

La parade n'existe pas pour contrer les futures affaires WannaCry

L'attaque **WannaCry** fait grand bruit. Au dernier décompte, plus de 200 000 personnes ou entreprises auraient été touchées par ce ransomware. Un « kill switch » a été repéré dans la version initiale du malware. Procédé bien évidemment retiré des dernières moutures en circulation.

La particularité de cette offre est d'être capable de se diffuser **via les partages Windows**, sans qu'il soit nécessaire de l'exécuter sur chacun des postes. Cette faille avait été précédemment corrigée par Microsoft, y compris sous Windows XP ([voir ce lien du site de la firme](#)).

Reste que si ce correctif stoppe la diffusion automatique du malware sur le réseau de l'entreprise, il n'empêchera en rien **l'infection d'une machine isolée**. Au vu du volume de mails infectés reçus par les professionnels à leur travail, le phénomène WannaCry est donc loin de s'éteindre.

Fausse polémique contre vrai problème

Microsoft s'est récemment plaint du fait que les services de renseignement gardaient secrètes les vulnérabilités qu'ils trouvaient, au lieu de les partager avec les éditeurs de logiciels. Certes, c'est grâce à ceci que l'attaque WannaCry a pu être menée. Mais il convient de rester logique : même si les agences de renseignements se mettaient à partager leurs découvertes en matière de sécurité informatique, **les pirates restent capables de trouver des failles...** et seront peu prompts à en avertir les éditeurs.

Second souci, ce type de malware peut également prendre la forme d'une application légitime, du point de vue de l'OS et de ses outils de sécurité. Rappelons en effet que les ransomwares se bornent à manipuler les fichiers présents dans le compte de l'utilisateur. Certaines entreprises vont ainsi découvrir ce lundi qu'elles ne sauraient passer à côté **d'une stratégie de protection des données**. Par sauvegarde, chiffrement et vérification d'intégrité.

À lire aussi :

[WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA](#)

[Vault 7 « Dark Matter » : comment la CIA pirate les Mac et iPhone](#)

[Un groupe de pirates menace de réinitialiser 200 millions d'iPhone](#)