深信服智安全
SANGFOR SECURITY

2025 年 Q2 网络威胁与情报跟踪

深信服科技股份有限公司

2025 年 5 月 21 日

说明

本通告涵盖 2025 年 4-5 月深信服团队发现或追踪的全球网络安全事件，以期达到及时分享网络安全现状及最新网络安全热点事件的目的，欢迎业内人士讨论指正。文档内引用了部分互联网已公开的数据信息，已在文档里标明出处。

深信服千里目安全技术中心公众号二维码

目录

一、2025 年第二季度典型安全事件

（一）科研与教育行业

澳大利亚西悉尼大学单点登录系统被攻破

2025 年 4 月，攻击者利用身份验证漏洞入侵西悉尼大学的单点登录（SSO）系统，导致约 1 万名师生的个人信息（包括人口统计、注册信息、学业进展数据）被非法访问。部分受影响成员的个人信息随后在暗网上被泄露，造成严重隐私风险。该事件暴露出教育行业在身份管理和数据保护方面的薄弱。

勒索软件攻击频发，教育行业成为高风险目标

2024 年至 2025 年，勒索软件对教育机构的攻击同比增长 35%，攻击手法从传统加密勒索转向数据窃取勒索，攻击团伙如 Hive（后更名 Hunters International）针对教育领域勒索金额累计超过 1 亿美元。此外，攻击者还利用教育机构预算有限、数据量大且安全防护不足的特点，频繁发动钓鱼、恶意软件和 DDoS 攻击。

（二）企业领域

Marks and Spencer 遭受大规模网络攻击

2025 年 4 月，英国跨国零售商 Marks and Spencer（M&S）在复活节长假期间遭遇严重网络攻击，导致其线上交易系统和礼品卡处理服务瘫痪。为应对此次安全事件，M&S 暂停了官网及 APP 的接单功能，但产品页面仍可浏览，实体店

照常营业。此次攻击影响了非接触支付等关键服务，给客户购物体验带来较大不便。公司已公开致歉，并紧急求助第三方网络安全专家进行取证和恢复。攻击疑似为勒索软件所为，攻击者可能先通过钓鱼邮件等手段入侵网络，随后加密关键系统，造成业务中断。此次事件暴露出零售行业对线上服务依赖高且安全防护仍有不足的风险。

邮件营销服务商 Mailchimp、SendGrid 和 HubSpot 遭遇网络钓鱼攻击

2025 年 4 月，多个知名邮件营销平台如 Mailchimp、SendGrid 和 HubSpot 遭受大规模网络钓鱼攻击。攻击者通过伪造合法邮件，诱导企业用户点击恶意链接，窃取账户凭证后进一步渗透企业内部网络，导致数据泄露和业务中断。此次攻击反映出钓鱼攻击依旧是企业初始访问的主要手段，且针对企业邮箱的攻击频率和成功率持续上升，给企业信息安全带来严峻挑战。

Hitachi Vantara 遭 Akira 勒索软件攻击

2025 年 4 月 26 日，日本日立集团旗下的 Hitachi Vantara 遭遇 Akira 勒索软件攻击，导致部分服务器被加密，数据访问受限。为遏制事件扩散，公司主动将服务器下线，限制数据中心的进出流量，并聘请第三方安全专家协助调查和修复。此次攻击影响了包括政府项目在内的多个客户系统，远程运维和支持服务暂时中断。Akira 勒索软件以高效渗透和数据窃取著称，攻击者通过钓鱼等手段入侵网络，随后加密文件并索要赎金。该勒索团伙自 2023 年起活跃，已针对全球多家大型企业实施攻击，2025 年勒索总额预计达数亿美元。

租车巨头 Hertz 披露大规模数据泄露事件

2025 年 4 月 2 日，Hertz 全球控股公司披露一起涉及供应商平台的重大数据泄露事件。未经授权的数据访问始于 2024 年末，攻击者利用供应商 Cleo Communications US，LLC 系统中的零日漏洞入侵。此次泄露可能暴露客户姓名、联系方式、出生日期、信用卡信息、驾驶执照及护照信息等敏感数据。Hertz 已向执法部门和监管机构报告事件，并为受影响客户提供两年免费身份监控和暗网监控服务。虽然尚未发现数据滥用，但公司敦促客户密切监控信用报告和账户活动。此事件引发投资者担忧，导致公司股价盘后下跌 2.5%，凸显数据泄露对企业声誉和财务的潜在冲击。

（三）能源行业

全球能源企业遭遇针对性网络攻击激增

能源行业正面临日益严峻的网络威胁。2025 年 4 月，Resecurity 发出警告，针对能源企业的网络攻击不断增多，部分攻击背后是旨在影响国家基础设施的大规模活动，未来或成新型战争手段，美国能源部已发布相关指南应对。黑客行动主义、与多国相关的国家间谍行为也构成威胁，地缘政治因素是主要诱因。此外，技术变革如云技术促使 IT 与 OT 网络融合，以及 AI 的应用，都增加了网络攻击风险，给能源行业带来新挑战。

（四）金融与银行（含加密货币）

约旦科威特银行遭 Everest 勒索软件攻击

2025 年 4 月，约旦科威特银行（Jordan Kuwait Bank）成为 Everest 勒索软件的攻击目标。攻击者成功窃取了高达 11.7GB 的敏感数据，其中涵盖大量客

户信息及重要业务数据，这一事件不仅给银行的正常运营带来了巨大风险，还严重威胁到客户的隐私安全。一旦数据泄露，客户可能面临诸如身份信息被盗用、账户资金面临风险等问题，而银行也将面临客户信任危机、监管处罚以及潜在的法律诉讼等一系列严重后果。

Everest 勒索软件在网络犯罪领域较为活跃，其通常采用复杂的攻击手段，通过漏洞利用、钓鱼邮件等方式入侵目标系统，进而加密数据并窃取敏感信息，以向受害者勒索高额赎金。此次针对约旦科威特银行的攻击，再次凸显了金融机构在网络安全防护方面面临的严峻挑战。

Web3.0 领域加密货币安全事件频发

CertiK 于 4 月 2 日发布的《Hack3D 报告》显示，2025 年第一季度 Web3.0 领域的加密货币安全形势异常严峻。该季度共发生了 197 起安全攻击事件，黑客盗取金额约达 16.7 亿美元，与上一季度相比，增长幅度高达 303.4%。如此大规模的资金损失，给加密货币市场带来了极大的冲击。 其中，Bybit 交易所遭遇的安全事件最为引人注目，导致了 14.5 亿美元的巨额损失，黑客利用了 Bybit 交易所智能合约中的漏洞，篡改交易签名逻辑，成功从离线存储的冷钱包中转移资产，暴露了中心化交易所技术架构中存在的致命缺陷。

除了交易所遭受攻击外，私钥泄露事件在本季度也发生了 15 起，造成的损失达 1.4 亿美元。攻击者通过深度伪造、恶意浏览器扩展、合约操纵等多样化且复杂的手段，不断突破现有的安全防线，给投资者和整个加密货币生态系统带来了严重的安全隐患。

传统银行面临合规与安全投入双重挑战

金融监管部门不断加强对银行的监管力度。中国人民银行正式发布《中国人民银行业务领域数据安全管理办法》，自 2025 年 6 月 30 日起施行。该《办法》旨在规范金融业务领域数据全生命周期安全管理，平衡数据开发利用与风险防控，覆盖货币信贷、支付清算、征信、反洗钱等十大央行监管业务领域。银行需要投入大量的人力、物力和财力来确保自身业务符合这些法规要求，否则将面临严厉的处罚。

在安全防护方面，传统银行由于业务规模庞大、系统复杂，机构越大攻击面越广，成为了黑客攻击的重点目标。攻击者常常利用复杂的社会工程学手段以及系统技术漏洞，频繁对银行进行渗透攻击。与传统银行相比，DeFi（去中心化金融）领域的智能合约漏洞和闪电贷攻击导致的损失更为巨大。例如，去中心化的永续期货交易所 KiloEx 在 2025 年 4 月 15 日被攻击，损失约 740 万美元，原因在于其顶层合约缺乏访问控制检查，导致预言机价格被操控。

