Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack

By Bill Goodwin

Published: 2020-03-22 · Archived: 2026-04-05 14:38:49 UTC

Cyber gangsters have attacked the computer systems of a medical research company on standby to carry out trials of a possible future vaccine for the Covid-19 coronavirus.

The Maze ransomware group attacked the computer systems of Hammersmith Medicines Research (HMR), publishing personal details of thousands of former patients after the company declined to pay a ransom.

The company, which carried out tests to develop the Ebola vaccine and drugs to treat Alzheimer's disease, performs early clinical trails of drugs and vaccines.

The cyber crime group published HMR's medical files only days after the Maze crime group made a public promise not to attack medical research organisations during the coronavirus pandemic.

HMR said that IT staff discovered a "severe attack" in progress on Saturday 14 March, but were able to halt it and restore its computer systems and email by the end of the day.

"We repelled [the attack] and quickly restored all our functions. There was no downtime,"said Malcolm Boyce, managing and clinical director and doctor at HMR, adding that the organisation had "beefed up" its defences substantially.

The hacking group published a notice on a website claiming it had attacked the company with ransomware on 14 March.

It stepped up pressure on the organisation 21 March by publishing historic sensitive medical and personal information about thousands of former patients on the internet.

The files, which HMR said are likely to date back 8 to 20 years, contain medical questionnaires, copies of passports, driving licenses and national insurance numbers of more than 2,300 of the organisation's patients.

Computer Weekly has established that the documents, which represent a sample of HMR former patients chosen with surnames beginning G, I and J, include at least one copy of a currently valid passport.

Ransom demand

Boyce said that the hackers had sent the company medical files of former patients which were 8 to 20 years old as proof they had gained access to the company's data, along with a ransom demand.

He said that most of the sample files sent to HMR contained details of young people who had taken part in clinical trials while travelling and would be difficult to trace.

“What they have sent us was 8 to 20 years old, and we would not know how to contact them. They are probably young people who have mostly returned to their country of origin,” he said. “They are from Australia and South Africa, which were frequent visitors to this country at at this time, and took part in clinical trials.”

Boyce said he was aware that the hackers had released further records on the internet, but had not seen their content.

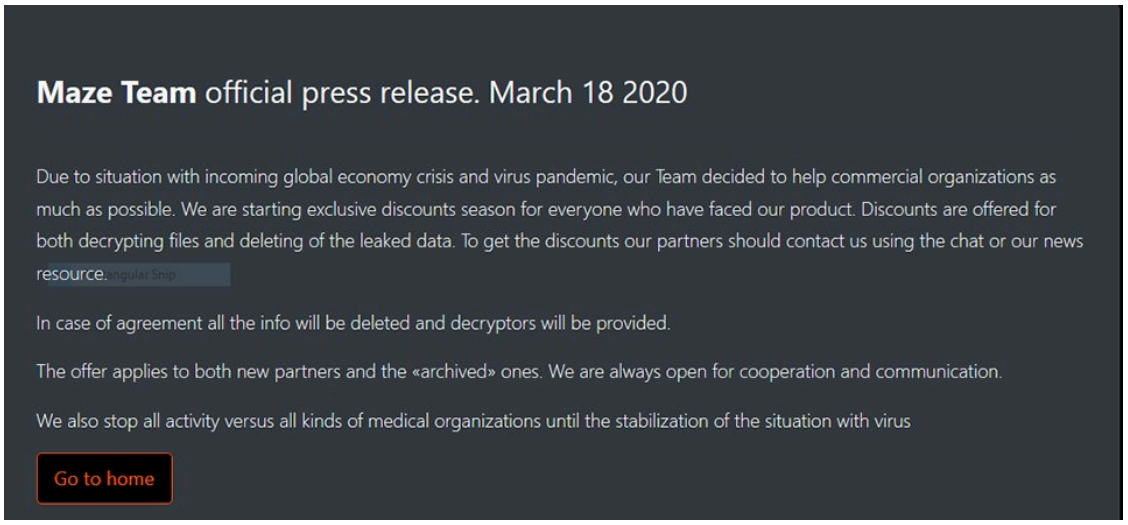
The research company is not a pharmaceutical company and does not have the funds to pay a ransom demand even it wanted to, Boyce told Computer Weekly.

“We have no intention of paying. I would rather go out of business than pay a ransom to these people,” he said.

Maze breaks promise not to attack medical organisations

The Maze group, which first came to notice in May 2019, extorts victims by encrypting the files of an organisation and demanding a ransom payment to release the files.

It upped the ante in late 2019 by naming companies on websites that refused to pay ransoms, and publishing documents and data stolen from their computer networks.



Maze’s statement on 18 March

The group made a public promise in a ‘press release’ on 18 March not to attack medical organisations during the coronavirus outbreak.

“Due to [the] situation with incoming global economy crisis and virus pandemic, our team decided to help commercial organisations as much as possible. We are starting exclusive discounts season for everyone who have faced our product,” it said.

“We also stop all activity versus all kinds of medical organisations until the stabilisation of the situation with the virus.”

Criminals ‘only interested in money’

Raj Samani, chief scientist at computer security specialist McAfee, said that Maze's apparent reversal of its policy not to attack medical intuitions shows that the criminals' only focus was making money.

"We have had previous assertions from other ransomware groups that they aren't going to go after medical environments, but it really shows us we can't take what these individuals say as trustworthy," he said.

HMR's Boyce said: "They are unscrupulous individuals and they are pretending now that there is an amnesty because of the Covid-19 virus."

> **"They are pretending now that there is an amnesty because of the Covid-19 virus"**
>
> *Malcolm Boyce, HMR*
>
> .

HMR has not disclosed how the Maze group gained access to its network, but the hacking group frequently relies on Exploit kits, which contain software designed to attack known software vulnerabilities to penetrate company defences.

The hacking group has also used phishing emails to deliver malware to employees who may be tricked into downloading malicious software.

Troy Mursch, chief research officer at threat intelligence company Bad Packets, said that historical data showed that Hammersmith Medicines Research used a Fortinet VPN server, which may have had a vulnerability that Maze could have exploited.

Brett Callow, threat analyst at security company Emsisoft, said that Maze had initially mis-attributed the leaked files from HMR to another company, which may suggest that Maze attacked a datacentre used by HMR and other companies.

"I can't help but wonder whether they've got their hooks into one or more datacentres that haven't properly isolated their clients' networks," said Callow. "If companies were more open about these incidents, it may be possible to get a handle on what they're doing, which could help other companies avoid being hit."

ICO and NCA making enquiries

HMR has reported the incident to the Information Commissioner's Office (ICO), which told Computer Weekly that it is making enquires.

An ICO spokesperson said: "People's medical data is highly sensitive information, not only do people expect it to be handled carefully and securely, organisations also have a responsibility under the law.

"When a data breach occurs, we would expect an organisation to consider whether it is appropriate to contact the people affected, and to consider whether there are steps that can be taken to protect them from any potential adverse effects."

A spokesperson from the National Crime Agency said: "We are aware of an incident affecting Hammersmith Medicines Research Limited. We are working with partners to support the organisation and understand the impact of the incident."

Software companies offer help

Computer security companies have offered to assist medical research companies and hospitals fighting ransomware attacks during the Covid-19 outbreak.

Emsisoft said it had teamed up with Coveware to offer free help to healthcare providers affected by ransomware during the coronavirus crisis, including threat analysis, development of decryption tools, and – as a last resort – negotiating with cyber attackers.

HMR

HMR is on standby to test vaccines for the coronavirus

Samani said that McAfee would assist any organisation that is having to fight on the front line, trying to find a vaccine or trying to combat Covid-19.

“Anyone that does have ransomware, we will do everything to try to get them online as quickly as possible,” he said.

Boyce said that HMR was on standby for testing possible vaccines to the coronavirus when they are ready. “We fully expect to be involved in that when they appear,” he added.

Update of Maze statement

Following publication of this story, the Maze ransomware group has removed more than 2,300 highly sensitive medical files from former patients of Hammersmith Medicines Research (HMR) from its website.

The group said in a press release on 22 March that it had attacked HMR on the 14 March before it publicly promised not to attack medical institutions on 18 March, though it was silent on why it published HMR’s patient medical files on 22 March.

Maze’s statement, published within two hours of Computer Weekly’s report, attacked computer security professionals failing to do their jobs, who Maze claimed “prefer to chat in social networks or watch porn”.

The group claimed the companies were earning billions of dollars from the internet, but did not care about protecting privacy. “The only thing [they] care about is to avoid lawsuits and fines for loosing that information,” said Maze.

“We want to show that the system is unreliable. The cyber security is weak. The people who should care about the security of information are unreliable. We want to show that nobody cares about the users,” the group said.

Maze compared its actions to the actions of Julian Assange and Edward Snowden, warning that further attacks would follow.

“Now it’s our turn. We will change the situation by making irresponsible companies to pay for every data leak. You will read about our successful attacks in the news more and more,” it added.

Additional research by Matt Fowler.
