Cyberattaque mondiale WannaCry : l'analyse de Vladimir Kolla, expert en cybersécurité chez NetXP

mai 2017 par Vladimir Kolla, expert en cybersécurité chez NetXP

En mars dernier, le groupe ShadowBrokers a publié la clef permettant de déchiffrer une archive publiée auparavant et contenant documents et outils de la NSA. Parmi ces outils, se trouvaient des exploits permettant de compromettre des systèmes Windows (mais pas que) à partir de vulnérabilités non connues de Microsoft, dites 0-days.

En particulier, il s'y trouvait des vulnérabilités sur le service SMB de partage de fichiers de Microsoft (utilisé souvent en entreprise, dès que vous accédez à vos partages réseau).

Lors de leur publication, ces vulnérabilités avaient été qualifiées de « wormable », c'est-à-dire qu'elle pouvait être inclues dans un vers qui pourrait s'auto-répliquer grâce à elles.

Des vulnérabilités « wormable » et non corrigées permettant de prendre le contrôle de système Windows à distance, cela aurait pu être le fin du monde mais :
• Une bonne pratique est de ne pas exposer ce type de service sur Internet (mais on trouve encore sur internet près de 3 millions de services SMB exposés) ;
• Miraculeusement, le bulletin de sécurité de Microsoft de mars MS17-010 corrigeait ces vulnérabilités.

Le vers WannaCry

La vie étant ce qu'elle est, de nombreux systèmes vulnérables perdurent :
• Des systèmes obsolètes et ne bénéficiant plus de correctifs de sécurité comme Windows XP, Windows 2003 et Windows 8 ;
• Des caisses de paiement, bornes d'achat, vitrines, distributeurs... sous Windows XP Embedded POSReady pour Point Of Sale (Supporté jusqu'en 2019) mais peu souvent mis à jour ;
• Des systèmes supportés mais non mis à jour (Windows 7, 8.1, 10, Windows Serveur 2008, 2012, 2016) ;
• Des postes ou serveurs infectés par la porte dérobée (backdoor) de la NSA, nommée DoublePulsar.

Ce qui devait arriver arriva : vendredi dernier, un vers nommé WannaCry a commencé à faire son apparition, exploitant une de ces vulnérabilités et réutilisant la porte dérobée de la NSA.