# Un malware qui reste lors d’une réinstallation du système d’exploitation


Un malware qui reste lors d’une réinstallation du système d’exploitation

---

**Conçu en particulier pour dérober des données bancaires, l’écosystème Nemesis comporte un logiciel malveillant qui s’installe à très bas niveau sur le disque dur.**

Les équipes de Mandiant (FireEye) ont découvert, en septembre dernier, un logiciel malveillant employant des méthodes de persistance peu communes : il s’immisce dans le processus d’initialisation de l’ordinateur infecté, avant même le chargement du système d’exploitation, afin de pouvoir compromettre celui-ci à coup sûr et, surtout, résister à une tentative de nettoyage de la machine par réinstallation de son système d’exploitation – « un moyen largement considéré comme le plus efficace pour éradiquer un logiciel malveillant », soulignent les chercheurs de FireEye dans un billet de blog.

**Analyse comportementale : la clé de la sécurité ?**

E-handbook : L’analyse comportementale joue un rôle non négligeable dans la sécurité de votre entreprise.

Ce logiciel malveillant fait partie de Nemesis, un ensemble d’outils malicieux utilisé par le groupe FIN1, qui semble « localisé en Russie, ou un pays russophone », spécialisé dans le vol de données de cartes bancaires et, plus généralement, d’informations « aisément monétisables en provenance d’organisations telles que banques, organismes de crédit, opérations de DAB », etc.

Comme le rappellent les chercheurs de FireEye, le secteur d’amorçage des disques durs, le fameux MBR (Master Boot Record), ne contient pas que des données inertes relatives aux partitions définies : il recèle également quelques éléments de code utilisés durant le processus de démarrage ; « ce code cherche la partition active principale et passe ensuite le contrôle au VBR (Volume Boot Record) de cette partition ». Ce dernier contient également du code exécutable « spécifique au système d’exploitation présent sur cette partition », et lui permettant de lancer son démarrage.

Baptisé Bootrash, le logiciel malveillant découvert par les équipes de Mandiant, pirate ce processus en remplaçant le code d’amorçage du VBR par son propre code malicieux chargé d’appeler le bootkit Nemesis. Celui-ci « intercepte certaines fonctions du processus de démarrage et injecte les composants Nemesis dans le noyau de Windows ».

Les chercheurs de FireEye soulignent que ce n’est pas une première, mais que l’utilisation d’un bootkit MBR ou VBR n’est pas courant. Une chance, peut-être, car la détection peut s’avérer particulièrement difficile : ces logiciels malveillants peuvent « être installés et s’exécuter presque complètement en dehors du système d’exploitation Windows », passant au travers des mécanismes de vérification de son intégrité ou encore des anti-virus – à moins d’examiner méticuleusement la mémoire vive.

---

Réagissez à cet article

Source : http://www.lemagit.fr/actualites/4500260472/Un-malware-qui-reste-lors-dune-reinstallation-du-systeme-dexploitation