The Opt-in Social Protesting Botnet

DAMBALLA
Take Back Command-and-Control

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

5/31/2010 FIRST 2010 - The Opt-in Social Protesting Botnet – Gunter Ollmann
• 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/
• 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
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**

<table>
<thead>
<tr>
<th>DATE</th>
<th>ATTACKER</th>
<th>FLAGS</th>
<th>DOMAIN</th>
<th>OS</th>
<th>VIEW</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>krommeweg1.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>zjosque.wimdesign.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>wimcomputers.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>wimwebsitesolutions.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>birdmanproduction.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>osv95.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>dekomiezen.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>jrfp.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>cbatie.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>aa-consultancy.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>totalrecreatief.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>fotoposters.ru</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>golfmints.com</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>tiel-pekt-uit.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>tiel-centraal.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>restaurant-rembrandt.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>shoefairtiel.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>shoefair.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>babyzaak-riando.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>microport-int.com</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>ik-laat-je-dansen.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>lightbox.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>cafeedewaterpoort.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>franchiseadviseur.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>web-products.nl</td>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>2008/08/25</td>
<td>nEt^DeViL</td>
<td>H M</td>
<td>onzepassie.nl</td>
<td>Linux</td>
<td></td>
</tr>
</tbody>
</table>

Hundreds of Dutch web sites hacked by Islamic hackers
- Mass defacement
- August 2008
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

<table>
<thead>
<tr>
<th>Location</th>
<th>Result</th>
<th>Min. RTT</th>
<th>Avg. RTT</th>
<th>Max. RTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Florida, U.S.A.</td>
<td>Okay</td>
<td>59.4</td>
<td>59.9</td>
<td>60.5</td>
</tr>
<tr>
<td>Amsterdam, Netherlands</td>
<td>Okay</td>
<td>149.3</td>
<td>164.6</td>
<td>278.4</td>
</tr>
<tr>
<td>Melbourne, Australia</td>
<td>Okay</td>
<td>170.9</td>
<td>174.5</td>
<td>175.0</td>
</tr>
<tr>
<td>Singapore, Singapore</td>
<td>Okay</td>
<td>208.5</td>
<td>214.0</td>
<td>229.2</td>
</tr>
<tr>
<td>New York, U.S.A.</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amsterdam, Netherlands</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austin, U.S.A.</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>London, United Kingdom</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stockholm, Sweden</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cologne, Germany</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chicago, U.S.A.</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austin, U.S.A.</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amsterdam, Netherlands</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Krakow, Poland</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paris, France</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copenhagen, Denmark</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>San Francisco, U.S.A.</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vancouver, Canada</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Madrid, Spain</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shanghai, China</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lille, France</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zurich, Switzerland</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Munchen, Germany</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Milan, Italy</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Johannesburg, South Africa</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Porto Alege, Brazil</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sydney, Australia</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mumbai, India</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Santa Clara, U.S.A.</td>
<td>Packets lost (100%)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Citizen-based hactivism against internal political sites
  – Iran elections, June 2009

Overload Khamenei’s website  
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  
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!

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

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 Needham, our sustainable seafood markets expert, to learn more about Greenpeace’s campaign to persuade 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!
Protesting for anyone...
• 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.

<table>
<thead>
<tr>
<th>Site</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>400,000,000</td>
</tr>
<tr>
<td>MySpace</td>
<td>130,000,000</td>
</tr>
<tr>
<td>Skyrock</td>
<td>22,000,000</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>65,000,000</td>
</tr>
<tr>
<td>Orkut</td>
<td>100,000,000</td>
</tr>
<tr>
<td>Bebo</td>
<td>40,000,000</td>
</tr>
<tr>
<td>Hi5</td>
<td>80,000,000</td>
</tr>
<tr>
<td>Nexopia</td>
<td>1,400,000</td>
</tr>
<tr>
<td>Mixi</td>
<td>24,000,000</td>
</tr>
<tr>
<td>Vkontakte</td>
<td>75,000,000</td>
</tr>
<tr>
<td>Netlog</td>
<td>62,000,000</td>
</tr>
<tr>
<td>Habbo</td>
<td>162,000,000</td>
</tr>
<tr>
<td>Friendster</td>
<td>115,000,000</td>
</tr>
</tbody>
</table>

- Huge numbers of online members
- Almost all sites have the ability to create new “groups” or “forums” for discussion and information sharing
• Example: Military actions in the Gaza territory led to new social network groups supporting the opposing sides (Jan 2009)
Iran Protesting – June 2009

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 leave this. Please redigg everywhere! We need your help!

2 Comments

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

ALL PEOPLE AROUND THE WORLD ARE INVITED...help Iranians to cam back their simply click on the link and it opens the site in new tab. it will not stop you from brow there are the links:
1- http://www.pagereboot.com/?url=http://fars.i& ...
2- http://www.pagereboot.com/?url=http://www.farsnews ...
3- http://www.pagereboot.com/?url=http://iranews.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.itib.ir/ ...
8- http://www.pagereboot.com/?url=http://www.itibnews ...

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 an Youtube, Twitter, Facebook, etc. If you have any contacts in Iran, tell them immediately.
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.
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”

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
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
Common network DDoS testing tool
1. Community members download the attack tool
2. At a specified date & time they launch their attack
3. Combined volume of attack traffic causes the target to stop functioning

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

- Easy to use (and create)
  - “Point and shoot”
  - Regionalization of tools
  - Themed versions

Tool developed in China to target CNN.com in response to CNN’s coverage of the Olympic torch protests.
• 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
Bridging Tools for Social Networking Sites
Social Networking Bots

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

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

MySpace Bots

Social Networking

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

Social Networks

MySpace Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)

Buy Now $180.05

$140.00

MyYearBook Accounts Creator with Picture Uploader, Profile & Layout Manager (Winsock)

Buy Now $180.05

$275.00

Twitter Accounts Creator (Winsock) / CAPTCHA OCR Bypass!

Buy Now $160.05

$225.00

Fubiar Accounts Creator with POP Verifier (Winsock) and Picture Uploader and Profile Updater (Basic Info, Gender, Yahoo IM, Zip Codes, Music, Interests, About Me etc.)

Buy Now $170.05

$250.00

YouTube Accounts Creator

Buy Now $170.05

$95.00

Facebook Accounts Creator

Buy Now $170.05

$140.00

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

*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 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 software/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...

Figure 1.0 - The Opt-In Social Protesting Botnet
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?

5/31/2010

FIRST 2010 - The Opt-in Social Protesting Botnet
Cyber Protest Steamroller
Social network coordinated DDoS

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?

- **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...

Community Toolkit
Combination Attack Tool

Why limit the tool to a single group or community?

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

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

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.
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
• 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...

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

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
- Deep Content Inspection
- Flood Control
- IPS
- ADS
- 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!

Gunter Ollmann - VP of Research

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

All images copyright their respective authors
• The Opt-in Botnet Generation

• The Botnet vs. Malware Relationship