Instituto Federal do Pará

Ricardo José Cabeça de Souza
ricardo.souza@ifpa.edu.br
2010
Fundamentos de Microinformática
Segurança

Vírus de Computador 

- São pequenos programas criados para se espalharem de um computador para outro e interferir na operação do computador
- Um vírus pode corromper ou apagar dados no seu computador, usar seu programa de email para se espalhar para outros computadores ou até mesmo apagar todo o seu disco rígido

Vírus de Computador 

- É um código de computador que se anexa a um programa ou arquivo para poder se espalhar entre os computadores, infectando-os à medida que se desloca
- Ele infecta enquanto se desloca
- Os vírus podem danificar seu software, hardware e arquivos
- Código escrito com a intenção explícita de se autoduplicar
- Um vírus tenta se alastrar de computador para computador se incorporando a um programa hospedeiro

Vírus de Computador 

- Ele pode danificar hardware, software ou informações.
- Assim como os vírus humanos possuem níveis de gravidade diferentes, como o vírus Ebola e o vírus da gripe, os vírus de computador variam entre levemente perturbador e totalmente destrutivo
- A boa notícia é que um verdadeiro vírus não se dissemina sem ação humana
- É necessário que alguém envie um arquivo ou envie um email para que ele se alastre.

Vírus de Computador 

- Os vírus são mais comumente espalhados por anexos em mensagens de email ou em mensagens instantâneas
- É por isso que você nunca deve abrir anexos de email a menos que conheça o remetente ou esteja esperando por eles
- Os vírus podem ser disfarçados como anexos de imagens engraçadas, cartões de felicitações ou arquivos de áudio e vídeo

Vírus de Computador 

- Os vírus também se espalham através de downloads da Internet
- Eles podem estar escondidos em softwares ilícitos ou em outros arquivos ou programas que você baixar.

Vírus de Computador 

- Para que um computador seja infectado por um vírus, é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:
  - abrir arquivos anexados aos *e-mails*;
  - abrir arquivos do Word, Excel, etc;
  - abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
  - instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, *pen drives*, CDs, DVDs, etc;
  - ter alguma mídia removível (infectada) conectada ou inserida no computador, quando ele é ligado

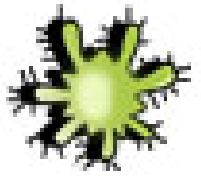
Vírus de Computador 

- Para ajudar a evitar vírus, é essencial:
  - manter o computador atualizado com as atualizações mais recentes
  - Usar ferramentas antivírus
  - Manter-se informado sobre ameaças recentes
  - Seguir algumas regras básicas durante a navegação pela Internet, o download de arquivos e a abertura de anexos

Vírus de Macro

- Uma macro é um conjunto de comandos que são armazenados em alguns aplicativos e utilizados para automatizar algumas tarefas repetitivas
- Um exemplo seria, em um editor de textos, definir uma macro que contenha a seqüência de passos necessários para imprimir um documento com a orientação de retrato e utilizando a escala de cores em tons de cinza
- Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo que utiliza macros

Vírus de Macro



- Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.
- Existem alguns aplicativos que possuem arquivos base (modelos) que são abertos sempre que o aplicativo é executado
- Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será

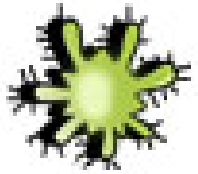
Vírus de Macro

- Arquivos nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access, são os mais suscetíveis a este tipo de vírus
- Arquivos nos formatos RTF, PDF e *PostScript* são menos suscetíveis, mas isso não significa que não possam conter vírus.

Vírus de Celular

- Um vírus de celular se propaga de telefone para telefone através da tecnologia *bluetooth* ou da tecnologia MMS (*Multimedia Message Service*)
- A infecção se dá da seguinte forma:
  - O usuário recebe uma mensagem que diz que seu telefone está prestes a receber um arquivo.
  - O usuário permite que o arquivo infectado seja recebido, instalado e executado em seu aparelho.
  - O vírus, então, continua o processo de propagação para outros telefones, através de uma das tecnologias mencionadas anteriormente.

Vírus de Celular



- A infecção se dá da seguinte forma:
  - Os vírus de celular diferem-se dos vírus tradicionais, pois normalmente não inserem cópias de si mesmos em outros arquivos armazenados no telefone celular, mas podem ser especificamente projetados para sobrescrever arquivos de aplicativos ou do sistema operacional instalado no aparelho.
  - Depois de infectar um telefone celular, o vírus pode realizar diversas atividades, tais como:
    - destruir/sobrescrever arquivos, remover contatos da agenda, efetuar ligações telefônicas, drenar a carga da bateria, além de tentar se propagar para outros telefones.

