Le malware bancaire Dridex devient hyper furtif, grâce au AtomBombing

Comme les logiciels standards, les malwares connaissent leur cycle d'évolution. S'il est rare que leurs développeurs y associent des numéros de version, Dridex fait exception à la règle. IBM X-Force a ainsi mis la main sur un échantillon de la version 4 du célèbre malware bancaire. Déjà à l'œuvre contre des banques au Royaume-Uni selon Big Blue, cette mouture exploite une nouvelle méthode pour contourner les outils de détection, une technique connue sous le nom d'AtomBombing.

Comme ses versions antérieures, Dridex s'attache à monitorer le trafic de ses victimes en direction des sites bancaires afin de leur dérober leurs login et mots de passe. Mais cette v4 fait appel à une méthode d'injection de code toute récente, puisqu'elle a été détaillée en octobre 2016 seulement par les chercheurs de la société enSilo. Cette technique repose sur les tables atomiques de Windows, soit des appels élémentaires de l'OS de Microsoft permettant aux applications de stocker et accéder à des données temporaires, ainsi que sur l'API native de l'OS appelée NtQueueApcThread. Dridex v4 « *a ensuite recours à NtSetContextThread (autre API de Windows, NDLR) pour appeler une chaîne return-oriented programming (ROP, technique permettant de prendre le contrôle d'une pile d'exécution au sein d'un programme, NDLR) qui alloue un espace de mémoire en lecture/écriture/exécution, copie la charge utile et en assure l'exécution. Enfin, il restaure le contexte original de la tâche détournée* », écrit IBM X-Force. Une approche bien plus furtive que les précédentes techniques d'injection de code employées par Dridex, qui avaient recours à des appels à des API devenus facilement repérables par les outils de détection. Les injections de code sont un processus suivis de très près par les antivirus et autres outils de protection.

Dridex va être imité, dit IBM X-Force

« *Dridex est le seul cheval de Troie bancaire à employer AtomBombing à notre connaissance*, écrit IBM X-Force dans son billet de blog. *Ce changement est d'autant plus significatif qu'il s'agit d'un malware qui est supposé être mis en œuvre par un gang de cybercriminels organisé, ce qui signifie qu'il est probable que d'autres codes malveillants vont adopter la même méthode à l'avenir.* »

Or, AtomBombing, qui touche toutes les versions de Windows, ne résulte pas d'une vulnérabilité de l'OS, et ne peut donc pas être corrigé par un patch. La technique exploite simplement la façon dont certains mécanismes du système d'exploitation ont été pensés. Comme l'avait noté EnSilo dans un billet de blog en octobre dernier, la seule manière d'éviter des attaques utilisant AtomBombing consiste à monitorer les injections de code exploitant les API de Windows en cause dans cette méthode.

Notons, au passage, que les auteurs de Dridex ont amélioré la technique décrite par EnSilo. S'ils emploient AtomBombing pour écrire la charge utile en mémoire, ils utilisent d'autres méthodes pour gagner les droits d'exécution de leur programme et en assurer l'exécution proprement dite, selon les auteurs du rapport de X-Force, Magal Baz et Or Safran. D'autres raffinements ont aussi été apportés à la v4 de Dridex, notamment dans le nommage et le chiffrement. Objectif, une fois de

plus : éviter la détection du malware par les outils de protection.

A lire aussi :

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

Avec Proteus, le malware tout-en-un débarque

Pour les RSSI, les solutions de cybersécurité ne sont pas satisfaisantes

Crédit photo © igor.stevanovic / shutterstock