全球数据泄露态势月度报告

（2026 年 8 月）

数世咨询
Digital World Consulting

全球数据泄露态势月度报告

（2026 年 8 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。

报告名称：全球数据泄露态势月度报告 8 月

发布时间：2026 年 9 月 22 日

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

报告审核：数世咨询联合创始人&主编 闫志坤

目 录

《全球数据泄露态势月度报告》

(2026 年 8 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。

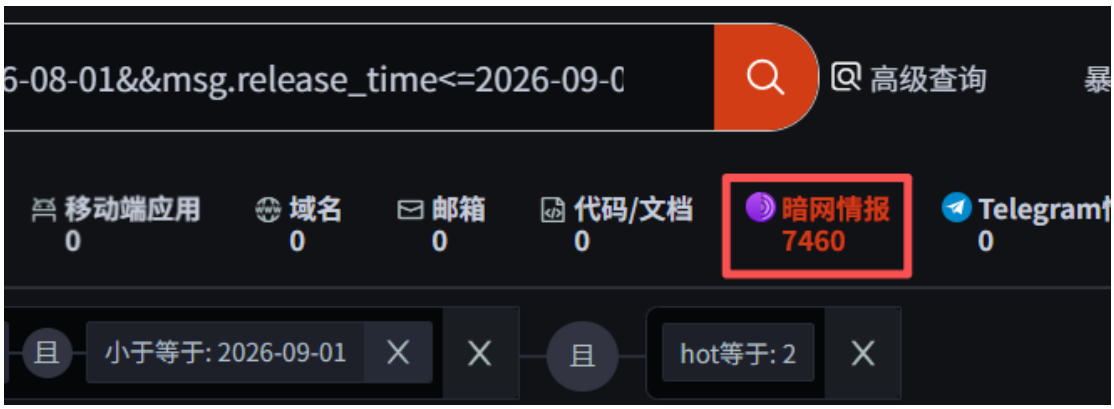
为了掌握数据泄露态势，应对日益复杂的安全风险，数世咨询联合零零信安，基于 0.zone 安全开源情报系统，共同发布《全球数据泄露态势》月度报告。该系统监控范围包括明网、深网、暗网、匿名社群等约 10 万个威胁源。除了月度的数据泄露概况以外，报告还会针对一些典型的数据泄露事件进行抽样事件分析。如果发现影响较大的数据伪造事件，还会对其进行分析和辟谣。

本期报告的统计区间 2026 年 8 月。

一、数据泄露市场

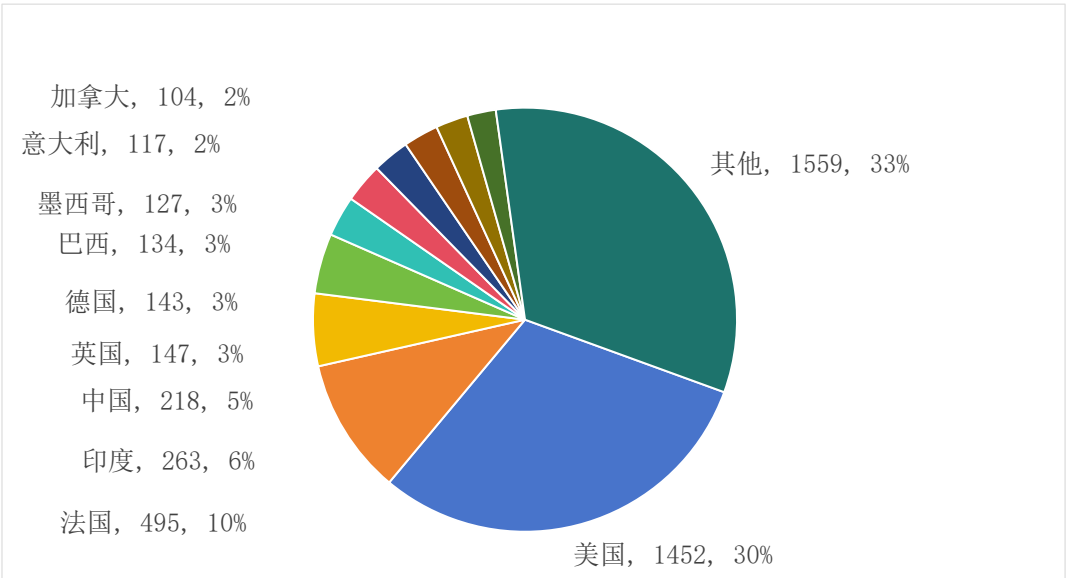
2026 年 8 月共监控到全球 DWM（Dark Web Market）情报：

- 深网和暗网有效情报 127,362 份；
- 泄露数据的高价值买卖情报 7,460 份。



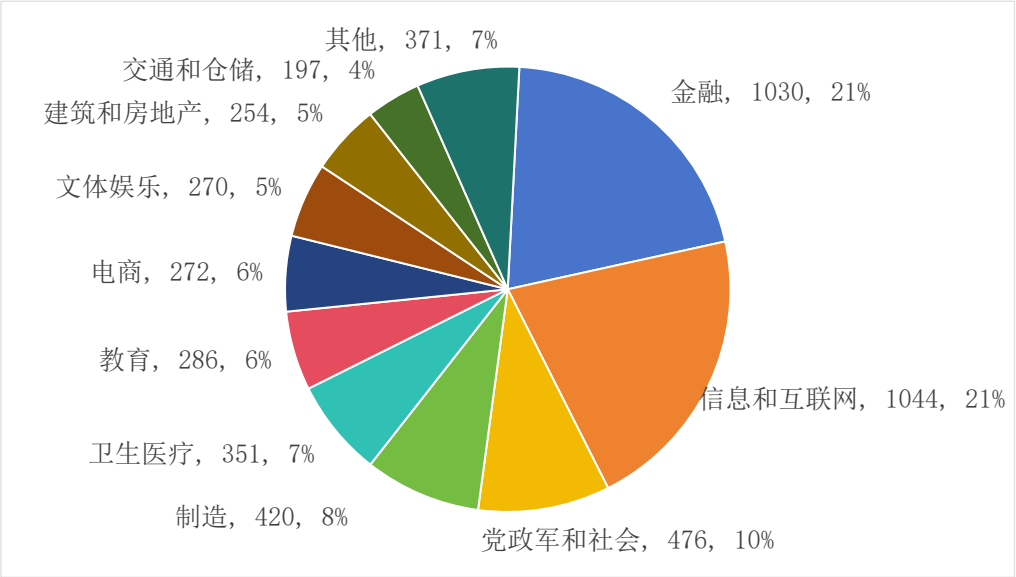
1、国家分类

其中美国是数据泄露第一大国，共泄露数据 1,452 份，其他数据泄露较多的国家还包括法国、印度、中国、英国等。详情如下图所示：



2、行业分类

8 月份行业属性数据占泄露数据总量约 93%左右，泄露的行业数据主要包括金融行业、信息和互联网行业、党政军和社会行业、制造行业、电商行业等。6%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

8 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

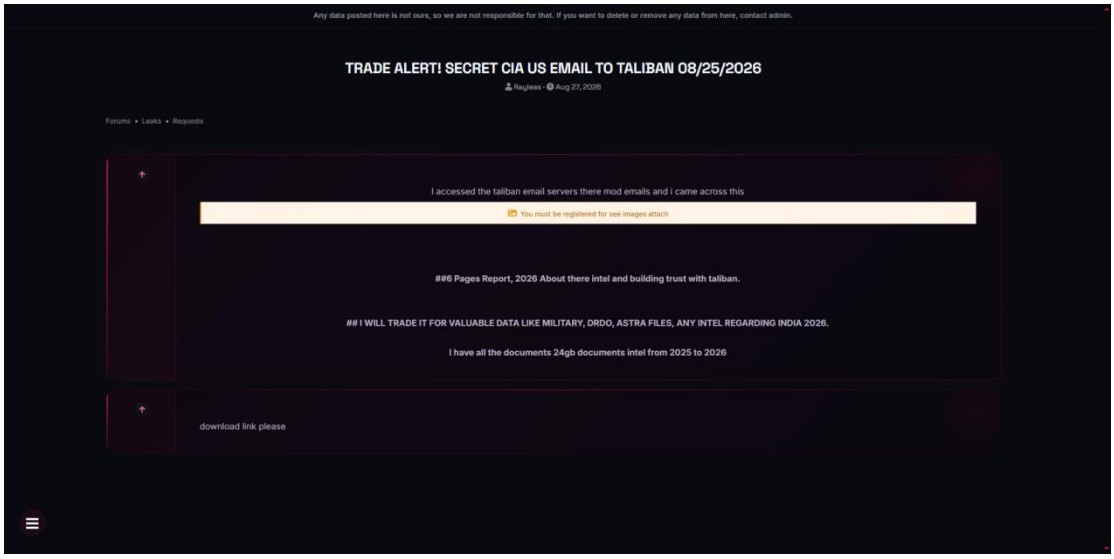
1、美国中央情报局（CIA）发给塔*班的邮件数据泄露

发布时间：2026.8.27

泄露数量：

售卖/发布人：Rayleas

事件描述：某暗网数据交易平台有人宣称正在售卖一份美国中央情报局（CIA）发给塔利*班的机密邮件及相关情报文件。卖家称此份数据共 24GB 文档（含 6 页 2026 年报告及 2025–2026 年情报资料），数据字段包含邮件内容、情报报告及相关文档等，此份数据的价格未知。



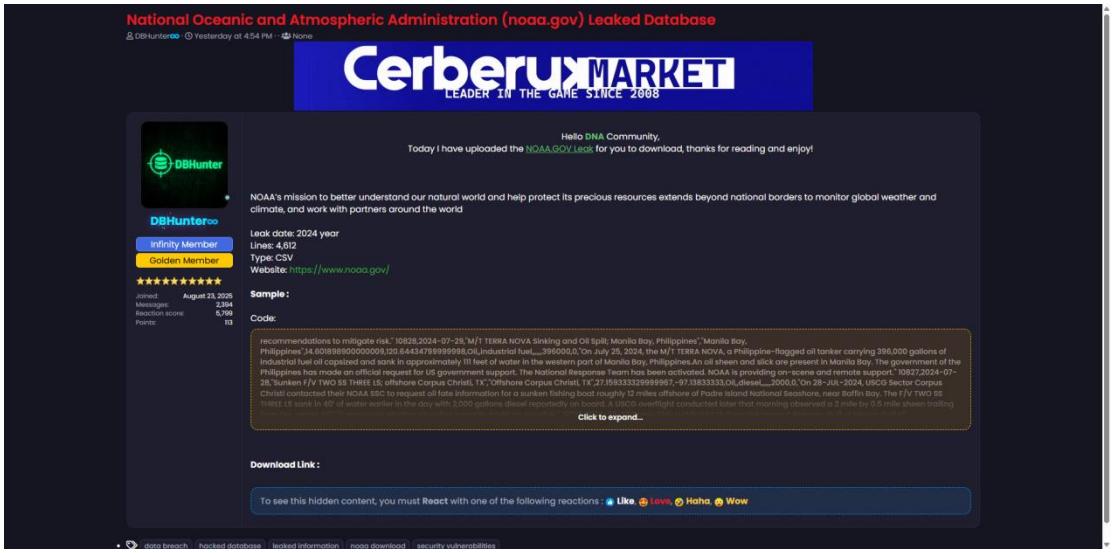
2、美国国家海洋和大气管理局数据泄露

发布时间：2026.8.24

泄露数量：4,612

售卖/发布人：DBHunter

事件描述：2026.8.24 某暗网数据交易平台有人宣称正在售卖一份美国国家海洋和大气管理局（NOAA / noaa.gov）泄露数据库。卖家称此份数据共 4,612 条记录（CSV），数据字段包含 incident reports、location、date、oil type、quantity 等，此份数据的价格未知。



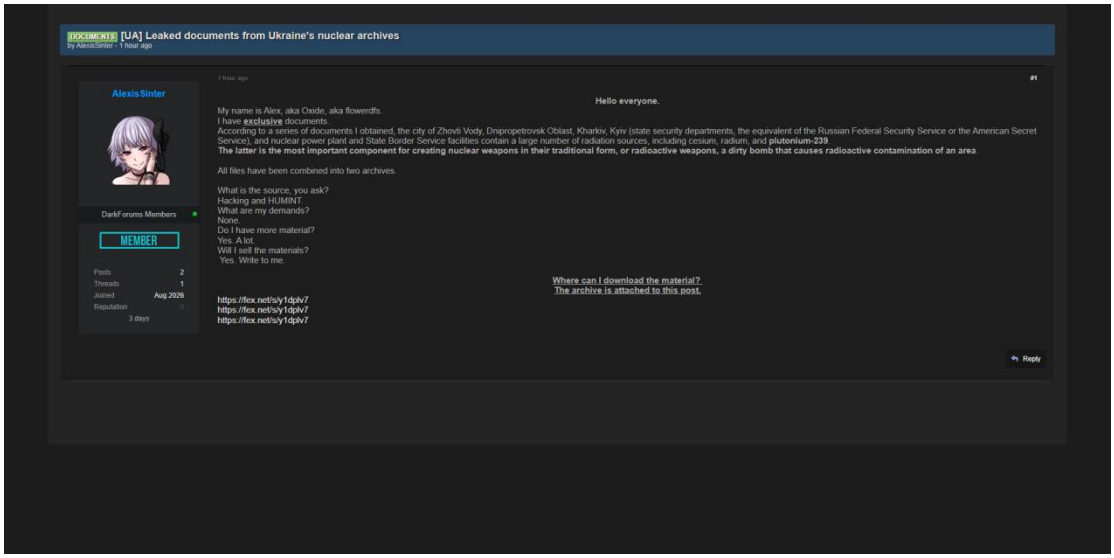
3、乌克兰核相关档案泄露文件

发布时间：2026.8.30

泄露数量：

售卖/发布人：AlexisSinter

事件描述：2026.8.30 某暗网数据交易平台有人宣称正在售卖一份据称乌克兰核相关档案泄露文件。卖家称此份数据共两个压缩包，数据字段包含核设施档案、辐射源相关记录、官方文档等，此份数据的价格未知。



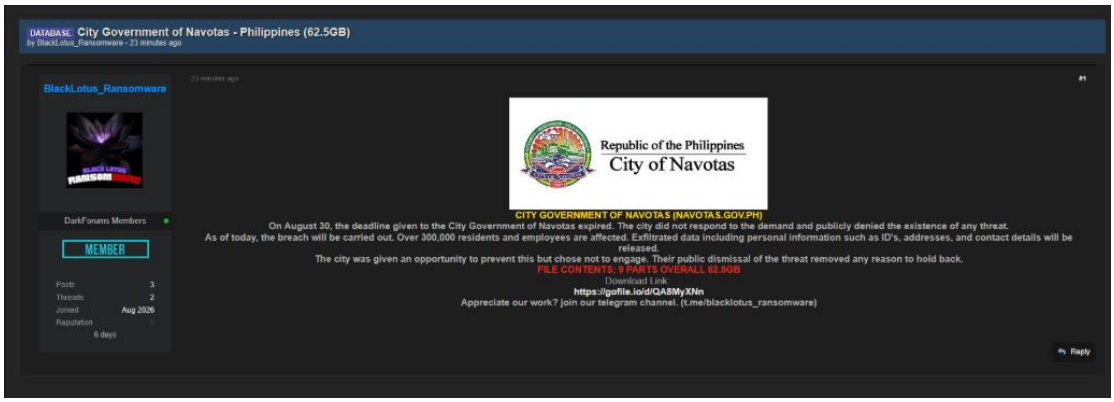
4、菲律宾 Navotas 市政府数据泄露

发布时间：2026.8.30

泄露数量：

售卖/发布人：BlackLotus_Ransomware

事件描述：2026.8.30 某暗网数据交易平台有人宣称正在售卖一份菲律宾纳沃塔斯市政府（City Government of Navotas）数据库。卖家称此份数据共 62.5GB（9 个分卷，据称涉及超 30 万居民及雇员），数据字段包含 IDs、addresses、contact details 等，此份数据的价格未知。



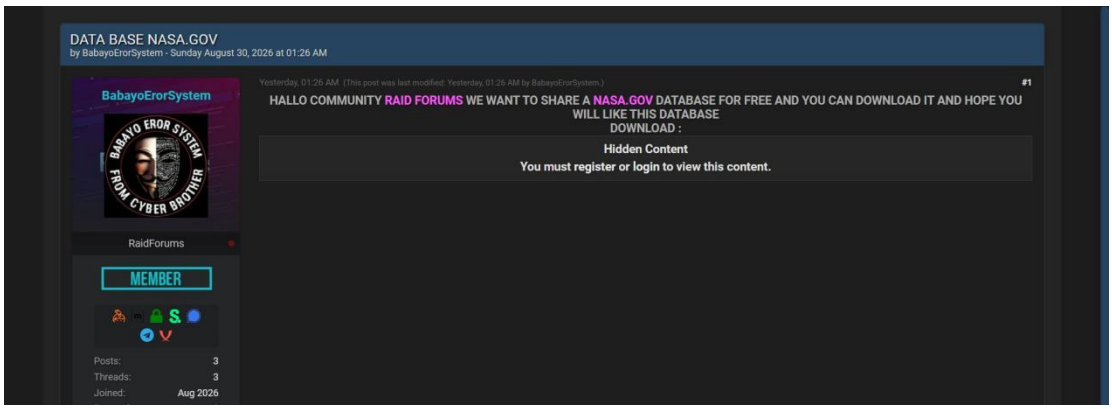
5、美国国家航空航天局（NASA / nasa.gov）数据泄露

发布时间：2026.8.30

泄露数量：

售卖/发布人：BabayoErorSystem

事件描述：2026.8.30 某暗网数据交易平台有人宣称正在售卖一份美国国家航空航天局（NASA / nasa.gov）数据库。卖家称此份数据共系统级记录数据集，数据字段包含未披露的数据库记录等，此份数据的价格未知。



6、中国物流公司数据泄露

发布时间：2026.8.27

泄露数量：102,000,000

售卖/发布人：killbibi

事件描述：2026.8.27 某暗网数据交易平台有人宣称正在售卖一份中国物流公司数据库。卖家称此份数据共 102,000,000 条记录，数据字段包含姓名、手机号、地址等，此份数据的价格未知。

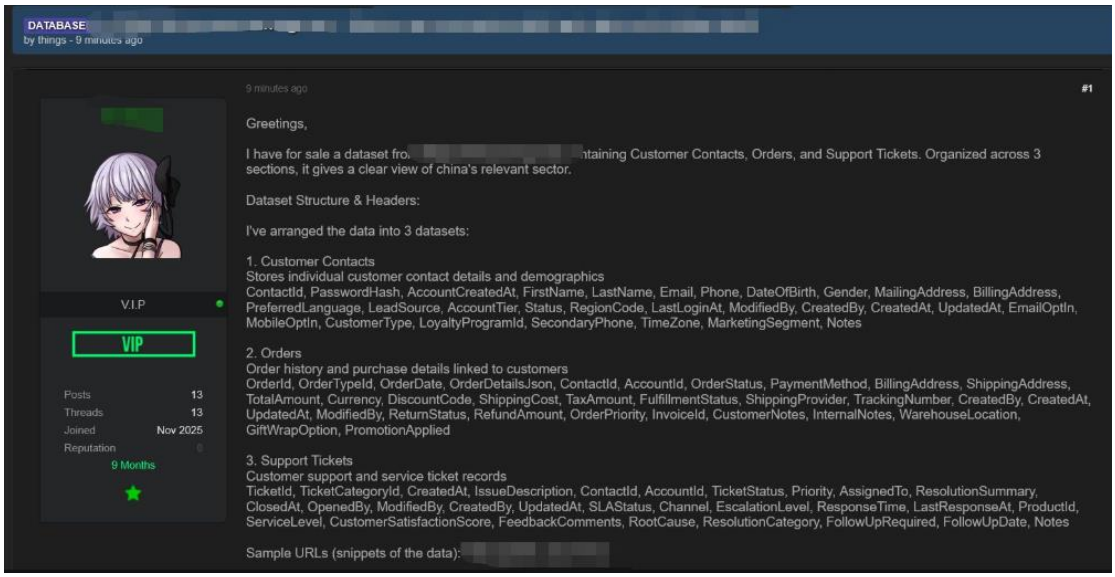
7、中国购物平台数据泄露

发布时间：2026.8.28

泄露数量：478,000

售卖/发布人：things

事件描述：2026.8.28 某暗网数据交易平台有人宣称正在售卖一份中国购物平台用户账户数据库。卖家称此份数据共约 478,000 条记录，数据字段包含 FirstName、LastName、Email、Phone、DateOfBirth、Gender、MailingAddress、BillingAddress、PasswordHash、Orders、Support Tickets 等，此份数据的价格未知。



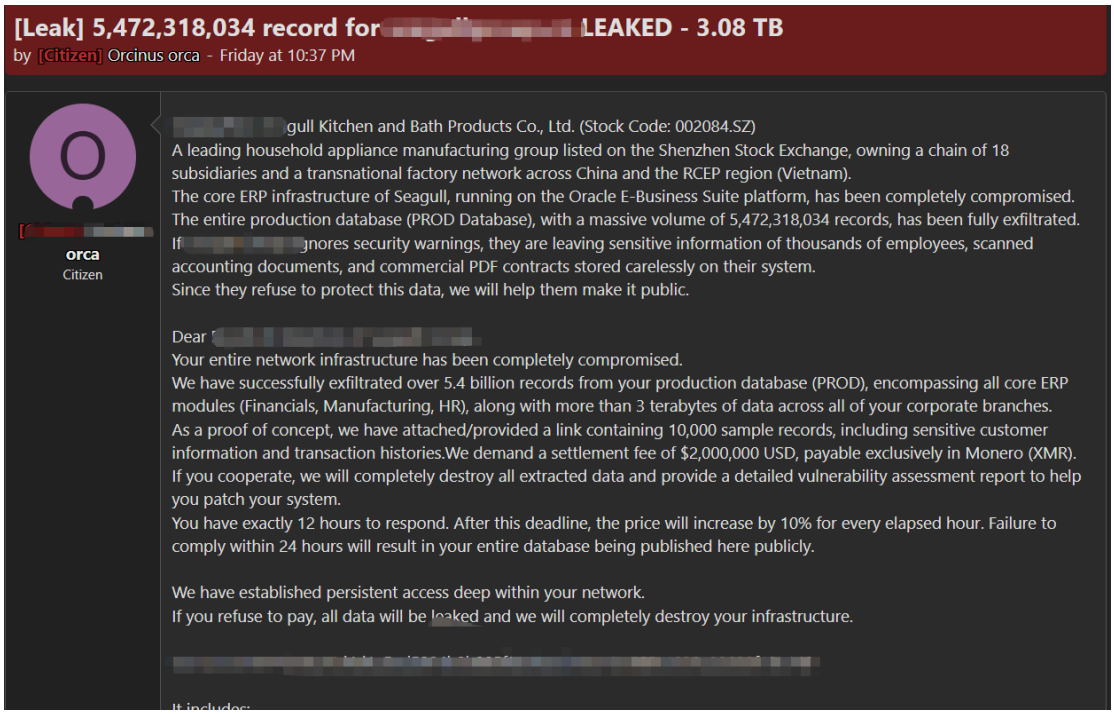
8、 中国卫浴用品平台数据泄露

发布时间：2026.8.28

泄露数量：5,472,318,034

售卖/发布人：Orcinus orca

事件描述：2026.8.28 某暗网数据交易平台有人宣称正在售卖一份中国卫浴用品平台生产数据库。卖家称此份数据共 5,472,318,034 条记录（约 3.08TB），数据字段包含 employee information、accounting documents、commercial contracts、ERP production records 等，此份数据的价格未知。



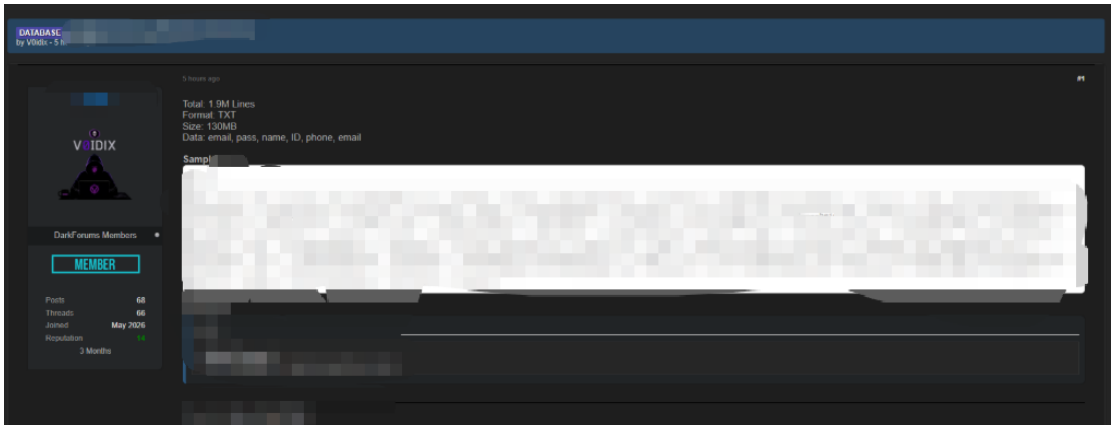
9、中国预定平台数据泄露

发布时间：2026.8.29

泄露数量：1,900,000

售卖/发布人：V0idix

事件描述：2026.8.29 某暗网数据交易平台有人宣称正在售卖一份中国预定平台数据库。卖家称此份数据共 190 万条记录（约 130MB），数据字段包含 email、pass、name、ID、phone 等，此份数据的价格未知。



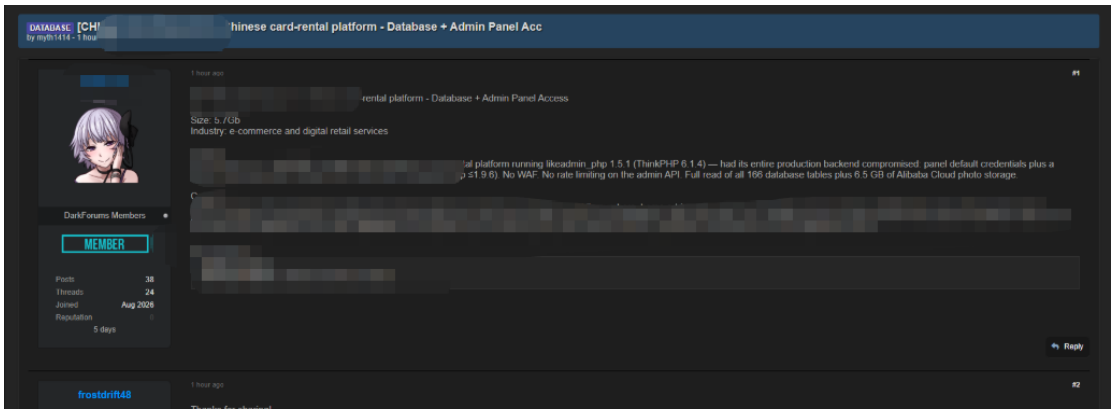
10、中国卡券租赁平台数据泄露

发布时间：2026.8.31

泄露数量：

售卖/发布人：myth1414

事件描述：2026.8.31 某暗网数据交易平台有人宣称正在售卖一份中国卡券租赁平台数据库。卖家称此份数据共约 6.70GB，数据字段包含 user accounts、national ID、name、mobile、address、login IP、password hash、rental orders、bank card records、SMS codes、face-verification photos、admin operation logs 等，此份数据的价格未知。



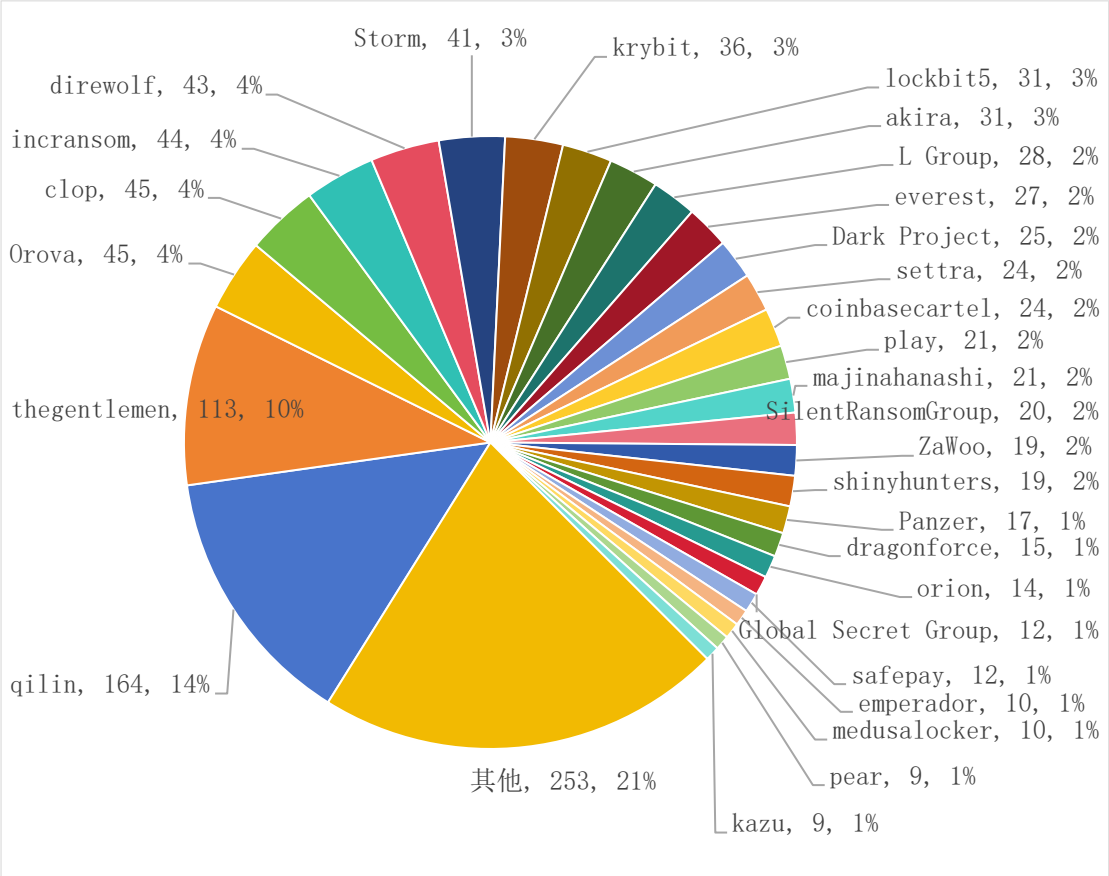
三、勒索软件和黑客组织

1、活跃商业黑客组织综述

2026 年 8 月全球活跃的商业黑客组织（有勒索发布行为）共 85 个，公开的勒索事件共 1182 件，TOP 10 的黑客组织如下所示：

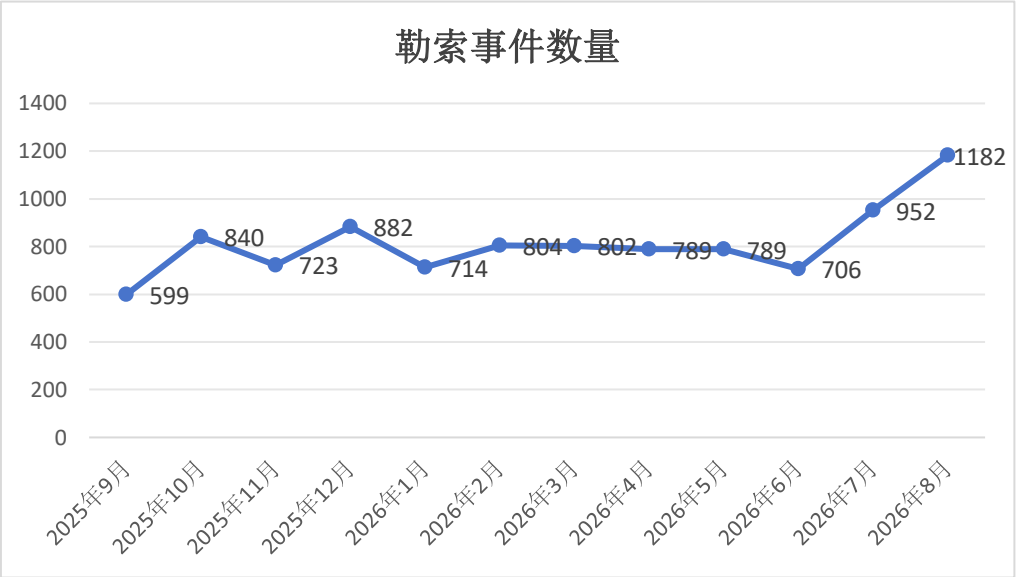

数世咨询
Digital World Consulting
X
零零信安
活跃商业黑客组织
TOP 10
排名
组织标识
组织名称
发布数量
01
qilin
164
02
THE GENTLEMEN
The gentlemen
113
03
OROVA
Orova
45
04
CL0P^_-LEAKS
clop
45
05
INC Ransom
Inc ransom
44
06
DIREWOLF
Direwolf
43
07
stormous
Storm
41
08
KRYBIT
krybit
36
09
lockbit5
31
10
AKIRA
Akira
31
数据来源 | 2026年8月《全球数据泄露态势月度报告》

TOP 30 的商业黑客组织公开发布的勒索事件占全部事件的 79%，如下所示：

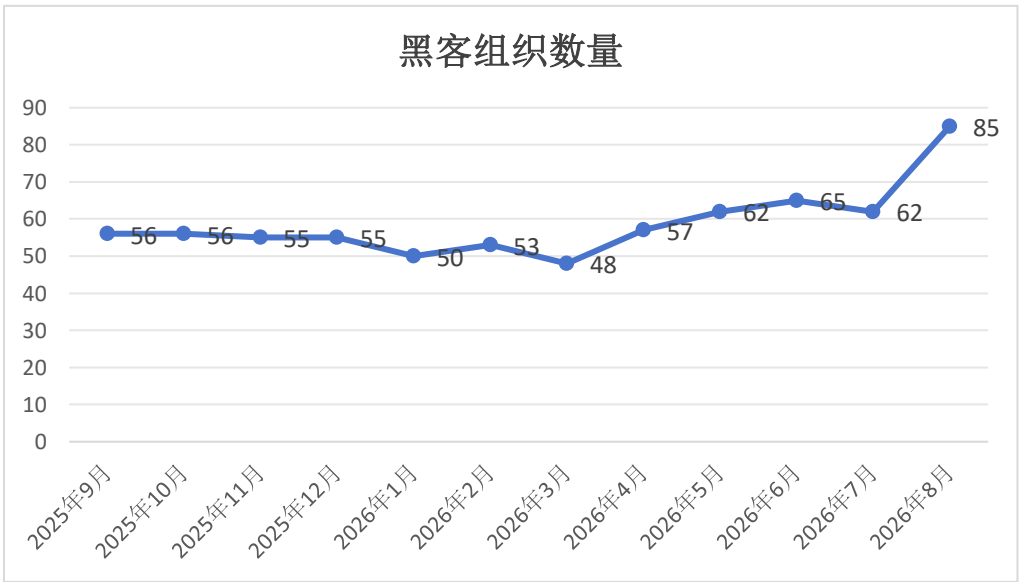


2、黑客组织活度趋势

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 8 月）达到一年前统计前端（2025 年 9 月）的 179.3%：



