répression Pour la police, une hydre difficile à chasser

A.JE, J.MA., A.SE.

Enquêter sur les ransomwares reste un boulot complexe. Policier à la Computer Crime Unit régionale (RCCU) de la police judiciaire liégeoise, Christophe Axen fait partie de ces enquêteurs belges qui se rendent régulièrement sur des scènes de cybercrime. Sa mission : tenter d'identifier par quel accès, par quel outil, par quelle structure les criminels sont passés. « Ça ne marche pas toujours », concède-t-il, « Ça reste un domaine assez récent, où les enquêteurs doivent aussi se mettre à jour. » D'autant que les effectifs spécialisés sont limités. Il faut souvent se concentrer sur les cas les plus lourds. « Globalement, quand ce sont des petites entreprises, on s'investit assez peu, soit parce qu'il n'y a pas de préjudice important, soit parce que ça ne nous est pas signalé. »

Sur les scènes de crime, la collaboration entre la police, les victimes et les sociétés informatiques qui leur proposent de l'assistance ne va pas toujours de soi. Les intérêts des uns et des autres étant souvent contradictoires. « Les victimes ne veulent pas forcément qu'on identifie les auteurs et qu'on les poursuive, elles veulent récupérer les données le plus vite possible », pointe Christophe Axen.

Récents coups de filet

Face à une menace invisible, décentralisée et globalisée, le travail d'enquête ne mène que rarement à des personnes en chair et en os. En octobre et en novembre, Europol, l'agence européenne de police criminelle, a néanmoins communiqué à trois reprises sur des arrestations menées sous sa coordination en Ukraine, en Suisse et en Roumanie. Parmi les criminels attrapés, des membres (de différents échelons) d'un groupe travaillant notamment sous le nom de Lockergoga, à l'origine d'une des attaques les plus violentes à avoir frappé l'Europe – celle du géant norvégien de l'aluminium Norsk Hydro, en 2019.

Qu'a appris Europol de ces opérations ? « Elles montrent que l'on est vraiment passé au Ransomware-as-a-Service, c'est un business model très bien établi, avec différents types d'acteurs qui utilisent des voies de communication différentes, avec des structures dans différentes juridictions », note Philipp Amann, directeur stratégique de l'EC3, département d'Europol en charge de la cybercriminalité. « Tout cela rend difficile l'accès à leurs infrastructures, qui sont cryptées, et implique de la collaboration internationale et le fait de travailler avec l'industrie et la recherche, pour trouver des moyens de "suivre l'argent". On voit aussi des criminels qui s'adaptent et changent constamment leur modus operandi. »

Convergence des criminalités

Europol observe aussi un basculement de la criminalité « classique » vers cette nouvelle forme de criminalité, plus « sûre ». Certaines des arrestations récentes témoignant du fait que le cliché du hacker adolescent exerçant depuis sa cave est en passe de devenir un souvenir. « Par le passé, l'organisation des groupes cybercriminels était assez différente de celle d'autres groupes criminels. Mais on voit maintenant une convergence vers le cyberespace. » Le milieu du ransomware n'étant plus à l'abri des effusions de violence, selon Philipp Amann. « Dans le cadre d'une opération récente, l'une des cibles a par exemple tiré vers les unités de police avec un AK47. »

En revanche, Europol estime qu'un grand nombre d'attaques sont bien moins sophistiquées que ne l'imaginent leurs victimes. « Les bonnes vieilles méthodes d'ingénierie sociale, d'utilisation très rapide des vulnérabilités des serveurs dès qu'elles sont connues ou la recherche systématique de serveurs qui n'ont pas été mis à jour fonctionnent toujours très bien. »

En octobre et en novembre, Europol a coordonné plusieurs opérations de police en Ukraine, en Suisse et en Roumanie, permettant l'arrestation de personnes liées aux « familles » de ransomwares Revil et Lockergoga. © EUROPOL 2021.

Des victimes belges aux profils divers

Besix
Selon une information publiée sur son site web le 17 octobre dernier, l'entreprise spécialisée dans la construction indique qu'elle « gère actuellement un incident de cybersécurité après avoir découvert une activité non autorisée sur son réseau . Depuis le samedi 9 octobre 2021, les systèmes ont été sécurisés, certains mis hors ligne, et des enquêtes approfondies ont débuté avec le concours des autorités et professionnels de la cybersécurité ». Contactée par *Le Soir*, la porte-parole du groupe ne souhaite pas discuter plus avant les détails de l'attaque. Il semble que seule une partie du périmètre belge de l'entreprise ait été affectée et qu'aucune des implantations internationales de Besix n'ait été touchée.

Société wallonne du logement
C'est en pleine crise des inondations, durant l'été, alors que ses équipes planchaient sur les problèmes de relogement des sinistrés que la Société wallonne du logement (SWL) a été l'objet d'une attaque par ransomware. « Un message des pirates nous a indiqué qu'ils allaient nous envoyer une demande de rançon, que nous n'avons jamais reçue », note le porte-parole de la SWL, Daniel Pollain. « Mais nous n'avions de toute manière aucune intention de l'honorer. Aujourd'hui tout est rentré dans l'ordre. »

Des données perdues ou se retrouvant en ligne ? « Nous avons perdu environ deux semaines de données », reconnaît Daniel Pollain. « Cependant, comme nos boîtes de courrier électronique n'ont pas été touchées, nous avons pu reconstituer tout ce qui avait été détruit. Par contre, nous n'avons jamais été informés que des données de la Société wallonne de logement auraient été exposées sur des sites web. »

Le barreau de Charleroi
Le cas de l'attaque au ransomware qui a raflé les données du barreau de Charleroi a fait grand bruit début octobre. Derrière l'assaut, on retrouve un groupe nommé Lockbit 2.0., lequel a publié quelques jours plus tard les fichiers dérobés sur son site hébergé sur le darknet. Preuve que la victime n'a pas succombé à la pression de la rançon.

Près de deux mois plus tard, Nathalie Monforti, bâtonnière du barreau carolo, ne regrette pas sa décision. « Très rapidement, on a réalisé que l'on saurait récupérer les données dérobées car on les avait sauvegardées dans un cloud externe. A ce moment-là, avec notre assurance, notre informaticien et la police, il a été décidé de ne pas payer. Je n'avais de toute façon pas envie de payer une organisation criminelle. »

Reste à devoir vivre en sachant qu'un grand nombre de données sont à ce jour encore accessibles sur le darknet. « Oui, les fichiers ont été mis en ligne », tient à relativiser Nathalie Monforti, assurant qu'a priori les informations les plus sensibles, à savoir celles reprises dans les dossiers disciplinaires du barreau, n'ont pas été divulguées. En être sûr à 100 % nécessiterait cependant un travail de vérification de longue haleine. « Et vous pensez bien que j'ai autre chose à faire que passer en revue les 9.000 documents qui se trouvent sur le darknet. » A.JE., A.SE.

1.800

Le lundi 21 juin dernier, les 1.800 PC de l'administration communale liégeoise ont multiplié les signes de faiblesse, entraînant très vite la paralysie de quasiment tous ses services. Le coupable : Ryuk, un ransomware découvert en 2018.

9.000

Début octobre, c'est le barreau de Charleroi qui a fait l'objet d'une attaque au ransomware. Derrière l'assaut, on retrouve un groupe nommé Lockbit 2.0., qui a publié quelques jours plus tard, sur son site hébergé sur le darknet, quelque 9.000 fichiers dérobés.

cybersécurité Des négociateurs en prise directe avec les rançonneurs

J.MA., A.SE.

De nombreuses sociétés actives dans le domaine de la cybersécurité ont fait de l'appui technique aux victimes de ransomwares leur spécialité. Parmi elles, certaines offrent un service de négociation sur mesure aux « rançonnés ». Après une attaque, les hackers laissent effectivement un moyen de les contacter. De quoi ouvrir une fenêtre de discussion. Des échanges peuvent alors s'engager pour tenter de faire baisser les enchères. Les négociateurs interrogés par *Le Soir* assurent dans certains cas être parvenus à diminuer par dix, voire par quinze, les montants initialement réclamés.

Garder la tête froide

Geert Baudewijns est le patron de Secutec, une société « cyber » belge ayant pignon sur rue – elle décrochait en mars un juteux contrat avec le Centre de cybersécurité de Belgique (CCB). Il revendique 221 négociations à son actif, « toutes réussies », dont une cinquantaine pour des clients belges. Des marathons qu'il dit enchaîner à un rythme de plus en plus effréné. « Dans mon cas, je fais en moyenne entre deux à quatre négociations par semaine. En 2019 et 2020, j'en avais une ou deux tous les mois. Ça a véritablement explosé », dit-il.

En la matière, chacun y va de sa méthode. « Je prends d'abord 48 heures pour voir comment les attaquants sont entrés, ce genre de choses. Puis je prends contact avec d'autres négociateurs, un peu partout dans le monde. Je leur demande qui est en train de négocier avec la même "famille" que moi et là, je mets le dossier dans la boucle », explique Geert Baudewijns. En mettant en relation ces différents « cas », les négociateurs peuvent ajouter un peu de pression sur les pirates. Car si après le versement d'une rançon par un client, il s'avère qu'un gang ne livre pas de clé de décryptage, l'information aura vite fait de circuler et de décrédibiliser l'organisation criminelle. Et les autres victimes seront alors nettement moins enclines à payer.

Geert Baudewijns, le patron de Secutec, revendique 221 négociations à son actif, « toutes réussies ». © BELGA.

Double discours des pirates

Créateur belge de la société de cybersécurité Lupovis, basée en Ecosse, Xavier Bellekens a lui aussi déjà plusieurs négociations à son actif. « La première chose, c'est de garder la tête froide. Le criminel joue sur le fait que le client vient de se rendre compte qu'il a perdu ses données », préconise-t-il. « Il faut donc essayer de diminuer l'importance de l'attaque pour la société. » Laisser entendre que l'entreprise dispose de peu de moyens est aussi un levier à utiliser.

Toutefois, même en cas d'acceptation de l'offre, la clé de décryptage peut ne jamais arriver. « Nous avons également eu des situations où la rançon est payée, puis l'acteur ou le groupe à l'origine de la menace révèle que ce montant ne valait que pour une des clefs de décryptage et que l'entreprise doit donc encore payer pour recouvrer un accès complet à ses données », poursuit Bruce Webster-Jacobsen, directeur des opérations de renseignement chez GroupeSense (USA).

La méthode, qui pousse à jouer le jeu des criminels, est aussi controversée. Tous les négociateurs interrogés en conviennent : payer doit rester un ultime recours. « Mais le choix n'est pas si évident lorsque vous avez des factures à honorer, du personnel à payer et que la survie de votre entreprise en dépend », nuance Julien Pélabère, expert en négociations complexes et fondateur du groupe Nera (France).