

FACULDADE SENAC DE CIÊNCIAS EXATAS E
TECNOLOGIA

João Pedro da Silva

Evolução das Pragas Virtuais

São Paulo
2005

João Pedro da Silva

Evolução das Pragas Virtuais

Trabalho de conclusão de curso
apresentado ao Centro Universitário
Senac como exigência para
obtenção da Pós Graduação em
Segurança de Redes e Sistemas

Orientador Prof. Marcelo Lau

São Paulo
2005

Aluno: João Pedro da Silva
Título: Evolução das Pragas Virtuais

A banca examinadora dos Trabalhos de Conclusão em
sessão pública realizada em _____, considerou o(a)
candidato(a):

() aprovado () reprovado

1) Examinador(a) _____

2) Examinador(a) _____

3) Presidente _____

RESUMO

O presente trabalho, intitulado "Evolução das Pragas Virtuais" propicia o estudo do vírus de computador, comparando diferentes ameaças, utilizando como parâmetros a abrangência e impacto dos ambientes e aspectos de funcionalidade e atuação de características dos vírus que comprometem os dados (malware). Verificamos o histórico do desenvolvimento do vírus de computador, bem como o uso de antivírus e procedimentos para poder eliminar o código que propicia o mau funcionamento do equipamento. Os vírus de computador são criados para efeitos de invasão para obter informações que tornarão possíveis a obtenção de lucros de forma indevida, mas também são feitos por adolescentes que utilizam programas que criam vírus somente para mostrarem que são capazes para amigos. Todo o processo da criação do vírus até a inoculação nos computadores e permitir a coleta de dados, só torna mais acirrado o mundo do comércio de antivírus que movimenta dezenas de empresas em busca de soluções para as empresas e para os usuários comuns.

Palavras-chave: vírus, antivírus, virtual, pragas.

ABSTRACT

The present work, entitled " Evolution of the Virtual Plagues " propitiates the study of the computer virus, comparing different menaces, using as parameters the inclusion and impact of the atmospheres and functionality aspects and performance of characteristics of the viruses that commit the data (malware). We verified the historical of the development of the computer virus, as well as the antivirus use and procedures to eliminate the code that propitiates the bad operation of the equipment. The computer viruses are created for invasion effects to obtain information that will turn possible the obtaining of profits in an improper way, but they are also done by adolescents that use programs that only create virus for they show that are capable for friends. The whole process of the creation of the virus to the inoculation in the computers and to allow the collection of data, it only turns more intransigent the world of the antivirus trade that moves dozens of companies in search of solutions for the companies and for the common users.

Keywords: virus, antivirus, virtual,plagues.

SUMÁRIO

1. INTRODUÇÃO	8
2. OBJETIVO	8
3. DESENVOLVIMENTO	9
3.1 Vírus	9
3.2 Malware	10
3.2.1 Vermes(worms)	10
3.2.2 Cavalo de Tróia	10
3.3 Os Primeiros Vírus de computador com impacto ao negócio	11
3.3.1 Israelense ou Sexta-Feira 13	11
3.3.2 Lehigh	13
3.3.3 Ping-pong	14
3.3.4 Brain Paquistanês	14
3.3.5 Alameda	16
3.3.6 Vírus 1704	17
3.4 As primeiras Pragas Virtuais	19
3.4.1 CHI ou Chernobyl	19
3.4.2 Melissa	20
3.4.3 Love Letter	21
3.4.4 Code Red	21
3.4.5 Nimda	22
3.4.6 Bugbear	24
3.4.7 Blaster	25
3.4.8 My Doom	26
3.4.9.NetSky	27
3.5 Quadro evolutivo,comparativo de infecção e abrangência	28
3.6 Fatores de Contribuição para evolução e disseminação	30

3.6.1 Internet, e-mail e redes P2P(peer-to-peer)	30
3.6.2 Engenharia Social	31
3.6.3 As Vulnerabilidades dos Sistemas operacionais e produtos	34
3.7 Pragas relacionadas ao furto de informações	36
3.7.1 SpyWare	36
3.7.2 Keylogger	37
3.8 Proteção contra os vírus	37
3.8.1 Antivírus	37
3.8.2 Como agem os antivírus	38
3.8.3 Prevenção	41
3.8.4 Detecção	41
3.8.5 Recuperação	42
3.8.6 Exclusão	42
3.9 O perfil dos criadores de vírus	43
4.0 Ameaças do futuro	45
5.0 CONCLUSÃO	46
REFERÊNCIAS BIBLIOGRÁFICAS	49
GLOSSÁRIO	51

1. INTRODUÇÃO

A evolução das Pragas Virtuais que compreende desde os primeiros vírus relativamente simples surgidos nos anos 80 até os dias de hoje com os chamados *malware*(software mal intencionado) temos uma enorme variedade de ameaças as organizações de todos os portes causando em alguns casos grande impacto ao negócio.

A relativa facilidade de propagação que temos hoje com rede mundial de computadores (Internet) a utilização de e-mail, redes de compartilhamento de arquivos P2P(peer-to-peer) e as falhas de segurança dos produtos e sistemas operacionais ajudam em muito a esta propagação atingir escalas mundiais em questão de horas.

2. OBJETIVO

Esta monografia tem objetivo de mostrar como os primeiros vírus surgidos nos anos 80 se propagavam e o grau destruição que causavam as empresas, seguindo uma evolução até os dias atuais com os *malware*(software mal intencionado).

Comparando diferentes ameaças, utilizando como parâmetros a abrangência e impacto dos ambientes, aspectos de funcionalidade e atuação dos vírus que comprometem os dados e redes.

3. DESENVOLVIMENTO

3.1 Vírus

Os vírus são pequenos segmentos de códigos, programados com o intuito de provocar algum sintoma indesejável ao usuário do computador infectado. Possuem a característica de se agregarem ao código de outros programas e, ao serem executados inocentemente pelo usuário, trazem em seu bojo, o código alterado para causar intromissões indevidas no processamento normal, causando ou não, danos de leves a irreparáveis. (Cidale, 1990)

O código do vírus funciona como uma função de programa que se apodera de áreas importantes de comando do sistema, de onde podem transferir réplicas de seus códigos a outros arquivos já presentes na memória ativa e a arquivos que estejam armazenados nos discos rígidos e disquetes, além de áreas de controle destes meios contaminando-os. (Cidale, 1990)

Esta capacidade de se multiplicar pela contaminação através de arquivos transmitidos por disquetes, cds entre usuários e pela facilidade de quebrar fronteiras através dos e-mails, levou a similaridade e comparação com os vírus biológicos que infectam, por auto-reprodução, diversos órgãos do corpo humano. (Cidale, 1990)

3.2 Malware

O termo *malware*, é uma abreviatura da expressão “malicious software” (software mal-intencionado), pode ser usado como um substantivo coletivo para se referir a vírus, vermes e cavalos de tróia que executam deliberadamente ações mal intencionadas em um sistema de computador. [5]

3.2.1 Vermes

Verme usa um código mal intencionado e auto propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede, um verme pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local podendo causar um ataque de negação de serviço ou seja indisponibilidade.[5]

3.2.2 Cavalo de Tróia

Programa que parece útil ou inofensivo, mas contem códigos ocultos desenvolvidos para explorar ou danificar o sistema o qual é executado, os Cavalos de Tróia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a finalidade e função do programa.[5]

3.3 Os Primeiros Vírus de computador com impacto ao negócio

A importância dos vírus que serão descritos a seguir, se dá devido à repercussão que tiveram no período em que foram criados bem como os danos que causaram para usuários comuns e empresas.

3.3.1 Israelense ou Sexta-Feira 13

A troca de disquetes foi o principal canal na rápida propagação do vírus Israelense, Esse vírus, uma obra de arte de programação, foi descoberto em 1987 na Universidade Hebraica, em Israel. Esse fato demonstrou o potencial do vírus digital como uma arma de terrorismo e protesto político. O criador do vírus poderia ter destruído milhares de arquivos, representando anos de trabalho de professores, estudantes e administradores. Sob a mira do vírus estavam descobertas científicas, registros financeiros, listas de estudantes e outros importantes tipos de dados normalmente encontrados em universidades e rotineiramente confiados aos computadores para guardá-los. O vírus contaminou sistemas IBM e compatíveis em muitas outras instituições israelenses. Caso não fosse descoberto, provavelmente teria entrado nos sistemas de defesa de Israel, que contêm informações secretas e de segurança nacional. Felizmente, os primeiros efeitos da contaminação foram descobertos em tempo e medidas foram tomadas, graças a alguns erros de programação cometidos pelo autor do vírus. (Cidale, 1990)

O objetivo do autor do vírus era destruir o maior número de arquivos possível no dia 13 de maio de 1988, uma sexta-feira, data comemorativa dos 40

anos do fim do Estado Palestino. Mas o autor cometeu erros que fizeram com que o vírus fosse identificado antes que pudesse causar qualquer dano aos sistemas. (Cidale, 1990)

O vírus Israelense, programado para contaminar arquivos com extensões COM e EXE, deveria encontrar tais arquivos e verificar se já não tinham sido contaminados antes de contaminá-los. A verificação não funcionou, e a contaminação foi repetida várias vezes em alguns arquivos EXE, aumentando seu tamanho em 1800 bytes a cada repetição. Os arquivos cresceram de tal forma que a memória dos computadores já não podia contê-los. A lentidão na execução dos programas e a perda do desempenho alertou os usuários antes de a destruição se efetivar. Os engenheiros de software israelenses conseguiram encontrar o vírus e tomar medidas, impedindo que ele fosse ativado e causasse danos em massa no dia 13 de maio — a data da ativação. (Cidale, 1990)

Os engenheiros da universidade rastrearam o vírus até o compilador de assembler do sistema. A operação de resgate do sistema mostrou o quão valiosa pode ser a detecção antecipada da contaminação. Os programadores da universidade criaram em poucas horas softwares programados para localizar os sistemas contaminados e administrar um antídoto. (Cidale, 1990)

A data de ativação do vírus e outras evidências deixaram claro que o motivo da sabotagem foi político. Esse episódio marcou a criação de uma nova e perigosa invenção no campo da informática, capaz de ameaçar sistemas militares e industriais. (Cidale, 1990)

3.3.2 Lehigh

O vírus é ativado depois de quatro contaminações. Como outros vírus de vida curta, a probabilidade de ser detectado antes de destruir arquivos é muito pequena. Felizmente, o *Lehigh* é de contaminação vagarosa, pois seu curto período de vida não lhe permite contaminar um grande número de arquivos e disquetes antes de ser ativado. (Barrett, 1993)

O nome *Lehigh* tem sua origem na primeira contaminação registrada na Universidade de *Lehigh*, Estado da Pensilvânia, Estados Unidos em 1987. O vírus contaminou um grande número de PCs de professores e alunos da universidade, causando a destruição em massa de importantes informações e interrompendo o curso normal de suas atividades. O vírus *Lehigh* contamina o arquivo processador de comandos do DOS – COMMAND.COM – e usa os comandos normais do DOS para se reproduzir. A contaminação atingiu todos os disquetes de sistema (disquetes contendo os arquivos de sistema e usados para dar o *boot*) e diretórios de sistema em discos rígidos. Depois que um arquivo COMMAND.COM é infectado, ele contamina outros quatro discos, assim, todos os dados do sistema eram destruídos. (Barrett, 1993)

O vírus contamina o sistema colocando-se dentro do arquivo Command.com, escondendo-se em uma área denominada *program stack*. A única indicação de contaminação antes da destruição de dados é a mudança de data e hora de criação do arquivo COMMAND.COM. Como a maioria dos usuários não se lembra da data de criação original, a detecção do vírus antes da ativação é rara. (Barrett, 1993)

Entretanto, se o vírus for descoberto a tempo, a descontaminação é simples. Apenas o arquivo COMMAND.COM é contaminado, portanto, tudo o que se tem a fazer é apagar o arquivo e fazer uma nova cópia do disquete original do sistema operacional DOS para o disco. Se o vírus não for descoberto a tempo, ele se autodestrói juntamente com o resto dos arquivos quando for ativado. (Barrett, 1993)

3.3.3 Ping-pong

Esse vírus surgiu em 1988, e é um dos mais criativos no mercado. Uma bolinha aparece na tela e começa a pular de um lado para o outro, tornando a operação do PC quase impossível. O *Ping-Pong* se esconde na área de inicialização do sistema operacional (área de *boot*). Os programas antivírus que não verificam essa localização remota do disco rígido não conseguem detectá-lo. *Ping-Pong* é executado diretamente de um endereço especial na memória chamado ROM-BIOS, fazendo com que não precise ficar residente e exposto na memória RAM. O *Ping-Pong* não destrói arquivos. (Pitkowski, 1992)

3.3.4 Brain Paquistânês

Esse vírus, que se aloja na área ou segmento de boot do disco, foi identificado pela primeira vez em 1986. Os primeiros sintomas incluem uma atividade excessiva dos drives de disquetes quando estes não deveriam estar sendo endereçados. (Barrett, 1993)

O *Brain Paquistânês* foi um problema para milhares de usuários em dezenas

de países esse vírus, entretanto, teve um efeito positivo no tocante à pirataria de software. Produtores de software perdem bilhões de dólares todos os anos em cópias piratas. O advento do vírus fez com que os usuários pensassem duas vezes antes de obter um software de forma ilegal. O software pirata é hoje a causa número um da contaminação de sistemas por vírus digitais. (Barrett, 1993)

O vírus Paquistanês originou-se nos disquetes piratas vendidos pelos irmãos *Amjad Farooq Alvi* e *Basit Farooq Alvi* em sua loja - *Brain Computer Services* - na cidade de *Lahore* no Paquistão. Os *Alvi* ganharam muito dinheiro durante anos vendendo cópias ilegais de softwares americanos famosos, como o processador de textos *WordStar* e a planilha eletrônica *Lotus 1-2-3*. Esses softwares eram vendidos por menos de 1 % dos preços originais. *Amjad* é um programador brilhante, formado pela Universidade de Punjab, e era um consultor bem-sucedido antes de adquirir a loja. Ironicamente, depois que seus próprios programas foram pirateados por clientes, *Amjad* criou o vírus Paquistanês contra a pirataria, como forma de vingança. Quando *Amjad* e *Basit* se tornaram piratas, começaram a infectar os disquetes piratas que vendiam para turistas estrangeiros e particularmente para os americanos. (Barrett, 1993)

O vírus Paquistanês foi levado para muitos países, especialmente para os Estados Unidos, e contaminaram todos os sistemas pertencentes aos clientes do software pirata. Os compradores do software contaminado distribuíram cópias à vontade, e uma verdadeira corrente de contaminação foi criada. Não demorou muito e o vírus foi inadvertidamente distribuído para todo o resto do mundo, via disquetes mandados pelo correio. O vírus chegou até a contaminar um serviço de vacinas criado pelos próprios autores do vírus nos *Estados Unidos*. (Barrett, 1993)

Mesmo os poucos vírus que têm uma identificação visível passam

desapercebidos na maioria das vezes, até que tenham a oportunidade de causar sérios danos ao sistema. Uma contaminação do vírus *Brain* destruiu os dados de 300 computadores no *Providence Journal* no Estado de *Rhode Island*, no leste dos *Estados Unidos*. Ninguém tinha notado a presença do vírus até que alguns dos computadores começaram a ter seus dados destruídos. Um engenheiro de software estudou o problema por várias horas tentando desvendar o que estava acontecendo. O fenômeno do vírus digital era então desconhecido. O ousado vírus chegou a mudar o nome do disco (*Volume Label*) para (c) *Brain*, apostando no fato de que a maioria dos usuários não lê o nome do disco e diretórios mesmo quando mostrados na tela. (Barrett, 1993)

Este foi o primeiro exemplo de como os jornais, revistas, telégrafos e outros meios de comunicação estão vulneráveis aos vírus digitais. O vírus Paquistânês contaminou todos os departamentos do jornal e foi encontrado também nas casas dos funcionários, escritórios de correspondentes e colaboradores, e até no escritório de contabilidade que fazia as contas da empresa. (Barrett, 1993)

O vírus Paquistânês é um dos mais complexos vírus já criados. O software possui estruturas internas para evitar que seja identificado, destruído ou danificado. O vírus efetua seu objetivo principal, reproduzir-se, de maneira efetiva e impressionante. (Barrett, 1993)

3.3.5 Alameda

Esse é um vírus que também se instala na *área de boot* do disco, e de certa maneira é similar ao vírus *Brain* Paquistânês. Entretanto, esse vírus tem uma fraqueza: guarda as informações da *área de boot* original durante a contaminação,

mas não as protege contra a gravação de novos dados. À medida que o disco é usado, o setor de boot original pode ser coberto por novas gravações, assim o vírus será destruído. O vírus Alameda pode contaminar apenas disquetes na hora do boot. Esse vírus, detectado pela primeira vez na faculdade *Alameda College* em maio de 1988, é responsável por um percentual significativo de contaminações. (Barrett, 1993)

3.3.6 Vírus 1704

Esse vírus também é conhecido como *Blackjack* em algumas partes da Europa. O nome vem do fato de que todos os programas infectados são acrescidos em seu tamanho de 1704 bytes. Na Alemanha, o jogo de cartas *Blackjack* é conhecido como "17+4", daí o apelido europeu do vírus. (Barrett, 1993)

O 1704 é um vírus diferente dos outros que contaminam os PCs. Tem duas características singulares:

Com Criptografia se codifica para evitar detecção e dificultar análises. A técnica de criptografia usada pelo vírus é muito interessante, pois seu resultado muda a cada arquivo que é infectado. Esse fato complica ainda mais as tentativas de se desenvolver programas de recuperação de arquivos contaminados.

Está ativo apenas durante os meses de outubro, novembro e dezembro.

O 1704 é similar ao Israelense em vários aspectos. Um programa residente é responsável pela contaminação de programas quando estes são executados. Pode contaminar programas em discos rígidos e disquetes e muda o tamanho e o CRC dos arquivos sem mudar a data e hora de criação. O 1704 contamina apenas arquivos EXE. Este é um dos poucos vírus que podem infectar arquivos escondidos

(*hidden*) e arquivos protegidos contra gravação (*read-only*). O 1704 tentará contaminar até os arquivos em disquetes protegidos contra gravações. A tentativa de contaminação será executada cinco vezes, e este é o único sintoma que pode alertar a vítima da presença do vírus. As tentativas de gravar em um disquete protegido contra gravação fará com que o sistema operacional apresente mensagens e avisos.

O aspecto mais peculiar do 1704 é o jeito pelo qual é ativado. Como dissemos, o vírus entra em ação apenas durante os meses de outubro, novembro e dezembro. Durante o resto do ano, o vírus apenas se reproduz sem qualquer efeito sobre o sistema contaminado. Outro aspecto curioso é que o vírus somente será ativado se determinados tipos de monitores de vídeo estiverem sendo usados pelo sistema. Sistemas usando vídeos monocromáticos e sem capacidade de apresentar gráficos não serão afetados.

Os sinais visuais do vírus são inconfundíveis. Primeiro uma letra, depois outra se deslocará do resto dos caracteres na tela. Um por um, os caracteres começarão a flutuar, como folhas caindo de uma árvore, até o fundo da tela, onde permanecerão amontoados. Depois de algum tempo, a tela ficará totalmente incompreensível, e o sistema terá de ser desligado e ligado novamente. .

O vírus 1704 original apenas perturbava a tela. Outras versões, entretanto, também destroem programas e arquivos de dados. Uma das versões chega ao ponto de formatar o disco rígido no dia primeiro de dezembro.

A versão mais notável do vírus 1704 foi identificada pela primeira vez na Inglaterra em janeiro de 1989. (Barrett, 1993)

3.4 As primeiras Pragas Virtuais

Antes da internet e o e-mail serem adotados como principal meio de comunicação pelo mundo, os vírus eram espalhados principalmente através de discos removíveis, disquetes, CDs etc, que continham arquivos já infectados ou um executável do código do vírus em um setor de boot, onde a contaminação era lenta.

Com a internet e o e-mail como aliados destas pragas virtuais a disseminação e contaminação se dá em questão de horas, a seguir vou comentar algumas das principais pragas.

3.4.1 Vírus CHI ou Chernobyl

Escrito na Ásia, apareceu pela 1ª vez em junho de 1998, os vírus CIH atacam arquivos do Windows 95 que estão no formato PE (PortableExecutable). O vírus ataca de forma a cada dia 26 (versão 1019) nessas datas o vírus CIH tenta sobrescrever o conteúdo da BIOS (do tipo Flash-BIOS) se a BIOS está configurada para aceitar que se sobrescreva que é o caso da maioria das modernas placas mães o ataque do vírus torna a máquina inoperante, já que não mais se consegue dar Boot .[10]

O vírus CIH sobrescreve porções do disco rígido com sujeira no caso das versões 1003 e 1010 o ataque só ocorre no dia 26 de abril.

Este vírus é um clássico tipo de código malicioso destrutivo com período de incubação, o vírus não afeta visivelmente os computadores, se espalha apenas de um sistema para outro, esperando a data de ativação, onde este período é chamado

de “período de incubação”. [10]

3.4.2 Virus Melissa

O vírus W97/Melissa é um vírus de macro que iniciou sua propagação no dia 25 de março de 1999, o primeiro a atingir escala mundial, atacando diversos micros através da Internet como um arquivo.doc anexado ao e-mail. [6]

Pela sua ação, de enviar 50 cópias de si mesmo pelo e-mail de cada usuário infectado em poucas horas acabou causando problemas em servidores de e-mail, que caíram por excesso de tráfego.

Esse vírus, embora disseminado primordialmente pela Internet, só contamina o Word 97, ou Word 2.000, pela ação do usuário que ao receber um e-mail que contem como subject: "Mensagem Importante de " onde é o nome completo do usuário que foi contaminado acaba lendo-o sem passar antes anti-vírus, por achar que a mensagem provem de fonte confiável

O vírus W97/Melissa contamina o modelo global Normal.DOT, desta forma contaminando outros arquivos que forem criados após a contaminação original, e permitindo mais uma rota de contaminação para outros usuários, mesmo que não usando e-mail.[6]

Com o surgimento do Melissa, o impacto econômico dos vírus se tornou uma grande preocupação, como resultado, usuários e empresas começaram a se preocupar seriamente com as conseqüências que um ataque de vírus poderia ocasionar para a segurança de seus sistemas e computadores.

Essa foi a forma dos usuários descobrirem os programas de antivírus, que começaram a ser instalados de forma massiva.

3.4.3 Vírus Love Letter

Love Letter descoberto em abril de 2000 originado nas Filipinas conforme descrito no site da Mcafee se propaga por e-mail, através do MS Outlook.

O vírus recebido através de e-mail contem um arquivo com extensão.VBS (script visual basic) ao executar o anexo o vírus faz uma cópia de si mesmo na pasta de sistema e a envia para todos os endereços do livro de endereços do Outlook.[10]

Utiliza uma técnica chamada "*double extension*" (extensão dupla). A extensão dupla faz com que um anexo pareça ser inocente, escondendo a extensão original do arquivo para o usuário, o arquivo sonho.jpg se tornaria sonho.jpg.vbs e seu conteúdo seria uma cópia do script do vírus.[10]

Este Vírus na época foi considerado a pior praga de todos os tempos por seu poder e velocidade de disseminação conforme fonte ICISA (International Computer Security Association), organização independente ligada a segurança de computadores, onde em apenas um dia já havia atingido escala mundial, infectando aproximadamente 1 milhão de computadores.

3.4.4 Code Red

O Code Red surgiu em julho de 2001 origem desconhecida, fonte Mcafee, onde explora vulnerabilidade (falha de segurança) dos sistemas Windows NT 4.0 com o serviço IIS(Internet Information Server) 4.0 e 5.0 bem como o Windows com 2000 com IIS 4.0 e 5.0 , o Vírus se propaga utilizando o servidor infectado para fazer

uma conexão TCP (Protocolo de Controle de Transmissão) na porta 80, que é a porta padrão de sites na Internet, rastreamento outros servidores com a mesma falha e infectando.[10]

O vírus, desfigura sites hospedados nestes servidores, deixando uma página com o título de "HELLO!" e a seguinte mensagem: "Welcome to <http://www.worm.com> ! Hacked By Chinese.

O vírus conforme a CERT (Computer Emergency Response Team), infectou 250 mil servidores em apenas 9 horas, isto mostra o potencial de disseminação que a internet proporciona para a infecção em larga escala das pragas e também a nova vertente das pragas focadas na exploração das vulnerabilidades.

Apesar da Microsoft ter disponibilizado uma correção para falha outra variante do vírus o Code Red II, explorou outra falha mostrando para o mundo o quando os sistemas e produtos eram suscetíveis a tais ataques.

3.4.5 Nimda

O vírus Nimda conforme fonte da McAfee fornece data de surgimento da praga em setembro de 2001 e origem desconhecida, porém a Panda software nos fornece como País de origem China, a praga se propaga de três maneiras: via e-mail, através de conexões da rede, por servidores com o Internet Information Server (IIS) e também pelo Internet Explorer versão 5.01 e 5.5.

