



## Communiqué de Presse

### Contact Presse :

Annabelle Sou  
Fortinet, Inc.  
04 89 87 05 76  
[asou@fortinet.com](mailto:asou@fortinet.com)

## Les Recherches de Fortinet sur les Principales Menaces Révèlent le Top 5 des Familles de Logiciels Malveillants sous Android

*La Rapport Dévoile Egalement une Nouvelle Vulnérabilité qui permet de « rooter » un système Android*

Sophia Antipolis, 8 Décembre 2011 — [Fortinet®](#) (NASDAQ: FTNT) - l'un des principaux acteurs du marché de la sécurité réseau et le leader mondial des systèmes unifiés de sécurité UTM (Unified Threat Management) – publie aujourd’hui ses recherches du mois de Novembre. Ce mois-ci, FortiGuard Labs a publié son Top 5 des familles de logiciels malveillants sous Android et a analysé une nouvelle vulnérabilité qui affecte les téléphones Android.

### Le Top 5 des Logiciels Malveillants sous Android

Le 15 Novembre, le cabinet d’analystes Gartner a publié un rapport indiquant que le système d’exploitation mobile Android de Google représente 52.5% de part de marché mondiale des smartphones, tandis que l’iOS se positionne en troisième place, derrière Symbian, avec une part de marché de 18%. FortiGuard Labs a trouvé intéressant la disparité entre la quantité de logiciels malveillants détectés sur le système d’exploitation Android par rapport à ceux trouvés sur l’iOS compte tenu de leurs parts de marché respectives.

*“La quantité de familles malveillantes trouvées par FortiGuard Labs sur l’OS Android est environ cinq fois supérieure à celles que nous avons trouvé sur l’iOS,”* déclare Axelle Apvrille, chercheur senior anti-virus sur mobiles chez Fortinet. *“Nous pensons que cette disparité peut*

*être due à la manière dont Apple gère le développement et la distribution des applications iOS. Contrairement à Android, qui facilite la mise à disposition des applications pour le téléchargement par les utilisateurs, l'iOS exige que les développeurs se soumettent à certaines procédures strictes d'Apple avant que l'application puisse être accessible sur l'Apple Store. Cela ne veut pas dire qu'Apple soit totalement à l'abri de logiciels malveillants – le ver bancaire Eeki le prouve - mais cela explique pourquoi nous voyons si peu d'activité sur la plateforme iOS.”*

*“Malheureusement, nous croyons que la part de marché élevé d'Android et que son environnement de développement ‘open source’ ont un prix” poursuit Axelle Apvrille. “A ce jour, nos Labs ont vu une augmentation de 90% de familles de logiciels malveillants sur Android en 2011 par rapport à 2010, tandis que les familles malveillantes iOS n'ont augmenté seulement que de 25%. Bien sûr, ces statistiques ne tiennent pas compte des taux d'infection ou de dangerosité.”*

Le Top 5 des familles de logiciels malveillants pour lesquelles FortiGuard Labs a reçu le plus d'échantillons en 2011 sont :

- Geinimi: le premier botnet Android, qui envoie la localisation géographique de la victime et contrôle son téléphone à distance. Par exemple, Geinimi peut forcer le téléphone infecté à appeler un numéro de téléphone en particulier.
- Hongtoutou: un cheval de Troie sous forme de fond d'écran qui vole des informations privées telles que le numéro d'abonné de la victime (IMSI) et se rend automatiquement sur les sites Internet sur lesquels le logiciel malveillant le dirige.
- DroidKungFu: Un autre botnet qui a des capacités multiples telles que l'installation d'autres logiciels malveillants à distance, le démarrage d'applications spécifiques et l'ajout de pages dans la liste des favoris.
- JiFake: Une fausse application de messagerie instantanée qui envoie des SMS à des numéros surtaxés
- BaseBridge: Un cheval de Troie qui envoie des SMS à des numéros surtaxés

Les logiciels malveillants ci-dessus ainsi que d'autres sont détectés par les machines antivirus de Fortinet. Notons également que des logiciels malveillants tels que BaseBridge ont été disponibles sur l'Android Market mais ont ensuite été retirés. Le plus souvent, les logiciels malveillants essaient de se faire passer pour une véritable application. Cependant, des logiciels malveillants ont également été trouvés dans une application légitime qu'ils ont infectée.

*"DroidKungFu est un exemple de logiciel malveillant qui a été reconditionné dans un utilitaire VPN légitime, alors que Geinimi a été trouvé au sein d'une application légitime appelée 'Sex Positions,'"* ajoute Karine de Ponteves, analyste de logiciels malveillants chez Fortinet.

### **La dernière vulnérabilité Android**

Le mois dernier, Jon Larimer et Jon Oberheide ont publié une vulnérabilité de la plateforme 2.3.6 d'Android qui s'est révélée être un moyen facile pour les pirates et développeurs de logiciels malveillants de gagner et d'exploiter l'accès *root* d'un appareil Android. Ceci permet aux cybercriminels d'accéder aux fichiers système et d'en changer les paramètres qui sont normalement seulement consultables. De là, ils peuvent installer d'autres logiciels malveillants tels que les ransomware, spambots et keyloggers.

### **A propos de FortiGuard Labs**

Les statistiques et les tendances des menaces établies par le FortiGuard Labs pour cette période sont fondées sur les données recueillies par les appliances de sécurité réseau [FortiGate®](#) déployées à travers le monde. Les clients qui utilisent les [FortiGuard Services](#) de Fortinet devraient déjà être protégés contre les menaces décrites dans le présent rapport.

Les Services [FortiGuard](#) offrent un large éventail de solutions de sécurité dont l'antivirus, la prévention d'intrusions, le filtrage du contenu Web et l'anti-spam. Ces services assurent une protection contre les menaces sur l'ensemble des couches applicatives et du réseau. Les FortiGuard Services sont mis à jour par le FortiGuard Labs, qui permet à Fortinet d'offrir une sécurité multi-couches et une protection rapide contre les menaces nouvelles et

émergentes. Pour les clients abonnés à FortiGuard, ces mises à jour sont livrées sur tous les produits FortiGate, FortiMail™ et FortiClient™.

Tous les rapports sur les principales menaces de Fortinet sont disponible [ici](#). Le podcast vidéo de la Minute de la Sécurité de Novembre, comprenant les commentaires des dernières menaces est également disponible [ici](#). Les recherches en cours sont consultables au [FortiGuard Center](#) ou via [FortiGuard Labs' RSS feed](#). D'autres discussions sur les technologies de sécurité et les analyses des menaces sont disponibles sur [Fortinet Security Blog](#).

### **A propos de Fortinet ([www.fortinet.fr](http://www.fortinet.fr))**

Fortinet (code NASDAQ : FTNT) est un des principaux fournisseurs de solutions de sécurité réseau et le leader du marché des systèmes unifiés de sécurité *Unified Threat Management* ou UTM. Nos produits et services d'abonnements assurent une protection étendue, intégrée et efficace contre les menaces dynamiques, tout en simplifiant l'infrastructure de sécurité informatique. Parmi nos clients figurent des administrations, des fournisseurs d'accès et de nombreuses entreprises, dont la plupart font partie du classement 2009 du Fortune Global 100. FortiGate, le produit phare de Fortinet, intègre des processeurs ASIC pour une meilleure performance et plusieurs fonctions de sécurité conçues pour protéger les applications et les réseaux contre les menaces Internet. Au-delà de ses solutions UTM, Fortinet offre une large gamme de produits conçus pour protéger le périmètre étendu des entreprises – du terminal au périmètre et au cœur de réseau, en passant par les bases de données et applications. Fortinet, dont le siège social se trouve à Sunnyvale en Californie (États-Unis), dispose également de bureaux dans le monde entier.

###

*Copyright © 2011 Fortinet, Inc. Tous droits réservés. Les symboles ® et ™ indiquent respectivement les marques déposées et non enregistrées de Fortinet, Inc., et de ses filiales et partenaires. Les marques Fortinet incluent mais ne sont pas limitées : Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB and FortiWeb. L'ensemble des marques commerciales citées dans le présent communiqué sont la propriété de leurs détenteurs respectifs. Fortinet n'a pas vérifié de façon indépendante les déclarations ou les certificats ci-dessus attribués à des tiers et Fortinet n'a pas approuvé de telles déclarations. Le présent communiqué peut contenir des déclarations prévisionnelles impliquant des incertitudes et des hypothèses. Si les risques ou les incertitudes se concrétisent ou si les hypothèses se révèlent inexactes, les résultats peuvent différer sensiblement par rapport à ceux exprimés ou sous-entendus. Toutes les déclarations autres que celles des faits historiques sont des déclarations qui pourraient être considérées comme des déclarations prévisionnelles. Fortinet n'a aucune obligation de mettre à jour les déclarations prévisionnelles dans l'éventualité où les résultats réels diffèrent et n'en a pas l'intention.*

**FTNT-O**