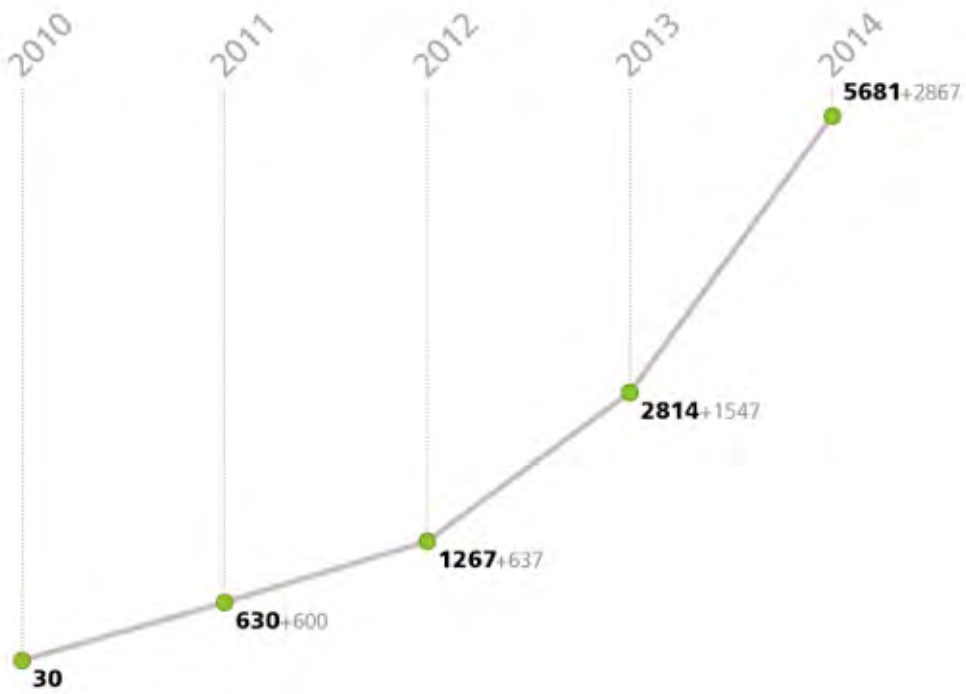
Les vols via les mobiles

Android est le système d'exploitation le plus populaire parmi les utilisateurs des appareils mobiles et malheureusement aussi parmi les cybercriminels puisque c'est l'OS le plus exploité par les pirates après Windows. Les premiers logiciels malveillants ciblant Android sont apparus en 2010.

La plupart des logiciels malveillants ciblant les appareils mobiles sont conçus pour l'OS Android, il est très utilisé et son code est ouvert.

Ce graphique représente le nombre d'entrées dans la base virale Dr.Web.



L'évolution du nombre de menaces en 2014 est de 102% !

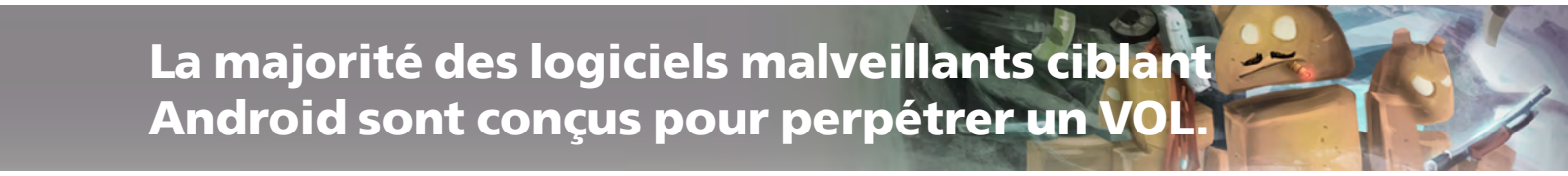
Depuis 2010, le nombre de signatures de malwares ciblant Android a été multiplié par 189!

Le 1er avril 2015, le nombre de signatures ajoutées à la base virale Dr.Web a atteint presque 7 000.

Autrement dit, pour le 1er trimestre 2015, le volume de la base a augmenté de 25% !

Il faut noter qu'à l'aide d'une signature, Dr.Web peut détecter plusieurs logiciels malveillants.

