内部资料 免费交流

出版物准印证号：内资准印证 京内资准字 2124-L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

网络安全的年度记忆

——2024 年值得关注的网络安全现象

第48期

2024 年 12 月

奇安信
新一代网络安全领军者

API安全卫士

曾获首届数据安全大赛金奖（产品能力评比）

检测、分析、防护闭环解决方案

守护API安全 数据安全

扫一扫 了解更多

我们怎么告别 2024？

在 1948 年的一次演讲中，前英国首相丘吉尔曾引用过哲学家乔治 · 桑塔亚那的名言：“不从历史中汲取教训的人，注定要重蹈覆辙。”汲取教训、避免重蹈覆辙同样应用于网络安全防护。

尽管我们在不断重复同样的错误，让攻击者得以侵入其系统。但为了确保 2025 年尽可能少地重复今年的错误，我们在年底最后一期总结了 2024 年的现象级事件，也就是本期专题“网络安全的年度记忆”，这些 2024 年影响广泛的现象，也必将在未来持续带来深远的影响。

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，提升网络对抗的硬实力，成为网络防护者迫在眉睫的任务。

2024 年，勒索软件攻击仍然是最常见的网络攻击形式。攻击不仅直接影响机构的正常运营，还由于普遍采取“双重勒索”手段，导致大量的机密数据泄露，对各个行业造成巨大的财务、运营和声誉损失。我国上市公司、金融机构也成为受害者。

对网络安全行业来说，从一系列因简单错误而引发的攻击就可以看出，新的一年显然有很大的提升空间。

在 2024 年，2007 年最常见的编码错误类别仍然位居榜首。尽管软件开发商已经降低了最常见的编码错误的发生率，但从整体上看，软件行业并没有有效消除常见的编码错误。

2024 年，陈旧系统成为攻击者的重要目标。随着各行业提高新技术的安全性，攻击者现在更多地关注那些通常不经常升级或修复的老旧基础设施。

2024 年的网络安全事件还显示，即使是市场上最好的工具，也容易受到攻击组织的攻击。联合健康集团 (UnitedHealth Group) 旗下数据处理公司 Change 攻击者利用泄露的凭证入侵了 Citrix 远程访问桌面的应用，因为缺乏多因素身份验证，攻击者得以在系统内横向移动并窃取数据。

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。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”。

当然，2024 年的网络安全也并非缺乏亮点。“网络安全人工智能”可能是今年最大的亮点，安全专家认为，可以通过使用人工智能技术增强网络防御能力，来消除网络攻击的影响。因此全球的网络安全公司都在产品中嵌入生成人工智能功能来提高运营自动化和效率。

2025 年再见！

总编辑

李建平

2024 年 12 月 1 日

CONTENTS 目录

安全态势

网络安全的年度记忆

——2024 年值得关注的网络安全现象

P17

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。

《网安 26 号院》编辑部
主办　奇安信集团

总　　编　　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
安全之道主编：张少波
奇安资讯主编：陈　冲
报告速递主编：刘川琦
专　　栏主编：任润波

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：内资准印证 京内资准 2124-L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 12 月 26 日

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。

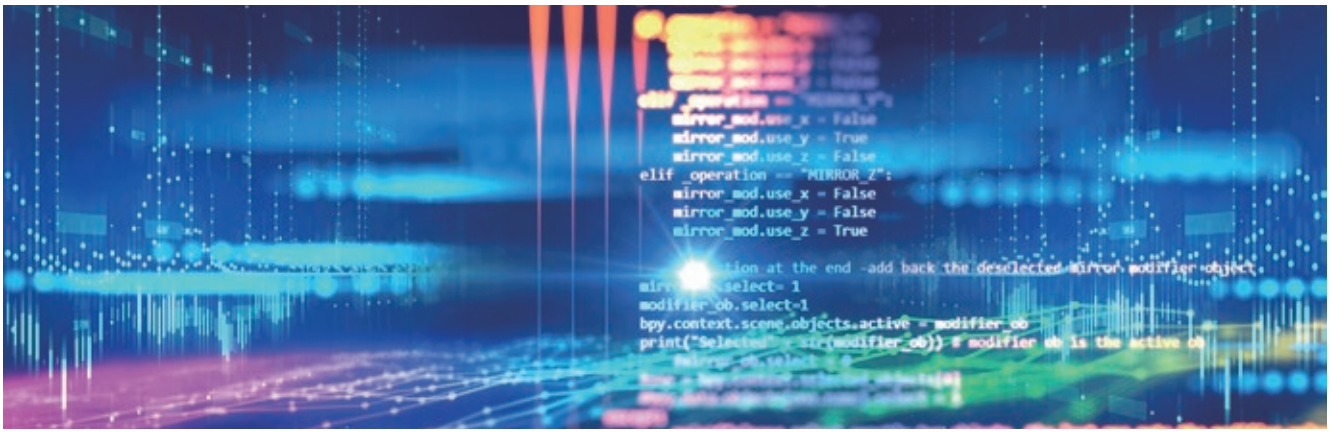
Palo Alto Networks PAN-OS 身份认证绕过漏洞安全风险通告

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。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。



对抗篇

国内攻防演习 11 月态势：哪些薄弱点最易被利用？

作者 | 奇安信安服团队

一、本月演习整体情况

2024 年 11 月，奇安信 Z-TEAM 团队共承接攻防演习服务 29 场，行业级攻防演习 1 场，省级攻防演习 1 场，省级行业攻防演习 2 场，客户自主攻防演习 25 场。

本月承接攻防演习数量较上月的月均场次呈明显上升趋势（见图 1）。

本月承接的攻防演习涉及政府部委、企业、金融行业较多，此情况较上月承接攻防演习涉及行业范围类似，但政府部委、运营商行业攻防演习数量明显增多，金融行业攻防演习数量略有减少（见图 2）。

11 月攻防演习成果如表 1 所示：

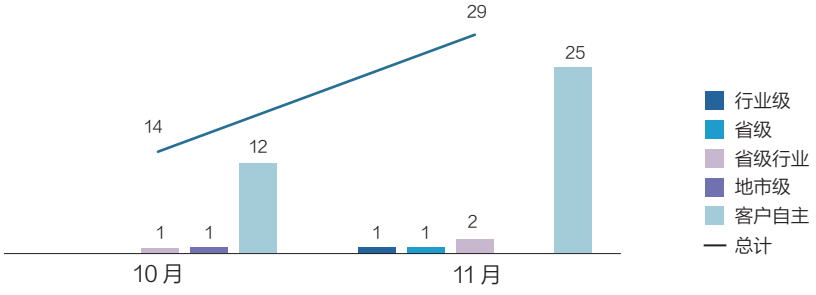


图 1 10-11 月 Z-TEAM 承接攻防演习数量统计图

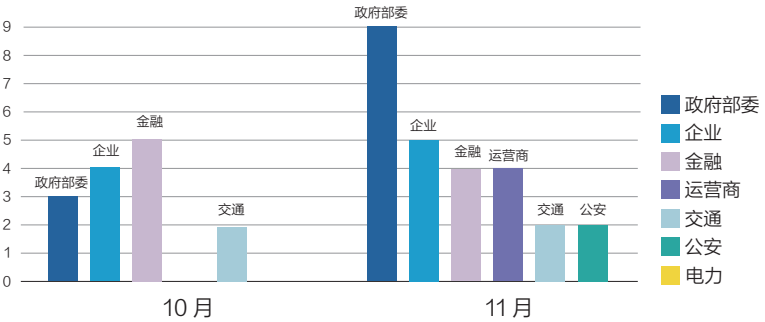


图 2 10-11 月攻防演习涉及行业统计图

二、任务目标特点

本月攻防演习和评估任务行业比较分散，演习目标覆盖面较广，涵盖了政府部委、企业、金融、运营商、交通、公安等行业。随着计

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	48	63	103	71	203	412	702	3763

表 1

算机和网络技术的迅猛发展，政府部委业务系统对互联网和内部网络的依赖程度逐渐加深。然而，随着科技的发展，安全问题亦日益凸显。例如，黑客和病毒等攻击手段日趋复杂，数据泄露、篡改或滥用等风险亦不断增加。这些威胁使得政府部委网络信息系统的安全面临越来越大的挑战。因此，为有效应对这些安全威胁，必须采取一系列切实有效的措施来确保网络信息系统的安全稳定运行。在本月攻防演习中，政府部委行业占比最高，为 31%（见图 3）。

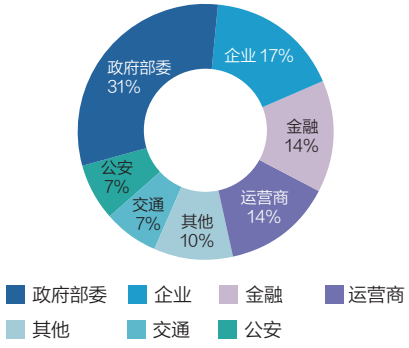


图 3 11 月攻防演习分布

三、主要攻击手段分析

基于奇安信 Z-TEAM 团队实战成果，本月任务中主要针对多行业不同目标网络，使用攻击手段也有所不同，如政府部委、交通等行业外网突破的主要手段包括漏洞扫描利用和口令爆破等；金融、企业行业主要是钓鱼攻击和隐秘隧道外联等；公安、运营商行业外网突破的主要手段包括漏洞利用和 VPN 仿冒接入等。各个行业使用的主要技术手段分布如下（见图 4）。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、钓鱼攻击、口令爆破、VPN 仿冒接入、隐秘隧道外联技术等。

整体攻击手段与上月对比，漏洞扫描利用手段有明显上升趋势，口令爆破和 VPN 仿冒接入利用率基本趋同，钓鱼攻击和隐秘隧道外联手段有明显下降趋势（见图 5）。

四、典型攻击手段实现案例

伴随着信息通信业的迅猛发展，计算机病毒、系统安全漏洞和网络违法犯罪等网络与信息安全问题日渐突出，网络安全对政府部委来说，是一个重要且不可忽视的方面。政府部委的网络安全事关国家安全、社会稳定、公共利益，是维护国家主权、安全、发展利益的重要基础。因此，提高政府部委网络安全的防护水平，构筑坚不可摧的网络安全防线，是目前的当务之急。

案例：0day+nday 组合利用，突破多道防线

孙子兵法有云：知己知彼，百战不殆。奇安信攻击队在对某政府部委的攻防演练中，攻击队员们各司其职，充分发挥个人所长，将“知己”原则运用至极致。同时，他们采取多种手段，尽可能广泛地搜集目标单位的资产信息和敏感信息，以实现“知彼”目标。这些信息为制定更为全面和有效的攻击策略提供了坚实的信息基础，从而在对抗中占据先机。

在对收集到的信息进行筛选时，攻击队迅速地识别出一系列可攻击的目标，包括 IP 地址、网站、系统和应用程序等。他们特别发现，该单位的一个业务板块中，泛微 OA 系统存在一个未公开的 0day（零日）漏洞，并且该系统正暴露于互联网之上。利用泛微 OA 系统的 0day 漏洞利用程序，攻击团队迅速获得了该 OA 系统服务器的控制权。经过多次的探索和尝试，他们最终利用该 0day 漏洞成功获取了门户网站的应用程序和操作系统的管理员权限，从而成功地进入了该单位的办公内网。

在进入该单位办公内网后，攻击队决定利用某防火墙 0day 突破逻辑隔离措施，利用这一时机进行内网的横向拓展。他们巧妙地结合一个 Confluence nday（已公开多日的）漏洞来控制该单位 Zabbix 集权系统，从而获取了该

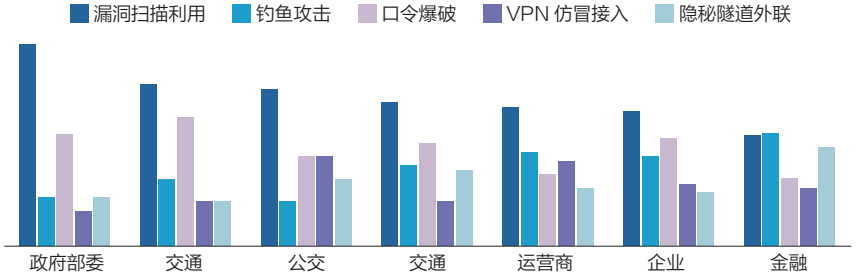


图 4 11 月行业攻击手段分布图

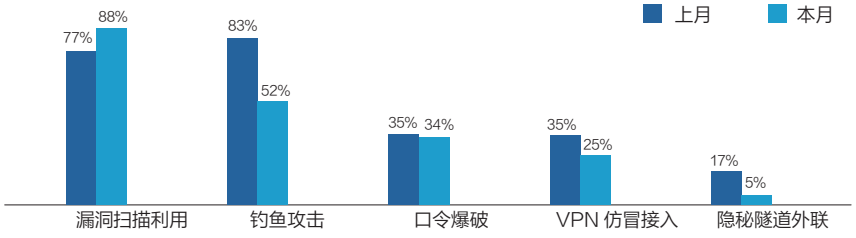


图 5 攻击手段对比图

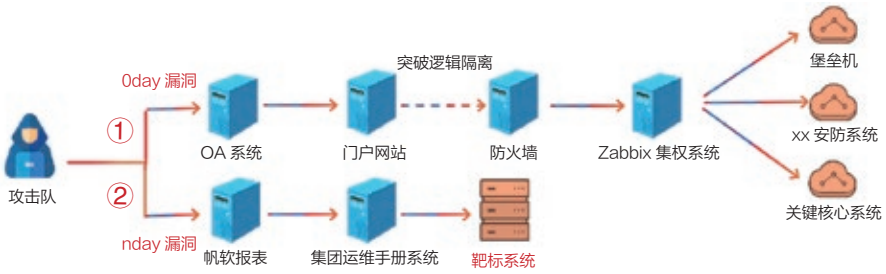


图 6 案例攻击路线图

单位生产环境Zabbix平台的控制权限，通过该平台攻击队可间接管控其他 237 台服务器。此外，他们还通过绕过堡垒机的权限限制，成功获取了堡垒机的后台管理权限，进而能够控制生产线的运维系统及 XX 安防系统等关键核心系统。

同时，攻击队的另一支小组成员通过帆软报表的 nday 漏洞，成功地侵入了该单位集团的内网，他们利用 Springboot nday 漏洞和后台系统的弱口令，找到集团系统运维手册。根据手册中的信息，他们确定了靶标系统的地址和账户信息，最终成功地控制了目标系统。

五、安全加固建议

在历次攻防演练活动中，0day+nday 组合利用已成为攻击团队突破防线的有力武器。在遇到 0day 攻击时可以从梳理排查、情报预警、安全布防、监测处置、常态化运营 5 个层面建立 0day/nday 漏洞综合防护体系，有效防范 0day/nday 攻击，尽最大可能地降低 0day/nday 带来的危害。

· 全面资产梳理，快速锁定影响范围

全面梳理资产，通过内外部风险及暴露面的排查和加固，厘清资产，发现风险及隐患，防微杜渐、减少攻击面。通过攻击路径和网络访问路径资产的梳理，减少互联网出口，梳理并关闭三无资产，形成清晰的资产图谱和清单，能够快速定位、掌握各类资产的情况，尤其是具有特殊权限的资产；收集盘点历史 0day 情报数据，统计并分析单位资产所涉及的历史 0day 情况；针对存在潜在安全风险的供应链安全、代码安全、域安全、云平台安全、API 安全等进行脆弱性检测，发现安全隐患，及时进行加固。

· 情报及预警能力建设，提升 0day 漏洞预警能力

加强漏洞情报收集，是做好 0day 漏洞预防的基础。定向收集商业软件和开源软件的 0day/nday 漏洞情报，通过云地结合的漏洞情报，强化基于情报的精准分析。情报与内部资产进行匹配，迅速锁定可能受到影响的资产范围。通过情报预警信息的接收、研判、推送及应急联动响应机制，确保网络安全事件处理过程中信息的快速获取、传递、联动响应和统计分析，从而达到早预警、早响应、早处置的目标，有效提升对 0day 漏洞安全事件的应急处置能力。

· 综合布防，有效防范 0day 攻击

1) 加强终端及主机防护：部署漏洞攻击防护系统，基于内存指令流检测技术，在内存指令层检测网络攻击行为，有效抵御 0day 漏洞攻击、高级后门、APT 攻击等各类漏洞利用攻击带来的风险。终端及主机部署 EDR 或主机防护系统，配置主机系统加固功能，能阻止漏洞利用后的下一步行为，如提权、反弹 shell、监听原始套接字、对外进程执行危险命令。启用应用运行时自防护（RASP），基于分析流量上下文、执行行为特征检测，使应用程序能够自我监控和识别有害的输入和行为，能有效防御基于传统签名方式无法有效防护的应用漏洞，有效提高 0day 及未知攻击的防护。

2）蜜罐伪装，重点布防。单位围绕自身互联网业务系统场景，分类部署多维度交互蜜罐系统。通过监测蜜罐系统访问攻击流量，捕获攻击者访问的特殊 API 路径，并及时在对应真实网站的测试环境做访问验证，协同专业服务人员分析漏洞特征及利用方法，针对性进行加固升级，形成对 0day 漏洞的“监控——捕获——处置”闭环。

· 强化全面监测，及时高效处置减少损失

全网部署的威胁监测分析系统，加强对互联网、办公网、分支机构、第三方接入、专网接入、VPN 接入和内网各个关键区域的安全威胁分析，针对网络攻击和异常访问实时进行分析和发现，构建覆盖全局的主动监测体系，从而形成主动防御的安全能力基础。通过云地结合的预警、分析、研判、响应处置服务，集中精力和兵力，做到监测及时、分析准确、处置高效；结合自动化处置工具，切实提高监测响应的处置效率，将安全威胁影响降到最低。

· 常态化安全运营，安全工作高效闭环

基于平战融合、云地协同的网络安全运营原则，建立常态化的资产、漏洞、威胁的安全运营，通过人 + 工具 + 流程的方式，基于安全监测、终端和主机安全防护等措施，持续地进行发现识别、监测分析、研判处置等闭环管理，实现漏洞威胁的动态清零，在持续的运营过程中提升 0day/nday 防御能力。安

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。

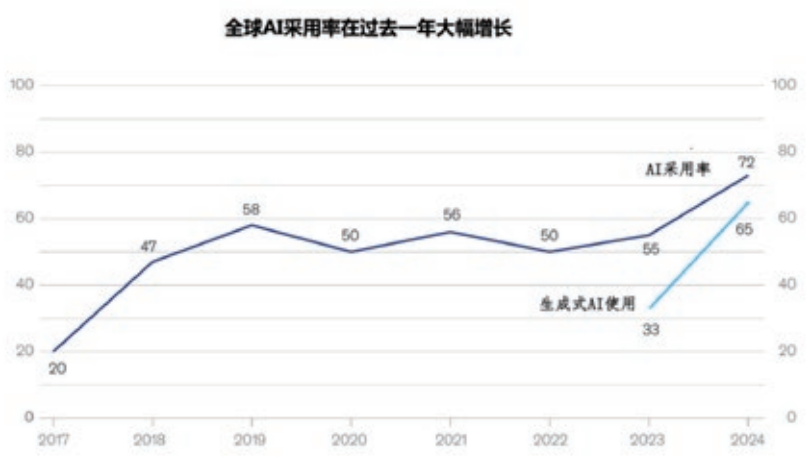
2024 年，银行机构、科技行业，以及医疗保健行业的勒索软件攻击最为严重。2024 年 2 月，美国最大的医疗 IT 公司 Change Healthcare 遭受勒索软件攻击——这是历史上最严重的医疗保健网络攻击，也是有史以来最大的医疗保健数据泄露事件。攻击组织窃取了约 1 亿人的个人、健康和财务信息。攻击对美国医疗系统产生了重大影响，导致许多药店无法处理处方。

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

作者　奇安信漏洞应急响应中心

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

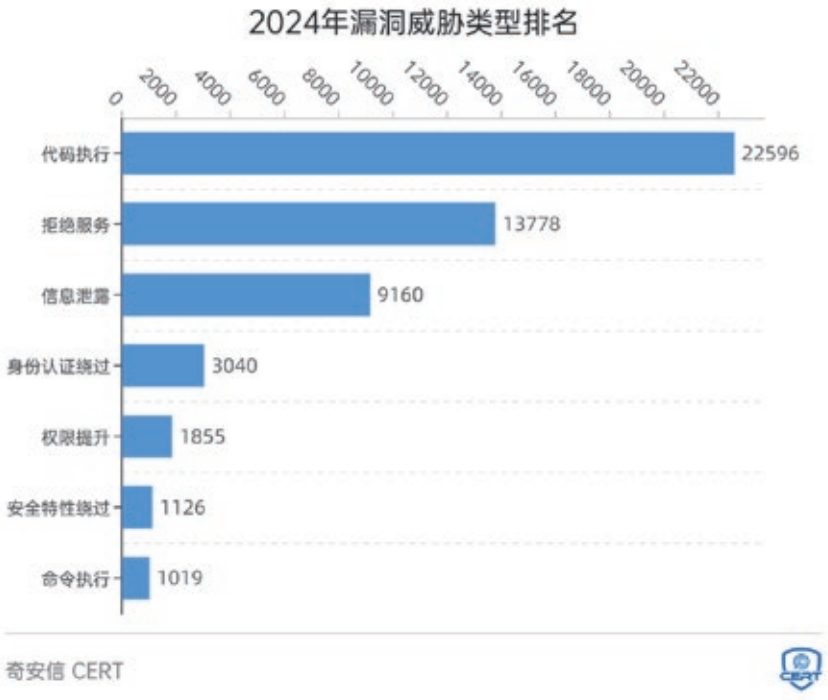


图 1-2 漏洞威胁类型排名

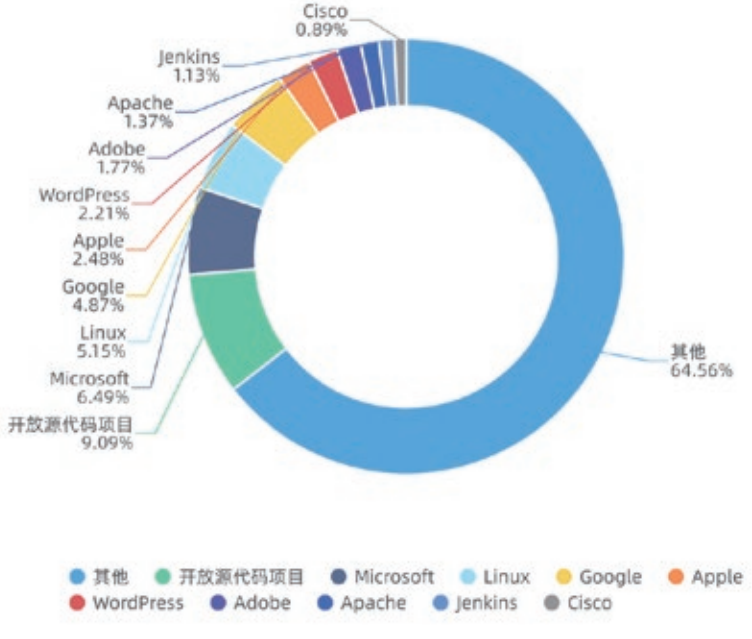


图 1-3 漏洞影响厂商占比

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

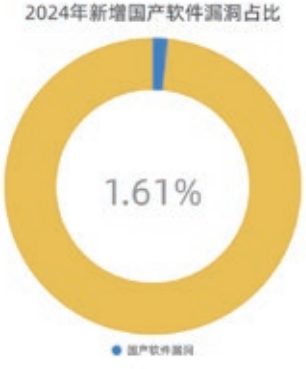


图 1-4 国产软件漏洞占比

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：

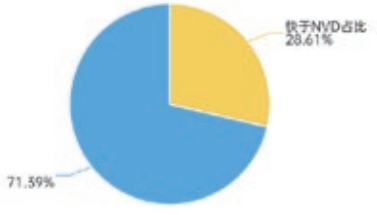


图 1-9 漏洞收录快于 NVD 占比

图 1-10 漏洞定级速度快于 NVD 占比

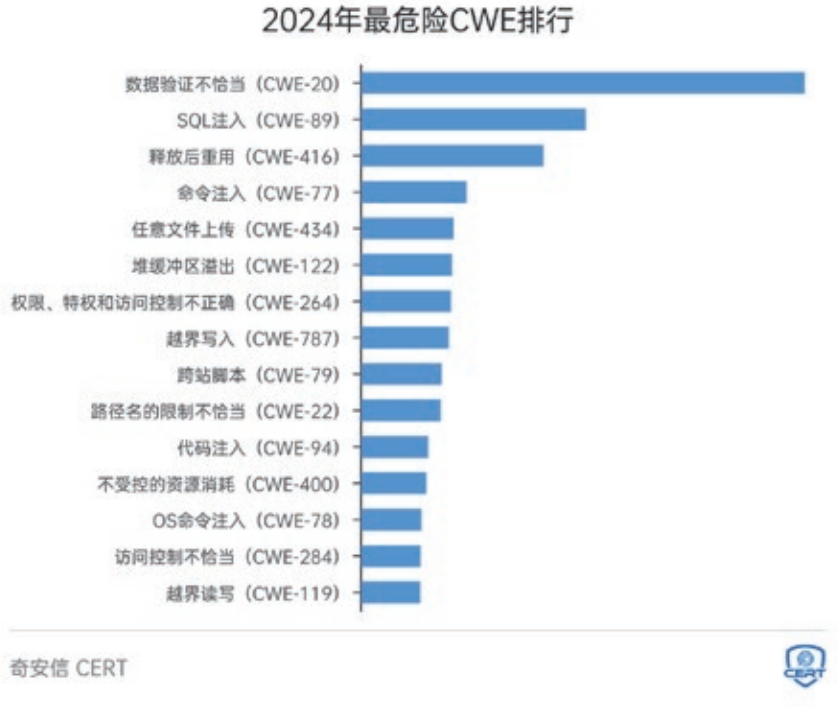


图 1-8 2024 年最危险 CWE 排行

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

作者　赵慧杰

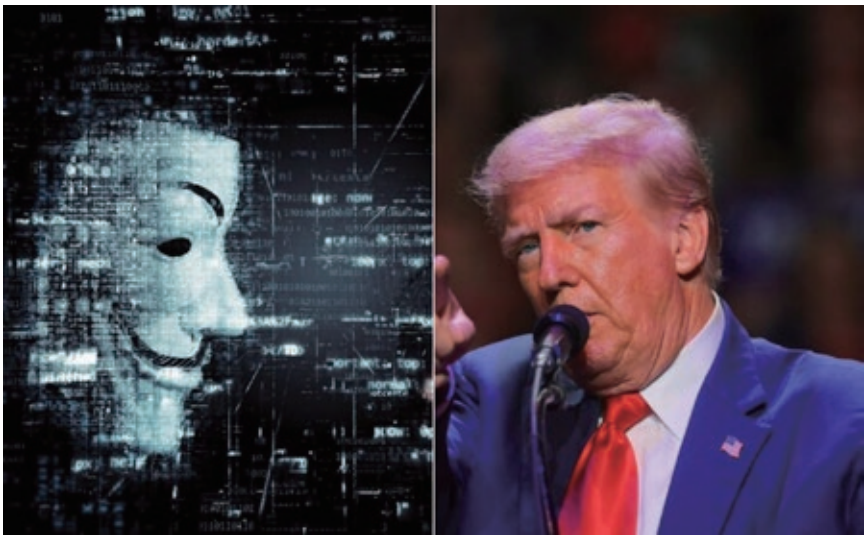
2024 年，全球网络空间呈现区域性和阵营性紧张态势，世界强国国防网络建设竞争持续加速，网络空间正加速演变为战略威慑与控制新领域。国家间网络斗争博弈日益加剧，网络空间斗争从技术力量抗衡走向体系化国家力量比拼，网络战成为国家实现政治、军事、经济等利益的重要手段。

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 Al 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。安

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）

作者　裴智勇

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。

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。

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

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。

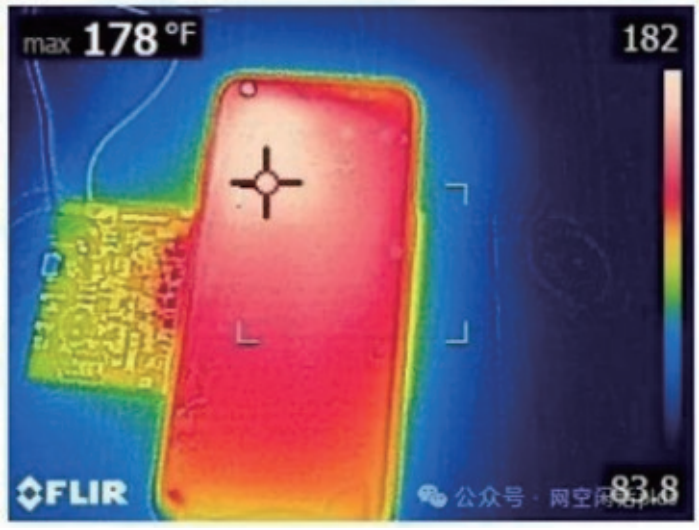
无线充电系统通常依靠电磁感应原理，利用电磁场在两个物体之间传递能量。充电器包含一个发送线圈，交流电在其中流过，产生振荡磁场，智能手机包含一个接收线圈，从磁场中捕获能量，并将其转换为电能，为电池充电。

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。安

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一——数世咨询认证

拥抱趋势，务实前行

——2024 年网络安全建设标杆案例回顾

2024 年，各行各业的政企机构对于网络安全的投入和建设，少了一些盲从，多了一些务实，逐渐褪去浮华，更加聚焦场景和价值。面对依然肆虐的勒索攻击、数据泄露、APT 攻击等网络威胁，以及合规监管日益严格的趋势，政企机构在 2024 年积极拥抱新趋势，持续探索不同场景下的安全建设方案。

他山之石，可以攻玉。《网安 26 号院》在本年度若干个标杆案例中，逐步梳理出共性，结合不同场景，剖析客户在网络建设中的探索历程，以飨读者，为从业者提供参考。

趋势之数据安全：

华南某市数据安全“三同步”样板间探索

2024 年，数据安全建设依然是高频热词。各地积极开通公共数据授权运营，“数据二十条”加速探索落地，数据要素政策稳步实施，数据流通交易日渐活跃，多重因素叠加，数据安全掀起新一轮建设浪潮。

华南某市是珠三角中心城市之一，粤港澳大湾区重要节点城市，国家历史文化名城之一。近年来，该市政数局大数据中心随着各委办局数字化业务不断扩大，数据治理与共享业务不断增多，一期原有的单数仓技术架构主件难以满足实际的数据共享需求，中心随即启动二期“一湖双仓”新技术架构设计工作，基于新技术架构的数据安全保障亟待完善。

经过多方比较，该市政数局最终选择和奇安信合作，双方依托数据安全治理、数据安全技术、数据安全运营三大体系，本着治理先行、循序渐进的原则，形成贴合实际需求的整体解决方案，树立了政务数据安全“三同步”建设的样板间。

该市政数局面临的数据安全挑战来自于三个层面：

1、政务数据价值高、覆盖面广，亟需进行分级保护；

2、存在跨边界数据传输需求，需要对数据调用全面监控；

3、数据在采集、流转过程中链

条很长，对于接触数据的相关方需要严格管理。

为了解决这些问题，该市政数局和奇安信合作，遵循治理先行、防范泄露、持续运营的路线节奏，稳步推进。

在建设思路方面，采用完整的治理、技术、运营三大体系，形成贴合实际需求的整体方案。

在治理阶段，双方遵循“安全有道，治理先行”原则，在合规指导之下，开展数据安全治理服务，具体包括：

1、共同调查数据安全现状，评估服务内容，识别数据安全关键风险，给出风险缓解措施和整改建议；

2、建立组织框架，编制制度和规范，进而推动数据安全分类分级，绘制敏感数据流转视图；

3、结合业务战略、合规、治理和风险容忍度等，制定数据安全总体目标、方针和策略；

4、结合现状评估结果，设计数据安全防护体系及演进路线。

在技术阶段，奇安信以防范泄露，杜绝勒索为目标，通过技术手段强化安全能力，具体包括：

1、通过防泄露方案设计，帮助客户实现数据资产可视，数据风险可知，泄密行为可管，安全事件可溯源四个目标；

2、通过数据态势——数据资产地图能力，结合数据安全治理资产梳理服务，形成安全视角下的一湖双仓数据资产可视化；

3、通过专业产品能力和定制化安全策略，检测数据库访问、API 访问、特权访问三大重点应用场景下安全风险；

4、通过数据安全态势感知汇集安全日志关联分析，构建风险检测模型。

在运营阶段，奇安信帮助客户建立常态化数据安全运营体系，以及应急响应体系，确保管理得到有效执行、技术得到有效使用。

1、建立了“专家 + 流程 + 平台”的运营机制，根据业务数据及风险情况，实时调整安全策略，依托多源数据汇聚、数据流动监测、监测与分析、安全事件及时发现、审计溯源等做整体态势感知。

2、基于运营机制建设了数据安全运营中心，承担全局感知、集中运营、风险闭环、合规保障等职责。在运营体系中，分为日常运营和场景化运营两大部分：日常运营包括数据资产运营、安全策略运营、安全风险运营、安全事件运营、运营监控等；场景运营包括数据安全风险评估、系统上线评估、应急响应、重大保障、赋能培训等。

数据安全建设年终共性小结

2024 年的客户数据安全建设，经历了从局部到整体，从单一到体系、从静态到动态的跃迁和提升。过去，很多客户更聚焦于 API 数据安全，特权账号管理、数据库审计、数据跨境等单一场景，而在华南某数据局的某能源集团、某大型制造企业等客户实践中，充分验证了奇安信数据安全的“三步走”方法论的可行性和良好效果，通过治理、技术、运营的闭环形成，让安全能力与日俱增，让政企机构数据处于持续安全的状态，保障数字化行稳致远。

趋势之安全运营自动化：

某城市银行的安全运营体系化建设之路

金融安全是国家安全的重要组成部分，是经济平稳健康发展的重要基础。金融行业的数字化程度普遍较高，业务环境非常复杂，网络和数据安全要求更严苛、挑战更艰巨。在2024年，金融客户更加务实、更加聚焦如何提升网络安全建设的实际效果，如何显著提升安全运维的效率，如何让安全运营的价值指标化、成果可视化，是他们最关心的话题。

作为国内知名的城市商业银行，C银行在金融科技的浪潮之中，积极应对各方面挑战，通过网络安全运营体系的建设，探索出效率和效果双提升之路。

C银行在数字化转型过程中，提出了“生态银行”的战略，核心就是要把资源整合连接起来，打造为客户赋能、为客户创造价值的超级链接的开放银行，以生态场景为触点，通过API、SDK、小程序等技术连接生态各方。毫无疑问，数据开放扩展了数据边界、技术交互延伸了网络边界、业务融合打破了产业边界，金融科技的运用和业务场景的重构，导致网络安全、数据安全等面临全新的安全挑战。

网络安全运营的建设不是一蹴而就的，C银行在安全运营体系建设的各个阶段中，都遇到了不同程度的难题。

第一阶段的难题是安全难以管理，数据零散，缺少抓手，运营无从下手。

第二阶段的难题是告警疲劳问题突出，海量数据无法有效管理。

第三阶段，最突出的矛盾在于，平台在管理、流程等方面的联动能力缺位，没有以平台为中心形成一套体系，各类系统未能打通，运营能力存在缺位。

基于以上挑战，C银行安全运营的建设思路可以归纳为：以当前低位安全能力为基底，通过大数据、机器学习、SOAR、NDR、TIP等技术和工具，结合自动化流程，建设智能化、自动化、实战化的安全运营中心，打造“威胁感知、分析定位、智能决策、响应处置”的快速安全闭环能力，帮助C银行打造安全效果，提升安全运维和安全管理效率、展现安全成果，最终实现“自动响应闭环、持续安全运营”的目标。

安全运营技术体系是安全建设的重中之重，C银行的技术体系示意图如下图所示。

其中，NGSOC是整个安全运

营体系的“大脑”，是安全运营工作得以持续开展的“管理中枢”，而SOAR、NDR、TIP等工具是安全运营体系的“四肢”，通过打通内部管理流程、协同各类安全工具能力，打造发现威胁、分析威胁、研判威胁、处置威胁的多维安全能力闭环。

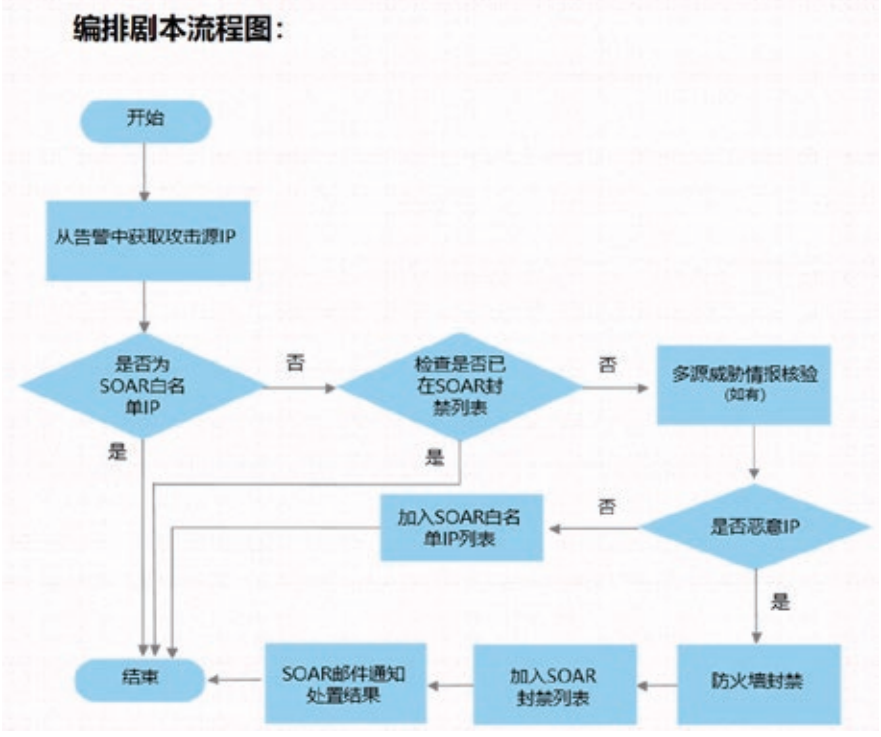
C银行安全运营第一步工作是构筑安全运营四大基础底座。即通过安全运营分析平台（NGSOC）、安全编排自动化与响应系统（SOAR）、网络流量威胁检测系统（NDR）和威胁情报平台（TIP）共同构筑。

底座1：态势感知与安全运营平台（NGSOC）是驱动安全运营体术体、系运行的“基础”。

底座2：安全编排自动化与响应系统（SOAR）是安全运营技术体系协同运行的“纽带”。

底座3：网络流量威胁检测系统（NDR）是安全运营技术体系实战对抗的重要“抓手”。

底座4：威胁情报平台（TIP）是发挥安全运营技术体系实战化能力的“核心”。



搭建好四大基础底座之后，C银行将工作重点放在安全能力的全面提升上，可以归纳为“智能化”“自动化”和“实战化”三个层面。

首先是打造“智能化”的安全分析能力。基于NGSOC的多源异构安全大数据采集与处理能力，实现数据采集融合和综合管理。

其次是打造“自动化”的响应处置能力。为了解决运营成本高、安全响应慢等问题，C银行采用了安全编排、自动化与响应技术，来实现安全事件处置和安全管理过程跟踪自动化。

再次是打造“实战化”的安全防守能力。通过多个基座产品等综合运用，构建“防得住”的安全运营体系，全面提升实战能力。

最后，在“智能化”“自动化”和“实战化”的基础上，C银行还进一步实现了安全运营价值指标化与成果可视化，便于监督和指导安全管理工作。通过这些工作，C银行不断提升网络安全分析智能化、响应自动化和防守实战化水平，有效降低未知风险引发安全事件的概率，实现企业现有安全运维效率和安全建设效果的双提升！

安全运营建设年终共性小结

在2024年的众多项目实践中，越来越多的企业客户关注运营自动化和效果可视化。从中化集团的“人+工具+流程”三位一体，到某制药集团、佛山大学、某省铜业集团等，他们充分依托NGSOC+SOAR工具来提升运营效率，并积极探索安全运营需要与业务价值紧密相连，并通过可视化方式展示出来，让运营价值更加直观可视，实现安全投入和安全效果的正向联动。

趋势之信创替代：

某电网公司信创终端替代一体化解决方案

2024 年，是信创替代党政、金融等行业逐步向运营商、能源电力、教育等行业全面拓展的一年。然而，信创并不意味着安全，甚至可以说，信创更需要安全。因为信创工程是我国信息化建设重塑的先导工程，面临的新场景、新威胁更加复杂，对安全提出了更高的挑战。

某电网公司拥有 34W+ 终端、1000+ 应用系统，有点多、面广、战线长、架构复杂、业务更新快等特点，在信息安全方面天然存在资产盘点困难、风险暴露面广，以及隐藏风险和不确定风险多等问题。

为了深化项目的信息化建设，实现信息化集约管理、有效管控、安全管控、防范各类风险，应对各类常态化专项任务期间的安全挑战，该电网决定采用信创终端一体化建设和准入安全统一管控的方式确保项目的标准化防护，以及对单位基础设施的完善和信息化水平的提高提供强有力的支持。

当前，该电网公司面临的挑战主要来自于几个方面：

1、终端统一管理：在信创替代过程中，Wintel 终端与信创终端将长期并存，迫切需要实现全终端的统一管理和安全管控。

2、信创终端多样化：该公司内部部署的信创终端操作系统包括麒麟软件和统信 UOS，应用的芯片架构涵盖兆芯（x86）、鲲鹏（ARM）、龙芯（MIPS）。由于历史版本多且部署分散，终端的管理和维护面临较大挑战。

3、业务访问体验一致性：在上千个业务系统中，许多系统尚未具备迁移条件，员工在信创终端上难以获得与 Wintel 终端相同的应用体验，导致业务访问和日常办公效率受到影响。

4、实现利旧共用：在信创替代过程中，除了统一管理安全管控，还需要实现对现有准入产品的利旧共

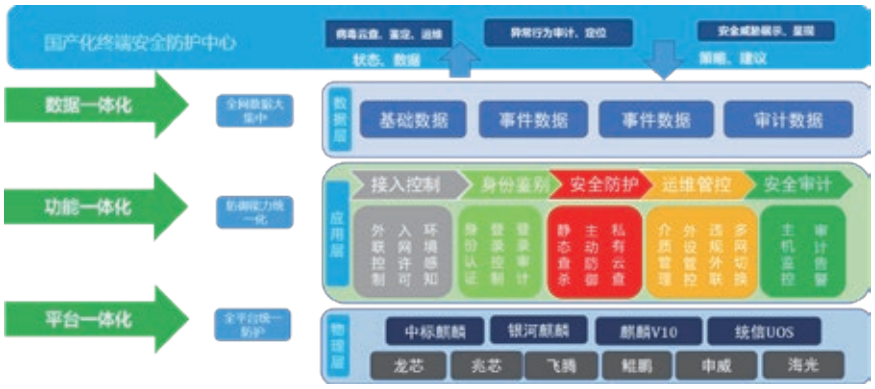
用，以有效降低成本投入并确保系统平稳过渡。

经过充分调研与论证，某电网公司总部外网部署了奇安信天擎终端安全管理系统及准入系统，以全面提升终端安全能力。该系统具备病毒防护、多网切换、主机防火墙、主机审计等核心功能，同时在终端准入和移动存储设备管控方面，实施了针对性解决方案。

在建设过程中，除了增强常规终端安全能力，还特别针对两大迫切问题采取了针对性措施。

1、终端准入：通过准入功能与现有身份认证服务结合，统一身份认证和入网认证过程；通过主机防火墙功能，统一管理终端访问权限；通过非法外联探测能力，防范潜在的安全风险。

2、移动存储设备管控：通过设备注册、标签授权、设备授权、挂失管理、外出管理、终端申请、漫游管理、移动存储例外等多种控制模块，实现对移动存储设备的全生命周期管控，按需分配权限，提供全面的注册、授权和审计功能。同时，系统具备对移动存储设备状态的集中管理，便于管理员进行实时管控。



该方案具备以下优势：

1、统一管理：成功实现了Wintel终端与信创终端的长期共存和统一管理，保障了整体信息安全管控的一致性。

2、同等管控力度：确保信创终端与Wintel终端在合规性和安全管控要求上的统一标准，提供同等级的管控力度。

3、业务访问体验一致性：解决了信创终端与Wintel终端间业务访问体验不一致的问题，显著提升了员工的工作效率和应用流畅性。

4、数据驱动安全：通过建设终端安全运营可视化系统，为终端安全治理提供强有力的数据支持，实现了数据驱动的安全管理模式。

在该项目的建设中，在国产化替代、政策合规、终端管理、威胁闭环等方面，充分体现出了全方位的亮点。

1、全面的信创安全防护体系：成功建立了完整的信创环境下终端安全防护体系，有效应对了新型环境下的安全挑战。

2、行业政策符合性：全面满足了身份鉴别、终端管控等行业政策要求，确保符合国家及行业安全合规标

信创安全建设年终共性小结

在2024年不同行业的信创替代建设中，跨平台的平滑过渡、统一管理、访问体验一致性等是共性话题，在某国家部委全国数十万系统用户向信创平台的平滑迁移，到某头部电网公司的信创替代，都面临大规模、复杂系统的信创替代难题。因此，信创替代不是简单的更换，更是需要兼顾过渡期的业务连续性和稳定性，相关系统的易用性和管理效率，以及整体的安全可靠性和政策合规，只有兼顾整体，才能真正实现国产化替代。

准。

3、终端数据集中管理：实现了全网终端安全数据的集中管理，显著提升了威胁风险的精准定位与快速响应能力，增强了整体安全态势感知。

4、安全威胁闭环防御：构建了涵盖预防、防护、检测和响应的安全威胁闭环防御机制，有效降低了潜在安全风险。

总体来看，该电网公司通过奇安信信创终端替代平滑过渡解决方案，成功解决了其统一终端安全管理与运营的问题，提升了信息安全管理水平，并符合行业政策要求。该方案有效解决了其信创终端的标准化管理不足、信息安全漏洞遗留及服务质量不均等问题。结合“数据驱动安全”理念，建设了终端安全运营可视化系统，实时呈现终端安全效果，针对性分析当前不足，将真替、真用效果可视化，综合提升了其终端安全管理成熟度。

趋势之云安全：

重任在肩迎风而上，国企安全上云探索与实践

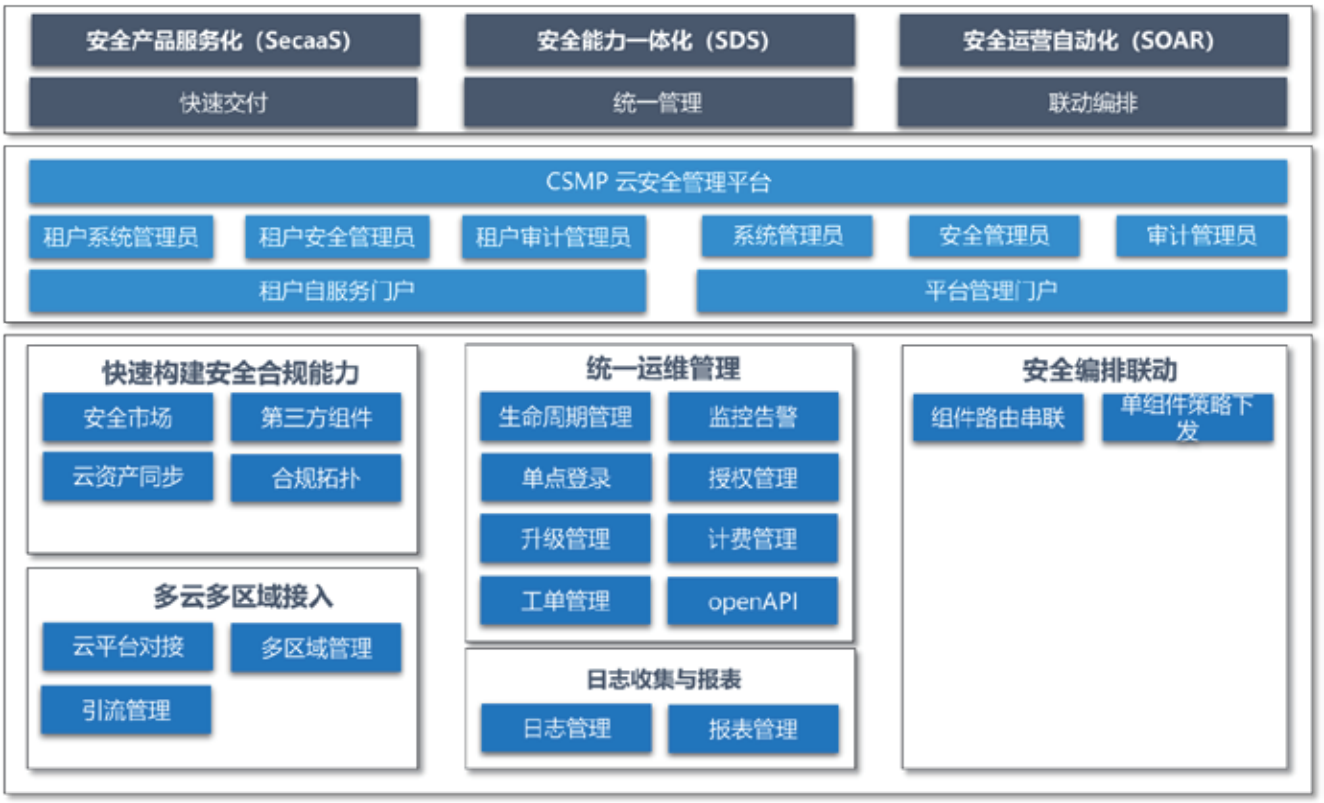
作为数字化转型的“先锋队”和“主力军”，2024 年以来，国有企业全面加速上云、用云的进程，带头引领以云计算为代表的新一轮科技革命，成为数字经济发展的重要力量。

