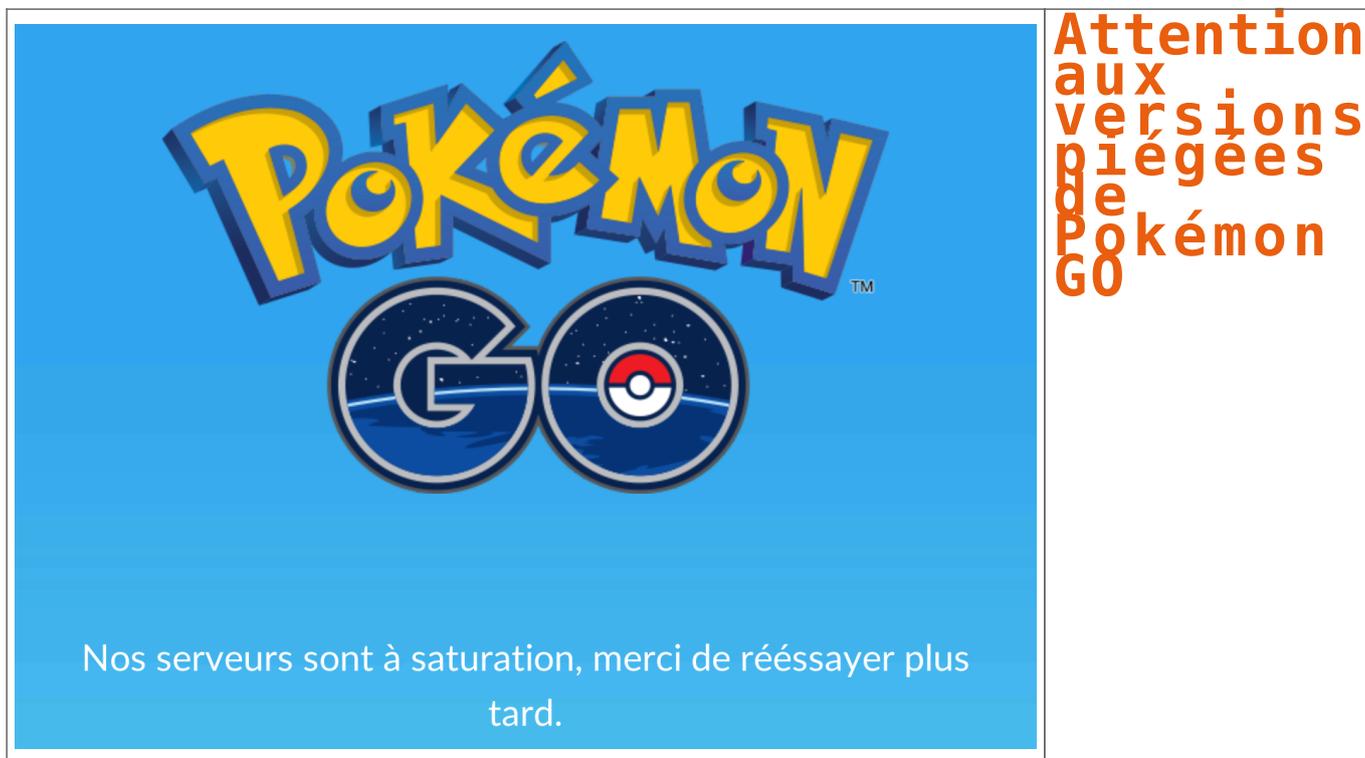


# Attention aux versions piégées de Pokémon GO



**L'application Pokémon Go fait un carton dans les smartphones. Prudence, non encore officiel en Europe, installer le jeu via des boutiques hors de contrôle des auteurs met en danger votre vie privée.**

Pas de doute, le phénomène Pokémon GO débarque en force en cet été 2016. L'application tirée du jeu éponyme de Nintendo permet de s'éclater à trouver des Pokemons un peu partout dans le monde. De la réalité virtuelle bien venue pour l'été.

Édité par Niantic, le créateur de Pokémon GO ne propose son appli qu'aux États-Unis, en Australie et en Nouvelle-Zélande. Un pré lancement pour tester les serveurs, très sollicités, et la stabilité du jeu. Bref, normalement, il n'est pas possible d'y jouer en Europe, et donc en France. Sauf qu'il y a toujours des possibilités, comme celle d'installer Pokémon GO via l'APK (le programme) proposé par de nombreux sites Internet non officiels.

Attention ! des sites qui ne sont pas maîtrisés et contrôlés par les auteurs. Des espaces de téléchargements qui sont des limites du Play Store de Google et de l'App Store d'Apple. Bref, à vos risques et périls.

J'ai déjà pu repérer des APK piégés (ransomwares, cheval de Troie, ...) proposés, je l'avoue, dans des lieux peu recommandables. Prenez l'avertissement très au sérieux. Pokémon GO ne vous demandera JAMAIS d'accéder à vos messages [SMS, MMS], à vos appels téléphoniques. Si l'APK que vous avez téléchargé vous propose ces « autorisations », ne l'installez surtout pas. Attendez la version officielle.

Je ne me voile pas la face, le phénomène attire beaucoup d'internautes, jeunes et moins jeunes. Et avec les vacances, une bonne occasion de sauter sur le jeu pour smartphone de l'été. Des milliers de Français l'ont fait. J'en croise beaucoup, dans la rue, comme le montre ma photographie, prise ce 13 juillet dans les rues de Paris. Je rentre de New York, l'engouement est... pire !



A noter que plusieurs éditeurs d'antivirus ont mis la main sur une version « malveillante » de Pokémon GO. Bitdefender, par exemple, parle de DroidJack. Ce cheval de Troie ouvre une backdoor et donne l'accès aux données des appareils mobiles infectés, permettant ainsi leur prise de contrôle à distance par les pirates. Ce malware disponible pour seulement 200 dollars sur certains sites Web, offre au pirate une interface de contrôle facile à utiliser lui permettant par exemple de surveiller l'activité des appareils corrompus, de passer des appels, d'envoyer des SMS, de localiser l'appareil, d'utiliser l'appareil photo ou le microphone ou même d'accéder aux dossiers.

#### **La version iPhone malmenée par la version officielle**

Autre mise en garde pour les joueurs de Pokémon GO : sur iOS, l'application semble demander plus d'autorisations que nécessaire. L'accès à l'application via un compte Google semble conférer au développeur Niantic (ex Start-up de Google), un accès complet aux comptes des utilisateurs. Ce problème est en cours de résolution et n'est pas présent dans les versions Android.

Article original de Damien Bancal



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : ZATAZ Pokémon GO, prudence  
aux fichiers vérolés – ZATAZ