全球数据泄露态势月度报告

（2026 年 3 月）

数世咨询
Digital World Consulting

全球数据泄露态势月度报告

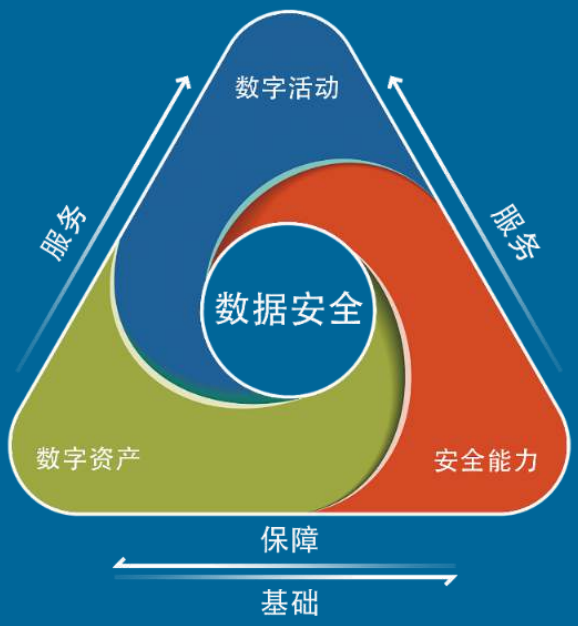
（2026 年 3 月）

数字安全是指，在全球数字化背景下，合理控制个人、组织、国家在各种活动中面临的数字风险，保障数字社会可持续发展*的政策法规、管理措施、技术方法等安全手段的总和。

这里的风险，不再局限于围绕数字化资产的攻防对抗，还包括了数字资产所承载业务的稳定性、连续性和健康性。这里的安全不再特指有意还是无意，天灾还是人祸，保安还是保险，而是更为广义的安全状态（SecSafe）。

*“世界环境与发展委员会出版的《我们共同的未来》报告中，将可持续发展定义为：“既能满足当代人的需要，又不对后代人满足其需要的能力构成危害的发展。”

——数世咨询，2023 年 11 月



以安全能力、数字资产和数字活动为三元素，以数据安全为核心目标，即三元一核的“数字安全三元论”。

“数字安全三元论”由“网络安全三元论”（数世咨询于 2020 年提出）更新迭代而来，旨在匹配数字中国建设的进程，保障数字基础设施稳定、可持续运行，保障数据有效流动、激发数据要素价值。

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构 . 网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

数世咨询&零零信安

数世智库 数字安全能力研究院

目　录

一、　数据泄露市场 3

1、　国家分类 3

2、　行业分类 4

3、　泄露数量 4

二、　事件抽样分析 5

1、　印度尼西亚雅加达首都特区地方代表理事会中官员财富报告数据库泄露 5

2、　南非统计局官方数据库泄露 5

3、　以色列摩萨德数据泄露 6

4、　美国联邦调查局 FBI 探员数据泄露 7

5、　墨西哥塔毛利帕斯州检察院供应商数据泄露 8

6、　中国*****平台用户数据库泄露 8

7、　中国*****地数据泄露 9

8、　中国多家*****公司内部数据泄露 10

9、　中国*****研究设施数据泄露 11

10、　中国浙江*****有限公司的数据泄露 11

三、　勒索软件和黑客组织 12

1、　活跃商业黑客组织综述 12

2、　黑客组织活度趋势 14

3、　本月典型事件说明 15

1) 欧盟委员会 16

2) 美国联邦调查局 16

3) 阿联酋联邦海关总署 17

4、　本月涉及中国企业的勒索事件说明 18

5、　典型黑客组织简介（Anubis） 19

四、　匿名社交社群 23

《全球数据泄露态势月度报告》

（2026 年 3 月）

本报告由数世咨询 & 零零信安 共同发布

在万物互联的数字化时代，数据做为第五大生产要素，要实现充分的流动才能创造出无限的价值。同时，数据安全风险也随之而来。数据的流动性意味着安全的巨大挑战，数据泄露事件成为常态。

为了掌握数据泄露态势，应对日益复杂的安全风险，数世咨询联合零零信安，基于 0.zone 安全开源情报系统，共同发布《全球数据泄露态势》月度报告。该系统监控范围包括明网、深网、暗网、匿名社群等约 10 万个威胁源。除了月度的数据泄露概况以外，报告还会针对一些典型的数据泄露事件进行抽样事件分析。如果发现影响较大的数据伪造事件，还会对其进行分析和辟谣。

本期报告的统计区间 2026 年 3 月。

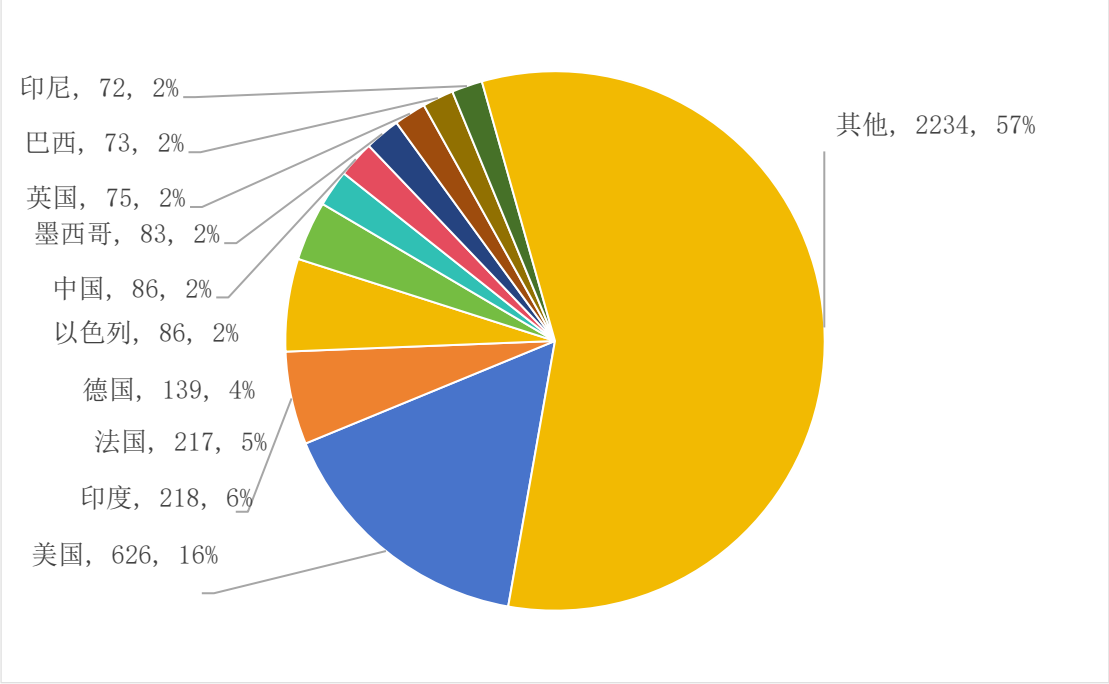
一、数据泄露市场

2026 年 3 月共监控到全球 DWM（Dark Web Market）情报：

- 深网和暗网有效情报 133,550 份；
- 泄露数据的高价值买卖情报 6,028 份。

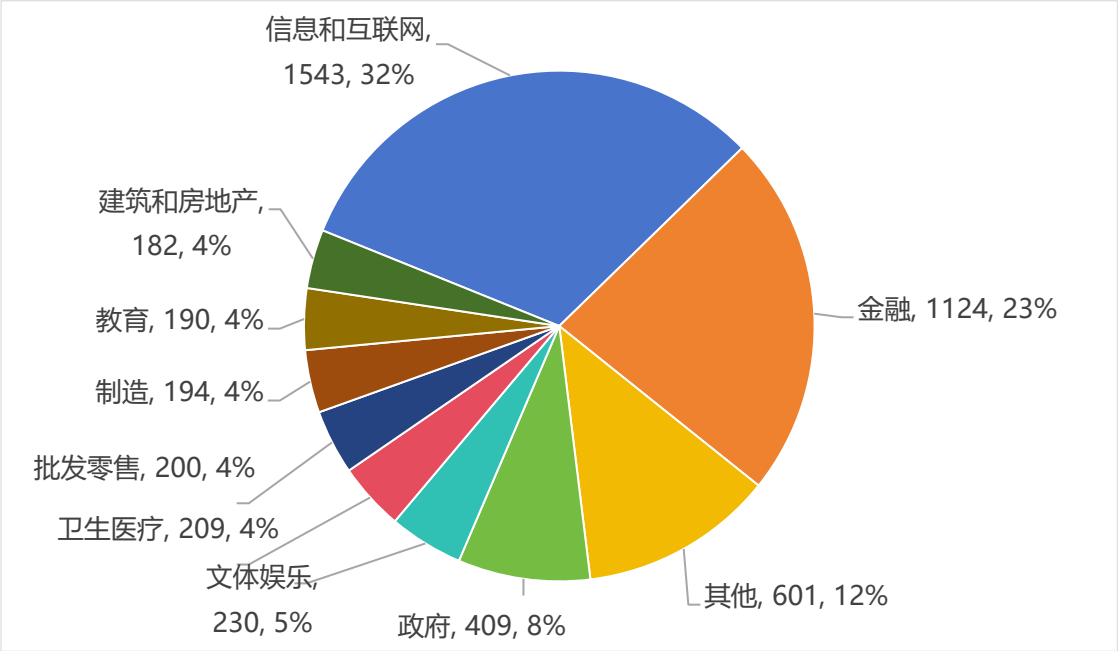
1、国家分类

其中美国是数据泄露第一大国，共泄露数据 626 份，其他数据泄露较多的国家还包括印度、法国、英国、德国、以色列等。详情如下图所示：



2、行业分类

3 月份行业属性数据占泄露数据总量约 88%左右，泄露的行业数据主要包括信息和互联网行业、金融行业、党政军和社会、文体娱乐行业、批发零售行业等。12%左右的泄露数据无明显行业属性，包括邮箱密码二要素数据、无明显泄露源的公民个人信息数据、批量的企业工商数据等。详情如下图所示：



3、泄露数量

3 月份泄露的数据中包含数份数十亿三要素日志数据、数十份数十亿二要素数据、十亿条个人邮箱电话数据泄露，除上述数据外，全球整体数据泄露量达到数百亿行以上。排除该类数据泄露，具有明确泄露源的非二要素新数据泄露量约在数十亿行以上。

二、事件抽样分析

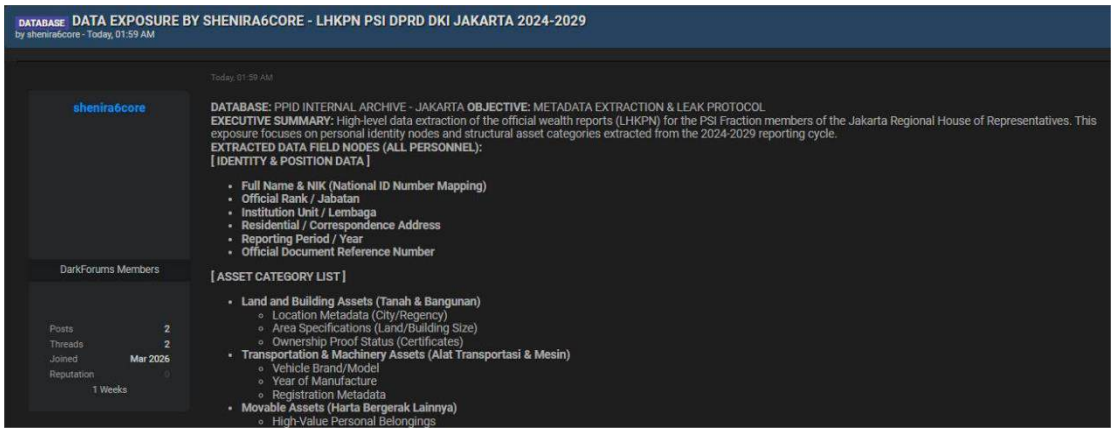
1、印度尼西亚雅加达首都特区地方代表理事会中官员财富报告数据库泄露

发布时间：2026.3.30

泄露数量：

售卖/发布人：shenira6core

事件描述：2026.3.30 某暗网数据交易平台有人公开泄露了一份印度尼西亚雅加达首都特区地方代表理事会数据。卖家称此份数据包括共 6 名中印尼团结党派系成员的官员财富报告，数据字段包括姓名、国民身份证号码、职位、住址，及其详细的资产类别，涵盖土地房产、交通工具、证券、现金、债务等敏感财务信息。



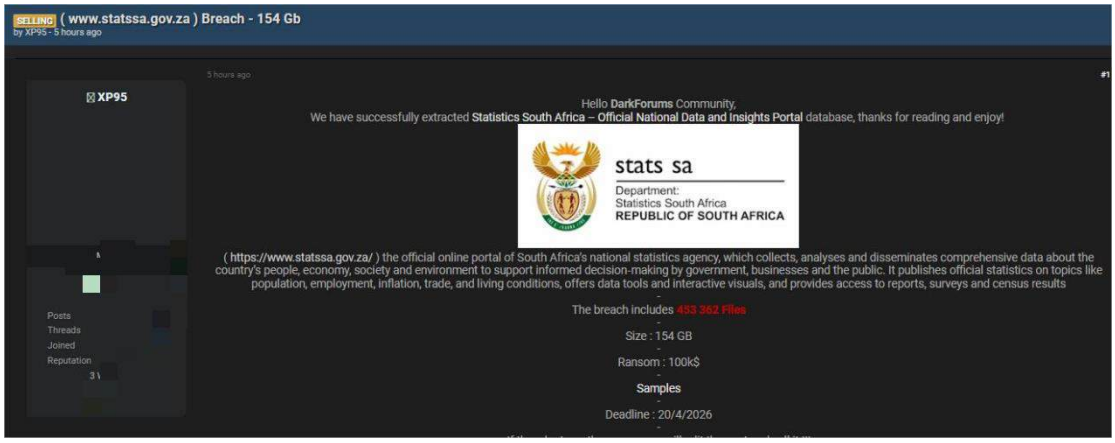
2、南非统计局官方数据库泄露

发布时间：2026.3.29

泄露数量：453,362

售卖/发布人：XP95

事件描述：2026.3.29 某暗网数据交易平台有人声称已成功窃取南非统计局（Statistics South Africa）的官方数据库，卖家称此份数据共 453,362 条，数据字段包括包含该国人口、经济、社会和环境信息等字段。



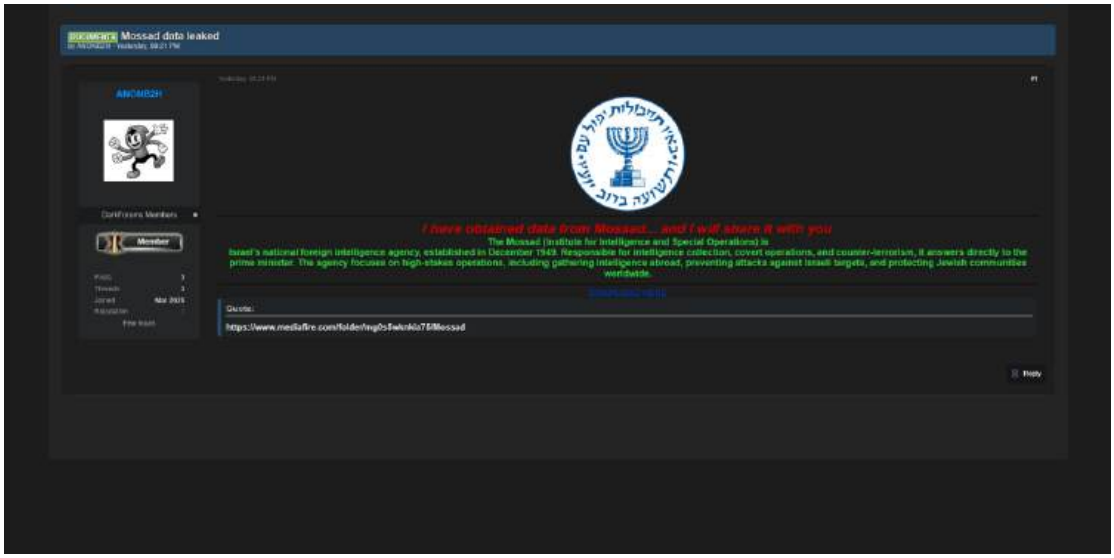
3、以色列摩萨德数据泄露

发布时间：2026.3.26

泄露数量：

售卖/发布人：ANONB2H

事件描述：2026.3.26 某暗网数据交易平台有人发布了一份以色列摩萨德数据。发帖人宣称已成功获取以色列情报和特殊使命局（摩萨德）的内部数据，并表示将该数据对外公开分享。