（五）其他

非洲 MTN 集团数据泄露：MTN 集团是非洲最大移动网络运营商，在 4 月披露数据泄露事件，部分用户个人信息被暴露，但核心网络、计费及金融服务基础设施未受影响。该集团在非洲和中东 18 国服务超 2.9 亿用户，在约翰内斯堡证券交易所上市，服务收入超 110 亿美元。

印巴网络战升级：5 月，印巴在网络安全领域攻防频发。5 月 5 日，巴基斯坦支持的 “Pakistan Cyber Force” 黑客组织入侵印度军事工程服务和马诺哈尔·帕里卡尔国防研究与分析研究所，篡改装甲车辆有限公司网站；4 月 29

日，“IOK Hacker”或“Internet of Khilafah”攻击四个印度国防相关设施，包括网站篡改、DDoS 攻击和窃取个人信息；还有组织试图篡改印度陆军公共学校网站。印度采取实时检测阻断、网站下线审计、加强防御及反击等措施，印度黑客组织声称入侵巴基斯坦部分机构数据库。

迪奥客户信息外泄：5 月 12 日晚，迪奥向中国客户发短信称，5 月 7 日发现未经授权外部人员获取部分客户数据，包括姓名、性别、手机号码、电子邮箱、邮寄地址、消费金额和偏好等。初步调查因数据库遭未经授权访问，迪奥已采取措施避免事态扩大，在专家协助下调查应对并报备监管部门。

65 款 APP 违法违规收集使用个人信息被通报：截至 5 月 13 日，国家网络与信息安全信息通报中心通报 65 款移动应用存在违法违规收集使用个人信息问题。部分应用首次运行时未以明显提示让用户阅读隐私政策，甚至默认选择同意；隐私政策未详细列出收集使用信息的目的、方式和范围；处理信息时未提供有效更正、删除功能，影响用户知情权、选择权及权益。通报旨在提醒用户并督促企业遵守相关法律法规。

二、MITRE ATT&CK 分析与行业趋势总结

（一）科学研究与教育行业

主要攻击技术

- 初始访问：钓鱼邮件、凭证填充、SSO 系统漏洞利用
- 执行与持久化：恶意软件、后门植入
- 数据收集与泄露：数据库窃取、文件打包

- 防御规避：禁用安全工具、加密通信

趋势

教育机构由于预算限制和数据敏感性，成为勒索软件和数据窃取的高频目标。攻击者利用 AI 驱动的社会工程学手段提高钓鱼成功率，攻击速度加快，数据泄露事件频发。

（二）企业领域

主要攻击技术

- 初始访问：钓鱼、供应链攻击
- 横向移动：利用 RDP、SMB 协议渗透
- 权限提升：漏洞利用、凭证窃取
- 影响：勒索软件加密、业务中断

趋势

企业面临多管齐下的攻击，攻击速度和复杂度显著提升。勒索软件从加密转向数据窃取勒索，攻击者以业务中断和声誉损害为主要勒索手段。AI 辅助攻击和云环境漏洞成为新兴风险点。

（三）能源行业

主要攻击技术

- 初始访问：钓鱼、供应链攻击

- 横向移动：IT-OT 融合漏洞利用、RDP
- 权限提升：系统漏洞利用
- 影响：数据泄露、物理破坏威胁

趋势

国家级黑客和黑客主义者频繁针对能源基础设施发动攻击，IT 与 OT 系统融合带来横向移动风险。AI 和 IIoT 设备的普及扩大了攻击面，云计算环境安全成为重点防护对象。

（四）金融与银行（含加密货币）

主要攻击技术

- 初始访问：钓鱼、暴力破解、智能合约漏洞利用
- 执行：恶意代码执行、闪电贷攻击
- 数据收集与泄露：私钥窃取、数据库访问
- 影响：勒索软件加密、资金盗窃

趋势

传统银行加强合规和安全投入，但攻击面随机构规模扩大而增加。DeFi 领域频发智能合约漏洞、闪电贷攻击和预言机操纵，传统安全框架难以完全适用。AI 辅助威胁检测和强制安全审计成为行业发展方向。

三、综合趋势分析

勒索软件攻击持续演进

勒索软件攻击在近年来经历了极为显著的演变，勒索软件从加密转向数据窃取勒索，攻击者以业务中断和声誉损害为主要勒索手段。攻击团伙为了最大化利益并向受害者施加全方位压力，开始采用多重勒索策略，在加密数据前，会先精心窃取大量敏感数据。部分攻击团伙还会威胁发动 DDoS 攻击，使受害者的网络服务陷入瘫痪，严重影响其正常业务运营。

数据泄露事件频发且影响深远

数据泄露事件正以前所未有的频率发生，大量用户的姓名、地址、电话号码、电子邮箱甚至生物识别信息等被不法分子窃取。企业敏感数据，包括商业机密、研发成果、供应链信息等，也被不同的攻击者所觊觎。这些被窃取的数据大多流向暗网，在那里被公然出售给有需求的买家，形成了一条庞大而隐蔽的数据犯罪产业链。 数据泄露事件频发不仅对个体和企业造成了巨大冲击，也对整个社会的信息安全生态构成了严重威胁。

国家级与黑客主义威胁加剧

在当今复杂的地缘政治格局下，国家级与黑客主义威胁在网络空间中日益加剧，尤其是在能源等关键基础设施领域。国家支持的网络攻击行动愈发频繁，这些攻击往往具有明确的政治、经济或战略目的，成为地缘政治博弈的新工具。关键基础设施，如能源供应系统、交通网络、通信枢纽、金融体系等，因其对国家

经济运行和社会稳定的重要性，成为了首要攻击目标。攻击者通过精心策划的网络攻击，试图破坏这些关键基础设施的正常运行，进而对目标国家的经济、社会秩序造成严重混乱。

IT-OT 融合带来新安全挑战

随着工业数字化转型的加速推进，关键基础设施行业中的 IT（信息技术）与 OT（运营技术）系统融合趋势愈发明显。这一融合虽然带来了生产效率提升、管理优化等诸多益处，但也引入了全新的安全挑战。传统的 IT 系统主要关注信息的处理和存储，而 OT 系统则侧重于对物理设备和生产过程的实时控制。在融合过程中，攻击者可以利用系统间的通信接口和协议漏洞，运用横向移动技术，从 IT 系统突破防线，进而渗透到 OT 系统。

新兴技术风险显著

随着 AI、云计算、IIoT 设备的广泛普及，网络安全领域的攻击面被极大地拓宽，新兴技术带来的风险日益显著。在 AI 领域，一方面攻击者利用 AI 技术辅助攻击，此外还可以被用于自动化漏洞扫描和攻击脚本生成，大大提升了攻击效率和隐蔽性。另一方面，AI 系统自身也面临安全威胁，如模型窃取、对抗样本攻击等，可能导致 AI 决策被恶意操控。

云计算环境中，由于多租户共享资源的特性，若安全隔离措施不到位，攻击者可能通过漏洞突破自身租户边界，访问或篡改其他租户的数据。同时，云服务提供商的安全管理漏洞也可能被攻击者利用，引发大规模的数据泄露事件。IIoT 设备，由于其计算资源有限、安全防护能力相对薄弱，且数量庞大、分布广泛，

成为了攻击者易于下手的目标。攻击者可以通过控制大量 IIoT 设备组建僵尸网络，发动大规模 DDoS 攻击，或者窃取设备采集的敏感数据。

加密货币和 DeFi 安全风险突出

加密货币和 DeFi（去中心化金融）领域近年来发展迅猛，但其安全风险也愈发突出。在加密货币领域，私钥作为用户资产的关键凭证，一旦泄露，用户的加密货币资产将瞬间被盗取。私钥泄露的原因多种多样，可能是用户自身安全意识不足，也可能是钱包软件存在安全漏洞，被攻击者利用。智能合约漏洞也是导致加密货币安全事件频发的重要因素。智能合约在 DeFi 应用中广泛使用，其代码一旦存在漏洞，攻击者就可以通过操纵交易逻辑，窃取用户资金。链上攻击手段层出不穷，如重入攻击、闪电贷攻击等，攻击者利用区块链网络的特性和智能合约的缺陷，在极短时间内获取巨额非法收益。为了有效应对这些风险，需要创新安全策略，如加强智能合约的代码审计、采用多签名钱包技术、建立实时监测和预警机制等，以保障加密货币和 DeFi 生态系统的安全稳定运行。