MAZE Relaunches "Name and Shame" Website

By Sarah Coble

Published: 2020-01-10 · Archived: 2026-04-05 19:48:22 UTC

A threat group has once again taken to the internet to publish data stolen from alleged victims who refuse to cooperate with its ransom demands.

In December 2019, the MAZE ransomware group published online a portion of the 120 GB of data they claimed to have stolen from Southwire, North America's most prominent wire and cable manufacturer, after the company refused to pay a $6m ransom.

The data was published on the http(colon)//mazenews(dot)top/ site, which was hosted at an ISP in Ireland. Southwire subsequently filed a lawsuit in the Northern District of Georgia, USA, on December 31 against the MAZE operators and won their case, and the site was taken down.

But yesterday at around 5 p.m. ET the "mazenews" website was back up online, this time hosted out of Singapore via Alibaba.

Using an ominous black backdrop and bright red text, the website lists the companies that have allegedly been compromised. In some instances, the total amount of data that has been exfiltrated is also displayed.

On the site, MAZE states: "Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!"

Companies listed so far are Southwire, RBC, THEONE, Vernay, Bakerwotring, BILTON, greccoauto, Groupe Igrec, Mitch Co International, Einhell, CONTINENTALNH3, Groupe Europe Handling SAS, Auteuil Tour Eiffel, Fratelli Beretta, Randalegal, crossroadsnet, SAXBST, American tax advisory firm BST & Co, and laboratory testing facility MDL. The Florida city of Pensacola is also listed.

Downloadable files, presented as proof that a compromise has taken place, are available for Einhell, Fratelli Beretta, Crossroadsnet, MDL, BST & Co, SAXBST, Auteuil Tour Eiffel, and Southwire. Under the "proofs" category for the other companies, MAZE has written only "coming soon."

The ransomware group claims to have exfiltrated 3 GB of data from Fratelli Beretta, and 25 GB of data each from SAXBST and BST & Co. MAZE further claims that 10% of the 120 GB it allegedly stole from Southwire is "available for downloading."

For some unstated reason, the threat group showed mercy on alleged victim Pensacola.

"We are going to make a gift to City of Pensacola: we will not publish leaked private data, but we publish the list of leak data and hosts to proof, that we did it, we really hacked City of Pensacola," wrote MAZE.

The city's operational departments that MAZE claims to have compromised include the treasury, finance, risk management, executive, legal, housing, and human resources departments.
