极牛网络安全通讯 • 社群期刊

2024 年 12 月 第 42 期

网安观察

第42期
2024年12月

CONTEN

目录

安全态势

国际视野

P9 国家安全部：境外间谍机关利用众包模式对我开展窃密活动

CONTENTS

专题报道

第 4 2 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，各行业深化推进网络安全体系建设。国家发改委修订发布《电力监控系统安全防护规定》，教育部发文要求做好教育系统软件正版化工作，七部门联合印发《推动数字金融高质量发展行动方案》要求做好数字安全，17 家行业组织联合发布《工业和信息化领域数据安全合规指引》等；

国际上，欧洲理事会通过《网络团结法案》《网络安全法案》修正案两项法案，旨在进一步加强欧盟抵御网络威胁的能力和跨国 / 跨境合作，完善欧盟网络安全制度体系。

国内

四部门发布《中小企业数字化赋能专项行动方案（2025—2027 年）》

12 月 13 日，工业和信息化部、财政部、中国人民银行、金融监管总局发布《中小企业数字化赋能专项行动方案（2025—2027 年）》，旨在由点及面、由表及里、体系化推进中小企业数字化转型。该文件部署了 7 类 18 个重点任务，其中包括全面增强中小企业数据与网络安全防护能力。该重点任务要求引导中小企业建立健全网络和数据安全管理制度，促进态势感知、工业防火墙、入侵检测系统等安全产品部署应用。支持中小企业开展网络和数据安全演练，提升中小企业网络风险防御和处置能力。鼓励中小企业通过购买网络安全保险等方式降低安全风险。

国家发改委公布《电力监控系统安全防护规定》修订版

12 月 11 日，国家发展和改革委员会修订出台了《电力监控系统安全防护规定》。该文件共 6 章 37 条，包括总则、安全技术、安全管理、应急措施、监督管理、附则。此次修订主要做了多方面调整完善，一是强化安全接入区防护要求，明确安全接入区加密认证、安全监测等技术要求；二是强化技术防护措施，在坚持十六字原则的基础上，补充安全免疫、态势感知、动态评估和备用应急措施；三是定义电力监控专用网络，明确承载电力监视和控制业务的专用广域数据网络、专用局域网络及专用通信线路属于电力监控专用网络范畴，四是强化供应链及电力监控系统专用安全产品管理，明确运营者应当以合同条款的方式对电力监控系统供应商提出安全要求，明确由国家电力调度控制中心牵头组建电力监控系统专用安全产品管理委员会。

《政务计算机终端核心配置规范》等 2 项网络安全国家标准获批发布

12 月 6 日，根据 2024 年 11 月 28 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（2024 年第 29 号），全国网络安全标准化技术委员会归口的 2 项网络安全国家标准正式发布。具体包括《网络安全技术 网络安全产品互联互通 第 1 部分：框架》《网络安全技术 政务计算机终端核心配置规范》。

教育部、国家版权局发布《关于做好教育系统软件正版化工作的通知》

12 月 11 日，教育部、国家版权局发布《关于做好教育系统软件正版化工作的通知》，旨在进一步完善教育系统软件正版化工作长效机制，推进教育系统软件正版化工作规范

化、常态化、制度化。该文件要求强化软件采购源头管理，新购置的办公终端应预装或配套采购正版操作系统软件、办公软件和杀毒软件；要将软件正版化工作与教育数字化、网络安全、信息技术应用创新等工作相衔接，整体设计、一体推进，建立健全本单位软件正版化工作管理制度，明确责任分工、工作要求和工作程序，压实工作责任；要将软件正版化纳入教育数字化、网络安全等相关工作宣传内容，增强教师、学生使用正版软件的意识和习惯。

广电总局发布《管理提示（AI 魔改）》

12 月 7 日，广电总局网络视听司发布《管理提示（AI 魔改）》。该文件指出，近期，AI“魔改”视频以假乱真、“魔改”经典现象频发，如《甄嬛传》变身“枪战片”，《红楼梦》改成“武打戏”，孙悟空骑着摩托车扬长而去等。该文件认为，这些视频为博流量，毫无边界亵渎经典 IP，冲击传统文化认知，与原著精神内核相悖，且涉嫌构成侵权行为。为营造清朗网络视听空间，该文件提出具体管理要求，一是各相关省局督促辖区内短视频平台排查清理 AI“魔改”影视剧的短视频，并于 12 月 10 日反馈工作情况。二是严格落实生成式人工智能内容审核要求，举一反三，对各自平台开发的大模型或 AI 特效功能等进行自查，对在平台上使用和传播的各类相关技术产品严格准入和监看，对 AI 生成内容做出显著提示。

中共中央办公厅、国务院办公厅公布《关于推进新型城市基础设施建设打造韧性城市的意见》

12 月 5 日，中共中央办公厅、国务院办公厅公布《关于推进新型城市基础设施建设打造韧性城市的意见》。该文件部署了 11 项重点任务，其中包括保障网络和数据安全。该重点任务要求严格落实网络和数据安全法律法规和政策标准，强化信息基础设施、传感设备和智慧应用安全管控，推进安全可控技术和产品应用，加强对重要数据资源的安全保障。强化网络枢纽、数据中心等信息基础设施抗毁韧性，建立健全网络和数据安全应急体系，加强网络和数据安全监测、通报预警和信息共享，全面提高新型城市基础设施安全风险抵御能力。

《网络安全技术 基于互联网电子政务信息安全实施指南 第 1 部分：总则》等 2 项国家标准公开征求意见

12 月 2 日，全国网络安全标准化技术委员会归口的《网络安全技术 基于互联网电子政务信息安全实施指南 第 1 部分：总则》和《信息技术 安全技术 网络安全 第 6 部分：无线网络访问安全》2 项国家标准现已形成标准征求意见稿，现公开征求意见。据介绍，第一项标准给出了基于互联网电子政务的参考模型、网络安全技术体系、体系实施原则及两种安全体系实施架构；第二项标准描述了与无线网络相关的威胁、安全要求、安全控制和设计技术，为使用无线网络进行安全通信提供所需的技术选择、实施和监控指导。

工信部《国家智能制造标准体系建设指南 (2024)》公开征求意见

12 月 2 日，工业和信息化部科技司组织编制形成《国家智能制造标准体系建设指南（2024 版）》（征求意见稿），现公开征求社会各界意见。该文件提出，智能制造标准体系结构包括基础共性、关键技术、行业应用等 3 个部分，其中基础共性标准包括通用、安全、可靠性等 6 大类，位于体系结构的最底层。安全标准主要包括功能安全、网络安全、数据安全等 3 个部分。功能安全标准主要包括智能制造中功能安全系统的设计、实施、测试等标准。网络安全标准指以确保智能制造中相关终端设备、控制系统、工业互联网平台、工业数据等可用性、机密性、完整性为目标的标准，重点包括企业网络安全分类分级管理、安全管理、安全成熟度评估和密码应用等标准。数据安全标准主要包括工业数据质量管理、加密、脱敏及风险评估等标准。

国家数据局《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》公开征求意见

11 月 29 日，国家数据局会同有关部门研究起草了《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》，现公开征求意见。该文件要求到 2027 年年底，基本构建成规则明晰、产业繁荣、多方协同的数据流通安全治

理体系。该文件部署了七大主要任务，包括明晰企业数据流通安全规则、加强公共数据流通安全管理、强化个人信息流通保障、完善数据流通安全责任界定机制、加强数据流通安全技术应用、丰富数据流通安全服务供给、防范数据滥用风险。

中共中央办公厅、国务院办公厅公布《关于数字贸易改革创新发展的意见》

11 月 28 日，中共中央办公厅、国务院办公厅公布《关于数字贸易改革创新发展的意见》，要求按照创新为要、安全为基等原则，促进数字贸易改革创新发展。该文件共 18 条举措，其中涉及数字安全的有 2 条。一是促进和规范数据跨境流动。健全数据出境安全管理制度，完善相关机制程序，规范有序开展数据出境安全评估。在保障重要数据和个人信息安全的前提下，建立高效便利安全的数据跨境流动机制，促进数据跨境有序流动。二是加强数字领域安全治理。持续推动全球数字技术、产品和服务供应链开放、安全、稳定、可持续。

国家能源局印发《关于加强电力安全治理 以高水平安全保障新型电力系统高质量发展的意见》

11 月 27 日，国家能源局印发《关于加强电力安全治理 以高水平安全保障新型电力系统高质量发展的意见》。该文件共 5 章，包括总体要求、健全电力安全治理体系、增强电力安全治理能力、完善电力安全治理措施、提升电力安全监督管理效能。该文件多处涉及网络安全，如重点梳理涉网管理、运行控制、网络安全等与电力安全强相关的标准规范清单，在规划设计阶段针对重点地区、特殊场景合理提升设防标准；建立健全电力监控系统网络安全监测预警机制，进一步提高网络安全态势感知水平和应急处置能力；完善并网电厂涉网安全管理联席会议机制和网络安全联席会议机制。

七部门联合印发《推动数字金融高质量发展行动方案》

11 月 27 日，中国人民银行、国家发展改革委、工业和信息化部、金融监管总局、中国证监会、国家数据局、国家外汇局等七部门联合印发《推动数字金融高质量发展行动方案》。该文件共 6 章 23 条，其中 4 条涉及数字安全。一是营造高效安全的支付环境。确保支付系统安全、稳定、连续运行，持续完善广泛覆盖、高效安全的现代支付体系。二是培育高质量金融数据市场。在依法安全合规前提下，支持客户识别、信贷审批、风险核查等多维数据在金融机构间共享共用和高效流通，建立健全数据安全可信共享体系。三是强化数字金融风险防范。指导金融机构加强数字金融业务合规管理，多维度开展新技术应用适配测试与安全评估，引导金融机构持续提升信息系统安全可控水平，强化模型和算法风险管理，督促金融机构加强外包风险管理。四是加强数据和网络安全防护。指导金融机构严格落实数据保护法律法规和标准规范，组织金融机构定期进行数据和网络安全风险评估，开展网络安全相关压力测试，搭建证券业数据和网络安全公共服务平台等。

四部门联合印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》

11 月 26 日，公安部、国家发展和改革委员会、工业和信息化部、中国人民银行联合印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》。该文件的惩戒对象包括因实施电信网络诈骗及其关联犯罪被追究刑事责任的人；经认定具有非法买卖、出租、出借电话卡、物联网卡、固定电话、电信线路、短信端口、银行账号、支付账户、数字人民币钱包、互联网账号等行为的单位、个人或相关组织者。该文件提出，综合运用金融惩戒、电信网络惩戒、信用惩戒等惩戒措施，同时保留被惩戒对象基本的金融、通信服务，确保满足其基本生活需要。对不同惩戒对象分别设置 2 年或 3 年的惩戒时限，对惩戒期限内多次纳入惩戒名单的，连续执行惩戒期限不得超过 5 年。

国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》

11 月 23 日，国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》，提出到 2028 年，可信数据空间运营、技术、生态、标准、安全等体系取得突破，建成

100 个以上可信数据空间。该文件要求两类安全保障能力，一是安全防护能力，可信数据空间应针对数据流通的全生命周期，构建必要的防范、检测和阻断等技术手段，防止数据泄露、窃取、篡改等危险行为发生，并建立相关的管理制度和应急处置措施；二是合规监管能力，可信数据空间应监测空间中违反相关法律法规的行为，并应在行为发生时，及时采取相应的处置措施。

国家数据局《国家数据基础设施建设指引》公开征求意见

11 月 22 日，国家数据局组织起草了《国家数据基础设施建设指引（征求意见稿）》，现公开征求意见。该文件提出，国家数据基础设施应全程安全可靠，需要构建标准化、多层次、全方位的安全防护框架，推动安全防护由静态保护向动态保护、由边界安全向内生安全、由封闭环境保护向开放环境保护转变，形成贯穿数据全生命周期各环节的动态安全防护能力，系统保障数据基础设施相关的网络、算力、数据安全。该文件专门设立了“安全防护”章节，重点对国家数据基础设施安全保障、数据流通利用安全提出具体要求。

《网络安全标准实践指南——粤港澳大湾区（内地、香港）个人信息跨境处理保护要求》发布

11 月 21 日，网安标委秘书处联合香港私隐公署编制了《网络安全标准实践指南——粤港澳大湾区（内地、香港）个人信息跨境处理保护要求》，以促进粤港澳大湾区个人信息跨境安全有序流动。该文件规定了粤港澳大湾区（内地、香港）个人信息处理者或者接收方，在大湾区内地和香港间通过安全互认方式进行大湾区内个人信息跨境流动应遵守的基本原则和要求，适用于指导大湾区内个人信息处理者开展个人信息跨境处理活动。

《工业和信息化领域数据安全合规指引》正式发布

11月19日，中国钢铁工业协会、中国有色金属工业协会、中国石油和化学工业联合会等 17 家行业组织联合发布《工业和信息化领域数据安全合规指引》，引导工业和信息化领域数据处理者规范开展数据处理活动。该文件共 9 章，包括概述、数据分类分级、数据安全管理体系、数据全生命周期保护、数据安全风险监测 & 预警 & 报告 & 处置、数据安全事件应急处置、数据安全风险评估、数据出境安全管理、数据交易。该文件聚焦数据处理者在履行数据安全保护义务过程中的难点问题，明确数据安全合规依据，提供实务指引，指导数据处理者开展数据安全合规管理，以提升数据安全保护能力。

国家密码管理局《关键信息基础设施商用密码使用管理规定》公开征求意见

11 月 15 日，国家密码管理局研究起草了《关键信息基础设施商用密码使用管理规定（征求意见稿）》，现公开征求意见。该文件共 26 条。该文件要求，关键信息基础设施运营者应当加强关键信息基础设施商用密码使用的制度保障、人员保障、经费保障。该文件明确了商用密码使用具体要求，包括商用密码技术、产品、服务使用要求，数据安全保护、个人信息保护要求，规划、建设、运行等阶段要求及过渡安排，商用密码应用安全性评估要求。

国际

美国 2025 财年国防授权法案公布，聚焦提升美军网络攻防能力

12 月 7 日，美国国会两院军事委员会联合公布了 2025 财年国防授权法案的最终协议文本。该法案针对网络行动、网络安全、网络情报等事务向美国防部提出针对性要求。在网络行动方面，法案要求美国防部长将联合部队总部 – 国防信息网络指定为美国网络司令部下属的次级统一司令部；要求美国防部制订黑客马拉松计划，使得作战司令部指挥官和军事部门部长根据该计划每年举办不少于 4 次黑客马拉松；要求美国防部制订网络威胁桌面演习计划，

