DAMBALLA

Take Back Command-and-Control

The Opt-in Social Protesting Botnet

22nd ANNUAL FIRST CONFERENCE MIAMI

JUNE 13-18, 2010

About

- **Gunter Ollmann**
  - VP of Research, Damballa Inc.
- **Damballa Inc.**
  - Atlanta based security company focused on enterprise detection and mitigation of botnets
- **Brief Bio:**
  - Been in IT industry for two decades – over half of which has been 100% employed in security. Built and run international pentest teams, R&D groups and consulting practices around the world.
  - Formerly Chief Security Strategist for IBM, Director of X-Force for ISS, Professional Services Director for NGS Software, Head of Attack Services EMEA, etc.
  - Frequent writer, columnist and blogger with lots of whitepapers…
    - http://blog.damballa.com & http://technicalinfodotnet.blogspot.com/

In a nutshell

- Hacktivism – what's it all about?
- Why isn't it always "hacktivism"?
- Where's the social element?
- What tools are available?
- How will cyber-protesting change things?
- Using social networks for command and control?
- How will this impact business?

The Growth of Hacktivism

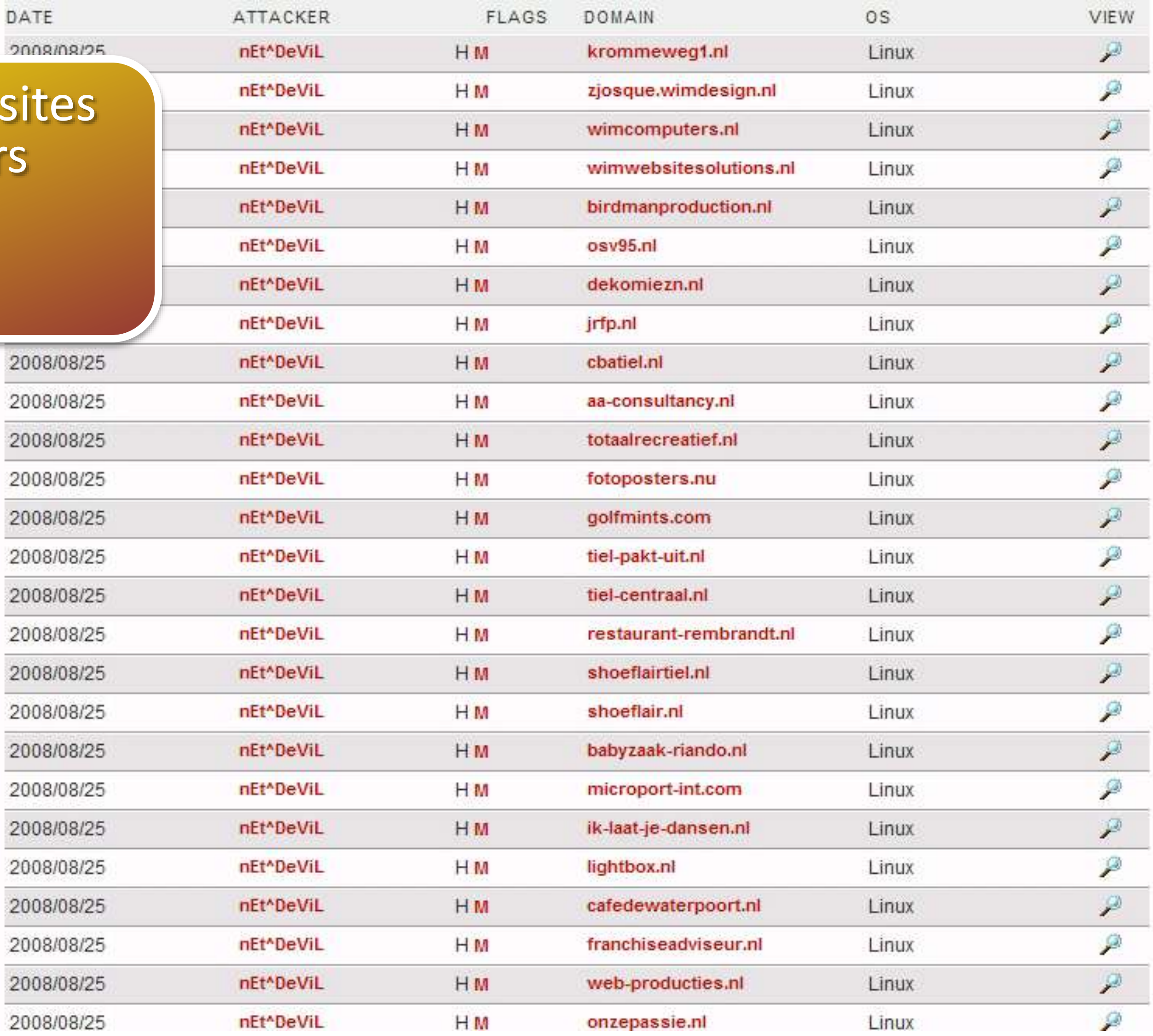
Hacktivism

- **A definition of "Hacktivism"…**
  - "The nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends."
  - "These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development."

Hacktivism - Defacement

Hundreds of Dutch web sites hacked by Islamic hackers

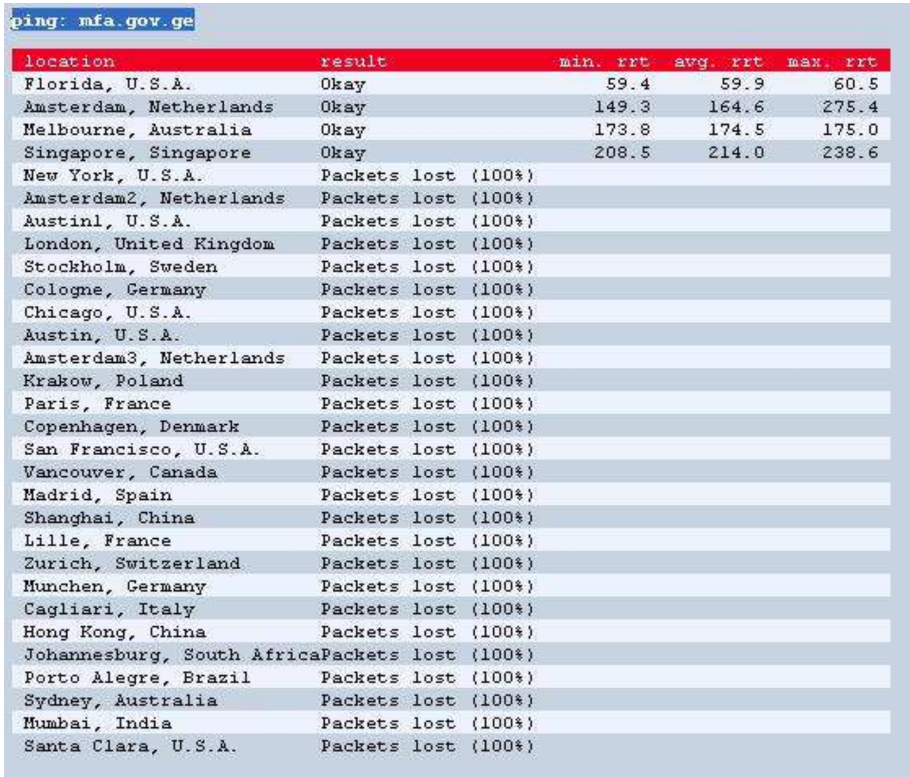
- Mass defacement
- August 2008



DATE	ATTACKER	FLAGS	DOMAIN	OS	VIEW
2008/08/25	nEt^DeViL	H M	krommeweg1.nl	Linux	🔍
	nEt^DeViL	H M	zjosque.wimdesign.nl	Linux	🔍
	nEt^DeViL	H M	wimcomputers.nl	Linux	🔍
	nEt^DeViL	H M	wimwebsitesolutions.nl	Linux	🔍
	nEt^DeViL	H M	birdmanproduction.nl	Linux	🔍
	nEt^DeViL	H M	osv95.nl	Linux	🔍
	nEt^DeViL	H M	dekomiezn.nl	Linux	🔍
	nEt^DeViL	H M	jrfp.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	cbatiel.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	aa-consultancy.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	totaalrecreatief.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	fotoposters.nu	Linux	🔍
2008/08/25	nEt^DeViL	H M	golfmints.com	Linux	🔍
2008/08/25	nEt^DeViL	H M	tiel-pakt-uit.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	tiel-centraal.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	restaurant-rembrandt.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	shoeflairtiel.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	shoeflair.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	babyzaak-riando.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	microport-int.com	Linux	🔍
2008/08/25	nEt^DeViL	H M	ik-laat-je-dansen.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	lightbox.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	cafedewaterpoort.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	franchiseadviseur.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	web-producties.nl	Linux	🔍
2008/08/25	nEt^DeViL	H M	onzepassie.nl	Linux	🔍

Hacktivism - DDoS

- **Coordinated Russia vs Georgia cyber attacks**
  – August 2008
- **Hactivist messages left across Web forums**
  – “For our motherland, brothers!”
  – “Your country is calling you”
- **Distributed lists of targets**
  – DDoS
  – Site defacements
  – SQL Injection

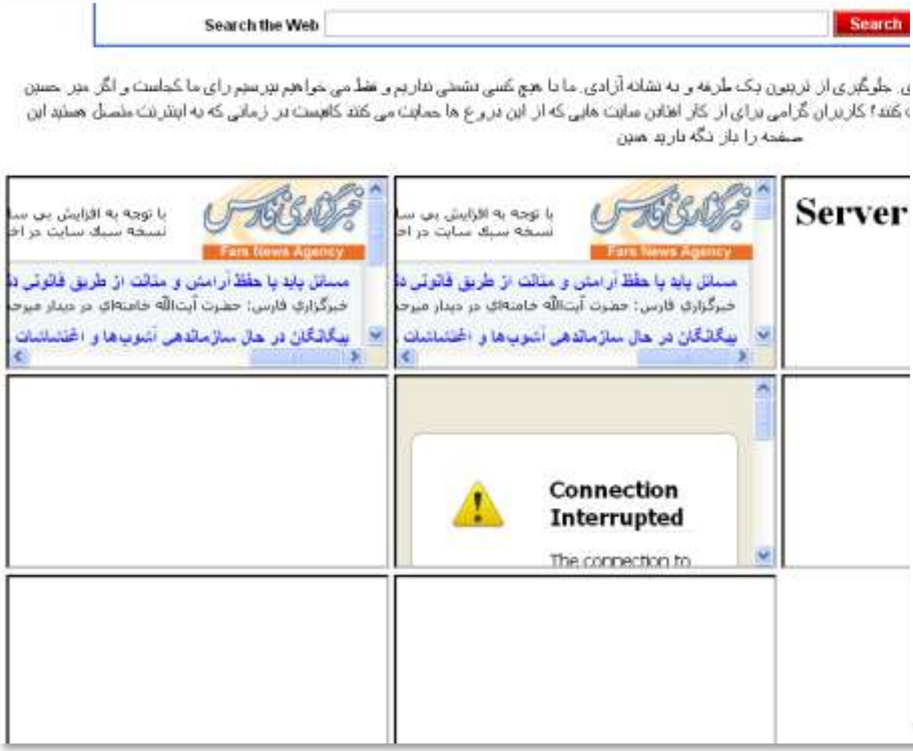


ping: mfa.gov.ge

location	result	min. rrt	avg. rrt	max. rrt
Florida, U.S.A.	Okay	59.4	59.9	60.5
Amsterdam, Netherlands	Okay	149.3	164.6	275.4
Melbourne, Australia	Okay	173.8	174.5	175.0
Singapore, Singapore	Okay	208.5	214.0	238.6
New York, U.S.A.	Packets lost (100%)			
Amsterdam2, Netherlands	Packets lost (100%)			
Austin1, U.S.A.	Packets lost (100%)			
London, United Kingdom	Packets lost (100%)			
Stockholm, Sweden	Packets lost (100%)			
Cologne, Germany	Packets lost (100%)			
Chicago, U.S.A.	Packets lost (100%)			
Austin, U.S.A.	Packets lost (100%)			
Amsterdam3, Netherlands	Packets lost (100%)			
Krakow, Poland	Packets lost (100%)			
Paris, France	Packets lost (100%)			
Copenhagen, Denmark	Packets lost (100%)			
San Francisco, U.S.A.	Packets lost (100%)			
Vancouver, Canada	Packets lost (100%)			
Madrid, Spain	Packets lost (100%)			
Shanghai, China	Packets lost (100%)			
Lille, France	Packets lost (100%)			
Zurich, Switzerland	Packets lost (100%)			
Munchen, Germany	Packets lost (100%)			
Cagliari, Italy	Packets lost (100%)			
Hong Kong, China	Packets lost (100%)			
Johannesburg, South Africa	Packets lost (100%)			
Porto Alegre, Brazil	Packets lost (100%)			
Sydney, Australia	Packets lost (100%)			
Mumbai, India	Packets lost (100%)			
Santa Clara, U.S.A.	Packets lost (100%)			

Hacktivism – Internal…

- **Citizen-based hactivism against internal political sites**
  - Iran elections, June 2009



Search the Web Search

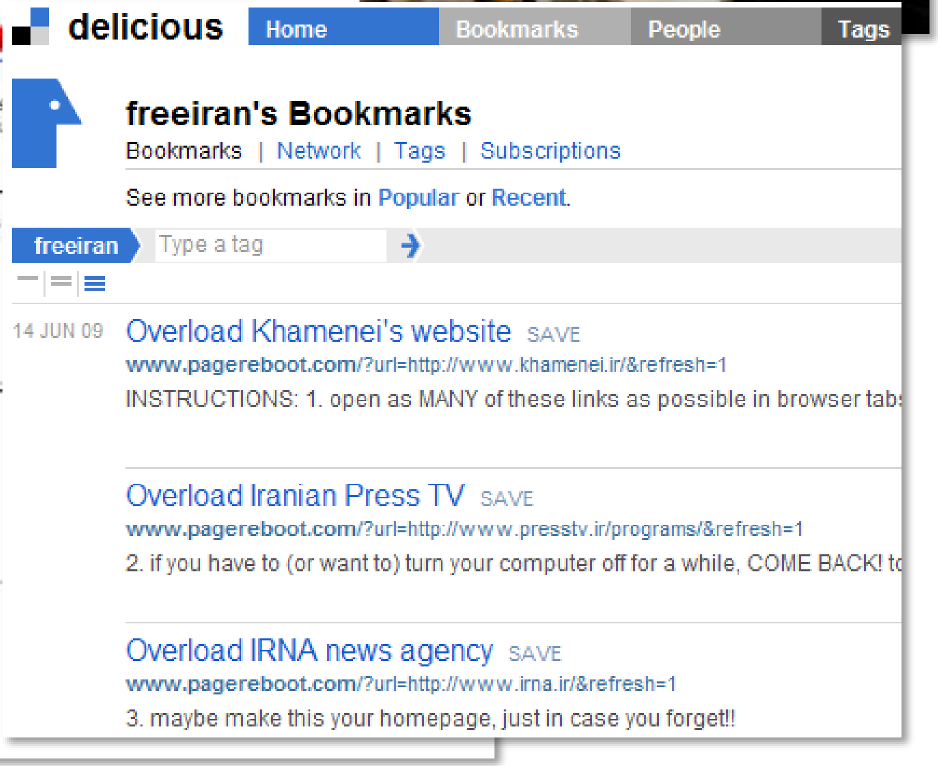
ی. جلوگیری از تریبون یک طرفه و به نشانه آزادی. ما با هیچ کسی دشمنی نداریم و فقط می خواهیم بپرسیم رای ما کجاست و اگر میر حسین
ه کنند؟ کاربران گرامی برای از کار افتادن سایت هایی که از این دروغ ها حمایت می کنند کافیست در زمانی که به اینترنت متصل هستید این
صفحه را باز نگه دارید همین

با توجه به افزایش بی سا
نسخه سبک سایت در اخ
مسئلن باید با حفظ آرامش و متانت از طریق قانونی د
خبرگزاری فارس: حضرت آیت‌الله خامنه‌ای در دیدار میرح
بیگانگان در حل سازماندهی آشوب ها و اغتشاشات

Server

Connection Interrupted

The connection to



delicious Home Bookmarks People Tags

freeiran's Bookmarks

Bookmarks | Network | Tags | Subscriptions

See more bookmarks in Popular or Recent.

freeiran Type a tag

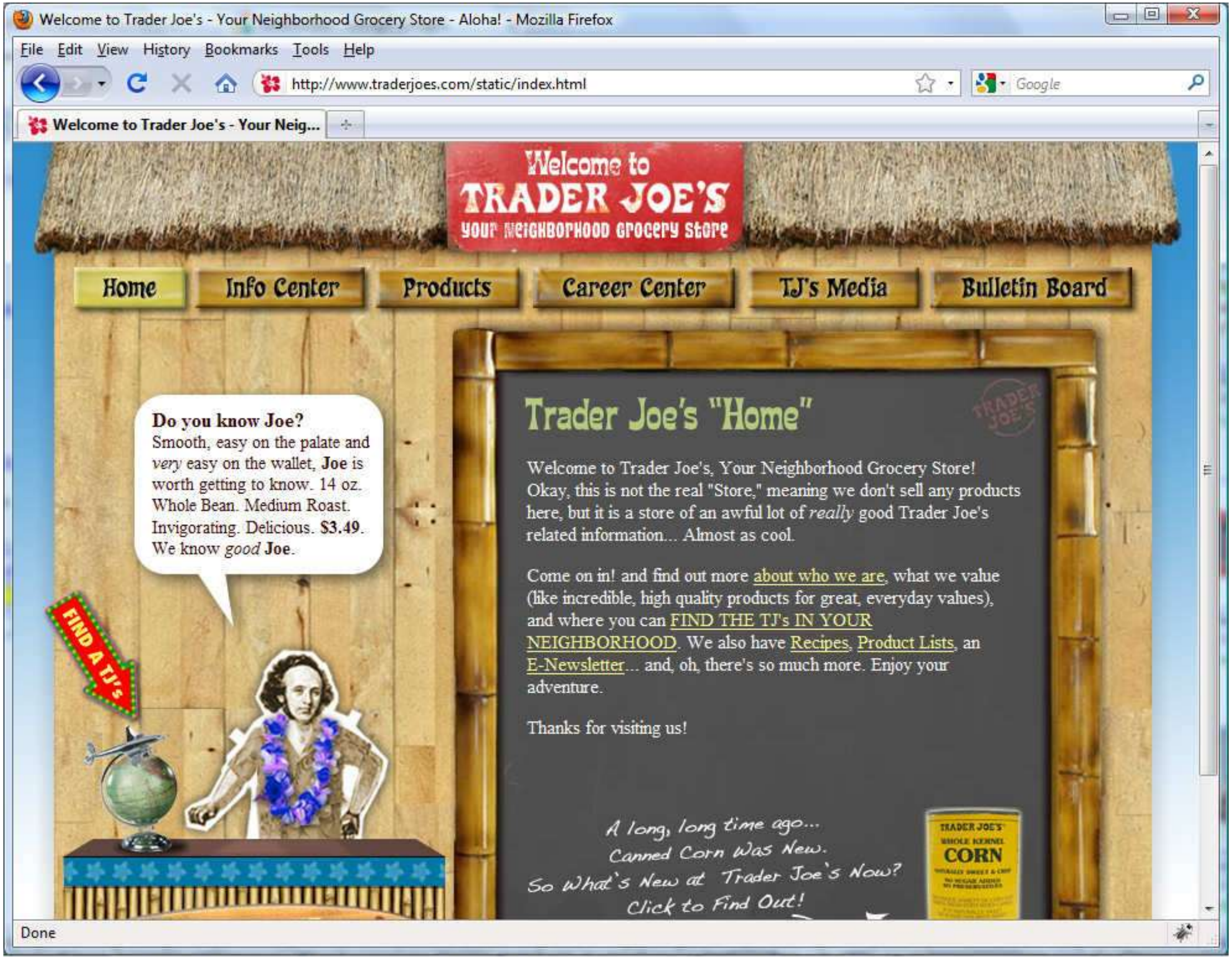
14 JUN 09

Overload Khamenei's website SAVE
www.pagereboot.com/?url=http://www.khamenei.ir/&refresh=1
INSTRUCTIONS: 1. open as MANY of these links as possible in browser tab

Overload Iranian Press TV SAVE
www.pagereboot.com/?url=http://www.presstv.ir/programs/&refresh=1
2. if you have to (or want to) turn your computer off for a while, COME BACK! to

Overload IRNA news agency SAVE
www.pagereboot.com/?url=http://www.irna.ir/&refresh=1
3. maybe make this your homepage, just in case you forget!!

Changing times…


Welcome to Trader Joe's - Your Neighborhood Grocery Store - Aloha! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.traderjoes.com/static/index.html
Google
Welcome to Trader Joe's - Your Neig...
Welcome to
TRADER JOE'S
your neighborhood grocery store
Home
Info Center
Products
Career Center
TJ's Media
Bulletin Board
FIND A TJ's
Done

Do you know Joe? Smooth, easy on the palate and *very* easy on the wallet, **Joe** is worth getting to know. 14 oz. Whole Bean. Medium Roast. Invigorating. Delicious. **$3.49**. We know *good* **Joe**.

