ATAQUES A COMPUTADORES

INFORMÁTICA I

PROFESSOR: OTTON TEIXEIRA DA SILVEIRA FILHO
GRUPO: LUCIANO BEZERRA
PEDRO BOECHAT
SABRINA CAMPOS
STEFAN CARDOSO
RENATO TRISTÃO

ÍNDICE

A – INTRODUÇÃO

1- INTRODUÇÃO

Computadores sempre foram alvos de ataques, tais como os vírus, vermes, cavalos-de-tróia, entre outros, que tinham a finalidade de causarem danos nas máquinas, fosse para causar prejuízos ou apenas como diversão. Mas esse conceito vem mudando, a internet está sendo cada vez mais usada para fins lucrativos e maliciosos, como roubo de senhas, números de contas bancárias e de cartões de crédito, o que a torna bastante perigosa.

Com hackers e crackers cada vez mais habilidosos criando softwares mais e mais sofisticados, a internet se tornou um local sem muita segurança, no qual qualquer um que nela esteja conectado, tanto o computador quanto o próprio internauta, está sujeito a todos os tipos de perigos que esta oferece. Crimes virtuais vão crescendo de acordo com o aumento da quantidade de computadores, e também com a expansão da internet, principalmente a internet banda larga, que quanto mais rápida mais propícia a ataques ela está.

Dessa forma, ataques a computadores é uma área em constante expansão, e, ciente desse fato, os internautas devem ficar bem atentos ao acontece em seus computadores.

2- DEFINIÇÃO DE ATAQUES A COMPUTADORES

Ataques a computadores são tipos de crimes virtuais que visam, entre outras coisas, prejudicar computadores alheios. Crimes dos quais todos os internautas correm o risco de sofrer, mas que nem sempre sabem exatamente o que são, como agem e quais danos podem vir a causar aos computadores.

Existe uma gama de possibilidades de se vitimar um computador, as técnicas mais usadas são através de e-mails, arquivos compartilhados e páginas da web infectadas. Suas conseqüências também são bastante variadas, algumas têm como instrução infectar computadores alheios para, em seguida, danificar seus componentes, seja excluindo arquivos, seja alterando o funcionamento da máquina ou até mesmo deixando o computador vulnerável a outros tipos de ataques. Porém existem aqueles que não visam prejudicar a máquina, mas sim, seu usuário, como os softwares que têm como objetivo capturar informações sigilosas, como senhas e números de cartões de créditos para repassá-las para terceiros, causando graves transtornos às vítimas.

3- CONCEITOS

3.1- MALWARE

Termo geralmente aplicado a qualquer software desenvolvido para causar danos em computadores. Estão nele incluídos vírus, cavalos-de-tróia e vermes.

3.1.1- Vírus

Pequenos programas de computador criados para causar danos na máquina infectada, apagando dados, capturando informações ou alterando o funcionamento da máquina.

O nome vem da grande semelhança que estes programas têm com os vírus biológicos, pois, depois de infectar um computador, ele se instala em um programa e o usa como hospedeiro para se multiplicar e se disseminar para outros computadores. Podem anexar-se a quase todos os tipos de arquivos. Podem mostrar apenas mensagens ou imagens, sem danificar arquivos da máquina infectada, mas consumindo a capacidade de armazenamento e de memória ou diminuindo o desempenho do computador infectado. Podem também destruir arquivos, reformatar o disco rígido, ou até a destruição total do sistema operacional.

Os primeiros vírus foram criados em Assembly e C, mas atualmente são muito mais simples de serem criados, podendo ser desenvolvidos através de scripts e de funções macros de determinados programas.

Os usuários dos sistemas operacionais da Microsoft são as principais vítimas dos vírus, já que esses sistemas são os mais usados no mundo, existindo para este sistema os mais variados tipos diferentes de vírus. Existem também vírus para os sistemas operacionais Mac e Unix, mas estes são extremamente raros e bastante limitados.

Até algum tempo atrás, a contaminação era feita através do compartilhamento de arquivos em disquete, mas agora a internet é o seu principal meio de propagação, podendo contaminar milhares de computadores em pouco minutos. Os métodos mais comum são através de e-mails, comunicadores instantâneos e páginas html infectadas.

3.1.2-Vermes (ou Worms)

Programa auto-replicante, assim como o vírus, porém a principal diferença entre eles é a forma de propagação, os vermes podem se propagar rapidamente para outros computadores, pela net ou por redes locais, tirando cópias de si mesmo em cada computador. É um programa completo, não precisando de um hospedeiro para entrar em ação, como o vírus. Primeiro, ele controla os recursos que permitem o transporte de arquivos e informações, depois o verme se desloca sozinho para outros computadores. Seu grande perigo é sua enorme capacidade de replicação.

Pode ser projetado para fazer muitas coisas, como, por exemplo, excluir arquivos em um sistema, enviar documentos por e-mail ou podem provocar danos apenas com o tráfego

de rede gerado pela sua reprodução em massa, como é o exemplo do verme Mydoom, que causou lentidão generalizada na Internet no auge do seu ataque. Podem também trazer embutidos programas que geram algum problema ou que tornam o computador infectado vulnerável a outros ataques.

Há também um tipo de verme, como é o caso do Sobig, que abre o computador para ataques via Internet, transformando os computadores infectados em computadores zumbis que são utilizados para enviar e-mail ou para atacar outros computadores. Há também um tipo de verme, o Doomjuice, que utiliza essas "brechas" deixadas por outros tipos de vermes, para se espalhar.

3.1.3- Cavalo-de-Tróia

Também chamado de Trojan Horse, ou apenas Trojan, este programa, diferentemente dos vírus e dos vermes, não se duplica, alguns sendo até programado para se auto-destruir após algum tempo ou com algum comando do cliente. A infecção ocorre através de arquivos anexos a e-mails, mensagens instantâneas, downloads, por CDs ou disquetes. O programa é quase sempre uma animação ou imagens pornográficas, mas é durante a exibição dessas imagens que o computador está sendo infectado.

São famosos pela sua facilidade de uso, com ele qualquer pessoa pode controlar o computador de outros, sendo conhecido como "ferramentas de script kid".

Sua função é abrir o computador para o ataque de um eventual invasor, passando para este o controle da máquina infectada.

Os cavalos-de-tróia são divididos em duas partes: o servidor e o cliente. O servidor geralmente fica oculto em algum arquivo, que, quando executado, permite que o servidor seja instalado no computador da vítima, sem que esta saiba. Daí por diante o cliente passa a ter controle do computador infectado.

3.1.4- Spyware

Esse é um programa automático de computador que recolhe informações sobre o usuário e repassa para uma entidade externa na internet que não tem como objetivos a dominação ou a manipulação do sistema do usuário, e tem como intuito permanecer desapercebido no sistema. Ele Pode ser obtido por download de websites, mensagens de e-mail, mensagens instantâneas e conexões diretas para o compartilhamento de arquivos, podendo também estar contidos em vírus.

Costumava ser legalmente embutido em software e freeware, sendo removidos quando era feito a compra do software ou de uma versão mais completa e paga.

3.1.5- Phishing

Um tipo de golpe on-line de falsificação. Seus criadores são ladrões especializados em tecnologia que, geralmente, usam falsas páginas de inscrição para serviços comuns da Internet, como leilões, processadores de pagamentos ou serviços bancários, para tentar conduzir o receptor a revelar informações sigilosas e pessoais, como números de contas bancárias, cartões de crédito e senhas.

Usam também spam, websites, mensagens instantâneas e de e-mail com pretextos falsos para fazer com que as supostas vítimas baixem e executem arquivos que permitem o roubo futuro de informações ou o acesso não autorizado ao sistema infectado.

3.1.6- Spam

São mensagens de e-mail indesejadas, geralmente, anúncios não solicitados e enviadas em massa. É um problema sério de segurança, pois pode ser usado para transmitir vírus, cavalos-de-tróia, vermes, spywares, etc, além de alguns poderem conter links para websites com conteúdo não desejados.

Existem vários tipos de spam. Um dos mais conhecidos são os chamados hoaxes, que são histórias falsas recebidas por e-mails, seus conteúdos podem ser correntes, apelos sentimentais ou religiosos, campanhas ou ainda falsos vírus que ameaçam destruir, infectar ou formatar o disco rígido do computador. Tem como objetivo capturar endereços de e-mail que são passados ou vendidos para spammers (pessoas que passam spams)**.**

Há também as famosas correntes (chain letters), mensagens que prometem sorte, riqueza ou algum outro tipo de benefício àqueles que a repassarem para um número mínimo de pessoas em um tempo pré-determinado, e que dizem que aqueles que forem capazes de interromper a corrente sofrerão muitos infortúnios.

Outra forma do spam são os chamados golpes ou scam, que nada mais são do que golpes que garantem oportunidades de empregos, negócios, empréstimos facilitados, etc.

Sendo assim, com tantos tipos diferentes e modos distintos de persuasão, o spam acaba se tornando um dos mais perigosos tipos de golpes existente na Internet.

3.1.7- Ataques DoS

Ataque DoS (Denial of service, ou, em português, Ataque de negação de serviço) é um tipo de ataque onde o atacante procura vulnerabilidades dos Sistemas Operacionais específicos. São tentativas de impedir usuários legítimos de utilizarem determinado serviço utilizando técnicas que podem sobrecarregar uma rede a tal ponto que seus usuários não consigam mais usá-la, ou derrubar uma conexão entre dois ou mais computadores. Ou seja, o atacante tenta fazer com que os serviços fiquem impossibilitados de serem acessados.

É importante frisar que quando um computador/site sofre ataque DoS, ele não é invadido, mas sim, sobrecarregado, independente do sistema operacional utilizado.

Uma das formas de ataque mais conhecidas é a SYN Flooding, no qual um computador tenta estabelecer conexão com um servidor através de um sinal conhecido como

SYN (syncronize). Estabelecida a conexão o servidor envia ao computador solicitante um sinal chamado ACK (acknowledgement), o problema é que o servidor não consegue responder a todas as solicitações e então passa a recusar novos pedidos.

3.1.8- Ataques DDoS

Ataque DDoS (Distributed Deniel of Service) é um tipo de ataque DoS mais complexo, pois envolve a quebra da segurança de vários computadores conectados a Internet. É um tipo de ataque que, para que seja bem-sucedido, é necessário uma grande quantidade de computadores zumbis, podendo ser dezenas, centenas, ou até milhares de máquina controladas, para então atacar uma determinada vítima. A melhor forma de fazer isso é através de softwares maliciosos, como os vírus.

Após ter acesso às máquinas, o atacante instala o software de DDoS nelas que permitira a ele controlar essas máquinas podendo, agora, atacar qualquer site. Esses ataques esgotam o bandwidth, capacidade de processamento dos roteadores ou recursos de rede, fazendo a vítima perder a conexão com a internet enquanto o ataque estiver ocorrendo.

Esse tipo de ataque é um dos mais eficazes que existem e já prejudicou sites como os da CNN, Amazon, Yahoo, Microsoft e eBay.

B – VISÃO GERAL DOS ATAQUES

1- INTRODUÇÃO

Após a introdução de termos e apresentação dos conceitos, discutiremos mais profundamente sobre ataques a computadores, conceituando alguns elementos que comumente fazem parte da análise deste assunto e apresentando uma breve explicação sobre as motivações da adoção de uma classificação, bem como exemplificações de casos à luz de uma adotada por nós.

2- CLASSIFICAÇÃO

Pensando num ataque como uma concretização de uma ameaça, uma ação danosa para encontrar e explorar vulnerabilidades do sistema computacional que, se bem sucedida, causa uma intrusão indesejada no mesmo, o termo vulnerabilidade pode ser pensado como um conjunto de características do sistema que possibilitem um ataque.

Dentro deste cenário percebemos a existência de outros dois elementos além do próprio objeto da ação (sistema computacional): o elemento ativo, o *sujeito* da ação, um usuário ou um processo, que por sua vez encontra-se em busca do segundo elemento, um *objetivo* dentro do sistema computacional, que se concretiza como um meio de acesso e de uso do mesmo. Caracterizando por acesso a interação que se dá entre o sujeito e o tal objeto durante a qual há troca de informações, diz-se por incidente o ato do ataque seguido da reação/resposta do sistema computacional a ele.

O principal propósito de qualquer classificação é o de sugerir características pelas quais o objeto da classificação seja descrito de forma completa ou o mais próximo disso. Em nosso caso particular, o estudo de uma taxonomia tem como finalidade ajudar-nos a compreender conceitos gerais sobre esse tipo de interação homem-máquina, mais do que uma tentativa de enquadrá-la e dissecá-la por completo.

A classificação aqui apresentada é parte de uma extensa pesquisa realizada pelo doutor Howard J. D. em sua tese de curso nomeada “An analysis of security incidents on the Internet” (Uma análise dos incidentes de segurança na Internet), datada de 1995, e que, apesar de antiga, ainda provê uma ótima base para a compreensão e análise de tais ameaças digitais.

Esta classificação começa enfocando o assunto por um ângulo operacional, no qual atacantes estariam desejosos por conectar-se aos seus objetivos de alguma forma.

Apresenta o mecanismo de intrusão como uma série de “maneiras, meios e fins” para tal finalidade – principais alicerces de seu estudo – e os renomeia mais apropriadamente para “ferramentas, acesso e resultados”.

ATACANTES	➡	FERRAMENTAS	➡	ACESSO	➡	RESULTADOS	➡	OBJETIVOS

2.1- TIPOS DE ATACANTES

O trabalho de definição do alvo do mecanismo de ataque começa com a categorização dos tipos mais comuns de atacantes, numa tentativa de mapeamento de suas possíveis motivações. Interessante ressaltar a diferenciação de tratamento entre usuais categorizações e aquela escolhida, na qual *hackers* e vândalos são separados de outros invasores por conta de uma suposta motivação não criminosa.

Abaixo estão identificados os diferentes tipos vislumbrados pelo autor associados às suas possíveis intenções:

2.1.1- Hackers clássicos

Invadem sistemas primariamente pelo desafio e o status de tal ação.

2.1.2- Espiões

Buscam obtenção de informações que podem ser utilizadas para extorsões, barganhas ou negociatas políticas.

2.1.3- Terroristas

Têm como motivação a instauração do caos por meio de ações danosas a serviços vitais a sociedade civil ou o roubo de informações governamentais sigilosas.

2.1.4- Hackers corporativos

Indivíduos contratados por companhias com a finalidade de atacar os sistemas computacionais de seus adversários.

2.1.5- Criminosos profissionais

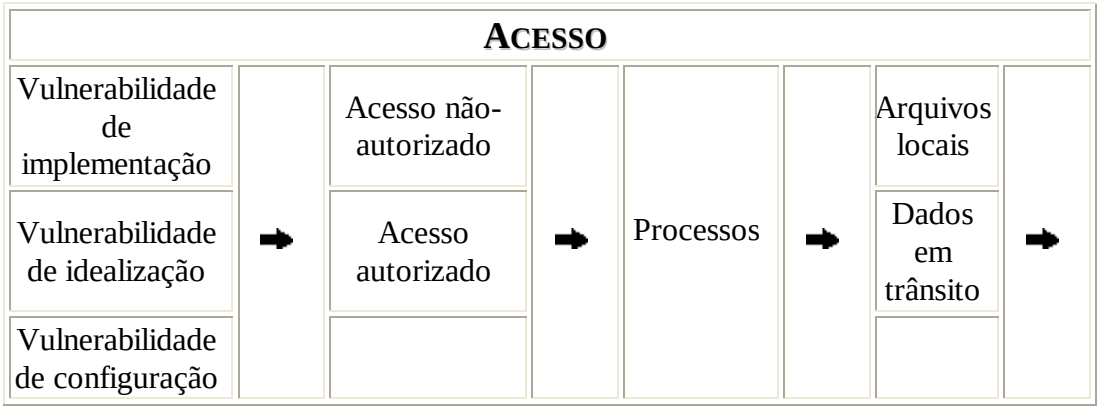
Aqueles que invadem sistemas para ganho financeiro próprio.

2.1.6- Vândalos

Atacam computadores única e exclusivamente para causar dano e prejuízo.

2.2- ACESSO

O acesso, até agora definido como o meio, visto de maneira ainda um pouco abstrata, de obtenção de um resultado, o acesso pode ser dito “não autorizado” ou “autorizado” e é obtido sobre *processos* residentes ou em dados em trânsito, através de *processos*. Tal acesso seria obtido através da exploração de vulnerabilidades, separadas em três categorias: *vulnerabilidades de implementação*, *vulnerabilidades de idealização* e *vulnerabilidades de configuração.*



Fluxo do processo de obtenção de acesso

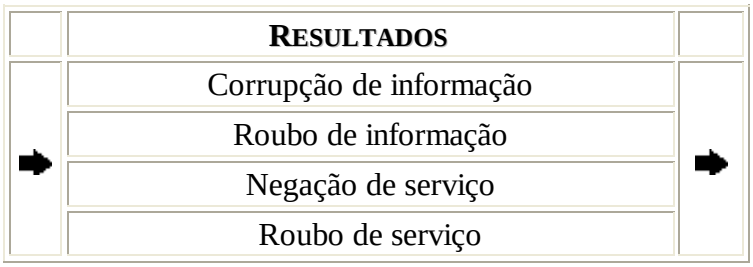
O tipo de vulnerabilidade mais conhecido e comumente explorado é aquele existente por conta de falhas de seguranças de um programa. Tais vulnerabilidades, conhecidas como *bugs*, não se dão devido a erros conceituais na elaboração do software, mas devido à inabilidade humana na hora de implementá-lo. O segundo tipo introduzido, então, é potencialmente muito mais sério e de difícil correção. A gravidade de tal vulnerabilidade é facilmente enxergada por conta do duplo esforço exigido para saná-la: tal medida conta não só com a necessidade de re-elaboração do processo/algoritmo realizado pelo software, mas como uma nova implementação do mesmo.

Não menos problemático, o último tipo de vulnerabilidade exposto é comumente algo de fácil prevenção/resolução, mas de ocorrência muito alta. Como colocado pelo autor, muitos vendedores de software embarcam-nos com uma configuração “confiável”, como conveniência ao usuário final, que o deixa normalmente muito vulnerável a ataques. Vulnerabilidades de configuração abarcam problemas de segurança como: usuários com senhas padrão, arquivos de controle com permissão de escrita “global”, exposição à Internet de serviços muito sensíveis ao contexto local, etc.

Outra particularidade interessante mencionada no artigo é uma estimativa de que cerca de 80% das quebras de segurança se dá através do uso abusivo de recursos por parte de usuários realmente autorizados – uma realidade da época provavelmente não muito condizente com a atual. Contudo, o autor também coloca como forma mais ocorrente de incidentes de segurança na Internet o roubo de acesso não-autorizado.

2.3- RESULTADOS

Um resultado de um ataque é o passo do sequenciamento de um ataque no qual o atacante dispõe de acesso ao sistema invadido e, estando livre para explorá-lo, pode alterar arquivos, negar serviços, obter informações ou desfrutar de alguma outra forma dos recursos disponíveis. O texto descreve três categorias clássicas de resultado e introduz uma a mais: o roubo de serviço.



Resultados de um ataque.

As categorias dos resultados de ataques são definidas da seguinte maneira:

2.3.1- Corrupção de informação

Qualquer alteração não autorizada de arquivos armazenados em um computador, ou data em trânsito através de uma rede.

2.3.2- Roubo de informação

A disseminação de informação a qualquer um que não esteja autorizado a conhecê-la.

2.3.3- Negação de serviço

A degradação intencional ou o bloqueio de um recurso computacional local ou de rede.

2.3.4- Roubo de serviço

O uso não autorizado de um computador ou serviço de rede sem degradá-lo.

2.4- FERRAMENTAS

A conexão final a ser feita na seqüência operacional que leva um atacante ao seu objetivo são as *maneiras de ataque*. Este conceito também é o mais trabalhoso de ser definido, dada a enorme variedade de métodos disponíveis para explorar vulnerabilidades computacionais. O autor comenta que se absteve de um erro grave, identificado em outras taxonomias, ao não tentar categorizar os métodos de ataque, simplesmente os ilustrando

através das ferramentas utilizadas. Utilizando tal aproximação, foi possível então a seguinte categorização das ferramentas:

2.4.1- Comandos de usuário

O atacante insere comandos maliciosos na linha de comandos ou interface gráfica.

2.4.2- Scripts ou programas

São introduzidos diretamente pelo atacante, iniciados no alvo, com a intenção de explorar as vulnerabilidades do sistema.

2.4.3- Agentes autônomos

Um programa, ou fragmento de programa, iniciado pelo atacante o qual, a partir de então, opera independentemente a fim de explorar as vulnerabilidades do sistema.

2.4.4- Kits de ferramentas

Pacotes de software que contêm scripts, programas, ou agentes autônomos.

2.4.5- Ferramentas distribuídas

Ferramentas distribuídas em diversos computadores secundários a fim de promover um único ataque coordenado e simultâneo (voluntário ou não) a um sistema alvo.

2.4.6- Interceptação de dados

Utilização de aparelhos capazes de “escutar” a radiação eletromagnética de um cabo carregando o tráfego de rede.

	FERRAMENTAS	
	Comando de usuário	
	Scripts ou programas	
	Agentes autônomos	
	Kits de ferramentas	
	Ferramentas distribuídas	
	Interceptação de dados	

Categorias de ferramentas utilizadas em um ataque

2.5- EXEMPLIFICAÇÕES

Tendo em vista a opção pela classificação das ferramentas sobre a definição das metodologias de ataque, nossas exemplificações se situarão em campos de casos bastante concretos. Há inúmeras outras ferramentas que poderiam constar nesta seção, mas a escolha das aqui utilizadas seguiu o critério de maior popularidade, basicamente pela maior chance de reconhecimento da mesma por parte do leitor. Segue abaixo uma ilustração para cada categoria de ferramentas anteriormente introduzidas.

2.5.1- Comandos de usuário

Um exemplo bastante corriqueiro desta categoria de ferramenta de ataque é o uso indevido do *software telnet*. Por intermédio desta ferramenta abre-se uma sessão remota com um sistema alvo, dentro da qual o usuário estará habilitado a executar comandos no mesmo. Para obter acesso a esse recurso, no entanto, é necessário que o atacante burle o processo de identificação/autenticação, o que pode ser conseguido de formas diversas, como pela adivinhação de senhas ou entrando-se longas cadeias de caracteres para explorar um esperado *bug* de *software*.

2.5.2- Scripts ou programas

Um tipo de *malware* bastante conhecido que se enquadra dentro desta categoria é o cavalo-de-tróia.

2.5.3- Agentes autônomos

Um agente autônomo se distingue de um programa de outros scripts ou programas maliciosos pelo fato de escolher e inserir-se em novos sistemas alvo por conta própria. O exemplo mais conhecido de agente autônomo é o vírus, que já contém a lógica de programação necessária para se auto-replicar e se disseminar entre sistemas.

2.5.4- Kits de ferramentas

Nos anos recentes se tem percebido o aumento do uso de kits de ferramentas. Kits de ferramentas agrupam scripts, programas e agentes autônomos em pacotes, manipulando-os, normalmente, por interfaces gráficas amigáveis. Um kit de ferramentas grandemente usado através da Internet é o *rootkit*, o qual contém um *sniffer* (programa utilitário que captura pacotes trafegando por uma rede local) e cavalos-de-tróia que podem ser usados em conjunto para abrir “portas de acesso” para uso posterior.

2.5.5- Ferramentas distribuídas

O que difere um programa malicioso que se enquadra nesta categoria de outros é a natureza múltipla e síncrona dos ataques. Uma ocorrência famosa do uso de ferramentas distribuídas é o envio de diversos pacotes ICMP através da utilização do *ping* em diversos computadores, a fim de sobrecarregar o tráfico de rede um sistema alvo de tal forma que sua conexão fique inutilizável.

2.5.6- Interceptação de dados

Dispositivos eletromagnéticos, como computadores e cabos de rede, geram campos magnéticos que podem ser explorados a fim de revelar informações temporárias em memória volátil (RAM) ou interceptar informações em trânsito pela rede. Esta categoria se difere muito das anteriores por utilizar uma forma física de ataque. A adição desta classe de ferramentas foi apenas necessária para manter a completude da classificação, mas como atestado pelo próprio CERT (Time de Resposta a Emergências Computacionais, em inglês), não há registros de nenhum ataque utilizando ferramentas desta natureza.

C – VISÃO GERAL DAS DEFESAS

1- INTRODUÇÃO

Existe um Quarteto Fantástico de softwares de segurança que todo usuário necessita ter. Um firewall, um antivírus, um anti-spyware e um anti-spam. Mas só isso não basta. O usuário tem que ter os três últimos atualizados diariamente e os seus aplicativos e sistema operacional tem que estar na sua última versão (*patches*) .

Neste tópico discutiremos intensamente sobre como tentar evitar ataques aos nossos computadores.

2- EVITANDO UM ATAQUE

Existem vários sites de segurança que divulgam dicas de como proteger o seu micro, iremos enumerar as 15, que em nossa opinião, são as mais importantes:

1º- Instale um bom programa antivírus e mantenha o mesmo atualizado diariamente, melhor se através do sistema de atualização automática. O programa deve ser configurado para filtrar em tempo real todos os programas que forem executados ou entrarem no computador de qualquer maneira e, de preferência, para executar uma varredura completa em busca de algum vírus a cada dia ou pelo menos uma vez por semana. Boas opções de programa Antivírus são: Kaspersky Lab, PandaVirus, NOD32 (Eset), Norton/Symantec e AVG. Alguns destes programas existem em versão limitada e gratuita.

2º- Instale um bom programa *Anti-spyware*. Configure este programa para filtrar todos os programas executados ou que entrem no computador de qualquer maneira. O programa deverá ainda ser configurado para se atualizar automaticamente e para executar uma varredura completa diariamente. Boas opções de programas deste tipo são: Microsoft AntiSpyware (grátis), Spy Sweeper, Spyware Doctor e Counter Spy.

3º- Instale um bom programa de *Firewall* e o configure para proteção intermediária ou máxima. Caso tenha problemas para executar tarefas no seu computador depois disso poderá ir diminuindo o nível de proteção ou excluindo certas funções. Algumas boas opções gratuitas na internet são: Comodo Personal Firewall (www.comodo.com), Sygate Personal Firewall (agora retirado pela Symantec, que incorporou a Sygate), Zone Alarm, Kerio Personal Firewall e Agnitum Outpost Firewall.

