Ransomware Profile: Egregor

By Emsisoft Malware Lab

Published: 2021-02-15 · Archived: 2026-04-05 14:37:36 UTC

Egregor is an aggressive strain of ransomware that targets large organizations. It has been extremely active since its discovery in September 2020, claiming hundreds of victims across multiple industries.

The above chart shows the number of Egregor samples submitted to ID Ransomware, an online tool that allows users to identify which ransomware strain has encrypted their files and provides a free decryptor should one be available.

The submission data shows that Egregor claimed a large number of victims in a very short space of time and possibly amassed victims quicker than any other group. This surge of attacks was likely the result of former Maze affiliates bringing lists of already-compromised networks to the Egregor affiliate program.

Within a month, however, a significant drop in the rate of the attacks occurred. This decrease was likely due to the affiliates who crossed over from Maze quickly exhausting their lists of already-comprised networks and effectively running out of easy prospective targets.

What is Egregor?

Egregor is a sophisticated strain of ransomware that encrypts files using ChaCha and RSA encryption and uses advanced obfuscation techniques to thwart analysis efforts. “Egregor” is derived from the ancient Greek term for “wakeful,” an occult concept referring to the collective energy of a group of people working toward a common goal – an appropriate name for a ransomware group.

Like many other modern ransomware groups, Egregor’s operators exfiltrate data from victims and store it on their servers before the data is encrypted on the target’s machine. Egregor demands a swift response, giving victims just 72 hours to make contact with attackers.

In the event of non-payment, the stolen data is published on the attacker’s website, Egregor News, which can be accessed on both the clear web and dark web. One of the last known banner messages on the Egregor News website was the Christmas greeting: “Egregor Team wishes all clients happy holidays. Christmas gifts are waiting for you. Details in your personal chat!”

Egregor operates under the ransomware-as-a-service model, whereby affiliates receive a portion of ransom payments in exchange for dropping the malware onto victims’ networks. Egregor affiliates earn 70 percent of the ransom payments they generate, with the remaining 30 percent going to the Egregor group. It is believed that the Egregor affiliate program attracted many ex-Maze affiliates following the sudden retirement of the Maze ransomware gang in November 2020.

The Egregor-Sekhmet-Maze connection

Egregor, Sekhmet and Maze share almost exactly the same base code. Sekhmet, a now inactive strain of ransomware that was first detected in March 2020, is identical to Maze apart from one small tweak to the way it uses file markers. Egregor, in turn, is identical to Sekhmet, except for having a different file marker value and ransom note text.

While it's not clear if the creators of Sekhmet and/or Maze are responsible for Egregor, the three variants clearly share significant similarities. The Sekhmet leak platform – which exposed just six victims in total – went offline at around the same as the launch of the Egregor News site.

The History of Egregor

Egregor was first observed in September 2020. It was an extremely active threat from the outset, claiming more than 130 victims in the first 10 weeks, including high-value targets in the industrial goods, retail and transportation sectors.

Suspected Egregor operators arrested

In February 2021, alleged Egregor operators were arrested in Ukraine following a joint investigation by French and Ukrainian police, which was coordinated by Europol. Investigators were able to track down the unnamed suspects by following the flow of bitcoins being handled by the alleged operators. According to France Inter, the arrested suspects provided hacking, logistical and financial support for the Egregor group. On February 17, 2021, the Ukrainian Security Service confirmed an undisclosed number of arrests in connection with the Egregor operation.

The group's extortion site went offline around the time of the arrests, making it impossible for victims to pay a ransom or contact the ransomware group. It's worth noting that the Egregor extortion site had been going offline intermittently for some time prior to the arrests, so it's possible that the disruption is unrelated.

Egregor ransom note

After encrypting the target system, Egregor drops a ransom note titled "RECOVER-FILES.txt" in all infected directories. The ransom note is fairly vague and contains no specific payment instructions. Instead, it instructs victims to install the TOR browser, navigate to the operators' website and open a live chat with the threat actors, who will then provide further instructions. The note states that stolen data will be published if no contact is made within three days.

The note claims that after receiving payment attackers will provide full decryption of all affected machines, a file listing of downloaded data, confirmation of the deletion of exfiltrated data and complete confidentiality. Audaciously, the note also states that operators will provide paying victims with recommendations for securing their networks to prevent future breaches.

Egregor is the only ransomware family known to print ransom notes via available printers on compromised networks.

Who does Egregor target?

Egregor targets large organizations. While the industrial goods and services sector was initially most heavily hit, enterprises across a wide range of verticals have since been impacted by Egregor.

Egregor primarily targets U.S.-based organizations, although a number of companies in South America, Africa, Asia, Europe and Oceania have also been infected.

Before encrypting data on a compromised machine, Egregor checks the Default Language ID of the system and user account. The ransomware does not execute if any of the following languages are detected: Uzbek, Romanian, Azerbaijani, Turkmen, Georgian, Kyrgyz, Ukrainian, Kazakh, Tatar, Russian, Tajik, Armenian, Belarusian, Romanian.

How does Egregor spread?

The information currently available suggests that the infection chain typically starts with a phishing email, which contains a malicious macro embedded in an attached document.

Upon execution, the macro downloads commodity malware such as Qakbot, IcedID and/or Ursnif, which are used to gain an initial toehold in the target environment. The operators of QakBot, a banking Trojan that is commonly used to drop malware onto infected networks, recently switched from dropping ProLock, another prominent ransomware strain, to dropping Egregor.

