Chers clients,

Cela ne vous a probablement pas échappé, le monde a été frappé en fin de semaine dernière par une vague de cyber-attaques.

150 pays, du Mexique à la Russie en passant par l'Espagne et le Vietnam ont été victimes d'un ransomware ou "rançongiciel" dénommé WANNACRY.

Voici le mode de fonctionnement de ce type de logiciel

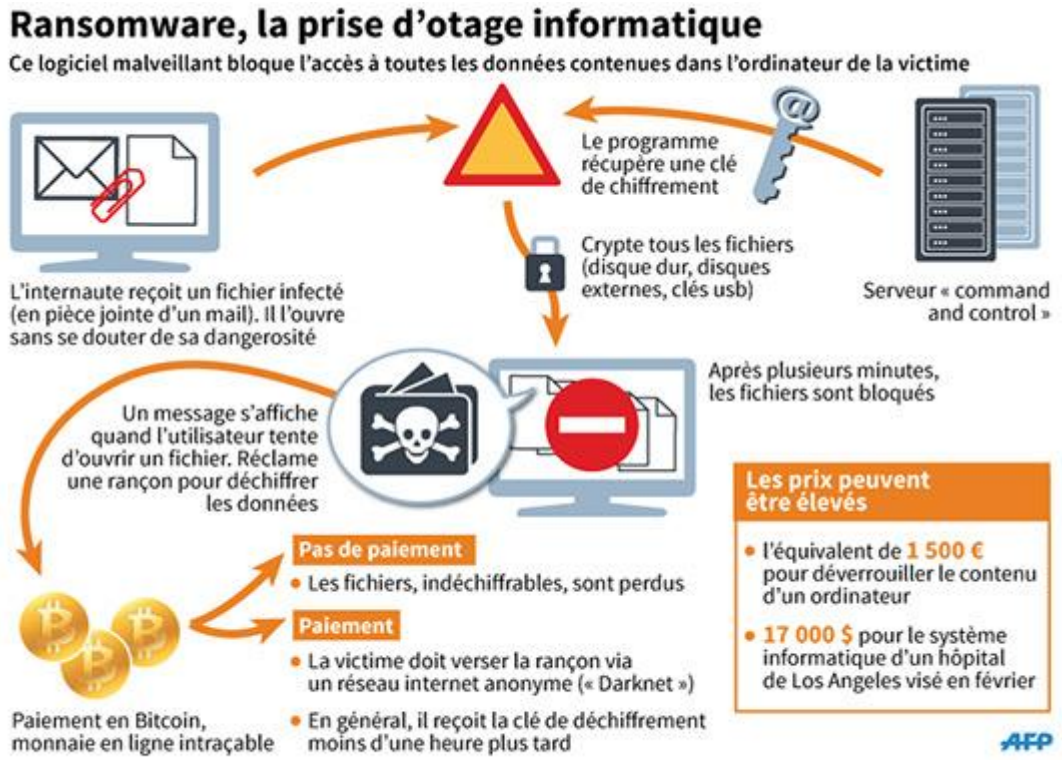

Schéma Récapitulatif du fonctionnement d'un Ransomware – Source AFP

Au sein de ces pays, des entreprises ont été touchées : le National Heath Service au Royaume-Uni, Fedex aux Etats-Unis, l'usine Renault à Douai... En France, les pirates ont envoyé pas moins de **350.000 courriels** à des entreprises de toutes tailles en vue de les piéger

Les « rançongiciels » (« ransomware » en anglais) promettent de libérer vos données contre le paiement d'une rançon. Quelques conseils pour se prémunir contre ce type d'attaques ou y faire face.

Une attaque informatique d'ampleur touche des dizaines de pays depuis vendredi, suscitant l'inquiétude des experts en sécurité. Elle est opérée à l'aide d'un logiciel malveillant appelé WCry, WannaCry, WanaCrypt0r, WannaCrypt ou Wana Decrypt0r. Voici quelques conseils pour lutter contre ces « ransomwares » (« rançongiciels » en français) qui promettent de libérer vos données contre le paiement d'une rançon.

POUR NE PAS ETRE IMPACTE

Ne pas cliquer sur n'importe quoi.

Avant toute chose, il est important de se méfier des e-mails suspects, ceux qui arrivent sans texte dans le corps du message notamment. Attention : ce n'est pas parce que l'adresse de l'expéditeur est connue qu'elle n'est pas usurpée.

Faire des sauvegardes.

Le meilleur moyen de ne pas s'arracher les cheveux en cas d'attaque et de faire le plus souvent possible des copies de ses données, sur des disques durs externes par exemple. Vous vous sentirez ainsi moins dépourvu le jour où un inconnu menace de ne pas vous rendre vos fichiers.

Mettre à jour les logiciels et les antivirus.

Les spécialistes conseillent de mettre à jour, dès que cela est proposé, son système d'exploitation, le lecteur PDF et les principales applications bureautique. Samedi après-midi, Microsoft a d'ailleurs réactivé la mise à jour de sécurité pour les utilisateurs qui ne l'avaient pas installée lors de sa première sortie. Mais aussi de se doter d'un antivirus sérieux, en y mettant le prix s'il faut, qui saura reconnaître les derniers programmes malveillants.

Si vous êtes touché...

Isoler le mal. Si vous travaillez en réseau, au sein d'une entreprise par exemple, il faut immédiatement déconnecter le matériel infecté du reste du réseau. Et alerter le chef du service informatique. Selon le rapport 2016 de Symantec, les entreprises représentent 43 % des cibles infectées (contre 57 % pour les particuliers). Une proportion qui ne cesse de croître.

Payer la rançon ? Les menaces peuvent impressionner. Dans le cas de WCry, on jure que si l'argent n'est pas versé dans les sept jours les fichiers piratés sont effacés. Mais, prévient l'ANSSI, « le paiement ne garantit en rien le déchiffrement de vos données ». Selon une étude du spécialiste japonais de la cybersécurité Trend Micro, 50% des entreprises françaises infectées paient la rançon, sans pour autant récupérer leurs fichiers. De plus, les données bancaires ainsi renseignées peuvent être utilisées par la suite.

LES CYBER-RISQUES POUR LES ENTREPRISES

L'hôpital américain Hollywood Presbyterian Medical Center en Californie a récemment été paralysé pendant une semaine entière suite au piratage d'un groupe de hackers malveillants.

L'établissement a été victime d'une « ransomware », une attaque informatique ciblant tout particulièrement les entreprises. Pour surmonter le chaos engendré par le virus informatique à cause duquel le personnel n'avait plus accès aux données des patients, l'hôpital n'a pas eu d'autre choix que de s'acquitter d'une rançon de 17 000 dollars.

Cette situation redoutable pourrait se reproduire ailleurs. Les hôpitaux français sont aujourd'hui tout aussi vulnérables face à ce type de menace. La sécurité des systèmes d'information de nos entreprises et institutions n'est pas toujours au point face à ces attaques sophistiquées. Au mois de janvier dernier, c'est le ministère des transports qui était attaqué par des cybercriminels.
Face à ces nouveaux risques, du vol de données à la paralysie d'un site web, les assureurs proposent des solutions pour compenser les préjudices subis : coûts de l'intervention technique interne ou externe, dommages-intérêts dus aux clients, pertes d'exploitation.

Les pirates ont utilisé une faille découverte par les services de renseignement américains. 150 pays ont été touchés. En France, où Renault a été contraint d'arrêter la production de certains sites, le parquet a ouvert une enquête.

Enquêteurs et experts informatiques internationaux traquaient toujours dimanche les pirates informatiques à l'origine de la cyberattaque mondiale "sans précédent", qui pourraient frapper à nouveau dans les jours à venir.

On évoque désormais « 200.000 victimes dans au moins 150 pays » visés par les pirates informatiques et de nombreuses entreprises ou services publics reconnaissaient avoir été

touchés, ou avoir fait l'objet d'attaques. Mais il faudra attendre suite à ce WE la réouverture des entreprises pour dresser un bilan plus complet de cette attaque.

Une faille de Windows découverte par la NSA

Les pirates ont apparemment exploité une faille dans les systèmes Windows, divulguée dans des documents piratés de l'agence de sécurité américaine NSA. Ce qui a donné l'occasion à Edward Snowden de fustiger un peu plus son ancien employeur.

« Si la NSA avait discuté en privé de cette faille utilisée pour attaquer des hôpitaux quand ils l'ont 'découverte', plutôt que quand elle leur a été volée, ça aurait pu être évité », a regretté sur Twitter Edward Snowden, l'ancien consultant de l'agence de sécurité américaine qui avait dévoilé l'ampleur de la surveillance de la NSA en 2013.

Peu d'utilisateurs ont utilisé le correctif publié au printemps par Microsoft

Peu après que cette faille ait été rendue publique, Microsoft a publié une correction pour éviter les attaques, mais nombre de systèmes n'ont visiblement pas été mis à jour par leurs utilisateurs, ce qui a été mis à profit par les pirates qui ont vu grand et rédigé leur demande de rançon (celle qui apparaît sur l'écran des victimes et le bloque) en 17 langues.

Et le géant informatique américain n'a pas manqué, dès vendredi de publier une longue note destinée à expliquer comment se protéger plus particulièrement des attaques liées à WANNACRYPT. Y soulignant notamment la mise à disposition d'une mise à jour de Windows Defender, le système maison de protection contre les logiciels malveillants.

De même, selon Microsoft, les utilisateurs dont les machines tournent sous Windows 10 ne seraient pas l'objet d'attaques.

« Contrairement à des virus normaux, ce virus se répand directement d'ordinateur à ordinateur sur des serveurs locaux, plutôt que par email », a précisé Lance Cottrell, directeur scientifique du groupe technologique américain Ntrepid. « Ce logiciel de rançon peut se répandre sans que qui que ce soit ouvre un email ou clique sur un lien ».

Plus de 200.000 attaques

Le logiciel utilisé par les pirates verrouille les fichiers des utilisateurs et les force à payer une somme d'argent sous forme de bitcoins pour en recouvrer l'usage. Une pratique, appelée "ransomwares" et qui devient de plus en plus courante.

« 200.000 victimes dans au moins 150 pays » (directeur Europol) : tel est le dernier bilan, dimanche à la mi-journée.

Les experts étaient restés très prudents samedi sur l'expansion du virus :
"On ne sait pas encore si on est sur une pente ascendante ou descendante", a expliqué à l'AFP Laurent Maréchal, expert en cybersécurité chez McAfee.

Des attaques repoussées en Russie

En Russie MegaFon, ou la banque Sberbank avaient indiqué avoir été attaqués. Samedi, la banque centrale russe a annoncé qu'elle avait détecté des attaques informatiques "massives" contre des banques russes qui avaient réussi à les contrecarrer. La presse russe indique par ailleurs que la société des chemins de fer nationaux a été prise pour cible de ces attaques mais qu'elle est également parvenue à les repousser.

Arrêts de production chez Renault

Outre Fedex, plusieurs autres entreprises ont indiqué avoir été touchées ou avoir fait face à des problèmes. Ce samedi le constructeur automobile français Renault a indiqué faire partie des victimes. "Nous avons été touchés", a indiqué une porte-parole du groupe, en précisant que le constructeur était en train d'analyser la situation. "Une action est en place depuis hier (vendredi) soir. On fait le nécessaire pour contrer cette attaque", a-t-il précisé.

Des problèmes ont nécessité la mise à l'arrêt de certains sites de production dont celui de Sandouville en France, mais aussi en Slovénie où la filiale du constructeur, Revoz, a arrêté la production d'une de ses usines

Selon l'Agence nationale de la sécurité des systèmes d'informations (Anssi), Renault serait la seule victime française répertoriée. Mais, il est "probable qu'il y ait d'autres victimes en France", même si ces dernières ne sont pas connues, explique Guillaume Poupart, directeur général de l'Anssi. Et d'ajouter, en ironisant sur l'accident de Tchernobyl et de son nuage radioactif, qu'"il n'y a pas de raison que le nuage se soit arrêté aux frontières" de l'Hexagone.

De nombreux services publics touchés

La liste des pays touchés est particulièrement longue et les spécialistes n'ont guère de doute sur le fait que tous les incidents recensés sont liés. Et ce d'autant plus que dans de nombreux cas, les mêmes messages, contenant une demande de rançon de 300 dollars payables en bitcoins sont apparus sur les écrans des victimes.

Des organisations publiques, des entreprises ont ainsi été touchées aux Etats-Unis (où le géant de livraison de colis FEDEX a reconnu avoir été infecté) et au Royaume-Uni mais aussi en Espagne, en Australie, en Belgique, en France, en Allemagne, en Italie, au Mexique, en Chine, en Ukraine ou bien encore à Taïwan.