Vírus de Celular

- Algumas das medidas de prevenção contra a infecção por vírus em telefones celulares são:
  - mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário
  - Caso isto não seja possível, consulte o manual do seu aparelho e configure-o para que não seja identificado (ou "descoberto") por outros aparelhos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível");
  - não permita o recebimento de arquivos enviados por terceiros, mesmo que venham de pessoas conhecidas, salvo quando você estiver esperando o recebimento de um arquivo específico;

Vírus de Celular

- Algumas das medidas de prevenção contra a infecção por vírus em telefones celulares são:
  - fique atento às notícias veiculadas no *site* do fabricante do seu aparelho, principalmente àquelas sobre segurança;
  - aplique todas as correções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
  - caso você tenha comprado uma aparelho usado, restaure as opções de fábrica (em muitos aparelhos esta opção aparece como "Restaurar Configuração de Fábrica" ou "Restaurar Configuração Original") e configure-o como descrito no primeiro item, antes de inserir quaisquer dados.

Worm

- Um worm, assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente via falhas de softwares/hardware
- Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações
- Depois que o worm contamina o sistema, ele se desloca sozinho
- O grande perigo dos worms é a sua capacidade de se replicar em grande volume

Worm

- Diferente do vírus, o *worm* **não** embute cópias de si mesmo em outros programas ou arquivos e **não** necessita ser explicitamente executado para se propagar
- Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores

Worm

- Por exemplo, um worm pode enviar cópias de si mesmo a todas as pessoas que constam no seu catálogo de endereços de email, e os computadores dessas pessoas passam a fazer o mesmo, causando um efeito dominó de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a Internet como um todo
- Quando novos worms são lançados, eles se alastram muito rapidamente
- Eles obstruem redes e provavelmente fazem com que você (e todos os outros) tenha de esperar um tempo maior para abrir páginas na Internet.

Worm

- Uma subclasse de vírus
- Um worm geralmente se alastra sem a ação do usuário e distribui cópias completas (possivelmente modificadas) de si mesmo através das redes via falhas de software/hardware
- Um worm pode consumir memória e largura de banda de rede, o que pode travar o seu computador.

Worm

- *Worms* são notadamente responsáveis por consumir muitos recursos
- Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar
- Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

Worm

- Como os worms não precisam viajar através de um programa ou arquivo "hospedeiro", eles também podem se infiltrar no seu sistema e permitir que outra pessoa controle o seu computador remotamente
- Exemplos recentes de worms incluem o worm Sasser e o worm Blaster

Worm Sasser 

- O worm Sasser (W32.Sasser.A e seus variantes) exploram uma falha de segurança no Serviço de Subsistema de Segurança Autoritária Local (LSASS) que a Microsoft endereçou com a liberação de uma atualização de segurança
- O Sasser explora computadores com software não atualizados e esses computadores permanecem no risco de infecção até que a atualização seja instalada
- Recomendamos aos clientes que instalem a atualização do **Boletim de Segurança Microsoft MS04-011** para ajudar na proteção contra softwares maliciosos

Worm Blaster 

- Os objetivos do worm Blaster (W32.Blaster.A e suas variantes) é usar uma falha de segurança com a função Chamada de Procedimento Remoto (RPC) que a Microsoft solucionou com a liberação de uma atualização de segurança
- O Blaster tem como alvo computadores com softwares antigos, e nesses computadores permanece o risco de ser infectado até que uma atualização seja instalada
- Recomendamos que clientes instalem a atualização liberada no **Boletim de Segurança MS03-039** para se protegerem contra softwares maliciosos.
-

Worm Blaster

- Se o seu computador está infectado, o seu computador poderá operar normalmente, poderá parecer lento, ou poderá reiniciar a cada poucos minutos sem o seu comando.

Cavalo de Tróia

- Conta a mitologia grega que o "Cavalo de Tróia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso a cidade de Tróia
- A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia
- Daí surgiram os termos "Presente de Grego" e "Cavalo de Tróia".
- Na informática, um cavalo de tróia (*trojan horse*) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Cavalo de Tróia

- Assim como o mitológico cavalo de Tróia parecia ser um presente, mas na verdade escondia soldados gregos em seu interior que tomaram a cidade de Tróia, os cavalo de Tróia da atualidade são programas de computador que parecem ser úteis, mas na verdade comprometem a sua segurança e causam muitos danos
- Um cavalo de Tróia recente apresentava-se como um email com anexos de supostas atualizações de segurança da Microsoft, mas na verdade era um vírus que tentava desativar programas antivírus e firewalls

Cavalo de Tróia

- Um programa de computador que parece ser útil, mas na verdade causa danos
- Os cavalos de Tróia se alastram quando as pessoas são seduzidas a abrir o programa por pensar que vem de uma fonte legítima
- Para proteger melhor os usuários, as empresas enviam com freqüência boletins de segurança via email, mas eles nunca contêm anexos
- Também são publicados alertas de segurança antes de enviá-los a clientes

Cavalo de Tróia

- Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:
  - instalação de *keyloggers* ou *screenloggers*
  - furto de senhas e outras informações sensíveis, como números de cartões de crédito;
  - inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador;
  - alteração ou destruição de arquivos

