High-Tech

Collectivités locales, hôpitaux... Les nouveaux terrains de jeu des hackers

Par David Bensoussan et Antoine Izambard le 28.05.2020 à 14h00

ABONNÉS

ENQUÊTE - Collectivités locales, universités et hôpitaux sont devenus des cibles privilégiées des rançongiciels. Et les pirates restent le plus souvent insaisissables.

La métropole Aix-Marseille-Provence a fait l'objet d'une sévère attaque par rançongiciel lors du premier tour des élections municipales.

ANNE-CHRISTINE POUJOULAT / AFP

COMMENTER

C'est un véritable cyberattentat, qui a mis hors d'état de marche les institutions de la deuxième ville de France. Une attaque exceptionnelle par son ampleur et son

impact, quasi éclipsée par la crise sanitaire. Le 14 mars, veille des élections municipales, un virus virtuel s'infiltre dans les serveurs de la métropole Aix-Marseille-Provence. Un fonctionnaire raconte : "90 % des données sont cryptées et rendues inutilisables. Notre site Web était planté, la comptabilité ne fonctionnait plus, nous ne pouvions plus régler les entreprises de BTP. Le virus a ensuite contaminé la mairie et a eu des conséquences dramatiques sur les services au public." Selon , 400 applications sont touchées. Les procurations pour les élections doivent être traitées à la main, le service Allô Mairie est indisponible, les listes d'inscription des enfants dans les écoles ont disparu et l'état-civil est hors service. Pendant des semaines, Marseille ne peut faire remonter les chiffres de décès du Covid-19. Il faudra près de deux mois pour rebâtir le système.

Le responsable de cette apocalypse numérique se nomme Pysa. Il fait partie des "rançongiciels" qui constituent, selon l'Agence nationale de sécurité des systèmes d'information (Anssi), "la menace informatique actuelle la plus sérieuse pour les entreprises et les institutions, par le nombre d'attaques quotidiennes et leur potentiel sur la continuité d'activité". On ne connaît pas encore précisément le vecteur initial de l'infection. L'assaillant aurait pu pirater, dans un premier temps, les protocoles RDP permettant l'accès à distance des postes sous Windows, des connexions suspectes ayant été repérées avant l'attaque. Le logiciel a ensuite désactivé les défenses antivirus, crypté les données et fait apparaître plusieurs textes formulant des demandes de rançon dans un anglais approximatif. L'un d'eux propose le déchiffrement gratuit de deux fichiers, en gage de bonne foi et de savoir-faire.

"Le mode opératoire semble compatible avec un acteur opportuniste motivé par un but lucratif", estime l'Anssi, qui n'a pas révélé le montant demandé. En octobre 2019, l'agglomération de Cognac s'était vue réclamer une rançon de 180.000 euros. "Il est recommandé de ne jamais payer, mais il est probable que certaines entités cèdent, car la rançon est souvent inférieure aux dépenses nécessaires pour remettre le système en état", souligne l'ex-policier Cédric Pernet, passé chez le spécialiste de la cybersécurité Trend Micro. Aux Etats-Unis, la mairie de Baltimore, qui a refusé de payer 100.000 dollars, a dû débourser 18 millions de dollars pour redémarrer son système.

S'ils ont longtemps répandu leurs virus par grandes vagues, contaminant particuliers et petites entreprises, les criminels se livrent désormais à ce que l'Anssi appelle le la chasse au gros gibier. L'an passé, l'agence a traité 69 attaques. Certaines ont concerné de grands groupes tels Altran, Fleury Michon, M 6 ou Bouygues Construction (lire encadré ci-dessous). Mais les collectivités locales et la santé sont de plus en plus ciblées. "Cela peut montrer l'intérêt des attaquants pour des entités réputées faiblement dotées en sécurité informatique ou dont la rupture d'activité aurait un impact social important". Dans les hôpitaux, elle peut mettre la vie des patients en danger, surtout en pleine crise sanitaire.

Durant le confinement, des rançongiciels ont notamment visé un centre de soins spécialisés à Paris et l'hôpital de Lomagne, dans le Gers. Dans cet établissement de 400 lits, les dossiers des patients ont été rendus illisibles pendant trois semaines, faute de payer la rançon de 40.000 euros. L'an passé, ce sont les hôpitaux privés du groupe Ramsay et les CHU de Montpellier et d'Issoudun qui ont été touchés. La cyberattaque la plus retentissante a eu lieu à Rouen en novembre. L'ouverture d'une pièce jointe dans un courriel malveillant a permis au virus de s'infiltrer. "Dans les grandes entreprises, l'accès au webmail privé est souvent bloqué, mais on a du mal à imposer ce réflexe dans les hôpitaux", note le consultant spécialisé Vincent Trély, directeur associé du cabinet Weliom et président de l'Association pour la sécurité des systèmes d'information de santé. Le rançongiciel dénommé Clop va provoquer l'arrêt de nombreux équipements, comme les dispositifs d'imagerie médicale. Des messages automatiques réclament une rançon de 40 bitcoins, soit 300.000 euros. Les soignants sont alors obligés de demander aux patients de reporter leurs visites ou de s'adresser à d'autres hôpitaux.

Les serveurs tournant sous Linux ont été épargnés et l'équipe informatique a pu rétablir la situation en 48 heures. Mais l'épisode est remonté jusqu'à l'Elysée et a fait office d'électrochoc, accélérant la mobilisation du ministère de la Santé. "On essaye d'être davantage dans la prévention que dans la réaction", avance le haut fonctionnaire Philippe Loudenot, qui fait le lien avec l'Anssi et pilote des audits réguliers pour détecter des vulnérabilités. "C'est déjà le cas pour la quinzaine de CHU de référence, et les audits sont étendus au fil de l'eau à tous les hôpitaux et cliniques." Le ministère procède aussi à des simulations d'attaques pour tester les résistances internes. A cela s'ajoute aussi les initiatives de groupes spécialisés comme Orange Cyberdefense ou PWC qui ont mis en place durant le confinement une hotline avec un numéro vert à destination des hôpitaux. "Certaines des attaques sont assez sophistiquées et impliquent de réagir très rapidement" plaide Michel Van Den Berghe, le directeur général d'Orange Cyberdefense.

Quant à coincer les cybercriminels, souvent étrangers, c'est une autre paire de manches. Si l'assaillant de Marseille reste inconnu, l'Anssi soupçonne le groupe criminel russophone TA505 d'avoir attaqué le CHU de Rouen. Connu pour cibler le secteur de la finance, mais aussi des universités, à Anvers et Maastricht, il serait, selon l'éditeur Proofpoint, très actif depuis le confinement, lançant des campagnes de courriels "hameçons" pour répandre ses virus et viser des laboratoires et des hôpitaux américains. "On arrive à cartographier les attaques, mais leur attribution précise reste difficile", reconnaît François-Xavier Masson, le patron de l'OCLTIC, l'office central de la police judiciaire spécialisé dans la cybercriminalité. Et il est aisé pour les pirates de falsifier les preuves. "Ils utilisent des serveurs "rebond" renvoyant à d'autres adresses IP ou glissent des caractères d'un alphabet étranger dans une ligne de code", note Emmanuel Gras, le patron de la start-up de cybersécurité Alsid. "Certains se procurent des kits de rançongiciels prêts à l'emploi

sur le darknet, ce qui brouille encore les pistes", ajoute Alice Chérif, qui pilote la section spécialisée du parquet de Paris, chargée de centraliser les procédures. "Désormais, face à cette cybercriminalité, on s'assure que les services d'enquêtes partagent bien leurs informations", prévient-elle. Comme dans l'antiterrorisme.

> "On a vraiment eu chaud", se souvient un cadre de Bouygues Construction. Le 30 janvier, les 3.200 salariés du siège se retrouvent au chômage technique. Un virus vient de verrouiller leurs données et une rançon de 10 millions de dollars est réclamée. Le responsable de ce raid de haut vol, dénommé Maze, est considéré par l'Anssi comme "le rançongiciel ayant le plus fort impact potentiel sur les entreprises et les institutions". Outre le cryptage, il permet aux pirates d'exfiltrer les données et de menacer de les divulguer en ligne. Cela aurait été le cas pour des fichiers dérobés à Bouygues. Maze avait déjà publié des données de la société américaine Southwire. "Ces groupes évoluent vers plus de communication, note Thierry Delville, associé du cabinet PwC. Maze revendique ses attaques et informe le public de l'avancement du paiement de la rançon." En mars, les pirates s'étaient même fendus d'un communiqué promettant aux victimes un geste commercial durant le confinement.

MARSEILLE

SUR LE MÊME SUJET

EasyJet cible d'une cyberattaque, les données de 9 millions de clients exposées

Nouvelle vague de "cyberbraquages" dans l'Hexagone

Le Cned et Bpifrance victimes de cyberattaques

Les Hôpitaux de Paris victimes d'une cyberattaque en pleine crise du Covid-19