Petya : 5 questions pour comprendre le ransomware qui terrorise les entreprises

Les premières analyses de l'infection par ransomware qui, une nouvelle fois, a fait le tour de la planète hier montre que les assaillants peuvent se contenter d'accommoder de vieilles recettes pour créer des menaces capables de mettre des entreprises entières au chômage technique. En croisant les sources disponibles à ce stade, *Silicon.fr* décortique le fonctionnement de ce nouveau ransomware, une variante de Petya, un malware connu depuis 2016.

1) L'infection initiale

Plusieurs sources, dont Microsoft et Kaspersky, pointent désormais en direction de M.E.Doc, un éditeur ukrainien qui développe un logiciel de gestion des taxes, MeDoc. Selon Microsoft, qui affirme détenir des preuves, c'est le système de mise à jour de cet éditeur qui a été compromis hier, aux environs de 10h30, via une ligne de commande aboutissant à l'installation d'une variante du ransomware Petya. Notons que M.E.Doc nie pour l'heure être à l'origine de l'infection.

Ce point de départ est-il suffisant pour expliquer la diffusion mondiale de la souche Petya ? C'est une des questions qui reste discutée à ce stade. L'infection par MeDoc peut très bien expliquer certaines contaminations de groupes de taille mondiale : la compagnie maritime Maersk, n°1 mondial, utilisait par exemple ce logiciel dans sa filiale en Ukraine et le système était connecté à son siège au Danemark. Mais certains pensent que le malware s'est également déployé via de classiques e-mails piégés, renfermant des documents Office exploitant une faille de la suite bureautique dévoilée en avril dernier (la faille dite HTA).

2) La diffusion sur le réseau local

Plus que l'infection initiale, c'est la diffusion de la menace au sein des réseaux locaux des entreprises qui rend le nouveau ransomware particulièrement dangereux. Comme Wannacry, Petya a recours à la faille SMB de Windows dévoilée via la mise au jour des exploits EternalBlue et EternalRomance de la NSA. Une faille que Microsoft a corrigée sur tous ses systèmes, y compris ceux n'étant plus officiellement supportés. Après la crise mondiale créé par Wannacry, voir des systèmes, particulièrement du côté bureautique (là où Petya a fait le plus de victimes), encore vulnérables peut paraître surprenant.

« *Mais il est probable que la faille SMB ne soit pas le vecteur principal de propagation* », explique Vincent Nguyen, le directeur du CERT de Wavestone, le centre de réponse aux incidents du cabinet de conseil. Car Petya renferme une autre fonction redoutable : la récupération de codes d'accès à d'autres machines ou services directement dans la mémoire de Windows. Un fonctionnement qui rappelle celui d'un utilitaire utilisé par les experts en sécurité : Mimikatz. D'ailleurs, selon Microsoft, des parties du code source de ce dernier sont bien embarquées dans Petya. Si, par chance, le malware se déploie sur une machine ayant des droits d'administration élevés, c'est le jackpot. Car ces sésames en main, la souche va scanner le réseau local et utiliser des services légitimes de Windows (PSEXEC et WMIC) pour tenter d'exécuter à distance le malware sur les systèmes auxquels elle a accès. En somme, cette menace « *adopte le comportement d'un ver, capable d'aller infecter jusqu'au*

réseau de partenaires de l'entreprise initialement touchée », résume Vincent Nguyen. Spécialiste de virologie informatique, et en particulier des ransomwares, le chercheur de l'Inria Jean-Louis Lanet souligne que l'alliance d'un outil de type Mimikatz et du ransomware était redoutée depuis quelques temps par les spécialistes : « *le ransomware devient alors un vecteur d'infection en lui-même* ».

3) La charge utile

Une fois installé sur un poste ou un serveur, Petya ajoute au système une tâche programmée (au minimum 10 minutes ou une heure plus tard, selon les sources). Le malware modifie le Master Boot Record (le secteur de démarrage du disque dur) afin de lancer, après un reboot, le chiffrement et afficher ensuite la demande de rançon. Environ 60 extensions de fichiers sont visées par l'opération d'encodage, menée avec une clef AES propre à chaque machine, et Petya tente également de réécrire le MBR, afin d'empêcher les tentatives de récupération de données à partir d'un autre système.

Pendant le chiffrement, un faux message d'alerte s'affiche, expliquant qu'une opération de réparation du disque est en cours. Une façon de dissuader les utilisateurs de débrancher leur machine. Puis l'écran affiche une demande de rançon (l'équivalent de 300 $ par poste, en bitcoin).

4) Un feu de paille ?

Peut-être plus encore que Wannacry, la crise déclenchée par Petya a été extrêmement soudaine. Démarrée aux environs de 10h45 en Ukraine, elle a touché la France en début d'après-midi, hier. Et les experts avec qui nous avons pu échanger sur le sujet confirment qu'à l'intérieur d'une organisation, l'infection est souvent à la fois massive et soudaine, touchant des centaines, voire des milliers de machines en quelques minutes. Par contre, la crise semble se résorber d'elle-même. Comme l'écrit MalwareTech, le jeune chercheur britannique qui s'était fait un nom en découvrant le Kill Switch de Wannacry (un domaine permettant de désarmer la menace), une heure après l'attaque, le risque de nouvelle infection devient faible, le malware ayant déjà effectué son scan de réseau et ayant chiffré les machines vulnérables. « *Ce matin, nous n'assistons pas à de nouveaux déclenchements de crise chez nos clients*, confirme Vincent Nguyen. *Comme Petya détruit l'ensemble des postes qu'il infecte, il n'a plus de moyen de rebond.* »

5) Les antivirus dans les choux ?

Même si certains éditeurs de solutions assurent que leurs technologies ont stoppé la menace Petya (c'est le cas de Kaspersky), force est de constater que, quand il est parvenu à s'immiscer dans des organisations, Petya a fait de gros, de très gros dégâts même. Poussant des entreprises comme Saint-Gobain mais aussi WPP à renvoyer des contingents entiers de salariés chez eux. « *Les entreprises qui ont été touchées disposaient bien d'outils de protection*, relève Vincent Nguyen, de Wavestone. *Aujourd'hui (le 28 juin, NDLR), ces outils sont efficaces contre Petya, mais hier à la même heure, ce n'était pas encore le cas.* » Pour Jean-Louis Lanet (Inria), le chiffrement par Petya du MBR constitue pourtant une signature « *assez simple à détecter* ». Preuve probablement que les moteurs d'analyse comportementale des solutions de protection des postes de travail, censées détecter des menaces nouvelles via leurs comportements suspects, ont encore bien des progrès à faire…

A lire aussi :

Le ransomware GoldenEye infecte plusieurs entreprises, dont Saint-Gobain

WannaCry : le ransomware qui n’a plus besoin du phishing

Jean-Louis Lanet, Inria : « si le ransomware parfait existait… »