Cavalo de Tróia

- Por definição, o cavalo de tróia distingue-se de um vírus ou de um *worm* por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.
- Normalmente um cavalo de tróia consiste em um único arquivo que necessita ser explicitamente executado.
- Podem existir casos onde um cavalo de tróia contenha um vírus ou *worm*
- Mas mesmo nestes casos é possível distinguir as ações realizadas como conseqüência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou *worm*

Cavalo de Tróia

- É necessário que o cavalo de tróia seja executado para que ele se instale em um computador
- Geralmente um cavalo de tróia vem anexado a um *e-mail* ou está disponível em algum *site* na Internet.
- Os cavalos de Tróia também podem ser incluídos em software que você baixa gratuitamente
- Nunca baixe software de uma fonte em que você não confia
- Sempre baixe as atualizações e patches da Microsoft a partir do **Microsoft Windows Update** ou do **Microsoft Office Update**

Cavalo de Tróia

- Cavalos de Tróia de acesso remoto (RATs – Remote Access Trojan) são programas de software mal-intencionados que os criminosos usam para controlar seu computador por meio de sua conexão com a Internet.
- Um RAT pode permitir que um criminoso exiba e altere os arquivos e funções de seu computador, monitore e registre suas atividades e use seu computador para atacar outros computadores sem o seu conhecimento.

Cavalo de Tróia

- Normalmente, os RATs estão ocultos em programas de software ilegais e outros arquivos e programas que você pode baixar da Internet
- Eles também podem aparecer em mensagens de email ou em mensagens instantâneas, disfarçados de anexos como imagens engraçadas, cartões de saudações ou arquivos de áudio e vídeo
- Se você clicar no anexo para abri-lo, um RAT também pode ser baixado sem o seu conhecimento
- Às vezes, um RAT pode atingir seu computador sem que você execute qualquer ação, aproveitando as vulnerabilidades de software ou da Internet

Cavalo de Tróia

- Um RAT fornece controle remoto sobre seu computador por meio de sua conexão com a Internet
- Os criminosos podem usar essa capacidade para:
  - Expor você a golpes
    - Alguns programas de RAT podem fazer com que você acredite que um site fraudulento seja realmente um site confiável (como um site bancário online)
    - Senhas e outras informações fornecidas no site fraudulento podem ser usadas para roubar seu dinheiro ou sua identidade.
  - Localizar seus arquivos e exibi-los, copiá-los, alterá-los ou excluí-los
    - Os RATs podem ser programados para fazer isso uma vez ou para executar essas tarefas automaticamente sempre que você reiniciar seu computador
  - Registrar o que você digita e enviar essas informações para outro computador
    - Os criminosos processam essas informações por meio de software especial que os ajuda a localizar os nomes de usuário e senhas que você digitou em seu computador

Cavalo de Tróia

- Os criminosos podem usar essa capacidade para:
  - Capturar vídeo e áudio de dispositivos que você conectou a seu computador, salvar a mídia em arquivos e enviá-los para o computador do criminoso
  - Executar ou encerrar um programa, processo ou conexão em seu computador.
  - Criar pop-ups exibidos na tela para perturbá-lo ou para fazer com que você visite sites mal-intencionados.
  - Atacar outros computadores
    - Alguns RATs são usados para formar **"exércitos de zumbis",** que são grandes grupos de computadores controlados por criminosos para que possam executar tarefas como sobrecarregar servidores com mensagens ou espalhar vírus ou spyware

Cavalo de Tróia

- **Como ajudar a se proteger de RATs**
- Pratique uma comunicação online segura
  - Só compartilhe seu endereço principal de email com pessoas conhecidas
  - Evite listar seu endereço de email em grandes diretórios da Internet e em sites de empregos e tenha cuidado ao participar de grupos de usuários online
  - Não abra anexos em mensagens instantâneas ou de email, a menos que tenha certeza do que são e de quem são
  - Leia Como lidar com emails suspeitos.

Cavalo de Tróia

- **Como ajudar a se proteger de RATs**
- Use software confiável de empresas conhecidas
  - A Internet está repleta de programas de software que oferecem divertimento ou funções úteis a um preço baixo ou de graça
  - No entanto, o custo real às vezes está oculto no software mal-intencionado que acompanha esses produtos
  - Verifique com cuidado antes de executar, baixar ou usar qualquer software que não seja de uma fonte conhecida e confiável.

Cavalo de Tróia

- **Como ajudar a se proteger de RATs**
- Use um firewall
  - Um firewall é um programa de software ou um hardware que pode eliminar RATS ou outro software mal-intencionado
  - Se você usa o Windows Vista ou o Windows XP Service Pack 2 (SP2), você já possui um firewall incorporado e ativado por padrão
  - Se você não usa esses sistemas operacionais, consulte **Como ativar seu firewall**.

Cavalo de Tróia

- **Como ajudar a se proteger de RATs**
- Mantenha seu computador atualizado
  - Visite **Microsoft Update** para ajudar a garantir que você tenha as atualizações mais recentes para seu computador
- Use um software antivírus e mantenha-o atualizado
  - Um software antivírus pode ajudar a proteger contra alguns RATS
- Use um software antispyware e mantenha-o atualizado
  - Um software antispyware, como o Windows Defender, pode oferecer proteção contra alguns RATS

Spam

- Spam é o termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas

Spam

- Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *Unsolicited Commercial E-mail*).

Spam *Zombies*

- São computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como *worms*, *bots*, vírus e cavalos de tróia
- Estes códigos maliciosos, uma vez instalados, permitem que *spammers* utilizem a máquina para o envio de spam, sem o conhecimento do usuário
- Enquanto utilizam máquinas comprometidas para executar suas atividades, dificultam a identificação da origem do spam e dos autores também
- Os spam *zombies* são muito explorados pelos *spammers*, por proporcionar o anonimato que tanto os protege.

Spam

- Desde o primeiro spam registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias
- Atualmente, o spam está associado a ataques à segurança da Internet e do usuário, propagando vírus e golpes
- Tão preocupante quanto o aumento desenfreado do volume de spam na rede, é a sua natureza e seus objetivos

Spam

- Problemas causados
  - Não recebimento de e-mails
  - Gasto desnecessário de tempo:
  - Aumento de custos
  - Perda de produtividade
  - Conteúdo impróprio ou ofensivo
  - Prejuízos financeiros causados por fraude

Tipos de Spam

- Correntes (*chain letters*)
  - pede para que o usuário (destinatário) repasse a mensagem um determinado número de vezes ou, ainda, "para todos os amigos" ou "para todos que ama"
- Boatos (*hoaxes*) e
  - os boatos geralmente contam histórias alarmantes e falsas, sensibilizando o usuário (destinatário) a continuar a propagação
- Lendas Urbanas
  - São as histórias disseminadas na Internet, sejam elas tristes, alegres, assustadoras ou misteriosas
  - Podem ser confundidas com os boatos, mas, diferem, principalmente, pelas justificativas utilizadas para atrair a atenção do usuário, conferindo veracidade aos relatos.

Tipos de Spam

- Propagandas
  - Os spams com conteúdo de propaganda são conhecidos como UCE (*Unsolicited Comercial E-mail*)
  - A publicidade pode envolver produtos, serviços, pessoas, *sites* etc.
- Ameaças, brincadeiras e difamação
  - envio de grande quantidade de e-mails ou mensagens eletrônicas contendo ameaças, brincadeiras inconvenientes ou difamação de amigos ou ex-(maridos, esposas, namorados e namoradas
- Pornografia
  - envio de material de pornografia por meio de mensagens não solicitadas

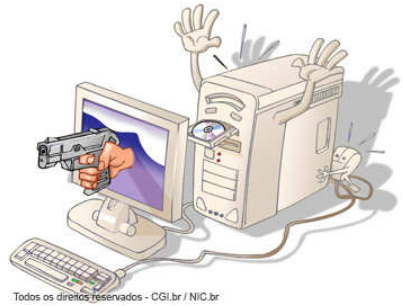
Tipos de Spam

- Códigos maliciosos
  - São programas que executam ações maliciosas em um computador
  - Diversos tipos de códigos maliciosos são inseridos em *e-mails*, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo
- Fraudes
  - Usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados
- Spit e spim
  - Refere-se ao "spam via Internet *Telephony*". Assim, as mensagens não solicitadas também se propagam por outros meios, atingindo os usuários dos "telefones IP" (VoIP)
- Spam via redes de relacionamentos
  - *Orkut* (www.orkut.com), além do *Linked In* (www.linkedin.com) e outros com as mesmas características
  - Esses *sites* propiciam um terreno fértil para a propagação de spam, principalmente, de boatos e propagandas

Golpes (*Scams*)

- Os antigos, já praticados por meio de cartas ou ligações telefônicas, migraram para a Internet, propagados via spam
- Um exemplo é o Golpe da Nigéria, também conhecido como golpe do 419 ou do 171, os famosos "contos do vigário".
- Os golpes nigerianos são classificados como AFF (*advance fee fraud*), ou seja, fraude da antecipação de pagamentos
- Utilizando engenharia social, são elaboradas mensagens longas, contando histórias mirabolantes e pedindo que o usuário envie determinada quantidade de dinheiro, prometendo altas recompensas no futuro, quando o objetivo colocado na história for concretizado

Golpes (*Scams*)

