# Egregor Ransomware DFIR Analysis Report

By Author:

Archived: 2026-04-05 17:45:42 UTC

Egregor ransomware is part of the Sekhmet malware family that has been active since mid-September 2020. The ransomware operates by hacking into organizations, stealing sensitive user documents, encrypting data, and demanding a ransom to exchange encrypted documents. Egregor is ransomware associated with the cyberattacks against GEFCO and Barnes & Noble, Ubisoft, and numerous others.
The SentinelOne Singularity platform fully protects our customers from this ransomware and related families.
DFIR Analysis Report
Egregor Ransomware
Executive Summary


©2020 SentinelOne, All Rights Reserved
Multiple intelligence and security companies believe that there are ties between past Maze affiliates (now defunct) and Egregor. There have been reports of ties to Sekhmet, ProLock, and LockBit as well (both of which have also been tied to Maze. With regards to Sekhmet, there are deep similarities in the configuration format and obfuscation style. SentinelOne affiliated security researcher Vitali Kremez noted these similarities in an early November tweet.
As is the case with other modern ransomware groups, the actors behind Egregor exfiltrate victim data and theatin to post it publically should the victim fail to comply with their demands.
The primary distribution method for Egregor is Cobalt Strike. Targeted environments are therefore previously compromised through various means (RDP exploit, Phishing) and once the Cobalt Strike beacon payload is established and persistent, it can then be utilized to deliver and launch the Egregor payloads. That being said, Egregor is a RaaS, with multiple affiliates, and delivery/weaponization tactics can therefore vary. There have been limited and uncorroborated reports of Egregor utilizing CVE-2020-0688 (a remote code execution flaw in Microsoft Exchange). They have also been shown to use LOTL (Living off the Land) tools (bitsadmin) to download or update components (DLLs). We have also observed the use of AdFind and Sharphound for additional reconnaissance tasks.
Threat Prominence & Analysis
z

---

Source: https://assets.sentinelone.com/labs/Egregor