



数据泄露态势月度报告

101010

(2024年9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9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

本报告版权属于北京数字世界咨询有限公司(以下简称数世咨询)。 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

-,		数据泄露市场	2
	1,	国家分类	2
	2,	行业分类	3
	3,	泄露数量	4
Ξ,		事件抽样分析	4
	1,	peopledatalab 数据泄露 12 亿条	4
	2,	俄罗斯机密军事文件数据泄露	5
	3,	俄罗斯核文件数据泄露	9
	4、	美国机密军事计划黑矛计划数据泄露	13
	5,	中情局关于俄罗斯逃避制裁策略的报告数据泄露	15
	6,	旅行团数据泄露	15
	7、	台湾兵役数据泄露	16
	8,	******市政府领导信息数据泄露	17
	9、	台湾就业详情和抵押状态数据泄露	17
	10,	、 38.7万个中国账号数据泄露【老密】	18
Ξ、		勒索软件和黑客组织	19
	1,	活跃商业黑客组织综述	19
	2,	黑客组织活度趋势	21
	3,	本月典型事件说明	23
		(1) 美国法警局	23
		(2) 美国艾肯房屋委员会	24
		(3) 美国住房和城市发展部	25
	4,	本月涉及中国企业的勒索事件说明	26
	5,	典型黑客组织简介(Arcus Media)	27
四.		匿名社交社群	29

《数据泄露态势月度报告》

(2024年9月发布)

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《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 2024 年 8 月。

一、数据泄露市场

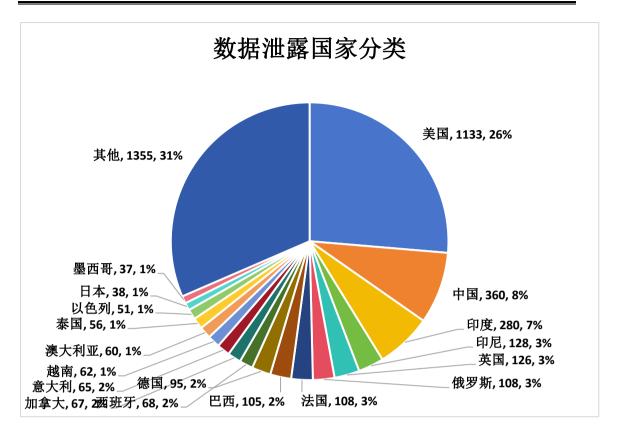
2024年8月共监控到全球 DWM (Dark Web Market) 情报:

- ▶ 深网和暗网有效情报 2,365,643 份;
- ▶ 泄露数据的高价值买卖情报 4,302 份。



1、国家分类

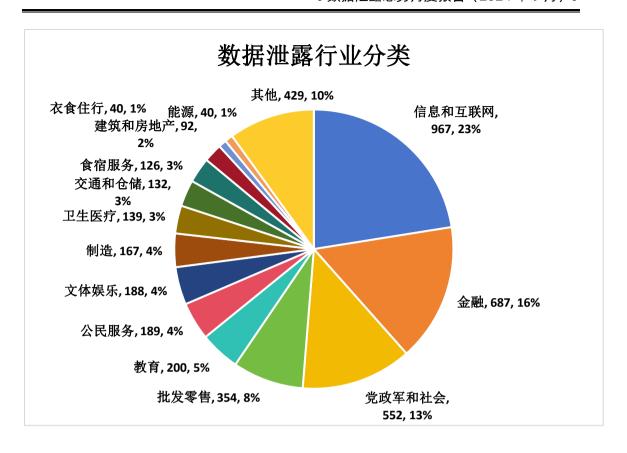
其中美国是数据泄露第一大国,共泄露数据 1133 份,其他数据泄露较多的国家还包括:中国、印度、印尼、英国、俄罗斯、法国、巴西、德国等。详情如下图所示:



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

8 月份行业属性数据占泄露数据总量约 90%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、党政军与社会、批发零售业、教育行业等。10%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数份十数亿三要素数据泄露,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数十亿行以上。

二、事件抽样分析

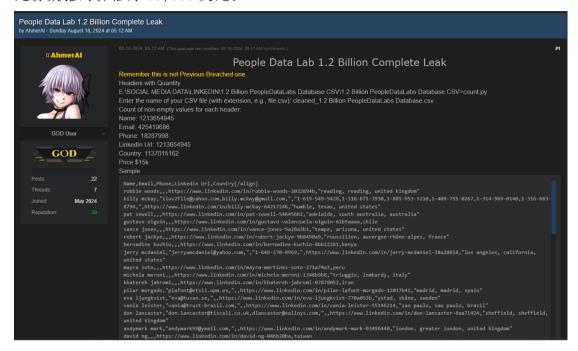
1、peopledatalab 数据泄露 12 亿条

发布时间: 2024.8.18

泄露数量: 1,213,654,945

售卖/发布人: AhmerAI

事件描述: 2024.8.18 某暗网数据交易平台有人宣称正在售卖一份 peopledatalab数据。卖家称此份数据与此前 peopledatalab 泄露过的 4 亿条数 据不是同一份, 称此份数据有效姓名字段超 12 亿条; 有效邮箱字段超 4 亿条; 有效电话字段超 1800 万条; 有效领英链接超 12 亿条; 有效国家字段超 11 亿条, 此份数据的价格为 15,000 美元。



