数据泄露态势月度报告

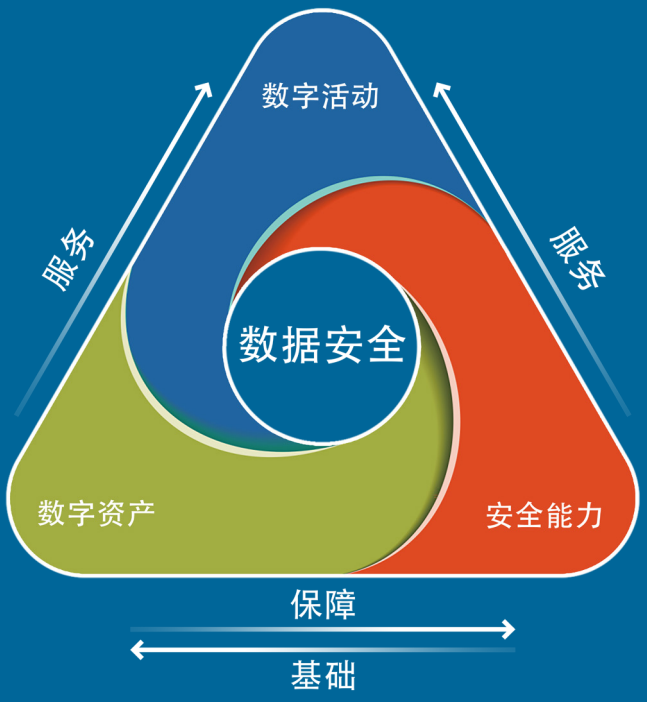
（2024 年 1 月）

北京数字世界咨询有限公司 & 北京零零信安科技有限公司

数据泄露态势月度报告

（2024 年 1 月）

北京数字世界咨询有限公司 & 北京零零信安科技有限公司



数字安全的三个元素分别为，安全能力、数字资产和数字活动。数字资产是安全能力的保护对象，数字活动是安全能力以及数字资产的服务对象，而数据安全则是三元论的核心目标。对于这四者关系的深度理解和相关技能掌握是做好数字安全工作的关键。

数字安全能力模型研究的基础，来自于数世咨询 2020 年首次提出的“网络安全三元论”。三元分别为，网络攻防、信息技术和业务场景。

随着数据成为第五大生产要素为典型标志的数字时代来临，“网络安全三元论”在 2022 年进行了更新迭代升级为“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”，以适应我国数字中国建设的进程。

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

版权声明

目 录

目 录

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。

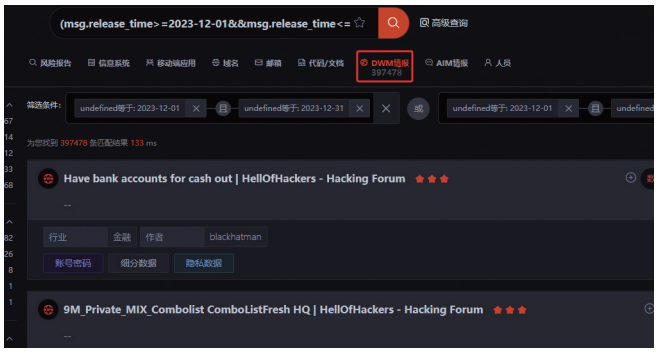
为了掌握数据泄露态势，应对日益复杂的安全风险，数世咨询联合零零信安，基于 0.zone 安全开源情报系统，共同发布《数据泄露态势》月度报告。该系统监控范围包括明网、深网、暗网、匿名社群等约 10 万个威胁源。除了月度的数据泄露概况以外，报告还会针对一些典型的数据泄露事件进行抽样事件分析。如果发现影响较大的数据伪造事件，还会对其进行分析和辟谣。

本期报告的统计区间 2023 年 12 月。

第一章　数据泄露市场

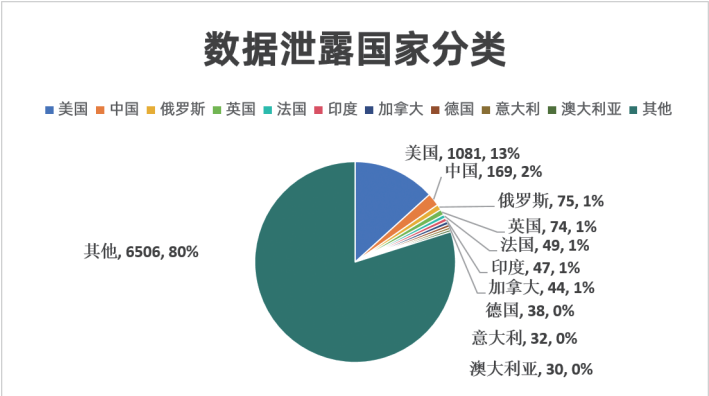
2023 年 12 月共监控到全球 DWM（Dark Web Market）情报：

- 深网和暗网有效情报 307,478 份；
- 泄露数据的买卖情报份 8,145 份。



1、国家分类

其中美国是数据泄露第一大国，共泄露数据 1,081 份，其他数据泄露较多的国家还包括：中国、俄罗斯、英国、法国、印度、加拿大等。详情如下图所示：

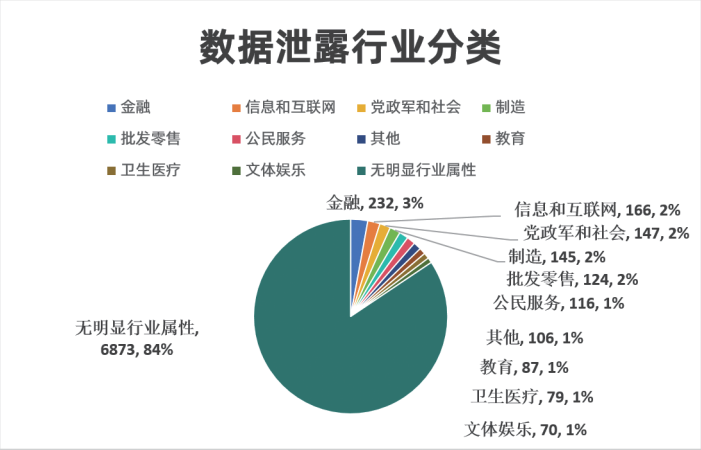


在“其他”数据中包含其他国家以及无法准确进行国家分类的数据泄露事件，例如二要素数据（账号：密码 / 邮箱：密码）、LOG 记录等。

2、行业分类

12 月份行业属性数据占泄露数据总量约 16% 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、党政军与社会、制造业、批发零售业等。84% 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

12 月份泄露的数据中包含数份超十亿的二要素个人数据泄露，因此除上述数据外，全球整体数据泄露量达到**数十亿行以上**。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**十亿行以上**。

第二章　事件抽样分析

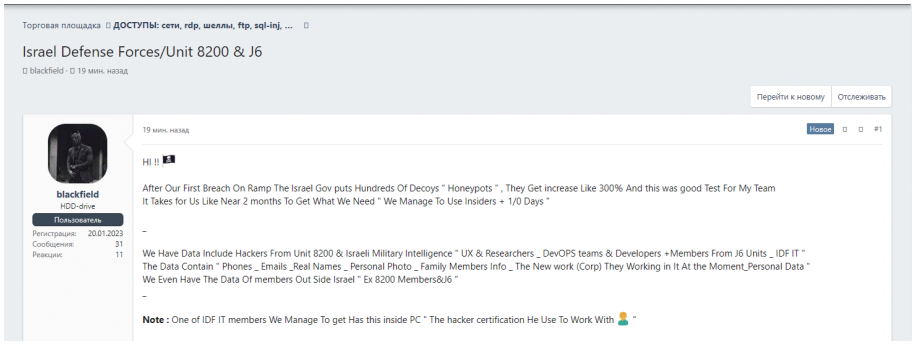
1、以色列国防军情报部门数据泄露

发布时间：2023.12.22

泄露数量：

售卖/发布人：blackfield

事件描述：2023.12.22 某暗网数据交易平台有人宣称正在售卖一份以色列国防军情报部门数据。该黑客出售的数据中包含了以色列军事情报局 8200 部队以及以色列 J6 和网络防御局军队成员信息数据，数据包含了：电话、电子邮件、姓名、个人照片、家庭成员信息、他们目前在其中工作的新工作（公司）等个人数据，同时该黑客还上传了一些个人照片作为样例。该数据售卖的价格为 50000 美元。