Trader Joe's "Home"

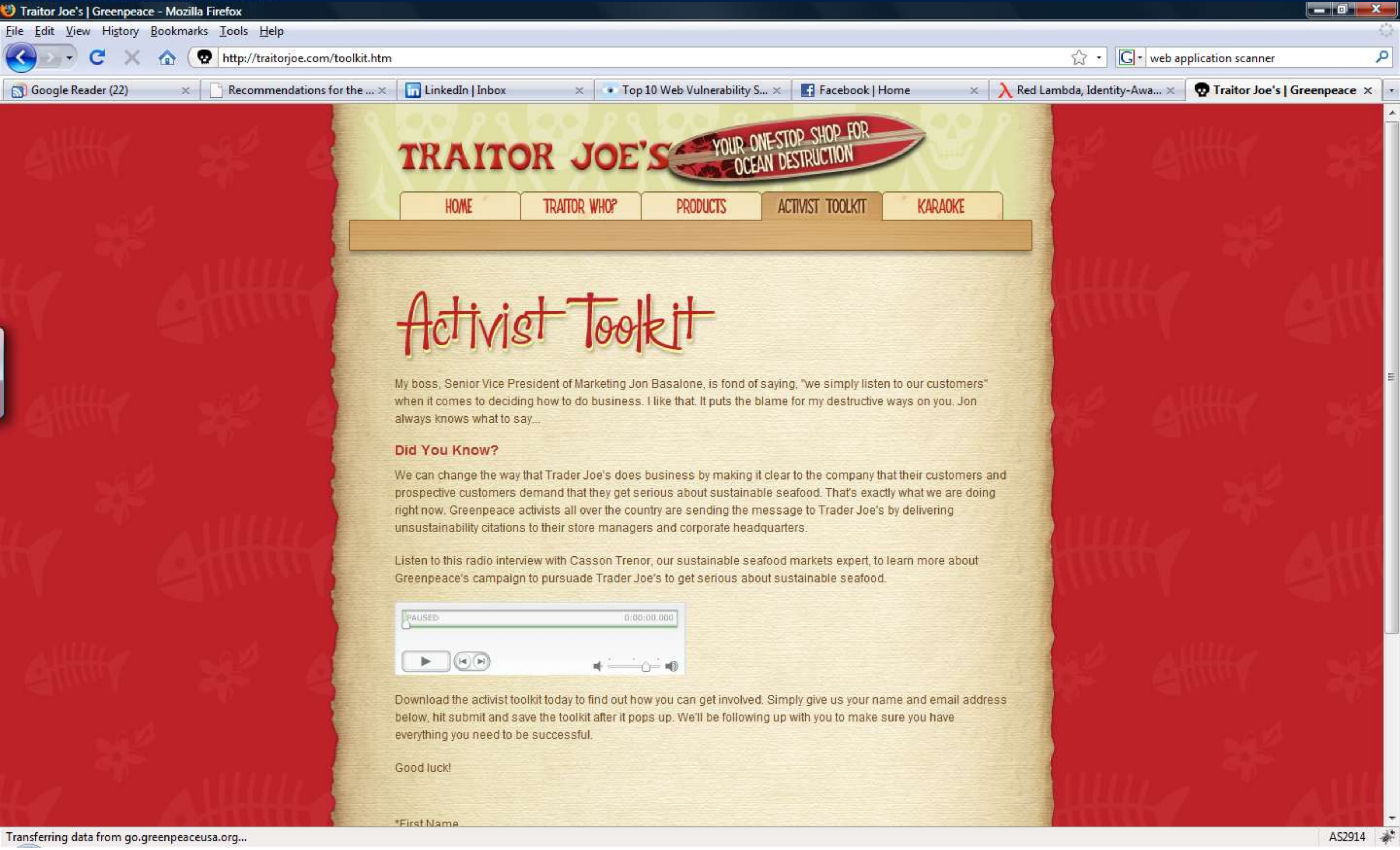
Welcome to Trader Joe's, Your Neighborhood Grocery Store! Okay, this is not the real "Store," meaning we don't sell any products here, but it is a store of an awful lot of *really* good Trader Joe's related information... Almost as cool.

Come on in! and find out more about who we are, what we value (like incredible, high quality products for great, everyday values), and where you can FIND THE TJ's IN YOUR NEIGHBORHOOD. We also have Recipes, Product Lists, an E-Newsletter... and, oh, there's so much more. Enjoy your adventure.

Thanks for visiting us!

A long, long time ago...
Canned Corn Was New.
So What's New at Trader Joe's Now?
Click to Find Out!

… define “political”?


Traitor Joe's | Greenpeace - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://traitorjoe.com/toolkit.htm
web application scanner
Google Reader (22)
Recommendations for the ...
LinkedIn | Inbox
Top 10 Web Vulnerability S...
Facebook | Home
Red Lambda, Identity-Awa...
Traitor Joe's | Greenpeace
TRAITOR JOE'S
YOUR ONE-STOP SHOP FOR OCEAN DESTRUCTION
HOME
TRAITOR WHO?
PRODUCTS
ACTIVIST TOOLKIT
KARAOKE
PAUSED
0:00:00.000
Transferring data from go.greenpeaceusa.org...
AS2914

Activist Toolkit

My boss, Senior Vice President of Marketing Jon Basalone, is fond of saying, "we simply listen to our customers" when it comes to deciding how to do business. I like that. It puts the blame for my destructive ways on you. Jon always knows what to say...

Did You Know?

We can change the way that Trader Joe's does business by making it clear to the company that their customers and prospective customers demand that they get serious about sustainable seafood. That's exactly what we are doing right now. Greenpeace activists all over the country are sending the message to Trader Joe's by delivering unsustainability citations to their store managers and corporate headquarters.

Listen to this radio interview with Casson Trenor, our sustainable seafood markets expert, to learn more about Greenpeace's campaign to pursuade Trader Joe's to get serious about sustainable seafood.

Download the activist toolkit today to find out how you can get involved. Simply give us your name and email address below, hit submit and save the toolkit after it pops up. We'll be following up with you to make sure you have everything you need to be successful.

Good luck!

*First Name

Protesting for anyone...

Introduction

- Social Network phenomenon creating new forums for mass communication and event coordination
- Virtual community "groups" can be created to address passionate topics, political ideals and social injustices
- Groups tend to attract like-minded communities of interest and can swell their ranks rapidly
- Members of a group with targeted agenda's can promote calls to action and facilitate "mob" responses
- Distribution of cyber arms and coordinated attacks possible

Social Networking Sites

- Social networking sites on the increase e.g.

- Huge numbers of online members
- Almost all sites have the ability to create new "groups" or "forums" for discussion and information sharing

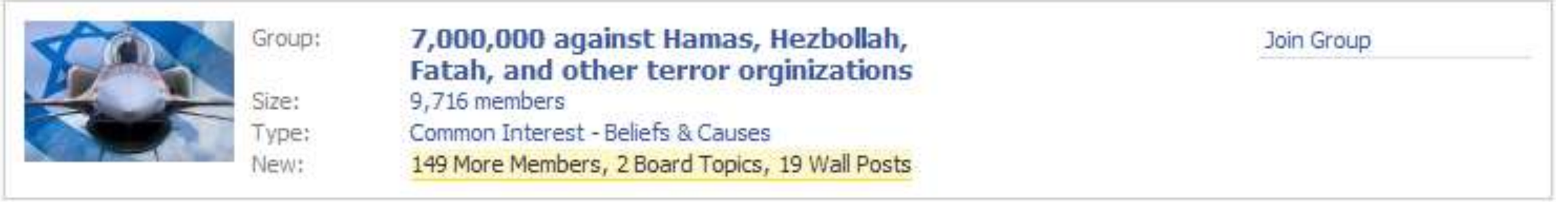
Site	Members
Facebook	400,000,000
MySpace	130,000,000
Skyrock	22,000,000
LinkedIn	65,000,000
Orkut	100,000,000
Bebo	40,000,000
Hi5	80,000,000
Nexopia	1,400,000
Mixi	24,000,000
Vkontakte	75,000,000
Netlog	62,000,000
Habbo	162,000,000
Friendster	115,000,000

Wikipedia

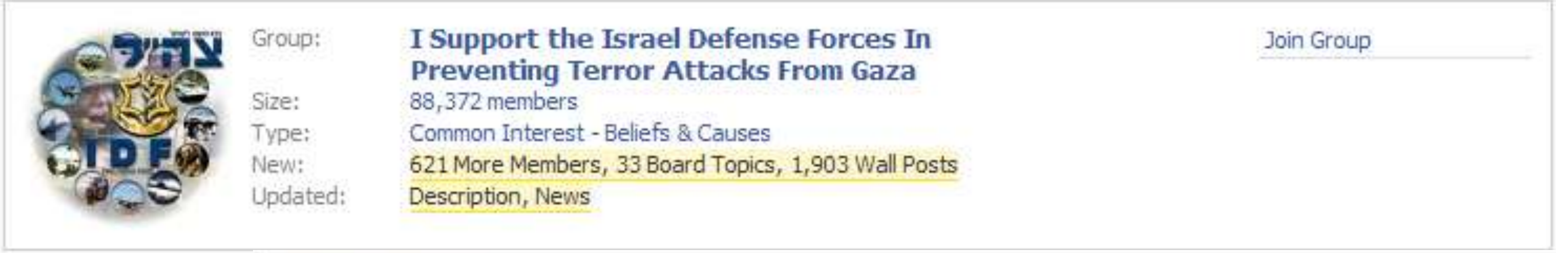
DAMBALLA
Take Back Command-and-Control

Common Interest Social Network Groups

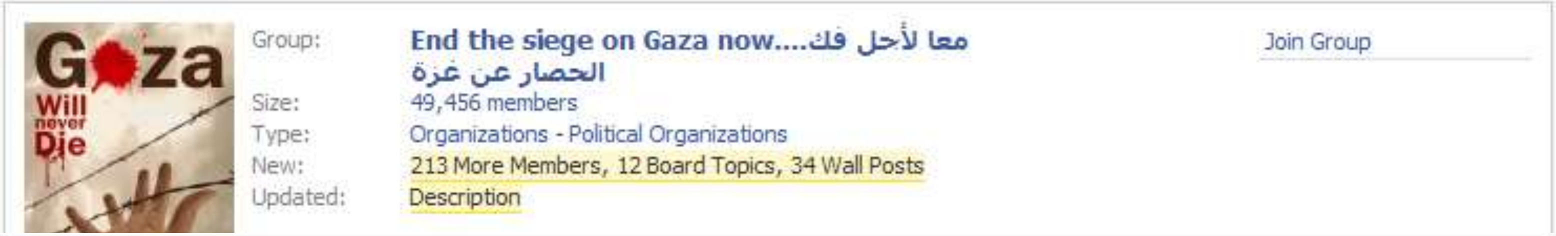
- **Example: Military actions in the Gaza territory led to new social network groups supporting the opposing sides** **(Jan 2009)**



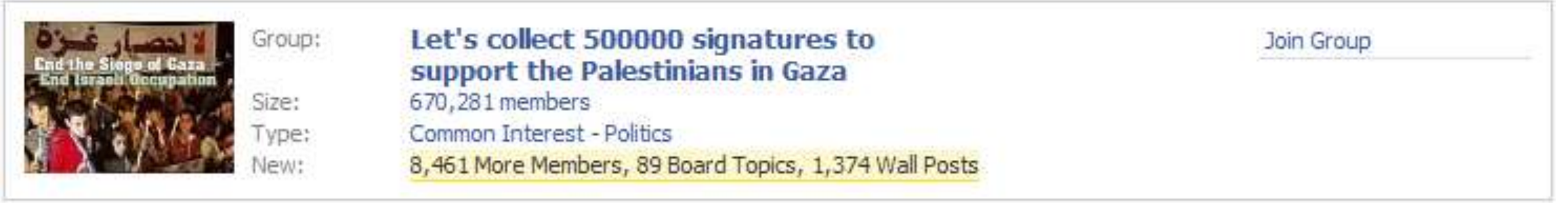
Group: 7,000,000 against Hamas, Hezbollah, Fatah, and other terror orginizations
Size: 9,716 members
Type: Common Interest - Beliefs & Causes
New: 149 More Members, 2 Board Topics, 19 Wall Posts



Group: I Support the Israel Defense Forces In Preventing Terror Attacks From Gaza
Size: 88,372 members
Type: Common Interest - Beliefs & Causes
New: 621 More Members, 33 Board Topics, 1,903 Wall Posts
Updated: Description, News



Group: End the siege on Gaza now....معا لأجل فك الحصار عن غزة
Size: 49,456 members
Type: Organizations - Political Organizations
New: 213 More Members, 12 Board Topics, 34 Wall Posts
Updated: Description

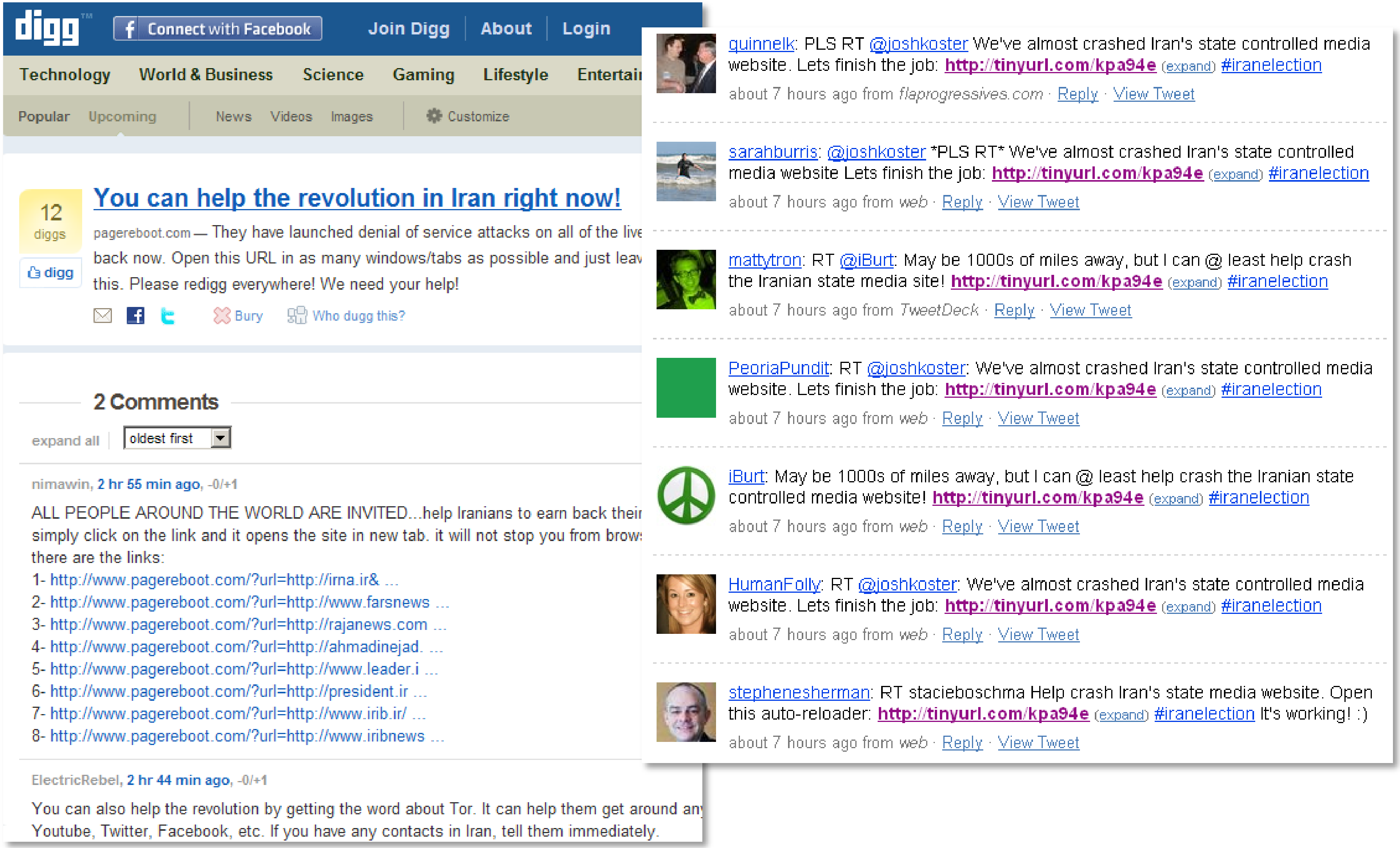


Group: Let's collect 500000 signatures to support the Palestinians in Gaza
Size: 670,281 members
Type: Common Interest - Politics
New: 8,461 More Members, 89 Board Topics, 1,374 Wall Posts

DAMBALLA

Take Back Command-and-Control

Iran Protesting – June 2009



12 diggs

digg

You can help the revolution in Iran right now!

pagereboot.com — They have launched denial of service attacks on all of the live back now. Open this URL in as many windows/tabs as possible and just leav this. Please redigg everywhere! We need your help!

2 Comments

expand all | oldest first

nimawin, 2 hr 55 min ago, -0/+1

ALL PEOPLE AROUND THE WORLD ARE INVITED...help Iranians to earn back their simply click on the link and it opens the site in new tab. it will not stop you from brows there are the links:

1- http://www.pagereboot.com/?url=http://irna.ir& ...
2- http://www.pagereboot.com/?url=http://www.farsnews ...
3- http://www.pagereboot.com/?url=http://rajanews.com ...
4- http://www.pagereboot.com/?url=http://ahmadinejad. ...
5- http://www.pagereboot.com/?url=http://www.leader.i ...
6- http://www.pagereboot.com/?url=http://president.ir ...
7- http://www.pagereboot.com/?url=http://www.irib.ir/ ...
8- http://www.pagereboot.com/?url=http://www.iribnews ...

ElectricRebel, 2 hr 44 min ago, -0/+1

You can also help the revolution by getting the word about Tor. It can help them get around any Youtube, Twitter, Facebook, etc. If you have any contacts in Iran, tell them immediately.

quinnelk: PLS RT @joshkoster We've almost crashed Iran's state controlled media website. Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection

about 7 hours ago from flaprogressives.com · Reply · View Tweet

sarahburris: @joshkoster *PLS RT* We've almost crashed Iran's state controlled media website Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection

about 7 hours ago from web · Reply · View Tweet

mattytron: RT @iBurt: May be 1000s of miles away, but I can @ least help crash the Iranian state media site! http://tinyurl.com/kpa94e (expand) #iranelection

about 7 hours ago from TweetDeck · Reply · View Tweet

PeoriaPundit: RT @joshkoster: We've almost crashed Iran's state controlled media website. Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection

about 7 hours ago from web · Reply · View Tweet

iBurt: May be 1000s of miles away, but I can @ least help crash the Iranian state controlled media website! http://tinyurl.com/kpa94e (expand) #iranelection

about 7 hours ago from web · Reply · View Tweet

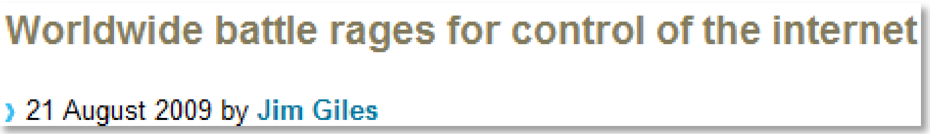
HumanFolly: RT @joshkoster: We've almost crashed Iran's state controlled media website. Lets finish the job: http://tinyurl.com/kpa94e (expand) #iranelection

about 7 hours ago from web · Reply · View Tweet

stephenesherman: RT stacieboschma Help crash Iran's state media website. Open this auto-reloader: http://tinyurl.com/kpa94e (expand) #iranelection It's working! :)

about 7 hours ago from web · Reply · View Tweet

… the governmental response


Worldwide battle rages for control of the internet

21 August 2009 by Jim Giles

- WHEN thousands of protestors took to the streets in Iran following this year's disputed presidential election, Twitter messages sent by activists let the world know about the brutal policing that followed. A few months earlier, campaigners in Moldova used Facebook to organize protests against the country's communist government, and elsewhere too the internet is playing an increasing role in political dissent.
- **Now governments are trying to regain control. *By reinforcing their efforts to monitor activity online, they hope to deprive dissenters of information and the ability to communicate.***
- The latest evidence of these clampdowns comes in a report on the Middle East and north Africa by the OpenNet Initiative (ONI), a collaboration of researchers based in the UK and North America. ***Among the restrictions it reports are clampdowns on Facebook in Syria and the use of hidden cameras in Saudi Arabia's internet cafes.***

NewScientist

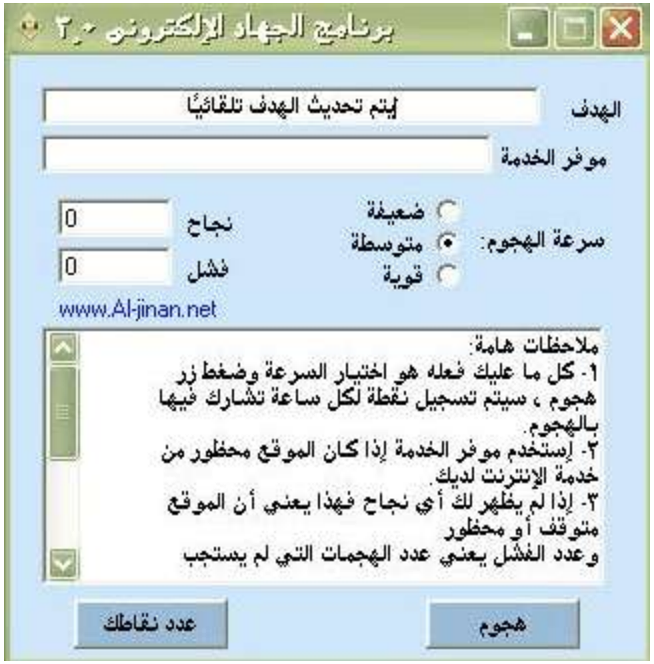
Moving Beyond "Discussion"

- **Popular movements and causes within a social network may stretch beyond *joining* an online group and *participation* in group discussions**

- **Online groups are an ideal vehicle for organizing more influential or disrupting mass protests**
  - Physical
    - "here's the private phone number of the ambassador. Tell her what you really think."
    - "meet outside the French embassy on Sunday with your plaque"
  - Cyber
    - "everyone email staff@embassy.fr with your photos"
    - "their Web site reboots if you type ###### in to the visa request page. If we all do this, no one will be able to get a visa!"

Cyber-Jihad Communities

- **Numerous external Web sites already exist specifically for the coordination of cyber attacks**
  - Most sites are organized along religious and political views
  - Independent of social network sites – but often referred to from them
- **Several Web sites also offer tools that community members can download and target a mutual adversary**
  - Often referred to as a “Cyber-Jihad”



برنامج الجهاد الإلكتروني ٢.٠

الهدف: يتم تحديث الهدف تلقائيًا

موفر الخدمة:

سرعة الهجوم: ○ ضعيفة ● متوسطة ○ قوية

نجاح: 0

فشل: 0

www.Al-jinan.net

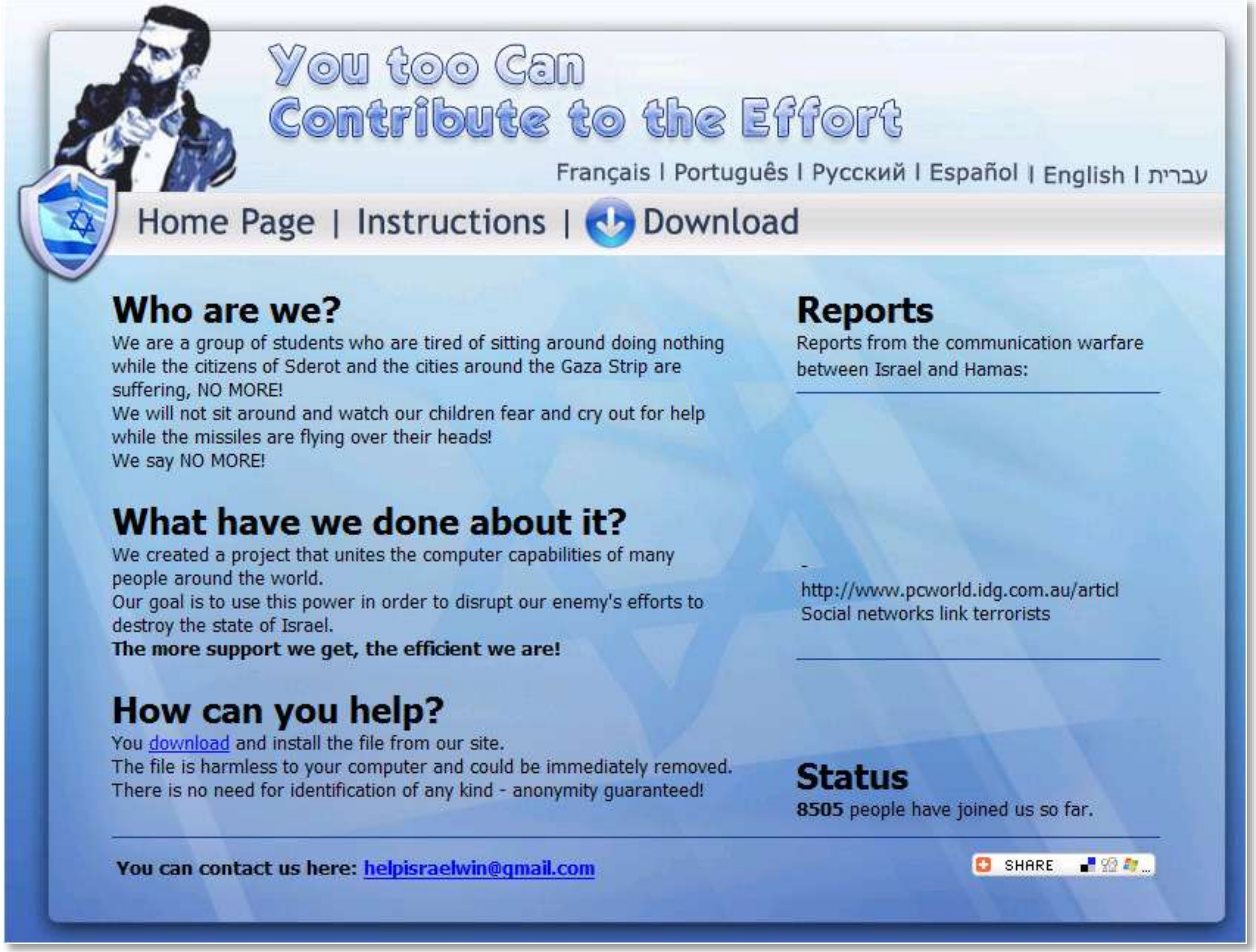
ملاحظات هامة:
١- كل ما عليك فعله هو اختيار السرعة وضغط زر
هجوم ، سيتم تسجيل نقطة لكل ساعة تشارك فيها
بالهجوم.
٢- إستخدم موفر الخدمة إذا كان الموقع محظور من
خدمة الإنترنت لديك.
٣- إذا لم يظهر لك أي نجاح فهذا يعني أن الموقع
متوقف أو محظور
وعدد الفشل يعني عدد الهجمات التي لم يستجب

> “Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline. The application even includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button.”

Al-jinan site(s) shut down late 2007

External Cyber Jihad Coordination

- **External Web sites promoting tools and tactics to target adversaries**
- **Social network forums and groups often *link* to external tool distribution sites**


Français I Português I Русский I Español I English I עברית
Home Page | Instructions | Download
SHARE

You too Can Contribute to the Effort

Who are we?

We are a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering, NO MORE!
We will not sit around and watch our children fear and cry out for help while the missiles are flying over their heads!
We say NO MORE!

What have we done about it?

We created a project that unites the computer capabilities of many people around the world.
Our goal is to use this power in order to disrupt our enemy's efforts to destroy the state of Israel.
The more support we get, the efficient we are!

How can you help?

You download and install the file from our site.
The file is harmless to your computer and could be immediately removed.
There is no need for identification of any kind - anonymity guaranteed!

Reports

Reports from the communication warfare between Israel and Hamas:

-
http://www.pcworld.idg.com.au/articl
Social networks link terrorists

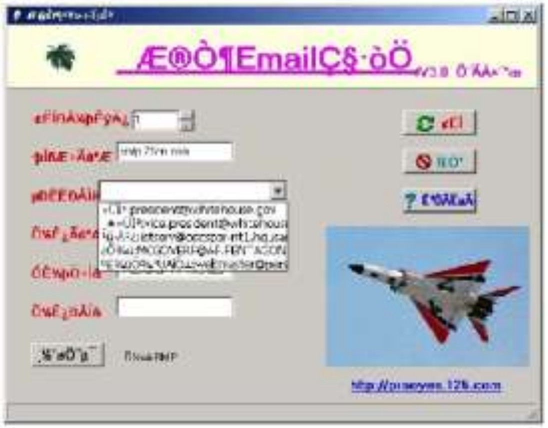
Status

8505 people have joined us so far.

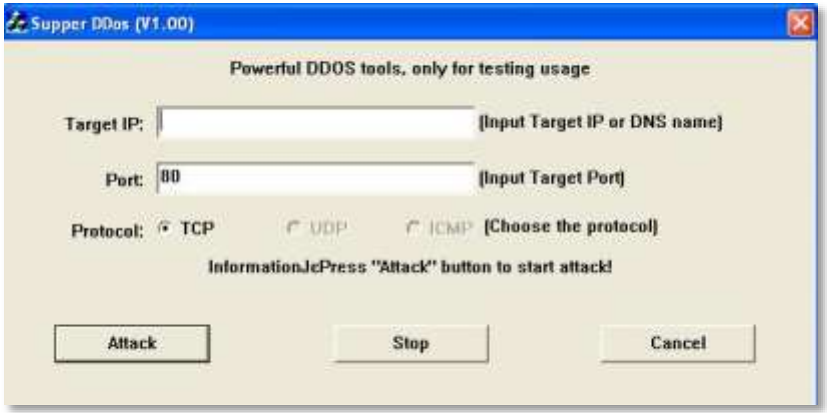
You can contact us here: helpisraelwin@gmail.com

Community Attack Tools

- **Tools used for community targeted attacks are typically of the distributed denial of service (DDoS) variety**
- **Target lists normally agreed in advance**
- **Most common DDoS tool categories used for cyber-jihad:**
  - Mail bombers
    - Send hundreds of emails per minute to a specific email address
  - Network flooders
    - Saturate Web site connections
    - Exhaust system resources
    - ICMP flooding



Korean mail bomber circa. 2007


Supper DDos (V1.00)

Powerful DDOS tools, only for testing usage

Target IP: (Input Target IP or DNS name)

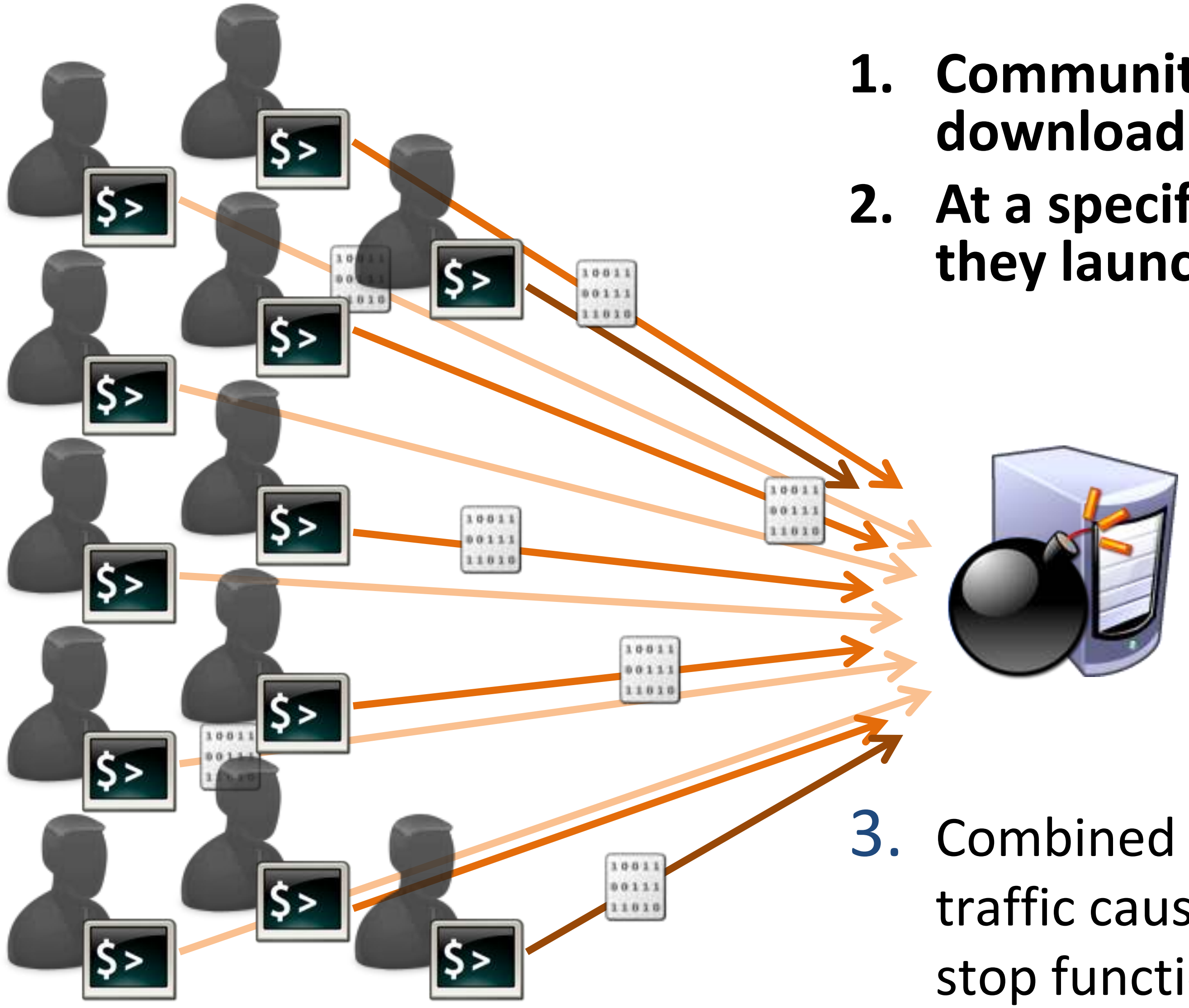
Port: 80 (Input Target Port)

Protocol: ● TCP ○ UDP ○ ICMP (Choose the protocol)

Information.JcPress "Attack" button to start attack!