Later in the attack chain, operators use Cobalt Strike to gather information, escalate privileges, move laterally across the network and prepare the system for encryption. To exfiltrate data, operators typically use Rclone, an open-source command line program used to manage cloud storage. There have also been instances of operators using Cobalt Strike to create an RDP connection with other endpoints on the network and copying Egregor to them.

It is important to note that because Egregor is a ransomware-as-a-service operated by multiple affiliates, infection methods can vary. We have heard rumors of Egregor utilizing flaws in Microsoft Exchange, VBScript Engine and Adobe Flash Player, but these reports are still unsubstantiated.

Major Egregor attacks

Ubisoft

In October 2020, Egregor captured the attention of the cybersecurity industry with a high-profile attack on video game developer Ubisoft. Threat actors initially released a few hundred megabytes of data relating to in-game assets, before later releasing 560GB of source code from Ubisoft’s latest action-adventure game Watch Dogs: Legion.

Barnes & Noble

In October 2020, Barnes & Noble was hit with Egregor. The incident forced the U.S. bookstore giant to shut down their network to stop the attack from spreading, resulting in Nook users being unable to access their eBook libraries. Threat actors claimed to have stolen financial and audit data during the attack, while email addresses, billing addresses, shipping addresses and purchase history were also exposed on the compromised systems.

TransLink

In December 2020, Metro Vancouver transport agency TransLink faced significant disruption after falling victim to Egregor. The attack impacted phones, online services and payment systems, leaving commuters unable to pay for fares with credit cards or debit cards. During the incident, ransom notes were printed from TransLink printers as well as dropped digitally in infected directories.

Randstad

In December 2020, Randstad, one of the largest recruitment agencies in the world, announced that their network had been breached by Egregor. Operators published a 32.7 MB archive of exfiltrated data, which they claimed was just 1 percent of the total data stolen during the attack. The leaked data contained a range of business documents, including financial reports, legal documents and accounting spreadsheets.

How to protect the network from Egregor and other ransomware

The following practices may help organizations reduce the risk of an Egregor incident.

- **Cybersecurity awareness training**: Because the majority of ransomware spreads through user-initiated actions, organizations should implement training initiatives that focus on teaching end users the fundamentals of cybersecurity. Ransomware and propagation methods are constantly evolving, so training must be an ongoing process to ensure end users are across current threats.
- **Credential hygiene**: Practicing good credential hygiene can help prevent brute force attacks, mitigate the effects of credential theft and reduce the risk of unauthorized network access.
- **Multi-factor authentication**: MFA provides an extra layer of security that can help prevent unauthorized access to accounts, tools, systems and data repositories. Organizations should consider enabling MFA wherever possible.
- **Security patches**: Organizations of all sizes should have a robust patch management strategy that ensures security updates on all endpoints, servers, and appliances are applied as soon as possible to minimize the window of opportunity for an attack.
- **Backups**: Backups are one of the most effective ways of mitigating the effects of a ransomware incident. Many strains of ransomware can spread laterally across the network and encrypt locally stored backups, so organizations should use a mixture of media storage, and store backup copies both on- and off-site. See this guide for more information on creating ransomware-proof backups.
- **System hardening**: Hardening networks, servers, operating systems and applications is crucial for reducing the attack surface and managing potential security vulnerabilities. Disabling unneeded and potentially exploitable services such as PowerShell, RDP, Windows Script Host, Microsoft Office macros, etc. reduces the risk of initial infection, while implementing the principle of least privilege can help prevent lateral movement.
- **Block macros**: Many ransomware families are delivered via macro-embedded Microsoft Office or PDF documents. Organizations should review their use of macros, consider blocking all macros from the Internet, and only allow vetted and approved macros to execute from trusted locations.
- **Email authentication**: Organizations can use a variety of email authentication techniques such as Sender Policy Framework, DomainKeys Identified Mail, and Domain-Based Message Authentication, Reporting

and Conformance to detect email spoofing and identify suspicious messages.

- **Network segregation**: Effective network segregation helps contain incidents, prevents the spread of malware and reduces disruption to the wider business.
- **Network monitoring**: Organizations of all sizes must have systems in place to monitor possible data exfiltration channels and respond immediately to suspicious activity.
- **Penetration testing**: Penetration testing can be useful for revealing vulnerabilities in IT infrastructure and employees' susceptibility to ransomware. Results of the test can be used to allocate IT resources and inform future cybersecurity decisions.
- **Incident response plan**: Organizations should have a comprehensive incident response plan in place that details exactly what to do in the event of infection. A swift response can help prevent malware from spreading, minimize disruption and ensure the incident is remediated as efficiently as possible.

How to remove Egregor and other ransomware

Egregor uses sophisticated encryption methods that currently make it impossible to decrypt data without paying for an attacker-supplied decryption tool.

Victims of Egregor should be prepared to restore their systems from backups, using processes that should be defined in the organization's incident response plan. The following actions are recommended:

- Take action to contain the threat.
- Determine the extent of the infection.
- Identify the source of the infection.
- Collect evidence.
- Restore the system from backups.
- Ensure all devices on the network are clean.
- Perform a comprehensive forensic analysis to determine the attack vector, the scope of the incident and the extent of data exfiltration.
- Identify and strengthen vulnerabilities to reduce the risk of a repeat incident.
