

Mardi 24 janvier 2012

Des virus et des vers incontrôlables engendrent une nouvelle menace informatique imprévisible

Des malwares fusionnent accidentellement et créent de dangereux hybrides

Des virus infectent accidentellement des vers déjà présents sur les ordinateurs infectés, créant un malware hybride capable de se propager plus rapidement et de s'attaquer de façon chaotique aux systèmes, comptes bancaires et données confidentielles, d'une manière que les créateurs des malwares eux-mêmes n'avaient pas imaginée.

Une analyse de Bitdefender a détecté début janvier plus de 40 000 exemples de ces « Frankenmalwares » lors de l'étude de 10 millions de fichiers infectés, soit 0,4% des malwares vérifiés. Si ce ratio s'applique aux 65 millions de malwares estimés dans le monde, environ 260 000 de ces associations toxiques pourraient menacer la sécurité informatique.

« La présence de l'un de ces hybrides sur votre ordinateur peut être synonyme de nombreux problèmes : détournements financiers, bugs informatiques, usurpation d'identité, et en bonus l'envoi de vagues de spam de manière aléatoires » déclare Loredana Botezatu, Analyste des e-menaces pour les Laboratoires Bitdefender et à l'origine de l'étude sur cette nouvelle espèce de malwares hybrides. « L'apparition de ces malwares-sandwiches constitue un nouveau rebondissement dans l'univers des malwares. Ils se diffusent plus efficacement et deviennent de plus en plus difficiles à prévoir et du coup à éradiquer. »

Bien qu'il n'existe pas de données antérieures concernant ces « malwares-sandwiches », le nombre de ces hybrides a augmenté ces dernières années et devrait continuer à progresser au même rythme que celui des malwares en général. Une étude de Bitdefender estime que le nombre de malwares connaîtra une hausse de 17% cette année.

Tous les malwares hybrides analysés par Bitdefender se sont jusqu'à présent formés accidentellement. Cependant, le risque que présentent ces associations de malwares pourrait augmenter considérablement si des cyber-criminels commençaient à fabriquer leurs propres combinaisons, ou lançaient des malwares spécifiquement conçus pour encourager la création aléatoire de « malwares-sandwiches », explique Loredana Botezatu.

Bitdefender a lancé sa propre étude sur les « malwares-sandwiches » après avoir découvert le ver Rimecud, infecté par Virtob, un infecteur de fichiers. Rimecud dérobe des mots de passe de comptes bancaires en ligne, de boutiques en ligne, de réseaux sociaux et de messageries, entre autres fonctions. Virtob permet quant à lui de recevoir des commandes d'un attaquant à distance, échappe aux pare-feu et assure sa pérennité en injectant du code dans Winlogon, un des processus critiques de Windows.

Une version chaotique de cet hybride est déjà en circulation, ainsi que d'autres types de malwares-sandwiches qui peuvent accroître de manière spectaculaire le risque d'infection des ordinateurs et ainsi accentuer le taux de machines infectées.

« Imaginez maintenant que ces deux malwares combinés puissent fonctionner ensemble – volontairement ou non - sur le même système corrompu. » écrit Loredana Botezatu dans son rapport sur le site www.malwarecity.fr. « Ce PC se retrouve alors confronté à un double malware, avec deux fois plus de serveurs de contrôle et de commande desquels recevoir des instructions du pirate. De

plus, deux backdoors sont ouvertes, deux techniques d'attaques sont actives et plusieurs méthodes de diffusion sont mises en place. Là où une technique échoue, l'autre réussit ».

Pour retrouver Bitdefender en ligne et rester au fait de l'actualité des e-menaces, inscrivez-vous à nos fils d'information :

- [Flux RSS](#)
- [Facebook](#)
- [Twitter](#)
- [La communauté MalwareCity](#)

À propos de Bitdefender®

Bitdefender est une entreprise internationale qui développe, édite et commercialise des solutions de sécurité dans plus de 100 pays. Sa technologie proactive, en évolution permanente, protège aujourd'hui plus de 400 millions de particuliers et d'utilisateurs professionnels dans le monde et est reconnue et certifiée par les organismes de tests indépendants comme l'une des plus efficaces et rapides du marché.

Depuis 2001, Bitdefender confie, pour la France et les pays francophones, l'édition et la commercialisation de ses solutions à la société Editions Profil.

Pour plus d'informations sur les produits Bitdefender : www.bitdefender.fr

À propos d'Editions Profil

Editions Profil est une société française indépendante créée en 1989 qui développe, édite et commercialise des solutions de sécurité et de filtrage de contenus numériques adaptées aux particuliers et aux entreprises. Ses produits phares sont édités sous les marques Bitdefender et Profil Technology.

Plus d'informations sur www.editions-profil.eu



Editions Profil édite et commercialise les solutions Bitdefender pour la France et les pays francophones.