Dimnie : le malware furtif qui cible les développeurs sur GitHub

Des cibles à haut retour sur investissement ? C'est probablement à cette aune qu'il faut interpréter la campagne Dimnie, du nom d'un malware dont les agissements sont détaillés par Palo Alto Networks et qui cible spécifiquement les développeurs partageant du code sur GitHub. Selon les chercheurs de la firme de sécurité, alertés par des messages de développeurs portant sur des e-mails suspects qu'ils avaient reçus, Dimnie est un malware modulaire offrant de nombreuses options à ses commanditaires : keylogging (idéal pour récupérer des codes d'accès à des services par exemple), captures d'écran, extraction de données, accès à la liste des processus exécutés sur une machine ou encore destruction des environnements infectés.

A l'image d'autres souches infectieuses sophistiqués, ce malware d'origine inconnue emploie des techniques évoluées pour masquer ses traces, notamment pour empêcher que les envois de données depuis et vers les serveurs contrôlés par les assaillants ne soient repérés par les technologies d'analyse de trafic. Dimnie crée par exemple une « *requête proxy http apparemment légitime vers un service Google* » ; en réalité l'appel renvoie à un service de Mountain View tombé en désuétude et servant de « *camouflage* » à une connexion vers un serveur de contrôle et de commande aux mains de ceux qui orchestrent cette opération. Le malware masque aussi ses exfiltrations d'informations en chiffrant des données dans de faux en-têtes d'images Jpeg.

Dimnie bat les hypothèses des défenseurs

Par ailleurs, « *chaque module de Dimnie est injecté dans la mémoire de processus Windows essentiels, compliquant un peu plus l'analyse* », du fait de l'absence de toute écriture sur le disque dur, relèvent les chercheurs de l'unité 42 de Palo Alto Networks. Bref, à l'image de quelques malwares détectés récemment, Dimnie se range dans la catégorie des menaces furtives. « *En masquant son trafic réseau montant et descendant derrière l'activité inoffensive des utilisateurs, Dimnie a pris l'avantage sur les hypothèses des défenseurs quant à ce que doit être le trafic légitime. Cet ensemble de techniques, combiné à la propension initiale (des assaillants, NDLR) à cibler des systèmes d'utilisateurs russophones, a probablement permis à Dimnie de rester relativement peu connu* », écrivent les chercheurs de l'Unit 42.

En réalité, la souche est même restée sous les radars très, très longtemps, puisque Palo Alto affirme avoir observé des versions du malware datant de début 2014 et utilisant les mêmes mécanismes de commande et de contrôle. Notons d'ailleurs que Dimnie a été identifié via sa méthode d'infection, dès plus classiques, et non par son activité. Les assaillants emploient en effet du spearphishing (hameçonnage ciblé), promettant la plupart du temps un emploi ou de l'argent aux développeurs destinataires. Evidemment, les détails du poste ou du contrat promis figurent, prétendument, dans un fichier joint, un .doc renfermant une macro malveillante qui exécute une commande PowerShell déclenchant l'installation du malware. Ce sont ces mails suspects qui ont attiré l'attention de certains développeurs ; ces derniers les ont signalés sur des forums.

Cybercriminels ou Etat ?

Reste à savoir qui se cache derrière Dimnie ? Un terrain sur lequel Palo Alto ne s'avance pas. Le malware pourrait être l'oeuvre de cybercriminels, qui pourraient avoir trouvé sur GitHub une population nombreuse (le site compte plus de 24 millions d'utilisateurs) et à haut potentiel. Mais Dimnie pourrait aussi avoir été conçu par un Etat, à des fins d'espionnage, par exemple en récupérant des données de développeurs ciblés ayant accès à des informations sensibles. Voire, pourquoi pas, en se servant des accès de ces profils pour modifier directement les codes source de logiciels, afin de se ménager des backdoors… « *L'objectif premier des modules que nous avons observés est de voler de l'information et de pratiquer des actions de reconnaissance* », se contente de relever Palo Alto, qui ajoute que le caractère modulaire du malware lui ouvre une palette très large de fonctionnalités malveillantes.

A lire aussi :

Domain Fronting : comment les services russes masquent leurs attaques

Le malware bancaire Dridex devient hyper furtif, grâce au AtomBombing

Anatomie du malware super furtif, caché dans la mémoire des serveurs

Crédit photo : © igor.stevanovic / shutterstock