malware robô que abre uma "porta dos fundos", por meio da qual o atacante pode dar instruções. O computador infectado torna-se, então, um escravo, ou zumbi, servindo um computador mestre que pertence a outra pessoa. Quando o hacker já infectou computadores em número suficiente, pode usar os recursos conjuntos da botnet para deflagrar ataques distribuídos de recusa de serviço, campanhas de *phishing* ou e-mails "spam" não solicitados.

Noventa por cento de spam e 80% do *malware* do mundo são transmitidos via botnets. A botnet Grum, que já foi considerada a terceira maior do mundo, por exemplo, teria sido responsável por 18% do tráfego de spam em todo o mundo (totalizando 18 bilhões de mensagens de spam por dia), quando foi encerrada em 19 de julho de 2012. A certa altura, a Grum havia infectado e controlado de 560 mil a 840 mil computadores.

Crimes de informática

A maioria das atividades realizadas pelos hackers é composta por atos criminosos, e a vulnerabilidade dos sistemas que acabamos de descrever faz deles alvos para outros tipos de **crimes de informática**, que são definidos pelo Departamento de Justiça dos Estados Unidos como "quaisquer violações da legislação criminal que envolvem conhecimento de tecnologia da informática em sua perpetração, investigação ou instauração de processo". A Tabela 8.2 fornece exemplos do computador tanto como um alvo quanto como um instrumento de crime. A Seção Interativa sobre Organizações descreve um dos maiores casos de crimes de informática relatados até o momento.

SEÇÃO INTERATIVA: ORGANIZAÇÕES

O ASSALTO AO BANCO DO SÉCULO XXI

Seis atiradores mascarados, com capas de chuvas e metralhadoras, arrombando o cofre-forte e com sacos transbordando dinheiro: essas imagens dos ladrões de banco dos séculos XIX e XX foram amplamente exiladas para o domínio do cinema. A tecnologia do século XXI marcou o início de um novo conjunto de ferramentas: laptops, bancos de dados bancários, códigos de acesso, tarjas magnéticas e caixas eletrônicos. Um dos dez principais assaltos a banco de todos os tempos ocorreu em dezembro de 2012 e em fevereiro de 2013, quando uma rede mundial de criminosos cibernéticos apropriou-se de um total de US$ 45 milhões a partir de duas operações de *hacking* digital.

O primeiro passo foi obter acesso às informações das contas. Em dezembro, uma empresa na Índia foi alvo, e, em fevereiro, uma empresa com sede nos Estados Unidos. Ambas processam transações de cartões de débito pré-pagos da Visa e da MasterCard. Nenhuma delas foi designada. Os processadores de pagamento são conhecidos por empregar uma segurança de rede menos rigorosa do que as instituições financeiras. Os hackers procuraram os cartões de débito pré-pago emitidos por dois bancos do Oriente Médio cujos bancos de dados proporcionavam outro ponto falho de segurança: o Rakbank (Banco Nacional de Ras Al-Khaimah) nos Emirados Árabes Unidos e o Banco de Muscat em Omã.

Em uma nova reviravolta, em vez de acumular vários números de contas, os hackers eliminaram o limite de retirada de apenas um punhado de cartões. Havia dois benefícios para essa estratégia. Em primeiro lugar, apenas alguns cartões infiltrados poderiam render um saque imenso. A informação a partir de apenas cinco cartões emitidos do Rakbank gerou o valor inicial de US$ 5 milhões, com apenas 12 cartões do Bank of Muscat conquistando a melhor parte no segundo ataque. Em segundo lugar, nenhuma conta individual ou empresarial do banco foi exaurida. Em vez disso, os fundos foram extraídos do conjunto de contas reserva, a partir do qual as transações com cartão de débito pré-pago são deduzidas imediatamente e as subcontas individuais (o valor associado a um cartão), reduzidas simultaneamente. Ambas as táticas foram projetadas para atrasar a detecção.

Em seguida, os hackers criaram novos números PIN (número de identificação pessoal) para os cartões. Então, utilizando codificadores de cartões comercialmente disponíveis conectados por portas USB a laptops e PCs, uma rede de subordinados simplesmente usou o software embutido para inserir os dados da conta, clicou Gravar ou Codificar, e passou todos os cartões de plástico com tarja magnética que eles poderiam ter em suas mãos, incluindo cartões de crédito vencidos e os usados como chave de hotel. Com os cartões falsificados em mãos, a quadrilha começou a sacar de caixas eletrônicos em mais de 24 países, incluindo Japão, Rússia, Romênia, Egito, Colômbia, Grã-Bretanha, Sri Lanka, Canadá e Estados Unidos. O roubo de US$ 45 milhões foi realizado por meio de 36 mil transações bancárias durante o período de dez horas.

Cada uma das células, em seguida, pegou a sua cota e enviou o saldo para os líderes dessa máfia do crime cibernético ou enviou-lhes a sua parte na forma de mercadorias de luxo. Em maio de 2013, sete membros da célula de Nova York foram presos; o oitavo, e suposto líder, havia sido encontrado assassinado na República Dominicana no mês anterior. Os líderes da máfia globais ainda não tinham sido capturados e os investigadores ficaram em silêncio sobre seu paradeiro. Uma mochila cada vez mais cheia de dinheiro, como se vê em uma progressão de fotos de vigilância, ajudou a derrubar a gangue de Nova York. Fotos do telefone celular que registraram suas farras e euforia reforçaram o processo contra eles.

As tarjas magnéticas representam uma tecnologia antiga, de mais de quatro décadas atrás, que grande parte do mundo desenvolvido já abandonou. Elas são tão vulneráveis a falsificação, replicação e roubo via fraudadores de cartão portáteis que a indústria de cartões de crédito teve que adotar várias práticas corretivas. Por exemplo, os padrões de uso típico são coletados, de forma que as compras que não se encaixam no molde são marcadas para revisão ou rejeitadas. No entanto, de acordo com a empresa de pesquisa e consultoria Aite Group, todos os anos ocorrem fraudes em cartão de pagamento no total de US$ 8,6 bilhões nos Estados Unidos. Além disso, o Relatório Nilson descobriu que, em apenas 23% do total de compras feitas com cartão internacional, os Estados Unidos registraram 47% de fraudes com cartão de pagamento.

Outras grandes regiões do mundo têm utilizado o cartão com tecnologia EMV (Europay, MasterCard e Visa) por quase 20 anos. O EMV, desenvolvido pela primeira vez em 1994, é um padrão global para cartão com chip (circuito integrado) e seus terminais de atendimento PDV (ponto de venda) e caixas eletrônicos. Muitas vezes denominado sistema de PIN e chip, esses cartões inteligentes armazenam as informações da conta em um chip embutido, e, ao contrário de cartões de tarja magnética, os dados são criptografados com um forte algoritmo de criptografia. A criptografia é usada para autenticar o cartão, o emissor e os dados armazenados. Para maior segurança, o usuário deve digitar um PIN para verificar se essa pessoa é o titular do cartão. À medida que os países implantaram o EMV, suas taxas de fraude de cartão de pagamento despencaram.

No entanto, bancos e comerciantes dos Estados Unidos recusaram-se a bancar o custo envolvido na mudança do processo do sistema de pagamentos. E isso não é uma questão trivial. Existem ao menos 600 milhões de cartões de crédito e 520 milhões de cartões de débito que devem ser trocados. Mais de 15 milhões de leitores de cartões de PDV devem ser substituídos. Mais de 350 mil caixas eletrônicos em todo o país devem ser adaptados ou substituídos. Cada loja, restaurante, salão de cabeleireiro, posto de gasolina, consultório médico, quiosque e máquina de venda automática serão afetados, assim como toda a infraestrutura de processamento de pagamentos de bancos, onde as contas dos comerciantes recebem os depósitos de vendas de cartão de crédito. Processadores de pagamento, que fornecem os sistemas de software e tecnologia de interface com os cartões associados (Visa, Mastercard etc.) e processam as transações dos cartões, também serão afetados.

Enquanto isso, em nome de interoperabilidade global, o resto do mundo deve continuar a emitir cartões EMV com tarja magnética e manter a infraestrutura da tarja magnética. Contudo, a transição dos Estados Unidos poderá finalmente estar próxima, assim como muitas nações estão fixando prazos para parar a produção ou a aceitação de cartões de tarja magnética. Primeiro de abril de 2013 foi o prazo imposto pela Visa e pela MasterCard para que os bancos adquirentes e bancos que processam os pagamentos estejam em conformidade com o padrão EMV para cartão com chip. A partir de outubro de 2015 até o final de 2017, os emissores de cartão EMV, comerciantes, bombas de gasolina e caixas eletrônicos que não estiverem em conformidade com o EMV estarão sujeitos a uma transferência de obrigação de indenizar. Se um comerciante não estiver em conformidade com o EMV na data prevista, assumirá a obrigação de indenizar transações fraudulentas e disputadas judicialmente. O convencimento dos comerciantes para aceitar o risco dos cartões não EMV foi utilizado com sucesso para incentivar empresas europeias a atualizar seus equipamentos PDV nessa última década.