4º- Use o *Filtro de Spam* fornecido por seu provedor, ou se não for disponível

adquira um para utilizar junto ao seu cliente de e-mail. Ter um sistema capaz de filtrar as mensagens de spam de forma eficaz é importante, pois grande parte dos e-mails com arquivos maliciosos anexados são normalmente identificados como spam.

5º- Configure seu navegador (Internet Explorer, FireFox, Netscape...) para que *sempre* peça autorização e confirmação antes de baixar ou executar qualquer coisa na internet. Depois, não o autorize a baixar nada a não ser que saiba muito bem do que se trata. Como regra, nunca execute ou abra códigos diretamente da internet, se necessário os salve e rode depois.

6º- Antes de utilizar um novo site de compras e fornecer dados dos seus cartões de crédito ou banco, procure informações sobre a credibilidade, confiabilidade, solidez, segurança e eficiência dele. Também verifique se o site utiliza, para a troca de dados e informações, uma área segura baseada em criptografia (SSL). Para isso confirme que no seu navegador apareça um pequeno cadeado fechado ou uma chave no canto inferior da tela.

7º- Desconfie e rejeite sempre comunicados, propostas e ofertas milagrosas de qualquer tipo que possam chegar por qualquer meio (e-mail, MSN, salas de bate-papo, P2P, *chat systems* em geral e etc).

8º- Nunca anote senhas e outras informações confidenciais em lugares de fácil acesso (inclusive arquivos não criptografados dentro do seu computador) ou visíveis.

9º- Criminosos podem criar sites que parecem os de bancos ou outras entidades, com o intuito de enganar as vítimas desavisadas e de capturar suas senhas e dados sigilosos. Neste caso o primeiro cuidado é verificar se o endereço que aparece no navegador é realmente o do banco e se este permanece inalterado na hora que aparece o site. O segundo cuidado é o chamado teste da senha errada ou do "falso positivo". É só tentar acessar utilizando uma senha propositalmente errada e ver se o site aceita esta senha. Sites falsos aceitam qualquer coisa, já os verdadeiros sabem reconhecer a senha válida de uma errada. Se lembre que a enorme maioria dos casos de fraudes envolvendo internet *banking* acontece por descuidos do usuário e não por falhas de segurança do bancos.

10º- Sempre utilize um computador confiável para acessar sua conta e/ou dados sigilosos. *Nunca* use computadores públicos, de terceiros ou ainda computadores que não tenham sistemas de proteção eficientes para acessar sua conta ou qualquer outra informação sigilosa ou que necessite de uma sua senha (por exemplo, uma caixa de e-mail). Portanto, tome sempre os devidos cuidados quando acessar sua conta e, de forma geral, usar o seu computador.

11º- Evite navegar em sites arriscados e *nunca* baixe qualquer coisa de site que não conheça bem e que não seja totalmente confiável. Como regra geral, sites com

material pornográfico e sites que promovem pirataria de software e outros crimes são perigosos, pois freqüentemente contém vírus, cavalos-de-tróia ou outros programas maliciosos.

12º- Nunca responda à e-mails não solicitadas (spams), nem para pedir sua remoção de listas de envio ou para reclamar ou solicitar qualquer informação. Eles usam sua resposta para confirmar a existência do seu endereço de e-mail e aí sim que não irão parar nunca. Também não clique em *links* de descadastramento ou, de forma geral, em qualquer tipo de *link* ou site sugerido ou de outra forma presente nestas mensagens e *não* se assuste quando receber e-mails ameaçadores com cobranças, cancelamentos de documentos ou benefícios, ações na justiça etc... Também desconfie de mensagens que aparentam ter sido enviadas por bancos, repartições públicas, lojas famosas e programas televisivos. Não acredite e não leve a sério este tipo de mensagens, os respectivos órgãos e empresas *nunca* enviam mensagens por e-mail com este intuito. Sobretudo *não* abra nenhum arquivo anexado a estes tipos de e-mails nem acesse nenhum link sugerido.

13º- Nunca execute ou abra quaisquer arquivos anexados a mensagens de origem desconhecida ou não solicitadas. Sobretudo *não* abra arquivos dos tipos: .EXE, .COM, .SCR, .PIF, .BAT, .CMD, .DPR e .ASX. Também lembre de configurar o seu programa cliente de e-mail (Outlook, Eudora, Thunderbird...) para que não abra automaticamente os anexos. Na maioria dos casos estes programas são vírus, cavalos-de-tróia ou vermes.

14º- Não forneça seu endereço de e-mail para publicação em fóruns, salas de bate papo e grupos de discussão. A mesma regra vale para qualquer outra informação pessoal como nome completo, endereço, telefone, números de documentos (RG, CPF, CNH...), lugar de trabalho etc. Se não puder evitar publicar em algum lugar um endereço de e-mail, substitua o "@" por “(ARROBA)".

15º- Por fim, crie um endereço de e-mail alternativo em algum serviço gratuito de webmail (BOL, Hotmail, Yahoo, Gmail, IG...) e utilize exclusivamente este endereço (e não o seu pessoal e/ou profissional) para cadastramento em sites, fóruns, blogs, bate papos etc,quando isso for inevitável.

3- COMBATENDO O ATAQUE

Altamente combatido por outros países, o uso das técnicas descritas nos outros tópicos estão, a pouco tempo, também sendo combatidas no Brasil. No entanto, no Brasil, são punidas as ameaças que se encaixem ou no artigo 171 do Código Penal Brasileiro, estelionato, ou no artigo 241 da Lei 8069 de 13 de julho de 1900, pedofilia.

Apesar de tais limitações, a Polícia Federal ainda consegue realizar várias operações bem sucedidas. Abaixo seguem algumas operações já realizadas.

ANO 2001

Operação Cash Net (07/Novembro)

- Ocorreu simultaneamente em 2 estados;
- Mais de 70 policiais mobilizados;
- 17 pessoas presas;
- U$46 milhões roubados (estimativa).

ANO 2003

Operação “Cavalo de Tróia I” (05/Novembro)

- Ocorreu simultaneamente em 4 estados
- Mais de 200 policiais mobilizados;
- 30 mandados de prisão;
- 27 pessoas presas;
- U$14 milhões roubados (estimativa).

ANO 2004

Operação “Cavalo de Tróia II” (20/Outubro)

- Ocorreu simultaneamente em 4 estados
- Mais de 80 policiais mobilizados;
- 90 mandados de prisão;
- 64 pessoas presas;
- U$110 milhões roubados (estimativa).

ANO 2005

Operação “Pégasus” (25/Agosto)

- Ocorreu simultaneamente em 8 estados
- Mais de 400 policiais mobilizados;
- 100 mandados de prisão;
- 85 pessoas presas;
- U$33 milhões roubados (estimativa).

ANO 2006

Operação Scan (14/Fevereiro)

- Ocorreu simultaneamente em 7 estados
- Mais de 300 policiais mobilizados;
- O líder tinha 19 anos de idade;
- 63 pessoas presas;(9 eram menores);
- U$4.7 milhões roubados (estimativa).

D – FATOS E CURIOSIDADES

1- INTRODUÇÃO

Todos os dia ouvimos ou lemos alguma coisa que realmente chamou a nossa atenção. Vírus que explodiam máquinas quando o disquete era colocado, ou então como um joguinho que você perdia o seu sistema operacional... Bizarrices verídicas e histórias da carochinha podem ser encontradas aqui. Sem contar os fatos mais marcantes da história dessas pragas.

2- LINHA DO TEMPO

1982- Surgiu o primeiro vírus, chamado Elk Cloner, foi escrito por um estudante, Rich Skrenta. O vírus se espalhava por disquetes quando o computador realizava o Boot. Quando o computador dava o 50ª Boot com o disquete infectado, aparecia um poema na tela da máquina.

1983- Começou a ser desenvolvido o primeiro vírus experimental. O programa foi criado em um sistema Unix, pelo engenheiro elétrico norte-americano Fred Cohen, para um seminário sobre segurança de computação.

1986- Surge o Brain, primeiro vírus para MS-DOS a se ter conhecimento, infectava apenas disquetes, ocupando todo o espaço disponível. Foi também o primeiro vírus com a capacidade de ocultar-se, pois mostrava o espaço infectado como disponível.

1986- Ainda nesse ano, foi lançado o primeiro cavalo-de-tróia, o PC-Write.

1987- Nesse ano o assunto começou a tomar proporções maiores, com o surgimento de vírus novos e cada vez mais perigosos. O Lehigh infectava o command (.com), um software básico do sistema operacional DOS, e o Suriv-02 infectava os arquivos executáveis (.exe) que culminaram no Jerusalém, um vírus que era ativado toda as sextas-feiras 13 e apagava qualquer arquivo acessado nesse dia. Surgiu também um programa chamado Christmas que se replicava rapidamente (cerca de 500 mil por hora), atingindo os computadores da IBM.

1988- Um vírus chamado MacMag começou a atacar os Macintosh, computadores pessoais fabricados e comercializados pela Apple. Ainda nesse ano, surgiu Morris worms, considerado o primeiro verme de internet, infectando e paralisando cerca de 10 % da rede, sendo também o primeiro verme a receber atenção da mídia. Fato que levou à criação, nos Estados Unidos, do primeiro CERT (Computer Emergency Response Team), centro de resposta rápida a incidentes desse tipo.

1989- Começaram as aplicações de golpes através dos vírus. Como é o exemplo de um software que ao ser instalado criptografava o disco rígido e a única foma de recuperá-lo era com o pagamento de uma taxa ao autor.

1990- Foi lançado o primeiro livro e criado o primeiro fórum sobre vírus. E, ainda nesse ano, a Norton lançou seu antivírus, tendo como resposta a criação de programas como o Tequila, primeiro vírus polimórfico, ou seja, tipo de vírus que se modificava a cada infecção para evitar a detecção.

1992- Surgiu um novo vírus, denominado Michelangelo. Vírus que nesse ano foi motivo de preocupação sobre seus possíveis danos. Estimou-se a "destruição" de 5 milhões de computadores, mas apenas cerca de 5 a 10 mil foram efetivamente infectados.

1994- Surgiram os primeiros Hoaxes (boatos), um exemplo era o vírus "Good Times" que apagaria todo o disco rígido apenas com a abertura do e-mail.

1995- Chegaram os vírus macros que exploravam falhas nos sistemas operacionais Windows, infectando os documentos do Word.

1996- Surgiu o primeiro vírus para Linux. E por essa época já existiam vírus desenvolvidos especialmente para arquivos do Windows 95 e do Excel.

1998- A linguagem Java passou a ser atacada por vírus, mais especificamente, pelo Strange Brew, um vírus parasita que contaminava um hospedeiro, mas não atrapalhava seu fincionamento. Nesse ano também surgiu o BackOrifice, um sistema de controle de computadores que atacava pela internet.

1999- Os vermes começaram a sua dominação nos ataques. O primeiro a surgir foi o Melissa, uma espécie de mistura de vírus macros e vermes, que tinha como objetivo a infecção de arquivos do Word e utilizava e-mails para se propagar automaticamente para contatos do Outlook e Outlook Express. Ainda nesse ano, foi criado um outro verme chamado Bubbleboy, este também utilizava mensagens de e-mail para se propagar, porém este não precisava de arquivos anexos às mensagens para contaminar outras máquinas, pois ele aproveitava as falhas do navegador Internet Explorer e bastava a visualização de uma mensagem de e-mail para o computador ser infectado. Conceito que foi aproveitado por muitos outros vermes que vieram depois.

2000- Surgiu nesse ano o vírus "LoveLetter" ou " I Love You" como ficou conhecido no Brasil, este vírus causou um prejuízo de até 9 bilhões de dólares, por meio de uma "carta de amor", cujo anexo era uma atualização do vírus Melissa. Tornando-se assim um dos mais bem sucedidos vírus da história. Nesse ano também aconteceram os primeiros ataques de negação de serviço sérios, os quais paralisaram sites como Yahoo! e Amazon. E ainda esse ano surgiram também os primeiros códigos maléficos para Palmtops, para sistemas de telefonia integrados à Internet, para sistema de arquivos do Windows NT e para a linguagem de programação PHP.

2001- Foi lançado o primeiro vírus capazes de infectar tanto os sistemas Windows quanto o Linux. Também surgiram os primeiros vermes que se propagavam por sistemas de trocas de arquivos, pelo programa de bate-papo Mirc, os baseados na linguagem de programação AppleScript, dos computadores Macintosh, e os que infectavam os softwares de PDF da Adobe. Novos tipos de vermes também surgiram como, por

exemplo, o Nimda, o Sircam e o CodeRed, este último se multiplicou mais de 250 mil vezes, em aproximadamente nove horas.

2002- Apareceram os primeiros vírus que infectavam tecnologia, como a linguagem C# e o SQL Server (todos produtos da Microsoft), arquivos Flash, a rede de troca de arquivos do programa Kazaa, servidores Apache rodando sobre o sistema FreeBSD e arquivos de imagem JPEG.

