Pragas Virtuais

Pragas virtuais[1]

Oi sou o Praguinha, bom camarada, mas tenho uns irmãos não muito honestos, as vezes chatos e nada colegas.

Estes foram divididos e classificados ao longo do tempo, tamanha a quantidade e complexidades destes. Minha família só tende a aumentar.

Obs.: as imagens foram copiadas da Internet, inclusive eu.

Vamos lá dar uma olhada em alguns "praguentos do mal". Vejam as caras deles, coisa horrorosa! Em contra partida sou bonitinho, fofinho e do bem:

O que são malwares?

Os **malwares**, conhecidos pelo termo *malicious software* (do inglês software malicioso), são programas desenvolvidos para executarem ações danosas e ilícitas em um sistema. Entre os danos mais conhecidos, podem ser destacados a perda de dados e o roubo de informações sigilosas.

O que são vírus?

Os vírus foram a primeira denominação dada, tudo era vírus por causa do seu comportamento nos micros. Hoje, continuam sendo um dos tipos mais comuns de malware. Tais pragas são programas que se espalham por meio da inserção de uma cópia de si mesmo em outros softwares e arquivos. É muito comum que sejam propagados por meio de arquivos executáveis, porém, eles só conseguem infectar outras aplicações do sistema, quando executados. Parece aquele jogo de copos colocados dentre outros copos.

Normalmente, os vírus são propagados via mensagens de e-mails e até mesmo por meio de mídias removíveis (como pen drives). Por exemplo, quando um usuário executa um arquivo infectado, o qual foi anexado a uma mensagem de e-mail, a praga se instala

[1] http://www.techtudo.com.br/artigos/noticia/2013/06/entenda-o-que-sao-virus-spywares-trojans-worms-e-saiba-como-se-proteger.html

em seu sistema e, então, começa a se autocopiar para os demais arquivos e programas do ambiente.

Além de causar danos ao sistema hospedeiro, os vírus se propagam à medida que o usuário os enviar (sem saber) para outros, via e-mail ou mídias removíveis. Desse modo, o ciclo será reiniciado e outras máquinas também serão infectadas.

Nossa, estes meus irmãos viajam.

O que são Worms?

Tem irmão que parece ter nome pomposo, worms, mas nada mais são do que vermes, "uehuehueh". Diferente dos vírus, os worms possuem a capacidade de se propagarem automaticamente e enviar cópias completas de si mesmos para outros computadores. Ou seja, eles não precisam se anexar a outros arquivos para conseguir infectar uma máquina e podem se mover entre hospedeiros por conta própria.

Quando um worm se aloja em um computador, além de ser capaz de executar ações danosas ao sistema, ele também busca por meios de se auto propagar. Por exemplo, ele pode acessar a lista de contatos de e-mails dos usuários do sistema e, então, enviar cópias de si mesmo para os computadores alvos. Eles serão transmitidos por meio da internet e, quando se instalam em outros hospedeiros, o ciclo de infecção será reiniciado. Devido à capacidade de se auto copiarem e moverem entre computadores, os worms podem consumir muitos recursos da máquina hospedeira e banda de rede ou capacidades de transmissão de rede.

O que é um Trojan?

Mais conhecidos pelo termo cavalo de tróia (do inglês – Trojan Horse), os trojans são programas ou códigos maliciosos que se disfarçam de softwares legítimos para executarem ações danosas ao computador do usuário. Diferentes dos vírus e worms, eles não possuem a capacidade de se anexarem a outros arquivos e também de se autorreplicarem.

Uma das formas mais comuns de propagação deste tipo de malware, ocorre via mensagens de e-mail. De novo, estes manos gostam de um e-mail. Neste caso, eles poderão se disfarçar de programas teoricamente "inofensivos", como cartões virtuais, protetores de tela, entre outros, para infectar o sistema do usuário. A partir deste ponto, eles poderão executar ações que vão desde o acesso remoto do computador até o roubo de dados sigilosos e financeiros.

Segurança na Internet é maior com usuários mais velhos

O que é Spyware?

Estes irmãos eram legais, mas com o tempo eles foram puxados para o lado negro da maldade. Os spywares são programas espiões que, uma vez instalados no sistema do usuário, realizam o monitoramento de suas atividades e enviam as informações coletadas para terceiros, por meio da internet. Originariamente, eles tinham um enfoque mais publicitário. Ou seja, investigavam os hábitos dos usuários com o objetivo de direcionar propagandas. Com o passar do tempo, ganharam características de cunho ilegítimo como, por exemplo, o roubo de dados confidenciais.

Entre as variantes mais conhecidas dos spywares, destacam-se os adwares e os keyloggers. Enquanto o primeiro tipo possui o objetivo de apresentar propagandas (como citado anteriormente), o segundo realiza a interceptação das teclas digitadas e utiliza as informações capturadas para obter, geralmente, vantagens financeiras sobre o usuário do sistema.

O que é Rootkit?

O termo rootkit é proveniente das palavras "root" (que é um superusuário ou administrador de sistemas Unix, pronuncia-se "rut") e "kit" (um conjunto de programas usados para manter os privilégios de uma conta root). Tal tipo de malware é um programa – geralmente malicioso – que possui a capacidade de se esconder dos mecanismos de segurança do sistema do usuário.

Também caracterizados como uma espécie de trojan, os rootkits adotam um conjunto de técnicas avançadas – como a interceptação de ações do sistema operacional e a ocultação de suas chaves do registro – para garantirem tanto a sua presença como a de outros códigos maliciosos no computador alvo.

De forma semelhante outras categorias de malwares, os rootkits também são propagados por meio de arquivos enviados via e-mails ou sites da internet. Olha os e-mails de novo "aiiiiiiiii, Gentiiiiiiii, tunsquidu, tunsquidu, tunsquidu". Ao executar um arquivo malicioso, o usuário está abrindo brechas para que este tipo de praga se instale em seu sistema.

Dicas básicas de prevenção contra malwares

Como pode ser notado, o preferido dos meus manos são os e-mails, por consequência ligado a Internet. Fica bastante claro que os malwares são ameaças que estão à espreita daqueles que utilizam a internet. Portanto, é muito importante tomarmos alguns tipos de ações preventivas que visam diminuir os riscos de termos os nossos sistemas infectados por tais pragas virtuais.

Uma das formas mais básicas e eficazes de prevenção contra malwares, consiste na instalação de do meu paizão, o antivírus – que na maioria dos casos detectam vírus, worms e trojans – e antispywares. Porém, tal ação terá maior eficácia, quando for

acompanhada pela constante atualização tanto dos softwares de segurança, quanto do sistema operacional e seus programas. O ambiente contará com as soluções mais recentes para sanar as brechas.

Outro ponto que deve ser observado diz respeito às mensagens de e-mail e à navegação por meio de sites duvidosos. Muitos e-mails de remetentes maliciosos costumam conter anexos infectados ou, até mesmo, links com textos do tipo "olha esta foto que tirei com você…" ou "atualize as suas informações bancárias…". Ao pairar o mouse sobre estes tipos de links, o usuário pode notar no seu próprio navegador uma referência para arquivos do tipo zip, exe, ou até mesmo para páginas web que contenham possíveis armadilhas. Portanto, além de possuir um bom antivírus e um antispyware instalado, analise com bastante calma estes tipos de mensagens e sites. Não adianta ter tudo OK e permitir que programa seja executado ou clicar num link duvidoso. A curiosidades matou o pragão, você usuário. O usuário é o elo fraco deste conjunto todo. Todo mundo gosta de coisas gratuitas e tem muita curiosidade, mas contenha-se. Provavelmente você vai dançar. Quem avisa é o praguinha que conhece a família que tem.

O melhor sistema de segurança é você!

Não tenha dúvida com relação a esta afirmação. O usuário faz toda a diferença para a efetividade da sua própria proteção. Não adiantaria você instalar todo um arsenal de aplicativos de segurança se baixasse arquivos de fontes suspeitas e clicasse em links desconhecidos.

Boa parte da defesa do seu computador é garantida pelo seu bom senso, tomando cuidado com todo o tipo de conteúdo que reproduz na máquina. Lembre-se: o melhor sistema de segurança do seu PC é você!

Outra coisa importante, meu paizão, o antivírus, não trabalha de graça. As versões não pagas dele são para teste. Não ache que com uma versão destas instaladas você está seguro. Isto é difícil até com a comercial, imagine outra coisa qualquer.

O custo de uma versão para 3 micros, por 2 anos, fica em torno de R$90,00 a R$120,00, dependendo da versão se é mais completa e marca. Não sou garoto propaganda de nenhuma marca, apesar de lindo e fofinho, mas como membro da família das pragas garanto que não vale a economia.

Um pouco de história dos vírus

Conhecer um pouco de história é sempre bom, para verificar o tipo de evolução dos meus manos. Então vou lembrar de algumas, que perturbaram muito, eram destrutivas, tudo de forma intencional.

Vou lembrar de algumas pragas O blog **Segurança Digital**[2] elencou 10 pragas que, independentemente da sua capacidade de se disseminar, foram bastante destrutivas - intencionalmente.

1. Bugbear

O Bugbear ou Tanatos é um vírus que se espalhou por e-mail em 2002. Ele não se espalhou tanto quanto outros worms do gênero, nem mesmo pragas da mesma época, como o Klez ou LoveLetter (também conhecido como "I Love You"). Mesmo assim, ele conseguiu inundar a internet com mensagens e causar lentidão na entrega de e-mails, olha o e-mail novamente.

O Bugbear tinha uma característica interessante: as impressoras, compartilhadas na rede, eram tratadas como pastas compartilhadas. Assim, bugbear enviava o código do programa para impressoras, que então imprimiam símbolos e caracteres aparentemente sem significado. Só depois de limpar o vírus do computador é que a impressora voltava ao normal. Um grande problema é que na época não existiam tantas ferramentas para tirar o vírus. Haja paciência, não?

2. Blaster

O Blaster foi o primeiro vírus inconveniente a se espalhar automaticamente por computadores domésticos na internet, em 2003. Servidores já tinham sido contaminados por outras pragas e o vírus Opaserv passou despercebido por muitos ao infectar silenciosamente as máquinas com Windows ME, 98 e 95. Mas o Blaster não era nada silencioso: ser infectado pelo Blaster significava ver um aviso dizendo que o sistema seria reiniciado em 60 segundos. O computador ficava inutilizável, já que precisava ser constantemente reiniciado, e a icônica contagem regressiva foi parar (acidentalmente) até em transmissões de TV.

3. Witty

Apesar de ter o emoticon "(^.^)" em seu código, o Witty não era muito amigável. Ele se espalhou de um computador para outro em 2004 tirando proveito de falhas em

[2] http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-10-pragas-digitais-que-destruiram-dados-e-redes.html

softwares de segurança da Internet Security Systems, sendo até hoje o ataque de maiores proporções contra programas de proteção. Passado um tempo e depois de algumas tentativas de contaminar outros computadores na rede, o vírus começa a intercalar as tentativas de ataque com a remoção de dados aleatórios no disco, corrompendo arquivos e programas silenciosamente.

4. CryptoLocker

O CryptoLocker trouxe a "solução definitiva" (do ponto de vista dos criminosos) para os ransomware, ou "vírus de resgate". Em vírus anteriores, a chave era gerada no computador da vítima ou era fixa. No CryptoLocker, cada sistema contaminado criptografa os arquivos com uma chave específica e a chave para decifrar é diferente da chave usava para embaralhar os arquivos. Com isso, a chave necessária para reaver os arquivos jamais tem contato com o computador e não há meio para recuperar os dados sem pagar o resgate (ou até que a polícia recupere a chave diretamente dos autores da praga).

O CryptoLocker deu origem a outros vírus do gênero, que ainda estão ativos. Um deles é o CryptoWall, que é a versão de ransomware mais comum na América Latina, segundo dados da FireEye[3].

5. "100% Mexicano"

Conhecido pelo nome técnico de "Windang.B", esse vírus trata documentos do Word (arquivos ".doc") como programas, infectando-os e depois renomeando os arquivos. O código do vírus abre o documento que ainda está contido no arquivo, então, se a extensão do arquivo não for verificada, tudo parece normal. O vírus continua a contaminar arquivos, mas, depois de algumas horas, substitui o conteúdo de todos os arquivos no disco com uma mensagem em espanhol:

"O vírus MlourdesHReloaded atacou este computador (...) é um vírus 100% Mexicano, não muito perigoso, mas você foi um oponente muito fraco. Adeus! (...) Feliz 2004". Foi a mensagem, que aparecia em todos os arquivos substituídos pelo vírus, que rendeu a ele o apelido de "100% mexicano".

Só um programa de recuperação de dados pode tentar resgatar os arquivos: diferente dos vírus de resgate, o vírus não dá nenhuma possibilidade de desfazer a destruição. Por ser tão destrutivo, o vírus não se espalhou muito, mas fez várias vítimas no Brasil.

6. Michelangelo (Stoned)

O vírus Stoned criado em 1987 para atacar disquetes do MS-DOS é um dos mais notórios da época e deu origem a muitas variações. O vírus não danificava nada, exceto em circunstâncias específicas nas quais o código não funcionava direto. Mas a praga foi modificada e "variações" se espalharam. A mais notória é a "Michelangelo": criado em 1991, o vírus estava programado para apagar os primeiros setores do disco, impossibilitando o uso dos dados armazenados, sempre que a data fosse 6 de março.

---

[3] A FireEye é uma empresa líder em eliminar cyber ataques avançados que utilizam malware avançado, exploração do dia zero, e táticas de APT. As soluções da FireEye suplementam firewalls tradicionais e de próxima geração, IPS, antivírus, e gateways, que não podem impedir ameaças avançadas, deixando buracos de segurança nas redes.

Houve até quem sugeriu mudar o relógio do computador para que a data nunca fosse 6 de março, só por garantia.

7. Wiper / MBR Wiper

O Wiper é a versão moderna dos programas maliciosos que apagam discos rígidos. Segundo autoridades americanas, o Wiper teria destruído dados no Irã. Variações do ataque foram usadas contra a Coreia do Sul, onde diversos computadores foram inutilizados após uma onda de ataques sofisticados que conseguiram se infiltrar em bancos, empresas de comunicação e em uma usina de energia em 2013 e 2014.

8. Morris

A primeira praga a se espalhar automaticamente de um computador para outro na internet, em 1988. Leva o nome do seu criador, Robert Tappan Morris. Morris foi o primeiro a ter uma condenação pela lei de cibercrime norte-americana (o "Computer Fraud and Abuse Act", de 1986). O vírus era bastante persistente, consumindo recursos em excesso dos computadores da época, o que o tornou ainda mais prejudicial, mas também fácil de identificar. Partes inteiras da internet (que não era tão grande, na época) foram desconectadas para evitar que o vírus voltasse antes da limpeza nas redes estar concluída.

Outras pragas que causaram estrago semelhante em servidores da internet foram a Code Red, Slammer e Slapper.

9. Chernobyl

O vírus Chernobyl tem duas características curiosas para a época (1998): a de conseguir contaminar arquivos preenchendo "espaços", de maneira que um arquivo contaminado tem o mesmo tamanho de antes da contaminação, e a de apagar o chip da BIOS de alguns modelos de placas-mãe no dia 26 de abril, aniversário do acidente na usina nuclear de Chernobyl (daí o nome do vírus). O vírus também apaga o primeiro megabyte do disco rígido, o que impede o computador de ligar mesmo que a placa-mãe não tenha sido danificada. A data de ativação do vírus foi uma coincidência: a data também é o aniversário da criação do código. Quem teve o azar de possuir uma placa-mãe vulnerável ao código do vírus teve que substituir a peça ou pagar um técnico para retirar o chip e usar um hardware especial para reprogramá-lo. Este irmão teve várias variações, pois os usuários evitavam a data citada, então criaram um dia antes e depois. Este teve aproximadamente 11 variações. Os manos acreditam muito na frase “crescei e multiplicai”.

Um semelhante foi o “Leandro e Kelly”, só que este não tinha data e não destruía os dados. Só alterava a bios[4] Em função destes manos foi colocado uma senha no acesso bios e uma proteção contra escrita na mesma.

10. Stuxnet

O vírus Stuxnet conseguiu se infiltrar em usinas nucleares do Irã, provavelmente por meio de pen drives USB, e alterar a operação de centrífugas até danificá-las. Enquanto isso, a praga falsificava as informações que apareciam nos terminais de monitoramento,

[4] Binary input output system.

deixando engenheiros e técnicos sem entender o que acontecia. É o primeiro vírus (e até hoje o único) que conseguiu causar danos físicos. As ações da praga vieram a público em 2010.

Existem muitos outros como: madona, variações do Chernobyl, mas o primeiro que se tem noticia, aconteceu na rede mundial da IBM, via e-mail, de novo. No início da década de oitenta, de forma inocente um programador fez um e-mail desejando feliz natal, que pegava a sua lista de relacionamentos e reenviava para eles o mesmo, carregando o vírus. Depois de alguns dias o tráfego da rede caiu muito, o sistema de e-mail estava abarrotado, por pouco a rede não parou. Para resolver, não podia abrir o mesmo e era só apagar.

Anexo

Cartilha

4. Códigos maliciosos (*Malware*) [5]

Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
- pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário.

Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam* (mais detalhes nos Capítulos Golpes na Internet, Ataques na Internet e *Spam*, respectivamente).

Os principais tipos de códigos maliciosos existentes são apresentados nas próximas seções.

4.1. Vírus

[5] https://cartilha.cert.br/malware/

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

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de *e-mail*. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen-drives*.

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. Alguns dos tipos de vírus mais comuns são:

> **Vírus propagado por *e-mail*:** recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador.
> **Vírus de *script*:** escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador *Web* e do programa leitor de *e-mails* do usuário.
> **Vírus de macro:** tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).
> **Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (***M**ultimedia **M**essage **S**ervice*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

4.2. *Worm*

Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

O processo de propagação e infecção dos *worms* ocorre da seguinte maneira:

a. **Identificação dos computadores alvos:** após infectar um computador, o *worm* tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras:
   - efetuar varredura na rede e identificar computadores ativos;
   - aguardar que outros computadores contatem o computador infectado;
   - utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;
   - utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de *e-mail*.
b. **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*;
   - via canais de IRC (***I****nternet* ***R****elay* ***C****hat*);
   - via programas de troca de mensagens instantâneas;
   - incluídas em pastas compartilhadas em redes locais ou do tipo P2P (*Peer to Peer*).
c. **Ativação das cópias:** após 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 sendo executados no computador alvo no momento do recebimento da cópia;
   - diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;
   - pela realização de uma ação específica do usuário, a qual o *worm* está condicionado como, por exemplo, a inserção de uma mídia removível.

d. **Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo passa a ser também o computador originador dos ataques.

4.3. Bot e botnet

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar *spam*.

Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de *spam zombie* quando o *bot* instalado o transforma em um servidor de *e-mails* e o utiliza para o envio de *spam*.

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*.

Quanto mais zumbis participarem da *botnet* mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

O esquema simplificado apresentado a seguir exemplifica o funcionamento básico de uma *botnet*:

a. Um atacante propaga um tipo específico de *bot* na esperança de infectar e conseguir a maior quantidade possível de zumbis;
b. os zumbis ficam então à disposição do atacante, agora seu controlador, à espera dos comandos a serem executados;
c. quando o controlador deseja que uma ação seja realizada, ele envia aos zumbis os comandos a serem executados, usando, por exemplo, redes do tipo P2P ou servidores centralizados;
d. os zumbis executam então os comandos recebidos, durante o período predeterminado pelo controlador;
e. quando a ação se encerra, os zumbis voltam a ficar à espera dos próximos comandos a serem executados.

4.4. Spyware

Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

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

Legítimo: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.
Malicioso: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações

referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas *spyware* são:

***Keylogger*:** 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*.

***Screenlogger*:** similar ao *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 em *sites* de *Internet Banking*.

***Adware*:** projetado especificamente para apresentar propagandas. Pode ser 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. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

4.5. Backdoor

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.

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

Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, 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.

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se 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. Esses casos constituem uma séria 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.

4.6. Cavalo de troia (*Trojan*)

Cavalo de troia[1], *trojan* ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Exemplos de *trojans* são programas que você recebe ou obtém de *sites* na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas.

Há diferentes tipos de *trojans*, classificados[2] de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns destes tipos são:

> ***Trojan Downloader*:** instala outros códigos maliciosos, obtidos de *sites* na Internet.
> ***Trojan Dropper*:** instala outros códigos maliciosos, embutidos no próprio código do *trojan*.
> ***Trojan Backdoor*:** inclui *backdoors*, possibilitando o acesso remoto do atacante ao computador.
> ***Trojan DoS*:** instala ferramentas de 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 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 de *proxy*, possibilitando que o computador seja utilizado para navegação 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 ao atacante.
> ***Trojan Banker* ou Bancos:** coleta dados bancários do usuário, através 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.

[1] O "Cavalo de Troia", segundo a mitologia grega, foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. 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 Troia. voltar
[2] Esta classificação baseia-se em coletânea feita sobre os nomes mais comumente usados pelos programas *antimalware*. voltar

4.7. Rootkit

Rootkit[3] é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

O conjunto de programas e técnicas fornecido pelos *rootkits* pode ser usado para:

- remover evidências em arquivos de *logs* (mais detalhes na Seção 7.6 do Capítulo Mecanismos de segurança);
- instalar outros códigos maliciosos, como *backdoors*, para assegurar o acesso futuro ao computador infectado;
- esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc;
- mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede;
- capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego.

É muito importante ressaltar que o nome *rootkit* não indica que os programas e as técnicas que o compõe são usadas para obter acesso privilegiado a um computador, mas sim para mantê-lo.

Rootkits inicialmente eram usados por atacantes que, após invadirem um computador, os instalavam para manter o acesso privilegiado, sem precisar recorrer novamente aos métodos utilizados na invasão, e para esconder suas atividades do responsável e/ou dos usuários do computador. Apesar de ainda serem bastante usados por atacantes, os *rootkits* atualmente têm sido também utilizados e incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados pelo usuário e nem por mecanismos de proteção.

Há casos de *rootkits* instalados propositalmente por empresas distribuidoras de CDs de música, sob a alegação de necessidade de proteção aos direitos autorais de suas obras. A instalação nestes casos costumava ocorrer de forma automática, no momento em que um dos CDs distribuídos contendo o código malicioso era inserido e executado. É importante ressaltar que estes casos constituem uma séria ameaça à segurança do computador, pois os *rootkits* instalados, além de comprometerem a privacidade do usuário, também podem ser reconfigurados e utilizados para esconder a presença e os arquivos inseridos por atacantes ou por outros códigos maliciosos.

[3] O termo *rootkit* origina-se da junção das palavras "*root*" (que corresponde à conta de superusuário ou administrador do computador em sistemas Unix) e "*kit*" (que

corresponde ao conjunto de programas usados para manter os privilégios de acesso desta conta). voltar

4.8. Prevenção

Para manter o seu computador livre da ação dos códigos maliciosos existe um conjunto de medidas preventivas que você precisa adotar. Essas medidas incluem manter os programas instalados com as versões mais recentes e com todas as atualizações disponíveis aplicadas e usar mecanismos de segurança, como *antimalware* e *firewall* pessoal.

Além disso, há alguns cuidados que você e todos que usam o seu computador devem tomar sempre que forem manipular arquivos. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança.

Informações sobre os principais mecanismos de segurança que você deve utilizar são apresentados no Capítulo Mecanismos de segurança. Outros cuidados que você deve tomar para manter seu computador seguro são apresentados no Capítulo Segurança de computadores.

4.9. Resumo comparativo

Cada tipo de código malicioso possui características próprias que o define e o diferencia dos demais tipos, como forma de obtenção, forma de instalação, meios usados para propagação e ações maliciosas mais comuns executadas nos computadores infectados. Para facilitar a classificação e a conceituação, a Tabela 4.1 apresenta um resumo comparativo das características de cada tipo.

É importante ressaltar, entretanto, que definir e identificar essas características têm se tornado tarefas cada vez mais difíceis, devido às diferentes classificações existentes e ao surgimento de variantes que mesclam características dos demais códigos. Desta forma, o resumo apresentado na tabela não é definitivo e baseia-se nas definições apresentadas nesta Cartilha.

Tabela 4.1: Resumo comparativo entre os códigos maliciosos.

Códigos Maliciosos							
	Vírus	***Worm***	***Bot***	***Trojan***	***Spyware***	***Backdoor***	***Rootkit***
Como é obtido:							
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		✓	✓	✓	✓	✓	✓
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 próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por *e-mail*		✓	✓				
Não se propaga				✓	✓	✓	✓
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	✓				✓	✓	✓

'Supervírus' Equation é capaz de infectar hardware do disco rígido[6]

'Equation' estaria ligado ao Stuxnet, diz Kaspersky Lab.

Organizações no Brasil também sofreram ataques.

A fabricante de antivírus russa Kaspersky Lab divulgou detalhes técnicos de uma série de ataques batizada pela empresa de "Equation". Especialistas da companhia chamaram os códigos usados pelos ataques de "a Estrela da Morte da galáxia dos malwares", em referência à arma da série "Guerra nas estrelas" capaz de destruir planetas.

As informações foram publicadas nesta segunda-feira (16), junto de uma palestra sobre os ataques apresentada no Security Analyst Summit (SAS), um evento promovido pela Kaspersky Lab que ocorre em Cancun, no México.

O Equation engloba uma série de programas de espionagem usados para roubar informações de instituições financeiras, governamentais e militares, além de atacar organizações de setores como comunicação, pesquisa nuclear, nanotecnologia e empresas de segurança envolvidas no desenvolvimento de criptografia.

Os códigos foram usados apenas contra alvos específicos de espionagem. Os países mais atacados são o Irã, a Rússia e o Paquistão, o Afeganistão, a Índia, a China, a Síria e Mali. No Brasil, uma organização do setor aeroespecial aeronáutica teria sido invadida pelos espiões. A Kaspersky Lab estima que há pelo menos 500 vítimas do Equation no mundo.

Um dos componentes das pragas do grupo, chamado de "nls_933w.dll", é capaz de reprogramar o firmware de discos rígidos. O firmware é o software que controla a operação básica do disco, o que significa que o vírus infecta o próprio disco rígido, não apenas os dados nele armazenados. O firmware também controla sua própria memória, por isso o único meio garantido de remover o vírus é retirando e reprogramando fisicamente o chip do disco, o que nem sempre é possível sem danificar o hardware.

Ataques contra hardware são dificultados pelas diferenças entre fabricantes, mas isso não impediu os programadores do Equation. O "nls_933w.dll" consegue funcionar em equipamentos de mais de uma dúzia" de marcas, incluindo Seagate, Western Digital, Samsung, Toshiba, Maxtor e IBM. Apesar de a função estar presente, ela foi raramente usada, segundo a Kaspersky Lab.

Nos casos em que o disco rígido foi alterado, o vírus ganhou acesso a compartimentos de armazenamento "secretos" que não são removidos pela formatação, garantindo a permanência do código espião no sistema infectado.

Possível envolvimento dos Estados Unidos

A Kaspersky Lab não informou quem são os responsáveis pela Equation, mas revelou alguns deslizes cometidos pelos programadores dos códigos que dão pistas sobre a

---

[6] http://g1.globo.com/tecnologia/noticia/2015/02/supervirus-equation-e-capaz-de-infectar-hardware-do-disco-rigido.html - **Altieres Rohr** Especial para o G1

origem dos programas. Em um dos arquivos aparece a palavra "implante", comum no vocabulário da Agência de Segurança Nacional dos Estados Unidos (NSA).

Outra palavra encontrada nos arquivos é "Grok", que também aparece em documentos secretos da NSA publicados pelo jornal alemão "Der Spiegel".

Em outro caso, uma das pragas ligadas ao Equation, chamada de "Fanny", utilizava em 2008 uma brecha de segurança desconhecida que seria corrigida só com a descoberta do vírus Stuxnet, em 2010. Segundo documentos secretos e uma reportagem do "New York Times", o Stuxnet foi desenvolvido pela NSA em colaboração com o serviço secreto de Israel.

Distribuição via interceptação de CDs

A Kaspersky Lab informou no alerta que uma praga digital do Equation foi distribuída em 2009 por meio de um CD-ROM de uma "prestigiosa conferência científica internacional" em Houston. A vítima, que não foi identificada, recebeu o CD da organização da conferência. O disco deveria conter fotos do evento, mas era capaz de infectar o computador imediatamente ao ser lido pelo sistema, usando três falhas de segurança – duas delas sem correção na época.

Além da interceptação de encomendas durante o transporte para infectar CDs, o Equation seria distribuído também por meio de pen drives USB e sites maliciosos.

O Equation pode estar ativo pelo menos desde 2001, mas endereços usados pelos espiões chegam a ser registros datados de 1996.

O nome do grupo significa "equação" em português. A Kaspersky Lab deu esse nome por conta da preferência do grupo por complexos esquemas de criptografia. Tecnologias de criptografia costumam de depender de equações matemáticas complicadas para que a chave da criptografia (o "X") não possa ser descoberta.

Cookies

Os cookies são **pequenos arquivos de texto armazenados nos computadores pelos browsers** de Internet ao visitar sites. A informação guardada pelos cookies tem inúmeros objetivos: pode ser utilizada para **guardar preferências de visualização e personalizar páginas Web**, recolher informação demográfica sobre visitantes ou monitorizar estatísticas dos banners mostrados, entre outros.

Por exemplo, caso um utilizador visite frequentemente determinada página Web, o cookie pode recordar o nome de usuário e senhas utilizadas e automatizar o acesso à página.

Apesar dos cookies **não representarem um risco direto, podem ser utilizados de forma maliciosa por outro software** e ameaçar a privacidade dos utilizadores afetados, pois a informação contida nos cookies pode ser aproveitada para criar perfis de usuários sem estes se aperceberem, enviando os detalhes para terceiros.

Exploits (exploração de vulnerabilidades)

Trata-se de uma técnica ou programa que **explora falhas de segurança e vulnerabilidades** em determinadas comunicações, sistemas operacionais, ferramentas informáticas e mesmo em aplicações comuns de software, para permitir a **intrusão no computador afetado**.

Estas falhas permitem ações que resultam num funcionamento anormal das aplicações, podendo ser provocado intencionalmente por utilizadores maliciosos, possibilitando-lhes a execução remota de ações maliciosas, o lançamento de ataques de negação de serviços, o roubo de informação ou a alteração de privilégios.

Os principais fabricantes de software desenvolvem e disponibilizam regularmente **pacotes de correções para vulnerabilidades** que vão sendo identificadas, cujo exemplo mais conhecido são as habituais atualizações da Microsoft. A aplicação destas correções é de extrema importância para reduzir o nível de risco a que os computadores estão expostos, e impedir a sua utilização por terceiros.

FIREWALL

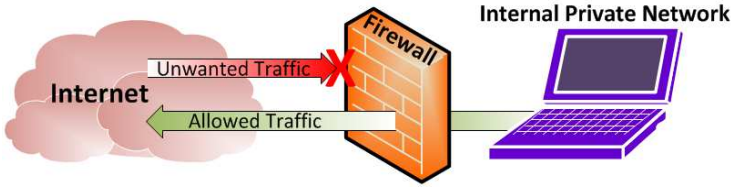
Firewall é uma solução de segurança baseada em hardware e/ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

A palavra firewall[7] tem estado cada vez mais comum no nosso cotidiano, ainda mais agora que a segurança digital está dia após dia mais em evidência. Você certamente já deve estar familiarizada com ela, mas sabe o que é o firewall ou o que ele faz? Continue acompanhando este artigo e descubra.

Parede de fogo

Assim como a metáfora por trás do nome sugere, firewall é uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo. Em inglês, "firewall" é o nome daquelas portas antichamas usadas nas passagens para as escadarias em prédios.

Na informática, os firewalls são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede mas também a confidencialidade deles.



Firewall em forma de softwares

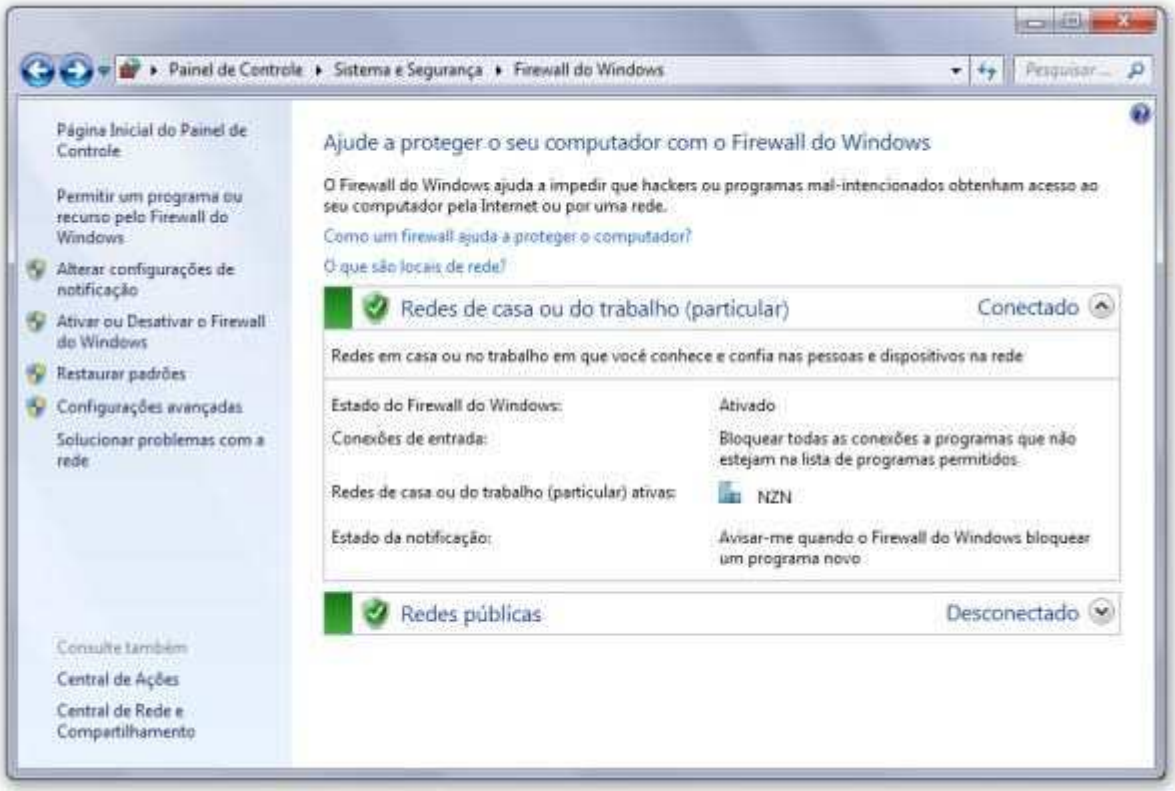
Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final.

Além do firewall presente em cada máquina, é bastante comum empresas usarem computadores específicos que agem como um "guardião" de uma rede, filtrando todo o trânsito de dados entre os PCs locais e um ambiente mais hostil, como a internet. Usando essa segunda opção, é possível até aplicar regras exclusivas como: "Máquina X pode enviar arquivos por FTP à vontade, todas as outras estão limitadas apenas a downloads".

Vale lembrar que, em ambos os casos, todas essas regras podem ser personalizadas à vontade, permitindo que o protocolo de segurança seja modificado de acordo com as

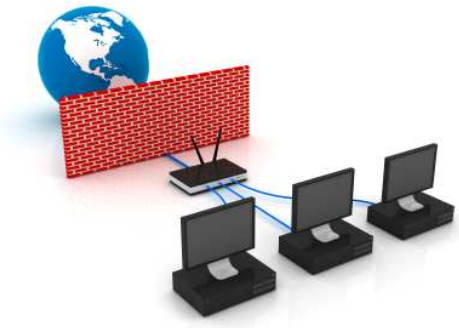
[7] https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm

suas necessidades. No Windows 7, você pode checar as configurações do firewall entrando em *Painel de Controle > Sistema e Segurança > Firewall do Windows*.



Painel de controle do firewall do Windows (Fonte da imagem: Tecmundo)

Outra medida muito usada são os filtros por portas e aplicativos. Com eles, o firewall pode determinar, exatamente, quais programas do seu computador podem ter acesso ao link de internet ou não. As portas de comunicação também podem ser controladas da mesma forma, permitindo que as portas mais "visadas" pelos malware sejam bloqueadas terminantemente.



Firewall como hardware

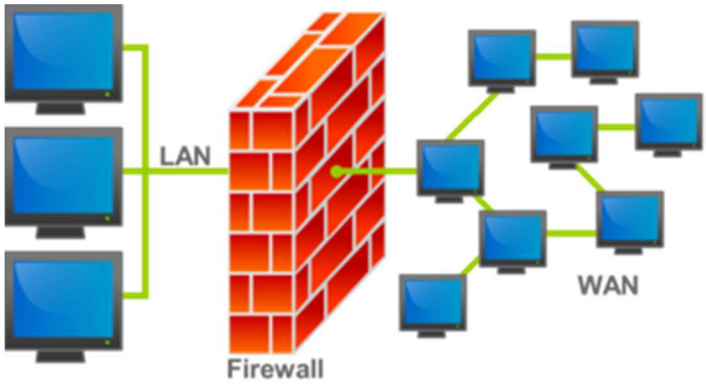
Os firewalls em forma de hardware são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais. A vantagem de usar equipamentos desse tipo é que o hardware é dedicado em vez de compartilhar recursos com outros aplicativos. Dessa forma, o firewall pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.


Equipamentos de firewall empresariais (Fonte da imagem: Reprodução/eHow)

Boa parte dos roteadores de rede domiciliar disponíveis hoje também conta com algum tipo de aplicação de firewall. Uma das mais básicas é o controle sobre os computadores que estejam habilitados a se conectar na rede, impedindo que as "sanguessugas" de plantão usem a sua Wi-Fi sem permissão. Você pode aprender mais sobre a segurança de redes sem fio com este artigo do Tecmundo.

Firewall[8] **Leitura mais técnica**

Origem: Wikipédia, a enciclopédia livre.



Firewall separando redes LAN e WAN

Um ***firewall*** (em português: parede de fogo) é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. O firewall pode ser do tipo filtros de pacotes, *proxy* de aplicações, etc. Os firewalls são geralmente associados a redes TCP/IP.

Este dispositivo de segurança existe na forma de *software* e de *hardware*, a combinação de ambos é chamado tecnicamente de "appliance". A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

[8] https://pt.wikipedia.org/wiki/Firewall

História firewall

Os sistemas *firewall* nasceram no final dos anos 80, fruto da necessidade de criar restrição de acesso entre as redes existentes, com políticas de segurança no conjunto de protocolos TCP/IP. 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 tornando-se alvos fáceis para a incipiente comunidade *hacker*.

Casos de invasões de redes e fraudes em sistemas de telefonia começaram a surgir, e foram retratados no filme *Jogos de Guerra* ("War Games"), de 1983. 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 governamentais e de ensino), provocando um verdadeiro "apagão" na rede.

O termo em inglês firewall faz alusão comparativa da função que este desempenha para evitar o alastramento de acessos nocivos dentro de uma rede de computadores a uma parede anti-chamas, que evita o alastramento de incêndios pelos cômodos de uma edificação.

Primeira Geração - Filtros de Pacotes

- A tecnologia foi disseminada em 1988 através de pesquisa sustentada pela DEC;
- Bill Cheswick e Steve Bellovin da AT&T desenvolvem o primeiro modelo para *Prova de Conceito*;
    - O modelo tratava-se de um filtro de pacotes responsável pela avaliação de pacotes do conjunto de protocolos TCP/IP;
    - Apesar do principal protocolo de transporte TCP orientar-se a um estado de conexões, o filtro de pacotes não tinha este objetivo inicialmente (uma possível vulnerabilidade);

Até hoje, este tipo de tecnologia adota um equipamento de rede para permitir configurações de acesso simples (as chamadas "listas de acesso"). O *ipchains* é um exemplo recente de um *firewall* que utiliza a tecnologia desta geração. Hoje o "ipchains" foi substituído pelo iptables que é nativo do Linux e com maiores recursos.

Regras Típicas na 1ª Geração

- Restringir tráfego baseado no endereço IP de origem ou destino;
- Restringir tráfego através da porta (TCP ou UDP) do serviço.

Segunda Geração - Filtros de Estado de Sessão

- A tecnologia foi disseminada a partir de estudo desenvolvido no começo dos anos 90 pelo Bell Labs;
- Pelo fato de o principal protocolo de transporte TCP orientar-se por uma tabela de estado nas conexões, os filtros de pacotes não eram suficientemente efetivos se não observassem estas características;
- Foram chamados também de *firewall* de circuito.

Regras Típicas na 2ª Geração

- Todas as regras da 1ª Geração;
- Restringir o tráfego para início de conexões (NEW);
- Restringir o tráfego de pacotes que tenham sido iniciados a partir da rede protegida (ESTABLISHED);
- Restringir o tráfego de pacotes que não tenham número de sequência corretos.

Firewall Statefull: Armazena o estado das conexões e filtra com base nesse estado. Existe três estados para uma conexão:

- NEW: Novas conexões;
- ESTABLISHED: Conexões já estabelecidas, e;
- RELATED: Conexões relacionadas a outras existentes.

Terceira Geração - Gateway de Aplicação

- Baseado nos trabalhos de Gene Spafford (co-autor do livro *Practical Unix and Internet Security*), Marcos Ranum (fundador da empresa TIS), e Bill Cheswick;
- Também são conhecidos como "*Firewall* de Aplicação" ou "Firewall Proxy";
- Foi nesta geração que se lançou o primeiro produto comercial em 13 de Junho de 1991—o SEAL da DEC;
- Diversos produtos comerciais surgiram e se popularizaram na década de 90, como os *firewalls* Raptor, Gauntlet (que tinha sua versão gratuita batizada de TIS) e Sidewinder, entre outros;
- Não confundir com o conceito atual de ''Firewall'' de Aplicação: *firewalls* de camada de Aplicação eram conhecidos desta forma por implementarem o conceito de *Proxy* e de controle de acesso em um único dispositivo (o *Proxy Firewall*), ou seja, um sistema capaz de receber uma conexão, decodificar protocolos na camada de aplicação e interceptar a comunicação entre cliente/servidor para aplicar regras de acesso;

Regras Típicas na 3ª Geração

- Todas as regras das gerações anteriores;
- Restringir acesso FTP a usuários anônimos;
- Restringir acesso HTTP para portais de entretenimento;
- Restringir acesso a protocolos desconhecidos na porta 443 (HTTPS).

Quarta Geração e subsequentes

- O *firewall* consolida-se como uma solução comercial para redes de comunicação TCP/IP;
    - *Stateful Inspection* para inspecionar pacotes e tráfego de dados baseado nas características de cada aplicação, nas informações associadas a todas as camadas do modelo OSI (e não apenas na camada de rede ou de aplicação) e no estado das conexões e sessões ativas;
    - Prevenção de Intrusão para fins de identificar o abuso do protocolo TCP/IP mesmo em conexões aparentemente legítimas;
    - *Deep Packet Inspection* associando as funcionalidades do *Stateful Inspection* com as técnicas dos dispositivos IPS;

- A partir do início dos anos 2000, a tecnologia de *Firewall* foi aperfeiçoada para ser aplicada também em estações de trabalho e computadores domésticos (o chamado "*Firewall* Pessoal"), além do surgimento de soluções de *firewall* dedicado a servidores e aplicações específicas (como servidores Web e banco de dados), ou mesmo usuários.

Classificação

Os sistemas *firewall* podem ser classificados da seguinte forma:

Filtros de Pacotes

Estes sistemas analisam individualmente os pacotes à medida que estes são transmitidos, verificando apenas o cabeçalho das camadas de rede (camada 3 do modelo ISO/OSI) e de transporte (camada 4 do modelo ISO/OSI).

As regras podem ser formadas indicando os endereços de rede (de origem e/ou destino) e as portas TCP/IP envolvidas na conexão. A principal desvantagem desse tipo de tecnologia para a segurança reside na falta de controle de estado do pacote, o que permite que agentes maliciosos possam produzir pacotes simulados (com endereço IP falsificado, técnica conhecida como IP Spoofing), fora de contexto ou ainda para serem injetados em uma sessão válida. Esta tecnologia foi amplamente utilizada nos equipamentos de 1a.Geração (incluindo roteadores), não realizando nenhum tipo de decodificação do protocolo ou análise na camada de aplicação.

Proxy Firewall ou Gateways de Aplicação

Os conceitos de *gateways* de aplicação (*application-level gateways*) e "bastion hosts" foram introduzidos por Marcus Ranum em 1995. Trabalhando como uma espécie de eclusa, o *firewall* de *proxy* trabalha recebendo o fluxo de conexão, tratando as requisições como se fossem uma aplicação e originando um novo pedido sob a responsabilidade do mesmo *firewall* (*non-transparent proxy*) para o servidor de destino. A resposta para o pedido é recebida pelo *firewall* e analisada antes de ser entregue para o solicitante original.

Os *gateways* de aplicações conectam as redes corporativas à Internet através de estações seguras (chamadas de *bastion hosts*) rodando aplicativos especializados para tratar e filtrar os dados (os *proxy firewalls*). Estes *gateways*, ao receberem as requisições de acesso dos usuários e realizarem uma segunda conexão externa para receber estes dados, acabam por esconder a identidade dos usuários nestas requisições externas, oferecendo uma proteção adicional contra a ação dos *crackers*.

Desvantagens

- Para cada novo serviço que aparece na Internet, o fabricante deve desenvolver o seu correspondente agente de *Proxy.* Isto pode demorar meses, tornando o cliente vulnerável enquanto o fabricante não libera o agente específico. A instalação, manutenção e atualização dos agentes do *Proxy* requerem serviços especializados e podem ser bastante complexos e caros;
- Os *proxy's* introduzem perda de desempenho na rede, já que as mensagens devem ser processadas pelo agente do *Proxy*. Por exemplo, o serviço FTP manda

um pedido ao agente do *Proxy* para FTP, que por sua vez interpreta a solicitação e fala com o servidor FTP externo para completar o pedido;
- A tecnologia atual permite que o custo de implementação seja bastante reduzido ao utilizar CPUs de alto desempenho e baixo custo, bem como sistemas operacionais abertos (Linux), porém, exige-se manutenção específica para assegurar que seja mantido nível de segurança adequado (ex.: aplicação de correções e configuração adequada dos servidores).

Stateful Firewall (ou Firewall de Estado de Sessão)

Os *firewalls* de estado foram introduzidos originalmente em 1991 pela empresa DEC com o produto SEAL, porém foi só em 1994, com os israelenses da Checkpoint, que a tecnologia ganharia maturidade suficiente. O produto Firewall-1 utilizava a tecnologia patenteada chamada de *Stateful Inspection*, que tinha capacidade para identificar o protocolo dos pacotes transitados e "prever" as respostas legítimas. Na verdade, o *firewall* guardava o estado de todas as últimas transações efetuadas e inspecionava o tráfego para evitar pacotes ilegítimos.

Posteriormente surgiram vários aperfeiçoamentos, que introduziram o *Deep Packet Inspection*, também conhecido como tecnologia SMLI (*Stateful Multi-Layer Inspection*), ou seja *Inspeção de Total* de todas as camadas do modelo ISO/OSI (7 camadas). Esta tecnologia permite que o *firewall* decodifique o pacote, interpretando o tráfego sob a perspectiva do cliente/servidor, ou seja, do protocolo propriamente dito e inclui técnicas específicas de identificação de ataques.

Com a tecnologia SMLI/*Deep Packet Inspection*, o *firewall* utiliza mecanismos otimizados de verificação de tráfego para analisá-los sob a perspectiva da tabela de estado de conexões legítimas. Simultaneamente, os pacotes também vão sendo comparados a padrões legítimos de tráfego para identificar possíveis ataques ou anomalias. A combinação permite que novos padrões de tráfegos sejam entendidos como serviços e possam ser adicionados às regras válidas em poucos minutos.

Supostamente a manutenção e instalação são mais eficientes (em termos de custo e tempo de execução), pois a solução se concentra no modelo conceitual do TCP/IP. Porém, com o avançar da tecnologia e dos padrões de tráfego da Internet, projetos complexos de *firewall* para grandes redes de serviço podem ser tão custosos e demorados quanto uma implementação tradicional.

Firewall de Aplicação

Com a explosão do comércio eletrônico, percebeu-se que mesmo a última tecnologia em filtragem de pacotes para TCP/IP poderia não ser tão efetiva quanto se esperava. Com todos os investimentos dispendidos em tecnologia de *stateful firewalls*, os ataques continuavam a prosperar de forma avassaladora. Somente a filtragem dos pacotes de rede não era mais suficiente. Os ataques passaram a se concentrar nas características (e vulnerabilidades) específicas de cada aplicação. Percebeu-se que havia a necessidade de desenvolver um novo método que pudesse analisar as particularidades de cada protocolo e tomar decisões que pudessem evitar ataques maliciosos contra uma rede.

Apesar de o projeto original do TIS Firewall concebido por Marcos Ranum já se orientar a verificação dos métodos de protocolos de comunicação, o conceito atual de *Firewall* de Aplicação nasceu principalmente pelo fato de se exigir a concentração de esforços de análise em protocolos específicos, tais como servidores Web e suas conexões de

hipertexto HTTP. A primeira implementação comercial nasceu em 2000 com a empresa israelense Sanctum, porém, o conceito ainda não havia sido amplamente difundido para justificar uma adoção prática.

Se comparado com o modelo tradicional de *Firewall* -- orientado a redes de dados, o *Firewall* de Aplicação é frequentemente instalado junto à plataforma da aplicação, atuando como uma espécie de procurador para o acesso ao servidor (Proxy).

Alguns projetos de código-aberto, como por exemplo o ModSecurity para servidores Apache, IIS e Nginx, têm por objetivo facilitar a disseminação do conceito para as aplicações Web.

Vantagens

- Pode suprir a deficiência dos modelos tradicionais e mapear todas as transações específicas que acontecem na camada da aplicação Web proprietária;
- Por ser um terminador do tráfego SSL, pode avaliar hipertextos criptografadas (HTTPS) que originalmente passariam despercebidos ou não analisados por *firewalls* tradicionais de rede;

Desvantagens

- Pelo fato de embutir uma grande capacidade de avaliação técnica dos métodos disponibilizados por uma aplicação (Web), este tipo de *firewall* exige um grande poder computacional—geralmente traduzido para um grande custo de investimento;
- Ao interceptar aplicações Web e suas interações com o cliente (o navegador de Web), pode acabar por provocar alguma incompatibilidade no padrão de transações (fato que exigirá, sem sombra de dúvidas, um profundo trabalho de avaliação por parte dos implementadores);
- Alguns especialistas ou engenheiros de tecnologia refutam o *firewall* de aplicação baseando-se nas seguintes argumentações:
    - A tecnologia introduz mais um ponto de falha sem adicionar significativos avanços na tecnologia de proteção;
    - O *firewall* e o IDS/IPS já seriam suficientes para cobrir grande parte dos riscos associados à aplicação Web;
    - A tecnologia ainda precisa amadurecer o suficiente para ser considerada um componente indispensável de uma arquitetura de segurança;

Certamente esses argumentos serão bastante discutidos ao longo dos próximos anos como um imperativo para determinar a existência desta tecnologia no futuro.