400 millions de PC Windows sous la menace de Bashware

Les quelque **400 millions de PC opérés par Windows 10** aujourd'hui sont exposés à une nouvelle technique d'attaque baptisée **Bashware**.

« Nous avons récemment trouvé une méthode nouvelle et alarmante qui permet à tous les logiciels malveillants connus de contourner les solutions de sécurité les plus courantes, telles que les antivirus de prochaine génération, les outils d'inspection et les systèmes anti-ransomware, alerte Check Point par voie de blog.

« Cette technique, baptisée Bashware, exploite une nouvelle fonctionnalité de Windows 10 appelée Subsystem for Linux (WSL), qui vient de sortir de son statut bêta [en juillet dernier, NDLR] pour s'inscrire comme une fonctionnalité intrinsèque à Windows. »

WSL permet d'exploiter Linux à travers la commande Bash sous Windows 10. Un système hybride qui permet aux deux environnements de s'exécuter en même temps. Et d'exposer Windows aux risques d'attaques.

« Les solutions de sécurité existantes ne sont toujours pas adaptées pour surveiller les processus d'exécutables Linux fonctionnant sous Windows OS […], considère l'éditeur de sécurité démonstration à l'appui [voir vidéo en fin d'article]. *Cela peut ouvrir une porte pour les cybercriminels souhaitant exécuter leur code malveillant non détecté et leur permettre d'utiliser les fonctionnalités fournies par WSL pour se cacher des produits de sécurité qui n'ont pas encore intégré les mécanismes de détection appropriés. »*

Des processus similaires à ceux de NT

Concrètement, Bashware tire parti de la conception de la structure des processus Pico. Lesquels ne partagent pas les caractéristiques des processus Windows et ne peuvent donc être assimilés à des processus NT.

Pourtant, *« les processus Pico ont les mêmes capacités que les processus NT légitimes et ne représentent pas une menace moins élevée »*, note Check Point dans son rapport technique. Lequel s'emploie à décrire comment Bashware charge les processus en quatre étapes : chargement des composants WSL, basculement en mode développeur, installation de Linux et exécution sous Wine, un traducteur des appels d'API Windows dans Posix (Portable Operating System Interface) et qui permet d'exploiter les malware Windows depuis WSL.

Un risque certain d'exploitation alors que Check Point déclare avoir testé WSL sur la plupart des produits de sécurité du marché. *« Nous demandons à l'industrie de la sécurité de prendre des mesures immédiates et de modifier ses solutions de sécurité pour se protéger contre cette nouvelle méthode »*, lance l'éditeur.

Le fournisseur de solutions de sécurité IT, qui a lancé l'alerte, déclare avoir mis à jour ses solutions SandBlast Threat Prevention pour prévenir toute tentative d'attaque par la console Linux.

Entre les éditeurs de solutions de sécurité (à commencer par Microsoft) et les cybercriminels, la course est ouverte pour exploiter WSL.

Lire également
Linux + Windows = un nouveau cauchemar sécuritaire
Le sous-système Linux de Windows 10 cartonne en performances
Un malware Linux force les Raspberry Pi à miner de la crypto-monnaie

Code Linux Crédit Photo@isaak55-Shutterstock