2003- A programação se une à engenharia social e dá origem aos chamados "phishing scams". Surge também outros tipos de vermes, um chamado de Blaster, que atacava uma vulnerabilidade de um componente do Windows e se disseminava rapidamente. Outro, o Slammer, que atacava servidores SQL 2000 da Microsoft, também atacou nesse mesmo ano. O Sobig aliava seu próprio servidor de envio de mensagens a um sistema que permitia seu uso remoto por spammers.

2004- Aumentaram os ataques de "phishing", geralmente associados a cavalos-de-tróia. Apareceram também outros tipo de ameaças, com o Sasser, verme que afetava a vulnerabilidade do Windows e se disseminava via servidores de arquivos (FTP), os vírus Rugrat, voltado para sistemas Intel de 64 bits, o Cabir, primeiro a infectar telefones celulares da série 60 da Nokia, e o Scob, que surgiu em junho e atacava servidores Web baseados em Windows e, depois, por meio de um código Javascript inserido em todas as páginas do servidor afetado, instalava um cavalo-de-tróia no computador dos visitantes, com o objetivo de roubar senhas bancárias. Nesse ano também vulnerabilidades no sistema Mac OS X que permitiam ataques de vírus também foram detectadas e corrigidas.

2- DADOS ESTATÍSTICOS

- 95% dos ataques virtuais são feitos por *script kiddies*. Estes utilizam *exploits*, cavalos-de-tróia e ferramentas de cracking para alcançar seus objetivos.
- Segundo o McAfee Avert Labs, líder mundial em prevenção de intrusões e gerenciamento de risco em segurança, houve um aumento de 784% das páginas tipo *phishing* no primeiro semestre de 2007, sem previsão de redução.
- Segundo a Attrition.org, mais de 13,7 milhões de registros foram violados no primeiro semestre de 2007, um considerável aumento em relação ao mesmo período de 2006, quando cerca de 1,8 milhão de registros sofreram essa mesma violação.
- Desde 2005 o número de *spam* de imagem vem crescendo exponecialmente. Em 2005 esse número não passou dos 10%, em 2006 chegou aos 40%, e só no início de 2007, esse tipo de *spam*, entre todos os outros, alcançou a marca dos 65%.
- A variedade de vírus também está em crescimento, a Avert Labs classificou mais de 150 tipos diferentes desses *malwares*.

- Em torno de 200 mil computadores foram infectados desde o início de 2007, aumentando 10% em relação ao primeiro trimestre de 2006.
- No primeiro semestre de 2006 a Microsoft emitiu 32 boletins de segurança dos quais 19 foram classificados como críticos e 10 considerados importantes. Durante o mesmo período de 2007, foram emitidos 35 boletins, destes 25 foram classificados como críticos e 9 importantes.
- Diminui o número de ataques contra dispositivos móveis, como telefones celulares e *smart phones*. Caiu também o número de robôs que deixam o controle dos computadores na mão de oportunistas virtuais.
- Em 1999 eram conhecidos 250 tipos diferentes de cavalos-de-tróia, em 2000, esse número chegou a 550 e em 2003 já eram 27.000 tipos.
- Assim como os cavalos-de-tróia, cada vez mais tipos diferentes de vírus vem sendo descoberto: até 1990, 80 eram conhecidos, até 1995 surgiram cerca de 5.000 vírus, em 1999 já eram conhecidos 20.500 vírus, em 2000 esse número chegou aos 49.000, em 2001 eram 58.000 tipos diferentes. Em 2005 aproximou-se dos 72.010. Até 2007 esse número ainda é desconhecido.
- Foi identificado um cavalo-de-tróia, mas ainda não há antivírus. O Trojan.Trickanclick está se propagando por e-mail.

3- BOATOS

Muito cuidado. Foi lançado um vírus que, em duas horas limpa e queima seu disco rígido. Ele vem em uma mensagem com sapatinhos vermelhos dançando e uma música bem alegre. Vai vir com vários *links* com músicas. Não baixe!

Mais um boato que circulou na internet. Detalhe, esse era um boato já batido nos Estados Unidos da América que foi traduzido. No entanto, esse vírus nunca veio...

Se todos os boatos de vírus novos fossem verdade, estaríamos muito a frente com nossa tecnologia e as empresas de antivírus teriam ido à falência...

Facilmente pode ser desvendado um boato, a maioria segue um mesmo plano:

- Letras maiúsculas para chamar atenção

- Pedem que você repasse para o maior número de pessoas possível

- Normalmente, colocam empresas que não são ligadas ao combate de vírus

E – ASPECTOS CONCLUSIVOS

O trabalho discutiu aspectos importantes a cerca de ataques a computadores. Tanto os vírus, cavalos-de-tróia e vermes têm por finalidade causar danos às máquinas, ou simplesmente divertir seu criador. Tendo em vista que a internet é um dos meios mais eficientes para troca de informações nos dias atuais, tanto hackers quanto crackers, cada vez mais habilidosos na criação de softwares sofisticados, vem imprimindo um caráter maléfico na utilização da mesma. Um exemplo são os fins lucrativos e maliciosos, como roubo de senhas, números de contas bancárias e de cartões de crédito, ambicionados pelos hackers e crackers. É sabido que os crimes virtuais estão crescendo de acordo com o aumento da quantidade de computadores, e também com a expansão da internet, principalmente a internet banda larga, que quanto mais rápida mais propícia a ataques ela está. No entanto, focando um pouco mais na área de pesquisa, uma vez que aspectos relativos à visão geral dos ataques, das defesas e fatos e curiosidades já foram previamente explanados, buscar-se-á nesta parte final e conclusiva ilustrar tal aspecto.

Neste sentido, ataques a computadores é um ponto crucial para análise de grandes projetos. Evitá-los ao máximo garante não só a execução correta de um dado trabalho, como também a segurança das informações a ele vinculadas. Tendo em vista projetos de pesquisa na área aeroespacial brasileira, tal como a análise do comportamento de sistemas de proteção térmica para veículos espaciais, observa-se que qualquer incoerência nos dados fornecidos em última instância pode causar acidentes de proporções inimagináveis como, por exemplo, o que se sucedeu na base de Alcântara em 2003. **Claro deve estar que não se está vinculando tal acidente a um ataque a computador, mas sim servindo de exemplo ilustrativo de danos que podem se suceder de uma dada situação**. Atualmente o IAE/CTA juntamente com demais universidades realizam num período de 2 anos um grande projeto de pesquisa que busca subsidiar através da junção de conhecimentos em diversas áreas o projeto do veículo SARA (Satélite de Reentrada Atmosférica) por intermédio do Programa UNIESPAÇO financiado pela Agência Espacial Brasileira.

Um código computacional denominado *TPS-Nose*, que foi desenvolvido pelo Programa de Engenharia Mecânica da COPPE/UFRJ que é executado na plataforma simbólico-numérica *Mathematica 5.2* vai ser usado como exemplo prático de como uma alteração em informações pode levar até a perda completa do sistema de proteção térmica previamente projetado. Tendo em vista que o código inclui a interpolação das propriedades atmosféricas, cálculo da trajetória, determinação do aquecimento aerodinâmico, cálculo da ablação no ponto de estagnação e ao longo do corpo do veículo avaliar-se-á como a modificação inoportuna de dados de propriedades termofísicas pode implicar em situações inesperadas. Para isto considere apenas que uma das propriedades termofísicas do material do sistema de proteção térmica tenha sido, por exemplo, alterada. Na Tabela 1, serão mostradas as propriedades reais do material ablativo SLA-561V [virgin] que já vem sendo utilizado pela NASA a um bom tempo desde as missões para o planeta Marte e é tido como sendo um dos melhores materiais ablativos para compor um sistema de proteção térmica de uma aeronave em reentrada atmosférica.

Tabela 1 – Propriedades termofísicas do material SLA-561V [virgin]

	unidade	real	alterada
espessura do TPS	m	0.024	0.024
condutividade térmica do TPS	W/(m.K)	0.0592	0.0592
massa específica do TPS	kg/(m^3)	264	164
calor específico à pressão cte do TPS	J/(kg.K)	1160	1160
calor de ablação do TPS	J/kg	5.41*10^7	5.41*10^7
temperatura de ablação do TPS	K	588	588
emissividade do TPS		0.7	0.7

Depois de avaliarmos que a única modificação no código foi ao invés de colocar 264 termos colocado 164 temos que o material se queimará completamente antes de chegar ao solo como mostra a Figura 1 abaixo:

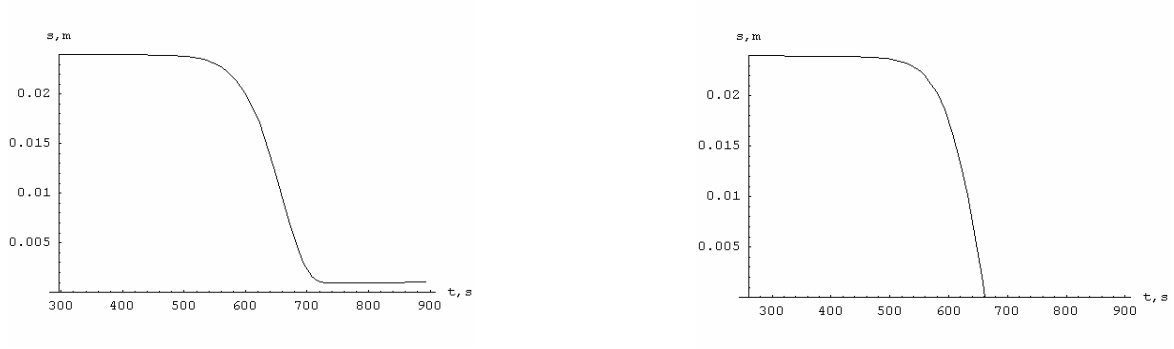


Figura 1 – Variação da espessura do material do sistema de proteção térmica em função do tempo de vôo

Desta forma, será criada uma situação constrangedora entre o projetista e o gerente de projeto uma vez que anteriormente tínhamos a missão dada como satisfatória, no entanto, agora passamos a ter o problema de não chegarmos até o solo de nosso planeta Terra. Sendo assim, observa-se que mesmo o projetista avaliando a situação com o rigor necessário, teremos uma incoerência nos resultados tendo em vista que um parâmetro interno já tido como correto foi burlado por um ataque a computador.

Finalmente, **observa-se que a segurança nas informações seja na entrada, saída ou processamento de dados deve ser máxima, para evitar prejuízos e problemas.**

Dessa forma, ataques a computadores é uma área em constante expansão, e, ciente desse fato, os usuários devem ficar bem atentos para os aspectos de segurança. Pois somente seguindo esses aspectos, será possível evitar que ataques a computadores sejam bem sucedidos.

F – GLOSSÁRIO

- **Antivírus:** Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

- **Ataque:** Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

– **Exploits:** é um programa, uma porção de dados ou uma seqüência de comandos que se aproveita das vulnerabilidades de um sistema como o próprio sistema operativo ou serviços de interação de protocolos (ex: servidores). Geralmente são elaborados por *hackers* como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por *crackers* a fim de ganhar acesso não autorizado a sistemas

- **Firewall:** Dispositivo constituído pela combinação de software e hardware, utilizado para dividir e controlar o acesso entre redes de computadores.

- **Phishing:** Forma de ataque em que crackers tentam se passar por empresas ou uma pessoa confiável. Eles fazem isso através de uma comunicação eletrônica oficial como um correio ou mensagem instantânea para "pescar" (fish) senhas e/ou números de cartões de crédito.

– **Script kiddies (garotos dos scripts):** nome dado a grupos de *crackers* inexperientes e geralmente pertencentes a uma faixa etária mais nova. Não possuem conhecimento de programação, mas aproveitam as ferramentas criadas por especialistas com a finalidade de ganhar fama, lucrar ou apenas para diversão.

- **Spam:** Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do Inglês Unsolicited Commercial E-mail).

- **Spyware:** Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

G – BIBLIOGRAFIA

- Clube do Hacker
(http://www.clubedohacker.com.br/index.php?option=com_content&task=view&id=91&Itemid=31)

- How Stuff Work
(http://informatica.hsw.uol.com.br/virus1.htm)

- HSBC Bank Brasil
(www.hsbc.com.br/common/seguranca/artigo-seguranca-historia-virus.shtml)

- IDG Now!
(http://idgnow.uol.com.br/seguranca/2007/06/06/idgnoticia.2007-06-06.0529548520/redirectViewEdit?pageNumber:int=2)

- InfoWester
(http://www.infowester.com/col091004.php)

- Total Security
(http://www.totalsecurity.com.br/article.php?sid=3123&order=0)

- Wikipédia
(http://pt.wikipedia.org/wiki/P%C3%A1gina_principal)

Howard, John D., 1995 - An Analysis Of Security Incidents On The Internet, Cáp. 6
(http://www.cert.org/research/JHThesis/)

- Infoguerra
(www.infoguerra.com.br)

- Comitê Gestor da Internet no Brasil
(http://cartilha.cert.br/)

- Monitor das Fraudes
(http://www.fraudes.org)

-Tristão Jr., R. M., 2006, "**Análise do Sistema de Proteção Térmica de Veículos Espaciais em Reentrada Atmosférica e Vôo Sub-orbital**", Projeto Final de Curso, Engenharia Mecânica, POLI/UFRJ.