Skimer, la nouvelle menace pour distributeurs de billets

Skimer, la nouvelle menace pour distributeurs de billets

Skimer, un groupe russophone, force les distributeurs automatiques de billets (DAB) à l'aider à dérober de l'argent. Découvert en 2009, Skimer a été le premier programme malicieux à prendre pour cible les DAB. Sept ans plus tard, les cybercriminels ré-utilisent ce malware. Mais le programme, ainsi que les escrocs, ont évolué ; ils représentent une menace encore plus importante pour les banques et leurs clients partout dans le monde.

Imaginons qu'une banque découvre avoir été victime d'une attaque. Étrangement, aucune somme d'argent n'a été dérobée et rien n'a été modifié dans son système. Les criminels sont partis comme ils sont venus. Serait-ce possible ? Je vous parlais de ce type d'attaque l'année dernière. L'éditeur Gdata m'avait invité en Allemagne pour découvrir l'outil malveillant qui permettait de pirater un distributeur de billets. Aujourd'hui, l'équipe d'experts de Kaspersky Lab a mis au jour le scenario imaginé par les cybercriminels et découvert des traces d'une version améliorée du malware Skimer sur l'un des DAB d'une banque. Il avait été posé là et n'avait pas été activé jusqu'à ce que les criminels lui envoient un contrôle : une façon ingénieuse de couvrir leurs traces.
Le groupe Skimer commence ses opérations en accédant au système du DAB, soit physiquement, soit via le réseau interne de la banque visée. Ensuite, après été installé avec succès dans le système, l'outil Backdoor.Win32.Skimer, infecte le cœur de l'ATM, c'est-à-dire le fichier exécutable en charge des interactions entre la machine et l'infrastructure de la banque, de la gestion des espèces et des cartes bancaires.
Ainsi, les criminels contrôlent complètement les DAB infectés. Mais ils restent prudents et leurs actions témoignent d'une grande habileté. Au lieu d'installer un skimmer (un lecteur de carte frauduleux qui se superpose à celui du DAB) pour siphonner les données des cartes, les criminels transforment le DAB lui-même en skimmer. En infectant les DAB avec Backdoor.Win32.Skimer, ils peuvent retirer tout l'argent disponible dans le distributeur ou récupérer les données des cartes des utilisateurs qui viennent retirer de l'argent, y compris le numéro de compte et le code de carte bancaire des clients de la banque.
Il est impossible pour un individu lambda d'identifier un DAB infecté car aucun signe de le distingue d'un système sain, contrairement à un DAB sur lequel a été posé un skimmer traditionnel qui peut être repéré par un utilisateur averti.

Un zombie dormant
Les retraits directs depuis un DAB ne peuvent pas passer inaperçu alors qu'un malware peut tranquillement siphonner des données pendant une longue période. C'est pourquoi le groupe Skimer n'agit pas immédiatement et couvre ses traces avec beaucoup de prudence. Leur malware peut opérer pendant plusieurs mois sans entreprendre la moindre action.
Pour le réveiller, les criminels doivent insérer une carte spécifique, qui contient certaines entrées sur sa bande magnétique. Après lecture de ces entrées, Skimer peut exécuter la commande codée en dur ou requérir des commandes via le menu spécial activé par la carte. L'interface graphique de Skimer n'apparaît sur l'écran qu'une fois la carte éjectée et si les criminels ont composé la bonne clé de session, de la bonne façon, sur le pavé numérique en moins de 60 secondes.
À l'aide du menu, les criminels peuvent activer 21 commandes différentes, comme distribuer de l'argent (40 billets d'une cassette spécifique), collecter les données des cartes insérées, activer l'auto-suppression, effectuer une mise à jour (depuis le code du malware mis à jour embarqué sur la puce de la carte), etc. D'autre part, lors de la collecte des données de cartes bancaires, Skimer peut sauvegarder les fichiers dumps et les codes PIN sur la puce de la même carte, ou il peut imprimer les données de cartes collectées sur des tickets générés par le DAB.
Dans la plupart des cas, les criminels choisissent d'attendre pour collecter les données volées afin de créer des copies de ces cartes ultérieurement. Ils utilisent ces copies dans des DAB non infectés pour retirer de l'argent sur les comptes clients sans être inquiétés. De cette manière, ils s'assurent que les DAB infectés ne seront pas découverts. Et ils récupèrent de l'argent simplement.

Des voleurs expérimentés
Skimer a été largement répandu entre 2010 et 2013. À son arrivée correspond une augmentation drastique du nombre d'attaques sur des distributeurs automatiques de billets, avec jusqu'à neuf différentes familles de malwares identifiées par Kaspersky Lab. Cela inclut la famille Tyupkin, découverte en mars 2014, qui est devenue la plus populaire et la plus répandue. Cependant, il semblerait maintenant que Backdoor.Win32.Skimer soit de retour. Kaspersky Lab identifie 49 modifications de ce malware, dont 37 ciblent les DAB émanant de l'un des plus importants fabricants. La version la plus récente a été découverte en mai 2016.
En observant les échantillons partagés avec VirusTotal, on note que les DAB infectés sont répartis sur une large zone géographique. Les 20 derniers échantillons de la famille Skimer ont été téléchargés depuis plus de 10 régions à travers le monde : Émirats Arabes Unis, France, États-Unis, Russie, Macao, Chine, Philippines, Espagne, Allemagne, Géorgie, Pologne, Brésil, République Tchèque… [Lire la suite]
Remarquable article de Damien Bancal

Réagissez à cet article

Source : *Skimer, la nouvelle menace pour distributeurs de billets – Data Security BreachData Security Breach*