Malwares sur mobiles : les comptes bancaires des internautes ciblÃ©s
Internet
PostÃ© par : JulieM
PubliÃ©e le : 27/2/2014 13:00:00

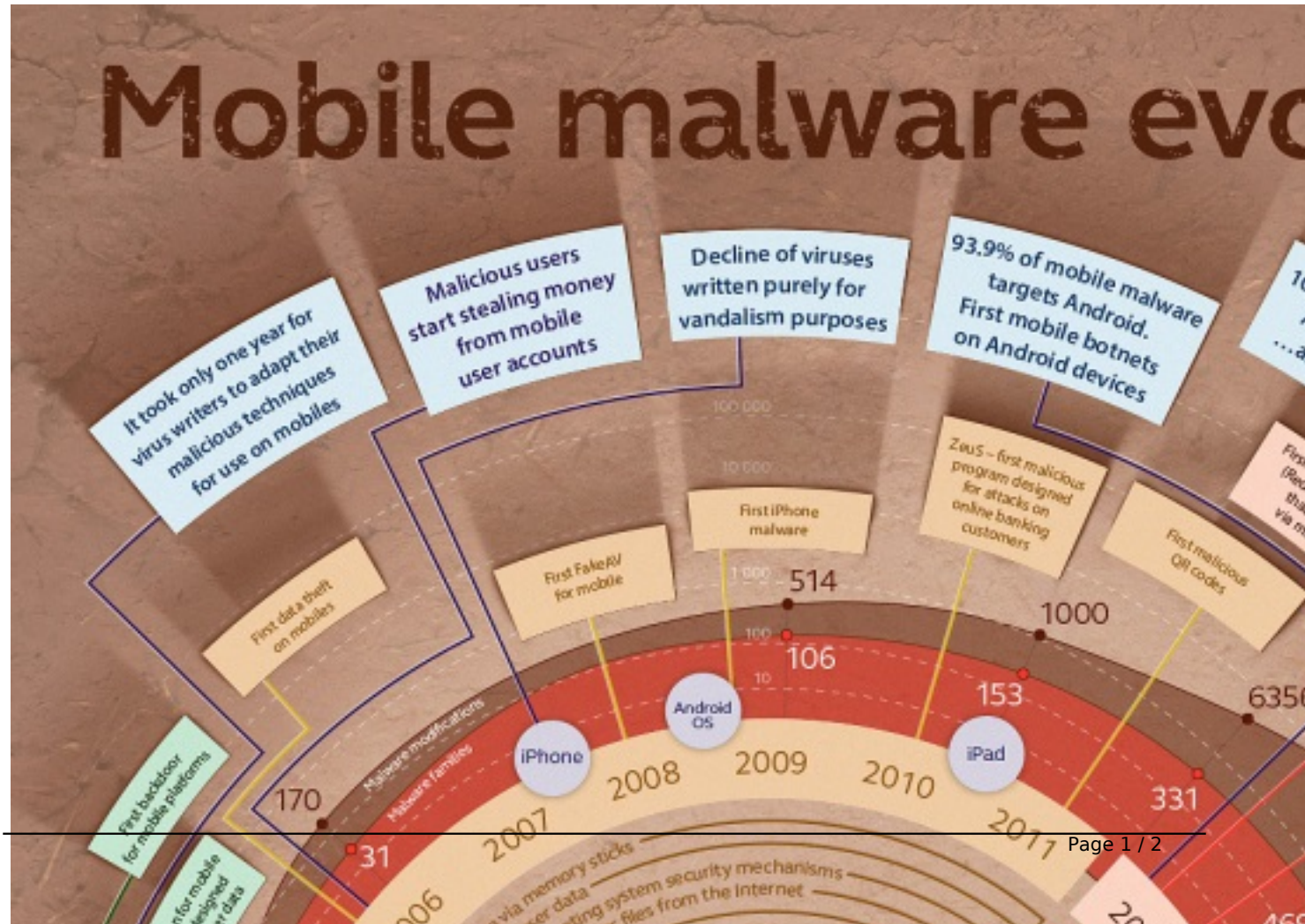
Le nombre de malwares sur mobiles conÃ§ues pour des attaques de phishing, le vol de coordonnÃ©es de carte bancaire et dâargent sur les comptes en banque, a quasiment Ã©tÃ© multipliÃ© par 20.
Les chevaux de Troie bancaires sont de loin les plus dangereux. Entre Janvier et dÃ©cembre 2013, leur nombre sâest multipliÃ© et l'on dÃ©nombrait 67 chevaux de Troie bancaires connus dÃ©but 2013, et Ã la fin de cette annÃ©e-lÃ , la base de donnÃ©es de Kaspersky Lab contenait dÃ©jÃ 1 321 variantes.

Â« *Aujourdâhui, la majoritÃ© des attaques par chevaux de Troie bancaires vise essentiellement la Russie et les autres pays de lâex-URSS. Cependant, cette situation ne devrait pas perdurer : Ã©tant donnÃ© le vif intÃ©rÃªt des cybercriminels pour les comptes bancaires, lâactivitÃ© des chevaux de Troie bancaires sur les mobiles devrait sâintensifier ailleurs dans le monde en 2014. Nous avons dâores et dÃ©jÃ connaissance de Perkel, un cheval de Troie pour Android qui sâattaque aux clients de plusieurs banques europÃ©ennes, ou encore du programme malveillant Wroba en CorÃ©e.* Â» explique Victor Chebyshev, Virus Analyst chez Kaspersky Lab.

Â

Â

Â



Â

Â

Â

Â

Des mÃ©thodes dâ□□infections de plus en plus Ã©laborÃ©es pour mieux tirer profit des contenus des Smartphones

â□¢ Les criminels recourent de plus en plus Ã la technique dâ□□Â« obfuscation Â», qui consiste Ã rendre dÃ©libÃ©rÃ©ment le code malveillant trÃ¨s complexe et donc plus difficile Ã analyser. Une solution antivirus mettra alors plus de temps Ã neutraliser le code laissant assez de temps aux cyber-criminels pour arriver Ã leurs fins.

â□¢ Parmi les mÃ©thodes pour toucher un mobile, on compte dÃ©sormais la contamination via des sites lÃ©gitimes compromis. La propagation du malware se fait par lâ□□intermÃ©diaire dâ□□Â« app stores Â» alternatifs et de Â« bots Â» (ces derniers sâ□□auto-propagent gÃ©nÃ©ralement par lâ□□envoi de textos, contenant un lien malveillant, aux destinataires qui figurent dans le rÃ©pertoire de la victime).

â□¢ Les failles sur AndroÃ¯d sont exploitÃ©es par les cybercriminels pour accroÃ®tre les privilÃ¨ges des applications malveillantes, Ã©viter leur dÃ©tection et compliquer leur nettoyage. Ils utilisent, par exemple, la vulnÃ©rabilitÃ© Master Key pour contourner le contrÃ´le dâ□□intÃ©gritÃ© du code au moment de lâ□□installation dâ□□une application.

En outre, le fait que seule la rÃ©ception dâ□□une mise Ã jour du fabricant permette la correction des vulnÃ©rabilitÃ©s vient encore compliquer la situation. En effet, si un modÃ¨le de Smartphone ou de tablette date de plus dâ□□un an, il est probable que le fabricant nâ□□en assure plus le support, en particulier la correction des vulnÃ©rabilitÃ©s.