Gabriel Mazurco Ribeiro RA: 1611014

Lucas Bueno RA: 142441

Escreva um ensaio sobre o Ovo do Cuco (Cucckoo's Egg), que envolveu Clliford Stoll no que foi considerado o primeiro caso documentado de resposta a um incidente e detecção de invasão

Clifford Stoll, narra em seu livro: O Ovo de Cuco escrito na década de 80, o acontecido em primeira pessoa sobre a caça a um hacker de computadores, que entrou em um computador no Lawrence Brkeley National Laboratory (LBNL).

Um dia seu supervisor, Dave Cleveland, pediu que Stoll resolvesse um erro de contabilização de US $0,75 nas contas de uso de computadores. Stoll rastreou o erro para um usuário não autorizado que usou somente 9 segundos de um computador e não pagou, eventualmente ele percebeu que esse usuário era um hacker que adquiriu acesso Superusuário ao sistema interno, que explorou a vulnerabilidade na função movemail do GNU Emacs original.

Stoll reuniu cerca de 50 terminais, bem como teleimpressores, compartilhadas das mesas de seus colegas de trabalho, assim ele teria fisicamente 50 linhas telefônicas recebidas. Quando o hacker entrou, Stoll localizou a linha telefônica, que estava vindo do serviço de roteamento Tymnet, com isso ele conseguiu rastrear a intrusão em um call center no MITRE, um empreiteiro de defesa em MCLean, Virginia. Durante 10 meses, ele gastou muito tempo e esforço rastreando o hacker. Ele viu que o hacker usava uma conexão de baud de 1200, através de um modem telefônico.

Depois de devolver os terminais de seus colegas que estava compartilhado com ele, Stoll deixou um teleprinter conectado à linha de intrusão para ver e registrar tudo o que o hacker fizer, ele observou como o hacker buscava e como ele conseguia o acesso não autorizados a bases militares ao redor do Estados Unidos, procurando arquivos que continham palavras como ”nuclear” ou “SDI”. O hacker montou um cavalo de Tróia para procurar arquivos de senhas, muitos administradores de sistemas nunca se preocupam em alterar as senhas de seus padrões de fábrica, mesmo em bases militares.

Com o tempo de investigação, Stoll entrou em contato com vários agentes do FBI, CIA, NSA e Air Force OSI. Este foi o primeiro ataque documentado, Stoll parece ter sido o primeiro a manter um diário de bordo das atividades do hacker. Mas o FBI era desinteressado porque nenhuma grande quantia de dinheiro estava envolvida.

Estudando seu diário de bordo, Stoll observou que o hacker estava familiarizado com VMS, AT & T Unix e que tendia ser ativo em torno do meio dia, hora do Pacífico, portanto ele levantou a hipótese de que, as contas de modem são mais baratas anoite, e a maioria das pessoas tem aula durante o dia ou trabalho, o hacker estava em um fuso horário a certa distância a leste.

Com ajuda de Tymnet e vários agentes, Stoll descobriu que a intrusão estava vindo da Alemanha Ocidental via satélite. Uma agência postal alemã a Deutsche Bundespost, que também tem autoridade sobre o sistema telefônico alemão e eles rastrearam os telefonemas para a universidade em Bremen. Para chamar a atenção do hacker, Stoll criou um elaborado hoax – conhecido hoje como honeypot – inventando um departamento fictício na LBL que supostamente tinha sido recém-formado por um contrato "SDI". Quando ele percebeu que o hacker estava interessado na entidade falsa SDI, ele enche. O trabalho deu certo, e o Deutsche Bundespost conseguiu localizar o hacker em sua casa em Hanover. Nome do hacker foi Markus Hess, e ele tinha sido contratado por alguns anos na venda dos resultados de suas invasões ao soviética KGB. Não havia prova auxiliares deste quando um húngaro espião contatado o SDInet fictícia no LBL pelo correio, com base em informações que ele só poderia ter obtido através de Hess. Aparentemente, esse era o método do KGB para verificar se Hess estava inventando as informações que ele estava vendendo.

Stoll mais tarde voou para a Alemanha para testemunhar no julgamento de Hess e um confederado.