***17- Scareware*, *ransomware* e c*lickjacking***

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

*Scareware* e *ransomware* são termos técnicos que designam tipos diferentes de *malware* (vulgarmente designados como vírus informáticos) e o c*lickjacking* é um método de infeção e disseminação de *malware*.

O que têm em comum? Todos se aproveitam da fraca consciencialização dos utilizadores para a segurança online, como meio para infectarem sistemas.

O *scareware*, que nasce do termo inglês *scare* (susto/medo), utiliza mensagens alarmistas, geralmente sob a forma de janelas de *pop-up* ou anúncios na internet, indicando que o sistema do utilizador está infectado com algum tipo de *malware* ou corre qualquer outro risco. Estas mensagens têm como objectivo assustar o utilizador e levá-lo a instalar precipitadamente, por livre e espontânea vontade, uma alegada ferramenta de antivírus ou de atualização de segurança, que mais não é do que ela própria um *malware*.

O *ransomware*, que nasce do termo inglês r*ansom* (resgate), consiste num tipo de *malware* que, ao infetar um determinado sistema, bloqueia a sua utilização e mostra ao utilizador uma mensagem de resgate para a sua desinfeção. Em muitos casos, a mensagem de resgate aparece como tendo tido origem num órgão policial, indicando que o utilizador terá sido detectado a cometer um determinado crime (ex.: consulta de sites de pornografia de menores) e exigindo o pagamento de uma multa. O utilizador, frequentemente por medo ou vergonha, acede ao pedido de resgate, efetuando a transferência monetária para o criminoso.

O *clickjacking*, que nasce da junção dos termos ingleses c*lick* e *hijacking* (sequestro), é um método que utiliza mensagens apelativas em redes sociais, geralmente sob a forma de imagens sedutoras ou notícias chamativas, com objectivo de levar o utilizador a clicar na mensagem para obter mais informação. Ao clicar nessa mensagem, o utilizador é reencaminhado para sites maliciosos que tentam infectar o seu computador. Adicionalmente, a mensagem que foi utilizada como chamariz é automaticamente replicada no seu próprio perfil (continuando desta forma a tentativa de disseminação da mesma pela Internet).

A principal forma de evitar estas ameaças passa pela adopção de uma atitude crítica relativamente aos conteúdos que lhe são apresentados enquanto navega. Não instale ferramentas de segurança (ou outras) de fontes desconhecidas, não ceda a pedidos de resgate ou pagamentos de multas e não clique em mensagens chamativas em redes sociais, especialmente se verificar que estas tem comportamento epidémico nos perfis dos seus amigos. Em caso de dúvida, fale com 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.

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

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