FACULDADE PITÁGORAS

PRONATEC

DISCIPLINA: SEGURANÇA DA INFORMAÇÃO

Prof. Msc. Carlos José Giudice dos Santos

Conteúdo Programático

Unidade 04
Ameaças à Segurança da Informação

- Classificação dos tipos de ameaças
- Vírus (tipos)
- Worms
- Spywares
- Trojans (backdoors)

AMEAÇAS À SEGURANÇA [1]

As ameaças são qualquer causa potencial de um incidente indesejado, que caso se concretize possa resultar em dano aos dados de um computador.

Ameaças exploram as falhas de segurança, que são os pontos fracos do conjunto hardware e software dos computadores, e, como consequência, provocam perdas ou danos aos valores de uma empresa, afetando seus negócios.

Ameaça pode ser uma pessoa, alguma coisa, um evento ou uma ideia capaz de causar dano a um recurso, alcançando um ou mais objetivos (ética, confiabilidade, integridade e disponibilidade).

AMEAÇAS À SEGURANÇA [2]

As ameaças exploram as vulnerabilidades ou fragilidades do sistema de informações para causar impactos, da mesma forma que um assaltante explora o descuido de terceiros que andam pelas ruas, distraidamente, falando ao celular (você está vulnerável).

A análise de ameaças e vulnerabilidades tenta definir qual a probabilidade de ocorrência de cada evento adverso e as consequências da quebra da segurança da informação.

AMEAÇAS À SEGURANÇA [3]
EXEMPLOS DE AMEAÇAS

- **Vulnerabilidade**: dormir de janela aberta.
- **Ameaça**: assalto.
- **Aspecto afetado**: integridade.
- **Impacto**: perda de conforto, bens, valores financeiros.

É como antes de sair de casa, você analisar como está o movimento nas ruas, se existem pessoas suspeitas circulando, se você não está chamando a atenção com suas roupas ou mochila, por exemplo, e analisar quais as chances de ser assaltado se for caminhando até um supermercado ou casa de um amigo e ainda mais, considerar na análise se você estiver com problemas físicos para em caso de necessidade de sair correndo e usar este recurso como opção de fugir de uma tentativa de assalto com mais segurança.

AMEAÇAS À SEGURANÇA [4]

A análise de impactos identifica os recursos críticos do sistema, ou seja, aqueles que mais sofrerão impactos na ocorrência de quebra de segurança.

Exemplo

Qual das situações seria mais impactante?

Roubarem seu celular, ou sua mochila, e saírem correndo,

ou

um assaltante dar um tiro ou uma facada em você para roubar seus pertences?

AMEAÇAS À SEGURANÇA [5]

Ameaça: é um evento ou atitude indesejável (roubo, incêndio, vírus etc) que potencialmente remove, desabilita, danifica ou destrói um recurso necessário e importante para você ou para uma empresa.

Vulnerabilidade: é uma fraqueza ou uma deficiência que pode ser explorada por uma ameaça. Normalmente ela está associada à possibilidade desta ameaça acontecer e aos problemas que esta ameaça irá ou poderá causar aos dados de um computador ou a uma rede de computadores.

Existem quatro tipos de ameaças fundamentais (aquelas que afetam os princípios da segurança da informação): 1) vazamento de informações; 2) violação de integridade; 3) indisponibilidade de serviços de informática; e 4) acesso e uso não autorizado.

1. Vazamento de Informações

Este é o primeiro tipo de ameaça fundamental à segurança da informação. O vazamento ou a disponibilização externa de dados de uma empresa pode acontecer de duas formas:

a) **Involuntária**: provocada por falha de hardware, desastres naturais, mensagem enviada a um endereço incorreto, erros de programação, erros de um usuário provocado por algum desconhecimento, tais como hierarquia, procedimentos, valores, entre outro, ou também por bugs (falhas) de software etc.;

b) **Voluntária**: este tipo, normalmente realizado por pessoas mal-intencionadas, consiste no roubo deliberado de dados, espionagem entre empresas ou organizações, fraudes por meio de adulteração de dados com identificação de usuários roubada, sabotagem, invasão de sites por hackers etc.

2. Violação de Integridade

O segundo tipo de ameaça fundamental consiste no comprometimento da consistência dos dados ou do sistema por intermédio de alterações não autorizadas de dados.

Podem ser considerados como violação de integridade a alteração da página de abertura de um site, um erro de software que, por exemplo, aumente por engano os salários de todos os funcionários de uma empresa ou apenas de um grupo de funcionários.

Esta violação também pode ser considerada voluntária ou involuntária.

3. Indisponibilidade de Serviços [1]

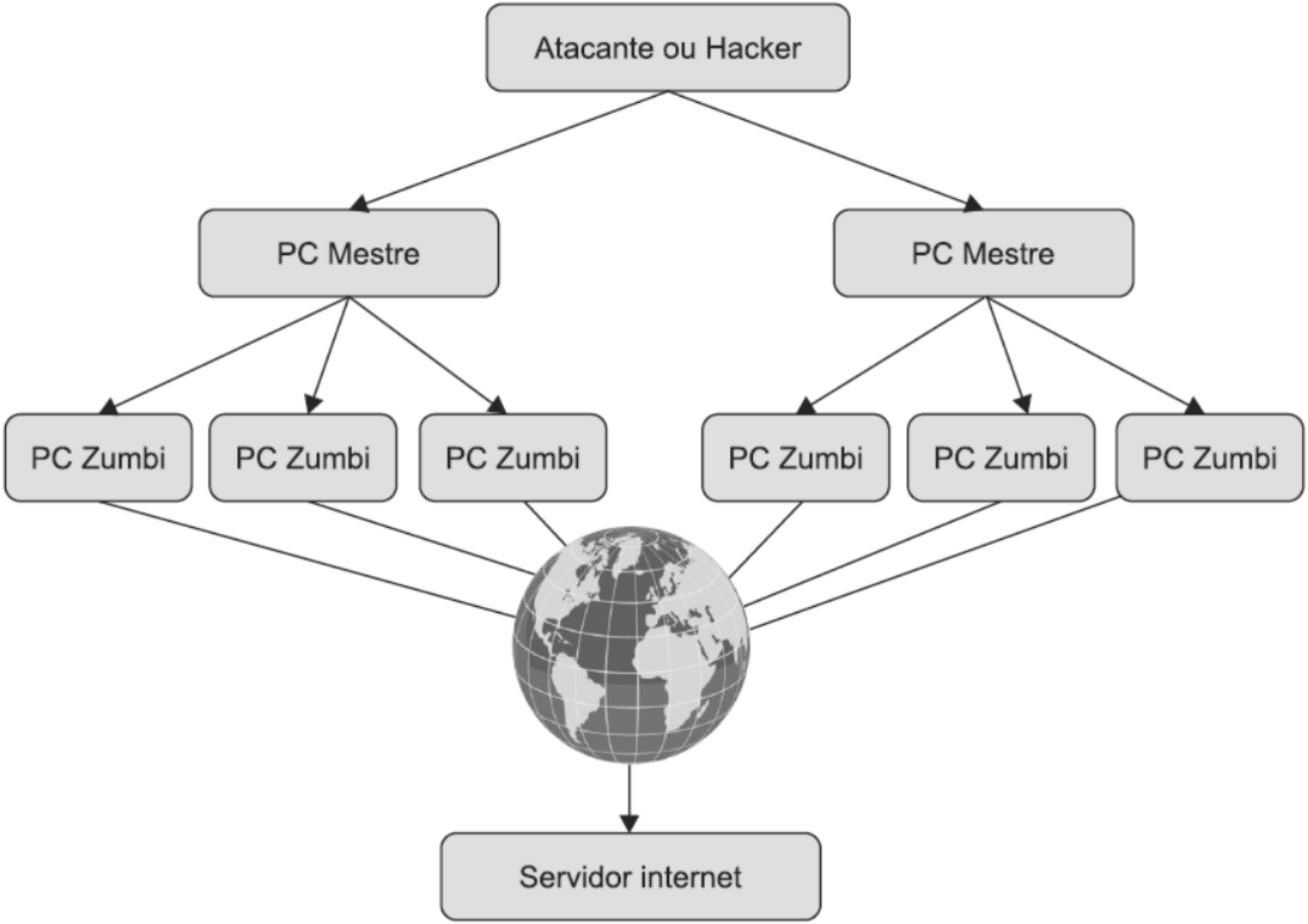
O terceiro tipo de ameaça fundamental configura-se como o impedimento deliberado do acesso aos recursos computacionais por usuários autorizados ou não.

Os ataques DoS (sigla para *Denial of Service*), por exemplo, são "ataques para causar negação de serviços de um site da internet". Eles são uma tentativa de fazer com que computadores – chamados de servidores Web – tenham muita dificuldade, ou até mesmo sejam impedidos, de executar suas tarefas.

Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina central de uma rede receba tantas requisições, até que não consiga atendê-las, ficando desta forma indisponível.

3. Indisponibilidade de Serviços [2]

Outro ataque deste tipo é o ataque DDoS (*Distributed Denial of Service*).



3. Indisponibilidade de Serviços [3]

Para entendermos a diferença entre eles, explicamos que este tipo de ataque se caracteriza por ser de grandes dimensões. Ele pode utilizar milhares de computadores infectados, que atuam como zumbis – por isso chama-se Distributed (Distribuído) –, para atacar uma determinada máquina (servidor Web), onde estão localizadas as páginas de um determinado site de uma empresa. Assim serão distribuídas estas ações de acesso simultâneo entre as milhares de máquinas zumbis.

Esse tipo de ataque, que aparece constantemente em jornais ou em publicações da internet, é o ataque mais comum à disponibilidade de informações.

3. Indisponibilidade de Serviços [4]

Em outras palavras, o computador fica tão sobrecarregado que nega os serviços ou acessos a um site. Você tenta acessar o site, mas ele não responde.

O interessante é que eles não têm como objetivo roubar dados, e sim "brincar", se é que se pode dizer isto. Eles tiram do ar sites de grandes empresas, principalmente as que prestam serviços comerciais, ou sites governamentais, o que caracteriza um procedimento mal-intencionado, não podendo ainda ser considerado como um ato criminoso em si.

4. Acesso e uso não autorizado

Acontece quando um recurso de algum sistema, site ou rede (um programa, dados, um relatório) é utilizado por uma pessoa não autorizada ou de forma não autorizada.

É comum em casos de roubo de senhas pessoais de acesso, quando, então, terceiros passam a acessar informações às quais não teriam acesso autorizado. Ou, ainda, em ataques diretos aos bancos de dados de uma rede.

Veremos, mais à frente, o que são trojans e como eles capturam senhas de rede, sites, bancos de dados, pessoal ou corporativo, e até mesmo bancários.

Outros tipos de ameaças [1]

Existem outros tipos de ameaças que, ao se efetivarem em um ataque, permitem a realização de uma ou mais ameaças fundamentais. Ou seja, são ameaças mistas e poderiam ter duas ou mais das classificações fundamentais.

Mascaramento: Quando alguma coisa (pessoa ou programa) se faz passar por outra.

Desvio de controles (bypass): Quando um hacker, por exemplo, explora falhas de um sistema e suas vulnerabilidades de segurança, burlando os controles para obter direitos de acesso não autorizados.

Outros tipos de ameaças [2]

Violação autorizada: Um usuário ou programa autorizado usa o sistema com propósitos ou em funções não autorizados.

Ameaças programadas: São códigos de software que se instalam em um sistema ou computador com o objetivo de comprometer sua segurança, alterando ou destruindo dados ou sistemas.

Outras ameaças comuns atualmente são os vírus, worms e trojans.

Vírus [1]

Um vírus é um pequeno programa escrito com o objetivo de alterar a forma como um computador opera, sem a permissão ou o conhecimento do usuário.

Denominam-se vírus os programas que possuem as seguintes características

1. São sempre autoexecutáveis. Geralmente, um vírus adiciona o seu próprio código no caminho de execução de outro programa. Ele associa-se a outro programa normal inserindo seu código de execução no outro;
2. Um vírus normalmente duplica a si próprio. Por exemplo, pode substituir outros arquivos executáveis por uma cópia do arquivo infectado por vírus. Os vírus podem infectar tanto desktops quanto servidores de rede.

Vírus [2]

Muitos dos vírus são programados para danificar o computador, corrompendo programas, apagando arquivos ou mesmo formatando o disco rígido (a pior das possibilidades).

Outros não são desenvolvidos para causar danos. Eles são criados apenas para se multiplicar e se tornar conhecidos por meio de mensagens de texto, vídeo e áudio.

Mesmo inofensivos, esses vírus podem criar problemas para o usuário do equipamento, pois interferem no funcionamento da memória do computador, que deveria estar sendo utilizada por programas legítimos.

Vírus [3]

Isso faz com que o desempenho dos computadores fique irregular e lento. Eles, inclusive, podem provocar um travamento completo do computador.

Além disso, diversos vírus provocam erros, que podem causar, além do travamento do sistema operacional, a perda significativa de dados.

Ambos, vírus e worms, são pragas virtuais que "infectam" o computador da vítima e causam algum tipo de dano ou prejuízo.

Mas as semelhanças param por aí. Para entendermos melhor, faremos, uma comparação entre vírus e vermes em um ambiente biológico.

Vírus [4]

Um vírus e um verme (worm) para computadores têm mais ou menos a mesma diferença que existe entre um vírus e um verme biológicos.

No ambiente biológico, um verme é um ser vivo completo, pluricelular e às vezes até visível a olho nu. Ele tem todas as funções biológicas necessárias para sobreviver. Mesmo que seja um parasita e roube alimento do corpo do hospedeiro, ainda assim é um ser vivo completo e autônomo.

Já um vírus é um ser vivo muito mais simples. Tão simples que sequer pode ser considerado como unicelular, já que ele nem é uma célula completa.

Vírus [5]

Ao contrário do verme, o vírus não é autônomo. Quando uma pessoa fica infectada (com o vírus da gripe, por exemplo), o vírus usa a estrutura das células humanas para se "completar". Ao contrário do verme, portanto, o vírus não existe sem as funções básicas providas pelas células animais.

Um vírus normalmente exige um processo, ou mecanismos de entrega (chamado de vetor), algo como um arquivo .zip ou algum outro arquivo executável anexado a um e-mail, para transportar o código do vírus de um local para o sistema.

O principal elemento que distingue um worm de um vírus de computador é essa necessidade de interação humana para facilitar e possibilitar a difusão de um vírus.

Trojan ou Cavalo de Troia [1]

Os cavalos de troia ou trojans são programas impostores ou arquivos que se passam por um programa desejável, mas que, na verdade, são prejudiciais.

Uma distinção importante entre programas cavalo de troia e os vírus efetivamente é que os trojans não se autoduplicam.

Os programas do tipo cavalo de troia contêm códigos maliciosos que, quando ativados, causam a perda e normalmente o roubo de dados, senhas de acesso etc.

Para que um cavalo de troia possa se espalhar, o próprio usuário deve instalá-lo no computador, mesmo que inconscientemente.

Trojan ou Cavalo de Troia [2]

Por exemplo, os casos mais comuns se dão ao abrir um anexo de e-mail, ao fazer downloads ou executar um arquivo diretamente da internet.

Como na lenda grega Ilíada, o cavalo de troia parece algo simples, sem maldade. Porém, quando aberto (ou melhor, executado), apresenta os vários soldados gregos que durante a noite abriram os portões da cidade para a entrada de mais soldados e a consequente dominação da cidade de Troia (no nosso caso o seu computador ou uma rede de computadores).

Há diferentes tipos de trojans, classificados conforme o tipo de ações maliciosas que executam ao infectar um computador. Alguns destes tipos são:

Trojan ou Cavalo de Troia [3]

- **Trojan Downloader**: instala outros códigos maliciosos, obtidos em sites.
- **Trojan Dropper**: instala outros códigos maliciosos que estão embutidos no próprio código do trojan.
- **Trojan Backdoor**: inclui backdoors, possibilitando o acesso remoto do atacante ao computador.
- **Trojan DoS**: instala ferramentas para a negação de serviço e as utiliza para desferir ataques.
- **Trojan Destrutivo**: altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.

Trojan ou Cavalo de Troia [4]

- **Trojan Clicker**: redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
- **Trojan Proxy**: instala um servidor proxy, possibilitando que o computador seja utilizado para navegação totalmente anônima e para envio de spam.
- **Trojan Spy**: instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las para um atacante.
- **Trojan Banker ou Bancos**: coleta dados bancários do usuário por meio da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy, porém com objetivos mais específicos.

Worms [1]

Worms (vermes) são programas que se duplicam, passando de um sistema para outro, sem utilizar um arquivo host (arquivo hospedeiro).

Portanto, os worms se diferenciam dos vírus, os quais requerem a existência de um arquivo host (arquivo hospedeiro) infectado e que seja espalhado.

Embora os worms geralmente existam dentro de outros arquivos, como documentos do Word ou Excel, há uma diferença no modo com que worms e vírus utilizam o arquivo hospedeiro.

Em geral, o worm cria um documento que já vem com um programa macro "worm" integrado ao documento.

Worms [2]

Quando o documento inteiro for passado de um computador a outro, ele pode ser considerado um worm.

Normalmente, worms são programas autossuficientes que atacam um sistema qualquer e exploram uma vulnerabilidade específica neste sistema.

Assim que houver a exploração bem-sucedida da vulnerabilidade, o worm copia seu programa do host de ataque para o sistema recém-explorado para começar o ciclo novamente.

Em janeiro de 2007, um worm infectou a conhecida comunidade MySpace. Usuários confiáveis habilitaram a propagação do worm, que começou a se replicar nos sites dos usuários com a desfiguração "w0rm.EricAndrew".

Exemplo de worm: O W32.Mydoom.AX@mm.

Tipos de Vírus

Os vírus conhecidos possuem cinco classificações:

1. Vírus de infecção de arquivo;
2. Vírus de setor de inicialização;
3. Vírus do registro mestre de inicialização;
4. Vírus múltiplos;
5. Vírus de macro.

Veremos as características de cada um destes tipos.

É necessário que você saiba identificar e dominar a tipologia (tipo de vírus que está infectando um computador), para poder no futuro reconhecê-los pelo seu comportamento e saber como combatê- los e evitá-los.

Vírus de infecção de arquivo [1]

Esses vírus têm como principal característica infectar arquivos de programas já instalados no computador. Em geral os arquivos infectados são aqueles com extensão .exe, .dll, .com, entre outros.

Geralmente, infectam códigos executáveis, arquivos que possuem extensão .com e .exe. Se prestarmos atenção, observaremos que quando executamos uma varredura com um programa antivírus, ele geralmente mostra a mensagem: "procurando na memória".

Entretanto, também podem infectar outros arquivos não executáveis, o que acontece quando um programa infectado é executado a partir de uma mídia removível, como um pen drive, ou na própria rede.

Vírus de infecção de arquivo [2]

Muitos desses vírus ficam residentes na memória do computador infectado.

Depois que a memória é infectada, qualquer arquivo executável não infectado que for executado irá tornar-se também um arquivo infectado, inclusive um programa antivírus.

Exemplos de alguns vírus de infecção de arquivos: *Jerusalém* e *Cascade* (ambos para o sistema DOS).

Vírus de setor de inicialização (boot) [1]

Os vírus de setor de inicialização são aqueles que infectam a área do sistema operacional de um disco ou o registro de inicialização de mídias removíveis regraváveis e discos rígidos.

O MBR (Master Boot Record – Registro Mestre de Boot) é o setor onde ficam os carregadores, isto é, os arquivos do sistema operacional do computador.

O registro mestre de inicialização fica no primeiro setor da unidade de disco rígido. Ele identifica onde a partição ativa está e inicia em seguida o programa de reinicialização para o setor de inicialização dessa partição.

Vírus de setor de inicialização (boot) [2]

O setor de inicialização identifica onde o sistema operacional está localizado e ativa as informações de inicialização a serem carregadas na RAM do computador. O registro mestre de inicialização inclui uma tabela que localiza cada partição presente na unidade de disco rígido.

Geralmente ele registra as partições primárias do disco rígido, onde há as chamadas imagens de boot (geralmente um arquivo .img ou .bin) em que existe uma cópia do sistema operacional do computador.

Ao ligar o computador, dependendo da sequência de boot, a BIOS procura por uma imagem de boot conforme a configuração de boot primária no disco rígido do computador (setup) ou na unidade de CD/DVD.

Vírus de setor de inicialização (boot) [3]

Quando ele efetua a busca no disco rígido, procura primeiro na MBR. Se ela não encontrar a imagem, aparecerá uma mensagem informando que o disco está sem sistema. Em seguida, o computador parará ou solicitará que o usuário tecle "enter" para carregar o sistema do CD/DVD, ou "esc" para sair.

Se achar, o sistema é carregado e passa à execução dessa imagem de boot, que carrega o sistema operacional no computador.

Todos os discos rígidos (incluindo discos contendo somente dados) contêm um pequeno programa no seu registro de inicialização que é executado quando o computador é iniciado.

Vírus de setor de inicialização (boot) [4]

Os vírus do setor de inicialização se anexam a essa parte do disco e são automaticamente ativados quando o usuário tenta iniciar o computador a partir de um disco rígido infectado, ou de um pen-drive ou CD/DVD também infectado.

Esses vírus sempre são residentes, ou melhor, ficam gravados na memória do computador.

A maioria deles é escrita para DOS. Porém, todos os computadores, independente de qual seja o seu sistema operacional, são alvos potenciais desse tipo de vírus.

Para que o computador seja infectado, basta uma tentativa de inicializá-lo utilizando um disco rígido infectado, ou outro tipo de mídia removível.

Vírus de setor de inicialização (boot) [5]

A partir deste momento, enquanto o vírus permanecer na memória, todos os discos ou mídias removíveis que não forem protegidos contra a gravação se tornarão infectados ao ser acessados.

Alguns exemplos destes vírus são: *Form*, *Disk Killer*, *Michelangelo* e *Stoned*.

Vírus do registro mestre de inicialização [1]

Os vírus do registro mestre de inicialização residem também na memória e infectam os discos da mesma forma que os vírus do setor de inicialização.

A diferença entre esses dois tipos é a localização do código com vírus. Os vírus do registro mestre de inicialização geralmente salvam uma cópia legítima deste registro mestre em um local diferente.

Os computadores com sistema operacional Windows NT (Server) que forem infectados por vírus do setor de inicialização ou vírus do setor de inicialização mestre não podem mais ser inicializados.

Isso ocorre em decorrência da diferença no modo em que esse sistema operacional acessa suas informações de inicialização em relação às outras versões do Windows.

Vírus do registro mestre de inicialização [2]

Em um sistema Windows NT (Server) formatado com partições FAT, geralmente é possívelremover o vírus inicializando o sistema via DOS e utilizando um software antivírus.

Se a partição de inicialização for do tipo NTFS, o sistema deverá ser reparado utilizando-se os discos de instalação do Windows (Server).

Alguns exemplos destes vírus são: *NYB*, *AntiExe* e *Unashamed*.

Vírus múltiplos

Os vírus múltiplos (também conhecidos como polypartite) infectam os registros de inicialização e os arquivos de programas.

Esses vírus são considerados os mais difíceis de remover pois se a área de inicialização for limpa por um antivírus, e não os arquivos do computador, essa área será infectada novamente.

O mesmo ocorre se somente os arquivos infectados forem limpos. Se o vírus não for removido da área de inicialização, quaisquer arquivos que tenham sido limpos serão novamente infectados.

Alguns exemplos destes vírus são: One Half, Emperor, Anthrax e Tequilla.

Vírus de macro [1]

Esse tipo de vírus também infecta arquivos de dados, principalmente arquivos do pacote Office.

Ele é um tipo extremamente comum e sua remoção tem sido a mais cara e demorada para as empresas.

Com o advento da utilização do Visual Basic desde a versão do Office 97, um vírus de macro já pode ser criado para infectar não apenas arquivos de dados, mas também outros tipos de arquivos, mesmo que não sejam do pacote Office.

Qualquer tipo de arquivo que possua micros em seu programa de leitura e gravação (como a macro de localização de textos do Word) pode ser infectado por este vírus.

Vírus de macro [2]

Ao utilizarmos alguns programas, como um editor de texto, e necessitarmos executar repetidas vezes em sequência alguma tarefa (por exemplo, substituir todas as ocorrências da palavra "abre" pela palavra "fecha"), por meio da opção pesquisar e substituir, podemos utilizar um comando único para efetuá-las, uma macro interna do programa.

O Word, por exemplo, abre uma janela para a palavra pesquisada e outra para colocar a palavra a ser substituída.

Esse comando é chamado de macro e pode ser salvo em um modelo de programação para ser executado em outros arquivos.

Vírus de macro [3]

Além dessa macro que apresentamos e que é comum no Word, um usuário com domínio da linguagem Visual Basic pode criar um modelo de macro mal-intencionado, com os comandos básicos da linguagem, nos editores de texto, e que também irão funcionar com modelos do Word.

Os vírus de macro atacam justamente esses arquivos, comprometendo o funcionamento do programa.

Os alvos principais são os próprios editores de texto (Word), as planilhas de cálculo (Excel) e, inclusive, arquivos de PowerPoint.

Novos casos de vírus de macro, que já estão infectando também outros programas, têm sido descobertos.

Vírus de macro [4]

Todos esses vírus utilizam a linguagem de programação interna de outro programa, a qual foi criada para permitir que os usuários automatizem certas tarefas naquele programa.

Em decorrência da facilidade com que esses vírus podem ser criados, há milhares deles em circulação.

Alguns exemplos destes vírus são: W97M.Melissa, *WM.NiceDay* e *W97M.Groov*.

Algumas conclusões sobre vírus [1]

Para conhecermos os conceitos que a Symantec, uma das maiores empresas especializadas em software antivírus, nos fornece sobre vírus e para enriquecer nosso conhecimento geral:

Um vírus é um software projetado e escrito para afetar de forma adversa o seu computador ao alterar a forma como ele trabalha sem o seu conhecimento ou permissão.

Em termos mais técnicos, um vírus é um código de programa que se implanta em um dos seus arquivos executáveis e se espalha sistematicamente de um arquivo para outro.

Algumas conclusões sobre vírus [2]

Os vírus de computador não são gerados espontaneamente. Eles precisam ser escritos e ter um objetivo específico. Em geral, um vírus tem duas funções distintas:

I. Ele se dissemina de um arquivo para outro sem sua participação ou conhecimento. Tecnicamente, isso é conhecido como autorreplicação e propagação.

II. Implementa o sintoma ou o dano planejado pelo seu criador.

As suas atividades incluem apagar um disco, corromper seus programas ou simplesmente provocar o caos no seu computador.

Algumas conclusões sobre vírus [3]

Tecnicamente, isso é conhecido como ação do vírus, que pode ser benigna ou maligna conforme a imaginação do seu criador.

Um vírus benigno é um vírus que foi projetado para não provocar danos ao seu computador.

Por exemplo, um vírus que se oculta até uma data ou hora predeterminada e, em seguida, não faz nada mais do que exibir algum tipo de mensagem é considerado benigno.

Um vírus maligno é aquele que tenta causar danos ao seu computador, embora o dano possa não ser intencional.

Algumas conclusões sobre vírus [4]

É significativa a quantidade de vírus desses tipo que causa danos devido a uma programação inadequada e bugs autênticos no código viral.

Um vírus maligno pode alterar um ou mais dos seus programas de modo que ele não funcione como deveria. O programa infectado pode terminar de modo anormal, gravar informações incorretas nos seus documentos ou o vírus pode alterar as informações do diretório em uma das áreas do seu sistema.

Isso pode evitar que a partição seja montada ou você pode não conseguir iniciar um ou mais programas ou os programas podem não conseguir localizar os documentos que você quer abrir.

As ameaças dos worms [1]

Os worms são programas de infecção autossuficientes , que utilizam com frequência técnicas de engenharia social. Eles se utilizam de nomes atrativos, normalmente associados a pessoas famosas, software pirata, conteúdos de caráter sexual e temas da atualidade, para camuflar arquivos suspeitos.

Em geral tentam despertar a curiosidade dos usuários, seja por intermédio de e-mails, endereços normalmente desconhecidos ou até como spam, propagandas de empresas etc.

A utilização deste tipo de técnica aumenta significativamente em épocas de datas festivas, como no dia dos namorados, natal, dia das mães e dia das bruxas.

As ameaças dos worms [2]

Os worms têm evoluído para uma nova dinâmica de formato de ataques dos malwares. O termo malware é proveniente do inglês e significa *malicious software*.

Trata-se de um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o objetivo de causar danos, alterações ou roubar informações, confidenciais ou não.

Em um primeiro momento, os worms eram desenvolvidos principalmente para demonstrar as capacidades de programação dos seus criadores, inflando o ego de jovens programadores. Como tal eram desenvolvidos para se propagar de forma massiva e pouco discreta, infectando computadores por todo o mundo, mas sem objetivos tão maléficos.

As ameaças dos worms [3]

Atualmente, os worms têm objetivos claramente financeiros e são utilizados para criar *botnets* massivas, as quais passam a controlar milhares de computadores em todo o mundo.

Para entender do que se trata uma *botnet* e como esta rede funciona, é necessário saber o que é um bot, seu termo de origem.

Bot, diferente de boot, é um tipo de código (programa) mal-intencionado, um vírus malicioso que transforma o computador infectado em um "zumbi", um morto-vivo, a serviço de alguém que o controla remotamente, da mesma forma que nos ataques DDoS.

As ameaças dos worms [4]

Computadores "zumbis" são computadores que podem ser controlados a distância por um invasor, independente das ações do usuário, e inclusive sem o usuário perceber.

A rede de computadores infectados por um **bot** é chamada de **botnet** (rede zumbi) e pode abrigar centenas ou milhares de máquinas.

As **botnets** geralmente são usadas para atacar sites, roubar dados, enviar spam, hospedar sites falsos. Elas são igualmente usadas para realizar ataques de negação de serviço, quando um site é acessado por milhares de máquinas simultaneamente e deixa de responder às solicitações de acesso.

As ameaças dos worms [5]

A maioria dos **bots** se espalha utilizando falhas no Windows e por meio de redes peer-to-peer (P2P), como eMule e Ares, ou programas como mtorrent, usados para troca de arquivos entre usuários do mundo todo.

Os mal-intencionados conseguem assim transmitir ordens e comandos aos computadores infectados para enviarem spam, lançar ataques de negação de serviços e transferir arquivos maliciosos.

O funcionamento de uma **botnet** se dá da seguinte maneira: em primeiro lugar ele é criado por um hacker (denominado **bot herder**) como um código de programa que é enviado como vírus (pode ser via e-mail ou pelo acesso a sites ou links de um site), que se instalará em computadores com acesso à internet.

As ameaças dos worms [6]

Uma vez instalado, o **bot** realiza o login em uma **botnet**, isto é, uma rede específica criada pelo hacker.

Inicia-se, então, o problema. Este hacker oferece a um interessado em enviar spam e pode até vender os serviços de sua rede **Botnet**.

Desta maneira, com a **botnet** espalhada pelos computadores infectados de uma rede, a mensagem de quem contratou o serviço é enviada a todos, em um processo que é controlado remotamente por um hacker.

Quanto maior for a facilidade de se propagar a **botnet**, mais destaque a comunidade que o controla possui. Existe um termo específico e público para roubos de informações online por meio de **botnet**, que é **SCRUMPING**.

As ameaças dos worms [7]

Agora sabemos que um ataque DDoS tem um worm no início de tudo, o processo malicioso para atacar e provocar a indisponibilidade de serviços de informática.

O **Conficker**, o **Gaobot** ou **Sdbot** são alguns dos mais conhecidos exemplos deste tipo de worm. Os worms são hoje em dia o terceiro tipo de malware com maior circulação.

Os computadores comprometidos podem ser utilizados normalmente sem que seu usuário perceba a existência da infecção. Apenas em determinadas ações realizadas pelos hackers, o usuário notará alguma redução de desempenho, embora não suspeite necessariamente de uma infecção.

As ameaças dos worms [8]

Exemplo: Foi identificado um grande ataque de **botnets** que atingiu aparelhos "inteligentes" entre 23 de dezembro e 6 de janeiro deste ano.

Dentre os aparelhos infectados estavam roteadores, centros multimídia, televisores e pelo menos uma geladeira. Por volta de 750 mil e-mails de spam foram enviados pelos aparelhos infectados.

