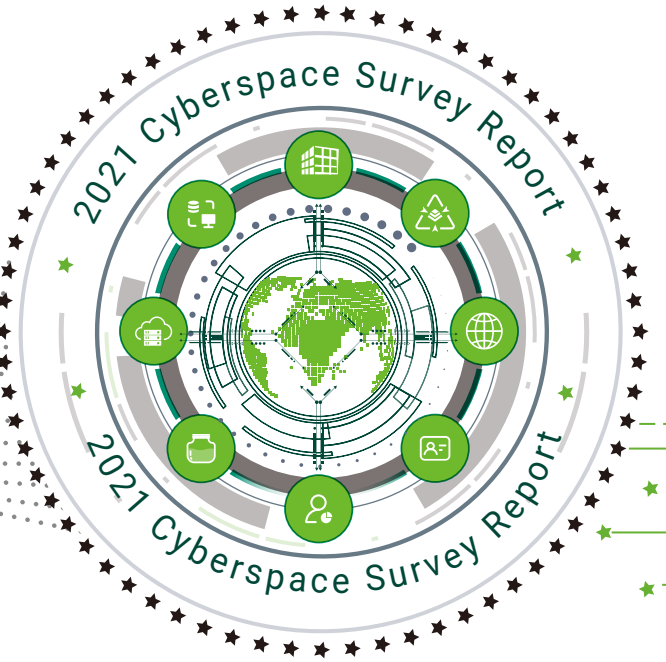
# 2021
# 网络空间测绘年报




NSFOCUS绿盟科技 中国电信 CHINA TELECOM 云堤 SECURITY

## 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 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，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、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

## 中国电信天翼安全科技有限公司

天翼安全科技有限公司（简称“安全公司”）是中国电信集约开展网络安全业务的科技型、平台型专业公司，以研发运营一体化方式，整合全集团云网、安全、数据等优势资源和能力，进行统一运营，为内外部客户提供云网安全、数据安全、信息安全等各类安全产品和服务。公司始终坚持以“传承红色基因，守护安全中国”为使命，致力于成为数字经济时代最可靠的网络安全运营商！

电信安全公司广目及物联网安全系列产品，从资产维度出发，结合运营商独特的网络资源优势，为用户提供精准的网络空间资产测绘台账、规避暴露面风险。其中，广目可以实现 IP、URL、端口、公众号、小程序、APP、网盘、源代码等维度的互联网资产暴露面排查及风险监测；物联网安全相关产品以终端软件、外置硬件等方式保障物联资产的接入可用、传输可信、边界可防、数据可靠、全程可视。广目及物联网安全相关产品已广泛应用于金融、医疗、政府、公安等行业。

---

## 版权声明

NSFOCUS

# CONTENTS

**观点 5** 015

近年云安全事件数量呈现上升趋势，特别是非法利用云资源挖矿和云上数据泄露。随着各个行业上云步伐加快，云化业务及数据变得越来越重要，势必吸引更多的攻击者针对云上目标展开攻击以谋取利益。同时，云上服务租户众多，因而相关漏洞的影响具有规模性。

**观点 6** 023

公有云市场蓬勃发展的同时，其安全风险突出，安全事件层出不穷。主流云厂商，如阿里云、腾讯云、华为云等，其上业务绝大部分的安全风险是因用户错误配置造成的，因而对云上资产测绘十分重要。

**观点 7** 045

相比 2020 年，2021 年 NVD 公布的物联网相关漏洞没有明显的变化趋势，相关漏洞仍具有攻击复杂度低、危害评级高的特点。而知名漏洞利用平台 Exploit-DB 近 5 年收录的漏洞利用总量及物联网相关漏洞利用数量均呈下降趋势，但该平台收录的漏洞以命令执行和信息泄露为主，危害程度高，各方仍应提高警惕。

**观点 8** 051

云上服务、资产数量巨大、类型众多，不同服务及资产暴露的攻击面均不相同，相应的安全成熟度也有较大差异，云上安全态势较为复杂。尽管诸如对象存储服务等公有云服务已经设置了多种提示和警告措施，云上数据泄露事件依然每年都在发生。云原生服务中，容器相关组件（如 Docker）由于落地时间较长，脆弱性暴露情况较少，但其他云原生组件却不容乐观。此外，云上常见物联网协议或服务（如 MQTT）普遍存在未授权访问风险，较为严重。

## ★ 观点 9



新冠疫情爆发以来，远程办公、协同办公的需求大增，大量相关服务暴露在互联网上，很多存在一个或多个安全漏洞。由于这些应用深度参与到企业生产过程中，它们的暴露风险对企业运作、业务运行有重要影响，使用这些应用的企业需要加大重视程度，监控自身业务暴露面和攻击面，非必要不暴露，及时更新修复相关安全漏洞，或积极践行零信任战略。

## ★ 观点 10



工业互联网风险面广、涉及行业多、造成的潜在风险大。安全风险主要来源于管理和技术这两个层面。工业互联网的风险往往关乎民生，生产与制造加工涉及的设备、网络、控制、数据、平台、工业 APP 等都可能成为突破口。

**观察 1** 020

2021 国内暴露的物联网资产数量相较于去年增加了 18 万个，暴露服务数量的前三，依次是摄像头约 104 万个，路由器约 52 万个，VoIP 电话约 2 万个。暴露数量最多的地区是台湾，其次是香港，最后是长三角和珠三角地区。

**观察 2** 029

国内工控资产暴露数量与工业发展水平成正相关，暴露较多的设备主要集中在我国东北老工业基地和东南沿海工业发达地区，并且工控资产会随业务和环境的变化呈现动态变化特征。暴露的工控资产使用最多的工控协议是 Modbus，占总数的 49.2%。这些资产所属的厂商以国际著名公司为主，主要包括摩莎、施耐德电气和西门子等。

**观察 3** 031

2021 年国内暴露的安全设备数量共计 146,459 个，其中，暴露数量最多的是防火墙、VPN 和 WAF，并且以国外厂商的设备居多。这些设备主要集中在我国台湾、香港、北京以及长三角和珠三角等沿海地区。出口类型方面，企业专线和数据中心占比较高，分别占 49.21% 和 43.43%。

**观察 4** 034

2021 年全国暴露在互联网上的常用数据库资产已超过 50 万个，其中，MySQL 暴露数量突破 47 万个，占比高达 92.9%, 并且仍有大量用户在使用已经停止更新的数据库版本，存在巨大的安全隐患。地理分布上，由于越来越多的企业将业务拓展到了国外，选择将服务部署在香港，导致香港成为国内数据库暴露数量最多的地区，接下来是北京和东南沿海经济发达地区。

**观察 5** 038

我们发现全国暴露在互联网上的智慧平台资产已超过 3000 个，包括校园、水利、医疗、交通、养老、物流、车联网、农业相关领域，其中智慧校园平台数量最多。随着数字化转型的稳步推行进，未来将会有更多领域和数量的智慧服务平台出现在互联网上，安全和数字化需要同步建设。

**观察 6** 059

我们针对目前市面上比较流行的云原生服务进行了资产、版本分布梳理以及相应的风险分析，这些服务包括 Docker、Kubernetes API Server、Istio、Kong、Prometheus，其中 Docker 资产暴露数量在国内仅有 179 个，风险分析方面，因暴露 2375 TCP Socket 端口导致的未授权访问漏洞，仍旧是 Docker 服务在互联网上面临的一大风险；Kubernetes API Server 资产数量在国内有近 2 万个，其中因暴露 6443 及 8080 端口导致的未授权访问漏洞资产数约 200 个，这个数量占总体的 1%，此外，暴露资产中约 77% 的资产受 CVE-2021-25741、CVE-2021-25735、CVE-2018-1002105 这三个漏洞的影响；Istio 资产在国内有近 2400 个，其中 443 和 80 端口数量最多；Kong 资产数量在国内暴露约 5900 个，其中命中 CVE-2021-27306 漏洞的资产数约占总资产数的 52%，命中 CVE-2020-11710 漏洞的资产数约占总资产数的 37%；Prometheus 资产在国内暴露约 5200 个，目前受到 CVE-2021-29622 漏洞影响的资产数量为 910 条，约占总量的 17%。

**观察 7** 071

互联网中暴露 32 余万个资产涉及 MQTT 服务，其中 77% 存在未授权访问风险，泄露了物联网设备的敏感信息。涉及 MQTT 协议的开源物联网框架存在明文存储 MQTT 配置、未修改默认密码等安全问题，攻击者可通过 MQTT 协议修改物联网设备数据，甚至可以控制物联网设备。

## 观察 8

081

我们针对目前市面上常见的两款协同办公软件 Confluence 和 Jira，从资产分布，版本分布以及脆弱性几个角度进行了风险分析。其中 Confluence 资产暴露数量 1799 个，Jira 资产暴露数据 4131 个。端口主要分布于 8090，以及 9090，占比均超过 7 成以上，这两个端口都是服务默认配置的端口。已识别出版本的资产中，大部分资产都没有升级到最新版本，存在着被已知脆弱性攻击利用的风险。其中命中 CVE-2021-26084 漏洞资产占比近 Confluence 总资产的 47%。命中 CVE-2021-39128，CVE-2017-17113，CVE-2021-39124，CVE-2021-26070 漏洞的资产均超过 Jira 总资产数的 86% 以上。

## 观察 9

086

根据《Global Market Insights 2020》调查，到 2026 年，全球 VPN 市场预计将同比增长 12%，价值 700 亿美元。由于 VPN 产品在企业网络中的重要性，其安全性常被黑客关注，尤其是销量靠前的产品，一旦曝出相关漏洞，往往评分较高，波及范围较广，例如已经被黑客武器化的数个 VPN 漏洞，Pulse Secure “Connect” VPN(CVE-2019-11510)、Fortinet FortiOS VPN(CVE-2018-13379) 和 Palo Alto Networks “Global Protect” VPN(CVE-2019-1579)，这些漏洞至今仍能对企业安全造成严重危害。

# 执行摘要

2021 年国家“十四五”规划强调，加快数字化发展和建设数字中国，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。这也将极大地推动企业数字化转型的进程。企业通过应用云、大、物、移、智等新技术实现以数据推动业务和管理 [1]。在数字化转型稳步推进的背景下，必定会有越来越多新兴的资产服务出现在互联网上，这些服务的暴露面及脆弱性管理对于网络安全而言仍是重要挑战。2021 年我们将物联网安全年报（2017-2020）更新为网络空间测绘年报 ( 由绿盟科技与中国电信天翼安全科技有限公司联合发布 )，今年的报告将会介绍物联网、公有云、工业控制系统、安全设备、数据库、智慧平台等关键领域资产在互联网上的暴露情况，并对物联网、云原生、工业控制系统等专题的脆弱性情况进行分析。

报告的主要内容如下：

第一章，我们筛选了 2021 较为重大的安全事件进行回顾。其中，从物联网 SDK 的安全事件可以看出，对软硬件结合的结构复杂的产业，厂商在管理好自身安全的同时还需要关注供应链安全。工业控制系统领域是勒索软件青睐对象，多数受害企业无法承受系统或生产停止的代价，攻击者有更大概率拿到赎金。“新冠”疫情大爆发以来，远程办公成为很多企业主要的工作方式之一，因此企业 VPN 产品相关漏洞受到攻击者的关注。此外，暴露在互联网上的数据库服务存在很大的安全风险，尤其是未授权访问以及弱口令问题，可能造成敏感信息泄露，甚至严重影响企业的正常业务。公有云安全方面，非法利用云资源挖矿和云上数据泄露占据主要地位。随着各个行业上云步伐的加快，云化业务及数据变得越来越重要，这势必吸引更多的攻击者针对云上目标展开攻击，以谋取利益。同时，云上服务面向多租户，相关漏洞的影响因而具有规模性。总之，2021 年网络攻击趋势仍在持续攀升中，勒索软件、错误配置、数据泄露以及供应链是需要关注的重点问题。

第二章，我们对互联网上关键领域资产暴露情况进行分析。随着 IoT、5G、云原生等技术发展，未来将会有更多的新兴资产和服务出现。业务资产暴露也会给企业组织带来了安全风险。摸清企业网络空间资产暴露情况，洞察网络风险是建立网络安全防御体系的第一步，也是最重要的一步。因此，第二章对网络空间关键领域资产进行了分析，介绍了国内的物联网、公有云、数据库、工业控制系统、安全设备、智慧平台以及蜜罐资产的暴露情况，以便快速感知安全风险，掌握安全态势，辅助威胁研判分析。

第三章，我们主要对网络空间关键领域脆弱性进行专题分析。首先，我们分析了物联网相关的年度漏洞披露情况：2021 年 NVD 公布的物联网相关漏洞相比 2020 没有明显的变化趋势，相关漏洞仍具有攻击复杂度低、危害评级高的特点。接着，我们对云计算相关风险及脆弱性进行了分析：首先是以 AWS S3 为代表的公有云对象存储服务，近年来数据泄露事件高发，我们将对这一现象及背后原因进行探索；其次是由 Docker、Kubernetes 等服务组成的云原生生态，我们将对互联网暴露的云原生生态组件进行梳理和分析，给出暴露情况和脆弱性态势；我们还以 MQTT 协议为例，对云上使用较多的物联网协议进行脆弱性分析，揭露云上 MQTT 服务的安全问题。另外，新冠疫情爆发以来，远程办公、协同办公的需求大幅增加，相关的团队协作工具、远程连接工具因此被大量部署。这些软件的安全性对企业运作、业务运行有重要影响。因此，我们还对以 Confluence、Jira 为代表的协同办公应用及用于远程连接的 VPN 进行测绘分析，探讨它们可能存在的风险。在本章的最后，我们介绍了工业互联网领漏洞趋势和风险分析，其中包括设备、网络、控制、数据、平台、工业 APP 等方面。

随着《关键信息基础设施安全保护条例》、《网络安全审查办法》和《网络数据安全管理条例》等法律法规政策的相继出台、实施，合规性要求将对网络空间资产安全态势起到正向促进作用。同时，对网络空间资产的暴露面和脆弱面进行持续测绘，起到长效监控作用，从而引起企业重视，未雨绸缪，防微杜渐，帮助企业收敛暴露面、修补安全漏洞。

# 01

# 2021 年重大网络空间安全事件回顾

## 1.1 CISA 公布物联网设备严重漏洞 8300 万台智能设备受影响

**观点 1：从 2021 年曝光的 ThroughTek Kalay SDK 和 H 厂商的摄像头未授权这两起安全事件，不难看出物联网安全问题有着“低级漏洞、高级风险”以及影响范围广的特点。目前物联网的软硬件产业结构也相对复杂，物联网厂商管理好自身安全的同时还需要关注供应链安全。**

### 1.1.1 事件回顾

2021 年 8 月 19 日，美国联邦网络安全和基础设施安全局（CISA）公布了一个物联网设备的严重漏洞，该漏洞出现在一个软件开发工具包（ThroughTek Kalay SDK）中。与这个 SDK 有关的设备有 8300 万台，这些设备每个月都产生超十亿次的网络连接。此漏洞不仅允许攻击者能够看到安全网络摄像头等设备拍摄的实时画面，可以随意连接到这些设备，检索音频和视频，并且在用户不知情的情况下控制这些设备，更改相机角度或者重启设备等操作 [2]。

### 1.1.2 原理简述

该事件利用的漏洞编号为 CVE-2021-28372。有此漏洞的 ThroughTek Kalay SDK，提供了一个可插拔的系统，用于将智能设备与其相应的移动应用程序连接起来。Kalay 平台为智能设备和其相应的应用程序提供代理，可以处理身份验证和发送数据，该漏洞存在于设备与其移动应用程序之间的注册程序中。这种设备与应用程序之间的连接对应关系，取决于每个设备的 UID，是 Kalay 协议交互唯一的标识符。如图 1.1 为攻击者利用漏洞的攻击过程，具体解释如下：

攻击者利用制造商的其他漏洞获取设备的 UID 并发起请求。

使用设备的 UID 和 Kalay 协议，攻击者可以重新注册设备的 UID，并以此挟持获取设备拥有者的账号与密码。

掌握了 UID 和密码的攻击者可以远程控制这些设备，再利用漏洞 CVE-2021-28372，攻击者可以实时观看网络设备拍摄的画面，还可以在设备上安装恶意固件。

因为攻击者获取了 UID 和密码，然后通过 Kalay 远程管理设备进行攻击行为，因此设备的拥有者无法通过重置设备或者删除数据来阻止入侵行为。

受到影响的设备可能会受到不当的访问控制，此漏洞可允许攻击者访问敏感信息或者执行远程代码。

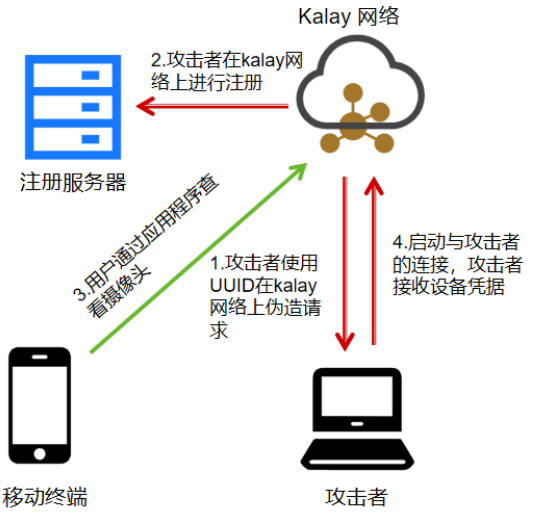



图 1.1　攻击者入侵原理示意图

### 1.1.3　事件分析

可以说，物联网已经应用到我们生活的方方面面，智能设备在给我们的生活带来极大便利的同时，安全问题也一定不能忽视，因为这些设备携带的都是用户的高度隐私信息，一个很小的漏洞可能就会对用户造成不可挽回的损失，所以在安全领域没有任何一个漏洞是小漏洞。提高这些设备的安全性需要设备厂商和各方的共同努力，作为使用者也需提高安全意识，此外，物联网的软硬件产业结构也相对复杂，物联网厂商管理好自身安全的同时还需要关注供应链安全。

## 1.2　H 厂商远程代码执行漏洞

### 1.2.1　事件回顾

2021 年 6 月，研究人员在 H 厂商 IP 摄像机设备固件中发现了一个未认证的远程代码执行漏洞，漏洞编号为 CVE-2021-36260。2021 年 8 月，H 厂商开始发布补丁和相关受影响的设备和固件。

### 1.2.2　原理简述

该漏洞的利用很简单，不需要用户的交互，攻击者只需要访问 HTTP 或 HTTPS 服务器的 80 或者 443 端口就可利用该漏洞，而且也不需要登录时的用户名，密码或者其他任何操作，摄像头本身也不会检测到任何登录信息，在获取设备信息（如图 1.2 和 1.3 所示）之后，添

加一个 root 账户，并进行登录。一旦攻击成功，攻击者可以读取和更改用户数据，而且还可以访问和攻击内部网络。

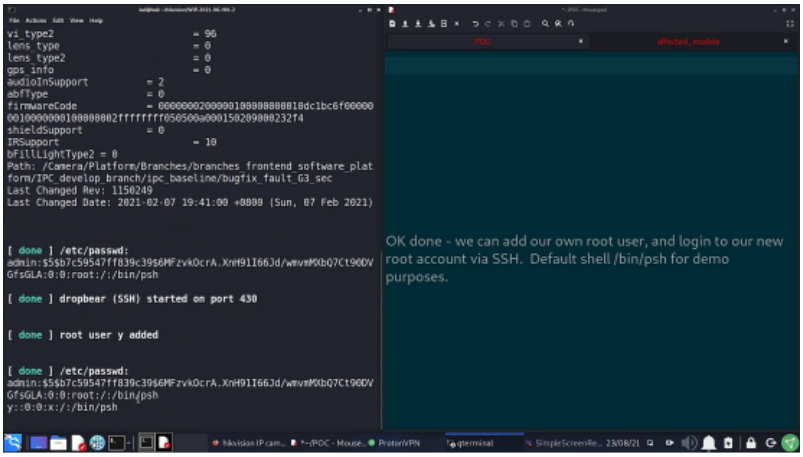



图 1.2　获取设备信息，添加自己的账户

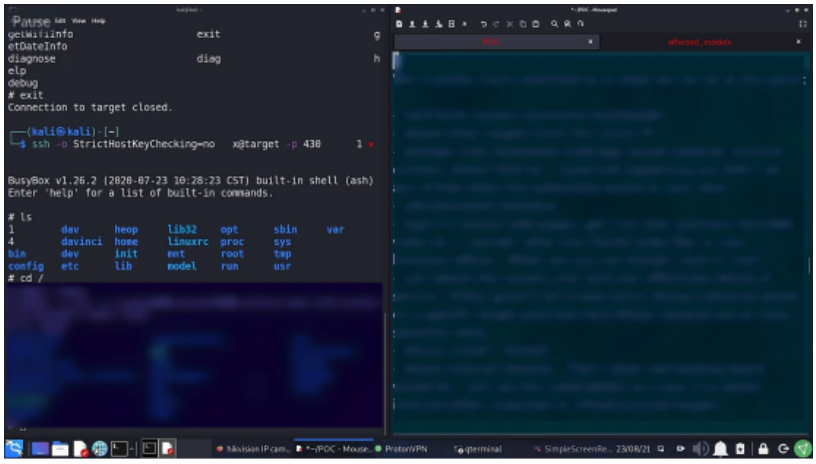



图 1.3　使用 /bin/sh shell 添加一个 root 账并登录

## 1.2.3　事件分析

当下，摄像头已经成为了家庭、企业单位必不可少的监控设备，这些设备的数据大多数情况下都是隐私数据，一旦被入侵或者非法利用后果不堪设想，轻则被用于肉鸡对其他互联网资产进行 DDoS 攻击，重则隐私数据泄露，被攻击者利用从而发起社会工程学攻击，造成财产损失。作为用户来讲，可以从以下两个方面提高设备的安全性：一个是关闭不必要的端口，减小攻击面，另一个是及时打厂商发布的补丁，尽量避免影响 [3]。

# 1.3 DarkSide 勒索软件攻击美国燃料管道商 Colonial Pipeline 公司

**观点 2：2021 年超过一半的工业控制系统领域攻击事件都与勒索软件有关，其中 REvil 和 DarkSide 家族占比最大。通常勒索团伙受惩风险很低，并且能获得高额的赎金，因为多数受害者无法承受停工停产的严重后果。**

## 1.3.1 事件回顾

2021 年 5 月 7 日，美国最大的燃油管道运营商 Colonial Pipeline 因受到勒索软件攻击被迫关闭了其美国东部沿海各州供油的关键燃油网络。此次勒索攻击使美国三个区域受到了断油的影响，共涉及 17 个州。5 月 9 日，联邦汽车运输安全管理局（FMCSA）发布区域紧急状态声明，放宽了 17 个州和哥伦比亚特区对携带汽油、柴油、喷气燃料和其他精炼石油产品运输司机的服务时间规定，允许他们额外或更灵活的工作时间，以减轻管道中断导致有关燃料短缺的影响 [4]。

此次勒索攻击事件是一个名为 DarkSide 的网络犯罪团伙发起的，该团伙入侵了 Colonial 的网络，并窃取了近 100GB 的数据，以此威胁如果不在一周内支付赎金会将其泄漏到互联网。该次事件的攻击者 DarkSide 是一个最早活跃于 2020 年下半年的新兴黑客组织，自 2020 年 8 月在地下黑客论坛出现以来，DarkSide 使用一种与组织同名的勒索软件开展大规模的攻击活动。同时在 2021 年 5 月 10 日，DarkSide 在暗网主页上发表声明，称其是单纯利益驱动组织，不需要将他们关联到政府组织或挖掘其他活动。

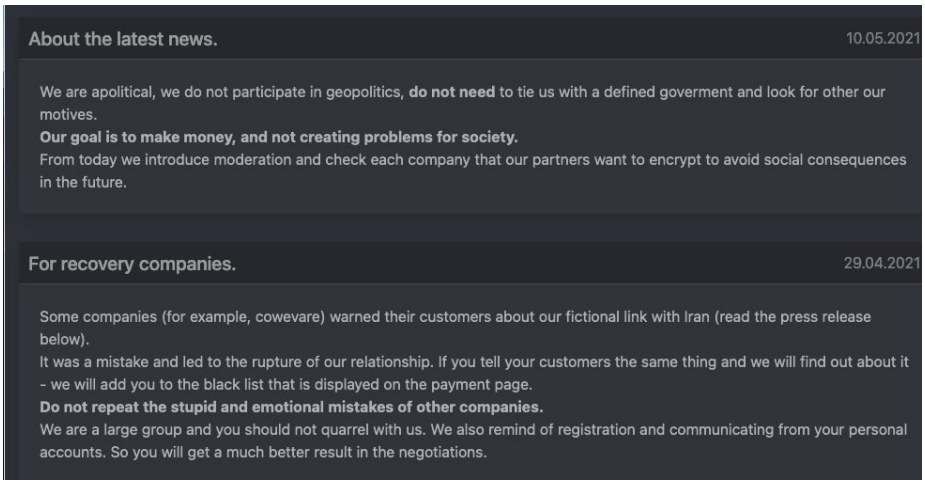



图 1.4 DarkSide 在暗网主页发表声明

### 1.3.2 原理简述

DarkSide 使用了一种雇佣式的恶意程序分发策略，因此与其相关的攻击事件中，各自的入侵手段表现了一定的差异性。在已发现的部分事件中，DarkSide 的使用者会通过已泄露账户等信息登录暴露在外的 VDI 设备，进而借助该设备进行局域网扫描并控制更多设备，最终投递 DarkSide 勒索软件本体。

DarkSide 本体程序运行后，会利用 COM 接口进行提权，随后进行删除卷影数据、清空回收站、窃取本地信息、加密文件、显示勒索内容等勒索软件的常规操作。DarkSide 在文件加密过程中使用 Salsa20 算法加密文件，但是使用 RtlRandomEx 生成的自定义矩阵进行加密，最后使用 RSA-1024 加密生成的矩阵，并将加密后的矩阵添加到加密后文件的末尾。

### 1.3.3 事件分析

虽然 DarkSide 也会对勒索软件主体进行维护和更新，但该组织显然将更多的精力投入到了对高价值目标的威胁上。DarkSide 会使用骚扰电话等方式对目标企业进行直接威胁，持续对其施加压力。

随着勒索软件事件越来越多样，企业应加强员工安全意识培训，加强主机账户口令复杂度及修改周期管理，并尽量避免出现通用或规律口令的情况；修改系统管理员默认用户名，避免使用 admin、administrator、test 等常见用户名；尽量避免危险端口对外开放，利用 IPS、防火墙等设备对危险端口（445、139、3389 等）的服务进行防护。

## 1.4 数百家工业组织在 SolarWinds 事件中遭受 Sunburst 恶意软件攻击

### 1.4.1 事件回顾

SolarWinds 软件在 2020 年 3-6 月期间发布的版本受到供应链攻击的影响，攻击者在这段期间发布的 2019.4-2020.2.1 版本中植入了恶意的后门应用程序，受此次供应链攻击影响的客户包括政府、国防、网络公司和关键基础设施提供商等，约有 18000 个用户下载了包含后门的恶意软件。

安全研究人员对使用后门版本的 SolarWinds 并成为受害者的工业组织进行研究，他们使用 Sunburst 恶意软件域名生成算法生成的 DNS 名称获得的可用内部域名，其中已解码和可

归属的域名将近 2000 个，按照行业划分，工业组织占比最高（32.4%），覆盖工业领域中制造业、运输与物流、建筑业、矿业和能源等（如图 1.5 所示），工业组织的地理分布也几乎覆盖整个世界 [5]。

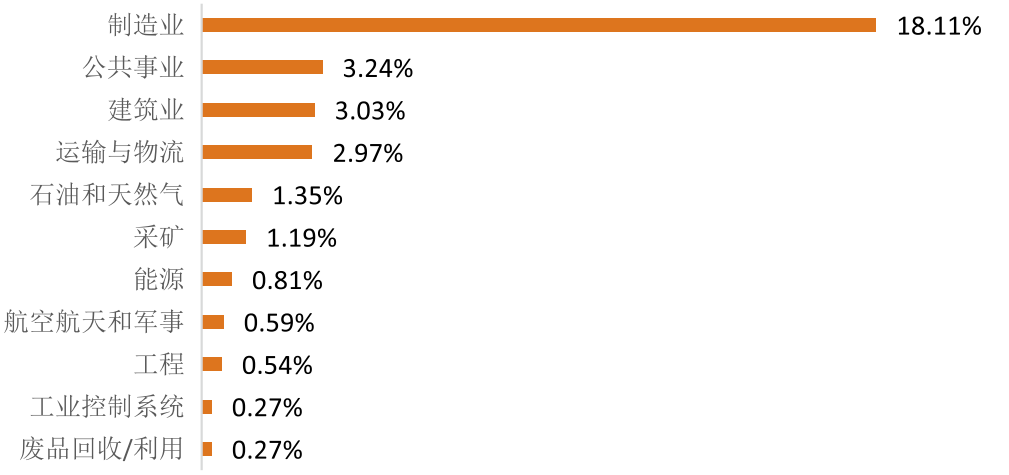



图 1.5　受影响的工业组织占比情况

## 1.4.2　原理简述

植入恶意后门的应用程序利用 SolarWinds 的数字证书绕过验证，并在休眠两周左右后会和第三方进行通信，并且根据返回的指令执行操作，包括传输文件，执行文件，重启系统等。这些通信会伪装成 Orion Improvement Program（OIP）协议并将结果隐藏在众多合法的插件配置文件中，从而达成隐藏自身的目的。

## 1.4.3　事件分析

SolarWinds 供应链攻击事件表明网络安全是各行业的迫切需求，并不是在受到攻击之后才被需要，因为攻击者可能破坏网络并长期隐藏网络访问和入侵活动；攻击活动的受害者不仅是大型组织，也包括中小型组织，尤其是关键基础设施和影响力行业；各类组织几乎都不存在真正的气隙隔离系统 [6]。

针对工业领域，建议实施基于网络的零信任和隔离保护，对于关键资产进行持续信号监控，防止物理资产受到网络攻击，如果发现安装了带有后门的恶意软件，应及时启动应急响应程

序，隔离受攻击的资产，检测网络日志、系统日志等排查非法账户身份验证，查找可疑进程活动并查看历史命令行数据。

## 1.5 Q 厂商终端安全管理系统未授权访问漏洞

**观点 3：从 2021 年曝出的针对安全设备的攻击事件中可以看出，漏洞利用是发起这些攻击的主要手段之一。而这些漏洞一旦被攻击者利用，用户可能会面临隐私泄露、被勒索、网站篡改、网络瘫痪等严重后果。安全设备通常被认为安全级别非常高，但从近两年公开的安全事件可见，其风险不容忽视。**

### 1.5.1 事件回顾

2021 年 4 月，研究人员在 Q 厂商终端安全管理系统发现一个未授权访问漏洞，漏洞编号 CNVD-2021-34259，攻击者可利用漏洞获取敏感信息。2021 年 6 月，Q 厂商发布了终端安全管理系统未授权访问漏洞安全公告及相关补丁信息，修复了此漏洞 [7]。

### 1.5.2 原理简述

未授权访问指权限认证地址或授权页面存在缺陷，导致无权限用户可以直接访问，从而引起的网站页面、数据库等敏感信息泄露。

终端安全管理系统未授权访问漏洞利用方法很简单，查看漏洞站点，在 API 接口访问数据库 /api/dbstat/gettablessize，返回数据表相关信息。


图 1.6 查看漏洞站点


图 1.7　查看数据库表相关信息

### 1.5.3　事件分析

未授权访问漏洞不仅造成无权限用户可访问操作、敏感数据泄露，还存在被勒索软件利用进行植入、勒索攻击的风险。

## 1.6　APT 组织正在利用 Fortinet VPN 安全漏洞进行攻击

### 1.6.1　事件回顾

2021 年 4 月，FBI 和 CISA（美国网络安全与基础设施安全局）发出告警，声称有 APT 组织正在利用 Fortinet FortiOS 网络安全操作系统中的已知漏洞，影响 Fortinet SSL VPN 产品 [8]。

告警中称，攻击者正在扫描 4443 端口、8443 端口和 10443 端口上的设备，找寻发现未修补的 Fortinet 安全设备，也正在利用 CVE-2018-13379、CVE-2019-5591 和 CVE-2020-12812 进行攻击，通过扫描这些漏洞，以获取政府、商业网站等的访问权限，以及利用关键漏洞进行 DDoS 攻击、勒索软件攻击、SQL 注入攻击、钓鱼攻击以及网站篡改等活动 [9]。

### 1.6.2　原理简述

CVE-2018-13379 是 Fortinet FortiOS SSL VPN 中的路径遍历漏洞，其中 SSL VPN 网站允许未经身份验证的攻击者通过特定的 HTTP 请求下载系统文件；

CVE-2019-5591 是 FortiOS 中默认配置漏洞，可允许在同一个子网中的未经认证的攻击者通过模拟 LDAP 服务器来获取敏感信息；

CVE-2020-12812 是 Fortinet SSL VPN 中的身份验证漏洞，用户可通过更改用户名中的大小写，允许用户登录成功，而不提示第二因素认证（FortiToken）。

攻击者一旦成功利用漏洞，就会进行横向移动，对目标网络进行侦察，获取关键基础设施部门网络的访问权限，进一步进行数据渗透、数据加密攻击。

### 1.6.3 事件分析

自 2019 年新冠疫情爆发，远程工作成为主要的工作方式之一，对 Fortinet 等 SSL VPN 需求的增加，使得 SSL VPN 漏洞受到攻击者关注。

安全研究人员提示各组织应立即修复 CVE-2018-13379、CVE-2019-5591 和 CVE-2020-1281 漏洞；定期离线备份数据；实施网络分段；需管理员凭证才能安装软件；尽可能使用多因素身份验证；禁用远程桌面协议端口并监控远程访问；审核用户账户权限，以最低权限配置访问控制；安装并定期更新杀毒软件；注重培训员工网络与信息安全意识。

## 1.7 云服务提供厂商 DreamHost 泄露 8 亿用户数据

**观点 4：数据库服务暴露在互联网上存在很大的安全风险，尤其是无身份验证、弱口令以及存在未授权访问漏洞的数据库，管理员往往忽视对数据库进行权限验证，造成敏感信息泄露，甚至严重影响到组织的业务。**

### 1.7.1 事件回顾

2021 年 4 月 16 日，研究人员发现一个来自云服务提供商 DreamHost 的无密码保护的数据库，其中包含超过 8 亿记录，暴露的数据为 WordPress 账号用户名、显示名称、电子邮件和与其他账户关联信息以及监控日志文件，暴露的日志文件是从 2018 年 3 月至今的记录，每个文件都包含托管和安装在 DreamHost 服务器上的 WordPress 账户和相关信息。

### 1.7.2 原理简述

DreamHost 此次泄露的数据总大小 86.15GB，DreamPress 管理员和用户信息，其中包括 WordPress 登录站点、用户名、用户角色 / 权限、主机 IP、时间戳、版本信息和允许公共访问配置。

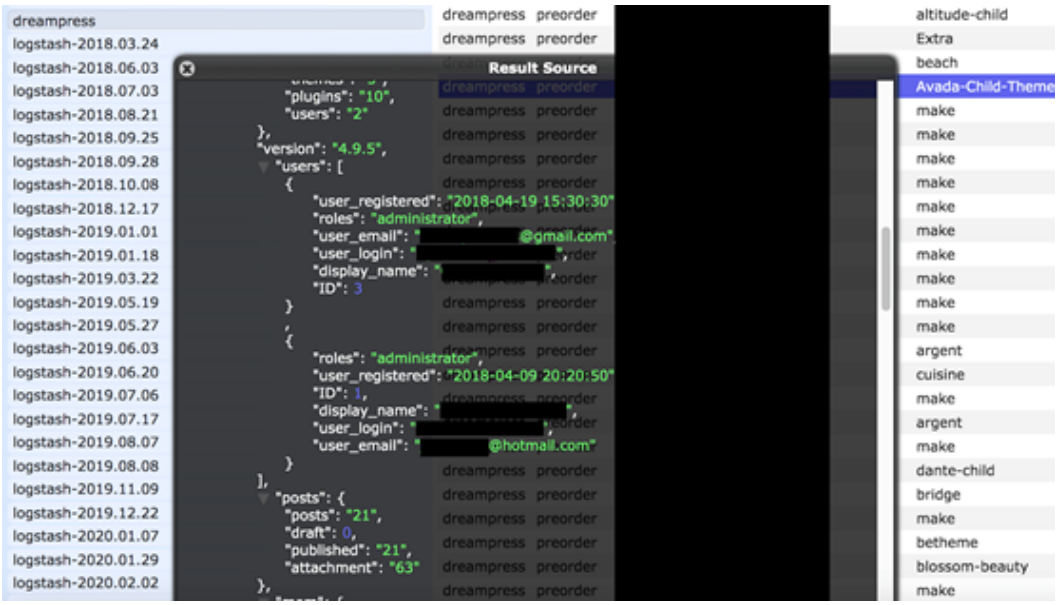



图 1.8　DreamHost 泄露数据

在 WordPress 账户关联的邮件地址中发现包括 .gov 和 .edu 在内的各种扩展域名，包括美国地质调查局、美国总务管理局、伦敦市政府等，这些邮件地址被暴露可能使攻击者发起针对性的钓鱼攻击或其他社会工程诈骗 [10]。

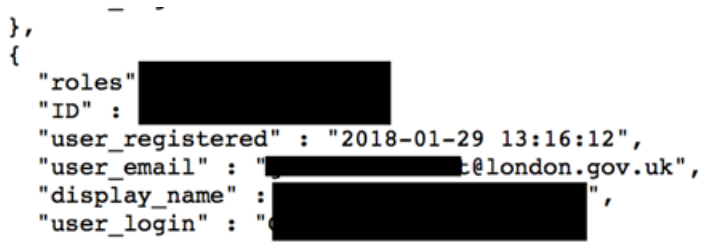



图 1.9　泄露 london.gov.uk 相关邮箱数据

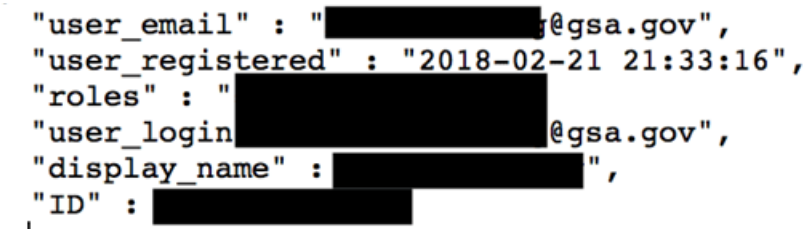



图 1.10　泄露 gsa.gov 相关邮箱数据

### 1.7.3 事件分析

目前尚不清楚 DreamHost 数据库公开暴露了多长时间，还有谁可以访问这些敏感信息、DreamPress 用户是否收到了数据泄露的通知。目前大多数网络犯罪是为了经济利益，社会工程学成为网络攻击中重要的方法之一，网络犯罪分子可能利用数据泄露通过社会工程攻击瞄准客户或尝试访问账户。

## 1.8 数据分析公司 Polecat 近 30TB 业务数据泄露，因 Elasticsearch 服务器未受身份验证

### 1.8.1 事件回顾

英国数据分析公司 Polecat 的一个 Elasticsearch 服务器因未做任何身份验证和加密保护措施，导致近 30T 数据遭泄露。该服务器存储的业务记录可追溯到 2007 年，数据包括员工用户名和密码、超过 65 亿条推文、从各种网站和博客收到的超过 10 亿条帖子以及 50 亿社交平台记录。

### 1.8.2 原理简述

关于 Polecat 泄露数据的信息被通报的第二天，便有威胁行为者成功访问到未受保护的 Elasticsearch 服务器，同时用自动化脚本扫描开放的数据库，找到后直接删除，经过两轮此类攻击，Elasticsearch 服务器仅剩 4TB 数据。不久之后，威胁行为者留下一张赎金票据，要求 Polecat 支付 0.04 比特币（约 550 美金）作为赎金以赎回数据 [11]。值得注意的是，这类勒索攻击通常是自动执行的，并且针对各类开放数据库。

### 1.8.3 事件分析

Polecat 泄露事件暴露出一系列受到保护的用户名和哈希密码，可以看出 Polecat 具有正常的数据保护和安全意识，因此数据泄露很可能是人为错误导致。人为错误也长期是数据库泄露的主要原因之一。

同时，近几年数据库勒索事件频频发生，建议企业和用户关闭不必要的高危端口；实行最小授权原则，使用户的权限最小化，对关键敏感数据进行标记；开启登录审计日志，审计和管控登录行为；每台服务器设置唯一口令，且提高复杂程度，要求用数字、特殊字符以及大小写字母的组合；做好数据备份。

## 1.9 TeamTNT 组织在 2021 年多次针对云计算目标进行攻击

**观点 5：近年云安全事件数量呈现上升趋势，特别是非法利用云资源挖矿和云上数据泄露。随着各个行业上云步伐加快，云化业务及数据变得越来越重要，势必吸引更多的攻击者针对云上目标展开攻击以谋取利益。同时，云上服务租户众多，因而相关漏洞的影响具有规模性。**

### 1.9.1 事件回顾

据相关报道[12]，TeamTNT 组织至少从 2011 年就开始活跃。他们攻击手法多样，近两年来，也多采用云及云原生相关攻击手段实施攻击。据不完全统计，TeamTNT 组织在 2021 年进行了一系列的云相关攻击活动：

- 2021 年 2 月，TeamTNT 被曝投放针对 Kubernetes 集群的非法加密挖矿软件[13]。
- 2021 年 5 月，TeamTNT 被曝针对 Kubernetes 进行蠕虫式攻击，至少五万个 IP 被感染[14]。
- 2021 年 9 月，TeamTNT 被曝发起了针对多个操作系统和应用的攻击行动“Chimaera”[15]。
- 2021 年 10 月，TeamTNT 被曝在 Docker Hub 上投放恶意镜像[16]。
- 2021 年 11 月，TeamTNT 被曝通过存在未授权访问漏洞的 Docker 控制服务器执行挖矿等恶意操作[17]。

### 1.9.2 原理简述

前述由 TeamTNT 发起的攻击事件多使用了针对脆弱云或云原生环境的攻击技术。这些技术主要包括：

1. 利用存在未授权访问漏洞的 Docker。攻击者能够利用存在未授权访问漏洞的 Docker 在目标服务器上部署恶意容器、获得宿主机 root 权限。
2. 利用存在未授权访问漏洞的 Kubelet。攻击者能够利用存在未授权访问漏洞的 Kubelet 在目标服务器上部署恶意容器、获得宿主机 root 权限。
3. 窃取云访问凭证。攻击者在攻入主机后，通过窃取云访问凭证，能够进一步控制更多云资源。

4. 窃取 Docker 凭证。攻击者在攻入主机后，通过窃取 Docker 凭证，能够向目标镜像仓库（默认为 Docker Hub）中上传恶意镜像。
5. 窃取 Kubernetes 服务凭证。攻击者在攻入主机后，通过窃取 Kubernetes 服务凭证，能够获得更高的 Kubernetes 集群权限。
6. 在 Docker Hub 上投放传恶意镜像。攻击者通过在 Docker Hub 部署恶意镜像，诱使用户或在攻入主机后拉取镜像进行挖矿等非法活动。
7. 部署特权容器。攻击者通过部署特权容器，实现容器逃逸。

### 1.9.3 事件分析

随着容器及云原生技术逐渐成熟，云原生化会成为常态。在初始渗透阶段，TeamTNT 并未利用高级的攻击手段，仅仅是目标主机的错误配置，就可以导致上万台主机失陷。上述一次次的事件必须引起我们的重视，加强云和云原生环境的基本配置核查、加固，避免给攻击者可乘之机。

## 1.10 ChaosDB：Azure 数据库服务错误影响数千公司

### 1.10.1 事件回顾

Azure Cosmos DB 是微软从 2017 年开始提供的非关系型数据库服务，不少世界 500 强公司都有使用。2021 年 8 月，来自 Wiz 的安全研究人员发现 Cosmos DB 数据库存在一系列严重的安全漏洞，可能导致大规模商业数据泄露，他们将这个系列的漏洞命名为“ChaosDB”，并于 2021 年 8 月 26 日披露了相关信息。

### 1.10.2 原理简述

从 2019 年起，微软向 Cosmos DB 中增加了 Jupyter Notebook 的功能[18]，用户可以直接在 Notebook 中可视化查询他们的数据，并创建自定义视图。从 2021 年 2 月起，所有 Cosmos DB 实例的 Jupyter Notebook 功能自动开启。

然而，研究人员发现，Jupyter Notebook 存在错误配置，进而引发了一系列安全问题，攻击者能够利用这些安全问题控制大量数据库。

漏洞点一共有三处[19]，下面我们一一说明。

1. 内置 Jupyter Notebook 存在权限提升漏洞。正常情况下，用户在 Jupyter 终端或默认的 Python3 Notebook 中以非特权身份 cosmosuser 执行命令。然而，如果用户执行的是 C# 语言编写的代码，相关代码却是以 root 权限执行。研究人员利用这个漏洞，向 /etc/passwd 中添加了一个新的 root 用户，然后在 Jupter 终端中执行 su 命令切换到该用户，实现了权限提升。提升权限后，研究人员开始探索 Jupyter Notebook 所在容器。
2. 不受限制的网络访问。在获得 root 权限后，研究人员在容器内执行 IPtables 命令，看到以下地址和地址段被禁止访问：由于已经具有 root 权限，研究人员删除了这些禁止规则，恢复了对这些地址的访问。

   a. 169.254.169.254，对应 IMDS 元数据服务 [20]。

   b. 10.0.0.0/16 子网。

   c. 168.63.129.16。
3. 获取到不属于自己的证书。研究人员发现，168.63.129.16 是微软的 WireServer[21]。借助该服务，研究人员获取并破解了若干微软证书和私钥。在这些信息的帮助下，研究人员成功访问了微软的 Service Fabric 服务，从而接触到了大量用户数据。

### 1.10.3 事件分析

本次事件的研究团队最终获得了四万美元的奖励，这也反映了相关漏洞的严重性。随着云计算的发展，越来越多的重要数据会被存储在云端；与此同时，越来越多的国家和地区开始从法律、政策上重视数据安全。这意味着，云服务商必须做好云上数据安全工作，丝毫不能大意。本次事件看似复杂，一开始的突破口在 Jupyter Notebook 对 C# 的权限错配上。由此可见，云上配置管理是云安全的重中之重。

## 1.11 小结

本章我们选取了 2021 出现较为重大的安全事件进行回顾。

从物联网 SDK 的安全事件可以看出，对类似物联网产业这种软硬件产业结构复杂的产业，厂商不仅管理好自身安全的同时还需要关注供应链安全。

工业控制系统领域主要是勒索软件青睐对象，因为对于多数受害企业来说，他们无法承受系统或生产线停止服务的代价，所以攻击者会有更大概率拿到赎金。

近年来越来越多的安全设备漏洞被披露出来，其中远程命令执行、SQL 注入和未授权访问较为常见。“新冠”疫情大爆发以来，远程办公成为很多企业主要的工作方式之一，因此企业 VPN 产品相关漏洞受到攻击者的关注。

公司业务系统的数据库直接暴露在互联网上存在很大的安全风险，尤其是存在未授权访问以及弱口令的数据库，造成敏感信息泄露，甚至严重影响到企业的正常业务。

公有云安全事件方面事，非法利用云资源挖矿和云上数据泄露占据主要地位。随着各个行业上云步伐的加快，云化业务及数据变得越来越重要，这势必吸引更多的攻击者针对云上目标展开攻击，以谋取利益。同时，云上服务面向多租户，相关漏洞的影响因而具有规模性。

总之，2021 年网络攻击趋势仍在持续攀升中，勒索软件、错误配置、数据泄露以及供应链是仍是安全需要关注的重点问题。摸清企业网络空间资产暴露情况，洞察网络风险是建立网络安全防御体系的第一步，也是最重要的一步。因此，第二章将会对网络空间关键领域暴露资产情况进行分析。

# 02

# 网络空间重点领域暴露资产分析

通过对 2021 年物联网、数据库、工业控制系统、公有云、安全设备领域的重点安全事件进行梳理和解读。不难发现，目前对互联网上资产的发起攻击趋势持续攀升，所以本章将介绍上述关键领域以及智慧平台、蜜罐资产的国内全网的暴露情况。

## 2.1 网络空间资产测绘简介

测绘最早来源于地理空间地图的绘制，主要研究测定和推算地面几何位置、地球形状及地球重力场，据此测量地球表面自然物体和人工设施的几何分布，编制各种比例尺地图的理论和技术的学科（维基百科）。网络空间测绘和地理信息测绘的技术路线类似，“测”是对网络空间内一切可获得数据的测量机制的建立，偏向于实现扫描和探测的工程问题；“绘”则是根据对网络空间测量数据分析和关联，包括地址地理、域名、风险脆弱性等信息的关联，目的是绘制出多维的网络空间地图，倾向于对数据的分析和研究。

相比于地理信息测绘，网络空间测绘存在一些特殊之处。首先从数据维度来讲，地理空间的测绘数据是三维的（经度、纬度、海拔）且连续，而网络空间中将 IP 地址转化为长整形后，地址数据是一维的，并且每个点都是独立存在并不连续。此外，二者还有一个最大的不同之处就是变化频率，地理信息测绘数据一般变化较慢，而且因为是连续的，所以变化趋势相对好预测，比如珠穆朗玛峰的每年都会以一定的高度在增长，但正常情况下一般不会突然升高或下降几十米。而网络空间测绘数据则不同，绝大多数的 IP 地址处于变化是常态。比如存活情况、开放服务、ASN、地理信息、地址所有者等等维度都是处在动态变化中，并且因为网络地址都是离散分布的个体，变化趋势也就更难预测。所以本报告提及的网络空间资产测绘结果，都是基于实时扫描一轮的数据展开的分析，以保证资产测绘的准确性。

## 2.2 物联网资产暴露情况分析

**观察 1：2021 国内暴露的物联网资产数量相较于去年增加了 18 万个，暴露服务数量的前三，依次是摄像头约 104 万个，路由器约 52 万个，VoIP 电话约 2 万个。暴露数量最多的地区是台湾，其次是香港，最后是长三角和珠三角地区。**

2016 年 Mirai 蠕虫大规模爆发感染大量的物联网设备，弱终端联网设备的安全得到了广泛的重视。从 2017 年开始，我们持续对互联网上的物联网资产暴露资产进行梳理，我们从第一章的安全事件，可以看出大量互联网上暴露的物联网设备和服务，目前仍是攻击者利用的目标。在物联网攻击事件频发的背景下，持续的对这些资产进行分析和梳理是有必要的。

### 2.2.1 设备类型分布情况

为保证资产存活的准确性，我们对 2021 年 11 月的国内全网段测绘一个轮次作为今年的资产暴露情况的展示数据（下同）。经过统计发现，国内有 201 万个物联网资产服务暴露在互联网上，相较于 2020 物联网安全年报 [22] 统计的数量共增加了 18 万，增长一方面是因为物联网资产暴露本身的增长，另一方面也与我们对设备指纹扩充有关。具体的暴露设备类型分布情况如图 2.1 所示。其中，摄像头、路由器、VoIP 电话数量分别位列前三，这个排序也和往年一致。

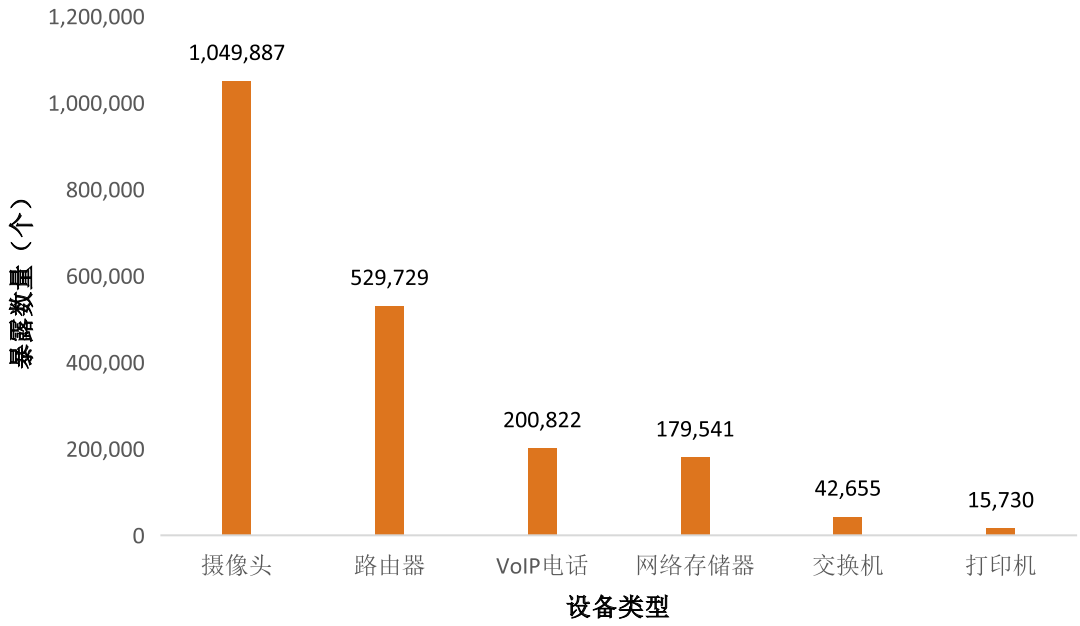



图 2.1 国内暴露物联网资产类型分布情况

### 2.2.2 厂商分布情况

暴露物联网资产的厂商分布情况如图 2.2 所示，从图可知，暴露数量最多的厂商是 H1，第二位是华硕，主要暴露的资产是其生产的路由器相关产品，第三位是思科，主要暴露资产是 VoIP 电话和路由器相关产品。

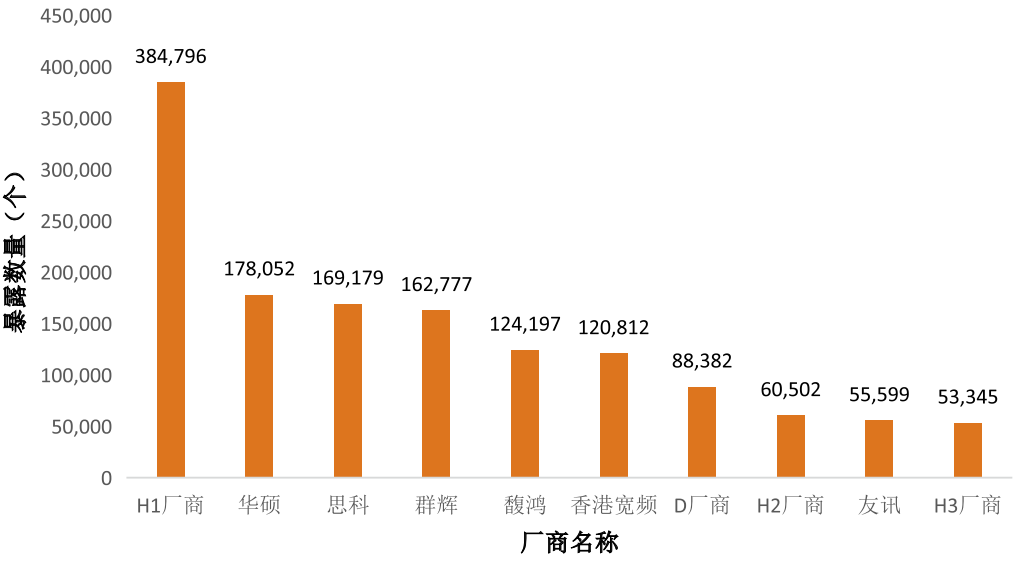



图 2.2　国内暴露物联网资产厂商分布情况

### 2.2.3　端口分布情况

国内暴露物联网资产端口分布情况如下图 2.3 所示，从图中可知，暴露最多的是视频流 RTSP 协议的默认端口 554、其次 Web 主流端口 443 和 80、第三是语音流协议 SIP 默认端口 5060。

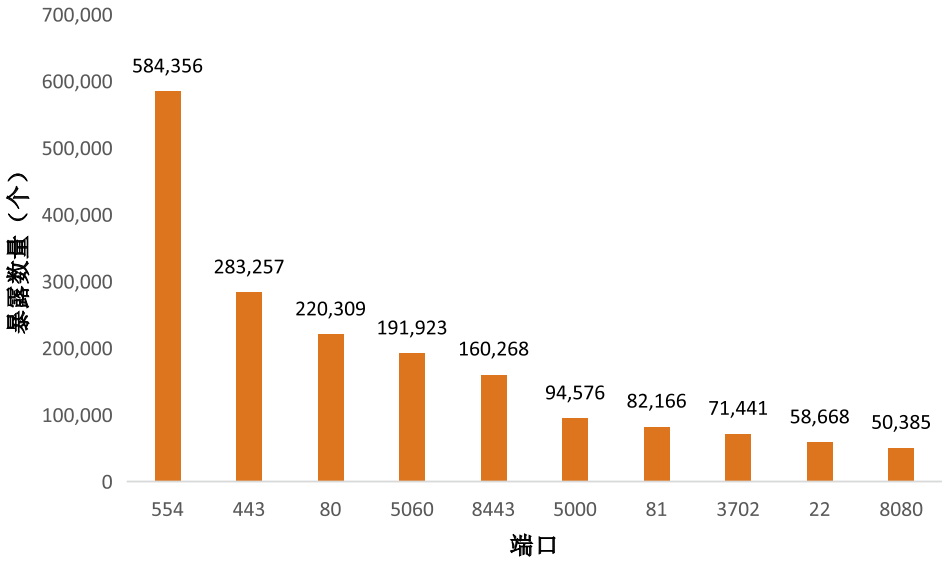



图 2.3　国内暴露物联网资产端口分布情况

### 2.2.4 地理位置分布情况

物联网资产的地域分布情况如图 2.4 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，接下来分布数量比较集中是长三角和珠三角地区的沿海城市，可见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。

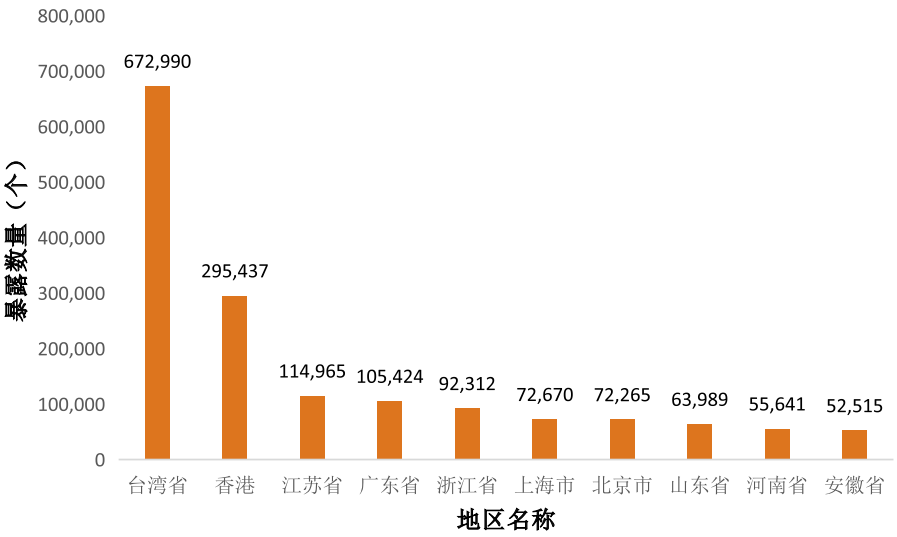



图 2.4 国内暴露物联网资产地区分布情况

### 2.2.5 小结

本节介绍国内物联网资产的暴露情况，物联网是数字化时代的重要基础设施，随着万物互联的智能场景的落地，暴露趋势将会持续增加，需要提高对物联网安全建设的关注度，所以未来我们将继续梳理物联网资产的暴露情况。

## 2.3 公有云资产暴露情况分析

**观点 6：公有云市场蓬勃发展的同时，其安全风险突出，安全事件层出不穷。主流云厂商，如阿里云、腾讯云、华为云等，其上业务绝大部分的安全风险是因用户错误配置造成的，因而对云上资产测绘十分重要。**

相比传统的本地硬件资源，云服务具备为计算、存储、网络等资源按需定制的优势，可以大大节省业务的维护和扩容成本。由于云服务的种种优势，政企领域已经逐步将业务系统

从本地向云端迁移。而相比私有云，公有云具备成本低、免维护、扩展性好等优势，因此公有云市场也在近几年内走向繁荣。到 2021 年上半年，国内公有云服务 (IaaS+PaaS+SaaS) 市场规模已达到 123.1 亿美元；在市场份额 (IaaS+PaaS) 上，阿里云最多，达到 37.9%；腾讯云其次，占比 11.2%；华为云第三，达到 10.9%[23]。

与此同时，云上安全风险也一直存在，安全事件层出不穷。风险态势评估的前提是资产梳理，对云上资产服务的宏观把握十分重要。因此，本节将对阿里云、腾讯云、华为云三大厂商在国内的活跃主机、开放端口以及对外服务进行测绘分析。

### 2.3.1 阿里云资产统计分析

目前，阿里云国内的活跃主机主要集中在浙江、北京、广东、上海等地。阿里云活跃主机地理位置分布如图 2.5 所示。

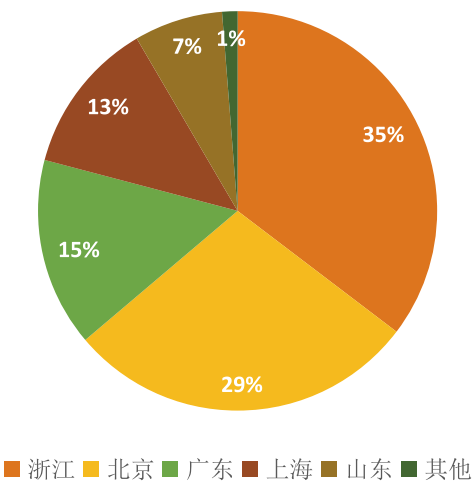



图 2.5 国内阿里云主机地理分布情况

阿里巴巴总部位于浙江杭州，阿里云的活跃主机数量在浙江也是最多的。此外，阿里云主机大部分活跃在北上广等超一线城市。另外，2018 年阿里巴巴开始在山东建立全国最大的阿里云创新中心[24]，因此山东也活跃着一定数量的阿里云主机。

阿里云开放数量前十的端口分别为 80 端口、22 端口、443 端口、21 端口、3306 端口、3389 端口、8888 端口、8080 端口、6379 端口以及 8081 端口。阿里云前十开放端口统计信息如图 2.6 所示。

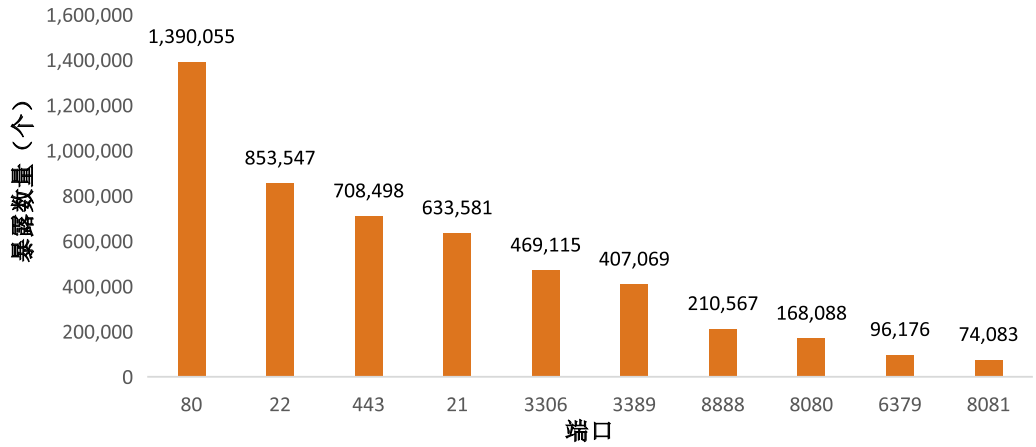



图 2.6　阿里云开放数量前十的端口情况

具体地，我们对约 246 万个阿里云服务进行了统计分析。其中数量最多的为 Nginx 服务，其次分别为 Apache 服务、OpenSSH 服务、Tengine 服务、IIS 服务器以及阿里云的 OSS 弹性存储服务。此外 Jetty 服务器、Kong 服务网关、Elasticsearch 存储服务等也以一定数量运行在阿里云上。阿里云服务统计信息如图 2.7 所示。

