

Les mobiles sous Java 2 Me en danger selon ISS

On le sait, les menaces virales pourraient se développer sur les mobiles, à mesure que ces terminaux ressemblent de plus en plus à des mini-PC connectés à haut débit.

Jusqu'à aujourd'hui, les virus mobiles n'ont pas fait beaucoup de mal. Ils ont surtout démontré leur existence et leur capacité à nuire.

Si les premiers virus observés s'attaquaient en priorité aux terminaux sous Symbian et au protocole Bluetooth, les éditeurs de sécurité repèrent désormais des chevaux de Troie visant spécifiquement les mobiles compatibles Java.

Après Kaspersky il y a quelques mois, c'est aujourd'hui ISS qui constate « *la multiplication des menaces visant les téléphones mobiles et assistants numériques équipés de Java 2 Me* »

De plus en plus utilisé par les constructeurs de téléphonie mobile pour des applications évoluées telles que la consultation des emails, des jeux interactifs ou la navigation internet (WAP), Java 2 Me permet l'accès au système de fichiers et l'installation d'applications, explique ISS. Les bibliothèques de code nécessaires à ces opérations sont de plus disponibles en accès libre sur les sites Internet de développeurs.

Internet Security Systems met donc en garde les utilisateurs contre les vulnérabilités nées de l'évolution du système d'exploitation intégré.

Selon lui, ces vulnérabilités sont d'ores et déjà exploitées à travers des codes malveillants qui prennent la forme de composants logiciels à télécharger mis à disposition sur des forums, soit en tentant d'accéder directement au système d'exploitation du téléphone mobile ou de l'assistant personnel via la fonction de connexion Bluetooth.

En mars dernier, cette hypothèse a été confirmée par l'apparition du cheval de Troie Redbrowser. Sous prétexte de simplifier l'accès à des sites WAP, ce code malveillant envoie à l'insu de l'utilisateur des messages vers des services SMS fortement surtaxés.

Pour autant, il faut tempérer le discours toujours alarmiste des éditeurs de sécurité. L'apparition de Redbrowser par exemple n'a pas été suivie d'une diffusion massive. Car comme le rappelle le site Vulnerabilite.com, en fonction des équipements et des versions, Java gère ou non la connexion Bluetooth. Ce qui tend aujourd'hui à réduire fortement la probabilité de diffusion d'un tel ver/virus utilisant Java et Bluetooth.