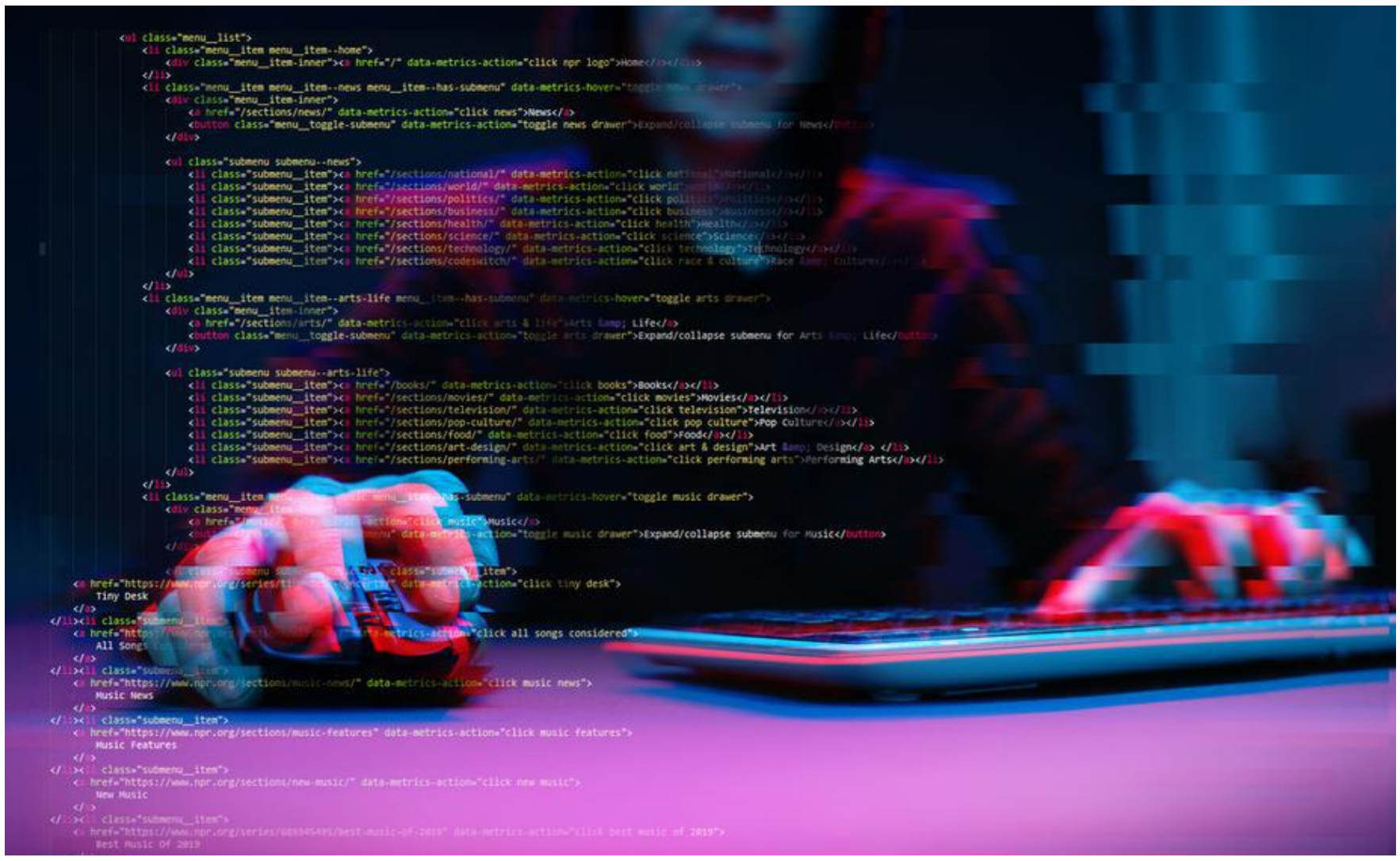
CYBERCRIMINALITÉ

Un nombre important d'institutions et de sociétés belges sont tombées dans le piège des ransomwares. Certaines paient une rançon, dans la plus grande discrétion. D'autres refusent. Leurs données sont publiées sur le darknet.



Les plaintes pour des actes de criminalité informatique ont explosé en dix ans : les chiffres de la police fédérale font état d'un bond de 150 % entre 2011 et 2020. © SHUTTERSTOCK.

Dans les filets des rançonneurs informatiques

ALAIN JENNOTTE
JOËL MATRICHE
ARTHUR SENTE

Un lundi matin d'octobre. Les yeux embués de sommeil, une employée de cette entreprise liégeoise tente de consulter son planning à distance. Mais le serveur est injoignable. Les e-mails refusent de quitter sa boîte d'envoi. Et la ligne téléphonique sonne dans le vide. C'est que durant la nuit, l'infrastructure informatique a été paralysée par un « ransomware », un logiciel qui crypte toutes les données et rend les services inutilisables. Les cybercriminels proposent à leurs victimes la clé de décryptage en échange d'une rançon proportionnée à la taille ou au chiffre d'affaires de leur victime.

La société affirme au *Soir* qu'aucune rançon n'a été versée, que peu de données ont été perdues car elle disposait de copies de sauvegarde. Aucune donnée sensible concernant les clients ou le personnel n'aurait été dérobée. Mais un mois après ce braquage informatique, tout n'est pas rentré dans l'ordre. Pour preuve, un message sur la page d'accueil du site, prévenant les clients que l'entreprise rencontre des problèmes d'e-mail et de téléphonie.

Selon des informations que *Le Soir* a pu consulter sur le darknet (lire ci-contre), des données concernant cette entreprise se retrouvent pourtant en ligne. On y propose à la vente des accès à tous les serveurs de l'entreprise, ainsi que la liste des documents qui auraient été exfiltrés. Souvent, les pirates menacent de mettre en ligne les données dérobées, mais aussi, en cas de non-paiement, de les vendre aux plus offrants.

Un véritable business

Le Soir a visité une quinzaine de ces sites de racket. Il ne s'agit pas de pages web bidouillées à la hâte mais de véritables vitrines commerciales. Avec un modèle économique semblable : lorsque le virus s'est propagé dans un système, le contenu de celui-ci est crypté. Vient ensuite le temps des négociations. Ou pas : certaines victimes choisissent, par principe ou par incapacité financière, de ne pas céder et de restaurer elles-mêmes leur infrastructure informatique. *Le Soir* a contacté par courriel neuf cartels de ransomware, aucun n'a donné suite. D'Europol à la Computer Crime Unit fédérale (CCU) en passant par le Centre belge pour la cybercriminalité, le message est très clair : pas d'argent pour la mafia.

La rançon liégeoise

L'absence de traces sur le darknet de données d'une entreprise qui a été attaquée ne peut souvent signifier que deux choses : soit elle a payé la rançon, soit ses données ont déjà été vendues à un tiers. Une question que l'on peut légitimement se poser au sujet d'un autre cas liégeois, celui de la Ville de Liège.

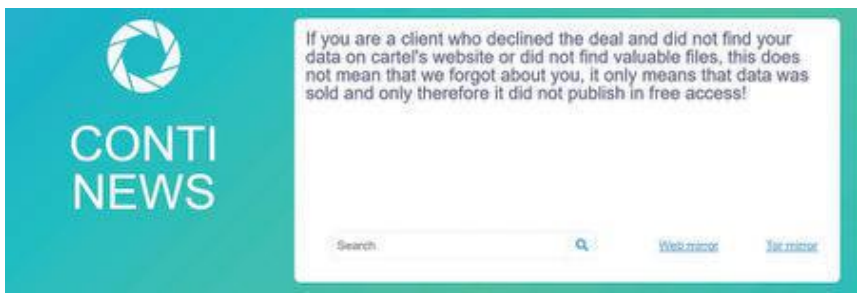
Le lundi 21 juin au matin, lorsque les employés communaux ont pris le travail, les 1.800 PC de l'administration ont multiplié les signes de faiblesse, entraînant très vite la paralysie des services. Le coupable : un ransomware nommé Ryuk. Ethias, qui assure la Ville contre les risques d'attaque informatique, a mis celle-ci en contact avec la firme néerlandaise de cybersécurité Northwave. « Leur aide nous a été très précieuse, de même que celle des experts de Microsoft », explique le directeur général de la Ville, Philippe Rousselle.

La Ville s'organise, pare au plus pressé. « L'essentiel a été restauré en un ou deux mois », se félicite Philippe Rousselle. Qui évalue les dommages à « environ un million d'euros, dont la moitié a été prise en charge par notre assureur ».

Selon les informations du *Soir*, une rançon a été versée aux attaquants, ceux-ci ont livré les clefs de décryptage. Le groupe à l'origine de l'attaque ne laisse en effet planer aucun doute quant à sa résolution, rappelant que lorsque les sommes réclamées ne lui ont pas été versées, les données piratées sont mises en libre téléchargement.

Une diffusion à tout vent que ne pouvait se permettre la Ville. Selon des témoignages concordants recueillis par *Le Soir*, un montant indéterminé aurait bel et bien été indirectement payé par l'assureur aux rançonneurs. Interrogés, Ethias et Northwave n'ont pas donné suite. Une information judiciaire a été ouverte. « Une dizaine de dossiers de ce type ont été ouverts dans l'arrondissement », précise le procureur Philippe Dulieu.

Refuser de payer la rançon – toujours exigée en cryptomonnaie – peut avoir des conséquences dramatiques. Témoin, cette immobilière bruxelloise attaquée cet été par le ransomware AvosLocker. Contacté, son gestionnaire informatique reconnaît s'être fait piéger. Il s'agirait même de la deuxième attaque subie par l'entreprise.



Le groupe Conti, à la base d'attaques avec le logiciel Ryuk, prévient : les données des victimes qui n'ont pas payé de rançon seront mises en ligne. © D.R.

« Payer une rançon ? C'est hors de question », affirment en chœur service informatique et direction. Quant à l'exfiltration possible de données, ils disent tout en ignorer. « Il n'y avait rien sur nos serveurs qu'il serait dangereux de laisser traîner en ligne. » Avant d'ajouter : « Nous n'avons d'ailleurs pas jugé utile d'effectuer des recherches pour nous en assurer. » Mais selon des documents découverts par *Le Soir*, des données de l'immobilière sont bien présentes en ligne. Parmi celles-ci, des listes de mots de passe, des factures, des listings destinés à la comptabilité (1). C'est le sort réservé aux « mauvais payeurs », histoire de mettre une pression maximale sur les autres victimes.

Les hôpitaux, des cibles de choix

Même le secteur des soins de santé n'est pas épargné. La clinique Saint-Luc de Bouge ou encore André Renard à Herstal en ont fait l'amère expérience. Mais le centre hospitalier de Wallonie picarde (Chwapi) de Tournai est, avec ses 2.700 collaborateurs, la plus importante cible hospitalière belge connue à ce jour. Une attaque y a été lancée le soir du 17 janvier 2021, à une heure où les effectifs étaient très limités. « Notre personnel de garde a reçu un appel pour un dysfonctionnement sur l'imagerie médicale. Rapidement il y a eu un emballement », se souvient Jacques Godart, directeur informatique du Chwapi. Ce soir-là, il décide de débrancher manuellement les serveurs pour sauver ce qui peut l'être – un peu moins d'un tiers des systèmes seront malgré tout compromis.

Le réseau informatique du Chwapi flanche, et avec lui, toute la chaîne médicale. « On a dû prendre la décision d'activer notre Plan d'urgence hospitalier et on est passé en service minimum. » Tout cela en pleine période covid. Heureusement, les serveurs contenant les données des patients n'auraient pas été compromis, assure la direction. Jacques Godard affirme que des fichiers dans lesquels se trouvait la demande de rançon n'ont été découverts que quelques jours plus tard sur les systèmes endommagés. Dans l'intervalle, « notre politique a très vite été de se dire que l'on avait la capacité de remettre nous-mêmes en place nos systèmes », poursuit-il. Près d'un an après les faits, la situation esquisse un retour à la normale.

Des assurances sur-mesure

Selon les statistiques de la police fédérale, le nombre d'attaques au ransomware connues a diminué entre 2017 et 2020. Mais « ces chiffres ne sont pas le reflet de la réalité », note Olivier Bogaert, de la FCCU. « Parce qu'il y a énormément de structures qui ne déposent pas plainte ou ne le signalent pas », surtout lorsqu'elles décident de payer. Les dénonciations pour des actes de criminalité informatique ont, pour leur part, bondi de 150 % entre 2011 et 2020.

De quoi pousser les assureurs à s'adapter. Axa, par exemple, a créé une offre sur mesure pour les très petites entreprises, les indépendants et les professions libérales. « Mais notre politique est, le cas échéant, de ne pas intervenir dans le paiement d'une rançon », intervient Pierre-Alexandre David, expert produits. Bâloise Insurance, par contre, peut intervenir dans ce paiement mais avec un plafond de 25.000 euros. Zürich Insurance peut également, selon ce qui est prévu dans les conditions générales de la police, procéder à un remboursement de ce qui a été payé.

(1) *Le Soir* a alerté l'entreprise avant la publication de ce dossier, lui recommandant de changer tous ses mots de passe si ce n'était déjà fait.

Darknet, l'autre réseau

Les appellations varient. On parle ici de darknet et là de dark web, voire de deep web. Mais quel que soit le nom que l'on donne à cette couche souterraine de l'internet, il s'agit d'un réseau auquel la majorité des internautes n'accède jamais, faute d'en connaître l'existence, et qui véhicule une aura particulièrement sulfureuse.
Et c'est vrai que l'on y trouve absolument tout : armes, munitions, drogues, médicaments sans ordonnance…
Les sites du darknet ressemblent certes à des sites classiques. Mais pour y accéder, on utilise un navigateur spécialisé – Tor est le plus populaire –, à même de se connecter de la manière la plus anonyme possible.
Pourtant, si ce darknet n'a guère bonne presse, il joue également un rôle clé et particulièrement bénéfique, et pas seulement dans le monde virtuel. Dans des régimes extrêmement répressifs, il a permis à des blogueurs d'informer en conservant un minimum de sécurité.
C'est là également que des leaks d'intérêt public ont été déposés. A.JE.