WanaCryptor : les recommandations, préventions et mesures du CERT-FR

Auteur : Jérôme Gianoli Dans Politique et économie 14/05/2017 0

Le centre gouvernemental de veille, d'alerte et de réponse aux attaques informations propose avec l'ANSSI, l'agence nationale de la sécurité des systèmes d'informations, un bulletin d'alerte concernant le ransomware WanaCryptor. Il est aujourd'hui, à l'aide d'outils de hacking dérobés à la NSA, à l'origine d'une attaque massive jugée sans précédent.

Identifié sous la référence , ce document nommé « *Propagation d'un rançongiciel exploitant les vulnérabilités MS17-010* » a été publié rapidement, dès le 12 mais 2017 puis mis à jour le 13 mai 2017. Il dresse un tableau de la situation, identifie les vecteurs d'infections, évoque les systèmes d'exploitation vulnérables et apporte des recommandations.

WanaCryptor n'est pas qu'un ransomware

WanaCryptor est à l'origine de l'installation et propagation d'un logiciel malveillant de type rançongiciel. La source initiale d'infection est probablement un courriel accompagnée d'une pièce jointe malveillante.

Une fois en place, le programme dispose de deux objectifs, mettre en place un rancongiciel afin de soutirer de l'argent à la victime. En parallèle, il assure son infection avec une propagation autonome via le réseau présent sur la machine. Cette seconde partie tire profil d'une faille de sécurité de Windows, une vulnérabilité SMB.

Les environnements vulnérables sont les systèmes d'exploitation Windows en réseau n'ayant pas installés le correctif MS17-010 proposé par Microsoft ou encore les versions Windows XP, Windows Server 2003, Windows 8, Windows Vista, Windows Server 2008, WES09 et POSReady 2009) ou le correctif KB4012598 n'est pas présent.

WanaCryptor, comment réagir ?

Le CERT-FR recommande avant toute chose l'application immédiate des mises à jour de sécurité permettant de corriger les failles exploitées pour la propagation (MS17-010 pour les systèmes maintenus par l'éditeur) et de limiter l'exposition du service SMB, en particulier sur internet.

MS17-010 a été publié le 17 mars dernier. Il vise quasiment toutes les versions de Windows allant de Windows 10 à Windows Vista en passant par Windows 7 ou Windows 8.1. Voici la description de Redmond.

> *« Cette mise à jour de sécurité corrige des vulnérabilités dans Microsoft Windows. La plus grave de ces vulnérabilités pourrait permettre l'exécution de code à distance si un attaquant envoyait des messages spécialement conçus à un serveur Windows SMBv1. Cette mise à jour de sécurité est de niveau « Critique » pour toutes les versions prises en charge de Microsoft Windows. Pour plus d'informations, consultez la section*

> *Logiciels concernés et indices de gravité de la vulnérabilité. La mise à jour de sécurité orrige les vulnérabilités en modifiant la manière dont SMBv1 traite les requêtes spécialement conçues. »*

A noter que Microsoft propose également un correctif pour les versions de Windows dites obsolètes à savoir Windows XP SP2 pour processeurs x64, Windows Server 2003, Windows XP SP3 pour XPe, Windows XP SP3, Windows Vista, Windows Server 2008, WES09 et POSReady 2009 (correctif KB4012598).

De manière préventive, si un serveur ne peut pas être rapidement et facilement mise à jour, l'agence recommande de l'isoler, voire de l'éteindre le temps d'appliquer les mesures adaptées de protection. En cas d'infection constatée, il faut déconnecter immédiatement du réseau les machines identifiées dans le but d'empêcher la

> *« poursuite du chiffrement et la destruction des documents partagés ».*

Comme souvent en matière de protection informatique, la sauvegarde de fichiers est primordiale. Le CERT-FR précise à ce sujet qu'il faut

> *« prendre le temps de sauvegarder les fichiers importants sur des supports de données isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes. »*