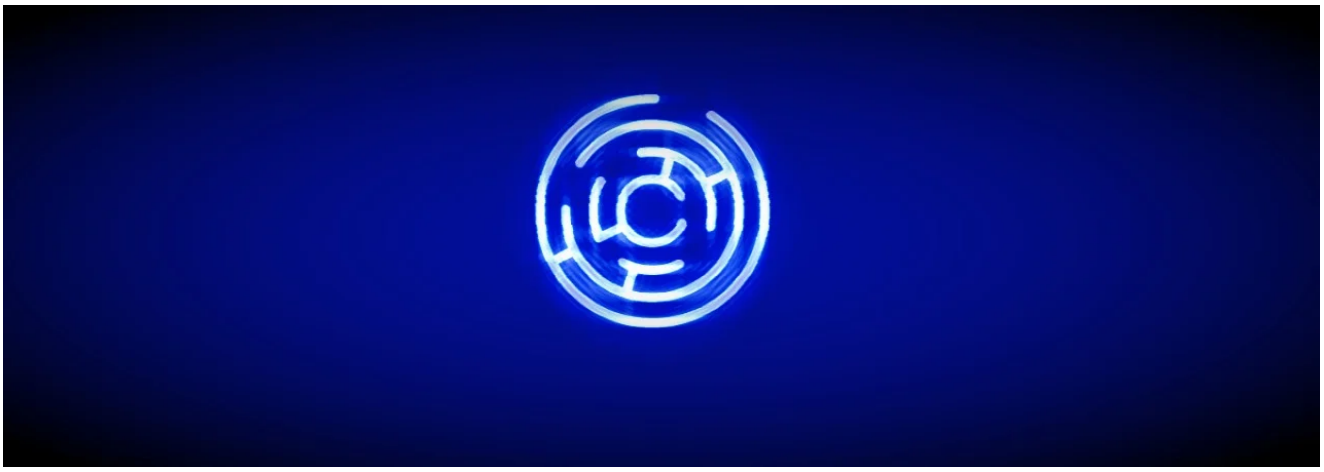
Maze Ransomware Behind Pensacola Cyberattack, $1M Ransom Demand

bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/

Lawrence Abrams

By
Lawrence Abrams

- December 11, 2019
- 01:57 PM
- 2



The operators behind the Maze Ransomware have claimed responsibility for the cyberattack affecting the City of Pensacola, Florida, but state that they are not affiliated with the recent shooting at NAS Pensacola.

In an email conversation with BleepingComputer, the operators of the Maze Ransomware stated that they were responsible for encrypting the city's data and have demanded a $1,000,000 ransom for a decryptor.

When Maze targets a network, they will steal the victim's files before they are encrypted. The attackers then tell the victim that they will publicly release these files unless the ransom is paid.

Maze is not the first ransomware to make these claims, but as we have seen with the release of Allied Universal's documents, the Maze crew appears to be willing to follow up with their threats.

Maze has shared documents that were allegedly stolen from the city, but did not state if they have given a deadline to Pensacola or will release them.

One item that appeared to be of concern to the Maze operators was the timing of their attack.

Without our prompting, the Maze Ransomware operators expressed concerns about being linked to the recent NAS Pensacola shooting and told BleepingComputer that they had nothing to do with it.

"We also must tell you that there is no any connections with the shooting event that occurred before running maze. We did not know about this. It is just coincidence."

Maze states they avoid emergency services

Maze also wanted to reassure us that they purposely avoided emergency services, or what they call 'socially significant services', such as 911.

"Also we want to emphasize that no one of the socially significant services has suffered (for example 911)."

When we asked if they purposely avoided services like these, they told us that medical care centers or other 'socially vital objects' are not allowed and will decrypt any that are encrypted for free.

"We don’t attack hospitals, cancer centers, maternity hospitals and other socially vital objects, up to the point that if someone uses our software to block the latter, we will provide a decrypt for free."

City Recovering

When we attempted to confirm if the information provided by Maze is accurate, Kaycee Lagarde, Public Information Officer for the City of Pensacola, told BleepingComputer that due to ongoing investigations they could not provide additional details.

Lagarde did tell us that the city is slowly recovering and that their mail servers are back up and that most landlines have been restored. Employees, though, continue to be unable to access their computers or the Internet until all of the issues are resolved.

We are currently in an assessment and recovery mode, and our IT Department is continuing to work diligently to make sure all computers are free of any viruses before we reconnect them to the network. We don’t have an estimated time of completion, but they are working to restore services as quickly as possible. As IT works to restore services, they are also looking into bringing experts in to assist with evaluating any potential impacts to data.

Our email servers are back up, but since IT still has our computers disconnected from the network, city employees only have limited access to email (via smartphone for employees who have city cell phones).

Most landlines have been restored.

The city remains operational, but we are somewhat limited since we aren't able to use our computers or internet until these issues are resolved. Emergency dispatch and 911 services were not impacted and continue to operate. Our website at cityofpensacola.com and online permitting services at mygovernmentonline.org were not impacted and remain operational.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New 'Cheers' Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt's ransomware fight hindered by limited reporting

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.