L'édito

Nicole Lamon
Rédactrice en chef adjointe

Enjeux sans frontières

Le réflexe primal en mars 2020, c'était de tout fermer. Des malades en Italie, on ferme la frontière, un premier cas au Tessin, on ne passe plus le Gothard, mon voisin qui tousse, je tire le verrou.

Au niveau planétaire, cela a rapidement donné des stratégies nationales en pagaille: de la Chine qui barricade au gros scotch sa population, jusqu'au Brésil qui nie l'existence du virus, en passant par la Suède qui laisse couler, s'essayant à la stratégie de l'immunité collective. Rien n'a fonctionné.

Et malgré l'expérience incroyable accumulée, ce réflexe primal nous a rattrapés tout récemment, à l'annonce de l'arrivée d'Omicron. Des malades en Afrique? Au Royaume-Uni? Aux Pays-Bas? *On impose des quarantaines aux voyageurs, alors que le dernier variant a, selon toute vraisemblance, déjà fait le tour du monde.* La stratégie pouvait marcher au temps long des diligences; à l'heure de la mondialisation, c'est peine perdue.

«Sans gouvernail planétaire, on pourra toujours continuer à chasser le virus du balcon, mais il reviendra par la fenêtre.»

Certes, le Conseil fédéral s'est rapidement repris, il vient de remplacer les quarantaines par des tests. Mais l'épisode est emblématique du manque de concertation internationale. Là où les nationalismes sanitaires et vaccinaux tournent en rond depuis deux ans, le multilatéralisme doit enfin parvenir à mieux se déployer. Car si ce n'est pas après une pareille crise planétaire, ce ne le sera jamais.

Cette semaine, l'Assemblée mondiale de la santé a adopté une résolution qui pourrait enfin faire bouger le paquebot en matière de gestion des pandémies. On verra dans les prochaines semaines si l'objectif d'une loi contraignante pour les presque 200 États membres de l'OMS est réaliste. Les pronostics sont réservés.

L'argument est aussi économique. L'Organisation de coopération et de développement économiques vient d'exhorter à accélérer la vaccination partout pour relancer la croissance. Selon elle, les pays du G20 auraient dépensé 10'000 milliards de dollars pour protéger leur économie, alors que vacciner la planète coûterait 50 milliards. Là encore, le manque de gouvernance mondiale est le principal écueil.

Tout comme la protection du climat, la lutte contre le Covid est un enjeu global. Sans gouvernail planétaire, on pourra toujours continuer à chasser le virus du balcon, mais il reviendra par la fenêtre.

À LIRE EN PAGE 8

nicole.lamon@lematindimanche.ch

Ils ont payé un million aux hackers: «C'était la seule chose à faire»

CYBERATTAQUE Cet été, la fondation vaudoise Le Relais et des entreprises genevoises ont vu leurs données cryptées par le redoutable groupe Black Matter. Les Genevois ont payé la rançon.

SYLVAIN BESSON, DOMINIQUE BOTTI, CHRISTIAN BRÖNNIMANN ET SVEN CORNEHLS

Le 16 août dernier, un lundi, vers 8 heures du matin, les employés de la fondation Le Relais, qui s'occupe de réinsertion sociale dans le canton de Vaud, découvrent qu'ils ont un sérieux souci informatique. *Sur leurs postes de travail, tous les documents sont bloqués. Le seul qu'ils peuvent ouvrir est une note intitulée «RQTNMTHNB.README». Elle est ornée d'un curieux logo évoquant la planète Saturne.*

«Qu'est-ce qui se passe? Votre réseau est crypté, et n'est plus opérationnel», dit la note, rédigée dans un anglais imparfait et signée par le groupe Black Matter. «Nous ne voulons que de l'argent. [...] Si vous ne nous contactez pas, nous publierons toutes vos données sur notre blog et les enverrons aux plus grands médias.»

Moment de sidération

À cet instant, à l'autre bout du Léman, plusieurs entreprises genevoises traversent la même phase de sidération: des écrans noirs, des ordinateurs qui ne démarrent pas, la paralysie totale. Il s'agit notamment d'une société de gestion de fortune, d'une entreprise de construction, d'un cabinet notarial et d'un distributeur de médicaments.

Tous partagent avec Le Relais un même prestataire informatique, X. Consulting. C'est lui qui a été piraté durant la nuit du dimanche 15 au lundi 16 août. Les cybermaîtres chanteurs réclament l'équivalent d'un million de francs en monnaies virtuelles, pour libérer les données des victimes et les détruire, sans les publier.

Près d'un million versé en bitcoins

Cette attaque n'est pas isolée. Elle s'inscrit dans une vague d'agressions aux rançongiciels (*ransomwares*) qui a frappé ces derniers mois les communes vaudoises de Rolle et Montreux, ou encore les EMS genevois de Vessy et des Châtaigniers. Ce qui est remarquable dans ce nouveau cas, c'est qu'une rançon a été payée – et que cela a fini par se savoir.

Plusieurs sources qui connaissent l'affaire ont confirmé au «Matin Dimanche» qu'un montant un peu inférieur au million de francs réclamé par Black Matter a été versé, en bitcoins. «Il a fallu décider de payer ou pas et nous avons payé, reconnaît l'une des entreprises genevoises concernées. Pour nous tous, l'enjeu était trop important. C'était malheureusement la seule chose qu'il y avait à faire pour protéger ce qu'il y avait à protéger.»

C'est un consortium, très vite mis sur pied entre les victimes genevoises de l'attaque, qui a réglé la facture. La fondation Le Relais – subventionnée à hauteur de plusieurs millions de francs par le Canton de Vaud pour s'occuper de quelque 2000 personnes en difficulté – a, quant à elle, refusé de payer.

Une fois la rançon versée, les hackers ont donné une clé de déchiffrement qui a permis aux Genevois de récupérer leurs données. «La plupart de ces groupes sont, entre guillemets, de «bonne foi». Ils donnent très souvent la clé de décryptage», explique Steven Meyer, de Zendata. Cette entreprise de cybersécurité a assuré la gestion de crise et les négociations avec les hackers de Black Matter.

L'attaque PowerShell

Ce groupe est un nouveau venu en Suisse, mais il a déjà sévi aux États-Unis et en Autriche. Son attaque sophistiquée s'appuie sur des logiciels pré-installés chez les victimes, comme «PowerShell», qui permet de prendre le contrôle de systèmes Windows à distance. Selon Steven Meyer, ses demandes de rançon s'échelonnent entre 100'000 et 7 millions de francs.

Comme d'autres hackers professionnels, Black Matter est un spécialiste de la double extorsion. Elle consiste à pénétrer les systèmes de la cible, par exemple avec un e-mail malveillant, puis à crypter ses données. Le groupe exige ensuite une rançon pour le décryptage. Et menace en plus de publier les données sur le Darknet si la cible ne s'exécute pas.

Apparue fin 2019, cette méthode a connu, depuis, une «croissance astronomique», selon Interpol. En Suisse aussi, on constate une «augmentation massive», selon Mathias Fuchs, de la société zougoise Infoguard.

De 30 à 50% des entreprises paient

Selon le centre fédéral de cybersécurité NCSC, les annonces pour des attaques aux rançongiciels ont triplé en 2021, avec 94 incidents rapportés au premier semestre.

Mais le nombre réel d'attaques est bien plus élevé. Selon Serdar Günal Rütsche, chef de la section cybercrime à la police zurichoise et responsable du réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), il faut multiplier par 20 le chiffre des annonces pour obtenir une estimation réaliste. Ce qui ferait plusieurs milliers d'attaques au rançongiciel cette année en Suisse.

Quelle est la proportion d'entreprises qui paient la rançon? Le sujet reste tabou, mais ce taux serait de 30 à 50%, selon Mathias Fuchs, d'Infoguard. En Suisse comme ailleurs, les autorités conseillent de ne pas payer. Mais ce ne sont que des recommandations. En réalité, les entreprises dont les données sont cryptées n'ont parfois pas le choix.

Mario Wagner

Les polices contre-attaquent, dans le monde comme en Suisse

C'est peut-être le début de la fin de l'impunité pour les hackers. Depuis le sommet Biden-Poutine à Genève, en juin dernier, une vaste offensive policière internationale cible les groupes criminels adeptes des rançongiciels.

Le 8 octobre, elle a conduit à l'arrestation en Pologne d'un Ukrainien de 22 ans, Yaroslav V. Il serait impliqué dans l'attaque de la société informatique américaine Kaseya, en juillet. L'arrestation s'inscrit dans une opération internationale, baptisée QuickSand/GoldDust, à laquelle ont contribué la police et la justice zurichoises.

Le 26 octobre, un membre suspecté d'un groupe de rançonneurs internationaux a été arrêté à Binningen, à côté de Bâle. Il s'agit probablement de la première arrestation liée aux rançongiciels jamais effectuée en Suisse. Toujours détenu, le suspect est sous enquête pour des soupçons de blanchiment d'argent et de destruction de données.

Sans commenter les enquêtes en cours, Serdar Günal Rütsche, chef de la section cybercrime à la police zurichoise, estime que ces arrestations marquent un tournant: «Nous avons travaillé des années sur les rançongiciels, pour accumuler de l'expérience et des compétences. Aujourd'hui, nous récoltons les fruits de ces efforts.» Selon lui, entre cinq et dix procédures pénales sont actuellement menées en Suisse pour des attaques aux rançongiciels.

«C'est un dilemme terrible à chaque fois. Sachant que chaque rançon s'apparente à une levée de fonds pour une start-up criminelle.»

Steven Meyer, expert en cybersécurité

«On a toujours très peu de temps pour prendre la décision de payer ou non, souligne Steven Meyer, de Zendata. Il faut peser le pour et le contre. Quelle est la conséquence de ne pas payer? Est-ce que l'entreprise pourrait faire faillite? Quel est le risque en cas de publication des données? C'est un dilemme terrible à chaque fois. Sachant que chaque rançon s'apparente à une levée de fonds pour une start-up criminelle.»

Comment négocier sa rançon

Si l'entreprise entre en discussion avec les assaillants, elle peut faire appel à des professionnels habitués à gérer ces situations, comme Infoguard ou Zendata. Leurs conseils: rester calme, respecter l'adversaire et s'engager dans la négociation avec une stratégie.

Veut-on payer pour régler le problème au plus vite, ou gagner du temps pour évaluer les dégâts et en savoir plus sur l'agresseur? Le négociateur peut se faire passer pour un novice ignorant des technologies, ce qui permet de ralentir les discussions.

Si l'on décide de payer, l'objectif est d'obtenir un rabais qui peut aller jusqu'à 70% de la rançon, selon Mathias Fuchs, d'Infoguard. Une tactique classique est de se faire passer pour un cadre subalterne, qui doit demander l'autorisation de payer à sa direction. Dans tous les cas, il faut considérer l'assaillant comme un homme d'affaires et mettre la discussion sur le plan du business, pas de la morale. «Ces groupes fonctionnent comme des entreprises, rappelle Sergio Alves Domingues, de l'entreprise de cybersécurité morgienne SCRT. Ils appellent leurs victimes des «clients».»

Six semaines pour redémarrer

Dans le cas de l'attaque de Black Matter les 15 et 16 août, les données des entreprises piratées ne sont pas apparues sur le Darknet après paiement de la rançon. Signe que ce groupe réputé sérieux a tenu parole.

Dans le canton de Vaud, la fondation Le Relais pense que les données de ses 2000 bénéficiaires sont sauves. «Jusqu'à preuve du contraire, il n'y a pas eu de vol de données, disent Claudine Wyssa et Sarah Benkhettab, présidente et directrice du Relais. Mais on n'en a pas la garantie. On ne peut pas avoir confiance dans les agissements des hackers, car même s'ils sont pros, ce sont des bandits.»

Le Relais a choisi de restaurer ses données à partir de sauvegardes des disques durs, avec l'aide de la société SCRT. La fondation a mis six semaines pour reprendre le contrôle de son système informatique.

COLLABORATION: RAPHAËL EBINGER

Trois groupes forment l'élite des cyberpirates

Avec des revenus se chiffrant en centaines de millions de dollars et des pertes infligées qui pourraient avoisiner 20 milliards de dollars en 2021, l'industrie du rançongiciel est devenue très professionnelle. Voici les trois groupes qui tiennent le haut du pavé dans cet univers.

Black Matter

Apparue en juillet 2021, cette nouvelle «marque» serait une réincarnation de Darkside, réseau de hackers d'origine russe qui a attaqué le pipeline américain Colonial Pipeline en mai dernier. Son successeur Black Matter a commis cet été la plus grande cyberattaque au rançongiciel à avoir frappé l'Autriche.

Dans un récent rapport, Google a qualifié Black Matter de «redoutable famille de rançongiciels». Encore actif début novembre, le groupe a, depuis, disparu du Darknet en raison de la trop forte attention du public et des autorités.

Conti

Peut-être le plus arrogant des groupes de hackers, Conti a fait des centaines de victimes depuis son apparition sur le Darknet en 2020. Dont des PME suisses comme Griesser (stores) et Habasit (fabricant de bandes transporteuses).

Le groupe possède des sites très professionnels où il propose, sur un ton cynique, de «prévenir tout dégât supplémentaire» à ses «clients» en décryptant leurs données. Conti est notamment derrière l'attaque au rançongiciel qui a frappé le système de santé irlandais en mai dernier.

Lockbit 2.0

Apparu en juillet dernier, Lockbit 2.0 serait actuellement le groupe de rançongiciel le plus actif. Son site très visuel expose les noms de ses victimes, avec des comptes à rebours indiquant le temps restant pour payer la rançon. Il se vanterait de posséder «le logiciel de cryptage le plus rapide au monde». Il a visé plusieurs PME suisses ces derniers mois, publiant leurs noms et dans certains cas leurs données sur le Darknet.