然而，国企数字化平台大都承载着关乎国计民生、社会稳定的业务和数据，一旦遭受黑客攻击或数据泄露和破坏，都会引发不可估量的严重后果。而全球频发的云基础设施频繁遭受攻击，更体现了这种严峻形势。如何在云体系建设过程中，提供安全可靠、自主可控的网络安全保障，成为摆在国资委和各国企面前迫切要解决的问题。

总体来看，国企云安全面临以下四个方面的挑战：

首先是云计算给现有安全架构带来了严峻挑战，安全隐患无处不在。

云计算弹性化带来了便利，同时带来了大量僵尸主机、不当暴露的端口、不当安全配置、弱口令等。同时，云计算导致传统安全域划分逐渐失



效，东西向流量不可见、横向移动无法及时发现等成为主要的安全问题。云上业务的复杂化导致更多暴露面，无文件攻击、供应链攻击等新型攻击方式出现，竖井式的安全设备无法及时发现问题。

其次是外部的网络攻击日益专业化、趋利化，对关键基础设施威胁加大。

云上算力高度集中、数据高度集中、以经济为目的，勒索、挖矿、数据窃取等攻击方式大行其道。数字货币起推波助澜的作用。云数据中心作为关键基础设施，以政治为目的，专业 APT 组织日益猖獗，国家关键基础设施成为主要攻击对象。

再次是虚拟化引入给云基础设施带来新的风险。

国企云基础设施防护包括构建云计算环境所需的云操作系统（云业务及云基础设施管理）、虚拟化层（Hypervisor）、基础设施（网络、计算、存储）的安全防护。云基础设施一旦被攻破，将威胁到云平台所承载的所有应用安全。

最后是提供国企云服务的企业，普遍面临来自 Web 安全、内容安全、应用安全等业务应用层的风险。

面对市属国有企业的数字化转型需求和网络安全挑战，在市国资委指导下，北控数科联合奇安信，共同建设和运营国企云，保障国企云安全，赋能市属国企数字化转型工作。以国企云核心能力为驱动，打造“北京方案”、创造“北京模式”、塑造“北京样板”，用数字化手段助推北京全球数字经济标杆城市建设。

首先，通过奇安信云安全管理平

台为北控数科云搭建云基础安全防护体系，并通过三项核心功能满足云计算数据中心安全需求。

① **安全产品服务化：**通过将安全产品资源池化，支持多资源池弹性部署，从而解决客户快速构建安全合规能力，和多云多区域接入的需求，实现快速交付；

② **安全能力一体化：**通过将安全能力整合在云安全管理平台，进行统一运维管理和数据展现，从而解决客户统一运维管理和日志收集报表展现需求，实现统一安全管理；

③ **安全运营自动化：**通过在平台整合安全组件的网络能力，支持如防火墙 WAF 的路由编排和策略下发，从而解决客户的安全联动需求，实现安全能力联动。

其次，云安全管理平台提供两类门户入口，支持租户通过自服务门户进行安全组件的创建和业务管理，也支持管理员通过平台管理门户进行统一管理，租户和管理员都支持三权分立模式，默认平台管理门户支持系统管理员，租户自服务门户支持租户系统管理员、租户审计管理员，开启三权后，支持系统、安全和审计三个角色。

针对云计算环境特性及安全需求分析，奇安信云安全管理平台遵循国家信息安全等级保护第三级要求和相关安全建设标准规范，构建了一套体系化的云计算环境安全保障体系，全面提升云计算安全管理水平，以及运营水平，并具备自适应、弹性伸缩、敏捷性等管理优势，以适应云计算动态变化的安全需求。

此外，国企云安全中心基于新一代网络安全框架，以及内生安全理念，着力构建体系化、集约化的安全能力，以保障国企云、市属国企云上业务安全，并提供定制化安全服务。通过部署奇安信态势感知与安全运营平台等产品，全面感知市属国企云数据中心的安全态势，为国企用户业务的统一安全监测提供技术支撑和数据支撑。

得益于双方的深度信任和默契合作，国企云安全中心在云平台建设之初就深度融入其中，从而把安全能力与业务系统和相关流程紧密结合起来，进行深度融合，将原来静态的、局部的、外挂式的安全策略，升级为动态的、系统的、内生的防护措施，从而建立自适应的安全免疫体系，真正实现内生安全“自适应、自主、自生长”的目标。

总体来看，本项目不仅是北京市国资委国企云安全建设的重要抓手，同时，这种模式对全国各地国企云建设及联合运营模式，有非常强的借鉴参考复制意义和价值。

云安全建设年终共性小结

“上云是常态，不上云是例外。”2024 年，以云计算为代表的数字技术与各行业的深度结合，引领新一轮数字化浪潮。各行业客户都充分意识到，云平台安全防护是整体项目的重要组成部分，云安全和云计算建设不能割裂来看。客户普遍遵循“同步规划、同步建设、同步运营”原则，“软件定义安全”理念构建云安全资源池。同时采用先进技术 SDS、NFV 的方式构建云安全保障体系，并提供弹性、自助、可视、可管、可控的安全保障能力，为云计算平台保驾护航。

大事记

奇安信集团与温氏集团签署战略合作，开创 AI 安全赋能农业新篇章

12 月 18 日，奇安信集团与国内最大的农牧集团温氏食品集团正式签署战略合作协议，旨在共同探索 AI 安全赋能业务的场景，在网络安全、数据安全及人工智能安全等多个领域展开深入合作，共建温氏“大安全体系”，并计划在智慧农业等新兴领域挖掘更多创新应用场景。

河南省政务大数据中心书记王彦生带队调研奇安信中原区域总部

近日，河南省政务大数据中心党委书记王彦生带领中心相关领导、省辖市大数据中心相关领导和专家一行 50 余人，到奇安信集团中原区域总部进行调研考察交流，奇安信集团河南省分区总经理熊国强陪同调研。

此次调研活动体现了大数据中心领导对政务系统网络安全和数据安全的高度重视。通过深入企业一线，参与调研的领导和专家们纷纷表示，详细了解到奇安信集团整体发展历程、企业荣誉、研发投入、技术实力，以及在河南省内运营发展规划、城市网络安全运营典型运营模式，并对集团公司的技术创新能力和市场前景给予了高度评价，并希望双方在网络安全运营保障等方面展开更深入、更广泛的合作。

齐向东到访大唐集团两大能源企业

12 月 9 日，奇安信集团董事长齐向东带队分别到访了中国大唐集团能源投资有限责任公司和大唐（内蒙古）能源开发有限公司，与两家公司的高层领导就网络安全防护技术在能源领域的应用进行了深入交流。

此次访问不仅加深了奇安信与大唐集团旗下两大重要能源企业的合作关系，也为未来网络安全技术在能源行业的广泛应用奠定了坚实的基础。奇安信将继续致力于提供最前沿的安全解决方案，助力企业构建更加坚固、智能的网络安全防护体系，让网络更安全，让世界更美好。

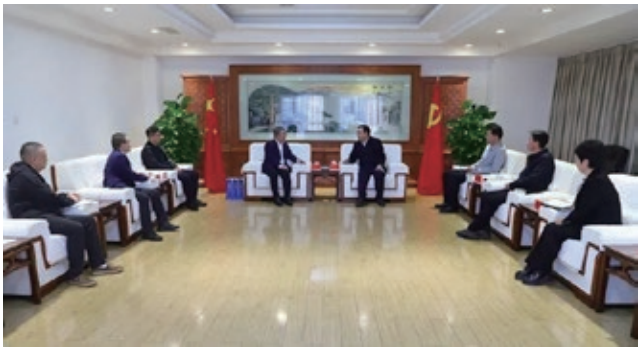
齐向东：用标准迎战大模型时代的安全挑战

12 月 8 日至 11 日，全国网络安全标准化技术委员会 2024 年第二次“标准周”活动在海口市举行。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东受邀出席。

齐向东在“网络安全大模型与安全协同能力的思考——用标准迎战大模型时代的安全挑战”主题演讲中表示，针对大模型时代对安全防护提出的各种挑战，可用强制性合规标准进行应对。当前，大模型在各行业广泛应用，我们必须加快制定并落实针对大模型的强制性合规标准，确保其研发、训练、部署全流程的安全要求与最佳实践得以严格遵循。

中卫市委书记刘国强会见奇安信集团董事长齐向东一行

12 月 5 日，中卫市委书记、市人大常委会党组书记刘国强会见奇安信集团董事长齐向东一行。



刘国强对齐向东一行来卫深化合作表示欢迎，对奇安信集团长期以来给予中卫发展的支持帮助表示感谢。希望双方在已有良好合作的基础上进一步加强沟通对接，深化多领域、全方位战略合作，同时发挥企业资源优势和桥梁纽带作用，吸引带动更多产业链上下游企业选择中卫、投资中卫，深度参与中卫数字信息产业发展，为中卫经济社会高质量发展助力赋能。

奇安信协办 2024 第三届北外滩网络安全论坛

12 月 5 日，2024 第三届北外滩网络安全论坛在上海世界会客厅举行。论坛以“新机遇、新挑战、新使命，高维推动网数安全、人工智能双向融合赋能”为主题，中国工程院邬江兴院士、黄殿中院士、吴世忠院士、童小华院士出席会议并发表演讲；30 余家行业主管、监管部门及百余家关基单位和网络安全头部企业代表出席，为网络安全、数据安全领域谋划提供新思路、新举措。

作为本次论坛的协办单位，奇安信集团全程深度参与，通过实际行动为推动全球网络空间的共建、共治、共享，作出积极贡献。

齐向东受邀参加“一带一路”建设工作座谈会

12 月 2 日，第四次“一带一路”建设工作座谈会在北京举行。中共中央总书记、国家主席、中央军委主席习近平出席并发表重要讲话强调，自 2013 年提出共建“一带一路”

倡议以来，在党中央坚强领导下，经过各方共同努力，共建“一带一路”始终秉持和平合作、开放包容、互学互鉴、互利共赢的丝路精神，始终坚持共商共建共享的原则，合作领域不断拓展、合作范围不断扩大、合作层次不断提升，国际感召力、影响力、凝聚力不断增强，取得了重大成就，为增进同共建国家友谊、促进共建国家经济社会发展作出了中国贡献。

中共中央政治局常委、中央办公厅主任蔡奇出席座谈会，中共中央政治局常委、国务院副总理丁薛祥主持座谈会。作为全国工商联副主席、优秀民营企业家代表，奇安信集团董事长齐向东受邀参会并在前排就坐。

河北省委常委、石家庄市委书记张超超与齐向东一行进行工作会谈

11 月 27 日，河北省委常委、石家庄市委书记张超超与全国工商联副主席、奇安信集团董事长齐向东一行进行工作会谈，双方就深化网络安全领域合作，提升石家庄城市数字化安全发展水平进行深入交流。

张超超说，石家庄大力推进“数字政府”和新型智慧城市建设，深化政务数据归集和共享应用，努力实现“一网通管”“一网通办”“一网协同”，这些离不开高水平网络安全服务的支持。奇安信集团在网络安全方面拥有雄厚的技术储备和丰富的实战经验。希望双方以此次会谈为契机，遵循市场经济规律和可持续发展理念，围绕智慧城市建设，深化在网络安全领域合作，实现共赢发展。我们将进一步优化营商环境，强化服务保障，为奇安信集团在石家庄发展创造良好条件。

北京市百名高端涉外法治人才研修班来访奇安信集团

11 月 22 日，北京市百名高端涉外法治人才培养项目研修班的三十余位成员走进奇安信集团，深入探讨奇安信在电子数据司法鉴定与数据安全合规等法律科技领域的前沿实践。此次活动聚焦涉外法治，通过深度互动与交流，探索法律与技术深度融合的新路径，为首都涉外法治建设注入强劲动能。

活动结束时，多位研修班成员表示，此次参观交流让他们对奇安信在司法鉴定和数据安全合规领域的创新实践有了更加深入的认识。他们认为，随着技术驱动的法律服务模式逐渐成为常态，奇安信提供的专业化、全链条解决方案为涉外法治事务中的合作带来了全新视角和更多可能。

产品动态

奇安信可信浏览器率先升级至 Chromium132 内核

近期，奇安信可信浏览器先锋版率先升级至 Chromium132 内核，再次实现了国产浏览器与业界最前沿 Chromium 内核的紧密同步。本次升级，在浏览器功能、产品性能、安全能力、用户体验等方面均有显著提升，以更贴近用户应用场景为出发点，为广大政企客户带来浏览器的极致体验。奇安信可信浏览器正是凭借稳定的内核升级速度，始终保持着国内企业浏览器赛道的技术领军地位。

信创市场再传捷报！奇安信中标某央企航空公司零信任项目

近日，奇安信中标某央企航空公司基于信创技术的零信任体系建设二期项目。奇安信将基于该集团零信任平台的发展需要，尤其是信创环境下的终端和业务安全风险场景，开展零信任二期建设，帮助公司进一步提升各类业务场景的安全能力，杜绝内外部威胁，保障应用系统和数字资产安全，为航空行业打造基于信创平台的零信任建设新标杆。

荣誉墙

第五届中国人工智能大赛：奇安信获两个 A 级最高荣誉

在12月20日的第五届中国人工智能大赛成果发布会上，主办方宣布，奇安信在大模型赋能网络安全及人工智能赋能代码生成能力赛两场比赛中双双获得 A 级证书。

据悉，本次比赛由国家互联网信息办公室、公安部指导，厦门市人民政府主办，厦门市数据管理局、厦门市互联网信息办公室、厦门市公安局、中国信息通信研究院、中国人工智能产业发展联盟联合承办。QAX-GPT 安全机器人及奇安信代码大模型双双获得 A 级证书。

夺冠！奇安信参赛选手荣获电子数据取证分析师赛项冠军

12 月 14 日 ~15 日，北京市第六届职业技能大赛闭幕式在国家会议中心举办。来自奇安信集团盘古石取证虎贲小队的参赛选手刘夕铭，在电子数据取证分析师赛项中凭借卓越的技术实力斩获冠军；同时，教练组长郑文鑫和奇安信集团，

荣获大赛组委会颁发的传承奖和优胜奖。

天工实验室安全研究成果入选 BlackHat ASIA 2025

奇安信天工实验室安全研究成果，入选国际顶级安全会议 BlackHat ASIA 2025，议题名称《vCenter Lost: How the DCERPC Vulnerabilities Changed the Fate of ESXi》，天工实验室安全研究员将于 2025 年 4 月在新加坡公开分享。

在本次大会上，将详细讲解在 vCenter DCE/RPC 协议组件中发现的 4 个高危漏洞，以及利用漏洞实现远程代码执行，并最终获得 root 权限的过程。

奇安信 AISOC 斩获 2024“金智奖”AI 创新应用大奖

近日，2024 年度（第八届）中国网络安全与信息产业“金智奖”评选结果正式揭晓。本次评选在延续以往对行业前沿创新能力和安全实力的深度挖掘基础上，首次增设了 AI 创新应用奖项，旨在表彰在人工智能领域取得显著成就和突出贡献的企业。经过紧张而激烈的评选，奇安信 AISOC 表现优异，最终斩获年度 AI 创新应用奖。

奇安信一科研成果获 2024 年世界互联网大会领先科技奖

近日，奇安信“加密流量高效检测与动态弹性编排关键技术及应用”项目获得世界互联网大会领先科技奖，并入编 2024 年世界互联网大会领先科技奖收录成果集《科技之魅》。领先科技奖由世界互联网大会举办，旨在奖励全球年度最具领先性的互联网科技成果。

奇安信洞鉴荣获首届“数证杯”电子数据取证分析大赛团体赛一等奖！

12 月 4 日，奇安信洞鉴团队在首届“数证杯”电子数据取证分析大赛中凭借卓越的技术实力和团队协作能力斩获团体赛一等奖。

首届“数证杯”电子数据取证分析大赛由公安部十一局指导，公安部第三研究所、公安部鉴定中心、安徽省公安厅联合主办，安徽省网络安全协会协办，公安部第一研究所、最高人民检察院检察技术信息研究中心、中国合格评定国家认可委员会、清华大学网络科学与网络空间研究院等单位作为支撑单位。

此次获得“数证杯”一等奖，是对奇安信洞鉴技术实力

和团队协作能力的高度肯定，也是多年来深耕电子数据取证与司法鉴定领域的最好证明。奇安信洞鉴将以此次大赛为契机，继续专注于技术突破和专业服务优化，不断为行业树立新标杆，为司法鉴定事业创造更多可能！

奇安信获评工信部 NVDB 漏洞治理合作“三星级技术支撑单位”

12 月 3 日，2024 年第十三届电信和互联网行业网络安全年会在北京召开。在会上，工信部网络安全威胁和漏洞信息共享平台（NVDB）通用网络产品安全漏洞专业库对 2024-2025 年度技术支撑单位进行授牌仪式；针对年度在网络产品安全漏洞管理方面作出杰出贡献的单位进行表彰，奇安信被授予“三星级技术支撑单位”（最高等级）荣誉。

奇安信再获北京市“隐形冠军”企业，持续引领网络安全技术创新

近日，北京市经济和信息化局公布了第一批隐形冠军企业到期复核通过名单。奇安信集团凭借卓越的技术实力和市场表现通过复审，继续保持“隐形冠军”企业的荣誉。这不仅是对奇安信在网络安全领域深耕细作的高度肯定，也标志着公司在高质量发展道路上迈出了坚实的步伐。

最新报告：奇安信获评 IDC 中国数据安全服务市场领导者

国际数据公司 IDC 最新发布的《IDC MarketScape: 中国数据安全服务 2024 厂商评估》报告，对 18 家数据安全服务提供商的市场规模、产品技术能力、行业客户拓展、生态系统建设等关键领域进行了专项评估。报告中，奇安信凭借全面的综合实力，位居数据安全服务市场领导者类别。

奇安信一数据安全项目获评“企业数据安全体系建设实践优秀案例”

11 月 28 日，由中国信息通信研究院（以下简称“中国信通院”）安全研究所主办，大数据应用与安全创新实验室承办的“数据安全共同体计划成员大会（2024）”在京成

功召开。会上公布了 2024 年数据安全“星熠”案例入选名单，中山市政务服务和数据管理局与奇安信的政务大数据中心数据安全项目共同获评《企业数据安全体系建设实践优秀案例》，信通院及评审专家高度评价奇安信在数据安全建设中的引领和示范作用。

奇安信连续 4 年稳居《网络安全企业 100 强》第一名

11 月 29 日，国内网络安全媒体安全牛发布第十二版《网络安全企业 100 强》。奇安信集团连续 4 年稳居中国网络安全企业百强第一名，并在技术创新、行业应用十强榜中均位居第一，彰显了奇安信在网络安全领域的综合实力与领先地位。

社会责任

“心安助农 · 乡村多功能足球场”在和田市依盖尔其小学正式启用

为积极响应国家乡村振兴战略，在北京市援疆和田指挥部的大力支持下，12 月 10 日上午，北京奇安信公益基金会“心安助农 · 乡村多功能足球场”项目捐赠落成仪式在和田市伊里其乡依盖尔其小学举行。这也是在新疆地区落成的第一个“心安助农 · 乡村多功能足球场”项目。

乡村换新颜 “和美乡村计划”助力贵州织金县乡村建设成效显著

2023 年年底，奇安信基金会“和美乡村计划”在贵州织金县落地，近日，该计划取得了一定成果，为当地乡村振兴贡献了重要力量。该计划旨在通过支持乡村人居环境改善和环境污染治理项目，推动乡村生态振兴，助力乡村生态宜居。

在织金县的龙场镇、白泥镇和实兴乡，奇安信基金会的“和美乡村计划”得到了深入实施。这些项目不仅有效改善了乡村的生态环境，还提升了村民的生活质量，为乡村振兴注入了新的活力。

“和美乡村计划”点亮乡村电商之光，助力乡村振兴

2023 年 10 月，北京奇安信公益基金会的 “和美乡村计划”， 为河北盐山和内蒙古敖汉两地的乡村电商发展注入了强大动力。这两个地区在乡村电子商务建设方面面临诸多困难，如设备陈旧落后、销售渠道匮乏、产品知名度低及专业人才短缺等。针对这些问题，该计划通过硬件设施升级、平台搭建、渠道拓展，以及人才培养等一系列措施，有力推动了两地乡村电子商务向高质量发展迈进。

经过一年的不懈努力，两地在电商领域取得了显著成效：多个平台推广账号纷纷建立，硬件水平显著提升，农畜产品销售渠道得以拓宽；通过整合本地特色农产品资源，服务效率和质量大幅提高；借助平台的精心运营与广泛宣传，本地农特产品和乡村电商的知名度不断攀升。该项目的实施不仅有效巩固了脱贫攻坚成果，还为乡村振兴搭建了坚实的桥梁，为现代化美丽乡村建设增添了新的活力与动力。

奇安信入选北京“西城青少年创新学院社会实践基地”

11 月 25 日，北京市西城区教育科研月活动开幕式在北京小学举行。本届教育科研月上成立了北京青少年创新学院西城分院，其首批 14 个区级培养基地和 1 个创新实验基地及 10 个高校实践基地和 10 个社会实践基地授牌成立，首批专家指导团成员获颁聘书。 西城区教委宣布奇安信集团成为首批“西城青少年创新学院社会实践基地”之一。基地将为开展创新人才培养等方面提供专业指导，共同致力于培养具有创新能力和实践能力的拔尖创新人才。

AI浪潮下 奇安信的2024

2024年，人工智能与网络安全深度交织，
奇安信于这一前沿领域奋勇开拓，成果斐然。

1月

北京两会之际，科学技术界别政协委员、全国工商联副主席、北京市商会副会长，奇安信集团党委书记、董事长齐向东提出，借助人工智能、深度学习赋能企业网络安全，拉开了奇安信2024年的AI安全探索大幕。

2月

奇安信集团对外发布《2024人工智能安全报告》（以下简称《报告》）。《报告》认为，人工智能技术的恶意使用将快速增长，在政治安全、网络安全、物理安全和军事安全等方面构成严重威胁，唤醒行业对AI安全隐患的重视。

3月

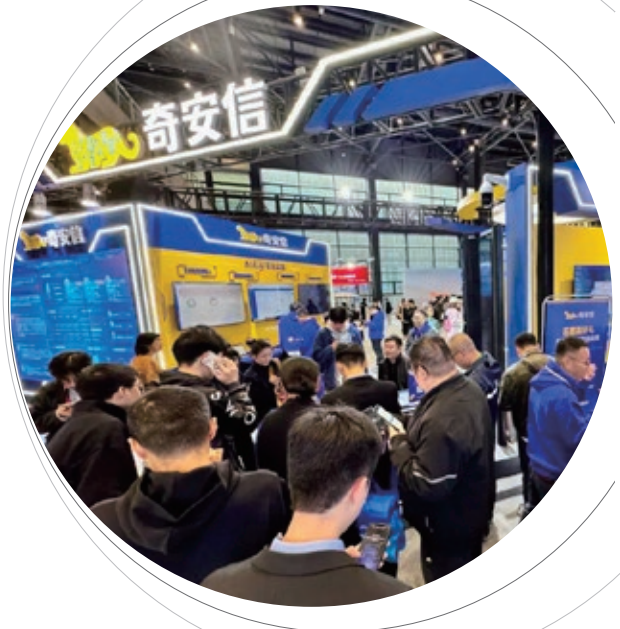
在全国两会上，全国政协委员、全国工商联副主席、奇安信董事长齐向东提交了《创新发展“AI+安全” 护航中国式现代化》提案，力促“人工智能+安全”创新应用探索。同期，新版QAX-GPT安全机器人在春季新品发布会面向全行业发售，其凭借智能优势，为企业网络安全防护筑牢新壁垒，是奇安信AI安全产品化的关键成果。

6月

以“AI 驱动安全”为主题的北京网络安全大会（BCS2024）盛大启幕。多国专家，学者与业界代表齐聚北京。奇安信集团董事长齐向东提出“AI 驱动安全”三大必备要素：优质训练数据、纵深防御体系及统一标准，并无私分享奇安信实践经验，推动全行业在 AI 安全领域的深度思考与进步。

7月

奇安信 AISOC、奇安信 AI 代码助手发布。AISOC 将奇安信 NGSOC 与 QAX-GPT 安全机器人进行深度融合，以安全大模型和大数据关联引擎双擎驱动，将 AI 能力嵌入到研判、调查、响应、报告、狩猎、策略创建等安全运营工作中，实现了运营效率的十倍、百倍、千倍提升；奇安信 AI 代码助手基于安全代码大模型，兼具软件开发高手和安全专家的知识和经验，成为软件开发人员的编程提效工具，提供高质量的安全编码建议，实现效率与安全兼顾。



11月

奇安信集团 AI 驱动安全系列产品首次在 2024 年世界互联网大会“互联网之光”博览会亮相。其中包括 QAX-GPT 安全机器人，以及 AI 赋能下的 AISOC，NDR（天眼）、EDR（天擎）、服务器安全（椒图）等产品，全部融入 QAX AI 安全大模型能力，且能分工协作、高效研判，自动化完成安全事件闭环处置。奇安信 AISOC 荣膺 “新光产品奖”。

深伪技术、鱼叉式钓鱼……解析 2024 年网络安全十大趋势

作者 GoUpSec

2024 年是网络安全行业发生巨变的一年，不仅攻击技术在 AI 的推动下更加复杂化，监管要求也更加严格。以下是对 2024 年呈现的网络安全十大新趋势的全面盘点和解析：

1、AI 编程助手暗藏风险

AI 编码助手的普及为开发流程带来了显著的效率提升，但也带来了不可忽视的风险。一些企业匆忙采用 AI 生成代码工具，但缺乏相应的开发者培训，导致代码缺陷率上升，甚至引发新的安全漏洞。研究显示，在许多情况下，AI 生成的代码在被部署后，其问题解决时间比传统开发流程更长。

AI 编程助手在高度结构化和易于衡量的任务（如静态应用程序安全测试中的漏洞修复）中表现出色，但广泛应用中却存在隐患。这表明，AI 工具的使用应更加谨慎，选择适合其优势的场景，而不是盲目推广。

未来，企业应加强对 AI 技术的监控和评估，确保在享受技术红利的同时，将潜在风险降到最低。

2、新法规推动上市公司安全事件透明化

美国证券交易委员会（SEC）2023 年出台的新规，对上市公司网络安全治理提出了更高要求。这些规定要求企业披露重大网络安全事件，并且必须在发现重大性风险后的四个工作日内提交报告。这一变化显著增加了安全领导者的披露责任。

SEC 的“重大性”定义不仅仅限于财务损失，还包括声誉损害、运营中断等定性风险。这为企业带来了评估难题：何时定义为重大性？如何平衡风险披露与商业秘密保护？

未来，透明化将成为监管环境下的主旋律，企业需构建更加完善的披露机制，同时提升对投资者的保护能力。

3、小型企业加速安全投资

过去，小型企业往往在快速成长

后才会关注网络安全。但如今，许多初创公司在早期阶段便引入虚拟 CISO（vCISO）服务，甚至在完成最小可行产品（MVP）前，便开始设计安全和合规策略。

与中大型企业的合规驱动不同，小型企业正通过安全认证（如 ISO 27001）加强其市场竞争力，以赢得大客户信任。这一趋势表明，网络安全正从“成本中心”转变为“业务助推器”。

对于初创企业而言，早期的安全规划不仅是风险管理的保障，也是未来增长的基石。

> 2024 年是网络安全行业发生巨变的一年，不仅攻击技术在 AI 的推动下更加复杂化，监管要求也更加严格。

4、云计算需要设立信任办公室以应对信任危机

信任危机的爆发。近年来，云服务商的多次重大安全事件（如 Snowflake 和 Okta 的停运事故）导致用户对其信任度大幅下降。传统的安全问卷和责任分摊模式，无法满足客户需求，这进一步放缓了云服务的采纳速度。

一些领先企业开始建立“信任办公室”，以透明的沟通方式重新赢得客户信任。这些办公室直接回应客户对数据安全、隐私和故障恢复的担忧，增强了客户的信心。

未来，随着 AI 和云技术的普及，信任办公室有望成为企业的标准配置，从而在客户关系中占据更加核心的位置。

5、第三方安全审查流程的优化需求

现有安全审查流程存在局限性。例如，供应商安全验证依赖烦琐的问卷和报告（如 SOC 2），但这些方法费时费力且效果有限，无法真正降低第三方供应链中的风险。数据显示，尽管企业花费了大量资源进行验证，第三方和第四方的安全漏洞仍在增加。

AI 工具正在加速问卷处理流程，使供应商能够更快、更准确地完成评估。然而，要彻底变革第三方安全审查流程，仍需要新的解决方案，以便在效率和安全性之间找到平衡。

未来，企业应探索更先进的验证机制，以应对供应链威胁日益复杂化的趋势。

6、针对鱼叉式钓鱼的应对需求增加

钓鱼攻击正变得越来越复杂。2024 年的钓鱼攻击不再是单一模板，而是通过高度定制化邮件，针对不同用户进行精确打击。这种方法不仅提高了攻击成功率，也增加了检测和响应的难度。

为了应对复杂化的钓鱼攻击，企

业需要加强事件响应能力，增加事件响应团队的人员配备，利用更先进的工具对邮件进行实时监控。与此同时，安全意识培训仍是防范此类攻击的关键。

未来，随着攻击者技术的不断提升，企业需要更多创新的检测手段来应对复杂的钓鱼活动。

7、AI 是柄双刃剑

AI 技术快速发展，但其潜在的安全威胁往往难以预料。安全团队需要实时监控 AI 系统的运行状况，以应对突发性风险。

企业必须为员工提供关于 AI 安全风险的教育，同时保持技术敏捷性，优化 AI 的正面效应，抵御可能的威胁。

未来，AI 技术将进一步渗透安全领域，但企业需要警惕其可能引发的系统性风险。

8、深伪技术成为新兴威胁

生成式 AI 推动了深伪技术的发展，这为身份伪造和欺诈提供了新的工具。攻击者利用逼真的假视频和语音进行诈骗，甚至可能在企业内部制造混乱。

安全团队需要通过 AI 和机器学习技术检测深伪内容，同时加强员工意识培训，帮助他们识别潜在的攻击，技术对抗与意识培训双管齐下。

未来，深伪技术的应用场景将更加广泛，安全团队需未雨绸缪，以应对其可能带来的重大威胁。

9、第三方威胁的复杂化与分散化

随着企业逐渐采用多云和 SaaS 架构，传统的边界防护策略已无法适应新环境中的风险管理需求。身份验证与访问控制成为现代安全管理的核心。

新的风险管理模式要求企业构建基于身份和数据的动态安全框架，以应对分布式环境中的复杂威胁。这种转变要求企业在安全策略上更加灵活，确保数据和系统的访问权限始终在控制范围内。

10、AI 与自动化重塑漏洞管理

AI 已经证明能够提升漏洞修复效率。借助 AI 工具，企业能够更快速地进行漏洞分类、优先级排序和分发。与传统的 SOAR 工具相比，AI 解决方案减少了对人工脚本的依赖，使漏洞管理更加高效。

在动态云环境中，海量漏洞的修复对团队资源提出了极高要求。AI 和自动化工具的引入，不仅缓解了资源压力，也显著提高了修复速度和准确性。

关于作者

GoUpSec 以国际化视野服务于网络安全决策者人群，致力于成为国际一流的调研、分析、媒体、智库机构。

从三大角度看 2024 年高校网络安全的发展

作者 杨红波

2024 EDUCAUSE 十大教育议题中，把“将网络安全作为核心竞争力：平衡成本与风险”放在首位。可见，当前网络安全仍然是高校面临的主要风险。

目前国内外各类网络攻击层出不穷，且攻击方式越来越多，网络安全形势越来越严峻。在这样的环境下，2024 年高校网络安全发展趋势可以总结为，人工智能下的数据安全、基础设施下的网络安全、全面监管下的供应链安全这三点。

趋势一：人工智能下的数据安全

人工智能（AI）技术是人类发展的新领域，以 ChatGPT 和 Sora 为代表的生成式人工智能技术带来了通用人工智能（AGI）的曙光。随着 AI 技术的深入应用，也会引发网络安全和数据安全隐患，犹如一个硬币的两面，需要我们关注并找到有效的应对方法。

目前，网络攻击的方式和手段在 AI 技术的推动下正在不断演变，呈现出分布式、智能化和自动化的特点。与此同时，AI 在训练和应用过程中，会处理包含敏感数据在内的大量数据，如用户的个人信息和生物识别数据，这些新颖的技术给网络安全防护带来了新的挑战。

针对人工智能下的数据安全，高校首先要对个人信息的收集和使用加强监管。第一，数据的采集要确保“一数一源”，这样既可以确保数据的一致性，又可以针对数据源加强防护；第二，在数据建设阶段，要遵循数据设计规范，保证数据的保密性、权威性，这样可作为数据源向学校数据中心提供基础数据；第三，在使用数据时，要确保数据必须有合法来源，内部信息要脱敏使用，第三方系统调用时要确保“只使用不存储”的原则。

2023 年 5 月，国家网信办等七部门联合发布了《生成式人工智能服务管理暂行办法》；2023 年 11 月，包括中国、美国与欧盟在内的 28 个国家代表，在全球首届 AI 安全峰会中签署了《布莱切利宣言》，一致同意加强国际合作，建立面向人工智能的监管框架。在这样的背景下，人工智能安全技术正在被全球监管机构、行业参与者和工业界持续关注和积极参与。未来，随着法律法规的逐步完善、公众意识的提高和技术的发展，个人信息保护的力度将持续加强。

趋势二：基础设施下的网络安全

当前，高校普遍都进入了智慧校园发展阶段，在国家政策引导、各部门协同推进下，新型智慧高校建设取得了显著成效，涌现出“一网通办”“OA 办公”“智能教室”等一

> 物联网、移动互联网、虚拟仿真等
> 新技术应用的不断推动带来了新的安全问题，
> 也进一步增加了网络空间和
> 物理空间安全的相互依赖性。

批创新应用。物联网（IoT）、移动互联网、虚拟仿真等新技术应用的不断推动带来了新的安全问题，也进一步增加了网络空间和物理空间安全的相互依赖性。

网络是联接物理设施的纽带，既是智慧校园发展的关键基石，也是支撑学校数字化高效协同、校园服务的载体。服务中断、勒索软件攻击、信息泄露等问题的发生，将对智慧校园的日常运营造成巨大的损失。随着网络安全监管理念的创新和监管手段的进步，应统筹推进安全风险分析、协同监管机制、智能监管技术和安全应急处置等方面建设，为智慧校园发展保驾护航。

趋势三：全面监管下的供应链安全

信息技术的蓬勃发展离不开高新企业的力量，高校网络产品和服务的供应链已演变为复杂的组成结构。供应链安全问题已不仅限于产品范畴，而是波及整个供应链的各个环节。如今，供应链安全威胁和风险攻击日益凸显。比如，某关键软件产品被曝高危漏洞，其带来的影响是巨大的，很大程度上会涉及多个高校或多个业务系统。在攻防演练过程中，红队就研究 VPN 或者 OA 系统的漏洞，一旦得到 PoC，便会波及多所高校。这时，产品在高校的通用性决定了其影响范围，其显著的特点就是“一点多面”，后果可想而知。所以，高校在供应链安全方面要严格把关，系统实施必须经过专家论证，系统上线必须经过源代码检查和安全检测，并经过一段时间的试运行，组织验收后才能正式上线。

高校业务系统数量较多，网络安全防护工作任重而道远。目前，北京外国语大学设有信息化建设与管理办公室，统筹学校信息化建设和网络安全管理工作，通过管理加技术多方位的手段，严格把关，对学校信息化系统掌握主动权，形成信息化系统资产台账，形成全生命周期的监管体系，形成高校环境下的网络安全防护体系。

