



Malware on a Mission

Amir Fouda
Senior Research Engineer
CA-HCL



Politics and Internet Security



- The world of politics has visited the world of Internet Security on many occasions
- Politically motivated cyber attacks are becoming more common
- Coinciding with real world political events
- Instigated by politically motivated malware authors and hacktivists (hacker + activist).



What's their agenda?



1. Malware distribution
2. Cyber espionage
3. Political expression
4. Disruption



1. Malware distribution

- Political news headlines means an opportunity for malware authors to exploit users
- War
- Civil disorder
- Elections
- Political tensions, incidents and scandals.



Delivering malware to the masses



- Email the more popular means of delivery
- Spammed to email accounts with information about an important political situation.
- Some malware families that have used political content in their spam campaigns:
 - Sober, Sintun, Pecoan, Luder (aka the “Storm worm”), Bancos, Banker, and Waledac.



Popular Issues



Political issue

U.S Politics and the Bush Administration

2008 U.S Presidential Election

War in Iraq

Death of Saddam Hussein

Israeli-Palestinian conflict

Tensions between U.S. and Iran

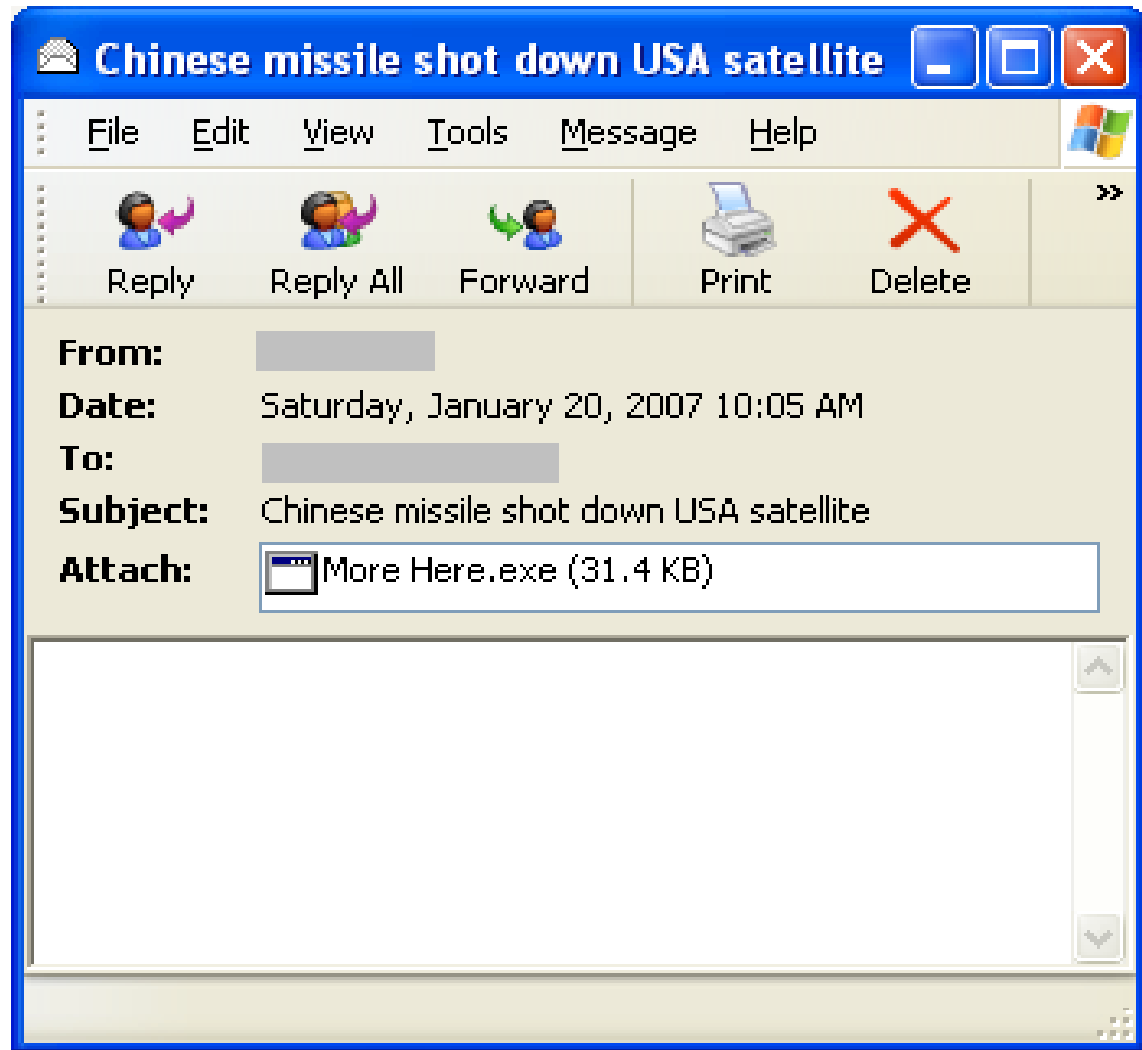
Tibet's struggle with China



January 11, 2007



“Storm worm” spam campaign, less than two weeks after China shot down one of its weather satellites in a missile test.



