Cutlet Maker: ce malware « pilleur de distributeur de billets » sévit encore

Dévaliser un distributeur de billets à la voiture bélier n'est plus nécessaire. Un couteau et une clé USB équipée des logiciels adéquats suffisent.

C'est du moins ainsi qu'un pirate (ou groupe de pirates) présente leur solution en vidéos depuis le portail du Dark Web ATMjackpot.

Sur l'une des vidéos, reprise par *Bleeping Computer*, on y voit un détrousseur retirer le panneau frontal supérieur d'un distributeur à l'aide d'un simple couteau de cuisine, repérer le port USB du système, y introduire une clé USB et lancer quelques instructions depuis un clavier sans fil pour activer la distribution frauduleuse de billets.

Un malware de 2016, voire 2014

Le malware se compose de deux fichiers : Cutlet Maker, l'application principale pour interagir avec le distributeur via son API, et Stimulator, qui permet de vérifier le contenu de l'appareil (inutile de s'attaquer à un distributeur vide), rapporte Kaspersky Lab.

Pour l'anecdote, Cutlet Dish désigne un plat de viande en anglais. Mais en argot russe, cela fait référence à « une liasse de billets ». *« Les criminels derrière le logiciel malveillant pourraient être de langue maternelle russe »*, pense Konstantin Zykov sur le blog de l'éditeur de sécurité.

Toujours selon le chercheur en sécurité, Cutlet Maker a été repéré dès juin 2016. Et serait lui-même une amélioration de Tyupkin qui avait sévit en 2014. C'est dire que les attaques logicielles de distributeurs de billets ne datent pas d'hier.

Cutlet Maker avait été vendu (5000 dollars) à partir de mai 2017 sur AlphaBay, la place de marché du Dark Web démantelée par les autorités américaines en juillet dernier.

Un malware qui a mué

Visiblement, le malware a su rebondir. Et s'améliorer.

Alors que la version étudiée par Kaspersky exploite 3 fichiers (Cutlet Maker, Stimulator et c0decalc, un générateur de code permettant de débloquer l'usage du logiciel), cette nouvelle mouture du malware disponible sur ATMjackpot se passerait du générateur de code, rapporte *Bleeping Computer*.

Le « nouveau » Cutlet serait vendu l'équivalent de 1500 dollars en bitcoins. Un tarif appelé à doubler au fil des mois poussant l'acheteur à passer à l'action très rapidement pour rentabiliser son investissement.

Kaspersky signale que Cutlet Maker est sans incidence sur les comptes et données des particuliers.

L'éditeur russe en profite pour rappeler que sa solution Embedded Systems Security *« aide à renforcer le niveau de sécurité des distributeurs de billets »*.

Mais, selon un rapport de Embedi, une société spécialisée dans la sécurité des systèmes embarqués, il est possible de contourner le dispositif de sécurisation proposé par Kaspersky.

(Photo credit: kohlmann.sascha via VisualHunt / CC BY-SA)

Lire également
Windows 10 : les distributeurs de billets s'y mettent enfin
95 % des distributeurs de billets sont encore sous Windows XP