此外，网络安全制度体系化、网络安全责任制同样发挥着非常重要的作用。高校加强网络安全责任体制落实、各部门主管责任落实、技术部门运维工作落实，外加高新公司的专业产品和安全服务，是目前网络安全工作运行与年度考核的机制。随着相关法律法规的制定和施行，高校未来的整体防护能力将会越来越强。

关于作者

杨红波

高级工程师，北京外国语大学信息技术中心主任。担任中国高等教育学会教育信息化分会监事、中国计算机用户协会网络应用分会常务理事、中国教育技术协会外语专业委员会常务理事、北京市高等教育学会教育信息技术研究分会副理事长等职务。

医疗保健网络安全：2024 年艰难，2025 年可能会更好

作者 Paul Shread

2024 年对于医疗保健网络安全来说是艰难的一年，但进入 2025 年，有一些充满希望的迹象，有效地控制和新规则即将到来。根据 2024 年医疗保健网络安全趋势，医疗保健网络防御受到前所未有的攻击，勒索软件和其他网络攻击危及患者安全和隐私的事件屡次抢占新闻头条。

Change Healthcare、Ascension 和 NHS London 是 2024 年最大的受害者之一，但数百家较小的医疗保健组织也遭受了损失，并且可能还有其他从未得到证实的攻击。

我们将回顾医疗保健网络安全的一年，包括一些好消息，以及 2025 年可能会发生什么。

2024 年全球针对医院的勒索软件攻击趋势

四年前，勒索软件组织承诺在 COVID-19 大流行期间不会攻击医疗保健基础设施。

时代已经发生了变化。2024 年，医疗保健勒索软件攻击的数量和严重性都有所增加，以下是今年一些最大的医疗保健网络攻击事件：

Change Healthcare 在 2 月份被勒索软件攻击，导致超过 1 亿美国人的保险和医疗保健记录被盗。此次泄露归因于传统服务器上缺乏多因素身份验证（MFA），最终可能使母公司 UnitedHealth Group 损失近 30 亿美元，并将网络安全推上了著名的美国医学会杂志（JAMA）的页面。Change Healthcare 在攻击后至少支付了一笔赎金，这并没有阻止数据泄露，同时增加了医疗保健行业作为网络犯罪分子目标的吸引力。

同样在 2 月，全球制药解决方案提供商 Cencora 数据泄露，影响了包括强生在内的十几家制药公司。

Ascension Healthcare 是另一个主要目标，其在 5 月份遭到的勒索软件攻击，导致该公司监管的 140 家医院中的一些医院出现混乱和中断。此次泄露事件表明，对医院的勒索软件攻击有多么危险，据报道，此次事件导致了患者护理的失误。

6 月，NHS London 医院成为医疗保健系统准备不足以应对勒索软件攻击的一个案例研究。这次特别的事件起因于对实验室服务提供商 Synnovis 的一次勒索软件攻击，该攻击导致了依赖 Synnovis 进行的血液检测服务

> 医疗保健行业的网络安全状况可能正在改善。人工智能和自动化技术的应用，可为解决数据泄露事件平均节省 220 万美元。

大幅下降了 96%。

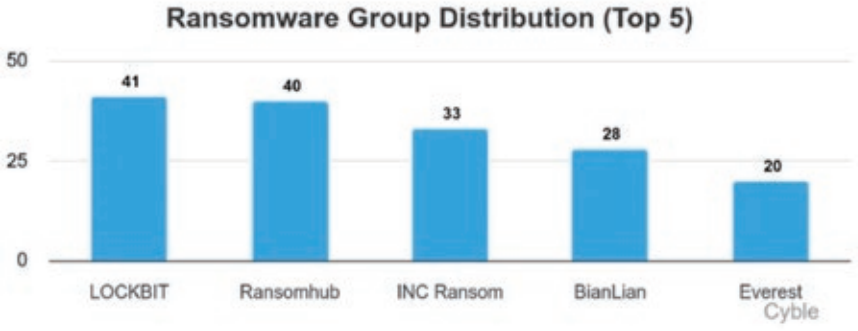
美国是医疗保健勒索软件攻击的主要目标

总体而言，美国仍然是网络攻击的最大目标，医疗保健也不例外。截至 12 月初，人工智能网络威胁情报公司 Cyble 研究人员记录的 339 次医疗保健勒索软件攻击中，有 251 次攻击了美国组织。

与 2023 年同期相比，2024 年前 11 个月，全球针对医疗保健组织的勒索软件攻击增加了 27%。在今年还剩几周的时间里，针对制药和生物技术行业的另外 62 次攻击使全球与医疗保健相关的勒索软件攻击总数超过 400 次。

或者换句话说，到 2024 年，医疗保健勒索软件攻击以每天超过 1 次的速度发生。

今年，针对美国医疗保健组织的勒索软件攻击增长了 36%。在这众多攻击中，一个常被忽视的问题是医疗设备的安全挑战。这些安全挑战增加了医疗保健行业面对网络犯罪分子时的脆弱性，从而使得这个行业成为了更加吸引网络犯罪分子的目标。

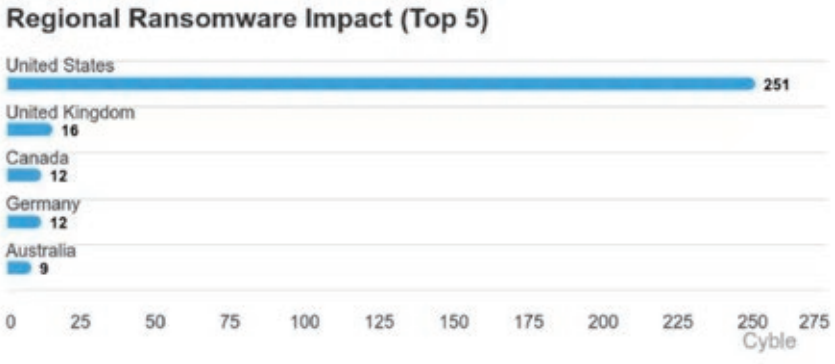


但最大的“赢家”是英国，在 2023 年只发生了两次医疗保健勒索软件攻击，今年已经遭受了 16 次攻击，增加了 700%。

加拿大、德国和澳大利亚位列前五（见下图）。

LockBit 是 2024 年打击医疗保健行业的头号勒索软件组织，但在执法行动中，该组织的活动有所下降，而 RansomHub 可能会在年底前占据榜首。INC、BianLian 和 Everest 位列前五（见上图）。

总体而言，在 Cyble 跟踪的 20 多个行业中，医疗保健是勒索软件组织最常针对的第三大行业，前两位分别是专业服务和建筑行业。



暗网上的医疗保健网络安全漏洞

另一个显示医疗保健网络安全事件急剧增加的证据是，暗网上出售的数据和凭证在增加。

Cyble 研究人员在暗网上记录了 181 起威胁行为者和网络犯罪分子的可信医疗保健索赔，另有 36 起针对制药和生物技术组织的索赔。这已经比 Cyble 在 2023 年全年在这两个领域记录的 140 起暗网索赔高出 50% 以上。

随着医疗保健组织对云基础设施依赖地不断增加，云安全已成为保护敏感数据和防止平台漏洞的关键焦点。在这一背景下，暗网监控变得尤为重要，因为云环境往往是网络犯罪分子试图利用漏洞的主要目标。

根据 IBM-Ponemon 的报告，暗网监控对于医疗保健公司而言是一

种重要的实践方法。它不仅能够加速检测到数据泄露事件，更重要的是，还能及时发现用户名和密码等登录凭据何时被泄漏到暗网。这类凭据往往是构成数据泄露中最常见的初始攻击的媒介。

好消息：医疗保健数据泄露的成本下降

一个好消息是，年度 IBM-Ponemon 数据泄露成本报告发现，今年医疗保健数据泄露的平均成本下降了 100 多万美元，从每次事件的 1093 万美元下降到 977 万美元。然而，这仍然是数据泄露平均成本的两倍，比排名第二的金融服务行业高出 60%，因为医疗保健行业独特的网络安全和数据保护挑战，使事件响应和清理变得极其困难。

积极的迹象是，医疗保健行业的网络安全状况可能正在改善。根据报告，人工智能和自动化技术的应用显示出独特的好处——这些技术可为解决数据泄露事件平均节省220万美元。

此外，还有其他几个积极的因素值得注意。首先，越来越多的数据泄露是由内部工具和团队首次检测到的，而不是通过第三方或攻击者得知，这标志着组织自身安全能力的增强。其次，在勒索软件攻击事件中引入执法部门进行处理，每次事件能够节省接近 100 万美元的成本。

最能降低泄露成本的安全工具是:

员工培训

AI 和机器学习驱动的见解

SIEM 系统

事件响应规划

加密

威胁情报

在这些工具中，加密与医疗保健行业特别相关，因为 98% 的医疗物联网设备流量是未加密的。

可以做些什么来改善医疗保健网络安全?

在美国，即将上任的唐纳德 · 特朗普（Donald J. Trump）政府预计会持有反监管的态度，但在医疗保健网络安全领域，民主党人和共和党人之间可能找到共识。近年来，两党在改善医疗保健网络安全方面提出了多项法案，最近一次提案是在上个月。尽管本届国会采取行动的时间已晚，但随着第 119 届国会将于 1 月开始工作，这预示着下一届国会在医疗保健网络安全方面，可能会取得一些进展。

为应对医疗保健网络安全的挑战，采用零信任架构是一种有潜力的方法。零信任原则强调“永不信任，始终验证”，这一理念在网络边界变得模糊不清的环境中特别有效，如医疗保健行业。通过实施零信任，该行业可以大大提升其防御能力。

此外，全球各地也在推进关键基础设施的安全措施。如英国、欧盟的 NIS2 指令、澳大利亚的网络安全法案等都在积极发展之中。这些动向表明，2025 年可能是全球关键基础设施安全状况显著改善的一个转折点。安

关于作者

Paul Shread

拥有 25 年的 IT 新闻工作经验，现任 The Cyber Express 和 Cyble 的国际编辑。他聚焦企业技术领域，撰写了关于端点安全和虚拟数据中心的获奖文章，并揭露了主要 SIEM 系统中的关键安全漏洞。

奇安信

新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结

从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

网安26号院 SECURITY INSIDER

征稿启事

当下，网络空间态势日趋严峻，关基设施成为重要攻击目标，因网络攻击导致的系统瘫痪、数据泄露现象频发。网络安全建设和运营需时刻因应形势变化进行创新。分享行业趋势、交流建设与运营之道成为提升安全防护水平的重要途径。

为此，奇安信《网安 26 号院》联合虎符智库、安全内参联合征稿。具体要求如下：

一、征稿对象：

投稿人为政企网络安全负责人、从业者，以及研究人员。

二、征稿时间：

本次活动活动长期有效。

三、征稿要求：

投稿论文应为投稿人原创，且尚未被任何期刊接受或发表。投稿人应对所投稿件的著作权及其他法律责任负责。

四、稿件说明：

来稿主题包括但不限于网络安全合规解读、网络攻防态势分析、网络安全建设经验、安全运营最佳实践，创新安全技术及应用等网络安全领域相关的议题。

稿件字数（含注释）原则上应控制在 4000 ~ 8000 字。

五、评选及奖励：

来稿经专家组评审入选刊登后，即获得相应的稿费（不低于 2000 元人民币）。

优秀获奖作者将有机会受邀参加 “BCS 北京网络安全大会”，发表主题演讲并分享研究心得。

六、其他荣誉：

长期供稿作者可以获聘“虎符智库”专家，授予聘书和徽章。

七、投稿方式：

投稿以附件形式通过电子邮件
发送至 lijianping@qianxin.com;
或者微信添加 security4 咨询联系。

扫码咨询

奇安信连续四年位居
“中国网安产业竞争力50强”
第一名

9月6日，中国网络安全产业联盟（CCIA）
公布“2024年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续四年高居榜单第一名。

“2024年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	启明星辰信息技术集团股份有限公司
3	深信服科技股份有限公司
4	华为技术有限公司
5	天融信科技集团股份有限公司
6	新华三信息安全技术有限公司
7	杭州安恒信息技术股份有限公司
8	亚信安全科技股份有限公司
9	绿盟科技集团股份有限公司
10	三六零安全科技股份有限公司
11	天翼安全科技有限公司
12	中电科网络安全科技股份有限公司
13	杭州迪普科技股份有限公司
14	北京山石网科信息技术有限公司
15	中孚信息股份有限公司