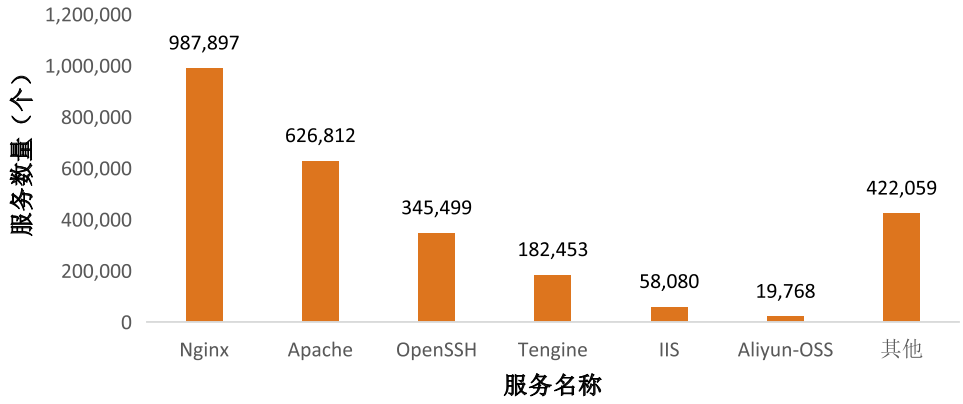



图 2.7　阿里云开放数量前六的服务情况

### 2.3.2　腾讯云资产统计分析

目前，腾讯云国内的活跃主机主要集中在上海、北京、广东、四川等地。腾讯云活跃主机地理位置分布如图 2.8 所示。

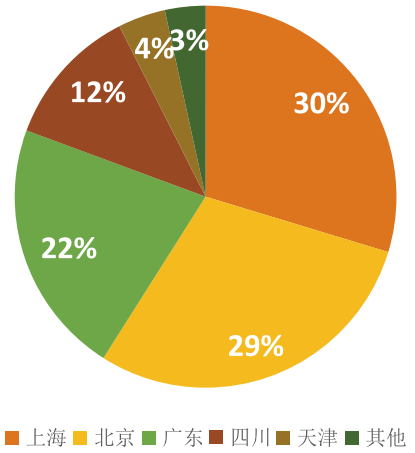



图 2.8　国内腾讯云主机地理分布情况

除北上广等一线城市外，腾讯云活跃主机大部分分布在四川省。主要原因是腾讯云为我国西南区域提供云服务的数据中心设置在四川成都 [25]。

腾讯云开放数量前十的端口分别为 3389 端口、135 端口、139 端口、80 端口、22 端口、443 端口、3306 端口、25 端口、110 端口以及 8888 端口。腾讯云前十开放端口统计信息如图 2.9 所示。

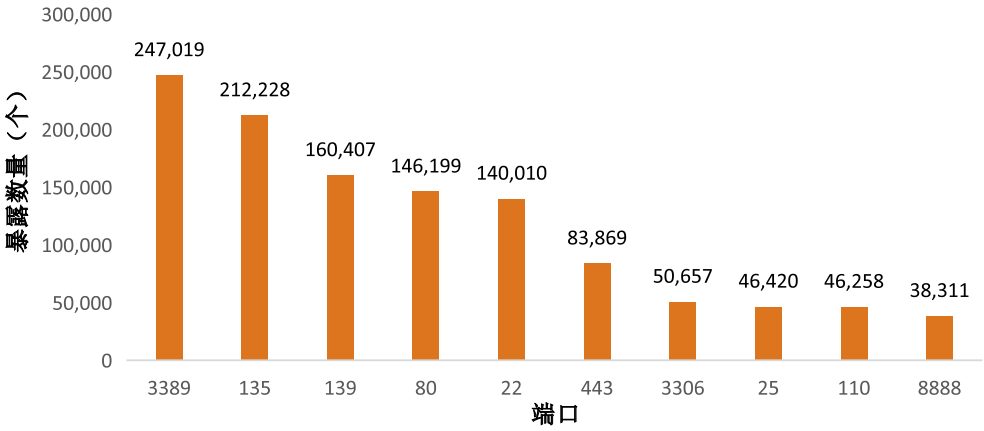



图 2.9　腾讯云开放数量前十的端口情况

我们对约 33 万个腾讯云服务进行了统计分析。其中数量最多的为 Nginx 服务，其次分别为 Apache 服务、OpenSSH 服务、IAS(Immediate Access Storage) 存储服务、Openresty 服务器以及 Tengine 服务。此外 Tornado 服务器、腾讯云对象存储 (TencentCOS)、rainloop 邮件服务器等也以一定数量运行在腾讯云上。腾讯云服务统计信息如图 2.10 所示。

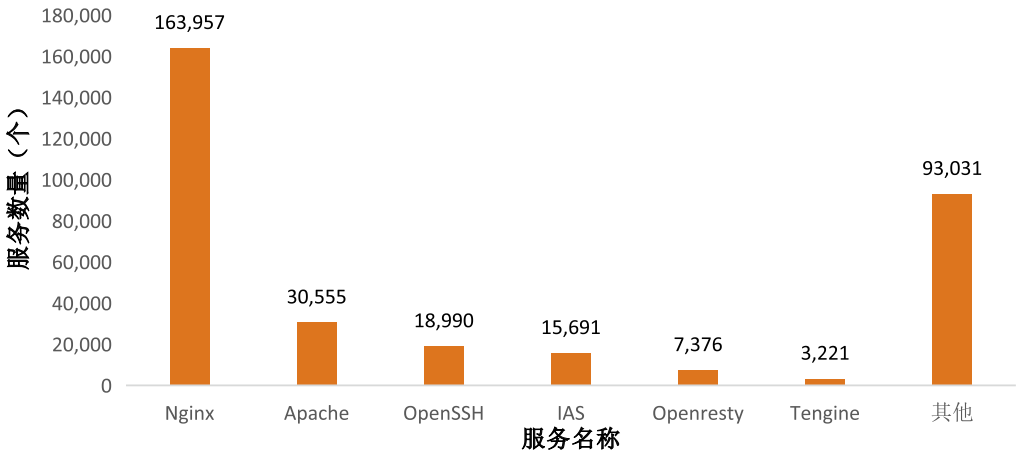



图 2.10　腾讯云开放数量前六的服务情况

### 2.3.3　华为云资产统计分析

目前，华为云国内的活跃主机主要集中在北京、广东、上海、贵州等地。华为云活跃主机地理位置分布如图 2.11 所示。

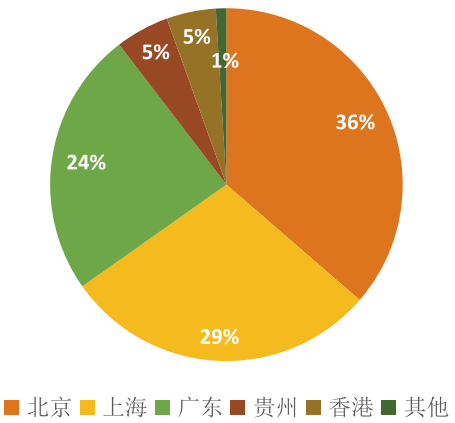



图 2.11　华为云主机地理信息分布图

华为云活跃主机除北上广外主要集中在贵州和香港。2021 年九月华为在贵州新成立的数据中心 [26] 在测绘数据中是所有体现的。而对于香港，华为云则是为扩展海外业务的企业提供了云服务节点 [27]。

华为云开放数量前十的端口分别为 22 端口、80 端口、443 端口、3389 端口、3306 端口、8080 端口、8888 端口、135 端口、21 端口以及 25 端口。华为云前十开放端口统计信息如图 2.12 所示。

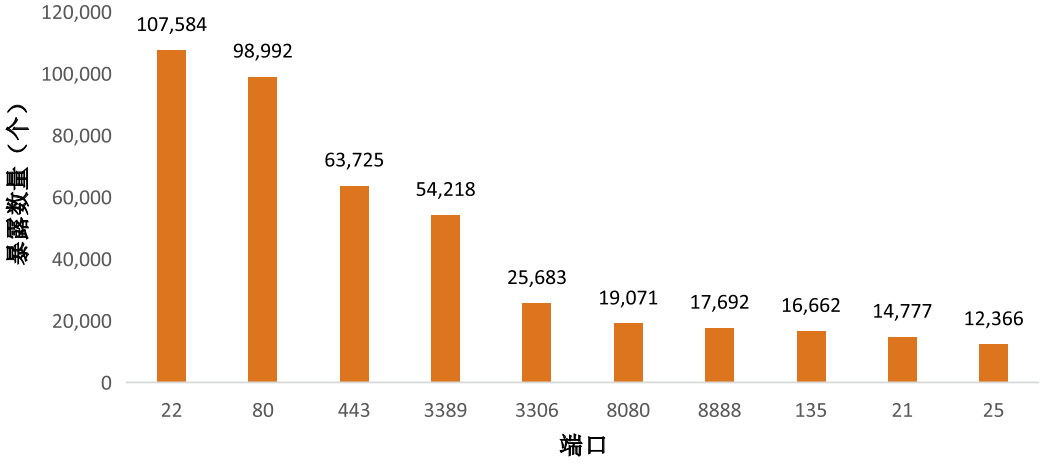



图 2.12　华为云开放数量前十的端口情况

我们对约 23 万个华为云服务进行了统计分析。其中数量最多的为 Nginx 服务，其次分别为 Apache 服务、云防火墙 CloudWAF、OpenSSH 服务、负载均衡器 ELB(Elastic Load Balance) 以及 IIS 服务器。此外 OBS 存储服务、华为云接入管理系统 FusionAccess 和微服务管理工具 Istio 等也以一定数量运行在华为云上。华为云服务统计信息如图 2.13 所示。

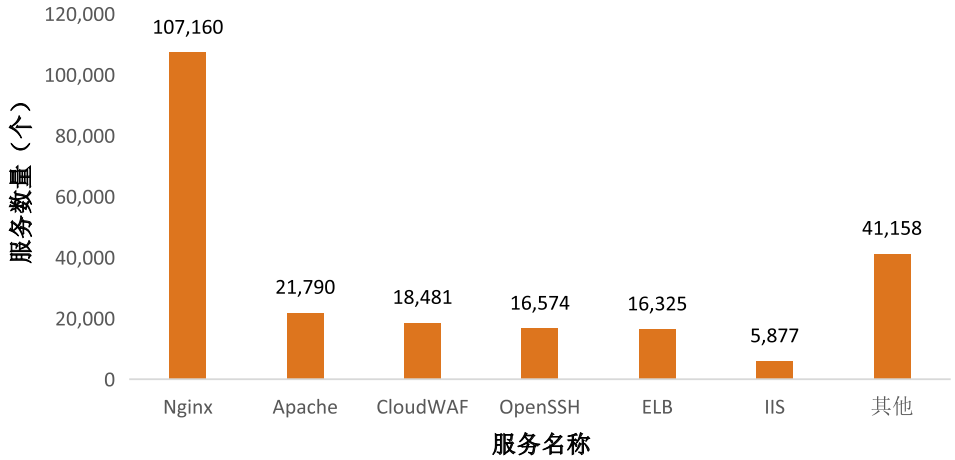



图 2.13　华为云开放数量前六的服务情况

## 2.3.4　小结

从主机活跃维度来看，目前国内阿里云存活主机最多、腾讯云次之、华为云第三。主机活跃的数量与云厂商所占市场份额有着较强的关联关系。

从端口开放维度来看，三大云厂商开放较多的端口为 80、22、443、3389、135、3306、8888 等端口。由此推测公有云上运行的大部分是基于 HTTP/HTTPS 协议的 Web 服务以及远程连接服务。

最后，服务维度的统计信息一定程度上佐证我们从端口信息中获得的推论。三大公有云厂商上运行最多的为基于 Nginx、Apache、Tengine、IIS 等框架的 Web 服务以及用于远程连接的 OpenSSH 服务。此外，阿里云的 OSS 对象存储服务、腾讯云的 COS 对象存储服务、华为云的 OBS 存储桶也以一定数量运行在公有云网络空间中。与阿里云、腾讯云不同的是，华为云上除了包含大量租户部署的 Web 服务外，还部署了大量的云防火墙、负载均衡器等功能性服务。

## 2.4 工控资产暴露情况分析

**观察 2：国内工控资产暴露数量与工业发展水平成正相关，暴露较多的设备主要集中在我国东北老工业基地和东南沿海工业发达地区，并且工控资产会随业务和环境的变化呈现动态变化特征。暴露的工控资产使用最多的工控协议是 Modbus，占总数的 49.2%。这些资产所属的厂商以国际著名公司为主，主要包括摩莎、施耐德电气和西门子等。**

随着工厂智能化的提升，企业内部的工业网络、管理网络与互联网逐步打通，导致大量的工控资产在互联网暴露，这将更易于攻击者对工控系统发起直接攻击，给企业带来严重的安全隐患。因此，本节重点对国内的工控资产暴露情况进行研究分析，为后续的安全防护工作提供数据支撑。

### 2.4.1 地理分布

国内各省市工控资产暴露情况如图 2.14 所示，台湾省位居首位，暴露数量占总数约 62.9%，达到一半以上，较《护航新征程 - 筑牢工业互联网数字安全屏障》[28] 中台湾省的工控资产暴露数量无明显的变化。接下来工控资产暴露较多的省市主要集中在我国东北和东南沿海地区，黑龙江省和吉林省作为我国老工业基地，工控资产暴露数量高于其他省市。值得注意的是，较《护航新征程 - 筑牢工业互联网数字安全屏障》[28] 中，各省市暴露的工控资产数量都存在上下波动，这主要是由于 IP 会随业务和环境变化而呈现出动态变化的特征，导致暴露的工控资产也会发生波动。

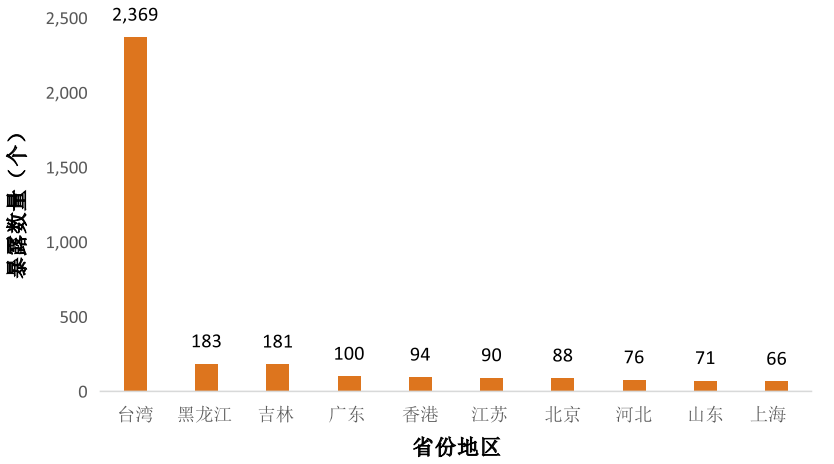



图 2.14　工控资产暴露量 TOP10 省市

## 2.4.2　协议分布

在工控协议方面，依据工业环境，以常用的十个协议 Modbus、MOXA-NPORT、S7、UMAS、ENIP、DNP3、ADS、OMRON、BACNET 和 MELSECQ 进行统计分析，分析结果如图 2.15 所示，发现使用 Modbus 协议的工控资产暴露量最多，占总数的 49.2%，且数量远远领先于排名第二位的 MOXA-NPORT。Modbus 是一种串行通信协议，是施耐德于 1979 年为使用可编程逻辑控制器（PLC）通信而发表，目前已经成为工业领域通信协议的业界标准，用于 PLC、DCS 和智能仪表等工业设备，也是国内工业电子设备之间最常用的通信协议，因此暴露数量最多。其次是 MOXA-NPORT 协议和 S7 协议。

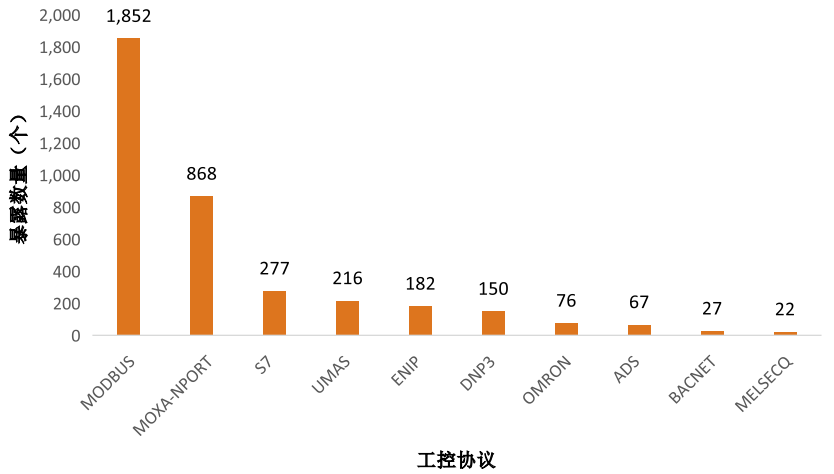



图 2.15　工控协议分布

### 2.4.3 厂商分布

国内暴露的工控资产厂商情况如图 2.16 所示，从图中可以看出，暴露的工控资产厂商主要以国际著名的工控厂商为主，包括了摩莎、施耐德电气和西门子等。最多的是摩莎，占比为 23.1%，其次是施耐德电气和西门子，占比分别为 10.9%、7.1%，三家企业暴露的工控资产占总数的 41.1%。

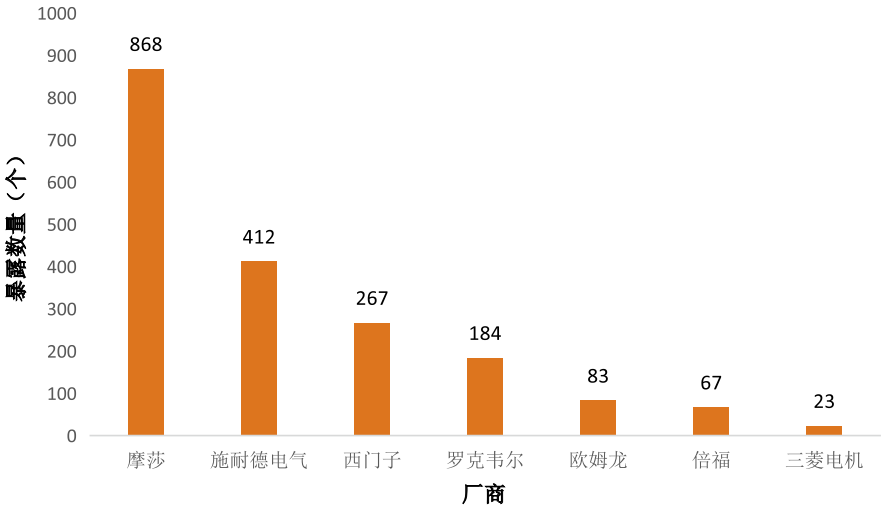



图 2.16 厂商分布

### 2.4.4 小结

通过对全国工控资产最新一轮的监测分析发现，国内很多地区存在工控资产暴露的情况，尤其是工业大省。工业领域的数据价值高、社会影响较大，使得近年来针对工控系统的勒索事件频发。而这些暴露在网络上的工控资产无疑会成为攻击者的入口，使得攻击者探测并锁定攻击目标变得更加容易，加剧了工控系统的安全风险。

## 2.5 安全设备暴露情况分析

**观察 3：2021 年国内暴露的安全设备数量共计 146,459 个，其中，暴露数量最多的是防火墙、VPN 和 WAF，并且以国外厂商的设备居多。这些设备主要集中在我国台湾、香港、北京以及长三角和珠三角等沿海地区。出口类型方面，企业专线和数据中心占比较高，分别占 49.21% 和 43.43%。**

安全设备作为网络基础设施，承担着维护网络安全的重要责任。但是近年来很多厂商的安全设备被曝出存在安全漏洞，如果不及时修复，将会成为攻击者的跳板，对网络发起进一步的渗透。因此，有必要对暴露在互联网上的安全设备进行研究分析，实时掌握这些资产的安全情况，避免成为攻击者入侵内网的入口。

### 2.5.1 类型分布

经统计，2021 年国内有 146,459 个安全设备暴露在互联网上，类型分布如图 2.17 所示。防火墙是使用范围最广泛的安全设备，作为网络安全中的第一道防线，用于保护本地网络免受不可预测、潜在的入侵，同时暴露数量也是最多的，占比高达 41.0%，其次是 VPN 和 WAF，分别占比 31.4% 和 26.1%。

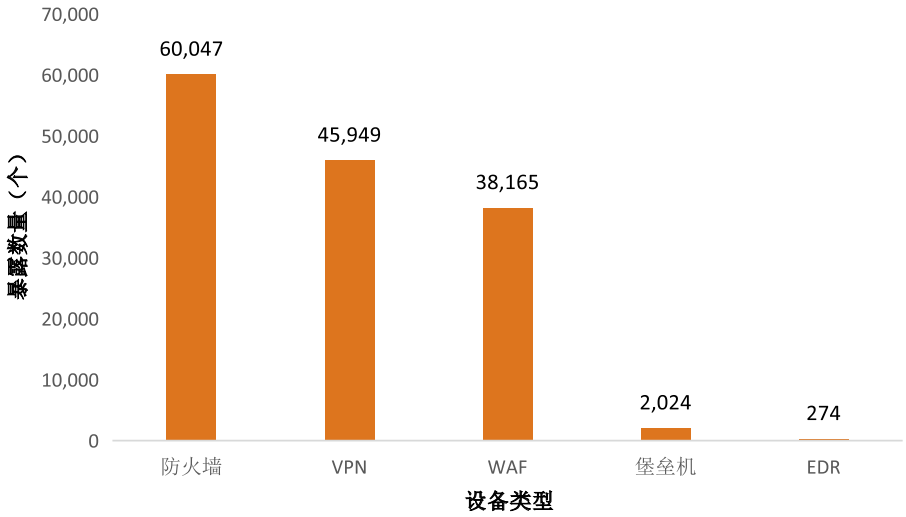



图 2.17 安全设备类型

### 2.5.2 厂商分布

暴露在互联网上的安全设备厂商情况如图 2.18 所示，暴露数量最多的是网络安全设备提供商 Fortinet 的产品，主要是防火墙和 VPN 等。其次是 S1 厂商和 T 厂商的产品，主要包括防火墙和 WAF 等。

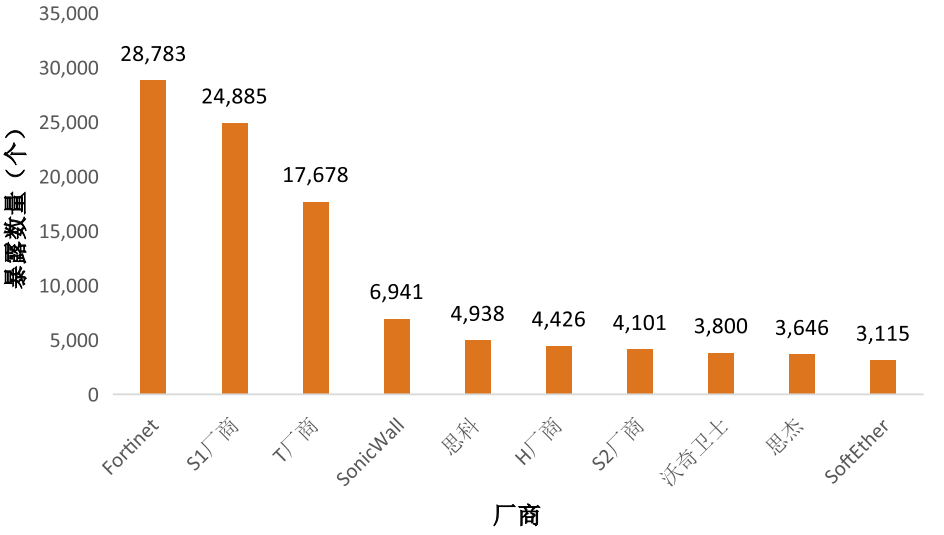



图 2.18　厂商分布

## 2.5.3　地理分布

暴露在互联网上的安全设备数量前三的是台湾、香港和广东，占比分别为 20.6%、14.6% 和 10.6%，占总暴露数量的 45.8%。其次是分布在长三角和珠三角沿海地区的一些省市，暴露的安全设备数量也比较多，如图 2.19 所示。

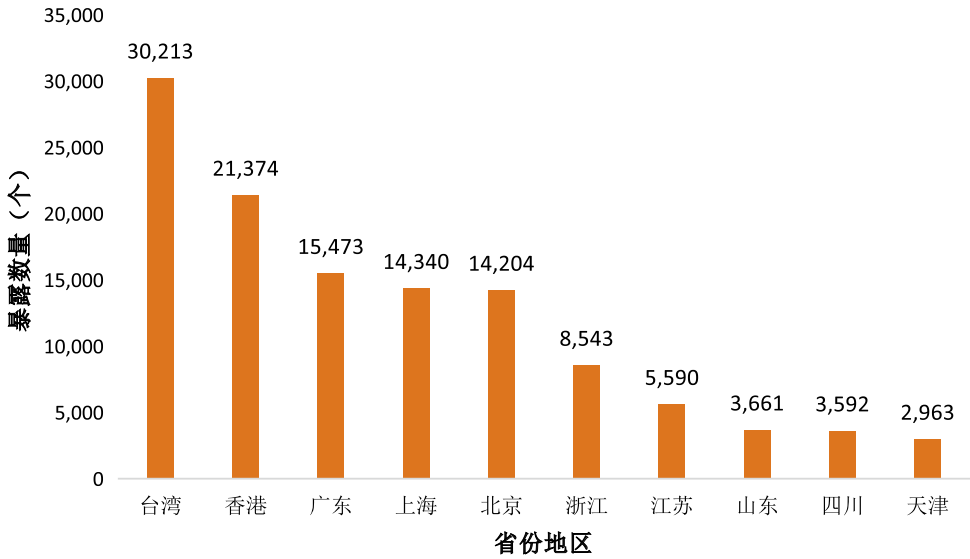



图 2.19　地理分布

### 2.5.4 出口类型分布

暴露的安全设备出口类型情况如图 2.20 所示，企业专线和数据中心占比较高，分别占 49.21% 和 43.43%。在全球化成为大趋势的背景下，越来越多的企业构建专线网络、建立数据中心，暴露的资产给企业的专线网络和数据中心带来安全风险。

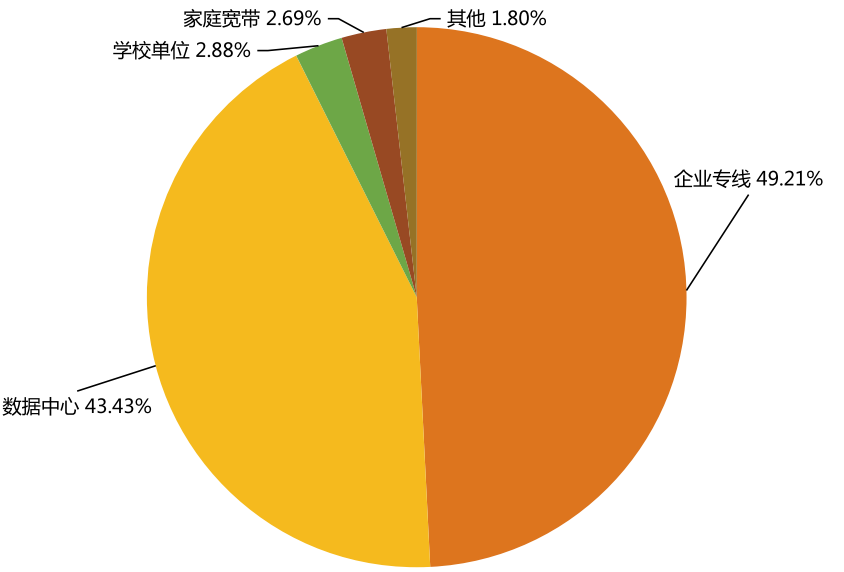



图 2.20 出口类型分布

### 2.5.5 小结

安全设备作为保障网络安全的基础设施，大量部署在互联网中。其中，防火墙、VPN 等作为保护用户内部网络的重要安全屏障，更是必不可少的，监测发现这些设备大量接入互联网。它们作为重要的网络节点，一旦被攻击者利用，后果将不堪设想，因此，安全设备自身的安全风险不容忽视。

## 2.6 数据库暴露情况分析

**观察 4：2021 年全国暴露在互联网上的常用数据库资产已超过 50 万个，其中，MySQL 暴露数量突破 47 万个，占比高达 92.9%, 并且仍有大量用户在使用已经停止更新的数据库版本，存在巨大的安全隐患。地理分布上，由于越来越多的企业将业务拓展到了国外，选择将服务部署在香港，导致香港成为国内数据库暴露数量最多的地区，接下来是北京和东南沿海经济发达地区。**

数据库作为网络空间数据承载的基础设施，存储着网络空间活动过程中的各类数据，涉及个人隐私和国家安全，这些数据被泄露将会造成严重的损失和影响。随着网络空间数据规模的扩大，数据库发生数据泄露的风险逐年增加，在线数据库泄露事件屡创新高。泄露的原因之一是直接接入互联网的数据库存在安全性差的问题，这些暴露在互联网上的数据库很容易被攻击者发现，增加网络攻击面。

本节将对全网数据库资产暴露情况进行分析，统计暴露在互联网的数据库数量、类型、地理分布，以及结合数据库版本观察已经停更但仍在被使用的数据库情况。

## 2.6.1 类型分布

国内暴露在互联网上的数据库资产类型分布如图 2.21 所示，MySQL 数据库暴露在互联网的数量最多，高达 477,256 个，远远超过其他类型数据库暴露数量总和，这主要是由于 MySQL 具有开源、高效和便捷的特性，被企业和个人广泛使用。其次是 Oracle 和 Elasticsearch 数据库，暴露的数量分别为 21,361 个和 9,113 个。

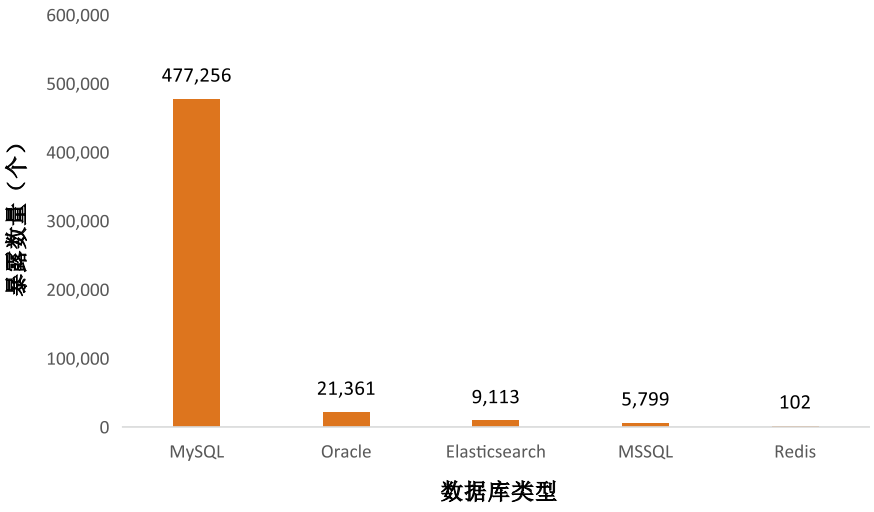



图 2.21 数据库资产类型分布

## 2.6.2 地理分布

国内各省市暴露在互联网的数据库资产情况如图 2.22 所示，香港特别行政区排名第一，暴露的数据库数量占总数的 48.6%，其次是北京市（11.7%）和浙江省（9.6%）暴露在互联网的数据库资产较多。从整体分布来看，东部沿海地区暴露在互联网的数据库数量高于内陆城市。

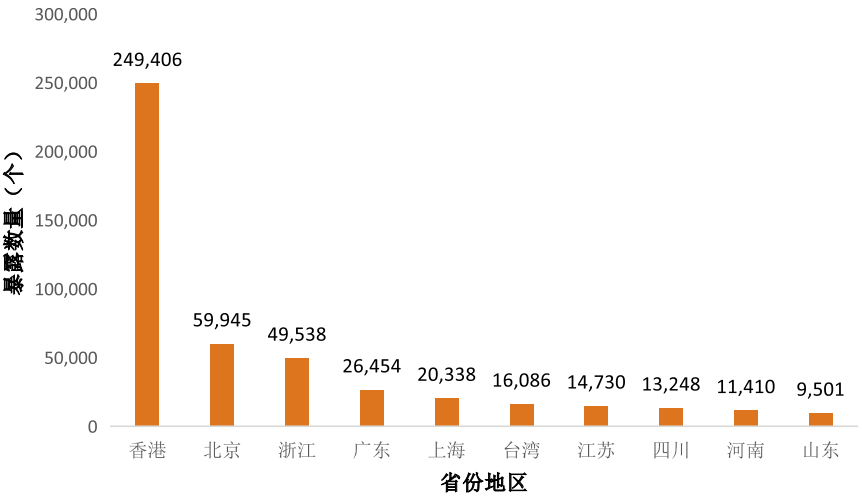



图 2.22　地理分布 TOP10 省市

## 2.6.3　版本分布

1. MySQL

通过分析发现，仍有大量用户在使用已经停止更新的数据库版本，这无疑会带来安全风险，更容易遭受黑客的攻击。暴露在互联网的 MySQL 数据库中，大约 45.6% 的官方已停止更新的 MySQL 仍在被使用，数量 TOP3 的分别是版本 5.6（41,905 个）和版本 5.5（32,497 个），版本 5.1（10,750 个）如图 2.23 所示。

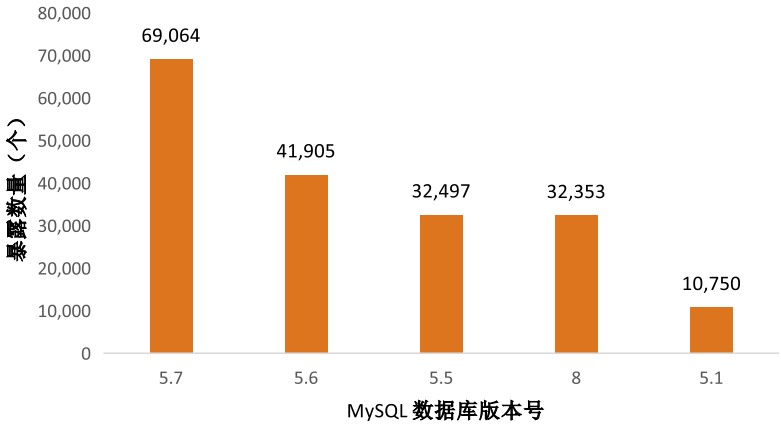



图 2.23　MySQL 数据库版本分布

表 2.1 为 MySQL 数据库版本的发布时间和停止更新时间，从表中可以看出，版本 5.1、5.5 和 5.6 都已经停止更新，版本 5.1 停止更新的时间更是长达 8 年，但是仍在被大量用户使用。

表 2.1　MySQL 数据版本发布和停更时间

| 数据库版本 | 发布时间 | 停更时间 |
|---|---|---|
| MySQL 5.1 | 2008/12 | 2013/12 |
| MySQL 5.5 | 2010/12 | 2018/12 |
| MySQL 5.6 | 2013/02 | 2021/02 |
| MySQL 5.7 | 2015/10 | 2023/10 |
| MySQL 8.0 | 2018/04 | 2026/04 |

2. Elasticsearch

暴露在互联网的 Elasticsearch 数据库中，暴露数量 TOP3 的分别是：版本 7.6（991 个）、版本 7.4（704 个）和版本 6.8（630 个），其中版本 7.6 和 7.4 是官方已经停止更新版本，如图 2.24 所示。

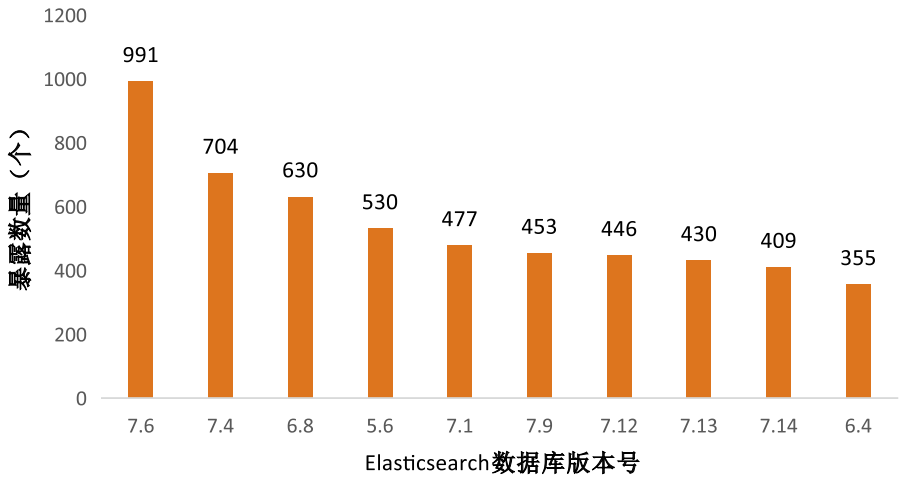



图 2.24　暴露 Elasticsearch 数据库版本号分布 TOP10

表 2.2 展示 Elasticsearch 数据库暴露数量最多的版本号和对应停止更新时间，发现在 Elasticsearch 版本 TOP10 中，仍有 67.9% 官方已停止更新的 Elasticsearch 版本在被使用，例如版本 5.6 暴露数量 530 个，官方已停止更新将近两年。

表 2.2　Elasticsearch 数据库版本停更时间

| 数据库版本 | 停更时间 |
| --- | --- |
| Elasticsearch 5.6 | 2019/03 |
| Elasticsearch 6.4 | 2020/02 |
| Elasticsearch 6.8 | 2022/02 |
| Elasticsearch 7.1 | 2020/11 |
| Elasticsearch 7.4 | 2021/04 |
| Elasticsearch 7.6 | 2021/08 |
| Elasticsearch 7.9 | 2022/02 |
| Elasticsearch 7.12 | 2022/09 |
| Elasticsearch 7.13 | 2022/12 |
| Elasticsearch 7.14 | 2023/02 |

### 2.6.4　小结

基于全网空间扫描结果，发现大量数据库暴露在互联网上，并且仍有大量用户在使用已经停止更新的数据库版本，这些数据库存在严重的安全风险，一旦被黑客攻陷，将导致用户的数据和个人隐私泄露，带来不可估量的危害。因此，除非特别需求，否则企业应及时关闭这些暴露在互联网上的数据库服务，避免被攻击者入侵和攻击。

## 2.7　智慧平台资产暴露情况分析

**观察 5：我们发现全国暴露在互联网上的智慧平台资产已超过 3000 个，包括校园、水利、医疗、交通、养老、物流、车联网、农业相关领域，其中智慧校园平台数量最多。随着数字化转型的稳步推行进，未来将会有更多领域和数量的智慧服务平台出现在互联网上，安全和数字化需要同步建设。**

### 2.7.1　介绍

智慧平台是指利用各种信息技术或创新意念，集成城市与农村的组成系统和服务，以提升资源运用的效率，优化管理和服务，以及改善民众生活质量。智慧平台的应用体系为智慧物流体系、智慧制造体系、智慧贸易体系、智慧能源应用体系、智慧公共服务、智慧管理体系、智慧交通体系、智慧健康保障体系、智慧安居服务体系、智慧文化服务体系。基于应用体系

与资产详情，本节重点关注以下领域：智慧校园、智慧水利、智慧医疗、智慧养老、智慧物流、智慧交通、智慧农业、车联网。

### 2.7.2 类型分布情况分析

国内各类型的智慧平台暴露资产类型分布情况如图 2.25 所示。如智慧校园，该智慧领域的暴露资产数量共计 975 个。通过观察统计数据，智慧校园、智慧水利、智慧医疗领域的暴露资产较多，而智慧农业和车联网领域暴露资产相对较少。随着智慧平台数字化技术的应用，各类资产也将呈现增长的趋势，这也意味着智慧平台的风险暴露面会随之增长，并更趋复杂化，再加上网络攻击技术的持续演进，智慧平台的网络安全将面临更加严重的压力。

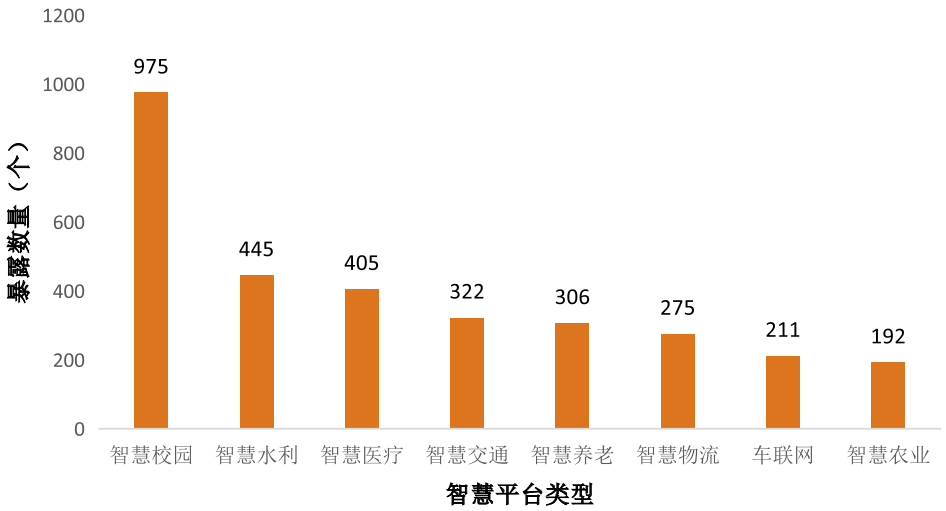



图 2.25 智慧平台暴露资产类型分布

### 2.7.3 地理位置分布情况分析

各类型的智慧平台暴露资产地理位置分布情况如图 2.26 所示。其中北京市、广东省、浙江省分别有 407 个、279 个、234 个暴露资产，位于前三位。人口相对较多的山东省、四川省、河南省分别有 94 个、75 个、43 个暴露资产，同样位于前列。2020 年 GDP 总值位于国内前 10 的江苏省、浙江省、湖北省、上海市也均位于前列。

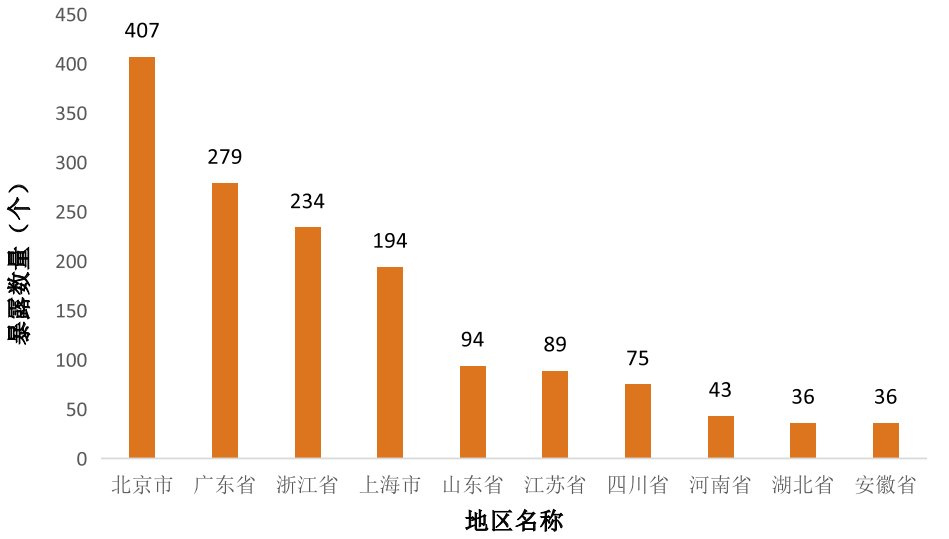



图 2.26　智慧平台暴露资产地理位置分布

### 2.7.4　小结

新型智慧平台极大地依赖物联网、云计算、 大数据、人工智能等新技术的使用，安全问题比数字城市时代更为严峻，需要建立健全信息网络安全保障机制与技术体系，保证新型智慧平台的安全稳定运行。

## 2.8　蜜罐资产暴露情况分析

蜜罐作为一种主动防御的网络系统，本身也属于安全设备的一个种类，但进行网络空间测绘时，蜜罐混杂在大量的资源之中，模拟其他资源设备，影响测绘结果的准确度。此外，蜜罐也会混淆资产指纹，影响资产识别的准确率。因此，对蜜罐的识别是网络空间测绘的一个重要环节。

### 2.8.1　蜜罐类型特征分析

根据所模拟的服务类型，蜜罐可以分为 Web 蜜罐，数据库蜜罐，服务器蜜罐，工控设备蜜罐以及混合蜜罐五种类型。我们调研了 GitHub 之中出现的不同类开源蜜罐以及观察数据得到的非开源蜜罐，通过测绘我们发现 2964 个国内发现国内存活蜜罐服务，涉及到的蜜罐类型以及分布情况如图所示。

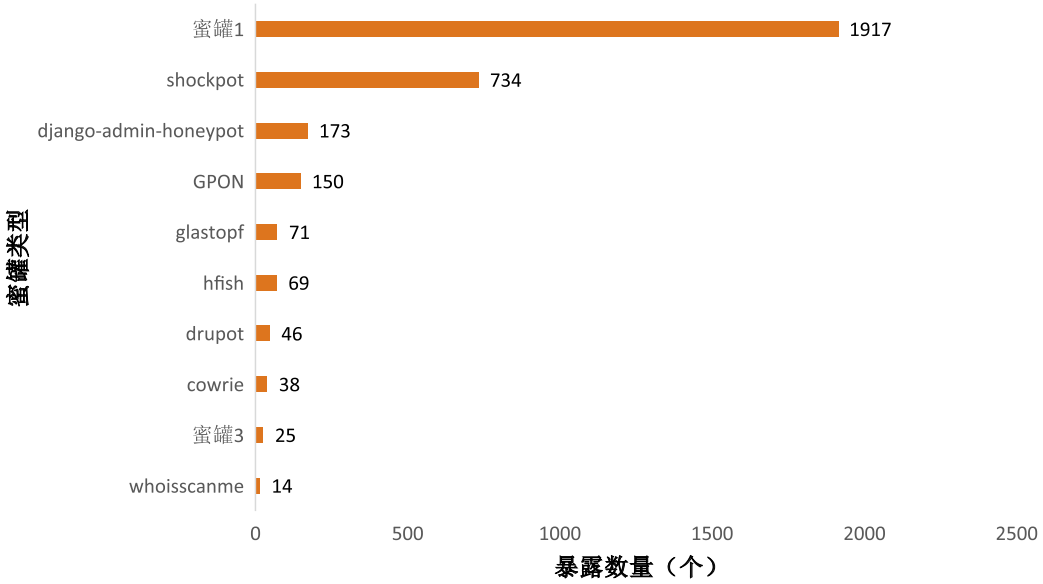



图 2.27　部分常见蜜罐暴露情况

这些蜜罐的指纹主要包含在服务器类型（Server），网站标题 (Title)，静态文件链接以及网页 HTML 之中。蜜罐为了模仿更多的服务类型，Header 部分会有多个 Server 字段，，比如 GPON 蜜罐的请求头的“Server”字段之中含有 9 个服务器类型。分布在网页标题之中的蜜罐指纹往往无法唯一确定是否为某种蜜罐，蜜罐的部署者会更改其中的部分描述，因此需要结合其他指纹进行判断。分布在静态文件链接之中指纹能够较为准确地确定蜜罐的类型，大多数的部署者都不会改变蜜罐的文件结构，因此特征文件的 URI 具有非常强的标识性。网页主体之中包含的指纹通常为隐藏的 input 组件，固定文本描述或者为含有大量设备指纹信息的注释段落。

## 2.8.2　蜜罐混淆资产情况分析

我们通过对蜜罐资源的指纹进行分析来探讨蜜罐都伪装了哪些服务。虽然大多数蜜罐都布置在公有云上面，但是它们模拟的设备却是多种多样的，包括摄像头、路由器、防火墙、API 网关、打印机等。蜜罐通过在服务器类型，标题或者网页主体中增加特定设备的指纹来模拟相关设备，如 GPON 蜜罐的标题是“GPON Home Gateway”，该类蜜罐伪装成为 GPON 路由器的管理界面，引诱攻击者对其发起攻击。而 Gloss 蜜罐则伪装成为一个博客界面，拥有“Blog”标题以及一个可以用于评价的输入框。我们发现大多数的蜜罐都会伪装成为登录界面，因为登陆界面往往是一个 Web 系统的入口，实现简单，不涉及具体的业务信息且无需前置验证信息。此外登陆界面也涉及许多常见的攻击方式，如弱口令爆破等。通过对比蜜

罐登录页面与正常登陆页面之间的差异，蜜罐登录页面具有如下特点：首先，蜜罐登陆页面之中往往含有隐藏的 input 模块；其次，蜜罐页面的表单提交请求的地址通常是发起请求的网址；蜜罐页面使用浏览器打开的时候往往会出现组件缺失或错位的情况。此外，有部分蜜罐会将多种不同设备的指纹信息包含在自身的伪装网页之中，以此吸引更多针对自身的攻击行为。

### 2.8.3 蜜罐地址出口类型分布

我们对不同类型蜜罐的出口类型进行统计，其结果在图 2.28 之中详细阐述。从该图可以看出，有 75.70% 的蜜罐部署在数据中心，4.46% 的蜜罐部署在企业专线，0.79% 的蜜罐部署在学校网络，0.52% 的蜜罐部署在其他地址类型，企业专线种部署数目最多的三类蜜罐从高到低为 Django Admin Honeypot，Shockpot 和 Cowrie。蜜罐的部署地址出口类型也是识别方法之一。

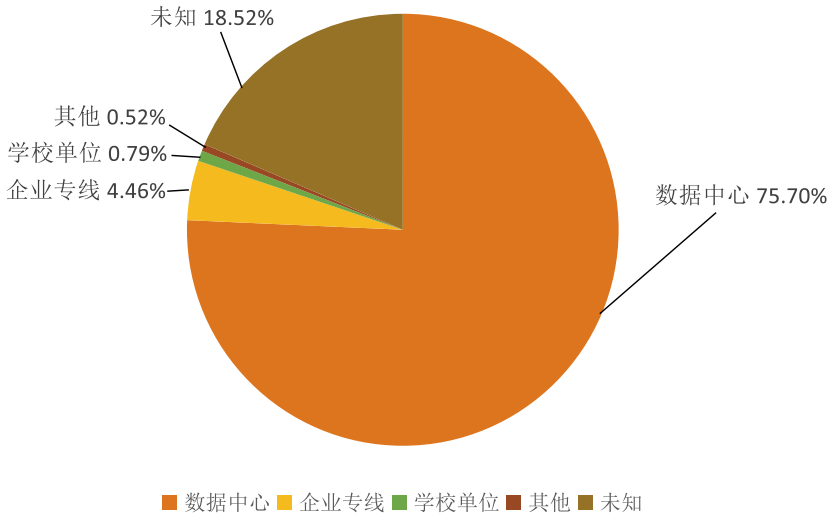



图 2.28 蜜罐出口类型分布统计

### 2.8.4 小结

在本节，我们对互联网之中的蜜罐种类、特征、混淆情况进行了分析。首先利用调研设计了相关的指纹，识别出 10 种开源蜜罐与 4 种非开源蜜罐。这些蜜罐模拟了登陆页面，路由器，摄像头，打印机等多种设备类型。它们的开放端口数目通常远超正常设备，以此吸引更多的攻击者。此外，大多数蜜罐都会部署在公有云，这是识别蜜罐的特征之一。对蜜罐服务的有效识别，可以增加资产识别的准确率，需要持续关注。

## 2.9 小结

本章介绍了国内的物联网、公有云、数据库、工业控制系统、安全设备、智慧平台以及蜜罐资产的暴露情况，我们需要关注的领域肯定不仅仅这些，其他的领域资产我们会持续关注。网络安全风险评估始于资产识别，互联网上资产暴露面的梳理是第一步，也是最重要的一步。第三章将继续介绍网络空间中的一些专题风险分析。

# 03

# 网络空间风险专题分析

本章介绍网络空间一些领域资产风险的专题研究。首先对物联网的漏洞披露和利用情况进行分析，然后介绍工业互联网漏洞趋势和风险分析，最后对公有云上的云原生组件、协议以及应用的风险分析。

## 3.1 物联网风险分析

**观点 7：相比 2020 年，2021 年 NVD 公布的物联网相关漏洞没有明显的变化趋势，相关漏洞仍具有攻击复杂度低、危害评级高的特点。而知名漏洞利用平台 Exploit-DB 近 5 年收录的漏洞利用总量及物联网相关漏洞利用数量均呈下降趋势，但该平台收录的漏洞以命令执行和信息泄露为主，危害程度高，各方仍应提高警惕。**

本节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。

### 3.1.1 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 2021 年 10 月，NVD[29] 平台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（2021 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。

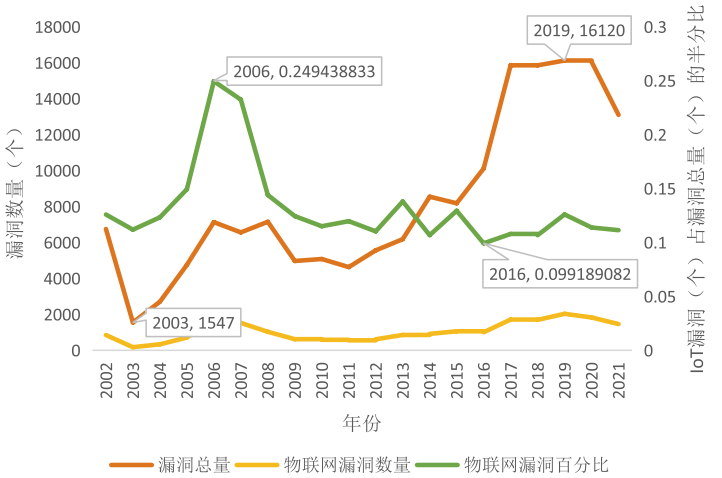



图 3.1 2002 年至 2021 年（10 月）NVD 漏洞数量变化趋势

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，2021 年 1 月至 10 月及 2020 年同期，NVD 披露的物联网相关漏洞攻击复杂度分布如图 3.2 所示。与 2020 年相同的攻击复杂度占比，说明 2021 年 NVD 收录的物联网相关的漏洞仍具有利用难度低的特点，没有明显变化。

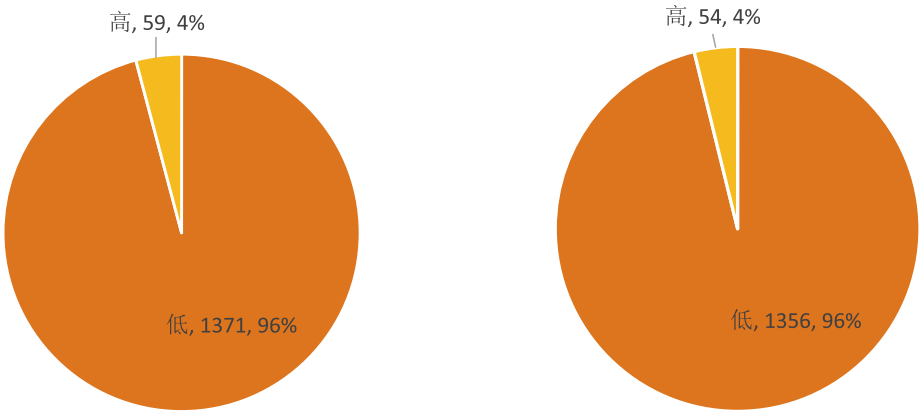



图 3.2　2021 及 2020 年 NVD 物联网相关漏洞攻击复杂度（左为 2021 年）

从漏洞 CVSS 3 评级的角度分析，2021 年 1 月至 10 月及 2020 年同期，NVD 公布的物联网相关漏洞评级分布如图 3.3 所示。与 2020 年相比，2021 年漏洞评级没有明显的变化趋势，各类占比分别为严重 13%，高危占比 48%，中危占比 38%，低危占比 1%。

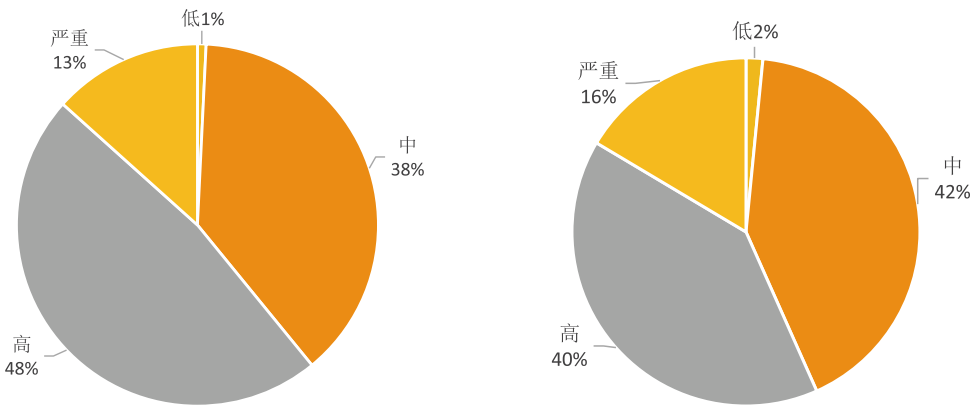



图 3.3　2021 及 2020 年 NVD 物联网相关漏洞 CVSS 3 评级分布（左为 2021 年）

最后，从各个维度来看，NVD 收录的物联网相关漏洞 2021 年与 2020 年相比没有明显变化趋势，仍具有攻击复杂度低，危害评级高的特点。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。

### 3.1.2 物联网漏洞的利用情况

为观察历年披露的物联网利用数量变化趋势，我们统计了 2017 年至 2021 年 10 月，Exploit-DB 平台 [30] 公布的漏洞利用总量以及物联网漏洞数量变化情况，如图 3.4 所示。可以看出漏洞总量及物联网漏洞利用数量均呈一定的下降趋势，但针对物联网相关漏洞利用占比，没有明显的变化趋势，维持在 10%-16% 的范围内波动。

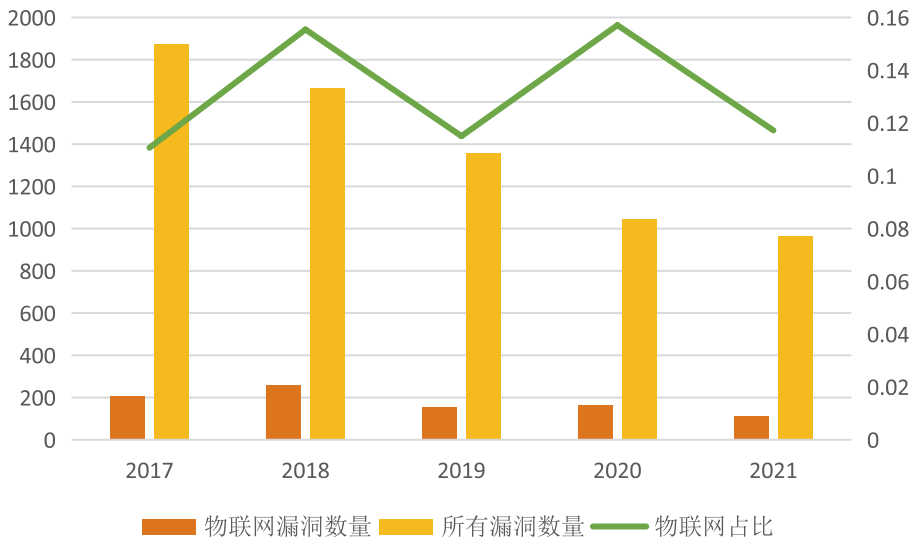



图 3.4 近五年 Exploit-DB 收录漏洞利用变化情况

2021 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 113 个，2021 及 2020 年 Exploit-DB 披露的物联网相关漏洞利用类型分布如图 3.5 所示。与 2020 年相比，占比较大的仍然为命令执行和信息泄露，值得注意的是，2021 年命令执行类的漏洞利用占比有一定提升。可以看出 Exploit-DB 收录的漏洞利用以命令执行、信息泄露等危险程度较高的漏洞利用为主，各方应提高警惕。

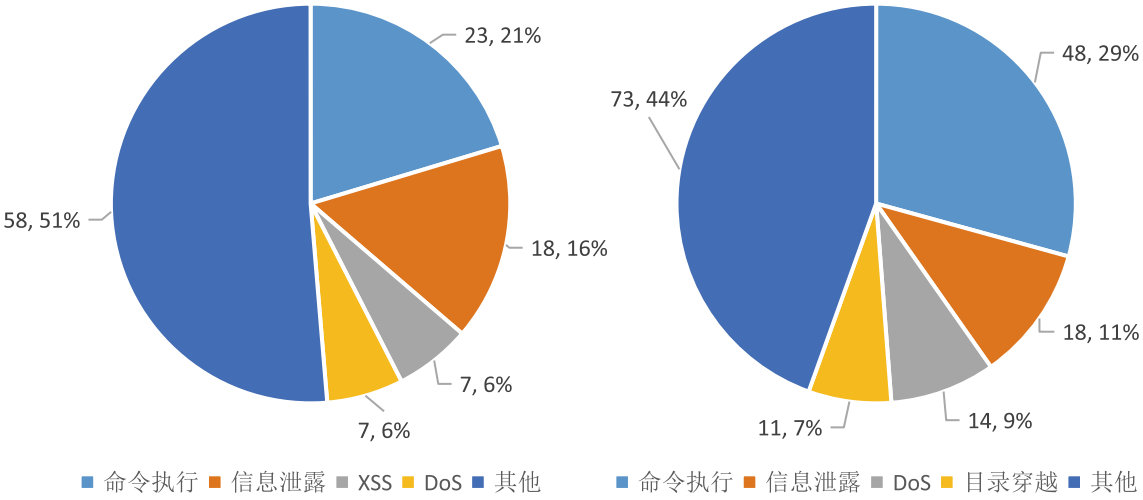



图 3.5　2021 年及 2020 年 Exploit-DB 物联网相关漏洞类型分布（左为 2021 年）

从各厂商被收录的漏洞利用来看，2021 及 2020 年 Exploit-DB 收录所有厂商漏洞利用占比如图 3.6 所示。Exploit-DB 收录各厂商的漏洞利用没有明显的偏好，2021 相比 2020 厂商存在一定的变化。但值得注意的是，WordPress 无论 2021 年还是 2020 年，占比均为最高，且 2021 年有较大的提高。

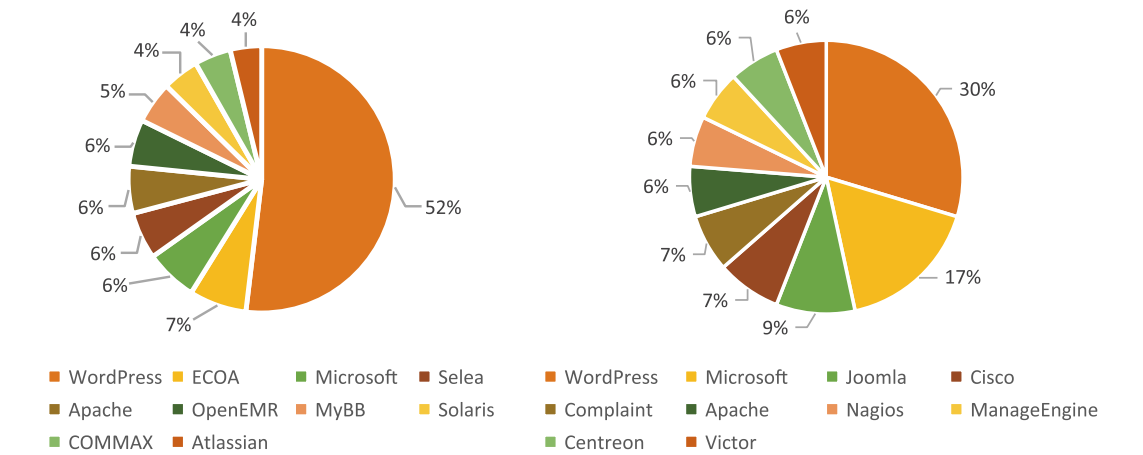



图 3.6　2021 及 2020 年 Exploit-DB 收录所有厂商漏洞利用占比（左为 2021 年）

从 Exploit-DB 收录各物联网厂商漏洞利用的占比情况来看，Exploit-DB 对厂商没有特别偏好的现象更为明显，2021 及 2020 年 Exploit-DB 收录的物联网厂商漏洞利用占比如图 3.7 所示。2021 年出现的物联网厂商与 2020 年几乎完全不一样，这也说明了物联网厂商众多，物联网设备存在的漏洞利用碎片化严重。

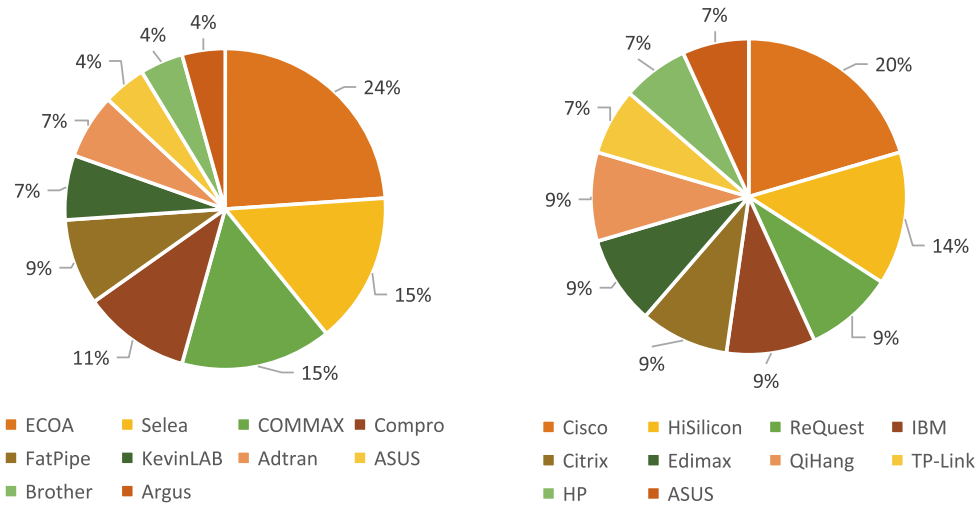



图 3.7　2021 及 2020 年 Exploit-DB 收录物联网厂商漏洞利用占比（左为 2021 年）

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。2021 及 2020 年 Exploit-DB 收录的物联网相关漏洞利用命中情况如图 3.8 所示。2021 年 1 月至 10 月，在 Exploit-DB 披露的 82 个物联网相关漏洞利用中，有 25 个被绿盟威胁捕获系统捕获，占比约 30%。

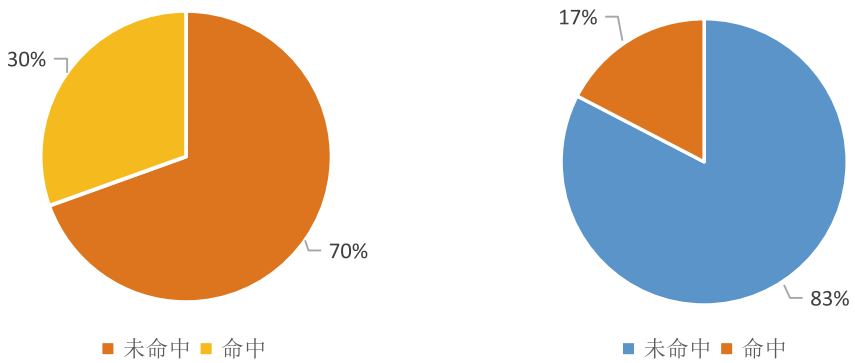



图 3.8　2021 及 2020 年 Exploit-DB 物联网相关漏洞利用命中情况（左为 2021 年）

2021 年，Exploit-DB 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 1 天，最长为 221 天。值得注意的是，2021 年出现了较多的攻击首次捕获日期早于 Exploit-DB 相关漏洞利用收录日期的情况，其中最长达 284 天，去年同期仅有个别漏洞利用首次捕获日期早于 Exploit-DB 的收录日期。说明 Exploit-DB 的收录已经出现一定的迟滞，研究人员需要扩展信息来源以应对日益复杂的攻击态势，仅依赖单一来源在与攻击方对抗的过程中将处于落后。

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） |
|---|---|---|---|
| 50422 | 2021/10/18 | 2021/1/7 | -284 |
| 50340 | 2021/9/28 | 2021/1/12 | -259 |
| 50254 | 2021/9/2 | 2021/1/19 | -226 |
| 50162 | 2021/7/29 | 2021/1/21 | -189 |
| 50069 | 2021/6/28 | 2021/2/2 | -146 |
| 49926 | 2021/6/2 | 2021/2/4 | -118 |
| 49730 | 2021/3/31 | 2021/2/20 | -39 |
| 49499 | 2021/1/29 | 2021/1/27 | -2 |
| 49955 | 2021/6/7 | 2021/6/8 | 1 |
| 50295 | 2021/9/15 | 2021/9/16 | 1 |
| 49782 | 2021/4/21 | 2021/4/26 | 5 |
| 50339 | 2021/9/28 | 2021/10/3 | 5 |
| 49738 | 2021/4/2 | 2021/4/7 | 5 |
| 49764 | 2021/4/14 | 2021/4/23 | 9 |
| 50211 | 2021/8/17 | 2021/8/31 | 14 |
| 50206 | 2021/8/16 | 2021/8/31 | 15 |
| 50099 | 2021/7/6 | 2021/7/26 | 20 |
| 50277 | 2021/9/13 | 2021/10/3 | 20 |
| 50285 | 2021/9/13 | 2021/10/3 | 20 |
| 50146 | 2021/7/21 | 2021/8/31 | 41 |
| 50160 | 2021/7/28 | 2021/9/14 | 48 |
| 50098 | 2021/7/6 | 2021/9/2 | 58 |
| 49455 | 2021/1/22 | 2021/6/18 | 147 |
| 49457 | 2021/1/22 | 2021/8/31 | 221 |
| 49456 | 2021/1/22 | 2021/8/31 | 221 |

### 3.1.3　小结

相比 2020 年，2021 年 NVD 公布的物联网相关漏洞没有明显的变化趋势，相关漏洞仍具有攻击复杂度低、危害评级高的特点。而知名漏洞利用平台 Exploit-DB 近 5 年收录的漏洞利用总量及物联网相关漏洞利用数量均呈下降趋势，但该平台收录的漏洞以命令执行和信息泄露为主，危害程度高，各方仍应提高警惕。攻击者对于物联网漏洞的利用，已经从去年对

Exploit-DB 平台的快速跟进，升级到多信息来源的快速跟进上。2021 年 Exploit-DB 披露的 82 个物联网相关漏洞利用中，有 25 个被绿盟威胁捕获系统捕获，占比约 30%，值得注意的是，2021 年出现了首次捕获日期早于 Exploit-DB 收录日期 284 天的情况，去年同期仅有个别漏洞利用首次捕获日期早于 Exploit-DB 的收录日期。可见，Exploit-DB 的收录已经出现一定的迟滞，研究人员需要扩展信息来源以应对日益复杂的攻击态势，仅依赖单一信息来源在与攻击方对抗的过程中将处于落后。

## 3.2 云上风险分析

**观点 8：云上服务、资产数量巨大、类型众多，不同服务及资产暴露的攻击面均不相同，相应的安全成熟度也有较大差异，云上安全态势较为复杂。尽管诸如对象存储服务等公有云服务已经设置了多种提示和警告措施，云上数据泄露事件依然每年都在发生。云原生服务中，容器相关组件（如 Docker）由于落地时间较长，脆弱性暴露情况较少，但其他云原生组件却不容乐观。此外，云上常见物联网协议或服务（如 MQTT）普遍存在未授权访问风险，较为严重。**

近年来，伴随着企业上云的步伐不断加快，云上风险和安全事件也层出不穷。只有在对云上风险有充足的认识和评估的基础上，才能够安全上云、确保业务在云上持续安全运行。本节，我们从以对象存储为代表的公有云服务、云原生服务组件和以 MQTT 为代表的云上物联网类协议三个角度出发，对云上风险进行梳理分析。

### 3.2.1 公有云服务风险分析——以对象存储服务为例

公有云租户可根据自身业务需求，定制化地租用存储桶服务并为存储桶配置合适的访问权限，供相关人员进行数据存储与共享。但正是这一款广受欢迎的对象存储服务，近年来却屡屡曝出数据泄露事件。那么，究竟是什么原因引发了存储桶的数据泄露事件呢？存储桶的数据泄露问题如今是否仍然存在呢？我们不妨通过事件分析与实验验证来一同探索这两个问题的答案。

存储桶（Bucket) 是对象的载体，可理解为存放对象的“容器”，且该“容器”无容量上限、对象以扁平化结构存放在存储桶中，无文件夹和目录的概念，用户可选择将对象存放到单个或多个存储桶中 [31]。由于存储桶具有扩展性高、存储速度快、访问权限可自由配置等优势，如今已纳入各大公有云厂商的关键基础设施，例如 Amazon 的 S3、Microsoft 的 Blob、阿里云的 OSS、腾讯云的 COS 等。

#### 3.2.1.1 S3 存储桶数据泄露风险

近年来，Amazon S3 屡屡被曝光数据泄露事件，不胜枚举，我们按照时间顺序列出了其中的一部分，如表 3.2 所示。

表 3.2 S3 存储桶数据泄露事件

| 时间 | 泄露内容 | 泄露规模 | 数据所属者 | 泄露原因 |
| --- | --- | --- | --- | --- |
| 2017-06-12 | 选民个人信息 | 超过 1.98 亿条 | Deep Root Analytics[36] | 公开访问 |
| 2017-09-06 | 互联网监控数据 | 数十亿条 | 美军中央及太平洋司令部 [37] | 登录访问 |
| 2017-09-27 | 虚拟机镜像 | 超过 100GB | 美国陆军情报与安全司令部（INSCOM）[38] | 公开访问 |
| 2018-08-24 | 医疗、个人信息 | 181 家机构，超过 3000 人 | MedCall Advisors（医疗服务提供商）[40] | 公开读写 |
| 2019-01-16 | 政府敏感文件、个人信息 | 约 3TB | 美国俄克拉荷马州安全部门 [41] | 公开访问 |
| 2020-04-23 | 用户个人信息 | 超过 700 万条 | BHIM（印度电子支付平台）[46] | 公开访问 |

除表 3.2 中所列出的数据泄露事件之外，S3 存储桶还发生过许多其他事件。网络上甚至已经有相关网页，专门收集、列举 Amazon S3 数据泄露事件 [32][33]，感兴趣的读者可以进一步了解。

从表 3.2 中我们可以看到，在选取的 6 个数据泄露事件中，有 4 个事件涉及到的 S3 存储桶是公开访问的。这意味着，只要在浏览器中输入了正确的域名，世界上任何人都可以访问这些数据；另外，有一个事件涉及的存储桶被设置为允许任何 AWS 登录用户访问，这看起来似乎比公开访问更安全些，但事实上，任何人都能够免费注册 AWS，因此这样配置的存储桶安全性并不高；最后，一个医疗数据泄露事件的相关存储桶竟然被设置为任何人均可读写，这是不可想象的。

既然大部分的数据泄露事件是由于存储桶被配置为公开访问导致的，下面将从 S3 存储桶的访问权限配置机制引入，说明 S3 存储桶的数据泄露风险。从图 3.9 中可以看到，在 S3 存储桶创建过程中，系统由明确的权限配置环节，且默认替用户勾选了“阻止全部公共访问权限”选项。


图 3.9　S3存储桶访问权限说明

若要将存储桶设为公开访问，首先要在“阻止公共访问权限”标签页中取消对“阻止公共访问权限”的选中状态，然后进入“访问控制列表”标签页设置“公有访问权限”，允许所有人“列出对象”，“读取存储桶权限”。而且每设置一步，都会有风险提示。具体流程如图 3.10 所示。

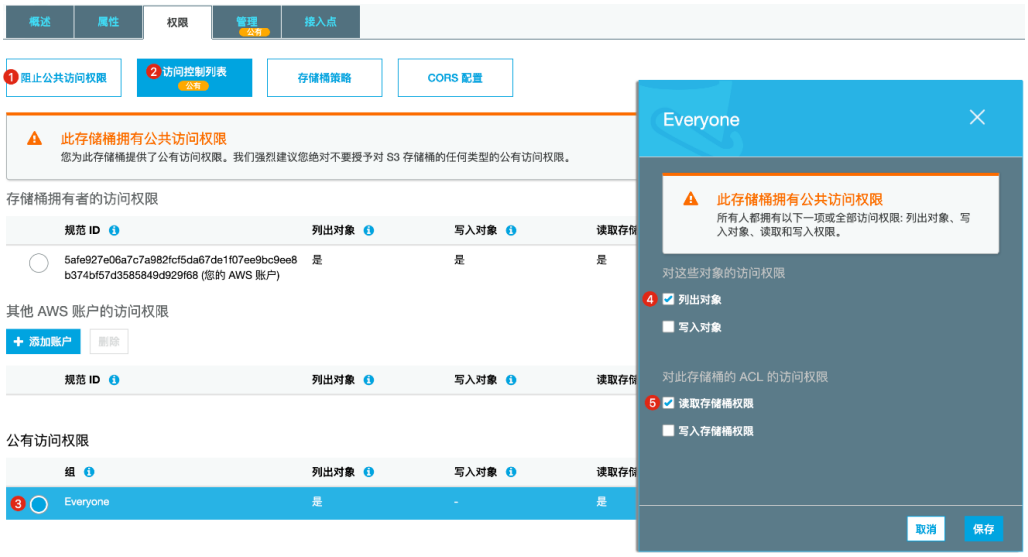



图 3.10　开启存储桶公共访问流程示意图

即便存储桶被设置为公开访问，还需要设置存储桶内文件的权限。由此看来，Amazon 在安全控制方面做得还是不错的，但是为什么还会不断有数据泄露事件发生呢?

有研究者指出[34]，问题的核心在于，有时完全弄清楚某个存储桶的公开程度是不容易的——虽然已经限制了存储桶级别的权限，但是桶内文件的访问权限覆盖了存储桶本身的限制。另外，随着时间的推移，用户添加的访问策略可能会越来越复杂，甚至有时出于特殊需要打开了访问限制，却忘记了关闭。

S3 存储桶数据泄露风险的主要原因是人为错误配置导致某些存储桶中的某些敏感信息被公开。

#### 3.2.1.2 S3 存储桶访问测试实验

本节将通过对 S3 存储桶进行访问测试实验进一步说明存储桶的数据泄露问题。

前文已经提及，通过输入正确的访问域名可以获取到 S3 存储桶中允许被公开访问的数据，那么构建出正确的访问域名便是进行访问测试的第一步。Amazon S3 存储桶的一种访问域名形式为[35]：

https://<bucket-name>.s3.<region>.amazonaws.com/<key-name>

其中的变量为存储桶名 bucket-name，存储桶所在区域 region( 可省略 ) 以及文件路径 key-name。我们对几家公有云厂商存储桶进行了访问测试，与 S3 存储桶类似，Microsoft Azure 的 Blob 以及阿里云的 OSS 访问路径中的变量也为上述三者。但不同的是，在对 Amazon S3 存储桶进行访问时，若是一级域名正确，则会返回存储桶内的文件信息，如图 3.11 所示。此后，根据返回的存储桶内文件信息，将域名进行拼接，则可获取存储桶内文件，如图 3.12 所示。此外，当域名中的 region 信息错误时，访问后还会返回正确的 region 信息，如图 3.13 所示。


图 3.11　通过一级域名获取文件信息示意图

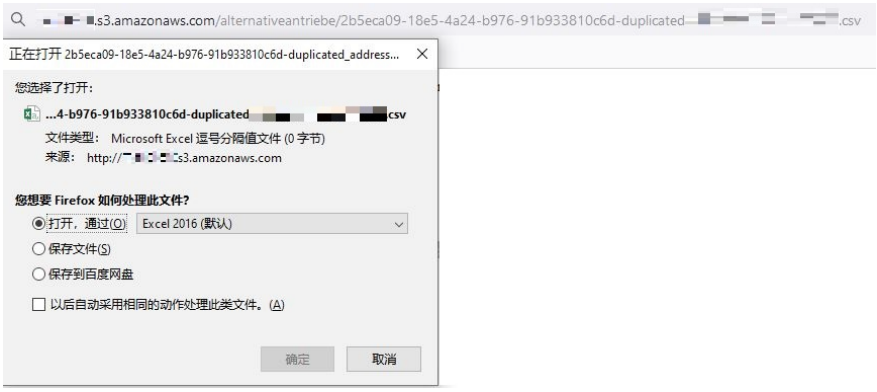



图 3.12　拼接文件名获取可访问文件示意图

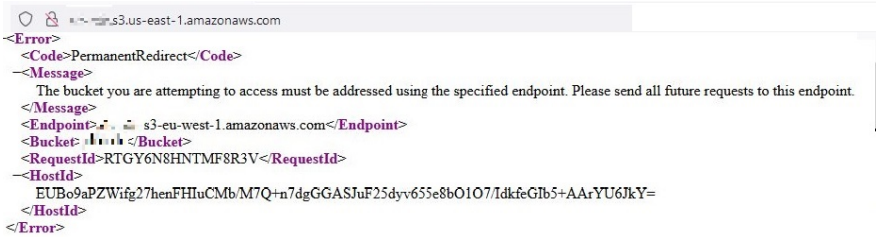



图 3.13　填写错误 Region 后返回正确 Region 信息示意图

Amazon S3 存储桶的访问域名变量可缩减到一个——存储桶名 (bucket-name)

既然 S3 存储桶的访问域名变量可缩减到一个，那么访问域名的生成问题则可以转化为存储桶名的构建问题。根据 AWS 的官方规定，S3 存储桶的 bucket-name 是由小写字母、数字、句号 (.) 以及连字符 (-) 组成的 3-63 位的字符串 [36]。全部遍历需要约次，显然无法实现。那么便需要对存储桶的命名规律进行分析，以构建合适的 bucket-name。

根据创建存储桶时的命名习惯，可以做出如下推论：

1. 对于某组织或企业的存储桶，一般会以组织或企业名、简称或包含上述信息的字符作为 bucket-name；
2. 对于某组织或企业下的某产品或某项目，一般会以产品名、项目名、产品或项目名与组织名的拼接或包含上述信息的字符作为 bucket-name；
3. 对于某个人用户，一般会以个人姓名、昵称或包含上述信息的字符作为 bucket-name。

基于上述推论，可利用模糊测试的方式定向对组织、企业或个人发起域名访问测试。我们利用模糊测试工具 Fuzzer[37] 对国外某公司进行了存储桶域名模糊测试，测试过程如图 3.14 所示。

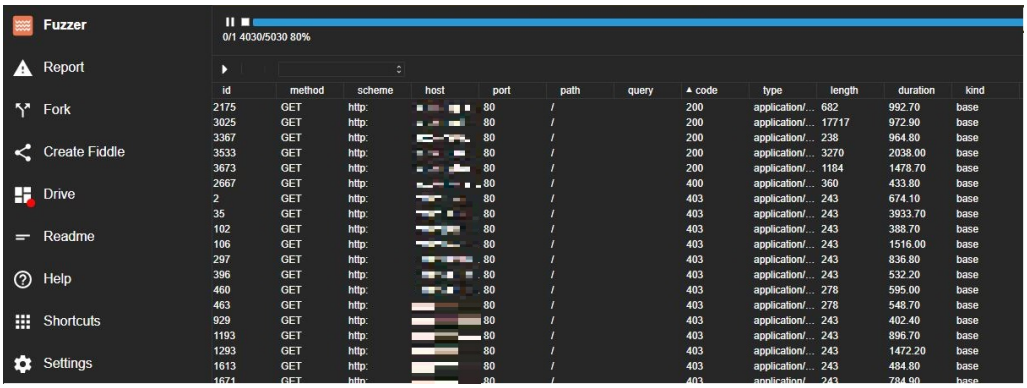



图 3.14　利用 Fuzzer 定向获取某公司存储桶域名

经过 15538 次域名访问，最终获取到可公开访问的存储桶域名 9 个，存在的但不可公开访问的存储桶域名 135 个。从测试结果来看，模糊测试可以相对完整地定向获取特定组织的存储桶域名，但命中率较低，访问耗时较长。

由于模糊测试的命中率较低，除个别需要定向渗透的场景外，使用模糊测试获取域名并不可行。若要获取更多的存储桶域名，进而评估其中是否存在敏感信息泄露的情况，还需要提高访问测试的命中率。

为此，我们对 Yago 数据集 [38] 进行了分析处理，提取出与上述推论相关联的信息，最终筛选整合出 7131 个字符作为 bucket-name 进行域名访问测试。我们利用了开源项目 S3scanner[39] 作为测试扫描器，测试过程如图 3.15 所示。

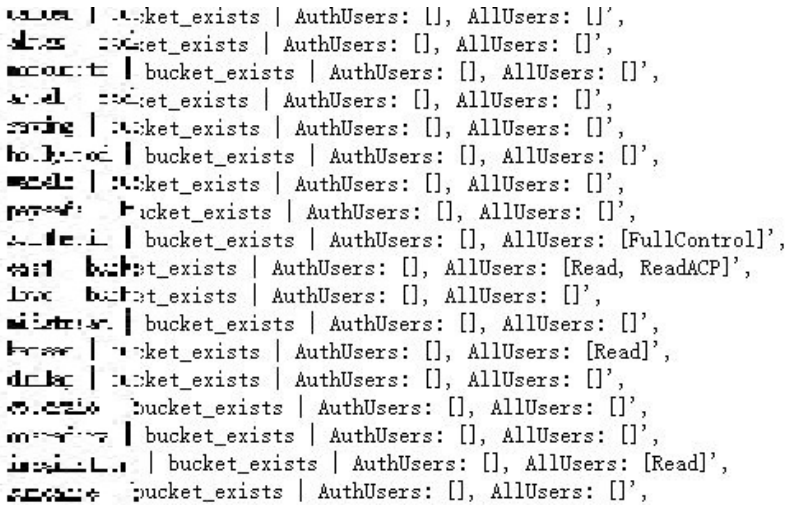



图 3.15　通过数据分析批量获取存储桶域名

经过访问测试，最终从 7131 个 bucket-name 命中到 3482 个存活存储桶。在这 3482 个存活存储桶中，有 268 个是可以公开访问的，其中还有 13 个的公开访问权限被设置为 FullControl。可公开访问的存储桶数量约占访问测试总次数的 3.7%，相比模糊测试大大提高了命中率。此次测试只使用了 Yago 数据集中的 company 类，其他符合推论条件的字符约有 28 万，从比例预估能够获得 10000 个可以公开访问的存储桶。

#### 3.2.1.3 S3 存储桶敏感信息发现

正常情况下，存储桶所有者在给某一文件配置为可以公开获取的前提是所有者期望其他人去访问这些信息且其中不包含敏感信息。但实际情况果真如此是这样么？

我们对已经发现的 268 个可以公开访问的存储桶中的数据进行了统计分析，具体信息如表 3.3 所示。

表 3.3　已捕获到公开访问的存储桶数据类型统计表

| 数据类型 | 文件后缀 | 数量 |
|---|---|---|
| 图像 | jpg\|png\|gif\|jpeg\|tif\|svg\|bmp | 54823 |
| Web 界面 | js\|html\|css\|xml\|htm | 12087 |
| 音频 | mp3\|frg | 6595 |
| 视频 | mp4\|swf\|wmv\|flv\|mov | 7962 |
| 文档 | txt\|pdf\|json\|doc\|ppt\|csv\|xlsx | 7768 |
| 压缩包 | gz\|gzIP\|zIP\|rar | 2835 |
| 其他 | | 5150 |

进一步地，各个类型的数据分布如图 3.16 所示。

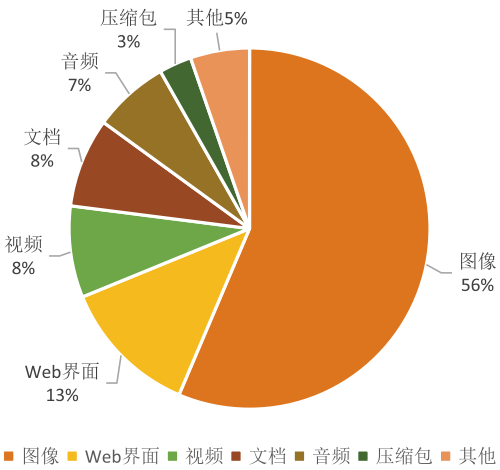



图 3.16　可公开访问存储桶数据类型分布图

此外，从目前发现的 97569 个存储桶数据中，仍有 37389 个数据文件是不可访问的，另外 60180 个数据文件可以公开访问。

从表 3.3 和图 3.16 的信息中可以看出，大部分用户使用 S3 来存储图像，其中大多数是 Web 界面的图像组件和企业的宣传海报以及 Logo。可见 S3 是一个相对便利的可进行宣传和信息共享的平台。Web 界面、视频以及音频类型的文件也大多是令其他用户浏览以及企业宣传使用。

因此，我们将重点关注对象放在了文档文件中，以检查其中是否存在敏感信息泄露的情况。

经验证，已经获取的可以公开访问的文档文件中存在一些非公开信息。例如，某一包含某企业某部门员工姓名、所在地以及个人邮箱的 CSV 文档，整个文档中共有约 500 条该企业员工的个人信息，如图 3.17 所示；此外，这些可以公开访问的文档文件中还包括一个某企业私有的项目需求文档，如图 3.18 所示。

| First | Last | Email | City | State | Department |
|---|---|---|---|---|---|
| | | inross.com | Toronto | Ontario | |
| | | law.com | Belleville | Ontario | |
| | | lakes.com | Toronto | Ontario | |
| | | can.com | Toronto | Ontario | |
| | | birdlaw.com | Toronto | Ontario | |
| | | n | Toronto | Ontario | |
| | | .com | Toronto | Ontario | |
| | | -law.com | Toronto | Ontario | |
| | | ulds.com | Toronto | Ontario | |

图 3.17　S3 公开数据中的某企业员工信息

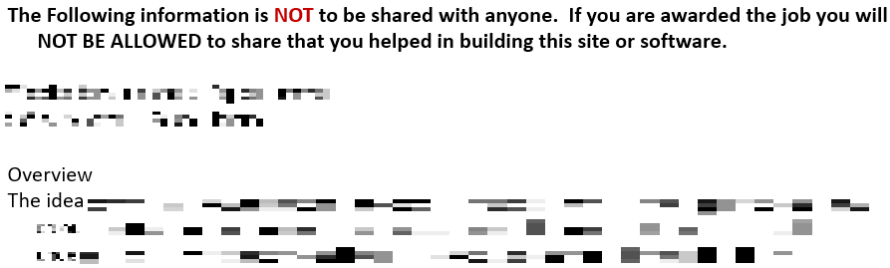



图 3.18　S3 公开数据中的某企业私有项目文档

由此看来，Amazon S3 的数据泄露情况仍在发生。

### 3.2.2 云原生服务风险分析

**观察 6：我们针对目前市面上比较流行的云原生服务进行了资产、版本分布梳理以及相应的风险分析，这些服务包括 Docker、Kubernetes API Server、Istio、Kong、Prometheus，其中 Docker 资产暴露数量在国内仅有 179 个，风险分析方面，因暴露 2375 TCP Socket 端口导致的未授权访问漏洞，仍旧是 Docker 服务在互联网上面临的一大风险；Kubernetes API Server 资产数量在国内有近 2 万个，其中因暴露 6443 及 8080 端口导致的未授权访问漏洞资产数约 200 个，这个数量占总体的 1%，此外，暴露资产中约 77% 的资产受 CVE-2021-25741、CVE-2021-25735、CVE-2018-1002105 这三个漏洞的影响；Istio 资产在国内有近 2400 个，其中 443 和 80 端口数量最多；Kong 资产数量在国内暴露约 5900 个，其中命中 CVE-2021-27306 漏洞的资产数约占总资产数的 52%，命中 CVE-2020-11710 漏洞的资产数约占总资产数的 37%；Prometheus 资产在国内暴露约 5200 个，目前受到 CVE-2021-29622 漏洞影响的资产数量为 910 条，约占总量的 17%。**

近年来，企业上云不断加速，相关技术落地成熟，公、私、混合云平台及业务得到长足发展。新冠疫情爆发以来，各行各业对远程办公、远程研发的需求大幅增加，进一步促进了云计算技术的发展和落地。进入云计算的下半场，以容器和 Kubernetes 为核心的云原生技术被越来越多的企业采用，大幅提高了生产效率。

与此同时，云计算安全风险和威胁也不断出现。2021 年以来，CVE-2021-30465、CVE-2021-25741 等可能导致容器逃逸的高危漏洞被陆续发现，“上云”虽好，“云上”却并不平静。

本小节，我们将对云原生生态下的核心程序及组件进行测绘分析，用数据来呈现云原生技术的落地情况和风险态势。

#### 3.2.2.1 Docker 风险分析

2013 年，DotCloud 开源了其内部的容器项目 Docker。Docker 除了基础的容器服务之外，还引入了一整套管理容器的生态系统，包括容器镜像模型、镜像仓库、RESTful API、命令行等。

**1) 资产暴露情况分析**

我们通过分析现有的测绘数据，对 Docker 资产的暴露情况进行了统计，下面将从地区分布及端口分布两个维度分别进行介绍。

从测绘数据中得到 Docker 相关资产共 179 条数据，地区分布如图 3.19 所示：

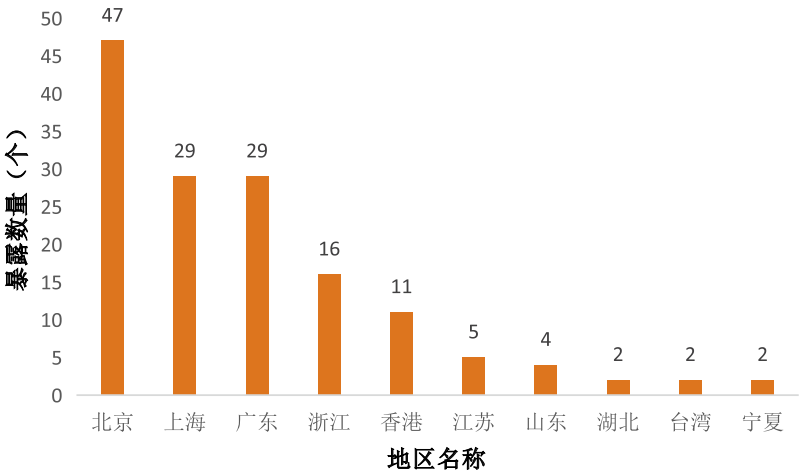



图 3.19　Docker 资产地区分布

针对测绘数据中 Docker 资产暴露的端口情况进行了统计，如表 3.4 所示：

表 3.4　Docker 资产端口分布

| 端口 | 资产数 |
| --- | --- |
| 2375 | 100 |
| 2376 | 13 |
| 其它 | 66 |

从上述数据可以发现，国内暴露的 Docker 资产信息中有约 67% 左右的数据来源于北京市、上海市、广东省、浙江省，其中北京市暴露 47 条数据位居第一；端口主要分布在 2375 和 2376 端口，其中 2375 端口数量 100 个位居第一。

用户使用 Docker 服务的安全意识有明显提高，可能和近一年容器安全技术在市场大规模落地相关。

**2）版本分布**

我们还对国内暴露的 Docker 资产版本分布做了统计，如图 3.20 所示：

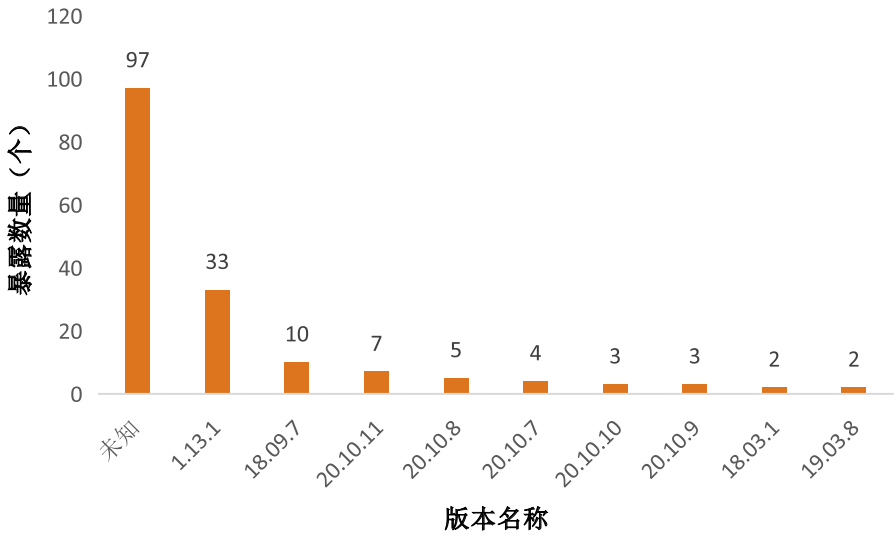



图 3.20　Docker 资产版本统计

从上述数据可以发现，约 50% 的资产未获取具体版本，剩余 50% 为可统计的 Docker 版本资产，其中 1.13.1 版本暴露最多，约占已知版本资产总数的 33%。

#### 3.2.2.2　Kubernetes API Server 风险分析

API Server 组件为各类 Kubernetes 资源对象的增删改查提供了 REST 接口，为贯穿整个 Kubernetes 系统的数据总线。

Kubernetes 集群中，API Server 运行在 Master 节点上，默认开放两个端口，分别为本地端口 8080 和安全端口 6443，其中，非认证或授权的 HTTP 请求通过 8080 端口访问 API Server；而 6443 端口用于接收 HTTPS 请求。Kubernetes 中默认不启动 HTTPS 安全访问控制。

API Server 在整个 Pod 工作流中主要负责各个组件间的通信，Scheduler, Controller Manager, Kubelet 通过 API Server 将资源对象信息存入 Etcd 中，当各组件需要这些数据时又通过 API Server 的 REST 接口来实现信息交互。

**1）资产暴露情况分析**

我们通过分析现有的测绘数据，针对 Kubernetes API Server 组件资产近一个月的暴露情况进行了统计，下面将从地区分布及端口分布两个维度分别进行介绍。

我们从测绘数据中得到 API Server 资产数据共计 19286 条，其中地区分布如图 3.21 所示：

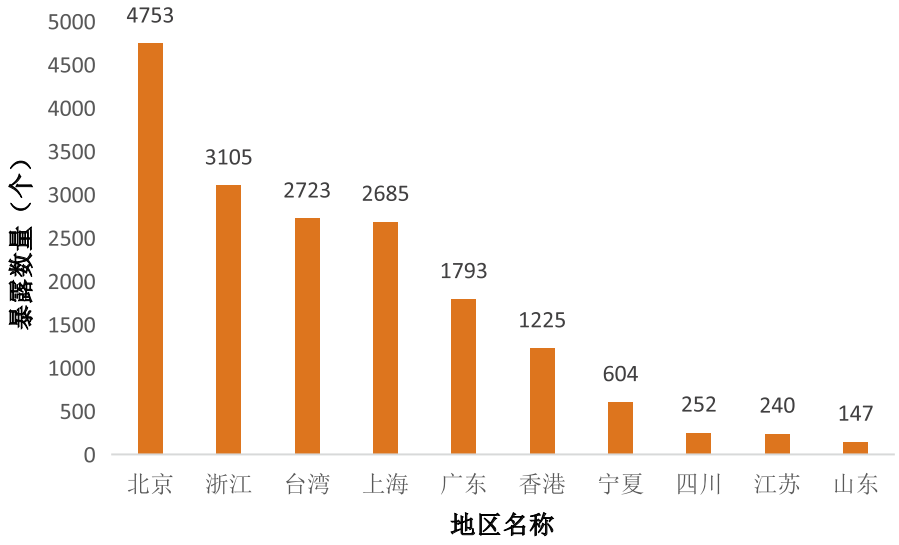



图 3.21　API Server 资产地区分布

我们对 API Server 资产暴露的端口情况进行了统计，如表 3.5 所示：

表 3.5　API Server 资产端口分布

| 端口 | 资产数 |
| --- | --- |
| 6443 | 14444 |
| 443 | 4744 |
| 其他 | 98 |

从上述数据可发现，国内暴露的 Kubernetes API Server 组件资产中有约 84% 左右的数据来源于北京市、浙江省、上海市、广东省、香港，其中北京市暴露 4288 条数据位居第一；端口主要分布在 6443、443 端口，其中 6443 口数量 14444 个位居第一。

**2）版本分布**

我们对测绘数据中国内暴露的 Kubernetes API Server 组件资产版本分布做了统计，如图 3.22 所示：

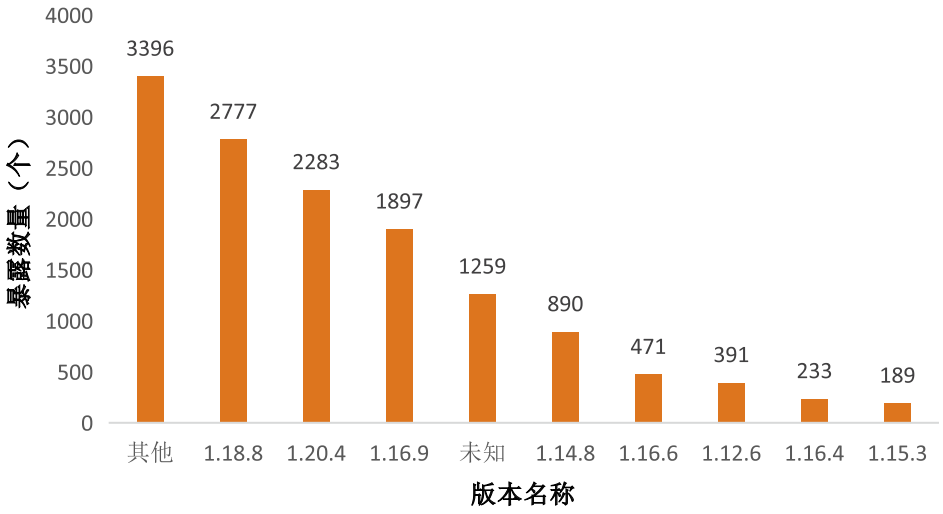



图 3.22　API Server 资产版本统计

从上述数据可以发现，以上信息可以看出在统计的资产中，未获取到具体版本信息的资产约 1259 个，约占所有资产的 9%，无法获取具体版本的原因有两个，第一个是暴露的资产无法被正常访问，正常情况下，需要访问资产 URL 后返回 200、403、404、401、302 等状态码才可以获取具体版本。第二个是如果用户在部署 Kubernetes 时，将 API Server 组件的“--anonymous-auth”配置项设为 false，也无法通过访问资产 URL 获取版本信息。除此之外，剩余的可获得版本的约 90% 资产中，绝大多数版本分布在 1.18.8、1.20.4、1.16.9、1.14.8、1.16.6 范围，其中暴露版本最多的为 1.18.8，约 2800 个，其次是 1.20.4，约 2300 个，最后是 1.16.9 版本，约 1900 个，其它版本由于存在数量较少，且分布范围较大，故统一归为“其它”版本，约 3400 个，通过分析测绘数据我们进一步发现这些暴露较多的版本资产中，约 90% 部署在阿里云上。

### 3）资产脆弱性暴露情况分析

首先，我们对国内暴露的 Kubernetes API Server 资产数据进行了脆弱性分析，从测绘数据中得出，在国内互联网暴露的 14550 个资产里，有 187 个资产存在未授权访问脆弱性，如图 3.23 所示：

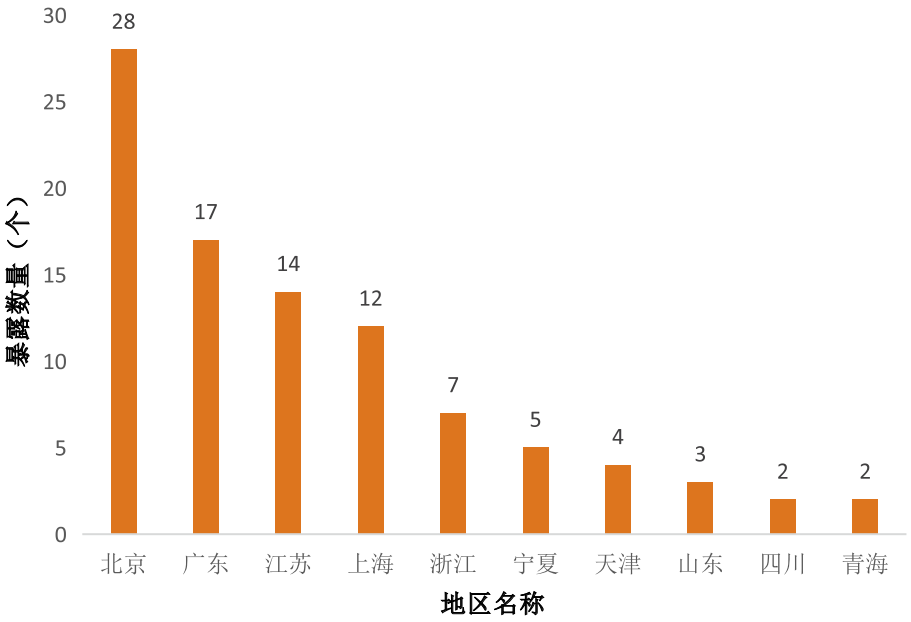



图 3.23　API Server 未授权资产统计

其中端口分布如表 3.6 所示：

表 3.6　API Server 未授权资产端口分布

| 端口 | 资产数 |
| --- | --- |
| 6443 | 61 |
| 8080 | 27 |
| 30001 | 12 |
| 8081 | 1 |

北京市、广东省、上海市、江苏省暴露的未授权访问资产最多，北京市暴露 52 个位居第一；存在未授权访问的 Kubernetes 资产只占总数的 1.3%，这是非常小的一个数目，也可间接说明用户现在的安全意识在逐步增强；从暴露未授权资产中，6443 端口及 8080 端口最多，约占未授权资产总数的 82%。

我们也从 CVE 漏洞维度统计了现有暴露资产的脆弱性分布情况，如图 3.24 所示：

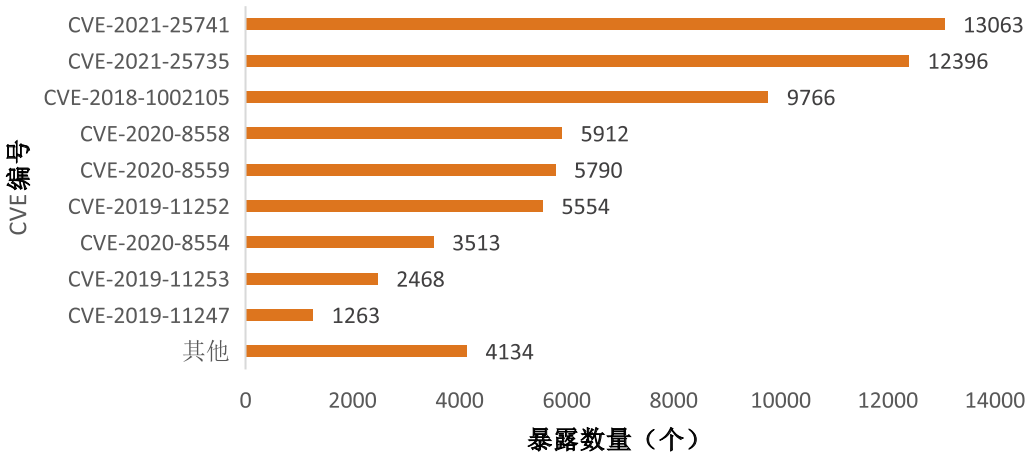



图 3.24　API Server 资产脆弱性统计

针对测绘数据分析，在国内互联网暴露的 14550 个 API Server 组件资产中，有 13071 个资产被曝出含有 CVE-2021-25741 漏洞，12403 个资产被曝出含有 CVE-2021-25735 漏洞，9773 个资产被曝出含有 CVE-2018-1002105 漏洞，其中每个资产可能命中多条 CVE。此外，通过图 3.27 我们也可以看出命中 CVE-2021-25741 漏洞的资产数约占总资产数的 90%，命中 CVE-2021-25735 漏洞的资产数约占总资产数的 85%，命中 CVE-2018-1002105 漏洞的资产数约占总资产数的 67%，由以上数据可以看出超过 80% 的资产会受到以上三个 CVE 的影响，可见影响面之大。

#### 3.2.2.3　Kong 风险分析

Kong 是一个云原生的、与平台无关的、可扩展的 API 网关，Kong 主要通过其具备的高性能和丰富的可扩展性插件生态为名。通过提供代理、路由、负载平衡、健康检查、认证（以及更多）的功能，Kong 作为中心层，可以较为平滑地协调微服务或传统的 API 流量。

**1）资产暴露情况分析**

我们通过分析现有测绘数据，对 Kong 组件资产近一个月的暴露情况进行了统计，下面将从地区分布及端口分布两个维度分别进行介绍。

我们从测绘数据中查询到国内的 Kong 资产共 5829 条数据，其中地区分布如图 3.25 所示：

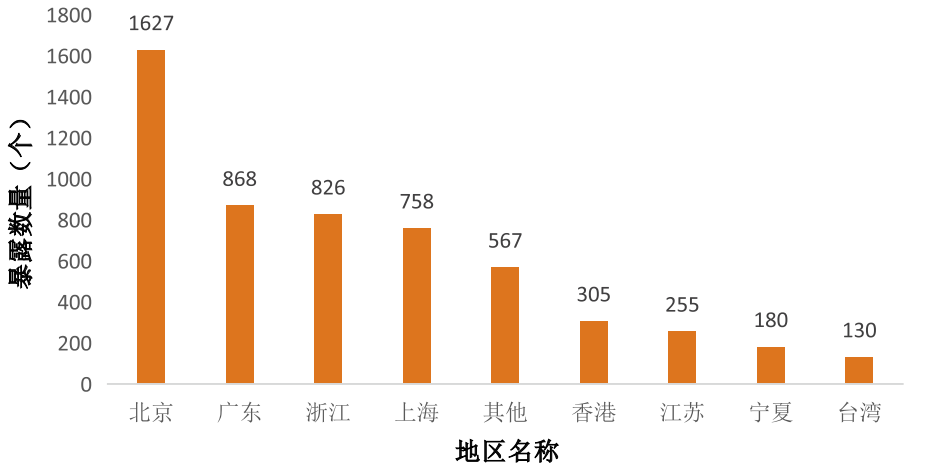



图 3.25　Kong 资产地区分布

我们通过分析测绘数据对 Kong 资产暴露的端口情况进行了统计，如图 3.26 所示：

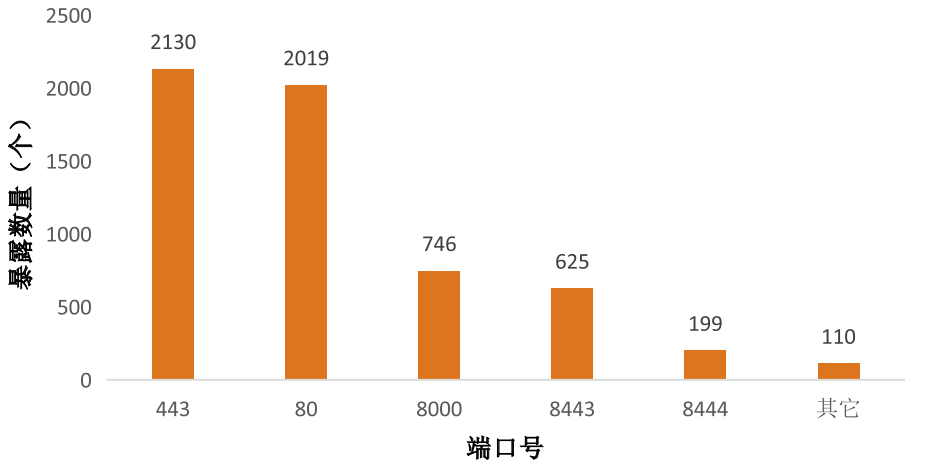



图 3.26　Kong 资产端口分布

从上述数据可以发现，国内暴露的 Kong 资产中有约 85% 左右的数据来源于北京市、广东省、浙江省、上海市、香港特别行政区、江苏省、台湾省、宁夏回族自治区，其中北京市暴露 1627 条数据位居第一。端口主要分布在 443、80、8000，其中 443 端口数量 2130 个位居第一、80 端口数量 2019 个位居第二。

**2）版本分布**

版本分布情况如图 3.27 所示：

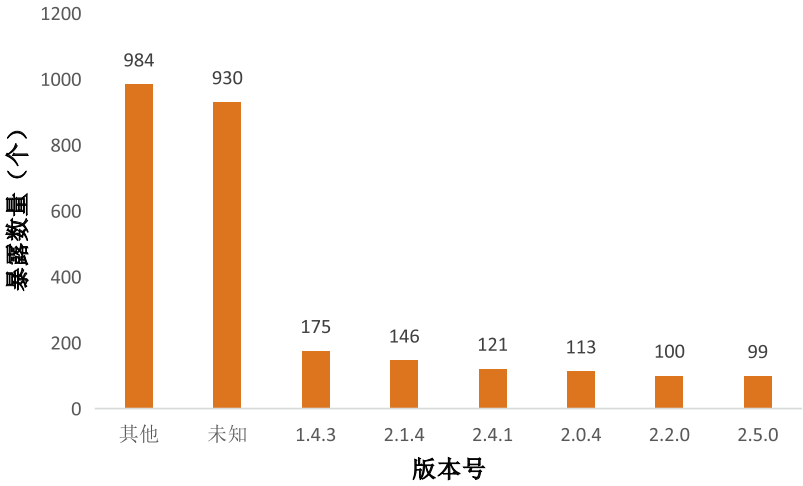



图 3.27　Kong 资产版本分布

根据统计，22% 的资产未获取到具体版本信息，原因为暴露的 Kong 资产需要被正常访问（状态码 200、403、404、302 等）。剩余资产中，绝大多数暴露版本分布在 1.4.3、2.1.4、2.4.4、2.0.4、2.2.0、2.5.0、0.14.1，值得注意的是，0.14.1 版本为 2018 年 8 月发布的版本，为相对早期的版本，但在互联网上暴露的资产数量却不少。

### 3) 资产脆弱性暴露情况分析

我们对国内暴露的 Kong 资产数据进行了脆弱性分析，针对 CVE 维度，我们统计了现有暴露资产的脆弱性分布情况，如图 3.28 所示：

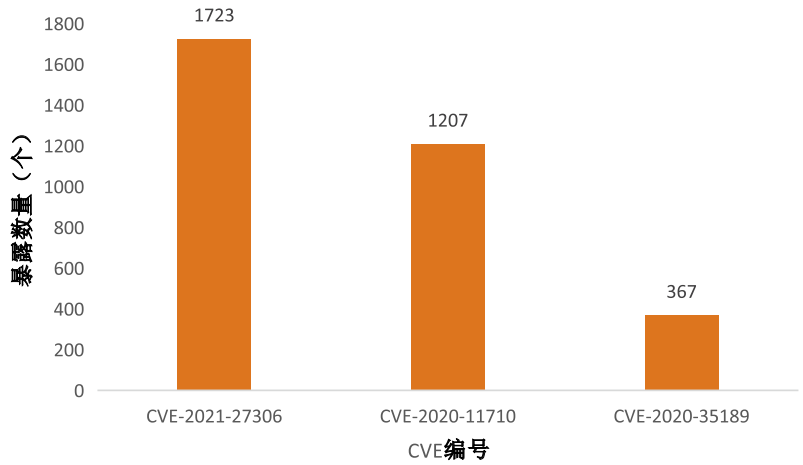



图 3.28　Kong 资产脆弱性分布

根据统计，国内互联网暴露的 5829 个 Kong 资产中，有 1723 个资产被曝出含有 CVE-2021-27306 漏洞，1207 个资产被曝出含有 CVE-2020-11710 漏洞 ,367 个资产被曝出含有 CVE-2020-35189 漏洞，其中每个资产可能命中多条 CVE。此外，我们也可以看出命中 CVE-2021-27306 漏洞的资产数约占总资产数的 52%，命中 CVE-2020-11710 漏洞的资产数约占总资产数的 37%，可见这两个 CVE 漏洞影响面较大。

#### 3.2.2.4 Istio 风险分析

Istio 是一个开源服务网格平台，它可以控制微服务之间数据的共享方式。 其附带的 API 可以将 Istio 集成到任何日志记录平台、遥测或策略系统中。 在设计上，Istio 可以在多种环境中运行：企业本地、云托管、Kubernetes 容器，或虚拟机上运行的服务等。

我们通过分析现有测绘数据，对 Istio 资产近一个月的暴露情况进行了统计，下面将从地区分布、端口分布两个维度分别进行介绍。

我们通过测绘数据查询到国内 2358 条数据，地区分布如图 3.29 所示：

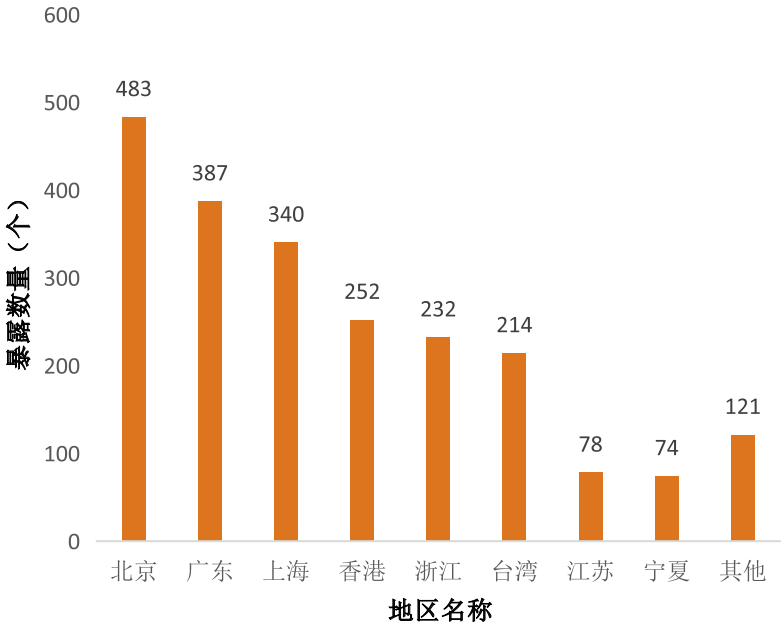



图 3.29　Istio 资产地区分布

我们通过测绘数据对 Istio 资产暴露的端口情况进行了统计，如图 3.30 所示：

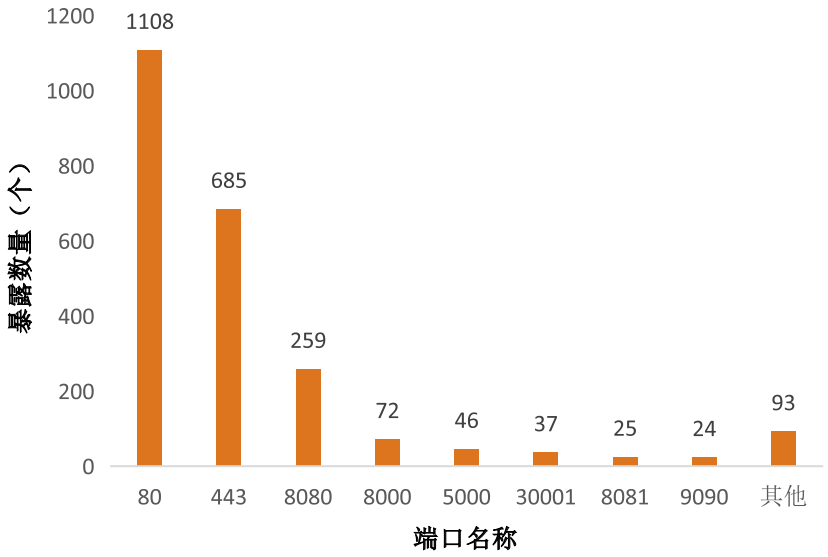



图 3.30　Istio 资产端口分布

国内暴露了 2358 个相关资产，其中 1911 个来源于北京市、上海市、广东省、香港特别行政区、浙江省、台湾省，其中北京市暴露 483 个位居第一。国内暴露的资产使用的端口主要分布在 80 和 443，其中 443 端口数量 1108 个位居第一。

#### 3.2.2.5　Prometheus 风险分析

Prometheus 是一款开源的、基于 Metric 的云原生应用时间监控和警报解决方案，由谷歌研发，目前已经被 CNCF 托管，是继 K8s 托管的第二个项目。

**1）资产暴露情况分析**

我们通过分析现有的测绘数据，对 Prometheus 资产的暴露情况进行了统计，下面将从地区分布、端口分布和版本分布三个维度进行介绍。

我们通过测绘数据查询到 5159 条数据，其中地区分布情况如图 3.31 所示：

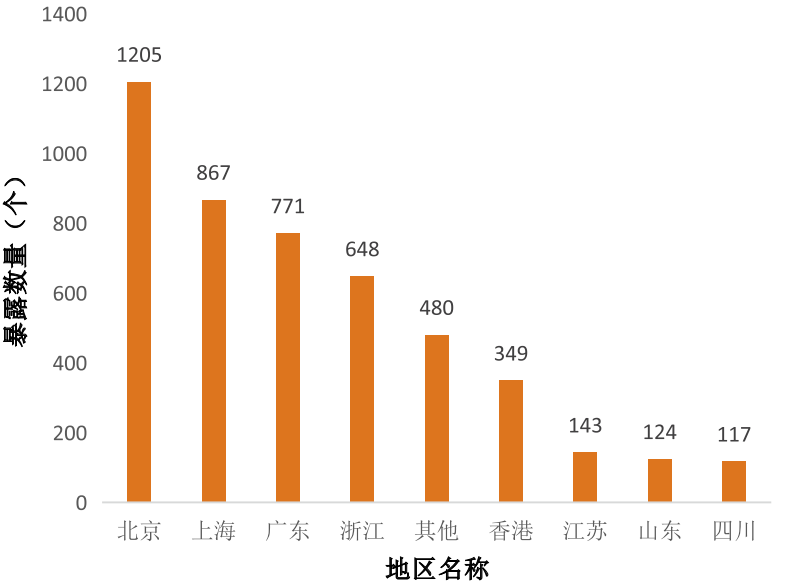



图 3.31　Prometheus 资产地区分布

端口分布情况如图 3.32 所示：

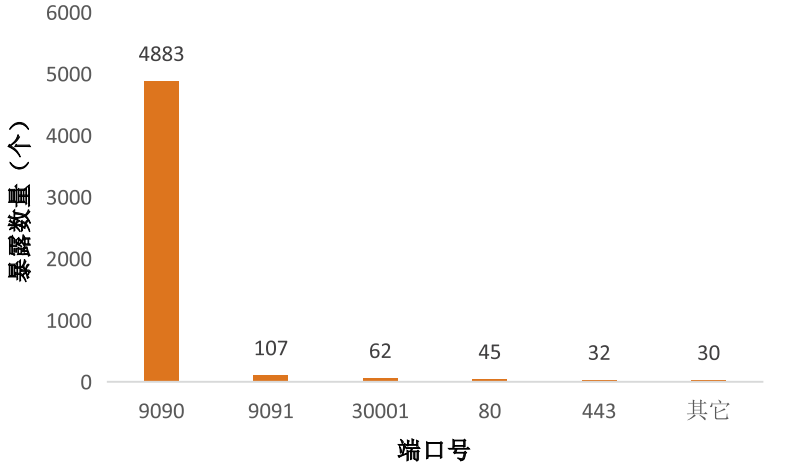



图 3.32　Prometheus 资产端口分布

从上述数据可以发现，国内暴露的 Prometheus 资产中约 74% 来源于北京市、上海市、广东省、浙江省、香港特别行政区这些地区，其中北京市稳居第一，暴露 1205 条；国内暴露的 Prometheus 资产主要分布在 9090 端口，占暴露资产的 95%，极少数分布在 9091 端口、30001 端口等。

**2）版本分布**

版本分布情况如图 3.33 所示：

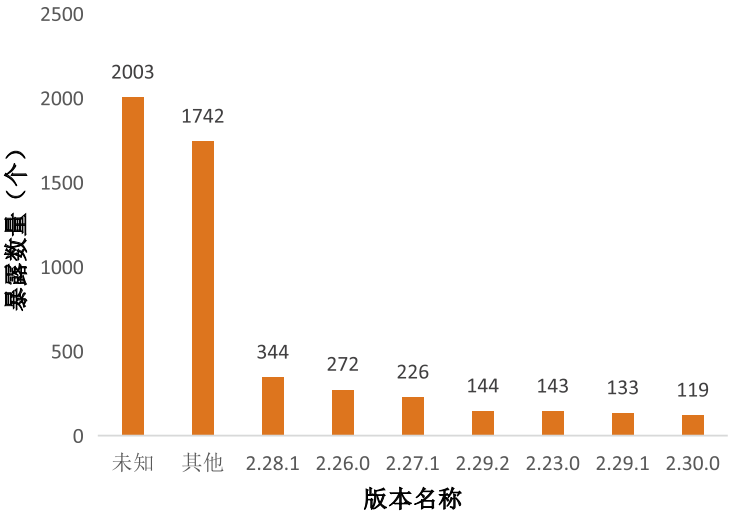



图 3.33　Prometheus 资产版本统计

目前互联网暴露的 Prometheus 资产中，可确定版本的占 65%，数量前三的版本为 2.28.1、2.26.0、2.27.1。

**3）资产脆弱性暴露情况分析**

我们对国内暴露的 Prometheus 资产数据进行了脆弱性分析，发现目前受到 CVE-2021-29622 漏洞影响的资产数量为 910 条，约占总量的 17%，该漏洞为重定向漏洞，虽然对业务运行本身无影响，但可用来作钓鱼攻击，仍存在一定危害。

## 3.2.3　公有云协议风险分析——以 MQTT 协议为例

**观察 7：互联网中暴露 32 余万个资产涉及 MQTT 服务，其中 77% 存在未授权访问风险，泄露了物联网设备的敏感信息。涉及 MQTT 协议的开源物联网框架存在明文存储 MQTT 配置、未修改默认密码等安全问题，攻击者可通过 MQTT 协议修改物联网设备数据，甚至可以控制物联网设备。**

### 3.2.3.1　MQTT 协议简介

MQTT 是一个基于客户端 - 服务端架构的发布 / 订阅模式的消息传输协议，适用于很多场景，尤其是资源受限环境，例如机器与机器的通信以及物联网。

如图 3.34 所示，MQTT 协议中有三种角色：发布者（PUBLISHER）、订阅者（SUBCRIBER）、代理（BROKER）。发布者将主题以及其对应的消息发送给代理；订阅者向代理“订阅主题”。订阅者可以接收到该主题的所有消息。

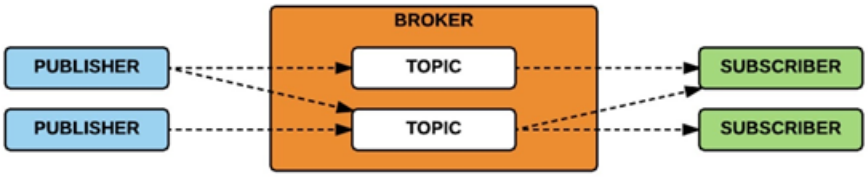



图 3.34　MQTT 模式

### 3.2.3.2　MQTT 资产暴露情况

#### 1）版本统计

如图 3.35 所示，我们对探测数据中涉及 MQTT 服务进行了版本识别与统计。共发现 32 万个 MQTT 服务，识别到 37493 个 MQTT 版本。在识别到的版本中，mosquitto version 1.4.13 占比最高，占到了 13%，其次是 mosquitto version 1.4.15， 占到了 11%。

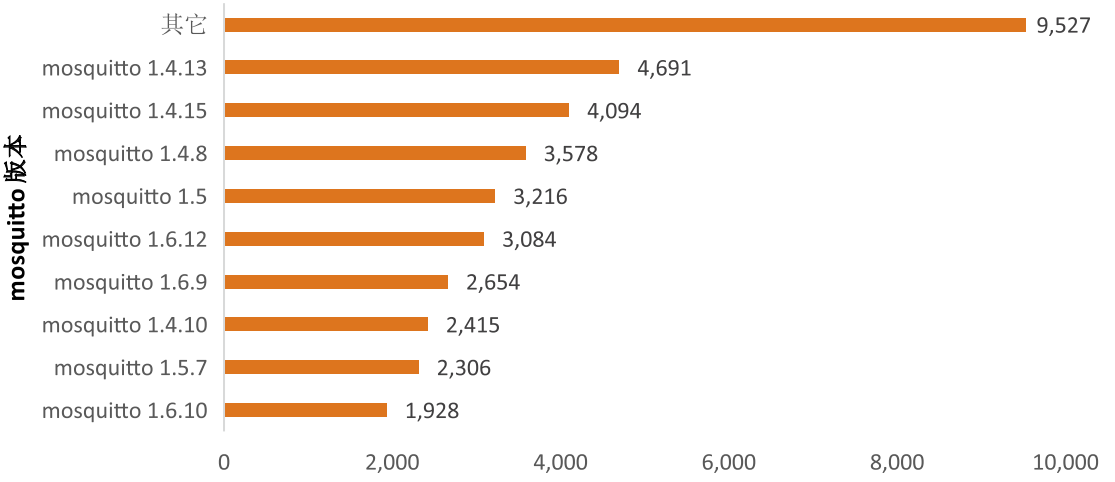



图 3.35　MQTT 版本统计

#### 2）地区分布

如图 3.36 所示，我们对探测数据中涉及 MQTT 服务的地区进行了统计。共发现 32 万个 MQTT 服务，部署在韩国占比最高，占到了 58%，其次是美国和中国，分别占到了 13% 和 5%。

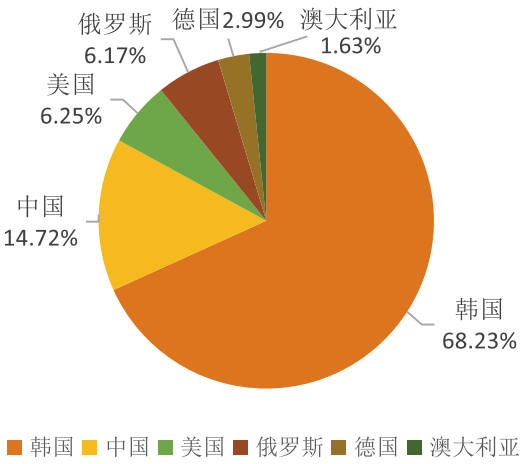



图 3.36　MQTT 服务地区分布

**3）未授权访问统计**

如图 3.37 所示，在暴露的 MQTT 资产中存在大量未授权访问情况，占到了 77%。

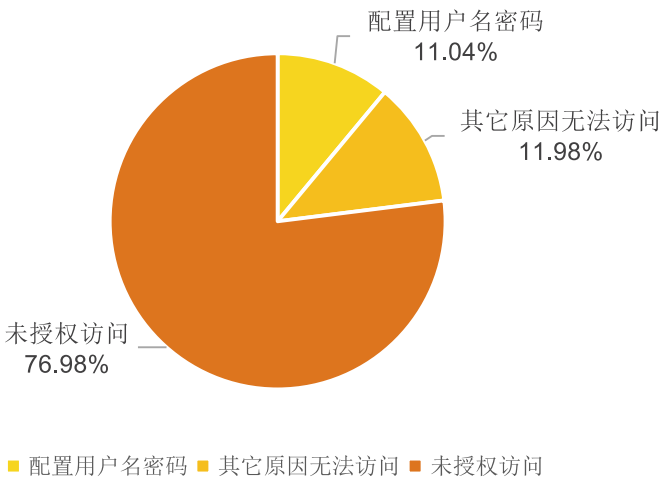



图 3.37　MQTT 未授权访问统计

### 3.2.3.3　MQTT 协议关键服务脆弱性分析——HomeAssistant

**1）HomeAssistant 简介**

HomeAssistant 是一款基于 Python 的智能家居开源系统，支持众多品牌的智能家居设备，可以轻松实现设备的语音控制、自动化等。HomeAssistant 支持内置的 MQTT 服务以及允许

用户配置自定义的 MQTT broker。

**2）HomeAssistant 暴露情况**

我们对探测数据中涉及 HomeAssistant 的服务进行统计，共发现 3142 条记录，涉及 2464 个独立 IP 地址。对 HomeAssistant 服务的地区进行统计，如图 3.38 所示，波兰占比最高，达到了 14%，其次是越南和中国。

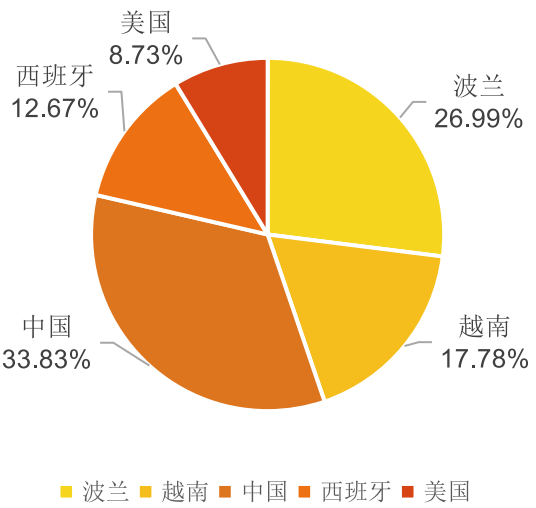



图 3.38　HomeAssistant 地区分布

**3）HomeAssistant 安全问题**

研究者可以首先查询 banner 中是否存在“MQTT Connection Code: 0”、“homeassistant”关键字。如果存在则意味着该 MQTT 服务涉及 HomeAssistant 服务，并且 MQTT 存在未授权访问。然后订阅“homeassistant/#”这个 topic，可以获得设备配置信息。根据配置信息可以得到每个设备的状态 topic 以及控制命令的 topic。根据状态 topic 可以获得设备的状态信息；根据设备控制命令的 topic，可以通过 MQTT 向该 topic 发送控制消息，达到控制设备的目的。

下面是在搭建的 HomeAssistant 服务中，模拟通过 MQTT 控制开关（switch）。图 3.39 展示了：开关 switch 最初开关的状态是关，通过向 command_topic: “home/bedroom/switch1/set”发送指令，达到了控制开关的目的。

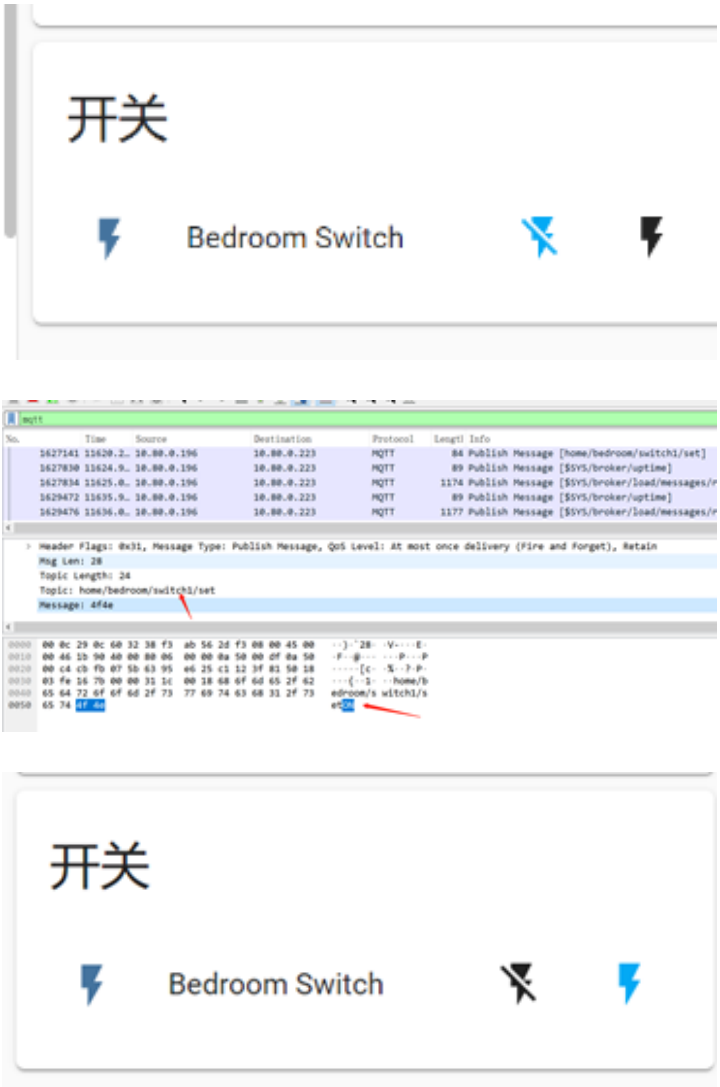



图 3.39　通过 MQTT 控制设备

### 3.2.3.4　MQTT 协议关键服务脆弱性分析——JetLinks

#### 1）JetLinks 简介

JetLinks 基于 Java8,Spring Boot 2.x,WebFlux,Netty,Vert.x,Reactor 等开发，是一个开箱即用，可二次开发的企业级物联网基础平台。JetLinks 实现了物联网相关的众多基础功能，能帮助快速建立物联网相关业务系统。JetLinks 支持设备以 TCP、UDP、MQTT、CoAP、HTTP 等协议接入系统。

### 2) JetLinks 暴露情况

如图 3.40 所示，我们在互联网暴露的服务中，发现了某 JetLinks 平台存在大量智能售货柜（嗨便利）的设备，并且可以获得设备相关的属性：

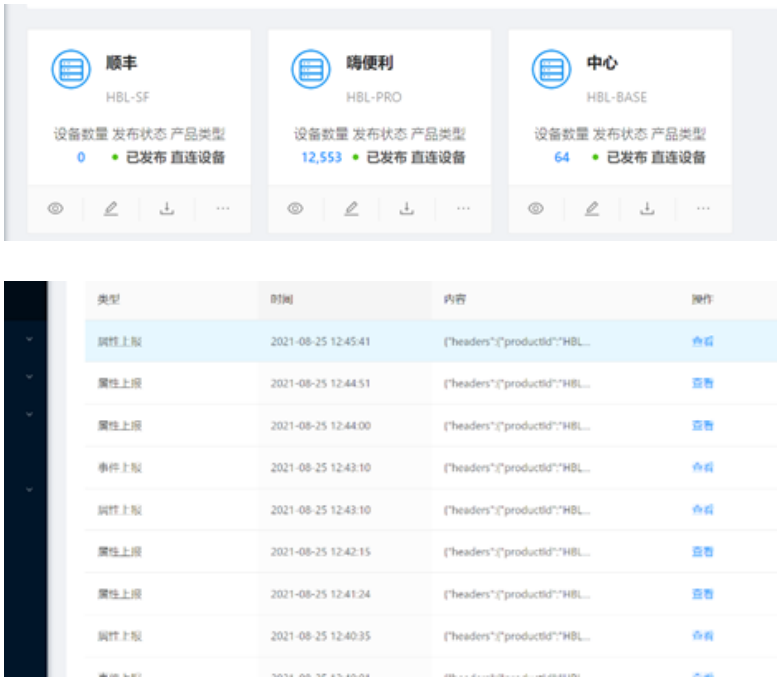



图 3.40　JetLinks 泄露案例

### 3) JetLinks 安全问题

如图 3.41 所示，在 JetLinks 中，MQTT 的连接信息以明文形式存储：

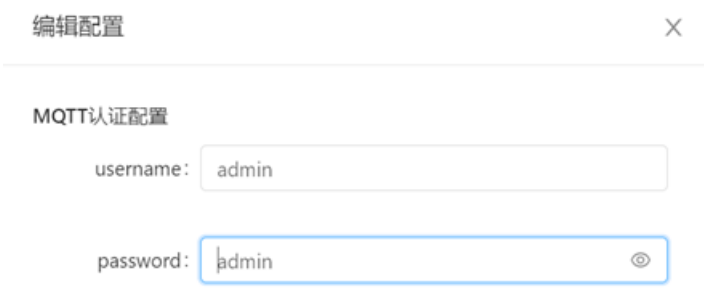



图 3.41　明文存储 MQTT 连接信息

在连接上 MQTT broker 后，攻击者可以修改设备数据，向设备发送指令。下面通过在自建的环境中，模拟修改设备的回传数据。

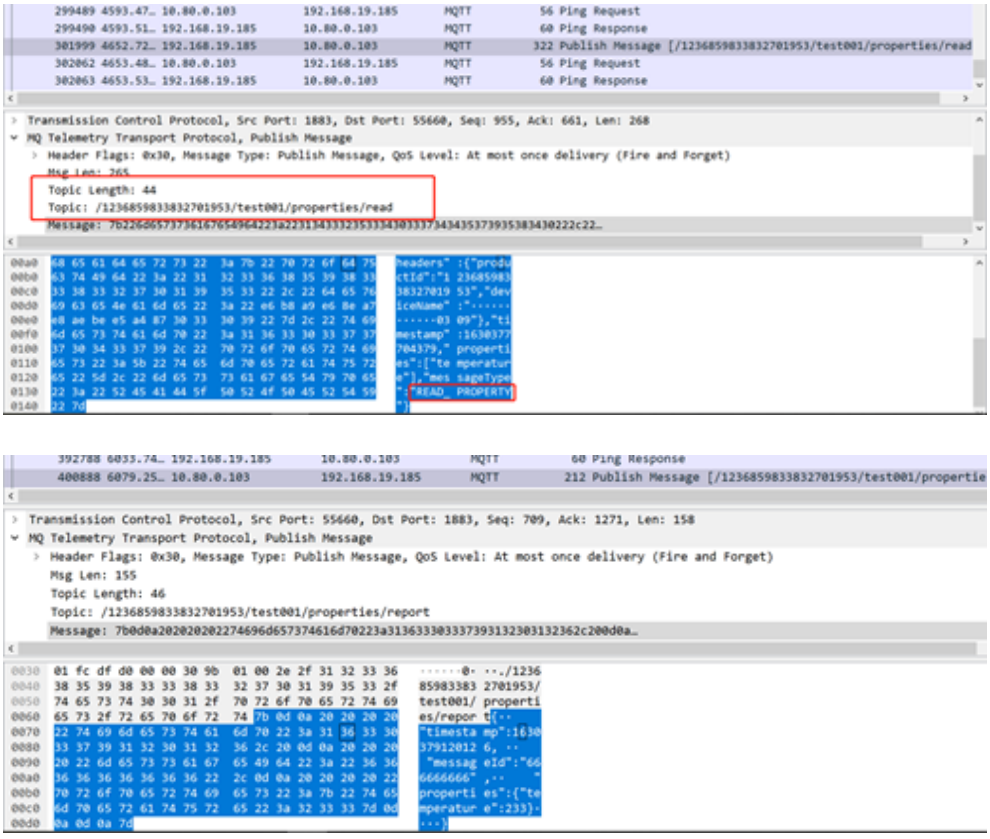







图 3.42　通过 MQTT 修改传感器数据

图 3.42 展示了：通过搭建的 JetLinks 平台，模拟篡改设备数据。攻击者登陆平台获得 MQTT 的连接信息，进一步模拟设备通过 MQTT 发送伪造的数据，达到篡改设备数据的目的。除此之外，攻击者还可以向平台发送假的告警事件、调用设备功能等。

#### 3.2.3.5 MQTT 协议关键服务脆弱性分析——ThingsBoard

**1) ThingsBoard 简介**

ThingsBoard 是一个开源物联网平台，用于收集和可视化物联网设备的数据。可以将来自物联网设备的数据发送到云服务器，在云服务器中可以通过自定义的仪表板查看或共享设备数据。ThingsBoard 通过 MQTT、CoAP 和 HTTP 实现设备连接，并支持云和本地部署。ThingsBoard 具有可伸缩性、容错性和性能优越的特点。

**2) ThingsBoard 暴露情况**

对探测数据中涉及 “ThingsBoard” 的服务进行统计，共发现 3775 条记录，涉及 704 个独立 IP 地址。对这些 IP 地址的地区信息进行统计，如图 3.43 所示：

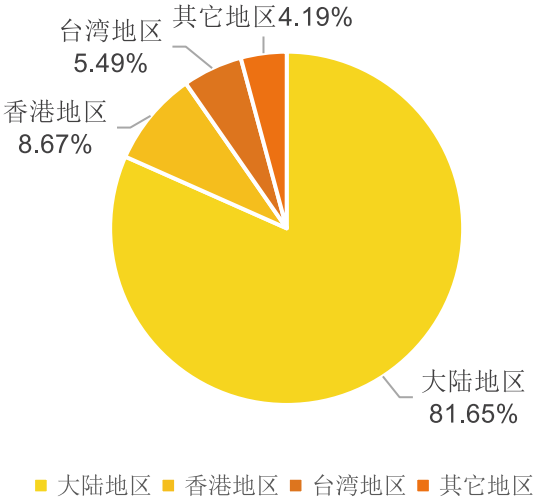



图 3.43 Thingsboard 地区分布

**3) ThingsBoard 安全问题**

如图 3.44 所示，在 ThingsBoard 中，MQTT 的连接信息以明文方式存储。

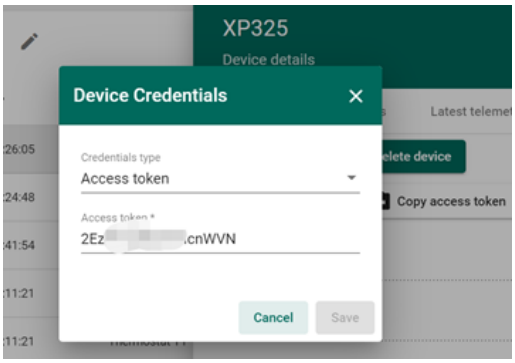



图 3.44　ThingsBoard 明文存储 MQTT 连接信息

以下是模拟通过 MQTT 篡改传入到 ThingsBoard 的数据。图 3.45 展示了通过 ThingsBoard 暴露的 Access Token 作为 MQTT 的用户名连接 MQTT broker，并且通过 MQTT 修改设备传到 ThingsBoard 的数据。

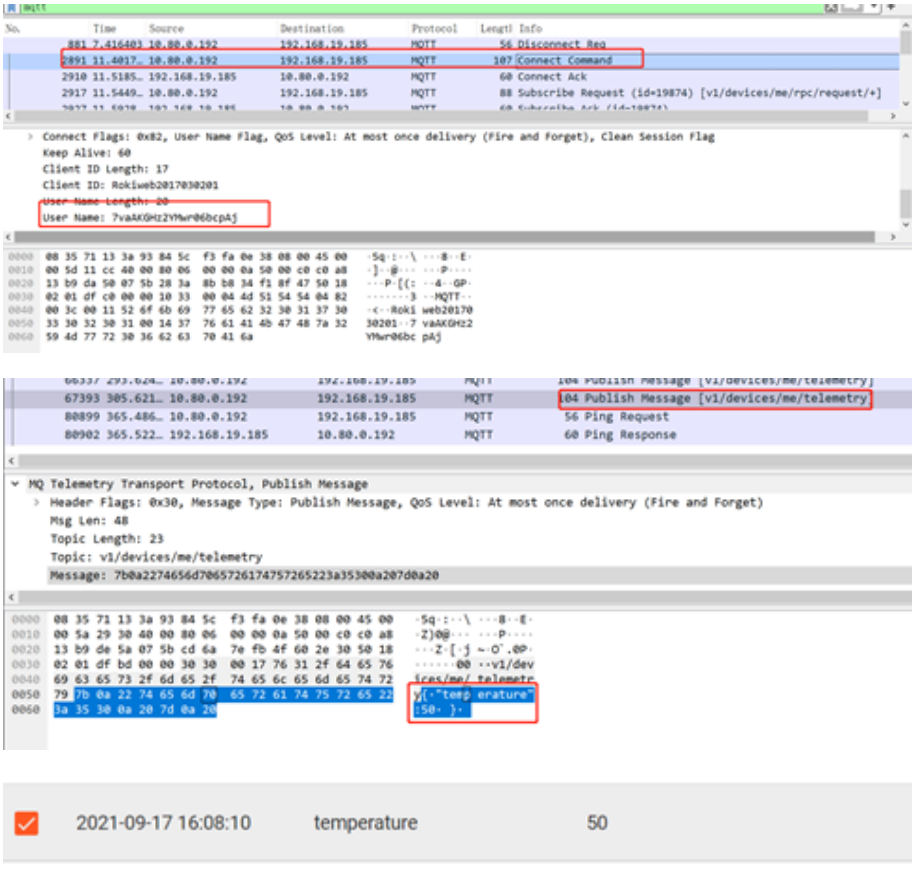



图 3.45　模拟通过 MQTT 修改设备数据

#### 3.2.3.6 MQTT 协议安全问题总结

MQTT 是轻量化的基于发布 - 订阅模式的传输协议，在物联网设备上有着广泛应用。在实际中，我们发现许多 MQTT 服务允许匿名连接，存在未授权访问问题，泄露了大量物联网设备的敏感数据。我们分析了三个涉及 MQTT 协议的平台以及服务：HomeAssistant、JetLinks 以及 ThingsBoard。智能家居平台 HomeAssistant 中的 MQTT broker 存在配置不当、允许匿名连接问题，这导致了 MQTT 未授权访问。最终泄露智能设备的敏感数据，甚至允许攻击者通过 MQTT 操控设备。JetLinks、ThingsBoard 这些开源物联网平台明文存储 MQTT 连接信息，这就导致安全出现了隐患。攻击者可以根据 MQTT 连接信息连接 MQTT broker，达到获得敏感数据、操控设备的目的。针对 MQTT 的安全问题，我们有如下建议：

1. 禁止 MQTT 匿名访问，在服务端设置认证，强制用户名密码验证。
2. 根据实际情况，优先使用加密传输数据，防止中间人攻击。
3. 使用最新的服务端程序架设服务。
4. 无论是 MQTT broker 的连接配置，还是使用 MQTT 的平台，采取复杂密码，避免弱口令。

### 3.2.4 小结

本节，我们从以对象存储为代表的公有云服务、云原生服务组件和以 MQTT 为代表的云上物联网类协议三个角度出发，对云上风险进行梳理分析。可以发现，相关服务面临着不同程度的安全风险，使用这些服务的企业需要给予足够重视。

## 3.3 应用风险分析

**观点 9：新冠疫情爆发以来，远程办公、协同办公的需求大增，大量相关服务暴露在互联网上，很多存在一个或多个安全漏洞。由于这些应用深度参与到企业生产过程中，它们的暴露风险对企业运作、业务运行有重要影响，使用这些应用的企业需要加大重视程度，监控自身业务暴露面和攻击面，非必要不暴露，及时更新修复相关安全漏洞，或积极践行零信任战略。**

本节，我们对 Confluence、Jira 为代表的协同办公应用及用于远程连接的 VPN 进行测绘分析，探讨它们可能存在的风险。

### 3.3.1 协同办公应用风险分析

**观察 8：我们针对目前市面上常见的两款协同办公软件 Confluence 和 Jira，从资产分布，版本分布以及脆弱性几个角度进行了风险分析。其中 Confluence 资产暴露数量 1799 个，Jira 资产暴露数据 4131 个。端口主要分布于 8090，以及 9090，占比均超过 7 成以上，这两个端口都是服务默认配置的端口。已识别出版本的资产中，大部分资产都没有升级到最新版本，存在着被已知脆弱性攻击利用的风险。其中命中 CVE-2021-26084 漏洞资产占比近 Confluence 总资产的 47%。命中 CVE-2021-39128，CVE-2017-17113，CVE-2021-39124，CVE-2021-26070 漏洞的资产均超过 Jira 总资产数的 86% 以上。**

#### 3.3.1.1 Confluence 应用风险

Atlassian Confluence Server 是 Atlassian 公司的一套具有企业知识管理功能，并支持用于构建企业 WiKi 的协同软件的服务器版本。

**1）Confluence 资产暴露情况分析**

我们通过分析现有的测绘数据，对 Confluence 组件资产近一个月的暴露情况进行了统计，总计数量 1799 条。下面将从地区分布、端口分布等维度分别进行介绍。

a）地区分布

从图 3.46 地区分布可以看出，国内 Confluence 主要分布于北京，上海，浙江，广东地区，北京市以 554 条数据位居第一。

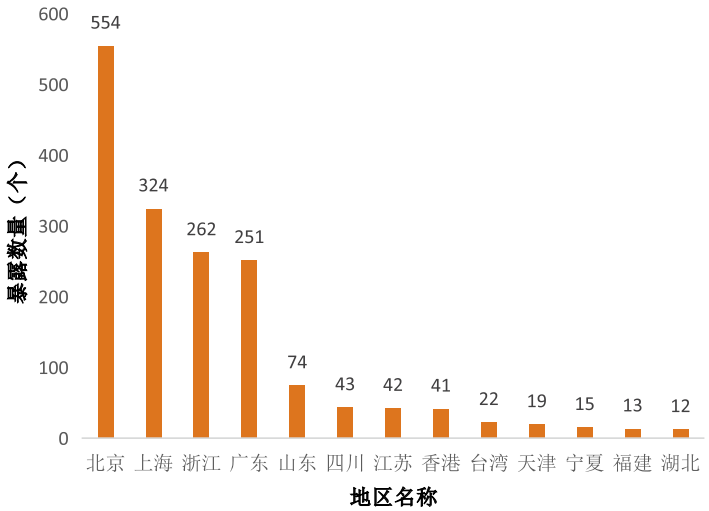



图 3.46　Confluence 地区分布情况

b) 端口分布

从图 3.47 可以看出，端口主要集中在默认的 8090 端口，占比超过 76%。

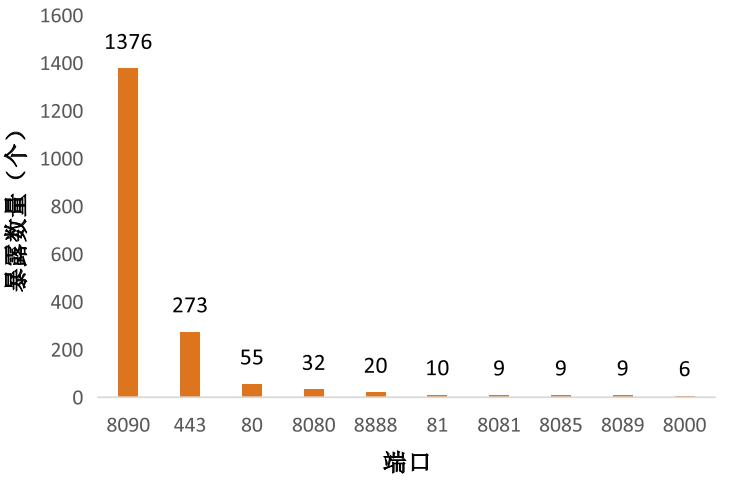



图 3.47 Confluence 端口分布情况

c) 版本分布

如图 3.48 所示，在可以识别出的版本的数据中，7.x 版本占据 6 成，6.x 版本及更低版本占据 4 成。Confluence 目前的最新版本 7.15.0。已知版本服务都没有升级到最新版本。低版本的服务可能存在已知的 Nday 的漏洞，存在较高的被攻击利用的风险。

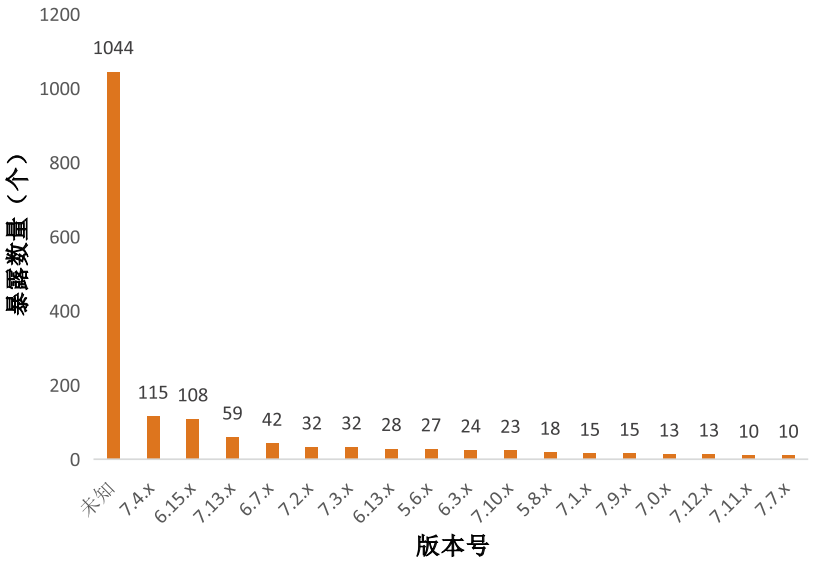



图 3.48 Confluence 版本分布情况

**2）Confluence 脆弱性暴露情况分析**

根据识别出的资产的版本信息以及公开出来的 CVE 脆弱性影响的资产的数据可以得出 Confluence 资产的脆弱性的影响情况如图 3.49 所示。

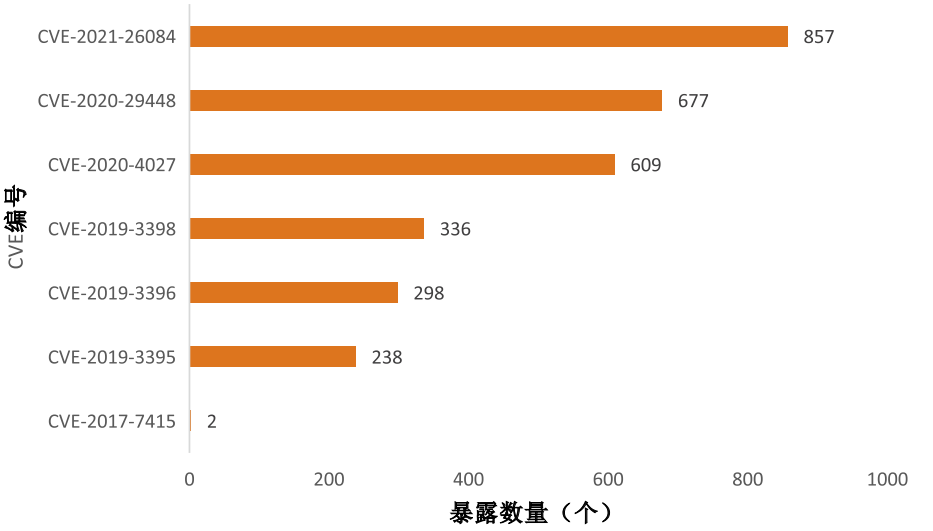



图 3.49　Confluence 脆弱性分布情况

在已识别出版本信息的资产中，大量的服务都运行在老旧版本之上，存在被攻击利用等风险。根据脆弱性分布情况可以看出，其中最新出现的 CVE-2021-26084 影响资产数量为 857 条。即使是 CVE-2020-29448，CVE-2020-4027 等出现了已经 1 年多的脆弱性问题，也有着很高的影响面。建议用户尽早升级最新版本服务。

### 3.3.1.2　Jira 应用风险

Jira 是 Atlassian 公司出品的项目与事务跟踪工具，被广泛应用于缺陷跟踪、客户服务、需求收集、流程审批、任务跟踪、项目跟踪和敏捷管理等工作领域。Jira 中配置灵活、功能全面、部署简单、扩展丰富，其超过 150 项特性得到了全球 115 个国家超过 19,000 家客户的认可。

**1）Jira 资产暴露情况分析**

本次总计统计国内资产数量 4131 台。根据地区分布情况、端口分布和版本分布等维度进行分析。

a）地区分布

从图 3.50 地区分布可以看出，国内 Jira 主要分布于香港，北京，上海，广东，浙江地区，

香港以 1703 条数据位居第一。

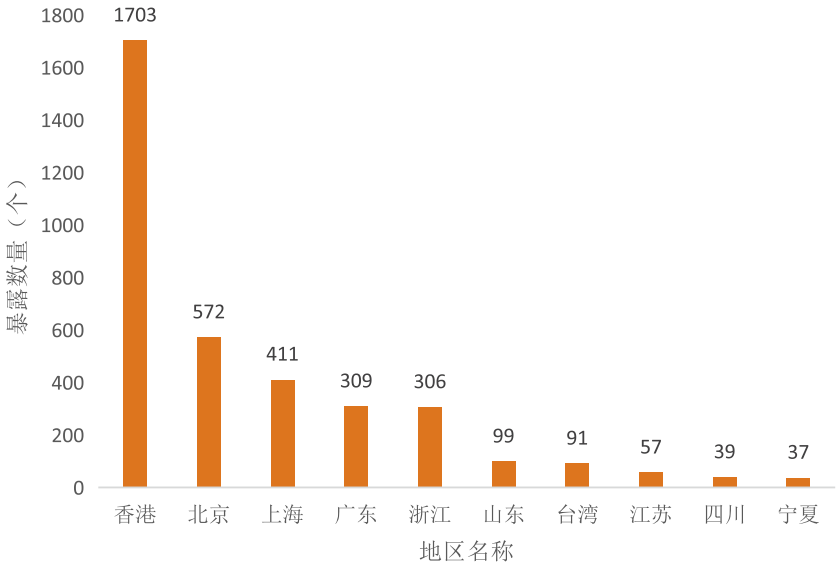



图 3.50　Jira 地区分布情况

b)　端口分布

如图 3.51 所示，端口主要集中在 9090、8080、443，其中默认端口 9090 的数据 2024 条数据位居第一。

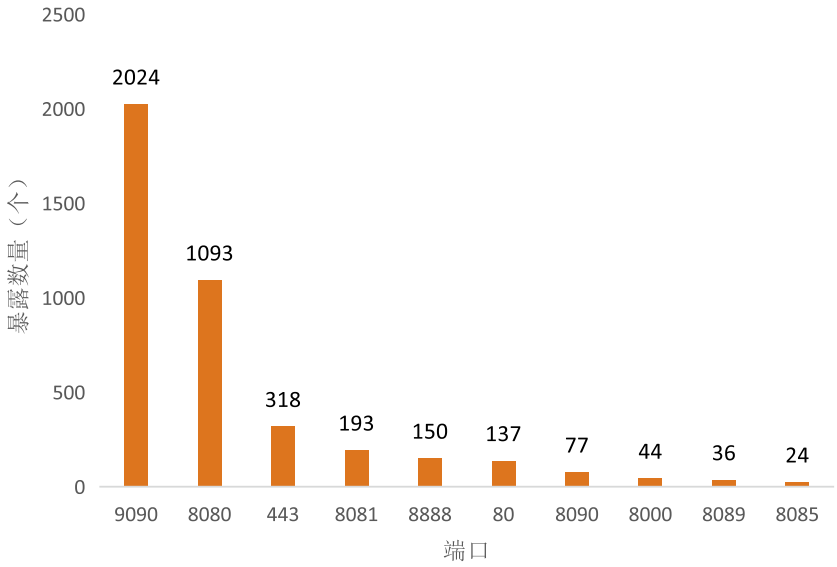



图 3.51　Jira 端口分布情况

c) 版本分布

如图 3.52 所示，版本分布情况中，8.13.2 版本以占据近 7 成的份额位列第一。目前 Jira 最新版本已经到 8.20.2 版本，这些低版本的 Jira 服务很可能存在各种已知的漏洞，存在被攻击利用的风险。

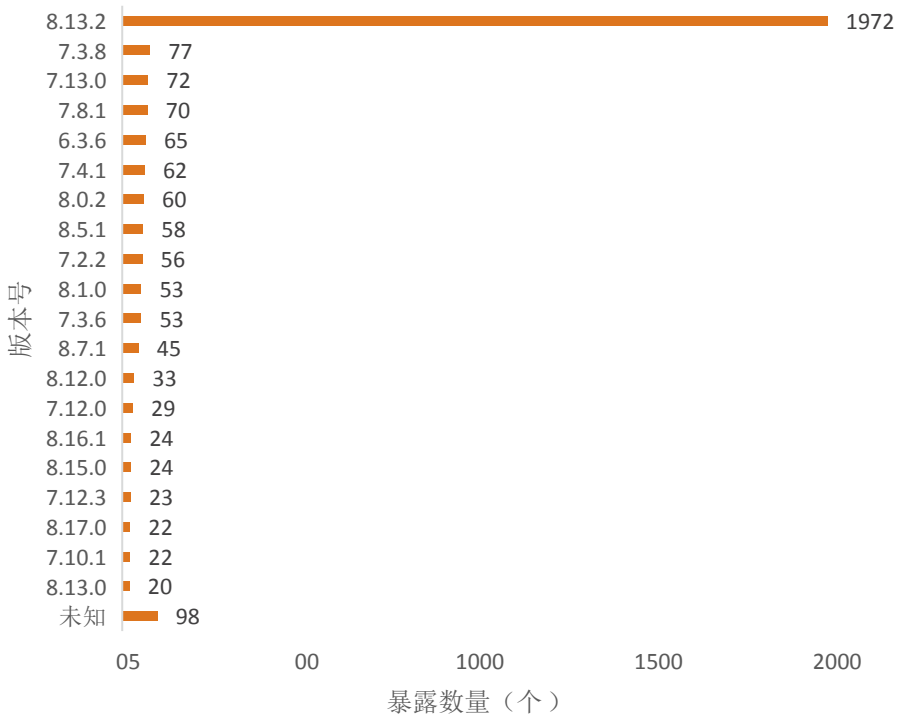



图 3.52　Jira 版本分布情况

**2) Jira 脆弱性暴露情况分析**

根据识别出的资产的版本信息以及公开出来的 CVE 脆弱性影响的资产的数据可以得出 Jira 资产的脆弱性的影响情况如图 3.53 所示，其中 CVE-2021-39128，CVE-2017-17113，CVE-2021-39124，CVE-2021-26070 都有着很高的覆盖面。

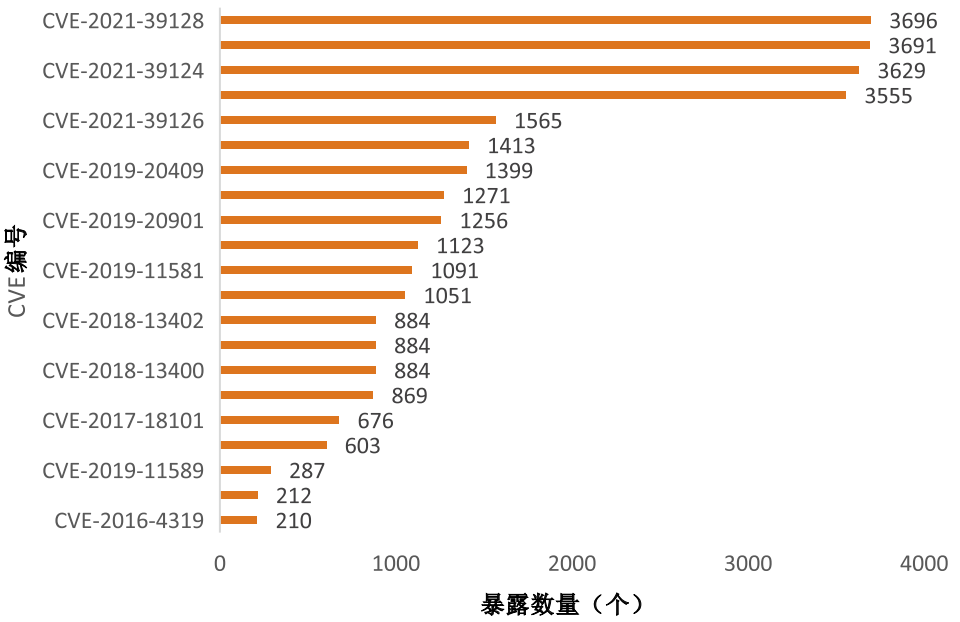



图 3.53　Jira 脆弱性分布情况

在脆弱性影响数据中可以看出，由于大部分的 Jira 服务都是运行的旧版本的服务，存在各种已知的脆弱性，其中不乏各种高危漏洞。在近期暴露的脆弱性风险中，CVE-2021-39128，CVE-2017-18113，CVE-2021-39124，CVE-2021-26070 这几个的脆弱性的影响面都超过了 80%，因而建议相关用户尽快升级到新版本服务。

### 3.3.2　VPN 风险分析

**观察 9：根据《Global Market Insights 2020》调查，到 2026 年，全球 VPN 市场预计将同比增长 12%，价值 700 亿美元。由于 VPN 产品在企业网络中的重要性，其安全性常被黑客关注，尤其是销量靠前的产品，一旦曝出相关漏洞，往往评分较高，波及范围较广，例如已经被黑客武器化的数个 VPN 漏洞，Pulse Secure “Connect” VPN(CVE-2019-11510)、Fortinet FortiOS VPN(CVE-2018-13379) 和 Palo Alto Networks “Global Protect” VPN(CVE-2019-1579)，这些漏洞至今仍能对企业安全造成严重危害。**

2020 年 2 月，以色列网络安全公司 ClearSky 发布报告 [40]，曝出伊朗“Fox Kitten”的网络间谍计划——利用未修补的 VPN 漏洞作为切入点，向全球政府和企业植入后门，引发安全界热议。在新冠疫情全球爆发、企业 VPN 使用量激增的背景下，我们要加大对 VPN 相关风险的重视程度。

本节将以 SonicWall 的 VPN 产品为例，对暴露在互联网上的 SonicWall SSL-VPN 服务进行发现与识别，基于所发生过的安全事件并梳理其脆弱性列表，对 SonicWall SSL-VPN 的脆弱性进行分析。

SonicWall 作为硬件防火墙、VPN 网关及网络控制设备制造商，在网络安全领域具有领先地位，是提供安全解决方案的佼佼者。该公司的 SSL-VPN 设备为中小型企业提供了易于使用的 VPN 解决方案。通过 VPN 设备在传统数据中心与 VPC 之间建立通信隧道，我们可方便地使用云平台的云服务器、块存储等资源。

#### 4.3.2.1 SonicWall VPN 资产暴露情况分析

**1）地区分布**

从现有测绘数据中查询到 184 条数据，其中地区分布情况如图 3.54 所示：

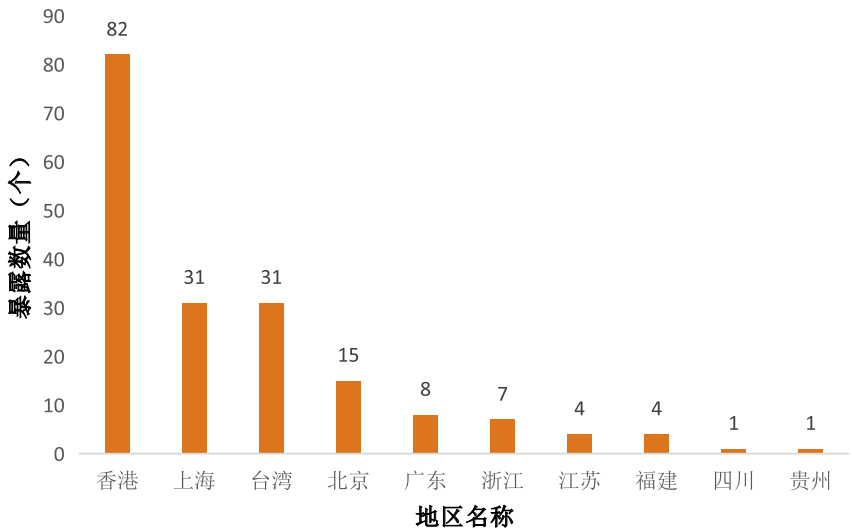



图 3.54 Sonicwall VPN 资产地区分布

**2）端口分布**

端口分布情况如图 3.55 所示：

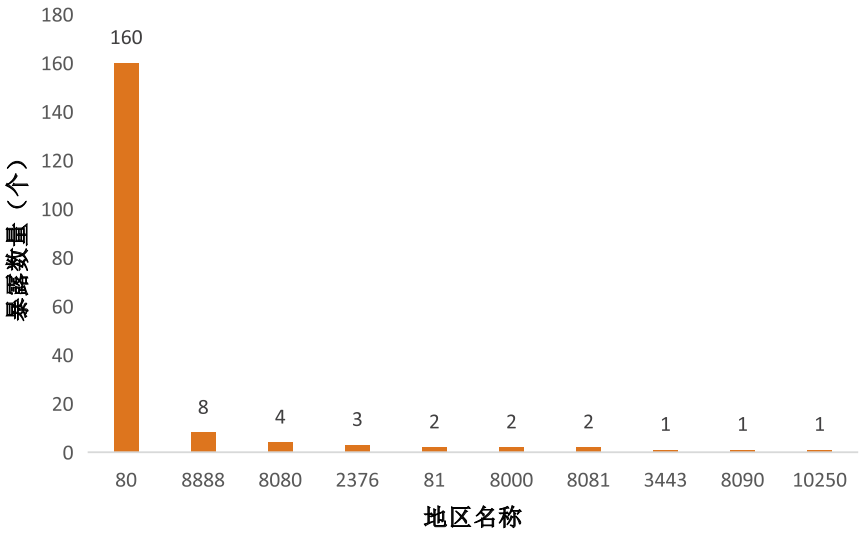



图 3.55　Sonicwall VPN 资产端口分布

国内暴露的 SonicWall VPN 资产中约 78% 来源于香港、上海市、台湾省等地区，其中香港地区占据第一，暴露 82 条

国内暴露的 SonicWall VPN 资产主要分布在 80 端口，占暴露资产的 87%，极少数分布在 8888 端口、8080 端口等

### 3) 版本分布

版本分布情况如图 3.56 所示：

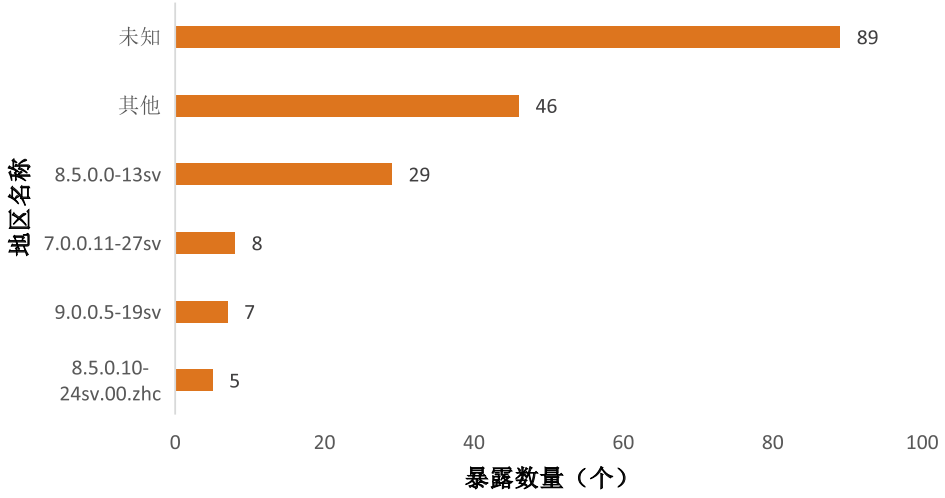



图 3.56　Sonicwall VPN 资产版本统计

#### 3.3.2.2 SonicWall VPN 脆弱性暴露情况分析

脆弱性分布情况如图 3.57 所示：

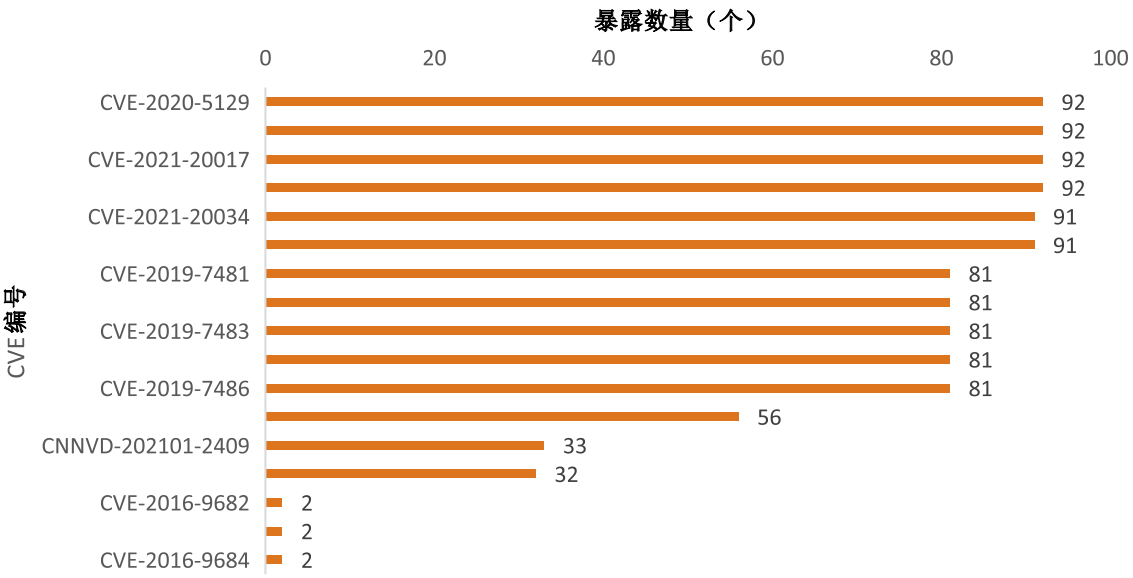



图 3.57 Soniwall VPN 资产脆弱性分布

通过对国内暴露的 VPN 资产进行静态和动态的脆弱性分析，发现 2019、2020、2021 年曝出的 CVE 影响面较大，占已知资产的 44%-50%，其中有 CVSS2.x 评分 9.0 的 CVE-2020-5146 和 CVSS2.x 评分 10.0 的 CVE-2016-9682、CVE-2016-9683、CVE-2016-9684。

因为产品本身的定位在公司企业网络中比较核心，所以针对该产品的漏洞挖掘工作积极性较高，一旦出现漏洞，影响面较为广泛。其中不少漏洞有公开的利用代码，在漏洞曝出之际至今，仍持续有在野利用的情况。

### 3.3.3 小结

蔓延全球的新冠疫情加速了远程协同办公应用生态的发展，推动了生产方式和合作模式的转型，这一趋势在可预见的未来将继续发展。然而，以上对协同办公应用和 VPN 应用的测绘分析发现，无论是 Confluence、Jira 还是 SonicWall VPN，都存在一定程度的脆弱性。显而易见的是，这些暴露资产的漏洞一旦被攻击者恶意利用，将会对相关业务造成损失，甚至可能导致长期的数据泄露等严重后果。因此，我们建议相关用户在使用这些产品时及时升级产品或更新补丁，避免受到漏洞影响，造成不必要的损失。

## 3.4 工业互联网风险分析

**观点 10：工业互联网风险面广、涉及行业多、造成的潜在风险大。安全风险主要来源于管理和技术这两个层面。工业互联网的风险往往关乎民生，生产与制造加工涉及的设备、网络、控制、数据、平台、工业 APP 等都可能成为突破口。**

### 3.4.1 工业互联网漏洞现状

工业互联网相关漏洞数量的上升趋势源于攻击者、研究人员和防御者同时参与了这场竞赛——寻找隐藏在工业网络中的漏洞。积极看待这一趋势的话，可以发现这是安全界对工业互联网中设备、产品等投入更大关注的明确信号，让很多存在于工业设施中多年的漏洞公之于众，而不是仅被少数知悉漏洞的恶意行为者暗中利用。

以下图表数据来自中国国家信息安全漏洞共享平台（CNVD）发布的漏洞信息：

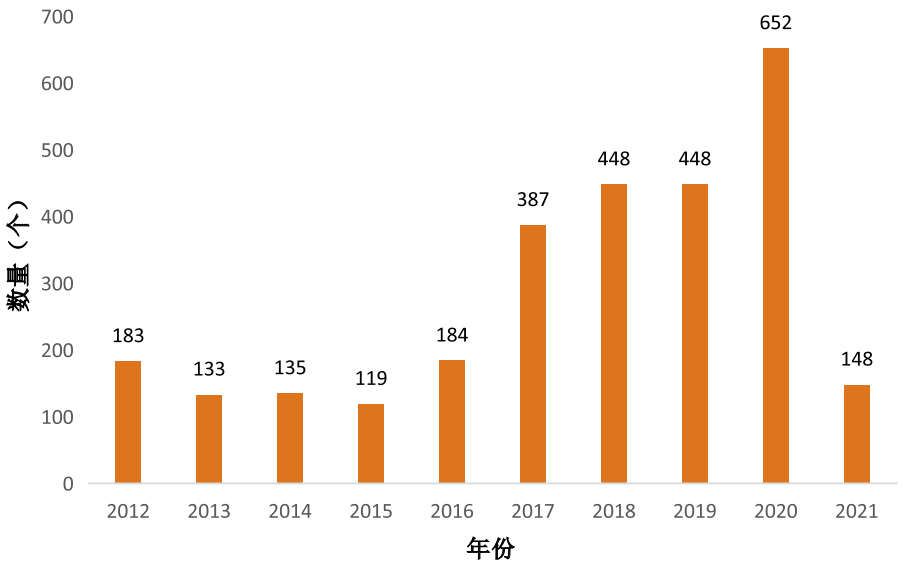



图 3.58 中国国家信息安全漏洞共享平台 CNVD 漏洞信息统计

以下图表数据来自美国工业控制系统网络应急响应小组（ICS-CERT）发布的漏洞信息：

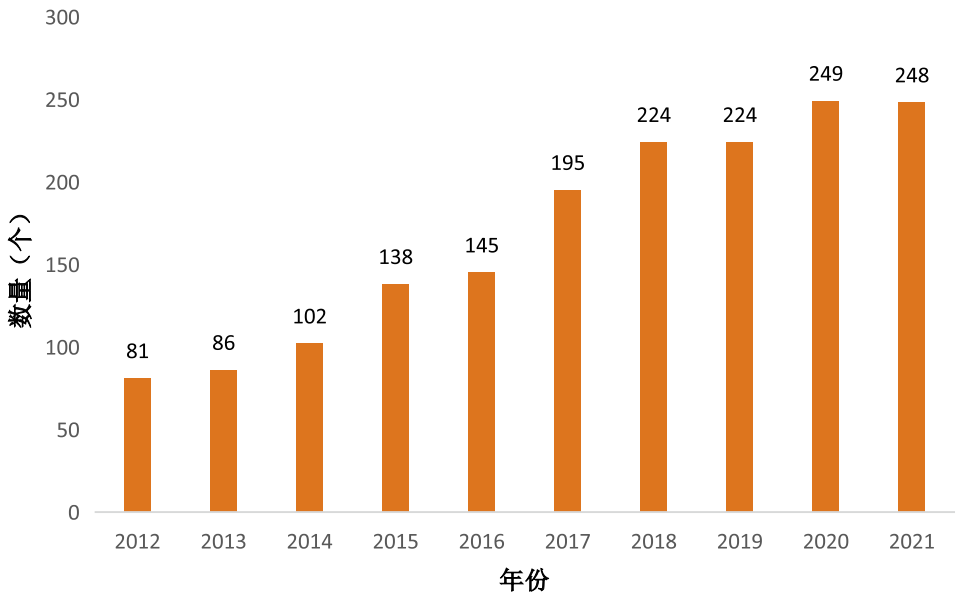



图 3.59　美国工业控制系统网络应急响应小组（ICS-CERT）漏洞信息

根据近些年各漏洞库收录的情况，大部分漏洞源于普度模型中的 LV3 级别，也就是操作管理方面，以及 LV2 级别的监控管理方面。剩下的漏洞集中于 LV1 的基本控制层以及更高的 IoT 层面。

缓解漏洞所带来风险的一个重要举措是及时为受影响设备打上补丁，不过前提是补丁已被发布了，那么现实中漏洞的修补情况如何呢？根据 Dragos 发布的报告统计显示，在其 2020 年分析的 703 个 ICS/OT 漏洞中，78% 的漏洞有可用补丁，剩下 22% 的在漏洞公告发布时并未提供补丁，而且在没有补丁的漏洞中，又有 64% 的漏洞甚至没有缓解建议。这部分既没有补丁又没有缓解建议的漏洞为企业带来的风险不言而喻。因此对于这种情况，严格管控暴露在互联网上的设备、有计划的进行应急演练、尽快实施网络分区与边界防护就尤为关键。

## 3.4.2　工业互联网风险

面对频频被发现的工业控制系统漏洞，工业互联网的风险主要包括技术层面的设备和网络安全以及管理层面的人员和操作流程规范。

### 3.4.2.1　工业互联网设备与网络安全风险

工业互联网设备是指应用在工业互联网领域内具备灵敏准确感知能力及行之有效的执行能力的智能设备，例如 PLC、SCADA、边缘网关以及智能机器人等。当前工业互联网设备正处于快速增长的发展阶段，设备制造商往往只注重产品的可用性和易用性，受限于硬

件资源、很难实现细粒度的系统安全措施，导致设备存在较多的安全缺陷。另外，真实的制造环境中往往需要多种类型、多个厂商的工业互联网设备协同工作，在缺乏统一安全技术要求规范来保证整个系统交互安全的情况下，大大增加了攻击面，给工业互联网的安全建设带来严峻的挑战。

**风险点 1：工业互联网设备自身安全防护手段薄弱。**

由于工业互联网智能设备软件更新缓慢以及对漏洞的不重视，导致大量暴露在互联网上的设备存在安全漏洞，攻击者可以利用精心构造的完整攻击链路，获取更高的系统权限。

已知风险信息的碎片化为漏洞排查增加了困难，却为攻击带来了便利，攻击者可以获取固件中的第三方库版本信息并查询相应版本的漏洞信息，就能轻而易举地获得固件存在的潜在风险。

开发阶段人员安全意识不足，在开发阶段引入不安全的第三方库文件、使用弱口令、硬编码密钥等，都极易引发严重的安全问题。

**风险点 2：工业互联网设备被用作跳板攻击其他在线运营系统。**

暴露在互联网上的智能设备，由于数量庞大，为承载分布式拒绝服务功能的恶意样本进行扫描和传播提供了便利，攻击者可以利用类似僵尸网络的技术，以工业互联网的智能设备为僵尸节点，向其他在线运行系统发起分布式拒绝服务攻击。

工业互联网的发展使得工厂内部的网络呈现 IP 化、无线化、组网灵活化与全局化的特点，工厂外部呈现出信息网络与控制网络的逐渐融合、企业专网与互联网融合等特点，这就导致了传统互联网中的安全风险开始向工业互联网蔓延。

工业互联网标识解析系统是工业互联网网络体系重要的组成部分，是支撑工业互联网互联互通的重要枢纽。整个系统涉及工业互联网终端、解析系统、网络、工控系统以及各种通信协议和软硬件，呈开放式与互联网相连接，势必为工业互联网标识解析发展带来许多新的安全隐患。工业互联网标识解析系统的安全风险主要为如下方面：

- 架构安全风险（节点可用性、节点协同风险、节点关联性等）
- 数据安全风险（数据窃取、数据篡改、隐私泄露等）
- 运营安全风险（访问控制、业务连续性等）
- 身份安全风险（身份认证、越权访问等）

#### 3.4.2.2 工业互联网管理风险

除了以上主要源于技术层面的风险点，工业互联网整体生产流程中的管理层面也面临很大挑战，涉及工业生产流程的数据、服务平台和 APP 等。企业管理人员除了需要部署必要的安全设备，提高生产环境对抗外部攻击的防御能力，还需要对操作员和技术人员进行针对性的培训，从管理方面杜绝可能发生的内部安全隐患。例如制定操作指南，从而规范操作员在处理关键设备和操作时的合理行为。通过针对性的培训，提高操作员的安全意识并且杜绝一些安全隐患，例如使用弱密码。

工业互联网的管理相较于传统互联网还处于发展阶段，没有成熟完善的体系可以参考，因此在工业控制场景由闭塞向开放转型的同时，需要确保人员的意识和操作也在同步转型。

### 3.4.3 小结

工业互联网安全涉及 IT 系统安全和 OT 系统安全。由于工业互联网安全包括设备、网络、控制、数据、平台、工业 APP 等多个方面，一味套用过去 IT 系统的安全策略无法全面覆盖攻击面，一旦发生安全隐患，会威胁到工业生产运行安全、人员生命安全甚至国家安全。因此在处理工业互联网安全时，除了技术层面需要提高安全性，还需要结合相关的政策法规、安全评估管理、人员操作流程规范，确保安全隐患提早发现、及时定位和迅速恢复。

## 3.5 小结

本章主要对网络空间关键领域的风险进行分析。首先，我们分析了物联网相关的年度漏洞披露情况，2021 年 NVD 公布的物联网相关漏洞相比 2020 没有明显的变化趋势，相关漏洞仍具有攻击复杂度低、危害评级高的特点；第二部分对公有云对象存储服务、云原生组件和 MQTT 协议等云计算领域风险进行了测绘分析；最后，我们对远程协同办公应用风险进行梳理和分析；接着，介绍了工业互联网领漏洞趋势以及工业互联网的设备、网络、控制、数据、平台、工业 APP 等方面的风险点。通过这些分析可以发现，网络空间中不同领域服务均存在不同程度的安全风险，且随着相关领域的发展而呈现上升趋势，企业需要对这些安全问题给予足够重视。

# 04

# 总结与展望

随着云、大、物、移、智等新技术发展以及数字化转型的落地，必定会有越来越多的新兴的资产服务出现在互联网上，对这些服务的暴露面以及脆弱性管理对于网络安全而言仍是重要挑战。回顾 2021 年的安全事件，可以总结出近年来网络空间资产的安全风险点，第一，供应链安全，对类似物联网产业这种软硬件产业结构复杂的产业，厂商在管理好自身安全的同时还需要关注供应链安全，采购安全可信的网络产品和服务。第二，勒索病毒，2017 年 WannaCry 利用“永恒之蓝”漏洞进行全球大范围的勒索，勒索病毒才真正被关注到，直至今天各类新型勒索病毒以及变种依层出不穷，尤其是大型的工业生产企业更应该关注暴露服务是否存在被勒索的风险，业务与安全应同步建设。第三，错误配置，弱口令和未授权访问等是老生常谈的问题，但仍然有大量存在错误配置的资产服务暴露在互联网上，甚至包括安全设备，错误配置虽然是低级漏洞，但是有着高级的风险，企业安全管理人员需做好资产核查工作，收敛企业的暴露面。第四，敏感数据泄露，近年来数字化转型的步伐加快，数据价值进一步突显，敏感数据泄露不仅损害企业的声誉和业务，如果隐私数据被诈骗团伙利用，将会影响人身财产安全，所以为了避免企业相关数据泄露事件发生，应该未雨绸缪，对重要的数据资产服务器进行重点防护与安全配置检查，定期进行漏洞扫描与评估等措施。总之，2021 年网络攻击趋势仍在持续攀升中，供应链、勒索病毒、错误配置、数据泄露仍是安全需要关注的重点问题。

网络空间资产暴露方面，随着 IoT、5G、云原生等技术发展，将会有更多的新兴资产和服务出现，业务资产暴露也会给企业组织带来了安全风险。摸清企业资产的暴露面，洞察网络风险是建立网络安全防御体系的第一步，也是最重要的一步。攻击者的目标已经不仅放在传统的 IT 资产上面了，VPN、公有云服务、第三方供应链以及物联网设备等都可成为企业的攻击入口。企业的系统随着技术和业务的拓展，其资产信息也断的在变化，对外公开的系统的脆弱性当然也随之发生变化。所以必须实时掌握对企业暴露的资产情况，力争优先于攻击者发现其自身脆弱性，并且对修复进度情况跟踪，这样才可以减少受到攻击的可能性，降低防守成本。

网络空间资产脆弱性方面，我们对网络空间关键领域的风险进行分析。首先分析了物联网相关的年度漏洞披露情况，2021 年 NVD 公布的物联网相关漏洞相比 2020 没有明显的变化趋势，相关漏洞仍具有攻击复杂度低、危害评级高的特点；接着，对公有云对象存储服务、云原生组件和 MQTT 协议等云计算领域资产和服务面临的风险进行了测绘分析；然后，我们对远程协同办公应用风险进行梳理和分析。最后，我们介绍了工业互联网领漏洞趋势以及工业互联网的设备、网络、控制、数据、平台、工业 APP 等方面的风险点。通过这些分析可以

发现，网络空间中不同领域服务均存在不同程度的安全风险，且随着相关领域的发展而呈现上升趋势，企业需要对这些安全问题给予足够重视。

最后，随着《关键信息基础设施安全保护条例》、《网络安全审查办法》和《网络数据安全管理条例》等法律法规政策的相继出台、实施，合规性要求将对网络空间资产安全态势起到正向促进作用。同时，对网络空间资产的暴露面和脆弱面进行持续测绘，起到长效监控作用，从而引起企业重视，未雨绸缪，防微杜渐，帮助企业收敛暴露面、修补安全漏洞。

# 参考文献


[1] https://0797cx.cn/zc?article_id=101270

[2] http://www.sc2p.com/guoji/20210902/25547.html

[3] https://watchfulIP.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html

[4] http://blog.nsfocus.net/darkside-colonial/

[5] https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/

[6] https://www.missionsecure.com/blog/solarwinds-fireeye-hack-urgent-case-for-cyber-attack-prevention-versus-detection-in-ot-ics-networks

[7] https://www.cnvd.org.cn/patchInfo/show/270661

[8] https://www.cisa.gov/uscert/ncas/current-activity/2021/04/02/fbi-cisa-joint-advisory-exploitation-fortinet-fortios

[9] https://www.ic3.gov/Media/News/2021/210402.pdf

[10] https://www.websiteplanet.com/blog/dreampress-leak-report/

[11] https://www.hackread.com/polecat-data-analytics-data-breach-30tb-data-exposed/

[12] https://fachanwalt-it.blogspot.com/2011/12/hackerangriff-anonymous-goldde-lka.html

[13] https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

[14] https://www.trendmicro.com/en_nl/research/21/e/teamtnt-targets-Kubernetes--nearly-50-000-IPs-compromised.html

[15] https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera

[16] https://www.uptycs.com/blog/team-tnt-deploys-malicious-docker-image-on-docker-hub-with-pentesting-tools

[17] https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html

[18] https://www.wiz.io/blog/chaosdb-how-we-hacked-thousands-of-azure-customers-databases

[19] https://www.wiz.io/blog/chaosdb-explained-azures-cosmos-db-vulnerability-walkthrough

[20] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=linux

[21] https://docs.microsoft.com/en-us/azure/virtual-network/what-is-IP-address-168-63-129-16

[22] http://blog.nsfocus.net/wp-content/uploads/2021/01/2020-IoT-Security-Annual-Report.pdf

[23] https://www.sdnlab.com/25419.html

[24] https://cn.technode.com/post/2018-09-30/alibaba-aliyun-shandong-innovation-center/

[25] https://sichuan.scol.com.cn/ggxw/201706/55931536.html

[26] http://www.gz.xinhuanet.com/2021-09/12/c_1127853073.htm

[27] https://www.huaweicloud.com/theme/562437-1-H

[28] https://nti.nsfocus.com/api/v1/search/getReportPDF/?file=Industry_Internet_Security_Trend_Research_20211018.pdf

[29] https://nvd.nist.gov/

[30] https://www.exploit-db.com/

[31] https://github.com/tencentyun/qcloud-documents/blob/master/product

[32] https://github.com/nagwww/s3-leaks

[33] https://businessinsights.bitdefender.com/worst-amazon-breaches

[34] https://www.helpnetsecurity.com/2019/09/23/s3-bucket-security/

[35] https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/userguide/VirtualHosting.html#virtual-hosted-style-access

[36] https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html

[37] https://fuzzer.secapps.com/

[38] https://yago-knowledge.org/

[39] https://github.com/sa7mon/S3Scanner

[40] https://www.clearskysec.com/fox-kitten/

NSFOCUS绿盟科技

扫描绿盟科技官微二维码
可在手机端直接观看报告电子书