Pourquoi Windows 10 est mieux protégé contre les ransomwares

Les ransomwares, le dernier argument brandi par Microsoft pour convaincre les utilisateurs de migrer vers Windows 10 ? En tout cas, Redmond vient de publier une note d'analyse expliquant comment Windows 10 a pu échapper, contrairement à la version 7 de l'OS et à Windows Server 2008, à la menace WannaCry. Selon Microsoft, ce sont les systèmes de défense internes au nouvel OS qui lui ont permis d'échapper à ce ransomware, de facture classique mais à la diffusion très rapide grâce à l'exploitation d'une faille du service SMB (Server Message Block) de Windows.

Le premier éditeur mondial met notamment en avant les fonctions de virtualisation de la sécurité protégeant Windows 10, même quand un malware parvient à contourner la première ligne de défense. C'est par exemple le cas de la fonction de contrôle du noyau (kernel Control Flow Guard ou kCFG) empêchant l'exécution de code malicieux. S'y ajoute la protection de la mémoire du noyau, empêchant les injections par Shellcode via des zones mémoires protégées et à l'emplacement aléatoire.

L'écosystème Microsoft pour mieux comprendre les menaces

Plus en profondeur, citons encore les défenses permettant de bloquer les activités malveillantes, une fois la souche implantée dans le système. Device Guard et l'antivirus de Windows se chargent de veiller à ne laisser tourner que les applications autorisées et à analyser les fichiers suspects. Au passage, Microsoft en profite pour faire un brin de promotion de son outil de protection des postes de travail, son antivirus Windows Defender AV, outil qui se base sur une infrastructure de Machine Learning dans le Cloud et « *des renseignements sur les menaces sur une échelle inégalée* ». Des données provenant des postes Windows (soit des centaines de millions d'utilisateurs), mais également des navigateurs Edge et IE, d'Office 365 (400 milliards d'e-mails analysés) et de Bing (18 milliards de pages scannés). « *Parmi l'ensemble des malwares bloqués par Windows Defender Antivirus, 99,992 % ont été détectés et arrêtés par Machine Learning et l'analyse comportementale, guidés par notre recherche sur les menaces* », écrit Microsoft.

Les apports de Windows 10 Creators Update

L'éditeur précise que la mouture Creators Update de Windows 10 intègre de nouvelles défenses, encore inconnues avec l'Anniversary Update. Comme l'apparition d'un tableau de bord permettant à l'utilisateur de paramétrer sa sécurité. Ou l'utilisation du Cloud pour détecter des fichiers suspects. Une autre manière de venir nourrir les algorithmes de Machine Learning que déploie Redmond pour protéger son OS. Plus important encore dans la lutte contre les ransomwares : l'apparition d'une fonction permettant de détecter les scripts JS ou VBS malicieux (une technique souvent employée pour déclencher le téléchargement d'un malware) ou encore l'enrichissement du moteur d'analyse comportementale afin de mieux surveiller l'interaction entre les fichiers et le

système. « *L'analyse comportementale est très puissante contre les tentatives de masquage et contre les protecteurs de code (packers) que les auteurs de logiciels malveillants utilisent pour échapper à la détection des antivirus basés sur des signatures de fichiers* », assure Microsoft.

Analyse comportementale : les menaces s'adaptent

Mais pour l'éditeur, encore faut-il que cette analyse comportementale soit suffisamment subtile, car les auteurs de virus se sont déjà adaptés. Les menaces les plus évoluées tentent ainsi d'échapper aux algorithmes de détection comportementale en éclatant les attaques en de multiples tâches unitaires et en de multiples processus, d'apparence bénigne quand on les analyse un par un. « *En surveillant ces activités découpées en multiples vecteurs, Windows Defender AV agit non seulement sur ce type de menaces, mais fournit également des informations utiles pour identifier et bloquer des composants similaires utilisés dans le cadre d'autres attaques* », assure Redmond, dans son document (PDF de 14 pages). S'y ajoute une nouvelle fonction de Windows Defender ATP (Advanced Threat Protection), permettant aux équipes de sécurité de mener leurs analyses sur les attaques et de partir en quête du patient zéro, une recherche utile notamment dans le cas des infections par ransomware.

A lire aussi :

WannaCry : le ransomware qui n'a plus besoin du phishing

WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA

UE : Kaspersky assigne Microsoft pour abus de position dominante