Double Extortion: An Emerging Ransomware Attack Pattern

Traditionally in Ransomware Attacks, cybercriminals deployed ransomware into the corporate network and encrypted all files and databases, locking the victims out of their own files. In order to get back to Business-as-usual, victims normally ended up paying attackers' ransom demand, hoping they would deliver the decryption keys. Had the victims refused to pay, their data and files would be destroyed.

As if that wasn't threatful enough, cybercriminals have come up with another tactic to inflict more pain on ransomware victims by adding an additional stage into their attacks – exfiltrating a copy of the data before encrypting and threatening the victim to publish it on their website or sell them to third parties, unless ransom demands are met. This evolution of ransomware attacks is referred as Double Extortion as it is a combination of a ransomware attack and a data breach.

Double Extortion, the most recent incarnation of ransomware attack, first emerged in late 2019 by the Maze Operators but has become quite prevalent in 2020. Researchers have found that many ransomware attack groups, such as Maze, REvil, DoppelPaymer etc., now boast of a dedicated website in which they list the names of non-cooperative victims and publish a sample of stolen data to put additional pressure on their victims. For instance, in the November 2019 attack against the Allied Universal, a large American security staffing company, the threat actors published 700 MB worth of stolen files including contracts, medical records (only 10% of the stolen information) when the company refused to pay 300 Bitcoin ($2.3 Million) ransom.

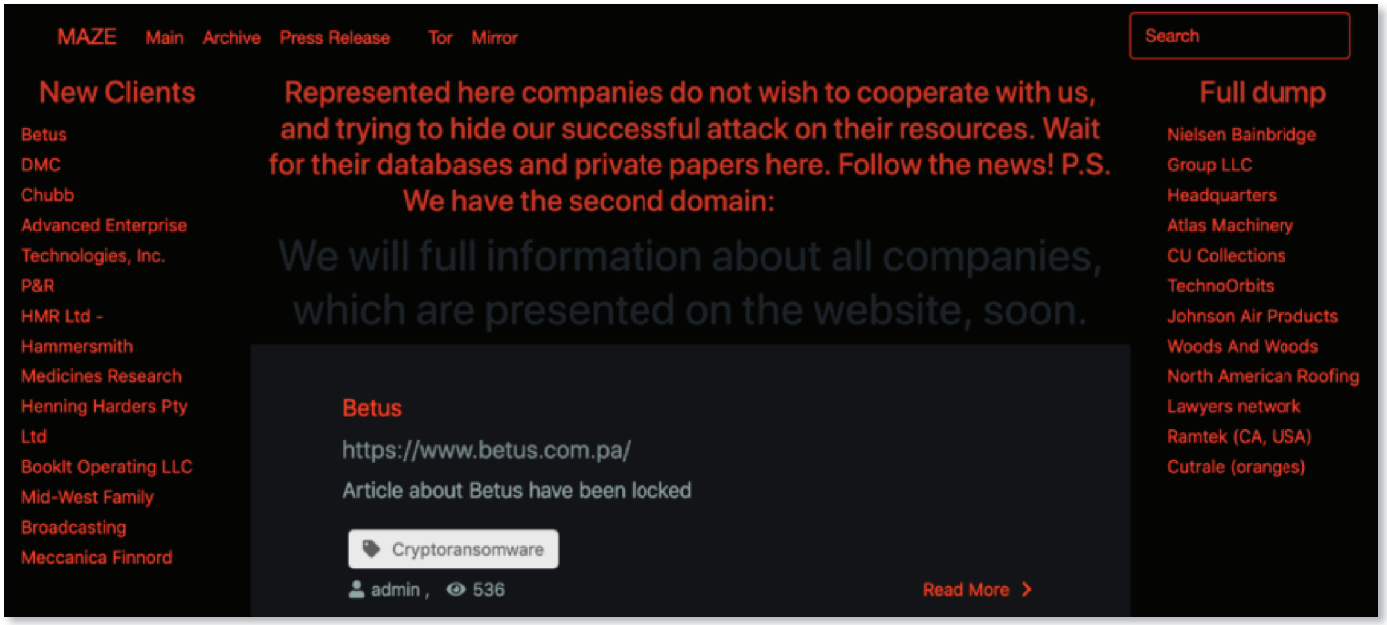

Fig1: Compromised data listed on Maze web page (Source: https://threatpost.com/double-extortion-ransomware-attacks-spike/154818/)