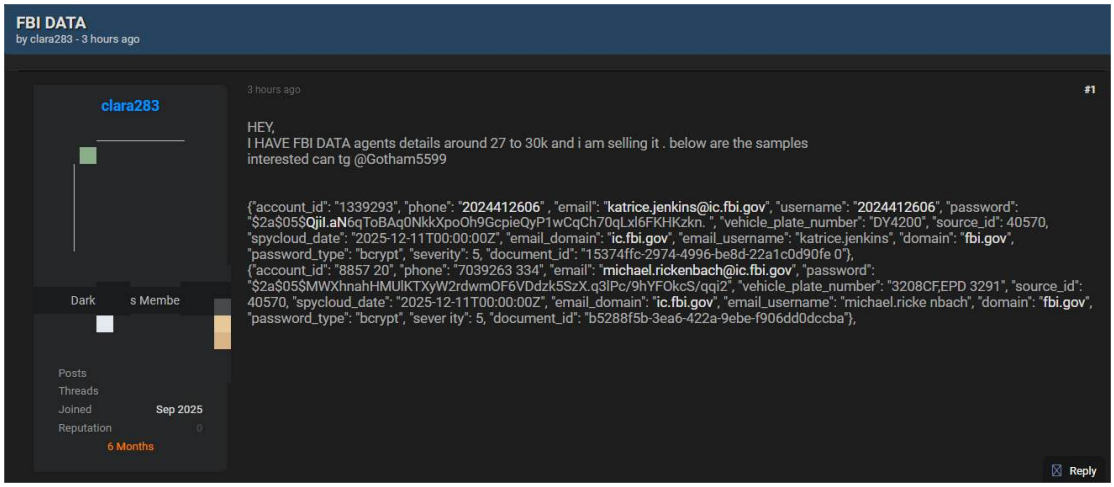
4、美国联邦调查局 FBI 探员数据泄露

发布时间：2026.3.26

泄露数量：27,000

售卖/发布人：clara283

事件描述：2026.3.26 某暗网数据交易平台有人声称正在出售据称来自美国联邦调查局的数据，卖家称此份数据包含约 27,000 至 30,000 名 FBI 探员的详细信息，泄露字段包含探员的账户 ID、电话号码、FBI 官方邮箱、用户名、加密密码、车牌号等字段。



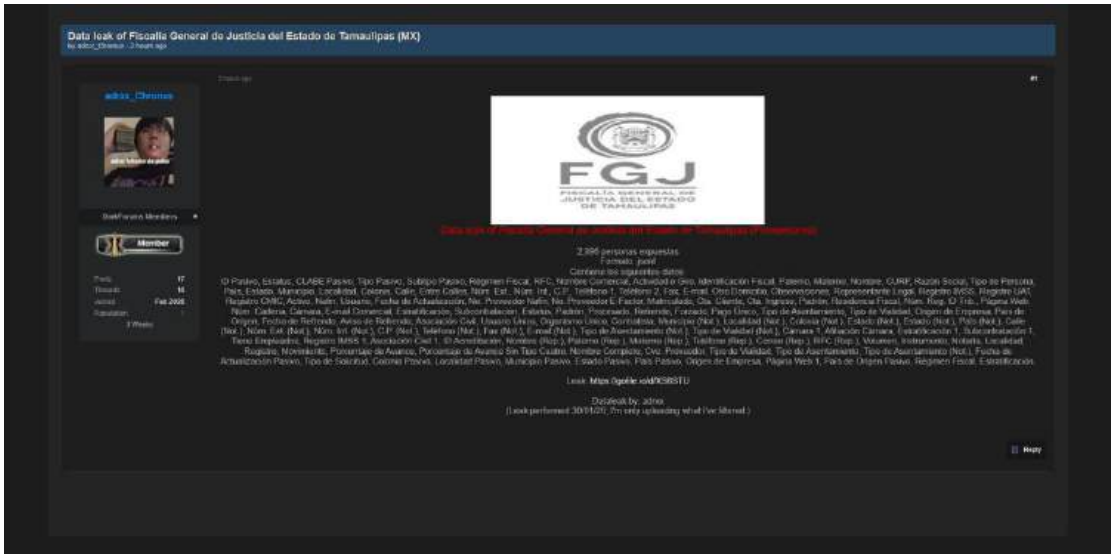
5、墨西哥塔毛利帕斯州检察院供应商数据泄露

发布时间：2026.3.29

泄露数量：4,000

售卖/发布人：adrxx_Chronus

事件描述：2026.3.29 某暗网数据交易平台有人发布了一份墨西哥塔毛利帕斯州总检察长办公室（FGJ）供应商数据。卖家称此份数据格式为 json，共包含 2896 条人员暴露数据，数据字段涵盖 ID Pasivo、税务登记号 RFC、企业 / 个人姓名、CURP 身份码、完整地址信息、多渠道联系方式、法律代表信息、供应商编号、税务状态、工商注册信息、资质认证信息等上百项内容。



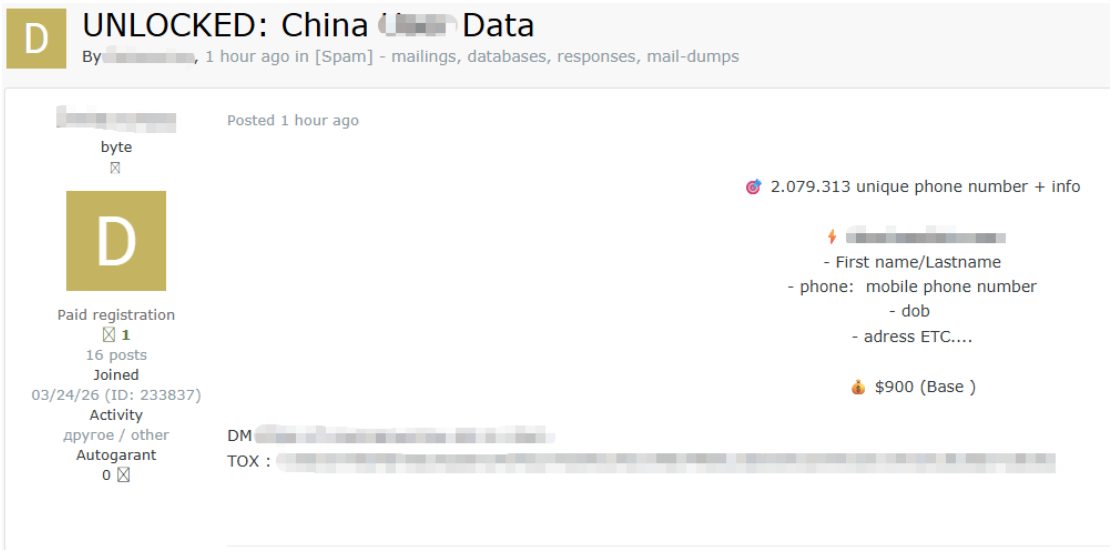
6、中国*****平台用户数据库泄露

发布时间：2026.3.31

泄露数量：2,079,313

售卖/发布人：Datavortex

事件描述：2026.3.31 某暗网数据交易平台有人声称出售一份中国用户数据。卖家称此份数据包含超过 2,070,000 条数据，来源于*****平台，泄露字段包含姓名、电话号码、出生日期、地址等字段。



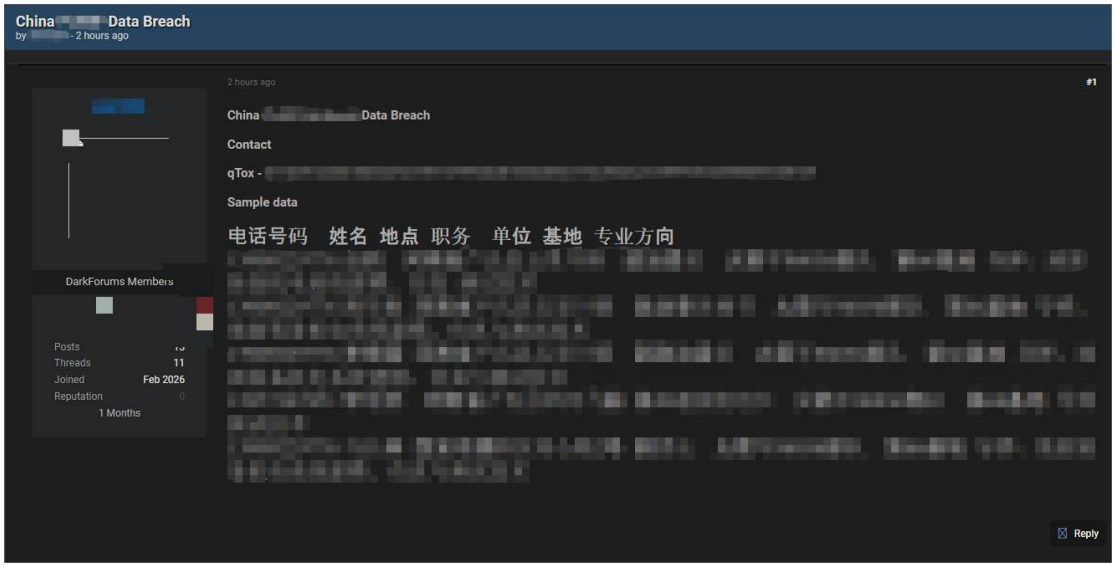
7、中国*****地数据泄露

发布时间：2026.3.30

泄露数量：

售卖/发布人：Jon1234

事件描述：2026.3.30 某暗网数据交易平台有人发布声称泄露一份中国*****地的数据。卖家称此份数据包括了多名军人的个人信息，泄露字段包括姓名、电话号码、地点、职务、所属单位、基地以及专业方向等。



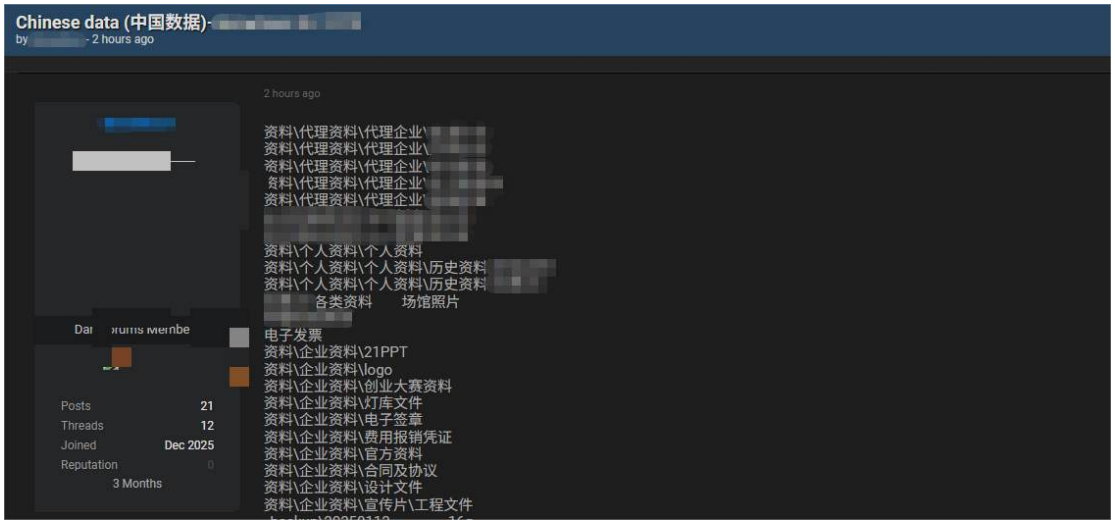
8、中国多家*****公司内部数据泄露

发布时间：2026.3.28

泄露数量：

售卖/发布人：SnowSoul

事件描述：2026.3.28 某暗网数据交易平台有人宣称泄露了多家中国*****公司的内部数据。卖家称此份数据包括了长*****有限公司，泄露的数据类型包括：企业资料、代理资料、个人资料、历史资料、财务数据、电子发票、场馆照片以及人事管理内容等字段。



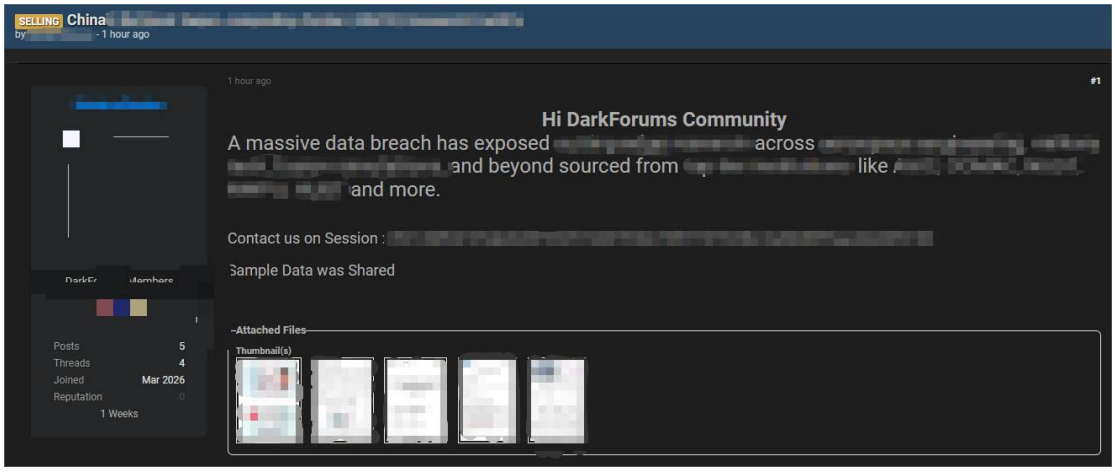
9、中国*****研究设施数据泄露

发布时间：2026.3.24

泄露数量：

售卖/发布人：ModernStealer

事件描述：2026.3.24 某暗网数据交易平台有人声称出售来自中国*****研究设施的数据。卖家称此份数据来源包括中国*****、中国*****、*****大学、*****大学、*****大学等顶级机构，泄露内容为尖端研究数据。



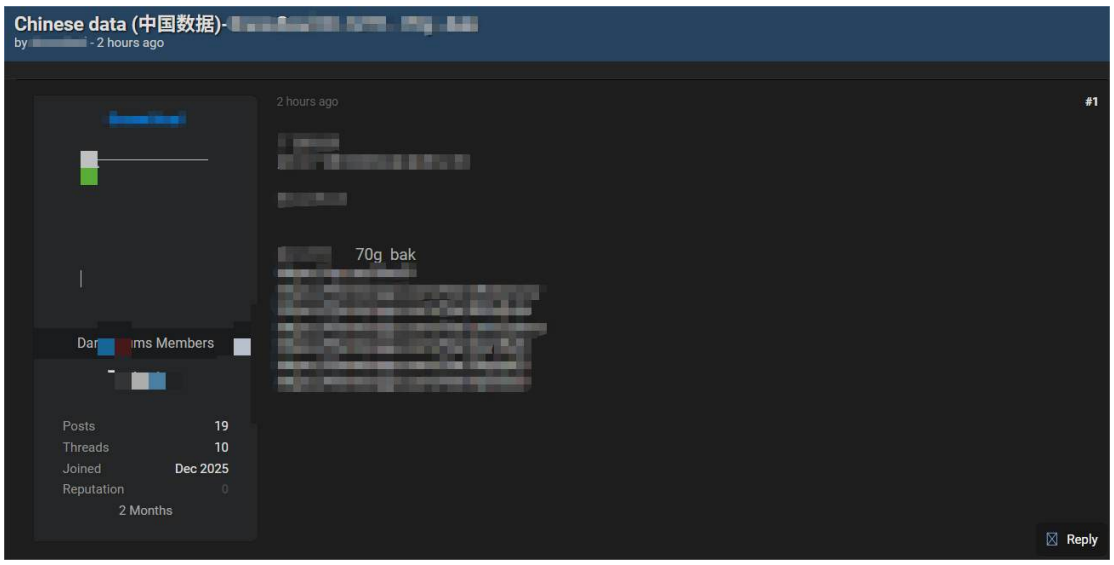
10、中国浙江*****有限公司的数据泄露

发布时间：2026.3.23

泄露数量：

售卖/发布人：SnowSoul

事件描述：2026.3.23 某暗网数据交易平台有人发布了一份据称属于浙江*****有限公司的数据。卖家称此份数据文件大小为 70GB，并提供了多个下载链接，具体数据类型可能包含该公司的内部数据或系统备份。



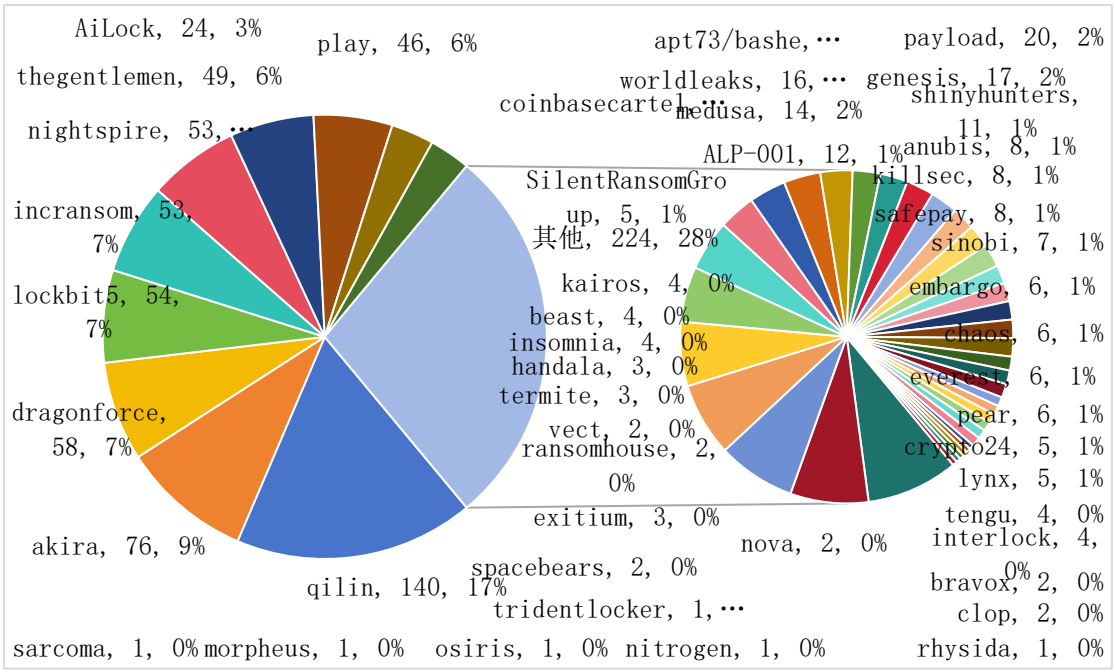
三、勒索软件和黑客组织

1、活跃商业黑客组织综述

2026 年 3 月全球活跃的商业黑客组织（有勒索发布行为）共 53 个，公开的勒索事件共 802 件，TOP 10 的黑客组织如下所示：


数世咨询 Digital World Consulting X OOSEC
活跃商业黑客组织
TOP10
排名 组织标识 组织名称 发布数量
1 qilin 140
2 Akira 76
3 DragonForce dragonforce 58
4 lockbit5 54
5 INC RANSOM Inc ransom 53
6 NightSpire nightspire 53
7 The gentlemen 49
8 PLAY play 46
9 COINBASECARTEL Coinbase Cartel 25
10 AiLock AiLock 24
—来自2026年3月《全球数据泄露态势月度报告》

