DOI: 10.5769/C2013006 or http://dx.doi.org/10.5769/C2013006

# Emprego da Engenharia Reversa para caracterização do *modus operandi* das máquinas caça-níqueis quanto à prática de jogo de azar ou outras fraudes

Cleverson Esteves da Silva, Galileu Batista de Souza, and Ricardo Zelenovsky

*Abstract*—**Despite gambling be forbidden in Brazil since 1941, the growing access to computer equipment brings a new kind of slot machines that, instead of using a specific hardware group, has its environment simulated by a computer program and is built with common and obsolete hardware items. Due to the uncertainty about internal behavior of the management programs that controls these equipments, the forensic exams have not been as conclusive whether they offer properties to allow player influence on final result. Using reverse engineering techniques, this study presents a set of evidences about gambling and frauds in the "Halloween" machines applications. Furthermore, in order to instruct future analyses on machines of different class, here is shown the methodology used to obtaining the necessary information by forensic exam, that could be adapted to other situations involving same kind of applications not covered in this study.**

***Palavras-chave: slot machines; gambling; reversing; forense computin; fraudg.***

## I. Introdução

Assim como a tecnologia tem invadido o cotidiano dos cidadãos de bem, de forma acelerada e irreversível, trazendo comodidade e celeridade para tarefas anteriormente dispendiosas, a criminalidade tem se especializado e utilizado a tecnologia ao seu favor [1].

Algumas modalidades de crime praticadas através de equipamentos eletrônicos encontram uma barreira na análise interna das instruções lógicas responsáveis por gerenciar tais recursos. Um exemplo notório são as máquinas caça-níqueis (videobingo), cujas constantes apreensões têm sido noticiadas nos meios de comunicação em todo o território nacional [2] [3], representando uma grande demanda de trabalho pericial aos órgãos de perícia oficial estaduais e Federal. Porém, um suposto controle por parte do apostador é o principal argumento de defesa para impedir que tais equipamentos sejam enquadrados no dispositivo legal que trata dos jogos de azar, alegando que não se trata de sorte, mas sim de técnica.

As máquinas de videobingo utilizam-se dos principais componentes de microcomputadores de plataforma *personal computer* como placa-mãe, microprocessador, memória e dispositivo de armazenamento (muitas vezes obsoletos e de baixo custo), visto que estes são de fácil aquisição. Tais equipamentos não necessitam de recursos especiais e a aplicação, responsável por simular o ambiente do jogo, é armazenada em um disco magnético ou dispositivo de memória semicondutora. Por usarem componentes padrões da indústria, seus elementos poderem ser facilmente transportados em separadamente sem que desperte qualquer suspeita sobre a sua destinação final.

A simplicidade e padronização do *hardware* contrastam com a incerteza do funcionamento interno dos aplicativos das máquinas de videobingo. Diante da carência de trabalhos que analisem em profundidade o comportamento interno dos programas computacionais que simulam o ambiente de uma máquina caça-níquel, bem como da escassez de documentação técnica sobre os elementos de *software* ou sobre os itens específicos de *hardware*, supostamente atribuídos a suspeita de ilegalidade que paira sobre esses equipamentos. O presente trabalho analisa em profundidade uma família de máquinas caça-níqueis visando caracterizar o comportamento do seu software controlador a fim de caracterizá-lo como jogo de azar e se o mesmo trabalha com parâmetros que permitem a manipulação do resultado do jogo.

Dos equipamentos recebidos a partir do ano de 2009 na Seção de Criminalística de Ji-Paraná (RO) para análise, somente integram o objeto de estudo do presente trabalho as máquinas que apresentam cartão de memória semicondutora conectada ao *slot* IDE da placa-mãe e que se mostraram operantes à época do recebimento. Aquelas máquinas, cuja aplicação está gravada em uma placa de circuito impresso que substitui a placa-mãe ou em placas que são inseridas em *slots* PCI ou ISA, foram descartadas da amostra por corresponderem a uma geração de equipamentos que está cada dia mais obsoleta devido à especificidade do *hardware*.

O universo de estudo do presente trabalho consiste de 08 (oito) exemplares de máquinas caça-níquel, todas pertencentes à categoria denominada "Halloween", que tem predominância absoluta no Estado de Rondônia e apresenta a mesma forma externa de interação e a mesma forma interna de exibição de resultados de máquinas analisadas por órgãos periciais de outras regiões brasileiras. Apesar da pequena quantidade de máquinas, o universo de estudo oferece ao todo 18 (dezoito) opções de jogos aparentemente distintos, mas com jogabilidade semelhante.

A realização de um experimento estatístico, traçando um perfil do seu funcionamento após exaustivas execuções das máquinas de videobingo [4], seria inviável, pois nas máquinas caça-níquel convencionais existe somente um elemento de interação com o equipamento, representado pela alavanca, ao passo que as máquinas que se pretende analisar no estudo proposto possuem diversos elementos de interação, representados pelos botões do painel, todos com finalidades específicas, o que aumenta de forma exponencial a quantia de combinações necessárias para se traçar um perfil de funcionamento confiável.

Mais precisamente, o estudo apresentado neste artigo tem por objetivos:

- Traçar um perfil de comportamento de tais máquinas com base no modo de operação inferido a partir dos elementos materiais coletados com técnicas de Engenharia Reversa. Assim, equipamentos similares podem ser examinados mais rapidamente por Peritos Criminais de todos os Estados da Federação. Ademais, poderão eles ser conclusivos em seus laudos no que se refere à prática de jogo de azar e outras fraudes, encerrando definitivamente a discussão que vem se prolongando no âmbito forense desde o surgimento de tais máquinas;
- Elencar pontos de similaridade de jogos aparentemente distintos, possibilitando que versões do aplicativo principal de máquinas tipo "Halloween" não analisadas neste trabalho sejam inferidas quanto à prática da modalidade de jogo de azar ou fraudes diversas, tanto através da comparação direta do arquivo executável, como através da identificação das características operacionais e comportamentais apresentadas pelo presente estudo;
- Apresentar uma metodologia de análise que auxilie o exame pericial de equipamentos similares apreendidos em todo o território Nacional, fornecendo diretrizes que visem à obtenção de informações relevantes à atividade pericial, inclusive em aplicações da mesma natureza que não pertençam à família "Halloween".

A organização do trabalho é como segue. Na seção II são apresentadas considerações acerca da definição dos jogos de azar a luz da legislação. A seção III compreende a análise interna dos jogos através da Engenharia Reversa, nas suas modalidades de análise *online* e *off-line* e tem como foco a comprovação do enquadramento como jogo de azar. Por fim, a seção IV exemplifica a metodologia empregada na análise, permitindo que máquinas similares sejam prontamente analisadas e que metodologia similar à descrita no artigo possa ser utilizada para os demais casos.

## II. Jogos de Azar

O jogo de azar é aquele onde a única ação disponível ao jogador é aguardar o resultado processado pelo mecanismo do jogo, quer ele seja manual ou automatizado, na esperança de que seja compatível com o valor escolhido, sem que haja qualquer possibilidade de interferência direta ou indireta depois de iniciado o processo, estando o praticante da ação "a mercê da sorte" [5].

Assim, para se caracterizar um determinado jogo como sendo de azar, deverá haver aleatoriedade suficientemente capaz de impedir a previsão de resultado, mesmo que haja circunstâncias matemáticas que contribuam para o aumento ou redução da probabilidade de determinado resultado ocorrer. Apesar de os jogos de azar variarem em relação à probabilidade de ganho ou perda, seus resultados, ainda assim, dependem exclusivamente do fator sorte.

Promulgado em 03 de outubro de 1941, pelo então Presidente da República Getúlio Vargas, o Decreto Lei nº 3688/41 institui a Lei de Contravenções Penais e define em seu art. 50 §3º o jogo de azar como sendo o jogo em que o ganho e a perda dependem exclusiva ou principalmente da sorte do apostador, acrescentando ainda ao rol de tal prática delituosa, as apostas em qualquer modalidade esportiva.

No caso das máquinas caça-níqueis, devido ao fato de os equipamentos possuírem um conjunto de botões que passa ao apostador uma falsa impressão de controle, tem sido constatada uma divergência de entendimento entre as sentenças prolatadas pelo Poder Judiciário em todo o território nacional [6] quanto ao enquadramento das máquinas caça-níquel atuais, na legislação especial sobre jogos de azar.

## III. Análise das Máquinas Caça-níquel

Ao examinar preliminarmente as máquinas de videobingo como um todo, observa-se que a caracterização do seu funcionamento em um aspecto amplo e geral está diretamente ligada a análises de itens específicos e de menor abrangência como as características físicas inerentes às formas de interação do usuário com o equipamento; o hardware que a compõe; os softwares que dão suporte ao hardware e ao ambiente do jogo; e o ambiente de execução da aplicação e o software aplicativo, propriamente dito, responsável por implementar toda a regra de negócio que irá determinar a resposta dada a cada interação sofrida.

Nesta ótica, a Engenharia Reversa de Software apresenta-se como importante ferramenta na análise forense de tais equipamentos, pois "(…) é executada com o objetivo de obter uma melhor compreensão de um sistema existente" e "(…) é composta de uma série de técnicas utilizadas para a descoberta de informações a respeito de um sistema de software" [7], sendo responsável pela obtenção de um modelo abstrato do comportamento do sistema [8].

### *A. Usabilidade*

A máquina apresenta um conjunto de jogos; uma vez escolhido um, ele é aberto em tela cheia exibindo em seu pano de fundo o motivo que dá nome ao jogo (Figura 1). No terço superior da tela são exibidas as informações referentes ao "crédito", que se refere ao saldo do apostador no equipamento

e ao "prêmio", que é calculado com base na aposta que foi realizada, caso haja um resultado favorável ao apostador.

O valor do prêmio tende ao crescimento a cada resultado desfavorável. É possível multiplicar o valor da "aposta" (consequentemente do prêmio), através do produto da quantia de combinações (linhas) escolhidas, por um fator multiplicador entre 1 e 10, escolhido através do botão "aposta" e cujo valor será deduzido do crédito do apostador.

No terço inferior da tela principal, o jogo exibe o valor "acumulado" (*jackpot*) pela máquina e que corresponde à premiação especial paga em caso de resultado compatível com uma sequência pré-estabelecida. Quanto maior o valor acumulado por uma máquina, maior é o apelo para que os apostadores a escolham. Um determinado jogo, conforme a sua versão, pode apresentar um ou mais acumulados.


Figura 1. Tela principal do jogo com a opção "linha 9" ativada.

O terço médio da tela, por sua vez, apresenta a área de exibição das figuras sorteadas, a qual é composta por 05 (cinco) colunas, contendo 03 (três) figuras cada, representando uma matriz de 3 x 5, que totaliza uma quantia de 15 (quinze) quadrantes, onde são distribuídas as 10 (dez) figuras distintas que compõem o jogo, conforme o sorteio realizado.

À direita e à esquerda da matriz são exibidos valores numéricos que variam conforme a quantidade máxima de linhas (apostas) suportadas pelo equipamento. As linhas são pré-estabelecidas pelo desenvolvedor da aplicação e são sempre formadas por 05 (cinco) imagens dispostas sequencialmente na horizontal ou diagonal.

Quanto mais linhas o apostador escolher, maior será o valor deduzido do seu crédito e disponibilizado na forma de aposta na rodada corrente, já que os créditos são deduzidos na proporção de 1 (um) para cada linha escolhida, na modalidade de aposta simples ou 10 (dez) para um, na modalidade de aposta máxima.

$$Aposta = n(Linhas\ Escolhidas) \times Fator\ de\ Aposta \qquad (1)$$

Até que sejam inseridos créditos, o equipamento permanece no modo de demonstração. Depois de inseridos créditos o apostador poderá:

- escolher em quantas linhas deseja apostar, pressionando qualquer um dos botões referentes a linhas;
- exibir a tabela de premiação através do botão "tabela";
- realizar uma jogada automática, com escolha de linhas e valores de aposta por parte da própria máquina, através do botão "auto";
- optar pela aposta máxima permitida pelo equipamento, configurando automaticamente o valor máximo de linhas e a modalidade máxima de aposta, através do botão "aposta máxima";
- escolher um valor entre 1 e 10 para a modalidade de aposta, que será multiplicado pela quantia de linhas escolhidas, através do botão "aposta";
- realizar o sorteio depois de configuradas as suas opções de aposta, através do botão "jogar";
- encerrar sua sessão na máquina, resgatando os créditos existentes, através de botão afixado na lateral do gabinete, caso esta opção seja oferecida pelo equipamento.

### *B. Aspectos Físicos*

Apesar de variar em sua forma externa, que geralmente consiste de uma caixa em madeira compensada pintada na cor preta, as máquinas de videobingo apresentam basicamente uma quantidade que varia entre oito e dez opções diretas de interação, representadas pelos botões do seu teclado, mas que se presume ter a capacidade de proporcionar diversas outras opções indiretas quando combinadas entre si.

Tais botões apresentam rótulos que fazem alusão modalidades de apostas como "cartelas" e "linhas", que apresentam opções numeradas, ou ações do apostador tais como "pagar", "aposta" e "jogar".

As máquinas de videobingo são compostas por uma placa-mãe da plataforma *personal computer,* com um cartão de memória representando o armazenamento persistente da máquina e com capacidade não superior a 512MB. Armazena o sistema operacional, a aplicação principal quanto os programas auxiliares, destinados à preparação do ambiente..

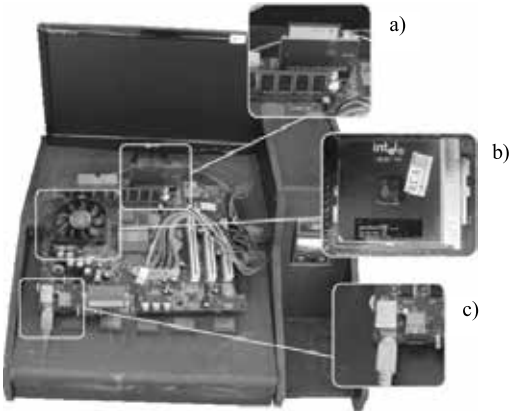


Figura 2. Composição gráfica ilustrando o interior dos equipamentos.

Durante a análise, observou-se que todos os conjuntos microprocessador pertencem à plataforma PC (*personal computer*), com predominância dos modelos Pentium III do fabricante Intel e K6 II do fabricante AMD, conforme destacado pela alínea "b" da figura 2, embora possa ser executado em qualquer outro processador da família 8086, superior ou inferior, conforme exames realizados.

A conexão do equipamento com o seu teclado customizado dá-se indiretamente através de conectores DIN 5 ou PS/2 com o auxílio de uma placa de circuito impresso, conforme destacado pela alínea "c", ou diretamente mediante a conexão de uma placa de circuito impresso, dotada de porta paralela, que recebe os valores produzidos pelos botões do teclado com o auxílio de um conector DB25.

A alimentação de créditos na máquina é realizada através de cédulas de moeda corrente com o auxílio de um dispositivo noteiro, diretamente ligado ao teclado customizado. Ele envia uma quantia *n* de pulsos, previamente estipulados para cada padrão calibrado [9] como se a tecla "P" houvesse sido pressionada *n* vezes no teclado convencional. Em suma, para o resto do equipamento, o noteiro e o teclado customizado comportam-se como um teclado convencional, com a correspondência de teclas apresentada na Tabela I.

TABELA I. Correspondência dos pinos da porta paralela

| Funcionalidade | Tecla | ASCII | Hexa | Pino 1 | Pino 2 |
|---|---|---|---|---|---|
| **Linha 1** | Y | 89 | 59 | 5 | 13 |
| **Linha 5** | J | 74 | 4A | 5 | 12 |
| **Linha 9** | H | 72 | 48 | 5 | 11 |
| **Linha 15** | M | 77 | 4D | 5 | 10 |
| **Linha 20** | N | 78 | 4E | 5 | 9 |
| **Tabela** | T | 84 | 54 | 4 | 13 |
| **Auto** | V | 86 | 56 | 4 | 12 |
| **Aposta Máxima** | F | 70 | 46 | 4 | 11 |
| **Aposta** | G | 71 | 47 | 4 | 10 |
| **Jogar** | B | 66 | 42 | 4 | 8 |
| **Encerrar jogo** | R | 82 | 52 | 5 | 6 |
| **Noteiro** | P | 80 | 50 | 24 | 25 |

### *C. Ambiente Operacional do Jogo*

A preparação do ambiente operacional do jogo foi caracterizada através da identificação e classificação dos arquivos presentes no dispositivo principal de armazenamento, separando aqueles que são de uso geral pelo sistema daqueles de uso exclusivo e que possuem influência direta na aplicação. Além disso, dentre os arquivos listados, foram identificados aqueles protegidos por senha ou dissimulados com o objetivo de dificultar o seu reconhecimento pelo sistema operacional e ferramentas de análise forense.

#### *1) Identificação dos arquivos*

A análise do interior dos dispositivos de armazenamento revelou que todos os equipamentos possuem em comum um conjunto de arquivos armazenados na raiz da única partição (FAT) presente no dispositivo de armazenamento. Ainda na raiz da partição há um diretório denominado "dos" e outro denominado "data", destinados ao armazenamento de arquivos da aplicação e da base de dados, respectivamente. O sistema operacional MS-DOS dificultou bastante qualquer análise, haja vista a carência de ferramentas de monitoramento e Engenharia Reversa para essa plataforma.

Ao examinar o arquivo "autoexec.bat", verificou-se que durante a inicialização da máquina, além de configurar a variável de ambiente "path" para o diretório "c:\dos", levanta-se a hipótese de criação de uma unidade virtual representada pela letra "d", onde é chamada posteriormente a execução do aplicativo "programa.exe".

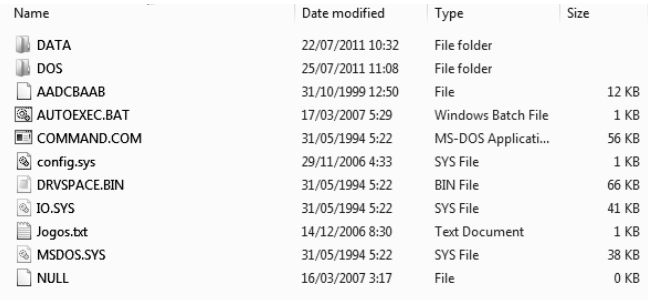


Figura 3. Arquivos presentes na raiz do dispositivo de armazenamento

Dentre os arquivos armazenados pelo diretório "data", somente o arquivo "base.dbf", apresenta-se relevante. Além de apresentar nome que sugere uma base de dados, possui assinatura compatível com o formato dBase. Ao ser editado, tal arquivo revelou uma listagem de campos aparentemente destinados à configuração das máquinas. Porém, parte dos campos não possui valor armazenado, sugerindo serem utilizados somente quando da execução da aplicação, enquanto que outros apresentavam conteúdo codificado. Apenas os campos que traziam valores em ponto flutuante, referentes aos índices de acumulação da máquina, apresentaram-se legíveis durante a análise *off-line*.

Da mesma forma, dos arquivos armazenados no diretório "dos", somente alguns apresentaram relevância para o presente estudo, como o arquivo "menu.exe", responsável pela exibição da tela de seleção de jogos e consequentemente por carregar o jogo escolhido e o arquivo "jogos.bin", que apresenta assinatura compatível com a base de dados em arquivo dBase.

Além desses dois arquivos que as várias máquinas possuem em comum, foram identificados arquivos com a extensão "sys", onde os nomes e a quantidade de arquivos apresentados por cada equipamento são compatíveis com os itens exibidos na tela de seleção de jogos. A convergência entre as opções apresentadas na tela inicial de seleção e os arquivos armazenados, indica que cada arquivo corresponde a um dos jogos oferecidos pelo equipamento.

Ao todo, nos equipamentos analisados, foram encontrados 23 (vinte e três) arquivos com extensão "sys", embora a análise preliminar dos equipamentos tenha apresentado uma lista de 18 (dezoito) jogos distintos.

Verificou-se que, com base na assinatura do cabeçalho, tratam-se de arquivos compactados no formato ZIP, com a

ferramenta de compressão de código "PKLite, com senha de proteção. A existência do arquivo "pkunzip.exe" no diretório "dos", que apresenta apenas a capacidade de descompressão do formato ZIP, sugere que tais arquivos são descompactados durante a execução da máquina.

Após descompactar os arquivos conforme descrito na próxima subseção, verificou-se que apesar da divergência de tamanho do arquivo final, cada um dos jogos consiste de uma quantidade variável de arquivos na extensão "dat", com nomes compatíveis entre si, e um único arquivo executável denominado "programa.exe". Nos vinte e três jogos presentes foram identificadas três variações de tamanho para o arquivo "programa.exe", sugerindo que ao invés de cada jogo possuir uma estrutura interna distinta, vários deles compartilham do mesmo arquivo principal.

TABELA II. Comparativo de conteúdo dos arquivos "sys".

| Nome | Executáveis | Tamanho | Total |
|---|---|---|---|
| bigb1ac.sys | programa.exe | 273 KB | 339 |
| buca2.sys | programa.exe | 281 KB | 335 |
| buca2ac.sys | programa.exe | 281 KB | 341 |
| camp2ac.sys | programa.exe | 281 KB | 314 |
| camp2007.sys | programa.exe | 281 KB | 321 |
| fruta.sys | programa.exe | 281 KB | 315 |
| fuga1ac.sys | programa.exe | 273 KB | 372 |
| fuga2acm.sys | programa.exe | 281 KB | 376 |
| gcard1.sys | programa.exe | 273 KB | 333 |
| goldcard.sys | programa.exe | 273 KB | 333 |
| hallo1.sys | programa.exe | 273 KB | 335 |
| hallo1ac.sys | programa.exe | 273 KB | 335 |
| hallo2.sys | programa.exe | 281 KB | 335 |
| hallo2ac.sys | programa.exe | 281 KB | 335 |
| hallo2tk.sys | programa.exe | 281 KB | 331 |
| hallofor.sys | programa.exe | 677 KB | 335 |
| oro2ac.sys | programa.exe | 677 KB | 236 |
| pantanal.sys | programa.exe | 273 KB | 373 |
| sexy2.sys | programa.exe | 281 KB | 333 |
| sexy2ac.sys | programa.exe | 281 KB | 373 |
| trago1ac.sys | programa.exe | 273 KB | 331 |
| vacalo2.sys | programa.exe | 281 KB | 374 |
| vakalo1.sys | programa.exe | 273 KB | 331 |

*2) Senha de proteção do programa*

Devido ao fato de os jogos serem carregados na memória somente quando escolhidos na tela de seleção de jogos, a descompressão é realizada automaticamente pela aplicação, sugerindo que a senha ou era armazenada em uma variável local da própria aplicação responsável pela descompressão, ou em algum arquivo que pudesse ser lido quando necessário.

A segunda hipótese mostrou-se verdadeira quando os arquivos de nome "jogos.bin" de cada máquina, que foram reconhecidos como sendo tabelas dBase. Eles revelaram uma tabela com as colunas "nomejogo", "mascara" e "senha", todas do tipo texto, porém com conteúdo codificado. A quantidade de registros da tabela é compatível com os itens apresentados pela sua tela de seleção de jogos e com a quantidade de arquivos com extensão "sys" disponíveis em cada equipamento.

Apesar de as informações armazenadas apresentarem-se ininteligíveis em um primeiro momento, indicando a adoção de alguma espécie de codificação, foi possível constatar que as senhas cadastradas para todos os jogos possui a mesma representação codificada, com comprimento de seis dígitos.

TABELA IV. Exemplo de conteúdo do arquivo "jogos.bin"

| NOMEJOGO | MASCARA | SENHA |
|---|---|---|
| §³´¸Á°±»Ž¸¹ | §³´¸œ™¿ÆÁ | ²§¹«ª¼ |
| §³´¸Á°±»Ž¸ | §³´¸›™¿ÆÁ | ²§¹«ª¼ |
| ¬µ³¬®¸‹¯®À³ | ¬©¨º›™¿ÆÁ | ²§¹«ª¼ |
| ¸»·»Š¾±ÅÇ | ¸«¿Á›˜¾ÅÀ | ²§¹«ª¼ |
| §¸¨»²¶°µ¿¯¾£¢£« | ¨§´¸›š›£›ÁÈÃ | ²§¹«ª¼ |
| «¸¼¼²¸³ | «¸¼¼ª˜¾ÅÀ | ²§¹«ª¼ |

Na tentativa de se encontrar um padrão entre os símbolos exibidos na coluna "mascara" e os nomes dos arquivos com extensão "sys", percebeu-se que o algoritmo de codificação consiste na substituição do caractere original por outro cuja representação numérica seja compatível com o resultado da soma de uma centena com o valor numérico do caractere que se deseja codificar, somado ainda ao valor referente à sua posição na cadeia de caracteres.

$$texto\_cifrado[i] = texto\_claro[i] + 100 + i; \quad (2)$$

Tendo elucidado o algoritmo de codificação, realizou-se a tradução das informações apresentadas pela tabela "jogos", que além de fornecer a senha de descompactação (MARCAR), demonstrou que os valores presentes no campo "mascara" referiam-se aos nomes dos arquivos que contém o jogo compactado, conforme ilustrado pela tabela a seguir.

TABELA VI. Tradução do conteúdo do arquivo "jogos.bin"

| NOMEJOGO | MASCARA | SENHA |
|---|---|---|
| HALLOWEEN II | HALLO2.SYS | MARCAR |
| HALLOWEEN I | HALLO1.SYS | MARCAR |
| GOLDEN CARD | GCARD1.SYS | MARCAR |
| SUPER SEXY | SEXY2.SYS | MARCAR |
| BRASILEIRAO 2007 | CAMP2007.SYS | MARCAR |
| FRUTINHA | FRUTA.SYS | MARCAR |

***D. Estrutura Interna***

Uma vez coletadas as informações disponíveis através da análise *off-line*, referentes ao ambiente operacional das máquinas caça-níquel, procedeu-se com a análise *online* do arquivo "programa.exe", extraído dos arquivos de extensão "sys", cuja assinatura de cabeçalho indica tratar-se de binário compilado em plataforma de 16bits.

Durante a análise binária do aplicativo principal do jogo, foram identificados três níveis de segurança para acesso dissimulado a parâmetros de leitura ou de ajuste de comportamento das máquinas caça-níquel.

### *1) Ambiente de Configuração*

Ao depurar o arquivo "programa.exe" através da ferramenta CodeView, verificou-se que durante a exibição da tela principal do jogo, além de aguardar pelo código das teclas listadas na coluna "Hexa" da Tabela I, é realizada uma comparação do conteúdo do registrador AL com o valor hexadecimal 0x34, que corresponde à tecla "4" do teclado convencional.

Esta *backdoor* leva a uma tela de administração do sistema com opções de leitura estatística de entradas e saídas e configuração de parâmetros do jogo (Figura 4). Esta funcionalidade é exibida somente caso o apostador ainda não tenha iniciado uma sessão com a inserção de créditos.

Dentre as opções apresentadas pela tela de configuração, a primeira delas é a de "leitura parcial", acessível através da tecla "Y" (Tabela I), que exibe as estatísticas da máquina quanto aos valores totais de "entradas", "pagamentos", "apostas" e "prêmios". É possível ainda obter o percentual de prêmios pagos e um balanço que se refere ao lucro da máquina, que corresponde ao resultado da subtração dos "pagamentos" pelo total de "entradas". O percentual de prêmios pagos, por sua vez, é obtido através da proporção do número de prêmios pagos em relação ao número de apostas.

```
        MENU PRINCIPAL - HALLOWEEN VS 2.01 - 09/12/2006 - (FS)


                LINHA 1  >> LEITURA PARCIAL

                LINHA 5  >> LEITURA OFICIAL

                LINHA 9  >> ULTIMOS PAGAMENTOS

                LINHA 15 >> ULTIMAS ENTRADAS

                LINHA 20 >> ULTIMOS 10 JOGOS

                TABELA   >> PARAMETROS

                JOGAR    >> VOLTAR AO JOGO


NUMERO DE SERIE 02-08/12-000
```

Figura 4. Tela de administração do sistema.

### *2) Primeiro nível de segurança*

Ao pressionar a tecla "J", referente à opção denominada "leitura oficial" (Figura 5), tem-se a impressão de que a aplicação não executa qualquer ação. Porém, ao analisar o seu código binário, verificou-se que ela aguarda o envio de um valor através do teclado. Este valor, por sua vez, é confrontado com uma cadeia de caracteres armazenada na seção de dados do arquivo executável, que corresponde à senha correta. Essa prática de armazenamento de senha é conhecida como *hardcoded* [9]. A senha para o primeiro nível de segurança, que é composta por 05 (cinco) dígitos numéricos, é o primeiro valor que antecede a cadeia de caracteres "Leitura Oficial" no arquivo executável do programa controlador.

A divergência entre as telas de "leitura parcial" e "leitura oficial" consiste tão somente na possibilidade de reiniciar os contadores da primeira leitura, sem que os valores totais da máquina sejam perdidos. Com isso, durante a análise de uma determinada máquina, a "leitura parcial" pode não refletir os valores totais arrecadados, sendo necessário confrontá-los com os valores da "leitura oficial".

```
        HALLOWEEN - LEITURA OFICIAL - 02-08/12-000 VS 1.35 (FS)

TOTAL DE ENTRADAS                          512600          5.126,00
TOTAL DE PAGAMENTOS                        445754          4.457,54
TOTAL DE APOSTAS                           761500          7.615,00
TOTAL DE PREMIOS                           701888          7.018,88



% PREMIOS                                                     92.17
TOTAL DE RODADAS                                              14313
TOTAL DE JOGOS GANHOS                                         11522
BALANCO                                     66846           668,46


<JOGAR> VOLTAR
```

Figura 5. Tela de leitura oficial acessível através de senha.

### *3) Segundo nível de segurança*

Ao contrário das demais opções que realizam mera consulta aos valores armazenados na base principal de dados, ao informar o código correspondente ao pressionamento da tecla "T", a aplicação permite a alteração de alguns parâmetros de comportamento do equipamento. Porém, o acesso a essa funcionalidade é controlado por um mecanismo de checagem de senha a ser informada pelo usuário.

```
DIGITE A SENHA CORRETAMENTE...
```

Figura 6. Tela de controle de acesso por senha de segurança.

```
DELAY CTR VELOCIDADE (0->1)        0.10

TERMINAL COM DISPLAY (S/N)   N         PERC ACUMULADO              0,30
TRAVA (S/N)                  S         PGTO. BOTAO (S/N)           S
VS COLOMBIA (S/N)            N
CONFIG IMPRESSORA            0
ACUMULADO(1) INICIAL       200
ACUMULADO(1) ATUAL         511         ACUMULADO(2) ATUAL          260
ACUMULADO MAXIMO          1000
PRECO $ CREDITO (* 100)              1
CREDITOS POR PULSO                 100



                                                    AP   -> + 1
                                                    MX   -> - 1
                                                    (S)AU-> + 100
INTERFACE (0, 1, 2)                  2 TIPO-2       (N)TB-> - 100
ANO      (00-99)                     8              PG   -> + 1000
MES      (01-12)                    12              20L  -> + 10000
SERIE    (0-999)           020812000                15L  -> +,01
< PAGTO > CONFIRMA VALORES                          09L  -> ZERA
OUTRA TECLA: DESCARTA                               05L  -> SAI
```

Figura 7. Tela de configuração de parâmetros.

Observando o comportamento da aplicação principal em relação ao valor de senha informado pelo usuário, verificou-se que este é confrontado com uma cadeia numérica com cinco dígitos de comprimento, armazenada também no próprio arquivo executável, porém diferente da senha utilizada para acessar a tela de leitura oficial. A senha para o segundo nível de segurança pode ser encontrada após a única ocorrência da cadeia de caracteres "**informe a senha corretamente**", depois de extraídas as cadeias de caracteres do arquivo binário.

Uma vez que a senha tenha sido informada corretamente, os parâmetros de configuração são exibidos um a um para que sejam ajustados conforme as instruções exibidas no quadrante inferior direito da tela (Figura 7). Todos os parâmetros são livremente configuráveis, exceto aquele intitulado "Config Impressora".

*4) Terceiro nível de segurança*

Ao selecionar este parâmetro ("Config Impressora"), ao invés de o valor informado ser armazenado no registrador correspondente, é realizada uma comparação com um terceiro valor armazenado no segmento de dados do arquivo, indicando tratar-se novamente de uma senha, diferente das duas senhas anteriores. A senha para o terceiro nível de segurança é o primeiro valor numérico contendo cinco dígitos que sucede a cadeia de caracteres "**Config Impressora**" no arquivo executável.

Nos vinte e três jogos analisados, foram encontradas ao menos duas senhas distintas para cada nível de segurança. Para o primeiro nível, parte dos jogos utilizava a senha "30114", enquanto que o restante utilizava a senha "43210". O segundo nível, por sua vez, apresentou as senhas "30113", "30118" e "01234" e o terceiro nível, as senhas "30116" e "36546" em predominância.

*5) Decodificação da base de dados principal*

Diante do fato de a base de dados principal, representada pelo arquivo "base.dbf" presente no diretório "data", apresentar conteúdo ininteligível, procedeu-se com a modalidade de análise *online* com o intuito de verificar o comportamento da aplicação principal em relação aos valores armazenados.

Durante a análise, constatou a existência de codificação das colunas originalmente definidas como do tipo "string" que armazenam valores numéricos. A codificação é trivial: cada byte que forma o número é registrado na forma da sua representação ASCII. Tendo em mente que a arquitetura x86 é *little endian*, a ordem é do menos significante para o mais significante. Como exemplo, considere o valor originalmente informado como "100", que era gravado como "d" (a representação ASCII do número).

Uma vez analisados os valores armazenados nos respectivos arquivos dos equipamentos sob investigação, foi possível constatar a função das principais colunas da tabela abrigada pelo arquivo "base.dbf". Assim, percebe-se que as colunas que trazem o termo "jack" referem-se sempre à ação de pagamento do "prêmio especial" ao apostador. "Jack" e "jackpar" armazenam os montantes referentes aos prêmios pagos pela máquina, sendo que o segundo é o valor parcial, pois pode ser zerado a qualquer momento pelo administrador do sistema. "Seqjack", por sua vez, guarda a quantidade numérica de prêmios pagos desde a instalação do equipamento.

Com isso, ao examinar o comportamento da aplicação em relação ao valor armazenado em "ctrjack", verificou-se que este obriga que a máquina limite-se a acumular o valor definido em "acummax".

*6) Parâmetros fraudulentos de configuração*

As colunas "perce" e "trava" são aquelas que evidenciam o maior poder lesivo da aplicação principal. A primeira delas, definida na tela de configuração como "Config. Impressora", cujo acesso é realizado através de dupla verificação de senha, refere-se ao percentual de retenção do equipamento, aceitando valores numéricos entre 0 e 4. Quanto menor o valor informado, maior a retenção praticada pela máquina. Em todas as máquinas analisadas, o valor de "perce" estava configurado como "0".

Tal ajuste influencia negativamente na aleatoriedade do resultado, uma vez que a aplicação apresenta um laço de repetição que obriga a realização de novo sorteio caso o nível de retenção do equipamento não tenha sido atingido.

