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

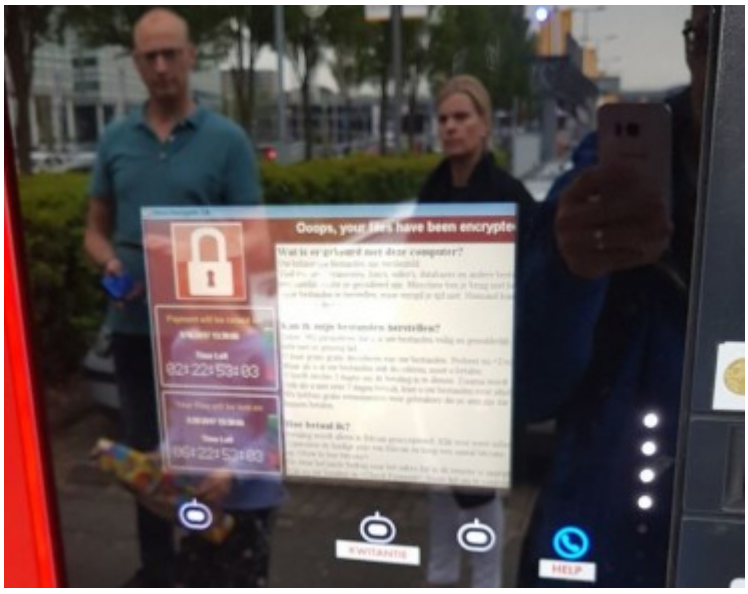
Une énorme confusion. La vague d'infection WannaCry a déclenché un bruit médiatique rarement atteint pour une cyberattaque. A tel point que de multiples versions ont circulé sur la nature précise de cette menace. L'une des questions principales qui demeurent en suspens est celle de la primo-infection. De ce que, par analogie avec la médecine, on appelle le patient zéro. Pour schématiser, deux thèses circulent. L'une explique que WannaCry a eu recours au phishing pour pénétrer dans les entreprises, la seconde estime que le malware est directement injecté aux machines vulnérables repérées sur Internet.

Ce week-end, la majorité des analyses sur WannaCry décrivait un malware s'introduisant dans les entreprises via un mail infecté – bref une opération de phishing -, puis se diffusant sur le réseau de l'organisation ciblée via ses fonctionnalités de ver, en exploitant la faille SMB de Microsoft. Une faille qui, rappelons-le, a été exposée au grand jour via des kits d'exploits dérobés à la NSA par un mystérieux groupe de hackers, les Shadow Brokers.

Mais cette version basée sur le phishing est contestée. « *Tout le monde cherche ce fameux e-mail initial et, en quatre jours, aucune équipe n'est parvenue à mettre la main dessus* », remarque Vincent Nguyen, le directeur du CERT de Wavestone, le centre de réponse aux incidents du cabinet de conseil. Selon lui, les assaillants scannent plutôt Internet à la recherche de machines exposées, des systèmes Windows sur lesquels les patchs proposés par Microsoft (y compris pour Windows XP et Windows Server 2003 depuis vendredi dernier) n'ont pas été appliqués et où le service SMB est accessible (via le port 445). Une version que corrobore l'expérience d'un chercheur qui, après avoir placé un honeypot pour WannaCry sur Internet ce week-end, a constaté que celui-ci était infecté en moins de trois minutes.

Conficker reloaded

« *On retrouve ici un mode de diffusion à la Conficker* », résume Gérôme Billois, senior manager en gestion des risques et sécurité de Wavestone, en référence à un ver apparu en 2008 et exploitant une autre faille massive de Windows. Pour cet expert, les environnements les plus exposés sont les systèmes de contrôle industriels et les systèmes métiers très particuliers. Des systèmes sur lesquels les entreprises n'appliquent pas les correctifs de peur de se heurter à une incompatibilité et qui sont souvent animés par des OS antédiluviens. Ce n'est



d'ailleurs pas un hasard si, parmi les systèmes touchés, on retrouve des écrans de contrôle dans des gares (Deutsche Bahn), des environnements exploités dans la santé (le NHS britannique), des robots industriels (Renault) ou encore des automates bancaires. « *Le premier conseil est bien-sûr de déployer les patchs, mais les entreprises ont aussi la possibilité de désactiver le service SMB* », dit Gérôme Billois.

Pour Quentin Gaumer, le directeur de l'activité cybersécurité, audit et compliance de Devoteam, un prestataire qui, lui aussi, dispose d'un CERT, le tableau n'est pas aussi simple. « *Des clients nous ont transféré des mails de phishing qu'ils ont reçus* », assure-t-il, précisant toutefois que l'étude de l'attaque est encore en cours. Selon lui, la primo-infection par phishing permet de bypasser les défenses périmétriques des entreprises. « *Cette première barrière passée, nos audits montrent que la sécurité en profondeur est en réalité peu présente dans la plupart des organisations* », ajoute Quentin Gaumer. Mais, pour ce dernier, ce mode d'infection a très bien pu cohabiter avec une infection directe, via le repérage de machines exposées sur Internet.

Fermer le port 445 : insuffisant ?

D'où son ensemble de recommandations. Qui démarrent par l'application des patchs mis à disposition par Microsoft en mars et vendredi dernier pour les systèmes qui n'étaient plus supportés. « *Les clients brandissent souvent les problèmes de régression que l'application de ceux-ci génèrent. Mais, en réalité, cela arrive de moins en moins, du fait des efforts des éditeurs pour développer des correctifs qui n'impactent pas les systèmes* », analyse Quentin Gaumer. Sans oublier évidemment de fermer le port 445 (celui qu'exploite SMB) sur le firewall. « *De toute façon, le laisser ouvert n'est pas normal*, ajoute l'expert. *Mais cette précaution seule ne suffit pas si l'infection arrive par mail.* » Et de recommander de fermer aussi le service SMB sur le réseau local s'il n'est pas utilisé pour le partage de fichiers ou d'imprimantes. Ce qui serait de plus en plus le cas, les entreprises préférant se tourner de plus en plus vers des technologies Web pour ces fonctionnalités.

In fine, pour les experts, WannaCry ne recèle aucune réelle innovation technique, et se contente d'agréger des procédés connus. Mais la menace se distingue avant tout par sa portée et sa soudaineté, avec des centaines de milliers de systèmes Windows infectés en un week-end. « *Les assaillants ont probablement mené un gros travail de préparation, avec un scan exhaustif des réseaux afin de repérer les machines exposées. On est très proche du cycle habituellement mis en œuvre par un service de renseignement, avec une première phase dédiée à la cartographie et à l'étude* », relève Quentin Gaumer. Contrairement à la plupart des attaques connues, WannaCry semble également ne pas avoir fait l'objet de phases de tests, utilisées d'habitude par les cybercriminels pour affiner le code de leurs malwares.

L'efficacité des outils de la NSA démontrée

Pour l'heure, selon les experts interrogés, la menace est en régression rapide, confirmant les données compilées par le chercheur en sécurité MalwareTech. Un coup d'arrêt qui doit beaucoup à la découverte par ce dernier d'un domaine dont la présence sur Internet suffit à annuler l'infection (en jargon un Kill Switch). Découverte par hasard par MalwareTech, cette fonction a permis de juguler la diffusion de la version initiale de WannaCry. Puis celle d'une réplique utilisant un second

domaine comme Kill Switch. « *Pour éviter toute infection par ces deux souches, il faut donc s'assurer que les deux domaines correspondant aux Kill Switch soient bien accessibles depuis le réseau de l'entreprise et modifier les DNS en conséquence* », précise Gérôme Billois.

Ce qui ne signifie pas, pour autant, que toute menace soit écartée. D'abord, il est fort possible que les assaillants, ou un autre groupe cybercriminel, développent une version sans Kill Switch. Une évolution que Kaspersky a cru à un moment avoir isolée, mais l'information reste à confirmer à l'heure où nous écrivons ces lignes. « *En tout cas, WannaCry montre que les outils diffusés par les Shadow Brokers (dont sont issus les exploits récupérés par le ransomware, NDLR) peuvent être rapidement et efficacement utilisés* », remarque Vincent Nguyen. Un message qui n'a pas du échapper aux organisations cybercriminelles, qui pourraient bien être tentées de remplacer le ransomware par un malware effaceur de données ou un Troyen par exemple. Une perspective qui rend l'application des patchs SMB assez incontournable.

A lire aussi :

WannaCry 2.0 : Renault n'est pas la seule entreprise touchée en France

WannaCry et maintenant les variantes !

WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA