www.leitejunior.com.br
Informática para Concursos Públicos
leitejuniorbr@yahoo.com.br
leitejuniorbr@hotmail.com

ÍNDICE

VÍRUS DE COMPUTADOR

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Parasitam os arquivos executáveis do computador (aqueles com extensão .EXE ou .COM).

MITOS

Um programa contaminado, salvo em um HD, não vai acionar o ataque do vírus. Por isso, se o evento que ativa o vírus não for acionado nunca pelo usuário, o vírus ficará "adormecido" até o dia em que o programa for executado.

O vírus não pode danificar o hardware do computador. Os vírus são softwares e, portanto não há como eles queimarem ou quebrarem dispositivos do computador. De certo, existem vírus que apagam o BIOS da placa-mãe, deixando-a sem capacidade para ser usada, dando a impressão de que foi danificada.

EXTENSÃO VIRÓTICA

- Arquivos Executáveis: com extensão EXE ou COM.
- Arquivos de Scripts (outra forma de executável): extensão VBS.
- Arquivos de Proteção de Tela (aquelas animações que aparecem automaticamente quando o computador está ocioso): extensão SCR.
- Arquivos de Atalhos: extensão LNK ou PIF (essa última é perigosíssima!)
- Arquivos de Documentos do Office: como os arquivos do Word (extensão DOC ou DOT), arquivos do Excel (XLS e XLT), Apresentações do Power Point (PPT e PPS), Bancos de Dados do Access (MDB).

Caso você receba por e-mail qualquer um desses tipos de arquivo, preste bastante atenção.

TIPOS DE VÍRUS OU PRAGAS VIRTUAIS

VÍRUS DE MACRO

Vírus de Macro é uma classificação de vírus que afetam os documentos do Office da Microsoft (Word, Excel, Power Point, Access, Outlook entre outros).

Uma Macro é um programa (conjunto de instruções) criado dentro de um documento qualquer, como do Word, por exemplo, para automatizar tarefas nesse aplicativo. Normalmente usa-se macros para realizar tarefas repetitivas. Essa macro é, na verdade, um programa escrito na linguagem VBA (Visual Basic for Applications).

VÍRUS POLIMÓRFICO

Os vírus polimórficos são vírus que têm a capacidade de sempre se copiar para outros arquivos com alguma diferença da versão anterior, no intuito de diminuir a possibilidade de ser detectado pelo software antivírus.

Muitos vírus de executável, de boot ou até mesmo de macro são vírus polimórficos. Eles usam essa técnica para se esconder dos antivírus.

VÍRUS DE BOOT?

São vírus que infectam o computador alvo copiando-se para um local no mínimo inusitado: o setor de boot (MBR) do HD.

O Setor de Boot (ou MBR – Master Boot Record – Registro Mestre de Inicialização) do disco rígido é a primeira parte do disco rígido que é lida quando o computador é ligado. Essa área é lida pelo BIOS (programa responsável por "acordar" o computador) a fim de que seja encontrado o Sistema Operacional (o programa que controla o computador durante seu uso).

WORMS(VERMES)

Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

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.

TROJANS/CAVALOS DE TRÓIA

São programas executáveis que transformam seu micro em um terminal de internet "aberto".

Estes programas eliminam as proteções que impedem a transferência de informações, ou seja, abrem uma porta de comunicação (backdoor) não monitorada.

Permite a um estranho acessar o seu micro, ou mesmo poder coletar dados e enviá-los para a Internet, sem notificar seu usuário.

Alguns e-mails contêm um endereço na Web para baixar o cavalo de Tróia.

SPYWARES

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.

HIJACKERS(SEQUESTRADORES)

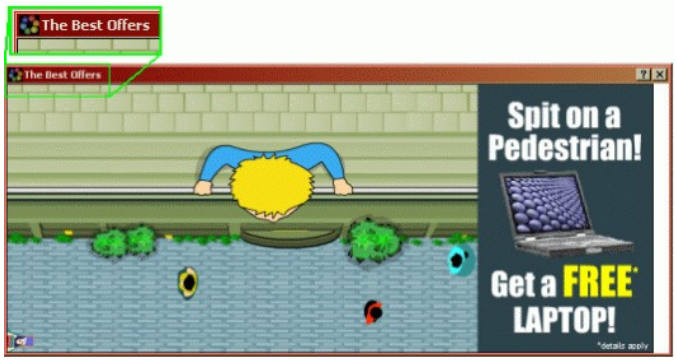
São programas ou scripts que "sequestram" navegadores de Internet, principalmente o Internet Explorer.

Quando isso ocorre, o hijacker altera a página inicial do browser e impede o usuário de mudá-la, exibe propagandas em pop-ups ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de software antivírus, por exemplo).

Os spywares e os keyloggers podem ser identificados por programas anti-spywares. Porém, algumas destas pragas são tão perigosas que alguns antivírus podem ser preparados para identificá-las, como se fossem vírus.

No caso de hijackers, muitas vezes é necessário usar uma ferramenta desenvolvida especialmente para combater aquela praga. Isso porque os hijackers podem se infiltrar no sistema operacional de uma forma que nem antivírus nem anti-spywares conseguem "pegar".

ADWARES



Os adwares são conhecidos como programas que trazem para a tela do usuário, algum tipo de propaganda.

Como geralmente são firmas comerciais que os desenvolvem, é comum os adwares virem embutidos em diversos programas freware (download gratuito).

RANSONWARE

Ransonwares são softwares maliciosos, recebidos por cavalo de tróia, que, ao infectarem um computador, criptografam todo ou parte do conteúdo do disco rígido.

Os responsáveis pelo software exigem da vítima, um pagamento pelo "resgate" dos dados.

Ransonwares são ferramentas para crimes de extorsão e são extremamente ilegais.

Nomes de alguns Ransonwares conhecidos : Gpcode-B / PGPCoder.

ROOTKIT

É um tipo de Malware onde sua principal intenção é se esconder, impedindo que seu código seja encontrado por qualquer antivírus.

Isto é possível por que estas aplicações têm a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado.

BACKDOOR

Pode ser instalado tanto presencialmente como remotamente.

Sua função é de abrir portas de comunicação sem o conhecimento do usuário, para que através delas, o mesmo sofra uma invasão ou um ataque.

PHISHING

Também conhecido como phishing scam ou phishing/scam.

Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros.

Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet.

Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

KEYLOGGER

Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.

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, ou armazenar a região que circunda a posição onde o mouse é clicado.

BOT(ROBOT)

É um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuracão de softwares instalados em um computador.

Adicionalmente ao worm, dispões de mecanismos de comunicação com o invasor, permitindo que o bot seja controlado remotamente.

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.

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).

BOATOS(HOAXES)

São textos que contam estórias alarmantes e falsas, que instigam o leitor a continuar sua divulgação. Geralmente, o texto começa com frases apelativas do tipo: "envie este e-mail a todos os seus amigos...". Algumas classes comuns de boatos são os que apelam para a necessidade que o ser humano possui de ajudar o próximo. Como exemplos temos os casos de crianças com doenças graves, o caso do roubo de rins, etc.

CORRENTES(CHAIN LETTERS)

São textos que estimulam o leitor a enviar várias cópias a outras pessoas, gerando um processo contínuo de propagação.

São muito semelhantes aos boatos, mas o mecanismo usado para incentivar a propagação é um pouco diferente, pois a maioria das correntes promete sorte e riqueza aos que não as interrompem e anos de má sorte e desgraça aos que se recusam a enviar N cópias do e-mail para Y pessoas nas próximas X horas! Como exemplo temos a corrente de oração, dentre tantas outras.

PROPAGANDAS

Tem o intuito de divulgar produtos, serviços, novos sites, enfim, propaganda em geral, têm ganho cada vez mais espaço nas caixas postais dos internautas.
Vale ressaltar que, seguindo o próprio conceito de spam, se recebemos um e-mail que não solicitamos, estamos sim sendo vítimas de spam, mesmo que seja um e-mail de uma super-promoção que muito nos interessa.

SPIM(SPAM VIA INSTANT MESSENGE)

São mensagens publicitárias ou indesejadas que chegam em massa em usuários de programas de mensagem instantânea.

É mais comum em programas que permitem que qualquer um, mesmo que não tenha sido previamente autorizado, consiga enviar mensagens para qualquer outra pessoa., como por exemplo o antigo ICQ ou Messenger.

SPIT(SPAM INTERNET TELEPHONY)

Ocorre quando um usuário atender uma ligação em seu telefone IP, e ouve gravações com mensagens indesejadas, em grande parte oferecendo produtos ou serviços não-solicitados.

Isso é possível graças a softwares que entram na web e discam para todos os usuários de serviço VoIP.

SPAM ZOMBIE

Computador infectado por código malicioso, capaz de transformar o sistema do usuário em um servidor de e-mail para envio de spam. Em muitos casos, o usuário do computador infectado demora a perceber que seu computador está sendo usado por um invasor para este fim.

DIFAMAÇÃO

Spams que são enviados com o intuito de fazer ameaças, brincadeiras de mau gosto ou apenas por diversão.

Casos de ex-namorados difamando ex-namoradas, e-mails forjados assumindo identidade alheia e aqueles que dizem: "olá, estou testando uma nova ferramenta spammer e por isto você está recebendo este e-mail", constituem alguns exemplos.

PHARMING

Sua função é modificar a relação que existe entre o nome de um site na Internet e seu respectivo servidor Web.

A técnica clássica é chamada de envenenamento de cache DNS (DNS Cache Poisoning, em inglês).

Neste ataque, um servidor de nomes (servidor DNS) é comprometido, de tal forma que as requisições de acesso a um site feitas pelos usuários deste servidor sejam redirecionadas a outro endereço, sob controle dos atacantes.

Pode ser um ataque, feito remotamente ou por meio de programas maliciosos como cavalos-de-tróia, a um arquivo presente nos computadores de usuários finais, chamado "hosts".

O QUE É UM SERVIDOR DE NOMES OU SERVIDOR DNS?

DNS - Domain Name System, e se refere ao sistema de atribuição de nomes de domínios e endereços eletrônicos em redes de computadores.

É um sistema dotado de um software que traduz os nomes dos sites (domínios), da linguagem humana para números (chamados de endereços IP, ou Internet Protocol), de forma que possam ser interpretados pelas outras máquinas da rede.

O QUE É CACHE DNS?

Cache é o nome geral dado a memória temporária de um programa ou máquina, que serve para armazenar informações já acessadas e diminuir o tempo de acesso na próxima vez que a informação for requisitada.

No caso do "Cache DNS", trata-se da memória temporária de um servidor DNS, de modo que o endereço IP de um site anteriormente acessado fique guardado na máquina, facilitando os acessos futuros.

COMO O PHARMING ATINGE USUÁRIOS DOMÉSTICOS?

De modo geral, ataques de pharming do tipo envenenamento de cache DNS não são dirigidos a usuários finais, e sim aos servidores de nomes de provedores de Internet ou de empresas com redes internas.

Mas um servidor de nomes atacado pode afetar milhares de usuários que utilizem esta máquina.

Se o servidor DNS de um provedor ou empresa sofrer um envenenamento de cache, todos os seus usuários poderão ser redirecionados para endereços e páginas falsas toda vez que tentarem acessar determinado site legítimo, sem precisarem ter instalado nada em suas próprias máquinas ou clicado em nenhum link malicioso.

O QUE VOCÊ PODE FAZER PARA SE PROTEGER?

A melhor forma de proteção para qualquer ameaça da Internet é manter-se atualizado, tanto em informações como em programas instalados no computador, e evitar ataques antes que eles aconteçam.

Manter o sistema operacional, navegador e programa de e-mail constantemente atualizados.

Instalar e manter atualizado um programa antivírus que tenha capacidade de identificar não só ameaças já identificadas, mas também ameaças desconhecidas, por meio da análise do comportamento do arquivo suspeito (análise heurística).

Também é importante instalar outros programas de proteção, como anti-spywares.

Instalar um firewall, programa que bloqueia todo o tráfego de entrada e saída de dados do computador e só deixa passar aquilo que o usuário autoriza.

Tomar cuidado com mensagens não solicitadas(SPAM), mesmo que pareçam vir de fontes confiáveis, e não clicar em links ou instalar arquivos referenciados nestas mensagens.

INVASORES (CRACKER E HACKER)

Usuário de computador com um vasto conhecimento tecnológico.

CRACKER

Cracker é o termo usado para designar quem quebra um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 pelos hackers em defesa contra o uso jornalístico do termo hacker.

- **Crackers de Sistemas:** piratas que invadem computadores ligados em rede.
- **Crackers de Programas:** piratas que quebram proteções de software cedidos a título de demonstração para usá-los por tempo indeterminado, como se fossem cópias legítimas(warez).
- **Phreakers:** piratas especialistas em telefonia móvel ou fixa.
- **Desenvolvedores de vírus, worms e trojans:** programadores que criam pequenos softwares que causam danos ao usuário.
- **Piratas de programas:** indivíduos que clonam programas, fraudando direitos autorais.
- **Distribuidores de warez:** webmasters que disponibilizam em suas páginas softwares sem autorização dos detentores de direitos autorais.

MOTIVAÇÕES DOS CRACKERS

- **Pichadores Digitais:** agem principalmente com o objetivo de serem reconhecidos. Desejam tornar-se famosos no universo cyberpunk e para tanto alteram páginas da internet, num comportamento muito semelhante aos pichadores de muro, deixando sempre assinado seus pseudônimos. Alguns deixam mensagens de conteúdo político o que não deve ser confundido com o ciberterrorismo.
- **Revanchista:** funcionário ou ex-funcionário de alguma empresa que por qualquer motivo resolve sabotá-la com objetivo claro de vingança. Geralmente trabalharam no setor de informática da empresa o que facilita enormemente seu trabalho já que estão bem informados das fragilidades do sistema.
- **Vândalos:** agem pelo simples prazer de causar danos a vítima. Este dano pode consistir na simples queda do servidor (deixando a máquina momentaneamente desconectada da Internet) ou até mesmo a destruição total dos dados armazenados.
- **Espiões:** agem para adquirirem informações confidenciais armazenados no computador da vítima. Os dados podem ter conteúdo comercial (uma fórmula de um produto químico) ou político (e-mails entre consulados) ou militar (programas militares).
- **Ciberterroristas:** são terroristas digitais. Suas motivações são em geral políticas e suas armas são muitas, desde o furto de informações confidenciais até a queda do sistema telefônico local ou outras ações do gênero.
- **Ladrões:** têm objetivos financeiros claros e em regra atacam bancos com a finalidade de desviar dinheiro para suas contas.
- **Estelionatários:** também com objetivos financeiros, em geral, procuram adquirir números de cartões de créditos armazenados em grandes sites comerciais. Geralmente utilizam uma técnica chamada "Phising Scam", enviando por e-mail um programa que é executado por algum usuário, tendo acesso às suas informações.

VARIAÇÕES DO TERMO CRACKING

- O ato de quebrar a segurança de um sistema, ao contrário do que é esperado, geralmente não é necessário nenhum brilhantismo hacker para realizar, mas de ficar repetindo uma série de tentativas a explorar (exploitar) as vulnerabilidades conhecidas do sistema alvo. Geralmente a maioria dos crackers sao medíocres hackers.
- O ato de quebrar uma senha ou criptografia atravez de bruteforce, tecnica de "tentativa e erro", onde todas as possibilidades sao tentadas.
- É o nome dado a ações de modificações no funcionamento de um sistema, de maneira geralmente ilegal, para que determinados usuários ganhem algo com isso.
- Remover a proteção contra copia de softwares, com o objetivo de burlar licenças de uso. Crackers difundem, pela Internet, programas para gerar códigos seriais, patches, cracks e outros códigos para a liberação de softwares proprietários.

HACKER

São denominados hackers (singular: hacker) indivíduos que criam e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Utilizadores maliciosos têm sido designados hackers pela imprensa, quando na realidade estes seriam mais corretamente classificados como crackers.

Os hackers e crackers são indíviduos da sociedade moderna, e possuem conhecimentos avançados na área tecnológica e de informática, mas a diferença básica entre eles é que os hackers somente constroem coisas para o bem e os crackers destroem.

ESPECIALIDADES DO HACKER

Outros termos utilizados na segurança da informação, para diferenciar os tipos de hacker/cracker são:

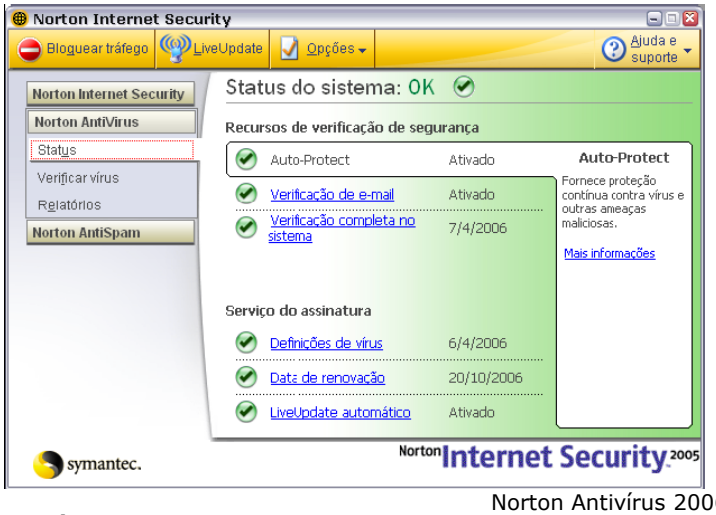
- **White hat** - (Chapéu Branco) utiliza os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei. A atitude típica de um white hat assim que encontra falhas de segurança é a de entrar em contacto com os responsáveis pelo sistema, comunicando do fato. Geralmente, hackers de chapéu branco violam seus próprios sistemas ou sistemas de um cliente que o empregou especificamente para auditar a segurança.
- **Gray hat** – (Chapéu Cinza) tem as habilidades e intenções de um hacker de chapéu branco na maioria dos casos, mas por vezes utiliza seu conhecimento para propósitos menos nobres. Um hacker de chapéu cinza pode ser descrito como um hacker de chapéu branco que às vezes veste um chapéu preto para cumprir sua própria agenda.
- Black hat - (Chapéu Preto) criminoso ou malicioso hacker, um cracker; Em geral, crackers são menos focados em programação e no lado acadêmico de violar sistemas. Eles comumente confiam em programas de cracking e exploram vulnerabilidades conhecidas em sistemas para descobrir informações importantes para ganho pessoal ou para danificar a rede ou sistema alvo.
- **Script kiddie** - Indivíduo que não tem domínio dos conhecimentos de programação, pouco experiente, com poucas noções de informática, porém tenta fazer-se passar por um cracker afim de obter fama, o que acaba gerando antipatia por parte dos hackers verdadeiros, cerca de 95% dos ataques virtuais são praticados por script kiddies.
- **Newbie** - É aquele jovem aprendiz de hacker que possui uma sede de conhecimento incrível, pergunta muito e é ignorado e ridicularizado maioria das vezes.
- **Phreaker** - hacker especialista em telefonia móvel ou fixa.

PROTEÇÃO - ANTIVÍRUS, ANTI-PESTES, FILTRO ANTI-SPAM FIREWALL E PROXY

A melhor forma para se proteger de um Vírus de Computador ou invasão é manter, em seu computador, um programa antivírus ativo e atualizado, um Anti-Peste, Filtro Anti-Spam, um Firewall e um Proxy.

ANTIVÍRUS

O Antivírus é instalado em um computador e fica residente na memória principal(RAM) desde a inicialização do Sistema Operacional..



Norton Antivírus 2006

CARACTERÍSTICA

É importante frisar que o Antivírus tem dois principais componentes:

- **VARREDURA PREVENTIVA** - o programa fica de olho em tudo o que pode ser vetor de transmissão de vírus, como e-mails, arquivos que entram por disquetes e Cds, etc.
- **VARREDURA MANUAL** – o usuário realizar sempre que desejar.

DEFINIÇÕES DOS VÍRUS OU ASSINATURA DE VÍRUS

É uma lista dos vírus que consegue detectar/limpar. Deve está sempre atualizada.

QUARENTENA

É uma área para os arquivos suspeitos ou definitivamente infectados. Quando os arquivos entram nessa área, o programa antivírus bloqueia o acesso à leitura e execução deles.

HEURÍSTICA

É uma técnica que utiliza algoritmos matemáticos complexos, onde tenta antecipar ações maliciosas que podem ocorrer quando um determinado código é executado.

PRECAUÇÕES

É bom manter, em seu computador:

- Um programa Antivírus funcionando constantemente (preventivamente);
- Esse programa Antivírus verificando os e-mails constantemente (preventivo);
- O recurso de atualizações automáticas das definições de vírus habilitado.
- As definições/assinaturas de vírus atualizadas sempre (nem que para isso sejam necessários, todos os dias, executar a atualização manualmente).

ANTIVÍRUS CONHECIDOS

- NORTON
- AVG: Antivírus gratuito disponível na Internet.
- AVAST!: Outro antivírus gratuito disponível na Internet.
- ESCAN
- NOD32
- AVIRA
- KASPERSKY
- PANDA
- MACAFEE

ANTI-PESTES

Um anti-peste é um software indicado para eliminar spywares e ad-wares.

Tal como os antivírus necessitam ter sua base de dados atualizada.

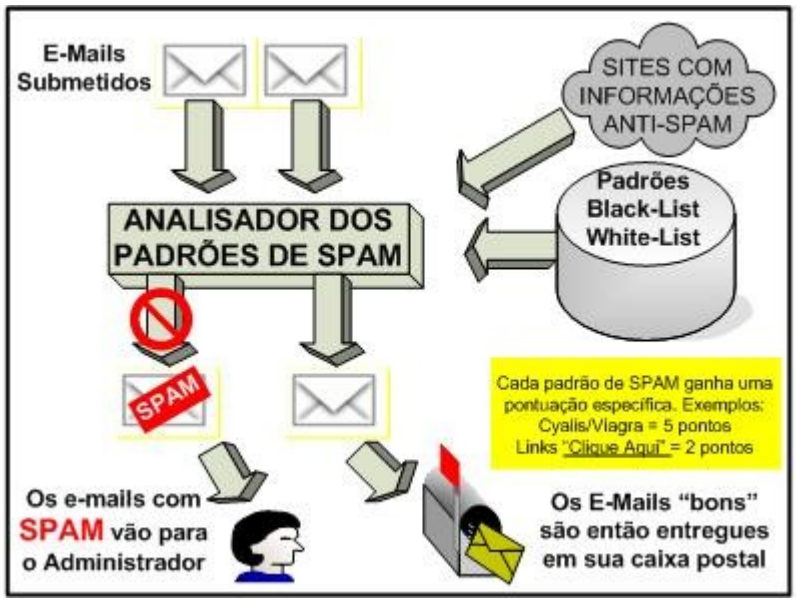
Atualmente recomenda-se a instalação de algum programa anti-peste (ou antispyware em inglês), pois como já foi comentado, certos softwares trazem consigo spywares ou adwares, ou mesmo o Internet Explorer pode ser contaminado por algum spywares, pois ainda não há certeza absoluta que ele possa ficar imune, das variadas formas de adwares desenvolvidos por firmas comerciais.

Programas anti-pestes mais utilizados:

- Microsoft Windows Defender - gratuito
- SpyBot - gratuito
- Ad-aware SE - versão gratuita
- eTrust™ PestPatrol® Anti-Spyware
- XoftSpy

ANTI-SPAM

- Permitem fazer uma triagem nos emails recebidos, separando os spams em potencial dos emails válidos.



FILTROS NO SERVIDOR DE EMAIL

- Atua em conjunto com o servidor de email (MTAs, Mail Transfer Agents) e sua principal vantagem é filtrar o spam logo na sua chegada (no servidor).
- Uma das técnicas mais usadas é a configuração de listas negras, conhecidas como RBLs (Realtime Blackhole Lists).

WHITE LIST / LISTA LIMPA: Definir uma lista de remetentes "conhecidos" e autorizados a enviar email para o(s) usuário(s), dono(s) da "White List "em questão. Assim, os emails recebidos de endereços não constantes na "White List" são barrados.

FILTROS NO CLIENTE DE EMAIL

- Atua em conjunto com o cliente de email do usuário final (MUA, Mail User Agents).
- Neste caso, alguns software MUAs como o Eudora e o Microsoft Outlook, por exemplo, têm mecanismos para filtragem de spam.
- Analogamente, os aplicativos de webmail, como o Squirrelmail, por exemplo, ou os webmails de provedores em geral, também possuem opções para filtragem de emails não-solicitados.
- Vale ressaltar que os filtros no MUA podem ser usados em conjunto com os filtros no servidor, o que aumenta a eficiência.
- A vantagem em se configurar filtros no software MUA é barrar o email indesejado, deixando a caixa postal do usuário mais "limpa". No entanto, alguns defendem que esta não é a melhor solução, já que os emails de spam já consumiram banda, espaço em disco e tempo de processamento no servidor, antes de serem filtrados no cliente.

TIPOS DE FILTRAGEM

- **ENDEREÇO IP**, usado nos casos onde é possível identificar o endereço IP origem do spam.
- **REDE**, usado nos casos onde o spam parte de vários IPs de uma mesma rede, ou ainda, em situações onde fica evidente o descaso dos administradores da rede origem do spam. Este método de filtragem é usado também para filtrar redes dial-up.
- **DOMÍNIO**, usado basicamente quando os responsáveis por um determinado domínio não coíbem a ação de spammers ou ainda, quando o referido domínio é reconhecidamente origem de freqüentes spams.
- **CONTEÚDO**, em busca de reconhecidas palavras usadas pelos spammers.

CONCLUSÃO

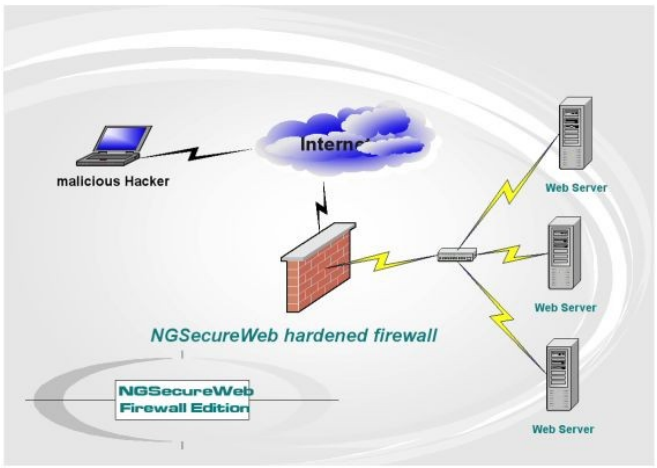
O spam está na ordem do dia em listas técnicas, jornais, revistas e na mídia em geral.

As soluções e recomendações para o combate ao spam têm proliferado. No entanto, soluções técnicas e legislação adequada não são suficientes para resolver o problema.

Hoje, não existe uma solução definitiva para o problema do spam, apenas algumas soluções de contorno que mitigam o seu impacto no trabalho e no humor de administradores de rede e usuários em geral.

Assim, uma alternativa é o próprio usuário final assumir parte da responsabilidade de combate ao spam, adotando posturas conscientes no uso do email e algum tipo de software de filtragem para diminuir o incomôdo causado por aquela enorme quantidade de mensagens não solicitadas depositadas diariamente em sua caixa postal.

FIREWALL



Atualmente uma das maiores preocupações do administrador de uma máquina conectada à internet, seja residencial ou empresarial, é manter a segurança de sua rede interna.

A primeira resposta (e na maioria das vezes a única) é configurar um firewall com um conjunto de regras que impeçam o acesso indevido de terceiros.

As ferramentas NIDS/IDS (Network Intrusion Detection System - que pode ser traduzido como "Sistemas de Detecção de Invasão de Redes") permitem aplicar um nível alto de segurança dentro de uma estrutura de rede.

Um firewall evita que perigos vindos da Internet espalhem-se na sua rede interna.

Colocado entre a rede interna e a externa, o firewall controla todo o trafego que passa entre elas, tendo a certeza que este trafego é aceitável, de acordo com uma política de segurança pré-estabelecida, oferecendo uma excelente proteção contra ameaças.

Entretanto, ele não é uma completa solução para segurança. Certos perigos estão fora do controle de um firewall.

Podemos dizer que um firewall é um separador, um bloqueador e um analisador, podendo ser, por exemplo, um roteador, um computador, ou uma combinação de roteadores e computadores.

O QUE UM FIREWALL PODE FAZER

UM FOCO PARA DECISÕES DE SEGURANÇA

Pense no firewall como um funil onde todo o trafego deve passar por ele. Isto permite que sejam concentradas todas as medidas de segurança neste ponto onde a rede interna conecta-se com a Internet.

FORTALECER A POLÍTICA DE SEGURANÇA

Muitos serviços são inseguros e o firewall pode filtrá-los de acordo com um conjunto de regras, permitindo que apenas serviços aprovados passem por ele. Por exemplo, serviços como NFS(**Network File System** - Serviço de rede que permite o compartilhamento transparente de sistemas de arquivos ou diretórios entre os nós de uma rede).

IMPLEMENTAR UM SISTEMA DE LOG EFICIENTE

Todo o trafego passa pelo firewall, que se apresenta como um ótimo ponto para se coletar informações sobre o sistema e uso da rede.

O QUE UM FIREWALL NÃO PODE FAZER

PROTEGER A REDE DE USUÁRIOS INTERNOS MAL INTENCIONADOS

O firewall pode evitar que certas informações saiam de uma companhia através da conexão de rede, mas não pode impedir que um usuário copie os dados num disquete e os carregue consigo. Atacantes internos requerem medidas de segurança interna, como segurança de host e educação de usuários.

PROTEGER CONTRA CONEXÕES QUE NÃO PASSAM POR ELE

O firewall pode apenas controlar o trafego que passa por ele. Se o seu site disponibilizar acesso discado para sistemas internos atrás do firewall, não ha nada que o firewall possa fazer para prevenir que intrusos tenham acesso a sua rede por esta via.

PROTEGER CONTRA NOVAS AMEAÇAS

Firewalls são projetados para proteger contra ameaças conhecidas.

PROTEGER CONTRA VÍRUS

Embora o firewall verifique todo o trafego que entra na rede interna, esta verificação é feita basicamente checando os endereços fonte e destino e os números de porta, não verificando os dados em si.

ARQUITETURA DE FIREWALLS

HONEY POT

- Simula a existência de computadores/serviços vulneráveis no seu ambiente, fazendo com que hackers caiam na armadilha e sejam facilmente identificados, além de provocar um grande atraso nas suas ações, permitindo pronta resposta.

BASTION HOST

- Um computador que deve ser altamente seguro por estar mais exposto a Internet sendo, portanto, mais vulnerável a ataques.

PERIMETER NETWORK

- Uma rede colocada entre a rede interna (protegida) e a rede externa com objetivo de adicionar mais uma camada de segurança. Esta rede é também chamada de DMZ (De-Militarized Zone).

PACKET FILTERING

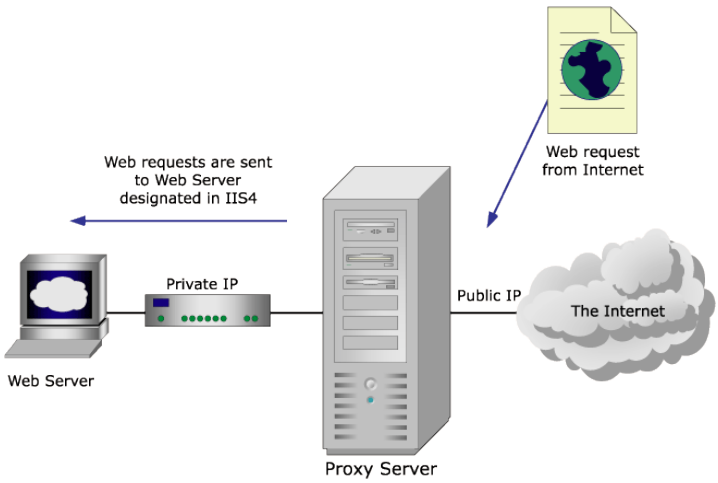
É um mecanismo de segurança que controla o fluxo de dados que entra e sai da rede. Para isto, é criado um conjunto de regras que especifica quais tipos de pacotes devem ser liberados e quais devem ser bloqueados.

Packet filtering é também conhecido como "screening" e pode ser implementado em um roteador, uma bridge ou em um host.

Para entender como o packet filtering funciona, veja a diferença entre um roteador comum e um screening router.

- Um roteador comum simplesmente olha o endereço destino de cada pacote e escolhe e melhor caminho para enviar o pacote. A decisão do que fazer com o pacote é baseado apenas no endereço destino.
- Um screening router, por outro lado, olha para mais detalhes do pacote (endereços fonte/destino e números de porta), para poder determinar se pode, ou não, rotear o pacote para seu destino.

PROXY



Proxy são aplicações ou programas servidores que rodam em um host que tem acesso a Internet e a rede interna.

Estes programas pegam o pedido do usuário para serviços de Internet e encaminha-o, de acordo com a política de segurança do site, para os verdadeiros serviços.

É um serviço transparente. O usuário acha que esta lidando diretamente com o servidor real, e este tem a ilusão que está lidando diretamente com o usuário.

Um serviço proxy requer dois componentes: um servidor e um cliente.

O cliente proxy é um versão especial do programa cliente real que interage com o servidor proxy ao inves do servidor real.

O servidor proxy avalia o pedido do cliente proxy e, caso o pedido seja aprovado, o servidor proxy entra em contato com o verdadeiro servidor na Internet em nome do cliente.

TIPOS DE ATAQUE

DDOS (DISTRIBUTED DENIAL OF SERVICE)

Ataques DDoS são bastante conhecidos no âmbito da comunidade de segurança de redes, são ataques que podem ser efetuados a partir de um computador de forma simples, através do envio indiscriminado de requisições a um computador alvo, visando causar a indisponibilidade dos serviços oferecidos por ele.

Neste novo enfoque, os ataques não são baseados no uso de um único computador para iniciar um ataque, no lugar são utilizados centenas ou até milhares de computadores desprotegidos e ligados na Internet para lançar coordenadamente o ataque.

IP SPOOFING

É uma técnica de subversão de sistemas informáticos que consiste em mascarar (spoof) pacotes IP com endereços remetentes falsificados.

SYN FLOODING OU ATAQUE SYN

É uma forma de ataque de negação de serviço (também conhecido como Denial of Service - DoS) em sistemas computadorizados, na qual o atacante envia uma seqüência de requisições SYN para um sistema-alvo.

Quando um cliente tenta começar uma conexão TCP com um servidor, o cliente e o servidor trocam um série de mensagens, que normalmente são assim:

- O cliente requisita uma conexão enviando um SYN (synchronize/start) ao servidor.
- O servidor confirma esta requisição mandando um SYN-ACK (synchronize acknowledge) de volta ao cliente.
- O cliente por sua vez responde com um ACK(acknowledge), e a conexão está estabelecida.

Isto é o chamado aperto de mão em três etapas (Three-Way Handshake).

Um cliente malicioso pode não mandar esta última mensagem ACK. O servidor irá esperar por isso por um tempo, já que um simples congestionamento de rede pode ser a causa do ACK faltante.

Algumas contra-medidas para este ataque são os SYN cookies ou limitar o número de novas conexões por tempo.

ATAQUES SMURF

Exploram erros de configuração em roteadores que permitem a passagem de pacotes ICMP ou UDP direcionados a endereços de broadcast transformando redes em "amplificadores" destes.

O **ICMP (Internet Control Message Protocol)** – O seu uso mais comum é feito pelos utilitários ping e traceroute. O ping envia pacotes ICMP para verificar se um determinado host está disponível na rede.

O traceroute faz uso do envio de diversos pacotes UDP ou ICMP e, através de um pequeno truque, determina a rota seguida para alcançar um host.

PING DA MORTE" (PING OF DEATH)

Recurso que consiste no envio de pacotes TCP/IP de tamanho inválidos para servidores, levando-os ao travamento ou impedimento de trabalho.

Este recurso foi muito utilizado no início dos provimentos Internet no Brasil, para o impedimento de serviços.

Atualmente são bloqueados por boa parte dos sistemas básicos de segurança.

PORT SCAN

É o processo utilizado para determinar quais portas estão ativas em um sistema.

O PortScan não determina qual protocolo ou aplicação específica esta sendo utilizado, apenas verifica quais estão abertas ou fechadas.

SNIFFER

Também conhecido como Packet Sniffer, Analisador de Rede, Analisador de Protocolo, Ethernet Sniffer em redes do padrão Ethernet ou ainda Wireless Sniffer em redes wireless).

Esta ferramenta, constituída de um software ou hardware, é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores. Conforme o fluxo de dados trafega na rede, o sniffer captura cada pacote e eventualmente decodifica e analisa o seu conteúdo.

Sniffing pode ser utilizado com propósitos maliciosos por invasores que tentam capturar o tráfego da rede com diversos objetivos, dentre os quais podem ser citados, obter cópias de arquivos importantes durante sua transmissão, e obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real.