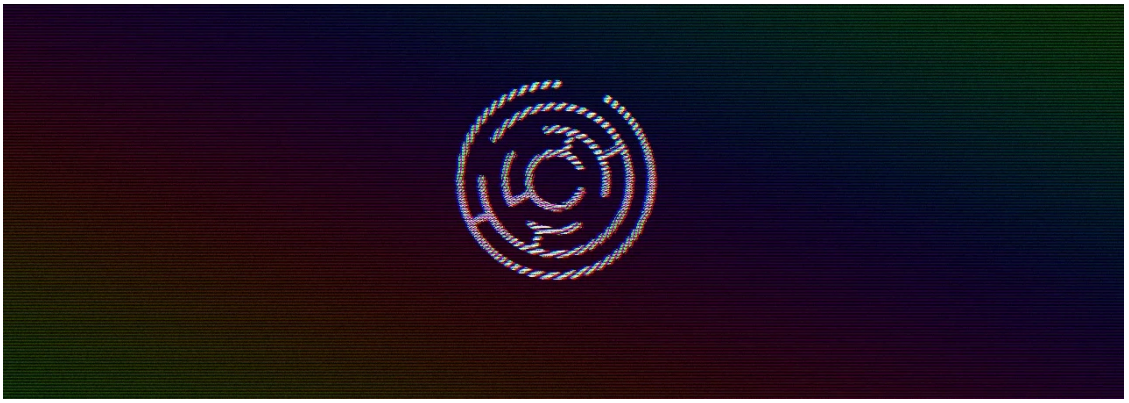
# Maze Ransomware Not Getting Paid, Leaks Data Left and Right

By Ionut Ilascu

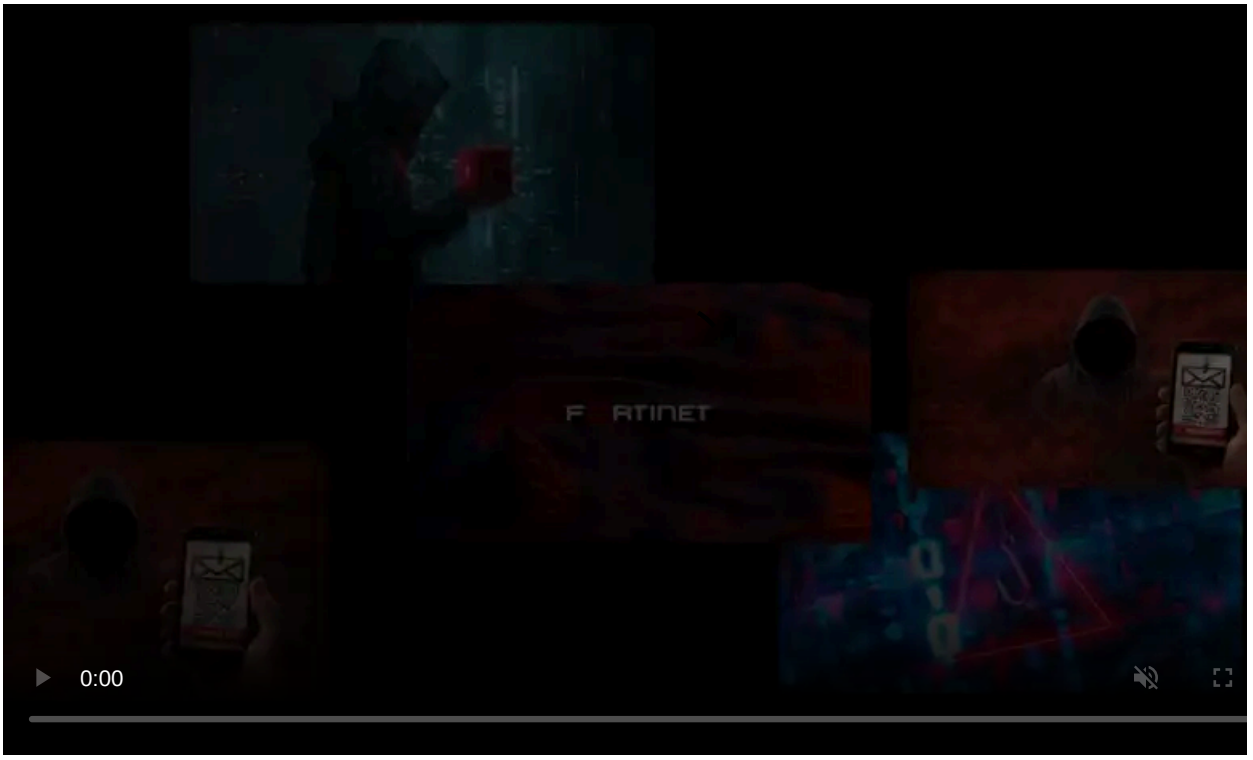
Published: 2020-01-23 · Archived: 2026-04-05 21:05:11 UTC

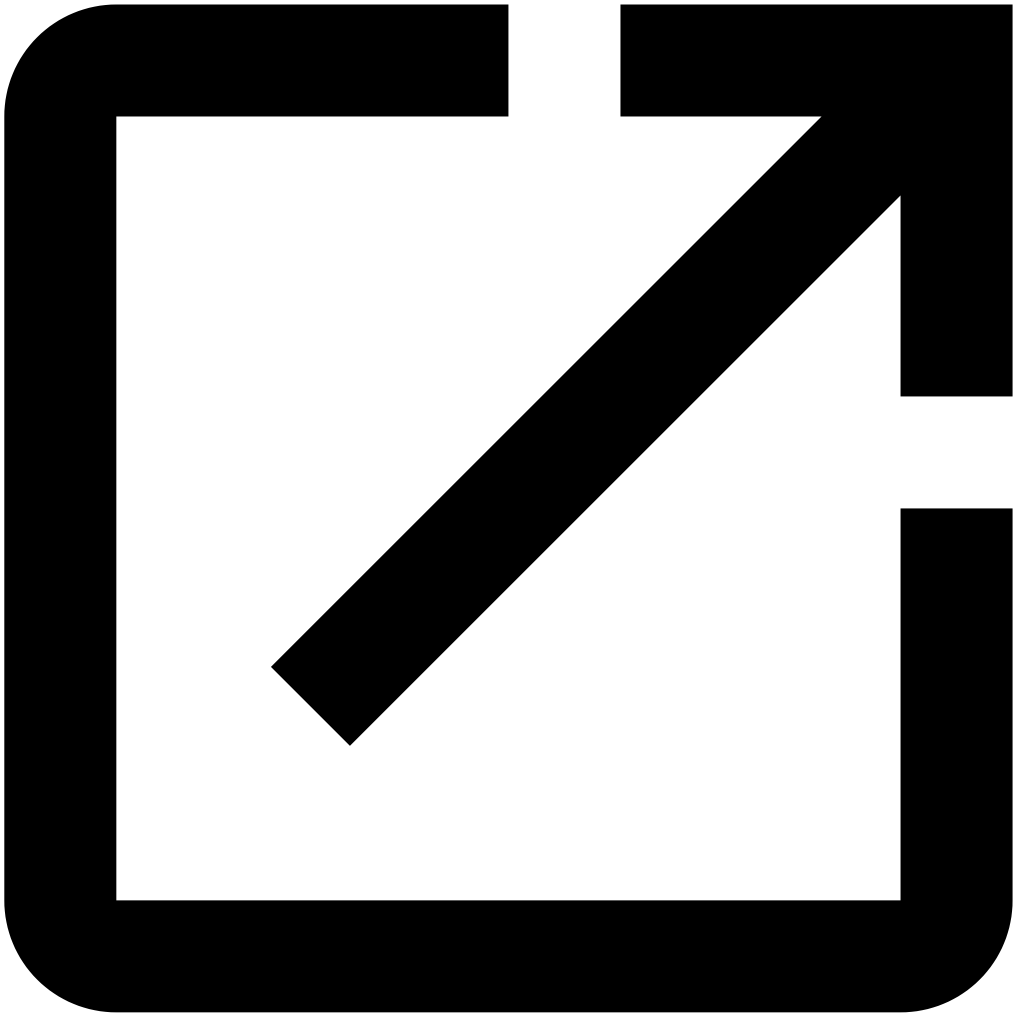


Maze ransomware operators have infected computers from Medical Diagnostic Laboratories (MDLab) and are releasing close to 9.5GB of data stolen from infected machines.

The actor also followed through with leaking an additional cache of files belonging to another of its victims that did not pay the ransom, Southwire, a wire and cable manufacturer from Carrollton, Georgia.

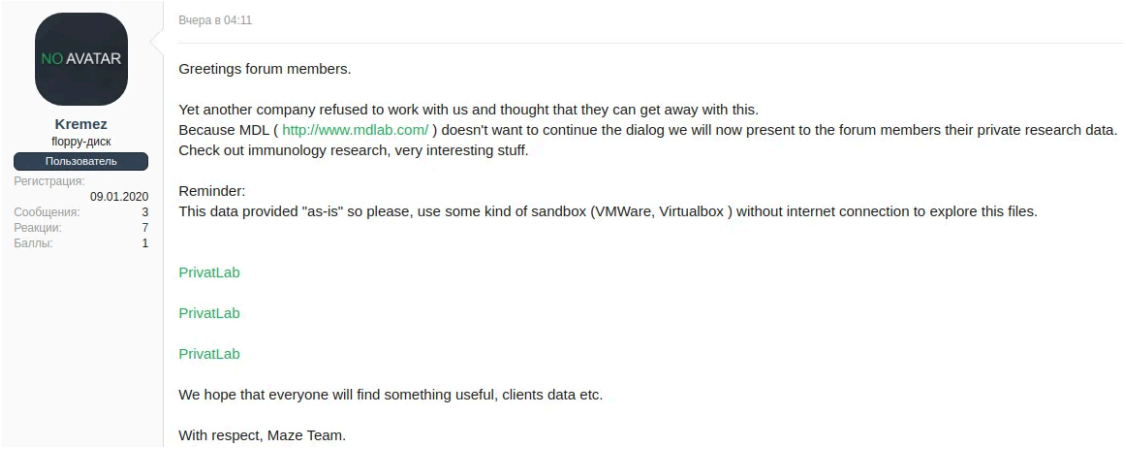
This action was prompted by the company's refusal to pay a ransom of 200 bitcoins (a little over $1.7 million today) that would buy from the attacker the file decryption key from the attacker and the promise to destroy the data.


F RTINET
0:00



## Between rock and a hard place

In a post on a forum, Maze says that "another company [MDLab] refused to work with us and thought that they can get away with this." As a result of halting the negotiations, the actor is releasing a cache of files exfiltrated from MDLab's computers to rekindle the discussion.




On their website, Maze says that files on 231 MDLab stations were encrypted on December 2, 2019 (date seems to be in European format).

The infected computers stored tens of terabytes of data but the actor told BleepingComputer that they exfiltrated archives totaling 100GB, which they plan to make public if the ransom is not paid. Some of the files relate to immunology research done by the company.

"Ransom amount: 100 BTC + 100 BTC. One part is for decryption, the second is for data destruction," the actor told us, adding that MDLab tried to get the purchase the cryptocurrency but could not do it" - Maze Ransomware

Maze further said that they directed MDLab to ransomware recovery company Coveware to negotiate the payment and seal the deal.

However, Coveware has a strict policy of not responding to referrals from ransomware actors, "even if the company is genuine and needs our help."

This may seem like a harsh, illogical reaction, but it is motivated by a simple principle:

"We don't want there to be any ambiguity on what side we are on, and any policy short of that would blur that line so we are strict about it. Any financial benefit from a criminal's referral is wrong in our book," Coveware.

This does not mean that the company leaves victims on their own as Coveware will point them in the right direction when this is possible.

The company denied being involved in negotiations with Maze on MDLab's part:

"That being our policy, the name you mentioned [MDLab] is also not familiar. We have not had any interaction with Maze about them, and don't have interactions with these groups outside of when we are negotiating on a client's behalf (which we would keep confidential)."

Coveware may have been contacted by Genesis Biotechnology Group, MDLab's parent company, which would explain why the name did not ring a bell to them.

MDLab has not reacted in any way about this incident. BleepingComputer reached out to the parent company for comment about the breach but received no answer at publishing time.

## New data leaked from Southwire

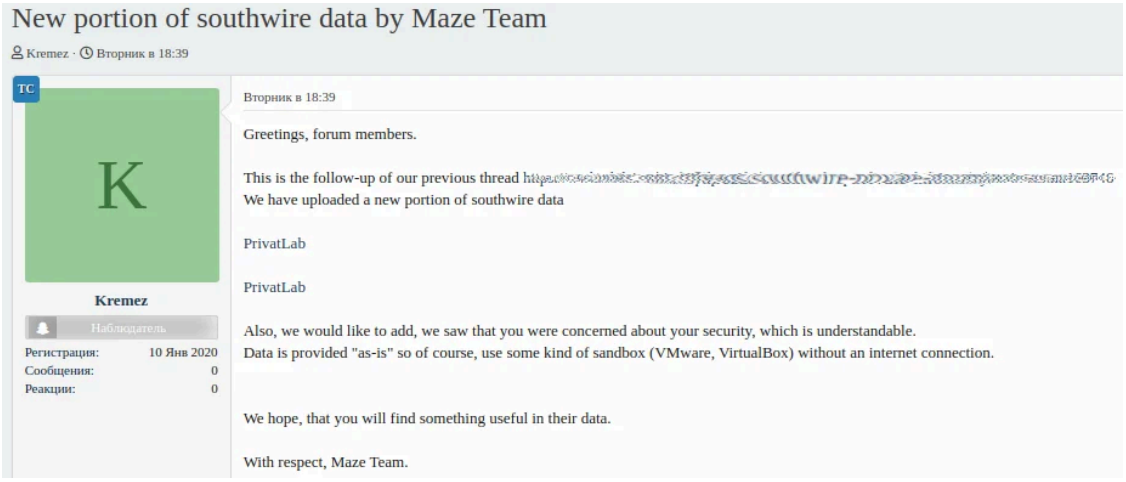
Maze keeps the Southwire data leaks going and releases two new archives allegedly stolen from the computers of the wire and cable manufacturer.

News of the attack emerged in mid-December and the ransom demand was 850 bitcoins, about $6 million at the time, as confirmed to us by the threat actor. In total, 120GB of data was stolen before encrypting 878 devices on the network.

Some time after the attack, seeing that they don't get paid, Maze operators published some company data to a site they controlled. Things escalated when Southwire filed a law suite against Maze that ended with the site being taken down temporarily. The effect was that Southwire data was no longer available to the public.

This did not stop Maze from spreading 14.1GB of the company files on a Russian hacking forum, though. They also promised to release 10% of the data every week until they get paid, or run out of files, something that could cause significant trouble to Southwire.

In a post on a Russian forum today, Maze announced that a fresh batch of Southwire data - two archives totaling about 10GB.



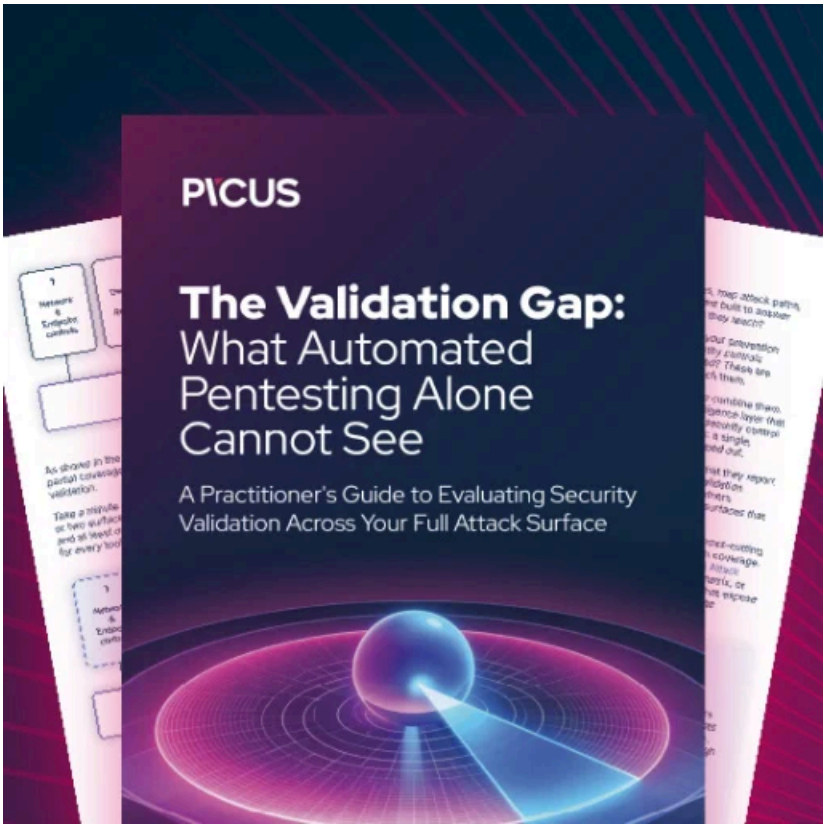

## Data theft changes the ransomware game

Late last year, Maze started this trend of threatening victims with publishing their files unless they paid after one of their victims, security staffing firm Allied Universal, missed the payment deadline.

They have been keeping their word and inspired other ransomware actors to do the same. Sodinokibi, Nemty, and BitPyLock adopted the same tactic (1, 2, 3).

Paying cybercriminals is not recommended as this encourages them to continue their business. Recovering from a ransomware attack is possible when backups are available. These incidents were not regarded as data breaches before the blackmail trend emerged.

This is a complication for victim companies as data stolen in a cyber attack requires a different reaction and can have drastic consequences (fines from data privacy watchdogs, secrets revealed to competitors, reputation damage), all leading to financial loss.




## Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/