# Egregor ransomware group explained: And how to defend against it

By by Cynthia Brumfield Contributing Writer

Published: 2021-02-19 · Archived: 2026-04-05 20:16:57 UTC

## Newly emerged Egregor group employs "double ransom" techniques to threaten reputational damage and increase pressure to pay.

## What is Egregor?

Egregor is one of the most rapidly growing ransomware families. Its name comes from the occult world and is defined as “the collective energy of a group of people, especially when aligned with a common goal,” according to Recorded Future’s Insikt Group. Although descriptions of the malware vary from security firm to security firm, the consensus is that Egregor is a variant of the Sekhmet ransomware family.

It arose in September 2020, at the same time the Maze ransomware gang announced its intention to shut down operations. Affiliates who were part of the Maze group appear, however, to have moved on to Egregor without skipping a beat.

Insikt and Palo Alto Networks’ Unit 42 think Egregor is associated with commodity malware such as Qakbot, which became prominent in 2007 and uses a sophisticated, evasive worm to steal financial credentials, as well as other off-the-shelf malware such as IcedID and Ursnif. These pieces of malware help attackers gain initial access to victims’ systems.

All security researchers seem to agree with Cybereason’s Nocturnus Team that Egregor is a rapidly emerging, high-severity threat. According to security firm Digital Shadows, Egregor has claimed at least 71 victims across 19 different industries worldwide.

*Update:* On February 9, a joint operation by US, Ukrainian, and French authorities resulted in the arrest of gang members behind Egregor as well as associates who were part of their affiliate program. The leader of the Egregor group was reportedly among those arrested. The group’s website was also taken offline. It is too early to know whether this action has taken Egregor down permanently.

## Egregor’s double extortion undercuts traditional defenses

Like most current ransomware variants used in the wild, Egregor uses “double extortion,” relying on a “Hall of Shame” or publicly accessible stolen data on leak pages to pressure victims into paying the ransom. Among the high-profile Egregor victims are Kmart, the Vancouver metro system, Barnes and Noble, video game developers Ubisoft and Crytek, and the Dutch human resources firm Randstad, from which the attackers stole data, a portion of which they published to the web.

Like many internet criminals, Egregor attackers have considered healthcare facilities and hospitals to be fair game during the coronavirus crisis. One health care provider that had to reduce some functions due to an Egregor ransomware attack is GBMC Healthcare in Maryland, which got hit in early December, 2020. The company said it had robust protections in place but nonetheless was forced to postpone some elective procedures.

The double extortion, or double ransom, characterizes this new breed of ransomware, undercutting the previous defense that most companies could deploy, which is to keep robust backups if attackers encrypted files. Egregor "just emerged really a couple of months ago and especially in September where it really started hitting all over the world, basically around the same time just when Maze ransomware operators" supposedly shut down, Jen Miller-Osborn, deputy director of threat intelligence for Unit 42 at Palo Alto Networks, tells CSO.

"If you have good offline backups and you know they work, if you're hit by ransomware, it's not that big of an issue," she says. "You take a hit for business purposes and downtime potentially, but if you have good backups, you've already kind of built that into your recovery plan."

Now groups like Egregor have "gotten wise to that idea. So, they're saying, 'Well, we've already stolen your data, so you have to pay us for that. Or we're just going to release it publicly and potentially ruin your business, or at least damage your business's reputation.' That takes away the good backup story that has worked for so long," Miller-Osborn says. "We saw that with Maze, and we're continuing to see that with Egregor."

As was true with Maze, Egregor is being sold as a ransomware-as-a-service (RaaS), with the gang selling it or renting it to other people to use maliciously. Some of the same affiliates of Maze have shifted over to Egregor, "so it seems that will be the next big thing post-Maze until someone else gets wise and comes up with a more creative variant," Miller-Osborn says.

## How to defend against Egregor

When it comes to protecting against the double ransom component of Egregor, stronger protections can help, Miller-Osborn says. "Ransomware typically is not particularly complicated. It's not super-stealthy malware in most cases."

A lot of ransomware infections come from phishing. "It remains hands-down the most common infection vector," so better protections and training around phishing could help. "Be careful about opening those emails; be careful about clicking on those links. It's the same kind of thing we say constantly, but that's the simplest thing you can do to avoid a ransomware attack."

"Internally there are some things companies can do in keeping their most sensitive data in enclaves," Miller-Osborn said, "basically not having a flat network and recognizing what the most sensitive or potentially catastrophic loss data is." For the most sensitive data, organizations should consider having an extra sensor, with extra monitored higher-level security controls than you might have for other parts of the network, she recommends. "Obviously, all of that costs money and is non-trivial."

Any organization's highly sensitive data will also likely be the target of corporate or state-sponsored espionage threats, so investing in the protection of those kinds of records is just overall a good idea. "The same kind of sensitive data that the ransomware actors are potentially going after and exfiltrating can also be the same kind of

data that an espionage motivated threat would be interested in," says Miller-Osborn. "So just having that data better protected and harder to access is good."

With training and increased network protection, it is possible to stop and block ransomware, Miller-Osborn says. "It just involves having the right security components configured properly and in the right places. It's a security posture design thing."

In terms of Egregor's connection to the Maze group, "We don't have a definitive smoking gun, but a lot of little things lead us to believe it's the same people," Miller-Osborn says. It's not uncommon to see this with commodity malware, where a group will claim to shut down only to pop up later as a rebranded version, and it's the same person or people. "It looks like they do that because there is too much attention on them. There's too much press. There's too much law enforcement looking for them," she says. "All they're trying to do is just separate themselves from that previous family, for whatever reason."

Unfortunately, this new era of highly damaging ransomware typified by the Egregor malware's rise won't end anytime soon. "This is just going to continue. I think we're going to see more actors, especially on the criminal side of the house, starting to take advantage of this. They recognize how much money they can potentially make doing it."

*Editor's note: This article, originally published in January 2021, has been updated to include information on the take-down of the Egregor group.*

---