Maze ransomware is shutting down its cybercrime operation

bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/

Lawrence Abrams

By
Lawrence Abrams

- October 29, 2020
- 12:31 AM
- 1

The Maze cybercrime gang is shutting down its operations after rising to become one of the most prominent players performing ransomware attacks.

The Maze ransomware began operating in May 2019 but became more active in November.

That's when the media-savvy operation revolutionized ransomware attacks by introducing a double-extortion tactic.

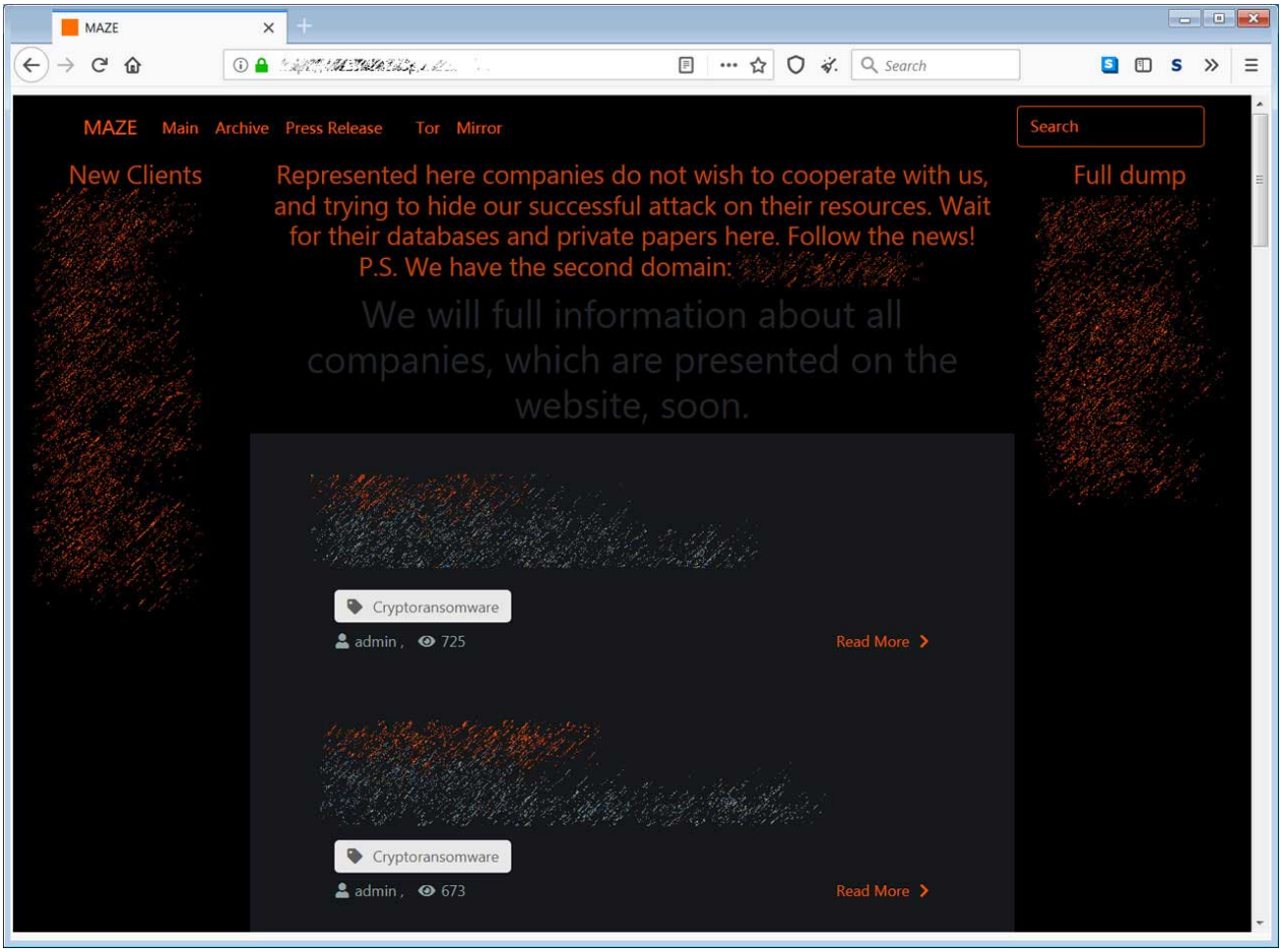
First, they steal your files, then encrypt them

While ransomware operations have always enjoyed taunting news sites and researchers, for the most part, they tended to ignore journalists' emails.