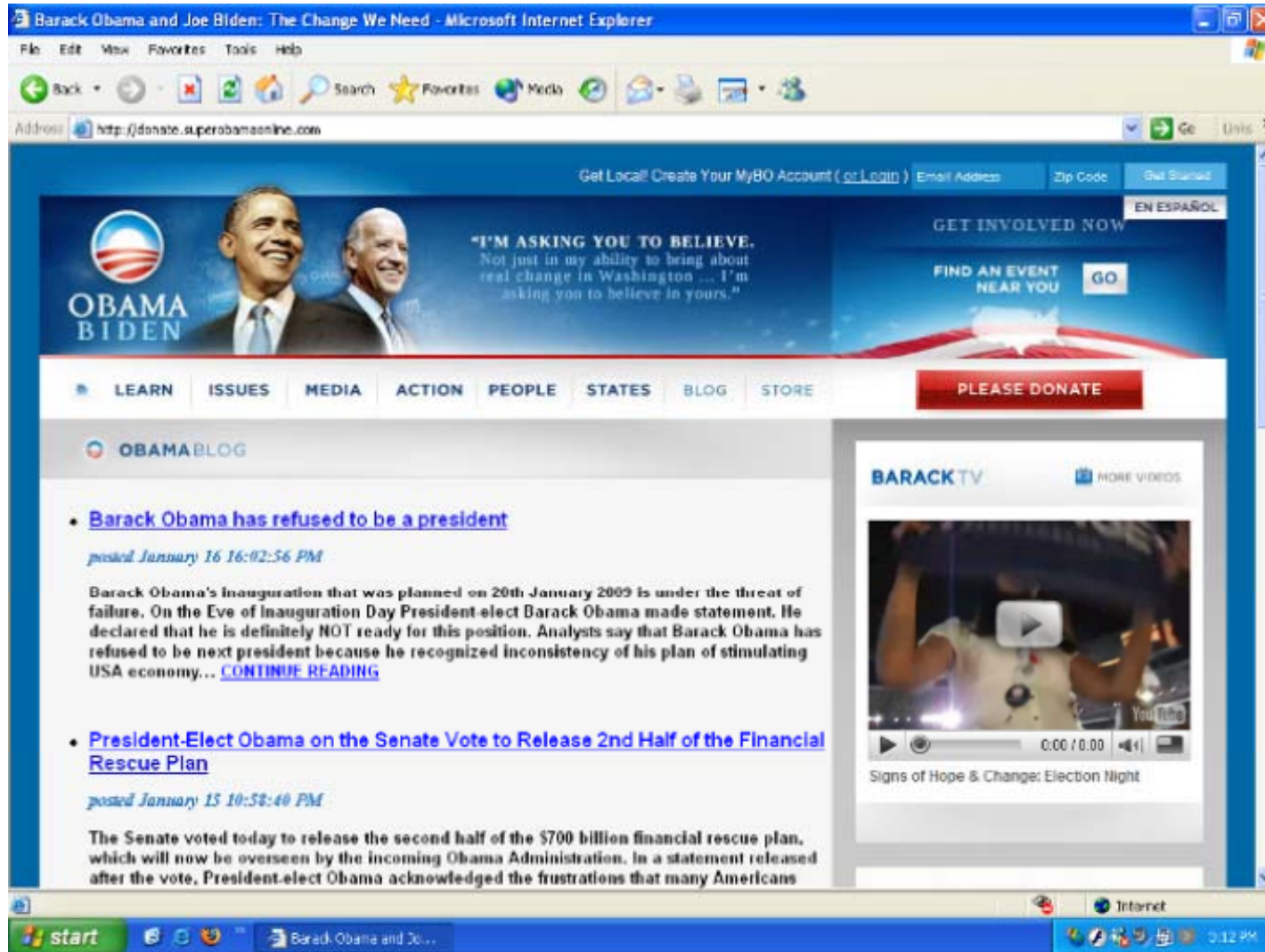
January 16, 2009



Days before Barack Obama's Inauguration ceremony, to be held on the 20th of January, Waledac spam campaign



Fake Obama website



Targeted Attacks



- Malware spammed only to specific individuals or groups
- Carefully crafted, seemingly legitimate, personalized looking emails that would appeal to the recipient.
- Malware often attached to email as an CHM, PDF, DOC, XLS, or PPT file



Targeted Attacks



- Just some of the government/political groups and organizations targeted in the past:
 - Pro-Tibetan and Uyghur groups and supporters
 - U.S Government agencies
 - UK Government departments
 - German ministry of Interior employees
 - Australian diplomats



Tibet Targeted Email



From: "Tenzin Taklha " <EMAIL ADDRESS>
Subject: Message on Burmese Demonstrations

Dear Friends & Colleagues, Please find enclosed a message from His Holiness the Dalai Lama in support of the recent pro-democracy demonstrations taking place in Burma. This is for your information and can be distributed as you see fit. Best wishes.

Tenzin Taklha
Joint Secretary
Office of His Holiness the Dalai Lama
<REMOVED>

INDIA

Ph.: +91 <REMOVED>

Fax: +91 <REMOVED>

www.dalailama.com



Tibet Targeted Attacks (con't..)



The screenshot displays two overlapping windows. The top window is titled "HTML Help" and contains the text "Free Tibet needs your support" in teal. Below this text is a black and white photograph of a young Tibetan girl with traditional headwear. To the right of the photo, the text reads "JOIN FREE TIBET TODAY!" in teal and "ADD YOUR VOICE TO THE CALL FOR CHANGE!" in red. The bottom window is titled "stand up for Tibet this summer.doc - Microsoft Word". The Word window shows a document with the following text:

My dear brothers and sisters:

Who will stand up for Tibet this summer? Who will inspire the entire world with their courage and character? Who will show us all that freedom of expression, religion and assembly truly matter?

If you are competing at the Beijing Summer Games, it could be you.

You have probably seen Tibetans and many world citizens protesting the Chinese government's use of the Olympic Games to whitewash its image and legitimize its claims on Tibet. Yet as an athlete who has spent a lifetime preparing for these Games, you may be concerned that they have seen so much protest.

Tibet Targeted Attacks (con't..)



China's Tibet.pdf - Adobe Reader

File Edit View Document Tools Window Help

1 / 3 100% Find

ROWMAN & LITTLEFIELD
1-800-462-6420 ♦ www.rowmanlittlefield.com

Order today and SAVE

CHINA'S TIBET?
Autonomy or Assimilation
By Warren W. Smith

CHINA'S TIBET?
AUTONOMY OR ASSIMILATION

Microsoft PowerPoint - [TIBET, A COUNTRY IN EXILE]

File Edit View Insert Format Tools Slide Show Window Help

Type a question for help

75% Times New Roman 24 Design New Slide

TIBET, A COUNTRY IN EXILE



Tibet Targeted Attacks (con't)



File name	Vulnerability
Petition to help Tibet.doc	CVE-2006-2492
Photos from 1st Europe Tibetan Congress.ppt	CVE-2008-0000
burma_april_9_torch_actions_final.xls	CVE-2008-0116
Free Tibet Olympics Protest on Mount Everest.doc	CVE-2008-2244
Tibet 50th anniversary of fighting against violence.doc	CVE-2008-3005
hhdl burma_001.doc	CVE-2008-4841



2. Cyber espionage



- The primary goal of these targeted attacks is to install a Trojan backdoor on the recipients system.
- Some of the Remote Access Trojans (RAT) spammed in the Pro-Tibetan Targeted attacks include:
 - PcClient
 - Poison Ivy
 - Gh0st RAT