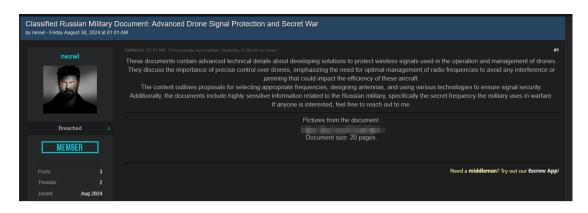
2、俄罗斯机密军事文件数据泄露

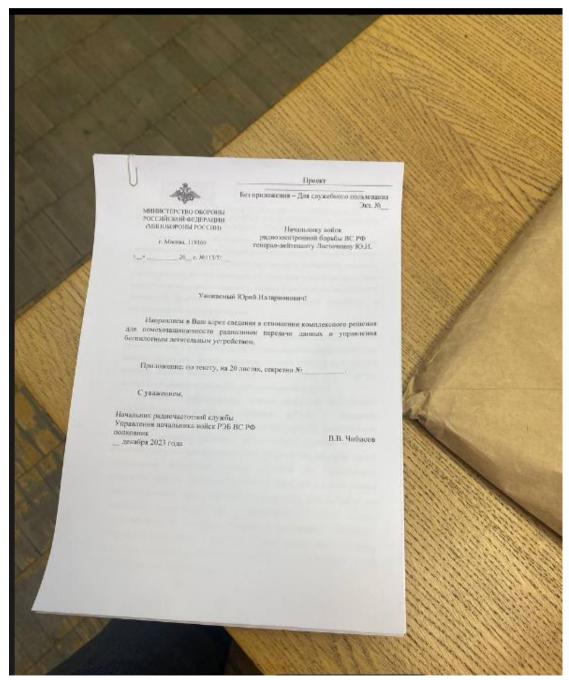
发布时间: 2024.8.30

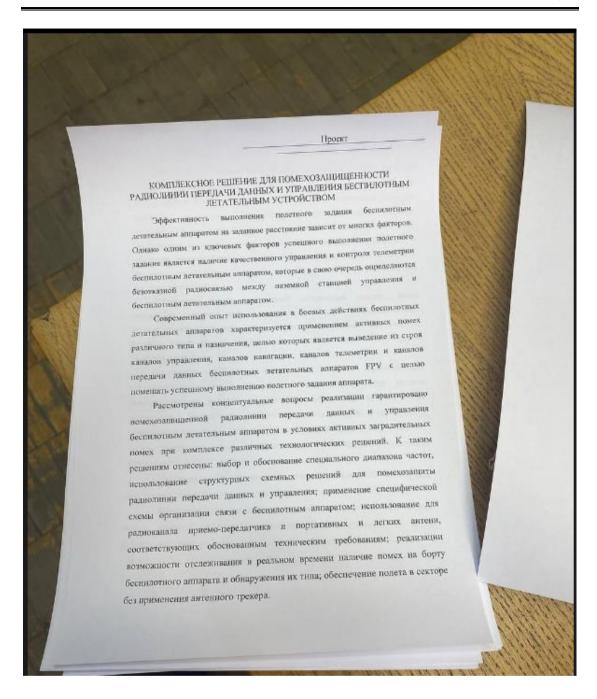
泄露数量:

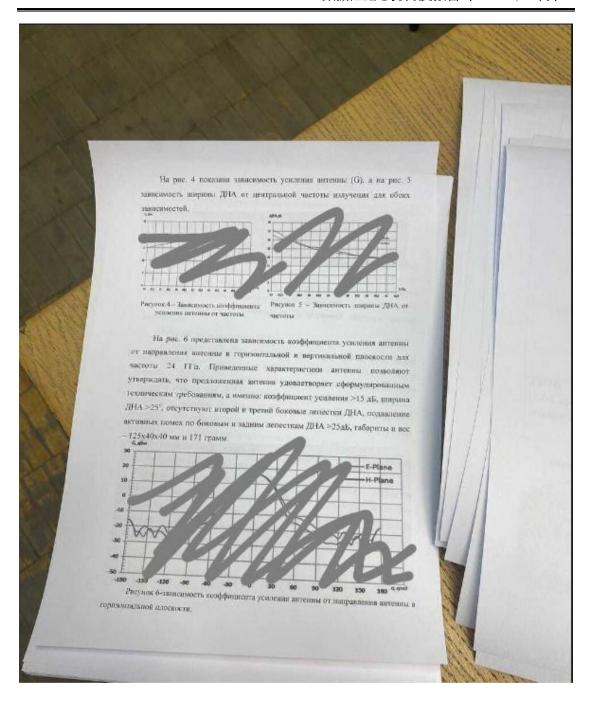
售卖/发布人: nexwl

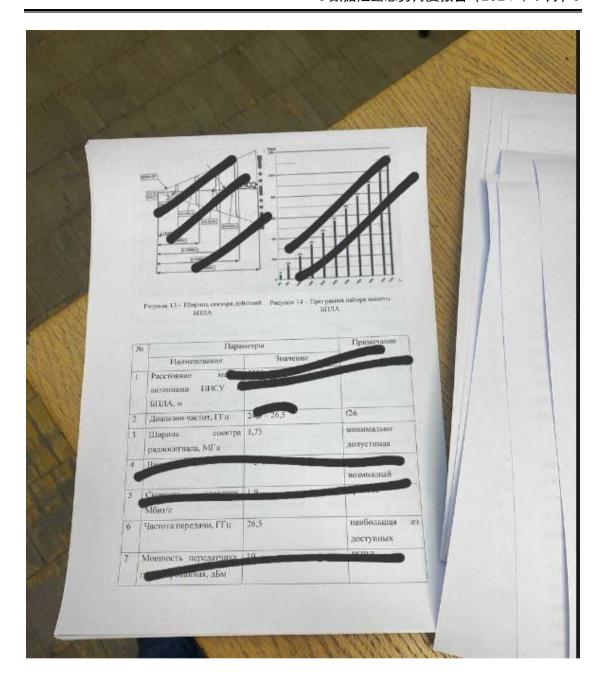
事件描述: 2024. 8. 30 某暗网数据交易平台有人宣称正在售卖一份俄罗斯机密军事文件。卖家称此份数据包含了: 有关开发解决方案以保护无人机操作和管理中使用的无线信号的先进技术细节。他们讨论了精确控制无人机的重要性,强调了对无线电频率进行最佳管理的必要性,以避免任何可能影响这些飞机效率的干扰或干扰。内容概述了选择合适频率、设计天线和使用各种技术来确保信号安全的建议。此外,这些文件还包括与俄罗斯军方有关的高度敏感信息,特别是军方在战争中使用的秘密频率。此份数据的价格为 10,000 美元。











3、俄罗斯核文件数据泄露

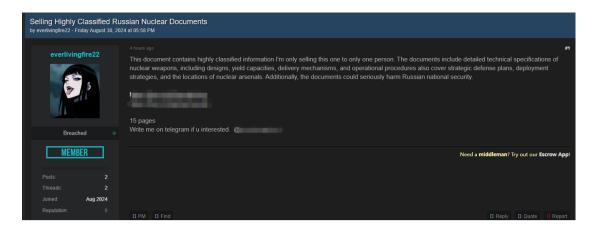
发布时间: 2024.8.30

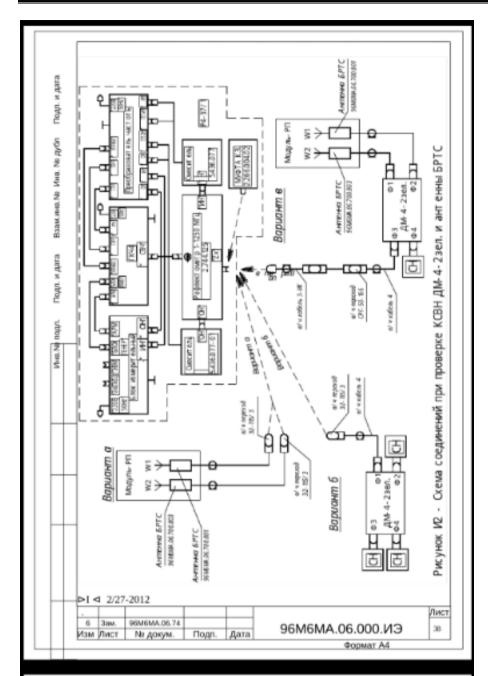
泄露数量:

售卖/发布人: everlivingfire22

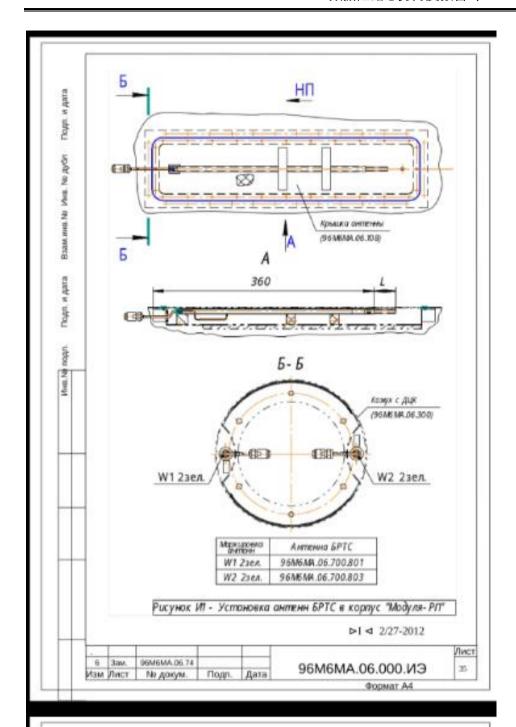
事件描述: 2024. 8. 30 某暗网数据交易平台有人宣称正在售卖一份俄罗斯核文件数据。卖家称此份数据包含: 核武器的详细技术规格,包括设计、当量能力、运载机制和操作程序,还包括战略防御计划、部署战略和核武库的位置。此外,这

些文件可能会严重损害俄罗斯的国家安全。此份数据的价格未知。





Если КСВН не соответствует требованиям, то произвести и дата подстройку антенны путем изменения длины выдвижного штыря. После настройки штырь припаять в соответствии с требованиями чертежа Toppi. 96M6MA.06.650CB. ИЗ.9 После настройки установить крышку и произвести повторную Visia. No Jayfin проверку антенны в соответствии с п.п. ИЗ.4 – ИЗ.7 настоящей инструкции. ИЗ.10 После проверки настроенную антенну отключить от прибора P4-37/I. MHB.No ИЗ.11 Подключить к прибору Р4-37/І вторую антенну. Произвести ее B13M.) проверку и настройку аналогично первой антенне. и дата И4 Проверка и настройка делителя мощности ДМ-4-2 зел. ДМ-4-2 зел. проверяются следующие И4.1 В делителе мощности



И2 Указания мер безопасности

e gara

Подл.

No Aydin

Взамляя. № Инв.

И2.1 К работе допускаются лица, прошедшие инструктаж по технике безопасности при работе с электро-радиоизмерительными приборами, изучищими техническое описание и инструкцию по эксплуатации на прибор Р4-37/I ЦЮ1.400.245 ТО, настоящую инструкцию, а также инструкцию по технике безопасности на данное рабочее место.

ИЗ Проверка КСВН и настройка антенны БРТС

ИЗ.1 Установить отсек с установленными антеннами так, чтобы на расстоянии двух метров от проверяемой антенны не было металлических

4、美国机密军事计划黑矛计划数据泄露

发布时间: 2024.8.24

泄露数量:

售卖/发布人: nexwl

事件描述: 2024. 8. 24 某暗网数据交易平台有人宣称正在售卖一份美国机密军事计划黑矛计划。黑矛计划: 美国加强国防的秘密倡议美国正在不断发展其防御战略,以保持对新兴全球威胁的优势。最近一项名为"黑矛计划"的机密倡议是朝着这个方向迈出的重要一步。该项目的主要目的是抵消敌对国家在导弹技术和网络能力方面的快速发展。黑矛项目是在国防情报局(DIA)、国家侦察局(NRO)和国家安全局(NSA)的联合指导下开发的一个高度机密的项目。它侧重于加强美国在多个领域的战略防御能力: 太空、网络和导弹防御。该倡议不仅寻求防御潜在威胁,还寻求在技术上实现跨越式发展,以保持决定性优势。卖家称拥有这个绝密项目的完整档案,包括运营细节、技术进步和战略计划。附加机密文件:一系列文件,揭示了美国国防战略、秘密资助机制和机构间行动的隐藏方面。

BS-XX-0323-7A.pdf





TOP SECRET/SCI/TALENT-KEYHOLE/GAMMA/SI-G/TK//HCS-PANTHEON | SPECIAL ACCESS REQUIRED: BLACK SPEAR EYES ONLY



UNITED STATES DEPARTMENT OF DEFENSE JOINT CHIEFS OF STAFF
OFFICE OF THE UNDERSECRETARY OF DEFENSE
FOR INTELLIGENCE & SECURITY USD(1&S) THE PENTAGON WASHINGTON, D.C. 20301-3010

PROJECT BLACK SPEAR Advanced Ground-Based Midcourse **Defense Augmentation** (AGBM-DA)

Access Program Designation: MJ-PANTHEON Document Control Number: BS-XX-0323-7A Issue Date: 25 April 2023 Review Date: 25 September 2023 Declassify On: 2043-04-25 (Subject to change upon review)

Document Classification:TOP SECRET/SCI/TALENT-KEYHOLE/GAMMA/SI-G/TK//HCS-PANTHEON Special Access Program Codeword: UMBRA CROWN
Document Serial Number: TS-365-BS-3010-X19T

Controlled Cryptographic Item (CCI) Code: ZETA-1923-KAPPA-TS-18

Handling and Distribution Directives: DISSEMINATION CONTROL MARKINGS: NOFORN, RSEN, FRD, ACCM, SIOP-ESI, OPSEC

Security Oversight Office: Special Access Programs Oversight Committee (SAPOC)

Authorized Distribution and Access: EYES ONLY / NEED-TO-KNOW BASIS

Access exclusively restricted to:

Chairman, Joint Chiefs of Staff (CJCS) President of the United States (POTUS)
Secretary of Defense (SECDEF)
Designated USD(I&S) personnel with UMBRA CROWN endorsement Select Congressional Leadership on the Intelligence Oversight Panel

TOP SECRET/SCI/TALENT-KEYHOLE/GAMMA/SI-G/TK//HCS-PANTHEON | SPECIAL ACCESS REQUIRED: BLACK SPEAR EYES ONLY

TOP SECRET/SCI/TALENT-KEYHOLE/GAMMA/SI-G/TK//HCS-PANTHEON | SPECIAL ACCESS REQUIRED: BLACK SPEAR EYES ONLY

WARNING

Unauthorized access, dissemination, or possession of this document or its contents, or any attempt thereof, is a federal offense punishable under the National Security Act of 1947, amended (50 U.S.C. 401, et seq.). Continuous monitoring by the Special Measures Unit (SMU) is active.

Special Access Control & Procedures:

Biometric and retinal scan authentication prerequisite for access. Nano-embedded microtaggants within paper ensure traceability. Storage mandated within an RF-shielded, dual-lock SCIF under constant environmental monitoring.

Declassification Review Date:

Indeterminate - Subject to Q-Review by the Director of National Intelligence (DNI).

Mandatory Destruction Protocols:

Thermal eradication at Classified Materials Burn Site, followed by a controlled electronic degaussing operation.



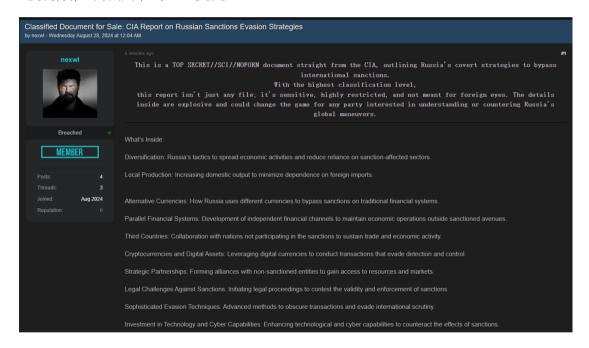
5、中情局关于俄罗斯逃避制裁策略的报告数据泄露

发布时间: 2024.8.28

泄露数量:

售卖/发布人: nexwl

事件描述: 2024. 8. 28 某暗网数据交易平台有人宣称正在售卖一份中情局关于俄罗斯逃避制裁策略的报告数据。卖家称此份数据"这是一份直接来自中央情报局的绝密文件,概述了俄罗斯绕过国际制裁的秘密战略。在最高分类级别下,这份报告不是普通的文件;它很敏感,高度受限,不适合外国人看。其中的细节具有爆炸性,可能会改变任何有兴趣理解或对抗俄罗斯全球演习的各方的游戏规则。"此份数据的价格为 2,000 美元。



6、旅行团数据泄露

发布时间: 2024.8.29

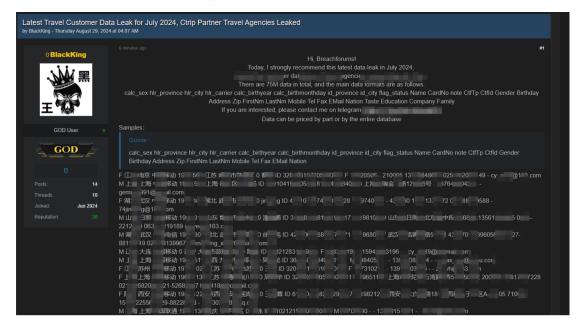
泄露数量: 75,000,000

售卖/发布人: BlackKing

事件描述: 2024.8.29 某暗网数据交易平台有人宣称正在售卖一份旅行团数据。

卖家称此份数据主要是与****程合作的旅行社客户数据库。数据字段有:姓名、

电话、地址、邮箱等, 此份数据的价格未知。



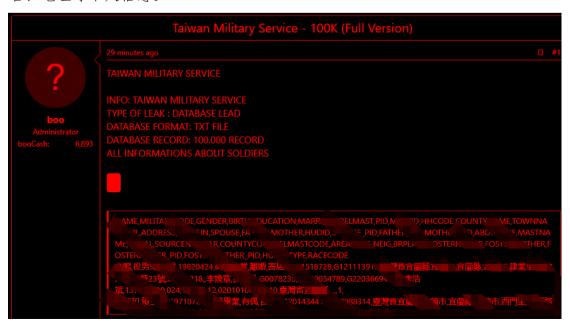
7、台湾兵役数据泄露

发布时间: 2024.8.30

泄露数量: 100,000

售卖/发布人: boo

事件描述: 2024. 8. 30 某暗网数据交易平台有人宣称正在售卖一份台湾兵役数据。 卖家称此份数据共有 10 万条,数据字段: 姓名、军人代码、教育水平、父母姓 名、地址等个人信息。



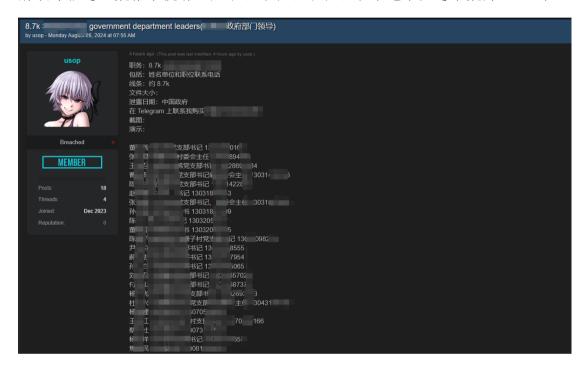
8、*****市政府领导信息数据泄露

发布时间: 2024.8.26

泄露数量: 8,700

售卖/发布人: usop

事件描述: 2024. 8. 26 某暗网数据交易平台有人宣称正在售卖一份******市政府领导信息。数据字段有: 姓名、单位、职位、联系电话,总条数为8700条。



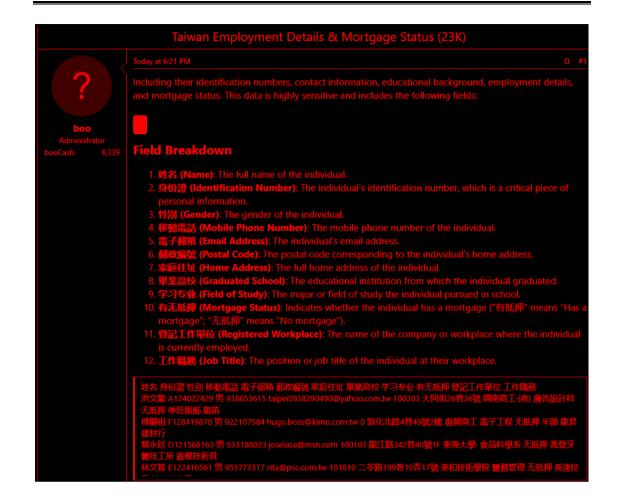
9、台湾就业详情和抵押状态数据泄露

发布时间: 2024.8.23

泄露数量: 23,000

售卖/发布人:

事件描述: 2024. 8. 23 某暗网数据交易平台有人宣称正在售卖一份台湾就业详情和抵押状态数据。数据字段有: 姓名、身份证号、性别、电话、邮箱、地址、学校、有无抵押情况、登记工作单位、工作职务,总条数为 23000 条。



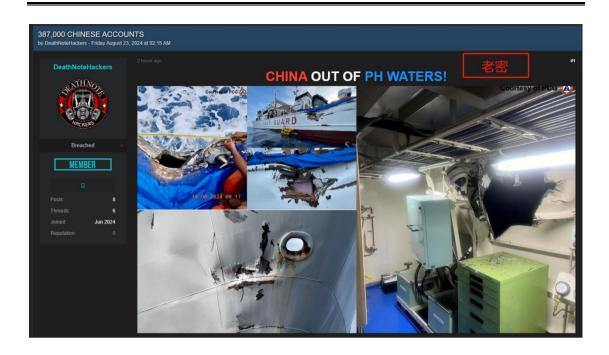
10、38.7万个中国账号数据泄露【老密】

发布时间: 2024.8.23

泄露数量: 387,000

售卖/发布人: DeathNoteHackers

事件描述: 2024. 8. 23 某暗网数据交易平台有人宣称正在售卖一份 38. 7 万个中国账号数据。其中,23. 6 万个中国教育机构账户以及 5. 1 万个淘宝账户并提供了下载链接。在经过对此数据抽样检查后,发现此三份数据均来自 2023 下半年的 naz. api 等相关数据集,通过关键词进行清洗得来。

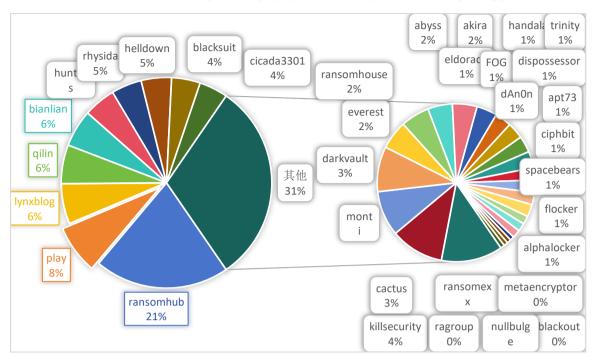


三、勒索软件和黑客组织

1、活跃商业黑客组织综述

2024年8月全球活跃的商业黑客组织(有勒索发布行为)共34个,公开的勒索事件共386件,TOP 10的黑客组织如下所示:

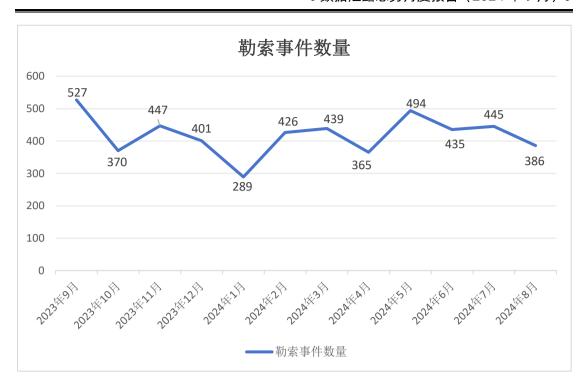
活跃商业黑客组织 **TOP10** 排名 组织标识 组织名称 发布数量 Ransomhub ransomhub 84 **PLAY** play 29 Lynx lynxblog 3 24 4 qilin 23 5 BianLian bianlian 22 Hunters 6 19 HUNTERS INTERNATIONAL international rhysida 18 helldown 18 Helldown Leaks 8 9 **Black suit** Black suit 17 cicada3301 17 10 ⚠ Cicada3301 -来自2024年8月《数据泄露态势》



TOP 10 的商业黑客组织公开发布的勒索事件占全部事件的 69%, 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增加),整体活跃度趋势正在逐步趋于稳定,统计末端(2024年8月)达到一年前统计前端(2023年9月)的73.24%:



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:



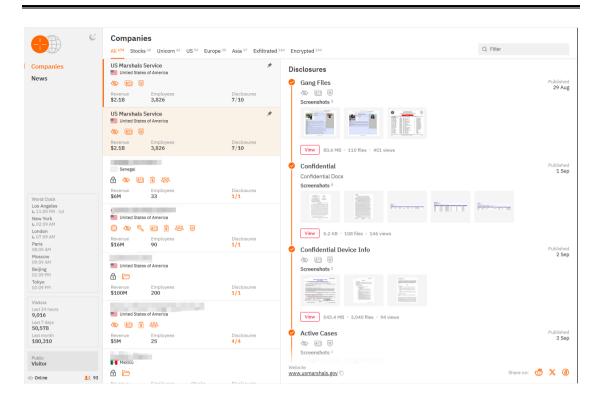
3、本月典型事件说明

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
https://www.usmarshals.g	美国法警局	2024/8/17	hunters
ov/			
Jeffersoncountyclerk.org	美国杰斐逊县书记办	2024/8/11	RansomHub
	公室		
http://www.huduser.gov	美国住房和城市发展	2024/8/7	Meow
	部		
http://www.kinetx.com	美国航空航天公司	2024/8/7	Play
	KinetX Aerospace		
https://aikenhousing.org	美国艾肯房屋委员会	2024/8/6	Black Suit
/			
nieul-sur-mer.fr	法国滨海尼约尔镇	2024/8/30	lockbit3
http://www.polycohealthl	保利可医疗有限公司	2024/8/28	RansomHub
ine.com			
http://www.alabamaplate.	阿拉巴马板材切割公	2024/8/26	RansomHub
com	司		
http://keystoneeng.com/	美国基斯通工程	2024/8/2	Space Bears
http://www.prismconstruc	棱镜建筑	2024/8/29	Monti
tion.co.uk			

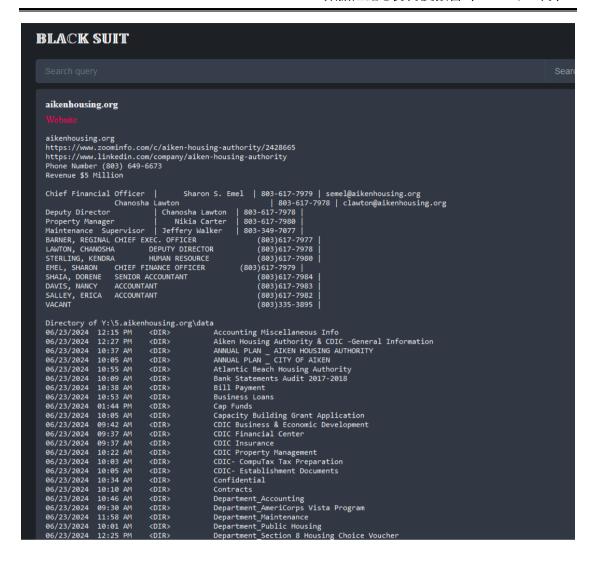
(1) 美国法警局

商业黑客组织 hunter 在 2024.8.17 公布了美国法警局被勒索的信息。该组织未按照规定时间内支付赎金, hunter 于 2024.8.29 释放了获取到的所有该组织的数据。



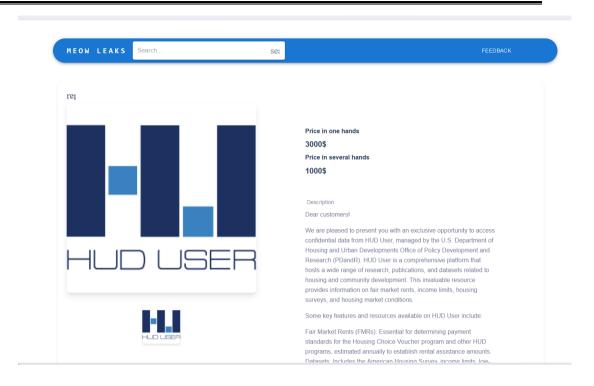
(2) 美国艾肯房屋委员会

商业黑客组织 Black Suit 在 2024. 8.6 公布了美国艾肯房屋委员会被勒索的信息。该组织未按照规定时间内支付赎金, Black Suit 于 2024. 8.23 释放了获取到的所有该组织的数据。



(3) 美国住房和城市发展部

商业黑客组织 Meow 在 2024.8.7 公布了美国住房和城市发展部被勒索的信息。该组织未按照规定时间内支付赎金, Meow 随后将这些数据以 1000-3000 美元的价格进行出售。



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
****勤科技集团	科技	2024/8/22	Helldown
****图书股份有限公司	教育	2024/8/28	RansomHub

■ 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

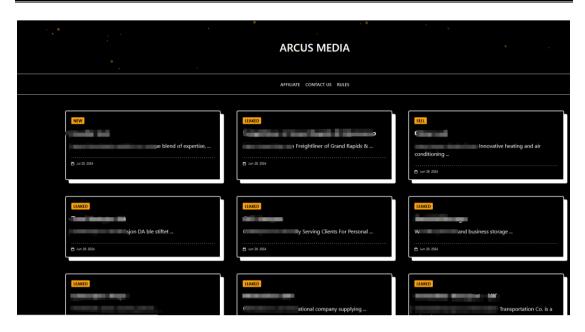
5、典型黑客组织简介(Arcus Media)

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 如需了解请翻阅往期报告。

本期介绍的是 Arcus Media 黑客组织。Arcus Media 于 2024 年 5 月中旬开始首次行动,截止 2024 年 7 月底共发动了 28 次勒索行动。其中 Arcus Media 5 月份成功发动的勒索软件攻击次数在勒索软件组织中排名第 10, 共有 11 次攻击成功。Arcus Media 使用带有恶意附件的钓鱼电子邮件获取初始访问权限。他们部署自定义勒索软件二进制文件和混淆脚本来执行有效负载,创建计划任务以保持持久性,并使用 Mimikatz 等工具进行权限提升。他们的方法包括常规勒索和双重勒索。

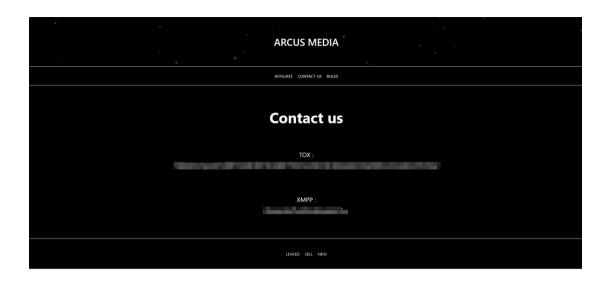
Arcus Media 以勒索软件即服务 (RaaS)的形式运营,允许其他威胁行为者使用他们的恶意软件。研究人员指出,他们有一个独特的联盟计划,要求新联盟必须由现有联盟推荐。该组织针对多个行业,包括政府、金融、医疗保健和教育,其中最著名的攻击是美国电信和伦敦医院。以下为Arcus Media的官网界面:



在其官网规则中介绍到"如果受害者不支付赎金或没人购买则他们会泄露数据 出来供他人下载"。

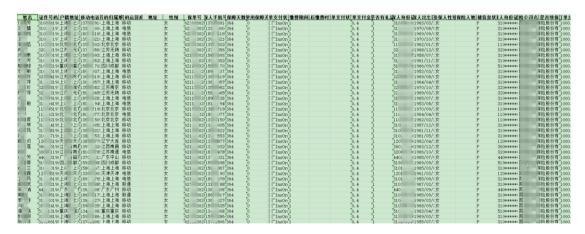


在联系方式上有 TOX 和 XMPP 两种联系方式,同时在其网页底部有泄露(leaked)、售卖(sell)和勒索新闻(new)三种分类:



四、匿名社交社群

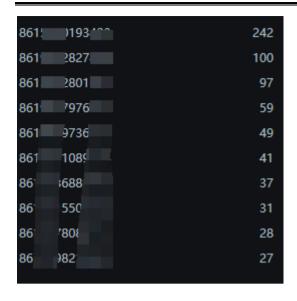
8月份监控到匿名社交社群情报总数量 15,066,767 条,提供的有效数据泄露 样例下载 7,784 份。涉及到我国数据泄露的内容包括:投资信息、保险信息、贷 款信息、房主信息、车主信息、购物信息等众多类型。以下随机选取展示部分样 本:



秦唐文文杉外丑以号子子。——"思西班里是以及是"英梅"——"春生"	1778 1.551 1377 1122 1868 1193 1345 4508 1398 5400 1345 6809 1398 5400 1345 6809 1386 87755 1588 9618 1337 3040 1343 3040 1343 3040 1344 5808 1357 3040 1358 3040 1357 3040 1358	211: 385 211: 163 211: 163 211: 163 211: 163 221: 153 221: 153 221: 153 221: 153 221: 153 221: 153 221: 153 221: 153 221: 153 221: 126 221: 127 221: 281 221: 281 221: 282 221: 282 221: 282 231: 311 221: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 231: 282 232	工規附當50CT1908 好來情當變 含質DOKT1946 含產者P1931187812 工規附指54KT10607 新加斯16号XMSCIG3722 新加斯16号XMSCIG3722 新加斯16号XMSCIG3722 新加斯16号XMSCIG3722 新加斯16号XMSCIG3722 新加斯16号XMSCIG3722 新加斯16号XMSCIG3722 第加斯16号XMSCIG3722 第加斯16号XMSCIG3722 第加斯16号XMSCIG3722 其份增高54KT10507 工規附當54KT10501 持加斯16号XMSCIG3722 持在曾述AMATYSTWSCIG3722 持在曾述AMATYSTWSCIG3722 其份增高54KT10501 其份增高54KT10501	366天投資投資。 1867年代 18	នកិត្ត ទេក ទេក ទេក ទេក ទេក ទេក ទេក ទេក ទេក ទេក	. 经转换线 经存储分别 医克里克氏 医克里克氏 医克里克氏 医二甲二氏 医二甲二氏 医二甲二氏 医二甲二氏 医二氏虫虫 医克里克氏 医二甲基二氏 医二氏 医二氏 医二氏 医二氏 医二氏 医二氏 医二氏 医二氏 医二氏 医	1776 1351 1377 1352 1377 1352 1377 1352 1377 1377 1375 1376	四四川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川川	移动动 女女 196. /15 斯特勒动女女 196. /15 196. /15 196. /15 196. /15 196. /16 196. /17 1	即用倫達加市 即用格達加州市 即用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 用用格達加州市 和市市市 和市市市 和市市市 和市市市市 和市市和市市市 和市市市市市市市市
公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公	具在张济游和风度,王英林广的颜朱初日和《曹昌王·杜的祖宗·斯勒斯伯诗字》 1.20 1.20 1.20 1.20 1.20 1.20 1.20 1.20	9 32 3 3 5 5 9 9 3 3 3 3 3 5 9 9 9 9 9 9 9 9 9	10 56	等。 1. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2.	是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是是		一年の日本の子子			3
姓名		身份证号	手机号	性别			ID绑定码		支付时间	扫码转出金额
走		52 6004 031	18 399		E2430657-			-808DDD5A16E9	2024-03-21 17:05:28	9218元
後		.0 640' L6:	13 041		191F230C			-D05B29892E79	2024-06-04 05:09:11	16708元
=		72 601()6:	13 861		9D05FA23-		-DC53-8	-EEFE2C3E0143	2024-03-28 01:19:52	8441元
		50 600: L8:	131 1336		28140F3D			-0F354B45D167	2024-03-17 22:43:39	16188元
ŧ		10 601()6:	137 .899		91CED56D			-155B631CAE62	2024-02-14 20:16:45	9269元
		50 640: 14:	139 .299		2FE5E79E			-40EF81A6A9F2	2024-02-20 14:07:21	19015元
		20 600 22	138 5634					-DAB1C3764595	2024-01-28 20:45:31	16908元
_		50 650 13	18 7707		05503E61	-5 5-	-B9EB-2	-16C1CB96C9C9	2024-03-03 07:49:59	19137元
-4	Ft (1)	70 1640 26	13 5999	男	BDAC491F	-F)-	-7B50-F	-7F54051C3209	2024-06-26 16:36:19	13400元

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1,562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8月份使用"86"开头的手机号的TOP 10信息:



* 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。



第三方独立

- 完全第三方背景
- 独立分析师团队

服务对象

- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品&服务供应商

调研对象

- 700+网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务内容

- 国家、行业智库
- 细分领域等调查研究报告
- 为服务对象提供面对面咨询
- 为产业各方提供资源对接

合作方式

- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA

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:北京市东城区鲜鱼口街90-2网安小酒馆

官方网站: www.dwcon.cn 联系邮箱: dw@dwcon.cn