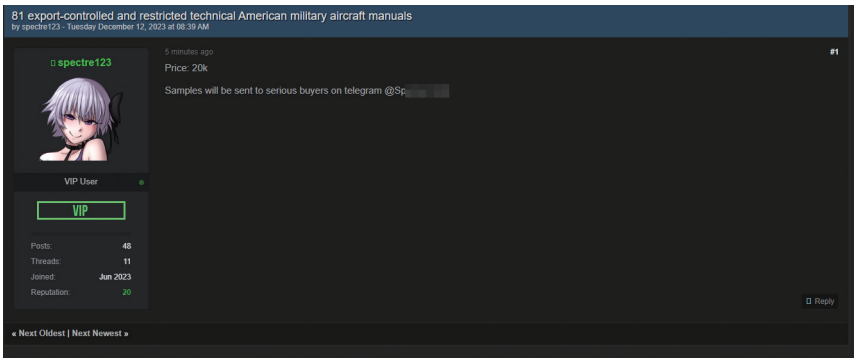
2、81 出口管制和受限技术美国军用飞机手册数据泄露

发布时间：2023.12.12

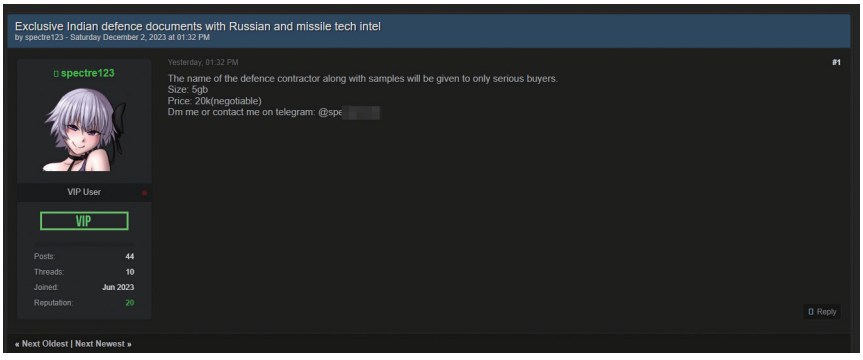
泄露数量：

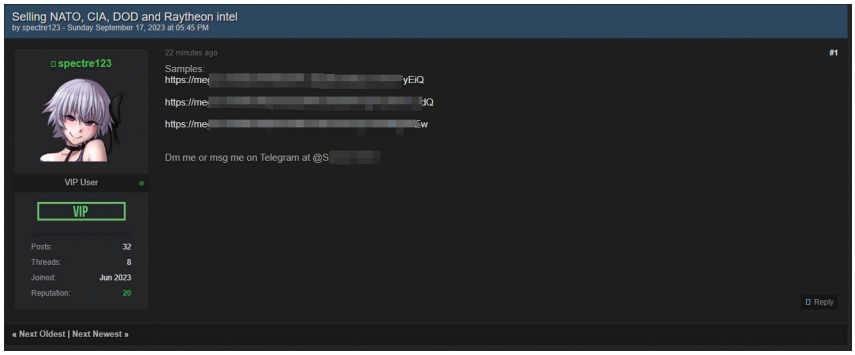
售卖 / 发布人：spectre123

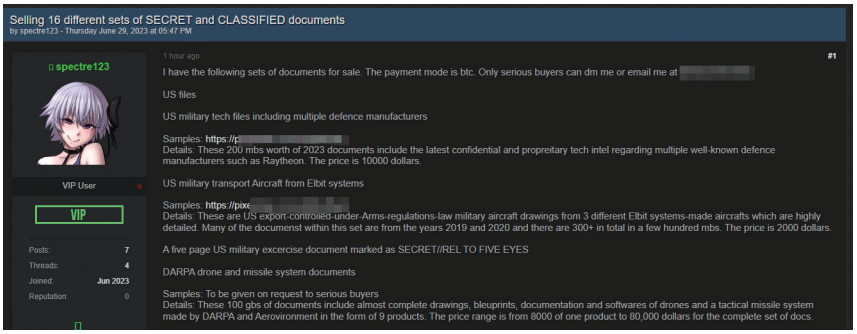
事件描述：2023.12.12 某暗网数据交易平台有人宣称正在售卖一份出口管制和受限技术美国军用飞机手册数据。据卖家称该数据总大小为 5GB，价格为 20000 美元并且可议价。该作者并未上传样例，但留下了自己的 telegram 联系方式并留言道“样例只会发给真正的卖家”。



值得注意的是，该作者攻击发布的 12 篇帖子中，除一篇求购贴和两篇企业数据外，剩余的帖子内容全部为出售各国军事数据，包括但不限于：印度国防文件、北约、美国中情局、美国国防部、美国军队、韩国军事信息、菲律宾海军和陆军信息等。







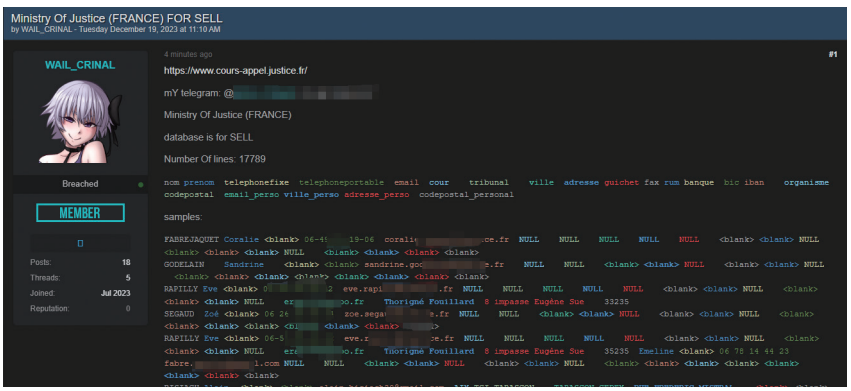
3、法国司法部数据泄露

发布时间：2023.12.19

泄露数量：17,789

售卖/发布人：WAIL_CRINAL

事件描述：2023.12.19 某暗网数据交易平台有人宣称正在售卖一份法国司法部数据，总条数为 17,789 条，给出的样例中有姓名、电话、邮箱、地址等个人信息数据。



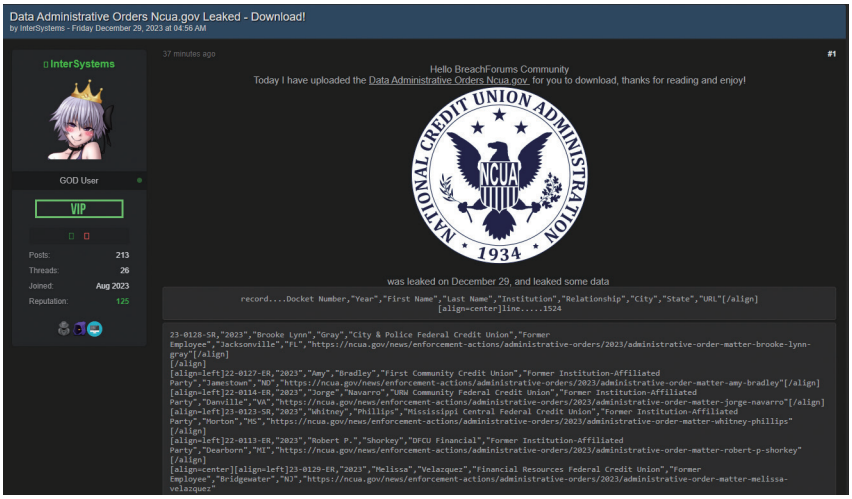
4、美国国家信用社管理局（NCUA）数据泄露

发布时间：2023.12.29

泄露数量：1,524

售卖 / 发布人：InterSystems

事件描述：2023.12.29 某暗网数据交易平台有人宣称正在售卖一份美国国家信用社管理局（NCUA）数据，给出的样例中可以看到的数据字段有：记录案卷号、年份、名字、姓氏、机构、关系等。该数据总条数为 1,524 条，价格暂时未知。



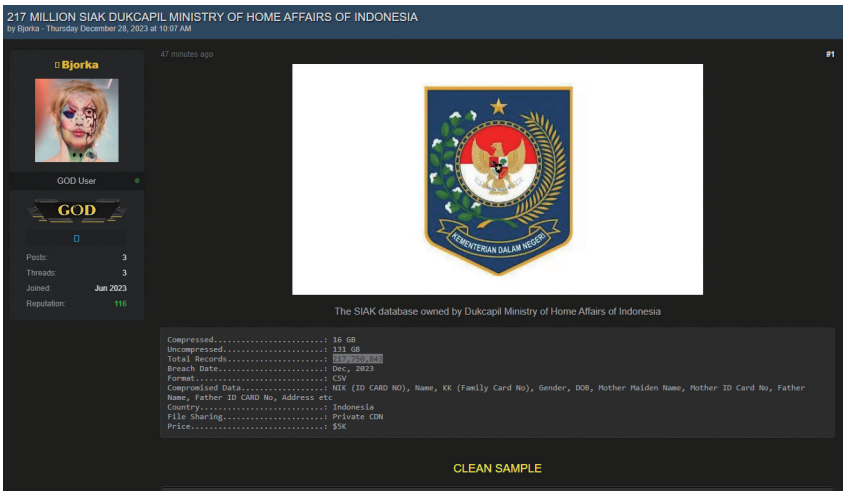
5、印度尼西亚民事登记局 SIAK 数据泄露

发布时间：2023.12.28

泄露数量：217,750,843

售卖 / 发布人：Bjorka

事件描述：2023.12.28 某暗网数据交易平台有人宣称正在售卖一份印度尼西亚民事登记局 SIAK 数据。该数据总计 217,750,843 条，总大小为 131GB，价格为 5000 美元。给出的样例中数据字段有：姓名、身份证号、出生日期、父 / 母亲姓名、父 / 母亲身份证号、地址等。



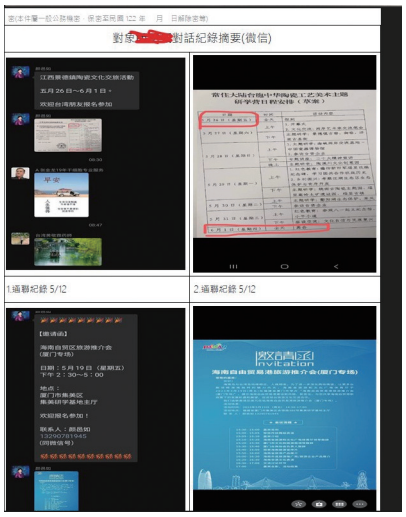
6、台湾政府数据泄露

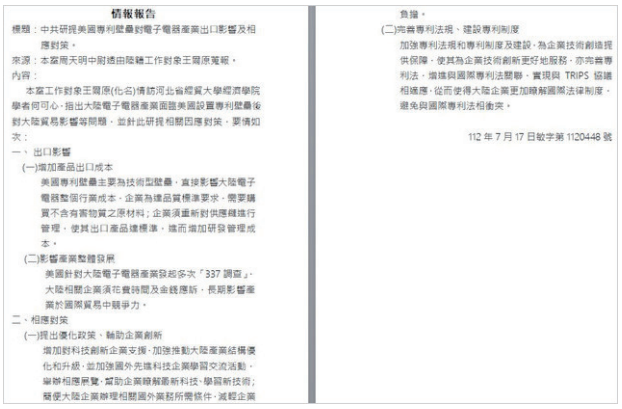
发布时间：2023.12.17

泄露数量：

售卖/发布人：carstongrice

事件描述：2023.12.17 某暗网数据交易平台有人宣称正在售卖一份台湾政府数据。据卖家称该数据总大小为 20GB 的图片和文档表格，并附上了一些看起来像聊天记录、工作任务安排、合同等文件，该数据的价格以及真假性暂且未知。





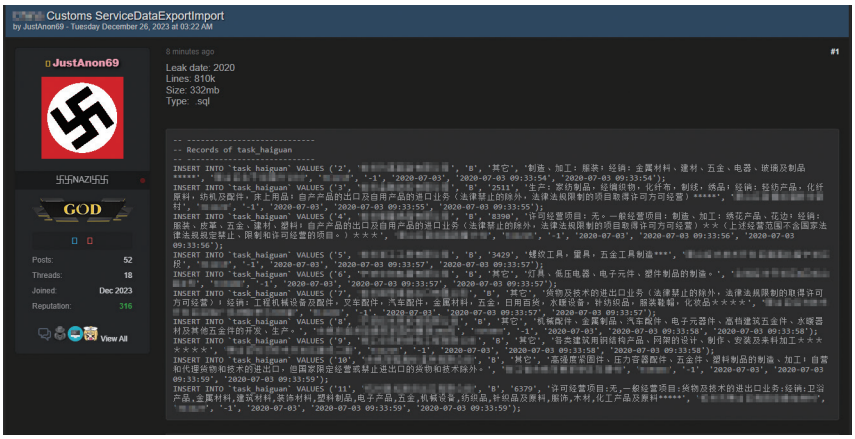
7、* 国海关总署数据出口进口数据泄露

发布时间：2023.12.26

泄露数量：810,000

售卖 / 发布人：JustAnon69

事件描述：2023.12.26 某暗网数据交易平台有人宣称正在售卖一份 * 国海关总署数据出口进口数据。据卖家称该数据共计 810,000 条，总大小为 332MB。根据卖家提供的样例数据判断，该数据大概率为拼凑出来的假数据。



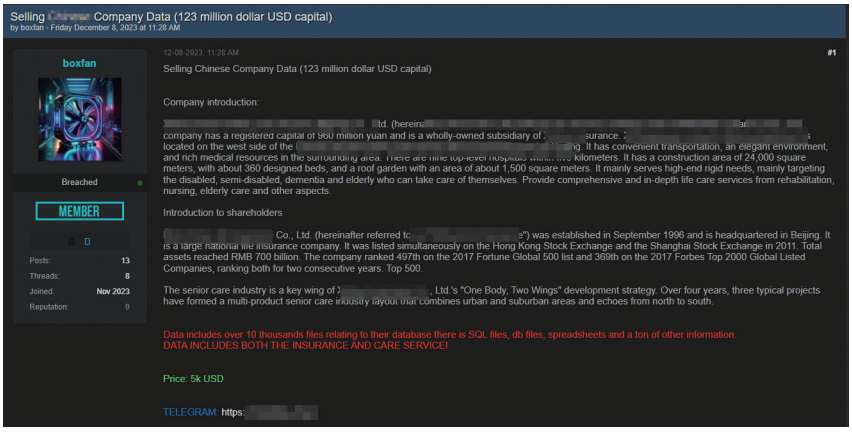
8、新 ** 家养老服务 (**) 有限公司数据泄露

发布时间：2023.12.8

泄露数量：

售卖/发布人：boxfan

事件描述：2023.12.8 某暗网数据交易平台有人宣称正在售卖一份新**家养老服务（**）有限公司数据。据卖家称该数据包括超过 1 万个与其数据库相关的文件以及电子表格和大量其他信息，泄露的数据内容主要包括保险和护理服务。该份数据被标价为 5000 美元。



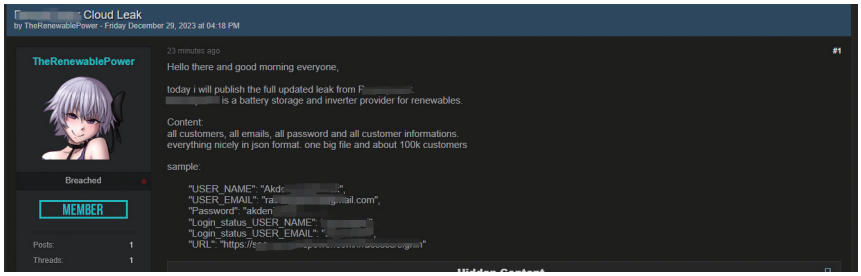
9、纳 ** 源数据泄露

发布时间：2023.12.29

泄露数量：100,000

售卖/发布人：TheRenewablePower

事件描述：2023.12.8 某暗网数据交易平台有人宣称正在售卖一份一家可再生能源电池存储和逆变器供应商纳 ** 源的客户数据。据卖家称该数据共计 100,000 条，给出的样例中的数据字段有：姓名、邮箱、密码等。



10、* 抖 ** 购物数据泄露

发布时间：2023.12.5

泄露数量：315,000,000

售卖 / 发布人：1******6

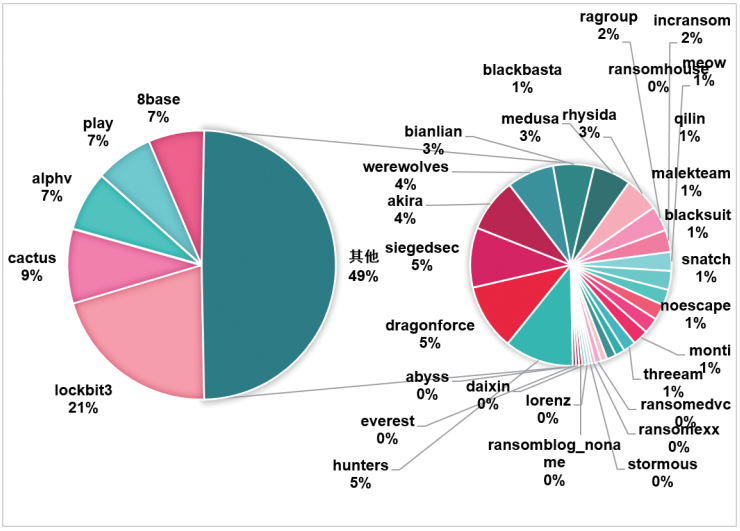
事件描述：2023.12.5 某暗网数据交易平台有人宣称正在售卖一份购物数据。该份数据共计 315,000,000 条，总大小为 49.2GB，售卖价格为 888 美元。卖家称该份数据的来源为 * 抖 **，给出的样例中数据字段包括：姓名 / 昵称、电话、地址、订单内容。

第三章　勒索软件和黑客组织

1、活跃商业黑客组织综述

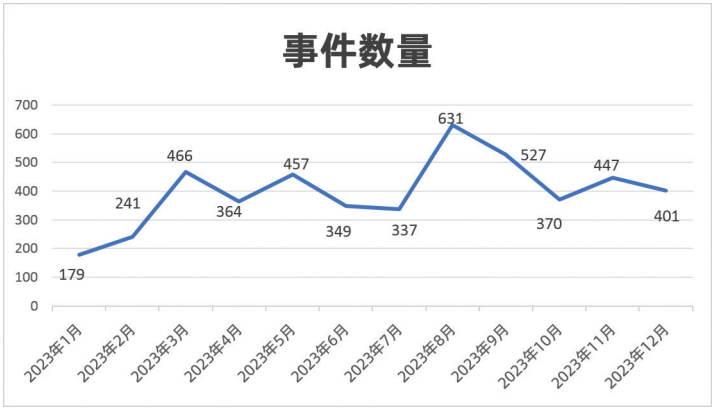
2023 年 12 月全球活跃的商业黑客组织（有勒索发布行为）共 33 个，公开的勒索事件共 401 件，TOP 10 的黑客组织如下所示：

TOP 10 的商业黑客组织公开发布的勒索事件占全部事件的 51%，如下所示：

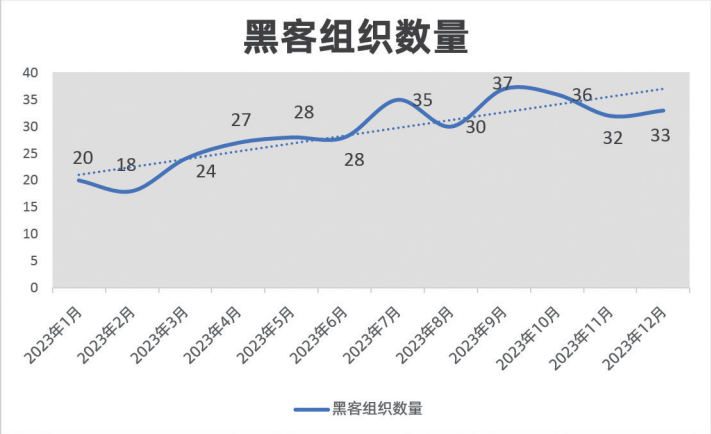


2、黑客组织活跃度趋势

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下降），但整体活跃度趋势正在逐步增加，统计末端（2023 年 12 月）已达到一年前统计前端（2023 年 1 月）的 224%：



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，本月活跃黑客组织数量达到历史新高。如下图所示：



3、本月典型事件说明

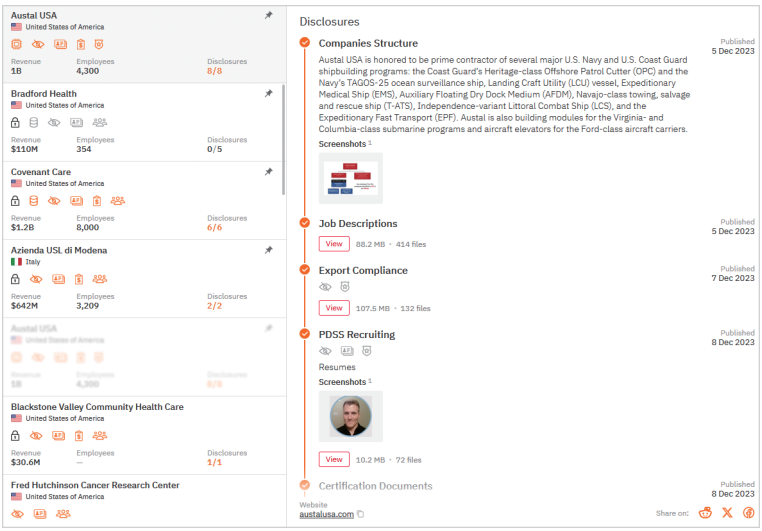
由于每月黑客组织行动数量庞大，无法在报告中枚举全部事件，分析员随机抽取展示 10 个典型样例事件，并对其中部分代表性事件进行细节说明：

事件	国家/组织	时间	黑客组织
Austal USA	美国奥斯塔	2023/12/5	HUNTERS INTERNATIONAL
HTC Global Services	美国 HTC 全球服务	2023/12/1	Alphv
Tipalti	蒂帕尔蒂	2023/12/3	Alphv
Prefeitura Municipal de Itabira	巴西伊塔比拉市政府	2023/12/24	Alphv
Abdali Hospital	阿卜杜勒医院	2023/12/26	Rhysida
Insomniac Games	美国失眠游戏	2023/12/12	Rhysida
Hacked IDF SMS system	以色列国防军短信系统	2023/12/24	Malek team
kitahirosima.jp	日本北广岛町社会福利协议会	2023/12/12	Lockbit3
goldwind.com	金**科技	2023/12/14	Lockbit3
dena.de	德国能源署	2023/12/12	Lockbit3

（1）美国海军承包商奥斯塔

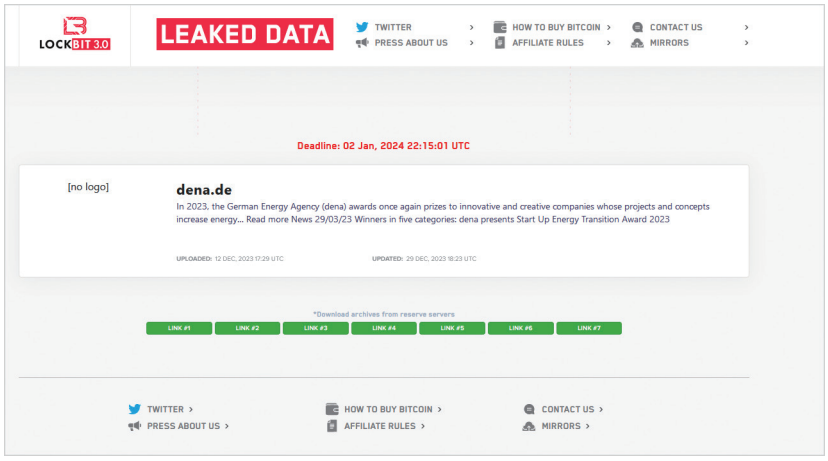
商业黑客组织 HUNTERS INTERNATIONAL 在 2023.12.5 公布了美国海军承包商奥斯塔被勒索的信息，该部门未按照勒索组织的要求在规定期限内支付赎金。HUNTERS INTERNATIONAL 共窃取了奥斯塔多达 13.2GB 的数据，超 5600 份文件，

并公布在互联网上提供下载。如下图所示：



（2）德国能源署

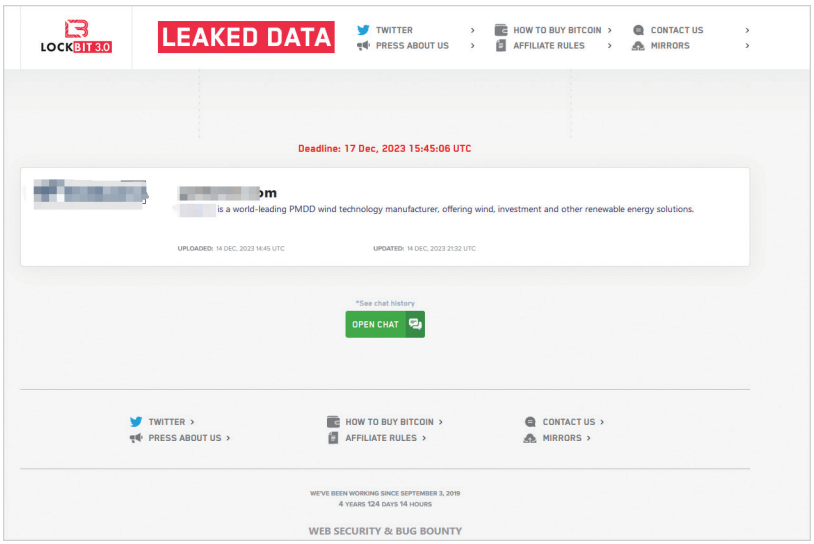
商业黑客组织 Lockbit 在 2023.12.12 公布了德国能源署被勒索的信息，该部门未按照勒索组织的要求在规定期限内支付赎金。Lockbit 共窃取了德国能源署多达 265.5GB 的数据，并公布在互联网上提供下载。如下图所示：



（3）金 ** 科技

商业黑客组织 Lockbit 在 2023.12.14 公布了金 ** 科技被勒索的信息，该部门未按照勒索组织的要求在规定期限内支付赎金，但 Lockbit 并未上传金 ** 科技的数据到官网上，同时在其官网上晒出了其与金 ** 科技人员聊天记录。

聊天记录显示：从 2023 年 12 月 2 日起，金 ** 科技一直试图和 lockbit 进行谈判来压低价格，但截止到 2024 年 1 月 3 日，lockbit 始终未接受减少赎金。如下图所示：



■ **对该类事件，本文分析员的观点和立场如下：**

(1) 坚决支持对勒索软件和黑客组织说“NO！”

(2) 企业 CISO 仍应加强自身安全建设，防止该类事件带来的损失；

(3) **访问 https://0.zone/DwmTab 获得全部勒索事件监控**

4、典型黑客组织简介（Alphv）

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

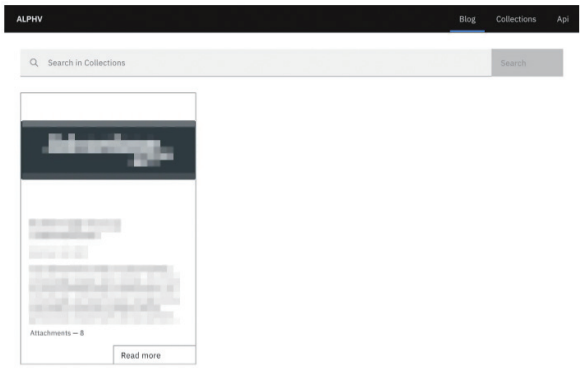
业人员对勒索软件和黑客组织的认知度。

已经介绍过的黑客组织有：Lockbit3，Royal，Play，Rhysida 如需了解请翻阅往期报告。

本期介绍 Alphv 勒索组织。Alphv（黑猫）黑客组织最早于 2021 年 11 月开始活跃，是一个存活时间很久的勒索组织。Alphv 黑客组织（也称为黑猫）被确认其前身是臭名昭著的 BlackMatter/DarkSide 黑客组织：DarkSide 于 2020 年 8 月开始活跃，由于攻击了美国最大的燃料运输管道遭执法部门关注，在 2021 年 5 月被关闭；随后于 2021 年 7 月以 BlackMatter 的身份回归，4 个月后由于被利用服务器漏洞导致服务器被查封；最后该组织更名为 Alphv。

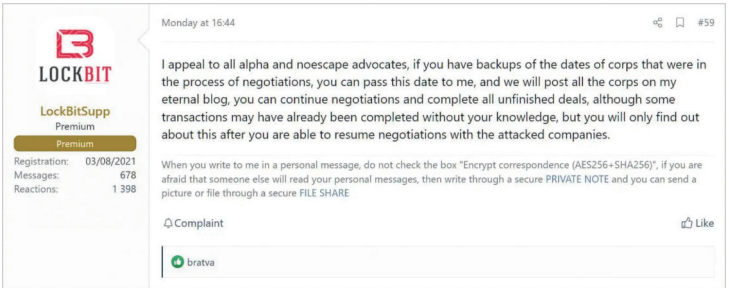
Alphv 勒索组织效率极高，可以算得上是一个顶尖勒索组织。截止 2023 年底共发布了 712 起勒索公告，平均每月就有 20 多个受害者遭受 Alphv 勒索组织攻击勒索。Alphv 的勒索金额大约从 250 万美元至 1000 万美元不等，并且他们并不在勒索留言中注明金额，而是要求受害者与他们进行联系和互动，以获取勒索金额。

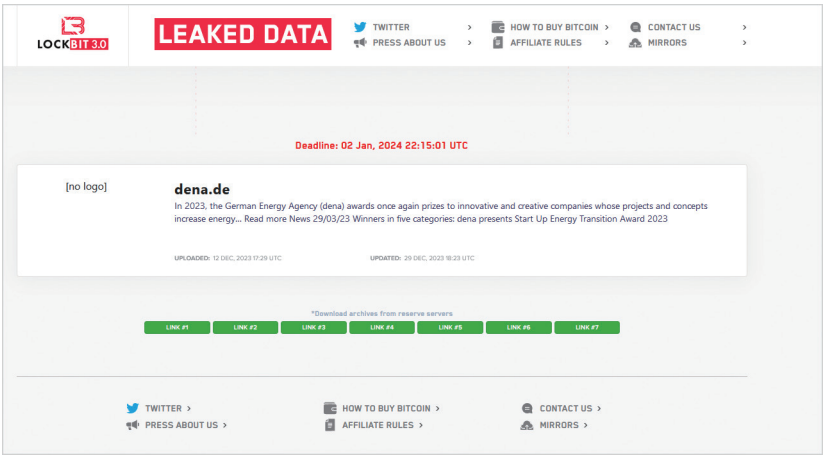
12 月 7 日，Alphv 官网突然无法打开，同时其谈判链接也无法打开，表明了该组织的公共基础设施出现故障，正在进行的谈判也已停止。12 月 12 日在其基础设施瘫痪的第五天后似乎又重新开始营业。但它只显示了一名受害者，而没有看到它通常列出的数百名其他受害者中的任何一个。该网站上唯一的列表日期为 12 月 13 日，即网站恢复后。ALPHV 管理员将问题归咎于托管问题，与此同时有消息称“本次基础设施瘫痪是被执法部门行动导致”。



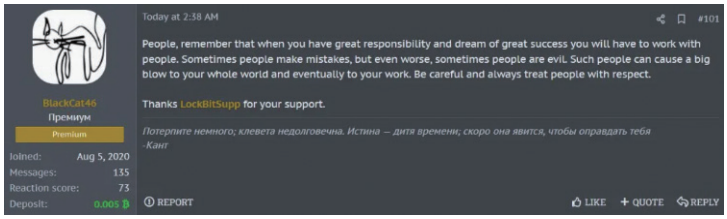
12 月 19 日，AlphV/Blackcat 勒索软件团伙的暗网网站被一个醒目的页面取代，宣布该网站已被 FBI 查获。FBI 称在获得该组织服务器的访问权限后，进行了长达数月的监视，同时没收了解密密钥，从而恢复了约 500 名勒索软件受害者的数据，避免了总计约 6800 万美元的赎金支付。但几小时后，该团伙声称已“夺回该站点”，同时还取消了攻击此前他们禁止攻击关键基础设施的目标规则。

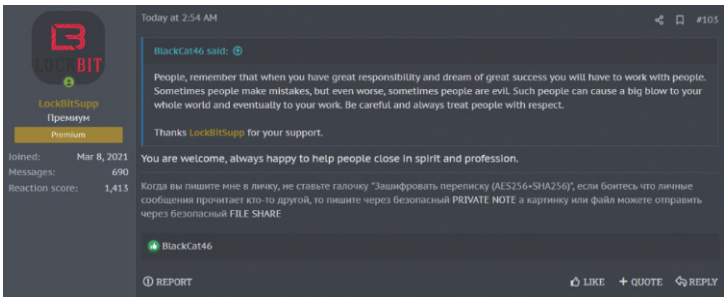
ALPHV 的服务器中断后，该组织中合作伙伴的信任度下降，其中一些人开始绕过该组织在 Tor 网络上的平台，通过电子邮件直接联系受害者。这是由于担心 ALPHV 的基础设施可能已受到损害。值得注意的是，LockBit 勒索组织将这种情况视为扩大其活动的机会，并邀请 ALPHV 附属机构加入，并视此次事件为“圣诞礼物”。虽然尚不清楚 ALPHV 附属机构是否已转移到 LockBit，但已在 LockBit 的数据泄露网站上发现了一名 ALPHV 的受害者（德国能源署 http://dena.de）。

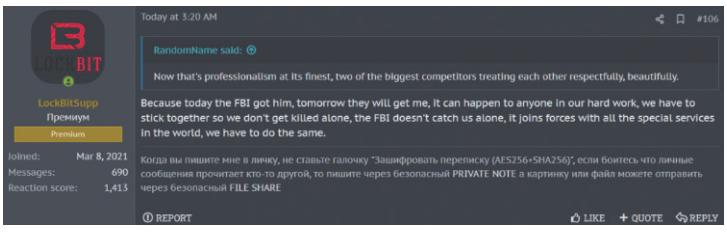


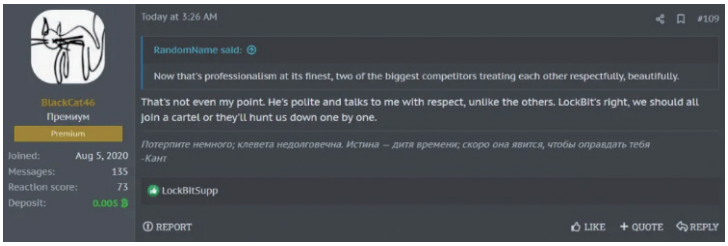


与此同时，Lockbit 和 ALPHV 在暗网上还谈及到要成立一个“黑客组织联盟”。ALPHV 在暗网上通过一条神秘的消息发起了对话，强调黑客在逆境面前需要团结一致。该消息包含对最近发生的事件的隐晦提及，以及感激 LockBitSupp 的支持。LockBit 则对此表示感谢，并表示愿意支持志同道合的伙伴。并提到“我们应该成立一个联盟”。令人惊讶的是，ALPHV 对此回应到“LockBit 是对的，我们都应该加入联盟，否则他们会一一追捕我们。”







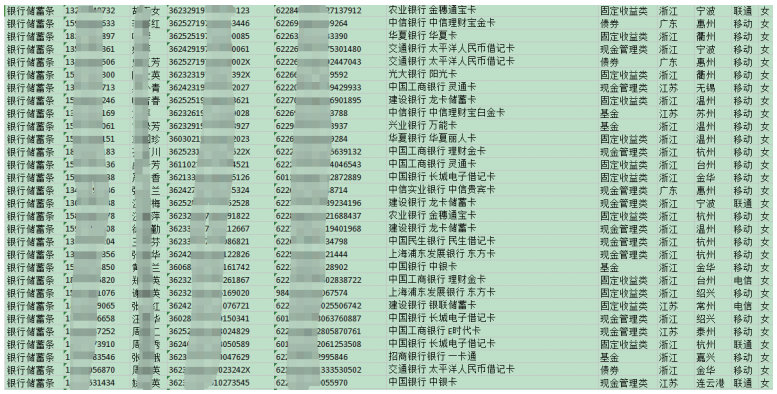


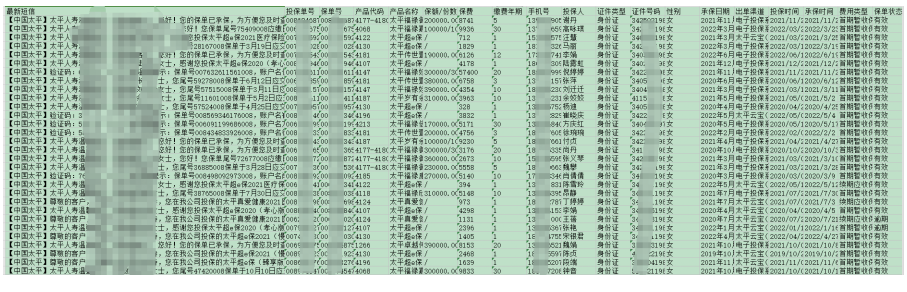
鉴于LockBit和BlackCat臭名昭著的历史,两者之间的合作尤其令人震惊。这两个组织都卷入了重大网络攻击，他们的联盟可能会扩大他们未来行动的规模和影响。如果此联盟成立，那么无疑是对全球网络安全工作的一个重大挑战。

第四章　匿名社交社群

12 月份监控到匿名社交社群情报总数量 8,031,411 条，提供的有效数据泄露样例下载 509,093 份。涉及到我国数据泄露的内容，包括：电销、股票、贷款、相亲、机票信息、公积金、购房信息、社保信息、医生和护士信息、教师和学生信息、网购等众多类型。

以下随机选取展示部分样本：





以上数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 12 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 640 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 12 月份使用“86”开头的手机号的 TOP 10 信息：

8615677674945	27
8617198210874	25
8613751106159	24
8616259234781	22
8618308313145	20
8617369271303	19
8618485688662	18
8618426200921	14
8617837223323	13
8613922942308	10

* 如果您对《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）是国内数字产业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，撰写发布过《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》、《中国数字安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、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 余家有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，投融资对接，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：北京市东城区鲜鱼口街 90-2 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