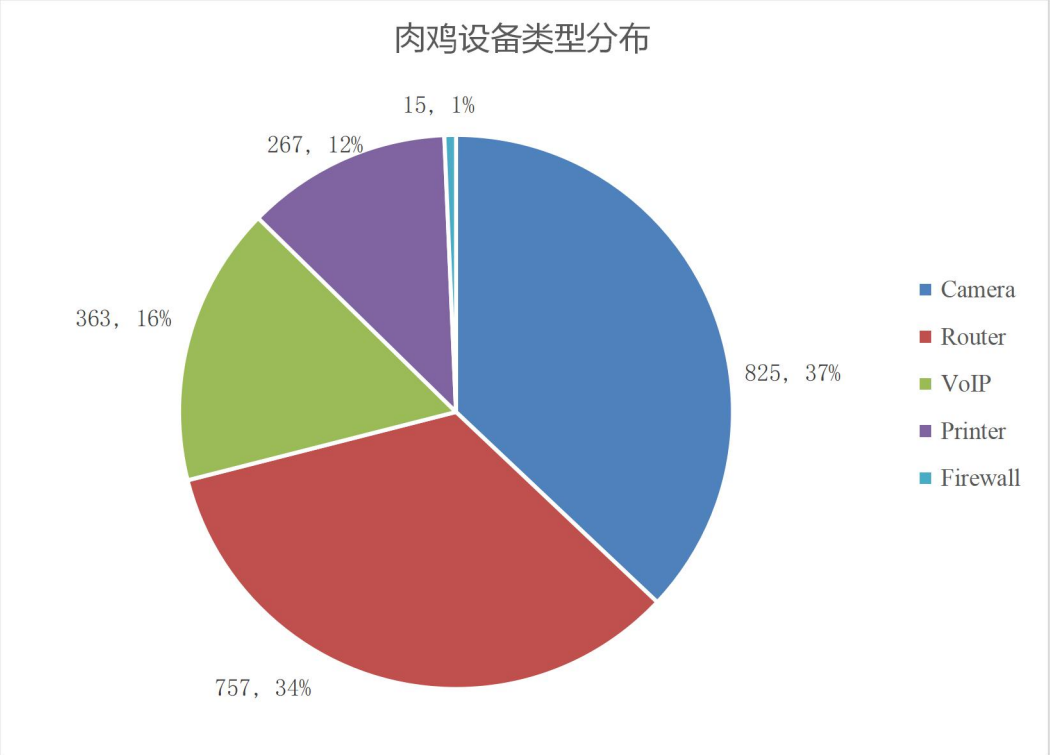

图 6.16 肉鸡设备类型分布

6.2.7.5 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 6-15 所示，该挖矿僵尸网络最常用的弱口令依然是 nproc-nproc。

表 6.15 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

6.2.7.6 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。

NSFOCUS

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