Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

	Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

Afin de voler leurs données, le malware utilise une campagne de diffusion massive ciblée en renvoyant les victimes vers un site gouvernemental libyen compromis et contenant le malware

Malgré le manque de sophistication du malware et un mécanisme de propagation rudimentaire, les auteurs de cette menace ont démontré qu'ils étaient capables de compromettre des sites gouvernementaux avec succès.
Au cours de leurs recherches, les **experts ESET** ont découvert que les attaquants compromettent des profils de réseaux sociaux (Facebook, Twitter…) et postent des liens amenant au téléchargement de logiciels malveillants. Le post est rédigé en arabe et explique : « le premier ministre a été capturé à deux reprises, dont cette fois-ci dans une bibliothèque ».

Ce message texte relativement court est suivi d'un lien vers le site gouvernemental compromis.

Figure 1 : Post sur Facebook renvoyant vers un lien comportant le malware

En plus de la diffusion massive de cette campagne, les cybercriminels mènent des attaques ciblées par l'envoi d'e-mail contenant une pièce jointe malveillante de type spearphishing. Pour convaincre les victimes d'exécuter le code malveillant, des astuces d'ingénierie sociale sont mises en œuvre, comme l'utilisation d'icônes MS Word et PDF à la place de celles des exécutables et de techniques de double extension dans les noms de fichier, comme .pdf.exe. Dans certains cas, le malware peut afficher un document leurre.
Les experts ESET ont identifié le malware comme appartenant à la famille des Chevaux de Troie qui tentent de recueillir diverses informations par le vol de données classiques. Il peut être déployé sous plusieurs configurations. **La version complète du logiciel malveillant peut enregistrer les frappes de clavier, collecter des fichiers de profil des navigateurs Mozilla Firefox et Google Chrome, enregistrer des sons à partir du microphone, réaliser des captures d'écran depuis la webcam, et recueillir des informations sur la version du système d'exploitation et du logiciel antivirus installé.** Dans certains cas, le logiciel malveillant peut télécharger et exécuter des outils tiers de récupération de mots de passe enregistrés à partir d'applications installées.
« Nous avons analysé un échantillon de ce malware qui est actif depuis au moins 2012 dans des régions spécifiques du globe. Par le passé, les auteurs de cette cybermenace utilisaient ce malware pour une diffusion massive. Il convient de noter qu'il est encore utilisé dans des attaques de spearphishing », explique Anton Cherepanov, malware researcher chez ESET.
Pour plus de détails sur ce malware, cliquez ici.
Source : ESET

Réagissez à cet article

Original de l’article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail