Maze Ransomware Targets the Hospitals and Labs Fighting Coronavirus | Tripwire

By Guest Authors

Published: 2020-05-05 · Archived: 2026-04-06 02:57:36 UTC

"Never let a good crisis go to waste." These wise words have been recently attributed to former Bill Clinton Chief of Staff Rahm Emanuel, though Freakonomics actually dates it back to 1976 and a completely different context. Regardless of who first uttered the phrase or some permutation of it, modern-day cybercriminals have taken the candid advice to heart and ramped up ransomware attacks on hospitals, labs, and other medical facilities that are engaged in the battle to keep the upper hand on Covid-19. We all remember ransomware, right? Before the recent pandemic consumed the entire news cycle, ransomware was all the rage as malicious hackers took over increasingly larger computer networks, even those used by major universities and cities, to threaten data destruction unless their ransom demands were paid in Bitcoin. Now the bad guys are going after the people on the frontlines who are trying to keep us alive.

https://commons.wikimedia.org/wiki/File:Ransomware-pic.jpg

Deploying Maze

In the early stages of Covid-19, hacking groups pledged to leave hospitals and medical organizations alone for a few weeks or until the outbreak subsided. Almost immediately after these assurances were given, a London-based lab, Hammersmith Medicines Research, an outfit that was researching vaccines, found itself under attack from a ransomware variant known as Maze. Soon similar attacks rolled out across the world. It was obvious that promises from these criminals had absolutely zero value. In the world of Dark Web entrepreneurialism, nothing is sacred, not even human life. Maybe especially *not* human life as it serves as the most powerful bargaining chip. Medical professionals might remember Hammersmith as the outfit that was involved with an Ebola solution a few years back and is making great strides on both Alzheimer's disease research and the Covid front. Maze has been the ransomware of choice during the current proliferation of attacks and, as might be expected, it comes with a clever (some might say evil) twist. In addition to the typical Bitcoin payment, Maze, which was discovered in May 2019, also threatens to post patient records online. This final twist of the knife of publicly posting private data puts an organization in immediate violation of GDPR and at risk of massive fines. Several hackers have already shown that the threat to release records is not an idle one. Some records have been released when organizations have chosen not to pay.

https://en.wikipedia.org/wiki/File:Mckie_cartoons_pants_ransom.jpg

The Good Guys Respond

You know it's a serious global issue when the International Criminal Police Organization (INTERPOL) gets involved, as they have with the current spate of Maze incursions. The organization has partnered with private

firms to come up with best-practice security and privacy tactics and are actively pursuing the capture and prosecution of various malfeasance engaged in this odious game. But in the final analysis, the same prevention and mitigation strategies that cybersecurity experts have been advising for years are the boots-on-the-ground solution. The delivery method of choice thus far has been via emails containing links that, once clicked, download the bug into your system. If you don't want the bug, don't click. So, here's a bit of handy advice to write down on a wall beside your desk somewhere: Don't click on email links unless you know *for sure* where it came from. Interpol has a half dozen tips that healthcare organizations should implement immediately. Among them are the following:

- As mentioned, don't click an email link or download a software or application unless you have triple-checked its authenticity.
- To emphasize, do NOT click email links or open attachments unless it is something you specifically requested or asked to receive. In other words, if it's an unknown sender, don't even think about touching it.
- Install state-of-the-art spam protection on email accounts. The latest generation of AI-powered spam detection applications has become fairly sophisticated at picking off the bad stuff and "learns" the longer it is in place.
- Backup system files and all data regularly, either to an external drive or, even easier, to a secured cloud storage account. If you have a copy of everything stored offsite, meaning separate from your working network, it's a simple matter to erase the ransomware and restore your system with the most recent backup.
- Keep anti-virus and anti-malware software installed, running, and up-to-date on your network and all mobile devices. Any point where the network is accessed from the outside is a threat vector. Regular software updates are a huge necessity so don't neglect this, as failure to do so opens your network to malware infection and/or zero-day exploits.
- You've probably heard this a lot already, but create strong, unique passwords for the network and all users and require them to be changed regularly.

Final Thoughts

The last bit of advice for healthcare organizations struggling to stay on top of Covid-19 and fight off hacker attacks at the same time. Pay attention to the prevention strategies up there, none of which require a degree in cybersecurity to implement. They just take a little time, which is admittedly in short supply right now, but if it prevents a complete system take-down, it's worth making room. Good luck and stay out of the Maze. By the way, Hammersmith refused to pay the ransom, so the hackers released some records publicly, though the company says the documents were a few decades old and not traceable to individuals.

About the Author: *Gary Stevens is an IT specialist who is a part-time Ethereum dev working on open source projects for both QTUM and Loopring. He's also a part-time blogger at Privacy Australia, where he discusses online safety and privacy.* **Editor's Note:** *The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.*