Cyber espionage



- Gives attacker full control of the system, allowing them to:
 - Browse through files and directories
 - Capture keystrokes
 - Take screenshots
 - Capture video and audio
 - Download files



Gh0st RAT



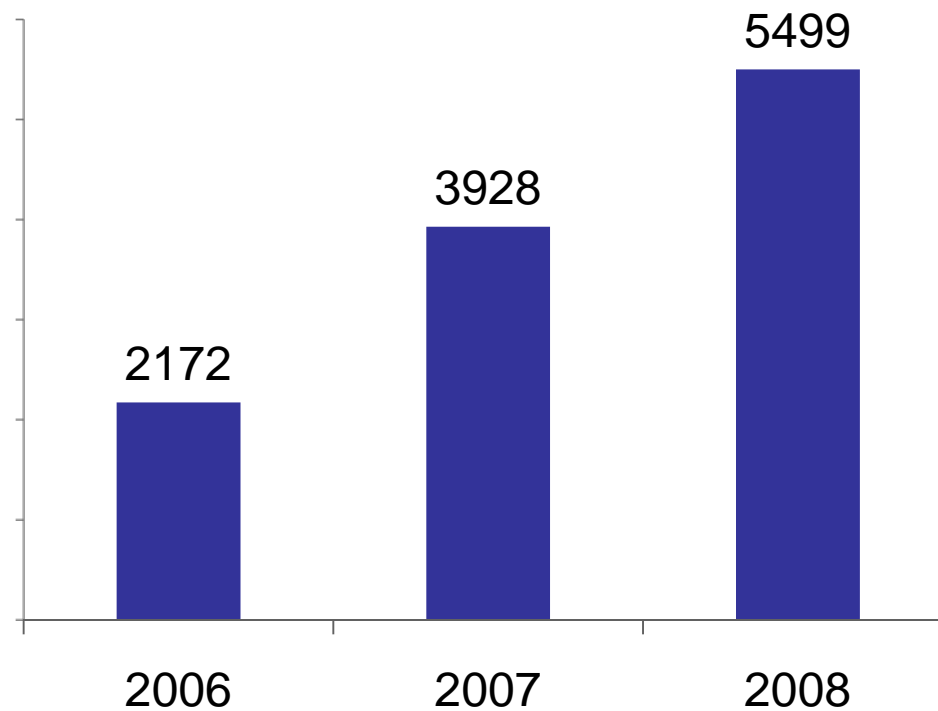
ID	WAN	LAN	Computer/User Name	OS Version	CPU	Ping	Camera
10	192	250	Victim	XP SP0 (Build 2600)	2826MHz	20	N/A



Cyber espionage



- Department of Homeland Security (April 2009):
 - Known breaches of U.S. government computers with malicious software



GhostNet revealed



- In March 2009, a report was published by the Information Warfare monitor, “Tracking GhostNet: Investigating a Cyber Espionage Network”
 - <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>
- A network of 1,295 infected computers in 103 countries
- 30% of those infected are high value diplomatic, political, economic and military targets



GhostNet findings



- While investigating, several confidential documents were observed being uploaded to a control server from the computer network of the Dalai Lama's private office
- Attackers can command an infected host to download additional Remote access Trojans, such as Gh0st RAT, onto the system.



3. Political expression



- A small number of malware families containing some sort of political message have appeared over the years.
- Communicating the creators political agenda to the compromised user via various means:
 - A message dialog box
 - A message in a dropped text file
 - An image on the desktop
 - Through the web browser (HTML file or website)
 - Email



Political expression (con't..)



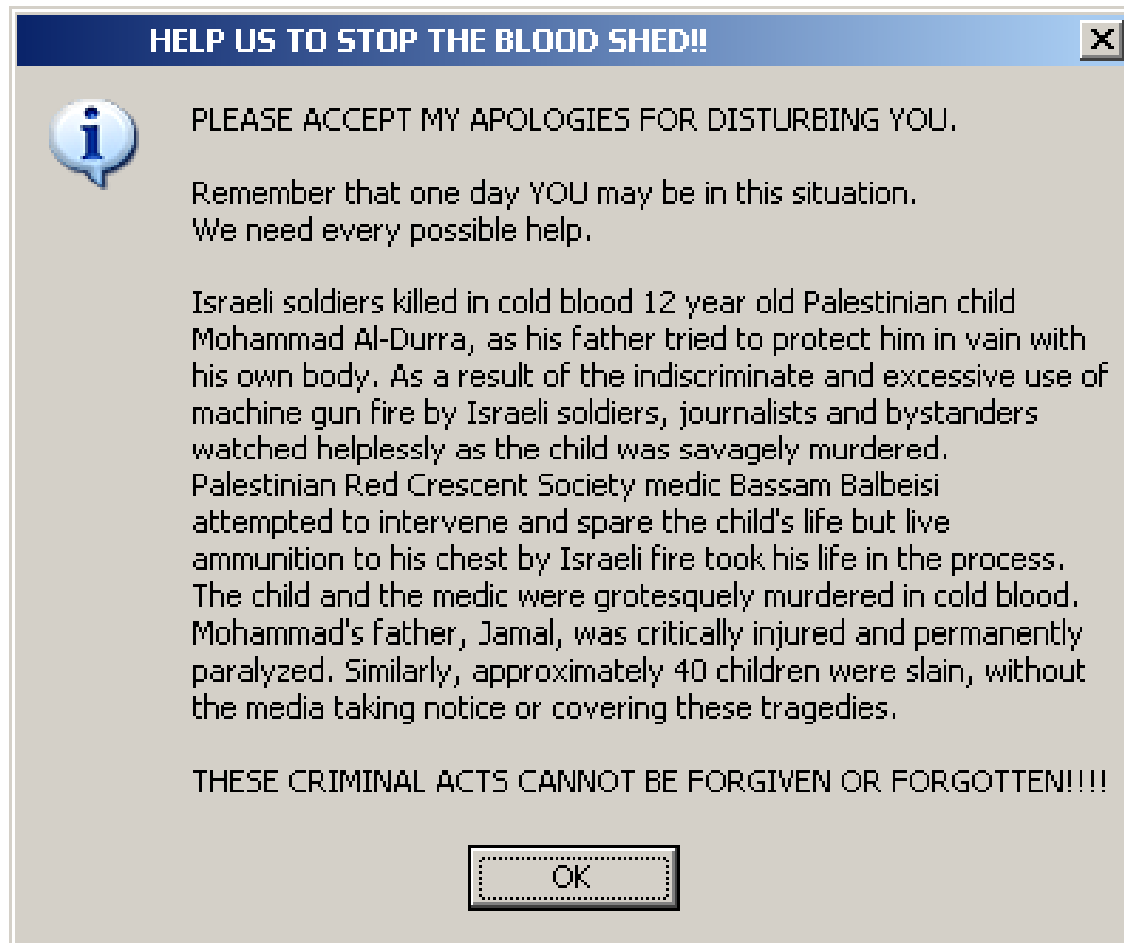
- Communicating the authors:
 - Nationalism
 - Protests over a particular event
 - Propaganda
 - Distaste for a particular nation, political figure or policy
 - Loyalty to a specific cause or political figure
 - Reminder about a certain political situation

Politically motivated malware



- 1989: WANK worm – Worm against Nuclear Killers
- 1990, “June 4”(also known as “Beijing” or “Bloody”), a boot sector Virus, displayed the message “*Bloody! Jun. 4, 1989*”
 - June 4, 1989: Date of the "Tiananmen Square" protests in Beijing China.
- Years to follow, malware communicating political messages appeared, majority being worms.

Some examples



VBS/Staple.A
(July 2001)



Win32/Etap
(March 2002)



Some examples (con't..)



*Battle for
Moscow*

БИТВА ЗА МОСКВУ:

*German
Sterligov
against
Atheists*

Герман Стерлигов против урючья.