以通过桌面演习让国防部和国防工业基础为冲突或战争期间或冲突期间的网络攻击做好准备；要求美国防部定期向美国国会汇报云计算合同情况。在网络安全方面，法案要求美国防针对军事行动中使用的物联网硬件，制订应用零信任策略的指南；要求美国制订多云环境的管理和网络安全战略；要求美国防部对移动设备的网络安全产品和服务进行详细评估，以确定可以改善美国防部使用的移动设备网络安全的产品和服务，包括减轻国防部面临的风险针对移动设备的网络攻击。

美商务部发布 ICTS 最终规则，确保信息与通信技术和服务供应链安全

12 月 5 日，美国商务部工业和安全局发布关于《保障信息与通信技术和服务的供应链安全》的最终规则。该规则旨在加强美国对信息与通信技术和服务（ICTS）供应链的监管，明确调查所谓外国对手对美国信息与通信技术和服务交易造成威胁时，须遵循的审查程序，防范所谓外国对手通过 ICTS 产品或服务威胁美国国家安全、经济利益和关键基础设施。本次最终规则是为具体落实美国《国际紧急经济权力法》和《国家紧急法》下，授权签发的第 13873 号行政令而发布，在原有出口管制的复杂制度体系外，新增进口管制、供应链管理交叉领域的行政法律程序和措施。

欧洲理事会通过两项新法案加强网络安全

12 月 2 日，欧洲理事会通过两项关于网络安全的法案，旨在进一步加强欧盟抵御网络威胁的能力和网络团结合作。这两项法律分别为《网络团结法案》和《网络安全法案》修正案，属于欧盟网络安全立法“一揽子计划”的一部分。欧洲理事会声明称，《网络团结法案》构建了欧盟在应对网络威胁方面的能力，同时加强了合作机制。如欧盟将建立一个由国家和跨境网络中心组成的“网络安全警报系统”，以实现信息共享、检测并应对网络威胁。该法案还提出建立网络安全应急机制，以提高欧盟的突发事件响应能力。《网络安全法案》修正案承认托管安全服务在预防、检测、响应和恢复网络安全事件方面的重要性日益增加，该修正案将有助于提高托管安全服务的质量，培养值得信赖的网络安全服务商。

美国消费者金融保护局发布提案，限制“数据经纪人”出售个人信息

12 月 3 日，美国消费者金融保护局发布了一项拟议规则，计划针对“数据经纪人”出售美国人个人信息的行为，出台更加严格的监管措施。拟议规则利用已有的《公平信用报告法》第五条“关于消费者报告中包含信息的要求”，来限制敏感数据的出售，保护美国人免受犯罪和非法外国监视。拟议规则将贯彻《公平信用报告法》中对消费者报告和消费者报告机构的定义，《公平信用报告法》中有关消费者报告机构何时可以提供消费者报告，以及用户何时可以获得消费者报告的部分规定，以确保《公平信用报告法》的保护措施适用于该法规，控制出售美国人敏感个人和财务信息的数据经纪人。

美国土安全部发布《关键基础设施中人工智能的角色和职责框架》

11 月 14 日，美国国土安全部发布《关键基础设施中人工智能的角色和职责框架》，为在关键基础设施中安全开发和部署人工智能提供建议。该文件梳理了关键基础设施中人工智能的三类漏洞，包括利用人工智能的攻击、针对人工智能系统的攻击、设计和实施失败。为解决这些漏洞，该文件针对每个关键利益相关者提出了行动建议，包括云和计算设施提供商、人工智能开发商、关键基础设施所有者和运营商、公民组织、公共部门等。该文件将推动建立行业标准，增强透明度和问责制，保护公民的权利和自由。

欧盟发布《通用人工智能实践准则草案（初稿）》

11 月 14 日，欧盟人工智能办公室发布了《通用人工智能实践准则草案（初稿）》，并对外征求意见。该文件由 4 个工作组的独立专家共同编写，包括透明度与版权规则、系统性风险识别与评估、系统性风险技术缓解、系统性风险治理缓解，旨在为未来可信、安全的通用 AI 模型的开发与部署提供指导框架。该文件提出，具有系统性风险的通用人工智能模型提供者，应采用、落实并公开其安全保障框架（Safety and Security Framework），详细说明各类风险、缓解措施、映射过程及局限性。

事件篇

全球关键基础设施威胁态势严峻，多国遭遇重大网络攻击事件。勒索攻击致重要能源数字系统瘫痪，哥斯达黎加政府安抚民众燃油供应稳定；乌干达央行被黑，超 1.2 亿元被盗，近半或损失；以色列支付龙头遭 DDoS 攻击，各地超市加油站等 POS 机瘫痪。

国内最大 IT 社区 CSDN 被挂马，CDN 可能是罪魁祸首

12 月 12 日奇安信威胁情报中心公众号消息，奇安信威胁情报中心研究员近日观察到，某恶意域名的访问量从 9 月初陡增，10 月底开始爆发，并观察到恶意的 Payload，基于相关日志确认 CSDN 被挂马。奇安信全球鹰测绘数据显示，国内大量网站正文页面中包含该恶意域名，包含政府、互联网、媒体等网站，所涉及的域名均挂有 CDN，对应 IP 也都为 CDN 节点，由于该研究缺乏大网数据，只能推测 CDN 厂商疑似被污染。

国家安全部：境外间谍机关利用众包模式对我开展窃密活动

12 月 4 日国家安全部公众号消息，国家安全部发文称，近年来，国家安全机关工作发现，境外间谍情报机关利用众包模式对我开展窃密活动，手法尤为隐蔽，需引起警惕。个别境外间谍情报机关借此大肆搜集我海洋水文、矿产分布、能源储备、高精度地理信息等敏感数据，对我国家安全造成危害。国家安全部指出两类典型行为易涉及“众包窃密”，一是境外间谍情报机关可能假借软件开发为由，在“众包”平台发布信息数据征集任务，要求参与者安装其开发的专业地理测绘软件，并到指定点位上传数据即可获取相应物质奖励。其指定点位往往涉及我敏感涉密场所，众人多角度数据上传将对我敏感点位信息安全造成威胁。二是境外间谍情报机关可能利用众包模式，向参与者提供相关物联网设备，要求参与者自行架设，企图运用无线通讯和区块链技术搭建点对点的无线网络，让所有参与者成为网络的运营者之一，这样参与者本人及其所收集的信息数据均上传至该网络。因其网络覆盖面较大、匿名性较强、物理真实性较好，可能构建去中心化情报信息收集网络。

百年伏特加知名品牌因勒索软件攻击宣布破产

12 月 3 日华尔街日报消息，在美国子公司遭勒索软件攻击和俄罗斯政府没收其最后两家酒厂的双重打击下，Stoli 集团美国公司被迫申请破产保护。Stoli 集团在烈酒行业有着悠久历史，旗下品牌斯托利伏特加（Stolichnaya）是全球最知名的伏特加品牌之一。2024 年 8 月，Stoli 集团遭遇勒索软件攻击，公司 ERP 系统瘫痪，包括财务、供应链在内的核心业务全面转入手动操作模式。Stoli 美国子公司总裁克里斯·考德威尔透露，这一事件不仅造成运营中断，还导致公司无法向贷方提供财务报告，因而被指控违约债务达 7800 万美元。“我们预计，完全恢复 IT 系统至少要到 2025 年初。”考德威尔在破产文件中写道。他还表示，这次攻击的影响超出了 Stoli 集团的美国业务，还波及到集团的全球运营。

勒索攻击致重要能源数字系统瘫痪，哥国政府安抚民众燃油供应稳定

12 月 2 日 The Record 消息，北美洲国家哥斯达黎加的国家石油公司（RECOPE）近期遭遇勒索软件攻击，被迫转为手动操作并寻求国际援助。该公司表示，11 月 27 日清晨发现了勒索软件攻击，攻击导致所有用于支付的数字系

统瘫痪，他们不得不转而手动处理燃料销售。对此，油轮码头在 11 月 27 日将运营时间延长至深夜，并于次日进一步扩大运营时间。RECOPE 补充道，公司正在与哥斯达黎加科学、创新、技术和电信部合作解决这一问题，同时，多次在社交媒体上向全国公众保证，燃料供应充足。哥斯达黎加科学、创新、技术和电信部发布了独立声明，称其安全团队正全力协助恢复工作，并再次强调全国的燃料供应未受影响。自事件发生以来，该部门还多次发布公告，澄清有关其他国家机构遭遇网络攻击的谣言。

乌干达央行被黑：超 1.2 亿元被盗 近半或损失

11 月 29 日路透社消息，东非内陆国家乌干达财政部的一名高级官员证实，该国中央银行的账户遭到了黑客攻击。乌干达银行在 11 月 28 日晚间发布声明称，警方正对一篇新闻报道进行调查。该报道指出，离岸黑客从中央银行窃取了 620 亿乌干达先令（约合人民币 1.22 亿元）。当地国有媒体《新愿景报》报道，自称为“Waste”的东南亚黑客组织侵入了乌干达银行的 IT 系统，并在本月早些时候非法转移了资金至他国，目前乌干达已追回超过一半的被盗资金，官方称需等待审计工作完成后才能公布细节信息。负责财政事务的国务部长亨利 · 穆萨西齐确认了此次黑客事件，并表示警方刑事调查局和审计长办公室正在对此事展开深入调查。

严重损害数据安全，湖南一 IT 公司被罚 20 万元

11 月 29 日网信湖南公众号消息，湖南省互联网信息办公室依法查明，湖南某信息技术有限公司存在不履行网络安全、数据安全保护义务行为，其相关系统未采取技术措施和其他必要措施保障数据安全，存在未授权访问漏洞，造成部分数据多次泄露，严重损害数据安全。湖南省互联网信息办公室依据《中华人民共和国数据安全法》和《湖南省网络安全和信息化条例》对该公司责令改正，给予警告，并对该公司、主管人员和直接责任人员分别进行罚款二十万元、三万元和二万元的行政处罚。

前实习生篡改代码攻击大模型训练，字节跳动起诉索赔 800 万

11 月 27 日 AI 前哨站公众号消息，字节跳动起诉前实习生田某某篡改代码攻击公司内部模型训练一案，已获北京市海淀区人民法院正式受理。字节跳动请求法院，判令田某某赔偿公司侵权损失 800 万元及合理支出 2 万元，并公开赔礼道歉。此前字节跳动 11 月发布内部通报指出，2024 年 6 月至 7 月，集团商业产品与技术部门前实习员工田某某，因对团队资源分配不满，通过编写、篡改代码等形式，恶意攻击团队研究项目的模型训练任务，造成资源损耗。今年 10 月，有媒体称“字节大模型训练任务被实习生攻击”，并有网传信息称“涉及 8000 多卡、损失上千万美元”。后字节跳动回应称确有其事，但部分内容存在夸大及失实信息。

网站漏洞致用户信息长期被爬，两家美国保险商被罚超 8100 万元

11 月 25 日 BankinfoSecurity 消息，美国纽约州当局对汽车保险巨头 Geico 处以 975 万美元（约合人民币 7068 万元）罚款，原因是该公司未能妥善保护客户驾驶证号等信息，导致 2021 年年初发生一系列网络安全事件。保险巨头 Travelers 也被处以 155 万美元（约合人民币 1123 万元）罚款，原因是黑客在 2021 年中利用被盗凭据窃取了驾驶证号等信息。纽约州金融服务部的调查人员发现，这两家公司都发生过黑客访问内部系统窃取未加密数据的事件，攻击者利用明文传输、API 暴露、窃取管理账号等多种手法，持续爬取两家保险商线上系统的用户个人信息，并在新冠疫情期间，使用窃取的驾驶证号提交了虚假的失业救济申请。该部门联合州检察总办公室通过评估确定了罚款金额。

警惕攻击新型手法！俄黑客远程入侵美国企业 WiFi 进入内网

11 月 22 日 Volexity 消息，美国网络安全公司 Volexity 曝光了一起令人震惊的网络攻击事件，俄罗斯黑客组织 APT28 成功突破物理攻击范围，入侵了万里之外的一家美国企业的 WiFi 网络。2022 年 2 月，美国首都华盛顿一家企业的 WiFi 网络被发现遭遇了极不寻常的攻击，这次攻击被归因

于俄罗斯国家黑客组织 APT28，后者过一种名为“近邻攻击”的新技术，瞄准目标企业附近建筑内的其他企业，通过渗透这些企业的网络设备和笔记本电脑进行跳板式入侵，使用暴力破解获取的有效用户凭据，远程连接了目标企业的 WiFi 网络并实施进一步攻击。此次事件暴露了企业 WiFi 网络被忽视的致命盲区和漏洞，同时也展现了 APT28 不断创新的攻击方式。

国家网络安全通报中心：多个与某大国政府有关的境外黑客组织持续攻击国内单位企业

11 月 21 日国家网络安全通报中心消息，中国国家网络与信息安全信息通报中心第二次公告，持续发现一批境外恶意网址和恶意 IP，有多个具有某大国政府背景的境外黑客组织，利用这些网址和 IP 持续对中国和其他国家发起网络攻击。这些恶意网址和 IP 都与特定木马程序或木马程序控制端密切关联，网络攻击类型包括建立僵尸网络、网络钓鱼、勒索病毒、窃取商业秘密和知识产权、侵犯公民个人信息等，对中国国内联网单位和互联网用户构成重大威胁，部分活动已涉嫌刑事犯罪。相关恶意网址和恶意 IP 归属地主要涉及美国、德国、加拿大、新加坡、芬兰、保加利亚等。

网安巨头 Palo Alto 全球数千防火墙被攻陷：因开发低级错误造成 0day 漏洞

11 月 19 日 CSO 在线消息，国际网络安全巨头 Palo Alto Networks 日前修复了两个已被积极利用的漏洞（CVE-2024-0012、CVE-2024-9474），攻击者通过组合利用这两个 0day 漏洞，可实现远程完全控制 PAN-OS 安全设备。公司旗下搭载 PAN-OS 10.2、11.0、11.1 和 11.2 版本软件的防火墙及虚拟化安全设备均受影响。据第三方监测，自攻击活动开始以来，已有约 2000 台 PAN-OS 设备被入侵。研究人员对官方修复补丁进行逆向工程，发现这些漏洞源于开发中的低级错误。

因泄露超 23.5 万患者数据，美国地方医疗机构赔偿超千万元

11 月 15 日 GovinfoSecurity 消息，美国纽约州一家法院已初步批准一项 150 万美元（约合人民币 1086 万元）的和解协议，用于解决针对 One Brooklyn Health 健康系统的修订后合并拟议集体诉讼。该诉讼源于 2022 年 11 月的一次网络攻击事件，该事件导致超过 23.5 万人的敏感健康数据遭到泄露，泄露数据包括用户身份、支付、诊疗、处方、保险等大量信息。此次事件波及 One Brooklyn Health 旗下位于纽约市布鲁克林区的三家医院，包括 Brookdale 医院医疗中心、Interfaith 医疗中心和 Kingsbrook 犹太医疗中心，以及多个护理院和健康诊所。

美国知名律所因泄露用户个人信息赔偿超 5700 万元

11 月 12 日 GovinfoSecurity 消息，美国加利福尼亚北区联邦地区法院 8 日最终批准了针对奥睿律师事务所（Orrick, Herrington & Sutcliffe）的集体诉讼和解协议，总金额达 800 万美元（约合人民币 5782 万元）。根据和解协议，集体诉讼成员人均最高赔偿现金 7.2 万元及额外三年的信用监控服务，该律所还承诺部署持续漏洞扫描、EDR、MDR 等数据安全整改措施。该诉讼涉及一起 2023 年 3 月的黑客攻击事件，奥睿多个医疗保健客户受影响，泄露数据包括个人姓名、地址、出生日期、社会安全号码、健康信息等，涉及超过 63.8 万人。

以色列支付龙头遭 DDoS 攻击，各地超市加油站等 POS 机瘫痪

11 月 11 日 TheRecord 消息，以色列各地的信用卡刷卡设备在 10 日出现故障，疑似由于网络攻击影响了支撑这些设备运行的通信服务。超市和加油站的顾客因设备故障无法进行支付，事件持续了大约一个小时。据《耶路撒冷邮报》报道，故障原因是当地支付网关公司 Hyp 旗下产品 CreditGuard 遭到 DDoS 攻击，导致各地的 POS 机终端与线上支付服务断联，任何信息或支付数据均未受影响。据《以色列时报》报道，以色列第 12 频道新闻和陆军电台声称，一个与伊朗有关的黑客组织声称对此次攻击负责，但未提供具体信源。

漏洞篇

据奇安信鹰图资产测绘平台数据显示，近期披露的多个漏洞在国内均有大量资产受影响，包括 Palo Alto Networks PAN-OS 身份认证绕过漏洞 (CVE-2024-0012)、GitLab LFS Token 权限提升漏洞 (CVE-2024-8114)、ProjectSend 身份认证绕过漏洞 (CVE-2024-11680)、Zabbix SQL 注入漏洞 (CVE-2024-42327) 等，建议客户尽快做好自查及防护。

Apache Struts 文件上传漏洞安全风险通告

12 月 12 日，奇安信 CERT 监测到官方修复 Apache Struts 文件上传漏洞 (CVE-2024-53677)，Apache Struts 的文件上传逻辑中存在漏洞，若代码中使用了 FileUploadInterceptor，当进行文件上传时，攻击者可能构造恶意请求利用目录遍历等上传文件至其他目录。如果成功利用，攻击者可能能够执行远程代码、获取敏感数据、破坏网站内容或进行其他恶意活动。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

SonicWall SMA100 SSLVPN 多个高危漏洞安全风险通告

12 月 6 日，奇安信 CERT 监测到官方修复 SonicWall SMA100 SSLVPN Web 管理页面栈缓冲区溢出漏洞 (CVE-2024-45318) 和 SonicWall SMA100 mod_httprp 栈缓冲区溢出漏洞 (CVE-2024-53703)，SonicWall SMA100 SSLVPN 的 Web 管理界面和 Apache Web 服务器加载的 mod_httprp 库分别存在两个栈缓冲区溢出漏洞，这些漏洞可能允许远程攻击者执行任意代码，造成系统敏感数据泄露，甚至服务器被接管等严重安全威胁。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

ProFTPD 权限提升漏洞安全风险通告

12 月 4 日，奇安信 CERT 监测到官方修复 ProFTPD 权限提升漏洞 (CVE-2024-48651)。ProFTPD 是一款流行的 FTP 服务器软件。在 Linux 系统中，每个用户都有一个主组和零个或多个附加组，主组是用户登录时默认分配的组，而附加组是用户可以随时加入的其他组。此漏洞是由于在受影响的版本中，如果用户没有任何明确分配的附加组，则会继承 GID 为 0(root) 的附加组。这将允许攻击者获得对目标系统的 root 访问权限，最终可能导致系统完全受损。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 21447 个，关联 IP 总数为 20019 个。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Zabbix SQL 注入漏洞安全风险通告

12 月 2 日，奇安信 CERT 监测到官方修复 Zabbix SQL 注入漏洞 (CVE-2024-42327)，Zabbix 的 addRelatedObjects 函数的 CUser 类中存在 SQL 注入，此函数由 CUser.get 函数调用，具有 API 访问权限的用户可利用，造成越权访问高权限用户敏感信息及执行恶意 SQL 语句等危害。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 31748 个，关联 IP 总数为 6852 个。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

7-Zip 代码执行漏洞安全风险通告

11 月 30 日，奇安信 CERT 监测到 7-Zip 代码执行漏洞 (CVE-2024-11477)，由于对用户提供的数据缺乏验证，导致在写入内存前发生整数下溢，攻击者可能通过构造包含特制数据或压缩内容的恶意文件并诱使目标用户解压，从而执行任意代码。目前此漏洞细节和 PoC 已在互联网公开，奇安信 CERT 已成功复现，建议客户尽快做好自查及防护。

ProjectSend 身份认证绕过漏洞安全风险通告

11 月 28 日，奇安信 CERT 监测到 VulnCheck 分配 CVE-2024-11680，开源文件共享网络应用程序 ProjectSend r1720 之前的版本存在身份认证绕过漏洞，远程未经身份验证的攻击者可以通过向 options.php 发送精心设计的 HTTP 请求来利用此漏洞，从而在未经授权的情况下修改应用程序的配置。成功利用此漏洞后，攻击者可嵌入恶意代码、开启创建账户功能并上传 Webshell。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 10068 个，关联 IP 总数为 2925 个。鉴于此漏洞已发现在野利用，建议客户尽快做好自查及防护。

GitLab LFS Token 权限提升漏洞安全风险通告

11 月 27 日，奇安信 CERT 监测到官方修复 GitLab LFS Token 权限提升漏洞 (CVE-2024-8114)，由于 GitLab 对 LFS 令牌的处理存在缺陷，使得攻击者可以利用用户的个人访问令牌（PAT）来获取 LFS 令牌，进而以该用户的身份执行未经授权的操作，如读取或修改存储在 LFS 中的敏感文件。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 2246075 个，关联 IP 总数为 57863 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Apple 多个在野高危漏洞安全风险通告

11 月 20 日，奇安信 CERT 监测到 Apple 发布新版本修复了存在在野利用的 Apple 多款产品输入验证错误漏洞 (CVE-2024-44308)，远程攻击者可以诱骗受害者访问特制的网页并在系统上执行任意代码。Apple 多款产品跨站脚本漏洞 (CVE-2024-44309)，诱骗受害者点击特制的链接，在用户浏览器中的任意网站的上下文中执行任意 HTML 和脚本代码。鉴于这些漏洞已发现在野利用，建议客户尽快做好自查及防护。

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

11 月 19 日，奇安信 CERT 监测到官方修复 Palo Alto Networks PAN-OS 身份认证绕过漏洞 (CVE-2024-0012)，PAN-OS 设备管理 Web 界面中存在身份认证绕过漏洞，未经身份验证的远程攻击者可以通过网络访问管理 Web 界面，从而进行后续活动，包括修改设备配置、访问其他管理功能，甚至利用 Palo Alto Networks PAN-OS 权限提升漏洞 (CVE-2024-9474) 获取 root 访问权限。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 13039 个，关联 IP 总数为 2260 个。目前该漏洞技术细节与 PoC 已在互联网上公开，鉴于此漏洞已发现在野利用，建议客户尽快做好自查及防护。

Ivanti Endpoint Manager SQL 注入漏洞安全风险通告

11 月 13 日，奇安信 CERT 监测到官方修复 Ivanti Endpoint Manager SQL 注入漏洞 (CVE-2024-50330)，在 Ivanti EPM 的代理门户中，存在一个 SQL 注入漏洞。该漏洞允许远程未经身份验证的攻击者执行远程代码，从而控制受影响的系统，造成敏感信息泄露甚至获取系统权限等危害。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。

网络安全的年度记忆

——2024 年值得关注的网络安全现象

2024 年不同于往年，正在迎来前所未有的变局。在全球经济放缓的背景下，网络攻击却在持续加剧，勒索赎金创下历史新高，规模性数据泄露成为常态。作为网络守护者的安全设备，却已经成为攻击组织的目标。生成式人工智能带来的安全风险成为全球各国关注的焦点，各类监管法案与规范持续发布；开源软件的复杂供应链攻击，揭露了开源软件的严重安全威胁及资源严重不足的现实情况。

2024 年值得关注的 5 个安全现象

一、数据盗窃和勒索威胁持续增加

2024 年，多国发生多起数亿规模的数据泄露事件，使得大规模数据泄露成为行业需要面对的常态。

2024 年 1 月，据印度网络安全公司 CloudSEK 披露，一个包含约 7.5 亿印度个人信息的庞大数据库在暗网上出售。该数据库大小为 1.8TB，包含姓名、手机号码、地址和 Aadhaar 个人身份识别码等个人信息。对黑客发布的样本数据集进行分析后发现，这些信息来自印度所有主要电信运营商用户。

2024 年 4 月 8 日，美国国家公共数据（NPD）遭到攻击，导致 29 亿条个人隐私数据泄露，这也是仅次于 2013 年雅虎事件（影响 30 亿）的数据泄露事件。被盗信息为美国、英国和加拿大个人的高度敏感个人信息，包括姓名、社会保障号、家庭住址和已知亲属。事件直接导致国家公共数据公司申请破产。

9 月 23 日，美国背景调查和公共记录服务公司 MC2 Data 发生大规模数据泄露事件，暴露了该公司 2.2TB 的敏感数据，包含超过 1 亿美国公民的个人信息，涉及姓名、电子邮箱、电话号码、家庭住址、加密的密码、部分支付信息、房产记录、法律记录、就业经历、家庭亲戚及邻居信息等，严重威胁了个人隐私与信息安全。

此外，2024 年勒索软件继续占据新闻头条，网络行业报告显示，2024 年勒索软件的数量保持稳定或增长，成为全球企业面临的最普遍威胁之一。勒索软件攻击日益复杂，对各个行业造成巨大的财务、运营和声誉损失。

勒索软件攻击不再仅限于加密数据以索要赎金，而是普遍采取“双重勒索”手段，即除了锁定系统，还会窃取敏感信息。受害者不仅面临无法访问其数据的威胁，还面临机密信息在暗网上出售

或公开曝光的风险。

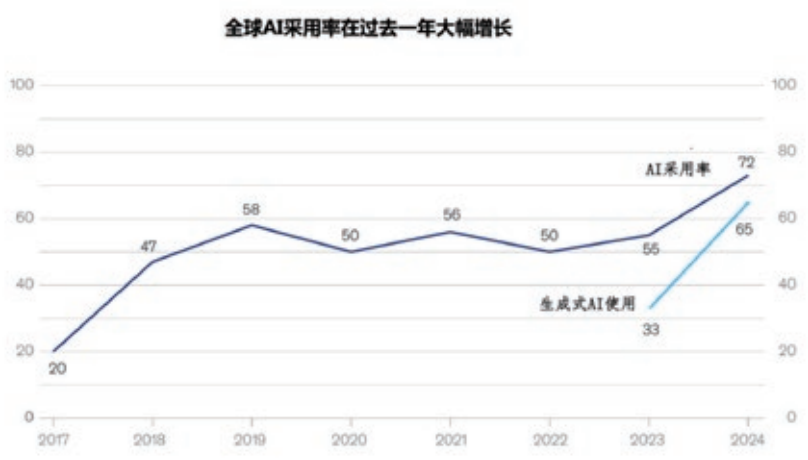
2024 年，银行机构、科技行业，以及医疗保健行业的勒索软件攻击最为严重。2024 年 2 月，美国最大的医疗 IT 公司 Change Healthcare 遭受勒索软件攻击——这是历史上最严重的医疗保健网络攻击，也是有史以来最大的医疗保健数据泄露事件。攻击组织窃取了约 1 亿人的个人、健康和财务信息。攻击对美国医疗系统产生了重大影响，导致许多药店无法处理处方。

2024 年，勒索赎金创下历史新高。黑暗天使勒索组织，从一位未具名的受害者那里获取了 7500 万美元（约合人民币 5.42 亿元）的赎金，是全球有史以来最大金额的赎金。几乎是此前公开报道的勒索软件赎金最高记录的两倍，但即使支付赎金也不能保证数据恢复。勒索软件报告发现攻击后 43% 的数据无法恢复。

漏洞利用仍然是勒索软件攻击最常见的根本原因。钓鱼邮件攻击也是重要的途径。来自未修补漏洞的攻击会产生更严重的后果，包括更高的赎金要求和更长的恢复时间。

二、生成式人工智能快速崛起引发安全忧虑

如果说 2023 年是世界发现生成式人工智能的一年，2024 年则是各类组织真正开始使用这项新技术并获取商业价值的一年。2024 年，AI 应用激增，人工智能整变得无处不在。2024 年麦肯锡全球人工智能的调查发现，AI 采用率已跃升至 72%，而且这种趋势是全球性的。生成式 AI 的使用率则高达



65%，是 10 个月前调查的两倍。从行业来看，专业服务业的采用率增幅最大。

生成式人工智能的快速崛起带来了新的风险和监管挑战，包括信息泄露、不准确或有害输出等，各国正在为生成式人工智能可能带来的潜在风险做好准备。加强对人工智能的监管，确保大模型安全开发和使用，成为 2024 全球的热点。

2024 年 3 月，联合国大会通过首项关于人工智能的决议——关于“抓住安全、可靠和值得信赖的人工智能系统机遇，促进可持续发展”的 A/78/L.49 号决议。决议草案由 125 个国家共同发起，强调不当或恶意使用人工智能系统所带来的风险，尤其是偏见数据所带来的风险。联合国大会“决心促进安全、可靠和值得信赖的人工智能系统，以在全面实现《2030 年可持续发展议程》方面加快取得进展”。决议内容将在未来进一步指导国家和国际层面对人工智能技术的监管发展。

我国针对人工智能，尤其是生成式人工智能的安全与治理，陆续发布了多项标准与指南。包括，3 月 4 日，全国网络安全标准化技术委员会发布《生成式人工智能服务安全基本要求》技术文件，规定了生成式人工智能服务在安全方面的基本要求，包括语料安全、模型安全、安全措施等，并给出了安全评估要求，适用于服务提供者开展安全评估、提高安全水平，也可为相关主管部门评判生成式人工智能服务安全水平提供参考。

5 月 23 日，全国网络安全标准化技术委员会发布国家标准《网络安全技术 生成式人工智能服务安全基本要求》征求意见稿，规定了生成式人工智能服

务在安全方面的基本要求，包括训练数据安全、模型安全、安全措施等，并给出了安全评估参考要点。

9 月 9 日，全国网络安全标准化技术委员会发布《人工智能安全治理框架》1.0 版，以有效防范化解人工智能安全风险为出发点和落脚点，提出了包容审慎、确保安全，风险导向、敏捷治理，技管结合、协同应对，开放合作、共治共享等人工智能安全治理的原则。

9 月 14 日，中央网络安全和信息化委员会办公室发布《网络安全技术人工智能生成合成内容标识方法》国家标准的征求意见稿，描述了人工智能生成合成内容显式标识和隐式标识的方法，适用于规范生成合成服务提供者和内容传播服务提供者对人工智能生成合成内容开展的标识活动。

在此前，欧洲议会于 2024 年 3 月通过了《人工智能法案》，并于 8 月 1 日生效。欧盟《人工智能法案》是全球首部全面监管人工智能的法规。其目的在于，推动普及值得信赖的人工智能。

与欧盟强化 AI 治理不同，美国的 AI 治理具有“发展为先、基于实证、顶层设计、行政牵引、场景立法、小步快走”的特征。美国政府于 10 月 24 日发布首份关于人工智能的国家安全备忘录，旨在确保美国在抓住人工智能机遇和管理人工智能风险方面发挥领军作用，鼓励联邦政府采用人工智能来推进国家安全使命，并寻求塑造围绕人工智能使用的国际规范。

加州议会通过的《安全与可靠前沿人工智能创新法案》(SB-1047)，被加州州长以“监管要基于技术发展和风险实证”“风险监管离不开场景”“不能仅仅因为大而监管”而否决，对我国 AI 治理也颇具启发意义，即治理应体现激励相容、鼓励创新原则；治理应基于科学、基于实证，不过分夸大风险，软法为先；治理应基于场景、基于痛 / 难点、小步快走，防止大而全、形而上。

三、微软蓝屏带来网络弹性教训

2024 年 7 月，全球企业和政府因重大 IT 系统宕机而陷入混乱，850 万台 微软 Windows 设备受到影响，导致全球航空公司、银行、广播公司、医疗保健提供商、零售支付终端和自动取款机大面积中断，估计损失达 10 亿美

元。

此次大面积系统宕机是由全球领先网络安全公司 CrowdStrike 的安全软件 Falcon 更新引发的，简单的配置文件更新让数百万台 Windows 系统瘫痪。CrowdStrike 引发的大面积 IT 系统故障，肯定会在人类重大技术故障史占据重要地位。

值得警惕的是，软件企业匆忙发布更新，并将其直接推送到全球环境已成为主流，这意味着任何软件供应商都可能再次制造此类混乱。

首先，微软把责任推给了网络安全公司 CrowdStrike，但微软应承担一部分责任。长期以来，全球用户把 IT 鸡蛋放在微软 Windows 篮子里。篮子被打翻导致鸡飞蛋打的后果难以避免。CrowdStrike 用户少，中国 Windows 用户受影响较小，但这不是我们庆幸的理由。一方面推动国产操作系统的 Windows 替代，可以避免鸡蛋都放在“微软 Windows 篮子里”的风险，但少数本土操作系统软件主导同样会面临可靠性挑战。毕竟国产化仅仅实现了可控目标，而非安全与可靠的保障。

其次，CrowdStrike 是此次故障的罪魁祸首，凸显出网络安全公司在速度和质量间的艰难平衡。作为以技术卓越和速度而闻名的企业，CrowdStrike 深受用户信任，但很少有人会想到，本来用以避免混乱的安全公司会成为史上最大 IT 故障的肇事者。安全形势瞬息万变，安全企业每天都会发布更新。CrowdStrike 可能为保持敏捷性而牺牲了一些步骤，或者对风险评估松懈了。部署任何更新前，都应进行彻底测试，尤其是在软件对关键系统

组件具有最高程度的访问权限时。未在临时或测试环境中进行充分测试，就把更新部署到生产环境，无疑会制造灾难性的后果。对于 CrowdStrike 这样规模的企业来说，这种根本性错误是不可原谅的。

IT 企业应警醒： 在保护用户免受威胁时，不应忽视自身可能造成的风险。较高的开发质量、严格的测试、应对故障的安全机制和适度的谦逊必不可少。对政企用户来说，在选择安全供应商时，也应将具有较高开发质量保障和是否有充分测试作为重要标准之一。

CrowdStrike 制造的系统故障，可以被视为墨菲定律的典型实例——任何可能出错的事情最终都会出错。

对微软蓝屏事件的教训，我们需要进行深入总结。毕竟，网络安全的下一个重大威胁可能是另一次更新。事件的灾难后果提醒我们，智能融合时代的数字基础设施是多么脆弱，以及网络弹性在数字世界中的重要性。

四、更多攻击活动瞄向网络安全设备

在 2024 年，网络攻击组织特别关注针对防火墙和 VPN 等网络安全设备进行攻击。这些安全设备作为 IT 环境的前门，使其成为备受青睐的目标。

2024 年刚过两周，网络安全界就遭遇了危机，Ivanti VPN 被大规模利用。这一攻击标志着 2024 年网络攻击的主要主题之一——攻击者针对网络安全设备进行攻击。正如 Xage Security 首席执行官 Geoffrey Mattson 所说，攻击的讽刺之处在于“安全设备让业界变得不那么安全，访问设备为坏人提供了访问权限”。

2024 年 1 月，安全供应商 Ivanti 确认其 Connect Secure 和 Policy Secure 网关中存在两个 0day 漏洞。

有关漏洞和野外攻击的报告迅速出现，影响了政府、军事、电信、技术、金融、咨询和航空航天等多个领域的客户。研究人员表示，数千台 Ivanti VPN 设备遭到入侵。美国网络安全和基础设施安全局（CISA）发布了一项紧急指令，要求所有政府民事联邦机构修复两个 0day 漏洞。

2024 年 2 月，CISA 披露，影响 Fortinet FortiOS 操作系统多个版本的“严重”漏洞正被利用进行攻击；10 月份，攻击者又利用 Fortinet FortiManager 中的 一个严重漏洞，开展国家间谍活动。4 月份，思科系统披露了两个 0day 防火墙漏洞，并宣称遭受国家背景攻击者的利用，开展针对全球政府的间谍活动。与此同时，9 月份，Arctic Wolf 的研究人员表示，攻击者正在利用一个影响多种 SonicWall 防火墙的严重漏洞，部署勒索软件。

11 月份，研究人员披露，攻击者利用派拓网络（PAN） AN-OS 软件两个 0day 漏洞（CVE-2024-0012、CVE-2024-9474），实现远程完全控制 PAN-OS 安全设备。公司旗下搭载 PAN-OS 10.2、11.0、11.1 和 11.2 版本软件的防火墙及虚拟化安全设备均受影响，至少已有约 2000 台 PAN-OS 安全设备被入侵。据第三方监测，自攻击活动开始以来，研究人员对官方修复补丁进行逆向工程，发现这些漏洞源于开发中的低级错误。

安全专家表示，没有迹象表明针对防火墙和 VPN 的攻击会在短期内减少。这些安全设备已经成为有吸引力的攻击目标，因为一旦黑客侵入防火墙、路由器或 VPN 系统，就处于非常适合发起攻击的位置。

五、XZ 后门事件揭露开源安全残酷真相

震惊开源社区的 XZ 恶意后门，揭开了一场精心策划、实施多年的供应链攻击，这一对 Linux 系统构成严重威胁的事件，为开源软件安全再次敲响警钟。

3 月底，开源软件领域披露了一场差点就要成功的软件供应链攻击：广泛采用提供数据压缩功能的开源 XZ Utils 组件，被发现植入后门。

这个后门被评为 CVSS 10 分（严重程度最高级），如果未被及时发现，将会酝酿出一场重大的全球网络安全危机。安全专家表示，这可能是开源项目有史以来最复杂的供应链攻击。攻击的复杂程度反映出攻击者是经过精心策划才实施的：攻击者逐步获得合法开发人员的信任，甚至成为其核心维护团队的成员，从而使能在不被注意的情况下植入后门。

现在，手机、汽车、飞机，甚至许多尖端人工智能程序都使用开源软件。《2024 年开源安全与风险分析报告》发现，其所研究的代码库中 96% 包含开源代码。

但 XZ 后门事件说明，企业软件堆栈中嵌入的大部分开源代码来自小型、资源不足、由志愿者运营的项目。这意味着使用开源组件的组织最终要对软件的安全负责。

对开源软件安全性的担忧并非新鲜事。但通常只有像 Log4Shell 漏洞和 XZ Utils 后门的发现，才能真正让人们意识到组织所使用代码组件的脆弱性。这些代码通常来自资源严重不足且维护极少的开源项目。

供应链攻击并不是一个新问题，XZ 后门的新颖之处，在于攻击者获得了对行业普遍使用代码的访问权限，禁用了检测所利用功能的安全工具，并在广泛使用的程序植入了高度复杂的后门。实际上，2021 年至 2024 年 2 月期间，攻击者对至少 7 个开源项目提交了 6000 次代码更改。安全专家认为，要确定这些更新的所有影响几乎是不可能的。

Tidelift 联合创始人兼首席执行官唐纳德 · 菲舍尔指出，大多数组织对其软件供应链这一部分的安全性和弹性缺乏足够的了解，因此无法评估风险。XZ utils 黑客攻击凸显了企业组织所依赖的开源软件供应链的健康和弹性投资不足的风险。

开放源代码安全基金会和 OpenJS 基金会在一份联合声明中表示，试图在 XZ Utils 中插入后门的行为“可能并不是孤立事件”。他们表示，至少有三个不同的 JavaScript 项目成为攻击目标。攻击者要求进行可疑更新或要求成为目标软件的维护者。

针对 XZ 后门事件，用户可以根据奇安信威胁情报部门发布的“事件紧急通告”，来检测当前环境是否可能使用后门版本的 XZ Utils。但在开源组件普遍的环境下，最紧迫的是必须实施管理开源风险的措施，就像管理内部开发的代码一样。

2024 年度漏洞态势：数量持续增长再创新高

2024 年，全球网络安全领域继续面对日益严峻的挑战。在数字化转型的大背景下，漏洞利用成为网络攻击的重中之重。根据统计，全球新增漏洞数量再创新高，漏洞的复杂性加剧，修复周期也在不断缩短。然而，攻击者的手段日趋复杂，基于漏洞的攻击路径更加隐蔽且复合化。开源项目、云计算、物联网（IoT）、国产软件及关键基础设施领域漏洞威胁显著增加。

一、漏洞数量：同比增长 46.7%。

2024 年 1 月 1 日至 12 月 31 日期间，奇安信安全监测与响应中心（又称奇安信 CERT）共监测到新增漏洞 43757 个，较 2023 年同比增长 46.7%。其中，有 5498 个高危漏洞触发了人工研判。经研判：本年度值得重点关注的漏洞共 965 个，达到奇安信 CERT 发布安全风险通告标准的漏洞共 392 个，并对其中 82 个漏洞进行深度分析 。其中，高危、极危漏洞数量为 7777 个，占总量的 17.8%。

漏洞数量激增的主要原因包括技术生态复杂化、开源组件应用增加及攻击者专业化程度提升。2024 年奇安信 CERT 漏洞库每月新增漏洞信息数量如图 1-1 所示。

2024 年漏洞披露高峰为 1 月和 6 月，这与年度安全更新周期和大规模披露活动相关。攻击集中时间在下半年，攻击者利用企业年末漏洞修复滞后的情况。

二、漏洞类型：三种类型最高

代码执行、信息泄露和权限提升是攻击者利用的核心手段，特别是在复杂攻击链中。 根据漏洞威胁类型，对 2024 年度新增 43757 个漏洞进行分类总结，如图 1-2 所示。

图 1-1 2024 年奇安信 CERT 漏洞库每月新增漏洞信息数量

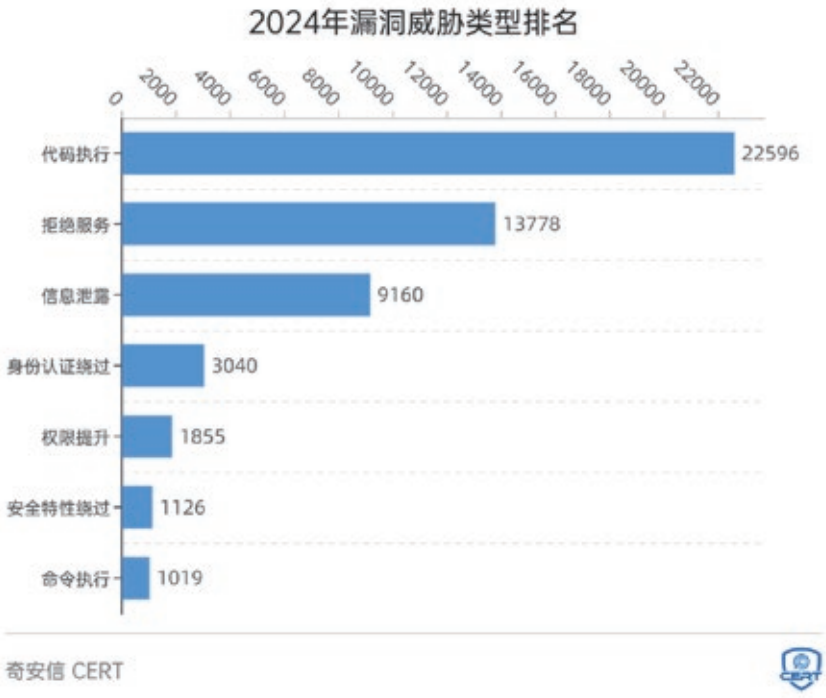


图 1-2 漏洞威胁类型排名

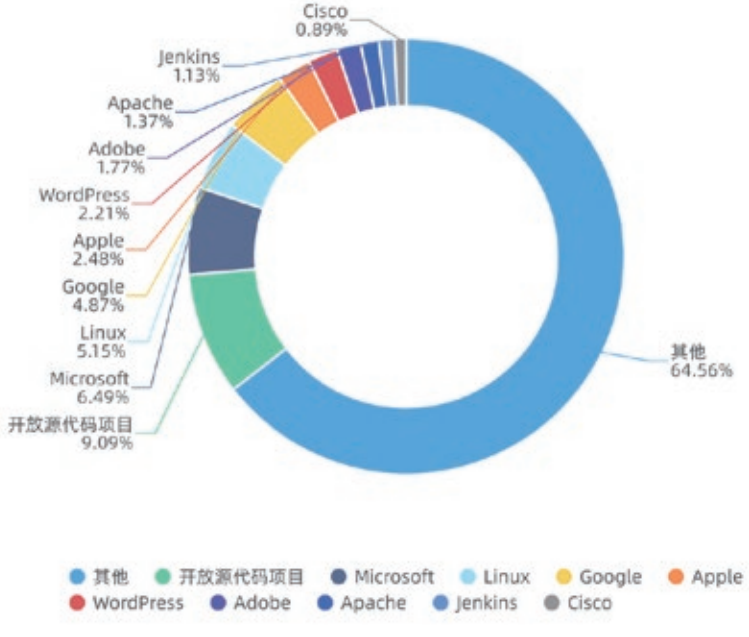


图 1-3 漏洞影响厂商占比

其中漏洞数量占比最高的前三种类型分别为：代码执行、拒绝服务、信息泄露。这些类型的漏洞通常很容易被发现、利用，其中代码执行、权限提升等类型的漏洞可以让攻击者完全接管系统、窃取数据或阻止应用程序运行，具有很高的危险性，是安全从业人员的重点关注对象。

三、漏洞分布：开源项目最多

将 2024 年度新增的 43757 个漏洞信息根据漏洞影响厂商进行分类总结，如图 1-3 所示：

其中漏洞数量占比最高的前十家厂商为：开放源代码项目、Microsoft、Linux、Google、Apple、WordPress、Adobe、Apache、Jenkins、Cisco。Google、Microsoft、Apple 这些厂商漏洞多发，且因为其有节奏的发布安全补丁，为漏洞处置的关注重点。开源软件和应用在企业中被使用的越来越多，关注度逐渐攀升。部署在网络边界的网络设备在攻防行动中占据了重要地位，因而获得了安全研究员的重点关注。

2024 年新增的 43757 个漏洞中，有 706 个漏洞在 NVD 上没有相应的 CVE 编号，未被国外漏洞库收录，为国产软件漏洞，占比情况如图 1-4 所示。这些漏洞重 OA 和 ERP 系统尤为突出。受影响行业包括：政府机构（APT 攻击的首要目标）、金融领域（高危漏洞利用频发）、能源与关键基础设施（攻击者重点关注的领域）。

热度排名	漏洞名称	漏洞编号	危险等级	修复建议
1	OpenSSH 远程代码执行漏洞	CVE-2024-6387	高危	升级至 OpenSSH 9.8p1 或更高版本
2	Windows 远程桌面授权服务远程代码执行漏洞	CVE-2024-38077	高危	安装补丁
3	Windows TCP/IP IPv6 远程拒绝服务 / 代码执行漏洞	CVE-2024-38063	高危	安装补丁
4	XZ Utils 工具库恶意后门植入漏洞	CVE-2024-3094	高危	目前官方尚无最新版本，需对软件版本进行降级 5.4.X，请关注官方新版本发布并及时更新
5	Oracle WebLogic Server JNDI 注入漏洞	CVE-2024-20931	高危	安装补丁
6	Internet 快捷方式文件安全特性绕过漏洞	CVE-2024-21412	高危	安装补丁
7	7-Zip 代码执行漏洞	CVE-2024-11477	高危	升级至 7-Zip 24.07 或更高版本
8	VMware vCenter Server 多个堆溢出漏洞	CVE-2024-37079 CVE-2024-37080	高危	建议受影响用户升级至最新版本：VMware vCenter Server 8.0 U2d、VMware vCenter Server 8.0 U1e、VMware vCenter Server 7.0 U3r、VMware Cloud Foundation 5.x/4.x KB88287
9	Jenkins Remoting 任意文件读取漏洞	CVE-2024-43044	高危	升级至 Jenkins 2.471、LTS 2.452.4、LTS 2.462.1 或更高版本
10	Apache Tomcat 拒绝服务漏洞	CVE-2024-34750	高危	升级至 Apache Tomcat 9.0.90、10.1.25、11.0.0-M21 或更高的版本

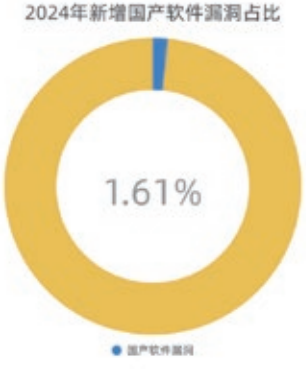


图 1-4 国产软件漏洞占比

此类漏洞具有较高威胁，如果被国家背景攻击组织利用将导致严重后果。

四、漏洞热度排名 TOP 10

根据奇安信 CERT 的监测数据，2024 年漏洞舆论热度榜 TOP 10 漏洞如上表：

在本年度总热度舆论榜前十的漏洞中，热度最高的漏洞为 OpenSSH 远程代码执行漏洞 (CVE-2024-6387)。该漏洞是由于 OpenSSH 服务器 (sshd) 中的信号处理程序竞争问题，未经身份验证的攻击者可以利用此漏洞在 Linux 系统上以 root 身份执行任意代码。该漏洞为之前 CVE-2006-5051 的二次引入，当前的漏洞利用代码仅针对在 32 位 Linux 系统上运行的 OpenSSH，64 位 Linux 系统上利用该漏洞的难度会更大，在 Linux 系统上以 Glibc 编译的 OpenSSH 上成功利用，不过利用过程复杂、成功率不高且耗时较长。平均要大于 10000 次才能赢得竞争条件，需要 6~8 小时才能获得远程 root shell。在以非 Glibc 编译的 OpenSSH 上利用此漏洞也是可能的，但尚未证实。虽然目前还没有发现真正实现远程代码执行的 PoC，鉴于此漏洞影响范围较大，建议受影响用户升级至 OpenSSH 9.8p1。

五、2024 年最危险的 CWE

CWE 是代码、设计或架构中可能导致漏洞的常见软件弱点或缺陷的列表，它们本身列在常见漏洞和披露（CVE）数据库中。某些漏洞通常很容易找到并被加以利用，攻击者通过这些漏洞能够窃取数据、完全接管系统或阻止应用程序运行。CWE 是这些漏洞的根本原因。

为了定义软件弱点的严重性级别，2024 年，奇安信 CERT 汇集本年度 7777 个高危、极危漏洞，从中总结出

最危险 CWE 列表供参考。2024 年最危险 CWE 排行如图 1-8 所示，该排名不仅为开发人员和安全专业人员提供了可靠信息，还为企业和公司提供了安全战略指南。

2024 年，在 7777 个高危、极危漏洞中，数据验证不恰当（也称为“输入验证不恰当“（CWE-20））占据首位，有 1201 个漏洞，占总数的 15.44%。

SQL 注入，也称为“SQL 命令中使用的特殊元素的不当中和”（CWE-89）位居第二，有 608 个漏洞，且存在很多已知被利用的相关漏洞，占总数的 7.82%。

第三名是释放后重用（CWE-416），有 494 个漏洞，占总数的 6.35%。

建议查看此列表并通过它获悉软件安全策略。在开发和采购流程中优先考虑这些弱点有助于防止软件生命周期核心的漏洞。

六、漏洞修复时效性

2024 年漏洞平均修复时间：45 天，较 2023 年缩短 10%。0day 漏洞修复不足：75 个。0day 漏洞中 30% 修复时间超过 30 天，部分漏洞已在披露前被利用。披露与利用时间差：公开后 4 天内被利用的漏洞占 50%。

值得注意的是，2024 年新增的 43757 个漏洞中，有 33564 个漏洞存在 CVE 编号，其中有 9602 个存在 CVE 的漏洞，在 NVD（National Vulnerability Database，美国国家漏洞数据库）收录前，奇安信 CERT 优先收录，占本年度存在 CVE 漏洞总数的 28.6%，且漏洞平均定级速度快于 NVD 约 61%。这些漏洞通过奇安信 CERT 多源汇聚技术，在厂商发布安全通告的第一时间即可捕获漏洞信息，由分析人员研判入库。快于 NVD 占比如图 1-9 和图 1-10 所示：

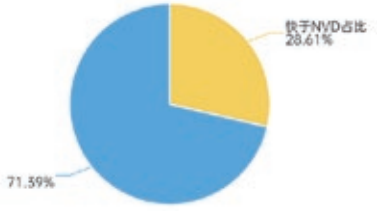


图 1-9 漏洞收录快于 NVD 占比

图 1-10 漏洞定级速度快于 NVD 占比

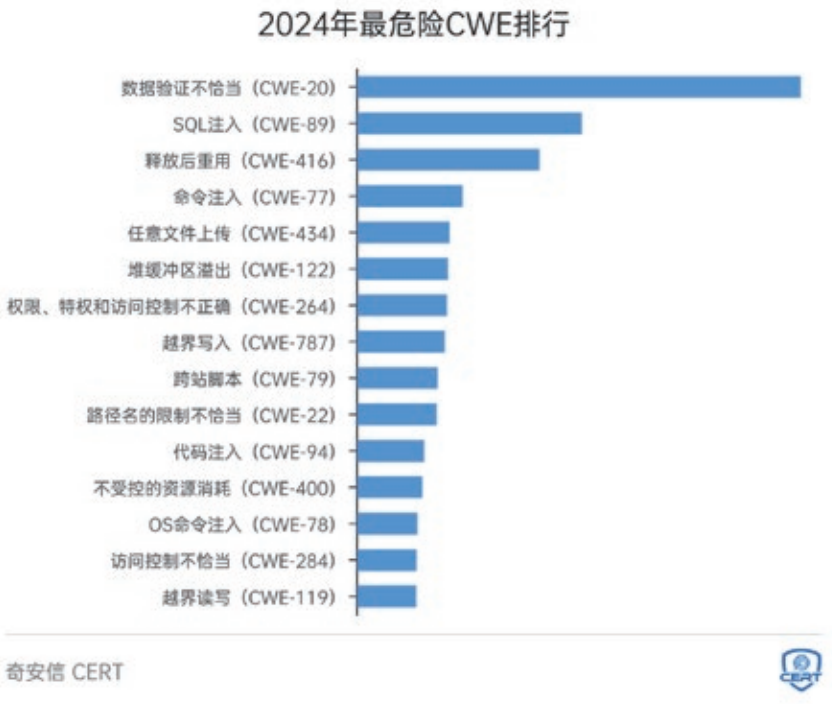


图 1-8 2024 年最危险 CWE 排行

在这些漏洞中，奇安信 CERT 漏洞收录时间平均快 NVD 约 6 天 4 小时，其中，Rancher Kubernetes Engine 信息泄露漏洞（CVE-2023-32191）收录时间快 NVD 约 119 天，达到本年度之最。奇安信 CERT 在 2024 年 6 月 20 日捕获漏洞信息源，由分析人员研判入库，而 NVD 在长达 119 天后的 2024 年 10 月 16 日公开此漏洞。漏洞时间线如

2024 年 06 月 11 日	Rancher 通告 Github 公开修复漏洞
2024 年 06 月 18 日	SNYK 率先发布 CVE，公开漏洞信息
2024 年 06 月 20 日	奇安信 CERT 捕获到厂商发布 CVE，分析人员研判入库
2024 年 10 月 16 日	NVD 发布并公开 CVE 信息

表 1-11 CVE-2023-32191 漏洞公开时间线

表 1-11 所示。

漏洞发现的时效性在网络安全领域至关重要，它直接影响到组织和个人的数据安全、业务连续性和声誉。漏洞发现得越早，攻击者利用该漏洞进行攻击的时间窗口就越小。及时的漏洞发现可以减少攻击者利用漏洞的机会。一旦发现漏洞，组织可以迅速采取行动，如打补丁、更新系统或采取临时的缓解措施，以防止潜在的攻击。及时修复漏洞可以减少数据泄露、服务中断和其他安全事件造成的损害，从而降低相关的财务成本和声誉损失。

七、通用处置建议及最佳实践

✓ 网络访问限制：关闭网络设备管理接口，如 Telnet、SSH、Winbox，以及用于广域网（WAN）的 HTTP。使用强安全性的密码和加密来保护通信。

✓ 网络分段：对设备的网络进行适当的分段，使其只能与支持其特定业务功能的设备通信。

✓ 密码保护：强制使用复杂密码及多因素身份验证（MFA），包括第三方服务账户。同时考虑提供密码管理服务，以防止在浏览器中存储凭据。

✓ 账户清单：对系统中的服务账户和其他特权账户进行清单盘点。确保它们遵循最小特权原则，并为其配置长而复杂的密码。限制这些账户在整个系统中的使用范围。

✓ 全面覆盖：对所有设备和系统启用适当的防病毒软件或端点检测和响应工具，以提供对利用或威胁活动的最大可见性。有价值的检测用例需要端点日志记录或可见性记录。

✓ 资产清单：确保拥有一个完整且定时更新的资产清单，并对所有使用设备和应用程序的版本号进行详细说明。

✓ 补丁管理：检测软件升级，并将补丁应用于具有高严重性或已知在野利用漏洞的系统。

✓ 缓解措施：如果无法立即应用补丁或补丁失效，请实施厂商提供的缓解措施。

✓ 最大可见性：增加对易受攻击设备的日志记录。这将扩展现有警报的覆盖范围，并允许实施更多检测用例，以捕捉异常行为或可疑的内部流量。

✓ 最新风险通知：奇安信漏洞订阅服务可以帮助你从互联网海量的漏洞信息里筛选出真正有价值的那一部分，及时获得与组织相关的安全漏洞情报。

从技术抗衡走向体系化国家力量比拼

——2024 全球网络战呈现五大特点

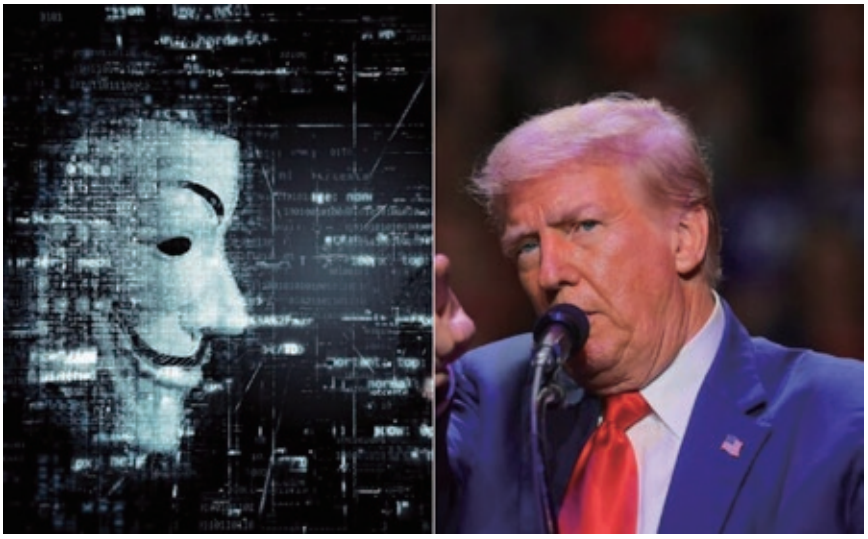
2024 年，全球网络空间呈现区域性和阵营性紧张态势，世界强国国防网络建设竞争持续加速，网络空间正加速演变为战略威慑与控制新领域。国家间网络斗争博弈日益加剧，网络空间斗争从技术力量抗衡走向体系化国家力量比拼，网络战成为国家实现政治、军事、经济等利益的重要手段。

一、实施针对政治安全的“网络干扰选举战”，具有“统筹运作、多管齐下”的特点。

互联网近年来已成为政治角力新战场，网络攻击政治化趋势日益明显。“网络干扰选举战”是指，在网络空间发起的针对选举系统、候选人、选民等网络攻击和网络影响力活动，旨在阻碍选举进程、扭曲选举结果并破坏国家政治生态。2024 年是“超级选举年”，全球超过 50 个国家举行选举，包括美俄总统大选、欧洲议会选举等，地缘政治紧张、局势紧张引发诸多针对选举的高强度、针对性网络干扰活动。

针对美国大选的网络干扰活动上升到新高度，网络攻击和网络影响力活动层出不穷。冒充美国总统拜登的假机器人电话 1 月 21 日开始在新罕布什尔州流传，敦促民主党人不要在初选中投票，这是首个使用人工智能生成音频虚假信息干扰美国选举的案例。特朗普的竞选团队 8 月 10 日表示，伊朗黑客攻击并泄露其内部通讯信息，目的是干涉 2024 年大选并在美民主进程中制造混乱。为特朗普提供咨询的美国优先政策研究所的计算机系统 10 月 12 日遭网络入侵，成为第二起因支持特朗普而成为网络攻击目标的事件。

微软威胁分析中心 4 月 17 日发布报告称，COLDRIVER 等俄罗斯黑客组织的网络活动显著增加，可能



是旨在推动干扰美国 11 月大选系列黑客活动的“第一波”。网络安全公司 Recorded Future 于 6 月 24 日发布报告称，与俄罗斯有关的威胁行为者 CopyCop 正试图利用虚假新闻网站和生成式人工智能影响，即将到来的美国总统大选。微软 8 月 9 日发布报告称，伊朗正加速开展旨在影响美国大选的在线活动，包括开展电子邮件网络钓鱼攻击、创建虚假新闻网站等，试图煽动分裂并影响美国大选。微软 9 月 17 日发布报告称，俄罗斯公关人员已将其影响和虚假宣传策略转向参加美总统大选的民主党候选人，并炮制伪造视频和其他虚假内容，试图抹黑竞选活动。英国战略对话研究所 10 月 24 日发布报告称，俄罗斯国家媒体在社交媒体上散布虚假言论，指责美国政府在飓风海伦和米尔顿过后严重无能，以在美总统大选前影响选民。

美国家情报总监办公室、联邦调查局和网络安全和基础设施安全局 8 月 19 日发布联合声明，指责伊朗正在进行“针对美国公众的影响行动和针对总统竞选的网络行动”。美国国家情报总监办公室 9 月 6 日称，俄罗斯正利用秘密资助的团体和国营媒体对美国选民开展“多管齐下”的虚假宣传活动，试图激化美国内分裂，并增加对特朗普的支持。美国司法部 9 月 27 日公布了一份起诉书，指控 3 名伊朗黑客发起“黑客泄密”活动，旨在影响 2024 年美国总统大选。美国国家情报总监办公室 10 月 22 日表示，俄罗斯等外国对手在美国大选前已经加速影响力行动。美国国家情报总监办公室、联邦调查局和网络安全和基础设施安全局 11 月 1 日发布联合声明称，俄罗斯行为者制作并广泛传播试图影响美选举的虚假视频。

罗马尼亚国家机构解密报告显示，在罗马尼亚总统首轮选举期间，该国的选举基础设施遭到 8.5 万多次的网络攻击，威胁行为者还获得并泄露了与选举有关网站的访问凭证；选举遭受了网络影响力运动，其中 100 多名拥有 800 多万活跃粉丝的 TikTok 罗

马尼亚网红被操纵，传播宣传总统候选人加里 · 乔治斯库的选举内容。罗马尼亚宪法法院 12 月 6 日裁定取消首轮总统选举结果，并决定，举行新选举。此次事件成为首个网络活动导致选举失效的案例，欧盟也决定就俄罗斯网络干扰罗马尼亚选举对 TikTok 展开调查。

除美国和罗马尼亚外，全球还发生了众多针对选举的网络干扰事件。韩国国家情报院 2 月 28 日称，朝鲜间谍机构近期开设了自己直接经营的虚假媒体，针对韩国受众散布虚假信息，并正利用人工智能技术为韩国 4 月大选前传播虚假新闻做准备。俄罗斯中央选举委员会表示，在俄罗斯 3 月 15 日至 17 日举行第八次总统选举期间，该国远程电子投票系统门户遭受了 10 余万次外国网络攻击。非营利组织 AI Forensics 于 4 月 17 日发布报告称，俄虚假信息网络 Doppelganger 正通过 Facebook 虚假账户购买广告传播亲俄言论，开展针对欧盟大选的影响力活动。亲俄黑客组织 HackNeT 于 6 月 6 日攻击了三个荷兰政党网站，并称“荷兰是第一个选举新一届欧洲议会的国家，因此也是第一个遭受 DDoS 攻击的国家”。

二、实施针对战场行动的“网络军事攻击战”，具有“渗打互融，情战给合”的特点

网络空间既是一个作战领域，也是辅助和支持其他领域物理作战的赋能领域。战争冲突正在成为战场网络行动演变的“强大催化剂”，促发各国不断创新和发展网络攻击技战术。“网络军事攻击战”是指针对军事人员、装备和设施的网络攻击行动，旨在实现窃取军事情报、瘫毁军事目标、辅助动能作战等一系战场目标。年内，在俄乌冲突、中东危机中，美俄以伊等国开展了一系列军事网络行动。

乌克兰安全局 1 月表示，乌方拆

除了 2 个遭俄罗斯黑客入侵的在线监控摄像头，上述基辅住宅楼上的摄像头遭俄罗斯入侵和劫持，并被用于监视基辅的防空部队和关键基础设施；自俄乌冲突以来，SBU 已封锁了约 1 万个数字摄像头，因为这些摄像头可能被俄用于对乌进行导弹袭击的准备工作。乌克兰国家网络安全协调中心 1 月警告称，俄罗斯正加大网络间谍活动力度，试图通过窃取军事人员凭据，来侵入乌军事态势感知和指挥控制系统。网络安全公司 Securonix 于 2 月发布报告称，俄罗斯 APT 组织 Shuckworm 已针对乌克兰军方发起了有针对性的攻击活动，试图渗透和危害目标系统。乌克兰国家安全局 4 月表示，有证据表明，俄罗斯军队入侵特定军事人员设备，并曾借此引导对第 128 山地突击旅的导弹袭击，造成至少 19 名乌士兵死亡。乌克兰国家特殊通信和信息保护局 5 月表示，俄罗斯军事黑客增加了对乌克兰军用手机的网络攻击次数，越来越多地利用信使和社交工程策略来传播恶意软件。

曼迪昂特公司 7 月发文称，俄罗斯对乌克兰的网络作战方法发生了显著变化，攻击目标由民用关基设施转向军事目标，寻求最大限度地整合网络作战能力与常规作战能力；越来越多的证据表明，从 2023 年乌大反攻前的几个月开始，多个俄网络单位已将目标从战略性的民用目标转向了士兵的计算机和移动端点，以便在乌前线实现战术性军事目标；俄已重新平衡其总体作战概念，将重点放在那些能够为常规部队提供更直接、更具象的战场优势的目标上；上述变化表明，

俄情报部门已调整思维方式，最大限度地整合网络作战能力与常规作战能力，以更好地支持未来几个月，俄在乌东部发起的新一轮攻势。文章认为，俄罗斯调整后的网络战工作将主要实现以下三个目标：一是渗透乌克兰前线士兵使用的设备；二是渗透乌军用于指挥控制、态势感知和其他操作需求的数字系统；三是定位乌军事装备和阵地。

乌克兰国家特殊通信和信息保护

局 9 月发布《2024 年上半年俄罗斯网络行动》报告称，2024 年以来，俄罗斯黑客的关注点转向与战场直接相关的目标，以及对服务提供商的攻击，不再只是利用所能利用的漏洞，而是瞄准对其军事行动的成功和支持至关重要的领域，旨在保持低调以在与战争和政治相关的系统中保持存在。

作为对伊朗支持的胡塞武装 1 月攻击美军驻约旦后勤基地的报复行动，美国 2 月对伊朗军事间谍船贝赫沙德号开展了网络攻击。美国官员表示，此次行动的目的是遏制贝赫沙德号与胡塞武装分享情报的能力，后者一直在红海攻击货船。伊朗伊斯兰革命卫队（IRGC）10 月表示，10 月 1 日晚对以色列的导弹袭击非常成功，此次行动还包括一次大规模网络攻击，令敌人“措手不及”。

三、实施针对金融体系的“网络资金盗窃战”，具有“隐蔽实施，见缝

插针”的特点

网络金融和加密货币的兴起和蓬勃发展带来了新机遇，同时也面临众多不断变化的网络威胁，针对数字资产存储和交易的网络攻击风险日益加剧。“网络资金盗窃战”是指出于经济动机利用网络安全漏洞、社会工程活动等开展的，针对数字金融资产、平台或其基础系统的网络攻击，旨在通过互联网渠道盗窃资金。2024 年，朝鲜继续利用互联网开展金融盗窃行动，用于补充资金支持自身广泛目标。

联合国朝鲜问题专家小组 3 月 20 日发布年度报告称，朝鲜对加密货币的网络盗窃为其提供约 50% 的外汇收入，并将所获用于支持其核计划；自 2017 年以来，朝鲜网络犯罪分子通过 58 起针对加密货币服务的网络攻击，以及其他非法网络操作，估计已窃取 30 亿美元的虚拟资产。联合国制裁监察员 5 月 10 日提交联合国安理会制裁委员会的文件显示，朝鲜 3 月通过虚拟货币平台 Tornado Cash 洗钱 1.475 亿美元。

加密货币管理平台 CoinStats 于 6 月 23 日发布公告称，该公司遭受了网络攻击，影响了平台上所有托管钱包的 1.3%，即 1590 个加密钱包，大量证据表明，朝鲜黑客组织 Lazarus 黑客发动了此次攻击。微软公司 11 月 22 日发布报告称，与朝鲜有关的威胁

行为者 Sapphire Sleet 在 6 个月内策划的社会工程活动中，窃取了价值超过 1000 万美元的加密货币。去中心化金融平台 Radiant Capital 于 12 月 6 日表示，朝鲜国家附属黑客组织 Citrine Sleet 于 10 月 16 日通过网络攻击侵入其系统，盗窃 5000 万美元加密货币。

信息安全公司 SlowMist 于 4 月表示，朝鲜黑客组织 Lazarus Group 已升级其欺诈活动，正通过利用 LinkedIn 冒充加密货币行业的知名人士来策划网络钓鱼攻击，进而部署旨在窃取关键信息和数字资产的恶意软件。谷歌 6 月 13 日发布报告称，朝鲜黑客 Pukchong 引诱毫无戒心的受害者下载伪装成加密货币价格跟踪器的恶意软件，针对巴西加密货币交易所、金融科技公司和个人发起网络攻击。微软 8 月 30 日发布报告称，隶属于朝鲜侦察总局 121 局的威胁行为者 Citrine Sleet 利用谷歌远程代码执行漏洞攻击了加密货币行业。Jamf 威胁实验室 9 月 16 日发布报告称，朝鲜威胁行为者试图利用 LinkedIn，针对去中心化金融（DeFi）、加密货币和类似业务的员工传播恶意软件 RustDoor。安全研究人员 10 月 13 日称，朝鲜威胁行为者正使用名为 FASTCash 的恶意软件从 ATM 机上进行未经授权的现金提取。网络安全公司卡巴斯基 10 月 23 日发布报告称，朝鲜黑客组织 Lazarus 策划出新的、复杂的社会工程方案，对全球加密货币行业实施网络攻击。网络安全公司 SentinelOne 于 11 月 7 最新研究指出，朝鲜威胁行为者 BlueNoroff 使用带有虚假新闻标题和加密货币相关主题的电子邮件，以及针对 macOS 系统的恶意软件，瞄准加密货币行业。

四、实施针对社会民生的“网络关基毁瘫战”，具有“攻击面广，影响广泛”的特点

关键基础设施关系国家安全、国计民生和公共利益，具有基础性、支撑性、全局性作用，是国家社会经济生活秩序正常运转的重要支撑，也因此成为黑客实施网络攻击的高价值目标。“网络关基毁瘫战”是指针对国家关键基础设施系统开展的网络渗透、劫持、攻击、瘫毁等活动，旨在实现削弱社会基础、影响国家稳定、造成经济损失等广泛目标。年内，针对关键基础设施的网络攻击事件高发频发，针对关键基础设施的网络威胁的复杂性和有效性日益激增。

网络安全公司 KnowBe4 于 8 月

发布报告称，针对电网、通信系统、交通网络、港口和其他基础设施的网络攻击成为“新的地缘政治武器”；针对关键基础设施的网络攻击在全球范围内激增，对国家安全和经济稳定构成重大风险；在全球范围内，自2020年以来，每周针对公用事业的网络攻击平均数量增加了4倍；2023年1月至2024年1月期间，全球关键基础设施遭受了超过4.2亿次网络攻击，即每秒约13次攻击。

网络性能检测公司Netscout发布2024年上半年“DDoS威胁情报报告”称，过去4年中，银行、金融服务、政府和能源供应商等公共事业等关键基础设施部门遭受DDoS攻击增加了55%；随着针对发电厂、供水系统和其他重要系统的攻击不断增加，关键基础设施运营技术已成为安全行业日益紧迫的关注重点。

乌克兰利沃夫市一家市政区域能源公司1月遭受网络攻击，此次攻击使用了新的恶意软件变种“霜冻粘液”，导致600多栋公寓楼的供暖中断两天。乌克兰最大国有石油天然气公司Naftogaz、乌克兰国家邮政服务提供商Ukrposhta，乌克兰国家运输安全局（DSBT）和乌克兰铁路运输公司Ukrzaliznytsia于1月遭受网络攻击，导致重要服务中断。乌克兰国防部情报总局年内持续对俄罗斯众多关键部门实施攻击，重要情况包括：窃取了500多个俄罗斯军事基地的建设计划；破坏俄罗斯国防部关键通信服务器；扰乱俄罗斯城市地铁票价支付系统；摧毁了俄罗斯军工企业等使用的数据中心；攻击了莫斯科污水网络通信系统运营公司Moskollector；导致克里米亚等地至少25万人断网；导致俄罗斯城市停车支付系统瘫痪；致瘫4家俄罗斯银行在线服务等。

以色列最大的移动电话提供商Pelephone于1月23日因遭黑客组织“匿名苏丹”攻击而陷入中断服务。以色列黑客组织“我们红色邪恶”针对伊朗通信系统开展网络攻击，导致伊朗部分地区8月1日晚间互联网接入中断。伊朗中央银行和其他几家银行8月14日遭受了一次重大网络攻击，导致该国银行系统大范围中断，评估表明，这是有史以来针对伊朗国家基础设施的最大网络攻击之一。伊朗第一副总统穆罕默德·礼萨·阿里夫9月透露，该国燃料分配系统一年内遭受两次相同的网络攻击。以色列黑客组织“红色邪恶”和“我们红色邪恶”9月声称，入侵了黎巴嫩政党和准军事组织真主党使用的供水系统，并设法改变了氯含量。伊朗10月12日遭受大规模网络攻击，导致伊朗政府服务中断、重要信息被窃取，尤其是核设施也受到影响。

五、实施针对民心士气的“网络舆论心理战”，具有“因情制宜，润物无声”的特点

随着信息网络技术的迅猛发展，世界主要国家均将网络心战纳入新型作战样式。“网络舆论心理战”是指利用网站、社交媒体、电子邮件等互联网传播媒介，向特定受众传播具有明确目标的倾向性、误导性、蛊惑性

舆论宣传活动，旨在达到打击民心士气、扭曲事实观点、制造分裂对抗、造成局势混乱等目的。当前，网络舆论心理战已经成为大国战略博弈、地缘政治斗争、武装战争冲突的新形态和新战法，人工智能技术的发展和运用正将网络心理战的技术能力和效能提升到新层次。

俄罗斯黑客 2 月攻击了《乌克兰真理报》、Liga.net、Apostrope 和 Telegraf 等多家媒体，并传播了同一条假消息，即“俄摧毁了乌东城市阿夫季夫卡的一支乌克兰特种部队”。网络安全公司 ESET 于 2 月发布报告称，与俄有关的黑客分针对乌不同群体，如普通民众、地方政府和能源公司、旅外乌克兰人和异见人士等，多次开展所谓“特克森托行动”，主要目标是“散布怀疑”。乌克兰安全局 4 月表示，俄罗斯情报部门针对乌克兰高级政府和军事官员发起大量虚假信息和心理行动。5 月 9 日，亲俄罗斯黑客劫持了乌克兰电视频道和拉脱维亚电视网络，转播莫斯科胜利日阅兵；俄罗斯克里米亚地区、巴什基里亚地区以及奥伦堡、鄂木斯克和伊尔库茨克等城市的多家广播服务网络也遭到黑客攻击，播放与乌克兰有关的，视频以及反对派媒体的头条新闻。乌克兰国家特殊通信和信息保护局 7 月称，Telegram 上的几个热门乌克兰新闻频道遭到黑客攻击，并传播与乌克兰总统泽连斯基有关的虚假消息。10 月 7 日，俄国家电视广播公司遭受大规模网络攻击，乌克兰政府称“乌克兰黑客通过对全俄国家电视广播公司进行大规模攻击来‘祝贺’普京的生日”。乌克兰计算机应急响应小组 10 月警告称，与俄罗斯相关的黑客组织 UAC-0050 近期针对乌克兰机构发起了大规模信息宣传活动，通过虚假威胁称已在乌机构内安置炸弹来制造恐慌。

网络安全公司 SentinelLabs 和 ClearSky Cyber Security 于 2 月发布报告称，俄罗斯 Doppelgänger 影响力行动网络精心策划针对美西方

的影响力行动，传播旨在影响公众舆论的宣传和虚假信息内容，特别是针对当前与民众相关的地缘政治和社会经济话题。网络安全公司 Recorded Future 于 5 月 9 日发布报告称，与俄罗斯有关联的CopyCop影响力网络，能够利用人工智能抓取来自主流媒体的合法内容，将其转化为带有政治偏见的宣传，并自动利用虚假媒体进行传播；CopyCop 已证明人工智能大规模生成虚假信息的可行性，使得合法媒体机构面临着其材料被窃取、剽窃和武器化，以支持敌对国家叙事的风险。

Recorded Future 公司 10 月发布报告称，俄罗斯信息战理论将网络空间视为战场和战略优势领域，已经将战略性信息攻击（SIA）纳入俄罗斯武器库；SIA 是一种融合心理和技术战术的概念，旨在破坏和破坏对手的国家网络信息稳定；SIA 将俄通过非动能手段对敌方国家关键基础设施造成战略破坏的能力进行概念化，通过“心理攻击”（影响行动）和“技术攻击”（网络攻击）来瞄准对手，以造成精确的战略损害；SIA 的目标是利用战略性非动能能力使冲突升级，并通过造成重大基础设施破坏，迫使对手屈服；SIA 的心理攻击重在塑造对手的看法，并削弱对其领导层和机构的信任，通过传播真假信息或利用现有的社会紧张局势，试图制造广泛的混乱和动乱；SIA 技术攻击包含旨在破坏或摧毁国家关键基础设施的复杂网络攻击，旨在造成长期广泛而非短期有限的影响。

微软威胁分析中心 2 月发布题为《伊朗大力开展网络影响力行动以支持哈马斯》的报告，称伊朗针对以巴冲突开展的网络影响力行动旨在实现四项目标，包括：一是通过分化来破坏以色列国内稳定；二是对以色列实施报复；三是恐吓以色列公民及其支持者；四是破坏国际社会对以色列的支持。具体策略包括：一是冒充以色列活动团体和伊朗合作伙伴；二是动员以色列人开展实地行动；三是通过文本和电子邮件以更高的频率和复杂性来放大影响；四是利用官方媒体来放大网络行动。网络安全公司 Recorded Future 于 5 月 8 日

发布报告称，与伊朗结盟的行为者 Storm-1364 发起被称为 Emerald Divide 的复杂影响力活动，旨在通过扩大意识形态分歧和削弱对以色列政府的信任来操纵以色列社会，特别是利用对以巴冲突和其他社会和政治问题的反应。

法国国防和国家安全总秘书处下属的、负责打击外国数字信息干扰的机构 VIGINUM 于 2 月宣布，一个涉及 193 个网站的旨在向西方传播亲俄内容的网络“Portal Kombat”发表了超过 15 万篇文章和帖子，其中大部分转发自俄罗斯和亲俄罗斯媒体，主要目的是为俄在乌军事行动辩护，内容带有“强烈的意识形态偏见”和“明显的虚假和误导性故事”。德国外交部文化与传播部 3 月表示，俄罗斯旨在破坏欧洲对乌克兰支持的虚假信息活动规模、技巧和隐蔽性都显著增强；该部发现在社交媒体平台 X 上发现了由超过 5 万虚假账户组成并每天发布 20 万个帖子的网络，这是迄今为止最大的操纵德公众舆论的企图之一；当前的虚假信息旨在歪曲观点、扭转争论的天平，这种技术更像是行为科学中的“轻推”，即利用小的社会和信息线索来巧妙地改变观点或行动。

人工智能公司 OpenAI 于 5 月 30 日发布的第一份有关其模型滥用报告称，俄罗斯、伊朗和以色列的恶意行为者一直在利用 OpenAI 的工具在社交媒体平台上创建和发布有关各种地缘政治和社会经济问题的宣传内容，试图通过制作虚假的社交媒体评论、文章和多种语言的翻译文本来影响政治结果和公众言论，该公司在过去 3 个月内已成功揭露并封杀了 5 起此类行动。OpenAI 于 10 月再次发布报告称，该公司自 2024 年年初以来已经破坏了 20 多次网络和秘密影响行动。

赵慧杰：虎符智库专家、网络空间安全军民融合创新中心高级研究员、奇安网情局主编。

2024 网络攻击新途径与新方法（上）

网络攻防，既是攻防技术的对抗，也是脑洞的较量。本期梳理总结 2024 年出现的一些比较有趣、甚至有点奇葩的网络攻击新途径与新方法。

一、网络物理攻击的新天地

网络物理攻击，是指通过网络攻击的形式，造成实质性的物理伤害。2024 年，越来越多的网络物理攻击方法浮出水面，并以以色列对黎巴嫩真主党的传呼机炸弹事件为标志，达到了高潮。

1、生成式 AI 将推动网络物理攻击时代来临

越来越多的专家开始担心：随着黑客们广泛使用人工智能（AI）工具，我们可能正在进入“网络物理攻击”时代。这些黑客可能是独狼，也可能得到国家的支持。

麻省理工学院工程系统教授、斯隆管理学院网络安全系联合创始人 Stuart Madnick 认为，随着生成式 AI 的广泛普及，网络犯罪者在下一阶段发动物理攻击的概率正在增长。

Madnick 带领研究团队在实验室里模拟了网络攻击，结果引发了物理爆炸。他们成功入侵计算机控制的带泵电动机，并使其燃烧。Madnick 指出，如果攻击可以导致温度计故障、压力值爆表、电路被绕过，也会在实验室环境中引发爆炸。这样的结果表明，传统网络攻击只是让系统暂时离线，而网络物理攻击带来的后果远甚于此。

Madnick 说：“如果通过传统网络攻击让发电厂停止运行，它很快就会恢复并重新上线。但是，如果黑客让发电厂爆炸或烧毁，就无法在一两天后恢复在线状态，因为这些专用系统中许多零件是定制的。人们还未意识到，停机时间可能会很长。”“借助 AI 技术，网络攻击技术已经能对物理系统造成严重破坏。”

安全厂商 Lacework 的首席信息安全官 Tim Chase 也指出，存在大量使用可编程逻辑控制器（PLC）的系

越来越多的专家开始担心：
随着黑客们广泛使用人工智能（AI）工具，
我们可能正在进入“网络物理攻击”时代。

统是美国基础设施的薄弱环节。黑客可能利用生成式 AI 辅助为 PLC 创建代码。一旦恶意行为者控制了 PLC，他们就可以对工业系统造成严重破坏，导致实际的物理问题。虽然工业控制系统很难被黑客攻击，但 Chase 担心 AI 为“中等水平的黑客”提供了提高攻击技能的工具。

Chase 认为：“AI 可以使那些缺乏技能和耐心的人更容易攻击工业控制系统。”

在美国，很多工业和医疗系统仍然严重依赖几十年前的遗留系统，这些系统的保护措施非常薄弱。AI 的到来将使这些漏洞更为容易利用。Chase 说：“每当攻击变得更容易，攻击的发生频率就会增加。”

美国叶史瓦大学卡茨科学与健康学院项目主任兼教授、网络安全管理平台 Onyxia 首席执行官 Sivan Tehila 也担心网络物理攻击的潜在上升。

Tehila 说：“AI 支持的网络攻击可能很快就会发生，它们极为复杂、难以检测和缓解。”但是，她认为 AI 也在帮助防守方。Tehila 表示：“AI 可以分析大量数据并实时识别恶意活动，在增强网络防御方面发挥关键作用。”Tehila 曾在以色列国防军服役，从事网络安全工作。

Michael Kenney 是匹兹堡大学教授兼该校马修 · 邦克 · 李奇微国际安全研究中心主任。他认为，网络犯罪分子如果尝试摧毁物理基础设施，也会面临风险。他们不想大面积摧毁互联网，毕竟互联网是他们的立足之本。他说，一般来说，恐怖分子更有可能使用过去奏效的现有工具，如武器和军事装备。

> 很多工业和医疗系统仍然严重依赖几十年前的遗留系统，这些系统的保护措施非常薄弱。AI 的到来将使这些漏洞更为容易利用。

但是，Madnick 仍然忧心忡忡地表示：“一个物体爆炸时，不仅会摧毁其本身，还会摧毁附近的其他物体。这会带来更大的问题，还会造成人身伤害。”

2、利用无线充电器注入语音指令损坏智能手机

佛罗里达大学和 CertiK 的学术研究人员的研究成果显示，一种名为“Volschemer”（伏特图式）的新攻击可以通过现成的无线充电器发出的磁场注入语音命令，来操纵智能手机的语音助手。Volschemer 还可用于对移动设备造成物理损坏，并将靠近充电器的物品加热到280摄氏度以上。相关技术论文将 Volschemer 描述为一种利用电磁干扰来操纵充电器行为的攻击。

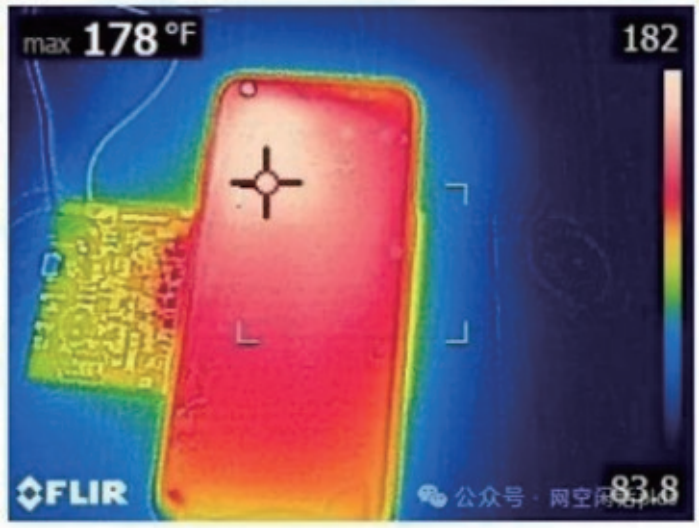
无线充电系统通常依靠电磁感应原理，利用电磁场在两个物体之间传递能量。充电器包含一个发送线圈，交流电在其中流过，产生振荡磁场，智能手机包含一个接收线圈，从磁场中捕获能量，并将其转换为电能，为电池充电。

攻击者可以操纵充电器输入的电压，并微调电压波动（噪声），以产生干扰信号，从而改变产生的磁场的特性。电压操纵可以通过插入设备引入，不需要对充电站进行物理修改，也不需要对智能手机设备进行软件感染。

研究人员表示，这种噪音信号会干扰充电器和智能手机之间的常规数据交换，从而扭曲电源信号，破坏高精度传输的数据。充电站和智能手机都使用微控制器来管理充电过程。

从本质上讲，Volschemer 利用了无线充电系统硬件设计中的安全漏洞和控制其通信的协议。这为 Volschemer 攻击开辟了至少三种潜在的攻击途径，包括过热 / 过度充电、绕过 Qi 安全标准，以及在充电的智能手机上注入语音命令。

研究人员用三星 Galaxy S8 设备



描述了他们的实验：

注入 CE 包增加功率后，温度迅速上升。不久之后，由于手机过热，手机试图通过传输 EPT 包来停止电力传输，但研究人员的电压操纵器引入的电压干扰破坏了这些，使充电器无响应。

充电器受到虚假 CE 和 RP 包的误导，不断提升传输功率，进一步升高温度。手机进一步激活了更多的保护措施：关闭应用程序，并在 52.2 摄氏度时，限制用户交互，在 76.7 摄氏度时启动紧急关机。尽管如此，电力传输仍在继续，保持着危险的高温，稳定在 81.1 摄氏度。

3、通过耗尽系统阻尼能力来破坏海上风电场

来自康科迪亚大学和魁北克水电公司的研究人员发布的一项新研究成果显示，研究者根据 VSC-HVDC 系统和孤岛式海上交流电网的特点，识别出 VSC-HVDC 系统引入的新的网络物理漏洞。然后设计了两个针对海上 VSC 电压幅度和频率控制的攻击向量，利用 VSC-HVDC 的快速响应，通过耗尽系统阻尼能力来破坏 OWF 的稳定性。实验表明，精心调整的攻击向量可以有效地破坏 OWF 的稳定性，尽管普遍假设 VSC-HVDC 连接的 OWF 与主交流电网脱钩，但造成的振荡可能会传播到主电网。

当所有海上风电场都产生最大输出时，这些扰动可能会引发海上风电场阻尼不良的功率振荡。如果这些网络引起的电气干扰是重复的，并且与阻尼不良的功率振荡的频率相匹配，则振荡可能会被放大。然后，这些放大的振荡可能会通过高压直流系统传输，可能会影响主电网的稳定性。虽然现有系统通常内置冗余，以保护其免受物理意外事件的影响，但这种针对网络安全漏洞的保护很少见。

4、利用恶意改装通信设备制造爆炸事件

2024 年 9 月 17 日、18 日，黎巴嫩连续发生传呼机和对讲机爆炸事件，主要针对黎巴嫩真主党成员，造成至少 39 人死亡，数千人受伤。黎巴嫩真主党指责对手以色列发动了这些攻击，称其已越过“所有红线”，并誓言将实施“正义的惩罚”。

黎巴嫩真主党为规避以色列的追踪和监听，自 2024 年 2 月以来，放弃使用智能手机等设备，转而使用技术含量较低的对讲机和传呼机进行内部通信。

初期报道认为，设备被远程控制

导致电池升温发生爆炸，但后续分析显示爆炸并非电池本身升温所能造成。有报道称，传呼机在供应商交付给真主党前被以色列方面预先安装了爆炸物，并通过远程引爆开关控制爆炸。

另一种说法是，以色列可能破解了真主党的传呼机，将爆炸装置植入电池里，或者利用高能材料提升爆炸威力。

此次事件引发了关于网络安全和恐怖组织通信方式的深刻反思，是一起利用网络攻击技手段实施的恐怖主义活动。

二、智能手机上的新陷阱

1、可静默采集手机指纹的彩信

2024 年 2 月，瑞典网络安全公司 Enea 的研究人员发现，以色列 NSO 集团提供了一种前所未知的技术，可以将其臭名昭著的“飞马”手机间谍软件工具，部署到全球范围内任意特定个人的移动设备上。

有趣的是，这名研究员是在调查一份 NSO 集团转销商与加纳电信监管机构的合同条款时，发现了这一技术。这份合同属于 2019 年 WhatsApp 与 NSO 集团诉讼的法庭公开文件的一部分，前者指控 NSO 集团利用 WhatsApp 漏洞，在全球范围内将“飞马”部署到记者、人权活动家、律师等人的设备上。

根据合同描述的“MMS 指纹”，NSO 客户只需发送一条多媒体短信（国内一般叫彩信，简称 MMS）消息，即可获取目标的黑莓、安卓或 iOS 设备及其操作系统版本的详细信息。合同指出：“不需要用户交互、参与或打开消息，就能获取设备指纹。”

分析与测试显示，NSO 集团合同中提到的技术可能与彩信流程本身，而非任何特定操作系统的漏洞有关。简单说，在彩信流程中，接收方的设备在得知有彩信需要接收时，会首先上报本机的指纹信息（如机型、操作系统、SIM 卡信息等），之后服务商系统才会根据手机指纹特征，发送适配手机的彩信信息。而 NSO 集团的技术很可能就是利用了彩信收发的这一流程，截获了手机的指纹信息。

如使用这些信息，NSO 集团的行动者可以利用移动操作系统中的特定漏洞，或者为目标设备定制“飞马”和其他恶意负载。

NSO 是一家知名的以色列网络军火商。2016 年震惊世界的“iOS 三叉戟漏洞”事件，也是该公司所谓。当时，该公司以 100 万美元 / 年的服务费，向阿联酋政府出售一款网络武器，用以追踪反政府人士。目标人在收到钓鱼短信，只要点开短信中的链接，苹果手机就会立即被完全控制。该网络武器利用了 iOS 系统和苹果浏览器的总共 3 个 0day 漏洞发动攻击，因此得名“三叉戟漏洞”。该事件因某位目标人“高度警惕”，将钓鱼短信发给安全公司审查后才得以曝光。

2、可监控全球的定位系统漏洞

2024 年 5 月，美国马里兰大学的安全研究人员发表论文披露苹果设备的 Wi-Fi 定位系统（WPS）存在安全设计缺陷，可用于大规模监控全球用户（不使用苹果设备的人也会被监控），从而导致全球性隐私危机。

苹果和谷歌等科技巨头推出的基于 Wi-Fi 的定位系统 (WPS)，允许移动设备通过查询服务器上的 Wi-Fi 接入点信息来获取自身位置。简单来说，使用过 GPS 定位的移动设备，会定期

> 苹果和谷歌等科技巨头推出的
> 基于 Wi-Fi 的定位系统 (WPS)，
> 能够监控全球范围内的设备，
> 并可以详尽地跟踪设备进入和离开目标地理区域。

一觉醒来，
你的移动设备上的数据可能已经被全部远程擦除了。
这样离奇的事情在英国就发生了。

向 WPS 上报所观察到的 Wi-Fi 接入点的 MAC 地址（即 BSSID）及其对应的 GPS 坐标。WPS 服务器会存储这些上报的 BSSID 位置信息。

总之，WPS 为客户端设备提供了一种比全球定位系统（GPS）更节能的定位方式。在题为《通过 Wi-Fi 定位系统监视大众》的论文中，美国马里兰大学博士生 ErikRye 和副教授 DaveLevin 介绍了一种全新的苹果 WPS 查询方法，可被滥用于大规模监视，甚至不使用苹果手机（以及 Mac 电脑和 iPad 等苹果设备）的人也可被监控。

这种全新的 WPS 查询方法能够监控全球范围内的设备，并可以详尽地跟踪设备进入和离开目标地理区域。研究者对苹果 WPS 提供的数据进行了系统的实证评估，发现这些数据涵盖了数亿台设备，并且允许我们监控 Wi-Fi接入点和其他设备的移动情况。而苹果的 WPS 最为危险。

研究者还在俄乌战场和以色列哈马斯加沙冲突地带实际验证了该漏洞的有效性和危险性。研究者首先利用苹果的 WPS 分析了进出乌克兰和俄罗斯的设备移动情况，从而获得了有关正在进行的战争的一些见解。研究者发现疑似军用人员将个人设备带入战区，暴露了预部署地点和军事阵地。研究结果还显示了一些离开乌克兰并前往世界各地的人员信息，这验证了有关乌克兰难民重新安置地点的公开报道。

以色列 – 哈马斯加沙战争：研究者使用苹果的 WPS 追踪加沙地带居民的离境和迁徙情况，以及整个加沙地带设备的消失情况。该案例研究表明，研究者可以利用苹果的 WPS 数据跟踪大规模停电和设备丢失事件。更糟糕的是，被追踪设备的用户从未选择加入苹果的 WPS，在研究者进行这项研究时也没有退出机制。仅仅处于苹果设备的 Wi-Fi 范围内，就可能导致设备的位置和移动信息被广泛公开。事实上，研究者在苹果的 WPS 中识别了来自 1 万多家不同厂商的设备。

3、入侵服务商远程擦除设备数据

一觉醒来，你的移动设备上的数据可能已经被全部远程擦除了。这样离奇的事情在英国就发生了。

2024 年 8 月，总部位于英国的移动设备管理（MDM）公司 Mobile Guardian 遭到网络攻击，导致上万台客户设备被远程抹除。8 月 4 日，该公司对外检测到平台遭到未授权访问，为控制事态并防止进一步的破坏，服务器被紧急关闭。

此次攻击的动机尚不明确。黑客未经授权访问注册在 Mobile Guardian

平台上的大量 iOS 和 Chrome OS 设备，将这些设备从 MDM 平台中注销并远程抹除了设备中的数据。

虽然事件目前仍在调查中，但 Mobile Guardian 在声明中表示，目前没有证据表明攻击者获取了用户数据。

此次事件影响到了北美、欧洲和新加坡的大量客户。目前被擦除数据的设备具体数量尚未明确，虽然 Mobile Guardian 表示仅占总数的“较小百分比”，但根据部分受影响用户的反馈，被擦除的设备规模可能将数以万计。

受影响客户之一新加坡教育部表示，26 所学校的 1.3 万名学生的设备（包括 iPad 和 Chromebook）均被攻击者远程抹除，在新加坡造成了重大混乱，学生无法访问储存在 iPad 和 Chromebook 上的应用程序和信息。新加坡教育部表示，此次事件后将从所有 iPad 和 Chromebook 设备上移除 Mobile Guardian 应用程序。

三、合法软件的新利用

1、利用远控软件发起的攻击

2024 年 7 月，威胁情报公司微步披露了一批利用具备“远控”功能的合法软件进行的攻击事件，其中既包括真实的黑产攻击事件，也包括各类攻防演练活动相关的攻击事件。以下是文章中介绍的一个攻防演习事件。

在某次攻防演练期间，某云官方被演习红队攻击，导致某软件云端官方升级文件被投毒，升级包中包含阿里云助手软件（远控程序）。然后，攻击队以安全厂商的名义传播该软件存在漏洞诱导客户进行升级，升级该软件的客户会从云端下载升级文件，其中就包括攻击者嵌入的阿里云助手软件（远控程序）。

微步对类似事件中使用的攻击手法进行了总结。大致过程如下。

首先，攻击者伪装成试用客户向远控软件供应商进行申请试用，如果供应商缺乏审核或者审核不严，就会导致攻击者获取到远控程序的安装包。

攻击者在获取到合法远控后，一般会直接修改受控端安装程序名，伪装成各种钓鱼文件名称，诱导受害者点击。这些受控端程序不需要受害者进行确认就可以做到无感安装。

有时，攻击者也会对受控端安装文件进行打包，并在打包程序的安装脚本中加入一些恶意功能，比如，搜索杀毒软件程序并诱导用户关闭，打开诱饵文档迷惑受害者等。

合法远控存在不同类型，对于提供 C/S 架构安装包的远控供应商，攻击者会在申请到使用资格后，在攻击者服务器上部署远控程序控制端，然后生成受控端安装包，分发给受害者进行控制，受害者主机上受控端程序链接的也是攻击者服务器地址。

对于提供 SaaS 化部署的远控程序，攻击者会申请使用的是一个 SaaS 化的管理平台账号，通过登录管理平台来进行操作受控端，攻击者在管理平台上获取到受控端的安装包或者下载链接，分发给受害者进行安装，然后攻击者就可以在管理平台上对受控端进行控制，受害者主机上受控端程序链接的是 SaaS 化平台的地址。

2、利用安全软件发起的攻击

2024 年 9 月，安全公司 Malwarebytes 披露了一起新的勒索软件攻击案例：勒索软件 RansomHub 能够利用卡巴斯基的 TDSSKiller 工具，关闭目标系统上的 EDR（终端检测和响应）并能够在目标系统上部署其他恶意工具，用于窃取登录凭据。

据了解，TDSSKiller 是 Kaspersky 开发的一款免费工具，用于扫描系统中的 rootkit 和 bootkit 这两类非常难以监测的恶意软件。由于 TDSSKiller 可以与内核级服务交互、关闭或删除服务，因此可以查杀很多顽固木马。由于 TDSSKiller 是由卡巴斯基签名的合法工具，因此不会被安全解决方案标记为恶意软件。

而在安全公司 Malwarebytes 观察到的攻击案例中，RansomHub 的攻击过程主要有以下几个步骤。

Step1：通过网络侦察，枚举管理员组使用命令，如“net1 group ‘Enterprise Admins’ /do”。

Step 2：使用 TDSKiller 工具特定命令关闭 EDR 系统。

Step 3：部署 LaZagne 工具，LaZagne 工具从系统中提取密码，如浏览器、电子邮件客户端和数据库。

为了防御这种类型的攻击，一般需要激活 EDR 解决方案的防篡改保护功能，以确保攻击者无法使用一些工具，如 TDSSKiller 关闭 EDR 服务。另外，监控 TDSSKiller 的执行和“-dcsvc”标志（用于关闭或删除服务的参数）也可以帮助检测和阻止恶意活动。

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