Cavalo de Troia responde por 60% das ameaças no semestre

Foram reportadas 2.552 vulnerabilidades para o banco de dados da Common Vulnerabilities and Exposures

O Cavalo de Troia foi a principal ameaça verificada pela Trend Micro no primeiro semestre deste ano. Conforme levantamento, esse problema respondeu por 60% de todos os ataques verificados no período, superando a média de 53%.

Em nota divulgada à imprensa, a multinacional informou ter identificado o resultado na infraestrutura Trend Micro Smart Protection Network, que recebe 45 bilhões de consultas, bloqueia cinco bilhões ameaças e processa 2.5TB de dados diariamente. Em média, 80 milhões de usuários conectam-se à rede todos os dias.

A empresa observou um crescimento significativo no número de URLs maliciosas, que aumentou de 1,5 bilhão no começo do ano para mais de 3,5 bilhões até junho. A América do Norte foi a maior fonte, enquanto a região da Ásia e Pacífico teve o maior número de tentativas de acesso a esses sites, que em sua maioria apresentam conteúdo adulto.

Foram reportadas 2.552 vulnerabilidades para o banco de dados da Common Vulnerabilities and Exposures (CVE).

Setores

Entre os setores mais visados pelos cibercriminosos, o de educação ficou com o primeiro lugar, uma vez que metade das infecções por malware ocorreu dentro de escolas e universidades.

Em seguida estão os setores governamentais e de tecnologia, cada um com 10% de todas as infecções.

Spam

Em relação ao spam, a Europa se tornou a maior fonte em todo o mundo (38%), sendo as mensagens em HTML a forma mais comum pela qual essas mensagens indesejadas se manifestam. Na sequência, aparece a região da Ásia e Pacífico (31%), América do Norte e América do Sul (ambas com 14%) e o restante (3%) vêm de regiões desconhecidas.

Apesar de conhecido como uma fonte substancial de spam, o conteúdo pornográfico compõe apenas 4% do total. O que predominam são mensagens comerciais, golpes e anúncios médico-farmacêuticos, que respondem por 65% do spam mundial.

Fonte: IT Web, 19 out. 2010. [Portal]. Disponível em: <http://www.itweb.com.br>. Acesso em: 20 out. 2010.