TOP 10 的商业黑客组织公开发布的勒索事件占全部事件的 70%，如下所示：

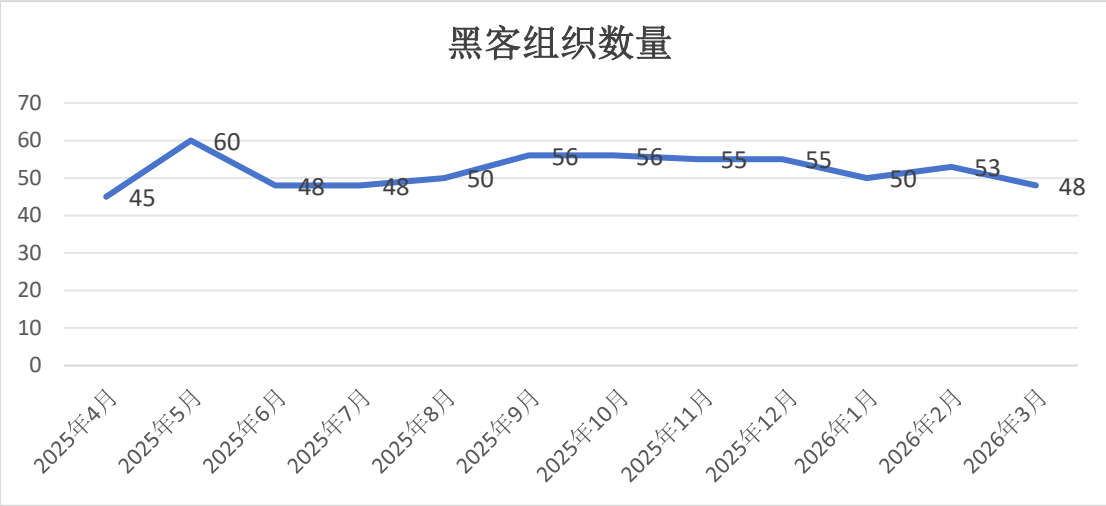


2、黑客组织活度趋势

下图为近一年来黑客组织活跃度趋势图，从下图可看出，虽然每个月全球商业黑客组织的活动波动性较强（本月与上月相比有所减少），整体活跃度趋势正在逐步趋于稳定，统计末端（2026 年 3 月）达到一年前统计前端（2025 年 4 月）的 106.5%：

随着 TI+AI（开源情报+人工智能自动化）的攻击方式逐步成熟，尤其是 2023

年以来，WormGPT 和 FraudGPT 的发布和发展，黑客组织正在向精英化、小型化、自动化演进，这也促使更多的黑客组织逐渐分裂、诞生和成长，本月活跃的黑客组织的数量如下图所示：



3、本月典型事件说明

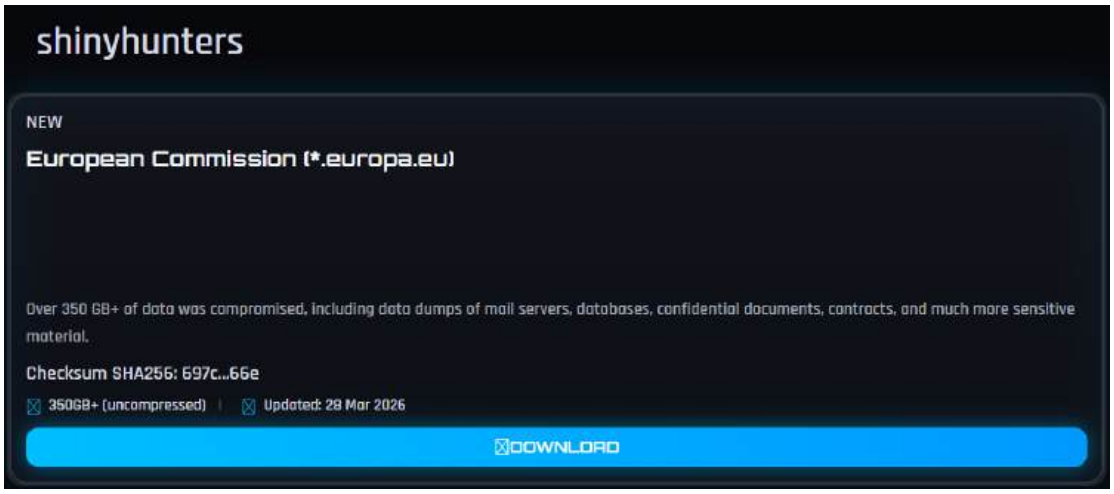
由于每月黑客组织行动数量庞大，无法在报告中枚举全部事件，分析员随机抽取展示 10 个典型样例事件，并对其中部分代表性事件进行细节说明：

事件	国家/组织	时间	黑客组织
European Commission	欧盟委员会	2026/3/28	ShinyHunters
Kash Patel current director of the FBI Hacked	美国联邦调查局	2026/3/27	Handala Hack
UAE Customs (Federal Customs Authority)	阿联酋联邦海关总署	2026/3/26	NASIR SECUTRIY
Mossad’s Former Chief Falls into the Trap	以色列情报机构摩萨德	2026/3/25	Handala Hack
City of Los Angeles	美国洛杉矶市政府	2026/3/23	worldleaks
Nandrin Municipality	比利时南德兰市	2026/3/20	LOCK BIT5.0

rovinj-rovigno.hr	克罗地亚罗维尼-罗维尼奥市	2026/3/16	LOCK BIT
meridenct.gov	美国康涅狄格州梅里登市	2026/3/12	INC Ransom
Jerusalem’s Security Cameras	以色列耶路撒冷市	2026/3/9	Handala Hack
City of Hart	美国哈特市地方市政组织	2026/3/7	GENESIS

1) 欧盟委员会

商业黑客组织 ShinyHunters 在 2026/3/28 公布了欧盟委员会（European Commission ）被勒索的信息。欧盟委员会是欧洲联盟的常设执行机构，负责提出立法建议、执行欧盟政策与预算、管理欧盟日常事务及监督条约实施等核心治理工作，承担欧盟行政决策、政策推行与法律维护等关键职能。截止本篇报告发出之时，黑客组织 ShinyHunters 尚未发布更多关于欧盟委员会的数据。



2) 美国联邦调查局

商业黑客组织 Handala Hack 在 2026/3/27 公布了美国联邦调查局（FBI）

被勒索的信息。美国联邦调查局是美国司法部下属的主要联邦执法与情报机构，负责调查违反联邦法律的犯罪行为、保护美国免受恐怖主义及外国情报威胁、维护国家安全及刑事司法公正，承担联邦执法、反恐情报、网络安全及重大刑事犯罪调查等核心职能。截止本篇报告发出之时，黑客组织 Handala Hack 尚未发布更多关于美国联邦调查局的数据。

3) 阿联酋联邦海关总署

商业黑客组织 NASIR SECUTRIY 在 2026/3/26 公布了阿联酋联邦海关总署被勒索的信息。阿联酋联邦海关总署是阿拉伯联合酋长国负责海关管理、边境管控及国际贸易监管的联邦机构，负责制定和执行海关政策、征收关税、打击走私

及保障边境安全，承担国家海关执法、贸易便利化及边境保护等核心职能。截止本篇报告发出之时，黑客组织 NASIR SECUTRIY 尚未发布更多关于阿联酋联邦海关总署的数据。

4、本月涉及中国企业的勒索事件说明

在当今数字化时代，网络安全问题日益突出，勒索软件袭击已成为全球范围内的一大威胁，中国也不例外。近年来，我国频繁发生的勒索软件事件已经引起了广泛关注，但我们仍需进一步重视起来，以防范这一威胁。勒索组织的攻击手段日益多样化，其针对性强、隐蔽性高，一旦遭受攻击，可能会导致巨大的经济损失和社会影响。尤其是对于我国重要基础设施、金融系统、企业以及个人用户，都存在着潜在的安全隐患。

以下为本月涉及中国企业的勒索事件说明：

组织	所属行业	时间	黑客组织
厦*****股份有限公司	矿业	2026/3/31	BEAST

特*****集团	批发零售业	2026/3/30	The Gentlemen
汉*****集团	金融业	2026/3/30	The Gentlemen
海*****集团	信息和互联网科技	2026/3/22	ALP-001
杰*****股份有限公司	建筑和房地产业	2026/3/17	LOCK BIT5.0
诺*****股份有限公司	生物技术业	2026/3/15	coinbasecartel
深*****股份有限公司	制造业	2026/3/6	AiLock
湖*****有限公司	制造业	2026/3/3	BEAST
纽*****有限公司	服务业	2026/3/3	Gunra
幺*****股份有限公司	制造业	2026/3/1	lockbit5

5、典型黑客组织简介（Beast）

由于国内安全行业尚处于从以合规为目标向实战化攻防的转型初期，我们计划在每期报告中对一个典型的商业黑客组织进行科普性介绍，以普遍增加从业人员对勒索软件和黑客组织的认知度。

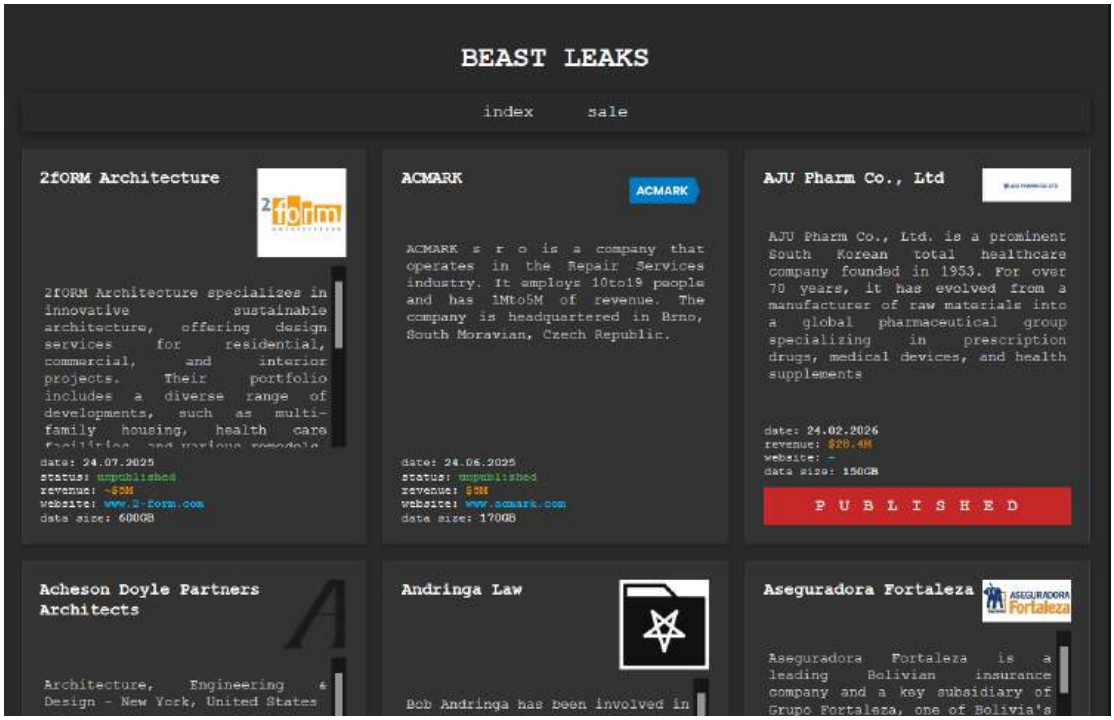
已经介绍过的黑客组织有：Lockbit3，Royal，Play，Rhysida，Alphv，8base，Hunters International、BianLian、Akira、Cactus、Abyss-Data、Black Suit、Arcus Media、space bear、killsec、fog、Funksec、Babuk-Bjorka、Hellcat、Babuk2、NightSpire、Dragonforce、Handala、D4RK4RMY、Warlock、World Leaks、sinobi 、Interlock、Qilin、Anubis、The Gentlemen 如需了解请翻阅往期报告。

本期为您介绍的是 Beast 勒索软件黑客组织，Beast 是一个于 2022 年出现的勒索软件，作为早期“Monster”勒索软件的增强迭代版本。它采用

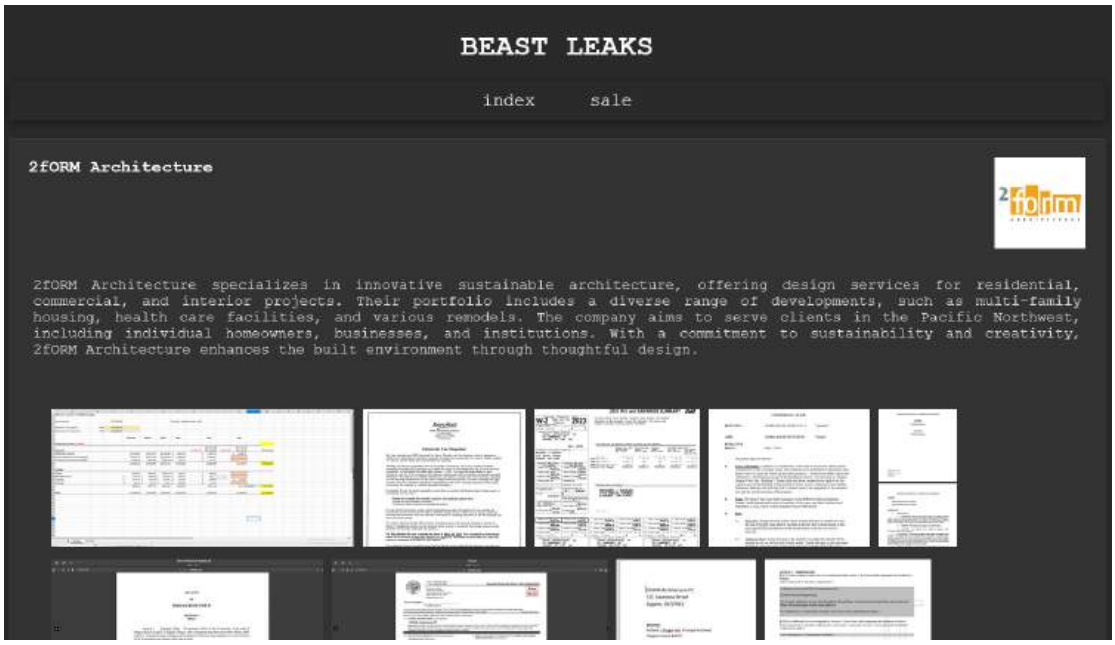
Ransomware-as-a-Service（RaaS）模式运营，为附属程序提供丰富的自定义选项，以创建针对 Windows、Linux 和 VMware ESXi 系统的定制二进制文件。其关键技术能力包括混合椭圆曲线 +ChaCha20 加密、分段文件加密、ZIP 包装模式（将文件加密为带有嵌入勒索信的 zip 档案）、多线程处理、服务终止、影子副本删除、隐藏分区使用以及子网扫描。附属程序被提供可配置的离线构建器，实现跨多个平台的简化部署。

截至 2026 年 3 月初，Beast 已声称多个受害者，主要针对全球多个国家/地区（亚太、北美、欧洲、南美等，包括中国、韩国、美国、英国、加拿大、巴西、澳大利亚等），重点行业包括制造业、建筑、医疗保健、教育、法律服务、制药及消费服务等，常造成数据永久加密的风险、运营全面中断（包括 ERP、邮箱、网站瘫痪）、备份破坏和监管合规问题。典型案例包括对中国*****股份有限公司、韩国 Sungwoo Co., Ltd、英国 Communicate UK 等攻击，常伴随数 TB 数据外泄威胁和针对关键行业的适应性提升。

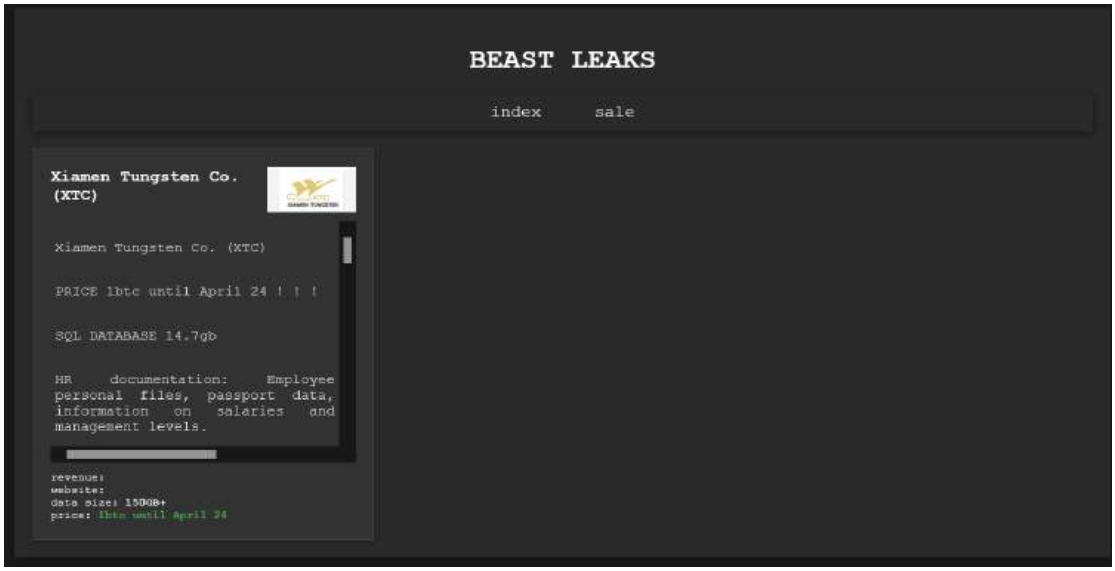
下图为 Beast 所运营的数据泄露网站：



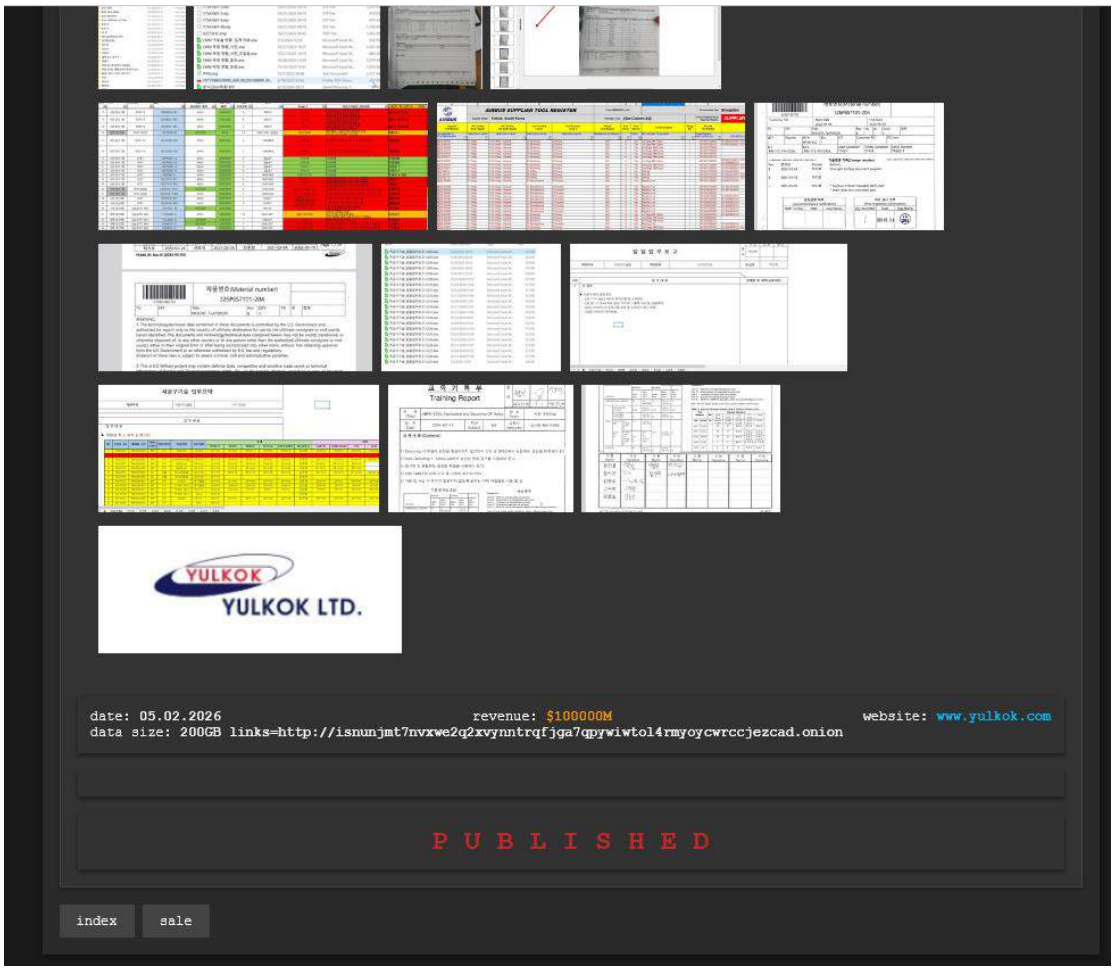
下图为 Beast 运营的数据泄露网站事件详情：



下图为 Beast 运营网站上的 sale 模块：

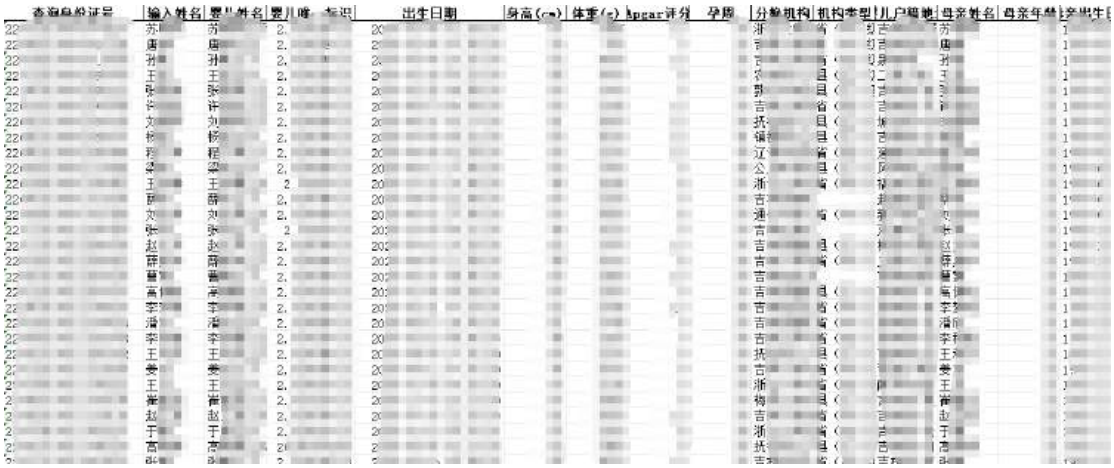


如勒索不成，会把他们获取到的全部受害者数据上传到他们运营的数据泄露网站上：

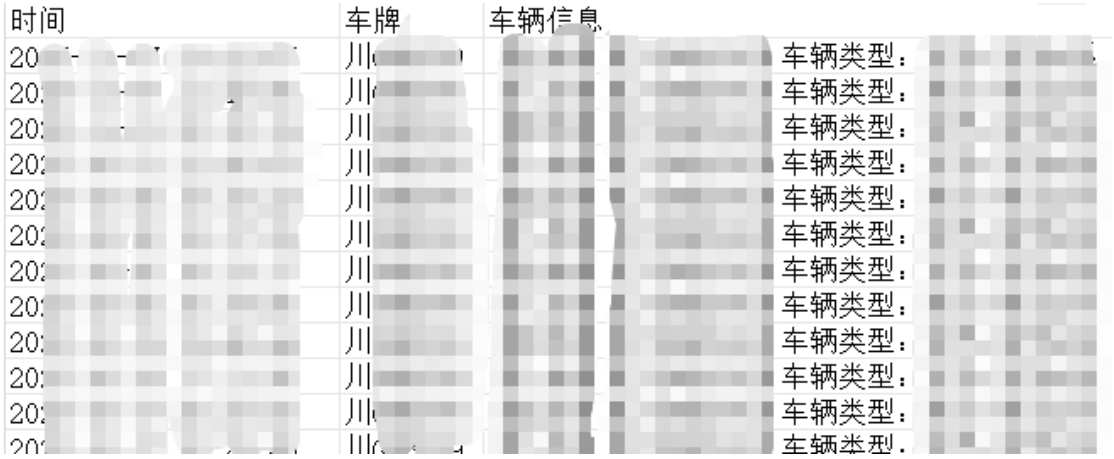


四、匿名社交社群

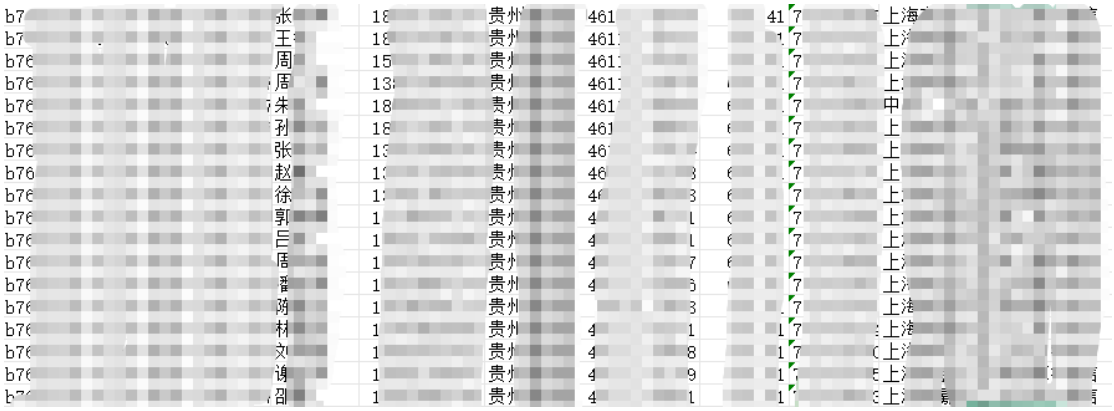
3 月份监控到匿名社交社群情报总数量 14,142,874 条，提供的有效数据泄露样例下载 4,315 份。涉及到我国数据泄露的内容包括：快递信息、银行信息、学生信息、就医信息、打车信息、退休人员信息、医护信息、车主信息、网贷信息、投资信息等众多类型。以下随机选取展示部分样本：



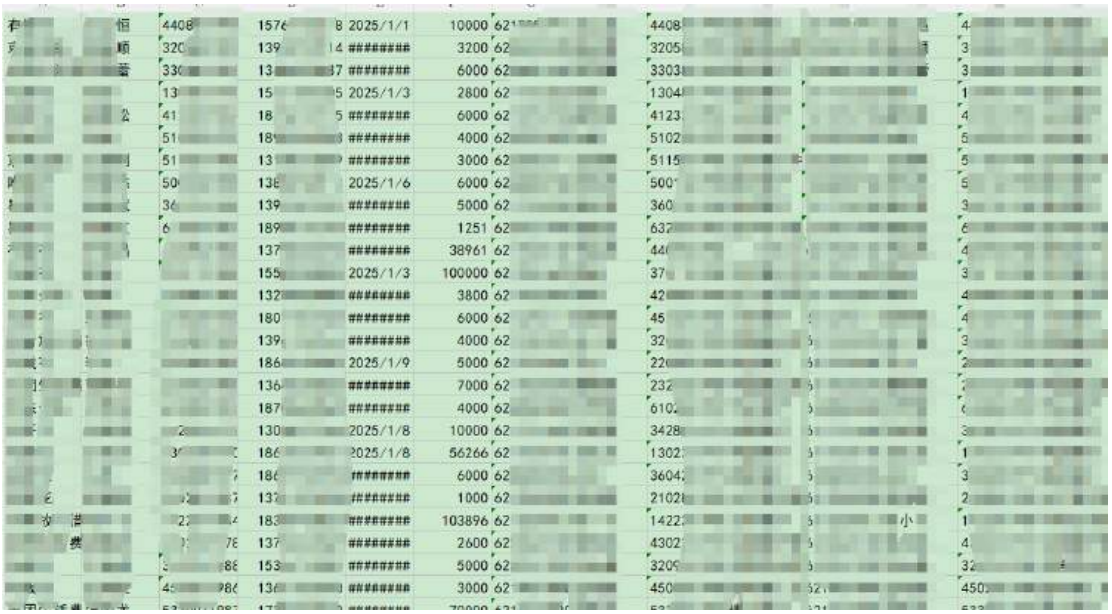
查询身份证号	输入姓名	婴儿姓名	婴儿性别	出生日期	身高(cm)	体重(g)	Apgar评分	孕周	分娩机构	机构类型	户籍地	母亲姓名	母亲年龄	产次
22	苏	苏	2.	20					浙	省	丽吉	苏		1
22	唐	唐	2.	2					吉	省	丽吉	唐		1
22	孙	孙	2.	2					吉	省	丽吉	孙		1
22	王	王	2.	2					黔	县	吉	王		1
22	张	张	2.	2					吉	省	吉	张		1
22	许	许	2.	2					抚	省	吉	许		1
22	刘	刘	2.	2					镇	县	吉	刘		1
22	杨	杨	2.	2					辽	省	吉	杨		1
22	程	程	2.	2					公	县	吉	程		1
22	梁	梁	2.	2					浙	省	吉	梁		1
22	王	王	2	2					吉	省	吉	王		1
22	薛	薛	2.	2					通	省	吉	薛		1
22	刘	刘	2.	2					吉	省	吉	刘		1
22	张	张	2	2					吉	县	吉	张		1
22	赵	赵	2.	2					吉	省	吉	赵		1
22	薛	薛	2.	2					吉	省	吉	薛		1
22	曹	曹	2.	2					吉	县	吉	曹		1
22	高	高	2.	2					吉	省	吉	高		1
22	李	李	2.	2					吉	省	吉	李		1
22	潘	潘	2.	2					吉	省	吉	潘		1
22	李	李	2.	2					吉	省	吉	李		1
22	王	王	2.	2					抚	县	吉	王		1
22	姜	姜	2.	2					吉	省	吉	姜		1
22	王	王	2.	2					浙	省	丽	王		1
22	曹	曹	2.	2					梅	县	吉	曹		1
22	赵	赵	2.	2					吉	省	吉	赵		1
22	于	于	2.	2					浙	省	吉	于		1
22	高	高	2.	2					抚	县	吉	高		1



时间	车牌	车辆信息
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：
20	川	车辆类型：

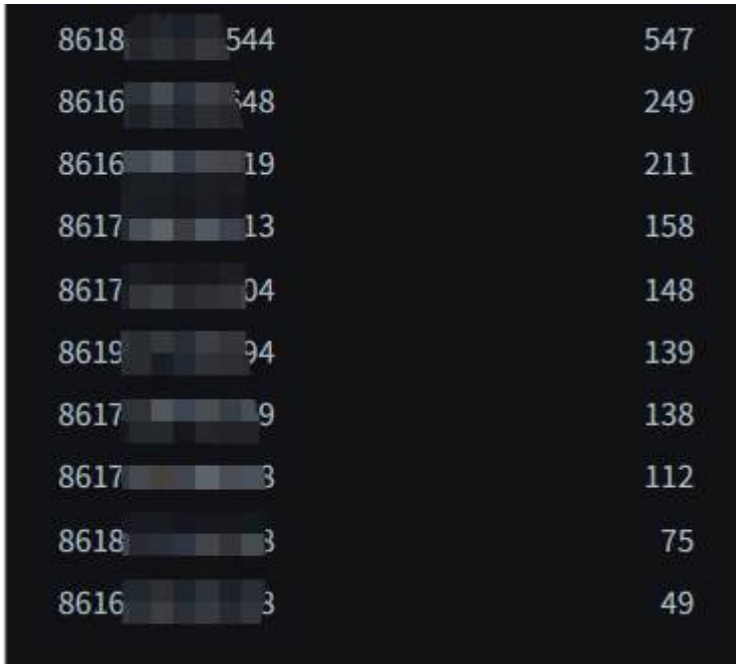


b7	张	18	贵州	461	41	7	上海	
b7	王	18	贵州	461	1	7	上	
b76	周	15	贵州	461		7	上	
b76	周	13	贵州	461		7	上	
b76	朱	18	贵州	461	6	7	中	
b76	孙	18	贵州	461	6	7	上	
b76	张	13	贵州	46	6	7	上	
b76	赵	13	贵州	46	8	7	上	
b76	徐	13	贵州	4	3	7	上	
b76	郭	1	贵州	4	1	7	上	
b76	吕	1	贵州	4	1	7	上	
b76	周	1	贵州	4	7	7	上	
b76	曹	1	贵州	4	6	7	上	
b76	邓	1	贵州		3	7	上	
b76	林	1	贵州	4	1	1 7	上	
b76	刘	1	贵州	4	8	1 7	上	
b76	谭	1	贵州	4	9	1	上	
b7	邵	1	贵州	4	1	1	上	



据仅为在匿名社交社群中，攻击者展示的样例数据，每份样例会提供数十至数百条不等。即：匿名社交社群中仅每个月发布的我国数据泄露的样例数据就有 10 万条左右，全数据量估算在 1000 万条以上。

此外，检索到 3 月份使用匿名社交软件的活跃用户中，以“86（我国区号）”开头的手机号共发信息 4,789 条。使用匿名社交软件的用户，不会受到实名监管，其目的性值得考虑。以下为 3 月份使用“86”开头的手机号的 TOP 10 信息：



注：本篇内容中的数据均为暗网交易平台卖家宣称内容，数据真实性、实际泄露范围未经过权威核实，仅作为网络安全风险态势分析参考，不构成事实认定依据。

* 如果您对《全球数据泄露态势月度报告》有任何问题或意见，包括引用、指正或合作，请通过电子邮件 dw@dwcon.cn 与我们联系。

北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆

数世咨询
Digital World Consulting
数字安全领域独立第三方调研机构