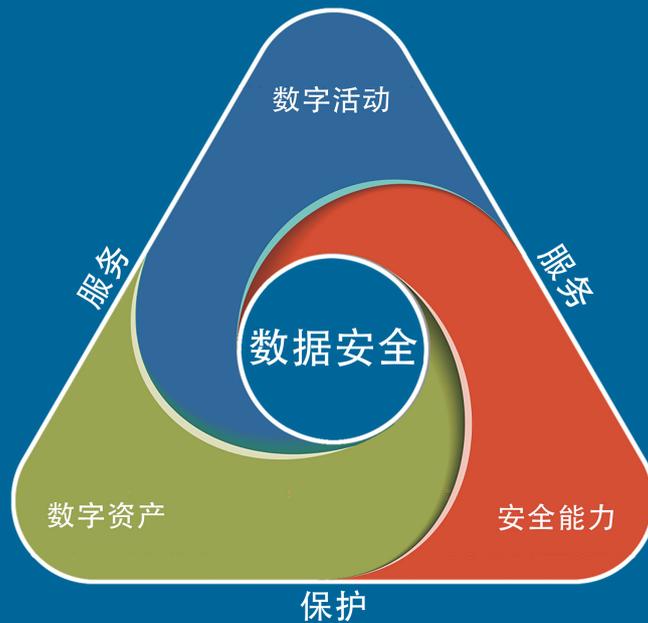






# 数据泄露态势月度报告

(2023年12月)



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、网安企业等合作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

本报告版权属于北京数字世界咨询有限公司。  
任何转载、摘编或利用其他方式使用本报告文字或者观点，应注明来源。  
违反上述声明者，数世咨询将保留依法追究其相关责任的权利。

# 目 录

第一章 数据泄露市场 .....	2
1、国家分类 .....	2
2、行业分类 .....	3
3、泄露数量 .....	3
第二章 事件抽样分析 .....	4
1、美国国防部高级研究计划局数据泄露 .....	4
2、爱达荷国家实验室数据泄露 .....	6
3、美国政府合同数据泄露 .....	7
4、孟加拉国议会数据泄露 .....	7
5、北卡罗来纳州亨德森维尔市政府雇员数据泄露 .....	8
6、* 拼 * 购物数据泄露 .....	8
7、** 云和 ** 宝数据泄露 .....	9
8、** 手两亿订单数据泄露 .....	10
9、湖北 ** 工 *** 行数据泄露 .....	10
10、** 信绑定数据泄露 .....	11

# 目 录

第三章 勒索软件和黑客组织.....	13
1、活跃商业黑客组织综述 .....	13
2、黑客组织活跃趋势 .....	14
3、本月典型事件说明 .....	15
(1) 中 ** 工程有限公司 .....	16
(2) 佛罗里达州退伍军人事务部 .....	16
(3) 大英图书馆 .....	17
4、典型黑客组织简介 (Rhysida) .....	17
第四章 匿名社交社群 .....	20

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。

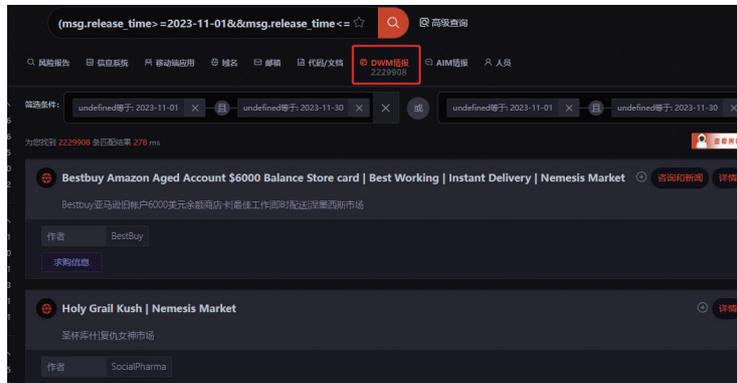
为了掌握数据泄露态势，应对日益复杂的安全风险，数世咨询联合零零信安，基于 0. zone 安全开源情报系统，共同发布《数据泄露态势》月度报告。该系统监控范围包括明网、深网、暗网、匿名社群等约 10 万个威胁源。除了月度的数据泄露概况以外，报告还会针对一些典型的数据泄露事件进行抽样事件分析。如果发现影响较大的数据伪造事件，还会对其进行分析和辟谣。

本期报告的统计区间 2023 年 11 月。

# 第一章 数据泄露市场

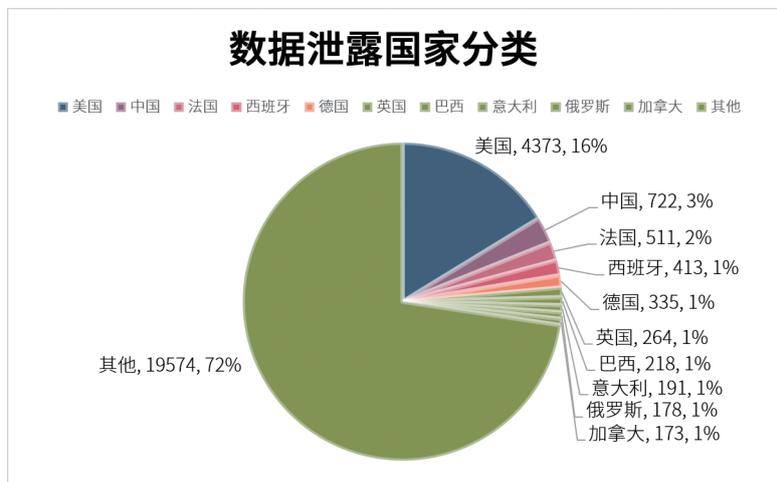
2023 年 11 月共监控到全球 DWM（Dark Web Market）情报：

- 深网和暗网有效情报 2,229,908 份；
- 泄露数据的买卖情报 26,952 份。



## 1、国家分类

其中美国是数据泄露第一大国，共泄露数据 4,373 份，其他数据泄露较多的国家还包括：中国、法国、西班牙、德国、英国、巴西等。详情如下图所示：

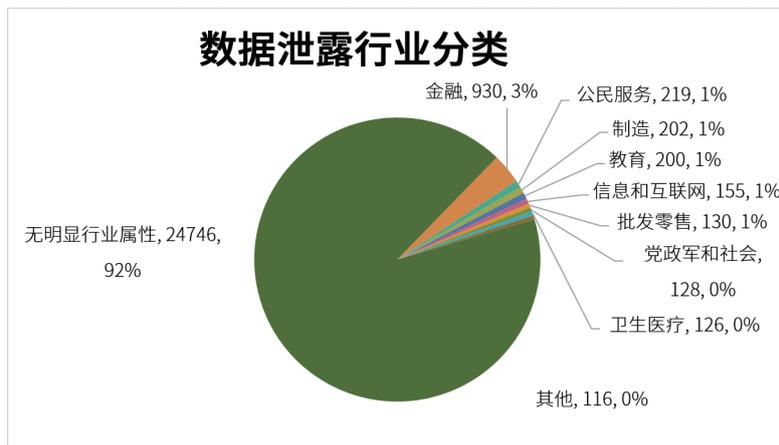


在“其他”数据中包含其他国家以及无法准确进行国家分类的数据泄露事件，例如二要素数据（账号：密码 / 邮箱：密码）、LOG 记录等。

## 2、行业分类

11 月份行业属性数据占泄露数据总量约 8% 左右，泄露的行业数据主要包括金融行业、公民服务行业、制造业、教育业、信息和互联网行业等。92% 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

11 月份泄露的数据中包含一份据称 145 亿条购物数据，数份超十亿的二要素个人数据泄露，因此除上述购物数据外，全球整体数据泄露量达到两百亿行以上。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一百亿行以上。

## 第二章 事件抽样分析

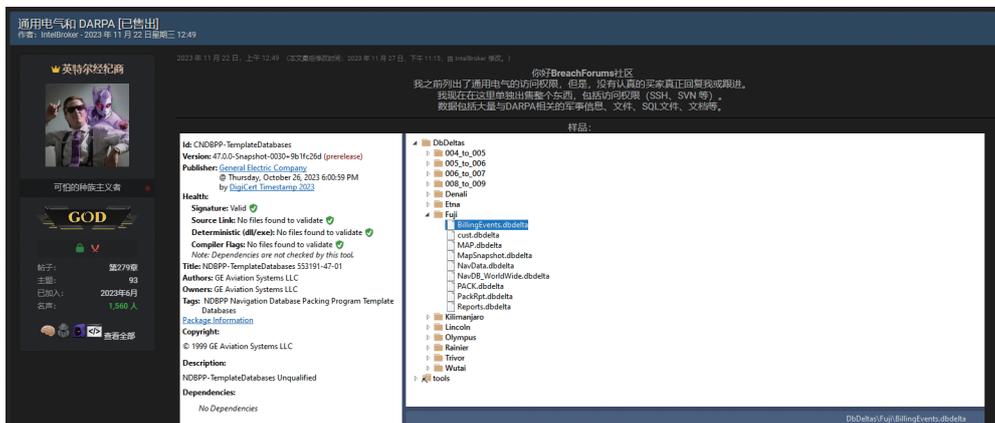
### 1、美国国防部高级研究计划局数据泄露

发布时间：2023.11.22

泄露数量：未知

售卖 / 发布人：IntelBroker

**事件描述：**2023.11.22 某暗网数据交易平台有人宣称正在售卖一份大量与 DARPA（美国国防部高级研究计划局）相关的军事信息。本月早些时候，该黑客试图在黑客论坛上以 500 美元的价格出售通用电气“开发和软件管道”的访问权限。在没有出售成功所谓的访问权限后，威胁行为者再次发帖称，他们现在正在出售网络访问权限和据称被盗的数据。“我之前列出了对通用电气的访问，但是，没有认真的买家真正回复我或跟进。我现在在这里单独出售整个东西，包括访问权限（SSH、SVN 等），”威胁行为者在黑客论坛上发帖说。“数据包括大量与 DARPA 相关的军事信息、文件、SQL 文件、文档等。”作为泄露的证据，威胁行为者分享了他们声称被盗的 GE 数据的屏幕截图，其中包括 GE Aviations 的一个数据库，该数据库似乎包含有关军事项目的信息。截止本篇报告发出时，该黑客成功售出了这个数据。



**Id:** DataServiceConsoleMethods  
**Version:** 1.0.0-Snapshot-0004+922aa64 (prerelease)  
**Publisher:** [General Electric Company](#)  
 @ Friday, September 15, 2023 1:35:42 PM  
 by [DigiCert Timestamp 2023](#)

**Health:**  
**Signature:** Valid ✓  
**Source Link:** Missing Symbols ✖  
**Deterministic (dll/exe):** Non deterministic ✖  
**Compiler Flags:** Missing ✖  
*Note: Dependencies are not checked by this tool.*

**Title:** Data Services Console Methods  
**Authors:** GE Aviation Systems LLC  
**Tags:** Console Methods  
[Package Information](#)

**Copyright:**  
 © 2023 GE Aviation Systems LLC

**Description:**  
 Data Services Console Methods Unqualified

**Dependencies:**  
 .NETCoreApp,Version=v6.0  
 No Dependencies



VDDswpartnumber
Rev #
releasedate

Version Description Document  
 for the  
 identifier

Prepared by:	GE Aviation Systems LLC 3290 Patterson Avenue SE, Grand Rapids, MI, 49512-1934, USA
--------------	--

<p><b>GE Aviation Systems LLC Proprietary Information</b></p> <p>The information contained in this document is GE Aviation Systems LLC proprietary information and is disclosed in confidence. It is the property of GE Aviation Systems LLC and shall not be used, disclosed to others or reproduced without the express written consent of GE Aviation Systems LLC, including, but without limitation, it is not to be used in the creation, manufacture, development, or derivation of any repairs, modifications, spare parts, designs, or configuration changes or to obtain FAA or any other government or regulatory approval to do so. If consent is given for reproduction in whole or in part, this notice and the notice set forth on each page of this document shall appear in any such reproduction in whole or in part.</p> <p>Export Controlled Technical Data</p> <p>This technical data is considered subject to the Export Administration Regulations (EAR) pursuant to 15 CFR Parts 730-774. Transfer of this data by any means to a Non-U.S. Person, whether in the United States or abroad, without the proper U.S. Government authorization (e.g., License, exemption, NLR, etc.), is strictly prohibited.</p> <p>This technical data is designated EAR99 under the EAR; No License Required (NLR).</p>
--

© copyrightdate GE Aviation Systems LLC, USA

GE Designated: CONFIDENTIAL – authorized distribution only

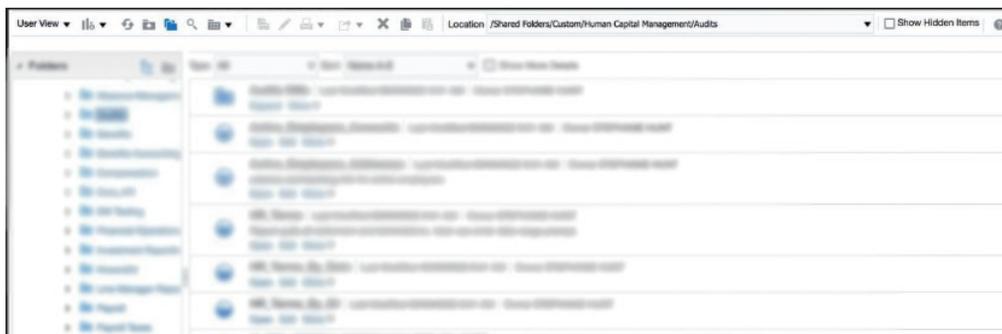
## 2、爱达荷国家实验室数据泄露

发布时间：2023. 11. 20

泄露数量：100,000

售卖 / 发布人：SiegedSec

**事件描述：**2023. 11. 20 某暗网数据交易平台有人宣称正在售卖一份爱达荷国家实验室（美国核试验研究所 inl.gov）数据。目前，INL 正致力于下一代核电站、轻水反应堆、控制系统网络安全、先进车辆测试、生物能源、机器人、核废料处理等方面的研究。正如该组织（SiegedSec）之前针对 NATO 和 Atlassian 的违规行为一样，他们在黑客论坛和该组织运营的 Telegram 频道上公开泄露被盗数据，不顾与受害者谈判或索要赎金。在 Telegram 上，SiegedSec 还通过分享 INL 内部用于文档访问和公告创建的工具的屏幕截图来发布所谓的违规证据。攻击者还展示了在 INL 系统上创建了自定义公告，以便让综合体中的每个人都知道此次违规行为。



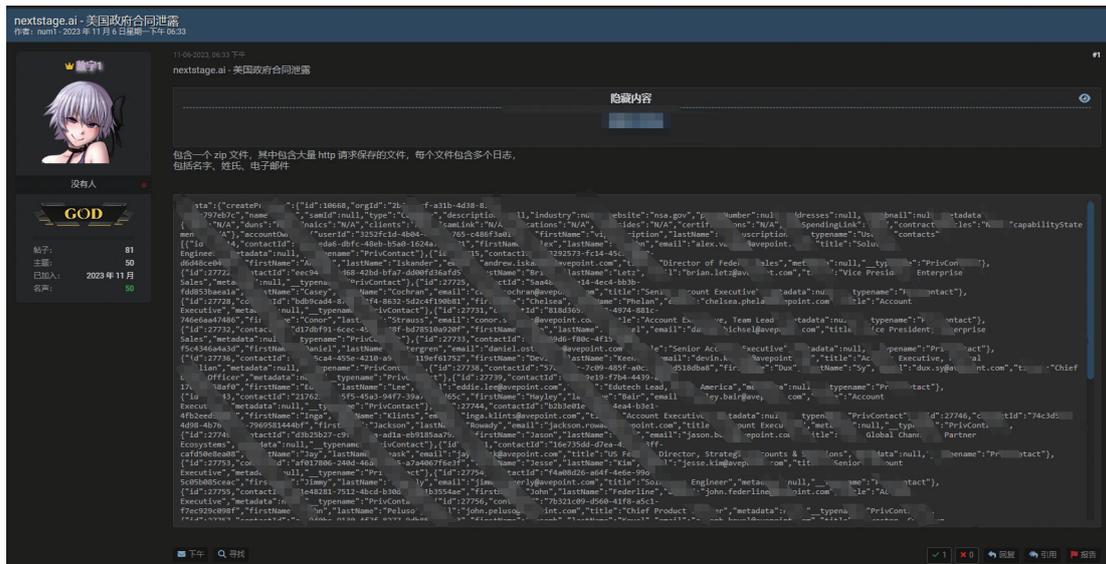
### 3、美国政府合同数据泄露

发布时间：2023. 11. 6

泄露数量：未知

售卖 / 发布人：num1

**事件描述：**2023. 11. 6 某暗网数据交易平台有人宣称正在售卖一份 nextstage.ai 网站数据，该网站是一个与政府为政府承包商构建的客户管理系统。该售卖人声称窃取到的数据包含一个 zip 文件，其中包含大量 http 请求保存的文件，每个文件包含多个日志，包括名字、姓氏、电子邮件等。



### 4、孟加拉国议会数据泄露

发布时间：2023. 11. 28

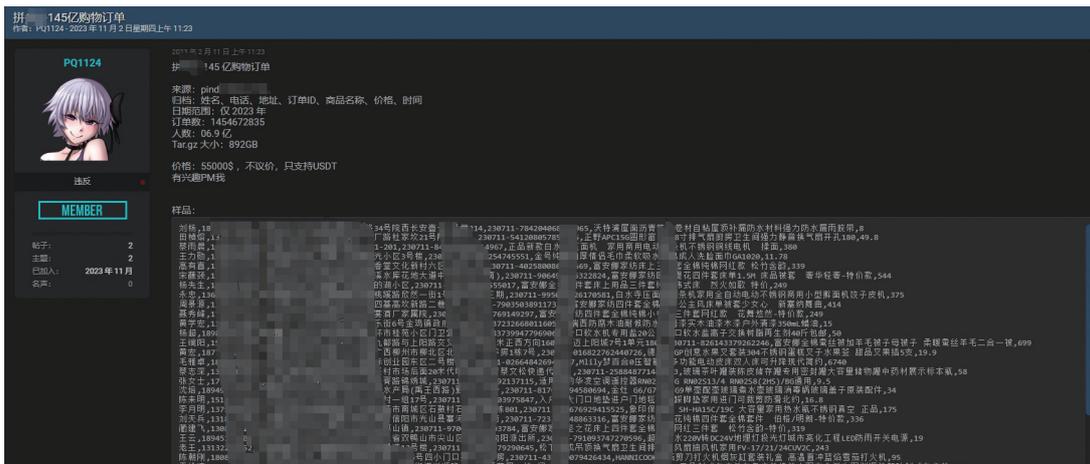
泄露数量：未知

售卖 / 发布人：ZinPin

**事件描述：**2023. 11. 28 某暗网数据交易平台有人宣称正在售卖一份孟加拉国议会网站访问权限和数据。该作者上传了两张关于权限的截图，标价 1000 美元并留下了自己的 telegram 联系方式。



价格、下单时间，总大小为 892GB，标价为 55000 美元。根据经验以及研究发现，该玩家为刚注册的新账号且支付方式单一：只支持 USDT 支付和站内联系他，并且该用户上线了之后并没有很积极的回复论坛下的问题，登录也是几天登录一次，这些行为并不符合一个想出售数据的暗网玩家。由零零信安安全分析师根据样本、价格、售卖习惯、黑客信誉、暗网玩家特性等综合分析，该数据售卖行为判断为诈骗的可能性极高。



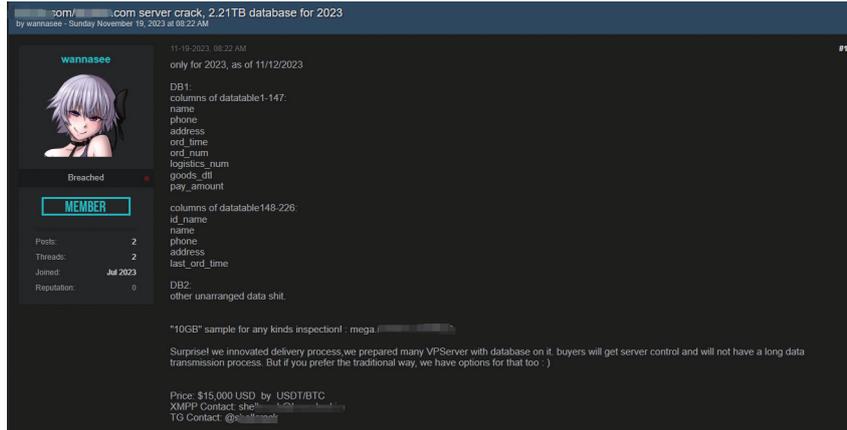
## 7、\*\* 云和 \*\* 宝数据泄露

发布时间：2023. 11. 19

泄露数量：未知

售卖 / 发布人：wannasee

**事件描述：**2023. 11. 19 某暗网数据交易平台有人宣称正在售卖一份 \*\* 云和 \* 宝数据，数据字段有：名称，电话，住址，订单时间，订单编号等，总大小为 2.21TB，售卖价格为 15000 美元，卖家还附上了一个 10GB 样例的链接并留下了 XMPP 和 tg 联系方式。



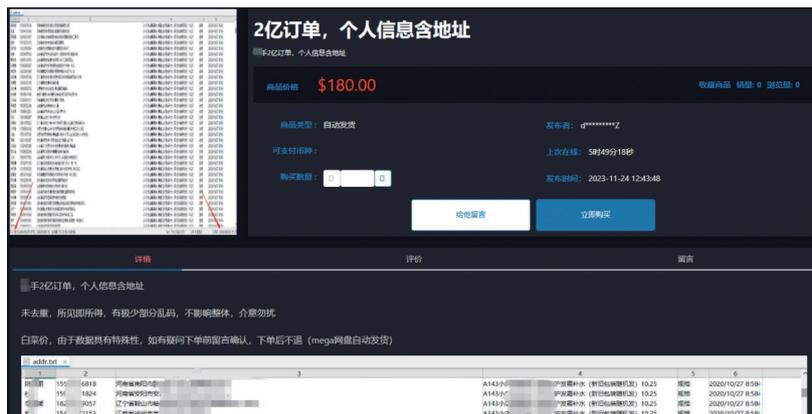
## 8、\*\* 手两亿订单数据泄露

发布时间：2023. 11. 24

泄露数量：200000000

售卖 / 发布人：d\*\*\*\*\*Z

**事件描述：**2023. 11. 24 某暗网数据交易平台有人宣称正在售卖一份 \*\* 手 2 亿订单数据，卖家附上了一张样例，数据字段有：姓名，电话，地址，购买商品名称等，售卖价格为 180 美元。



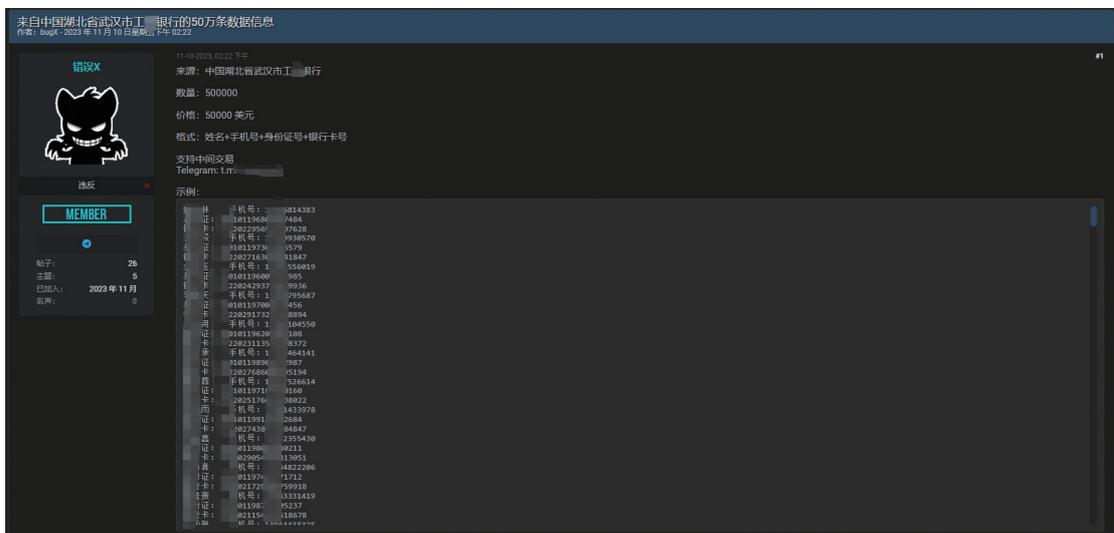
## 9、湖北 \*\* 工 \*\*\* 行数据泄露

发布时间：2023. 11. 10

泄露数量：500000

售卖 / 发布人: bugX

**事件描述:** 2023. 11. 10 某暗网数据交易平台有人宣称正在售卖一份湖北省武汉工\*\*银行客户数据, 总数量为 50 万条, 数据字段有: 姓名, 电话, 身份证号, 银行卡号, 价格为 50000 美元并附上了中间交易人联系方式和数据样例。两天后该卖家又在论坛下方评论道“价格错误, 5000 美元是正确的价格”, 目前数据的真假性未知, 但综合判断, 该数据售卖行为判断为诈骗的可能性极高。



## 10、\*\* 信绑定数据泄露

发布时间: 2023. 11. 8

泄露数量: 49000000

售卖 / 发布人: 1894761

**事件描述:** 2023. 11. 8 某暗网数据交易平台有人宣称正在售卖一份\*\*信绑定数据, 总数量为 4900 万条, 价格为 188 美元, 卖家附上的样例中数据字段有: 姓名, 手机号, 身份证号等。

交易编号	53720	商品单价	188 (美元)	商品交易状态	正常	上架日期	2023-11-08	加入收藏
卖家编号	1894761	单价折算	0.00531 (比特币)	本单累计成交	0	卖家状态	刚刚在线	公开留言
关注数	63	咨询热度		卖家累计在线	27小时	风险对比	8 : 0	(好评值; 风险值, 仅供参考, 单个买家指出的风险并非绝对风险)

商品购买资金宝(支付宝)  
需要核对您的交易密码

ID	买家	购买数量	成交金额	付款时间	最后付款次数	交易担保期截止	资金结算期	状态	打开
----	----	------	------	------	--------	---------	-------	----	----

商品描述  
数据详情请看图, 感兴趣的来, 便道出了, 数据来源等 广告

mega网盘发货

附件:

155	7101	刘	532	0301	13	2022-02-14 19:34:04	WxMP	124
1780	776	侯龙	530	0510	14	2022-03-08 20:16:56	WxMP	377
1500	719	杜	341	09112	14	2022-02-14 19:38:25	WxMP	211
1800	058	倪日	320	09805	37X	2022-02-14 19:43:24	WxMP	151
1536	025	蔡	441	09740	560	2022-02-14 19:44:00	WxMP	596
1773	511	陈	140	09991	036	2022-02-14 19:45:31	WxMP	422
1806	788	任	320	09780	412	2022-02-14 19:48:05	WxMP	527
1320	445	杜	620	0972	01X	2022-02-14 19:48:13	WxMP	486
136	419	占	340	0976	016	2022-02-14 19:59:51	WxMP	203
178	0061	华	440	0981	0353	2022-02-14 20:05:34	WxMP	745
130	3804	林	52	2003	0017	2022-02-14 20:12:43	WxMP	313
199	5143	谷	43	0197	30083	2022-02-14 20:21:09	Android	
157	7668	李	23	02197	26119	2022-02-14 19:24:16	WxMP	234
150	5367	李	34	2200	173870	2022-02-14 19:25:38	WxMP	404
18	17393	阮	41	6199	1184011	2022-02-14 19:26:09	WxMP	650

## 第三章 勒索软件和黑客组织

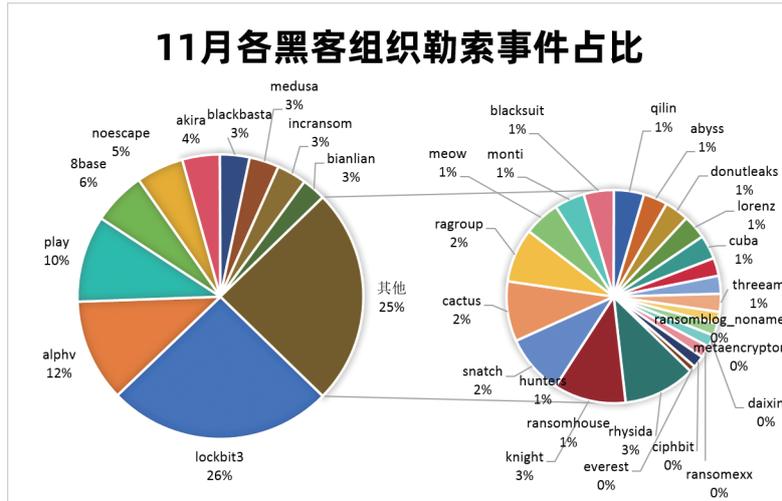
### 1、活跃商业黑客组织综述

2023 年 11 月全球活跃的商业黑客组织（有勒索发布行为）共 32 个，公开的勒索事件共 447 件，TOP 10 的黑客组织如下所示：

组织标识	组织名称	发布数量
 lockbit3	lockbit3	114
ALPHV	alphv	52
PLAY	play	44
 8base	8base	27
 noescape	noescape	24
 Akira	Akira	19
 Black basta	Black basta	15
 medusa	medusa	15
INC RANSOM	Inc ransom	15
 bianlian	bianlian	12

—来自2023年11月《数据泄露态势》

TOP 10 的商业黑客组织公开发布的勒索事件占全部事件的 75%，如下所示：

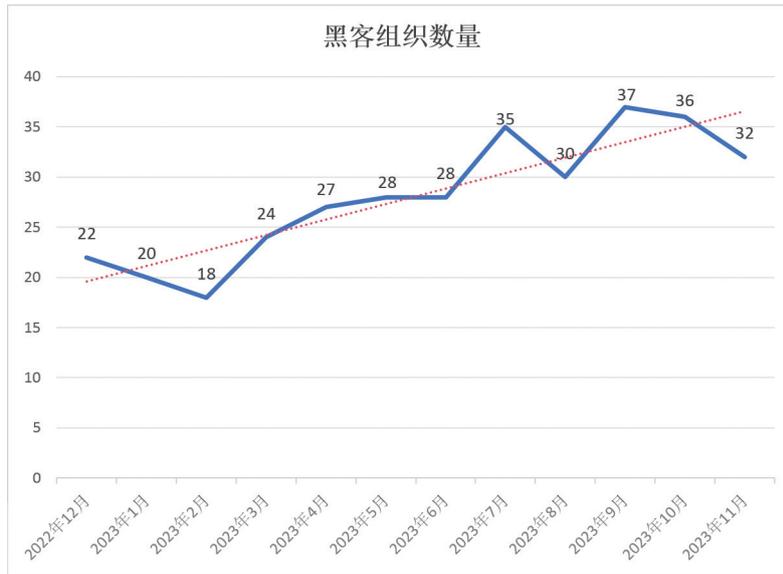


## 2、黑客组织活跃趋势

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（本月与上月相比少量增加），但整体活跃度趋势正在逐步增加，统计末端（2023年11月）已达到一年前统计前端（2022年12月）的44.66%：



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较上月有所降低但仍保持高活跃度状态。如下图所示：



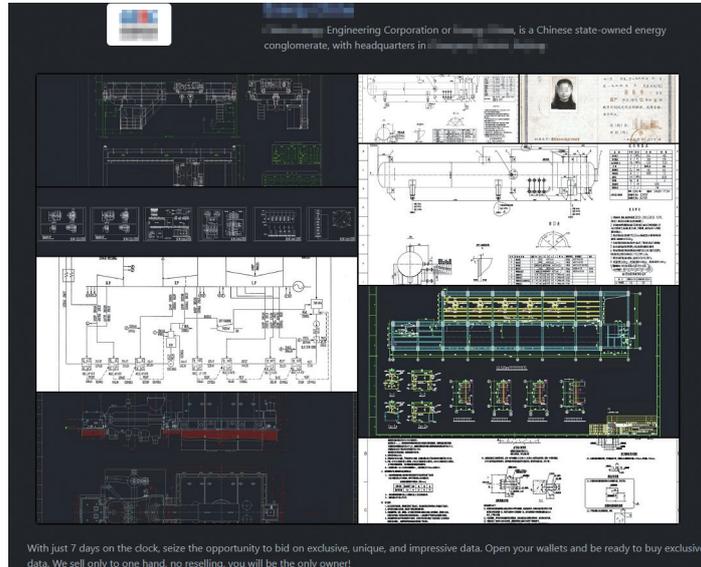
### 3、本月典型事件说明

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
yamaha-motor.com.ph	雅马哈汽车菲律宾公司	2023/11/15	Inc Ransom
Toyota Financial	丰田金融	2023/11/15	Inc Ransom
ICBCFS	工银金融服务有限责任公司	2023/11/8	Lockbit3
Energy China	中国能源工程有限公司	2023/11/24	Rhysida
British library	大英图书馆	2023/11/20	Rhysida
Fidelity National Financial	富达国民金融	2023/11/8	Alphv
Japan Aviation Electronics Industry, Ltd.	日本航空电子工业株式会社	2023/11/7	Alphv
China Petrochemical Development	中国石油化学工业开发股份有限公司 (台湾)	2023/11/28	Alphv
Florida Department of Veterans' Affairs	佛罗里达州退伍军人事务部	2023/11/30	Snatch
nal.res.in	国家航空航天实验室 (印度)	2023/11/28	Lockbit3

