Sécurité : Windows 10 S n'est pas à l'abri des macros Word infectieuses

La sécurité est l'un des arguments mis en avant par Microsoft pour distinguer Windows 10 S, une version Cloud et limitée de Windows 10 en direction du secteur de l'éducation, notamment. L'OS interdit en effet toute installation de logiciel externe à son magasin d'applications, le Windows Store. Et même dans celui-ci, certaines n'ont pas le droit de cité. C'est notamment le cas des distributions Linux et autres applications qui permettraient un accès au système en ligne de commande, via un outil de script ou PowerShell. Navigateurs et antivirus tiers sont également exclus.

Cette stratégie d'un OS propriétaire et fermé s'inscrit, aux yeux de son éditeur, comme la clé de la sécurité des utilisateurs qui ne risquent ainsi pas d'installer, volontairement ou non, des applications compromettantes. *« Aucun système de ransomware connu ne fonctionne contre Windows 10 S »*, assure Microsoft sur son blog. A voir. Nos confrères de *ZDNet* ont demandé au chercheur en sécurité Matthew Hickey de vérifier si les systèmes de protection de l'OS étaient à la hauteur des qualités que Microsoft lui prête. Il lui a suffit de quelques heures pour démontrer le contraire.

Une macro Word pour injecter une DLL

Pour tromper le système installé sur une Surface Laptop, seul PC à embarquer Windows 10 S pour l'heure, le chercheur co-fondateur de la société Hacker House s'est appuyé sur… une macro Word. L'éditeur de texte est lui-même téléchargeable depuis le Windows Store. Et ces petits scripts d'automatisation de tâche intégrés dans des documents Office s'inscrivent comme un des vecteurs d'attaques utilisés par les cyber-criminels. Matthew Hickey a créé sa propre macro permettant d'injecter une DLL (bibliothèque logicielle) dans l'OS sans passer par le magasin applicatif.

Normalement, Word bloque par défaut l'exécution des macros téléchargées depuis le Net ou en pièce jointe d'un e-mail. Mais pas depuis un réseau partagé, un environnement que Windows 10 S considère comme sain par défaut. Il a ensuite suffit d'autoriser l'exécution de la macro en cliquant sur le bouton dédié dans le message d'alerte qui s'affiche sous le menu de Word à l'ouverture du document. L'installation de la macro aurait également pu se faire en la copiant depuis une clé USB à condition de débloquer le fichier en éditant ses propriétés. Et, bien sûr, en bénéficiant d'un accès physique au PC.

Accès aux droits administrateurs

L'exécution de la macro lui a donné accès au Shell de Windows avec des droits administrateurs à partir duquel il a utilisé Metasploit, un outil de test de pénétration, qui a connecté le PC affecté à son serveur de commandes et contrôle. Depuis sa console, le chercheur a désactivé toutes les protections du système (antivirus, antimalware, firewall…) et a remplacé des fichiers sensibles de Windows. De quoi rendre la machine complètement perméable aux malwares de toutes sortes, y compris aux ransomwares.

Certes, le modèle d'attaque du chercheur n'est pas accessible au premier pirate en herbe venu. Au-delà de l'écriture de la macro, il nécessite notamment de réussir à installer le fichier infectieux sur un réseau partagé et convaincre l'utilisateur d'activer le script qu'il contient. Mais, au-delà de leurs prouesses techniques, les cybercriminels ont démontré plus d'une fois leurs talents en matière de manipulation des victimes pour parvenir à leurs fins. Les responsables informatiques qui choisiront de déployer Windows 10 S pour son environnement sécurisé devront garder cette idée en tête.

Lire également
Windows 10 S, un OS un peu trop propriétaire
Linux est interdit de Windows 10 S
10 choses à savoir sur Windows 10 S

Photo credit: sk8geek via Visual hunt / CC BY-SA