Crime virtual fica mais sofisticado
Gustavo Brigatto

Seguindo a mais básica lei de mercado, os preços de informações de contas bancárias, números de cartões de crédito e contas de e-mail roubadas de usuários da internet está subindo no submundo da rede, onde esse tipo de informação vale ouro.

Tome-se o caso dos números de cartões de crédito. No primeiro semestre de 2007 essa informação podia ser encontrada em sites especializados por um preço máximo de US$ 5. Um ano e meio depois, o valor já havia subido seis vezes, para US$ 30. Para uma conta bancária, o valor pago subiu 2,5, de US$ 400 para até US$ 1 mil. De acordo com os números de relatório que a empresa de segurança na internet Symantec divulga hoje em todo o mundo, essas informações foram as mais populares nos sites especializados no assunto em 2008, com 51% do total de ofertas.

A lei de mercado funciona tão bem para a indústria de crimes digitais que até ganhos de escala são passados aos compradores. Tanto no caso dos cartões, quanto das contas bancárias houve deflação nas compras realizadas em grandes quantidades. O valor unitário para números de cartão de crédito comprados no varejo caiu de US$ 0,50 para US$ 0,06 e o de contas bancárias de US$ 30 para US$ 10.

Ganhos financeiros e a facilidade de se criar novas ameaças que têm o objetivo de capturar esse tipo de informação são os motores dessa economia de acordo com Paulo Vendramini, gerente de engenharia de sistemas da Symantec. Segundo ele, só em 2008 a empresa detectou 1,65 milhão de ameaças aos computadores de todo o mundo. O volume é tão grande que representa, em apenas 12 meses o equivalente a 60% de todas 2,6 milhões de amostras de códigos coletadas pela empresa até hoje. O cavalo de troia, programa que rouba informações dos computadores sem o conhecimento do usuário representaram 68% do total dos 50 principais códigos detectados em 2008, uma pequena redução frente aos 69% de 2007.

"Mesmo que 98% dos códigos não sejam muito ameaçadores, ainda assim temos que lidar com eles", diz. Vendramini explica que a maior parte das ameaças está sendo criada por meio de ferramentas conhecidas como "toolkits", programas que permitem que com apenas alguns cliques qualquer pessoa possa desenvolver uma nova ameaça de segurança. Essas novidades, no entanto, são geralmente baseadas em programas já conhecidos, o que facilita sua detecção pelos programas anti-vírus. Esta aliás, é uma definição ultrapassada. "As ameaças hoje combinam diversas estratégias para atingir seus objetivos", explica o gerente da Symantec.

A mais badalada do momento, o Conficker, é um exemplo. Usando uma técnica muito comum antes da internet, a contaminação de dispositivos removíveis, ele também se camufla no sistema para aproveitar a conexão à internet e baixar atualizações de si mesmo ou até mesmo outras ameaças. "O perigo das ameaças que têm muita repercussão não são os danos que ela pode causar, mas o que pode vir depois junto com ela", diz Vendramini. Ele conta que esta foi a maior preocupação da empresa com o Conficker: a possibilidade dele ser apenas uma distração.

Uma das técnicas que tem ganhado espaço entre os criminosos digitais é a infecção de sites confiáveis. Quando entra em algum link, o usuário é direcionado ao conteúdo que deseja acessar, mas, sem que ele perceba, também acessa um conteúdo nocivo que abre o computador para a coleta de informações sigilosas, e também pode transformá-lo em uma ferramenta a serviço do crime. Das vulnerabilidades detectadas pela Symantec para o ambiente da web em 2008, 3,4 mil estavam relacionadas a este tipo de ataque, um aumento de 26% em relação a 2007.

No ano passado, 78% das ameaças enviaram para criminosos informações bancárias e pessoais dos internautas, sendo que 76% delas utilizaram ferramentas para gravação de dados digitados, os chamados keyloggers. E assim os sites de comércio dessas informações continuam sendo supridos, deixando essa economia praticamente imune à crise.

Economia do submundo

Radiografia das ameaças à segurança da informação

Preço das informações roubadas (em US$)

Item	Faixa de preços em 2007*	Faixa de preços em 2008
Números de cartão de crédito	0,50 a 5	0,06 a 30
Contas bancárias	30 a 400	10 a 1000
Endereços de emails**	2 a 4	0,33 a 100
Mailers	8 a 10	2 a 40
Scams***	10	3 a 40

Origem de ataques com destino à América Latina

	País	Porcentual: Da região	Porcentual: Global
1º	Estados Unidos	58%	25%
2º	China	8%	13%
3º	Chile	3%	1%
4º	Argentina	3%	1%
5º	Brasil	3%	3%
6º	Espanha	2%	3%

Tamanho das redes bot na América Latina

	País	Porcentual: Da região	Porcentual: Global
1º	Brasil	42%	6%
2º	Argentina	17%	2%
3º	Peru	10%	1%
4º	Chile	9%	1%
5º	México	7%	1%
6º	Colômbia	4%	1%

Ameaças por país na América Latina

2008	2007	País	Porcentual geral em 2008	Porcentual geral em 2007	Ranking em 2008: Códigos maliciosos	Ranking em 2008: Spam	Ranking em 2008: Sites de phishing	Ranking em 2008: Bots	Origem dos ataques
1º	1º	Brasil	34%	31%	2º	1º	1º	1º	1º
2º	2º	México	17%	22%	1º	5º	4º	5º	2º
3º	3º	Argentina	15%	13%	6º	2º	2º	2º	3º
4º	4º	Chile	8%	8%	5º	4º	3º	4º	5º
5º	5º	Colômbia	7%	6%	3º	3º	5º	6º	4º
6º	6º	Peru	4%	5%	8º	6º	8º	3º	7º

Fonte: Relatório sobre ameaças de segurança Symantec *Até setembro **Por megabyte ***Por semana

Fonte: Valor Econômico, São Paulo, 14 abr. 2009, Empresas & Tecnologia, p. B1.