Botnet : Emotet évolue pour s'attaquer au Wi□Fi

Cette nouvelle version d'Emotet diffère des précédentes qui ciblaient uniquement les réseaux câblés locaux. Le botnet Emotet a fait son apparition en 2014 en tant que cheval de Troie bancaire.

Au début, il se répandait par email et était automatiquement transféré aux listes de contacts de ses victimes. Plus tard, le botnet a évolué pour diffuser des charges utiles malveillantes supplémentaires, telles que des ransomwares.

Aujourd'hui, il a de nouveau progressé, cette fois pour exploiter les points d'accès Wi□Fi vulnérables. Comme cela est le cas pour de nombreux botnets, les cybercriminels qui exploitent Emotet peuvent lui adjoindre différents modules destinés à exécuter diverses tâches malveillantes.

Avant cette mise à jour, Emotet disposait déjà de capacités de diffusion de base semblables à celles des vers. S'il détecte un réseau câblé connecté, il essaie de se propager à d'autres appareils présents sur ce réseau en se servant de mots de passe par défaut ou de techniques élémentaires de crackage des mots de passe par force brute.

Cette version mise à jour comprend toutefois un nouveau module de propagation Wi□Fi unique, qui permet au malware de s'étendre à des réseaux sans fil non sécurisés, tels que ceux de nombreux points d'accès Wi□Fi publics.

Le mode opératoire d'Emotet est le suivant :

1. Emotet utilise l'adaptateur sans fil de la victime pour analyser l'espace de signal Wi□Fi local, puis dresse la liste de tous les réseaux sans fil (SSID) identifiés. Cette analyse Wi□Fi peut avoir lieu sans que l'appareil de la victime soit connecté à l'un des réseaux trouvés.
2. Après avoir identifié les réseaux cibles potentiels situés à proximité, le malware tente de s'y connecter à partir d'une liste de mots de passe Wi□Fi courants. S'il parvient à se connecter à l'un d'eux, il passe à la phase suivante de l'attaque.
3. Une fois connecté au réseau Wi□Fi d'une victime, Emotet recherche les autres appareils connectés et tous les dossiers qu'ils partagent publiquement. S'il en trouve un, il lance un autre type d'attaque par force brute, en essayant cette fois de se connecter au partage à l'aide de noms d'utilisateur et mots de passe courants.
4. Si Emotet réussit à se connecter à l'un des partages trouvés sur le réseau Wi□Fi, il charge une copie de lui-même sur ce partage et utilise les commandes réseau de Windows pour tenter d'exécuter cette nouvelle copie. En cas de succès, le processus se réinitialise prenant pour cible une nouvelle victime.
5. Enfin, le malware envoie des informations sur les scans Wi□Fi et les nouveaux systèmes compromis à son serveur de commande et contrôle (C&C). Au terme de la phase de propagation, Emotet reste connecté au botnet en tant que client bot via un serveur C&C. Les cybercriminels à l'origine de l'attaque disposent alors d'un contrôle total sur l'ordinateur de la victime et peuvent exécuter n'importe quelle action malveillante en

fonction des modules Emotet qu'ils ont installés.

Pour préserver vos réseaux sans fil du module de propagation Wi□Fi d'Emotet, il suffit d'appliquer les règles élémentaires de sécurité des points d'accès Wi□Fi.
Si vous gérez un réseau Wi□Fi, protégez-le en utilisant le dernier protocole de sécurité WPA3 et un mot de passe unique de plus de 15 caractères. Cela devrait empêcher un ordinateur infecté par Emotet, situé à proximité de votre point d'accès, de trouver votre mot de passe SSID par force brute.

Pour aller plus loin, certains réseaux Wi-Fi publics s'appuient sur des solutions permettant l'isolation des clients Wi-Fi entre eux : deux ordinateurs connectés au même réseau Wi-Fi pourront alors certes accéder à Internet, mais ne pourront pas communiquer entre eux.

De même, les entreprises pourront également déployer des solutions permettant d'empêcher les clients de se connecter à des points d'accès voisins (afin de limiter la propagation du ver) et, bien entendu, de filtrer le trafic du réseau afin de détecter les usages malveillants !