## (1) 中\*\*工程有限公司

商业黑客组织 rhapsida 于 2023. 11. 24 公布了中\*\*工程有限公司被勒索的信息，并给了其 7 天时间支付赎金：



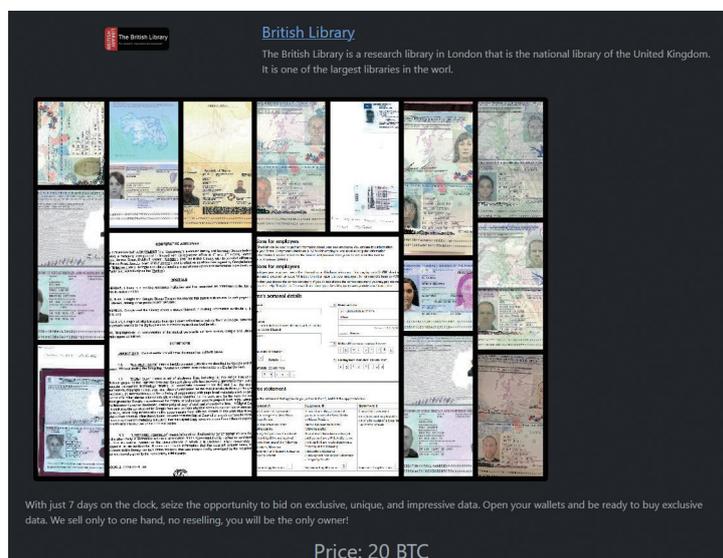
## (2) 佛罗里达州退伍军人事务部

商业黑客组织 snatch 于 2023. 11. 30 公布了佛罗里达州退伍军人事务部被勒索的信息，并给了其 7 天时间支付赎金：



### (3) 大英图书馆

商业黑客组织 rhysida 于 2023. 11. 20 公布了大英图书馆被勒索的信息，并给了其 7 天时间支付赎金：



#### ■ 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) 我们将与某些公益组织合作，为受到勒索和黑客组织攻击的单位提供免费技术支持，该计划预计在近期内上线。

## 4、典型黑客组织简介 (Rhysida)

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 如需了解请翻阅往期报告。

本期介绍 Rhysida 勒索组织，Rhysida（希腊语“卫蜈蚣”）是一家于

2023年5月出现的勒索软件企业，在入侵智利军队（Ejército de Chile）并在网上泄露被盗数据后迅速声名狼藉。Rhysida于2023年下半年6月开始活跃。截止本篇文章发布时已发布66个勒索事件，其中已售卖或发布的事件63个，待售卖或发布的事件3个。其中该组织的攻击目标涵盖11个行业，其中以教育行业、政府、卫生医疗行业为主，占比为67%。

Rhysida黑客组织对于攻击和勒索成功的企业或组织会发布如下声明和留言，并与其进行勒索交涉：



尊敬的XX公司，

这是来自网络安全团队 Rhysida 的自动警报。一个不幸的情况出现了——您的数字生态系统遭到破坏，大量机密数据已从您的网络中泄露。这样做的潜在后果可能是可怕的，包括将您的数据出售、发布或分发给竞争对手或媒体机构。这可能会造成重大的声誉和经济损失。

然而，这种情况并非没有补救措施。

我们的团队开发了一种独特的密钥，专门用于恢复您的数字安全。这把钥匙代表了从这种情况中恢复的第一步，也是最关键的一步。

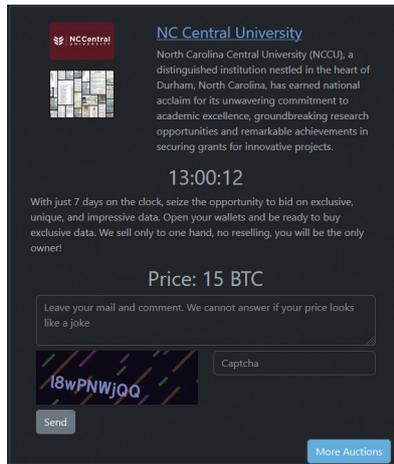
请务必注意，任何单独解密加密文件的尝试都可能导致永久性数据丢失。我们强烈建议不要采取此类行动。

时间是减轻此违规行为影响的关键因素。随着时间的流逝，潜在的损害会不断升级。您需要立即采取行动并充分合作才能有效地驾驭这种情况。

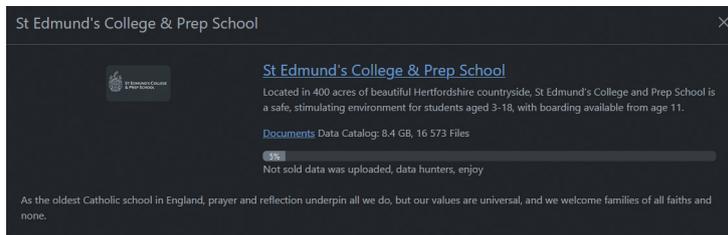
请放心，我们的团队致力于指导您完成此过程。解决问题的旅程始于使用唯一密钥。我们可以共同恢复您的数字环境的安全性。

此致敬礼

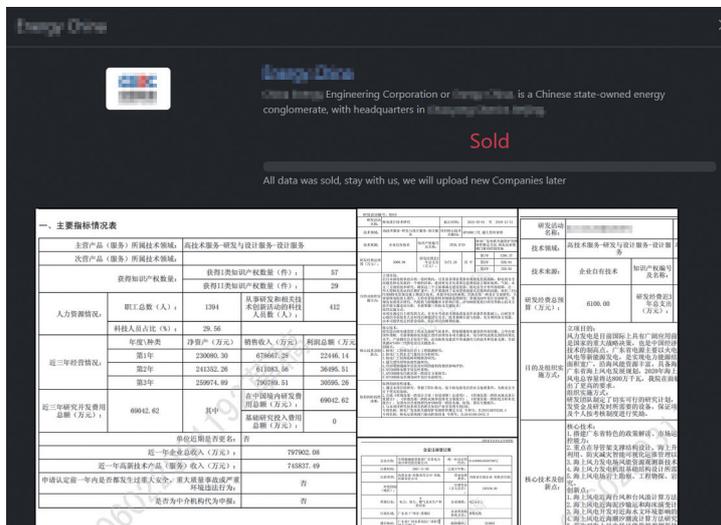
该组织会在其官网上发布一些获取到的数据样例和售价，并提示“在仅有 7 天的时间里，抓住机会竞标独家、独特和令人印象深刻的数据。打开钱包，准备购买独家数据。我们只卖一手，不转售，你将是唯一的拥有者！”以及“留下你的邮箱和评论，如果你的价格太不公道我们不会回复你”：