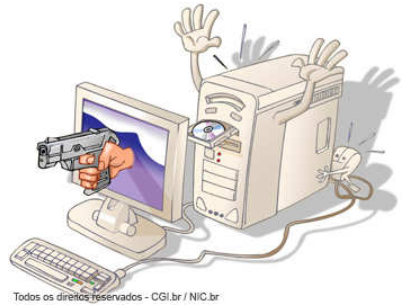


- Ao responder a este tipo de mensagem e efetivar o pagamento antecipado, você não só perderá o dinheiro investido, mas também nunca verá os milhares ou milhões de dólares prometidos como recompensa.
- Normalmente, estas mensagens apresentam quantias astronômicas e abusam da utilização de palavras capitalizadas (todas as letras maiúsculas) para chamar a atenção do usuário
- Palavras como "URGENT" (urgente) e "CONFIDENTIAL" (confidencial) também são comumente usadas no assunto da mensagem para chamar a atenção do usuário

Phishing

- *Phishing*, também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários

Phishing



- A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da Internet
- Atualmente, este termo vêm sendo utilizado também para se referir aos seguintes casos:
  - mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
  - mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

Mensagens que contêm *links* para programas maliciosos

- Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, onde o texto procura atrair sua atenção, seja por curiosidade, por caridade, pela possibilidade de obter alguma vantagem (normalmente financeira), entre outras
- O texto da mensagem também pode indicar que a não execução dos procedimentos descritos acarretarão conseqüências mais sérias, como, por exemplo, a inclusão do seu nome no SPC/SERASA, o cancelamento de um cadastro, da sua conta bancária ou do seu cartão de crédito, etc
- A mensagem, então, procura induzí-lo a clicar em um *link*, para baixar e abrir/executar um arquivo.

Como o fraudador consegue acesso ao seu computador

- Ao clicar no *link* de uma mensagem ou de um site que faz parte de um esquema de fraude, será apresentada uma janela, solicitando que você salve o arquivo
- Depois de salvo, se você abrí-lo ou executá-lo, será instalado um programa malicioso (*malware*) em seu computador, por exemplo, um cavalo de tróia ou outro tipo de *spyware*, projetado para furtar seus dados pessoais e financeiros, como senhas bancárias ou números de cartões de crédito
- Caso o seu programa leitor de *e-mails* esteja configurado para exibir mensagens em HTML, a janela solicitando que você salve o arquivo poderá aparecer automaticamente, sem que você clique no *link*

Adware

- *Adware* (*Advertising software*) é um tipo de *software* especificamente projetado para apresentar propagandas, seja através de um *browser*, seja através de algum outro programa instalado em um computador.
- Em muitos casos, os *adwares* têm sido incorporados a *softwares* e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos
- Um exemplo do uso legítimo de *adwares* pode ser observado no programa de troca instantânea de mensagens MSN Messenger.

Spyware

- O termo **spyware e outros softwares indesejados** refere-se a um software que realiza certas tarefas no seu computador, geralmente sem o seu consentimento
- O software pode exibir anúncios ou tentar coletar informações pessoais sobre você

Spyware

- Spyware é um termo genérico usado para softwares que realizam certas atividades como anúncios, coleta de informações pessoais ou alteração das configurações do seu computador, geralmente sem o seu devido consentimento

Spyware

- Talvez você tenha spyware ou outros softwares indesejados no seu computador se:
  - Você vir anúncios em forma de pop-ups na Web
  - A página que o seu navegador da Web abre primeiro (sua página principal) ou suas configurações de pesquisa do navegador foram alteradas sem seu conhecimento
  - Você nota que há uma nova barra de ferramentas em seu navegador que você não deseja e acha difícil se livrar dela
  - Seu computador leva mais tempo que o normal para finalizar certas tarefas
  - Você percebe um aumento repentino de panes no computador

Spyware

- O spyware está associado a um software de exibição de anúncios (chamado adware) ou a um software que rastreia informações pessoais e confidenciais
- Isso não significa que todo software que exiba anúncios ou controle suas atividades online seja nocivo
- Por exemplo, você pode fazer a assinatura de um serviço de música gratuito, mas "pagar" pelo serviço permitindo que a empresa ofereça anúncios personalizados
- Se você está ciente dos termos e os aceita, pode ser um negócio vantajoso
- Talvez você também aceite que a empresa rastreie suas atividades online para determinar que anúncios devem ser exibidos a você

Spyware

- O spyware pode entrar em seu sistema de várias maneiras
- Um truque comum é a instalação oculta do software durante a instalação de outro software desejado, como um programa de compartilhamento de arquivos de música ou vídeo
- Sempre que instalar algo em seu computador, leia com atenção todas as informações relacionadas, inclusive o contrato de licença e a declaração de privacidade
- Às vezes, a inclusão de um software indesejado em uma determinada instalação de software está documentada, porém isso é mencionado somente no fim de um contrato de licença ou declaração de privacidade
-

Spyware

- Funcionalidades implementadas em *spywares*, que podem ter relação com o uso legítimo ou malicioso:
  - monitoramento de URLs acessadas enquanto o usuário navega na Internet;
  - alteração da página inicial apresentada no *browser* do usuário;
  - varredura dos arquivos armazenados no disco rígido do computador;
  - monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;

Spyware

- Funcionalidades implementadas em *spywares*, que podem ter relação com o uso legítimo ou malicioso:
  - instalação de outros programas *spyware*;
  - monitoramento de teclas digitadas pelo usuário ou regiões da tela próximas ao clique do *mouse*
  - captura de senhas bancárias e números de cartões de crédito
  - captura de outras senhas usadas em *sites* de comércio eletrônico.

Spyware

- Tipos de downloads que podem conter spyware
  - Jogos gratuitos baixados da Internet
  - Programas de compartilhamento de arquivos de música, filmes e outros softwares baixados da Internet ou de outros computadores
  - Figuras animadas para a sua área de trabalho
  - Proteções de tela gratuitas baixadas da Internet
  - Barras de ferramentas para o navegador da Internet
  - Bloqueadores de pop-up gratuitos que aparecem no seu computador quando você está online

Spyware

- Sinais de spyware
  - Vejo anúncios em forma de pop-ups o tempo todo
  - Minhas configurações foram alteradas e não consigo configurá-las de volta ao estado original
  - Meu navegador da Web contém componentes adicionais que eu não me lembro de ter baixado
  - Meu computador parece lento

Spyware

- Para remover spyware
  1. Baixe uma ferramenta de remoção gratuitas e instale-a
  2. Execute a ferramenta para verificar se há spyware ou outros softwares indesejados no seu computador
  3. Verifique os arquivos encontrados pela ferramenta que procurou por spyware e outros softwares indesejados
  4. Selecione os arquivos suspeitos a remover seguindo as instruções da ferramenta.

- Veja a seguir algumas ferramentas que podem ajudá-lo a detectar e remover softwares indesejados do seu computador:
  - Lavasoft Ad Aware
  - Spybot Search & Destroy (S&D)

Spyware

- Como evitar spyware
  - Spyware e outros softwares indesejados podem invadir sua privacidade, bombardeá-lo com janelas de pop-up, tornar seu computador lento e até causar pane no computador

Passo 1: Atualize seu software

Passo 2: Ajuste suas configurações de segurança do navegador Internet Explorer

Passo 3: Use um firewall

Passo 4: Navegue e faça download com mais segurança

Backdoors

- Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão
- Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado.
- A esses programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de ***backdoor***

Backdoors

- A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet)
- Pode ser incluído por um invasor ou através de um cavalo de tróia
- Uma outra forma é a instalação de pacotes de *software*, tais como o ***BackOrifice*** e ***NetBus***, da plataforma Windows, utilizados para administração remota
- Se mal configurados ou utilizados sem o consentimento do usuário, podem ser classificados como *backdoors*

Backdoors

- *Backdoors* podem ser incluídos em computadores executando diversos sistemas operacionais, tais como:
  - Windows (por exemplo, 95/98, NT, 2000, XP)
  - Unix (por exemplo, Linux, Solaris, FreeBSD, OpenBSD, AIX)
  - Mac OS, entre outros.

Keylogger

- *Keylogger* é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador
- Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito
- A ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou *Internet Banking*
- Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).

Keylogger

- As instituições financeiras desenvolveram os teclados virtuais para evitar que os *keyloggers* pudessem capturar informações sensíveis de usuários
- Então, foram desenvolvidas formas mais avançadas de *keyloggers*, também conhecidas como *screenloggers*
- De posse destas informações um atacante pode, por exemplo, descobrir a senha de acesso ao banco utilizada por um usuário

Keylogger

- Normalmente, o *keylogger* vem como parte de um programa *spyware* ou cavalo de tróia
- Desta forma, é necessário que este programa seja executado para que o *keylogger* se instale em um computador
- Geralmente, tais programas vêm anexados a *e-mails* ou estão disponíveis em *sites* na Internet

Screenlogger

- Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado
- Capazes de:
  - armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou
  - armazenar a região que circunda a posição onde o *mouse* é clicado.
-

Bot

- O *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador
- Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente

Bot

- Normalmente, o *bot* se conecta a um servidor de IRC (*Internet Relay Chat*) e entra em um canal (sala) determinado
- Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão sendo enviadas para este canal
- O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*
- Estas seqüências de caracteres correspondem a instruções que devem ser executadas pelo *bot*

Bot

- Um invasor, ao se comunicar com um *bot*, pode enviar instruções para que ele realize diversas atividades, tais como:
  - desferir ataques na Internet;
  - executar um ataque de negação de serviço
  - furtar dados do computador onde está sendo executado, como por exemplo números de cartões de crédito;
  - enviar *e-mails* de *phishing*
  - enviar *spam*

Botnet

- *Botnets* são redes formadas por computadores infectados com *bots*
- Estas redes podem ser compostas por centenas ou milhares de computadores
- Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, desferir ataques de negação de serviço, etc.

Rootkits

- Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido
- O conjunto de programas que fornece estes mecanismos é conhecido como ***rootkit***
- É muito importante ficar claro que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para mantê-lo
- Isto significa que o invasor, após instalar o *rootkit*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador

Rootkits

- Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podem ser citados:
  - programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como arquivos, diretórios, processos, conexões de rede, etc;
  - *backdoors*, para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos *rootkits*);
  - programas para remoção de evidências em arquivos de *logs*;

Rootkits

- Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podem ser citados:
  - *sniffers*, para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
  - *scanners*, para mapear potenciais vulnerabilidades em outros computadores;
  - outros tipos de *malware*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

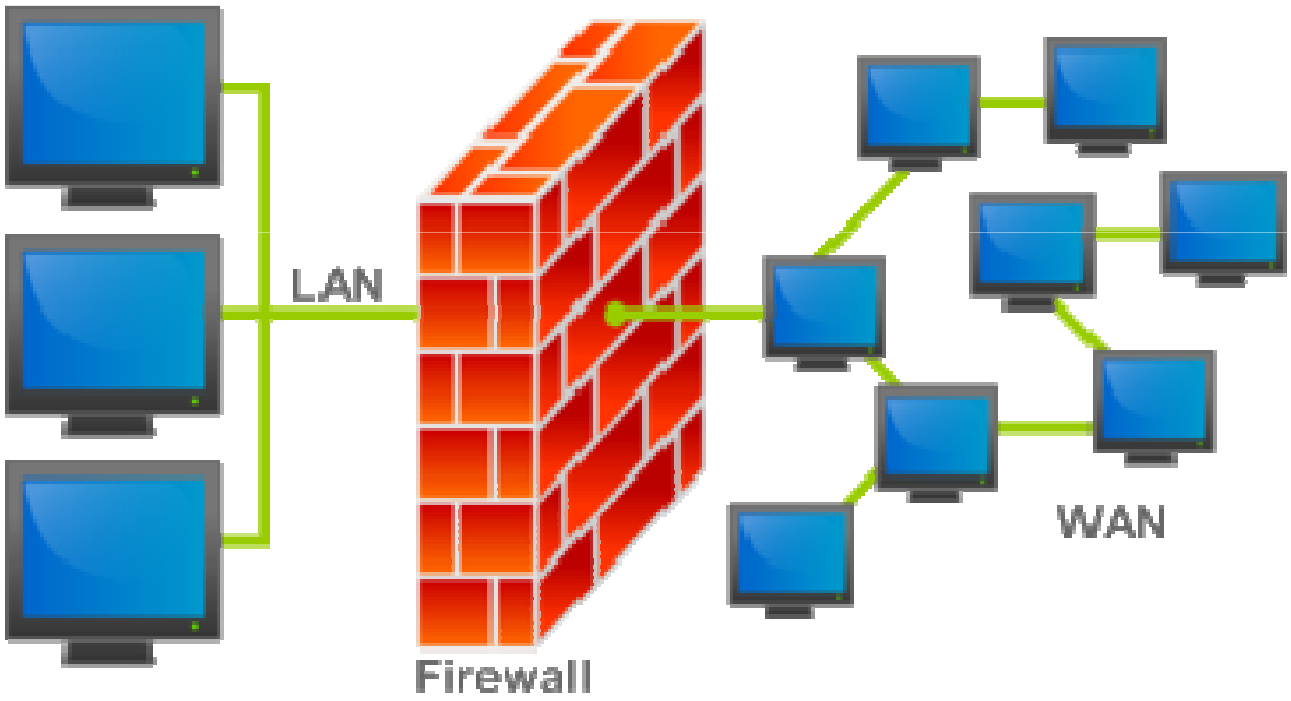
Engenharia Social

- Não fornecer dados pessoais, números de cartões e senhas através de contato telefônico;
- Ficar atento a *e-mails* ou telefonemas solicitando informações pessoais;
- Não acessar *sites* ou seguir *links* recebidos por *e-mail* ou presentes em páginas sobre as quais não se saiba a procedência;
- Sempre que houver dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entrar em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.

Firewall - Conceito

- Nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede
- Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra
- Logicamente falando, um firewall é um separador, um bloqueador e um analisador, enquanto a implementação física varia de site para site, podendo ser, por exemplo, um roteador, um computador, ou uma combinação de roteadores e computadores

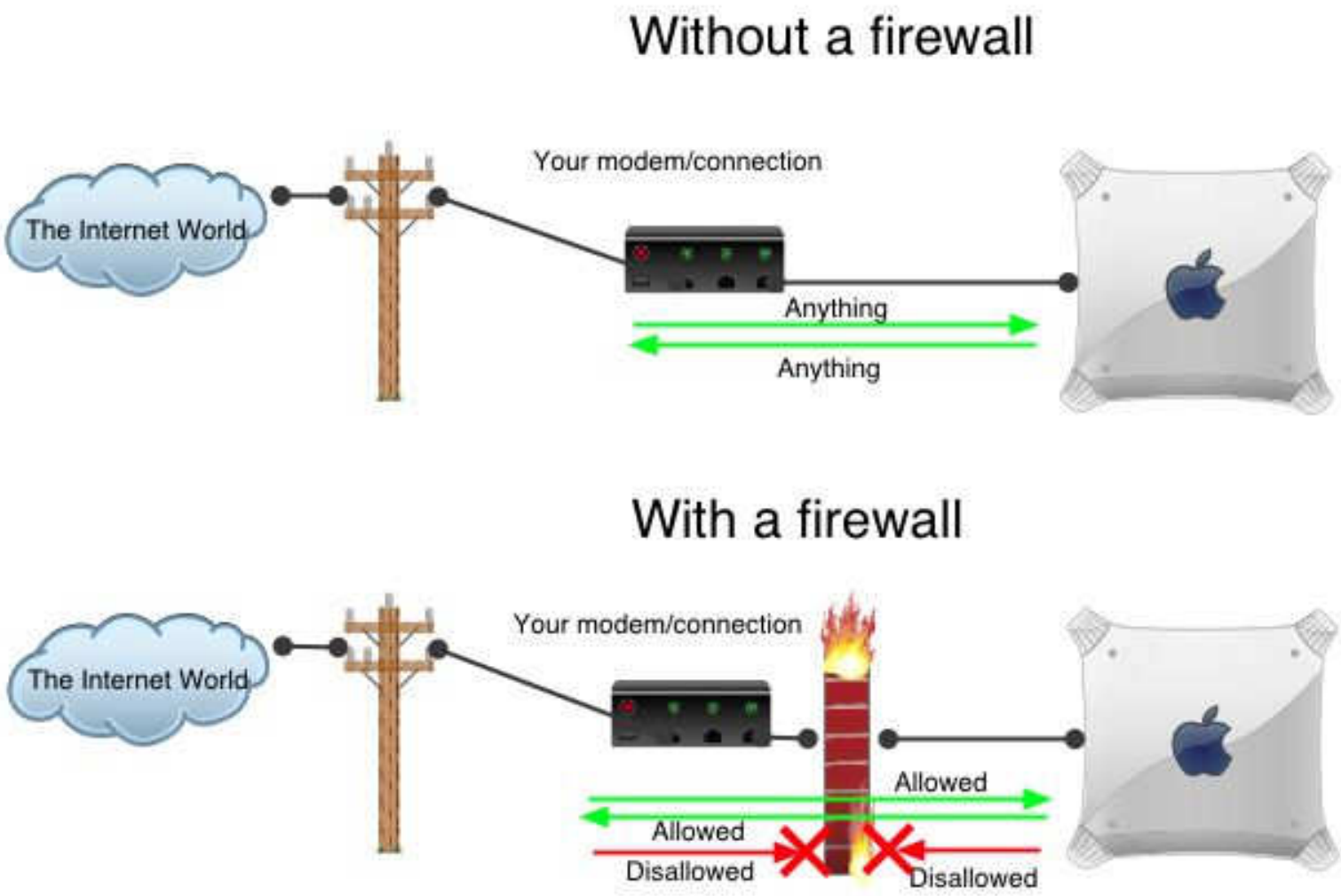
Firewall - Conceito



Firewall - Conceito

- Uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet)
- Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados
- Mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e a filtragem de dados

Firewall


Without a firewall
Your modem/connection
The Internet World
Anything
Anything
With a firewall
Your modem/connection
The Internet World
Allowed
Allowed
Disallowed
Disallowed

História

- Os sistemas *firewall* nasceram no final dos anos 80, fruto da necessidade de criar restrição de acesso entre as redes existentes
- Nesta época a expansão das redes acadêmicas e militares, que culminou com a formação da ARPANET e, posteriormente, a Internet e a popularização dos primeiros computadores tornou-se um prato cheio para a incipiente comunidade *hacker*
- Casos de invasões de redes, de acessos indevidos a sistemas e de fraudes em sistemas de telefonia começaram a surgir, e foram retratados no filme *Jogos de Guerra* ("***War Games***"), de 1983

História

- Em 1988, administradores de rede identificaram o que se tornou a primeira grande infestação de vírus de computador e que ficou conhecido como **Internet Worm**
- Em menos de 24 horas, o ***worm*** escrito por ***Robert T. Morris Jr*** disseminou-se por todos os sistemas da então existente Internet (formado exclusivamente por redes de ensino e governamentais), provocando um verdadeiro "apagão" na rede

Referências

- http://www.microsoft.com/brasil/athome/security/viruses/intro_viruses_what.mspx
- http://www.microsoft.com/brasil/athome/security/viruses/virus101.mspx
- http://www.microsoft.com/brasil/athome/security/spyware/default.mspx
- http://cartilha.cert.br/malware/sec1.html#sec1