*Our return
Address*

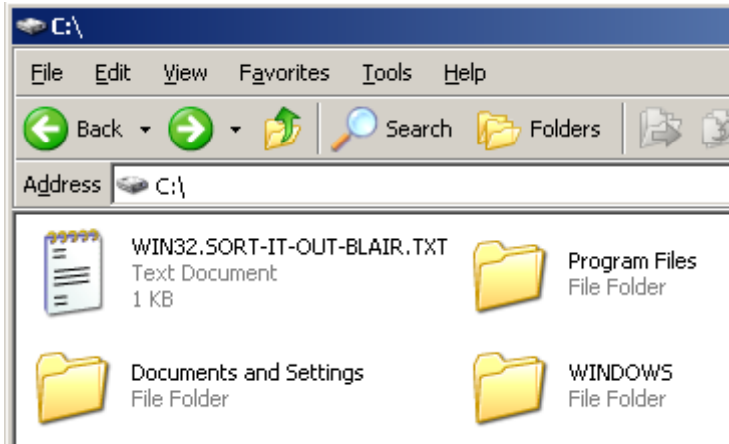
Наш обратный адрес: www.sterligov.ru



Win32/SEXER.E
(Nov 2003)



Some examples (con't..)



Win32/Blare.A
(Sep 2003)



Win32/Cone.B
(March 2004)



Win32/Sober.H (June 2004)



Bankrott des Gesundheitswesens durc...

File Edit View Tools Message Help

Reply Reply All Forward Print Delete

From: [redacted]
Date: Monday, June 14, 2004 7:48 PM
To: [redacted]
Subject: Bankrott des Gesundheitswesens durch Auslaender!

Die verschwiegenen Gruende der Kostenexplosion:

Unlaengst aeusserte der Bayerischen Hausaerzte Wolfgang Hoppenthaller auslaendischer 'Gesundheitstouristen' m Angehoerigen und Freun uns die aertzliche Verso Der Schaden sei laut Dr Hoppenthaller 'bestimmt Defizit der Krankenkass

Mehr fuer Auslaender als fuer Deuts

File Edit View Tools Message Help

Reply Reply All Forward Print

From: [redacted]
Date: Wednesday, June 23, 2004 1:56 AM
To: [redacted]
Subject: Mehr fuer Auslaender als fuer Deuts

Lese selbst:
http://www.dsz-verlag.de/Artikel_04/NZ15_1.html

Libanesen in Berlin

File Edit View Tools Message Help

Reply Reply All Forward Print Delete

From: [redacted]
Date: Wednesday, June 16, 2004 12:01 AM
To: [redacted]
Subject: Libanesen in Berlin

Habe eben im Fernsehen einen Bericht gesehen, in dem klar hervorging, dass libanesische und kurdische Moslems in Berlin die Drogenszene und teilweise sogar das Rotlicht-Milieu beherrschen. Der Clou an der Geschichte ist jedoch, dass die Libanesen, die in kriminelle Aktivitaeten verwickelt und Millionen scheffeln, ebenfalls vor dem Sozialamt erscheinen um ihre Sozialhilfe



Some examples (con't..)



Win32/Deadcode.A
(Feb 2005)

Website defacements



- Website defacements have also been used by hacktivists to communicate their political message.
- Online vandalism
- Attracts attention of regular media, helping spread the hacktivists message further



Website defacements



- Reports of politically motivated website defacements are particularly high during or after times of military conflict
- “Patriotic hackers”, loyal to one sides cause, target websites of their perceived enemy.
- More often then not, owners of these targeted websites have nothing to do with the conflict.



Website defacement incidents



- China-US Aircraft collision (April 2001)
 - Hacktivists from both sides defaced a number of websites, replacing their content with pro-Chinese, anti-U.S. or Pro-American messages
- War in Iraq (March 2003):
 - Over 10,000 websites defaced by various hacker groups, many protesting against the war in Iraq.

Website defacement incidents



- Prophet Mohamed Cartoons controversy (Feb 2006):
 - Thousands of Danish and western websites defaced with messages of violence and calls for boycotts of Danish products.
- Israel–Palestinian conflict (Dec 2008/Jan 2009)
 - Over 10,000 websites defaced with Pro-Palestinian, anti-Israeli and anti-U.S. messages.



Website defacement snippets



4. Disruption



- Distributed Denial-of-Service (DDoS) attacks against targeted websites are used quite often by hacktivists.
- Knocking out the targeted site for periods at a time by overloading them with traffic.

DDoS Attacks



- April 2007: Estonian DDoS attacks
- July 2008: Georgian DDoS attacks
- June 2009: Iranian Pro-Ahmadinejad DDoS attacks
- August 2009: Twitter DDoS attacks
- September 2009: Australian Government DDoS



How are these DDoS attacks launched?



- Existing botnets, leased by cyber criminals at a price
- Malware authors launch Denial-of-Service attacks through their malware
- Use of DDoS tools, webpage refresher tools, multiple IFrame loading scripts, perl scripts, etc..

DoS payload



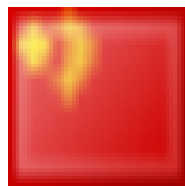
Malware	Target sites	Year
Win32/Yaha worm	Pakistan government sites	2002
Win32/Blare.A worm	Official site of UK prime minister	2003
Win32/Cone.B worm	Islamic Republic News agency	2004
Win32/Zafi worm	Republic of Hungary Parliament	2004
Win32/Maslan.C worm	Chechen rebel movement	2004
Win32/Robknot worm	Israeli government and Indonesian Tourism site	2005
Win32/Mydoom.BT worm	U.S. and South Korean government and Financial sites	2009

People Power



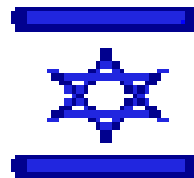
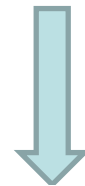
- At times, hacktivists look to recruit average Internet users
- Providing them with customized DDoS tools.

hackcnn.com



antiCnn

help-israel-win.org



Patriot
Patriot
The Patriots





antiCnn DDoS Tool



*Red Flag
Action – Use
rationality to
show your
patriotism*

Target

目标: www.cnn.com

龙啸

挂机

退出





You too Can Contribute to the Effort

Français | Português | Русский | Español | English | עברית

Home Page | Instructions |  Download

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:

- [Social networks link terrorists](#)
- [Israel vs. Palestine - which side do you prefer survey](#)
- [Reciprocal attacks on the web](#)
between Israel & Hamas

Status

8118 people have joined us so far.

You can contact us here: helpisraelwin@gmail.com

SHARE 

Social Networks, the Hacktivists friend




- After the re-election of Ahmadinejad as Iranian President, many Iranians went to the streets in Protest.
- And many participated in DDoS attacks against Pro-Ahmadinejad websites
- DIY DDoS tools, webpage refresher tools, multiple IFrame loading scripts were shared amongst activists through forums and social networking sites.


DDoS tools on Twitter and webforums



Help for DDoS: [redacted] s

Dear friends,
We are two Java developers from Australia and have created this program primarily to overload Iranian websites: [Home](#) ([redacted])

 Click this bar to view the full image.



Twitter Help

Used

- [http://keyfarnews.ir\[63.3152058\]](http://keyfarnews.ir[63.3152058]) sleeping
- [http://www.irannews.com\[7.13106528\]](http://www.irannews.com[7.13106528]) working /
- [http://www.ima.com\[15.30127058\]](http://www.ima.com[15.30127058]) sleeping

@s[redacted] i I created a small program to oveload liar/spy websites of the gov of Iran [http://\[redacted\]](#) #iranelection # [redacted]

1:47 PM Jun 27th from Power Twitter



DDoS tool



The screenshot shows a DDoS tool interface with a list of targets and a real-time traffic graph. The targets are:

- 1. Fars News.txt
- 1. Gerdab.txt 466.9KB (URL: 258 0% error)
- 2. IRNA.txt 7.58MB (URL: 113 84% error)
- 2. Raja News.txt 467.6KB (URL: 35 0% error)
- 3. Keyhan.txt 4.73MB (URL: 81 27% error)
- 3. Tabnak.COM.txt
- 4. All URLs.txt

At the bottom, a green bar displays the following statistics: Hit:20061 | Received:13.21MB | Speed:9.4KB/s | Limit:10.0MB/s



Prevention



- Socially engineered emails:
 - User education
- Cyber espionage:
 - Protect highly confidential information, audit and log network activity, behavioral monitors

Prevention (con't..)



- Website defacements
 - Secure web servers
- DDoS attacks
 - Hard to defend against, but Rate-based Intrusion Prevention System (IPS) may help
- Peace on Earth?



Conclusion



- Politically motivated cyber threats will continue to pose a threat to political and government organizations
- The nature of the Internet means more people can participate in these attacks from the comfort of their own homes.
- Advances such as Social networking sites means hacktivists will use it to their advantage
- The average user will play a bigger role





MISSION OVER

Questions?

