Maze: the ransomware that introduced an extra twist | Malwarebytes Labs

By Pieter Arntz

Published: 2020-05-28 · Archived: 2026-04-05 19:10:07 UTC

An extra way to create leverage against victims of ransomware has been introduced by the developers of the Maze ransomware. If the victim is not convinced that she should pay the criminals because her files are encrypted, there could be an extra method of extortion. Over time, more organizations have found ways to keep safe copies of their important files or use some kind of rollback technology to restore their systems to the state they were in before the attack.

To have some leverage over these organizations, the ransomware attackers steal data from the infiltrated system while they deploy their ransomware. They then threaten to publish the data if the victim decides not to pay. Depending on the kind of data, this can be a rather compelling reason to give in.

Maze introduces leaked data

In the last quarter of 2019, Maze's developers introduced this new extortion method. And, as if ransomware alone wasn't bad enough, since the introduction of this methodology, many other ransomware peddlers have started to adopt it. The most well-known ransomware families besides Maze that use data exfiltration as a side-dish for ransomware are Clop, Sodinokibi, and DoppelPaymer.

The dubious honor of being noted as the first victim went to Allied Universal, a California-based security services firm. Allied Universal saw 700MB of stolen data being dumped after they refused to meet the ransom demand set by Maze. Nowadays, most of the ransomware gangs involved in this double featured attack have dedicated websites where they threaten to publish the data stolen from victims that are reluctant to pay up.

Characteristics of Maze ransomware

Maze ransomware was developed as a variant of ChaCha ransomware and was initially discovered by Malwarebytes Director of Threat Intelligence Jérôme Segura in May of 2019. Since December of 2019, the gang

has been very active making many high profile victims in almost every vertical: finance, technology, telecommunications, healthcare, government, construction, hospitality, media and communications, utilities and energy, pharma and life sciences, education, insurance, wholesale, and legal.

The main forms of distribution for Maze are:

- malspam campaigns utilizing weaponized attachments, mostly Word and Excel files
- RDP brute force attacks

Initially Maze was distributed through websites using an exploit kit such as the Fallout EK and Spelevo EK, which has been seen using Flash Player vulnerabilities. Maze ransomware has also utilized exploits against Pulse VPN, as well as the Windows VBScript Engine Remote Code Execution Vulnerability to get into a network.

No matter which method was used to gain a foothold in the network, the next step for the Maze operators is to obtain elevated privileges, conduct lateral movement, and begin to deploy file encryption across all drives. However, before encrypting the data, these operators are known to exfiltrate the files they come across. These files will then be put to use as a means to gain extra leverage, threatening with public exposure.

MAZE uses two algorithms to encrypt the files, ChaCha20 and RSA. After encryption the program appends a string of random 4-7 characters at the end of each file. When the malware has finished encrypting all the targeted files it changes the desktop wallpaper to this image:

In addition, a voice message is played to the user of the affected system, alerting them of the encryption.

IOCs for Maze ransomware

Maze creates a file called DECRYPT-FILES.txt in each folder that contains encrypted files. It skips some folders among which are:
• %windir%
• %programdata%
• Program Files
• %appdata%local

It also skips all the files of the following types:
• dll
• exe

• lnk
• sys

This ransom note called DECRYPT-FILES.txt contains instructions for the victim:

```
Attention!

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

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

We have also downloaded a lot of private data from your network, so in case of not contacting us as soon as possible this
data will be released.
If you do not contact us in a 3 days we will post information about your breach on our public news website and after 7
days the whole downloaded info.

To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware

After the payment 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 our servers.
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:/[redacted].onion/xxxxxxx
  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/xxxxxxxx
  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!

P.S. Dear system administrators do not think you can handle it by yourself. Inform leadership as soon as possible.
By hiding the fact of the breach you will be eventually fired and sometimes even sued.----------------------------------
----------------------------------------
THIS IS A SPECIAL BLOCK WITH A PERSONAL AND CONFIDENTIAL INFORMATION! DO NOT TOUCH IT WE NEED IT TO IDENTIFY AND AUTHORIZE
YOU
---BEGIN MAZE KEY---
%base64key%
---END MAZE KEY---
```

They then promise that:

> After the payment the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

SHA 256 hashes:

19aaa6c900a5642941d4ebc309433e783befa4cccd1a5af8c86f6e257bf0a72e

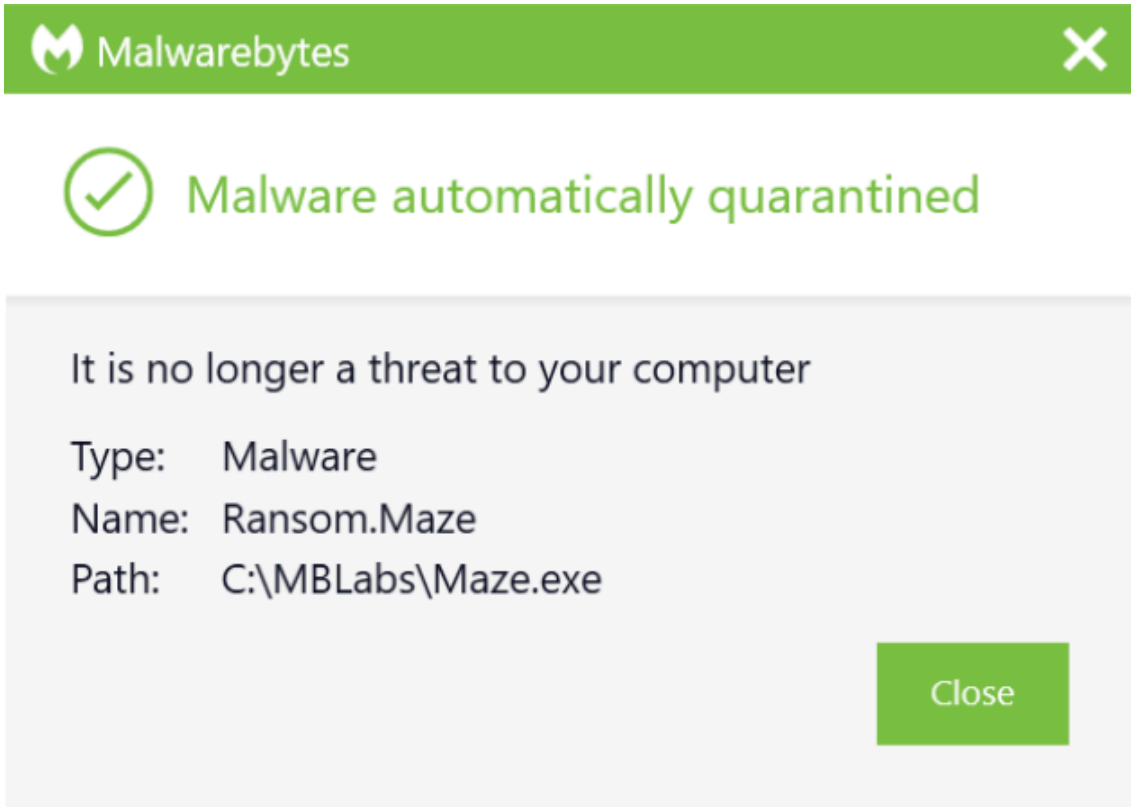
6878f7bd90434ac5a76ac2208a5198ce1a60ae20e8505fc110bd8e42b3657d13

9ad15385f04a6d8dd58b4390e32d876070e339eee6b8da586852d7467514d1b1

b950db9229db2f37a7eb5368308de3aafcea0fd217c614daedb7f334292d801e

Protection

Malwarebytes protects users with a combination of different layers including one that stops the attack very early on and is completely signature-less.



Besides using Malwarebytes, we also recommend to:

- Deny access to Public IPs to important ports (RDP port 3389).
- Allow access to only IPs which are under your control.
- Along with blocking RDP port, we also suggest blocking SMB port 445. In general, it is advised to block unused ports.
- Apply the latest Microsoft update packages and keep your Operating system and antivirus fully updated.

Payments

While our advice as always is not to pay the criminals since you are keeping their business model alive by doing so, we do understand that missing crucial files can be a compelling reason to pay them anyway. And with the new twist of publishing exfiltrated data that the Maze operators introduced, there is an extra reason at hand. Throwing confidential data online has proven to be an effective extra persuasion as many organizations can’t afford to have them publicly available.

Stay safe, everyone!

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
