

O Brasil na Rota dos Ataques Internacionais

Pela sua participação na internet mundial, o Brasil é alvo cobiçado e explorado por sofisticados ataques internacionais.

São Paulo, 24/06/08. O Brasil possui, no dia de hoje, 1.362.974 domínios registrados com a terminação .br. Nesse total estão tanto os domínios mais conhecidos, como .com.br, .org.br e .adv.br, quanto o menos usado de todos – .zlg.br – com apenas 3 registros.

Um domínio pode ser descrito como o nome próprio de um site na internet, e os dados de registro nos informam que temos hoje um potencial de bem mais de 1 milhão de sites publicando as mais diversas informações, acessíveis a partir de qualquer país.

Os sites possuem também, na sua maioria, áreas destinadas a receber informações das pessoas que os acessam. Empresas, por exemplo, recebem currículos, sugestões, reclamações etc. Instituições de ensino recebem inscrições, pedidos de informação e até trabalhos de alunos. Associações de classe recebem artigos, sugestões e solicitações de seus associados.

Quando uma instituição possui um site na internet, é preciso tomar medidas para se proteger de diversos tipos de ameaças, entre elas ataques de bandidos que agem via internet.

Nos dois últimos anos temos observado, com uma frequência cada vez maior, que o Brasil está na rota dos mais sofisticados ataques internacionais. Não bastasse os usuários de sistemas bancários online estarem sendo vítimas de golpes praticados no Brasil por quadrilhas especializadas, conforme atestam as operações da Polícia Federal, ataques originados do exterior, em especial da Ásia, tem provocado prejuízos e preocupações para diversas instituições no Brasil.

Somente neste mês de junho, uma onda de ataques originada em uma rede de computadores infectados e voluntários adulterou mais de 200.000 páginas na internet e atingiu milhares de sites no Brasil. Essa onda de ataques se aproveitou de uma vulnerabilidade que é bastante comum, embora seja pouco conhecida e, muitas vezes, mal entendida.

As áreas dos sites destinadas a receber informações de seus usuários precisam abrir pequenas partes para que o usuário remoto grave informações, como por exemplo, um currículo, uma petição, um contrato ou um simples pedido de informações. Através da exploração de falhas no processamento dessas gravações – via injeção de código SQL – é que foi possível essa adulteração massiva de mais de 200.000 sites em poucos dias. Só um dos sites usados no ataque, “heihei117.cn”, consta no Google, nesta data, em mais de 105.000 páginas adulteradas.

Neste momento, o leitor pode estar se perguntando, “para que adulterar um site?”, ou “o que se ganha com isso?”.

	<i>Press Release</i>	PÚBLICO
---	----------------------	---------

Aí é que entra a segunda parte do ataque, pois – diferentemente do que acontecia até pouco tempo – o objetivo de adulterar um site não é mais fazer uma pichação, ou deixar uma marca na calçada da fama dos *hackers*. O objetivo, agora, é usar o site como um intermediário na distribuição de vírus que visam a obter o controle do computador do usuário. Ou seja, a página adulterada passa a servir como um distribuidor involuntário de um vírus de computador, muitas vezes sem que isso fique evidente para o usuário que está acessando ou para o administrador do site. E para piorar ainda a situação, algumas variantes dos vírus distribuídos neste mês eram tão recentes que ainda não são detectadas pela maioria dos anti-vírus do mercado.

Através desse tipo de vírus, do tipo cavalo-de-tróia, é possível furtar dados do computador dos usuários que acessaram o site, incluindo senhas de acesso a banco e arquivos confidenciais. De posse dessas informações diversos tipos de golpes podem ser iniciados, muitos deles tendo como vítima o usuário final.

Esses recentes eventos ilustram de modo inequívoco a necessidade de submeter os sites publicados para a internet a análises periódicas de segurança que incluam as mais modernas técnicas de ataque. Com mais de 1 milhão de domínios e mais de 30 milhões de usuários, o Brasil é hoje um alvo cobiçado e explorado por sofisticados ataques internacionais.

Dinamérico Schwingel é sócio-diretor da e-trust, Certified Information Security Manager (CISM) e mestre em ciência da computação.