"HACKTIVISMO"

por:
Tiago Reis Alves
Departamento de Engenharia Informática, FCTUC
talves@student.dei.uc.pt

Resumo:
Apresenta-se um pequeno estudo acerca do que é o *hacktivismo*. O conceito de *hacktivismo* é aqui distinguido dos outros tipos de lutas online. Descrevem-se as várias formas e técnicas usadas pelos *hacktivistas*, apresentando casos reais de ataques. No final, obteve-se uma clarificação acerca dos efeitos do *hacktivismo* nos dias de hoje e para o futuro.

Palavras chave: Hacktivismo, activismo, cyberterrorismo.

1. Introdução

A Internet veio trazer grandes novidades à nossa sociedade a partir do momento em que começou a ser largamente divulgada, assumindo um papel pelo menos tão importante como os outros meios de comunicação. Só que ao contrário dos outros, essa informação não é necessariamente manipulada pelos que têm mais poder económico e político, mas por vezes pelos que têm poder tecnológico. Sendo assim, é natural que as comunidades que não têm poder de expressão usem este meio de divulgar as suas ideias, que de outra forma dificilmente atingiriam o mesmo nível de atenção.

2. Activismo online, hacktivismo e Cyberterrorismo

"*Hacktivismo*" um conceito em si pouco definido, sendo muitas vezes confundido com outros tipos de luta ligados aos computadores e Internet. Um deles é o activismo, que engloba a utilização legítima da Internet para difundir informações (web sites dedicados ao tema), recolher informações acerca do que se passa realmente sem as barreiras de censura que por vezes são levantadas pelos governos, e local para fóruns de discussão e coordenação das acções. "*Hacktivismo*" consiste na convergência do activismo puro, com o uso de métodos de "hacking" normalmente declarados como ilegais e por vezes destrutivos, mas em que a ideia principal é a de transmitir uma mensagem ao maior número de pessoas. Subindo na escala em termos de radicalismo, temos o "*Cyberterrorismo*", em que o objectivo passa por causar estragos consideráveis, embora ainda os maiores ataques de *cyberterrorismo* já realizados nunca chegarem ao efeito de um ataque bombista, por exemplo. Muitas vezes torna-se difícil distinguir onde acaba o *hactivismo* e começa o *Cyberterrorismo*.

3. *Bloqueio ou manifestação virtual*

1. O que é?

Uma manifestação com bloqueio no mundo físico tem como objectivo ocupar uma organização de modo a não permitir o seu funcionamento normal, impedindo a entrada dos que a ele quiserem aceder. A versão virtual consiste em fazer com que os participantes invadam um site, gerando o maior tráfego possível, de modo a que o seu acesso esteja restrito ao utilizador normal.

2. Como?

Estes bloqueios explícitos a sites, na sua forma mais simples, podem ser conseguidos pelo o simples uso excessivo do site, mobilizando o maior número de pessoas possível para um ataque sincronizado. Apesar de ser um método bastante simples, existem relatos de ataques "bem- sucedidos" (ex: ataque de 21 de Dezembro de 1995 realizado pelo grupo Strano Network).

Para aumentar o efeito do ataque, ao longo do tempo foi sendo desenvolvido software que faz pedidos repetidos ao servidor vítima de modo a que os participantes apenas tenham que fazer o download do respectivo sofware.

3. É legal?

Apesar de serem ataques explícitos a sites, a sua legalidade não é fácil de determinar, por envolverem apenas acessos simples ao servidor. O mesmo já não se pode dizer dos que desenvolvem software e o distribuem com estes objectivos.

4. Quem usa este tipo de métodos?

Estes ataques são normalmente coordenados por grupos de grande influência neste meio, já que o seu sucesso depende em grande parte do número de pessoas que adere.

