L'utilisation malveillante de Windows PowerShell augmente

L'interpréteur de ligne de commande Windows PowerShell de Microsoft est largement utilisé par les administrateurs système. Il l'est aussi par les attaquants, Symantec en témoigne dans un livre blanc. Les échantillons étudiés représentent un total de 111 familles de programmes malveillants utilisant PowerShell. Et, 95,4 % des scripts Windows PowerShell analysés sont malveillants, selon Symantec.

« Au cours des trois derniers mois, nous avons bloqué une moyenne de 466 028 emails avec des fichiers JavaScript malveillants par jour. Et 211 235 macros Word corrompues (W97M.Downloader) par jour sur les terminaux », indique l'éditeur de sécurité. Dans ce domaine, les malwares W97M.Downloader (9,4 % des échantillons analysés), Trojan.Kotver (4,5 %) et JS.Downloader (4 %) sont les plus répandus. Par ailleurs, outre le téléchargement de charges utiles, des scripts PowerShell malveillants sont utilisés pour effectuer d'autres tâches, dont la désinstallation de produits de sécurité, la détection d'environnements de test *« sandboxed »* ou encore la recherche de mots de passe sur un réseau.

Symantec rappelle que plusieurs cyberattaques d'ampleur récentes ont utilisé des scripts PowerShell. C'est le cas, par exemple, d'attaques contre des organisations financières et des utilisateurs du réseau interbancaire SWIFT. Ces attaques auraient été menées par un groupe de pirates à l'origine du cheval de Troie Odinaff, présentant des similitudes avec le programme Carbanak. D'autres attaquants encore s'appuient sur Trojan.Kotver. Ce programme utilise le langage de script pour créer une infection sans fichier intégrée dans le registre…

Outil d'attaque privilégié

« Si de nombreux administrateurs système utilisent les scripts PowerShell pour la gestion de tâches quotidiennes, nous constatons également que des attaquants les utilisent de plus en plus dans le cadre de leurs campagnes », explique dans un billet de blog Candid Wueest, chercheur chez Symantec.

« PowerShell est installé par défaut sur la plupart des ordinateurs Windows, et la plupart des organisations n'ont pas la journalisation étendue activée pour le framework, ajoute-t-il. *Ces deux facteurs font de PowerShell un outil d'attaque privilégié. De plus, les scripts peuvent facilement être occultés et permettre aux charges utiles d'être exécutées directement depuis la mémoire »*. PowerShell permet aussi un accès distant par défaut et laisse peu de traces exploitables. Ce sont autant d'avantages pour les pirates.

Dans ce contexte, Symantec recommande aux sysdamins d'opter pour la version la plus récente de PowerShell, de ne pas omettre les mises à jour et d'activer la journalisation étendue. Dans un bulletin publié en début d'année, le CERT-FR recommandait lui-même de *« journaliser l'exécution de commandes ou scripts PowerShell »*. Une action qui *« permettra l'analyse détaillée des scripts exécutés en cas de compromission, mais pourra aussi se révéler précieuse dans l'analyse de dysfonctionnements »*.

Lire aussi :

Windows 10 : Microsoft remplace cmd.exe par PowerShell

L’histoire de Microsoft PowerShell en 10 questions (quiz)
Microsoft libère le code de PowerShell et le porte sous Linux !