« Crime as a service » : les rançongiciels s'industrialisent

Description

Ils s'appellent SamSam, Dharma, RobinHood, Prolock, Conti, Ryuk ou encore BitPaymer et sont quelques-uns des nombreux rançongiciels qui sévissent à travers le monde. Le procédé, apparu pour la première fois en 1989, est toujours le même. Il consiste à bloquer un équipement ou un réseau informatique, en cryptant toutes les données qu'il contient, avec pour objectif d'extorquer une rançon en échange de la clé de déchiffrement (voir *La rem* n°41, p.54).

Si certains de ces virus se répandent automatiquement sur le réseau, la plupart des attaques passent par l'intermédiaire d'un « cheval de Troie », programme informatique malveillant masqué sous l'apparence d'un fichier Word, PDF ou encore ZIP, envoyé en pièce jointe d'un mail et qu'immanquablement le destinataire va ouvrir. Selon la 6e édition du baromètre annuel du Cesin (Club des experts de la sécurité de l'informatique et du numérique), qui regroupe les responsables de la sécurité informatique de 700 entreprises françaises, une entreprise sur cinq déclare en 2020 avoir subi au moins *« une attaque par* « ransomware » *au cours de l'année, provoquant un chiffrement et/ou un vol de données, assortie d'une demande de rançon pour délivrer une clé de déchiffrement et/ou un chantage à la divulgation de données »*.

Il existe actuellement plusieurs centaines de familles de rançongiciels et, comme l'explique l'Agence nationale de la sécurité des systèmes d'information (Anssi), *« si certains n'entraînent que le chiffrement des données d'une seule machine, d'autres sont en mesure de chiffrer l'ensemble des ressources d'un réseau, supprimer les copies cachées, voire atteindre les systèmes de sauvegarde »*. Ces attaques par rançongiciel sont de trois types : *« spray and pray »* (ou *« fire and forget »*) désigne des attaques massives, peu sophistiquées et non ciblées, qui peuvent être effectuées par un attaquant sans véritables compétences informatiques, comptant sur le hasard pour tomber sur une victime mal protégée ; les *« attaques massives à propagation automatique »*, la plus importante ayant eu lieu en mai 2017 avec le rançongiciel Wannacry qui a infecté 200 000 systèmes informatiques dans 150 pays en une seule journée (voir *La rem* n°44, p.50) ; et enfin les attaques ciblées, appelées *« Big Game Hunting »*. Selon le Threat Report 2021, de la société de cybersécurité Sophos, si le nombre d'attaques par rançongiciel visant des entreprises semble avoir baissé entre 2017 et 2020, c'est qu'en réalité les pirates informatiques ont délaissé le *« spray and pray »*, d'ampleur massive et au caractère aléatoire, au profit du *« Big Game Hunting »* (la chasse au gros) ciblé, sophistiqué et bien plus rémunérateur, les demandes de rançon dépassant parfois le million de dollars, voire bien davantage. Ainsi Bouygues Construction s'est vu réclamer dix millions d'euros à la suite de l'intrusion du rançongiciel Maze en février 2020. En outre, ces attaques s'accompagnent souvent d'un vol de données sensibles, extraites des systèmes d'information de la victime, la menace de leur divulgation ajoutant un moyen de pression pour le paiement rapide de la rançon.

Autre évolution, les cybercriminels collaborent de plus en plus étroitement et se comportent davantage *« comme des cartels de la cybercriminalité que comme des groupes indépendants »*, dénonce la société Sophos. Selon Jérôme Notin, directeur du GIP Acyma, qui gère en France le site d'assistance aux victimes (cybermalveillance.gouv.fr), il existe *« une véritable chaîne d'approvisionnement du cybercrime, ce que l'on appelle le* « crime as a service ». *Pour les rançongiciels, il est possible d'acheter une attaque prête à lancer, il y a même des tutoriels en ligne et du reporting sur la rentabilité de l'attaque »*. Ces écosystèmes, très compartimentés, sont particulièrement difficiles à démanteler. Selon Éric Freyssinet, chef du pôle national de lutte contre les cybermenaces, *« les organisations cybercriminelles recrutent beaucoup de petites mains qui prennent une grande part des risques. Souvent, ces acteurs ne commettent qu'une petite infraction sur de petits montants, pas toujours réprimée dans tous les pays. Cela rend difficile l'identification du haut de la chaîne de valeur, de ceux qui prennent tous les bénéfices et nécessite des coopérations complexes entre les services à l'échelle internationale »*.