Electronic Disturbance Theater (EDT)

Este grupo foi desde sempre organizador das maiores manifestações *hacktivitas*, ou pelo menos as que mobilizaram mais pessoas por todo o mundo a se unirem a favor de uma causa. Foram criadores do software FloodNet (uma Applet em Java) que tentava aceder ao servidor vítima repetidamente. Além disso, permitia que as mensagens no log de erros do servidor fossem escolhidas pelos manifestantes (por exemplo "Human_rights not found on this server" ao tentar aceder à página não existente com o nome "human_rights"). FloodNet era a "arte conceptual da rede que dá poder às pessoas através da expressão activa/ artística", como definido por Stalbaum, o escritor deste programa. Tudo o que os manifestantes tinham que fazer era fazer o respectivo download de um dos sites da FloodNet

Uma dessas causas foi o Zapatismo. Os Zapatistas são um grupo cuja principal luta é pela defesa dos direitos da população de Chiapas no México. O "Digital Zapatismo" tem sido responsável pela criação de uma rede de

distribuição com mais de 100 nós independentes. Em 1998, este grupo recebeu inclusivamente a escolha da revista "Wired" para uma das 25 presenças mais importantes na Internet. Segundo Ricardo Dominguez (da EDT), este meio tem "possibilitado ao Exercito Zapatista de Libertação Nacional (EZLN) falar ao mundo sem passar por nenhum filtro de comunicação social dominante".

A 9 de Setembro de 1998, o grupo Electronic Disturbance Theater (EDT) organizou uma grande manifestação ou bloqueio a favor dos Zapatistas, primeiramente contra o site do presidente Zedillo do México e depois contra vários sites governamentais como o da Casa Branca (Presidente Clinton), do Pentagono, do "School of the Americas", da Bolsa de Frankfurt, e da Bolsa Mexicana. O EDT estimou que cerca de 10,000 pessoas participaram.

No princípio, só o site do Pentágono ripostou ao ataque, redireccionando os clientes para uma outra Applet (chamada "HostileApplet"), que uma vez instalada nos clientes, levava os computadores a fazer sucessivas tentativas de acesso a um documento inexistente, levando as máquinas à rotura até serem reiniciadas. Mais tarde o site do Presidente do México fazia os browsers dos manifestantes abrirem janelas sucessivas até crasharem. Os responsáveis pelo site da Bolsa de Frankfurt afirmaram que tinham conhecimento do ataque, mas que este não surtiu qualquer efeito, já que os seus servidores estão habituados a uma carga normal de 6 milhões cliques por dia.

Este grupo mantém-se bastante activo, colocando à disposição no seu site (http://www.thing.net/~rdom/ecd/ecd.html) várias causas que vão desde o conflito no Médio Oriente até política aplicada pela Starbuck. Assim, muito ao estilo de um self-service, o visitante só tem que escolher a luta da sua preferência, e de seguida o método: ligação web simples, Applets Java, ou até sripts em perl.

Electrohippies

Em Dezembro de 1999, este grupo de cinco pessoas organizou um ataque aos servidores do World Trade Organization. Segundo as suas estimativas, 452,000 manifestantes juntaram-se à causa, causando interrupções de 4 a 5 horas nas vitimas.

No dia 1 de Abril do ano seguinte, 78 servidores foram surpreendidos por uma partida ("April fool") diferente: um novo ataque com o título "Resistance is fertile" contra os alimentos modificados geneticamente.

Muitos outro grupos podiam ser referidos, como por exemplo, os "cDc" ou os "l0pht".

4. *"Hacking" de servidores*

1. O que é?

Esta continua a ser uma grande forma de expressão dos *hacktivistas*. Ao contrário das manifestações apresentadas no capítulo anterior, estes ataques têm por objectivo alterar os conteúdos dos sites, substituindo-os por mensagens de acusação ou denúncia. Este é o ponto que distingue o *hacktivism* do *hacking/cracking* normal de sites.

2. Como?

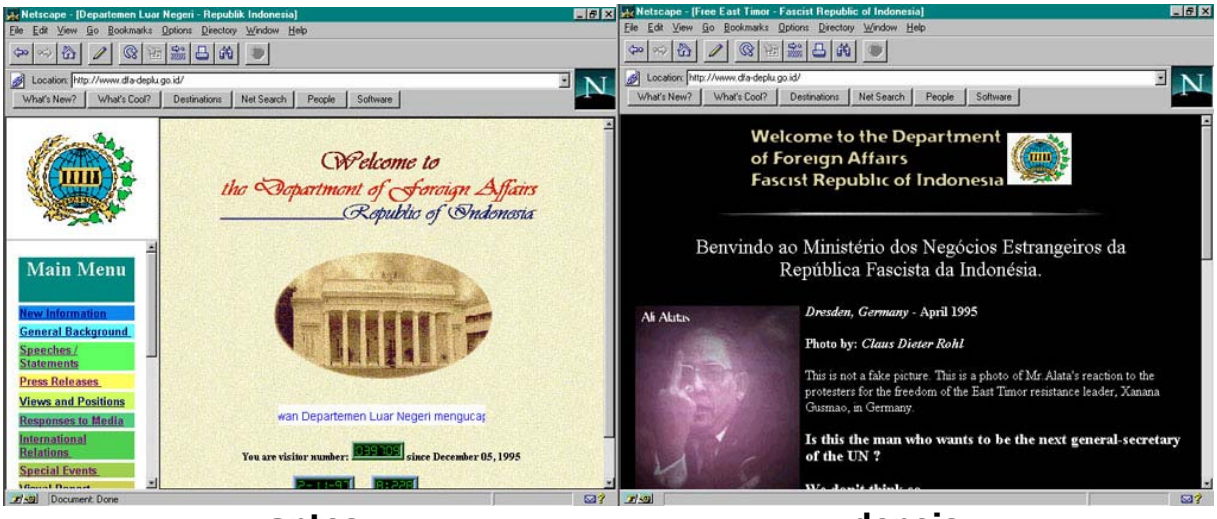
Os métodos usados para realizar este tipo de ataques são semelhantes aos usados pelos "*crackers*" para ganhar acesso ao servidor. Este tipo de *hacktivistas* distinguem-se pelos seus conhecimentos em segurança em redes.

Outra técnica usada é o **DNS tampering** que consiste basicamente em fazer com que o servidor de DNS resolva o domínio para o IP de uma outra máquina, alterando o conteúdo da sua base de dados. Assim, não é o servidor que é atacado explicitamente, mas os conteúdos são redireccionados para outra máquina.

3. Exemplos

Ataques a sites da Indonésia

Era impossível falar em *hacktivismo* sem mencionar o grupo de portugueses responsável por vários ataques a sites do governo da Indonésia em 1997. Estou a falar do grupo **Toxyn** que conseguiu alterar o site do departamento de negócios estrangeiros:



antes **depois**

Neste ataque nada foi destruído ou apagado. A intenção deste grupo, de mostrar ao mundo o que se estava a passar com o povo Timorense, estava bem definida à partida. Procuraram atrair atenção para a necessidade de independência de Timor Leste.

Depois deste ataque, muitos foram realizados, também por portugueses. Em 1998, mais de 40 servidores indonésios foram modificados para passarem a apresentar mensagens como "Free East Timor" em letras grandes, e links para sites acerca da violação dos direitos humanos por parte do governo da Indonésia.

Em Agosto de 1999, Ramos Horta avisou que estava a ser preparada uma rede global de "hackers" , com cerca de 100 pessoas, na maioria adolescentes, que iria deixar a Indonésia literalmente parada.

Milw0rm

Em Junho de 1998, este grupo internacional de *hackers* manifestou o seu protesto contra a realização de testes de armas nucleares na Índia. A pagina web do "Bhabha Atomic Research Center (BARC)" passava agora a mostrar um grande cogumelo atómico em que se lia qualquer coisa como: "se a guerra nuclear começar, tu serás o primeiro a gritar...". As intenções destes seis adolescentes entre 15 e 18 anos são questionáveis. Eles próprios afirmaram que o fizeram principalmente pelo desafio e pelo gozo. Além disso, eles deixaram alguns estragos para trás ao apagar dados em 2 servidores do (BARC) roubando várias páginas de email entre cientistas Hindus e Israelitas e documentos científicos.

Nesse mesmo ano, com a ajuda de um outro grupo de *hackers* intitulados por "Ashtray Lumberjacks", fizeram *tampering* ao servidor de DNS do ISP Britânico EasySpace. Com isto, mais de 300 domínios alojados neste servidor passaram a apontar para uma máquina dos Milw0rm com páginas de protesto contra a corrida às armas nucleares.

Na Califórnia, um jovem estudante com a alcunha de Bronc Buster, com a ajuda de um amigo seu conhecido por Zyklon, *crackou* uma rede Chinesa, alterando um site do governo acerca dos direitos humanos e interceptando a censura. Este jovem pertencia a um grupo de *hackers* com o nome de Legion of the Underground (LoU). Em 1998, um dos membros deste grupo declarou, em conferência de imprensa no IRC, *cyberguerra* contra as redes do Iraque e da China, alegando desrespeito pelos direitos humanos.

No entanto, esta medida não foi muito bem vista por outros dos mais importantes grupos de *hackers* do mundo. Numa carta co-assinada pelos *hackers* do 2600, the Chaos Computer Club, the Cult of the Dead Cow (CDC, criadores do Back Orifice), !Hispahak, L0pht Heavy Industries, Phrack, Pulhas (grupo *hacker* português), e vários membros da comunidade *hacker* alemã, lia-se a denúncia deste ataque dizendo: "declarar uma guerra contra um país, é a coisa mais irresponsável que um *hacker* pode fazer. Isto não tem nada a ver com *hacktivismo* ou ética *hacker* e não é nada que um *hacker* se deva orgulhar." Como disse Reid Fleming pertencente ou CDC, "Uma pessoa não pode legitimamente esperar melhorar o acesso livre à informação de um país, desactivando as suas redes de dados." Por esta altura já os membros do LoU tinham afirmado que esta não era a posição do grupo.

Em Agosto de 1999 deu-se o início de uma *cyberguerr*a entre os *hackers* da China contra *hackers* do Taiwan. Os Chineses colocavam em sites do governo mensagens que diziam que o Taiwan deveria pertencer sempre à China, enquanto os slogans alteraram o conteúdo de um site de tecnologia

chinês, com slogans anticomunistas. Isto só piorou as relações entre os dois países, já que normalmente nestes casos os governos tendem para culpar dos outros países.

Muitos outros casos poderiam ser referidos, como por exemplo, ataques durante a guerra do Kosovo....

5. *"E-mail bombs"*

1. O que é?

Estes ataques consistem em mandar uma grande quantidade de emails por dia. Isto além de gerar grande tráfego na rede (causando o mesmo efeito de uma manifestação virtual), torna impossível para a vitima de receber o seu correio legítimo. Este tipo de ataques são usados normalmente como meio de vingança e ameaça, mas também há quem os use para protestar contra medidas dos governos. Aqui torna-se ainda mais difícil distinguir onde começa o *Cyberterrorismo*, já que um dos grandes objectivos é deitar abaixo o sistema de email de uma instutuição.

2. Como?

Toda a gente sabe que o protocolo de SMTP é em si muito pouco seguro, sendo que se torna muito fácil criar software que além de mandar várias mensagens por minuto, encapsula o remetente, tornando impossível a filtragem do mesmo.

3. Exemplos

Em 1998, um grupo denominado por "Internet Black Tigers" iniciou aquele que seria o primeiro ataque realizado por terroristas ao sistema informático de um país. Este grupo pertencia ao grupo de guerrilha Tamil, que lutava pela independência daquele povo. Este ataque consistiu no envio de 800 mensagens por dia para as embaixadas do Sri Lanka.

6. *Uso de vírus e worms*

1. O que é?

O uso destes métodos está também muito ligado ao *cyberterrorismo*. Aqui existe uma intenção explicita de causar estragos. No entanto podem ser criados vírus ou *worms* que carreguem uma mensagem para os computadores vítimas.

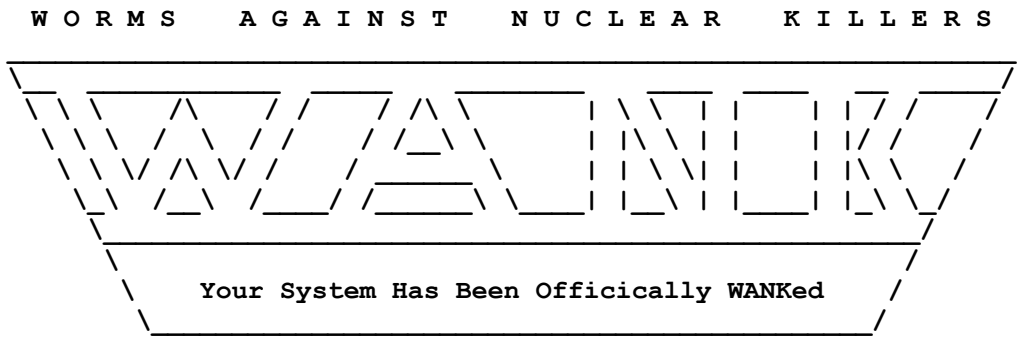
2. Como?

