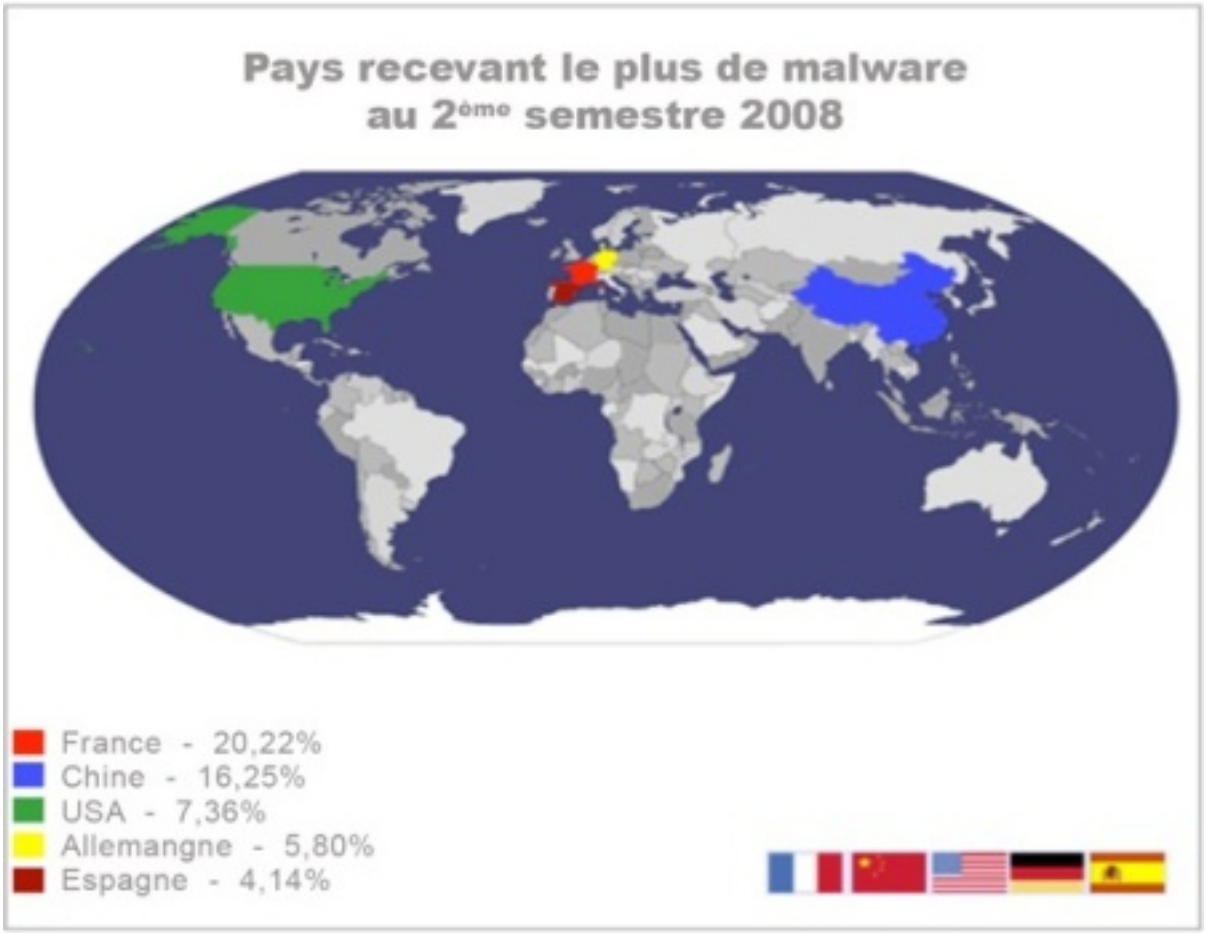
BitDefender publie son rapport sur lâ□□Ã©tat des e-menaces
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 16/1/2009 0:00:00

Les principales e-menaces au second semestre 2008 BitDefenderÂ®, lâ□□un des fournisseurs les plus rÃ©compensÃ©s de solutions antivirus et de sÃ©curitÃ© des donnÃ©es, publie son rapport sur les principales e-menaces au second semestre 2008, ainsi que ses prÃ©visions pour lâ□□annÃ©e 2009.
Les tendances observÃ©es par les Laboratoires BitDefender dans leur prÃ©cÃ©dent rapport sur les e-menaces (E-threats Landscape Report) montraient que les crÃ©ateurs de malwares se consacraient principalement Ã produire et Ã diffuser des chevaux de Troie ainsi qu'Ã exploiter les vulnÃ©rabilitÃ©s systÃ¨me.



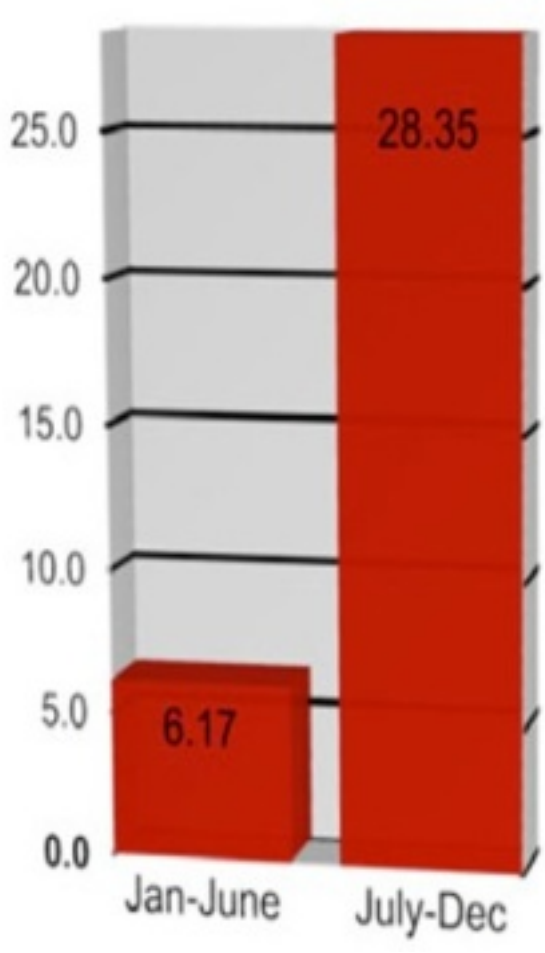
Â
- Plus de 80% des malwares transmis dans le monde appartiennent encore Ã la catÃ©gorie des chevaux de Troie.
- Â¾ des chevaux de Troie intÃ¨grent dÃ©jÃ des mÃ©canismes de mise Ã jour Ã©laborÃ©s, la capacitÃ© de tÃ©lÃ©charger et de transmettre furtivement des donnÃ©es et la possibilitÃ© de diffuser des spywares ou des rootkits.
- Le volume de menaces issues du web a augmentÃ© de 460%.
- Les exploitations de failles JavaScript via injections SQL ont triplÃ©.

- Les thÃ¨mes les plus utilisÃ©s pour la diffusion d'e-menaces au cours du deuxiÃ¨me semestre Ã©taient : la supposÃ©e volontÃ© des Etats-Unis d'envahir l'Iran, les Jeux Olympiques de 2008 et les Ã©lections amÃ©ricaines.
- Le texte simple continue d'Ãªtre le format prÃ©fÃ©rÃ© pour l'envoi de spam par e-mail ; il a Ã©tÃ© utilisÃ© dans 80% des cas fin 2008, contre seulement 1,5% pour le spam-image.
- Le nombre d'e-mails non sollicitÃ©s contenant des fichiers joints infectÃ©s ou des liens vers une page oÃ¹ l'on demandait Ã l'utilisateur de tÃ©lÃ©charger un malware a augmentÃ© de 400%.

