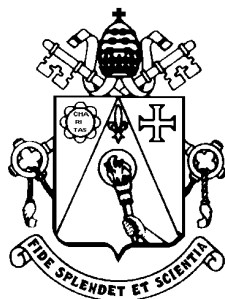


Segurança da Informação

Perigos do Mundo Virtual¹



Pontifícia Universidade Católica de Campinas
Faculdade de Análise de Sistemas

Guilherme Cestaroli Seleguim²

Resumo

Você precisa ter consciência de que seu computador é uma porta aberta para o mundo, com a agravante de não se poder ver quem o está olhando. Quem compartilha um universo tão diversificado, deveria, independentemente de qualquer coisa, prevenir-se contra surpresas desagradáveis.

Palavras-chave

Segurança da Informação; Internet; Hackers; Crackers; Trojans; Rede de Computadores;

Security of Information–Dangers in the Virtual World

Summary

You need to know that your computer is an open door to the world, the problem is that you can't see who is watching you. When you are sharing a universe that is so diversified, you should, be independent of anything, protect yourself against disagreeable surprises.

Keywords

Security of Information; Internet; Hackers; Crackers; Trojans; Computer Networks;

¹ Trabalho desenvolvido na Faculdade de Análise de Sistemas da PUC-Campinas

² Aluno da Faculdade de Análise de Sistemas da PUC-Campinas

1. Introdução

No final da década de 60, surgia a Internet. Inicialmente ela foi criada e desenvolvida para ser utilizada pelo exército americano, a fim de não centralizar todas as informações registradas em computadores em um único local do país. Desta forma, ficaria muito vulnerável quanto à destruição dos servidores por forças militares inimigas. Como solução, resolveram distribuir os dados em vários servidores distribuídos por todo o território nacional, todos interligados compartilhando as informações.

Para a comunicação entre os servidores, foram criados protocolos, dentre os quais está o protocolo IP³, que hoje em dia é o principal protocolo usado na Internet. O protocolo IP foi criado somente para a transmissão de informações entre os servidores do exército, então não se preocuparam com a segurança contra a captação de informações entre os servidores.

Com o crescimento e a popularização da Internet, englobando não só computadores militares americanos, mas muitos outros pelo mundo, com transmissão de vários tipos de informações, e acessados por vários perfis de pessoas, surge a necessidade de assegurar que as informações trafegadas na rede estarão seguras.

Transações bancárias e *e-commerce* (comércio via Internet) necessitam de muita segurança, pois trafegam informações dos usuários de suma importância e sigilo, tais como números de cartão de crédito e senhas. Estas informações devem ser protegidas tanto para a transmissão quanto no armazenamento e acesso posterior. Informações corporativas e documentos confidenciais também devem ser protegidos[BREDARIOL, 2001].

Muitas empresas e usuários domésticos não se preocupam tanto com a segurança de seus sistemas, podendo levar à perda de dados, indisponibilização de um serviço, indisponibilização de um sistema, entre outras possibilidades mais graves.

A maioria dos ataques são feitos à distância, geralmente por *Hackers*⁴ e *Crackers*⁵ que se utilizam da Internet para conseguirem acesso às máquinas internas das empresas, mas um ponto muito importante é a segurança física dos computadores e da própria rede corporativa.

3 IP: Internet Protocol. Endereço de computador em uma rede, utilizado para a comunicação entre computadores na rede. Exemplo de endereço IP: 200.231.13.13.

4 Hacker: Tem conhecimentos reais de programação e de sistemas operacionais, principalmente o Linux e o Unix, que são os mais usados em servidores da Internet. Conhece quase todas as falhas de segurança dos sistemas e está sempre em busca de outras. Desenvolve suas próprias técnicas e programas de invasão[M@RCIO, 2000].

5 Cracker: É o “Hacker do Mal”, que invade sistemas, rouba dados e arquivos, números de cartão de crédito, faz espionagem industrial e quase sempre provoca algum tipo de destruição, principalmente de dados. É confundido pela imprensa que lhe atribui erroneamente o nome de Hacker[M@RCIO, 2000].

2. Importância do Tema

Atualmente o investimento em segurança das informações não é mais uma opção e sim uma exigência da coletividade pois o vazamento de dados críticos pode causar prejuízos de grande quantidade para toda a sociedade.

Até pouco tempo atrás o investimento em segurança das informações era uma opção da empresa, pois não havia nenhuma exigência legal. Passado algum tempo, o investimento passou a ser necessário pois proporcionava maior confiança dos consumidores nas empresas e agregava valor aos produtos. Hoje, o investimento no setor de segurança das informações passou a ser uma exigência legal porque a própria lei, em diversos diplomas, passou a exigir a conservação de arquivos em formato digital. Como por exemplo:

O art. 11 da Lei nº 8.218, de 29 de agosto de 1991 determina que as pessoas jurídicas que possuem patrimônio líquido superior a Cr\$ 250.000.000,00 e utilizam sistema de processamento eletrônico de dados para registrar negócios e atividades econômicas, escriturar livros ou elaborar documentos de natureza contábil ou fiscal ficarão obrigados à manter, em meio magnético ou assemelhado, à disposição do Departamento da Receita Federal, os respectivos arquivos e sistemas durante o prazo de cinco anos. A inobservância poderá acarretar multa de meio por cento do valor da receita bruta da pessoa jurídica no período ou multa de cinco por cento sobre o valor da operação correspondente, aos que omitirem ou prestarem incorretamente as informações solicitadas.

As empresas que trabalham com venda ao consumidor final também estão obrigadas a aumentar seus investimentos em segurança da informação pois segundo o Código de Defesa do Consumidor (Lei nº 8.078/90) art. 39, inciso VIII, é vedado ao fornecedor de produtos ou serviços colocar no mercado de consumo qualquer produto ou serviço em desacordo com as normas expedidas pelos órgãos oficiais competentes ou, se normas específicas não existirem, pela Associação Brasileira de Normas Técnicas (ABNT).

Pela própria inteligência dos artigos supramencionados vê-se que o investimento em segurança das informações é uma obrigação e todos aqueles que não se atêm a esta situação poderão amargar grandes prejuízos[GOMES, 2002].

3. Como a Segurança é Burlada

3.1 Técnica de invasão

Invasão é a entrada em um site, servidor, computador ou serviço por alguém não autorizado. Mas antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objetivo é avaliar a segurança de uma rede e identificar seus pontos vulneráveis.

Mas não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como *Hacker* ou *Cracker*. Ambos usam seus conhecimentos para se dedicarem a testar os limites de um sistema, ou para estudo e busca de conhecimento ou por curiosidade, ou para encontrar formas de quebrar sua segurança ou ainda, por simples prazer.

Mas também pode ser por mérito, para promoção pessoal, pois suas descobertas e ataques são divulgados na mídia e eles se tornam conhecidos no seu universo, a diferença é que o *Cracker* utiliza as suas descobertas para prejudicar financeiramente alguém, em benefício próprio, ou seja, são os que utilizam seus conhecimentos para o mau.

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a respeito. Abaixo serão descritas algumas das mais conhecidas.

3.1.1 Spoofing

Nesta técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um usuário externo se faz passar por um usuário ou computador interno.

3.1.2 Sniffers

É um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegalmente por um intruso, para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações TCP/IP não serem criptografados.

Entretanto, para utilizar o sniffer, é necessário que ele esteja instalado em um ponto da rede, onde passe tráfego de pacotes de interesse para o invasor ou administrador.

3.1.3 Ataque do tipo DoS - Denial of Service

É um ataque de recusa de serviço, estes ataques são capazes de tirar um site do ar, indisponibilizando seus serviços. É baseado na sobrecarga da capacidade ou em uma falha não prevista.

Um dos motivos para existirem esse tipo de falha nos sistemas é um erro básico de programadores, na hora de testar um sistema, muitas vezes, eles não testam o que acontece se um sistema for forçado a dar erro, se receber muitos pacotes em pouco tempo ou se receber pacotes com erro, normalmente é testado o que o sistema deveria fazer e alguns erros básicos. O invasor parte deste princípio e fica fazendo diversos tipos de testes de falhas, até acontecer um erro e o sistema parar.

Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo indeterminado, dependendo da equipe existente na empresa para disponibilizá-lo novamente e dependendo do negócio da empresa, este tempo de indisponibilidade pode trazer muitos prejuízos.

De acordo com um estudo da Universidade da Califórnia, *Crackers* tentam realizar em torno de 4 mil ataques do tipo DoS por semana. Os alvos mais comuns são grandes empresas.

3.1.4 Ataque do tipo DDoS – Distributed Denial of Service

São ataques semelhantes ao DoS, tendo como origem diversos e até milhares de pontos disparando ataques DoS para um ou mais sites determinados. Para isto, o invasor coloca agentes para dispararem o ataque em uma ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes, ao serem executados, se transformam em um ataque DoS de grande escala. Uma ferramenta criada recentemente, de nome *DDoS Attack*, desenvolvida pelo programador brasileiro que se intitula OceanSurfer⁶, é capaz de causar negação de serviços em computadores na Internet através de uma inundação de conexões em determinada porta.

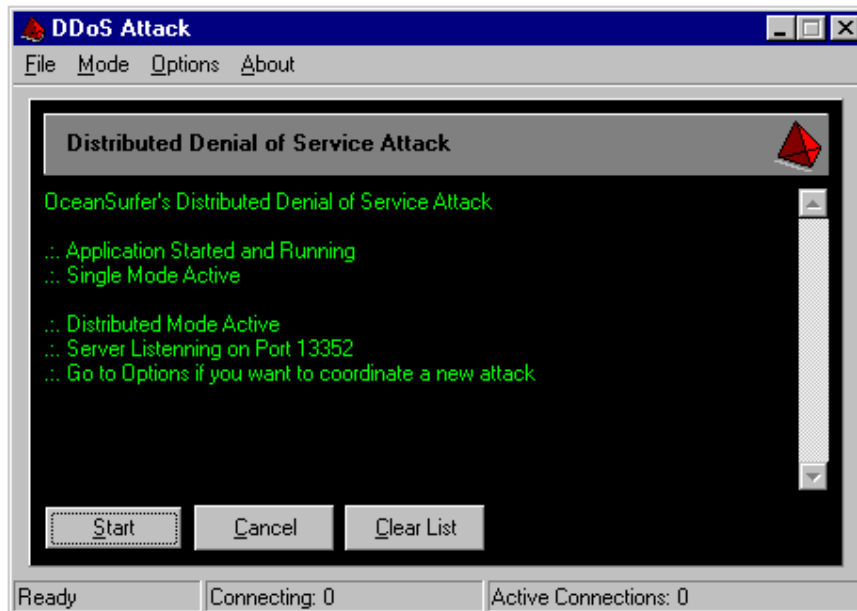


Fig. 1 – *DDoS Attack* de OceanSurfer

3.1.4.1 Funcionamento Técnico do DDoS Attack

O software foi escrito em Delphi 5 com o intuito de ajudar administradores de redes a sanarem possíveis falhas em configurações de softwares na rede que se utilizam de *sockets* para funcionarem, especificamente softwares servidores de serviços. À seguir seguem informações técnicas sobre o programa.

3.1.4.1.1 Portas

Portas identificam serviços que rodam em servidores. Um servidor pode conter vários serviços instalados, ou seja, o mesmo computador pode ser um servidor de correio eletrônico, servidor de FTP (*File Transfer Protocol* ou Protocolo de Transferência de Arquivos) e servidor Web (páginas na Internet);

O servidor é identificado por um endereço IP, mas os serviços também precisam

⁶ OceanSurfer: Pode ser encontrado em: oceansurfer@newocean.cjb.net e pelo UIN:69340992 no programa ICQ.

ser identificados individualmente. Para cada serviço, então, é associada uma **porta** que é um número de identificação entre 0 e 65535. Existem programas chamados de *scanners* que podem verificar quais portas estão abertas em um computador remoto como por exemplo o *scanner* construído também por OceanSurfer.

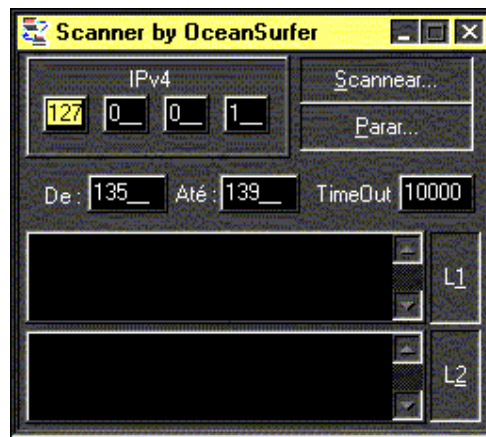


Fig. 2 – Scanner de portas de OceanSurfer

3.1.4.1.2 Os Sockets

Um *socket*, por definição, é um canal de comunicação entre computadores em uma rede e identifica uma conexão entre eles, normalmente entre um cliente e um servidor. Através dos *sockets* os computadores podem trocar informações através de uma rede. Para identificar uma conexão ente dois computadores, um *socket* deve ser definido, por meio das seguintes informações:

- Endereço IP do servidor;
- Porta onde se encontra o serviço solicitado;
- Endereço IP do cliente;
- Porta através da qual o cliente solicita o serviço.

Um bom exemplo de um estabelecimento de uma conexão entre computadores através de *socket* seria o acesso à uma página da Internet. Um servidor Web tem a porta 80 como porta padrão de comunicação entre os clientes. Quando digitamos um endereço de um site no Internet Explorer do Windows, automaticamente esse endereço é convertido em seu respectivo endereço IP. Se estamos numa rede, nosso micro tem um único endereço IP. E finalmente, junto deste processo, uma porta em seu computador é disponibilizada dinamicamente, sendo um número maior que 1024, para esta conexão.

Então, temos todas as informações necessárias para estabelecer a conexão, tendo assim um *socket*. O cliente, no caso de uma conexão à uma página da Internet, é quem a solicita através de um *browser* (Internet Explorer, por exemplo), e o servidor é quem disponibiliza a página para ser acessada.

Como visto, o servidor Web trabalha na porta 80, enquanto que outros serviços têm também suas respectivas portas padrão, como o FTP que trabalha na porta 21, o Telnet que trabalha na porta 23, o SMTP que trabalha na porta 25 e o POP3 que trabalha na porta 110.

3.1.4.1.3 A ação do programa

Para o programa funcionar, é necessário saber qual a porta que se quer testar e qual o IP do computador alvo na rede. É solicitado a quantidade de tentativas de conexões simultâneas que se deseja fazer para a determinada porta. Basta então clicar no botão *Start* e é iniciado o ataque e se o software que estiver trabalhando na porta determinada for mal construído, com certeza será derrubado e parará de operar, indisponibilizando aquele serviço.

O teste pode ser feito de um atacante só, ou também em modo distribuído, com quantos atacantes quiserem. O interessante é que mesmo sem estar em modo distribuído, foi constatada falha em diversos programas, inclusive em *Firewalls*, que travavam, comprometendo em muito a segurança das redes.

3.1.5 Quebra de Senhas

Para acessar algo é necessário uma senha de acesso, muitos invasores tentam quebrar estas senhas através de técnicas de quebras de senhas, como tentar as senhas padrões de sistemas ou as senhas simples como nomes pessoais, nome da empresa, datas, entre outros. Mas para facilitar a descoberta da senha, existem diversos programas, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobrir a senha.

3.1.6 Vírus

O vírus de computador é outro exemplo de programa de computador, utilizado maliciosamente ou não, que se reproduz embutindo-se em outros programas. Quando estes programas são executados, o vírus é ativado e pode se espalhar ainda mais, geralmente danificando sistemas e arquivos do computador onde ele se encontra. Um exemplo deste tipo de programa é o *Worm*, criado por Robert Morris[**SETTE, 2001**].

Os vírus não surgem do nada, ou seja, seu computador não tem a capacidade de criar um vírus, quem cria os vírus são programadores de computador mal intencionados. Os vírus se ocultam em arquivos executáveis, ou seja, com extensão .EXE ou .COM, e de bibliotecas compartilhadas, de extensão .DLL.

Quanto a arquivos de dados, você pode abrí-los sem medo! Assim, pode rodar tranquilamente seus arquivos de som (.WAV, .MID, .MP3), imagem (.BMP, .PCX, .GIF, .JPG), vídeo (.AVI, .MOV) e os de texto que não contenham macros (.TXT, .WRI, .DOC), mas Kerñell⁷, um especialista em sistemas Linux, afirma que esses arquivos não são totalmente seguros e que as falhas podem ser exploradas.

Para que o vírus faça alguma coisa, não basta você tê-lo em seu computador.

7 Kerñell: Certificado como Engenheiro Linux e Desenvolvedor de Sistemas Linux, pode ser encontrado em: kernel_hacked@ig.com.br e pelo UIN:117168826 no programa ICQ.

Para que ele seja ativado, passando a infectar o micro, é preciso executar o programa que o contém. E isto você só faz se quiser, mesmo que não seja de propósito. Ou seja, o vírus só é ativado se você der a ordem para que o programa seja aberto, por ignorar o que ele traz de mal pra você. Se eles não forem “abertos”, “executados”, o vírus simplesmente fica alojado inativo, aguardando ser executado para infectar o computador.

Após infectar o computador, eles passam a atacar outros arquivos. Se um destes arquivos infectados for transferido para outro computador, este também vai passar a ter um vírus alojado, esperando o momento para infectá-lo, ou seja, quando for também executado. Daí o nome de vírus, devido à sua capacidade de auto-replicação, parecida com a de um ser vivo.

Por que os vírus são escritos ? Esta pergunta foi feita na convenção de Hackers e fabricantes de vírus na Argentina. As respostas seguem abaixo:

- *Beacause it's fun;*
- Para estudar as possibilidades relativas ao estudo de vida artificial (de acordo com a frase de Stephen Hawkind: “Os vírus de computador são as primeiras formas de vida feitas pelo homem”). Esta proposta é seguida por vários cientistas.
- Para descobrir se são capazes de fazer isso, tentando seus conhecimentos de computação, ou para mostrarem aos colegas que são capazes de fazer;
- Para conseguir fama;
- Fins militares. Falou-se sobre isso na Guerra do Golfo, mas os vírus para uso militar são uma possibilidade.

3.1.7 Trojans

A denominação “Cavalo de Tróia” (Trojan Horse) foi atribuída aos programas que permitem a invasão de um computador alheio com espantosa facilidade. Nesse caso, o termo é análogo ao famoso artefato militar fabricado pelos gregos espartanos. Um “amigo” virtual presenteia o outro com um “presente de grego”, que seria um aplicativo qualquer. Quando o leigo o executa, o programa atua de forma diferente do que era esperado.

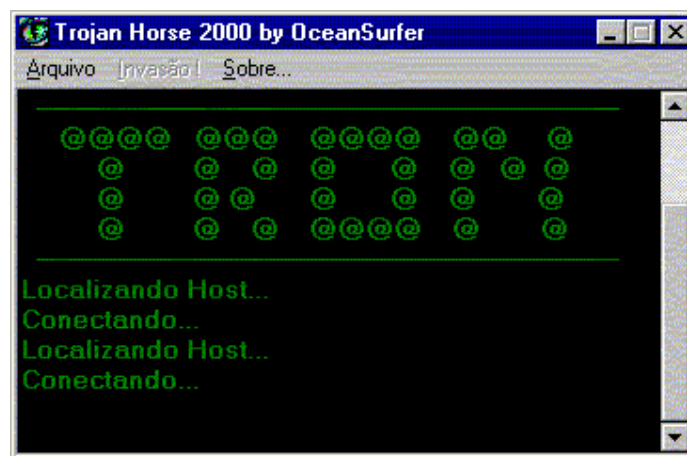


Fig. 3 – Trojan Horse (parte cliente) de OceanSurfer

Ao contrário do que é erroneamente informado na mídia, que classifica o Cavalo de Tróia como um vírus, ele não se reproduz e não tem nenhuma comparação com vírus

de computador, sendo que seu objetivo é totalmente diverso. Deve-se levar em consideração, também, que a maioria dos antivírus fazem a sua detecção e os classificam como tal. A expressão “Trojan” deve ser usada, exclusivamente, como definição para programas que capturam dados sem o conhecimento do usuário.

O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conectar-se à Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente. Só quem já esteve dentro de um computador alheio sabe as possibilidades oferecidas[M@RCIO, 2000].

4. Acontecimentos

4.1 Kevin Mitnick

Periodicamente, muitas histórias sobre *Hackers* e *Crackers* são contadas através dos veículos de comunicação. A mais popularizada no mundo foi a de dois personagens feríssimas. Eles se chamam Kevin Mitnick e Tsutomu Shimomura (o farejador). Kevin era um garotão californiano, autoconfiante, que roubou, nada mais, nada menos, que cerca de 20.000 números de cartões de crédito dos associados da rede Netcom, que também é uma provedora de acesso à Internet. Não satisfeito com sua façanha e tendo conhecimento da existência de Shimomura como o principal especialista em segurança de redes de computadores ligado ao FBI, Mitnick desconfiou que estaria sendo perseguido por ele. Então invadiu o computador desse gênio nipo-americano e, por várias vezes, deixou mensagens de desafio e afronta – do tipo “sou o melhor” – para chamar-lhe mais ainda a atenção.



Com o sangue frio que caracteriza sua ascendência, Shimomura começou um processo de investigação digno de cinema e ficou sabendo que os dados que haviam sido tirados de seu computador por Kevin estavam armazenados na Netcom. O segurança cibernético não titubeou e rumou para San Jose, na Califórnia, onde está localizada a empresa.

Um dos erros de Kevin Mitnick foi subestimar a capacidade de Shimomura e pensar que jamais poderia ser rastreado pelo agente americano, o que resultou numa tremenda caçada por parte desse que é considerado o maior farejador cibernético da atualidade. Ao chegar à cidade, Shimomura descobriu que as ligações de Mitnick eram provenientes de um telefone celular da Carolina do Norte. Com toda colaboração da companhia telefônica e após muitas peregrinações, ele conseguiu um carro munido de aparelhos sofisticados, capazes de captar a frequência de telefones celulares. De posse destes recursos, ficou fácil a captura de Mitnick.

