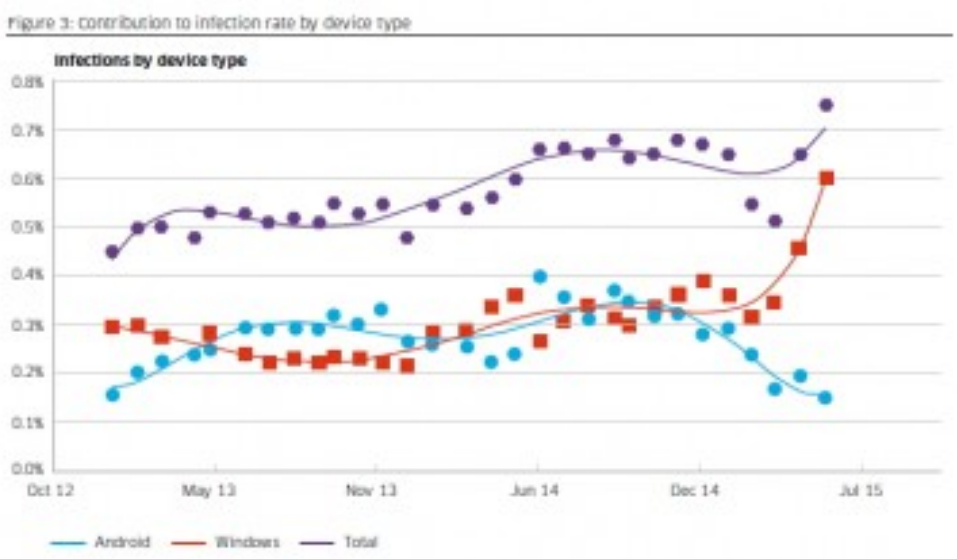
Le nombre de smartphones Android infecté s'affiche à la baisse

S'il ne se passe presque pas un jour sans qu'un nouveau malware mobile apparaisse dans les stores alternatifs, il ne faudrait pas négliger le dynamisme des infections qui touchent toujours les PC Windows et les interactions entre les deux environnements. C'est l'objectif qui anime les experts des Motive Security Labs d'Alcatel-Lucent. Lesquels s'appuient sur la plate-forme Motive Security Guardian qui surveille le trafic de plus de 100 millions de terminaux, fixes et mobiles, dans le monde pour prendre la température de la tendance du moment.

Selon les données ainsi recueillies sur le premier semestre 2015, 80% des infections touchant le réseau mobile proviennent… des PC Windows connectés en Wifi, via des clés USB d'opérateur ou en se servant d'un smartphone comme modem cellulaire. C'est d'ailleurs la faute à Windows (ou plus exactement aux agents malveillants qui y tournent) que le taux d'infection mobile est monté à 0,75% au deuxième trimestre alors qu'il avait baissé à 0,50% au premier contre 0,68% fin 2014 avec la réduction du nombre de terminaux Android affectés.



Windows a la faveur des cybercriminels

Les appareils sous Windows *« ont toujours la faveur des cybercriminels professionnels inconditionnels qui ont un énorme investissement dans l'écosystème de logiciels malveillants Windows*, souligne le rapport. *Comme le réseau mobile devient le réseau d'accès principal pour de nombreux PC Windows, les logiciels malveillants se déplacent avec eux »*. Windows reste dont la plate-forme d'attaque de choix. Et l'année 2015 le confirme alors qu'en 2013 et 2014, la répartition des taux d'infection étaient équitablement répartie entre les deux plates-formes. Cette évolution s'explique notamment par les efforts de Google à éliminer les malwares de son store Play et l'introduction de la fonctionnalité Verify Apps activée par défaut depuis Android 4.2 Jelly Bean (à condition que l'utilisateur en autorise l'exécution).

Il n'en reste pas moins que les maliciels continuent de s'en donner à cœur joie sur l'environnement mobile de Google (qui concentre 99% des menaces). Les logiciels espions sont particulièrement prisés puisque le rapport en compte 10 parmi les 25 menaces les plus répandues sur smartphones. Souvent distribuées avec des jeux et des logiciels gratuits, ils permettent d'espionner les appels, SMS, déplacements géographique, e-mail, navigation et autre données personnelles.

Un malware qui résiste à la réinitialisation usine

Les équipes de Motive Security mettent particulièrement l'accent sur Stagefright, la vulnérabilité d'Android qui permet de prendre le contrôle du terminal à partir d'une pièce jointe qui s'ouvre automatiquement à la réception d'un MMS. Un malware susceptible de toucher potentiellement 1 milliard de smartphones Android. Si des correctifs sont disponibles (quand ils sont efficaces), ils ne sont pas nécessairement distribués puisque les mises à jour dépendent de la volonté des constructeurs des terminaux et des opérateurs qui les distribuent. En attendant et par sécurité, mieux vaut désactiver l'exécution automatique propre aux fichiers multimédia joints dans un message.

Vol d'identité, chevaux de Troie bancaires, ransomware, SMS surtaxé, publicité indésirable… la diversité des malwares Android est riche. Et en hausse. Le rapport note ainsi que le nombre d'échantillons de malwares a doublé au cours des six premiers mois de 2015. Les experts ne cachent d'ailleurs pas leur inquiétude face à la sophistication améliorée des agents malveillants dans leurs capacités de Command & Contrôle (C&C) et de persistance sur le terminal. Les chercheurs viennent d'ailleurs, pour la première fois, de découvrir un malware capable de résister à une réinitialisation usine du smartphone. Dommage qu'ils n'en fournissent pas (encore) le nom.

Table 1. Top 25 Android malware detected in H2 2014

NAME	LEVEL	%	PREVIOUS
Android.MobileSpyware.Kasandra	High	31.30	New
Android.Adware.Uapush.A	Moderate	28.82	1
Android.Trojan.SmsTracker	High	22.36	3
Android.MobileSpyware.Gappusin	High	2.86	New
Android.MobileSpyware.SpyMob.a	High	2.05	5
Android.Trojan.FakeFlash	High	1.46	7
Android.MobileSpyware.CellSpy	High	0.98	New
Android.MobileSpyware.Tekwon.A	High	0.87	16
Android.Trojan.Wapsx	High	0.86	8
Android.Bot.Notcompatible	High	0.77	6
Android.Trojan.SMSreg.gc	High	0.74	41
Android.MobileSpyware.Phonerec	High	0.55	15
Android.Trojan.Qdplugin	High	0.54	10
Android.ScareWare.SLocker.A	High	0.52	New
Android.MobileSpyware.GinMaste	High	0.47	9
Android.MobileSpyware.Spyoo.C	High	0.39	27
Android.Backdoor.Agent.bz	High	0.34	New
Android.Downloader.Stew.a	High	0.29	New
Android.MobileSpyware.FakeDoc	High	0.28	21
Android.ScareWare.Koler.C	High	0.26	13
Android.Adware.Kuguo.A	Moderate	0.22	18
Android.Backdoor.Advulna	High	0.21	14
Android.MobileSpyware.SpyBubbl	High	0.2	13
Android.Backdoor.Opfake.a	High	0.17	34
Android.Trojan.Cajino	High	0.15	New

Lire également

Google a supprimé la moitié des malwares sous Android en 2014
Neuf malwares sur 10 échappent aux listes noires
Cybercrime : un coût de 2100 milliards de dollars pour les entreprises d'ici 2019

crédit photo : Twin Design / Shutterstock.com