


# Appgate Labs Analyzes New Family of Ransomware— “Egregor”

---

 [appgate.com/news-press/appgate-labs-analyzes-new-family-of-ransomware-egregor](https://appgate.com/news-press/appgate-labs-analyzes-new-family-of-ransomware-egregor)

appgate



Appgate SDP

SDP Overview

Learn how Appgate SDP reduces risk and complexity, and why it's the industry's most comprehensive Zero Trust network access solution.



## How Appgate SDP Works

Find out about the inner-workings of the most flexible and adaptable Zero Trust Network Access solution available today.



## SDP Integrations

Explore security, IT and business-system integrations that can enhance and help you adapt Appgate SDP to your existing workflows



## SDP for Developers

Access developer tools and resources to maximize the value of your Appgate SDP deployment.

Zero Trust Network Access for:

[Secure Remote Access](#) [Secure Hybrid Enterprise](#) [Zero Trust for Cloud](#) [Third-Party Access](#)  
[Secure DevOps Access](#)

## Risk-Based Authentication



### Overview

Learn how Risk-Based Authentication provides a frictionless, intelligent and data-informed approach to user authentication.



### Strong Authentication

Find out how you can provide secure, frictionless access with the right multi-factor authentication method.

### Transaction Monitoring

Explore the tools you can use to intelligently identify and prevent online fraud.

### Behavioral Biometrics Service

Learn how behavioral analysis and machine learning stop fraudulent online web activity in real-time.

## Digital Threat Protection

### Overview

Discover how you can gain unparalleled threat visibility and the risk management tools that enable early identification and elimination of potential attacks.



### Key Features

Take a deep dive into the features and tools contained within our industry-leading Digital Threat Protection (DTP) solution.

#### [News & Press](#)

**MIAMI, FL –October 2, 2020** – This week our team analyzed a new family of ransomware that calls itself "Egregor", which seems to be a Sekhmet ransomware spin-off.

The threat group behind this malware seems to operate by hacking into companies, stealing sensitive data, and then running Egregor to encrypt all the files. According to the ransom note, if the ransom is not paid by the company within 3 days, and aside from leaking part of the stolen data, they will distribute via mass media where the company's partners and clients will know that the company was attacked.

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.

At the time of this advisory, there is at least 13 different companies listed in their "hall of shame", including the global logistic company GEFCO, which suffered a cyber attack last week. Egregors' ransom note also says that aside from decrypting all the files in the event the company pays the ransom, they will also provide recommendations for securing the company's network, "helping" them to avoid being breached again, acting as some sort of black hat pentest team.

### **About Appgate**

Appgate is the secure access company that provides cybersecurity solutions for people, devices and systems based on the principles of Zero Trust security. Appgate updates IT systems to combat the cyber threats of today and tomorrow. Through a set of differentiated cloud and hybrid security products, Appgate enables enterprises to easily and effectively shield against cyber threats. Appgate protects more than 1,000 organizations across government and business. Learn more at [appgate.com](https://www.appgate.com).

### **Press Contact:**

Robert Nachbar

ZAG Communications

206-427-0389

[rob@zagcommunications.com](mailto:rob@zagcommunications.com)