Segundo especialistas, vários tipos de **botnets** infectaram milhões de computadores ao redor do mundo. Mas o conhecido como **Chuck Norris** é incomum e uma novidade. Ele afeta os modems DSL e os roteadores, em vez dos PCs, usando a senha padrão de administrador destes equipamentos.

O processo de propagação dos worms [1]

Passo 1: Identificação dos computadores-alvo

Após infectar um computador, o worm tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores-alvo, nos quais tentará se reproduzir, o que pode ser feito por uma ou mais das seguintes maneiras:

- Efetuar varredura na rede e identificar quais são os computadores ativos;
- Aguardar que outros computadores contatem com um dos computadores infectados;
- Utilizar listas, predefinidas ou obtidas na internet, contendo a identificação dos computadores-alvo (endereços IP);

O processo de propagação dos worms [2]

Passo 1: Identificação dos computadores-alvo

- Utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de e-mail.

Você já deve ter ouvido falar de casos em que uma pessoa envia e-mails sem que tenha efetivamente realizado e escrito este e-mail. Simplesmente alguém informa a esta pessoa que recebeu um e-mail com vírus de um amigo, que não tem ideia de quem possa tê-lo enviado.

Estes são casos em que um worm se instalou no computador e no programa cliente de e-mail de alguém. Ao ter acesso à lista de endereços de e-mail deste computador, disparou os e-mails maliciosos e de spam.

O processo de propagação dos worms [3]

Passo 2: Envio das cópias

Após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

- Como parte da exploração de vulnerabilidades existentes em programas instalados no computador-alvo;
- Anexadas a e-mails. Os casos mais comuns são de e-mails sem sentido ou e-mails enviados supostamente por um amigo que o convida a ver uma foto antiga: "olhe a foto nossa que encontrei";
- Por intermédio de qualquer programa de chat ou de troca de mensagens instantâneas;
- Incluídas em pastas e arquivos compartilhados em redes locais ou redes sociais ou do tipo P2P (peer-to-peer).

O processo de propagação dos worms [4]

Passo 3: Ativação das cópias

Uma vez realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

- Imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas executados no computador-alvo no momento do recebimento da cópia;
- Diretamente pelo usuário, com a execução de uma das cópias enviadas ao seu computador, como um arquivo obtido por download, em especial, se tiver extensão .exe.
- Pela realização de uma ação específica do usuário, a qual o worm está condicionado, como a inserção de uma mídia removível (por exemplo, um pen drive).

O processo de propagação dos worms [5]

Passo 4: Reinício do processo

O reinício do processo de propagação e ativação de worms inicia-se após o computador alvo ter sido infectado e este será reiniciado a partir deste momento, ele que em um primeiro momento representava o primeiro alvo, agora passa a ser um gerador de ataques.

O que são spywares [1]

Spyware é um programa criado e projetado para monitorar as atividades de um sistema qualquer e enviar as informações coletadas para outras pessoas sem que a pessoa que está utilizando o computador perceba.

Pode ser usado tanto de forma legítima quanto maliciosa, dependendo de como é instalado, de quais ações são realizadas, do tipo de informação que é monitorada e do uso que é feito por quem recebe as informações coletadas.

Ele pode ser classificado de duas maneiras: Legítimo ou Malicioso.

O que são spywares [2]

Legítimo: quando está instalado em um computador pessoal ou de rede, pelo próprio usuário proprietário ou com consentimento deste, com o objetivo de verificar se outras pessoas estão utilizando os recursos deste computador de modo abusivo ou não autorizado.

Malicioso: quando ele executa ações que podem comprometer a privacidade do usuário e a segurança do computador e/ou de uma rede, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário em rede, ou identificação e senha em um determinado sistema e/ou banco de dados).

Spywares - Keyloggers

É um tipo de programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

De qualquer forma, este programa captura tudo o que o usuário digitou no teclado e envia para aquele que instalou o keylogger.

Spywares - Screenloggers

Este formato é muito parecido a um keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado.

É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente nos sites de Internet Banking.

Spywares - Adwares

Este tipo de spyware é projetado especificamente para encher nosso browser de propagandas quando estamos navegando na internet.

Normalmente é usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos, ou como patrocínios de sites diversos.

Também pode ser usado para fins maliciosos quando as propagandas apresentadas são direcionadas para sites específicos, abrindo outras janelas por trás de sua tela de acordo com a navegação, sem que você saiba que tal monitoramento está sendo feito, ou que o desvio está sendo realizado.

Backdoors [1]

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim em uma invasão anterior.

Pode ser incluído pela ação de outros códigos maliciosos, vírus que tenham previamente infectado o computador, ou por malwares, que exploram as vulnerabilidades existentes nos programas instalados no computador para poder invadi-lo.

Após incluído, o backdoor é usado para assegurar o acesso futuro a um computador comprometido, permitindo que ele tenha acesso remoto sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

Backdoors [2]

Um backdoor típico consiste normalmente em dois componentes: clientes e servidor.

O servidor é a máquina atacada, e o cliente é o atacante. Isto é chamado de ligação direta, quando o cliente liga diretamente para o servidor.

Um atacante usará o programa do cliente para se comunicar com os componentes maliciosos do servidor, que então são instalados em algum sistema.

A forma usual de inclusão de um backdoor consiste na disponibilização de um novo serviço do sistema operacional ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto.

Backdoors [3]

Programas de administração remota que permitem acesso a um computador determinado de uma rede, como **BackOrifice**, **NetBus**, **SubSeven**, **VNC** e **Radmin**, se forem mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como backdoors.

Há casos de backdoors incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas de operação dos mesmos. Esses casos devem ser considerados uma grave ameaça à segurança de um computador que contenha um destes programas instalados, pois além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

Consequências dos Backdoors [1]

Dependendo do nível de sofisticação de uma máquina cliente da rede, ele pode incluir recursos como:

- Permitir ao atacante criar, apagar, renomear, copiar, ou modificar qualquer arquivo, executar comandos, alterar as configurações do sistema e modificar registros do Windows;
- Permite ao atacante controlar o hardware do computador, alterando suas configurações de desligamento ou reiniciando o computador sem a permissão do usuário;

Consequências dos Backdoors [2]

- Permite que o atacante roube identificações de login e senhas pessoais, assim como monitore as atividades dos usuários (log);
- Realizar backup de tudo o que o usuário digitou no teclado e capturar as telas em uso;
- Enviar os dados coletados para um destino especificado (endereço de e-mail, servidor FTP, ou uma conexão com um host remoto);
- Acionar a webcam para monitorar o que se passa dentro da residência de alguém. Isto, claro, parece coisa de filmes, mas é real e possível hoje.

O que são rootkits [1]

O rootkit é uma espécie de backdoor, ou seja, uma porta em que o usuário (bem ou mal intencionado – na maioria das vezes a intenção é má) pode entrar e sair livremente, fazendo o que bem entender. A origem do rootkit vem dos sistemas Unix e Linux, em que kits de programas são criados para controle de computadores ou sistemas.

"Root" é a denominação usada para os usuários que têm o controle total da máquina. Deste modo, ao juntar "root" e "kit" tem-se o kit que permite controlar de maneira absoluta um computador.

A principal característica deste tipo de arquivo é esconder-se nos sistemas operacionais para que esses usuários mal intencionados possam fazer o que quiserem quando bem entenderem. Existem dois tipos bastante frequentes entre os sistemas operacionais Windows e Linux/Unix.

O que são rootkits [2]

No Windows, normalmente, eles infectam as tarefas e processos de memória, anulando os pedidos do programa que está com esta praga. Isso faz com que o programa não encontre os arquivos necessários para funcionar. Pode-se simplificar dizendo que os rootkits "enganam" o programa, fazendo-o acreditar que o arquivo não está lá, provocando mensagens de erro.

Já no Linux/Unix, o que acontece é um pouco diferente. O rootkit que infectar um sistema deste tipo irá substituir um programa de listagem de arquivos. Uma vez que ele mesmo exiba as listas, o trojan ficará são e salvo, escondido no sistema. Se ninguém descobre que ele está lá, fica fácil para o sujeito de más intenções exercer o direito de ir e vir no seu computador. Entretanto, ninguém quer alguém "indo e vindo" no seu próprio computador. O que fazer para evitar os rootkits?

O que são rootkits [3]

Assim como a maioria dos vírus, trojans e várias outras pragas digitais, os rootkits se proliferam em emails e sites maliciosos como aqueles que imitam páginas da Receita Federal e bancos. Clicar em um desses emails pode ser perigoso sob vários aspectos. Além de poder roubar as suas informações pessoais, estes backdoors, rootkits e outros malwares dão acesso a quem souber invadir computadores.

Neste caso, é imprescindível contar com a proteção de um bom antivírus e um firewall. Porém, melhor do que essa combinação, é importante também ter um anti-spam que seja eficiente. Afinal, boa parte dos endereços que enviam estes emails são suspeitíssimos e devem ser denunciados aos serviços anti-spam. Entretanto, se você não tiver algo que bloqueie spams ou redirecione-os para longe da sua caixa de entrada, procure não abrir e-mails de remetentes desconhecidos. Isto pode evitar muitas dores de cabeça.

O que são rootkits [4]

Bons programas antivírus pagos (que englobam também a função de firewall e anti-spyware) geralmente conseguem bloquear a maioria dos rootkits, mas além disso, devemos manter o sistema sempre atualizado.

Este texto está disponível em:

http://www.tecmundo.com.br/antivirus/2174-o-que-e-rootkit-.htm

Algumas conclusões

Atualmente é muito raro que vírus ou worms sejam programados apenas para ações que assustem ou notifiquem o usuário de que algo está errado, que você pode notar por meio de comportamentos estranhos do computador, como paradas repentinas ou lentidão.

Este comportamento explica-se pelo fato de os ataques com worms e com backdoors visarem lucro financeiro – ou seja, instalarem vírus que permitam o roubo de senhas e identificação de cartões de crédito, entre outros, ou ações políticas de impacto mundial.

Uma cartilha básica de segurança da internet recomenda que não se deve abrir anexos estranhos, que se deve atualizar sempre o antivírus e desconfiar quando um e-mail promete um prêmio especial em um concurso de que você não lembra de ter participado.

TABELA 1

Códigos maliciosos							
	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Como ele vai parar no seu computador							
Recebido automaticamente pela rede		✓	✓				
Recebido por e-mail	✓	✓	✓	✓	✓		
Baixado de sites na internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓

TABELA 2

Códigos maliciosos							
	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Como ocorre a instalação							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga							
Insere cópia de si em arquivos	✓						
Envia cópia de si automaticamente pela rede		✓	✓				
Envia cópia de si automaticamente por e-mail		✓	✓				
Não se propaga				✓	✓	✓	✓

TABELA 3

Códigos maliciosos							
	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Ações maliciosas mais comuns							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