La majorité des logiciels malveillants ciblant Android sont conçus pour perpétrer un VOL.



Les appareils mobiles ont beaucoup de fonctionnalités et les malfaiteurs essaient de voler tout ce qu'ils peuvent voler:

- De l'argent – sur les comptes bancaires, les systèmes de banque en ligne ou carte de crédit,
- les logins et mots de passe pour accéder aux systèmes de banque en ligne, aux comptes sur les réseaux sociaux.
- Des SMS
- Des appels
- Des e-mails
- Des photos – les malfaiteurs peuvent les utiliser afin de faire chanter la victime ou de porter un préjudice moral en les publiant sur Internet.
- Des enregistrements des appels de l'utilisateur, même s'il ne les a pas passés lui-même (le Trojan peut le faire)
- Les adresses des contacts
- Les coordonnées GPS de l'appareil, autrement dit, l'emplacement de son propriétaire et ses déplacements
- Des données techniques sur l'appareil (les identifiants IMEI/IMSI/SID, le numéro de téléphone, la version de l'OS, la version du système SDK, le modèle de l'appareil, les données sur le fabricant de l'appareil)

Dans de nombreux cas, les utilisateurs eux-mêmes, à leur insu, téléchargent et installent sur leurs appareils mobiles des logiciels malveillants !

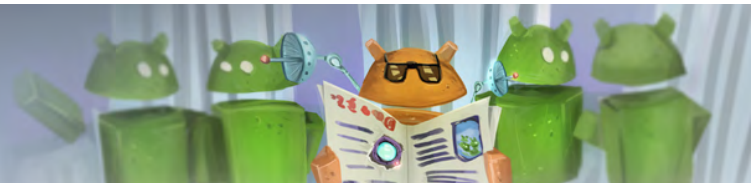
Par exemple, Android.Plankton, conçu pour recueillir les données sur l'appareil infecté a été téléchargé 150 000 fois (!) sur Google Play, avant qu'il ne soit supprimé par l'administration du site.

Selon les statistiques de Dr.Web pour Android, environ 50% de nos utilisateurs ont activé l'option « installer les applications depuis des sources inconnues » (hors de Google Play). Cela signifie que les utilisateurs peuvent installer des applications (parfois malveillantes) téléchargées sur des forums ou des sites douteux.

Les cybercriminels utilisent souvent l'ingénierie sociale pour distribuer les Trojans. Par exemple, **plus de 30 000** utilisateurs sud-coréens ont téléchargé le Trojan bancaire Android.SmsBot.75.origin suite à la réception d'un message relatif à l'état d'un envoi postal.

La plupart des utilisateurs pensent qu'ils remarqueront l'activité d'un Trojan sur l'appareil mobile.

Un bon Trojan est un Trojan invisible pour l'utilisateur.



Il y a longtemps que les malfaiteurs ont appris cette leçon.

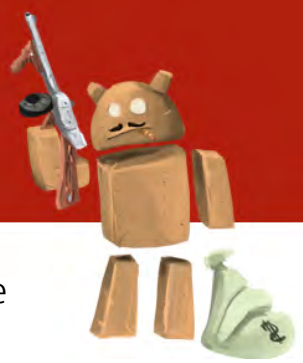
Dans la plupart des cas, les victimes détectent le vol une fois que leur compte est vidé.

- Par exemple, le Trojan dialer Android.Dialer.7.origin désactive le haut-parleur de l'appareil mobile lorsqu'il passe des appels, supprime toutes les données sur ses appels dans le log du système ainsi que la liste des appels pour réduire la probabilité de sa détection.
- Les Trojans qui abonnent les utilisateurs à des services payants peuvent également se masquer sur l'appareil mobile infecté. En règle générale, les services payants envoient des SMS de confirmation de l'abonnement, mais le Trojan peut intercepter ces SMS, ce qui permet de cacher l'abonnement à l'utilisateur. Certains logiciels malveillants peut automatiquement envoyer des SMS avec le code de confirmation pour abonner à des services payants — ces messages sont interceptés et cachés.

- Beaucoup de Trojans sophistiqués se propagent sous couvert de logiciels légitimes puis, après leur lancement, suppriment leur icône et fonctionnent à l'insu de l'utilisateur.
- Parfois les malfaiteurs peuvent intégrer des Trojans au sein du système d'exploitation ou d'images de firmwares. Ces malwares ont donc des privilèges élargis et peuvent exécuter beaucoup d'actions à l'insu de l'utilisateur.
- Pour éviter la détection par les antivirus, certains Trojans peuvent résister à ces logiciels : les logiciel antivirus peuvent être bloqués ou même supprimés complètement de l'appareil.

Trojans bancaires

Ce sont des familles de Trojans conçus pour voler de l'argent sur les comptes bancaires ou les systèmes de banque en ligne.



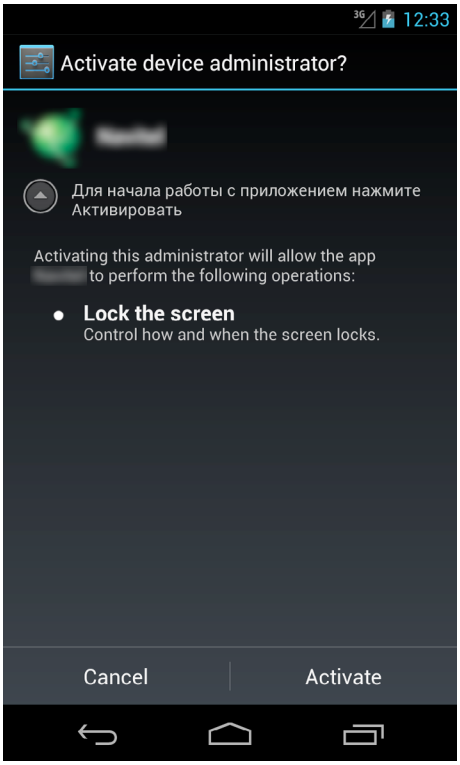
Beaucoup de banques offrent à leurs clients des services de banque en ligne conçus pour Android, notamment. Ils sont utilisés pour les opérations individuelles, mais peuvent également être utilisés par les entreprises. Souvent, ce sont les dirigeants de l'entreprise qui gèrent ces comptes.

Le vol d'argent est une des activités les plus importantes des pirates informatiques.

Android.BankBot.33.origin

Fonctionnalités:

- obtenir les données sur le solde du compte ou la liste des cartes bancaires liées à l'appareil mobile;
- Voler les identifiants des comptes de banque en ligne en téléchargeant dans le navigateur web un site frauduleux qui imite la page de la banque où la victime doit entrer ses données d'accès confidentielles;
- Effectuer des virements du compte de l'utilisateur vers le compte des malfaiteurs.



La victime peut ne pas remarquer le vol durant un certain temps car Android.BankBot.33.origin peut intercepter et bloquer les SMS informant des opérations effectuées.

Les utilisateurs installent souvent eux-mêmes ce Trojan (si la possibilité d'installer des applications téléchargées à partir de toutes sources est activée dans les paramètres du système d'exploitation)!

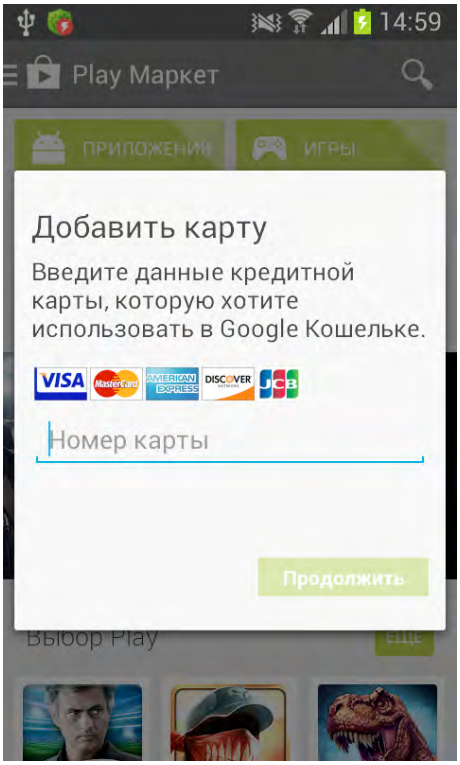
De janvier à avril 2015, ce Trojan a été détecté sur les appareils protégés par Dr.Web Antivirus 62 840 fois.

Android.SpyEye.1

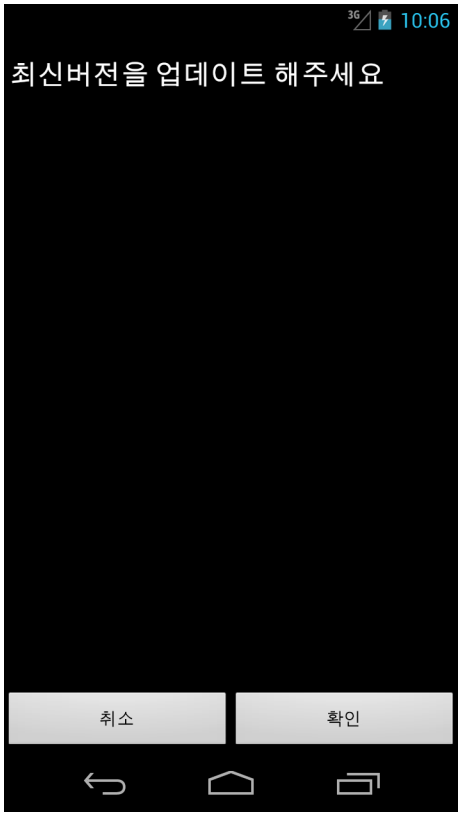
Si l'utilisateur ouvre un site de banque dont l'adresse est enregistrée dans le fichier de configuration du Trojan bancaire qui a infecté le mobile, celui-ci injecte son code dans la page qui peut ensuite afficher un texte ou des formulaires web pour saisir les données d'authentification. De cette façon, la victime trouve sur la page web de sa banque un message d'alerte sur de nouvelles précautions de sécurité devant être suivies. On lui demande de télécharger une application spéciale pour accéder à la banque en ligne. En réalité, ce logiciel contient un Trojan. Ce logiciel malveillant peut intercepter et renvoyer des SMS contenant les mots de passe pour accéder au système de banque en ligne.

Android.BankBot.21.origin

Pour obtenir les données en question et voler de l'argent, le Trojan Android.BankBot.21.origin vérifie si la fenêtre de Google Play est active. Si oui, le Trojan imite le formulaire standard pour lier la carte au compte utilisateur. Les données saisies sont envoyées au serveur appartenant aux malfaiteurs. Le reste est déjà bien connu.



Android.BankBot.29.origin



Le Trojan essaie d'obtenir les droits administrateur, pour ce faire, il masque la requête pour ces droits par une autre fenêtre, c'est pourquoi la victime peut donner les droits administrateur au logiciel malveillant à son insu. Le reste est déjà bien connu.

Le vol des SMS entrants

Le vol de SMS est un vrai problème. Mais tout dépend du but du SMS qui a été envoyé et/ou intercepté par les malfaiteurs.

Quels types de SMS entrants les Trojans volent-ils ?

- Des SMS de confirmation ou de demande de permission de se connecter à des services payants. Ils sont volés pour que la victime ne sache pas, le plus longtemps possible, qu'elle est abonnée à un service payant et pour qu'elle n'effectue pas des actions visant à stopper le fonctionnement du Trojan.
- Des SMS contenant les codes mTAN provenant des systèmes de banque en ligne.

Les SMS volés sont envoyés au serveur de gestion appartenant aux malfaiteurs. Cette fonctionnalité est présente dans les Trojans de plusieurs familles.

Vol d'argent en envoyant des SMS (messages sortants).

Par exemple, les Trojans de la famille Android. SmsSend peuvent prélever de l'argent du compte de la victime en envoyant des SMS payants.

Selon les données recueillies par Dr.Web pour Android, le nombre de détections des Trojans de la famille Android.SmsSend a atteint 20 223 854 en 2014.

Les Trojans de la famille **Android.SmsBot** peuvent envoyer, intercepter et supprimer des SMS.

Selon les données recueillies par Dr.Web pour Android, le nombre de détections des Trojans de la famille Android.SmsBot a atteint 5 985 063 en 2014.

Vol d'argent via des appels à des numéros payants

Les dialers représentent une famille de Trojans Android qui peuvent passer des appels à des numéros payants à l'insu de l'utilisateur. C'est un moyen pour gagner de l'argent assez populaire parmi les malfaiteurs.

Selon les données recueillies par Dr.Web pour Android, le nombre de détections des Trojans de la famille Android.Dialer a atteint 177 397 en 2014.

Vol des adresses des contacts du téléphone

Cela ne porte pas forcément préjudice à l'utilisateur en termes financiers, mais cette activité est néanmoins un vrai business. Tout contact " vivant " peut être vendu, et il existe différentes catégories d'acheteurs.

1. Les spammeurs. Le "Spamming" est une affaire prospère et avantageuse. Et elle n'est pas uniquement liée à l'envoi de publicités.

L'envoi de SMS contenant un lien pour télécharger un logiciel malveillant devient de plus en plus répandu.

Android.Wormle.1.origin peut par exemple être distribué via des SMS parmi les amis du propriétaire de l'appareil mobile infecté. A la fin du mois de novembre 2014, Android.Wormle.1.origin avait infecté plus de 15 000 appareils mobiles sous Android dans 30 pays.

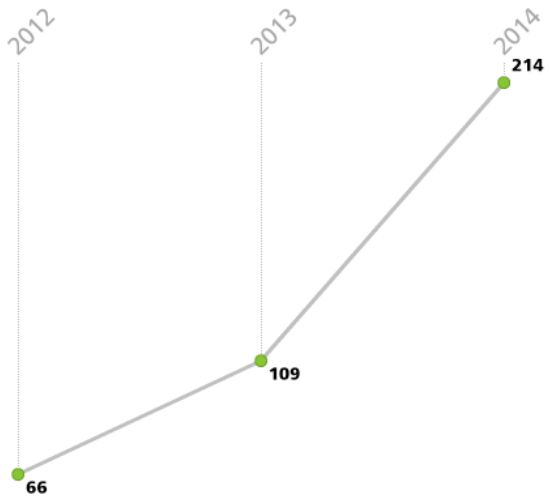
2. Les phishers. Ils recueillent les contacts pour envoyer des emails de phishing contenant des liens vers des sites de banques ou de systèmes de paiement. Si vous allez sur ces sites, le malfaiteur peut obtenir vos identifiants pour accéder à votre système de banque en ligne ou vos données de carte bancaire. Et vous allez vous-même saisir ces données dans les formulaires de phishing en croyant que vous êtes sur le site de la banque.

3. Les organisateurs d'attaques DDoS – ils ont besoin des contacts des propriétaires des appareils mobiles qui peuvent être infectés et utilisés afin de lancer des attaques DDoS.

4. Les espions (services de renseignement, concurrents). Chaque contact représente une source de revenus potentielle pour l'espion ou le maître chanteur. De plus, le gens qui vous surveillent peuvent lire l'historique de vos messages, enregistrer vos appels, télécharger vos photos.

Par exemple, Android.Spy.130.origin vole les données confidentielles comme les SMS, les appels, les coordonnées GPS, il peut également appeler un numéro spécifié qui peut transformer l'appareil infecté en appareil d'écoute.

Evolution du nombre d'entrées pour les Trojans de la famille Android.Spy dans la base virale Dr.Web.



Vous utilisez activement des services

- Google Play
- Google Play Music
- Gmail
- WhatsApp
- Viber
- Instagram
- Skype
- « VKontakte «
- « Odnoklassniki «
- Facebook
- Twitter...?

Les malfaiteurs peuvent utiliser les données de vos comptes pour les vendre ou faire chanter la victime !

Dr.Webprotège les appareils sous Android contre le vol via mobile

Composants de protection

Antivirus
Protection contre les Trojans et autres logiciels malveillants

Antivol
Permet de retrouver le mobile en cas de vol ou de perte et de supprimer à distance les données confidentielles

Antispam
Protège contre les messages et les appels non sollicités

Service Cloud Checker
Permet de restreindre les visites sur les pages web non-sollicitées quel que soit le niveau de mise à jour des bases virales de votre Dr.Web pour Android

Pare-feu
Contrôle l'activité réseau des applications

Contrôleur de sécurité
Analyse le système afin de détecter les problèmes de sécurité et propose des solutions

Liens utiles

Le projet de Doctor Web consacré au "vol via mobile "