



## Communiqué de Presse

### Contact Presse :

Annabelle SOU  
Fortinet, Inc.  
+33 4 89 87 05 76  
[asou@fortinet.com](mailto:asou@fortinet.com)

## Les Recherches de Fortinet sur les Principales Menaces Préviennent d'une Nouvelle Vulnérabilité du Serveur Apache

*"L'Opération Occuper Wall Street" Aidée par les "Anonymous" Repose sur des Injections SQL et Attaques DoS*

**Sophia Antipolis, 4 Octobre 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 son dernier rapport sur les principales menaces, qui révèle que le nouvel outil "Apache Killer" est actuellement utilisé pour exploiter une vulnérabilité du Serveur Apache et qui pourrait être utilisé pour lancer des attaques de déni de service (DoS) contre les serveurs Web fonctionnant sur d'anciennes versions d'Apache. Apache a corrigé la faille et recommande aux utilisateurs de passer immédiatement à la version [Apache 2.2.20](#).

### Les réformateurs de Wall Street aidés par les "Anonymous"

"L'Opération Occuper Wall Street," un mouvement de protestation populaire formé début Juillet ayant pour intention de protester contre la corruption et la cupidité de Wall Street, a été aidé fin Août par le groupe d'hacktivistes "Anonymous." Anonymous, largement connu pour sa mobilisation en faveur du directeur de WikiLeaks, Julian Assange, en s'engageant dans des attaques par déni de service distribué (DDoS) contre PayPal, MasterCard, Visa et autres, a récemment élaboré un nouvel outil de déni de service appelé #RefRef, qui exploite des vulnérabilités SQL de serveurs.

*“ Après Apache Killer et Low Orbit Ion Cannon (LOIC), #RefRef est la nouvelle arme des Anonymous,” déclare Derek Manky, stratège en sécurité chez Fortinet. “Contrairement au LOIC qui nécessite plusieurs utilisateurs pour cibler un site en inondant le serveur avec des paquets TCP et UDP, #RefRef ne requiert qu’une seule attaque. Une fois en place sur un système cible vulnérable, le logiciel utilise la puissance du processeur du système contre lui-même jusqu’à ce qu’il succombe en raison de l’épuisement des ressources. »*

FortiGuard a publié une signature IPS '[RefRef.DoS](#)' pour pallier à cette menace.

### **Les virus emails deviennent un peu plus malins**

Durant la seconde quinzaine de Septembre, le top 10 des logiciels malveillants se composait essentiellement de malwares qui se propageaient par le biais de pièces jointes ou de liens malveillants. La plupart des emails étudiés avaient des pièces jointes infectées, tels qu’un document PDF/Word, une facture, une notification PayPal ou un document zippé. Une des caractéristiques comportementales intéressantes de ces pièces jointes est leur capacité à se supprimer après avoir été exécutées par un utilisateur, ce qui peut compliquer la détection.

L’astuce utilisée par ces créateurs d’emails malveillants pour inciter les utilisateurs peu méfiants à cliquer sur une pièce jointe infectée est de camoufler l’icône exécutable des logiciels malveillants avec une icône légitime qui est associée avec les différents types de documents utilisés aujourd’hui. Le moyen le plus sûr d’éviter ce type d’infections est de ne pas double-cliquer sur les pièces jointes, mais, d’enregistrer la pièce jointe sur votre ordinateur en faisant un clic droit sur l’icône, puis, clic droit sur le document enregistré pour vérifier les propriétés du fichier. Si cette manipulation ne parvient pas à révéler la nature du document, le fichier douteux peut être soumis au scanner de virus en ligne de FortiGuard : [http://www.fortiguard.com/antivirus/virus\\_scanner.html](http://www.fortiguard.com/antivirus/virus_scanner.html)

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

Les statistiques et les tendances des menaces établies par le FortiGuard Labs en Septembre 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, comprenant le classement des menaces les plus élevées dans plusieurs catégories, est d'ores et déjà 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, FortiIOS, 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**