https://doi.org/10.48009/1_iis_2012_133-143
Issues in Information Systems
Volume 13, Issue 1, pp. 133-143, 2012

HACKERS GONE WILD: THE 2011 SPRING BREAK OF LULZSEC

Stan Pendergrass, Robert Morris University, wspst2@mail.rmu.edu

ABSTRACT

Computer hackers, like the group known as Anonymous, have made themselves more and more relevant to our modern life. As we create and expand more and more data within our interconnected electronic universe, the threat that they bring to its fragile structure grows as well. However Anonymous is not the only group of hackers/activists or hacktivists that have made their presence known. LulzSec was a group that wreaked havoc with information systems in 2011. This will be a case study examination of their activities so that a better understanding of five aspects can be obtained: the Timeline of activities, the Targets of attack, the Tactics the group used, the makeup of the Team and a category which will be referred to as The Twist for reasons which will be made clear at the end of the paper.

Keywords: LulzSec, Hackers, Security, AntiSec, Anonymous, Sabu

INTRODUCTION

Information systems lie at the heart of our modern existence. We deal with them when we work, when we play and when we relax; texting, checking email, posting on Facebook, Tweeting, gaming, conducting e-commerce and e-banking have become so commonplace as to be nearly invisible in modern life. Yet, within each of these electronic interactions lies the danger that the perceived line of security and privacy might be breached and our most important information and secrets might be revealed and exploited. Sometimes this fear is based on an imagined vulnerability inherent within the system itself or it could be based on a fear that individuals will somehow actively exploit those vulnerabilities for their own unknown purposes. Those individuals have over the years become known as "hackers."

While the term hackers can be used to designate any number of individuals or groups with any number of purposes or connections, as of late, it has been used more and more to define one internet-based group known as "Anonymous." They have organized and participated in Distributed Denial of Service (DDoS) attacks, rendering websites temporarily unavailable and unusable, hurting companies through lost potential revenue and increased security expenses. They have organized and participated in electronic and physical protests and operations which have run the gamut from serious political statements to harmless fun.

But Anonymous is not the only group of hackers in cyber space. Other groups have reared up and come into the spotlight. In the Spring and Summer of 2011, one group was particularly active and eclipsed Anonymous for a time. This group called itself LulzSec, a portmanteau of Lulz (the plural of the acronym for "Laughing Out Loud" or lol) and Security and announced they were in the business of stealing information and distributing it to the world, "for the lulz of it." For eight weeks that year, they taunted law enforcement authorities, hacked into multi-billion dollar corporations, federal agencies, internet security firms and government institutions and brazenly posted their ill-gotten goods for the all the world to see. Then, they suddenly announced their retirement and were gone, just as quickly as they had appeared. However their story did not end when they supposedly retired. That story is playing out even today, in ways that were almost unbelievable. This paper will look at the activities of LulzSec and describe the events of this recent hacker group and the ways it operated, so that the complete story might be better understood.

RESEARCH METHODOLOGY

This study involved no participants per se, in that there were no direct interviews with people who might claim to be a part of LulzSec or claim to know someone who is or was in the group. There is almost no way to verify those claims and those who are or were in the group are most likely not going to admit it pending legal action or indictment. Therefore, all information was taken from secondary data collection.

Data was collected from a variety of secondary sources using a variety of means. There has not been a lot of detailed academic research devoted to the actual group, most likely because it is so contemporary. Most of the information came from news sources who reported on LulzSec's activities. This formed the bulk of the data collected. Additional electronic sources of material were also used which included hacker blogs, twitter accounts, web pages, posted information and announcement in Pastebin and file sharing sites. Media taken from sources other than the internet were also used; newspapers, magazines, radio and television broadcasts, and documentaries. Official government reports, announcements and documents were included as well as legal indictments which have been unsealed and released to the public.

In order to condense such a huge amount of information and turn it into a coherent, concise story, the case study method of research was the model. Yin [30] described two criteria for using this method of study. First, a case study methodology is useful in order to understand a real-life phenomenon in depth, and secondly, a case study copes with a technically distinctive situation where there are many more variables of interest than data points and multiple sources of evidence [30]. This case study looked at a wide variety of secondary data collected from a variety of sources to try and determine an overall understanding of several aspects of LulzSec.

