Anonymous and LulzSec: The impact hacktivist organizations have on our perceptions of hackers and information security.

John Yamich and Anthony Smith
3/1/2012
Recently, there has been a large upsurge of cyber attacks on organizations throughout the world, most notably occurring in the United States. These attacks target small private companies to large government agencies and are typically politically or socially motivated. The outcome in many cases results in highly publicized data breaches or website interruption. Cyber attacks and the motivations behind them have given rise to a new term called hacktivism. This paper seeks to better understand what hacktivism is, who the major players are, their attacks as well as response, and how they affect our perceptions of hackers and information security.

Hacktivism sometimes spelled as “hactivism”, is defined by Webopedia as "the concept of hacking into a Web site or computer system in order to communicate a politically or socially motivated message. Hacktivists conduct the same types of disruptive actions as malicious hackers but do so as a way to draw attention to a cause rather than as a means to cause harm or illegally profit from their actions ("Hacktivism," n.d.).” As the definition describes, the goals of hacktivists are to communicate social or political messages. This often comes in the form of retaliatory attacks in opposition to company or government policies.

Who are these groups? In 2011, the two biggest groups that are considered hacktivist groups are called 'Anonymous' and 'LulzSec.' The name 'Anonymous' comes from the fact that members never reveal their identity and the number of members the group has is somewhat of a mystery. It is also unclear as to whether or not the group has a leader or a central command structure that guides its actions. Although calling Anonymous a group helps to understand it better, it can be thought of as more of a collective identity in which anyone can be a part of so long as they know the rules and how to apply them (Herwig, 2011).

LulzSec is another closely related group to Anonymous. In fact, this group was born out of AnonOps, which is a division of Anonymous. They came into being by breaking off from Anonymous and
forming their own group. “What Anonymous brought to the online party was the democratization of hacking,” says Steve Gold, editor of Infosecurity magazine. “LulzSec is the natural evolution of the trend that Anonymous started – focused on online hactivism. Its membership is born from the online gaming community.” (Park, 2011) While being closely associated with Anonymous, LulzSec operates a little differently. For one thing, they have six high-profile members each responsible for a specific role as well as a leader (Poeter, 2011). For the most part, these two aforementioned groups carry out the same activities such as hacking, leaking information, and taking down web sites to bring attention to a particular cause.

These hacktivist groups are relevant for a couple major reasons. First, they force people to think about information security. It forces computer users to think beyond how secure their passwords are, but also what information do they have out on the internet, who is the custodian of that information, and what are those custodians doing to protect their data. In addition, it also forces people to think about important social or political causes whether it be in support of or against those causes.

Anonymous started to gain the attention of the media in 2008 when it protested the Church of Scientology. Jana Herwig of The Guardian News writes, "Three years later, Anonymous has not only gained a sizeable collection of adversaries and critics – including government agencies, IT security companies and digital rights advocacies who criticise its methods – it has also won scores of secret and not so secret admirers, especially among the highly social media literate, digital creative class." She goes on, stating "The reputation of its members as defenders of truth and seekers of knowledge, digital avengers who cannot be lied to because they will hijack the emails of those who try, seems to strike a chord with many."
LulzSec gained notoriety when they made headlines around the world with a 50 day hacking, leaking, DDoSing\(^1\), and website defacing spree (Poeter, 2011). They launched attacks against three online games - Minecraft, Eve Online, and League of Legends as well as popular web sites such as Sony Pictures and the CIA. The online games and the CIA's website were taken offline with customer data from the Sony Pictures being stolen (Park, 2011).

As mentioned previously, the CIA and Sony Pictures were targets of these attacks among others. This section of the paper will discuss these attacks as well as other attacks in a little more in depth so as to further understand LulzSec and Anonymous.

On April 3rd, 2011, the hacktivist group Anonymous announced that it would take down the Sony Pictures website in retaliation for their legal actions against George Hotz, a hacker that posted information online that allowed users to install unauthorized software on the Sony Playstation 3 game console (Newman, 2011). The group posted online that Sony's behavior was an "unforgivable offense against free speech and internet freedom" and that Sony would "feel the wrath of Anonymous," promising to down the company's website (Benedetti, 2011). On April 4th and 5th, Sony.com, Playstation.com, as well as the Playstation Network (used by Playstation 3 users) were intermittently down. Sony's official response was the following:

"We are currently investigating, including the possibility of targeted behavior of an outside party. If this is indeed caused by such act, we want to once again thank our customers who

---

\(^1\) DDoS (attack) is short for Distributed Denial of Service. It is an attack where an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack. It is a denial of service because the attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer (McDowell, 2009)
have borne the brunt of the attack through interrupted service. Our engineers are working to restore and maintain the services, and we appreciate our customers' continued support."

It appears that Sony was able to keep their services running although the following day Anonymous changed up their method by seeking personal information about company executives and their families (Benedetti, 2011). Although this matter never officially came to an end, the attacks against Sony have cooled down.

In mid-summer of 2011, the group LulzSec hacked an FBI-affiliated website. The group took responsibility for hacking the Atlanta chapter of Infragard, which is a "partnership between the FBI and the private sector dedicated to preventing terrorist and criminal acts against the U.S." (Rodriguez, 2011) The result of the hack was that their website, infragardatlanta.org was defaced along with its member database being leaked. Over 180 members of the Atlanta chapter had their usernames and passwords published online. The members who used the same login information for sites such as LinkedIn or Gmail found that those accounts were compromised as well. Infragard's response to the hacking was downing their website and notifying their members of the hack (Swartz, 2011).

On June 15th, 2011, the U.S. Central Intelligence Agency's website was taken offline by LulzSec. The CIA website was taken down for several hours from a denial of service attack or DoS attack. In this attack LulzSec overloaded the CIA web servers with requests which made the website unavailable to other users, thereby making it appear as being offline (Mangis, 2011). The hacktivist group claimed responsibility for the attack through the following Twitter posting, also called a 'tweet'.

"Tango down - cia.gov - for the lulz," @LulzSec tweeted around 5:48PM ET.

The group also took responsibility for attacking the Senate website causing a brief outage. The group said "We don't like the US government very much. Their boats are weak, their lulz are low, and their
sites aren’t very secure. In an attempt to help them fix their issues, we’ve decided to donate additional
lulz in the form of owning them some more! (Bosker, 2011)

Clearly these groups have had an impact on organizations through their public facing websites, but what has been law enforcement’s or the government’s (U.S.) response to these attacks? The answer as been arrests occurring worldwide. One such arrest was of a British teenager named Ryan Cleary, who was charged with five offenses of hacking websites. His arrest was linked to the LulzSec group. He allegedly constructed a botnet2 to perform a distributed denial of service (DDos) attack, mentioned earlier, against three websites including the CIA and Senate websites (Dodd & Halliday, 2011). Three alleged hackers were also arrested in the United States. Cody Kretsinger of Arizona, Christopher Doyon of California, and Joshua Covelli of Ohio were arrested by the FBI and charged with "conspiracy to cause intention damage to a protected computer." They allegedly took part in denial of service attacks mentioned earlier. Additional arrests took place in the Netherlands, Australia, Spain, and Turkey as international law enforcement worked to track down members of Anonymous and LulzSec (Richmond, 2011).

While the arrest of alleged hacktivists is one result of their activities, there is a real cost to web hacking. Acuentix, a web application security company, lists the potential negative effects of attacks on organizations as follows:

- Loss of customer confidence, trust and reputation with the consequent harm to brand equity and consequent effects on revenue and profitability;
- Possible loss of the ability to accept certain payment instruments e.g. VISA, Mastercard

---

2 A botnet is a collective computing network consisting of many bots and bot herders under the control of a single hacker, giving him or her access to the computing power of many thousands of machines simultaneously ("Stratfor").
• Negative impact on revenues and profits arising from any falsified transactions and from employee
downtime;
• Website downtime which is in effect the closure of one of the most important sales channels for an
e-business;
• The expenditure involved in repairing the damage done and building contingency plans for
securing compromised websites and web applications; and,
• Legal battles and related implications from Web application attacks and lax security measures
including fines and damages to be paid to victims ("Web hacking," 2011).

The impact on everyday web users can be just as severe. User data that is stolen in many cases can be used for identity theft. "Some hackers can gain access to sensitive information which could be used to fuel identity theft. This identity theft can cause damages to credit ratings from consumer agencies, run-ins with the law because the person who stole the identity committed a crime, or other damages which may not be repairable at all ("What are the," n.d.)."

Although LulzSec and Anonymous have been making enemies through their cyber warfare, the public at large seems to have taken a different view. In a recent poll conducted by The Inquirer, the majority of respondents supported the group's actions in some form or another. When asked "Do you support its actions?," referring to LulzSec, a little over two-thirds responded that they did support the group (Neal, 2011). In another poll run by Sophos, a web security company, nearly 40 percent of readers agreed with the actions of LulzSec & Anonymous, calling them "funny while making a serious point about security." The other 43 percent said their actions were "no laughing matter" (Rangan, 2011). Whether or not people agree with their tactics, one thing is clear, they are popular. At the time this paper has been written, the LulzSec official Twitter page had nearly 360,000 people following them.
An online article, by John Thorpe of Business Insider, is titled *LulzSec, Anonymous Are Freedom Fighters*. The article shows strong support for these groups as evidenced by the following excerpt:

"Look, folks, despite the negative media attention and outright lies being spread by the government, the work being done by Anonymous, Lulzsec, and Wikileaks is the most important social movement of our lives. With enough popular support, they will revolutionize the world. They are bringing down the walls of secrecy that keep the world trapped in cycles of poverty, oppression, and in some parts, outright slavery.

They are the George Washington and John Adams of this generation. With every hack and data release, they are the giant eff-you John Hancock signature to the powerful. They are Anonymous. We are Anonymous. I am Anonymous. Are you?" (Thorpe, 2011)

Obviously this is only one opinion of many of these groups, but it is particularly interesting how strongly people feel. It would be interesting to see how that author's views might change if it were his information that was impacted by the attacks mentioned earlier.

This paper has so far detailed several key aspects of hacktivism including two of two most popular groups, by describing their motives, their organization, some of their attacks, as well as the public's reaction and perceptions of those attacks. Thus at this point it should be clear that hacktivists have impacted the public's view of hackers and information security by shedding light on important weaknesses in data protections.
References


Hacker organizations have been become popular these days with 2011 being an especially busy year. Two such groups made headlines around the world for nearly every month in 2011. A couple hacker organizations, named 'Anonymous' and 'LulzSec,' are two of the more popular groups that have been consistently been covered in newspapers, magazines, and television. Although these organizations have a member-base of hackers, two new terms, hacktivism and hactivist, have come into use that better define the objectives of these groups. The techtarget.com website defines hacktivism as "the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist." The website goes on to say that "hacktivists use the same tools and techniques as a hacker, but does so in order to disrupt services and bring attention to a political or social cause." In many of the attacks perpetrated by these groups, there were threads that tied these actions back to political and social causes.

While there are documented attacks by these groups, there are also documented arrests of suspected members of these groups (Dodd & Halliday, 2011). Linking suspects to specific groups has not often been successful, but it is clear that these groups do exist. What is not exactly clear is public opinion of these groups. One article written describes these groups as freedom fighters who work to expose fraud, corruption, hypocrisy, and evil that dominates corporate and government worlds (Thorpe, 2011). Another article refers to poll results that showed 18 percent of respondents welcoming the work of these groups, 9 percent agreeing that the group is entertaining, 44 percent agreeing that something needed to be done to expose insecurity and hypocrisy. Another 29 percent responding that they did not like these groups altogether (Neal, 2011). It is unclear how the poll was conducted but it is clear that further investigation should be done to understand what the public think of these groups and how they respond their activities.

Hacktivism: http://searchsecurity.techtarget.com/definition/hacktivism