The Opt-In Botnet Generation

Social Networks, Hacktivism and Centrally-Controlled Protesting

By Gunter Ollmann, VP of Research, Damballa

Introduction

As businesses and governments have moved their presence online, protesting and other public forms of disaffection against them have followed. Growing numbers of people have been motivated to take up the cyber-equivalents of protest placards, highway sit-downs and Molotov cocktails.

The last few years have shown a steady increase in the sophistication of the tools and tactics the disaffected use online. Social networking applications, Web 2.0 technologies and the general availability of what can best be described as "military grade" cyber attack tools make it a trivial task for protestors to launch crippling attacks from anywhere around the world.

The massive adoption of social networking portals and micro-blogging services in turn created a new generation of centralized Command-and-Control (CnC) capabilities that quickly and easily organize protests for international participants from all walks of life. The simplicity with which these technologies can be leveraged for attack coordination against governments and commercial organizations cannot be underestimated.

A second generation of cyber-protesting tools has emerged, encompassing a disturbing blend of criminal technology and activist enthusiasm. A growing number of movements are asking their members to deliberately install botnets on their hosts and within their networks in order to participate in more sophisticated and effecting cyber-protests.

Botnets have always been considered a severe threat that removes PCs and servers from IT control. However, botnet compromises have always come from the accidental and unknowing installation of bot malware. The purposeful and intentional acceptance of bot malware, however laudable the cause, presents a dangerous challenge to any organization concerned about maintaining control over network assets and demonstrating proper fiduciary responsibility.

In short, the introduction of social networking CnC and an increasingly diverse range of motivations and common-cause group memberships is opening the doors to new cyber-protesting possibilities – and to criminal misappropriation of hacktivist botnets. This whitepaper examines the evolutionary path of opt-in botnets, including how tactics have changed, why anyone would willingly choose to join a botnet, and what activist botnets mean to organizations that find themselves both victims and enablers of a botnet-driven attack.

Hacktivism

The term "hacktivism" has often been used as a blanket description for the nonviolent use of illegal or legally ambiguous cyber-attack tools in pursuit of political ends. By way of definition:

> *The act of "black hat" hacking that is not specifically motivated by malice, curiosity or criminal intent, but for political purposes. This may include altering the content of a website (defacement), or preventing or inhibiting communication (such as through a denial of service attack). This term describes motive only, as the techniques employed are similar or identical to those of crackers.*
>
> – Definition of "Hacktivism" by the Parliament of Victoria, Australia

These attacks historically took the form of Web site defacements, denial of service attacks, and the redirection or hijacking of DNS configuration settings. The tools and methodologies utilized by hacktivists are similar to other online attacks. However, unlike script-kiddie attacks (motivated by notoriety amongst peers) or cybercriminal attacks (motivated by financial reward), political events lie at the heart of these threats.

Notable Historic Events

Hacktivism has a long and notable history:

1989 – In October of 1989, a specially crafted ***worm*** targeted US Department of Energy and NASA systems worldwide and replaced terminal login screens with anti-nuclear banner messages. Interestingly enough, the worm included specific instructions to avoid infecting computers in New Zealand, probably because New Zealand had declared itself a "Nuclear Free Territory" in 1984.

1995 – December of 1995 saw a group calling itself "Strano Network" conduct a ***virtual sit-in*** against Web sites operated by various French government agencies to protest nuclear and social policies. At the appointed time, participants from around the world were instructed to point their Web browsers at the government Web sites. The ***denial of service*** attack resulted in those targeted Web sites being unable to serve content.

1998 – In June of 1998, the hacking group "Milw0rm" ***hacked*** in to the Bhabha Atomic Research Centre (BARC) and replaced the center's Web site with an anti-nuclear message in protest against India's nuclear testing practices. The following month saw Milw0rm and the group "Ashtray Lumberjacks" conduct a ***mass-defacement*** of some 300 Web sites with similar anti-nuclear messages.

1998 – The later part of 1998 saw an offshoot of the Liberation Tigers of Tamil Eelam initiate an ***email bombing*** campaign against Sri Lankan embassies, which crashed email servers around the world. Around 800 emails were sent each day for two weeks with the message "We are the Internet Black Tigers and we're doing this to disrupt your communications".

1999 – Following the accidental NATO bombing of the Chinese Embassy in Belgrade on May 7th of 1999, groups of Chinese citizens and students responded by targeting US government institutions. Several Web servers and government systems were ***hacked*** and ***defaced*** with pro-Chinese and anti-US messages.

Groups of US hackers ***retaliated*** by targeting Chinese government websites, leaving obscenity-laden anti-Chinese statements.

1999 – The 21st of October 1999 saw the first "Jam ECHELON Day". In response to the deployment of ECHELON (an international electronic communications surveillance network filtering any and all satellite, microwave, cellular, and fiber-optic traffic), protestors attached long lists of surveillance keywords to emails and other electronic messages. The attack was designed to ***jam*** ECHELON systems and cause them to ***crash*** by overloading their processing capabilities.

Recent Hacktivism

Hacktivist attacks have become better organized over the past decade, increasing in scope and ambition, growing in scale and receiving broader mass-media coverage. However, the tactics and methods of attack have remained largely unchanged, relying mostly on Web site defacements and distributed denial of service (DDoS) attacks.

For example, a number of public protests accompanied the Olympic Torch procession in the run up to the Beijing Olympic Games. The goal was to protest Chinese government policies concerning Tibet and the nation's poor human rights record, and efforts received extensive international media coverage. Chinese hacker groups such as "Revenge of Flame" responded by targeting CNN with DDoS attacks (SYN and ICMP network floods). While CNN took preemptive mitigation steps, the attacks did appear to slow down or disrupt the targeted corporate systems in Asia. In parallel, new malware such as the Fribet Trojan were developed and planted on pro-Tibet websites that subsequently infected site visitors.

Figure 1: Example of the DDoS agent used by "Revenge of Flame" members designed to specifically target www.cnn.com

Hundreds of Dutch Web sites were defaced by Islamic hackers in August of 2008 in response to the public release of the film "Fitna" in March of that same year by Dutch parliamentarian Geert Wilders. One hacker – going by the name of "nEt^DeViL" – managed to conduct a mass-defacement after penetrating a shared hosting provider, and recorded the process in the Zone-H defacement catalogue. Similar mass defacements had occurred in 2006 following the publication of twelve editorial cartoons in a major Danish newspaper which depicted the Islamic prophet Muhammad in a satirical light.

DATE	ATTACKER	FLAGS	DOMAIN	OS	VIEW
2008/08/25	nEt^DeViL	H M	krommeweg1.nl	Linux	
2008/08/25	nEt^DeViL	H M	zjosque.wimdesign.nl	Linux	
2008/08/25	nEt^DeViL	H M	wimcomputers.nl	Linux	
2008/08/25	nEt^DeViL	H M	wimwebsitesolutions.nl	Linux	
2008/08/25	nEt^DeViL	H M	birdmanproduction.nl	Linux	
2008/08/25	nEt^DeViL	H M	osv95.nl	Linux	
2008/08/25	nEt^DeViL	H M	dekomiezn.nl	Linux	
2008/08/25	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	

Figure 2: Hundreds of Dutch web sites hacked by Islamic hackers and publicly listed on the defacement reporting website Zone-H

Perhaps the most studied hacktivism event to occur to date relates the to cyber attacks against Georgia in August 2008 during a broader armed conflict that broke out between the Russian Federation and the Republic of Georgia over South Ossetia. In this example, international political and military conflict was accompanied – or even preceded – by a coordinated cyber offensive.

South Ossetia had became a *de facto* independent state from Georgia in 1991, but remained recognized by the international community as part of Georgia. On August 7, Georgian forces launched a surprise attack against the separatist forces in South Ossetia. Russia responded the following day by conducting military operations within Georgia. Cyber attacks were launched at the same time against a number of Georgian government Web sites.

Several Georgian government sites were defaced, often using SQL Injection and new targeted attack malware variants. However, the most devastating attacks were DDoS efforts estimated to average over two hours per target, per incident. Some attacks lasted as long as 6 hours, with traffic peaking in excess of 800 Mbps.

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%)			

Figure 3: Attempts to access the Georgian government site mfa.gov.ge from various US and international locations during a DDoS attack.

The beginning of 2009 saw a new escalation in hacktivism between pro-Israeli and pro-Palestinian supporters following an Israeli ground invasion of the Gaza strip on January 3rd 2009, which itself was a response to intensified rocket and mortar attacks against Israel.

There was no shortage of Web site defacements, targeted malware and DDoS attacks between either side of the wider conflict. The difference in this hacktivism event is that is was the first major cyber campaign to utilize popular social networking sites. Hacktivists on both sides created social network groups that rapidly attracted hundreds of thousands of international supporters and served as protest coordination centers.

Figure 4: Examples of some pro-Israeli and pro-Palestinian Facebook groups that appeared during the Gaza War in early 2009.

Social networking groups were used to attract supporters and coordinate a wide variety of physical-world protesting and hacktivist attacks, both during the conflict and afterwards. In many cases supporters provided detailed instructions and target lists for cyber attacks.

The Iranian elections of June 2009 saw the development of new and improved hacktivist tactics – specifically, the widespread use of micro-blogging technologies that provided real-time coordination of attacks against Iranian government websites.

Figure 5: Example of a denial of service attack page serving multiple framed instances of the targeted website, and responses from the server indicating their relative success.

In response to voting irregularities in the election, Iranian supporters of defeated presidential candidates launched multiple "grass-root" DDoS attacks. The preferred vehicle for attack was to view Web pages that contained multiple embedded frames that then opened up multiple instances of the targeted Web site. The locations of these "master" frame-loading pages were passed on to protesters through a broad spectrum of electronic communications technologies – but it was via the micro-blogging sites (e.g. Twitter) that the protests drew the most attention and attracted

worldwide participation in the attacks. As the Iranian government filtered, blocked and shutdown Iranian Web sites hosting attack pages, new pages were created by supporters and their locations rebroadcast on the micro-blogging sites.

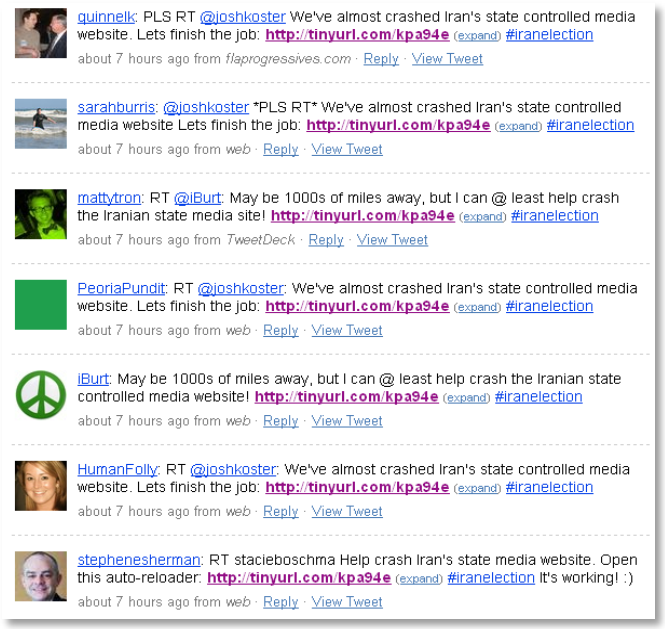

Figure 6: Example of the Twitter memestream - #iranelection – being used to coordinate hacktivist attacks.

A Protesters Tool Chest

Online protests take many different forms. While political motivations lie at the heart of classic hacktivism, there are many other reasons for the dissatisfied or aggrieved to take their protests online. Depending upon the topic at hand, technical capabilities of protesters and willingness to do harm, a wide range of tools and technologies exist that deliver a diverse array of tools and technologies for launching successful cyber attacks.

The technical capabilities of the protesters and their willingness to remain anonymous dictates many of the tactics that can be employed *en mass*. Defacements of Web sites and the construction of fake or defamatory Web sites, require above-average technical skills. As such, the majority of coordinated mass-attacks rely upon easy-to-use technologies and software agents that already exist in the public domain.

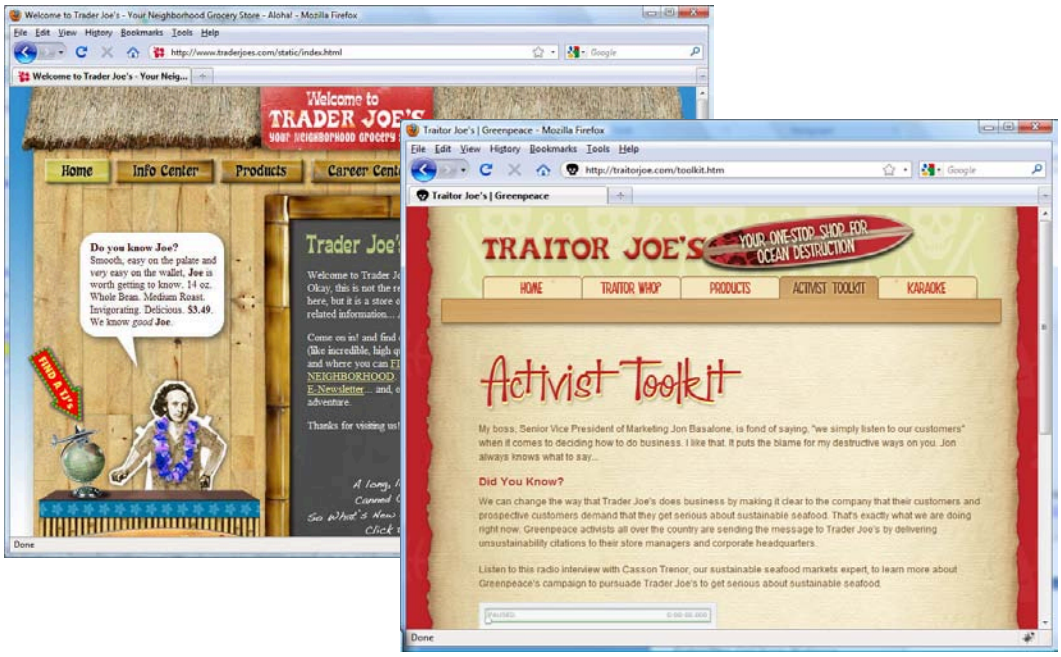

Figure 7: Example of cyber-protesting tactics satirizing names and domain registration. Here the website of Trader Joes is parodied as Traitor Joes to protest selling certain goods. The hacktivist site recruits additional protesters.

Despite all of the technologies that might be used to launch a cyber-protest, two tactics are at the core of today's mass attacks today:

- Network Flooding
- Mail bombing

Networking Flooding

Networking Flooding is a broad term that covers most network Denial of Service attacks. Network floods may be conducted from single or multiple sources, and typically focus on one networking protocol at a time (e.g. HTTP).

Network floods have proved to be a successful attack tactic for over two decades. They are regularly employed by cyber-criminals (for extortion purposes) and by script-kiddies (for venting anger). As such, there is no shortage of public information on how to launch, create or acquire the ability to generate a "point-and-shoot" network flood.

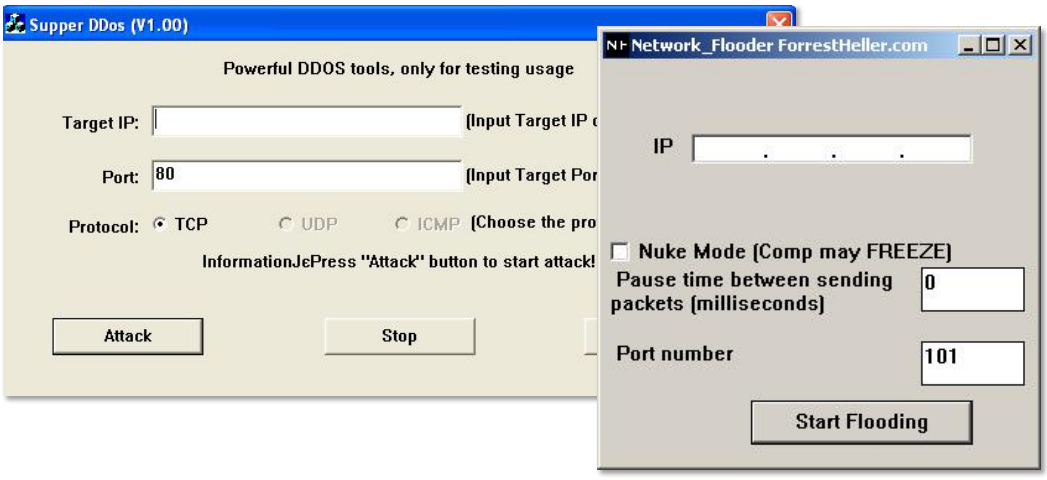

Figure 8: Examples of public domain network flooder and DDoS software agents.

Networking flooding technologies and tactics used for cyber-protesting can be divided in to the following categories:

Bandwidth Consumption – The purpose of this tactic is to flood the target's Internet connection(s) such that no additional (i.e. legitimate) traffic can reach the organization's servers. The network protocol and the targeted services are largely irrelevant, and may affect any third-party networking devices in the "stream" of the flood.

Malicious Packet Flood – Specially constructed network packets are launched repeatedly at the targeted organization's networking infrastructure or servers. Fewer network packets are needed to cause systems to fail (e.g. crash, slow down or loose data), which means the attack requires fewer resources to launch a successful attack.

Web Site Denial of Service – Web servers can only respond to a certain number of page requests per second. If the number of page requests exceeds this capacity, then the Web server will be unable to answer additional requests. Therefore, flooding a Web server with multiple repeated Web page requests can cause a denial of service

Any and all of these tactics may be used by a single protestor or by a larger collective – or by a single user via the use of a botnet. When these network flood attacks are used by multiple protesters in multiple locations, using multiple systems, the resultant attack is commonly referred to as a "Distributed Denial of Service" (DDoS).

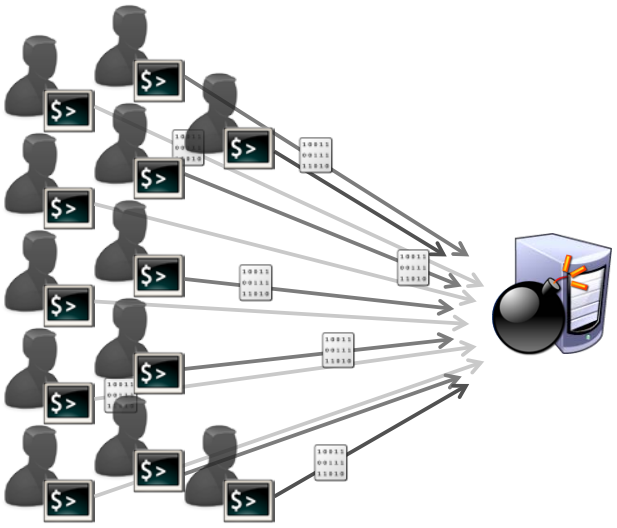

Figure 9: Multiple protesters launching a network flood simultaneously causes a DDoS.

Generic network flooding tools are easy to find using public search engines and can be accessed for free. However, a growing number of hacktivists and other cyber-protesters create their own DDoS software agents, themed for a particular cause, and shared or advertised over the Internet.

Many of these "themed" network flooding agents promote or defend specific religious and political views, and are almost always presented in the local language or dialect of their audience. Web sites that host the software and promote its use (including operating instructions and attack coordination information) have often been referred to as "Cyber-Jihad" sites.

For example, Al-jinan sites (shut down late 2007) included the following tools and information:

> *"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."*

Figure 10: The "Electronic Jihad" agent provided via Al-jinan sites in 2007 (right), and a DDoS agent built to target specific government sites in response to the shooting down of a jet fighter.

Mail Bombing

Mail bombing purposefully sends multiple email messages to targeted recipients in an attempt either to saturate email inboxes or to cause the receiving mail server to crash.

How to launch a mail bomb attack is relatively simple process. In fact, the first mail bombing tools predate the Internet and were often used on dial-up bulletin board systems (BBS) to deny service to a particular BBS member or to crash the entire mail system of the BBS. Today, there are over 180+ different email bomber applications in circulation, and it is a trivial task to create yet another one.

Most email bomber software is easy to use, typically requiring nothing more than a list of target email addresses and the message to be sent. Once an attack has been initiated, the protester can send many thousands of emails per minute. The ease of use and low cost make this class of protesting tool very popular. At the same time, the overall success rate of this attack vector has dropped in recent years, mostly due to widespread deployment of anti-spam technologies within enterprise and government networks.

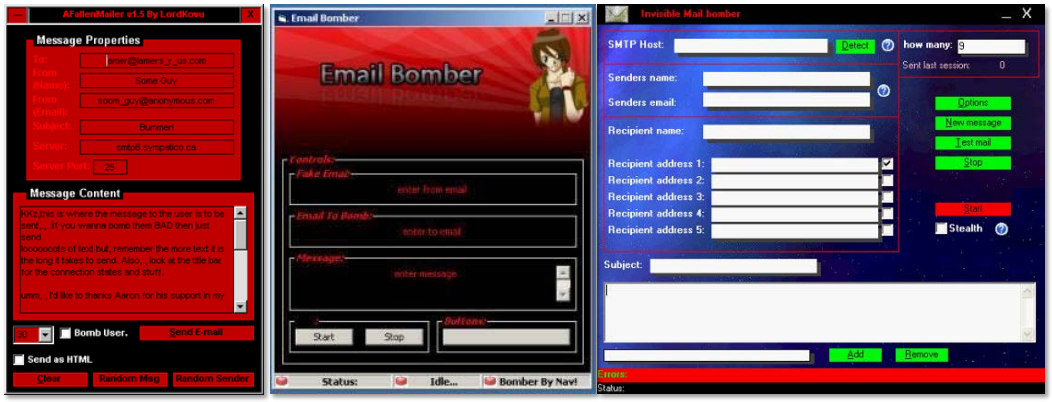

Figure 11: Examples of some of the more than 180 email bomber applications currently in circulation over the Internet.

The Social Network Element

As social networks and their associated micro-blogging capabilities have matured, they have been increasingly incorporated into cyber-protesting frameworks. The ability to attract very large groups of similarly motivated individuals from around the world and communicate with them in real-time creates an irresistible opportunity for cyber-protest coordinators.

The social network phenomenon itself continues to create new forums for mass communications and event coordination. Virtual communities can be created instantly to address passionate topics, political ideals and social injustices, as well as serve as epicenters for new protest movements. These communities of like-minded individuals can rapidly swell in size.

Figure 12: A selection of some of the more popular social networking services.

With the number of members counted in the tens or hundreds-of-millions, popular social networking sites such as Facebook, MySpace, Orkut, Skyrock and LinkedIn have memberships in the tens and hundreds of millions, which makes them fertile ground for modern cyber-protesting. As evidenced during the 2009 Israel-Gaza conflict, Facebook groups alone supporting the different factions attracted hundreds of thousands of members almost overnight. The more active and fanatical members within some of these groups promoted aggressive calls to action and openly facilitated "mob" responses – including the distribution of cyber arms and DDoS attack coordination.

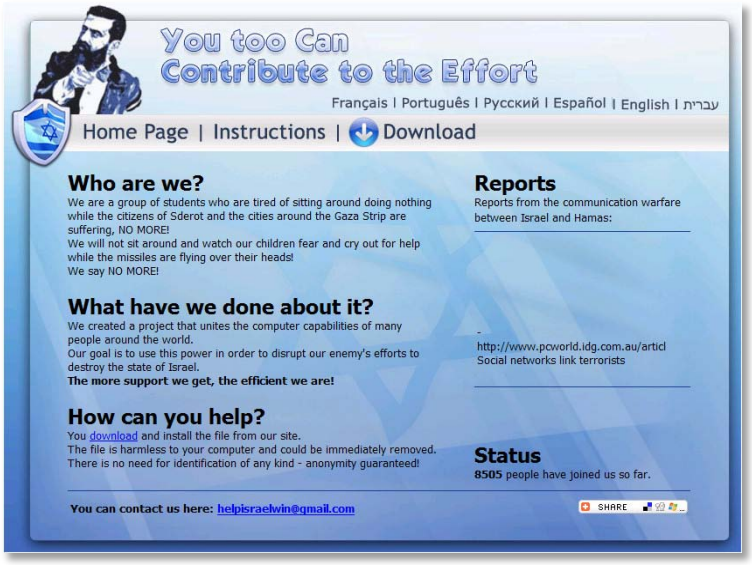

Figure 13: Example of a pro-Israeli Web site promoted within Facebook that asked members to visit the site, install the centrally controlled DDoS bot agent, and take an active role in DDoS attacks. Here we see 8,505 people have chosen to participate in this specialized botnet.

Moving beyond "Discussion"

While social networks and micro-blogging sites provide a convenient vehicle for organizing aggressive mass protests, it is important to understand how group members may be persuaded to take up cyber arms and participate in Internet attacks in the first place. The ability to share key information about likely or proposed targets within social networking groups is significant – and may take different forms:

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 ###### i to the visa request page. If we all do this, no one will be able to get a visa!"*

Sharing this kind of information and coordinating these activities is one thing, but motivating and incenting members to take an active role in a cyber-protest is another. There are however two key ingredients – ease of use, and vagueness over any legalities – which are illustrated through the following real-life examples:

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?"*

Plugged into Social Networks

Most successful social networking sites rely upon "Web 2.0" technologies in order to provide an application framework. These platforms allow members to extend the features of the social network and build new applications on top of the interactive portal. To date, social networks with the best and most flexible frameworks for custom tools and site integration have proved to be the most successful in terms of attracting large groups of members.

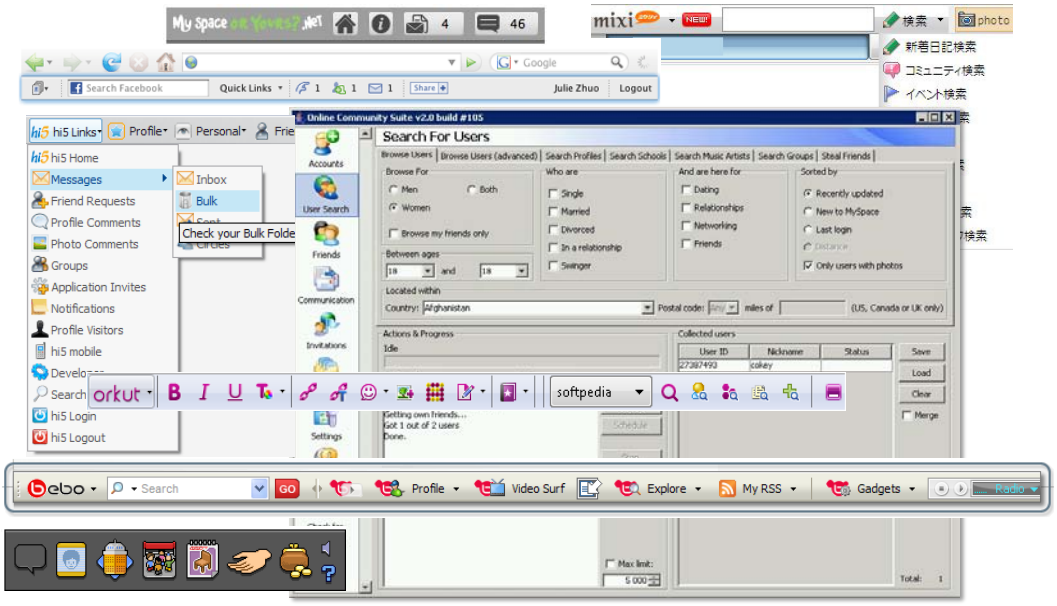

Figure 14: Some of the toolbars and other applications designed to integrate with and operate within social networking Web sites and their custom portals.

There are two primary classes of tool development commonly employed by social network application developers:

- Browser toolbars and installable applications that maintain constant links and communication streams with the social network site.
- In-site application "widgets" that can be installed within page content and shared among users when interfacing directly with the site.

Of course, this custom application development framework has not escaped the notice of technically savvy cyber-protesters.

The Future Protesting Tool

The rapid evolution and acceptance of hacktivism and other forms of cyber-protesting has in turn generated new suites of online tactics. Given how easy it is to develop new tools that plug in to social network communication channels to send and receive control data, and the general availability of source code and instructions for launching DDoS attacks, it is a foregone conclusion that new cyber-protesting tools integrate within social network groups and make it substantially easier to participate.

Figure 15: Combining technologies and tactics

Protesters use social networks to attract large groups of members, coordinate target information, arm these groups with standard DDoS attack technologies, and blend the mix with Web 2.0 integration tools. The end result delivers automation and cross-platform support – a cyber-protesting steamroller!

Figure 16: A cyber-protesting steamroller.

The cyber-protesting steamroller is, in essence, a community toolkit for launching coordinated attacks against selected targets. Core features include:

Simplicity – Download the software package, install it, and participate in the attack.

Stealth – The (subscribed) social network group provides the Command-and-Control (CnC) instructions for coordinating the attack amongst tens-of-thousands of members.

Sophistication – Web, email and network DDoS functionality, inclusive, is built in for "fire and forget" attacks.

Additional features and functionality will continue to emerge as cyber-protesting becomes increasingly easier and capable. Just as social networking portals allow members to join more than a single group, future capabilities would likely include the ability to also subscribe to multiple groups and participate in multiple cyber-protests – perhaps offering the ability to "time-share" spare computer and network capacity among multiple "worthy" causes. Some other likely adoptions include:

- Automatically leave defamatory messages, disinformation and comments in popular forums and blogs.
- Hook in to multiple social networking sites and communication channels in order to recruit wider circles of new members or DDoS targets.
- Integrate VoIP functions to leave voice messages and subsequently DDoS the telephony systems of targets.

Most popular social networks provide application frameworks that can be accessed from smartphone technologies. It is reasonable to expect that new and additional forms of cyber-protesting will make use of technologies that *only* exist on smartphones – but are coordinated via the cyber-protesters CnC.

Figure 17: Social networking applications already incorporate Smartphone features.

Smartphone integration within the cyber-protest steamroller enables additional attack vectors:

- SMS and MMS flooding capabilities
- Voice and voice-mailbox denial of service
- Proximity-based WiFi denial of service and exploitation

The Opt-In Botnet

Cybercriminals have been making use of botnets and associated malware for over a decade. The ability to remotely control thousands or millions of compromised computer systems, and then to task them with scripted malicious actions, has become a defining feature of organized crime and fraud over the Internet.

In practically all criminal botnet cases in the past, the owners or users of the bot-infected computers have been unwitting participants in an attack. This aspect of botnet participation fundamentally changes in the context of cyber-protesting, since as users *intentionally* install botnet software agents, *subscribe* to a particular CnC, and *choose* to participate in coordinated attacks against a target category.

Whether it's because of a vagueness in the understanding of laws governing cyber attacks and electronic denial of service, or a perception of only being a small cog in a much wider effort that will never result in them being singled out, there seems to be few inhibitors to taking protesting in to the cyber world and taking an active role in the call to action. Add to this the relative ease of participation from a technology perspective, and the opt-in botnet comes of age – along with a steamroller effect capable of crushing any sized target.

Reasons to Cyber-Protest

The creation of new groups within social networking portal sites and the ability attract tens-of-thousands of like-minded souls are just a few clicks away. As such, there has been an explosion in the creation of groups that cater to all ends of the social ideological spectrum – many of which focus upon a very narrow subject area or cause.

This ability to create new groups rapidly and attract new members from a deep global pool of users– in reaction to a particular event or critique – will have a growing impact on the way businesses conduct operations online and why people (including their own customers) may be motivated to participate in attacks against them.

Group creation and "mob" attacks will be driven by an increasingly broad spectrum of issues. For example:

- 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…"*

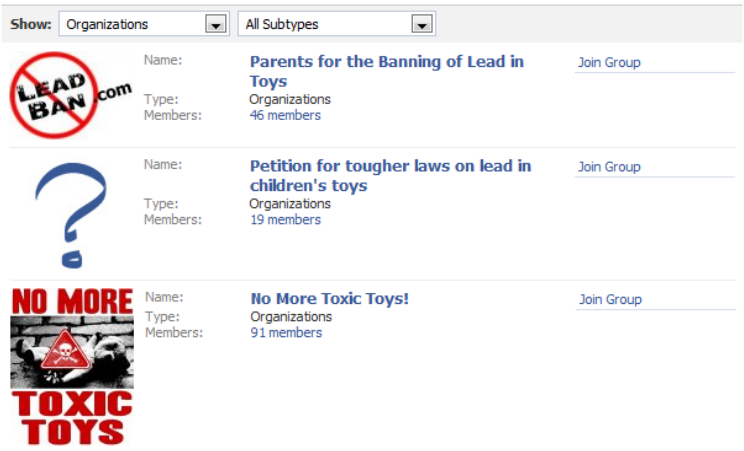

Figure 18: A sample of Facebook groups created to discuss, petition and protest lead-based paint in children's toys.

Forms of Attack

As previously discussed, there are a wide range of attack technologies already in circulation and available to anyone who wishes to yield them for a particular cause. While hacktivism has been focused on political causes and ideology (relying heavily upon denial of service tactics), the broader scope of cyber-protesting and its causes have a more significant effect on businesses – both for why they are being targeted and the nature of the impending attack.

Business executives and corporate security teams should consider the wider implications of the following example forms of attack:

Denial of Service – Customers and clients may be prevented from accessing Internet services, gateways and other critical corporate business systems.

Economic Exhaustion – While ISP and other cloud-based service models will allow businesses to continue to conduct Internet business, there is typically a high financial cost to thwarting DDoS attacks. Long term, sustained, DDoS can be financially debilitating for Internet-only businesses.

Loss of Internet Communications – Not only may cyber-protesters target an organization's visible Internet services and prevent customers or clients from accessing business systems, but other critical business systems may be affected – preventing employees from reaching customers and other business partners.

Swamping of Internal Systems – Internal business systems may be swamped by attack traffic (e.g. email bombing, WiFi denial of service), which disrupts other business processes.

Public Disinformation – Defamatory comments and disinformation may be spread to other Web sites and portals beyond the organization's control. These malicious comments and disinformation can cause brand erosion and permanently scar an organization's public reputation (and the reputations of its executives and employees).

Harassment of Business Executives – Key contact and location information about business executives are often mentioned or traded by protestors. Executives can then be personally targeted through electronic means – e.g. home phone numbers, cell phone numbers, personal email, family members social networking pages, etc.

Unreachable Telephony Systems – VoIP technologies and the bleed-over of social networking technologies to smartphones means that both business and executive telephony systems may come under direct attack and denial of service.

Victim or Enabler?

Being the subject of a cyber-protest and ultimate victim of the attack are fairly easy to comprehend – and appropriate steps can be taken to limit the impact upon business systems. It does however raise questions as to how an organization should pursue its attackers.

Organizations that have successfully dealt with (and prosecuted) the cybercriminals behind the botnets that attempted to extort or rob them have traditionally been seen in a very favorable light by the news media and their customers. The same response is unlikely to be forthcoming in the context of opt-in botnets and cyber-protests – where the people attacking the organization may be existing customers, or could be customers in the future. Any attempts to pursue and prosecute them would cause significant damage to the organization's reputation.

Quite apart from being a victim of a cyber-protest, what are the implications of being an enabler? Facilitating an attack on another organization comes with its own very serious legal implications.

Consider the fact that company employees can opt-in to a botnet, install the tools needed for launching an attack, and take an active role in an ongoing cyber-protest - using company assets (even during work hours). Or, that corporate Web sites, portals and forums may become a compromised host broadcasting libelous messages and disinformation.

Businesses must:

- Seek to ensure that employees fully understand the consequences of misusing corporate systems for cyber-protesting.
- Prevent employees from installing opt-in botnet software and other attack tool technologies on corporate systems.
- Be able to identify and block CnC traffic to/from opt-in botnet software – thereby preventing participation in cyber-protests.
- Prevent any and all outbound attack traffic from reaching external targets/victims.

- Monitor corporate Web sites, portals and forums for abuse and the presence of defamatory material posted as part of a coordinated or automated cyber-protest.

And yet, this internal threat, introduced inadvertently or on purpose by trusted employees and contractors, is often the least understood and most under-protected part of enterprise security. Ironically, many organizations claim proper maintenance of fiduciary responsibility while these serious, remote-controlled breaches expose the enterprise to significant legal and financial liability. It's only a matter of time before this disconnect becomes a serious crisis.

Conclusions

Having evolved from hacktivist origins, cyber-protesting and its affiliation with the social networking phenomenon represents a rapidly growing threat to business. The ability to attract tens or hundreds of thousands of like-minded individuals from around the world – and to persuade them to participate in automated attacks against targeted organizations for the slightest of reasons – must be a major concern for business.

In short, just as businesses have embraced the Internet for faster communications and operational efficiencies, protestors have similarly embraced Internet technologies and continue to hone their disruption capabilities. The precedents have been set. The tools are cheap, easy to find and simple to apply. These new platforms allow attacks to be controlled and coordinated from anywhere around the globe, and the vagueness of protesting legalities and relative ease of participation means that more and more people will join cyber-protests.

The threats will only grow in scale and seriousness. For example, the merging of social networks and smartphone technologies are resulting in a new range of cyber-protesting opportunities. Something as simple as the ability to "donate" $20 of calls and SMS messages to a smartphone-based opt-in botnet agent could result in a wave of targeted cellular attacks against business executives – as well as a surge in data volume that could also easily cripple the network provider .

Organizations need to understand this new world, both as a potential victim of a cyber-protest, and as an enabler, either intentional or unwitting. Attempted prosecution of cyber-protestors – who may in all likelihood be dissatisfied customers – is unlikely to yield favorable results, either in the courts or with news media and public opinion. If an organization's own employees partake in a cyber-protest using corporate systems, the likelihood of prosecution as an enabler of the crime grows substantially – while the potential legal and financial liability to the business itself grows dramatically.

Opt-in botnets are a now a fact of life, whether businesses are ready for them or not. That cyber-protesting steamroller is on its way. The only way to avoid it is to see it well in advance and to be prepared.

Additional Reading

"Coordinated Russia vs Georgia cyber attack in progress ",Dancho Danchev, August 2008, http://blogs.zdnet.com/security/?p=1670

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

"Cyber Attacks Against Georgia: Legal Lessons Identified", Cooperative Cyber Defence Centre of Excellence, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

About Damballa, Inc.

Damballa stops crimeware threats that exploit enterprise networks for illegal activity by finding and disrupting the hidden communications channels used to control internal servers and hosts. This concentrated focus on malicious remote control delivers fast, accurate insight into advanced network threats, including termination of criminal activity and remediation guidance. Damballa's technology integrates easily with existing infrastructure for cost-effective protection against dangerous security breaches that evade other solutions. The result is smarter, more flexible network security that stops current and future threats, prevents fiduciary breaches and enhances regulatory compliance. Damballa's customers include major banks, Internet service providers, government agencies, educational organizations, manufacturers and other organizations concerned with taking back the command-and-control of their networks. Privately held, Damballa is headquartered in Atlanta, GA. Visit us at: http://www.damballa.com