UNIBRATEC

POS-GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

ALESSANDRO FERREIRA LIMA TENÓRIO

alessandroflt@gmail.com

ESTUDO DAS CLASSIFICAÇÕES DOS MALWARES

RECIFE

2008

ALESSANDRO FERREIRA LIMA TENÓRIO

ESTUDO DAS CLASSIFICAÇÕES DOS MALWARES

Monografia apresentada para a Unibratec como requisito para a obtenção de título na Pós-Gradução de Segurança da Informação.

ORIENTADOR: Prof.M.S.c Márcio Luiz Machado Nogueira

RECIFE

2008

DEDICATÓRIA

Aos meus pais, Jademilson Lima Tenório e Elcimar Ferreira Tenório.

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo dom da vida e os talentos que me são concedidos na minha formação acadêmica;

Aos meus familiares, em especial aos meus pais, por sempre me apoiar em minhas decisões;

Ao meu orientador, Prof.M.S.c Márcio Luiz Machado Nogueira, pela orientação e preciosas sugestões;

Enfim, a todos que contribuíram direta ou indiretamente para a realização desse projeto.

RESUMO

Tem sido cada vez mais comum a quantidade de incidentes relacionados a segurança dos sistemas de informação, sendo cada vez mais crescente a quantidade de *malwares*, nem sempre tendo surgido por mentes maliciosas, mas por simples precaução aos sistemas existente é que os malwares tornou-se sinônimo de dificuldade e causador de problemas nos computadores existente. Todos são programas indesejáveis, não convidados, potencialmente perigosos, porém, importantes diferenças existem entre todos eles com relação à manifestação. Um *malware* pode infectar arquivos e setores de inicialização de disquetes, discos de armazenamento de dados em microcomputadores pessoais e em servidores de dados.

O processo de infecção inclui sobregravação, preposição e anexação em arquivos. Um *malware* de sobregravação normalmente se instala no início do programa, diretamente sobre o código do programa original, de modo que o programa fica quebrado ou dividido, quando se tenta executá-lo nenhuma ação se realiza com exceção de que o *malware* contamina outro arquivo, deste modo a infecção se torna completa, é facilmente detectado e removido.

Um *malware* de preposição pode simplesmente colocar todo seu código sobre o programa original e quando se opera um programa infectado, primeiro o código do *malware* opera e na seqüência o programa original é executado.

Os *malwares* se tornaram cada vez mais sofisticados de modo que foi necessário fazer uma classificação entre os surgidos. Importante, é salientar que a cronologia de sua aparição é muito relevante, pois conseguimos observar sua evolução.

Palavras-chave: *Malwares*, Classificação, Evolução.

ABSTRACT

The amount of related incidents has been each more common time the security of the information systems. Being each more increasing time the amount of *malware*s, nor always having appeared for malicious minds, but for simple precaution to the existing systems.

Malware became synonymous of difficulty and causer of problems in the existing computers. All are programs undesirable, not guests, potentially dangerous, however important differences exist between all they with regard to the manifestation. One *malware* can infect archives and sectors of initiation of floppies, records of storage of data in personal microcomputers and servers of data.

The infection process includes sobregravação, preposition and annexation in archives. One *malware* of sobregravação normally if installs at the beginning of the program, directly on the code of the original program, in way that the program is broken or divided, partitiond and when if to try it executes it, no action if it carries through, with exception of that *malware* contaminates another archive, plus one another one e, in this way, the infection if it becomes complete, easily it is detected and removed.

One *malware* of preposition can simply places all its code on original program e, when is infect program is operated, first the code of *malware* operates e, in the sequence, the original program is executed.

*Malware*s if had become each time more sophisticated and was necessary to make a classification between the appeared ones. Important to point out that the chronology of its appearance is very excellent, therefore we obtain to observe its evolution.

Key Words: *Malwares*, Classification, Evolution

LISTA DE TABELA

SUMÁRIO

1 INTRODUÇÃO

Com o crescimento da Internet e os padrões da mesma sendo aberto e de domínio público, nos últimos anos, pessoas ou organizações mal intencionada podem interceptar dados que trafegam pela rede.

Com o desenvolvimento da tecnologia surgiram os computadores e com eles os vírus da informática. Esses são programas de software malicioso que tem a finalidade de registrar, corromper, eliminar dados ou propagar-se para outros computadores. Os mesmos são transmitidos através da *internet*, *pen-drives*, disquetes.

Ainda há muita confusão entre os usuários, as palavras vírus e *malwares.* Consideramos *malwares* de uma forma mais abrangente, incluindo os vários tipos de vírus, cavalos de tróia, *spywares, rootkits, keyloggers, worms* dentre outros. Os *malwares* variam entre um efeito ligeiramente inconveniente a um elevado grau de dano e assumem constantemente formas novas e diferentes.

O conteúdo deste trabalho irá definir *malwares* suas características, sua forma de atuação como se propagam e sua história.

Segundo Gaudin (2008), a empresa de segurança Sophos encontra uma nova página infectada na internet a cada cinco segundos:

> “Para se ter uma idéia, durante 2007, a varredura da Sophos encontrava uma página infectada na web a cada 14 segundos. O relatório avalia que a internet continua a ser o meio preferido pelos criadores de *malwares* para disseminar seus ataques, devido à crescente dependência que as pessoas estão tendo da rede para encontrar informações. O aumento na taxa de páginas infectadas está relacionado ao declínio observado em e-mails atingidos. Segundo a Sophos, cerca de um em cada 2,5 mil e-mails contém *malware*, comparado ao índice de um em cada 909 verificado em 2007”.

Com esse estudo queremos demonstrar a evolução e classificação dos *malwares* no final dos anos 60, quando se deu o início das descobertas dos

malwares até os dias atuais, contudo com a evolução e propagação dos mesmo não temos como dar uma data limite, tendo encontrado *malwares* novos até os dias atuais.

Os *malware*s são *softwares* que inspiram fascínio, atenção e estimula a curiosidade de profissionais e estudantes de informática.

Alguns motivos podem ser citados:

- Por diversão e entretenimento.
- Para se estudar as possibilidades relativas à vida artificial, tendo em vista a idéia de que "*Os vírus de computador são as primeiras formas de vida feitas pelo homem*". (Stephen Hawking).
- Para se descobrir se, como Hackers, têm a capacidade e competência técnica necessária para a concretização da criação de um vírus, para execução de testes de conhecimento.
- Por motivo de frustração, vingança ou conseguir fama.
- Curiosidade, uma das formas de conhecer sobre vírus é "criando um novo".
- Para punir usuários que copiam programas indevidamente e não pagam pelos direitos autorais.
- Finalidades militares com o objetivo de atrapalhar as informações do inimigo.

Esse trabalho será desenvolvido com a seguinte estrutura:

- no capítulo 2 explicamos os *malwares* e seu histórico no decorrer dos anos com suas descobertas e evoluções, detalhamos os *backdoor*, cavalo de tróia, spywares, *rootkits*, *logger*, *worm* e vírus dando um detalhamento maior neste por ser mais difundido e existir vários tipos.
- No capítulo 3 falaremos das características dos malwares citados, como eles agem, o que é executado, o que eles criam, onde se escondem, dentre várias coisas que o mesmo provoca.
- No capitulo 4 falaremos de taxonomia, como os *malwares* podem ser agrupados e damos uma proposta de taxonomia, pois não existe uma única classificação para os *malwares*.
- No capítulo 5 temos a conclusão.
- No capítulo 6 informaremos as referências bibliográficas.

1.1 OBJETIVO

1.1.1 Objetivo Geral

Construção de uma taxonomia para os *malwares*.

1.1.2 Objetivo Específico

- Histórico
- Evolução dos *Malwares*
- Caracterização dos *Malwares*

2. *MALWARES*

Segundo Zeltser (2005) *malwares* ou códigos maliciosos são programas de computador, que através de um invasor tem o objetivo de atacar um sistema ou rede, os *malwares* têm como objetivo causar algum prejuízo altera o funcionamento de um computador sem a permissão e/ou conhecimento de seu usuário.

Gaspar (2007) define *malwares* como programas maliciosos e são especificamente programados para executar ações danosas em um computador. Os tipos mais conhecidos *malwares* são: cavalos de tróia (*trojan horses*), vírus, vermes (*worms*), bombas lógicas (*logic bombs*) e bactérias ou *rabbits*.

Vírus, *worms* e *trojans* são tipos de códigos maléficos da categoria *malware* (*malicious software*) desenvolvidos para executar ações que causam danos em um computador. [SYMANTEC 1995]. Uma vez instalados no computador da vítima, podem permitir que o criador da praga obtenha o controle completo da máquina infectada.

De forma intencional ou não, as falhas de programação que causam danos ou roubo também podem ser consideradas *malwares*, que está em diversos meios utilizados atualmente entre eles, e-mail, *websites* e arquivos infectados com vírus obtidos por *download*.

Portanto, qualquer *software* que tem como finalidade infiltrar ou gerar um dano em um computador individual, servidor ou rede, pode ser considerado um *malware*. Neste termo geral estão englobados, por exemplo, vírus, *spyware*, *trojan horses*, *worms* e *adware*.

Como existem vários tipos de *malwares*, e eles se desenvolvem rapidamente um estudo completo não tem sido fácil, a bibliografia ainda é muito escassa, contudo tentamos estudar e classificá-los através de suas técnicas, criando categorias de *malwares*.

2.1 HISTÓRICOS DOS *MALWARES*

Códigos maliciosos não são recentes. É do final dos anos 60 e início dos anos 70, período em que o computador tipo *mainframes* dominava as grandes corporações e centros de pesquisa. São deste mesmo período os programas denominados "*rabbits*". Os "*rabbits*" faziam cópia de si mesmo nas máquinas que eram executados, utilizando-se dos recursos e deixando lento o desempenho do sistema.

Ainda segundo Zeltser (2003), entre 1981-1982 já havia relato do vírus "*Elc cloner*" criado por Rich Skrenta, estudante americano de apenas 15 anos que se divertia com brincadeiras que eram passadas para amigos. O mesmo alterava cópias piratas de jogo para que elas se destruíssem depois de algumas vezes que eram jogadas, mostrando algum tipo de verso, um vírus inocente que não prejudicava a ninguém, elaborado para os micro da Apple II, de 8 bits, o *Elc cloner* após 50 boots mostrava uma mensagem em forma de poema que falava de sua capacidade de proliferar:

> "*Elc cloner: the program with a personality*
> *It will get on all your disks*
> *It will infiltrate your chips*
> *Yes it's Cloner!*
>
> *It will stick to you like glue*
> *It will modify tam too*
> *Send it the cloner!*"

Em 1983 no dia 10 de novembro, o estudante Fred Cohen da Universidade do Sul da Califórnia em sua pesquisa para doutorado criou o primeiro vírus documentado da história da informática.

Cohen foi o primeiro a demonstrar como é que um vírus poderia prejudicar o funcionamento de softwares.

Em 1986 foi criado o primeiro vírus para sistema MS-DOS, batizado de Brian Vírus. Segundo Theriault (1999) acredita-se ter sido escrito por dois irmãos do Paquistão, eles seriam vendedores de *software*, e o desenvolveram para evitar cópias não autorizadas dos programas que eles desenvolviam. Ele

infectava apenas disquetes e ocupava todo o espaço disponível no disco rígido, ou seja, quando o disquete infectado fosse inserido em um computador ele apresentava como rótulo o texto "© *Brian*", mas não era possível ser detectado pelo usuário. Esse também foi o primeiro vírus a ter capacidade de ficar oculto.

Segundo o prof. Vargas (2000) em 1987, os vírus começaram a causar danos reais para administradores de sistema, começando com *Lehigh* um vírus criado por Ken Van Wyk. O *Lehigh* contaminava apenas arquivos command.com e residia na memória, seu campo de disseminação era limitado, pois o mesmo se autodestruía após quatro replicações sobrecarregando as áreas de *boot*. Ainda segundo Vagas (2000) esse ano surgiu os primeiros vírus em Tel Aviv*,* o *Suriv* (palavra vírus escrita ao contrário) um vírus residente na memória, com capacidade de infectar qualquer arquivo com extensão.com, e que em seguida veio o *Suriv-02*, vírus que só infectava arquivos com extensão.exe.

Ainda esse ano segundo Miguet & Tim Read (2008) surge o *Jerusalém* (*viernes 13*), vírus que residi na memória, infectando arquivos e quando ativado apagavas os arquivos infectado. Vagas (2000), relatar que o *Jerusalém* (sextas-feiras 13) foi baseado nas versões anteriores do *Lehigh, Suriv* e *Suriv2*, porém evitava infectar o arquivos command.com por causa da publicidade que ocorreu em torno do *Lehigh*, o vírus residia na memória infectando arquivos do tipo.exe, .bin, .com, pif, .ovl e apagava os arquivos quando ativado.

Em 1988 surgiu o *Morris*, primeiro *"Internet Worm"*, segundo Schmidt (2001), esse foi o incidente mais marcante da década, aconteceu em novembro de 1988 infectou mais de 6.000 computadores nos Estados Unidos, paralisou redes e causou prejuízos estimados em 96 milhões de dólares. Como conseqüência destes ataques foi necessária a criação nos Estados Unidos do Centro de Resposta Rápida a Incidentes - CERT (*Computer Emergency Response Team*). A partir daí os vírus passaram a ser um assunto bastante discutido pela comunidade da informática.

Segundo Zeltser (2000), o *worm Morris* explorava algumas vulnerabilidades comuns para se espalhar através da rede a uma velocidade fenomenal. O objetivo básico do *Morris* era ganhar acesso a outra máquina para que pudesse duplicar-se na nova máquina e continuar a reproduzir-se. O *worm* quando se instalava em novo anfitrião comprometido se utilizava de

buffer overflow, uma técnica que lhe permitia executar um pequeno programa arbitrário que possibilitava o seu processo de cópia. O *worm* explorava vulnerabilidade viáveis de programas como o rexec ou rsh (usado para facilitar a administração em múltiplas máquinas), isso possibilitava examinar listas locais de nomes de anfitriões dos quais o anfitrião infectado tinha conhecimento. Depois de ganhar acesso, o *worm* conseguia ligar-se à máquina remota fazendo-se passar por um utilizador legítimo.

Ainda em 1988 aparece esta família dos vírus, Chernobyl, escrita no Sudeste Asiático, apareceu primeiramente em junho. Atualmente há pelo menos 35 variantes disponíveis. Este vírus conte um payload data ativado. Este vírus Chernobyl, que é uma referência direta ao acidente na planta nuclear do mesmo nome que ocorreu em 26 de abril de 1986.

Em 1989, apareceram alguns novos vírus e a IBM deu a seus clientes cópias de seu próprio *software* do antivírus, em virtude dos vírus surgidos no ano anterior, a IBM criou seu antivírus interno para checagem de arquivos e programas, intensivando os estudos sobre os antivírus por ter ocorrido uma situação desagradável com vírus, pois até então se tinha duvidas a respeito dos vírus. Segundo o Kaspersky Lab (2008), no final do ano de 1989 um famoso *trojan*, o disquete *AIDS*, foi distribuído e causou imenso dano enviado 20000 discos a endereços em Europa, África, Austrália e WHO. Os endereços tinham sido roubados da base de dados do *PC Business World*.

Ainda a Kaspersky Lab em 1990 aparece o primeiro vírus *polymorphic*, vírus que mudam sua forma, encriptando parte do seu código, para evitar detecções pelo software de antivírus. No final de 1991 grandes companhias estavam no mercado do antivírus. Os vírus estavam espalhados no mundo inteiro, e os vírus polymorphic difundidos.

A Norton, empresa de antivírus, criou z\um antivírus em 1990 e como retaliação foi criado o vírus Tequila, é um vírus que infecta o registro mestre de inicialização (mbr) do primeiro disco rígido e ficheiros .exe. Ela usa uma criptografia avançada variável rotina para evitar a detecção e remoção.

Em 1991 segundo Dr Herman (1998) foi criado por um grupo alemão chamado VDV (*Verband Deutscher Virenliebhaber*) o VCS um kit de criação de vírus. VCS é um programa primitivo que requeria um arquivo texto de no máximo 512 bytes. Ele incorpora o arquivo texto com a parte funcional do vírus

e gera um arquivo.com. Após um numero específico de replicações, o vírus mostrava a mensagem que foi especificada e apagava o autoexec.bat e config.sys, era um software de fácil entendimento que até pessoas com pouco conhecimento conseguia construir arquivos maliciosos.

Em 1992 um vírus denominado de *Michelangelo* afetava o principal setor do HD e tinha data marcada para fazer isso, dia 6 de março, a data de aniversário do *Michelangelo* de onde denominou o nome, mas como a notícia se alastrou como uma febre foi tomada iniciativas de contenção, mesmo assim na data marcada mais de 8.000 computadores foram infectados pelo vírus.

Segundo Ghonaimy, M. Adeeb; El-Hadidi, Mahmoud T, Aslan, Heba K (2002) em 1993, apareceu mais, o vírus do *Tremor*, residente na memória, e que utiliza técnicas de invisibilidade e polimorfismo para evitar ser detectado por antivírus. Além disso, utilizava técnicas específicas para se esconder de alguns programas antivírus. O vírus *Tremor* infecta a cópia do *comamand.com* que é apontada pela variável, do *DOS*, *comspec*. Uma vez instalado na memória, *Tremo*r contamina todo arquivo.exe que seja executado. Um sistema infectado se tornava lento na execução de comandos ou programas. Dois outros efeitos que o *Tremor* demonstra, apareciam após 03 (três) meses de infecção, quando se dava um *boot* (*WARM BOOT = CTRL+ALT+DEL*). Nesses momentos o vírus mostrava uma mensagem na tela e apareciam tremores na tela e sons aleatórios aconteciam. Após o aparecimento da mensagem ou o sistema travava, ou então é liberado após alguns segundos, tornou-se famoso após infectar a TV alemã com um *pkunzip.exe.*

Em 1994, surgem os primeiros *Hoax*, é o nome dado à mensagem que tem um conteúdo “alarmante”, como por exemplo, o alarme de ataque de um vírus perigoso que tenha sido detectado. Normalmente estas mensagens informam que não se deve abrir um determinado arquivo de correio eletrônico que possua alguma determinação de assunto como “*Good Times*”, “*Join The Crew*”, “*Penpal Greetings*” e “*Win a Holiday*” ou caso não obedeça, seu microcomputador será contaminado por vírus, ou o disco rígido será formatado e etc. Em resumo, é um Spam uma mensagem não solicitada, como uma propaganda publicitária normal, enquanto que o Hoax também é uma mensagem que conta estórias falsas como a infecção por vírus, podendo ser considerado um falso vírus.

O vírus de macro que são códigos escritos para que, sob certas condições se "reproduza", fazendo uma cópia dele mesmo. Como outros vírus, eles podem ser escritos para causar danos, apresentar uma mensagem ou fazer qualquer coisa que um programa possa fazer. Surgiu em 1995 e infectava documentos de *software* populares de edição de testo e planilhas eletrônicas.

Segundo Harrigton (2005) em 1998 aparece o primeiro vírus de java, o *JavaApp.StrangeBrew*, é um vírus parasita, se agarra a um programa hospedeiro sem atrapalhar seu funcionamento, especificamente os arquivos .class. Funciona sem preconceito contra qualquer sistema operacional, tanto faz ser Unix, Win95, dentre outros. Ainda nesse mesmo ano surge *Backorifice* primeiro *trojan*, uma vez instalado permite acesso externo à máquina, permitindo quase tudo, até mesmo ejetar *CDs* ou resetar o micro remotamente. O *Backorifice* opera de uma forma muito semelhante aos programas de administração remota, com possibilidade de alterar a porta TCP escutada pelo programa, ou mesmo estabelecer uma senha de acesso, tanto que algumas pessoas chegam a utilizá-lo para tal. O problema é que o BO não dá nenhum aviso ou advertência ao usuário e é difícil de detectar uma vez ativo.

> “No final da década de 90, conseguiram construir um vírus denominado *Melissa* que era a união de *worm* e macro, com capacidade de infectar arquivos do Word e utilizar e-mails para se distribuir automaticamente para os contatos do *Outlook* e *Outlook Express*. Sendo assim, infectou milhares de sistemas de computadores. Outro *worm* criado em 1999, que também utilizava mensagens de e-mail para se difundir, foi o *Bubbleboy*. Este programa maléfico não exigia o envio de arquivos anexados às mensagens para contaminar as máquinas. Em vez disso, aproveitava-se de falhas no navegador Internet Explorer e tinha capacidade de infectar apenas com a visualização de uma mensagem de e-mail. Este conceito foi aproveitado pelo *worm Kak* e por vários outros que surgiram depois.” Harrington (2005).

Temos ainda em 1998, segundo Gaspar (2007), o Netbus é instalado como se fossem programas supostamente úteis, entretanto abrem portas para permitir que o invasor controle remotamente as máquinas contaminadas.

Em 2000, surge o *worm* mais rápido, foi um dos primeiros ataques distribuído de negação de serviço, que é uma tentativa em tornar os recursos de um sistema indisponíveis para seus usuários. O *Worm Love Letter* conhecido aqui no Brasil como *I Love You* conseguiu derrubar vários serviços de email, por sua velocidade de replicação. Segundo Machado (2002), as redes de computadores em todo o mundo foram invadidas pelo *VBS/Loveletter*, o vírus que detém até hoje o título de invasor de propagação mais rápida. Em questão de horas, o *I Love You*, como o vírus ficou conhecido, infectou mais de 3 milhões de máquinas. A extensão VBS do anexo fica oculta em boa parte das máquinas *Windows*. Assim, o arquivo parece apenas um inocente.txt. Além disso, o programa também tinha a capacidade de se propagar através de canais de bate-papo. Em pouco tempo, pipocaram mais de 03 (três) dezenas de variantes do vírus. Elas diferiam da versão original apenas no texto das mensagens ou no nome do arquivo anexo. Tudo isso, mais a capacidade de utilizar o mecanismo de envio através de clientes de e-mail, permitiram ao *Loveletter* atingir uma velocidade jamais vista. Embora não tivesse carga destrutiva, o *Loveletter* causou profundos estragos ao produzir uma inédita enxurrada de e-mails que congestionou servidores ao redor do mundo.

Também neste mesmo ano surge vírus para *Palmtops*, para sistemas de telefonia integrados à Internet, para sistema de arquivos do *Windows NT* e para a linguagem de programação php.

Segundo Harrigton (2005), em 2001 foi o ano da criação de *worm* para os mais derivados *softwares*, desde sistemas operacionais como *Windows* e *Linux* até *softwares* de aplicativos como *adobe* e arquivos de imagem JPEG também foram vítimas dos *worms*. Eles se distribuíam por arquivos de troca e pelo programa de bate papo *mirc*. Os vírus tomaram uma força inovadora entre eles estão os primeiros a infectar a tecnologia. Net, a linguagem C# e o SQL Server (todos os produtos da *Microsoft*), arquivos Flash, a rede de troca de arquivos do programa *Kazaa*, servidores *Apache* rodando sobre o sistema *Freebsd*.

Segundo Machado (2003), Em 2003 o *Sobig* é um invasor que envia mensagens em massa, travando os sistemas de e-mail, planta um programa-espião nos sistemas invadidos. Chega como anexo de uma mensagem com assunto, texto e arquivo anexo de nomes variáveis. Quando executado, ele se instala no computador e varre o disco rígido à procura de endereços de e-mail e usa um mecanismo próprio de *SMTP* para enviar mensagens contaminadas. É importante notar que o *Sobig* falsifica o endereço do remetente da mensagem. O nome que segue com o e-mail contaminado não corresponde à máquina de onde partiu a mensagem. O vírus escolhe, ao acaso, um endereço qualquer entre aqueles que coleta no sistema invadido. Aliava seu próprio servidor de envio de mensagens a um sistema que permitia seu uso remoto por *spammers*.

Segundo a *Microsoft* (2003), outro *worm*, *Blaster* tem como alvo computadores com *softwares* antigos se espalhou pela *Internet* no ano de 2003. Sua programação direcionava um ataque de negação de serviço distribuído (*DDoS*) ao site de atualização do *microsoft windows*. Os computadores infectados apresentavam falha de segurança por finalizar o processo de RPC (Chamada de Procedimento Remoto) do Windows, ainda esse ano surgi *worm Slammer.* É um *worm* da *Internet* que tem como objetivo atingir sistemas *SQL Server 2000* e *MSDE 2000* que não tenham sido atualizados com o *patch* de segurança. O *worm* provoca intenso volume de tráfego na rede, tanto na Internet como em redes privadas internas.

No ano de 2004, segundo Harrigton (2005) houve um grande aumento de ataques de *phishing*, geralmente associados a cavalos-de-tróia. Foi também neste mesmo ano que surgiu o *Sasser*, que afetava outra vulnerabilidade do *Windows* e se disseminava via servidores de arquivos (FTP). Vulnerabilidades no sistema *Mac OS X* que permitiam ataques de vírus também foram detectadas e corrigidas.

Foi lançado ainda em 2004 o vírus *Rugrat*, segundo a Symantec (2007) é um vírus de infecção de ação direta que sai da memória após a execução, em arquivos executáveis portáteis do *IA64 Windows* (PE, *Portable Executable*). Estes arquivos PE incluem a maioria dos programas Windows de 64-bit exceto as.dll. Infectar arquivos que estão na pasta onde está alojado e em suas subpastas. Este é o primeiro vírus conhecido para o *Windows 64-bit* e usa as

estruturas *Thread Local Storage* (Armazenamento de Segmento Local) para executar o código viral. Este é um método incomum de executar um código.

Para a Microsoft (2005) o *Cabir* em 2004, foi primeiro *worm* a infectar telefones celulares. Afeta terminais que utilizem o sistema operativo *Symbian*. Propaga-se através de um ficheiro - *Caribe.sis* - o qual se instala de forma automática quando o utilizador aceita a sua transmissão e propaga-se a outros dispositivos através de *Bluetooth* afetando seriamente a autonomia (bateria) do aparelho. Outra novidade foi o *Scob*, surgido em junho do mesmo ano, atacava servidores *Web* baseados em *Windows* e, depois, por meio de um código j*ava script* inserido em todas as páginas do servidor afetado, instalava um cavalo-de-tróia no computador dos visitantes, com o objetivo de roubar senhas bancárias.

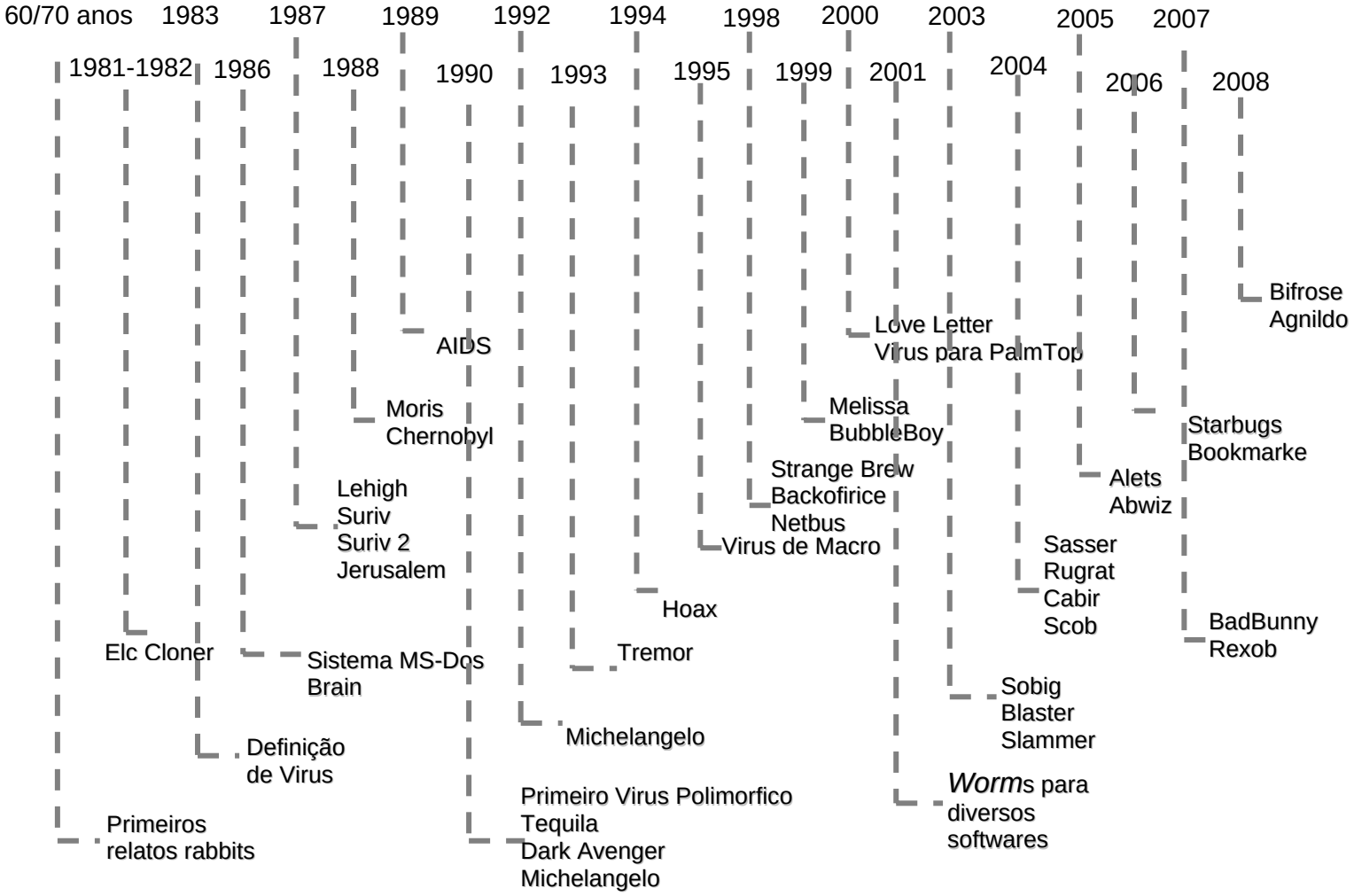
Segundo a Symantec (2008), para o ano de 2005 temos conhecido os *malwares Backdoor* Aletsb é uma mistura de *Backdoor* com Cavalo de Tróia que permite um ataque remoto sem a autorização do usuário através de canais de IRC e o *Abwiz* que permite ataques remotos sejam executadas várias vezes sem autorização, comprometendo o computador. Em 2006, *Starbugs* um vírus de macro escrito em *Starbasic* e contamina outros arquivos através de documentos do *staroffice* e *openoffice*, ainda neste mesmo ano temos o *bookmaker* que modifica a página principal do *Internet Explorer* e adiciona marcadores aos favoritos e arquivos do *desktop*. Em 2007 foi descoberto o *Badbunny* que é um *worm* que se espalham através de IRC, encontramos ainda neste mesmo ano *Rexob* ataca o sistema operacional Linux através de uma detecção genérica de um cavalo de tróia, permitindo que o computador seja comprometido através de um *backdoor*.

Ainda segunda a Symantec (2008), no ano de 2008 citamos os seguintes, *Bifrose* infecta os seguintes sistemas operacionais: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000, é um cavalo de tróia que compromete o computador através de um *backdoor* e *Agnildo* que contamina os sistemas operacionais Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000 é um *worm* de e-mail que recolhe os endereços do computador comprometido.

Segundo Vomicae (2008) os quantitativos de malwares conhecidos são:

- Até 1990 - 80 vírus
- Até 1995 - 5.000 vírus
- Até 1999 - 20.500 vírus
- Até 2000 - 49.000 vírus
- Até 2001 - 58.000 vírus
- Até 2005 - 72.010 vírus aproximadamente

***Timeline* de descoberta de M*alwares*:**

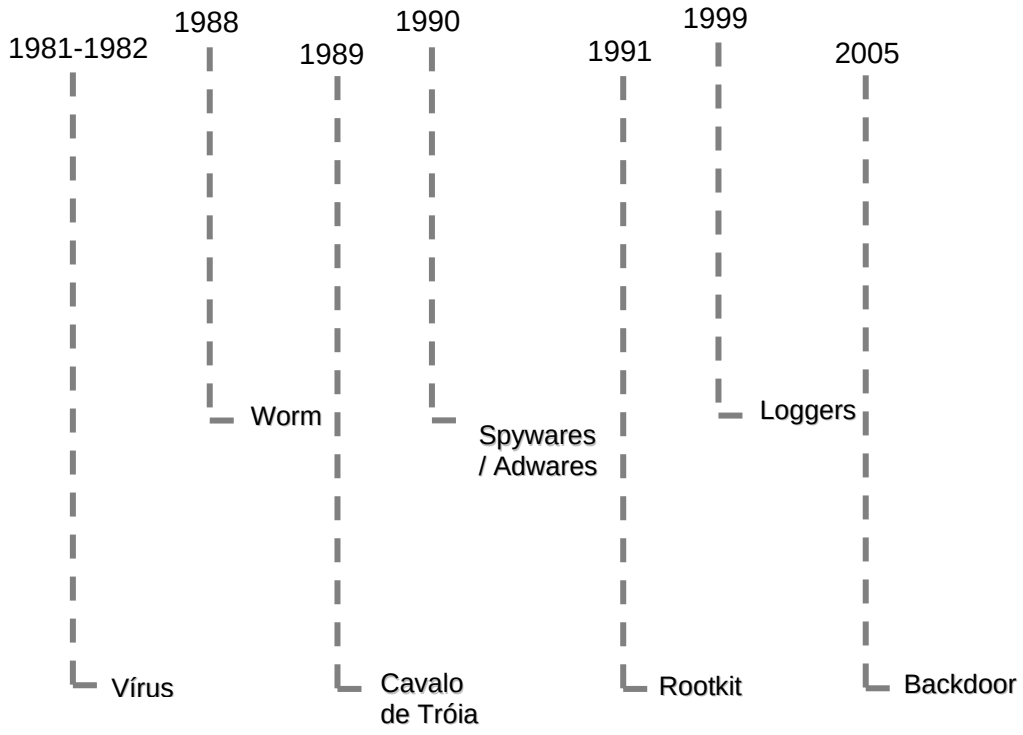


Baseado no Timeline acima verificou o surgimento dos *Malwares* ao longo do tempo, conhecido os primeiros relatos entre os anos 60 e 70, contudo a definição de vírus só tem no ano de 1983. Os *malwares* têm evoluído, muitas vezes é de difícil classificação, pois eles têm sido criados com mais de um tipo.

2.2 TIPOS DE *MALWARES*

Com o levantamento histórico dos *malwares*, conseguimos fazer uma cronologia e o modis operandis de cada.

***Timeline* dos tipos de M*alwares*:**



Com esse timeline identificamos o aparecimento de cada de tipo de *malwares*, surgido na história.

2.2.1 Virus

Segundo revista Info (2003) e Zeltser (2003) definem vírus de computador como:

> *"A program that infect other programs by modifying them to include a, possibly evolved, version of itself."*

Conforme Gaspar (2007) afirma o seguinte: "Vírus é um pedaço de código malicioso especialmente desenvolvido para infectar sistemas

computacionais. O vírus de computador, análogo ao vírus biológico, infecta o sistema, faz cópia de si mesmo e tenta se espalhar para outros computadores (organismos). Entretanto, ele precisa de uma aplicação hospedeira para se replicar e infectar outros sistemas.

Os virus são programas espúrios inseridos em computadores contra vontade do usuário e desempenham funções indesejadas. Alguns vírus têm a capacidade de se reproduzir e infectar outros dispositivos por toda a rede ou em CD vendidos em publicações, quem nos dá esse definição de virus é Carlos Medeiros (2001).

Temos a seguinte definição de André Faneli e Vanderlei Marchezini (2007), um programa ou fragmento de código, incapaz de funcionar de forma autônoma, requerendo por isso um programa hospedeiro, ao qual se anexa. Uma vez instalado num sistema, entra em operação quando o programa infectado é executado. Utiliza uma técnica de autopropagação, sendo capaz de infectar outros programas presentes no mesmo sistema ou alcançar outros sistemas através de emails com anexos infectados.

É um programa sempre malicioso, feito por programadores, para infectar um sistema, vírus de computador é um programa planejado e feito para se auto-copiar e se desenvolver em outros locais do computador e até em outros computadores, sem o conhecimento e permissão do usuário, utilizando-se de diversos meios. Um vírus infecta um programa e necessita deste programa hospedeiro para se propagar.

Comumente as contaminações acontecem quando o usuário executa um arquivo infectado, também pode acontecer a contaminação por um sistema operacional desatualizado. Existem alguns tipos que permanecem ocultos em determinados momentos, apenas atuando em horas específicas.

A contaminação entre máquinas pode ser realizada através de dispositivos removíveis (disquetes / Cds / pen-drive) ou pela rede (anexos de e-mail, arquivos do office). Os vírus típicos ficam com o controle temporário do sistema operacinal, fazendo cópias em novos aplicativos.

2.2.1.1 Ciclo de vida dos vírus

a) Hibernação – para enganar o usuário, fazendo com que propague o mesmo sem saber.
b) Propagação – faz cópias idênticas em outros aplicativos ou em algumas áreas do disco.
c) Ativação – “acorda” após ocorrer algum evento.
d) Execução – quando o vírus é ativado, indo da inofensiva a perigosa, desde apenas uma mensagem na tela como na exclusão de algum arquivo.

2.2.1.2 Tipo de vírus

a) Parasitas – quando executado um aplicativo ele se replica;
b) Residentes na memória – ficando como parte residente do sistema, contaminando qualquer aplicativo que seja executado;
c) Setores de boot – infecta o Master Boot Record, quando o sistema é ligado ele se espalha;
d) Oculto – este foi desenvolvido contra os sistemas *anti-virus*, ficando oculto;
e) Mutante – se modifica a cada infecção, dificultando a detecção.

2.2.2 Worms

Segundo Nelson Murilo e Klaus Steding-Jessen (2001), *worms* são programas com a capacidade de comprometer outras máquinas e se propagar para elas de modo automático usando a rede. Tipicamente executam uma varredura por sistemas e serviços vulneráveis, exploram essas vulnerabilidades e se copiam para a máquina recém explorada. Uma vez instalados na nova máquina, o ciclo à procura de novas máquinas recomeça.

Para Carlos Medeiros (2001), *worms* são *trojans* ou vírus que fazem cópias do seu próprio código e as enviam para outros computadores, seja por e-mails ou programas de bate-papo, dentre outras formas de propagação pela

rede. Eles têm se tornador cada vez mais comuns e perigosos porque o seu poder de propagação é muito grande.

Segundo Vírus & Cia. (2001), os Vermes (*Worms*) são programas autônomos que se propagam, se ativam sozinhos nos sistemas infectados, e procuram outros sistemas na rede que estejam acessíveis. Também é um tipo de vírus de computador, que tem como principal característica a autoduplicação, não necessitam se anexar a outros programas e residem e se multiplicam em ambientes Multitarefa, sendo que têm a característica de explorar as facilidades para executar processos remotamente em sistemas distribuídos.

O *worm* é um programa de reprodução que não infectar outros programas como faz os vírus, em vez disto, ele faz cópias dele mesmo, e fica se reproduzindo na tentativa de se espalhar em outras máquinas. Os *Worms* usam as memórias e as redes de banda larga, retardando os PCs e seus usuários. Muitas vezes os *worms* suprimem dados e espalham-se rapidamente.

Programas que tem como finalidade se propagar e infectar grande número de computadores, fazendo com que eles automaticamente enviem milhares de e-mail, ataque sites ou realizem tarefas específicas.

Worms significa vermes, considerado como um vírus mais inteligente que os demais. A principal diferença entre eles está na forma de propagação: os *worms* podem se propagar rapidamente para outros computadores, seja pela Internet, seja por meio de uma rede local, sendo assim um programa auto-replicante. É um programa completo e não precisa de outro programa para se propagar, dissemina-se criando cópias de si mesmo ou de suas partes em outros sistemas, com isso são responsáveis por utilizar muitos recursos (lotando o disco rígido).

Geralmente, a contaminação ocorre de maneira discreta e o usuário só nota o problema quando o computador apresenta alguma anormalidade. O que faz destes vírus inteligentes é a gama de possibilidades de propagação. A propagação se dá por conexão de rede ou anexos de e-mail.

Quando se propaga pode fazer as seguintes ações:

a) procura outros sistemas para infectar;

b) realiza conexão com o sistema remoto;

c) executa uma cópia dele mesmo para o sistema remoto e executa essa cópia.

Sua forma de proteção não é fácil. Alguns programas antivírus conseguem identificá-lo e impede que ele se propague. Pode ser evitado quando o sistema operacional e software sem vulnerabilidades estão atualizados e corrigidos. *Firewall* pode evitar que um *worm* explore uma possível vulnerabilidade em algum serviço disponível em seu computador ou pode evitar que explore vulnerabilidades em outros computadores.

2.2.3 Cavalo de Tróia

Carlos Medeiros (2001) nos dá a seguinte definição, os torjans são códigos maliciosos, geralmente camuflados como programas inofensivos que uma vez instalados no computador da vítima, podem permitir que o criador da praga obtenha o controle completo sobre a máquina infectada, que passa a ser chamda de “zumbi”.

Julio Cesar Gonçalves (2002) nos dá o seguinte conhecimento, a lenda do Cavalo de Tróia (em inglês *“Trojan Horse”*), diz que um grande cavalo de madeira foi presenteado pelos gregos aos troianos, como sinal de que estavam desistindo da guerra, porém o cavalo escondia no seu interior um grupo de soldados gregos, que esperaram a noite, abriram os portões da cidade de Tróia e o exército grego invadiu e dominou a cidade. Desta maneira, o nome “*Trojan*” um programa que oculta o seu objetivo sob uma camuflagem de outro programa útil ou inofensivo, é um programa que informa que executa uma atividade (que pode fazer ou não), mas na realidade ele realmente executa outra ação, sendo que essa segunda ação pode danificar seriamente o computador. André Faneli e Vanderlei Marchezini (2007), assim definem Cavalo de Tróia, programa que se apresenta contendo uma determinada finalidade, que realmente tem, mas adicionalmente e de forma secreta, possui uma segunda função cujo objetivo é abrir o computador para invasões, acessos remotos ou roubo de informações (senhas, por exemplo).

É um progama que além de executar as funções para as quais foi projetado, também executa outras funções maliciosas sem o consentimento do usuário.

O Cavalo de Tróia distingue-se por não replicar, por não infectar outros arquivos ou propagar cópias de si mesmo automaticamente. O arquivo precisa ser executado, suas ações se assemelham aos vírus e *worms*.

As seguintes ações maliciosas podem ser executadas:

a) alteração ou destruição de arquivos

b) furto de senhas e outras informações sensíveis

c) inclusão de backdoors, permitindo controle total sobre o computador

Muita gente confunde os "*Trojan Horses*" (Cavalos de Tróia) com vírus, ou vice-versa. Na verdade, os *Trojans* são programas que deveriam executar uma função, mas executam outra, geralmente destrutiva. Por exemplo, alguém pode fazer um programa e dizer que ele muda as letras do DOS. O programa tanto pode fazer isso como não, mas ao mesmo tempo formata seu disco rígido ou apaga todos os arquivos do diretório. Além disso, ele pode ser um vírus *dropper*, ou seja, pode liberar um vírus em seu sistema.

Com forma de proteção é a instalação de um bom antivírus, com a utilização de *Firewall* é possível bloquear o recebimento de alguns cavalos de tróia, as técnicas anti-spam filtram e-mails com cavalos de tróia. As medidas utilizadas para a proteção contra a infecção de vírus também tem bons resultados.

2.2.4 Spywares / Adwares

Para Mário Furlaneto Neto e José Augusto Chaves Guimarães (2003) *spywares / adwares* são programas espiões que enviam informações do computador do usuário da rede para desconhecidos, de maneira que até o que é teclado é monitorado como informação, sendo que alguns spywares / *adwares* têm mecanismos que acessam o servidor assim que o usuário fica on-line e outros enviam informações por e-mail.

Sergio Santolim (2004), assim define programas de computador, a maior parte deles fornecida gratuitamente (em sistema denominado freeware), cuja

utilidade declarada, para o usuário é uma, mas que se prestam na realidade a extrair e remeter informações deste mesmo usuário com finalidade comercial. Assim sem o conhecimento do consumidor, o programa, por exemplo, monitora quais os sites por ele acessados, e com que freqüência isto é feito permitindo a identificação do seu perfil de preferências, o que constitui em um núcleo de informações dotado de interesse comercial. Com a venda ou disponibilização destes dados a terceiros, o fornecedor do software licenciado “gratuitamente” ao usuário obtém sua remuneração.

São programas espiões que enviam informações do computador do usuário para desconhecidos da rede, essa definição quem nos dá é Juliana Tourinho, Patrícia Moura, Tadeu Fernandes e Thiago Silva.

Monitoram o uso do computador, podendo roubar informações como a sua lista de endereços de e-mail, por exemplo, enviando-a para *spammers*, programa automático que colhe informações sobre o usuário, seus hábitos na Internet e transfere essas informações, sem conhecimento e consentimento. Como é espionagem existem pessoas dispostas a pagar por essas informações.

Podem ser desenvolvidos por firmas para monitorar os hábitos de seus usuários para verificar seus costumes e vender informações / dados pela *Internet*. Essas informações têm por finalidade informar aos anunciantes que tipos de bens e serviços são susceptíveis de compra.

Os *spywares* / *adwares* podem vir legalmente sem que o usuário saiba, aceitando um contrato de licença de usuário final de um programa de software. Não é fácil identificar a sua presença, contudo como forma de proteção é a instalação e atualização de um bom *antivírus*, o sistema operacional e softwares sem vulnerabilidades atualizados e corrigidos, os *firewalls* pessoais não os elimina, porém se bem configurados são úteis para barrar a comunicação entre o invasor e o *boot* instalado no computador.

2.2.5 *Rootkit*

Para Nelson Murilo e Klaus Steding-Jessen (2001), o termo *rootkits* refere-se a um conjunto de ferramentas usadas pelo invasor não para obter privilégios de root, mas sim para manter esses privilégios.

Para Thiago Andrade (2005), *rootkits* é uma coleção de softwares projetados para não deixar pistas de um invasor e fornecer portas de fundo para futuras invasões no sistema, normalmente também contêm limpadores de log. A defesa é feita de um software de avaliação de integridade, mas se o *rootkits* atacar o Kernel (Núcleo do Sistema) a defesa é a prevenção através de scanners de *rootkits*, ou seja, fazer uma varredura no sistema a procura de *rootkits*.

> "Um *rootkits* é um conjunto de ferramentas usadas para implementar secretamente uma backdoor de nível administrativo em um sistema violado" (HORTON,MUGGE, pg. 200, 2003).

O *rootkit* é um tipo de vírus considerado novo, pois surgiu nos últimos anos. Seu principal objetivo é de se camuflar, com isso, faz com que seu código não seja encontrado por qualquer antivírus. Quando é feito um pedido para que um arquivo de leitura seja aberto, o virus captura os dados que são solicitados, permitindo apenas que o que passa sejam códigos não infectos, isso torma difícil que um antivirus ou outra ferramenta encontre o arquivo malicioso.

Ao realizar uma invasão, o invasor, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como *rootkits*.

As ferramentas que o compõem um *rootkits* não são usadas para obter acesso privilegiado, mas sim para mantê-lo. Isso quer dizer que o invasor, após instalar o *rootkits*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um *rootkits* pode fornecer programas com as mais diversas funcionalidades, tais como:

- Programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como arquivos, diretórios, processos, conexões de rede, etc;
- *Backdoor*, para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos *rootkits*);
- Programas para remoção de evidências em arquivos de *logs*;
- *Sniffer*, 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*, para mapear potenciais vulnerabilidades em outros computadores;
- Outros tipos de *malwares*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

Existem programas capazes de detectar a presença de um grande número de *rootkits*, mas isso não quer dizer que são capazes de detec tar todos os disponíveis (principalmente os mais recentes). Como os *rootkits* são projetados para ficarem ocultos, ou seja, não serem detectados pelo responsável ou pelos usuários de um computador, sua identificação é, na maioria das vezes, uma tarefa bem difícil. Os *rootkits* por ser novo utiliza avançadas tecnicas de programação, os mais avançados são difíceis de serem removidos.

2.2.6 *Loggers*

De acordo com Cert.br (2006), o keylogger normalmente vem como parte de um programa spyware ou cavalo de tróia. Dessa forma, é necessário que este programa seja executado para que o keylogger se instale em um computador. Geralmente, tais programas vêm anexados a emails ou estão disponíveis em sites na Internet.

Keyloggers tem a capacidade de capturar o pressionamento de teclas ou a área clicada ao redor do *mouse*. Seu objetivo é capturar informações

pessoais, tais como conta e senha bancárias de usuários vitimados pelas ações do código, essa é a descrição de C.E. Atílio (2003), T.A. Siqueira e A.M. Casiam(2003), da UNESP.

Keyloggers significa registrador do teclado o programa tem como finalidade monitorar tudo que é digitado. Comumente é utilizado de forma ilícita, seu principal objetivo é capturar senhas.

Alguns casos de *phishing*, e outros tipos de fraudes virtuais, são baseados em algum tipo de *Keylogger*, instalado no computador sem o conhecimento e consentimento do usuário, as informações são capturadas e enviadas a um cracker, que posteriormente irá utilizá-los com finalidades fraudulentas. Comumente se infiltra no computador do usuário através de e-mails e falsos links. O usuário só irá perceber a instalação indevida do *keylogger* quando o cracker já entrou no sistema e “pegou” as senhas capturadas.

É importante que computadores conectados a internet seja protegido por algum softwatre "*Anti-Spyware*", um "*Firewall*" e um "*Antivírus*".

Os *Keylogger* podem ser programados de diversas maneiras. Alguns para salvar os logs no próprio computador, esses são usados comumente em empresas, mas também por pais para verem o que seus filhos digitam no computador entre outros.

Contudo há *Keylogger* produzidos unicamente para fins ilícitos, sendo muito perigoso para as pessoas que são infectadas pois o seu criador pode ser um *script kiddie* (normalmente chamado de *Lammers*), baixá-lo e configurá-lo com o intuito de roubar dados como senhas de jogos*, MSN, emails* e *Orkut*. O usuário poderá ser alvo de duas ou mais pessoas; por sua programação ser feita já para redirecionar ao email do autor as informações capturadas. Existem também os chamados *keybank*, que são *Keylogger* feitos especialmente para roubar senhas bancárias e de cartão.

2.2.7 *Backdoor*

Para Greg McKlein, os backdoors são focalizados em dar ao atacante o acesso à máquina de alvo. Este acesso podia fazer exame de muitos

formulários diferentes, dependendo dos objetivos do atacante e do detalhe *backdoor* no uso.

Carlos Henrique Chaves e Antonio Montes dão a seguinte definição para os *backdoor*, os atacantes, após terem comprometido um sistema, normalmente utilizam um mecanismo para conseguir acesso a esse sem que uma vulnerabilidade em um software tenha que ser explorada. Este mecanismo é chamado de *backdoor*. Esse é freqüentemente instalado com a intenção de facilitar o retorno do atacante, bem como dificultar a sua detecção.

A definição de *backdoor* para Nelson Murilo e Klaus Steding-Jessen é a seguinte, após uma fase inicial de varredura o atacante localiza uma máquina com alguma vulnerabilidade e a explora, obtendo assim acesso privilegiado. Nesse momento a preocupação é não ser detectado e garantir futuros meios de acesso ao sistema através da instalação de *backdoors*. Este ciclo eventualmente recomeça com a utilização da máquina invadida para a varredura e invasão de outros sistemas vulneráveis.

Os *backdoor* necessitam de hospedeiros. Inicialmente foi usado de forma legítima para que desenvolvedores pudessem dar manutenção nas aplicações, sem que necessitassem passar por demorados processos de autenticação.

> “Aos programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de *backdoor*.” cert.br (2006).

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da *Internet*). Pode ser incluído por um invasor ou através de um cavalo de tróia.

Alguns dos casos em que a existência de um *backdoor* não está associada a uma invasão são:

- Instalação através de um cavalo de tróia;
- Inclusão como conseqüência da instalação e má configuração de um programa de administração remota;

Backdoors podem ser incluídos em computadores executando diversos sistemas operacionais, tais como Windows, Unix, Mac OS, Linux, entre outros. Existem casos em que a disponibilização de uma nova versão ou de um *patch* está associada à descoberta de uma vulnerabilidade em um *software*, que permite a um *hacker* ter acesso remoto a um computador, de maneira similar ao acesso aos *backdoors*.

Os acessos através de *backdoors* passaram a tornar-se ameaça por programadores inescrupulosos, o conceito veio a partir de simples programas onde obrigava a pessoa a inserir uma senha, levando ao usuário a pensar que estava realizando uma operação legítima, diferente de vírus e *worms* não criam replica de si mesmo.

É uma falha de segurança, pois permite a invasão do sistema por um *cracker*, podendo assim ter controle total da máquina. Utiliza-se *backdoor* para instalação de vírus e / ou programas maliciosos.

Como forma de proteção medidas de segurança deve ser focada no desenvolvimento dos programas, os softwares devem ser mantidos atualizados e aplicar as correções.

3 CARACTERÍSTICAS

Visto o timeline do capítulo 2 e capítulo 1, agora descrevemos as características técnicas de cada *malware*, com isso, pretendemos mostrar uma tabela comparativa a fim de agrupar os *malwares* conforme suas semelhanças técnicas.

Nas caractéristicas conseguimos informar o modis operandis dos *malware*s encontrados, sua forma de atuação, como se segue. Com o crescente número de malwares e sua evolução fica difícil determinarmos um último malware e classificá-lo como um único tipo.

3.1 BRAIN

Segundo a McAfee A única forma de infectar um computador com um Máster Boot Record (MBR) / Boot Sector infectar a partir de um disquete infectado. O setor de inicialização do disquete possui o código para determinar se o disquete é inicializável, e para apresentar o "Non-sistema de disco ou disco erro" mensagem. É este código que abriga a infecção, até o momento o sistema de não-disco mensagem de erro surge, a infecção ocorreu. Uma vez que o vírus é executado, ele irá infectar o disco rígido no setor de inicialização tornando-se residentes na memória, todos os subseqüentes boot o vírus será carregado na memória e tentará infectar disquete acessado pela máquina.

3.2 JERUSALÉM

Segundo a McAfee, Symantec e Sophos a ficha técnica do Jerusalém é a seguinte:

A única forma de infectar um computador com um arquivo vírus infectante é executar um arquivo infectado no computador. O arquivo infectado pode ser proveniente de uma multiplicidade de fontes, incluindo: disquetes, downloads através de um serviço online, rede, etc Uma vez que o arquivo infectado é executado, o vírus pode ser ativado.

Este vírus o vírus residia na memória infectando arquivos do tipo.exe, .bin, .com, pif, .ovl e apagava os arquivos quando ativado, não infecta arquivos do tipo COMMAND.COM.

3.3 AIDS

Segundo a Kaspersky a ficha técnica do AIDS é a seguinte:

Quando o disco infectado é carregado, o programa, automaticamente, instala-se no sistema, criando seus próprios arquivos e diretórios ocultos, modificando os arquivos do sistema. Após várias vezes carregado, o sistema operacional codifica os nomes de todos os arquivos, tornando-os invisíveis e deixando apenas um arquivo acessível. Este arquivo recomenda o depósito de dinheiro para uma determinada conta bancária.

3.4 TEQUILA

Segundo a Symantec, Kaspersky, Sophos e o AGV a ficha técnica do Tequila é a seguinte:

Com a execução de um arquivo infectado, o vírus infecta somente o registro mestre de boot. Na próxima vez que o sistema é recarregado o vírus ativa a memória e infecta todo o arquivo, entra em ação quando executa qualquer arquivo.EXE. Quando esse vírus é disparado, apresenta no canto superior um gráfico com as seguintes palavras:

Execute: mov ax, FE03 / int 21. Key to go on!.

Se as instruções forem executadas, aparecerá o seguinte:

Welcome to T. TEQUILA'S latest production

Contact T. TEQUILAP/P.o. Box 543/6312 St'hausen/Switzerland

Loving thoughts to L.I.N.D.A.

BEER and TEQUILA forever !

Quando infecções são realizadas nos hardwares uma cópia do registro de *boot* original é armazenada no último setor físico da divisória da primeira movimentação. Este vírus faz uma modificação nas divisórias dos *hardwares*, reduzindo o tamanho para proteger esta área.

3.5 TREMOR

Segundo a Symantec e AVG a ficha técnica do vírus Tremor é a seguinte:

Uma série de rotinas é executada quando este vírus é executado tanto para executar uma infecção quanto uma desinfecção de arquivos sob algumas circunstâncias específicas. Quando um arquivo é infectado, uma verificação da versão do sistema também está sendo executada. Se o sistema operacional for mais velho de 3.30, o arquivo é executado normalmente. Se o vírus estiver ativo na memória e a função de cópia estiver sendo executada em um arquivo infectado, o vírus desinfetar o arquivo de destino.

Quando o vírus está tentando carregar na memória verifica se há o uso de XMS e de UMB. Se encontrado, o vírus mover-se-á na memória estendida ou elevada; se indisponível, o código do vírus é movido para a parte superior da memória convencional.

Quando esse vírus é disparado, a seguinte mensagem apresenta no canto superior um gráfico com as seguintes palavras:

- => T.R.E.M.O. R foi feito por NEUROBASHER…

Depois que a mensagem acima é indicada, a tela retorna ao normal.

Segundo Sophos a ficha técnica do vírus Tremor é a seguinte:

Tremor produz um efeito tremendo a tela de forma aleatória, que é semelhante a um defeito monitor, o computador então trava. Um segundo efeito colateral é também invocada uma base aleatória e exibe a mensagem "-=> TREMOR foi feito por NEUROBASHER / Maio-Junho de'92, Alemanha <=--MOMENTO-DE-terror-IS-THE-INÍCIO DE LIFE-"depois de limpar a tela. O computador não congela no presente caso.

3.6 HOAX

Segundo a Symantec os HOAX são falsos vírus, mensagens normalmente enviadas por e-mail, que representam nada mais do que cartas

do tipo corrente. A seguir estão algumas das frases mais comuns utilizadas nesses avisos de falsos vírus:

- Se receber um e-mail chamado [nome do falso vírus de e-maill, não o abra!
- Exclua-o imediatamente!
- Ele contém o vírus [nome do falso vírus].
- Ele excluirá tudo em seu disco rígido e [perigo máximo e improvável especificado.
- Esse vírus foi anunciado hoje por [nome de uma empresa reconhecida.
- Envie esse aviso a todos os seus conhecidos!

A maioria dos avisos de falsos vírus segue esse modelo. Caso não esteja certo se um aviso de vírus é legítimo ou se é um alarme falso.

3.7 BACKORIFICE

Segundo a Symantec a ficha técnica do Backorifice é a seguinte:

Quando Backorifice é executado, faz o seguinte:

1. Espera por conexões incomuns ou locais pré-configurado. Se um invasor consegue conectar, eles podem:

- Upload e download de programas
- Iniciar programas
- Excluir arquivos
- Desligar o computador
- Bloquear o computador
- Controlar o teclado e o mouse

2. Dependendo da variante, realiza cópia de se mesmo nas seguintes pastas:

- %Windir%
- %System%
- %Temp%

3. Cria um valor do registro que consulta o arquivo que foi copiado na etapa 2 em qualquer destes registros:

- HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ funcionam HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ RunServices

Segundo McAfee a técnica do Backorifice é a seguinte quando o programa é executado em uma máquina Windows95/98, ele copia-se ao disco local, sob o nome “.Exe” (primeiro caracter é espaço, tamanho é de 124928 bytes) e instala uma referência a esse arquivo no registro, para que ele é executado sempre que a máquina reiniciar, o programa esconde a sua própria existência - não é visível como uma tarefa, embora seja permanentemente executando em segundo plano aguardando para os comandos provenientes do cliente através da rede. Após o programa está instalado em um computador, a pessoa que controla o cliente tem controle remoto sobre a máquina executando o programa do servidor, este controle inclui a gravação das teclas pressionadas, reiniciando ou bloqueando a máquina, reiniciar, modificar e transferir arquivos.

3.8 STRANGE BREW

Segundo a Sophos a ficha técnica do Strange Brew é a seguinte:

Quando um programa infectado (um arquivo Java. Classe) é executado, ele olha para os outros arquivos .class não infectado no diretório atual do usuário. O vírus copia-se em tais arquivos, modificá-los de modo que, quando são executados no futuro, recebam um controle, esses arquivos contêm erros que causam danos.

Segundo a Symantec e Kaspersky a ficha técnica do Strange Brew é a seguinte:

Uma vez que o vírus se localiza um arquivo infectado o seu conteúdo e carregados na memória, ele começa a olhar para os novos arquivos para infectar. Se um. "Classe" ficheiro tem um tamanho que é uniformemente divisível por 101, o vírus irá assumir que o ficheiro já está infectado porque a Strange Brew vírus atualizar todos os ficheiros que infecta a ter um tamanho divisível por 101. No entanto, esta lógica também irá fazer com que o vírus de

passar mais de alguns arquivos não infectados que acontecer de ter um Strange Brew-like tamanho. Uma vez que o vírus encontra uma. "Classe" arquivo que não parece estar infectada, ele verifica o arquivo para ver se ele é adequado para a infecção, com base em alguns critérios internos. Se o arquivo não é adequado para a infecção, o vírus irá inserir um número de bytes no arquivo para aumentar o seu tamanho para ser divisível por 101. Se o vírus encontra uma. "Classe" arquivo que é adequado para a infecção, ele irá inserir-se em este novo arquivo host (que é um arquivo infectado por um vírus é referido como um arquivo host). O vírus infecta novo. "Classe" arquivos, criando uma nova seção (um novo método) no arquivo e adicionar o seu próprio programa lógico para esta seção. O vírus então patches de acolhimento inicial do programa lógica para transferir o controle para o recém-inserido virais lógica. Durante este patch, o vírus vai realmente mudar o anfitrião, o programa de manipulação de erro, causando em alguns programas infectados a funcionar corretamente. No entanto, muitas aplicações Java continuará a funcionar corretamente. Finalmente, o vírus irá atualizar uma série de outras tabelas e campos no arquivo.

O vírus tentará infectar todos os arquivos .class arquivo no diretório atual antes de retornar o controle para o acolhimento aplicação, aumentando o tamanho do arquivo de cada um por cerca de 3.890 bytes. O vírus também muda o diretório data e hora de cada ficheiro que tenha processado.

3.9 NETBUS

Segundo a Sophos, Symantec e McAffe a ficha técnica do Netbus é a seguinte:

Netbus pode funcionar em Windows 95, em 98 e em NT, permite que um hacker alcance a máquina do usuário através do TCP/IP. O Netbus tem as peças do cliente e do usuário. A peça do usuário é instalada em um sistema remoto quando acessada. Quando executada, será instalada ao diretório do Windows e será executada automaticamente durante a seguinte execução do Windows através do registro do sistema e normalmente na seguinte posição:

- HKLM \ software \ Microsoft \ Windows \ CurrentVersion \

O servidor se separa em partes para proteger-se de ser removido do sistema - esconde seu nome no processo de gerenciamento de tarefa de Windows e nega o acesso ao arquivo na tentativa de não ser remotivo ou renomeado.

3.10 CIH – CHERNOBYL

Segundo a Symantec e McAfee a ficha técnica do Chernobyl é a seguinte:

Segundo Symantec CIH é um vírus que infecta o Windows 32-bit 95/98/NT arquivos executáveis, mas só pode funcionar com o Windows 95/98 e ME. Ela não funciona no Windows NT ou Windows 2000. Quando um programa infectado é executado no Windows 95/98/ME, o vírus se torna residente na memória.

Segundo McAfee os vírus de W95/CIH podem se separar e se instalar no corpo do código do vírus colocando-o dentro das partes não utilizadas do arquivo infectado (os arquivos .PE geralmente contêm espaço não utilizado). Tais arquivos não serão executados no NT, no Windows 2000 ou no XP porque sua estrutura é inválida.

O vírus contêm um payload muito perigoso, tentam reescrever o flash-BIOS. Se o flash-BIOS estiver permitido para reescrever (e este é o caso na maioria dos computadores modernos com um flash-BIOS) isto rende a máquina instável porque já não carregará. Ao mesmo tempo, reescreve o disco rígido com lixo.

3.11 BUBBLEBOY

Segundo a Symantec, McAfee e Kaspersky a ficha técnica do Bubbleboy é a seguinte:

Este é um *worm* de Internet que requer o Internet Explorer 5 com o Windows Script Host instalado - WSH é padrão no Windows 98 e Windows 2000 instalações. Ele não corre no Windows NT devido a limitações embutido

em código. Este *worm* está escrito em VB Script. Existem duas variantes, o. B variante é criptografada.

Este *worm* afeta somente as versões em Inglês e espanhol do Windows. No MS Outlook, este *worm* exige que você abra o e-mail. Ele não será executado se estiver usando o Preview Pane. No MS Outlook Express, o *worm* é ativado quando Preview Pane é usado! Em ambos, se as configurações de segurança para a Internet Zone em IE5 estão configuradas como Alta, o *worm* não será executado. A vulnerabilidade explorada por este *worm* tem sido abordada pela Microsoft com um patch de segurança. A instalação deste patch Internet Explorer irá impedir a execução do presente *worm* sob configurações de segurança padrão. Network Associates recomenda aplicar este patch para todos os computadores executando o IE.

Depois o VB Script executa, ele grava o arquivo UPDATE.HTA para a máquina local e durante a próxima inicialização do Windows, o. HTA arquivo é invocado.

Este *worm* cria o arquivo UPDATE.HTA na pasta C: \ Windows \ startmenu \ Programas \ pasta Inicializar. Após a inicialização do Windows ou reiniciar, o *worm* código é invocado.

Webshield para Solaris 4,0 detecta o vírus Bubbleboy no correio SMTP quando configurados a varredura de Alto Nível e configurado para Descartar arquivos infectados. Portadores do vírus mail será enviado para o seu destino com um aviso de remoção do vírus no local do código HTML original.

Gauntlet para UNIX 5.5 detecta o vírus Bubbleboy no correio SMTP quando configurado para usar uma agente local varredura. O agente deve ser configurado para verificar todos os arquivos e para Descartar arquivos infectados. Portadores do vírus mail será enviado para o seu destino com um aviso de remoção do vírus no local do código HTML original.

O UPDATE.HTA arquivo é codificado para fazer o seguinte:

- Altera o proprietário registrado através do registro de Bubbleboy
- Altera a organização registrada para Vandelay Industries
- Envia embutida em si mesmo uma mensagem de correio eletrônico para cada contacto em todos os e-mails do MS Outlook LISTA DE ENDEREÇOS

- Define a chave de registro para indicar que a distribuição tenha ocorrido. Distribuição de e-mail não será repetida.

O e-mail é uma mensagem com as seguintes informações:

- De: pessoa que enviou *worm* involuntariamente
- Assunto: Bubbleboy está de volta!
- Corpo da mensagem: O Bubbleboy incidente, imagens e sons
- http://www.towns.com/dorms/tom/bblboy.htm
  Esta não é uma página web válida.

Chave de modificação:

- HKLM \ Software \ OUTLOOK.BubbleBoy = OUTLOOK.Bubbleboy 1,0 por zulu
- HKLM \ Software \ OUTLOOK.BubbleBoy \ OUTLOOK.Bubbleboy = 1,1 por zulu
- HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ RegisteredOwner = BubbleBoy
- HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ RegisteredOrganization = Vandelay Industries

Segundo Sophos Bubbleboy é um vírus e sua ficha técnica é a seguinte:

A mensagem contém um arquivo HTML contendo um embutido viral Visual Basic Script. Este arquivo não é um apego. Se você estiver usando o MS Outlook, o script é executado quando você abrir o e-mail. Se você estiver usando o MS Outlook Express, o script pode ser executado a partir do painel de visualização também.

O script é capaz de atacar uma falha de segurança nos produtos da Microsoft que permite que dois controles activex potencialmente malicioso (Scriptlet. Typelib e Eyedog) a serem executado.

Uma vez que o vírus se executa, ele desce um arquivo para a inicialização do Windows diretório chamado UPDATE.HTA. Após a inicialização, este arquivo executa e edita o registro do sistema. Trata-mails, em seguida, uma cópia de si próprio, utilizando o Outlook, para cada endereço em seus catálogos de endereços do Outlook.

3.12 MELISSA

Segundo a Symantec e AGV a ficha técnica do Melissa é a seguinte:

Melissa (também conhecido como W97M. Melissa) é um vírus macro típico de que utiliza payload incomum. Quando um usuário abre um arquivo infectado, o vírus enviará uma cópia deste arquivo para 50 outros e-mails, usando a Microsoft Outlook.

Infecta os arquivos do MS Word 97 e do MS Word 2000 adicionando um VBA5 novo (macro) Melissa nomeado módulo. Embora não haja nada original na rotina da infecção deste vírus macro, tem um payload que utilize o MS Outlook para emitir um arquivo infectado. Quando um usuário abrir ou fechar o arquivo infectado.

Verificando a seguinte chave do registro:

- "HKEY_CURRENT_USER\Software\Microsoft\Office\" as "Melissa?" value.

Se não encontrar a entrada do registro, o vírus faz o seguinte:

- 1. Abre o MS Outlook.
- 2. Usando chamadas de MAPI, começa o perfil de usuário usar o MS Outlook.
- 3. Cria uma mensagem nova do e-mail a ser emitida para 50 endereços alistados no livro de endereço do MS Outlook do usuário.
- 4. Dá à mensagem do email uma linha sujeita: "Important Message From USERNAME", onde o username é feito exame do ajuste do MS Word.
- 5. O corpo da mensagem do email é: "Here is that document you asked for ... don't show anyone else ;-)"
- 6. Une o original ativo (o original infectado que está sendo aberto ou fechado) à mensagem do email.
- 7. Emite os e-mails.

3.13 LOVE LETTER

Segundo a Symantec, McAfee, e Kaspersky a ficha técnica do Love Letter é a seguinte:

Esta é uma detecção do vírus:

I-*Worm*, Loveletter IRC / Loveletter Love Bug LOVE-LET. VBS carta de amor-DE-YOU.TXT. Vbs Loveletter Troj / Lovelet-A VBS. Loveletter. A VBS / Lovelet VBS-A / B Lovelet-VBS / Lovelet VBS-C / Lovelet-E VBS / Loveletter. A VBS / Loveletter. *Worm* Vbs_loveletter veryfunny. Vbs WIN-BUGSFIX.EXE

Verificar se as extensões.VBS. HTM estão incluídas quando a pesquisa.*

Como esta detecção abrange muitas variantes, podem existir outros sintomas diferentes, este vírus chega em um e-mail com este formato:

- Assunto "ILOVEYOU"
- Mensagem "gentilmente verificar o acompanha Loveletter próximos de mim."
- Penhora "carta de amor-DE-YOU.TXT. vbs"

Note que outras ameaças podem usar nomes semelhantes, tais como W95/MTX.gen @ M, que utiliza o nome do arquivo carta de amor-DE-YOU.TXT.pif):

Se o usuário executar a penhora é executado usando o Windows Script Host programa. Esta não é normalmente presentes no Windows 95 ou Windows NT a menos que o Internet Explorer 5 esteja instalado.

Primeiro executa cópias de si mesmo e escreve um. HTM arquivo nos seguintes lugares:

- WINDOWS \ SYSTEM \ MSKERNEL32.VBS
- WINDOWS \ WIN32DLL.VBS
- WINDOWS \ SYSTEM \ carta de amor-DE-YOU.TXT.VBS
- WINDOWS \ SYSTEM \ carta de amor-DE-YOU.HTM

Acrescenta também as chaves do Registro:

- HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ MSKernel32 = WINDOWS \ SYSTEM \ MSKernel32.vbs
- HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices \ Win32DLL = WINDOWS \ Win32DLL.vbs

Este vírus busca todas as unidades ligadas ao sistema de acolhimento e substitui os seguintes arquivos:

- *. JPG
- *. JPEG

Com cópias de si mesmo e se acrescenta a extensão. VBS para o nome do arquivo original. Então PICT.JPG seria substituída com PICT.JPG.VBS e isso iria conter o vírus. Também substitui os seguintes arquivos:

- *. VBS
- *. VBE
- JS *.
- *. Jse
- *. CSS
- WSH *.
- SCT *.
- *. HTA

Com cópias de si mesmo e renomeia os arquivos para *. VBS. Este vírus também localiza os seguintes tipos de arquivo:

- MP3 *.
- *. MP2

Se for encontrado, torna-os escondidos e cópias em si, exceto com nomes como estes. VBS extensão. O vírus cria um arquivo "carta de amor-DE-YOU.HTM", que contém o vírus e este é depois enviada para os canais de IRC mirc, se o cliente estiver instalado. Depois de uma curta demora, o vírus usa a Microsoft Outlook para enviar cópias de si mesmo para todas as entradas no livro de endereços. Os e-mails serão do mesmo formato do original.

3.14 SLAMMER

Segundo a Symantec, McAfee, e Kaspersky a ficha técnica do Slammer é a seguinte:

Quando o *worm* W32.SQLExp.*Worm* ataca um sistema vulnerável, ele faz o seguinte:

- Envia uma cópia de si mesmo para o SQL Server Resolution Service, o qual monitora a porta 1434 do UDP.
- Explora uma vulnerabilidade de transbordo de buffer que permite que uma porção da memória do sistema seja sobrescrita. Ao fazer isso, ele é executado no mesmo contexto de segurança do que o serviço do Servidor SQL.
- Chama a função API do Windows, GetTickCount, e utiliza o resultado como fonte para gerar endereços IP aleatórios.
- Abre um soquete no computador infectado e tenta enviar uma cópia de si mesmo repetidamente à porta 1434 do UDP nos endereços IP que gerou, usando uma porta de fonte temporária. Como o *worm* não ataca os hostes seletivamente na sub-rede, o resultado é uma grande quantidade de trânsito.

3.15 BLASTER

Segundo a Symantec, McAfee, Sophos e Kaspersky a ficha técnica do Blaster é a seguinte:

Quando o W32.Blaster.*Worm* é executado, ele faz o seguinte:

1. Verifica se o computador já está infectado e se o *worm* está sendo executado. Em caso positivo, o *worm* não irá infectar o computador novamente.
2. Adiciona o valor à chave de registro;
   - "windows auto update"="msblast.exe"
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run

Para que o *worm* seja executado na inicialização do Windows.

3. Gera um endereço IP e tenta infectar o computador que possui aquele endereço. Esse endereço IP é gerado de acordo com os seguintes algoritmos:
   - Para 40% do tempo e endereço IP gerado é da forma A.B.C.0, onde A e B são iguais às primeiras duas partes no endereço IP do computador infectado.

- C também é calculado pela terá parte do endereço IP do computador infectado. Entretanto, para 40% do tempo o *worm* verifica se C é maior do que 20. Se for, um valor aleatório menor do que 20 é subtraído de C. Uma vez que o endereço IP é calculado, o *worm* irá tentar acessar um computador cujo endereço IP seja A.B.C.0.

O *worm* então irá incrementar a última parte do endereço IP (0), tentando acessar outros computadores baseados no novo endereço IP, até que este atinja 254.

- Com probabilidade de 60%, o endereço IP gerado é completamente aleatório.

4. Envia dados para a porta TCP 135 que podem explorar a vulnerabilidade do RPC do DCOM. O *worm* envia um de dois tipos de dados: um para explorar a vulnerabilidade no Windows XP e outra para o Windows 2000. Em 80% do tempo os dados para o Windows XP serão enviados e para 20% dados para o Windows 2000.
5. Usa o Cmd.exe para criar uma interface remota e oculta que irá monitorar a porta TCP 4444, permitindo ao invasor executar comandos no computador infectado de maneira remota.
6. Monitora a porta UDP 69. Quando o *worm* recebe uma solicitação de um computador conectado através da vulnerabilidade do RPC do DCOM ele enviará o arquivo msblast.exe e executará o *worm*.
7. Se a data atual for dia 16 ou superior dos meses de janeiro a agosto, ou se o mês atual for de setembro a dezembro, o *worm* tentará executar um ataque Dos (Negação de Serviço) no servidor do Windows Update. Entretanto, essa tentativa só terá sucesso se uma das condições abaixo ocorrer:

- O *worm* está ativo em um computador que executa o Windows XP e este foi infectado ou reiniciado durante o período onde o *worm* causa maior dano.
- O *worm* está ativo em um computador que executa o Windows 2000 e que foi infectado durante o período onde o *worm* causa maior dano e não foi reiniciado desde o momento da infecção.

- O *worm* está ativo em um computador que executa o *Windows* 2000 e que foi reiniciado desde que foi infectado, durante o período onde o *worm* causa maior dano, e o usuário logado no momento é Administrador.

8. O tráfego do DoS possui as seguintes características:

- Gera um alto tráfego de pacotes para porta 80 do windowsupdate.com.
- Tenta enviar 50 pacotes RPC e 50 pacotes HTTP a cada segundo.
- Cada pacote possui o tamanho de 40 bytes.
- Se o *worm* não encontrar a entrada de DNS para o windowsupdate.com, ele usará 255.255.255.255 como endereço de destino.

Algumas características corrigidas do TCP e dos cabeçalhos IP são:

- Identificação do IP = 256
- Tempo de vida = 128
- Endereço IP original: = a.b.x.y, onde a.b são do ip do host e x.y aleatórios. Em alguns casos a.b também são aleatórios.
- Endereço IP de destino: = resolução dns de "windowsupdate.com"
- A porta TCP de origem está entre 1000 e 1999
- A porta TCP de destino = 80
- Número de seqüência do TCP sempre possui dois bytes de menor valor definidos como 0; os dois maiores valores são aleatórios.
- Tamanho da janela TCP = 16384

O *worm* contém o seguinte texto, que nunca é exibido:

- I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!! (Tradução: Eu só queria dizer EU TE AMO, SAN!! billy gates porque você deixa isso acontecer? Pare de ganhar dinheiro e corrija seu software!!).

3.16 SOBIG

Segundo a Symantec, McAfee, Trend Micro e Sophos a ficha técnica do Sobig é a seguinte:Este *worm* é escrito em MSVC e tenta espalhar através de e-mail e partilhas de rede, este worm também é capaz de descarregar ficheiros a partir de determinados sites. Ele roda em Windows 98, ME, NT, 2000, XP e Server 2003.

Propagação por e-mail:

As mensagens são de email são formatadas como segue:

- From: big@bos s.com
- Subject: Como segue:
  - Re: Filmes
  - Re: Amostra
  - Re: Documento
  - Re: Referente a amostra
- Attachment: 65,536 bytes com um dos seguintes nomes de arquivo:
  - Filme_0074.mpeg.pif
  - Documento003.pif
  - Untitled1.pif
  - Amostra.pif

Os endereços de email podem ser colhidos dos arquivos na máquina da vítima com as seguintes extensões:

- WAB
- DBX
- HTM
- HTML
- EML
- TXT

Propagação por rede:

O *worm* enumera partes na rede, pretendendo copiar as seguintes pastas em máquinas remotas:

\WINDOWS\ALL USERS\START MENU\PROGRAMS\STARTUP ou \DOCUMENTS AND SETTINGS\ALL USERS\START MENU\PROGRAMS\STARTUP

3.17 SCOB

Segundo a Symantec, McAfee, Trend Micro, Sophos a ficha técnica do Scob é a seguinte:

Este Cavalo de Tróia realiza um arquivo Ads.vbs, não um arquivo malicioso que é normal um utilizado na administração Microsoft IIS, no diretório atual. Em sistemas com o IIS instalado. Arquivos DLL na pasta System.

Arquivos DLL seguir o seguinte formato:

- iisXXX.dll (XXX é composto por acaso dígitos hexadecimais.)

São encontrados os seguintes arquivos, JS_SCOB. com arquivos DLL. e modifica as propriedades do IIS Web sites na máquina de um modo que a derrubada. DLL arquivo predefinido torna-se rodapé do documento. Isto significa que os códigos dos arquivos. Dll são escritos e executados na parte inferior das páginas da Web IIS quando eles são acessados.

3.18 CABIR

Segundo a Symantec e McAfee a ficha técnica do Cabir é a mesma, porém na hora de classificar pra Symantec é worm e para McAfee é vírus, a ficha técnica do Cabir é a seguinte:

O worm repetidamente envia-se para o primeiro dispositivo Bluetooth ativado que possa encontrar independentemente do tipo de dispositivo. Por exemplo, até mesmo uma impressora Bluetooth - permitido será atacado, se for dentro do alcance.

O worm se espalha como um arquivo. SIS arquivo, que é instalado no diretório APPS. Não há nenhuma carga, além do reduzido substancialmente a vida da bateria provocada pela constante pesquisa de dispositivos Bluetooth-permitida.

3.19 RUGRAT

Segundo a Symantec, McAfee e Kaspersky a ficha técnica do Rugrat é a seguinte:

O Rugrat um vírus de infecção de ação direta (ele sai da memória após a execução) em arquivos executáveis portáteis do IA64 Windows (PE, Portable Executable). Estes arquivos PE incluem a maioria dos programas Windows de 64-bit exceto os .dll.

O vírus infecta arquivos que estão na pasta onde está alojado e em suas subpastas. Este é o primeiro vírus conhecido para o Windows 64-bit e usa as estruturas Thread Local Storage (Armazenamento de Segmento Local) para executar o código viral. Este é um método incomum de executar um código.

Ele não infecta arquivos PE de 32-bit e não será executado em plataformas Windows 32-bit. O vírus é escrito em um código IA64 assembly.

O Rugrat. é um vírus proof-of-concept (com algo novo ou que nunca foi visto), razoavelmente simples. O vírus usa um pequeno número de API Win64 a partir de três bibliotecas diferentes:

- NTDLL.DLL
- SFC_OS.DLL
- KERNEL32

De NTDLL.DLL, o vírus usa estas funções:

- LdrGetDllHandle()
- RtlAddVectoredExceptionHandler()
- RtlRemoveVectoredExceptionHandler()

O vírus suporta tratamento vetorizado de exceção para evitar travamentos durante as infecções.

A função SfcIsFileProtected() de SFC_OS.DLL é usada para evitar a infecção de executáveis protegidos pelo System File Checker (SFC).

As 16 funções a seguir são usadas do KERNEL32.DLL para implementar uma infecção padrão de arquivo de uma imagem do executável portátil do IA64:

- CreateFileMappingA()
- CreateFileW()

- CloseHandle()
- FindFirstFileW()
- FindNextFileW
- FindClose()
- GetFullPathNameW()
- GetTickCount()
- GlobalAlloc()
- GlobalFree()
- LoadLibraryA()
- MapViewOfFile()
- SetCurrentDirectoryW()
- SetFileAttributesW()
- SetFileTime()
- UnmapViewOfFile()

O vírus carrega dentro dele a seguinte string, que nunca é exibida:

- Shrug - roy g biv

A rotina de infecção do arquivo é padrão. A última seção do executável é marcada como executável, o corpo do vírus é inserido dentro dela e um número aleatório de bytes é anexado ao final do corpo do vírus.

3.20 SASSER

Segundo a Symantec, McAfee, Trend Micro, Sophos e Kaspersky a ficha técnica do Sasser é a seguinte:

O Sasser é um *worm* que tenta explorar a vulnerabilidade Microsoft Security Bulletin MS04-011. Ele se propaga verificando endereços IP selecionados aleatoriamente de sistemas vulneráveis.

