APLICAÇÃO DE TÉCNICAS DE ANTI-FORENSE COMPUTACIONAL EM ARQUIVOS NTFS

Nataniel Corrêa de Oliveira[1], Paulo João Martins[1]

[1]Curso Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) - Criciúma - SC - Brasil.

nco@terra.com.br, pjm@unesc.net

Abstract. The objective of the study is based on the use of tools and anti-forensics techniques in a device with NTFS file system, seeking the protection of the files to ensure their content security and privacy. The encryption stands out as the best known method to hide files, but steganography can also be used. Forensic expertise tools were used to scan the device, first without anti-forensic techniques, then, as a second step, applying encryption through TrueCrypt and BitLocker tools. Results show that, by using a strong key, the encryption in the storage unit with NTFS files system could not be broken. On the other hand, with the device being unprotected all its contents could be recovered, including files that had been deleted; similarly, even the AES-256 encryption could be broken by using a weak key.

Resumo. O objetivo deste trabalho baseia-se no uso de ferramentas e técnicas de anti-forense computacional em um dispositivo com sistema de arquivos NTFS, buscando a proteção dos arquivos para garantir a segurança e privacidade de seu conteúdo. A criptografia destaca-se como método mais conhecido ou, podem-se esconder arquivos empregando a esteganografia. Ferramentas de perícia forense foram utilizadas para vasculhar o dispositivo, inicialmente sem técnicas anti-forense e em um segundo momento, aplicando criptografia com as ferramentas TrueCrypt e BitLocker. Como resultado, ao fazer uso de uma chave forte, não foi possível quebrar a criptografia na unidade de armazenamento com sistema de arquivos NTFS. Em contrapartida, com o dispositivo desprotegido todo seu conteúdo foi recuperado, inclusive arquivos que haviam sido excluídos. Da mesma forma, mesmo com criptografia AES-256, ao utilizar-se uma chave fraca, conseguiu-se a quebra da mesma.

1. Introdução

Atualmente, uma gama de produtos e serviços encontram-se disponíveis na rede mundial de computadores no intuito de facilitar o dia a dia das pessoas. Porém, a utilização destas facilidades por pessoas mal intencionadas acabou por gerar um antagonismo entre o bom e o mau uso dos recursos, não tardando para que fossem utilizados em práticas ilegais e criminosas.

Ferramentas específicas e poderosas são criadas para investigar máquinas, periféricos e dispositivos em busca de vestígios e provas desta nova modalidade de crime.

2. Metodologia

Criptografia e esteganografia foram as técnicas escolhidas e aplicadas por meio dos softwares TrueCrypt e BitLocker para criptografia e JPHS, esteganografia. Dentre as

técnicas anti-forense, são as que melhor se enquadram no contexto desta pesquisa, a proteção de dados e informações.

2.2 Análise Dos Dados E Resultados

A realização de uma perícia forense computacional segundo a metodologia SOP envolve sete fases. Sendo o objetivo deste trabalho a proteção da confidencialidade das informações em um dispositivo de armazenamento, somente as fases de aquisição e exame/análise foram empregadas.

3. Conclusão

Utilizando as ferramentas da perícia forense não foi possível quebrar a criptografia na unidade de armazenamento com sistema de arquivos NTFS, seja utilizando o TrueCrypt, software livre e gratuito, como o BitLocker, presente no Windows 7.

Demonstra-se assim que o emprego destas ferramentas deveria ser preconizado por qualquer órgão, empresa ou indivíduo que não deseje que informações privadas e sigilosas sejam acessadas e expostas.

Torna-se importante salientar que o ser humano muitas vezes é o elo mais fraco nesta questão segurança. Por ser necessária a criação de uma chave(senha) o mais complexa possível com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais como @, ^, $, e o preconizado pelo próprio TrueCrypt que possua no mínimo 20 e até 64 caracteres(quanto mais longo, melhor), o local de armazenamento desta senha é de primordial importância.

Referências

BARRETO, Luiz Gustavo (2009). Utilização de Técnicas Anti-Forense Para Garantir a Confidencialidade. Curitiba, PUC-PR. Disponível em: < http://www.ppgia.pucpr.br/~jamhour/Download/pub/RSS/MTC/referencias/TCC%20-%20Gustavo%20Luis%20Barreto.pdf > Acesso em: 16 maio 2011.

BOTERO, Armando; CAMERO, Iván; CANO, Jeimy (2009) . Técnicas Anti-Forense Em Informática: Ingeniería Reversa Aplicada a TimeStomp. Bogotá, Colômbia: PUJ. Disponível em: <http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6%283%29.pdf> Acesso em: maio 2011.

BRYANT, Robin. The Challenge Of Digital Crime (2008). Disponível em: < http://media.wiley.com/product_data/excerpt/03/04705160/0470516003.pdf> Acesso em: out. 2011

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira (2011). Desvendando A Computação Forense. São Paulo: Novatec. 200p.

FREITAS, Andrey Rodrigues de (2006). Perícia Forense Aplicada à Informática. Rio de Janeiro: Brasport. 216p.

GALVÃO, Kléber Ricardo M. (2009). Perícia Forense Computacional. In: SEGINFO WORKSHOP DE SEGURANÇA DA INFORMAÇÃO, 4., Rio de Janeiro. Disponível em: < http://www.cefetrn.br/~rk/seginfo2009_2_rk.pdf> Acesso em: out. 2011.