CRÓNICA VISÃO ELECTRÓNICA
Nº 117 / 2011-04-14
http://www.gestaodefraude.eu
Edgar Pimenta

>> Vírus, vírus e mais vírus

1. Eu ainda sou do tempo… em que nas quintas-feiras, dias 12 de um qualquer mês se alterava o relógio do PC, evitando que o mesmo passasse pela famigerada e temida data de sexta-feira 13. Era o tempo do vírus Jerusalém e notícia constante nessas quintas-feiras dia 12. Estávamos na década de 80, a década da guerra-fria. Três décadas depois… todos os dias são sextas-feiras 13.

Os vírus informáticos têm tido evoluções, mutações e degenerações diversas. Deixámos de falar de vírus. Passámos a falar de *malware* para designar todo o software malicioso. Seja vírus, *worms*, *trojans*, *keyloggers*, *spyware*, etc…Toda uma parafernália de coisas estranhas e esotéricas (nota ao leitor: no final do artigo tem um breve glossário).

Consequentemente, é natural o receio actual que nos leva a tentarmo-nos proteger de todas estas ameaças. Mas esse desejo é igualmente usado para nos enganar. É o caso, por exemplo, do *scareware* – um tipo de *malware* que consiste em diversos avisos de que o nosso computador está infectado mas que, coincidentemente, existe um produto, altamente eficaz e de preço acessível que nos resolve todos os problemas e mais alguns. Obviamente, todos estes avisos são acompanhados das necessárias imagens de barras vermelhas indicadoras de perigo, cintilantes avisos de elevado números de vírus e tudo o que nos possa levar a agir rapidamente (entenda-se, adquirir o produto milagroso). A banha da cobra virtual. Fraudes com milhares de anos… Mudam-se os tempos, mantém-se as fraudes…

2. Mas pese o tom jocoso, existe obviamente *malware* que não deve ser tomado de forma tão leviana. Veja-se, por exemplo, o caso do Zeus, um trojan que tem como principal objectivo obter as credenciais de acesso a sistemas de *homebanking*, usando, entre outros, o *phishing* e o spam como meios de difusão. Não existem números exactos de computadores que foram infectados mas estima-se que terão sido vários milhões em todo o mundo.

Outro exemplo, e que é actualmente um caso de estudo, é o *Stuxnet*. Este vírus foi concebido e construído de forma perfeitamen-

te genial, tendo como alvo um conjunto de sistemas até agora "esquecidos" – os sistemas SCADA (muito sucintamente, sistemas de controlo de equipamentos industriais). O seu processo de criação, forma de ataque e o facto do País mais afectado ter sido o Irão e os seus sistemas nucleares ajudam a criar a suspeição de que o *Stuxnet* terá sido construído por uma equipa altamente especializada e com elevados recursos. Algo que só estaria ao alcance de algumas (poucas) nações mundiais. É por isso considerado uma das primeiras e mais representativas armas cibernéticas usadas até agora no espaço virtual. Não terá sido apenas mais um vírus. O seu código e *modus operandi* têm sido exaustivamente estudados e poderá fazer escola. É esperado que variantes deste vírus possam começar a surgir em breve.

3. Todo este mundo do *malware* é um negócio de milhões para as empresas de antivírus. Têm inclusive sido frequentes os rumores e teorias de conspiração de que muitas vezes são estas mesmas empresas e criar e difundir os próprios vírus. Se é assim ou não, dificilmente se saberá. Mas lembro-me, numa conferência, de ouvir alguém dizer: porquê gastar dinheiro a fazer vírus se existe tanta gente a faze-lo de graça? É um argumento que me parece válido. Mas o negócio de milhões não é apenas para as empresas de antivírus. Um novo negócio prolífera no submundo da internet: o aluguer de "ataques".

4. O conceito é simples. Se eu tenho um conjunto de recursos que construí para efectuar algum tipo de ataque, porque não rentabilizá-lo e alugar essa capacidade de processamento e/ou de distribuição de *malware* vendendo esse serviço a terceiros?

Suponhamos, por exemplo, que eu detenho o controlo de uma *botnet* (conjunto de *bots* ou agentes de software residentes em computadores infectados, permitindo o seu controlo remoto) com vários milhares de computadores. Ao invés de a utilizar para provocar *Denial-of-Service* (inundar um site com um número de pedidos anormal, fazendo com que ele deixe de conseguir responder) posso contactar uma empresa com uma "proposta": Caso não seja pago um determinado valor, é lançado um ataque de *Denial-of-Service* aos servidores da empresa, deixando esta de conseguir operar. Se, por outro lado, o valor for pago, para além de não se efectuar o ataque, dá-se um desconto caso a empresa pretenda encomendar um ataque à concorrência. Parece extorsão? Talvez

porque seja mesmo extorsão. Mais uma vez, uma forma de fraude que não é recente mas que ganha novas dimensões no maravilhoso (quase) novo mundo virtual.

Glossário breve

Botnet – conjunto de *bots* ou agentes de software residentes em computadores infectados através de *malware*. Estes bots actuam de forma coordenada em resposta a comandos de um controlo centralizado (controlado por hackers)

Denial of Service – Consiste em sobrecarregar um servidor com um elevado número de pedidos ilegítimos, tornando-se impossível a este dar resposta a qualquer pedido, mesmo quando seja legítimo. O uso de botnets permite lançar ataques de *Denial of Service* de vários pontos distintos, tornando-se mais difícil a sua defesa. São os designados *Distributed Denial of Service*.

Malware – Considera-se como *malware* todo o software de carácter malicioso.

Entre os vários tipos de *malware*, podemos distinguir:

- *Virus* – Pequenos programas que infectam os programas que temos instalados nos nossos computadores, levando a modos de funcionamento fora do normal.
- *Worms* – São um género de vírus mas que se propaga de forma automática (via rede, via e-mail, etc.)
- *Trojan* – ou cavalos de Tróia. São pequenos programas que correm nos computadores sem afectar de forma aparente o funcionamento destes, mas recolhendo informação do utilizador ou permitindo o acesso remoto de um atacante. Os trojans podem vir associados a programas aparentemente legítimos.
- *Keyloggers* – Pequenas aplicações que recolhem a informação digitada pelo utilizador no teclado.
- *Spyware* – Todo o software que tem como objectivo espiar a actividade dos utilizadores.
- *Scareware* – Software que pode ou não causar dado mas

cujo principal objectivo é levar os utilizadores a adquirirem um produto.

Conforme se consegue inferir, existe *malware* que pode ser simultaneamente classificado nestas várias categorias (e noutras aqui não referidas).

Phishing – Consiste em ludibriar o utilizador, levando-o a fornecer dados pessoais ou credenciais de acesso (tipicamente, a sites de *home banking*).

SCADA - Supervisory Control and Data Acquisition – São sistemas de monitorização de sistemas industriais (por exemplo, sondas). Usados frequentemente em sistemas de automação industrial.

Spam – Envio indiscriminado de mensagens não solicitadas (tipicamente por e-mail).