



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 Révèlent que les Faux Antivirus Représentent 58% de l'activité des nouveaux logiciels malveillants en Août

La Variante du Botnet Zeus Est en 2^{ème} Place dans l'Activité Mensuelle des Malwares Due à son Code Source Cracké et Divulgué

Sophia Antipolis, 12 Septembre 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 faux antivirus [W32/FraudLoad.OR](#) a représenté 58 pourcent de l'activité des nouveaux logiciels malveillants en Août.

"Traditionnellement, FraudLoad installe de faux antivirus sur les systèmes d'utilisateurs non avertis, mais dans nos laboratoires, il n'est pas rare de constater que ce genre de botnets télécharge des malwares supplémentaires tels que des spam bots, bots dédiés à l'envoi de spams," déclare Derek Manky, stratégyte en sécurité chez Fortinet.

Juste derrière FraudLoad, une variante du botnet Zeus, récemment découverte, a été le second malware le plus actif en Août.

"Le regain d'activité de Zeus ne nous surprend pas étant donné la popularité du botnet et le fait que son code source ait été piraté et par la suite divulgué publiquement en Mai dernier," poursuit Manky. *"Il est très probable que nous continuerons de voir Zeus et SpyEye — un*

autre botnet populaire dont le code source a été récemment cracké et divulgué publiquement — se propager dans les prochains mois.”

Informations supplémentaires en bref:

En Août, le botnet W32/Yakes et quatre variantes se sont propagés via des spams en exploitant des formulaires standards utilisés par les principales sociétés émettrices de cartes de crédit. L'email que reçoit la victime a généralement pour objet : "Carte de crédit bloquée." Le courriel explique que la carte de crédit a été impliquée dans des opérations illégales et a été désactivée. L'email conseille alors à la victime d'ouvrir le fichier joint pour plus de détails. Lorsque l'utilisateur clique sur la pièce jointe, le botnet Yakes s'installe sur son ordinateur.

A propos de FortiGuard Labs

Les statistiques et les tendances des menaces établies par le FortiGuard Labs en Août 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.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