Les Dernières Recherches de Fortinet sur les Principales Menaces Montrent la Ré-Emergence du Botnet Torpig

Le Rapport Montre Egalement que le Nombre d'Adresses IPs Utilisées pour émettre du Spam Reste Stable Malgré la Réduction du Volume Total de Spams

Sophia Antipolis, 20 Avril 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 des 30 derniers jours, qui montre la ré-émergence du Botnet Torpig, représentant 30% de l'activité des botnets. La plupart des détections des centres de commande et de contrôle (C&C) de Torpig provenaient de machines localisées en Russie et au Soudan. En comparaison, le botnet Hiloti représentait approximativement 15% du trafic des botnets – dont la majorité était en Australie et en Suède.

"*Le botnet Torpig existe depuis des années et se propage généralement par le biais de pages Web malicieuses comportant un rootkit (mebroot) qui infecte* le *master boot record du système*," déclare Derek Manky, stratégiste en sécurité chez Fortinet. "*En compromettant l'intégrité du système dès le démarrage, Mebroot rend inefficace les pare-feux personnels. Les appliances Fortinet peuvent minimiser cette menace en bloquant le trafic lié à Mebroot*."

L'activité des Spams

Le taux de spams demeure inférieur à la moyenne, à environ 30%, suite au démantèlement du botnet Rustock en Mars. Bien que les taux restent faibles, le nombre d'adresses IP envoyant des spams (machines) n'a pas connu une forte baisse. La plupart de ces adresses observées étaient des machines aux Etats-Unis, en Inde et au Brésil.

"*Souvent, les machines sont infectées par de multiples virus ou botnets qui continuent d'envoyer des spams, même si un des bots a été neutralisé*," déclare Manky.

A propos de FortiGuard Labs

Les statistiques et les tendances des menaces établies par le FortiGuard Labs pour les quatres dernières semaines 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 des solutions de sécurité de grande envergure 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 de février, 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.

###

FTNT-O