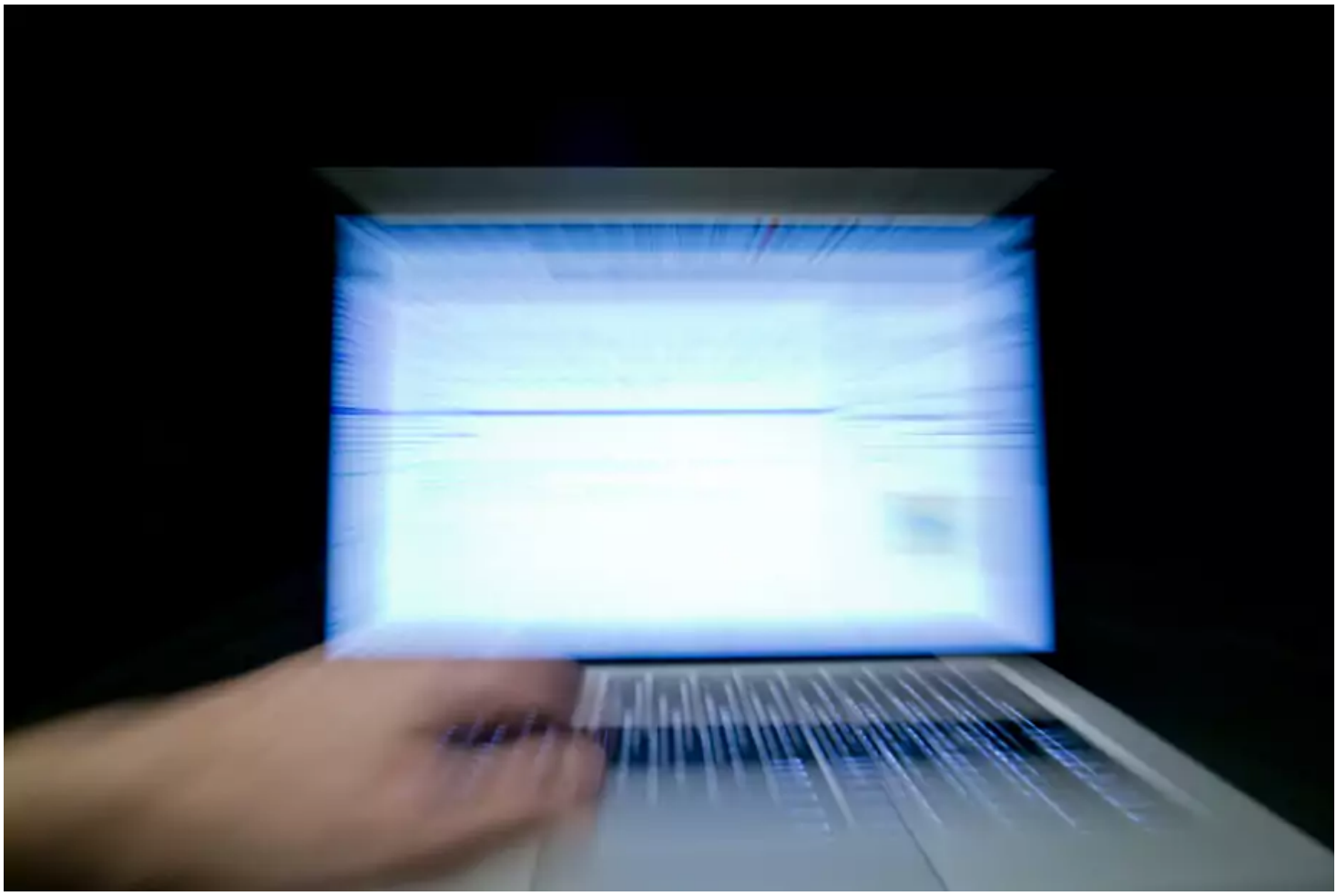
Des pirates s’attaquent à des infrastructures souterraines critiques de Montréal

Hugo Joncas ⁝



Des cyberpirates se sont attaqués à des infrastructures critiques : les conduites d’électricité et de télécommunication souterraines de Montréal.
L’organisme public chargé du réseau a refusé une demande de rançon de deux millions de dollars américains.

L’attaque informatique du gang LockBit a eu lieu le 3 août, précise la Commission des services électriques de Montréal (CSEM), dans un communiqué transmis à *La Presse*.

« En toute responsabilité et de concert avec le conseil d’administration de la CSEM, notre décision fut de refuser la rançon initiale de deux millions de dollars américains.
Ceci, considérant le caractère public et la mission de la CSEM, en termes de gouvernance et de saine gestion des deniers publics », explique le président de la Commission, Sid Zerbo, dans un courriel.

En plus du président nommé par Québec, le CA de la CSEM inclut deux représentants de la Ville de Montréal, un représentant d’Hydro-Québec et un représentant des compagnies de télécommunications.
L’organisation est responsable du réseau de 770 kilomètres de conduites par lesquelles passent les fils électriques, de téléphone et de câble.

Les premiers impacts se sont fait sentir dès le lendemain [de l’attaque] avec des pannes impactant notre fonctionnement.

la CSEM dans son communiqué

Certains services qu'elle livre à ses partenaires connaissent toujours « des impacts limités », ajoute l'organisation.
« La CSEM déploie actuellement de nombreux efforts pour résorber les aléas de cette attaque informatique. »

« Aucune négociation »

« Il n'y a même eu aucune négociation » avec LockBit, assure Karim Ganame, expert en cybersécurité chez StreamScan, la firme qui aide la Commission à se relever de l'attaque. C'est lui qui avait la responsabilité de communiquer avec les pirates.

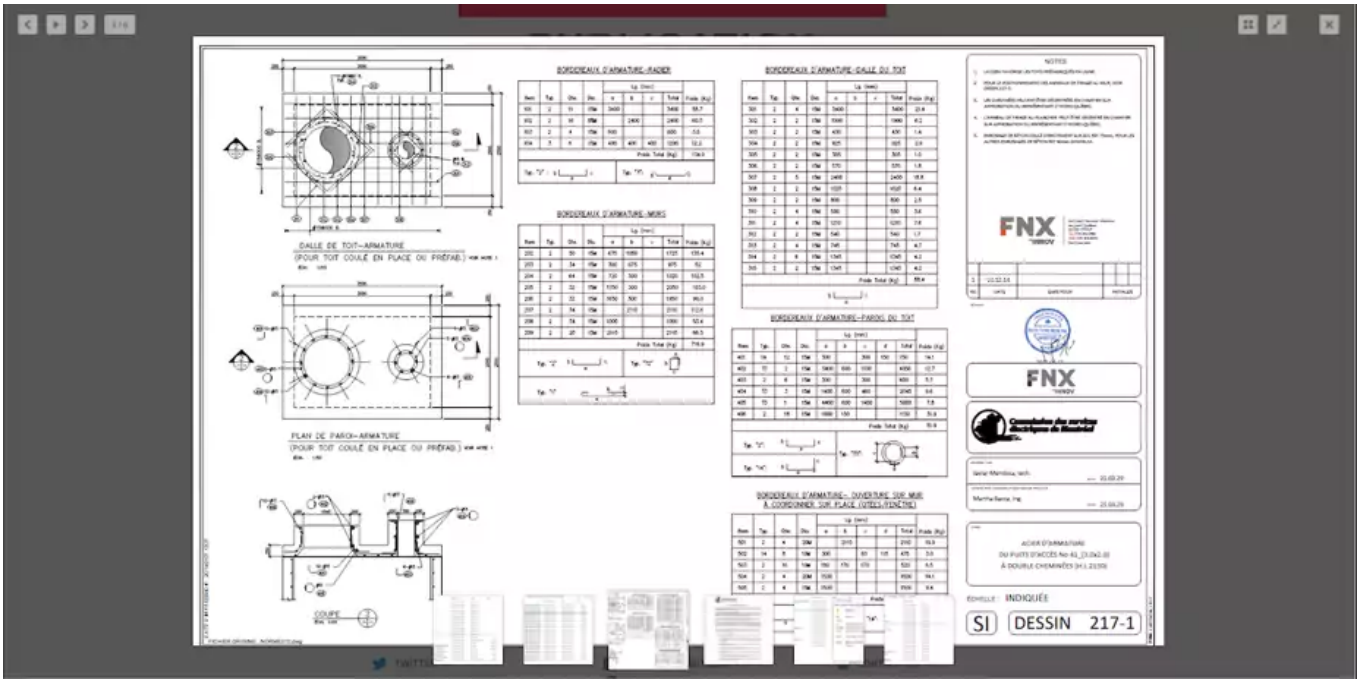
Depuis le 9 août, le gang affiche sur son site du web caché (*dark web*) une série de copies d'écran représentant des dossiers qu'il dit avoir volés sur les serveurs de la CSEM.

Selon ce qu'il affirme sur son site du web caché, le gang a dérobé des dizaines de dossiers portant des noms comme « chefcomptable », « Instructions de travail », « PAYE », « Gestion des systèmes » et « Gestion du réseau ».

CAPTURE D'ÉCRAN

LockBit menace de publier l'ensemble des données volées le 24 août. Typiquement, les pirates exigent une rançon de leur victime, pour promettre en échange de ne pas publier les renseignements dérobés.

Les cyberpirates montrent aussi un plan en coupe de conduits filaires.



CAPTURE D'ÉCRAN

Des plans de coupe de conduites affichés sur le site de LockBit dans le web caché

Analyse de risques

Malgré le chantage des pirates, la CSEM a rapidement pris la décision de ne pas payer, assure Karim Ganame.

« Quand on parle au pirate, il communique la liste de tous les fichiers qu'il a sortis.
Il a besoin de prouver qu'il a effectivement des données, explique l'expert en rançongiciels.
La compagnie analyse tout ça avant de prendre des décisions. »

De façon générale, les spécialistes s'entendent pour dire que les paiements sont à éviter.

« Dès qu'une compagnie paye une rançon, ça crée un appel d'air, explique Karim Ganame.
Le message que ça envoie aux pirates, c'est : la deuxième fois, on est prêts à payer encore. »

Avec l'argent, les cybercriminels peuvent financer leur organisation et améliorer leur mode d'action pour de futures attaques.

Infrastructure critique

Ancien militaire et ex-responsable de la sécurité de l'information au gouvernement du Québec, Steve Waterhouse se dit « rassuré » que la CSEM n'ait pas payé de rançon. « Mais je ne suis pas rassuré qu'ils aient été piratés », ajoute-t-il.

Il souligne que l'organisation détient une grande quantité d'informations sur des infrastructures critiques.

Est-ce que les pirates comprennent l'importance stratégique de savoir par où passent tous les types de câbles en ville ?
Si je suis un pas fin, je peux couper le bon fil et couper tout le *back bone* de Montréal.

Steve Waterhouse, ex-responsable de la sécurité de l'information au gouvernement du Québec

Alexis Dorais-Joncas, spécialiste des cybermenaces chez Proofpoint, souligne lui aussi l'importance des renseignements que détient la CSEM.
« Savoir où sont les fils, les points de jonction des réseaux, clairement, ce sont des choses qui ne doivent pas se retrouver entre les mains de quelqu'un de malveillant », dit-il.

Gang hyperactif

Dans une note conjointe en juin, les autorités de cybersécurité du Canada et de six autres pays ont identifié LockBit comme le rançongiciel le plus actif en 2022.
Il aurait fait « au moins 1000 victimes dans le monde », indique le FBI dans une plainte déposée contre un Russo-Canadien arrêté en octobre en Ontario pour avoir utilisé le programme à des fins d'extorsion.

Malgré cette frappe, le gang n'a jamais cessé d'être actif et d'afficher de nouvelles victimes sur son site du web caché.

Au Québec, LockBit s'est notamment attaqué à la Ville de Westmount en novembre dernier.

En savoir plus

- 22 %
  Proportion des attaques au rançongiciel attribuables à LockBit au Canada en 2022

Understanding Ransomware Threat Actors : LockBit (Cybersecurity & Infrastructure security Agency)

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230810
"C'est ensemble qu'on avance"