

Ill will: Hackers hold healthcare data to ransom

November 9 2022



Credit: Pixabay/CC0 Public Domain

Australia's biggest private health insurer Medibank is at the centre of the latest major attack by hackers holding health systems, hospitals and, increasingly, patients' health records, to ransom in one of the trends in cybercrime.

AFP looks at some of the bigger recent attacks on health institutions targeted by ransomware, in which criminals infiltrate and paralyse a target's IT systems, then demand payments in order to restore them:

May 2021: Irish health system shut down

In May 2021, Ireland's health service suffered what it called a "catastrophic" hack of its IT systems.

Health workers were forced to use paper records and many outpatient visits were cancelled after the [health](#) service shut down all its computers to try to halt the attack, which targeted patients' records.

Irish officials blamed the Russian-based Conti ransomware group for the attacks, which ended with the hackers handing over the encryption codes. Ireland said no money changed hands.

2019-2022: France under attack

French hospitals and laboratories have been a top target in recent years, with the government saying in early 2021 that an attack was taking place every week.

In August this year, cyberattackers dumped the records of patients online after a failed attempt to extort money from Corbeil-Essonnes [hospital](#) near Paris.

One of the country's biggest data breaches took place in February 2021, when the [medical records](#) of nearly half a million people, including their HIV and fertility status, were leaked online after being stolen from a laboratory network.

Oct. 2020: Finnish therapy records hacked

In Finland, the records of tens of thousands of psychotherapy patients were hacked and some leaked online in October 2020 after hackers stole files belonging to Vastaamo, a company that runs 25 therapy centres.

Patients received emails with a demand for 200 euros (\$200) in Bitcoin to prevent the contents of their discussions with therapists being made public.

Sept. 2020: One dead in Germany

In Germany, a ransomware attack was blamed for the death of a woman whose transfer to hospital was delayed by an hour in September 2020 after Duesseldorf University Hospital's computer system was disconnected from from the ambulance network.

The woman was taken to a hospital further away and died afterwards.

May 2017: UK hospitals hit by 'Wannacry'

In May 2017, dozens of hospitals in the UK were forced to divert ambulances and scrap operations after the country's state-funded National Health Service was caught up in the international "WannaCry" ransomware attack, which infected some 300,000 computers in 150 countries.

The United States and Britain blamed North Korea for the attack, in which hackers demanded payment of \$300 in Bitcoin to unlock encrypted files.

Feb. 2016: LA hospital pays ransom

In February 2016 a Los Angeles hospital, the Hollywood Presbyterian Medical Center, paid \$17,000 in Bitcoin to hackers who took control of

its computers for more than a week.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom," the [hospital](#)'s president said.

© 2022 AFP

Citation: Ill will: Hackers hold healthcare data to ransom (2022, November 9) retrieved 25 March 2023 from <https://techxplore.com/news/2022-11-ill-hackers-healthcare-ransom.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.