CRÓNICA VISÃO ELECTRÓNICA
Nº 148 / 2011-11-17
http://www.gestaodefraude.eu
Edgar Pimenta

>> Pescar à rede ou com arpão?

No mundo da ciberfraude, o *phishing* é um termo que data de aproximadamente meados dos anos 90. A semelhança das fonéticas de *fishing* (pescar) e *phishing* não é uma mera coincidência. O objectivo deste último é precisamente o de pescar, apanhar, roubar, informação pessoal que possa ser utilizada de forma indevida e em proveito próprio. Toda e qualquer informação pessoal pode ser alvo de *phishing*, consoante o objectivo dos defraudadores. Por razões que são evidentes, a mais desejada são as credenciais de acesso a *sites* com serviços bancários (vulgo nome de utilizador e palavra-chave).

Existem técnicas de *phishing* relativamente sofisticadas, criadas sobretudo com o objectivo de ultrapassar as diversas protecções criadas pelos bancos (são exemplos destas últimas as matrizes de confirmação e o envio de códigos para sms do cliente). Mas o principio básico estriba-se em técnicas mais simples e que consistem, por exemplo, no envio de emails com origem aparentemente legítima (mas apenas aparentemente), solicitando-nos acções urgentes e para as quais devemos clicar no link fornecido no e-mail. E esse é o primeiro passo para comprometer os nossos dados pessoas (e idealmente, intransmissíveis). Tipicamente, estes *emails* são enviados de forma indiscriminada, entupindo os nossos correios electrónicos (o famoso *spam*). É como pescar com rede. Atira-se ao mar e vê-se o que aparece.

Outra técnica frequentemente usada no *phishing* é o denominado *malware* (vírus, cavalos de tróia e afins). Também este pode ser distribuído de forma indiscriminada, seja por e-mail seja através do acesso a sites "maliciosos" ou ainda através do download de ficheiros infectados. Esse pequeno programa fica escondido no nosso computador, tentando apanhar os nossos dados pessoais. Mas mais uma vez, esta é uma técnica de pesca à rede.

Mais recentemente, começou a surgir uma nova forma de pescar. Ao invés de lançar a rede e ver o que aparece, o alvo é escolhido de forma meticulosa e atacado directamente, com um arpão directo ao alvo. É o denominado *spear-phishing*.

Frequentemente, o objectivo de um ataque destes não são os

CRÓNICA VISÃO ELECTRÓNICA
Nº 148 / 2011-11-17
http://www.gestaodefraude.eu
Edgar Pimenta

nossos dados pessoais mas sim informação à qual teremos acesso na organização onde trabalhamos. O alvo deixa de ser a pessoa e passa a ser a organização. Entramos no mundo da ciber-espionagem industrial. As técnicas utilizadas não diferem muito do phishing "tradicional". Passa pelo envio de um e-mail de chamariz com um ficheiro infectado, com um link para um site malicioso. No entanto, nestes casos, o e-mail é feito com o maior cuidado, de forma a não levantar suspeitas. E muitas vezes utiliza vulnerabilidades das aplicações que não são conhecidas publicamente, tornando a sua defesa ainda mais difícil.

Como de costume, a melhor protecção para este tipo de ataques está entre a cadeira e o teclado. A sensibilização de todos nós para estas situações, a aculturação com os riscos existentes e a criação de um cepticismo positivo são o melhor caminho. A formação é indispensável.