WebRAY 盛邦安全 | 股票代码 688651

让网络空间更有序

网络空间资产测绘与反测绘年度报告

2024

指导单位：

中国指挥与控制学会

联合发布单位：

清华大学

远江盛邦安全科技集团股份有限公司

中国指挥与控制学会网络空间测绘专业委员会

版权声明

报告撰写单位及撰写人：

清华大学

远江盛邦安全科技集团股份有限公司

权晓文、何鹏程、杨伦、李新征

前 言

随着云计算、物联网（IoT）、大数据、人工智能等新兴技术的广泛应用，企业的网络环境日趋复杂，网络空间资产在规模、类型与分布上呈现出高度动态性与异构性。与此同时，网络安全威胁持续演进，高级持续性威胁（APT）、零日攻击、数据泄露、供应链安全事件层出不穷，对网络空间资产的可见性与安全防护能力提出了更高要求。

网络空间资产测绘，作为保障网络空间安全的关键能力之一，指通过技术手段对分布于网络中的各类资产进行全面发现、分类与定位，为用户提供准确、可持续的数据支持与风险评估依据。它融合了计算机网络、数据挖掘、人工智能与信息安全等多个领域的理论与实践，是一门新兴的交叉学科。其核心目标在于系统揭示网络资产的分布格局、属性特征、关联关系及其动态变化过程，为科学研究、行业治理和政策制定提供坚实的数据基础。

在全球数字化进程加速、网络边界愈发模糊的今天，网络空间资产测绘的重要性日益凸显，已成为学术界、产业界及监管机构的共同关注焦点，相关技术和实践也正加速落地。本报告旨在系统梳理过去一年网络空间资产测绘与反测绘的最新动态与发展趋势，帮助企业、研究机构与政策制定者全面理解当前面临的风险、挑战与应对路径。我们希望本报告不仅作为了解网络空间资产测绘与反测绘现状的重要窗口，也能为相关从业者提供具有前瞻性、可操作性的决策参考与技术启发。

目录

Contents

Part I 全球网络空间资产测绘

Part II 网络空间资产反测绘

Part III DayDayMap 介绍

Part 1

全球网络空间资产测绘

1. 背景

1.1. 网络空间资产测绘定义和重要性

《GBT 20984-2007 信息安全技术 信息安全风险评估规范》中，对于资产的定义为“对组织有价值的信息或资源，是安全策略保护的对象”，网络空间资产本质是各种信息资源的集合，它不仅包含网络和主机，还包括运行在网络和主机上的数据、软件和服务，面对网络空间资产的特殊性，在资产的风险管理方面，不仅关注资产归属，其风险、资产的变更情况以及资产联通关系等同样是资产管理的核心关注点。

美国“智库”兰德公司曾断言“工业时代的战略战是核战争，而信息时代的胜利则取决于网络战。”随着《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等法律法规颁布，网络空间安全所承载的战略价值不言而喻。作战必先有“图”，因此，发展网络空间测绘能力，构建完善的“网络空间地图”尤为重要。网络空间已成为陆海空天之外的“第五维空间”和人类生活的“第二空间”，为支撑网络空间“指挥控制”和“态势感知”，构建网络空间地图迫在眉睫。我国在 2016 年首次相对系统地提出了“网络空间地图”与“网络空间测绘”的概念，由解放军信息工程大学的罗向阳教授等专家指出，构建网络空间地图的技术核心即是网络空间测绘。时至 2022 年，盛邦安全成功发布了首张网络空间地图——“网络空间坤舆图”，标志着该领域的研究与探索进入了新的阶段。

1.2. 网络空间资产测绘挑战

尽管网络空间资产测绘的重要性已被广泛认识，但在实际应用中仍面临一系列挑战：

海量数据处理：网络空间资产数量庞大，数据更新迅速，如何高效处理、存储与检索海量测绘数据是一大挑战。

隐私保护与法律合规：资产测绘过程中可能涉及敏感信息和隐私数据，如何在合法合规的前提下进行测绘，避免侵犯他人权益，是技术与法律交织的复杂问题。

资产动态性与隐蔽性：部分资产可能具有动态 IP、隐藏服务、加密通信等特点，增加了发现与识别难度。

跨域测绘技术：全球网络空间资产分布广泛，跨越不同地域、网络环境和权限边界，实现跨域测绘需要突破技术壁垒。

标准不统一：资产测绘数据格式、接口、分类标准等缺乏统一规范，导致数据互操作性差，阻碍了跨组织、跨平台的数据共享与整合。

1.3. 网络空间资产测绘市场预期

根据国际咨询公司 IDC 的预测，“到 2027 年，中国将有40%的企业采用量化模型来管理网络风险，寻求网络风险量化供应商的协助，以评估遭受网络攻击的概率及可能的经济损失。网络空间地图（cyberspace map）即网络空间测绘相关技术，正是解决这一需求的关键，成为构建数字世界不可或缺的基础技术能力，预计至 2027 年，其市场规模将达到 61.5 亿元人民币。”

1.4. 网络空间测绘典型应用场景

1、网络空间安全风险监管与预警

网络空间地图，通过全面搜集资产信息，为网络安全态势提供了精确的视图。这一工具在监管网络安全风险和预警方面扮演着至关重要的角色。监管机构可以利用网络空间地图实时监控安全风险，全面了解安全状况和趋势，及时发现问题资产、违规配置以及潜在的安全威胁。

借助网络空间地图的直观可视化功能和多维数据关联，监管单位能够迅速识别问题所在，并提前发现风险，为及时响应提供数据支撑。资产状态、漏洞情况和安全影响都清晰可见，使得在安全漏洞或事件发生时，相关单位能够立即收到警报，快速定位受影响资产，并立即采取必要的应急措施。

这种全面的网络空间测绘不仅提高了网络安全的透明度，也为风险管理和应急响应提供了强有力的工具，确保网络安全防护工作更加高效和有针对性。

2、网络空间军事行动指挥控制

网络空间地图作为攻防双方进行网络攻防演练的态势底图，可实时展示演练进展，为网络对抗演练活动指挥提供清晰的视图基础。它汇聚地理域、网络域、社会域等多维度交叉信息，是防御方全面理解和掌握网络对抗演练态势的关键工具。网络中的信息中枢、关键设施、防御要点和可用资源都能通过网络空间地图系统得到深度感知和明确标识，为相关单位提供有力的态势感知和指挥支持。

3、智慧城市数字资产感知与运营

网络空间地图是智慧城市深度感知和高效运营的基础。通过网络空间地图，管理者可清晰辨识环境中的数字资产，深度感知其IT 环境，并了解其生命周期阶段，从而有效控制安全风险并提升安全运营效率。基于网络空间地图获取的状态信息，管理者可制定并执行针对性的数字资产管理计划，分析资产利用率，进行预算规划，提高资产利用效率，优化成本。此外，网络空间地图还为漏洞发现、威胁感知、事件响应和故障排除等工作提供了技术和数据支持，进一步提升智慧城市的整体运营效率。

4、企业外部攻击面管理

大型企业级客户，尤其是跨国企业，在面对传统网络资产管理不足所带来的风险之外，还必须应对广泛存在的泛资产风险。例如境外云服务上部署的仿冒/钓鱼网站、源代码托管平台上泄漏的企业重要系统代码、在线文库泄露的敏感文件、暗网/黑市上正在出售的企业人员邮箱和密码或者业务客户信息、疏于管理或被伪造的小程序或公众号等。企业除了使用本地测绘平台对自己管辖的内、外网地址段进行测绘之外，还需要借助具备全球网络空间(含泛资产空间)的空间测绘厂商的数据，收集泛资产测绘数据，形成企业攻击面管理的重要部分，快速发现和处置隐患。

5、网络空间资产多维度整合治理

通过整合网络空间内分散的各种资产数据，构建一个全面、精确且实时更新的资产数据库，可以有效地管理和监控网络空间资产，帮助企业更好地了解自己的网络环境，管理网络资源，并做出数据驱动的决策。通过建立统一的数据标准，比如实施标准化的资产分类、标识和描述流程，能够实现不同来源和格式资产数据的兼容性与共享性，从而提升数据的准确性和实用性。这一过程还需确保资产数据的收集、处理和共享遵循所有适用的法律法规，包括但不限于个人信息保护法和网络安全法等，以保障数据的合法合规使用。

同时，也需要遵守企业内部的数据管理政策和道德规范，例如数据隐私政策、数据归档政策等。通过对资产数据的分析和挖掘，可以发现隐藏在数据中的有价值的信息和知识。有助于企业更好地管理和利用自己的网络资产数据，实现数字化转型和升级。

6、国内运营商 IPv6 资产管理

面对 IPv6 地址空间的巨大和复杂性，运营商和城市运营中心采取了部署可扩展的扫描集群、先进的 IPv6 测绘引擎、服务赋能、共享成果的方式，提升了自身的网络安全管理能力的同时，还为不具备大算力资源的普通企业，梳理了自身的 IPv6 资产。

7、暗网等隐蔽空间测绘

暗网和深网的测绘正成为网络安全的新焦点。这些隐蔽的网络空间不仅难以用传统方法测绘，而且常常是非法活动的温床。随着监管部门对这些空间的重视增加，暗网测绘不仅需要技术手段，还需要多维度的治理策略。这有助于及时发现并应对其中的违法犯罪行为，从而减少网络犯罪，增强网络空间的透明度和安全性。

8、威胁情报数据生产

网络空间测绘厂商基于主动探测获取的资产数据，配合进一步研发的恶意应用识别、AI 智能分析等恶意识别技术，自动提炼出黑灰产资产名单（包括黄赌毒网站、钓鱼网站、被篡改网站、代理服务网站、黑客控守资源网站、C&C 地址等），成为威胁情报数据的服务提供商。

9、面向网络安全防护策略调优的网络空间测绘数据分析

主动感知、研判全网安全态势，提供智能数据取证，为专网安全管理工作提供全面可靠的数据支撑。通过多维度捕捉网络攻击痕迹，深度挖掘异常网络行为，从而强化网络暴露面及边界设备风险隐患监测，帮助管理者消除网络监管盲区，强化网络管控能力。

10、供应链安全风险管理

通过测绘技术识别企业供应链上下游的软硬件资产关联关系，助力构建“开发单位-使用单位-产品”的关系图谱，用于快速定位供应链漏洞影响范围，指导上下游同步修复。此外，通过测绘还可识别供应链网络中存在的未授权或仿冒设备，快速发现具有隐患的非标设备接入，及时消除供应链攻击风险。

2. 网络空间资产分析概述

随着数字化进程在全球范围内的加速推进，网络空间已深度融入社会经济生活的各个层面。网络空间资产作为数字世界的关键构成要素，其规模持续膨胀，涵盖了从传统的服务器、网络设备，到新兴的云计算资产、IoT 设备以及海量的域名和 IP 地址资源等。对网络空间资产进行精确测绘，犹如绘制数字世界的“地图”，不仅能够清晰洞察网络架构的全貌，更可为网络安全防护、运营管理以及战略决策提供坚实的数据支撑，意义重大。

本次报告聚焦于全球网络空间资产，以全面展现数字化浪潮下世界范围内的网络资产态势。通过对不同地域、行业、组织规模的网络实体进行广泛监测与分析，旨在挖掘隐藏在网络深处的各类资产信息，网络空间资产测绘绘制数字世界的精准地图，对于全面掌握网络架构、精准识别潜在风险、有力保障网络安全具有不可估量的意义。本报告基于全球网络空间资产测绘，对本年度网络空间资产状况展开深入剖析，旨在为各界提供决策依据，共筑网络安全防线。

本次报告聚焦全球网络空间，涵盖七大洲各个国家和地区，涉及不同行业领域，包括但不限于金融、能源、电信、交通等，全方位呈现网络空间资产全景。测绘的目标包括全球的IP和域名，云和 IoT、暴露的数据库等。

IP 地址：追踪全球 IP 地址动态，解析其所属网络、地理位置、组织归属，洞察网络接入热点区域与潜在扩张趋势，为威胁情报生产、网络流量分析、攻击溯源提供关键线索。

域名：监测全球域名注册、解析流向，挖掘域名背后的所有者身份、业务关联，甄别恶意域名注册行为，如用于网络钓鱼、恶意软件分发的可疑域名，守护网络访问入口安全。

云资产：针对主流云计算平台上的虚拟机、存储、负载均衡等云组件进行深度探测，评估云迁移浪潮下企业云资产暴露风险、配置脆弱性，以及跨云协同中的安全隐患。

IoT 设备：扫描电子屏、路由交换设备、工业物联网、网络打印机、智能机器人等物联网等领域海量设备，涵盖智能摄像头、工业传感器、智能硬件等，剖析设备品牌分布、固件版本、开放端口，揭示易被入侵的薄弱环节。

暴露的数据库：探寻全球范围内开放的数据库端口，分析数据库的类型、版本、访问权限设置，以及其中存储的数据敏感性，评估因数据库暴露而引发的数据泄露风险。

报告网络空间测绘分析主要内容详述如下：

一、网络空间资产全景分析：

基于 DayDayMap 测绘数据分析概括，我们对全球网络空间资产进行统计，从暴露服务与端口、IPv6 资产、IoT 资产、工控资产、终端截图资产、Starlink 、DNS 劫持等维度详细介绍。

二、行业细分测绘：

面向关键基础设施，关系国家安全的金融、能源、电信、交通几个行业细分分析。根据每个行业特点，基于测绘数据分析 2024 年梳理行业资产暴露面。对行业高位资产和典型漏洞，遭受攻击的案例进行分析。

三、资产暴露的影响力与成本评估：

资产暴露可能造成数据泄漏、网络中断、合规性等影响，通过对不同场景下造成的影响和成本评估。分别从金融、能源、电信、交通行业评估可能造成的社会影响。

四、改进建议与防护措施：

对本次 2024 年网络空间测绘主体及发现的问题，该章节分别从资产识别和监控、端口服务管理、漏洞管理，行业协作、政策建议、教育培训，AI 在资产测绘与风险识别中的应用前景，外部攻击面管理、零信任架构对资产暴露的缓解作用，多源情报融合的未来趋势，资产和漏洞管理中台，打通外部和内部资产，自动化攻击和防护等多个方面提供改进建议和防护措施。

3. 网络空间资产全景分析

3.1. 全球网络资产概览

图 3-1-1 全球网络空间资产分布可视化

• 资产总量统计

目前监测到 2024 年新增 47 亿资产，其中 IPv6 在线超过 35 亿，独立 IPv6 数超过 16 亿。2024 年，新增暴露的非 80 高危端口超过 7000 万，如 3389 端口超过 680 万，23 端口超过 140 万，21 端口超过 3400 万等；80 端口新增独立 IP 超过 15 亿。根据取整统计，目前组织机构资产 2.6 亿，脆弱性资产 2.5 亿，网络摄像头资产 1800 万，路由交换设备 4000 万，工业控制设备 100 万，云服务资源 100 万，安全防护设备 1200 万，网络打印机设备 130 万，数据库开放端口超过 50 万。

• 区域分布

各国的暴露资产占比 TOP5，美国 3,104,092,851；日本 332,409,660；中国 223,751,260；英国 181,915,445；以色列 136,273,138。

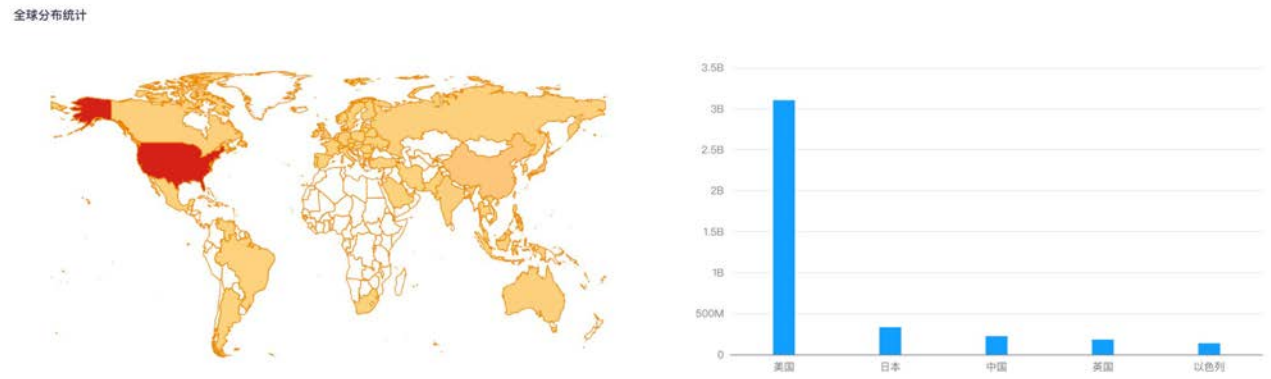


图 3-1-2 全球网络空间资产暴露资产 TOP5

中国的暴露资产占比 TOP5，国内分别是香港特别行政区 59,832,399、北京市 20,306,796、广东省 18,423,540、台湾省 18,398,153、上海市 15,237,006。

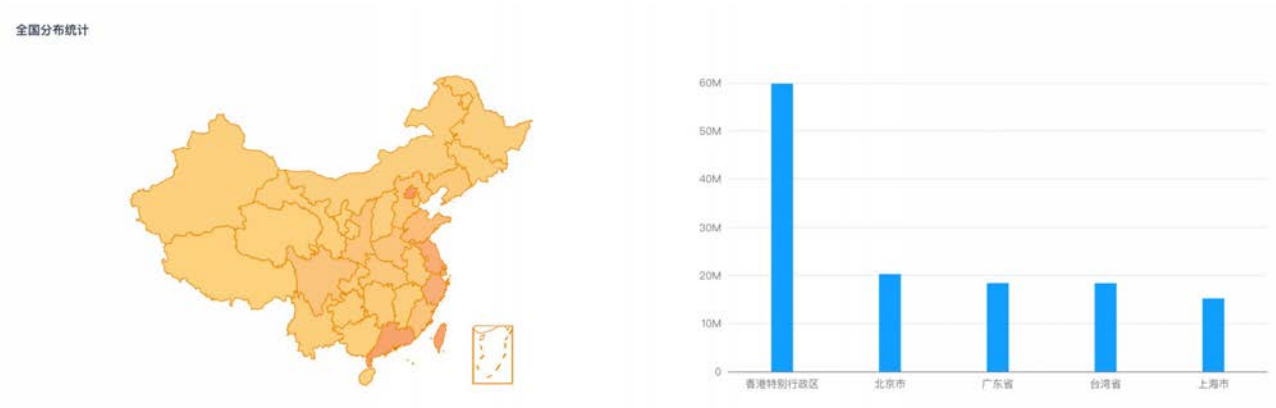


图 3-1-3 中国网络空间资产暴露资产 TOP5

经过分析，IPv6 在整体资产的新增占比 74%，数据说明全球网络正稳步迈 IPv6 时代，越来越多的网络设备、服务器以及各类终端纷纷启用 IPv6 地址，以满足未来海量设备连接、高速数据传输的需求。随着 IPv6 的普及，其独特的地址结构与特性也在重塑网络架构与应用模式，为诸如物联网、智能交通、工业互联网等新兴领域提供了坚实的基础支撑。

当前，全球约 30% 的企业云实例存在至少一种高危配置错误，65% 的云安全事件与配置错误有关，如过度开放的存储权限，允许未经授权访问企业敏感数据，导致数据泄露事件频发。79% 的企业经历过至少一次严重的云安全事件。相关网络空间资产测绘工具探测到约 50 万个开放的数据库端口，其中 10% 的数据库未设置任何访问限制，内含海量敏感数据，随时面临被窃取风险。金融行业尤为突出，部分中小金融机构数据库因配置不当，在过去一年中遭受多次 SQL 注入攻击，导致客户资金账户信息泄露，引发信任危机。政府部门网络中的部分边缘节点，因业务需求临时开放端口后未及时关闭，被外部扫描发现，存在关键信息泄露隐患。

3.2. 暴露服务与端口

2024 年，新增暴露的 3389 端口超过 680 万，23 端口超过 140 万，22 端口超过 8000 万，21 端口超过 3400万，1443 端口超过 50 万，25 号端口超过 200 万，3306 端口超过 2500 万，5432 端口超过 120 万，873 端口超过 30万，69 端口超过 20 万；新增tftp服务 17 万，ftp 服务 2100 万，telnet 服务 250 万，rdp 服务 670 万，ssh 服务 9000 万，smtp 服务 90 万，postgresql 服务 110 万，mysql 服务 840 万。

2024 年新增暴露端口统计：

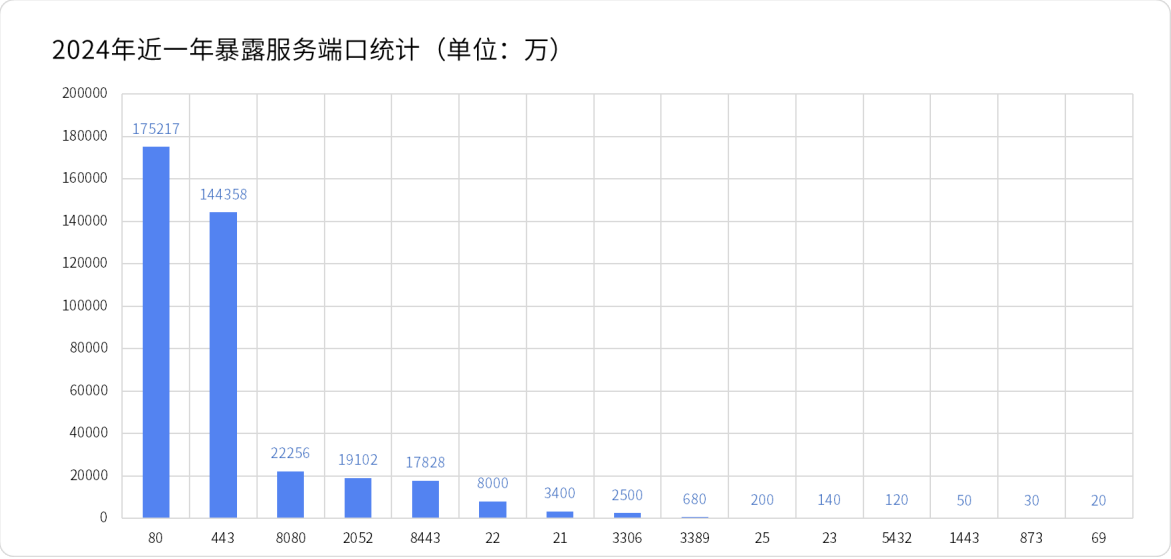


图 3-2-1 2024 年近一年暴露端口（部分）统计

2024 年新增暴露服务统计：

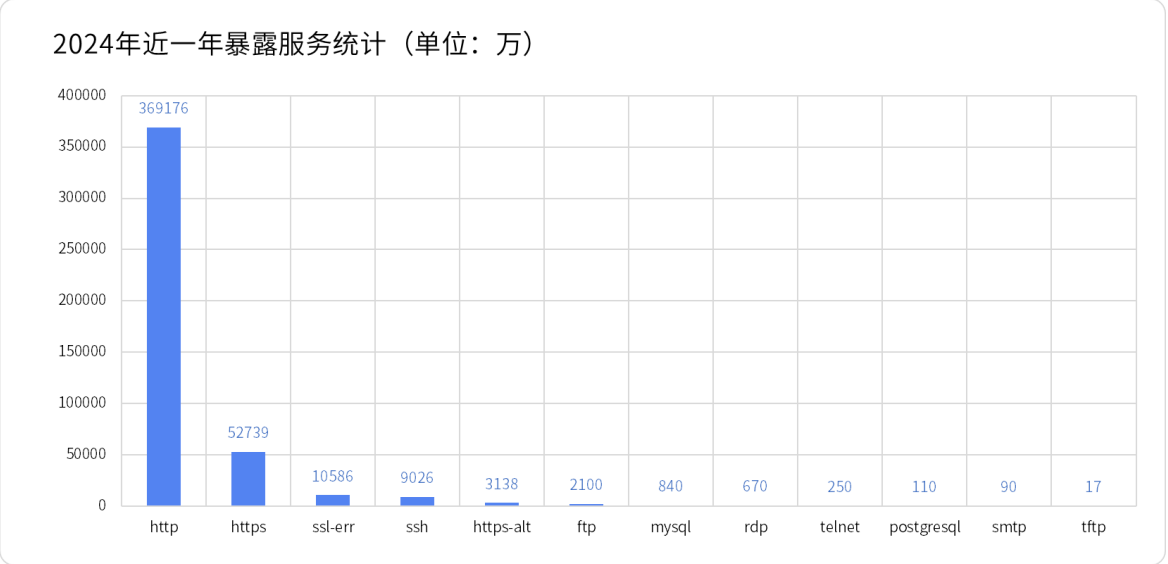


图 3-2-2 2024 年近一年暴露服务（部分）统计

- **常见暴露端口：**如 HTTP / HTTPS（80 / 443）、RDP（3389）、SSH（22）、Telnet（23）等。
- **未保护服务：**如 PostgreSQL、MySQL、FTP 等。

全球约 25% 的服务器存在至少一个不必要的高风险开放端口，如 Telnet（23 端口）、FTP（21 端口）等。这些端口犹如敞开的大门，成为黑客发动暴力破解、恶意软件植入的“便捷通道”，常引发大规模数据泄露事件。在企业边缘网络，近 30% 的网络设备开放 SNMP（161 端口）服务且采用默认团体名，攻击者极易获取设备配置、运行状态信息，进而利用 SNMP 协议漏洞，通过修改设备配置参数，为进一步渗透企业核心网络“大开方便之门”，常引发大规模数据泄露事件。黑客通常先利用端口扫描工具，大范围搜索目标网络中的开放端口，一旦发现上述高风险端口，便针对端口对应的服务漏洞进行攻击。例如，对于开放的FTP端口，尝试使用常见的弱密码字典进行暴力破解，若成功登录，即可上传恶意文件或窃取敏感数据。

3.3. IPv6 资产

2024年，盛邦安全 DayDayMap 平台基于 62 亿的 IPv6 地址池，实时监测，其中 IPv6 在线超过 35 亿，独立 IPv6 数超过 16 亿。其中，TOP5 的国家分布占比分别是美国 2,720,740,297，占比 76% ；日本 2,720,740,297 占比 8%，英国 148,492,579 占比 3%，以色列 148,492,579 占比 3%，印度 42,857,302 占比 1%。

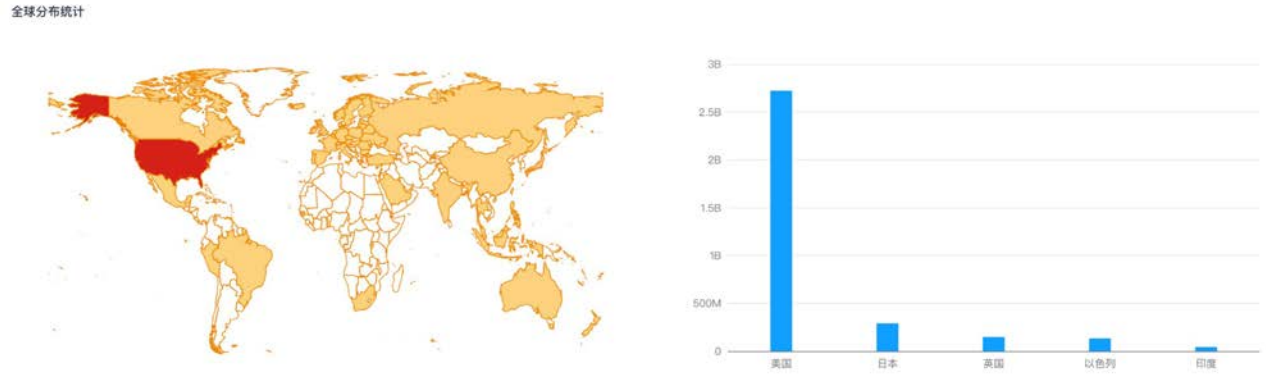


图 3-3-1 IPv6 全球网络空间资产暴露资产 TOP5

TOP5 的端口分布占比分别是 80 端口 1,473,646,658 占比 41.25%；443 端口 1,219,417,941 占比 34.14%；8080 端口 203,971,088 占比 5.71%；2052 端口 190,690,234 占比 5.34%；8443 端口 162,106,372 占比 4.54%。

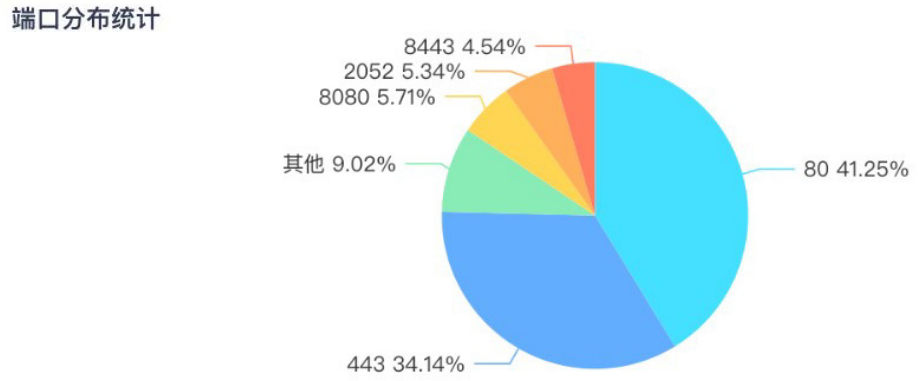


图 3-3-2 IPv6 全球网络空间资产端口分布统计

随着全球 IPv6 部署加速，约 15% 的 IPv6 网络前缀存在路由泄露问题，导致网络可达性异常，外部攻击者可利用此漏洞绕过部分安全防护机制，直接访问内部网络资源。IPv6 过渡机制中的双栈环境下，近 20% 的节点在 IPv4 与 IPv6 转换过程中出现配置错误，引发协议兼容性漏洞。攻击者可利用此漏洞，在双栈节点处实施中间人攻击，通过劫持 IPv6 流量，窃取敏感数据。IPv6 过渡机制中的双栈环境下，近 20% 的节点在 IPv4 与 IPv6 转换过程中出现配置错误，引发协议兼容性漏洞。攻击者首先通过网络扫描工具识别双栈环境中的目标节点，然后利用协议漏洞，向目标节点发送伪造的 IPv6 邻居 solicitation 消息，诱使目标节点将流量转发至攻击者控制的设备，进而窃取数据。

3.4. IoT 资产

- **电子屏资产分析**

在城市繁华商圈、交通枢纽等地广泛部署的户外电子显示屏，约 15% 存在弱密码或默认密码未修改问题。这些电子屏一旦被黑客控制，可肆意播放非法广告、虚假信息，扰乱社会秩序。我们对市场占有率前 100+ 的数字电子屏的品牌的设备进行指纹采集和分析。

图 3-4-1 全球电子屏分布可视化图

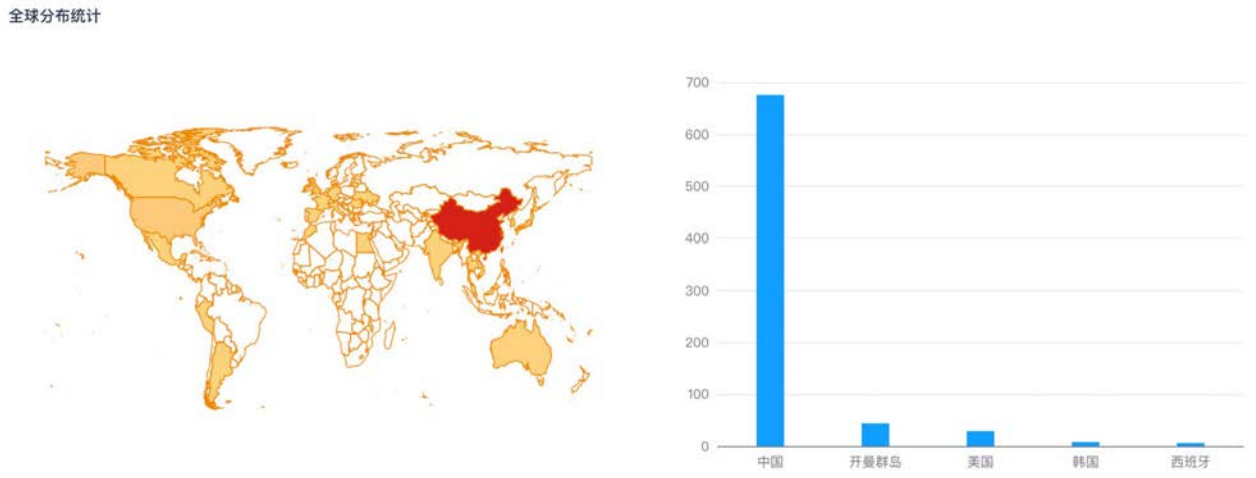


图 3-4-2 电子屏全球分布统计

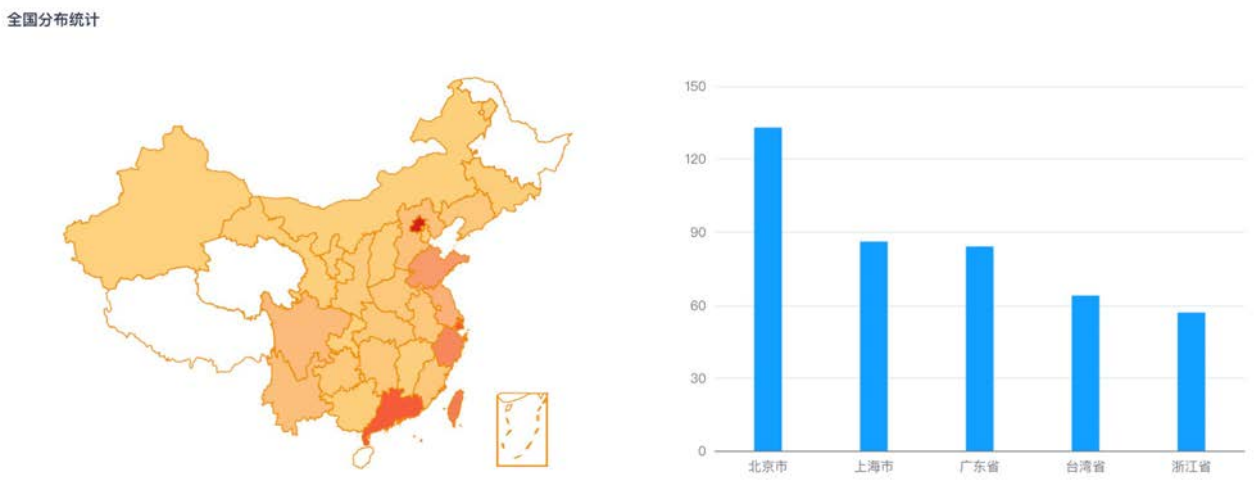


图 3-4-3 电子屏中国分布统计

部分电子屏控制系统采用老旧的 Windows 系统，微软已停止更新，致使大量已知漏洞未修复，如永恒之蓝漏洞。黑客利用该漏洞可远程执行代码，完全掌控电子屏，将其变为传播恶意信息的工具。攻击者首先通过工具搜索暴露在网络上的电子屏设备，锁定目标后，尝试使用常见弱密码登录。若失败，则利用漏洞扫描工具查找系统漏洞，一旦发现可利用漏洞，如上述永恒之蓝漏洞，便上传恶意软件，实现对电子屏的操控。

- **网络摄像头**

2024年监测到新增网络摄像头新增独立 IP 超 300 万，其中 TOP5 的国家分别为中国占比 21.6%，美国占比 17.9%，越南占比 9.6%，韩国占比 6.5%，巴西占比 5.4%。

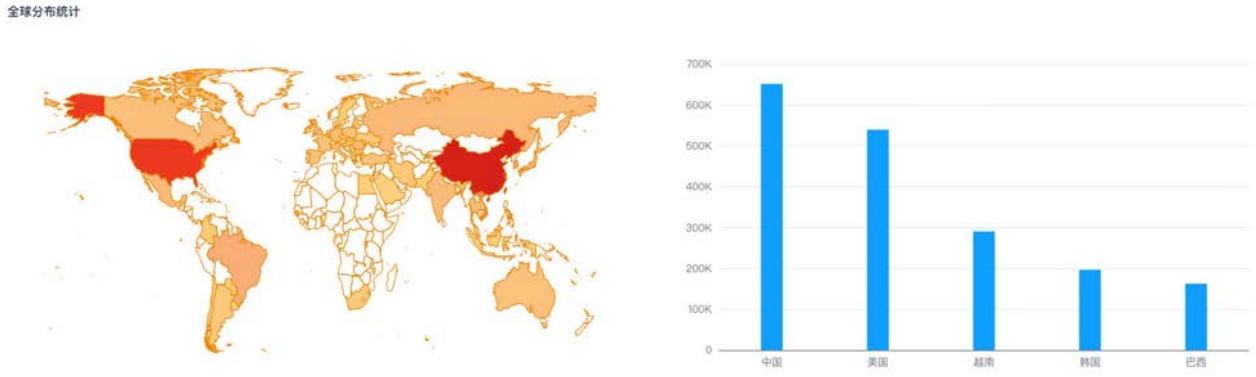


图 3-4-4 网络摄像头全球分布统计

国内 TOP5 的区域分别为台湾省，江苏省、广东省、香港特别行政区、浙江省。

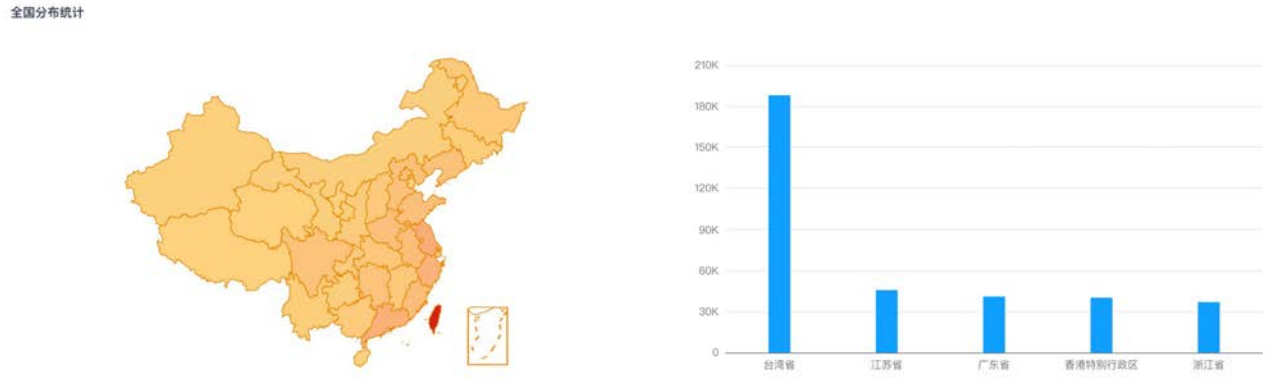


图 3-4-5 网络摄像头中国分布统计

端口和服务统计，其中 80 端口占比 29.82%，81 端口占 比10.74%，8080 端口占比 6.33%，443 端口占比 5.4%，554 端口占比 3.93%。rtsp 服务占比 4.18%，http 服务占比 87.4%，hikvisionsdk 服务占比 0.33%、hikvisionsdk8000 服务占比 0.46%。

图 3-4-6 网络摄像头端口和服务全球分布统计

大量的网络摄像头存在非合作远程访问执行问题，超 40% 的家用网络摄像头存在弱密码漏洞，出厂默认密码广泛存在，黑客可轻易远程控制摄像头，窥探用户家庭隐私，甚至利用摄像头麦克风监听室内声音，引发严重隐私危机。工业物联网场景下，约 30% 用于工厂安防、生产监控的网络摄像头固件常年未更新，已知的缓冲区溢出、命令注入等高危漏洞未修复。一旦遭受攻击，攻击者不仅能获取工厂内部实时画面，还可通过篡改摄像头指令，干扰正常生产秩序，造成巨额经济损失。

对于家用摄像头，黑客常通过搜索引擎工具，批量搜索存在弱密码的摄像头，获取 IP 地址后，使用默认密码尝试登录，成功后即可进行远程操控。在工业场景下，攻击者先对目标工厂网络进行渗透测试，识别出老旧未更新固件的摄像头，再利用已知漏洞发送恶意指令，引发混乱。

• 路由交换设备

2024 年监测到新增路由交换设备新增独立 IP 超 110 万，其中 TOP5 的国家分别为中国、美国、巴西、日本、委内瑞拉。

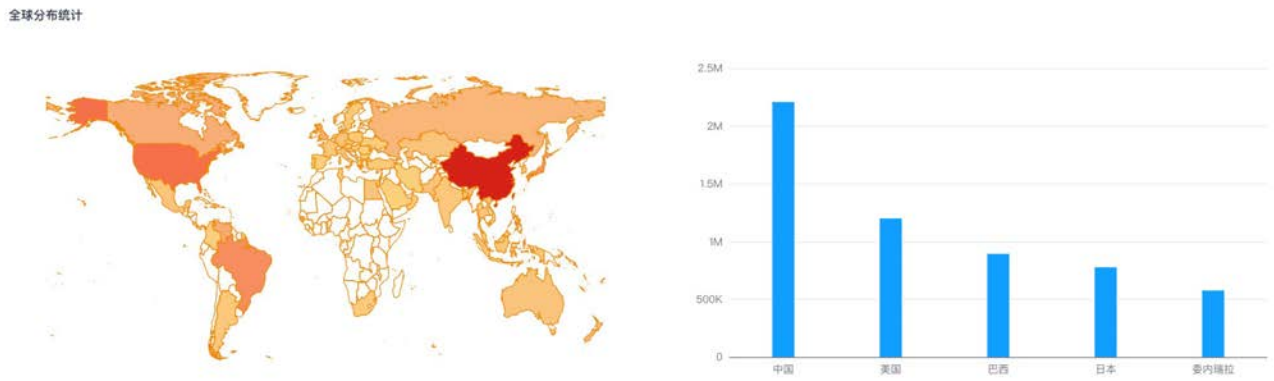


图 3-4-7 路由交换设备全球分布统计

国内 TOP5 的区域分别为台湾省、香港特别行政区、江苏省、广东省、浙江省。

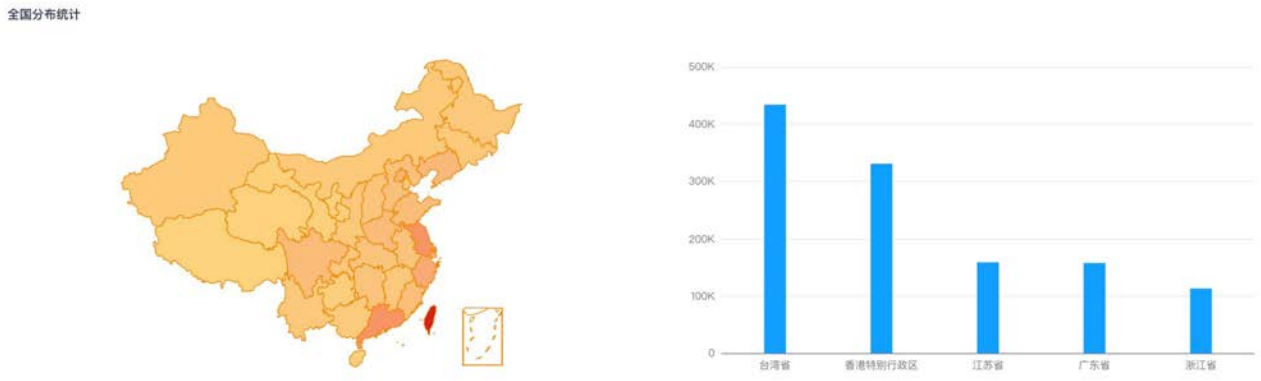


图 3-4-8 路由交换设备中国分布统计

端口和服务统计，其中 80 端口占比 10.77%，8443 端口占比 15.14%，8080 端口占比 4.42%，443 端口占比 14.97%，7547 端口占比 25.03%。ftp 服务占比 2.59%，http 服务占比 56.5%，telnet 服务占比 1.63%、bgp 服务占比 2.19%，https 服务占比 34.07%。

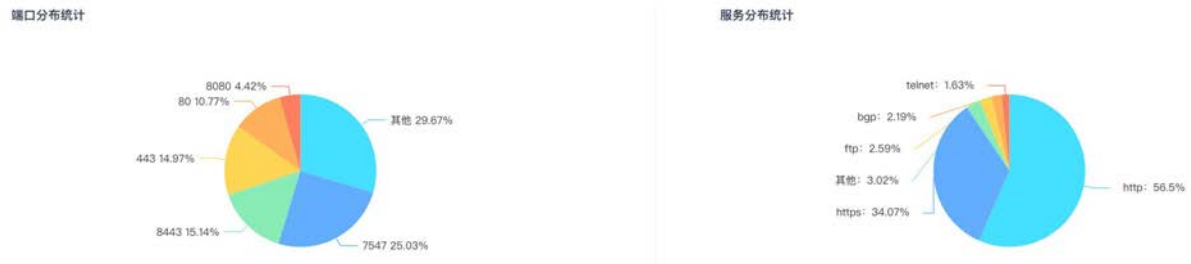


图 3-4-9 路由交换设备端口和服务全球分布统计

全球范围内，约 20% 的路由交换设备存在默认配置未更改问题，如默认的管理员账号和密码未修改，使得攻击者可轻易登录设备，篡改路由表、嗅探网络流量，严重威胁网络传输安全。部分厂商的路由交换设备被爆出存在后门漏洞，如某北美知名品牌曾被发现特定型号设备在固件中有隐藏的远程登录后门，攻击者知晓后门密码后，可绕过正常认证机制，直接控制设备，窃取网络数据或发动中间人攻击。攻击者通常先利用端口扫描工具，识别网络中开放的路由交换设备端口，尝试使用默认账号密码登录。若遇到采用非默认配置的设备，则利用漏洞扫描工具查找已知漏洞，发现后门漏洞后，即刻利用其获取设备最高权限，为后续攻击行为奠定基础。

• 网络打印机

2024年监测 130 万的暴露的网络打印机设备，新增网络打印机设备新增独立 IP 8.1 万，其中 TOP5 的国家分别为中国、美国、韩国、法国、德国。

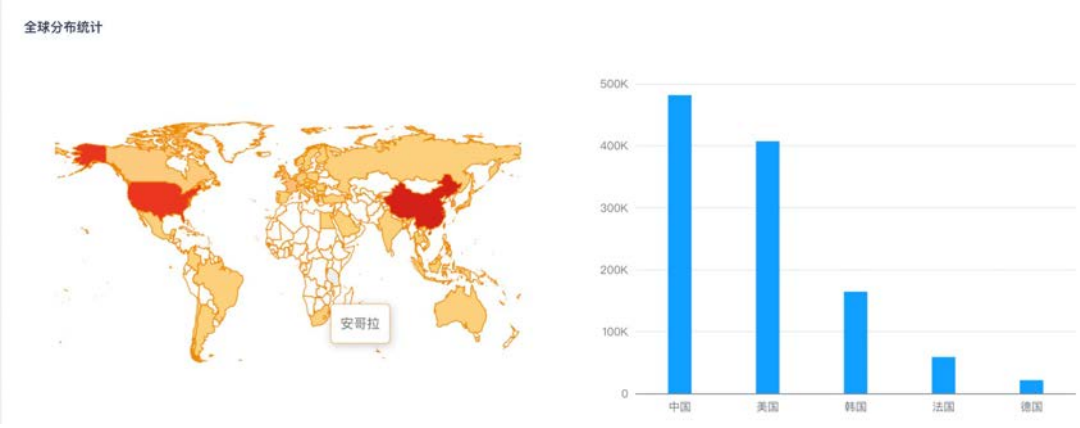


图 3-4-10 网络打印机全球分布统计

国内 TOP5 的区域分别为台湾省、香港特别行政区、北京市、广东省、江苏省。

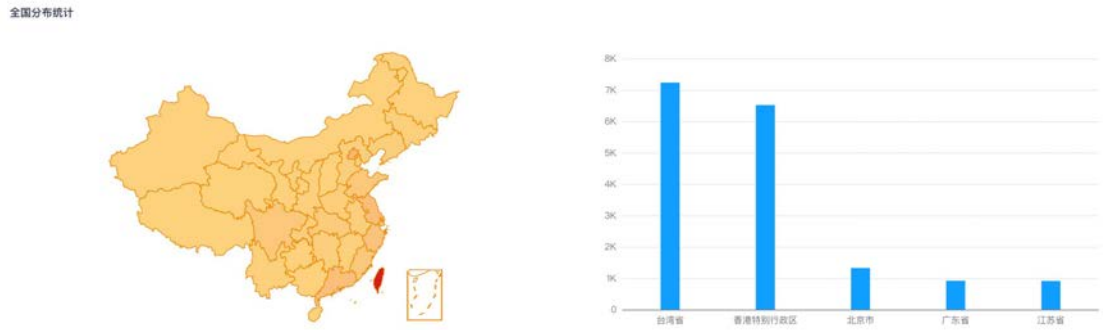


图 3-4-11 网络打印机中国分布统计

端口和服务统计，其中 80 端口占比 26.55%，631 端口占比 20.71%，8080 端口占比 11.79%，443 端口占比 14.02%，515 端口占比 6.86%。ipp 服务占比 11.47%，http 服务占比 55.63%，ipd 服务占比 6.86%、pil 服务占比 4.19%，https 服务占比 16.77%。

图 3-4-12 网络打印机端口和服务全球分布统计

在企业办公环境中，约 25% 的网络打印机存在未授权访问漏洞，可被外部人员轻易发现并连接，打印敏感文件，导致企业商业机密泄露。许多网络打印机支持Web管理界面，但部分界面存在身份验证漏洞，如简单的密码猜测即可绕过登录，进入管理界面后，攻击者不仅能查看打印机的打印队列、配置信息，还能上传恶意固件，将打印机变为僵尸网络中的一员，参与 DDoS 攻击等恶意活动。攻击者首先通过网络扫描工具搜索开放的网络打印机端口，尝试直接连接。若受阻，则针对打印机的 Web 管理界面进行密码猜测攻击，成功进入后，依据攻击目的，或是窃取打印文档，或是篡改打印机配置，使其沦为攻击工具。

• 其他物联网设备

工业物联网领域，大量老旧工业传感器固件常年未更新，已知的缓冲区溢出、命令注入等高危漏洞未修复，一旦遭受攻击，生产线可能瞬间瘫痪，造成巨额经济损失。以智能家居为例，智能家电设备存在弱密码或未加密通信问题，黑客可通过破解密码或截获通信数据，控制家电设备，不仅侵犯用户隐私，还可能引发用电安全等问题。攻击者先利用工具搜索特定类型的物联网设备，锁定目标后，针对不同设备的常见弱点展开攻击。对于有弱密码的设备，进行密码破解；对于未加密通信的设备，使用网络嗅探工具截获数据并分析，进而控制设备实现恶意目的。

3.5. 工控资产

2024 年监测 100 万 的暴露的工控设备，新增工控设备独立 IP 19 万，其中 TOP5 的国家分别为中国、美国、韩国、土耳其、印度尼西亚。

图 3-5-1 工控资产全球分布统计

国内 TOP5 的区域分别为台湾省、北京市、浙江省、广东省、江苏省。

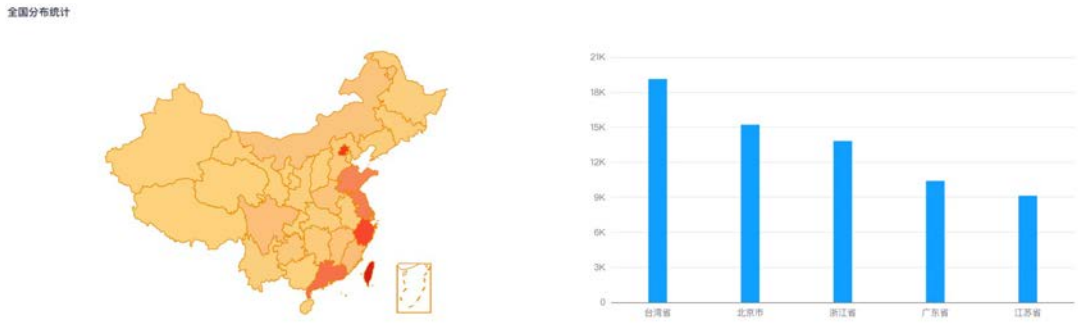


图 3-5-2 工控资产中国分布统计

端口和服务统计，其中 502 端口占比 17.02%，102 端口占比 14.98%，2404 端口占比 14.39%，47808 端口占比 11.94%，2000 端口占比 27.95%。dnp 服务占比 28.2%，modbus 服务占比 25.84%，s7 服务占比 14.98%、iec 服务占比 14.39%，bacnet 服务占比 11.94%。

图 3-5-3 工控资产端口和服务全球分布统计

全球范围内，约 20% 的工业控制系统存在未授权访问漏洞，多因老旧系统默认账户未更改或弱密码设置，攻击者可直接登录操作界面，篡改工业流程参数，危及工厂安全生产。在电力、化工等关键行业，近 10% 的工控网络与企业办公网络、互联网之间边界防护薄弱，缺乏有效隔离，存在跨网攻击隐患。一旦办公网络被攻破，攻击者可通过横向渗透，轻易进入工控网络，对关键生产设备进行恶意操作。攻击者往往以钓鱼邮件、恶意软件植入等方式突破企业办公网络防线，获取内部员工权限后，利用网络扫描工具发现工控网络入口，再凭借工控系统的未授权访问漏洞，登录操作界面，实施破坏行为。

3.6. 远程终端

2024 年监测 435 万的暴露的远程桌面终端 RDP，3389 端口占比 97.87%，新增远程桌面终端独立 IP 189 万，其中 TOP5 的国家分别为中国、美国、德国、日本、俄罗斯。

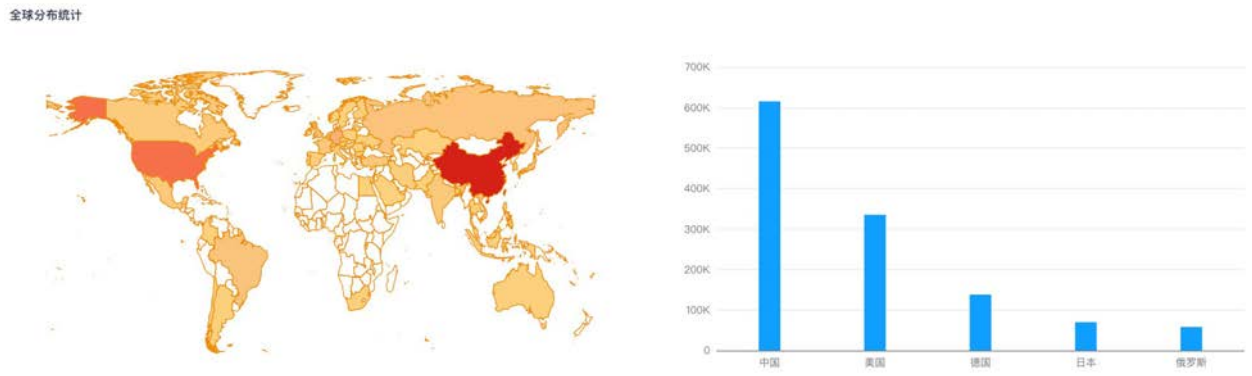


图 3-6-1 远程终端全球分布统计

国内 TOP5 的区域分别为香港特别行政区、广东省、上海市、北京市、江苏省。

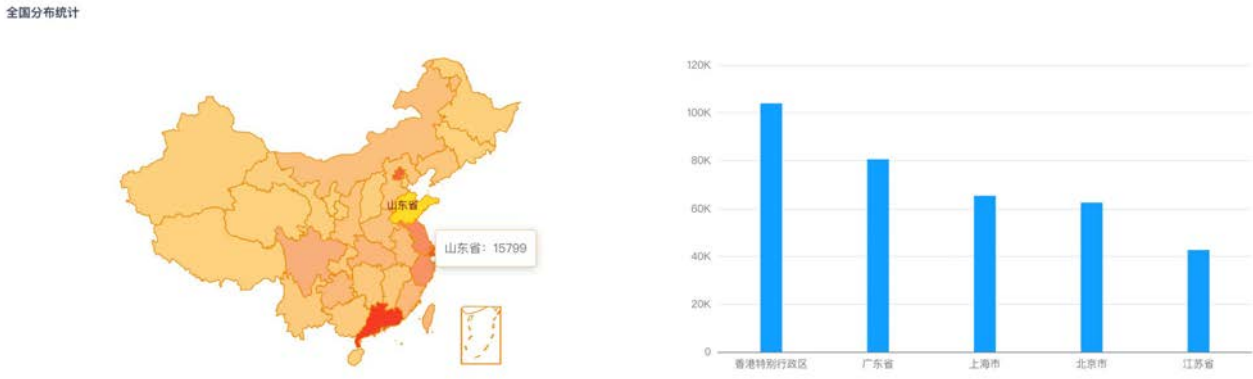


图 3-6-2 远程终端中国分布统计

全球范围内，约 15% 的企业级远程桌面服务存在安全配置错误，如未启用强身份验证机制、允许空密码登录或使用默认端口 3389 且未做任何访问限制。这些脆弱点使得攻击者极易发现并尝试入侵，进而获取企业内部敏感信息或操控内部系统。在 2024 年 6 月，一家位于欧洲的制药企业遭遇严重攻击。该企业为方便员工远程办公，启用了远程桌面服务，但未及时更新系统补丁。攻击者利用微软 RDP 协议的一个未修复漏洞，无需密码即可登录企业内部服务器，窃取了正在研发的新药配方以及大量患者临床试验数据，给企业带来了毁灭性打击，不仅研发进程受阻，还面临巨额赔偿风险。攻击者首先通过工具搜索暴露在网络上的远程桌面服务，锁定目标后，尝试利用已知漏洞或弱密码进行登录。若遇到采用非默认配置的服务，则利用漏洞扫描工具查找系统漏洞，一旦发现可利用漏洞，如上述 RDP 漏洞，便迅速利用其获取访问权限，依据攻击目的，或是窃取数据，或是植入恶意程序，实现长期控制。

3.7. Starlink

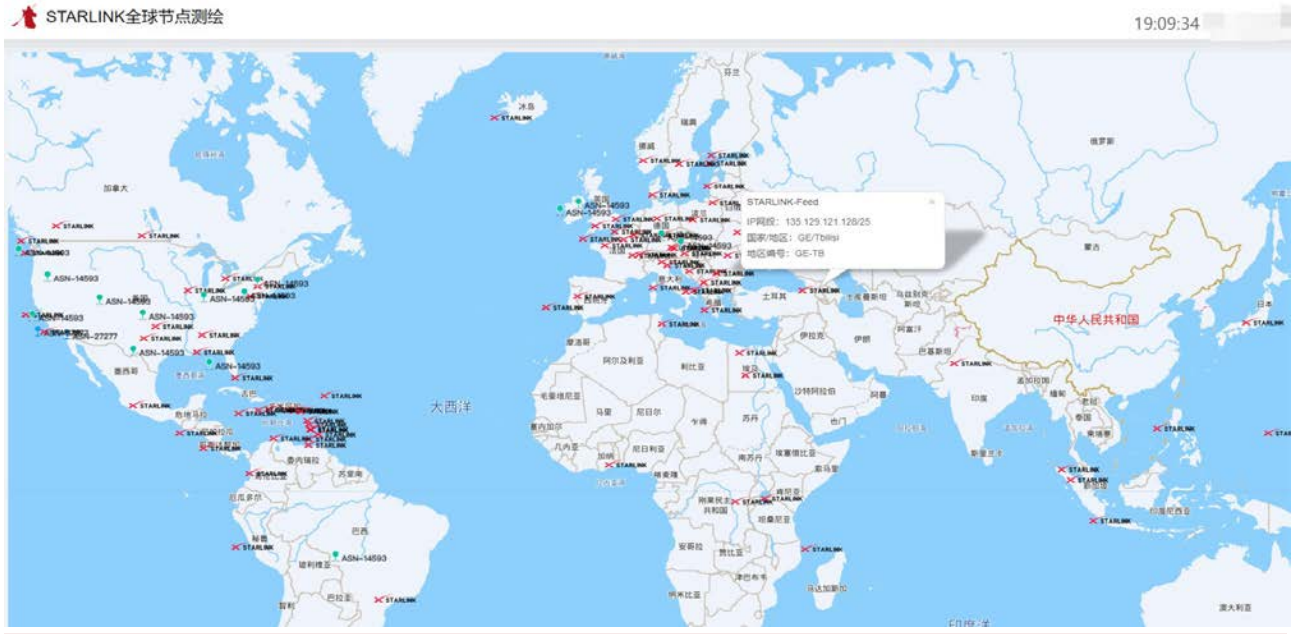


图 3-7-1 星链 PoP 点部署全球分布可视化

2024 年监测到 2 万多新增的星链独立 IP，其中 TOP5 的国家分别为美国、加拿大、乌克兰、智利、澳大利亚。

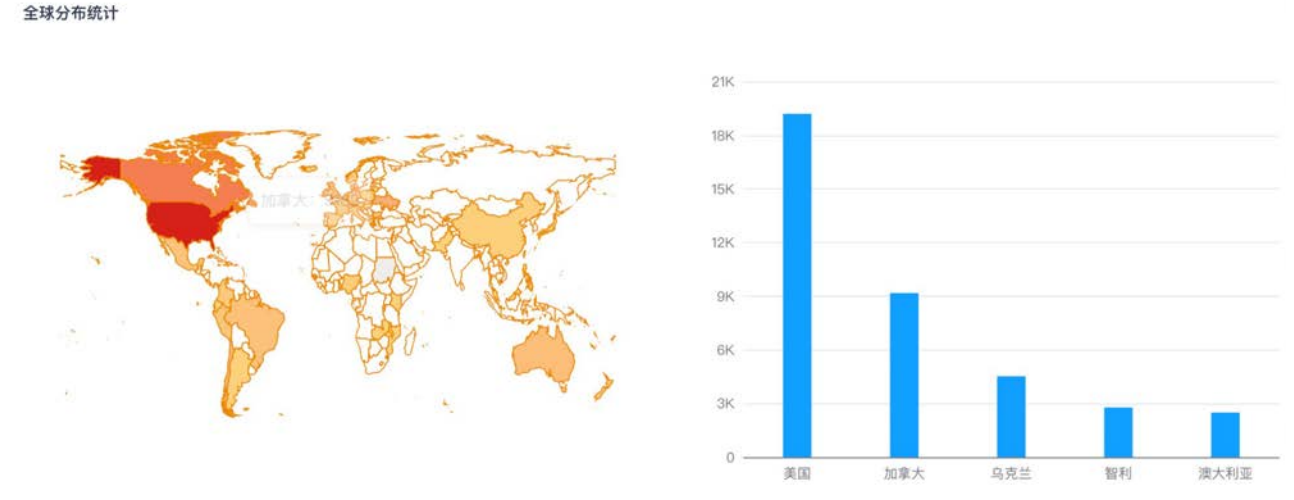


图 3-7-2 Starlink 全球分布统计

端口和服务统计，其中 500 端口占比 10.86%，22 端口占比 8.48%，161 端口占比 4%。Snmpv3 服务占比 3.85%，isakmp 服务占比 10.79%，ssh 服务占比 9.39%、http 服务占比 21.62%，https 服务占比 21.94%。

图 3-7-3 Starlink 全球端口和服务分布统计

作为新兴的卫星互联网资产，Starlink 约 5% 的地面终端设备存在身份验证漏洞，黑客可仿冒终端接入卫星网络，非法占用网络带宽，甚至篡改卫星通信数据，干扰正常通信业务。在偏远地区依赖 Starlink 网络的关键基础设施（如小型电站、通信基站），由于网络拓扑相对简单，约 8% 的节点易受 DDoS 攻击，影响当地基本服务供应。攻击者利用 Starlink 网络的分布式特点，组织大规模僵尸网络，对目标节点发起海量请求，使其瘫痪。在 2024 年 9 月，位于南美洲某偏远山区的一个小型水电站，其依赖 Starlink 网络进行远程监控和数据传输。黑客发现该电站 Starlink 地面终端设备的身份验证漏洞后，仿冒终端接入卫星网络，不仅窃取了电站的运行数据，还篡改了部分控制指令，导致水电站的发电设备出现异常运行，险些造成水坝溃坝事故。同时，周边地区的通信基站也受到 DDoS 攻击影响，当地居民的通信中断长达数小时，给生活带来极大不便。针对 Starlink 地面终端，黑客先通过网络嗅探工具捕获终端认证信息，分析其认证协议漏洞，然后伪造认证数据包，成功接入卫星网络。对于易受 DDoS 攻击的节点，攻击者事先在全球范围内控制大量僵尸主机，在预定时间向目标节点发起攻击，阻断服务。

3.8. DNS 劫持

2024 年监测 DNS 新增独立 IP 7.2 万，其中 TOP5 的国家分别为美国、中国、印度、俄罗斯、德国。

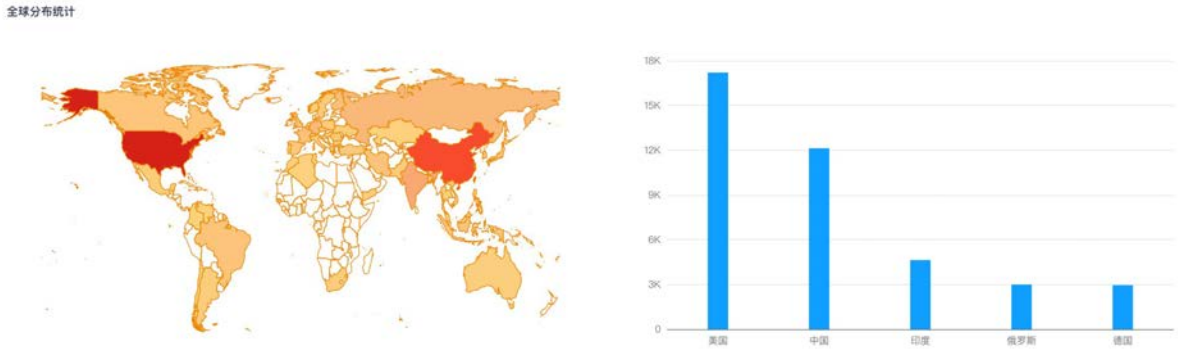


图 3-8-1 DNS 全球分布统计 TOP5

全球约 10% 的 DNS 服务器存在配置脆弱性，易遭受 DNS 劫持攻击，攻击者篡改域名解析结果，将用户导向恶意网站，进行网络诈骗、恶意软件下载等非法活动，危害网络浏览安全。在部分发展中国家地区，由于网络基础设施薄弱，DNS 劫持发生率高达 15% ，当地互联网用户频繁遭遇访问异常，如正常购物网站被替换为仿冒诈骗网站，造成大量财产损失。薄弱的 DNS 服务器配置，如缺乏域名缓存安全机制、易被篡改的 DNS 解析记录，为劫持者提供了可乘之机。2024 年 7 月，某非洲国家的互联网服务提供商 DNS 服务器被黑客入侵。黑客获取管理员权限后，修改了大量热门电商网站和金融机构网站的域名解析记录。当地用户在访问这些网站时，被自动引导至仿冒的诈骗网站。据不完全统计，在短短一周内，就有数千名用户上当受骗，损失金额累计达到数百万美元，严重扰乱了当地的网络经济秩序，民众对网络安全的信任度也大幅下降。攻击者通常先渗透进 DNS 服务器所在网络，利用服务器漏洞获取管理员权限，然后修改 DNS 解析记录，将热门域名指向自己控制的恶意服务器。当用户访问这些域名时，就会被引导至诈骗或恶意软件下载页面。

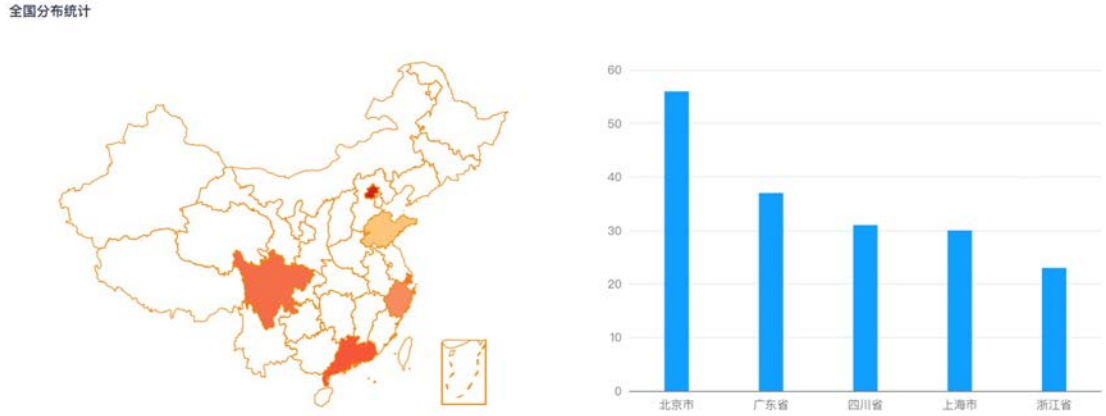


图 3-8-2 DNS 劫持资产中国分布统计 TOP5

DNS 劫持资产 TOP5 国内区域分别为北京市、广东省、四川省、上海市、浙江省。

从 2024 年 5 月开始，国内部分家用路由器开始出现间歇性断网、域名解析延迟高以及解析到海外 IP 等情况，今年 8 月该现象变得尤为严重。前几天在做应急响应时候发现某企业暴露在公网上的路由器配置的 DNS 地址被莫名其妙篡改了，主 DNS 地址是一个阿里云上的节点，备用 DNS 地址为 1.1.1.1。起初以为这次事件跟近期的攻防演习相关，后面经过深入分析发现该事件并不是个例，我们已排查到有大量暴露在公网上的路由器都存在 DNS 被篡改的情况，且大部分用户基本没有感知。经过初步统计，攻击者使用的劫持 DNS 节点数已有百余个，用户访问受影响的目标主要覆盖了阿里云 CDN、腾讯云 CDN、华为云 CDN 等，导致了一系列的解析异常。短时间范围内，大量用户投诉对国内重要目标单位访问异常，造成严重安全隐患。盛邦安全烽火台实验室 Beacon Tower Lab 联合 Panabit 对该事件进行了专项分析，这起事件是属于典型的 DNS 劫持攻击事件，符合国外黑灰产组织的攻击特征。攻击者通过搜集公网可访问的路由器地址，利用漏洞或弱口令获取路由器控制权限，修改路由器 DNS 服务器地址，达到中间人攻击的效果。整体的攻击流程如下图所示：

（图中假设攻击者对 webray.com.cn 进行了 dns 劫持）

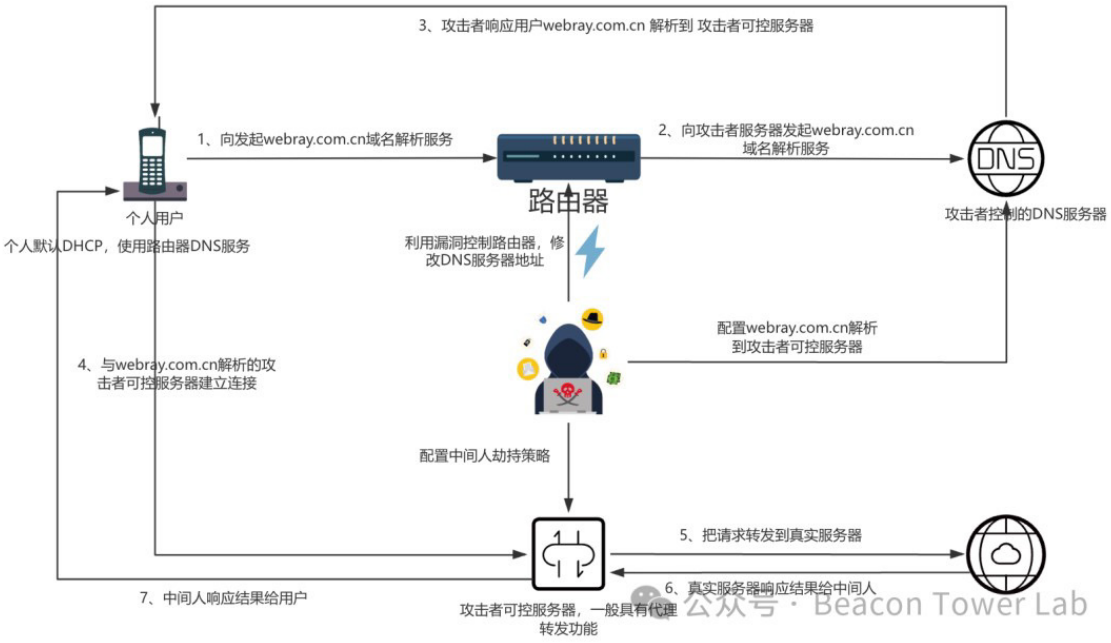


图 3-8-3 DNS 劫持攻击流程

用户在发起 HTTP 请求之前首先会进行 DNS 请求，由于绝大部分个人用户不会自定义 DNS 服务器，所以默认情况下会使用路由器的 DNS 服务器来进行域名解析。攻击者通过漏洞把路由器 DNS 服务器篡改为自己可控的恶意 DNS 服务器，并添加解析记录 webray.com.cn 到恶意 IP 地址。用户拿到 webray.com.cn 响应的 IP 地址之后会与攻击者可控恶意 IP 建立链接，攻击者可控恶意IP通过实现中间人代理功能，把用户的请求转发的真实目标服务器并响应真实服务器结果给用户。

基于 DNS 劫持的中间人攻击一般可以造成做到用户无感知，但这个事件还是导致了用户访问异常，从而慢慢发酵了出来，引起用户访问异常的原因有以下两点：

1、经过攻击者可控的服务器进行代理转发之后，会明显降低系统访问速度，造成访问请求延迟增大。

2、用户访问 https 协议的网站目标时，会因为中间人可控服务器没有受信任的证书而导致访问失败。

中间人攻击是一种常见的网络攻击方式，一般情况下可以造成下面的两种危害：

1、造成信息泄漏，通过中间人攻击可以劫持用户流量，通过对流量中的敏感信息进行提取，获取用户认证信息等敏感内容。

2、造成远程权限获取，通过中间人攻击可以篡改用户流量，一般情况下中间人会把用户请求转发到真实服务器，但是部分情况下可以通过对流量进行篡改达到 RCE 的效果。其中经典的用法是通过修改软件的升级更新包的响应内容，通过把响应内容替换为木马文件，达到自动运行的效果。

由于事件还在发酵，很难判断攻击者的最终目的是属于流量获取还是远程权限获取。但是不论何种情况，对用户来说都是属于较大的安全隐患。

那么用户应该如何排查自己的 DNS 服务器是否正常呢?我们把目前的情况做了总结，本次事件中的恶意 DNS 服务器普遍具有以下特征：

1、能解析的域名ttl改为了 86400 秒，即 1 天

2、使用 unbound-1.16.2 作为版本名称

以已知的恶意 DNS 60.205.130.150 为例，查询 DNS 服务器中 ttl 时间，可以通过 dig 发送任意一个未解析过的域名，此处的 daydaymap.com 可替换为随机其它域名。

```
dig @60.205.130.150 daydaymap.com
```

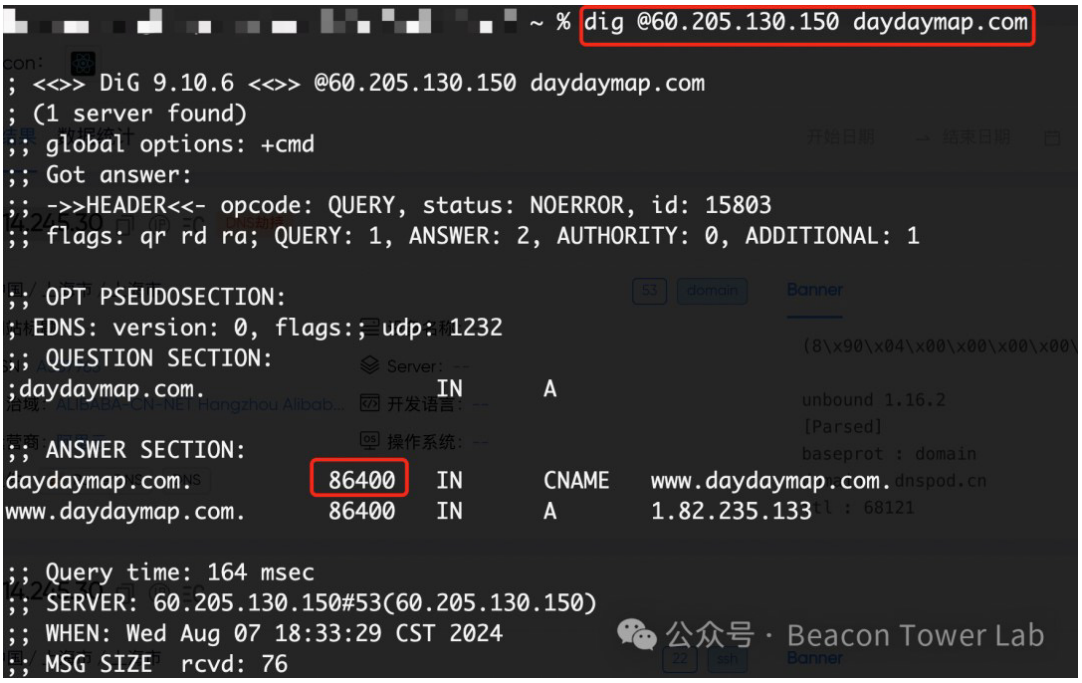


图 3-8-4 查询 DNS 服务ttl时间

查询 DNS 服务器中版本名称，可以通过 dig 发送 version.bind 的 txt 查询请求，并通过 chaos 的方式进行展示。

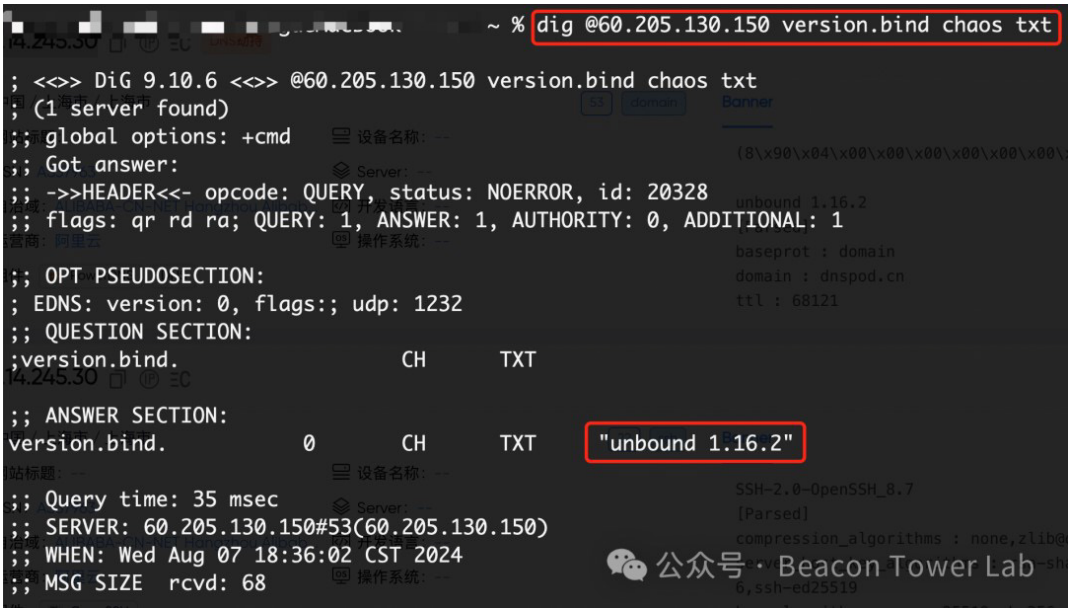


图 3-8-5 查询 DNS 服务器版本名称

如果满足以上两个特征，基本就可以认定是被劫持的 DNS 服务器。我们基于以上特征对互联网上的 DNS 服务器做了全网摸排，情况不容乐观。典型的被劫持IP包括：

```
47.109.22.11
8.140.204.39
47.108.228.50
47.103.220.247
39.108.114.149
120.77.221.246
106.15.3.137
120.26.147.194
106.15.192.10
106.14.245.30
47.108.190.138
47.106.38.96
47.100.115.82
122.9.187.125
120.79.129.196
47.108.55.233
123.56.132.204
101.37.182.110
101.201.60.214
```

图 3-8-6 典型被劫持 IP

目前这些 IP 都还存活，且基本都是国内公有云上的 IP，更多被劫持的 IP 我们会在 www.daydaymap.com 上陆续公开出来，查看方式如下：

访问 DayDayMap 首页，点击 DNS 劫持标签：

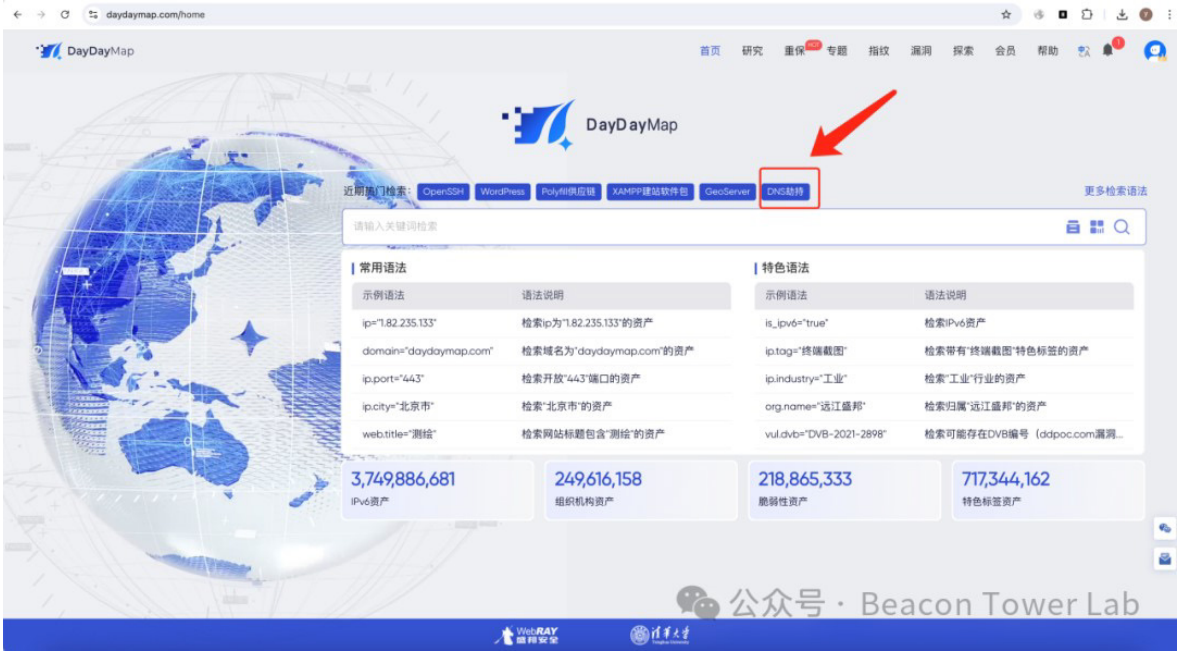


图 3-8-7 DayDayMap 的 DNS 劫持标签

点击后会检索语法 ip.tag="DNS 劫持"，列出已探测到的被篡改的 DNS 地址：

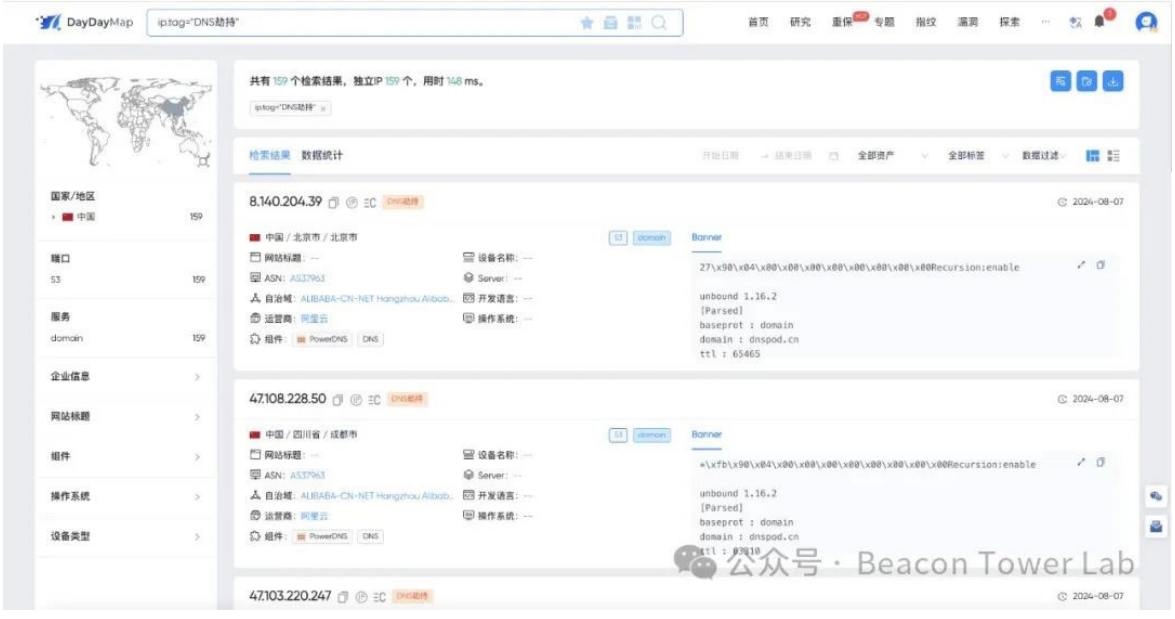


图 3-8-8 DayDayMap 查询 DNS 劫持 IP

用户自查方式：

1、登陆路由器后台，查看现有的 DNS 配置，如果备用 DNS 地址已被改为了 1.1.1.1 ，需要尤其引起注意！

2、将主备 DNS 地址输入 www.daydaymap.com 进行查询，看是否有“ DNS 劫持”的标签，如存在该标签，尽快更换路由器并进行终端安全检测。

3.9. 微软蓝屏事件测绘

2024 年 7 月 19 日下午 2 点左右，一场突如其来的事件席卷全球：大量外资企业和机构的 Windows 机器出现蓝屏死机（ BSOD ）问题。这一事件波及范围广泛，受影响的机器不仅自动蓝屏，还无法通过重启解决问题，导致多家知名机构和企业的业务中断，引发了全球范围内的广泛关注和讨论。

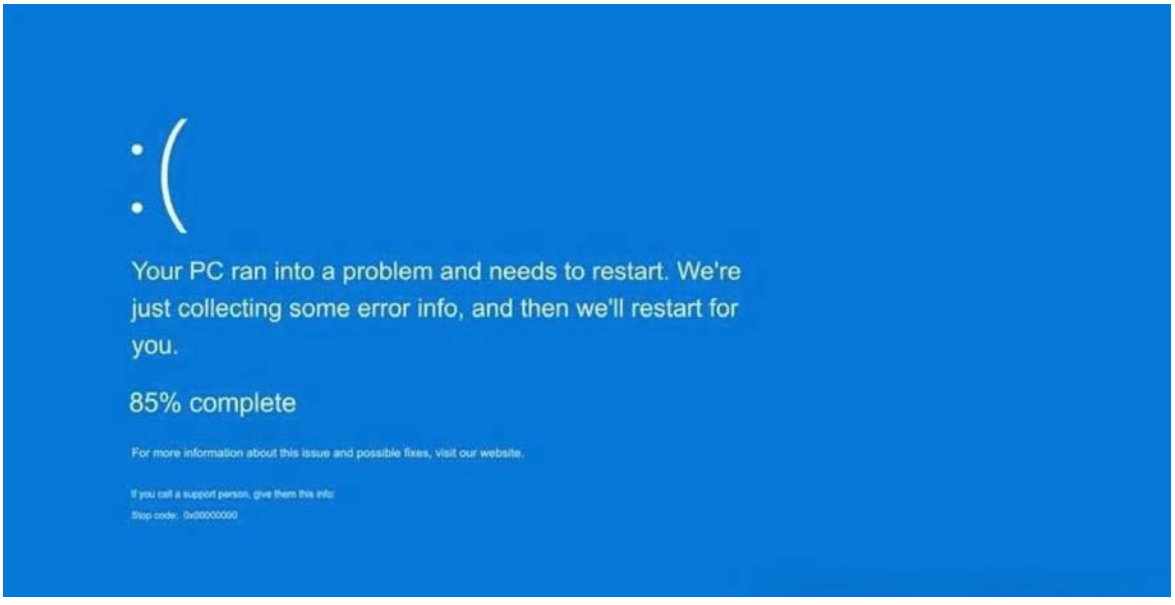


图 3-9-1 Windows 蓝屏死机

1、蓝屏事件带来的全球性影响

在短时间内，全球多个地区爆发了因蓝屏导致的业务无法正常开展的事件，影响了各行各业：

• **美国航空业：**美国达美航空、联合航空和美国航空等主要航空公司的所有航班受蓝屏事件影响，宣布当天上午停飞。数以千计的乘客行程被迫取消或延误，航空公司的运营受到严重打击。

• **Microsoft 365服务：**部分用户无法访问 Microsoft 365 订阅服务，包括 SharePoint Online、OneDrive for Business、Teams 等核心应用，给企业的日常运作带来了极大不便。

• **金融市场：**英国伦敦证券交易所宣布因蓝屏事件暂停交易，金融市场的稳定性受到威胁。

• **公共交通：**日本轨道交通公司因蓝屏事件无法查看列车实时运行情况，被迫取消多条线路，影响了无数通勤者的出行。印度靛蓝航空、阿卡萨航空和香料航空在内的多家航空公司受蓝屏事件影响停飞，航班运营因此中断。

• **各行业影响：**澳大利亚的航空公司、银行、政府网络、企业和超市自动收银机等均受到影响，日常生活和经济活动陷入混乱。

• **在中国的企业：**上海的多家外企受到影响，环球影城和迪士尼等娱乐设施无法正常结算，游客体验大打折扣。

2、事件原因及应对

微软发言人迅速回应称，此次蓝屏事件是由第三方软件平台更新引发的。具体来说，安全软件公司 CrowdStrike 的 Falcon Sensor 安全产品更新导致了 Windows 电脑蓝屏。CrowdStrike 是美国加利福尼亚州森尼韦尔的一家电脑安全技术公司，主要提供端点安全、情报威胁和网络攻击的安全服务。

CrowdStrike 创始人兼 CEO George Kurtz 在社交媒体上回应称，CrowdStrike 正积极与受影响的客户合作，解决这一问题。需要注意的是，Mac 和 Linux 主机不受此次事件影响，这也进一步表明此次事件并非网络攻击或安全事件。目前，CrowdStrike 已提供了临时解决方案：受影响的用户需将电脑启动到安全模式或恢复环境，导航至 C:\Windows\System32\drivers\CrowdStrike 目录，找到与“C-00000291*.sys”匹配的文件并将其删除，以恢复正常启动。

3、对网络安全的深刻启示

尽管此次蓝屏事件并非网络攻击所致，但它揭示了 Windows 操作系统在全球互联网中的重要性及其潜在的安全风险。根据 DayDayMap 全球互联网资产测绘平台（www.daydaymap.com）数据显示，Windows 操作系统在全球范围内的使用量极大，其中中国的 Windows 用户占比接近 60%。

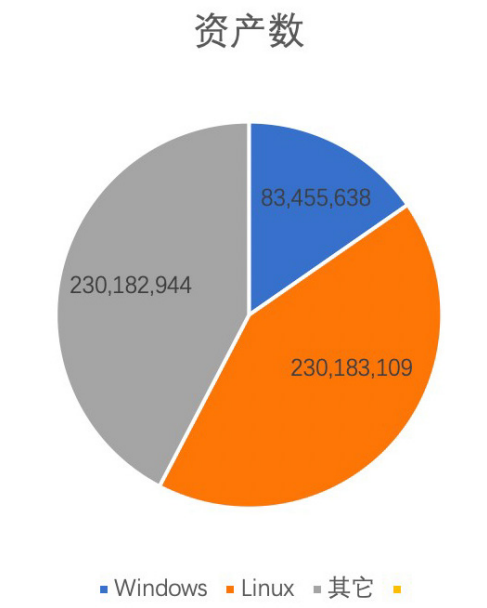


图 3-9-2 全球操作系统分类占比

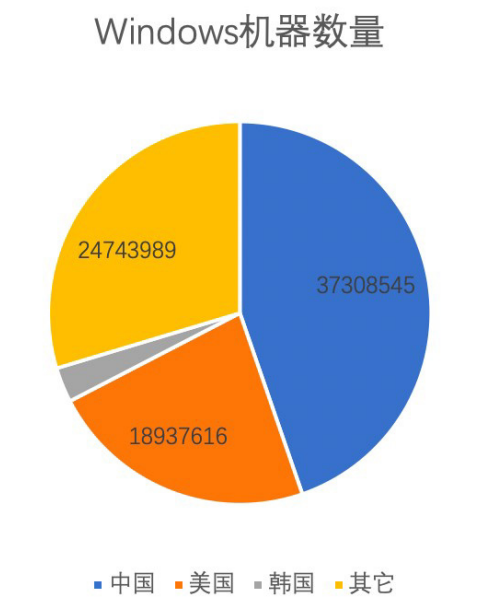


图 3-9-3 全球Window 机器分布

从上面的数据可以看出，如果某个 Windows 操作系统层面的漏洞被别有用心的攻击者控制，将对国家安全造成严重的安全隐患。当前中美关系紧张，如果由美国控制的微软公司在 Windows 操作系统的升级程序中植入恶意程序，一方面可以窃取大量国内单位的敏感信息，另一方面也可以对关基设施进行毁瘫，其造成的安全隐患会非常巨大，对供应链安全来说也提出了新的挑战。

本次微软蓝屏事件虽然不是由网络攻击造成的，但是 Windows 操作系统潜在的破坏性仍然值得相关单位警惕。我们很难保证在特殊时刻美国不会把 Windows 作为攻击我国的武器，对我国敏感设施进行网络攻击。由此可见，国家发展具有国家自主知识产权的信创产品（包括国产化操作系统、数据库、中间件等）是具有长远战略意义的。

4、修复

CrowdStrike 官方的解决方案是删除该公司驱动程序，最终使得驱动程序失效。具体操作为，建议受影响的用户将电脑启动到安全模式或恢复环境，导航至 C:\Windows\System32\drivers\CrowdStrike 目录，找到与“C-00000291*.sys”匹配的文件并将其删除，即可正常启动电脑。

4. 行业分析

4.1. 金融资产测绘

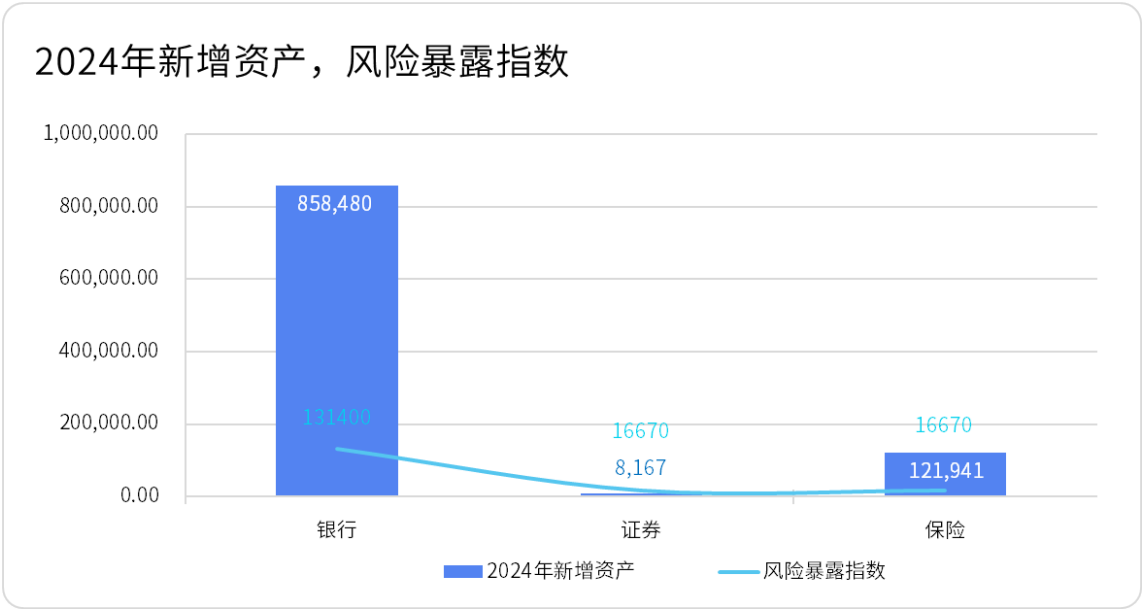


图 4-1-1 2024 年银行证券保险新增资产和风险暴露指数

2024 年，金融行业在全球经济格局中持续扮演着核心枢纽角色，网络空间资产作为支撑金融业务高效运转的关键要素，其规模庞大、架构复杂，涵盖了银行、证券、保险等众多细分领域的核心系统、交易平台、数据中心以及海量终端设备,如图 4-1-1 根据测绘数据分析，银行业务分布更广，互联网 APP 等暴露的风险指数更高。识别金融网络资产全貌，能够提前锁定系统漏洞、错误配置以及潜在的攻击切入点，狙击黑客的恶意侵袭、防范客户数据泄露，抵御金融诈骗团伙的网络钓鱼攻击，资产测绘所生成的详实情报都为制定针对性极强的安全策略奠定了坚实基础。随着全球金融监管法规日益严苛，如巴塞尔协议对金融机构风险管理的强化要求、各国数据保护法规对客户隐私的严格规范，金融企业必须精准把控自身网络资产状况，然而金融核心业务仍存在大量缓冲区溢出漏洞、权限提升漏洞，这些漏洞一旦被利用，可能导致交易数据被篡改、客户资金被盗取。

端口		服务		操作系统		组件		设备类型	
443	1,637,723	https	177,183	linux	27,271	银行	1,440,313	安全防护设备	10,951
80	14,900	tls	4,896	windows	17,601	akamaighost	1,287,511	其它网络设备	4,927
8443	11,277	ssl-err	2,653	windows server 2016	2,301	akamai cdn	1,261,990	负载均衡设备	3,634
8089	2,871	imaps	66	ubuntu linux	1,478	digicert	676,194	认证服务器	705
4443	2,427	pop3s	55	red hat linux	1,338	cert_untrust	593,491	云服务资源	453

图 4-1-2 2024 年金融网络空间资产测绘分类统计

金融核心业务系统风险，以某国际知名银行的信贷管理系统为例，在 2024 年第二季度被发现存在 SQL 注入漏洞。黑客利用该漏洞，通过精心构造恶意 SQL 语句，绕过系统身份验证，成功登录系统后台，窃取了大量企业客户的信贷资料，包括贷款金额、还款计划、抵押物信息等，不仅给银行带来巨大的潜在信用风险，还引发了严重的客户信任危机。攻击者通常先通过网络情报收集，锁定金融机构的核心业务系统域名或 IP 地址，然后利用漏洞扫描工具，如 Nessus、OpenVAS 等，全面探测系统漏洞。一旦发现可利用漏洞，便根据漏洞类型精心编写攻击脚本，尝试获取系统最高权限，进而窃取敏感数据或植入恶意程序，长期潜伏监控，等待最佳时机发动更大规模的攻击。

金融网络基础设施风险，全球相当金融机构网络设备存在不安全的配置，大量路由器开放不必要的高危端口，并有防火墙策略配置不当等问题，允许外部非法流量进入内部网络，极大地增加了网络被入侵的风险。在 2024 年 5 月，某证券交易所网络遭受攻击，原因是其边缘网络的一台交换机存在默认配置未更改问题，攻击者利用交换机 SNMP ，获取了网络拓扑结构和设备运行状态信息，进而通过 ARP 欺骗技术，将内部网络流量导向其控制的恶意服务器，窃取了大量实时交易数据，导致当日部分股票交易出现异常波动，市场信心受挫。攻击人员通过大范围搜索金融机构网络边界的开放端口，一旦发现上述高危端口或配置薄弱的网络设备，便针对端口对应的服务漏洞或设备配置缺陷进行攻击。

金融移动终端风险，在移动金融领域，金融一半的 APP 存在至少一个安全漏洞，其中部分涉及隐私泄露漏洞，如未加密存储用户登录凭证、敏感信息明文传输，存在权限滥用漏洞，APP 申请过多不必要的手机权限，如获取通讯录权限却未用于正当业务功能，增加用户信息泄露风险。在 2024 年 9 月被曝光存在未加密存储用户银行卡信息的漏洞。黑客通过逆向分析 APP 代码，轻松获取用户银行卡号等关键支付信息，随后利用这些信息在电商平台进行盗刷，导致大量用户遭受经济损失，银行也面临着客户投诉和监管处罚的双重压力。攻击者首先从应用商店或

黑市获取金融 APP，利用反编译工具对其进行逆向分析，查找潜在漏洞。一旦发现隐私泄露或权限滥用等漏洞，便通过恶意软件植入、网络劫持等手段，窃取用户在使用 APP 过程中的敏感信息，或操控APP进行非法转账、查询等操作，实现经济利益最大化。

4.2. 能源资产测绘

本次能源资产测绘分析，覆盖石油、天然气、电力等主流能源领域。能源作为全球经济发展的命脉，其行业的数字化转型进程持续加速。从传统的石油、天然气开采与输送，到新兴的太阳能、风能发电，以及智能电网的广泛应用，网络空间资产已深度渗透至能源产业链的各个环节。2024 年监测到新增能源服务 top5 的 https 为 2,555,204；http 为 165,247；ethernetip 为 29,988；bacnet 为 26,726；modbus 为 20,846 。暴露最多的国家分别是韩国、美国、中国、卡塔尔、日本。

图 4-2-1 2024 年全球能源行业暴露资产分布统计

其中近一年新增使用设备类型最多的为物联网设备 2,470,082；工业控制设备 195,472 ；路由交换设备 1,050；安全防护设备 255。Linux：26,838；android：23,181；windows：8,773；ubuntu linux：3,977；embedded：2,437。

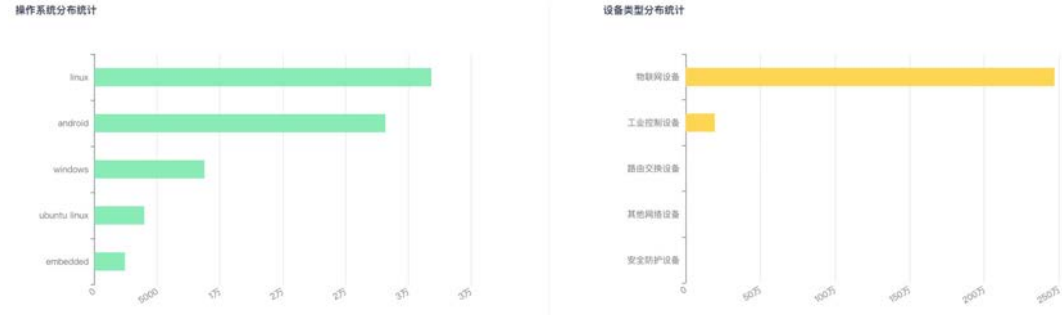


图 4-2-2 2024 年全球能源行业暴露操作系统和设备类型分布统计

全球能源生产存在资产分布广、老旧系统众多、工控系统品牌多、地理位置分散、防护薄弱等特点。能源生产控制系统中存在较多已知未修复漏洞，如缓冲区溢出漏洞、权限提升漏洞，这些漏洞一旦被利用，可能导致能源生产流程失控、关键设备损坏，或窃取敏感数据或植入恶意程序，长期潜伏监控，等待最佳时机发动更大规模的攻击，干扰能源生产进程，甚至引发灾难性的安全事故。以某中东地区大型石油开采公司为例，在 2024 年第二季度，其钻井平台的自动化控制系统被发现存在缓冲区溢出漏洞。黑客利用该漏洞，通过向控制系统发送精心构造的恶意数据包，成功突破系统安全防线，篡改了钻井参数，导致钻井设备失控，引发井喷事故，不仅造成了巨大的经济损失，还对当地生态环境造成了严重破坏。

2024 年 5 月，日本光伏行业工控电子制造商 Contec 遭受网络攻击，800 台 SolarView 远程监控设备被劫持，攻击者利用了未修复漏洞 CVE-2022-29303 ，通过该漏洞传播Mirai僵尸网络。大型光伏电网的中央控制系统若被入侵，黑客可控制多个光伏电场，甚至中断整个电网运转。负责将太阳能板直流电转换为交流电的逆变器，因具备通信功能且连接网络或云服务，面临更严重的风险，可能成为黑客攻击的目标，进而影响电网的可靠性和稳定性。

4.3. 电信资产测绘

图 4-3-1 2024 年全球电信行业暴露资产分布可视化

电信行业作为全球信息通信的核心枢纽，在支撑经济社会数字化转型、促进信息互联互通方面发挥着无可替代的作用。其网络空间资产涵盖了从基础网络设施到各类通信服务平台，规模庞大且结构复杂。电信行业网络资产是实现全球语音通话、数据传输、互联网接入等通信服务的基础保障。2024年暴露监测新增 TOP5 的国家分别为中国、日本、法国、德国、美国。

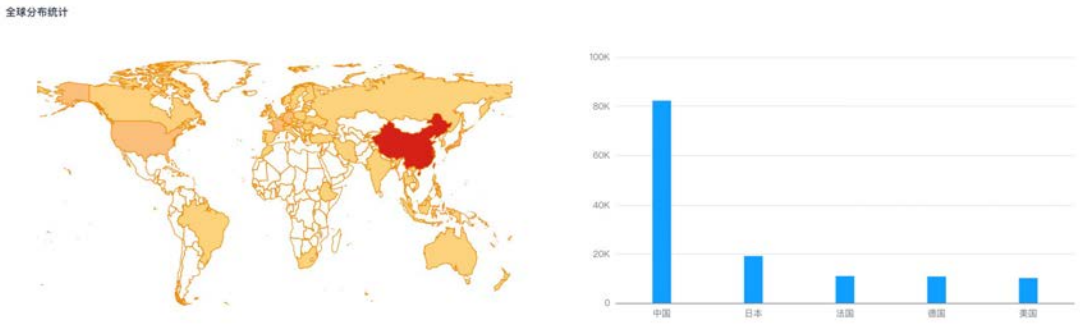


图 4-3-2 2024 年全球电信行业暴露资产 TOP5 分布统计

电信企业借助资产测绘可清晰掌握自身网络资产布局及状态变化，进而优化资源配置，在 5G 、物联网、云计算等新兴技术应用与业务拓展方面抢占先机，推动行业持续创新升级。本次分析涉及到全球电信行业网络空间，覆盖包括移动运营商、固定网络运营商、互联网服务提供商（ISP）等在内的各类电信主体。从核心网、传输网、接入网等基础网络设施，到移动语音、短信、移动数据、宽带互联网等业务系统，再到云平台、大数据中心以及为客户提供服务的各类终端设备等全方位的网络资产。2024 年暴露监测中国新增 TOP5 的区域分别为广东省、浙江省、江苏省、内蒙古自治区、北京市。

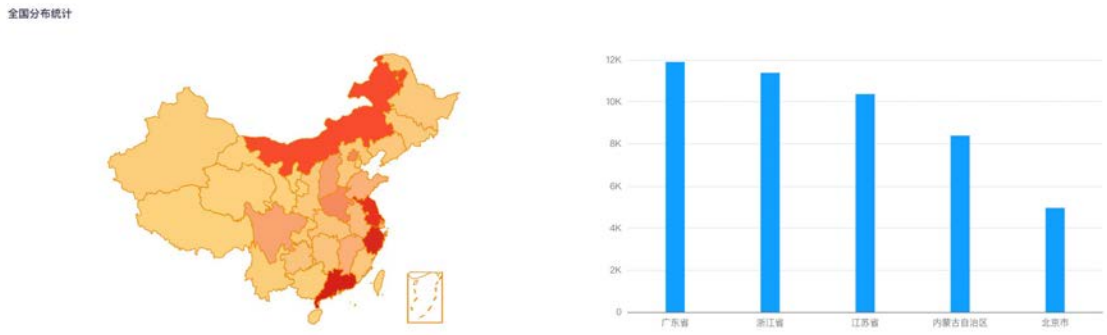


图 4-3-3 2024 年中国电信行业暴露资产 TOP5 分布统计

暴露的端口和服务占比统计如下：

图 4-3-4 2024 年全球电信行业暴露服务和端口分布统计

暴露的设备类型统计如下：

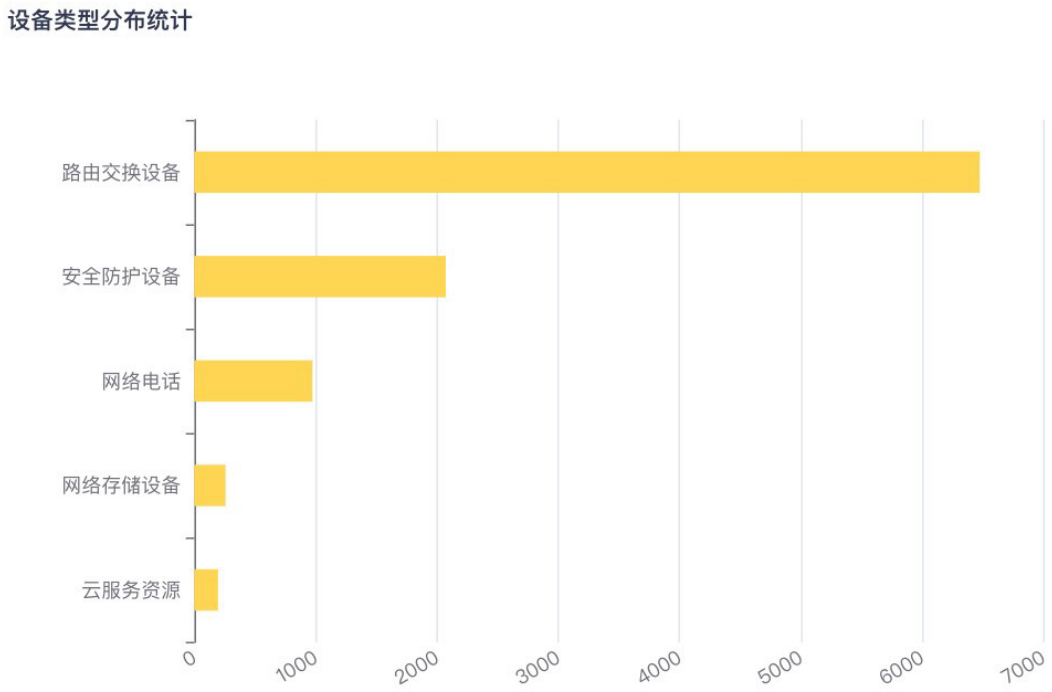


图 4-3-5 2024 年全球电信行业暴露设备类型分布统计

全球的电信核心网络设施存在已知未修复漏洞，如远程代码执行漏洞、配置漏洞导致的网络路由篡改风险等。这些漏洞一旦被利用，可能导致网络拥塞、通信中断，甚至核心网络被非法控制，影响大规模用户的通信服务。例如在 2024 年 4 月，某大型移动运营商的核心网路由器被发现存在远程代码执行漏洞。黑客利用该漏洞，通过网络向目标路由器发送特制的恶意数据包，成功在路由器上执行恶意代码，篡改了部分路由表项，使得部分地区的用户手机信号出现异常，通话中断、数据业务无法正常使用，引发大量用户投诉，对运营商的声誉造成了严重损害。

2024 年 4 月，某海外运营商的核心网路由器被发现存在远程代码执行漏洞。黑客利用该漏洞，通过网络向目标路由器发送特制的恶意数据包，成功在路由器上执行恶意代码，篡改了部分路由表项，使得部分地区的用户手机信号出现异常，通话中断、数据业务无法正常使用，引发大量用户投诉，对运营商的声誉造成了严重损害。

2024 年 9 月，某海外云平台发生一起安全事件，部分云服务器因未及时更新补丁，被黑客利用一个零日漏洞入侵。黑客获取服务器权限后，不仅窃取了存储在云服务器上的企业客户业务数据，还利用虚拟机逃逸漏洞，尝试访问其他用户的云资源，严重破坏了云平台的安全性和用户信任度。

4.4. 交通资产测绘

交通行业作为国民经济的基础性、先导性产业，正加速向数字化、智能化转型。网络空间资产广泛渗透于航空、铁路、公路、水运等各个领域。本次测绘对象，面向全球交通行业网络空间，全面涵盖航空、铁路、公路、水运等主要运输方式。涉及机场航班控制系统、空中交通管理系统、铁路信号调度系统、公路智能交通管理系统、港口集装箱管理系统、船舶航行控制系统等核心业务系统；以及遍布各地的交通枢纽、线路沿线的网络基础设施，包括路由器、交换机、基站、服务器等。探测全球航空的飞行管理系统、铁路的列车运行控制系统、公路的智能交通信号控制系统、水运的船舶自动识别系统等，剖析系统架构、版本信息、暴露的端口、服务漏洞状况。

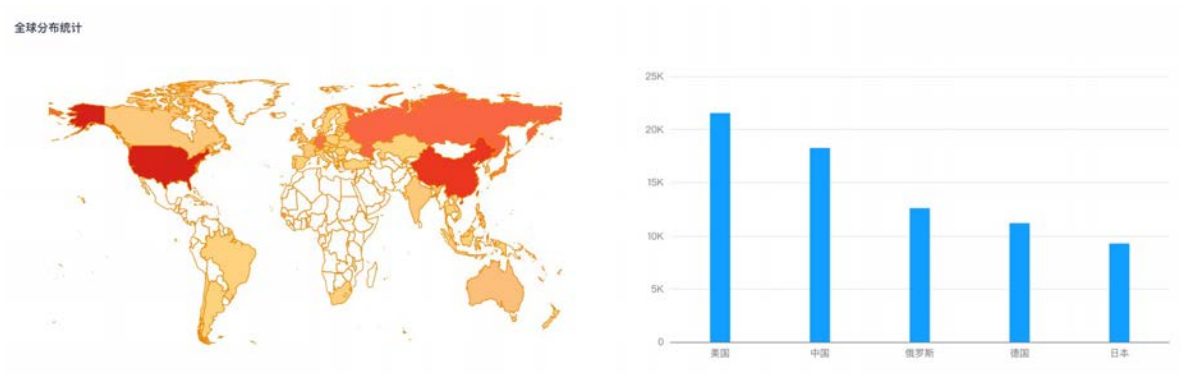


图 4-4-1 2024 年全球交通行业暴露资产 TOP5 分布统计

2024 年暴露监测新增 TOP5 的国家分别为美国、中国、俄罗斯、德国、日本。

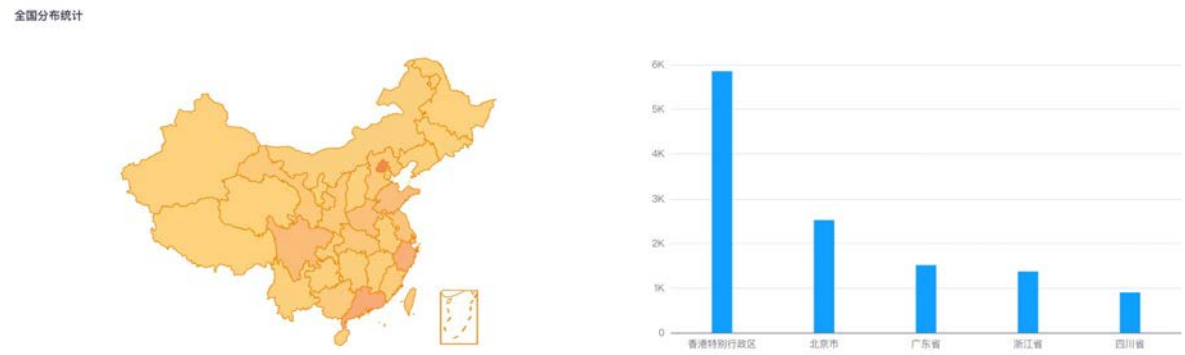


图 4-4-2 2024 年中国交通行业暴露资产 TOP5 分布统计

2024 年暴露监测中国新增 TOP5 的区域分别为香港特别行政区、北京市、广东省、浙江省、四川省。

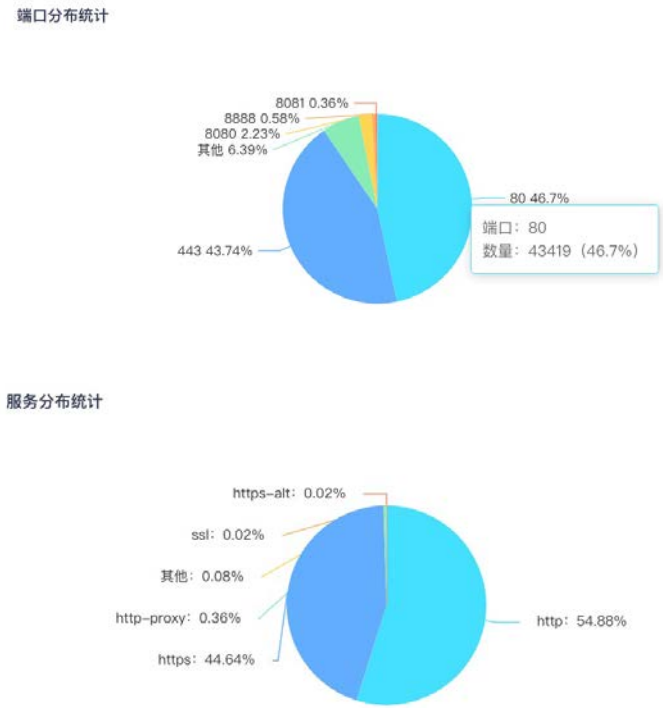


图 4-4-3 2024 年全球交通行业暴露服务和端口分布统计

全球交通核心业务控制系统存在权限绕过漏洞、远程代码执行漏洞等漏洞，这些漏洞一旦被利用，可能导致交通指挥失控，引发严重安全事故。且较多的交通网络基础设施存在不安全配置，其中大量路由器开放不必要的高危端口。2024 年，某航班控制系统被发现存在权限绕过漏洞。黑客利用该漏洞，伪装成合法管理员登录系统，篡改航班起降时间、登机口分配等关键信息，致使多架航班延误、旅客滞留，不仅造成巨大经济损失，还严重影响机场声誉和旅客出行体验。2024年10月，美国某州的公路收费系统因数据库安全漏洞而发生数据泄露问题，大量用户的个人信息和车辆信息被泄露。黑客利用该数据库“访问控制机制不完善”的漏洞，通过非法获取管理员权限，直接访问数据库，窃取了大量用户数据，包括姓名、地址、车牌号、信用卡信息等。此外，该系统在数据传输过程中，对数据的加密处理也存在缺陷，使得黑客能够在数据传输过程中截获并破解加密数据，进一步获取用户的敏感信息。

5. 资产暴露的影响与成本评估

5.1. 业务风险

• 数据泄漏

资产暴露可能造成企业数据泄露，企业在发现数据泄露后，需要立即投入资源开展检测工作，确定泄露源头、范围以及影响程度等。这涉及到调用内部安全团队或聘请外部专业安全机构进行调查，可能使用专业的数据分析工具、入侵检测系统等，相关成本包括人力成本、工具采购或使用费用等，根据泄露规模和复杂程度不同，这部分费用可能从几千元到数十万元不等。例如，小型电商企业发生小规模数据泄露，聘请外部安全顾问进行初步检测和分析，可能花费 2 - 3 万元；而大型金融机构遭遇大规模数据泄露时，仅专业工具的临时租用费用就可能达到数十万元。

修复受损的数据系统、数据库结构以及加强安全防护措施是后续关键步骤。这可能需要对数据库进行重新配置、打补丁、加密升级等操作，同时要对相关应用程序进行漏洞修复和安全优化。购买加密软件、数据库管理工具以及支付技术人员加班费用等，都构成这部分成本，花费范围大致在几万元到几百万元。比如，一家中型互联网企业在数据泄露后，对数据库进行全面加密和漏洞修复，购买软件及人力投入累计花费约 50 万元左右。

按照法律法规以及道德责任要求，企业必须及时通知受影响的用户、合作伙伴、监管部门等相关方。通知方式多样，如发送邮件、短信，甚至可能需要刊登报纸公告等，同时还需安排客服团队应对各方咨询和投诉，这会产生通信费用、公告费用以及人力成本等。以通知 10 万名用户为例，仅短信通知费用按每条 0.05 元计算，就需要 5000 元，加上其他成本，总花费可能达到数万元。

为了降低用户因数据泄露而面临的后续风险，企业往往需要为受影响用户提供一定期限的信用监控服务或者协助用户采取身份保护措施，如购买专业的信用监控服务套餐、提供身份盗窃保险等。若涉及大量用户，这将是一笔可观的费用，例如为 100 万名用户提供一年的信用监控服务，按每人每年 10 - 20 元的服务价格估算，费用可达 1000 - 2000 万元。

数据泄露事件曝光后，客户对企业的信任度会大打折扣，直接导致业务量下滑。对于依赖客户数据开展精准营销、个性化服务的企业影响尤为明显，新客户获取难度增大，老客户流失严重。例如，在线旅游平台数据泄露后，用户担心个人信息安全，预订量可能锐减 30%-50%，若平台原本年营收为 10 亿元，那么业务损失可能达到 3-5 亿元。

企业的品牌形象会因数据泄露事件遭受重创，负面舆论在社交媒体等平台迅速传播，影响潜在客户的选择。为挽回声誉，企业需要投入大量资金进行品牌重塑活动，如开展广告宣传、赞助公益活动、参与行业展会等，这些费用少则几百万元，多则数千万元甚至更多，且声誉恢复是一个长期过程，后续还需持续投入。

受影响的用户、合作伙伴或者监管机构可能会对企业提起法律诉讼，要求赔偿损失。企业不仅要承担自身的律师费、诉讼费等法律相关费用，还可能需要向原告支付高额赔偿款。例如，在一些大规模数据泄露导致用户隐私严重受损的案例中，企业最终支付的赔偿总额加上法律费用可能达到数亿元。

• 网络中断

资产暴露可能被入侵导致网络中断，网络中断发生后企业需迅速组织技术人员进行抢修，查找故障点、修复受损设备（如路由器、交换机、工控系统、生产系统故障维修或更换）、恢复服务器运行等，可能涉及硬件设备采购、软件系统重新安装配置等，同时技术人员加班加点产生的人工费用也不容忽视。对于中等规模企业，一次持续数小时的网络中断，应急修复成本可能在几万元到几十万元之间。而大型的能源工控生产业务，应急修复成本可能达到数千万到数亿元。

为了尽快恢复业务运营，企业可能会采取临时措施，如租用备用服务器、增加网络带宽、调用备份数据等，这些额外的资源投入都会增加成本。例如，金融企业在核心交易系统网络中断期间，租用高规格的备用服务器以保障部分紧急业务能够继续办理，按天计算的租金可能高达数万元。

网络中断会使企业的日常运营陷入停滞，无法正常接收订单、处理业务、提供服务等，导致收入锐减。制造业企业生产线因网络故障停工，每小时的产值损失可能达数十万元；电商企业无法处理订单，错过销售旺季的订单高峰，损失更是难以估量。

长时间的网络中断会让客户对企业的服务能力产生质疑，从而转向竞争对手，合作伙伴也可能因担心合作风险而减少合作项目或终止合作关系，这对企业未来的市场拓展和业务发展带来长期的负面影响，损失可能体现在未来数年的营收减少上。

• 合规性罚款

如欧盟的《通用数据保护条例》（GDPR）规定，企业若未能妥善保护用户数据，导致数据泄露等违反规定的情况发生，将面临高额罚款。罚款额度最高可达企业全球年营业额的 4% 或 2000 万欧元中的较高者。例如，一家跨国科技企业年营业额为 50 亿欧元，若因资产暴露引发的数据泄露事件违反 GDPR，可能面临高达 2 亿欧元的巨额罚款，这对企业的财务状况将产生极其严重的冲击。

5.2. 社会风险

金融行业的核心资产如银行的核心交易系统、证券交易所的交易撮合系统、支付清算系统等若暴露并遭受攻击，可能引发系统性金融风险。例如，黑客入侵银行系统，篡改客户账户余额、交易记录等信息，会导致金融交易的混乱，客户资金安全无法保障，进而引发挤兑风波，影响整个金融市场的稳定。同时，支付清算系统故障可能使资金流转受阻，影响企业间的贸易结算、个人的日常消费支付等，波及范围广泛，甚至可能引发全球性的金融动荡。金融数据泄露还可能被不法分子用于金融诈骗活动，通过分析客户交易习惯、资产状况等信息，精准实施诈骗，导致大量个人和企业遭受经济损失，破坏金融生态的健康发展，削弱社会对金融体系的信任度。

能源行业的关键基础设施包括电力的发电、输电、配电系统，石油天然气的开采、输送管道以及能源储备设施等。若这些资产暴露出现安全漏洞，黑客攻击可能导致电力供应中断，影响医院、交通枢纽、通信基站等重要设施的正常运行，给人们的生活和社会秩序带来极大不便。例如，大面积停电可能使电梯停止运行，危及被困人员生命安全；交通信号灯失灵，引发道路交通事故和拥堵；通信基站断电，影响应急通信和人们的日常通信联络。石油天然气管道若被攻击导致泄漏或爆炸，不仅会造成周边环境的严重破坏，威胁居民生命财产安全，还可能引发能源供应短缺，导致能源价格大幅波动，影响工业生产、居民取暖等诸多方面，对整个社会的经济运行产生连锁反应。

交通领域的关键资产涵盖航空的飞行控制系统、机场塔台指挥系统，铁路的信号调度系统、列车运行控制系统，公路的智能交通管理系统以及水运的船舶导航与监控系统等。一旦这些系统资产暴露被攻击，后果不堪设想。例如，航空飞行控制系统遭到黑客干扰，可能导致航班偏离航线、失去控制，引发空难事故，造成大量人员伤亡；铁路信号系统故障会使列车发生追尾、脱轨等严重事故，危及乘客生命安全，同时导致铁路运输瘫痪，影响货物运输和人员出行，打乱整个物流供应链和社会出行计划。公路交通管理系统出现问题，交通信号灯失灵、电子收费系统故障等，会造成城市交通拥堵加剧，影响应急救援车辆的快速通行，耽误救援黄金时间，在遇到自然灾害、突发事件时，无法保障救援通道畅通，增加社会的不稳定因素。

电信网络作为信息传播的关键基础设施，其核心资产如骨干网络、基站、域名服务器（DNS）等若暴露受攻击，会出现大面积网络中断、通信瘫痪的情况。人们无法正常拨打电话、发送短信、使用互联网，这在现代社会将严重影响人们的生活、工作以及应急救援等活动。例如，在发生地震等自然灾害时，若电信网络瘫痪，灾区与外界的通信联络受阻，救援指挥无法有效开展，延误救援时机，增加灾害损失。随着5G、物联网等新兴技术的发展，大量智能设备接入电信网络，若这些设备相关资产暴露被控制，可能被利用发动大规模的网络攻击，如分布式拒绝服务攻击（DDoS），进一步冲击整个电信网络乃至其他关联的关键基础设施，威胁国家安全和社会稳定。

6. 改进建议与防护措施

6.1. 业务层面

• 资产识别与监控

定期进行数字资产测绘：

企业应制定完善的资产测绘计划，按照固定周期（如每月或每季度）对自身的数字资产进行全面梳理，包括但不限于网络设备（路由器、交换机、防火墙等）、服务器、数据库、应用程序、云服务资源以及各类终端设备等。通过资产测绘，清晰掌握资产的数量、分布、运行状态、所属业务系统等关键信息，构建详细的资产清单，以便在面对潜在风险时有准确的对象进行分析和应对。

利用专业的资产测绘工具，结合人工核查的方式，确保资产信息的准确性和完整性。例如，网络空间资产测绘平台和一些网络扫描工具可以帮助发现网络中新增或遗漏的设备，同时安排专人对业务系统中的关键应用和数据资产进行手动盘点，避免出现遗漏。并且在企业网络架构发生变更（如新增业务线、拓展分支机构、采用新的云服务等）时，及时更新资产清单，保证资产信息与实际情况相符。

部署安全防护工具（如 WAF、EASM 平台）：

Web应用防火墙（WAF）：对于面向互联网提供服务的网站和 Web 应用程序，部署 WAF 至关重要。它能够基于预设的规则和算法，实时监测和过滤来自互联网的网络流量，识别并拦截诸如 SQL 注入、跨站脚本攻击（XSS）、恶意文件上传等常见的 Web 攻击行为，保护 Web 应用的安全。例如，当黑客试图通过在网站登录页面输入恶意 SQL 语句来窃取数据库信息时，WAF 能够检测到异常流量模式并阻断该请求，防止数据泄露和系统被入侵。

外部攻击面管理（EASM）平台：借助 EASM 平台，企业可以从外部攻击者的视角，全面监测自身在互联网上暴露的资产情况，包括域名、IP 地址、开放端口、运行服务等信息，及时发现可能被利用的风险点。它能自动扫描互联网环境，分析资产的脆弱性，提供风险评估报告，并对潜在的威胁进行预警。例如，若企业某个测试服务器因配置失误意外暴露在公网上，EASM 平台可以迅速检测到并提醒企业及时采取措施进行修复或隐藏，避免被黑客发现并攻击。

• 端口与服务管理

关闭未使用端口：企业应定期对网络设备和服务器上的端口进行清查，明确各业务系统实际所需的端口，并关闭那些长期未使用或者不必要的端口。例如，对于只用于内部办公且不需要远程访问的服务器，可关闭远程桌面协议（RDP）对应的 3389 端口，防止外部攻击者通过扫描发现该端口开放后尝试进行暴力破解攻击。关闭不必要端口可以有效减少企业网络的攻击面，降低被入侵的风险。

限制高风险服务访问：识别并梳理企业网络环境中存在的高风险服务，如 Telnet（端口 23）服务，因其采用明文传输认证信息，容易被攻击者截获用户名和密码，应尽量避免使用；若确实因业务需求必须开启某些高风险服务，要严格限制其访问来源，通过设置访问控制列表（ACL）、防火墙规则等方式，仅允许特定的 IP 段（如企业内部办公区域的 IP 地址范围）进行访问，禁止来自外部互联网的随意连接，确保高风险服务在可控范围内运行，最大程度降低安全风险。

• 漏洞管理

及时应用补丁：建立完善的补丁管理机制，安排专人关注操作系统、数据库、应用程序等各类软件供应商发布的安全补丁信息，及时下载并在测试环境中进行兼容性测试，确保补丁不会对现有业务系统造成负面影响后，迅速在生产环境中进行部署应用。例如，当微软发布 Windows Server 操作系统的重要安全补丁，用于修复可能导致远程代码执行的漏洞时，企业的系统管理员应尽快获取该补丁，在测试服务器上验证无误后，在所有运行该操作系统的生产服务器上进行安装，防止黑客利用未修复的漏洞入侵系统。对于一些关键业务系统，可与软件供应商协商获取提前的补丁通知或者优先获取渠道，以缩短补丁应用的时间差，降低因漏洞未及时修复而被攻击的窗口期。

持续漏洞扫描：利用专业的漏洞扫描工具，定期（如每周或每月）对企业的网络环境、系统和应用进行全面的漏洞扫描，涵盖网络层面的端口扫描、服务漏洞检测，以及应用层的代码漏洞分析等。扫描完成后，根据漏洞的严重程度（如高危、中危、低危）进行分类整理，生成详细的漏洞报告，明确指出漏洞所在位置、可能造成的危害以及修复建议等信息。针对扫描发现的漏洞，制定合理的修复计划，按照优先级顺序进行处理，对于高危漏洞要立即采取措施修复，确保企业网络资产始终处于相对安全的状态，同时将漏洞扫描作为一种常态化的安全运维工作持续开展下去，及时发现新出现的安全隐患。

6.2. 行业层面

• 行业协作

建立跨行业的威胁情报共享机制：不同行业的企业往往面临着相似的网络安全威胁，通过建立跨行业的多源威胁情报融合共享平台，各企业可以将自身遭遇的攻击事件、发现的新型威胁、识别出的恶意IP地址、可疑域名等信息进行共享。例如，金融行业某银行发现的针对网上银行系统的钓鱼网站攻击手段，及时分享给行业的其他金融企业，提前做好防范，检查自身支付系统是否存在类似的被攻击风险，避免遭受同样的诈骗攻击。

定期组织跨行业的网络安全交流会议、研讨会等活动，促进各行业之间的沟通与协作，让安全专家和从业者能够分享应对网络威胁的最佳实践案例、新技术应用经验等，共同提升应对网络安全问题的能力，形成全行业的安全防护合力，有效应对复杂多变的网络攻击形势。

行业主管及辖区监测：各行业主管部门应加强对本行业内企业网络资产安全的监督管理，制定明确的网络安全规范和标准，要求企业定期上报网络资产状况、安全防护措施落实情况以及安全事件报告等信息，以便及时掌握行业整体的网络安全态势。例如，工业和信息化主管部门对电信行业企业进行定期检查，查看其核心网络设施的维护情况、数据保护措施是否到位等。

在辖区层面，地方政府相关部门可以联合专业的网络安全监测机构，对辖区内的重点企业、关键基础设施单位进行网络安全监测，通过部署攻击面监测平台、网络空间探测系统、监测探针、流量分析系统等手段，实时发现辖区内可能存在的资产暴露风险和网络攻击行为，并及时通知相关企业进行处置，保障本地的网络安全环境稳定。

• 政策建议

加强资产暴露监管要求：政府应出台更为严格、细致的法律法规，明确企业在网络资产保护方面的责任和义务，对于资产暴露导致的数据泄露、网络安全事故等情况制定具体的处罚措施。例如，规定企业必须在规定时间内对暴露的资产进行修复和整改，若违反规定将面临高额罚款、停业整顿等严厉处罚，促使企业高度重视网络资产安全，主动采取有效措施减少资产暴露风险。

• 教育培训

提高公众和企业对暴露资产风险的认识：面向公众开展网络安全普及教育活动，通过社区宣传、学校课程、线上科普等多种形式，向普通民众讲解资产暴露可能带来的危害，如个人隐私泄露、遭遇网络诈骗等，提高公众的安全防范意识，教导大家如何正确使用互联网服务、保护个人信息（如不随意点击不明链接、谨慎下载安装来源不明的应用程序等）。

针对企业，组织专门的网络安全培训课程和讲座，邀请专家为企业管理人员、技术人员讲解资产暴露的风险点、如何进行有效的资产安全管理以及应对网络攻击的策略等知识，提升企业整体对网络资产安全的重视程度和管理水平，帮助企业建立健全自身的网络安全保障体系。

6.3 . 人才培养

网络空间资产测绘作为网络安全领域的重要分支，其人才培养需要结合技术实践、理论知识以及行业需求，以下是相关人才培养的现状和建议：

• 现状与需求

实战化需求：网络空间资产测绘需要具备实战能力的人才，能够快速识别和管理网络资产，同时应对复杂的网络安全威胁。

多学科交叉：该领域涉及网络技术、数据管理、安全分析等多个学科，要求人才具备跨学科知识。

行业缺口：当前网络安全人才缺口较大，尤其是具备实战能力的网络空间资产测绘人才更为稀缺。

• 培养途径

高校教育：

· 专业设置：高校应加强网络空间安全、信息安全等相关专业的建设，开设网络空间资产测绘相关课程。

· 实践教学：通过实验室建设、校企合作等方式，为学生提供实践机会，如与网络安全企业合作建立实习基地。

产学研合作：

联合培养：高校与企业联合开展人才培养项目，如“网络空间安全国家急需高层次人才培养专项”，实现产学研深度融合。

技术交流：通过举办网络空间测绘大会、技术论坛等活动，促进技术交流与合作。

• 培训课程示例

红蓝对抗实战演练：

·内容包括资产梳理、漏洞挖掘、入侵检测、应急响应等。

·采用沙盘演练、靶机实战等方式，提升学员的攻防能力。

数据安全与合规管理：

针对数据安全治理、合规性管理等领域，开展认证培训。

网络空间测绘技术：

结合主被动测绘技术，培养学员对网络资产的全面识别和管理能力。

• 未来发展方向

AI技术融合：随着AI技术的发展，网络空间资产测绘人才需要掌握AI驱动的自动化测绘技术，提升效率和准确性。

国际视野：培养具有国际视野的人才，参与国际规则制定和技术交流。

通过高校、企业和社会的共同努力，可以有效提升网络空间资产测绘人才的培养质量，满足行业发展的需求。

7. 未来展望与趋势预测

7.1. 暴露资产趋势

• 未来 3-5年 资产暴露增长率预测

随着数字化转型的加速以及网络攻击手段的日益复杂，预计未来 3-5 年资产暴露的增长率将呈现上升趋势。企业和组织的数字化资产不断增加，包括数据、网络设备、应用程序等，这为攻击者提供了更多的目标。据相关机构预测，未来几年内全球企业因网络攻击导致的资产暴露事件可能会以每年 10%-15% 的速度增长。同时，物联网、云计算等新兴技术的广泛应用，也使得资产暴露的风险进一步扩大。例如，中国信息通信研究院预计，2025 年我国物联网连接设备数量将达到 85 亿，2030 年我国移动物联网连接数将达到百亿级规模，物联网设备的大量部署使得企业的攻击面增加。据中国信通院统计，当前我国云计算市场规模已超过 6000 亿元，预计 2027 年将超过 2.1 万亿元，随着各个行业上云步伐加快，云上业务及数据变得越来越重要，而云计算环境中的数据存储和处理也面临着更多的安全挑战。

• 影响增长率的因素分析

技术发展：新技术的出现和应用往往会带来新的安全漏洞和风险。如人工智能和机器学习在各个领域的广泛应用，其自身的算法和模型可能存在被攻击和篡改的风险，从而导致相关资产暴露。

网络攻击手段演变：黑客攻击手段越来越复杂和多样化，从传统的病毒、木马攻击到如今的勒索软件、供应链攻击等，攻击的频率和强度都在增加，这也将导致资产暴露的事件增多。

企业安全意识和防护能力：部分企业对网络安全的重视程度不够，安全防护措施不到位，缺乏有效的风险评估和监测机制，容易成为攻击者的目标，进而推动资产暴露增长率上升。

7.2. 新兴威胁

• 5G / 智能设备风险加剧

5G 网络风险：5G 网络的高速率、低延迟和大连接特性使其成为未来数字经济的关键基础设施，但也带来了新的安全风险。其核心网设计、无线接入网络和用户设备的交互更为复杂，潜在漏洞增多，黑客可通过针对特定协议的攻击，远程控制设备、窃取敏感信息或进行拒绝服务攻击，从而导致网络中断、数据泄露等问题。

智能设备风险：智能设备如智能家居、智能穿戴设备等的普及，使人们的生活更加便捷，但这些设备往往存在较多安全隐患。由于其计算能力和存储资源有限，安全防护机制相对薄弱，容易被黑客攻击，导致用户的个人信息、隐私数据泄露，甚至可能被用于发起更大规模的网络攻击。

• AI 风险加剧

AI 自身缺陷导致的风险：当前AI存在“幻觉”等特殊缺陷，其生成的内容可能存在错误或误导性信息，在一些关键领域如金融、医疗等的应用中，可能会导致决策失误，从而造成重大损失。此外，AI 的不可解释性、不可推论性和不可判识性等内生安全个性问题，也使得其在出现问题时难以定位故障点和进行有效的风险控制。

AI 被恶意利用的风险：AI 可被用于编写攻击软件、生成钓鱼邮件、制作恶意代码等，大大降低了网络攻击的门槛，不懂技术的普通人也可能成为黑客，导致攻击数量增加、攻击手段更加隐蔽和难以防范，进而加剧了网络安全风险。

7.3. 量子计算与抗量子加密

• 量子计算的潜在影响

量子计算具有强大的计算能力，其基于量子比特和量子门的运算方式，能够在极短时间内完成传统计算机需要大量时间才能完成的复杂计算任务。在网络空间测绘领域，量子计算可能会对现有的测绘协议产生重大影响。一方面，它可以加速网络扫描和数据分析的过程，使攻击者能够更快速地获取目标网络的资产信息，包括更高效地破解一些基于传统加密算法的防护机制，探测到隐藏更深的网络资产和漏洞。例如，利用量子计算强大的并行计算能力，攻击者可以在短时间内对大量 IP 地址进行全面扫描，分析出目标网络中更多的开放端口和服务，极大地提高测绘效率。

• 抗量子加密技术的应对策略

面对量子计算带来的威胁，抗量子加密技术应运而生。这种加密技术采用新型的数学算法和加密原理，能够抵御量子计算机的攻击。在反测绘中，抗量子加密技术可以用于保护网络资产的关键信息，防止攻击者通过量子计算手段获取。例如，基于格密码、哈希密码等新型密码体制的抗量子加密算法，可以为网络资产的标识、位置信息以及通信数据等提供更安全的加密保护，确保在量子计算环境下，攻击者难以通过测绘手段获取有价值的信息，从而重构反测绘协议，提升网络空间的安全性。

• 对测绘与反测绘协议的重构

量子计算和抗量子加密技术的发展促使测绘与反测绘协议进行重构。在测绘方面，新的协议需要考虑如何利用量子计算的优势，同时规避其可能带来的风险，例如开发基于量子计算的安全扫描技术，确保在获取网络资产信息的同时，不被抗量子加密技术阻挡，并且能够检测出采用抗量子加密保护的资产。在反测绘方面，协议需要强化对量子计算攻击的防御机制，通过加密技术和欺骗技术的结合，使攻击者即使拥有量子计算能力也难以准确测绘网络资产。例如，采用动态加密密钥管理和基于抗量子加密的蜜罐技术，让攻击者难以判断网络资产的真实情况，增加反测绘的有效性。

7.4. 虚实结合的网络空间态势

• 元宇宙与数字孪生概念

元宇宙是一个基于虚拟现实、增强现实等技术构建的虚拟世界，它与现实世界相互映射、交互，用户可以在其中进行社交、工作、娱乐等各种活动。数字孪生则是对现实世界中的实体或系统进行数字化建模，通过实时数据交互，实现对实体状态的实时监测和模拟。在网络空间中，数字孪生可以构建网络资产的虚拟模型，反映其真实的运行状态和属性。

• 对网络空间态势感知的作用

全面可视化呈现：元宇宙和数字孪生技术可以将网络空间资产以三维可视化的形式呈现出来，构建一个虚实结合的网络空间场景。管理员可以在这个虚拟场景中，直观地观察网络资产的分布、连接关系以及运行状态，实现对网络空间态势的全面感知。例如，将网络拓扑结构、服务器、网络设备等以逼真的三维模型展示在元宇宙环境中，通过实时数据更新，管理员可以随时了解各个资产的性能指标、流量情况等，及时发现潜在的安全问题。

实时模拟与预测：利用数字孪生技术对网络资产进行实时模拟，结合元宇宙的交互性，可以预测网络空间的变化趋势和潜在风险。通过在虚拟环境中模拟各种网络攻击场景，观察网络资产的响应和变化，提前制定应对策略。例如，模拟 DDoS 攻击对网络带宽的影响，预测攻击可能导致的网络瘫痪范围，从而提前调整网络配置，增强网络的抗攻击能力。

协同防御与决策支持：在元宇宙的虚拟空间中，不同的网络安全团队可以进行协同工作，共同应对网络安全威胁。通过共享数字孪生模型和实时数据，团队成员可以更直观地交流和协作，制定更有效的防御策略。同时，基于元宇宙和数字孪生提供的全面态势感知，决策者可以获取更准确的信息，做出更科学的决策，提高网络空间安全管理的效率和效果。

• 应用场景与挑战

应用场景：在大型企业网络安全管理中，利用元宇宙和数字孪生技术构建企业网络空间的虚拟模型，实现对企业内部网络资产的全面监控和管理。在智慧城市建设中，通过数字孪生技术对城市的网络基础设施进行建模，结合元宇宙的交互性，实现城市网络安全的统一管理和应急响应。

挑战：元宇宙和数字孪生技术在网络空间态势感知中的应用面临着技术复杂性高、数据隐私保护难、标准规范缺乏等挑战。例如，构建高精度的网络资产数字孪生模型需要大量的技术投入和专业知识，同时确保模型中的数据安全和隐私保护是一个关键问题。此外，由于缺乏统一的标准规范，不同系统之间的数字孪生模型和元宇宙平台可能难以实现有效对接和协同工作。

7.5. 资产测绘技术发展趋势

资产测绘是构建数字世界必备的基础技术能力，作为连接网络虚拟空间和物理空间的桥梁和安全的基础，资产测绘产品未来可期。测绘产品发展将促使资产测绘技术获得持续创新与提高，加速应用人工智能、推动测绘技术与其他安全技术的融合应用等将成为未来发展的重点领域与方向。例如，人工智能技术在测绘各环节将获得广泛应用，实现一体化智能化，自动化技术研发赋能提高测绘精度与广度。具体来看：

• AI 在资产测绘与风险识别中的应用前景

AI 技术可以通过机器学习算法对海量的网络数据进行分析，自动识别企业网络环境中的资产信息，包括那些隐藏较深或者容易被忽视的资产。例如，通过对网络流量模式的学习，AI 能够准确判断出某个新出现的 IP 地址是否属于企业内部资产但未被登记在册，及时发现新增的未知资产，完善资产清单。

在风险识别方面，AI 可以根据历史的网络攻击数据、漏洞信息以及资产的运行状态等多维度因素，构建风险预测模型，提前预判潜在的资产暴露风险点。比如，通过分析以往黑客攻击企业数据库系统时的行为特征，AI 能够在类似的异常流量出现时，快速准确地识别出可能正在进行的攻击尝试，并及时发出预警，帮助企业提前采取防御措施，有效降低损失。

• 外部攻击面管理、零信任架构对资产暴露的缓解作用

外部攻击面管理（EASM）：随着企业网络边界逐渐模糊，传统的基于边界防护的安全策略面临挑战，EASM 从外部视角持续监测企业暴露在互联网上的所有资产，实时掌握资产的变化情况和风险态势。它能够精准定位那些可能被外部攻击者利用的漏洞和薄弱环节，通过及时修复、隐藏不必要资产等措施，有效缩小企业的外部攻击面，降低资产暴露风险，保障企业网络安全的第一道防线。

零信任架构：零信任架构摒弃了传统的基于网络边界信任的观念，而是对任何试图访问企业资源的主体（用户、设备等）都进行严格的身份验证和授权，无论其是来自内部网络还是外部网络。通过多因素认证、最小权限原则等机制，即使企业的部分资产意外暴露在外部环境中，攻击者也很难在没有经过严格验证的情况下获取访问权限，进而保护了企业的核心资产和敏感数据，从根本上缓解了因资产暴露可能引发的安全问题。

• 多源情报融合的未来趋势

在未来的网络安全领域，多源情报融合将成为一种重要趋势。企业将整合来自内部安全系统（如入侵检测系统、漏洞扫描工具等）、外部威胁情报平台、行业共享情报以及政府部门发布的安全预警等多方面的情报信息，通过大数据分析、关联分析等技术手段，构建更为全面、准确的安全态势感知体系。例如，当企业内部发现某个异常 IP频繁尝试访问敏感资产时，结合外部威胁情报中该 IP 已被标记为恶意攻击者的信息，能够更快速、精准地判断出这是一次真实的攻击行为，并及时采取针对性的防御措施，提升应对网络威胁的整体效能。

• 资产和漏洞管理中台，打通外部和内部资产

资产和漏洞管理中台能够将企业内部不同部门、不同业务系统中的资产信息以及对应的漏洞情况进行统一整合管理，打破信息孤岛。同时，它还可以与外部的资产监测平台、安全情报源进行对接，实现内外资产信息的互联互通。例如，企业的分支机构在不同地区使用的各类网络设备、服务器等资产信息以及检测到的漏洞情况，都可以汇总到中台，中台再结合外部获取的关于这些资产在互联网上暴露的风险情报，进行综合分析，为企业提供一站式的资产和漏洞管理解决方案，帮助企业更高效地进行安全决策和风险处置。

• 自动化攻击和防护

自动化攻击方面：网络攻击者正在越来越多地利用自动化工具和脚本，发起大规模、快速的攻击行动，如自动化的暴力破解工具可以在短时间内尝试大量的用户名和密码组合，对企业的网络账户进行破解攻击；自动化的漏洞利用工具能够针对已知的系统漏洞，快速发起攻击，提高攻击的成功率和效率。这对企业的安全防护提出了更高的要求。

自动化防护：相应地，企业也在不断发展自动化防护技术，如自动化的防火墙策略配置、入侵检测与响应系统等。当检测到异常网络行为时，自动化防护系统能够立即按照预设的规则进行阻断、隔离等操作，无需人工干预，大大缩短了响应时间，提高了防护的及时性和有效性，在面对自动化攻击时能够更好地保障企业网络资产的安全。

通过上述改进建议与防护措施在不同层面的落实与推进，有望全方位提升对资产暴露风险的应对能力，保障网络空间资产的安全，推动数字经济健康、稳定地发展。

• 数据可视化技术

网络空间测绘数据可视化技术在过去几年取得了显著进展。早期，该技术主要依赖简单的图表和地图来展示基础网络信息，如 IP 地址分布、域名解析关系等。随着大数据、人工智能等技术的融合发展，其能力得到极大提升。如今，先进的算法能对海量且复杂的网络空间数据进行深度挖掘和分析，以 3D 网络空间地图与动态态势感知，更直观、多维的方式呈现网络资产全貌、流量动态以及潜在威胁分布。

在应用场景方面，网络空间测绘数据可视化技术已广泛融入多个领域。在网络安全领域，它帮助安全团队快速定位网络漏洞、监测异常流量，及时发现并应对各类网络攻击，提升网络安全防护能力。在智慧城市建设中，通过可视化呈现城市网络基础设施的运行状态，助力城市管理者优化资源配置，保障城市数字化服务的稳定运行。

展望未来，该技术将朝着更智能化、精细化方向发展。一方面，人工智能和机器学习技术将进一步赋能数据可视化，实现对网络空间态势的实时智能分析与预测，提前预警潜在的网络安全风险。另一方面，随着虚拟现实（VR）和增强现实（AR）技术的成熟，网络空间测绘数据有望以沉浸式的方式呈现，为用户提供更直观、更具交互性的体验，推动网络空间测绘数据可视化技术在更多领域实现创新性应用。

8. 政策与标准化建设

8.1. 政策建议与对策

监管加强：全球范围内对网络资产安全的重视程度将不断提高，监管力度也会进一步加强。各国政府将出台更加严格的法律法规，要求企业和组织加强对网络资产的保护，提高安全防护能力。例如，欧盟的《通用数据保护条例》（GDPR）已经对企业的数据保护和隐私政策产生了深远影响，未来类似的法规可能会在更多国家和地区实施，并且处罚力度可能会进一步加大。

数据保护与隐私法规完善：随着数据成为重要的生产要素，数据的保护和隐私问题将成为政策法规关注的重点。各国将制定更加细致和严格的数据保护法规，明确企业在数据收集、存储、使用、共享等环节的责任和义务，加强对用户个人信息的保护。同时，对于跨境数据流动的监管也将更加严格，以防止数据泄露和滥用。

行业特定法规出台：针对关键基础设施、金融、医疗等重要行业，可能会出台专门的网络资产安全法规和标准，要求这些行业的企业采取更加严格的安全措施，保障关键信息系统和数据的安全。例如，金融行业可能会加强对网上银行、移动支付等业务的安全监管，要求金融机构采用先进的加密技术、身份认证技术等，确保客户资金和信息的安全。

国际合作与协调：网络资产安全是全球性问题，需要各国之间加强合作与协调。未来，国际组织和各国政府之间将加强在网络安全领域的交流与合作，共同制定全球性的网络安全战略和法规框架，推动网络资产安全标准的国际化和统一化，加强对跨国网络犯罪的打击力度。

8.2. 网络空间测绘数据交换格式与标准定制

全国网络安全标准化技术委员会批准了由远江盛邦（北京）网络安全科技股份有限公司牵头，联合中国网络安全审查认证和市场监管大数据中心、公安部第一研究所、清华大学等 50 余家应用单位申请的国家标准《网络安全技术 网络空间测绘数据交换格式》立项。我司将在制定国家标准过程中，广泛征求国内行业及专家意见，汇聚行业智慧，形成高质量的标准成果。

附件

44项网络安全国家标准项目立项清单

序号	项目名称	工作组	类型	承担单位
25	网络安全技术 分布式控制系统（DCS）安全技术要求	WG 5	制定	北京赛西科技发展有限责任公司、国家工业信息安全发展研究中心、宁波和利时信息安全研究院有限公司等
26	网络安全技术 网络空间可视化表达方法	WG 5	制定	中国科学院地理科学与资源研究所、公安部第一研究所、中国科学院软件研究所等
27	网络安全技术 网络空间测绘数据交换格式	WG 5	制定	远江盛邦（北京）网络安全科技股份有限公司、中国网络安全审查认证和市场监管大数据中心、公安部第一研究所等
28	网络安全技术 工业控制系统网络安全防护能力成熟度模型	WG 5	修订	中国电子技术标准化研究院、国家信息技术安全研究中心、公安部第三研究所等

由于资产测绘工作缺乏统一的数据标准格式，不同机构和企业在进行网络空间测绘时所采用的数据格式各异，导致数据的共享、整合和分析困难重重，严重制约了网络空间测绘技术在经济、社会各领域的广泛应用和产业的健康发展，制定网络空间测绘数据标准格式迫在眉睫。

该国家标准拟从可观测性视角，完成对资产测绘时的资产分类、数据交换格式，以统一来自不同资产测绘源的测绘数据。解决不同测绘源数据格式不统一问题，并为资产测绘数据共享、挂图作战、网络空间安全图谱构建等提供基础数据保障。有助于规范网络空间测绘行为，提高数据质量和安全性，为网络空间的有序发展提供有力支撑。

9. 跨学科研究深化

9.1. 网络空间地理学

• 网络资源分布、网络空间测绘与地缘政治的关联

网络空间测绘是获取网络空间各类信息的重要手段，它为研究网络空间地理学提供了数据支撑，让我们能更清晰地洞察网络资源分布与地缘政治的紧密联系。

网络资源分布与测绘：借助网络空间测绘技术，我们能够精准定位网络基础设施，如服务器、网络节点、域名系统（DNS）等在全球的分布情况。像美国拥有众多世界知名的互联网企业和数据中心，在全球网络资源中占据主导地位。通过测绘可以发现，美国的网络服务器数量多、性能强，分布广泛且集中在一些科技产业发达的地区。而发展中国家的网络资源相对匮乏，网络基础设施建设存在一定差距，部分地区甚至存在网络覆盖不足的问题。这些测绘数据直观地展现了全球网络资源分布的不均衡性。

地缘政治与网络空间测绘：地缘政治因素深刻影响着网络空间测绘的开展和应用。从国家层面来看，各国都非常重视本国网络空间的安全和主权，会通过制定相关政策和法规，限制外国机构对本国网络空间进行测绘。例如，一些国家要求外国企业在进行网络相关业务时，必须遵守本国的网络安全规定，防止关键网络信息被非法获取。同时，地缘政治博弈也促使各国积极开展自身的网络空间测绘工作，以便更好地了解本国网络安全态势，应对潜在的网络威胁。在国际竞争中，网络空间测绘成为各国维护自身地缘政治利益的重要手段之一。

9.2. 网络法学

• 网络空间测绘视角下跨国测绘行为的法律定性

在网络空间测绘日益发展的背景下，跨国测绘行为的法律定性变得愈发复杂，需要从多个角度进行深入分析。

跨国测绘行为的界定与法律依据：从网络空间测绘角度出发，跨国测绘行为不仅包括传统的地理空间测绘，还涉及网络空间测绘数据的跨境获取、传输和使用。以相关法律法规为依据，外国组织或个人在中国从事测绘活动，必须依法获得批准，并遵循相应的程序和规定。在网络空间中，获取他国网络空间测绘数据，同样可能构成违法行为。例如，通过网络技术手段非法入侵他国网络服务器，获取其中存储的网络拓扑结构测绘相关信息，就违反了相关法律规定。

法律定性的考量因素：在对跨国测绘行为进行法律定性时，需要综合考虑多方面因素。首先，要判断测绘行为的主体是否具备合法资质，是否按照规定的程序获得许可。其次，要考量测绘行为的目的和动机，是否存在恶意获取敏感信息、危害他国安全的意图。再者，对于测绘数据的处理和使用方式也是关键因素，包括数据的存储、传输、共享等环节是否符合法律要求。此外，在国际层面，还需要考虑不同国家法律之间的冲突和协调问题，通过国际合作和多边协议，共同规范跨国测绘行为。

从网络空间测绘角度来看，网络空间地理学和网络法学紧密相连。网络空间测绘为网络空间地理学研究网络资源分布与地缘政治关联提供了有力工具，让我们更深入地认识到全球网络空间格局背后的地缘政治因素。而网络法学则在规范网络空间测绘行为，特别是跨国测绘行为方面发挥着重要作用，通过明确法律责任和定性标准，保障各国在网络空间的主权和安全。随着网络技术的不断发展，未来需要进一步加强网络空间测绘技术的研究和应用，完善相关法律法规，加强国际合作，共同应对网络空间带来的各种挑战，维护全球网络空间的和平与稳定。

10. 学术科研

图 10-1 DayDayMap 全球网络空间资产测绘平台 学术科研页

DayDayMap 学术科研致力于打造网络空间测绘学术社区，如聚集了网络空间测绘相关的最新研究成果。当前已经收录网络空间资产测绘方向的研究内容数百篇，文章详细内容，可登录 DayDayMap 全球网络空间资产测绘平台 www.daydaymap.com 研究页面查看阅读。

10.1. IPv6 测绘研究

IPv6 测绘技术涉及对 IPv6 地址空间的分布情况、网络拓扑结构、流量分析等方面的研究内容。常用的方法包括基于网络探测的活跃测绘技术、基于路由信息的 passively 测绘技术、基于流量数据的 passively 测绘技术等。

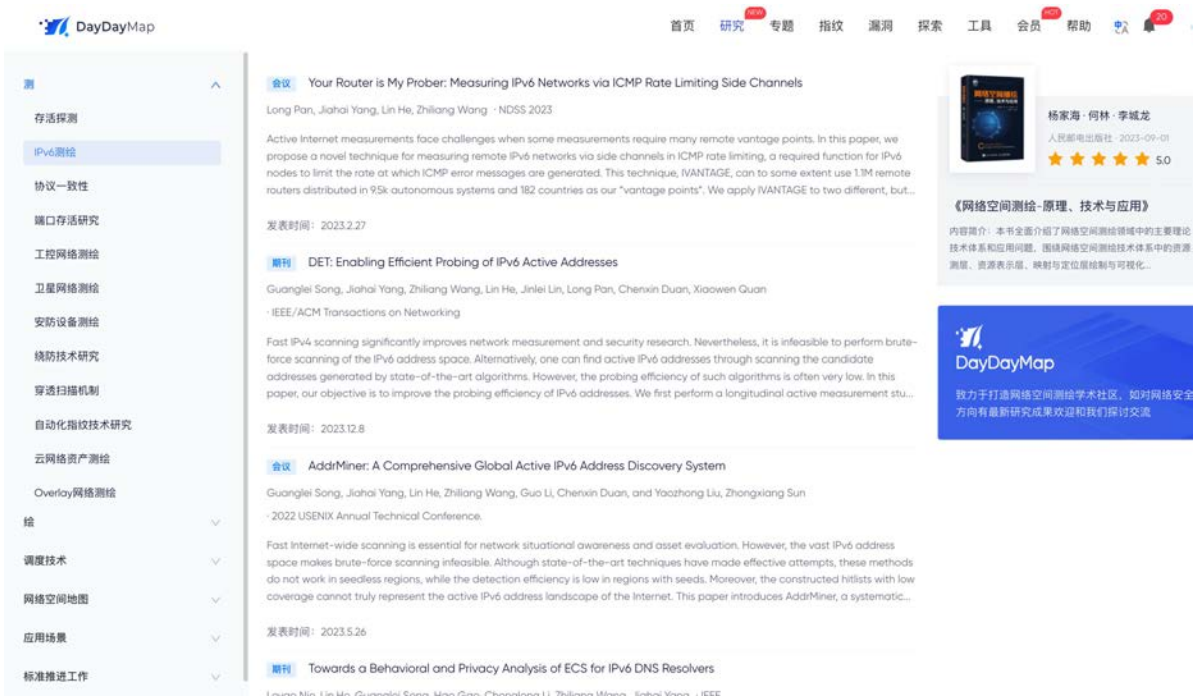


图 10-1-1 DayDayMap 全球网络空间资产测绘平台 学术科研 IPv6 测绘论文期刊图

文章详细内容，可登录 DayDayMap 全球网络空间资产测绘平台 www.daydaymap.com 研究- IPv6 测绘页面查看阅读。

10.2. 绕防技术研究

安全设备的拦截可能会导致在测绘过程中未能获得完整的网络数据。绕防技术研究致力于克服安全设备和防护措施对测绘过程的干扰，通过找到一些方法来规避安全设备的拦截规则，以便更深入地进行网络空间测绘。

10.3. 自动化指纹技术研究

自动化指纹技术是指利用自动化技术和工具来识别和收集网络设备、服务和应用程序的指纹信息的研究。自动化指纹技术能够快速、准确地识别和收集网络设备和应用程序的指纹信息，帮助建立完整的网络资产清单和拓扑图。

10.4. 社会组织识别研究

社会组织识别是指在网络空间资产测绘中，通过对测绘数据进行分析，识别资产所属的组织机构，从而推断出这些资产所属的具体组织或部门，帮助组织了解其网络拓扑结构、资产分布情况以及可能存在的安全风险。

10.5. 资产权值分析技术研究

资产权值分析技术用于评估网络中不同资产的价值和重要性。通过这项技术，研究人员可以对网络中的各种资产进行定量分析，为其赋予权值和评分，以便更好地了解网络资产的分布情况、优化资源配置、评估风险和制定安全策略值分析技术。

10.6. 反溯源技术研究

反溯源技术主要是指在网络空间资产测绘中，通过使用匿名化技术、加密通信、混淆数据等手段，防止测绘节点被溯源的技术。该技术旨在保护测绘节点的隐私和安全，防止恶意用户或攻击者通过技术手段追踪和识别测绘节点的位置和身份。

10.7. 攻击面管理研究

攻击面管理是指对系统、网络或应用程序中的潜在攻击面进行分析、识别和管理的过程。这种管理旨在识别可能被攻击者利用的漏洞、弱点或暴露的安全隐患，以便采取相应的安全措施来减少系统受攻击的可能性。

10.8. 资产安全治理研究

资产安全治理是指对网络空间资产进行资产摸底、备案审核、立体化防御、自动化运营和紧急响应的资产全生命周期治理过程。通过对网络空间进行测绘，特别是通过对网络拓扑图、网络流量分析等手段能够更清晰的确定网络中的各类资产，提供治理源数据。

10.9. 网络空间地图模型构建研究

网络空间地图模型构建是为了增强网络空间资源的的可见性和交互性，从传统的地理和社会的二元空间扩展到地理、社会、网络信息的三元空间，通过三元空间之间的实体关系、网络结构、资源分布进行网络空间地图模型的构建，有助于促进人们对网络空间的统一认识。

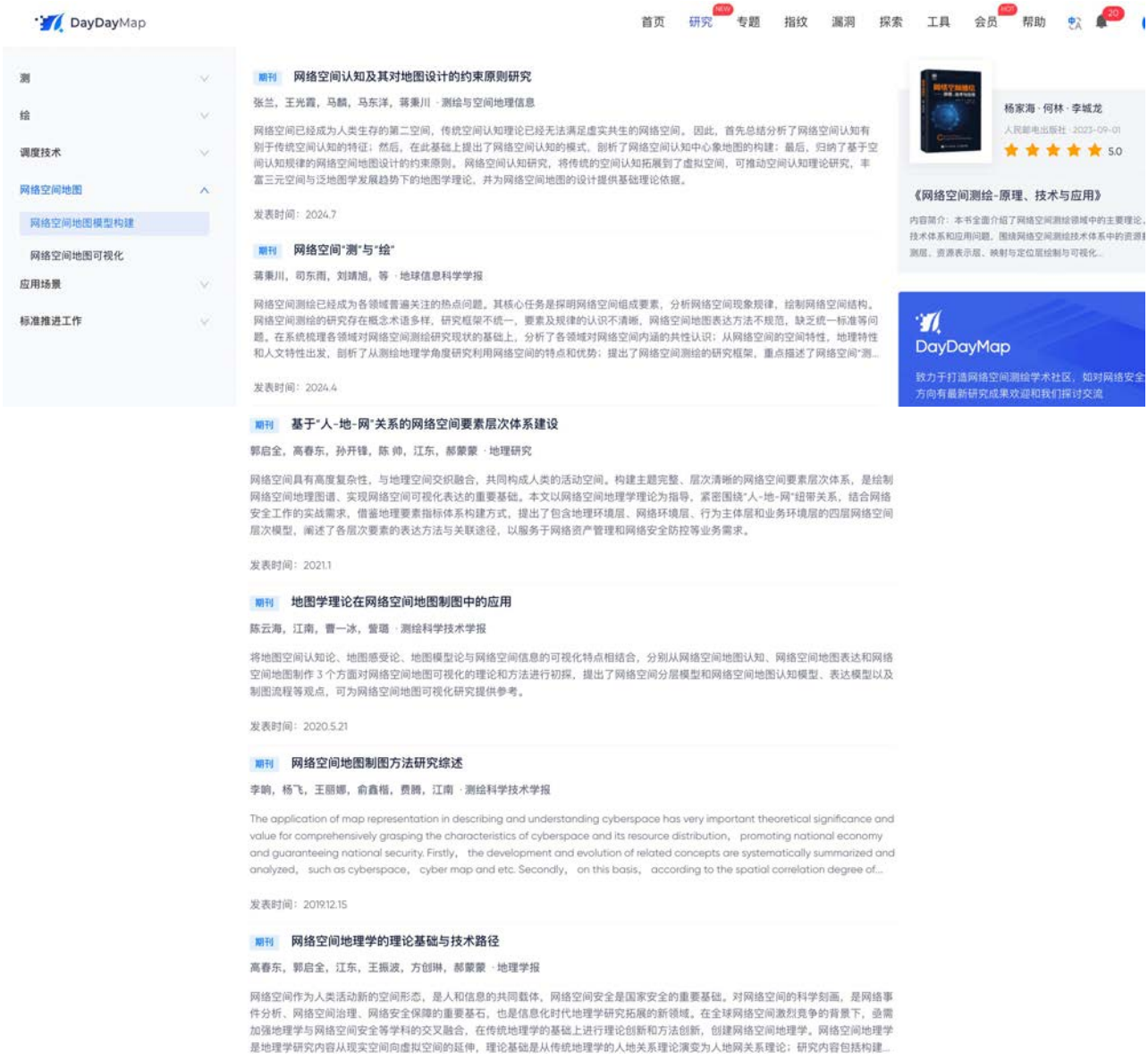


图 10-9-1 DayDayMap 全球网络空间资产测绘平台 学术科研网络空间地图模型构建论文期刊图

•《网络空间认知及其对地图设计的约束原则研究》张兰，王光霞，马麟，马东洋，蒋秉川 · 测绘与空间地理信息

•《网络空间“测”与“绘”》蒋秉川，司东雨，刘靖旭，等

· 地球信息科学学报

•《Virtual geo-cyber environments: metaphorical visualization of virtual cyberspace with geographical knowledge》Bingchuan Jiang, Xiong You, Ke Li, Tingting Li, Xiao Wang & Dongyu Si

· International Journal of Digital Earth

•《论网络空间的地理属性与地理学思维》江东，高春东，郭启全，陈帅，郝蒙蒙

· 地球信息科学

文章详细内容，可登录 DayDayMap 全球网络空间资产测绘平台 www.daydaymap.com 研究-网络空间地图模型构建页面查看阅读。

10.10. 网络空间地图可视化研究

网络空间地图是描述网络空间的重要工具之一，它直观地反映了网络空间的资源分布、网络结构。从传统的地理地图到主题地图，再从主题地图到网络结构图，最后从网络结构图到抽象的隐喻地图，都以图形化的方式呈现复杂的网络空间数据和关系，能够帮助用户快读获取和理解信息的关键点。

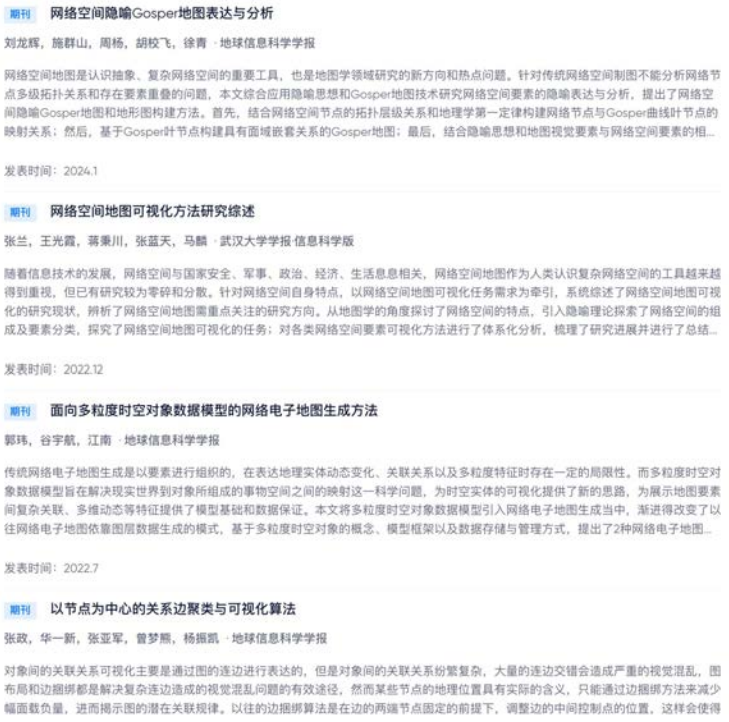


图 10-10-1 DayDayMap 全球网络空间资产测绘平台 学术科研网络空间地图可视化论文期刊图

文章详细内容，可登录 DayDayMap 全球网络空间资产测绘平台 www.daydaymap.com 研究-网络空间地图可视化页面查看阅读。

Part II

网络空间资产反测绘

1. 网络空间资产反测绘背景

1.1. 反测绘的重要性和必要性

网络空间安全呈现出攻防双方持续对抗、激烈博弈的态势。在这场较量中，防御方凭借网络空间测绘技术，对网络空间里的各类资产及其相关信息展开主动或被动的探测、采集与深入分析，从而达成对网络空间资产的实时监测与精准剖析，构建起全面的网络空间态势感知体系。这一技术助力防御方精准识别网络威胁、及时检测网络攻击，并迅速采取针对性的安全防护举措，显著提升网络安全防御能力与应急响应效率，有力保障自身联网资产的安全。

反观攻击者，他们极有可能借助网络空间测绘领域的先进技术，针对攻击目标展开细致侦查与深度分析，借此获取目标的开放端口、子域名、系统信息等关键数据。同时，攻击者还能依托现有的网络空间搜索引擎，快速勾勒出全网攻击面，高效发现并收集攻击资源，进而肆意扩大攻击范围。

值得注意的是，金融、能源、通信、交通等领域的关键信息基础设施，作为经济社会运行的核心神经中枢，无疑是网络安全防护的重中之重。据 DayDayMap 数据显示，2024 年暴露面资产（涵盖 IPv4 与 IPv6）新增总数高达 47 亿，其中脆弱性目标占比 3.5%，可渗透利用目标占比约 0.027%，且这两个比例均呈上升态势。如此大规模的暴露面激增，对我国互联网生态以及关键信息基础设施建设产生的影响极为严重，危害不容小觑。

学术界提出了“网络空间反测绘”的概念，利用反测绘技术，能够有效防范攻击性的测绘行为，增加攻击成本，拖延攻击方的行动，为防御方争取更多防御时间，增强防御方的主动性。一些国家和重要单位已经开始采取各种反测绘技术手段，防止测绘方通过测绘技术获取到真实、有效的信息，进而不能得到全面准确的网络空间地图，实现保护、隐藏己方网络和网络资产的目标。

1.2. 反测绘技术的挑战

在网络空间的安全对抗领域内，反测绘技术占据了与网络测绘技术相抗衡的战略高地。其核心职责聚焦于精确识别并揭露所有网络测绘行动，随后，通过精心策划并执行一系列周密的策略措施，对这些测绘行为进行阻断或误导，致使测绘作业难以有效推进，进而导致测绘分析所得出的结论与网络环境的真实状况产生显著偏差。

反测绘技术与测绘技术的发展历程，实质上是一个在持续博弈中不断更新与演进的复杂过程。当前，尽管反测绘技术已取得一定进展，但仍面临着诸多挑战与未解难题。

• 测绘技术不断演进

在网络空间安全领域，测绘技术始终处于动态发展的进程中，持续迭代演进。新的测绘工具和方法层出不穷，像分布式测绘技术，借助多个节点并行作业，极大地提升了测绘效率与范围；智能测绘算法则凭借强大的数据分析与处理能力，能够更精准地挖掘网络空间中的关键信息。作为测绘技术的博弈方，反测绘技术必须保持高度的敏锐性，紧跟其步伐，不断实现自身的更新与升级。

• 加密与隐蔽技术难题

攻击者为了避免测绘行为被发现，越来越多地采用加密技术和隐蔽通信手段来隐藏测绘数据和通信过程。反测绘技术需要具备强大的解密和识别能力，能够从海量加密数据中分析出潜在的测绘行为，这对反测绘技术的检测能力提出了极高的要求。

•网络环境复杂多变

网络空间规模宏大，结构错综复杂，各类网络设备日新月异，网络协议持续迭代，网络应用层出不穷。不同的网络环境，无论是企业内部网络、广域互联网，还是新兴的物联网环境，都各自具备独特的特征与差异化的安全机制。以云计算环境为例，其资源的动态分配特性，使得服务器、存储等资源随业务负载灵活调配；多租户特性又让不同用户共享同一物理基础设施，这共同导致网络拓扑时刻处于变化之中，资产信息也随之频繁更迭。在此背景下，反测绘技术面临着极高的要求。它必须具备强大的适应性，能够无缝融入多样化的网络环境，精准识别并妥善应对各类潜在的测绘行为，从而在复杂多变的网络空间中筑牢安全防线。

1.3. 网络空间测绘源区域分布

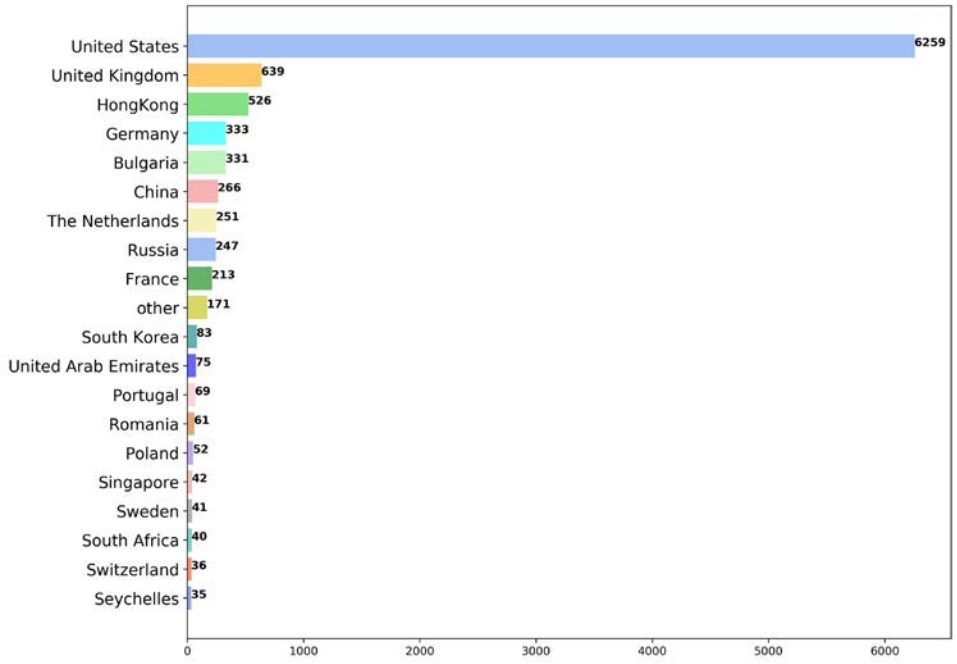
以下分析结果基于 2024 年 Q4 在全球多个主要城市的24个IP流量数据，并由反测绘探测识别引擎进行识别。

全球测绘：

主要来源北美州、欧洲、亚洲等；

图 1-3-1 2024 年 Q4 全球主流网络空间测绘平台测绘源统计

国家 TOP 20：



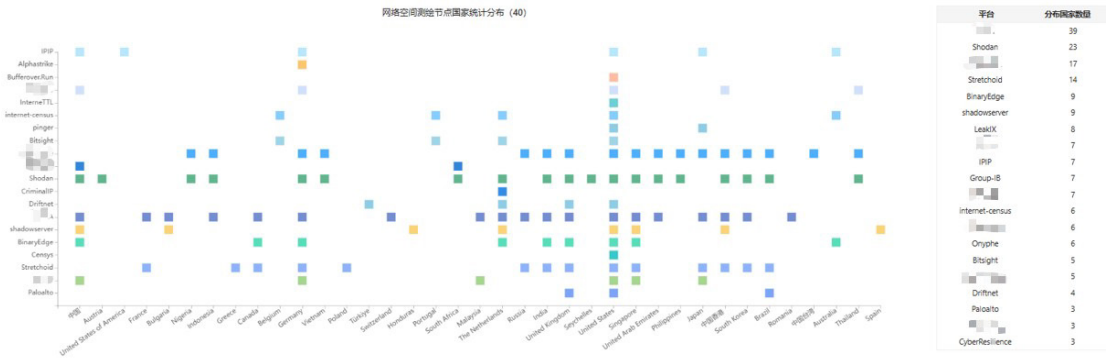


图 1-3-2 全球的网络空间测绘部署探测和扫描节点

- 全球测绘源平台在 52+ 个国家存在部署探测和扫描节点
- 全球测绘源平台当前部署最多的已有 39 个国家
- 共 46+ 个探测和扫描平台持续不断地对互联网进行扫描和探测

2. 目标测绘的方法方式研究

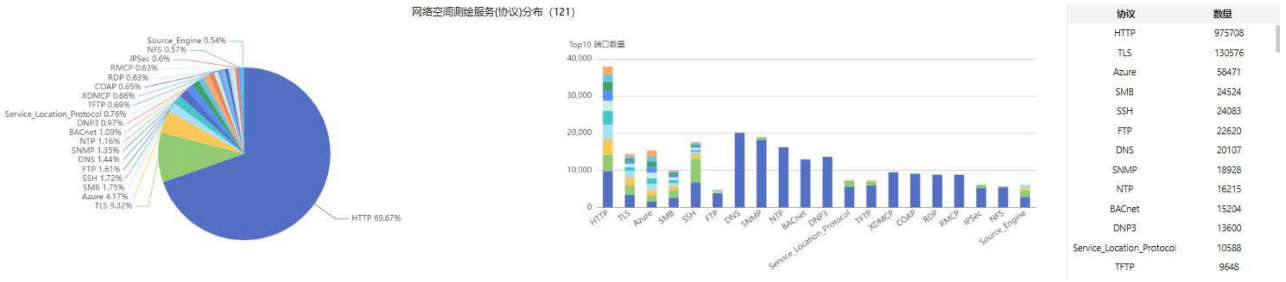


图 2-1 全球的网络空间测绘服务和协议分布

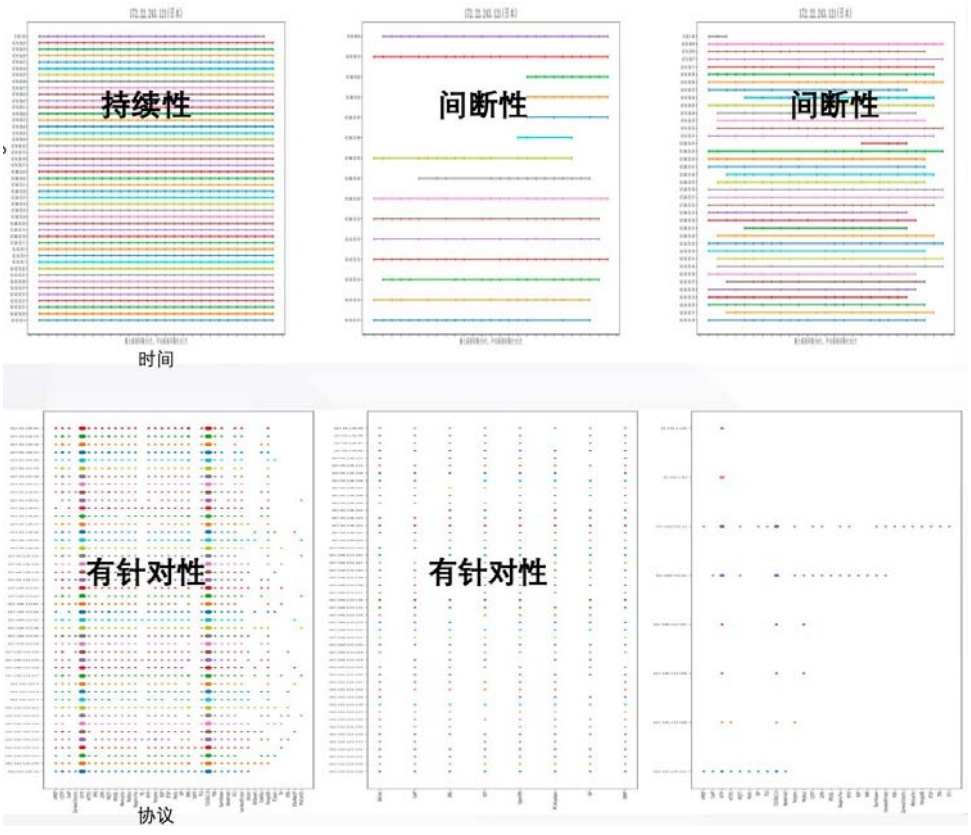


图 2-2 全球的网络空间测绘源主流平台测绘方式方法

以 Censys 为例，不同的IP职能不同，网络化探测和扫描的方式也不同。具体表现为：探测扫描更具有针对性；更多样化和离散化；方式方法更趋于精细化。

探测扫描更具有针对性：

- 将目标划分为不同集合，有针对性扫描；
- 时间上趋于持续性、间断性和偶发性。

更多样化和更离散化：

- 具有不同的探测扫描策略，更多样化；
- 短时间内针对同网段或同网络目标更离散化

方式方法更趋于精细化：

- 探测内容去特征化；
- 探测方法更精细。

3. 主流平台的测绘行为

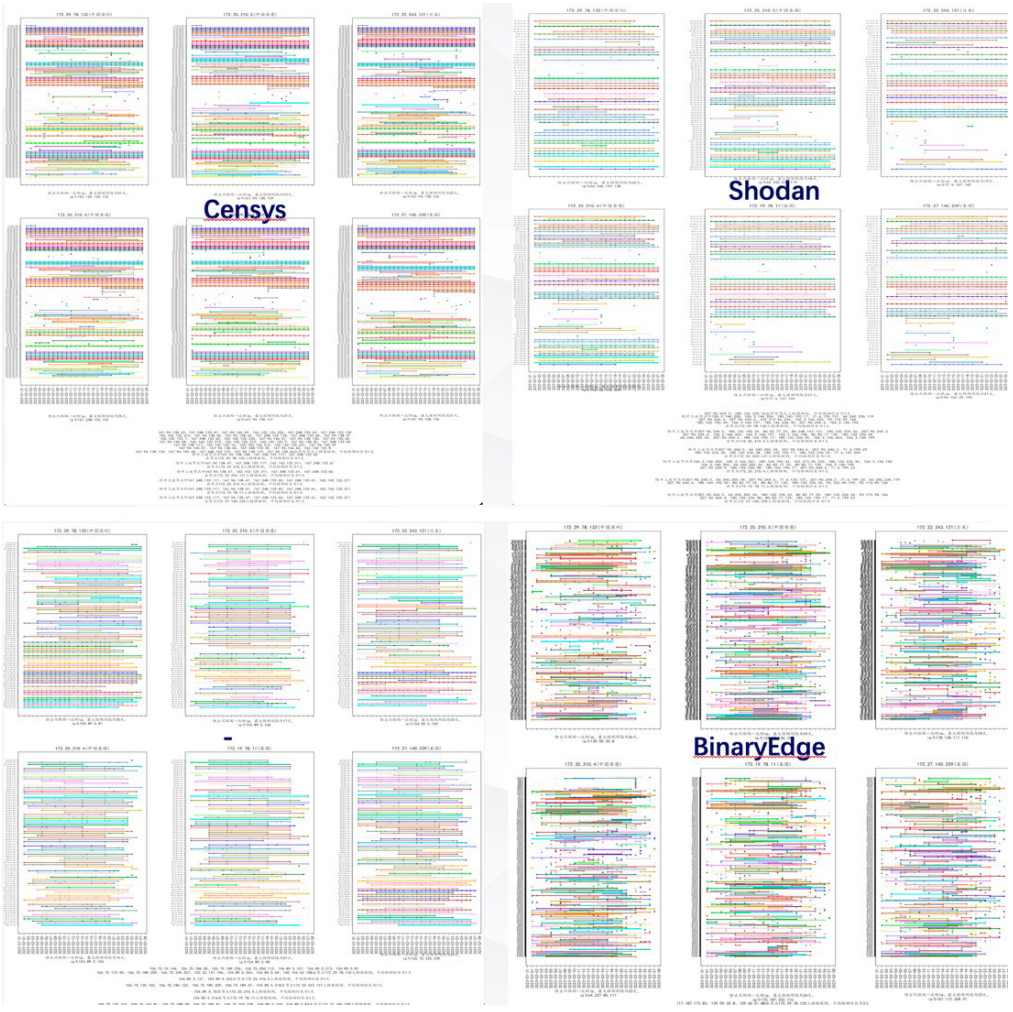


图 3-1 全球的网络空间测绘源主流平台测绘行为分析

Censys：通过全球分布的扫描节点对互联网上的 IP 地址进行主动扫描，扫描数覆盖 IPv4 和 IPv6 地址空间。其数据库信息涵盖开放的端口、服务、协议等。收集和分析 TLS/SSL 证书，识别证书的签发机构、有效期、域名等信息。扫描包括 HTTP、HTTPS、FTP、SSH 等。其扫描节点 IP 地址通常来自 AWS、Google Cloud、Azure 等云服务提供商，IP 段可公开查询。

Shodan:扫描覆盖全球范围内的服务器、摄像头、路由器等物联网设备。Shodan 抓取服务的 Banner 信息，包括服务类型、版本、配置等。能够识别设备的类型、操作系统、硬件信息等。能够精确定位设备的地理位置，精度可达城市级别。

Shodan 平台每天平均有 3 个探测节点对单个反测绘节点探测，平均对单个反测绘节点的探测次数为 1 次，最大探测次数为 7 次，最小探测次数为 1 次。

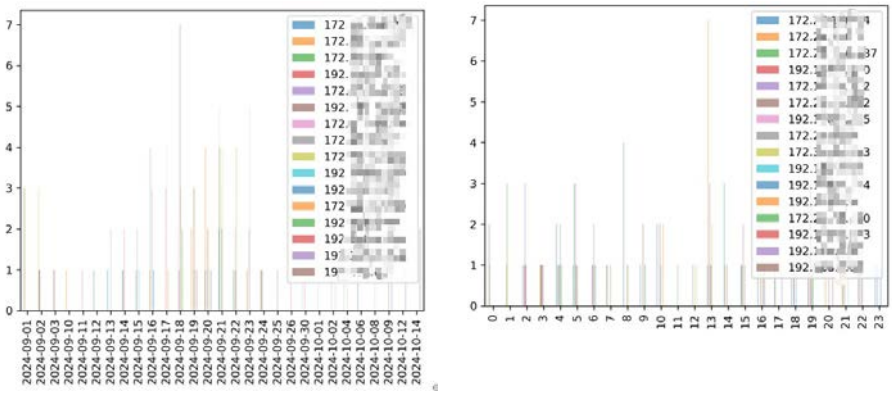


图 3-2 Shodan 反测绘行为分析

BinaryEdge:扫描覆盖 IPv4 和 IPv6 地址空间。对全网进行周期性扫描，包括 HTTP、HTTPS、FTP、SSH 等，并提供漏洞的详细信息，已监控涵盖电子邮件、密码、API 密钥等。扫描节点 IP 地址通常来自全球各地的数据中心，IP 段可公开查询。

BinaryEdge 平台每天平均有 3 个探测节点对单个反测绘节点探测，平均对单个反测绘节点的探测次数为 2 次，最大探测次数为 12 次，最小探测次数为 1 次。

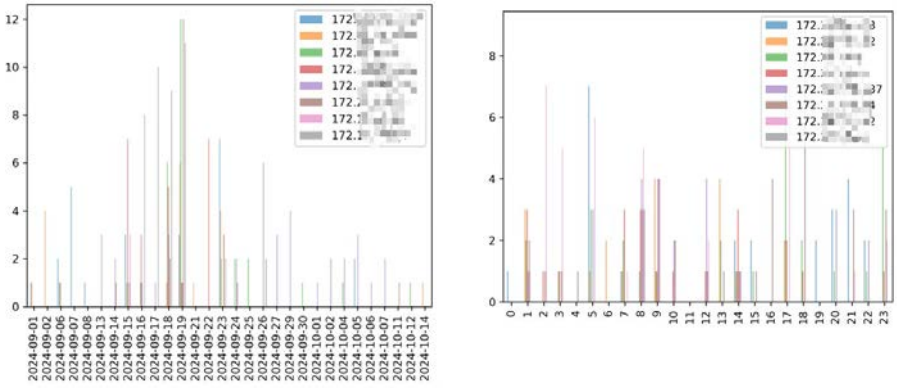


图 3-3 BinaryEdge 反测绘行为分析

4. 反测绘关键技术

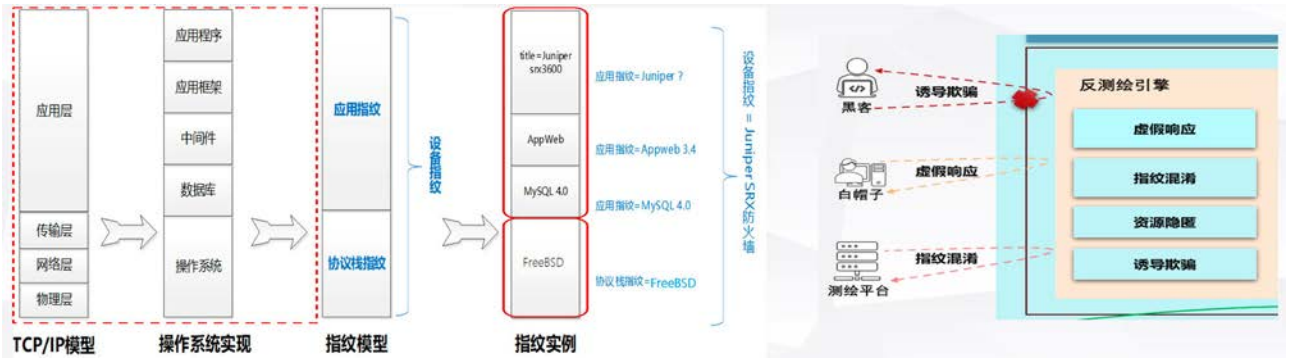


图 4-1 反测绘原理机制图

• 反测绘关键措施一：反探测

基于 IP 地理位置库、扫描器指纹库、探测指纹库、爬虫指纹库、流量行为分析（+自学习建模）技术，精准感知非法请求、敌对网络测量、测绘以及非法探测行为，阻断资源泄露风险，提升网络空间防控预警能力。

图 4-2 网络空间反测绘措施-反探测

• **反测绘关键措施二：虚假响应**

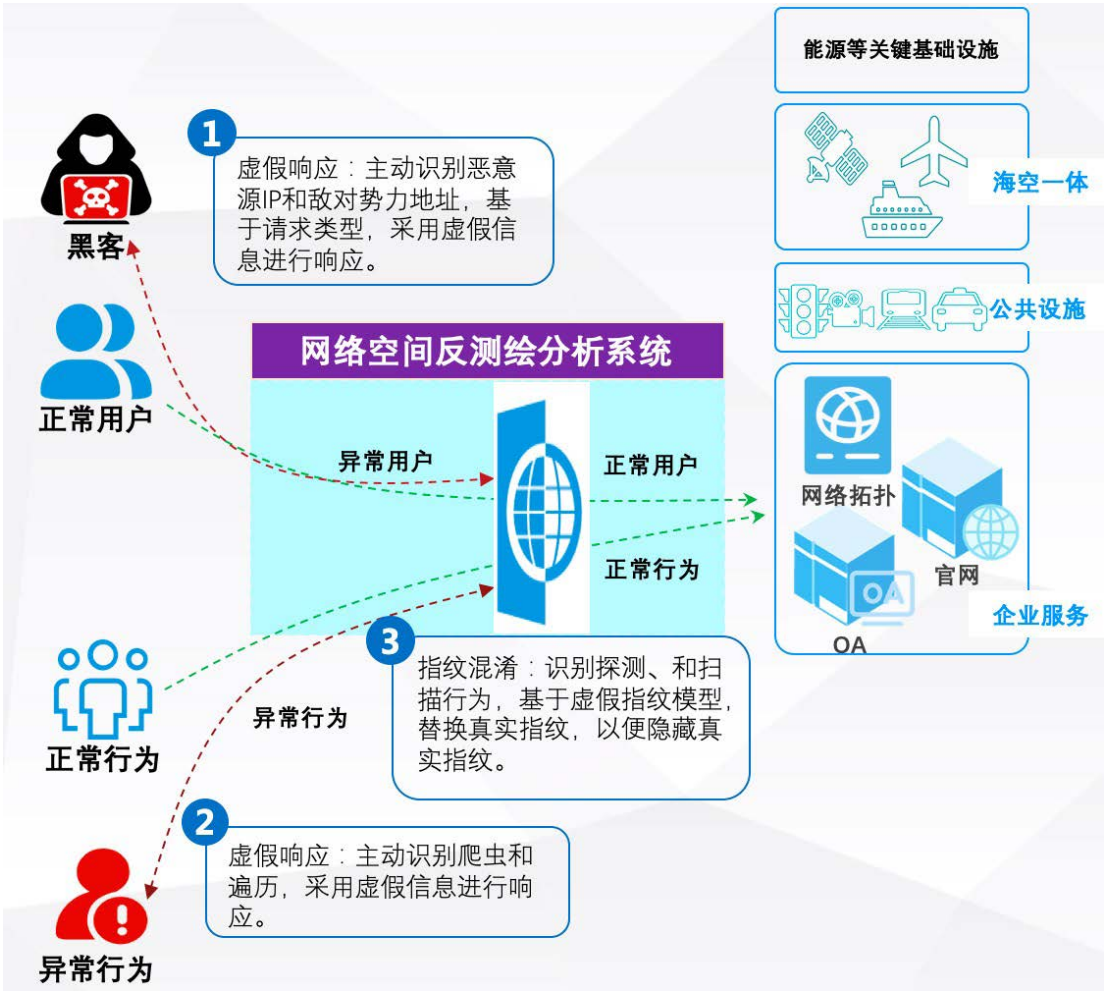


图 4-3 网络空间反测绘措施-虚假响应

• 虚假指纹模型：梳理设备、系统、服务及应用等指纹结构和关系，构建虚假的指纹层次结构和关联关系，以便识别到探测及扫描行为时，能够高效的替换和混淆指纹；

• 虚假响应模型：梳理不同协议的响应内容，保留静态资源，剥掉动态数据，当发现恶意IP和敌对势力地址、爬虫及遍历异常行为时，则会采用协议的静态资源+动态生成数据响应对方，或将代码植入响应中进行响应。

虚假响应：

• 主动识别恶意源IP和敌对势力地址，根据访问请求协议类型和内容，基于虚假响应模型进行响应。

• 主动识别爬虫和遍历异常动作行为，根据访问请求协议类型和内容，基于虚假响应模型进行响应。

指纹混淆：

主动识别网络探测、和扫描行为，基于虚假指纹模型，替换真实指纹，隐藏真实指纹，减小业务暴露风险。

• 反测绘关键措施三：诱骗扰乱

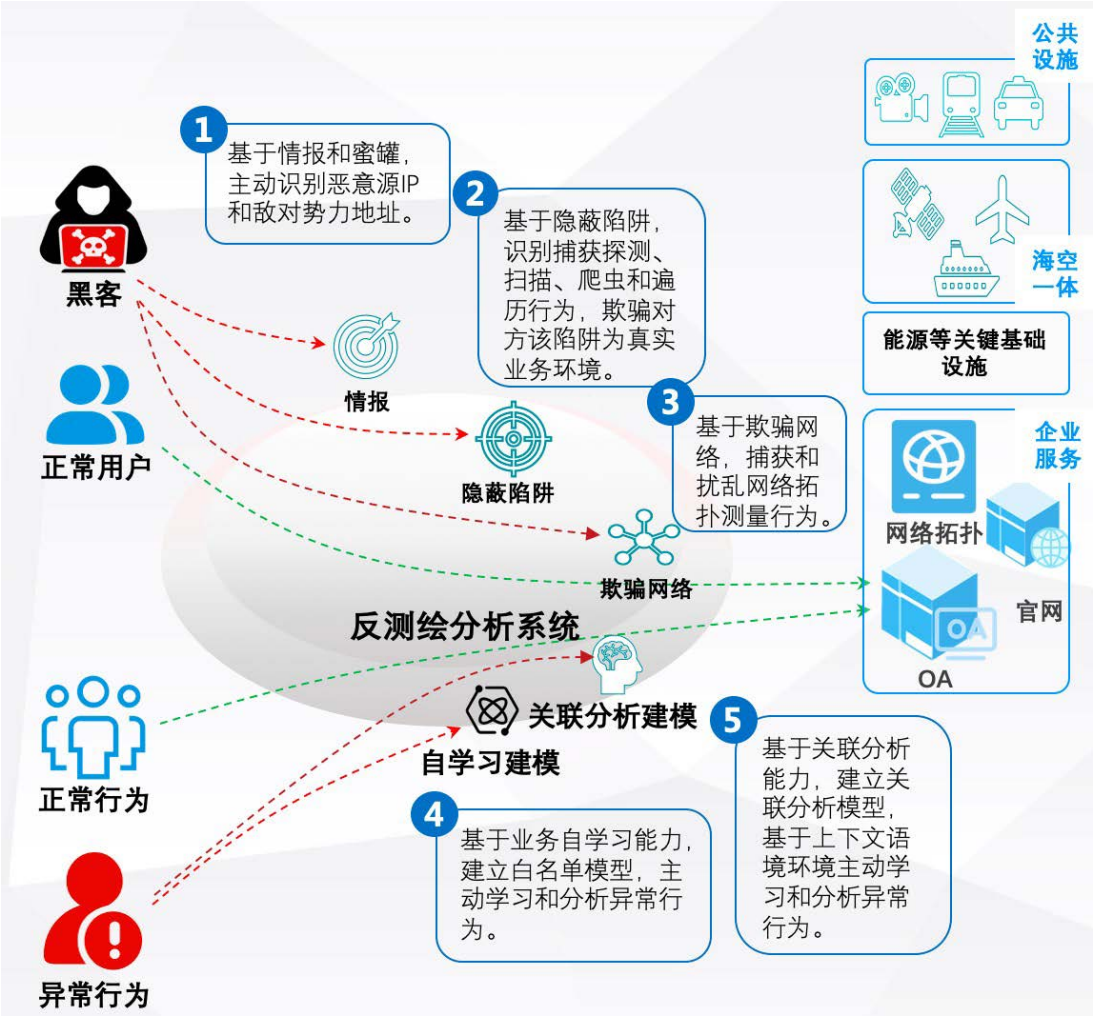


图 4-4 网络空间反测绘措施-诱骗扰乱

• 自学习模型：自动梳理业务结构，识别业务保护对象；基于学习结果建立白名单模型，建立非白即黑策略；

• 关联分析模型：基于关联分析能力，建立关联分析模型，基于上下文语境环境主动学习和分析异常行为。

采用虚假的设备、服务应用、资源数据及网络陷阱欺骗非法访问者；扰乱其探测和扫描等行为，使其得到错误的结果。

• 基于情报和蜜罐，主动识别恶意源IP和敌对势力地址，诱骗并诱使其访问隐蔽陷阱等进行联动防御。

• 基于隐蔽陷阱，识别和捕获探测、扫描、爬虫和遍历行为，欺骗异常访问者该隐蔽陷阱为真实业务环境。

• 基于欺骗网络，捕获和扰乱网络拓扑测量行为，提供虚假的拓扑响应。

• 反测绘关键措施四：对抗大数据

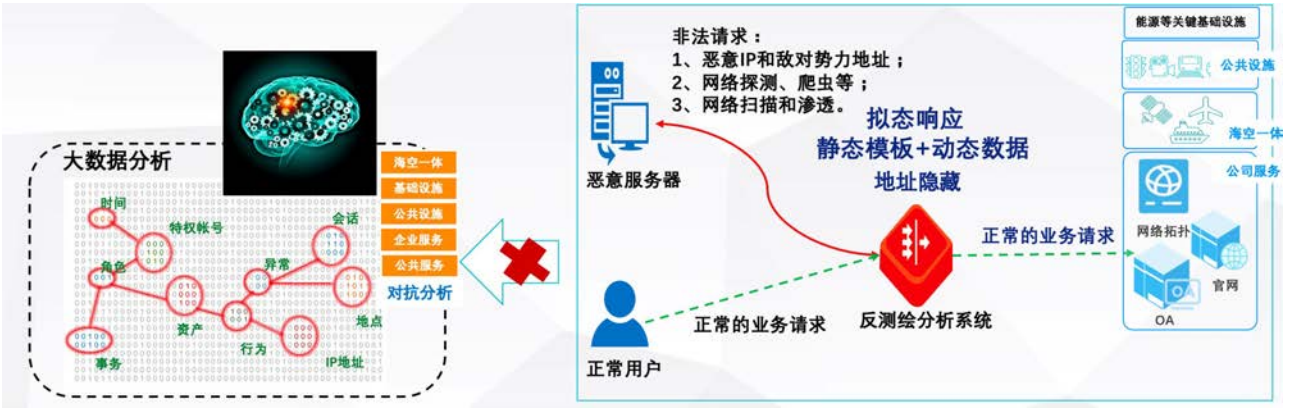


图 4-5 网络空间反测绘措施-对抗大数据

拟态响应：

• 根据用户业务，构造和模拟真实的用户响应；

• 去除单一化，应多样化交互；

• 避免被识别为虚假业务或蜜罐。

静态模板+动态数据：

• 构造静态响应模板，预留动态数据插入点；

• 根据动态数据插入点，适时构造动态响应数据，插入响应数据中，进行响应；

• 基于静态模板+动态数据，保持响应的动态性和数据的无关性。

地址隐藏：

• 构建地址隐藏服务，将真实的业务地址隐藏起来；

• 基于地址漂移能力，使大数据无法关联分析，减小真实业务的暴露信息。

5. 军事网络反测绘策略

军事网络空间反测绘策略是应对网络空间测绘技术带来的威胁、保护关键信息基础设施和军事网络资源的重要手段。以下是基于最新研究和实践总结的军事网络空间反测绘策略：

5.1. 核心理念

军事网络空间反测绘的核心是通过阻断测绘方的探测行为和扰乱其数据关联分析，基于大数据人工智能分析，使对方无法绘制出动态、实时、可靠的网络空间地图。其主要策略包括禁探测、指纹混淆、诱骗扰乱、伪装隐匿、网络隐遁等。

关键技术与策略：

(1) 禁探测

禁探测是网络空间反测绘的核心能力，通过IP地理位置库、扫描器指纹库、探测指纹库、爬虫指纹库以及流量行为分析和自学习建模技术，精准感知非法探测行为，阻断资源泄露风险。

(2) 指纹混淆

通过构建虚假的指纹层次结构和关联关系，在识别到探测行为时，替换和混淆真实指纹信息，使测绘方无法准确获取目标设备和服务的真实信息。

(3) 诱骗扰乱

采用虚假设备、服务、资源数据和网络陷阱，欺骗非法访问者，使其获取错误结果，扰乱其探测和扫描行为。

(4) 伪装隐匿

为关键设备和服务穿上“马甲”，隐藏其真实信息，减少关键资产在网络空间中的暴露点和暴露面。

(5) 对抗大数据

通过动态响应和数据无关性技术，使测绘方的大数据分析无法关联真实业务信息，减少关键信息的暴露。

5.2. 军事应用场景

(1)军事网络空间

在网络空间军事化背景下，反测绘技术用于保护军事网络基础设施、卫星测控系统、气象服务等关键节点，防止被敌方测绘和攻击。

(2)关键信息基础设施

针对能源、电力、交通、金融等关键信息基础设施，反测绘技术可以有效减少暴露面，隐藏关基核心网络资产，保护关键资源免受测绘和攻击。

5.3. 实践与案例

盛邦安全在网络空间反测绘领域进行了大量实践，其技术体系结合了反探测、欺骗响应、指纹混淆、诱骗扰乱等多项关键技术，通过异常行为分析和大数据分析模型，实现对关键资源的隐匿和保护。

随着网络空间测绘技术的不断精进，反测绘技术也需要持续演进。未来的研究方向包括：

- AI 驱动的反测绘技术：利用人工智能和机器学习技术提升反测绘的智能化水平。
- IPv6 网络空间反测绘：针对 IPv6 网络的特点，开发高效的探测和反探测技术。
- 多域视图融合：构建多域视图，提升反测绘的全面性和动态性。

通过以上策略和技术手段，军事网络空间反测绘能够降低关键信息资产的暴露风险，增强网络空间的防御能力，为军事网络安全提供重要保障。

6. 研究总结

6.1. 资产测绘与反测绘的技术演进

• 网络空间资产测绘技术演进

早期阶段：早期的网络空间资产测绘主要依赖于简单的端口扫描工具，如 Nmap 。这些工具通过向目标 IP 地址发送探测数据包，根据返回的响应来识别开放的端口和运行的服务，从而初步了解网络资产的基本信息。但这种方式只能获取有限的表面信息，对于复杂的网络架构和隐藏的资产难以全面探测。

发展阶段：随着技术的发展，出现了基于搜索引擎技术的资产测绘，如 Shodan 。它可以对网络上的设备进行大规模搜索，通过分析设备在网络上暴露的特征信息，如 HTTP 头信息、设备指纹等，来识别各种网络资产，包括服务器、摄像头、工业控制设备等。这大大拓展了资产测绘的范围和深度，但对于加密通信和动态变化的网络环境适应性不足。

当前阶段：如今，资产测绘技术融合了大数据分析、人工智能和机器学习等先进技术，如 DayDayMap 。利用大数据分析技术，可以对海量的网络数据进行整合和挖掘，发现潜在的资产关联和安全威胁；人工智能和机器学习算法则能够自动学习和识别网络资产的行为模式，实现更精准的资产识别和风险评估。

• 网络空间反测绘技术演进

被动防御阶段：早期的反测绘主要是通过关闭不必要的网络服务和端口，隐藏网络资产的基本信息，减少被探测到的可能性。同时，采用防火墙等安全设备对网络流量进行过滤，阻止未经授权的探测请求。但这种方式相对被动，难以应对复杂多变的测绘手段。

主动防御阶段：随着测绘技术的发展，反测绘技术也逐渐向主动防御转变。出现了蜜罐技术，通过部署虚假的网络资产和服务，吸引攻击者进行探测和攻击，从而收集攻击者的行为信息，及时发现测绘活动，并采取相应的防御措施。此外，还发展了网络欺骗技术，通过伪造网络拓扑结构和资产信息，误导攻击者的测绘方向，增加其测绘难度。

智能防御阶段：当前，反测绘技术开始融合人工智能和机器学习技术，实现智能防御。利用机器学习算法对大量的网络攻击数据进行分析和学习，建立测绘行为的识别模型，能够自动识别和检测各种新型的测绘手段。例如，通过分析网络流量的特征，判断是否存在基于人工智能的自动化测绘工具的活动，及时采取阻断措施。

6.2. 资产测绘与反测绘的应用价值

• 网络空间资产测绘的应用价值

网络安全防御：全面了解网络资产状况是构建有效网络安全防御体系的基础。通过资产测绘，能够发现网络中的薄弱环节和潜在的安全风险，如未打补丁的系统、配置错误的服务等，从而有针对性地采取安全措施，加强网络安全防护。例如，在发现某个服务器存在高危漏洞时，及时进行补丁更新，防止黑客利用漏洞进行攻击。

合规性检查：许多行业和领域都有严格的网络安全合规要求，如金融、医疗等。资产测绘可以帮助企业和组织快速准确地了解自身网络资产是否符合相关的合规标准，及时发现不符合要求的资产和配置，进行整改和优化，避免因合规问题带来的法律风险和经济损失。

业务优化：通过对网络资产的测绘和分析，企业可以更好地了解自身业务的运行情况，发现网络资源的瓶颈和浪费，优化网络架构和资源配置，提高业务运行效率。

• 网络空间反测绘的应用价值

保护网络资产安全：反测绘技术能够有效地防止攻击者获取网络资产的详细信息，减少被攻击的风险。通过隐藏真实的网络资产信息，误导攻击者的测绘方向，使攻击者难以找到有效的攻击入口，从而保护网络资产的安全。例如，利用网络欺骗技术，让攻击者误以为虚假的资产是真实的目标，消耗其攻击资源和时间。

维护网络安全态势：及时发现和阻止测绘活动，可以避免攻击者对网络进行全面的侦察和分析，维护网络的安全态势。通过监测和识别测绘行为，采取相应的防御措施，能够防止攻击者利用测绘结果进行后续的攻击，保障网络的正常运行。

保障国家关键信息基础设施安全：对于国家关键信息基础设施，如能源、交通、电信等、金融领域，反测绘技术尤为重要。它能够防止外部势力对关键信息基础设施进行测绘和侦察，保护国家的核心利益和安全。例如，在能源领域，防止黑客对电力系统的网络资产进行测绘，避免其获取关键信息后发动攻击，导致电力供应中断。

6.3. 当前挑战与未来机遇的辩证关系

• 当前挑战

技术复杂性：随着网络技术的不断发展，网络空间资产的种类和数量日益增多，网络架构也变得更加复杂。这使得资产测绘和反测绘技术面临巨大的挑战，需要不断更新和升级技术手段，以适应复杂多变的网络环境。例如，5G网络、物联网、工业互联网等新兴技术的应用，带来了大量新的网络资产和安全风险，传统的测绘和反测绘技术难以满足需求。

数据安全与隐私保护：在资产测绘和反测绘过程中，如何在保证技术有效应用的同时，确保数据的安全和隐私保护。

法律法规不完善：目前，网络空间资产测绘和反测绘相关的法律法规还不够完善，对于一些行为的界定和规范存在模糊地带。这导致在实际应用中，可能会出现法律风险和纠纷。例如，对于一些合法的网络安全监测和测绘行为，可能会被误解为非法的攻击行为，需要明确的法律法规来进行规范和保障。

• 未来机遇

技术创新推动：面对当前的挑战，也为技术创新提供了机遇。随着人工智能、区块链、量子计算等新兴技术的不断发展，为网络空间资产测绘和反测绘技术的创新提供了新的思路和方法。例如，利用区块链技术的去中心化和加密特性，可以提高数据的安全性和可信度，为资产测绘和反测绘提供更可靠的数据支持；量子计算技术的发展可能会对传统的加密算法产生冲击，也促使反测绘技术研发新的加密和防护手段。

市场需求增长：随着网络安全意识的不断提高，企业和组织对网络空间资产测绘和反测绘技术的需求也在不断增长。特别是在关键信息基础设施保护、金融安全等领域，对网络安全的要求越来越高，这为相关技术的发展提供了广阔的市场空间。例如，金融机构为了保障客户资金安全和业务稳定运行，需要高精度的资产测绘和有效的反测绘技术来防范网络攻击。

国际合作加强：网络空间安全是全球性问题，需要各国加强国际合作。在资产测绘和反测绘领域，国际合作可以促进技术交流和经验分享，共同应对跨国网络攻击和测绘活动。例如，各国可以共同建立网络安全信息共享平台，分享测绘和反测绘技术的研究成果和实践经验，共同制定相关的国际标准和规范，提高全球网络空间安全水平。

• 辩证关系总结

当前挑战与未来机遇是相互依存、相互转化的辩证关系。挑战为技术创新和市场需求提供了动力，促使企业和研究机构加大对网络空间资产测绘和反测绘技术的研发投入，推动技术的不断进步。而技术创新和市场需求的增长又为解决当前挑战提供了可能，通过新技术的应用和市场的规范发展，可以逐步克服技术复杂性、数据安全与隐私保护、法律法规不完善等问题。同时，国际合作的加强也有助于在全球范围内共同应对挑战，抓住机遇，实现网络空间资产测绘和反测绘技术的可持续发展，保障网络空间的安全和稳定。

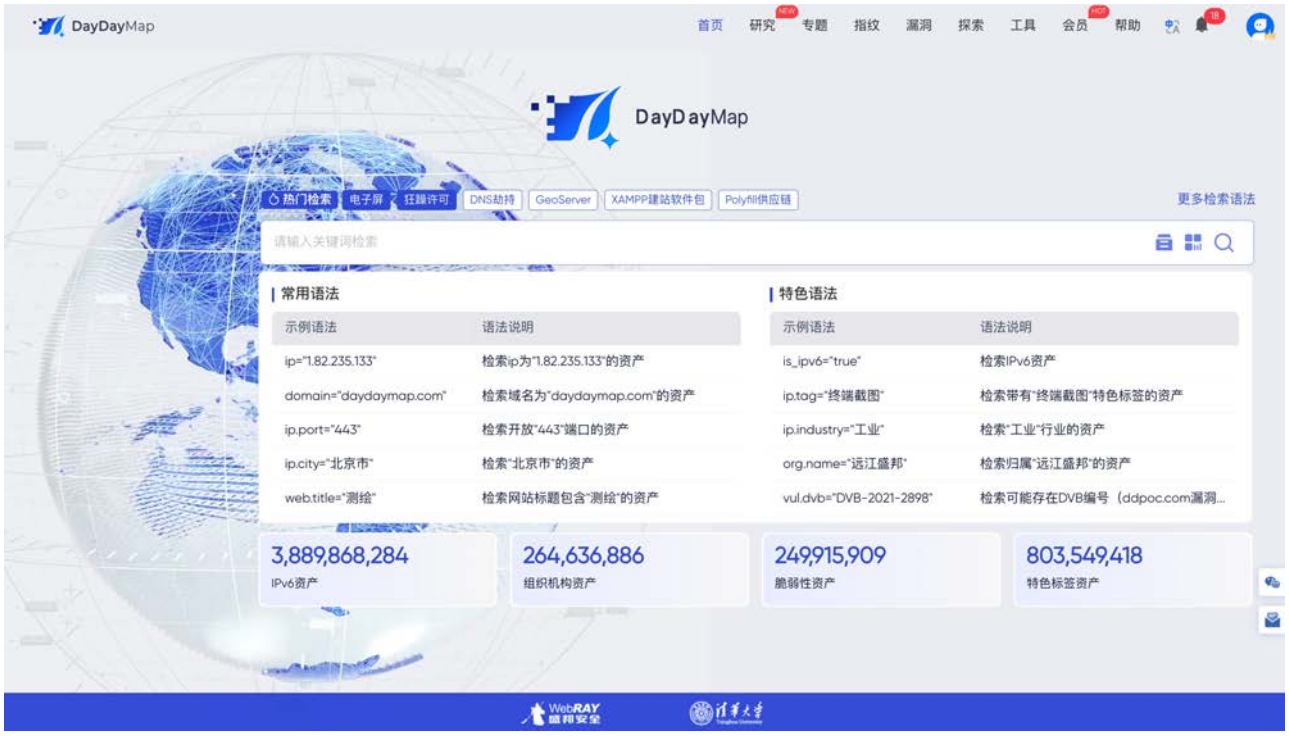
Part III

DayDayMap 介绍

1. DayDayMap 概述

DayDayMap 全球网络空间资产测绘平台：

https://www.daydaymap.com



盛邦安全推出的一款产学研一体的聚焦空间测绘科研领域的全球网络空间资产测绘平台 DayDayMap，致力于让网络空间资产可感知、易定位、更有价值。DayDayMap 自动扫描和智能识别用户在互联网上的多元资产，包括域名、IP 地址、端口、服务、组件等信息。通过构建详尽的资产和主机画像，能够揭示出互联网资产的暴露边界，并精准识别各类资产属性，实现互联网资产的可查、可定位。DayDayMap 具备领先 的IPv6 探测技术（IPv6 地址池资产数据 68 亿条）、强大的科研加持，迅捷的指纹检索能力，可定位资产社会属性、多维资产画像、漏洞详情以及友好的使用界面而获得业内认可。其在相似性检索、空间定位、资产拓线等方面，有计划加大重点投入。

2. DayDayMap 优势创新

网络空间的瞬息万变及浩渺庞杂对网空测绘提出了极大挑战。充分利用机器学习和其他人工智能技术实现网空测绘的智能化是未来发展大势，多层次网络发现、微分段、IPv6 、则是重要技术着力点。2024 年 5 月，盛邦安全针对 IPv6 的新一代网空测绘平台—— DayDayMap 全球网络空间资产测绘平台正式发布，受到业界广泛关注。

DayDayMap 可以对目标资产梳理，挂图作战，绘制网络空间资产底图，对抗先机，提升网络攻防实战能力，而 DayDayMap 全球网络空间资产测绘系统，处于 ATT&CK 攻击矩阵的第一个步骤“侦察”。是攻击前的情报侦察，为制定战术、战法、武器选配提供数据和脆弱性分析提供辅助支撑。一般用于目标网络打点攻击前情报获取，平台同时做无痕化处理和设计。DayDayMap 提供卫星互联网测绘服务，能够分析和测绘全球的卫星网络资产，如星链 starlink 等。

2.1. IPv6 测绘技术

为保证资产覆盖的全面性，DayDayMap 支持 IPv4 和 IPv6 类型资产的测绘能力，IPv6 地址池数量 68 亿，在线 IPv6 资产不少于 38 亿。同时通过无状态防溯源探测、高性能端口扫描等技术、大规模分布式扫描引擎资源，在业界处于领先地位。对于海量的 IPv6 数据，基于传统的扫描机制很难遍历全部存活数据，因此，而采用基于 IP 集的熵预测算法能够极大程度解决这个问题。IPv6 测绘技术涉及对 IPv6 地址空间的分布情况、网络拓扑结构、流量分析等方面的研究内容。常用的方法包括基于网络探测的活跃测绘技术、基于路由信息的 passively 测绘技术、基于流量数据的 passively 测绘技术等通过无状态防溯源探测、高性能端口扫描等技术、大规模分布式扫描引擎资源。

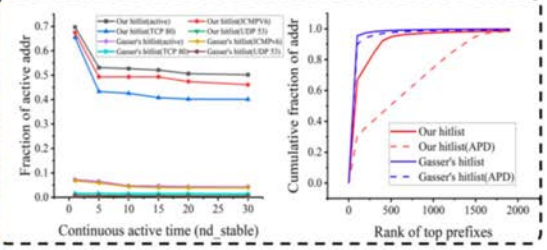
存活地址库信息

Table 6: Overview of our IPv6 Hitlist on September 8, 2021

Name	#IPs	#IPs[1]	#PFXes	#PFXes[2]	#Top AS1	#Top AS2	#Top AS3	#Top AS4	#Top AS5
1d-stable	2.1B	1.7B	86.4K	83.8K	20.40%★	16.39%■	13.20%◆	9.45%★	4.65%▶
7d-stable	1.5B	1.1B	85.7K	83.1K	23.41%★	21.48%■	14.44%◆	14.02%★	2.49%■
30d-stable	1.3B	919.4M	80.6K	78.0K	34.96%★	29.75%■	24.05%◆	3.85%★	1.73%■
60d-stable	1.3B	860.2M	80.3K	77.6K	36.74%★	31.83%■	19.62%◆	4.11%★	1.85%■
100d-stable	1.2B	783.7M	80.1K	78.5K	39.58%■	34.93%★	13.58%★	4.52%◆	2.03%■

[1] Removing aliased addresses using aliased prefix detection ★ Amazon, ■ Fastly, ◆ Imperva, ▶ ChinaTelecom, ★ Cloudflare, ■ Akamai.
[2] Removing aliased prefixes using aliased prefix detection

地址库质量



地址库对比

对比现有活跃地址库，包含更多IPv6地址资产，更进一步推进IPv6网络测量和安全研究。

地址源	地址量	是否公开	是否包含指纹信息
APNIC	2.2亿	否	否
TMU	680万	是	否
我们的地址库	62亿	是	是

2.2. 学术科研

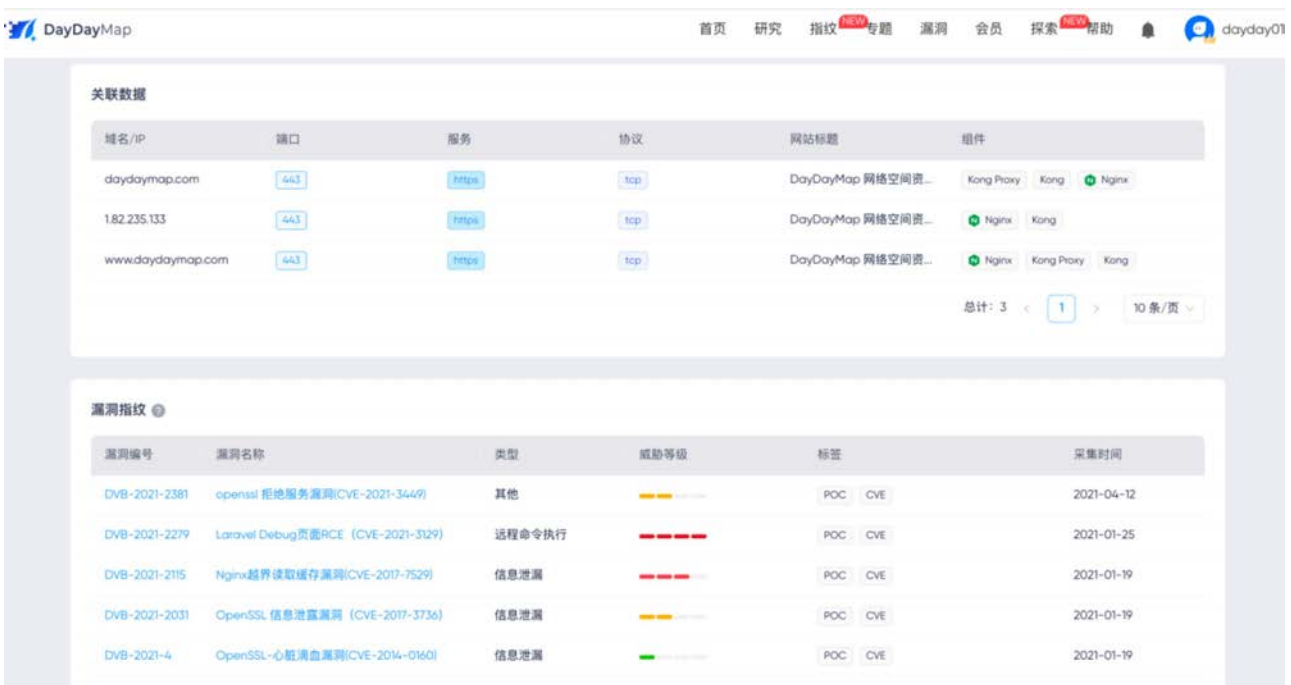
打造最具科研属性的网络空间资产测绘平台，与清华大学、中科院计算所等科研机构开展深入合作，保证探测数据的准确性、可靠性和科学性。

2.3. 数据融合与组织归属

多维度数据关联融合分析，精确识别资产归属与行业等信息，智能关联分析资产的归属单位，发现未知或未监控资产、服务和数据。

2.4. 联动 DayDayPoc 漏洞社区

联动 DayDayPoc 漏洞社区，基于指纹信息精确定位资产漏洞，实现紧急漏洞的快速评估、响应与全生命周期的监控。



2.5. AI 驱动特色指纹识别

精细化指纹识别，内置多种资产标签，有效识别蜜罐、挖矿、仿冒等多类站点，提升资产价值挖掘和风险控制能力。

利用机器学习和深度神经网络，对无特征或弱特征目标进行指纹识别，针对 DayDayMap 采集到的网站样本数据，提高识别精度利用大预言模型编码技术对网站内容进行编码，并基于长短时记忆神经网络算法对序列化数据实现分类任务，识别网站是否含不合法内容。

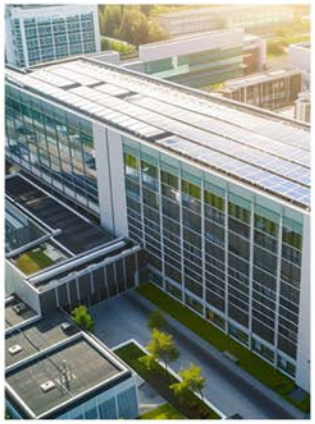
- 利用大语言模型中 Transformer-Encoder 技术对自然语言进行编码。结合 Bert 模型对不同国家语言的良好兼容性，具有极高的编码效率和模型通用性。
- 通过长短时记忆神经网络算法 LSTM 对编码后的序列化文本进行分类，准确率高。
- 不依赖于传统非法网站识别的关键字，排除人为关键字收集不全导致的模型不准确因素。
- 具有一定的自学习能力，通过少量的人工结果标注反馈，能自动化对模型进行优化。

3. DayDayMap 场景应用

提供全球网络资产全景视图、丰富的研究数据，助力科研人员研究网络空间的结构、演化规律、安全态势等，为网络安全、互联网治理、数字经济等相关领域理论研究提供丰富的真实数据支撑。

基础理论探索	关键技术研发	标准化工作	数据支撑与验证	攻击面梳理	攻防演习
研究网络空间资产的定义、分类、标识体系等基础理论问题，为资产测绘提供理论框架	开发高效、精准的资产发现、识别、追踪与分析技术，包括主动探测、被动监听、数据融合、深度学习等	参与制定网络空间资产测绘的国际、国内标准，推动数据格式、接口规范、测评方法等的统一	获取并分析大量真实网络环境中的资产数据，为模型构建、算法优化、效果评估提供实证支持	为高校等教育单位提供公网资产攻击面梳理，摸清家底，提升应急响应能力	对教育攻防演习提供目标资产梳理，绘制网络空间资产底图，对抗先机，提升网络攻防实战能力

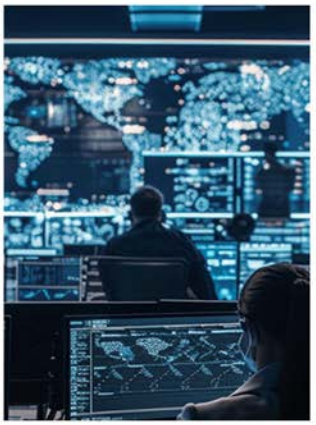
借助 DayDayMap 平台，各类组织能全面提升对其在线资产分布的洞察力，强化对数字化资产的整体管理和安全保障。能够增强组织对未知威胁的预警和响应能力，全面掌控网络空间资产的安全态势，及时感知并减轻潜在安全风险。优化资产安全管理成本，实现安全防护与经济效益的双重提升。



- 科研院所

- 监管机构

- 大型事业单位



- 安全研究者

科研院所：为科研院所提供测绘数据支撑，探索创新课题，研究测绘大数据产业化应用模型

监管机构：为监管机构提供态势分析，管辖决策，掌控辖区网络空间资产影响分布，挖掘并打击网络黑灰产

大型企事业单位：为大型企事业单位提供公网资产攻击面梳理，摸清家底，提升应急响应能力

安全研究者：为安全研究者提供目标资产梳理，对抗先机，提升网络攻防实战能力

附录

- **统计数据来源：** DayDayMap 全球网络空间资产测绘平台 www.daydaymap.com
- **Part I 10.学术科研 截图来源：**DayDayMap 全球网络空间资产测绘平台研究页

- **术语与定义：**

EASM（外部攻击面管理）：外部攻击面管理（External Attack Surface Management，EASM）是一种网络安全管理方法，专注于从外部攻击者的视角来识别、分析、监控和管理组织在互联网上暴露的资产、系统、服务、应用程序和数据等元素所构成的攻击面。它的目的是帮助企业全面了解自身在外部环境中的安全态势，及时发现潜在的安全风险和漏洞，以便采取有效的措施进行防护，降低遭受外部攻击的可能性。

IoT（物联网）：（Internet of Things，IoT）是指通过互联网等通信技术将各种物理设备（如传感器、执行器、智能家电、工业设备等）相互连接起来，实现设备之间的数据交换、协同工作以及远程监控和管理的网络。这些设备可以自动收集和传输数据，或者接收并执行远程指令，从而使物理世界与数字世界深度融合，为人们的生活、工业生产、城市管理等诸多领域带来智能化的变革。

Starlink（星链）：是 SpaceX（太空探索技术公司）推出的一个旨在通过在太空部署大量低地球轨道（LEO）卫星星座，为全球提供高速宽带互联网接入服务的项目。其目标是构建一个覆盖全球的卫星通信网络，解决偏远地区网络覆盖不足以及提供更高效的全球通信解决方案。

- **相关资源：**

[1]中华人民共和国国务院令 第 790 号《网络数据安全管理条例》

[2]《通用数据保护条例》（General Data Protection Regulation，简称GDPR）

[3]IDC《网络空间地图市场洞察，2023——生成式 AI 加持》

- **参考文献：**

[1] https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm《网络数据安全管理条例》

[2] https://mp.weixin.qq.com/s/6r4KxS3rtj6k1T4yCNV2Dw 引用盛邦安全实验室《国内大量家用路由器网络访问异常和流量劫持事件分析》

[3] https://mp.weixin.qq.com/s/8H3N6ouEKjdS0jAMhgoghQ 引用盛邦安全烽火台实验室《全球蓝屏危机？关于微软蓝屏事件的一些思考》

[4] https://developer.aliyun.com/article/1584411 参考阿里云《2024云安全洞察报告：趋势与策略》

远江盛邦安全科技集团股份有限公司

热线：4006 911 199

网址：www.webray.com.cn