- 5% du spam liÃ© Ã des tentatives de phishing comprenait des piÃ¨ces jointes au format HTML destinÃ©es Ã voler des donnÃ©es confidentielles via des scripts PHP (contre 1% au premier semestre 2008).

Afin d'augmenter l'efficacitÃ© du spam, les spammeurs ont concentrÃ© leurs efforts sur les mÃ©canismes confirmant la rÃ©ception des messages envoyÃ©s.

Les spams les plus diffusÃ©s ont Ã©tÃ© :



- MÃ©dicaments et autres drogues (Â« Viagra Â») 49%
- E-mail contenant une piÃ¨ce jointe infectÃ©e 10%
- E-mail de phishing 9.50%
- Vente de contrefaÃ§on 7%
- Pseudo prÃªts financiers â□□ 6.50%

Fin 2008, environ 70% des tentatives de phishing faisaient rÃ©fÃ©rence au contexte financier international.

Les Ã©tablissements bancaires dont l'identitÃ© a Ã©tÃ© la plus souvent usurpÃ©e sont : Bank of America, Chase Bank, Citibank, HSBC et Halifax Bank.

Le 3Ã¨me semestre a Ã©tÃ© marquÃ© par l'apparition de spam imitant la prÃ©sentation de newsletters et de messages provenant d'agences de presse comme CNN, CBS ou ABC.

Le phishing ayant pour cible ou sujet les sites de rÃ©seaux sociaux a augmentÃ© Ã la fin de l'annÃ©e.

Les pays les plus touchÃ©s par les malwares au second semestre 2008 sont : la France, la Chine, les Etats-Unis, l'Allemagne et l'Espagne (voir carte ci-dessous) :

PrÃ©visions 2009 pour les e-menaces

Presque 45% des e-menaces dans le monde sont transmises exclusivement par e-mail ou dÃ©pendent de ce mode de diffusion dans une certaine mesure. Dans ce contexte, sÃ©curiser les communications par e-mail devrait devenir une prioritÃ© en 2009.

En 2009, la production de malwares continuera probablement sur une courbe ascendante et exploitera les capacitÃ©s Web intÃ©grÃ©es par les chevaux de Troie, les spywares et les rootkits. On a observÃ© fin 2008 une augmentation de 460% du nombre d'infections sur Internet et de 400% du nombre de SPAM diffusant des chevaux de Troie.

Il est certain que de nombreuses familles dâ□□e-menaces connaÃ®tront d'importantes mises Ã jour et de mutations en termes de furtivitÃ© et dâ□□automatisation des mÃ©canismes de diffusion.

L'annÃ©e 2009 exploitera Ã©galement les vulnÃ©rabilitÃ©s des applications, comme le montre la dÃ©tection rÃ©cente dâ□□un programme de dÃ©tournement de mots de passe que les chercheurs BitDefender ont identifiÃ© dÃ©but dÃ©cembre. DissimulÃ© sous la forme dâ□□un plugin pour MozillaÂ® FirefoxÂ® Â« Trojan.PWS.ChromeInject.A Â» rÃ©cupÃ¨re les donnÃ©es envoyÃ©es par les utilisateurs vers plus de 100 sites bancaires en ligne.

Il convient de prÃªter une attention particuliÃ¨re au nombre croissant de sites Web 2.0 et Ã leur dÃ©veloppement rapide. En 2009, les applications Web 2.0 les plus visÃ©es par les malwares demeureront les rÃ©seaux sociaux. Fin 2008 a vu l'apparition de Â« Win32.Worm.KoobFace.A Â» qui touchait Ã la fois les utilisateurs de FacebookÂ® et ceux de MySpaceâ□¢.

DerniÃ¨re menace et non des moindres, il est probable que les smart phones et autres appareils â□□intelligentsâ□□ ayant un accÃ¨s permanent Ã Internet seront en 2009 la cible des nouvelles gÃ©nÃ©rations de malwares pour plateformes mobiles.

Pour consulter le rapport complet (en anglais) **cliquez ici**