



CYBER ATTAQUE **MAIRIE DE SAINT-CLOUD**

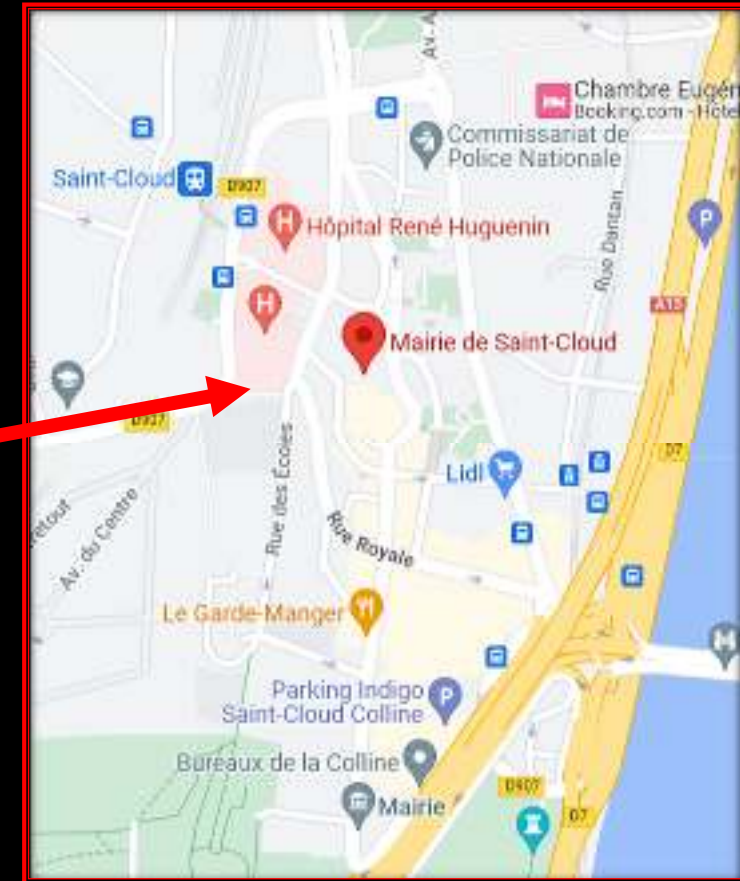


QUI ?



→ ***LES SYSTÈMES
INFORMATIQUES DE LA
MAIRIE DE SAINT-CLOUD***

où ?



À SAINT-CLOUD DANS LES HAUTS-DE-SEINE (92)

QUAND ?

DANS LA NUIT DU 20 AU 21 JANVIER

2022



PAR QUI ?

L'ATTAQUE A ÉTÉ REVENDIQUÉE PAR LE GROUPE DE HACKERS LOCKBIT 2.0

LOCKBIT 2.0 : GROUPE QUI TIRE SON NOM DU RANSOMWARE DU MÊME NOM, IL MARCHE EN TANT QUE SERVICE, IL PROPOSE DE LOUER UNE ATTAQUE PERSONNALISÉE, À L'HEURE ACTUELLE LE GROUPE REVENDIQUE PLUS DE 400 ATTAQUES.

POURQUOI ?

**COMME SOUVENT ÉCHANGER DES DONNÉES
CONTRE UNE RANÇON (RANSOMWARE) SINON LES
DONNÉES CONFIDENTIELLES SERONT DIVULGUÉES.**

ILS AVAIENT JUSQU'AU 10 FÉVRIER...



COMMENT ?

**IL SEMBLERAIT QUE CE SOIT PAR PHISHING
MAIS CE N'EST PAS COMPLÈTEMENT SÛR**

**PHISHING = SE FAIRE PASSER POUR UN TIERS
DE CONFIANCE (BANQUE, IMPOTS...)**

CONSÉQUENCES

DIFFUSION DE DOCUMENTS INTERNES À LA VILLE SUR LE DARKWEB :

- INFORMATIONS RELATIVES À LA GESTION DE LA CRISE SANITAIRE**
- INFORMATIONS LIÉES À L'ACTIVITÉ DE LA POLICE MUNICIPALE**
- COORDONNÉES DE 391 PERSONNES**

**SERVICES DE LA MAIRIE PERTURBÉS : ACCÈS LIMITÉ À INTERNET,
PAS D'IMPRIMANTES, SCANNERS...**

RÉACTIONS/SOLUTIONS

LA MAIRIE S'EST ENTOURÉE D'EXPERTS AFIN DE TRAITER L'INCIDENT, UNE PLAINTÉ A ÉTÉ DÉPOSÉE AUPRÈS DE L'ANSSI ET UNE ENQUÊTE JUDICIAIRE A ÉTÉ OUVERTE PAR LE PARQUET DE PARIS.

SOURCES

<https://www.saintcloud.fr/actualite/la-mairie-de-saint-cloud-victime-dune-cyberattaque-0>

<https://lagazette-ladefense.fr/2022/02/16/cyberattaque-les-hackers-diffusent-des-documents-internes-apres-le-refus-de-la-mairie-de-payer-la-rancon/>

<https://www.futura-sciences.com/tech/actualites/cybersecurite-lockbit-20-groupe-hackers-revendique-attaque-ministere-justice-96429/>