Investigação internacional desmonta quadrilha que vendia senhas de cartões

Na era da tecnologia digital, os crimes cibernéticos (*cibercrimes*) se tornam progressivamente mais sofisticados e os criminosos mais atrevidos, na avaliação do Departamento de Justiça dos EUA, que anunciou o fim de uma investigação internacional que envolveu 13 países, durou dois anos e resultou no indiciamento de 28 pessoas. Todas foram processadas por crime de "carding". Isto é, elas operavam em uma espécie de *e-Bay* para cibercriminosos — um mercado eletrônico no qual se podia vender e comprar cartões de crédito roubados e de dados completos dos cartões e também de contas bancárias.

Esse mercado também dispunha de mecanismos para testar os dados e confirmar a validade de cartões de crédito e de contas bancárias. Entre os dados, eram disponibilizados nomes das vítimas, nome de usuário, senhas, número do *Social Security* (o CPF americano), endereços e dados de verificação usuais, como código do cartão (normalmente impresso no verso), número de identificação pessoal (*pin number*), data de expiração do cartão, CEP, nome de solteira da mãe, número da conta bancária e *e-mails* de usuários.

O esquema também dispunha de fóruns de informações e mecanismos para testar os dados e validade dos cartões, quando os dados não eram completos ou duvidosos. Uma das práticas era a de fazer doações mínimas e insuspeitas a entidades beneficentes, só com a finalidade de confirmar a utilidade do cartão ou de dados bancários roubados. Só no ano passado, *hackers* do Leste Europeu obtiveram nomes, números de contas, *e-mails* e extratos de contas de mais de 200 mil clientes do *Citibank*, diz o *New York Times*.

Nesse mercado, também se trafica *malwares*, programas que servem para se obter dados de cartões e de contas bancárias diretamente dos sistemas das empresas ou dos computadores das vítimas. O Departamento de Justiça processou, por exemplo, o americano Michael Hogue (conhecido como "xVisceral") por vender um *malware* que dispunha de ferramentas de acesso remoto (RAT – *remote acess tools*), que permite o controle de computadores à distância. Essa ferramenta possibilita ao usuário ligar remotamente a *webcam* da vítima, para espiá-la, e gravar cada tecla digitada em seu computador, para obter nomes de usuário, senha e outros dados, quando ela operava sua conta bancária eletronicamente, por exemplo, ou fazia compras com um cartão de crédito. Hogue vendia o RAT por US$ 50 a cópia, informou o FBI.

Também foi processado o americano Jarand Moen Romtveit (conhecido como "zer0"), por usar ferramentas de *hacking* para roubar informações de bancos de dados internos de um banco, de um hotel e de vários varejistas *online*. Depois, ele vendia os dados a "frequentadores autorizados" do sistema, segundo os autos do processo. Em fevereiro deste ano, vendeu informações de cartões de crédito, pelas quais foi pago com um *laptop*, a um "frequentador autorizado" que, na verdade, era um agente do FBI.

O americano Mir Islam (conhecido como "JoshTheGod") também foi processado por vender dados de mais de 50 mil cartões de crédito, segundo os autos. De acordo com as acusações, Islam se declarou membro da organização *UGNazi hacking group* que, segundo o FBI, "reclamou crédito por inúmeros casos de *hacking* na Internet" e também fundador de um dos fóruns de *carding*, o "Carders.org". Ainda

segundo o FBI, ele foi preso quando tentou usar um cartão de crédito falsificado, carregado com dados roubados, em um caixa eletrônico de Nova York. Ele teria comprado o cartão de um agente que se passava por "frequentador autorizado" dos fóruns.

Os fóruns *UGNazi.com* e *Carders.org*, que serviam de plataforma para o tráfico de cartões de crédito e de dados de contas bancárias, só aceitavam frequentadores conhecidos pela comunidade ou que fossem indicados e avalisados por algum membro dos fóruns, que eram os "frequentadores autorizados". Havia um terceiro fórum, com as mesmas finalidades e mesmas políticas de aceitação de frequentadores, o *Carder Profit*. Mas, na verdade, esse fórum foi criado e operado pelo FBI. Serviu de isca para pegar a maioria dos processados. Os *sites* foram fechados e seus servidores apreendidos.

Os *sites* de operação de *carding* também vendiam objetos furtados, que iam de *iPads*, *iPhones* e outros objetos eletrônicos sofisticados a joias, óculos escuros, roupas, purificadores de ar e maconha sintética. Duas pessoas foram indiciadas por operar um sistema de entrega fraudulento. Elas forneciam endereços de casas desocupadas, com caixas de correio, para onde as mercadorias podiam ser despachadas, sem nunca comprometer os usuários dos cartões roubados.

Das 28 pessoas processadas, 24 foram presas: 13 nos Estados Unidos, seis no Reino Unido, duas na Bósnia, uma na Bulgária, uma na Alemanha, uma na Noruega, uma na Itália e uma no Japão. As outras quatro indiciadas, todas dos EUA, ainda não foram encontradas pelo FBI, que coordenou as operações em todos os países. Na Austrália, Canadá, Dinamarca e Macedônia, onde também há suspeitos, ninguém foi preso ou processado até agora. Com exceção de dois menores da Califórnia, todos os indiciados têm de 18 a 25 anos, noticiaram o *InformationWeek Security* e o *New York Times*.

Pelo tamanho da operação, os resultados não chegam a ser grandiosos, em termos de quantidade de cartões roubados envolvidos, diz o *New York Times*. Só neste ano, a Global Payments, uma processadora de transações sediada em Atlanta, Georgia, relatou violações que afetaram 1,5 milhão de cartões de crédito. E em 2008, o mercado subterrâneo de dados foi inundado com mais de 360 milhões de dados pessoais roubados, a maior parte de cartões de crédito e de débito. Mas, há uma expectativa de que os procuradores do Departamento de Justiça vão tentar obter penas exemplares para os que forem considerados culpados, como uma forma de desestimular esse tipo de crime.

Date Created
30/06/2012