L'Echo

La cybercriminalité, "un défi plus grand que le terrorisme"

15 mai 2017 10:37

L'attaque informatique d'une ampleur mondiale qui a déjà touché 200.000 victimes dans 150 pays continue encore de s'accroître ce lundi alors que des millions d'ordinateurs professionnels sont rallumés en ce premier jour de semaine. En Belgique, la Justice estime que la cybersécurité devient un plus grand défi, "plus grand que le terrorisme", selon le procureur fédéral Frédéric Van Leeuw.

La cyberattaque sans précédent qui a touché plus de **200.000 victimes** dans au moins **150 pays** depuis vendredi alimente la crainte d'un "*cyberchaos*", les experts redoutant une recrudescence du virus ce lundi alors que des millions d'ordinateurs sont rallumés, en Asie notamment.

Microsoft de son côté a averti les gouvernements dimanche contre la tentation de cacher des failles informatiques qu'ils auraient repérées, comme cela a été fait dans le cas de cette attaque, où la brèche dans le système Windows utilisée par les pirates avait été décelée depuis longtemps par la NSA (L'agence de sécurité nationale américaine) avant de tomber dans le domaine public via des documents piratés au sein de la NSA elle-même.

"*Les gouvernements devraient voir cette attaque comme un signal d'alarme*", a insisté Brad Smith, le directeur juridique de Microsoft, dans un blog: "*Un scénario équivalent avec des armes conventionnelles serait comme si l'armée américaine se faisait voler des missiles Tomahawks*".

En attendant d'éventuelles nouvelles victimes, le bilan de cette cyberattaque mondiale est déjà imposant.

"*Le dernier décompte fait état de plus de 200.000 victimes, essentiellement des entreprises, dans au moins 150 pays. Nous menons des opérations contre environ 200 cyberattaques par an, mais nous n'avions encore jamais rien vu de tel*", a déclaré dimanche le directeur d'Europol, **Rob Wainwright**, à la chaîne de télévision britannique ITV.

"Rançongiciel"

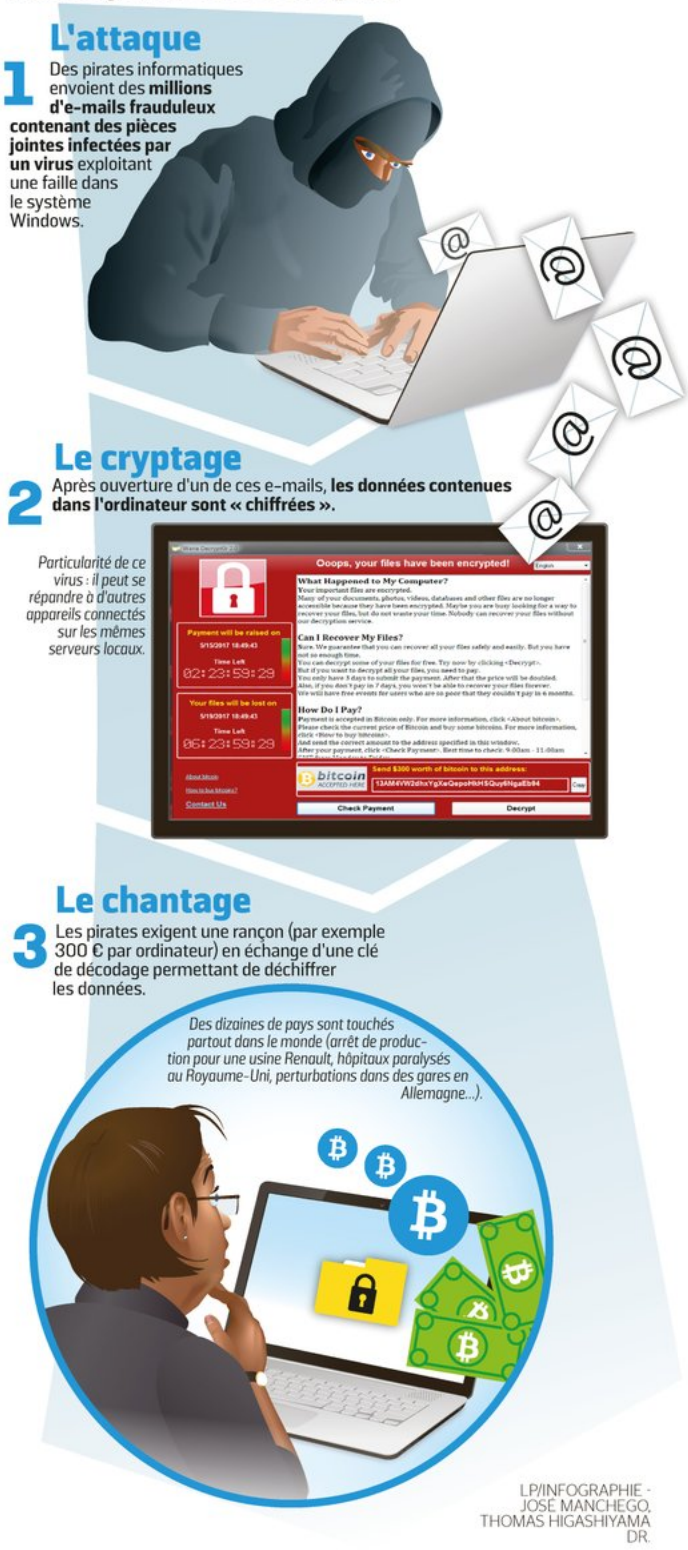
Le patron d'Europol, qui avait annoncé dimanche craindre **une augmentation du nombre de victimes** "*lorsque les gens retourneront à leur travail lundi et allumeront leur ordinateur*", après un dimanche plutôt calme, a vu juste. Des autorités et entreprises en Chine, mais aussi en Japon, en Inde ou encore en Indonésie ont déjà fait part de nouvelles attaques ce lundi (développement complet en fin d'article).

"*A partir du moment où l'échelle est très grande, on peut se demander si le but recherché est le cyberchaos*", s'interrogeait **Laurent Heslault**, directeur des stratégies de sécurité chez la société de sécurité informatique Symantec.

De la Russie à l'Espagne et du Mexique au Vietnam, des centaines de milliers d'ordinateurs, surtout en Europe, ont été infectés depuis vendredi par un logiciel de rançon, un **"*rançongiciel*" exploitant une faille dans les systèmes Windows**. Ce logiciel malveillant verrouille les fichiers des utilisateurs et les force à payer 300 dollars (275 euros) pour en recouvrer l'usage. La rançon est demandée en monnaie virtuelle **bitcoin**, difficile à tracer.

Selon Rob Wainwright, qui ne donne pas de chiffre, "*il y a eu étonnamment peu de paiements jusque-là*". La société de sécurité informatique Digital Shadows a fait état dimanche d'un montant total de **32.000 dollars**

versés. "*Payer la rançon ne garantit pas la restitution des fichiers*", a de son côté mis en garde le département américain de la Sécurité intérieure.



Le Parisien Infog
@LeParisienInfog

Follow

Tout comprendre sur la cyberattaque mondiale >>
l.leparisien.fr/s/M5U7 #CyberAttack

10:25 AM - 14 May 2017

20 11

L'attaque a affecté les **hôpitaux britanniques**, le constructeur automobile français **Renault**, **le système bancaire russe**, le groupe américain de logistique **FedEx**, la compagnie de télécoms espagnole **Telefonica** ou encore des universités en Grèce et en Italie.

Europol, qui estime qu'aucun pays en particulier n'a été visé, a insisté sur la rapidité inédite de la propagation de ce virus "***Wannacry***", qui combine pour la première fois les fonctions de logiciel malveillant et de ver informatique.

"*Il a commencé par attaquer les hôpitaux britanniques avant de se propager rapidement à travers la planète. Une fois qu'une machine est contaminée, le virus va scanner le réseau local et contaminer tous les ordinateurs vulnérables*", a expliqué le porte-parole d'Europol, Jan Op Gen Oorth.

Selon la ministre britannique de l'Intérieur, Amber Rudd, dans une tribune au Sunday Telegraph, il faut désormais s'attendre à d'autres attaques. Et on ne "*connaîtra peut-être jamais la véritable identité des auteurs*" de celle en cours, a-t-elle ajouté.

Un surfeur pour 'sauveur'

Le chercheur en cybersécurité britannique de 22 ans qui a permis de ralentir la propagation du virus a également prévenu que les pirates risquaient de revenir à la charge en changeant le code, et qu'ils seraient alors impossible à arrêter.

"*Vous ne serez en sécurité que lorsque vous installerez le correctif le plus rapidement possible*", a-t-il tweeté sur son compte @MalwareTechBlog.

Ce jeune chercheur britannique, qui souhaite rester anonyme, a été qualifié de "*héros*" qui a "sauvé le monde" par la presse. Le Mail on Sunday britannique a retrouvé une photo du jeune homme, surfeur à ses heures perdues, qui vit encore chez ses parents dans le sud de l'Angleterre.

Pour contrer l'attaque, **Microsoft** a de son côté réactivé une mise à jour de certaines versions de ses logiciels. Le virus s'attaque notamment à la version Windows XP, dont Microsoft n'assure plus en principe le suivi technique. Le nouveau logiciel d'exploitation (OS) Windows 10 n'est pas visé.

"*Il est très difficile d'identifier et même de localiser les auteurs de l'attaque. Nous menons un combat compliqué face à des groupes de cybercriminalité de plus en plus sophistiqués qui ont recours à l'encryptage pour dissimuler leur activité. La menace est croissante*", a souligné le patron d'Europol, Rob Wainwright.

La cyberattaque continue de sévir en Asie

"*La plupart des attaques arrivent par courriel, aussi y a-t-il de nombreux 'champs de mine' qui attendent dans les boîtes de réception des gens*", estime Michael Gazeley, directeur d'une société hongkongaise de cybersécurité, Network Box. Michael Gazeley a ajouté que ses services avaient découvert une nouvelle version du "*vers*", qui n'attire pas les victimes par des e-mails malveillants. Au lieu de cela, il charge des scripts dans les

sites internet piratés, où les usagers qui cliquent sur un lien malveillant voient leurs ordinateurs directement infectés.

- **En Chine**, le géant de l'énergie PetroChina a annoncé ce lundi que les systèmes de paiement de certaines de ses stations-service avait été touchés, mais a ajouté avoir réussi à restaurer la plupart d'entre eux. Plusieurs acteurs gouvernementaux chinois, notamment la police et les autorités chargées de la circulation, ont dit avoir été affectés, selon des billets publiés sur des plate-formes de micro-blogging officielles. Le journal en langue anglaise China Daily a annoncé qu'au moins 200.000 ordinateurs avaient été infectés en Chine, en particulier dans des écoles et des universités, d'après des estimations de la société technologique chinoise Qihoo 360. Tous les systèmes de **la Bourse de Hong Kong** fonctionnent normalement, a déclaré un porte-parole de la place financière, l'une des plus importantes de la région.

- **Au Japon**, la police nationale a signalé que les cyberattaques avaient touché dimanche un hôpital et un particulier. Le conglomérat industriel Hitachi a déclaré quant à lui que la cyberattaque avait affecté dans une certaine mesure ses systèmes au cours du week-end, les usagers ne pouvant plus, dans certains cas, recevoir ni envoyer de courriels, ni ouvrir les pièces jointes. Le problème n'était toujours pas résolu lundi, a ajouté le conglomérat.

- **En Inde**, le gouvernement dit n'avoir été informé que de quelques attaques contre des systèmes informatiques et a exhorté ceux qui étaient touchés à ne verser aucune rançon. Aucune grand groupe indien n'a signalé de perturbation de ses activités. De manière générale, les entreprises ont demandé à leurs employés de ne pas cliquer sur les pièces jointes, ni sur les liens transmis par des courriels suspects.

- Une école **en Corée du Sud** a interdit à ses élèves de se rendre sur internet. **Le gouvernement taïwanais** semble avoir échappé à l'infection, notamment grâce à des règles obligeant tous les services de l'Etat à installer les mises à jour informatiques à mesure qu'elles deviennent disponibles. Microsoft a réactivé le mois dernier et vendredi une mise à jour permettant de réparer la faille qui a permis au virus de se disséminer dans les réseaux La présidence sud-coréenne a annoncé lundi que neuf cas d'infection avait été détectés dans le pays, sans fournir davantage de précision.

- **En Australie**, seules trois entreprises ont été affectées, tandis que **la Nouvelle-Zélande** semble avoir complètement échappé au virus.

- **En Indonésie**, le plus grand centre de soins anti-cancer, l'hôpital Dharmais de la capitale Djakarta, a vu plusieurs dizaines de ses ordinateurs touchés par les cyberattaques, ce qui a occasionné des retards dans le traitement des patients.

Source: AFP