POST MORTEM ANALYSIS EM MEMÓRIAS DE TOTEM CAÇA-NÍQUEL

Tagliarini, E. B.[1*], Morais, J.M.[2]
[1] Núcleo de Perícias Criminalísticas de Campinas (IC-SPTC-SP), Campinas, SP
[2] Equipe de Perícias Criminalísticas de Mogi-Guaçu (IC-SPTC-SP), Mogi-Guaçu, SP
* *eduardobecker@hotmail.com*

RESUMO
Utilizando-se técnicas de *post mortem anailysis*, logrou-se encontrar vestígios de prática de jogo de azar em totem para acesso de serviço *web*. Os achados permitiram identificar a aplicação de linguagem Java na execução de *scripts* que permitem ao usuário Administrador habilite rotinas que fazem conexão via VPN com servidor de jogos de azar, baixando o arquivo **.bl**, que habilita o acesso dos jogadores ao jogo de caça níquel armazenado na Nuvem.
Palavras-chave: caça-níquel, nuvem, computação forense

Introdução
Com as propostas de inclusão digital, a empresa WordLink desenvolveu totem para acesso a serviço *web*, o qual era locado para estabelecimento comercial que ofertam serviço de acesso à *web*.
No Estado de SP esse equipamento é habitualmente encontrado em estabelecimento do tipo bar, onde segundo denúncias seriam utilizados como caça-níqueis.
O HDD de um totem apreendido foi encaminhado ao NPC de Campinas, um HDD retirado de totem para acesso a serviço *web*, para perícia, visando buscar vestígios da prática de jogo de azar, pois segundo denúncias tal totem seria utilizado para uso de jogo.

Objetivos
Utilização de *post mortem analysis* na busca vestígios da prática de jogo de azar em totem de acesso à *web* da marca WordLink.

Métodos
Realização de imagem clone do HD peça de exame, a qual foi submetida a análise com *software* Autopsy, que permitiu:

1. Identificar as partições do discos e o sistema operacional instalado;
2. Identificação dos usuários;
3. Analisar a *timeline* do sistema para identificar os arquivos utilizados;
4. Recuperar arquivos, inclusive os apagados e posterior exportação;
5. Análise do conteúdo dos arquivos exportados e virtualização da imagem clone.

Resultados e Discussão
Como resultado identificou-se que:

- O sistema operacional instalado era o Ubuntu 12.04;
- Três contas de usuários: “Kiosk, “Administrador” e “Root”;
- falta de uso dos serviços *web* disponíveis no usuário “Kiosk”;
- presença do arquivo *KiosK-withLibs.jar*, tratava-se de uma compilação de *scripts*, os quais só eram executados pelo usuário “Administrador”;
- existência diretório PT, onde o resultado do arquivo *KiosK-withLibs.jar* eram armazenados e ao final da execução eram apagados.
- Utilização de *Virtual Private Network* (VPN)
- Existência de arquivos de criptografia pública;
- Vestígios de arquivos na área de *swap* de jogo do tipo caça-níquel;
- Quando da virtualização da imagem clone identificou-se, após a obtenção da senha de acesso, obteve-se sucesso ao acesso ao *site* www3.housesk.com e ter acesso a jogo do tipo caça-níquel.

Conclusão
Os exames realizados permitiram encontrar vestígios da prática de jogo de azar no HDD do totem, a partir de *login*, com acesso a jogo de azar via VPN, configurando o delito previsto no art, 50 da Lei Contravenções Penais.

Referências bibliográficas (padrão ABNT)
SILVA, C. E. da. Emprego da engenharia reversa para caracterização do modus operandi das máquinas caça-níqueis quanto à prática de jogo de azar e outras fraudes. 2012.