**Fraudes em caixas eletrônicos – Análise do software utilizado para coletar dados**

Terminais bancários de autoatendimento, popularmente conhecidos como caixas eletrônicos, são equipamentos construídos para facilitar o acesso do cliente aos serviços bancários básicos. A praticidade e a agilidade do atendimento automatizado são alguns dos motivos pelos quais podemos encontrar este serviço em diversos tipos de estabelecimentos, de supermercados a postos de gasolina.

A facilidade de acesso a esses equipamentos, muitas vezes em locais sem a devida segurança, é um atrativo para a ação de criminosos. Ataques com explosivos ou ferramentas industriais, com o objetivo de extrair o dinheiro contido nas máquinas, são o exemplo mais comum de ações criminosas. Por outro lado, o cliente tem a vulnerabilidade de seus dados bancários, que podem ser obtidos através da simples observação da utilização do terminal, ou com o auxílio de equipamentos eletrônicos preparados para coletar informações contidas nos cartões e/ou digitadas no teclado.

O presente trabalho apresenta o estudo de caso de um equipamento eletrônico, que simula um terminal de autoatendimento bancário, preparado para coletar informações dos clientes que tentassem fazer transações. A carcaça do dispositivo eletrônico possui as mesmas características físicas de um terminal de autoatendimento e é instalado sobre a tela e teclado de um terminal de um banco. Os objetivos dos exames são constatar a eficácia do equipamento em coletar senhas e dados de cartões magnéticos, identificar dados de possíveis vítimas armazenados na memória do equipamento e revelar para onde são enviadas estas informações.

Para responder a estes questionamentos, foi adotada a metodologia de análise do programa instalado no HD do dispositivo, além da descrição dos componentes eletrônicos utilizados em sua construção.

A análise do equipamento ocorreu no setor de perícias em equipamentos eletrônicos do departamento de Criminalística SPTC-ES, ambiente com equipamentos adequados. Pela análise visual, constatou-se que o equipamento era composto por teclados, baterias, leitor de cartões magnéticos e um notebook, adaptados em uma carcaça de fibra de vidro que imitava um terminal bancário.

 

**Figura 1.** Parte Frontal do equipamento. **Figura 2.** Parte traseira do equipamento.

Para iniciar a análise do programa, foi retirado o disco rígido do dispositivo e realizado o procedimento de duplicação forense. Da análise dos dados contidos na mídia, observou-se a presença do arquivo executável do programa, o qual simulava a operação de um terminal de autoatendimento real, porém não foi encontrado qualquer banco de dados ou arquivos com as informações solicitadas ao exame pericial.

Sem resultados satisfatórios por mecanismos de busca, partiu-se para uma outra abordagem, que se mostrou mais eficaz. Foi realizada a análise estática avançada do software por meio de engenharia reversa do código, utilizando um programa descompilador. Neste tipo de análise, a linguagem de máquina de um programa compilado é revertida em linguagem de programação de alto nível, podendo, assim, ter suas instruções analisadas pelo examinador. O software descompilador utilizado foi o “dotPeek” (software gratuito disponível em “https://www.jetbrains.com/decompiler/”).

O descompilador foi capaz de apresentar o código fonte do programa na linguagem “C#”, tornando possível o entendimento das funções e, principalmente, localizar, na estrutura de pastas da mídia, os arquivos com as informações solicitadas.

Em resumo, o programa simulava as telas normais de operação de um terminal de autoatendimento, solicitava a inserção do cartão do usuário, assim como a senha numérica e a senha de segurança alfabética. Ao final da tentativa de transação, exibia a mensagem de erro de comunicação e solicitava ao cliente se dirigir a outro terminal. Os dados digitados e as informações contidas nas trilhas da tarja magnética do cartão inserido no equipamento eram criptografados e armazenados em um arquivo de biblioteca dinâmica (.dll) e também enviados via SMS para dois números telefônicos.

Analisando o código fonte do programa, foi possível identificar a função de criptografia e a chave criptográfica utilizada para cifrar os dados coletados. Com essas informações, gerou-se um algoritmo (na linguagem C#) para descriptografar os dados. O programa tem como entrada o arquivo .dll com os dados criptografados e, como saída, um arquivo de texto com os dados descriptografados: informações das trilhas magnéticas e senhas.

Por último, realizou-se o teste do equipamento completo. Foi instalado a cópia forense do HD no dispositivo e retirado o modem de comunicação, para evitar que qualquer informação pudesse ser enviada. Tomadas as ações necessárias, simulou-se a utilização do equipamento, com a inserção de um cartão magnético de teste e uma senha fictícia. Logo após, o HD foi retirado e, ao descriptografar o arquivo de biblioteca dinâmica, foram encontrados os dados do cartão e a senha falsa digitada, comprovando a funcionalidade do equipamento.

Após todas as etapas do exame, comprovou-se a eficácia do equipamento em coletar senhas de usuários e dados de cartões magnéticos. As informações relevantes foram obtidas com sucesso, e um novo procedimento operacional padrão para exames periciais nesse tipo de equipamento foi criado.

REFERÊNCIAS BIBLIOGRÁFICAS

1. VELHO, Jesus Antônio; Vários Autores.*Tratado de computação Forense*. 1º ed. Campinas-SP, 2016.

2. DEITEL. Harvey. *C# - Como Programar*. São Paulo-SP, Ed. Pearson Education, 2003.