CHALMERS

Threat modelling of hacktivist groups

Organization, chain of command, and attack methods

Master of Science Thesis in Secure and Dependable Computer Systems

THOMAS CHOPITEA

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
Göteborg, Sweden, Aug 2012

Threat modelling of hacktivist groups
Organization, chain of command, and attack methods

THOMAS CHOPITEA

Examiner: ERLAND JONSSON

Chalmers University of Technology
University of Gothenburg
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

The logo of Anonymous, a large hacktivist group

Department of Computer Science and Engineering
Göteborg, Sweden Aug 2012

ACKNOWLEDGMENTS

I would like to thank my colleagues at CEIS who all contributed to a very nice work environment during my stay there: Anastasia Rumyantseva, Alexandre Durand, Charles Ibrahim, Aurélien Della, Elena Vlasova, and Lucas Piferrer.

I would also like to thank my supervisors there, Nicolas Caproni, whose deep insight in cybercrime and ever-lasting good mood were very welcome, and Barabara Louis-Sidney, whose knowledge about cyber-related legislation came in very handy.

Special thanks go to my supervisor at Chalmers, Erland Jonsson, for his patience, guidance, and good advice, despite the distance between Gothenburg and Paris.

Thanks to Scot, Jericho, and Félix, who took the time to answer my questions.

Finally, I would like to thank my family and friends, who supported me throughout the whole adventure.

Thank you.

ABSTRACT

As the social web emerges, increasingly more people are starting to adopt the Internet as a means of communication. Activists are no exception to the rule, as can be seen by the number of online protests and movements organized through Facebook or Twitter. As a consequence of this, a particular branch of online activists, also known as hacktivists, have evolved into a full-blown online threat.

The aim of this report is to provide a technical insight on the attack methods and motivations of hacktivist groups, and provide a solid understanding of the full extent of their capacities. The report includes a technical background on hacker and activist culture, which is essential in order to properly understand the hacktivist mindset. Some real-world incidents have been selected, and their attack scenarios have been reconstructed as precisely as possible in order to evaluate, in each case, the technical skills of the attacker. Based on an evaluation of both technical expertise and motivations, we have deduced a threat model that corresponds to most hacktivist groups. At last, the research also covers the way in which these kinds of threats fit into the geopolitical landscape; how important the threat is, and what are its limitations.

TABLE OF CONTENTS

INTRODUCTION

The web 2.0, or social web, has had deep changes in the way people communicate and interact with each other, as individuals or as groups. Content-sharing websites make information flow at incredibly high rates (Softpedia, 2012), and publishing platforms such as blogs make an excellent broadcasting medium. This "empowerment of information" is not without repercussions on its security. A whole industry has developed around financially motivated cybercrime; some analysts suggest the cost of cybercrime is "greater than the combined effect on the global economy of trafficking in marijuana, heroin, and cocaine, which is estimated at $388bn" (The Register, 2011). But online crime is not the only way in which the social web has changed the information security landscape. The new social dimension of the Internet is key in all kinds of political activities – including activism.

Enter the "hacktivist": Portmanteau word for "hacker" and "activist", the hacktivist is the intersection between the politically inclined and the computer literate parts of the population. Before the web, we had pamphlets, meetings, strikes, and propaganda. Nowadays, we have blogs, forums, DDoS attacks, and "doxing".

The purpose of this thesis is to examine how activism has evolved since the dawn of the social Internet, understand the motivations behind each type of cyber-activist, their organization, and attack methods, based on real-world case studies. The work will also try to test the permeability of such groups, and try to see how easily they can be infiltrated – by law enforcement agencies and terrorist groups alike – and what incidence does this have on the general geopolitical panorama. This will result in a threat model that will hopefully lead to a better understanding of the threat represented by hacktivists on the global Internet, as well as the role they play.

The research behind this thesis will be mostly based on publicly available information and open source intelligence. Field experts, researchers, authors, and activists will be interviewed in order to bring more value to some parts of the research.

1 TECHNICAL BACKGROUND

This section will cover some notions that are essential to the proper understanding of the hacktivist persona. We will briefly discuss the origins of hackers, the influence of the social web on activism, and will give an overview of hacktivist groups in their different forms. Finally, we will deduce a set of common characteristics shared by most hacktivist groups. This information will be useful to determine how to interpret the causes and consequences of the case studies discussed further in the report.

1.1 Hacking and political dissidence

The term "hacker" was first used in the 60s to describe a specific computer programmer subculture amongst the students of the Massachusetts Institute of Technology. The Jargon File (The Jargon File, 1990) describes the hacker as "A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary". The extensive understanding of these systems often lead hackers to the discovery of techniques to make systems act in a specific way. These techniques were called "hacks". Exploring, learning and controlling: this can be defined as the earliest hacker instance of hacker culture. It then comes as no surprise that most hackers eventually started focusing on information security. By understanding systems, they were the most suited to discover new weaknesses and the ways malicious people could abuse them. The information security ("infosec") industry was born. Today, a hacker is mostly regarded as an expert in information and computer security.

1.2 Hacking as a form of protest

A complete study of hacker sociology and culture falls outside of the scope of this work, and would make a whole paper by itself. What is of interest in the context of this research is how hacking and the hacker subculture relate to politics and activism. The relation becomes clear when we understand that hacking may be seen as a way to study a given system in order to break free from its constraints. The more constraining an environment is, the more work will be done in order to study it and find ways to overcome or bypass it.

In this way, the hacker and the political activist are no different in nature. Both have something to fight against, and both are trying to break free from constraints they judge unacceptable. So what happens when a given individual has the mindsets of both the hacker and the activist?

1.3 Hacktivism

The *hacktivist* – halfway between activist and hacker – can be described as a hacker with political motivations. Even though both terms are usually indistinctively employed, we can consider that hacktivists differ slightly from cyber-activists. The latter will transpose activism to the online world, using classical communication methods: blogs, email campaigns, online propaganda, etc.

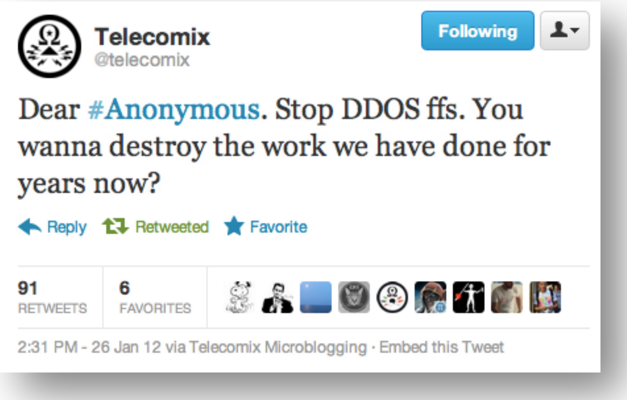
Hacktivists will go one step further, to the point where they will use their technical skills to divert and bypass security systems in order to increase the impact of their messages. If cyber-activists are the people on the street distributing pamphlets, then hacktivists will be the ones breaking into testing labs and freeing the animals there.

1.3.1 Anonymous and Telecomix

All hacktivist groups are not alike. Two of the most striking examples are Anonymous and Telecomix, which have similar goals but totally different approaches.

Telecomix, much like Anonymous, are self-described as a decentralized "occurrence" of people gathering around different causes (Telecomix, 2012). One of the better-known projects involving Telecomix is the installation of dial-up modems to enable Egyptian dissidents to bypass the local government's Internet censorship (WeRebuild, 2012). They carried out similar activities in Syria, and also helped publish log files pertaining to the surveillance systems of the American company Blue Coat. This forced Blue Coat to admit that U.S. products were being used by the Syrian government in their repression (The Wall Street Journal, 2011).

Anonymous' techniques, on the other hand, are notorious for being much more offensive. Their methods include gaining unauthorized access to servers, publicly disclosing personal or sensitive data (*doxing*), discrediting their opponents, and carrying out Distributed Denial of Service (DDoS) attacks. Anonymous' *modus operandi* will be discussed in more details in further sections of this report. Telecomix, on the other hand, has not been known for doxing individuals, and refuse to use DDoS as part of their protest actions.



Telecomix
@telecomix

Dear #Anonymous. Stop DDOS ffs. You wanna destroy the work we have done for years now?

91 RETWEETS 6 FAVORITES

2:31 PM - 26 Jan 12 via Telecomix Microblogging · Embed this Tweet

Figure 1: Telecomix criticizes Anonymous for their use of DDoS attacks.

Both groups share similar concerns for net neutrality, information flow, and general Internet and data freedom – or, as Telecomix puts it, *Datalove*. But both use information security-related techniques in order to achieve their goals, even though their methods vary in legality. (For a more detailed list of Telecomix and Anonymous' operations, please see Appendix A.) Another striking similarity that both groups share is their structure. They have no official hierarchy, and subgroups (Anonymous organizes around "Ops", whereas Telecomix has "sub-clusters") usually define their main activities.

Of course, the popularity of such movements amongst the population has not been without consequences. It has inspired the most "trigger-happy" part of the hacker population to form new groups, or "crews", and carry out their own, personal campaigns.

1.4 Non-political hacker groups

Other hacker groups share similarities with Anonymous or Telecomix, without maintaining any particular political agenda. This is the case for groups like *LulzSec* (which will be further studied in this paper), *TeaMp0isoN*, *UGNazi*, or the group behind Operation *AntiSec* (which seemed to include some members of Anonymous). The main goal of these groups is to promote general mayhem in large companies. They are not motivated by curiosity, not by the challenge, but for what they call "the Lulz" (a deformation of "LOL", the Internet slang term meaning "laughing out loud"). As opposed to "classic" hacktivist groups like Anonymous which do have their share of characteristic humor, these groups make "humor" their main motive of action.

1.5 Patriotic hackers

Some hackers also act individually in order to defend what they consider to be their countries' best interests. In contrast to government-sponsored attackers, they do not have any government backing, and therefore have fewer resources (time, expertise, funding…). There have been many cases of these types of attacks during the last year: The French government websites being subject to Turkish distributed denial of service attacks in protest against a law regarding the Armenian genocide (PC Inpact, 2011), the constant skirmish between Saudi and Israeli hackers (InformationWeek, 2012), which had consequences on the UAE stock exchange (Haaretz, 2012). Another example of patriot hackers is The Jester (also known as th3j35t3r), a lone-wolf hacker who has also been notorious for his support to the American army as well as online campaigns against supporters of Wikileaks and Anonymous.

1.6 Common factors

All the groups mentioned above have their own particularities, but they also have common characteristics:

- *Decentralized hierarchy.* Hacker groups, especially big movements such as Anonymous or Telecomix claim to be headless and decentralized. This makes tracking individual members difficult, since there is no center of command.
- *Leverage "low-hanging fruit" vulnerabilities.* Most attacks carried out by these groups are made possible through easy-to-exploit vulnerabilities, such as SQL injections or weak passwords. Other cases have proven to be more complex: we will discuss them further in this report.

- *Instantaneity.* Their operations have a very short window of action. They usually follow a "get in – grab – destroy – get out" pattern. This renders detection difficult, since little or no evidence is left behind to analyze the attack and track down the perpetrators, and chances of catching them "in the act" are very slim.
- *Extensive use of the social web.* Hacktivist groups make extensive use of social networking sites such as Facebook or Twitter to advertise and publicize their campaigns. They use IRC as a main means of communication, organization, and even to control opt-in DDoS attacks.
- *Cooperation.* Even though smaller crews tend to have clear membership status, they sometimes associate with members from other larger collectives to conduct attacks (ABC Australia, 2011). Since boundaries between groups are extremely blurry, it makes regular members more difficult to identify.

1.6.1 Cyber-guerrilla and asymmetric warfare

One could argue that cyberspace is a "terrain" where large forces are hard to defend. The larger the entity, the larger its attack surface, and the more complex it is to install and maintain foolproof security mechanisms. This is a direct reference to the oldest adage of information security: "the system is as strong as its weakest link".

Because of this particularity, cyberspace cannot be considered as a classic theater of operations, where the most "powerful" party (i.e. the most resourceful, larger party) has greater chances of victory against "weaker" parties. This makes asymmetric warfare and guerilla tactics especially attractive to these weaker parties.

Classical guerrilla tactics involve the use of small and mobile groups, taking advantage of the terrain, and a non-negligible surprise factor (Creveld, 2000). Hacktivists operate precisely according to these rules: their teams and numbers cannot be clearly distinguished, the origin of the attacks can easily be spoofed, and their duration is usually very short.

Besides these characteristics, two additional points are worth highlighting:

- Firstly, hacktivists rely heavily on the "weakest link" law mentioned above: it generally only takes one breach to take control over a whole system.
- Secondly, they usually do not seek complete compromise over a system (as could be the case of government-sponsored threats), but just enough information as to publicly discredit their victims.

Knowing this, the probability of a large system having at least one point of entry, multiplied by the probability of quickly finding useful information (as opposed to the probability of gaining complete control over the system), make the success rate of hacktivist attacks fairly high.

All these common factors will be used as input in the research conducted as a part of this thesis in order to better interpret the real threat posed by hacktivist groups. Throughout this paper, the term "hacktivist" or "hacktivist group" will be used to refer to an individual or group of individuals that observe the aforementioned characteristics.

2 RELATED WORK

Countless people have been interested by the hacker culture since it blossomed. The same, if not more, can be said of political activism. Hacktivism, a more recent phenomenon, has already started attracting attention, and some studies have already been done on the subject.

This section will cover the state of affairs in research on hacktivist groups and their methods. We will cover the work of anthropologist Gabriella Coleman, who has spent long hours studying the Anonymous phenomenon, their motives and organization. We will also mention Imperva's Hacker Intelligence reports, which bring great insight into the technical methods used by hacktivist groups.

Most of the websites included in the references section can also be considered as investigation or research related to this thesis.

2.1 Sociological research

Gabriella Coleman has been studying the anthropological origins of hacktivist groups, especially Anonymous, for over four years. She is undoubtedly one of the most well known researchers of the social dimensions of Anonymous and their *raison d'être.*

In her essay "Our Weirdness is Free" (Coleman, Our Weirdness Is Free, The logic of Anonymous—online army, agent of chaos, and seeker of justice., 2012), Coleman details the results of her ongoing study of the hacktivist group. She explains that originally, Anonymous' fight focused on the Church of Scientology and was mostly aiming at the "Lulz". In 2010, the massive publication of secret documents by Wikileaks and the ensuing financial cut-off they experienced caused Anonymous to organize Operation Payback, which could be regarded as their first real political operation.

Coleman highlights the unpredictability of their organization and the vagueness of their structure – characteristics typical of hacktivist groups that will be taken into account in this paper. She also notes that the media has had great interest in Anonymous-related activities, and that despite this high media notoriety, individual anonymity within the group is preserved.

Although less focused on technical aspects, Coleman's work on social or anthropological aspects of Anonymous is interesting because it analyses both social structure and motivations of Anonymous; insight on these two characteristics is capital in the scope of threat modeling.

Gabriella Coleman's work is not limited to this particular essay. She has done other studies on digital media and the hacker culture. A full listing of her academic publications can be found on her personal website (Coleman, Academic Publications, 2012).

2.2 Technical research

Imperva, an American information security company that primarily focuses on database, web application, and file system security, has published a significant amount of documents as part of their Hacker Intelligence Initiative (HII). The HII's goal is to go "inside the cyber-underground and provide analysis of the trending hacking techniques and interesting attack campaigns".

Hacker Intelligence Initiative report #10, "Dissecting a Hacktivist Attack", specifically focuses on hacktivist campaigns and attacks, by taking the example of an attack launched on the websites militarysingles.com. The report focuses on the attacks that led to the compromise of said website: remote file upload, which combined with Local File Inclusion led to remote command execution, and the dumping of all the users' data. MilitarySingles is a website that focuses on dating for people within the military – it was especially embarrassing for the administrators to see their users' personal identifiable information published on the Internet. Imperva also goes through some analysis about web 2.0 and how it should be used in the public sector, password policies, and advice on how to secure a website from these types of basic attacks.

A summary report titled "The Anatomy of an Anonymous Attack" focuses on Anonymous' attack on the Vatican's systems. It is the first known report of a full Anonymous attack – from recruitment to execution. The report is based on Imperva's Web Application Firewall logs and some investigation, and shows that the attackers started recruiting on social networks, tried some basic SQL injection and Cross-Site Scripting attacks. When that failed, they searched for resource consuming webpages (such as search forms) in order to organize a large-scale DDoS attack. This report is further discussed in section "6.3 – Target selection".

These reports provide very valuable information for anyone wanting to gain insight on how Anonymous (and other hacktivist groups) typically attack an organization. Concretely, it helped filling some gaps in the investigation of the high-profile incidents discussed in section "5 – Case studies".

2.3 Contributions

Hacktivist groups follow a certain structure (e.g. headless chain of command, swarm psychology, specific moral standards), and they evolve in a special environment that has no frontiers, where communication is instantaneous, and traceability is low. It would be a mistake to consider hacktivist groups like classic guerilla groups, since cyberspace is a completely different terrain than land, water, air, or space.

This paper is more focused on the technical and geopolitical dimensions of hacktivism than its social and sociological aspects. What this paper tries to contribute to current research is a concrete understanding of how hacktivist groups are organized and how that same organization impacts the use of their tools and defines their behavior in cyberspace. The environment in which hacktivists evolve cannot be dissociated from their nature. This association, as well as its importance, is precisely what this research is trying to highlight.

3 RESEARCH METHODOLOGY

Evaluating the threat posed by hacktivist groups is not an easy exercise. The only concrete documentation that can be found comes either from media or private security firms. One could assume that the media does not have the technical knowledge to accurately place hacktivist-related events into an information security context. Government sources, on the other hand, may lack transparency, and therefore exaggerate facts in order to spread fear, uncertainty, and doubt ("FUD", in the infosec community) and increase their potential control over the population[1]. Fortunately, whether this is true or not falls far from the scope of this thesis.

This section will discuss the research methodology behind this paper, the caveats that were encountered when using a classical research approach, and how they were countered using investigative techniques.

The research work will focus on actual attacks, real tools, and real methods being used by hacktivist factions. It will be based on publicly known (and sometimes highly mediatized) attacks. The reaction of the media, government, blogosphere, and "twittersphere" will be taken into account. The research will also include open-source information, technical analysis of tools, and interviews of different experts and hacktivists.

3.1 Investigative research

While carrying out the research necessary for the elaboration of this paper, it became apparent that a classical, systematic approach would not work. There were too many unknowns in order to confidently establish a ground for hypothesis: hacktivist groups can differ wildly in certain aspects, and be identical in others. Their volatility was not compatible with the rigor of classical scientific methods.

Instead, the research methodology used throughout this paper stands halfway between those of the investigative journalist and the police detective: the collection and correlation of hard facts, forensic analysis, and public records (open-source intelligence). Putting together each bit of information allowed us to draw conclusions and lead us towards the next subject of interest. This allowed for a much higher degree both of freedom and adaptability, which was much welcomed in order to follow the studied subjects. The information obtained this way was easier to combine with our technical knowledge in information security.

This seems like an important point to take into account when carrying out research on hacktivist groups. The ability to treat a wide array of topics (ranging from politics to information security) and to determine the links between them is extremely important.

The study of a specific incident can thus be described as follows:

[1] The plausibility of such a stance is extremely hard to determine, and is a great source of debate online, to the point where groups (such as the AntiSec movement) have even started questioning full (and responsible) disclosure procedures, proclaiming that they are but another way to spread fear and control consumers.

1. Obtain as much information as possible on the incident. This information will usually come from public media, and gives a good idea of how the incident was interpreted at the time.
2. Determine which steps in the incident are not thoroughly described (e.g. "How did the hackers gain root access?" "Where did they obtain the passwords from?" etc.)
3. Investigate further into those details. Blog posts, data dumps, hack logs, and even tweets can yield useful information. Interviews may also be conducted.
4. Once all details are filled in, evaluate the attack in its entirety. Details on how the evaluation criteria of each attack are discussed in section 4.2.

3.2 Research on major hacktivist attacks

The research will analyze major attacks over the past few years, and try to reconstruct them as accurately as possible, in order to evaluate the technical skills and organization necessary to carry out such an attack.

Attacks will include the retaliation against the closing of Megaupload, the data leaks from Sony's systems, and HBGary's compromise.

For each attack, we tried to establish how the following mechanisms worked:

Organization and recruitment. Some attacks could not have been launched without careful organization and some kind of operational command. Are hacktivist groups organized in a standard way? Or does their organization change according to their target? How do their recruit their members?

Technical aspects of the attack. What is the necessary level of skill to make an attack successful? What are the key tools, programs, and vulnerabilities leveraged by the attackers?

Consequences and worst-case scenarios. All attacks had consequences: are they negligible, or did they have an important impact on their victims? What about the industry? How did the media and government react? In any attack, what could have gone wrong if the attackers wanted, and had the possibility, to cause more damage?

Answering these questions for each case study will shed light on hacktivist groups' actual and potential power. The conclusions drawn will be useful when trying to establish a threat model for this type of attacker.

The methods used to answer these questions will vary from case to case. It will generally involve extensive open-source intelligence research (OSINT), and interviews with field experts. Direct contact with members of hacktivist groups will also be attempted, although it is to be noticed that the recent arrests and betrayals within the hacktivist community (Wired, 2012) are going to make the opportunities for interviews scarcer.

3.3 Information sources

The main information sources in this report are web-based. This differs from classical research, usually based on established literature and essays, but was necessary for the following reasons.

The investigation being focused on relatively recent events, a large part of the information that is available as of today falls outside of the classical editorial timeframe. Internet publications tend to be much more reactive than paper-based literature.

Hacktivists use the Internet extensively, not only to carry out attacks but also to publish content on blogs, Facebook pages, Twitter accounts, or pastebin posts. Information obtained via these channels is therefore of great value, since it is left uncensored, and direct access to the channels is possible.

3.3.1 OSINT: Open Source INTelligence

The definition of open-source intelligence given by the United States Director of National Intelligence and the United States Department of Defense is as follows (U.S. Congress, 2006):

> *"(1) Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."*

3.3.1.1 OSINT and the social web

The social web has brought a completely new dimension to the world of OSINT, the amount of information available increasing exponentially in number. The nature of this information is also new – the world has now access to personal, real-time information about people, organizations, celebrities, and even government staff. Satellite imagery, GPS coordinates taken from EXIF data in uploaded pictures, blogs, Twitter accounts, Facebook or LinkedIn profiles, Pastebin dumps and P2P torrent files, make information obtained online extremely granular, and thus extremely valuable.

Besides, hacktivist groups constantly make use of social tools to communicate, and almost exclusively so. Anonymous has more than one official Twitter handle[2], and their six-figure follower numbers show their support to the group by displaying Fawkian masks, or repeating their motto. Anonymous is just one example, but Telecomix, LulzSec, or TeaMp0isoN members all have or have had their own window to the public world. Whether it is to propagate their political ideologies, or to boast about their defacements and data dumps, public communication is an essential part of any hacktivist activity, since activism draws its power from the people, and their ability to be influenced.

Blogs and the social web are an inherent part of the hacktivist ecosystem and are worth being studied carefully. This report relies heavily on blog posts,

[2] @AnonymousIRC, @Anonymous__fr, @YourAnonNews, @anonops, @AnonymousMexi, @AnonyOps, @Anon_Central,…

tweets, and press releases (both official and unofficial) gathered around the web. When crosschecked with factual research results, the information thus collected will become even more valuable.

3.3.2 IRC

Ensuring communication within an open, public and anarchic group can become quite a daunting task. Forums are not reactive enough, and instant messaging (as it is popularly known today) is too personal. Enter IRC: Internet Relay Chat.

First described in RFC 1459 (J. Oikarinen, 1993) in 1993, IRC is an instant messaging protocol that enables participants to create different communication channels in order to hold group discussions. Today, it has risen in popularity since its flexibility is well suited for hacktivist groups' needs: Public "channels" can be created for distinct topics; "operators" can be assigned to moderate the discussion or ban users. Private channels for smaller-group conversations can be created, and one-to-one communication is also possible. It is an effective tool to organize any sort of action: pamphlet distribution, video editing, translations, or denial of service attacks.

IRC is a great source of information to better understand hacktivist groups. Anyone may connect to the IRC servers and join any channel of interest. This openness, of course, has several consequences on operational security.

The fact that IRC servers are open and public means that law enforcement agencies are probably snooping on conversations. This, in turn, means that some mechanism must exist in order to privately discuss the details of an operation (as long as it falls out of what is legally allowed). Whereas DDoS campaigns are discussed publicly, it is reasonable to think that more "sensitive" conversations are held out-of-band: on private (invisible, or selective) IRC channels or through some entirely different communication service. This may be interpreted as a contradiction between the "total transparency" and the "absence of leadership" endorsed by movements such as Anonymous, but it is nevertheless a necessary burden to them.

In the scope of this study, IRC servers at `irc.anonops.com` were visited in order to discuss with members of Anonymous (and their derived groups). Special attention was paid to the channels `#Francophone`, `#antisec`, `#anonops`, and `#tutorials`. This was particularly fruitful when attacks in response to the seizure of Megaupload started, coordinated from the channel `#OpMegaupload`. Concrete observations of these events will be discussed further into the report.

3.3.3 Interviews

The aim of using IRC was also to contact hacktivists directly. Unfortunately, the wave of arrests (The Associated Press, 2012), (Fox News, 2011) and treason (The Guardian, 2012) within several hacktivist groups caused great mistrust towards newcomers – with good reason. It was therefore very difficult to rely only on IRC for information about their attacks.

Interviews with field experts are to be carried out: penetration testers, security and OSINT analysts, and security experts have been contacted to shed light on some matters discussed in this paper.

4 CASE STUDIES

Throughout this section, we will analyze some real-world attacks commandeered by members of different hacktivist groups. For each case study we will identify:

- *Modus operandi*: planning and execution of the attack, and aftermath;
- *Attack vector*: leveraged vulnerabilities, attacks launched, tools used;
- *Consequences*: for the target, for the attackers, and for the environment;
- *Worst-case scenario*: Where the attack stopped, how it could have gone further, and why it did not.

Most studies will be based on open-source information, so it is possible that some specific aspects of the attacks may be more detailed than others.

4.1 Operation Megaupload

On January 9 2011, the FBI (Federal Bureau of Investigation, 2012) announced the indictment of seven individuals, including Kim Schmitz, alias Kim Dotcom, and two companies, one of which was called *Megaupload Limited.* They were charged with "engaging in a racketeering conspiracy, conspiring to commit copyright infringement, conspiring to commit money laundering, and two substantive counts of criminal copyright infringement." The FBI describes the action as being "among the largest criminal copyright cases ever brought by the United States."

Megaupload.com was one of the most popular content-sharing websites on the planet. It accounted for 4% of the total Internet traffic, had 150 million registered users and 50 million daily visitors. Unofficially, it was one of the main "direct download[3]" platforms for content such as the latest movies, series, games, or music - usually copyrighted.

Anonymous reacted very badly to this. While megaupload.com was indeed used for storing copyrighted material, it also served as a file-sharing platform for legal content. The sudden shutdown and seizure of the totality of the files on megaupload.com was seen by Anonymous as a clear violation of freedom of speech, and, by extension, human rights.

4.1.1 Critical mass

It did not take long before the channel `#OpMegaupload` was created on Anonymous' IRC server. Immediately, swarms of people joined. One of the members said the amount of people on the channel was one of the highest he had seen since he had joined the movement, when Anonymous was still focused exclusively on the Church of Scientology.

[3] Type of file sharing where the data transfer occurs entirely from the server to the user, as opposed to the peer-to-peer (P2P) model, where data flows from user to user.

What makes the case of Megaupload really interesting is all the power that the event itself invested in Anonymous' momentum. Granted, some Anonymous members were concerned about freedom of speech and human rights. But the extremely high attendance rate, and the amount of newcomers ("fresh blood", to use Anonymous' terms), also showed that the "general public" felt concerned by this. Did it feel concerned by the alleged human rights violation, or by the fact that they would not be able to watch their favorite series easily anymore? The answer to this question is left as an exercise to the reader…

The amount of people that had joined the movement was so large that critical mass was easily attained to take down the websites of the US Department of Justice, Universal Music Group, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), Broadcast Music Inc. (BMI), and the FBI.

4.1.2 Distributed Denial of Service attacks (DDoS)

Then DDoS campaign against the aforementioned websites was, according to Anonymous, "the single largest Internet attack in history" (RT, 2012). Distributed Denials of Service (DDoS) occur when a large number of hosts flood the targeted network or host with random data of fallacious connection attempts. A simple Denial of Service (DoS) counts only one host on the attacking side, and usually exploits a specific flaw in the target system to make it unresponsive.

A DDoS attack is classically launched from a *botnet*. A botnet is a network of computers that have fallen under the control of one same attacker, usually by means of viral infection. The infected computers are called *bots* or *zombies*. In order to cover its traces, the botnet owner (*botmaster*) will usually use other infected hosts as Command and Control (C&C) servers. Instead of connecting directly to the botmaster, the bots will connect to the C&C servers and receive the botmaster's orders from there.

Running a botnet has its advantages. Botnet time can be rented to spammers to send bulk emails, or to criminals who want to launch a punctual DDoS attack against a host. In a more Orwellian world, a larger botnet could be even used in a Spying-as-a-Service infrastructure!

4.1.3 Opt-in DDoS

Anonymous has been notorious for their successful DDoS campaigns. Whether they use botnets or not is not clear, but the official version is that their DDoS do not come from zombie hosts, but from real people, opting-in to the attacks. What kind of software supports this?

4.1.3.1 LOIC / HOIC

LOIC (Low Orbit Ion Cannon) and HOIC (High Orbit Ion Cannon) were widely used in these DDoS attacks, but also against previous targets of Anonymous, such as the Church of Scientology, or the financial companies targeted during Operation Payback (Wikipedia, 2011).

LOIC and HOIC are both participative DDoS tools. The concept is simple: people willing to participate in the operations have to install the software on their computers, and activate a feature called HIVEMIND. The software will then automatically recover the targets coordinates from a specified IRC server and launch the attacks. This allows people in control of the IRC server to precisely coordinate attacks, instead of relying solely on human-to-human communication through IRC channels or Twitter.

LOIC uses a combination of TCP and UDP flood in order to (hopefully) clog up the victim's bandwidth. Unfortunately for the attackers, LOIC does not spoof the source address of the packets sent, which makes identification of the perpetrators trivial. Besides, IP spoofing could easily be implemented in LOIC since it does not rely on full TCP connections.

HOIC, on the other hand, completes a TCP connection to the web server (once again making any perpetrators immediately identifiable). HOIC is a somewhat more elaborate tool than LOIC: it allows the user to use "booster" scripts. These scripts specify arrays of user-agents and extra headers to be sent along with the HTTP request, in order to disguise actual attacks as legitimate Internet traffic. An array of URLs to request can also be specified in the scripts (one would think to include URLs which are the most resource consuming, like the ones executing heavy database operations).

Traffic could be anonymized by the use of a web proxy, but HOIC does not seem to support them natively. On the other hand, both LOIC and HOIC could be tunneled through a VPN. Onion routing systems such as Tor could also be an option, although the network's latency is too high for such bandwidth-demanding attacks.

These tools are not very impressive from a technological standpoint. However, the ability to use scripts in HOIC and the HIVEMIND feature in LOIC make them evident choices for any group of people wanting to carry out opt-in DDoS attacks in a simple way.

Researchers at Trustwave SpiderLabs have conducted a thorough analysis of the many versions of LOIC (SpiderLabs, 2011) and HOIC (SpiderLabs, 2012). According to them, the attacks launched by these tools can be easily stopped with correct firewall or IDS/IPS rules, since the data they send has a distinct footprint. Their analysis also points out that these tools have no spoofing mechanism, making the attacks easy to trace and attackers easy to identify.

4.1.3.2 Slowloris

Slowloris (RSnake, 2009) differs from LOIC and HOIC in the sense that it actually exploits a special feature of the HTTP protocol instead of mindlessly flooding the victim with traffic. Slowloris makes an effective DoS tool for low-end web servers, since one single attacker could be able to freeze an HTTP server.

Slowloris abuses of partial HTTP requests in order to tie up all available sockets on a remote server. It slowly (hence the name) and progressively sends each header in the HTTP request at intervals just below the timeout threshold, therefore occupying each socket for the maximum amount of time. It does this repeatedly, until the server has no additional sockets to attribute to legitimate connections.

Though much more effective than LOIC and HOIC, this tool is just as anonymous as the others: since it relies on completing a TCP handshake, the IP can be easily traced back to the owner. Once again, VPNs, chained proxies, or the Tor network could be used to conceal the origin of the attacks, with the same limitations than the other tools.

4.1.4 Fallout

The DDoS campaign of Anonymous did have its 15 minutes of fame. Virtually every single media talked about Megaupload, and all the websites Anonymous brought down in their anger. However, DDoS (and DoS, for that matter), usually do not have lasting effects on their victims: the site remains down for as long as the bots are active and goes up not long after the attacks stop. Only availability is affected – no data is otherwise destroyed, copied, or altered.

The same cannot be said for the attackers. In fact, participating in distributed denial of service attacks can have severe consequences. On July 19 2011, over 20 people were arrested in relation with the attacks on Paypal, as part of Anonymous' "Operation Avenge Assange" (BBC News, 2011), (U.S. Department of Justice, 2011). Users running these tools through VPNs or proxy servers are only as hidden as their proxy providers are legally willing to protect them… On the other hand, Anonymous (as the headless organization it claims to be) greatly benefited from the notoriety gained through these acts. Everybody knew who the Anonymous were, and what they were capable of.

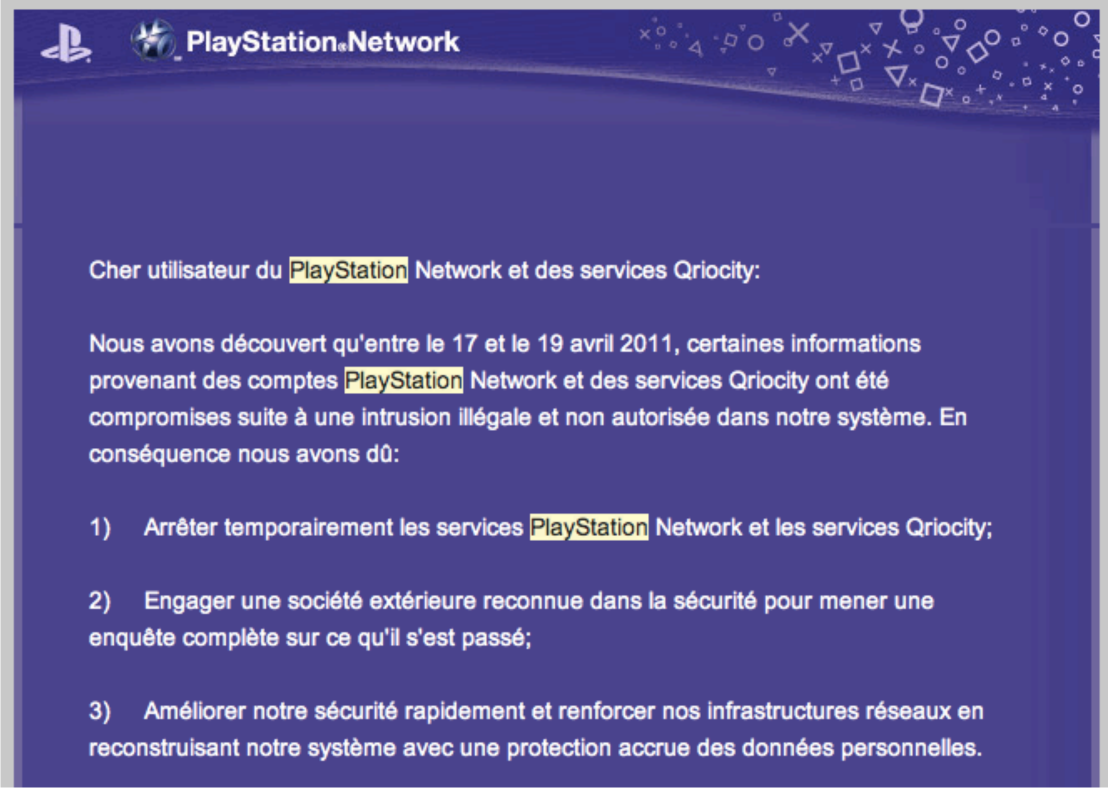
4.2 Sony and the Play Station Network

It is fair to say that 2011 was a very bad year for Sony Corporation (The Tech Herald, 2011). The outage following the attack on Sony's "Play Station Network" in April of the same year was dubbed of the most important security incidents in history (CBC News, 2011). The security website *attrition.org* runs a pretty concise history (Security Curmudgeon, 2011) of all the security incidents that Sony had to face between April and October 2011, counting no less than 21 security incidents. The website specifies that there is no evidence pointing towards any kind of coordination between separate attacks.

4.2.1 First breach by unknown attackers

On April 26 2011, Sony publicly admits to a huge breach during April 17 and April 19. This breach was first attributed to Anonymous, which had allegedly been launching DDoS attacks on Sony's networks (AnonNews) in response to their lawsuit (Engadget, 2011) on George Hotz (a.k.a. geohot) for having developed the first software jailbreak for their PlayStation 3 gaming console. This was later denied by a communiqué from Anonymous.

The consequences of the breach were massive: 77 million records were extracted from their databases, including personal information such as names, physical and email addresses, Play Station Network credentials, and possibly credit card information (Dataloss DB, 2011). In a letter to the American Congress (Sony, 2011), Sony's forensic teams estimate that the "intruders had used very sophisticated and aggressive techniques to obtain unauthorized access, hide their presence from system administrators and escalate privileges inside the servers.” (Industry Gamers, 2011)



Cher utilisateur du PlayStation Network et des services Qriocity:

Nous avons découvert qu'entre le 17 et le 19 avril 2011, certaines informations provenant des comptes PlayStation Network et des services Qriocity ont été compromises suite à une intrusion illégale et non autorisée dans notre système. En conséquence nous avons dû:

1) Arrêter temporairement les services PlayStation Network et les services Qriocity;

2) Engager une société extérieure reconnue dans la sécurité pour mener une enquête complète sur ce qu'il s'est passé;

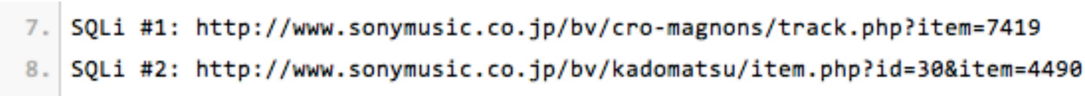
3) Améliorer notre sécurité rapidement et renforcer nos infrastructures réseaux en reconstruisant notre système avec une protection accrue des données personnelles.

