极牛网络安全通讯 • 社群期刊

2025 年 2 月 第 44 期

网安观察

第44期
2025年2月

CONTEN

目录

安全态势

国际视野

P7 美国网络安全和基础设施安全局发布《产品安全不良实践》第二版

CONTENTS

专题报道

第 44 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：陈艇鑫
移动安全主编：蔡国兆
网安人才主编：林俊濠
涉网犯罪主编：胡铭凯
网安产业主编：张九史
网安态势主编：郑泽彬

公众号　小程序　网站

电子版请访问 www.geeknb.com 阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

政策篇

国内，个人信息保护配套制度陆续出台。个人信息保护合规审计首个配套细则《个人信息保护合规审计管理办法》发布，十八部门联合印发《困境儿童个人信息保护工作办法》，规范困境儿童个人信息使用，全国网安标委发布《网络安全标准实践指南——人脸识别支付场景个人信息安全保护要求》；

国际上，人工智能安全治理日益深化。欧盟委员会发布禁止类人工智能实践指南，对危害欧洲价值观和基本权利的技术进行监管，法国等 19 国网络安全机构发布《通过基于网络风险的方法构建可信 AI》，以加强 AI 应用和服务安全。

国内

国家网信办公布《个人信息保护合规审计管理办法》

2 月 14 日，国家互联网信息办公室公布《个人信息保护合规审计管理办法》，自 2025 年 5 月 1 日起施行。该文件明确了个人信息处理者开展合规审计的两种情形。一是个人信息处理者自行开展合规审计的，应当由个人信息处理者内部机构或者委托专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。二是履行个人信息保护职责的部门发现个人信息处理活动存在较大风险、可能侵害众多个人的权益或者发生个人信息安全事件的，可以要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计。该文件要求，个人信息处理者按照履行个人信息保护职责的部门要求开展合规审计的，应当为专业机构正常开展合规审计工作提供必要支持并承担审计费用，在限定时间内完成合规审计，报送合规审计报告并进行整改。

强制性国家标准《导航电子地图安全处理技术基本要求》公开征求意见

2 月 13 日，自然资源部组织起草了《导航电子地图安全处理技术基本要求（征求意见稿）》强制性国家标准，现公开征求意见。该文件规定了公开出版、销售、传播、展示和使用的导航电子地图在数据采集、制作和表示过程中，空间位置技术处理、传输安全技术处理、服务安全技术处理的要求，以及不应采集和表示的内容，适用于公开出版、销售、传播、展示和使用的导航电子地图。该文件提出，导航电子地图服务应由具备专有存储、计算和网络资源的计算平台提供。计算平台能够接收、存储、处理、更新、分发导航电子地图。计算平台应采用相应技术措施对导航电子地图进行安全处理，保护涉密、敏感地理信息或与之关联的敏感个人信息。导航电子地图确需向中国境外提供的，应符合数据出境安全评估要求。

国家标准《数据安全技术 机密计算通用框架》发布

2 月 12 日，根据 2025 年 1 月 24 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2025 年第 2 号），全国网络安全标准化技术委员会归口的国家标准《数据安全技术 机密计算通用框架》正式发布，自 2025 年 8 月 1 日起施行。根据此前公布的征求意见稿，该文件给出了机密计算通用框架，包括框架的核心组件、基础功能、安全服务及服务接口类型，适用于指导机密计算相关产品、服务或解决方案的设计、研发、部署和使用，也适用于指导网络运营者对机密计算技术的应用，第三方测评机构也可参照使用。

李强签署国务院令，公布《公共安全视频图像信息系统管理条例》

2 月 10 日，中国政府网公布《公共安全视频图像信息系统管理条例》全文。该文件已于 2024 年 12 月 16 日国务院第 48 次常务会议通过，自 2025 年 4 月 1 日起施行。该文件要求，公共安全视频系统管理单位应当履行系统运行安全管理职责，履行网络安全、数据安全和个人信息保护义务，建立健全管理制度，完善防攻击、防入侵、防病毒、防篡改、防泄露等安全技术措施，定期维护设备设施，保障系统连续、稳定、安全运行，确保视频图像信息的原始和完整。公共安全视频系统管理单位委托他人运营的，应当通过签订安全保密协议等方式，约定前款规定的网络安全、数据安全和个人信息保护义务并监督受托方履行。

《人工智能安全标准体系（V1.0）》公开征求意见

1 月 26 日，全国网络安全标准化技术委员会秘书处组织编制了《人工智能安全标准体系（V1.0）》（征求意见稿），现公开征求意见。该文件指出，人工智能安全标准体系主要由基础共性、安全管理、关键技术、测试评估、产品与应用等 5 部分组成。人工智能安全标准体系旨在支撑落实《人工智能安全治理框架》，围绕《框架》中明确的内生安全风险和应用安全风险，系统梳理了可帮助防范化解相关人工智能安全风险的重点标准，同时，与网络安全国家标准体系进行有效衔接，以科学、合理的标准布局前瞻应对各类风险挑战，促进人工智能技术及应用健康发展。

《网络安全标准实践指南——人脸识别支付场景个人信息安全保护要求》发布

1 月 26 日，全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——人脸识别支付场景个人信息安全保护要求》。该文件给出了人脸识别支付场景数据收集、存储、传输、导出、删除等环节的安全要求，可为人脸识别支付服务提供方、人脸验证服务方、场所管理方、设备运营方处理个人信息提供参考。

《中国人民银行业务领域网络安全事件报告管理办法》公开征求意见

1 月 24 日，中国人民银行起草了《中国人民银行业务领域网络安全事件报告管理办法（征求意见稿）》，现面向社会公开征求意见。该文件共 5 章 32 条，包括总则、网络安全事件分级、网络安全事件报告、法律责任、附则。该文件明确了网络安全事件分级管理要求，提出特别重大、重大、较大、一般等级网络安全事件的分级标准底线规则。该文件将替代 2002 年发布的《银行计算机安全事件报告管理制度》。

十八部门联合印发《困境儿童个人信息保护工作办法》

1 月 23 日，民政部等十八部门印发《困境儿童个人信息保护工作办法》（以下简称《办法》），规范困境儿童个人信息使用，保护困境儿童个人信息安全，维护困境儿童合法权益。《办法》第十二条明确规定各有关部门要规范困境儿童个人信息的处理，不得违规披露、泄露困境儿童个人信息；第十五条明确规定任何组织和个人不得将困境儿童标签化，不得利用困境儿童个人信息博眼球、赚流量，不得利用困境儿童个人信息进行募捐、直播带货等。《办法》指出，对违反本办法规定处理困境儿童个人信息、侵害困境儿童合法权益的，按照《中华人民共和国个人信息保护法》等有关规定依法处置。

工信部办公厅印发《关于加强互联网数据中心客户数据安全保护的通知》

1 月 14 日，工业和信息化部办公厅印发《关于加强互联网数据中心客户数据安全保护的通知》。该文件共 5 章 16 条，包括基础要求、加强服务器托管业务场景保障能力、加强数据存储与计算业务场景保障能力、加强数据安全供给支撑、工作实施。该文件要求，按照“权责一致、分类施策、技管结合、确保安全”的原则，加强客户数据安全保障能力建设，提升客户数据安全保护水平。该文件还针对设备供应链管理、算力等重点服务安全管理等方面提出了能力要求。

四部门印发《关于促进数据标注产业高质量发展的实施意见》

1 月 13 日，国家发展改革委、国家数据局、财政部、人力资源社会保障部印发了《关于促进数据标注产业高质量发展的实施意见》。该文件共 6 章 13 项任务，包括总体要求、深化需求牵引、增强创新驱动、培育繁荣生态、优化支撑体系、加强保障措施。该文件专门设立了“促进标注产业安全发展”任务，包括建立健全数据标注安全性风险识别、监测预警、应急响应等相关规范，落实数据标注全过程相关主体的安全责任。合理保护数据标注企业在数据流通过程中形成的相关权益。加强数据标注隐私保护、人工智能对齐、安全评估能力建设。

国际

日本内阁批准主动网络防御法案，授权军警可摧毁敌方服务器

2 月 7 日，日本内阁批准并向国会提交了《防止针对重要电子计算机的违规行为造成损害的法案》，授权警方和自卫队在关键基础设施遭到网络攻击时可摧毁敌方服务器，以加强日本的主动网络防御能力。该法案的目标是提升日本的网络安全能力，力争达到与美国及主要欧洲国家相当的水平。警方将首先行动，负责摧毁敌方服务器。在必要时，自卫队的网络单位将在首相指示下介入。当外国政府或相关实体对关键计算机发起高度组织化的网络攻击时，自卫队将采取介入措施。所谓的关键计算机，指的是日本中央政府和地方政府使用的计算机、核心基础设施运营商使用的计算机，以及自卫队和驻日美军使用的计算机。

法国等 19 国网络安全机构发布《通过基于网络风险的方法构建可信 AI》

2 月 7 日，在法国巴黎 AI 行动峰会举办前，法国网络安全局（ANSSI）联合加拿大、德国、英国等其他 18 个国家的网络安全机构发布《通过基于网络风险的方法构建对人工智能的信任》文件。该文件旨在为 AI 系统的安全部署和 AI 供应链的安全提供一种基于风险的策略方法，其重点关注 AI 特定风险识别、AI 攻击类型分析、建议措施、风险评估和检查清单共 4 个方面。该文件为 AI 用户、运营方和开发人员提供了一系列实用的指导原则，包括调整 AI 系统的自主性级别、绘制 AI 供应链图谱、跟踪 AI 系统与其他信息系统的关联度、持续监控和维护 AI 系统等。

加拿大政府发布 2025 版国家网络安全战略

2 月 6 日，加拿大公共安全部发布 2025 版国家网络安全战略，为通过国内和国际的努力，加强当前和未来的网络安全提供指导，旨在确保加拿大的数字化未来。该战略提出，确保加拿大网络安全与繁荣依赖于强大的网络安全，网络安全必须成为国家安全、经济安全和公共安全的基本基石。加拿大网络安全方针将遵循两项总体原则，通过推进三大支柱任务以取得成果。两项总体原则包括全社会参与、敏捷领导力，三大支柱包括与合作伙伴携手保护加拿大民众和企业免受网络威胁、让加拿大成为全球网络安全行业的领军者、检测并阻止网络威胁行为者。

欧盟委员会发布禁止类人工智能实践指南

2 月 4 日，欧盟委员会发布了根据《人工智能法案》定义的禁止类人工智能实践指南草案。该文件提供了法律解释和实际示例，以帮助利益相关方理解并遵守《人工智能法案》的要求。《人工智能法案》第 5 条列出了构成不可接受风险的被禁止的人工智能行为，包括操纵技术、利用漏洞、社交评分、犯罪风险分析、未经授权的面部识别、情感推断、生物特征分类，以及 " 实时 " 生物特征识别的某些用途，这些行为危害了欧洲价值观和基本权利。需要注意的是，禁止类人工智能实践指南已于 2 月 2 日起生效。

五眼联盟发布保护网络边缘设备系列指导文件

2 月 4 日，五眼联盟及国际网络安全机构联合发布了 4 份保护网络边缘设备指导文件，包括由加拿大网络安全中心

牵头编写的《边缘设备安全注意事项》，由英国国家网络安全中心牵头编写的《网络设备和电器生产商的数字取证和保护监测规范指南》，由澳大利亚网络安全中心牵头编写的《边缘设备缓解策略：执行指南》《边缘设备缓解策略：实践指南》。这些指南旨在帮助组织保护网络边缘设备和电器，推动设计安全和默认安全，遏制网络边缘设备漏洞频遭滥用趋势。

美国网络安全和基础设施安全局发布《产品安全不良实践》第二版

1月17日，美国网络安全和基础设施安全局（CISA）、联邦调查局联合发布了《产品安全不良实践》第二版，概述了被认为风险极高的产品安全陋习，尤其是对生产用于关键基础设施或国家关键功能的软件的软件制造商而言，并为软件制造商提供了降低相关风险的建议。第二版整合了CISA收到的公众意见，增加了更多不良实践类型、建议使用内存安全语言、明确修补已被利用漏洞时间表及其他建议。

美国运输安全管理局发布公告，延长管道网络安全指令有效期

1月17日，在特朗普就任总统前几天，美国国土安全部运输安全管理局（TSA）在《联邦公报》上发布公告，将两项针对管道的网络安全指令的期限延长一年，分别为Pipeline-2021-01和Pipeline-2021-02，并进行了部分修订，以提升其有效性和清晰性。这两份针对管道运营商的网络安全指令，始于2021年Colonial管道公司的勒索软件攻击事件。该事件导致美国主要汽油输送服务一度中断。

美国联邦贸易委员会最终确定《儿童在线隐私保护》规则修正案

1月16日，美国联邦贸易委员会全票通过了《儿童在线隐私保护规则》（以下简称COPPA规则）的修改。针对儿童个人信息的收集、使用和披露制定了新的要求，为家长提供了新的工具和保护措施，以帮助他们控制向第三方提供的关于其子女的数据。更新后的COPPA规则在《联邦公报》上公布60天后生效。根据修订后的COPPA规则，运营者在披露从儿童收集的个人信息用于定向广告或其他非其网站或在线服务“核心功能”的目的之前，必须单独获得可验证的家长同意。此外，运营者还需建立、实施并维护合理的书面信息安全计划和数据保留政策，禁止无限期保存儿童的个人信息。

拜登发布第二份网络安全行政令，全面加强美国国家网络防御创新

1月16日，美国总统拜登正式签发其任内第二份网络安全行政令，承诺在2021年首份网络安全行政令的基础上采取更多行动来改善美国的网络安全，旨在解决联邦系统、关键基础设施和私营部门的脆弱性，追捕和制裁破坏美国互联网和电信系统的外国对手或黑客组织。该文件强调，为应对敌对国家和犯罪分子继续针对美国和美国民众的网络攻击，必须采取更多措施来提高国家网络安全。该文件包括八项重点内容：一是实现第三方软件供应链的透明度和安全性；二是提高联邦系统的网络安全；三是保护联邦通信；四是打击网络犯罪和欺诈；五是利用人工智能促进网络安全；六是确保政策与实践相结合；七是保护国家安全系统和破坏性影响系统；八是采取额外措施打击重大恶意网络活动。

美国商务部发布最终规则，限制中国网联汽车技术进入美国市场

1月14日，美国商务部工业与安全局（BIS）发布了题为《保护信息和通信技术与服务供应链：网联汽车》的最终规则，禁止向美国进口和在美国销售特定的与中国有关的车辆连接系统（VCS）硬件与包含VCS或自动驾驶软件的网联汽车整车，主要针对乘用车市场，适用于总重量不超过10000磅（约4,536公斤）的道路机动车辆。BIS解释称，出台该规则的主要原因是应对智能网联汽车供应链安全风险。这是2024年2月29日和2024年9月23日BIS分别发布该规定的拟议规则预通知和拟议规则通知的最终规则，于2025年3月17日生效。

事件篇

DeepSeek 爆火后遭遇大量网络威胁。据奇安信 XLab 实验室监测显示，DeepSeek 近一个月来一直遭受大量海外攻击，春节假期攻击手段持续升级，官方因此限制国外账号注册；有研究发现超 2000 个山寨 DeepSeek 网站，DeepSeek 发布公告首次公开辟谣；黑产团伙专门窃取 DeepSeek API 密钥，经发现已有多个泄露。

泄露百万用户数据，美国一医疗公司赔偿超 5000 万元

2 月 12 日 Govinfo Security 消息，美国虚拟精神健康服务提供商 Brightline 已同意支付 700 万美元（约合人民币 5098 万元），以和解一项拟议中的联邦集体诉讼。该诉讼涉及 2023 年的一起数据泄露事件，勒索软件团伙 Clop 利用软件供应商 Fortra 旗下托管文件传输软件 GoAnywhere 的 0day 漏洞发动攻击，受影响人数约为 100 万人。根据协议，每位符合条件的集体诉讼成员可申请最高 5000 美元的赔偿，以弥补因该事件导致的身份盗窃、欺诈等可证明损失。作为替代方案，集体诉讼成员可选择一次性 100 美元的现金赔偿。此次事件还导致其他上百家 GoAnywhere 客户数据泄露，相关公司正在被诉讼中。

美国知名报业集团被黑，近百家报纸印刷发行受影响

2 月 10 日 BleepingComputer 消息，美国最大的报业集团之一 Lee Enterprises 业务系统在上周遭遇网络攻击，导致连续宕机多天，并对业务运营造成影响。该公司在 2 月 7 日提交给美国证券交易委员会（SEC）的文件中称，2 月 3 日发生的网络攻击引发系统宕机，影响了业务正常运营。Lee Enterprises 新闻编辑部表示，此次网络攻击迫使公司关闭多个网络系统，导致数十家报纸的印刷和发行受到干扰，美国多州大量读者反馈没有收到印刷报纸和访问电子报等。据悉宕机事件在整个报业集团引发混乱，不仅 VPN 无法使用，记者和编辑们也无法访问自己的文件。

黑产团伙专门窃取 DeepSeek API 密钥，已有多个泄露

2 月 8 日 DarkReading 消息，安全研究团队发现，有黑产团伙开始专门窃取云上部署 DeepSeek 大模型的 API 密钥，对外以 30 美元 / 月售卖使用权限。据悉，这类黑产团伙过去长期窃取 OpenAI、AWS、Azure 等各类大模型服务的 API 密钥，对外提供违规生成服务，仅此次研究期间就发现，超 20 亿个 token 被滥用，给付费用户和平台造成了巨大损失。DeepSeek 的最新大模型 V3 和 R1 刚发布几天，黑产团队就已经实现 API 适配支持。目前，研究团队在某个黑产团队的系统中，已经发现了 55 个疑似被窃取的 DeepSeek API 密钥。

超 2000 个山寨 DeepSeek 网站出现，六成 IP 在美国

2 月 9 日央视新闻消息，DeepSeek 发布公告首次公开辟谣称，近期部分与 DeepSeek 有关的仿冒账号和不实信息对公众造成了误导和困扰，该公司目前仅在微信公众号、小红书等三个社交媒体平台拥有唯一官方账号，且 DeepSeek 官方网页端与官方正版 App 内不包含任何广告和付费项目。据奇安信 XLab 实验室统计，2024 年 12 月 1 日至 2025 年 2 月 3 日期间，共出现了 2650 个仿冒 DeepSeek 的域名。大规模的仿冒域名注册活动从 2025 年 1 月 26 日开始，并在 1 月 28 日达到高峰。这些仿冒域名主要用于钓鱼欺诈、域名抢注的非法用途，其中钓鱼欺诈主要通过窃取用户密码账号，利用相似域名和界面误导用户、诱

骗用户下载一些恶意软件，窃取个人信息或者骗取订阅费用。从当前仿冒 DeepSeek 域名解析结果来看，这些仿冒的域名中有 60% 解析 IP 位于美国，其余主要分布在新加坡、德国、立陶宛、俄罗斯和中国。

武汉一国企官网遭篡改被挂上“还钱”字样，涉事公司回应

2 月 8 日上游新闻消息，有网友反映，湖北武汉一国企官网挂上了“码农的钱你也敢吞，还钱”字样，引发关注。据悉，涉事企业为武汉汇科智创科技有限公司，属于国有独资企业。根据其发布的官网截图显示，该国企的官网为“www.focuz-in.com”，点击网页后，无法正常浏览官网主页，只能看到“码农（网络用语，特指专门写代码的程序员）的钱你也敢吞，还钱”。天眼查显示，武汉汇科智创科技有限公司隶属于武汉市汉阳城建集团旗下，实际控制人为武汉市汉阳区财政局（汉阳区政府国有资产监督管理局）。武汉汇科智创科技有限公司相关负责人贾某表示，官网被黑系恶意行为，公司方面已经报警，网警正在核查此事，所谓“还钱”一事不属实，后续肯定要澄清。

2024 年受害企业支付了约 60 亿元勒索软件赎金

2 月 5 日 Bleeping Computer 消息，据区块链情报公司 Chainalysis 统计，2024 年，勒索软件攻击者收到的赎金同比下降 35%，总计 8.1355 亿美元（约合人民币 59.28 亿元），低于 2023 年的 12.5 亿美元，同比下降了 30%。此外，在与勒索软件攻击者展开谈判的受害者中，最终支付赎金的比例仅约 30%。数据还显示，数据泄露网站上的披露数量有所上升。这表明攻击者难以勒索到赎金，因此试图通过增加攻击活动来弥补损失。据分析，企业对勒索软件风险的认知提升及全球勒索软件执法行动促成了这一转变。

DeepSeek 遭受大量境外网络攻击：春节假期持续升级 官方限制账号注册

1 月综合消息，1 月 28 日，DeepSeek 官网的服务状态页面显示：近期 DeepSeek 线上服务受到大规模恶意攻击，为持续提供服务，暂时限制了 +86 手机号以外的注册方式，已注册用户可以正常登录。据奇安信 XLab 实验室监测显示，DeepSeek 近一个月来一直遭受大量海外攻击。1 月 27 日起手段升级，除了 DDoS 攻击还出现了大量的密码爆破攻击。1 月 30 日凌晨烈度升级，攻击，指令较 1 月 28 日暴增上百倍，XLab 实验室观察到至少有 2 个僵尸网络参与攻击，这标志着职业打手开始下场。

IT 供应商 Conduent 被黑，导致美国多地公共服务被迫中断多天

1 月 22 日 The Record 消息，美国政府技术承包商 Conduent 日前遭受网络攻击，操作系统被破坏，导致业务中断。此次攻击事件导致美国多州部分社会保障服务中断多日，无法按时发放款项，众多家庭生计受到影响。美国威斯康星州儿童和家庭事务部门通知居民，由于 Conduent 遭遇系统中断，该机构无法处理通过邮件收到的付款。一些家长和受益人抱怨称，系统中断导致他们几天内无法完成付款。威斯康星州官员透露，此次中断影响了 4 个州，但未具体说明其他受影响州的名称。Conduent 对于中断的影响范围未予置评。

AI 助手泄露客户信息，英国行业软件龙头 Sage 暂时停用相关功能

1 月 20 日 The Register 消息，英国头部企业软件厂商 Sage 集团确认，由于 Sage Copilot 在会计工具中泄露了客户信息给其他用户，公司决定本月暂时停用这款 AI 助手。此前客户发现，Sage Copilot 回复的内容会夹杂一些其他客户的数据，如发票数据等，官方确认问题并表示已停用功能并进行修复，目前已恢复上线。

因遭勒索软件泄露超近 250 万人临床信息，恩佐生化赔偿 5400 万元

1 月 17 日 The Record 消息，美国生物技术公司恩佐生化（Enzo Biochem）1 月 15 日向美国证券交易委员会提交

报告称，决定就一起勒索软件攻击案件与集体诉讼方达成和解，同意赔偿 750 万美元（约合人民币 5487 万元）。此次攻击导致约250万人次的诊断测试信息和个人数据遭到泄露，引发了公众的强烈反响。这起事件发生在 2023 年 4 月，攻击者使用两个长期不修改密码的共享账号入侵了公司网络，姓名、测试结果及大约 60 万个社会保障号码等敏感信息已遭未授权访问。此前，恩佐生化已在 2024 年同意就此次事件向 3 个州政府支付 450 万美元（约合人民币 3292 万元）的赔偿。

2024 年美国医疗行业泄漏了 1.8 亿患者数据

1 月 16 日 SecurityWeek 消息，根据美国卫生与公众服务部民权办公室（HHS OCR）维护的医疗数据泄露数据库统计，2024 年 1 月 1 日至 12 月 31 日期间，共报告了 720 起医疗数据泄露事件（平均每天发生两起泄漏事件）。这些事件导致大约 1.86 亿条用户记录被泄露。不过，由于个人信息可能在多起事件中重复出现，实际受影响人数可能低于 1.86 亿。医疗行业泄漏的数据更为敏感，报告统计的泄露信息类型包括姓名、联系方式、出生日期、社会安全号码、保险信息、医疗记录及金融信息等。

CNCERT 发布美网络攻击我国某先进材料设计研究院事件调查报告

1 月 17 日 CNCERT 公众号消息，国家互联网应急中心 CNCERT 发布报告，公布了美国对我国某先进材料设计研究院的网络攻击详情，为全球相关国家、单位有效发现和防范美网络攻击行为提供借鉴。报告称，此次攻击流程分为三步，利用电子文件系统漏洞进行攻击入侵、软件升级管理服务器被植入后门和木马程序、大范围 PC 被植入木马。2024 年 11 月 6 日至 16 日，攻击者先后 3 次针对性窃取了该单位重要商业信息、知识产权信息文件共 4.98GB。CNCERT 还公布了部分打码后的跳板 IP 信息。

CNCERT 发布美网络攻击我国某智慧能源和数字信息大型高科技企业事件调查报告

1 月 17 日 CNCERT 公众号消息，国家互联网应急中心 CNCERT 发布报告，公布了美国对我国某智慧能源和数字信息大型高科技企业的网络攻击详情，为全球相关国家、单位有效发现和防范美网络攻击行为提供借鉴。报告称，此次攻击流程分为三步，利用微软 Exchange 邮件服务器漏洞进行入侵、在邮件服务器植入高度隐蔽的内存木马、对内网 30 余台重要设备发起攻击。2023 年 5 月至 2023 年 10 月，攻击者发起了 30 余次网络攻击，窃取了大量敏感邮件数据、核心网络设备账号即配置信息、项目管理文件等。

Fortinet 防火墙近期频遭攻击，因 0day 漏洞被利用

1 月 15 日 DarkReading 消息，安全厂商 Arctic Wolf 的研究人员发现，近期一系列针对 Fortinet FortiGate 防火墙设备的攻击均利用了一个 0day 漏洞 CVE-2024-55591。据分析，这些设备的管理接口暴露在互联网上，攻击者利用这些接口实施了未经授权的管理员登录、修改配置、创建新账号，并执行了 SSL VPN 认证操作等。此次攻击活动分为四个阶段，2024 年 11 月中旬执行漏洞扫描、11 月底实施侦察活动，12 月初修改 SSL VPN 配置，12 月中旬至下旬横向移动。Frotinet 公司在 2025 年 1 月 15 日首次披露 CVE-2024-55591 并称已遭在野利用，Arctic Wolf 研究员随后称此次事件利用的就是该漏洞。

攻击者绕过微软 OpenAI 云安全护栏，对外售卖违规内容生成服务

1 月 10 日 CyberScoop 消息，在近期提交给美国弗吉尼亚东区法院的文件中，微软起诉了 10 名个人，指控他们使用被盗凭证和定制软件入侵运行微软 Azure OpenAI 服务的计算机，生成“有害内容”，并申请关闭外国网络犯罪分子用于绕过生成式 AI 系统安全指南的互联网基础设施。据悉，2024 年 7 月至 8 月，攻击者利用被盗的 API 密钥，访问微软 Azure OpenAI 服务中的设备和账号，使用软件工具绕过安全护栏，生成了“数千张”违反内容限制的图片，并对外出售这些访问权限。微软称，被告人至少有 3 名是位于外国的服务提供者，其他人可能是服务使用者。

漏洞篇

近期，国际上多款网络安全产品被披露漏洞已遭利用，包括 Palo Alto Networks PAN-OS 身份验证绕过漏洞 (CVE-2025-0108)、Fortinet FortiOS 和 FortiProxy 身份认证绕过漏洞 (CVE-2024-55591) 等，建议客户尽快做好自查及防护。

Palo Alto Networks PAN-OS 身份验证绕过漏洞安全风险通告

2 月 13 日，奇安信 CERT 监测到官方修复 Palo Alto Networks PAN-OS 身份验证绕过漏洞 (CVE-2025-0108)，该漏洞是由于 PAN-OS 中 Nginx/Apache 对路径的处理不同导致的。未经授权的攻击者可以利用这一漏洞绕过系统身份验证，直接访问 Web 界面，从而造成敏感数据泄露或系统被接管等更大的危害。奇安信鹰图资产测绘平台数据显示，该漏洞关联的全球风险资产总数为 44223 个，关联 IP 总数为 24427 个。目前该漏洞技术细节与 PoC 已在互联网上公开，奇安信威胁情报中心安全研究员已成功复现。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Rsync 堆缓冲区溢出漏洞安全风险通告

1 月 22 日，奇安信 CERT 监测到官方修复 Rsync 堆缓冲区溢出漏洞 (CVE-2024-12084)。Rsync 是一款高效、灵活的文件同步工具，该漏洞存在于 Rsync 的守护进程中，由于对用户控制的校验和长度 (s2length) 处理不当，当 Rsyncd 配置为允许匿名访问时，攻击者可以构造恶意的校验和长度，从而将恶意代码写入内存并执行。攻击者可以利用这一漏洞实现远程代码执行，甚至接管服务器权限。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

FortiOS 和 FortiProxy 身份认证绕过漏洞在野利用通告

1 月 15 日，奇安信 CERT 监测到官方修复 Fortinet FortiOS 和 FortiProxy 身份认证绕过漏洞 (CVE-2024-55591)，FortiOS 和 FortiProxy 中存在一个身份认证绕过漏洞。未经身份验证的远程攻击者可以通过向 Node.js websocket 模块发送特制请求，成功利用此漏洞可使攻击者获得超级管理员权限。目前该漏洞已发现在野利用，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Ivanti Endpoint Manager 多个信息泄露漏洞安全风险通告

1 月 15 日，奇安信 CERT 监测到 Ivanti Endpoint Manager 信息泄露漏洞 (CVE-2024-10811、CVE-2024-13161、CVE-2024-13160、CVE-2024-13159) 在互联网上公开。在 Ivanti EPM 的代理门户中，存在多个绝对路径遍历漏洞。这些漏洞允许远程未经身份验证的攻击者泄露敏感信息。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

《报告》：七大活跃海外组织紧盯中国目标，广东受攻击情况最为突出

近期《2024 网络安全威胁年度报告》发布，涉及高级持续性威胁、勒索攻击等相关内容。

2024 年涉及我国的高级持续性威胁事件主要发生在科研教育、信息技术、制造、政府机构等领域，受害目标集中在广东等地区。DarkHotel、海莲花、伪猎者、虎木槿、蔓灵花、摩诃草等组织积极针对国内重点目标实施攻击。

第一章 高级持续性威胁

高级持续性威胁（APT）多年来一直是网络威胁的重要组成部分，攻击者通常有国家背景支持，主要以敏感数据收集和情报窃取为目的，因此行动隐秘，不易被受害者察觉。本章将分别介绍中国国内和全球范围在 2024 年遭受的高级持续性威胁。

国内高级持续性威胁的内容及结论主要基于对奇安信威胁雷达数据、奇安信红雨滴团队在客户现场处置排查的真实 APT 攻击事件、使用奇安信威胁情报的全线产品的告警数据等信息的整理与分析。全球高级持续性威胁的内容与结论主要基于对公开来源的 APT 情报（即“开源情报”）的整理与分析。

一、国内高级持续性威胁总览

奇安信威胁情报中心通过使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘，2024 年监测到我国范围内大量 IP 地址疑似和数十个境外 APT 组织产生过高危通信。从地域分布来看，广东省受境外 APT 团伙攻击情况最为突出，其次是浙江、上海、北京、江苏等地区。

奇安信威胁雷达是奇安信威胁情报中心基于奇安信大网数据和威胁情报中心失陷检测（IOC）库，用于监

> DarkHotel、海莲花、伪猎者、
> 虎木槿、蔓灵花、摩诃草等
> 海外攻击组织积极针对国内重点目标。

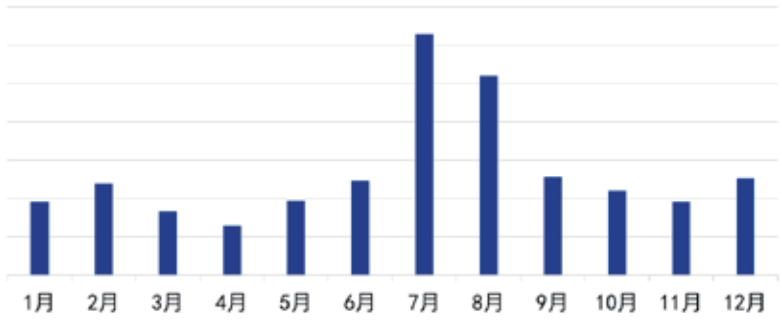

图 1 2024 年中国境内疑似受控 IP 数量月度分布

图 2 2024 年中国境内每月新增疑似受控 IP 数量变化趋势

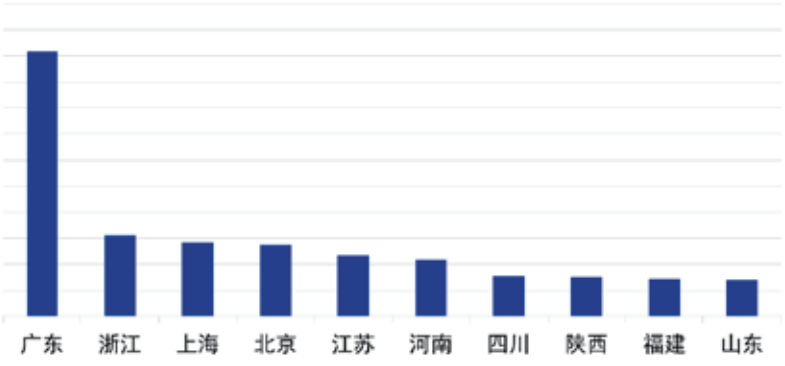

图 3 2024 年中国境内疑似受控 IP 地域分布

控全境范围内疑似被 APT 组织、各类僵木蠕控制的网络资产的一款威胁情报 SaaS 应用。通过整合奇安信的高、中位威胁情报能力，发现指定区域内疑似被不同攻击组织或恶意软件控制的主机 IP，了解不同威胁类型的比例及被控主机数量趋势等。可进一步协助排查重点资产相关的 APT 攻击线索。

基于奇安信威胁雷达境内的遥测分析，我们从以下方面对我国境内疑似遭受的 APT 攻击进行了分析和统计。

（一）受控 IP 数量和趋势

奇安信威胁情报中心基于威胁雷达在 2024 年监测到数十个境外 APT 组织针对我国范围内大量目标 IP 进行通信，形成了大量的境内 IP 与特定 APT 组织的网络基础设施的高危通信事件。其中还存在个别 APT 组织通过多个 C2 服务器与同一 IP 通信的情况。

图 1 所示为 2024 年奇安信威胁雷达遥测感知的我国境内每月连接境外 APT 组织 C2 服务器的疑似受害 IP 地址数量统计，平均每月有超 2500 个境内 IP 地址疑似受控。其中，7 月份受控 IP 数据量明显高于其他月份。

2024 年中国境内每月新增疑似被境外 APT 组织控制的 IP 数量变化趋势如图 2 所示，反映了 APT 组织攻击活跃度变化走向。7月为全年数值高峰。

（二）受害目标地域分布

图 3 所示为 2024 年中国境内疑似连接过境外 APT 组织 C2 服务器的 IP 地址地域分布，分别展示了各省疑

似受害 IP 地址的数量：广东省受境外 APT 团伙攻击情况最为突出，占比达 24.6%，其次是浙江、上海、北京、江苏等地区。

（三）受害行业分布

进一步通过奇安信威胁雷达的遥测感知和奇安信红雨滴团队基于客户现场的 APT 攻击线索，并结合使用了奇安信威胁情报的全线产品告警数据进行分析：2024 年涉及我国科研教育、信息技术、制造、政府机构、建筑、医疗健康行业的高级威胁事件占主要部分，占比分别为 16.0%，14.8%，14.8%，8.0%，6.1%，6.1%。其次为交通运输、能源、金融、新闻媒体等领域。受影响的境内行业具体分布如图 4 所示。

根据归属于各个 APT 组织的 IOC 告警量排名，攻击我国境内的前十 APT 组织及其针对的行业领域如表 1 所示。

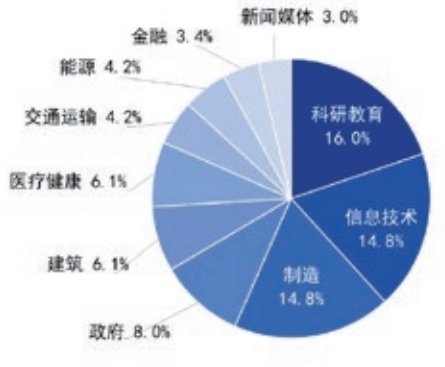

图 4 2024 年高级威胁事件涉及境内行业分布情况

排名	组织名称	涉及行业
TOP1	APT-Q-31（海莲花）	政府、科研教育
TOP2	APT-Q-82 (Gamaredon)	政府、科研教育、电信
TOP3	FaceDuck	科研教育
TOP4	APT-Q-27 (GoldenEyeDog)	博彩、诈骗
TOP5	APT-Q-20（毒云藤）	国防军事、政府、信息技术、科研教育
TOP6	APT-Q-37（蔓灵花）	政府、科研教育、信息技术、能源
TOP7	APT-Q-29 (Winnti)	信息技术、金融
TOP8	APT-Q-1 (Lazarus)	政府、金融、国防军事
TOP9	APT-Q-39（响尾蛇）	科研教育、建筑、制造
TOP10	APT-Q-36（摩诃草）	科研教育、医疗健康、信息技术

表 1 IOC 告警量排名前十 APT 组织及针对的目标行业

二、全球高级持续性威胁总览

公开来源的 APT 情报（以下简称“开源情报”）分析是了解全球网络安全研究机构安全关注、认知全球高级持续性威胁发展趋势的重要手段之一。2024 年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。

奇安信威胁情报中心在 2024 年

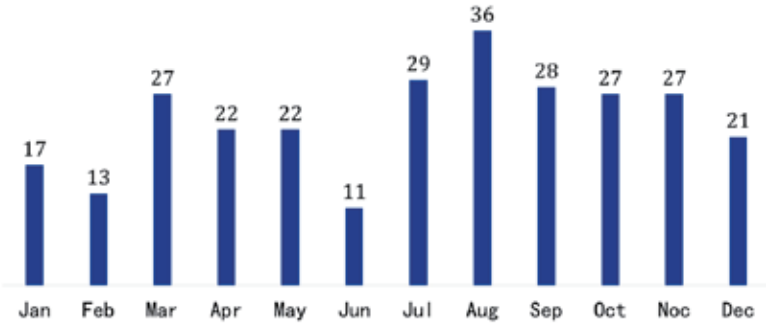

图 5 2024 年全球公开的高级威胁报告数量月度统计

图 6 2024 年公开披露的高级威胁活动针对的国家和地区

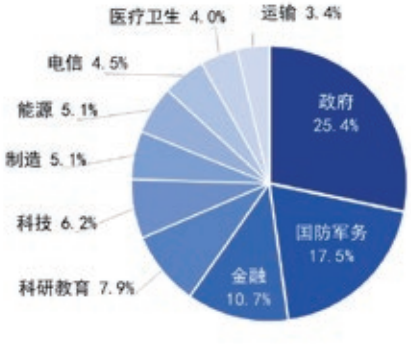

图 7 2024 年全球高级威胁事件涉及行业分布

监测到的高级持续性威胁相关公开报告总共 279 篇。各月监测数据如图 5 所示。

（一）受害目标地域分布

高级威胁活动涉及目标的国家和地域分布情况统计如图 6 所示（摘录自公开报告中提到的受害目标所属国家或地域），可以看到公开披露的大部分高级威胁攻击活动集中在乌克兰、中国、美国、以色列、韩国等几个国家。

（二）受害行业分布

开源情报数据显示，全球高级持续性威胁首要针对的三大行业分别为政府机构、国防军事、金融。2024 年国内外披露的 APT 相关活动报告中，涉及政府机构（包括外交、政党、选举相关）的攻击事件占比为 25.4%；涉及国防军事的攻击事件占比为 17.5%；涉及金融的攻击事件占比为 10.7%；科研教育相关的事件占比为 7.9%。此外，攻击事件发生较多的行业还有科技、制造、能源、电信、医疗卫生、交通运输。

2024 年高级威胁事件涉及行业分布情况如图 7 所示。

（三）活跃高级威胁组织情况

本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率 Top 5 的 APT 组织分别是：Kimsuky 10.1%，Lazarus 7.9%，摩诃草 3.2%，APT28 3.2%，C-Major 2.9%，如图 8 所示。

进一步对高级威胁活动公开报告中提及或命名的攻击行动 / 攻击者名称，按照同一背景来源进行归类处理，得到的统计情况如图 9 所示，2024 年高级威胁活动公开报告总共涉及 103 个命名的威胁来源。

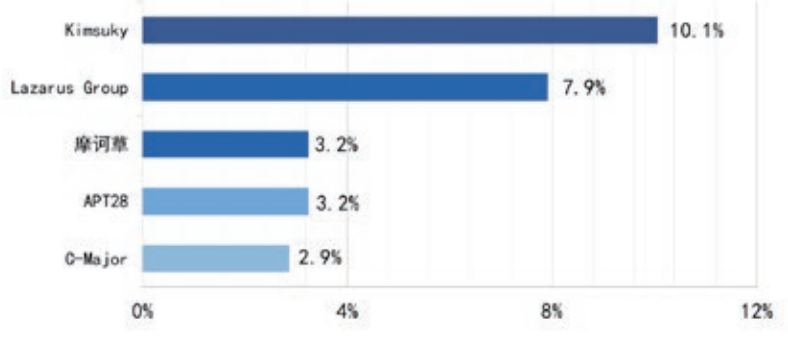

图 8 2024 年全球活跃高级威胁组织

图 9 2024 年公开披露的高级威胁类攻击组织和行动

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全

7436084028