

Et si charger la batterie de son smartphone via un port USB était dangereux ?



Et si charger la batterie de son smartphone via un port USB était dangereux ?

On s'est tous probablement retrouvés un jour ou l'autre dans une situation où il nous restait peu de batterie sur notre téléphone et que nous n'avions pas de chargeur à portée de main. Le pire, c'est ce que ça nous est arrivé au moment même où on en avait le plus besoin, comme attendre un appel important, un message ou un e-mail, etc.



Il paraît donc tout à fait normal de chercher une source d'électricité à proximité lors d'une telle situation, par exemple utiliser un port USB. Mais est-ce bien sûr ? Non, en réalité cela peut s'avérer dangereux. Via une connexion USB, n'importe qui peut s'emparer de vos fichiers, infecter votre smartphone d'un virus ou même le rendre inutilisable.

Chevaucher la foudre

Avant d'aborder le problème des hackers, il est important de préciser que toutes les sources d'électricité ne sont pas forcément bonnes pour votre téléphone. Il existe beaucoup de plaintes sur Internet, principalement d'utilisateurs tentant de charger leur téléphone dernier cri en les connectant à des adaptateurs ou des chargeurs d'occasion (ou non originaux). Dans certains cas, les téléphones ont été rendus inutilisables. Dans certains cas encore plus étranges, des personnes prenant leur téléphone alors qu'ils étaient en charge ont été sérieusement blessées ou même tuées.

Follow

Daily Mail Online

MailOnline

Teen dies after being electrocuted in her sleep while charging her iPhone <http://dailymail.co.uk/1076145>

2:18 PM - 31 Jul 2014



Teenager was electrocuted in her sleep while charging her iPhone

A 18-year-old woman has died in Xinjiang, China, after being electrocuted in her sleep while charging her iPhone 4s. It is not known if she was using an authentic Apple phone charger.

dailymail.co.uk

.

.

148140 Retweets

.

2424 Likes

Malheureusement, il s'agit plus que de simples accidents. Par exemple, l'année dernière un appareil a été baptisé à juste titre : le tueur USB. Il contenait un impressionnant ensemble de condensateurs hébergés dans une carte mémoire flash USB, qui déchargeait 220 V dans le port USB auquel il était connecté. Une telle décharge pourrait dans le meilleur des cas détruire le port USB et dans le pire sans doute la carte mère de tout l'ordinateur. Nous doutons que vous souhaitiez tester la durabilité de votre téléphone de cette façon.

Montrez-moi vos fichiers

Deuxièmement, les ports USB n'ont pas été conçus uniquement pour la charge, mais aussi pour transférer des données. Les téléphones consommant le plus de données sont ceux conçus sur la plateforme Android 4 x et les versions antérieures, ils se connectent sur le mode MTP (Media Transfer Protocol) par défaut, exposant tous les fichiers de l'appareil.

En moyenne, il faut plus d'une centaine de kilo octets de données rien que pour le système hôte des fichiers et dossiers du téléphone. Pour vous donner une idée, il s'agit de la taille d'une copie de l'e-book d'Alice au pays des merveilles.

Bloquer votre téléphone vous éviterait de courir un tel risque mais honnêtement seriez-vous prêt à vous passer de votre téléphone pendant qu'il est en charge ? Et à toujours le débrancher du port USB lorsque vous recevez un message par exemple ?

A présent, jetons un coup d'œil de plus près aux données qui sont transmises du port USB même lorsque le mobile est en mode (bloqué) » charge seule = . La taille de ces données varie, dépendant de la plateforme du mobile et du système d'exploitation de l'hôte. Mais dans tous les cas, il s'agit plus que d'une » simple charge » . Comme nous l'avons découvert, ces données incluent le nom du mobile, le nom du fournisseur et le numéro de série.

Accès complet et au-delà

Vous devez sûrement penser que vous ne voyez pas où est le problème, seulement il y en a un, puisque nous avons trouvé en cherchant des informations accessibles au public qu'un fournisseur en particulier autorise beaucoup plus que ce qui est spécifié par le système.

Comment est-ce possible ?

Cela est rendu possible via un ancien système de commandes appelées commandes AT. Ces dernières ont été développées il y a quelques dizaines d'années afin de permettre les communications des modems et ordinateurs. Plus tard, elles ont été intégrées au standard du GSM et désormais sont toujours utilisées sur les smartphones.

Pour vous donner une idée de l'usage des commandes AT, laissez-moi vous donner quelques exemples que nous avons été en mesure de découvrir à la surface d'Internet : elles permettent à un hacker d'obtenir votre numéro de téléphone et de télécharger les contacts enregistrés dans la carte SIM. Ces commandes permettent d'établir un appel à n'importe quel numéro, et ce à vos frais, bien entendu. Et si vous êtes en roaming, de tels appels inattendus peuvent vite faire grimper la facture. Dépendant du vendeur, le mode du roaming peut faciliter l'accès à un hacker d'installer n'importe quel type d'applications, y compris malveillantes.

Tout ce qu'on vient de mentionner est possible, même si votre smartphone est bloqué !

En résumé, ne vous fiez pas aux apparences d'un port USB car il pourrait bien » cacher des choses » . Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchiez.

Article de Alexey Komarov



Dans Le Net Expert est Expert Informatique assermenté spécialisé en cybersécurité et en protection des données personnelles.

• Expertises techniques (virus, spywares, phishing, Rootkits, attaques Internet...) et judiciaire (procédureurs téléphoniques, dossier de plainte, contenus, détournement de clientèle...)

• Expertises de systèmes de vote électronique ;

• Formations et conférences en cybersécurité ;

• Formateur de C.I.A. (Correspondants Informatique et Libertés) ;

• Accompagnement à la mise en conformité ONL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : *Les dangers de charger la batterie de son smartphone via un port USB – Kaspersky Daily – | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.*