# Egregor: Sekhmet's Cousin

By Tomas Meskauskas

Published: 2020-10-29 · Archived: 2026-04-05 21:31:24 UTC

The year 2020 will be remembered none too fondly for several reasons. For much of the world, the global pandemic that resulted in many countries going into lockdowns resulting in massive disruptions to daily life will feature prominently in humankind's shared memory for some time. For the InfoSec community, it will be the unabashed use of the pandemic by hackers to further their goals. Moreso, the community will remember the year ransomware gangs became even more ruthless and began leaking data of those victims who refuse to pay the ransom.

In a year that has already seen several new families cropping up, a new ransomware strain has joined the ranks of those looking to apply increased pressure on victims by leaking sensitive and confidential data.

## Egregor, Occult in Name

The name of the new ransomware strain, Egregor, is derived from Western Occult traditions and is seen as the collective energy of a group of people, especially when aligned to a common goal. The name is appropriate on some level, as ransomware gangs tend to be aligned for the purpose of extorting funds from victims. This is certainly not a purpose for the common good, but nonetheless a purpose is a purpose and, as with practitioners of magic, no rule says they must be good. This rule most certainly applies to those behind Egregor.

Not too much is known about the ransomware and the tactics employed by the gang, as researchers are looking to reverse-engineer samples they have acquired. The first mention of the ransomware on a public forum occurred Sept. 18. Since then, researchers have begun to uncover the ransomware's mysteries. What is currently agreed upon is that Egregor does seem to be closely related to Sekhmet, which, being discovered in March, is older than its cousin by only a couple of months. According to researchers, the similarities between the two variants include similar tactics, obfuscation, API calls and ransom notes, to name a few. Regarding Egregor technical details, researchers noted,

> "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."

The InfoSec community at large must be eagerly awaiting a technical writeup to better defend networks against the threat posed by Egregor. However, this may be delayed—while the ransomware employs the same level of sophisticated code and functionality as many of its rivals, it seems to have an ace in the hole preventing analysis. The ransomware boasts a high number of anti-analysis techniques including code obfuscation and payload

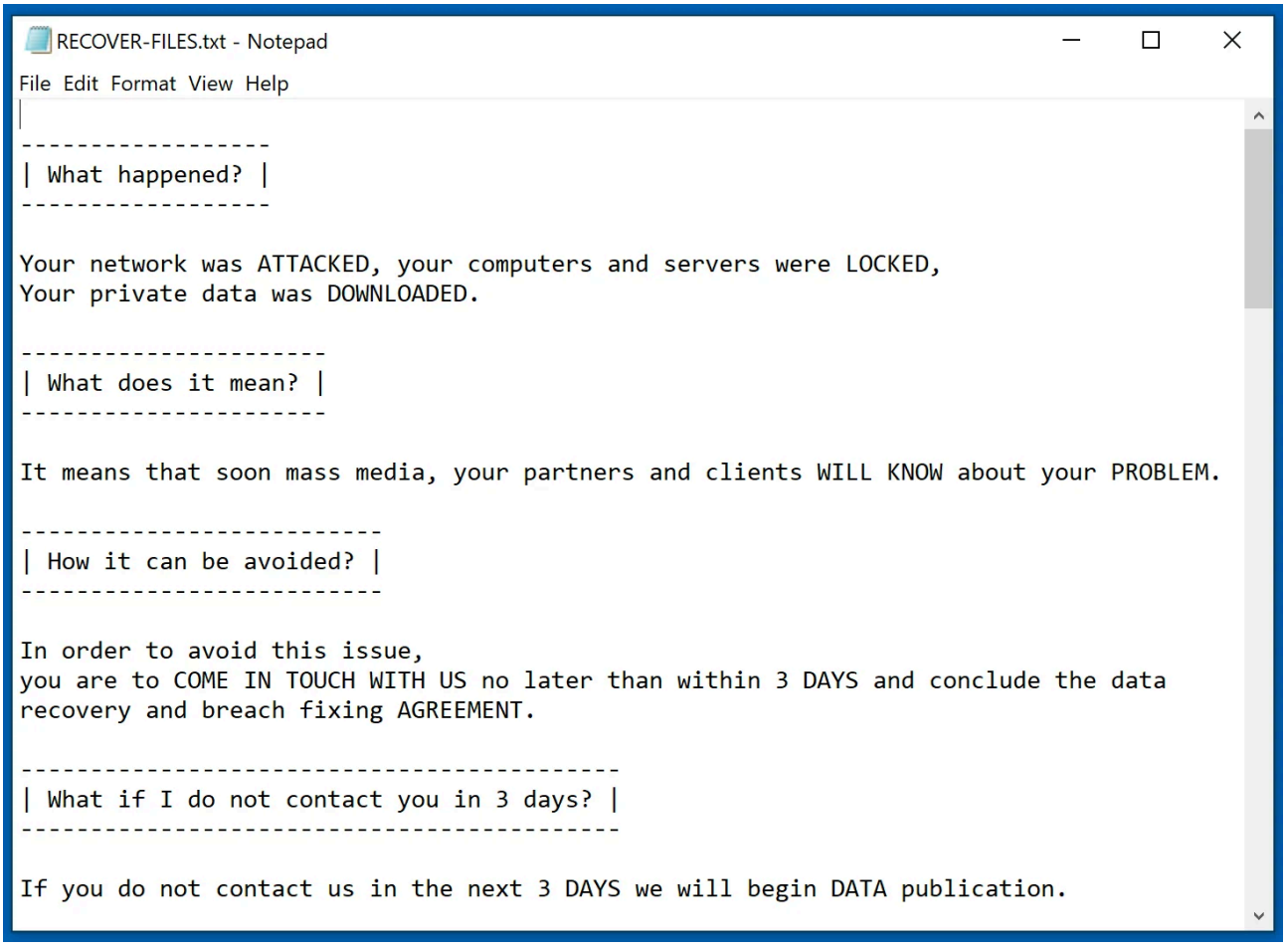
encryption, making the reverse engineering process harder than what researchers wished. What is not shrouded in mystery is the tactic of threatening to release stolen data if ransomware demands are not met within three days.

## Victim Numbers Increasing

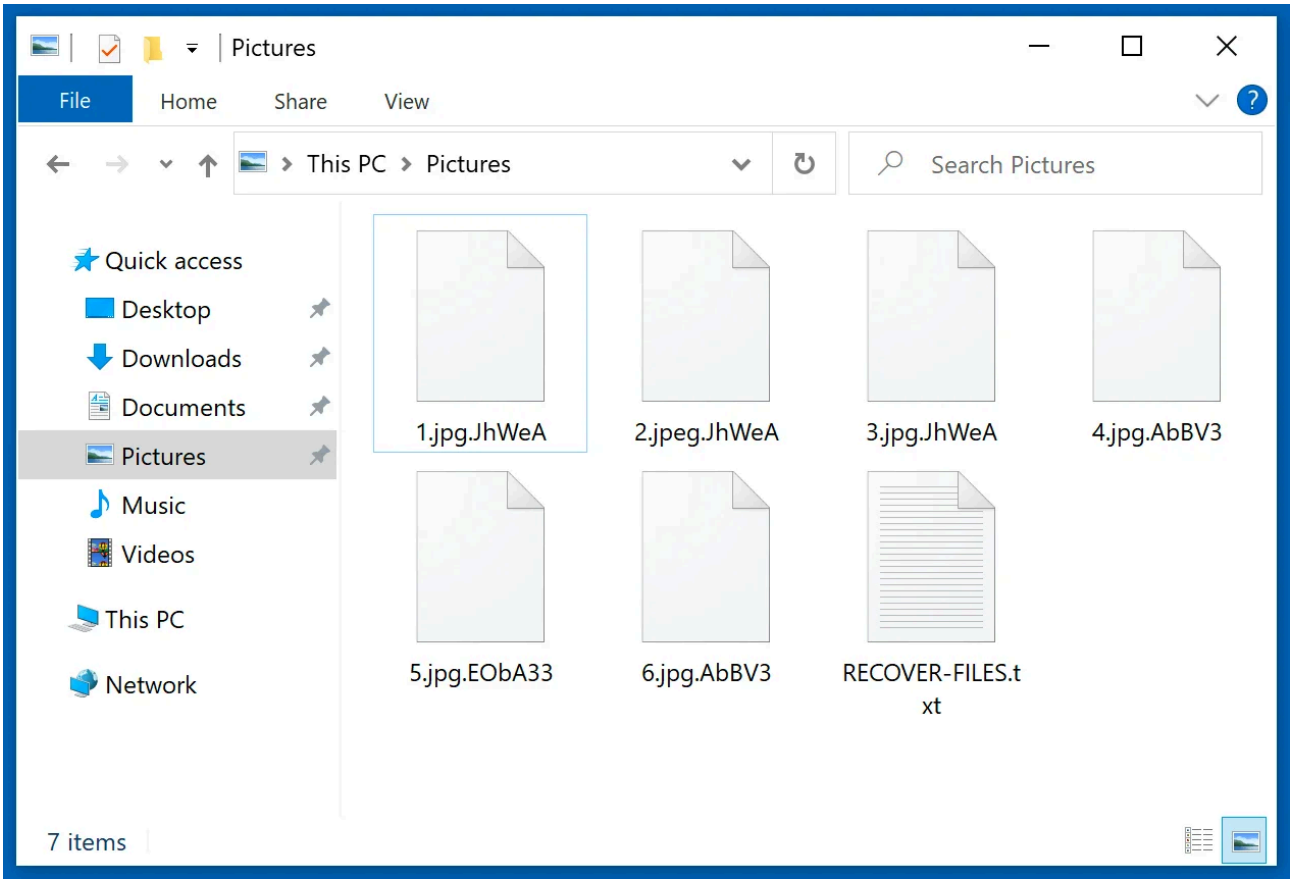
According to the website used by Egregor to announce what data the group has stolen and providing a small amount to prove the data's origin, the gang has amassed 13 victims so far, three of which have managed to make news headlines. It is important to note that two of the three cases still need to be confirmed by the victims that they suffered a ransomware attack; however, there is a sufficient amount of evidence to suggest they have and Egregor may have been the culprit.

The latest of these victims to make headlines was U.S. brick-and-mortar bookstore giant Barnes and Noble. While the InfoSec community is still awaiting confirmation by the affected company, Barnes and Noble did make a statement to the public confirming a cyber incident that may have compromised customer data. That being said, several researchers believe the company may have suffered a ransomware incident—in particular, Egregor. The assumption is based on several things, including how the company networks were affected, resulting in increased periods of downtime preventing customers from accessing certain services.

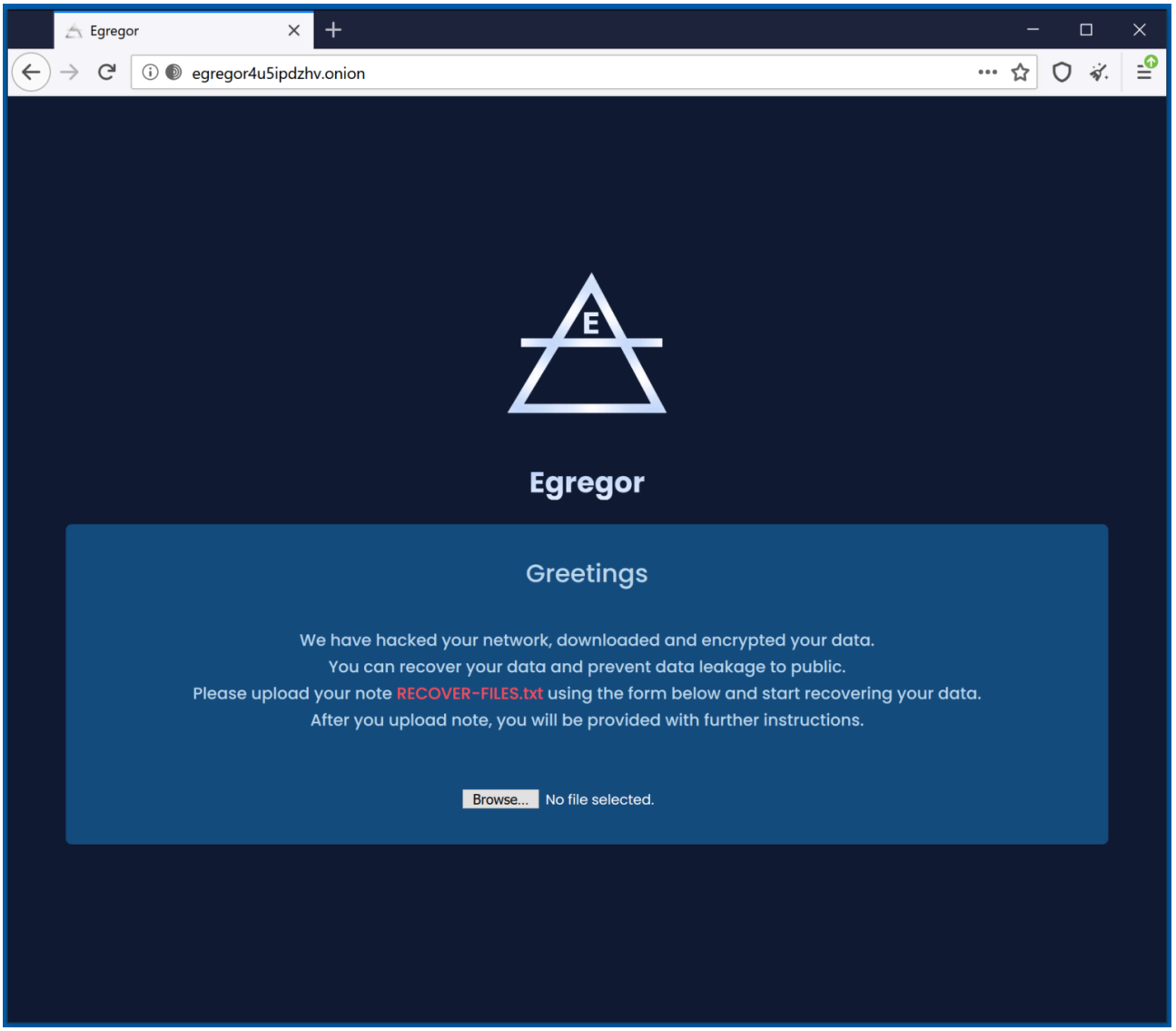
Egregor ransom-demanding message:




Files encrypted by this ransomware:




Tor website of Egregor ransomware:




The most convincing evidence, although rather strange, is the data released by the gang via their leak site. As is often the case, ransomware gangs release data that can be easily traceable to the victim as proof they indeed have done what they said they have. This invariably means the leak of documents; however, the Egregor gang released two Windows Registry hives supposedly taken from Barnes and Noble's servers. The ransomware gang contends that it successfully stole financial data about audits from the company; however, while the leak of the data indicates they in all likelihood may have been behind the attack, the evidence is far from conclusive.

The other two victims to make headlines were games industry giants Crytek and Ubisoft. The former confirmed that it had been hit by a ransomware attack and nearly 400MB of data belonging to the game's developer have been released by the Egregor gang. The data pertained to the company's popular "Warface" first-person shooter and the now-canceled "Arena of Fate MOBA" game as well as some of the company's network operations. The gang also claimed that it stole the source code for Ubisoft's upcoming title "Watchdogs: Legion"; to prove the claim, the gang released 20MB of data it said is in-game assets for the game. The assets themselves don't prove beyond a shadow of a doubt that they belong to Ubisoft and could have been stolen from elsewhere. Ubisoft has not confirmed whether an incident did indeed take place; however, it is believed that Ubisoft employees have suffered from phishing attacks in the past. This, too, is speculation, as the company refuses to respond to questions posed by both journalists and security researchers.

## Egregor's Cousin Sekhmet

Given how little the public knows about Egregor, it is wise to look at its cousin Sekhmet. The name given to the ransomware is from Ancient Egyptian mythology, which says Sekhmet was the warrior goddess of healing. Ancient Egyptian mythology has strong links to many Western occult traditions, so at the very least the gang behind both appears to have a naming convention in place. Sekhmet is older by a few months, but both share tactics such as leaking data from victims via a dedicated website. Unfortunately, as with Egregor, technical details about the ransomware strain are thin. At the time of writing, no information is available regarding how the malware is distributed, the infection chain or attack vectors. Researchers believe that Sekhmet may be dropped by other malware or downloaded via malicious websites, but little else about the ransomware is public knowledge.

In June, news emerged that two companies had suffered a Sekhmet infection. The first, IT firm Excis, was announced at the end of May by those operating the ransomware, who subsequently released data supposedly belonging to the IT firm on its leak site called "leaks, leaks, leaks." The operators released the data in response to the company director saying that no important data was stolen. The second victim, SilPac, a gas handling solutions company based in Santa Clara, California, appeared to have been affected later in June; the gang attacked the company twice in short succession. Again, the attacks were announced via Sekhmet's leak site. It is believed that the attackers managed to retain a presence on the victim's network even after encryption occurred.

## The Age of the Leak Site

Many high-profile ransomware gangs that seemingly only target large corporate networks operate leak sites. The list seems to grow unabated from month to month. The flood of bad news can leave individuals feeling helpless but, importantly, these attacks are preventable. In recent months ransomware operators have targeted known vulnerabilities with VPN servers, and although these attacks have been well-publicized, some corporate networks are still vulnerable. Gaining access to a corporate network is now a big business, as "initial access brokers" look to sell access to networks they have compromised. Ransomware operators are potential clients, with some even looking to bring in talent as affiliates who can compromise networks and then drop the ransomware payload.

Given the high number of high-profile victims that have emerged this year alone, this trend of new ransomware strains creating leak sites is expected to continue for some time. Although these attacks are preventable, some security researchers are suggesting that ransom payments be made illegal to try and curb the current threat posed by ransomware. The hope is that such laws would dissuade payments and dry up the profits generated by ransomware gangs. The call to make ransom payments may be extreme and seen as punishing the victim of the crime rather than the perpetrator, but measures to prevent these attacks seem to be failing.

Recent Articles By Author

---