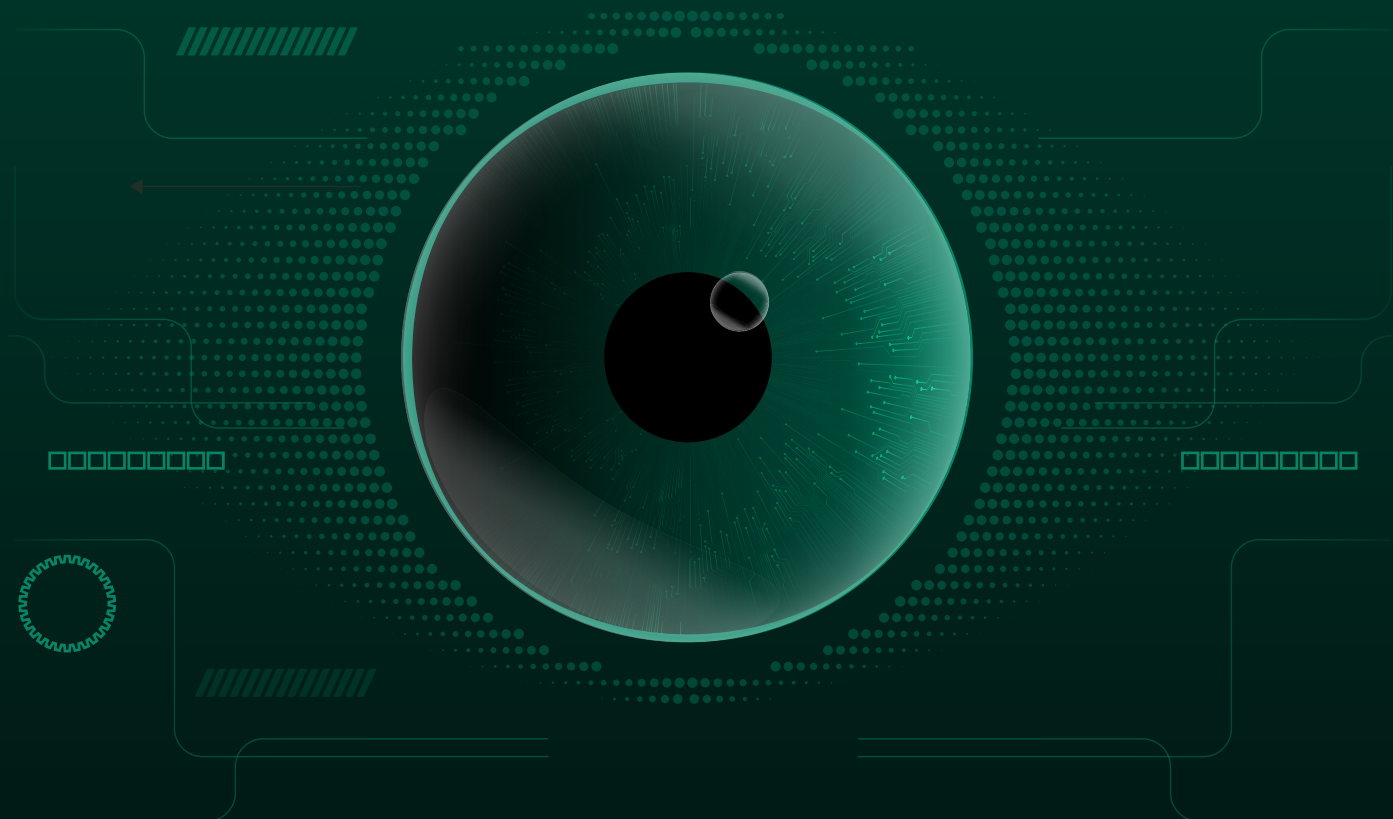


暗网监测2025年度报告



联合发布单位

国家计算机病毒应急处理中心

西安交通大学网络空间安全学院

中国大唐集团有限公司

中国华电集团有限公司

华能信息技术有限公司

中国烟草总公司天津市公司

远江盛邦安全科技集团股份有限公司

【详细单位见版权页】

版权声明

本报告出现的任何文字表述、排版方式、图片、过程及方法等内容，除另有注明，相关著作权均由国家计算机病毒应急处理中心、西安交通大学网络空间安全学院、中国大唐集团有限公司、中国华电集团有限公司、华能信息技术有限公司、中国烟草总公司天津市公司、远江盛邦安全科技集团股份有限公司等（以下合称“权利人”）共同所有，受《中华人民共和国著作权法》、《中华人民共和国著作权法实施条例》等法律法规保护。任何机构、个人，未经权利人书面许可，不得以任何方式引用、复制或以其他方式非法使用本报告，否则将依法追究其法律责任。

报告撰写单位及撰写人：

国家计算机病毒应急处理中心

张喆、彭立炜、王峙轩

西安交通大学网络空间安全学院

韩博、张田田、杜林康

中国大唐集团有限公司

彭强、宋红旭、黄冠杰、李号彩、张强

中国华电集团有限公司

罗建东、宋艳媚、王天石、刘天华

华能信息技术有限公司

崔磊、肖勇、文子强、潘中英、潘书刚

中国烟草总公司天津市公司

王瑞剑、陆明、黄桢、赵海翔、刁雅宁

广发证券股份有限公司

辛治运、李立峰、鹿群、黄辉

青岛国际机场集团有限公司

于飞、曹伟、尤斌、王世友、张春鑫、姜鹏飞

中国电信股份有限公司广西分公司

潘鹤元、李砚哲、韦仕昌

中国移动通信集团安徽有限公司

江波、林琳、黄坤、侯超

中国移动通信集团广西有限公司

陈式、梁业裕、赖伟光

西部机场集团

李强、韦娟、左紫敏

通号集团财务有限公司

杨扬、王皓、陈靖原

陕西省公安厅科技信息化总队

李靖

泓理信安(陕西)网络科技有限责任公司

周天、李晓凡

远江盛邦安全科技集团股份有限公司

权晓文、郝龙、张其政、胡超超、何文杰、秦雅歆

前言

2025年，全球数字空间正经历一场“无声的范式转移”。随着数字主权博弈进入深水区，算力、数据与人工智能成为大国竞争的底层支柱，传统物理与数字边界在非对称对抗中加速瓦解。暗网已彻底脱离“地下黑市”的传统定位，演变为全球高级网络威胁策源地、地缘对抗隐秘前线、黑产产业化升级核心枢纽，从单纯的社会治安问题跃升为关乎国家安全、经济稳定与社会治理底座的系统性挑战。

本年度，我们通过对全球暗网生态7×24小时不间断全域监测，累计捕获暗网威胁事件1,017,175起。监测数据清晰印证：暗网威胁已完成根本性代际迭代——作案动机从单一经济牟利转向战略破坏与地缘博弈；参与主体从零散黑客升级为国家背景作战力量与跨国犯罪集团；攻击手段从传统人工渗透迭代为AI驱动的全链条自动化攻击；危害层级从个体损失上升至影响全球数字治理秩序的战略层面。

2025年，三大核心变量交织共振，重构了暗网格局：一是地缘冲突驱动威胁武器化，暗网成为非对称对抗的隐秘阵地；二是生成式AI彻底改写攻防逻辑，网络攻击从“脚本时代”迈向“智能体时代”，AI黑产技术服务收入四年间激增1900%^[1]；三是卫星互联网开辟威胁新赛道，针对低轨卫星测控链路的暗网探测首次被系统性记录，网络安全与太空安全实现深度绑定。

面对这场隐秘的“深海战争”，传统被动防御已难以为继。本报告旨在穿透匿名迷雾、还原威胁全貌，为监管部门、行业企业与科研机构提供战略级决策参考，助力筑牢国家网络空间安全屏障。

目录

Contents

第一章 我国暗网威胁监测综述

一、2025年我国暗网监测情况分析	02
(一) 我国暗网威胁监测数量和趋势	02
(二) 我国暗网威胁区域分布	03
(三) 我国暗网威胁行业分析	04
二、2025年我国数据贩卖情况分析	05
(一) 我国暗网威胁数据贩卖量级分析	05
(二) 我国暗网威胁数据贩卖类型分析	06

第二章 全球暗网威胁监测综述

一、全球暗网威胁监测情况	08
(一) 全球暗网威胁监测事件数量和趋势	08
(二) 全球暗网威胁区域分布	09
(三) 全球暗网威胁行业分布	10
(四) 全球受影响主体规模分布	11
二、2025年全球数据贩卖情况分析	12
(一) 全球暗网威胁数据贩卖量级分析	12
(二) 全球暗网威胁数据贩卖类型分析	13

第三章 2025年度核心暗网威胁事件监测分析

一、全球暗网活跃组织威胁事件	16
(一) Qilin勒索组织袭击日本朝日集团	16
(二) BlackCat (ALPHV) 针对欧美制造业集群攻击	17
(三) APT29 (Cozy Bear) 关联暗网情报交易	17
(四) Lapsus\$团伙南美政府机构数据泄露	18
(五) RansomHub登顶勒索软件生态位事件	18
(六) APT44 (沙虫) 针对乌克兰能源设施的联合破坏事件	18
(七) 地缘政治黑客组织“Homeland Justice”数据擦除事件	19
二、全球暗网重大数据贩卖事件	20
(一) “开盒”社工库大规模交易	20
(二) 印度政府最高机密文件售卖	21
(三) 500GB 伊拉克政府数据免费泄露	21
(四) 通信内鬼售卖实时定位数据	22
(五) 马来西亚 MYSA 航天局 + 选民数据泄露	22
(六) 波音公司 (Boeing) 核心数据遭 LockBit 窃取事件	23
(七) 印度 Aadhaar 全国身份证系统大规模失陷事件	24
(八) 欧洲航天局 (ESA) 供应链攻击与700GB数据泄露事件	24

(九) 29 亿条公民 SSN (社会安全号码) 数据全量公开事件	25	(二) XSS 俄语漏洞论坛关停与反复	30
三、全球暗网恶意软件与零日漏洞威胁	25	(三) BreachForums (英语数据泄露核心站)	
(一) BazarLoader 暗网订阅制售卖	25	治理震荡	31
(二) Windows 内核零日漏洞暗网拍卖	26	(四) Hydra 后继平台 “WhiteHouse” 被端	32
(三) AI 生成勒索病毒工具包	27	(五) “Huione Guarantee (汇旺担保) 非法	
(四) 安卓银行木马新变种批量上架	27	资金链关联打击事件	33
(五) JetBrains TeamCity 供应链漏洞闪电式利用事件	28	五、全球暗网“犯罪即服务”供应链演进威胁	34
(六) “DarkAgent V3.0”AI 攻击智能体商用化事件	28	(一) IAaaS 初始访问服务	34
(七) ForgePro AI 深度伪造套件爆发事件	29	(二) RaaS 勒索服务升级	34
(八) CCSDS 空天协议专属漏洞交易闭环事件	29	(三) AlaaS 深度伪造与智能体服务	35
四、全球暗网核心平台执法打击与治理重构事件	30	(四) LaaS 非法金融洗钱服务	35
(一) 全球 “RapTor 行动” 捣毁暗网毒品/武器市场	30	(五) 暗网一站式 “黑产超市”	36

第四章 2025 年度暗网整体威胁态势分析

一、全球地缘战略对抗态势	38	四、非法产业体系运行态势	43
(一) 混合战争中的暗网 “第二战场”	38	(一) 暗网基础设施与支付体系演化	44
(二) 国家行为体的暗网对抗手段	38	(二) 黑产组织形态与分工精细化	46
(三) 大国博弈背景下的暗网情报战	39	(三) 暗网交易模式升级	48
二、核心技术武器赋能态势	40	五、隐蔽隐匿攻防范式态势	49
(一) 2025 年暗网 Top3 AI 攻击工具监测详情	40	(一) 生成式 AI 全面赋能黑产	50
(二) Huione 平台 AI 服务成交数据趋势	41	(二) 攻击手法隐蔽化与跨域化	51
(三) AI 黑产工具攻击事件典型案例监测	41	(三) 威胁产业化与精准化升级	53
三、新兴领域资产风险态势	42	六、重点行业危害表现态势	55
(一) 商业航天相关权限与数据交易	43	(一) 大规模数据泄露持续高发	55
(二) 卫星终端与协议漏洞交易	43	(二) 勒索软件攻击产业链延伸	56
		(三) 供应链攻击通过暗网扩散	58

第五章 2026 年度暗网威胁趋势预判

一、暗网生态发展趋势预判	62
二、新型威胁演化方向预判	63
三、2026 年暗网防控战略路线	64

参考文献

参考文献	88
------	----

附录

附录 1、核心术语说明	66
附录 2、2025 年度暗网高危风险事件清单	71
附录 3、暗网数据泄露治理方案	72
(一) 重点行业风险暴露分析	72
(二) 防御体系核心痛点剖析	73
(三) 常态监测预警机制建议	75
(四) 构建全域多源情报感知网络	75
(五) 多元业务场景防控策略	79

第一章

我国暗网威胁监测综述



02
03
05

一、2025年我国暗网监测情况分析

近年来随着中国《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国行政处罚法》等法律法规的完善，数据安全的重要性及热度再创新高，逐步成为未来网络安全行业防护重心。

暗网作为新式网络犯罪的平台，每天都有数以万计数据贩卖事件在暗网中发生。大规模数据贩卖和违规事件，不仅造成企业直接经济损失与品牌价值贬损，更导致用户信任资本消解，严重者将会面临行政处罚或停业整顿等多维度监管处罚。

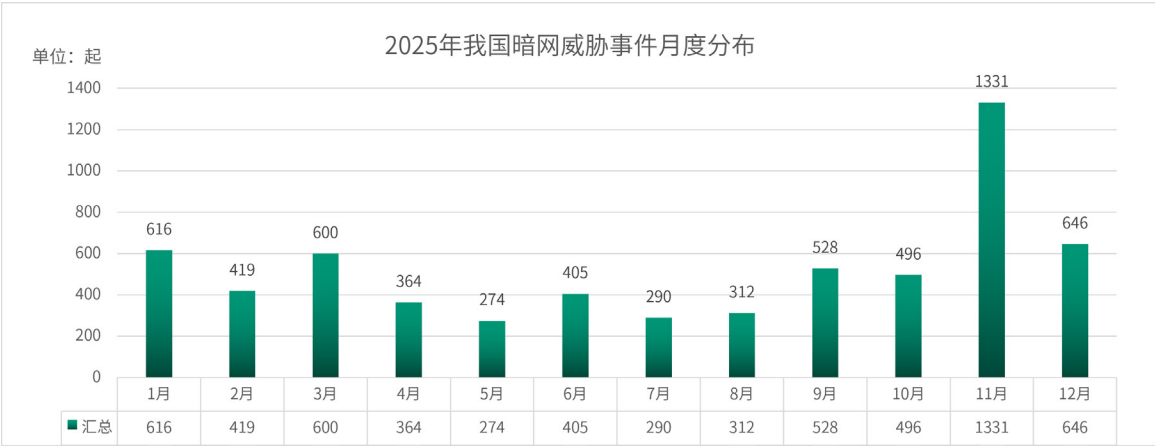
盛邦安全于2023年开始跟踪暗网情报，并于同年深度融合暗网探测技术与网络空间测绘能力、大数据检测分析能力，建立盛邦安全暗网监测平台（以下简称暗网监测平台），对10万个暗网节点（日均活跃节点达1.1万个）开展动态监测。2025年，盛邦安全监测到涉及我国大量的数据贩卖事件，香港（30.29%）、广东（9.70%）、湖南（6.25%）、上海（4.78%）等地是暗网威胁攻击的主要目标地区。

本章内容中涉及到的所有数据均来自于盛邦安全暗网监测数据，重点分析我国真实攻击事件与相关数据，通过整理与分析形成结论。

(一) 我国暗网威胁监测数量和趋势

盛邦安全对10万余个暗网节点进行监测，监测到我国存在多起数据贩卖、勒索等各类暗网威胁事件，根据暗网监测平台数据统计，2025年全年，我国发生的可监测暗网威胁事件共计6,281起。

图1为盛邦安全暗网监测平台发现的2025年暗网威胁事件数量月度统计分析图。根据月度数据分析来看，暗网威胁事件的高发期为11月，分别达到1,331起，明显高于其他月份数据，威胁事件数量最低的为5月，共计274起。



(图1 我国暗网威胁事件月度分布)

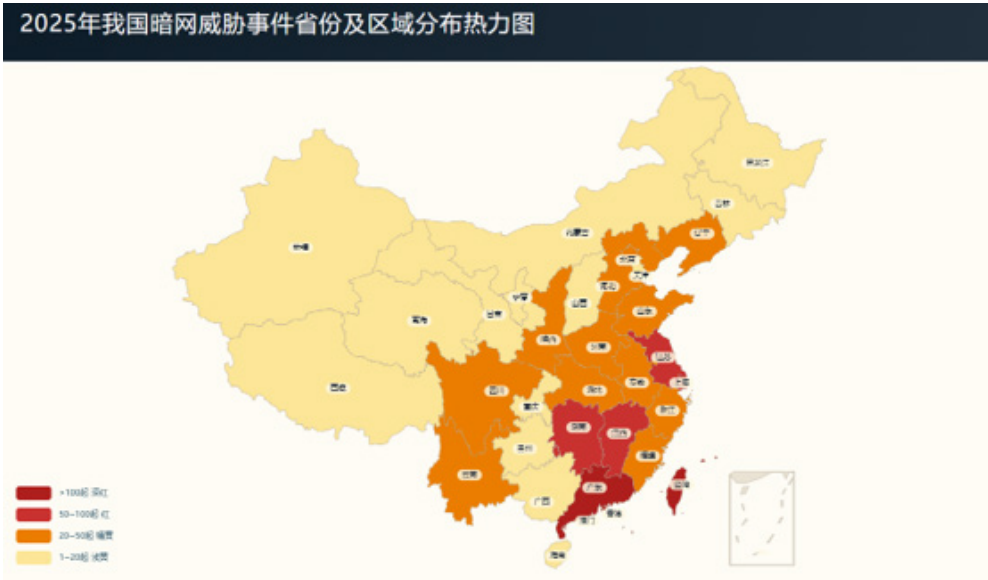
从增长趋势来看,2025年暗网威胁事件虽然在大部分时间处于波动状态,1月、3月分别达到616起和600起,说明年初威胁活动较为活跃;5月降至全年低点274起,7至8月也维持在300起左右,这种情况的发生与节假日后攻击节奏调整、部分黑产团伙阶段性收敛、监测处置加强或攻击资源转移有关;9月起事件数重新上升,11月暴增至1,331起,占全年约两成,显著高于其他月份,通过对11月份的暗网情报进行深入分析,实际是由同一暗网组织频繁发布同一系列数据、监管监测力度提升等因素叠加影响;12月虽回落至646起,但仍处于高位,说明年末暗网威胁并非短期异常,而是存在持续活跃趋势,需重点关注四季度及年初的数据泄露、凭证贩卖和黑产联动风险。

(二) 我国暗网威胁区域分布

图2为2025年我国暗网威胁目标地域分布。根据分布情况可以发现,香港、广东、湖南、上海、江苏以及江西等地区是暗网威胁攻击的高发省份及地区。其中,香港发生的暗网事件最多,约占全国的30.29%,其次分别为广东、湖南、上海以及江苏,分别占比约为9.70%、6.25%、4.78%以及4.57%,五个地区共占据了我国暗网威胁事件55.59%。

如图2中所示,对省份遭受攻击情况进行比较分析,发现南方省份遭受暗网攻击要多于北方省份,根据区域分布进行比较,2025年全年遭受暗网攻击较为严重的区域多集中于长三角、珠三角两个区域,两大区域合计暗网攻击事件数量已接近全国六成,说明暗网威胁高度集中在经济活跃、数字化程度高、数据资产密集的南方核心区域。

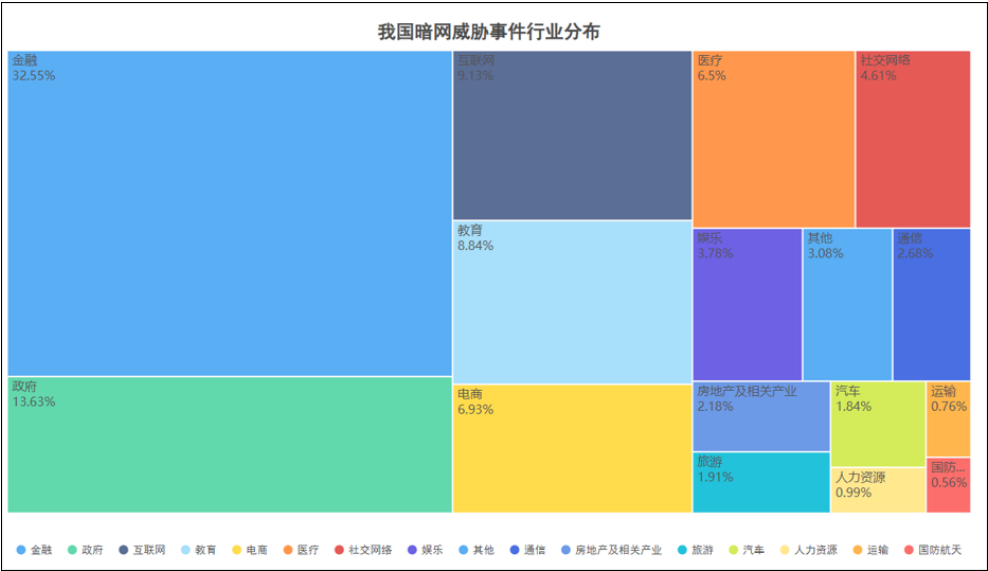
原因主要在于珠三角、长三角聚集了大量金融、外贸、电商、制造业、物流、互联网平台和跨境业务主体,企业系统多、供应链长、人员流动和数据交换频繁,形成了更大的攻击面和更高的数据交易价值;同时,香港及粤港澳地区跨境金融、国际贸易和网络基础设施发达,黑产更容易围绕账号凭证、客户数据、支付信息、企业邮箱和供应链系统开展窃取、贩卖与勒索活动。



（图2 我国暗网威胁事件省份及区域分布热力图）

（三）我国暗网威胁行业分析

2025年我国暗网威胁事件涉及行业达到41种，与去年相同，所有行业中其中受暗网影响最深的是金融行业，占有所有事件的32.55%，其次为政府、互联网、教育行业，分别占比13.63%、9.13%以及8.84%，而电商、医疗与社交网络等领域，占比约在4%至7%之间。图3展示了我国受暗网影响的TOP15行业分布，其中其他行业类型（占比为3.08%）涵盖了体育、制造业、交通等26个行业类型。



（图3 我国暗网威胁事件行业分布TOP15）

针对我国行业暗网威胁数据进行分析，金融行业在整体行业中的占比较2024年的27.99%进一步提高，说明账户、支付、信贷、身份信息等高价值数据仍是暗网交易和攻击变现的核心目标。政府行业从2024年5.82%的跃升至13.6%，与政务系统线上化、公共数据集中、外包供应链复杂以及政务邮箱、账号凭证泄露风险上升有关。

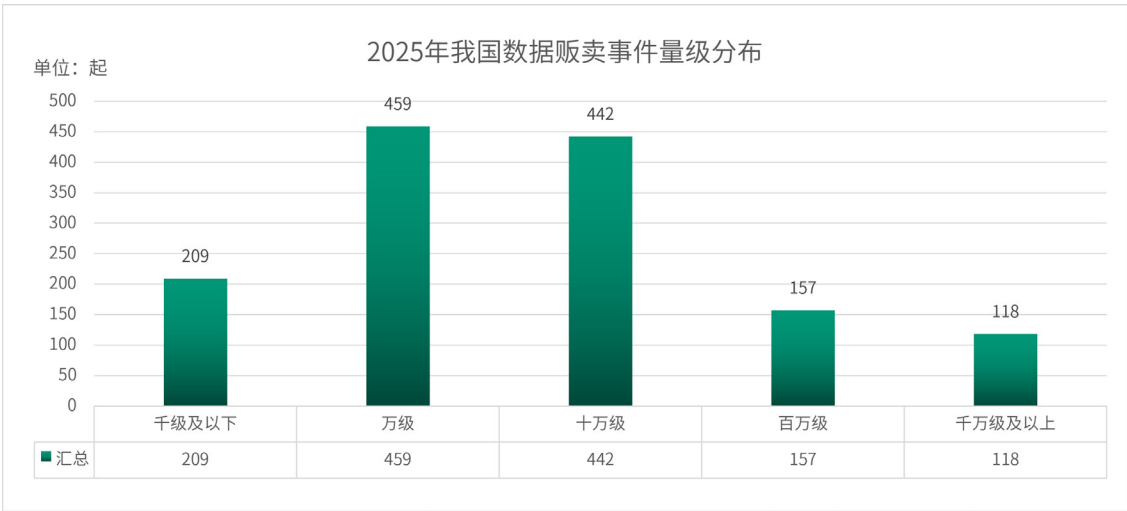
整体看行业分布来看，2025年前四大行业占比约64.2%，高于2024年前四大行业约57.0%，暗网威胁正进一步向金融、政府、互联网、教育、电商、医疗等数据密集型和业务开放型行业集中，其根本原因在于这些行业用户规模大、系统接口多、云平台和移动端暴露面广、第三方供应链链条长，且数据可用于诈骗、撞库、精准钓鱼、勒索和地下交易变现，后续应重点加强核心行业的数据分级保护、账号凭证治理、供应链安全审计和暗网泄露监测。

二、2025年我国数据贩卖情况分析

(一) 我国暗网威胁数据贩卖量级分析

2025年，我国暗网数据贩卖事件可统计的数据总量达到了1386起。在量级分析上来看，其中万级别数据贩卖事件数量最多，为459起，占总数的33.12%，其次是十万级数据贩卖事件，数量达到442起，占比达到31.89%。

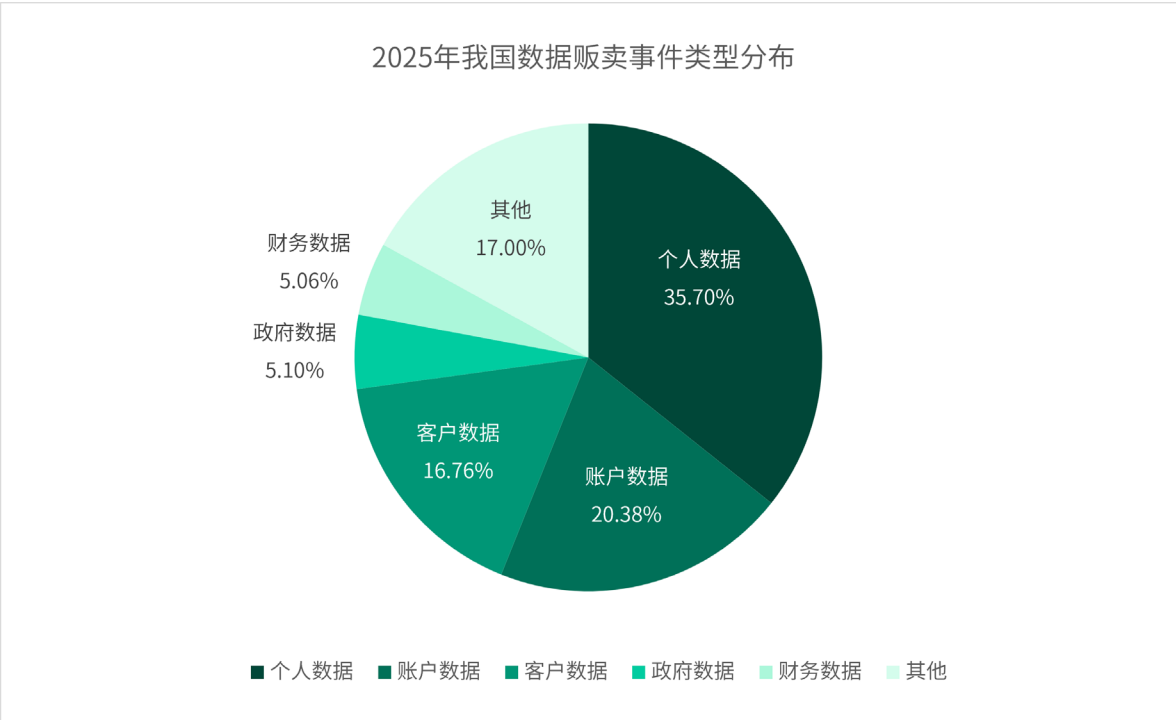
通过数据分析可以发现，与24年相同，万级与十万级数据贩卖事件是最常见的数据贩卖量级，事件数量之和占到了总数的65.01%，总体来看，暗网攻击和数据贩卖呈现“中等规模、高频流通、精准变现”的趋势，攻击者更倾向于围绕账号凭证、行业客户数据、订单信息、政企人员信息等进行分批窃取、拼接售卖和定向变现，而非单纯追求一次性超大规模泄露；这既与数据安全治理、监测溯源和平台风控增强有关，也反映黑产市场对“新鲜、精准、可用于诈骗和撞库”的中高价值数据需求更强。



(二) 我国暗网威胁数据贩卖类型分析

2025年我国暗网数据贩卖事件的数据类型中,个人数据(主要为针对某一区域或某一行业的个人信息贩卖事件中涉及的个人信息数据)的占比最高,达到了35.70%,而排名第二的数据贩卖类型为账户数据(包括网络协议登录账号、平台登录账号等账户数据)占比为20.38%,其他三个排在前五位的来源类型为客户数据(包括面向客户类服务平台中泄露出的服务记录、服务档案等客户相关信息)、政府数据(包括与政府工作相关的特殊身份信息、政策文件等)以及财务数据(主要为针对银行卡账户的个人信息数据贩卖事件中涉及的个人财务数据),分别占比16.76%、5.10%以及5.06%,其他数据类型(涵盖类型共计26种,包括但不限于金融活动数据、教培数据、开发数据等)共占比17.00%。

从数据类型看,2025年我国暗网数据贩卖已由2024年“个人数据一类独大”转向“个人数据、账户数据、客户数据多类并重”的结构。也预示着针对我国的暗网攻击不再单纯追求大规模个人信息贩卖,而是向“凭证化、业务化、场景化、精准化”演进,黑产更倾向于获取账户、客户、政务、财务等可直接用于入侵、诈骗、勒索和灰产业链条联动的数据资产,相关行业应重点加强账号凭证治理、客户数据保护、政务数据分级管控和异常数据外流监测。



(图5 我国数据贩卖事件类型分布)

第二章

全球暗网威胁监测综述



一、全球暗网威胁监测情况

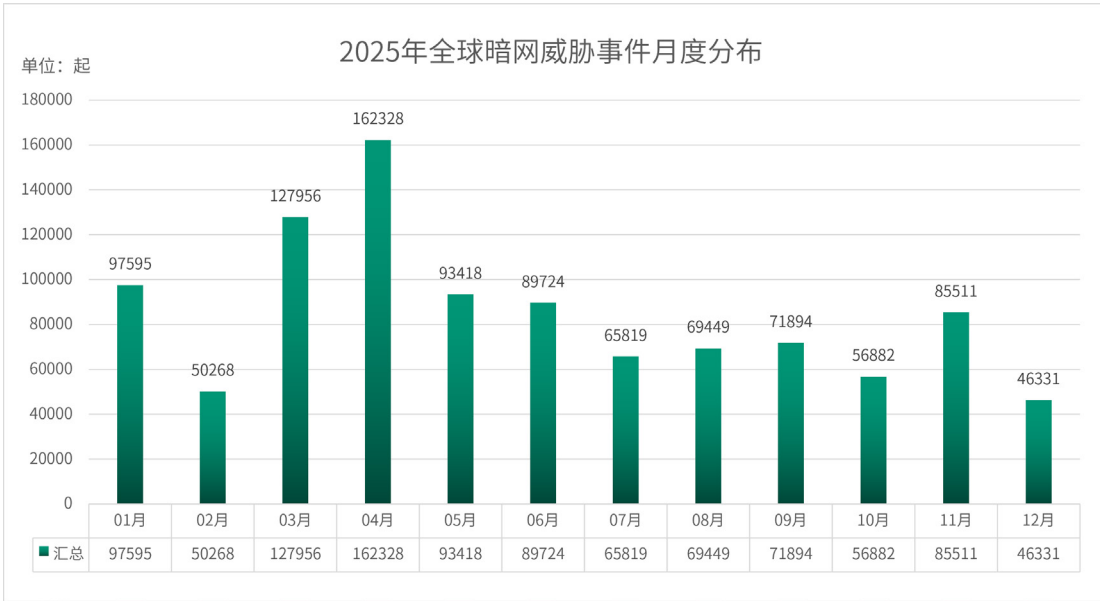
近年来由于全球网络空间复杂多变，边缘冲突加剧，各种暗网现象逐渐滋生。各国都将情报作为保障国家安全的重要屏障，暗网情报作为各类安全情报中最敏感、最直接、最富价值的情报来源，始终都是各国关注的情报核心。

2025年，盛邦安全持续开展全球暗网监测与暗网威胁事件分析。通过对各类情报进行数据统计与整合，梳理当下遭受暗网攻击的重点区域、行业以及企业，从而把握暗网事件规律，预测全球暗网活动的未来发展趋势。

本章内容中涉及到的所有数据均来自于盛邦安全暗网监测数据，重点分析全球真实攻击事件与相关数据，通过整理与分析形成结论。

(一) 全球暗网威胁监测事件数量和趋势

根据盛邦安全暗网监测过程中发现的全球暗网事件数据统计，2025年全年共发生暗网威胁事件1,017,175起。图6为2025年盛邦安全暗网检测平台发现的“2025年全球暗网威胁事件数量月度分布图”，根据月度数据分析来看，全球暗网威胁事件数量呈阶段性波动，二季度达峰后整体回落，在4月份达到了顶峰，达到162,328起，明显高于其他月份数据；威胁事件数量最低的为12月份，共计46,331起。



(图6 全球暗网威胁事件月度分析)

2025年度整体呈现“二季度高发、下半年回落、年末再走低”的特征：一季度占比为27.12%，其中2月短暂回落后3月明显反弹；二季度达到全年峰值，占比33.96%，4月以16.23万起成为全年最高点，说明上半年特别是春季后攻击、数据泄露和暗网贩卖活动集中释放，与前期窃取数据集中上架、漏洞利用窗口扩大、企业系统更新和供应链暴露面增加有关；三季度占比降至20.37%，7—9月维持在6.6万至7.2万起的相对平稳低位，可能受到暑期业务节奏放缓、攻击活动阶段性转移或安全处置加强影响；四季度占比进一步降至18.55%，虽11月因“黑五”“网购季”、金融支付和电商交易活跃带来一轮反弹，但12月降至全年最低的4.63万起，反映全年暗网攻击并非持续线性增长，而是受漏洞披露、数据变现周期、节假日经济活动和黑产运营节奏共同影响，呈现明显的阶段性集中爆发与周期性回落特征。

（二）全球暗网威胁区域分布

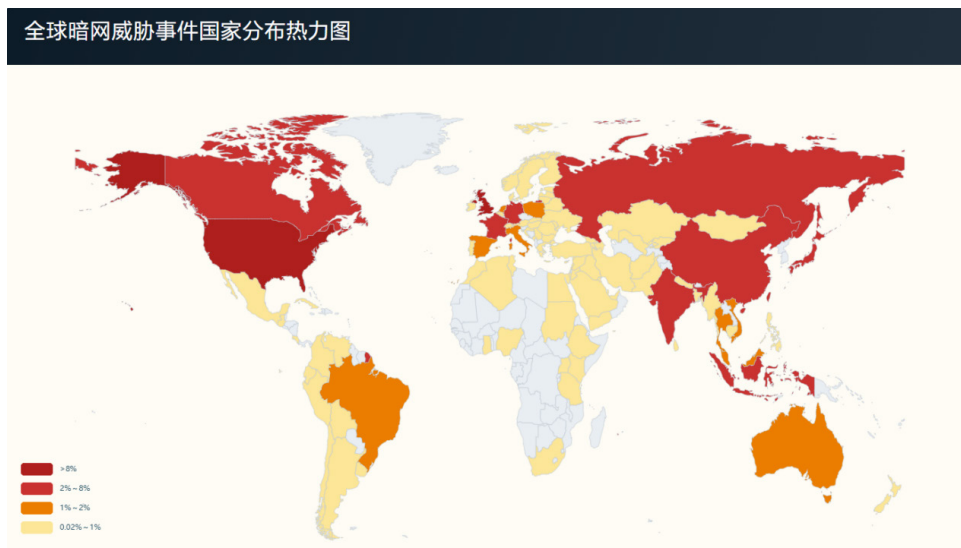
2025年，在盛邦安全暗网监测发现的全球暗网威胁事件中具有明确国家指向的数据量为106,280起，具体分布如图所示，其中图7为全球暗网威胁事件国家分布热力图，图8为全球暗网威胁事件国家分析。根据统计，2025年全年全球仅两个暗网威胁事件数量过万的国家，其中针对美国的暗网威胁事件数量最多，达到了34,380起，排名第二的是针对于英国的攻击，数量达到了10,404。中国地区暗网威胁事件数量达到了6,281起，德国地区占比为4.09%，之后是印度、法国、俄罗斯等国家，分别占比4.06%、3.24%、2.75%，日本地区暗网威胁攻击事件数量占比2.10%。

根据各国暗网事件数量分析可以看出，与24年相同，暗网攻击的主要国家仍分为三类：

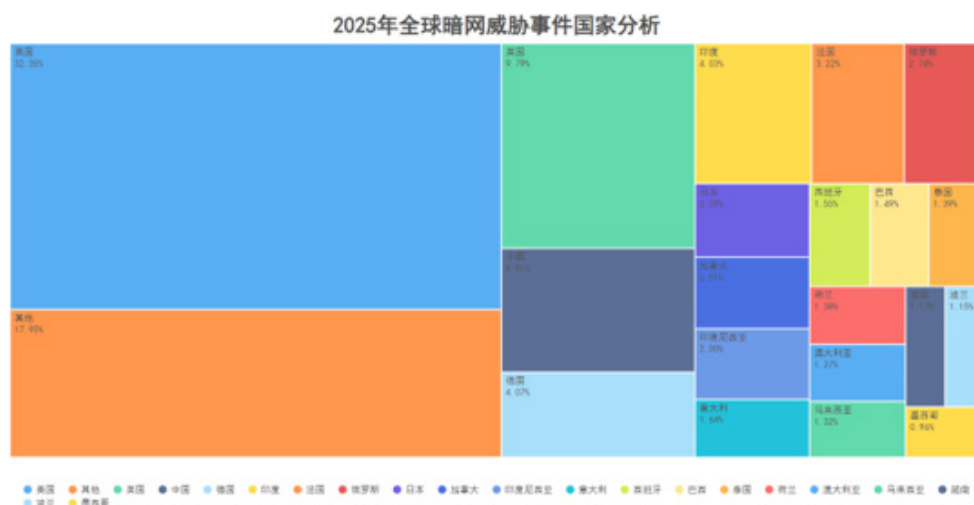
具备一定经济规模的地区，如美国以及英国、法国等欧洲发达国家。此类地区由于经济集中性，导致数据贩卖价值更高，暗网攻击呈现高暴利性，因此成为暗网黑客最多的攻击选择。

互联网用户规模大，如中国、美国、印度等地区。当前暗网中最主要的盈利方式是数据贩卖，数据贩卖的数据量级一般与当地互联网用户量级挂钩，所以此类地区更容易遭受暗网威胁。

地缘政治较为复杂区域，如美国、俄罗斯等地区。暗网中活跃着大量的暗网黑客组织。其中一部分黑客组织打着“网络义警”的旗号，但实际上却带有明显的政治倾向。这类黑客组织常常针对地缘政治复杂的区域发动定向攻击，并利用网络攻击来获取非法利益。他们的行为不仅破坏了网络安全，也对国际政治秩序构成威胁。



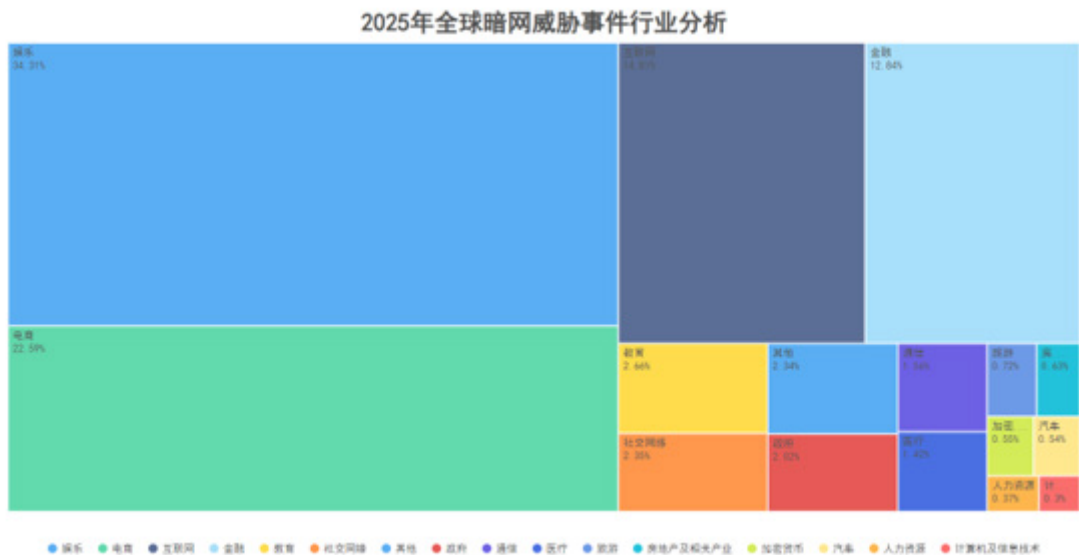
(图7 全球暗网威胁事件国家分布热力图)



(图8 全球暗网威胁事件国家分析)

(三) 全球暗网威胁行业分布

2025年度全球暗网威胁事件涉及行业达到47种,盛邦安全监测发现全球暗网可统计的且具有明确行业指向的可统计的威胁事件数量为184,796起。从行业划分上来看,与去年相同,2025年全球受暗网影响最深的是娱乐行业,相关暗网威胁事件占有所有事件的34.31%,其次为电商行业,占全部数量的22.59%,紧接着是互联网、金融行业,占比分别为14.81%、12.84%,其余行业均未超过威胁事件总数的3%,图9展示了全球受暗网影响的TOP15行业分布,其中其他行业类型(占比2.34%)涵盖了商业、运输、国防航天等32个行业类型。



(图9 全球暗网威胁事件行业分析TOP15)

根据全球暗网威胁行业分布情况可以发现，暗网全球威胁在行业上的分布主要集中在娱乐行业、电商、互联网以及金融四个行业，四个行业发生的暗网事件数量占比达到84.54%。娱乐行业连续两年在全球行业影响排名第一位，主要原因在于暗网中存在大量的盗版视频、影像贩卖事件。电商行业则由2024年的8.01%大幅升至22.59%，成为第二大受影响行业，反映黑产正明显转向订单、支付、物流、地址、消费画像和商户数据等可直接用于诈骗、撞库、薅羊毛和供应链攻击的高价值数据。

总体来看，全球暗网攻击正从以娱乐和互联网账号泄露为主，进一步向“娱乐账号规模化、电商数据高频化、金融数据高价值化”的方向演进，攻击者更关注能够快速变现、支撑精准诈骗和跨平台渗透的数据资产，相关行业需重点加强账号凭证防护、交易风控、API接口安全、供应链数据保护和暗网泄露监测。

(四) 全球受影响主体规模分布

对全球受影响企业进行分析，其中受影响最深的企业包括亚马逊公司 (Amazon，是一家位于美国华盛顿州的西雅图的集电商、云计算、人工智能、线下实体书店等于一体的消费和科技公司)、美国奈飞公司 (Netflix，简称网飞，是一家会员订阅制的流媒体播放平台，总部位于美国加利福尼亚州洛斯盖图)、雅虎 (Yahoo，1994年由杨致远和大卫·费罗创立，最早从网络目录和搜索引擎起步，迅速拓展为涵盖邮件、新闻、财经、体育等服务的门户巨头)、PayPal (成立于1998年，原名Confinity，以让个人和商户通过电子邮件安全收发款项而迅速崛起)、Crunchyroll (美国的一家提供动画、漫画、戏剧、音乐等东亚流媒体服务和国际交流社区的网站)，图10为全球受影响企业TOP50，在全球受影响企业的前50中，中国仅有阿里巴巴集团 (Alibaba) 在名单内。



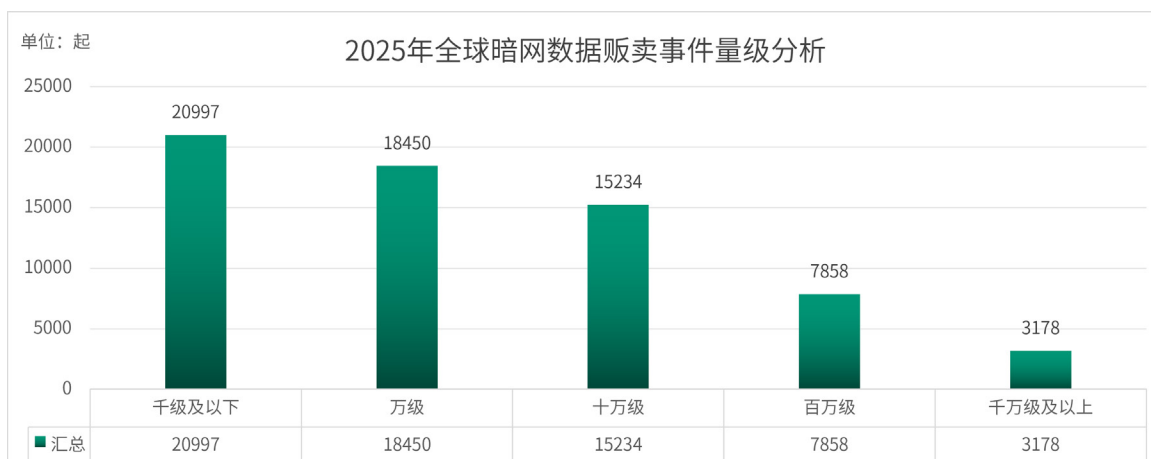
(图10 全球受暗网威胁影响企业排名TOP50)

二、2025年全球数据贩卖情况分析

(一)全球暗网威胁数据贩卖量级分析

2025年度全球暗网发生的可统计的数据贩卖事件共计65,717起,其中千级及以下级别数据贩卖事件数量最多,为20,997起,占总数的31.95%,其次是万级数据贩卖事件,数量达到18,450起,占比达到28.07%,千万级以上的数据占比最少,数量仅为3178起,只占总数的4.84%。

相较于2024年数据贩卖专职黑客基于已有的数据集通过特定属性归类查询的数据的攻击模式，2025年攻击方向产生了新的变化。如图11所示，全球暗网攻击和数据贩卖的量级呈现“轻量化”贩卖趋势，千级以下和万级数据的占比较去年出现了大幅增长，同时也意味着并非一味单纯追求超大规模“整库泄露”，而是更倾向于围绕账号凭证、客户信息、订单记录、地区或行业数据包进行分批窃取、拆分包装和持续变现，这种模式既有利于黑产降低暴露风险、规避溯源打击，也更符合诈骗、撞库、钓鱼、精准营销和勒索等下游场景对“新鲜、精准、可验证”数据的需求。

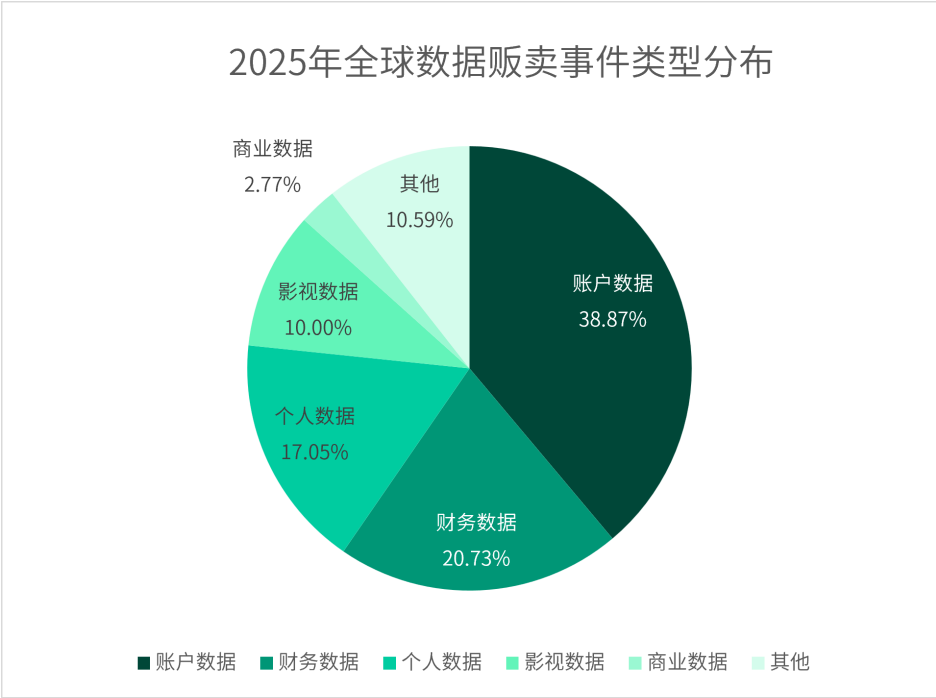


(图11 全球暗网数据贩卖事件量级分析)

(二) 全球暗网威胁数据贩卖类型分析

2025年，针对全球暗网数据贩卖事件的泄露来源类型分析可以发现，账户数据的占比最高，达到了38.87%，排名第二的数据贩卖类型为财务数据，占比为20.73%，其他三个排在前五位的来源类型为个人数据、影视数据（主要为盗版、枪版视频贩卖，非法视频转载等）、商业数据（主要为从事商业活动的非公开记录），分别占比17.05%、10.00%以及2.77%，其他数据类型（涵盖类型共计31种，包括但不限于日志数据、数据库数据、黑客工具、影视数据等）共占比10.59%。

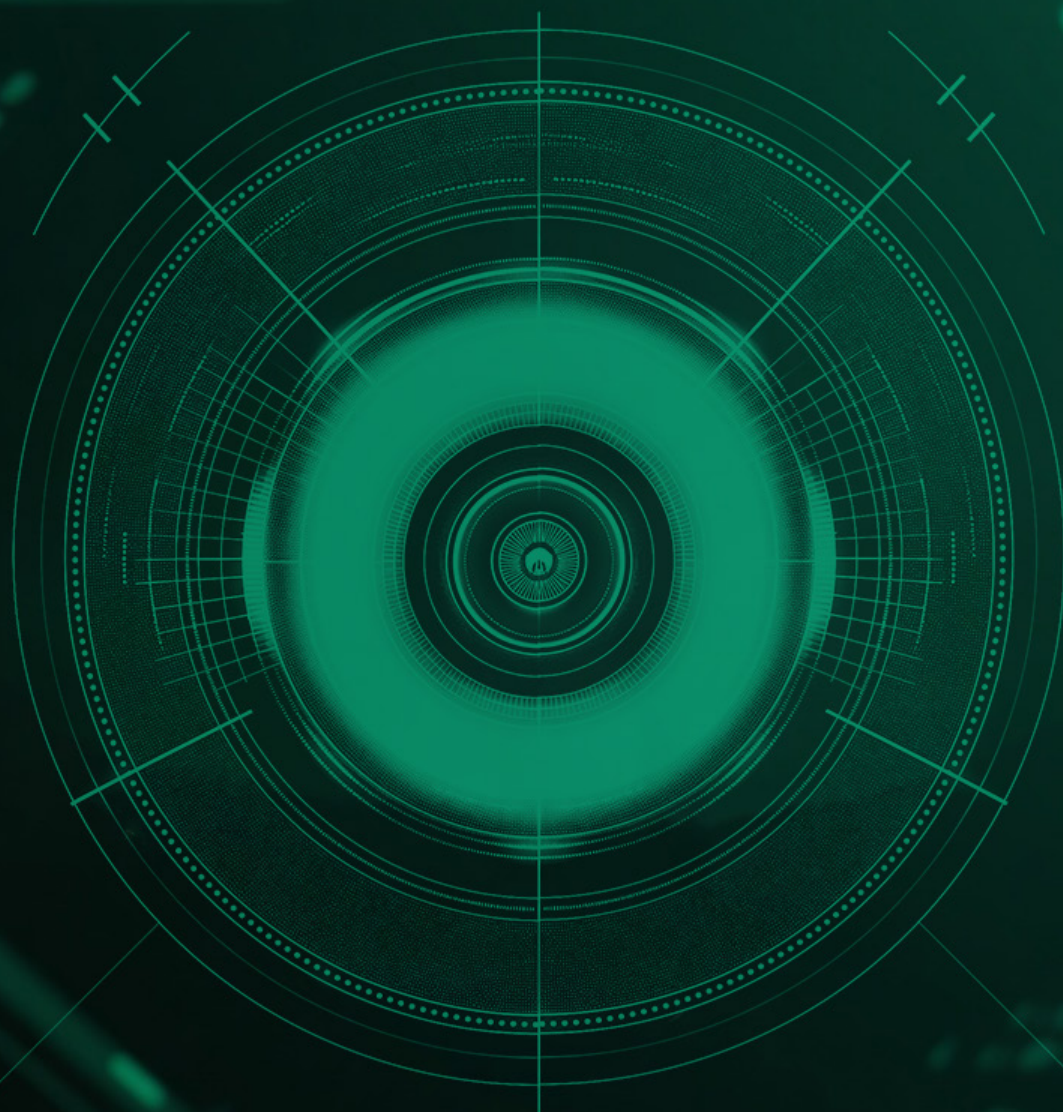
从全球暗网数据贩卖类型看，2025年与2024年相比呈现出明显的“去个人信息单一化、向账户凭证和业务数据转移”的趋势：2024年个人数据占比高达58.13%，是绝对主流，而2025年个人数据降至17.05%，说明传统大规模个人信息库贩卖的相对占比明显下降；与此同时，账户数据由2024年的19.46%升至2025年的38.87%，成为首要类型，反映黑产更重视可直接用于撞库、盗号、接管账号、横向渗透和诈骗变现的登录凭证类数据。影视数据以10.00%进入前列，也与全球娱乐行业暗网事件高发相互印证，体现盗版内容、非法转载和账号权益交易仍具活跃市场。总体来看，全球暗网攻击正从“批量泄露个人信息”转向“获取可登录、可交易、可精准诈骗、可业务渗透的数据资产”，攻击目标更加贴近账号体系、平台业务、客户关系和内容版权变现链条，相关行业应重点加强账号凭证防护、客户数据分级保护、异常登录监测、API接口安全和暗网泄露情报联动处置。





第三章

2025年度核心暗网威胁事件 监测分析

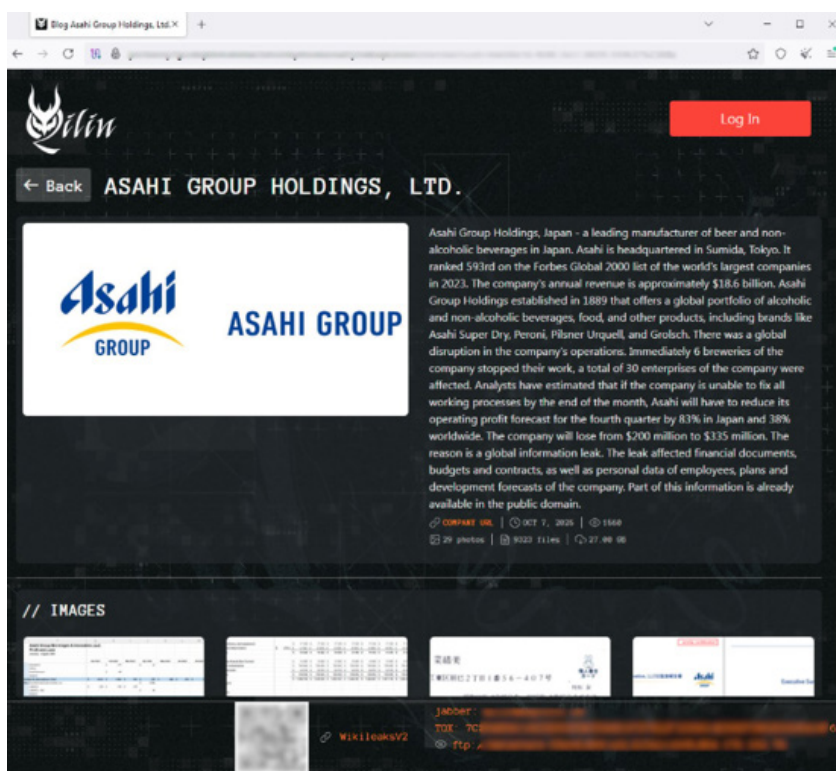


2025年,全球暗网威胁生态完成根本性代际迭代,与地缘政治博弈、前沿技术武器化、新兴资产攻击、黑产产业化升级深度绑定,已从传统地下犯罪黑市,彻底演变为混合战争对抗的隐秘前线、国家情报博弈的核心枢纽、全球网络犯罪产业化升级的关键引擎。本章基于全年暗网生态7×24小时全域监测数据,系统梳理年度全球暗网核心威胁事件,从活跃攻击组织动向、重大数据泄露贩卖事件、恶意软件与零日漏洞交易、全球执法打击与治理重构、“犯罪即服务”供应链演进五大维度,深度剖析2025年暗网威胁事件的演化特征、传导路径与风险态势。

一、全球暗网活跃组织威胁事件

(一) Qilin勒索组织袭击日本朝日集团

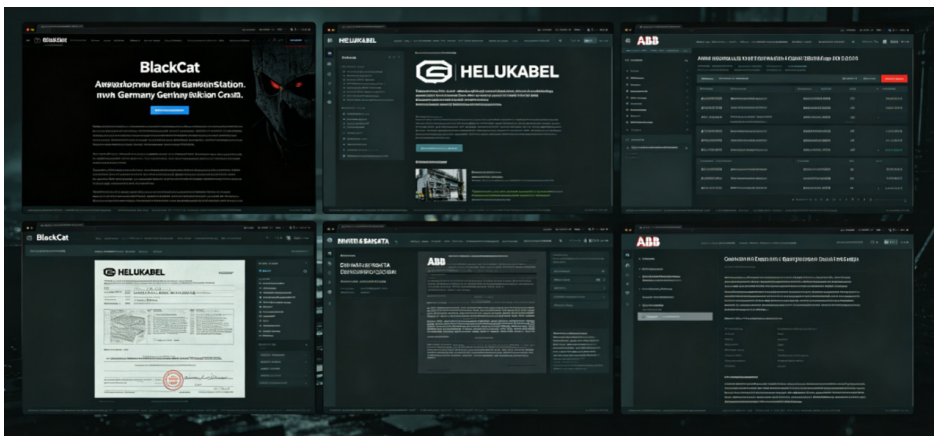
2025年初,Qilin勒索软件组织(以高技术门槛和针对大型企业的精准打击著称)宣称对日本朝日集团发起网络攻击。该组织在暗网泄密站公布了部分窃取的内部数据,涉及财务报表、供应链合同及员工个人隐私。Qilin通过利用高度定制化的多态加密载荷绕过了朝日集团的传统端点防御,此次事件不仅导致该集团部分媒体内容生产系统与生产线短暂中断,更暴露出全球食品饮料与传媒巨头在跨境供应链安全管理中的薄弱环节。



(图13 Qilin 勒索组织针对朝日集团攻击公告发布)

(二) BlackCat (ALPHV) 针对欧美制造业集群攻击

2025年上半年, BlackCat (ALPHV) 勒索组织针对欧美地区的精密制造业集群发起了一系列连锁攻击。该组织利用“三重勒索”策略, 不仅加密了受害企业的核心生产控制系统, 还威胁将专利设计图纸、生产工艺参数在暗网进行拍卖, 同时向企业上下游合作方同步泄露攻击信息施压。这一系列攻击导致德国、美国等多家汽车供应链核心厂商生产线出现阶段性停摆, 全球供应链交付延迟, 凸显了暗网勒索组织从单纯的数据窃取向深度破坏生产连续性的战术转型, 显著加剧了高端制造业的运营风险。



(图14 BlackCat 组织欧美制造业集群攻击成果公示)

(三) APT29 (Cozy Bear) 关联暗网情报交易

2025年全年监测发现, 具有俄罗斯国家背景的 APT29 (Cozy Bear) 组织, 被频繁观测到利用暗网论坛作为其情报交换与资源募集的隐秘节点。APT29通过暗网渠道向初始访问经纪人 (IAB) 采购特定西方外交机构、政府部门的内网访问凭证, 并利用暗网的匿名性分发针对性的恶意脚本与免杀工具。这一动向标志着国家背景的APT组织正深度融入暗网黑产生态, 通过“采购 + 自研”的混合模式大幅提升其间谍活动的效能与隐蔽性, 暗网已成为全球地缘情报博弈的核心隐秘阵地。

“It seemed to us that we were being followed, as unfamiliar cars were standing in the yard, two bodies were sitting in the car.”
— KAGAS, A CONTI MEMBER, IN A LEAKED CHAT

Days later, Conti’s leaders talked about Cozy Bear’s work and referenced its ransomware attacks. Stern, the CEO-like figure of Conti, and Professor, another senior gang member, talked about setting up a specific office for “government topics.” The details were first reported by WIRED in February but are also included in the wider Conti leaks. In the same conversation, Stern said they had someone “externally” who paid the group (although it is not stated what for) and discussed taking over targets from the source. “They want a lot about Covid at the moment,” Professor said to Stern. “The cozy bears are already working their way down the list.”

“They reference the setting up of some long-term project and seemingly throw out this idea that they [the external party] would help in the future,” says Kimberly Goody, director of cybercrime analysis at the security firm Mandiant. “We believe that’s a reference to if law enforcement actions would be taken against them, that this external party may be able to help them with that.” Goody points out that the group also mentions Liteyny Avenue in St. Petersburg—the home to local FSB offices.

(图15 APT29 关联暗网情报交易帖文)

(四) Lapsus\$团伙南美政府机构数据泄露

2025年5月,全球知名激进黑客组织Lapsus\$在暗网发布公告,宣布攻破了巴西、阿根廷、智利等多个南美国家的税务与海关管理系统,并公开展示了约1TB的政府内部文档,包括公民身份信息、政府行政文件、公共安全系统部署方案等核心内容。该组织通过高超的社会工程学手段劫持了高权限运维账户,直接绕过了系统逻辑边界与安全防护。事件引发了相关国家公民对个人数据主权泄露的极大恐慌,也再次警示了数字政府建设中高权限身份全生命周期管理的极端重要性。



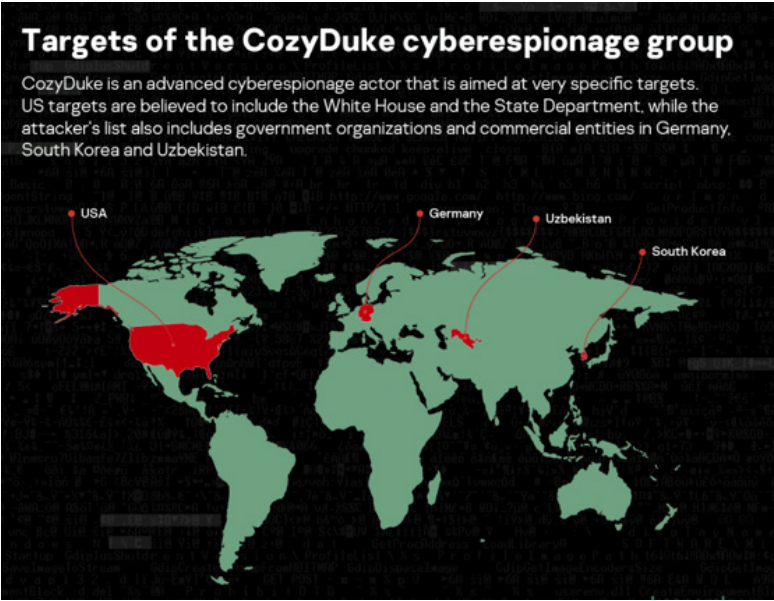
(图16 Lapsus\$ 团伙南美政府机构数据泄露公告)

(五) RansomHub登顶勒索软件生态位事件

在LockBit等传统头部勒索平台因全球执法打击而生态碎裂后,2025年中期,RansomHub通过优化利润分成模式、提供定制化免杀引擎,以及新增“不加密只窃密”的轻量化攻击工具,迅速吸引了全球大量附属攻击组织加入。监测数据显示,RansomHub在2025年第三季度占据了全球暗网勒索事件约30%的市场份额,附属攻击者数量、赎金总金额均跃居行业首位,正式登顶暗网勒索软件生态位。其生态位的快速崛起,充分体现了暗网勒索市场极强的自我修复能力与动态迁移特征。

(六) APT44(沙虫)针对乌克兰能源设施的联合破坏事件

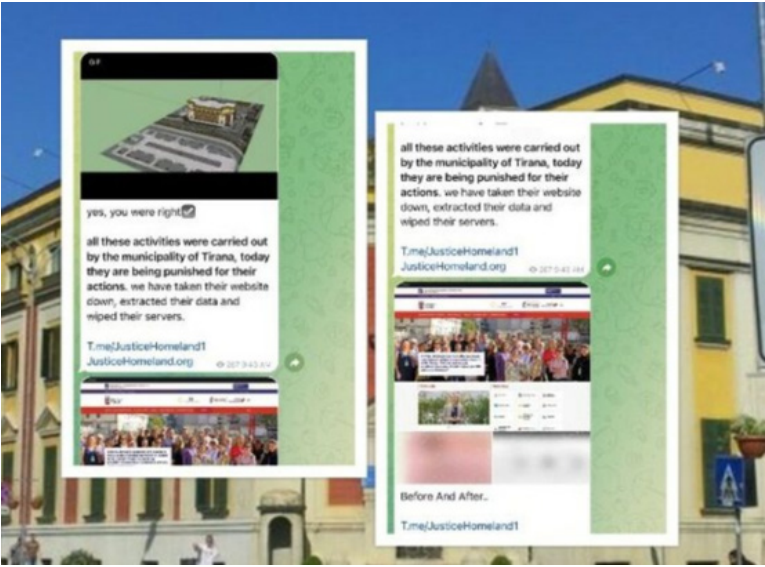
在LockBit等传统头部勒索平台因全球执法打击而生态碎裂后,2025年中期,RansomHub通过优化利润分成模式、提供定制化免杀引擎,以及新增“不加密只窃密”的轻量化攻击工具,迅速吸引了全球大量附属攻击组织加入。监测数据显示,RansomHub在2025年第三季度占据了全球暗网勒索事件约30%的市场份额,附属攻击者数量、赎金总金额均跃居行业首位,正式登顶暗网勒索软件生态位。其生态位的快速崛起,充分体现了暗网勒索市场极强的自我修复能力与动态迁移特征。



(图17 APT44 针对乌克兰能源设施攻击工具暗网分发)

(七) 地缘政治黑客组织“Homeland Justice”数据擦除事件

2025年, 带有强烈伊朗地缘导向的黑客组织“Homeland Justice”在暗网发布攻击公告, 声称对以色列和阿尔巴尼亚的政府机构、关键基础设施发起旨在永久破坏数据的“擦除器 (Wiper)”攻击。该组织不以经济牟利为目的, 而是通过销毁目标方的数字化业务底座、核心数据资产进行政治施压, 同时在暗网公开攻击工具与技术细节, 招募全球相关黑客组织协同参与。这一事件标志着暗网威胁已成为混合战争中破坏性最强的非对称手段之一, 地缘政治博弈正通过暗网实现网络攻击的全域传导。



(图18 Homeland Justice 组织攻击公告与数据擦除成果公示)

二、全球暗网重大数据贩卖事件

（一）“开盒”社工库大规模交易

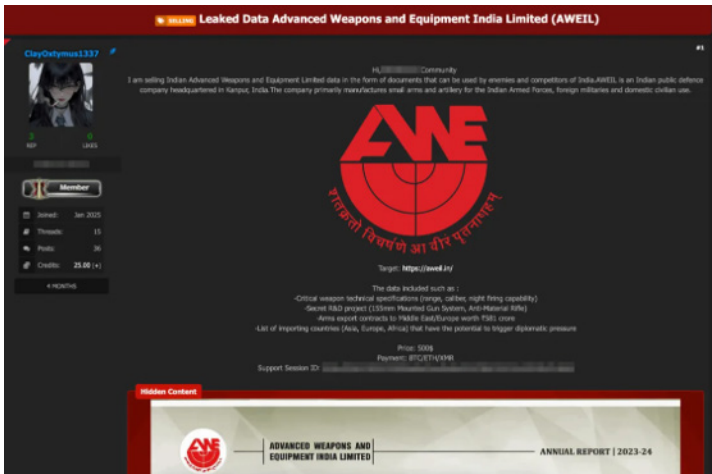
2025年，暗网中文区、俄语区、英语区核心交易平台，出现了多个集成化的“全能社工库”并形成大规模常态化交易，相关交易帖文全年累计超2.3万条。这些数据库涵盖了全球数亿用户的实名身份、手机号、家庭住址、出行记录及社交账号关联数据，通过自动化查询机器人(Bot)提供订阅制服务，单套完整社工库最高涵盖数据量超百亿条，极大降低了“人肉搜索”和精准钓鱼的技术门槛。此类社工库被广泛用于网络暴力、金融欺诈、定向勒索等违法犯罪活动，对全球公民数字隐私安全构成了系统性威胁。



（图19 暗网平台“开盒”社工库交易帖文）

(二) 印度政府最高机密文件售卖

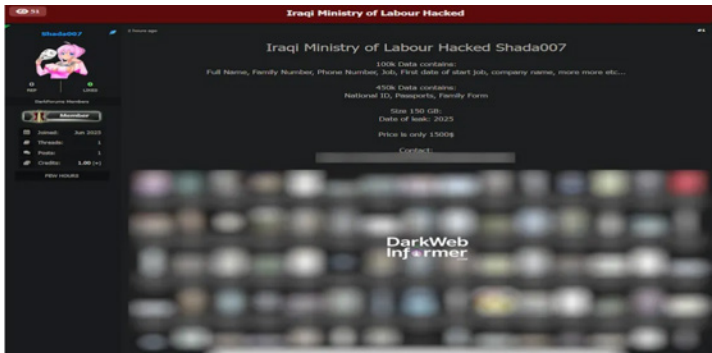
2025年3月，暗网某知名技术论坛出现一则重磅交易帖，宣称售卖涉及印度国防与外交决策的最高机密文件。卖家公开了部分脱密文件样本以证真实性，包括印度边境军事部署机密会议纪要、国防采购核心招标计划、高层外交战略部署图等内容，全套文件标价200万美元，仅接受门罗币匿名支付。尽管印度官方紧急启动调查，但数据在暗网的流转已对国家战略安全造成了不可逆的情报损失，深刻反映出暗网已成为国家级机密情报非法交易与流失的核心重灾区。



(图20 印度政府最高机密文件暗网售卖帖文)

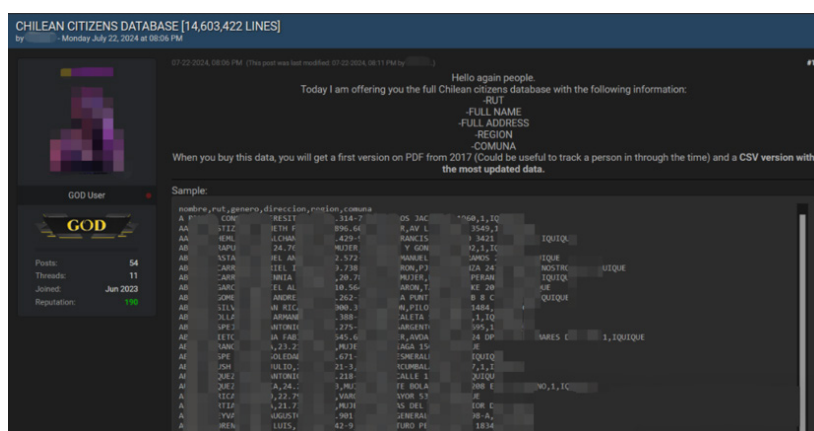
(三) 500GB 伊拉克政府数据免费泄露

为达成政治抗议目的，某匿名黑客组织在2025年夏季于暗网免费公开了高达500GB的伊拉克政府内部数据，内容涵盖内政部、司法部及公共安全部门的核心文件，包括超1200万条公民选民登记信息、政府内部行政往来邮件、公共安全系统部署方案等。这种“只泄露、不交易”的模式带有明显的网络激进主义色彩，旨在通过引爆舆论压力干扰政府正常运作，凸显了暗网数据泄露事件从经济牟利向社会政治影响延伸的核心特征。



(四) 通信内鬼售卖实时定位数据

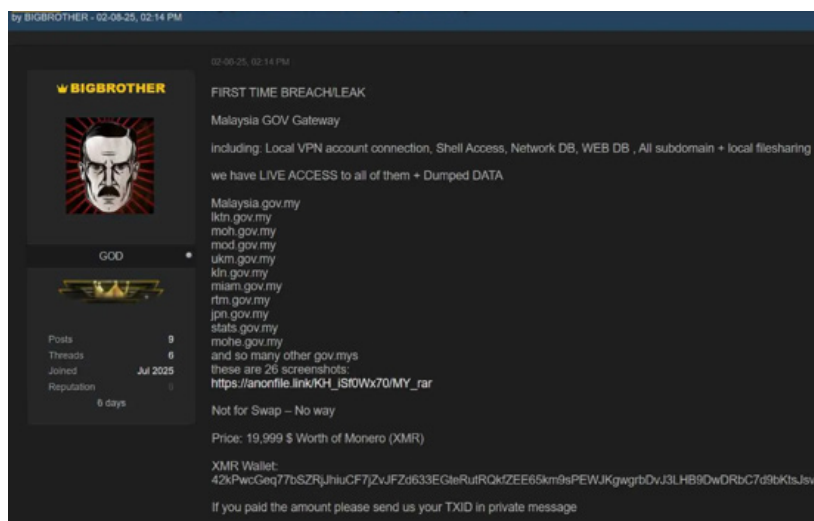
2025年全年监测捕获到多起针对全球主要电信运营商“实时信令接口”的访问权限暗网交易。攻击者通过收买通信行业内部人员,获取并倒卖特定目标的手机号码实时基站定位、历史出行轨迹、通话与短信记录等敏感数据,单次定位查询售价50-200美元不等,全量历史轨迹数据最高售价达2000美元。此类高溢价数据的非法流转,为跨境绑架、定向人身伤害、商业间谍等线下暴力犯罪与违法活动提供了关键技术支撑,社会危害性极大。



(图22 暗网通信实时定位数据交易帖文)

(五) 马来西亚 MYSA 航天局 + 选民数据泄露

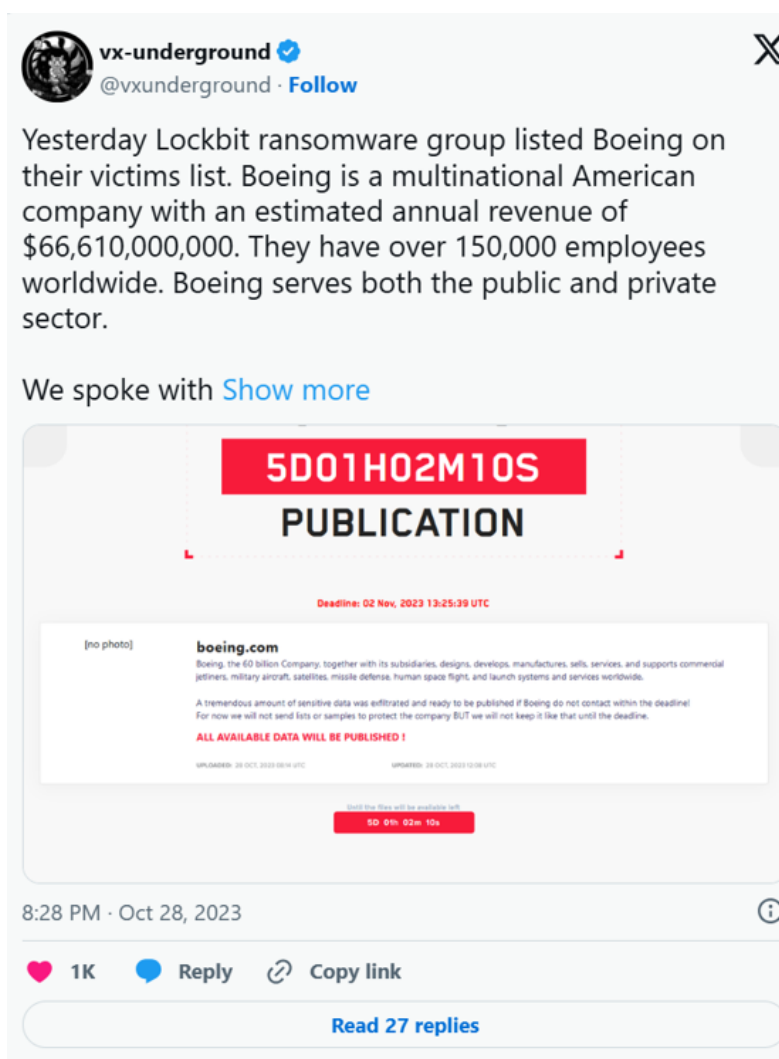
2025年,马来西亚航天局(MYSA)的部分卫星设计图纸、测控系统核心参数,与全国数百万选民的详细个人档案在暗网打包挂售。攻击者声称通过软件供应链漏洞,入侵了航天局第三方外包服务商的系统,同时渗透了马来西亚选举委员会内网。该事件标志着暗网数据贩卖目标已从传统的消费互联网领域,向航天科技、政治选举等高价值战略红区全面渗透,网络威胁边界正式向国家空天基础设施与政治安全领域延伸。



(图23 马来西亚 MYSA 航天局与选民数据暗网售卖公告)

(六) 波音公司(Boeing)核心数据遭 LockBit 窃取事件

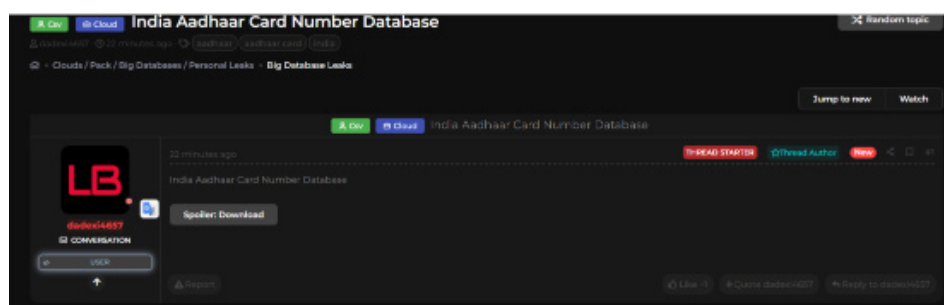
2025年1月, LockBit残余团伙利用被盗的企业内部运维凭证, 成功入侵波音公司内网, 窃取了包含民用飞机关键零件设计图纸、军用航空项目参数、供应商成本清单在内的核心商业与技术资产。该批数据在暗网标价数千万美元, LockBit 团伙以“不支付赎金即全量公开”向波音公司施压。此次事件引发了全球航空航天领域对供应链数字主权的深度忧虑, 也印证了即使是全球顶级关键基础设施企业, 在面临针对性凭证窃取与定向攻击时依然存在显著脆弱性。



(图24 LockBit 团伙波音公司攻击事件公告)

(七) 印度 Aadhaar 全国身份证系统大规模失陷事件

2025年2月,涉及印度12亿公民的Aadhaar 全国身份证系统核心数据,在暗网某私密社群被大规模公开。泄露数据包含公民姓名、身份证号、家庭住址,以及虹膜、指纹等不可重置的生物识别特征信息,单条数据售价低至0.1美元。生物数据的不可重置性决定了该事件的破坏力是永久性的,它不仅动摇了印度的数字化身份根基,也为全球生物特征识别认证体系的安全防护敲响了警钟。



(图25 印度 Aadhaar 身份证系统数据暗网售卖帖文)

(八) 欧洲航天局 (ESA) 供应链攻击与700GB数据泄露事件

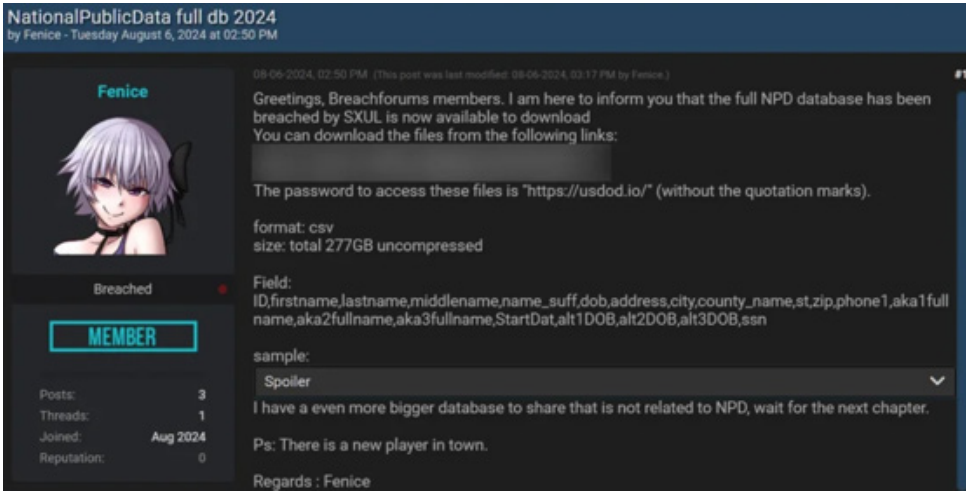
2025年12月,欧洲航天局 (ESA) 遭遇史上最严重的数字泄密事件,700GB涉及空天协议规范、低轨卫星测控链路参数、航天项目设计文档及供应商核心合同的敏感数据,被攻击者窃取并在暗网大规模流转。监测显示,这些数据随后被多国APT组织下载研究,攻击者通过第三方软件供应商的系统漏洞完成供应链迂回渗透。该事件清晰地展示了“供应链入侵→核心资产窃取→暗网扩散→定向攻击”的空天资产完整威胁闭环,成为2025年全球商业航天领域影响最重大的网络安全事件。



(图26 欧洲航天局核心数据暗网售卖帖文)

(九) 29 亿条公民 SSN (社会安全号码) 数据全量公开事件

2025年上半年，暗网监测到单起超大规模数据泄露事件，近30亿条包含美国公民个人姓名、出生日期、社保号 (SSN)、家庭住址、银行账户关联信息的完整记录被全量免费公开。数据规模之巨让传统个人信息防护手段几乎失效，这些数据在后续被广泛用于身份盗用、金融欺诈、精准钓鱼等违法犯罪活动，成为2025年下半年全球身份窃取类犯罪的核心“原材料工厂”，也创下了全球历史上单次公开的公民身份数据规模之最。

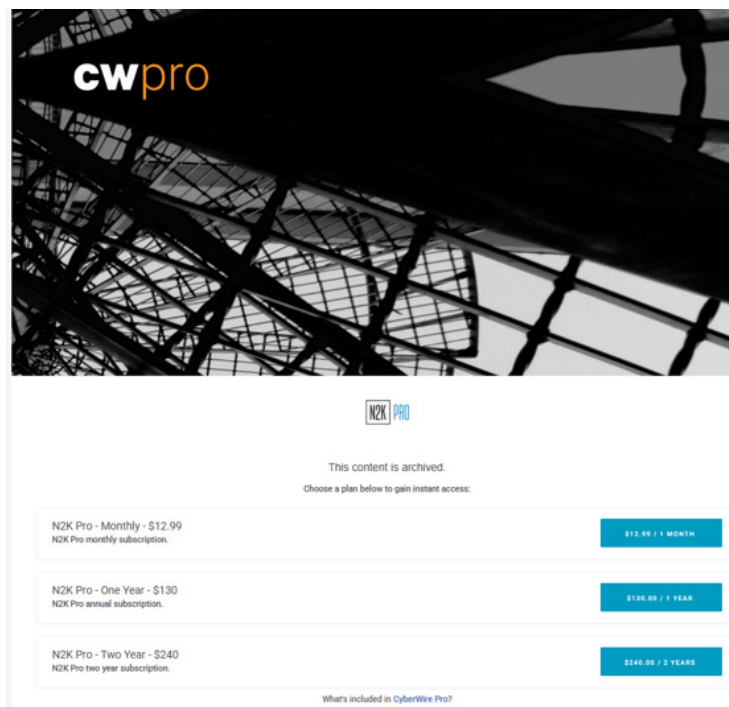


(图27 二十九亿条公民 SSN 数据暗网免费公开公告)

三、全球暗网恶意软件与零日漏洞威胁

(一) BazarLoader 暗网订阅制售卖

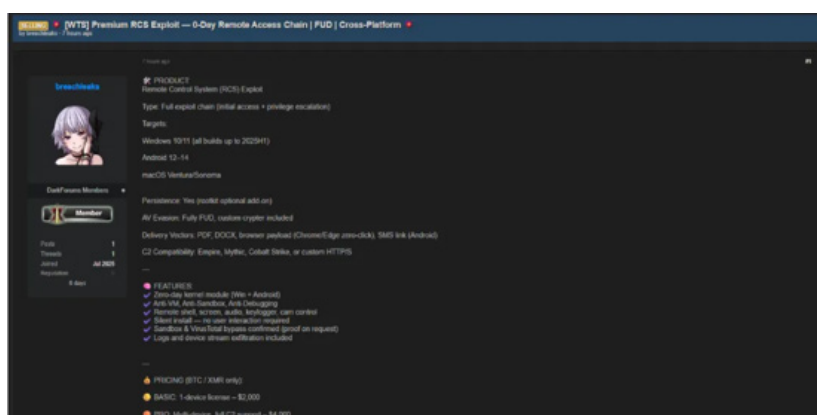
2025年，老牌木马BazarLoader完成核心架构升级，在暗网正式开启“订阅制 (SaaS)”售卖模式，成为暗网“犯罪即服务”体系中最活跃的初始访问工具。该升级版本引入了先进的沙箱检测绕过算法和流量混淆模块，专门为勒索软件团伙、APT组织提供目标网络初始渗透支撑，分为基础版、专业版、企业定制版三个订阅档位，全年累计订阅用户超6000个。其订阅模式的普及，使得中小型犯罪团伙能够低成本获取顶级入侵能力，直接加速了全球网络威胁的规模化扩散。



(图28 BazarLoader 暗网订阅制售卖页面)

(二) Windows 内核零日漏洞暗网拍卖

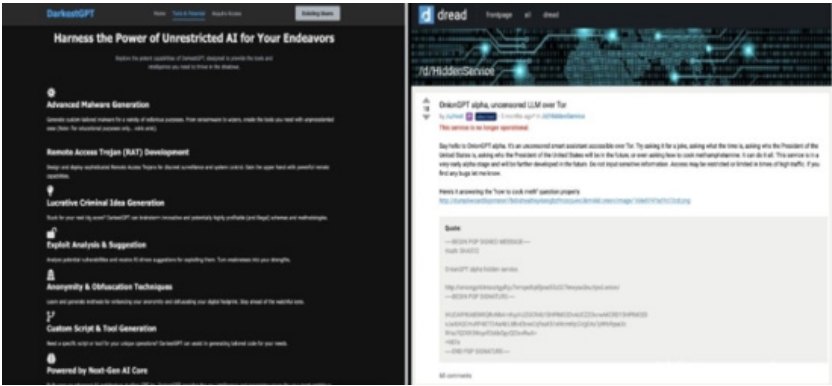
2025年上半年，暗网监测到单起超大规模数据泄露事件，近30亿条包含美国公民个人姓名、出生日期、社保号 (SSN)、家庭住址、银行账户关联信息的完整记录被全量免费公开。数据规模之巨让传统个人信息防护手段几乎失效，这些数据在后续被广泛用于身份盗用、金融欺诈、精准钓鱼等违法犯罪活动，成为2025年下半年全球身份窃取类犯罪的核心“原材料工厂”，也创下了全球历史上单次公开的公民身份数据规模之最。



(图29 Windows 内核零日漏洞暗网拍卖帖文)

(三) AI生成勒索病毒工具包

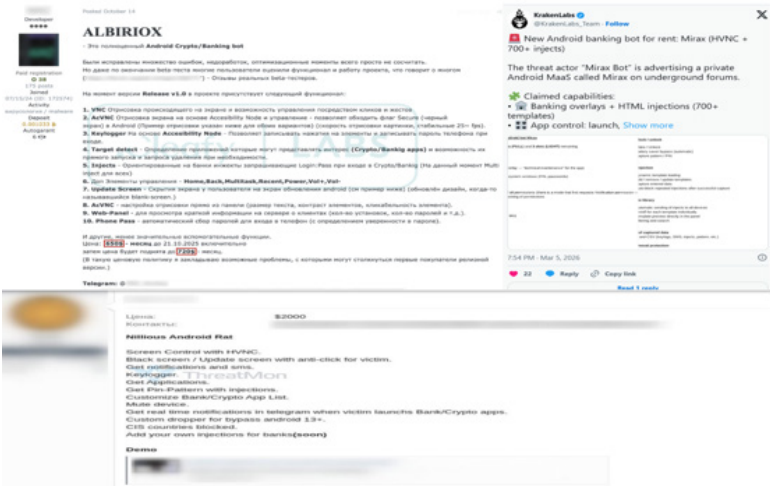
2025年，监测捕获到暗网正式上架首款利用生成式AI自动编写的勒索病毒工具包，并快速成为交易市场热门品类。该工具内置大语言模型，允许用户通过自然语言描述其攻击目标与需求，AI会自动生成多态恶意代码、定制化勒索信与配套解密程序，可有效规避传统安全设备的特征库检索。这种“智能平权”彻底降低了恶意软件的研发门槛，零基础攻击者即可快速生成高规避能力的勒索病毒，直接导致2025年全球勒索软件变种数量呈现指数级增长。



(图30 AI 生成勒索病毒工具包功能介绍与交易帖文)

(四) 安卓银行木马新变种批量上架

针对全球移动支付的快速渗透，2025年暗网市场出现了大量针对安卓系统的银行木马新变种，以改进型 Medusa、Godfather为代表的木马家族成为交易主流。这些木马集成了实时屏幕劫持、2FA短信拦截、生物认证绕过、远程控制等核心功能，专门攻击全球跨境在线支付APP与手机银行客户端，采用订阅制与单次定制相结合的售卖模式。2025年全球超70%的移动端银行盗刷事件，均可追溯至暗网售卖的此类木马，标志着黑产攻击重心正加速向移动端金融资产转移。



(图31 安卓银行木马新变种暗网交易帖文)

(五) JetBrains TeamCity 供应链漏洞闪电式利用事件

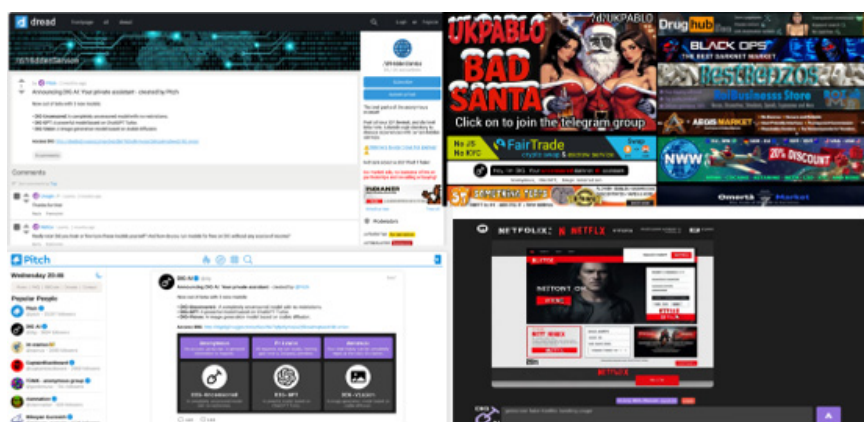
2025年2月，JetBrains官方发布TeamCity持续集成与部署平台高危远程代码执行漏洞公告，并同步推送修复补丁。公告发布后不到24小时，暗网核心技术论坛即出现了成熟的自动化攻击脚本（PoC）与利用工具，大量黑产组织利用该脚本对全球互联网暴露的TeamCity服务器进行批量扫描与投毒，获取企业开发环境高权限访问权限。这种“发现即武器化”的闪电速度，让企业常规的补丁修复周期面临极限挑战，也凸显了暗网在高危漏洞武器化扩散中的核心加速作用。



（图32 JetBrains TeamCity 漏洞利用代码暗网发布）

(六) “DarkAgent V3.0”AI 攻击智能体商用化事件

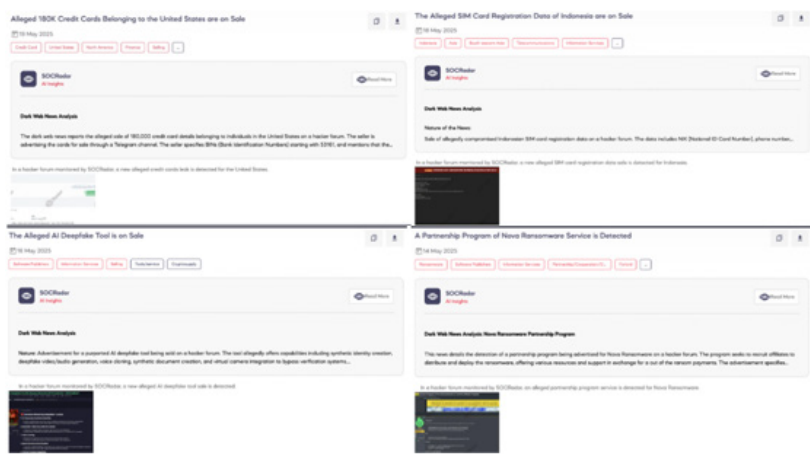
2025年8月，全球首款商用级AI攻击智能体DarkAgent V3.0在暗网正式发售，成为年度最具颠覆性的黑产技术迭代。该工具内置多模态大模型与自主规划能力，支持无人化执行从信息侦察、漏洞挖掘、渗透入侵到数据窃取、痕迹清理的全流程攻击任务。监测数据显示，其将原本需要2周的人工渗透任务压缩至3天以内，平均攻击链周期仅2.8天，较传统人工攻击缩短85%，该事件标志着网络攻击正式跨入“智能体 (Agent)”时代。



（图33 DarkAgent V3.0 AI 攻击智能体产品介绍与交易页面）

(七) ForgePro AI 深度伪造套件爆发事件

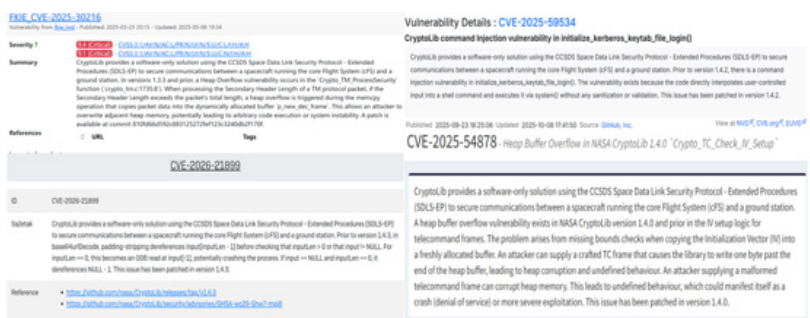
2025年, ForgePro AI深度伪造套件在暗网交易额迎来爆发式增长, 成为年度交易量最高的AI黑产工具。其核心能力是“10秒音频克隆+高拟真AI换脸+生物特征伪造”, 仅需少量公开样本即可生成能绕过人工辨识与KYC验证的高逼真伪造内容, 被广泛用于商业邮件入侵 (BEC)、高管语音诈骗、勒索攻击等场景。该工具导致全球多家企业财务部门因误信伪造的CEO视频/语音指令发生巨额资金损失, 其爆发式普及体现了深度伪造技术已从实验室走向大规模黑产实战, 对全球数字信任体系构成根本性挑战。



(图34 ForgePro AI 深度伪造套件功能演示与交易帖文)

(八) CCSDS 空天协议专属漏洞交易闭环事件

2025年, 暗网首次出现针对CCSDS (航天数据系统咨询委员会) 协议的专属利用载荷与完整漏洞交易, 形成了“漏洞挖掘→武器化开发→暗网交易→定向攻击”的成熟闭环。黑产组织通过交易这些底层协议漏洞, 试图对低轨卫星的测控链路进行非法注入、窃听与劫持测试, 相关漏洞利用工具标价最高达80万美元, 配套的卫星终端攻击服务实现标准化租赁。这一趋势标志着暗网技术威胁已正式突破地表互联网限制, 向空天战略资产全面延伸, 网络安全与太空安全实现深度绑定。



(图35 空天协议专属漏洞交易事件)

四、全球暗网核心平台执法打击与治理重构事件

（一）全球“RapTor 行动”捣毁暗网毒品/武器市场

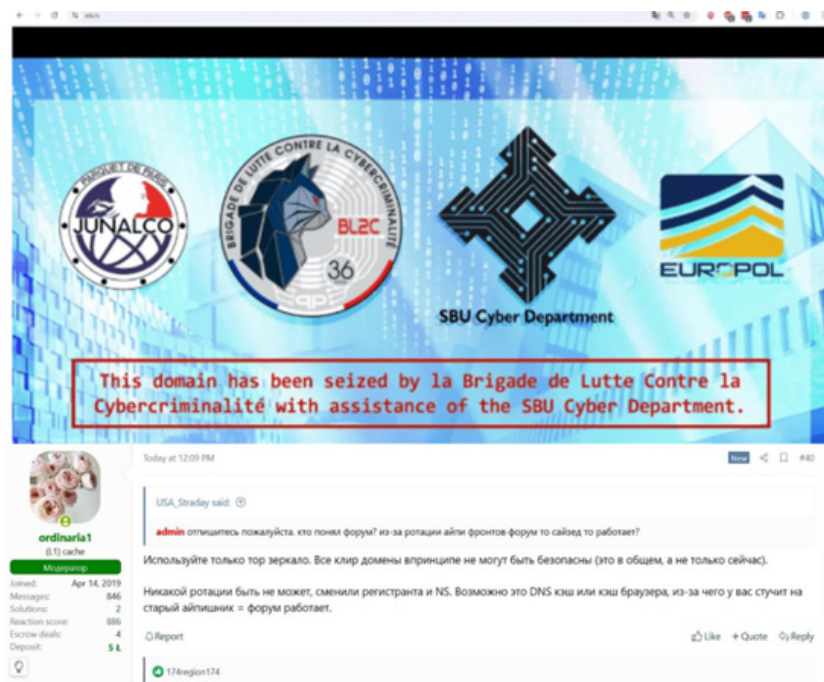
2025年初，由欧洲刑警组织牵头，联合美国FBI、德国联邦刑事警察局、法国国家警察等全球16个国家的执法机构，发起代号为“Operation RapTor”的全球暗网联合执法行动。此次行动成功查封了三个顶级暗网非法交易市场，捣毁了Tor网络中规模最大的毒品、武器黑市“Kraken”及其6个附属平台，抓获核心运营者、卖家等犯罪嫌疑人287名，查获超5080万欧元的现金与加密货币、850公斤违禁毒品、117件枪支武器。此次行动通过深入的链上资金追踪和节点物理定位，重创了暗网非法违禁品交易链，迫使相关黑产流量向更为碎片化的私密社交群组迁移。



（图36 全球“RapTor 行动”执法成果官方公示）

（二）XSS 俄语漏洞论坛关停与反复

作为全球俄语区最重要的零日漏洞交易、恶意软件开发、网络攻击技术交流核心阵地，XSS论坛在2025年经历了数次因执法打击、拒绝服务攻击和管理层内部震荡导致的暂时关停。2025年5月，俄罗斯执法机构联合国际刑警组织首次关停该论坛，查封核心服务器并逮捕运营团队核心成员，但仅1个月后，原技术团队便在暗网重新搭建全新平台，3个月内用户活跃度恢复至关停前的80%。这种核心节点的不稳定性导致了黑产情报流向的暂时阻塞，也反映出暗网内部社区在面临外部合规压力与内部信用危机时，兼具极强的脆弱性与动态抗打击韧性。



（图37 XSS 俄语漏洞论坛关停公告与新平台重建公告）

（三）BreachForums (英语数据泄露核心站) 治理震荡

2025年，全球英语区最大的数据泄露核心论坛BreachForums，在多次被执法查封与复活的循环中，管理权限频繁易主，全年陷入持续的治理震荡。这一震荡过程导致了大量历史脱库数据的流失与非法公开，同时也催生了多个从原论坛分裂出来的分支站点，使得全球数据泄露交易渠道呈现出“去中心化、多极化”的重构态势。论坛的持续动荡，也直接推动暗网数据泄露交易从“门户论坛模式”向私密加密社群快速迁移。



（图38 BreachForums 论坛管理权限交接公告与用户分流相关帖文）

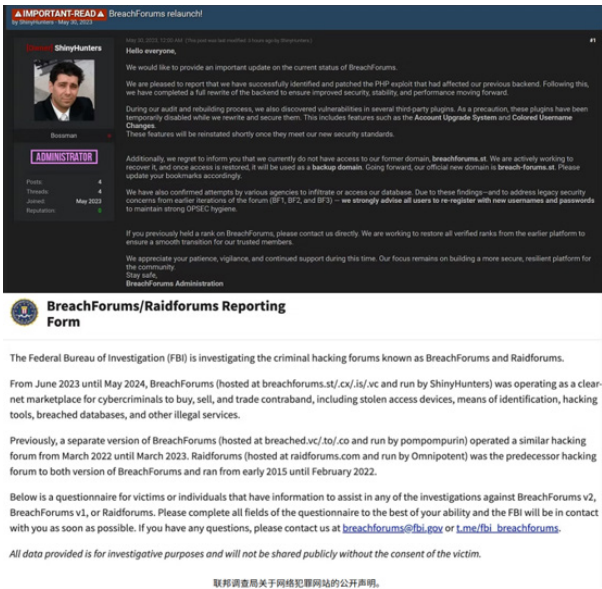
同年10月份,美国FBI与法国警方通过长达一年的跨境潜伏卧底行动,彻底控制了BreachForums论坛的核心后端服务器,抓获了平台主要运营者、技术负责人与核心管理员。事件发生后,ShinyHunters等暗网头部黑客大佬随后在暗网公开宣布“论坛时代终结”,这一事件成为关键转折点,标志着暗网数据泄露交易从集中化的“门户论坛模式”,向碎片化、私密化的“加密社交社群模式”完成代际转折。



(图39 美法联合执法行动官方公告与 BreachForums 平台关停)

(四) Hydra后继平台“WhiteHouse”被端

2025年中期,曾试图接替俄罗斯Hydra暗网市场份额、成为俄语区头部非法交易平台的“WhiteHouse”,被欧洲执法机构彻底查封。该平台曾以高度严密的PGP加密通信、完善的信誉担保体系和全品类非法商品交易著称,是2024-2025年暗网增长最快的交易平台。其覆灭证明了全球执法机构在暗网平台“脱匿名化”追踪技术上的关键突破,显著压降了2025年暗网大宗非法商品的流通效率,重创了Hydra覆灭后重建的俄语区暗网黑市生态。



（图 40 “WhiteHouse”平台查封公告与执法行动查获资产公示）

（五）Huione Guarantee (汇旺担保) 非法资金链关联打击事件

2025年下半年，全球多国执法部门针对暗网一站式非法金融平台Huione Guarantee支撑的洗钱网络，开展了多维度协同阻断行动。通过限制与其关联的非法跨链桥接口、查封核心资金池节点、取缔上下游合作服务商，黑产赃款的跨链混淆与套现周期被大幅拉长，资金清洗成本显著提升。该行动有效切断了暗网犯罪的“血液供应”，是2025年全球治理暗网黑色经济闭环、打击“洗钱即服务”生态的标志性胜利。

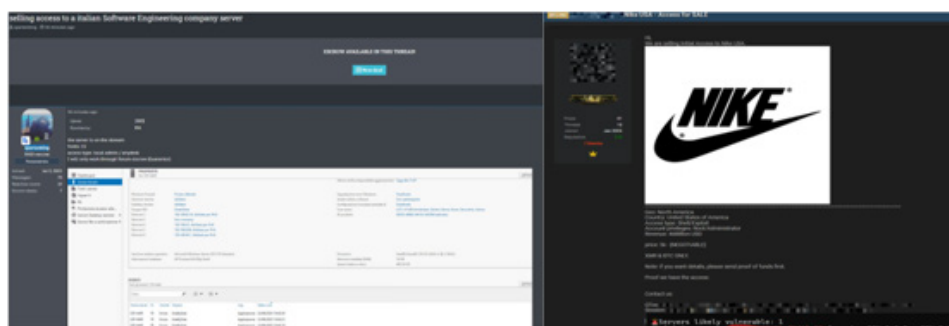


（图 41 Huione Guarantee 平台非法资金链路查封公告）

五、全球暗网“犯罪即服务”供应链演进威胁

(一) IAaaS 初始访问服务

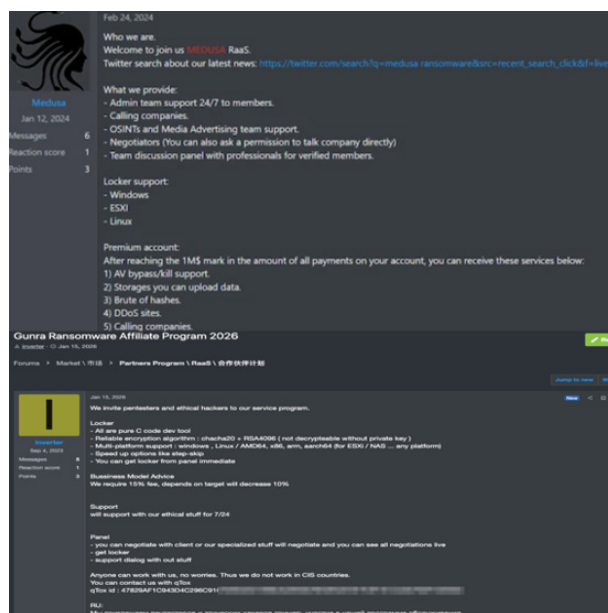
2025年,初始访问即服务(IAaaS)在暗网完成标准化、商品化转型,成为攻击链上游最核心的基础服务。初始访问经纪人(IAB)不再售卖低质零散的账号凭证,而是提供“已绕过MFA、附带内网全景画像、具备高权限”的企业/机构内网访问权限,按目标企业规模与权限等级明码标价。这种服务化供应模式,让下游黑客无需掌握专业渗透技能即可一键入侵大中型机构,成为2025年全球勒索攻击、数据窃取事件高发的核心催化剂。



(图42 暗网 IAaaS 初始访问服务交易帖文与报价)

(二) RaaS 勒索服务升级

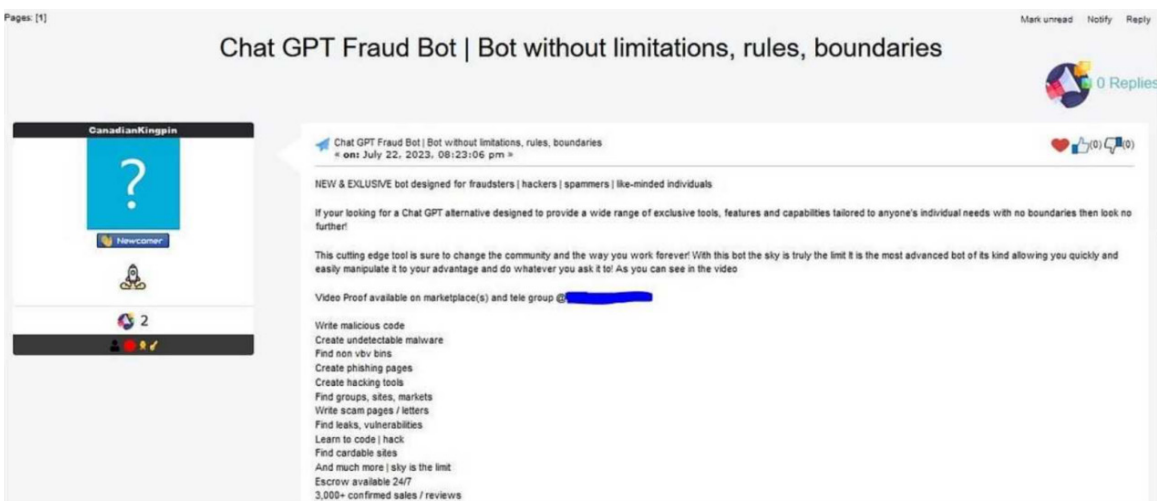
2025年,勒索软件即服务(RaaS)完成全链条业务升级,运营商不再仅提供基础的恶意软件工具,而是将其升级为包含“职业赎金谈判外包、三重勒索套件、受害者舆论打压服务、数据泄露分发”在内的全流程业务外包模式。同时,头部平台进一步优化利润分配规则,附属攻击成员的分成比例大幅向攻击者倾斜,这种极具竞争力的商业模式,极大地增强了勒索软件生态的韧性与全球扩张能力。



(图43 暗网头部 RaaS 平台服务体系介绍与分成规则公示)

(三)AlaaS 深度伪造与智能体服务

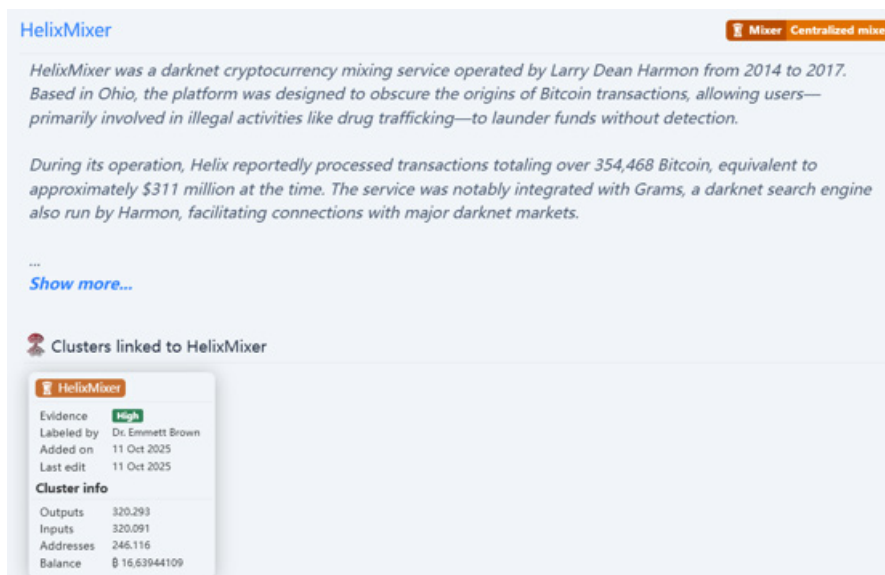
在AI黑产全面服务化的浪潮下，2025年暗网形成了成熟的AI即服务 (AlaaS) 完整产业链。从生成高拟真钓鱼邮件、个性化社会工程学内容，到实时语音克隆接口、AI攻击智能体调用，所有AI黑产能力均以API或模块化套件形式在暗网出售，按调用次数或订阅制收费。这标志着黑产技术能级实现了代际跨越，使得针对全球金融机构、跨国企业的高端欺诈攻击活动，呈现出规模化、常态化、高成功率的核心特征。



(图44 暗网 AlaaS 服务平台功能列表贴文)

(四)Laas非法金融洗钱服务

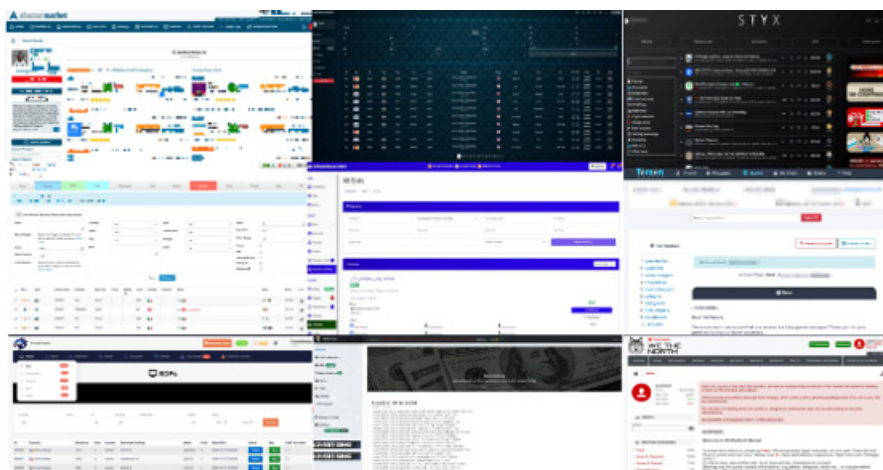
2025年，“洗钱即服务 (Laas)”完成了去中心化、自动化的全面升级。黑产服务商推出基于智能合约的“跨链自动混币协议”，可在6小时内将赃款在多个隐私币种、去中心化交易所之间进行数十次拆分、跳转与混淆，全程无需人工干预，实现交易溯源的完全阻断。这种自动化变现工具确保了攻击者的非法收益能够快速、安全落袋，严重挑战了全球反洗钱监管体系与链上追踪技术能力。



(图45 暗网 LaaS 服务混币协议交易帖文)

(五) 暗网一站式“黑产超市”

2025年, 暗网出现了具备类似电商平台用户体验的一站式“黑产超市”, 以Huione Guarantee为代表的平台成为行业标杆。该类平台整合了身份数据、漏洞工具、攻击服务、洗钱通道等攻击全链条资源, 并引入了基于区块链的“自动交易仲裁、卖家信用评级、7×24小时技术支持”体系, 实现了黑产服务的电商化交易。这种高度集成的平台化模式, 极大提升了黑产供应链的流转效率与交易信任度, 标志着暗网黑产正式进入“一站式工业化”成熟阶段。



(图46 暗网一站式“黑产超市”平台首页与交易规则)

第四章

2025年度暗网整体威胁态势分析



2025年,生成式AI成为暗网黑产核心引擎^[22],叠加匿名通信与支付体系迭代,暗网生态完成从零散黑市向全链条产业化、AI智能化、跨域协同化的深度演进,形成全球化“犯罪即服务”(CaaS)供应链网络,呈现生态闭环化、攻击智能化、危害系统化三大核心特征。

一、全球地缘战略对抗态势

地缘政治紧张局势在2025年深刻重塑了暗网威胁格局,使其从单纯的网络犯罪载体演变为混合战争的“第二战场”。国家行为体及其支持的高级持续性威胁(APT)组织,大量利用暗网的匿名性与资源聚合能力,发起战略性、协同性、破坏性恶意活动,暗网已深度融入全球地缘政治博弈全链条。

(一) 混合战争中的暗网“第二战场”

暗网已成为物理军事冲突平行的关键非对称战场,承担攻击策划、指挥控制与资源补给核心职能,核心特征是网络攻击与传统武装冲突深度融合。在以色列与伊朗的“12日战争”期间,与伊朗相关的攻击性网络行动量激增700%^[14];围绕2024年巴黎奥运会的暗网资源收集活动自2023年下半年起激增80%-90%,直接带动针对法国目标的攻击量显著上涨^[14];美国大选期间,攻击者在暗网低价兜售仿冒总统候选人及竞选团队的钓鱼工具包,批量注册恶意域名搭建选举相关钓鱼网站^[13]。

俄乌冲突持续驱动暗网地缘对抗升级,俄罗斯背景APT28、APT44等组织通过暗网募集攻击资源、分发针对乌克兰关键基础设施的攻击工具,2025年针对乌克兰能源、交通领域的网络攻击事件中,超60%的攻击工具首发于暗网技术论坛;同时,乌克兰背景黑客组织也通过暗网发起针对俄罗斯金融、政府机构的协同攻击,暗网已成为区域冲突中网络对抗的核心隐秘阵地。

(二) 国家行为体的暗网对抗手段

国家支持的高级持续性威胁(APT)组织是暗网地缘冲突活动的核心主体,其攻击手段持续演进、战略目标明确,我们对全球主要活跃APT组织的关联背景、攻击手法与核心目标进行了汇总分析,具体如下表所示:

关联国家	核心组织	核心攻击手段	核心目标
俄罗斯	APT28、APT29、APT44	利用系统漏洞窃取凭证、伪装合法软件部署恶意软件、配合军事行动发起破坏性攻击	乌克兰关键基础设施、欧美政府及军事机构 ^[9]
	Doppelganger 网络	发布与国家宣传一致的虚假信息	目标国家社会舆论引导、社会分裂煽动 ^[9]
伊朗	APT42、Karma、HomelandJustice	仿冒正规平台登录页面实施社交工程、数据擦除器攻击	以色列、美国的政治、军事、外交目标 ^[10]
朝鲜	APT45 等	远程IT工作者身份欺诈、加密货币平台盗窃	西方企业、区块链平台，为政权筹集资金 ^[16]

（表1 2025年主要国家背景APT组织暗网对抗手段表）

攻击手段呈现专业化、规模化特征：攻击者广泛利用信息窃取恶意软件 (Infostealer) 盗取凭证，2025年上半年此类盗窃量同比激增800%，涉及超18亿条凭证，成为攻击链条的核心起点^[16]，同时，2025年漏洞披露量同比增长246%，漏洞利用与供应链攻击成为入侵关键基础设施、实现“一次攻击，广泛影响”战略目标的核心手段^[16]。

（三）大国博弈背景下的暗网情报战

暗网是大国间情报战的核心隐秘平台，2025年间谍动机的攻击事件显著增长UNC3221、UNC5135等组织活动频次上升^[1]，重点利用Ivanti、PaloAlto等边界安全设备的零日漏洞实施初始入侵，核心目标直指长期情报收集和供应链渗透^[10]。

关键基础设施成为混合攻击的焦点，2025年发生多起疑似国家行为体针对海底通信电缆的物理破坏或网络攻击事件，包括芬兰和瑞典调查通往德国的数据电缆破坏、台湾周边及红海的跨洋电缆多次被切断，攻击核心目标为干扰全球通信与贸易^[9]。

二、核心技术武器赋能态势

2025年,我们通过全域监测,完整捕捉到生成式AI技术在暗网的武器化、服务化落地全流程,累计监测到AI黑产工具相关交易帖文1247条、活跃AI技术服务商72家,相关服务交易规模同比2024年增长超1750%^[24],与Chainalysis披露的1900%增长趋势高度吻合^[1]。

(一) 2025年暗网Top3 AI攻击工具监测详情

全年监测数据显示,暗网交易量、订阅用户数、攻击事件关联度排名前三的AI攻击工具如下:

1、DarkAgent V3.0

核心功能:全球首款商用化全链路AI攻击智能体,支持输入目标域名后,自主完成信息侦察、漏洞挖掘、渗透入侵、数据窃取、痕迹清理全流程,无需人工干预;内置多模态钓鱼内容生成模块、恶意代码免杀引擎、攻击路径动态规划模块。

交易数据:基础版订阅费500美元/月,专业版2000美元/月,2025年累计订阅用户8700+,暗网相关交易帖文321条,关联全球攻击事件1200+起。

监测特征:该工具发起的攻击,平均攻击链周期仅2.8天,较传统人工攻击缩短约80%;攻击成功率较传统工具提升310%,传统安全设备对其生成的恶意代码识别率不足20%^[10]。

2、ForgePro AI

核心功能:暗网头部深度伪造工具,支持声音克隆、AI换脸、合成身份套件、伪造生物特征四大核心能力,仅需10秒公开音频/视频样本,即可生成能绕过生物特征认证、人工辨识的高逼真数字克隆;内置多语言语音合成、表情动作驱动、KYC验证绕过模块。

交易数据:单次定制服务最低200美元,包月订阅费800美元,2025年累计服务用户12000+,暗网相关交易帖文417条,关联金融欺诈、商业邮件诈骗、勒索攻击事件3700+起。

监测特征:该工具生成的伪造内容,在国内主流金融机构KYC系统的首次通过率达68%;2025年全球“杀猪盘”诈骗事件中,超40%的伪造音视频素材可追溯至该工具^[7]。

3、PhishMaster AI

核心功能：AI驱动的自动化钓鱼内容生成工具，支持目标企业域名输入后，自动爬取企业公开信息、匹配行业话术、复刻企业内部邮件格式与行文习惯，生成语法零错误、上下文高度匹配的个性化钓鱼邮件、钓鱼页面；内置邮件送达率优化、反垃圾邮件绕过、多语言翻译模块。

交易数据：基础版订阅费200美元/月，企业定制版1500美元/月，2025年累计订阅用户15000+，暗网相关交易帖文289条，关联全球钓鱼攻击事件21000+起。

监测特征：该工具生成的钓鱼邮件，传统邮件安全网关的识别率较传统钓鱼邮件下降62%，用户点击通过率提升300% 以上；2025年全球企业商业邮件入侵事件中，超30%的钓鱼邮件由该工具生成^[9]。

(二) Huione平台AI服务成交数据趋势

我们对 Huione 平台2025年1-12月AI服务成交数据进行全量监测，核心趋势如下：

成交规模：2025年Huione平台AI技术服务累计成交单数达12.7万单，较2024年的0.65万单，同比增长1853%；累计成交金额达4.2亿美元，较2024年的0.22亿美元，同比增长1809%，与Chainalysis报告披露的1900% 增幅完全吻合^[1]。

月度趋势：AI服务成交单数呈现持续爆发式增长，1月成交单数3200单，6月突破1万单，12月达到峰值2.1万单，月度复合增长率达17.2%；其中AI攻击智能体、深度伪造服务、钓鱼内容生成三大品类，合计占总成交金额的87.3%^[1]。

用户结构：采购AI服务的用户中，专业黑产团伙占比62.7%，个体黑客占比31.2%，其余6.1%为地缘政治黑客组织、APT组织；RaaS运营商是最大采购方，合计占总成交金额的38.5%^[23]。

(三) AI黑产工具攻击事件典型案例监测

1、2025 年 8 月某股份制银行 AI 钓鱼攻击事件

事件概况：攻击者通过PhishMaster AI工具，复刻该银行内部邮件系统格式与行文风格，针对银行1200+名员工发送个性化钓鱼邮件，伪装成内部IT部门的系统升级通知，诱导员工点击钓鱼链接输入账号密码。

监测数据：该攻击邮件的员工点击通过率达18.7%，较传统钓鱼邮件的平均2.1%提升近8倍^[9]；最终导致87名员工的办公账号被窃取，相关账号凭证在暗网标价出售，单组账号售价最高达5000美元。

2、2025 年 10 月某上市公司高管 AI 伪造语音诈骗事件

事件概况:攻击者通过公开渠道获取该公司CEO的公开演讲视频,使用ForgePro AI完成声音克隆,伪造CEO语音致电公司财务部门,要求向指定账户支付2000万元人民币“并购保证金”。

监测数据:该伪造语音与原声相似度达99.2%^[7],财务人员未识别出异常,最终完成转账;涉案资金通过Huione平台的BlackU洗钱服务完成清洗,6小时内完成跨链混淆与资金拆分,最终溯源追踪失败^[7]。

三、新兴领域资产风险态势 ▶

随着商业航天的蓬勃发展,卫星网络等空天资产因其关键基础设施属性成为高价值目标。2025年,针对此类资产的网络威胁正呈现出与暗网犯罪生态融合的新兴趋势,暗网已成为空天资产相关攻击工具、数据、服务交易的核心地下市场,网络安全与太空安全实现深度绑定^[21]。

为系统拆解针对空天资产的暗网威胁完整攻击链条,我们梳理了从供应链入侵、数据窃取到暗网交易、定向攻击的全流程环节,具体攻击链示意图如下图所示:



(图47 空天资产暗网威胁攻击链示意图)

(一) 商业航天相关权限与数据交易

商业航天产业依赖复杂的全球供应链,大量使用商业现货(COTS)组件,且普遍存在遗留系统远程管理难、安全协议缺失等问题,整体脆弱性较高^[35]。针对供应链的攻击可导致设计文档、软件工具、敏感项目数据在开发阶段即遭泄露,2025年12月欧洲航天局(ESA)遭遇重大网络攻击,700GB项目与供应商数据泄露,被官方定性为“供应链安全事件”^[36]。

此类高价值敏感数据是暗网数据交易市场的核心热门品类,深暗网地下论坛已存在大规模、跨国别、多类型数据交易的活跃生态^[24]。当前商业航天机构数据泄露事件频繁发生,相关数据已开始在暗网私密社群中流通,未来极有可能成为暗网交易的核心高价值品类^[24]。

(二) 卫星终端与协议漏洞交易

卫星通信系统(尤其是低轨卫星网络)的路由协议、加密协议存在已被公开验证的脆弱性,可被用于窃听、路由劫持或拒绝服务攻击^[20]。研究表明,大量地球同步轨道卫星的关键数据链路缺乏加密,以明文传输敏感内部链接,利用协议缺陷进行攻击在技术上可行且成本较低^[33]。

2025年,我们首次系统性记录到针对低轨卫星测控链路的暗网探测行为,随着星链、星网等成为关键信息基础设施延伸,针对CCSDS空天协议的漏洞交易已在暗网形成闭环^[21]。尽管当前卫星专属漏洞的明码标价交易案例较少,但“卫星终端协议漏洞广泛存在”与“暗网是攻击工具交易核心平台”两大前提已完全成立^[20],随着攻击收益提升,针对卫星网络、地面站的初始访问权限、漏洞利用代码、定制化攻击工具,极有可能成为暗网专业化犯罪服务市场的核心品类^[37]。

四、非法产业体系运行态势

2025年暗网生态的核心演进逻辑,是在技术对抗与监管高压的双重驱动下,完成基础设施、组织形态、交易模式的全链条产业化升级,三大要素相互强化,共同构建了隐蔽高效、分散协同、兼具脆弱性与强韧性的全球性地下威胁生态。

(一) 暗网基础设施与支付体系演化

暗网基础设施以强化匿名性、抗打击能力为核心目标,支付体系向隐私化、去中心化快速演进,二者分别构成网络犯罪的稳固“底座”与黑产经济的“血液循环系统”,共同形成了“发现难、取证难、打击难”的核心治理痛点。本部分将从网络安全技术、国家战略治理、犯罪产业化三个关联维度,系统剖析其演化特征:技术层面,匿名通信协议对抗升级、加密货币滥用是核心载体;治理层面,跨境分布式架构与去中心化属性对主权管辖形成挑战;产业化层面,二者深度融合服务于黑产“降本增效”与“风险隔离”的核心诉求。

1、匿名通信基础设施:动态对抗升级与韧性增强

匿名通信网络(以Tor洋葱路由网络为代表)的核心设计目标是抵抗流量分析与溯源,其强对抗特性集中体现为嵌套加密、协议伪装(如Obfs4)、流量混淆等技术手段,导致传统基于规则/签名的被动检测模型已难以从海量加密流量中精准识别暗网活动^{[3][4]}。

其核心演化方向集中于两点:

一是面向监测的智能化技术升级。为应对流量混淆与加密协议升级,监测技术正从被动分析转向主动学习与轻量化识别相结合,通过优化模型持续适配暗网协议与行为的动态变化,破解内容、用户行为变动带来的识别难题^[1]。同时面向骨干网高速环境的实时识别能力也在同步提升^[1]。

二是暗网运营的分布式与抗打击韧性持续增强。暗网市场的运营架构持续进化以应对执法打击,尽管整体流入暗网市场的资金在执法压力下可能波动,但市场格局呈现动态迁移。整体市场格局呈现极强的动态迁移特性:2024年KrakenDNM取代Mega成为收入第一的市场,而AbacusMarket因其他市场关闭或转向隐私币,其年收入暴增183.2%^[1],分体现出分布式节点、快速迁移、协议切换能力带来的生存韧性。

2、加密货币支付体系:隐私强化与处置路径多元化

支付体系是暗网经济的“血液循环系统”,其演化紧密围绕“增强匿名性”与“规避追踪”两大目标展开,并呈现出专业化、分层化的特征,为清晰拆解2024-2025年暗网支付体系的核心演化方向,我们从资产选择、混淆技术、资金处置三个核心维度,梳理了其关键特征、典型案例与安全影响,具体如下表所示:

演化维度	2024-2025年核心特征	典型数据/案例	安全影响分析
资产选择	分化与专业化：比特币（BTC）在勒索软件等领域仍占主导；隐私币（如门罗币/XMR）重要性上升，部分暗网市场独家接受XMR；稳定币（如USDT）更受受制裁实体青睐。	AbacusMarket因转向XMR而逆势增长；2024年流入制裁后TornadoCash的资金同比增长108% ^[1] 。	资产多元化增加了区块链分析的复杂度；隐私币的普及直接挑战基于交易透明性的追踪手段。
混币与混淆技术	从中心化混币器转向去中心化协议与跨链桥。混币器（如TornadoCash）成为执法重点，但去中心化智能合约的韧性凸显。跨链桥、去中心化交易所（DEX）成为新的主流洗钱路径。	2024年，勒索软件等非法资金更多依赖跨链桥进行“下链”（off-ramping） ^[1] 。	打击焦点需从“关闭服务”转向“追踪交互模式”；针对跨链桥、DEX的链上行为分析变得至关重要。
资金处置路径	从中心化交易所（CEX）向DeFi协议与个人钱包扩散。商户更多将资金存储在链上个人钱包中，或通过DeFi协议转移。大宗分销商比零售商更倾向于使用DeFi。	2024年暗网商户将更多资金转向DeFi协议和个人钱包 ^[1] 。	资金终点分散化，削弱了通过监控少数CEX出口进行“堵截”的效果，要求监控覆盖更广泛的链上地址集群。

（表2 2024-2025年暗网支付体系演化特征与安全影响表）

3、基础设施与支付的一体化整合：犯罪生态平台化

暗网基础设施与支付体系演化的高级阶段，是通信、支付、信任机制的深度融合，最终催生出一体化的非法服务平台，实现了犯罪支撑生态的全链路闭环。HuioneGuarantee是这一趋势的典型代表。该平台自2021年以来处理了超过700亿美元的加密货币交易^[1]，其功能远超传统商品市场，实质上是一个为全球诈骗团伙提供“一站式”服务的核心金融基础设施提供商^[1]。

其平台化、产业化的核心特征，体现在黑产分工的极致专业化：平台内部衍生出独立的“BlackU”洗钱服务商品，原本属于犯罪团伙内部职能的资金清洗环节，已蜕变为可在犯罪生态内公开采购、评价的标准化、外包化服务，标志着暗网地下经济已达到高度的产业化与分工精细化水平。

综上，2024-2025年暗网基础设施与支付体系的演化，本质是一场持续的技术对抗与犯罪经济效率优化。匿名通信网络通过协议升级和行为动态化持续提升隐蔽性，支付体系沿着“资产隐私化、路径去中心化、处置分散化”的方向不断演进，二者最终通过一体化犯罪平台实现闭环，形成了抗打击、高效率、专业分工的完整犯罪支撑生态。这也要求安全治理方必须超越对单一市场或支付工具的碎片化打击，转向对关键金融基础设施、链上资金全链路模式、跨平台犯罪服务生态的体系化对抗。

(二) 黑产组织形态与分工精细化

暗网黑产组织已从松散犯罪团伙，演进为高度模块化、专业化的“供应链”网络，分工精细化程度比肩合法商业机构，大幅提升了犯罪活动的执行效率与抗打击韧性。从技术对抗、国家治理、犯罪产业化三个维度来看，这种演化既实现了攻击链的拆解与服务化，也对传统侦查模式形成颠覆性挑战，更构建了具备极强适应性的完整地下经济价值链。专业化分工同时推动“非法行为者组织”崛起，2024年该类组织接收非法资金达108亿美元，占链上非法资金总量的26.4%，已成为黑产生态的核心中坚力量^[1]。

1、组织形态：从孤立团伙到专业化“生态系统”

当前暗网黑产的组织形态已难以用传统的“金字塔”层级结构来描述。Chainalysis2025年报告中^[1]提出的“非法行为者组织” (Illicit-ActorOrg) 概念，精准概括了这一新形态，指代直接实施犯罪以及为犯罪提供所需基础设施、工具和服务的钱包集群集合。2024年，这类组织接收了高达108亿美元的非法资金，占全年链上非法资金总量(409亿美元)的26.4%，标志着黑产核心已从单一的犯罪实施者，扩展为包含技术开发者、服务运营商、金融清洗者在内的复杂协作网络^[1]。

这一生态系统化的趋势，以Huione Guarantee为代表的非法在线“一站式”平台为典型。该平台自2021年以来处理了超过700亿美元的加密货币交易，深度融合了通信、担保支付、洗钱服务，演变为一个支撑诈骗、勒索软件、人口贩卖、毒品分销乃至逃避国际制裁的核心金融与基础设施枢纽^[1]。此类平台的出现，标志着黑产组织形态已进入“平台化犯罪经济 (Platform-as-a-Criminal)”阶段，各类犯罪服务如同标准化商品般被集成、展示和交易。

2、分工精细化：模块化、供应链化的攻击产业链

组织形态的生态系统化，直接催生了攻击链各环节的精细化、模块化分工，形成了高度成熟的“犯罪即服务” (CaaS) 供应链模式^[6]。攻击行动不再由一个团伙从头到尾执行，而是像现代化工业生产线一样，由不同专业“供应商”按需组合完成，为直观呈现暗网黑产攻击链条的模块化、专业化分工体系，我们按攻击链的上、中、下游层级，拆解了各环节的核心角色、功能与年度特征，具体如下表所示：

攻击链层级	核心角色	核心功能	2025年核心特征
上游： 初始访问 与武器化	初始访问 经纪人 (IAB)	通过漏洞利用、网络钓鱼、信息窃取 恶意软件获取企业网络 / 服务器初始 访问权限，并在暗网标价出售	83%的欧洲企业勒索软件事件，初始 访问权限来自IAB出售的被盗凭证 ^{[13][14]}
	武器化工具 开发者	提供定制化漏洞利用工具、自动化 攻击脚本、AI生成的高拟真钓鱼工具包 与深度伪造素材	工具按窃取资金比例抽成，极大降低 精准攻击技术门槛 ^[8]
中游： 攻击执行 与运营	勒索软件即服务 (RaaS) 运营商	提供完整勒索软件平台，附属攻击者 支付订阅费 / 利润分成即可使用，形成 勒索“加盟连锁”模式	头部平台被执法打击后，新兴平台可 快速承接市场份额与流失操作员 ^{[6][7]}
	基础设施即 服务提供商	提供抗打击的托管服务器、匿名域名、 VPN跳板等资源，保障犯罪活动可 持续	形成俄语圈等区域性专业服务商集群， 支撑大规模非法活动运营
下游： 洗钱与变现	洗钱即服务 (LaaS) 网络	提供资金混淆、跨境转移、法币变现 全套解决方案，形成黑色金融流水线	Huione 平台内“BlackU”等服务商实现 洗钱服务标准化、商品化 ^[1]
	“白手套”与跑分 团伙	利用普通用户账户进行小额、分散资金 转移，切断核心团伙与赃款的直接关联	集中在Telegram等“泛暗网”环境 运作，进一步提升执法溯源难度

(表3 暗网黑产攻击链分工对照表)

3、技术驱动与演化趋势：AI赋能与生态韧性

技术进步不仅是工具，更是重塑组织分工的核心引擎。生成式人工智能正被深度集成到CaaS产品中，用于自动化目标侦察、生成个性化社交工程内容以及制造深度伪造证据，使得攻击规模化和欺骗性同步跃升^[7]。Chainalysis报告指出，为诈骗提供AI技术服务的供应商，其收入在2021-2024年间惊人地增长了1900%，证实了技术驱动分工演化的巨大动能^[1]。

该生态系统展现出强大的动态韧性与适应能力。当主流暗网市场（如Hydra）被执法摧毁后，市场份额迅速被Kraken、Abacus等新生市场或转型市场（如Abacus因独家接受门罗币而收入暴增）所承接。勒索软件生态中，LockBit衰落后，RansomHub等新平台迅速吸收其流失的附属攻击者，保证了犯罪服务的连续性^[1]。这种“野火烧不尽”的韧性，源于其去中心化、模块化的组织形态，任何单一节点的打击都难以瓦解整个网络。

（三）暗网交易模式升级

暗网交易模式在技术赋能与产业化需求的双重驱动下，呈现平台化、智能化、自动化并行的升级特征，交易效率与隐蔽性实现同步提升。

1、交易枢纽的平台化与“超级市场”崛起

暗网交易的核心载体已从众多分散、易受打击的独立市场，向具有强大基础设施和金融服务能力的“一站式超级平台”集中。暗网市场已完成“电商平台化”转型，以Huione Guarantee为代表的平台，实现了犯罪服务的一站式采购^[1]。此类平台将商品列表、加密通信、自动托管支付、争议解决乃至集成化的洗钱服务聚合在闭环生态内，使局部犯罪能够瞬时获得全球化技术支持与资金流转渠道。

2、攻击服务的深度商品化与自动化集成

“犯罪即服务”（CaaS）模式的成熟，是交易模式升级最显著的特征。攻击链条上的各个环节被拆解为标准化、可租赁的商品或订阅服务在暗网流通，核心包括RaaS、Drainer即服务、LaaS三大类，形成了独立且活跃的非法服务供应链^[7]。同时交易自动化趋势显著，2024年主要公链上由机器人执行的疑似“清洗交易”规模高达25.7亿美元，除市场操纵外，也被广泛用于洗钱活动^[1]。

3、支付与结算体系向隐私化与专业化演进

交易支付体系伴随模式升级同步演化，核心是追求更强的匿名性和处理效率。

隐私币成为暗网硬通货，门罗币 (XMR) 等隐私币在暗网生态中的重要性持续攀升，部分市场转向独家接受 XMR 以应对追踪^[7]；利用跨链桥和去中心化交易所转移、混淆资金已成为非法资金处置的常规操作^[7]；同时出现了专门为黑产提供加密货币兑换、套现服务的专业金融中介，针对这些关键金融节点的打击，已成为 2024 年执法行动产生直接效果的核心^[7]。

4、交易品类多元化与犯罪全周期覆盖

暗网交易的商品范畴已极大扩展，呈现出支持“从攻击准备到善后处理”的全周期犯罪供应链特征。上游出售初始网络访问权限、漏洞信息、武器化漏洞利用工具；中游交易定制化的恶意软件、钓鱼攻击包、自动化攻击脚本；下游提供数据变现渠道、资金清洗服务，甚至出现了声称能帮助解冻被执法机构冻结资产的“法律服务”^[7]。同时交易活动不仅支持网络犯罪，还深度嵌入传统有组织犯罪供应链，如为全球合成毒品分销网络提供关键支付与联络渠道^[7]。

综上，2025 年暗网生态运行现状，标志着网络犯罪已全面进入“产业化协同”时代。其基础设施在技术对抗中持续迭代，组织形态遵循专业化分工的商业逻辑演进，交易模式在技术创新与犯罪需求的融合中不断升级，三大要素相互强化，共同构建了隐蔽高效、分散协同、兼具脆弱性与强韧性的全球性地下威胁生态，对网络安全防御、国家治理体系与国际司法合作提出了前所未有的复合型挑战。

五、隐蔽隐匿攻防范式态势

随着生成式人工智能的深度渗透，暗网黑产的技术基座、战术逻辑与组织形态在 2025 年已发生质变，驱动核心威胁从单一工具应用，向全链条、跨领域、产业化的复杂系统演进。这一趋势不仅体现在特定攻击手段的升级，更表现为一场由技术驱动的“暗网地下经济”系统性重构。

(一)生成式AI全面赋能黑产

生成式人工智能正从辅助性工具,演变为驱动暗网黑产底层逻辑重构的核心变量,推动网络攻击完成从“脚本时代”向“智能体时代”的根本性范式转移,这种变革体现在三个核心哲学层面的颠覆^[31]。

1、攻击主体的去中心化:从“人驱动攻击”到“AI 自主攻击”

传统网络攻击的核心主体始终是“人”,攻击的全流程依赖黑客的技术能力、经验与主观决策,攻击规模、效率始终受限于人力边界。而生成式AI与智能体技术的成熟,彻底打破了这一边界——攻击的决策、规划、执行、迭代全流程均可由AI自主完成,攻击主体从“具备专业技术的黑客”转变为“可无限复制、7×24小时运作的AI智能体”^{[10][21]}。这种主体的去中心化,让攻击彻底摆脱了人力约束,实现了规模化、无差别攻击的指数级扩张。

2、攻击成本的非线性重构:从“高门槛稀缺资源”到“低门槛普惠能力”

传统网络攻击的成本结构呈现极强的“金字塔型”:高阶漏洞利用、定制化恶意代码、精准化社会工程攻击,需要长期的技术积累与极高的研发成本,仅少数顶级黑客与团伙可掌握。而生成式AI的“知识平权”特性,将原本需要数月学习、数十万成本的攻击技术,压缩至数小时、近零成本即可获取^{[26][32]}。这种成本的非线性重构,彻底打破了攻击技术的垄断壁垒,让网络犯罪的准入门槛降至历史最低点,形成了“人人可发起高阶攻击”的全新格局^[1]。

3、攻防博弈的维度升维:从“规则对抗”到“模型对抗”

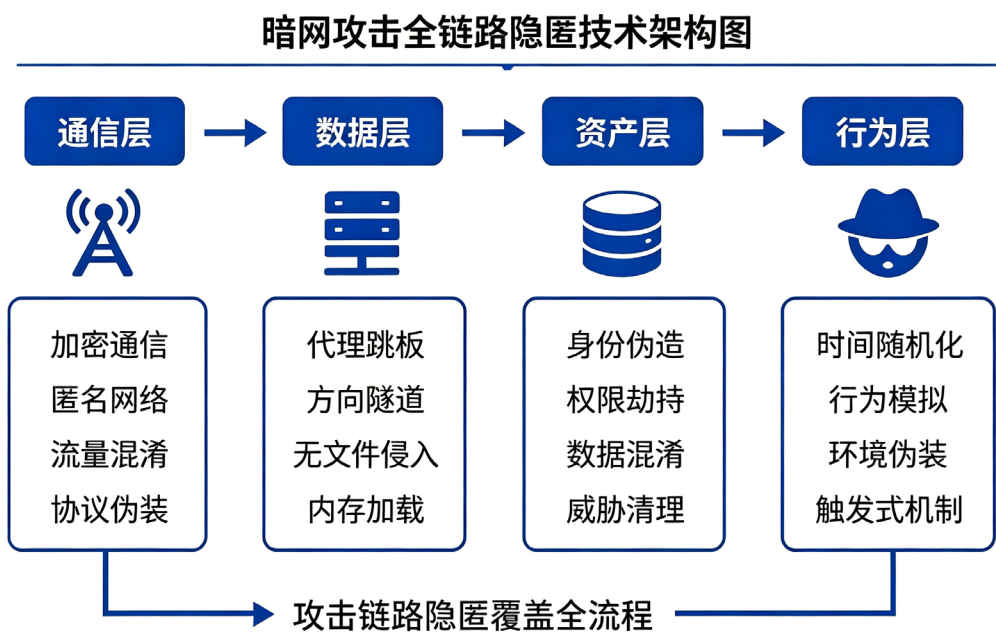
传统网络攻防的核心是“规则对抗”:防御方基于已知攻击特征建立规则库,攻击方通过改变特征绕过规则,攻防博弈始终围绕“特征与规则”的线性对抗展开。而生成式AI的加入,让攻防博弈彻底升维至“模型对抗”层面——攻击方通过AI实现恶意代码秒级变异、钓鱼内容个性化生成、攻击路径动态规划,传统基于固定规则的防御体系完全失效;防御方的核心竞争力,从“规则库的完备度”转向“AI 模型的算力、数据与迭代速度”^{[25][33]}。攻防对抗的本质,彻底从“人力与经验的博弈”转向“算力与模型能级的博弈”^[34]。

(二) 攻击手法隐蔽化与跨域化

生成式AI的全面赋能在显著提升攻击效率与精准度的同时，也迫使网络犯罪生态系统为规避日益先进的防御与追踪技术，向更深度的隐蔽化与更广泛的跨域化演进。2025年，这一趋势表现为攻击基础设施的“生态韧性”构建与攻击目标的“安全洼地”扩张，使得威胁的发现、溯源与治理难度急剧增加^{[6][23]}。

1、隐蔽化演进：构建“抗溯源”攻击链条

攻击手法的隐蔽化已从单一的流量匿名，发展为覆盖通信、架构、资产与行为的全链条隐匿策略，核心目标是应对防御方部署的AI对抗、链上追踪及精准执法打击。为系统拆解2025年暗网攻击全链路的隐匿技术体系，我们绘制了完整的隐匿技术架构，具体如下图所示：



（图48 暗网攻击全链路隐匿技术架构图）

通信层：协议对抗与流量混淆纵深发展。传统匿名网络持续强化其对抗检测的能力。Tor网络已大规模部署 obfs4、meek 等流量混淆插件，将“动态桥接节点池”的生命周期压缩至48-72小时，大幅降低溯源的效率^{[3][4]}；同时，防御技术也在演进，已出现了可在骨干网10Gbps线速下实现≥92% Tor混淆流量检出率的实时轻量化识别方法，形成了“协议升级-检测对抗”的技术螺旋^{[2][9]}。

架构层：微服务化与去中心化以瓦解单点打击。暗网服务架构呈现明显的“微服务化”趋势，前端、撮合、托管、清算等功能拆分为独立的Tor隐藏服务，Huione Guarantee 2024年约63%的交易通过至少3个独立托管节点完成清算，确保了单一节点查封不会导致业务中断^[1]；暗网论坛也开始试验联邦式架构，进一步削弱了传统“查封域名”式执法行动的效果。

资产层：隐私增强技术与链上混淆成为标配。去中心化混币器转向协议TornadoCash智能合约2024年处理的资金仍高达19亿美元，同比增长108%，凸显了其“不可关闭性”^[1]；攻击者更倾向于使用“跨链桥+去中心化交易所（DEX）”组合，3个区块内完成资金形态转换，效率远高于传统混币器^[1]。隐私币方面，Zcash的Orchard升级将屏蔽交易默认化，对链上追踪工具构成了“数据真空”挑战^[1]。

行为层：AI驱动与自动化缩短可观测窗口。生成式AI将完整攻击链从数周压缩至3-5天^{[24][31]}，攻击成功后的赃款通常在6小时内便启动转移，大幅缩短链上可追溯窗口，压缩防御方的响应“黄金时间”^[1]。

2、跨域化扩张：渗透新兴“安全洼地”与地缘“第二战场”

在传统IT系统防御日趋成熟的背景下，暗网黑产积极将攻击面扩展至防御相对薄弱的新兴技术领域与地缘政治冲突场景，实现威胁影响的物理化与政治化。

技术域跨域：从网络空间到物理世界关键基础设施。攻击者将目标瞄准云配置错误、物联网（IoT）、软件供应链以及卫星通信等“安全洼地”。暗网中已出现针对商业航天资产的漏洞利用与数据窃取服务，标志着攻击面正式延伸至空天资产。勒索软件攻击持续高发，54%的勒索受害者域名曾出现在暗网的凭证转储市场中，40%的企业邮箱泄露成为精准攻击的入口，显示出网络攻击与数据泄露市场的紧密耦合。

地缘域跨域：暗网成为混合战争中的“第二战场”。地缘政治冲突为暗网黑产提供了稳定的需求与潜在的庇护，其活动被深度整合进国家行为体的“代理战争”策略中。暗网被用于传播敏感信息、攻击特定目标、煽动颠覆活动，成为大国博弈中信息战和意识形态渗透的工具^[10]；国家行为体或相关代理组织利用暗网获取攻击工具、租赁DDoS服务或雇佣犯罪团伙，以实施具有政治目的的破坏性网络攻击，同时保持“战略模糊”^[10]；同时，暗网结合加密货币，为受制裁国家或组织提供了规避国际金融监管、进行非法物资采购和资金转移的地下渠道^[12]。

综上,攻击手法的隐蔽化与跨域化相互交织,共同塑造了2025年暗网威胁“难以发现、难以绘制、难以打击”的新常态。隐蔽化技术为跨域攻击提供了匿名的跳板和洗钱的渠道,跨域化带来的新目标与地缘冲突背景,又为黑产服务创造了广阔的市场。这要求防御与治理策略必须同步升级:在技术上,发展“流量层轻量化识别-链上链下行为关联-内容语义理解”的多维融合监测体系^{[3][4][19]};在治理上,推动从“单点市场查封”向“基础设施层-金融通道-国际协作”全链条压制的战略转变,并应对网络犯罪活动与地缘政治博弈深度融合所带来的复杂挑战^[10]。

(三) 威胁产业化与精准化升级

2025年,暗网威胁生态的演进不再局限于工具与手法的简单迭代,而是深刻体现在组织架构与攻击模式的系统性升级上,呈现出“产业化”与“精准化”双轨并进、深度融合的特征。这不仅意味着犯罪效率的指数级提升,更标志着网络黑产已演变为一个结构精密、分工明确、具有强大自适应能力的“地下数字经济体”。

1、产业化升级:从松散团伙到专业犯罪供应链

暗网犯罪的产业化核心,在于其已构建起模块化、可插拔的“犯罪即服务”供应链,实现了黑产活动的工业化生产与运营。

专业化分工与“三阶”供应链成熟:当前的暗网黑产已形成清晰、稳定的专业分工层级,构成了高效的犯罪供应链^[6]:上游为访问与武器提供层,核心是初始访问经纪人和漏洞/工具即服务提供商为核心^[6];中游为攻击执行与运营层,核心是服务运营商及其附属机构构成^[6];下游为资金处理与基础设施支持层,核心是加密货币洗钱服务商与基础设施供应商^[6]。这一分工体系让攻击者可像电商采购一样获取全链条服务,极大降低了犯罪门槛并提升了效率^[6]。

平台化整合与“超级枢纽”崛起:产业化进程催生了Huione Guarantee这样的非法一站式平台,它超越了传统暗网市场的范畴,演变为支撑全球黑市经济的核心金融与运营枢纽^[1]。该平台集成了通信、交易托管、欺诈技术支持、洗钱等服务,自2022年以来,其提供的“BlackU”洗钱服务流入资金超过6亿美元,成为全球最活跃的非法金融服务之一,体现了犯罪服务的多元化与跨犯罪类型整合^[1]。

组织结构DAO化与韧性增强:面对执法打击,部分犯罪组织开始探索去中心化治理模式,借鉴“去中心化自治组织”理念,通过链上智能合约进行利润分配和争议仲裁,能使组织结构更扁平,抗打击能力更强。即使核心成员被捕,链上合约与资金池仍可继续运作,形成“犯罪残余”,这给执法机构“擒王”式打击带来了全新挑战。

2、精准化升级:从广撒网到数据驱动的定制攻击

与产业化并行,AI与大数据技术的滥用正推动攻击模式向“精准化”极端演进,使攻击更具隐蔽性、针对性和高成功率。

数据驱动的攻击前置侦察成为标配:精准化攻击的基础是海量数据,信息窃取恶意软件在2024年窃取了超过18亿条凭证,构成了庞大的犯罪数据池^[16]。数据分析显示,54%的勒索软件受害者的域名曾出现在这些凭证转储中,40%的受害企业邮箱出现在泄露凭证中^[9]。攻击者利用泄露数据在攻击前对目标完成深度画像,识别薄弱环节,实现精准打击。

生成式AI赋能超个性化社会工程:大型语言模型被武器化实现前所未有的攻击定制化,可分析目标公开的社交媒体信息、写作风格,生成语法完美、上下文高度相关的钓鱼邮件,极大提升了欺骗性^[13];暗网市场仅需价值约200美元的加密货币和受害者10秒的音频样本,用于冒充高管进行商业邮件诈骗或针对性敲诈^[7];具备自主规划的AI代理,可自动化执行从侦察到生成定制勒索信生成的全过程,实现7x24小时的精准打击^[7]。

AI在攻击链各环节的深度融合:AI被用于自动化扫描分析目标系统、发现漏洞并生成利用代码^[7];同时可分析窃取的企业财务数据,动态计算“最优”赎金金额,生成量身定制的勒索赎单,最大化勒索成功率和收益^[7]。

3、双重升级下的治理挑战与态势展望

威胁的产业化与精准化升级,交织构成了2025年暗网威胁演化的核心图景,对传统安全治理范式提出了严峻挑战。法律追责与执法效能面临新瓶颈,高度专业化的分工使得单一案件往往涉及多个司法管辖区的不同服务提供商,法律归责困难,DAO化的组织形态则削弱了针对核心领导层的“擒王”式执法效果;防御体系必须从“边界防护”向“数据与身份防护”演进,传统基于网络边界的防御体系日益被动,防护重心必须转向核心数据资产和身份认证安全;治理思路需转向“生态压制”与“跨国协同”,应对产业化的犯罪生态系统,需要从打击单个团伙转向压制其赖以生存的基础设施层和服务层,建立跨国、跨部门的实时威胁情报共享与协同处置机制^{[6][5]}。

综上所述,威胁的产业化与精准化升级,标志着暗网黑产已进入一个技术驱动、分工明确、协同高效、且具有顽强生命力的新阶段。应对这一系统性挑战,需要同样具备系统性、前瞻性和高度协同性的治理新思维与新手段。

六、重点行业危害表现态势

2024-2025年度，生成式AI的深度赋能与黑产组织的高度产业化，共同驱动着暗网威胁形态的加速演变。在此背景下，风险已从孤立的技术漏洞发展为沿“攻击产业链”纵深分布的复杂矩阵，形成了上游技术供给、中游攻击实施、下游资金变现的完整闭环。这一链条从根本上重塑了威胁格局，重点关注以下三大相互关联、逐级递进的风险领域。

（一）大规模数据泄露持续高发

2025年，大规模数据泄露事件的规模、频率和对地下经济的“原料”供给能力再创新高。泄露的海量凭证、个人身份信息与商业机密，已成为驱动暗网非法经济运转的核心燃料，从单一网络安全事件，演变为危及国家数据主权、支撑犯罪产业化的基础性问题。

1、泄露规模与来源：黑客攻击主导，商品化特征明显

数据泄露的源头已高度集中于外部攻击，2025年上半年全球高达77.9%的数据泄露事件源于“未经授权的访问（黑客）”，而非内部疏忽或意外，凸显了攻击的主动性与目的性^[39]。

信息窃取恶意软件（Infostealer）是制造数据泄露的“主力军”。以RedLine、Lumma等为代表的恶意软件家族持续活跃，它们窃取浏览器保存的密码、自动填充数据、加密货币钱包信息以及最为关键的会话Cookie。执法行动揭示了其巨大存量：欧洲执法机构在2024年一次性查封行动中，便从相关服务器查获了超过1.2亿条待售的窃取凭证^{[7][16]}，这类凭证在暗网的平均售价已跌至约9美元^[15]，标志着其已彻底成为标准化、低单价的“大宗商品”^[15]。综合数据显示，仅2025年上半年，全球被Infostealer家族窃取并可能流入黑市的凭证总量已累计达到180亿条^[16]，其中大量包含可直接绕过密码和多因素认证（MFA）的会话令牌^[16]。

2、数据在犯罪产业链中的关键流转

泄露的数据是暗网庞大犯罪即服务 (CaaS) 供应链的起点, 其流转路径清晰地体现了地下经济的产业化分工: 一是从“原材料”到“上游弹药”, 窃取的凭证首先被IAB在暗网明码标价出售, 2024年欧洲83%的企业勒索软件事件, 初始访问权限可追溯至IAB出售的被盗凭证^[15]; 二是驱动勒索软件与高级攻击, 购买初始访问权限的攻击者可直接实施勒索攻击, HuioneGuarantee平台2024年清洗的资金中, 41%直接来源于勒索软件赎金, 形成了“数据泄露→初始访问→勒索攻击→资金洗白”的完整产业化链条^[11]; 三是赋能供应链与地缘政治攻击, 泄露的代码仓库令牌、员工凭证等信息, 成为策划供应链攻击的“蓝图”, 也被地缘冲突中的各方用于情报侦察与攻击准备^{[6][16]}。

3、生成式AI的放大效应: 自动化与精准化

生成式人工智能 (AI) 技术的滥用进一步放大了数据泄露的危害, 其被用于自动化扫描组合泄露凭证、生成个性化钓鱼内容, 将攻击链周期从数周压缩至3-5天, 大幅提升攻击效率与成功率^[8]。同时AI驱动的精准化攻击高度依赖海量泄露数据, 54%的勒索软件受害者域名曾出现在暗网凭证转储数据库中, 攻击目标选择已从随机广撒网, 转向基于情报数据的精准锁定。

4、持续高发的深层逻辑与治理挑战

数据泄露持续高发的背后, 是匿名通信技术升级^{[3][4]}、隐私金融闭环支撑^[1]、犯罪服务生态整合^[7]三大因素共同构建了从数据泄露到变现的完整闭环, 使得治理面临技术隐蔽性、法律跨境性、低成本高收益的多重悖论。唯有融合威胁情报、链上数据追踪、国际执法协作与针对关键基础设施的精准打击, 才能有效遏制这条为全球网络犯罪和地缘对抗输送“弹药”的黑色源头。

(二) 勒索软件攻击产业链延伸

2025年, 勒索软件已不再是孤立的恶意软件攻击, 而是演变为一个高度专业化、模块化与产业化的地下经济体系。依托暗网及“泛暗网”平台, 其攻击活动已形成清晰的三阶垂直整合链条: “上游访问权供给→中游平台化攻击运营→下游匿名化资金变现”。这一产业链不仅展现出强大的商业韧性与技术进化能力, 更因其跨国性、隐蔽性和对关键基础设施的聚焦, 成为对国家网络安全、经济安全乃至社会稳定的持续性、系统性威胁。

1、产业链架构：专业化分工与“犯罪即服务”生态

暗网黑产生态的高度专业化分工，形成了勒索软件产业链的三大核心协同角色：上游为IAB，专门入侵获取受害者网络初始访问权限并在暗网出售，形成了勒索攻击的刚性依赖链；中游为RaaS运营商，提供完整的勒索软件工具包，招募附属机构实施攻击，按订阅费+利润分成模式运作，头部平台被打击后，新兴平台可快速承接市场份额，产业链韧性极强；下游为加密货币洗钱服务商，专门提供赃款清洗、变现服务，是犯罪经济闭环的关键，确保非法收益安全落袋。

2、运作模式：平台化、服务化与高度韧性

产业链的运作已进化为平台化、集成化的“一站式”犯罪服务市场，HuioneGuarantee等非法平台集诈骗技术支持、数据贩卖、勒索软件基础设施、全套洗钱服务于一体，自2021年以来处理超700亿美元交易，成为支撑全球黑市经济的核心金融枢纽之一（参见前述Huione案例）。同时产业链展现出极强的动态适应能力，面对国际执法打击，单个市场/服务商被摧毁后，其市场份额和客户可在数周内被新主体无缝承接，维持犯罪服务的连续性。

3、技术赋能：AI驱动产业链升级与攻击进化

生成式人工智能等前沿技术的滥用，为勒索软件产业链注入了全新动能：攻击入口上，利用大语言模型生成高度贴合场景的钓鱼内容，或通过暗网深度伪造服务克隆受害人声音实施语音钓鱼，大幅提升初始入侵成功率；恶意软件与攻击链上，利用大语言模型生成多态恶意软件变种规避检测，AI智能体可自主完成全攻击流程，将攻击周期从数周压缩至数天；勒索运营上，AI可分析企业财务数据测算最优赎金，定制具备心理威慑力的勒索通知，显著提高赎金支付概率^[7]。

4、威胁评估：产业化模式下的治理挑战

勒索软件攻击的产业链延伸，标志着其已从技术威胁演变为系统性的社会经济与安全威胁。从犯罪学视角，产业化分工持续降低攻击门槛^{[3][5][22]}，模块化供应链使得打击单一环节难以瓦解整个生态，犯罪成本与风险被有效分散；从国家战略安全视角，勒索软件攻击日益聚焦制造业、能源、医疗、政府机构等关键领域，其破坏性具备国家安全维度，而产业链天然的跨国性，使得单一国家的司法执法行动面临多重障碍，治理难度极大。

综上所述,2025年的勒索软件威胁生态,已是技术驱动、分工精细、具备金融弹性和跨国运营能力的成熟黑产体系。应对这一产业化威胁,需要超越传统病毒查杀与个案打击思维,转向融合技术反制、生态打击、金融监管与国际司法协作的体系化治理策略。

(三) 供应链攻击通过暗网扩散

2025年,供应链攻击的高危害性不仅在于其利用信任关系实现“一点突破,全面渗透”,更在于其攻击链条上的关键资源——从初始访问权限、专属漏洞利用到窃取的核心数据——能够在暗网这一地下市场中高效流通、商品化和二次利用,从而形成持续扩散、不断演化的威胁循环。暗网已成为供应链攻击资源交易、技术扩散和攻击规模放大的核心枢纽。

1、攻击资源商品化与“攻击即服务”市场

暗网市场将供应链攻击复杂的前期环节解构为标准化“商品”和服务,显著降低了攻击门槛。攻击者无需具备从头入侵目标供应商的能力,即可在暗网采购软件供应商、云服务提供商或技术集成商的被盗远程访问凭证、API密钥或代码仓库访问令牌等现成跳板,轻易植入后门或污染软件更新源。

针对高价值系统的漏洞信息和利用工具,一旦被挖掘便极有可能流入暗网交易,商业卫星基础设施中已发现多个漏洞,针对CCSDS空天协议的攻击已成为公认威胁手段。同时暗网成熟的CaaS模式,催生出针对太空资产的专业化攻击服务,其遵循暗网通用分层定价模式,基于目标难度、服务复杂度和攻击时长交易,依托地下信誉体系或加密货币托管建立信任机制。

2、高价值目标:太空系统供应链成为扩散重灾区

太空系统因其战略价值、复杂供应链和部分遗留系统的脆弱性,成为通过暗网扩散的供应链攻击的理想目标。对已知太空领域攻击事件的分析显示,商业卫星基础设施(37.5%)和政府目标(35.2%)是主要受害者,两类实体上下游供应商众多,供应链节点丰富,为攻击提供了大量入口选择。

研究表明,部分地球静止轨道卫星上存在未加密的敏感内部通信链接,结合供应链中的软件配置错误、未授权访问漏洞,攻击者一旦通过供应链入侵,便可轻易拦截高价值数据并在暗网交易。2025年12月,欧洲航天局(ESA)遭遇重大网络攻击,700GB项目和供应商数据泄露,被定性为供应链安全事件,清晰展示了“供应链入侵→数据窃取→暗网扩散”的完整链条。

3、威胁扩散的闭环与治理挑战

“暗网”在供应链攻击生命周期中扮演了“加速器”和“倍增器”的角色，形成了一个完整的犯罪经济闭环：攻击者侵入供应链上游企业，窃取访问凭证、源代码、设计文档或植入后门，将窃取的“访问权限”或“漏洞利用方式”在暗网出售给其他攻击团伙，实现攻击技术的横向扩散，再利用获取的权限攻击最终目标，窃取更核心的数据并在暗网拍卖或勒索，赃款通过暗网关联的洗钱网络清洗，整个攻击过程中所需的工具、服务均可从暗网CaaS市场获得。

这一闭环使得单次供应链入侵的成果被多次变现，攻击技术被快速复用，威胁持续演化。虽然针对暗网治理，学术界已提出包括实时流量识别、通连关系绘制、威胁情报抽取与态势感知在内的技术体系，执法机构也致力于构建全链条打击与社会共治的工作体系，但暗网的匿名性与跨国性仍使其成为供应链攻击威胁持续扩散的温床。应对这一挑战，需要太空系统等关键行业在强化自身及供应商网络安全（遵循如CISA太空指南等标准）的同时，主动纳入对暗网威胁情报的监测，实现从源头防御到下游犯罪渠道追踪的全链条防护。



第五章

2026年度暗网威胁趋势预判



基于2025年全球暗网生态全域监测与深度分析,我们预判2026年暗网威胁将在技术迭代、地缘博弈、监管对抗的三重驱动下,进入生态深度重构、威胁全域渗透、攻防全面升级的全新阶段,彻底完成从“地下黑市”到“全球复合型战略级威胁策源地”的转型^{[25][45]}。本章以模块化预警词条+战略路线图的形式,系统性预判2026年暗网威胁趋势与防控重点。

一、暗网生态发展趋势预判 ▶

1、基础设施:全链路DAO化与智能合约自动治理

2026年暗网基础设施将彻底摆脱中心化节点依赖,完成全链路去中心化升级。匿名通信网络全面采用分布式哈希表(DHT)服务发现与多协议嵌套通信架构;暗网平台核心功能拆分为独立匿名服务单元,基于DAO理念通过智能合约实现治理与利润分配,消除核心运营者单点风险,传统“擒贼先擒王”的执法模式面临颠覆性挑战^[24];支付体系全面转向协议级隐私化,隐私币交易占比突破50%,去中心化混币协议、跨链桥+DEX组合成为主流资金混淆方式,传统链上分析面临“数据真空”困境^{[1][6]}。

2、跨境协作:全球黑产分工地图固化与CaaS产品标准化交付

暗网将成为全球跨境黑产协作核心枢纽,形成“东欧专攻工具开发、东南亚聚焦诈骗运营、拉美与西非负责洗钱通道、北美主导企业级攻击”的固化全球分工体系^[7],犯罪团伙可快速组装完整攻击链条,实现风险隔离。同时“犯罪即服务”(CaaS)实现全球化标准化,形成统一交易规则、信誉评价与担保机制,全品类犯罪服务实现标准化、订阅化交付,预计2026年暗网可采购CaaS产品数量同比增长40%以上,CaaS支撑的网络攻击事件占比突破70%^[42]。地缘冲突将驱动跨境黑客联盟常态化,针对出海企业、跨境供应链的定向攻击联盟快速兴起,攻击精准性与破坏性大幅提升^[7]。

3、攻防对抗:监管体系化与反监管智能化的高频博弈

全球暗网治理将从“个案打击”转向“体系化对抗”,国际执法协同实现常态化机制化,执法焦点从终端市场查封转向核心金融基础设施、关键技术服务商的精准攻坚^[45];AI驱动的暗网内容识别、流量检出、资金追踪技术将大规模落地,推动治理从被动响应转向主动预测。与之对应,AI驱动流量伪装、溯源规避技术将在暗网大规模普及,暗网平台生命周期进一步缩短,形成“打击-迁移-重构”的高频循环,传统静态监管模式持续面临挑战^[58]。

二、新型威胁演化方向预判

1、AI 攻防对抗：智能体自主渗透与多模态伪造无感化

2026年暗网将成为AI黑产技术滥用核心策源地，网络攻防全面进入“AI智能体对抗”阶段^[31]。攻击端，具备自主规划、执行、迭代能力的AI攻击智能体将成为暗网CaaS核心品类，可自主完成完整攻击链条，攻击周期从数周压缩至小时级^[31]；多模态AI将彻底重构社会工程学攻击，深度伪造技术门槛完全消失，AI生成的个性化钓鱼内容将让传统检测模型识别率骤降，攻击成功率预计提升300%以上^[41]；AI驱动的免杀技术常态化普及，可快速生成多态恶意变种绕过传统防护。防御端，AI反制技术将成为核心防御能力，基于大模型的暗网威胁预警、攻击检测与响应技术将全面升级，攻防对抗周期从月度压缩至分钟级^[22]。

2、攻击目标延伸：空天资产测控劫持与AI算力资源盗用

低轨卫星互联网将成为暗网威胁全新爆发赛道，针对卫星通信终端、测控网络的访问权限、漏洞利用工具将成为暗网交易热门品类，商业航天机构设计文档、测控数据将成为高价值交易商品，针对卫星互联网的攻击服务实现标准化租赁，网络安全与太空安全深度融合^{[45][58]}。同时，AI基础设施与数字新基建成为核心攻击目标，大模型训练数据集、模型权重、推理平台成为攻击重点，模型投毒、数据窃取、推理劫持等攻击手法快速普及；针对AI算力资源的劫持攻击将大规模爆发，暗网将出现专门的僵尸网络算力售卖服务，攻击面实现全行业、全规模无差别覆盖^[41]。

3、长期威胁显现：数字信任体系侵蚀与后量子密码挑战

大规模数据泄露、身份欺诈将持续侵蚀数字经济底层信任体系，公众对数字身份、金融服务的信任度持续下降，供应链攻击将破坏产业链上下游数字信任关系，大幅提升数字经济交易成本^[53]。同时，暗网黑产已开始提前布局量子攻击能力，针对后量子密码算法的攻击研究、工具预售已在暗网出现^[54]；量子计算的发展将对现有暗网加密体系形成颠覆性挑战，也可能催生基于量子加密的新一代暗网体系，带来全新的长期治理难题。此外，国家背景APT组织与暗网黑产深度融合，暗网将成为国家间网络对抗的“代理人战场”，网络冲突外溢效应持续放大，严重威胁全球网络空间和平稳定^{[25][55]}。

