CYBERCRIMINALITÉ

Les « ransomwares », le (cyber)mal du moment

Des cas de vols de données contre rançon ont récemment mis à mal plusieurs cibles notables en Belgique, qu'il s'agisse d'entreprises privées ou d'institutions publiques. La face visible d'une « cyberpandémie » dont l'ampleur reste largement sous-évaluée.

ARTHUR SENTE

Cette semaine, c'était la Clinique Saint-Luc de Bouge, à Namur. La précédente, c'était le barreau de Charleroi. Et avant cela, durant l'été, d'autres institutions publiques amenées à jongler avec des données personnelles de leurs chers administrés comme la Ville de Liège ou le CPAS de Courcelles. Presque plus une semaine sans que l'on n'apprenne qu'une cible notable, en Belgique ou par-delà nos frontières, a été victime d'une cyberattaque. Enfin, pas de n'importe quel type de cyberattaque. Le terme d'attaque au « ransomware » – ou au rançongiciel, en français – est utilisé pour décrire le mode opératoire ici à l'œuvre, et dont la méthode se résume ainsi, pour faire (très) simple : après infiltration dans un système, généralement via une tentative victorieuse d'hameçonnage, l'auteur exfiltre des données et/ou les crypte grâce à un logiciel malveillant pour en bloquer l'accès à leur propriétaire. Pour en recouvrir l'usage, ce dernier est appelé à mettre la main au portefeuille. Les montants réclamés peuvent rapidement dépasser les dizaines voire les centaines de milliers d'euros.

Méthodes professionnalisées

En toile de fond, il y a l'essor inexorable d'organisations criminelles dont les méthodes se sont professionnalisées au fil des ans. Certains « gangs » de hackeurs, comme celui qui se cache derrière Lockbit 2.0. (le logiciel qui a dérobé les données du barreau carolo), mettant désormais à disposition – moyennant commission – leurs capacités de nuisance au profit de tiers, qui choisissent eux-mêmes leur cible. « Seul vous décidez durant la communication combien la société visée vous paiera, » vante l'entreprise criminelle dans ses « conditions d'utilisation » affichées sur son site, consultable sur le dark web.

Pour des cibles la plupart du temps impréparées, c'est la panique générale garantie. Notamment parce qu'en bloquant la machinerie informatique de leurs victimes, ces attaques ont des effets on ne peut plus concrets sur leur fonctionnement quotidien. « Le CPAS a été à l'arrêt total pendant plus d'une semaine », se remémore ainsi Aurore Goossens, présidente du CPAS de Courcelles, près de trois mois après l'attaque dont ses serveurs ont fait l'objet. Si à ce jour elle assure que son administration a pu recouvrir l'accès aux fichiers numériques relatifs aux dossiers sociaux des bénéficiaires, « par contre, on a totalement perdu le serveur qui contenait toutes les informations de la maison de repos ». A Saint-Luc de Bouge comme dans d'autres hôpitaux ciblés (à l'instar du Chwapi de Tournai, en janvier 2021), ce sont des rendez-vous de patients qui ont dû être annulés.

Tenir bon n'est pas si simple. Payer est totalement non recommandé, mais quand vous en parlez autour de vous, vous constatez que beaucoup de gens le font

Nathalie Monforti

Bâtonnière du barreau de Charleroi

Les inquiétudes concernant la sécurité des informations visées sont tout aussi réelles. A la Ville de Liège, où l'administration a été victime d'une frappe d'ampleur en juin, l'investigation a montré qu'il y avait bien eu « exfiltration de données ». Benoît Joseph, directeur des systèmes informatiques de l'administration, se veut néanmoins rassurant. Son service « a pris toutes les mesures en son pouvoir pour éviter l'exploitation de ces données. Sur ce point, l'affaire est considérée comme résolue. » Comprenez : à ce jour, aucune trace des données considérées comme « touchées » par l'attaque n'aurait été repérée sur le dark web par les experts en charge d'épauler la Ville face à ses déboires. Est-ce pour autant qu'elles sont restées au chaud dans les serveurs liégeois ?

Céder à l'appel de la rançon ou pas, la question se pose également. Car « si la structure ne paie pas, "ils" publient, » pointe Anis Haboubi, analyste en cybersécurité et autorevendiqué « hackeur éthique ». « On en a eu l'exemple avec le barreau de Charleroi », dont les fichiers ont fini par être mis à disposition via le dark web sur le site de Lockbit 2.0. Nathalie Monforti, bâtonnière du barreau carolo, assure qu'il ne fut pas si simple de « tenir bon ». « Payer est totalement non recommandé, mais quand vous en parlez autour de vous, vous constatez que beaucoup de gens le font », dit-elle. « Un confrère m'a dit qu'il y avait eu la même chose et qu'il avait payé illico. »

Chiffre noir

Assiste-t-on à un véritable emballement de cette forme de criminalité en Belgique ? Cela reste difficile à déterminer par les chiffres, même si le *feeling* est réel. En 2019, le Cert – à la fois « pompier » et « docteur » numérique belge chargé, sous l'autorité du Centre pour la cybersécurité de Belgique (CCB), de recueillir autant d'information que possible en cas de cyberattaque – n'a ainsi reçu « que » 94 signalements, pour 82 en 2020. « Mais le nombre réel est en réalité bien supérieur : les entreprises ou les particuliers ne déposent que rarement plainte », pointe Kathrine Eggers, porte-parole du Cert et du CCB. « Beaucoup de firmes se débrouillent, paient, et on n'entend parler de rien. »

Pour le reste, la multiplication des attaques « visibles » en Belgique n'est que le maigre reflet d'une problématique qui dépasse de loin la situation de notre pays. « Ce n'est pas un épiphénomène, mais un phénomène mondial », alerte Anas Haboubi, allant jusqu'à parler d'une « cyberpandémie » qui a déjà démontré qu'elle pouvait affecter des services critiques, avec des conséquences sous-jacentes colossales. En mai dernier, les serveurs de Colonial Pipeline, le propriétaire du système d'oléoduc qui garantit le flux de près de 45 % des carburants pour automobiles consommés sur la côte Est des USA, était ainsi pris pour cible, avec un effet direct sur l'approvisionnement des pompes. De quoi donner des sueurs froides aux plus hautes autorités américaines. La semaine dernière, Paul Nakasone, directeur de la NSA (l'Agence nationale de la sécurité), prédisait qu'il fallait s'attendre à des cyberattaques frappant « tous les jours » pour les cinq prochaines années au moins.

KROLL

ENSEIGNEMENT SUPÉRIEUR

Le nombre augmente

Le décret Paysage se targue d'augmenter le nombre de diplômés. Sur base des données que « Le Soir » a pu se procurer, ce taux est plutôt en diminution. Mais cette tendance était déjà en marche sous Bologne.

CHARLOTTE HUTIN
ERIC BURGRAFF

Alors que le décret Paysage s'apprête à subir une énième modification, quel est son impact sur le parcours des étudiants ? Cette question sensible fait l'objet de nombreux débats entre « pro-Paysage » d'un côté, et « anti-Paysage » de l'autre. Un débat où les chiffres se font rares, et où la couleur politique se glisse inlassablement. La question est pourtant cruciale. Implémenté à la rentrée 2014-2015 par l'ancien ministre Jean-Claude Marcourt (PS), ledit décret se targuait d'un objectif bien assumé : augmenter le nombre de diplômés du supérieur en favorisant l'accumulation de crédits. Qu'en est-il réellement ? Pour répondre à cette question, *Le Soir* a pu se procurer le suivi des cohortes des hautes écoles et écoles supérieures des arts, ainsi que des six universités francophones. Résumons.

1

Les tendances en hautes écoles et ESA

L'Ares (l'Académie de recherche et d'enseignement supérieur) a récolté les résultats des étudiants de première génération (qui s'inscrivent pour la première fois). La base de données commune débute pour l'année académique 2010-2011 et s'achève en 2020-2021. « Les étudiants sont suivis jusqu'à l'obtention de leur bachelier ou jusqu'à leur premier abandon », précise l'Ares. Après, ils disparaissent de la base de données.

Que montrent les chiffres ? Sous Bologne (de 2010 à 2014), 27 % des étudiants obtenaient leur bachelier à l'heure. Ceux inscrits sous Paysage n'étaient plus que 22 %. Soit une diminution de 5 %. C'est seulement sept ans après l'inscription en bachelier que le taux de diplomation sous Paysage atteint (sans le dépasser) le taux de diplomation sous Bologne. D'après une étude menée par Catherine Dehon, professeure de statistique à l'ULB et experte au cabinet de la ministre Valérie Glatigny (MR), il y aurait 2 % de diplômés en moins après cinq ans. Du côté des abandons, le constat semble tout aussi alarmant. Le taux d'abandon en première année reste stable (environ 22 %), mais il augmente après trois ans (de 6,6 à 7,3 %). Au fil du temps, les diplomations se font plus tardives, tout comme les abandons ; le parcours de l'étudiant s'allonge.

Cette tendance est-elle uniquement imputable au décret Paysage ? Pas vraiment selon l'Ares. « Le retard dans la diplomation était déjà en marche sous Bologne . Il faut prendre en compte l'attitude d'étudiants qui n'ont plus envie d'aller trop vite dans leur parcours. Ce comportement est récent. Ils se sont servis de la possibilité offerte par Paysage, c'est un choix de vie. Or, les chiffres n'expliquent pas le choix de vie… »

En revanche, la différence entre le taux de diplomation « à l'heure » sous Bologne et sous Paysage semble bel et bien significative ; sous Paysage, moins d'étudiants réussissent leur bachelier en trois ans. Si l'effet se marque davantage pour les élèves issus du secondaire qualifiant, les élèves du secondaire de transition sont eux aussi impactés. Cet effet disparaît pour les élèves inscrits en septembre 2016. « On a un taux de réussite bien meilleur avec le covid », expose l'Ares. « Le covid va tout changer dans les analyses, rendant les années avant et après difficilement comparables. »