Paradas e recomeços são esperados. A resistência dos comerciantes ainda não foi totalmente superada. Ainda assim, dentro de quatro a cinco anos, a tarja magnética amigável ao hacker deve finalmente estar com seus dias contados. Mas não foi a tempo de frustrar o grande assalto de US$ 45 milhões dos caixas eletrônicos em 2013, sendo que nunca se espera que esses sacos cheios de dinheiro sejam recuperados.

Fontes: Colleen Long e Martha Mendoza, "Bloodless bank heist impressed cybercrime experts", *Associated Press*, 10 mai. 2013; Colleen Long, "Feds in NYC: Hackers stole $45M in ATM card breach", *Associated Press*, 10 mai. 2013; Marc Santora, "In Hours, Thieves Took $45 Million in A.T.M. Scheme", *New York Times*, 9 mai. 2013; Peter Svensson, Martha Mendoza e Ezequiel Abiú López, "Global network of hackers steals $45M from ATMs", *Associated Press*, 10 mai. 2013; "EMV Chip Technology, Secure Electronic Payments", *Forbes*, 7 mar. 2013; "EMV in the USA: After 8 Years of Foot-Dragging and Delays, What's the Real Timeline for Adoption Look Like?", *PRNewswireiReach*, 21 fev. 2013.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Descreva as vulnerabilidades de segurança exploradas pelos hackers.
2. Quais fatores humanos, organizacionais e tecnológicos contribuíram para esses problemas?
3. Quais soluções estão disponíveis para esse problema? Quão difícil é a implantação dessas soluções? Por quê?

Tabela 8.2

Exemplos de crime de informática.

Computadores como alvos de crime
Violar a confidencialidade de dados computadorizados protegidos
Acessar um sistema de computador sem autorização
Acessar intencionalmente um computador protegido para cometer fraude
Acessar intencionalmente e infligir danos a um computador protegido, de maneira negligente ou deliberada
Transmitir intencionalmente um programa, código de programa ou comando que deliberadamente danifique um computador protegido
Ameaçar causar danos a um computador protegido
Computadores como instrumentos de crime
Roubo de segredos comerciais
Cópia não autorizada de software ou de material com propriedade intelectual registrada, como artigos, livros, músicas e vídeos
Esquemas para defraudação
Usar e-mail para ameaças ou assédio
Tentar interceptar comunicações eletrônicas intencionalmente
Acessar ilegalmente comunicações eletrônicas armazenadas, inclusive e-mail e caixa postal de voz
Possuir material de pedofilia armazenado em um computador ou transmiti-lo eletronicamente

Ninguém sabe a magnitude do problema dos crimes de informática — quantos sistemas são invadidos, quantas pessoas estão envolvidas nessa prática ou o prejuízo econômico total. Conforme o estudo sobre o custo anual de crime cibernético, realizado em 2012 pelo Instituto Ponemon e patrocinado pela HP Enterprise Security, o custo médio anual de crimes cibernéticos das organizações pesquisadas foi de US$ 8,9 milhões por ano (Ponemon Institute, 2012). Muitas empresas relutam em registrar esse tipo de crime, seja porque pode haver funcionários envolvidos ou porque a organização teme que, ao tornar pública a sua vulnerabilidade, sua reputação fique manchada. Os tipos de crime de informática mais danosos do ponto de vista financeiro são os ataques DoS, as atividades de códigos maliciosos e os ataques baseados na Web.

Roubo de identidade

Com o crescimento do comércio eletrônico e da Internet, o roubo de identidade tem se tornado especialmente perturbador. **Roubo de identidade** é um crime em que um impostor obtém informações pessoais importantes, como número de identificação da Previdência Social, número da carteira de motorista ou número do cartão de crédito para se passar por outra pessoa. As informações podem ser usadas para obter crédito, mercadorias ou serviços em nome da vítima, ou para dar falsas credenciais ao ladrão.