

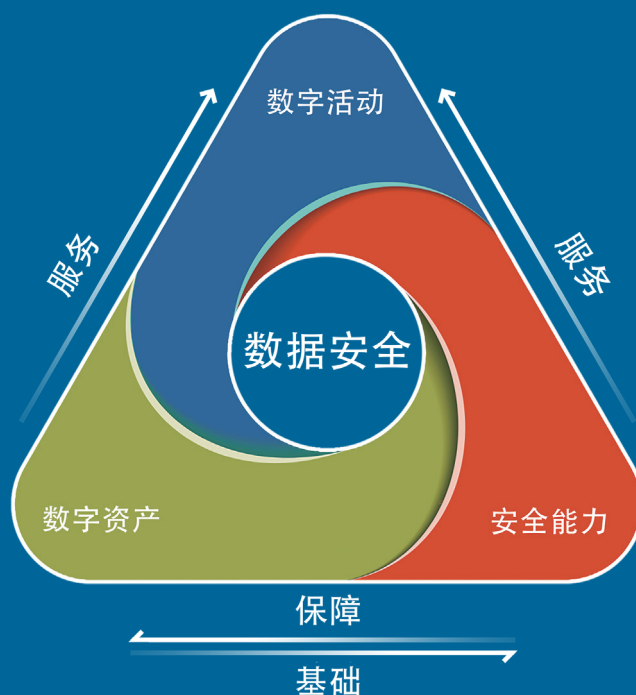
数据泄露态势月度报告

(2024 年 4 月)



数据泄露态势月度报告

(2024 年 4 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、北约军事数据泄露	4
2、FBI 数据泄露	5
3、DOD 数据泄露	6
4、俄罗斯军队领导数据泄露	7
5、泰国内部安全行动指挥部数据泄露	8
6、*** 省公共资源交易中心数据泄露	10
7、*** 省社会保障局数据泄露	11
8、***** 置业搬迁服务有限公司数据泄露	11
9、*** 集团高端客户数据泄露	12
10、* 国公民四要素数据泄露	13

目 录

第三章 勒索软件和黑客组织.....	14
1、活跃商业黑客组织综述	14
2、黑客组织活跃度趋势	15
3、本月典型事件说明	16
(1) 美国田纳西州谢尔比县下属城市 Bartlett	17
(2) 联合国开发计划署	17
(3) 大陆航空航天技术	18
4、本月涉及中国企业的勒索事件说明	19
5、典型黑客组织简介 (BianLian)	19
第四章 匿名社交社群	22

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。

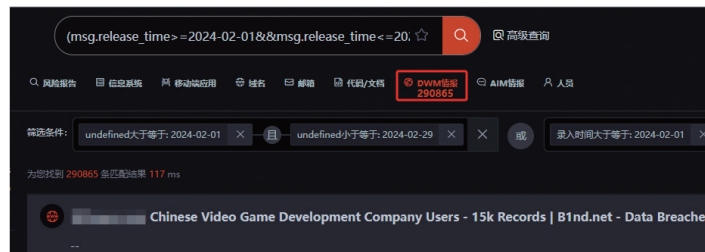
为了掌握数据泄露态势，应对日益复杂的安全风险，数世咨询联合零零信安，基于 0. zone 安全开源情报系统，共同发布《数据泄露态势》月度报告。该系统监控范围包括明网、深网、暗网、匿名社群等约 10 万个威胁源。除了月度的数据泄露概况以外，报告还会针对一些典型的数据泄露事件进行抽样事件分析。如果发现影响较大的数据伪造事件，还会对其进行分析和辟谣。

本期报告的统计区间 2024 年 3 月。

第一章 数据泄露市场

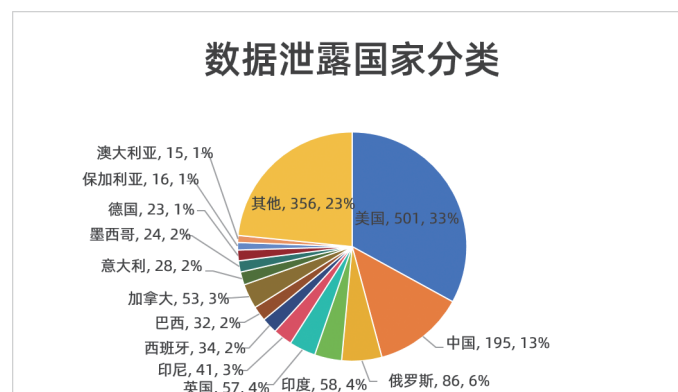
2024 年 3 月共监控到全球 DWM（Dark Web Market）情报：

- 深网和暗网有效情报 290,865 份；
- 泄露数据的买卖情报份 1,519 份。



1、国家分类

其中美国是数据泄露第一大国，共泄露数据 501 份，其他数据泄露较多的国家还包括：中国、俄罗斯、印度、英国、印尼、西班牙、巴西等。详情如下图所示：

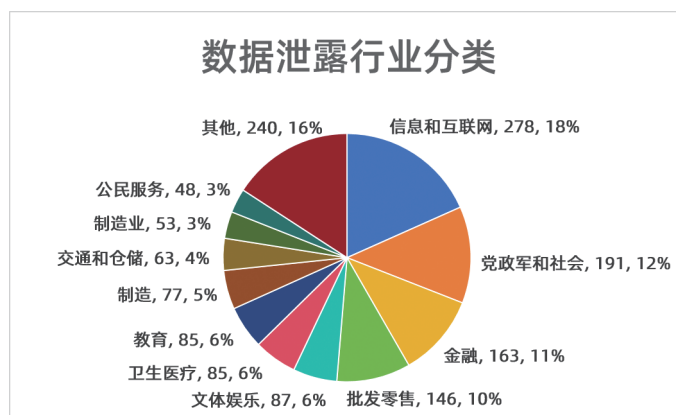


在“其他”数据中包含其他国家以及无法准确进行国家分类的数据泄露事件，例如二要素数据（账号：密码 / 邮箱：密码）、LOG 记录等。

2、行业分类

3 月份行业属性数据占泄露数据总量约 84% 左右，泄露的行业数据主要包括信息和互联网行业、党政军与社会、金融行业、批发零售业、文体娱乐业等。16% 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**数十亿行以上**。

第二章 事件抽样分析

1、北约军事数据泄露

发布时间：2024. 3. 11

泄露数量：

售卖 / 发布人：aaron_bushnell

事件描述：2024. 3. 11 某暗网数据交易平台有人宣称正在售卖一份北约军事数据。该卖家称他们窃取了超过 5GB 的数据，售价为 20,000 美元。卖家称此份数据包括 4000 个关于军事地图的敏感文档，在 NATO 工作的雇员和军人的信息，秘密合同等。此黑客团队 Aaron Bushnell 的攻击对象主要是以色列和北约以及其成员国，他们声称所有售卖数据所得到的资金将用于对巴勒斯坦人道主义的支持。

NATO Military Infrastructures Hacked By Aaron Bushnell Hackers
By aaron_bushnell · Monday, March 11, 2024 at 08:53 PM

11 members rep

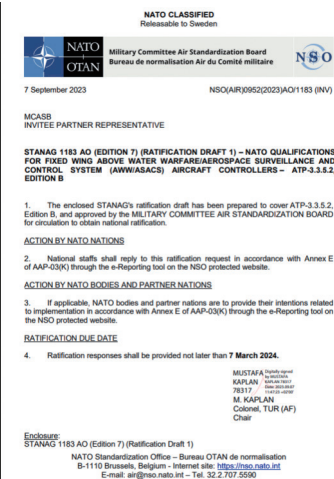
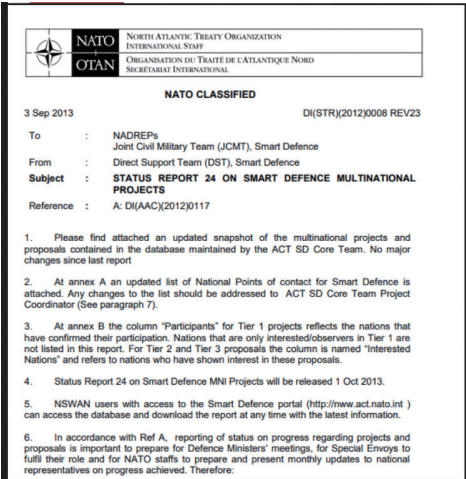
Aaron Bushnell hackers hacked the military infrastructures of NATO for the sale of the Palestinians and they stole more than 5GB of data including 4000 sensitive docs about military maps, info of employees and military men and women working in NATO, the secret contracts etc.

