



Communiqué de Presse

Contact Presse :

Annabelle Sou
Fortinet, Inc.
04 89 87 05 76
asou@fortinet.com

Les Recherches de Fortinet sur les Principales Menaces Montrent la Propagation de la Famille des Logiciels Malveillants 64-Bit

*Ce mois-ci, le Faux Antivirus Fraudload.OR a été le Plus Important Virus Détecté,
avec une Forte Présence en Afrique*

Sophia Antipolis, 9 Juin 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 détaille deux importantes détections de la famille de rootkits TDSS infectant les systèmes d'exploitation Windows 64-bit. Le rootkit TDSS, difficile à détecter et à supprimer, a l'accès complet à tous les systèmes qu'il infecte et masque son activité aux administrateurs et utilisateurs finaux.

“Microsoft a publié un avis de sécurité mi-avril pour corriger une vulnérabilité liée à la mise en application d'une signature des pilotes que la famille de rootkits TDSS exploitaient,” déclare Derek Manky, stratège en sécurité chez Fortinet. “Comme TDSS est toujours actif et puissant, nous recommandons fortement de faire cette mise à jour qui est importante si vous avez une édition x64 infectée de Microsoft Windows. Ces rootkits se propagent par des méthodes d'infection courantes comme des sites Internet malveillants qui hébergent des kits d'exploitation de failles, et nous avons vu émerger récemment un nouveau rootkit 64-bit qui utilise une méthode tout à fait différente pour contourner les systèmes x64.”

Augmentation de faux antivirus ciblant les Mac

Le plus important virus détecté par FortiGuard Labs au cours du mois de mai a été Fraudload.OR, qui prend souvent la forme d'un faux logiciel d'antivirus, même si Fraudload peut également télécharger d'autres chevaux de Troie et logiciels malveillants sur le système infecté d'un utilisateur.

“Le faux logiciel d'antivirus est un modèle éprouvé pour les cybercriminels, opérant souvent sur une base de paiement à l'achat à travers laquelle les cybercriminels qui infectent le système d'un utilisateur reçoivent une commission pour chaque victime qui commande une version du faux logiciel” continue Manky. *“Récemment, ce type de logiciels malveillants s'est propagé sur la plateforme Mac OSX sous la forme de MacDefender et MacGuard.”*

A propos de FortiGuard Labs

Les statistiques et les tendances des menaces établies par le FortiGuard Labs 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 Services FortiGuard 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 principales dans plusieurs catégories, est d'ores et déjà disponible. Les recherches en cours sont consultables au FortiGuard Center ou via le FortiGuard Labs' RSS feed. D'autres discussions sur les technologies de sécurité et les analyses des menaces sont disponibles sur le Fortinet Security Blog et sur Security Minute videocast.

A propos de Fortinet (www.fortinet.com)

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