

Objet: Identification of a new cybercriminal group : Lockean

 cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

S.G.D.S.N

Agence nationale
de la sécurité des
systèmes d'information

Paris, le 03 novembre 2021

N° CERTFR-2021-CTI-009

Affaire suivie par: CERT-FR

le 03 novembre 2021

Rapport Menaces et Incidents du CERT-FR

Gestion du document


Référence	CERTFR-2021-CTI-009
Titre	 Identification of a new cybercriminal group : Lockean
Date de la première version	03 novembre 2021
Date de la dernière version	03 novembre 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.

Version française :

Based on incidents reported to the ANSSI and their commonalities, investigations were carried out by the Agency to confirm the existence of a single cyber criminal group responsible for these incidents, understand its modus operandi and distinguish its techniques, tactics and procedures (TTPs). First observed in June 2020, this group named Lockean is thought to have affiliated with several Ransomware-as-a-Service (RaaS) including DoppelPaymer, Maze, Prolock, Egregor and Sodinokibi. Lockean has a propensity to target French entities under a Big Game Hunting rationale.

Indicators of compromise are available in structured formats on the page [CERTFR-2021-IOC-004](#).

[DOWNLOAD THE REPORT](#)

Gestion détaillée du document

le 03 novembre 2021

Correction de la conjonction de coordination "ET" par son homologue anglais "AND"

le 03 novembre 2021

Version initiale