Appgate Labs Analyzes New Family of Ransomware— “Egregor”

Published: 2020-10-02 · Archived: 2026-04-06 00:40:31 UTC

MIAMI, FL – October 2, 2020 – This week our team analyzed a new family of ransomware that calls itself "Egregor", which seems to be a Sekhmet ransomware spin-off.

The threat group behind this malware seems to operate by hacking into companies, stealing sensitive data, and then running Egregor to encrypt all the files. According to the ransom note, if the ransom is not paid by the company within 3 days, and aside from leaking part of the stolen data, they will distribute via mass media where the company's partners and clients will know that the company was attacked.

The sample we analyzed has many anti-analysis techniques in place, such as code obfuscation and packed payloads. Also, in one of the execution stages, the Egregor payload can only be decrypted if the correct key is provided in the process' command line, which means that the file cannot be analyzed, either manually or using a sandbox, if the exact same command line that the attackers used to run the ransomware isn't provided. Furthermore, our team found the "Egregor news" website, hosted on the deep web, which the criminal group uses to leak stolen data.

At the time of this advisory, there is at least 13 different companies listed in their "hall of shame", including the global logistic company GEFCO, which suffered a cyber attack last week. Egregors' ransom note also says that aside from decrypting all the files in the event the company pays the ransom, they will also provide recommendations for securing the company's network, "helping" them to avoid being breached again, acting as some sort of black hat pentest team.

About Appgate

Appgate is the secure access company that provides cybersecurity solutions for people, devices and systems based on the principles of Zero Trust security. Appgate updates IT systems to combat the cyber threats of today and tomorrow. Through a set of differentiated cloud and hybrid security products, Appgate enables enterprises to easily and effectively shield against cyber threats. Appgate protects more than 1,000 organizations across government and business. Learn more at appgate.com.
