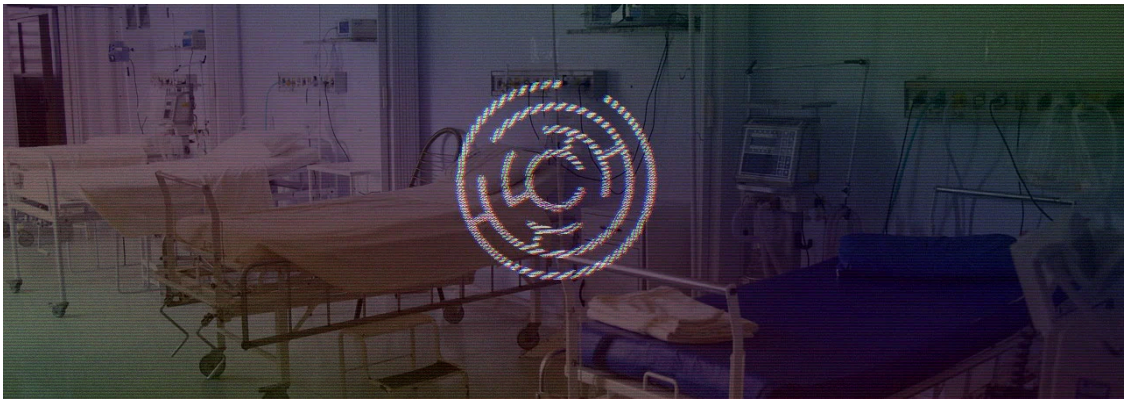
Drug testing firm sends data breach alerts after ransomware attack

By Lawrence Abrams

Published: 2020-04-07 · Archived: 2026-04-05 14:12:19 UTC

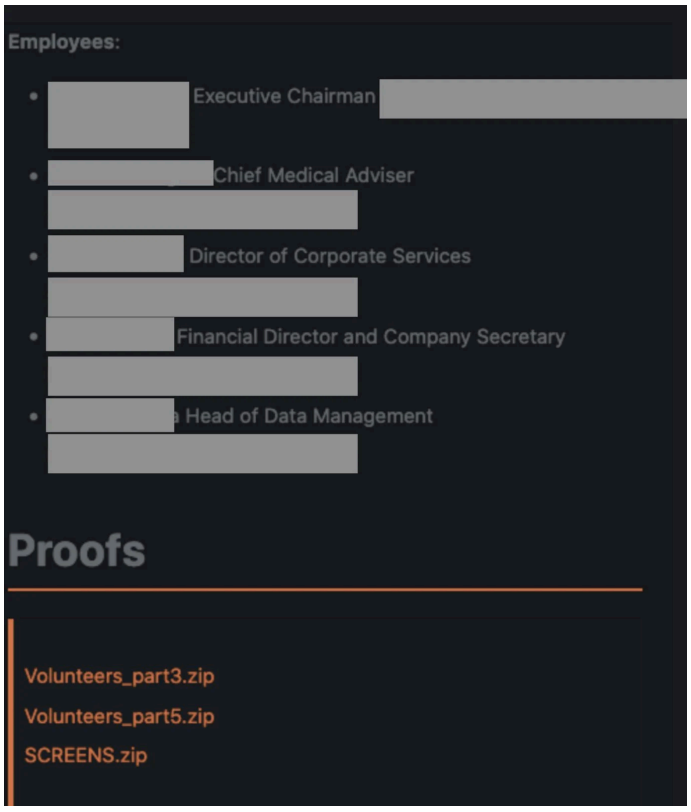


Hammersmith Medicines Research LTD (HMR), a research company on standby to perform live trials of Coronavirus vaccines, has started emailing data breach notifications after having their data stolen and published in a ransomware attack.

This attack occurred on March 14th, 2020, when the Maze Ransomware operators stole data hosted on HMR's network and then began to encrypt their computers.

After the ransom was not paid, the Maze operators published some of the stolen data on their "News" site on March 21st to further extort HMR into making a payment.


DIE LINKE.
0:00



Leaked HMR Data

At that time, HMR stated that they could not afford the ransom demand and wouldn't pay even if they could.

"We have no intention of paying. I would rather go out of business than pay a ransom to these people," Malcolm Boyce, managing and clinical director and doctor at HMR, told Computer Weekly.

According to HMR's data breach notification, the stolen records contained the personal information for volunteers who surnames begin with D, G, I, or J.

"We're sorry to report that, during 21–23 March 2020, the criminals published on their website records from some of our volunteers' screening visits. The website is not visible on the public web, and those records have since been taken down. The records were from some of our volunteers with surnames beginning with D, G, I or J."

The personal information exposed in these leaked documents include:

- name,
- date of birth,
- identity documents (scanned passport, National Insurance card, driving license and/or visa documents, and the photograph we took at the screening visit),
- health questionnaires,
- consent forms,
- information from general practitioners,
- some test results (including, in a few cases only, positive tests for HIV, hepatitis, and drugs of abuse).

HMR states that most of the government IDs that they have in their possession have since expired, but they warn potential victims that they should contact the issuing organization to report the stolen IDs.

HMR also recommends that victims contact CIFAS (the UK's Fraud Prevention Service) and apply for a protective registration, which alerts companies to take extra measures when opening financial accounts or services under the registrant's identity.

Ransomware operators continue to attack health care

On March 18th, BleepingComputer contacted numerous ransomware operators and asked if they would attack hospitals and health care organizations during the Coronavirus pandemic.

Four of the ransomware operators, including Maze, Clop, DoppelPaymer, and Nefilim, stated that they would not target hospitals and medical organizations during the pandemic and would decrypt any that are accidentally encrypted.

When Maze publicly released HMR's documents on March 21st, it was seen as a breaking of this pledge. Maze, though, argued that HMR was attacked on the 14th before the pledge was made.

Maze continues to tell BleepingComputer that they will not attack healthcare organizations after their March 18th pledge.

Other ransomware operators, though, continue to target hospitals with no sign of letting up.

For example, Ryuk Ransomware continues to target hospitals and medical organizations with four attacks occurring this past month.

Microsoft has also seen an uptick in ransomware operators targeting hospitals and health care organizations.

To assist these organizations, Microsoft has started to proactively contact hospitals and healthcare organizations that are using publicly accessible VPN and gateway devices with known vulnerabilities targeted by ransomware.