Ao se espalhar pelo correio eletrônico, ele chega com o anexo "readme.exe" e, segundo a McAfee nem é necessário que o usuário abra o anexo para que a contaminação ocorra, apenas a visualização é suficiente.[10]

De acordo com informações publicadas no site do SANS Institute, que

monitora a ação dos vírus na internet, o Nimda pode ainda infectar uma máquina apenas através da visitação de páginas web contaminadas. Durante o processo, códigos JavaScript tentam efetuar o download da praga para o cliente em arquivo nomeado como "readme.eml".

Caso a versão do browser Internet Explorer do usuário esteja vulnerável, o vírus é automaticamente executado.[15]

Quando executado, o virus substitui uma ".dll" legítima do Windows, a Riched20.dll, e modifica o System.ini para depois se auto copiar para o diretório C:WindowsSystem com o nome de load.exe. Da mesma forma, ele se auto copia para a pasta de temporários em C:/Windows/Temp, como Mep*.tmp.exe.

Através do recurso MAPI, o Vírus pode ler endereços eletrônicos disponíveis no inbox do usuário da máquina afetada. As funções MAPI são suportadas pelos softwares Outlook e Outlook Express. Via SMTP, o vírus se auto envia como anexo, sem corpo de texto, com assuntos aleatórios e randômicos.

Servidores sem a correção de segurança do IIS são afetados porque o vírus utiliza um antigo "Unicode Web Traversal Exploit". Assim, ele se auto copia para o servidor web como Admin.dll. [15]

Este arquivo é, então, executado remotamente pelo vírus para que a máquina seja infectada.

Segundo informações da Symantec, ele procura ainda arquivos .htm, .html e asp para modificar e abre uma conexão da rede afetada, permitindo o acesso remoto aos computadores.[15]

Seguindo os passos do Code Red, o Nimda também foca sua disseminação na exploração de falhas de segurança,ou seja vulnerabilidades dos sistemas operacionais e produtos Microsoft ,começamos a ter uma tendência forte e

poderosa de destruição.

3.4.6 Bugbear

O vírus Bugbear conforme fonte Panda Software surgiu em setembro 2002, porém não consta País de origem, em outros sites pesquisados apresenta como Malásia o local de origem da praga.

Mais uma vez seguindo a tendência das últimas pragas anteriormente apresentadas este vírus, utiliza o e-mail e vulnerabilidades do Internet Explorer versões 5.01 e 5.5 SP1, para propagação e infecção.

A praga recebida por e-mail vem com anexo de 50.688 bytes escrito em Visual C++ (linguagem de programação de Microsoft), este anexo tem com dupla extensão e nomes aleatórios segue exemplos: Hello, Just a reminder, etc... [12]

Os anexos executados ou pela simples visualização do e-mail em sistemas que não corrigiram a falha de segurança conhecida como "Incorrect Mime Header", pela Microsoft em seu Security Bulletin MS01-020, no ano de 2001, devido a Praga NIMDA, automaticamente são infectados. [12]

Com esta praga damos mais um passo na evolução onde a mesma não tenta somente infectar o maior número de máquinas, mas também paralisar redes, roubar senhas, desativar sistemas de Firewall e antivírus.

Além de se espalhar por e-mail, o BugBear também se utiliza dos compartilhamentos das redes locais para espalhar seu código a todos os dispositivos.

Uma das características que davam sinais da rede estar infectada com a praga é que as impressoras da rede local começaram a imprimir sem parar mensagens sem sentido.

A praga ativa na memória da máquina infectada tenta desativar os produtos de antivírus e firewall, para posterior instalação de um cavalo de tróia, com objetivo de permitir que Hackers possam comprometer a segurança dos dados do usuário contaminado, como senhas de sistema, senhas pessoais, números de cartão de crédito, etc.... [6]

3.4.7 Blaster

O Vírus Blaster, surgiu em agosto de 2003, conforme fonte da Panda Software e não consta País de origem.

A Microsoft Technet divulgou que a praga explora uma vulnerabilidade do RPC (Remote Procedure Call) que é um protocolo usado pelo sistema operacional Windows NT, 2000, XP e 2003; o RPC fornece um mecanismo de comunicação entre processos que permite que um programa de um computador execute sem diferenças códigos em um sistema remoto. [12]

A propagação da praga é executada através do escaneamento de micros com a porta TCP 135 aberta, ao encontrar na rede máquinas com esta porta aberta o vírus tenta instalar na máquina vítima um arquivo executável de nome msblast.exe.

Esta praga conforme o site da Panda Software descreve tinha por objetivo causar um DOS (denial of Service) negação de serviço, contra do site da Microsoft de atualizações de produtos o windowsupdate.com, porém nesta tentativa de infectar o maior número de máquinas para efetuar tal a ataque, máquinas de todo mundo começaram a se auto reiniciar devido a falha na execução do RPC. [12]

3.4.8 MyDoom

A praga MyDoom, surgiu em janeiro de 2004 conforme fonte Panda Software, porém não consta País de origem.

Esta praga ao contrário da outras pragas antes descritas não tira vantagem de nenhuma nova falha ou vulnerabilidade de software, esta praga foi projetado para convencer os destinatários de um e-mail a abrir um arquivo anexo e executar os programas nele contidos, a praga chega às caixas de mensagem com um arquivo com extensão exe,.cmd,.scr,.zip,.bat ou .pif, e pode conter na linha de assunto uma de várias expressões:Status, Error, Hi, Mail Delivery System, Test, Server Report, Mail Transaction Failed ou Hello. [12]

A execução destes arquivos recebidos por e-mail por usuários nos leva a outro ponto eficaz na disseminação das pragas o tema “Engenharia Social” que será abordado mais adiante.

Outra forma de disseminação e infecção desta praga esta relacionada a utilização de programas de compartilhamento de arquivos como o KaZaA,que trafegam pela redes chamadas P2P(peer to peer), onde a praga faz copias de si mesmo dentro da pasta My Shared Folder, originária do programa KaZaA.

O objetivo da praga era causar uma negação de serviço do site da SCO empresa de software americana o que realmente conseguiu, deixando página da empresa indisponível, outro objetivo da praga era carregar cavalos de tróia possibilitando abertura de portas TCP 3127 à 3198 através do componente SHIMGAPI.DLL, permitindo que hackers possam tomar controle da máquina infectada remotamente.[12]

De acordo com a F-Secure empresa Finlandesa de segurança de computadores o Mydoom é, em termos de propagação, "o pior vírus de computador da história", em apenas um dia registrava uma taxa de infecção de 40% de todos os e-mails no mundo.

3.4.9.NetSky

O vírus Netsky ,surgiu em fevereiro de 2004 conforme fonte da Panda Software, seguindo os passos do Mydoom, surgido em janeiro do mesmo ano,usa o e-mail e as redes P2P, como principal fonte de propagação e infecção, o que mostra uma nova vertente dos autores das pragas de agora se utilizarem do descuido de despreparo dos usuários em identificar e-mail de fontes conhecidas e manterem suas máquinas atualizadas com relação a antivírus bem como a aplicação de correções de segurança da Microsoft.[12]

A praga Netsky,vem por e-mail com arquivo anexo na maioria dos casos com extensão .zip e exe , outra maneira de infecção é através da redes P2P, onde a praga se auto copia para todos os diretórios de rede compartilhados da máquina infectada.