Yin [30] described several analytical strategies which can be used to analyze the collected data. This study created a descriptive framework for organization and analysis. This strategy is useful when a lot of data has been collected without having settled on an initial set of research questions or propositions [30]. Yin's example of the organizational model of the Middletown sociological study [20] could be considered relevant and therefore was adapted for this study. LulzSec's activities were grouped into five categories for analysis: the "Timeline" of activities, the "Targets" of attack, the "Tactics" the group used, the makeup of the "Team" and a category which will be referred to as "The Twist" for reasons which will be made clear at the end of the paper.

RESULTS

Timeline

Between 17 and 19 April, 2011, Sony's PlayStation Network (PSN) and Qriocity Network were hacked and users' personal data, to include usernames, credit card information, etc. had been compromised. [24]

On 20 April, Sony completely shut down their networks but did not mention to the public the reason; that their network had been invaded. It would take another two days before that announcement would take place and even then Sony did not announce that personal information had been compromised. That announcement would take place on 26 April. On the first of May, bowing to public outrage over this public relations nightmare, Sony executives formally apologized and said they expected full service to be up by mid-May [24]. They blamed Anonymous for the hack however persons who claimed to be part of Anonymous denied having any involvement. If that were true, then perhaps there was some new agent on the hacking scene. That realization would be made clear within the week.

On the 7th of May, an announcement from a new group was released; they called themselves "LulzSec." LulzSec announced that unlike Anonymous' reasoned and determined hacks and attacks, they were only in it "for the lulz of it" [9]. Their first announcement stated:

> Hello, good day, and how are you? Splendid! We're LulzSec, a small team of lulzy individuals who feel the drabness of the cyber community is a burden on what matters: fun. Considering fun is now restricted to Friday, where we look forward to the weekend, weekend, we have now taken it upon ourselves to spread fun, fun, fun, throughout the entire calender [sic] year.
> As an introduction, please find below the X-Factor 2011 contestants' contact information. Expect more to come, and if you're like us and like seeing other people get mad, check out our Twitter!
> http://twitter.com/LulzSec. [14]

Their method of dissemination was quick, simple and seemingly untraceable. Tweets on the Twitter page they established contained links to unattributed Pastebin announcements which often contained http addresses of Pirate Bay postings where files of hacked information could be downloaded by anyone. On 10 May, LulzSec announced their hack of Fox.com and posted links to files containing inner-working and sales database information along with a list of sales department's emails and passwords [9]. LulzSec urged their followers to try and use the emails and passwords to log into Facebook, MySpace and PayPal accounts to see what further damage could be caused.

On 15 May a hack of U. K. ATM machine data was released [9]. In their announcement LulzSec confessed that while there appeared to be little profitable information in the data, perhaps someone could find it useful in some way. Included in their hack release were altered lyrics set to the theme song from the 1970's television series *The Love Boat* which also included an ASCII representation of a Viking boat which they christened The Lulz Boat.

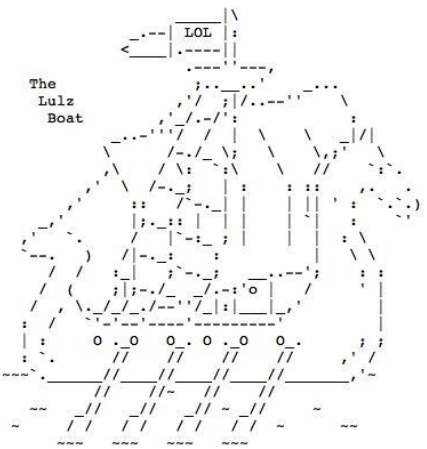

Figure 1. ASCII Art representation of the LulzBoat on May 15, 2011 PasteBin Press Release

The 23rd of May brought a release of data from Sonymusic.co.jp databases; nothing particularly useful but still another hack of a Sony website [9]. On the 24th of May, PBS ran a Frontline Series documentary titled *WikiSecrets* and focused on PFC Bradley Manning, the American soldier accused of leaking classified information and documents on the war to the whistleblower website WikiLeaks. In retaliation for what they claimed was a biased and unflattering portrait of Manning and WikiLeaks founder, Julian Assange, on 30 May, LulzSec hacked into and defaced the PBS.org website by posting a fake news story on the site which stated that rappers Tupac Shakur and Biggie Smalls, were not deceased but were alive and well and living in an unnamed small town in New Zealand [7, 9].

Figure 2. Hacked PBS.org Website article stating Tupac Shakur is living in New Zealand

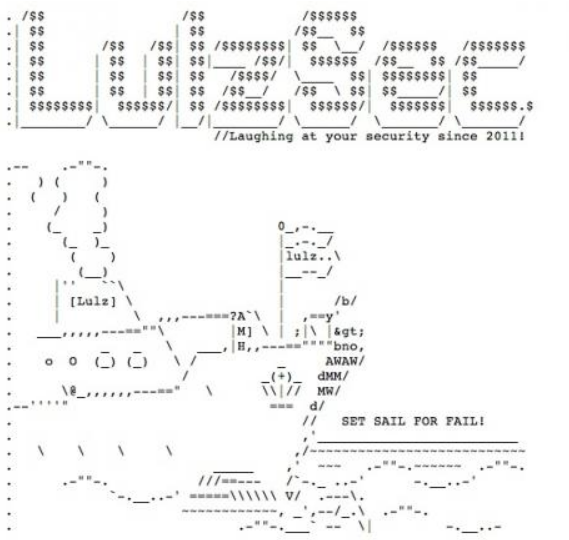

Figure 3. ASCII Art Press Release Banner on May 30, 2011 PasteBin Press Release

On 2 June, LulzSec released data from their latest hack which they labeled Sownage, for Sony + Ownage. LulzSec said it was able to gain passwords, e-mail addresses, home addresses, birthdates, and all Sony opt-in data associated with users' accounts from some one million users of SonyPictures.com [9]. Some of the exposed personal information also included home telephone numbers which was confirmed by the Associated Press. None of the users' IDs and passwords were encrypted by Sony; this, still after the other numerous hacks months before! Information from the databases of Sony BMG Belgium and the Netherlands were also included as well as a varied assortment of Sony user and staffer information [9, 22].

Purportedly in response to a White House announcement that an act of cyber sabotage on the United States by another country could be considered an act of war [11], LulzSec defaced the website and released email, username

and password information of a company that does business with the FBI; Infragard, specifically the Atlanta office. They also obtained personal and company email of one of Infraguard's employees, a Mr. Karim Hijazi, as he had also established a company, Unveillance, which specializes in data breaches and botnet detection. After LulzSec contacted Mr. Hijazi to inform him of the breach, he offered to hire LulzSec hackers to attack his competitors. LulzSec posted the web chat records in their release to mock and embarrass him.

Sownage 2 was announced on 6 June when 54MB of SVN Sony developer code as well as internal network maps of Sony BMG were displayed. Four days after that a collection of 26,000 user email addresses and passwords to a pornography website, pron.com were released. LulzSec specifically pointed out, by highlighting them at the top of the list, addresses from 6 users who used their government computers' address as account information and 55 admin/webmasters of other porn sites [9].

On 13 June, two announcements were released for two separate hacks. Senate.gov server information and Bethesda Softworks, ZeniMax Media and Brink internal data were displayed. In an unusual twist, LulzSec reported that they would not release information they claimed they had on over 200,000 Brink users because they actually liked the game and wanted Bethesda to speed up development work on the next installment of their video game series, *The Elder Scrolls V: Skyrim.* On the 15th of June, LulzSec set up a telephone line with an answering machine and tweeted a solicitation for suggestions as to whom they should go after next [27]. That same day, the CIA was the focus of a Denial of Service (DoS) attack. The CIA's public web site was briefly down however it came back online fairly quickly [9, 21, 28].

LulzSec apparently went to war with Anonymous on 16 June. It began when LulzSec called for a "DDoS party" on a variety of websites and game servers popular with videogamers, including that of *EVE Online*, *League of Legends* and *Minecraft*; all the websites suffered outages or slow downs. Those who frequented 4Chan's /v/ board for video games enthusiasts caught wind of the attacks and called for an attack on LulzSec. Then LulzSec tweeted a link to 4Chan's /b/ board to slow it down and also released 62,000 random logins in return for flooding /b/ [8, 9]. The next day, LulzSec celebrated their 1000th Tweet with a sort of manifesto to their friends and foes reiterating that they were in the hacking game purely for the fun of all the confusion and consternation they create.

Two days later, three days after their attack on Anonymous, on 19 June, LulzSec announced the start of Operation AntiSec. AntiSec stood for Anti-Security, was to be an ongoing operation where both LulzSec *and* Anonymous would team up to steal and leak any classified government information they could get their hands on. Prime targets were announced to be banks and other high-ranking establishments [1, 9]. Anonymous amazingly confirmed this by tweeting through their Tweet account AnonOps, "We are not at war [with LulzSec]. We are bros of teh internetz [sic]" [4].

However, LulzSec's fortunes were apparently starting to change. All this mischief was not going unnoticed by the authorities. On the 21st of June, Ryan Cleary, a 19 year old U. K. hacker, also known as ViraL [9, 26] was arrested by U. K. police and charged with violating the country's computer fraud laws for participating in cyber attacks on various British organizations [2]. LulzSec tried to distance themselves from him claiming he was "at best, only mildly associated" with them. They claimed that his only involvement was allowing LulzSec to use his servers.

On 23 June, LulzSec released what they called their "Chinga La Migra Bulletin #1 6/23/2011" [18]. With it, they released hundreds of private intelligence bulletins, training manuals, personal email correspondence, names, phone numbers, addresses and passwords belonging to Arizona law enforcement officials. They claimed to target Arizona law enforcement to protest Arizona Senate Bill 1070 which was a controversial strict anti-illegal immigration bill. The Bulletin further announced that they would be releasing more and more classified documents each week in a demonstration against governments, corporations, police and militaries around the world [18].

Just two days later, 50 days since LulzSec began making announcements and taking credit for releases of massive amounts of information, they suddenly announced their retirement as a hacking group. The last official document reiterated their manifesto ideals, professed continued support of Operation AntiSec and ended with links to hacked

information on their website and Pirate Bay. After that, LulzSec disappeared just as suddenly as it had appeared. Their two months of terror, fun and chaos had ended. The retirement announcement ended with the following:

> So [ ] it's time to say bon voyage. Our planned 50 day cruise has expired, and we must now sail into the distance, leaving behind - we hope - inspiration, fear, denial, happiness, approval, disapproval, mockery, embarrassment, thoughtfulness, jealousy, hate, even love. If anything, we hope we had a microscopic impact on someone, somewhere. Anywhere.
> Thank you for sailing with us. The breeze is fresh and the sun is setting, so now we head for the horizon. Let it flow...
> Lulz Security - our crew of six wishes you a happy 2011, and a shout-out to all of our battlefleet members and supporters across the globe. [19]

Targets

When examined over the timeline of their attacks, LulzSec's victims would seem to have little in common with one another, however, if one looks at the types of websites were attacked, distinct patterns emerge. Websites fall into two distinct divisions, either Government or Media websites. Those can be further divided into related sub-categories. Government can be grouped into Federal (i.e., Senate, FBI, Infraguard, CIA) or State (Arizona law enforcement). Media can be grouped into News (Fox, PBS) and Entertainment, (Fox, Sony, PBS, pron.com, Bethesda Softworks, ZeniMax Media, Brink, EVE Online, League of Legends and Minecraft). There was also the attack on 4Chan /b/ board however that was only because Anonymous members were attacking LulzSec at the time for the DoS to online gaming websites and did not appear to be forethought actions.

Tools

LulzSec's greatest tool was their attack. Two methods of attacks were used. The first and most extensively used was Structured Query Language (SQL) code injections into websites. When successful, it would allow LulzSec access to website internal information such as system files, content and the most valuable content, users' identification data. This type of attack was where LulzSec's had its greatest successes. Nearly all of their influence was as a result of leaked data and information they were able to obtain from hacked websites and databases. The second method was through DDoS attacks however they rarely used this. DDoS attacks require either a large number of participants or continued use of special software which repeatedly bombards websites until the shut down.

Once they had SQL injection-obtained data, there were a number of social media, utility and file sharing sites they used to announce, store and thus disseminate the data. For instance, Twitter (@LulzSec) was used to make public announcements of activities, actions, success, and to convey whatever up-to-the-minute information LulzSec wanted to convey. Some Twitter feeds would have attachments which linked to PasteBin posts which could lead to their more formal and lengthy press releases. Those releases were often more than Twitter's limit of 140 characters so PasteBin was used. LulzSec was also fond of including ASCII art in the header and body of the release. Press releases and Twitter Tweets often included addresses to links on the file sharing site Pirate Bay which often in turn contained torrent files with the stolen data. This way, as long as Pirate Bay hosted the link, anyone could access and download the data files. Internet Relay Chat (IRC) Channels were used for active and prolonged conversations within the group [10]. LulzSec even solicited BitCoin electronic cash donations to fund their continued activities [17].

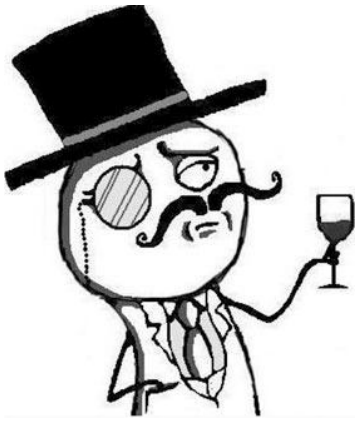

Figure 4. LulzSec Twitter account logo

None of this could have been accomplished without another important tool, anonymity. In order to achieve continued anonymity, they had to use anonymity-guaranteeing software such as The Onion Router (TOR). TOR software was originally developed by the Navy to provide anonymity to users. Users access the TOR network by installing the free software package. By using the software, all content is passed between random guard, relay and exit node servers so that the user's unique Internet Protocol (IP) address cannot be directly traced back to the original point of entry, i.e., their own computer. Anonymity allowed LulzSec to communicate, hack, post and taunt without law enforcement being able to detect where or even who they were. Of course this anonymity was only possible it one used the TOR software and network exclusively [25, 29].

Tactics

The name the group chose for themselves, a portmanteau of Lulz and Security, could be considered telling in that it was an indication of both their motivation (lulz) and inclination (security). Their motivation was to randomly hit a wide variety of targets and post the stolen data for anyone to use. While in some cases they hinted at how it might be used [16], for the most part it was posted with no provided purpose other than for their own amusement to show the world what they did and that they could do it. These actions had a direct and profound effect on perceived internet security, their inclination. Taken in a broader context, it was the security of the system itself which was affected, not necessarily security entities themselves. For instance, while they did attack some websites belonging to entities whose actual purpose was security (Infraguard, FBI, CIA, Arizona Law Enforcement), they also went after entities that had nothing to do with security per se (Sony, PBS, Fox News, Bethesda Softworks). But in the end, all of those sites as well as sites which had nothing to do with LulzSec attacks, were stained with the hackers' brush. Those effects continue to linger on through to today.

The lulz showed through in a variety of ways. For instance, their press releases and tweets were often very funny and clever. Their second announcement ended with the below divider before the hacked Fox.com emails and password information.

> ---
> ---
> --Raped material goes below the shiny dashes oh god they're so shiny--
> ---
> ---------- [15]

There was a taunting aspect to everything they did. Press releases often dared the authorities to come after them. It was a braggadocio attitude that undoubtedly infuriated those who were trying to track them down, not only law enforcement agencies but other white hat and black hat hackers who were working to expose them as well.

Team

LulzSec has always maintained that they were a small team of hackers. Their initial press release announced that they were "a small team of lulzy individuals". Their final press release at the end of the 50 days of LulzSec mentioned that they were a "crew of six" [19]. Given the timing of the hacks, some coming days after the previous one, the type of attacks conducted, on individual and specific websites and limited use of DDoS barrages, the conclusion is that the group was indeed, small, fast, agile and closely knit. Anonymous' method of getting the hive mind to come to a moral cause to attend to, getting legions of individuals to commit to a coordinated and persistent action, requires a lot of participants. LulzSec on the other hand, moved quickly and stealthily and announced what they had done for the most part after the fact, not before. This would seem to support the conclusion that LulzSec was indeed a small team of closely knit hackers.

The Twist

After the arrest of LulzSec member Ryan Cleary on the 21st of June and their sudden retirement on 25 June, 2011, LulzSec seemed to have faded back into the crowd as nothing was heard from the group after that. That is not to say that hacking died the day LulzSec packed up. There continued to be hacks of various websites, some of them were attributed to Anonymous [3] and some of them even waved the AntiSec banner, but nothing like what LulzSec had accomplish. The group just seemed to vanish.

However, on 6 March, 2012, almost a year after LulzSec first popped up, an indictment filed in August in the United States District Court of Southern New York was unsealed. The indictment was against a Hector Xavier Monsegur, also known as Sabu, the avowed leader of LulzSec [12]. Inside, it detailed his hacks with a variety of hacker groups; first Anonymous, then with a group which called itself Internet Feds and finally with LulzSec. Seemingly coincidentally the same day the indictment was unsealed, four members of LulzSec and one member of Anonymous were also arrested by U.S. and U.K. law enforcement agents.

> Ryan Ackroyd (AKA Kayla), 23, of Doncaster, United Kingdom, Jake Davis (AKA Topiary), 29, of Lerwick, Shetland Islands, Darren Martyn (AKA pwnsauce), 25, of Galway, Ireland, and Donncha O'Cearrbhail (AKA palladium), 19, of Birr, Ireland, were charged with various offences connected to LulzSec
>
> O'Cearrbhail was further charged in a separate case with intentionally disclosing an unlawfully intercepted wire communication - a conference call between law enforcement officers on both sides of the Atlantic discussing investigations against members of Anonymous that was leaked by the hacktivist collective last month.
>
> A fifth suspect – Jeremy Hammond (AKA Anarchaos), 27, of Chicago, Illinois – was arrested on access device fraud and hacking charges, and is suspected of involvement in the December Anonymous hack on security intelligence outfit Stratfor. [3, 13]

As it turns out, Sabu had been working for the FBI since 7 June as an informant of sorts. He was forced into this position after the authorites had arrested him and threatened him with jail time which would have placed his nieces into foster homes as he was their sole guardian while their mother was in prison. The FBI had earlier identified him as the likely head of the group after he made the mistake of failing to use the TOR Network every time he used his computer. "He logged into an Internet relay chatroom from his own IP address without masking it. All it took was once. The feds had a fix on him" [5, 29].

Back in June, another hacker named Virus, who was upset with what LulzSec was doing, had figured out Sabu's real identity and posted his name and address online. "Law enforcement feared Sabu would see he'd been outed and begin destroying evidence of his hacking career—and all traces of those he'd worked and communicated with online [29]. So they arrested him on 7 June, threatened him with the full legal consequences of his actions, made him an offer to rejoin the collective with a government computer, monitored at all times by the FBI and continue his

activities with LulzSec. He agreed and about a week later, reappeared on LulzSec IRC Channels continuing to urge his followers on to continue the hacks for the Lulzs!

On 15 June, LulzSec took down the CIA website with a DoS attack [21]. Sabu immediately intervened and convinced the group that they were playing with fire and to stop the action. LulzSec complied. As it turned out, the FBI put pressure on him to get the activities to stop. He was clearly back in the group, but under the control of the government. Everything that happened after that was recorded and closely monitored by the FBI. As it turned out, the Chinga La Migra Arizona law enforcement hacks could have been worse, but Sabu worked with the authorities to minimize the damages from the attack.

On 15 August, Sabu plead guilty to the charges in the sealed indictment and continued to work with the government, helping the FBI make their case against not only the four remaining members of LulzSec but also with other hackers who called themselves members of Anonymous. No one ever suspected, until the morning of the 6th of March when agents began showing up and arresting the hackers.

Evidence of Sabu's betrayal and the fear that the FBI might have more names to go after did not end hacking. Hackers who called themselves members of Anonymous immediately struck back with a hack against the Vatican that same day [23] and have continued, albeit less actively since the wild days of LulzSec. Other hackers have even attempted to resurrect LulzSec, if in name only [6]. But clearly, with the arrest of the six core members of the LulzSec group, ViraL, Sabu, Kayla, Topiary, pwnsauce and palladium, as well as a member of Anonymous, Anarchaos, the hacker community has suffered a high visibility black eye, and the days of assumed hacker anonymity and impunity, if not over, seem to be waning.

CONCLUSIONS

By examining this case study of a hacker group and the actions and activities associated with it, we can draw some conclusions as to what they did wrong and how they might have done things differently to avoid capture. First, if a group of hackers is to remain anonymous, then continued and sustained use of anonymity-ensuring software and procedures *mus*t be maintained. Through a single login on a computer using an identifiable IP address, location can be established and identity narrowed. Sabu did not use the TOR network that one time that we know of so when he signed on the IRC channel "unencrypted" the FBI confirmed his identity.

Secondly, everyone eventually gets caught, and if not by your actions, it could be because of the actions or inactions of others. The other members of LulzSec, with the exception of ViraL whom the UK identified and arrested early on, were not brought down because of mistakes they made, rather it was the mistake that someone *else* made, namely Sabu, which caused them to be identified. Additionally, Virus, a hacker who was concerned that LulzSec was doing more harm than good, was able to identify Sabu's identity and post it on the internet for all to see. This then forced the hand of the FBI so that they had to act immediately to prevent Sabu from destroying evidence or moving since his name and address were now public knowledge.

Next, by only using a small core group of individuals, LulzSec could coordinate hacks on a variety of platforms. The SQL attacks which freed up a wealth of site information, were most likely controlled by Sabu. LulzSec did not use what has become Anonymous' tool, the DDoS attack from the collective. Instead, sites were raided and the results posted to embarrass and draw attention to not only the site, but to LulzSec as well. LulzSec loved the limelight as much as Anonymous, they just went after results in a different way. Anonymous could be likened to a large ship where it takes a lot of long-term effort to affect changes in its course. LulzSec on the other had could be equated to a speed boat, changing course quickly and easily because they did not come with the baggage of a large collective. Nor were they hampered by an ideal, which is the case of Anonymous. LulzSec had no agenda other than creating chaos and consternation for its own sake. For the lulz of it!

This model of study can be used for future researchers hoping to understand group dynamics where there is a large amount of secondary data only. Descriptive frameworks can help to focus on specific aspects of a case so that like

aspects can be compared and contrasted. There will certainly be hacker groups exploiting information systems for the foreseeable future and if they are to be understood then this method could be useful in that task.

REFERENCES

1. Albanesius, C. (2011, June 20). LulzSec, Anonymous team up for 'Operation Anti-Security'. *PC Magazine*. Retrieved from http://www.pcmag.com/article2/0,2817,2387264,00.asp
2. Albanesius, C. (2011, June 22). UK hacker formally charged for cyber attacks. *PC Magazine*. Retrieved from http://www.pcmag.com/article2/0,2817,2387435,00.asp#fbid=zwNIHl7tGfU
3. Anderson, N. (2012, March 6). Stakeout: how the FBI tracked and busted a Chicago Anon. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/news/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon.ars
4. AnonOps (anonops). "Attention #Media: about #Lulzsec and #Anonymous, we are not at war. We are bros of teh internetz. Also, /b/ != Anonymous". 17 June 2011, 2:44 p.m. Tweet.
5. Biddle, S. (2012, March 6). LulzSec leader betrays all of Anonymous. *Gizmodo*. Retrieved from http://gizmodo.com/5890825/lulzsec-leader-betrays-all-of-anonymous
6. Bright, P. (2012, March 21). Anonymous revives LulzSec for new campaign of hacks and attacks. *Ars Technica.* Retrieved from http://arstechnica.com/tech-policy/news/2012/03/anonymous-reincarnates-the-lulzsec-name-for-new-campaign-of-hacks-and-attacks.ars?clicked=related_right
7. Couts, A. (2011, May 30). Hackers post fake Tupac story to PBS.org after WikiLeaks piece. *Digital Trends*. Retrieved from http://www.digitaltrends.com/computing/hackers-post-fake-tupac-story-to-pbs-com-after-wikileaks-piece/
8. Couts, A. (2011, June 16). LulzSec wages war with Anonymous and 4Chan, releases 62,000 logins [update]. *Digital Trends*. Retrieved from http://www.digitaltrends.com/computing/lulzsec-wages-war-with-anonymous-and-4chan-releases-62000-logins/
9. Fox News. (2011, June 21). A brief history of the LulzSec hackers. *Fox News*. Retrieved from http://www.foxnews.com/scitech/2011/06/21/brief-history-lulzsec-hackers/
10. Gallagher, R. & Arthur, C. (2011, June 20). Inside LulzSec: chatroom logs shine a light on the secretive hackers. *The Guardian*. Retrieved from http://www.guardian.co.uk/technology/2011/jun/24/inside-lulzsec-chatroom-logs-hackers
11. Gorman, S. & Barnes, J. (2011, May 30). Cyber combat: act of war. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html
12. Greenberg, A. (2012, March 6). Top LulzSec hacker Sabu identified, reportedly worked as government informant. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2012/03/06/lulzsec-leader-sabu-identified-reportedly-worked-as-government-informant/
13. Leyden, J. (2012, March 7). The one tiny slip that put LulzSec chief Sabu in the FBI's pocket. *The Register.* Retrieved from http://www.theregister.co.uk/2012/03/07/lulzsec_takedown_analysis/
14. LulzSec. (2011, May 7). LulzSec Press Release Number 1.
15. LulzSec. (2011, May 10). LulzSec Press Release Number 2.
16. LulzSec. (2011, June 10). LulzSec Press Release Number 13.
17. LulzSec. (2011, June 13). LulzSec Press Release Number 14.
18. LulzSec. (2011, June 23). LulzSec Press Release Number 18.
19. LulzSec. (2011, June 25). LulzSec Press Release Number 19.
20. Lynd, R. & Lynd, H. (1929). *Middletown: A Study in Contemporary American Culture*. New York: Harcourt, Brace, and Company.
21. Olivarez-Giles, N. (2011, June 15). CIA website down temporarily; LulzSec takes credit for the hack [Updated]. *Los Angeles Times.* Retrieved from http://latimesblogs.latimes.com/technology/2011/06/lulzsec-claims-hack-on-cias-website-sets-up-hack-request-line.html
22. Paul, I. (2011, June 3). Lulz Boat Hacks Sony's Harbor: FAQ. *PCWorld.* Retrieved from http://www.pcworld.com/article/229316/lulz_boat_hacks_sonys_harbor_faq.html

23. Perlroth, N. (2012, March 7). After Hacker Arrests, an Attack on the Vatican and a Growing Anxiety. *The New York Times.* Retrieved from http://bits.blogs.nytimes.com/2012/03/07/after-hacker-arrests-an-attack-on-the-vatican-and-existential-crisis/
24. Sangani, K. (2011). Sony security laid bare. *Engineering & Technology.* September 2011, 6 (8), pp. 74-77. doi:10.1049/et.2011.0810
25. Terban, S. (2011, September 5). The hidden wiki: layers of the onion router networks. *Infosec Island.* Retrieved from http://www.infosecisland.com/blogview/16290-The-Hidden-Wiki-Layers-of-The-Onion-Router-Networks.html
26. The Hacker News. (2011, June 21). UK police arrest suspected LulzSec 19 year old mastermind. *The Hacker News.* Retrieved from http://thehackernews.com/2011/06/uk-police-arrest-suspected-lulzsec-19.html
27. The Lulz Boat (LulzSec). "Call us: 614-LULZSEC (now accepting calls) | Join the party: irc.lulzco.org (port 6697 for SSL channel #LulzSec or http://chat.lulzco.org/)". 15 June 2011, 4:52 p.m. Tweet.
28. The Lulz Boat (LulzSec). "Tango down - https://www.cia.gov/ - for the lulz.". 15 June 2011, 5:48 p.m. Tweet.
29. Winter, J. (2012, March 6). Exclusive: unmasking the world's most wanted hacker. *Fox News.* Retrieved from http://www.foxnews.com/scitech/2012/03/06/exclusive-unmasking-worlds-most-wanted-hacker/
30. Yin, R. (2009). *Case Study Research: Designs and Methods, Fourth Edition*. Thousand Oaks, CA: Sage.