Cybercriminals leaked massive volumes of stolen PII data from Thailand in Dark Web

Back

Cyber Threat Intelligence

22 Jan 2024

data leak, data breach, personal data protection, PII, APAC, Thailand

Massive Leak of Stolen Thai PII Data on Dark Web by Cybercriminals

Recently, the Criminal Court in Thailand issued an order to block the website 9near.org. This action was taken after the site threatened to disclose the personal information of **55 million Thai citizens**, allegedly obtained from vaccine registration records. The court further declared that any other websites found distributing data from "9near.org" would also face blocking. This measure follows a request from the **Digital Economy and Society (DES) Ministry**, which is preparing for the likely apprehension of the individual responsible for the hack.

The person running the website, who goes by "**9Near – Hacktivist**", made an announcement on the Breach Forum website, claiming they had accessed personal details of **55 million people from Thailand**. This data includes full names, birthdates, ID card numbers, and phone numbers. Recently, the Rural Doctors Society suggested that this information might have originated from a leak at the **Public Health Ministry's Immunization Centre**.

Thailand is swiftly becoming a key player in the digital arena, particularly in the field of **Information and Communication Technology (ICT)**, within the Asia-Pacific region. Notably, from the latter part of 2022 to the early months of 2023, there's been a significant drop in incidents of data breaches in the country. To put it in perspective, during the third quarter of 2022, for every thousand people in Thailand, about 6.8 instances of data exposure were recorded. Impressively, this number plummeted to just 1 per thousand by the first quarter of 2023. But as we step into 2024, this trend might see a change. There are reports of cybercriminals, known in the shadowy corners of the Dark Web as **Naraka**, circulating large amounts of stolen personal identifiable information (PII) of Thai citizens. It's believed that these sensitive details were sourced from various breached platforms.

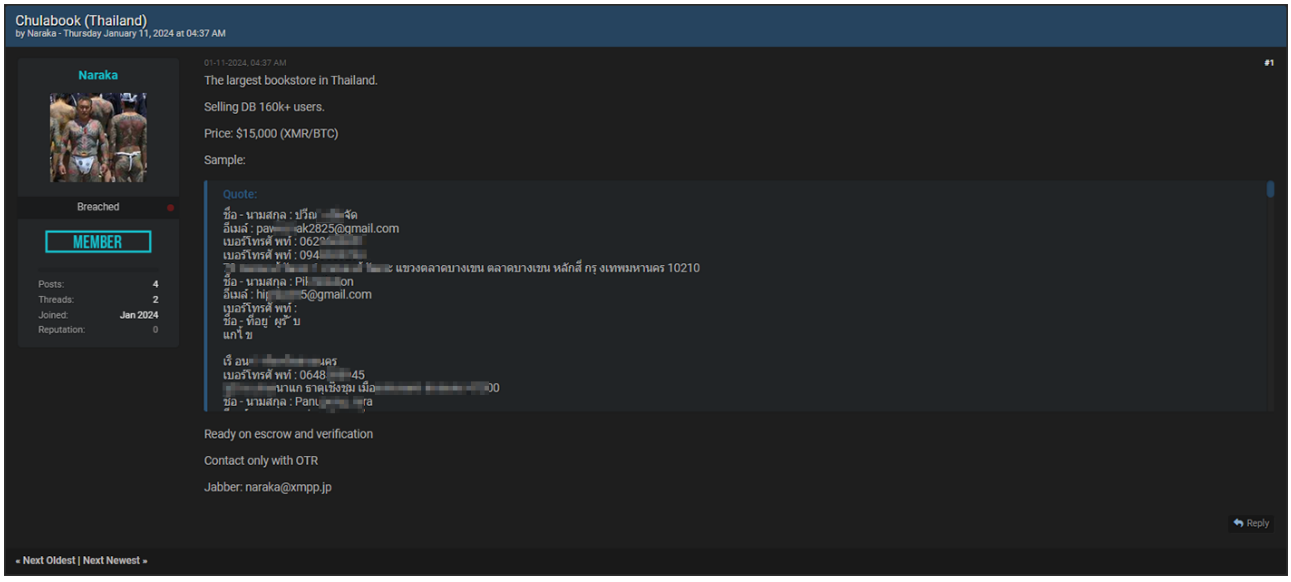
- The beginning of 2024 saw a noticeable increase in data leaks from consumer-focused platforms, confirming that threat actors are actively targeting the personal data of Thai citizens.

- Threat actors target Thai-based e-commerce, fintech and government resources due to a large presence of personal documents both in text and graphical form used for KYC ("Know Your Customer").

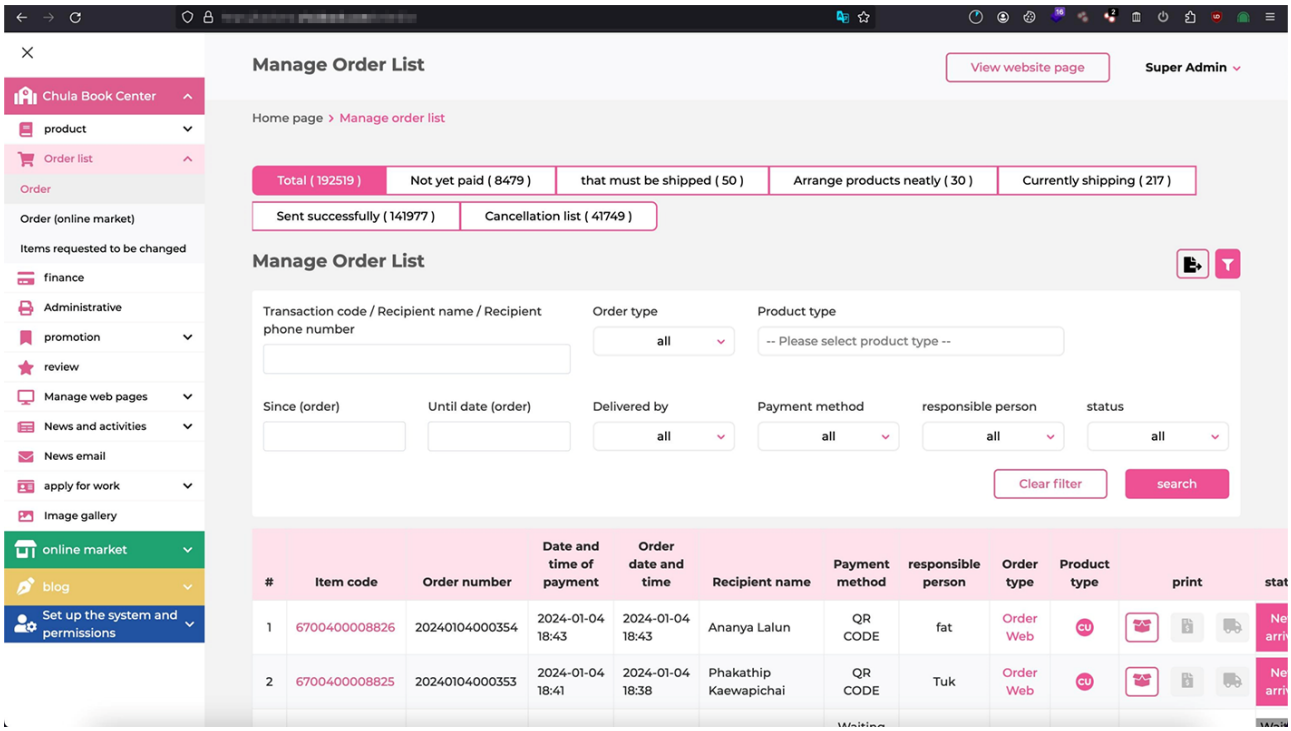
- Compared to 2023, there has been an increase in the frequency of attacks, as evidenced by the rising number of leaked data incidents involving consumers and businesses from Thailand on the Dark Web. In the early part of January 2024 alone, at least 14 significant data breaches exposing citizens' information were posted on cybercriminal forums, nearly surpassing the annual volume of compromised records identified last year.