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

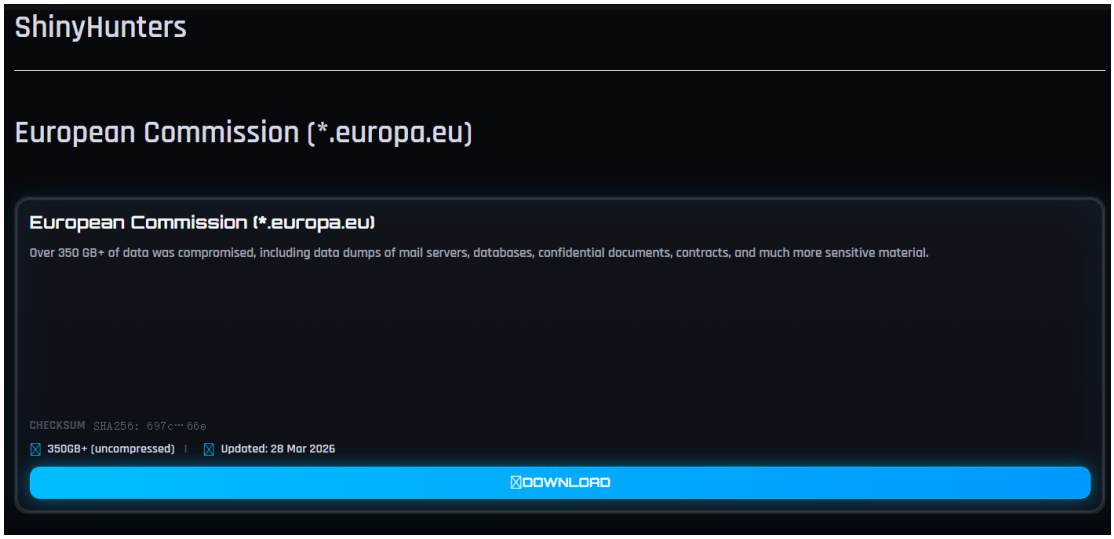
由于每月黑客组织行动数量庞大，无法在报告中枚举全部事件，分析员随机抽取展示 10 个典型样例事件，并对其中部分代表性事件进行细节说明：

事件	国家/组织	时间	黑客组织
European Commission	欧盟委员会	2026/8/5	ShinyHunters
City of McMinnville OR	美国俄勒冈州市政府	2026/8/6	RansomHouse
www.talbotdes.org	美国塔尔伯特县应急服务部门	2026/8/7	Lynx
Blog City of Winchester	英国温彻斯特市政府	2026/8/7	QiLin
Pierce Township	美国皮尔斯镇	2026/8/16	Rhysida
Otter Tail County, Minnesota	美国明尼苏达州奥泰尔县	2026/8/17	INC Ransom
City of Mitchell	美国米切尔市	2026/8/23	STORM
Blog ATF	美国烟酒枪炮及爆炸物管理局	2026/8/26	QiLin
Berlin, Germany	德国柏林市政府	2026/8/27	Rhysida
Blog Commission de la construction du Quebec	加拿大魁北克建筑委员会	2026/8/31	QiLin

1）欧盟委员会

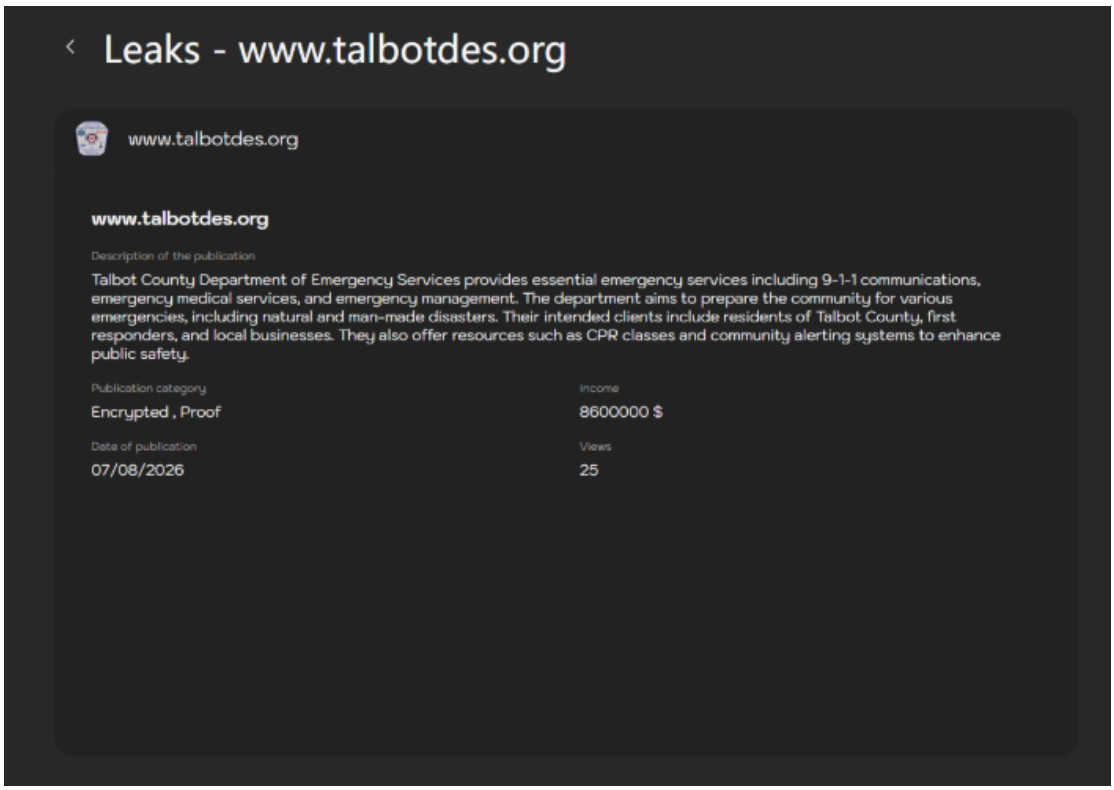
商业黑客组织 ShinyHunters 在 2026/8/5 公布了欧盟委员会（European Commission）被勒索的信息。欧盟委员会是欧盟的行政机关，负责提出立法建议、执行欧盟政策和日常行政事务。欧盟委员会位于比利时布鲁塞尔，以推动欧洲一体化和管理欧盟共同政策为特色。截止本篇报告发出之时，黑客组织

ShinyHunters 尚未发布更多关于欧盟委员会的数据。



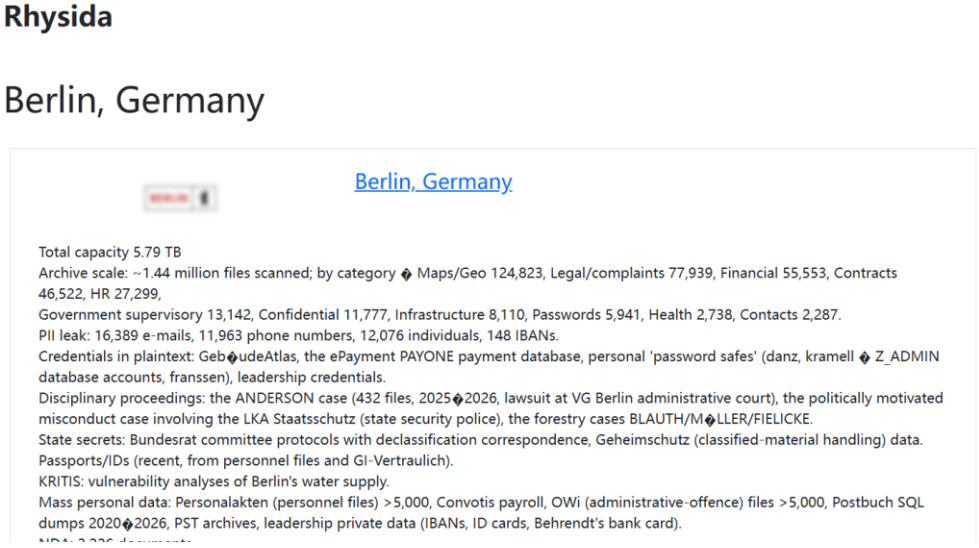
2）美国塔尔伯特县应急服务部门

商业黑客组织在 2026/8/7 公布了美国马里兰州 Talbot County 应急服务局被勒索的信息。美国马里兰州 Talbot County 应急服务局是 Talbot County 的一个地方政府应急管理机构，负责 911 通讯、应急医疗服务和应急管理。Talbot County 应急服务局位于美国马里兰州 Talbot County，以社区应急准备和公共安全服务为特色。截止本篇报告发出之时，黑客组织尚未发布更多关于 Talbot County 应急服务局的数据。