Figure 2: Email received from Sony Corp. after the April breach

4.2.2 LulzSec attacks

Even though the perpetrators of the first attack and their methods remain unknown to the public (Anonymous is strongly suspected, but denied the facts), not all groups that attacked Sony in 2011 were as low profile.

On May 23, the hacking crew known as *LulzSec* published a pastebin document announcing that they had dumped the databases of a Japanese branch of Sony, `www.sonymusic.co.jp` (Pastebin, 2011). As proof, they published their database structure right under their announcement. But this time, the attack vector is clearly specified: LulzSec used SQL injections on two different pages.



```
SQLi #1: http://www.sonymusic.co.jp/bv/cro-magnons/track.php?item=7419
SQLi #2: http://www.sonymusic.co.jp/bv/kadomatsu/item.php?id=30&item=4490
```

Figure 3: The vulnerable URLs used by LulzSec on the sonymusic.co.jp site

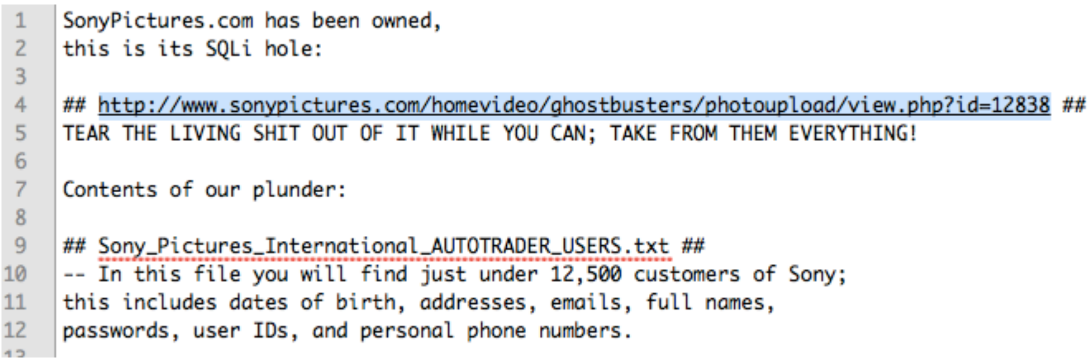
On June 2nd 2011, LulzSec hit Sony again, this time defacing their main site, `SonyPictures.com`, and compromising over 1 million user accounts and their personal data (Pastebin, 2011). The method used is also disclosed, as LulzSec is amused to point out (emphasis added):

“Our goal here is not to come across as master hackers, hence what we're about to reveal: ***SonyPictures.com was owned by a very simple SQL***

***injection**, one of the most primitive and common vulnerabilities, as we should all know by now.*

From a single injection, we accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?"

They also provide the URL used for the attack (The Pirate Bay, 2011):



```
SonyPictures.com has been owned,
this is its SQLi hole:

## http://www.sonypictures.com/homevideo/ghostbusters/photoupload/view.php?id=12838 ##
TEAR THE LIVING SHIT OUT OF IT WHILE YOU CAN; TAKE FROM THEM EVERYTHING!

Contents of our plunder:

## Sony_Pictures_International_AUTOTRADER_USERS.txt ##
-- In this file you will find just under 12,500 customers of Sony;
this includes dates of birth, addresses, emails, full names,
passwords, user IDs, and personal phone numbers.
```

It seems SQL injections are a major tool in the arsenal of low-resource attackers such as hacktivist groups or crews like LulzSec. As can be seen in attrition.org sum-up, these were not the only two SQL injection attacks carried out on Sony over 2011.

4.2.3 SQL injections

SQL injections are the most prevalent vulnerability in web applications. It comes first (along with all other injection attacks) in OWASP's (Open Web Application Security Project) 2010 Top Ten vulnerabilities for web applications (OWASP, 2010), especially those implemented in ASP or PHP. Administrators are advised to consider the severity level of SQL injections as high.

OWASP defines SQL injections as follows (OWASP, 2012):

"A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands."

For example, consider the following query:

```
SELECT id, name, description, price
FROM items
WHERE category id=$parameter;
```

In this case `$parameter` is user supplied, and probably expects an integer as an argument. To follow the first example in Figure 2, consider the following URL:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php?item=7419
```

The query will look like this:

```
SELECT id, name, description, price
FROM items
WHERE category id=7419;
```

This will retrieve the record with an `id` value of `7419` from the database. An attacker can then manipulate the parameter in order to manipulate the final query. For example, the attacker could change the URL to:

```
http://www.sonymusic.co.jp/bv/cro-magnons/track.php?item=-1 UNION
SELECT id, last_name, cc_number, cvv FROM credit_card_info
```

The resulting query will be:

```
SELECT id, name, description, price
FROM items
WHERE category id=-1 UNION SELECT id, last_name, cc_number, cvv FROM
credit_card_info;
```

Assuming a `credit_card_info` table exists, all the selected data (database ID, last name of cardholder, credit card number, and CVV code) will be displayed on the attacker's browser, since the SQL engine will interpret a new query.

The attack depicted above is really simple, and is called UNION-based SQL injections. Other scenarios could involve the use of more advanced techniques, such as blind SQL injections or out-of-band channeling, manually or by using automated tools.

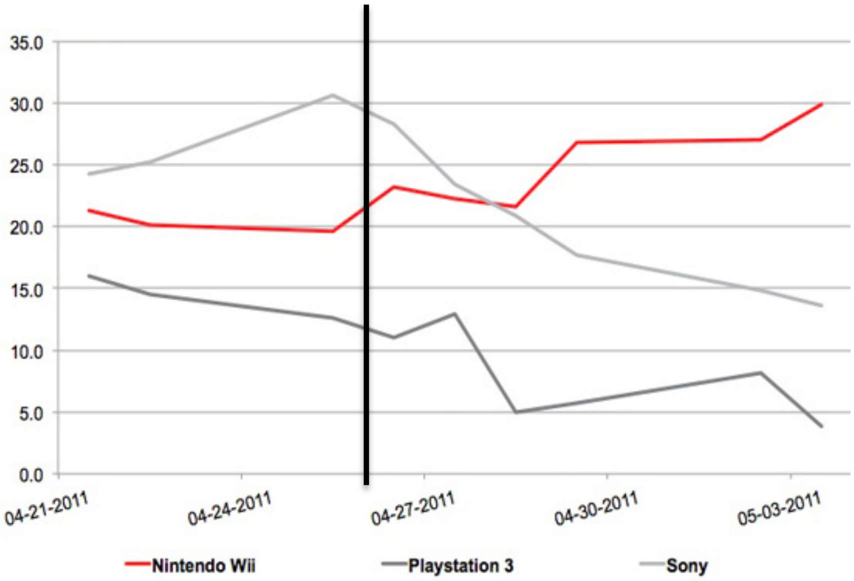
Countermeasures can be taken in order to prevent web applications from being vulnerable to such simple SQL injections. Their ease of implementation can vary according to the security level needed (escaping SQL control characters, validating user input, parameterized requests, setting up Web Application Firewalls), and backend architecture (MySQL, MSSQL, Hibernate, Oracle...).

The simplicity of SQL injections, combined with the prevalence of vulnerable architectures has drawn the interest from both security professionals and individuals with malicious intentions. Special tools have been released that automate the process of detecting and exploiting SQL injections, such as Havij or sqlmap.

4.2.4 Fallout

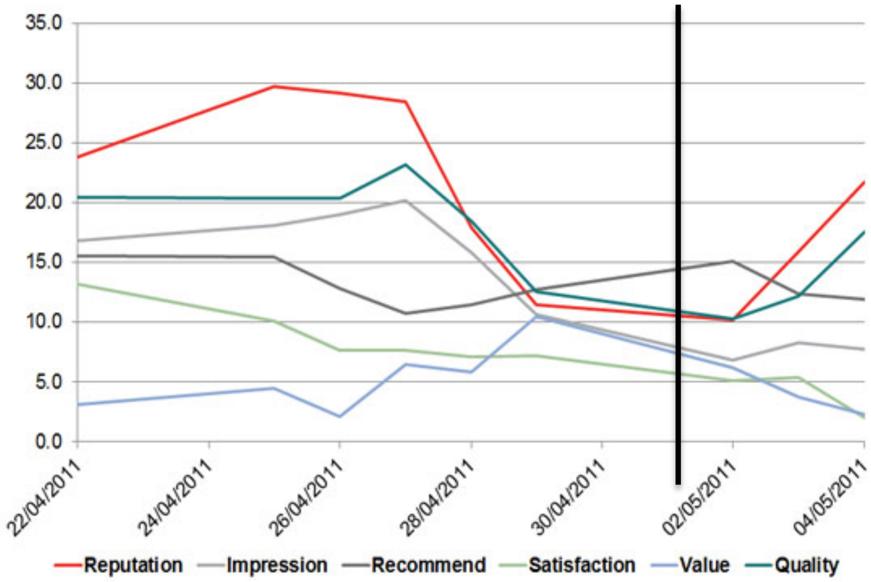
The 21 attacks on Sony Corporation's systems were not without consequences. First of all, the reputation of the Sony brand started to plummet. Who wants to give credit card information to a company who is not serious enough to keep them safe? How come the hackers' statements that Sony was breached with very simple attacks contradict Sony's initial mention of "highly sophisticated attacks"?

Since the disclosure of the first breach (April 26 2011), Sony's reputation started to plummet, as can be seen in the chart below (BrandIndex, 2011).



Graph 1: Game Console Brand Scores, taken from www.brandindex.com. The black marker corresponds to the date of April 26 2011.

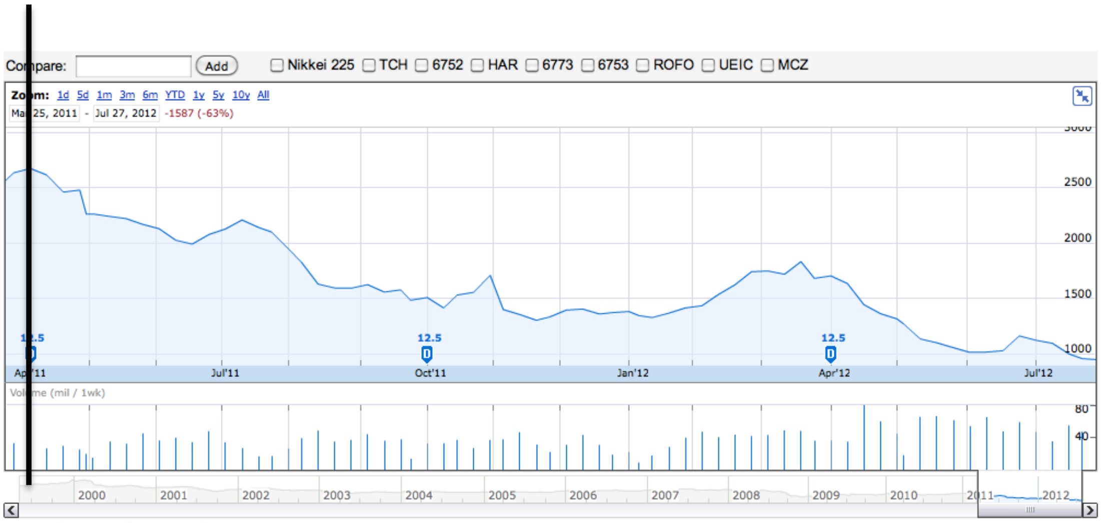
However, when Sony publicly apologized the breaches on May 1st 2011 and started communicating on the incidents (Neohapsis, 2011), their reputation slowly started rebuilding.



Graph 2: Game Console Brand Scores, taken from www.brandindex.com. The black marker corresponds to the date of May 1st 2011.

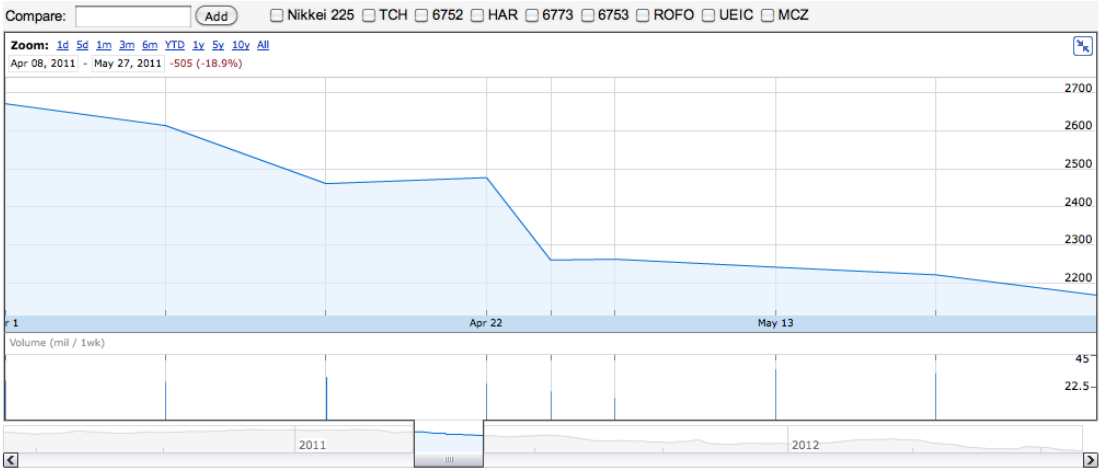
The Tech Herald interviewed with field experts in order to better explain which consequences Sony was about to face (The Tech Herald, 2011). Most predictions were that no long-term brand degradation was issued, and almost all of them insisted that the best public-relations posture a company could have when facing this kind of events is to publicly communicate on the issue.

The stock market was not as forgiving:



Graph 3: Sony Corp's stock value since April 2011 (black line)

A gradual fall in Sony's stock value can be noticed since April 2011. Given the current global economical context, it is hard to say if the attacks were the reason behind the long-term fall, but it is safe to say that it did not help Sony's situation on the short run:



Graph 4: Sony Corp's stock value from April 05 to May 30 2011

In one of their communiqués, LulzSec states:

"Due to a lack of resource on our part (The Lulz Boat needs additional funding!) we were unable to fully copy all of this information, however we have samples for you in our files to prove its authenticity. In theory we could have taken every last bit of information, but it would have taken several more weeks."

What else could have happened if they had taken additional information? The financial and reputational impact on Sony would have certainly been much worse. If the hackers had had access to all of their systems (corporate financial information, intellectual property, etc.) and crippled them, Sony could have had a very hard time to fully recover. In this case, it seems that the hackers were stopped by a lack of resources (and probably fear of being caught if they had stayed longer). One would also hope that corporate and business systems were run on a network isolated from the attacked web servers.

4.3 HBGary Federal

It seems that Sony's attacks were not politically motivated, besides for the initial DDoS attack from Anonymous (which, as previously stated, was in response to George Hotz's lawsuit against Sony).

The case of HBGary Federal is different. The attackers were chasing companies that have deep ties within the political and military entities of the United States government. This not only makes operations more "risky" in terms of getting caught, but also includes a non-negligible part of political disagreement.

HBGary Federal was a technology security company that provided services to the US government and many of its agencies. It was a subsidiary of HBGary Inc. (founded by Greg Hodlund), which provided similar services for the private sector. HBGary Federal caught the attention of Anonymous after its CEO, Aaron Barr, started claiming that he could use social media in order to track down the real identities of Anonymous' top members back in 2010. Some time later, Barr declared that he actually was in possession of said identities and was ready to disclose them at the BSides security conference in San Francisco in February 2011, in a talk titled "Who needs NSA when we have Social Media?" (Ars Technica, 2011).

These claims did not please Anonymous. Ars Technica runs an excellent 3-part story (Ars Technica, 2011) on how they started penetrating HBGary Federal's networks. The interview the Ars Technica reporter had with one of the five-member team who broke into their servers is enlightening, and is a perfect illustration of what can go *worse* once a frontend webserver gets compromised.

It is important to point out that this attack differs greatly from the other two in terms of skill and wit. The attackers showcased great technical skills, knowing exactly what to do in every situation. They also went much further to attain their objectives, taking the risk to stage social engineering attacks. This, as we will see later in the report, is key to understanding the part played by hacktivist groups in cyberattacks.

4.3.1 CMS vulnerabilities

HBGary Federal was running a website on `www.hbgaryfederal.com`. The website displayed dynamic content, which implied a database backend and probably a nice and clean content-management system (CMS) for non-technical people to be able to update it. The CMS itself was not an open-source CMS such as *Drupal*, *Wordpress*, *Joomla*, or *Spip*, all of which benefit from an active community and regular bug fixes, patches, and updates. Instead, HBGary chose to have a custom-built CMS.

Anonymous was quick to find an SQL injection bug in the web application, on this precise URL:

```
http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27.
```

One (probably both) of the parameters `pageNav` and `page` were vulnerable to injection. At this point, as we have seen, it was trivial to recover the contents of the entire database, including the usernames and passwords of the people in charge of updating the website's content.

4.3.2 Weak password policy

Anonymous got hold of the website passwords, which had been previously hashed using the MD5 algorithm.

MD5 is a cryptographic hash function. Basically put, a hash function takes arbitrary data as input (in this case, a plain-text password) and outputs a deterministic 16-byte hash value, in such a way that the original data cannot be deduced from the hash. It is worth noting that the security of MD5 has been severely compromised over the years (J. Black, 2006) (Arjen Lenstra, 2005), and very large rainbow tables (pre-calculated key–hash tables used to accelerate the cracking process) have already been computed. The use of stronger, more collision-resistant algorithms such as SHA256 is now recommended.

MD5 is inherently weak, but could be strengthened by the use of iterative hashing or salting. Unfortunately, none of these methods were implemented in HBGary Federal's CMS. This allowed the use of rainbow tables, and passwords were recovered virtually instantly: both the CEO (Aaron Barr) and COO (Ted Vera) used six lowercase letters and two numbers in their passwords. These passwords could also have easily been compromised using a classical brute-force attack on MD5.

To make matters worse, these users' passwords were reused across a number of other websites: Twitter, LinkedIn, and, more importantly, their owners' email accounts.

Anonymous did not stop there. They used Ted Vera's credentials to log onto the SSH server located at `support.hbgary.com`, and snooped around. Gaining root access in this case was trivial, since the system was outdated and ready-to-use exploits to elevate privileges could be easily found online (Ormandy, 2010). Once this was accomplished, they had access to several gigabytes of backup data.

4.3.3 Social Engineering

The most interesting part of the HBGary attack was the way they used Aaron Barr's credentials. Barr also reused passwords across a number of sites, including his corporate email. In fact, HBGary used Google Apps to manage their emails, and Barr was one of the administrators. By getting into Barr's Google Apps account, they had access to the email spool of virtually the entire company. Special attention was given to the account belonging to the CEO, Greg Hodlund, who owned a separate website at `rootkit.org`.

The stunt that Anonymous pulled off with the information obtained through the email account could serve as a lesson for many a system administrator. They found emails indicating that the root passwords for `rootkit.com` where either `88j4bb3rw0cky88` or `88Scr3am3r88`. They also noticed that Jussi Naakonaho, Chief Security Specialist at Nokia, also had root access to that computer, and therefore the ability to change and reset passwords. As a security measure, logging in remotely as `root` was disabled. Therefore, they needed to get in as a normal user, and then elevate privileges to gain control on the server.

In a bold social engineering attack, they proceeded to exchange emails with Naakonaho, successfully getting him to open an SSH access and reset Hodlund's password. Below is the transcript of the email exchange, posted on pastebin on Februrary 8 2011 (Pastebin, 2011) (emphasis added).

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 1:59 PM
To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
thanks

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:06 PM
To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at 2:08 PM
To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because im ready
for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public
ip and ill ssh in and reset my pw.

From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011 at 2:10 PM
To: Greg Hoglund <greg@hbgary.com>
ok, takes couple mins, i will mail you when ready. ssh runs on 47152

A few moments later, they had root access to Hodlund's server.

4.3.4 Fallout

Needless to say, this incident had extremely severe consequences on HBGary's business and personnel.

Firstly, the stolen documents and emails revealed that HBGary Federal had been working tightly with Bank of America in order to prepare a response to the disclosure of confidential documents Wikileaks was planning to release since 2009 (ComputerWorld, 2009). The response was to be prepared by Hunton and Williams, a law firm recommended by the Department of Justice to Bank of America. Along with Palantir Technologies, Berico Technologies, and HBGary, Hunton and Williams would find a way to bring down Wikileaks and discredit its founder, Julian Assange.

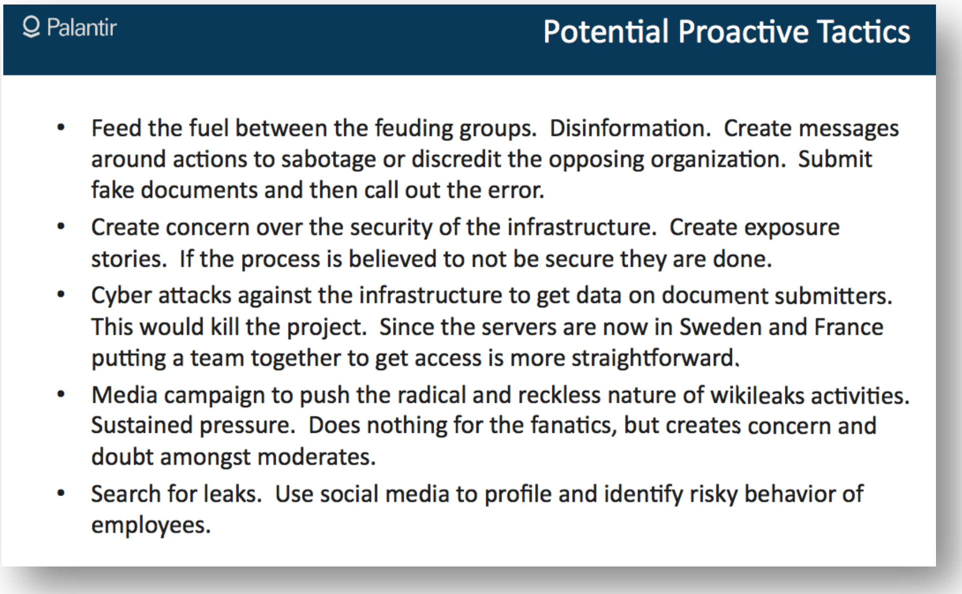
The methods that were going to be used were unconventional at best, illegal at worst (Wikileaks) (See Figure 4)

This not only tarnished HBGary Federal's reputation, but all companies involved distanced themselves from HBGary. The US Chamber of Commerce denied the allegations (Free Enterprise, 2011), and Palantir and Berico severed all ties with HBGary Federal (The Tech Herald, 2011). Aaron Barr resigned (Threatpost, 2011) shortly after.

Financially, this attack cost a lot to both HBGary and HBGary Federal, which was about to be sold at about the exact same time Anonymous attacked. The sale was apparently cancelled. HBGary Federal ceased to exist and HBGary was sold to ManTech International one year later (Bizjournals, 2012).

This might be one of the incidents Anonymous could be the proudest of. The publicity campaign they had was enormous – the story was mentioned in many newspapers worldwide. Besides, Anonymous was lucky to find and release material that showed that HBGary was in an active campaign against Wikileaks. It helped in making the attack popular with public opinion, and strongly contributed to the "Robin Hood" dimension of their movement.

As for HBGary and Aaron Barr, it probably could not have been much worse. Barr resigned, and HBGary's reputation was tarnished. Even one year later, at least everyone remembers HBGary as "the computer security company who was owned by Anonymous". Or as "the interwebz" would put it: EPIC FAIL (see Figure 5).

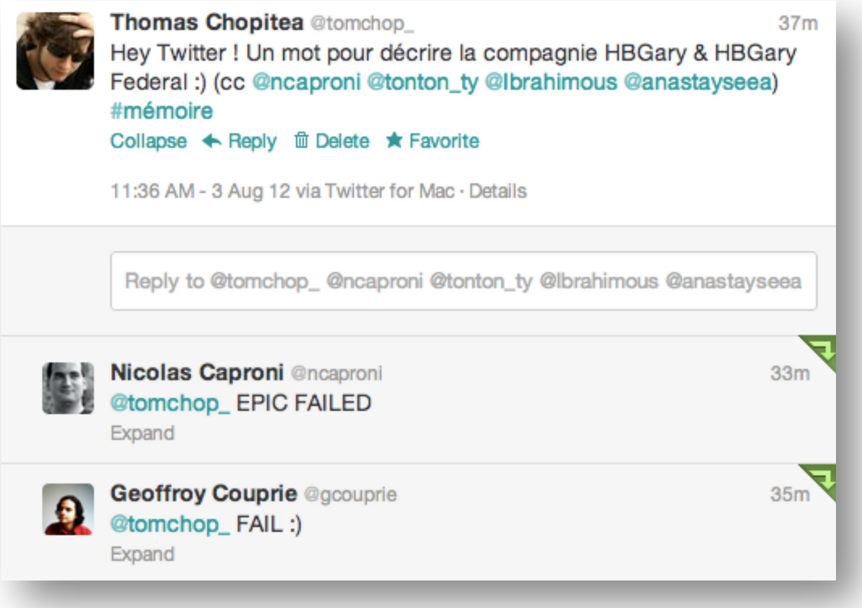


Palantir

Potential Proactive Tactics

- Feed the fuel between the feuding groups. Disinformation. Create messages around actions to sabotage or discredit the opposing organization. Submit fake documents and then call out the error.
- Create concern over the security of the infrastructure. Create exposure stories. If the process is believed to not be secure they are done.
- Cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France putting a team together to get access is more straightforward.
- Media campaign to push the radical and reckless nature of wikileaks activities. Sustained pressure. Does nothing for the fanatics, but creates concern and doubt amongst moderates.
- Search for leaks. Use social media to profile and identify risky behavior of employees.

Figure 4 : Extract of the presentation describing the plan to bring WikiLeaks down



Thomas Chopitea @tomchop_ 37m

Hey Twitter ! Un mot pour décrire la compagnie HBGary & HBGary Federal :) (cc @ncaproni @tonton_ty @Ibrahimous @anastayseea) #mémoire

11:36 AM - 3 Aug 12 via Twitter for Mac · Details

Reply to @tomchop_ @ncaproni @tonton_ty @Ibrahimous @anastayseea

Nicolas Caproni @ncaproni 33m

@tomchop_ EPIC FAILED

Geoffroy Couprie @gcouprie 35m

@tomchop_ FAIL :)

Figure 5: A tweet answering the question "One word to describe HBGary and HBGary Federal"

5 THE THREAT MODEL OF HACKTIVIST GROUPS

The basis of threat modeling is to understand and predict how a system can be vulnerable to different attacks. Although the usual definition of threat modeling implies building a security model at design time, in this specific case we will be taking an attacker-centric: understanding the attacker in order to be one step ahead of him.

This section will evaluate the credibility and importance of the threat represented by hacktivists and hacktivist groups. Their attacks will be confronted to reality, from the perspective of a security-savvy person. We will do a thorough assessment of the following characteristics:

- Their technical skills and the complexity of the attacks and tools employed;
- Their motives and goals, and how far they are willing to go to pursue them;
- Their target-selection criteria.

Evaluating the technical threat is crucial to predict their actions and estimate the amount of damage they could inflict on individuals, organizations or governments.

How this threat fits into the geopolitical landscape will be discussed in the next section.

5.1 Technical skills

The hacktivist campaigns covered in this paper vary greatly in display of technical knowledge.

DDoS attacks like the ones we have seen require little or no technical knowledge to execute. The "average" Internet user could launch them. It could be said that the only real know-how comes from the people or organizations behind the software – usually, they have nothing to do with hacktivist groups.

- *LOIC* is a stress-test tool designed by Praetox Technologies (Praetox Technologies, 2009);
- *Slowloris* was built by hacker / security researcher RSnake (RSnake);
- *sqlmap* was developed by information security researchers Bernardo Damele A. G. and Miroslav Stampar;
- *Havij*, a windows-based SQL injection client, was developed by ITSecTeam.

SQL injection attacks require more skill than simply clicking on a button to launch a DDoS attacks. Most simple injections remain within the grasp of any computer literate individual, but harder ones could tend to quickly discourage most of them. Tools like sqlmap are very welcome in this case, even for the hardened penetration tester looking to exploit a complicated blind SQL injection.

Then again, the attacks launched by these tools are easy to detect. As we have seen before, LOIC usually sends the same type of requests to the webserver, making signatures trivial to establish. The case with HOIC is a little more complicated: custom configuration can be used to modify the request for each target (e.g. user-agent, requested URL). But common patterns such as the order in which headers are sent can easily be used to establish an attack signature. sqlmap and havij both use custom user-agents when executing their SQL injection attacks, which can easily be detected.

5.1.1 Similarities with Advanced Persistent Threats

Some of the media has categorized hacktivist groups as Advanced Persistent Threats (APTs). APTs refer to entities with the determination, knowledge, time, and resources to effectively target and penetrate into a network. The term APT is usually employed when talking about government-sponsored attacks, such as Operation ShadyRAT (Reuters, 2011) or Operation Aurora (Google Blog, 2010). These cyber-espionage campaigns were carried out over several years, and were aiming at extremely high-value targets. Both operations targeted a big number of organizations: private companies (including Google), defense contractors, the United Nations. Stuxnet, the trojan that infected the industrial control systems in the Iranian nuclear facility of Natanz, was a joint U.S.-Israeli operation called “Operation Olympic Games” (The New York Times, 2012). The cyber-espionage malware dubbed “Flame” was also part of the same operation. Both pieces of software used state-of-the art technology. They exploited several 0-day vulnerabilities (BBC News, 2010), both in their target’s software and in well-known cryptographic primitives (CWI, 2012). These operations all fall into the category of Advanced Persistent Threats, and show a level of technical skill and resources still far from what hacktivist campaigns seem to be capable of nowadays.

Malware attacks, which are typical of APTs, are definitely not amongst the hacktivists’ weapon of choice. Some examples of hacktivists using tailored software exist (e.g. the use of modified versions of HOIC or botnets), but the creative efforts of hacktivists remain slim in comparison to those of state-sponsored threats. This can be partially explained by the ever-changing nature of their targets, which is not compatible with the long-term objectives that the creation and use of tailored malware entails. Besides, the cost of creating such malware, in terms of technical skills and time, are too high for the typical hacktivist agenda, which privileges high reactivity at the cheapest possible price.

Furthermore, most hacktivist campaigns (e.g. DDoS, defacements, minor data dumps) could be discarded as the work of “script kiddies” or as opportunist attacks. That being said, some of these attacks go far beyond simple defacement or denial of service; it is then fair to say that they share similarities with Advanced Persistent Threats. In these cases, attackers had a real will to do maximum damage and penetrate deep into their targets’ systems. The use of high-risk methods, such as social engineering, and the exploitation of several well-found (albeit basic) security flaws show that not all targets are targets of opportunity, but are carefully planned from the start. *From this, we can deduce that a minority of individuals within these hacktivist communities does possess the skills necessary to represent a threat to the average organization.*

5.2 Motivations

Classic cybercriminals always strive to find a balance between ease of exploitation and profitability. If a target requires too much investment for the profit it may yield, then the attack will not go through.

Even though hacktivists are not looking for monetary gain, they follow a similar logic. If what cybercriminals want is money, then what hacktivists want is attention. Their goal is to be heard, whatever the means, and as loudly as possible, so that their political agenda reaches the most people. Media attention is the driving force of the hacktivist economy.

Chaotic as they are, they have shown an incredible faculty to adapt to their environment. When the FBI surprised the world by seizing Megaupload by surprise, Anonymous' IRC channels was crawling with people from all over the world wanting to "help". Organization was chaotic at best. Targets were being dealt randomly, and people were having trouble following instructions, from setting up HOIC to launching it simultaneously. Nevertheless, their targets were brought down long enough for the media to notice and speak of "the retaliation of Anonymous".

Hacktivist groups may have a chaotic organization, but that is specifically what allows them to have such a great adaptability. Since there was nothing to react to, LulzSec had much more time to plan their attacks on Sony – they went further than the simple DDoS and got the media attention they wanted. A thirty-minute downtime on Sony's systems would probably have gone unnoticed from the media. The attacks on HBGary were well executed; even more so that the emails the attackers retrieved were quite compromising for the company. Anonymous hit the jackpot on this one: not only they had compromised a cyber-security company with ties deep into the government, but they had also retrieved actual proof of how "evil" they were. How could the media ignore this scandal?

5.3 Target selection

From this, we can deduce that hacktivists, just like cybercriminals, will assess if the entity they plan of attacking is worth the trouble. They have to calculate media profitability: small amounts of high-profile hacks (HBGary, Stratfor, Sony, etc.) or many low-profile hacks (countless defacements, targets of opportunity, doxing, etc.). Will spending ten hours attacking this server will attract enough media attention? Or is it better to spend one hour defacing ten different websites?

A hacktivist working on its own can individually choose whether an organization "deserves" to be attacked or not. A member of Anonymous will submit his proposal to the community through IRC. If his proposal sticks with the moral values of the group, it may attract the community's interest and end in a full-blown attack project, depending on the target's profile, and the ability to successfully break into their systems.

An interesting example of this idea is Imperva's study on attacks on the Vatican's website (Imperva). The paper follows the attack from start to finish, basing their deductions on Imperva's Web Application Firewall logs. They distinguish three phases in the attack:

- Recruitment over social networks and IRC;
- Reconnaissance and web application attack;
- If the application attacks fails, then a DDoS attack is attempted, after gathering enough volunteers by means of a publicity video.

Targets of opportunity are selected by searching the web (or "Google dorking"[4]) for vulnerable web-applications, and then decide which server in the list is worth attacking. If the attack succeeds, it is then publicized or at least notified. If it is unsuccessful, then no report is made whatsoever, and the attack is probably never heard outside of the hacktivist community since it would bring bad publicity to the group.

As a side note, attacks announced by hacktivist groups before they are actually carried out are rare. Imperva points out that the threats against Facebook the Mexican drug cartels have been inconclusive (and so have been their threats against the root DNS servers) (Pastebin, 2012). This leads us to believe that the majority of their targets are in fact targets of opportunity rather than carefully chosen targets.

Hacktivist groups are usually after easy targets, whose compromise would have a high media impact. How they find and select targets is closely related to the balance these two characteristics.

[4] Google dorking is the act of using the Google search engine with specific queries ("dorks") that yield vulnerable webpages or servers. Results can be filtered to contain specific top-level domains (e.g. .mil, .gov)

6 HACKTIVISTS AND GEOPOLITICS

In addition to media and the general public, hacktivism has also managed to attract the attention of governmental agencies. In January 2012, the FBI declared that the "cyberthreat, which cuts across all [FBI] programs, will be the number one threat to the country" (ABC News, 2012), beyond the terrorist threat. The National Security Agency said that Anonymous could probably attack the national power grid (CNET News, 2012). Attempts have been made to infect hacktivist tools with malware (Symantec, 2012), with efforts going as far as creating a special operating system, Anonymous OS (The Next Web, 2012).

This section will show that hacktivist groups make excellent targets for manipulation. Placing ourselves in a geopolitical context, we will examine the permeability of hacktivist networks (i.e. how easily they can be infiltrated by third parties, both well- and ill-intentioned), and how they can be used as gambits in false-flag operations. Finally, we will assess the plausibility of them executing attacks against the power grid or other critical infrastructure.

6.1 Infiltrating hacktivist networks

On March 6 2012, law enforcement agents arrested five top members of the LulzSec crew. LulzSec "mastermind", Hector Xavier Montsegur – a.k.a. Sabu – had ben arrested by the FBI and turned confidential informant in August of the previous year. He greatly helped FBI efforts to track down the identities of the rest of the LulzSec crew. This shows how delicate trust schemes in hacktivist group are.

This is the main flaw in the internal trust model of hacktivist groups. Members hardly know each other, but then again are willing to share a certain degree of personal information. Jeremy Hammond – a.k.a. Anarchaos – had confessed to Monstegur that he had been arrested in New York City in 2004, and then again during a "Midwest Rising" protest in August 2011, and that he had served time in a federal prison. This was enough for the FBI, with whom Montsegur was working, to track down and arrest Hammond. Hammond had no reason to doubt his brother-in-arms, and was confident enough to share details that could have been irrelevant, had Montsegur not been turned by the FBI.

6.2 Hacktivism and terrorism

If a hacktivist can be turned to work for the FBI, why would he be impervious to attempts from terrorist organizations to turn them? In an interview with Security & OSINT analyst Scot Terban, it came clear that the "online Jihad" was not yet a reality.

Mr. Terban pointed out that Jihadist terrorists had mostly been using the Internet as some form of command, control and recruitment through radicalization and propaganda. They also may create revenue streams from classic online crime, but there has been no evidence of them trying to infiltrate the ranks of Anonymous or other hacktivist groups. Mr. Terban thinks this will eventually change, but that jihadist terrorists are currently not savvy enough on cyber terror or cyber warfare strategies.

In theory though, infiltrating a hacktivist group could be as easy as placing an asset in their IRC channels, create a fake persona, and start building a reputation, or just try to steer general opinion towards targets on a secret agenda. Mr. Terban's opinion is that it will not be the work of jihadists, but more the work of nation-states.

6.3 False-flag operations

The nebulous and decentralized aspect of hacktivist groups has its advantages – with no leadership, it is difficult to decide which member to focus on, let alone "cut off their head". Besides, Anonymous has always claimed to be "the work of the masses". According to them, everyone and anyone can be an Anonymous, as long as they rally to the same causes, and act accordingly. This is not exactly true, since many operations that have been attributed to Anonymous (because of their distinctive logo, or the message "hacked by Anonymous" were left behind) were immediately denied by Anonymous. Apparently, there is some kind of decision-making process. A handful of people have access to their Twitter account; some people are operators in their IRC channels. Someone is in charge, but no one can be held accountable.

Groups like Anonymous benefit from a *repudiation power* that far exceeds that of any other political party, government, or organization. This makes them particularly suitable for false-flag operations. They are the perfect decoys to use, the perfect entity to point fingers to.

According to Wikipedia, False-flag operations are "covert operations designed to deceive in such a way that the operations appear as though they are being carried out by other entities". False-flag operations are especially useful during peacetime, when an entity A seeks to attack an entity B with which there is no ongoing conflict, and without triggering a full-scale war between the two parties. On the other hand, false-flag operations can also be executed to have a pretext for declaring war, or taking other measures that would otherwise have been judged unacceptable.

If a nation-state wanted to carry out a cyberattack, the use of hacktivists as false-flags would be a very good option. The attacker would leave fabricated evidence on the server pointing towards a hacktivist group, and the hacktivist group would deny it. Since this is not an uncommon scenario, the victims will probably fail to see the connection with the original nation-state. In this case, the attacker would not even need to infiltrate the hacktivist network.

False-flag operations can also be used to impact negatively on a given group. Operations could be carried out in order to turn public opinion against the hacktivist groups, which would impair the group's credibility and slowly make it disappear. Such operations could also be conceived in order to justify tighter legislation or harsher measures against hacktivist groups.

On the other hand, hacktivist groups could also be hijacked by carrying out large volumes of high-profile operations in their name. This will eventually shift attention, reputation, influence, and power on these new actors, which will have a much larger control over which targets are decided on.

6.4 Attacks on critical infrastructure

During the past years, and especially thanks to Stuxnet, SCADA and industrial process control systems have attracted a lot of interest on behalf of the information security community. Lots of research has been done in order to evaluate the risk that internet-facing SCADA devices entail, and the results are not good (Wired, 2012) (NakedSecurity, 2011). Search engines such as Shodan (http://www.shodanhq.com/) easily allow searching for specific devices throughout the Internet. Seeing as how vulnerable these systems are, and how easy it is to find them, what are the probabilities that SCADA or PLC devices become the targets of hacktivist groups, or people posing as them?

The recent arrests of hacktivist members have shown the world that even if they try hard to cover their traces, they will eventually make a mistake, and be found. If hacktivists (or a more radical subgroup) would carry out attacks against SCADA controlled public infrastructure systems (water plants, power grid, nuclear plants, etc.) and *be found*, then they would probably be hunted down much more violently than their LOIC-waving counterparts. Consequences would be dire. Hacktivists, unlike sociopaths, understand that actions like these have consequences (it could jeopardize the lives of other people, or even their own), and will therefore refrain to go “that far”. Besides, recent large-scale attacks have shown that hacktivist groups tend to cause financial loss and try to expose corrupt institutions by releasing incriminating evidence. Hacktivists are trying to do “good” (by their standards), and have not yet resorted to extreme strategies like bringing down the power grid – and probably will not.

Terrorists, on the other hand, rely on extreme measures to send their message. A serious group of jihadists with the necessary skills could pull off an attack on public infrastructure. They would not target something massive like the whole power grid, as the media would lead us to believe, but something smaller, like a water treatment plant or, at best, a hydroelectric dam. These attacks would no doubt be conducted by exploiting internet-facing SCADA systems, seeing how vulnerable they are by design. Terrorists would not make use of false-flags, since the own attribution of attacks is key in their propaganda process. That being said, they might be interested in infiltrating hacktivist networks in order to influence targets or to gather knowledge about current attack methods and techniques.

6.4.1 Threat credibility

Mr. Terban thinks that a determined attacker, with time and knowledge, could in fact carry out such an attack. “However, were it to happen and Anonymous claimed it, then I would tend to think that it was a false-flag operation by someone else (nation state) to diffuse any finger pointing at them (said nation state)”.

By the time Stuxnet was discovered and analyzed, preliminary evidence pointed towards the U.S. and Israel as the main entities behind it (Wired, 2011). Several arguments were put forward. Several 0-days were used, and the design of the virus was a perfect match to the layout of the Natanz nuclear power plant. Hacktivists could not have gone this far in their information-seeking endeavors. Besides, text strings were found in the code that referenced the Hebrew Bible (The New York Times, 2010). In this case, it would probably have been useful for the U.S. and Israel to have fingers pointed somewhere else. For political reasons, it was hard to imagine Anonymous carrying out such an operation. For technical reasons, it was even harder to imagine an independent group of anti-Iran hacktivists designing such an elaborate piece of malware. Had a false flag being used, the bluff would have been called immediately, and it would probably have given more material to further investigate the real source of the project.

7 Discussion

Throughout this paper, we have tried to understand how hacktivist groups operate, as well as the role they play in the information security scene. The study was mainly based on the groups Anonymous and LulzSec, and some of the operations they have carried out.

A first hypothesis on their *modus operandi* was built, based on open-source information. In the days of the social web, open-source information and discussion channels can provide great information when put in context with official sources. The comparison between their methods and guerilla tactics also yielded interesting leads in order to understand why they operate how they operate.

Three hacktivist operations were taken into account: The denial of service attacks in response to the Megaupload incident, the database leaks of Sony networks, and the in-depth penetration of HBGary Federal's networks. This showed us that hacktivist attacks vary greatly in elaboration, and technical difficulty.

This allowed us to build a threat model that summarizes what to expect of a hacktivist attack, to understand the risks they are willing to take and the information they are after. This was put in contrast with nation-state APTs. We pointed out the differences but also the similarities that both models share.

These similarities make hacktivist models and their repudiation capability high-value assets when considering false-flag operations. Nation-states could use hacktivist groups to carry out cyber-attacks and deflect attention towards said groups.

Terrorist groups, on the other hand, do not seek to use false-flag operations, but can take advantage of hacktivist networks by influencing targets and then claiming responsibility, by gaining knowledge, or by finding new recruits.

The degree of manipulation permitted in hacktivist groups shows the limitations of their models. This, in addition to the weak trust links that members can establish between themselves, makes hacktivist models non-sustainable on the long run.

For the time being, they do play a key part in geopolitical cyber operations. They are the perfect wildcard, and as long as false-flag operations are needed and useful, there will be a place for them. However, the recent revelations about Obama's cyber-strategy have not been commented by official government sources. Are we approaching a new epoch in which cyber-deterrence is becoming the new priority? Is showing the possession of offensive cyber-capabilities now more important than denying a full-blown attack on a nuclear power plant's systems? This might well be the dawn of a new arms race – in cyberspace.

7.1 Further improvements

The research on the major incidents was as thorough as possible. As one could imagine, not all information was openly available on the Internet, and some grey areas still remain.

One possible way of improving this research would have been to have direct contact with the hacktivists who carried out the attacks. The wave or arrests and treason within these groups made their members extremely untrusting towards newcomers. Besides, it is easy to imagine why someone would like to keep those details from a complete stranger. Trust is hard to gain, especially on the Internet, and very easy to lose. That being said, researchers like Gabriella Coleman do have a certain degree of trust and respects amongst hacktivists. This shows that participating in operations is not the only way to gain trust, even though one has to be patient and prove to the hacktivist community that they really mean no harm. More time and involvement in the hacktivist community would have been necessary.

Another way of making this research more interesting is by having direct access to a variety of logs from before, during, and after a hacktivist attacks. Running the Vatican's defensive systems allowed Imperva to come by this kind of logs, and conduct a very interesting study. First-hand access to this type of evidence would have allowed for a much more thorough analysis of hacktivist groups' *modus operandi*. Doing this thesis in a company covering these aspects of cybercrime would have been a great advantage.

8 CONCLUSION

The objective of this thesis was to establish a threat model of hacktivist groups by gaining a thorough understanding of their working methods, objectives, and organization.

In order to determine this, research was done on high-profile incidents involving different entities. A threat model was then deduced, and was applied to real-world situations by including a larger context.

Throughout this study, it becomes apparent that hacktivist groups, because of their structure, skills, and chain of command, do represent an important pawn in the larger geopolitical board.

9 Works Cited

U.S. Congress. (2006, January 6). National Defense Authorization Act for Fiscal Year 2006. U.S. Government Printing Office.

U.S. Department of Justice. (2011, July 19). *Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks.* Retrieved 2012, from U.S. Department of Justice: http://www.justice.gov/opa/pr/2011/July/11-opa-944.html

WeRebuild. (2012). *WeRebuild.* Retrieved 2012, from Telecomix: http://werebuild.telecomix.org/wiki/Egypt/Main_Page#Internet_Access

Wikileaks. (n.d.). *The WikiLeaks Threat.* Retrieved 2012, from Wikileaks.org: http://wikileaks.org/IMG/pdf/WikiLeaks_Response_v6.pdf

Wikipedia. (2011, March 29). *Operation Payback.* Retrieved 2012, from Wikipedia, The Free Encyclopedia: http://en.wikipedia.org/wiki/Operation_Payback

Wired. (2011, July 11). *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History* . Retrieved 2012, from Wired: http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/

Wired. (2012, January 19). *Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software* . Retrieved 2012, from Wired: http://www.wired.com/threatlevel/2012/01/scada-exploits/

Wired. (2012, March 06). *LulzSec Leader Was Snitch Who Helped Snag Fellow Hackers* . Retrieved 2012, from Wired: http://www.wired.com/threatlevel/2012/03/lulzsec-snitch/

ABC Australia. (2011, June 20). *Lulzsec teams up with Anonymous* . Retrieved 2012, from ABC Australia: http://www.abc.net.au/technology/articles/2011/06/20/3248520.htm

ABC News. (2012, January 31). *FBI Director Says Cyberthreat Will Surpass Threat From Terrorists.* Retrieved 2012, from ABC News: http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/

AnonNews. (n.d.). *Operation Payback brings you #OpSony.* Retrieved 2012, from AnonNews: http://anonnews.org/?p=press&a=item&i=787

Arjen Lenstra, X. W. (2005, March 1). *Colliding X.509 Certificates* . Retrieved 2012, from Cryptology ePrint Archive: http://eprint.iacr.org/2005/067

Ars Technica. (2011, February 6). *Anonymous speaks: the inside story of the HBGary hack.* Retrieved 2012, from Ars Technica: http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

Ars Technica. (2011, February 10). *How one man tracked down Anonymous—and paid a heavy price.* Retrieved 2012, from Ars Technica: http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/

BBC News. (2011, July 19). *Police arrest 'hackers' in US, UK, Netherlands* . Retrieved 2012, from BBC News: http://www.bbc.co.uk/news/world-us-canada-14212110

BBC News. (2010, September 23). *Stuxnet worm 'targeted high-value Iranian assets'.* Retrieved 2012, from BBC News: http://www.bbc.co.uk/news/technology-11388018

Bizjournals. (2012, February 28). *Cyber security firm HBGary bought by ManTech International.* Retrieved 2012, from Bizjournals: http://www.bizjournals.com/sacramento/news/2012/02/28/hb-gary-sacramento-man-tech-cyber-securi.html

BrandIndex. (2011, 5 5). *Sony security breach rattles consumers* . Retrieved 2012, from BrandIndex: http://www.brandindex.com/article/sony-security-breach-rattles-consumers

CWI. (2012, June 7). *CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware* . Retrieved 2012, from Centrum Wiskunde & Informatica: http://www.cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware

CBC News. (2011, April 27). *PlayStation data breach deemed in 'top 5 ever'* . Retrieved 2012, from CBC News: http://www.cbc.ca/news/business/story/2011/04/27/technology-playstation-data-breach.html

CNET News. (2012, February 21). *Scared of Anonymous? NSA chief says you should be.* Retrieved 2012, from CNET News: http://news.cnet.com/8301-13506_3-57381598-17/scared-of-anonymous-nsa-chief-says-you-should-be/?tag=cnetRiver

Coleman, G. (2012). *Academic Publications.* Retrieved 2012, from Gabriella Coleman: http://gabriellacoleman.org/?page_id=6

Coleman, G. (2012, January). *Our Weirdness Is Free, The logic of Anonymous—online army, agent of chaos, and seeker of justice.* (T. Canopy, Editor) Retrieved from Triple Canopy: http://canopycanopycanopy.com/15/our_weirdness_is_free

ComputerWorld. (2009, October 9). *Wikileaks plans to make the Web a leakier place* . Retrieved 2012, from ComputerWorld: http://www.computerworld.com/s/article/9139180/Wikileaks_plans_to_make_the_Web_a_leakier_place

Creveld, M. V. (2000). Technology and War II: Postmodern War? In C. Townshend, *The Oxford History of Modern War* (pp. 356-358). New York, NY, USA: Oxford University Press.

Engadget. (2011, January 12). *Sony follows up, officially sues Geohot and fail0verflow over PS3 jailbreak* . Retrieved 2012, from Engadget: http://www.engadget.com/2011/01/12/sony-follows-up-officially-sues-geohot-and-fail0verflow-over-ps/

Dataloss DB. (2011, April). *Sony Corporation Data Breach.* Retrieved 2012, from Dataloss DB: http://datalossdb.org/incidents/3634

Federal Bureau of Investigation. (2012, January 19). *Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement* . Retrieved 2012, from Federal Bureau of Investigation: http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement

Fox News. (2011, July 19). *16 Suspected 'Anonymous' Hackers Arrested in Nationwide Sweep.* Retrieved 2012, from Fox News: http://www.foxnews.com/tech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous/

Free Enterprise. (2011, February 10). *More Baseless Attacks on the Chamber* . Retrieved 2012, from Free Enterprise: http://www.freeenterprise.com/2011/02/more-baseless-attacks-on-the-chamber/

Google Blog. (2010, January 3). *A new approach to China.* Retrieved 2012, from Google Blog: http://googleblog.blogspot.fr/2010/01/new-approach-to-china.html

Industry Gamers. (2011, May 12). *PlayStation Network: Here's The Official Letter Sony Sent to Publishing Partners [Exclusive].* Retrieved 2012, from Industry Gamers: http://www.industrygamers.com/news/playstation-network-heres-the-official-letter-sony-sent-to-publishing-partners-exclusive/

InformationWeek. (2012, January 11). *Israeli, Saudi Hacker Battle Escalates* . Retrieved 2012, from InformationWeek: http://www.informationweek.com/news/security/cybercrime/232400184

Imperva. (n.d.). *Imperva's Hacker Intelligence Summary Report - The Anatomy of an Anonymous Attack.* Retrieved from Imperva: https://www.imperva.com/docs/HII_The_Anatomy_of_an_Anonymous_Attack.pdf

Haaretz. (2012, January 17). *Israeli hackers bring down Saudi, UAE stock exchange websites.* Retrieved 2012, from Haaretz: http://www.haaretz.com/news/diplomacy-defense/israeli-hackers-bring-down-saudi-uae-stock-exchange-websites-1.407846

J. Black, M. C. (2006, March 3). *A Study of the MD5 Attacks: Insights and Improvements.* Retrieved 2012, from University of Colorado: http://www.cs.colorado.edu/~jrblack/papers/md5e-full.pdf

J. Oikarinen, D. R. (1993, May 1). Internet Relay Chat Protocol. Internet Engineering Task Force.

NakedSecurity. (2011, December 13). *FBI acknowledges more SCADA attacks, increases cyber budget* . Retrieved 2012, from NakedSecurity: http://nakedsecurity.sophos.com/2011/12/13/fbi-acknowledges-more-scada-attacks-increases-cyber-budget/

Neohapsis. (2011, May 3). *[Dataloss] Sony Online Entertainment (SOE) breach letter.* Retrieved 2012, from Neohapsis: http://archives.neohapsis.com/archives/dataloss/2011-05/0001.html

OWASP. (2010, June 11). *OWASP Top Ten Project* . Retrieved 2012, from The Open Web Application Security Project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP. (2012, August 7). *SQL Injection.* Retrieved 2012, from The Open Web Application Security Project: https://www.owasp.org/index.php/SQL_Injection

Ormandy, T. (2010, October 18). *The GNU C library dynamic linker expands $ORIGIN in setuid library search path.* Retrieved 2012, from Full Disclosure mailing list archives: http://seclists.org/fulldisclosure/2010/Oct/257

Pastebin. (2012, February 12). *Untitled (Operation Global Blackout).* Retrieved 2012, from Pastebin: http://pastebin.com/NKbnh8q8

Pastebin. (2011, June 2). **V2 Update* LulzSec versus Sony Pictures.* Retrieved 2012, from Pastebin: http://pastebin.com/GyhXiWaK

Pastebin. (2011, May 23). *LulzSec hates Sony too.* Retrieved 2012, from Pastebin: http://pastebin.com/NyEFLbyX

Pastebin. (2011, Februrary 8). *owning rootkit.com* . Retrieved 2012, from Pastebin: http://pastebin.com/tSiQevxe

PC Inpact. (2011, December 27). *Déni de service : le site du Sénat toujours inaccessible* . Retrieved 2012, from PC Inpact: http://www.pcinpact.com/news/67903-senat-attaque-dos-turquie-genocide.htm

Praetox Technologies. (2009, April 23). *Praetox Technologies.* Retrieved 2012, from Praetox Technologies: http://web.archive.org/web/20100921205654/http://praetox.com/n.php/sw/sauce

Symantec. (2012, March 02). *Anonymous Supporters Tricked into Installing Zeus Trojan* . Retrieved 2012, from Symantec: http://www.symantec.com/connect/blogs/anonymous-supporters-tricked-installing-zeus-trojan

Security Curmudgeon. (2011, June 4). *Absolute Sownage, A concise history of recent Sony hacks.* Retrieved 2012, from Attrition.org: http://attrition.org/security/rants/sony_aka_sownage.html

Softpedia. (2012, July 20). *Burger King Employee Stomps on Lettuce, Identified via GPS Data from Picture.* Retrieved 2012, from Softpedia: http://news.softpedia.com/news/Burger-King-Employee-Stomps-on-Lettuce-Identified-Via-GPS-Data-from-Picture-282286.shtml

Sony. (2011, May 3). *Letter to Bono Mack and Butterfield_pg1.* Retrieved 2012, from Flickr: http://www.flickr.com/photos/playstationblog/5686965323/in/set-72157626521862165/

SpiderLabs. (2012, January 27). *HOIC DDoS Analysis and Detection* . Retrieved 2012, from SpiderLabs: http://blog.spiderlabs.com/2012/01/hoic-ddos-analysis-and-detection.html

SpiderLabs. (2011, January 28). *LOIC DDoS Analysis and Detection* . Retrieved 2012, from SpiderLabs: http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html

Reuters. (2011, August 3). *"State actor" behind slew of cyber attacks.* Retrieved 2012, from Reuters: http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803

RSnake. (n.d.). *Slowloris HTTP DoS.* Retrieved from ha.ckers: http://ha.ckers.org/slowloris/

RSnake, J. K. (2009, June 17). *Slowloris HTTP DoS* . Retrieved 2012, from ha.ckers: http://ha.ckers.org/slowloris/

RT. (2012, January 20). *Internet strikes back: Anonymous' Operation Megaupload explained* . Retrieved 2012, from RT: http://rt.com/usa/news/anonymous-barrettbrown-sopa-megaupload-241/

Telecomix. (2012). *Telecomix.* Retrieved 2012, from Telecomix: http://telecomix.org

The Wall Street Journal. (2011, October 29). *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web* . Retrieved 2012, from The Wall Street Journal: http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

The Associated Press. (2012, February 28). *25 Suspected Hackers Arrested in International Raids* . Retrieved 2012, from The New York Times: http://www.nytimes.com/2012/02/29/world/europe/25-suspected-hackers-arrested-in-international-raids.html

The Guardian. (2012, March 7). *LulzSec leader Sabu was working for us, says FBI* . Retrieved 2012, from The Guardian: http://www.guardian.co.uk/technology/2012/mar/06/lulzsec-sabu-working-for-us-fbi

The Jargon File. (1990). *Hacker.* Retrieved 2012, from The Jargon File: http://www.catb.org/jargon/html/H/hacker.html

The New York Times. (2010, September 19). *In a Computer Worm, a Possible Biblical Clue.* Retrieved 2012, from New York Times: http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=3&pagewanted=2&hpw

The New York Times. (2012, June 1). *Obama Order Sped Up Wave of Cyberattacks Against Iran.* Retrieved 2012, from The New York Times: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2

The Next Web. (2012, March 15). *Anonymous claims that the operating system, 'Anonymous OS' is fake.* Retrieved 2012, from The Next Web: http://thenextweb.com/insider/2012/03/15/anonymous-claims-that-the-operating-system-anonymous-os-is-fake/

The Pirate Bay. (2011, June 2). *Sownage.* Retrieved 2012, from The Pirate Bay: http://thepiratebay.se/torrent/6443601/

The Register. (2011, September 7). *Cyber crime now bigger than the drugs trade.* Retrieved 2012, from The Register: http://www.theregister.co.uk/2011/09/07/cost_is_more_than_some_drug_trafficking/

The Tech Herald. (2011, February 11). *Firm targeting WikiLeaks cuts ties with HBGary - apologizes to reporter* . Retrieved 2012, from The Tech Herald: http://www.thetechherald.com/articles/Firm-targeting-WikiLeaks-cuts-ties-with-HBGary-apologizes-to-reporter/12767/

The Tech Herald. (2011, May 23). *Seven security incidents in two months - Sony's nightmare grows (Update).* Retrieved 2012, from The Tech Herald: http://www.thetechherald.com/articles/Seven-security-incidents-in-two-months-Sonys-nightmare-grows-(Update)/13611/

The Tech Herald. (2011, May 23). *Seven security incidents in two months - Sony's nightmare grows (Update).* Retrieved 2012, from The Tech Herald: http://www.thetechherald.com/articles/Seven-security-incidents-in-two-months-Sonys-nightmare-grows-(Update)/13611/

Threatpost. (2011, February 28). *HBGary Federal CEO Aaron Barr Steps Down.* Retrieved 2012, from Threatpost: http://threatpost.com/en_us/blogs/hbgary-federal-ceo-aaron-barr-steps-down-022811

Appendix A: List of hacktivist groups and operations

Anonymous

Anonymous is one of the most well known hacktivist groups today. Its origins can be retraced back to 2003, in the infamous imageboard 4chan, which was known for its total lack of "good taste", anarchic governance, and anonymity.

Anonymous first became famous for their actions against the Church of Scientology as part of their Operation Chanology. But they truly caught the media's attention when they started Operation Payback, a massive DDoS campaign against the financial blockade on Wikileaks on behalf of MasterCard, Visa, and other financial institutions.

The structure and behavior of Anonymous is discussed in the report, as they probably are the group that fits best into the threat model presented in this report.

Notorious actions include Operation Payback (DDoS campaigns against anti-piracy institutions and, later, detractors of Wikileaks), the attacks on HBGary Federal described in this report, Operation Sony (DDoS against Sony, in retaliation to their legal actions against George Hotz), Operation BART (against the Bay Area Rapid Transit's actions to cut off protesters' cell phone communications and the police shooting that ensued), the attack on Stratfor, a competitive intelligence firm nicknamed the "private CIA", the attacks in response to the Megaupload incidents (discussed in this report), operation DarkNet (taking down of several child pornography websites running on anonymous networks), and several other leaks and DDoS attacks. Anonymous also participated in actions related to several of the Arab Spring revolutions (Operation Tunisia, Operation Syria).

A full list of their operations can be found on the Wikipedia page on events associated with Anonymous.

Anonymous generated various spinoffs such as AntiSec, which collaborated with LulzSec in a number of operations.

Lulzsec

LulzSec, or LulzSecurity is a hacker group that operates with no specific political agenda. Their only goal is to have fun, or to hack for the "lulz" (a deformation of the internet-slang LOL, acronym for Laughing Out Loud). They started their hacking campaign after the HBGary incidents, and were officially dismantled on 26 june 2011, after their "50 days of lulz" statement. Most of their members were arrested after their leader, Sabu, was found to have been cooperating with the FBI after his arrest.

LulzSec were notorious for their attacks against Sony (detailed in this report) and Fox News (revealing several thousands of personal records of X Factor contestants). They also targeted some government-related websites, such as the senate.gov website, and launched DDoS attacks on the website of the CIA, taking it down for more than two hours.

LulzSec teamed up with Anonymous to carry out Operation Anti-Security, or AntiSec, as a way of protesting against Internet censorship and monitoring. As part of this operation, AntiSec attacked the British Serious Organised Crime Agency (SOCA) and the highly mediatized attacks on Stratfor (where large amounts of data and internal emails were dumped and sent to Wikileaks for publication).

The Jester

The Jester can be described as a lone-wolf hacker. The Jester's targets are consistent with a pro-US mentality: The Jester has targeted Jihadist websites, Wikileaks or Bradley Manning supporters, and Anonymous-related websites. He claims to use a Denial of Service tool called "XerXeS", that he allegedly programmed himself.

The Jester is notorious for having taken down several pro-jihadist websites. Nevertheless, these takedowns are temporary (as it is common with denial of service attacks), which has garnered quite some criticism of both hacktivist and information security researchers interested in the matter.

Telecomix

Telecomix is a hacktivist group that focuses more on defense and education than offensive strategies. They follow a completely decentralized structure and are committed mainly to freedom of expression, and what they call "datalove".

They have been very active in the Arab Spring revolutions (Egypt and Syria), educating citizens of those countries on means of evading censorship and communicating securely. They have released logs showing that BlueCoat products were being used in Syria to intercept communications and spy on citizens.

Telecomix has been subject to many denial-of-service attacks, and is offline at the time of this writing.