# Maze Ransomware Demands $6 Million Ransom From Southwire

By Sergiu Gatlan

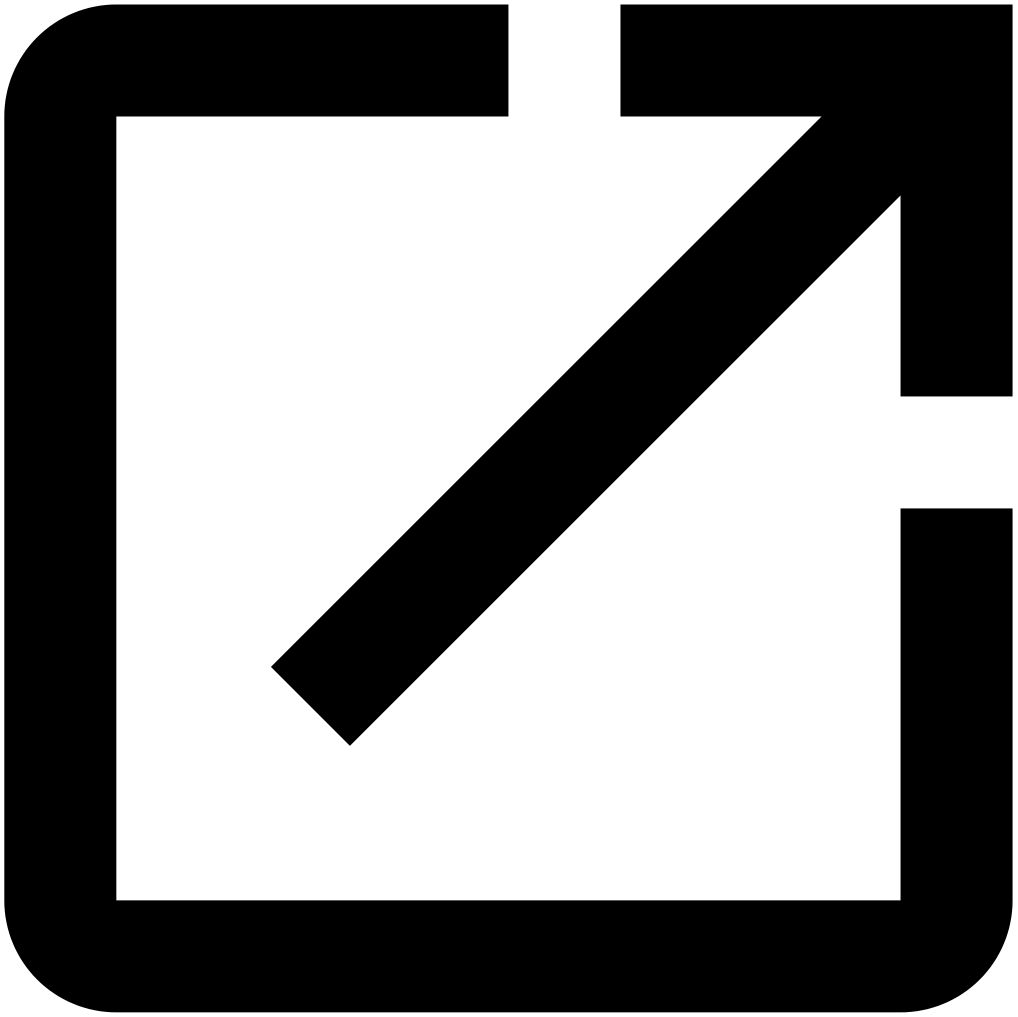
Published: 2019-12-12 · Archived: 2026-04-05 15:14:22 UTC


Maze Ransomware operators claim responsibility for another cyber attack, this time against leading wire and cable manufacturer Southwire Company, LLC (Southwire) from Carrollton, Georgia.

Southwire is one of North America's leading wire and cable makers, "building wire and cable, utility products, metal-clad cable, portable and electronic cord products, OEM wire products and engineered products" per a press release published in January 2019.

Maze Ransomware, a variant of Chacha Ransomware, was discovered by Malwarebytes security researcher Jérôme Segura in May. The malware strain has become increasingly more active starting with May 2019.


DIE LINKE.
0:00



Its affiliates are also increasingly more notorious, with ProofPoint identifying one as the TA2101 threat actor after observing them while conducting various malspam campaigns impersonating government agencies.

## $6 million ransom

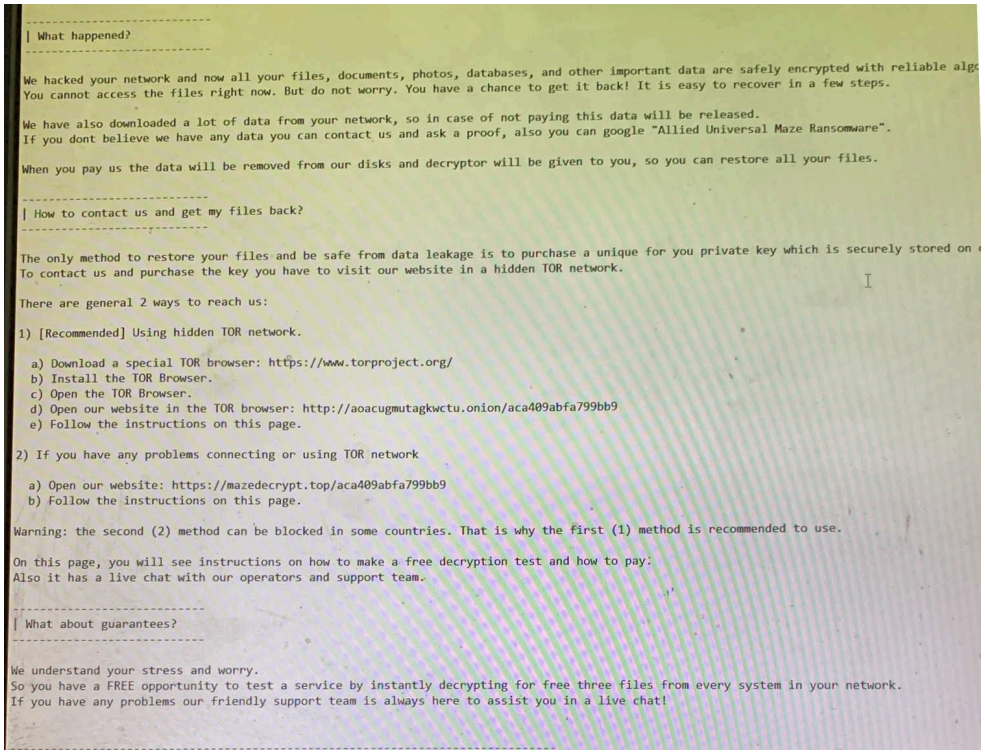
The ransom demanded is 850 BTC, amounting to approximately $6 million. As customary in the case of Maze Ransomware, the ransom note also says that company data has also been exfiltrated, ready to be published if the ransom is not paid.

In an email conversation with BleepingComputer, the group refuted rumors of a $9 million ransom that started on Reddit and also sent proof that Southwire data was downloaded from their servers.

"We would like to point out that we noticed this article here. Indeed that was our work, but they say the price is 9 millions USD, this is not true," they said.

"We do not know who spreads this rumors, the actual price for their network is 850 BTC which is about 6 million USD. We have attached some proofs of their data to this letter."

One of Southwire's employees working at the Rancho Cucamonga plant also shared the ransom note planted on the company's encrypted systems.



```
----------------------------
| What happened?
----------------------------

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable alg
You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have also downloaded a lot of data from your network, so in case of not paying this data will be released.
If you dont believe we have any data you can contact us and ask a proof, also you can google "Allied Universal Maze Ransomware".

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

----------------------------
| How to contact us and get my files back?
----------------------------

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on
To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR Browser.
  c) Open the TOR Browser.
  d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/aca409abfa799bb9
  e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

  a) Open our website: https://mazedecrypt.top/aca409abfa799bb9
  b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay:
Also it has a live chat with our operators and support team.

----------------------------
| What about guarantees?
----------------------------

We understand your stress and worry.
So you have a FREE opportunity to test a service by instantly decrypting for free three files from every system in your network.
If you have any problems our friendly support team is always here to assist you in a live chat!
```

**Southwire ransom note**

Maze ransomware's operators have recently claimed a number of other attacks including one against the City of Pensacola, Florida, that came with a $1 million ransom, and another one that impacted security staffing firm Allied Universal that was asked to pay $2.3 million to have their network decrypted.

## The Southwire ransomware attack

Southwire has been hit by the ransomware attack during early Monday and affected computing on a companywide basis.

The company's IT staff started getting affected systems back online one day later according to an Atlanta Business Chronicle report. Southwire's website is still down at the time this article was published.

"We immediately self-quarantined by shutting down the entire network," Jason Pollard, vice president of Talent Acquisition and Communications for the wire manufacturer told the Chronicle.

"The incident did cause some disruption in our ability to make and ship our products," he also added. When asked if the company reported the ransomware incident to law enforcement agencies, Pollard stated that Southwire is "considering all avenues that may assist us with this investigation."

The safety of our employees, the quality of our products and our commitment to our customers are critically important to us. Today, we're bringing critical systems back online, prioritizing manufacturing and shipping functions that enable us to create and send product to our customers. We are dedicated to restoring all systems and bringing all of our employees back to work as safely and as quickly as possible. - Pollard

Southwire has more than 7,500 employees and it had a revenue of $6.1 billion in 2018, topping the previous $5.5 billion from 2017. The wire manufacturer is also on Forbes' list of America's largest private companies.

BleepingComputer also reached out to Southwire for additional details regarding the attack but had not heard back at the time of this publication. This article will be updated with updated info when a response is received.



---

Source: https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/