EPIDEMIA DIGITAL: O AVANÇO DOS MALWARES E O SEU IMPACTO NA SOCIEDADE EM REDE

Ivandro CLAUDINO DE SÁ
CEFET - PB, R.Osório Queiroga de Assis Nº 130, 83-99315660, e-mail: desapb@yahoo.com.br

RESUMO

Nesta sociedade em rede, onde é cada vez maior o número de computadores conectados à internet, incidentes relacionados à segurança da informação tornam-se cada vez mais freqüentes. Casos de roubos de documentos sigilosos, clonagens de cartões de crédito, ataques a organizações governamentais e outros crimes tecnológicos saem do imaginário popular e dos filmes de ficção e se materializam no mundo real. Os *malwares* (malicious softwares, ou códigos maliciosos) por sua vez, assumem papel de destaque neste contexto. Aproveitam de vulnerabilidades nos sistemas, espalham-se pela rede de forma veloz, modificam-se e automatizam ações antes realizadas por seres humanos, contaminando em poucas horas milhares de computadores em todo o planeta. Essas particularidades, por sua vez, assumem características típicas de uma epidemia. Mas uma epidemia diferente, pois o seu agente transmissor não é um organismo biológico e sim um conjunto de códigos feito pelo ser humano e com um objetivo específico. Sendo assim, este artigo tem como objetivo geral conhecer os fatores que motivam o crescimento dos casos reportados de *malwares*, bem como o impacto ocasionado por eles. Pretende levar ao debate a importância da segurança da informação, além de conhecer e classificar os *malwares* a partir da sua forma de ação. Trata-se de uma compilação bibliográfica, onde houve, num primeiro momento, a coleta de dados e informações relevantes, seguido do seu fichamento, elaboração do texto, correção e apresentação.

Palavras-chave: Segurança da Informação, Malwares, Vírus de Computador.

1. INTRODUÇÃO

Vivemos numa sociedade onde cada vez mais a comunicação trafega em redes de computadores e a informação assume um caráter estratégico. Das simples trocas de mensagens entre pessoas a complexas transações financeiras em nível global, essas redes assumem uma posição *sine qua non* diante da atual conjuntura, derrubando barreiras, rompendo fronteiras e facilitando o comércio e a interação entre os povos.

Essa condição cria um ambiente propício para um novo tipo de crime, o crime cibernético. Este, por sua vez, utiliza de várias técnicas e movimenta uma indústria bilionária. Entre essas técnicas destaca-se um novo tipo de praga: os *malwares*. Pequenos programas de computador que carregam em seu núcleo códigos maliciosos e dotados de características específicas como o poder de infecção, propagação, incubação, entre outras, assemelham-se a microorganismos existentes na natureza e utilizam as redes e os sistemas e arquivos de computadores como meio hospedeiro e meio de propagação.

A velocidade com que a informação e os dados trafegam na rede permite o aumento da incidência dessa praga virtual e garante que, em curto espaço de tempo, um mesmo agente transmissor (*malware*) se propague por todo o planeta, criando assim uma epidemia digital.

É dentro dessa realidade que este artigo pretende se adentrar, tendo como principal motivação suscitar o debater acerca da segurança da informação, além de conhecer as características e classificações do *malwares*, bem como os fatores que determinam o crescimento dos casos reportados e seu impacto na sociedade. Trata-se de uma compilação bibliográfica e a metodologia utilizada partiu da divisão do estudo em quatro etapas: coleta de dados e informações relevantes, onde foi buscado em bibliotecas e na internet o material adequado; fichamento, etapa de esquematização da leitura a partir do material colhido; elaboração do texto, cujo desenvolvimento se deu a partir da técnica de análise de conteúdo; correção e apresentação.

2. MALWARES

O termo *malware*, ou *malicious software*, surgiu com o intuito de referir genericamente aos diversos tipos de programas desenvolvidos para executar alguma ação danosa em um computador ou sistema, podendo-se entender como danoso o ato de comprometer a integridade, privacidade, autenticidade, disponibilidade e confiabilidade de uma informação. Como exemplos de malwares podemos citar os Vírus, *Worm*, Cavalo de Tróia, *Backdoor*, *Spyware*, *Keylogger*, *Bots* e *RootKit*, sendo o *Spam* também considerados por alguns autores um tipo de *malware*.

No entanto, apesar do termo ter sido adotado pela sociedade, atualmente não existe um órgão ou instituição responsável que regulamente e normatize a definição de *malware* bem como seus subtipos e características, o que ocasionalmente causa divergência tanto na classificação como nos métodos de combate e prevenção. Essa indefinição faz com que os *malwares* como um todo também sejam conhecidos simplesmente como "vírus de computador" ou "*worms*", sendo assim tratados como sinônimos apesar das diferenças técnicas e conceituais.

Os ataques por *malwares*, por sua vez, vêm crescendo consideravelmente a cada ano e se consolidando como o principal tipo de ameaça à segurança da informação. Este tipo de ataque, nos últimos anos, destaca-se principalmente por automatizar ações ilícitas até então realizadas manualmente, tornando o ato mais eficiente e complexo de auditar ou efetuar perícias.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), o total de incidentes reportados cresceu de forma considerável de janeiro de 1999 à junho de 2008, sofrendo variações no ano de 2007, saltando de 3.107 casos reportados em 1999 à 197.892 em 2006 e 160.080 casos em 2007. Destes totais, o número de ataques por *worms* (*malwares*) é o que mais se destaca, correspondendo a 56% em 2004, 25% em 2005, 55% em 2006 e 48% em 2007.

Figura 1 – Total de Incidentes Reportados ao CERT.br por Ano. (Fonte: CERT.BR, 2008)

Do total de ameaças destacadas e reportadas, atualmente os vírus (*malwares*) são considerados o principal tipo de incidente de segurança, representando 66% das ameaças às informações das empresas, segundo a Módulo Security (2003). Essas ameaças vêm crescendo consideravelmente a cada ano, seja devido a melhoria das condições de acesso aos computadores, seja devido a expansão da internet e dos meios de comunicação, além dos mecanismos de armazenamento e distribuição de dados. Segundo Telafici, em artigo para a revista SAGE (2008. p.4): "Com computadores com banda larga conectados 24 horas à Internet, a oportunidade de atacar sistemas em tempo real e de utilizar a capacidade ociosa da banda larga de máquinas contaminadas para outros ataques é um recurso tentador demais para ser ignorado" e completa "A expansão e a diversificação do papel dos computadores na sociedade moderna também contribuem para maiores oportunidades para aqueles que buscam capitalizar no cibercrime".

Figura 2 – Principais Ameaças à Segurança da Informação. (Módulo, 2003)

Os vírus também recebem destaque como o principal problema que ocasionou perda financeira, sendo que no Brasil ainda não existe um balanço de prejuízos econômicos ocasionados por ataques de malwares, mas estima-se que em todo o mundo o prejuízo, no ano de 2007, seja na ordem de 13,3 bilhões de dólares. De acordo com a Módulo Security (2006), as organizações governamentais são as que menos quantificam as perdas causadas por problemas de segurança, correspondendo a 56% do percentual, enquanto que o setor financeiro é o que mais sabe quantificar, correspondendo a 24% dos segmentos analisados.

3. CLASSIFICAÇÃO DE MALWARES

A classificação de *malwares* não é normatizada, cabendo as empresas, academia e a sociedade em geral definir padrões próprios para organizar os diversos tipos de códigos viróticos existentes, bem como traçar estratégias adequadas para combatê-los. Devido a esta falta de padronização única e a possibilidade de um mesmo *malware* se comportar de formas distintas, a categorização é prejudicada, dando-se a partir da característica mais evidente. Sendo assim, de acordo com Nogueira (2007), algumas das características comuns aos *malwares* são:

- **Inicialização**: Capacidade que o *malware* tem de se instalar em setores de inicialização do sistema operacional;
- **Infecção**: Competência que o código malicioso possui para inserir um algoritmo em um sistema ou arquivo hospedeiro;
- **Ocultação**: Destreza em esconder-se, camuflando-se ou tornando-se oculto perante o usuário e sistemas de proteção como antivírus;
- **Incubação**: Característica que o *malware* possui de se reservar, crescendo e replicando para atuar em momento específico;
- **Engenharia social**: Necessidade de interação com o usuário para que o código malicioso consiga se infiltrar no sistema;
- **Propagação**: Capacidade de se replicar e expandir sua área de atuação utilizando vulnerabilidades do sistema operacional;
- **Acesso Remoto**: Habilidade de realizar conexões e transmissão de dados remotamente;

