

Maze ransomware was behind Pensacola “cyber event,” Florida officials say

Enlarge / Pensacola was hit by Maze ransomware, which has apparently stolen data before encrypting it in other cases.

Paul Harris / Getty Images

reader comments

14 with 13 posters participating

Share this story

An email sent by the Florida Department of Law Enforcement to all Florida county commissioners indicated that the ransomware that struck the city of Pensacola on December 7 was the same malware used in an attack against the private security firm Allied Universal, according to a report by the Pensacola News Journal. That malware has been identified elsewhere as Maze, a form of ransomware that has also been distributed via spam email campaigns in Italy.

Bleeping Computer's Lawrence Abrams reported in November that the Maze operators had contacted him after the Allied Universal attack, claiming to have stolen files from the company before encrypting them on the victims' computers. After Allied apparently missed the deadline for payment of the ransom on the files, the ransomware operators published 700 megabytes of files from Allied and demanded 300 Bitcoins (approximately \$2.3 million) to decrypt the network. The Maze operators told Abrams that they always steal victims' files to use as further leverage to get them to pay:

It is just a logic. If we disclose it who will believe us? It is not in our interest, it will be silly to disclose as we gain nothing from it. We also delete data because it is not really interesting. We are neither espionage group nor any other type of APT, the data is not interesting for us.

Stealing data as proof of compromise—and to therefore encourage payment by ransomware victims—is rare but not new. The RobbinHood ransomware operator that attacked Baltimore City in May also stole files as part of the attack and posted screenshots of some files—faxed documents sent to Baltimore City Hall’s fax server—on a Twitter account to encourage city officials to pay. Baltimore did not pay the ransom.

Theft of data opens up another problem for targets of ransomware who in the past would pay quietly to decrypt their data, as it introduces the possibility that they will have to report the breach to customers and government regulators. So in some cases, it may ironically remove some of the motivation for victims to pay, since their data may be sold off by the attackers whether they pay or not.

The use of the data to blackmail the victim, and in Allied’s case, the threat to use Allied’s certificates and domain name to spam customers with additional ransomware attacks, is something new.”This is the first time this has ever happened, as far as we know,” said Brett Callow, a spokesperson for the antivirus software vendor Emsisoft.” Ransomware groups usually encrypt, not steal. We expect data exfiltration to become more and more commonplace. Whether Pensacola’s data was exfiltrated, I obviously can’t say.”

“Broad targeted” attacks

Maze, Ryuk, and other ransomware attacks against government agencies and companies have moved increasingly toward what Raytheon Cyber Services Senior Manager Dylan Owen referred to

as a “broad targeted” attack—while they rely on spam for the initial breach, the attackers “are poking around figuring out who they breached” before they launch the attack.

“They don’t necessarily target a specific agency,” Owen told Ars. “The attackers have often either gotten a list of emails from another source, or they “have programs that randomly try emails, or combinations of username, first name/last name, middle initial, all different kinds of combinations,” he explained. “They might do a little bit of research if they were going for a particular type of organization, but usually they’re very broad-based... then once they get a beacon back saying, ‘Hey, somebody clicked on my link’, they go and figure out who it was.” And if the click came from a larger organization rich in targets, Owen said, they go forward.

State and local agencies have been particularly vulnerable to these sorts of attacks because of the economics of their IT operations. “They’re dependent on the funding through taxes or whatever, and that money can only go so far,” Owen noted. “They also have a preponderance of older IT systems because of the lack of funding over the years. So it’s something that’s built upon itself. A lot of them also have proprietary software, so it’s not commercial, off the shelf—they hired somebody to create some special code, and that code may not run on newer operating systems. So now they have older operating systems that are harder to patch.”

On top of that, many state and local agencies haven’t done the work of segregating those vulnerable systems and putting additional defenses around them to reduce the risk posed by legacy systems, Owen explained. But he said that’s starting to change. “I know with Louisiana particularly, the governor had said that cyber security is going to be a really big focus for 2020,” he said. “They put a lot of money in it in 2019.” And while Louisiana had to take the drastic step of cutting off many services during the recent Ryuk attack, it was effective in stopping the spread of the attack.

<https://arstechnica.com/?p=1631441>