-

Blog

gus

Campanha - Use Tor, Use Signal!

May 25 2017

A coluna do Estadão publicou nessa semana que o presidente Michel Temer recebeu um celular criptografado desenvolvido pela Agência Brasileira de Inteligência, a Abin. O aparelho utiliza um sistema operacional Android customizado, desenvolvido pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc), área de pesquisa da própria agência. Desde a semana passada, o presidente virou alvo de investigação pela Procuradoria Geral da República, após a delação premiada do empresário Joesley Batista. Enquanto alguns procuram a criptografia para obstruir a justiça de revelar seus esquemas, há ativistas, jornalistas e cidadãos comuns que têm sido alvos frequentes de violação da privacidade. Na Grampolândia, a falta de privacidade afeta todos!

Durante crises institucionais é comum os governos "desligarem o botão" da Internet, bloquearam aplicativos e redes sociais como forma de impedir o acesso à informação pela população. Já vimos isso recentemente acontecer no Egito e na Turquia, assim como os sucessivos bloqueios ao WhatsApp no Brasil. E uma vez censurada, fica difícil conseguir encontrar bons tutoriais e manuais de como escapar do bloqueio. Retomando a máxima cypherpunk: "Criptografia para os fracos, transparência para os poderosos", escrevo aqui **o mínimo** que você deve fazer para se proteger hoje, agora, já!, antes do próximo protesto ou do governo desligar a Internet.

Use Tor!

O Tor é um programa feito para você navegar anonimamente e burlar a censura na Internet. O Tor garante o seu anonimato através do roteamento em camadas do seu tráfego: tudo o que você acessar passará por pelo menos três nós da rede de servidores Tor, os quais estão espalhados pelo mundo todo. A sua localização verdadeira é preservada e parecerá que você está em outro país. Todo o tráfego dentro da rede Tor é criptografado e ninguém conseguirá bisbilhotar. O Tor é software livre, desenvolvido há mais de 10 anos e auditado por uma comunidade ativa.

Baixe o Tor hoje! Para desktops você pode baixar o navegador Tor para todos os sistemas operacionais: Windows, Mac e Linux. Lembre-se: sempre baixe o Tor do site principal do projeto: https://torproject.org. Você pode acessar o manual do navegador Tor em português.

Para celulares, você possui duas opções no Android:

Orbot - que funciona também como uma VPN roteando todas as conexões de aplicativos pela rede Tor. Isso é algo bastante útil para acessar aplicativos bloqueados em casos de censura na Internet.

Orfox - um navegador que funciona com o Tor (você precisa do Orbot instalado para fazer a conexão com a rede).

Você pode baixá-los na Play Store ou usando a app store para software livres F-Droid. No boletim Antivigilância #15 há um passo a passo de como usar os dois aplicativos.

Por causa da forma como a Apple funciona para o desenvolvimento de aplicativos para iOS, é difícil construir uma solução completa para iPhones. Mas existe o Onion Browser que está tentando fornecer algum suporte para usuários de iPhones, que você também pode encontrar na Apple Store.

É importante você saber que:

- Alguém observando o seu tráfego de internet saberá que você está usando o Tor, mas **o que** você está fazendo ninguém saberá. É possível ofuscar o tráfego do Tor, mas isso é tema para um outro artigo.
- A conexão do nó de saída da rede Tor com o site que você quer acessar nem sempre estará criptografada, pois isso dependerá **do site que você está acessando**. O navegador Tor possui a extensão https-everywhere por padrão. Você pode baixá-la para o seu outro navegador.
- Tome cuidado ao acessar sites de redes sociais (Facebook, Twitter, Instagram), contas de bancos e serviços de pagamento como Paypal e o Gmail via Tor, eles tendem a bloquear a sua conta devido a mudança da sua localização. O Facebook possui um serviço onion: facebookcorewwwi.onion . Se você for usar as redes sociais pelo Tor, certifique-se primeiro que você conseguirá responder as perguntas de segurança de recuperação da sua conta, senão você ficará bloqueado da sua própria conta.
- A sua conexão não tornará menos segura usando Tor, pelo contrário, ao usar Tor você não estará expondo os seus dados privados como, por exemplo, a sua localização real.
- Você pode aumentar o nível de segurança do navegador Tor usando o menu "Security Settings" (Configurações de segurança), impedindo inclusive de

sites maliciosos enviarem malware para o seu computador.
- Tor não é "deep web"! Deep web não existe. O termo surgiu como um pseudo-conceito técnico para a) justificar a narrativa do medo contra a liberdade: empregue pelas agências de segurança dos governos para dizer que a "internet não é um lugar seguro para as criancinhas e precisamos monitorar e vigiar todas as pessoas" e b) vender a ideia e, principalmente, artigos click-baits de que há lugares ~sombrios~ na Internet.
- Não existe programa 100% seguro. Programas são escritos por seres humanos.
- Utilize sempre o navegador Tor por padrão. Evite surpresas no futuro! Além do roteamento cebola, o Tor possui outras alterações no navegador para impedir que o seu tráfego seja rastreado.
- Cuidado com os boatos e o "ouvi dizer que o Tor não é seguro". Peça sempre mais informações. Evite o F.U.D!

Use Signal!

O Signal é um software livre que utiliza criptografia ponto a ponto, ou seja, apenas você e seus amigos que usam Signal conseguirão abrir aquelas mensagens. Se alguém interceptá-las no meio do caminho, não será possível ler. O Signal utiliza o protocolo criptográfico de mesmo nome, Signal, o qual é uma referência na comunidade de segurança. O programa está disponível para Android e iOS, também possui versão desktop para o navegador Chrome e também para o projeto de código aberto Chromium. O programa é desenvolvido pela Whisper Systems e é endossado por especialistas da área de segurança da informação, ativistas e jornalistas investigativos, dentre eles Edward Snowden, Laura Poitras, Bruce Schneier e Matt Green.

Ao instalar e usar o Signal, além das mensagens criptografadas você terá automaticamente duas outras propriedades criptográficas interessantes: o sigilo encaminhado (forward secrecy) e o sigilo futuro (future secrecy), isto é, mesmo que *hipoteticamente* uma mensagem sua seja interceptada e decifrada, ainda assim as suas futuras mensagens e as enviadas no passado não serão ou foram comprometidas! (Ouvi você dizendo "UAU!"?!) Além disso, o Signal permite chamadas de vídeo, de voz, batepapos em grupo e troca de arquivos: tudo criptografado!

No ano passado houve tentativa de censura ao Signal em outros países. A reação dos desenvolvedores foi implementar a técnica de *domain fronting* para burlar o bloqueio. A técnica consiste em fingir que você está acessando um grande site não bloqueado, por exemplo, a CloudFlare, quando na verdade você está apenas usando-o para se conectar ao Signal. (Ouvi você dizendo "UAU!" de novo?!) O censor até pode descobrir o truque, mas o custo político de censurar um serviço popular será altíssimo: cairá a máscara da democradura. Um dos aspectos positivos dessa técnica é que você não precisará fazer nada para desbloquear o serviço do aplicativo, ele voltará a funcionar normalmente, sem precisar de configurações extras.

Instale o Signal a partir da loja de aplicativos no seu smartphone. Disponível para iOS e Android!

É importante você:

- Após instalar o Signal habilitar em cada contato para que as mensagens desapareçam após um período. Você pode escolher alguns segundos até uma semana. Pouco tempo é ruim, pois as pessoas não estão online o tempo todo. Mas em períodos mais críticos como numa manifestação ou na rua, você pode redefinir o tempo para algumas horas ou minutos. Você pode sempre redefinir o período de tempo, mas isso não se aplicará as mensagens já enviadas.
- Não acumule histórico de conversas. Apague diariamente suas conversas.
- O celular não é um dispositivo bom para guardar dados. Afinal, quem nunca teve um celular roubado?
- Criptografe o seu celular! Os novos iPhones já são criptografados por padrão. No Android você precisa fazer isso. Não use métodos de desbloqueio como impressão digital, reconhecimento facial ou escaneamento de íris. Se você for detido, podem forçar você a desbloquear. Use senhas fortes com pelo menos 12 dígitos.
- Convidar seus amigos para migrarem para o Signal.
- Quando encontrar seus amigos, faça uma verificação do código signal. Leva apenas alguns segundos e dará a garantia que você está falando com quem você pensa!
- Lembrar que mesmo usando Signal, a segurança do sistema operacional do seu aparelho (e o hardware em si) limita a sua segurança, isto é, se o seu celular estiver desatualizado, um atacante poderá contornar a criptografia e acessar tudo!

Isso é o mínimo para você fazer **AGORA**! Você não deve esperar a solução perfeita de segurança para agir, até porque, a situação está ficando mais crítica e mesmo assim você não deixou de fazer coisas que podem comprometer a sua segurança.

Se você se interessou e quer ler mais, além dos posts anteriores desse blog, um guia completo está aqui: Guia de Autodefesa Digital.

Faça a sua parte na campanha e divulgue: **Use Tor! Use Signal!**

Escrito por gus May 25 2017 seguranca anonimato

sobre

Um blog sobre segurança e privacidade.

Publicações recentes

- Cebolizando SP - Atividades do Tor em maio em São Paulo!
- Meltdown & Spectre: Boletim de segurança do Riseup
- A Safra de Outono do Tor: a Próxima Geração dos Serviços Onion
- POPSEG - Bastardos Inglórios
- #freeBogatov - Liberdade para Dmitry Bogatov!

Tópicos

grampo, vulnerabilidade, mensageria, seguranca, politica, anonimato, gag order, threat model, censura, agenda, privacidade, canaria, criptografia, projetos, opsec, cryptorave

Links

- Grampolândia
- Baralho OpSec
- TRETA
- CryptoRave
- Tem Boi Na Linha
- Antivigilancia

sobre

Um blog sobre segurança e privacidade.

Publicações recentes

- Cebolizando SP - Atividades do Tor em maio em São Paulo!
- Meltdown & Spectre: Boletim de segurança do Riseup
- A Safra de Outono do Tor: a Próxima Geração dos Serviços Onion
- POPSEG - Bastardos Inglórios
- #freeBogatov - Liberdade para Dmitry Bogatov!

Tópicos

grampo, vulnerabilidade, mensageria, seguranca, politica, anonimato, gag order, threat model, censura, agenda, privacidade, canaria, criptografia, projetos, opsec, cryptorave

Links

- Grampolândia
- Baralho OpSec
- TRETA
- CryptoRave
- Tem Boi Na Linha
- Antivigilancia