Package delivery giant Pitney Bowes confirms second ransomware attack in 7 months

By Written by Catalin Cimpanu, ContributorContributor May 11, 2020 at 9:13 a.m. PT

Archived: 2026-04-05 19:43:55 UTC

Package and mail delivery giant Pitney Bowes has suffered a second ransomware attack in the past seven months, *ZDNet* has learned.

The incident came to light today after a ransomware gang known as Maze published a blog post claiming to have breached and encrypted the company's network.

The Maze crew provided proof of access in the form of 11 screenshots portraying directory listings from inside the company's computer network.

pitney-bowes-maze-proof.png

Pitney Bowes confirmed the incident today in an email to *ZDNet*.

"Recently, we detected a security incident related to Maze ransomware. We are investigating the scope of the attack, specifically the type of data that had been accessed, which appears to be limited," a spokesperson said.

The company said it worked with third-party security consultants to take steps to stop the attack before any of its data was encrypted.

"At this point, there is no evidence of further unauthorised access to our IT systems," Pitney Bowes said, while also adding that "the investigation remains ongoing."

Second incident after the October 2019 Ryuk infection

In October 2019, Pitney Bowes disclosed a first ransomware attack. At the time, the company said it had some critical systems infected and encrypted by the Ryuk ransomware gang. The incident caused limited downtime to some package tracking systems.

Both the Ryuk and Maze ransomware gangs are what experts call "human-operated" ransomware strains. These types of ransomware infections take place after hackers breach a company's network, and take manual control of the malware to expand access to as many internal systems as possible before executing the actual ransomware to encrypt data and demand a ransom.

The Maze gang is different from Ryuk, though, as Maze also runs a website where it lists victims and leaks sensitive data if they don't pay the decryption (ransom) fee. Maze pioneered this tactic, and is currently one of nine ransomware gangs that run a "leak site."

The Maze gang has been very active this year, being behind a large number of high-profile ransomware infections, such as Chubb, Cognizant, Bouygues Construction, Southwire, the city of Pensacola, and more. Cyber-security firms Crowdstrike, FireEye, and Palo Alto Networks have recently noted this increase in activity from the Maze gang and have published reports analyzing the Maze gang's tactics and malware payloads.

In 2019, Pitney Bowes had more than 11,000 employees and pulled $3.2 billion in revenue. The company has expanded from its classic postage meter business and is one of today's most important delivery services for the e-commerce sector.

Being the victim of a human-operated ransomware gang is bad enough, but getting hit by two different gangs raises serious questions.

The FBI's most wanted cybercriminals

Security
