Objet: 🇬🇧 The Egregor Ransomware

cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/

S.G.D.S.N

Agence nationale
de la sécurité des
systèmes d'information

Paris, le 02 mars 2021

N° CERTFR-2021-CTI-007

Affaire suivie par: CERT-FR

le 02 mars 2021

Rapport Menaces et Incidents du CERT-FR

Gestion du document

Référence	CERTFR-2021-CTI-007
Titre	🇬🇧 The Egregor Ransomware
Date de la première version	02 mars 2021
Date de la dernière version	03 mars 2021
Source(s)	
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

French version: 🇫🇷

Active since September 2020, the Egregor ransomware is currently being used in Big Game Hunting operations. Part of the Sekhmet malware family, Egregor is sometimes considered the successor to Maze. It is made available to various affiliates, explaining the different chains of infection reported. Trojans such as Qakbot, Ursnif and IcedID, can be used to deliver Egregor.

This report provides a synthesis of ANSSI's knowledge on this malware.

Indicators of compromise are available on the page CERTFR-2020-IOC-006.

DOWNLOAD THE REPORT

Gestion détaillée du document

le 02 mars 2021
-

le 02 mars 2021
Version initiale

le 03 mars 2021
-