Egregor Ransomware Launches String of High-Profile Attacks to End 2020

By By: Trend Micro Research Dec 14, 2020 Read time: 3 min (870 words)

Published: 2020-12-14 · Archived: 2026-04-05 12:41:19 UTC

In late 2020, the operators behind Maze ransomware, one of the more notorious ransomware families in recent memory, announced that they were shutting down operationsnews article. However, in just a short period after Maze's retirement, the ransomware known as Egregor has stepped in to fill the void, allegedly becoming the ransomware of choice for previous Maze affiliates. Like Maze, Egregor makes use of a "double extortion" technique where the ransomware operators threaten the victim not only with the loss of their data, but with a warning that their data will go public if they fail to pay the ransom.

What is Egregor?

A sophisticated piece of ransomware that first surfaced around September 2020, Egregor has since been involved in a number of high-profile attacks in a short period, including attacks that were launched against major retailers and other organizations.

This ransomware is often distributed as a payload along with remote access trojans (RATs) such as QAKBOT. In turn, QAKBOT has been previously observed to be connected with the MegaCortex and ProLock ransomware families, which indicates either a possible partnership between QAKBOT and Egregor or a new payload from the QAKBOT threat actors.

Similar to the double extortion technique used by the new breed of ransomware families such as Ryuk, Egregor pressures the victim to pay by threatening to release stolen information. In addition to encrypting data, operators behind Egregor also make threats about informing mass media — and hence, the public — that the company has been compromised.

On the surface, Egregor seems like a copy of the Sekhmet ransomware, as it shares most of its codes and routines, most notable of which are its obfuscation techniques, functions, as well as API calls and strings. Furthermore, like Sekhmet, it also appends a random extension per file. However, it is possible that Egregor and Sekhmet are operated by entirely different groups given the differences between the data leak sites that are used by the two.

Although there is no concrete information on how exactly Egregor gains initial access, it is likely that it uses techniques that are similar with other targeted ransomware such as RDP hacks, compromised websites, or stolen accounts.

One of Egregor's defining characteristics is its use of advanced obfuscation techniques, wherein it requires a specific argument to decrypt the payload, thereby making it difficult to perform static or dynamic analysis on the ransomware variant without this argument.

According to the Egregor ransom note, victims that manage to pay the ransom will not only have their data decrypted. In fact, the threat actors also offer to provide recommendations for securing the company's network.

A simplified version of its attack chain can be found in the following figure:

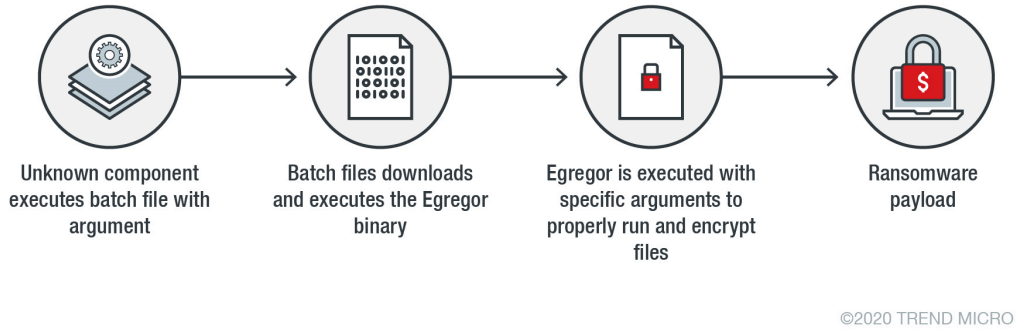

Figure 2. Egregor attack chain

From our Trend Micro™ Smart Protection Network ™ data, Egregor has been active primarily in the US, with Japan and the UK also seeing a number of infections.

What are the recent incidents involving Egregor?

A number of Egregor's attacks have occurred against high profile targets, including a leading bookstore in October and a major retailer in December. In the former, the ransomware operators behind Egregor claimed to have gathered unencrypted financial and auditing data, although the precise nature of the data that was stolen is unclear.

Egregor has also been observed printing ransom notesopen on a new tab. Based on our analysis, printing ransom notes was not intentional on the operators' end. Rather, it occurred as part of the ransomware's encryption routine, which enumerates any type of network resources — including printer resources. It then connects to the network resource to encrypt files and drop the ransom note. It's also possible that the printers and point-of-sale (POS) machines were connected to the infected machines, which resulted in the ransom notes being physically printed.

Other recent victims of Egregor include major organizations in both the gaming and human resources industries.

How can the impact of Egregor and other ransomware be minimized?

Although there is still no concrete evidence on how Egregor gains initial access to the system, other ransomware variants such as Maze are known to exploit vulnerabilities as part of their routine. Therefore, it is important for organizations to patch and update their systems' software to address any exploitable vulnerabilities. Additionally, businesses are encouraged to keep their machines and their systems updated to prevent this from happening.

Businesses should also perform regular security audits of their systems to ensure that they are as secure as possible. Company data should also be periodically backed up whenever possible, preferably by adhering to the 3-2-1 rulenews article, which involves keeping three copies in two different formats with at least one copy off-site.

Meanwhile, employees should be given proper training on the best practices for cybersecurity, especially when it comes to the common initial access techniques used by ransomware, such as email-based attacksnews-cybercrime-and-digital-threats and compromised websites.

For a more robust and proactive line of defense against ransomware, we recommend the following Trend Micro solutions:

- Trend Micro Smart Protection Suitesproducts applies AI and analytics for earlier detection of threats across endpoints and other layers of the system.
- Trend Micro™ Deep Discovery™ Inspectorproducts detects, blocks, and analyzes malicious email attachments through custom sandboxing and other detection techniques.
