Egregor operation takes huge hit after police raids

intel471.com/blog/egregor-arrests-ukraine-sbu-maze-ransomware

Law enforcement action carried out last week in Ukraine has targeted the people behind some of the most notorious ransomware gangs of the past year.

On Feb. 9, 2021, Ukrainian law enforcement conducted a joint operation with U.S. and French authorities against several Ukrainian nationals believed to be deeply involved with Egregor ransomware operations. Intel 471 has learned that authorities targeted the purported ring leaders, as well as associates who helped run the related affiliate programs. Egregor is responsible for hundreds of ransomware attacks against high-profile targets worldwide since September 2020. According to law enforcement, over 150 companies have been hit by Egregor, resulting in losses of more than US$80 million.

The raid has hit Egregor hard. Following the law enforcement action, Egregor's blog, used to shame victims that didn't pay ransoms, was taken offline. Additionally, one of the associates appears to have deactivated his profile on one of the most popular forums on the cybercriminal underground.

While not confirmed by law enforcement, the arrests point to links between the Egregor operations and the Maze ransomware gang. In the late stages of 2020, Maze announced it was shutting down, with operations shifting to Egregor. It is widely believed among threat intelligence professionals that a large portion of the affiliates that were attached to Maze followed the move to Egregor. Members of those affiliate programs were either raided or arrested last week.

It is unclear how many people were targeted in the raid, but several Ukrainian press releases say the "organizer" was arrested. Intel 471 will continue to watch how the greater cybercrime underground reacts to the actions taken by law enforcement.