Conseils pour protÃ©ger un Smartphone Ã Sotchi
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/2/2014 15:00:00

Il aura fallu 7 ans et plus de 37 milliards dâ□□euros pour organiser les Jeux Olympiques d'hiver de 2014 Ã Sotchi, une station balnÃ©aire russe au bord de la Mer Noire. Jamais dans lâ□□histoire des Jeux, autant de force nâ□□aura Ã©tÃ© dÃ©ployÃ©e pour la sÃ©curitÃ© ; certains pays comme les Ã□tats-Unis ont Ã©galement envoyÃ© leurs propres Ã©quipes de sÃ©curitÃ©. MalgrÃ© toutes ces prÃ©cautions, les cyber-criminels russes se prÃ©parent dÃ©jÃ pour les Jeux Olympiques de Sotchi.
Un rÃ©cent reportage de la chaÃ®ne amÃ©ricaine NBC pointait du doigt les risques auxquels sâ□□exposaient les visiteurs se rendant Ã Sotchi : leurs appareils seraient pris pour cible en quelques heures seulement.

MÃªme s'il est vrai que la Russie est un pays Ã haut risque en matiÃ¨re de sÃ©curitÃ© informatique, cela ne signifie pas que les visiteurs se feront pirater dÃ¨s leur descente de l'avion. Lookout prÃ©sente quelques conseils pour protÃ©ger au mieux son Smartphone. En 2013, 62,91% des Smartphones russes Ã©quipÃ©s des solutions Lookout ont Ã©tÃ© confrontÃ©s Ã des logiciels malveillants. C'est le double comparÃ© Ã la Chine (28,45%) et prÃ¨s de 15 fois supÃ©rieur Ã la France (2,8%).

Une stratÃ©gie complexe

A cause dâ□□une surveillance et dâ□□une juridiction plus laxiste, les dÃ©veloppeurs de logiciels malveillants dâ□□Europe de lâ□□Est profitent dâ□□un marchÃ© trÃ¨s lucratif qui est confrontÃ© au plus grand nombre de menaces sur mobile dans le monde.

Les dÃ©veloppeurs de logiciels malveillants russes utilisent des publicitÃ©s qui font Ã©cho de lâ□□actualitÃ© pour attirer leurs victimes.

Les dÃ©veloppeurs de logiciels malveillants russes s'adaptent donc trÃ¨s rapidement aux grands Ã©vÃ©nements qui sont susceptibles dâ□□attirer un large public en maquillant leurs logiciels malveillants avec des images et du texte pour les rendre plus crÃ©dibles.

Puis, grÃ¢ce Ã des outils d'optimisation SEO, ils font remonter leur malware dans les premiers rÃ©sultats des moteurs de recherche.

Si lâ□□on doit se rendre dans un pays comme la Russie pour un Ã©vÃ©nement majeur comme les Jeux Olympiques, une simple recherche sur le terme Â« Jeux Olympiques dâ□□hiver de Sotchi Â» renvoie vers beaucoup de liens malveillants.

ParticuliÃ¨rement ceux qui pointent directement vers un fichier (APK). Câ□□est probablement ce que lâ□□Ã©quipe de NBC a fait et ils sont donc tombÃ©s sur des logiciels malveillants. Afin d'infecter un appareil, les dÃ©veloppeurs malveillants dÃ©sactivent la restriction empÃªchant l'installation de sources non fiables, ce qui permet dâ□□exÃ©cuter le fichier d'installation suspect et au final accepter automatiquement toutes les demandes d'autorisation.

Dans ce cas particulier, ce n'est donc pas le lieu oÃ¹ lâ□□on se trouve qui met l'appareil en danger, mais plutÃ´t le comportement de l'utilisateur.

Comment sÃ©curiser son Smartphone?

Pourquoi les possesseurs de Smartphones russes sont plus exposÃ©s que les franÃ§ais ? Principalement car en France, les utilisateurs passent par les stores officiels Google Play ou AppStore alors quâ□□en Russie beaucoup passent par des forums tels que "4pda.ru" - aprÃ¨s avoir autorisÃ© des sources non fiables.

Donc, pour ceux qui se rendent aux Jeux de Sotchi, il faut rester serein et suivre quelques conseils simples pour protÃ©ger son Smartphone :

1. Ne pas laisser son Smartphone sans surveillance, et avoir un code PIN de verrouillage pour sâ□□assurer que personne ne puisse avoir accÃ¨s Ã son tÃ©lÃ©phone et que des donnÃ©es personnelles tombent entre de mauvaises mains. Activer "Device Encryption" comme un niveau supplÃ©mentaire de sÃ©curitÃ©.
2. Utiliser une application de sÃ©curitÃ© tels que Lookout Mobile Security pour se prÃ©munir des logiciels malveillants et aider Ã le rÃ©cupÃ©rer en cas de perte ou de vol.

3. Ne pas tÃ©lÃ©charger et installer des applications provenant de sites peu fiables, et veiller Ã ce que le rÃ©glage "sources inconnues" reste dÃ©cochÃ©. De mÃªme, ne pas ouvrir les piÃ¨ces jointes de courriels suspects. En cas de doute, vÃ©rifier auprÃ¨s de la personne qui a envoyÃ© ce courriel afin de s'assurer qu'il est authentique et quâ□□il ne craint rien.

4. Nâ□□utiliser le WIFI que sâ□□il est sÃ©curisÃ©, en cas de doute utiliser le rÃ©seau 3G/4G Ã la place.
5. N'utiliser que son chargeur ou le chargeur dâ□□une personne de confiance afin dâ□□Ã©viter les faux chargeurs programmÃ©s pour voler des donnÃ©es.
6. Utiliser un bootloader ou craquer son appareil uniquement si lâ□□on est sÃ»r de ce que lâ□□on fait et prendre les prÃ©cautions nÃ©cessaires dans un pays Ã haut risque.

Â