3.1. Inicialização

Todo sistema computacional possui uma rotina de inicialização. Esta rotina é iniciada com o acesso ao *Basic Input/Output System* (BIOS) e o *Power On Self Test* (POST) do computador, seguido do acesso à tabela de partição *Master Boot Record* (MBR) que por sua vez carregará e executará o *Booststrap*, ou setor de inicialização da partição. O *Bootstrap* é específico do sistema operacional e normalmente executa o *kernel* (núcleo) do sistema operacional. Este, por sua vez, carregará em memória todos os programas e registros necessários para a execução do mesmo.

Em se tratando da família de Sistemas Operacionais Microsoft Windows, o processo de *boot* possui cinco fases: seqüência de pré-boot, seqüência de *boot*, carga do *kernel*, inicialização do *kernel* e *logon*. Sendo que para cada fase do sistema determinados arquivos são necessários, carregando na memória informações sobre o hardware e seus respectivos *drivers*. Além de gravar informações no registro do sistema e carregar os serviços configurados para a inicialização automática, finalizando com a fase de *logon* (serviço winlogon.exe) que inicializará a Autoridade Local de Segurança (LSA, lsass.exe) para a autenticação do usuário e carregamento do seu perfil.

> Os serviços configurados para inicialização automática são inicializados e carregados na memória do computador. Os serviços são inicializados em uma ordem específica, de acordo com as dependências existentes entre os respectivos serviços. Por exemplo, vários serviços dependem do serviço Remote Procedure Call (RPC). O serviço RPC deve ser inicializado antes dos serviços que dele dependem, caso contrários a inicialização destes últimos irá falhar. (BATISTTI, 2003)

Tabela 1 - Arquivos utilizados no processo de boot do Windows XP (BATISTTI, 2003)

Arquivo	Localização	Fase
Ntldr	Raiz da partição de sistema C:\	Pré-boot e boot
Boot.ini	Raiz da partição de sistema C:\	Boot
Bootsect.dos	Raiz da partição de sistema C:\	Boot
Ntdetect.com	Raiz da partição de sistema C:\	Boot
Ntoskrnl.exe	systemroot\System32	Carga do kernel
Hal.dll	systemroot\System32	Carga do kernel

System	systemroot\System32\Config	Inicialização do kernel
Device drivers (*.sys)	systemroot\System32\Drivers	Inicialização do kernel

Um malware que infectar o setor de inicialização carregará em memória seu código em uma das fases do processo de boot, fazendo assim com que o sistema inicialize o processo virótico automaticamente.

3.2. Infecção

O processo de infecção de um sistema ou arquivo por um código malicioso se dá através da inserção de instruções algorítmicas em arquivos já existentes e carregados na memória de acesso aleatória (RAM). Essa técnica é possível uma vez o *malware*, estando residente na RAM, poderá acessar determinadas posições da tabela de dados utilizadas pelo arquivo carregado. Uma vez feito isso, o *malware* inserirá algoritmos específicos no código binário do arquivo em questão, contaminando-o. Vale destacar que ao fazer isso, o código virótico alterará o tamanho original e a assinatura do arquivo, conseqüentemente o *MACTime* do mesmo.

O *MACTime* é uma maneira abreviada de se referir a três atributos de tempo (*Mtime, Atime e Ctime*) anexados a qualquer arquivo ou diretório em um sistema de arquivos, seja Unix, Windows, ou outro.

> O atributo Atime refere-se à última data/hora em que o arquivo ou diretório foi acessado. O Mtime, ao contrário, muda quando o conteúdo de um arquivo é modificado. O atributo Ctimee monitora quando o conteúdo ou as meta-informações sobre o arquivo mudaram: o proprietário, o grupo, as permissões de arquivo e assim por diante. O atributo Ctime também pode ser utilizado como uma aproximação de quando um arquivo foi excluído. (FARMER; VENEMA, 2006, p.16)

3.3. Ocultação

Essa característica reporta a necessidade que o código malicioso tem de se esconder, seja do usuário final, seja do sistema operacional e dos mecanismos de segurança. A ocultação dificulta o conhecimento e conseqüentemente a remoção do mesmo e para isso utiliza técnicas que possibilitam esconder-se e camuflar-se.

É comum os *malwares* utilizarem de um atributo próprio do sistema de arquivos para ocultar-se. Esse atributo pode ser facilmente acessado através do comando 'attrib' existente tanto na família de Sistemas Operacionais Microsoft Windows quanto na família Unix/Linux. A camuflagem também é um artifício utilizado pelos códigos maliciosos. Este artifício é utilizado a partir do momento em que o *malware* se passa por um arquivo pré-existente do sistema, como o explorer.exe. Casos reportados demonstram que é comum a substituição de um arquivo existente por outro infectado, ou até mesmo a utilização de nomes iguais ou semelhantes, mas em pastas distintas.

3.4. Incubação

Um *malware* pode passar por um período de incubação. Este período varia entre os softwares maliciosos que utilizam esse artifício, podendo ser contado a partir do calendário ou relógio do sistema, ou até mesmo a partir de instruções realizadas pelos usuários. Há casos reportados de *malwares* que só atacam em um determinado dia (ex. Vírus Sexta-feira 13), outros só atacam após uma determinada quantidade de replicações realizadas, ou quando é executado um determinado software.

A incubação também pode ser entendida como um momento de 'maturação' do código malicioso, onde este pode utilizar desta característica para interpretar o comportamento do usuário e assim conseguir burlar mecanismos de defesa que utilizem sistemas de heurística.

3.5. Engenharia Social

A engenharia social é uma característica que visa aproveitar-se da vulnerabilidade do ser humano e não do sistema automatizado. Busca convencer o usuário a realizar determinada tarefa que facilitará a ação do código malicioso.

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como

> resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia. (MITNICK; SIMON, 2003, p.6)

Considerado por muitos especialistas como o elo mais fraco dos sistemas de segurança da informação, o fator humano é exaustivamente explorado pelos desenvolvedores de *malwares*. Mitnick destaca:

> A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo. (MITNICK; SIMON, 2003, p.16)

Como exemplo de engenharia social aplicada, podemos destacar as fraudes de *phishing* recebidas por correio eletrônico. Mensagens destinadas a usuários carregam em si links para páginas obscuras, ou arquivos contendo softwares maliciosos nos mais diversos idiomas e com extrema qualidade técnica. De acordo com Dirro e Kollberg em artigo intitulado Alemanha: o *malware* aprende o idioma, (SAGE, 2008, p.22), com os lucros potenciais causados pelas redes de *bot*, cavalos de tróia que roubam dados, as fraudes de *phishing* recebidas por correio eletrônico estão ficando mais sofisticados a cada dia e destaca: "Antigamente as mensagens eram compostas em um alemão rudimentar que parecia um texto original em inglês ou russo traduzido pelo BabelFish. Provavelmente foi o que aconteceu. Hoje podemos ler textos escritos em um alemão perfeito, referindo-se a eventos atuais e jogando com os desejos das pessoas."

3.6. Propagação

A propagação é a capacidade que o *malware* tem de se replicar, fazendo uma cópia de si mesmo para outras pastas e arquivos e ampliando sua área de atuação. Os principais vetores de ameaça de *malware*, de acordo com o Centro de Orientação de Segurança (MICROSOFT, 2004), são as redes externas, clientes convidados, arquivos executáveis, documentos, e-mails e mídias removíveis (CD-Rom, DVD-Rom, unidades Zip, disquetes, *pendrives* e cartões de memória).

O *malware* Slammer/Saphire é um exemplo do poder de replicação que estes códigos podem assumir. A Cooperative Association for Internet Data Analysis (CAIDA.ORG), no ano de 2003, informou que este *malware* conseguiu infectar 420 hosts/hora, atingindo o tempo de saturação da população infectada em apenas 30 minutos. Seu antecessor, o Code Red, teve uma taxa de infecção de 1.8 host/hora e tempo de saturação da população infectada em 24 horas. Para isso, o Slammer utilizou uma falha no Microsoft SQL Server 2000 e no SQL Data Engine 2000.

3.7. Acesso Remoto

O acesso remoto pressupõe a utilização de um meio de comunicação entre o host infectado e o host atacante, possibilitando que o mesmo controle a vítima através de protocolos de comunicação como o TCP/IP.

3.8. Tabela Comparativa

Tabela 2 - Elementos de Malwares (Fonte: Nogueira, 2007)

Malware	Inicialização	Infecção	Ocultação	Incubação	Eng. Social	Propagação	Remoto
Vírus	X	X	X	X	X		
Worm					X	X	
Trojan					X		
Backdoor	X				X		
Rootkits	X		X		X		X
Loggers	X		X		X		X

Spywares					X		X
Bots	X	X	X			X	X

4. TIPOS DE MALWARES

4.1. Vírus

Inicialmente descrito por Fred B. Cohen, em 1983, na Universidade da Califórnia, os vírus de computador se disseminaram e evoluíram rapidamente em todo o mundo, recebendo essa denominação por sua semelhança, na forma de contágio e atuação, aos vírus biológicos.

Os vírus de computadores são pequenos programas e caracterizam-se por possuírem em seu código-fonte instruções maliciosas que serão incorporadas a outro programa hospedeiro, sendo executado e replicado a outros programas assim que o mesmo for iniciado. Geralmente a forma de contaminação e atuação varia entre os diversos tipos de vírus existentes, mas podemos concluir que geralmente os vírus possuem duas etapas: contaminação e ataque.

> Na fase de contágio, o vírus fica inibido, afim de multiplicar o máximo possível. Por exemplo, no caso de um vírus de arquivo, ao executar um arquivo contaminado o vírus não irá destruir os dados imediatamente. Ficará residente na memória, fazendo uma cópia de si próprio para todos os arquivos executáveis que forem chamados a partir daquele momento, "infectando" arquivos antes "limpos". (TORRES, 2001, p. 1261)

Normalmente costumam infectar arquivos executáveis, mas também podem contaminar bibliotecas de dados e registros comumente acessadas por outros programas. Alguns vírus de computador também inserem códigos em arquivos e registros de inicialização do computador ('vírus de boot'), para assim interceptar as sub-rotinas do sistema operacional residentes na memória de acesso aleatório, alterando os dados ou multiplicando-se. De acordo com Torres (2001), "Como ficam residentes em memória, devem ser extremamente pequenos, de modo que não sejam facilmente percebidos pelo usuário e de modo que sua presença não atrapalhe o funcionamento 'normal' do micro."

4.2. Worm

Os *Worms* são pequenos programas capazes de propagar rapidamente através das redes de computadores. Enviam cópias de si mesmos, abrindo caminho para outros softwares maliciosos ou até mesmo executando instruções nocivas a cada host infectado.

> Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores. (CERT.BR, 2006, P.75)

4.3. Cavalo de Tróia

A história conta que o Cavalo de Tróia foi uma técnica utilizada pelos gregos para invadir a cidade de Tróia, até então considerada impenetrável. Conta a lenda que após anos de batalha, o guerreiro Odisseu teve a idéia de construir um enorme cavalo de madeira com interior oco, que levaria soldados gregos e tinham como missão abrir os portões de Tróia na surdina da noite. O cavalo então foi construído e deixado próximo a fortaleza. Acreditando que este seria um pedido de paz, o "presente grego" foi levado para dentro das muralhas, ocasionando então o sucesso do plano de Odisseu.

> Finalmente, seguindo um estratagema proposto por Odisseu, o famoso cavalo de Tróia, os gregos invadiram a cidade governada por Príamo terminaram a guerra. O cavalo de Tróia revelou-se uma armadilha, um falso pedido de paz grego. Sendo um presente para o rei, os troianos levaram o cavalo para dentro das muralhas da cidade; à noite, quando todos dormiam, os soldados gregos que se escondiam dentro da estrutura ôca de madeira do cavalo saíram e abriram os portões para que todo o exército entrasse e queimasse a cidade. (http://pt.wikipedia.org/wiki/Guerra_de_Tr%C3%B3ia)

Essa história serviu de base para a construção de um dos *malwares* mais disseminados. Também conhecidos como *Trojan Horse*, ou simplesmente *Trojan*, os Cavalos de Tróia são códigos maliciosos que se disfarçam de programas legítimos. Utilizando técnicas de engenharia social, o *trojan* normalmente é enviado à vítima como um presente, que ao ser recebido e executado pode instalar *keyloggers*, *screenloggers*, ou *backdoors*, com o intuito de roubar informações sigilosas.

> Na informática, um cavalo de tróia (*trojan horse*) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário. (CERT.BR, 2006, P.68)

4.4. Backdoor

São softwares que garantem a disponibilidade de um novo serviço de comunicação remota ou substituição de um determinado serviço por uma versão alterada. Garantem o acesso remotamente sem o consentimento do usuário e geralmente são utilizados para garantir "uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado". (CERT.BR, 2006, p.72)

4.5. Spyware

Também conhecido como software espião, normalmente utiliza a conexão com a internet para transmitir informações sem o conhecimento do usuário. Tem como principal objetivo monitorar os hábitos e informações pessoais dos usuários, enviando essas informações para terceiros.

Normalmente os *Spywares* utilizam de outros mecanismos existentes, como os *keyloggers, event loggers, cookies e screenloggers*. São extremamente resistentes a remoções, permanecem ocultos e visam o lucro financeiro. Seus sintomas são: lentidão no PC, pop-ups de propagandas não solicitadas, mensagens de erro aleatórias ao utilizar o navegador, novos ícones, redirecionamento para sites não requisitados, entre outros.

4.6. Keylogger

Keylogger é um software capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Geralmente seu armazenamento é feito em arquivos texto simples e são enviados remotamente para o agente atacante. O objetivo dos *keyloggers* é capturar informações sigilosas, como senhas de banco, números de cartões de crédito, entre outros.

> Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou *Internet Banking*. Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*). (CERT.Br, 2006, p.73)

Criados com o intuito de burlar os teclados virtuais normalmente acessados por mouse, os *screenloggers* são considerados variantes dos *keyloggers*. Sua ação ocorre através da captura das telas do computador e tem como objetivo obter a posição do cursor na tela no momento em que o botão do mouse é clicado.

4.7. Bot

Usado para ataques utilizando computadores zumbis, é um software que permite que um sistema seja controlado remotamente por outro computador denominado *Bot Herder*. Semelhante ao *worm*, é um software capaz de se propagar automaticamente, explorando vulnerabilidades ou falhas de configuração de softwares instalados em um sistema.

BotNet é uma rede de computadores zumbis, onde um único computador (*Bot Herder*) comandará vários outros computadores, através de servidores públicos como *Internet Relay Chat* (IRC) ou *Domain Name Server* (DNS), para realizar uma determinada ação de forma distribuída. Essa técnica é comum em ataques do tipo *Distributed Deny of Service* (DDOS).

> Normalmente, o *bot* se conecta a um servidor de IRC (*Internet Relay Chat*) e entra em um canal (sala) determinado. Então, ele aguarda por instruções do invasor, monitorando as

> mensagens que estão sendo enviadas para este canal. O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*. Estas seqüências de caracteres correspondem a instruções que devem ser executadas pelo *bot*. (CERT.BR, 2006, p.76)

4.8. RootKit

Originalmente criado para referenciar um conjunto de ferramentas administrativas para sistemas baseados em Unix, essas ferramentas foram modificadas para ocultar atividades maliciosas e garantir acesso privilegiado em um sistema que já foi atacado. De acordo com o CERT.BR (2006, p.77), um *rootkit* pode conter:

- programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como arquivos, diretórios, processos, conexões de rede, etc;
- *backdoors*, para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos *rootkits*);
- programas para remoção de evidências em arquivos de *logs*;
- *sniffers*[8], para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- *scanners*[9], para mapear potenciais vulnerabilidades em outros computadores;
- outros tipos de *malware*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

5. CONCLUSÃO

A sociedade vem, cada vez mais, utilizando das redes e dos computadores para mediatizar a comunicação. A informação é então percebida como ativo e vista estrategicamente. Dentro dessa realidade atual, o número de incidentes de segurança da informação reportados cresceu consideravelmente desde o ano de 1999. As possíveis causas para tamanho crescimento são decorrentes da massificação do acesso às redes de computadores, em especial a internet e os serviços de banda larga; da popularização do computador e da diversificação do seu uso; e das possibilidades de capitalização através dos crimes cibernéticos.

Os *malwares* por sua vez são considerados os principais tipos de incidentes de segurança e são cada vez mais utilizados para automatizar ações ilícitas até então realizadas manualmente. Apesar de não existir uma organização que padronize as definições e características dessas pragas, é notória a importância que há em compreender e aprimorar as técnicas de prevenção e combate por parte das empresas, academia e sociedade em geral. Perceber os diferentes tipos de códigos maliciosos, conhecer suas formas de atuação e criar padrões de categorização são condições necessárias para o sucesso da segurança da informação.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023: Informação e documentação - Referências - Elaboração**. Rio de Janeiro: ABNT, 2002.

_____. **NBR 10520: Informação e documentação: Citações em documentos: Apresentação**. Rio de Janeiro: ABNT, 2002.

BATTISTI, J. **Boot no Windows 2000/XP e o arquivo Boot.ini.** JulioBattisti.com.br, abril 2003. Disponível em: <http://www.juliobattisti.com.br/artigos/windows/boot.asp>. Acesso em 3 jul. 2008.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet v. 3.1.** São Paulo: CGI.BR, 2006. Disponível em: <http://cartilha.cert.br/download/>. Acesso em: 10 mar. 2008.

_____. **Estatísticas Sobre Notificações de Incidentes.** CERT.br, 2008. Seção Estatísticas. Disponível em: <http://www.cert.br/stats/>. Acesso em: 4 ago. 2008.

CENTRO DE ORIENTAÇÕES DE SEGURANÇA. **O Guia de Defesa Profunda com Antivírus.** Microsoft, 2004. Disponível em: <http://www.microsoft.com/brasil/security/guidance/recent/avdind_0.mspx>. Acesso em 10 jun. 2008.

COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS. **The Spread of the Sapphire/Slammer Worm.** CAIDA.ORG, 2003. Disponível em: <http://www.caida.org/publications/papers/2003/sapphire/sapphire.html>. Acesso em: 10 mar. 2008

FARMER, D.; VENEMA, W. **Perícia Forense Computacional: Teoria e Prática Aplicada. Como investigar e esclarecer ocorrências no mundo cibernético**. Tradução Edson Furmankiewicz e Carlos SchaFranski. São Paulo: Pearson, 2006.

MITNICK, K.; SIMON, W.L. **A arte de enganar**. Tradução Kátia Aparecida Roque. São Paulo: Pearson, 2003.

MÓDULO SECURITY. **9ª Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro: Módulo, 2003. Disponível em: <http://www.modulo.com.br>. Acesso em: 12 mar. 2008.

_____. **10ª Pesquisa Nacional de Segurança da Informação**. Rio de Janeiro: Módulo, 2006. Disponível em: <http://www.modulo.com.br>. Acesso em: 5 ago. 2008.

NOGUEIRA, M. **Segurança da Informação: Virologia Computacional.** Recife, abr. 2008. 16 slides, formato PPT.

SAGE: VISÃO DE SEGURANÇA DA MCAFEE AVERT LABS. Califórnia, Santa Clara: McAfee, vol.2, nº1, 2008. Disponível em: <http://www.mcafee.com/br/local_content/reports/sage_2008.html>. Acesso em 10 jun. 2008.

SANTOS. D. Vírus geram perdas de mais US$ 13 bilhões, de acordo com estudo. **IDGNow**, São Paulo, jun. 2007. Disponível em: <http://idgnow.uol.com.br/seguranca/2007/06/13/idgnoticia.2007-06-13.3829996661/>. Acesso em: 10 jun. 2008

TORRES. G. **Hardware: Curso Completo.** 4ª ed. Rio de Janeiro: Axcel Books, 2001.

WIKIMEDIA FOUNDATION. Guerra de Tróia. **Wikipedia**, ago. 2008. Disponível em: <http://pt.wikipedia.org/wiki/Guerra_de_Tr%C3%B3ia>. Acesso em 5 ago. 2008.