**O que são botnets?**

Autor: CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática

As botnets são redes de computadores ou *smartphones* infetadas por um determinado tipo de *malware* (também conhecido como “vírus informático”), controladas por um indivíduo ou grupo, e que servem vários propósitos ilegais tais como: roubo de identidade, roubo de informações confidenciais, extorsão, fraudes bancárias e ataques ou tentativas de infeção de outros sistemas online. Uma vez infectado, o seu dispositivo quase de certeza servirá de plataforma para atacar terceiros, protegendo a identidade do atacante.

As formas de infeção são variadas e vão desde o envio de mensagens de correio electrónico, a serviços de conversação instantânea ou de *posts* em redes sociais com *malware*, páginas na internet que quando visitadas infectam automaticamente o utilizador, credenciais fracas de acesso a serviços online, até à distribuição dissimulada em aplicações que parecem legítimas (ex: um software de antivírus ou uma *app* que aumenta a longevidade da bateria do dispositivo, mas que na verdade apenas infecta o sistemacom *malware*).

De forma a precaver-se contra as *botnets* deve adotar um comportamento mais crítico online, desconfiando de mensagens de correio electrónico, mensagens instantâneas ou *posts* suspeitos - mesmo que estas tenham sido enviadas por pessoas que conhece; utilizar e manter sempre atualizado o software antivírus no seu sistema; utilizar credenciais de acesso robustas e instalar apenas software com alguma credibilidade (em caso de dúvida numa breve pesquisa na *internet* encontrará *feedback* de outros utilizadores) e distribuído através dos canais fidedignos como as lojas oficiais dos fabricantes (*GooglePlay*, *AppStore*, etc...), sendo que, mesmo nestes casos, deve sempre validar a credibilidade da mesma (ex: através dos mecanismos de reputação e *feedback* dos utilizadores).

Alguns dos sintomas que podem indiciar uma infecção no seu sistema são o aparecimento de aplicações desconhecidas, a alteração de configurações no sistema ou browser (página inicial, motor de pesquisa), mensagens de erro ao atualizar o seu sistema ou antivírus, desativação de mecanismos de segurança (firewall, antivírus), lentidão de funcionamento ou surgimento de chamadas telefónicas ou mensagens estranhas.

Caso suspeite que o seu sistema está infectado, não o utilize, desligue-o da Internet e leve-o a um especialista.

---------------------------------------------------------------------------

**Mês Europeu da Cibersegurança**

Este artigo é da autoria de especialistas do CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática (www.cert.pt) da FCCN-Fundação de Computação Científica Nacional (www.fccn.pt/pt) e insere-se na campanha "Uma dica por dia" integrada no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013.

O Mês Europeu da Cibersegurança é uma iniciativa da ENISA - Agência Europeia para a Segurança das Redes e Informação (www.enisa.europa.eu) e o seu objectivo é informar os utilizadores sobre a importância da segurança da informação, bem como demonstrar algumas medidas simples para proteger os seus dados.

----------------------------------------------------------------------------

**Nota aos editores da Imprensa regional**

Os artigos da autoria dos técnicos do CERT.PT incluídos no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013, surgem no site da Ciência na Imprensa Regional numerados, de forma a permitir a sua mais fácil identificação. No entanto, eles são absolutamente independentes uns dos outros e podem ser publicados pelos órgãos de comunicação de forma avulsa.

------------------------------------------------------------------------------

Imagem de Lorenzo Rossi

(Existem ficheiros de imagem de mais alta resolução disponíveis para download)