Álvaro Vilobaldo Rios da Silva

Antiforense com uso de rootkits

São Paulo

2013

Álvaro Vilobaldo Rios da Silva

Antiforense com uso de rootkits

Monografia de Conclusão de Curso apresentada à Universidade Presbiteriana Mackenzie de São Paulo como requisito parcial à obtenção do título de Especialista em Computação Forense do Curso Lato Sensu em Computação Forense

Orientador:
Ivete Irene dos Santos

UNIVERSIDADE PRESBITERIANA MACKENZIE

São Paulo

2013

Monografia sob o título Antiforense com uso de rootkits, desenvolvida por Álvaro Vilobaldo Rios da Silva, e aprovada em 20 de março de 2013, São Paulo capital, pela banca constituída por:

Ivete Irene dos Santos
Orientador

Epígrafe

"Se você conhecer o inimigo e a si mesmo, não precisa temer o resultado de uma centena batalhas. Se você se conhecer a si mesmo, mas não o inimigo, para cada vitória você também sofrerá uma derrota. Se você não conhecer nem o inimigo, nem a si mesmo, você sucumbirá em todas as batalhas." (TZU, IV a.C)

Resumo

Esta monografia é um estudo sobre antiforense com utilização de rootkits visando mostrar como funciona um rootkit e como ele pode ser usado na antiforense. Definições de antiforense e rootkits com suas práticas comuns e respectivos históricos junto com algumas técnicas de subversão demonstrarão que o uso combinado de técnicas antiforenses incorporadas a rootkits cria mecanimos de destruíção de provas de forma sistemática e eficiênte.

Abstract

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

A monografia apresenta uma incursão na antiforense focada na utilização de rootkits em ambientes Microsoft principamente Windows, visando mostrar seu funcionamento, as práticas mais comuns e como o rootkit pode ser usado na antiforense.

O rootkit é em geral utilizado por atacantes avançados com fins maliciosos e oferece grande obstáculo para ser detectado, pois seu uso força o perito a ter um conhecimento amplo além de usar técnicas sofisticadas. Entender o seu funcionamento é determinande para uma pericia bem sucedida. Para desenvolver esse tema foi utilizada vasta bibliografia, exemplos práticos e aplicações de rootkits comuns.

Ao longo dos capítulos são desenvolvidos os conhecimentos para o entendimento do tema proposto, onde cada um foi dividido em um assunto específico. No primeiro capítulo será mostrado uma visão ampla do que é a ciência forense e como ela é aplicada na computação. No segundo capítulo são apresentados conceitos de antiforense e os tipos de antiforense. Por fim no terceiro capítulo conduz a uma visão do funcionamento de um rootkit e algumas técnicas para subverter os sistema.

1 *Forense Computacional*

A humanidade sempre teve assuntos divergentes, onde em outrora esses assuntos eram resolvidos com o mais forte ou hapto sobrepujando a vontade doutro, com o advento da civilização se convencionou o uso de um mediador que em teoria deve ser alguem neutro.

Quando trata-se de assuntos de disputa de interesse, espera-se que o mediador busque e chegue o mais próximo possível da verdade antes de tomar uma decisão. Hoje é dado esse poder de mediação ao juiz, contudo em diversos conflitos se faz necessário conhecimentos técnicos especificos. Nesses casos ele é auxiliado por um especialista ou perito no assunto técnico em discussão. Para tal, esse especialista utiliza-se da ciência forense para trazer luz os fatos respaldando a decisão do juiz sobre o assunto.

Segundo Houaiss e Villar (2009) ciência é um "corpo de conhecimentos sistematizados adquiridos via observação, identificação, pesquisa e explicação de determinadas categorias de fonômenos e fatos, e formulados metódica e racionalmente." e forense é "relativo aos tribunais e à justiça". Logo as ciências forenses é a utilização da ciência "à análise de vestígios, no intuito de responder às demandas judiciais" (VELHO; GEISER; ESPINDURA, 2012, p. -3).

De certo a área médica foi a primeira a ser requisitada em tribunais construindo técnicas que levaram ao desenvolvimento ao longo dos anos da medicina legal. No Império Romano médicos eram chamados para lucidar mortes diz França (2008), outro exemplo histórico da importância do parecer técnico pode ser visto no *Código Criminal Carolino* feito em 1532 por Carlos Magno que definia a análise médica em determinados crimes.

Com o avanço da tecnologia e o valor da pespectiva especializada, foi natural que outras áreas também fossem utilizadas no foro. A computação forense, apesar da tecnologia e inovação inatas, conceitualmente ainda se propõe a grosso modo a usar a ciência para mostrar fatos demandados judicialmente, como podemos ver em Machado e Eleutério (2011), "[...] computação forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área da informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais [...], por métodos técnicos-científicos, conferindo-

lhes validade probatória em juízo.”.

2 *Antiforense Computacional*

Harris (2006) define antiforense como método para prevenir ou agir contra a ciência usada a favor das leis civis e criminais que são aplicadas por órgãos como a polícia. Berinato (2007), amplia essa ideia mostrando que é mais que uma técnica usada, é uma abordagem crimosa. Assim todas as tentativas de afetar negativamente a existência, quantidade e / ou qualidade da evidência de uma cena de crime, ou fazer a análise e exame das provas difíceis ou impossíveis de realizar, para Rogers (2005) será considerada antiforense. Dessa forma concluímos resumidamente que a antiforense computacional pode ser definida como qualquer ação praticada para obstruir, dificultar ou destruir evidências ou provas no âmbito computacional.

Dentre as modalidades de antiforense computacional, Blunden (2009a) as categoriza em cinco grandes grupos, sendo eles: destruição de dados, ocultação de dados, corrupção de dados, fabricação de dados e eliminação da fonte de dados.

3 *Rootkits*

Malware é a junção das palavras em inglês *malicious* e *software*, termos em inglês que pode ser traduzido livremente como aplicativo malicioso. Dessa forma podemos considerar como malware os vírus, worms, trojans, botnets kit dentro outros, contudo o inverso não é valido, ou seja, todo vírus é um malware, mas nem todo malware é um vírus.

Os vírus e worms são feitos para se espalha a diferença está em como eles se espalham. O vírus precisa ser ativado ou executado pelo usuário e em geral fica atrelado a algum executavel que pode ser ou não um programa legitimo subvertido (LUDWIG, 1995), ao contrário do worm que não precisam da ação direta do usuário para se espalhar e permanece apenas na memória (MCAFEE, 2013).

Uma *botnet* é uma rede de computadores controlados por cybercriminosos(KASPERSKY, 2013). Basicamente quando um computador é infectado pelo agente da *botnet* o mesmo se torna parte da rede e é controlado pelo dono da botnet.

No universo *UNIX*[1] ou *UNIX-like*[2] a conta de usuário com menor restrição de segurança é referênciada como conta *root* sendo que em alguns sistemas o nome de usuário é literalmente root, mas isso é apenas uma convenção histórica do que uma imposição (BLUNDEN, 2009b). Enquanto *kit* significa conjunto de peças (SANTOS, 2000).

Rootkit pode ser visto como um "kit" composto de pequenos programas úteism por exemplo, binários, scripts, arquivos de configuração que permitem a um atacante manter o acesso "root". Em outras palavras, um rootkit é um conjunto de programas e de código, que permite a presença permanente ou consistente, não detectável em um computador (HOGLUND; BUTLER, 2005).

Essa coleção de ferramentas que permitem aos invasores ocultarem suas atividades em um computador, de modo que eles podem secretamente monitorar e controlar o sistema por um período prolongado, ou seja, existem três serviços que o são inerentes dos rootkits, ocultação,

[1] Um sistema operacional multiusuário amplamente utilizado.
[2] Sistemas Operacionais baseados no Unix, como o GNU/Linux

comando e controle (C2) e vigilância (BLUNDEN, 2009b). Ocultação, o rootkit deve passar despercebido, sem que o usuário e/ou antivírus o detecte; vigilância ou monitoramento basicamente consiste em acompanhar as ações do usuário, o rootkit tem que ser capaz de saber o que o usuário está fazendo; e comando e controle, permite ao dono do rootkit o controle remoto sobre o mesmo, definindo suas ações e direcionando. Desses três serviços o mais importante para o rootkit é a furtividade, pois um rootkit detectável vai durar muito pouco.

Como pode ser visto cada um desses agentes subversivos tem definições e características próprias diferentes e uma em comum todos eles subvertem o sistema de alguma forma, contudo é bom resaltar que nem todo rootkit é um malware, pois existem aplicações legítimas para o mesmo, como de computadores coorporativos e inclusive aplicações investigativas.

Os primeiros rootkits apareceram em de 30 anos atrás no fim dos anos 80 e início dos 90, quando alguns foram percebidos comportamentos anormais em computadores como espaço em disco utilizado sem identificação, conexões de rede não-listadas e uso anormal do CPU (ROSANES, 2011).

Jamie Butler, the creator of the FU rootkit

O uso de rootkits é limitado a usuários avançados sendo que seu desenvolvimento exige conhecimentos profundos tanto de arquitetura de computadores quanto do funcionamento do Sistema Operacional que o mesmo vai corromper.

Rootkits proporcionam uma grande variedades de opções e pode ser utilizado para quase tudo,

vem sendo utilizado historicamente para subverter sistemas dando permissão

O fato de alguns eventos e rootkits terem ficados famosos, como é o caso do stuxnet(), torna esse assunto muito interessante de ser abordado, porque

A grosso modo rootkits sempre tentarão esconder sua presença e seus rastros, logo a anti-forense desde o inicio já é parte ...

não são novidades e sua aplicação já não é

e durante o avanço do trabalho, poderão ser notadas diversas formas de detecção de rootkits além de indícios de seu uso em análises.

Referências Bibliográficas

BERINATO, S. *The Rise of Anti-Forensics*. 2007. Disponível em: <http://www.csoonline.com/article/221208/the-rise-of-anti-forensics>.

BLUNDEN, B. Anti-forensics: The rootkit connection. Black Hat USA 2009, 2009. Disponível em: <http://www.blackhat.com/presentations/bh-usa-09/BLUNDEN/BHUSA09-Blunden-AntiForensics-PAPER.pdf>.

BLUNDEN, B. *The rootkit arsenal*. 1ª. ed. Plano, Texas: Wordware Publishing, 2009. ISBN 978-1-59822-061-2.

FRANçA, G. V. *Medicina Legal*. 8ª. ed. Rio de Janeiro - RJ: Guanabara-kooga, 2008. ISBN 978-85-7302-9635.

HARRIS, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital investigation 3S (2006) s4-s49*, 2006. Disponível em: <http://www.dfrws.org/2006/proceedings/6-Harris.pdf>.

HOGLUND, G.; BUTLER, J. *Rootkits: Subverting the Windows Kernel*. 1ª. ed. [S.l.]: Addison Wesley Professional, 2005. ISBN 0-321-29431-9.

HOUAISS, A.; VILLAR, M. de S. *Dicionário Houaiss da língua portuguesa*. 1ª. ed. Rio de Janeiro - RJ: Objetiva, 2009. ISBN 978-85-7302-9635.

KASPERSKY. *Computer Security FAQ*. 2013. Disponível em: <http://www.kaspersky.com/threats_faq>.

LUDWIG, M. A. *The rootkit arsenal*. 1ª. ed. Show Low, Arizona: American Eagle Publications, Inc., 1995.

MACHADO, M. P.; ELEUTéRIO, P. M. da S. *Desvendando a Computação Forense*. 1ª. ed. [S.l.]: Novatec, 2011. ISBN 978-85-7522-260-7.

MCAFEE. *Glossary*. 2013. Disponível em: <http://home.mcafee.com/virusinfo/glossary>.

ROGERS, D. M. Anti-forensic presentation given to lockheed martin. San Diego, 2005.

ROSANES, P. Rootkits. *GRIS - Grupo de Resposta a Incidentes de Segurança. Universidade Federal do Rio de Janeiro*, 2011. Disponível em: <http://www.gris.dcc.ufrj.br/documentos/artigos/rootkits-survey>.

SANTOS, C. M. *Dicionário Inglês-Português*. 2ª. ed. Santa Terezinha, São Paulo: Rideel, 2000.

TZU, S. *A Arte da Guerra*. Tradução de Candida de Sampaio Bastos. 1ª. ed. [S.l.]: Golden Books, IV a.C. 47 p. ISBN 978-85-7501-272-7.

VELHO, J. A.; GEISER, G. C.; ESPINDURA, A. *Ciências Forenses*. 1ª. ed. Campinas - SP: Millenniumn, 2012. ISBN 978-85-7625-249-8.