3.5 Quadro evolutivo, comparativo de infecção e abrangência.

Ano	Vírus	Sistema Operacional Afetado	Método de propagação	Infecção	Abrangência	Evolução
1986	Brain	MS-DOS	Troca de disquetes	Setor de boot	Restrita	Considerado 1º Vírus
1987	Sexta-feira a 13	MS-DOS	Troca de disquetes	Setor de Boot	Restrita	Exclusão de arquivos
1988	Ping Pong	MS-DOS	Troca de disquetes	Setor de Boot	Restrita	Apresenta Sinais gráficos na tela uma bolinha passando
1989	1704	MS-DOS	Troca de disquetes	Setor de Boot	Restrita	Uso de Criptografia e sinais gráficos as letras caem na tela
1998	Chernobyl	Windows 95	Troca de disquetes, e arquivos via FTP, rede local	Arquivos com extensão exe	Consta infecções em todo o mundo	Formata o disco rígido e também infecta a Bios da Placa Base
1999	Melissa	Windows 95/98/NT	Arquivos recebido via e-mail, Internet, FTP	Vírus de macro infecta arquivos texto	Considerado 1º vírus a atingir escala mundial confirmada	Auto propagável se dissemina enviando copias de si mesmo
2000	Love Letter	Windows 95/98/NT/2000	Arquivos recebidos via e-mail, internet	Altera as extensões do arquivos para .VBS	Mundial	Uso de linguagem de programação Visual Basic no código
2001	Code Red	Windows NT\2000\XP	Internet	Desconfiguração de sites	Mundial	Exploração de falhas de segurança
2001	Nimda	Windows 95 ao XP	Via e-mail Internet e redes P2P	Arquivos com extensão exe	Mundial	Exploração de falhas de segurança, abertura de portas com cavalos de

Ano	Vírus	Sistema Operacional Afetado	Método de propagação	Infecção	Abrangência	Evolução
2002	Bugbear	Windows 95 ao XP	e-mail internet, redes P2P	Arquivos exe, alteração de dll	Mundial	Exploração de falhas de segurança Desativação de sistemas de firewall e antivírus
2003	Blaster	Windows 95 ao XP	e-mail internet, redes P2P	Arquivos exe, alteração de dll	Mundial	Exploração de falhas de segurança Scanearmen- to de portas TCP 135 abertas para se auto copiar
2004	My doom	Windows 95 ao XP	e-mail internet, redes P2P	Arquivos exe, alteração de dll	Mundial	Se auto copia pelas redes P2P, bem como se envia através de e-mail com endereços da maquina infectada
2004	Netsky	Windows 95 ao 2003	e-mail internet, redes P2P	Arquivos exe, alteração de dll	Mundial	Se auto copia pelas redes P2P, bem como se envia através de e-mail, apaga entrada de registro do Windows outros vírus

O período que compreende dos anos de 1990 a 1997, não foram citados mediante a não constarem referencias de vírus relevantes baseado nas fontes pesquisadas.

3.6 Fatores de Contribuição para evolução e disseminação

3.6.1 Internet,e-mail e redes P2P

A internet em conjunto com e-mail e as redes P2P (Peer to Peer) ponto a ponto se tornaram na forma mais amplamente usada de se enviar e receber informações bem como compartilhar arquivos, porém infelizmente também serve como a maneira mais rápida de espalhar vírus e outras ameaças.

Nos dias atuais ter acesso a internet é fácil através de provedores de acesso gratuito e até mesmo para quem não tem computador, pois podem se utilizar de Cyber Café, LanHouse, escolas de cursos de informática ,etc,.

Com esta facilidade do mundo inteiro estar conectado na rede, é onde as pragas e seus criadores mais evoluíram, explorando a vulnerabilidades dos sistemas operacionais e produtos que será descrito mais adiante.

Conforme fonte da Panda Software, o e-mail é a forma mais comum de espalhar um vírus ou outra ameaça, é onde quase 80 por cento das infecções se originam, devido a transmissão rápida, uma mensagem infectada pode em apenas algumas horas infectar milhares de computadores, o e-mail pode ser emitido e recebido de qualquer tipo de computador e plataforma,as pragas atuais tem capacidade de utilizar o catalogo pessoal de endereços para se reproduzir ,enviando copias de si mesmo para todos os contatos da máquina infectada.

Outro ponto de contribuição para entrada e disseminação de vírus são as redes P2P(Peer to Peer) ponto a ponto, tecnologia que possibilita a troca de arquivos em rede onde os usuários se conectam utilizando softwares como KaZaA,Shareaza, Morpheus, etc., formando como se fosse uma enorme rede local

entre os usuários.

Esta tecnologia consiste em que cada equipamento conectado as redes P2P se torne um servidor e cliente ao mesmo tempo pois abre conexões na máquina para compartilhar arquivos se tornando um servidor de arquivos, bem como um cliente ou seja buscando arquivos de outros usuários.

Com esta facilidade da troca de arquivos onde o usuário copia diretamente para sua máquina o arquivo desejado, junto pode conter as pragas virtuais, se por descuido ou mesmo por ingenuidade do usuário que não se atenta para manter seu antivírus atualizado bem como as correções de falhas de segurança dos sistemas e produtos, ele vai se tornar um alvo fácil para infecção.

As pragas como Nimda, Bugbear, Mydoom e Netsky, se utilizaram destas redes para se disseminarem, utilizando a copia de arquivos para infectar bem como o compartilhamento das máquinas conectadas a estas redes, a praga Mydoom é apontada pela Panda Software como a primeira praga a se disseminar criando copias de si mesmo através do compartilhamento de rede entre as máquinas conectadas a rede P2P.

3.6.2 Engenharia Social

A definição de Engenharia Social é descrita pelo autor Antonio Mendes da Silva Filho em artigo da revista Espaço Acadêmico de dezembro de 2004 como "...Termo utilizado para qualificar os tipos de intrusão não técnica, que coloca ênfase na interação humana e frequentemente envolve a habilidade de enganar pessoas objetivando a violação de procedimentos de segurança.

Outro autor do site SCUA, segurança e Gestão em TI, Marco Aurélio Maia,

define Engenharia Social como “...é o termo utilizado para obtenção de informações importantes de uma empresa, através de seus usuários e colaboradores. Essas informações podem ser obtidas pela ingenuidade ou confiança.....”

Como podemos ver pelas definições acima a Engenharia Social trata do elemento ser humano que dentro do ciclo de segurança que compreende hardware, software e plataforma utilizada é considerado o elemento mais vulnerável pois possui traços comportamentais e psicológicos que o torna susceptível a ataques de engenharia social, dentre destes traços podemos destacar: [16]

- Vontade de ser útil - o ser humano comumente procura agir com cortesia bem como ajudar outros quando necessário.
- Busca por novas amizades - o ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável a aberto a dar informações.
- Persuasão – compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas.

Utilizando das características acima citadas a engenharia social segue uma seqüência de passos na qual um ataque pode ocorrer:

- Desenvolvimento de relacionamento.
- Exploração de um relacionamento para coleta de dados - O hacker ou engenheiro social busca as mais diversas informações dos usuários como CPF, data de nascimento, nome dos pais, senhas, dados de conta bancária ou cartão de crédito ,etc.
- Execução do Ataque – Com base nas informações obtidas é realizado o ataque ao usuário ou empresa.

As formas de ataque da engenharia social estão presente no dia a dia das pessoas, através de telefones de supostas empresas de venda de cartão de

credito,prestadoras de serviço de telefonia, provedores de internet onde por trás da ligação pode estar uma pessoa mal intencionada realizando a coleta de dados, porem sem dúvida a forma mais perigosa e bem sucedida de ataque da engenharia social é feita pela internet e correio eletrônico o e-mail.[16]

As maiores pragas que atingiram escala mundial tiveram o e-mail como seu maior aliado devido a ingenuidade e curiosidade dos usuários; pragas como o vírus Melissa,love letter,Nimda,Mydoom usaram deste artifício para se tornarem destaque mundial, o criador do vírus pensa em uma maneira de fazer o usuário clicar no texto anexo e assim executar o vírus, a maneira mais fácil é despertar a curiosidade das pessoas utilizando temas como sexo,sorteio de brindes,noticias atuais,temas relacionados a traição, etc.

Podemos citar como exemplo clássico o vírus Love Letter onde o tema vinha com a descrição “I love You” a pessoa com a curiosidade de ter um admirador ou admiradora secreta executava o arquivo anexo causando a infecção, outro exemplo clássico é o tema da traição, mensagens com o tema “O amor da sua vida está te traindo” clique no link para ver as fotos,estes temas relacionados ao sentimento são fortes aliados para a infecção e disseminação das pragas.

Outras formas de ataque que podem ser lavadas em consideração são as mensagens que chegam com link de sites bancários onde usuário é induzido a executar o mesmo sendo direcionado para um site falso onde o objetivo é a coleta de dados,outra forma de ataque são as salas de bate papo onde pessoas mal intencionadas podem coletar dados de pessoas mais ingênuas.

Os autores aqui citados apontam para mesma solução para tentar atenuar e prevenir os ataques desta natureza, essas medidas compreendem;

- Educação e treinamento – conscientizar as pessoas sobre o valor da

informação que elas possuem e manipulam dentro da empresa, seja ela pessoal ou institucional.

- Classificação das informações da empresa, onde cada colaborador saiba o que pode ser divulgado e o que não pode.
- Estabelecer política de segurança – permitindo aos usuários permissões mínimas para execução das suas tarefas.
- Desconfiar de ofertas mirabolantes que circulam na internet.
- Ao receber telefonema de uma pessoa estranha que tenta solicitar dados pessoais tente se certificar que a ligação realmente é procedente.
- Desconfie das mensagens de correio eletrônico onde o remetente não é conhecido.

3.6.3 As vulnerabilidades dos sistemas operacionais e produtos

Vulnerabilidade é o termo usado para definir uma fraqueza ou falha de segurança de produtos e sistemas operacionais.

O vírus Code red foi uma das primeiras pragas a se utilizar de vulnerabilidades dos sistemas operacionais e produtos Microsoft para se disseminar e abrindo um precedente para todas as outras pragas que vieram depois, esta praga se utilizou da vulnerabilidade dos sistemas Windows NT 4.0 com o serviço IIS(Internet Information Server) 4.0 e 5.0 bem como o Windows com 2000 com IIS 4.0 e 5.0 , o Vírus se propaga utilizando o servidor infectado para fazer conexões TCP entre servidores com a mesma vulnerabilidade.

Os criadores das pragas perceberam o potencial da disseminação e destruição que poderiam alcançar focando seu ataques nesta fonte, a Microsoft

após a praga Code Red, começou a se preocupar mais com a correção e divulgação das falhas de segurança disponibilizando estas correções em seu site, porém a divulgação constante de novas falhas age em conjunto com a criação de novas pragas.

Após o Code Red, tivemos o Nimda,bugbear,Blaster, mydoom,netsky entre outros vírus todos explorando as vulnerabilidades dos sistemas operacionais e produtos Microsoft,onde podemos destacar entre as principais e que mais contribuíram para o sucesso destas pragas apontas pela Panda software e Cert.org. as vulnerabilidades de todos os sistema operacionais da família Windows, do 95 ao XP, Internet Explorer versões 5.01,5.5 e 6.0, o Outlook do 98 ao 2002, os serviços de IIS(internet Information Server) versões 4.0 e 5., RPC(remote procedure Cal).

Conforme série de artigos publicados pela Panda Software e traduzido pela Modulo Security Magazine “A evolução dos Vírus de Computador” [22],vem corroborar com os pontos abordados referentes aos fatores de evolução e disseminação, o artigo cita “..A Internet e o e-mail revolucionaram as comunicações. No entanto, como era de se esperar os programadores de vírus não demoraram a perceber que estas novas maneiras de comunicação também se tornariam excelentes meios para disseminação de seus códigos maliciosos.....” [22]

O artigo também destaca o uso da Engenharia social citando a praga Love Letter atuando em conjunto com a exploração de vulnerabilidades, “...Love Letter,que utilizava uma simples;mas efetiva artimanha,que seria considerada como um novo tipo de engenharia social . A isca do worm era simples: ela induzia o usuário a pensar que recebeu uma carta de amor....”[22], seguindo o artigo destaca a exploração das vulnerabilidades; “.....outra tática que se tornou o centro das

atenções ultimamente: a exploração de vulnerabilidades em software largamente utilizados no mercado. Tal estratégia oferece uma série de possibilidades para o invasor, dependendo da falha de segurança a ser explorada.....”[22].

O artigo também faz menção a criação de novas linguagens de programação como um dos fatores determinantes para evolução “.....alguns campos particulares da ciência da computação têm sido mais determinantes do que outros quando analisamos a evolução dos vírus de computador. E uma das maiores influências nessa área refere-se ao desenvolvimento das linguagens de programação....”[22]

3.7 Pragas relacionadas ao furto de informações

3.7.1 Spyware

Em artigo publicado pela Microsoft “Como Proteger o seu Computador do Spyware e do Adware “ de outubro de 2004 ,o autor Jerry Honeycutt define Spyware como “...software que envia suas informações pessoais para um terceiro, sem sua permissão ou conhecimento. Isso pode incluir informações sobre Web-sites que você visita ou algo mais sensível, como seu nome de usuário e senha.” [7]

O spyware pode se instalar na sua máquina ao baixar músicas de programas de compartilhamento de arquivos, jogos gratuitos de sites não confiáveis ou baixar outros softwares de qualquer fonte desconhecida. [7]

O spyware é freqüentemente associado a um software que exibe anúncios, chamado adware,alguns anunciantes podem instalar secretamente o adware em seu sistema e gerar um fluxo de anúncios não-solicitados, travando seu computador e afetando sua produtividade os anúncios também podem conter material

pornográfico ou outros que você pode considerar impróprios o processamento extra, exigido para rastreá-lo ou exibir os anúncios, pode sobrecarregar seu computador e comprometer o desempenho do sistema.[7]

3.7.2 Keylogger

Keylogger é o tipo de programa espião, furtivo e ilegal, com objetivo de roubar dados ou informações digitados pelo teclado (em alguns casos, também cliques de mouse), para depois enviá-los via Internet para algum destino mal intencionado. Por ser um programa maléfico, o keylogger em geral chega ao computador disfarçado, embutido ou escondido, comumente através de uma fraude fingindo ser um cartão postal animado, um exibidor de imagens ou outra coisa aparentemente inofensiva. Esta técnica de dissimulação é conhecida como cavalo-de-tróia, ou em inglês trojan-horse já descrito anteriormente.[20]

3.8 Proteção contra os Vírus

3.8.1 Antivírus

São pacotes de software que podem checar seu disco rígido HD e suas unidades de disquete ou CD-ROM quanto à presença de programas não desejados e prejudiciais aos sistemas operacionais os famosos vírus.

A função principal é proteger a máquina ou seja alertar da presença do vírus em um arquivo que por ventura o usuário estiver copiando para sua máquina através de disquetes, cds ou de outras formas já mencionadas anteriormente como arquivos

recebidos por e-mail, download de programas, musicas MP3 pelas redes P2P, bem como limpar arquivos infectados, deixando os dados originais intactos; no entanto, isto nem sempre é possível, pois alguns vírus causam danos irrecuperáveis. Às vezes, a única forma de nos vermos livres de um arquivo infectado é excluí-lo.

Existem uma enorme variedade de fabricantes entre as principais podemos citar a McAfee, Trend, Symantec, Panda que são softwares pagos porem existem fabricantes que fornecem seu produto gratuitamente para uso domestico como a GRISOFT que fornece o antivírus AVG, este produtos oferecem a prevenção e uma série de facilidades para monitorar constantemente as atividades dos arquivos em seu computador, todas as vezes que você copiar um arquivo de um disquete, transferir, compartilhar ou executar um programa, o software antivírus fará a verificação dos dados, a seguir será dada uma visão resumida do funcionamento destes softwares.

3.8.2 Como agem os Antivírus

Os programas antivírus agem, principalmente, lançando mão de 4 formas diferentes, para conseguir detectar o máximo de vírus possível. (Cidale, 1990)

- **Escaneamento de vírus conhecidos**

Este é o método mais antigo, e ainda hoje um dos principais métodos utilizados por todos os programas antivírus do mercado envolve o escaneamento em busca de vírus já conhecidos, isto é aqueles vírus que já são conhecidos das empresas de antivírus.

Uma vez que as empresas recebem uma amostra de um vírus eles separam uma string (um grupo de caracteres seqüenciais) dentro do código viral que só seja

encontrada nesse vírus, e não faça parte de nenhum programa ou software conhecido.

Essa string é uma espécie de impressão digital do vírus, e passa a ser distribuída semanalmente pelos fabricantes, dentro de suas vacinas.

O antivírus usa esse verdadeiro banco-de-dados de strings para ler cada arquivo do disco, um a um, do mesmo modo que o sistema operacional lê cada arquivo para carregá-lo na memória e ou executá-lo, se ele encontrar alguma das strings, identificadoras de vírus, o antivírus envia um alerta para o usuário, informando da existência do vírus. (Cidale, 1990)

- **Análise Heurística**

Os programas antivírus utilizam análise heurística, isto é, a análise do código de cada programa que esteja sendo executado em memória ou quando um escaneamento sob demanda for solicitado pelo usuário, antivírus varre os programas em busca de códigos assembler que indicam uma instrução que não deva ser executada por programas normais, mas que um vírus pode executar.

Um exemplo seria a descoberta de uma instrução dentro de um arquivo que faça uma chamada para a gravação dentro de um arquivo executável.

Este é um processo muito complexo, e sujeito a erros, pois algumas vezes um executável precisa gravar sobre ele mesmo, ou sobre outro arquivo, dentro de um processo de reconfiguração. (Cidale, 1990)

Por isso em alguns casos poderá ocorrer falsos alarmes o que é chamado de falso positivo (um aviso de vírus é dado, mas ele na verdade é falso).

Os antivírus devem monitorar constantemente as operações que são executadas a cada instante no computador, visualizando acessos a arquivos e sinais de atividades suspeitas, tal como um arquivo tentando se auto-copiar em

outros arquivos.

- **Busca Algorítmica**

Alguns programas antivírus se utilizam da aplicação de algoritmos descritos em suas vacinas.

Esse método é mais eficaz que o primeiro método, porém leva a um código muito maior para as vacinas e, além de consumir maior tempo para escanear todo o computador. (Cidale, 1990)

- **Checagem de Integridade**

Além dos métodos de escaneamento existem outras técnicas possíveis, tal como a técnica de checagem de integridade essa técnica cria um banco de dados, com o registro dos dígitos verificadores para cada arquivo existente no disco, que é salvo no disco para comparações posteriores. (Cidale, 1990)

Mais tarde, quando executada novamente esta checagem, o banco de dados é utilizado para conferir que nenhuma alteração, nem mesmo de um único byte, seja encontrada em se encontrando algum arquivo que o novo dígito verificador não bata com o gravado anteriormente, é dado o alarme da possível existência de um arquivo contaminado. (Cidale, 1990)

3.8.3 Prevenção

No ato de sua instalação, o antivírus deve ser configurado para ter seu

programa de residência em memória carregado automaticamente, sempre que se liga o computador neste caso o antivírus assume o papel de um vírus benigno que, ocupando as mesmas áreas de controle que o vírus ocuparia, averte o usuário no instante da tentativa de invasão, da presença de vírus com base na assinatura existente no banco de dados de nomes de vírus que acompanham o software. (Pitkowski, 1992)

A atualização dos antivírus nos dias atuais ocorrem semanalmente e em casos críticos com casos de pragas altamente contagiosas que possuem variantes, a atualização chega a ser diária, a maioria do antivírus possuem mecanismos automáticos de atualização, porém esta atualização pode ocorrer manualmente em situações de crise como já mencionado, onde os fabricantes disponibilizam em sites a nova lista de vírus contendo as informações necessárias para seus produtos identificarem a nova ameaça e lançando o alerta as empresas para efetuarem a atualização imediata.

A manutenção do antivírus sempre atualizado é a melhor maneira de prevenção contra as pragas.

3.8.4 Detecção

A detecção de vírus pode ocorrer de duas maneiras, partindo do princípio que o antivírus esteja sendo executado ou seja ativo na máquina e atualizado, o usuário pode receber um alerta da presença de vírus ao tentar gravar algum arquivo em sua máquina por cópia de através de disquetes, cds, transferência de arquivos pela internet conhecido com Download, ao receber e-mail com arquivos anexos.

A outra forma de detecção é a ativação da varredura ou escaneamento da

máquina a procura vírus, dispositivos que todos os produtos de antivírus possuem, esta forma de detecção é recomendada pelos fabricantes que seja executada semanalmente, devido as constantes atualizações. (Pitkowski, 1992)

3.8.5 Recuperação

Este modo, anda em conjunto com detecção pois ao identificar o vírus o software de antivírus em muitos casos efetuam a recuperação do arquivo infectado, ou seja efetua a limpeza do arquivo, em outros casos dão a opção de colocar o arquivo em quarentena ou seja deixar o arquivo suspeito em observação. (Pitkowski, 1992)

3.8.6 Exclusão

Para o caso do antivírus encontrar arquivo infectado que não possa ser limpo, deverá haver uma notificação na tela exibida pelo Antivírus.

A única solução neste caso é a exclusão dos arquivos contaminados, mas não sem antes, anotar o nome dos arquivos e verificar se há cópias de reserva (backup) deles, fora do computador, em disquetes ou CD-ROM ou na rede em que, porventura, o computador se conecte.

A exclusão pode ser efetuada automaticamente por configuração do antivírus e também manualmente.

É altamente recomendado que a opção automática seja sempre evitada, para permitir a montagem de uma lista de arquivos contaminados para análise prévia das conseqüências, para o computador, quanto à exclusão dos arquivos

listados.

Se o usuário identificar o arquivo contaminado como sendo um arquivo executável ou com extensões (.COM, DLL, etc.) e não identificar a natureza do mesmo, a probabilidade de um aplicativo como o Word, Excel, jogos etc, ou do sistema operacional serem afetados, pela exclusão do arquivo contaminado, passa a ser muito grande, podendo inclusive impedir a abertura do sistema operacional

Neste caso, muitas vezes, torna-se necessário, dependendo da importância do arquivo contaminado para o sistema como um todo, ou da quantidade de arquivos contaminados a reinstalação de aplicativos ou reinstalação do Sistema Operacional ou formatação do HD com perda de todos os dados obrigando-se a uma reinstalação geral. (Pitkowski, 1992

3.9 O perfil dos criadores de vírus

Os vírus de computador normalmente tem associado a sua criação a hackers o dicionário Michaelis nos dá a definição de hacker como “(**hac.ker** *sm Inform réker*) pessoa viciada em computadores, com conhecimentos de informática, que utiliza esse conhecimento para o benefício de pessoas que usam o sistema, ou contra elas” outra definição do dicionário Houaiss nos fornece a seguinte descrição “entusiasta de computador; aquele que é perito em programar e resolver problemas com o computador; pessoa que acessa sistemas computacionais ilegalmente”, recentemente tem sido mais usada para se referir a todos aqueles que, de uma forma ou de outra, abusam dos meios de informática ou de comunicações para ações perturbadoras ou danosas às informações computadorizadas alheias ou ao patrimônio dos proprietários dessas informações ,são pessoas altamente

competentes em linguagens de programação, com grande conhecimento em redes, sistemas operacionais e principalmente atento a suas falhas de segurança.

Podemos citar algumas características que levam estas pessoas a criar o vírus:

- contestação contra organizações, governos e a sociedade em geral;
- resposta a desafios pessoais perante grupo em que participa;
- sabotagem como vingança contra ex-patrões;
- fazer brincadeira, principalmente entre estudantes;

Assim, quem faz vírus pode ser considerado um hacker, mas, nem todo hacker é capaz de fazer vírus; pode ser considerado hacker também aquele que penetra em sistemas informatizados alheios para apenas obter informações das quais se aproveita com fins lucrativos ou não.

Outra característica dos criadores destas pragas é que geralmente são jovens segue alguns exemplos:

O norte-americano Jeffrey Lee Parson, de 18 anos, criou uma variante do vírus Blaster; o chinês Chen Ing-hau, de 24 anos, admite ter criado o vírus Chernobyl, o filipino Onel de Guzman, de 23 anos, criou o vírus I Love You, David Smith, 34 anos criou o vírus Melissa. [8]

Podemos concluir que o hacker, é uma pessoa geralmente jovem muito capacitada e determina a aprender, que passa horas a fio conectada e vasculhando na internet a procura de informações, assimilando linguagens de programação e topologia de redes, tudo que lhe de condições de atingir seu objetivos seguindo as motivações anteriormente expostas.

4.0 Ameaças do Futuro

Dentre outras pragas não abordadas neste trabalho e que podem ser exploradas como temas em trabalhos futuros podemos citar os Vírus para Celular e Fraudes Virtuais(Phishing Scams).

Em artigo publicado pela IDG NOW referente a um estudo apresentado pela McAfee, a disseminação de pragas em massa parece estar perdendo força, de acordo com especialistas os Hackers estão concentrando esforços em ações mais lucrativas e maliciosas, entre elas a distribuição de pragas para telefones celulares, fraudes virtuais(Phishing scams) e em explorar vulnerabilidades.

Os Phishing scams estão entre as ameaças com maior índice de crescimento

neste tipo de ataque os hackers utilizam e-mails para chegar até os usuários e posteriormente os conduzem para sites bancários ou de e-commerce falsos para capturar seus dados pessoais.

Os Vírus para aparelhos portáteis estão na lista das ameaças a caminho, a McAfee havia detectado cinco ameaças no quarto trimestre de 2004 e agora o montante chega a 50, dentre eles podemos citar o Commwarrior e o Cabir. [21]

Em entrevista a Módulo Security Magazine “Vírus: a evolução de uma ameaça eletrônica” o especialista em vírus digital Peter Szor, que recentemente lançou o livro “The Art of Computer Virus Research and Defense”, onde dedica um capítulo inteiro sobre a nova geração de pragas relacionadas exclusivamente a telefonia móvel, indicando que uma nova tendência de pragas para celulares estão por vir. [23]

Nesta entrevista ele também faz uma previsão sobre a evolução dos vírus seguindo o mesmo pensamento do relatório da McAfee, que as fraudes virtuais é que irão concentrar o maior potencial de construção de pragas motivadas pelo fator

financeiro ele cita "...Hoje,os programadores de vírus têm uma nova cara.Eles trabalham com spammers e fraudadores para obter vantagens financeiras.Eles desenvolvem pragas para abrir backdoors nos sistemas afetados, com intuito de vender essas redes para os spammers e fraudadores poderem agir...."[23]

4.0 CONCLUSÃO

Podemos através do estudo apresentado neste trabalho concluir, que a evolução do vírus de computador até chegar aos dias atuais sendo conhecido como praga virtual, está diretamente ligado a fatores determinantes:

- a criação de novas linguagens de programação
- evolução computacional, maquinas com maior poder de processamento
- a implementação de novos sistemas operacionais e produtos
- as falhas de segurança , vulnerabilidades destes sistemas e produtos
- a internet (rede mundial de computadores)
- o correio eletrônico (e-mail)
- as redes P2P

Nos anos 80 os primeiros vírus causavam a principio apenas perda de informação, lentidão da máquina infectada, bem como sinais gráficos na tela como o vírus Ping Pong e o vírus 1704 e a transmissão era basicamente feita através de disquete, a partir de 1998 com o vírus Chernobyl sentimos uma evolução considerável onde vírus era capaz de danificar também o hardware danificando a placa base.

Em 1999 com a praga Melissa sentiu-se o poder de disseminação e infecção

do e-mail considerada a primeira praga a atingir escala mundial confirmada, seguido pelo vírus LoveLetter, também se utilizando do e-mail para se propagar .

Em 2001 com o vírus Code Red temos a abertura de um precedente para a disseminação das pragas que concluo foi a principal na cadeia da evolução a exploração das vulnerabilidades, ou seja falhas de segurança dos sistemas operacionais e produtos Microsoft, todos as pragas que vieram a seguir tiveram poder de propagação , infecção e de destruição muito mais elevados.

Devemos também destacar a rede mundial de computadores e as redes P2P como fatores determinantes para esta evolução, as pragas evoluíram a ponto de se auto copiar para máquinas conectadas a estas redes , como descrito no Vírus Mydoom.

A pragas virtuais serão uma constante devido a todos os fatores já descritos anteriormente e como podemos ver no item ameaças do futuro outros segmentos de pragas estão a caminho e ganhando força entre os criadores; os vírus para celular, e as fraudes virtuais.

Durante a pesquisa realizada para o desenvolvimento deste trabalho, pude observar a importância sobre a evolução das pragas virtuais,o profissional de informática precisa conhecer o histórico da evolução das principais pragas, isto pode ajudá-lo a detectar possíveis infecções nos sistemas e ao descobrir as diversas maneiras de proliferação destas pragas e métodos de infecção, faz com que sejam criados sistemas mais eficientes de proteção, o que nos dias de hoje é essencial para os usuários domésticos e empresas.

A complexidade do tema, acredito ter sido a principal desvantagem encontrada durante a realização desta pesquisa,explicar minuciosamente os diversos casos de pragas virtuais descobertos até o momento, tornaria este trabalho

maçante, o principal objetivo é alertar os profissionais e usuários que precisamos ter um cuidado especial quando utilizarmos as inúmeras facilidades do mundo virtual não podemos ignorar a possibilidade de falhas e devemos ficar sempre alertas, afinal ainda nada é 100% seguro.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BARRETT, Pat. PC para iniciantes vírus, Dos e memória, softwares, manutenção. Rio de Janeiro: Campus, 1993.

[2] CIDALE, Ricardo A. Vírus digital. Uma abordagem para prevenção e manutenção

de seus sistemas de informação. São Paulo: Makron McGraw-Hill, 1990.

[3] PITKOWSKI, André. Vírus: prevenção, planejamento e controle, proteção de rede local, vírus mais comuns. São Paulo: Atlas, 1992.

[4] Vírus, Trojans e Worms. Disponível em: http://www.modulo.com.br/pt/page_i.jsp

[5] Guia de Defesa Profunda com Antivírus. Disponível em:
http://www.microsoft.com/brasil/security/guidance/recent/avdind_1.mspx#EGAA

[6] Biblioteca Técnica de Vírus. Disponível em: <http://www.pybbr.com/virusalerta.asp>

[7] Como Proteger o seu Computador do Spyware e do Adware : Disponível em:
http://www.microsoft.com/brasil/windowsxp/using/security/expert/honeycutt_spyware.mspx

[8] Alguns Vírus que Marcaram a Internet. Disponível em:
http://www.iq.unesp.br/pg_sti/pg4.htm

[9] The Twenty Most Critical Internet Security Vulnerabilities. Disponível em:
<http://www.sans.org/top20/#threats>

[10] McAfee Virus Information Library. Disponível em :
<http://vil.nai.com/vil/default.asp>

[11] Hyperlink Vírus & Pragas. Disponível em:
<http://www.mhavila.com.br/link/security/virus.html>

[12] Panda Software Enciclopédia de Vírus. Disponível em :
http://www.pandasoftware.es/virus_info/enciclopedia/

[13] Hackers Quem e Porque?. Disponível em :
<http://www.istf.com.br/vb/showthread.php?t=5615>

[14] Trend Virus Encyclopedia Search. Disponível em:
<http://www.trendmicro.com/vinfo/virusencyclo/default.asp>

[15] Symantec Enciclopédia de Vírus e Alarme Falso de Vírus On-line. Disponível em:
<http://www.symantec.com.br/region/br/avcenter/vinfodb.html>

[16] Formas de Ataques - Engenharia social. Disponível em:
http://www.scua.com.br/seguranca/conceitos/ataques_engsocial.htm

[17] Ataques de engenharia social na Internet. Disponível em:
<http://www.infowester.com/col120904.php>

[18] Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações. Disponível em:
<http://www.espacoacademico.com.br/043/43amsf.htm>

[19] Vulnerabilities, Incidents & Fixes. Disponível em:
http://www.cert.org/nav/index_red.html

[20] SpyBot Dicionário Keylogger. Disponível em:
<http://www.safer-networking.org/pt/dictionary/keylogger.html>

[21] McAfee alerta para as ameaças do futuro. Disponível em:
<http://idgnow.uol.com.br/AdPortalv5/SegurancaInterna.aspx?GUID=82A35AAC-263F-4DF3-82EC-CB7B82AD5A22&ChannelID=21080105>

[22] A evolução dos vírus de computador . Disponível em:
<http://www.modulo.com.br/index.jsp?page=3&catid=2&objid=376&pagenumber=0&idiom=0>

[23] Vírus: a evolução de uma ameaça eletrônica. Disponível em:
<http://www.modulo.com.br/index.jsp?page=3&catid=6&objid=84&pagecounter=0&idiom=0>

[24] <http://www.google.com.br>

GLOSSÁRIO

Análise Heurística - Análise informática de um programa de software antivírus que visa analisar um potencial vírus. Esta análise conclui se o arquivo é ou não suspeito,

se é susceptível de ter vírus.

Assembler – Linguagem de programação

Bios - O Basic Input/Output System, que identifica o Software responsável pela inicialização do computador, antes da localização do disco do sistema. Este localiza-se na memória ROM (Read Only Memory) do computador, que ao contrário da RAM (Random Access Memory) permanece guardada permanentemente.

DOS - Modelo de sistema operacional

DoS –(denial of service) negação de serviço, deixar um sistema indisponível

Download - ato de baixar arquivos através da internet

Extensão .exe , .com, .dll – referencias a terminação de arquivos de programas de computador e sistemas operacionais ex: word, windows XP

Firewall - Funciona como uma barreira que analisa toda a informação que passa das redes internas para as externas e vice versa podendo ser um software/hardware que analisa a informação que circula entre as duas redes e a bloqueia se não estiver conforme com as regras pré-definidas.

Internet – rede mundial de computadores

MP3 - formato de compressão utilizado em arquivos de música

Variante - Versão modificada de um vírus - concebida pelo autor do vírus, intencionalmente, ou por outra pessoa com o objetivo de emendar o seu código. Se as mudanças forem significativas o software antivírus pode não detectar esta variante do vírus.

Vulnerabilidade – termo utilizado para se referir a uma fraqueza ou falha se segurança de sistemas operacionais.