Quando o Sasser é executado, ele faz o seguinte:

- Tenta criar um mutex chamado Jobaka3l e é finalizado se a tentativa falha. Isso assegura que não mais de uma instância do *worm* pode ser executada em um computador ao mesmo tempo.
- Cria uma cópia de si mesmo como %Windir%\avserve.exe.
- Adiciona o valor:

        - "avserve.exe"="%Windir%\avserve.exe"
- À chave de registro:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Run
- Para que o *worm* seja executado sempre que o Windows for iniciado.
- Utiliza a API AbortSystemShutdown para atrapalhar as tentativas de desligar ou reiniciar o computador.
- Iniciam um servidor FTP na porta TCP 5554. Este servidor é usado para disseminar o *worm* para outros servidores.
- Percorre todos os endereços IP dos hosts procurando endereços que não possua qualquer das seqüências abaixo:
    - 127.0.0.1
    - 10.x.x.x
    - 172.16.x.x - 172.31.x.x (inclusive)
    - 192.168.x.x
    - 169.254.x.x
- Usando um destes endereços IP, o *worm* irá gerar um endereço IP aleatório.
    - Em 52% das vezes, o endereço IP será completamente aleatório.
    - Em 23% das vezes, os últimos três octetos são alterados para números aleatórios.
    - Em 25% das vezes, os dois últimos octetos são alterados para números aleatórios.
- Conecta-se a um endereço IP gerado aleatoriamente na porta TCP 445 para determinar se o computador remoto está online.
- Se a conexão for feita a um computador remoto, o *worm* irá enviar um código para ele, o qual fará com que este abra a porta TCP 9996.
- Utiliza a abertura no computador remoto para reconectar ao servidor FTP do computador infectado, executado na porta TCP 5554, e obter uma cópia do *worm*. O nome desta cópia terá quatro

ou cinco dígitos, seguindo de _up.exe. Por exemplo, 74354_up.exe.

- O processo Lsass.exe irá travar se o *worm* explorar a vulnerabilidade do LSASS do Windows. O Windows exibirá um alerta e desligará o sistema dentro de um minuto.

3.21 ALETS

Segundo a Symantec a ficha técnica do Alets é a seguinte:

Este Backdoor quando executado realize as seguintes ações:

1. Cria uma cópia de si mesmo:
   - %Windir%\svshost.exe
2. Adciona o seguinte valor:
   - "Microsoft Services" = "%Windir%\svshost.exe"

Para a seguinte chave de registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Com isso é executado todas as vezes que o Windows é iniciado.

3. Abre um backdoor que contem o servidor de IRC com o endereço de IP 140.239.119.102 através da porta TCP 32440. Isto permite que um acesso remoto não autorizado acesse o computador.

Estes comandos podem permitir que o atacante remoto termine processos ou download e execute arquivos no computador comprometido.

3.22 ABWIZ

Segundo a Symantec, Mcaffe e Sophos a ficha técnica do Blaster é a seguinte:

Quando executado realize as seguintes ações:

1. Faz cópia de si mesmo
   - %System%\win32.exe.
2. Drops the file %System%\zlbw.dll.

3. Adiciona os valores:

- "wupd" = "%System%\win32.exe"

e a subchave de registro:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Com isso é executado todas as vezes que o Windows é iniciado.

4. Envia informações para o computador contaminado através de HTTP POST para o seguinte endereço:

- 217.159.201.176

5. Baixa e executa atualizações através do seguinte URL:

- [http://]217.159.201.176/[REMOVED]/cntr/bin/latest.exe

3.23 BOOKMARKER

Segundo a Symantec, Mcaffe e Sophos a ficha técnica do Bookmarker é a seguinte:

Quando executado realiza as seguintes ações:

1. Cria os seguintes arquivos:

- %UserProfile%\Desktop\BEST DATING SITE IN THE NET.lnk
- %UserProfile%\Desktop\BEST DATING SITES CATALOGUE.lnk
- %UserProfile%\Desktop\BEST ONLINE DATING CHAT ROOMS.lnk
- %UserProfile%\Desktop\BEST ONLINE DATING MAGAZINE.lnk
- %UserProfile%\Desktop\BEST ONLINE DATING WEBCAMS.lnk
- %UserProfile%\Favorites\BEST DATING SITE IN THE NET.lnk
- %UserProfile%\Favorites\BEST DATING SITES CATALOGUE.lnk
- %UserProfile%\Favorites\BEST ONLINE DATING CHAT ROOMS.lnk
- %UserProfile%\Favorites\BEST ONLINE DATING MAGAZINE.lnk
- %UserProfile%\Favorites\BEST ONLINE DATING WEBCAMS.lnk

2. Faz cópia dele mesmo no seguinte arquivo:

- %System%\datingtool.exe

3. Adiciona o valor:

- "ControlPanel" = "%System%\datingtool.exe internet.dll,Datingtool"

para a subchave de registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run

com isso é executado todas as vezes que o Windows é iniciado.

4. Adiciona o valor:

- "Start Page" = "[http://]dating.enetcap.com/Datin[REMOVED]"

para a subchave de registro:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

para modificar a página inicial do Internet Explorer.

5. Ajusta as entradas para casa 60 segundos de registro.

6. Abre uma nova janela do Internet Explorer com o seguinte endereço de URL a cada 300 minutos:

- [http://]dating.enetcap.com/Datin[REMOVED]

3.24 BADBUNNY

Segundo a Symantec, Mcaffe e Sophos a ficha técnica do Badbunny é a seguinte:

Quando executado cria os seguintes arquivos:

- c:\drop.bad (A copy of IRC.Badbunny)
- C:\badbunny.js (A copy of JS.Badbunny)
- BadBunny.pl (A copy of Perl.Badbunny)
- badbunny.rb (A copy of Ruby.Badbunny)
- badbunnya.rb (A copy of Ruby.Badbunny)
- C:\mirc\script.ini (A copy of IRC.Badbunny)
- C:\mirc32\script.ini (A copy of IRC.Badbunny)
- C:\Program Files\mirc\script.ini (A copy of IRC.Badbunny)
- C:\Program Files\mirc32\script.ini (A copy of IRC.Badbunny)

Então baixa o arquivo com o seguinte endereço de URL:

Quando executado cria os seguintes arquivos:

- [http://]www.gratisweb.com/badbunny/badbun[REMOVED]

3.25 BIFROSE

Segundo a Symantec, Mcaffe e Kaspersky a ficha técnica do Bifrose é a seguinte:

Quando executado cria os seguintes arquivos:

- %System%\netview.exe
- %System%\waults.exe
- %System%\ld.exe

Cria os seguintes registros de entrada, para ser executado todas as vezes que o Windows inicia:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\"waults" = "%System%\waults.exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"netview" = "%System%\netview.exe"
- HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\"waults" = "%System%\waults.exe"
- HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\"waults" = "%System%\waults.exe"

Com isso cria os seguintes registros de entrada:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}\"stubpath" = "%System%\netview.exe s"
- HKEY_CURRENT_USER\Identities\"Last User Identity" = "0x00029B46"

Isso cria as seguintes subchaves de registro:

- HKEY_LOCAL_MACHINE\SOFTWARE\SKav\nck
- HKEY_CURRENT_USER\SOFTWARE\SKav
- HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}

- HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A5CDF7EC-751B-46aa-AD69-4005FE080DE8}
- HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\SOFTWARE\SKav
- HKEY_CURRENT_USER\VirtualStore\MACHINE\SOFTWARE\SKa

Esse cavalo de tróia esconde-se criando um novo página do Internet Explorer para se infiltrar nesse processo.

Periodicamente, acessa os seguintes endereços de Web:

- [http://]ginzz.3322.org
- [http://]tyosyozz.3322.org
- [http://]takahashi.3322.org

Resumo do Modis Operandi dos *Malwares*:

	Vírus	Falso Vírus	Cavalo de Tróia (Trojan Horse)	*Worm*	*Backdoor*	*Spyware*
Brain	X					
Jerusalém	X X X					
AIDS			X			
Tequila	X X X					X
Tremor	X X X X					
HOAX		X X X X X X				
BackOrifice			X X X			
Strange Brew	X X X					
NetBus			X X X		X X X	
Chernobyl	X X					
BubbleBoy	X			X X X		
Melissa	X X					
Love Letter	X X X					
Slammer				X X X		
Blaster				X X X X		
Sobig				X X X X		
Scob			X X X X			
Cabir				X X		
Rugrat	X X X					
Sasser				X X X X X		
Alets			X		X	
Abwiz			X X X	x		
Bookmarker			X X X			
Badbunny	X X X			X X X		
Bifrose			X X X		X	

X – Symantec / X – Sophos / X – Kaspersky / X – McAfee / X – AVG /Trend micro

Através da tabela acima, concluimos que as empresas de antivirus nem sempre têm um padrão de definição para as centenas de malwares exitente, são coincidentes nas fichas técnicas, contudo na classificação podemos encontrar algumas diferenças.

Todos os malwares citados acima foram pesquisado no sites das grandes empressas de antivírus.

Mostraremos a seguir uma proposta de taxonomia como agrupar os malwares e comom classificar os mesmo.

4 TAXONOMIA

Taxonomia é uma forma de classificação, agrupamento que pode ser realizado em algum tipo de organismo. Pela diversidade dos *malwares* e cada vez mais rápida sua evolução não é uma tarefa fácil, contudo possível de ser agrupado.

Taxonomia, do Grego verbo: ασσεῖν ou tassein = "para classificar" e νόμος ou nomos = lei, ciência, administrar, cf "economia"), segundo a enciclopédia livre Wikipedia. Contudo de acordo com o Moderno Dicionário da Língua Portuguesa, Michaelis: (*táxio+nomo+ia*) 1 Estudo dos princípios gerais da classificação científica. 2 Distinção, ordenação e nomenclatura sistemáticas de grupos típicos, dentro de um campo científico.

Iniciou-se como a ciência de classificar organismos vivos (*alpha taxonomy*), contudo na evolução do tempo a palavra tornou-se num sentido mais abrangente, podendo aplicar-se a uma das duas, classificação de coisas ou aos princípios subjacentes da classificação. Quase tudo pode ser classificado de acordo com algum esquema taxonômico - objectos animados, inanimados, lugares e eventos.

O *malwares*, por sua natureza inteligente, pode ser comparado superficialmente aos serem biológicos, e sendo assim podem ser classificados em forma taxonômica.

> “Vírus de computador são pedaços de código que se enxerta em programas existentes e legítimos e subvertem as ações normais desses programas. Eles podem viajar em disquetes trocados, ou através de redes. Eles são tecnicamente distintos de *worm*s que são programas inteiros em seu próprio direito, normalmente viajando através de redes. Bastante diferentes são os “cavalos de tróia”, uma terceira categoria de programas destrutivos que não são auto-reprodutores, mas dependem de humanos para reproduzi-los por causa de seu conteúdo pornográfico ou atraente de outras formas.” Dawkins.

4.1 COMO AGRUPAR OS *MALWARES*

Segundo Goldani (2005), os *malwares* podem ser classificados de acordo com o seu *modis operandi*, maneira como é executado, como se replica e pelo que faz. A classificação não é perfeita porque estas funções freqüentemente se sobrepõem e as diferenças nem sempre são óbvias. Os dois tipos mais comuns de *malwares* são os vírus e os vermes (*worms*). Ambos têm em comum a capacidade de se auto-replicarem, ou seja, podem divulgar cópias para outros computadores ou sistemas. A diferença conceitual entre um vírus e um verme é que este último opera independente de outros arquivos ou programas, enquanto o primeiro depende de um hospedeiro para ser distribuído.

Temos também a classificação de vírus segundo Gaspar (2007), o vírus de computador, análogo ao vírus biológico, infecta o sistema, faz cópia de si mesmo e tenta se espalhar para outros computadores (organismos). Entretanto, ele precisa de uma aplicação hospedeira para se replicar e infectar outros sistemas. "..." O verme (*worm*), diferente do vírus, não precisa de um portador para se replicar. Ele se auto-replica, espalhando-se de um computador para outro e ainda pode conter vírus para infectar os sistemas. Os vermes exploram as vulnerabilidades dos serviços e utilizam quaisquer mecanismos para se propagarem.

Considerando-se como e onde os programas de um sistema infectam podemos dar a classificação de um vírus. Basicamente o vírus tem apenas duas rotinas distintas:

a) uma rotina de propagação;

A rotina de propagação procura por programas não contaminados e ao achar um, infecta-o de diversos modos.

b) uma rotina de atuação;

A rotina de atuação determina a periculosidade do vírus. Este utiliza os recursos do sistema de modo a realizar uma tarefa, que varia de alteração de arquivos, formatação de discos rígidos, roubo de informações confidenciais, alteração das configurações dos sistemas.

4.2 PROPOSTAS DE TAXONOMIA

Taxonomia é a ciência da identificação. Como já identificamos, não existe uma única classificação para as *malwares*, isso também se dá porque os *malwares* stão cada vez mais modernos e se confundem com outros tipos e adquirem caracteristicas diferentes.

Encontramos classificação de *malwares*, que os classificam como que necessitam ou não de hospedeiros, e outros a forma de se replicarem. Também temos as classificações dos vírus, que a mais encontrada foi a separação de virus, *worm* e cavalo de tróia.

Usaremos duas abordagens para classificar os códigos maliciosos.

Na primeira abordagem classificaremos o objetivo dos agentes maliciosos e na segunda abordagem os mecanismos de reprodução. Contudo os códigos maliciosos podem ter características de mais de um único tipo, como exemplo, existem programas que após infectarem um grupo de sistemas podem ser controlados remotamente.

4.2.1 Agentes Maliciosos

Na tabela a seguir, na coluna mencionamos a forma de infecção de como eles contaminam os computadores e na linha temos os tipos de *malwares*.

Forma de infecção x *Malwares*

	Virus	***Worm***	**Cavalo de Tróia**	**Spywares**	***Rootkit***	**Loggers**	**Backdoor**
Propagação via rede		X					

	Virus	*Worm*	Cavalo de Tróia	Spywares	*Rootkit*	Loggers	Backdoor
Infectar Arquivo	X						
Afeta Arquivo de Inicialização	X				X	X	X
Executável	X		X		X	X	X
Auto-Executável		X		X			
Auto-Replicável	X						
Remoto				X	X	X	X
Camuflagem	X				X	X	
Necessita Hospedeiros	X		X	X		X	X
Independente		X			X		
Monitoramento				X		X	

4.2.1.1 Agentes de Propagação Rápida

Como o próprio nome já diz é a velocidade com que os agentes se propagam na rede, normalmente causa sobrecarga nos canais de comunicação e servidores de rede, pode até paralisar as redes. O seu maior objetivo é atingir o maior número de computadores num menor espaço de tempo possível.

4.2.1.2 Agentes de Espionagem

Seu objetivo é “roubar” informações confidenciais das máquinas infectadas para repassá-las aos invasores. Essas informações também podem ser utilizadas para subsidiar outro ataque ao sistema infectado.

4.2.1.3 Agentes Controlados Remotamente

São criados canais de comunicação em que o invasor explora remotamente o sistema infectado.

4.2.1.4 Agentes de Ataque Coordenado

Inicia quando o invasor começa um ataque conjunto a um servidor ou a uma rede, onde vários sistemas foram previamente infectados, causando a indisponibilidade de um ou mais serviços.

4.2.2 Mecanismos de Reprodução

Podemos classificar em três categorias distintas:

- Vírus
- Worms
- Cavalos de Tróia

Vírus, *worm*s e cavalos de tróia são tipos de códigos maléficos da categoria *malware* (malicious software) desenvolvidos para executar ações que causam danos em um computador.

Vírus – programa (ativado pela execução de um aplicativo) criado para se espalhar e infectar computadores, danificando *software* e até mesmo *hardware* no processo.

Worm – programa (ativado pela execução de um aplicativo ou por uma vulnerabilidade do sistema) criado para se propagar em larga escala em um computador, enviando cópias de si mesmo pela rede para infectar outros computadores, por meio, por exemplo, de uma lista de *e-mail* armazenada nos programas Outlook, Eudora, etc., criando lentidão na rede e lotando o disco rígido dos computadores.

Cavalo de tróia – programa (ativado pela execução de um aplicativo) criado para parecer um presente ou algo benéfico (ex: protetor de tela), que pode até servir para a sua suposta finalidade, mas que executa operações maliciosas no sistema sem o conhecimento do usuário, como a instalação de *keyloggers* ou de *screenloggers* (para capturar dados e senhas), a instalação de um *backdoor* e a desativação do antivírus ou do *firewall* (para facilitar um ataque).

5 CONCLUSÃO

Nos dias atuais existe diversos e diferentes tipos de *malwares* e este número aumenta a cada dia. As pessoas com intenção de criarem esses códigos maliciosos se utilizam de métodos avançados para programar.

Apesar de toda a evolução não existe uma única ferramenta de solução para prevenção de vírus que se adapte a todos os estilos e ambientes computacionais.

Não é fácil trabalhar em sistemas de proteção e recuperação de infecções de vírus, pois eles estão cada vez mais rápidos e modernos e se propagam numa velocidade assustadora, contudo se feita correta e sistematicamente é possível programar e manter.

O problema com infecção de vírus é real e a cada dia mais preocupa ao longo do tempo. Contudo uma das principais vulnerabilidades são os usuários despreparados, quem são as vítimas dos *malwares* (vírus, cavalo de tróia, *spywares, worms, loggers, rootkits*, etc).

Por haver vários tipos de *malwares* e eles se camuflarem fica difícil sua classificação. Em alguns momentos encontramos classificação de *malwares* e em outros as classificações são de vírus.

Atualmente existem vários tipos de antivírus, que “prometem” soluções, contudo nem toda solução é totalmente confiável, tanto pela inexperiência dos usuários, quanto pela evolução dos *malwares*.

Os códigos maliciosos representam grande ameaça a integridade, confidencialidade e disponibilidade da informação. As pesquisas estão cada vez mais constantes e as ferramentas de desenvolvimento e técnicas de segurança específicas são criadas para detecção e contenção dos mesmos.

O que se pode concluir sobre o assunto dos métodos de ataque com suas respectivas formas de infiltrações é que, para se produzir um sistema seguro deve-se projetar os componentes do sistema (por exemplo, os diretórios) assumindo-se que as outras partes (pessoas ou programas) não são confiáveis devido a variações de comportamento.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AZEVEDO, Marcos Alves Trindade**, monografia destinada a avaliação na disciplina Projeto Final de Curso do Departamento de Ciência da Computação da Universidade Católica de Goiás**, novembro de 2006. disponível em: <http://saltador.uspnet.usp.br/pub/psylinux/psylinux/DocumentaoInicial/Documentacao.pdf>. Acessado em 05 de agosto 2008.

Atílio, C.E. et. al... **Análise Dinâmica de Código Malicioso Baseado em Sistemas Windows: Conceitos e Procedimentos**. 2003. Disponível em: http://www.acmesecurity.org/publicacoes/artigos/acme-artigo-i2ts-2003-analisedin.pdf. Acessado em 04 de novembro 2008

Andrade, Thiago. **Perícia Forense Computacional Baseada em Sistema Operacional Windows.** 2005. Disponível em: http://www.batori.com.br/downloads/trabalhosacademicos/periciaforensecomputacional.pdf. Acessado em 03 de novembro 2008

Dawkins, Richard. **Os Vírus da Mente**. Disponível em: <HTTP://ateus.net/artigos/psicologica/os_virus_da_mente.php> Acessado em 28 de agosto 2008.

Dr Herman. **v i r t u a l i s**, 1998. Disponível em: <http://www.etext.org/Zines/ASCII/Virtualis/virt002.txt> Acessado em 02 de setembro 2008.

Dvorak, John C.; Pirillo, Chris; Taylor, Wendy. **Online! The Book. Because the internet does not come with a manual**. Ed. Prentice Hall. 2004, ISBN 0131423630, 9780131423633.

Faneli, André et. al... **OPENVPN: Implementação de VPN Através de SSL em Ambiente de Sortware Livre**. 2007. Disponível em: http://www.multicast.com.br/sergio/arquivos/monografia-pos-seguranca-openvpn-com-ssl-no-linux.pdf. Acessado em 14 de novembro 2008

Gaspar, Philipe. **Pragas Eletrônicas: Ainda não Estamos Livres Delas**. Junho, 2007. Disponível em: < http://www.philipe.eti.br/> Acessado em 23 de setembro 2008.

Gaspar, Philipe. **Pragas Eletrônicas: Ainda não Estamos Livres Delas**. Julho de 2007. Disponível em: <http://www.philipe.eti.br/artigo-003.pdf> Acesso em 12 de agosto de 2008.

Goldani, Carlos Alberto. ***Malware*. Unicert Brasil Certificadora**. Abril de 2005. Disponível em: <https://www.unicert.com.br/arquivos/sobre_conteudos/UBC%20722%20-%20*Malware*.pdf> Acesso em 12 de agosto 2008.

Ghonaimy, M. Adeeb; El-Hadidi, Mahmoud T.; Aslan, Heba K. **Security In The Information Society: Visions and Perspectives**. Ed. Kluwer Academic, 2002, pag. 172 , ISBN 1402070306, 9781402070303.

Guia Definitivo para Detecção, Eliminação e Proteção contra *Malwares*. 28/08/04. Disponível em: <http://www.baboo.com.br/*malware*/> Acessado em 12 de agosto 2008.

Gonçalves, Júlio César. **O Gerenciamento da Informação e seu Segurança contra Ataques de Vírus de Computador Recebidos por Meio de Correio Eletrônico**. 2002. Disponível em: http://www.unitau.br/cursos/pos-graduacao/mestrado/gestao-e-desenvolvimento-regional/dissertacoes/dissertacoes-2002-1/goncalves_julio_cesar.pdf Acessado em 12 de novembro 2008

Harrington, Jan. **Types of *Malware* Based on Propagation Methods, Network Security a Pratical Appoch**. 2005, pag 185, ISBN 0123116333, 9780123116338

Kanellis, Panagiotis; Kiountouzis, Evangelos; Kolokotronics, Nicholas; Martakos, Draukolis. **Digital Crime and Forensic Science in Cyberspace**. 2006, P.35, ISBN 1591408725, 9781591408727.

Kaspersky Lab. **Polymorphic Viruses**. Disponível em: <http://www.viruslist.com/eng/viruslistbooks.html?id=50> Acessado em 06 de agosto 2008.

Machado, Carlos. **Vírus I Love You faz dois anos esta semana**, 2002. Disponível em <http://info.abril.com.br/aberto/infonews/042002/30042002-18.shl> Acessado em 03 de setembro 2008.

Machado, Carlos**. Vírus Sobig.F também traz programa-espião,** 2003. Disponível em < http://info.abril.com.br/aberto/infonews/082003/22082003-11.shl> Acessado em 15 de setembro 2008.

M.ª Miguet, Jesús & Tim Read. **Informática Fundamental (2a ED).** 2008, p.205, ISBN 848004828X, 9788480048286.

Medeiros, Carlos. **Segurança da Informação – Implementação de medidas e Ferramentas de Segurança da Informação**. 2001. Disponível em: http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf. Acessado em 12 de novembro 2008

Microsoft, **Microsoft Security – Slammer** <http://www.microsoft.com/brasil/security/boletim_slammer.mspx**>** Acessado em 04 de setembro 2008.

Microsoft, **Spam, Vírus, *Worm*s e Trojans atacam telemóveis**, 2005, Disponível em <http://www.microsoft.com/portugal/seguranca/bcp/newsletter_fev_2005.mspx> acessado em 13 de setembro 2008.

Moir, Robert. **Definindo Softwares Mal Intencionados (*Malwares*)**. Outubro de 2003. Disponível em: <http://www.technetbrasil.com.br/Artigos/Seguranca/SoftMalIntenc.aspx.> Acessado em 11 de agosto 2008.

Murilo, Nelson et. al... **Sistema de Detecção de Backdoors e Canais Dissimulados,** 2007. Disponível em: http://www.gray-world.net/cn/papers/sistema_deteccao.pdf. Acessado em 20 de novembro 2008

Murilo, Nelson et. al... **Métodos para Detecção Local de Rootkits e Módulos de Kernel Maliciosos em Sistemas Unix,** 2001. Disponível em: https://www.spenneberg.com/papers/chk*rootkit*-ssi2001.pdf. Acessado em 12 de novembro 2008

McKlein, Greg. **Tipos Diferentes de Acesso Backdoor**. Disponível em http://e-articles.info/t/i/1868/l/pt/. Acessado em novembro 2008

Network Associates Inc. **Brain Vírus**. Disponível em: <http://hq.mcafeeasap.com/dispVirus.asp?virus_k=221> Acessado em 25 de agosto 2008.

Neto, Mário et. al... **Crimes na Internet: elementos para uma reflexão sobre a ética informacional.** 2003. Disponível em: http://www2.cjf.jus.br/ojs2/index.php/cej/article/view/523/704. Acessado em 03 de novembro 2008

O Que São os *Malware*? Perguntas Mais Comuns Sobre *Malware*. Disponível em: <http://www.pypbr.com/infovir/*malware*.asp> Acessado em 10 de agosto 2008.

O'Connor, Tom. **Virus and *Malware* Prevention**. Disponível em: <http://faculty.ncwc.edu/toconnor/426/426lect16.htm> Acessado em 25 de agosto 2008.

Pioner, Pedro et. al... ***Malwares*: Estudo e compreensão de Mecanismos de ataques e defesas em diversos tipos de códigos maliciosos**. Disponível em: http://www.exatec.unisinos.br/~glaucol/arquivos/artigo_malware.pdf. Acessado em novembro 2008.

Reportagem da revista info. **Primeiro vírus digital completa 25 anos**. Segunda-feira, 16 de julho de 2007 - 16h57 Disponível em: <http://info.abril.com.br/aberto/infonews/072007/16072007-15.shl>. Acessado em 10 de agosto 2008.

Schmidt, Charles et. al.. **The History of *Worm* Like Programs,** 2001. Disponível em: <http://www.snowplow.org/tom/*worm*/history.html>. Acessado em 13 agosto 2008.

Schmidt, Charles et. al.. **The What, Why, and How of The 1988 Internet *Worm***, 2001. Disponível em: <http://www.snowplow.org/tom/*worm*/*worm*.html> Acessado em 31 agosto 2008.

Symantec, **W64.Rugrat.3344**, 2004. Disponivel em <http://www.symantec.com/pt/br/security_response/writeup.jsp?docid=2004-052617-2620-99&tabid=1 > acessado em semtebro 2008.

Symantec, ***Malware***. Disponível em: <http://www.symantec.com/pt/br/norton/security_response/*malware*.jsp>. Acessado em 21 agosto 2008.

Sophos. **Computer Vírus Demeystified**. Disponível em: http://www.securitytechnet.com/resource/rsc-center/vendor-wp/sopho/demy_wen.pdf. Acessado 18 em agosto 2008.

Santolim, César. **Os Princípios de Proteção do Consumidor e o Comércio Eletrônico no Direito Brasileiro.** 2004. Disponível em: http://www.lume.ufrgs.br/bitstream/handle/10183/12684/000398647.pdf?sequence=1. Acessado em 15 novembro 2008

Tourinho, Juliana et. al... **Crimes Informáticos,** 2006. Disponível em: http://www.frb.br/ciente/2006.1/ADM/ADM.TOURINHO.F2.pdf. Acessado em 03 de novembro 2008

Virus Scan Software. **The History of Computer Viruses**. Disponível em: <http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml>. Acessado em 24 agosto 2008.

Vomicae, **História: A Evolução do Vírus e Antivírus de Computador**, 2008. Disponível em http://vomicae.net/programas/historia-a-evolucao-do-virus-e-antivirus-de-computador/. Acessado em agosto de 2008.

Zeltser, Lenny. ***Malware*: Fighting Malicious Code**. 2003, p.16, ISBN 0131014056, 9780131014053.

Zeltser, Lenny. **The evolution of malicious agents**. Disponível em: <http://www.zeltser.com/agents>. Acessado em agosto 2008.

Symantec, **Ficha Técnica,** Disponivel em <http://www.symantec.com> acessado em semtebro 2008.

Sophos, **Ficha Técnica,** Disponivel em <http://www.sophos.com/> acessado em semtebro 2008.

McAfee, **Ficha Técnica,** Disponivel em <http://vil.nai.com/ > acessado em semtebro 2008.

Kaspersky, **Ficha Técnica,** Disponivel em < http://www.viruslist.com > acessado em semtebro 2008.

AVG, **Ficha Técnica,** Disponivel em < http://www.avg.com/virbase > acessado em semtebro 2008.

Trend Micro, **Ficha Técnica,** Disponivel em < http://www.trendmicro.com/vinfo/virusencyclo > acessado em semtebro 2008.