Les applications mobiles nous mettent-elles en danger ?

Données confidentielles, malwares ou encore « applications grises », nous sommes tous confronté à ce langage technique devant lequel bien souvent notre absence de connaissances nous rend vulnérable et désarmé. OpinionWay fait le point sur la sécurité des applications mobiles et ses limites.

Le marché des applications mobiles se déploie constamment. Les revenus générés dépasseront 77 milliards de dollars en 2017, tandis que 9 applications mobiles téléchargées sur 10 sont gratuites. Avec ce fort développement, la protection des consommateurs devient de plus en plus complexe. Car le nombre d'applications malveillantes ne cesse de se développer. OpinionWay, dans une étude réalisée pour le spécialiste de la sécurisation des terminaux mobiles Pradeo, fait le point sur la sécurité des applications mobiles et ses limites.

La confidentialité de nos données mise à mal

Les menaces que nous rencontrons de nos jours sont majoritairement des « screenloggers » (51%) et des Chevaux de Troie (33%). Les « screenloggers » sont des technologies qui permettent de faire des captures d'écran du smartphone à l'insu des utilisateurs, dans le but de récupérer des images contenant des informations confidentielles. Le Cheval de Troie, très connu dans le domaine de la cybersécurité, sert à récupérer le maximum de données confidentielles concernant l'utilisateur.

À l'avenir, nous devrons faire face à de nouveaux malwares. Parmi eux, l'intercepteur OTP (one-time-password), qui cible les transactions marchandes nécessitant une validation de paiement par la saisie d'un code OTP. L'objectif

du pirate est alors de récupérer ce code à l'insu de l'utilisateur et de sa banque. Egalement, le Ransomware, qui prend clairement le mobile en otage en chiffrant son contenu. Enfin, le phénomène « d'apps grises », qui devient de plus en plus problématique. Pour ce type d'application, il n'y a pas vraiment de règles préétablies. C'est le consommateur ou l'entreprise qui doit discerner, selon ses propres règles, si l'application en question est malveillante ou acceptable. La menace devient donc subjective.

Les apps, une source de danger pour 69 % des Français

D'après l'étude OpinionWay, 80% des Français enregistrent des données confidentielles voire très confidentielles sur leurs smartphones. Pourtant, plus de la moitié d'entre eux n'ont pas confiance dans leurs applications.

Et pour cause ! Les analyses démontrent que sous Android, 30% des applications récupèrent des données relevant de la vie privée de l'utilisateur. Parmi celles-ci, des informations sur le matériel (62,6%), les identifiants du terminal (56,9%) ou encore des fichiers de l'utilisateur (48,9%). Dans la catégorie des applications les plus dangereuses on retrouve celles dédiées aux jeux, au divertissement et les utilitaires.

L'anti-virus est mort

« L'antivirus est mort », tel est le constat de Brian Dye, ancien VP Information Security chez Symantec qui estime que le modèle des apps a rendu obsolète l'approche classique des antivirus. Dans un livre blanc lié à l'étude Opinion Way, Pradeo met le doigt sur les deux raisons principales qui sont à l'origine de cette inefficacité des antivirus :

- Le « modèle apps » impose une instantane?ite? dans la re?ponse de se?curite? : lorsqu'un utilisateur te?le?charge une application, il l'utilise imme?diatement apre?s. Il est inutile de savoir qu'il s'agit d'un malware quelques semaines apre?s son utilisation. Or dans les me?canismes mis en œuvre par les antivirus, la de?tection d'un malware, puis la ge?ne?ration d'une signature virale et enfin la re?ponse de protection, forment un cycle beaucoup trop long pour faire face aux menaces instantane?es et aux cycles courts des applications mobiles.
- Le « mode?le apps » impose e?galement une subjectivite? dans l'analyse de se?curite? : le fait qu'une application re?cupe?re un nume?ro de te?le?phone ou une ge?olocalisation peut e?tre conside?re? comme acceptable par certains et inadmissible par d'autres. La caracte?risation d'une menace devient donc subjective. Face à cela l'antivirus ne fournit aucune re?ponse car dans son code ge?ne?tique la re?ponse de se?curite? est force?ment globale et ne laisse pas de place a? la personnalisation des re?gles au contexte propre de l'entreprise.

La sécurité des applications en entreprise est-elle vraiment respectée ?

Mais aujourd'hui, la menace ne proviendrait pas uniquement des applications mobiles. Dans la catégorie des applications « métier », près de 40% des salariés adoptent un comportement suspect qui représente une menace pour leurs vies privées et près de 20% d'entre eux mettent en danger la sécurité de leurs terminaux et de son contenu. Pourtant 53% des sondés pensent que leur entreprise a déjà fait le nécessaire pour les protéger et pour se protéger des menaces liées à la mobilité.

Alors que les exigences de sécurité des entreprises se font plus fortes, car ces applications accèdent à leurs systèmes d'information, plusieurs d'entre elles comme Pradeo font de la chasse aux pirates mobiles leurs activités principales. Une application dédiée à évaluer la fiabilité de ses compères pourrait-elle voir le jour ?