Valéry Rieß-Marchive **@ValeryMarchive** *Mon Oct 17 14:29:45 +0000 2022*

Et une nouvelle #colterr victime de #cyberattaque "de grande ampleur" (lisez: #ransomware) en ■■ cc @ransomwaremap **https://t.co/unT1d0ToHf**

Donc, pour tous ceux pour qui ce n'est pas encore clair : "cyberattaque de grande ampleur" veut dire "cyberattaque avec ransomware". #pudeur

https://twitter.com/AlvieriD/status/1582357529799299072?s=20&t=pKwlEQjFzjH_XKZ47sVXQw

Tiens, continuons sur la #comcrise, avec ma grille de lecture des communications officielles.

Je lis : "Tout a été arrêté, par mesure de sécurité."

Je comprends : "Plus rien de marchait, du coup, planté pour planté, on a coupé le réseau".

Je lis : "le temps de repérer le type d'attaque".

Je comprends : "vous avez dit, quoi ? Rançonmachin ? Naaan... pas chez nous."

Je lis : "pour l'instant, nous n'avons pas détecté de vol de fichiers."

Je comprends : "on n'a pas de logs réseau et aucune d'idée de ce qu'ils ont pu nous piquer."

Je lis : "il n'y a pas eu de demande de rançon."

Je comprends : "on n'a pas suivi les instructions de la ransom note".

Je lis : "c'est un logiciel tout nouveau, jamais vu avant, fait tout rien que pour nous".

Je comprends : "avec le packer, les bases de signatures des AV n'ont rien vu".

Je lis : "on ne sait pas encore de quel ransomware il s'agit".

Je comprends : "on n'a pas envie de vous le dire, des fois que... on sait jamais..."

Je lis : "on a détecté très vite la cyberattaque".

Je comprends : "on a rien vu venir, mais quand le ransomware a tout pété, ça nous a sauté aux yeux".

Voilà, c'est tout pour moi, là comme ça, en coup de vent. Si vous en voyez d'autres, n'hésitez pas à allonger la liste. C'est fait pour ça : malheureusement, un jour ou l'autre, ça pourrait rendre service à un #dircom pour éviter certains écueils classiques de la #comcrise.