COVID-19 data put for sale in Dark Web

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

Back

Cybercrime Intelligence

25 Aug 2022

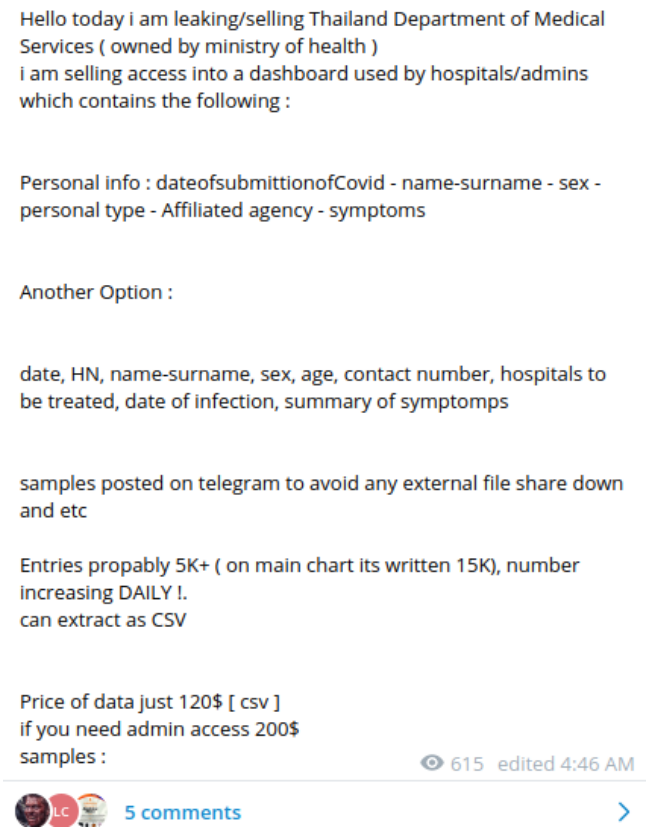
Dark Web, privacy, data breach, e-crime

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.

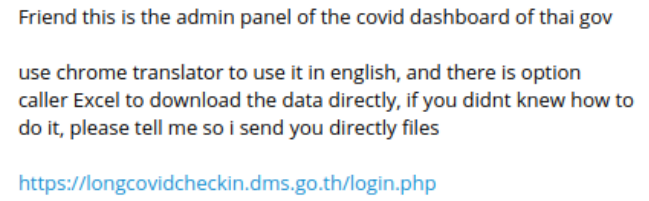
Resecurity, Inc. (USA) is monitoring data leaks and the exposure of digital identity data in Dark Web and has already alerted law enforcement and Thai CERT.

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.

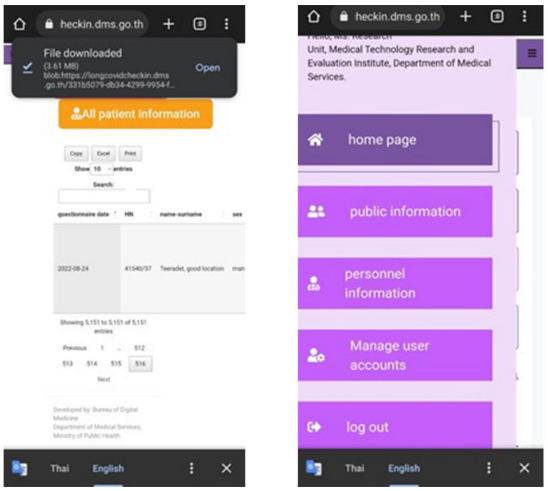
According to the actors, they were able to steal sensitive and personal information including but not limited to last name, first name, sex, age, contact details, medical history, and related local healthcare identifiers:



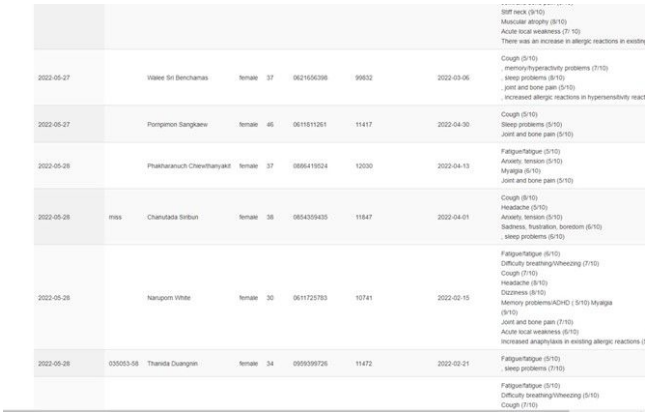
Based on further engagement it has been confirmed, the bad actors have attacked a WEB-app (https://longcovidcheckin.dms.go.th) provided by the Department of Medical Sciences of Thailand for online-surveying and data collection surrounding COVID-19 from citizens and tourists visiting the country.



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:

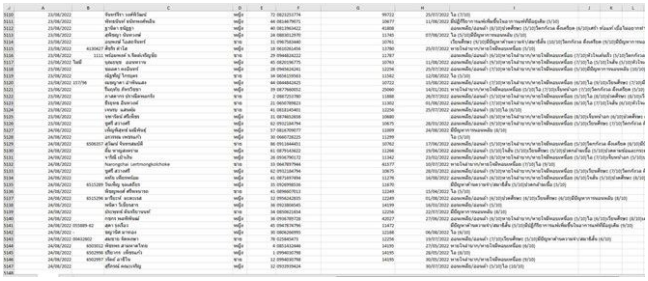


The access was possible due to an active SQL-injection vulnerability in an authorization module of the WEB-app. According to OWASP Top 10 classification such vulnerabilities are extremely common issue exploited by hackers due to insecure parameters filtering, such vulnerabilities may lead to a significant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



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 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9186528/
- COVID-19 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/
- Security researchers at threat intelligence firm Cyble discovered over 230.000 Indonesian COVID-19 patients records leaked in the darknet. https://securityaffairs.co/wordpress/105043/deep-web/indonesian-covid-19-patients-leak.html

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 Privacy and Cookies Policy

Cloud Architecture