**Ciberconflitos: atores e ameaças**

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

Na era digital, também as arenas das guerras e do terrorismo foram transpostas para a Internet. As motivações permanecem as mesmas, mas o vetor de ataque é novo. Desde a espionagem patrocinada por Estados ou para fins comerciais, passando pela guerra político-económica até à criminalidade organizada, estes são os principais interesses que provocam ciberconflitos em larga escala no mundo moderno.

Ainda estão frescos na memória os ataques de 2007 às infra-estruturas governamentais e bancárias na Estónia. O incidente terá sido desencadeado, entre outros eventos, pela deslocação de uma estátua da era soviética do centro de Tallin, tendo os ciber-ataques subsequentes, de uma sofisticação nunca antes vista a esta escala, sido vistos como uma retaliação por parte da Rússia. O impacto provocado por estas ações motivou intervenção por parte da NATO e Centros de Resposta a Incidentes de países aliados, no sentido de mitigar as consequências. O sucedido teve profunda influência em organizações militares nacionais e transnacionais, relativamente ao papel do ciberespaço no quadro dos conflitos globais, sendo que muito se modificou nas políticas e planos de segurança ao mais alto nível.

De igual modo, os prejuízos provocados pelo vírus “Stuxnet” no desenvolvimento das capacidades nucleares do Irão também tiveram grande divulgação. Muito se especulou acerca do envolvimento de governos na produção deste “software” malicioso, sobre o envolvimento de redes de espionagem na infeção de uma central de produção de energia nuclear e sobre as motivações subjacentes. Certo é que o programa nuclear iraniano sofreu um sério revés, como consequência de um programa informático com cerca de 1,5 MB de tamanho, transmitido por uma pen USB, provocando sérias avarias em equipamento de alta tecnologia difícil de substituir.

É tido como certo que o desafio crescente do domínio do ciberespaço é crucial para determinar quem sai vencedor nos grandes conflitos à escala global, independentemente dos interesses que os motivam, sejam económicos, políticos ou militares. O mundo tenta a todo o custo adaptar-se, tanto na componente legislativa como técnica, a um conjunto de ameaças que não conhece fronteiras e, nesse sentido, escapa a jurisdições e controlo legislativo. A resposta parece residir na cooperação entre Estados, envolvendo organizações policiais, centros de resposta a incidentes, empresas privadas e o conjunto de *stakeholders* ligados ao ciberespaço. Destaque-se, a nível Europeu, os recentes esforços da ENISA (Agência Europeia para a Segurança das Redes e da Informação) no sentido de aumentar este nível de cooperação e colaboração, de perseguir boas práticas na implementação de legislação e na chamada de atenção para a realidade específica da Proteção de Infra-estruturas Críticas.

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

**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.

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

Foto de Michael Selivanov

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