## Qu'est-ce qu'un malware « macro-less » et pourquoi cela vous dit-il quelque chose ?

L'année dernière, des pirates liés au groupe de hackers russe APT28 ont démarré une attaque comme en 1999 avec un malware basé sur Microsoft Word qui ne déclenche aucune alerte de sécurité dans son parcours. Ces types d'attaques sont appelées « macro-less malware » car ils contournent les alertes de sécurité mises en place dans les logiciels Microsoft Office en réponse aux macro malwares traditionnels tels que le virus Melissa à la fin du 20ème siècle.

Dans une analyse de novembre 2017, le géant de la sécurité McAfee a mis à jour une campagne d'APT28 utilisant une combinaison de 'phishing' (hameçonnage) et de malware « macro-less » pour installer un spyware (logiciel espion) dans l'ordinateur de leurs victimes.

Les malwares « macro-less » exploitent un protocole Microsoft appelé DDE (Dynamic Data Exchange) pour exécuter du code malicieux au sein de documents Microsoft Office. DDE a également des usages légitimes, principalement pour partager des données entre différentes applications. Dans ce cas, les pirates peuvent utiliser DDE pour lancer d'autres applications, comme PowerShell, et exécuter du code malicieux.

Ces nouvelles attaques DDE nécessitent toujours une certaine interaction de la part des utilisateurs, comme les attaques macro traditionnelles sur Office. Afin que le code DDE malicieux puisse s'exécuter, l'attaquant doit convaincre sa victime de désactiver le Mode Protégé et de cliquer sur au moins une fenêtre supplémentaire. Ce qui diffère des attaques macro traditionnelles est la façon dont sont conçues les fenêtres de dialogue pour l'utilisateur.

Avec Microsoft Office 2003 et ses versions suivantes, Microsoft a changé les fenêtres de dialogue macro pour souligner leurs implications en matière de sécurité, en utilisant des boucliers jaunes et des messages proéminents « Alerte de Sécurité ». Les fenêtres d'exécution DDE toutefois, sont de simples boîtes de dialogue grises, parfois sans aucune mention de sécurité, qui demandent aux utilisateurs « Ce document contient des liens pouvant mener à d'autres fichiers. Voulez-vous mettre à jour ce document avec les données provenant du fichier associé ? » En d'autres termes, DDE est maintenant géré de la même façon que les macros traditionnels il y a vingt ans dans Office 97. Nouvelle méthode d'attaque, mais interaction des utilisateurs similaire.

Les macro malwares et macro less malwares ont tous deux le même résultat – ils permettent aux attaquants d'exploiter le moteur de script de Microsoft Windows pour télécharger et exécuter des contenus malicieux. Alors que des macros peuvent embarquer du code Visual Basic directement dans un document Word, DDE doit lancer une application séparée, telle que PowerShell, pour effectuer des tâches complexes telles que télécharger et exécuter un malware.

Donc pourquoi les attaquants font-ils cela ? Les attaques par macro-less malware sont efficaces pour la même raison que les macro malwares l'étaient durant plus de vingt ans. Une large proportion des utilisateurs ne lit simplement pas les fenêtres de dialogue avant de cliquer sur « oui ». Les attaquants accroissent souvent leurs chances de succès en utilisant des tactiques d'ingénierie sociale telles que des instructions explicites visant à accepter tous les messages afin « d'accéder au message important ». Les cyber criminels sont connus pour recycler tout ce qui fonctionne, donc il est courant de voir des tactiques malicieuses comme celle-ci réapparaître régulièrement sous des formes différentes.

Heureusement, il existe des mesures à prendre pour se protéger. Dans le sillage des attaques d'APT28, Microsoft a publié un message de sécurité avec des instructions permettant de désactiver entièrement

le protocole DDE. Beaucoup de solutions avancées de 'sandboxing' anti malware peuvent détecter les malwares basés sur DDE et les stopper avant qu'ils ne pénètrent dans le réseau. Plus important toutefois, les utilisateurs finaux doivent être formés à l'identification des attaques de 'phishing' et aux méthodes d'ingénierie sociale que les pirates utilisent pour persuader leurs victimes de cliquer sur les fenêtres de dialogue DDE.

Microsoft a déjà commencé à améliorer le traitement par Office des malwares macro-less en ajoutant plusieurs contrôles invisibles afin de stopper la progression du code DDE malicieux. Il est probable que Microsoft parviendra très rapidement à améliorer les fenêtres de dialogue de DDE pour mieux avertir les victimes potentielles. Mais ces alertes de sécurité, bien que très visibles, n'ont pas réussi à tuer les macro malwares, ce qui veut dire que les deux types d'attaques devront toujours être prises en considération dans l'avenir. Comme toujours, en cas de doute, il vaut mieux s'abstenir de cliquer sur quelque chose d'inattendu ou que l'on ne comprend pas.

Pascal Le Digol, Country Manager France de WatchGuard