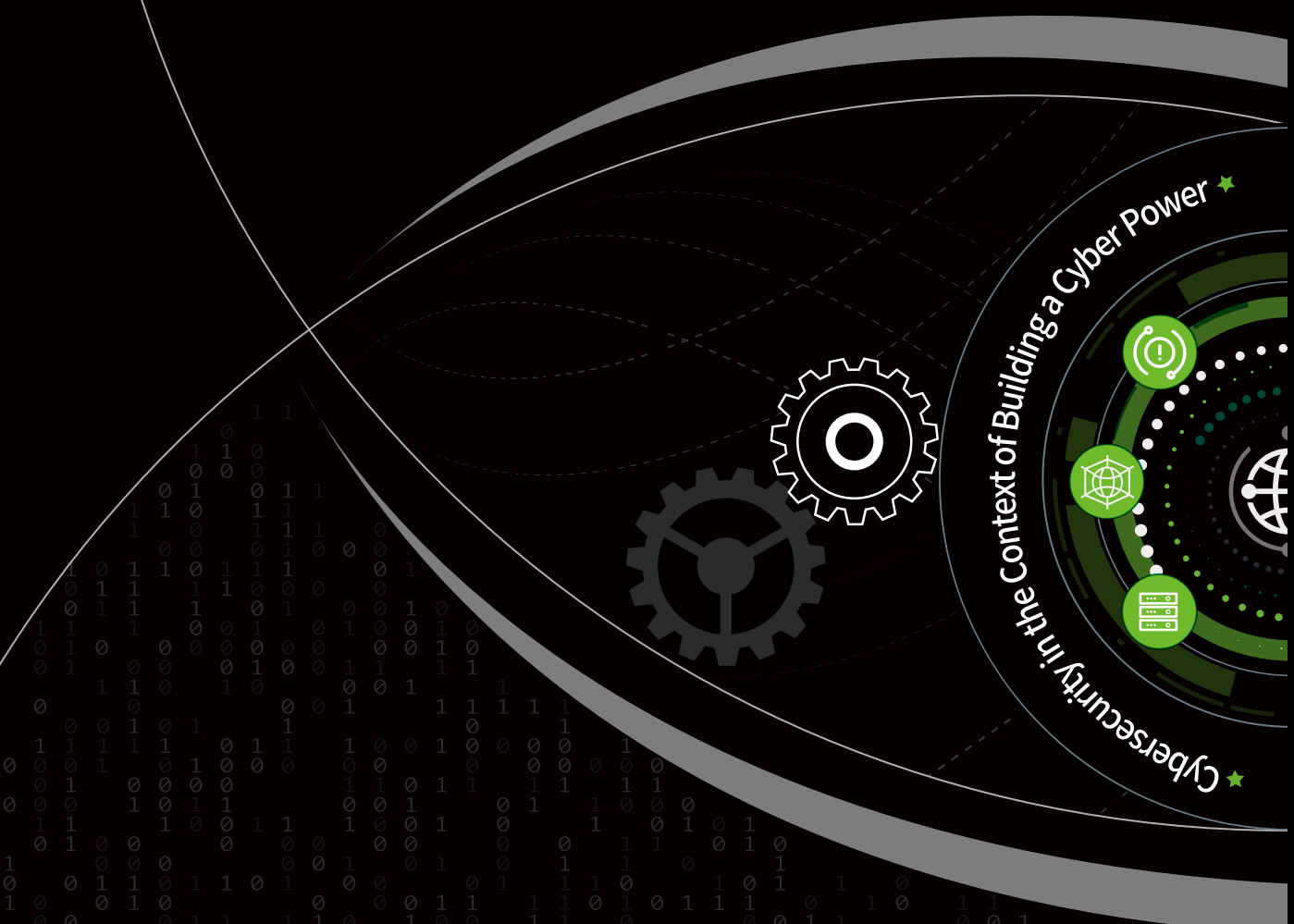
守望高质量

网络安全2022



NSFOCUS绿盟科技

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。

版权声明

卷首语

2021 年是“党和国家历史上具有里程碑意义的一年”。在胜利实现第一个百年奋斗目标基础上，党的十九届六中全会、中央经济工作会议相继胜利召开，开启了我国深入推进高质量发展的华彩序章。

网络安全作为数字经济发展的关键基础要素之一，在“稳中求进工作总基调”下更成为高质量发展的题中应有之义。回顾过去的一年，“网络安全现代化”“供应链安全”“数据安全”“漏洞管理”等成为引发高关注度的国内外网络安全高频热点领域。而其背后反映的实质，则是网络安全的云化、生态化、基础化趋势正在加速发展布局。

绿盟科技作为深耕网络安全产业前沿的一分子，密切关注国内外网络安全发展态势，并积极赋能网络安全供给侧创新研发。为此，我们依托自身研究队伍积淀，结合持续热点跟踪，将核心研究成果集结成册、形成本报告。

本报告包括三个篇章，即：态势篇、威胁篇、数字基础设施篇，筛选汇聚了我司本年度在网络安全攻防相关领域的核心研究成果。其中，态势篇重点梳理和分析了我国网络安全发展区域的威胁态势；威胁篇重点梳理和分析了网络安全面临的漏洞、恶意软件和高级可持续威胁等主要风险因素；数字基础设施篇重点梳理和分析了网络安全基础设施相关的热点事件、市场发展和领域趋势。

辞旧迎新之际，寄望本报告能为支撑国家网络安全主管部门决策略尽绵薄。并期待依托我司技术产品和服务，秉承“专攻术业，成就所托”的宗旨，全力服务于构筑国家高质量发展的网络安全屏障，并为全面加强国家网络安全保障体系和能力持续贡献力量。

2022年1月

CONTENTS

重点观察

★ 观察 1：区域威胁

2021 年，全国网络资产暴露加剧，数字资产暴露面不断扩大，用户的数据和个人隐私面临泄露风险，这些潜在威胁不容忽视。与此同时，安全漏洞、高风险端口开放、DDoS 攻击、恶意软件等网络威胁几乎遍布全国各省市，为我国的网络安全防护工作带来了严重挑战。

★ 观察 2：漏洞态势

新增漏洞数量相比 2020 年，呈现上升的趋势。跨站脚本 CWE-79 类型的漏洞数量最多；Windows ms17-010 系列漏洞扫描攻击事件最多；服务器中 Web 服务器受到的攻击是最多，Web 服务器中 CGI 的漏洞利用数量最多。

★ 观察 3：恶意软件

2021 年，勒索软件主要攻击目标为制造业、服务业等传统行业，美国遭受勒索软件攻击数量最多；僵尸网络仍然以 Mirai、Gafgyt 等传统 DDoS 家族为主；窃密木马与钓鱼邮件仍深度绑定，企业应注意钓鱼邮件的潜在风险。

★ 观察 4：高级持续性威胁

2021 年，受地缘政治影响，南亚、东亚和东欧地区依然是 APT 组织最为活跃的地区，朝鲜组织 Kimsuky 和 Lazarus 及新出现的东欧 APT 组织 Lorec53 的活跃度排名前列。

★ 观察 5：IPv6 安全威胁

IPv6 规模部署取得明显成效的同时，安全问题也逐渐暴露出来，IPv6 Web 攻击、漏洞利用和扫描事件占比位居前三。相比 2020 年，IPv6 漏洞和利用攻击事件大幅增加，境外的 IPv6 攻击源大幅增加，成为了国内企业面临的主要 IPv6 威胁来源，教育行业依旧是被攻击的重灾区。

★ 观察 6：数据安全

随着 2021 年《数据安全法》和《个人信息保护法》正式落地和实施，如何遵循合规性和保护敏感数据成为国内企业必答的一个安全命题。2021 年数据安全泄露问题依然严峻，其中在国内源代码泄露事件中， 金融和政府行业需重点关注。

★ 观察 7：物联网安全

随着物联网设备数量呈指数级增长，其攻击面暴涨。2021 年针对物联网的攻击事件数量上升，不断出现新的攻击方式，并带来巨大的危害，物联网安全相关标准化与自动化的需求迫在眉睫。

★ 观察 8：工业互联网安全

工业互联网攻击事件频发，勒索软件攻击占比最大。工业互联网是国家发展重要的战略，政策持续利好，工业互联网安全企业向安全服务、攻防靶场布局。

★ 观察 9：车联网安全

车联网相关威胁攻击不仅对网络空间中的信息安全带来影响，而且与物理空间中的人身、财产安全有着直接密切的关联。车联网产业链长，所需防护环节众多，构建覆盖全链条的综合防御体系将是车联网安全发展的必然趋势。

★ 观察 10：5G 安全

5G 作为新基建的重要基础设施之一，新漏洞 CVD-2021-0047 通过攻陷某一切片并对其他切片资源进行访问，进而获取未经授权访问的数据或发起 Dos 攻击。随着 5G 专网在各行各业的部署与应用，5G 专网安全也将势必开启新的市场。

★ 观察 11：人工智能安全

人工智能技术的蓬勃发展，拓展了数字世界的边界，AI 安全性问题逐渐暴露，相关事件频发，包括自动驾驶引发交通事故、基于 Deefake 合成语音与视频的诈骗等。安全可信 AI 已成为现阶段重点攻关方向。

★ 观察 12：云安全

云安全事件呈现上升趋势，非法利用云资源挖矿和云上数据泄露占据主要地位。政策及合规要求驱动云安全厂商及云服务提供商积极研发云安全产品及服务，云安全市场正处于快速增长期。

★ 观察 13：区块链安全

2021 年区块链被黑客攻击损失的数字货币价值已达 71 亿人民币。攻击的类型主要有欺骗、利用智能合约漏洞攻击、钓鱼攻击等方式实施攻击。区块链是新一代数字技术的重要组成部分，区块链的智能合约安全为主要方向。

★ 观察 14：供应链安全

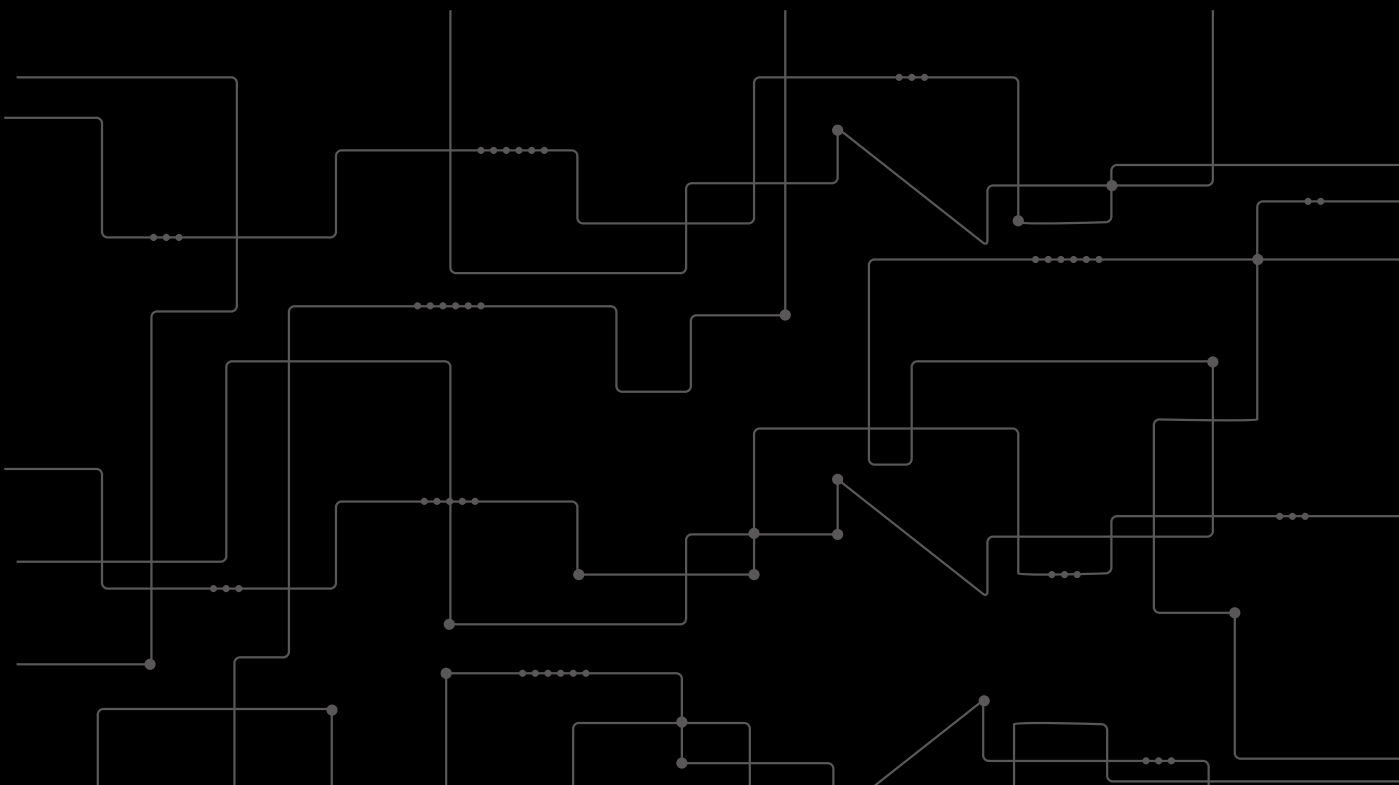
供应链安全隐患正在成为网络安全防护上最薄弱的环节，供应链安全事件频发，严重威胁着关键信息基础设施的安全。各国政府通过制定相应法律、政策和标准要求、指导和促进供应链安全市场的发展。

★ 观察 15：无线通讯安全

以 5G、移动物联网、北斗为代表的各类无线技术广泛应用于社会生活的各方面，成为数字中国建设的关键技术。针对无线宽带 Wi-Fi、蓝牙 Bluetooth 等安全事件频繁发生，所以在日常的使用过程中一定要注意提高安全意识。

1

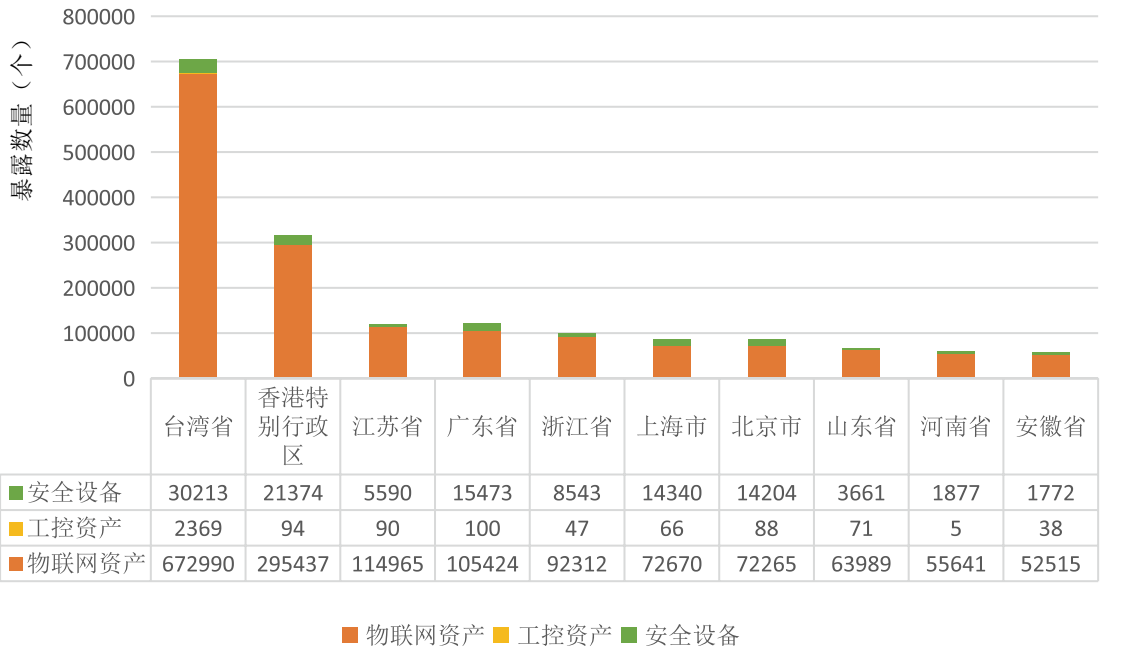
态势篇



1.1 网络资产暴露情况

1.1.1 重要硬件资产

截至 2021 年 11 月 26 日，全国共暴露重要硬件资产数量为 2,168,588，包括物联网资产、工业控制系统和安全设备，如图 1.1 所示。暴露总数排名前三的省市分别为台湾、香港和江苏，接下来暴露数量比较多的是长三角和珠三角地区的沿海城市。其中，物联网资产暴露数量最多，约占总暴露资产的 2,018,364，并且香港和台湾最多，主要是由于这两个地区的 IP 地址分配的较多，很多物联网设备直接使用公网 IP 接入互联网。工控资产暴露数量靠前的分别是台湾、黑龙江省和吉林，暴露数量与各省市的工业发达程度相关。安全设备暴露数量前三的是台湾、香港和广东。



	台湾省	香港特别行政区	江苏省	广东省	浙江省	上海市	北京市	山东省	河南省	安徽省
安全设备	30213	21374	5590	15473	8543	14340	14204	3661	1877	1772
工控资产	2369	94	90	100	47	66	88	71	5	38
物联网资产	672990	295437	114965	105424	92312	72670	72265	63989	55641	52515

图 1.1 全国暴露重要硬件资产规模分布 TOP10 省市

暴露数量最多的物联网资产依次为摄像头、路由器、VoIP、网络存储器、交换器和打印机等。其中，摄像头和路由器是暴露数量最多的物联网资产，占比分别为 52.0% 和 26.2%，如图 1.2 所示。暴露在互联网上的摄像头存在巨大的安全隐患，一旦被黑客控制，可能会造成个人隐私泄露，给用户的隐私安全带来了严重威胁。

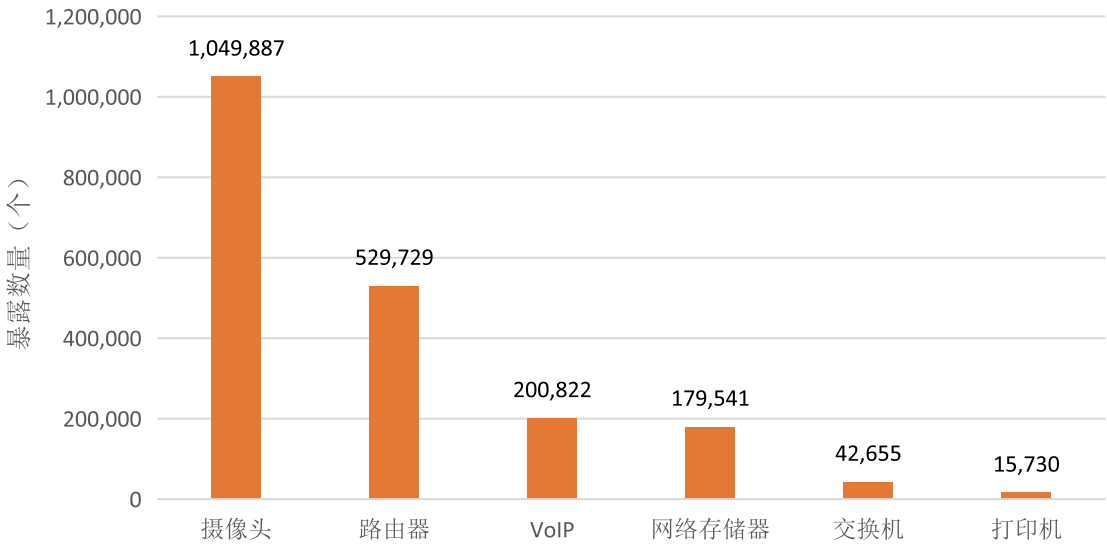
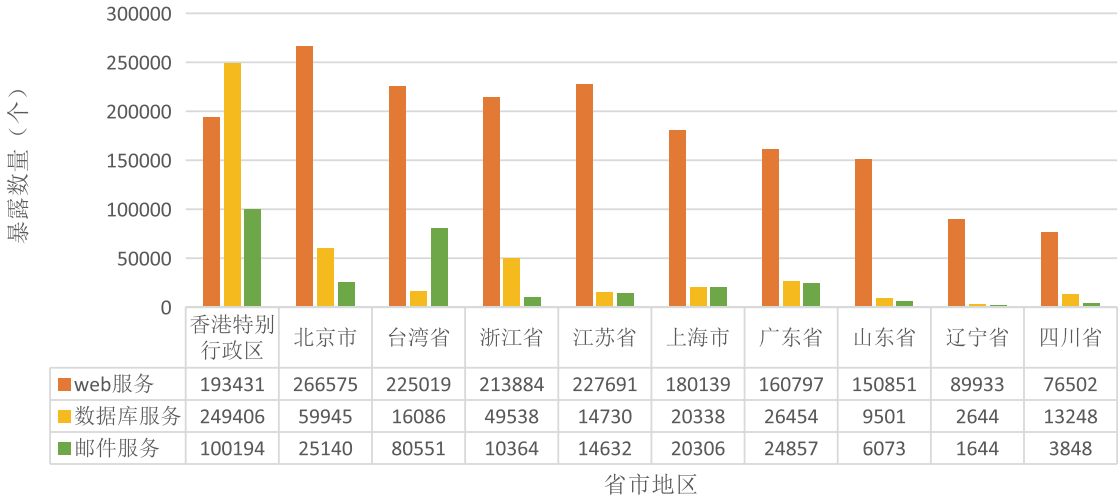


图 1.2　暴露物联网资产类型分布

1.1.2　重要服务资产

互联网上的应用层出不穷，web 服务、数据库服务和邮件服务应用最为广泛，因此，接下来重点对这三类应用的分布情况进行研究分析。全国范围内，应用这三类服务最多的省市分别是香港特别行政区、北京和台湾。其中，web 服务应用最多，占比为 74.9%，应用数量 TOP3 的省市分别为北京、江苏和台湾，如图 1.3 所示。数据库服务和邮件服务应用数量较多的省市分别为香港特别行政区、北京、浙江和台湾。香港特别行政区有着得天独厚的地理位置，邻近大陆，出口国际带宽充足，成为用户选择云服务的首选，三类重要服务的应用数量最多；北京市作为向全世界展示我国形象的首要窗口，将建设成为全球数字经济标杆城市，信息化水平处于国内领先地位，三类服务的应用数量排名第二。同时，面临的安全风险也较大，这些互联网服务很可能成为黑客攻击的入口，获取服务器权限，进而入侵内网。



	香港特别行政区	北京市	台湾省	浙江省	江苏省	上海市	广东省	山东省	辽宁省	四川省
web服务	193431	266575	225019	213884	227691	180139	160797	150851	89933	76502
数据库服务	249406	59945	16086	49538	14730	20338	26454	9501	2644	13248
邮件服务	100194	25140	80551	10364	14632	20306	24857	6073	1644	3848

图 1.3　互联网重要服务分布 TOP10 省市

全国暴露在互联网上的数据库服务数量为 513,636，如图 1.4 所示，暴露的数据库基本覆盖了常见的数据库类型，例如 MySQL、Oracle、Elasticsearch 等。数据库服务暴露在互联网上将会带来巨大的安全风险，因为黑客攻陷服务后有可能造成敏感数据泄露或数据勒索等事件。因此，应及时关闭非必要开放的数据库服务，对必须开放的服务进行访问控制，避免数据库被攻陷后带来的重大影响。

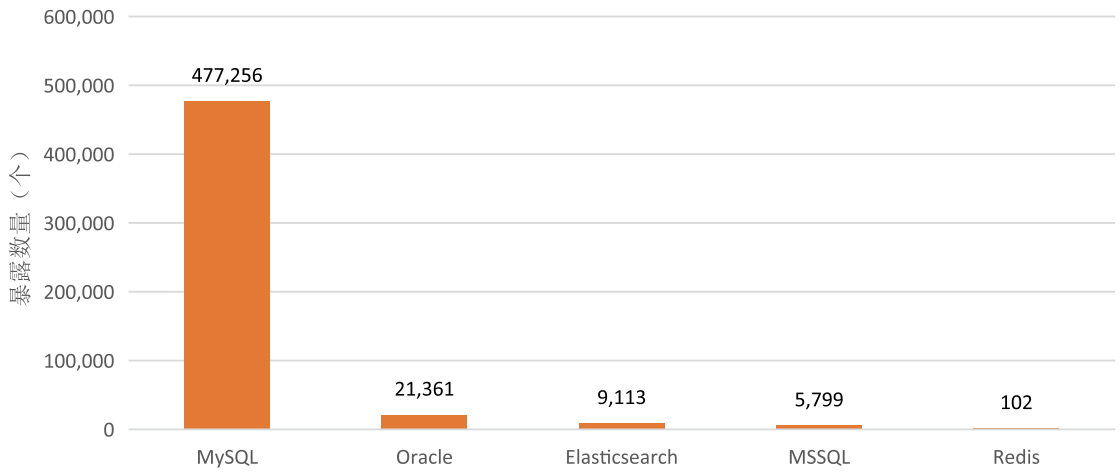


图 1.4　数据库服务类型分布

全国暴露在互联网上的邮件服务数量为 310,458，如图 1.5 所示，主要包括 SMTP、POP 和 IMAP 等类型。邮件服务也是黑客最常用的网络攻击渠道之一，攻击者往往会利用邮件传播恶意软件、窃取身份验证、实施网络钓鱼和金融诈骗等。

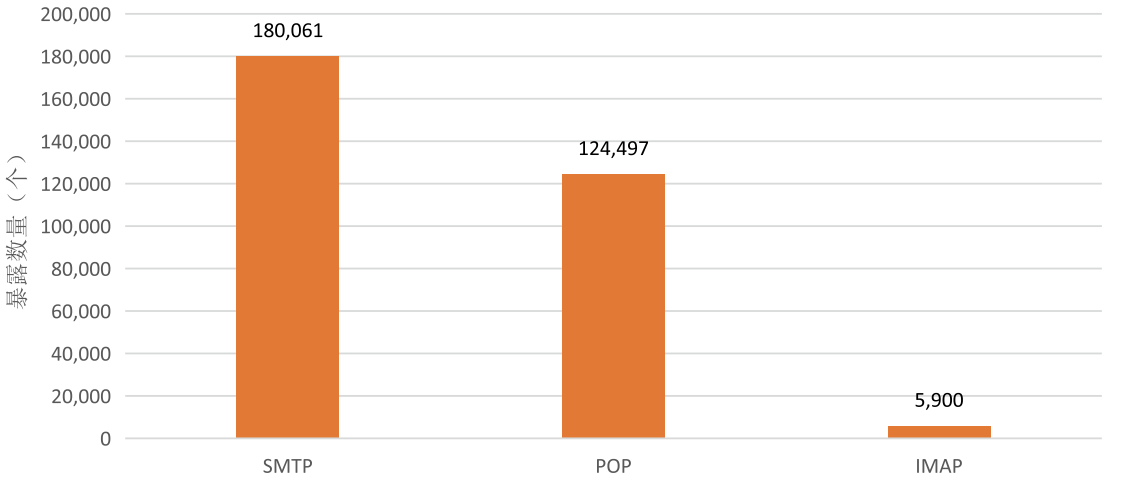


图 1.5　邮件服务类型分布

1.2　高风险主机

1.2.1　高风险端口开放情况

在互联网上暴露高危服务端口，会降低系统的安全性，增加黑客攻陷系统的概率。在本年的热点事件中，除了传统的高危 21、22 端口， 3389 端口和 2375 端口也频繁被黑客或 APT 组织利用，危害很大。

通过绿盟威胁情报中心的统计，全国开放了高风险端口的资产数量共计 5,962,519 个，如图 1.6 所示。其中，开放 22、3389、21 和 2375 端口的资产数量占比分别为 49.4%、26.5%、24.1% 和 0.0001%。从地理分布上看，香港特别行政区暴露在互联网上的总资产最多，开放高风险端口也是最多的，总计开放端口数量 1,218,303 个，其次是上海市和北京市，分别开放端口数量 671,997 个和 668,537 个，高风险端口的开放情况基本与各省市暴露的总资产数量成正相关。

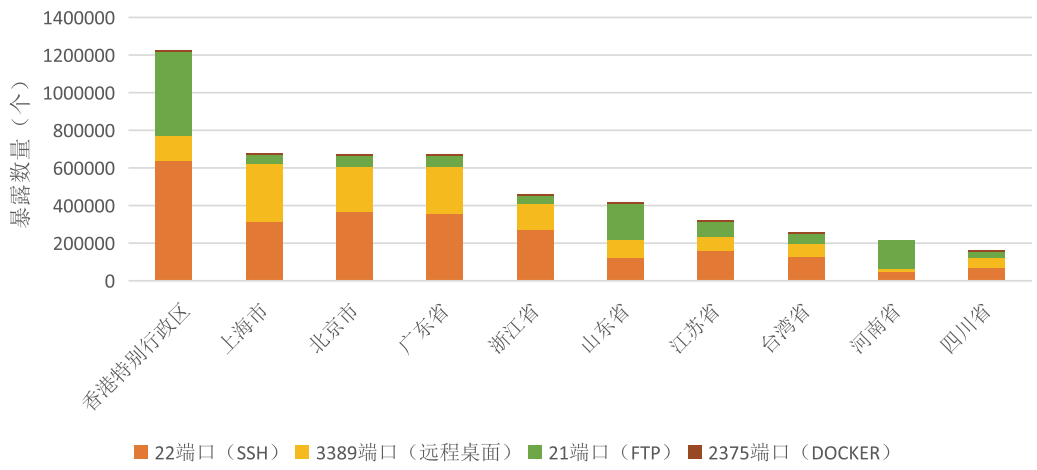


图 1.6　高风险端口地理分布 TOP10 省市

1.2.2　DDoS 反射攻击资源情况

互联网暴露 DDoS 反射攻击主机是暴露在互联网上，可能会被黑客利用来发起 DDoS 攻击的资产。这类资产被黑客利用参与 DDoS 攻击后，不仅耗费自身的网络带宽，影响自身系统可用性，而且也会成为黑客对其他关键基础设施可用性攻击的“帮凶”。

绿盟威胁情报中心，对云端的互联网资产测绘发现，全国有 1,959,355 个 IP 可能会被黑客利用打 DDoS 反射攻击，常见类型包括：UPNP、NTP 和 DNS 类型等具体服务器，如图 1.7 所示。从地理分布上来看，江苏、台湾和浙江的 DDoS 反射攻击资源数量分列前三位，分别是 198,539 个、189,225 个和 187,397 个。

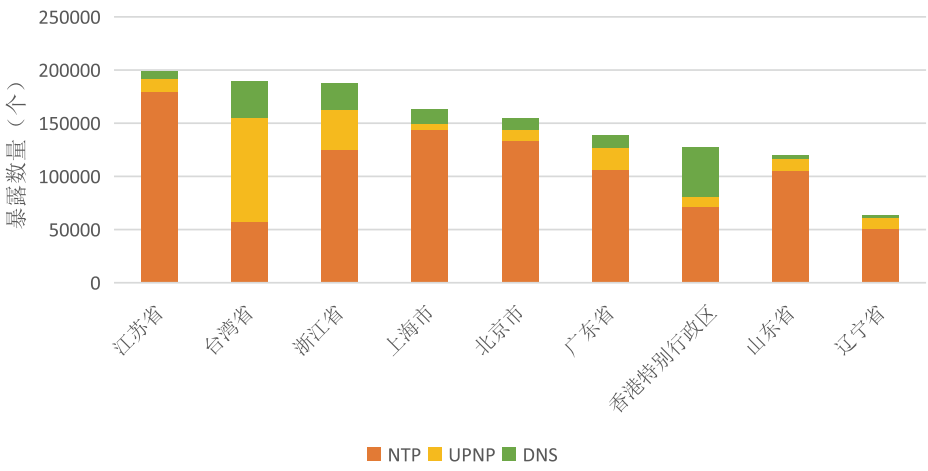


图 1.7　DDoS 反射攻击资源地理分布 TOP10 省市

1.2.3 使用停更数据库的主机

通过绿盟威胁情报中心的统计分析发现，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。暴露在公网的 MySQL 数据库中，大约 45.6% 的官方已停止更新的 MySQL 版本仍在使用，数量较多的分别是：版本 5.1（10,750）、版本 5.6（41,905 个）和版本 5.5（32,497 个），如图 1.8 所示。

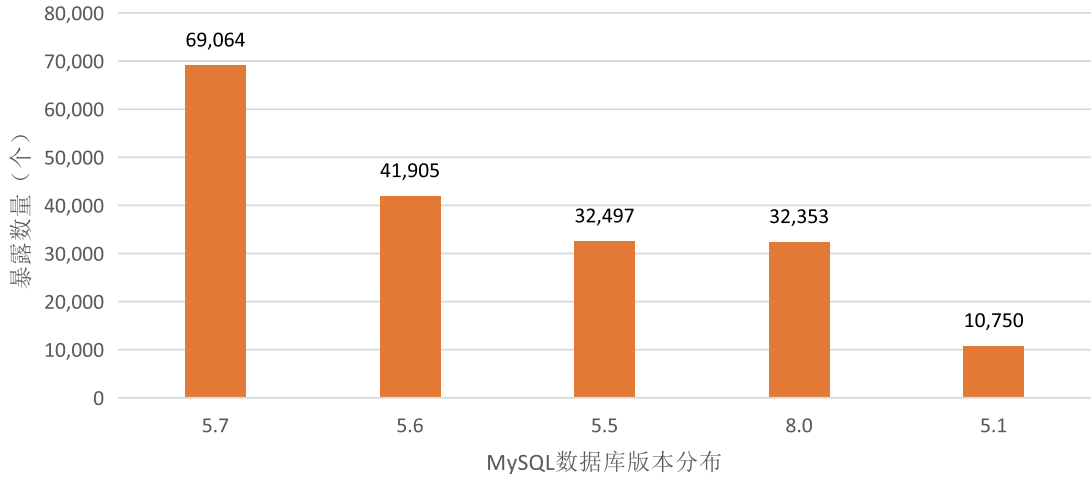


图 1.8 MySQL 数据库版本分布 TOP5

表 1.1 为 MySQL 数据库暴露数量最多的五个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 1.1 MySQL 暴露版本发布和停更时间

版本	发布时间	停更时间
MySQL5.1	2008 年 12 月	2013 年 12 月
MySQL5.5	2010 年 12 月	2018 年 12 月
MySQL5.6	2013 年 2 月	2021 年 2 月
MySQL5.7	2015 年 10 月	2023 年 4 月
MySQL8.0	2018 年 4 月	2026 年 4 月

已经停止更新但仍在被使用的 MySQL 数据库地理分布如图 1.9 所示，与暴露数据库服务的地理分布基本重合，排名前三的是香港、北京和浙江，已停更但仍在使用的 MySQL 数据库占各省市暴露数据库服务的比例分别是 4.6%、10.0% 和 11.5%。

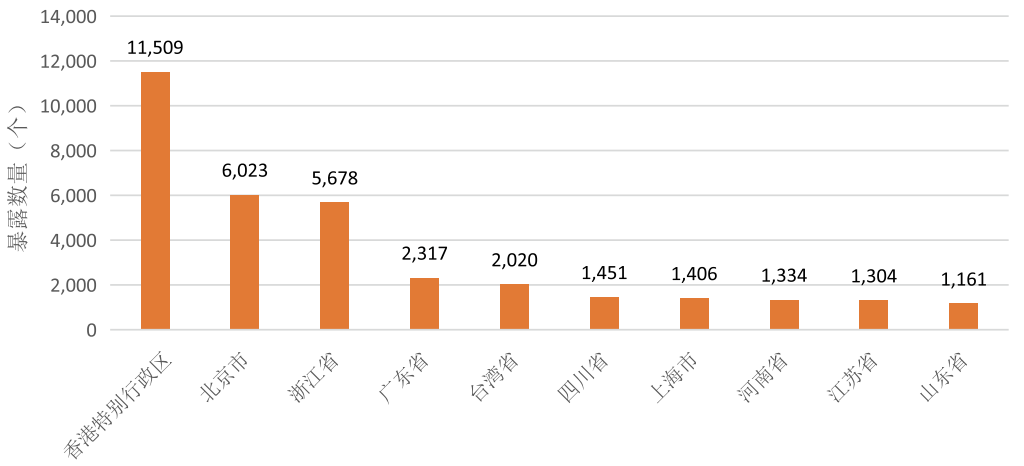


图 1.9　已停更 MySQL 数据库仍被使用情况地理分布

1.3　恶意 IP 态势

1.3.1　攻击类型

从恶意 IP 攻击类型来看，主要包括拒绝服务、僵尸网络、扫描、垃圾邮件、Web 攻击、漏洞利用等，具体分布如图 1.10 所示。拒绝服务攻击因攻击成本低、攻击效果明显等特点，仍然是互联网用户面临的最常见网络安全威胁之一，攻击数量占总数的 72.8%，其次是僵尸网络攻击和扫描攻击，分别占比为 6.5% 和 5.0%。

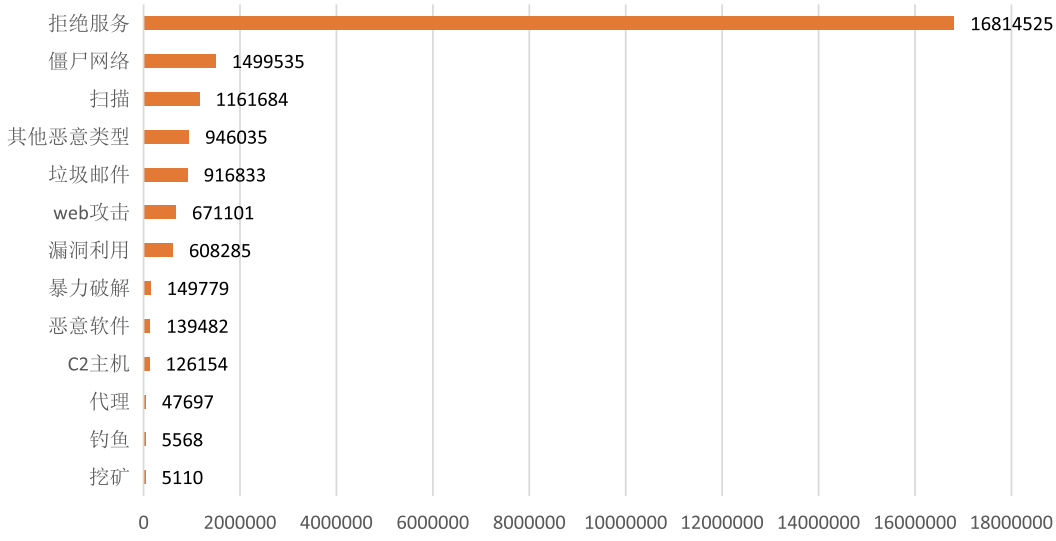


图 1.10　攻击类型分布

1.3.2 攻击源地理分布

从攻击源 IP 的地理分布来看，广东省、山东省和浙江省的攻击源 IP 数量分列前三位，分别是 593,714 个、508,104 个和 456,542 个，具体分布如图 1.11 所示。

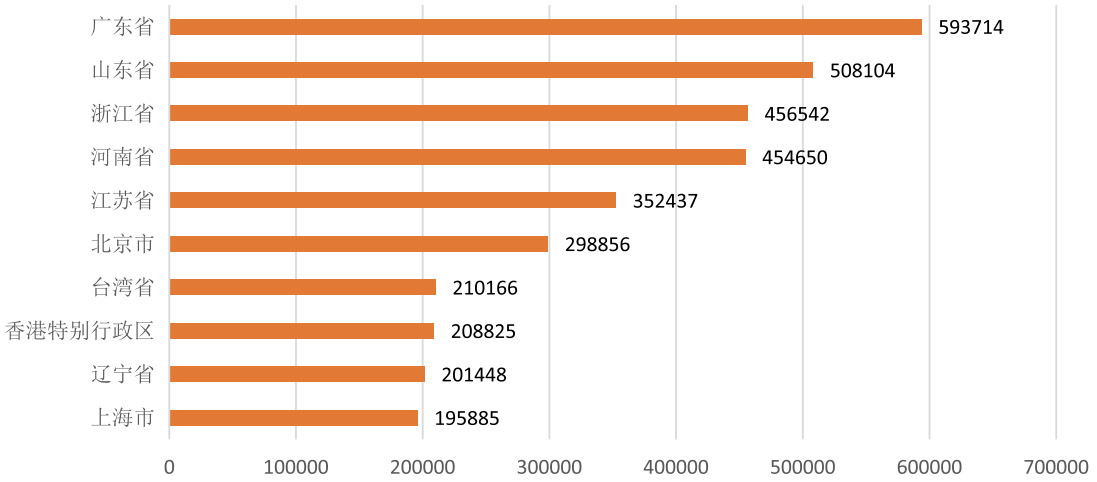


图 1.11 攻击源全国分布 TOP10

1.3.3 攻击目标地理分布

从攻击目标 IP 的地理分布来看，上海市、广东省和北京市的攻击目标 IP 数量分列前三位，分别是 787,348 个、734,885 个和 556,501 个，具体分布如图 1.12 所示。

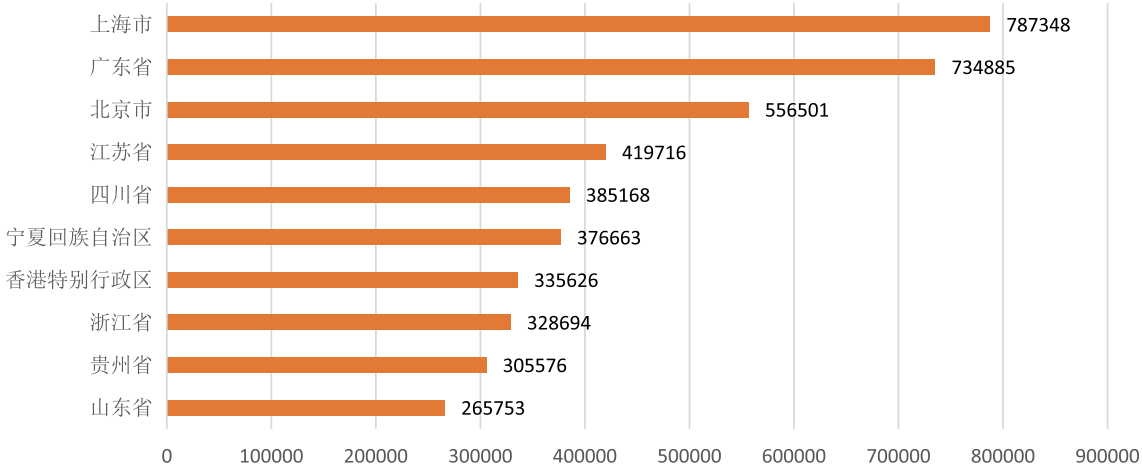
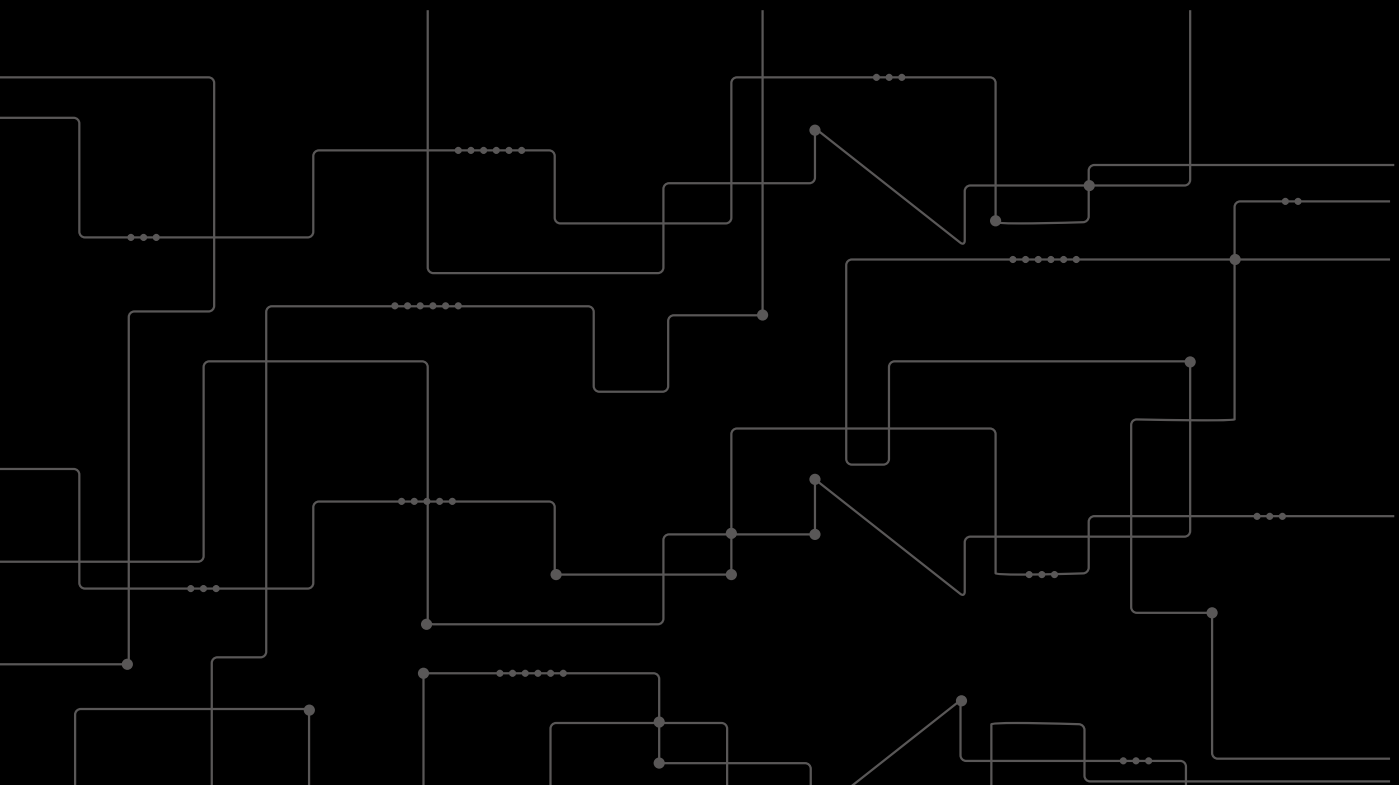


图 1.12 攻击目标全国分布 TOP10

2

威胁篇



2.1 漏洞态势

2.1.1 漏洞总体态势

根据 NVD 数据库已收录的公开发布漏洞数目进行观察，截至 2021 年 12 月 31 日，2021 年新增加的漏洞数量为 19780 个[1]，相比 2020 年呈上升趋势。

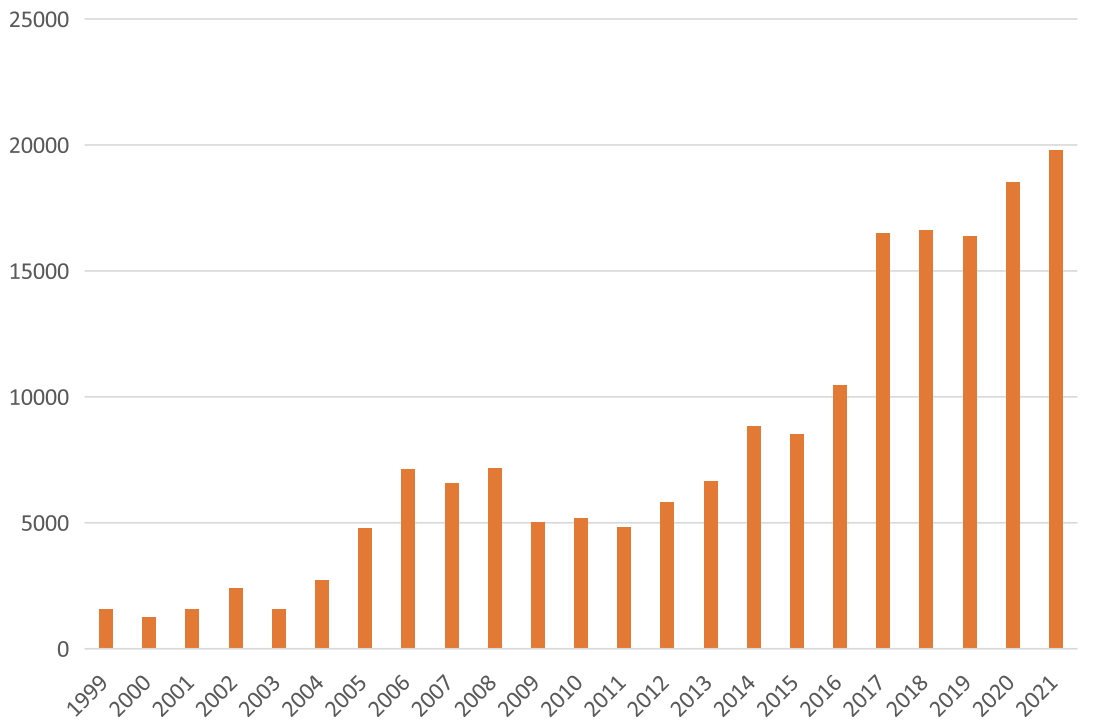


图 2.1 历年漏洞数量统计

截止 2021 年 12 月 31 日共有 19520 个漏洞分配 CVSS 3.1 等级。根据 CVSS 3.1 标准，漏洞等级被划分为四级，9.0-10.0 为危急漏洞，7.0-8.9 为高危漏洞，4.0-6.9 为中危漏洞，0.1-3.9 的则为低危漏洞，各个等级按数量分布的占比如图 2.2 所示。

[1] 该漏洞数量包含了在 2021 年内新增的往年漏洞数据

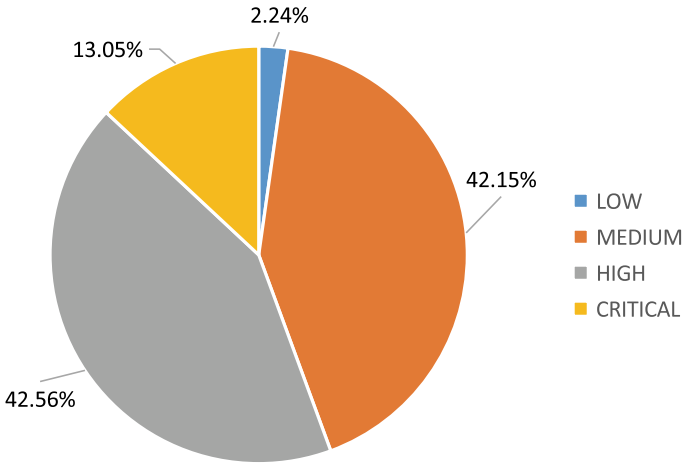


图 2.2　漏洞 CVSS 3.1 按数量分布

危急漏洞占比 13.05%，高危漏洞占比 42.56%，两者占比达到 55.61%，攻击者利用此类漏洞可以远程执行任意命令或者代码，有些漏洞甚至无需交互就可以达到远程代码执行的效果。

NVD 数据库提供 CWE 条目，可对漏洞成因进行统一的分析，并且一个漏洞可分配多个 CWE ID。2021 年收录的漏洞中，共分配了 19992 个 CWE ID，图 2.3 给出了 TOP10 CWE 漏洞类型 [1]。

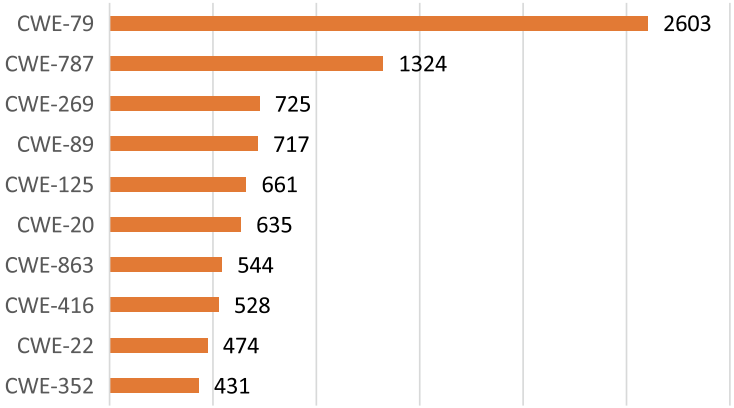


图 2.3　2021 年 TOP10 漏洞类型

其中跨站脚本 (CWE-79) 类型的漏洞数量最多。跨站脚本漏洞主要是由于 Web 应用程序对用户的输入没有进行严格的过滤所导致的，攻击者利用此类漏洞可以将恶意的 JS 或 HTML 代码注入到用户浏览的网页上。

[1]　该排名不包含 NVD-CWE-noinfo（信息不足）和 NVD-CWE-Other（其他）的数据。

2.1.2 漏洞利用

根据绿盟科技威胁情报中心监测到的安全事件，绿盟科技整理出了 2021 年告警中与漏洞利用相关的攻击事件，提取了告警数量比较高的 10 个漏洞信息，如表 2.1 所示。

表 2.1　2021 年漏洞利用告警数量 TOP10

漏洞编号	漏洞名称	告警数量
ms17-010	windows ms17-010 系列漏洞扫描攻击	8265202
CVE-2016-7288	microsoft edge 远程内存破坏漏洞 (ms16-145)	6442952
CVE-2017-0144	windows smb 远程代码执行漏洞 ((ms17-010)	1877732
CVE-2016-0800	openssl sslv2 弱加密通信方式易受 drown 攻击	1759425
CVE-2014-6271	gnu bash 环境变量远程命令执行漏洞 (cve-2014-6271)	707579
CVE-2017-5638	struts2 远程命令执行漏洞 (s2-045)(s2-046)	536958
CNNVD-201211-555	fckeditor ‘fileupload()’ 函数任意文件上传漏洞	511677
CVE-2016-6277	netgear dgn1000b setup.cgi 远程命令注入漏洞	461292
CVE-2018-10561/10562	gpon home gateway 远程命令执行漏洞	442892
CVE-2008-2214	castle rock computing snmpc 超长团体字符串栈溢出漏洞	421839

从表 2.1 中数据可以发现，10 年以上的高龄漏洞仍然在活跃，说明互联网上依然存在着大量长期未更新的软件和系统，如物理隔离环境下的内网中，就可能存在没有及时更新补丁或版本的核心系统、数据库等系统和软件，攻击者一旦进入内网就可以利用这些成熟的漏洞利用代码发起有效的攻击。根据监测到的漏洞利用事件，绿盟科技统计了常见的攻击类型，如图 2.4 所示，TOP3 攻击类型为 CGI 攻击、畸形攻击以及溢出攻击。

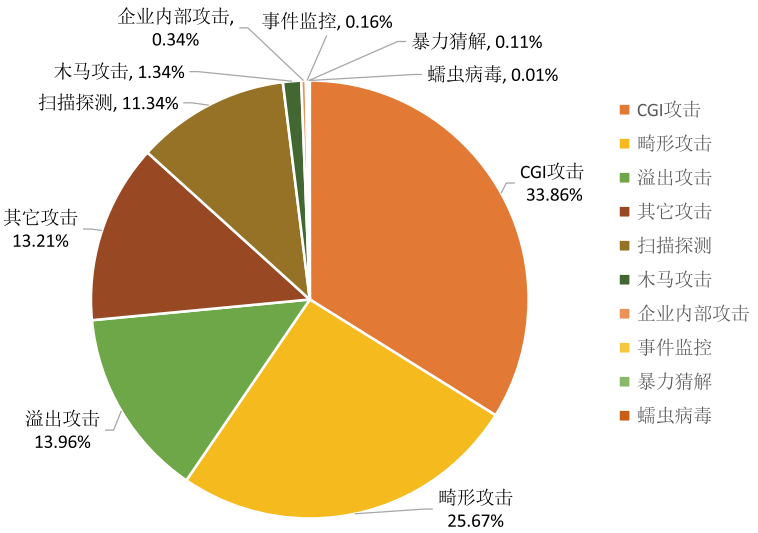


图 2.4　漏洞利用攻击类型统计

2.1.3 服务器漏洞

服务器漏洞主要为服务器上的系统服务与程序，用于支撑或提供网络管理与实际业务。服务器类型主要包含 Web 服务器、扫描服务器、Windows 服务器、DNS 服务器中、数据库服务器、邮件服务器等。根据绿盟威胁情报中心监测到的数据，统计了各类服务在漏洞利用中的占比，如图 2.5 所示。其中 Web 服务器受到的攻击是最多，占比 68.14%。

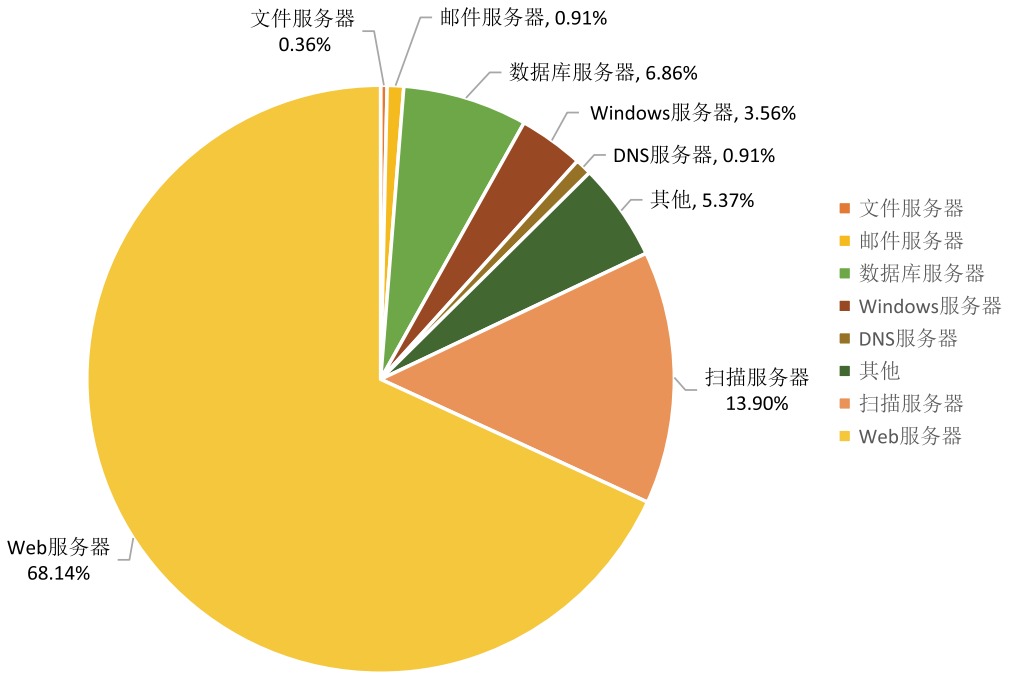


图 2.5 服务器漏洞利用统计

绿盟科技对具体的服务类型进行统计，统计数据为各服务类型的漏洞利用数量相加，统计结果如图 2.6 所示。从图中可以看到漏洞利用最多的服务是 CGI（Common Gateway Interface，公共网关接口）。CGI 是 Web 服务器与外部应用程序之间交换数据的标准接口。CGI 漏洞主要是由于配置错误、输入验证错误、边界条件错误等引起的，攻击者利用此类漏洞可以进行信息泄露、代码执行等操作。

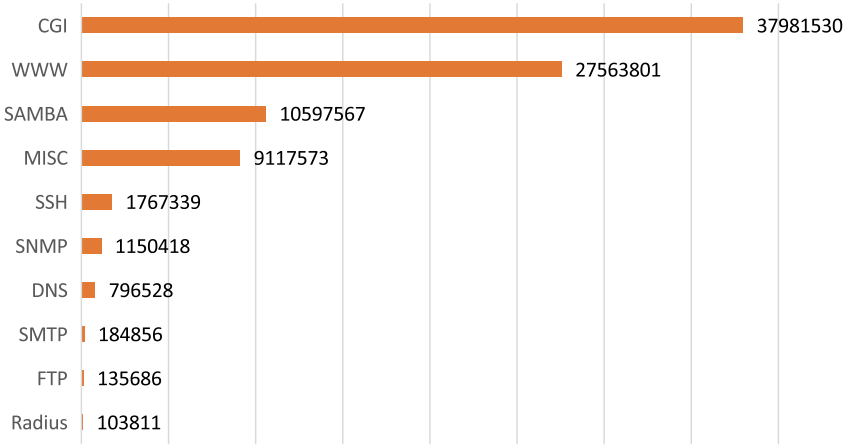


图 2.6　TOP10 漏洞利用服务类型

2.1.4　应用软件漏洞

常见的应用软件包括浏览器、Office 办公软件、Flash 播放器、PDF 阅读器以及移动终端软件等。绿盟科技统计了各类应用软件在漏洞利用中的占比，如图 2.7 所示。攻击者利用钓鱼邮件，通过恶意链接、恶意附件的形式投递恶意程序，在用户点击相关资源时，对应程序的漏洞会被触发，最终导致感染和信息泄露。浏览器作为攻击的入口在实际利用中深得攻击者的关注，在实际网络攻击中达到了 83.51% 的比例，远超 2020 的 48.54% 比例。

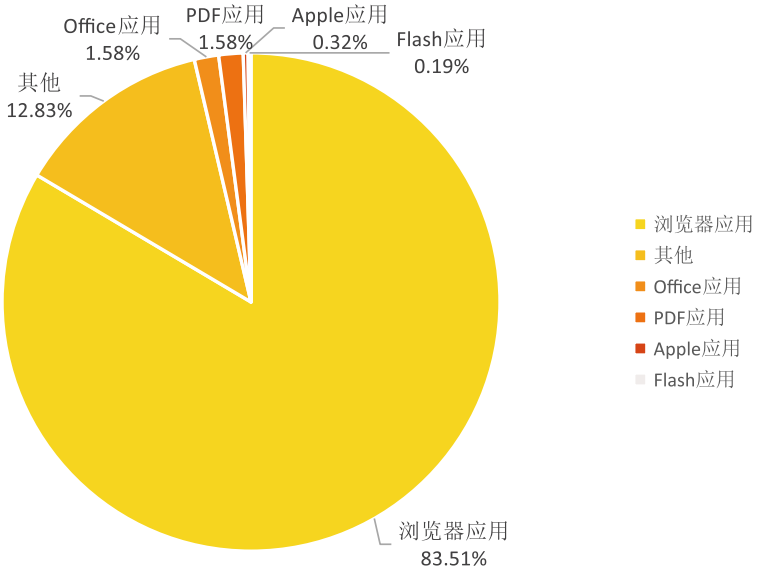


图 2.7　应用软件漏洞利用分布

浏览器的漏洞中告警最多的应用是微软的 Edge 浏览器，相关的漏洞有 CVE-2016-7288、CVE-2016-0193 等，大都由 Edge 处理内存对象不当触发的，攻击者利用这些漏洞可达到任意代码执行的目的。

Flash 漏洞在实际利用中的占比持续下降，2021 年更是下降至 0.19%，随着 Adobe 对 Flash 插件的淘汰，各大厂商都对其采取了一系列的封杀机制，在今后的一段时间内，Flash 的漏洞利用将面临消亡。

2.2 恶意软件态势

2.2.1 勒索软件

2021 年以来，由于疫情导致远程工作增加，勒索软件攻击数量呈上升趋势，对制造业、服务业、金融、医疗等行业构成重大威胁。

2.2.1.1 勒索软件攻击目标分布

根据绿盟科技长期观测，2021 年较活跃的勒索软件主要有 MountLocker，PYSA，REvil，CLOP，AVADDON 及 DarkSide，其中 REvil 家族全年活跃并在 9-10 月份达到最高峰。

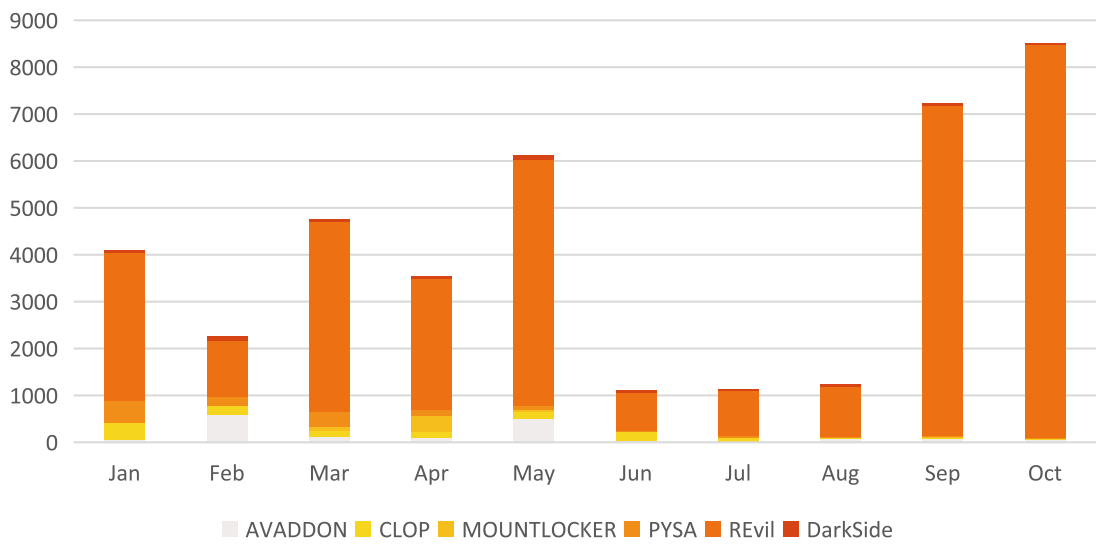


图 2.8 勒索软件月度活动分布

在受害者地区分布方面，欧美国家为勒索软件的重灾区，其中美国占比高达 62.65%。

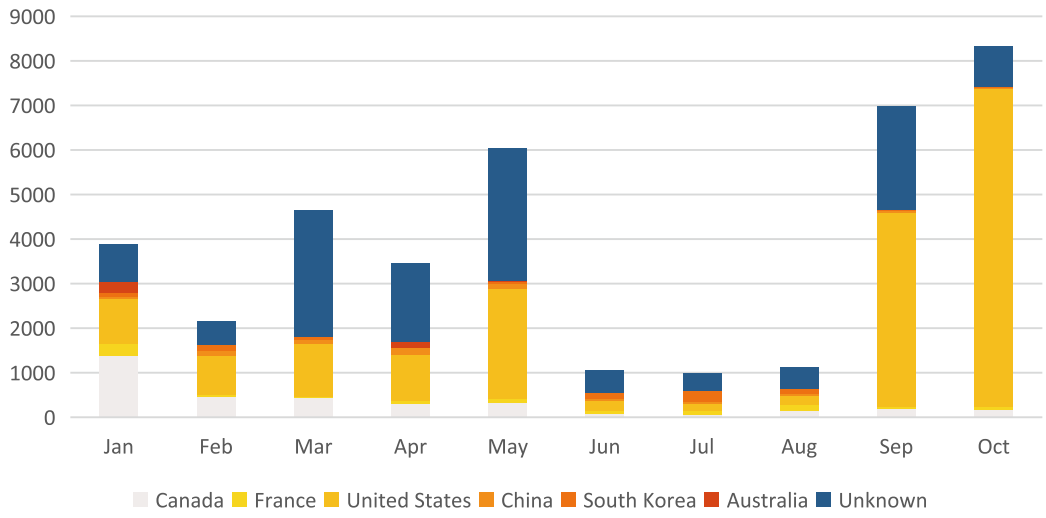


图 2.9　勒索软件国家分布

在受害者行业分布方面，制造，服务，金融，法律，医疗行业占据前 50%，以制造业为最。

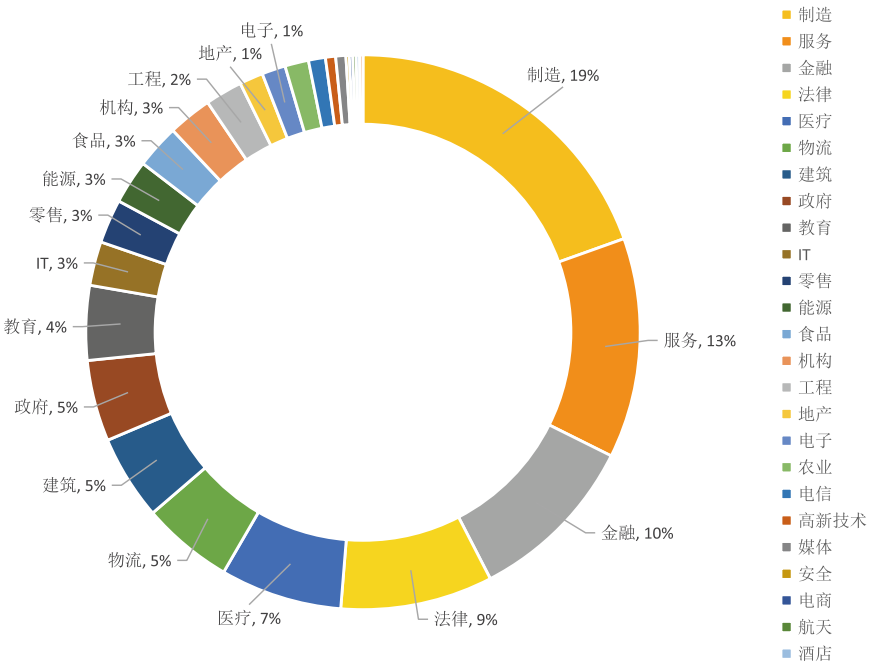


图 2.10　勒索软件受害者行业分布

2.2.1.2 国内勒索软件攻击态势

北上广等经济发达地区为勒索软件实施打击的主要目标。

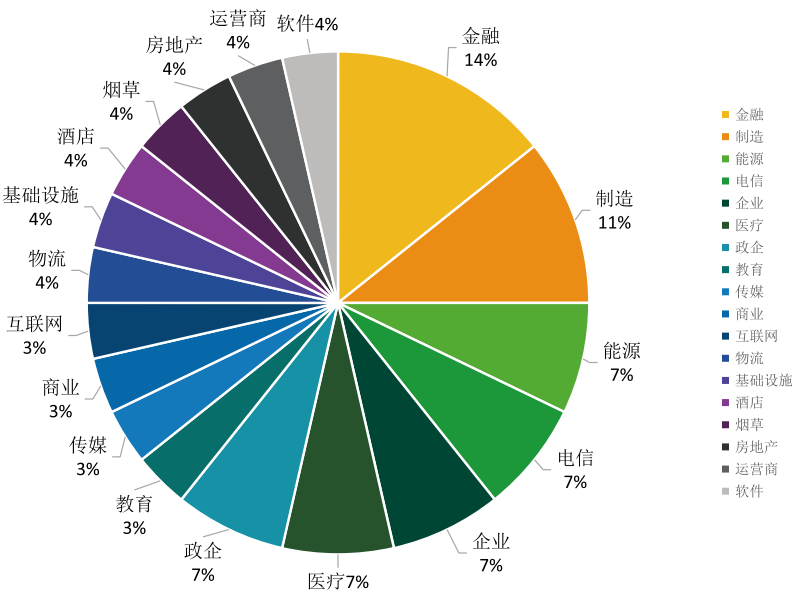


图 2.11 国内勒索软件受害者行业分布

在受害者目标选择方面，金融，制造，能源，电信，医疗产业仍旧为主要行业。

在目标脆弱性方面，仍以弱口令，弱凭据，组件漏洞不及时修复所导致。

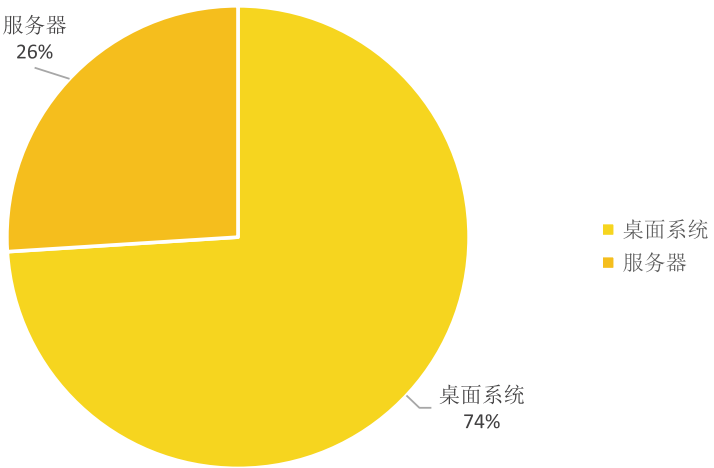


图 2.12 勒索攻击事件中受影响设备类型占比

在操作系统方面，勒索软件主要影响服务器系统，但也有约 25% 的勒索软件受害者是桌面系统。

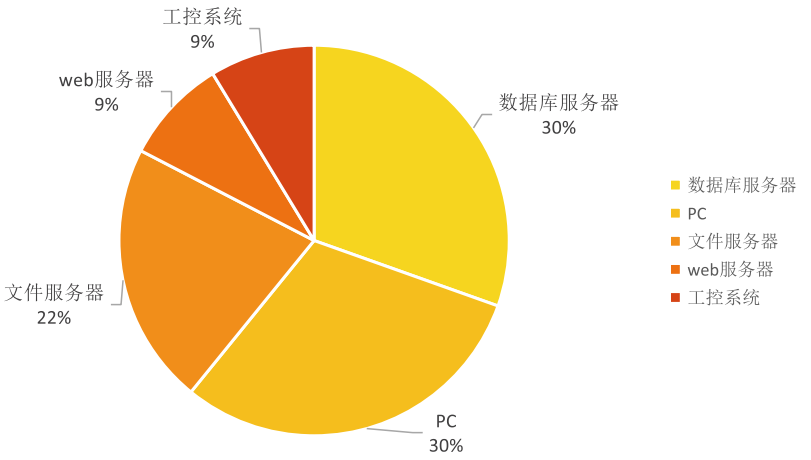


图 2.13　受勒索攻击业务系统类型占比

勒索软件攻击者在业务类型选择方面，主要针对数据库业务和文件服务业务。

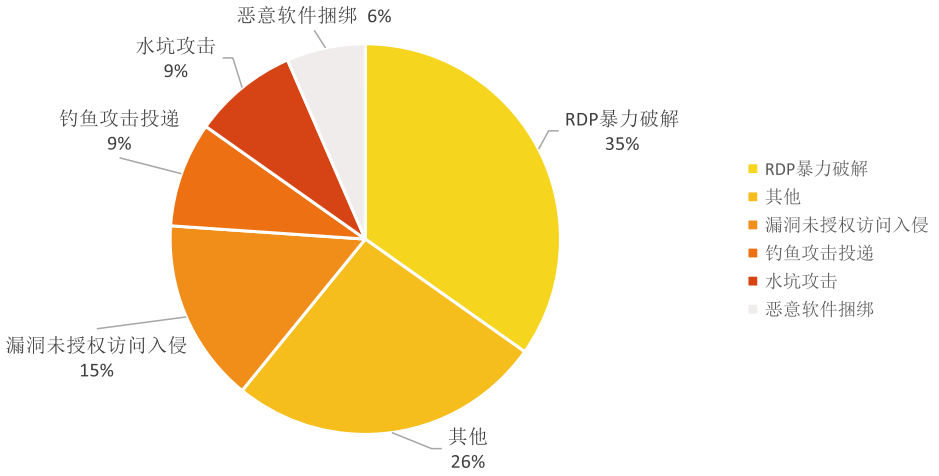


图 2.14　勒索攻击事件中勒索软件入侵方式

勒索软件攻击者最常用的入侵手段为 RDP 暴力破解，在下半年流行的针对个人勒索的应急与观察中，也采用了恶意软件捆绑和水坑攻击传播。

2.2.1.3　攻击模式变化趋势

渗透方式方面：由于勒索软件传播能力较弱，多不具备横向移动特性，因此越来越注重

与僵尸网络、银行木马、远控木马、钓鱼邮件等相结合，以加强其投放能力。CLOP 通常依赖钓鱼邮件释放的木马在受害者机器立足，SDBbot 木马曾多次释放 CLOP，CLOP 采用代码签名方式，将自己伪装成合法软件；Avaddon 与 Smoke Loader、IRC Botnet、Phorpiex Botnet 合作进行投放，还利用 RDP 及 VPN 爆破进行渗透；REvil 在初始阶段常采用 RDP 爆破；DarkSide 的攻击往往以 RDP 爆破及漏洞利用开始，入侵成功后在受害者机器安装 R AT 软件，实现长期控制，还会利用 CS Beacon 工具进行横向传播。

