



## 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 Développement de Logiciels Malveillants Android Ultra-Perfectionnés**

*DroidKungFu Agit comme un Véritable Botnet, Capable de Télécharger des Logiciels Malveillants Supplémentaires, d'Ouvrir des Applications et des Navigateurs sur Demande, de Supprimer des Fichiers et Plus Encore*

**Sophia Antipolis, 4 Novembre 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 d'Octobre. Ce mois-ci, FortiGuard Labs a observé le développement continu du nouveau logiciel malveillant [DroidKungFu](#), qui a de multiples variantes et se comporte de façon similaire aux logiciels malveillants que l'on trouve aujourd'hui sur les PC.

*“DroidKungFu représente clairement la prochaine évolution des logiciels malveillants sur mobiles,”* déclare Derek Manky, sénior stratéguiste en sécurité chez Fortinet. *“Tandis que les premières tentatives de logiciels malveillants sur Android, comme Zitmo (Zeus in the Mobile), sont capables d'intercepter le type d'authentification à deux-facteurs que les banques utilisent pour valider l'identité du titulaire du compte lorsqu'il se connecte, DroidKungFu fait beaucoup plus. En prenant la forme d'une application client VPN légitime, le logiciel malveillant s'implante rapidement dans les appareils en utilisant l'ingénierie sociale. Une fois exécuté, DroidKungFu télécharge d'autres logiciels malveillants, ouvre des URL dans un navigateur, lance des programmes et supprime des fichiers du système.”*

## **Le Danger des Services de Raccourcis d'URL**

Les services de raccourcis d'URL, tels que [TinyURL®](#) offrent un moyen pratique de transmettre des adresses de sites Internet longues et compliquées à des destinataires spécifiques. Quand un utilisateur clique sur un lien raccourci, il est rapidement redirigé sur l'adresse d'origine du site Internet. Comme les services de raccourcis d'URL réduisent le nombre de caractères, ils sont très appréciés des utilisateurs de Twitter. Ils sont également fréquemment utilisés dans les objets d'emails, car certaines applications d'emails ont tendance à rompre les liens les plus longs pendant l'envoi ou à la réception. Cependant, l'avantage du service de raccourcis d'URL est aussi sa plus grosse faiblesse, car le service permet aux criminels de masquer des liens malveillants qui peuvent infecter le système d'un utilisateur. Historiquement, Fortinet a toujours recommandé aux utilisateurs de placer leur curseur sur l'URL douteuse avant de cliquer dessus pour voir si le lien redirige vers une page douteuse. Cette mesure de sécurité n'est pas applicable aux URL raccourcies. Il n'y a aucun moyen sûr de prévenir à l'avance un utilisateur qui clique sur une URL raccourcie s'il sera redirigé vers un site malveillant.

“Les progrès en matière de techniques antispam permettent aujourd'hui de détecter une grande partie des logiciels malveillants dotés d'un lien raccourci,” poursuit Manky. “Toutefois, nous commençons aujourd'hui à voir des créateurs de logiciels malveillants qui conçoivent leur propres services de raccourcis d'URL pour contourner les toutes dernières technologies de détection de spams. C'est encore un autre exemple de CaaS (*crime as a service*) que les cybercriminels proposent.”

Une façon de déterminer si une URL raccourcie pointe vers un site malveillant est de vérifier le domaine à la fin du lien. La plupart des services de raccourcis d'URL malveillants observés récemment ont utilisé le domaine .info. Une autre façon de détecter si une URL raccourcie redirige vers un site malveillant est de vérifier le lien douteux dans un outil de filtrage d'URL, comme le [URL Lookup](#) de Fortinet. Enfin, une bonne solution de filtrage Web

protège contre les services de raccourcis d'URL car le domaine tout entier est encore déterminé et vérifié.

### **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 [FortiGuard Services](#) 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™.

La version intégrale du rapport sur les principales menaces est d'ores et déjà [disponible](#). Le podcast vidéo de la [Minute Sécurité](#), comprenant les commentaires des dernières menaces est également disponible. 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**