勒索失败后，该组织会在其官网发布新闻，并在其官方服务器上上传数据，以供访问者免费下载：



勒索成功后，该组织会在官网上泄露进度条上标记“sold”：



## 第四章 匿名社交社群

11月份监控到匿名社交社群情报总数量31,843,483条，提供的有效数据泄露样例下载3002份。涉及我国数据泄露的内容，包括：教育信息、同住人信息、股票信息、贷款信息、公积金、购房信息、社保信息、医生和护士信息、网购等众多类型。

以下随机选取展示部分样本：

地址	发货信息	数量	实付金额	快递单号
黑龙江省大庆市让胡路区南户	工厂电焊挂衣橱衣服裤子架	1,268.0	46.0	050190
内蒙古自治区赤峰市宁城县八	鞋架博曼多需家用经济型防	1,204.0	46.0	7058906
内蒙古自治区保山市隆昌二	工厂电焊挂衣橱衣服裤子架	1,268.0	46.0	7068088
广东省深圳市光明区新田公	88016吸顶灯客厅LED筒灯	1,298.0	46.0	7058871
河北省唐山市开平区河新四小	翰林汇电脑桌家用舒适久坐	1,133.0	46.0	7067437
北京市石景山区翠明庄	工厂电焊挂衣橱衣服裤子架	1,268.0	46.0	7058227
辽宁省沈阳市浑南区白塔街	花草置物架阳台铁艺落地式	1,730.0	46.0	7054623
内蒙古自治区赤峰市松山区	现代简约真皮沙发客厅组合	1,588.0	46.0	7066848
山西省晋中市榆次区西韩村	工厂电焊挂衣橱衣服裤子架	1,268.0	46.0	7055010
河北省唐山市古冶区西新街	【AKI】庭院灯射灯射灯	1,29.9	46.0	7067164
山西省太原市古交市清城	意司可家用家用衣服裤子架	1,26.9	46.0	7067009
山东省临沂市沂水县安山镇	向米小户型阳台干鞋架挂布	1,108.0	46.0	053816
山东省临沂市沂水县富国街	全钢脚踏车脚踏车脚踏车	1,108.0	46.0	056095
辽宁省沈阳市沈河区新城市	全麦燕麦麸皮沙茶杂粮煎饼	1,2759.0	46.0	965998
内蒙古自治区通辽市科尔沁	爆款第一排化太阳能路灯	1,88.0	46.0	156308
河北省唐山市滦南县滦州天	新款太阳能户外LED路灯	1,49.9	46.0	66393
河北省廊坊市广阳区银河北	【智能语音台灯】儿童护眼	1,86.0	46.0	77688
山西省临汾市翼城县康兴镇	【福利】新到联系客服补发	1,19.99	46.0	36655
河北省邢台市清河县流湖小	广东中山灯具大五金全铝	1,178.8	46.0	1579
河北省邢台市清河县流湖小	花架子家用落地式置物架	1,148.0	46.0	2044
贵州省遵义市红花岗区新	客厅落地式茶几电视柜组合	1,29.9	46.0	2268
河南省商丘市梁园区平安街	木马鞋柜家用门口鞋架	1,59.0	46.0	6912
上海市松江江区方松街道	【可循环降解】黄香茅	1,36.8	46.0	2762
河北省保定市徐水区安肃镇	室内铁艺置物架	1,19.99	46.0	1004
江苏省徐州市云龙区子房街	木马鞋柜家用门口鞋架	1,59.0	46.0	3351
福建省福州市晋安区新店镇	【福利】LED吸顶灯圆形	1,49.9	46.0	7712
河北省衡水市阜城县河北省	太阳能射灯	1,29.89	46.0	3669
山东省烟台市龙口市石良镇	VOLLSUN旺成【新款美家	1,34.9	46.0	9884

创建时间	订单编号	收件人	电话	地址	发货信息
2023/11/7 22:59:42	2789251	姜	134 352	河北省唐山市遵化市西二	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	包	151 890	内蒙古自治区通辽市科	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	姜	137 959	山西省朔州市平鲁区山西	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	王	13 955	天津天津市东丽区金钟街	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	陈	15 88	河北省沧州市任丘市西	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	付	13 89	内蒙古自治区呼和浩特市	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	张	13 81	黑龙江省佳木斯市桦南县	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	王	13 09	内蒙古自治区巴彦淖尔市	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	张	13 71	河北省衡水市阜城县阜	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	2789251	张	15 63	内蒙古自治区巴彦淖尔市	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	2789251	李	13 97	吉林省辽源市龙山区区	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	2789251	李	13 82	江苏省常州市武进区薛	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	2789251	曹	13 228	陕西省榆林市神木市神	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	2789251	曹	13 228	辽宁省抚顺市顺城区铁	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	曹	13 279	云南省红河州弥勒市	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	曹	13 856	北京市昌平区回龙观	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	曹	131 1333	内蒙古自治区赤峰市松	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	曹	130 1136	江西省景德镇市珠山区	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	278925	曹	155 1061	山西省运城市平陆县山	【哈哈奇】2023新款 大米米
2023/11/7 22:59:42	27892512	曹	134 0277	湖北省随州市随县随	【哈哈奇】2023新款 大米米

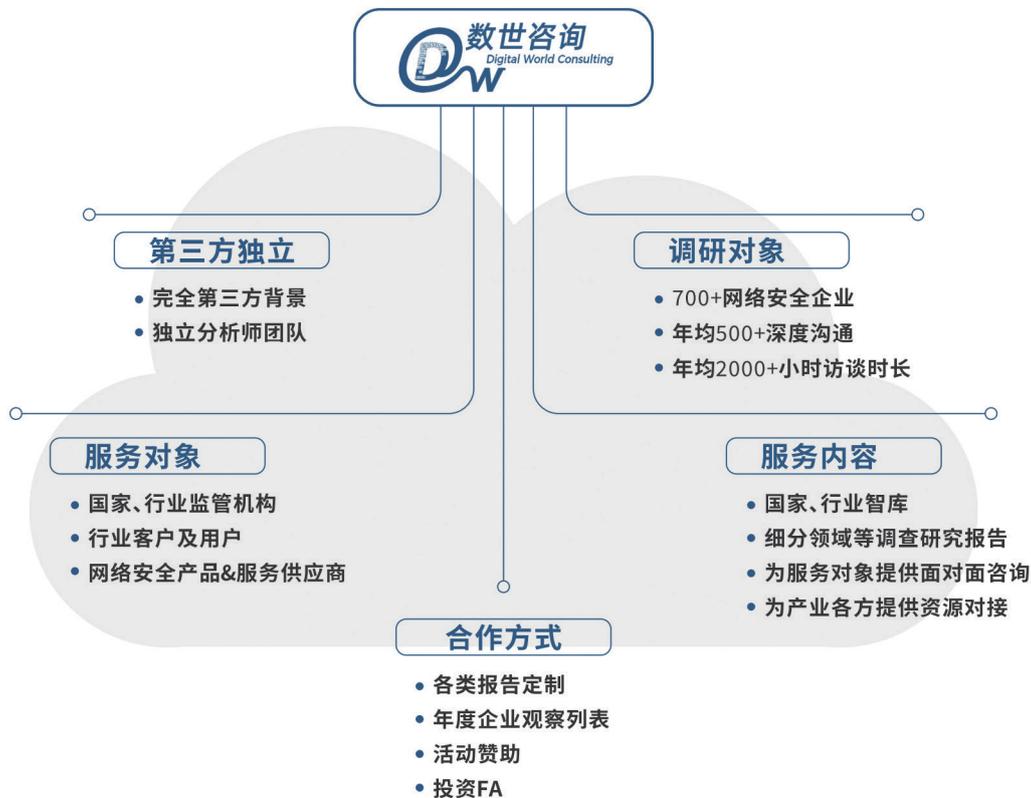
156	63	移动	河北邯郸	女	2.0E+09	27	邯郸	粉丝89	关注8	1.05E+11	MS4wLjA8https://p26.douyinpic.com/ave		
158	26	移动	湖南长沙	女	1.1E+09	31	Ruang	粉丝282	关注358	1.01E+11	MS4wLjA8https://p26.douyinpic.com/avg		
158	940	移动	广东广州	不可知	1.1E+09	26	泸州	粉丝295	关注224	1.08E+11	MS4wLjA8https://p11.douyinpic.com/ave		
18	732	移动	重庆	安	女	xy1	046	26	重庆	粉丝11	关注75	7.18E+10	MS4wLjA8https://p5-ipr6.douyinpic.com
136	930	移动	广东深圳	安	女	841	072	27	邵阳	粉丝255	关注231	6.83E+10	MS4wLjA8https://p29.douyinpic.com/ave
136	1139	移动	甘肃兰州	叶	女	2.1E+09	37	粉丝33	关注110	1.72E+15	MS4wLjA8https://p3.douyinpic.com/aven		
183	458	移动	山东潍坊	仪	女	dyf	90c	27	潍坊	粉丝97	关注187	2.51E+15	MS4wLjA8https://p3.douyinpic.com/aven
159	728	移动	广西南宁	露	女	dyf	at	51	南宁	粉丝87	关注159	3.51E+15	MS4wLjA8https://p6.douyinpic.com/avg
182	410	移动	广西梧州	李	女	1116		54	梧州	粉丝58	关注149	1.06E+11	MS4wLjA8https://p3.douyinpic.com/aven
139	911	移动	湖北武汉	刘	女	1.1E+08	27	武汉	粉丝103	关注128	7.42E+10	MS4wLjA8https://p6.douyinpic.com/aven	
199	255	移动	河南周口	程	女	1.1E+09	27	粉丝180	关注48	1.02E+11	MS4wLjA8https://p26.douyinpic.com/ave		
151	992	移动	湖北黄冈	姚	女	dyf	av	27	黄冈	粉丝51	关注463	2.17E+15	MS4wLjA8https://p3.douyinpic.com/aven
158	964	移动	福建福州	胡	女	8.4E+08	31	福州	粉丝307	关注1151	2.04E+10	MS4wLjA8https://p5-ipr6.douyinpic.com	
1341	753	移动	广东深圳	ca	女	ca	sz1	41	惠州	粉丝93	关注38	9.71E+10	MS4wLjA8https://p26.douyinpic.com/ave
1889	906	移动	湖南长沙	阿	女	dy0	47a	27	岳阳	粉丝159	关注206	4E+15	MS4wLjA8https://p26.douyinpic.com/avg
1390	767	移动	湖南张家界	鱼	女	1.1E+08	43	粉丝495	关注1510	7.51E+10	MS4wLjA8https://p6.douyinpic.com/avg		
1873	191	移动	河南郑州	周	390	女	1.1E+09	32	郑州	粉丝96	关注837	1.01E+11	MS4wLjA8https://p6.douyinpic.com/aven
1547	118	移动	辽宁大连	可	女	dy1	dir1	31	大连	粉丝2	关注16	4.2E+10	MS4wLjA8https://p5-ipr6.douyinpic.com
159	239	移动	河南许昌	薛	女	3.1E+08	37	许昌	粉丝559	关注339	8.5E+10	MS4wLjA8https://p26.douyinpic.com/ave	
136	143	移动	江苏宿迁	潘	女	qit	ngt	27	宿迁	粉丝30	关注513	2.42E+14	MS4wLjA8https://p3.douyinpic.com/aven
15	321	移动	福建龙岩	李	女	4.1E+08	30	undefined	粉丝156	关注489	6.22E+10	MS4wLjA8https://p6.douyinpic.com/aven	
15	552	移动	安徽蚌埠	王	女	2.1E+09	42	蚌埠	粉丝504	关注815	1.11E+11	MS4wLjA8https://p3.douyinpic.com/aven	
16	976	移动	陕西西安	王	女	161	1371	31	西安市	粉丝836	关注984	5.91E+10	MS4wLjA8https://p3.douyinpic.com/aven
15	687	移动	安徽六安	王	女	dy	zdd1	51	六安	粉丝31	关注196	1.54E+15	MS4wLjA8https://p6.douyinpic.com/aven
15	3348	移动	湖北荆州	王	女	1.1E+09	42	长沙	粉丝145	关注193	1.1E+11	MS4wLjA8https://p6.douyinpic.com/aven	
15	8216	移动	广东清远	王	女	2.1E+09	35	清远	粉丝24	关注27	1.05E+11	MS4wLjA8https://p6.douyinpic.com/avg	
18	7606	移动	江西上饶	王	女	1.1E+09	27	上饶	粉丝181	关注130	1.04E+11	MS4wLjA8https://p5-ipr6.douyinpic.com	
15	3743	移动	河南新乡	王	女	56	903	27	粉丝47	关注431	5.15E+10	MS4wLjA8https://p5-ipr6.douyinpic.com	
18	03273	移动	安徽淮北	王	女	1.1E+09	45	淮北	粉丝1156	关注1560	6.73E+10	MS4wLjA8https://p5-ipr6.douyinpic.com	

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，全球数据量估算在 1000 万条以上。

此外，检索到 11 月份使用匿名社交软件的活跃用户中，以“86(我国区号)”开头的手机号共发送信息 2372 个。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 11 月份使用“86”开头的手机号的 TOP 10 信息：

8615075326725	112
8616259234781	104
8619152561632	88
8618905416913	74
8617688038777	38
8618716491091	34
8616630833582	32
8613534395193	31
8613127101954	29
8613360499330	29

\* 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](mailto: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





数字安全领域独立第三方调研机构

