

暗网报告

2024上半年



目录

TABLE OF CONTENT

| | | |
|-----------|---------------|-----------|
| 01 | 序言 | 03 |
| 02 | 总体数据概览 | 04 |
| | 勒索软件数据 | 04 |
| | 数据泄露数据 | 06 |
| | 黑客攻击数据 | 08 |
| 03 | 典型事件 | 11 |
| | 国内事件 | 11 |
| | 国外事件 | 14 |
| 04 | 半年特点总结 | 19 |

01 POINT

序言

为全面了解暗网威胁态势，确保客户数据和网络的安全，天际友盟将基于自有暗网监测平台持续发布暗网半年报告。该平台的监控范围广泛，覆盖了勒索软件数据泄露站点、暗网交易市场、黑客论坛、海外 Telegram 交易频道等多个渠道。

通过持续的监测工作，天际友盟将跟踪、整理和分析与勒索软件攻击、敏感数据泄露、黑客攻击相关的数据信息。这将有助于我们加强对暗网威胁的防范，并制定相应的对策措施。鉴于暗网威胁的复杂性和严峻性，未来天际友盟将持续提升监测能力和分析技术，并加强与各方合作，共同构建一个更加安全可靠的网络环境，以更好地应对暗网威胁。

02

POINT

总体数据概览

2.1 勒索软件数据

2.1.1 Top10 勒索组织

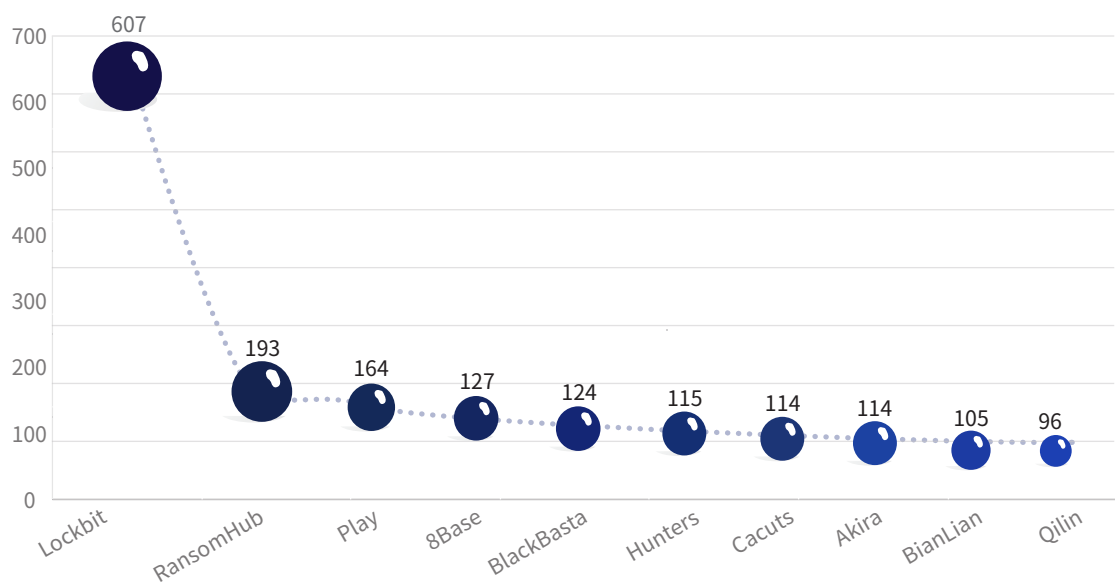


图 1 Top10 勒索组织

从图 1 可以看出，LockBit 依然以 607 名受害者数量远超其它勒索组织，而其它排名有了明显的变动，2024 年 2 月份才出现的勒索组织 Ransomhub 异军突起，排名跃至第二位，成为目前最为热门的勒索团伙之一。Play 和 8Base 勒索软件较 2023 年下半年均有所上升，而 Hunters 和 Qilin 组织则首次挤进前十。

2.1.2 Top10 勒索国家

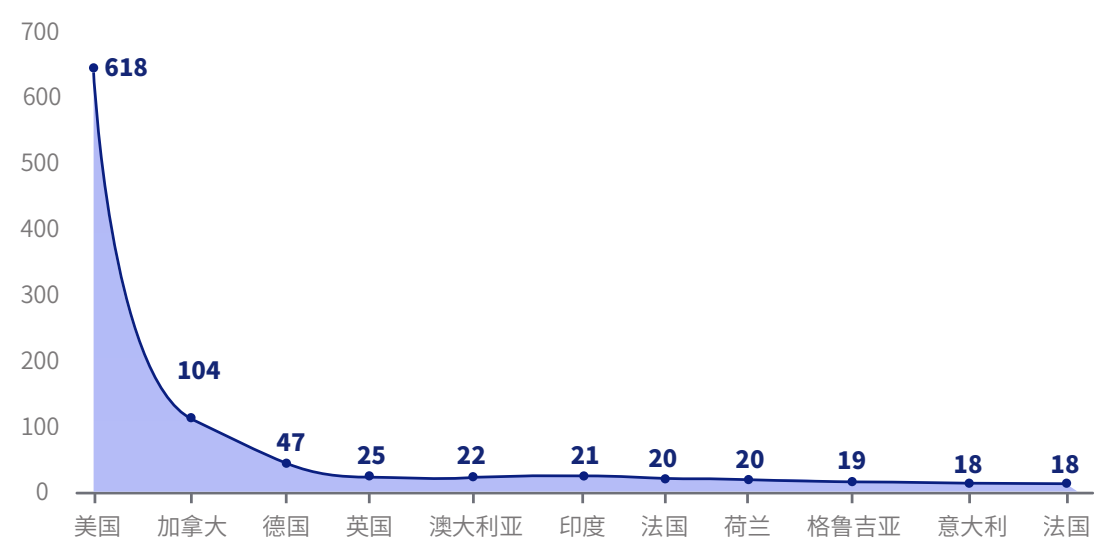


图 2 Top10 勒索国家

根据图 2 可以看出，2024 年上半年，美国成为了遭受勒索软件攻击最为严重的国家，以其惊人的数字遥遥领先。而其他受影响较大的国家包括加拿大、德国、英国、澳大利亚、印度、荷兰、格鲁吉亚、意大利和法国等。这些国家在网络安全领域面临着巨大的威胁和挑战，令人担忧。

2.1.3 Top10 勒索行业

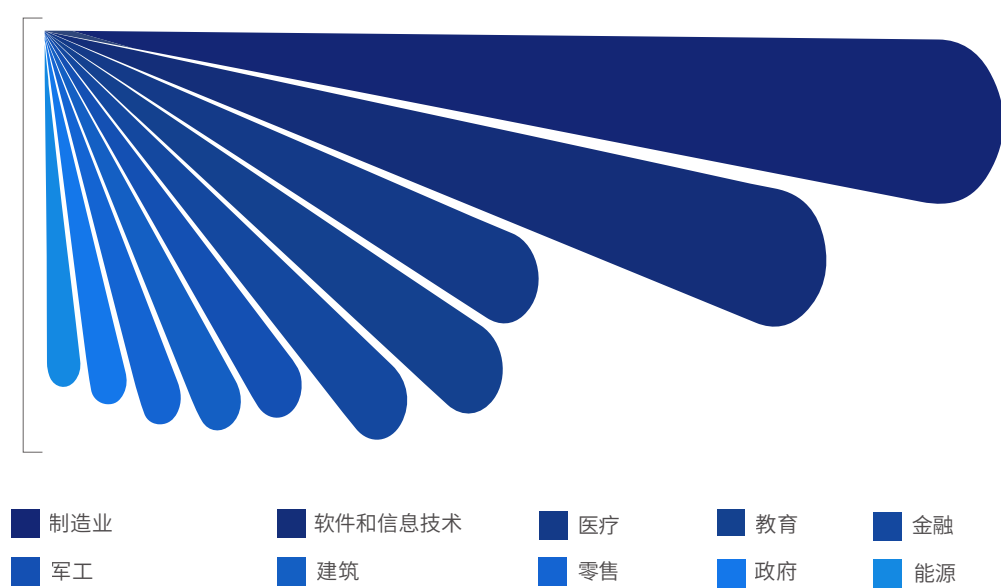


图 3 Top10 勒索行业

根据图 3 的数据显示，2024 上半年，勒索软件攻击广泛分布于多个行业，主要集中在制造、软件信息技术和医疗领域，中小型企业受到的影响显著。同时，教育、军工、金融、建筑、政府、零售和能源等领域也受到较大波及。

2.1.4 Top10 勒索金额

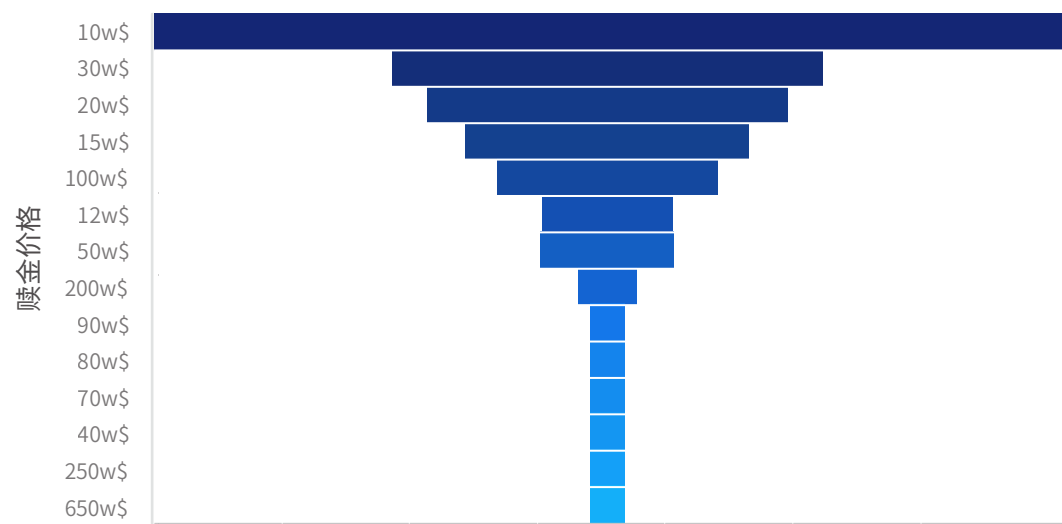


图 4 Top10 勒索金额

图 4 显示，勒索软件团伙在赎金价格的设定上存在较大差异。这种差异主要是因为他们所攻击的目标企业收入水平各不相同。因此，勒索软件团伙会针对每个受害公司的具体情况，设置个性化的赎金价格。根据数据统计，最常见的赎金价格最低为 10 万美元，而最高则可高达 650 万美元。这一数字差异显示了勒索软件团伙在赎金策略上的巧妙和灵活性。

2.2 数据泄露数据

2.2.1 Top10 涉及国家

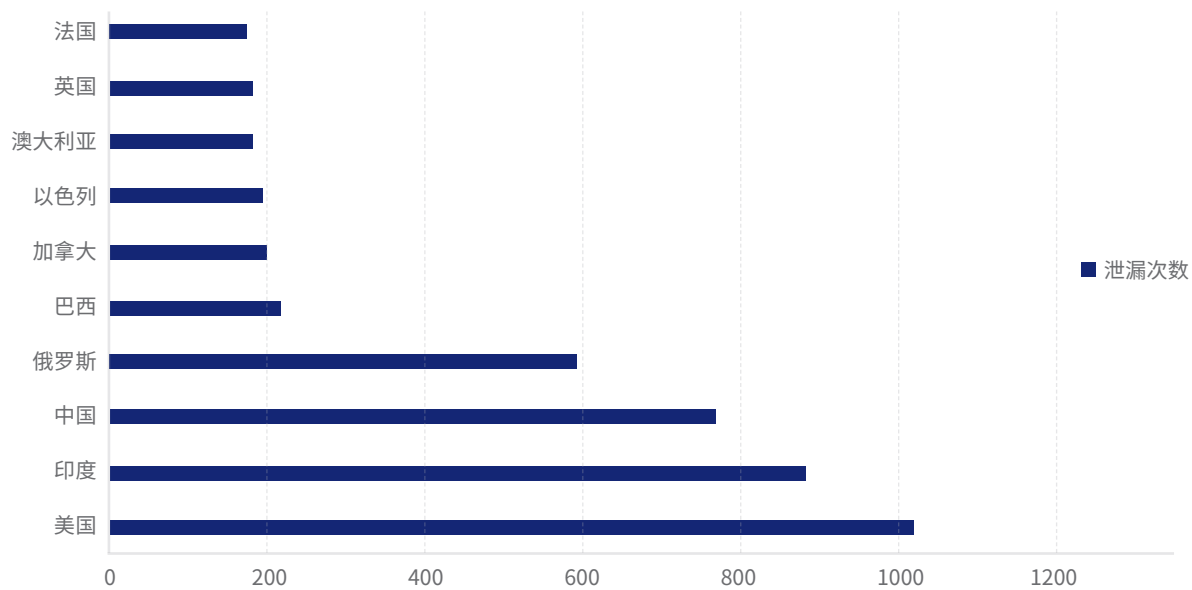


图 5 Top10 涉及国家

图 5 数据显示，美国、印度、中国以及俄罗斯等大国是 2024 年上半年数据泄露问题最为严重的国家。

不仅如此，巴西、加拿大、澳大利亚、英国和法国等地也是数据泄露高发区。这些数据揭示了全球范围内数据泄露问题的严峻形势。大国之间的数据泄露风险引起了广泛关注，因为这些国家拥有庞大的互联网用户群体和复杂的网络基础设施。而其他国家的数据泄露情况，则反映了数据泄露问题的全球化趋势。

2.2.2 Top10 影响行业

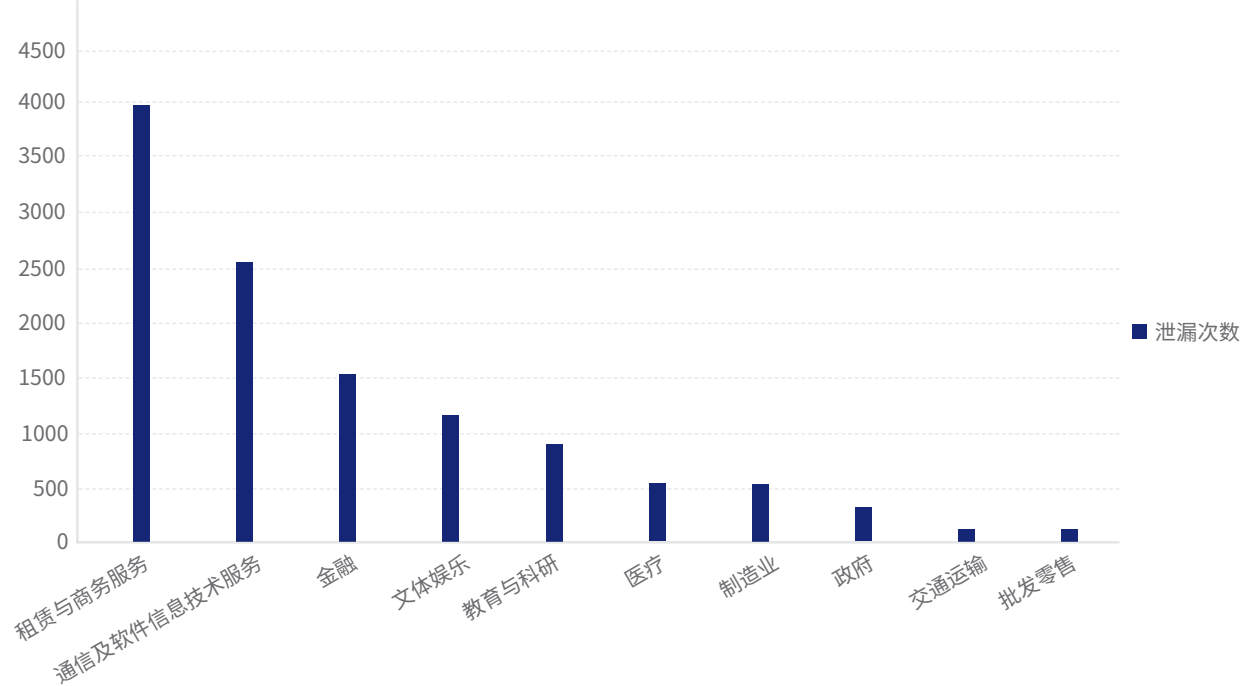


图 6 Top10 影响行业

图 6 数据显示，2024 年上半年，租赁与商务服务、通信及软件信息技术服务以及金融这三个行业所面临的数据泄露风险最为突出。此外，文体娱乐、教育与科研、医疗、制造业、政府、交通运输以及批发零售等行业也在不同程度上存在数据泄露问题。这一数据展示，在信息时代，数据安全已成为各行各业共同面临的重要课题。

2.2.3 Top10 售卖金额



图 7 Top10 售卖金额

根据图 7 的数据可以看出，售卖数据的犯罪分子通常以非常低廉的价格进行交易，最低可以仅为 2 美元，最高也不超过 400 美元。这一数字范围的窄幅差异表明了被售卖的数据多为二次贩卖的低价值数据。这种现象侧面反映了数据市场中低价值数据的普遍存在。低价值数据的特点可能是因为它们已经在黑市上被多次交

易，或者它们的信息已过时或不再具有实用性。然而，不要低估了这些低价值数据所带来的潜在风险。即使数据的价值相对较低，但在犯罪分子手中，仍可能被滥用和利用，给个人和企业带来巨大的损失和风险。

2.3 黑客攻击数据

2.3.1 Top10 黑客组织

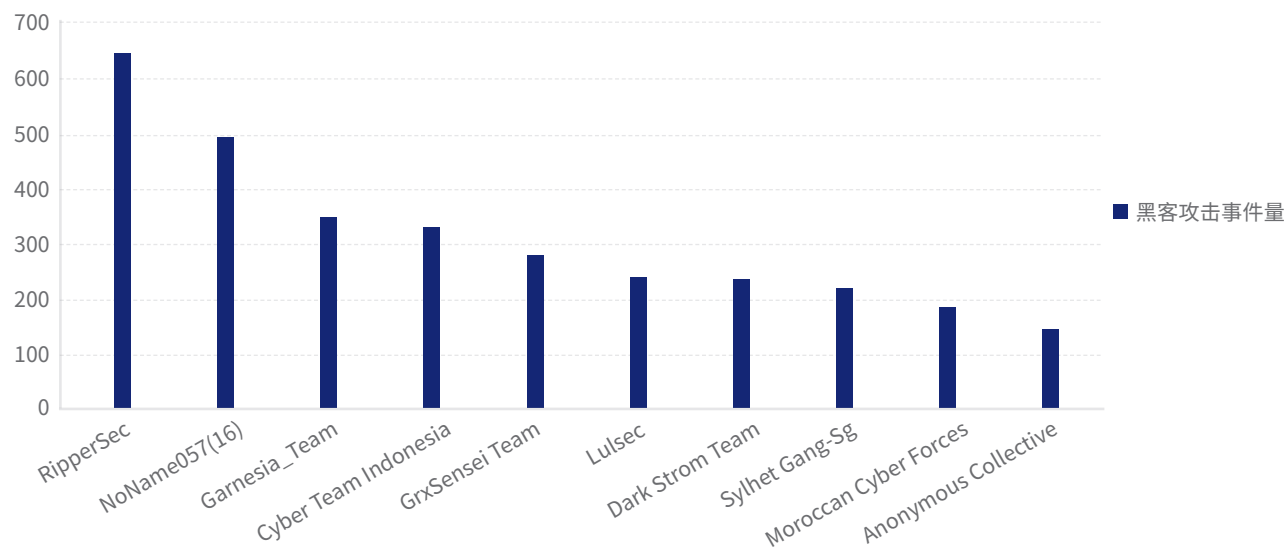


图 8 Top10 黑客组织

图8数据显示,RipperSec在2024年上半年成为了最为活跃的黑客组织,其攻击频率高于其他黑客组织,展现了其在黑客领域的卓越实力。紧随其后的是亲俄黑客组织 NoName057(1), 尽管与前者存在一定的差距,但也表现出了相当的活跃度。除此之外,还有 Garnesia_Team、Cyber Team Indonesia、GrxSensei Team、LulzSec、Dark Strom Team、Sylhet Gang-Sg、Moroccan Cyber Forces 以及 Anonymous Collective 等黑客组织也进入了活跃的 Top10 名单。这些黑客组织的活跃度展示了当前黑客行业的繁荣。

2.3.2 Top10 目标国家

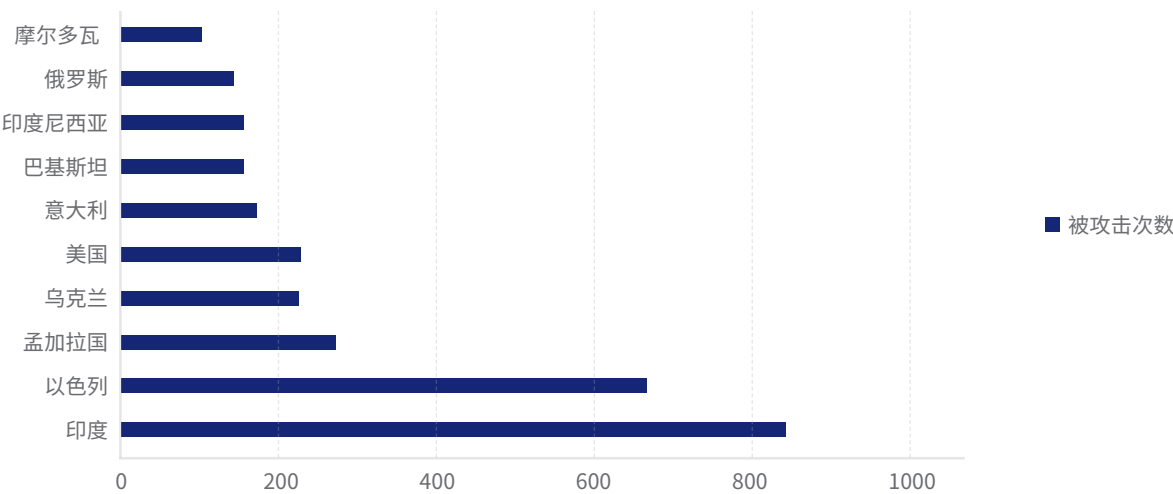


图 9 Top10 目标国家

图 9 数据指出，印度和以色列是遭受黑客攻击最为频繁的目标地区。其他知名国家包括乌克兰、美国、巴基斯坦和俄罗斯等也面临着相当高频率的黑客攻击。这种现象背后的原因是黑客组织往往带有一定的政治色彩。由于当前国际政治的不稳定，地缘冲突频繁爆发，这为许多黑客组织提供了活跃的空间。这些黑客组织通常会选择立场，并以实现特定目标为动机，号召民族主义者或其它民众对关键目标国家进行高频度的报复性攻击。这些黑客攻击不仅仅是简单的数据侵入，还可能对国家安全、经济稳定以及个人隐私造成重大威胁，也可能对当地敏感的政治、军事冲突产生微妙的影响。

2.3.3 Top10 目标行业

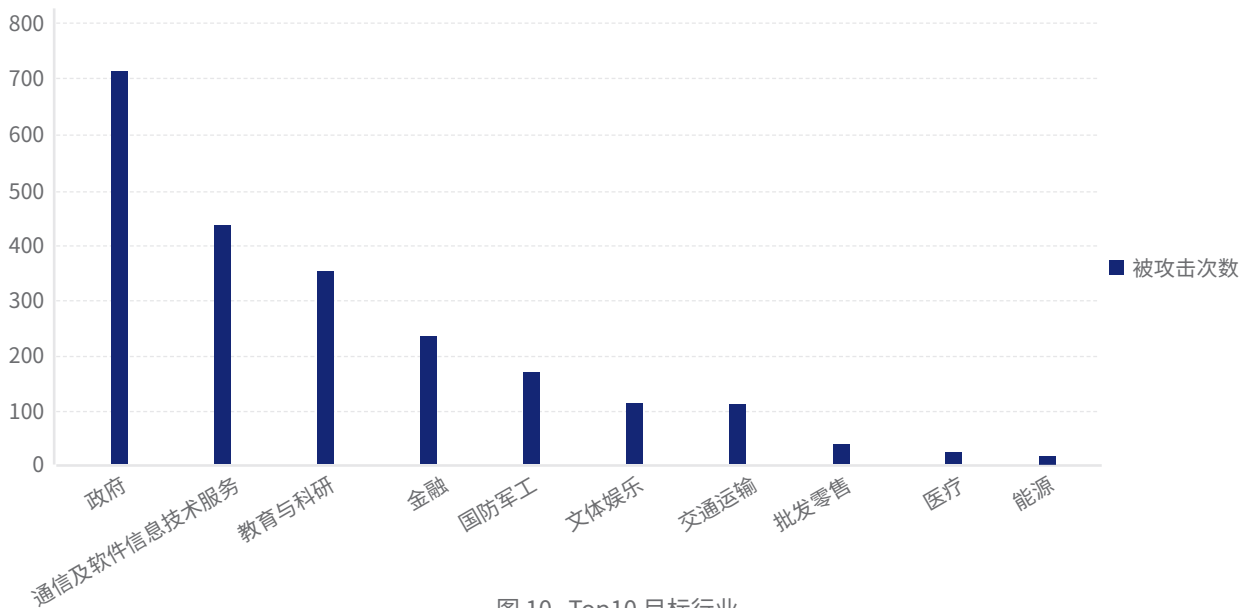


图 10 Top10 目标行业

根据图 10 可以看出，政府、通信及软件信息技术服务、教育与科研等关键行业成为黑客攻击的主要目标。这些行业对一个国家的正常运行至关重要，因此对黑客来说，攻击这些行业能够最有效地实现其警示和破坏的目的。其中，政府部门的被攻击可能影响国家安全和政治稳定；通信及软件信息技术服务行业被攻击可能导致重要信息的泄露和网络服务的中断；教育与科研行业被攻击可能导致知识产权的盗窃和科技创新的受阻。

2.3.4 Top5 攻击手段

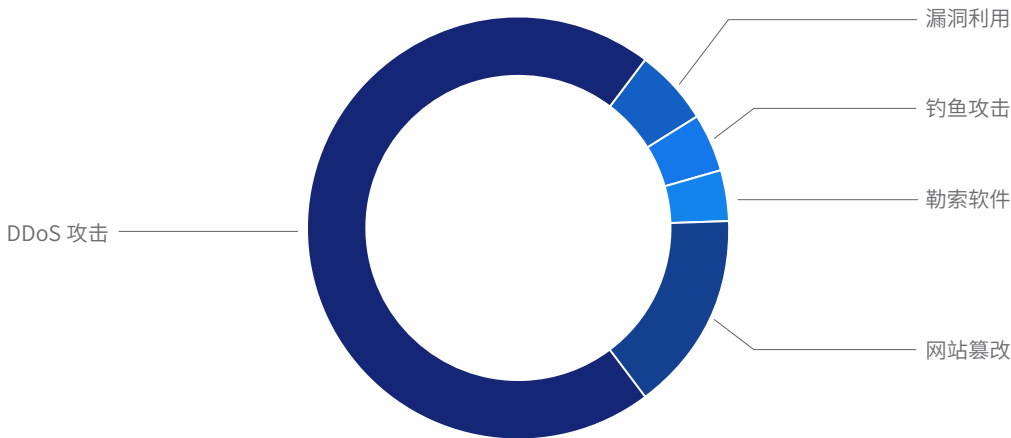


图 11 Top5 攻击手段

根据图 11 的数据显示，黑客组织几乎只使用 DDoS 攻击手段对网站发起攻击，这表明他们的主要目的是通过最容易实现的手段达到恐吓和报复的目的，即让目标网站不能正常提供服务。除了 DDoS 攻击之外，黑客组织还采用了其他手段，如篡改网页、漏洞利用、钓鱼和勒索软件等方式，这些手段旨在破坏网站的完整性、窃取用户信息、迫使受害者支付赎金等。

03

POINT

典型事件

3.1 国内事件

3.1.1 勒索攻击类

| 时间 | 勒索软件 | 影响行业 | 勒索软件 |
|-----------|-------------------------------|-------------|------------|
| 2024/1/19 | Lockbit 对台湾某光学机能材料制造公司发起攻击 | 制造业 | Lockbit |
| 2024/3/5 | LockBit 组织入侵国内某通信公司 | 通信及软件信息技术服务 | Lockbit |
| 2024/4/15 | 中国某纸业公司遭 Lockbit 勒索团伙渗透 | 制造业 | Lockbit |
| 2024/4/16 | 台湾地区某化工公司遭 Black Suit 勒索软件感染 | 制造业 | Black Suit |
| 2024/5/24 | 国内某皮革行业公司遭到 Black Suit 勒索软件攻击 | 制造业 | Black Suit |
| 2024/6/10 | 中国台湾某光纤制造商遭到 Cactus 团伙勒索 | 制造业 | Cactus |

表 1 2024 年上半年国内勒索攻击典型事件

根据表 1 可以看出，2024 年上半年，制造业作为我国经济的支柱产业，成为勒索攻击的重点目标，而 Lockbit 和 Black Suit 两大勒索软件组织则扮演着重要的角色，以其高度专业化的技术手段，对该领域企业发起攻击，加密关键数据并勒索赎金。这种勒索攻击不仅导致企业生产中断和财务损失，还可能造成供应链的瘫痪和客户信任的破坏。

PS:

Lockbit: 该勒索团伙起源于俄罗斯，遵循 RaaS 运营模式，且后期主要采用“双重勒索”策略（文件加密 + 数据披露）来敲诈受害者。LockBit 团伙的同名恶意软件于 2019 年首次浮出水面，并于 2021 年 6 月推出了 LockBit2.0，2022 年 7 月再次推出 LockBit3.0。通过不断构思新策略，已将自己打造为地下犯罪组织中最专业的犯罪团伙之一。目前，LockBit 勒索软件攻击范围遍及北美、欧洲和亚太地区，似乎并无国界之分。其中，美国、法国、英国、中国等国家为重灾区。此外，LockBit 的攻击目标并不局限于某一特定组织，其目标行业来自各行各业，且尤其青睐软件和信息技术、制造、政府、网络安全、国防等关键行业。

Black Suit: 该勒索团伙于 2023 年 5 月首次出现，主要攻击医疗保健、教育、信息技术、政府、零售和制造业的实体。该团伙没有公共附属机构，但似乎与 Royal 勒索软件团伙有着密切的联系，而该团伙又是臭名昭著的 Conti 集团的继承者。据悉，其勒索软件有效负载通过网络钓鱼或第三方框架（如 Empire、Metasploit、Cobalt Strike）传播，主要针对 Linux 和 Windows 系统，采用 AES 加密算法，加密完成后会在文件末尾附加“.blacksuit”扩展名，并会更改桌面壁纸，最终留下一封名为“README.BlackSuit.txt”的勒索信。

3.1.2 数据泄露类

| 时间 | 泄露事件 | 影响行业 | 数据量 | 泄露类型 |
|-----------|----------------------------|---------------|---------|-------------|
| 2024/1/2 | 国内某第三方支付平台会员信息遭售卖 | 通信及软件和信息技术 | 104.85W | 会员个人信息 |
| 2024/1/2 | 国内某行业监管机构员工信息遭公开贩卖 | 政府 | 未知 | 员工个人信息 |
| 2024/1/6 | 某国有集团内部资料泄露 | 交通运输、金融、建筑与地产 | 未知 | 公司内部文件资料 |
| 2024/1/11 | 国内某健康产业集团泄露客户购买记录 | 医疗 | 54136 条 | 客户购买记录 |
| 2024/1/12 | 国内某考研教育机构学生课程信息遭公开贩卖 | 商务服务 | 未知 | 学生课程信息 |
| 2024/1/15 | 中国某上市房企公司机密信息在暗网出售 | 建筑与地产 | 8.67GB | 公司机密信息 |
| 2024/1/17 | 国内某理财公司客户数据泄露 | 金融 | 未知 | 客户数据 |
| 2024/1/21 | 台湾某金融管理部门投资人信息在暗网出售 | 政府 | 19W | 投资人信息 |
| 2024/1/26 | 香港某汽车保险公司后台遭渗透 | 金融 | 274W+ | 客户数据 |
| 2024/1/27 | 国内某证券公司客户理财数据泄露 | 金融 | 未知 | 客户理财数据 |
| 2024/3/6 | 国内某保险公司数据库遭渗透 | 金融 | 未知 | 数据库信息 |
| 2024/3/16 | 国内某共享单车品牌泄露 8000 万用户信息 | 交通运输 | 8000w | 用户数据 |
| 2024/3/16 | 国内某留学服务机构后台遭渗透 | 商务服务 | 25760 | 学生用户订单信息 |
| 2024/4/1 | 国内某理财公司客户数据泄露 | 金融 | 未知 | 客户数据 |
| 2024/4/9 | 国内某大学教师数据泄露 | 教育与科研 | 37612 | 教师信息 |
| 2024/4/9 | 国内某跨境电商平台 300W 数据遭泄露 | 通信及软件和信息技术 | 300W | 客户信息 |
| 2024/4/10 | 国内某农村金融机构客户数据泄露 | 金融 | 未知 | 客户数据 |
| 2024/4/13 | 国内某招聘平台用户数据泄露 | 通信及软件和信息技术 | 未知 | 用户数据 |
| 2024/4/15 | 国内某景区数据库遭渗透 | 文体娱乐 | 324W | 实名制数据库信息， |
| 2024/4/21 | 国内某借贷平台用户数据泄露 | 金融 | 未知 | 用户信息 |
| 2024/5/2 | 澳门某赌场酒店数据库遭渗透 | 文体娱乐、餐饮住宿 | 未知 | 数据库 |
| 2024/5/9 | 2024 年市区县全国政府机关领导联系方式在暗网售卖 | 政府 | 700 条 | 政府机关领导联系方式 |
| 2024/5/12 | 中国台湾某网络服务公司数据在暗网售卖 | 通信及软件信息技术服务 | 1600w | 用户数据 |
| 2024/5/15 | 国内某知名汽车公司数据泄露 | 制造业 | 6w | 公司数据 |
| 2024/5/16 | 某国有企业员工数据泄露 | 政府 | 未知 | 员工数据 |
| 2024/5/16 | 香港某本地论坛数据泄露 | 通信及软件信息技术服务 | 未知 | 用户数据 |
| 2024/5/22 | 国内某财税网校官方用户数据泄露 | 商务服务 | 未知 | 用户数据 |
| 2024/5/25 | 国内某金融服务机构泄露商户 POS 交易数据 | 金融 | 未知 | 商户 POS 交易数据 |

| 时间 | 泄露事件 | 影响行业 | 数据量 | 泄露类型 |
|-----------|---------------------------|-------------|--------|---------|
| 2024/5/31 | 中国台湾地区某政府委员会数据遭售卖 | 政府 | 1w | 委员会成员数据 |
| 2024/6/6 | 国内某教育科技公司学员订单信息泄露 | 教育与科研 | 未知 | 学员订单信息 |
| 2024/6/7 | 中国某国有电力公司数据遭售卖 | 能源 | 未知 | 公司信息 |
| 2024/6/10 | 国内某知名体育博彩公司客户信息泄露 | 文体娱乐 | 28w | 客户信息 |
| 2024/6/15 | 国内某航空服务公司培训管理平台数据库访问权限遭售卖 | 交通运输 | 未知 | 数据库访问权限 |
| 2024/6/16 | 香港某科技公司数据库信息在暗网出售 | 通信及软件信息技术服务 | 510w | 数据库信息 |
| 2024/6/17 | 国内某招投标咨询公司客户信息泄露 | 商务服务 | 4.5w | 客户信息 |
| 2024/6/23 | 国内某领先的医疗器械集团数据遭泄露 | 医疗 | 8.71GB | 公司信息 |
| 2024/6/28 | 国内某教育平台官网后台遭渗透 | 教育与科研 | 未知 | 数据库信息 |

表 2 2024 上半年国内数据泄露典型事件

根据表 2 和下图 12，可以发现数据泄露对国内金融、政府、通信和软件信息技术服务及租赁与商务服务行业造成了最为明显的困扰。这些行业泄露涉及的数据类型主要包括用户信息、数据库信息和公司内部文件等。其中用户信息的泄露频率最高，数据泄露量从 700 条到 8000 万不等。这说明无论数据量大小与否，都有可能成为犯罪分子的交易筹码。泄露的用户信息可能包括个人身份信息、金融账户信息以及其他敏感数据，给用户的隐私和财产安全带来了巨大威胁。数据库信息的泄露可能导致公司商业机密的泄露，造成严重的经济损失和竞争劣势。同时，公司内部文件的泄露可能暴露出组织的战略规划、商业计划以及内部运营细节，给企业带来不可挽回的损失。