3）德国柏林市政府

商业黑客组织 Rhysida 在 2026/8/27 公布了德国柏林被勒索的信息。德国柏林是德国的首都和联邦州，负责城市行政管理与公共服务。柏林位于德国东北部，以政治中心、历史文化和文化多元为特色。截止本篇报告发出之时，黑客组织 Rhysida 尚未发布更多关于柏林的数据。



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
易*****有限公司	批发零售业	2026/8/31	Nightspire
耀*****股份有限公司	科技业	2026/8/31	Orova
复*****股份有限公司	制造业	2026/8/31	Orova
Pr******公司	科技业	2026/8/30	The Gentlemen
E*****会计师事务所	居民服务	2026/8/30	ZaWoo
德*****集团有限公司	建筑和房地产业	2026/8/29	Orova
南*****有限公司	食衣住行	2026/8/29	Orova
杭*****有限公司	卫生医疗业	2026/8/28	global
上*****有限公司	建筑和房地产业	2026/8/28	global
A******公司	科技业	2026/8/28	global
阿*****有限公司	制造业	2026/8/25	Orova
百*****事务所	居民服务	2026/8/25	Orova
c*****m	其他	2026/8/25	chaos
智*****限公司	科技业	2026/8/23	The Gentlemen
R*****团	科技业	2026/8/22	coinbasecartel
U*****C	其他	2026/8/19	Deadlock

德*****有限公司	金融	2026/8/19	Orova
ww*****o	其他	2026/8/19	krybit
逸*****有限公司	卫生医疗业	2026/8/18	Inc Ransom
Sm*****t 公司	科技业	2026/8/16	Orova
鸿*****有限公司	科技业	2026/8/12	clop
大*****股份有限公司	制造业	2026/8/12	clop
h*****m	其他	2026/8/12	krybit
赣*****有限公司	制造业	2026/8/11	Orova
药*****有限公司	卫生医疗业	2026/8/10	The Gentlemen
香*****大学	教育	2026/8/10	The Gentlemen
动*****公司	能源	2026/8/9	QiLin
熊*****中分公司	交通和仓储	2026/8/9	QiLin
春*****有限公司	制造业	2026/8/9	QiLin
深*****有限公司	卫生医疗业	2026/8/7	Clop
拉*****有限公司	制造业	2026/8/7	L Group
R*****份有限公司	制造业	2026/8/6	Barracuda
E*****术设备公司	科技业	2026/8/4	Orova
确*****公司	文体娱乐	2026/8/4	Orova
DB*****x 公司	制造业	2026/8/4	Orova
U*****e 公司	批发零售业	2026/8/4	Orova
京*****司	制造业	2026/8/4	Orova
S*****公司	批发零售业	2026/8/4	Orova
三*****有限公司	批发零售业	2026/8/4	Orova
达*****限公司	制造业	2026/8/4	Orova
J*****限公司	金融	2026/8/4	Orova
百*****斩	信息和互联网	2026/8/3	Dragonforce
途*****国	文体娱乐	2026/8/3	Dragonforce

5、典型黑客组织简介（direwolf）

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。

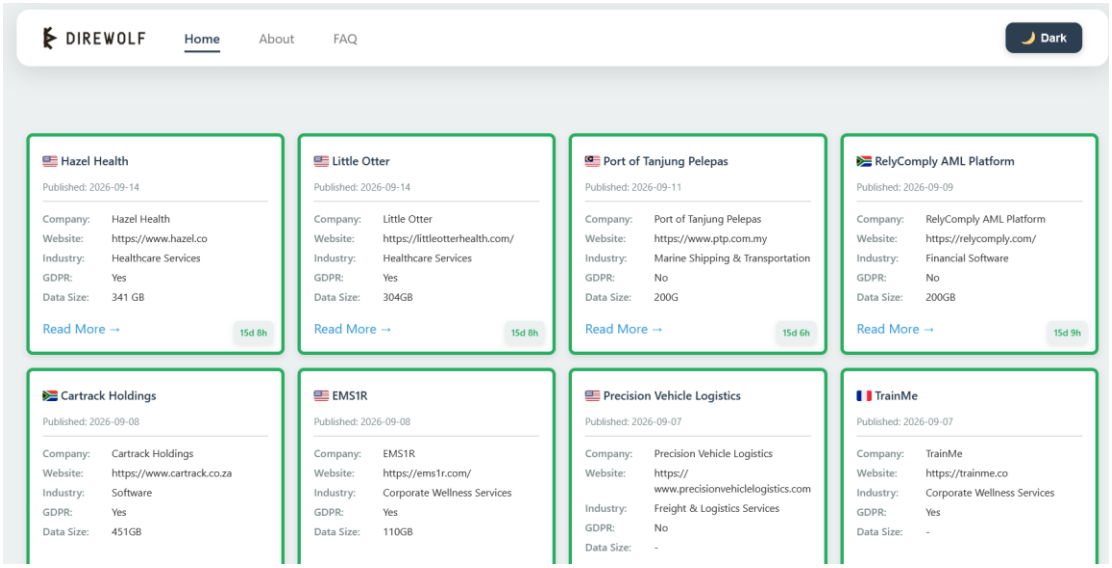
已经介绍过的黑客组织有：Lockbit3，Royal，Play，Rhysida，Alphv，8base，Hunters International、BianLian、Akira、Cactus、Abyss-Data、Black Suit、Arcus Media、space bear、killsec、fog、Funksec、Babuk-Bjorka、Hellcat、Babuk2、NightSpire、Dragonforce、Handala、D4RK4RMY、Warlock、World Leaks、sinobi 、Interlock、Qilin、Anubis、The Gentlemen、Beast、ShinyHunters、INC Ransom、Krybit、CL0P 如需了解请翻阅往期报告。

本期为您介绍的是 Dire Wolf 勒索软件黑客组织，Dire Wolf（亦写作 Direwolf / DireWolf）是一个于 2025 年 5 月公开现身的双重勒索新兴团体，由相对封闭的核心团队人工操作，而非开放式大规模 RaaS 加盟网络。它采用“数据窃取+加密勒索”模式运营，以 Go 语言编写、UPX 加壳的 Windows 加密器锁定文件并追加.direwolf 扩展名，同时删除备份、清除日志并终止关键服务以阻断恢复，再通过定制化勒索信、Tox 即时通讯以及面向单个受害者的 Tor 谈判门户施压。其关键技术能力包括针对企业环境的人工入侵与横向移动、数据外泄先于加密、多线程并行加密、防御规避与反取证，以及通过 Tor 数据泄露站点（DLS）进行公开点名和赎金谈判。公开情报显示其赎金要求可达约 50 万美元量级，并以“只为钱、无政治立场”自我定位，对制造业、科技、医疗、专业服务与金融等行业实施机会主义打击。

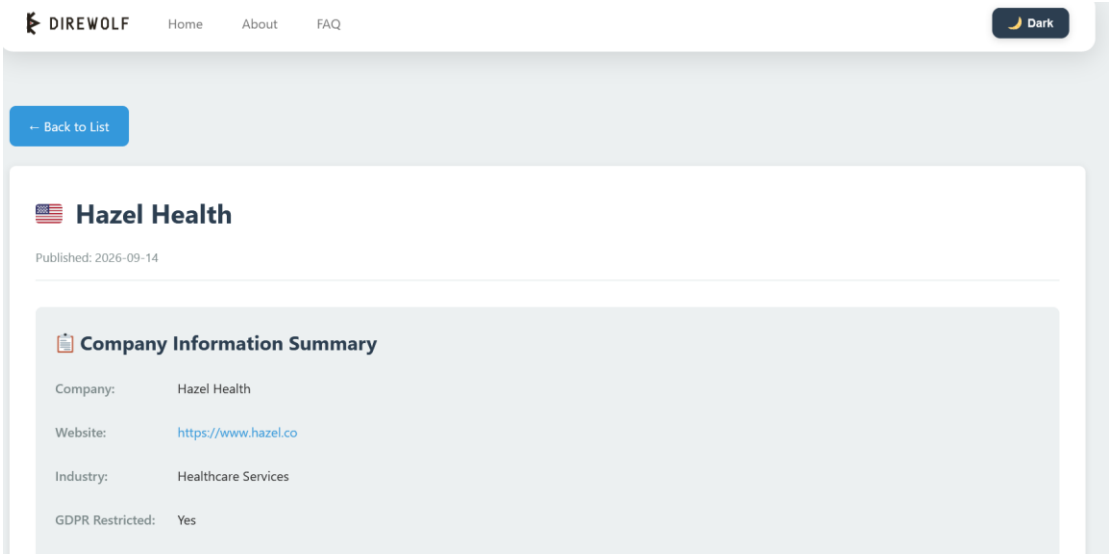
截至 2026 年 8 月，Dire Wolf 已累计声称约 130 余个受害者，近 30 天仍

保持较高更新节奏，主要针对全球约 30 余个国家/地区（美国、马来西亚、泰国、巴西、英国、新加坡、澳大利亚等），重点行业包括医疗健康、专业服务、技术、制造业和金融服务，常造成敏感数据外泄、源代码与设计图纸暴露、运营中断、声誉损害、监管合规问题以及持续的公开 DLS 勒索压力。典型案例包括对西澳大利亚法律执业委员会、* 湾*****业（S*****r）、阿德莱德游戏开发商 Mighty Kingdom（声称逾 260 个代码仓库）、Wolfram Research（声称约 2.5TB 数据）、马来西亚丹绒帕拉帕斯港（Port of Tanjung Pelepas）、巴西科技公司 TOTVS，以及 Hazel Health、DodoPayments 等组织的攻击，常伴随数 GB 至 TB 级数据外泄威胁，并对亚太制造业与科技供应链表现出明显适应性。

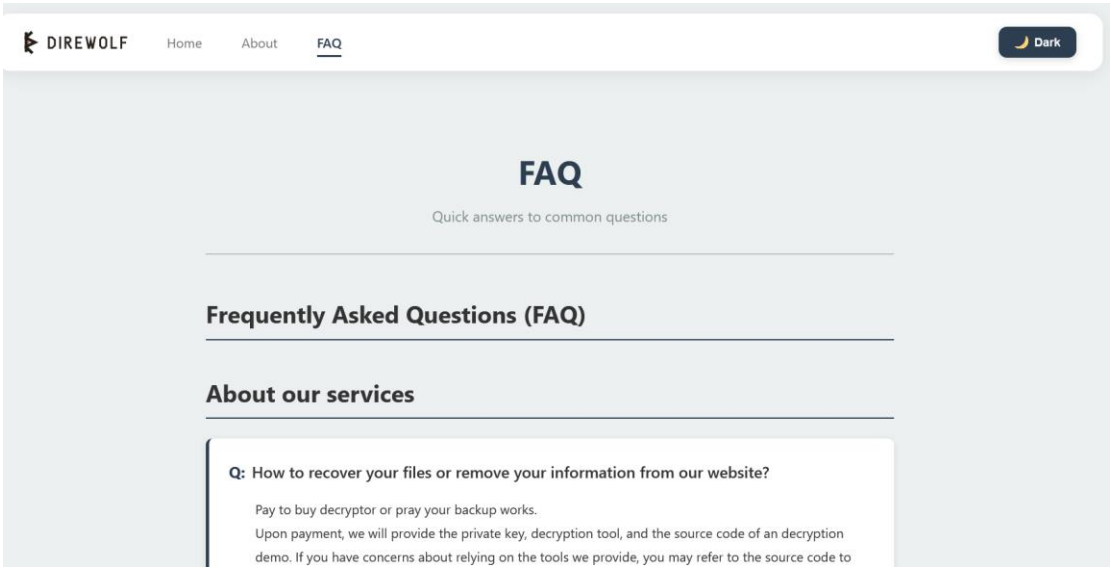
下图为 Dire Wolf 所运营的数据泄露网站：



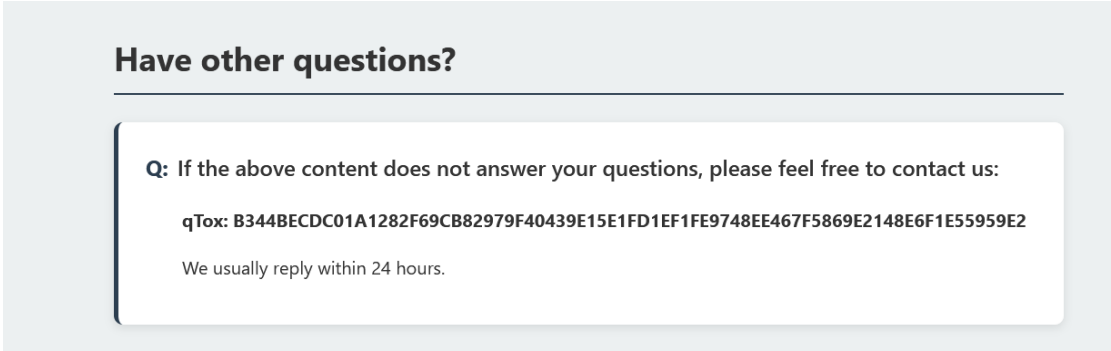
下图为 Dire Wolf 运营网站上的泄露事件详情：



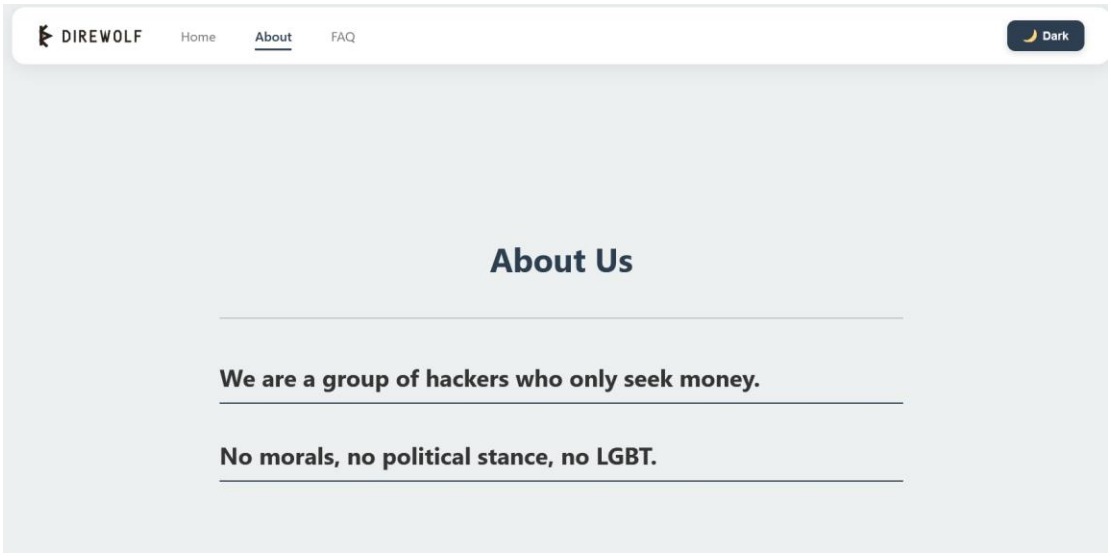
下图为 Dire Wolf 运营网站上的 FAQ 页面：



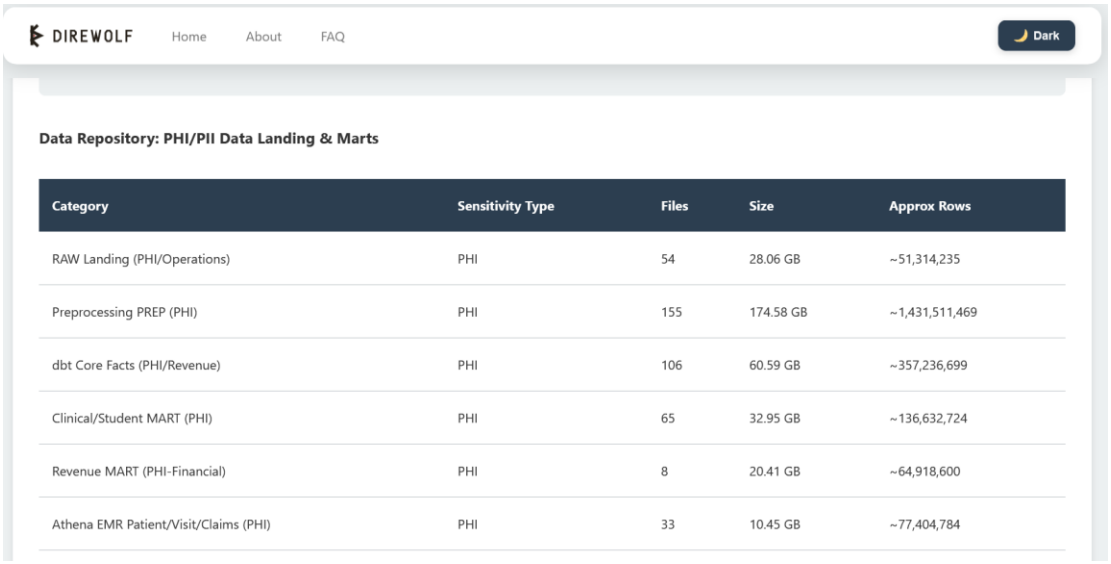
下图为 Dire Wolf 运营网站上的联系方式：



下图为 Dire Wolf 运营网站上的 About Us 页面：



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：

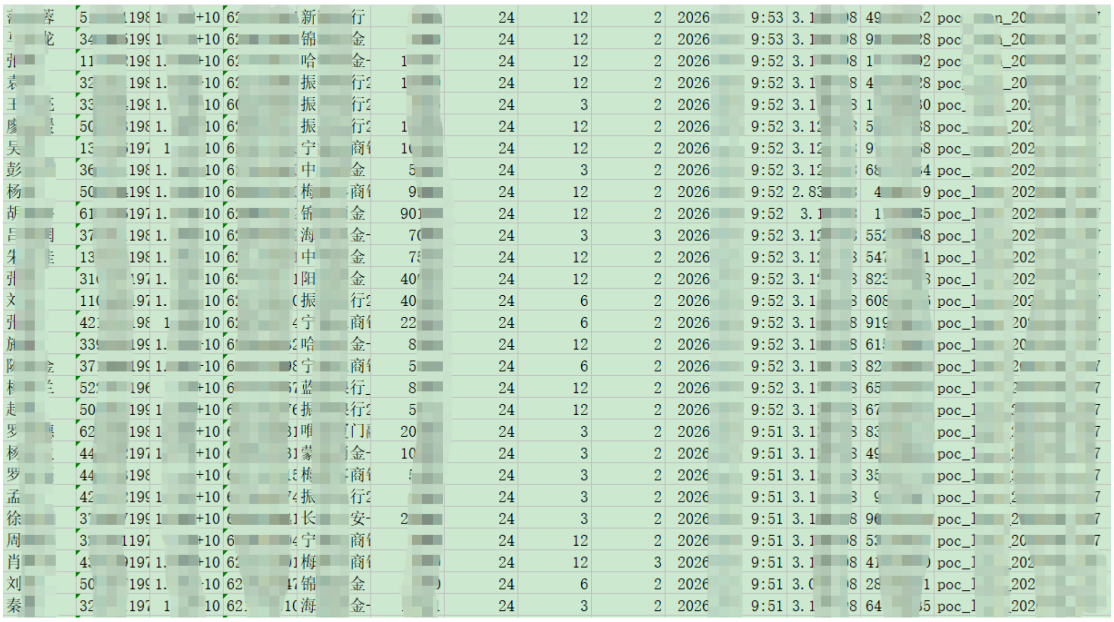


四、匿名社交社群

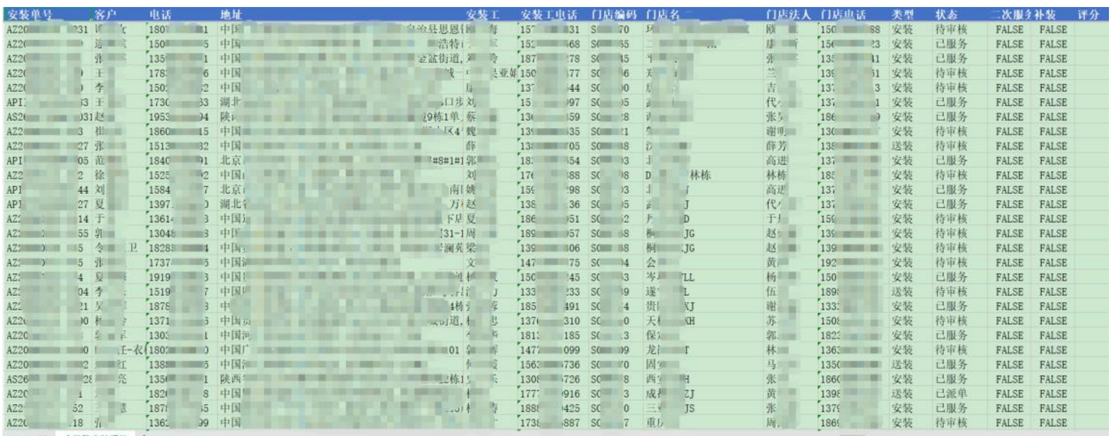
8 月份监控到匿名社交社群情报总数量 19,493,513 条，提供的有效数据泄露样例下载 3,980 份。涉及到我国数据泄露的内容包括：快递信息、银行信息、

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：

客户ID	姓名	昵称	手机	手机归属地	订单ID	购买服务	应付金额	会员实付	支付时间
[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	39.9	39.9	[illegible]
[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	39.9	39.9	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	39.9	39.9	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	39.9	39.9	[illegible]
[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	39.9	39.9	[illegible]
[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	9.9	9.9	[illegible]



序号	需求编号	目标品牌	目标店铺	商品名称	购买（频次）	收藏（频次）	性别（男，女）	父母年龄	孩子年龄	常用收货地址（省，市，区）
1	[illegible]	[illegible]	[illegible]	[illegible]						[illegible]
2	[illegible]	[illegible]	[illegible]	[illegible]						[illegible]
3	[illegible]	[illegible]	[illegible]	[illegible]						[illegible]

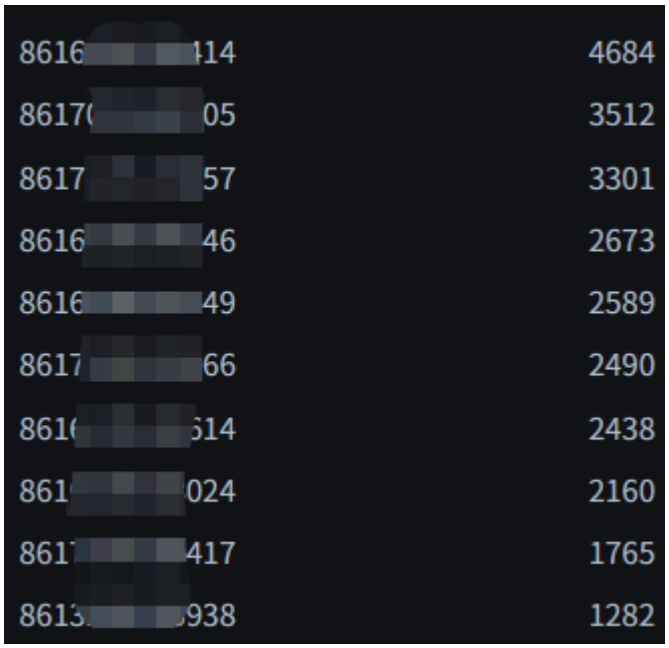


安装单号	客户	电话	地址	安装工	安装工电话	门店编码	门店名	门店法人	门店电话	类型	状态	二次服务补装	评分

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

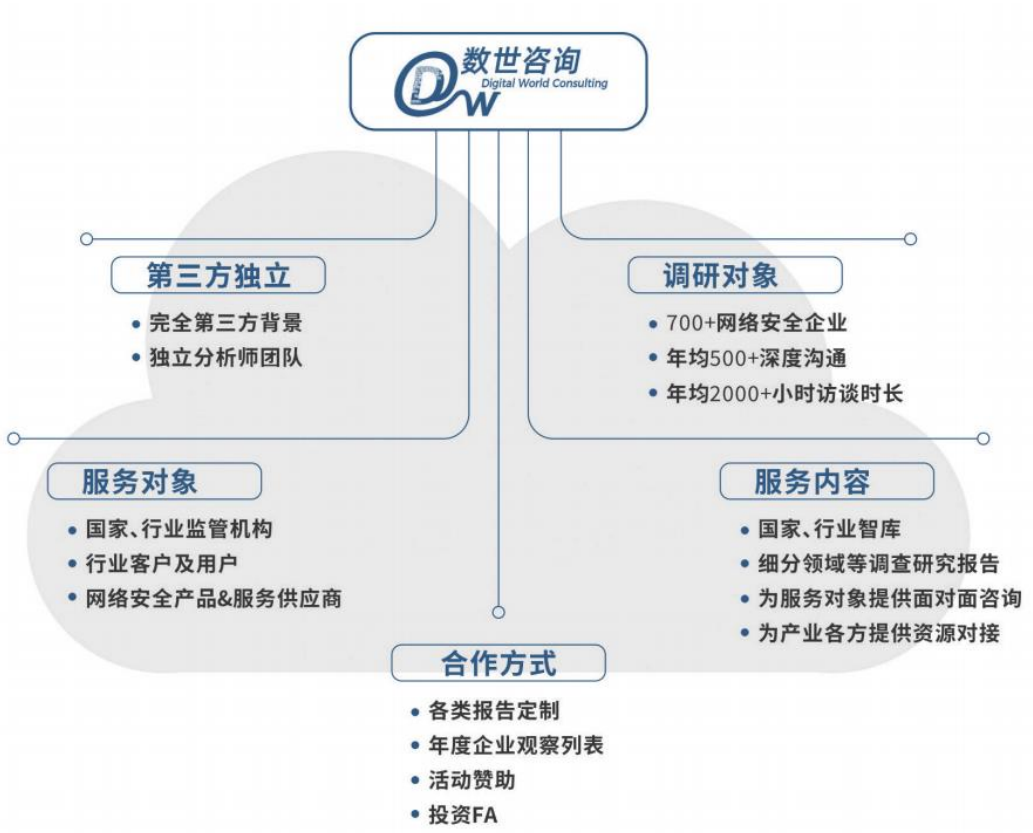
10 万条左右，全数据量估算在 1000 万条以上。

此外，检索到 8 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 38116 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 7 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800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