Common network DDoS testing tool

DDoS Mechanics



1. **Community members download the attack tool**
2. **At a specified date & time they launch their attack**

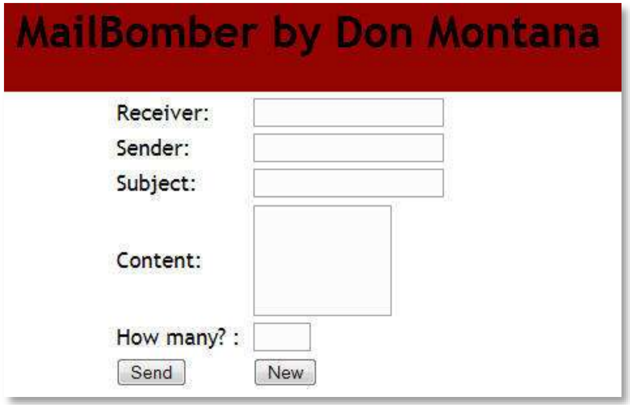
5,000 home DSL users launching a simultaneous attack can create:
  * 1.3 Gbps traffic volume,
  * 150m emails per hour,
  * 250k transactions per second

3. Combined volume of attack traffic causes the target to stop functioning

Tools for anyone…

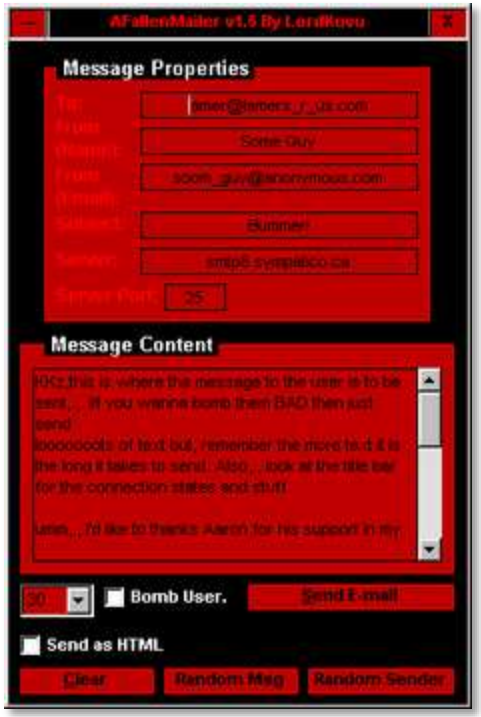
Mail Bombers

- **Mail bomber software freely available**
- **180+ bombers currently in circulation**
  - Mail bombers are very easy to create
  - Source code is widely available



MailBomber by Don Montana

Receiver:
Sender:
Subject:
Content:
How many? :



AFallenMailer v1.5 By LordKuvu

Message Properties

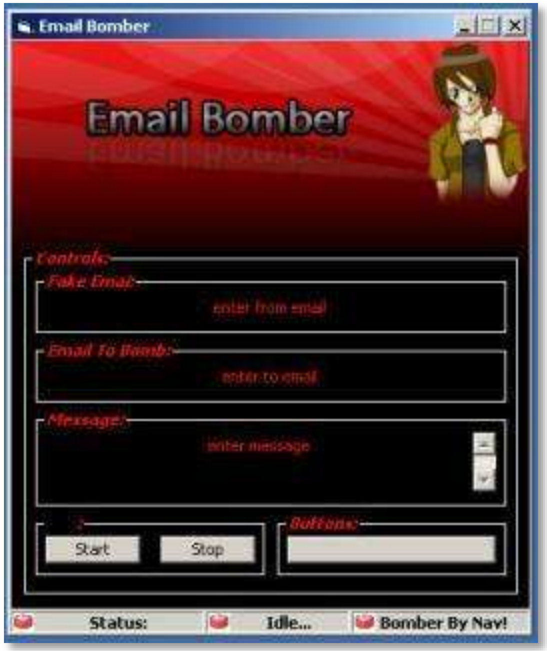
To: amer@ambers_r_us.com
From (Name): Some Guy
From (Email): sooh_guy@anonymous.com
Subject: Bummer
Server: smtp8.sympatico.ca
Server Port: 25

Message Content

KKz this is where the message to the user is to be sent.... if you wanna bomb them BAD then just send
looooooots of text but, remember the more text it is the long it takes to send. Also... look at the title bar for the connection states and stuff

umm... i'd like to thanks Aaron for his support in my

30 □ Bomb User.
□ Send as HTML

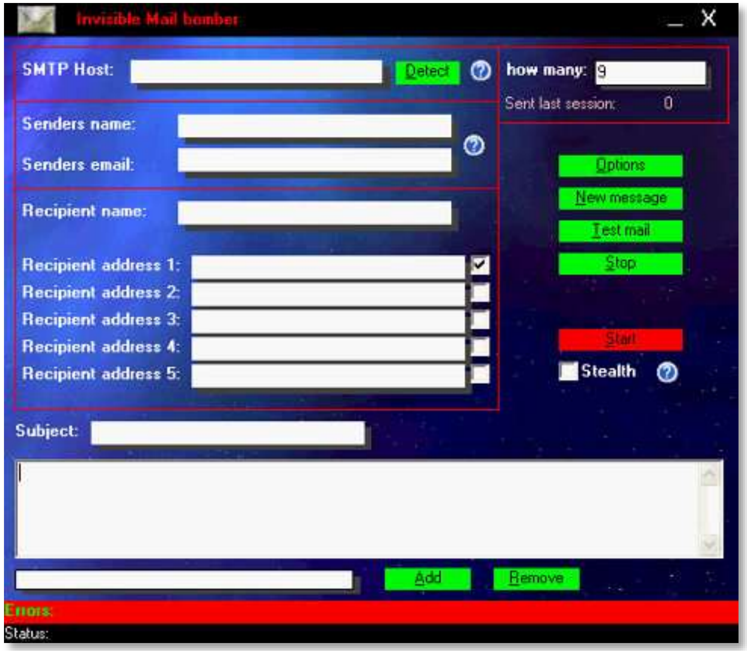


Email Bomber

Email Bomber

Controls:
Fake Email: enter from email
Email To Bomb: enter to email
Message: enter message

Status: Idle... Bomber By Nav!



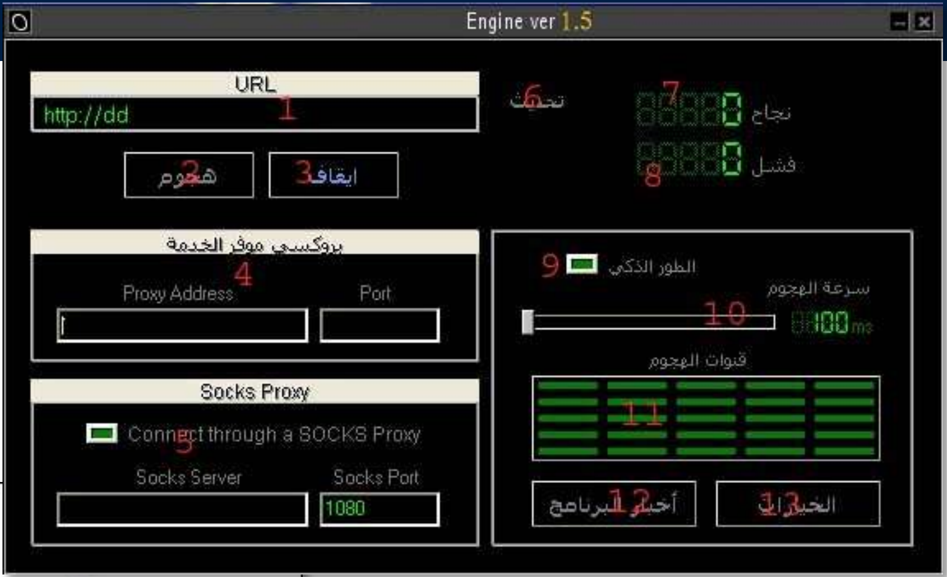
Invisible Mail bomber

SMTP Host:
how many: 9
Sent last session: 0
Senders name:
Senders email:
Recipient name:
Recipient address 1: ☑
Recipient address 2: □
Recipient address 3: □
Recipient address 4: □
Recipient address 5: □
Subject:
□ Stealth

Errors:
Status:

Network Flooders

- **Easy to use (and create)**
  - "Point and shoot"
  - Regionalization of tools
  - Themed versions



Engine ver 1.5

URL: http://dd

هجوم | ايقاف

نجاح 00000

فشل 00000

بروكسي موفر الخدمة

Proxy Address | Port

Socks Proxy

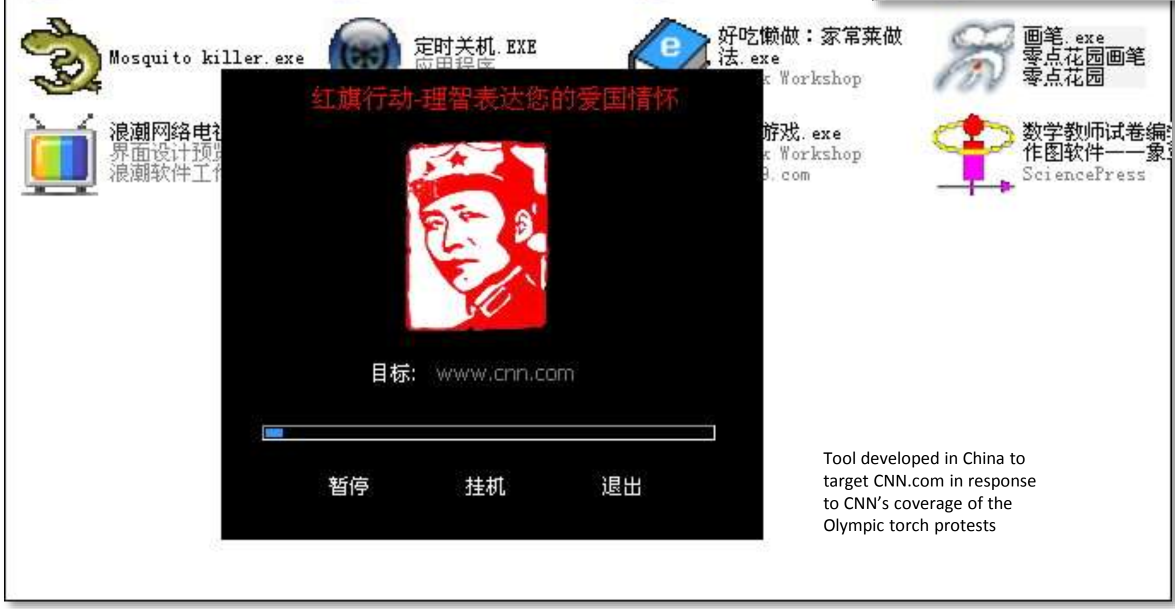
Connect through a SOCKS Proxy

Socks Server | Socks Port: 1080

الطور الذكي

سرعة الهجوم: 100 ms

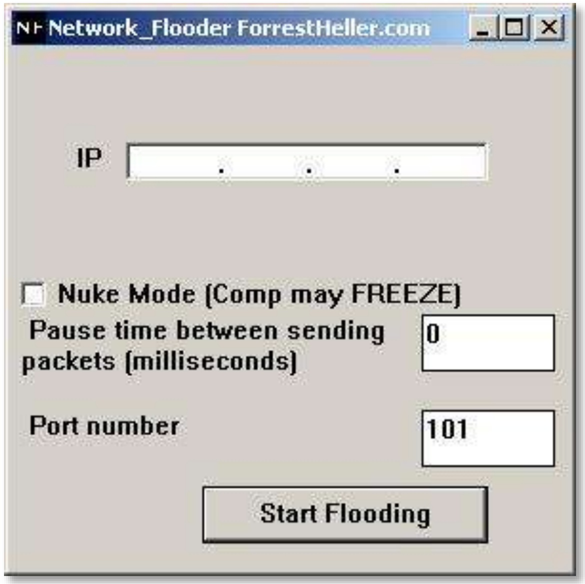
قنوات الهجوم



红旗行动-理智表达您的爱国情怀

目标: www.cnn.com

Tool developed in China to target CNN.com in response to CNN's coverage of the Olympic torch protests



Network_Flooder ForrestHeller.com

IP: . . .

☐ Nuke Mode (Comp may FREEZE)

Pause time between sending packets (milliseconds): 0

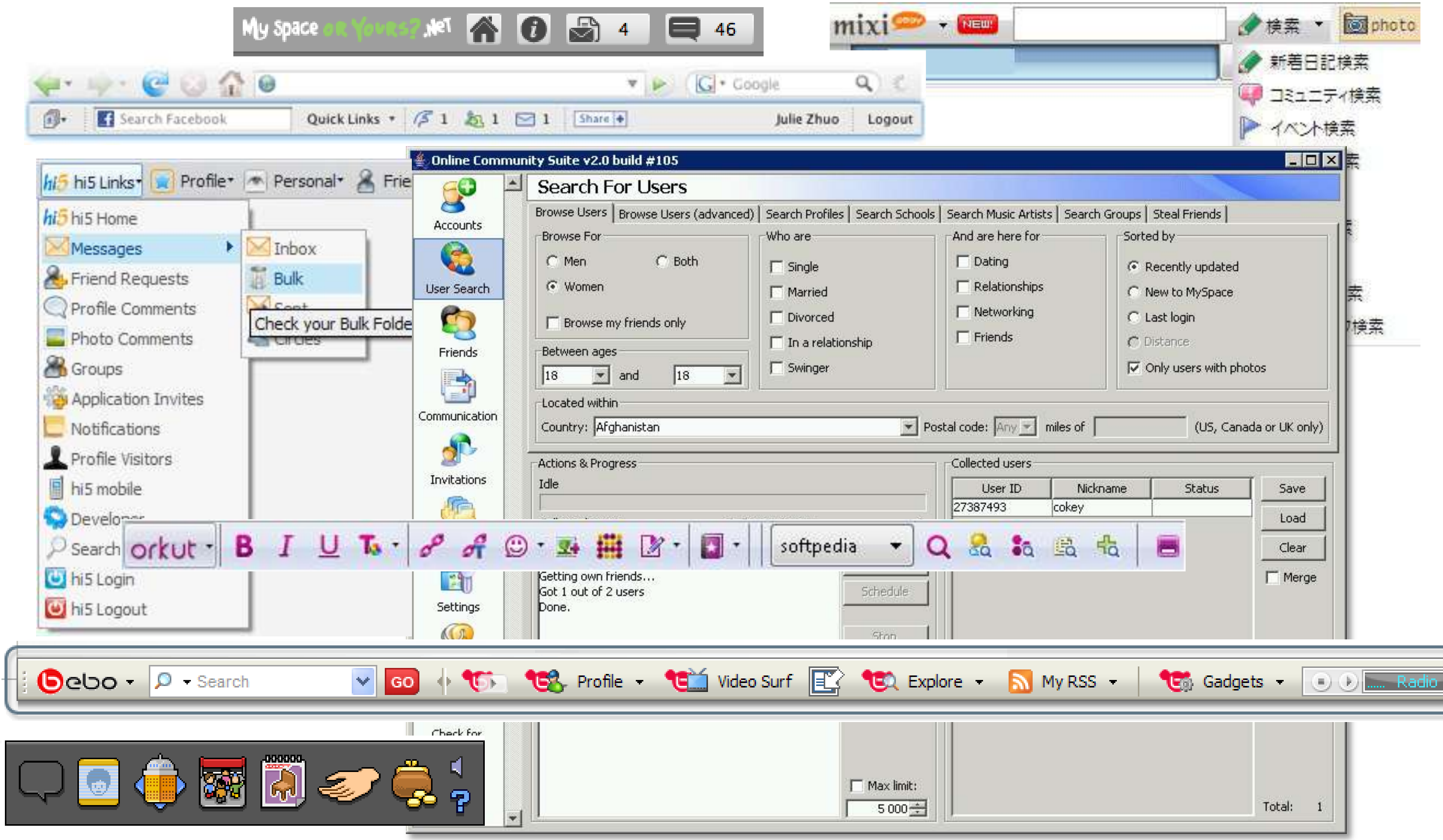
Port number: 101

Plugging in to Social Networks

- **Most popular social networking sites are Web 2.0 enabled**
  - Typically have their own framework and development languages
  - Developers can create custom tools for site integration
- **Two primary classes of tool development**
  - Browser toolbars and installable applications that maintain a constant link and communication stream with the social network site
  - In-site application “widgets” that can be installed within page content and shared amongst users when interfacing directly with the site
- **Site-specific tools already a security issue**
  - Worms that propagate through scripts embedded within site content
  - Widgets that automatically crawl accounts to retrieve personal information

DAMBALLA
Take Back Command-and-Control

Bridging Tools for Social Networking Sites



Online Community Suite v2.0 build #105

Search For Users

Browse Users | Browse Users (advanced) | Search Profiles | Search Schools | Search Music Artists | Search Groups | Steal Friends

Browse For: ○ Men ○ Both ● Women
□ Browse my friends only

Who are: □ Single □ Married □ Divorced □ In a relationship □ Swinger

And are here for: □ Dating □ Relationships □ Networking □ Friends

Sorted by: ● Recently updated ○ New to MySpace ○ Last login ○ Distance
☑ Only users with photos

Between ages: 18 and 18

Located within
Country: Afghanistan Postal code: Any miles of (US, Canada or UK only)

Actions & Progress
Idle

```
Getting own friends...
Got 1 out of 2 users
Done.
```

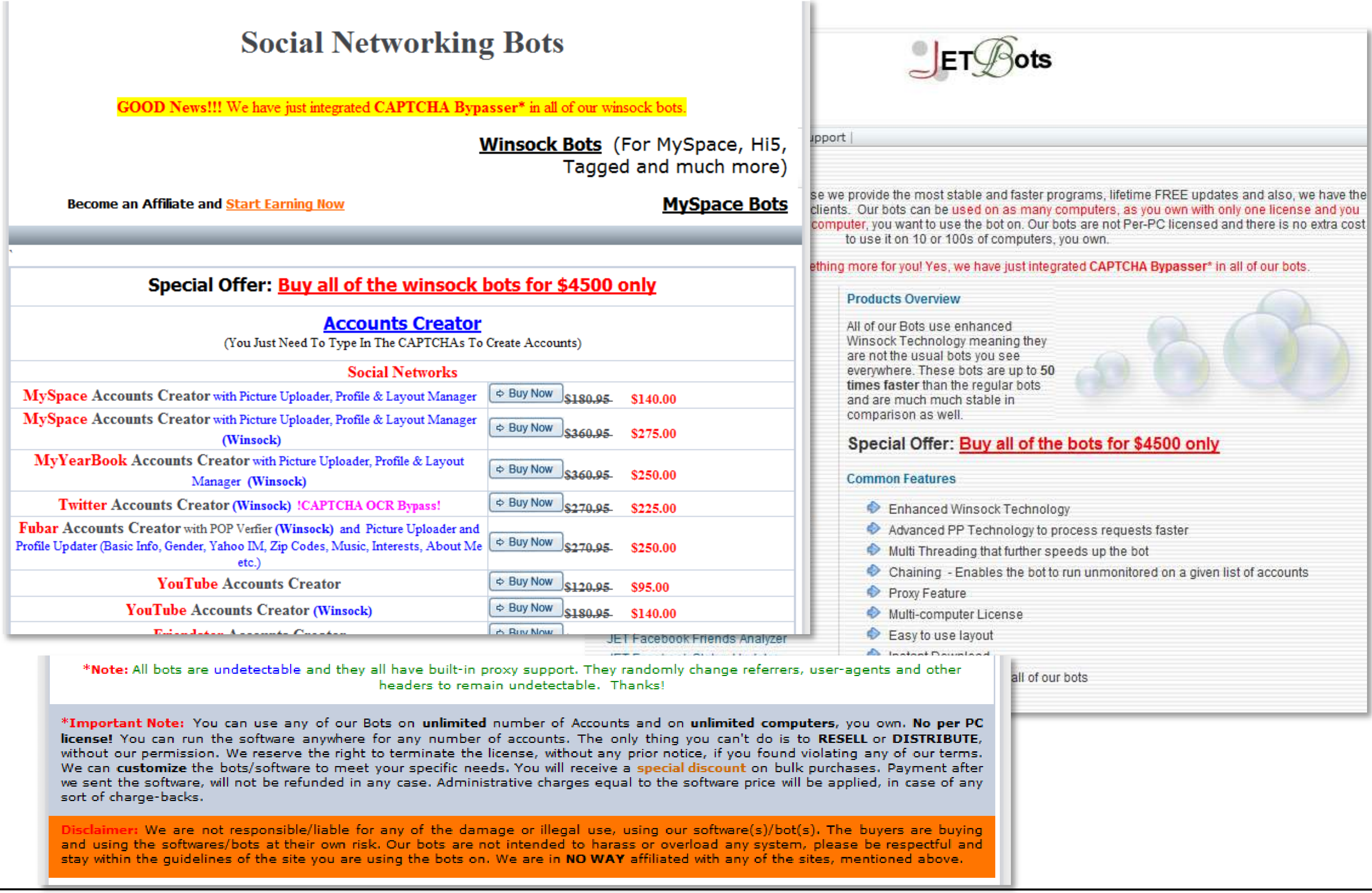
□ Max limit: 5 000

Collected users

User ID	Nickname	Status
27387493	cokey	

Total: 1

Social Networking Bots



Social Networking Bots

GOOD News!!! We have just integrated **CAPTCHA Bypasser*** in all of our winsock bots.

Winsock Bots (For MySpace, Hi5, Tagged and much more)

Become an Affiliate and Start Earning Now

MySpace Bots

Special Offer: Buy all of the winsock bots for $4500 only

Accounts Creator

(You Just Need To Type In The CAPTCHAs To Create Accounts)

Social Networks

MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager	Buy Now	~~$180.95~~	$140.00
MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)	Buy Now	~~$360.95~~	$275.00
MyYearBook Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)	Buy Now	~~$360.95~~	$250.00
Twitter Accounts Creator (Winsock) !CAPTCHA OCR Bypass!	Buy Now	~~$270.95~~	$225.00
Fubar Accounts Creator with POP Verfier (Winsock) and Picture Uploader and Profile Updater (Basic Info, Gender, Yahoo IM, Zip Codes, Music, Interests, About Me etc.)	Buy Now	~~$270.95~~	$250.00
YouTube Accounts Creator	Buy Now	~~$120.95~~	$95.00
YouTube Accounts Creator (Winsock)	Buy Now	~~$180.95~~	$140.00
Friendster Accounts Creator	Buy Now		

JET Bots

upport |

se we provide the most stable and faster programs, lifetime FREE updates and also, we have the clients. Our bots can be used on as many computers, as you own with only one license and you computer, you want to use the bot on. Our bots are not Per-PC licensed and there is no extra cost to use it on 10 or 100s of computers, you own.

ething more for you! Yes, we have just integrated **CAPTCHA Bypasser*** in all of our bots.

