

DI|S|I

Dia Internacional de
Segurança em Informática

Kit Básico de Sobrevivência na Internet



Ronaldo Castro de Vasconcellos
Analista de Segurança, CAIS/RNP

Dia Internacional
de Segurança em Informática
30 de Novembro de 2005



Introdução

- Nenhuma das soluções é isolada
- Dicas para usuários domésticos
- **Usuários corporativos: consulte o departamento de informática responsável antes de tomar qualquer ação**
 - Correções de segurança podem afetar aplicações
 - Instalação de falsas correções (hoax)
- Dicas voltada para usuários de Windows



1. Personal Firewall

- **Companheiro inseparável: Anti-Vírus**
- **Instale-o antes de qualquer outro software, antes de conectar a máquina à Internet de preferência**
- **Funciona como um guarda que cuida da entrada e saída de tráfego de rede de sua máquina, permitindo ou negando baseado no que você determinou.**
Também chamado de “Desktop Firewall”.

- **O Personal Firewall perfeito (Jeff Sengstack, 2000):**

- **barato, fácil de instalar e usar**
- **configuração clara e bem explicada**
- **registra ameaças reais e em potencial**
- **alerta a respeito de ataques sérios**
- **garante que nada entre ou saia de seu PC sem sua autorização**



1. Personal Firewall (2)

- É comum que possuam funções de privacidade, bloqueio de pop-up e banners de propaganda
- Mais importante que instalar é saber qual sua função e como operá-lo
- Cada filtro normalmente se baseia em 3 variáveis:
 - porta de origem e destino
 - máquina de origem e destino
 - aplicação
- Exemplo:
 - Permitir Mozilla Firefox, qualquer máquina remota `www.example.com`, portas 80 (HTTP) ou 443 (HTTP Seguro)



1. Personal Firewall (3)



1. Personal Firewall (4)

- **Dicas de uso**
 - **Leia o manual do usuário**
 - **Remova todas as regras periodicamente e execute todas os seus softwares que necessitam de acesso Internet em seguida**
 - **Desabilite o Windows Firewall (SP2) ou versões anteriores se optar por um software de terceiros**
 - **Lembre-se de que existem programas do sistema (Windows) que usam a rede (lsass.exe, spoolsv.exe, svchost.exe, userinit.exe, winlogon.exe, etc.)**
 - **É comum que aplicações de rede precisem de conexão com a própria máquina - conexões com o endereço IP 127.0.0.1 ou com “localhost”**
 - **Configure registro (log) das atividades**
 - **Na dúvida, bloqueie e consulte seu departamento de suporte técnico**



1. Personal Firewall (5)

- Ferramentas

- Zone Labs ZoneAlarm (usuário iniciante, gratuito para uso pessoal e não comercial)

<http://www.zonelabs.com/store/content/company/products/znalml/FreeDownload.jsp>

- Windows XP Service Pack 2 - Noções básicas sobre o Firewall do Windows

http://www.microsoft.com/brasil/windowsxp/using/security/internet/sp2_wfintro.mspx

- Outros Personal Firewalls (evite os das seções “Not Reviewed”, “Gone or Fading Away” e “Not Recommended”)

<http://www.firewallguide.com/software.htm>

- CAIS - Uma visão geral dos firewalls pessoais

<http://www.rnp.br/newsgen/0201/firewall-pessoal.html>



2. Anti-Vírus

- Companheiro inseparável: Personal Firewall
- Software que tenta identificar, demover e eliminar vírus de computador e outros softwares maliciosos
- Busca por padrões específicos que confirmam com um perfil – assinatura - de algo que reconhecidamente causa danos



2. Anti-Vírus (2)

- De pouca utilidade se
 - seu banco de dados de definições não for atualizado pelo menos diariamente
 - o host não for varrido por completo ao menos uma vez por semana
- Verifique os arquivos com seu anti-vírus sob demanda, depois de receber um arquivo ou antes de anexá-lo a uma mensagem
- Verifique se seu anti-vírus pode ser configurado para arquivo que entra em seu computador – ótimo aliado da varredura semanal



2. Anti-Vírus (3)

- **Algumas Ferramentas gratuitas, disponíveis para uso pessoal e não-comercial**

- **AVG Anti-Virus Free Edition**

<http://free.grisoft.com>

- **BitDefender 8 Free Edition**

<http://www.bitdefender.com/site/Main/view/Download-Free-Products.html>

- **Anti-Virus Guide**

<http://www.firewallguide.com/anti-virus.htm>



3. Patches de Segurança

- Manter seu sistema atualizado é uma das melhores maneiras de ficar livre de worms e outros softwares maliciosos
- Cuidado com as falsas correções – hoax (boato) ou instalação de malware
- O tempo entre a divulgação de uma vulnerabilidade, o surgimento de um “exploit” e sua exploração por um worm é cada vez menor:
 - Zotob: 5 dias (MS05-039 - 14/08/2005)
 - Sasser: 17 dias (MS04-011 - 13/04/2004)
 - Blaster: 26 dias (MS03-026 - 16/07/2003)
 - Slammer: 185 dias (MS02-039 - 24/07/2002)
 - Nimda: 336 dias (MS00-078 – 17/10/2000)



3. Patches de Segurança (2)

- Mantenha todos os seus softwares atualizados, não apenas o Sistema Operacional (Windows)
- Patch Tuesday – toda primeira terça-feira do mês é dia de patch Microsoft
- Onde buscar atualizações para Windows:
 - Microsoft Security Bulletin Advance Notification
<http://www.microsoft.com/technet/security/bulletin/advance.msp>
 - Windows Update
<http://update.microsoft.com>
 - Microsoft Online - Office Update
<http://office.microsoft.com/en-us/officeupdate>
 - Windows XP Service Pack 2
http://www.microsoft.com/brasil/windowsxp/using/security/internet/sp2_wfintro.msp



4. Anti-*

- **Anti-Vírus** não é mais suficiente, diversas outras ameaças surgiram nos últimos anos
- **Outros “Anti”** que se tornaram essenciais:
 - **Anti-Spam**
 - **Anti-Spyware e Anti-Adware**
 - **Anti-Phishing**
 - **Anti-Pharming**
- **São disponíveis isoladamente, mas podem ser integrados em um único pacote**



4.1. Anti-Spam

- **Filtra mensagens não solicitadas, não necessariamente de cunho comercial. Vetor de propagação de golpes de phishing, softwares maliciosos (keyloggers), etc.**
- **Pode ser implementado de diversas maneiras**
 - **Servidor e/ou Cliente**
 - **Marca mensagens consideradas Spam de alguma forma**



4.1. Anti-Spam (2)

- Normalmente implementam filtros bayesianos
 - Primeiro você “treina” o sistema com diversas mensagens consideradas lixo
 - Depois você treina o sistema com diversas mensagens que você considera desejáveis
 - Novas mensagens passam a ser classificadas automaticamente
 - Gradualmente você corrige os erros de julgamento do software
- Ferramentas disponíveis
 - SpamLinks - Client Side Spam Filters
<http://spamlinks.net/filter-client.htm>



4.2. Anti-Spyware e Adware

- **Anti-Vírus não é mais suficiente para eliminar softwares maliciosos. Uma nova família de softwares: Spyware e Adware**
- **Sintomas mais comuns**
 - **Surgimento de novas barras de ferramenta e página inicial (home page) no browser**
 - **Pop-ups insistentes**
 - **Softwares instalados sem o seu conhecimento (EULA obscura)**
- **Propaganda agressiva com componentes de data mining, cavalos de tróia (trojans), malware, sequestradores de browser e componentes de rastreamento**



4.2. Anti-Spyware e Adware (2)

- Ferramentas

- Ad-Aware Personal (uso pessoal e não comercial)

<http://www.lavasoftusa.com/software/adaware/>

- Microsoft Windows AntiSpyware (Beta)

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>



4.3. Anti-Phishing

- Usam de subterfúgios técnicos e engenharia social para roubar a identidade dados pessoais e financeiros
- Mensagens de e-mail forjadas que levam usuários a sites falsos projetados para fazer o usuário divulgar dados financeiros (cartão de crédito, userid, senhas, CPF, RG, etc)
- Uso de marcas conhecidas para dar credibilidade
- Instalação de malware com intuito criminoso (crimeware)
- Assunto para uma apresentação inteira



4.3. Anti-Phishing (2)

- São tantas os subterfúgios técnicos que é cada vez mais difícil orientar o usuário a identificar este tipo de golpe
- Barras de ferramenta Anti-Phishing para browser
 - Avisam quando aquele URL já foi notificado como hospedeiro de Phishing
 - Quando ainda não foi notificado – permite que o usuário desconfie de um site de banco hospedado em um outro país



4.3. Anti-Phishing (3)

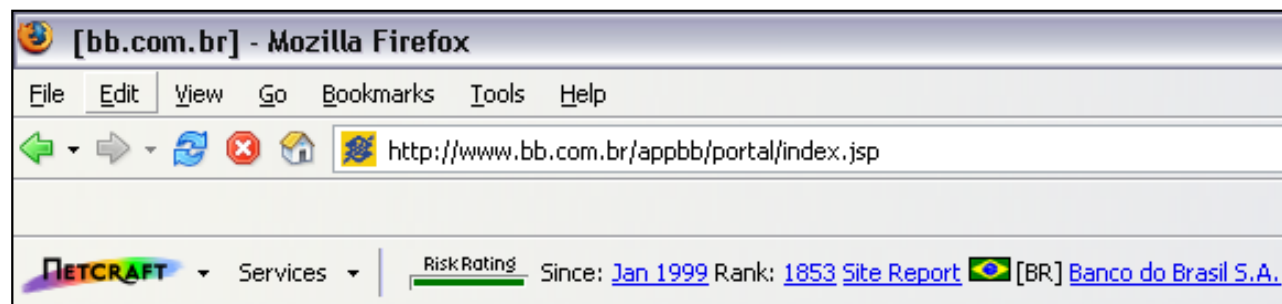
- Ferramentas

- Microsoft® Phishing Filter Add-in for MSN® Search Toolbar (incorporada ao IE7)

<http://addins.msn.com/phishingfilter/>

- Netcraft Anti-Phishing Toolbar

<http://toolbar.netcraft.com/>



4.4. Anti-Pharming

- Mais um nome que começa com “Ph”
- Exploração de alguma vulnerabilidade no DNS (Domain Name System) que permite que um cracker tome o domínio de um site e direcione o tráfego daquele website para outro
- Nome novo para ataques antigos
 - Sequestro de DNS (DNS Hijacking)
 - Envenenamento de DNS (DNS Poisoning)
- Difícil de ser detectado por usuários comuns
 - O domínio exibe o URL esperado
 - Se o site é seguro (HTTPS) apenas o certificado pode dar uma pista



4.4. Anti-Pharming (2)

- Ferramentas para uso não-comercial
 - **NGSEC AntiPharming** – configure-o com três servidores DNS de sua instituição
<http://www.ngsec.com/ngproducts/antipharming/download.php?lang=en>
 - **AntiPharming es distribuido en el CATA (RED.ES)**
<http://alerta-antivirus.red.es/portada/>



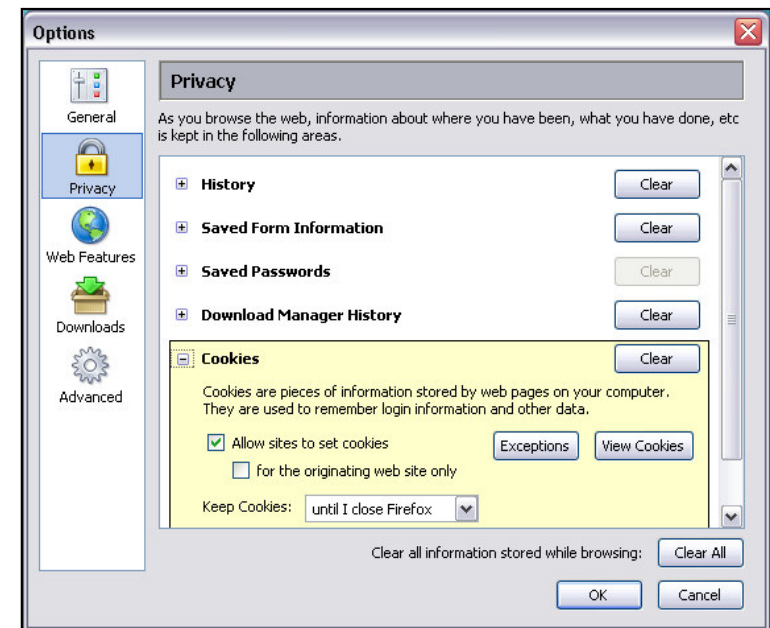
5. Configuração Segura do Browser

- O browser é uma das principais portas de entrada para softwares maliciosos
- Mantenha-o sempre em sua última versão
- Procure pelas configurações de segurança de seu browser



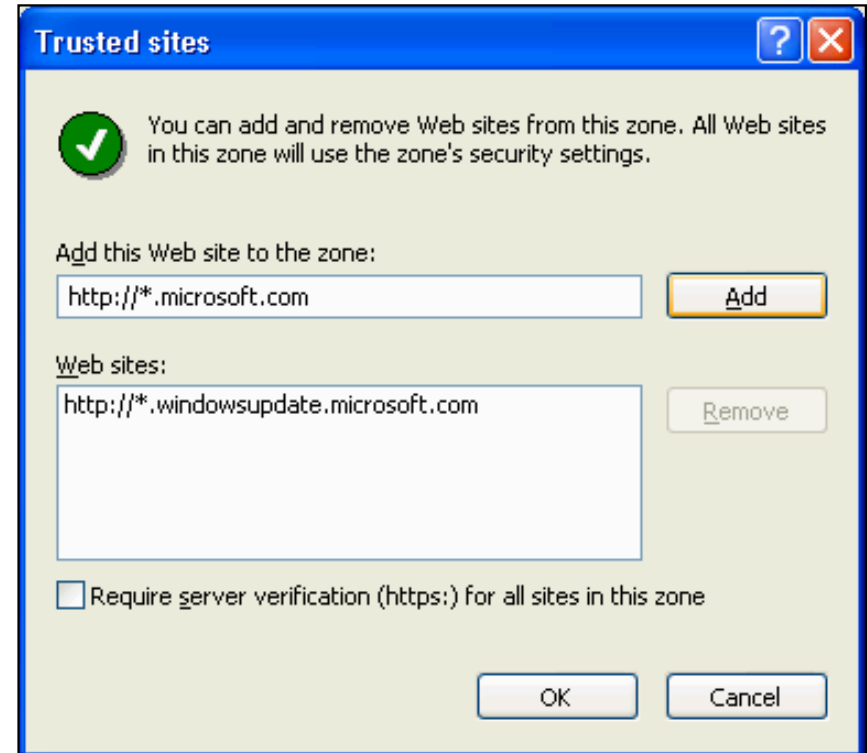
5. Configuração Segura do Browser (2)

- **Mozilla Firefox**
 - **Menu Tools > Options > Privacy**
 - **Desmarcar “Saved Form Information”**
 - **Desmarcar “Save Passwords”**
 - **Em “Cookies” selecionar a opção “Keep Cookies: until I close Firefox”**
 - **Menu Tools > Web Features**
 - **Marcar “Block Popup Windows”**
 - **Desmarcar “Allow sites to install software”**
 - **Desmarcar “Enable Java”**
(pode afetar certas aplicações, permita seletivamente)



5. Configuração Segura do Browser (3)

- **Internet Explorer 6**
 - Nível de segurança como “High/Alto”
 - Menu Ferramentas > Opções da Internet > Aba “Segurança” > Ícone Internet
 - Adicione os websites que considera seguros a “Sites Confiáveis”
 - Bloquear janelas pop-up



- **Mais informações:**

Improve the safety of your browsing
and e-mail activities

http://www.microsoft.com/athome/security/online/browsing_safety.mspx



5. Configuração Segura do Browser (4)

- **MSN Search Toolbar – Bloqueador de janelas pop-up e filtro de Phishing (já mencionado) para versões anteriores a Windows XP SP2**

<http://toolbar.msn.com/>



7. Em último caso...

Você ignorou todos os Alertas do CAIS.

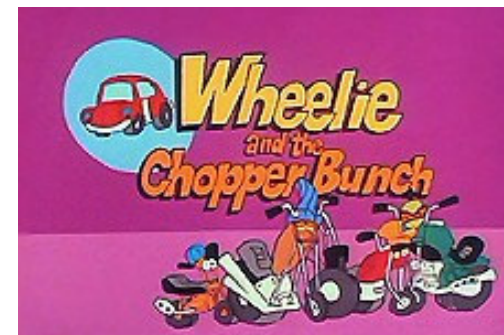
Nosso velho amigo Confuso tem algo a
lhe dizer:



Kit Básico de Sobrevivência na Internet

“Mas eu te disse, eu te disse!”

-- Scrambles, Wheelie and The Chopper Bunch (NBC-1974)



7.1. Removedores de Malware

- Ferramentas desenvolvidas para remover softwares maliciosos automaticamente
- Eliminam a necessidade de remoção manual, impraticável em ambientes com uma grande quantidade de usuários
- Devem ser vistos como medida paliativa, ou seja, não eliminam a necessidade de Anti-Vírus e outras tecnologias de proteção



7.1. Removedores de Malware (2)

- Microsoft Malicious Software Removal Tool – atualizada com frequência e disponível no Windows Update

<http://www.microsoft.com/security/malwareremove>

- McAfee AVERT Stinger

<http://vil.nai.com/vil/stinger/>

- Symantec Security Response – Removal Tools

<http://securityresponse.symantec.com/avcenter/tools.list.html>

- F-Secure - Free Virus Removal Tools

<http://www.f-secure.com/download-purchase/tools.shtml>



7.2. Removedores de Rootkit

- **Rootkits**
 - **Origem do nome - surgiram em UNIX e eram usados para elevar os privilégios de um usuário local para root**
 - **Em Windows trabalham de uma maneira diferente e normalmente são usados para esconder malware de um software anti-vírus, por exemplo**
- **Diversos tipos: Persistent, Memory-based, User-mode e Kernel-mode**



7.2. Removedores de Rootkit (2)

- Ferramentas para Windows (voltadas para usuários avançados)

- Sysinternals RootkitRevealer

<http://www.sysinternals.com/Utilities/RootkitRevealer.html>

- F-Secure BlackLight™ (Beta Release)

<http://www.f-secure.com/blacklight/>



7.3. Anti-Vírus Online

- Symantec Security Check (requer ActiveX)

<http://security.symantec.com>

- F-Secure Online Virus Scanner

<http://support.f-secure.com/enu/home/ols.shtml>

- CATA – Útiles Gratuitos

<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=1>

- Virustotal – varre o arquivo submetido com vários anti-vírus diferentes

<http://www.virustotal.com>



Referências

- **CERT/CC - Before You Connect a New Computer to the Internet**

http://www.cert.org/tech_tips/before_you_plug_in.html

- **CERT/CC - Home Computer Security**

<http://www.cert.org/homeusers/HomeComputerSecurity/>

- **NCSA - Stay Safe Online**

<http://www.staysafeonline.info/>



Kit Básico de Sobrevivência na Internet



Participe!

- Divulgue conhecimento
- Algumas das atividades traduzidas
- Envie e-mails de Phishing Scams para phishing@cais.rnp.br
- Envie e-mails contendo malwares anexados ou links para malwares para artefatos@cais.rnp.br
- Receba gratuitamente os alertas de segurança divulgados pelo CAIS:
 - CAIS Alerta
<http://www.rnp.br/cais/alertas/>
 - CAIS Alerta por RSS
<http://www.rnp.br/cais/alertas/rss.xml>



DISI

Dia Internacional de
Segurança em Informática

Kit Básico de Sobrevivência na Internet



Centro de Atendimento a Incidentes
de Segurança – CAIS/RNP

Ronaldo Castro de Vasconcellos

Analista de Segurança, CAIS/RNP

ronaldo arroba cais.rnp.br

Dia Internacional
de Segurança em Informática

30 de Novembro de 2005



Glossário

- **ActiveX** – controles desenvolvidos pela Microsoft que customizam e acrescentam interatividade a websites
- **Adware** – propaganda integrada ao software
- **DNS** – Domain Name System, sistema que traduz endereços IP em nomes (www.example.com)
- **EULA** – End User License Agreement, licenças apresentadas ao usuário no momento da instalação de um software
- **Firewall** – dispositivo de software e/ou hardware que previnem algumas comunicações proibidas pela política de segurança, controlando o tráfego de rede entre duas zonas de confiança (Internet e rede interna, por exemplo)
- **Hoax** – Boato. Tentativa de enganar um usuário de forma que ele acredite que algo falso é real. Em segurança induzem o usuário a remover arquivos inadvertidamente, repassar informações incorretas
- **HTTP** - Hyper Text Transfer Protocol, protocolo de comunicação que permite a navegação Web
- **HTTPS** – HTTP over SSL, HTTP Seguro



Glossário (2)

- **IP** – Internet Protocol
- **Malware** – Software Malicioso, projetado para tomar controle ou danificar o Sistema Operacional. Vírus e Cavalos de Tróia estão incluídos nessa categoria de softwares.
- **Spyware** – categoria ampla de softwares maliciosos com propósitos específicos, instalados por meio de vulnerabilidades, softwares de terceiros ou mesmo enganando o usuário. Alguns exemplos: CoolWebSearch, 180 Solutions, HuntBar, etc
- **UNIX** – Sistema Operacional multi-tarefa desenvolvido pela AT&T em 1969
- **URL** – Uniform Resource Locator, o endereço de um recurso na Internet
- **Vírus** – programa que se replica ao inserir cópias de si em outros arquivos executáveis ou documentos
- **Worm** – semelhantes aos vírus pela capacidade de se auto-replicar, mas diferente porque se propaga por si mesmo

