Segurança, Privacidade e Colaboração - Reset the Net

O Fight for the Fortune deu origem ao Reset the Net e é um grupo sem fins lucrativos que é dedicada a expandir o poder transformador da Internet para o bem.

Nosso objetivo: "Construir um movimento popular para garantir que todos possam acessar muitos recursos da Internet de forma simples, livre de interferência ou de censura e com plena privacidade".

Nossa visão: "Um mundo onde todos possam desfrutar da liberdade básica para expressar, criar e se conectar online".

Outros grupos por trás do Reset the Net incluem Demand Progress, Reddit, the Libertarian Party, and the Free Software Foundation.

De acordo com eles, os governos estão tornando a Internet uma prisão virtual. Mas, enquanto a NSA e os seus aliados, como a UK's Government Communications Headquarters (GCHQ) acham que podem invadir qualquer pessoa "... eles esquecem que não podem invadir todos.

Gente como a NSA depende de coleta de dados inseguros. Eles dependem de nossos erros - erros que podemos e devemos corrigir".

No primeiro aniversário da primeira revelação do Snowder, que aconteceu dia 5 de junho de 2013, precisamos tomar os cuidados que estiverem ao nosso alcance e nos empenhar por conhecer mais sobre o assunto e fazer mais ainda. Vamos ficar atentos ao site, que está coordenando o movimento:

https://www.resetthenet.org/ e este https://www.fightforthefuture.org/

Algumas ponderações

Embora a NSA tenha divulgado que quebrou a segurança do SSL, precisamos lembrar que eles dizem mais do que fazem para a tal da guerra psicológica e tentar ganhar a guerra antes mesmo de ela começar. Precisamos lembrar também que a falha do SSL já foi corrigida e novas versões mais fortes já foram liberadas (não esqueça de atualizar seu servidor).

Por mais poder que tenha a NSA e seus aliados, por mais dinheiro e recursos tecnológicos a seu dispor é muito importante ressaltar que apenas um único ser humano sem a ajuda de ninguém conseguiu minar o poder do grande "império". Isso nos mostra que nem sempre ajuda ajuda. Isso mostra que quem trabalha com segurança deve ter em mente, não existe segurança perfeita.

É de conhecimento dos que leram o livro publicado que relata a saga do Snowden e seus parceiros, que ele ao final contou com a colaboração imprescindível de alguns jornalistas selecionados criteriosamente e que também o Assenge colaborou com a fuga do Snowden de Hong Kong para Moscou. Somos gratos e temos um grande débito para com todos.

Vem bem a calhar lembrar do filme “Vida de Inseto”, onde grandes gafanhotos, bem mais fortes e sem caráter, mantém formigas, menores, mesmo em um muito maior número, mas desorganizadas e sem consciência do poder que detêm. Finalmente contando com o sacrifício de uma frágil e jovem formiga, após observarem a mesma afirmar sob as pancadas do gafanhoto chefe, que as formigas não precisam obedecer e ser subservientes, ao contrário as formigas são nobres e não inúteis como quer dizer o gafanhoto e não precisam ficar sob o jugo dos mesmos. Num final emocionante as formigas se unem e expulsam os gafanhotos.

Qualquer semelhança com a nossa atual realidade, o caso Snowden e o que está por vir não será mera coincidência. Precisamos ter consciência de que podem até nos espionar, nos controlar, nos prejudicar, mas tudo isso somente até o momento em que percebermos o poder que temos e decidirmos nos unir e nos rebelar. O exemplo Snowden para mim teve especiamente três pontos fortes: a inteligência dele foi algo invejável, o controle emocional do camarada é também algo que quero um dia para mim e a terceira característica, que é a mais importante das três, pois sem ela nada disso teria acontecido, é sua nobreza e generosidade que fez com que ele sacrificasse quase tudo que tinha, família, namorada, um salário anual de 200 mil dólares e amigos em nome de uma causa que julgou superior a tudo que deixou para traz sem arrependimento, a causa coletiva dos que estão sendo espionados e de certa forma oprimidos e prejudicados. Ele tem o sentimento que motiva os herois.

Usuários do Linux, FreeBSD e similares

Se você usa um sistema destes já está rasoavelmente seguro, mesmo em uma instalação padrão, sem nenhuma customização ou firewall.

Vários são os aspectos que tornam estes sistemas mais seguros. Citando alguns de forma simplificada:

- Eles foram projetados para funcionar em grandes redes, mas também funcionam muito bem em ambientes desktop e isso exige um maior cuidado com a segurança;

- Eles não pegam virus, pelo menos da forma que conhecemos no windows. Pinte o seguinte quadro em sua mente:

- Você está no Linux e recebe um e-mail com um arquivo malicioso em anexo. Para reforçar, o arquivo em anexo é um script com código executável para Linux, malicioso e disfarçado para destruir todo o diretório do usuário quando executado.

- Sem saber da ameaça você faz o download e tenta curiosamente executar, já que o nome do arquivo é “fotodasuaesposasaindomotel.jpg” (curioso é que com nomes assim até solteiros e mulheres baixam e tentam executar e os cracker sabem disso). Mas, diferente do Windows, nenhum arquivo baixado pode ser executado apenas com um duplo clique, como naquele sistema. Então o que você precisa fazer para que o arquivo, disfarçado mas maléfico realmente possa ser executado e apague todos os arquivos e diretórios do seu home? Cuidado, o link no e-mail pode mostrar “fotosdasuaesposanomotel.jpg” e por baixo chamar realmente o arquivo “removadirusuario.sh” ou outro qualquer ja que um executável no linux pode ter qualquer nome e qualquer extensão e até nenhuma.

- Não existem arquivos executáveis no Linux. No Windows quando criamos um arquivo e queremos que ele seja executável ele basta ter a extensão EXE, BAT por exemplo.

Se um arquivo exe receber um duplo clique no Windows ele será executado geralmente. No Linux qualquer arquivo criado ele é inativo por padrão. Por segurança o arquivo não tem **permissão** de execuão. No Linux, executável é uma permissão que o usuário dá ou retira do arquivo e não um tipo de arquivo. Ele **está** executável. Ele não **é** executável.

- Um outro aspecto é que somente se você for um usuário administrador ou souber seu login e senha dele, somente assim você poderá executar algum arquivo com abrangência global no sistema, caso contrário somente poderá afetar a área do usuário atual. Finalmente ainda precisará saber o que fazer para transformá-lo em executável e somente então ele terá permissão de executar. Nem vou dizer como se faz isso, para o caso de você ser usuário Windows e ter se interessado pelo Linux, espero que tenha disposição para estudar e passe a ser um novo usuário de um grande sistema operacional.

Dizem alguns que não existe virus para Linux, mas péssimos administradores (sysadmin). É admirável este cuidado, um verdadeiro esmero com a segurança, em especial se lembrarmos que são desenvolvidos por voluntários generosos e em seu tempo livre e ainda por cima entregue gratuitamente a qualquer um que se interesse.

- Ainda tem um fator que favorece estes sistemas, é que eles atualmente são utilizados por uma fatia bem menor que a do Windows e por isso os crackers acham mais proveitos ter como alvo o Windows.

Usuário do Windows

Bem, seu sistema é realmente inseguro e cheio de buracos, mas ainda assim, se quizer ter algum trabalho e gostar de aprender poderemos reduzir sua insegurança.

O cuidado mais importante que conheço para reforçar a segurança no Windows não é a instalação de anti-virus, antispy, firewall e cia, mas a criação de um usuário comum, sem privilégios e usar o computador com este usuário. Para ter uma idéia este usuário não tem permissão de instalar programas (alguns softwares já estão conseguindo), instalar dispositivos, desinstalar, nem mesmo de gravar um arquivo no raiz do C. Se você, como usuário comum não consegue é de se esperar que o virus também não.

Bem, se o computador é seu e quer ter controle total em alguns momentos, basta que ao tentar instalar ou desinstalar um programa, que forneça a senha do administrador. Se for entregar para um usuário leigo é melhor que não passe essa senha para ele, mas claro que fica ao seu critério.

Permita que o Windows faça suas atualizações para corrigir bugs e falhas de segurança publicadas.

Também instale um bom anti-virus e lembre de deixar que ele atualize automaticamente.

Se quizer reforçar a segurança instale um antispy e um firewall de terceiros, pois o do windows é muito ruim, mas não caia na tentação de desabilitar o do Windows, mesmo ruim é importante. É bom lembrar que isso roubará muito processamento do seu computador e lembro de uma época que usava Windows e instalei o Norton Antivirus. Desinstalei e preferi enfrentar os virus, pois pelo menos assim ainda conseguia

razoavelmente usar o computador e com o Norton era inviável, de tão pesado.

Usuários do Windows 8 e 8.1 Tomem Cuidado

Caros amigos, quando fui instalar meu último computador, com Windows 8.1, na hora de criar o usuário ele me pediu que eu faizesse login no site da Microsoft (antigo MSN acho) e que use este usuário para instalar o computador. Achei isso muito complicado e altamente invasivo. Mesmo que eu confiasse na Microsoft não seria interessante, pois sem internet não teria acesso ao computador. Na primeira vez não insinti e instalei como usuário da Microsoft, mas fui verificar e criei outro usuário mas desta vez olhei com calma e criei um usuário local e do tipo administrador. Fiz logout e login com este novo usuário. Então removi o usuário criado para locar com a conta da Microsoft. Vale lembrar que a Microsoft foi a primeira empresa a se aliar a NSA.

Se quizer detalhes de como criar o usuário somente com acesso local basta fazer uma busca e se quizer privacidade na busca procure no:

https://duckduckgo.com/

Aqui um:

http://www.meuwindows8.com/criar-contas-de-usuario-no-windows-8/

Vale lembrar “Conhecimento é poder”, portanto informe-se para cuidar melhor da sua segurança e privacidade. Visite o site do Reset the Net para novidades.

Ferramentas recomendadas:

Use Adium ou Pidgin como chat no lugar do Gtalk, Facebook, Yahoo, MSN, XMPP/Duck Duck Go e outros.

Textsecure e Redphone para Android e iPhone (esperamos), para privativos SMS e chamadas de voz.

HTTPS Everywhere para habilitar HTTPS nos navegadores - https://www.eff.org/https-everywhere

GPGtools e Enigmail (para usuários avançados)

Tor - https://www.torproject.org/index.html.en

Extensão para o Firefox - https://www.eff.org/https-everywhere/faq

Ative, se possível, o HTTPS no servidor do seu site/blog.

Navegadores

Enquanto Chrome, Firefox, Opera e Safari suportam HSTS, o Internet Explorer não suporta, ou seja, não existe site seguro se você usar o Microsoft IE. Se isto é uma armadilha proposital ou não, não importa agora, mas se você pretende maior segurança é melhor usar um dos outros navegadores.

Firewall Simples no Linux Debian, Ubuntu e derivados e ainda outras

Quem usa Linux e quer configurar o firewall mais conhecido nesse mundo, sabe que é trabalhoso configurar o IPTables. Mas o pessoal do Ubuntu, mais uma vez resolveu facilitar a vida dos usuários e administradores e criou uma ferramenta que de fato é uma interface para o IPTables, mas muito mais simples de configurar. Com as três linhas abaixo você já tem em seu computador pessoal mais uma boa camada de segurança.

```
sudo apt-get install ufw
sudo ufw enable
sudo ufw status verbose
```

Este comando acima mostra:
Estado: ativo
Logando: on (low)
Default: deny (incoming), allow (ougoing), disabled (routed)
O que nos diz que seu computador pode acessar qualquer site, mas ninguém pode acessar seu computador vindo da internet.

Também podemos bloquear e liberar portas específicas de forma simples:

```
sudo ufw allow ssh
sudo ufw allow http
```

Ou

```
sudo ufw allow 22/tcp
sudo ufw allow 22/udp
sudo ufw allow 80
```

```
sudo ufw deny from 192.168.0.1 to any port 22
sudo ufw deny from 192.168.0.7 to any port 22
sudo ufw allow from 192.168.0.0/24 to any port 22 proto tcp
```

Mais informações:
https://help.ubuntu.com/community/UFW
https://help.ubuntu.com/10.04/serverguide/C/firewall.html
ufw manual: http://manpages.ubuntu.com/manpages/lucid/en/man8/ufw.8.html
project wiki: https://wiki.ubuntu.com/UncomplicatedFirewall
http://savvyadmin.com/ubuntus-ufw/

Para quem usa o ambiente gráfico existe o software gráfico que usa o ufw, no caso o GuFW. Instale com:

```
sudo apt-get install gufw
```