500 % des tentatives dâ□□attaques malveillantes sur les mobiles
Internet
PostÃ© par : JulieM
PubliÃ©e le : 11/3/2022 13:00:00

Les Ã©quipes de recherche Proofpoint ont dÃ©tectÃ© depuis fÃ©vrier 2022 une augmentation de 500 % des tentatives dâ□□attaques par logiciels malveillants sur les tÃ©lÃ©phones portables Ã travers lâ□□Europe.

Alors que les attaques smishing (phishing par SMS) avaient diminuÃ© fin 2021, celles-ci sont en constante hausse depuis le dÃ©but de lâ□□annÃ©e 2022, particuliÃ¨rement au mois de fÃ©vrier.

â□¢ Ces attaques impliquant des logiciels malveillants ne concernent plus seulement les vols dâ□□identifiants. Elles sont dÃ©sormais capables dâ□□enregistrer des fichiers audio et vidÃ©o (appels inclus), traquer la gÃ©olocalisation, dÃ©truire des donnÃ©es et effacer des contenus. Certains logiciels malveillants tels que FluBot peuvent mÃªme envoyer des textos ou passer des appels. Dâ□□autres, comme TianySpy, contrÃ´lent, surveillent ou encore modifient les accÃ¨s WIFI.

â□¢ Le smishing se dÃ©cline dans toutes les langues et sâ□□adapte Ã toutes les rÃ©gions du monde. Les zones les plus touchÃ©es restent lâ□□Europe et lâ□□AmÃ©rique du Nord.
â□¢ La plupart des logiciels malveillants se propagent par le biais de fausses applications tÃ©lÃ©chargÃ©es sur les App Store, en particulier ceux qui autorisent le tÃ©lÃ©chargement provenant de parties tierces comme le Play Store dâ□□Android.

â□¢ Les techniques dâ□□ingÃ©nierie sociale pour tromper lâ□□utilisateur Ã©voluent constamment et la sensibilisation aux risques de smishing et logiciels malveillants sur mobile est primordiale. La premiÃ¨re Ã©tape est dâ□□installer un anti-virus.

Jacinta Tobin, vice-prÃ©sidente de Cloudmark Operations dÃ©clare : Â« Les utilisateurs de smartphones doivent se montrer extrÃªmement prudents face aux SMS provenant de sources inconnues. Et il est primordial de ne jamais cliquer sur les liens inclus dans des textos, mÃªme s'ils semblent rÃ©alistes.

Si vous souhaitez contacter le prÃ©tendu vendeur qui vous envoie un lien, faites-le directement sur son site Internet et saisissez toujours manuellement l'adresse web/URL. Concernant les codes d'offres promotionnelles, saisissez-les Ã©galement directement sur le site. Enfin, il est essentiel de ne jamais rÃ©pondre aux SMS provenant de sources inconnues. Ce faisant, vous confirmerez souvent aux futurs escrocs que vous Ãªtes une personne rÃ©elle. Â»

Pour plus dâ□□***information*** Ã propos des logiciels malveillants dÃ©tectÃ©s par Proofpoint sur les tÃ©lÃ©phones portables.