A coluna "trava", também configurada através da tela ilustrada pela Figura 7, quando marcada positivamente, impede a exibição das figuras compatíveis com as sequências de bônus, sem prestar qualquer esclarecimento ao usuário da máquina, levando-o a erro.

Outro indício de fraude foi constatado na tela de bonificação denominada internamente como "maçã". Quando da montagem da interface em tempo de execução, os valores da matriz não são previamente sorteados. Ao contrário disso, o sorteio acontece tão somente quando um dos quadrantes é escolhido pelo apostador. Entretanto, assim como ocorre com o sorteio na tela principal, o resultado é confrontado com o nível de retenção do equipamento antes que este seja exibido ao usuário. Caso seja necessário, outro valor é sorteado sem que o usuário tenha ciência disso.

## IV. Metodologia de Análise Proposta

Assim, com base na adaptação do método utilizado por Vênere [11] na análise de código malicioso para atender ao modelo proposto pelo NIST [12], infere-se a seguinte metodologia de análise de máquinas caça-níquel que pertençam ou não à família Halloween:

- Devido à existência de parâmetros não identificados de configuração do ambiente operacional, que normalmente impedem a execução de uma imagem do dispositivo de armazenamento em um ambiente

controlado, deve-se realizar uma cópia bit a bit do dispositivo de armazenamento, a fim de preservar a integridade do conteúdo armazenado no dispositivo original;

- O equipamento deve ser iniciado com o dispositivo que contém a cópia bit a bit e deve-se realizar uma análise comportamental inicial com base na usabilidade da interface, onde serão identificadas as principais funcionalidades da aplicação;
- De posse da análise comportamental, deve-se realizar um inventário dos itens de hardware do equipamento, identificando os componentes de interação com a aplicação, tais como dispositivos de entrada e saída. Durante a confecção do inventário, as funcionalidades identificadas na etapa anterior são mapeadas aos códigos produzidos pelos dispositivos de interação;

Tendo uma ideia formal inicial do comportamento da aplicação principal, havendo similaridade gráfica ou elemento que indique tratar de jogo pertence à família Halloween, deve-se determinar a relação seguindo os seguintes critérios:

- Localizar os arquivos de jogos com extensão "sys" gravados no diretório "DOS";
- Localizar o arquivo "jogos.bin" e, com base na fórmula apresentada, traduzir as informações da base de dados que contém as senhas de descompressão dos arquivos de jogos;
- Examinar os arquivos de imagens dissimulados e o arquivo binário "programa.exe", que representa o núcleo da aplicação;
- Extrair as cadeias de caracteres do arquivo binário e localizar as senhas dos três níveis de segurança.

Uma vez que atendam os quatro passos descritos acima, três abordagens distintas para identificação de similaridade entre as diferentes versões disponíveis [17] comprovou que os jogos da família Halloween possuem essencialmente o mesmo núcleo operacional, adotando comportamento semelhante apesar das aparentes diferenças que possam existir quanto à temática do jogo ou à exibição de um ou mais prêmios acumulados (*jackpot*).

Porém, caso a máquina não se enquadre como da família Halloween por não apresentar similaridade aparente ou por não atender aos quatro requisitos descritos anteriormente, deve-se:

- Realizar uma análise do ambiente operacional da aplicação, identificando arquivos responsáveis por subsidiar a execução do programa que gerencia os dispositivos de interação. Nesta etapa devem ser catalogados e separados os arquivos referentes à preparação do ambiente de suporte dos arquivos diretamente vinculados à aplicação;
- Dentre os arquivos vinculados à aplicação, devem-se identificar aqueles que correspondem ao jogo propriamente dito e a possíveis bases de dados utilizadas pela aplicação principal ou por aplicativos que deem suporte a ela, pois a existência de bases de dados sugere a utilização de parâmetros de configuração do ambiente e registro estatístico de jogadas;
- Abrir as bases de dados encontradas e caso o conteúdo esteja codificado, tentar a decodificação delas através das fórmulas propostas. Caso as fórmulas não sejam aplicáveis, buscar a decodificação usando padrões recorrentes em nomes de jogos similares ou pela análise *online* do código binário com o auxílio de um *debugger*;
- Uma vez decodificadas as bases de dados, realizar um mapeamento inicial entre os valores armazenados, referentes a parâmetros de configuração do ambiente e registro estatístico de jogadas, e os elementos apresentados pela interface;
- Caso os arquivos referentes a jogos fornecidos pela máquina estejam na sua forma binária, abri-lo através de uma ferramenta *debugger* e realizar a análise on-line retificando ou ratificando o mapeamento inicial realizado entre os valores armazenados na base de dados e os elementos de entrada e saída apresentados pela interface da aplicação principal;
- Caso os jogos tenham sido comprimidos com a utilização de senha, verificar se alguma das bases de dados identificadas possui as senhas armazenadas e realizar a descompactação. Por sua vez, caso os jogos tenham sido submetidos a uma ação de empacotamento, utilizar uma ferramenta de *unpacking* para ter acesso ao código-binário original ao invés do código-binário do desempacotador. Em alguns casos, o arquivo principal pode ter sido submetido primeiramente a uma função de empacotamento e posteriormente a uma função de compressão. Neste caso, deve-se realizar primeiramente a descompressão e em seguida o desempacotamento;
- Durante a análise *online* deve-se procurar por funções de captura de texto e geração de números randômicos em arquiteturas de 32-bits ou superiores, ou interrupções de relógio interno e teclado em arquiteturas de 16-bits, para facilitar a identificação de áreas ocultas de configuração de parâmetros ou das evidências da prática de jogo de azar, respectivamente;
- Ainda durante a análise on-line, quando da identificação de regiões obscuras de acesso a configurações de parâmetros com verificação de senha, buscar pela existência de senhas *hardcoded* gravadas na área de dados do código binário ou simplesmente realizar a alteração do *flag* responsável por decidir o desvio adotado por determinado salto condicional presente no código diante da verificação da senha de acesso;
- Realizar testes de operação, ajustando os parâmetros e observando a mudança de comportamento da aplicação, a fim de produzir um modelo comportamental mais apurado. Esse modelo visa constatar as fraudes provenientes da dissimulação de funcionalidades identificadas na etapa de análise inicial do comportamento e que induzem o apostador a acreditar que o equipamento comportar-se-á de maneira distinta daquela que foi programada.

## V. Considerações Finais

Diante da incerteza que paira sobre o comportamento das máquinas caça-níquel simuladas por programas de computador, em todo o território brasileiro tem havido divergência no entendimento dos magistrados quanto ao seu enquadramento ou não no rol dos jogos de azar. Por simularem certa jogabilidade, tais máquinas despertam a falsa impressão de que a habilidade do apostar pode influenciar na probabilidade de ganho ou perda.

Com o objetivo de pacificar a discussão, o presente trabalho aplicou técnicas de Engenharia Reversa para realizar a análise do comportamento geral da aplicação das máquinas tipo "Halloween" desde o momento em que o apostador aciona o botão que dispara o mecanismo de sorteio, até o momento em que o resultado é exibido na tela.

Durante a análise foram encontrados parâmetros de configuração ocultos ao apostador com até três níveis de segurança por verificação de senha de acesso. Ao relacionar esses parâmetros com o comportamento da aplicação, percebeu-se que alguns deles influenciam diretamente no percentual de retenção (lucro) da máquina e no pagamento de premiação. Foram evidenciadas ainda dissimulações de arquivos e de opções de configuração.

Além de o sorteio seja realizado de forma aleatória, sem qualquer hipótese de o apostador influenciar no resultado depois de disparada a ação correspondente, foram constatados parâmetros de configuração que impedem que uma determinada sequência de premiação seja exibida na tela. Com isso, é evidenciado não só a prática de jogo de azar (aleatoriedade do sorteio) como também a possibilidade de fraude (bloqueio não transparente de opção de premiação).

As contribuições do presente trabalho têm seu foco na caracterização da prática de jogo de azar ou fraudes. São elas:

- Caracterização do comportamento interno dos programas de computador que controlam as máquinas tipo "Halloween", para subsidiar a instrução de laudos periciais confeccionados por Peritos Criminais ao analisar jogos idênticos aos abordados pelo presente trabalho;
- Apresentação de uma metodologia de análise que permite aos Peritos Criminais realizar, por analogia, o exame de programas que controlam máquinas incompatíveis com o tipo "Halloween".

Como trabalho futuro, sugere-se o aprofundamento da pesquisa referente ao comportamento interno da aplicação para instruir o desenvolvimento de uma ferramenta que realize a aferição automática dos percentuais de ganho ou perda do equipamento. De forma completamente automatizada, a aplicação realizará *n* interações com o jogo e verificará os resultados gerados, mantendo um histórico independente da relação aposta x ganho, otimizando a abordagem proposta por Nogueira [4] em seu estudo.

## Referências


[1] Costa, Marcelo A. S. Lemos. Computação Forense. 2.ed. Campinas: Millennium, 2003, p.5-8.

[2] G1. Videobingo. Disponível em: g1.globo.com/brasil/noticia/2011/12/operacao-tio-patinhas-apreende-108-maquinas-caca-niqueis-no-para.html. Acesso em: 31 de janeiro de 2012.

[3] G1. Videobingo. Disponível em: g1.globo.com/parana/noticia/2012/01/policiais-civis-fecham-cassino-que-funcionava-em-mansao-em-curitiba. html. Acesso em: 31 de janeiro de 2011.

[4] Nogueira, José Helano Matos. Máquinas Caça-Níqueis. Perícia Federal, Março de 2002, a.4, n.12, p.18.

[5] Bello, Leo. Aprendendo a Jogar Poker: Princípios, Técnicas e Prática. 2.ed. Rio de Janeiro: Nova Fronteira, 2008.

[6] Silva Júnior, A. Lopes. A contravenção de exploração de jogo de azar. Disponível em: jus.com.br/revista/texto/10110/a-contravencao-de-explo racao-de-jogo-de-azar. Acesso em: 5 de janeiro de 2012.

[7] Eilam, Eldad. Reversing: Secrets of Reverse Engineering. Indianapolis: Wiley, 2005.

[8] Pressman, Roger S., Engenharia de Software. 6.ed. São Paulo: McGraw-Hill, 2006.

[9] ICT. Products/Bill Acceptor. Disponível em: www.ict-america.com/product/bill_ acceptor.asp. Acesso em: 17 de agosto de 2011.

[10] Narvaja, Ricardo. Introducción al cracking con OllyDBG. Disponível em: Ricardo narvaja.info. Acesso em: 5 de setembro de 2011.

[11] Vênere, Guilherme. Engenharia Reversa de Código Malicioso. São Paulo: Escola Superior de Redes/Rede Nacional de Pesquisa, 2009.

[12] Peters, James F. & Pedrycz, Witold. Engenharia de Software: Teoria e Prática. Rio de Janeiro: Campus, 2001. p.561-2.

[13] Schneier, Bruce. & Ferguson, Niels. Practical Cryptography. Indianapolis: Wiley, 2003.

[14] Flake, Halvar. Structural Comparison of Executable Objects. DIMVA. Disponível em: citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.83.6632. Acesso em: 21 de novembro de 2011.

[15] Dullien, Thomas & Rolles, Rolf. Graph-based Comparison of Executable Objects. Disponível em: citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.96.5076. Acesso em: 21 de novembro de 2011

[16] Eagle, Chris. The IDA Pro book: The unofficial guide to the world's most popular disassemble. San Francisco: No Starch Press, 2008.

[17] SILVA, C. Esteves, ZELENOVSKY, Ricardo, SOUSA, G. Batista. Emprego da Engenharia Reversa para caracterização do modus operandi das máquinas caça-níquel quanto à prática de jogo de azar ou outras fraudes. Dissertação de Mestrado, Publicação PPGENE.DM - 103 A/2012, UnB: Brasília, 112p.