

Ces malwares qui n'en veulent qu'à notre porte-monnaie.

Info

Posté par : JPilo

Publié le : 7/2/2013 13:00:00

FortiGuard Labs a étudié des échantillons de malwares qui montrent quatre méthodes typiquement utilisées par les cybercriminels pour soutirer de l'argent à leurs victimes.

En outre, le rapport montre une augmentation de l'activité des variantes de malwares sur mobiles en matière de kits de publicité Plankton sur Android ainsi qu'une hausse des scans de vulnérabilités des serveurs Web par les hacktivistes.

Quatre Malwares permettant de Gagner de l'Argent à Surveiller en 2013

Au cours des trois derniers mois, FortiGuard Labs a identifié quatre épidémies de malwares, montrant des niveaux d'activité élevés dans un délai de temps très court (allant d'une journée à une semaine). Ces derniers représentent quatre méthodes typiquement utilisées par les cybercriminels aujourd'hui pour monétiser leurs malwares:



1. Simda.B: Ce malware sophistiqué se fait passer pour une mise à jour Flash pour inciter les utilisateurs à accepter la totalité des droits d'installation. Une fois installé, le malware vole les mots de passes de l'utilisateur, ce qui permet aux cybercriminels d'infiltrer les comptes des réseaux sociaux et emails de la victime pour spammer ou propager des malwares, d'accéder aux comptes admin des sites Web pour hâberger des sites malveillants et détourner de l'argent des comptes des systèmes de paiement en ligne.

2. FakeAlert.D: Ce faux antivirus signale aux utilisateurs via une fenêtre pop-up d'apparence convaincante que leur ordinateur a été infecté par des virus, et que, moyennant des frais, le

faux antivirus supprimera les virus de l'ordinateur de la victime.

3. Ransom.BE78: C'est un ran'ngiciel (ransomware en anglais), un malware frustrant qui empâche les utilisateurs d'accâder â leurs donnâes personnelles. Typiquement, soit l'infection empâche de dâmarrer la machine de l'utilisateur, soit elle crypte les donnâes stockâes de la machine de la victime, puis exige le paiement pour recevoir la clâ qui lui permettra de les dâcrypter. La principale diffârence entre le ransomware et le faux antivirus est que le ransomware ne donne pas le choix â la victime concernant l'installation. Le ransomware s'auto-installe sur la machine de l'utilisateur puis exige le paiement pour âtre supprimâ du systâme.

4. Zbot.ANQ: Ce cheval de Troie est le composant "du câtâ client" d'une version du fameux kit Zeus. Il intercepte les tentatives de connexion bancaire en ligne de l'utilisateur puis utilise l'ingânierie social pour inciter les utilisateurs â installer un composant mobile du malware sur leurs smartphones. Une fois que l'âlâment mobile est installâ, les cybercriminels peuvent alors intercepter les SMS de confirmation bancaire, et par la suite, transfârer les fonds â un compte de passeur d'argent (money mule en anglais).

*"Bien que les mâthodes de monâtisation des malwares ont âvoluâ au fil des annâes, les cybercriminels semblent aujourdâhui âtre plus ouverts et frontaux dans leurs demandes d'argent â pour des rendements plus rapides," dâclare **Guillaume Lovet**, Responsable Sânior de l'Equipe Râponses aux Menaces FortiGuard Labs de Fortinet. âDorânavant, il ne s'agit pas seulement de voler des mots de passe en toute discrâtion, il s'agit aussi d'intimider les utilisateurs infectâs en les faisant payer. Les mesures de protection âlâmentaires que les utilisateurs peuvent prendre cependant n'ont pas changâ. Ils devraient avoir des solutions de sâcuritâ installâes sur leurs ordinateurs, mettre â jour constamment leurs logiciels avec les derniâres versions et correctifs, effectuer des scans râguliers et faire preuve de bon sens."*

Les Kits de Publicitâs sur Mobiles Android

Dans le dernier rapport sur les principales menaces, FortiGuard Labs a dâtectâ une forte augmentation des kits de publicitâs Plankton sur Android. Cet âlâment de certaines applications intâgre un ensemble d'outils communs qui affichent des publicitâs non dâsirâes sur la barre dâtat du tâlâphone, pistent l'utilisateur â travers leur numâro IMEI (International Mobile Equipment Identity) et ajoutent des icânes sur l'âcran de l'appareil.

Au cours des trois derniers mois, l'activitâ du kit a diminuâ. A la place, FortiGuard Labs a dâtectâ la hausse des kits de publicitâs qui semblent âtre directement inspirâs de Plankton et qui ont atteint le mâme niveau âlevâ d'activitâs que Plankton il y a trois mois.

*"L'activitâ des kits de publicitâs que nous avons observâs indiquent soit, que les auteurs essaient dâviter la dâtection, soit, que d'autres auteurs de Plankton tentent eux-aussi d'avoir une part du gâteau publicitaire. Quoiqu'il en soit, le niveau d'activitâs que nous avons constatâ avec les kits de publicitâs aujourdâhui indiquent que les utilisateurs Android sont trâs ciblâs et donc devraient âtre particuliârement vigilants lorsqu'ils tâlâchargent des applications sur leurs smartphones," dâclare **Guillaume Lovet**.*

Les utilisateurs peuvent se protâger en prâtant une attention particuliâre aux droits demandâs par l'application au moment de l'installation. Il est âgalement recommandâ de tâlâcharger des applications mobiles qui ont âtâ trâs bien notâes et vârifiâes.

L'Outil de Scan des Hacktivistes Passe â la Vitesse Supârieure

Au troisième trimestre de 2012, FortiGuard Labs a détecté des niveaux d'activités élevées de ZmEu, un outil qui a été développé par des hackers Roumains pour scanner les serveurs Web fonctionnant sur des versions vulnérables du logiciel d'administration MySQL (phpMyAdmin) dans le but de prendre le contrôle de ces serveurs. Depuis Septembre, le niveau d'activités a été multiplié par neuf avant de se stabiliser finalement en Décembre.

"Ce pic d'activité indique un regain d'intérêt par les groupes d'hacktivistes pour faciliter les différents mouvements de protestation et activistes dans le monde. Nous nous attendons à ce qu'une telle activité de scans demeure élevée car les hacktivistes mènent de plus en plus de causes et font connaître leurs succès," poursuit **Guillaume Lovet**.