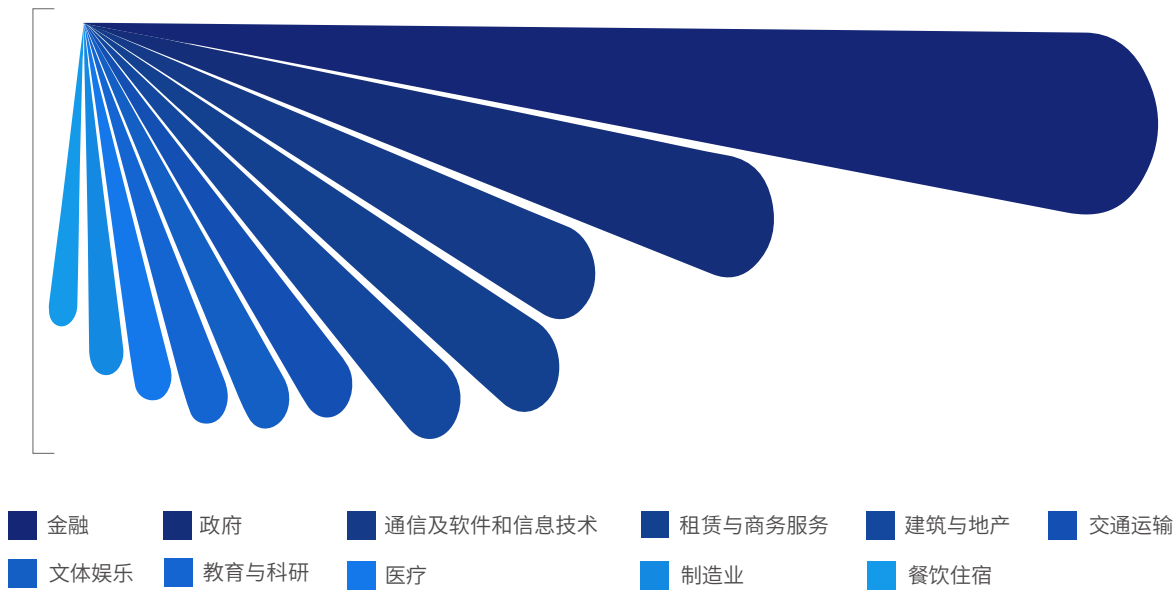


图 12 国内数据泄漏行业分布

3.1.3 黑客攻击类

在黑客攻击方面，中国企业被攻击的事件较少被黑客公开披露，这一现象可能是由于中国不明确站队于国际几大战场（如俄乌、巴以），同时不参与涉及政治的组织活动。因此，黑客组织就没有理由大胆的进行报复攻击。这也说明了中国企业在黑客攻击事件中相对较少受到损害，但也不能得出中国企业没有遭受黑客攻击的结论。例如，2024 年上半年，国内某科技公司就遭到了 R00TK1T 黑客组织的攻击。据悉，该黑客组织于 2024 年 4 月 15 日下午在其 TG 频道中声称对国内某个以无人机技术而闻名的科技公司 (DJI, 大疆创新) 发起了攻击，因为该公司向乌克兰提供了无人机，用于与俄罗斯的持续冲突。不久后，R00TK1T 表示其成功攻破了受害公司的安全系统，并获取了大量的客户数据，包括订单 ID、日期和时间、客户姓名、跟踪号、价格、无人机规格、联系信息、运输详情、付款方式等敏感信息。要保护企业的网络安全，我们仍需持续加强网络防御和安全措施，以及加强国际合作，共同应对全球范围内的网络威胁。

PS:

R00TK1T 黑客组织名称来自网络术语“rootkit”。rootkit 是一种恶意软件，允许黑客未经授权访问网络或系统并窃取数据。R00TK1T 黑客组织以其隐秘的行动而闻名，之前曾以教育、医疗保健、交通、电信、金融机构、政府数据库和跨国公司为目标，还声称对过去许多备受瞩目的网络攻击负责，包括法国化妆品公司欧莱雅、卡塔尔航空公司、索迪斯南非分公司、黎巴嫩社会事务部等。该组织的主要攻击手法包括利用软件漏洞、部署恶意软件和执行复杂的网络钓鱼攻击等。

3.2 国外事件

3.2.1 勒索攻击类

| 时间 | 勒索事件 | 影响行业 | 涉及地区 | 勒索组织 |
|-----------|--|-----------------|------|------------|
| 2024/1/2 | Lockbit 对德国 IDEA 工业物流服务提供商发起攻击 | 交通运输 | 德国 | Lockbit |
| 2024/1/17 | 能源巨头施耐德电气遭受 Cactus 勒索软件袭击 | 能源 | 法国 | Cactus |
| 2024/2/21 | 英国 Helical Technology 制造公司遭 8Base 渗透 | 制造业 | 英国 | 8Base |
| 2024/2/28 | 孟加拉国警方遭 Mogilevich 勒索组织渗透 | 政府 | 孟加拉国 | Mogilevich |
| 2024/3/18 | 波兰工业机械制造商 Grupatopex 遭 Cactus 勒索软件袭击 | 制造业 | 波兰 | Cactus |
| 2024/3/27 | 美国 Lambda Energy Resources 能源组织遭 Play 勒索团伙渗透 | 能源 | 美国 | Play |
| 2024/4/1 | Clop 勒索团伙窃取英国 the7stars 媒体机构数据 | 文体娱乐 | 英国 | Clop |
| 2024/4/7 | 马来西亚 MIDF 金融机构遭 Rhysida 勒索软件袭击 | 金融 | 马来西亚 | Rhysida |
| 2024/4/10 | 荷兰 Nexperia 半导体公司遭 Dunghill 勒索团伙渗透 | 制造业、通信及软件信息技术服务 | 荷兰 | Dunghill |
| 2024/4/17 | 美国 Lee 大学遭 Medusa 勒索组织袭击 | 教育与科研 | 美国 | Medusa |

| 时间 | 勒索事件 | 影响行业 | 涉及地区 | 勒索组织 |
|-----------|--|-------------|----------|------------|
| 2024/4/18 | Lockbit 勒索团伙攻破美国 DC 政府门户网站 | 政府、金融 | 美国 | Lockbit |
| 2024/4/21 | USDoD 勒索组织公开商业情报公司毕威迪数据 | 金融 | 美国 | USDoD |
| 2024/4/22 | 8base 勒索团伙入侵美国 Tech Interactive 科技博物馆 | 文体娱乐 | 美国 | 8Base |
| 2024/5/23 | Bianlian 勒索团伙渗透北美 NUTEC 制造商 | 制造业 | 美国 | Bianlian |
| 2024/5/24 | Lockbit 勒索组织攻陷新加坡 KNS 半导体公司 | 制造业 | 新加坡 | Lockbit |
| 2024/5/26 | Bianlian 勒索团伙渗透美国 NPS Media Group 媒体公司 | 文体娱乐 | 美国 | Bianlian |
| 2024/6/3 | Lockbit 勒索组织攻陷美国 EMA 公司 | 通信及软件信息技术服务 | 美国 | Lockbit |
| 2024/6/3 | 日本 Nidec 马达电机制造商遭到 8Base 勒索团伙攻击 | 制造业 | 日本 | 8Base |
| 2024/6/5 | Daixin 勒索团伙入侵阿联酋迪拜市政府 | 政府 | 阿拉伯联合酋长国 | Daixin |
| 2024/6/11 | Arcusmedia 团伙渗透美国 WinFashion 公司 | 通信及软件信息技术服务 | 美国 | Arcusmedia |
| 2024/6/11 | 英国 Apex 工程服务公司遭到 APT73 勒索团伙攻击 | 建筑与地产 | 英国 | APT73 |
| 2024/6/17 | 美国知名啤酒公司 FIFCO USA 遭到 dAn0n 勒索组织攻击 | 制造业 | 美国 | dAn0n |
| 2024/6/17 | RansomHub 勒索团伙攻陷意大利 GB RICAMBI 备件生产商 | 制造业 | 意大利 | RansomHub |
| 2024/6/24 | Cactus 勒索团伙渗透加拿大 HYDMEC 机械公司 | 制造业 | 加拿大 | Cactus |
| 2024/6/24 | 美国 HARRIS 牛肉生产商遭到 RansomHub 勒索组织攻击 | 制造业 | 美国 | RansomHub |

表 3 2024 年上半年国外勒索攻击典型事件

经过对表 3 的抽样数据进行深入分析，我们注意到上半年在国家 and 行业层面上，美国和制造业仍然是最欢迎的攻击目标，这与第二节中关于勒索软件数据的总体统计结果相吻合。同时，Lockbit 也是最为活跃的勒索组织，其影响力不容忽视。此外，令人瞩目的是，除了知名企业施耐德电气、Nidec 马达电机制造商、啤酒公司 FIFCO USA 遭受攻击外，孟加拉国警方、美国 DC 政府、阿联酋迪拜市政府等高度权威的实体也成为了勒索软件挑战的目标。这一现象表明，大多数勒索软件并没有明显的偏好，更多地是机会主义的行为，它们选择目标是基于机遇而非特定领域。

3.2.2 数据泄露类

| 时间 | 泄露事件 | 影响行业 | 涉及地区 | 数据量 | 泄露类型 |
|-----------|------------------------------------|---------------|------|--------|-----------|
| 2024/1/8 | 马来西亚核中心企业邮箱泄露 | 能源 | 马来西亚 | 2.9GB | 企业邮箱 |
| 2024/1/14 | 美国 NASA 内部数据泄露 | 政府 | 美国 | 1.44GB | 内部数据 |
| 2024/1/15 | 瑞典国防企业萨博 SAAB 集团内部数据泄露 | 制造业 | 瑞典 | 2.83GB | 内部数据 |
| 2024/1/18 | 麦当劳公司内部数据泄露 | 服务业 | 美国 | 未知 | 内部数据 |
| 2024/1/24 | 泰国劳保局数据泄露 | 政府 | 泰国 | 270W | 个人数据 |
| 2024/2/1 | 巴西 TIM 运营商泄露 1562 万数据 | 通信及软件信息技术服务 | 巴西 | 1562W | 个人数据 |
| 2024/2/24 | 乌克兰海关数据库泄露 | 政府 | 乌克兰 | 28W+ | 海关数据 |
| 2024/3/23 | 韩国三星股票证券投资人员数据泄露 | 金融 | 韩国 | 70w | 投资人员信息 |
| 2024/3/25 | 印度 TrueCaller 公司数据遭泄露 | 通信及软件信息技术服务 | 印度 | 未知 | 公司信息 |
| 2024/4/1 | 印度警察成员信息泄露 | 政府 | 印度 | 未知 | 警察成员信息 |
| 2024/4/7 | 美国环境保护署联系人列表数据库泄露 | 政府 | 美国 | 未知 | 联系人列表数据库 |
| 2024/4/7 | 以色列国防部网站信息泄露 | 国防军工 | 以色列 | 未知 | 数据库 |
| 2024/4/15 | 美国 Space-eyes 地理空间情报服务商网站数据库信息遭公开 | 政府、国防军工、科研与教育 | 美国 | 未知 | 数据库 |
| 2024/4/22 | 英国皇家银行组织数据泄露 | 金融 | 英国 | 70w | 用户投资理财信息 |
| 2024/5/6 | 英国政府门户网站数据库泄露 | 政府 | 英国 | 100w | 数据库 |
| 2024/5/13 | 阿拉伯 Aramex 跨国物流公司数据泄露 | 交通运输 | 阿拉伯 | 43GB | 公司信息 |
| 2024/5/15 | 俄罗斯政府服务公务员数据泄露 | 政府 | 俄罗斯 | 未知 | 公务员数据 |
| 2024/5/20 | 美国 Gemini 加密货币交易所数据泄露 | 通信及软件信息技术服务 | 美国 | 750w | 用户信息 |
| 2024/5/25 | 美国 USPAY 电子支付平台用户数据泄露 | 通信及软件信息技术服务 | 美国 | 52w | 用户信息，涉及用户 |
| 2024/5/27 | 西班牙迪卡侬员工信息遭公开 | 批发零售 | 西班牙 | 6644 条 | 员工信息 |
| 2024/6/3 | 新加坡 Tech in Asia 英语科技媒体公司数据库遭泄露 | 文体娱乐 | 新加坡 | 23w | 数据库信息 |
| 2024/6/7 | BlackBerry 公司 Cylance 安全部门数据在暗网上出售 | 通信及软件信息技术服务 | 美国 | 34m | 客户和员工信息 |
| 2024/6/12 | 意大利求职网站泄露用户信息 | 通信及软件信息技术服务 | 意大利 | 未知 | 用户信息 |
| 2024/6/19 | 印度有线宽带服务提供商 Hathway 泄露光纤网络业主数据 | 通信及软件信息技术服务 | 印度 | 300w | 业主数据 |
| 2024/6/23 | 印度外交部海外就业司 Emigrate 系统数据泄露 | 政府 | 印度 | 20w+ | 数据库信息 |

| 时间 | 泄露事件 | 影响行业 | 涉及地区 | 数据量 | 泄露类型 |
|-----------|----------------------------------|-------------|-------|---------|---------|
| 2024/6/24 | 印度尼西亚军事战略情报局数据遭售卖 | 政府 | 印度尼西亚 | 33.7GB+ | 数据库机密文件 |
| 2024/6/26 | 泰国土地和建筑税务数据库访问权限遭泄露 | 政府 | 泰国 | 未知 | 数据库访问权限 |
| 2024/6/28 | 泰国 THAI 国际航空公司泄露乘客信息 | 交通运输 | 泰国 | 200w | 乘客信息 |
| 2024/6/30 | 印度尼西亚国家情报局 BIN 遭渗透 | 通信及软件信息技术服务 | 印度尼西亚 | 未知 | 数据库机密数据 |
| 2024/6/30 | 印度尼西亚 Kominfo 通信和信息技术部泄露 2 亿个人信息 | | 印度尼西亚 | 2 亿 | 个人信息 |

表 4 2024 年上半年国外数据泄露典型事件

表 4 数据显示，美国仍然是数据泄露问题最为典型的国家。上半年，不仅重要的政府机构（如 NASA、环境保护署），甚至知名的快餐品牌麦当劳公司都遭受了不同程度的机密内部数据泄露。此外，还有一系列其他引人注目的数据泄露事件，比如马来西亚核中心企业邮箱泄露事件、韩国三星 70 万投资人信息泄露事件、巴西 TIM 运营商 1562 万用户数据泄露事件、阿拉伯 Aramex 跨国物流公司数据泄露事件、BlackBerry 公司 Cylance 安全部门数据泄露事件、以色列国防部网站数据库信息泄露事件、印度尼西亚国家情报局 BIN 和军事战略情报局数据泄露事件等。这些事件表明，数据安全是一个全球性的挑战，不论是政府机构、知名企业还是普通用户，都需要高度重视和加强防范措施。

3.2.3 黑客攻击类

| 时间 | 攻击事件 | 影响行业 | 涉及地区 | 勒索组织 |
|-----------|--|-------------|----------|------------|
| 2024/1/1 | Twitch 游戏直播网站因 Anonymous Sudan 组织攻击而中断 | 通信及软件信息技术服务 | 美国 | Lockbit |
| 2024/1/12 | Anonymous Sudan 组织瞄准以色列 MedOne 数据中心 | 通信及软件信息技术服务 | 以色列 | Cactus |
| 2024/1/12 | 马尔代夫国防军官方网站被 UCC 黑客团伙攻陷 | 政府 | 马尔代夫 | 8Base |
| 2024/1/16 | Anonymous Sudan 瞄准阿联酋移动卫星服务提供商 Thuraya | 通信及软件信息技术服务 | 阿拉伯联合酋长国 | Mogilevich |
| 2024/1/24 | Anonymous_v7X 组织瞄准以色列 CellCom 电信公司 | 通信及软件信息技术服务 | 以色列 | Cactus |
| 2024/2/25 | Anonymous Sudan 组织瞄准阿联酋卫星基础设施 | 通信及软件信息技术服务 | 阿拉伯联合酋长国 | Play |
| 2024/2/29 | Ghosts of Palestine 团伙瞄准以色列教育组织 | 教育与科研 | 以色列 | Clop |
| 2024/3/1 | Alixsec 联合 12 个黑客组织袭击沙特阿拉伯的数字基础设施 | 通信及软件信息技术服务 | 沙特阿拉伯 | Rhysida |
| 2024/3/21 | UserSec 组织对卢森堡发起联合攻击 | 政府、交通运输 | 卢森堡 | Dunghill |
| 2024/3/25 | NoName057(16) 组织对荷兰发起 DDoS 攻击 | 政府 | 荷兰 | |
| 2024/3/27 | Türk Hack Team 组织攻陷瑞典萨博军事企业网站 | 国防军工、制造业 | 瑞典 | |

| 时间 | 攻击事件 | 影响行业 | 涉及地区 | 勒索组织 |
|-----------|--|----------------|-------|------|
| 2024/4/6 | NoName057(16) 组织对乌克兰关键基础设施发起 DDoS 攻击 | 政府、教育与科研、交通运输 | 乌克兰 | |
| 2024/4/26 | R3Xsec 黑客组织攻陷日本美容网站 | 医疗 | 日本 | |
| 2024/5/7 | Anonymous Arabia 组织对沙特阿拉伯电力公司发动大规模攻击 | 能源 | 沙特阿拉伯 | |
| 2024/5/15 | LulzSec 黑客组织攻陷以色列犹太复国主义战略研究所 | 社会组织 | 以色列 | |
| 2024/5/29 | 以色列 Tasmc 医疗中心系统遭到 Anonymous Collective 组织攻击 | 医疗 | 以色列 | |
| 2024/6/5 | 乌克兰国立教育机构遭到 Bloodnet 组织攻击 | 教育与科研 | 乌克兰 | |
| 2024/6/6 | 荷兰互联网基础设施遭到 NoName057(16) 组织攻击 | 交通运输、政府 | 荷兰 | |
| 2024/6/13 | 巴基斯坦 Forland 汽车网站遭 Team UCC 黑客组织攻陷 | 制造业 | 巴基斯坦 | |
| 2024/6/13 | 瑞士互联网基础设施遭到 NoName057(16) 组织攻击 | 政府、餐饮住宿 | 瑞士 | |
| 2024/6/15 | 美国 LAVR International 私营军事安保公司遭俄罗斯网军攻陷 | 国防军工 | 美国 | |
| 2024/6/20 | 罗马尼亚基础设施遭到 NoName057(16) 组织攻击 | 通信及软件信息技术服务、金融 | 罗马尼亚 | |
| 2024/6/23 | 以色列 Zerto 网络安全公司遭 Handala 组织攻陷 | 通信及软件信息技术服务、金融 | 以色列 | |

表 5 2024 年上半年国外黑客攻击典型事件

表 5 数据显示，2024 年上半年，中东地区的以色列、沙特阿拉伯、阿拉伯联合酋长国以及东欧地区的乌克兰国家成为黑客组织活动的主要热点场所。这一现象的根本原因在于巴以冲突和俄乌战争的影响扩展至网络世界。大量兼具政治色彩的黑客组织纷纷参与其中，对乌克兰、以色列及其支持的国家的重要基础设施发动了一系列 DDoS 攻击。举例来说，NoName057(16) 组织对荷兰发起了 DDoS 攻击，其原因是荷兰国防部代理部长卡伊萨·奥隆格伦在访问乌克兰后接受路透社采访时宣布今年下半年将向乌克兰移交首批美国 F-16 战斗机。R3Xsec 黑客组织攻陷了一家日本美容网站，旨在向世界揭示以色列及其武装力量的真实面貌，同时呼吁对支持以色列的国家发动网络战争，并声称只有在巴勒斯坦国获得独立地位之前才会停止攻击。Anonymous Arabia 组织对沙特阿拉伯电力公司发起了大规模攻击，其攻击的原因是因为沙特阿拉伯几天前宣布即将与以色列恢复正常关系，并将逮捕在社交媒体上发布反以色列内容的人员。

04 POINT

半年特点总结

2024 年上半年，国内外暗网威胁呈现严峻态势，尤其体现在勒索软件、数据泄露和黑客攻击活动方面，反映出络网络犯罪活动的多样化和复杂化趋势。以下是 2024 年上半年暗网攻击报告的主要特点总结：

1) 活跃勒索软件团伙攻击活动持续增加

上半年，Lockbit 勒索软件作为最活跃的一款，共攻击了 607 名受害者，相较于 2023 年下半年的 515 名，明显呈上升趋势。其他活跃的顶级勒索软件，如 Play 和 8Base，也在上半年展现出活动频率不断上升的趋势。此外，2024 年 2 月新出现的 Ransomhub 在上半年表现抢眼，成功占据了活跃勒索组织排名的第二位。新老勒索软件相互交替，通过 RaaS (Ransomware-as-a-Service) 模式广泛传播，降低了发动攻击的技术门槛，预计未来勒索行业发展的不可小觑，勒索攻击事件将持续增加，提升网络安全防护的重要性与紧迫性更加凸显。

2) 暗网数据泄露问题日益严重，影响全球各行各业

暗网数据泄露问题日益严重，对全球各行各业产生了显著影响。仅在 2024 年上半年，暗网数据泄露事件就达到了 26282 起，远超勒索攻击和黑客攻击事件的总和。这主要是因为暗网环境相对匿名和隐蔽，让犯罪分子更容易销售和交换被盗的数据。此外，暗网上的数据泄露交易越来越成熟和专业化，供应链庞大，涵盖个人身份、财务信息、商业机密等敏感数据。他们采用多样的交易方式，使用加密货币进行支付，给追踪和打击带来了更大的困难。暗网数据泄露已然成为最为严重的威胁，需要全球范围内的合作，加强网络安全防护，以保护重要信息的安全和机构的利益。


3) 地缘政治类黑客攻击活动加剧

随着不断升级的冲突，如以色列与哈马斯、俄罗斯与乌克兰之间的对抗，黑客攻击已经逐步延伸至政治对抗的网络领域。上半年，印度和以色列成为黑客组织主要关注的目标，他们的基础设施面临报复性和恐吓性的 DDoS 攻击。这些攻击不仅对目标国家的经济、社会和政治稳定造成严重威胁，也对全球网络安全产生了深远影响。尽管中国受到的影响相对较少，但也不能忽视防范的紧迫性。



天际友盟
TianJi Partners



 www.tj-un.com  400-081-0700

 市场合作: mkt@tj-un.com 客户服务: service@tj-un.com 合作伙伴: partner@tj-un.com