La moitié des écoles de Bordeaux victimes d'un ransomware

Selon nos confrères de Sud-Ouest, pas loin d'une école bordelaise sur deux a été la victime d'une attaque informatique. Le phénomène a démarré en septembre et s'est accéléré jusqu'aux vacances de Noël, pour toucher au total les serveurs d'environ 40 établissements sur les 101 écoles que compte la préfecture de la Gironde. Un audit est en cours pour tenter de déterminer l'origine de l'infection. L'adjointe au maire en charge de l'éducation, Emmanuelle Cuny, parle d'une attaque « *sans précédent* ».

S'il est encore trop tôt pour se montrer catégorique, l'infection semble provenir d'un ransomware qui s'est diffusé de machine en machine. Comme le note le site spécialisé DataSecurityBreach, l'Académie de Bordeaux dispose d'un contrat avec l'éditeur d'antivirus TrendMicro, pour le produit Internet Security. Reste à savoir si cette protection a été dupée par les cybercriminels ou si – comme c'est plus probable -, elle n'a pas été correctement installée dans les établissements victimes du fléau. Selon Sud-Ouest, les données pédagogiques sont menacées par cette épidémie.

Un ransomware 'soigne' 5 hôpitaux de Londres

Nouveau gagne-pain des cybercriminels, les ransomwares ciblent tous types d'organisations, en se diffusant le plus souvent via des fichiers piégés joints à des mails. En 2016, de nombreux hôpitaux aux Etats-Unis, mais aussi en France (citons le Centre Hospitalier d'Épinal ou l'hôpital Duchenne à Boulogne-sur-Mer), ont été les victimes de ce type de malware. Une fois la souche infectieuse activée par un utilisateur, elle chiffre les données de son poste de travail et se répand sur le réseau de l'organisation, pour prendre en otages d'autres fichiers. Pour restaurer l'accès à l'information, les cybercriminels réclament des rançons payables en cryptomonnaie. Tout récemment, des pirates ont réclamé l'équivalent de 9 000 euros à des établissements scolaires britanniques infectés par un ransomware. Seule solution pour éviter de payer : repartir des sauvegardes… pour peu que celles-ci existent et soient récentes.

Ce week-end, un établissement de santé britannique regroupant 5 hôpitaux de l'est de Londres (Royal London, St Bartholomew's, Whipps Cross, Mile End et Newham) a lui aussi reconnu avoir été victime d'une attaque. Les premières mesures prises – demande faite au personnel de ne pas ouvrir de pièces jointes d'expéditeurs inconnus, déconnexion de certains systèmes pour éviter leur contamination – indique, une fois de plus, une infection par un ransomware, ce que l'établissement, le Barts Health Trust, reconnaît dans un communiqué. L'étendue de l'infection et ses conséquences restent toutefois inconnues à l'heure où nous écrivons ces lignes, l'établissement de soin se contentant d'indiquer « *faire tout ce qui est possible pour les patients ne soient pas touchés* ». Les postes du Barts Health Trust fonctionnent encore sous… Windows XP.

A lire aussi :

Comment le ransomware est devenu le gagne-pain des cybercriminels

Après les ransomwares, la prochaine menace est le ransomworm

RansomFree, l'application qui leurre les ransomwares

Photo : portalgda via VisualHunt / CC BY-NC-SA