Ransomware : 3 infos sur l'attaque contre la Région Grand Est

Les rançongiciels, cybermenace numéro 1 pour les collectivités ?

Ainsi la « Gazette des communes » titrait-elle un article paru fin janvier à l'occasion du FIC.

L'Anssi a récemment relayé ledit article sur son Twitter.
En toile de fond, une attaque contre la Région Grand Est.

> *« Les rançongiciels, la #cybermenace numéro 1 pour les collectivités »#Cybersécurité @Lagazettefr présente la revue des enjeux actuels pour collectivités territoriales #CollTerr #FIC2020 #Presse https://t.co/Tl0lWFohyR*
>
> *— ANSSI (@ANSSI_FR) February 20, 2020*

Jean Rottner, président du conseil régional, y avait fait allusion le 14 février, à l'occasion de la commission permanente mensuelle de l'assemblée, réunie à Strasbourg.

« *Si votre messagerie ne fonctionne pas forcément génialement bien, c'est parce que depuis cette nuit, nous avons été victimes d'une attaque externe qui nous a obligés à couper nos serveurs et à agir en conséquence* », avait-il déclaré.

Le travail de milliers d'agents perturbé

La presse régionale avait commencé à se saisir de l'affaire la semaine suivante.

En première ligne, « L'Union ». Dans un article du 19 février, le média champenois affirmait que « tous les ordinateurs des agents et des élus [étaient] quasiment inutilisables ».

Le lendemain, France Bleu évoquait une attaque sur les postes de travail de 7 500 agents. Avec, pour conséquences, l'impossibilité d'accéder à la messagerie, aux serveurs communs, aux logiciels internes et au système de badgeuse.
L'accès aux e-mails était partiellement rétabli (envoi de pièces jointes bloqué), annonçait la radio. Elle précisait que l'attaque avait également touché les postes informatiques des lycées, gérés par la Région.

Le même jour, une fonctionnaire de la Maison de la Région (Strasbourg) déclarait à l'AFP : « *On arrive à travailler sur la plupart des logiciels* ».

Une demande de rançon non honorée

Dans la matinée du 21 février, « Le Monde » faisait état d'un bilan plus modéré. L'attaque aurait « déstabilisé le travail concret de 2 000 agents, [de] 169 élus et [des] 180 membres du Ceser, le

conseil économique, social et environnemental régional ».

D'après le quotidien, la Région n'était « pas entrée en contact » avec les « racketteurs ». Elle avait en l'occurrence pu rétablir la situation d'elle-même, avec l'aide d'un prestataire externe et de l'Anssi.

> *Toutes les mesures ont été prises pour gérer cette attaque qui peut encore entraîner quelques retards dans les réponses que nous apportons*
> *Un grand merci à tous nos collaborateurs de la @regiongrandest qui œuvrent au quotidien pour un retour à la normale.https://t.co/aRElXD49S1*
>
> *— Jean ROTTNER (@JeanROTTNER) February 20, 2020*

La piste Dridex

Numerama s'est entretenu avec Pierre Gundelwein, directeur du numérique de la Région.

Celui-ci a confirmé la désactivation provisoire de l'envoi de pièces jointes avec les adresses e-mail de la Région. Le temps notamment de rétablir les sauvegardes effectuées le 13 février au soir (80 serveurs touchés).

Le virus en cause semble apparenté au cheval de Troie bancaire Dridex. Sévissant depuis au moins 5 ans, il se propage généralement par l'intermédiaire de documents Word infectés. Sa diffusion sur le SI de la Région Grand Est s'est fait grâce à l'annuaire.

Photo d'illustration © lolloj – Shutterstock.com