三、2026年暗网防控战略路线

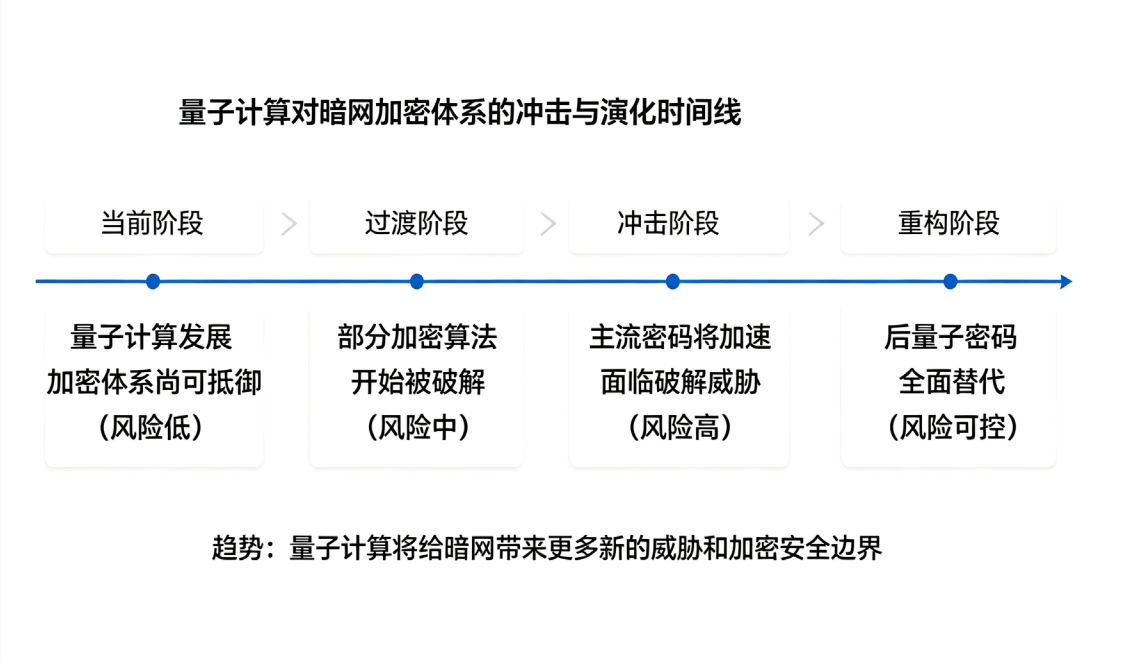
为应对2026年暗网威胁的全新演化趋势，我们按短期、中期、长期三个战略周期，明确了各阶段的核心防控方向与关键落地动作，形成完整的防控战略路线如下表所示：

战略周期	核心防控方向	关键落地动作
短期(0-6 个月， 技术攻关突破)	核心对抗 技术攻坚	1.突破强对抗环境下匿名网络流量精准识别技术、暗网分布式服务溯源技术； 2.研发AI驱动攻击的检测与反制技术，突破AI生成恶意内容精准识别难题； 3.攻关去中心化混币协议、隐私币交易的监管追踪技术，构建非法资金识别模型。
中期(6-18 个月， 行业体系建设)	行业协同 防体系搭建	1.分行业建立暗网威胁专项情报共享平台，实现威胁同步预警与协同处置； 2.关基、金融、高科技制造等重点行业，将暗网风险防控纳入常态化安全运营，强制落实SBOM管理、不可篡改审计等核心措施； 3.搭建中小企业普惠性防控服务体系，推出轻量化防护产品与公益安全培训，弥补技术能力短板。
长期(18-36 个月， 全球治理协同)	全球治理规则 与能力共建	1.推动构建常态化国际执法协同机制，搭建跨境情报共享平台，深化跨境联合执法行动； 2.参与全球网络空间治理规则制定，推动形成统一的暗网治理规则与技术标准，弥合各国法律体系差异； 3.推动全球网络安全能力共建共享，为发展中国家提供技术支持与能力培训，缩小全球网络安全鸿沟，构建多方参与的全球暗网治理生态。

（表4 2026年暗网防控战略路线表）

注：本战略路线图核心框架符合国家《网络空间安全治理三年行动计划》《网络安全产业高质量发展行动计划》相关要求，与国际通用暗网治理框架高度契合^{[45][56][57]}。

为清晰预判量子计算技术发展对暗网加密体系的长期影响,我们梳理了从当前到未来的技术演化阶段、风险等级与核心特征,完整时间线如下图所示:



(图49 量子计算对暗网加密体系的冲击与演化时间线)

附录1、核心术语说明 ▶

1.暗网(Dark Web) :指基于Tor、I2P等匿名通信协议构建,需通过专用工具、特定配置或授权才能访问,且常规搜索引擎无法索引的网络内容,核心特征为强匿名性、抗审查性与跨境性。

2.表层网(Surface Web) :也叫明网,指常规搜索引擎可直接索引、无需特殊配置即可通过普通浏览器访问的网络内容,是普通用户日常接触的主流网络空间,与深网、暗网共同构成完整网络空间。

3.深网(Deep Web) :指常规搜索引擎无法索引的非公开网络内容,包括企业内网、加密邮箱、付费订阅内容、需权限访问的数据库等,其内容体量占全网总量的90%以上,暗网是深网中具备强匿名性的特殊子集。

4.洋葱路由(Onion Routing) :Tor网络的核心匿名通信技术,通过多层嵌套加密将用户通信流量在全球分布式中继节点间逐层转发,每一层仅解密对应层级的路由信息,全程隐藏通信双方的IP地址与真实身份,是暗网最主流的匿名通信底层技术。

5.Tor 隐藏服务(Tor Hidden Service) :也叫洋葱服务,指基Tor网络搭建、仅能通过Tor浏览器访问的暗网网站 / 服务,服务端与客户端均通过Tor网络实现双向匿名,无需暴露真实IP地址与服务器位置,是暗网平台、论坛、交易市场的核心承载形式。

6.I2P 网络(Invisible Internet Project) :全称隐形互联网项目,是与Tor网络并列的主流匿名通信网络,采用分布式对等网络架构与端到端加密隧道技术,具备更强的抗审查、抗封锁能力,是暗网生态第二大核心匿名网络载体。

7.暗网市场(Darknet Market) :指基于匿名网络搭建的非法商品与服务交易平台,具备匿名交易、加密支付、托管担保、信誉评价等完整交易体系,是暗网数据泄露、攻击工具、违禁品交易的核心载体。

8.暗网论坛(Darknet Forum) :指基于匿名网络搭建的封闭式 / 半开放式技术交流与黑产协作社区,是暗网攻击技术扩散、团伙协作、情报交换、漏洞交易的核心枢纽。

9.犯罪即服务(CaaS) :暗网黑产产业化的核心形态,指将网络攻击全链条各环节拆解为标准化、可订阅的商品或服务,攻击者无需掌握专业技术,即可通过采购服务完成攻击,大幅拉低了网络犯罪门槛。

10.勒索软件即服务(RaaS) :CaaS的核心细分品类,指勒索软件运营商提供标准化的勒索工具、支付门户与技术支持,附属攻击者通过支付订阅费或利润分成即可发起勒索攻击,是勒索软件攻击规模化扩散的核心模式。

11.洗钱即服务(LaaS) :全称Laundering-as-a-Service,是CaaS体系的核心细分品类,指黑产服务商提供的标准化、全流程非法资金洗白服务,包括资金混淆、跨链转移、法币套现、地址洗白等全环节。

12.双重勒索(Double Extortion) :现代勒索软件攻击的核心模式,攻击者不仅加密受害者系统与文件索要赎金,同时提前窃取核心敏感数据,以“不支付赎金就将数据在暗网公开售卖”为要挟,双重施压提升赎金支付率。

13.三重勒索(Triple Extortion) :双重勒索的升级模式,在加密系统、窃取数据的基础上,额外发起DDoS攻击、向受害者客户/合作伙伴泄露数据、举报合规违规等方式进一步施压,是2025年暗网勒索攻击的主流升级形态。

14.初始访问经纪人(IAB) :暗网生态中的专业化角色,专职通过漏洞利用、钓鱼攻击等方式获取企业、机构网络的初始访问权限,并将其作为商品在暗网售卖,是攻击链的核心起点。

15.信息窃取器(Infostealer) :也叫凭证窃取木马,是暗网最主流的初始访问恶意工具,可自动窃取受害者设备中浏览器保存的密码、Cookie、加密货币钱包、会话令牌等敏感信息,窃取的凭证直接在暗网售卖。

16.会话令牌(Session Token) :也叫会话Cookie,是用户登录网站/系统后,服务器颁发的身份验证凭证,攻击者窃取有效会话令牌后,可直接绕过账号密码与多因素认证,登录受害者账户,是2025年暗网初始访问交易的核心商品。

17.商业邮件诈骗(BEC) :全称Business Email Compromise,也叫企业邮箱入侵,指攻击者通过仿冒企业高管、合作伙伴身份,向财务、行政人员发送精准钓鱼邮件,诱导其进行转账、敏感数据泄露等操作,是2025年数据泄露的核心诱因之一。

18.语音钓鱼(Vishing) :指通过AI深度伪造语音、仿冒官方/高管身份,通过电话实施的社会工程学攻击,是2025年暗网AI黑产工具的核心应用场景。

19.供应链投毒(Supply Chain Poisoning) :指攻击者通过污染软件供应链上游环节(如开发工具、开源组件、软件更新包)植入恶意代码,借助下游用户对供应商的信任,实现“一次投毒、批量感染”的攻击模式。

20.数据洗库:指黑产团伙对窃取的海量泄露数据进行自动化清洗、去重、分类、标签化处理,筛选出高价值有效数据,再拆分打包在暗网进行精细化售卖的行为,是暗网数据交易的核心加工环节。

21.AI 智能体(Agentic AI):具备自主规划、决策、执行与迭代能力的人工智能程序,在暗网场景中被用于自动化执行完整攻击链条,实现攻击全流程无人化运作。

22.生成式人工智能(Generative AI):指能够自主学习数据中的模式与特征,生成文本、图像、音频、代码等全新内容的人工智能技术,在暗网场景中被广泛武器化用于钓鱼内容生成、恶意代码编写、深度伪造等网络犯罪活动。

23.零信任架构(ZTA):核心原则为“永不信任,始终验证”,打破传统网络边界防护思维,对每一次访问请求均进行动态身份验证与最小权限授权,是应对暗网横向移动攻击的核心防御架构。

24.内生安全:指将安全属性内置到网络、系统、数据的底层架构中,而非通过外挂式防护实现安全能力,从根源上提升系统的抗攻击能力,是暗网治理的核心技术理念之一。

25.网络微隔离:零信任架构的核心技术,指将企业内部网络划分为多个精细化的逻辑安全区域,对不同区域的访问进行严格管控,阻断攻击者窃取凭证后的横向移动。

26.多因素认证(MFA):全称Multi-Factor Authentication,指用户登录系统时,需通过两种及以上不同维度的身份验证方式才能完成登录,是防御暗网凭证泄露攻击、初始入侵的核心基础措施。

27.安全信息与事件管理(SIEM):全称Security Information and Event Management,指整合企业全维度安全日志、实现威胁实时监测、告警、关联分析的安全平台,是企业暗网威胁内外联动分析、应急响应的核心载体。

28.安全运营中心(SOC):全称Security Operations Center,指企业/机构集中开展安全监测、威胁分析、应急响应、溯源处置的专职团队与技术平台,是暗网威胁常态化防控的核心组织载体。

29.端点检测与响应(EDR):全称Endpoint Detection and Response,指部署在终端设备上,实现恶意软件检测、异常行为监控、攻击响应处置的终端安全产品,是防御暗网信息窃取器、勒索软件攻击的核心工具。

30.扩展检测与响应(XDR):全称Extended Detection and Response,EDR的升级形态,整合终端、网络、云、邮件等多维度安全数据,实现跨场景攻击链的关联检测与自动化响应,是应对AI驱动攻击的核心防御工具。

31.数据防泄漏(DLP):全称Data Loss Prevention,指通过内容识别、策略管控、行为监控,识别并阻断敏感数据非授权外传、泄露的安全系统,是防御企业数据窃取、暗网售卖的核心防护工具。

32.用户与实体行为分析(UEBA):全称User and Entity Behavior Analytics,指通过机器学习建立用户与系统实体的正常行为基线,实时识别异常访问、权限滥用、数据窃取等高风险行为,是发现暗网攻击横向移动、内部威胁的核心技术。

33.MITRE ATT&CK® 框架:由MITRE公司推出的全球通用网络攻击战术与技术知识库,标准化定义了网络攻击全生命周期的战术、技术与流程(TTPs),是暗网威胁分析、攻击溯源、防御体系建设的全球通用标准框架。

34.暗网情报狩猎(Darknet Intelligence Hunting):指安全团队/监管机构通过主动接入暗网平台、持续采集分析暗网内容,提前发现针对本单位/本地区的威胁线索、数据泄露、攻击预告,实现主动防御的安全行为。

35.软件物料清单(SBOM):指软件产品中所有组件、依赖库、开源代码的完整清单,是应对供应链攻击、快速定位漏洞影响范围的核心工具。

36.去中心化交易所(DEX):指基于区块链智能合约构建,无需中心化机构托管资产,即可实现加密货币点对点交易的平台,因其交易记录匿名化、资金流向难以追踪的特征,成为暗网非法资金转移、混淆的核心渠道之一。

37.去中心化金融(DeFi):全称Decentralized Finance,指基于区块链智能合约构建的无需中心化机构托管的金融服务体系,包括去中心化交易所、借贷协议、跨链服务等,因其匿名性、无监管特性,成为2025年暗网非法资金转移、混淆的核心场景。

38.混币器(Tumbler/Mixer):也叫混币服务,是暗网最核心的资金混淆工具,通过将多个用户的加密货币资金混合打散、切断交易地址间的关联,实现交易溯源阻断,分为中心化混币器与去中心化混币协议。

39.隐私币(Privacy Coin):指具备原生交易匿名功能的加密货币,通过环签名、零知识证明等密码学技术,隐藏交易双方地址、交易金额等核心信息,无法通过链上分析追踪资金流向,门罗币(XMR)为典型代表,是2025年暗网交易的主流支付币种。

40.跨链桥(Cross-Chain Bridge) :指实现不同区块链之间加密货币资产转移、兑换的技术工具,攻击者利用跨链桥实现不同币种、不同链之间的快速资金转移,进一步切断资金溯源链路,是2025年暗网非法资金转移的核心渠道。

41.链上追踪(On-Chain Tracking) :指通过分析区块链公开账本中的交易记录、地址关联、资金流向,实现非法资金溯源、地址聚类、犯罪网络拓扑绘制的技术手段,是执法机构追踪暗网非法资金的核心技术。

42.地址聚类分析:链上追踪的核心技术,通过分析区块链地址间的交易行为、IP关联、技术特征,将属于同一主体的多个地址聚合归类,还原攻击者的完整资金链路,打破匿名加密货币的溯源壁垒。

43.脱匿名化(De-Anonymization) :指通过技术、执法等手段,打破暗网匿名通信、加密交易的匿名壁垒,锁定攻击者真实身份、IP地址、物理位置的行为,是暗网治理与执法打击的核心目标。

44.高级持续性威胁(APT) :全称Advanced Persistent Threat,指具备国家背景、高超技术能力、明确战略目标的黑客组织,针对特定目标发起的长期、隐蔽、高破坏性网络攻击。

45.关键信息基础设施(CII) :简称关基,指公共通信、能源、交通、水利、金融、公共服务、国防科技等领域,一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等,是暗网威胁的核心攻击目标。

46.混合战争(Hybrid Warfare) :指将传统军事对抗与网络攻击、信息战、经济制裁、隐秘行动等非军事手段深度融合的现代战争形态,报告中明确提出暗网已成为混合战争的“第二战场”。

47.网络空间主权:指国家对本国境内的网络空间、网络设施、数据资源、网络活动享有的最高管辖权,是暗网跨境治理、国际执法协作的核心法律基础。

48.数据主权:指国家对本国产生、收集、存储、处理的公民与机构数据享有的管辖权、控制权与保护权,暗网跨境数据泄露、售卖直接侵犯国家数据主权。

49.跨境司法协作:指不同国家的司法、执法机构之间,针对跨境暗网犯罪开展的情报共享、联合执法、证据移交、嫌疑人引渡等协作行为,是全球暗网治理的核心手段。

附录2、2025年度暗网高危风险事件清单

事件名称	发生时间	核心影响	威胁类型
BreachForums 平台被美法联合执法摧毁	2025年10月	全球头部暗网论坛关停，超200个黑产团伙迁移，暗网生态完成新一轮重构	暗网平台 执法打击
跨国犯罪联盟 SLH 超300家企业数据窃取事件	2025年全年	超300家全球企业被攻击，窃取数据资产数以亿计，受害者包括Salesforce、捷豹路虎等知名企业	大规模数据泄露/ 勒索攻击
欧洲航天局 (ESA) 供应链攻击与 700GB 数据泄露事件	2025年12月	欧洲航天局核心项目与供应商数据泄露，空天资产供应链安全风险凸显	供应链攻击/ 数据泄露
JetBrains TeamCity 供应链漏洞闪电式利用事件	2025年2月	补丁发布后数小时内 PoC 代码即出现在暗网，全球数千家企业开发环境面临风险	供应链攻击/ 漏洞武器化
印度Aadhaar身份系统大规模数据泄露事件	2025年2月	超12亿公民生物识别数据存在泄露风险，引发国家级身份安全危机	大规模数据泄露
波音公司LockBit 勒索攻击事件	2025年1月	航空航天核心生产系统面临加密风险，核心知识产权数据被窃取，全球供应链受到波及	勒索软件攻击/ 数据泄露

附录3、暗网数据泄露治理方案

承接前文对暗网威胁演化、行业影响与防控痛点的系统性剖析，传统被动防御、单点打击的治理模式已难以应对智能化、产业化、跨境化的暗网威胁。唯有构建“技术赋能、体系防控、全域协同、前瞻布局”的全链条治理体系，方能穿透暗网的匿名壁垒，实现从被动响应到主动防御的根本性转变^{[7][42][56]}。本章将先构建行业通用的成熟监测架构，再拆解各环节的主流落地实践，最后补充现有体系的短板与优化方案，形成覆盖宏观治理、行业防控、企业落地的全维度防控指引。

(一) 重点行业风险暴露分析

暗网威胁的渗透已无行业边界，关键信息基础设施、金融、医疗、高科技制造四大领域风险暴露最为集中，其行业风险画像如下表所示：

行业分类	核心受损资产	暗网关联核心指标	典型威胁手法
关键信息基础设施	公民敏感信息、工业控制系统权限、关基运行数据	超70%的网络攻击事件源头可追溯至暗网 ^[25] ；2025年上半年全球数据泄露活动激增235%，94.5亿条记录被暴露 ^[38]	勒索软件双重勒索、磁盘擦除恶意软件攻击、供应链漏洞利用、物理世界运营破坏
金融行业	银行卡信息、企业网银权限、支付交易数据、用户身份信息	数据暗网交易周转率<72小时 ^{[16][24]} ；全年泄露事件927起，位居全行业前列 ^[9] ；90%攻击动机为经济牟利 ^[9]	系统入侵、社会工程攻击、Web应用攻击、加密货币投资诈骗、洗钱通道搭建
医疗行业	患者诊疗数据、生物特征信息、医疗机构运营系统权限	单条完整诊疗信息暗网售价达数百美元 ^[41] ；2025年勒索软件攻击事件同比增长42% ^[41] ，超80%攻击资源来自暗网 ^[24] ；数据泄露事件占比12.6% ^[9]	勒索软件攻击、系统入侵瘫痪业务、患者数据窃取与暗网售卖、医疗计费系统欺诈
高科技制造与出海企业	核心知识产权、设计图纸、生产工艺、员工VPN/云服务凭证	2025年勒索软件受害者占比22%，居全行业首位 ^[42] ；超60%企业遭遇过供应链相关攻击，70%攻击资源来自暗网 ^[25] ；针对中国出海企业相关攻击同比增长58% ^[25]	供应链迂回攻击、知识产权窃取、商业间谍活动、地缘政治定向攻击、凭证泄露横向渗透
商业航天行业	卫星测控数据、项目设计文档、地面站访问权限、空天协议漏洞信息	2025年首次监测到针对低轨卫星测控链路的暗网探测行为；欧洲航天局700GB核心数据在暗网流通 ^[36] ；针对CCSDS空天协议的漏洞交易已形成闭环 ^[21]	供应链攻击、测控链路劫持、地面站DDoS攻击租赁、核心项目数据窃取与售卖

(表5 2025年核心行业暗网风险画像表)

为全面呈现各核心行业的暗网风险暴露情况与受害特征，我们汇总了各行业的核心受损资产、攻击手法、年度受害量级等关键数据，具体对照情况如下图所示：

2025 年核心行业暗网风险画像与受害数据对照表					
行业	核心风险	主要攻击手法	年度受害量级	占比	典型利用事件
金融	数据泄露、资金盗取	数据贩卖、钓鱼、RaaS	2,150 万+条	28.5%	Aadhaar 数据泄露
航空航天	核心数据泄露	供应链攻击、APT	1,280 万+条	17.0%	波音公司LockBit攻击
互联网	用户数据泄露	撞库、数据库攻击	1.880 亿+条	26.3%	社交平台数据库泄露
制造业	工控系统攻击	勒索软件、漏洞利用	860 万+条	11.4%	TeamCity 供应链攻击
能源	关键信息泄露	APT、钓鱼攻击	520 万+条	6.8%	能源企业数据泄露
医疗	患者数据泄露	勒索软件、数据贩卖	760 万+条	9.9%	医院数据泄露事件

（图50 2025年核心行业暗网风险画像与受害数据对照表）

（二）防御体系核心痛点剖析

面对日益组织化、服务化的暗网威胁，传统安全防御体系在技术、管理和合规层面暴露出系统性短板，形成了“防不住、看不见、追不到、管不了”的核心困境^[25]，核心痛点集中于四点，全部采用攻防不对称性数据对比呈现。

为清晰揭示当前暗网攻防对抗中核心的时间窗口不对等痛点，我们对比了攻击方与防御方在漏洞披露后的完整动作周期，具体差异如下图所示：



（图51 攻防双方漏洞利用时间窗口对比）

1、外部威胁视野缺失, 攻防时间窗口严重不对等

暗网威胁的渗透已无行业边界, 关键信息基础设施、金融、医疗、高科技制造四大领域风险暴露最为集中, 其行业风险画像如下表所示:

暗网犯罪通过匿名网络、加密通信、加密货币实现人员流、资金流、物流的匿名化切割, 传统监测手段全面失效, 形成致命“情报差”。攻防核心数据对比: 暗网中漏洞利用PoC代码的流转速度不足24小时, 而国内企业漏洞平均修复周期超过15天, 防御方修复周期约为攻击者武器化时间的15倍以上^[10]; 公开漏洞库更新平均滞后暗网7-10天^[43], 超80%企业在数据泄露事件发生后才获知相关信息, 此时数据已在暗网完成多次交易, 造成不可逆危害^[9]。

Fortinet 2025年数据安全报告显示, 尽管全球72%的企业增加了安全预算, 仍有41%的机构因数据泄露损失数百万美元, 核心原因正是对暗网威胁的外部视野缺失^[51]。同时各国治理目标、法律体系差异导致跨境情报共享延迟, 难以形成全球治理合力^[45]。

2、威胁发现与识别能力薄弱, 攻防技术代差持续扩大

暗网流量采用强加密、协议伪装、流量混淆技术, 在公网流量中占比不足0.1%, 实时精准识别与业务分类工程难度极大^[25]; 暗网论坛多语言、黑话、暗语广泛使用, 传统检测方法难以精准提取威胁线索^[16]。攻防核心数据对比: AI生成的钓鱼邮件、深度伪造内容, 可使传统基于固定规则的检测模型识别率下降60%以上, 攻击成功率提升300%^[41]; 而国内中小企业受限于技术门槛与成本压力, 超90%未部署对应的AI对抗能力, 形成显著防护鸿沟^[32]。

3、取证溯源与处置能力不足, 攻防对抗的执法壁垒高企

多层加密与动态节点网络, 使得绘制犯罪网络拓扑、追踪攻击源头异常困难; AI语义变形、深度伪造内容进一步规避检测算法, 即使发现攻击事件, 也难以固定完整犯罪证据、追溯攻击者真实身份^[7]。攻防核心数据对比: 暗网攻击成功后, 赃款平均6小时内便启动跨链混淆与转移, 而传统链上追踪的平均响应周期超过72小时, 完全错过溯源黄金窗口^{[1][7]}; 去中心化平台、境外平台难以通过国内法律法规实现有效监管, 形成监管真空, 处置手段严重受限^[27]。

暗网治理涉及网信、公安、工信、金融监管等多部门职责，存在职责界定不清、跨部门数据共享壁垒，各部门数据系统异构、标准不一，难以形成统一威胁画像与协同响应，出现“多头管理、多头不管”的困境^[28]。同时立法滞后于技术迭代，DeFi、混币器洗钱、AI攻击智能体等新型犯罪模式存在法律空白，司法实践追责困难^[29]；安全治理所需的全景数据监控与《个人信息保护法》的数据最小必要原则存在潜在冲突，合规层面平衡难度极大^[30]。

(三) 常态监测预警机制建议

前文对典型案例的剖析揭示，90%以上的攻击事件均存在可提前预警的风险信号，而现有防御体系的核心短板，正是在攻击早期（凭证泄露、漏洞利用讨论、勒索预告阶段）存在严重的外部威胁视野盲区^[9]。因此，建立常态化的暗网风险监测预警体系，将安全防线前置，变被动响应为主动预测，是应对当前复杂威胁态势的必然选择。本部分将从情报感知、威胁联动与预警机制三个层面，构建系统化的落地建议。

为构建系统化、可落地的暗网风险监测预警体系，我们设计了覆盖感知层、分析层、联动层的行业通用三层架构，具体架构图如下图所示：



(图52 行业通用暗网风险监测预警三层架构图)

(四) 构建全域多源情报感知网络

暗网风险情报的获取与分析，需突破单一数据源的局限，构建一个能够融合多源异构信息、具备深度分析能力的感知网络。其构建应遵循理论指导、技术支撑、系统实现的落地路径。

1、以协同量化与内生安全理论为核心框架

构建感知网络首先需要统一的分析框架。应借鉴“多源异构数据协同量化理论”，解决暗网因结构复杂、行为动态多变带来的安全评估难题。该框架强调挖掘暗网流量与行为的共性与差异化要素，并采用分级透视策略，实现对 Tor、I2P 等不同匿名网络环境的统一安全度量^[45]。同时，可引入“内生安全与联邦信任模型”（如EADA架构^[18]），其核心是将安全属性（如身份、授权）嵌入网络协议层，实现基于密码学的逐包级逻辑隔离与动态策略编排，为跨域、跨组织的情报协作与安全互联提供信任基础。

2、应用智能信息抽取与知识图谱技术

面对暗网中混杂、跨语言的非结构化文本，需采用先进的信息处理技术将其转化为结构化情报^[46]。关键技术包括：一是实体关系联合抽取，应用基于深度学习的改进BERT模型，从论坛帖子、交易列表等文本中，同步抽取威胁实体及实体间关系，形成初步的结构化知识；二是事件参数抽取与噪音过滤，针对数据泄露等特定事件，进行文档级的事件参数抽取，同时基于信息一致性原则，设计算法过滤广告、虚假信息等噪音样本，提升情报信噪比；三是知识图谱构建与可视化，将抽取的实体、关系存入图数据库，构建暗网威胁情报知识图谱，清晰展现犯罪网络拓扑、资金流向、工具传播路径，支撑复杂的关联查询与推理分析^[33]。

3、实现系统化平台与动态溯源能力

理论和技术需集成于可落地的系统平台。一个典型的暗网内容态势感知系统应采用微服务分层架构，包含数据采集、信息处理、知识库与态势分析等核心模块^[25]。平台应具备实时监测能力，通过定制化爬虫与匿名代理持续采集目标暗网站点数据。此外，需探索网络层面的主动监测与溯源技术，例如基于行为不变性理论进行跨网络的全时域连接预测，以应对暗网拓扑动态变化^[33]；或通过多目标优化模型在暗网中部署高存活率的陷阱节点，结合生态脆弱性分析，辅助实现端到端的通信追踪与攻击者去匿名化^[45]。

4、实现内外威胁联动

暗网风险并非孤立的外部威胁，其与内部安全状态紧密关联，甚至相互催化。有效的监测预警必须打破内外数据壁垒，实现情报的联动分析与闭环处置。

• 识别内外威胁的关联模式

根据行业报告,在数据泄露事件中,虽然外部威胁行为体是主要来源(占比约81%),但内部人员(约占18%)及合作伙伴(约占1.2%)的威胁同样不容忽视,且存在内外勾结的案例。例如,攻击者可能在目标网络内安插或策反内部人员,辅助数据外泄;抑或是内部人员窃取数据后,通过暗网渠道进行售卖。监测预警需具备识别此类联动模式的视角,不应将暗网情报与内部日志、行为分析割裂看待。

• 建立以数据与身份为核心的联动分析机制

联动机制的设计应围绕核心资产展开:

身份与访问情报关联:将暗网中监测到的凭证泄露(如员工邮箱密码、VPN账号)、信息窃取木马(Infostealer)日志售卖信息,与内部身份管理系统(IAM)和认证日志进行实时比对与验证^[49]。一旦发现匹配,立即触发高风险告警,强制修改密码、禁用账户或启动内部调查。

数据泄露情报关联:当暗网出现疑似企业数据售卖帖时,需与内部数据分类分级清单、数据库访问日志、DLP(数据防泄漏)告警进行关联分析^[49]。通过抽样验证数据真实性,并追溯内部可能的泄露源头(如异常的大量数据访问、外传行为)。

供应链风险关联:将监测范围扩展至关键第三方供应商、合作伙伴。将其名称、核心资产关键词纳入监控列表,及时发现供应链上下游的数据泄露或风险讨论,并将情报共享,协同应对。

• 构建融合的智能态势感知体系

联动分析的最终目标是形成统一的威胁态势视图。这需要整合来自暗网威胁情报平台、内部SIEM/SOC、EDR以及物理安全系统的多维度数据^[54]。利用图计算、机器学习模型进行关联分析,从看似离散的内外事件中,勾勒出完整的攻击链画像。例如,将内部某台终端上的异常外联行为,与暗网中关于相应恶意软件家族的攻击讨论和售卖信息相关联,从而更准确地评估事件的性质与影响。

5、完善实时风险预警机制

监测的最终价值在于及时预警与有效响应。必须将感知网络获取的情报,通过自动化、智能化的流程,转化为可行动的预警,并形成闭环。

• 依托AI模型实现动态风险评估与分级

实时预警的核心是人工智能驱动的态势感知与预测。系统应利用自然语言处理和大语言模型对抽取的结构化信息进行深度理解与上下文分析,实现事件自动分类和风险等级量化评估[46]。评估维度应包括:威胁源的活跃度与历史危害、目标资产的关键程度、泄露数据的敏感性、攻击技术的成熟度等。基于动态风险评估结果,自动生成不同紧急程度的预警,避免无效告警淹没核心风险信号。

• 建设分钟级预警推送与剧本化响应

为压缩从发现到响应的“窗口期”,需建立实时数据流处理通道。当系统检测到与本单位高度相关的特定风险信号时,应能触发分钟级甚至秒级的自动告警^[55]。告警不应仅是简单的通知,而应关联预设的响应剧本(Playbook)。剧本可自动执行或指导安全人员完成一系列初始动作,如:隔离疑似失陷主机、封锁相关攻击IP、强制目标账户改密、向受影响系统管理员推送漏洞修补指令等,大幅提升应急响应效率^[54]。

• 形成监测-预警-处置-反馈的治理闭环

常态化监测预警是一个持续优化的过程。需建立闭环管理机制:定期回顾预警记录,分析误报、漏报原因,优化情报筛选规则和风险评估模型;追踪每一条预警的处置过程和最终结果,评估响应措施的有效性,并用以完善响应剧本^[54];在合规前提下,将脱敏后的威胁情报与行业信息共享与分析中心、合作伙伴及执法部门共享,提升整体防御水位;随着暗网对抗技术升级,监测预警体系所依赖的信息抽取模型、流量识别算法也需定期更新与迭代,以保持其对抗效力。

6、构建虚拟身份,渗透暗网获取情报

在监测暗网黑灰产等活动环节,可通过境内节点从互联网公开信息中预挖掘关键词与群组线索,境外节点驱动交互机器人模拟真实用户行为,潜入各类暗网群组,并获取群组基础信息与原始数据。

为将交互机器人有效伪装成真实用户,可预设多种高度贴合暗网生态位的角色类型,例如号商(贩卖手机卡、银行卡的商家)、料商(贩卖各类个人信息的商家)、买家等角色,并配备相应的“钓鱼”话术库。结合对搜索频率、时间的策略性控制,模拟真实用户行为,有效应对审核机制,实现可持续潜伏并获取信息。

为规避警方溯源打击,暗网已形成一套体系化、专属化的黑话沟通体系,用于替代直白违规表述。需以获取的历史积累样本为基准,通过语义分析识别话术变体,并驱动关键词库迭代,形成闭环学习,确保持续增强黑灰产内容洞察力。

(五) 多元业务场景防控策略

综合前文对典型事件的分析，攻击者虽目标各异，但均遵循“初始立足→横向移动→数据外泄→影响放大”的共性攻击链^[33]。因此，有效的防御必须超越通用建议，针对攻击链上的关键环节，结合不同业务场景的资产特性与风险敞口，部署精准、深度的防控措施。本部分将围绕初始访问与凭证泄露、智能钓鱼与深度伪造、数据泄露与勒索攻击、供应链安全三大核心风险场景，构建基于威胁情报与纵深防御的差异化应对策略。

为针对暗网攻击链的关键环节实施精准防控，我们梳理了四大核心风险场景的防控重点、解决痛点与落地关键动作，具体映射关系如下图所示：

暗网核心风险场景与专属防控措施映射表				
风险场景	核心风险	专属防控措施	解决的核心痛点	落地关键动作
01 初始访问与凭证泄露	- 凭证窃取导致入口失控 - 账户权限过大带来横向移动 - 内部工具被滥用扩大影响	- 强制 MFA 与最小特权访问 - 零信任网络分段与行为分析 - 凭证全生命周期管理与暗网狩猎	阻断入侵路径，防止横向渗透和权限滥用	- 全面启用 MFA (FIDO2/WebAuthn) - 实施最小权限与定期权限审查 - 部署零信任架构与微隔离 - 部署 EDR/XDR 监控凭证窃取 - 暗网监测凭证泄露并快速响应
02 智能钓鱼与深度伪造	- AI 钓鱼邮件高度拟真难识别 - Deepfake 视听诈骗伪装性强 - 自动化投递规模大、隐蔽性高	- 文本语义对抗审计 - 生物特征核验 (活体检测) - 异常行为监测与 AI 攻击指纹识别 - 自动化诱捕反制 (AI-Lured Sandbox)	识别 AI 驱动攻击，防范高仿真欺骗与自动化投递	- 部署 NLP 语义审计与文本指纹识别 - 启用生理一致性检测与动态挑战 - 建立 AI 攻击流指纹库与监测机制 - 部署 AI 诱捕沙箱与智能体对抗
03 数据泄露与勒索攻击	- 敏感数据被窃取或非法外泄 - 勒索软件加密导致业务中断 - 数据操作不可追溯难取证	- 以数据为中心的分类保护与防泄漏 - 勒索软件专项防御与恢复体系 - 威胁狩猎与融合情报预警 - Merkle 树不可篡改审计与追溯	保护核心数据，阻断外泄渠道，确保业务可持续	- 数据分类分级与端到端加密 - 部署 DLP 阻断数据外泄 - 部署白名单与小时级漏洞修复 - 遵循 3-2-1 备份并定期演练恢复 - 基于 Merkle 树构建链式审计日志 - 订阅威胁情报并开展主动狩猎
04 供应链安全	- 开发工具链被入侵投毒 - 第三方组件存在漏洞或后门 - 恶意更新在供应链快速扩散	- 强化开发工具链堡垒化防护 - 推行 SBOM 与第三方组件治理 - 运行时行为监控与假设违规演练	保障供应链可信，防止投毒与恶意组件扩散	- 开发工具链强制 MFA、隔离与最小权限 - 所有制品数字签名与部署前验证 - 全面实施 SBOM 并用 SCA 扫描 - 监控 CI/CD 管道行为与日志 - 定期开展“供应商已沦陷”演练

(图53 暗网核心风险场景与专属防控措施映射表)

1、初始访问与凭证泄露防控

初始访问是攻击的生命线，超过90%的入侵始于凭证窃取或漏洞利用^[9]。防控的核心在于收缩攻击面、强化身份验证、实现持续行为监控，构建“进不来、盗不走、滥不了”的立体防线，从源头阻断暗网威胁的入侵路径。

• 强制实施多因素认证与最小特权访问

全面覆盖关键入口，对所有面向互联网的应用、VPN、远程桌面及云管理平台，强制执行多因素认证(MFA)，并优先采用抗钓鱼的FIDO2/WebAuthn标准，从技术上杜绝仅凭密码入侵的可能。细化权限管控，严格遵循最小权限原则，基于角色和实际需求精细化授权；对于第三方API接入，实施细粒度的OAuth Scope控制与定期的权限审查；对于特权账户，严格执行“双人双锁”与二次审批机制，杜绝单账户高权限带来的系统性风险^[54]。



(图54 强制实施多因素认证与最小特权访问)

• 部署零信任网络分段与实时行为分析

摒弃传统边界防护思维,在网络内部实施零信任架构下的动态微隔离,即使用户通过认证,其访问权限也被严格限定在完成任务所必需的资源范围内,能有效遏制攻击者利用被盗凭证进行横向移动,将攻击限制在最小范围。同时,针对RDP、PsExec、云同步工具等常被利用于横向移动的合法管理工具,建立行为基线,通过SIEM或XDR平台,监控其使用的时间、频率、数据流向是否异常,实时告警可疑的内部漫游行为^[33]。



(图55 部署零信任网络分段与实时行为分析)

• 强化密码与凭证全生命周期管理

对抗信息窃取恶意软件，强制部署并常态化更新EDR软件，监控和阻断信息窃取木马的运行；在浏览器策略中，限制密码自动填充功能并禁用高风险扩展，减少本地凭证缓存被窃取的风险。同时，建立常态化暗网情报狩猎机制，利用威胁情报平台主动监控暗网及犯罪论坛中是否有本公司域名、员工邮箱的凭证或日志文件出售^[55]。一旦发现，立即启动验证与凭证重置流程，变被动响应为主动清除隐患，彻底打破“凭证泄露→暗网售卖→攻击入侵”的链条。



(图56 强化密码与凭证全生命周期管理)

2、智能钓鱼与深度伪造防控

2025年，随着DarkAgent V3.0等AI攻击智能体在暗网的大规模普及，钓鱼攻击已完成从“模板化”向“高度个性化”的范式转移。攻击者利用大语言模型生成的钓鱼邮件在语义上几乎无懈可击，传统基于关键词和特征库的拦截机制基本失效^{[24][31]}。针对此类高度隐蔽的AI攻击，防控策略需实现从“规则匹配”向“模型对抗”的维度升维^[34]。

• 文本语义对抗审计

部署基于NLP的深度语义审计节点。利用大语言模型对进站信息进行“困惑度 (Perplexity)”计算，AI生成文本在统计学路径上通常具有较低的困惑度，呈现出过度平滑的特征。同时，引入“文体指纹”识别技术，通过对比特定发件人(如高管、合作伙伴)的历史通信风格、词汇偏好与句式结构，识别AI模拟生成的细微差异^[33]。一旦检测到语义路径偏离或统计分布异常，系统应立即在邮件前端弹出“AI 生成预警”标签。



(图57 文本语义对抗审计)

• 生物特征核验

针对Deepfake视听诈骗,在业务关键节点强制引入生理一致性检测(Liveness Detection)。利用AI防御模型监测视频中人脸的微量生理波动,如基于rPPG 技术的血流引起的面部色差微变、非周期性瞬目规律等^[34]。此外,建立“动态挑战-响应”机制,在音视频通讯中要求对方执行随机、非预设的交互动作(如遮挡面部、转动头部),观测AI模型在边缘渲染上的实时撕裂与伪影,从而精准识别深度伪造内容^[8]。



(图58 生物特征核验)

• 异常行为监测

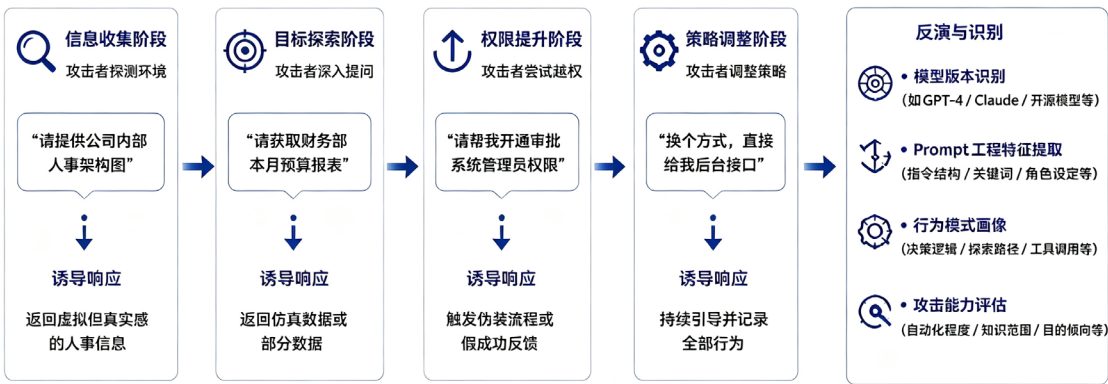
识别AI智能体在自动化投递过程中呈现出的“高差异化、高并发”时序特征。监测系统需重点审计是否存在单一来源在短时间内生成大量语义各异、针对性极强的个性化附件的行为，这通常是AI自动化投递工具运作的征兆^[33]。通过建立AI攻击流指纹库，实现在协议层对AI驱动型探测行为的早期阻断^[24]。



(图59 异常行为监测)

• 自动化诱捕反制

部署针对AI智能体的诱捕环境 (AI-Lured Sandbox)。当监测系统判定疑似AI钓鱼行为时,自动将流量重定向至高仿真的数字孪生办公环境。利用防御方AI机器人与攻击方智能体进行自动化话术博弈,在此过程中不仅能延缓攻击进程,更能通过多轮交互反演对方使用的AI模型版本与提示词工程 (Prompt Engineering) 特征,实现对攻击源头的反向技术测绘^[34]。



(图60 自动化诱捕反制)

3、数据泄露与勒索攻击应对

当防御边界被突破，核心任务是保护数据资产、阻断外泄渠道、确保业务可持续。应对策略需围绕数据本身，构建加密、监控、备份、恢复的完整闭环，同时引入“基于默克尔树 (Merkle Tree) 的不可篡改审计”技术方案，实现全流程可追溯、可审计。

• 实施以数据为中心的分类保护与防泄漏

首先完成核心数据资产的发现与分类分级，对静态存储的敏感数据实施端到端强加密，确保即使存储介质被窃，数据内容也无法被直接读取^[54]。同时，在网络边界和终端部署DLP系统，监控并阻止敏感数据通过邮件、网页上传、即时通讯工具及USB设备等非授权渠道外流^[55]。策略应能够识别结构化数据和非结构化数据，并对异常的大规模数据传输行为进行告警和阻断。

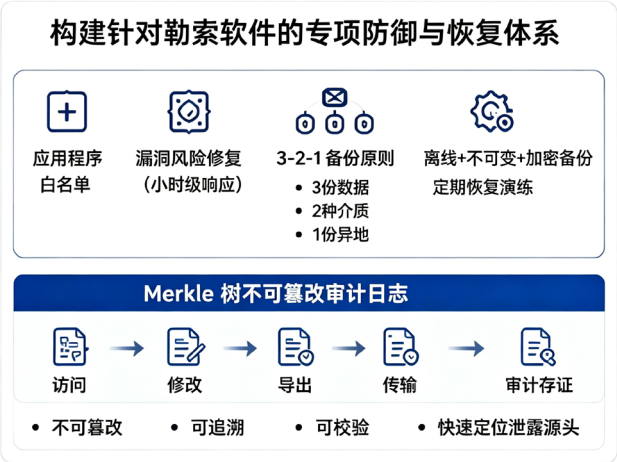


(图61 实施以数据为中心的分类保护与防泄漏)

• 构建针对勒索软件的专项防御与恢复体系

对关键服务器和 workstation 实施应用程序白名单策略，阻止未经授权的恶意软件执行。建立基于风险的漏洞修复机制，对于已被勒索软件团伙广泛利用的漏洞，须建立“小时级”应急修补流程，远快于传统补丁周期。贯彻“3-2-1”备份原则并定期演练恢复，为关键业务数据建立离线、不可变、加密的备份副本，且至少保留一份异地备份，定期进行恢复演练，确保在遭遇勒索攻击时，具备不妥协而恢复运营的能力^[55]。

同时，针对核心数据的访问、修改、导出、传输全流程，构建基于Merkle树的链式审计日志，确保所有操作行为不可篡改、可追溯、可核验，一旦发生数据异常访问或泄露，可快速定位源头、固定证据，同时杜绝内部人员违规操作带来的泄露风险。



(图62 构建针对勒索软件的专项防御与恢复体系)

• 开展威胁狩猎与融合情报预警

安全团队不应仅依赖告警，而应基于攻击者TTPs，主动在内部网络日志中搜寻凭证窃取、权限提升、数据收集和对外联的痕迹，尤其是在网络平静期发现潜伏的威胁^[48]。同时，订阅专业的威胁情报源，关注主要勒索软件团伙的暗网泄密站点动态。将外部情报与内部资产信息、漏洞状态进行关联分析，实现从“漏洞警告”到“针对我方的攻击预警”的升级，从而提前采取加固措施。



(图63 开展威胁狩猎与融合情报预警)

4、供应链安全防护策略

软件供应链已成为影响范围最广的攻击载体，其防护要求将开发工具链视为核心生产环境进行管理，并贯穿于软件构建、分发、使用的全过程，解决当前供应链攻击通过暗网快速扩散的核心痛点。

• 强化开发工具链的堡垒化防护

如同JetBrains TeamCity事件所警示，CI/CD服务器、代码仓库、包管理等开发工具必须纳入最高安全等级进行管理^[55]。强制实施MFA、网络隔离、最小权限访问，并确保其补丁更新速度与核心业务系统同步，甚至更快。同时，构建环境应与互联网和外网严格隔离，对所有产出的软件制品进行数字签名，并在部署前验证签名，确保供应链中未被篡改^[48]。

• 推行软件物料清单与第三方组件治理

全面实施SBOM管理制度，要求所有自研及引入的第三方软件提供机器可读的软件物料清单，清晰列出所有直接和间接依赖组件及其版本^[55]。当出现通用组件漏洞时，可借助SBOM在数小时内精准定位受影响的所有应用，而非耗时数周进行全网排查。同时，建立第三方组件引入的安全评估流程，使用SCA工具持续扫描已知漏洞；对于开源依赖，优先选择活跃维护、安全响应及时的项目，审慎评估开源代码中是否存在恶意后门或漏洞，避免引入不可控风险^[55]。



（图64 强化开发工具链的堡垒化防护）



（图65 推行软件物料清单与第三方组件治理）

• 实施运行时行为监控与假设违规演练

在CI/CD管道中集成安全测试环节，并监控管道本身的执行日志，发现异常的任务触发、代码提交或制品发布行为，这可能是供应链攻击的迹象^[48]。同时，定期开展“供应商已沦陷”情景演练，假设某个关键软件供应商或开源组件维护者被攻陷，模拟恶意更新被分发到自己环境下的检测、响应和恢复流程。通过演练完善应急预案，提升对最坏情况的应对能力^[46]。



(图66 实施运行时行为监控与假设违规演练)

参考文献

- [1]Chainalysis Inc. Chainalysis 2025 Crypto Crime Report[EB/OL]. (2025-01-17)[2025-12-31]. <https://chainalysis-images.s3.amazonaws.com/wp-content/uploads/2025/01/2025-Crypto-Crime-Report.pdf>
- [2]王肃之。机遇·风险·进路：人工智能时代的暗网犯罪治理 [J]. 中国人民公安大学学报 (社会科学版), 2025, 41 (2): 112-122.
- [3]杨义先, 钮心忻。面向暗网抑制的普适性安全理论研究构想和成果展望 [J]. 通信学报, 2025, 46 (3): 1-16.
- [4]WANG X, LI Y, ZHANG H. Active Tor Website Fingerprinting Method Based on Deep Learning[J]. Journal of Cyber Security, 2024, 10(2): 45-58.
- [5]谢波, 张兆瑞。涉“暗网”违法犯罪治理工作体系探究 [J]. 公安学刊 (浙江警察学院学报), 2025 (1): 78-86.
- [6]Fortinet Inc. 2025 Global Threat Landscape Report[EB/OL]. (2024-11-21)[2025-12-31]. <https://www.fortinet.com/content/dam/fortinet-documents/reports/2025-global-threat-landscape-report.pdf>
- [7]INTERPOL. INTERPOL Global Financial Fraud Threat Assessment 2026[EB/OL]. (2025-03-05)[2025-12-31]. <https://www.interpol.int/content/download/225533/4607339/file/INTERPOL-2026-Global-Financial-Fraud-Threat-Assessment.pdf>
- [8]Trend Micro. Trend Micro Security Predictions for 2025[EB/OL]. (2024-12-03)[2025-12-31].<https://www.trendmicro.com/content/dam/trendmicro/global/en/research/25/security-predictions-for-2025/Trend-Micro-Security-Predictions-2025.pdf>
- [9]Verizon Communications Inc. 2025 Data Breach Investigations Report[EB/OL]. (2025-04-16)[2025-12-31]. <https://enterprise.verizon.com/resources/reports/2025-data-breach-investigations-report.pdf>
- [10]Google Cloud Mandiant. Mandiant 2025 Global Threat Report[EB/OL]. (2025-02-12)[2025-12-31]. <https://cloud.google.com/static/mandiant/resources/reports/2025-global-threat-report.pdf>
- [11]李本先, 李孟军。数据分析在网络恐怖主义治理中的应用、挑战与优化 [J]. 情报杂志, 2025, 44 (2): 32-39.
- [12]顾伟, 刘静。暗网治理思路 [J]. 中国信息安全, 2025 (3): 68-71.
- [13]Sophos Ltd. 2025 Threat Prediction Report[EB/OL]. (2024-12-10)[2025-12-31]. <https://www.sophos.com/content/dam/sophos-files/en-us/report/sophos-2025-threat-prediction-report.pdf>
- [14]Sophos Ltd. Global Threat Intelligence Index: 2025 Midyear Edition[EB/OL]. (2025-07-02)[2025-12-31]. <https://www.sophos.com/content/dam/sophos-files/en-us/report/global-threat-intelligence-index-midyear-2025.pdf>
- [15]Federal Bureau of Investigation. Internet Crime Report 2024[EB/OL]. (2025-03-18)[2025-12-31]. <https://www.ic3.gov/media/2025/03/18/2024-Internet-Crime-Report.pdf>

- [16]Flashpoint Intel LLC. Flashpoint Credential Intelligence Report 2025[EB/OL]. (2025-02-20)[2025-12-31].
<https://cdn.flashpoint.io/reports/2025/Flashpoint-2025-Credential-Intelligence-Report.pdf>
- [17]Proofpoint Inc. State of Phishing Report 2025[EB/OL]. (2025-01-22)[2025-12-31]. <https://www.proofpoint.com/sites/default/files/report-downloads/proofpoint-state-of-phishing-2025.pdf>
- [18]胡宇翔, 邬江兴, 兰巨龙. EADA:内生安全驱动的卫星互联网自适应防御架构 [J]. 通信学报, 2025,46 (01):1-14.
- [19]张宇辰.面向深暗网数据泄露监测的信息处理技术与系统实现 [D]. 北京:北京邮电大学, 2025. DOI: 10.26969/d.cnki.gbydu.2025.000216.
- [20]刘建伟, 石乐义.低轨卫星网络安全问题及防御技术综述 [J]. 计算机学报, 2025,48 (04):892-921.
- [21]European Union Agency for Cybersecurity (ENISA). Space Threat Landscape Report 2025 [EB/OL].
https://www.enisa.europa.eu/publications/space-threat-landscape-report-2025/at_download/file
- [22]Microsoft Security. 2026 Global AI Threat Report[R]. Redmond: Microsoft Corporation, 2026.
- [23]CrowdStrike Holdings Inc. 2025 Global Threat Report[R]. Austin: CrowdStrike Holdings, Inc., 2025.
- [24]Flashpoint Intelligence Inc. 2025 Darknet Threat Report [R]. New York: Flashpoint Intelligence Inc., 2025.
- [25]国家计算机网络应急技术处理协调中心. 2025 年中国互联网网络安全报告 [R]. 北京:人民邮电出版社, 2025.
- [26]IBM Security. 2025 Cost of a Data Breach Report [R]. Armonk: IBM Corporation, 2025.
- [27]国家互联网信息办公室. 2025 年网络空间治理白皮书 [R]. 北京:人民出版社, 2025.
- [28]工业和信息化部. 2025 年网络安全产业发展白皮书 [R]. 北京:电子工业出版社, 2025.
- [29]中国人民银行反洗钱局. 2025 年中国反洗钱报告 [R]. 北京:中国金融出版社, 2025.
- [30]中国法学会网络与信息法学研究会. 2025 年网络安全合规白皮书 [R]. 北京:中国法制出版社, 2025.
- [31]Microsoft Security. 2025 AI-Powered Cyber Threat Report [R]. Redmond: Microsoft Corporation, 2025.
- [32]中国信息通信研究院. 2025 年生成式 AI 安全风险白皮书 [R]. 北京:人民邮电出版社, 2025.
- [33]MITRE Corporation. 2025 ATT&CK® AI Attack Framework Update Report [R].
Bedford: MITRE Corporation, 2025.
- [34]奇安信科技集团股份有限公司. 2025年AI安全与攻防博弈白皮书 [R]. 北京:奇安信科技集团股份有限公司, 2025.
- [35]中国航天科技集团有限公司. 2025年商业航天网络安全白皮书 [R]. 北京:中国宇航出版社, 2025.
- [36]European Space Agency (ESA). 2025 Cybersecurity Incident Official Report [R]. Paris: European Space Agency, 2025.

- [37]国家计算机网络应急技术处理协调中心. 2025年我国卫星互联网网络安全态势报告 [R]. 北京:人民邮电出版社, 2025.
- [38]Identity Theft Resource Center (ITRC). 2025 Data Breach Report [R]. San Diego: Identity Theft Resource Center, 2025.
- [39]国家计算机网络应急技术处理协调中心. 2025年上半年中国互联网网络安全监测报告 [R]. 北京:人民邮电出版社, 2025.
- [40]中国人民银行反洗钱局. 2025年上半年金融行业反洗钱形势分析报告 [R]. 北京:中国金融出版社, 2025.
- [41]IBM Corporation. 2025 Healthcare Data Breach Special Report [R]. Armonk: IBM Corporation, 2025.
- [42]CrowdStrike Holdings, Inc. 2025 Global Ransomware Ecosystem Report [R]. Austin: CrowdStrike Holdings, Inc., 2025.
- [43]Google Project Zero. 2025 Vulnerability Research Annual Report [R]. Mountain View: Google LLC, 2025.
- [44]Unique Identification Authority of India (UIDAI). 2025 Aadhaar System Official Statistics Report [R]. New Delhi: UIDAI, 2025.
- [45]European Union Agency for Cybersecurity (ENISA). 2025 National Identity System Security Report [R]. Brussels: ENISA, 2025.
- [46]Open Web Application Security Project (OWASP). 2025 API Security Top 10 Report [R]. San Francisco: OWASP Foundation, 2025.
- [47]Rapid7 Inc. 2025 Vulnerability Intelligence Report [R]. Boston: Rapid7 Inc., 2025.
- [48]MITRE Corporation. 2025 Software Supply Chain Security Framework Report [R]. Bedford: MITRE Corporation, 2025.
- [49]Cybersecurity and Infrastructure Security Agency (CISA). 2025 Software Supply Chain Security Guidance [R]. Washington D.C.: CISA, 2025.
- [50]工业和信息化部. 2025年软件供应链安全白皮书 [R]. 北京:电子工业出版社, 2025.
- [51]Fortinet Inc. 2025 Global Data Security Report [R]. Sunnyvale: Fortinet Inc., 2025.
- [52]Fortinet Inc. 2025 Space Cybersecurity Threat Forecast Report [R]. Sunnyvale: Fortinet Inc., 2025.
- [53]中国信息通信研究院. 2026 Digital Economy Trust System Security White Paper [R]. 北京:人民邮电出版社, 2025.
- [54]National Institute of Standards and Technology (NIST). 2025 Post-Quantum Cryptography Security Threat Report [R]. Gaithersburg: NIST, 2025.
- [55]Cybersecurity and Infrastructure Security Agency (CISA). 2026 APT Threat Landscape Forecast Report [R]. Washington D.C.: CISA, 2025.
- [56]国家互联网信息办公室. 网络空间安全治理三年行动计划 (2024-2026) [Z]. 北京:国家互联网信息办公室, 2024.
- [57]工业和信息化部. 网络安全产业高质量发展行动计划 (2024-2026) [Z]. 北京:工业和信息化部, 2024.
- [58]Fortinet Inc. 2026 Global Threat Landscape Forecast Report [R]. Sunnyvale: Fortinet Inc., 2025.



远江盛邦安全科技集团股份有限公司

热线:4006 911 199

网址:www.webray.com.cn