- Bad actors use stolen PII data to defraud Thai citizens and attack financial organizations, which are actively developing and cultivating digitization in the region to service 71.6 million people population.

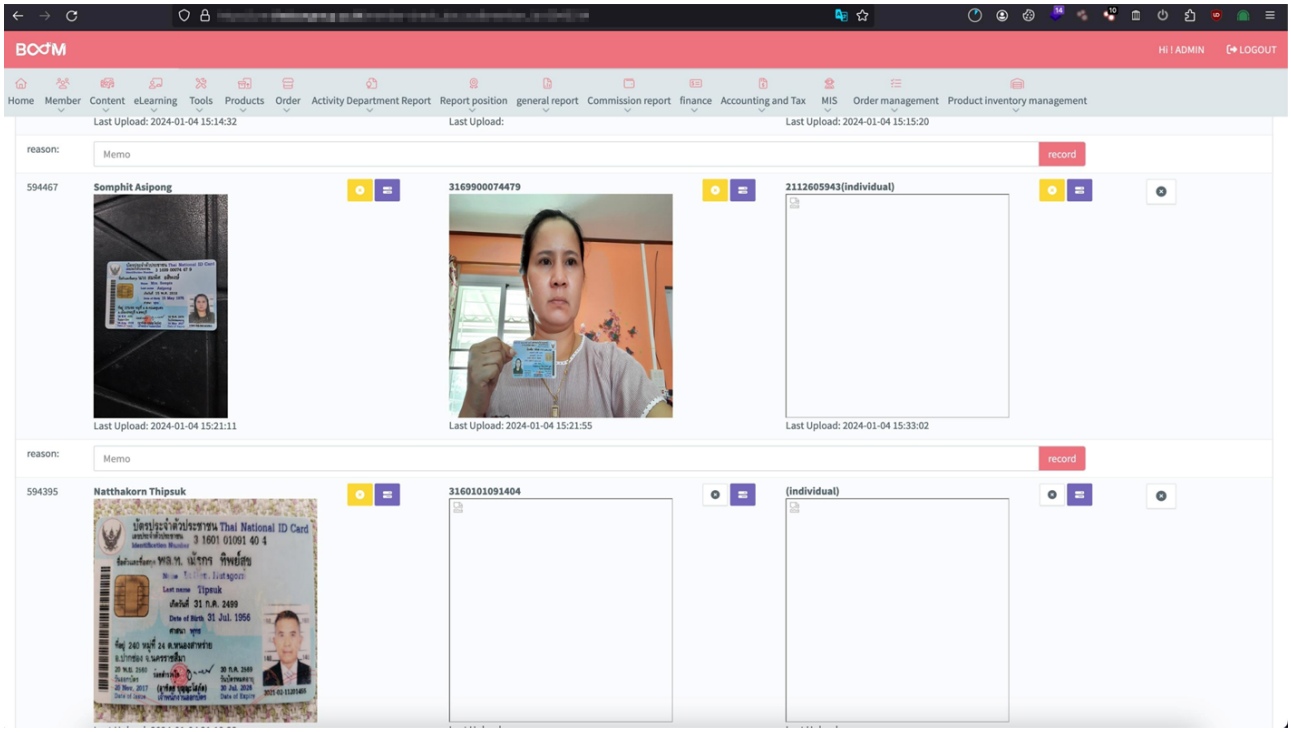
On **January 11th, 2024**, an individual known as **Naraka** listed a data dump for sale on **breachforums.is**, featuring one of Thailand's largest bookstores called Chulabook. This breach affected over **160,000 users**. Naraka specified payment in cryptocurrencies, specifically XRM (Monero) or BTC (Bitcoin).

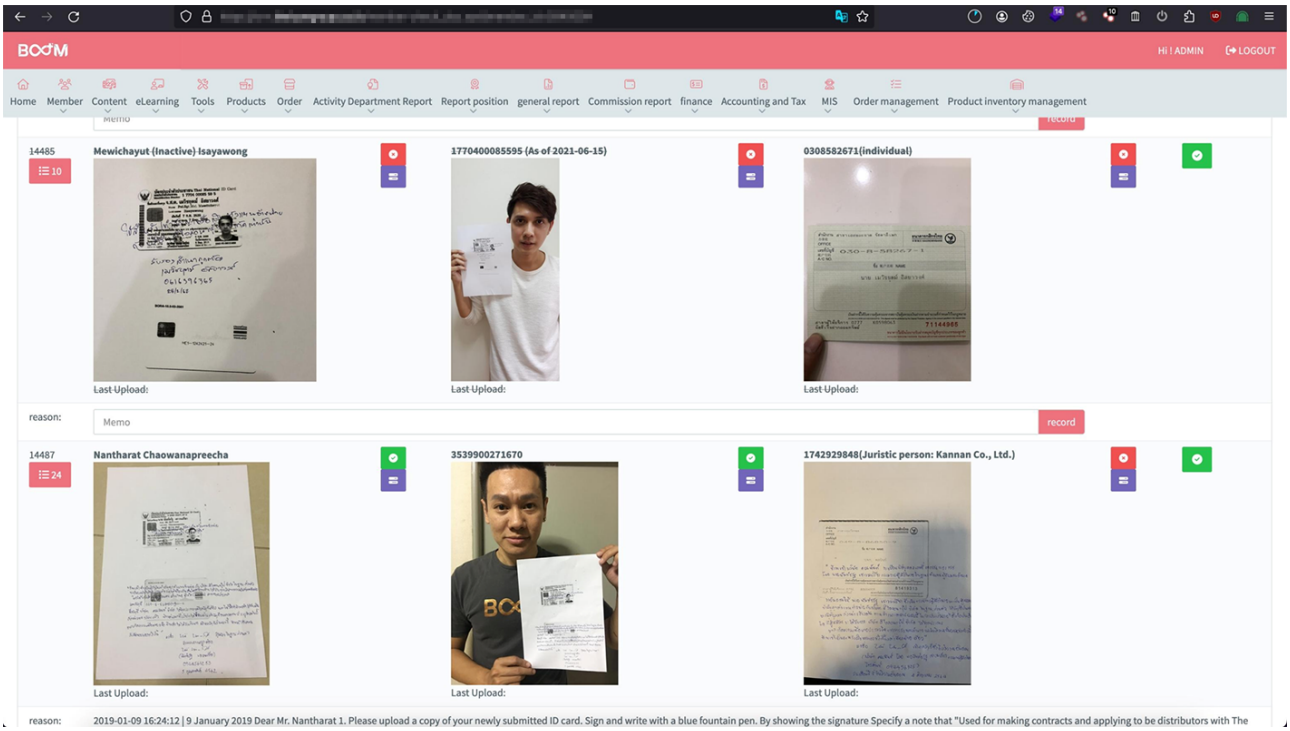


Resecurity alerted Chulabook and the Electronic Transactions Development Agency (ETDA), a government agency under the supervision of the Ministry of Digital Economy and Society responsible for the oversight of All Digital Service Providers who offer services to customers in Thailand. Our team acquired additional artifacts from the actor confirming successful access to the backend containing thousands of orders and customer records.



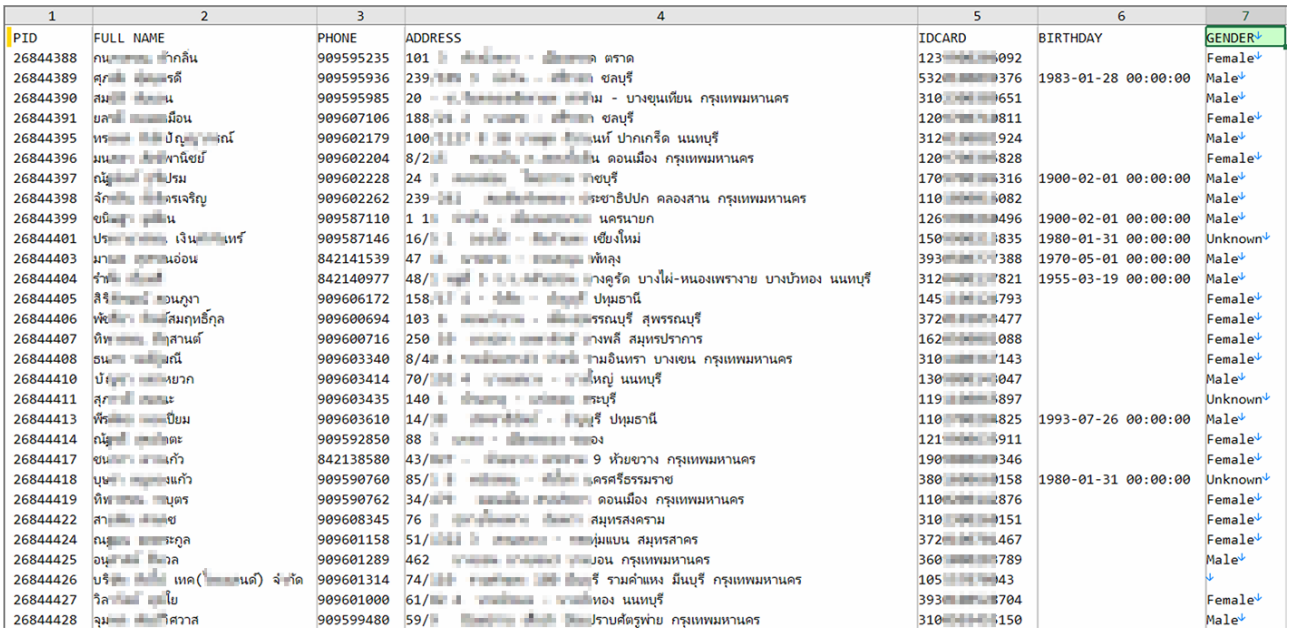
During interactions with the actor involved in the data breach, another compromised web resource in Thailand was identified. This additional breach was also found to be leaking personal identifiable information (PII) of Thai citizens.





Right before the New Year's Eve celebrations, it was discovered that the operators of the **UFO Market on Telegram** were actively selling stolen data. This compromised data included a staggering **538,418 records** featuring personal identifiable information (PII) of individuals, encompassing details like citizens' ID card numbers.

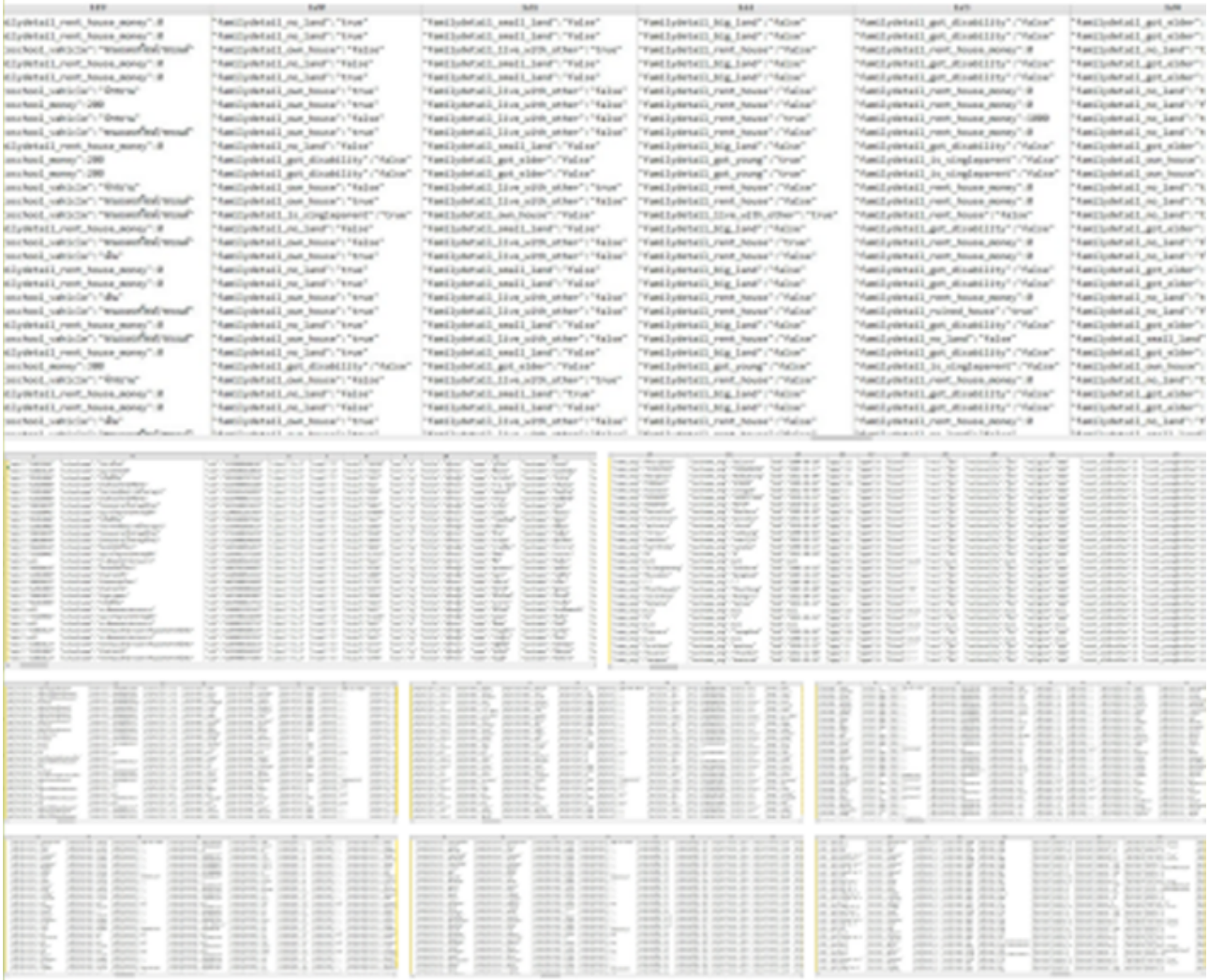
These large collections of stolen data are particularly prized by those involved in identity theft and financial fraud. The detailed personal information they contain provides these individuals with a comprehensive view of potential targets for online banking fraud and various internet scams.



1	2	3	4	5	6	7
PID	FULL NAME	PHONE	ADDRESS	IDCARD	BIRTHDAY	GENDER
26844388	กน[illegible]ก้ากลิน	909595235	101 [illegible] ตราด	123[illegible]092		Female
26844389	ศุภ[illegible]รดี	909595936	239[illegible] ชลบุรี	532[illegible]376	1983-01-28 00:00:00	Male
26844390	สม[illegible]น	909595985	20 [illegible]ม - บางขุนเทียน กรุงเทพมหานคร	310[illegible]651		Male
26844391	ยส[illegible]เมือน	909607106	188[illegible] ชลบุรี	120[illegible]811		Female
26844395	ทร[illegible]ปัญ[illegible]ณ์	909602179	100[illegible]นท์ ปากเกร็ด นนทบุรี	312[illegible]924		Male
26844396	มน[illegible]พานิชย์	909602204	8/2[illegible]น ดอนเมือง กรุงเทพมหานคร	120[illegible]828		Female
26844397	ณัฐ[illegible]ปรม	909602228	24 [illegible]ชบุรี	170[illegible]316	1900-02-01 00:00:00	Male
26844398	จักร[illegible]รเจริญ	909602262	239[illegible]ระชาธิปปก คลองสาน กรุงเทพมหานคร	110[illegible]082		Male
26844399	ชนิ[illegible]น	909587110	1 1[illegible] นครนายก	126[illegible]496	1900-02-01 00:00:00	Male
26844401	ประ[illegible] เงิน[illegible]เทร์	909587146	16/[illegible] เชียงใหม่	150[illegible]835	1980-01-31 00:00:00	Unknown
26844403	มาล[illegible]นอ่อน	842141539	47 [illegible]พัทลุง	393[illegible]388	1970-05-01 00:00:00	Male
26844404	ร่ำ[illegible]	842140977	48/[illegible]างคูรัด บางไผ่-หนองเพรางาย บางบัวทอง นนทบุรี	312[illegible]821	1955-03-19 00:00:00	Male
26844405	สิริ[illegible] ยอนภูงา	909606172	158,[illegible] ปทุมธานี	145[illegible]793		Female
26844406	พัช[illegible]สมฤทธิ์กุล	909600694	103 [illegible]รรณบุรี สุพรรณบุรี	372[illegible]477		Female
26844407	ทิพ[illegible]ศิสานต์	909600716	250 [illegible]างพลี สมุทรปราการ	162[illegible]088		Female
26844408	ธน[illegible]มณี	909603340	8/4[illegible]ามอินทรา บางเขน กรุงเทพมหานคร	310[illegible]143		Female
26844410	ปัญ[illegible]หยวก	909603414	70/[illegible]ใหญ่ นนทบุรี	130[illegible]047		Male
26844411	สุภ[illegible]ณะ	909603435	140 [illegible]ระบุรี	119[illegible]897		Unknown
26844413	พีร[illegible]ปียม	909603610	14/[illegible]รี ปทุมธานี	110[illegible]825	1993-07-26 00:00:00	Male
26844414	ณัฐ[illegible]ตะ	909592850	88 [illegible]อง	121[illegible]911		Female
26844417	ชน[illegible]แก้ว	842138580	43/[illegible] 9 ห้วยขวาง กรุงเทพมหานคร	190[illegible]346		Female
26844418	บุษ[illegible]แก้ว	909590760	85/[illegible]ครศรีธรรมราช	380[illegible]158	1980-01-31 00:00:00	Unknown
26844419	ทิพ[illegible]บุตร	909590762	34/[illegible] ดอนเมือง กรุงเทพมหานคร	110[illegible]876		Female
26844422	สา[illegible]ย	909608345	76 [illegible] สมุทรสงคราม	310[illegible]151		Female
26844424	ณ[illegible]ระกูล	909601158	51/[illegible]มุ่มแบน สมุทรสาคร	372[illegible]467		Female
26844425	อนุ[illegible]ิวล	909601289	462 [illegible]อน กรุงเทพมหานคร	360[illegible]789		Male
26844426	บริ[illegible] เทค([illegible]นด์) จำกัด	909601314	74/[illegible]รี รามคำแหง มีนบุรี กรุงเทพมหานคร	105[illegible]43		
26844427	วิล[illegible]ไย	909601000	61/[illegible]ทอง นนทบุรี	393[illegible]704		Female
26844428	จุม[illegible]ศิวาส	909599480	59/[illegible]ปราบศัตรูพ่าย กรุงเทพมหานคร	310[illegible]150		Male

Prior to this incident, the same culprits were involved in distributing a massive amount of data, specifically **3,149,330 records** related to students, which is believed to have been illicitly obtained from the **Basic Education Commission (OBEC)**. Such information is especially sensitive and could be highly valuable for nefarious purposes, considering the vulnerabilities of the younger population and the risk of them being targeted by malevolent entities in the online space.

UFO LEAK MARKET



SELLING THAILAND 3.1 MILLION STUDENT DATA Basic Education Commission (OBEC)

TOTAL RECORDS : 3,149,330

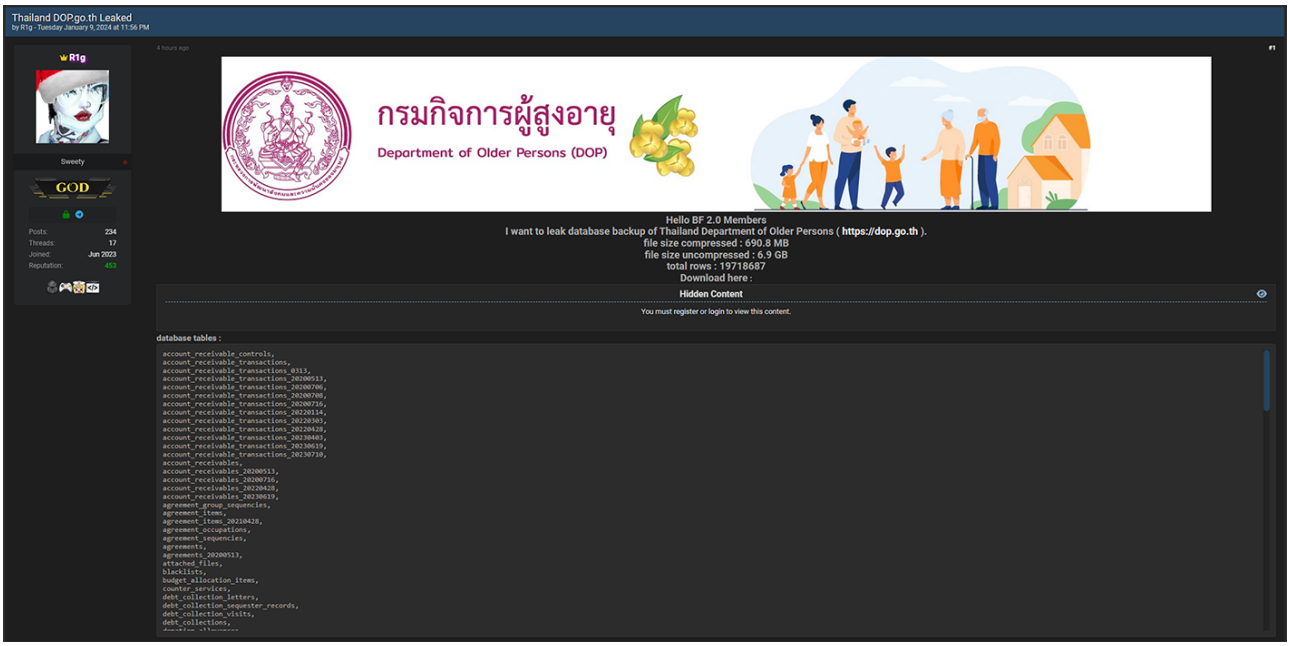
TOTAL SIZE ON DISK : 11.77 GB

Data include but not limited to :

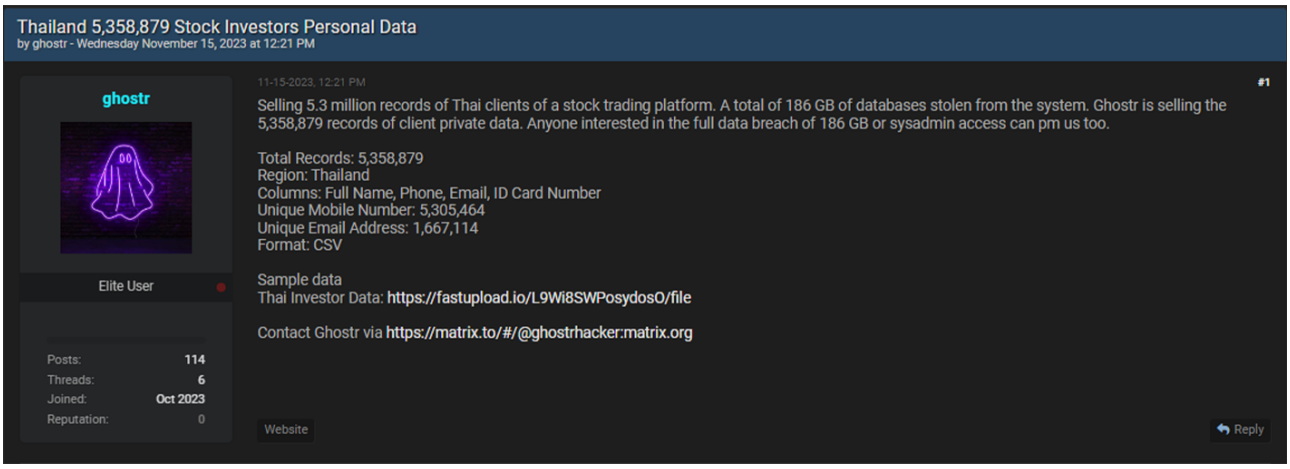
First name, last name, school name, dob, race, nationality, religion, fathername, fatherlastname, fathersalary, fathertel, mothername, motherlastname, mothersalary, mothertel, ptel, registhousecode, studentweight, studentheight, totalincome, familydetail_own_house

Some portions of this data were found being leaked at no cost – the wrongdoers are distributing it on the Dark Web. They're doing this to trade and use it in future schemes like spamming, online scams, and **Business Email Compromise (BEC)** campaigns. This free circulation makes the data more accessible for various malicious activities.

A separate data set was uncovered on a site known as **breachedforums.is**, labeled "**Thailand DOP.go.th Leaked**". This particular set is composed of personal identifiable information (PII) primarily concerning the elderly population in Thailand. It's a substantial collection, around 690MB in size, containing a whopping **19,718,687 rows of data**.



Earlier, a new data breach was revealed by an entity known as **Ghostr** on Breachforums.is. This particular leak was massive, involving about 186GB of data, and included a staggering **5.3 million records** from a stock trading platform. The leaked information encompassed comprehensive details of Thai users, including their full names, phone numbers, email addresses, and ID card numbers.



In a separate incident, a leak was reported by **Milw0rm** on [breachforum.is](). This particular dataset, released on **January 1, 2024**, is to Thai job seekers and includes an extensive range of personal information. The dataset is consists of **61,000 rows**, featuring detailed data such as usernames, passwords, email addresses, mobile and home telephone numbers, zip codes, birthdates, physical attributes like weight and height, current employment status, information about children, typing proficiency in Thai, and salary details.

THAILAND JOB SEEKERS - Dumped 2024

by Milw0rm - Sunday December 31, 2023 at 11:53 PM

Milw0rm

2003-2009

Posts: 58
Threads: 8
Joined: Sep 2023
Reputation: 42

12-31-2023, 11:53 PM (This post was last modified: 01-03-2024, 09:03 AM by Milw0rm.) #1

Hi Guys

❤️ HAPPY NEW YEARS 2024 ❤️

Target country: Thailand

Title: JOB SEEKERS

Records : 61000 rows

Dumped: 1/1/2024

Database Price :$150 USDT

Database & Vulnerability : $250 USDT

--->Please do not request samples for testing. I will not make the database public for COMBO<---

--->The source is said to be vulnerable only in case of purchase<---

Contact TG: @MilwOOrm

Columns

```
username password email mobiletelephone hometelephone zipcode birthday weight height currentworking children thaityping salary
```

Sample

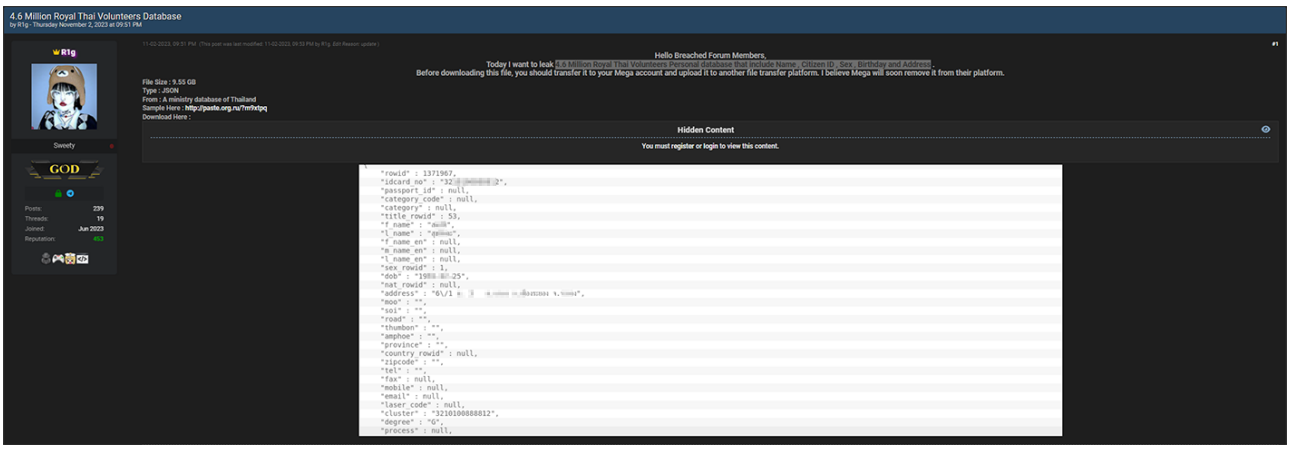
```
username password email mobiletelephone hometelephone zipcode birthday weight height currentworking children thaityping salary
Pornsit 3099po pornsit30@homail.com 800017601 080 001 7601 21130 6/30/1956 98 186 quit 2 0 50000
BomBom00 844563592 Panin_papa@hotmail.co.th 800050266 800050266 10600 12/9/1990 44 150 quit 0 0 8000
145273 145273 supoovong2523@hotmail.com 800051465 - 48000 12/7/1980 55 170 working 2 0 25
800054505 800054505 trumklovefern@hotmail.com 800054505 800054505 30140 1/10/1965 85 174 quit 2 20 20000
hidako 706081 hidakoj_t@hotmail.com 800056545 42161615 47130 9/20/1987 45 157 working 0 40 15000
171432 171432 Preaw-L_J13@hotmail.com 800060940 <blank> 46000 10/17/1989 49 159 working 0 25 15000
patcharee1 saranan patwa22@hotmail.com 800067289 - 40150 9/4/1991 49 159 working 0 40 40
800073384 800073384 to-go31133@hotmail.com 800073384 <blank> 46000 5/9/1990 69 175 working 0 0 10
paweena_601@hotmail.com 800075042 paweena_601@hotmail.com 800075042 <blank> 45170 11/25/2535 50 158 <blank> 0 0 15000
buatick 800084520 pp_999@windowslive.com 800084520 - 21130 12/9/1982 45 163 quit 1 0 8000
800098511 pon03032531 pon92737@gmail.com 800098511 800098511 39000 6/9/1996 65 165 working 2 0 25000
arexzandra 19092525 mayurasung@gmail.com 800100113 <blank> 10270 6/2/1984 53 158 working 0 20 8000
```

Excel Format

username	password	email	mobiletelephone	hometelephone	zipcode	birthday	weight	height	currentworking	children	thaityping	salary
Po	3	po gmail.com	8 7601	08 501	21130	6/30/1956	98	186	quit	2	0	50000
Bo 00	8 92	Pa hotmail.co.th	8 266	80 266	10600	12/9/1990	44	150	quit	0	0	8000
14	14	su 3@hotmail.com	8 465	-	48000	12/7/1980	55	170	working	2	0	25
80 505	80 505	tru @hotmail.com	8 505	80 505	30140	1/10/1965	85	174	quit	2	20	20000
hid	70	hid otmail.com	8 545	42 15	47130	9/20/1987	45	157	working	0	40	15000
17	17	Pr @hotmail.com	8 940	<bl	46000	10/17/1989	49	159	working	0	25	15000
pa ee1	sa	pa otmail.com	8 289	-	40150	9/4/1991	49	159	working	0	40	40
80 384	80 384	to @hotmail.com	8 384	<bl	46000	5/9/1990	69	175	working	0	0	10
pa na_601@ho	80 42	pa 1@hotmail.com	8 042	<bl	45170	11/25/2535	50	158	<blank>	0	0	15000
bu	80 20	pp dowslive.com	8 520	-	21130	12/9/1982	45	163	quit	1	0	8000
80 511	po 32531	po gmail.com	8 511	80 511	39000	6/9/1996	65	165	working	2	0	25000
are dra	19 5	ma @gmail.com	8 113	<bl	10270	6/2/1984	53	158	working	0	20	8000
ch amran	Pw 90c	w. an@hotmail.com	8 143	<bl	46000	9/6/1990	53	160	working	0	0	15000
Ap 0930	80 6	Pa @gmail.com	8 506	-	10310	3/30/1993	78	169	quit	0	0	9000
94	99	sa @hotmail.co.th	8 739	80 739	30000	1/5/1977	60	165	working	2	0	0
pa nok_makch y1 4	vi ok@hotmail.com	8 294	80 294	10240	12/6/1982	53	163	working	0	40	23000
80 828	80 28	to otmail.com	8 328	<bl	-	6/3/1991	90	185	working	0	35	16000
no nit	ha	lo ver76@yahoo.com	8 246	43 38	40000	11/9/1978	54	145	quit	2	0	6500
Mi 81	Mi 31	su 3581@hotmail.co.th	8 593	80 593	20130	11/17/1990	46	155	working	0	0	15000
sha	65 0	luc @hotmail.com	8 588	08 52688	21110	1/29/2011	41	158	quit	0	0	18000
mo arut	15 12	m @hotmail.com	8 490	53 69	50130	4/21/1988	100	175	quit	0	25	15000
85 307	85 07	ai otmail.com	8 734	80 734	70000	4/21/1990	58	165	quit	0	40	10
hm	171 1	jar geng@hotmail.com	8 619	80 619	21130	11/17/1981	45	156	working	0	30	9000
21	907 78	be 5@hotmail.co.th	8 714	80 714	10540	2/11/1996	50	158	quit	0	0	0
po oo	29 0	po ak@hotmail.com	8 558	38 63	20130	1/29/1987	56	169	working	0	35	9000
51 83	80 766	sir 2983@hotmail.com	8 766	<bl	10240	12/22/1990	<blank>	<blank>	working	0	22	0
25	251	ch @hotmail.com	8 985	038 6800 \xb5	20150	1/2/2010	68	172	working	3	0	0

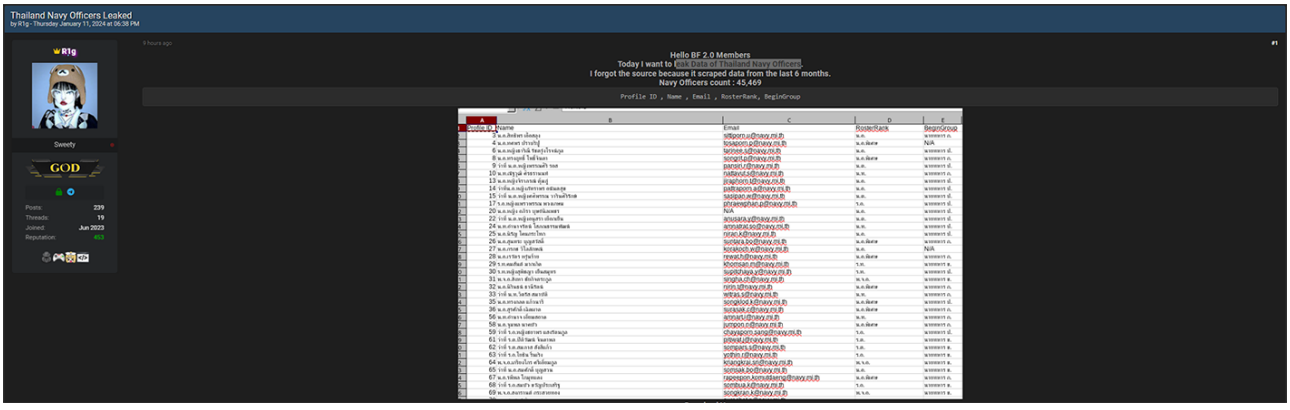
username	password	email	mobiletelephone	hometelephone	zipcode	birthday	weight	height	currentworking	children	thaityping	salary
Po	305	po omail.com	80 501	08 1 7601	21130	6/30/1956	98	186	quit	2	0	50000
Bo m00	844 92	Pa hotmail.co.th	80 266	80 266	10600	12/9/1990	44	150	quit	0	0	8000
14	14	su 23@hotmail.com	80 465	-	48000	12/7/1980	55	170	working	2	0	25
80 505	80 505	tru n@hotmail.com	80 505	80 505	30140	1/10/1965	85	174	quit	2	20	20000
hid	706	hid otmail.com	80 545	42 15	47130	9/20/1987	45	157	working	0	40	15000
17	171	Pr @hotmail.com	80 940	<bl	46000	10/17/1989	49	159	working	0	25	15000
pa ree1	sar	pa otmail.com	80 289	-	40150	9/4/1991	49	159	working	0	40	40
80 384	80 384	to @hotmail.com	80 384	<bl	46000	5/9/1990	69	175	working	0	0	10
pa na_601@ho	80 42	pa 1@hotmail.com	80 042	<bl	45170	11/25/2535	50	158	<blank>	0	0	15000
bu	80 520	pp dowslive.com	80 520	-	21130	12/9/1982	45	163	quit	1	0	8000
80 511	po 32531	po gmail.com	80 511	80 511	39000	6/9/1996	65	165	working	2	0	25000
are dra	19 5	ma @gmail.com	80 113	<bl	10270	6/2/1984	53	158	working	0	20	8000
ch amran	Pw 90c	w. an@hotmail.com	80 143	<bl	46000	9/6/1990	53	160	working	0	0	15000
Ap 0930	80 6	Pa @gmail.com	80 506	-	10310	3/30/1993	78	169	quit	0	0	9000
94	99	sa @hotmail.co.th	80 739	80 739	30000	1/5/1977	60	165	working	2	0	0
pa nok_makch y1 4	vi ok@hotmail.com	80 294	80 294	10240	12/6/1982	53	163	working	0	40	23000
80 828	80 28	to otmail.com	80 328	<bl	-	6/3/1991	90	185	working	0	35	16000
no nit	ha	lo ver76@yahoo.com	80 246	43 38	40000	11/9/1978	54	145	quit	2	0	6500
Mi 81	Mi 31	su 3581@hotmail.co.th	80 593	80 593	20130	11/17/1990	46	155	working	0	0	15000
sha	652 0	luc @hotmail.com	80 588	08 52688	21110	1/29/2011	41	158	quit	0	0	18000
mo arut	15 12	m @hotmail.com	80 490	53 69	50130	4/21/1988	100	175	quit	0	25	15000
85 307	852 07	ai otmail.com	80 734	80 734	70000	4/21/1990	58	165	quit	0	40	10
hm	171 1	jar geng@hotmail.com	80 619	80 619	21130	11/17/1981	45	156	working	0	30	9000
21	907 78	be 5@hotmail.co.th	80 714	80 714	10540	2/11/1996	50	158	quit	0	0	0
po oo	29 0	po ak@hotmail.com	80 558	38 63	20130	1/29/1987	56	169	working	0	35	9000
51 83	80 766	sir 2983@hotmail.com	80 766	<bl	10240	12/22/1990	<blank>	<blank>	working	0	22	0
25	251	ch @hotmail.com	80 985	038 6800 \xb5	20150	1/2/2010	68	172	working	3	0	0

Before, an individual known as **R1g** made a significant data dump involving the personal database of the **Royal Thai Volunteers**. This breach affected a substantial number of records, totaling **4.6 million**. The leaked data included sensitive personal information such as names, citizen ID numbers, gender, birthdates, and addresses.

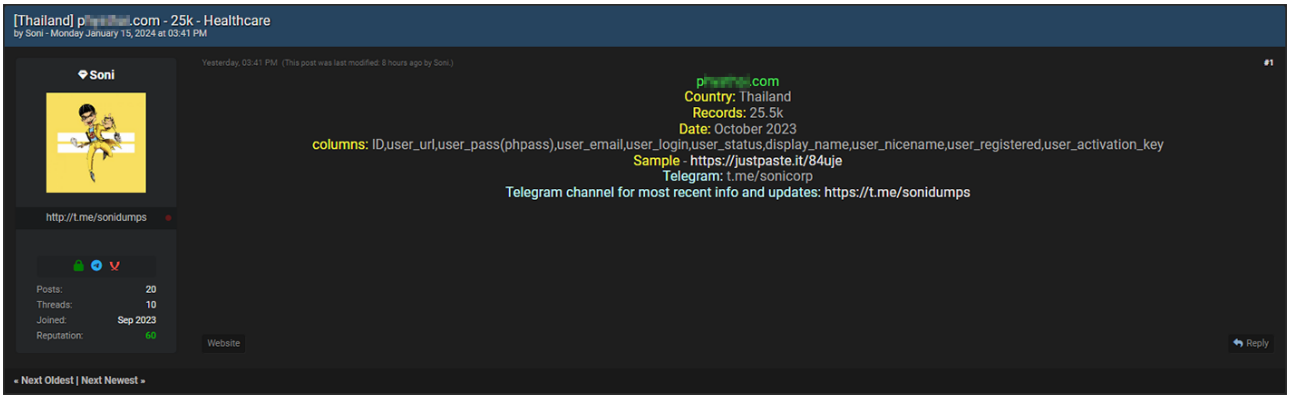


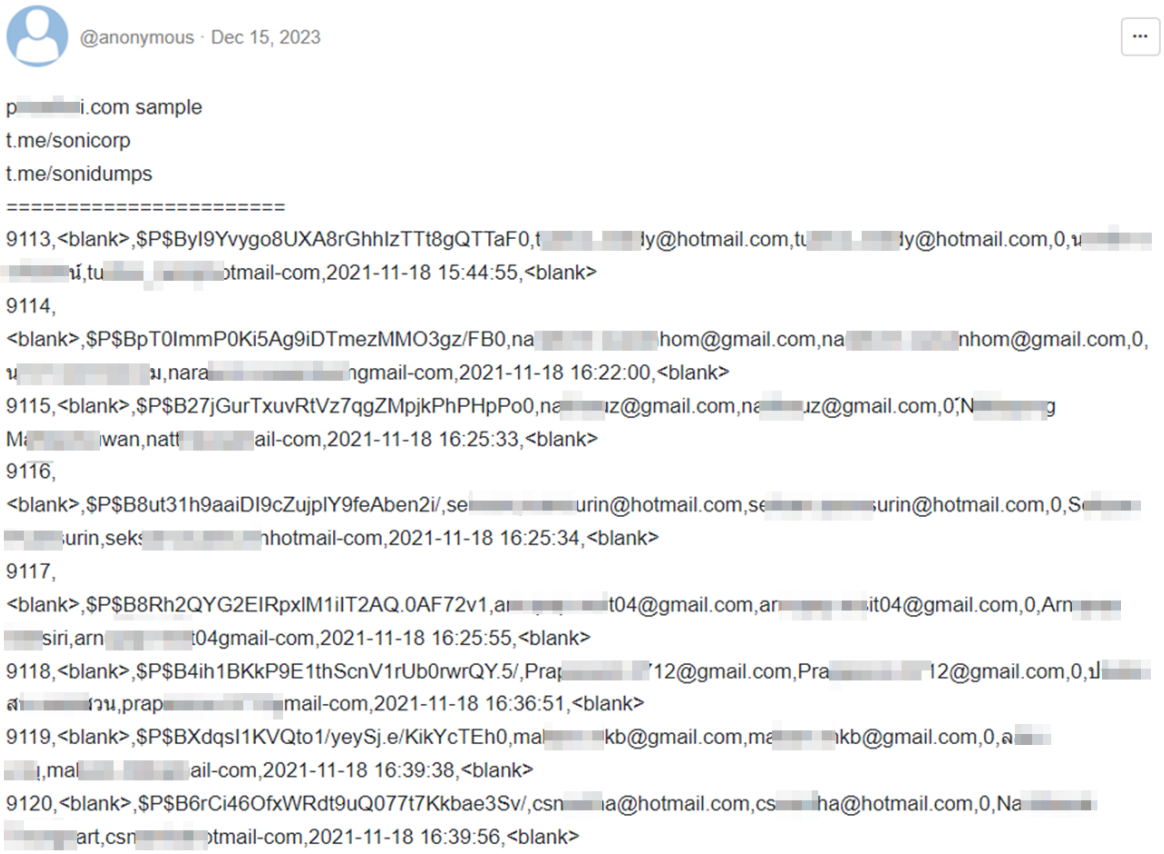

```
{
    "rowid" : 13[illegible]57,
    "idcard_no" : "32[illegible]2",
    "passport_id" : null,
    "category_code" : null,
    "category" : null,
    "title_rowid" : 53,
    "f_name" : "[illegible]",
    "l_name" : "[illegible]",
    "f_name_en" : null,
    "m_name_en" : null,
    "l_name_en" : null,
    "sex_rowid" : 1,
    "dob" : "19[illegible]25",
    "nat_rowid" : null,
    "address" : "6\/1 [illegible]",
    "moo" : "",
    "soi" : "",
    "road" : "",
    "thumbon" : "",
    "amphoe" : "",
    "province" : "",
    "country_rowid" : null,
    "zipcode" : "",
    "tel" : "",
    "fax" : null,
    "mobile" : null,
    "email" : null,
    "laser_code" : null,
    "cluster" : "3210100888812",
    "degree" : "G",
    "process" : null,
```


The same individual, **R1g**, was responsible for another major data leak on **Thursday, January 11, 2024**. This time, the breach involved sensitive information pertaining to **Thailand Navy Officers**, marking another significant security incident.



January 15th, 2024, the actor who goes by the alias **Soni** posted a leaked database related to healthcare**.** The data breach consists of **25.5k records** of user information including ID, user URL, encrypted passwords (phpass), user emails, login details, account status, display names, registration dates, and user activation keys The actor shared a sample of the data as proof.





Cybercriminals have also focused their attacks on the government and military sector in Thailand, breaching the personal identity details of officials and law enforcement personnel. This type of operation is typical for cyberespionage groups functioning within the realm of cybercrime.

The perpetrators disclosed various confidential documents, which included internal correspondences and interactions with law enforcement agencies in Cambodia. These leaks might have occurred due to a compromise by a third party. The origin of this breach remains unidentified, but the malicious cyber activities against Thai government officials could indicate a growing trend of targeting in the region.

Conclusion

In 2024, Thailand is set to play a crucial role in the global fight against cybercrime. As the nation progresses in its journey of digital transformation and expands its capabilities in Information and Communication Technology (ICT), it faces a growing wave of cyber threats, especially those involving breaches of personal data. This escalating challenge underscores the pressing need for Thailand to adopt and reinforce strong cybersecurity strategies.

The series of large-scale data breaches and the looming risk of misuse of sensitive information in Thailand serve as a stark reminder of the critical need for improved data protection and proactive cyber defense tactics. For Thailand, it's essential to strengthen its cybersecurity framework, enact stringent data privacy regulations, and cultivate a widespread culture of digital vigilance among both its population and institutions. Such measures are key not just for protecting the privacy and security of its citizens, but also for reinforcing Thailand's stature as a dependable and secure player in the international digital arena.

Cloud Architecture