L'HUMANITÉ DIMANCHE

PAYS : France
PAGE(S) :40;41;42;43
SURFACE :213 %

PERIODICITE : Hebdomadaire
RUBRIQUE : Nos vies
JOURNALISTE : Pierric Marissal

▶ **6 février 2020 - N°694**

NOS VIES

LES CYBER-ATTAQUES, UN FLÉAU VIRAL

À coups de systèmes piratés, d'e-mails frauduleux, les cybercriminels rançonnent de nombreuses victimes. Des dommages évalués à plusieurs centaines de milliards d'euros, auxquels s'ajoutent des effets souvent irrémédiables et potentiellement gravissimes, notamment pour les entreprises et les collectivités.

Selon une étude d'Accenture, les attaques par rançongiciel sont en hausse de 20 % sur un an, en France, et 76 % plus coûteuses pour les victimes. Les dommages causés par ces cyber-attaques s'élèveraient ainsi à près de 600 milliards d'euros à l'année, à l'échelle mondiale. La liste des victimes est longue. Altran (un groupe d'ingénierie), début 2019, a vu son système informatique paralysé pendant vingt-six jours, Fleury Michon (agroalimentaire) s'est fait attaquer en avril, puis Airbus, M6 et RTL en octobre, comme les pompiers de Dordogne et Bouygues Construction récemment… En mars 2018, 76 % des patrons d'entreprise de taille intermédiaire disaient avoir connu une cyber-attaque dans les douze derniers mois.

L'ouverture d'une simple pièce jointe d'un e-mail peut suffire à paralyser, en cryptant toutes les données, l'ensemble du système informatique d'une entreprise ou d'un service public. Privant les salariés d'accès à leur messagerie, à la comptabilité, au service de paye et de facturation, avec les contacts de prestataires et clients qu'on ne peut prévenir… À la place un message : en échange d'une rançon payable en bitcoins, les preneurs d'otages informatiques promettent une clé de déchiffrage. Une promesse à la fiabilité limitée. « Nous conseillons aux victimes de ne pas payer car, même si elles cèdent, il y a très peu de chance qu'elles récupèrent leurs données, et, heureusement, ça commence à se savoir », explique l'adjudant-chef Grégory Golynski, enquêteur N-Tech (technologies numériques), à la gendarmerie de Vannes (Morbihan).

LE SILENCE DES VICTIMES

« On ne connaît publiquement que 3 à 4 % des attaques, les entreprises refusent généralement de communiquer, voire de porter plainte, elles ont peur qu'être victime d'une cyber-attaque ne fragilise leur capital confiance auprès de leurs clients, il n'y a donc pas de partages d'expériences non plus », déplore Pierre Bogenschütz, président de Veyan, une entreprise du Morbihan qui accompagne les organisations dans la sécurisation de leur patrimoine numérique. Pire, ne pas communiquer entretient une forme de »

La liste des victimes est longue. Fleury Michon s'est fait attaquer en avril 2019, puis Airbus, M6 et RTL en octobre, Bouygues le 30 janvier 2020…

L'HUMANITÉ DIMANCHE

PAYS : France
PAGE(S) :40;41;42;43
SURFACE :213 %

PERIODICITE : Hebdomadaire
RUBRIQUE : Nos vies
JOURNALISTE : Pierric Marissal

▶ **6 février 2020 - N°694**

Image non disponible.
Restriction de l'éditeur

GETTY IMAGES

La prise de conscience tarde à venir. Les experts alertent : « On craignait le bug de l'an 2000 ? Aujourd'hui, il y a vingt ans de numérisation intensive en plus. »

L'HUMANITÉ DIMANCHE

PAYS : France
PAGE(S) :40;41;42;43
SURFACE :213 %

PERIODICITE : Hebdomadaire
RUBRIQUE : Nos vies
JOURNALISTE : Pierric Marissal

▶ **6 février 2020 - N°694**

déni de réalité. Jean-Philippe Pagès, en charge de ces questions chez Bessé, cabinet de conseil en assurance, a fait appel à la psychologie cognitive pour comprendre ce paradoxe. « La menace cyber représente encore un risque flou, lointain, difficile à cerner et donc à prendre en compte. En plus, la peur n'est pas un moteur pour les dirigeants d'entreprise. »

Beaucoup d'experts en cybersécurité en sont presque à attendre un « 11 Septembre » ou un « Fukushima » du numérique pour qu'il y ait une véritable prise de conscience. « Souvenons-nous des craintes autour du bug de l'an 2000, mais avec vingt ans de numérisation intensive en plus », avertit Jean-Philippe Pagès.

« LA SURVIE DE L'ENTREPRISE EN JEU »

La catastrophe, l'entreprise STLM, PME bretonne spécialisée dans le transport, l'a connue il y a quelques semaines. Elle s'est vu infecter par un rançongiciel un vendredi en fin d'après-midi, et, comme son système de sauvegarde s'active tous les trois jours, le temps de comprendre, le lundi suivant, ce qui s'était passé, tout était infecté. « On revenait seize mois en arrière sur la compta, l'exploitation, tout… On ne pouvait plus facturer non plus, la survie de l'entreprise était en jeu », raconte le patron. Pour autant, il n'a pas cédé à la demande de 15 000 euros en échange de la clé de décryptage. Il contacte son prestataire informatique local qui s'avoue perdu.

AUGUSTIN LE GALL/HAYTHAM-REA

Image non disponible.
Restriction de l'éditeur

Le C3N, département de la gendarmerie dédié à la cybercriminalité, témoigne tant de la progression que de l'évolution constante du phénomène.

Le chef d'entreprise porte plainte à la police de Vannes, qui se révèle tout aussi démunie. Au bout de quinze jours, on l'oriente vers une entreprise vannetaise spécialisée. Celle-ci décèle que, coup de chance dans son malheur, STLM a été victime de GandCrab. Ce rançongiciel a eu son heure de gloire, mais ses concepteurs, partis profiter de leurs larcins – ils auraient accumulé un butin de 2 milliards de dollars sur 1,5 million de victimes selon Bitdefender –, ont cessé de le mettre à jour. Les principes du chiffrement de GandCrab sont depuis connus. « Nous avons réussi à déchiffrer les données et, depuis, nous travaillons avec STLM pour que cela ne se reproduise pas », explique Pierre Lorcy, à la tête de la petite équipe de Lorcyber. Mais, entre le prix des prestations des experts et les pertes liées au gel de l'activité, le coût de l'attaque pour la PME s'élève à plusieurs milliers d'euros.

UN RISQUE VITAL

Le CHU de Rouen a lui été frappé le vendredi 15 novembre 2019. Peu avant 20 heures, l'équipe informatique repère un rançongiciel, le chiffrement des données se propage. Elle décide d'éteindre d'urgence tout le système informatique. Une procédure grave pour cet hôpital comptant 10 000 salariés et 2 500 lits, qui a vu son activité réduite au minimum pendant plusieurs jours. Même le téléphone entre les services était coupé, impossible également d'accéder aux dossiers médicaux des patients aux urgences. Dans le week-end, 50 experts de l'Anssi (Agence nationale de la sécurité des systèmes d'information) ont été dépêchés sur place. TA505 – auparavant connu sous le nom d'Evil Corp –,

BALTIMORE, VILLE PRISE EN OTAGE

Pendant plus de cinq semaines, les 15 000 ordinateurs municipaux de la ville de Baltimore, aux États-Unis, ont été pris en otage par des pirates informatiques et leur rançongiciel. Le 7 mai 2019, les 620 000 habitants se sont retrouvés d'un coup dans l'incapacité de payer leurs factures d'eau, leurs contraventions de stationnement ou encore leurs impôts locaux. Au moins 1 500 ventes immobilières ont été suspendues. Les agents municipaux se sont vus ce même matin privés de leur outil de travail. Ils n'avaient plus accès à leur messagerie électronique professionnelle. Un coup dur pour cette ville en grande difficulté. Baltimore est remontée de vingt ans dans le temps. La municipalité invitait ses administrés à se rendre aux permanences ou à la contacter par téléphone et à régler les amendes et factures d'eau en liquide, voire en chèque, moyen de paiement dont l'usage a grandement disparu des États-Unis. Le coût total pour la ville de Baltimore s'élève à plus de 18 millions de dollars, entre la remise en état du matériel et le préjudice financier lié à l'arrêt de l'activité, et en particulier de la facturation.

L'HUMANITÉ DIMANCHE

PAYS : France
PAGE(S) :40;41;42;43
SURFACE :213 %

PERIODICITE : Hebdomadaire
RUBRIQUE : Nos vies
JOURNALISTE : Pierric Marissal

▶ **6 février 2020 - N°694**

Attaqué par un rançongiciel, le CHU de Rouen éteint d'urgence tout son système informatique. Une procédure grave pour cet hôpital de 2500 lits, qui a vu son activité réduite au minimum pendant plusieurs jours.

organisation cybercriminelle la plus active du moment sur le secteur du rançongiciel, aurait exigé 1500 euros pour chacun des 6000 ordinateurs de l'hôpital, ce que ne confirme pas la direction de l'hôpital. « On a eu affaire à un attaquant qui voulait juste mettre la pression sur sa victime pour obtenir une rançon. Si on avait affaire à des attaquants beaucoup plus pervers, qui commencent à modifier des données d'analyses médicales, des dosages… il aurait pu y avoir des conséquences dramatiques, y compris pour la vie des personnes », s'alarmait, sur France Culture, le chef de l'Anssi, Guillaume Poupard.

L'agence a confirmé la forte activité de TA505 et de son programme baptisé Clop. Ils ont envoyé, depuis six mois, plusieurs centaines de millions d'e-mails contenant leur rançongiciel maison à destination des entreprises et des services publics d'une cinquantaine de pays. Le fondateur du groupe, Maksim Yakubets, un Russe d'origine ukrainienne, est devenu en décembre le cybercriminel le plus recherché au monde, le FBI offre désormais 5 millions de dollars pour toute information pouvant mener à sa chute.

« Ces criminels font évoluer leurs pratiques de manière constante, explique la lieutenante-colonelle Fabienne Lopez, commandante du Centre de lutte contre les criminalités numériques. Avant, en accompagnant les négociations, on réussissait à faire patienter les rançonneurs jusqu'à ce qu'on déchiffre leur programme et qu'on n'ait pas besoin de payer. Et puis, ils ont mis des ultimatums à 48 heures. Désormais, certains rançonneurs préfèrent menacer : si vous ne payez pas, on rend publiques les données. Les rançongiciels sont les fléaux d'aujourd'hui, et de demain. »

PIERRIC MARISSAL
pierric.marissal@humanite.fr

SE FAIRE PIRATER SA VOITURE, C'EST POSSIBLE

Armé de son ordinateur portable et d'un petit boîtier, Jérôme Blanchard pirate une voiture âgée de 7 ou 8 ans. Loin d'être malveillant, il finit son master 2 en « cybersécurité des systèmes embarqués » à l'université de Bretagne-Sud, qui développe un pôle d'excellence sur le domaine. Pour comprendre comment sécuriser les voitures, il faut aussi savoir les « hacker ». « Le plus dur est d'avoir un accès à distance au véhicule. Là je passe par le port de diagnostics, là où le garagiste vient brancher sa valise quand il y a un problème. Dans les voitures plus modernes, les interfaces de divertissement – GPS, autoradio, port d'accueil de smartphone… – constituent autant de portes d'entrée pour les pirates », explique-t-il.

Sur l'écran de son portable, des lignes de codes défilent. Chacune d'elles est une information : activation d'un clignotant, accélération, orientation du volant… « La voiture est contrôlée par des calculateurs, qui discutent en permanence. En analysant ces messages – comme ils ne sont pas cryptés –, on peut finir par en comprendre le sens. Et si je peux voir ces informations, je peux aussi en envoyer », explique le jeune homme. Joignant le geste à la parole, il propose un effet « sapin de Noël », allumant et éteignant successivement les phares et clignotants. Puis, à force de bombarder la voiture de messages, celle-ci sature, des messages d'erreur s'affichent sur le tableau de bord. « Toute l'électronique vient de tomber, note Jérôme Blanchard. On vient de faire un déni de service, j'ai envoyé tellement de requêtes que les informations vitales ne sont plus échangées, les calculateurs se sont mis en mode sécurité. Le conducteur garde la main sur la mécanique, mais n'a plus d'assistance au freinage, à la direction… C'est une attaque basique. D'autres plus subtiles permettent de tourner le volant, d'accélérer ou plus simplement de voler la voiture, mais cela prend plus de temps à mettre en place. »

Les constructeurs ont bien conscience de ces risques et commencent à intégrer des sécurités informatiques supplémentaires. Mais l'industrie automobile fonctionne sur un temps bien plus long que celui des pirates, il faut en moyenne quatre ans pour concevoir un véhicule.

Panique à bord ! Un pirate peut en théorie prendre le contrôle de votre volant, voire de votre accélérateur.

GETTY IMAGES/ISTOCKPHOTO