Des smartphones Android vendus en ligne avec des malwares préinstallés

« Nous observons depuis l'année dernière une nette augmentation du nombre d'appareils qui sont livrés directement avec des programmes malveillants et d'espionnage », alerte Christian Geschkat, responsable des solutions mobiles chez G-Data à l'occasion du Mobile Malware Report du deuxième trimestre 2015. Si l'année dernière, le smartphone Star N9500 avait défrayé la chronique pour les spywares qu'il hébergeait par défaut, l'éditeur de sécurité allemand a dénombré cette fois pas moins de 21 terminaux Android affectés par la présence de malwares avant même de sortir de leur boîte.

Si la plupart sont des modèles «exotiques» chinois (voir liste en bas d'article), le MI3 de Xiaomi, le G510 de Huawei ou encore le S860 de Lenovo sont également concernés par les infections. G-Data écarte toutefois toute pratique malhonnête des constructeurs. *« Des entreprises de renom ne risqueront pas leur réputation en distribuant des malwares dans le firmware »*, estiment les auteurs du rapport. L'éditeur soupçonne plutôt les intermédiaires qui *« en plus de leur marge sur la revente de l'appareil, tablent sur des revenus complémentaires via la commercialisation de données personnelles et la publicité ciblée »*. Autrement dit, tous les modèles concernés et vendus en ligne ne sont pas systématiquement infectés. Tout dépend de l'intégrité de la chaîne des fournisseurs par lesquels ils sont passés. Mais d'autres modèles que ceux de la liste de G-Data pourraient également être concernés. Visiblement, le phénomène se limite néanmoins aux appareils de marques chinoises.

Des malwares dans des applications légitimes

Le résultat n'en reste pas moins problématique puisque les terminaux affectés peuvent ainsi être totalement contrôlés à distance par un tiers. De plus, les agents malveillants se cachant dans des applications légitimes, comme Facebook, il est difficile de les déceler. Et de les supprimer. Pour les utilisateurs concernés, l'affichage intempestif de publicités constituera un moindre mal par rapport à l'installation d'applications non désirées, l'envoi de SMS surtaxés, le contrôle de la caméra à distance ou encore la copie de toutes les données du téléphone. Les utilisateurs pourront vérifier l'intégrité de leur smartphone avec l'application G-Data Internet Security light, la version gratuite de l'antivirus de l'éditeur allemand, téléchargeable depuis Google Play… avec pour conséquence de lui livrer une partie de leurs données (posséder un compte est obligatoire pour activer le logiciel).

Sauf à convaincre les constructeurs de faire le nettoyage dans leur chaine de distribution, cette pratique risque de s'étendre. G-Data suspecte d'ailleurs que les cybercriminels exploitent les logiciels espions créés par Hacking Team, à l'origine au profit des agences gouvernementales. Début juillet, la société de sécurité révélait avoir été victime d'un piratage et ses codes sources se sont retrouvés dans la nature. Des informations que le groupe de pirates Darkhotel n'a pas hésité à mettre à profit en tirant parti des failles décelées par l'éditeur de sécurité italien.

2 millions de nouveaux malwares Android en 2015

Au-delà de ce phénomène inquiétant, le rapport de G-Data révèle un nombre de malwares en hausse de 27 % entre le premier et le second trimestre 2015. Pas moins de 560 671 nouveaux logiciels malveillants sur plate-forme Android ont été découverts au cours du trimestre. Et plus d'un million rien que sur le premier semestre. A ce rythme, le seuil des 2 millions de nouveaux malwares Android devrait être allégrement dépassé sur l'année 2015.

** Xiaomi MI3, Huawei G510, Lenovo S860, Alps A24, Alps 809T, Alps H9001, Alps 2206, Alps PrimuxZeta, Alps N3, Alps ZP100, Alps 709, Alps GQ2002, Alps N9389, Andorid P8, ConCorde SmartPhone6500, DJC touchtalk, ITOUCH, NoName S806i, SESONN N9500, SESONN P8 et X i d o X1111.*

Lire également

Gunpoder : encore une nouvelle famille de malwares pour Android
Le mediaserver d'Android : un nid de failles de sécurité
Une faille Android permet de remplacer une application légitime par une autre

crédit photo © smex – Fotolia.com