Ce fut notamment le cas d'une opération conjointe des policiers français de la sous-direction de la lutte contre la cybercriminalité et de leurs homologues ukrainiens, qui a conduit, en février 2021, à l'arrestation en Ukraine de cybercriminels liés au groupe Egregor, accusés d'être à l'origine de centaines d'attaques par rançongiciel. Les rançons payées en bitcoins ont permis aux enquêteurs de retrouver la trace de ces criminels. Apparu en septembre 2020, ce groupe pourrait avoir repris les activités de Maze, autre association de cybercriminels sévissant dans le monde entier depuis la fin de l'année 2019 mais qui avait justement cessé ses activités. Les victimes du groupe Egregor se comptent par centaines, parmi lesquelles, en France, l'éditeur de jeux vidéo Ubisoft, le transporteur Gefco, le quotidien *Ouest-France* ou encore l'hôpital de Dax dans les Landes. L'hôpital de Rouen avait également été la cible d'un rançongiciel particulièrement agressif en 2019. Profitant de la suractivité due à la pandémie de Covid-19 et dénués de tout scrupule, les pirates s'attaquent désormais aux établissements de santé. En France, 27 ont été atteints par une attaque majeure en 2020. Et le rythme semble s'accélérer. Selon le secrétaire d'État chargé de la transition numérique, Cédric O, qui s'exprimait récemment devant les sénateurs, on compte désormais une attaque par semaine contre des hôpitaux en France ; 110 ont été accompagnés dans des audits de sécurité en collaboration avec l'Anssi, qui apporte une aide, au jour le jour, à onze d'entre eux.

En janvier 2021, Emotet, l'une des plus grosses infrastructures logicielles de cybercriminalité a également été démantelée après six ans d'enquête, menée conjointement par les autorités des Pays-Bas, de l'Allemagne, des États-Unis, du Royaume-Uni, de la France, de la Lituanie, du Canada et de l'Ukraine. Cette opération, lancée dans le cadre de la Plateforme multidisciplinaire européenne contre les menaces criminelles (EMPACT), a été coordonnée par Europol, l'Agence européenne de police criminelle et Eurojust, l'Unité de coopération judiciaire de l'Union européenne.

Si Emotet a été découvert pour la première fois en tant que cheval de Troie bancaire en 2014, le *malware* a évolué au fil des ans pour devenir l'une des plateformes de prédilection des cybercriminels. Infectant des systèmes d'information à partir d'une pièce jointe corrompue envoyée par mail, Emotet se propageait, après avoir récupéré les mots de passe et dérober la liste des contacts, *via* le contenu et les pièces jointes attachés

aux mails. Ensuite, le botnet Emotet, réseau d'ordinateurs et de serveurs infectés, était loué contre quelques milliers de dollars à d'autres groupes de cybercriminels qui déployaient à leur tour leurs propres virus ou rançongiciels, comme TrickBot, Egregor et Qbot, puis reversaient une partie des gains obtenus. D'innombrables cyberattaques prenant appui sur Emotet ont sévi encore récemment en Nouvelle-Zélande, aux États-Unis, au Canada, en Italie ou encore aux Pays-Bas. La France n'est pas en reste puisque, pour la seule année 2020, le tribunal de Paris, le conseil départemental d'Eure-et-Loir, l'Agence nationale pour la formation professionnelle des adultes (Afpa), les services administratifs du Grand Est et le groupement AP-HP ont été quelques-unes des victimes indirectes d'Emotet. Son démantèlement par Europol est encore en cours : les autorités néerlandaises et allemandes ont physiquement saisi les « serveurs de commande et de contrôle » des cybercriminels, disséminés un peu partout en Europe. Dorénavant, tous les équipements informatiques compromis par Emotet sont reliés aux infrastructures des forces de l'ordre, et non plus à celles des cybercriminels, le temps pour Europol de collecter les preuves et de mesurer l'ampleur des dégâts, en nombre de machines et de victimes. Il est prévu qu'à 12 heures, le 25 avril 2021, une mise à jour désinstallera automatiquement le virus de toutes les machines infectées. D'après l'Anssi, il est probable que le groupe de cybercriminels à l'origine d'Emotet soit rattaché au groupe TA542, des cybercriminels d'origine russophone.

Face à la recrudescence des attaques par rançongiciel, les autorités tentent de s'organiser. Rien qu'en France les cyberattaques ont quadruplé en 2020, selon les données de l'Anssi. Le développement massif du télétravail a fragilisé la sécurité informatique des entreprises qui n'est pas étendue de manière suffisamment efficace au domicile des salariés, créant autant de potentiels points d'entrée. Les services de cloud des entreprises offrent également aux pirates de nouvelles opportunités pour s'immiscer au sein des organisations. De plus, l'arrivée des réseaux 5G, avec la promesse d'interconnecter les entreprises, les usines, les commerces, en plus des salariés, va grandement complexifier les exigences de sécurité informatique. Au-delà des entreprises, la numérisation de la société tout entière permet d'innombrables ouvertures aux cyberattaquants. La domotique, les objets connectés, les voitures, les villes, les avions, les écoles, les hôpitaux et les réseaux de distribution d'énergie ou d'eau sont déjà ou seront probablement les prochaines cibles.

Pour tenter de mettre en place une riposte à la hauteur des risques, la Commission européenne espère débloquer un investissement de 4,5 milliards d'euros, financé par l'Union, les pays membres et l'industrie, afin de mettre en place un « bouclier européen » contre les cyberattaques. Bruxelles veut également se doter d'une « unité conjointe cyber » qui réunirait les autorités judiciaires, les responsables diplomatiques et les responsables de la sécurité des États membres, pour mieux partager les informations en matière de cybercriminalité. En France, Emmanuel Macron a annoncé, en février 2021, un plan d'un milliard d'euros d'ici à 2025 afin de renforcer la cybersécurité du pays. L'Anssi disposera d'un budget de 136 millions d'euros, consacré à la sécurité des services publics et tout particulièrement celle des hôpitaux et des collectivités locales, régulièrement ciblées par des rançongiciels comme pourraient le confirmer les mairies de Marseille, Angers, La Rochelle, Vincennes, Alfortville ou encore Tullins (Isère).

Gageons également que des sociétés de cybersécurité vont développer des systèmes de plus en plus

performants. C'est en tout cas la volonté de la société Tehtris, dirigée par Eléna Poincet et Laurent Oudot, tous deux passés par la Direction générale de la sécurité extérieure (DGSE) et qui ont créé une plateforme de sécurité en mode SaaS (*Software as a service*) innovante, Tehtris XDR Platform, déjà utilisée par de grandes entreprises à travers le monde. Une infrastructure XDR, pour eXtended Detection & Response, correspond à une nouvelle approche de la cybersécurité qui ne s'attache plus uniquement à vouloir sécuriser chaque terminal susceptible d'être piraté mais se déploie, en tant que plateforme modulaire de détection et de réponse aux incidents de sécurité, sur l'ensemble du parc et du réseau informatiques d'une entreprise. La société Tehtris, fondée en 2010, compte 139 salariés. Elle réalisait plus de 5 millions d'euros de chiffre d'affaires en 2020, vient de lever 20 millions d'euros et prévoit d'embaucher 300 personnes dans les trois prochaines années.

Comme le dit Keren Elazari, chercheuse en sécurité, *« si les données sont le nouveau pétrole, il faut s'attendre à des marées noires, c'est-à-dire des fuites de données dangereuses »*. En attendant, les communiqués de gouvernements, de tribunaux, d'entreprises ou de collectivités faisant état d'une cyberattaque continuent de tomber comme autant de feuilles en automne.

Sources :

- « The State of Ransomware 2020 – Results of an independent study of 5,000 IT managers across 26 countries », Sophos, Sophos.com, may 2020.
- « Le Tribunal de Paris victime d'une cyberattaque, une enquête a été ouverte », Alice Vitard, usine-digitale.fr, 7 septembre 2020.
- « Des voitures aux écoles, les pirates se jettent sur de nouvelles cibles », Leigh Kamping-Carder, *The Wall Street Journal & l'Opinion*, 12 octobre 2020.
- « Le malware-as-a-service Emotet », Agence nationale de la sécurité des systèmes d'information, cert.ssi.gouv.fr, 20 octobre 2020.
- « Cybersécurité : Tehtris lève un montant record de 20 millions d'euros », Frank Niedercorn, lesechos.fr, 14 novembre 2020.
- « Sophos' 2021 threat report highlights a path forward », Sophos, Sophos.com, November 18, 2020.
- « Cybersecurity threatscape : Q3 2020 », ptsecurity.com, December 21, 2020.
- « 5 Ransomware Predictions to Ring In 2021 », Jessica Lyons Hardcastle, SDxCentral News, sdxcentral.com, December 30, 2020.
- « Rançongiciel, fraude au QR Code… 2021, année noire en vue pour les cyberattaques », Anaïs Cherif, *La Tribune*, 14 janvier 2021.
- « Flambée d'attaques informatiques contre les mairies en France », Florian Dèbes, lesechos.fr, 26 janvier 2021.
- « Au cœur de la cybercriminalité internationale, le botnet Emotet a été démantelé » Alice Vitard, usine-digitale.fr, 27 janvier 2021.
- « Le botnet Emotet démantelé par Europol », Louis Adam, zdnet.fr, 27 janvier 2021.
- « World's most dangerous malware Emotet disrupted through global action », Europol, Europol.europa.eu, January 27, 2021.

- « Le réseau Emotet, l'un des plus gros logiciels de cybercriminalité, démantelé lors d'une opération internationale », Martin Untersinger, Florian Reynaud, lemonde.fr/pixels, 27 janvier 2021.
- « Les policiers ont programmé l'autodestruction du malware Emotet », François Manens, cyberguerre.numerama.com, 29 janvier 2021.
- « Aujourd'hui, la cybercriminalité est une véritable industrie », Arnaud Devillard, sciencesetavenir.fr, 29 janvier 2021.
- « État de la menace rançongiciel à l'encontre des entreprises et institutions », Agence nationale de la sécurité des systèmes d'information, cert.ssi.gouv.fr, 5 février 2020.
- « Cybersécurité : des pirates « Egregor », à l'origine de l'attaque contre Ouest-France, interpellés en Ukraine », Emmanuel Leclère, franceinter.fr, 12 février 2021.
- « Ransomware : Des opérateurs d'Egregor interpellés en Ukraine », Catalin Cimpanu, zdnet.fr, 15 février 2021.
- « Cybersécurité : le plan à 1 milliard de l'État » Florian Dèbes, lesechos.fr, 18 février 2021.

Categorie

1. Techniques

date créée
18 mai 2021
Auteur
jacquesandrefines