INTRODUÇÃO A ANÁLISE FORENSE COMPUTACIONAL: DETECTANDO ROOTKITS EM AMBIENTE MICROSOFT WINDOWS

SLAVOV, R.[1-2] ricardo.slavov@esamc.br ; MILANI, T.G.[3-4-5] thiagogmilani@gmail.com

[1]Escola Superior de Administração, Marketing e Comunicação – ESAMC, Sorocaba, SP; [2]Docente;
[3]Ex-Discente Centro Universitário Hermínio Ometto – UNIARARAS, Araras, SP.; [4]Mestrando em Ciências da Computação, UNESP, Rio Claro, SP; [5]Responsável pelo departamento de TI da Prefeitura de Santa Gertrudes; [5]Docente da Faculdade Anhanguera de Rio Claro;

RESUMO

A informática vem crescendo significativamente desde o seu nascimento, e com isso não precisou de muito para que estivesse presente em praticamente todas as atividades no qual o ser humano desempenha, incluindo assim o âmbito judiciário, e criminal. Com esse crescimento e domínio da informática diversas aplicações e funcionalidades surgem a todo momento para facilitar e agilizar o dia-a-dia das pessoas, seja com o envio e recebimento de um e-mail, publicação de uma notícia em alguma revista eletrônica, post em redes sociais, efetuar uma compra, rastrear a localização de um objeto, ou até mesmo pagar uma conta por um portal de internet-banking.

A Forense Computacional tem como objetivo, a partir de métodos científicos e sistemáticos, reconstruir as ações executadas nos diversos ativos de tecnologia utilizados em *cyber* crimes. (PEREIRA, E.; FAGUNDES, L. L.; NEUKAMP, P.; et. All. 2008).

Existem quatro principais terminologias da análises e coleta de evidências digitais:

Mídia de prova: engloba todos os objetos, dispositivos e mídias alvos da investigação;

Mídia de destino: imagem pericial fidedigna das mídias de provas armazenadas com proteção contra alteração;

Análise ao vivo: análise pericial realizada diretamente sobre as mídias de provas (geralmente acontece quando não se dispõe de recursos, e/ou tempo para a adequada geração de mídia de destino;

Análise post-mortem (*offline*): metodologia de perícia mais utilizada e recomendada onde a análise é feita sobre a mídia de prova ou sobre uma cópia, permitindo maior flexibilidade nos procedimentos adotados para a análise dos dados.

Um software malicioso e programado para se ocultar no sistema Windows, impossibilitando de ser reconhecido pelo usuário ou de ser detectado por alguma solução de antivírus existente no mercado, esse é o *Rootkit*. Esse *malware* altera processos na memória afim de quando houver a tentativa de ler o executável do *Rootkit*, seja retornado um erro indicando a não existência do programa e não permitindo a varredura pelo antivírus. É comum o seu processo de execução rodar “dentro” de algum processo essencial do sistema, como exemplo o Explorer no Windows, impossibilitando a sua visualização no gerenciador de tarefas. Existem diversos tipos de *Rootkits*, que podem variar do nível da camada mais baixa em *firmware* e *hardware*, como baseado no Modo

Usuário e Modo *Kernel*, além dos *Bootkits* (MBR) e nos *Hypervisor* da Intel VT e AMD-V.

Após saber o que é o *Rootkit* e os tipos existentes, existem diversas ferramentas gratuitas que auxiliam o profissional de TI na detecção e remoção desse software malicioso. Neste trabalho destacamos as ferramentas *Process Explorer* e o *Process Monitor* que estão presentes no conjunto de soluções da Microsoft chamada de *Sysinternals* que é gratuita e disponibilizada pela Microsoft para ajudar no suporte técnico e usuários avançados a extraírem o máximo de suas máquinas. Após identificado o processo “oculto” em um processo interno do Windows, pode ser executado o software GMER que analisa a fundo em busca desses processos ocultos e traz diversas ferramentas para auxiliar na remoção e eliminação dos processos do sistema.

REFERÊNCIAS BIBLIOGRÁFICAS

Davis, Michael A.; Bodmer, Sean; LeMasters, Aaron (2009-09-03). "Chapter 10: Rootkit Detection" (PDF). Hacking Exposed Malware & Rootkits: Malware & rootkits security secrets & solutions (PDF). New York: McGraw Hill Professional. ISBN 978-0-07-159118-8. Retrieved 2010-08-14.

Stevenson, Larry; Altholz, Nancy (2007). Rootkits for Dummies. John Wiley and Sons Ltd. p. 175. ISBN 0-471-91710-9.
Jump up

Skoudis, Ed; Zeltser, Lenny (2004). Malware: Fighting Malicious Code. Prentice Hall PTR. p. 335. ISBN 0-13-101405-6.

"Windows Rootkit Overview" (PDF). Symantec. 2006-03-26. Retrieved 2010-08-17.

Carvey, H. Windows Forensic Analysis Toolkit (Third Edition) ISBN: 978-1-59749-727-5

PEREIRA, E.; FAGUNDES, L. L.; NEUKAMP, P.; Et. All. Forense Computacional: fundamentos, tecnologias, e desafios atuais. VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Unisinos, 2008;

Links Úteis

http://www.gmer.net

https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx