Et si PokemonGo prennait en otage votre téléphone portable?

Et si PokemonGo prennait en otage votre téléphone portable?

Les pirates profitent de la frénésie autour de PokemonGo pour tester de nouveaux pièges comme ce cryptolocker aux couleurs de Niantic.

Est-ce vraiment une surprise ? Pas vraiment en fait ! Un pirate informatique, qui semble être originaire du Maghreb, a lancé un faux PokemonGo que certains internautes n'auraient jamais du attraper. C'est le chercheur Michael Gillespie qui a mis la main sur ce malveillant.

Ce PokemonGo pirate, signé par ce qui semble être un jeune algérien, est capable de chiffrer toutes les données du téléphone piégé, de les télécharger vers le serveur du pirate et d'ouvrir une porte cachée dans le smartphone, histoire que le voyou 2.0 réussisse à s'infiltrer tranquillement dans l'appareil. D'après l'équipe Bleeping Computer, ce ransomware semble préparer une campagne de diffusion à grande échelle. Un ransomware qui utilise un kit dédié aux cryptolockers vendu dans le blackmarket. Heureusement, il est assez basic.

En attendant, ce cryptolocker touche les appareils sous Windows et bloque la lecture des fichiers : .txt, .rtf, .doc, .pdf, .mht, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .htm, .gif, .png. Le microbe ne vise, pour le moment, que les utilisateurs d'Arabie Saoudite.

En cas d'infiltration, le pirate propose de lui écrire à « ***Vos fichiers ont été chiffrés, le décodage possible via me.blackhat20152015@mt2015.com et je vous remercie d'avance pour votre générosité***« .

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Cryptolocker : Quand PokemonGo prend en otage votre téléphone portable – ZATAZ