forbes.com

COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online

Davey Winder

4–6 minutes

A vaccine-testing facility is the latest to be hit by cyber-attackers

Getty

A medical facility on standby to help test any coronavirus vaccine has been hit by a ransomware group that promised not to target medical organizations.

The criminals behind the Maze ransomware attacks have struck again, stealing data from a victim and then publishing it online to get them to pay the ransom demanded. That, in and of itself, would not be particularly newsworthy, sadly. However, the Maze threat actors were amongst the leading cybercrime gangs which, just days ago, pledged not to attack healthcare and medical targets. The Maze threat actors didn't go as far as those behind the DoppelPaymer threat by offering free decryptor codes to those hit by accident. Nor, it would appear, did they mean what they said. The latest victim is Hammersmith Medicines Research, a British company that previously tested the Ebola vaccine and is on standby to perform the medical trials on any COVID-19 vaccine.

Maze group publishes patient data

online to 'encourage' payment

Malcolm Boyce, clinical director of Hammersmith Medicines Research, told Computer Weekly that the cyber-attack, which took place on March 14, was spotted in progress, stopped, and systems restored without paying any ransom. "We repelled [the attack] and quickly restored all our functions," he said, "there was no downtime." This was, admittedly, before Maze announced on March 18 that it would no longer target medical organizations. However, this pledge has not stopped it from continuing in attempts to extort them.

The Maze attackers apparently managed to exfiltrate data, in this case patient records, and has published some of them online. Boyce told Computer Weekly that the hackers had sent Hammersmith Medicines Research sample files containing details of people who participated in testing trials between eight and 20 years previously. The Maze operators then published samples of data on the dark web. I have seen the

posting from the Maze group that adds Hammersmith Medicines Research as a "new client," which is how it describes victims of its attacks.

No intention of paying the ransom

The FBI has already warned of a significant spike in COVID-19 scams, and I've alerted healthcare workers to a new Windows ransomware campaign that leverages coronavirus fears as the bait. It was thought by some, although not by me I have to say, that Maze would be one less worry for the healthcare sector during these troubled times. The public statement made by the Maze operators stated that it would "stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus." Infosecurity professional, John Opdenakker, is not at all surprised that the Maze actors broke this so-called promise. "Financial gain is, unfortunately, the only motive for criminal actors," Opdenakker says, "they also know that medical organizations are currently in a very

vulnerable situation due to the coronavirus outbreak, which only increases the probability that they'll pay extortion demands." Boyce, however, has said that he would rather go out of business than pay a ransom to release the data files and has no intention of doing so.

Free help for healthcare ransomware victims

So, what happens next? "The criminals almost certainly haven’t yet published all the data that was stolen," Brett Callow, a threat analyst at Emsisoft, says. "Their modus operandi is to first name the companies they’ve hit on their website and, if that doesn’t convince them to pay, to publish a small of the amount of their data, which is the stage this incident appears to be at with so-called proofs," Callow says. "Should the company still not pay," he adds, "more data is published, sometimes on a staggered basis, to ramp up the pressure on the company." If this pressure does not prove enough, there have been previous cases where data is

posted to notorious Russian cybercrime forums informing the recipients to use it in any way they want.

"The threat level is the same as ever, perhaps even higher," Callow warns, "and ransomware groups should not be provided with a platform that enables them to downplay that fact." In the meantime, Emsisoft is offering to help hospitals and healthcare providers hit by ransomware free of charge.

Follow me on Twitter or LinkedIn. Check out my website or some of my other work here.