Windows 10 toujours vulnérable aux attaques WannaCry

Les utilisateurs de Windows 10 qui avaient régulièrement appliqué les mises à jour de sécurité du système étaient d'emblée protégés par WannaCry, le ransomworm qui s'est propagé sur plus de 200□000 PC à partir du 12 mai dernier. Microsoft avait en effet fourni un correctif dès le mois de mars (le MS17-010) pour combler les vulnérabilités de SMB (Server Message Block), le serveur de partage d'imprimantes et fichiers qui permet au malware de se propager comme une trainée de poudre dans le réseau de l'entreprise.

Et pour cause, les vulnérabilités étaient exploitées par la NSA qui s'est fait dérober ses outils (notamment EternalBlue, EternalChampion, EternalSynergy, EternalRomance) par le groupe de hackers les Shadow Brokers qui les a versé en ligne. On peut supposer que l'agence de sécurité américaine avait alerté en amont les éditeurs de ces fuites et des vulnérabilités zero-day qui risquaient d'en découler afin qu'ils comblent les failles de leurs solutions respectives. Dont Windows 10.

Un metasploit pour contourner la sécurité

Mais c'était sans compter sur la pugnacité de chercheurs en sécurité qui se sont mis en tête d'exploiter EternalBlue pour compromettre une version non patchée de Windows 10 mais dont les ports SMB sont fermés par défaut. L'équipe de RiskSense a ainsi développé un metasploit, une sorte de couteau suisse pour exploiter les vulnérabilités et souvent utilisé dans le cadre de test d'intrusion. Le module permet de contourner les barrières de sécurité installées par l'éditeur de Redmond, dont Data Execution Prevention (DEP) et Address Space Layout Randomization (ASLR). La société spécialisée en gestion du cyber-risque a également intégré un APC (Asynchronous Procedure Call) qui permet de lancer une attaque sans passer par une backdoor. Du coup, considéré comme inutile, la porte dérobée DoublePulsar a été retirée de l'outil de la NSA.

RiskSense explique avoir développé ce metasploit pour démontrer la faisabilité d'une infection de Windows 10 par WannaCry afin de prévenir les éventuelles futures attaques du ransomware. Mais celles-ci ne seront pas à la portée du premier hacker venu. Dans son rapport, l'entreprise de sécurité précise avoir omis les détails permettant la réalisation du module d'attaque tout en fournissant assez d'information pour prendre les mesures préventives. *« La recherche porte sur une approche transparente (white-hat) de l'industrie de la sécurité de l'information pour accroître la compréhension et la connaissance de ces exploits afin de développer de nouvelles techniques qui empêchent ces futures attaques »*, peut-on lire dans le document.

Des informations que Microsoft serait donc bien inspiré de prendre en compte pour développer de nouveaux correctif à Windows 10 mais aussi à Windows XP et surtout Windows 7. L'OS de 2009 s'est révélé être le plus touché par WannaCry.

[Article mis à jour le 09/06/2017]

Lire également

EternalRocks, un ver mieux outillé que WannaCry

La France, 4eme pays le plus touché au monde par WannaCry

WannaCry : des millions de machines infectées ?