Vírus ou *worms* são pedaços de software desenhado para se propagar pelos computadores, causando alterações variadas no sistema. A diferença entre um vírus e um worm, consiste na dependência que um vírus tem, na sua propagação, de um ficheiro portador, ou de uma acção realizada pelo

utilizador (ex, abrir um *attachment* de um email). Um worm não necessita de estar ligado a um outro ficheiro espalhando-se por si mesmo.

3. Exemplos

O primeiro protesto deste tipo ocorreu já em 1989, em que foi lançado um worm com o nome de WANK (Worm Against Nuclear Killers) nos computadores do centro espacial da NASA em Greenbelt, quando estava para ser lançada a sonda Galilieo. Esta sonda estava preparada para chegar a Júpiter usando um sistema de propulsão com cerca de 15 toneladas alimentado de Plutónio radioactivo. Os cientistas, ao se ligarem às máquinas eram confrontados com o banner:



You talk of times of peace for all, and then prepare for war.

Em Fevereiro de 1999, o adolescente israelita Nir Zigdon foi promovido a herói nacional por ter limpado todo o conteúdo de um site governamental Iraquiano. Segundo as palavras deste jovem de 14 anos, o site "continha mentiras acerca dos Estados Unidos, Grã-Bretanha e Israel e ainda afirmações horríveis contra os judeus. (...) já que Israel tem medo de assassinar Saddam Hussein, o mínimo que eu podia fazer era destruir o seu site. Com a ajuda de software especializado, eu localizei o servidor do site até um dos estados do Golfo". Depois disto este *hacktivista* enviou um email dizendo que era um admirador Palestiniano de Saddam, e que tinha feito um vírus capaz de destruir sites israelitas. Isto foi motivo para abrirem um *attachment* contendo um vírus. Dentro de poucas horas, o site estava destruído. Pouco tempo depois Zigdon recebia uma mensagem do administrador do site, Faytz, com a mensagem "go to hell".

7. Conclusões

Ao analisar estes casos, vemos que certos tipos de *hacktivismo* como forma de protesto, não passa de uma adaptação para o mundo online do que se passa no mundo físico. Assim, temos bloqueios virtuais, comparáveis por exemplo com os protestos realizados pelos estudantes à porta das universidades impedindo o funcionamento das mesmas. Já alteração de sites de modo a conter mensagens de denúncia, são o correspondente virtual ao *graffitis* e cartazes colocados em locais bem visíveis ao público.

O resultado efectivo destes actos é difícil de determinar, mas nunca foi um factor decisivo na mudança de política de um país, ou de uma instituição. Estes eventos tornam-se particularmente mediáticos, trazendo à memória do publico em geral os assuntos problemáticos. Os *hacktivistas* usam assim estes meios para trazer publicidade às suas causas ou noutros casos a si próprios. Assim podem-se distinguir os *hacktivistas* verdadeiros, cujo único objectivo é transmitir uma mensagem ou marcar a sua posição acerca de um assunto. Por outro lado, existem aqueles que o fazem para mostrar a si próprios que são capazes de quebrar segurança em servidores, ou simplesmente por divertimento, causando uma deterioração da imagem dos próprios *hacktivistas*.

Em todo o caso, quer seja um apelo solitário de uma pessoa, ou uma grande campanha envolvendo milhares de pessoas, o *hacktivismo* continuará a ser uma arma poderosa de protesto, que irá ter cada vez mais importância à medida que a nossa sociedade se vai informatizando.

Referências:

1. Activism, Hacktivism, and Cyberterrorism:
   The Internet as a Tool for Influencing Foreign Policy:
   http://www.nautilus.org/info-policy/workshop/papers/denning.html

2. Hacktivism When Politics Meets Technology: http://hacktivism.openflows.org/

3. The Golden Age of Hacktivism: http://www.wired.com/news/politics/0,1283,15129,00.html

4. 2600 The Hacker Quarterly: http://www.2600.org/