JET Facebook Friends Analyzer

Products Overview

All of our Bots use enhanced Winsock Technology meaning they are not the usual bots you see everywhere. These bots are up to **50 times faster** than the regular bots and are much much stable in comparison as well.

Special Offer: Buy all of the bots for $4500 only

Common Features

- Enhanced Winsock Technology
- Advanced PP Technology to process requests faster
- Multi Threading that further speeds up the bot
- Chaining - Enables the bot to run unmonitored on a given list of accounts
- Proxy Feature
- Multi-computer License
- Easy to use layout
- Instant Download

all of our bots

***Note:** All bots are undetectable and they all have built-in proxy support. They randomly change referrers, user-agents and other headers to remain undetectable. Thanks!

***Important Note:** You can use any of our Bots on **unlimited** number of Accounts and on **unlimited computers**, you own. **No per PC license!** You can run the software anywhere for any number of accounts. The only thing you can't do is to **RESELL** or **DISTRIBUTE**, without our permission. We reserve the right to terminate the license, without any prior notice, if you found violating any of our terms. We can **customize** the bots/software to meet your specific needs. You will receive a special discount on bulk purchases. Payment after we sent the software, will not be refunded in any case. Administrative charges equal to the software price will be applied, in case of any sort of charge-backs.

Disclaimer: We are not responsible/liable for any of the damage or illegal use, using our software(s)/bot(s). The buyers are buying and using the softwares/bots at their own risk. Our bots are not intended to harass or overload any system, please be respectful and stay within the guidelines of the site you are using the bots on. We are in **NO WAY** affiliated with any of the sites, mentioned above.

Behold the future…

Looking to the Future…

Social Network Groups
Coordinating Information

DDoS Attack Tools
Web & Mail Saturation

Web 2.0 Integration Tools
Automation Bridge & Toolbars

If all these “features” are combined, what do we get?

DAMBALLA

Take Back Command-and-Control

Looking to the Future...

Cyber Protest Steamroller

Social network coordinated DDoS

[redacted]

[redacted]

Community Toolkit

Combination Attack Tool

- Download the software package, install, and participate
- Social network group provides command and control instructions
- Built-in DDoS functionality (Mail, Web, and more)

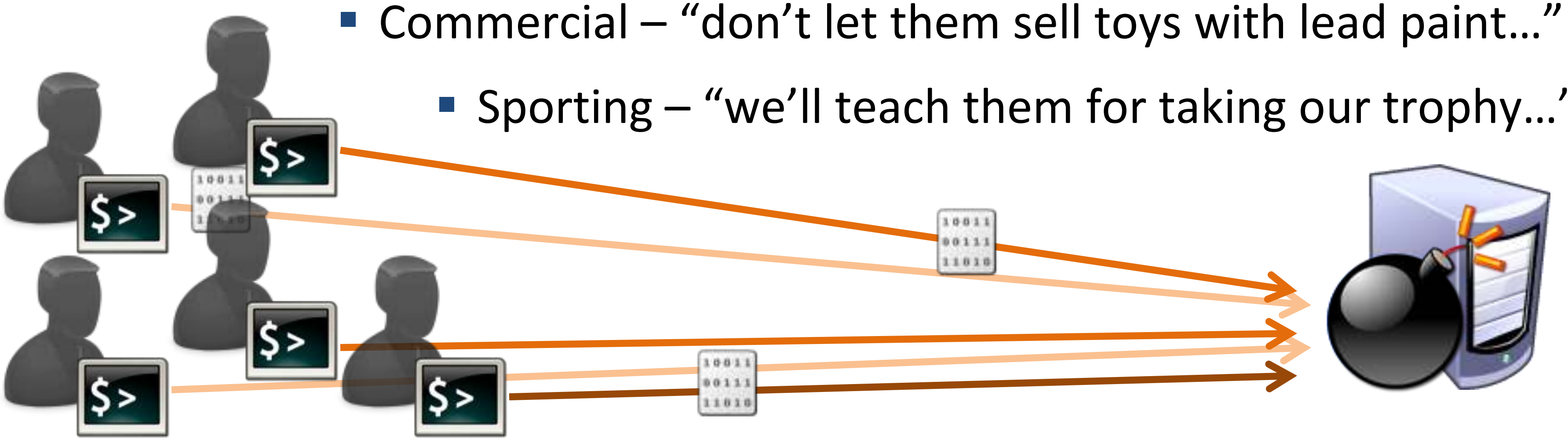
Why Would Anyone Do This?

These kinds of discussions already occur

- **Ease of participation**
  - “Donate the unused power of your computer to the cause…”
  - “Use your spare Internet bandwidth while you’re asleep…”
  - “Automatically further the cause just by installing this tool…”
- **Vagueness concerning legalities of the *protest***
  - “If it’s OK for me to send 20 emails with big attachments, why can’t I send 100, or a thousand, or even a million?”
  - “I can open 10 Web browser windows of their Web site and help prevent others from accessing the site. Why can’t I open 32,000 virtual windows?”
  - “Whenever I type ##### on their site it slows down for 5 seconds. Why can’t I send #### continuously all day tomorrow?”

Who are the Likely Targets?

- **Group creation and "mob" attacks will likely driven by an increasingly broad spectrum of issues – e.g.**
  - Political – "oppose the military junta in…"
  - Ideological – "eating meat is bad, close down XXX turkey farm…"
  - Theological – "Jedi is not a legitimate religion, don't let them recruit…"
  - Local – "stop the invasion of XXX within our community…"
    - Commercial – "don't let them sell toys with lead paint…"
      - Sporting – "we'll teach them for taking our trophy…"



Looking Further in to the Future…

Why limit the tool to a single group or community?

Beyond Web and Mail DDoS, what other capabilities could further an online protest?

Community Toolkit

Combination Attack Tool

Community Capabilities

- Automatically contribute tool access to each subscribed group.
- “Time-share” spare computer capacity with enabled groups.

Expanded Protest Features

- Automatically leave defamatory messages, disinformation and comments in popular forums and blogs.
- Hook other social network sites and communication channels to recruit or DoS – e.g. LinkedIn and Twitter.
- Integrate VoIP functions to leave voice messages and DoS telephony systems.

DAMBALLA
Take Back Command-and-Control

Tangential Community Attack Platforms

- **Social Network integration tools already porting over to Smartphone's…**
- **Additional attack vectors:**
  - SMS and MMS flooding capabilities
  - Voice and voice mailbox denial of service
  - Proximity-based WiFi DoS and exploitation

- Community engagement models
  - Make use of free same-provider calls
  - "Donate $20 of calls and SMS per month to the cause"
  - "Everyone dial 911 at the same time!"

Attack Ramifications

- **Economic Exhaustion**
  - Prevent customers/clients from accessing Internet services
  - Swamp internal systems and disrupt business processes
  - Drive up hosting and cloud costs
- **Public disinformation**
  - Defamatory information and brand erosion
- **Flooding of non-Internet systems**
  - Harassment of business executives
  - Unreachable telephony systems and emergency services

Dealing with the threat

Protection Strategies

- **The threat is as complex as it is broad**
  - No single protection solution will curtail the threat
- **Instead, measures need to be taken within:**
  - the Social Network site
  - the targeted organization
  - organizations whose employees can contribute to attacks
  - the ISP/Telco infrastructure routing the attack traffic
  - the abused intermediary sites that may host defamatory material

Social Network Sites

- Social Network sites bear the greatest burden in protecting organizations from being targeted by their members
- Most sites already have exhaustive user agreements that prohibit the discussion and participation of these attacks
  - Unfortunately, they appear to be rarely enforced…

Deep Content Inspection

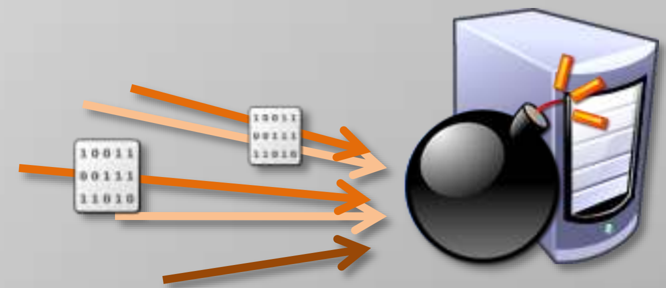
Monitoring Group Discussion Content
Identification of malicious code, attack coordination, and breach of site usage agreements

Content Filtering

Removal or Sanitization of Content
Filtering of offending content and discussions

Enterprise Protection

Stopping External Attacks



Mail Filtering

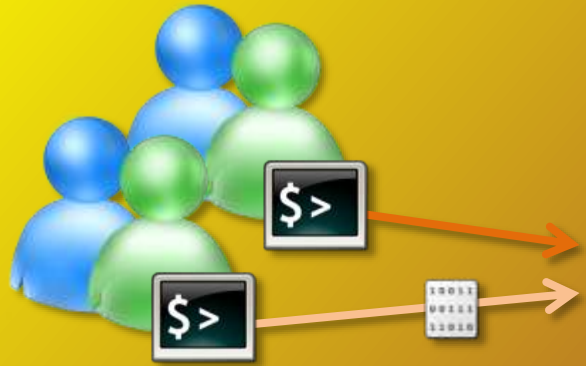
Deep Content Inspection

IPS

Firewall

Anti-DoS

Preventing Attack Participation



Mail Filtering

Anti-Virus

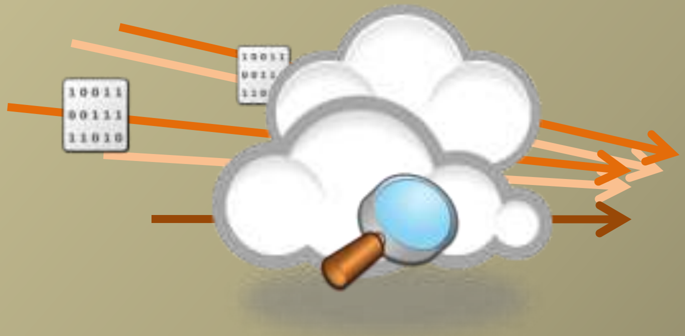
IPS

Firewall

Application Control

Intermediaries

ISP's & Telecom Operators



- Mail Filtering
- IPS
- Deep Content Inspection
- ADS
- Flood Control
- Firewall

Forum Owners & Blog Operators

- Anti-Spam
- Deep Content Inspection

Command & Control

- **Critical interception point…
… the CnC**
- **Leash through which cyber-protesting tools are managed and coordinated**
- **Weakest point for shutting down a cyber-protest**
  - Easiest vector for dealing with the threat
  - Within the capabilities of most enterprises

Conclusions

- **Cyber-protesting, get used to it…**
  - Hacktivism and cyber-protesting are different and diverging
- **Tools are growing in sophistication**
  - Easier to become involved in a protest
  - Ramifications are fuzzy…
- **Are you a victim or an enabler?**
  - Receiving end of an attack
  - Facilitating an attack on others

Thank You!

22nd ANNUAL FIRST CONFERENCE MIAMI
JUNE 13-18, 2010

Gunter Ollmann - VP of Research

gollmann@damballa.com
Blog - http://blog.damballa.com
Blog - http://technicalinfodotnet.blogspot.com

Further Reading

- **The Opt-in Botnet Generation**
  - http://www.damballa.com/downloads/r_pubs/Opt-In_Botnets.pdf
- **The Botnet vs. Malware Relationship**
  - http://www.damballa.com/downloads/d_pubs/WP_Botnet_vs_Malware.pdf