Un logiciel malveillant caché dans le chargeur d’une cigarette électronique

Un logiciel malveillant caché dans le chargeur d’une cigarette électronique

Selon des experts interrogés par The Guardian, si le véhicule de l’attaque est inédit, l »anecdote » en elle-même n’a rien de surprenante : les différents supports USB sont fréquemment à l’origine de virus informatiques.

Décidément, on ne peut plus se fier à rien de nos jours ! The Guardian rapporte l’histoire d’un cadre d’une grande entreprise qui s’est fait piéger par un logiciel malveillant codé dans son chargeur de cigarette électronique. »L’ordinateur d’un des cadres était infecté par un logiciel malveillant dont la source ne pouvait être déterminée. Le système était à jour, avait un antivirus et disposait de tous les dispositifs anti-malwares. […] Au final, après avoir cherché du côté de tous les moyens d’infection traditionnels, le service informatique a cherché d’autres possibilités. Ils ont demandé au cadre: « Y a-t-il des changements dans votre vie récemment? » Et le cadre a répondu: « oui, j’ai arrêté de fumer il y a deux semaines et me suis mis à la cigarette électronique », témoigne un membre du personnel informatique de l’entreprise en question sur le site Reddit.

Selon des experts interrogés par The Guardian, si le véhicule de l’attaque est inédit, l »anecdote » en elle-même n’a rien de surprenante : les différents supports USB sont fréquemment à l’origine de virus informatiques. Les clefs USB sont d’ailleurs plus difficiles à pirater que les périphériques USB. Pour Pierre-Yves Bonnetain, consultant sécurité informatique interrogé par France Info, il faudrait remonter l’ensemble de la chaîne de production des cigarettes électroniques pour en savoir plus. »La chaîne de fabrication est relativement complexe. A un moment ou à un autre, quelque part dans la chaîne, il est parfaitement possible qu’un des ces soust-traitants approvisionnent des composants qui ont déjà été frabriqués en étant malveillants », explique-t-il.

En août, deux chercheurs allemands, Karsten Nohl et Jakob Lell, ont réalisé une expérience pour montrer comment il est possible de transformer le code qui permet de faire fonctionner le périphérique USB pour installer un virus sur l’ordinateur. La faille, nommée Bad USB, permettait de mémoriser n’importe quelle saisie sur votre clavier : mots de passe, numéros de carte bancaire… Et à l’heure actuelle, il existe malheureusement très peu de solutions pour se protéger de ce type de virus. Morale de l’histoire : évitez d’acheter des contrefaçons qui circulent sur le net !

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.atlantico.fr/atlantico-light/cyber-piratage-logiciel-malveillant-cache-dans-chargeur-cigarette-electronique-1874188.html