Price: \$20,000

Note: Like our previous sale, the money received for this database is spent for humanitarian purposes in Palestine.

aaron_bushnell
Breached
MEMBER
Posts: 9
Threads: 5
Joined: Mar 2024
Reputation: 0

	A	B	C	D
1	Name	Username	Email	
2		natopaas	jpferr@nato-pa.int	
3		altersky	altersky@nato-pa.int	
4		grosins@nato.lv	grosins@nato.lv	
5		SSachs@nato-pa.int	SSachs@nato-pa.int	
6		ropoa@nato-pa.int	ropoa@nato-pa.int	
7		ra4@nato-pa.int	ra4@nato-pa.int	
8		loskutov@natomission.ru	loskutov@natomission.ru	
9		5FCHQ@rumsom12	varochaalk@nato-pa.int	
10		pandc	jSpandc@jsw.nato.int	
11		narbonne	jp.roves@hq.nato.int	
12		MarchKoz	m.kozel@hq.nato.int	
13		john.greaves@act.nato.int	john.greaves@act.nato.int	
14		HQ SACT - NATO	none@act.nato.int	
15		hc31	ussery@act.nato.int	
16		abildacci	abildacci@nrc.nato.int	
17		shieldk	shieldk@act.nato.int	
18		jansengers	j.sengers@hq.nato.int	
19		elidberg	mike.elidberg@shape.nato.int	
20		Mastriano777	douglass.mastriano@lhd.nato.int	
21		beckernato	becker@act.nato.int	
22		gmorittu	gmorittu@afsouth.nato.int	
23		ranellip	ranellip@nrc.nato.int	
24		franjo	francisco.saezgonzalez@nhqpa.nato.int	
25		b.stlaurent@ndc.nato.int	b.stlaurent@ndc.nato.int	
26		DeWaan@jcc.nato.int	devaan@jcc.nato.int	
27		lanmetti@jcc.nato.int	lanmetti@jcc.nato.int	
28		intel@jcc.nato.int	intel@jcc.nato.int	



2、FBI 数据泄露

发布时间：2024. 3. 5

泄露数量：

售卖 / 发布人：Team1956

事件描述：2024. 3. 5 某暗网数据交易平台有人宣称正在售卖一份美国联邦调查局（FBI）数据。此份数据售价为 499 美元，卖家称此份数据获取日期是 2024 年 1 月，泄露的数据字段有：身份证、电子邮件、地点、全名、号码、电话、机密文件、照片和其他数据。卖家还留下了他的 telegram 联系方式以供买家获取此数据的细节并购买。

Big data belonging to the FBI
by Team1956 - Tuesday, March 5, 2024 at 01:36 AM

Team1956

Country: US
Date: January 2024
File: ZIP

Columns: ID, email, location, full name, number, phone, confidential documents, photo. And other data.

Telegram: @man-tech
Our Telegram channel is where we post all our hacks:
<https://t.me/man-tech>
The price: 499\$ BTC/ETH

Note: If you want some samples, just contact us on our Telegram account and we will send you a clip with some documents

Project	Name	Position	Location	Number	Mobile	Email
MTISC	Darrell Leonard	Vice President	Chantilly	(703) 814-4226		Darrell.Leonard@ManTech.com
MTISC	Courtney McCoy	Executive Admin	Chantilly	(703) 814-4240	571-723-6432	Courtney.McCoy@ManTech.com
MTISC	Kyrstie Birchfield	Office Admin	Chantilly	(703) 814-4200		Kyrstie.Birchfield@ManTech.com
MTISC	Ceci Jett	Finance/Budget	Chantilly	(703) 814-4282		Ceci.Jett@ManTech.com
MTISC	Lindsay Williams	Finance/Budget	Chantilly	(703) 814-8395		Lindsay.Williams@ManTech.com
MTISC	Karen Glasgow	Finance/Budget	Chantilly	(703) 814-8375		Karen.Glasgow@ManTech.com
MTISC	Erin Kucharski	SAC Specialist	Chantilly	(703) 633-1381		Erin.Kucharski@ManTech.com
MTISC	Tanya Klawitter	Procurement	Chantilly	(703) 814-4228		Tanya.Klawitter@ManTech.com
MTISC	Nathaniel Tartick	Procurement	Chantilly	(703) 814-8374		Nathaniel.Tartick@ManTech.com
MTISC	Nelcia Manning	Procurement	Chantilly	(703) 488-2769		Nelcia.Manning@ManTech.com
MTISC	Jontae Lee	Recruiter	Chantilly	(703) 488-2673		Jontae.Lee@ManTech.com
MTISC	Dan Ayers	PM Projects	Chantilly	(703) 814-4283		Dan.Ayers@ManTech.com
MTISC	Christopher Campbell	PM Project	Chantilly	(703) 814-4247		Christopher.Campbell@ManTech.com
MTISC	Ernest Hayden	PM IT MSP	Chantilly	(703) 814-4246		Ernest.Hayden@ManTech.com
GPMS	Felix Martin	PM LBE	Chantilly	(703) 814-4317		Felix.Martin@ManTech.com
GPMS	Lorenzo Ceballos	PM LBE	Chantilly	(703) 814-8365		Lorenzo.Ceballos@ManTech.com
GPMS	Kevin Moyer	PM LBE	Chantilly	(703) 633-1321		Kevin.Moyer@ManTech.com
GPMS	Diane Lundy	Operations Manager	Chantilly	(703) 814-8380		Diane.Lundy@ManTech.com

ID	Name	Email ID	DeptID
600753	Weatherspool, Marlene R.	marlene.weatherspool@mail1.monmouth.army.mil	34112
601495	Loggia, Anthony J	anthony.loggia@mail1.monmouth.army.mil	34112
031429	Leonard, Darrell W	g6amtech1@hq.c5.army.mil	34411
033520	Varga, Joseph W	g6amtec2@hq.c5.army.mil	34411
034979	Robertson, Keith H	sgsauto2@hq.c5.army.mil	34411
601534	McMullan, Robert C.	GONE	34411
601497	Massey, William	GONE	34411
601055	Dik, Zoya, Malvi S.	GONE	34411
600848	Thompson, Kevin	au_k9@hotmail.com	34411
037053	Graham, Kimberly	g6amtech@hq.c5.army.mil	34411
035445	Anderson, Charles E	GONE	34411
035445	Anderson, Charles E	g6amtech3@hq.c5.army.mil	34411
035067	Rollins, Glen	sgsauto3@hq.c5.army.mil	34411
035121	Garner, Kevin L	GONE	34411
032081	Garner, Kevin L	GARNERK@FHU.DISA.MIL	34417
032148	Broten, Charles E	brotencc@hq.5sigcmd.army.mil	34417
033849	Thorne, Raymond W	ray.thorne@hq.amceur.army.mil	34417
601239	Klinner, Kenneth O.	ken.klinner@hq.amceur.army.mil	34417
034947	Malachi Jr, Leroy	lmalachi@hq.amceur.army.mil	34417
033622	Taylor, Terence N	G6AMTECH7@HQ.C5.ARMY.MIL	34417

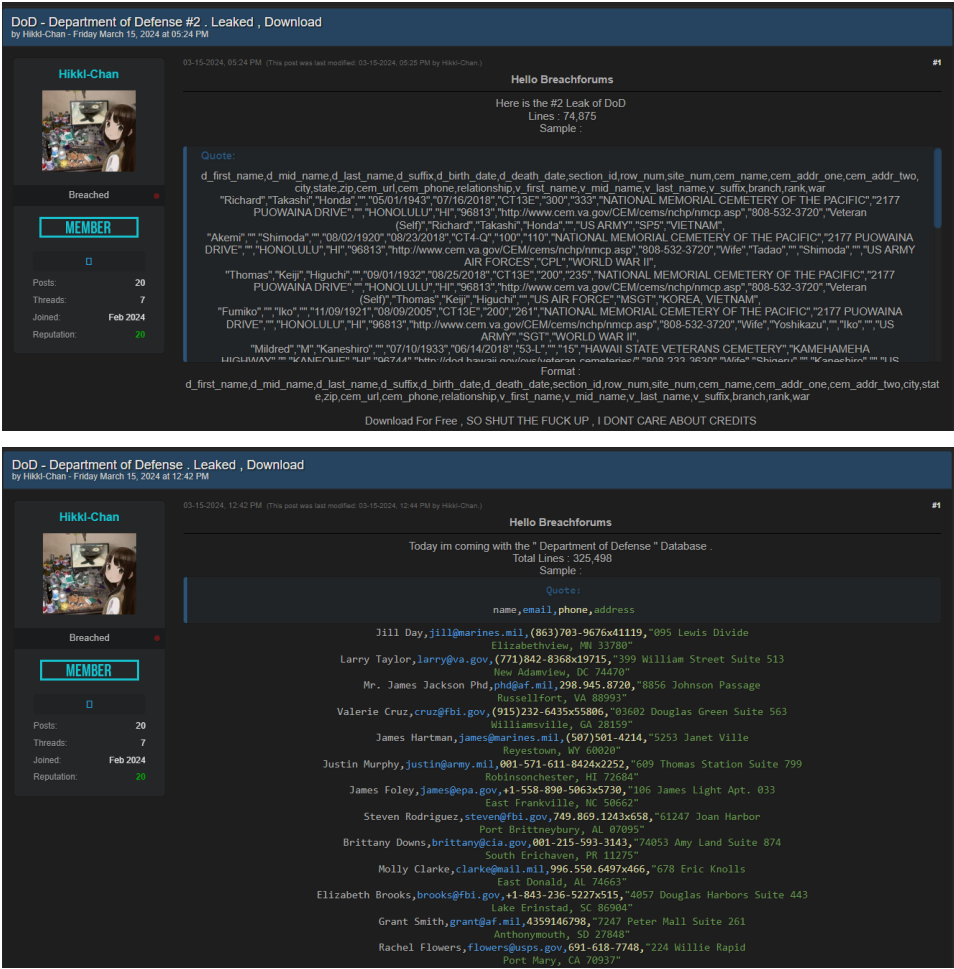
3、DOD 数据泄露

发布时间：2024. 3. 15

泄露数量：399,373

售卖 / 发布人：HikkI-Chan

事件描述：2024. 3. 15 某暗网数据交易平台有人宣称正在售卖一份美国国防部 (dod) 数据。卖家于 3 月 15 日前后两次上传了共计 399,373 条数据。其中第一份数据包含姓名，电话，城市、职位、参加过什么战争等字段，第二份数据包含姓名、电话、邮箱、地址等字段。卖家称两份数据的来源均是美国国防部官方网站 <https://dod.hawaii.gov/>。



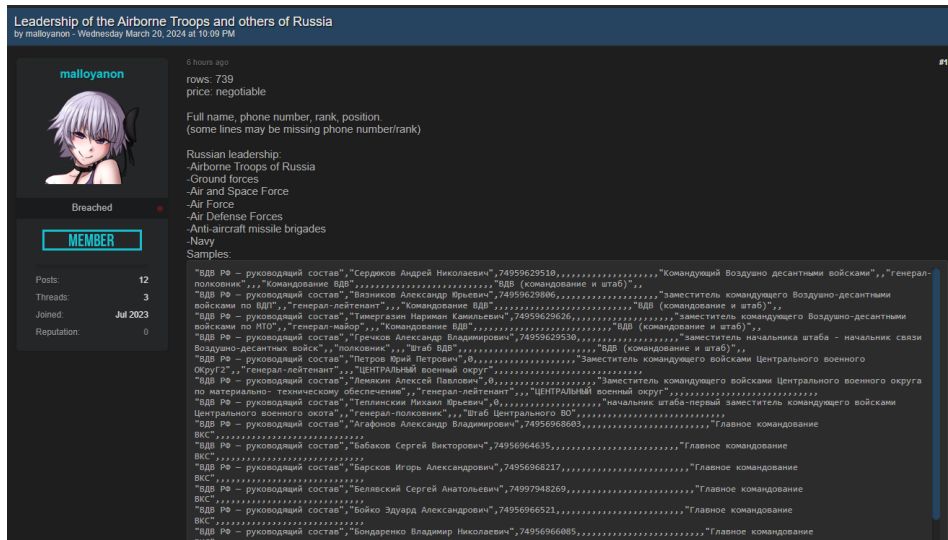
4、俄罗斯军队领导数据泄露

发布时间：2024. 3. 20

泄露数量：739

售卖 / 发布人：malloyanon

事件描述：2024. 3. 20 某暗网数据交易平台有人宣称正在售卖一份俄罗斯军队领导数据。此份数据的涉及部门有俄罗斯空降部队、地面部队、空军、防空部队、反舰导弹旅、海军等。数据样本包含用户名称，电话号码，军衔，职位等，价格暂时未知。



5、泰国内部安全行动指挥部数据泄露

发布时间：2024. 3. 6

泄露数量：

售卖 / 发布人：R1g

事件描述：2024. 3. 6 某暗网数据交易平台有人宣称正在售卖一份泰国内部安全行动指挥部（Internal Security Operations Command, 简称‘ISOC’）数据。内部安全行动指挥部（ISOC）是泰国皇家武装部队的政治部门。卖家称此份数据共 200GB，包含大量绝密、机密项目以及操作文件并附上了一些样例作为证明，价格卖家并未提及。

200GB Documents of Internal Security Operations Command

by R1g - Wednesday March 6, 2024 at 01:32 AM



R1g

say hello

GOD

Posts: 257
Threads: 23
Joined: Jun 2023
Reputation: 913

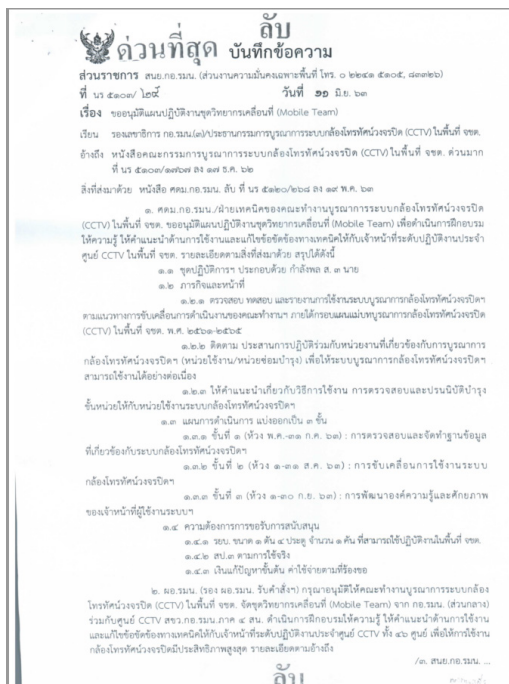
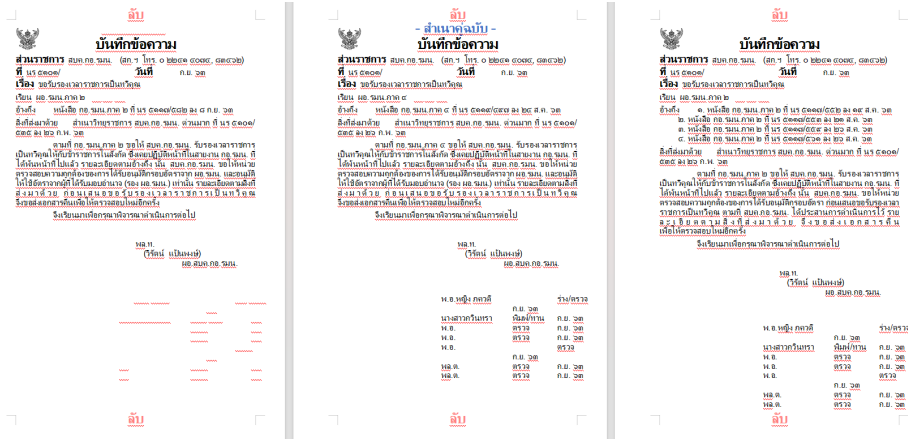
11 minutes ago · (This post was last modified: 8 minutes ago by R1g) Edit | Remove | #65 edited

I want to sell documents from Thailand ISOC (Internal Security Operations Command).
200GB of top secrets , secrets , project and operation files in various formats. I dumped this data from their Drive System in Jan/2024.
Sample Files : <https://bits.offshore.cat/r7jOZdn.7z>
Accept XMR and BTC . Please dont waste my time. Contact me via Tox or Telegram.
Tox : F17FSDFQ22412T9E814CD4D1C77DA2F4FA1FFB9BFDBBD5095708DE06978E37CGD36C0AD4CD
Telegram : @ExRlg

🔴 CamScanner 20-12-2566 09.14...	5.0 MB	PDF docum...	20 December 2023, 03:22
🔴 CamScanner 20-12-2566 09.4...	574.4 kB	PDF docum...	20 December 2023, 03:22
🔴 ISO๙แผนการดำเนินโครงการระยะ...	503.1 kB	PDF docum...	13 November 2023, 09:31
🔴 ทุกคนมาเที่ยวห้อง.pdf	207.1 kB	PDF docum...	24 December 2023, 04:05
🔴 นอ.สม.๒6 รายงานผลการตรวจ...	111.7 kB	PDF docum...	19 December 2023, 03:46
🔴 การรวมบุคลากรเข้าฝึก นอ.สม...pdf	1.8 MB	PDF docum...	20 December 2023, 03:22
🔴 การตรวจประเมินความเสียหายต่อ...	1.5 MB	PDF docum...	21 December 2023, 03:10
🔴 การทำให้ระบบมีความแข็งแกร่ง นอ...	5.0 MB	PDF docum...	20 December 2023, 03:21
🔴 การบริหารหลักประกัน จัดทำโดย ลอ...	3.1 MB	PDF docum...	13 November 2023, 09:31
🔴 อัตรานายยุทธพร สมย.pdf	6.4 MB	PDF docum...	07 December 2023, 07:10
🔴 ลิตตบทในการไม่เปิดเผยข้อมูล.pdf	2.7 MB	PDF docum...	20 December 2023, 04:05
🔴 เอกสารสนับสนุนการตรวจประเมิน...	573.7 KB	PDF docum...	15 December 2023, 08:02
🔴 คู่มือปฏิบัติงานส่งมอบผลจากขอ...	2.1 MB	PDF docum...	20 December 2023, 03:53
🔴 ข้อมูลยึดอำนาจเข้าป่าปฏิบัติการ...	1.3 MB	PDF docum...	20 December 2023, 04:05
🔴 ข้อมูลปฐาเนินการเพื่อเตรียมการร...	982.3 KB	PDF docum...	13 November 2023, 09:31
🔴 ข้อมูลปีเฉพาะทางการจัดทำประว...	13.6 MB	PDF docum...	13 November 2023, 09:31
🔴 ข้อมูลปีเฉพาะทางการรักษาความ...	6.0 MB	PDF docum...	13 December 2023, 08:25
🔴 ข้อมูลปี (ร่าง) รบมการเสริมรัถ...	644.8 KB	PDF docum...	27 December 2023, 01:55
🔴 ข้อมูลปี (ร่าง) รบมการเสริมรัถ...	669.2 KB	PDF docum...	27 December 2023, 01:55
🔴 คอมพิวเตอร์จีน 12 ก.ล. 66.pdf	448.1 KB	PDF docum...	12 December 2023, 07:28
🔴 กลังเลียดตั้งควบคุมเอกสาร.pdf	209.7 KB	PDF docum...	13 November 2023, 09:32
🔴 เนื้อหาการตรวจสอบการดำเนินการ...	1.2 MB	PDF docum...	20 December 2023, 03:21

 02cc-plan.zip	 02cc-spt.zip	 020cc-srt.zip	 020cc-ssn.zip	 04forest.zip	 10cc-1.zip	 10cc-2.zip	 10cc-3.zip	 10cc-4.zip
 10cc-7.zip	 10cc-6.zip	 adm.obf.zip	 budpl.obf.zip	 cco1.zip	 budma.obf.zip	 Charanintr.zip	 cyber.zip	 Cherd.zip
 dg-document.zip	 dir2.zip	 ISOC-PR .zip	 isoc.dpm.zip	 lt.zip	 isoc32.zip	 isocbkk.zip	 isocnongbuala mphu.zip	 lt.gen04isoc .zi p
 mhq-plans.zip	 mhq-sims1374.zip	 off.obf.zip	 oig.zip	 opm-e.zip	 opss-io.zip	 opss-region .zip	 osc-osc.zip	 osc-prc .zip
 plan04isoc.zip	 province-nkn.zip	 province-kjb .zip	 province-npt .zip	 province-skk.zip	 region-3-2.zip	 saikimmz.melo dy.zip	 sakon1.zip	 sakon2.zip
 stn.zip	 trad2.zip	 utt1.zip	 searmporn_yin zin	 energy/isoc.zip	 dsc-dir.zip	 10cc-5.zip	 opas_pha.zip	

[illegible]



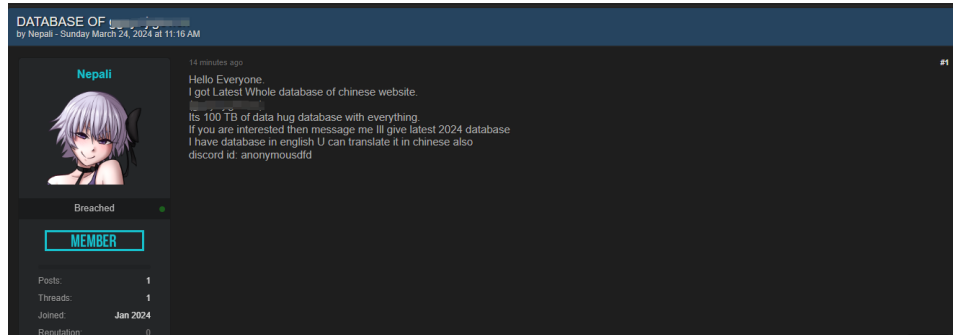
6、*** 省公共资源交易中心数据泄露

发布时间：2024. 3. 24

泄露数量：

售卖 / 发布人：Nepali

事件描述：2024. 3. 24 某暗网数据交易平台有人宣称正在售卖一份 *** 省公共资源交易中心数据。卖家称此份数据大小为 100TB，但并未给出任何样例也并未提及价格。



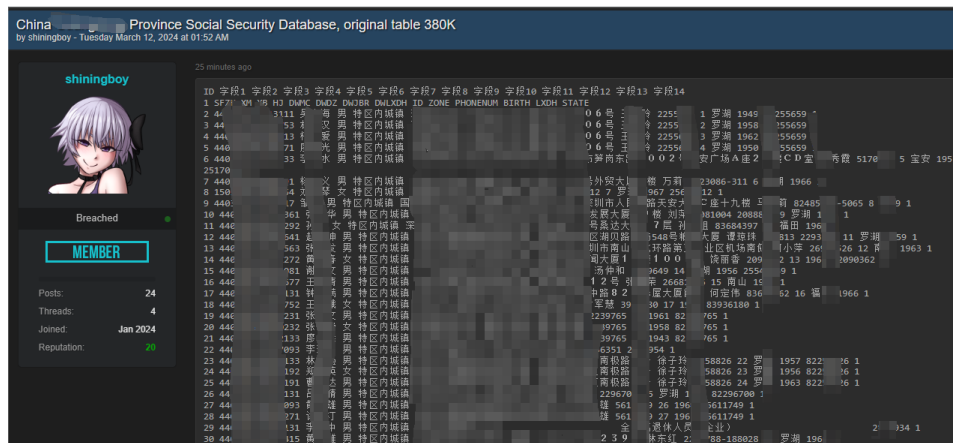
7、*** 省社会保障局数据泄露

发布时间：2024. 3. 12

泄露数量：

售卖 / 发布人：shiningboy

事件描述：2024. 3. 12 某暗网数据交易平台有人宣称正在售卖一份 *** 省社会保障局数据。卖家称此份数据共有 380,000 条，给出的样例中包含的字段有：姓名、手机号、公司名称、身份证号等。



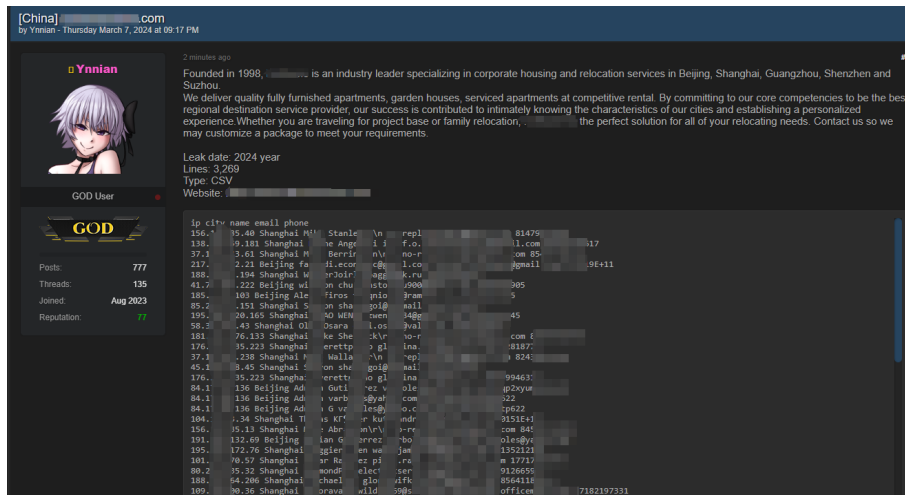
8、***** 置业搬迁服务有限公司数据泄露

发布时间：2024. 3. 7

泄露数量：3,269

售卖 / 发布人：Ynnian

事件描述：2024.3.7 某暗网数据交易平台有人宣称正在售卖一份 ***** 置业搬迁服务有限公司数据。该份数据共有 3,269 条，给出的样例中包含的字段有：ip 地址、城市、姓名、电话、邮箱。



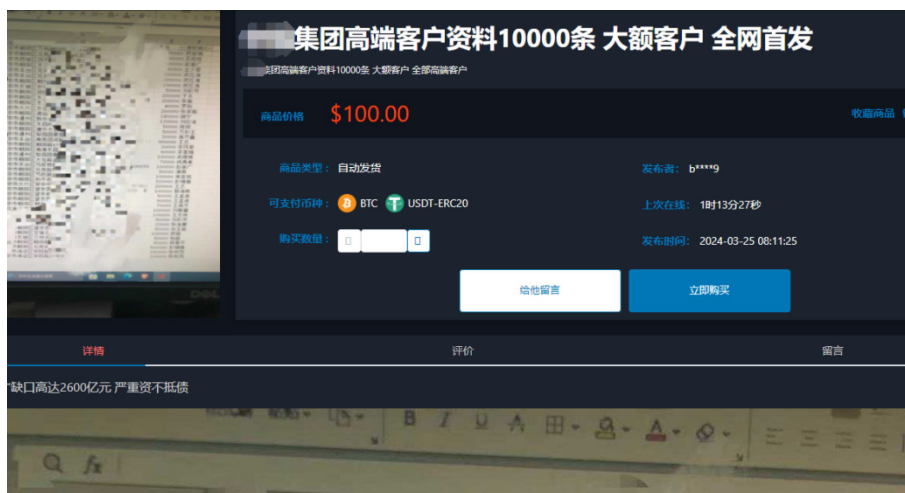
9、*** 集团高端客户数据泄露

发布时间：2024.3.25

泄露数量：100,000

售卖 / 发布人：b****9

事件描述：2024.3.25 某暗网数据交易平台有人宣称正在售卖一份 *** 集团高端客户数据。该份数据共有 100,000 条，售价为 100 美元。给出的样例中包含的字段有：姓名，电话，地址，身份证号等。



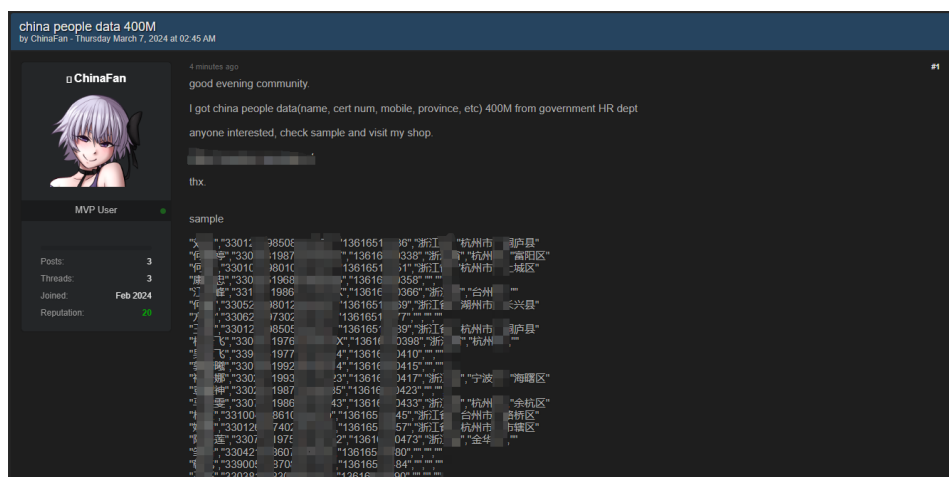
10、* 国公民四要素数据泄露

发布时间：2024. 3. 7

泄露数量：400,000,000

售卖 / 发布人：ChinaFan

事件描述：2024. 3. 7 某暗网数据交易平台有人宣称正在售卖一份 * 国公民四要素数据。卖家称该份数据共计四亿条，售价为 4,000 美元。给出的样例中包含的字段有：姓名，电话，地址，身份证号。



第三章 勒索软件和黑客组织

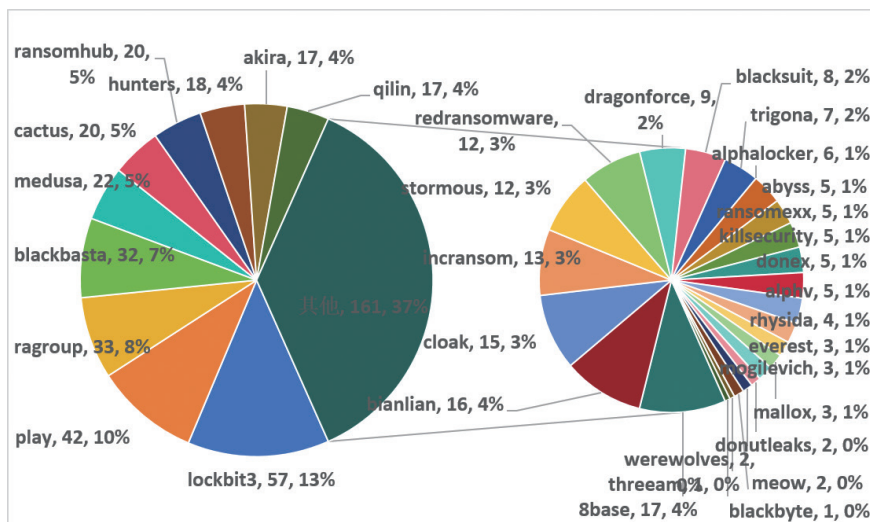
1、活跃商业黑客组织综述

2024 年 3 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 439 件，TOP 10 的黑客组织如下所示：

数世咨询 X ESEC 活跃商业黑客组织 TOP10			
排名	组织标识	组织名称	发布数量
1		lockbit3	65
2		play	42
3		ragroup	33
4		Black basta	32
5		medusa	22
6		cactus	20
7		Ransomhub	20
8		Hunters international	18
9		Akira	17
10		qilin	17

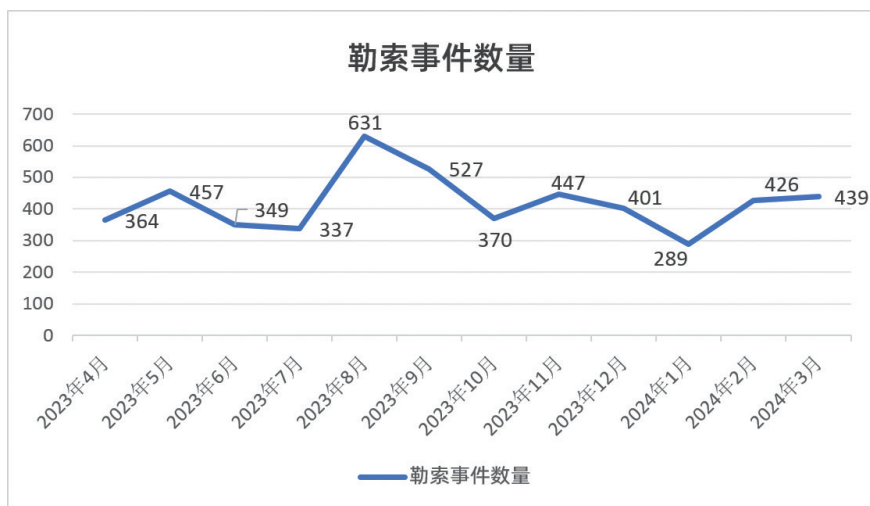
—来自2024年3月《数据泄露态势》

TOP 10 的商业黑客组织公开发布的勒索事件占全部事件的 64%，如下所示：

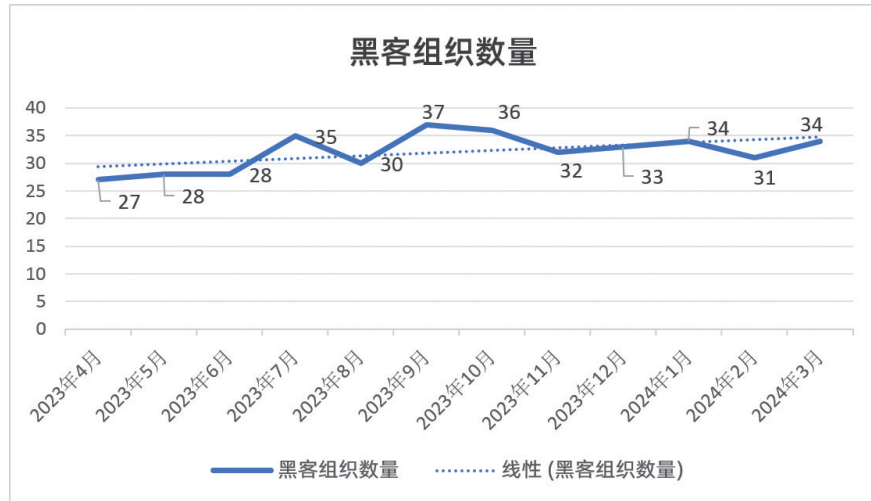


2、黑客组织活跃度趋势

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增加），整体活跃度趋势正在逐步增加，统计末端（2024 年 3 月）达到一年前统计前端（2023 年 4 月）的 126.9%：



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：



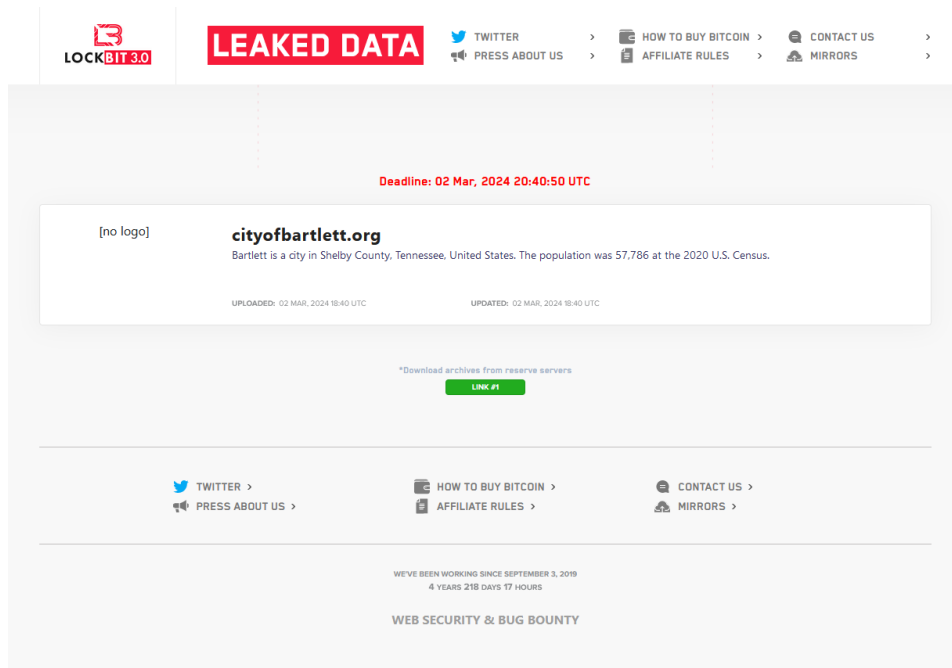
3、本月典型事件说明

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
water.cc	美国水能源组织 Living Water International	2024/3/4	Lockbit3
cityofbartlett.org	美国田纳西州谢尔比县下属 城市 Bartlett	2024/3/2	Lockbit3
SIEA	斯洛伐克创新与能量署 (SIEA)	2024/3/8	Ransomhub
gpaa.gov.za	南非政府养老金管理局 (GPAA)	2024/3/11	Lockbit3
UNDP	联合国开发计划署	2024/3/27	8base
Lawrence Semiconductor Research Laboratory	美国劳伦斯半导体研究实验室	2024/3/27	8base
mckimcreed.com	MCKIM & Creed	2024/3/25	Lockbit3
https://www.carri.com	美国开利公司	2024/3/26	Alphalocker
Premier Technology	卓越技术	2024/3/11	8base
Continental Aerospace Technologies	大陆航空航天技术	2024/3/6	Play

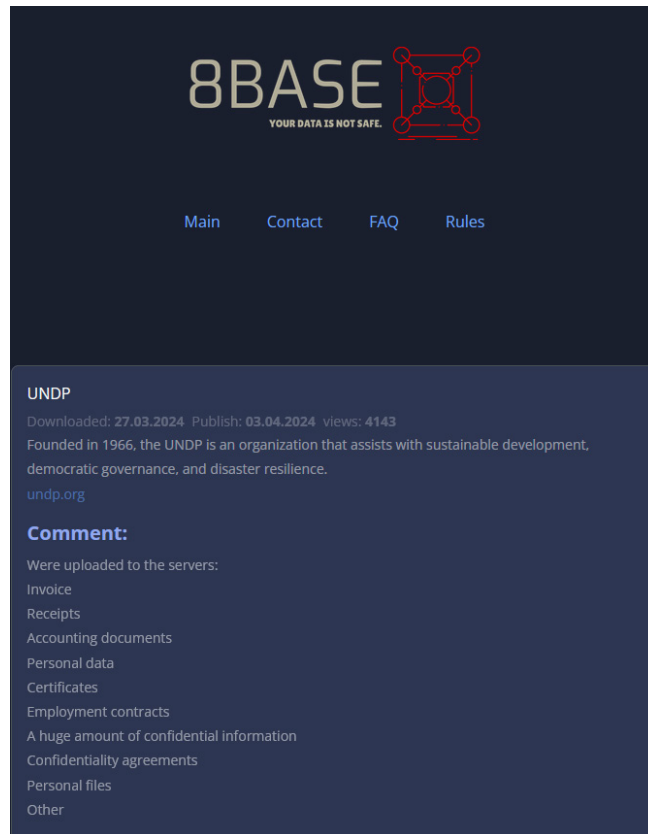
（1）美国田纳西州谢尔比县下属城市 Bartlett

商业黑客组织 lockbit3 在 2024. 3. 2 公布了美国田纳西州谢尔比县下属城市 Bartlett 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，随后 lockbit3 公布了窃取到的所有数据。



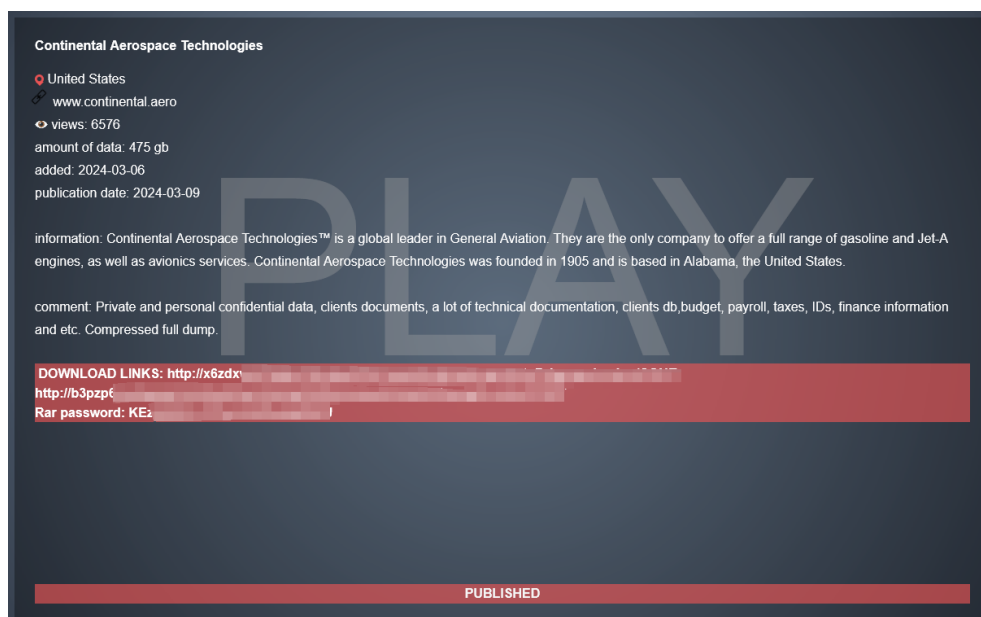
（2）联合国开发计划署

商业黑客组织 8base 在 2024. 3. 4 公布了联合国开发计划署被勒索的信息。该部门未按照勒索组织的要求在规定期限内支付赎金，8base 于 3. 27 公布了窃取到的所有数据。



(3) 大陆航空航天技术

商业黑客组织 play 在 2024. 3. 6 公布了大陆航空航天技术被勒索的信息。该部门未按照勒索组织的要求在规定期限内支付赎金，play 于 3. 9 公布了窃取到的所有数据。



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
A***L	制造业	2024/3/18	Hunters
*****电子有限责任公司	制造业	2024/3/19	Trigona
三***通信	信息与互联网	2024/3/5	Lockbit3
科*****科技有限公司	制造业	2024/3/7	Bianlian

■ 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（BianLian）

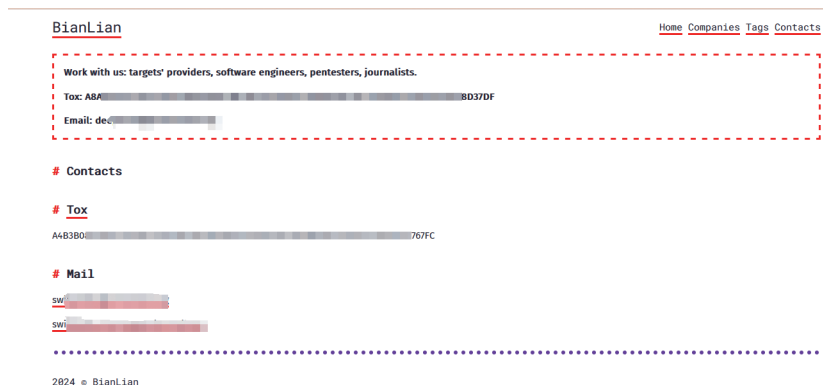
由于国内安全行业尚处于从以合规为目标向实战化攻防的转型初期，我们计划在每期报告中对一个典型的商业黑客组织进行科普性介绍，以普遍增加从业人员对勒索软件和黑客组织的认知度。

已经介绍过的黑客组织有：Lockbit3, Royal, Play, Rhysida, Alphv, 8base, Hunters International 如需了解请翻阅往期报告。

本期介绍 BianLian 黑客组织。BianLian 勒索软件行动始于 2021 年底，攻击和技术持续发展到 2024 年。该黑客组织进行双重勒索行动：要求支付解密器费用以及不公开被盗数据。该黑客组织托管一个 TOR 的公共博客，用于发布受害者身份和被盗数据。在勒索初始阶段，BianLian 并不会公开被害者的公司名称，只会写出该公司的简介。BianLian 黑客组织针对多个行业，几乎没有任何歧视。攻击对象多数为制造业但也会对医疗保健、教育和政府实体实施攻击。BianLian 的文件加密速度极快，全盘加密可能只需要几分钟甚至几秒。受害者在注意到发生异常情况之前就已完全加密。BianLian 受害者被指示通过 TOX 或安全的 onionmail 地址与其进行接触。以下是 BianLian 官网页面：



BianLian 黑客组织在其官方网站留下了 tox 和邮箱联系方式以供受害者来联系他们：



BianLian 黑客组织会对受害者的规模以及收入综合进行评估以此来决定

勒索金额。BianLian 的官网对于受害者的标签分类相较于其他黑客组织显得非常清晰，会对受害者进行国家、行业以及公司所开展业务领域进行分类。并且在勒索不成释放数据时也会按照数据的类型进行分类归纳：

BianLian

Home Companies Tags Contacts

Work with us: targets' providers, software engineers, pentesters, journalists.

Tox: ABAD0FD4C31CDA1408D5A60CBF38CEDF46B41E19AB55AEF1F1848AF3416AE52D278D37DF

Email: deepmind@onionmail.org

is an industry leader in underground pipeline construction. Established in 1991, is a 100% employee owned company (ESOP) with a huge emphasis on employee growth.

CEO: Craig Danley

Business email:

Mobile Phone: +1 (562) 239-55-63

Vice President / CFO: Tom Case

Business email:

Mobile Phone: +1 (949) 702-73-26

Vice President / CFO: Richard Vance

Business email:

Mobile Phone: +1 (909) 630-6863

Office Manager and Special Projects Coordinator: Julie Danley

Business email:

Mobile Phone: +1 (562) 712-20-98

HR & Personal

1stprof, hr_personal_1.zip, 1stprof, hr_personal_2.zip

Email archives

1stprof, al.com_mail_1.zip 1stprof, al.com_mail_2.zip 1stprof, al.com_mail_3.zip 1stprof, al.com_mail_4.zip 1stprof, al.com_mail_5.zip 1stprof, al.com_mail_6.zip 1stprof, al.com_mail_7.zip 1stprof, al.com_mail_8.zip 1stprof, al.com_mail_9.zip 1stprof, al.com_mail_10.zip 1stprof, al.com_mail_11.zip 1stprof, al.com_mail_12.zip 1stprof, al.com_mail_13.zip 1stprof, al.com_mail_14.zip 1stprof, al.com_mail_15.zip

Medical data

1stprof, al.com_medical_1.zip 1stprof, al.com_medical_2.zip 1stprof, al.com_medical_3.zip 1stprof, al.com_medical_4.zip 1stprof, al.com_medical_5.zip

Private & Confidential

1stprof, al.com_private_confidential_1.zip 1stprof, al.com_private_confidential_2.zip

Technical data

1stprof, al.com_technical_1.zip 1stprof, al.com_technical_2.zip 1stprof, al.com_technical_3.zip 1stprof, al.com_technical_4.zip 1stprof, al.com_technical_5.zip 1stprof, al.com_technical_6.zip 1stprof, al.com_technical_7.zip 1stprof, al.com_technical_8.zip 1stprof, al.com_technical_9.zip 1stprof, al.com_technical_10.zip 1stprof, al.com_technical_11.zip 1stprof, al.com_technical_12.zip 1stprof, al.com_technical_13.zip 1stprof, al.com_technical_14.zip 1stprof, al.com_technical_15.zip 1stprof, al.com_technical_16.zip 1stprof, al.com_technical_17.zip 1stprof, al.com_technical_18.zip 1stprof, al.com_technical_19.zip 1stprof, al.com_technical_20.zip 1stprof, al.com_technical_21.zip 1stprof, al.com_technical_22.zip 1stprof, al.com_technical_23.zip 1stprof, al.com_technical_24.zip 1stprof, al.com_technical_25.zip 1stprof, al.com_technical_26.zip 1stprof, al.com_technical_27.zip 1stprof, al.com_technical_28.zip 1stprof, al.com_technical_29.zip 1stprof, al.com_technical_30.zip 1stprof, al.com_technical_31.zip 1stprof, al.com_technical_32.zip 1stprof, al.com_technical_33.zip 1stprof, al.com_technical_34.zip 1stprof, al.com_technical_35.zip 1stprof, al.com_technical_36.zip 1stprof, al.com_technical_37.zip 1stprof, al.com_technical_38.zip 1stprof, al.com_technical_39.zip 1stprof, al.com_technical_40.zip 1stprof, al.com_technical_41.zip 1stprof, al.com_technical_42.zip

The rest data coming soon.

usa

medicine

it

21

第四章 匿名社交社群

3 月份监控到匿名社交社群情报总数量 11,410,547 条，提供的有效数据泄露样例下载 942 份。涉及到我国数据泄露的内容包括：基层事业单位人员信息、银行、网购、机票、股票、学生和家長信息、投资、公积金、装修信息、社保信息等众多类型。

以下随机选取展示部分样本：

731	478	淮	440883	00	50	F8	2	泸州	2024-03-1	深圳	2024-03-1	662.4	1871	1	男
479	814	江	320504	00	15	H9	1	沈阳	2024-03-1	南京	2024-03-1	694.9	1890	2	男
731	886	家	321181	51	170	F8	0	运城	2024-03-1	南京	2024-03-1	432.1	1516	0	男
731	537	凝	142724	00	105	F8	0	运城	2024-03-1	南京	2024-03-1	864	1503	7	男
731	709	勤	142623	61	164	F8	0	运城	2024-03-1	南京	2024-03-1	432	1553	1	女
731	732		142631	39	174	F8	0	运城	2024-03-1	南京	2024-03-1	865.8	1503	1	男
731	167		142701	34	130	F8	0	运城	2024-03-1	南京	2024-03-1	432	1801	34	男
859	180	晴	32132	92	87	L9	0	贵阳	2024-03-1	徐州	2024-03-1	690	1515	70	女
324	470	琦	42011	93	77	C4	7	青岛	2024-03-1	普陀山	2024-03-1	729.9	1582	77	女
324	702	莹	37130	96	60	C7	7	青岛	2024-03-1	普陀山	2024-03-1	1459.8	1526	31	女
324	000		37028	89	91	C7	7	青岛	2024-03-1	普陀山	2024-03-1	729.9	1866	29	男
324	176	安	43030	173	32	C3	3	烟台	2024-03-1	重庆	2024-03-1	512.4	1392	46	男
324	856	清	37021	186	72	C7	7	青岛	2024-03-1	普陀山	2024-03-1	729.9	1396	99	男
324	364	萍	37066	190	210	C3	3	烟台	2024-03-1	重庆	2024-03-1	1024.8	1386	37	女
731	259		42011	189	234	M4	14	杭州	2024-03-1	深圳	2024-03-1	1012	1329	32	男
731	276	诚	33050	190	169	M4	14	杭州	2024-03-1	深圳	2024-03-1	1012	1515	02	男
731	561	发	32011	198	172	M4	14	杭州	2024-03-1	深圳	2024-03-1	1012	1356	67	男
85	791	李	42231	198	252	L3	3	景洪	2024-03-1	大理	2024-03-1	630	180	66	男
4	845	李	3402	198	178	H	9	深圳	2024-03-1	南京	2024-03-1	665.3	182	23	女
7	413	月	3506	00	024	M4	18	三亚	2024-03-1	厦门	2024-03-1	2774	173	388	女
8	386	勤	4101	96	1066	D1	2	呼和浩特	2024-03-1	郑州	2024-03-1	365	135	823	男
7	708	李	6204	96	1150	M4	14	兰州	2024-03-1	衡阳	2024-03-1	602	18	588	男
8	931	刘	3624	91	2110	L1	2	南京	2024-03-1	赣州	2024-03-1	1132	15	2579	男
8	622	梁	3621	19	3140	L1	2	南京	2024-03-1	赣州	2024-03-1	1146	13	4947	男

姓名	性别	身份证号	出生日期	身份证到期时	婚姻状况	民族	签发机关	手机号	邮箱	政治面貌	从业状况	籍贯	联系地址	监护人姓名	监护人身份证号	监护人手机号	所属学院	学校
李	男	118	1999-12-31	2099-12-31	未婚	汉族	贵阳市公安局	188 112	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	211	17 1574-05-17	职业技术学院	职业技术学院
李	男	0001	1999-08-26	2027-07-05	未婚	汉族	市公安局	188 823	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	211	104 1574-10-04	职业技术学院	职业技术学院
李	男	0001	1999-11-08	2027-08-29	未婚	汉族	市公安局	871 071	qq	群众	学生	贵州省贵阳市	贵阳市	李	001	12 1968-08-12	职业技术学院	职业技术学院
李	男	0001	1999-09-02	2029-11-20	未婚	汉族	市公安局	852 852	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	18 1574-10-18	职业技术学院	职业技术学院
李	男	0001	1999-11-10	2030-02-17	未婚	汉族	市公安局	888 1566	qq	群众	学生	贵州省贵阳市	贵阳市	李	001	25 1977-12-25	职业技术学院	职业技术学院
李	男	0001	1999-05-07	2099-12-31	未婚	汉族	市公安局	850 998	qq	群众	学生	贵州省贵阳市	贵阳市	李	221	21 1573-10-21	职业技术学院	职业技术学院
李	男	0001	1999-12-10	2028-07-06	未婚	汉族	市公安局	668 904	qq	群众	学生	贵州省贵阳市	贵阳市	李	001	21 1972-01-21	职业技术学院	职业技术学院
李	男	0001	1999-07-18	2099-12-31	未婚	汉族	市公安局	133 501	qq	其他	学生	贵州省贵阳市	贵阳市	李	001	08 1576-10-08	职业技术学院	职业技术学院
李	男	0001	1999-08-30	2099-12-31	未婚	汉族	市公安局	50 051	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	13 1969-10-13	职业技术学院	职业技术学院
李	男	0001	1999-10-05	2099-12-31	未婚	汉族	市公安局	27 857	qq	群众	学生	贵州省贵阳市	贵阳市	李	001	17 1967-02-17	职业技术学院	职业技术学院
李	男	0001	1999-10-26	2030-01-31	未婚	汉族	市公安局	177 303	qq	其他	其他	贵州省贵阳市	贵阳市	李	001	12 1957-11-12	职业技术学院	职业技术学院
李	男	0001	1999-08-02	2028-06-29	未婚	汉族	贵阳市公安局	871 004	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	08 1963-07-08	职业技术学院	职业技术学院
李	男	0001	1999-07-28	2028-07-03	未婚	汉族	贵阳市公安局	64 101	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	14 1973-10-14	职业技术学院	职业技术学院
李	男	0001	1999-11-01	2026-06-06	未婚	汉族	市公安局	936 1225	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	12 1971-01-27	职业技术学院	职业技术学院
李	男	0001	1999-04-01	2019-12-21	未婚	汉族	贵阳市公安局	177 8215	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	04 1968-04-26	职业技术学院	职业技术学院
李	男	0001	1999-10-02	2099-12-31	未婚	汉族	广东省公安厅	250 1452	qq	共青团员	学生	贵州省贵阳市	贵阳市	李	001	0901 1969-09-01	职业技术学院	职业技术学院

320	196	黄强	1391	1319	吴中	直镇	长巨村委	主任助理	1987	男	江苏苏州市
341	196	刘公	1801	321	琅琊	洞街道	事处新集	工作者	1987	男	安徽滁州市
3304	196	蔡昌	1586	775	干奎	人民政府		一般办事人	1988	男	浙江嘉兴市
3208	196	蒋	1391	991	常熟	雪溪新	桥村村民	副主任	1981	男	江苏苏州市
3208	196	张明	1377	947	相城	太平街	澄社区	副书记	1981	男	江苏苏州市
3501	196	林	1395	399	福清	屏街	大社区	党工委宣	1989	男	福建福州市
3306	196	陈	1361	023	杭州	工干区	街道景华	科员	1987	男	浙江绍兴市
1201	96	曹	1350	402	天津	青区	北镇溪悦园	窗口	1984	男	天津市辖区
3202	97	曹	1309	567	无锡	美蓉管		办公室科	1976	男	江苏无锡市
3207	96	曹	1800	919	路南	首公园		党政办	1987	男	江苏连云港市
3304	96	曹	1375	138	中共	市委		党政综合	1983	男	浙江嘉兴市
3302	96	曹	1377	006	宁波	真海区	街道后施	建设办公	1980	男	浙江宁波市
1101	96	曹	1369	67	朝阳	东风地	佛营南里	党政综合	1980	男	北京市辖区
3209	197	兵	1377	58	黄涛	汤社区	委员会	党委副书记	1971	男	江苏盐城市
120	196	曹	1590	82	天津	南开区	路街延长	党政办公	1987	男	天津市辖区
3426	197	曹	1373	080	宁波	工东区	街道新源	党务办副	1977	男	安徽巢湖市
3208	196	曹	1866	245	元和	道姚祥		党政办公	1987	男	江苏苏州市
3208	97	曹忠	1392	772	张家	市塘桥	村村委会	主任	1978	男	江苏苏州市
1101	96	曹	1510	513	丰台	总工会		办事处副	1987	男	北京市辖区
1102	96	曹	1346	067	北京	通州区	镇绿茵小	一般办事	1986	男	北京市县
5101	97	曹	1388	782	天府	区太平	镇小堰村	村经联委	1972	男	四川成都市
1101	97	曹	1352	958	东城	东四二	居委会	党政办	1971	男	北京市辖区
1101	197	曹	1367	046	垡头	区社区		宣传干事	1974	男	北京市辖区
120	196	曹	1512	641	天津	可西区	每街道三	水科	1984	男	天津市辖区
320	196	曹	1322	66	盐力	道吴仲	委会	党政办	1984	男	江苏盐城市
110	197	曹	1368	62	北京	丰台区	罗园街道	马党政办	1972	男	北京市辖区
500	196	曹	1350	60	重庆	南岸区	医院	党政办科	1989	男	重庆市辖区
339	197	曹	1826	80	杭州	五愿	委会	党政办公	1979	男	浙江省直辖行政单位
330	1196	曹	1515	6	潮鸣	道刀	社区	党工委办	1982	男	浙江杭州市
110	5196	曹	1314	3	太阳	地区	药居四社	居基层事	1981	男	北京市辖区

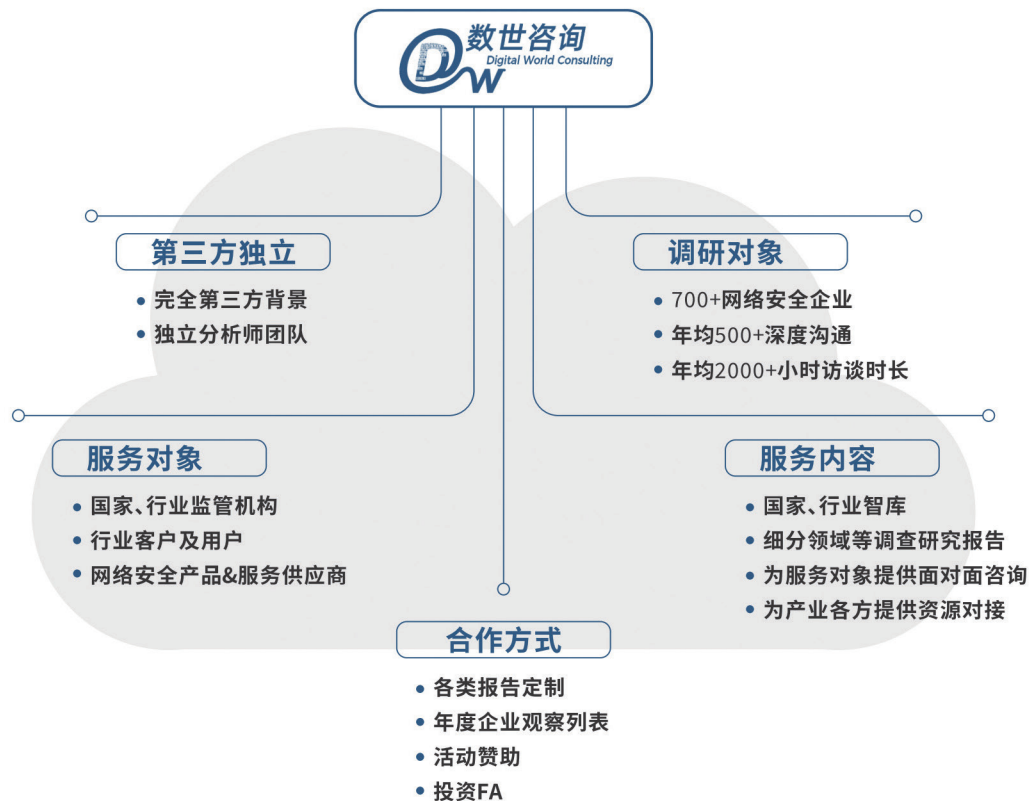
1368	7492	孙	1327	112	20	女	1971	PR201	6509581	人	寿保险有	限公司	河北	中国移	上海	上海
1596	9087	周	320	011	53	女	1969	PR201	8604910	人	寿保险有	限公司	江苏	中国移	江苏	苏州
1375	7845	车	132	050	50	女	1973	PR201	5381400	人	寿保险有	限公司	河北	中国移	天津	天津
1366	4828	朱	33	080	24	女	1975	PR201	3068232	人	寿保险有	限公司	浙江	中国移	浙江	台州
1317	7886	沈	33	030	28	女	1972	PR201	9268175	人	寿保险有	限公司	浙江	中国联	浙江	绍兴
18060	599	陈	350	100	1	女	1975	PR201	832538	人	寿保险有	限公司	福建	中国电	福建	福州
13930	592	高	130	3061	0	女	1973	PR201	750548	人	寿保险有	限公司	河北	中国移	河北	石家庄
13774	028	曹	42	1011	0	女	1975	PR201	937281	人	寿保险有	限公司	湖北	中国移	湖北	荆门
13736	578	钱	330	1032	2	女	1971	PR201	2670920	人	寿保险有	限公司	浙江	中国移	浙江	嘉兴
13597	704	洪	452	5010	6	女	1975	PR201	565876	人	寿保险有	限公司	广西	中国移	广西	玉林
15381	596	陈	330	2111	6	女	1972	PR201	942032	人	寿保险有	限公司	浙江	中国电	浙江	杭州
18230	988	李	130	122	7	女	1971	PR201	618276	人	寿保险有	限公司	河北	中国移	河北	秦皇岛
15324	550	张	410	0061	20	女	1970	PR201	304643	人	寿保险有	限公司	河南	中国电	河南	郑州
13012	747	叶	352	8040	14	女	1968	PR201	2493674	人	寿保险有	限公司	福建	中国联	上海	上海
15957	295	顾	330	1031	5X	女	1971	PR201	2066008	人	寿保险有	限公司	浙江	中国移	浙江	杭州
15860	823	王	350	0031	0X	女	1970	PR201	8896991	人	寿保险有	限公司	福建	中国移	福建	福州
18782	275	梅	510	4032	47	女	1974	PR201	1752389	人	寿保险有	限公司	重庆	中国移	四川	成都
15252	328	陈	321	0122	49	女	1970	PR201	00893405	人	寿保险有	限公司	江苏	中国移	江苏	扬州
15054	712	陈	372	0072	04	女	1975	PR201	78481766	人	寿保险有	限公司	山东	中国移	山东	临沂
136130	59	曹	61	512	26	女	1975	PR201	34075095	人	寿保险有	限公司	陕西	中国移	广东	深圳
136689	56	柳	44	112	24	女	1971	PR201	59529173	人	寿保险有	限公司	广东	中国移	广东	广州
137711	35	峰	32	505	024	女	1975	PR201	17657384	人	寿保险有	限公司	江苏	中国移	江苏	无锡
138192	51	王	33	808	023	女	1968	PR201	85026774	人	寿保险有	限公司	浙江	中国移	浙江	湖州
136563	50	曹	37	110	148	女	1971	PR201	78941073	人	寿保险有	限公司	山东	中国移	山东	聊城
186010	78	曹	41	502	529	女	1975	PR201	73237508	人	寿保险有	限公司	河南	中国联	北京	北京
18796	99	曹	32	512	067	女	1975	PR201	16928203	人	寿保险有	限公司	江苏	中国移	江苏	徐州
13577	528	曹	53	5905	340	女	1969	PR201	5630257	人	寿保险有	限公司	云南	中国移	云南	大理
18001	338	曹	32	7210	129	女	1972	PR201	11011124	人	寿保险有	限公司	江苏	中国电	江苏	南通
13891	636	曹	61	5805	208	女	1968	PR201	2924885	人	寿保险有	限公司	陕西	中国移	陕西	西安
13072	622	曹	42	7509	529	女	1975	PR201	8977257	人	寿保险有	限公司	湖北	中国联	湖北	武汉
15065	456	曹	37	7506	524	女	1975	PR201	0704850	人	寿保险有	限公司	山东	中国移	山东	济南
1385	208	曹	35	7206	121	女	1972	PR201	79068548	人	寿保险有	限公司	福建	中国移	福建	宁德
1391	5525	曹	32	7002	726	女	1970	PR201	35694900	人	寿保险有	限公司	江苏	中国移	江苏	苏州

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 900 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 10,092 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：

86 [REDACTED] 740	7990
86 [REDACTED] 590	576
86 [REDACTED] 2781	78
86 [REDACTED] 7194	72
86 [REDACTED] 0874	70
86 [REDACTED] 777	39
86 [REDACTED] 600	38
86 [REDACTED] 59	29
86 [REDACTED] 56	27
86 [REDACTED] 81	27

* 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