This changed in November 2019, when Maze contacted BleepingComputer to let us know that they stole the unencrypted data for Allied Universal before encrypting them.

Maze stated that if Allied didn't pay a ransom, their data would be publicly released. Ultimately, the ransom was not paid, and Maze released the stolen data.

Soon after, Maze launched a 'Maze News' site that they use to publish non-paying victims' data and issue "press releases" for journalists who follow their activities.



Maze data leak site

This double-extortion technique was quickly adopted by other large ransomware operations, including REvil, Clop, DoppelPaymer, who released their own data leak sites. This double-extortion technique has now become a standard tactic used by almost all ransomware operations.

Maze continued to evolve ransomware operations by forming a ransomware cartel with Ragnar Locker and LockBit, to share information and tactics.

During their year and a half cybercrime spree, Maze has been responsible for attacks on notable victims, including Southwire, City of Pensacola, Canon, LG Electronics, Xerox, and many more.

Maze started to shut down six weeks ago

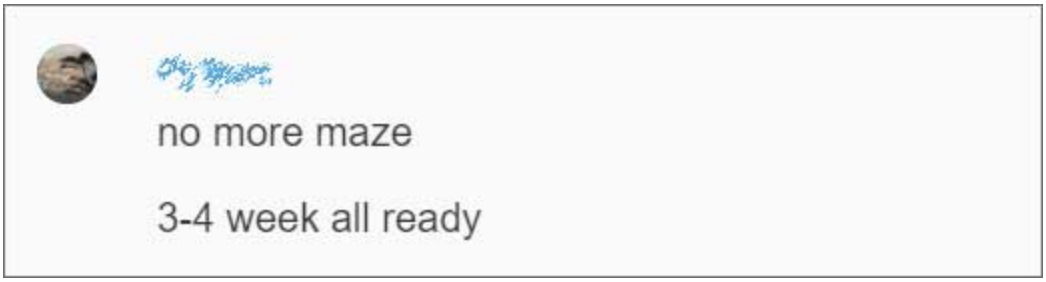
Early last month, BleepingComputer began hearing rumors that Maze was getting ready to shut down their ransomware operation in a similar manner as GandCrab did in 2019.

The closing of operations was later confirmed after BleepingComputer was contacted by a threat actor involved in the Barnes and Noble ransomware attack.

This threat actor stated that they take part in ransomware attacks by compromising networks and stealing Windows domain credentials. The compromised networks are then passed to affiliates who deploy the ransomware.

The group compromising networks, the affiliate, and ransomware developers then take equal shares of any ransom payments.

As part of our conversation, BleepingComputer was told that Maze was in the process of shutting down its operation, had stopped encrypting new victims in September 2020, and are trying to squeeze the last ransom payments from victims.



BleepingComputer told that Maze is shut down

When BleepingComputer reached out to Maze to confirm if they were shutting down, we were told, "You should wait for the press release."

This week, Maze has started to remove victims that they had listed on their data leak site. All that is left on the site are two victims and those who previously and had all of their data published.

The cleaning up of the data leak site indicates that the ransomware operation's shutdown is imminent.

It is not uncommon for ransomware operations to release the master decryption keys when they shut down their operation, as was done with Crysis, TeslaCrypt, and Shade.

BleepingComputer has reached out to Maze to ask if they will release their keys when they shut down their operation but have not heard back.

Affiliates move to Egregor ransomware

BleepingComputer has learned that many Maze affiliates have switched over to a new ransomware operation called Egregor.

Egregor began operating in the middle of September, just as Maze started shutting down their encryption operation. It quickly became very active, as seen by the ID-Ransomware submission graph below.

Egregor submissions graph to ID-Ransomware

Egregor is believed to be the same underlying software as both Maze and Sekhmet as they utilize the same ransom notes, similar payment site naming, and share much of the same code.

This was also confirmed by a ransomware threat actor who stated that Maze, Sekhmet, and Egregor were the same software.

Ransomware expert Michael Gillespie, who analyzed both Egregor and Sekhmet, also found that Egregor victims who paid a ransom were sent decryptors that were titled 'Sekhmet Decryptor.'

Egregor decryptor

Unfortunately, this shows that even when a ransomware operation shuts down, it does not mean the threat actors involved retire as well. They just move to the next ransomware operation.

Related Articles:

New RansomHouse group sets up extortion market, adds first victims

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

- Cyberattack
- Cybercrime
- Maze
- Ransomware
- Retirement

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

megakotaro - 1 year ago

-
-

Although they shut down, they didn't release free decrypter did they?

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: