QUAND LE NET JOUE AU RACKET

Ecran noir, disque dur bloqué… Le seul moyen de retrouver ses données informatiques ? Payer. Ces prises d'otages numériques se multiplient. L'arme utilisée par les pirates s'appelle rançongiciel, ou virus racketteur.

PAR EMMANUEL PAQUETTE ET ANNE VIDALIE
ILLUSTRATIONS : SÉBASTIEN THIBAULT

Trois fois, l'alerte a été donnée au centre hospitalier Duchenne de Boulogne-sur-Mer (Pas-de-Calais). Trois fois, entre la fin de février et le début de mars 2016, l'établissement a été la cible de tentatives de prise d'otage numérique. L'arme des cyberkidnappeurs ? Des courriels anodins dans lesquels se cachent des virus capables de chiffrer les contenus ou de paralyser les ordinateurs. On les appelle *ransomwares*, ou rançongiciels : leurs victimes doivent verser une rançon à l'auteur du programme malfaisant pour recevoir la clef de déchiffrement qui libérera leurs précieux fichiers devenus illisibles (documents, photos, vidéos, etc.).

A l'hôpital Duchenne, on a eu plus de peur que de mal. « Nous avons pu isoler très vite les postes infectés et restaurer les données à partir des sauvegardes, précise le directeur, Yves Marlier. Nous avons seulement perdu le travail des dernières heures, sans conséquences sur les dossiers de nos patients. »

Qu'ils s'appellent Locky, SamSam, Jigsaw, Petya, Maktub ou CryptoWall, ces virus d'un nouveau genre, aux noms de personnages de bandes dessinées ou de films d'horreur, se dissimulent dans les pièces jointes aux mails et, plus rarement, dans des bannières publicitaires qui parsèment les sites Web. Un clic ou une visite sur un site contaminé, et le mal est fait : le contenu de l'ordinateur devient inaccessible. Malheur à celui qui n'a pas sauvegardé ses fichiers sur un support externe…

Des années d'archives perdues

Aux Etats-Unis, les policiers fédéraux du FBI estiment que les pirates informatiques ont ainsi extorqué 209 millions de dollars à des sociétés ou à des particuliers au premier trimestre de 2016. Sur le seul mois de février, l'éditeur d'antivirus Kaspersky a dénombré 40 000 tentatives d'infection chez ses clients. En France, aucun chiffre officiel ne circule. Mais une certitude s'impose : « C'est un vrai business criminel en bande organisée, qui touche tout le monde. Vous et moi, les entreprises petites et grandes, les collectivités territoriales et les associations », observe le colonel Nicolas Duvinage, qui dirige le Centre de lutte contre les criminalités numériques de la gendarmerie. Au début de cette année, le pervers Locky a fait des ravages dans les PME françaises. « Les dégâts économiques et financiers sont significatifs, constate Sylvie Sanchis, à la tête de la brigade d'enquête spécialisée de la préfecture de Paris. Des chefs d'entreprise venus déposer plainte nous ont dit avoir perdu des années d'archives ou des fichiers entiers de contacts clients. »

Comme le centre hospitalier Duchenne, celui d'Epinal aurait été attaqué par Locky voilà quelques semaines. Outre-Atlantique, le Hollywood Presbyterian Medical Center a récemment versé 17 000 dollars pour retrouver les dossiers de ses patients. Au début du printemps, l'organisme de soins MedStar Health, qui gère une dizaine d'établissements dans le Maryland et ▶▶

dans la région de Washington DC, a dû désactiver son réseau à la suite d'une agression. A la fin du mois d'avril, le Lansing Board of Water and Light, fournisseur d'eau et d'électricité dans l'Etat du Michigan, a également coupé l'accès à la messagerie électronique de 250 employés afin d'éviter des dommages supplémentaires et a même dû suspendre son système électrique. Le FBI enquête actuellement sur ce cas sensible.

Les *ransomwares* n'en sont pas à leurs premiers méfaits. Mais leur mode opératoire a changé. Dans les années 2010 et 2011, ils ne chiffraient pas les contenus d'une machine. L'utilisateur de l'ordinateur recevait un (faux) message aux couleurs de la gendarmerie ou de la police nationale l'accusant, à tort, d'avoir visité des sites pornographiques ou téléchargé des films ou de la musique illégalement. La victime était sommée d'acquitter une amende de quelques centaines d'euros.

Remonter aux auteurs ? Une gageure...

Depuis 2013, une autre génération de rançongiciels a émergé : ce sont les redoutables cryptolockers, les chiffreurs de fichiers, toujours plus nombreux, plus sophistiqués, plus sadiques. Petya, par exemple, bloque l'ordinateur, qui ne peut alors plus redémarrer. Quant à Jigsaw, du nom du personnage central du film d'horreur *Saw*, il supprime les fichiers un par un, heure par heure, tant que la rançon n'est pas versée. « Quand le chiffrement est bien fait, il est incassable, même avec une puissance de calcul phénoménale », constate Vincent Strubel, sous-directeur chargé de l'expertise à l'Agence nationale de la sécurité des systèmes d'information.

Contrer ces envahisseurs n'est pas une mince affaire. « Certains, comme CryptoWall et Locky, comptent des centaines de variantes, explique Matthieu Bonenfant, directeur marketing des produits chez le spécialiste de cybersécurité Stormshield. L'objectif est toujours le même : échapper à la détection

Des fichiers supprimés un par un, heure par heure, tant que la rançon n'est pas versée

par les systèmes de sécurité. » Et infecter l'ordinateur incognito. Autre motif d'inquiétude : même le système d'exploitation Mac OS d'Apple et les serveurs sous Linux ne sont plus à l'abri des codes malveillants.

Experts en informatique, les cybercriminels ont aussi le sens du business : ils exigent des rançons suffisamment modestes pour que leurs victimes préfèrent payer – et récupérer au plus vite leurs données – plutôt que porter plainte : de quelques dizaines à quelques milliers d'euros, sauf exception. Les autorités préconisent, elles, de ne pas céder au chantage. Mais, selon une étude de l'éditeur de logiciels Bitdefender, près d'un tiers des Français seraient prêts à débourser jusqu'à 190 euros pour récupérer leurs fichiers. Pour ne pas tuer la poule aux œufs d'or, les pirates libèrent bel et bien les données lorsqu'ils ont reçu l'argent. Du moins, le plus souvent...

En matière de devise, les racketteurs ont un faible pour le bitcoin, la monnaie numérique créée en 2009, qui s'achète en ligne avec une carte bancaire. Question de confidentialité. « S'il est possible de tracer le cheminement des versements en bitcoins, il est en revanche quasiment impossible d'identifier le titulaire du portefeuille ou sa localisation géographique », souligne Manuel Valente, directeur de la Maison du bitcoin, à Paris.

Voilà qui complique sacrément la tâche des cyberdétectives. « Il est vain d'espérer retrouver la rançon, reconnaît François-Xavier Masson, patron de l'office spécialisé au sein de la police nationale. Et remonter jusqu'aux auteurs est une véritable gageure. » Planqués derrière leurs écrans, les assaillants prennent mille précautions. Ils communiquent entre eux de manière anonyme via le réseau Tor. Louent, pour quelques heures ou quelques jours, les puissants serveurs dont ils ont besoin pour mener leurs campagnes. Changent régulièrement de comparses afin de brouiller les pistes.

Sur l'origine des attaques, les experts sont unanimes. « La plupart semblent provenir d'Europe de l'Est – Russie ou Ukraine, affirme Eric Freyssinet, responsable du Centre expert contre la cybercriminalité français. Mais la technique se diffuse : on peut acheter, sur le marché noir de l'Internet, des kits d'exploitation, vraies boîtes à outils pour profanes. »

Pour l'instant, le tableau de chasse des cyberenquêteurs n'est pas très fourni. En 2012, six Russes, deux Géorgiens et deux Ukrainiens ont été arrêtés dans la région de Malaga (Espagne), et leur chef, russe lui aussi, interpellé à Dubaï. Grâce au rançongiciel Reveton, la petite bande engrangeait, bon an mal an, plus de 1 million d'euros. En 2015, la police néerlandaise, avec l'aide de Kaspersky, a envoyé deux pirates derrière les verrous et mis la main sur des milliers de clefs de déchiffrement. La traque n'en est qu'à ses débuts.