勒索方法方面：勒索软件多采用加密与泄密相结合的双重勒索模式，如果受害者拒付赎金，则勒索团伙将公开其敏感文件。一些勒索团伙，如 CLOP、REvil，还搭建了公示敏感文件的网站。此外，越来越多的勒索团伙，如 PYSA、Avaddon、REvil、DarkSide，都提供勒索软件即服务（Ransomware as a Service，RaaS），将勒索软件租赁给技术不完善的团伙。Avaddon 利用与 DDoS 僵尸网络相结合的优势，在加密勒索之外加入 DDoS 攻击，给受害者施以额外的压力。

漏洞利用方面：CLOP 利用 Accellion 文件传输产品漏洞 CVE-2021-27101、CVE-2021-27102、CVE-2021-27103、CVE-2021-27104 发起攻击；REvil 利用 SonicWall 产品漏洞 CVE-2021-20016 收集 SSL VPN 的账号密码凭证，利用 Exchange Server CVE-2021-27065 和 CVE-2021-26855 为后续行动建立根基；DarkSide 利用 ESXi 的 CVE-2020-3992 、CVE-2020-3992 进行攻击。

攻击事件方面：2021 年 2 月，DarkSide 团伙攻击 Canadian Discount Car and Truck Rentals 公司，并窃取 120G 数据。3 月，REvil 团伙攻击电脑巨头宏碁（Acer），索要 5000 万美元赎金。2021 年 5 月 7 日，DarkSide 团伙攻击美国主要的成品油管道公司 Colonial Pipeline，受此事件影响， 5 月 9 日，拜登政府宣布美国进入紧急状态。6 月，REvil 团伙攻击了全球最大肉食品加工商 JBS Food 的美国分部，索要 1100 万美元赎金，导致美国食品加工和交付出现重大中断。7 月 3 日，REvil 团伙攻陷 Kaseya VSA 服务器并感染数千节点，并利用其更新推送能力传播勒索软件，导致数百企业数据被加密。

打击勒索方面：2021 年 6 月，美国，乌克兰，韩国联合执法团队在乌克兰首都基辅附近，逮捕 CLOP 团伙中的 6 人，没收了作案设备及非法所得，封堵了其数字货币交易渠道。2021 年 11 月 4 日，美国国务院宣布提供 1000 万美元，悬赏 DarkSide 团伙主犯。11 月 8 日，美国国务院宣布提供 1000 万美元，悬赏 REvil 团伙主犯。2021 年 11 月，美国联邦司法部逮捕并起诉 REvil 团伙的骨干分子，关停了该团伙的数据泄露网站，REvil 的生命接近尾声。

2.2.2 僵尸网络

2021 年初，绿盟科技伏影实验室联合 CNCERT 共同披露了攻击组织 KekSec，该团伙通过 2021 年的运作，已发展至一定规模，也出现了大量的伪装为 KekSec 活动的僵尸网络运营者。KekSec 组织的运营者在各类社交渠道标榜其攻击成果，也为该组织博得了大量的关注。除了该组织外，绿盟科技伏影实验室也监控到了 Windows、IoT、MacOS 平台上的一些新型新的僵尸网络家族。伏影实验室僵尸网络威胁追踪平台 BotHunter 通过对僵尸网络家族进行长期追踪监控，也获知了诸如 Mirai、Gafgyt 等家族的 DDoS 攻击活动信息。

2.2.2.1 攻击态势

根据绿盟科技伏影实验室僵尸网络威胁平台 BotHunter 对 9 个热门僵尸网络家族的监控数据统计发现，Mirai 和 Gafgyt 拥有的 C&C 新增数量最多，长期维持在月度 60 个以上，远超其他普通窃密类僵尸网络，这是其开源属性及 IoT 平台相对疏于管理的网络安全环境造成的。这些僵尸网络的 C&C 月度数量在年末都呈现下降态势。不同的是，Mirai 和 Gafgyt 的 C&C 月度数量是整体呈现下降，而窃密类僵尸网络的 C&C 月度数量则在年中增长至峰值。在窃密类木马中，C&C 月度数量排在前两名的分别为远控木马 Gh0st 和窃密木马 AgentTesla。造成这种情况的原因是，Gh0st 木马因早年源码公开而产生了大量变种，而 AgentTesla 则通过阶梯式售价大量售卖而源源不绝，并通过钓鱼邮件进行广泛投递。

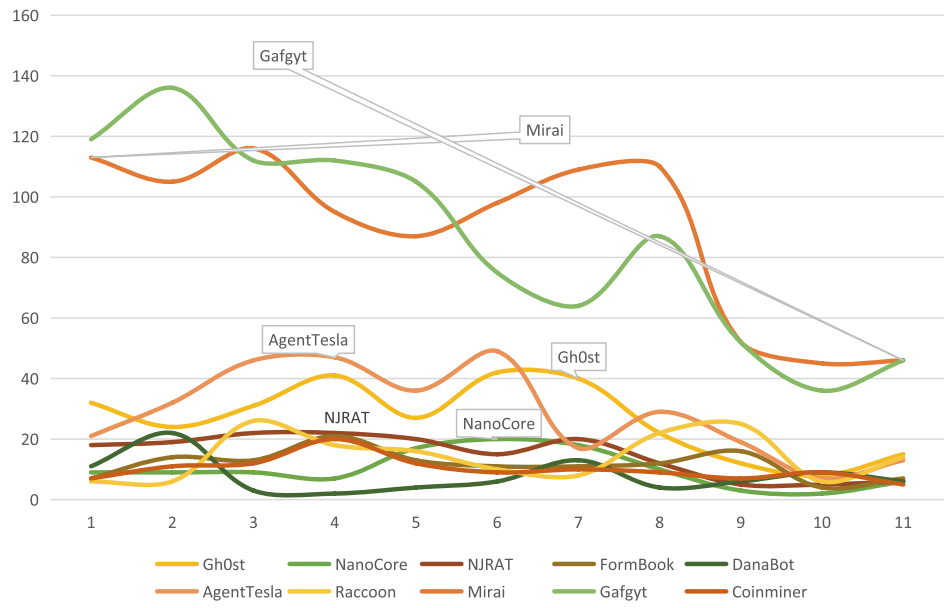


图 2.15　部分热门僵尸网络家族 C&C 月度变化

Mirai 作为长期称霸 DDoS 僵尸网络的家族，其平均单月新增 C&C 数量保持在 90 左右，平均每日就新增 3 个 C&C，生命力极其旺盛。这样的部署规模，使 Mirai 得以保持了全年的活跃度。

与 2020 年相比，检测到的 Mirai 与 Gafgyt 的新增 C&C 数量都有明显的下降，造成这种情况的主要原因是，其他修改自 Mirai / Gafgyt 源码的新家族频生，抢占了过往僵尸网络的空间。而且一些新家族在对抗措施有所补强，再加上 tor 网络节点的使用，相比原生 Mirai / Gafgyt 更难以检测。

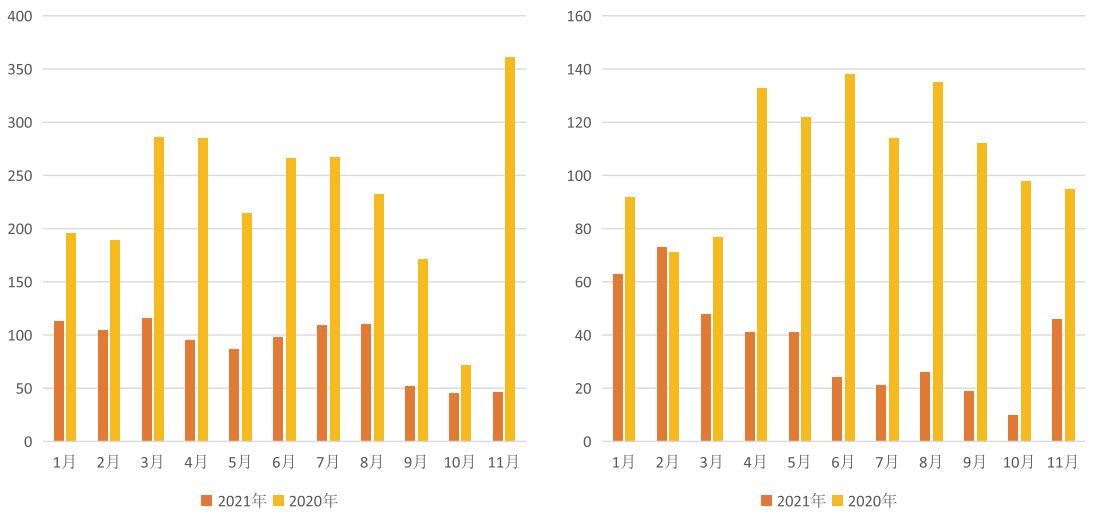


图 2.16　Mirai Gafgyt 2021 与 2020 月度新增 C&C 数量对比

2.2.2.2　热点家族及团伙

2.2.2.2.1　Mirai 及其变种

依据 Bothunter 监测数据，Mirai 本年度平均单月新增 C&C 数量保持在 90 左右，平均每日就新增 3 个 C&C，生命力极其旺盛；与 2020 年相比，检测到的 Mirai 的新增 C&C 数量有明显的下降，造成这种情况的主要原因是，其他修改自 Mirai 源码的新家族频生，抢占了过往僵尸网络的空间。而且一些新家族在对抗措施有所补强，再加上 tor 网络节点的使用，相比原生 Mirai 更难以检测。

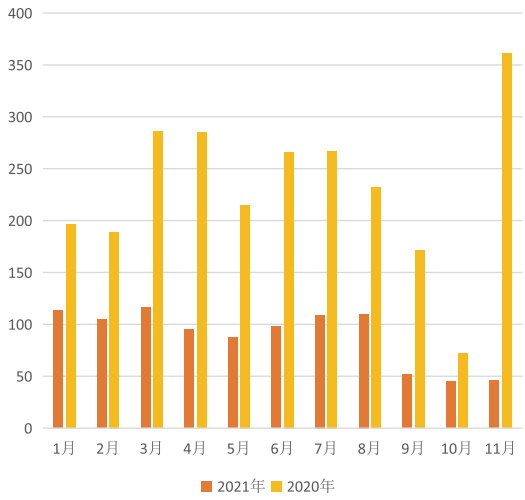


图 2.17　Mirai 2021 与 2020 月度新增 C&C 数量对比

Mirai 主要通过漏洞利用和弱口令环境传播，8 月出现的一类 Mirai 变种木马 fetch，携带的漏洞数量达到 31 个，范围涵盖 2021 年以前的多数常见漏洞以及两个疑似 0day 漏洞。在我们对漏洞利用情况的监测中发现，攻击者对披露的漏洞利用转化速度也越来越快，2016 年 Mirai 僵尸网络集成漏洞的速度约为 4.5 天，到 2020 年已经变为 1.8 天，2021 年已经变为 0.8 天，Mirai 因代码开源而导致大量变种产生，其变种将长期存在并不断新增，本年度依旧有大量基于 Mirai 架构的新家族出现，相较于 Mirai 又有许多创新，例如基于 Mirai 架构的 mirai_ptea 使用 TEA 算法加密敏感字符串和 C2 信息，在通信过程中使用 Tor Proxy 和 C2 建立连接，达到了比较好的规避效果。再如修改自 Mirai 源代码的 ZHtrap 僵尸网络为了提高扫描效率实现了一个监听常见端口的简易蜜罐，增加了自身扫描的目的性和成功概率。

2.2.2.2.2　Keksec 相关

2021 年初，绿盟科技伏影实验室披露了攻击组织 KekSec，该团伙通过 2021 年的运作，已发展至一定规模，甚至出现了大量的伪装为 KekSec 活动的僵尸网络运营者。僵尸网络运营者在各类社交渠道炫耀其所作所为，也为该组博得了大量的关注；KekSec 黑客组织创建于 2016 年，是一个极为活跃的黑客组织，该组织运营着多个僵尸网络家族进行 DDoS 攻击和挖矿，攻击工具丰富，采用多种技术架构，能够快速利用已公开漏洞。

本年度，绿盟科技伏影实验室发现该组织增加了新成员 ur0a[1]，多个新增的僵尸网络家族都归功于该成员；ur0a 在四月到九月期间新添加了多达五个僵尸网络，这包括了 Simps

[1]　http://blog.nsfocus.net/ryuk-botnet/

Botnet，gods of destny Botnet，Ryuk Botnet，Samael Botnet 以及 Akuryo Botnet。鉴于这些僵尸网络都是由 ur0a 开发，有着相同的风格，因此将它们统称为 ur0a Botnet，依据发现时间的先后顺序，排列如下：

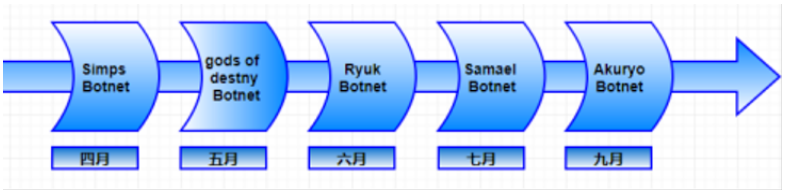


图 2.18　ur0a Botnet 发展时间线

ur0a 急于出名，在入侵设备后习惯于留下组织信息以及 instagram 和 Discord 联络方式，带有很强的宣传色彩；同时注意到这些新增的僵尸网络家族功能单一，主要攻击方式以 DDoS 为主，部分变种在开发后期仅停留在通过文件层面的处理来加强隐蔽性，缺少技术创新，这在一定程度上反应了开发者的真实水平。不过，上述这些僵尸网络家族版本迭代频繁，部分变种至今仍保持一定程度的活跃，显示了该组织人员在运营所持有僵尸网络时一直保持着信心和耐心。

本年度新发现的僵尸网络 lolfme Botnet 同样隶属于 KekSec 组织，但相较于 ur0a Botnet 却有着截然不同的风格；ur0a Botnet 感情热烈，个性张扬，带有极强的宣传目的；lolfme 相对低调，所有敏感的资源信息加密存储，通信过程也极为隐蔽，更具实战意义；lolfme 从发现至今经历了四次版本的更迭，功能趋于完善，隐蔽性也在不断增强；lolfme 最初涵盖了 x86-64，Intel 80386，ARM 等多个 CPU 架构，但在近期主要转战 ARM 平台，虽然该僵尸网络家族的活跃程度远不及如日中天的 Mirai 及 Gafgyt，但依然在不断更新升级并完善功能，需要给予足够的重视。

2.2.2.2.3　Pink

2021 年 10 月，绿盟科技伏影实验室联合 CNCERT 公开披露了一个藏在我们身边的巨型僵尸网络 Pink，相关事件发生于 2019 年 12 月份，黑客定向攻击某运营商的家庭用户设备并植入控制程序 Pink，使其成为僵尸网络节点，根据所涉运营商和设备厂商的初步评估，被黑客入侵并控制的设备数量超过百万，其中 96% 以上的受害者分布在中国境内，这或许是已公开的规模最大的 IOT 僵尸网络。鉴于 Pink 的规模和影响，我们已第一时间通报给相关运营商和主管部门，并联系相关设备厂商，协作处理和解决受影响的设备，绝大多数被入侵的设备已被修复。

此次事件中，黑客利用了设备生产供应链中的某些组件的 0-day 漏洞，入侵了多个品牌的家庭网关类设备，并在设备上植入了恶意程序。Pink 恶意程序从功能上可以划分为 3 个模块：植入、驻留、控制。

图 2.19　Pink 的模块及功能

此次攻击事件已经超出了僵尸网络的范畴，可以定性为一次高级定向攻击事件，特点如下：

高级性：黑客挖掘了运营商的特定设备、特定固件的 0-day 漏洞

定向性：针对特定品牌的设备设计了 0-day 攻击，北京区装机量最大

定制性：Pink 仅适配了特定设备的处理器架构

持久性：Pink 自己能够修改设备固件，保证自身能够长期存在

潜伏性：Pink 没有暴露自身的多余行动，如扫描攻击等

Pink 是一个融合了多种对抗技术的僵尸网络，攻击者通过 P2P 和 CNC 两种方式对 Pink 进行控制和管理，僵尸网络家族使用新通信协议，组合式通信协议能力上升，从流量上更加难以检测，P2P 的组网方式也为清除造成了一定的障碍，这也让我们想起了与 Pink 同年出现的僵尸网络 Mozi，其最显著的特点就是特有的通信协议，作为 P2P 僵尸网络的代表作，Mozi 僵尸网络健壮性极好， 即使部分节点瘫痪，整个网络仍然能工作，虽然 Mozi 的作者已被执法机关处置，但残余节点仍然会存活一段时间。

2.2.3　木马

2021 年，需要重点关注挖矿木马和窃密木马。挖矿木马通过利用各种手段，将挖矿程序植入到用户的计算机中，偷偷利用用户的计算机进行执行挖矿功能，从而获取收益。窃密木

马主要通过钓鱼邮件植入木马后，设法控制和篡改计算机，以此达到窃密的目的。

2.2.3.1 挖矿木马

2.2.3.1.1 Sysrv

2021 年 3 月，一个可针对 Windows 及 Linux 平台的恶意软件开始传播，此恶意软件结合的蠕虫和矿工两大组件，其中蠕虫部分主要作为传播模块，该蠕虫利用了企业常用软件和框架中的六个漏洞，其中包括 Mongo Express、XXL-Job、XML-RPC、Saltstack、ThinkPHP 和 Drupal Ajax；此外，该恶意软件所带来的额外风险是它的下载功能，通过下载并执行其它恶意程序，为攻击者提供了进一步的入侵。

表 2.2 漏洞利用表

Exploit	Software
CVE-2021-3129	Laravel
CVE-2020-14882	Oracle Weblogic
CVE-2019-3396	Widget Connector macro in Atlassian Confluence Server
CVE-2019-10758	Mongo Express
CVE-2019-0193	Apache Solr
CVE-2017-9841	PHPUnit
CVE-2017-12149	Jboss Application Server

Sysrv 是一个由 go 语言编写的 64 位可执行程序，有适用于 Windows 和 Linux 平台的两个版本。随着开发者对 Sysrv 的更新，Sysrv 不断地结合新的漏洞利用进行更有效地传播，绿盟科技伏影实验室针对 Sysrv 的衍变进行了梳理：

表 2.3 Sysrv 挖矿程序组件变化

时间	衍变版本	挖矿组件变化
2020.12	版本一	挖矿工具以 gzip 方式内嵌
2020.12	版本二	挖矿工具分离成模块化
2020.12	版本三	挖矿部分不变
2020.12	版本四	挖矿部分不变
2021.02	版本五	重新把挖矿工具以 gzip 内嵌
2021.03	版本六	以 ELF 文件方式内嵌挖矿工具
2021.04	版本七	新增混淆功能
2021.07	版本八	以网络代理方式访问矿池

从其衍变过程可以看出，该恶意程序越发倾向于隐蔽其挖矿模块，不断提高对该恶意程序的追踪难度。这个僵尸网络的威胁不仅仅是增加了受害主机的计算压力和严重的电力消耗，更严重的是，其同时可以充当一个加载器，并安装勒索软件和其他恶意软件，大大加剧了该僵尸网络的潜在威胁。

2.2.3.1.2 组织 TeamTNT

TeamTNT 是一个主要入侵在线容器并通过挖矿和 DDoS 进行牟利的攻击团伙。2021 年年初，该团伙被发现入侵了某 Kubernetes 集群，通过结合脚本和现有工具，最终在容器内植入挖矿木马。

TeamTNT 最初以利用不安全的 Docker 守护进程和部署恶意容器映像而闻名，随着不断地更新和衍变，逐渐地向 Kubernetes 环境作为攻击目标，以扩大其感染范围。

TeamTNT 通过攻破 Kubernetes 集群暴露在公网上的 Kubelet 节点，从而实现对 Kubernetes 的入侵。若 Kubelet 配置不当，接收未经身份验证的请求，导致匿名访问。正是这种允许匿名访问的 Kubelet，成为了攻击者进入到 Kubernetes 集群的内部并进行横向移动渗透的关键跳板。

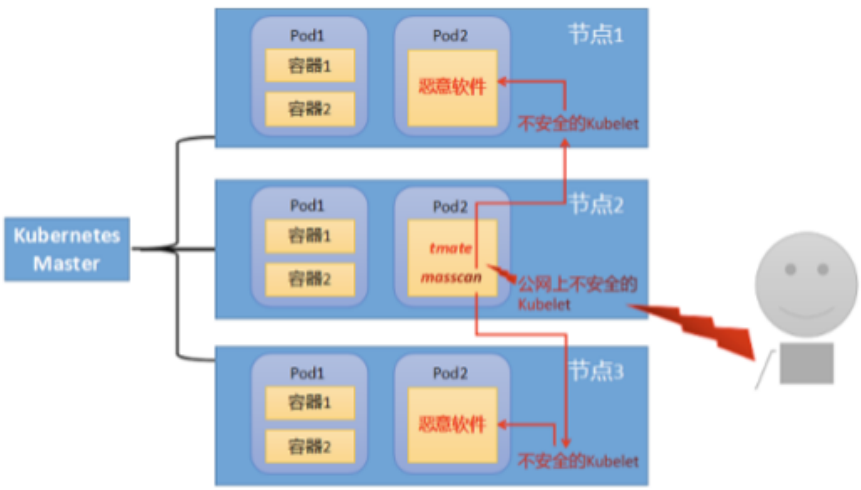


图 2.20 入侵方式

攻击者继续利用弱密码和错误配置来获取云环境中的初始访问权限，对于受害者而言，多个在线容器被植入挖矿木马，或将导致集群内主机资源耗尽，出现崩溃和拒绝服务的情况。因此，做好容器及容器管理组件的安全防范工作显得异常重要。

该恶意软件可以利用 Kubernetes 环境中丰富的计算资源进行加密劫持，并完全可以窃取集群中数以万计个应用程序的敏感数据；除了挖矿功能外，资源劫持和拒绝服务 (DoS) 是该恶意软件最显着的影响，从其丰富的功能模块和攻击目标可以看出，该恶意软件已经发展到武器化阶段。

2.2.3.1.3 H2Miner

H2Miner 是 Linux 下的僵尸网络，其主要目的是在受害主机上运行挖矿工具；它可以通过各种不同的方式入侵主机系统，其中包括 Hadoop yarn 未授权漏洞、Docker 未授权访问漏洞以及 Redis 远程命令执行 (RCE) 漏洞。

攻击者首先会对暴露在公网的 Redis 服务器进行密码暴力破解，一旦入侵成功后，攻击者修改服务器的 red2.so 文件；当 Redis 的主从服务器之间进行同步时，red2.so 文件同时也在服务器之间进行传播，攻击者通过加载此文件，可执行任意指令或发起反向连接

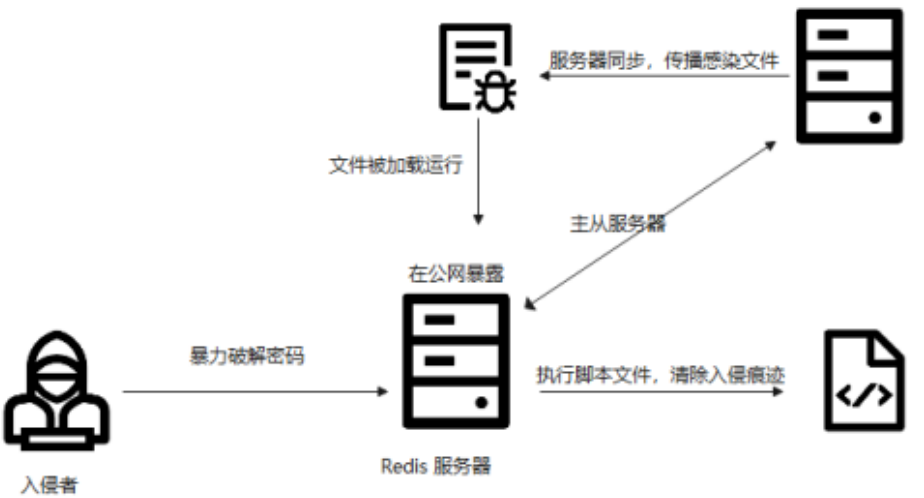


图 2.21 入侵方式

为了避免该恶意软件不断消耗主机系统的计算资源，Redis 组件不应暴露在公网上，并使用强密码进行保护。更为重要的是应定期检查 Redis 路径中是否遗留 red2.so 文件或是否包含名为 kinsing 的进程。

2.2.3.2 窃密木马

窃密木马主要通过邮件传播，通常用报价单、优惠券、求职信、热点事件等作为诱饵。此外，采用供应链攻击的情况也越来越多。2021 年 11 月，研究人员发现一起针对开源软件

仓库 NPM 的供应链攻击[1]，名为”coa”和”rc”的库的多个版本包含恶意程序，用于窃取受害者的口令信息，这 2 个库的累计下载量超过 2000 万次。

一些木马团伙，如 AgentTesla，提供恶意软件即服务（Malware as a service, MaaS），使得网络攻击的门槛更低。

2.2.3.2.1 Trickbot

Trickbot 首次出现在 2016 年，最初是一种银行木马，可窃取网银账号密码、邮件以及主机上的其它信息，常被攻击者用于传播和投放其它恶意软件。自 2021 年 1 月份 Emotet 遭到国际执法部门打击后，Trickbot 木马快速发展，不断增加新功能、新特性。在 2021 年的多个时期，Trickbot 都位居恶意软件榜首。

Trickbot 通常由多层 shellcode 和多个恶意模块组成，使用 shellcode 能够有效躲避安全防护软件的检测，通过大量使用加密和内存加载技术，增加了对其分析和溯源的成本。

Trickbot 不断寻求与其它网络攻击团伙合作。2021 年 10 月，与 Shathak 团伙合作，投放 Conti 勒索软件。Shathak 团伙又名 TA551，其惯用的攻击手法是发送钓鱼邮件，附件为包含恶意宏文档的加密压缩包。恶意宏文档下载执行 TrickBot，TrickBot 再部署勒索软件。

在中断十个月后，Emotet 恶意软件于 11 月中旬卷土重来[2]，通过 Trickbot 发送包含文档或压缩包的垃圾邮件进行传播。Emotet 归来后，必然会发起新的攻击，未来会如何发展，绿盟科技将持续跟踪。

2.2.3.2.2 AgentTesla

AgentTeslat 首次出现在 2014 年， 是典型的间谍类木马，主要功能是窃取各类浏览器中的凭证、各种 FTP 客户端应用中的用户信息、主机键盘记录、窗口程序中文本、并定时对受控端主机进行截屏。主要通过 SMTP 方式上传窃取信息至攻击者，也会通过 HTTP、FTP、Telegram 及 Discord 进行发送。

AgentTesla 提供恶意软件即服务，在一些网站公开售卖，因此本年度长期位于恶意软件排行榜前列。在多个组织的攻击活动中，都会出现 AgentTesla 的身影，常常通过钓鱼邮件进行投放。

[1] https://thehackernews.com/2021/11/two-npm-packages-with-22-million-weekly.html
[2] https://cyber.wtf/2021/11/15/guess-whos-back/

6 月 11 日，绿盟科技伏影实验室捕获到两封携带 cve-2017-11882 漏洞利用载荷的钓鱼文档。两封文档分别伪装成土耳其货运公司 ALATLI 的海关报表以及土耳其制造商 mgt air filters 物流部门相关工作人员的参会表。两封文档使用了类似形式的漏洞利用，会从同一个网络地址下载封装后的 AgentTesla 间谍木马并运行。

图 2.22　钓鱼附件截图

一些攻击者利用 XAMPP 技术搭建供 AgentTesla 访问的基础设施，并申请动态域名，能够在不固定的 IP 搭建 Web 服务。

AgentTesla 使用了更多的代码混淆技术，以躲避安全防护软件的查杀，增加分析成本。

2.2.3.2.3　Formbook

Formbook 是一款窃密木马，自 2016 年开始在多个黑客论坛上售卖。Formbook 主要利用钓鱼邮件进行传播，主要功能是窃取键盘记录，浏览器、Email 和 FTP 的密码，以及其它主机信息，还具有执行命令、下载运行恶意模块、更新、屏幕截图和数据回传等远程控制功能，通过 HTTP、SMTP、FTP、Telegram 及 Discord 等方式发送窃取的信息。

Formbook 的版本不断更新，攻击载荷高度混淆，采用反调试技术，并且使用多个 C2C 服务器，具有很强的对抗分析和反溯源能力，本年度长期位于恶意软件排行榜前列。Formbook 经常与 CVE 漏洞结合使用，早期版本多使用 CVE-2017-0199 和 CVE-2017-11882 等漏洞。

图 2.23　钓鱼邮件截图

2021 年 9 月份，Office365 的 CVE-2021-40444 漏洞公开后，新的 Formbook 变种充分使用 CVE-2021-40444 漏洞进行攻击。

除了攻击 Windows 用户外，Formbook 的新版本 XLoader 具备攻击 macOS 的能力。据信，攻击者可以以 49 美元的月租金租用 XLoader，这将对 macOS 系统的安全性带来很大的威胁。

2.3　高级可持续性威胁

2.3.1　态势总览

2021 年，受地缘政治影响，南亚、东亚和东欧地区依然是 APT 组织最为活跃的地区。根据国内外各大厂商所披露的报告，在发动攻击方面，朝鲜组织 Kimsuky 和 Lazarus 及新出现的东欧 APT 组织 Lorec53 的活跃度排名前列。而海莲花以及摩诃草这类针对中国的 APT 组织亦在活动，情况不容乐观。

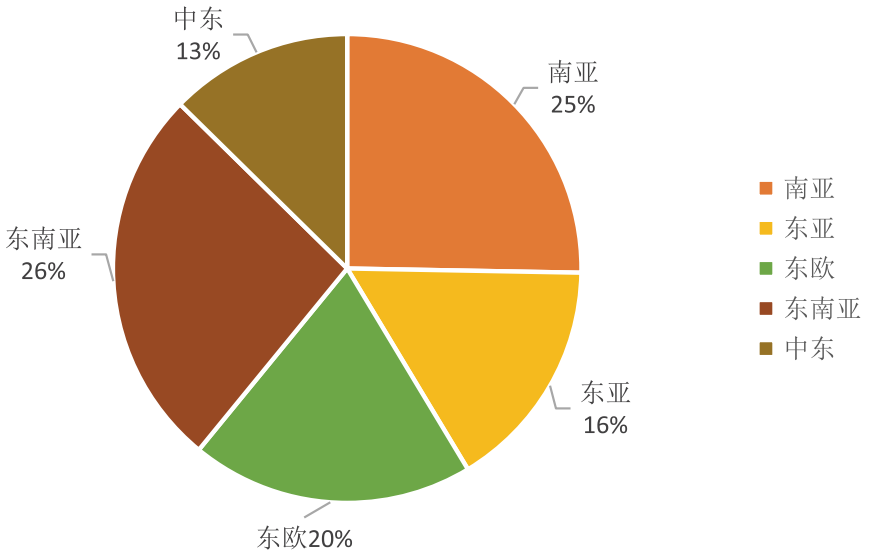


图 2.24　APT 组织所属地区活跃度对比

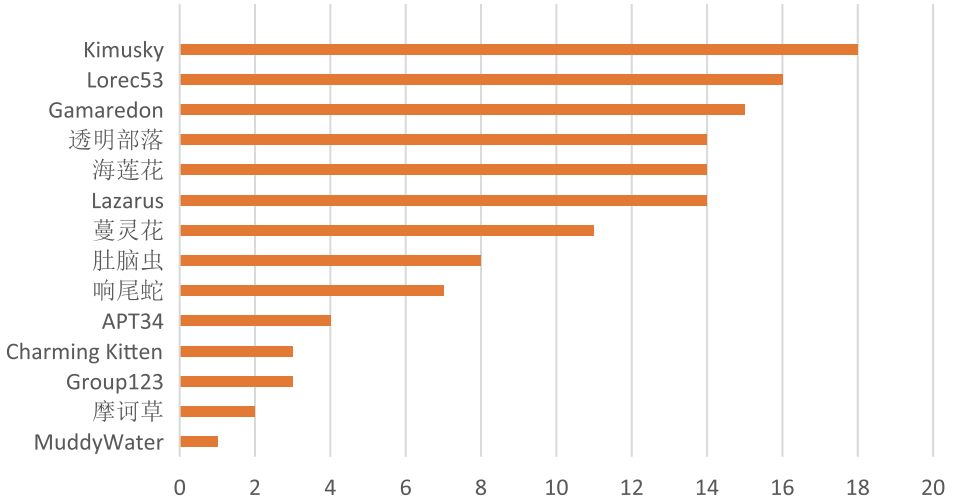


图 2.25　热门 APT 组织攻击事件数量

本年度，绿盟科技伏影实验室追踪发现各国家级 APT 组织的攻击活动依然主要围绕定制化的钓鱼邮件展开，最终通过其中的各类恶意附件文件达成攻击目的。被广泛使用的恶意附件类型包括文档、快捷方式文件、html 文件等。

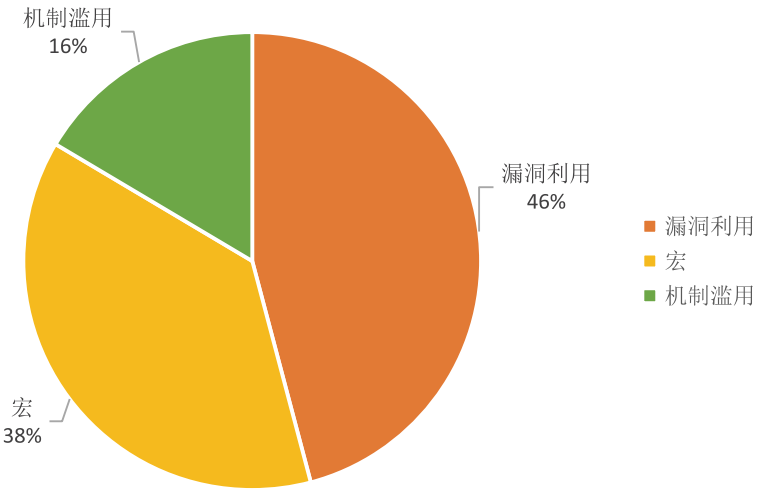


图 2.26　钓鱼文档诱饵攻击类型

经过多年发展，钓鱼文档相关技术已经成熟，恶意宏、漏洞利用、机制滥用等三类常见攻击实现途径。

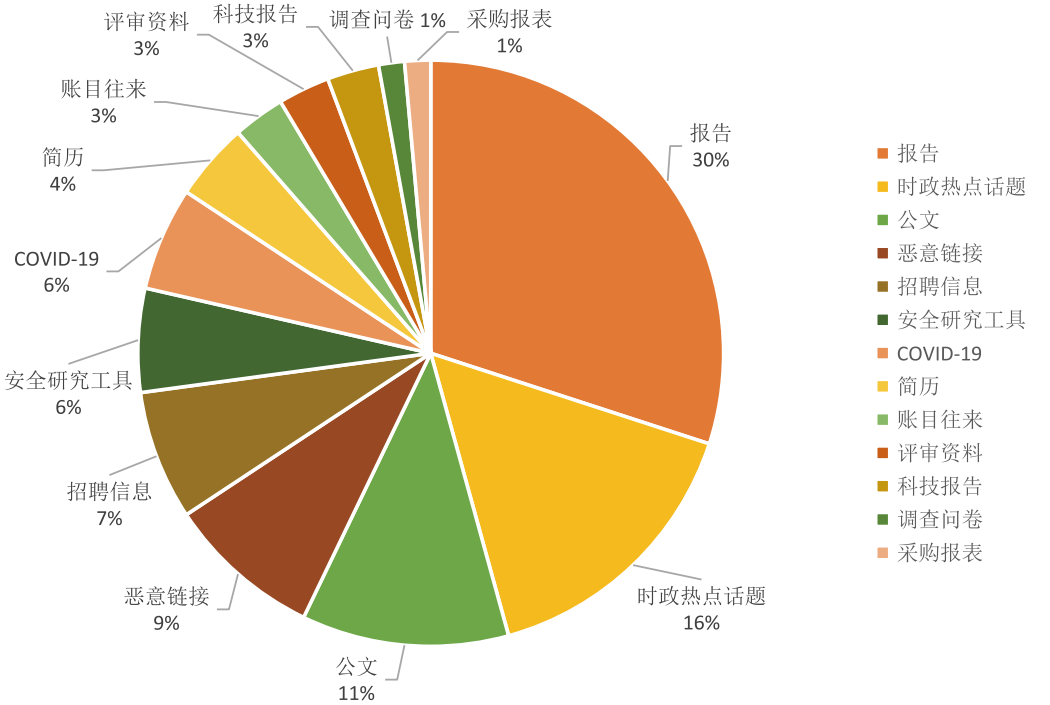


图 2.27　钓鱼诱饵内容分布情况

结合政府公文、报告、简历等数类敏感诱饵内容，再搭配长期发展过程中形成的自动化生成工具，就形成了 APT 组织钟爱的高效且覆盖面广的鱼叉攻击手段。虽然整体而言，钓鱼文档存在易检测、易拦截、易溯源的固有问题，但由于技术门槛较低、投入回报比较高，多个国家级 APT 组织依然依靠恶意文档提供基本面的攻击能力，为更高精度的定向攻击提供情报基础。

表 2.4　本年度通过钓鱼文档进行攻击的主要 APT 组织

归属区域	APT 组织
东欧	APT28、APT29、Gamaredon、FIN7、Lorec53
东亚	Lazarus、Konni、Kimsuky
南亚	Patchwork、SideWinder、SideCopy、Bitter、TransparentTribe、Donot
中东	APT34、Charming Kitten
非洲	SWEED
未确认 / 未知	TA505

恶意快捷方式文件成为 APT 组织在钓鱼文档之外的重要替代选择。由于历史遗留问题，windows 快捷方式文件能够提供扩展名隐藏、图标伪装、cmd 命令执行等多种方便攻击者使用的特性，可以轻易构建具有很强迷惑性的诱饵文件。配合近年来花样繁多的 hta、powershell、JavaScript 等脚本式木马，恶意快捷方式文件可以在无需额外交互的情况下完成提权、下载、展示诱饵信息、运行或注入木马等一系列操作，并且在整个过程中不被受害者感知。APT 组织在使用恶意快捷方式文件时，通常将文件与其他诱饵文件、钓鱼文档、无害文件等一同放入压缩包中，随鱼叉邮件进行投递。本年度，积极使用恶意快捷方式文件的 APT 组织包括 Lazarus、Lorec53、SideWinder 等。

面对邮件审查严格或入口相对封闭的机构或设施，APT 组织通常构建精致的水坑站点进行攻击。本年度，APT 组织常用的水坑诱饵网页包括各国主流邮箱服务的登录页面、常用软件或工具的下载页面、附带下载链接的政府情报公示页面等。广泛使用水坑站点进行攻击的 APT 组织包括毒云藤、Lorec53、Lazarus 等。

在隐匿技术方面，APT 组织通常使用信道加密的手段来躲避网络侧的检测。在 2021 年的 APT 活动监测分析中，APT 攻击组织常使用异或算法加密数据，进行隐匿传输。

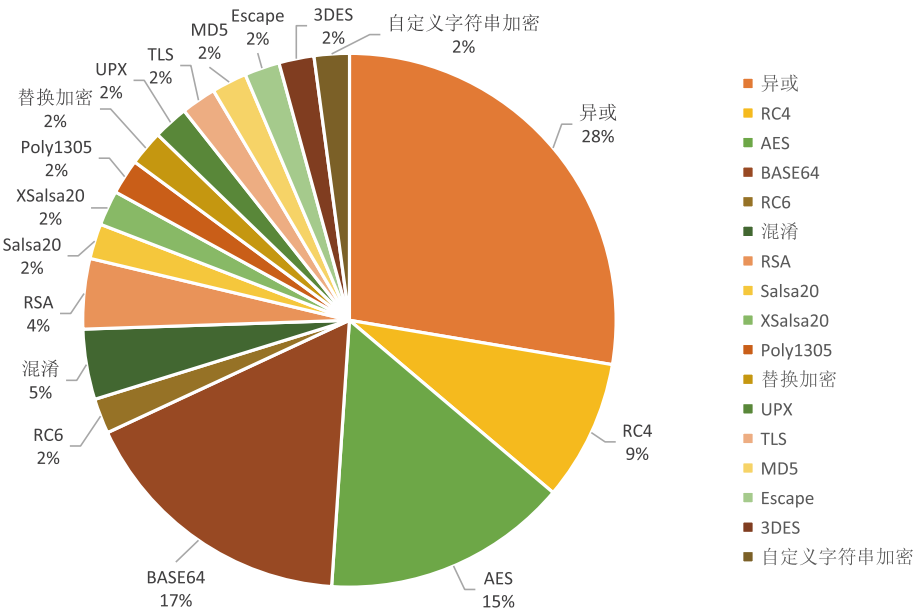


图 2.28　APT 组织使用的加密方法

本年度，APT 组织搭建控制信道时更偏好使用 HTTP 协议，HTTP 协议通信格式松散，可嵌入任意数据，不限制流量大小，通常网络防护设备不会针对该协议进行分析和拦截。另一方面，攻击者传输的行为也能很好地隐藏在正常的网页浏览流量中，降低了检出率。

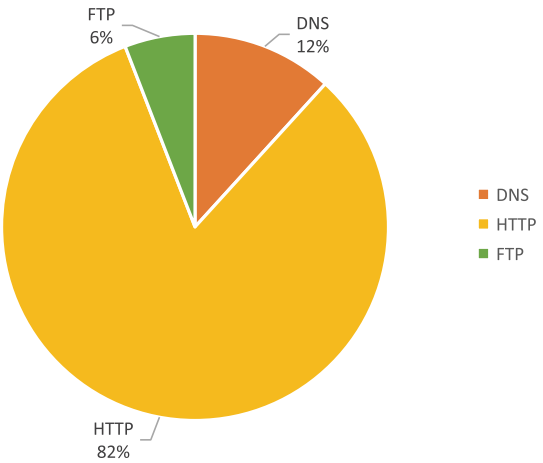


图 2.29　C&C 信道使用的协议类型

目前，国家级 APT 组织，整体上依然以地缘政治上的敌对势力作为主要攻击目标，并重点渗透在当前时段内能够对区域形势产生巨大影响的机构和设施，这些重点目标包括军事设

施、政府部门、法务部门等。同时，由于 COVID-19 疫情的蔓延，APT 组织也开始展开对各国卫生防疫机构的攻击。此外，为满足不断增长的攻击能力需求，APT 组织开始攻击安全研究人员，试图获取 0day 漏洞和渗透工具等，丰富自己的攻击手段。

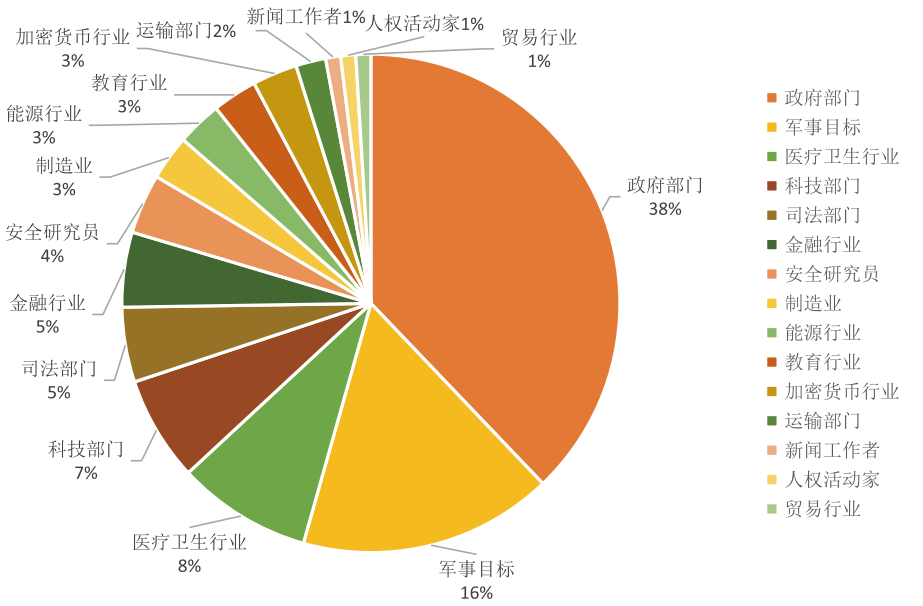


图 2.30　APT 攻击目标占比分析

本年度，绿盟科技伏影实验室通过高级威胁检测系统成功捕获到诸多已知 APT 组织或新兴组织对我国发起的网络攻击活动，对已经对外披露的 APT 组织攻击活动的攻击手法、攻击目标汇总如下表。

表 2.5　本年度针对中国的 APT 组织名称、归属、手法、目标对照表（已公开部分）

组织	归属	攻击手法	本年度主要攻击目标
Patchwork	印度	鱼叉邮件式钓鱼	中国军队
Bitter	印度	鱼叉邮件式钓鱼 水坑站点式钓鱼	中国高级政府部门、地方政府、学术机构
OceanLotus	越南	鱼叉邮件式钓鱼 基于字典爆破和漏洞扫描的渗透攻击	中国高级政府部门、疫情防疫相关部门、重点企业
Lazarus	朝鲜	鱼叉邮件式钓鱼 水坑站点式钓鱼 社交媒体钓鱼	国内安全研究人员
毒云藤	台湾	水坑站点式钓鱼	中国军队、高级政府部门、高校与研究机构
ARTEAM	未确认	鱼叉邮件式钓鱼	港澳台执法部门

针对我国的攻击活动数量与当前国际形势密切相关。本年度，各印度 APT 组织明显加强了对我国军队的网络攻击强度，企图通过此类间谍活动增加影响边境局势的筹码。印度 APT 组织在本年度的攻击活动中使用了大量与中巴两国利益相关的文档类诱饵，能够体现攻击者在相关领域的积累的深度。

随着国内近年来在网络安全领域的高速发展，持续积累的安全研究资产成为境外 APT 攻击者的新目标。为获取我国安全研究人员的工作成果，Lazarus 组织在 2020 年年底到 2021 年年初的一段时间内策划了利用社交媒体的钓鱼攻击活动，意图通过有针对性的社会工程学手段，获取国内安全研究人员掌握的未公开漏洞或攻击工具等资产。

由上述表格还可以看出，针对我国的 APT 组织对水坑站点式钓鱼攻击有一定的依赖度。以毒云藤、Bitter 为代表，攻击我国的 APT 组织通常会在短时间内制作大量水坑站点，伪装成 163 邮箱、126 邮箱、QQ 邮箱等国内主流的邮箱登录页面或政府部门的内网邮箱登录页面，窃取受害者的邮箱凭证和邮箱内容。

2.3.2 战术变化

本年度高级可持续性威胁的发展变化趋势中，针对安全研究人员和供应链的攻击需要引起关注。

2.3.2.1 社交工程的强化

2021 年，由于攻击目标的变化，导致某些 APT 组织在诱饵种类和社交工程等方面均发生变化。

攻击目标方面，国外的网络安全从业人员进入到 Lazarus 的攻击视野中。这主要是为了取长补短，窃取对方掌握的安全技术，有别于传统的基于政治经济因素的窃密。

诱饵种类方面，也随着攻击目标的变化而发生变化。传统的 APT 钓鱼攻击，其目标多为政府、军事、工业、能源机构以及学术团体，缺乏安全意识，因此诱饵多采用钓鱼邮件配以恶意文档的方式。而当网安人员成为攻击目标时，安全 / 开发工具对其则更具吸引力，如携带后门的 VS 工程和逆向软件等。

社交工程手法方面，传统的主要方法是获取目标的个人以及单位 / 公司的背景信息，以此制作出高度定向且本地化的钓鱼邮件。但这种手段因为安全研究人员而失效，所以攻击者改变攻击手段，花费了更长的时间来进行“自我价值”展示，以此获取目标的信任，充分体现了该组织因地制宜的特点。

此外，即便是针对非安全研究人员，攻击者也会花费精力与其进行更多交互。例如中东组织 Charming Kitten 组织通过多次与目标进行讨论来获取信任。这在某种程度上也显示了，传统的“一步式”钓鱼邮件对特定群体来说具有突兀感，会令人生疑，因此更深层次的交流显得必不可少。

2.3.2.2 供应链之痛

供应链攻击，可通过攻击上游机构来获取进入下游机构的通道，并达成一石多鸟的效果。

2020 年年末始，被称之为 UNC2452 的黑客组织攻击 SolarWinds 公司的供应链，并波及超过 18,000 家企业，影响范围大，造成了严重损失。攻击者入侵了 SolarWinds 公司的服务器并在关键产品中添加恶意代码，并通过该产品的更新，将后门植入到相关客户企业的设备中。当后门启动时，采取多种手段进行隐藏以对抗安全检测。

该事件发生在供应链安全中最为关键的开发环节，暴露出开发团队只关注程序正常运行问题，而忽视了对自身文件的完整性校验。由于缺失检测源码与最终可执行文件匹配度的手段，开发团队将无力察觉自身代码遭到注入，进而带来隐患。

本年度另一起供应链事件由 Lazarus 制造。与 SolarWinds 事件不同，该事件发生在供应链安全的渠道分发环节，即替换正常的工具。

当前，各类机构的 IT 产品都不再是完全自生自造，都或多或少依赖开源方案或其他公司的基础产品。这导致当今的软件生态越来越复杂，蕴含的安全风险也与日俱增。相比软件公司开发的产品，由个人和组织提供的开源方案更加缺少安全约束，更容易成为供应链攻击的目标。即便攻击者真正的目标只是下游机构中的少数，也会因为软件的分发而波及到其他无辜单位，从而扩大攻击面。

2.3.3 攻击区域

2.3.3.1 东欧 / 前独联体区域

Lorec53 组织是由绿盟科技伏影实验室在 2021 年度发现和披露的新的 APT 组织 [1]，主要针对乌克兰和格鲁吉亚的政府部门。该组织借鉴了 Gamaredon、Lazarus 的常用手法，其能力绝非新手范围，说明其身份可能是受到更高势力雇佣的民间攻击团体。

Gamaredon 是俄罗斯组织，至少从 2013 年开始活动，2021 年持续对乌克兰和部分俄语群体大量钓鱼攻击。Gamaredon 使用的诱饵话题多为俄乌周边的政治军事经济有关，并取材

[1] http://blog.nsfocus.net/lorec-53/

自乌政府各部分的文件。在攻击方面，Gamaredon 采用短时间内大量活动的策略，往往使得目标难以进行有效响应。

2.3.3.2 朝鲜半岛

Kimsuky 是朝鲜 APT 组织[1]，主要攻击韩国政府及韩美两国研究政治的学术团体，非常善于利用东北亚地缘政治话题制作诱饵。本年度 Kimsuky 全年活跃，攻击手法依然以投递钓鱼邮件为主，最终执行多种恶意自制组件进行窃密，同时也在个别事件中辅以钓鱼网站以获取目标账号。此外，Kimsuky 在本年度攻击中使用了修改自其 Windows 后门的 Android 版，并增加了对 PDF 漏洞的利用，扩充了其武器库。但总体而言，该组织的攻击方式没有发生显著变化。

Lazarus 同为朝鲜 APT 组织，针对韩国、中国及多个亚洲国家，非常活跃。该组织本年度持续对自身的攻击组件进行变形升级，在开发上保持对目标的威胁能力，并在攻击上另辟蹊径，主导了年初针对安全研究人员的大型间谍活动，以窃取最新漏洞利用方法。为了获取目标信任，Lazarus 采用了交互性更强的手段。该组织将自身伪造成安全从业人员，融入社交媒体，花费数月时间与其他安全人员展开接触，并搭建了以假乱真的技术博客并发布文章，逐步构建信任。待时机成熟时，Lazarus 便上传携带后门的工具供下载，达成了钓鱼攻击。同时，Lazarus 还“技术金钱一起抓”，对区块链行业进行了攻击，以获得经济利益。此外，Lazarus 还发起供应链攻击，入侵了韩国某些使用特定安全管理软件的网站，替换了其提供下载的软件，而由于安全管理软件在下载软件时的验证过程存在漏洞，导致用户安装了恶意后门；而在另一起事件中，Lazarus 用窃取的证书为后门签名，并部署在拉脱维亚某公司的网络内部，以此实施攻击。

而另一个同样擅长鱼叉攻击的朝鲜 APT 组织 Group123，其活跃度不及 Kimsuky 和 Lazarus。该组织另寻他路，将重点放对俄罗斯方面，开辟了新的“战线”。

2.3.3.3 南亚

印巴、中印问题争端不断，带动了这一区域 APT 组织进行活动。

透明部落（Transparent Tribe）是巴基斯坦 APT 组织[2]，主要使用钓鱼攻击，以及诱导目标下载 Android 后门。该组织本年度活动频繁，主要针对的目标包括印度陆军、印度国防部和医疗行业等部门。

[1] http://blog.nsfocus.net/apt-kimsuky/
[2] http://blog.nsfocus.net/transparent-tribe-activity-analysis-of-usbworm/

与巴基斯坦毗邻的印度有多个 APT 组织，长期向周边邻国发动攻击进行窃密活动，目标包括中国、巴基斯坦和尼泊尔，甚至还包括个别东南亚国家。在中印争端升级的情况下，印方不断炒作“中国网络威胁”，实为掩盖自己的攻击活动。

摩诃草是印度 APT 组织，主要针对中国和巴基斯坦的政府军工单位。该组织本年度曾利用 office 解析 esp 的漏洞，对中国发起钓鱼攻击，而这种利用 esp 漏洞的攻击方式多见于朝鲜 APT 组织针对韩国的事件中。

肚脑虫（Donot）同为印度 APT 组织，在本年度喜欢使用 rtf 文档进行攻击。该组织在利用公式编辑器漏洞上增加了一层保护，将带有漏洞的文档设置为模板放在远程服务器上，通过钓鱼 rtf 文档获取并加载。由于 rtf 文档可进行混淆用于对抗静态查杀，因此屡次出现在钓鱼攻击中。

另一个印度组织蔓灵花（Bitter）也是长期针对中国发动攻击。本年度该组织在诱饵类型使用上，除了 office 文档，蔓灵花还使用了 chm 类型的钓鱼文件，通过执行其中的恶意脚本下载后续组件。Chm 文档在中国有着一定流行度，为电子书发烧友常用，因此存在被钓鱼利用的风险。

2.3.3.4 东南亚

东南亚地区 APT 组织海莲花 [1]，是一个具有越南政府背景的境外黑客组织。长期以来针对中国及其他东亚政府部门和企业进行攻击。已披露的海莲花攻击事件中，大多使用侧加载攻击的方式，利用各种正规的应用程序，例如 Office 程序、各类国产软件组件等，加载和执行恶意载荷。2021 年海莲花仍然利用侧载攻击的手法，并对利用过程进行改进，通过下发的白文件替换服务、任务计划等涉及的目标可执行文件，实现侧载攻击和系统驻留。

2.3.3.5 中东

MuddyWater，伊朗 APT 组织，历来以中东各个国家为目标。2021 年初，该组织就利用鱼叉钓鱼邮件，以针对阿联酋、沙特、以色列和阿塞拜疆境内的政府机构文件为诱饵，发动对中东家的钓鱼攻击，传播合法的远程管理工具 ScreenConnect。

APT34，也是伊朗 APT 组织，主要针对中东各国和英语国家，善于采用通信隐匿技术来规避检测和追踪，本年度使用新木马 SideTwist 发动针对黎巴嫩目标的攻击活动，SideTwist 木马将通信数据以注释形式隐藏于 html 文本的 javascript 标签中，有极强的规避效果。

[1] http://blog.nsfocus.net/msmpeng-oceanlotus-0807/

Charming Kitten，伊朗 APT，善于使用鱼叉式钓鱼攻击投放定制的恶意软件，既往攻击活动以政府，国防技术，军事和外交部门为目标，本年度进行了针对医学专家的高级渗透攻击活动，这也代表着该组织在攻击目标上的转变。根据披露，Charming Kitten 在上半年冒充中东事务研究人员，以攻击在英国的同样研究中东事务的学者。为了获取信任，Charming Kitten 窃取了其他教授的姓名和泄露的电子邮箱来与目标进行对话。对话过程来来回回，经历多次讨论，直到目标有意参与如在线会议这样的活动，届时 Charming Kitten 则会推送伪造的注册页面，达成攻击。

2.4 IPv6 安全威胁

2021 年绿盟科技威胁情报中心通过对百余家国内单位的攻击告警数据进行分析，观察国内 IPv6 环境下的单位面临的威胁状况。

2.4.1 IPv6 漏洞

自 2002 年至今，CVE 公布的 IPv6 漏洞累计 507 个，2010 年后，IPv6 相关漏洞大幅增长，尤其在 2017 年和 2020 年涨幅较大，分别存在 74 个和 90 个 IPv6 相关漏洞，其中，高危漏洞占比较高。

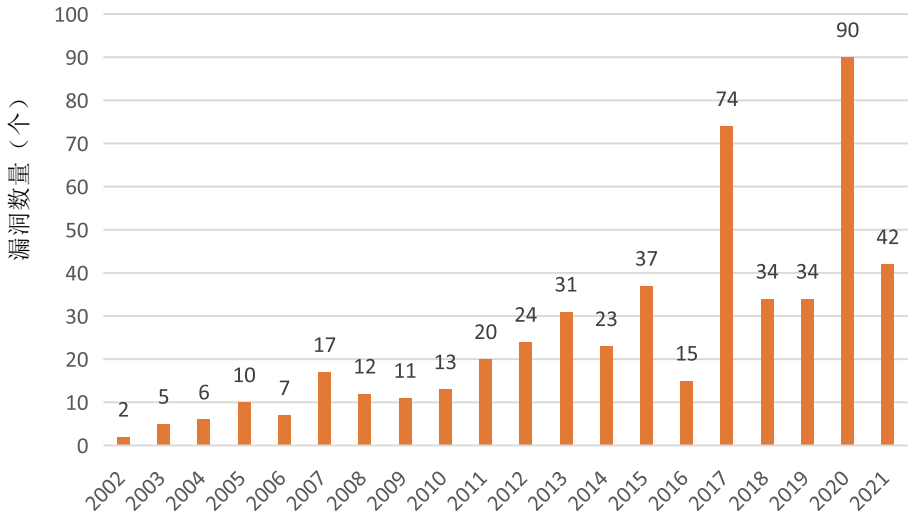


图 2.31　2002 年到 2021 年 IPv6 相关漏洞统计

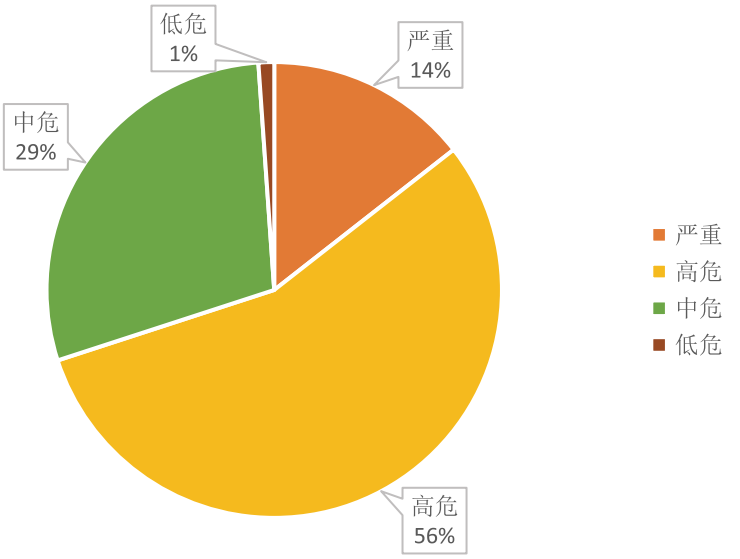


图 2.32　2020 年 IPv6 安全漏洞等级分布

2.4.2　攻击源

针对 2021 年国内百余家单位遭受攻击的告警进行分析，其中攻击来源国外的有 52,707 个，较 2020 年增加了 352.4%，来自国内的攻击源有 27,970 个，较 2020 年减少了 68.8%。

从观察的情况看，中国企业面临来自境外的攻击占比约 65%、来自中国地区的攻击占比约 35%，与 2020 年不同，2021 年来源境外的攻击成为了 IPv6 网络环境国内企业面临的主要威胁来源。

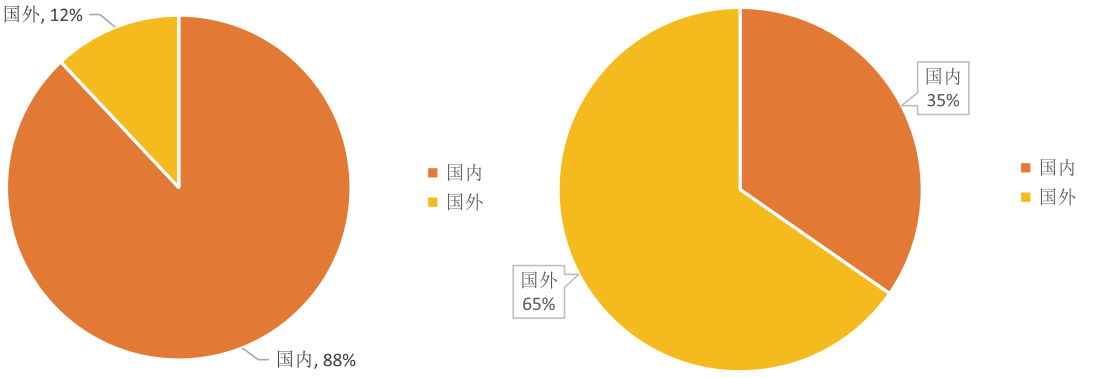


图 2.33　2020 年及 2021 年 IPv6 攻击源地域分布（右为 2021 年）

2.4.2.1 国外

针对攻击源位于国外的攻击事件进行分析，具体分布情况如图 2.34 所示，在攻击告警中占比最多的是美国，占比 86.26%，其次是巴西、俄罗斯和德国，分别占比 4.41%、1.93% 和 1.60%。与 2020 年相同的是，来源国外的攻击当中，美国仍占了大多数，不同的是，来源德国的攻击数量大幅减少。

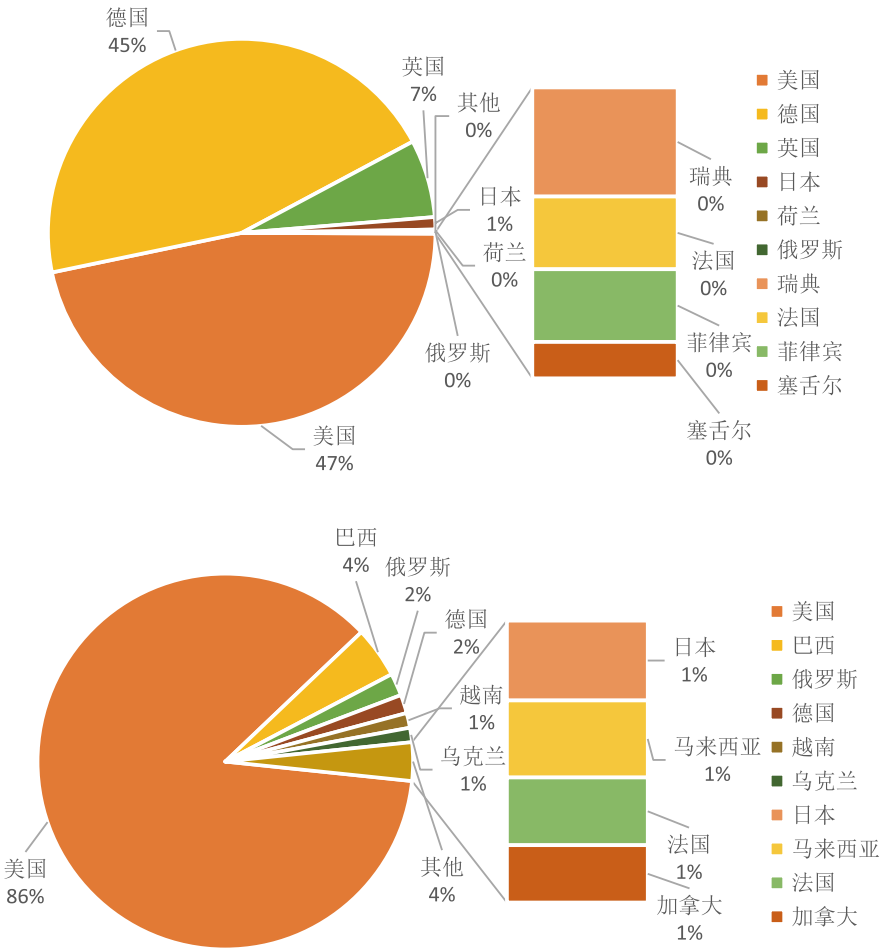


图 2.34　2020 年及 2021 年来源境外攻击地理分布 TOP10（下为 2021 年）

对境外攻击源进一步分析，可以发现僵木蠕是境外来源的攻击事件中常用的攻击方式，如表 2.6 所示。

表 2.6　来源境外 TOP10 攻击事件

攻击名称	数量
挖矿蠕虫 WannaMine 连接 DNS 服务器通信	10376
恶意程序 windows/Ramnit_a 网络通信	8517
挖矿程序查询 DNS 矿池服务器域名	6112
驱动人生下载器木马恶意域名 DNS 查询	1006
PHP 代码执行漏洞	634
可疑 Webshell 脚本文件上传行为	560
恶意程序 windows/PowerGhost_a 网络通信	527
木马后门程序 Chopper Webshell 检测	506
Discuz!X /utility/convert/index.php 远程代码执行漏洞	504
FCKEditor ‘FileUpload()’ 函数任意文件上传漏洞	441

2.4.2.2　国内

针对攻击源位于国内的攻击事件进行分析，具体分布如图 2.35 所示，在攻击告警数量排名 TOP3 的省市是山东省、浙江省和上海市。

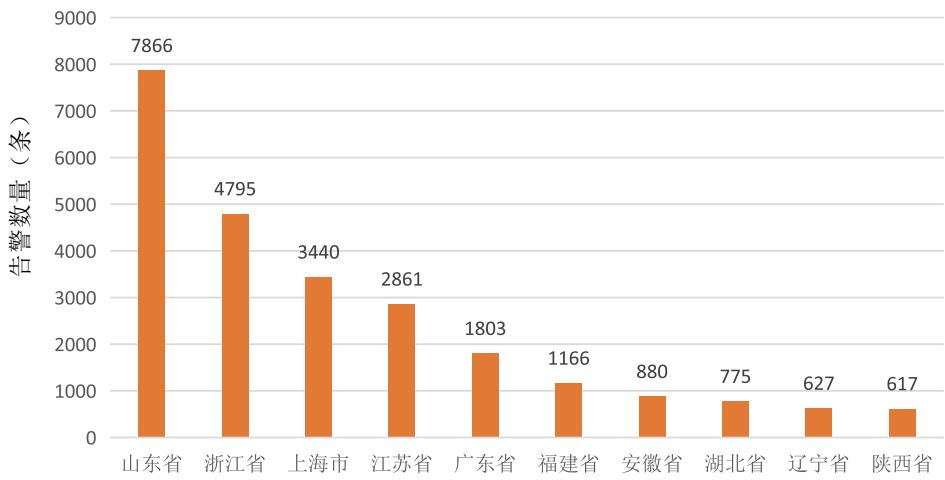


图 2.35　来源国内攻击地理分布 TOP10

针对攻击源是国内的 IPv6 地址发现，来自国内的攻击源将攻击目标更多的瞄准网站服务，同时国内攻击源还较多的使用安全漏洞进行攻击。相比来自境外的攻击，来自国内的攻击方式更复杂。

表 2.7　来源国内 TOP10 攻击事件

攻击名称	数量
ACK-Flood 拒绝服务攻击	7098
PHP 代码执行漏洞	3233
远程控制工具 TeamViewer 连接	2311
HTTP 请求敏感路径访问尝试	2103
HTTP 服务目录遍历漏洞	1555
驱动人生下载器木马恶意域名 DNS 查询	936
HTTP 请求 uri/referer 字段目录遍历	824
服务器端口扫描－ SYNACK 扫描	743
Apache Shiro 身份验证绕过漏洞 (CVE-2020-11989)	687
勒索病毒 WannaCry 尝试通信	432

2.4.3　攻击类型

在 2021 年 IPv6 网络攻击中，从恶意 IP 的攻击类型来看，各攻击类型分布如图 2.36 所示，排名在前三是 Web 攻击、漏洞利用和扫描，分别占比 42.2%、29.3% 和 13.6%。

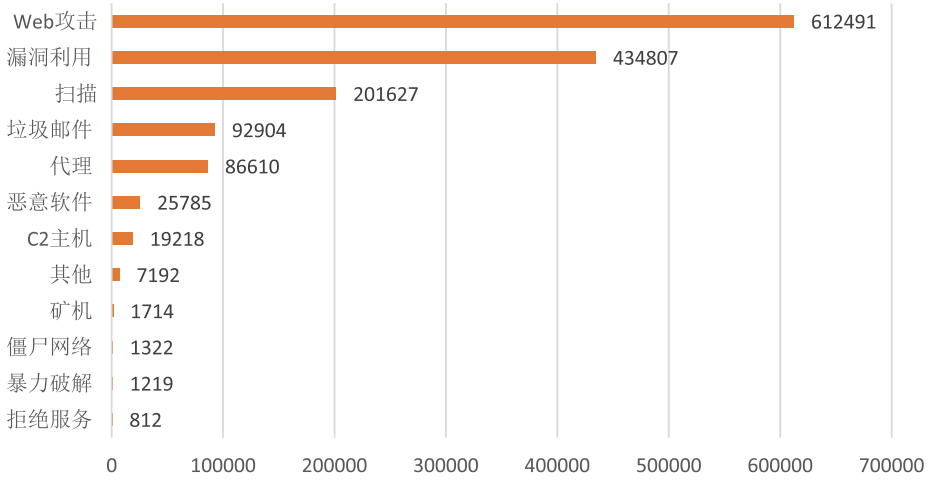


图 2.36　攻击类型分布

2.4.4　受威胁行业

2021 年，通过对国内 IPv6 环境下的教育、能源、金融和交通等多个单位攻击数据进行分析和统计，观察不同行业被攻击的情况如图 2.37 所示。

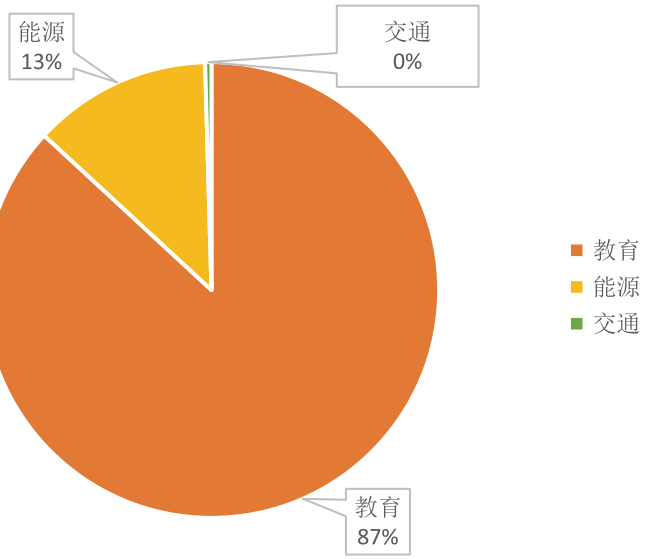


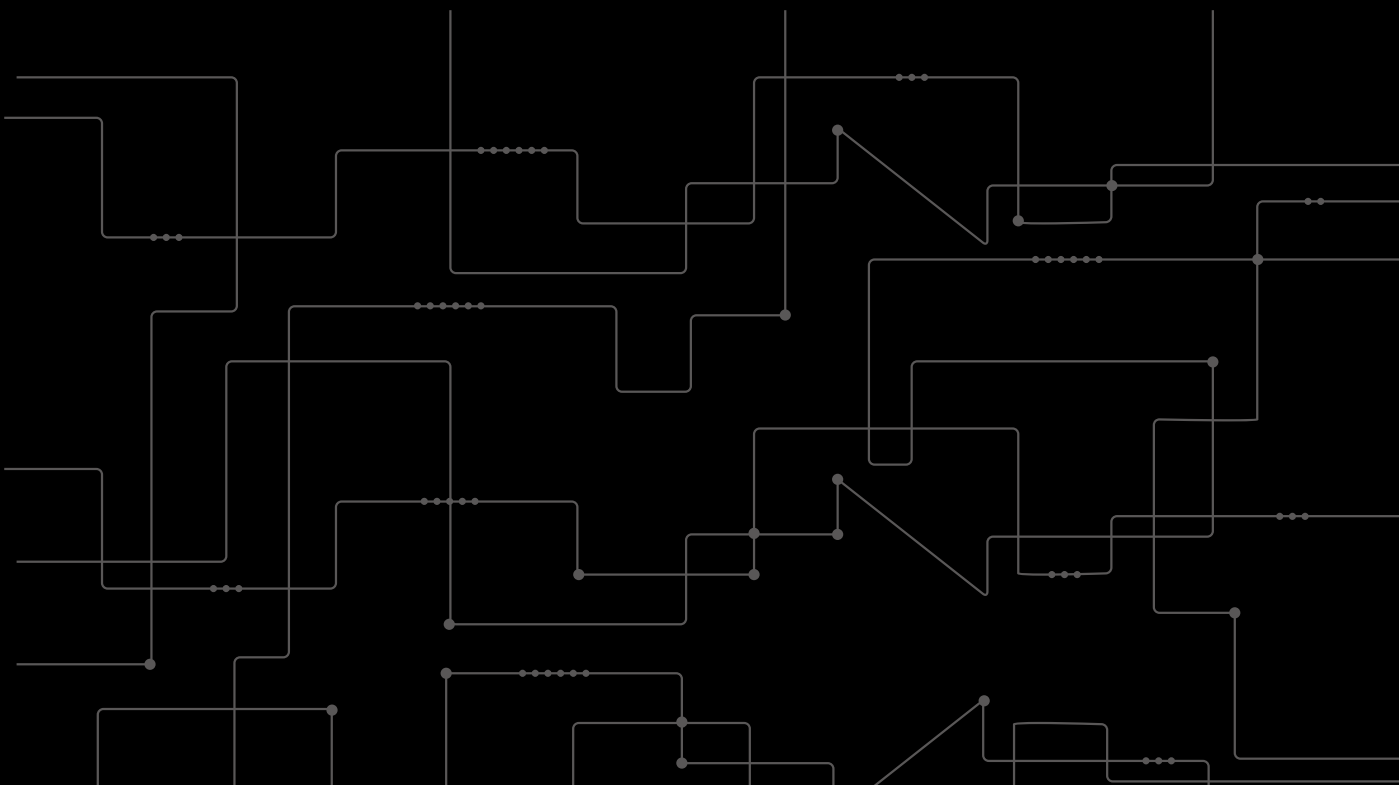
图 2.37　不同行业被攻击统计

从遭受攻击数量上看，排名第一的是教育行业，占比高达 86.9%，其次是能源行业和交通行业，分别占比 12.6% 和 0.4%

从观察结果来看，教育行业依旧是遭受攻击的重点行业，尤其是各大院校，IPv6 建设走在全国行业前列，IPv6 应用成熟度较高，成为攻击者的重点攻击目标。接下来是能源和交通行业，也遭受了不同程度的 IPv6 攻击，这主要是由于 IPv6 庞大的地址空间优势，在物联网、工业互联网等行业中得到广泛的应用，但是也逐渐成为了攻击者的重点攻击目标之一。

3

数字基础设施篇



3.1 数据安全

2021 年，我国《数据安全法》和《个人信息保护法》两部重要的数据安全相关法律相继正式实施，这标志我国数据安全领域进入强监管时代。满足合规性已经成为企业数据安全建设重要驱动力。本章节从热点数据安全事件、数据安全立法和执法事件以及数据安全发展趋势三个维度展开介绍。

3.1.1 热点安全事件

3.1.1.1 全球重大数据泄露事件

绿盟科技收集了 2021 全球数据大规模数据泄露的代表性事件，一共有 10 起，如表 3.1 所示。从泄露规模上看，上亿级别的数据记录泄露有 8 起，最高泄露 7 亿条。从泄露原因上看，互联网暴露和配置错误、黑客攻击是造成大规模数据泄露的主要原因。例如事件 1 和事件 5 均是黑客攻击后获取数据并在暗网或黑客论坛进行售卖；而剩下的事件中，除了事件 4 外，其他均是互联网暴露与配置错误，安全意识培训和基本的配置检查不可忽视。

表 3.1 2021 年国内外大规模数据泄露事件收录（按泄漏规模排序）

事件	时间	规模	事件描述	原因
1	2021 年 7 月	7 亿	美国 LinkedIn 公司 7 亿多条用户信息在论坛 RaidForums 被黑客出售 [1]	黑客攻击
2	2021 年 4 月	5.3 亿	美国 Facebook 公司有超 5.3 亿条用户数据在一个黑客论坛公开 [2]	互联网暴露与配置错误
3	2021 年 1 月	3.18 亿	国内 Socialarks 公司被曝泄露了 400GB 数据，涉及 3.18 亿条用户记录 [3]	互联网暴露与配置错误
4	2021 年 1 月	2.23 亿	巴西官方数据库遭到重大泄露，受影响人员 2.2 亿，几乎为所有巴西公民 [4]	未知原因
5	2021 年 1 月	2 亿	Cyble 的研究团队发现黑客在暗网出售 2 亿多中国公民的信息，包括 QQ 和微博的信息 [5]	黑客攻击
6	2021 年 9 月	1.4 亿	美国 Firebase 的数据库配置错误，导致 iOS / Android 应用程序泄露了超过 1.4 亿条信息 [6]	互联网暴露与配置错误
7	2021 年 8 月	1.26 亿	美国 OneMorelead 营销公司发生数据泄露，涉及 1.26 亿美国公民的信息 [7]	互联网暴露与配置错误
8	2021 年 8 月	1.06 亿	泰国游客的 ES 数据库暴露，泄露数据涉及 1.06 亿游客的个人信息 [8]	互联网暴露与配置错误
9	2021 年 8 月	3800 万	美国微软云平台暴露 3800 万条客户数据，涉及多个 COVID-19 接触者追踪平台等存储的敏感数据 [9]	互联网暴露与配置错误
10	2021 年 1 月	800 万	印度多个政府网站发生数据泄露，涉及 800 万 COVID-19 患者检测报告 [10]	互联网暴露与配置错误

[1] https://threatpost.com/data-700m-linkedin-users-cyber-underground/167362/
[2] https://www.identityforce.com/blog/533-million-facebook-users-data-leaked-online
[3] https://www.safetydetectives.com/blog/socialarks-leak-report/
[4] https://www.internetgovernancehub.blog/2021/02/06/the-largest-personal-data-leakage-in-brazilian-history/
[5] https://securityaffairs.co/wordpress/112966/deep-web/chinese-citizens-data-darkweb.html
[6] https://cybernews.com/security/research-popular-android-apps-with-142-5-million-collective-downloadsare-leaking-user-data/
[7] https://www.technadu.com/yet-another-massive-data-leak-marketing-company-exposes-126-million-us-citizens/293328/
[8] https://www.infosecurity-magazine.com/news/data-of-106-million-visitors-to/
[9] https://new.qq.com/omn/20210824/20210824A02DHP00.html
[10] https://www.bleepingcomputer.com/news/security/over-8-million-covid-19-test-results-leaked-online/

根据 IBM 发布的《2021 数据泄露成本报告》[1]，企业数据泄露平均成本为 424 万美元。数据安全事件导致的经济损失居高不下。为了降低数据泄露风险，企业可从以下各个方面进行改进和优化：

(1) 定期开展安全意识培训，提高员工对数据安全风险的认知和感知；

(2) 梳理重要数据服务器与资产，围绕数据资产开展安全防护措施，比如定期进行漏洞扫描与配置检查、更新软件补丁、身份权限管控、部署数据库防火墙等安全措施；

(3) 敏感数据进行全生命的安全防护，比如采取敏感数据发现、分类分级、数据脱敏与效果评估、数据加密、隐私计算等安全措施。

3.1.1.2 源代码泄露事件

源代码泄露是信息泄露中最常见并且后果最严重的事件之一。源代码泄露不仅会造成用户信息、网站资源等泄露影响企业竞争力，还容易降低攻击者对目标系统的攻击难度（黑客通过源代码级的研究更容易入侵客户系统造成更大的损失）。经绿盟威胁情报中心统计，2021 年涉及国内政府和企事业单位的源代码泄露事件中，源代码泄露事件的行业分布如图 3.1 所示，金融行业位居首位，占比 44%，其次是政府和能源行业，分别占比 27% 和 9%。这些泄露代码对组织和机构造成持续性威胁，攻击者可能利用泄露的源代码分析发现漏洞，对系统安全进行渗透，上传恶意程序获取访问权限，从而窃取关键敏感信息，或进行勒索攻击，这些威胁隐患都将给组织带去不可预计的损失。

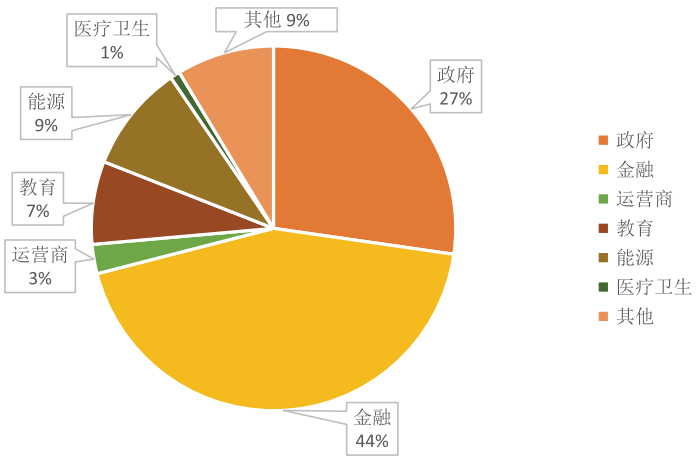


图 3.1 源代码泄露事件行业分布

[1] https://www.ibm.com/cn-zh/security/data-breach

根据源代码泄露事件中泄露代码类型和受影响程度，将事件分为高中低三个风险等级。其中高风险泄露事件包括泄露账号密码、业务代码、服务器秘钥等，中风险泄露事件包括泄露 API 调用接口、配置文件、网络拓扑地址、证书、组织业务资料等；低风险泄露事件包括泄露公司邮箱账号、前端代码等。可以看出，无论哪个等级的泄露事件，均可能被攻击者利用，进行进一步的攻击活动。经统计分析，高风险源代码泄露事件占比最多，高达 78%，其次是中风险泄露事件（17%）和低风险泄露事件（5%）。

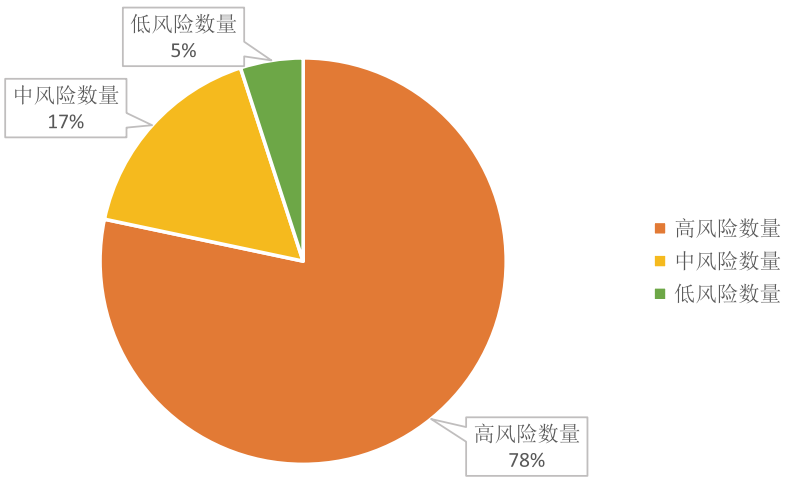


图 3.2　源代码泄露事件风险等级分布

3.1.1.3　暗网数据泄露事件

近几年，暗网作为数据泄露的主要途径之一以及暗网相关的网络犯罪活动频频发生，引起了国家相关部门的注意。经绿盟威胁情报中心统计，2021 年暗网数据泄露事件中，从地理分布来看，东部沿海地区数据泄露较为严重。在经济发展程度越高的地区，数据流转、共享和应用业务更加活跃，数据发生暴露和泄露风险更大。因此，做好数据安全风险监测、安全防护相关管理和技术措施不可或缺。

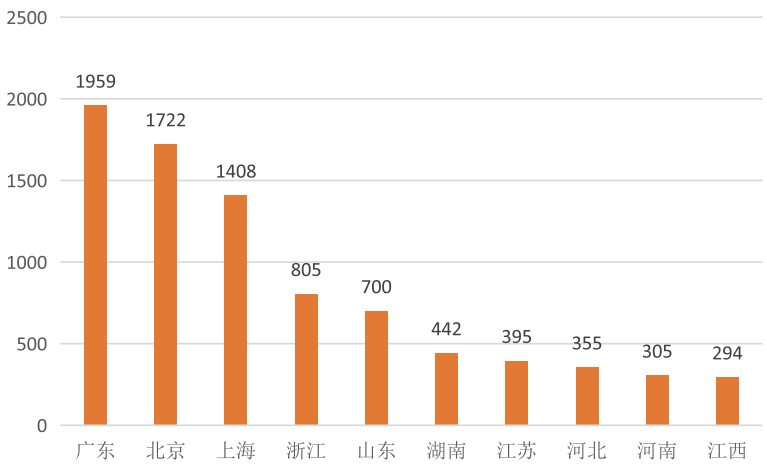


图 3.3　暗网数据泄露事件地理分布

3.1.2　政策和市场

3.1.2.1　国外现状

根据联合国贸易发展组织（UNCTAD）截至 2021 年 11 月 26 日统计[1]，全球 77% 个国家（共 194 个国家）完成了数据数据安全和隐私立法或者已经提出法律草案。其中包括欧盟、美国、中国、俄罗斯和印度和澳大利亚、加拿大和日本等绝大数国家。随着数字化转型的不断推进与深入，数据安全与隐私问题越来越严峻，现代化的数据安全与隐私保护立法已成为全球趋势。

根据 GDPR 的执法跟踪网站相关统计[2]，截至 2021 年 11 月 26 日，欧盟成员国在 2021 年共开出 362 件罚单，而 2018 年至 2020 年三年仅有 491 件；此外，2021 年 GDPR 罚单的总金额高达约为 10.6 亿欧元，而过去三年的罚款总额仅为 2.4 亿欧元，相当于是以往三年的 4.42 倍。由此可见，欧盟已经进入全面和严格的 GDPR 执法阶段。

根据执法跟踪网站相关统计[3]，绿盟科技整理了历史上 GDPR 单次罚款事件金额最高的前十名，如表 3.2 和图 3.4 所示。可以看出，世界三家巨头数字企业亚马逊、Facebook、谷歌均被高额罚款。其中，亚马逊和 WhatsApp（Facebook 收购）在 2021 被处罚，金额达到了 9.71 亿欧元。处罚力度之大，可见一斑。如图 3.5 和 3.6 所示，从罚款企业的所属行业来看，

[1] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[2] https://www.enforcementtracker.com/
[3] https://www.enforcementtracker.com/

媒体、电信和广播行业已经成为重灾区，这与该行业的大型平台企业存储大量的个人隐私数据，同时有丰富的面向用户（2C）的业务有关；从罚款的具体原因来看，数据处理的法律依据不足是主要的原因，比如 Cooike 信息的采集与处理，以及与第三方共享个人隐私数据；此外，违反数据处理的一般原则也是重要原因，包括透明性、最小化、用户同意等各项原则。

表 3.2　GDPR 单次罚款事件金额最高的前十名 [1]（截止日期当前 2021.12.01）

	企业组织	所示行业	罚款国家	罚款金额	日期	处罚主要原因
1	亚马逊	工商业	卢森堡	7.46 亿	2021 年 07 月	违反数据处理的一般原则
2	WhatsApp（Facebook收购）	媒体、电信和广播	爱尔兰	2.25 亿	2021 年 09 月	未能充分履行通知义务
3	谷歌	媒体、电信和广播	法国	5000 万	2019 年 01 月	数据处理的法律依据不足
4	H&M 在线商店	就业	德国	约 3525.9 万	2020 年 10 月	数据处理的法律依据不足
5	意大利电信移动(TIM)	媒体、电信和广播	意大利	2780 万	2020 年 01 月	数据处理的法律依据不足
6	英国航空	能源交通	英国	2204.6 万	2020 年 10 月	缺乏保障数据安全的技术和组织措施
7	万豪国际	酒店住宿	英国	2045 万	2020 年 10 月	缺乏保障数据安全的技术和组织措施
8	Wind Tre	媒体、电信和广播	意大利	1670 万	2020 年 07 月	数据处理的法律依据不足
9	沃达丰	媒体、电信和广播	意大利	约 12251.6 万	2020 年 11 月	违反数据处理的一般原则
10	NBB 公司	就业	德国	1040 万	2021 年 01 月	数据处理的法律依据不足

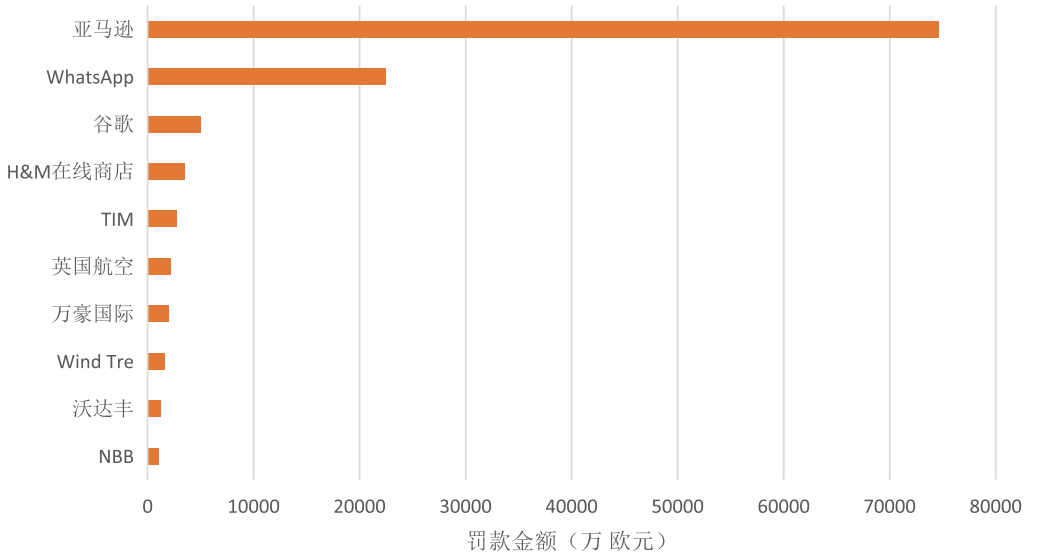


图 3.4　GDPR 单次罚款事件金额最高前十名以及企业

[1]　https://www.enforcementtracker.com/

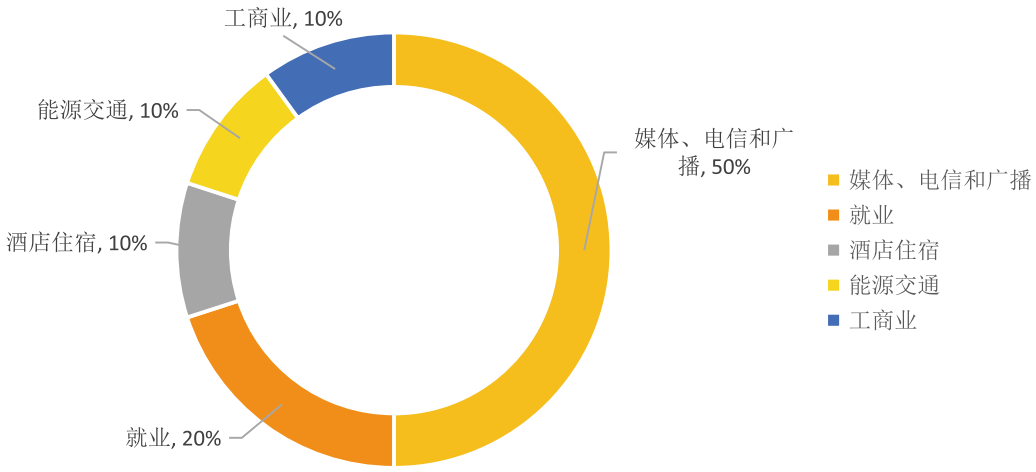


图 3.5　GDPR 单次罚款事件金额最高前十名所属行业

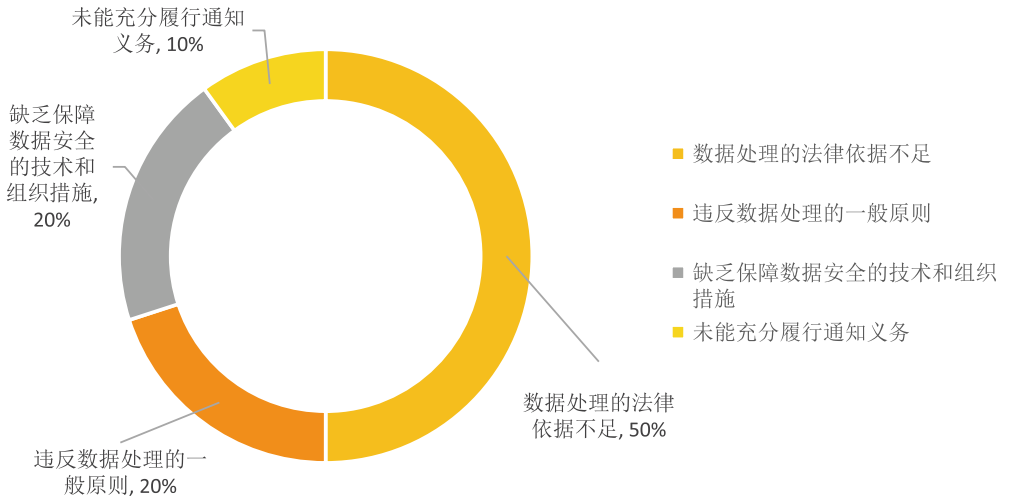


图 3.6　GDPR 单次罚款事件金额最高前十名的原因分析

3.1.2.2　国内现状

2021 年 6 月 10 日，我国正式通过《中华人民共和国数据安全法》（《数据安全法》）；同年 8 月 20 日，我国通过了《中华人民共和国个人信息保护法》（下面简称《个人信息保护法》）。这两部重磅级法律，分别已经从 9 月 1 日和 11 月 1 日正式实施。作为数据安全与个人信息领域两部综合性法律，《数据安全法》更加强调总体国家安全观，对国家利益、公共利益和个人、组织合法权益方面给予全面保护，《个人信息保护法》则则更加侧重于对个人信息、

隐私等涉及公民自身安全的进行个人信息与权益的保护。从国家层面来说，《数据安全法》对于我国的国家安全建设有着至关重要的意义，同时促进以数据为关键要素的数字经济健康发展；从企业层面来说，《数据安全法》和《个人信息保护法》是企业数据活动必须遵循的“行为规范”，是重要的法规监管依据。

除此以外，2021 年国内数据安全法规、政策、标准密集发布，如表 3.3 所示。这些可看成《数据安全法》和《个人信息保护法》的一些配套行政法规、行业规章和标准。尤其是 2021 年 11 月国家互联网信息办公室（国家网信办）发布了《网络数据安全管理条例（征求意见稿）》，对《数据安全法》和《个人信息保护法》的法律条款进行更加具体的细化、补充和延伸。

表 3.3　2021 年国内数据安全政策法规标准事件

时间	国家部门	政策法规事件
2021 年 01 月	工业和信息化部	《关于开展工业互联网企业网络安全分类分级管理试点工作的通知》
2021 年 03 月	国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅	《常见类型移动互联网应用程序必要个人信息范围规定》
2021 年 04 月	中国人民银行	《金融数据安全数据生命周期安全规范》(JR/T 0223-2021)
2021 年 04 月	国家医疗保障局	《国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知》医保发〔2021〕23 号
2021 年 06 月	国家卫健委	《互联网医疗健康信息安全管理规范（征求意见稿）》
2021 年 08 月	国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国交通运输部	汽车数据安全管理若干规定（试行）
2021 年 09 月	工业和信息化部	关于加强车联网网络安全和数据安全工作的通知
2021 年 09 月	工业和信息化部	《工业和信息化领域数据安全管理办法（征求意见稿）》
2021 年 10 月	国家互联网信息办公室	《数据出境安全评估办法（征求意见稿）》
2021 年 10 月	信息安全标准委员会	《信息安全技术 重要数据识别指南》（征求意见稿）
2021 年 11 月	国家互联网信息办公室	《网络数据安全管理条例（征求意见稿）》

如表 3.4 所示，2021 年国内数据安全执法事件主要集中在 App 个人信息侵权的整治，以及个人信息非法售卖。从执法部门应用的执法依据上看，在《数据安全法》和《个人信息保护法》发布之前，执法依据是一些分散在各个法律法规的条款。而这部综合性的法规实施后，执法依据将更加全面和具体，企业不得不重视数据安全与隐私的合规性要求。

表 3.4　2021 年国内数据安全执法事件

时间	执法部门	事件	执法依据
2021 年 01 月	杭州互联网法院	全国首例适用《民法典》的个人信息保护案宣判 [1]	《民法典》
2021 年 03 月	工信部	工信部通报下架 60 款侵害用户权益 App[2]	《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》等
2021 年 04 月	杭州市中级人民法院	“人脸识别第一案”二审宣判 [3]	《中华人民共和国网络安全法》等
2021 年 04 月	西湖法院	魔蝎科技非法缓存两千万条数据 被判侵犯个人信息罚三千万 [4]	《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等
2021 年 04 月	珠海网警	珠海网警在“净网 2021”专项行动破获侵犯公民个人信息的犯罪团伙 [5]	《刑法》
2021 年 07 月	国家互联网信息办公室	严重违法违规收集使用个人信息，滴滴 App 被全网下架 [6]	《中华人民共和国网络安全法》

3.1.3　发展趋势

在数据隐私法规监管的强有力推动下，数据安全成为国内外关注的热点。尤其是国内今年通过并正式实施《数据安全法》和《个人信息保护法》，数据安全与隐私合规已经成为企业关注的重点话题；而国外在 2021 年 RSA 大会的创新沙盒环节中，十家角逐的创新公司有三家（分别是 Cape Privacy、Open Raven 和 Satori 公司）与数据安全与隐私保护相关，这数量比任何一个其他安全细分领域对应的创新沙盒公司都要多。

据 Gartner 在《2021 隐私成熟度曲线》报告中预测指出：“2023 年之前全球 80% 以上的企业将面临至少一项以隐私为重点的数据安全保护规定；到 2024 年以数据隐私驱动的合规投入将突破 150 亿美元；到 2025 年 60% 的大型企业组织将在分析、商业智能或云计算中使用一种或多种增强隐私的计算技术”。由此可见，数据安全合规未来仍然有广阔的市场应用前景。然而，传统网络安全技术与手段，比如防火墙、入侵检测、身份认证等远远无法满足数据安全的需求，近年来数据安全技术不断推陈出新，新技术新方法如雨后春笋一般不断地涌现。

[1] https://china.zjol.com.cn/gnxw/202101/t20210116_21977755.shtml
[2] https://mp.weixin.qq.com/s/iL_KTArq_TcSMBKODHSypA
[3] https://mp.weixin.qq.com/s/Dxz0xTVtYmRb-y3UDFzqeQ
[4] https://new.qq.com/omn/20210416/20210416A00ICZ00.html
[5] https://www.thepaper.cn/newsDetail_forward_12006914
[6] http://www.cac.gov.cn/2021-07/09/c_1627415870012872.htm

3.2 物联网安全

近些年，随着 5G 等关键技术突破，物联网的发展突飞猛进，同时受疫情影响，远程办公需求增加，随之而来的是海量的设备接入互联网。“万物互联”带来便利的同时，也为攻击者带来了更多的攻击选择。物联网已经渗透进我们衣食住行的各个领域，频发的智能设备攻击威胁着个人的隐私安全，关键基础设施在实现数字化联网转型时也面临巨大风险。物联网安全不应局限在技术方面提高智能设备的安全性能，在处理随之产生的海量数据时，也需要合理的法规和完善的管理方案，确保风险的及时发现、准确定位和高效恢复。

3.2.1 热点安全事件

物联网技术正在加速向各行业渗透，根据中国信通院《物联网白皮书（2020 年）》内容显示：预计到 2025 年，物联网连接数的大部分增长来自产业市场，产业物联网的连接数将占到总体的 61.2%。智慧工业、智慧城市 、智慧交通、智慧健康、智慧能源等领域将最有可能成为产业物联网连接数增长最快的领域。当业界在推动产业物联网高速发展同时，物联网安全问题也给我们敲响了警钟。近些年，国内外挖矿、设备劫持事件频发，智能家居产品不断爆出安全漏洞，漏洞被利用时将造成不可逆的经济损失，同时也反映在物联网产业建设初期，安全作为物联网应用的基础设施的重要性。

3.2.1.1 智能摄像头频曝漏洞

2021 年 9 月，研究人员在海康威视 IP 摄像机 /NVR 设备固件中发现一个高位的安全漏洞 CVE-2021-36260，攻击者可以在未通过认证的情况下远程执行代码，影响当时所有 IP 摄像头和 NVR 设备固件，包括最新版本。攻击不需要与用户进行交互，在获取设备的 root 权限后，通过 shell 可以完全控制设备，可以获取所有者的任何信息，并继续横向攻击内部网络，并且不会在摄像头中留下任何日登陆信息。

智能家居，尤其是摄像头类产品，是最先走入人们日常生活中的物联网设备，在方便我们的同时，也给攻击者提供了大量的攻击机会。这些摄像头类产品，种类繁多，往往侧重于功能的拓展与成本的控制，便于在日益增长的物联网设备需求市场中率先占据席位。安全性的考量往往优先级不高，但是一旦被攻击者发现漏洞并且利用，造成的不仅是经济损失，同时也会对用户的隐私安全带来极大的威胁，进而影响到设备厂商的信誉和声望，造成更大的损失。

3.2.1.2 供应链风险不可忽视

SolarWinds 的后门事件，敲响了供应链风险的警钟，攻击影响极大，涉及政府部门、关

键基础设施以及多家全球 500 强企业。就在 2021 年 8 月，类似的供应链事件也袭击了 IOT 领域。研究人员发现了 IOT 设备硬件中使用的随机数生成器，存在严重漏洞，导致数十亿的物联网 IOT 设备都面临潜在的攻击风险。在物联网设备中，系统级芯片 (SoC) 装有一个专门的硬件 RNG 外设，称为真随机数生成器 (TRNG)，用于从物理过程或现象中捕获“随机性”。由于目前大多 IOT 设备在实现这一功能时欠缺合理的考量，导致在某些情况下，这个生成器并没有“随机”生成结果，而是“固定”和“可预测”地生成结果，例如非常简单的或者单纯由 0 构成的加密密钥，后果可想而知。

上述典型的安全事件，为我们敲响了警钟。在处理 IOT 环境的安全风险时，所面临的环境和限制条件都是有很大区别的，无法直接照搬解决方案。例如上述事件里的问题就只在 IOT 环境下才有可能发生，因为在传统 IT 系统中存在的典型的 API，比如调用随机数的 API（Unix 类系统下的 "/dev/random" 或者 Windows 系统下的 BCryptGenRandom），在 IOT 中并没有类似的可靠的 API 供使用，导致不同开发者使用不同的自定义实现方式，就会导致潜在的安全风险。除此之外，硬件的安全隐患不容忽视。所谓牵一发而动全身，硬件中的某个部件或功能一旦出现安全漏洞，影响的将是下游数百万乃至上亿的设备，而且这类漏洞往往通过固件补丁的方式无法完整修复，造成的影响是长远的，而且修复的代价是巨大的。

3.2.2 政策和市场

近年来，国内各个标准指南文件与物联网相关的大会召开，也都传达着国家对于物联网安全领域的发展规划以及重视，对于安全行业是一大利好，跟紧国家指导要求，及时调整策略，争先在物联网安全领域施展拳脚。

2021 年 5 月，工信部发布了《关于深入推进移动物联网全面发展的通知》，为物联网产业的更深入发展指明方向。在市场需求变化与政策全面支持下，在新基建加快落地的背景下，2022 年国内物联网产业的发展环境显然更加友好。随着物联网技术、市场、行业的普遍成熟，物联网产业生态的新一轮爆发期有望更快到来。

除此之外，八部门（工业和信息化部、中央网络安全和信息化委员会办公室、科学技术部、生态环境部、住房和城乡建设部、农业农村部、国家卫生健康委员会、国家能源局）联合印发《物联网新型基础设施建设三年行动计划（2021—2023 年）》。其中四个目标：创新能力有所突破、产业生态不断完善、应用规模持续扩大和支撑体系更加健全，涉及社会治理领域、行业应用领域和民生消费领域，加强标准体系建设、完善公共服务体系和强化安全支撑保障。贯彻落实《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》，

打造系统完备、高效实用、智能绿色、安全可靠的现代化基础设施体系，推进物联网新型基础设施建设，充分发挥物联网在推动数字经济发展、赋能传统产业转型升级方面的重要作用。

2021 年 10 月 25 日，工信部发布《物联网基础安全标准体系建设指南（2021 版）》，明确物联网终端、网关、平台等关键基础环节安全要求，满足物联网基础安全保障需要，促进物联网基础安全能力提升。到 2022 年，初步建立物联网基础安全标准体系。

《指南》明确了我国构建物联网基础安全标准体系的时间表。《指南》提出，到 2022 年，初步建立物联网基础安全标准体系，研制重点行业标准 10 项以上，明确物联网终端、网关、平台等关键基础环节安全要求，满足物联网基础安全保障需要，促进物联网基础安全能力提升；到 2025 年，推动形成较为完善的物联网基础安全标准体系，研制行业标准 30 项以上，提升标准在细分行业及领域的覆盖程度，提高跨行业物联网应用安全水平，保障消费者安全使用。

根据《指南》的定义，物联网基础安全标准主要是指物联网终端、网关、平台等关键基础环节的安全标准。物联网基础安全标准体系包括总体安全、终端安全、网关安全、平台安全、安全管理等 5 大类标准。产业发展，标准先行。《指南》中提出的目标任务主要关注自主的标准化研制和应用、动态更新以及开展全球化的国际交流合作。

2021 年 11 月 30 日，世界物联网大会 WIOTC 第四次召开，会议主题“开启物联时代新格局，打造物联世界新经济” 。2020 年 WIOTC 公布的世界物联网排行榜中，华为、中国移动、中国联通，以及 IBM、高通、Intel 等国内外知名厂商都赫然在列。在“万物互联”时代，物联网安全市场成为网安行业新蓝海。近年来，网络安全公司争相布局物联网安全业务，产品业务目前主要应用在公安、园区、医疗、教育等领域。

在 2017 年超过 1000 亿美元之后，全球整体物联网解决方案市场已经超过 2000 亿美元。据 Statista 称，到 2025 年，市场价值可能高达 1.6 万亿美元。物联网行业在 5G 和云计算技术的推动下显示出明确的长期成长性。根据 MarketsandMarkets 数据，2020 年全球物联网安全市场规模为 125 亿美元，预计 2025 年增至 366 亿美元。市场研究机构 Credence

Research 最新发布的报告预测，到 2026 年，全球物联网安全市场预计将达到 364.5 亿美元。

IOT ANALYTICS 发布的数据表明，2021 年全球物联网投入资金达到 1600 亿美元，增长 24%，主要受到相关软件以及安全的带动，并且预计逐步增长至 2025 年的 4100 亿美元。

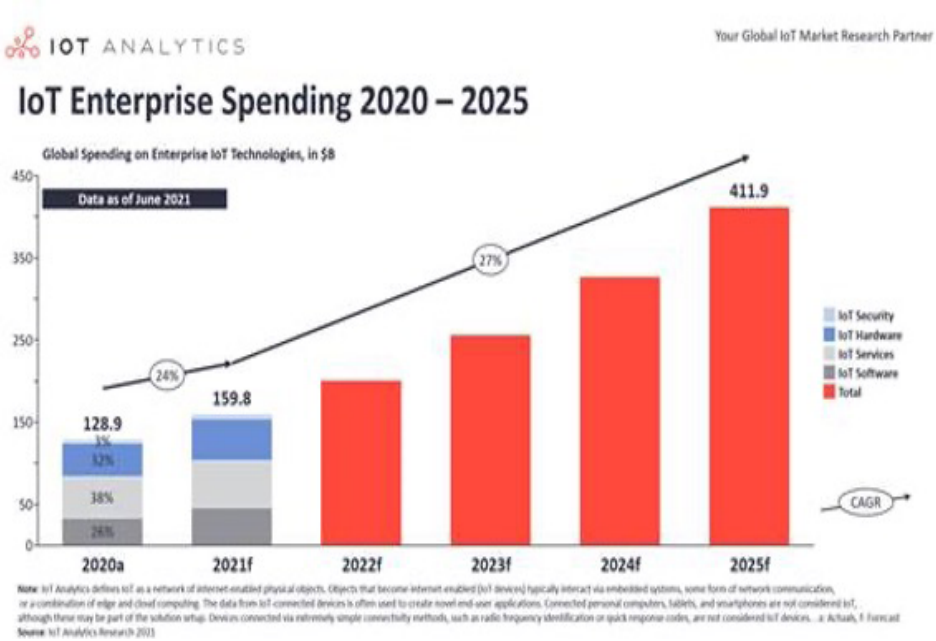


图 3.7　IOT 企业 2020-2025 年度预计投入趋势

以下是全球范围内主要的物联网厂商。

IoT 软件供应商

- Intel
- Cisco
- IBM
- Amazon
- SAP
- Google

IoT 云服务供应商

- Google Cloud
- AWS
- Microsoft Azure
- IBM Watson

- Oracle
- Salesforce

IoT 传感器供应商

- Bosch
- Honeywell
- IBM
- Ericsson
- Cisco
- GE
- ARM

其他 IOT 解决方案厂商

- PTC
- ABB
- Huawei
- Schneider Electric
- Belkin
- Advantech
- Bitdefender
- LG
- Nest
- Philips
- Ring
- Samsung
- Sonos

- Samsara
- Apple

巨大的市场福利同样带来了巨大的安全挑战，与传统的 it 安全相比，物联网需要不同的技术、程序、协议和标准。

3.2.3 发展趋势

随着 5G、移动计算等新技术的发展，近年来各类物联网场景快速得到应用，而应用场景的落地，使得攻击者嗅探到了数量庞大的物联网设备背后存在的攻击面。回顾过去几年出现的安全事件可以管中窥豹，推测物联网安全的趋势。

目前物联网安全有以下几个发展趋势：

1. 设备数量急速膨胀扩张，导致应用场景与安全边界随之扩张。据 IDC 预测，在 2025 年时，全球将有超过 400 亿设备接入互联网，同时会产生近 80ZB 的数据。供应商已经在逐步推出相关的物联网安全工具，但不够成熟，在市场上仍然处于初级摸索阶段。
2. 大量的设备带来的是大量的数据。随着 5G 技术的发展，物联网的影响将再次被放大。在考虑如何利用这些数据之前，如何储存海量的数据已经引起了很多争论。不论是利用边缘存储、数据中心还是云端存储，都必须确保这些数据是安全的。
3. 在海量设备和数据面前，将异常从这些日常数据中高效地定位和分离，自动化解决方案迫在眉睫。机器学习已经在风险管理、威胁情报以及安全信息和事件管理（SIEM）等领域初展拳脚，但是当事件量级暴增至百亿级别时，自动化将发挥至关重要的作用。
4. 海量的设备与场景，将会成为攻击者的乐园。物联网提供了大量的新攻击点，在物联网逐渐渗透进交通系统、智能家居、智慧城市、关键基础设施建设、工业系统、医疗系统等等中时，带来的同样还有大量的潜在风险。
5. 标准化的需求也至关重要。大量设备在大量不同场景中被不同厂商用不同的方式去实现，缺乏标准将导致安全开发、风险评估与安全防护混乱不堪。在面对存在大量脆弱性和攻击面的场景时，缺乏统一标准、各自为战将被攻击者找到漏洞并逐个击破，为整体物联网安全带来极大的隐患。

近 2 年出现的安全事件说明物联网安全面临两个挑战：一、影响范围方面，无论协议设计还是产品实现，物联网设备一旦出现漏洞，影响规模将非常广泛，后果严重。二、从攻击者的角度而言，其攻击目标和攻击手段并非一成不变，总能推陈出新，紧跟时政。所以，物

联网安全严峻的形势要求研究团队，扩大研究范围，杜绝思维僵化；而对监管方而言，合规性要求是必需，同时安全治理手段要与技术手段结合。

3.3 工业互联网安全

随着工业领域数字化、网络化的不断推进，网络安全威胁成为了工业领域的重要挑战。对工业互联网来说，“安全”是工业互联网健康有序发展的保障，工业互联网与传统工业相对封闭可信的制造环境不同，易于受到病毒、木马、高级持续性攻击等安全风险的威胁，一旦受到网络攻击，将会造成巨大的经济损失，并可能带来环境灾难和人员伤亡。同时，在工业互联网这个大系统中，任何一个环节出现安全问题，都有可能造成整个系统的崩溃，甚至危及公众安全和国家安全。因此，工业互联网的安全问题需要高度重视。

3.3.1 热点安全事件

自 2021 年 1 月份以来，影响关键信息基础设施运营的攻击数量急剧上升。制造业、电力、管道运输、水处理、国防工业、航空航天、石油化工、医疗器械、能源和医院等公用事业都受到黑客的高度关注。从互联网上收集到的 59 起攻击事件来看，有大约 59% 的攻击中都出现了勒索软件的身影。此类攻击方式泛滥的一个重要原因是勒索软件团体很少面临真正的后果，并且可以获得高额赎金，因为对于上述的受害行业和企业来说，他们大部分都无法承受系统或生产线持续停止服务的代价。美国最大的成品油运营商 Colonial Pipeline 就曾因遭受 DarkSide 黑客组织的勒索病毒攻击，使得美国东部沿海的燃油网络陷入瘫痪，无法提供管道服务，影响依赖燃油资源众多行业正常运转。

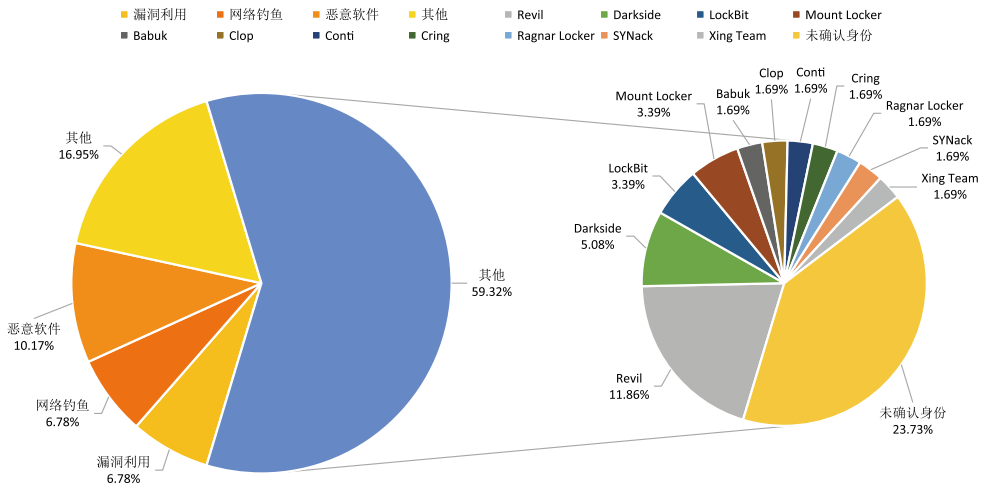


图 3.8 攻击类型占比情况

其他攻击手法也层出不穷，比如恶意软件常搭载着钓鱼邮件被四处散播，另一些攻击者利用 IT 网络中诸如邮件系统或者 VPN 的漏洞获得企业内部机器的控制权限，之后便潜伏在受影响系统中默默窃取内部数据。更有甚者，还会通过受控的管理员工作站，对工业隔离网络发起攻击。过去，勒索软件攻击会窃取受害者的机密数据，然后加密他们的文件以强制支付赎金，如果拒付赎金，会将数据公开拍卖以从中获利。随着时间的推移，攻击者的策略已经升级为对受害者的网络和网站进行 DDoS 攻击、向客户和记者发送电子邮件、甚至威胁将与证券交易所联系，这种对攻击行为的大肆宣扬无疑给受害组织构成了巨大的舆论压力。受害组织最常受到的影响是系统 / 服务中断、生产 / 供应中断、数据被窃，有些机密数据不光被盗取，作为威胁有的还被公开发布或售卖。另外，对于一些关乎民生安全的基础设施，被入侵的后果将不仅是财产和名誉的损失，美国佛罗里达州 Oldsmar 市的水处理系统遭入侵后，处理流程中的氢氧化钠（NaOH）浓度被提高到极其危险的水平，所幸发现及时并未造成人员伤亡。

在互联网上能够收集的攻击事件估计只是冰山一角，不少受害者或许因为担心监管或客户关系并不愿意公开谈论其内部遭受的损失，这种沉默也会导致公众对威胁的严重性缺乏了解。

表 3.5　2021 年工控相关安全事件汇总

月份	事件	目标国家 / 地区	目标行业 / 系统	攻击类型	造成危害
1	起重机制造商 Palfinger 遭受网络攻击	奥地利	机械制造	网络攻击	业务受损
1	包装企业 WestRock 遭受勒索软件攻击影响 IT 和 OT 系统	美国	包装业	勒索软件攻击	业务延误
1	燃料分销商 Ultrapar 遭受网络攻击	巴西	燃料分销	勒索软件攻击	系统中断
1	铁路运营商 OmniTRAX 遭受勒索软件 Conti 攻击	美国	铁道交通	勒索软件攻击	数据被盗
1	飞机制造商达索猎鹰遭受勒索软件 Ragnar Locker 攻击	法国	航空制造	Ragnar Locker 勒索软件攻击	数据泄露
1	能源及冶金企业遭受木马攻击	哥伦比亚	能源、冶金	远程访问木马	机密数据被窃
1	基础设施管理公司 Amey 遭受勒索软件 Mount Locker 攻击	英国	基础设施	Mount Locker 勒索软件攻击	被窃数据遭公布
1	数百家工业组织在 SolarWinds 事件中遭受 Sunburst 恶意软件攻击	广泛	众多（制造业、运输物流、石油天然气、采矿能源）	Sunburst 恶意软件攻击	受害系统遭受未授权访问
2	油田服务公司 Gyrodata 遭受网络攻击泄露员工数据	美国	石油化工	勒索软件攻击	敏感信息泄露

（续表）

月份	事件	目标国家 / 地区	目标行业 / 系统	攻击类型	造成危害
2	APT 组织 Lazarus 利用 ThreatNeedle 后门攻击国防工业组织	广泛	国防工业	网络钓鱼传播恶意软件、突破 IT 网络和 OT 网络的隔离限制	窃取机密信息
2	造船厂 Beneteau 遭受网络攻击	法国	船只制造	恶意软件入侵（疑似勒索软件攻击）	生产被迫停止
2	飞机制造商庞巴迪泄露飞机设计关键数据	加拿大	航空制造	利用软件漏洞入侵	被窃数据遭公布
2	两家电力公司遭受勒索软件攻击	巴西	电力	Darkside 勒索软件攻击	部分系统中断、窃取数据
2	供水设施被黑客远程攻击投毒	美国	水处理	远控软件入侵	试图将 NaOH 浓度提高 100 倍以上
3	能源供应商 Eversource 泄露客户个人信息	美国	能源	云服务器不安全造成信息泄露	信息泄露
3	制造业遭受恶意活动 A41APT 攻击	日本	制造	恶意活动 A41APT、恶意后门	数据被盗
3	工业企业 MIDC 的服务器遭受 SYNack 勒索软件攻击	印度	工业供应商	SYNack 勒索软件	工作被迫中断
3	船运公司 ECU Worldwide 遭受勒索软件攻击	印度	船舶运输	Mount Locker 勒索软件	数据被盗
3	计算机厂商宏碁遭受勒索软件 Revil 勒索 5000 万美元	中国台湾	计算机制造	REvil 勒索软件攻击	数据被盗、索要赎金
3	霍尼韦尔 IT 系统遭受恶意软件攻击	美国	工控厂商	恶意软件入侵	系统遭到未经授权访问
3	能源公司 Shell 因使用 Accellion FTA 设备泄露数据	广泛	能源石化	利用漏洞入侵、获得部分文件的访问权限	数据被窃
3	物联网设备制造商 Sierra Wireless 遭受勒索软件攻击致工厂停产	加拿大	物联网解决方案提供商	勒索软件攻击	生产被迫停止
3	中远海运疑遭受巴西黑客攻击	中国	航运	电子邮件系统遭入侵	电子邮件系统无法正常使用
4	光学制造商 Hoya 遭受勒索软件攻击	日本	非金属矿物加工	勒索软件攻击	机密数据被窃
4	电子制造服务商 Asteelflash 遭受 Revil 勒索软件攻击	法国	电子制造	Revil 勒索软件攻击	数据被盗
4	工业企业遭受 Cring 勒索软件攻击致生产关闭	德国	工业供应商	Cring 勒索软件攻击	生产服务器被加密

（续表）

月份	事件	目标国家 / 地区	目标行业 / 系统	攻击类型	造成危害
5	燃油管道商 Colonial Pipeline 在遭受勒索软件攻击后披露数据泄露	美国	燃气供应	DarkSide 勒索软件攻击（现在更名为 BlackMatter）	勒索赎金、窃取个人信息及文件、燃料供应大范围中断
5	水务公司 WSSC Water 遭受勒索软件攻击	美国	污水处理	勒索软件攻击	窃取用户信息
5	美国核武器承包商 Sol Oriens 遭受 REvil 勒索软件攻击	美国	国防、军事	REvil 勒索软件攻击	网站服务中断、未经授权访问窃取文件
5	最大丙烷供应商 AmeriGas 披露数据泄露事件	美国	丙烷供应商	钓鱼邮件导致内部账号被盗	员工信息泄露
5	管道服务公司 LineStar 遭受勒索软件攻击泄露 70 GB 数据	美国	管道运输	Xing Team 勒索软件	被泄数据遭公布
5	工程技术生产商 PurePower 遭受 Conti 勒索软件攻击	美国	燃料部件生产商	Conti 勒索软件攻击	部分被窃敏感文件被公布
5	制药公司 Siegfried 遭受网络攻击致生产中断	瑞士	医疗制药	恶意软件攻击	工厂生产中断
5	制造商 Yamabiko 遭受 Babuk 勒索软件攻击	日本	机械制造	Babuk 勒索软件攻击	部分被窃数据遭公布
5	新型恶意软件 Snip3 攻击航空航天领域组织	广泛	航空航天	钓鱼邮件传播恶意软件	远程控制、键盘记录、数据窃取
5	医疗保健提供商 Scripps Health 遭受勒索软件攻击	智利	医疗	勒索软件攻击	部分医疗护理活动中断
5	英国铁路网络 Merseyrail 遭受 Lockbit 勒索软件攻击	英国	铁道交通	Lockbit 勒索软件攻击	CEO 邮箱被劫持发布勒索通知、窃取信息
5	化学品分销商 Brenntag 遭受 DarkSide 勒索软件攻击	德国	化学品分销	DarkSide 勒索软件攻击	被迫以比特币形式支付了 440 万美元赎金
5	拖车生产商 Utility 遭受 Clop 勒索软件攻击	美国	汽车制造	Clop 勒索软件攻击	系统中断、员工信息泄露
6	航空宇宙产业公司遭受黑客攻击，泄露大量机密文件	韩国	航空	黑客入侵	大量机密文件泄露
6	飞机加油公司 JAFS 遭受勒索软件攻击	日本	航空	服务器受到了未经授权的访问、感染勒索软件	勒索赎金
6	原子能研究所 KAERI 遭受朝鲜黑客攻击	韩国	核工业	黑客利用 VPN 漏洞入侵	核心技术泄露
6	医疗保健巨头 Grupo Fleury 遭受 REvil 勒索软件攻击	巴西	医疗	REvil（Sodinokibi）勒索软件攻击	系统服务中断

（续表）

月份	事件	目标国家 / 地区	目标行业 / 系统	攻击类型	造成危害
6	攻击者冒充 DarkSide 勒索软件组织攻击能源和食品企业	巴西	食品加工	Revil 勒索软件攻击	支付赎金、服务中断
6	再生能源公司 Invenergy 遭受勒索软件 REvil 攻击泄露 4TB 数据	美国	能源	REvil 勒索软件攻击	窃取 4TB 机密信息，信息虽未被加密，但被威胁会公布机密信息
6	海运公司 HMM 电子邮件系统遭受网络攻击	韩国	海运	病毒攻击	电子邮件服务中断
6	美国医疗保健企业 CVS Health 超过十亿条记录在网上曝光	美国	医疗	信息泄露	10 亿条数据泄露
6	军用车辆制造商 Navistar 遭受网络攻击泄露数据	美国	车辆制造	勒索软件攻击	数据泄露
6	全球最大肉类加工企业 JBS Foods 遭受 REvil 勒索软件攻击	澳大利亚、美国	食品加工	REvil 勒索软件攻击	受影响的系统暂时关闭、生产线暂停、影响市场供应
7	两家污水处理厂遭到勒索软件攻击	美国	污水处理	勒索软件攻击	勒索赎金
7	伊朗收集西方国家工业控制系统情报	英国、法国和美国	货船系统、海事通信、智能建筑	收集民用基础设施情报	情报用于确定未来网络攻击目标
7	北方铁路公司售票机遭受勒索软件攻击	英国	铁道交通	勒索软件攻击	系统离线
7	伊朗黑客组织 Tortoiseshell 攻击国防及航空航天企业	美国、欧洲	国防及航空航天	利用 Facebook 平台实施社工，发送钓鱼邮件，散播恶意软件	间谍活动
7	铁路系统遭受网络攻击发布虚假信息	伊朗	铁道交通	针对铁路系统进行网络攻击	在车站显示屏上发布虚假信息，造成火车站的混乱
7	Wiregrass 电力公司遭受勒索软件攻击	美国	电力	勒索软件攻击	系统服务中断
7	航运公司 K Line 计算机系统遭受未经授权访问	日本	航运	系统遭到未经授权的访问	系统中断、信息有被泄露的可能性
8	黑客可通过输液泵漏洞控制药物剂量	德国	医疗器械	利用输液泵存在漏洞	控制药物剂量，危害生命安全
8	能源集团 ERG 遭受勒索软件攻击后通信出现轻微中断	意大利	能源	LockBit 2.0 勒索软件攻击	基础设施轻微中断

3.3.2 政策和市场

我国高度重视工业互联网发展。2021 年 1 月，工业和信息化部印发《工业互联网创新发展行动计划》，结合当前产业发展实际和技术产业演进趋势，确立了未来三年我国工业互联网发展目标。着力解决工业互联网发展中的深层次难点、痛点问题，推动产业数字化，带动数字产业化。其中包括到 2023 年，我国工业互联网安全保障能力进一步增强的发展目标，明确将开展安全保障强化行动的重点任务。

工控安全是工业互联网发展的保障。在 2021 年 11 月 MARKETSANDMARKETS 发布了工业控制系统安全市场报告 [1]，预计全球工业控制安全市场规模将从 2021 年的 171 亿美元增长到 2026 年的 235 亿美元，2021 年至 2026 年的复合年增长率为 6.6%。

图 3.9　2021-2026 年工业互联网安全市场投入趋势图

作为网络安全的一个细分赛道，投资机构对工控安全领域十分关注，2021 年 1-10 月，国内工控安全赛道的融资交易数量最多，为 11 起 [2]。

根据数世咨询 2021 年度发布的《中国数字安全能力图谱》[3]，可以看出在工业互联网细分的四个领域中，安全企业具备的专业能力和市场地位。

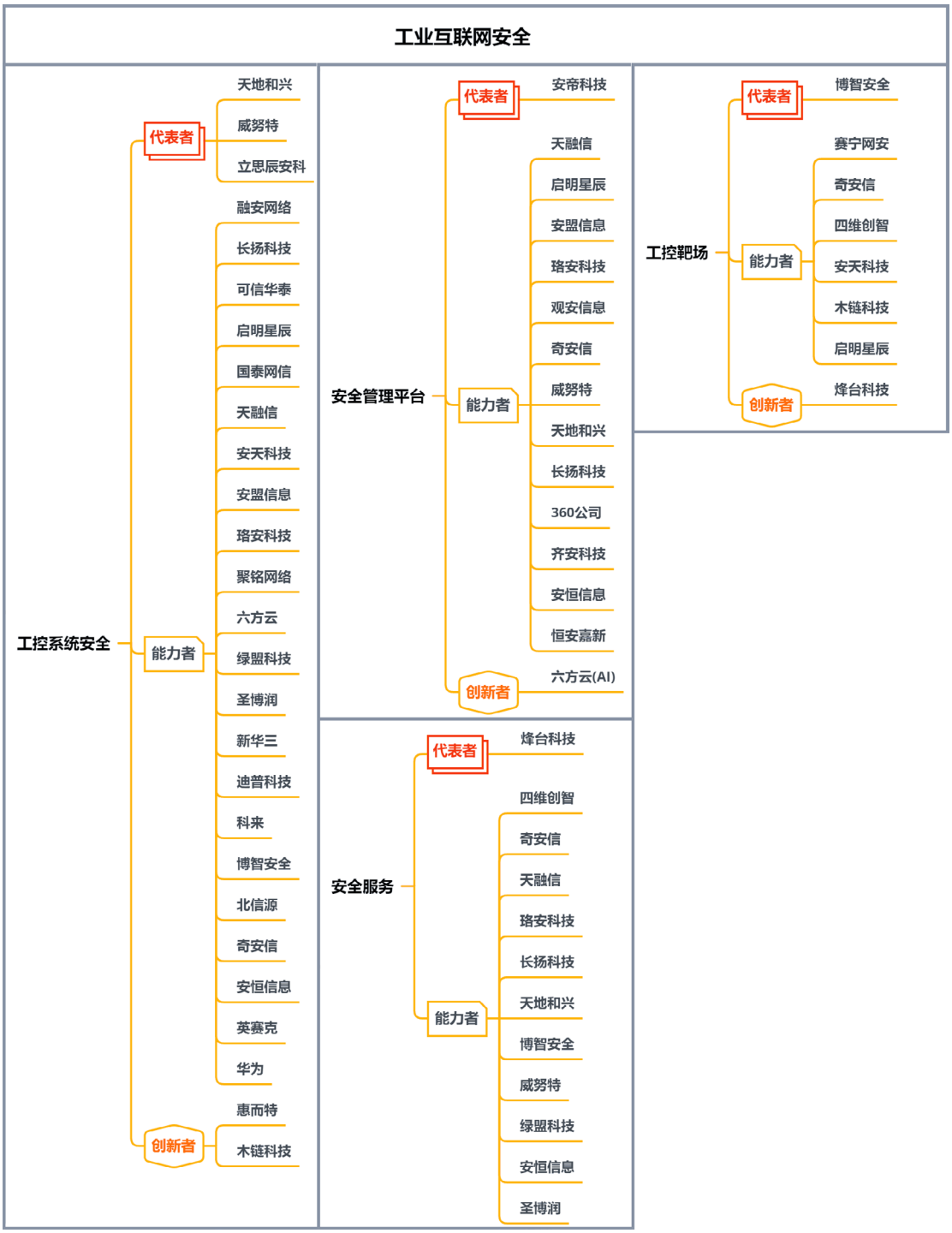


图 3.10　2021 年工业互联网安全企业能力图谱

3.3.3 发展趋势

工业互联网成为了世界各国发展战略的高点，我国工业互联网经过起步期的发展，取得了显著成效，在各行业的应用逐渐走向纵深。在日趋复杂的网络安全形势，以及新业态的融合，工业互联网安全将会呈现如下发展趋势。

1. 关键信息基础设施作为工业互联网战场的前沿，近年来攻击事件频发，在已知的攻击事件中，勒索软件攻击占比最大，攻击者向受害者施压的手段也越发激进。
2. 从工业互联网安全企业能力图谱可以看出，工业互联网安全企业向安全服务、攻防靶场布局。如何及时捕获针对业务的攻击，开展网络攻防仿真、推演、培训和新技术的论证与试验，以及应急演练，是未来工业互联网安全企业发展的主要趋势。
3. 工业互联网是国家发展重要的战略，政策持续利好。近年来大量资本涌入工业互联网，作为保障工业互联网快速发展的网络安全市场关注度持续上升。在已融资的工业互联网安全企业里，不乏有“国家队”的身影，这表明国家对工业互联网安全的重视，未来资本市场还会加大对工业互联网安全的投资。

3.4 车联网安全

车联网的广义概念指按照一定的通信协议和数据交互标准，在“人 - 车 - 路 - 云”之间进行信息交换的网络，是汽车、电子、信息通信和道路交通跨界融合的典型领域。从狭义上讲，车联网是智能网联汽车的重要组成部分，是指通过搭载先进传感器、控制器、执行器等装置，运用信息通信、互联网、大数据、云计算、人工智能等新技术，具有部分或完全自动驾驶功能，由单纯交通运输工具逐步向智能移动空间转变的新一代汽车。

无论是从广义还是狭义概念上看，车联网安全影响的都不止“看不见、摸不到”的信息安全层面，而是和人身财产安全有直接密切的关联！据世界卫生组织提供的数据显示 [1]，每年全球约有 130 万人的生命因道路交通事故而终止，还有 2000 万至 5000 万人受到非致命伤害。道路交通事故带来的损失占大部分国家国内生产总值的 3%。从中国统计年鉴提供的交通事故情况中可以看到 [2]，自 2001 年起，平均每年因交通事故而丧生的人有七万五千七百五十三人。

[1] https://www.who.int/zh/news-room/fact-sheets/detail/road-traffic-injuries
[2] http://www.stats.gov.cn/tjsj/ndsj/

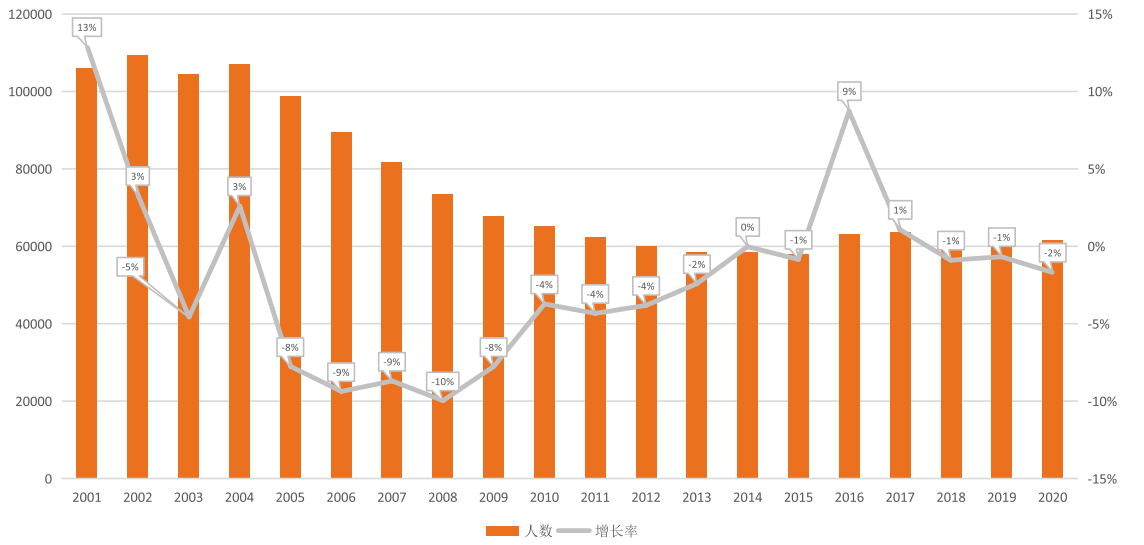


图 3.11　国内逐年交通事故死亡人数统计

从以上数据可以看出，自 2005 年以来除了个别年份外，交通事故死亡人数还是呈逐年下降的趋势，这说明公路交通安全防控能力以及交通事故救援救治效率等都在逐步提升。但不得不注意的是整体基数还是很大，究其原因，尽管造成交通事故的基本因素有很多，涉及人、车、路、环境与管理等多方面，但通常人确实是主要因素，而且以智能手机的普及程度来看，车内看手机引发的事故数量更不容忽视。世界范围内，因手机等联网需求导致的分心正超越酒驾成为造成交通事故的头号杀手。

“车路协同”在降低交通事故上是被给予厚望的，毕竟 AI 司机不会出现酒驾、疲劳驾驶或分心等状况，在肩负此重任的情况下，车联网自身的安全必然是其发展道路上的重中之重。

3.4.1　热点安全事件

安全事件的发生意味着潜藏的危机在某个条件具足的时刻被引爆，既然“爆炸”已经发生，那么惊慌、抵触之余，从中挖掘出危机根源，并将其作为将来排雷的指引，或许才是对这些安全事件的最大尊重。

3.4.1.1 黑莓 QNX 操作系统存在 BADALLOC 漏洞，多款车型使用此系统 [1]

2021 年 8 月 17 日，黑莓官方发布安全通告 [2]，公布其部分版本的 QNX Neutrino RTOS 中存在一个 CVSS 评分 9.0 的严重漏洞 (CVE-2021-22156)，恶意攻击者通过该漏洞可能获得对高度敏感系统的控制。受该漏洞影响的 QNX 产品和版本完整列表已公布，考虑到 QNX 软件产品嵌入的汽车数量庞大，即便漏洞利用存在条件，该漏洞的波及范围之广也是不容忽视的。

从该事件中，我们看到软件供应链安全早已是汽车行业最大的安全漏洞来源之一。随着软件在整车价值中的占比越来越高，造车壁垒已经由从前的上万个零部件拼合能力演变成将上亿行代码组合运行的能力。麦肯锡在 2020 年发布的报告中就曾指出“现代汽车已成为车轮上的数据中心。今天的汽车有多达 150 个 ECU 和大约 1 亿行代码，一架客机估计有 1500 万行代码，一架现代战斗机大约有 2500 万行代码，大众 PC 操作系统则接近 4000 万行”[3]。面对如此复杂的代码整合工作，汽车制造商将不可避免地被迫正视软件供应链中存在的风险和挑战。

面对这类波及范围广、修复难度大、修复周期长的软件供应链风险，解决措施和缓解方案在哪里？在国家层面，2021 年 6 月工信部发布的《车联网（智能网联汽车）网络安全标准体系建设指南（征求意见稿）》中显示，《车联网供应链安全风险管理指南》已被安排待制定。规范化的风险管理指南已经在路上了，那么在此之前，对于车联网供应链上的任一节点，需要认识到网络安全不应该再被视为附加成本，并被安排在生产的最后，而是应该被编入生产过程的每一个步骤，指导整个产品开发生命周期。比如包括与供应商密切合作，通过对供应商网络安全过程进行定期审查或在供应商协议中规定网络安全要求，提前发现相关组件在设计或架构中的弱点；自上而下地进行文化和流程的改变，自下而上采用最佳实践，利用流程和编码标准以及其他经过验证的方法来提高代码质量，对软件成分进行分析以及审查开源和第三方软件的已知漏洞，并创建软件物料清单，这些举措会对降低软件供应链风险起到关键作用。

[1] https://www.blackberry.com/us/en/company/newsroom/press-releases/2021/blackberry-qnx-software-is-now-embedded-in-over-195-million-vehicles
[2] https://www.blackberry.com/us/en/company/newsroom/press-releases/2021/blackberry-qnx-software-is-now-embedded-in-over-195-million-vehicles
[3] https://www.cstc.org.cn/zhinengwanglianqicheanquanshentoubaipishu.pdf

3.4.1.2 大众超 300 万名客户数据遭泄露

除了技术维度的风险外，从数据属性维度看，车联网数据还涉及个人数据安全、企业数据安全、国家数据安全等。2021 年 6 月中旬，大众汽车及旗下品牌奥迪遭到数据泄露，超 300 万名客户数据遭泄露。泄露发生的原因是一家供应商在 2019 年 8 月至 2021 年 5 月期间将客户数据“未经保护”的暴露在互联网上。被泄基础信息包括姓名、邮件地址、电话和车牌号，部分还包括驾驶执照号码、社保号码等。

该事件中泄露的信息确实可能给受影响客户带来困扰，比如最常见的是被收集到信息的攻击者发起社工攻击。但是我们对于车联网中信息泄露所能造成危害的认识不应该局限于此。实际中除了车主个人基础信息外，摄像头图像、生物特征数据、车辆位置、行驶速度和日期、导航历史记录等个人敏感信息都有可能被车辆的摄像头、雷达等传感器采集并上传至云端，在缺乏规范管理或信息不对称的情况下，这些信息的采集甚至是在个人没有知悉时进行的。此类蕴藏着巨大数据价值的信息如果像上述事件中那样未被妥善管理，那么泄露后造成的损失和危害将是无法预估的。

从 2021 年 10 月 1 日起起施行的《汽车数据安全管理若干规定（试行）》中就能看出国家对汽车数据处理的高度重视。其中就明确规定了汽车数据处理者处理个人信息和重要数据的原则、细化了个人敏感信息的处理要求、指明了个人信息与重要数据跨境传输的相关要求。

3.4.2 政策和市场

车联网安全发展过程中少不了政策的指引和规范，国家近年来已经出台了不少相关政策。

2021 年 3 月 12 日，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》对外公布，在“建设现代化基础设施体系”章节中明确提出要“积极稳妥发展工业互联网和车联网”。

2021 年 6 月 21 日，工业和信息化部发布《车联网（智能网联汽车）网络安全标准体系建设指南（征求意见稿）》，意在落实《中华人民共和国网络安全法》等法律法规要求，加强车联网（智能网联汽车）网络安全标准化工作顶层设计。其中构建了车联网网络安全标准体系框架，如图 3.12 所示。

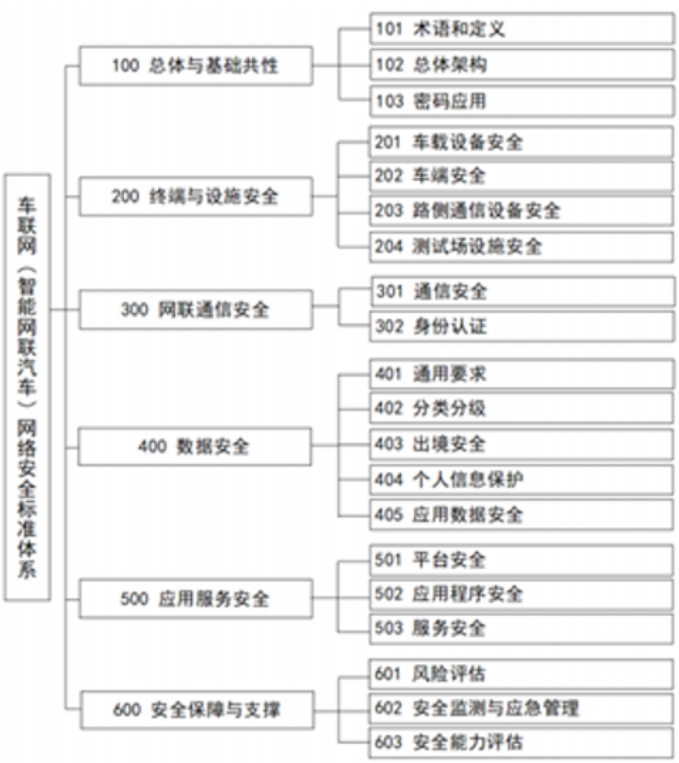


图 3.12　车联网（智能网联汽车）网络安全标准体系框架图

并计划到 2023 年底，初步构建起车联网（智能网联汽车）网络安全标准体系，就体系框架中给出的方向，完成 50 项以上重点急需安全标准的制修订工作，到 2025 年，形成较为完备的车联网（智能网联汽车）网络安全标准体系，完成 100 项以上重点标准。

2021 年 8 月 12 日，工业和信息化部在对政协第十三届全国委员会第四次会议第 2296 号《关于加强对智能汽车数据安全监管保障智能汽车产业安全健康发展的提案》的答复中表示：近年来，相关部门高度重视以智能汽车为主体的车联网安全监管，并开展了一系列工作。包括统筹推进车联网产业发展和安全保障、健全完善相关法律法规和政策要求、积极推动制定相关技术标准、强化安全技术保障。接下来，工业和信息化部还将会同相关部门进一步健全完善车联网安全监管工作体系和工作机制，一是进一步完善车联网安全管理制度、二是强化车联网安全监测和漏洞管理、三是加强车联网安全监管、四是促进车联网安全产业发展。

在市场投入方面，据 MarketResearch Future (MRFR) 提供的研究报告显示[1]，汽车网络安全市场在 2020 年市值为 21.6 亿美元，预计到 2028 年将达到 89.4 亿美元，在预测期内

[1]　https://support.blackberry.com/kb/articleDetail?articleNumber=000082334

（2021-2028）的年复合增长率为 18.56%，并表示汽车网络安全市场正在获得巨大的吸引力。国内方面，针对车联网持续升级的网络安全威胁和不断增强的合规要求，也对市场形成了有利的牵引。据中国信通院 2020 年发布的《中国网络安全技术与企业发展研究报告》统计，国内部分车联网安全企业实践如表 3.6 所示 [1]。

表 3.6　国内车联网安全领域创新企业（来源：中国信息通信研究院）

企业名称	技术领域 / 特点
安恒信息	● 基于驱动层安全监控防护技术，采用自学习的网络进程安全防护策略； ● 可针对物联网终端系统进行内核防护、数据加密和实时审计，通过物联网态势感知与管控中心进行智能分析。
开源网安	● 基于数据 CIA 模型和相关威胁分析方法构建威胁分析模型； ● 针对资产，确定其面临的威胁，通过预设攻击场景对相关威胁进行分级； ● 根据攻击概率和威胁严重程度确定面临的安全风险等级。
东软	● 覆盖车联网全生命周期； ● 基于自有引擎技术开发车载入侵防御系统； ● 为车载系统和数据提供整体化纵深式防御的可信计算平台。
观安信息	● 依据 6 大类 20 小类不同保护对象和多种安全需求建立分层的安全防护体系； ● 基于相关法律、法规及政策，分别设计各层的安全防护措施，建立统一的安全管理平台。
上海控安	● 支持基于五元组的以太网策略和基于安全模型和协议内容的 CAN/LIN 等总线策略； ● 基于 CAN、LIN 等总线协议的识别解析，实现基于总线协议等安全防护。
艾拉比	● 提供云、管、端全链路一站式解决方案，由云端的 OTA 管理平台、汽车端的升级逻辑控制及升级代理程序、连接汽车和云的通信管道三部分组成； ● 通讯协议支持私有协议和 OMA/DM 协议。
芯盾时代	● 通过终端安全沙箱、多层密钥体系、设备指纹技术等核心技术，为汽车生成全球唯一的“数字身份凭证”。
绿盟	● 基于车联网端、管、云三层架构体系，覆盖车辆终端、移动终端、路侧单元、TSP 云端服务等车联网要素，开展基于车联网端到端的威胁分析与风险评估。
银基信息	● 提供车、云、通讯三端的安全产品及服务，覆盖安全芯片、安全通讯技术、数据安全、PKI、态势感知、安全管理等。

3.4.3　发展趋势

车联网是“互联网 +”战略落地的重要领域，对推动汽车、交通、信息通信业的转型升级具有重要意义。目前我国已将车联网产业上升到国家战略高度，产业政策持续利好。车联网的安全随之也成为被高度重视与投入的领域。与传统网络系统相比，车联网系统有着新的系统组成、通信场景，这些都在系统安全性及用户隐私保护方面带来了新的需求与挑战。

[1]　http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/P020201223685469901767.pdf

通过回顾车联网安全事件、相关政策及市场投入，观察到车联网安全方面的以下几点现状：

1. 产业链长，所需防护环节众多，存在的安全问题复杂。且当前产业链中的不少环节对信息安全的重视程度还远没有达到要求；
2. 智能车上亿行代码带来的复杂性，使得可被利用的漏洞数也增加，攻击面众多，为了便利实现的远程操作功能成为攻击者的极佳切入点；
3. 海量数据采集、传输、上云，车辆数据保护面临挑战；

但是危机中也总是蕴藏着机遇，展望未来，车联网安全将发展成为安全行业中的一大重要领域，车企将会和网络安全公司有更广泛和紧密的合作，合力推进汽车网络安全检测和防护技术的研究及研发；构建覆盖全链条的综合防御体系将是车联网安全发展的必然趋势，安全标准的制定与落地会是助推车联网安全发展的必要手段，安全试点示范则将驱动车联网安全产业快速发展落地。

3.5 5G 安全

5G 作为新基建的重要基础设施之一，目前已经广泛应用于增强型移动宽带 (eMBB) 场景中，为移动设备间的通信开启了新篇章。随着 5G 新基建的推进，其所带来的变革不会仅限于移动通信领域，还将深入工业互联网、智慧城市、自动驾驶、智慧医疗等各行各业。在安全问题上，5G 网络自身的安全也势必会影响其所赋能的垂直行业的安全。而安全的价值通常随着业务价值的提高而提高，毫无疑问，5G 安全的重要性正在逐步提升。

3.5.1 热点安全事件

首先，我们先从 5G 网络爆出的安全漏洞入手，对 5G 的安全隐患进行简要探讨。

2021 年 2 月 4 日，移动安全公司 AdaptiveMobile 发现 5G 架构的网络切片和虚拟化网络功能存在安全漏洞，恶意攻击者可能利用此漏洞跨越 5G 网络的各个不同网络切片，发动数据访问和拒绝服务攻击，并其发现的安全漏洞编号为 CVD-2021-0047[1]。

CVD-2021-0047 造成的主要影响是通过攻陷某一切片并对其他切片资源进行访问，进而获取未经授权访问的数据或发起 DoS 攻击。其实现过程图 3.13 所示。

[1] https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements/

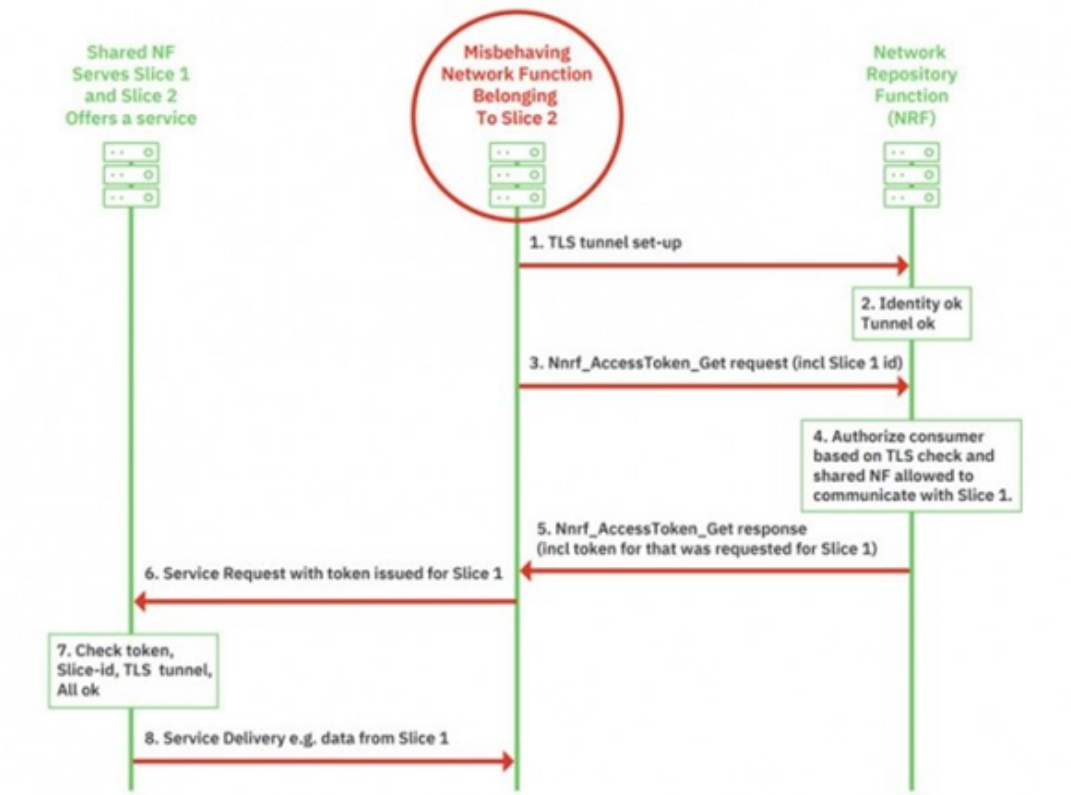


图 3.13　CVD-2021-0047 漏洞利用过程 [1]

AdaptiveMobile 表示，“5G 基于服务的架构可以提供多项业务功能，其中涵盖从前几代网络技术中汲取的宝贵经验。但另一方面，5G 基于服务架构本身仍是一种全新的网络概念，要求将网络开放给新的组织或服务，而这必然会带来新的安全挑战”。

上述攻击之所以有望奏效，是因为 5G 基于服务的架构在设计中，缺少信令层请求的切片身份认证机制。基于服务的架构虽然增加了 5G 网络切片的灵活性，但同时也带来了与 CVD-2021-0047 同类的未授权访问，横向移动攻击等安全风险。为了保证必要的安全性，切片虽然已经做了有效的网络隔离机制，但在运营商网络运行过程中发生的配置错误难免发生。例如在 2021 年 10 月 14 日，由于韩国电信运营商 KT 由于网络路径设置错误导致的大量用户通信受到影响 [2]。同样的，配置错误也会导致某些切片被暴露在公网中，从而被攻击者利用。因此，为切片间通信配置有效的认证授权机制和异常检测手段是十分必要的。

[1] https://zhuanlan.zhihu.com/p/360792410
[2] https://www.reuters.com/world/asia-pacific/police-investigate-network-outage-south-korean-telco-kt-2021-10-25/

3.5.2 政策和市场

本节将从政策和市场投入两方面展示 5G 安全的市场现状。

在国家政策方面，工信部于 2021 年 6 月在北京召开全国会议[1]，部署推进 5G 安全工作。会议指出，当前我国 5G 网络建设步伐加快，已建成 5G 基站近 85 万个，形成全球最大的 5G 独立组网网络。一方面 5G 继承了 4G 网络分层分域的安全架构并在服务域安全、统一认证框架、隐私保护和网间漫游安全等方面具备了比 4G 更强的安全能力。另一方面，由于 5G 引入网络功能虚拟化、网络切片、边缘计算等新技术，网络架构向云网融合，给网络建设运行和业务应用带来新的安全风险挑战。

市场投入方面，MARKETSANDMARKETS 在 2021 年 2 月发布了 5G 安全市场投入报告[2]。报告表明，全球 5G 安全市场投入在 2020 年达到 5.8 亿美元，并将以每年 44.3% 的比例增长，直到 2026 年预计达到 52.26 亿美元。

图 3.14　2020-2026 全球 5G 安全市场投入增长趋势图

此外，报告中还指出目前在全球 5G 安全市场进行投入的厂商包括 A10 Networks, Akamai, Allot, AT&T, Avast, Check Point, Cisco, Clavister, Colt Technology, Ericsson, F5 Networks, ForgeRock, Fortinet, G+D Mobile Security, 华为, Juniper Networks, Mobileum, Nokia, Palo Alto Networks, Positive, Technologies, Radware,Riscure, Spirent, Trend Micro 以及中兴。

[1] http://www.gov.cn/xinwen/2021-06/08/content_5616194.htm
[2] https://www.marketsandmarkets.com/Market-Reports/5g-security-market-261636732.html?gclid=EAIaIQobChMIuqGv8qWA9AIVKO_tCh1giAR1EAAYAiAAEgK0NfD_BwE

同时，国内安全厂商在 5G 安全领域也都作了相应的投入。对此，信通院在 2020 年 12 月发布的《中国网络安全技术与企业发展研究报告》[1] 展示了各大安全厂商在 5G 安全方向的投入与进展。其具体内容如表 3.7 所示。

表 3.7　国内安全厂商在 5G 领域的研究与实践投入

企业名称	技术领域 / 特点
山石网科	• 针对边缘计算场景提供租户、虚机、容器等层面的安全方案，提供资产、流量、威胁可视化能力和精细的访问控制能力； • 探索将零信任、人工智能等应用到 5G 安全之中。
绿盟	• 采用漏洞扫描、渗透测试、配置检查抽样、日志分析和顾问访谈等技术手段，对 5G 网络中各目标网络单元的业务及应用安全、拓扑安全、物理环境安全等进行基础调研核查及支撑服务。
华信设计院	• 提升 VNF 自身安全防护能力，对 gNB 基站设备、虚拟化网元实施安全防护与加固措施，针对虚拟化网元和 MEC 服务器，提供内置安全检测、防护以及按需动态服务的能力。
中兴	• MEC 设备中内嵌了自研的 vFW 组件，提供 MEC 边界安全防护以及 MEC 内部安全域间的安全防护能力。
恒安嘉新	• 利用边缘轻量级安全 Agent 与云端联动的方式实现虚拟机安全可视化管理和检测；从基础设施安全、边缘网络安全等多个维度实现对 MEC 分流网关的安全防护。
安恒信息	• 边缘统一安全管理中心主要完成对安全日志和流量的风险要素统一感知、关联分析、策略制定和自动任务编排等； • 完成相关的云端和边缘侧的云边安全协同机制。
天融信	• 研究实现 5G 网络各切片内的保护 / 管控、切片间隔离等安全增强加固，和基于轻量化架构实现 5G 网络二次认证、上层业务认证、跨域身份认证等技术能力等。
安博通	• 兼容多种虚拟化与云平台，通过预配置进行自动部署运行，灵活扩展能力可达到对应用业务或租户的安全与资源控制需求，提供不同安全等级应用之间的安全隔离和安全防护。
国瑞数码	• 研究开发行业特征等分类模型以及安全风险检测分析模型； • 拓展对 5G 新技术新应用的监测能力及安全风险发现能力，实现 5G 环境下多种核心应用场景的安全态势感知。

3.5.3　发展趋势

5G 已成为现阶段并将是未来十几年内的通信基础设施，它在业务上的重要性是毋庸置疑的。如何让 5G 安全稳定地为社会各界提供通信服务将是各大运营商与安全厂商需要持续承担的责任。

从市场现状来看，5G 安全领域有着较好的市场前景，且将在接下来的几年内持续繁荣。其中，5G 安全的主要市场机遇来源于面向大型企业、政府以及工业部门的 5G 专网。5G 专网将为自动驾驶、互联工厂、互联医疗、智能零售以及乡村宽带连接等垂直行业定义新的通信方式。随着 5G 专网在各行各业的部署与应用，5G 专网安全也将势必开启新的市场。

从技术角度来看，欧盟网络安全局 (ENISA) 在 2020 年 12 发布的“enisa-threat-landscape-report-for-5g-networks”[2] 报告中展示了 5G 各项新技术为 5G 网络带来的安全风险，

[1] http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/P020201223685469901767.pdf
[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

为安全策略的部署提供了思路。结合第一章提到的安全漏洞 CVD-2021-0047 与已有的 5G 安全研究经验，笔者认为 5G 网络所面临的安全问题主要源自新架构与新技术。新架构是指相比 4G 网络更加灵活开放的 SBA 服务化架构。这种架构主要应用在 5G 核心网和网络切片中。CVD-2021-0047 已经表明切片间未配置合适的身份认证机制会带来安全风险。同样的，部署在这种架构下的 5G 核心网中的各个网络功能也面临着这类风险。因此，为基于 SBA 架构的网络功能与切片进行有效地安全防护是必要的。而新技术则主要是指新引入 5G 网络的网络切片、网络功能虚拟化 (NFV)、软件定义网络 (SDN)、多平台边缘计算 (MEC)、管理与编排系统 (MANO)、5G 无线接入网 (NR-RAN) 等新技术。这些新技术的引入也将带来各样的新的安全问题。那么，还需要面对这些新技术所带来安全隐患进行合适地安全部署。

盼望 5G 在促进通信领域与各垂直行业高速稳健发展的同时，可以安全稳定地为社会各界提供服务。

3.6 人工智能安全

人工智能（Artificial Intelligence, AI）技术的蓬勃发展，拓展了数字世界的边界，全面促进了信息系统、物理系统与社会系统的融合，给各行业技术的升级提供了充分的驱动力。于此同时，网络空间攻防对抗战场快速延伸拓展到 AI 技术领域与场景中，AI 安全问题亦渗透到各行业、技术当中，成为不可忽视的安全风险要素之一。

3.6.1 热点安全事件

3.6.1.1 自动驾驶引发交通事故

基于高性能视觉传感器和基于 AI 的机器视觉模型及算法，是支撑当今自动驾驶技术的关键技术实现。然而，自 2016 年以来，美国国家公路交通安全管理局 NHTSA 已针对 31 起 Tesla 撞车事故进行深入调查，发现其中有 25 起事故涉及其 Autopilot 自动辅助驾驶技术的应用 [1]。在高速行驶或复杂路况条件下，自动驾驶、自动辅助驾驶技术依赖人工智能系统的感知与决策，给行驶安全带来了新的技术风险。一方面，机器视觉技术尚存动态环境下的识别鲁棒性、稳定性挑战，错误的障碍物识别和行驶环境判断，将导致自动行驶操作失效。另一方面，网联汽车的决策系统存在脆弱性暴露风险，带来全新的网络攻击面。Tesla Autopilot 关联的撞车事故，其底层技术原因仍需深入调查，但是不可避免了引发了社会和技术研发领域对 AI 在自动驾驶领域的安全性，以及 AI 负责任、可审计方面的广泛讨论。

[1] https://apnews.com/article/technology-business-61557d668b646e7ef48c5543d3a1c66c

3.6.1.2 TensorFlow 平台漏洞数量大幅增加

Google 开源平台 TensorFlow 是机器学习和人工智能领域应用最为广泛的框架之一，诸多厂商基于该框架的不同版本进行应用程序开发。随着该平台的深入应用功能，其安全性问题得到了安全业界的广泛关注。相关统计显示，自 2019 年以来，TensorFlow 代码漏洞数大幅增加：2019 年、2020 年、2021 年公开的 CVE 漏洞数分别为 7、25 和 201[1]。其中漏洞涉及拒绝服务攻击、远程代码执行、内存破坏、功能绕过等多种类型的漏洞。伴随着 AI 技术在各行业的广泛应用，其开发平台的安全性已成为不可忽视的关键要素。

表 3.8 TensorFlow 年度 CVE 漏洞统计

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2019	7	1	1	4											
2020	35	6	2	8	3										
2021	201	41	6	38	1					8	1				
Total	243	48	9	50	4					8	1				
% Of All		19.8	3.7	20.6	1.6	0.0	0.0	0.0	0.0	3.3	0.4	0.0	0.0	0.0	

基于 Deepfake 合成语音与视频的诈骗。Deepfake 技术基于语音和图像生成模型，能够实现对特定人声音与视频影像的仿冒，越来越多的被犯罪组织和团伙利用，来实现以假乱真的定向诈骗。据美国 Forbes 最新报道，迪拜调查人员正在调查一起大型抢劫案，其中使用了 AI 语音克隆技术，涉及金额达 3500 万美元[2]。国内也有类似的案件，2020 年湖南省破获了一起利用人工智能语音机器人帮助网络犯罪案，抓获犯罪嫌疑人 19 人，扣押涉案现金 100 余万元，冻结涉案资金 1000 余万元[3]。Deepfake 技术能够基于有限的定向样本采集，实现还原度极高的虚假内容合成，实现身份仿冒。在大众缺乏安全专业的安全意识培训、个人信息泄露频发的背景下，基于 Deepfake 技术的诈骗事件已成为最危险的网络犯罪类型之一。

3.6.2 政策和市场

AI 安全技术产业具有广阔的市场空间。在产业政策层次，2017 年，《新一代人工智能发展规划》指出，“在大力发展人工智能的同时，必须高度重视可能带来的安全风险挑战，加强前瞻预防与约束引导，最大限度降低风险，确保人工智能安全、可靠、可控发展。”2021 年 11 月 18 日，中共中央政治局召开会议，审议《国家安全战略（2021 — 2025 年）》。会议指出，必须坚持把政治安全放在首要位置，统筹做好政治安全、经济安全、社会安全、科

[1] https://www.cvedetails.com/product/53738/Google-Tensorflow.html?vendor_id=1224
[2] https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=51ba14a37559
[3] http://cyberpolice.mps.gov.cn/wfjb/html/gzdt/20200728/4739.shtml

技安全、新型领域安全等重点领域、重点地区、重点方向国家安全工作。其中，加快提升生物安全、网络安全、数据安全、人工智能安全等领域的治理能力，是践行五大安全领域的关键任务之一。可见，人工智能安全是社会经济数字化转型中，需要重点考虑的技术领域之一。

在市场投入层次，可以分别从 AI 安全性技术领域和 AI 安全防护领域来看。在 AI 安全性方面，《人工智能安全白皮书（2020）》对国内行业技术进展了简要总结，如表 3.9 所示 [1]。

表 3.9　国内 AI 安全性领域技术进展情况

企业名称	技术领域 / 特点概要
百度	百度是国内最早研究 AI 模型安全性问题的公司之一。当前百度建立了一套可衡量深度神经网络在物理世界中鲁棒性的标准化框架。事实上，物理世界中使用的模型往往与人们的衣食住行相关（如无人自动驾驶、医疗自动诊断等），这些模型一旦出现问题，后果将非常严重。因此，该框架首先基于现实世界的正常扰动定义了可能出现威胁的五大安全属性，分别是光照、空间变换、模糊、噪声和天气变化；然后，针对不同的模型任务场景，制定不同的评估标准，如非定向分类错误、目标类别错误分类到评估者设定的类别等标准；最后，对于不同安全属性扰动带来的威胁，该框架采用了图像领域中广为接受的最小扰动的 Lp 范数来量化威胁严重性以及模型鲁棒性。
腾讯	腾讯公司针对 AI 落地过程中面临的各类安全问题进行了细致的划分，具体分为 AI 软硬件安全、AI 算法安全、模型安全、AI 数据安全和数据隐私等部分。软硬件安全主要是考虑到部署 AI 模型的软件和硬件层面可能存在的安全漏洞，如内存溢出、摄像头劫持等问题；AI 算法安全主要考虑深度学习存在对抗样本的问题，容易出现错误的预测结果；模型本身的安全则涉及到模型窃取，这一问题目前实现方式比较多，常见的方法是直接物理接触下载模型并逆向获取模型参数，以及通过多次查询来拟合“影子”模型实现等价窃取；此外，模型的训练数据也会被污染，开源的预训练模型可能被恶意埋入后门，这些问题都被划分为 AI 模型的数据安全问题；当然，模型训练使用的数据集也会涉及用户的隐私，因此攻击者可能也会通过查询获取用户隐私。为了缓解这些问题，腾讯安全团队借助 AI 能力，针对性地构建了多种攻击检测技术。
华为	华为公司同样对 AI 安全问题展开了深入的研究，其将 AI 系统面临的挑战分为 5 个部分，包括软硬件的安全、数据完整性、模型保密性、模型鲁棒 性和数据隐私。其中，软硬件的安全涉及应用、模型、平台、芯片和编码中可能存在的漏洞或后门；数据完整性主要涉及各类数据投毒攻击；模型保密性则主要涉及到模型的窃取问题；模型鲁棒性考虑训练模型时的样本往往覆盖性不足，使得模型鲁棒性不强，同时模型面对恶意对抗样本攻击时，无法给出正确的判断结果等问题；数据隐私考虑在用户提供训练数据的场景下，攻击者能够通过反复查询训练好的模型获得用户的隐私信息。 为了应对这些挑战，华为主要考虑三个层次的防御手段：攻防安全、模型安全和架构安全。其中，攻防安全考虑针对已知的攻击手段，设计针对性的防御机制来保护 AI 系统，经典的防御技术包括对抗训练、知识蒸馏、对抗样本检测、训练数据过滤、集成模型、模型剪枝等。而针对模型本身存在的安全问题，考虑包括模型可检测性、可验证性和可解释性等技术，以提升模型应对未知攻击的能力。在业务中实际使用 AI 模型，需要结合业务自身特点，分析判断 AI 模型架构安全，综合利用隔离、检测、熔断和冗余等安全机制设计 AI 安全架构与部署方案，增强业务产品、业务流程与业务功能的健壮性。
RealAI	RealAI 是一家专注于从根本上增强 AI 的可靠性、可信性以及安全性的创业公司。该公司通过黑盒和白盒方式，对目标模型进行对抗样本攻击，并通过检测器和去噪器等方式构建模型的 AI 防火墙；此外，它们也考虑了模型窃取和后门检测等问题。

整体来看，AI 安全性，包括其鲁棒稳定性、透明可解释性、公平可信任性等多方面的属性，已成为 AI 技术深入应用过程中不可回避的关键研究领域。特别是在涉及关键领域，如经济、政治、军事领域的智能决策方面，这些特性是 AI 能否正确发挥其作用的必要条件。

在 AI 安全防护领域，国内外安全厂商积极投入，积极布局，升级传统的安全防护能力。国外相关安全厂商的 AI 技术特点，总结在表 3.10 中 [2]。

[1]　《人工智能安全白皮书（2020）》
[2]　https://www.comparitech.com/blog/information-security/leading-ai-cybersecuritycompanies/

表 3.10　国外 AI 安全防护领域技术进展情况

企业名称	技术领域 / 特点概要
CrowdStrike	CrowdStrike Falcon 系统的秘密武器是基于 AI 的检测系统，称为用户和实体行为分析 (UEBA)。 UEBA 概念是推动系统安全行业向前发展的重大创新之一，摆脱了传统易失效的抗病毒检测模型。CrowdStrike 采用的人工智能方法监控端点上的所有活动，分析每个用户的活动并观察在任何正常日子运行的所有系统进程。这建立了常规活动的基线。系统会继续监视所有进程，并在用户突然执行不同操作或之前未遇到的系统进程启动时发出警报。这是一个吸引额外活动跟踪程序的标志。
Darktrace	Darktrace 开发了企业免疫系统（Enterprise Immune System, EIS），作为其所有网络安全产品的平台。 EIS 使用 AI 方法并通过无监督机器学习填充状态规则库。 EIS 安装在网络上时需要做的第一件事是建立正常活动的基线。 这在 Darktrace 术语中被称为“生活模式”。 每个网络的流量模式、网络上每个设备的活动以及每个用户的行为都被建模以提供这种标准行为的记录。EIS 系统建立正常行为基线意味着它不必维护威胁数据库。 网络上的异常事件被视为威胁。检测到异常会触发自动响应，这也依赖于人工智能技术。 创建了一个完整的 AI 驱动的入侵防御系统 (IPS)。 人工智能还部署在 Darktrace Threat Visualizer 中，将具有相似特征的攻击联系在一起，使计划人员能够了解对企业资源的威胁的完整复杂性。
Cynet	Cynet 有一个产品，称为 Cynet 360。这是一个完整的网络安全系统，包括 抗病毒端点保护、设备检测、威胁预测、用户行为建模和漏洞管理。系统有一个发现阶段，它使用标准的网络拓扑映射方法来发现所有网络设备和端点。该系统检查事件日志并跟踪流量模式以建立常规网络活动的基线模型。 此日志记录阶段为流量来源和行为类型创建风险等级。 通过这些操作，Cynet 360 创建其 AI 知识库并可以开始威胁监控。
FireEye	FireEye 提供全套安全产品、情报和服务，以保护客户免受网络威胁。 FireEye 是第一个使用虚拟沙箱（称为 FireEye MVX）来识别绕过基于签名的传统解决方案的新威胁的公司。 FireEye Helix 安全运营平台。 FireEye Helix 将客户的安全基础设施集中起来，并使用人工智能来识别新威胁并自动执行人和机器的响应。
Check Point	该公司没有生产特定的基于 AI 的威胁管理产品，而是投资开发了三个 AI 驱动的平台，这些平台为许多业务的关键产品做出了贡献。它们是 Campaign Hunting, Huntress, and Context-Aware Detection (CADET)。Campaign Hunting 是一项集中式服务，可使用最新的攻击媒介和防御策略更新客户端威胁检测系统。这类似于防病毒提供商使用的病毒数据库。数据传输是双向的，因为当检测到任何新威胁时，现场实施会向 Check Point 实验室报告。该工具约占 Check Point 成功威胁预防事件的 10%。Huntress 是一个用于即将引入网络的软件的沙箱。基于人工智能的系统分析被检查程序的性能和行为，如果遇到异常，则向 Check Point 的中央系统报告。再次与 Check Point 的所有客户共享为此分析得出的解决方案。CADET AI 引擎实时聚合事件数据，因此可以阻止同时利用看似无关资源的攻击媒介。 CADET 的无监督机器学习功能磨练了威胁数据库，以减少严重的误报。它创建了一个数字安全分析师并自动触发预防措施。
Symantec	赛门铁克 Targeted Attack Analytics (TAA) 于 2018 年 5 月发布。它使用无辅助机器学习对网络上的行为模式进行建模并创建性能基线。任何与常规活动的偏差都会引发警报。 TAA 的 AI 功能位于赛门铁克网络防御平台之上，该平台能够同时从网络上的多个点收集性能数据。 TAA 主要集成到赛门铁克高级威胁防护系列产品中，但它可能最终会推广到所有赛门铁克网络安全软件包。
Sophos	两个主要的基于 AI 的 Sophos 产品是用于端点保护的 Intercept X 和用于保护网络的 XG 防火墙。Intercept X 使用人工智能来避免需要从中央位置分布的威胁数据库。该服务的热点是由 Invincea 开发的深度学习神经网络。这会监控受保护设备上的常规活动，并在发生意外事件时发出警报。端点检测和响应 (EDR) 会触发工作流和操作，以在检测到漏洞后关闭漏洞并隔离感染。XG 防火墙是网络的硬件设备。 它的仪表板提供有关网络上当前事件和流量的反馈，但其主要价值在于其自动响应机制，可以强制执行安全性，而不会因人为干预而造成延迟。
Fortinet	该公司开发了安全结构的概念来表达从企业中的多个点收集网络活动点以搜索威胁的策略。 此类服务的通用行业术语是“统一威胁管理”。 此工作流包括端点保护、访问保护、应用程序监控（例如电子邮件和 Web 安全）和高级威胁保护。组织中的各种数据收集点收集威胁情报，这些情报在网络的一个中心点进行编译，以监控入侵或感染。 Fortinet 开发了基于 AI 的自我进化检测系统 (SEDS) 作为安全结构的主要分析引擎。 防御机制需要访问网络资源，例如防火墙规则和操作系统，以使其能够触发自动防御操作以阻止任何检测到的威胁。
Cylance	Cylance 的所有产品都集成了 AI 技术。Cylance Protect 是一个端点安全系统。 从本质上讲，这是一个基于 AI 的反恶意软件系统，它寻找设备上活动模式的变化，而不是依赖于从 AV 提供商通过互联网分发的威胁列表。 除了检查活动外，该系统还控制对设备的访问。Cylance Optics 是 Cylance Protect 的企业版。 威胁检测应用于系统上的所有设备并集中存储。 对检测到的入侵的响应是自动触发的，使其成为经典的 IPS。Cylance Threat Zero 是该公司的咨询部门。 顾问提出混合产品，还可以定制保护软件。Cylance Smart Antivirus 是另一款基于 AI 的 AV 系统，适用于家庭用户和小型企业。
Vectra	该公司将其活动集中在一种称为 Cognito 平台的产品上。 这是一个威胁检测系统，它部署 AI 方法来建立整个企业的活动基线并识别异常情况。 该系统不包括对检测到的威胁的自动响应，因此不能将其归类为统一威胁管理器或入侵防御系统。该系统的分析引擎可在线访问，称为 Cognito Recall。 Cognito 平台收集的数据可以传输到此存储和分析工具，或者您可以将数据通过管道传输到 Zeek 工具（以前称为 Bro）并使用这些工具分析数据并设置自动响应。 数据传输和格式化由 Cognito Stream 执行。 另一个模块 Cognito Detect 允许创建威胁配置文件并具有一些自动预防措施。

从国外 AI 安全防御技术的发展来看，用户行为分析、基线分析与异常检测、终端上的分析增强、多源日志的关联融合，是 AI 防御技术应用的几个重要技术发力领域。与 AI 的安全性研究类似，在 AI 安全防御应用方面，同样需要在动态环境下的自适应性、透明可运营性、隐私防护性等多方面的技术新要求。随着网络安全攻防对抗态势的升级与安全大数据的规模效应凸显，利用 AI 技术促进防御自动化，降低对攻击者与攻击行为的发现时间、响应时间，已成为必然趋势。

3.6.3 发展趋势

随着 AI 技术的成熟与产业化应用，AI 安全性问题逐渐暴露，相关事件频发，愈发得到国家、市场、产业的关注。AI 技术的鲁棒安全，直接关系到 AI 技术应用场景下物理设备、信息系统以及人和社会的安全性与稳定性。可以预见，AI 技术的可信任性已成为现阶段 AI 技术应用的瓶颈和重点攻关领域。于此同时，网络威胁组织、犯罪团伙，利用开源、定制的 AI 技术，能够搭建更加自动化、更有针对性、更具杀伤力的攻击技术平台和产业链条，在网络攻击面拓展、攻击技战术更精细化的同时，攻击者的行踪更加隐匿，大幅增加了网络空间防御的难度。为此，利用 AI 技术，赋能安全防御，挖掘安全大数据的洞见深度与潜在关联，提升防御平台检测、溯源、响应流程的自动化水平，已成为安全产业发展的必然趋势。

3.7 云安全

时至今日，对于大众来说，云计算已经不是一个陌生的词汇。对于大中小企业来说，业务云化也不再是疑虑重重的决策，而是降本增效的首选方案。然而，云计算面临的风险和威胁却并未消失，反而更加复杂。随着越来越多的业务云化，云安全也必将得到越来越多的重视。安全的云计算才会带来长期稳定的业务增益。

3.7.1 热点安全事件

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，TeamTNT 团伙利用云原生相关技术发起了多次攻击 ..... 这些事件表明，“上云”虽好，“云上”却并不平静。

接下来，我们将为大家介绍 2021 年两个典型的云安全事件。

3.7.1.1 TeamTNT 组织对云计算目标进行多次攻击

据相关报道[1]，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[2]。
- 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[3]。
- 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”[4]。
- 2021 年 10 月，TeamTNT 被曝在 Docker Hub 上投放恶意镜像[5]。
- 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[6]。

这些由 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。

[1] https://fachanwalt-it.blogspot.com/2011/12/hackerangriff-anonymous-goldde-lka.html
[2] https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
[3] https://www.trendmicro.com/en_nl/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html
[4] https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera
[5] https://www.uptycs.com/blog/team-tnt-deploys-malicious-docker-image-on-docker-hub-with-pentesting-tools
[6] https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html

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。

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。

3.7.1.2 Azure ChaosDB 漏洞影响成千上万公司

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。

从 2019 年起，微软向 Cosmos DB 中增加了 Jupyter Notebook 的功能[1]，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[2]，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。

[1] https://www.wiz.io/blog/chaosdb-how-we-hacked-thousands-of-azure-customers-databases
[2] https://www.wiz.io/blog/chaosdb-explained-azures-cosmos-db-vulnerability-walkthrough

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 [1]。

   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[2]。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。

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。

3.7.2 政策和市场

本节将从政策和市场投入两方面展示云安全的市场现状。

政策方面，2021 年 7 月 12 日，工信部公开征求对《网络安全产业高质量发展三年行动计划 (2021-2023 年)(征求意见稿)》的意见。征求意见稿指出 [3]：面向多云、云原生、边缘云、分布式云等新型云计算架构，发展多云身份管理、云安全管理平台、云安全配置管理、云原生安全、云灾备等技术产品，推动云架构安全发展。面向云环境中云服务器、虚拟主机、网络等基础资源，加强基础信息采集水平，提升能够面向双栈（IPv4、IPv6）的流量可视化、微隔离、软件定义边界、云工作负载保护等安全产品能力，保障云上资源安全可靠。面向云上业务、应用等服务，提升安全访问服务边缘模型、云 Web 应用防火墙、云上数据保护等安全产品效能，保障云上业务安全运行。

[1] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=linux
[2] https://docs.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16
[3] https://wap.miit.gov.cn/gzcy/yjzj/art/2021/art_34f89fff961b4862bf0c393532e2bf63.html

市场方面，国际市场研究机构 ResearchandMarkets 于 2021 年 4 月发布的全球云安全市场报告[1]显示，全球云安全市场在 2021 年为 348 亿美元，预计将在 2026 年达到 676 亿美元，复合年均增长率约为 14.2%。市场增长的驱动力主要是持续增加的云服务依赖、网络犯罪和新型网络攻击、BYOD（Bring Your Own Device）与 CYOD（Choose Your Own Device）的趋势；新的市场机会包括政府推进的智慧基础设施项目、托管安全服务等。同时，云安全市场的增长也面临着一些制约和挑战。其中，企业与安全服务提供商缺乏强力合作、高级专家人才紧缺、严格的政府法规是主要制约因素。

3.7.3 发展趋势

云计算与各行各业 IT 基础设施进一步融合，云或是基础，或是组件。例如，5G、边缘计算和工业互联网，都需要云计算技术构建云化的基础设施或编排平台，那么这些新型系统的基础设施安全，其实本质上就是云计算 IaaS/PaaS/CaaS 的安全；此外，如欺骗技术、靶场技术等新的网络安全机制，或多或少地使用了虚拟化、容器等技术，因而，这些云计算技术融入后，就形成了新的、普适的安全技术，即“just security”。

一方面，云化的基础设施和平台需要安全防护，用传统安全手段赋能云计算；另一方面，云计算的各种新技术、新理念（如软件定义、虚拟化、容器、编排和微服务等），也在深刻变革着当前的安全技术发展路线，因而，未来的云安全，一定会将“云”这个定语去除，等价于安全本身，即安全技术必然覆盖云计算场景，安全技术必然利用云计算技术。

如果说云安全的未来等价于纯安全，而云计算的下半场是云原生，那不妨也做个推论：云原生的未来也会等价于原生安全。如果云原生安全成为原生安全，那就说明云原生已经融入到了各行各业，成为普适的云计算场景。事实上，随着国家大力推动新基建战略，包括 5G、物联网、工业互联网等信息基础设施，云计算、人工智能等新技术基础设施，数据中心等计算基础设施等。而这些基础设施，未来或多或少都会与云原生技术有所联系。

未来，我们十分看好云安全的市场前景，重视云上威胁和安全事件，建立健全云安全防御体系，为云上业务保驾护航。

[1] https://www.researchandmarkets.com/reports/5317111/global-cloud-security-market-2021-2026-by?utm_source=BW&utm_medium=PressRelease&utm_code=r7xvrv&utm_campaign=1572419+-+Global+Cloud+Security+Market+(2021+to+2026)+-+by+Application%2c+Security+Type%2c+Service+Model%2c+Deployment%2c+Organization+Size%2c+Industry+Vertical+and+Geography&utm_exec=jamu273prd

3.8 区块链安全

区块链是新一代数字技术的重要组成部分，是由分布式网络、加密技术、智能合约等多种技术集成的数字经济基础设施。区块链技术和产业在全球范围内快速发展，应用已经延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。下面通过区块链安全事件和分析、政策和市场投入、安全发展趋势和展望三个维度进行观察。

3.8.1 热点安全事件

随着数字经济的发展，区块链技术也越来越多的被广泛应用。但是伴随着产业和应用的发展区块链的安全问题也越来越突出，据不完全统计，2021 年区块链被黑客攻击损失的数字货币价值已达 71 亿人民币。攻击的类型主要有欺骗、利用智能合约漏洞攻击、钓鱼攻击等方式实施攻击。

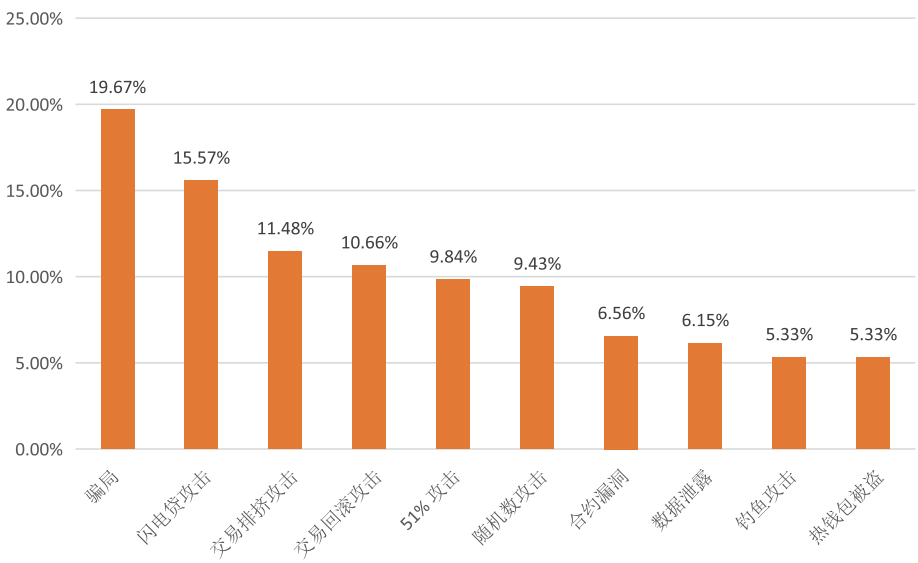


图 3.15 区块链安全事件攻击类型统计

2021 年 8 月 10 日，跨链互操作协议 Poly Network 突遭黑客攻击，在 Poly Network 现已集成的三大主流生态（以太坊、BSC、Polygon）上，黑客分别盗走了 2.5 亿、2.7 亿、8500 万美元的加密资产，损失总额高达 6.1 亿美元。此次攻击事件是黑客利用合约漏洞对跨链合约 EthCrossChainManager 修改了 keeper，黑客把 keeper 改为自己的账户地址后，进行了数字资产的转移，成功完成了攻击。后来黑客迫于压力基本全部退还了此次攻击非法所得的数字资产。此次攻击，黑客成功获得的数字货币详情如下：

- BSC 资产：6613 枚 BNB、87,603,671 枚 USDC、26,629 枚 ETH、1,023 枚 BTCB、32,107,854 枚 BUSD
- 以太坊资产：96,389,444 枚 USDC、1,032 枚 WBTC、673,227 枚 DAI、43,023 枚 UNI、14 枚 renBTC、33,431,197 枚 USDT、26,109 枚 WETH、616,082 枚 FEI
- Polygon 资产：85,089,719 枚 USDC

此次安全事件主要原因是智能合约的安全漏洞。虽然，poly network 项目的审计是由 NCC Group 完成，以太坊智能合约审计由 Certik 完成，但依然存在如此大的漏洞。

2021 年 5 月份，美国科洛尼尔管道运输公司（Colonial Pipeline）公司遭遇一个网络犯罪团伙攻击后中断网络运营后，科洛尼尔管道运输公司向黑客支付给了黑客 75 个比特币近 500 万美元的巨额赎金。目前，这一输油管道系统已开始恢复运营。后来联邦调查据对此次事件进行调查，并追回了勒索赎金的大部分数字资产 63.7 个比特币。美国联邦调查局调查发现，黑客网络攻击事件是由名为“阴暗面”（DarkSide）的网络犯罪团伙发起，在过去三年，DarkSide 曾发起多起网络攻击，造成数百亿美元损失。执法人员使用了区块链账本实时监控工具，追踪了比特币的数笔交易，并最终确认了接收赎金的地址。此外，他们通过破获黑客的服务器获取到了私钥（private key）追回了勒索的数字资产。

```
黑客勒索美国油管事件：
起点：fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264  #此交易油管公司给黑客的赎金交易

bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf              2            74.99998307  #给黑客的赎金 75BTC
bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45              2            63.74998561
bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45              0.0            0.04976631
bc1qu57hnxf0c65fsdd5kewcsfeag6sljgfhz99zwt              1            11.24962019
bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607              107.82             107.8
3EYkxQSUv2KcuRTnHQA8tNuG7S2pKcdNxB              1            63.7
bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq              2            69.60422177
bc1qpx7vyv5tp7dm0g475ev527krg764t73dh77gls              63.69996546            63.69996546 #此交易为FBI控制
bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq              1            5.90422177
bc1qvjh9cq6qlj4f4q5vxnkgt25mc6qld04vv20fhe              5.90419482            5.90419482
"""
```

图 3.16　美国油管公司勒索事件账本追踪

3.8.2　政策和市场

近几年，区块链迎来政策风口，区块链行业高速发展。区块链战略新兴产业地位持续提升。2020 年 4 月 20 日，国家发改委新闻发布会中，国家发改委创新和高技术发展司司长伍浩表示新型基础设施主要包括信息基础设施、融合基础设施和创新基础设施三个方面的内容，以

人工智能、云计算、区块链等为代表的新技术基础设施是信息基础设施的一个重要组成部分。区块链被正式纳入新基建范畴，其产业基础性得到认可。2019 年 10 月 24 日，中共中央政治局计算机行业深度研究将区块链作为核心技术自主创新的重要突破口后，国家层面政策出台进一步加快。2020 年 1 月央行、交通运输部、国家外汇管理局等 10 部委连发 11 则促进区块链与各领域结合的政策信息，并且区块链在多项技术中排列逐步靠前，全国 31 个省市也密集出台了一系列产业支持政策，区块链在产业变革中的作用的受重视程度显著提高。

2021.4 工信部《区块链与数据安全治理白皮书》梳理区块链与数据安全治理的政策法规、技术标准和产业现状，研究总结区块链与数据安全治理结合的技术可行性，探索利用区块链技术助力数据安全治理，为行业发展提供参考，推动数据安全治理工作有序开展。

2021 年 6 月工信部关于《中央网络安全和信息化委员会办公室关于加快推动区块链技术应用和产业发展的指导意见》中指出围绕制造强国和网络强国战略部署，以培育具有国际竞争力的产品和企业为目标，以深化实体经济和公共服务领域融合应用为路径，加强技术攻关，夯实产业基础，壮大产业主体，培育良好生态，实现产业基础高级化和产业链现代化。推动区块链和互联网、大数据、人工智能等新一代信息技术融合发展，建设先进的区块链产业体。

表 3.11　2016 年至今我国区块链相关政策

时间	发布机构	政策名称
2021.6	工信部	关于加快推动区块链技术应用和产业发展的指导意见
2021.4	工信部	《区块链与数据安全治理白皮书》
2021.3	中国通信院	《区块链安全能力测评与分析报告（2021 年）》
2021.3	国家工业信息安全发展研究中心	《区块链生态环境监管应用白皮书》
2020.1	国务院	2020 年中央一号文件
2019.10	中共中央政治局	第十八次集体学习
2019.8	国务院	《产业结构调整指导目录（2019 年本）》
2019.5	国家网信办	《推动建设区块链开源社区》
2019.1	国家网信办	《区块链信息服务管理规定》

中国区块链的市场规模也随着政策的引导高速的增长，2021 年中国区块链市场规模国内的区块链应用以联盟链为主，均为无币区块链，对于攻击者来说，很难从攻击中获利，攻击者能够做的就是对数据的破坏等，而区块链的分布式特性，使其天然具备数据抗毁性，少量节点的数据被破坏对整体系统应用没有大的影响。因此，到目前为止，联盟链的安全问题并不突出。

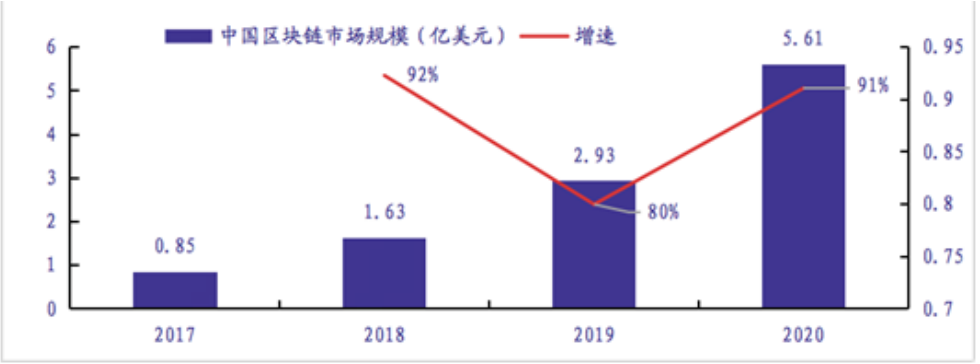


图 3.17　中国区块链市场规模及预测（亿美元）

3.8.3　发展趋势

2021 年区块链方面是分布式金融（DeFi）和非同质化代币（Non-Fungible Tokens NFT）增长最迅速的一年，DeFi 服务中存入的资金总额从 5 亿美元飙升至 2470 亿美元。甚至叫 DeFi 元年和 NFT 元年。DeFi 安全问题是分布式金融服务的最棘手的问题，也制约着 DeFi 的进一步发展，针对 DeFi 漏洞造成的损失截至到 2021 年为止总计约 120 亿美元。

区块链在未来一段时间将会迎来飞速发展，投资呈井喷式增长。据 IDC 数据，2019 年全球区块链应用支出预计为 27 亿美元，同比增长 80%，2023 年全球区块链支出金额将达 159 亿美元，并在 2018—2023 年的五年预测期内实现 60.2%的年复合增长率。其中，银行业将引领预测期内全球区块链支出，占比约 30%。内区块链应用也将持续高速发展。如前所述，国内区块链安全问题并不突出，未来一段时间内的市场规模较小。国内从事区块链安全的企业数量少、规模小，而从事区块链应用的很多，一些头部大企业都纷纷加入。

区块链的智能合约安全仍然是区块链安全方向的主要方向，自动化检测合约漏洞仍然是区块链安全研究的热点，同时区块链账本追踪技术也是区块链安全的另一个安全方向的主要研究点。另外区块链和金融服务、数字经济的结合如 2021 年爆发的 DeFi、NFT 等相关的部署都需要智能合约，智能合约和业务结合的安全需求会随着区块链金融服务的增长而增长。

3.9　供应链安全

随着中大型企业对网络入侵的防护的增强，攻击者的注意力更多地转移到了供应商身上，从历年的攻防演习中也可得出相同的结论：供应商正在成为关键信息基础设施安全防护上最薄弱的关节。

几乎所有企业都在使用来自外部的软硬件。开源经济的繁荣导致没有人愿意从零开始构建他们的技术，在这种习惯的背后存在着巨大的风险。每个购入的产品、下载的应用都潜藏着安全威胁。供应链安全几乎是每家信息化企业都需要面对的安全问题。

3.9.1 热点事件

供应链攻击是一种 APT 的惯用手段。其更像是一种入侵的战术与策略的创新，而非技术本身。因此我们在关注 APT 的先进性时，除了在代码质量上，例如漏洞利用和恶意软件方面，更应关注整体战术策略上的“高级”。供应链攻击是针对攻击目标和目标供应商两个组织发起的一次有关联性的复杂入侵，其中包含了同步规划、协同准备、并行开发，并执行了至少两次有效的攻击。因此在分析供应链攻击事件时我们至少应分析两次针对存在供需关系的不同组织实体的入侵。

根据供应链安全事件类型可推断出目前软件供应链的安全隐患更易引起攻击者的兴趣，因为现代软件产品包含了大量对其他代码的依赖，而这些依赖性代码的内部逻辑是否存在安全风险却又是开发者无暇顾及的，使得挖掘漏洞的难度有所降低，同时利用程序的潜伏性和对抗性也会更好。斯考克罗夫特战略与安全中心（Atlantic Council）的软件供应链安全研究报告统计了安全事件中攻击代码的分布如下图所示。

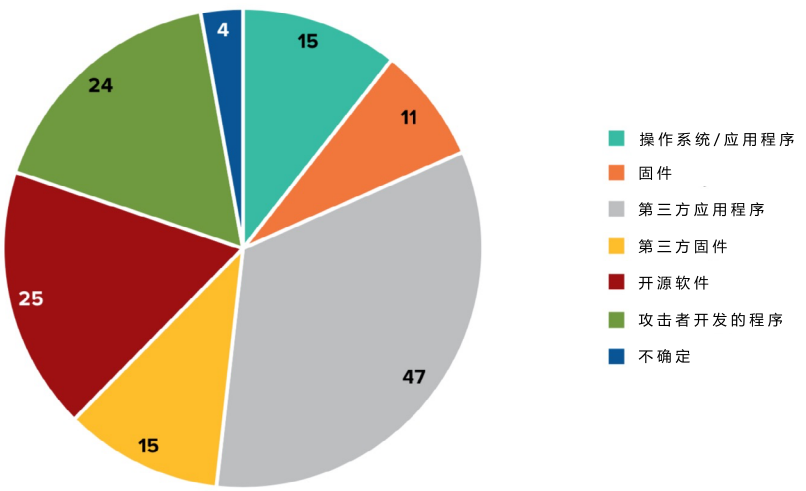


图 3.18　攻击代码分布的统计

供应链攻击事件并不罕见，早在 2015 年苹果非官方渠道的 Xcode 被攻击者篡改、植入恶意代码，著名的 XcodeGhost 事件，致使大量使用该工具开发的苹果 APP 遭受信息泄露、恶意弹窗和被远程控制的攻击。近年热点安全事件包括 SolarWinds、Mimecast 等事件。

3.9.1.1 SolarWinds 事件

SolarWinds 是一家国际 IT 管理软件供应商，其 Orion 软件更新服务器上存在一个被感染的更新程序，这导致美国多家企业及政府单位网络受到感染。

攻击者使用多种攻击技术破坏 SolarWinds 的 Orion 软件，修改了供应商的代码，滥用 SolarWinds 中客户的信任关系，基于 Orion 向 SolarWinds 的客户投递恶意软件，攻击者的最终目标是窃取 SolarWinds 客户的数据。

SolarWinds 事件是一起影响范围广、潜伏时间长、隐蔽性强、高度复杂的攻击，波及全球多个国家和地区的 18000 多个用户，攻陷了多个美国联邦机构及财富 500 强企业网络。2020 年 12 月，美国政府确认国务院、五角大楼、国土安全部、商务部、财政部、国家核安全委员会等多个政府部门遭入侵。其背后的攻击组织训练有素、作战指挥协同达到了很高的水准。

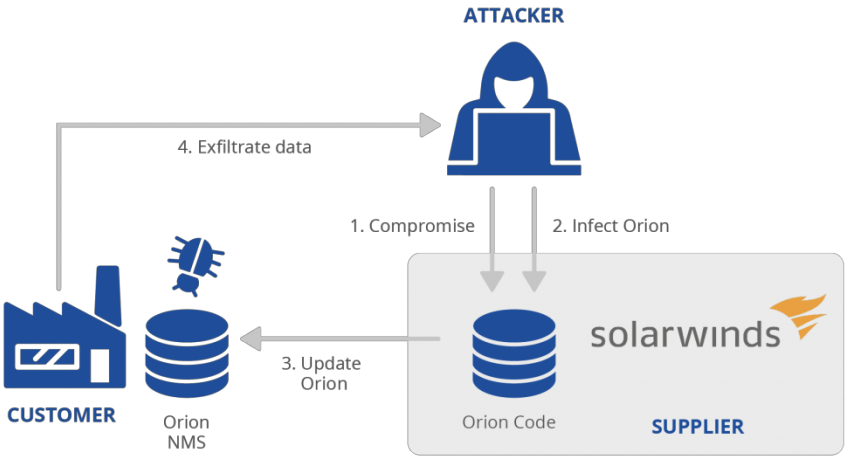


图 3.19　SolarWinds 供应链攻击

3.9.1.2 Mimecast 事件

Mimecast 是一家基于云的网络安全服务供应商，主要是提供电子邮件安全服务，服务要求客户安全地登陆到 Mimecast 服务器以使用其 Microsoft 365 帐户。攻击者通过利用了 Mimecast 与其客户的信任关系，成功地窃取了 Mimecast 使用者的数据，约 3600 家占用户总比例 10% 的 Mimecast 企业用户受到影响。

Mimecast 公司称此次事件与 SolarWinds 事件有关，攻击者通过 Sunburst 后门攻陷了 Mimecast 公司的网络，导致 Mimecast 部分源码被盗，进而影响到了 Mimecast 的用户。将 SolarWinds 事件和 Mimecast 事件放在一处分析，可看出供应链攻击造成的连锁效应。

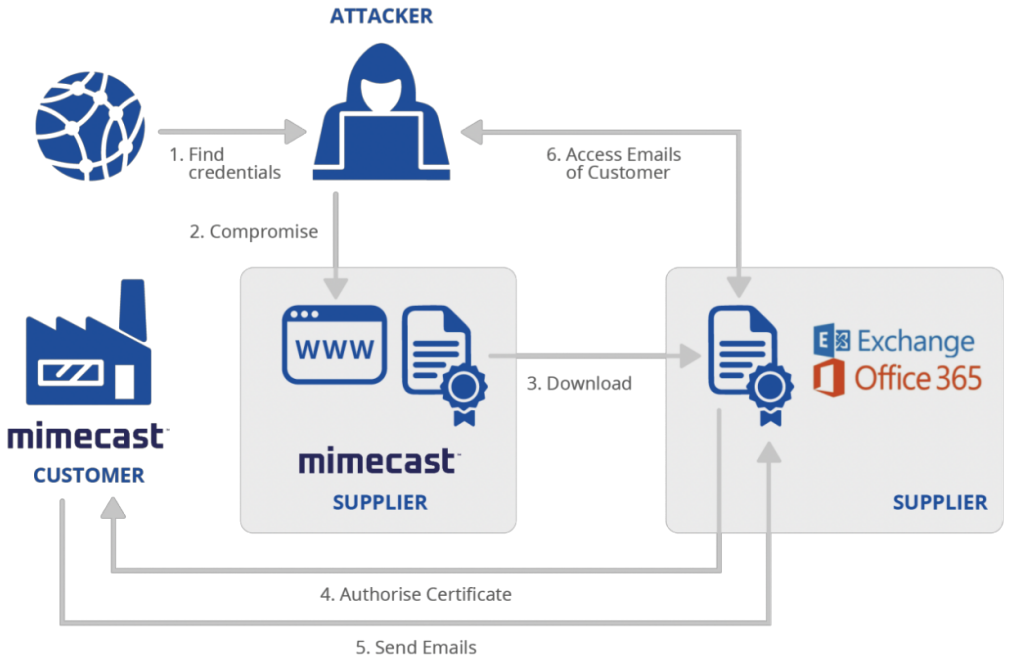


图 3.20　Mimecast 供应链攻击图

3.9.2　政策和市场

全球供应链安全市场的典型特性是由各国政府发起，通过相应的法律、政策及标准的要求、指导和促进行业整体发展。

2021 年 2 月美国拜登总统签署了第 14017 号行政命令《美国供应链》要求美国政府对关键供应链进行全面审查，以查明风险，解决脆弱性，并制定战略提升供应链复原力。2021 年 5 月美国第 14028 号行政命令《改善国家网络安全》中特别强调需加强软件供应链安全，提出了“关键软件”的概念，要求建立软件产品安全标准和严格的管控机制。美国的供应链安全市场由政府引导，已经在国家层面建立了相对完整的供应链安全监管组织架构，形成由美国白宫总统办公室统筹，美国网络安全与基础设施安全局（CISA）下设的 ICT 供应链风险管理特别工作组（ICT SCRM）指导，商务部、国防部、国土安全部、农业部、能源部、运输部、公共与卫生服务部等共同参与的顶层框架。

供应链安全早在我国《网络安全法》就已提出相应要求。第三十五条“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”和第三十六条“关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任”，分别从网

络安全审查、网络产品和服务安全角度对供应链安全提出要求。2019 年 7 月，国家互联网信息办公室联合四部门共同发布《云计算服务安全评估办法》，要求云计算服务安全评估工作中，应重点评估“云平台技术、产品和服务供应链安全情况”。申请安全评估的云服务商应提交“业务连续性和供应链安全报告”。2020 年 4 月，《网络安全审查办法》明确提出，“为了确保关键信息基础设施供应链安全，维护国家安全，对关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应进行网络安全审查”。2021 年 7 月 30 日正式颁布的《关键信息基础设施安全保护条例》第十九条明确指出：“运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查”。 我国颁布的其他相关政策和标准详见下表。

表 3.12　供应链安全政策及标准统计

序号	政策或标准	相关内容
1	《网络安全法》	分别从网络安全审查、网络产品和服务安全角度对供应链安全提出要求。
2	《网络安全审查办法》	要求对关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应进行网络安全审查。
3	《关键信息基础设施安全保护条例》	运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。
4	《网络产品安全漏洞管理规定》	网络产品提供者、网络运营者和网络产品安全漏洞收集平台应履行漏洞发现、验证、上报和修复等义务。
5	《云计算服务安全评估办法》	要求重点评估云平台技术、产品和服务供应链安全情况，申请安全评估的云服务商应提交业务连续性和供应链安全报告。
6	银办发〔2021〕146 号 《.. 关于规范金融业开源技术应用与发展的意见》	合理应用开源技术，提高应用水平和自主可控能力，促进开源技术健康可持续发展。
7	GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》	要求把供应商关系和供应链安全作为安全保护的重要项，着重强调供应链安全的管理。
8	GB/T 36637—2018《信息安全技术 ICT 供应链安全风险管理指南》	规定了信息通信技术（ICT）供应链的安全风险管理过程和控制措施，适用于 ICT 供方和需方、第三方测评机构等。
9	GB/T 32921—2016《信息安全技术 信息技术产品供应方行为安全准则》	从供应商角度入手，规定了信息技术产品供应方的行为安全准则。
10	GB/T 32926—2016《信息安全技术 政府部门信息技术服务外包信息安全管理规范》	规范了政府部门信息技术服务外包信息安全管理模型，明确了服务外包信息安全管理角色和责任，为政府部门信息技术服务外包的安全管理提供参考。
11	GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》	对云服务商的供应链从采购过程、外部服务提供商、开发商、防篡改、组件真实性、不被支持的系统组件、供应链保护等方面提出了安全要求。
12	GB/T 24420—2009《供应链风险管理指南》	给出了供应链风险管理的通用指南，适用于各类组织保护其在供应链上进行的产品的采购活动。
13	《信息安全技术 关键信息基础设施信息技术产品供应链安全要求 (报批稿)》	该标准提出了关键信息基础设施、政务信息系统信息技术产品供应链在设计、开发、采购、生产、交付和运维等环节的安全要求，适用于关键信息基础设施、政务信息系统加强信息技术产品供应链安全。
14	《信息安全技术 软件供应链安全 (草案)》	该标准规定了软件产品和服务供应链所涉及相关要素的安全要求，包括软件供应链组织管理要求，以及开发、交付、使用等环节的安全要求。

软件供应链安全主要涉及四类安全产品，详见下表所示，主要厂商包括绿盟科技、奇安信、启明、端玛、悬镜、棱镜七彩、黑鸭子、Fortify 等。

表 3.13　软件供应链安全产品统计

产品名称	功能介绍
静态应用程序安全测试（SAST）	用于自动地发现代码中的安全缺陷和违背安全规则的情况。 主流技术包括：词法分析技术、抽象解释技术、程序模拟技术、定理证明技术、数据流分析技术。
动态应用程序安全测试（DAST）	用于模拟黑客行为对应用程序进行动态攻击，分析应用程序的反应，从而确定该应用是否易受攻击。
交互式应用程序安全测试（IAST）	通过插桩技术，基于请求及运行时上下文综合分析，高效、准确地识别安全缺陷及漏洞，确定安全缺陷及漏洞所在的代码位置。 主要技术包括：流量采集、Agent 监控、交互扫描。
软件组成分析（SCA）	主要针对开源组件，通过扫描识别开源组件，获取组件安全漏洞信息、许可证等信息，避免安全与法律法规风险。主要功能包括：开源组件识别、组件清单、许可证清单、漏洞清单及漏洞详情跟踪。

3.9.3　发展趋势

供应链安全正在成为关键信息基础设施安全防护中最薄弱的关节，随着关键信息基础设施防护的加强，供应链安全也注定会引起更多地关注。据绿盟科技观测，在未来 1 到 2 年的供应链安全领域建设主要是开展围绕政策指引的技术创新、模式创新、产品创新等活动，在某些重要行业领域将会出现一批创新性试点项目；从市场角度看是从保护运营者企业安全向保护供应商安全的市场下沉，更为广阔的市场将迎来更多的安全厂商加入。

3.10　无线通讯安全

无线通讯包括远距离通讯和远距离通讯。常见的远距离通讯方式有蜂窝网络、数传电台、扩频微波、无线网桥、卫星通信、短波通信等；常见的近距离通讯方式有 ZigBee、蓝牙（Bluetooth）、无线宽带（Wi-Fi）、超宽带（UWB）、RFID 等。就整体市场来说安全关注顺序依次为无线宽带（Wi-Fi）、蓝牙（Bluetooth）等

3.10.1　热点安全事件

由于蓝牙本身自定义强，因此安全问题更多的是公司专有内容，相对于协议本身造成大规模影响范围的 Wi-Fi 协议较为突出，其 2021 年较为突出且公开的为 2020 年的针对 Wi-Fi 安全的漏洞，具体为纽约大学阿布扎比分校的安全研究员 Mathy Vanhoef 发现了一种堪称“核弹级”的 Wi-Fi 安全漏洞——FragAttacks（破片和聚合攻击），该漏洞存在于 1997 年 Wi-Fi

技术诞生以来的所有 Wi-Fi 设备（包括计算机、智能手机、园区网络、家庭路由器、智能家居设备、智能汽车、物联网等等），包括最新的 WPA3 规范。甚至 Wi-Fi 的原始安全协议（称为 WEP）也会受到影响。FragAttack 是一组漏洞，其中三个影响大多数 WiFi 设备，属于 Wi-Fi 802.11 标准帧聚合和帧分段功能中的设计缺陷，而其他漏洞是 Wi-Fi 产品中的编程错误。

所有披露（CVE）编号和描述如下：

- CVE-2020-24588：聚合攻击（接受非 SPP A-MSDU 帧）。
- CVE-2020-24587：混合密钥攻击（重新组装在不同密钥下加密的片段）。
- CVE-2020-24586：碎片缓存攻击（（重新）连接到网络时不清除内存中的碎片）。
- 允许在受保护的 Wi-Fi 网络中简单注入纯文本帧的实现漏洞被分配了以下 CVE：
- CVE-2020-26145：接受纯文本广播片段为全帧（在加密网络中）。
- CVE-2020-26144：接受以 EtherType EAPOL 的 RFC1042 标头开头的纯文本 A-MSDU 帧（在加密网络中）。
- CVE-2020-26140：接受受保护网络中的纯文本数据帧。
- CVE-2020-26143：接受受保护网络中的碎片明文数据帧。
- 其他实现缺陷被分配为以下 CVE：
- CVE-2020-26139：转发 EAPOL 帧，即使发送方尚未通过身份验证（应该只影响 AP）。
- CVE-2020-26146：使用非连续数据包号重新组装加密片段。
- CVE-2020-26147：重新组装混合加密 / 明文片段。
- CVE-2020-26142：将碎片帧处理为全帧。
- CVE-2020-26141：未验证碎片帧的 TKIP MIC。

就漏洞来看无线，2021 年 wifi 的 CVE 编号约 38 个（截止到 2021 年 11 月 25 日）基于配套驱动和应用的占比较多，由于驱动和应用的展现会比较明显。针对 Bluetooth 的 CVE 编号约 62 个（截止到 2021 年 11 月 25 日）同样基于驱动和应用的占比较大，由于 Bluetooth 协议本身的体现也在于驱动和应用。另外统计了关于 RFID 的 CVE 编号大约 2 个，可以判断相对于其它通信 RFID 的使用频率还是较少。

3.10.2 政策和市场

近年来，我国数字经济蓬勃发展，以 5G、移动物联网、北斗为代表的各类无线技术广泛应用于社会生活的各方面，成为数字中国建设的关键技术。基于各类无线技术形成了移动通信、物联网、卫星通信等多个细分产业，我国无线技术加速与实体经济深度融合，赋能传统产业数字化发展，催生新产业新业态新模式，无线经济正在成为壮大经济发展的新引擎，2020 年中国无线经济规模达 38313.03 亿元，较 2019 年增加了 5992.92 亿元，同比增长 18.5%，未来将继续保持增长。

市场研究机构 MarketsandMarkets 之前发布的研究报告显示，2014 年，全球无线网络安全市场规模将到 84.7 亿美元（约合人民币 528 亿元）。随着无线网络普及，到 2019 年，这一数据将达到 155.5 亿美元（约合人民币 969.3 亿元），年复合增长率约 12.94%。

根据 Market Research Future (MRFR) 市场报告指出，受物联网的普及影响，无线技术快速发展，导致全球无线安全系统市场在 2023 年将突破 140 亿美元，复合增长率达 11%(2017-2023)。

来自报告 2021-2027 全球与中国军事网络安全市场现状及未来发展趋势指出 2020 年全球军事网络安全市场规模达到了 881 亿元，预计 2027 年将达到 1168 亿元，年复合增长率 (CAGR) 为 4.1%。

针对无线安全领域，各个厂商均有所投入，就无线防护而言，主要集中入侵防御系统（WISP），针对企业级的安全防护市场，现阶段主要的产品为启明星辰的天清安全无线控制系统，绿盟无线防御系统 SWD，奇安信天巡无线入侵防御系统等。

针对企业级的安全防护市场，针对个人级别的无线类主要在与隐私内容，配套的民众买单率不会很大，也无法像 PC 杀毒领域一样免费来带来市场，无论企业还是个人市场大多都在 Wi-Fi 类，此外更多针对无线的攻击是依据使用时的问题的特殊化环境，未来想在这个领域进行安全覆盖，更多的需要无线设备类厂商进行安全配置简单化的优化来增加个人市场，对于商业市场特别是商业隐私市场，可以组建一些专业实施团队进行针对性安全优化，这个方向市场前景还是比较客观，且现在的专业程度还不够标准化。

3.10.3 发展趋势

无线作为使用电磁波的传播方式，在发展物联世界起到了关键作用。其特点的便捷大范围的特性作为网络的扩展提供了有效的支持。另外电磁波的特性，也使其在反恐与侦察中存

在大量使用潜力。通过信号的变化来针对目标的主动探测和对信号的长期的被动探测，使其在反恐中有效的发现敌方的相关位子等数据。就现在国际的大情况来说，长期的经济不稳定必然带来大量威胁社会的行为，因此在此方便的投入市场份额目前看来会增加。另外针对隐私相关的内容很多也关联上了无线的市场，随着隐私意识强化必然会伴随无线的市场增大。

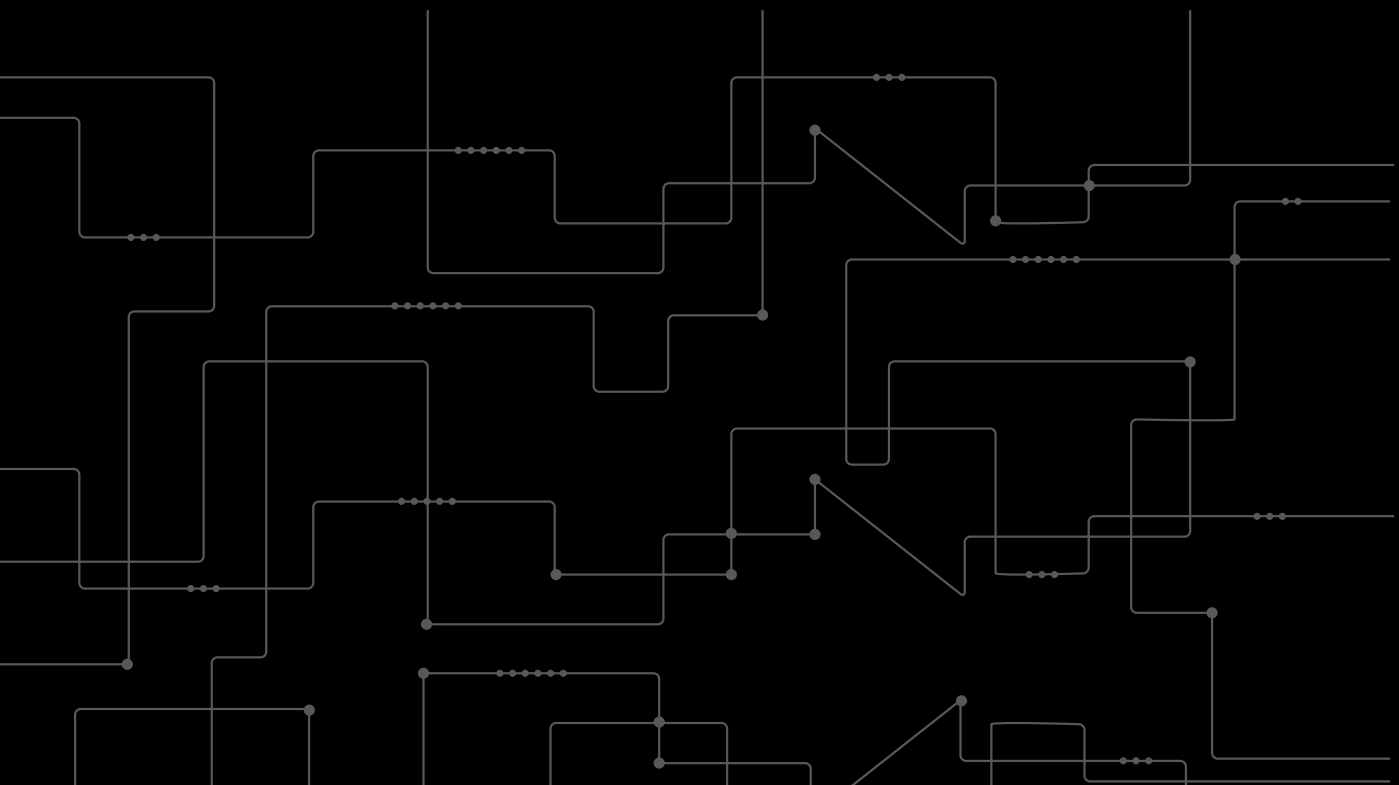
此外在各国都准备的 2035 年火星登录上，空间无线通信的发展有很多的想象空间，以及针对于海洋通信的无线解决方案也是接下来几年的重点需求。随着 5G 在军事领域的应用，美国已经测试在 F35 战机上安全 5G 模块来满足近程组网的数据交互，5G 的无线安全也会成为一向重点的攻击点。

另外在针对太赫兹的通信已经存在罗德与施瓦茨的测试，但其对物理分子的影响是无法避免的，这将带来一个消耗和通信比作为一个重要参数来引入到实体产业中。

近年来由于蓝牙和 Wi-Fi 过猛发展，导致 ZigBee 等无线通信的市场被占领，有一种蓝牙、Wi-Fi、蜂窝通信来占领整个市场的架势。就势头来看蓝牙在低功耗的特性如果被 Wi-Fi 取代后，市场将有 Wi-Fi、蜂窝来进行占据，从而近程通信 Wi-Fi 远程通信蜂窝加光纤。

4

总结



2021 年，全球新冠疫情还未结束，仍将继续面临新的、不断演化的网络安全威胁与挑战。同时，疫情掀起了“新基建安全”的又一轮热潮，以大数据、物联网、工业互联网、车联网、5G、人工智能、云计算、区块链、供应链和无线通讯为代表的新技术备受瞩目。网络信息安全态势愈加复杂，绿盟科技集中精力做好巨人背后的安全专家，提供基于自身核心竞争力的企业级网络安全产品、安全解决方案和安全运营服务。

参考文献

1. http://wiotc.org/en/news/372.html
2. https://targetmarketsize.com/
3. https://www.miit.gov.cn/jgsj/kjs/wjfb/art/2021/art_9e2dd241008d4970a52355326e205fb7.html
4. https://m.thepaper.cn/baijiahao_7295467
5. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/
6. https://www.datamation.com/trends/internet-of-things-iot-market/
7. https://www.marketsandmarkets.com/Market-Reports/industrial-control-systems-security-ics-market-1273.html
8. https://mp.weixin.qq.com/s/2EHQ6vJD3SxkRe1yHb5v8w
9. https://www.dwcon.cn/post/914
10. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge
11. https://www.marketresearchfuture.com/reports/automotive-cyber-security-market-2970https://www.marketresearchfuture.com/reports/automotive-cyber-security-market-2970
12. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202012/P020201223685469901767.pdf
13. https://www.miit.gov.cn/jgsj/xxjsfzs/wjfb/art/2021/art_aac4af17ec1f4d9fadd5051015e3f42d.html
14. https://hacked.slowmist.io/
15. https://xw.qq.com/cmsid/20201123A07ZLU00
16. https://en.wikipedia.org/wiki/Poly_Network_Exploit Did the FBI Hack Bitcoin? Deconstructing the Colonial Pipeline Ransom
17. https://pdf.dfcfw.com/pdf/H3_AP202111041527069351_1.pdf?1636060619000.pdf
18. Enisa. Threat Landscape for Supply Chain Attacks. 2021. [online] Available at: <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>.
19. Herr T. Breaking Trust–Shades of Crisis Across an Insecure Software Supply Chain[J]. 2021.
20. 绿盟科技伏影实验室 . SOLARWINDS 供应链攻击事件分析 . [online] Available at: <http://blog.nsfocus.net/solarwinds-attack-incident-analysis-1216/>.
21. 中国电子技术标准化研究院 上官晓丽 孙彦 李彦峰 . 信息通信技术供应链安全政策法规与标准研究 . 中国信息安全 . 2021.
22. 中国电子技术标准化研究院 吴江伟 . 软件供应链安全及防护工具研究 . 中国信息安全 . 2021.
23. BleepingComputer. Mimecast: SolarWinds hackers stole some of our source code. [online] Available at:https://www.bleepingcomputer.com/news/security/mimecast-solarwinds-hackers-stole-some-of-our-source-code/

24. http://www.eepw.com.cn/article/201807/383353.htm

25. https://www.chyxx.com/industry/202111/984204.html

26. http://cve.mitre.org/

27. https://www.fragattacks.com/#notpatched

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