Bitdefender : Mutation des virus et nouvelle menace informatique
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 25/1/2012 11:00:00

Bitdefender constate que des virus et des vers incontrÃ´lables engendrent **une nouvelle menace informatique imprÃ©visible**. Des malwares fusionnent accidentellement et crÃ©ent de dangereux hybrides,

Des virus infectent accidentellement des vers dÃ©jÃ prÃ©sents sur les ordinateurs infectÃ©s, crÃ©ant un malware hybride capable de se propager plus rapidement et de sâ□□attaquer de faÃ§on chaotique aux systÃ¨mes, comptes bancaires et donnÃ©es confidentielles, dâ□□une maniÃ¨re que les crÃ©ateurs des malwares eux-mÃªmes nâ□□avaient pas imaginÃ©e.

Une analyse de Bitdefender a dÃ©tectÃ© dÃ©but janvier plus de 40 000 exemples de ces Â« Frankenmalwares Â» lors de l'Ã©tude de 10 millions de fichiers infectÃ©s, soit 0,4% des malwares vÃ©rifiÃ©s. Si ce ratio sâ□□applique aux 65 millions de malwares estimÃ©s dans le monde, environ 260 000 de ces associations toxiques pourraient menacer la sÃ©curitÃ© informatique.

Â« *La prÃ©sence de lâ□□un de ces hybrides sur votre ordinateur peut Ãªtre synonyme de nombreux problÃ¨mes : dÃ©tournements financiers, bugs informatiques, usurpation dâ□□identitÃ©, et en bonus lâ□□envoi de vagues de spam de maniÃ¨re alÃ©atoire* Â» dÃ©clare **Loredana Botezatu**, Analyste des e-menaces pour les Laboratoires Bitdefender et Ã lâ□□origine de lâ□□Ã©tude sur cette nouvelle espÃ¨ce de malwares hybrides. Â« *Lâ□□apparition de ces malwares-sandwiches constitue un nouveau rebondissement dans lâ□□univers des malwares. Ils se diffusent plus efficacement et deviennent de plus en plus difficiles Ã prÃ©voir et du coup Ã Ã©radiquer.* Â»

Bien quâ□□il nâ□□existe pas de donnÃ©es antÃ©rieures concernant ces Â« malwares-sandwiches Â», le nombre de ces hybrides a augmentÃ© ces derniÃ¨res annÃ©es et devrait continuer Ã progresser au mÃªme rythme que celui des malwares en gÃ©nÃ©ral. Une Ã©tude de Bitdefender estime que le nombre de malwares connaÃ®tra une hausse de 17% cette annÃ©e.

Tous les malwares hybrides analysÃ©s par Bitdefender se sont jusquâ□□Ã prÃ©sent formÃ©s accidentellement. Cependant, le risque que prÃ©sentent ces associations de malwares

pourrait augmenter considÃ©rablement si des cyber-criminels commenÃ§aient Ã fabriquer leurs propres combinaisons, ou lanÃ§aient des malwares spÃ©cifiquement conÃ§us pour encourager la crÃ©ation alÃ©atoire de Â« malwares-sandwiches Â», explique Loredana Botezatu.

Bitdefender a lancÃ© sa propre Ã©tude sur les Â« malwares-sandwiches Â» aprÃ¨s avoir dÃ©couvert le ver Rimecud, infectÃ© par Virtob, un infecteur de fichiers. Rimecud dÃ©robe des mots de passe de comptes bancaires en ligne, de boutiques en ligne, de rÃ©seaux sociaux et de messageries, entre autres fonctions. Virtob permet quant Ã lui de recevoir des commandes dâ□□un attaquant Ã distance, Ã©chappe aux pare-feu et assure sa pÃ©rennitÃ© en injectant du code dans Winlogon, un des processus critiques de Windows.

Une version chaotique de cet hybride est dÃ©jÃ en circulation, ainsi que dâ□□autres types de malwaresâ□□sandwiches qui peuvent accroitre de maniÃ¨re spectaculaire le risque dâ□□infection des ordinateurs et ainsi accentuer le taux de machines infectÃ©es.

Â« *Imaginez maintenant que ces deux malwares combinÃ©s puissent fonctionner ensemble â□□ volontairement ou non - sur le mÃªme systÃ¨me corrompu.* Â» Ã©crit **Loredana Botezatu** dans son rapport sur le site : ***malwarecity.fr***. Â« *Ce PC se retrouve alors confrontÃ© Ã un double malware, avec deux fois plus de serveurs de contrÃ´le et de commande desquels recevoir des instructions du pirate. De plus, deux backdoors sont ouvertes, deux techniques dâ□□attaques sont actives et plusieurs mÃ©thodes de diffusion sont mises en place. LÃ oÃ¹ une technique Ã©choue, lâ□□autre rÃ©ussit* Â».

Pour retrouver Bitdefender en ligne