

McAfee : Les méthodes de vol de données les plus courantes sur le Net
Sécurité

Posté par : JPilo

Publié le : 12/3/2014 13:00:00

McAfee Labs révèle les principales menaces qui ont marqué le 4^{ème} trimestre 2013. Les chercheurs McAfee mettent notamment en lumière le rôle joué par le « dark web » dans l'industrie des logiciels malveillants, le catalyseur des attaques ciblant les points de vente en ligne, ainsi que les violations de données.

« Cet automne, les cybercriminels se sont appuyés sur les failles des sites marchands pour lancer leurs attaques. Ils ont su profiter de la période du shopping de Noël, où les gens se sentent le plus en confiance pour acheter pour accroître leur terrain de jeu », précise

François Paget, chercheur de menaces au sein de McAfee Labs.

1/ Vente des données personnelles relatives aux cartes de crédits

Le rapport met en lumière la facilité d'achat en ligne de logiciels malveillants, de données personnelles ainsi que la vente de numéros de cartes de crédit volées. McAfee Labs relève également que le nombre de signatures électroniques malveillantes a triplé au cours de l'année 2013 et qu'une accélération de cette tendance pourrait engendrer une importante menace à l'authentification des logiciels sécurisés, par l'autorité de certification.



« Pour les professionnels de la lutte contre le cybercrime, les nouvelles pratiques employées par les hackers, simples à réaliser et à utiliser, annoncent l'ère du CaaS (Cybercrime-as-a-Service) », poursuit **François Paget**.

2/ Recrudescence des malwares relatifs aux certificats d'authenticité

Fin 2013, McAfee a rÃ©fÃ©rencÃ© trois fois plus de malwares au sein de sa base de donnÃ©es (le *zoo*), aujourd'hui composÃ©e de plus de 8 millions de fichiers suspects. Au cours du quatriÃ¨me trimestre, les chercheurs du Labs ont ainsi identifiÃ© plus de 2,3 millions de nouvelles applications malveillantes, soit une augmentation de 52 % par rapport au trimestre prÃ©cÃ©dent.

Bien que le nombre total d'Ã©chantillons de logiciels malveillants intÃ©grent des donnÃ©es volÃ©es, achetÃ©es ou des certificats erronÃ©s, le moteur majeur de leur croissance rÃ©side dans les rÃ©seaux de distribution aux contenus douteux.

Ã

Ces organisations permettent aux dÃ©veloppeurs de tÃ©lÃ©charger leurs programmes, ou une URL qui est en lien vers une application externe, et de la transformer en malware. McAfee entend alerter sur la confusion que peut crÃ©er ces malwares signÃ©s et remettre Ã©galement en cause la viabilitÃ© du code source.

Ã« *Bien que les interventions des autoritÃ©s de certification aient considÃ©rablement rÃ©duit les coÃ»ts de dÃ©veloppement et de dÃ©livrance de logiciels pour les dÃ©veloppeurs, les normes d'identification de l'Ã©diteur ont Ã©galement diminuÃ© spectaculairement* Ã», ajoute *FranÃ§ois Paget*. Ã« *DÃ©sormais, nous devons apprendre Ã faire plus confiance Ã la rÃ©putation du fournisseur qui a dÃ©livrÃ©/signÃ© le fichier qu'Ã la simple prÃ©sence d'un certificat.* Ã»

3/ Et toujours :

â Les logiciels malveillants sur mobiles.

McAfee Labs a recueilli 2,47 millions de nouveaux Ã©chantillons en 2013, dont 744 000 sur le quatriÃ¨me trimestre. La base d'Ã©chantillonnage relative aux logiciels malveillants mobiles a augmentÃ© de 197 % depuis la fin 2012.

â Les ransomwares.

Leur volume a augmentÃ© d'un million cette annÃ©e, 50 % de plus ont Ã©tÃ© rÃ©fÃ©rencÃ©s au 4Ã¨me trimestre 2013, en comparaison de la mÃªme pÃ©riode en 2012.

â Les URL suspectes.

McAfee a enregistrÃ© une augmentation de 70 % du nombre d'URL suspectes sur l'annÃ©e 2013.

â La prolifÃ©ration des malwares.

En 2013, McAfee Labs a trouvÃ©, chaque minute, 200 nouveaux Ã©chantillons de malwares, soit plus de trois nouvelles menaces chaque seconde.

â L'enregistrement liÃ©s Master Boot.

2,2 millions de nouvelles -attaques ont Ã©tÃ© identifiÃ©es sur 2013.