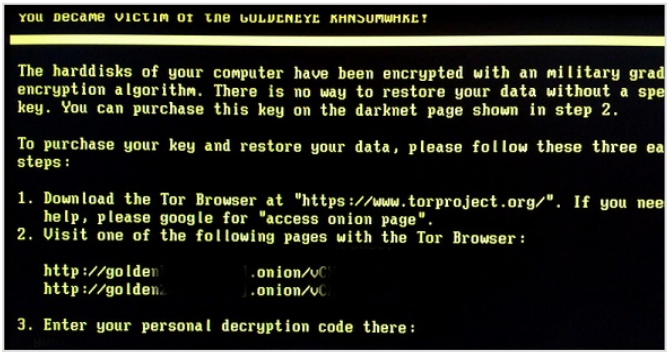
Cyber-attaque : L’austérité et la surveillance de masse responsables !



Déclenchée depuis vendredi, à l'heure où nous écrivons ces lignes, ce sont plus de 200 000 systèmes impactés et 150 pays concernés par le même piratage informatique ; on compte tout aussi bien des particuliers, des entreprises ou des services publiques. L'histoire de ce piratage traîne dans son sillage les maux la période et les pratiques calamiteuses des Etats.

Le procédé n'est en soi pas nouveau, on parle de virus type "ransomware" (ou rançongiciel) nommé WanaCrypt0r (WCry pour les intimes) ; le programme vise à chiffrer les données utilisateurs afin de les rendre inaccessibles, même à l'usage d'un système d'exploitation non-infecté, puisqu'il faut une clé de déchiffrement, détenu par les pirates seuls, qu'ils disent être prêt à échanger contre paiement. La nouveauté c'est qu’il s’agit d’une attaque à grande échelle. Un scénario déjà esquissé dans la première saison de la série *Mr. Robot* avec des intentions anticapitalistes bien plus honorables que les fins crapuleuses poursuivis dans cette version réelle.

La NSA première fautive !

En premier lieu, les velléités de la NSA au contrôle des flux de données numériques. Au delà des révélations Snowden sur l'espionnage des réseaux en masse, ce sont ici d'autres pratiques qui sont mises en lumières : la captation par la NSA de failles de sécurité de programmes ou systèmes, scellées dans le secret, et divulguées au cas par cas aux éditeurs de ces programmes en fonction de critères que maîtrisent l'agence. Cette non-divulgation était déjà dénoncée depuis plusieurs mois par des collectifs citoyens, des journalistes, des entreprises[1]... qui revendiquaient la publication de ces failles afin de garantir la fiabilité et la sécurité des systèmes d'information et des usages des particuliers.

Ces informations ont finalement été retirées par la force à la NSA. Dans un premier temps, un groupe se faisant nommé The Shadow brokers a capté puis tenter de vendre les outils de hacks utilisés par la NSA l'été dernier. Ensuite, les révélations nommées Vault 7 publiées sur Wikileaks en mars qui sont une série de documents détaillant les activités de la CIA dans le domaine de la surveillance, et qui comportaient moults détails concernant les failles de sécurité, tout systèmes informatiques confondus. Conscient des problématiques de sécurités, Wikileaks fit, à l'occasion, une entorse à ses habitudes de publications à la volé, et publia en premier lieu les informations devenues "obsolètes" du fait des corrections et mises à jour déjà en place. De plus, Wikileaks

transmit aux éditeurs informatiques les informations de failles jusque là demeurées inconnues (les failles dites "zéro day") afin qu'ils préparent les patchs correctifs et de sécurité. Une fois, les failles corrigées, Wikileaks les rendit publiques.

C'est l'une des ces fameuses failles (identifiée sous le bulletin de sécurité de Microsoft MS17-010) qui a été utilisée pour le piratage massif. Suite au piratage de la NSA rendant cette faille publique, Microsoft proposait le correctif dès le 14 mars. Son application ou pas étant de la responsabilité des organisations comme des individus, bon nombre d'ordinateurs comprenant un système Microsoft comportant cette faille n'ont pas été mis à jour.

Les dangers des politiques d'austérités à l'oeuvre

Si l'importance et la renommée des entreprises impactées ont souvent été citées (FedEx, Renault...), ce qui a été systématiquement présenté dans les médias, c'est la paralysie du NHS, le système public de santé du Royaume Uni, avec des médecins annulant des interventions à la dernière minute, des ambulances désorganisées et difficiles à coordonner. Dans ces entreprises et ces services, il s'agit d'une responsabilité relevant de la DSI (direction des systèmes d'information) et de sa politique de mises à jours des systèmes. Or au NHS, la mise à jour n'était même pas envisageable, puisque dans un souci d'économie et de réduction des budgets, et selon des chiffres de décembre 2016, l'environnement informatique serait resté à 90% sous Windows XP alors que ce système n'est plus supporté par Microsoft, qu'il ne reçoit plus de correctif ni de mise à jour de sécurité depuis 3 ans.

Outre le combat contre l'austérité et contre le capitalisme qui en est la source, il y a la nécessité de se défendre contre les politiques et systèmes de contrôle qu'ils soient mis en place par un gouvernement ou par les entreprises. Pour cela, l'ouverture et l'accès des codes sources de tous les programmes est nécessaire pour se prémunir des comportements indésirables et pour résoudre plus largement les problèmes de sécurités. Ceci permettrait aussi de lutter contre l'affaiblissement technique de chiffrement, contre l'installation de backdoor. Bien évidemment, il faut aussi démanteler les agences de renseignement et d'espionnage de masses.

---

[1] : L'exemple dernièrement de Mozilla : https://www.nextinpact.com/news/99834-to--browser

Frédérick Lorie, le 19 mai 2017