Le malware Rombertik détruit les PC quand il est détecté

Des chercheurs de **Talos**, l'entité de recherche en sécurité de l'équipementier américain **Cisco**, ont étudié une nouvelle génération de malware capable d'échapper à l'analyse et de détruire un disque dur lorsque le logiciel malveillant est malgré tout repéré. Le malware nommé **Rombertik** se propage via les spams et messages de phishing. Les cibles sont incitées à ouvrir une pièce jointe. Cette action malencontreuse permettra la propagation du programme malveillant.

Rombertik peut s'intégrer au navigateur de l'utilisateur et obtenir des informations sensibles exfiltrées vers des serveurs contrôlés par l'attaquant. *« Rombertik recueille des informations sur tous les sites web visités de manière indiscriminée »*, expliquent Ben Baker et Alex Chiu dans un billet de blog.

L'ordinateur infecté redémarre en boucle

Programme complexe, Rombertik dispose de multiples couches et fonctionnalités d'obscurcissement destinées à *« échapper aux outils d'analyse statique et dynamique, et rendre le débogage difficile »*. Rombertik peut échapper à une ***sandbox*** (zone d'exécution sécurisée de logiciels) et inonder les outils d'analyse d'une énorme quantité de logs (plus de 100 Go) difficiles et longs à digérer.

Si le logiciel malveillant Rombertik détecte qu'il fait tout de même l'objet d'une analyse, il finira par détruire le premier secteur de démarrage (**Master Boot Record** ou MBR) pour rendre le PC inutilisable, déclarent les chercheurs de Talos. Si les autorisations ne sont pas obtenues, Rombertik pourra s'attaquer à tous les fichiers présents dans le dossier *home* de l'utilisateur en chiffrant chaque fichier avec une **clé RC4** générée aléatoirement. Une fois le MBR modifié ou les fichiers chiffrés, l'ordinateur redémarre en boucle empêchant le système d'exploitation de se lancer.

Lire aussi :
Le malware PoSeidon met les terminaux point de vente en danger
Un malware résistant à un formatage de disque dur : l'œuvre de la NSA ?

crédit photo © Artur Marciniec – Fotolia