## **COVID-19** data put for sale in Dark Web



resecurity.com/blog/article/covid-19-data-put-for-sale-in-dark-web

<u>Back</u>

Cybercrime Intelligence

25 Aug 2022

Dark Web, privacy, data breach, e-crime

Cybercriminals have stolen PII data from Thailand's Department of Medical Sciences, the data contains information about patients with COVID-19 symptoms. The data was put for sale on several Dark Web marketplaces and is available for further purchase via a Telegram channel created by the bad actors.



Resecurity, Inc. (USA) is monitoring data leaks and the exposure of digital identity data in Dark Web and has already alerted law enforcement and Thai CERT.

Based on the acquired samples and additional insights related to the security incident, the bad actors were able to gain unauthorized access to the government portal allowing them to manage users and records illegally.

According to the actors, they were able to steal sensitive and personal information including but not limited to last name, first name, sex, age, contact details, medical history, and related local healthcare identifiers:

Hello today i am leaking/selling Thailand Department of Medical Services ( owned by ministry of health ) i am selling access into a dashboard used by hospitals/admins which contains the following: Personal info: dateofsubmittionofCovid - name-surname - sex personal type - Affiliated agency - symptoms Another Option: date, HN, name-surname, sex, age, contact number, hospitals to be treated, date of infection, summary of symptomps samples posted on telegram to avoid any external file share down and etc Entries propably 5K+ (on main chart its written 15K), number increasing DAILY!. can extract as CSV Price of data just 120\$ [ csv ] if you need admin access 200\$ samples: ● 615 edited 4:46 AM > 5 comments

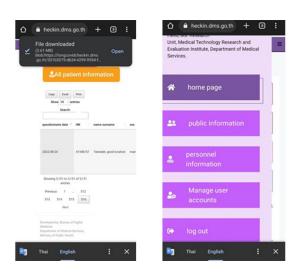
Based on further engagement it has been confirmed, the bad actors have attacked a WEB-app (https://longcovidcheckin.dms.go.th) provided by the Department of Medical Sciences of Thailand for online-surveying and data collection surrounding COVID-19 from citizens and tourists visiting the country.

Friend this is the admin panel of the covid dashboard of thai gov

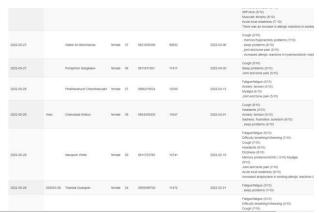
use chrome translator to use it in english, and there is option caller Excel to download the data directly, if you didnt knew how to do it, please tell me so i send you directly files

https://longcovidcheckin.dms.go.th/login.php

The screenshots acquired via HUMINT (human intelligence) means by Resecurity's HUNTER (threat intelligence and R&D unit) confirmed the source of the leak and compromised WEB-resource:



The access was possible due to an active SQL-injection vulnerability in an authorization module of the WEB-app. According to OWASP Top 10 classification such vulnerabilities are extremely common issue exploited by hackers due to insecure parameters filtering, such vulnerabilities may lead to a significant risk of data breach. The Resecurity team has addressed the proper recommendations to contain vulnerability.



At the time of breach identification, the bad actors could have accessed at least to 5,151 detailed records with a potential exposure of 15,000 in total. The access could also be used to monitor further updates and the collection of new records in real time – which obviously negatively impact privacy.

Thailand is not the only region where cybercriminals hunt for personal and medical data. Most healthcare services in Thailand are available in digital form for citizens, that's why they're always an attractive target for cyberespionage groups, and other Dark Web actors collecting information for malicious purposes, one example purpose is to use the stollen data for further identity theft.

| 21   |             |           |                            | 0 0   | - 4 |                 | - 4 |       |             | 1 1 1 1  |
|------|-------------|-----------|----------------------------|-------|-----|-----------------|-----|-------|-------------|--|
| 410  | 23/94/2022  |           | Systles softland           | welv  |     | 72 0821251774   |     | 99722 | 25/97/2022  |  |
| 444  | 21/04/2022  |           | vivrativel attensed with   | wije  |     | 44 0614479675   |     | 10477 | 11/86/3022  | Bilgffform rewichefulls a somewidth apular (1/10)  |
| 122  | 25/96/2002  |           | ander edean                | refer |     | 40.081396962    |     | 41808 | -533333     | dansella (dans) is/stra/sellera is/strileralica fineller is/streth elasel da lasera  |
| 1115 | 23/796/2002 |           | effect formed              | wide  |     | 24 0883012970   |     | 13745 | E1746/2022  | Te colonial from moreovaria coloni   |
| 5114 | 25/94/2012  |           | anned Specifyers           | 810   |     | 33 0967563440   |     | 36765 |             | claudines (V) (c) diagnosi renormati vizar della (co) (c) landica develua (c) (c) diagnosi re  |
| 1115 | 23/98/2022  | 413042    | r data esta                | wife  |     | 38 9606363454   |     | 13790 | 25/9/5/2022 | eraladary/realafagoorfus (t/tt)  |
| 5116 | 23/04/2022  | 207       | vdaponé s fesivierie       | 976   |     | 29 094603022    |     | 12797 |             | Analysis daily depend of the property of the second and the second of th |
| 5117 | 25/96/2002  | ted.      | MARKET REPORTED            | wife  |     | 65 0620396775   |     | 10743 | 11/86/2022  | สดาเหลือ (สดาเกราะสายาสายาสายาสายาสายาสายาสายาสายาสายาสา   |
| 5518 | 25/96/2002  |           | wasan malloorf             | wde   |     | 26 0949936045   |     | 12254 | 25/50/0622  | powerful (2004) (2000) to be be be to be the control of the contro |
| 5119 | 23/98/2022  |           | sixele/ Senses             | 716   |     | NA SANALISMOSIA |     | 11582 | 12/16/3022  | Na mon   |
| 5120 | 25/58/2022  | 12796     | STRONG ENTRAGE             | wife  |     | 46 OMMADICS     |     | 30722 | 25/66/3022  | ระยบองโดยระบา การกระบายโดยของโดยของสิทธิสายเลยใหญ่ การกระบายโดยสายเรียก การกระบายโดยสายเรียก   |
| 1121 | 23/96/2022  |           | funds feetime              | wife  |     | IN 0877660032   |     | 25090 | 16/81/0021  | พายใหล่านากกรายใหม่ของเหมือน เกวชาใน เทาชนร้องคร้ายก เกวชาร์อกก็กาย ตั้งเสียด เกว  |
| 1111 | 25/96/2022  |           | energy stroffements        | 978   |     | 2 0667252790    |     | 11000 | 36/9/2018   | paramile/apach ct/commission/worksforce/whiteforce/apach/apach   |
| 5128 | 25/94/2602  |           | forces Instront            | 576   |     | IN DAMESTORY    |     | 33362 | 61/06/3022  | poweds/pour cross-stars-systellarses-dansing to target laboration  |
| 1024 | 25/98/2022  |           | coope salterile            | 900   |     | AL DESERVATE    |     | 12256 | 25/82/3622  | espendin/sessit montle mon   |
| 125  | 25/96/2022  |           | product attains            | wife. |     | IS DETRICATED   |     | 10680 |             | parameter agents in the wife property will always a few and the property and the parameter and the par |
| 5120 | 25/98/2022  |           | net errort                 | with  |     | 62 0902586794   |     | 10675 | 26/99/3632  | passed to a particular of a recovered advanced and a particular of the design of the particular of the |
| 5127 | 34/94/2002  |           | chaptered solidered        | wde   |     | 17 0814709077   |     | 13909 | 24/96/3022  | £0sperintropyrollis (\$750)  |
| 5126 | 24/94/2602  |           | come regres)               | mGe . |     | 30 0660726225   |     | 11299 |             | Ne prom  |
| 5129 | 28/08/2022  | \$50620   | ration formands            | 476   |     | BE 095344401    |     | 10762 | 17/96/2012  | assendarapsah memerikahan sebesah diapanan berangan mendantan dan basa men   |
| 5130 | 24/94/2022  |           | fu vonancu                 | wife  |     | 63 0629343622   |     | 11206 | 29/96/3022  | essendaraged monthly combined or ordered and and monthly and an arrival  |
| 5131 | 34/98/2002  |           | while of table             | wde   |     | 26 0906790172   |     | 31342 | 23/90/2022  | parameter/appain (\$730) who have no have no half appointed in (\$730) for (\$750) down has (\$75  |
| 5132 | 26/95/2022  |           | Narongshei Leitmongkolchol | 100   |     | 33 0647897944   |     | 41577 | 10/07/2022  | พายใหล่ายาก/พายใหล้พลุดเพรื่อย (1700/โล 1970)  |
| 5133 | 34/94/2022  |           | pel errori                 | wife  |     | 62-0932386794   |     | 30975 | 26/95/2022  | สสาขาที่สารสองสำ สราสาขาที่ โดยาราชาวิทย์าราชาวิทย์ที่สาขาทรที่สาข สราสาขาที่สาขาที่สาขาที่  |
| 1114 | 24/94/9023  |           | sala offereday             | wife  |     | 45 0471457004   |     | 11276 | 14/96/3022  | parameter asset parameter and extra replacement of the parameter parameter parameter (a)   |
| 1110 | 34/94/2022  | 651526    | t budge smeller            | wife  |     | 25 0900099536   |     | 51670 |             | Observative contributed by incomplete deadly (1/20)  |
| 5136 | 24/25/2022  |           | Support effective          | 200   |     | 43 0096607513   |     | 32345 | 25/96/3022  | Na prim  |
| 5017 | 26/06/2022  | 651529    | Moreon leading             | wife  |     | 12 0996242935   |     | 12249 | 85/86/3032  | คลายหนึ่ง/สลาเล้า (ห/วถาล้วงศึกษะ (ห/วถาลัยหลักษะ (K/วถเลียนคาการและเหนืน (K/วถ)   |
| 5138 | 24/94/2022  |           | refer followers            | wife  |     | NE CHOMOSONS    |     | 14199 | 16/59/2022  | percendity/percels (5/35)  |
| 1119 | 38/98/2022  |           | strengt dualscream         | 970   |     | 34 DENONZUENA   |     | 12256 | 22/979/3022 | Many research (6/10)   |
| 5580 | 26/56/2022  |           | cons martiripal            | wife  |     | 36 0936399736   |     | 42527 | 27/96/3022  | comming against principal advantable principal and princip |
| 5361 | 28/98/2022  | 155895-62 | gen sofur                  | wife  |     | 61 094 N N N N  |     | 13672 | 11/22/11/19 | Elementras restrigant de extendició de entre de de la composição de la com |
| 5342 | 24/98/2022  |           | say the street             | wife  |     | NI DECKOMPRIS   |     | 12144 | 96/96/3022  | Ne more  |
| 5343 | 24/14/2002  |           | eternic Seniors            | 819   |     | 79 625845979    |     | 12256 | 29/5/2/2022 | paramility/dates/conference constitution of the conference of the  |
| 5546 | 34/04/2023  | ANDRE     | ow/security security       | wife  |     | 4-0851A32688    |     | 34199 | 29/85/3822  | wordsatterwww.eliafasawefae.te/on  |
| 5165 | 26/08/2022  | 650290    | (Supre oferace)            | wife  |     | 1.09403096      |     | 24295 | 26/85/3622  | Ne m/m   |
| 1146 | 24/94/2022  |           | ryled golfly.              | 50    |     | 12 0994030708   |     | 14099 |             | enellations/enellationserfactation   |
| SME  | 24/94/2022  | -         | aftered encountry          | wdr   |     | 12 (957)7579676 |     | -     |             | poweds/sewh monte rason  |
|      |             |           |                            |       |     |                 |     |       |             |  |

These types of attacks are becoming a common occurance, for example there was an attack which saw the release of over 230,000 Indonesian COVID-19 patient records in the Dark Web. The leaked data consisted of name, address, present address, telephone number, citizenship, diagnosis date, result, result date, and many more.

To prevent yourself from being a victim of identity theft – subscribe to Resecurity® Identity Protection (IDP), a mobile app and interactive WEB-service featuring a dashboard for continuous 24/7 protection. Resecurity® enables Dark Web monitoring, leaked credentials detection, and timely alerts about other identified threats targeting your persona online.

## References

- Dark Web Marketplaces and COVID-19: before the vaccine https://pubmed.ncbi.nlm.nih.gov/33500876/
- The use of the Dark Web as a COVID-19 information source: A three-country study <a href="https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9186528/">https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9186528/</a>
- COVID-19 Related Data Of Thousands Of Indians Allegedly Leaked On Dark Web <a href="https://www.vibesofindia.com/covid19-related-data-of-thousands-of-indians-allegedly-leaked-on-dark-web/">https://www.vibesofindia.com/covid19-related-data-of-thousands-of-indians-allegedly-leaked-on-dark-web/</a>
- Security researchers at threat intelligence firm Cyble discovered over 230.000
   Indonesian COVID-19 patients records leaked in the darknet.
   <a href="https://securityaffairs.co/wordpress/105043/deep-web/indonesian-covid-19-patients-leak.html">https://securityaffairs.co/wordpress/105043/deep-web/indonesian-covid-19-patients-leak.html</a>

## Newsletter

Keep up to date with the latest cybersecurity news and developments.

By subscribing, I understand and agree that my personal data will be collected and processed according to the <u>Privacy</u> and <u>Cookies Policy</u>

## **Cloud Architecture**

