Des attaques informatiques par Malwares de plus en plus perfectionnées…

	Des attaques informatiques par Malwares de plus en plus perfectionnées…

Les chercheurs de Palo Alto Networks nous mettent en garde contre des diffusions de spam ciblées qui visent à introduire un malware sans fichier via des documents Word en pièce jointe contenant une macro malveillante. Jusqu'il y a peu, cette pratique était connue uniquement chez les trojans bancaires comme Dridex et Dyre, mais il semblerait que cette méthode ancienne, mais toujours efficace, est utilisée pour d'autres malwares comme le voleur d'informations Grabit, l'espion BlackEnergy, le bot Kasidet et le ransomware Locky.

Dans le cas présent, Palo Alto rapporte que les messages malveillants sont diffusés en petites quantités vers des adresses professionnelles d'employés de sociétés américaines, canadiennes et européennes. Ces messages se présentent sous la forme de messages professionnels, contiennent le nom exact du destinataire ainsi que certaines informations sur la société pour laquelle il travaille. Ces petits détails, visiblement obtenus auprès de sources publiques, suffisent pour convaincre le destinataire d'accepter la demande de consulter le document en pièce jointe.
Si l'utilisateur ouvre le fichier malveillant et qu'il accepte l'activation des macros (les macros ne sont pas activées par défaut), il lance l'exécution du fichier powershell.exe masqué selon des arguments particuliers de la ligne de commande. La commande PowerShell exécutée dans ce cas, vise à identifier l'architecture Windows (32 ou 64 bits) et, en fonction du résultat, garantit le téléchargement d'un script PowerShell complémentaire avec code shell.
Cette charge utile permet de réaliser plusieurs vérification sur l'ordinateur infecté, de déterminer à quel point l'environnement d'exécution est hostile (machine virtuelle, bac à sable, débogueur) et de déterminer la valeur de la cible. Sur la base de listes noire et blanche, le malware recherche dans les paramètres réseau de la victime les lignes qui permettent d'identifier le profil de la machine attaquée, ainsi que les noms de quelques sites financiers et les noms Citrix, XenApp, dana-na (dossier partagé avec URL interne créee dans les VPN Juniper) dans les URL mises en cache.
« Il semblerait que ce malware tente dans la mesure du possible d'éviter les ordinateurs des médecins et des réprésentants du monde de l'enseignement. Il se concentre uniquement sur ceux qui réalisent des opérations financières » expliquent les chercheurs. « Au milieu de l'année 2015, des techniques similaires avaient été enregistrées dans la famille de malwares Ursnif. »
Le malware envoie les résultats des vérifications à son centre de commande. Si l'objet attaqué est intéressant pour les individus malintentionnés, le centre de commande envoie un fichier DLL crypté qui est enregistré temporairement sur le disque et qui est utilisé à l'aide de rundll32.exe.
Les chercheurs ont baptisé ce malware PowerSniff. Un des échantillons a même été analysé dans ISC SANS. D'après Palo Alto, l'ampleur de cette campagne malveillante n'est pas encore trop grande : à l'heure actuelle, seuls 1 500 messages de spam environ ont été référencés…. [Lire la suite]

Réagissez à cet article

Source : *Macros malveillantes dans des attaques ciblées – Securelist*