WannaCry met en lumière le phénomène des anti-updates

L'affaire **WannaCry** a été l'occasion pour tous les spécialistes en sécurité de faire entendre leur voix et de donner leurs conseils. Le plus judicieux, face à une attaque touchant les données des utilisateurs, reste d'effectuer des sauvegardes régulières, sur un support protégé.

Autre argument donné, la nécessité de disposer d'outils de sécurité à jour. Un conseil relativement inutile, la grande majorité des antivirus n'ayant rien vu venir.

Mais une revendication commence à poindre sur la Toile, sur un thème qui semble évident… mais visiblement pas pour les plus de 200 000 personnes et entreprises touchées par ce problème (dont Renault en France) : **« appliquez les mises à jour de Windows ! »**

Le coupable n'est pas Microsoft

Depuis des années déjà, un phénomène est à l'œuvre : **la non-application des mises à jour.** Nombre d'utilisateurs, y compris dans les DSI, acceptent d'installer un OS de type Windows, mais refusent d'appliquer les mises à jour du système. Pourquoi ? Mystère.

L'affaire WannaCry devrait rappeler les réticents de la vaccination numérique à la raison. Si un PC à jour peut voir ses données escamotées par WannaCry, la diffusion automatique de ce malware via les partages Windows est impossible si les mises à jour de l'OS sont installées.

Microsoft a en effet corrigé ce souci **le 14 mars 2017**, comme en témoigne le bulletin de sécurité MS17-010. Aucun PC sous Windows Vista, 7, 8.1, 10, ni aucun serveur sous Windows Server 2008, 2008 R2, 2012, 2012 R2 et 2016 n'aurait donc eu être touché. La firme de Redmond a même patché récemment Windows XP, Windows 8 et Windows Server 2003. Des OS qui ne sont pourtant plus supportés.

À lire aussi :
La parade n'existe pas pour contrer les futures affaires WannaCry
WannaCry 2.0 : Renault n'est pas la seule entreprise touchée en France
WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA