



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 Deux Nouvelles Variantes de Malwares Ciblant les Utilisateurs de Facebook

Le Botnet Coreflood qui a Infecté 2,3 Millions de Machines a été Démantelé par le FBI et le Niveau de Spams Poursuit sa Baisse de 15% Mois Après Mois Après le Récent Démantèlement du Botnet Rustock

Sophia Antipolis, 5 Mai 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 rapport sur les principales menaces, qui détaille deux nouvelles variantes de malwares ciblant les utilisateurs de Facebook. Ces malwares, prétendant venir directement de Facebook, affirment que les mots de passe des utilisateurs ont été réinitialisés et qu'une pièce jointe, malicieuse, contient leurs nouveaux mots de passe. En cliquant sur la pièce jointe, on est infecté immédiatement.

“Les variantes de malwares présentes sur Facebook que nous avons examinés chargent des bots, qui, lors de l'exécution, se connectent aux serveurs de commande et de contrôle pour télécharger et afficher un document qui révèle un faux mot de passe dans le but de paraître légitime,” déclare Derek Manky, stratéguiste en sécurité chez Fortinet. *“Ensuite, le botnet continue de tourner sur l'ordinateur et commande le chargement et l'exécution des fichiers, un à un. De façon générale, toujours se méfier des pièces jointes, ne jamais divulguer les informations provenant d'une demande non sollicitée, et tenter de confirmer l'identité de ceux qui vous contactent.”*

L'Activité des Spams Reste Faible

Le 16 Avril, une vaste opération de botnets Coreflood (environ 2002) a été démantelée par le FBI, la plus grande action coercitive de l'histoire des Etats-Unis. Les serveurs et domaines contrôlés par un groupe international de cybercriminels ont été saisis. Ce botnet a infecté 2,3 millions de machines et des millions de dollars ont été volés via des ordinateurs appartenant à d'utilisateurs non avertis.

“Coreflood se différencie du botnet Rustock, qui a été mis hors ligne mi-Mars avec l'aide de Microsoft et un certain nombre d'organismes fédéraux,” continue Derek Manky. *“En conséquence, les deux principaux botnets ont décliné et le taux de spams mondial est resté environ 15% inférieur comparé à celui qu'il était avant le démantèlement du Rustock.”*

A propos de FortiGuard Labs

Les statistiques et les tendances des menaces établies par le FortiGuard Labs en Avril 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](#) 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