

HACKTIVISM: AN ANALYSIS OF THE MOTIVE TO DISSEMINATE
CONFIDENTIAL INFORMATION

THESIS

Presented to the Graduate Council of
Texas State University-San Marcos
in Partial Fulfillment
of the Requirements

for the Degree

Master of SCIENCE

by

Warren V. Held, B.A.

San Marcos, TX
December 2012

HACKTIVISM: AN ANALYSIS OF THE MOTIVE TO DISSEMINATE
CONFIDENTIAL INFORMATION

Committee Members Approved:

Jay D. Jamieson, Chair

J. Pete Blair

Jeffrey M. Cancino

Approved:

J. Michael Willoughby
Dean of the Graduate College

COPYRIGHT

by

Warren V. Held

2012

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

This work is protected by the Copyright Laws of the United States (Public Law 94-553, section 107). Consistent with fair use as defined in the Copyright Laws, brief quotations from this material are allowed with proper acknowledgment. Use of this material for financial gain without the author's express written permission is not allowed.

Duplication Permission

As the copyright holder of this work I, Warren V. Held, authorize duplication of this work, in whole or in part, for educational or scholarly purposes only.

ACKNOWLEDGEMENTS

I would like to thank the family members, friends, professors, and others who have lent support, assistance, and guidance throughout the course of my education.

This manuscript was submitted on October 26th, 2012.

TABLE OF CONTENTS

	Page
ACKNOWLEDGEMENTS	v
LIST OF TABLES	ix
LIST OF FIGURES	x
CHAPTER	
I: INTRODUCTION.....	1
II: LITERATURE REVIEW.....	10
Expansionists and Instrumentalists	10
Hackers	12
Hacktivists.....	19
Cyber Terrorists	20
Government Profiles	23
III: HISTORY	28
IV: PROBLEM AND RESEARCH QUESTIONS	73
V: METHODOLOGY	76
Stages 1 & 2: Data Sourcing and Transcription – Creating the Basis for Qualitative Analysis	78
Stage 3: Unitization – Choosing the Unit of Analysis and Dividing the Material into Coding Units	78
Stage 4: Categorization – Developing a Scheme of Categories Relevant to the Research Problem	80
Stage 5: Coding – Assigning Category Codes to Text Units.....	82
VI: ANALYSIS	83
Stage 1 & 2: Data Sourcing and Transcription	83
Stage 3: Unitization.....	92

Stage 4: Categorization	94
Stage 5: Coding	97
Analysis of Final Output	100
VII: DISCUSSION	109
Research Questions	109
Expansionists and Instrumentalists	110
Hackers and Hacktivism	112
Cyber Terrorism and Policy Implications	112
VIII: CONCLUSION	114
APPENDIX	117
Appendix A: X Factor Leaked Contestants Database	118
Appendix B: Untitled [Fox Hack]	119
Appendix C: [LulzSec] Fox.com leakage phase 0/1/2/3	120
Appendix D: [ATM leak] ~LulzSec	122
Appendix E: LulzSec hates Sony too	124
Appendix F: LulzSec Hack PBS.ORG	125
Appendix G: Re: "LulzSec Exposed"	127
Appendix H: Sownage	128
Appendix I: Fuck FBI Fridayâ,,ç (FFF)	130
Appendix J: RE: Unveillance	132
Appendix K: Sownage 2	133
Appendix L: Bethesda Internal Data	134
Appendix M: LulzSec versus Bethesda & Senate.gov	136
Appendix N: LulzSec - 1000th tweet statement	138
Appendix O: Operation Anti-Security	140
Appendix P: LulzSec 2011 census released	141
Appendix Q: Snitches getting various stitches	143
Appendix R: Chinga La Migra	144
Appendix S: 50 Days of Lulz	145
Appendix T: Antisec01	147
Appendix U: Chinga La Migra II	148
Appendix V: Chinga La Migra III	150
Appendix W: Turkish Takedown Thursday	151
Appendix X: Fuck FBI Friday II: IRC Federal	153
Appendix Y: Military Meltdown Monday: Mangling Booz Allen Hamilton	154
Appendix Z: A message to PayPal, its customers, and our friends	158
Appendix AA: Fuck FBI Friday III: ManTech Mayhem	159
Appendix BB: Shooting Sheriffs Saturday	161
Appendix CC: Corrupt Brazil (Satiagraha)	164
Appendix DD: Fuck FBI Friday IV – Vanguard Defense Industries	167
Appendix EE: Texas Takedown Thursday: Chinga La Migra IV	169

Appendix FF: Fuck FBI Friday V: IACS Cybercrime Investigators Owned	172
Appendix GG: International Association of Chiefs of Police Owned	174
Appendix HH: AntiSec teaser 12/26.....	178
Appendix II: AntiSec teaser 12/29 (legit).....	181
Appendix JJ: AntiSec teaser 12/29	183
Appendix KK: CSLEA Hacked/Defaced or some rubbish, happy new year	186
Appendix LL: Puckett & Faraj Lawfirm – Hadidtha.....	195
Appendix MM: Boston Police Department Defacement	197
Appendix NN: FTC JACKHAMMERBUTTRAEPD BY ANONYMOUS ANTISEC.....	198
LITERATURE CITED	201

LIST OF TABLES

Table	Page
Table 1: Intercoder Consistency Comparisons	94
Table 2: Final Category Hierarchy Scheme.....	95
Table 3: Example of Assigning Thought Units a Category	97
Table 4: Intercoder Consistency-Matrix	99
Table 5: High and Mid Level Categories Frequencies	100
Table 6: Hacktivist Motivation Category Frequencies	101
Table 7: Remaining Actor Motivation Categories Frequencies	102
Table 8: Data Stolen Category Frequencies.....	105
Table 9: Hacker Act Category Frequencies	106
Table 10: Statements Category Frequencies.....	107
Table 11: Other Category Frequencies	108

LIST OF FIGURES

Figures	Page
1. LulzSec Twitter post describing the group's first actions against the Fox media corporation	31
2. LulzSec Twitter post describing additional actions against the Fox media corporation	33
3. LulzSec Twitter post describing British ATM information.....	34
4. LulzSec Twitter post describing the Sony hack.....	35
5. Image of the false story posted by LulzSec to the PBS website.....	36
6. LulzSec Twitter post describing actions against PBS.....	37
7. LulzSec Twitter post describing actions against the FBI.....	38
8. LulzSec Twitter post describing previous actions against the FBI.....	39
9. LulzSec Twitter post describing actions against Nintendo.....	40
10. LulzSec Twitter post describing the AntiSec movement.....	40
11. LulzSec Twitter post describing actions against the Sony corporation	41
12. LulzSec Twitter post describing actions against the United Kingdom's National Health Service	42
13. LulzSec Twitter post describing actions against Endgame Systems and Prolexic	43
14. LulzSec Twitter post describing actions of releasing user account information for various pornography websites.....	43
15. LulzSec Twitter post describing actions against an Islamic jihadist website	44

16. LulzSec Twitter post describing the announcement for accessing the leak information for the group's actions against the Bethesda software company and the United States Senate website..	45
17. LulzSec Twitter post describing actions against the Bethesda software company.....	45
18. LulzSec Twitter post describing actions for the group's Titanic Takeover Tuesday..	46
19. LulzSec Twitter post describing the takedown of the CIA's website.....	47
20. LulzSec Twitter post detailing information for user accounts.....	47
21. LulzSec Twitter post describing the group's relationship with Anonymous.....	47
22. LulzSec Twitter post regarding taking down a hacking forum.....	48
23. LulzSec Twitter post describing the group's beliefs on hacker typology.....	48
24. LulzSec Twitter post proclaiming the start of the AntiSec movement.	49
25. LulzSec Twitter post describing actions against the FBI.....	50
26. LulzSec Twitter post describing actions against the United Kingdom's Serious Organized Crime Agency	50
27. LulzSec Twitter post debunking a false LulzSec release.....	51
28. LulzSec Twitter post in response to Ryan Cleary's arrest.....	52
29. LulzSec Twitter post describing the Chinga La Migra operation.....	54
30. LulzSec Twitter post describing the 50 Days of Lulz release	56
31. LulzSec Twitter post describing the attack on <i>The Sun</i> newspaper.....	59
32. LulzSec's leader Sabu and an Anonymous member Twitter posts describing the Fuck FBI Friday VI release.....	69
33. Anonymous Twitter post describing the group's action against Interpol	69
34. Graph for Motivation Categories by Hacker Type	104

CHAPTER I

INTRODUCTION

Anonymous, LulzSec, and the AntiSec movement are Internet-based organizations seeking to obtain and disseminate confidential data. Governments worldwide have made an attempt to crack down on these groups in response to the actions taken by them. Several countries, including the United States (Federal Bureau of Investigation, 2011a; 2011b; Department of Justice, 2011), the United Kingdom (Halliday, Arthur, & Ball, 2011; Halliday, 2011b), Spain (Tremlett, 2011), France (Manach, 2012), the Netherlands (Associated Press, 2011), Italy, Switzerland, Turkey (Harris, 2011), Argentina, Chile, and Colombia (Associated Press, 2012) have made arrests and have raided residences belonging to Anonymous and LulzSec members. It is believed that hacktivist groups were responsible for more stolen data than cybercriminals during 2011 (Verizon, 2012), the first year that cybercriminals' participation in hacking was surpassed by another type of cyber actor. The infamy and notoriety gained by these organizations makes it clear; disseminated confidential information is a threatening phenomenon on the rise in the 21st century affecting governmental security worldwide. The Internet, the most crucial element for the facilitation of these groups' actions, is responsible for bringing them together.

The Internet is a blessing for the exchange of information between people, governments, corporations, and institutions worldwide. Its creation represents a paradigm

shift for the transmission of communication as it provides for the near instantaneous transfer of information. As a result, modern society has become dependent on the data flowing through the Internet's conduits. Electronic communications as simple as email, instant messaging, and voice-over-ip (VoIP) telephone calls to the more complex, such as web-based conferencing and video chatting, have become staples of life in much of the world. The use of these types of services is embedded into modern culture, and just as the morning routine and commute to work have become, are a part of everyday life. As of December 31, 2011 it was predicted that 78% of North America's and 32% of the world's population utilizes the Internet (World Internet Usage and Population Statistics, 2012). Cisco Systems, a world leader in computer networking technology, has predicted Internet traffic to increase by 32% a year from 2010 to 2015, and by 2015, there will be nearly a zettabyte (one billion terabytes) of information transferred annually via the Internet (Cisco, 2012a). In a companion study, the company also found more network devices than human beings were in existence at the end of 2011, and forecasted there to be two such devices for every human in existence by 2015 (Cisco, 2012b). The Internet has made a global penetration and is now a fundamental part of the 21st century's modernized society.

The Internet is also a curse. As society becomes ever more dependent on the luxuries afforded by the Internet, more opportunities arise for those wishing to take advantage of the reliance on digital data. Much like the real world's black market, a shadowy underworld exists on the Internet with the involvement of an innumerable amount of individuals and organizations. From hackers to hacktivists, cyber-criminals to cyber-terrorists, individuals and groups use the Internet to facilitate illegal activities

ranging from the benign or harmless to those of outright worldwide-organized criminal enterprise. In existence are Internet-based organizations which have stolen and disseminated confidential and private information for a variety of uses through various methods such as hacking into the databases of computer networks and websites, recording a user's keystrokes with employed computer viruses and/or trojans (key logging), or falsely soliciting passwords (phishing) through email or false websites.

Governments, militaries, and institutions fundamental to society such as banks and the media have come to rely on the capabilities of communication and data transfer provided by the Internet. Confidential data such as troop locations, covert government operations, embassy cables, end of the day bank account reconciliations, and business related email exchanges are routinely shared via the Internet between involved parties. The Internet has become instrumental for the operation and existence of these organizations, and because of this reliance, they now face risk of information being stolen, received by unintended parties, or simply falling into the wrong hands. Internet dependency has led to experiences of unforeseen and uncalculated events that have caused harm and disseminated confidential data, such as WikiLeaks' release of Stratfor's internal emails and multiple releases of United States government and military documents.

As a result of Internet dependence, securing digitized data and information on computer networks has become a pivotal issue in the 21st century. Governments worldwide have a vested interest in keeping their secret and confidential data out of the public eye. This issue was summed by Patrick Kennedy, the U.S. State Department's

Under Secretary of State for Management, in testimony presented to the United States Senate Committee on Homeland Security and Governmental Affairs on March 10, 2011:

.....The post-WikiLeaks environment reminds us that technology is a tool to execute solutions but is not in itself the answer. Simply put, we must more consistently sort out what we share before determining how we share it.

Connecting systems and networks may provide the means to share information, but we must still manage and share the content in the most appropriate way.

(Information sharing in, 2011).

As the previously mentioned institutions increasingly depend on computers and the Internet for their operations, it has become imperative to develop and routinely revise policies and procedures for conducting digital operations.

An understanding of how data is obtained disseminated and other issues pertaining to Internet security is important. When information is not managed correctly it can become *leaked*, or unintentionally disclosed or released, beyond its intended users. For the United States, the past century has witnessed several monumental and high profile leaks. Daniel Ellsberg, in 1971, gained access to confidential military documents while employed at Rand Corporation and leaked to the New York Times what became known as *The Pentagon Papers*. The papers generated controversy and a battle over their release found its way to the Supreme Court of the United States. In *New York Times Co. v. United State* (1971), it was decided that the Washington Post and New York Times (which later would become a WikiLeaks partner), under the privilege afforded to them by the First Amendment, could publish the information they received. *New York Times Co. v. United States* (1971) serves as a key First Amendment case. The following year, 1972,

FBI Associate Director Mark Felt, known at the time as the informant *Deep Throat*, leaked information relating to the Watergate scandal to the Washington Post. President Nixon resigned two years later. More recently the 21st century has witnessed the *United States v. Libby (2005)* scandal, the leaking of Gen. Stanley McChrystal's report regarding a troop surge in Afghanistan to The Washington Post's Bob Woodward (Woodward, 2009), and the formation of WikiLeaks, an organization which has gained infamy as the facilitator of history's largest leaks. All of these occurrences are related; information which is disseminated is received rather than retrieved by the releasing actors. This is not always the case although, as several groups seek to gather data themselves.

Information is also retrieved, analyzed, and disseminated to the public via computer hacking. Hacking, in its various forms, has always co-existed and co-evolved with computers. The original hackers of the 1960s and 1970s were students at American universities and were primarily interested in the workings of a developing technology. Their history has been described in detail by Stephen Levy in *Hackers: Heroes of the Computer Revolution* (1984), a seminal publication for the history of the rise of computer hacking. Hacking as it is known today began in the 1970s with the tampering of the telephone communication systems grid, also known as *phreaking*. John Draper who acted under the alias of *Captain Crunch* and Josef Engressia as *Joybubbles* were the most well-known phreakers of the decade and were both arrested for their activities involving the manipulation of the telephone communication grid and systems (McCraken, 2007). Draper would eventually move on to collaborate with Apple founders Steve Wozniak and Steve Jobs (Markoff, 2011).

Following phreaking, the 1980s were associated with the rise in the prominence of personal computers and the following surge in computer hacking. Formation of the first well-known hacker groups Legion of Doom, Masters of Deception, and The Cult of the Dead Cow (CDC) occurred during the middle part of the decade. Kevin Mitnick, one of history's most notorious hackers, began hacking during the period. The coining of the term *computer virus* by Fred Cohen (Cohen, 1984) and the start of popular hacker magazine *2600: A Hacker Quarterly* (2600, 2012) both occurred in 1984. The following decade, the 1990s, heralded in the creation of the World Wide Web, the emergence of Internet-based and spread computer viruses, worms, and trojans, and the first major occurrences of computer crime and the resulting law enforcement crackdowns. Operation Sundevil, conducted in 1990 by the United States Secret Service, served warrants in fourteen states to arrest hackers involved in credit card and computer fraud, and was one of the first wide spread media accounts of the United States government combating hackers (Sterling, 1992; Halbert, 1997). Kevin Mitnick, who at the time of his arrest was the United States most wanted computer criminal, was arrested in 1995 after five years on the lam and charged to forty-eight months of prison in 1999 (Department of Justice, 1995). The detention of Mitnick spawned the well-known *Free Kevin* campaign of the Internet underground during the decade (Coleman & Golub, 2008). The first DEFCON, today's largest computer hacking convention, started in 1993 (Official DEF CON, 2012).

The first decade of the 21st century experienced several high profile politically motivated and cyber theft hackings. Gary McKinnon, during 2001 and 2002, hacked into the networks belonging to the United States military and NASA in what was described as history's most prolific military hacking (Burns, 2009). McKinnon has been engaged in a

nearly ten-year long extradition battle between the United Kingdom and the United States. Alberto Gonzalez, who stole over 170 million financial related account numbers during a period of several years in the 2000s, was given a twenty year sentence in 2010, the longest sentence ever received for a computer crime (Verini, 2010). Most recently, in March 2012, the United States government arrested several individuals associated with the Anonymous, LulzSec, and AntiSec movements in a multi-state sweep, who were all indicted for their politically motivated hackings which saw the release of personal information belonging to law enforcement and military officials as well as internal documents belonging to several corporations and government agencies (United States v. Monsegur, 2012; United States v. Hammond, 2012; United States v. Ackroyd et al., 2012). During prior decades the hacker community, including CDC and 2600, staunchly protested hackers disrupting or harming networks for political reasons (D' Amico, 1999; 2600, 1999). The recent formation of the Anonymous organization and several related offshoots groups represents a shift in hacker ethic and these groups will be discussed in detail by this research.

The United States has attempted to combat leaking and hacking through legislation. The government's first legislative act making it a crime to access a computer network when not authorized and to disseminate stolen digital data was the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 which was later modified and became the Computer Fraud and Abuse Act of 1986 (CFFA). Important lawsuits involving provisions enacted by the CFFA include *United States v. Riggs* (1980) and *United States v. Morris* (1991). In *Riggs* the defendant was charged by the federal government for stealing and disseminating confidential data belonging to the telephone

company Bellsouth to hacker publication *PHRACK*, and in *Morris* the defendant was convicted of creating of one of the Internet's first worm-type viruses. *Riggs* and *Morris* serve as prominent cases for the United States government's prosecution of information disseminating computer crimes. The CFFA has also been used in several recent high profile cases: *United States v. Manning* (2011) is the ongoing court martial of Bradley Manning who has been charged with disseminating confidential United States Army intelligence; and *Sony Computer Entertainment America LLC v. Hotz et al.* (2011) in which defendants were charged for *jailbreaking*, or bypassing security measure to modify and/or explore an operating system, the PlayStation 3. In 1986, the same year as the enactment of the CFAA, the Electronic Communications Privacy Act of 1986 (ECPA) was passed that allowed for the government to expand wiretaps to electronic communications. Both CFAA and ECPA were modified by the US PATRIOT Act (2001).

Research conducted within this thesis will focus on the following groups which have in recent times gained a substantial amount of fame and attention for being involved in data leaks and hacking: hacker collective Anonymous, affiliated group LulzSec, and the associated movement AntiSec. These groups formed during the first decade of the 21st century as small organizations and have grown to become media staples garnering headlines across the globe. Information possessed by these organizations is handled in a similar fashion; each group hacks into computer networks to retrieve data and disseminates it to the public via the Internet and/or traditional media. The motivations for these groups appear similar as they all engage in anti-government activities and seek to make the public more aware of what occurs behind the closed doors of the world's most

powerful institutions and establishments. This research seeks to determine these motivations.

CHAPTER II

LITERATURE REVIEW

By understanding issues pertaining to hackers, such as motivation and typology, the correct analysis of this study's subjects can be conducted. The following concepts and classifications of actors involved in the cyber-acts discussed in this study will provide for profile definitions to be used as categories in the following Analysis chapter. Statements produced by the United States government and government actors pertaining to the typology and profiles of these groups will be additionally examined and synthesized.

Expansionists and Instrumentalists

Internet *instrumentalism* and *expansionism* are recent developments and are becoming more relevant to criminological and governmental studies as a result in the rise in the actions of groups seeking to disseminate confidential data, such as WikiLeaks and Anonymous. The work of Tavani (2005), Hwang (2010), and Sterner (2011) have provided the foundation of these evolving concepts.

Before the formation of WikiLeaks and Anonymous, Herman Tavani (2005) wrote about expansionists and what he labeled as *traditionalists*. In Tavani's case, *traditionalist* is another term for *instrumentalists*. Tavani described the relation between expansionists and traditionalists as a battle between the two relating to Internet and ethical behavior and examined whether advances in technology have altered existing or have created entirely new ethical conditions of man and if so, a revision to the ethical

framework is required. The ethical framework of man to Tavi is thought as the “system that is composed of normative principles, rules, and theories” (p. 217). Traditionalists believe ethical issues which are attributed to the advent of the Internet can be dealt with using the existing ethical framework. Expansionists believe the Internet has created new ethical issues with which to contend due to the Internet allowing for a much larger scale and scope of acts which can be potentially committed by those manipulating the Internet’s capabilities and that the existing ethical framework is not adequate to deal with these new issues (Tavani, 2005).

Expanding upon Tavani’s work, Tim Hwang (2010) wrote of expansionists and instrumentalists in article published by the Washington Post. Hwang likened the battle waged between governments and Internet activists on the Internet today to the period spanning between the start of World War I to the end of World War II and to the period in which South East Asia experienced the Korean and Vietnam wars. These conflicts are described as a *long war*: a war that, when observed over a long period of time, is not just a string of separate battles with differing catalysts and objectives but an overall war waged between democratic, communist, and fascist political systems competing for world domination. Hwang believes the Internet is involved in a similar type of long war: a war between the expansionists who fight for Internet freedom and government transparency and the instrumentalists who seek to mold the Internet to fit the world’s existing institutions and law (Hwang, 2010).

Eric Sterner (2011) of the George C. Marshall Institute expanded upon Hwang’s descriptions of the two views, using the same type of conflict-like writing style as Hwang, and applied the concepts to the WikiLeaks organization and government. To

Sternier, expansionists view the Internet as a requirement for freedom as it allows for individuals to be liberated and empowered above the constraints imposed upon them by social institutions. Expansionists value information and believe it should be allowed to flow freely and that any institution withholding it is doing humanity a disfavor.

Instrumentalists, on the other hand, value the safeguarding of information and see to it that information which is confidential remains so. Control of the information sharing infrastructure, of which the Internet is a component, is a key aspect for protecting the information instrumentalists wish to safeguard (Sternier, 2011).

Hackers

The term *hacker* has changed greatly over the years but is most commonly used today to describe an individual who is engaged in a wide variety of acts involving computers and computer networks. The Jargon File, created in 1975, served as the original collection of computer terminology and slang reflecting the values and culture of the original hacker communities (The Jargon File 4.4.7., 2012, Revision History section). It has been continually revised since its creation and has seen publication as Guy Steele's *The Hackers Dictionary* (1983) and as Eric S. Raymond's *The New Hackers Dictionary* (1986). The most current version of the Jargon File, 4.4.7 as of the time of this writing, defines a hacker as:

1. 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.
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is cracker. (The Jargon File 4.4.7., 2012, The Jargon Lexicon section)

More recent descriptions of hackers and activities carried out by them include those who engage in acts of accessing remote computer systems (Mizrach, 1997, Who is the computer underground); covertly revealing, manipulating, and exploiting vulnerabilities discovered in computer operating systems and software (Stohl, 2006, p. 236); reconfiguring and altering functions of computer hardware and software (Bachmann, 2010, p. 643); and trespassing into another's system or network (Himma, 2007, p. 87). The United States Computer Fraud and Abuse Act (1986) addresses those engaged in cyber-crime and hacking-like activities without specifically mentioning *hacker*, but for all purposes, including those considered as hackers, as an actor who "intentionally accesses a computer without authorization or exceeds authorized access..." (18 U.S.C. § 1030 (A) (2)).

The origin and evolution of hackers and hacking have been discussed at great length by Steven Levy in his seminal work, 1984's *Hackers: Heroes of the Computer Revolution*. Levy's work details the original hacking movement which began at the Massachusetts Institute of Technology's Artificial Intelligence Laboratory (MIT AI) and Stanford's Artificial Intelligence Laboratory (SAIL) during the 1960s. This first generation of hackers was perceived by the public without negative connotations and, as Levy (2010) describes, adhered and operated within an ethical framework of the following tenets: "Hands-On Imperative," meaning that people should have total access to computers and technology, and no barrier should exist between the two; "All information should be free," meaning that information should be free-flowing and without restriction in regards to restriction, control, and cost; "Mistrust Authority - Promote Decentralization," meaning that the original hackers believed bureaucratic and institutional control of technology would one day exist and the decentralization of computing would be necessary; "...Bogus Criteria," meaning that hackers are to be judged by their hacking activities and exploits (as in how they contribute to the hacking subculture) and not characteristics of gender, race, income, etc.; "You can create art and beauty on a computer," meaning that simple and efficient programming code is a work of art to hackers and different hackers will have their own unique style and approach; and "Computers can change your life for the better," meaning that the automation and unlimited potential possessed by computers and the ethic promoted by computer hackers can benefit the entire world and all of its inhabitants (Levy, 2010, pp. 28-31).

Following Levy's analysis and historical account of the original hackers, cyber-anthropologist Steven Mizrach (1997) revised the ethical framework for hackers

operating during the 1990s. Mizrach concluded the new ethical code to reflect the following tenets: “Above all else, do no harm,” meaning that computer systems, networks, and data they contain, if avoidable, are not to be damaged; “Protect Privacy,” meaning that it is necessary to protect and respect your own personal information; “Waste not, want not,” meaning that people should not be barred from access to computer systems when they are not in use; “Exceed Limitations,” meaning that hackers should attempt to solve problems and push current limitations; “The communicational imperative,” meaning that the capability of communication between individuals is a universal right and it should not be infringed upon; “Leave no traces,” meaning that hackers should not leave behind digital-like paper trails or foot prints in order for themselves, and other hackers, to avoid detection and subsequent repercussions; “Share!,” meaning that hackers are to share information with each other; “Self Defense,” meaning that hackers are to use their methods to attack powerful institutions (such as government and corporations) which can become overbearing and restrict individual rights, and as a result, are to be counter-attacked in self-defense if they attempt to restrict hackers; “Hacking Helps Security,” meaning that computer hacking is beneficial as it corrects security flaws and brings attention to the public issues of how important security, or the lack of, is to them; and “Trust, but Test!,” meaning that hackers should take the maintenance and manipulation of network systems into their own hands in order to have a better understanding for themselves and to further advance and evolve those systems for the better (Mizrach, 1997).

Mizrach (1997) further proposed that against the tenets of the new hacker ethics were acts of “Bootlegging,” or exploits of financially profitable hacking; “Freeloading,”

or never contributing to the hacking community and knowledgebase; “Trashing,” or malicious acts which destroy and damage computer hardware, software, and data; “Excessive Selfishness,” meaning the hacker movement should be communal and self-interest does nothing to advance and promote the cause; “The (Selective) Anti-Stealing Ethic,” meaning that the taking of information or theft of services from large governments and corporations is acceptable, but never from smaller, non-threatening entities or non-profit organizations, as computer data is not a tangible item that can be stolen in the traditional sense but can still be thieved; “Bragging,” meaning that hackers may brag to themselves, but never to governmental actors, systems administrators, or any authoritative figures, as well as distasteful public bragging, and especially never to the media; “Spying,” meaning that infringing upon what others expect to have a sense of privacy over is wrong; and “Narcising,” meaning that hackers are to not reveal or turn other hackers in to authorities (Mizrach, 1997).

Hacker ethics, according to Chiesa, Ducci, and Ciappi (2009), are adhered to by some form of hackers and rejected by others. Those who adhere to the code of ethics are constructive, hack to the best of their ability, and seek to improve computer and Internet security, and believe in the free flow and access of information (p. 175). Hackers who reject following the code do so for various reasons; such as a case-by-case rejection for financial gain, to stop to the flow of information, or those who work to put power back into the hands of institutions rather than individuals (pp. 175-176).

Today's hackers are negatively perceived as criminals who engage in acts of exploiting computer's vulnerabilities (Bachmann, 2010, p. 644). Hackers in general are more psychologically rational than intuitive, have high confidence in their approach to

problem solving, prefer complex to simple problems, and engage in more risky behavior than the general public (Bachmann, 2010, p. 652). They are the thrill seeking type and often wish to compete amongst each other (Ronczkowski, 2007, p. 223), and believe their activities are acceptable and justified as long as they do not harm or damage systems that are hacked into during the course of their actions (Young, Zhang, & Prybutok, 2008, p. 285). Not all forms of hacking and related beliefs of hackers are the same although as hackers are motivated for different reasons and engage in a wide variety of cyber-acts utilizing various methods. As a result of hacking's wide spectrum, several classifications of hackers exist. For the purpose of this study, three commonly known types will be discussed and used: black-hat, white-hat, and grey-hat. Hacktivists, a new phenomenon of hackers, will also be discussed in detail.

Black-hat hackers are those whose acts are carried out malicious intent (Graves, 2009, p. 4) and are illicit and/or illegal (Bachmann, 2010, p. 644). Malicious hacker activities have a wide breadth, from stealing bank and credit card account numbers, to bringing down websites, *bot herding* (infecting computers in order to carry out attacks remotely), and sharing information on vulnerabilities and exploits (Harper et al., 2009). Black-hats also destroy computer data and deny services to users of computer systems (Graves, 2010, p. 4) and penetrate computer systems regardless of opportunities for personal advantage (Chiesa et al., 2009, p. 47). The term refers to villainous cowboy-type characters in older western films which often were identified as the "bad guys" due to their black cowboy hats.

White-hat hackers are those whose actions are ethical and lack malicious intent (Graves, 2010, p. 4; Chiesa et al., 2009, p. 47). White-hat hacking is done with

permission by IT professionals (Graves, 2010, p. 4), those assisting authorities and the government (Chiesa et al., 2009, p. 47), academic researchers, and consultants employed to analyze performance and to discover any vulnerabilities for a target system (Red Hat, Inc., 2011, para. 1.3.1.1). Vulnerabilities discovered by white-hats are exploited and addressed with authorization (Harper et al., 2009, p. 47). In this case, the color white is used to identify them as the opposite of black-hat hackers as well as representing their pure and non-evil intentions. An example of a white-hat is someone who hacks into a computer which utilizes the Microsoft Windows operating system and in turn notifies Microsoft on the method for how the hack was carried out. Microsoft, in turn, can develop and distribute a *patch*, or solution, for the operation system vulnerability to fix the problem so all users of that particular version of Microsoft Windows will be protected from any black-hats who may try to exploit their way in.

Gray-hat hackers are those whose actions are a blend of the actions carried out by both black-and white-hat hackers. They neither adhere to nor disdain hacker ethics, such as white-and black-hats, but hack based upon mood or presented opportunity (Holt, 2010). When engaging in acts analogous to those conducted by white-hats, they differ as white-hats often have permission, whereas gray hats do not (Graves, 2010). Grey hats have been likened to or as white-hat hackers, such as Harper et al.s (2009) description of gray-hat hackers that engage in acts of discovering vulnerabilities, not exploiting them, and then notifying the creator in order for a patch to be developed to address the problem or issue. Grey-hats have also been likened to or as black-hats hackers when described as having the know-how and purpose of white-hat hackers but engaging in activities against the white-hats hackers' code of ethics (Red Hat, Inc., 2011, p. 19). Grey-hats have also

been described as outright refusing any labels which are attributed to them (Chiesa et al., 2009). For purpose of this research, cyber-acts and hacks that are neither malicious but not carried out with permission, or motivated by humorous ambition, fall into the category of gray-hat hacking.

Hactivists

The Internet has given birth to a new form of activism known as *hacktivism*; a combination of the terms hacking and activism. Hacktivism is the activity *hacktivists* engage in, just as activism is the activity activists engage in. Hacktivism is a phenomenon on the rise with focus on 2012 as a decisive year for the magnitude and importance of hacktivist related activities (McAfee Labs, 2011). According to Verizon, 2011 experienced the most significant increase in the amount of attacks on large organizations since the company began collecting its data starting in 2005; out of the 174 million total records released by hackers that year, 100 million were attributed to hacktivists, representing 58% of all data stolen by hackers in 2011 (Verizon, 2012). Hacktivism is not a recently created phenomenon however, as the origin of term can be dated back to the 1990s. A New York Times article titled '*Hactivists' of All Persuasions Take Their Struggle to the Web*' (Harmon, 1998) and journal article titled *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics* (Wray, 1998) were both published in 1998.

Hactivists are politically motivated and driven (Conway, 2007, p. 82; Himma, 2007, p. 87; Manion & Goodrum, 2000, p. 14; Samuel, 2004; Ronczkowski, 2007, p. 224). Unlike other types of hackers, they are not motivated for financial gain and often

seek revenge against their targets (M.G., 2011). They utilize computer systems to engage in civil disobedience (Denning, 2001, p. 263; Himma, 2007; Ronczkowski, 2007, p. 223); a non-violent and non-destructive breaking of perceived unjustified laws (Manion & Goodrum, 2000, p. 14). Hacktivists also engage in acts of digital protest and disruption against their targets and opponents (McLaurin, 2011, p. 233; Conway, 2007, p. 88), acts which can be considered as disobedience. These attacks against government and corporations are seen as a legitimate response to indifferences (McLaurin, 2011, p. 233-234). Not all hacktivists activities are classified as civil-disobedience, as some of the acts perpetrated by hacktivists are actual acts of cyber-crime (Mansfield-Devine, 2011, p. 7; McLaurin, 2011). Hacktivists differ from other classifications of hackers by publically disclosing what information was retrieved, such as computer account passwords, street addresses, and email addresses, and the method for how the hacking was accomplished (Mansfield-Devine, 2011, p. 10).

Hacktivists carry out their attacks by a variety methods such as electronic graffiti (Conway, 2007), website redirects (Hampson, 2012), theft of publications and information (Conway, 2007; Hampson, 2012), and denial of service (DoS) and distributed denial of service (DDoS) attacks (McLaurin, 2011; Hampson, 2012; Conway, 2007). DDoS attacks involve utilizing multiple computers to send out a massive amount of packets to a target website with the intention of shutting down the website to legitimate traffic (Mirvokic & Reiher, 2004).

Cyber Terrorists

Hactivism and other forms of hacking mentioned are often mislabeled or misunderstood as acts of *cyberterrorism* (Weimann, 2005, p. 135; Conway, 2007, pp. 82;

Stohl, 2006, p. 236; Talihärm, 2010, p. 62). This presents a problem, as it is important for acts that are not cyber-terroristic in nature to not be labeled as such, and by doing so, an untrue and misunderstood fear of cyberterrorism is continued to be propagated by the media (Weimann, 2005, p. 132; Conway, 2007, p. 82) and government (Stohl, 2006). The concern can partly be attributed to the fact that cyberterrorism is loosely defined and there is a lack of cohesive terminology regarding the term (Gordon & Ford, 2003, p. 3; Wilson, 2003, CRS-4; Conway, 2007, Conway, 2007, p. 78). As a result, acts committed via the Internet and the actors responsible for their execution are mislabeled and placed into erroneous categories.

Cyberterrorism has been defined by several researchers and academics in varying ways. Denning (2007) defined cyberterrorism as “highly damaging computer-based attacks or threats of attacks by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social” (p. 124). A previous and often cited definition by Denning (2000) is included in her congressional testimony to the Special Oversight Panel on Terrorism of the U.S. House of Representatives' Committee on Armed Services:

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe

economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

(*Cyberterrorism, 2000*)

Wilson has defined cyberterrorism as “politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies” (Wilson, 2003, CRS-4) and as “use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies” (Wilson, 2005, CRS-7). Wilson and Rollins (2007) devised two further definitions for cyberterrorism: *effects-based* that “exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals” and *intent-based* that “exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage” (Wilson & Rollins, 2007, CRS-3).

Additional definitions for cyberterrorism include those of Weimann (2005) as “the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)” (p. 130) and Talihärm (2010) as “politically or socially motivated attacks against computers, network and information, whether concluded through other computers or physically while causing injures or bloodshed, serious damage or fear comparable to a traditional act of terrorism” (pg. 60).

Although the examples and definitions provided in this chapter are far from constituting as a comprehensive review of all instances inferring a definition of cyberterrorism, it is apparent that no conclusive, cohesive, universally accepted definition for cyber-terrorism exists. A loose usage of the term is evident when the definitions range from attempting to influence a government, to causing physiological fear, to disrupting critical infrastructure systems, or to cause actual physical violence such as traditional acts of terrorism do.

The most important difference between cyberterrorism and hacktivism lies in the intent of the acts committed. Hacktivism does not seek for its acts to physically harm or maim or cause fear by the intimidation of violence or physical threat (Talihärm, 2010, p. 65; Weimann, 2005, p. 136; Conway, 2007; Himma, 2007, p. 92; Samuel, 2004; Manion & Goodrum, 2000, p. 16). Cyberterrorism should be seen as the facilitation of the traditional terrorist activities of causing psychological fear and physical harm via computer systems (Talihärm, 2010, p. 67). It is important to apply the cyberterrorism term only to cyber-activities in which a component of traditional terrorism is used (Stohl, 2006, p. 229), and the use of the term does not reflect acts of electronic civil disobedience (Manion & Goodrum, 2000, Hacktivism and Cyberterrorism section, para. 1).

Government Profiles

Several United States government agencies have released memos, press statements, and other various publications regarding Anonymous, LulzSec, and AntiSec. As expected, these publications are often very condemning of these groups. A wide

variety of terminology is used and a synthesis of the labels and profiles delineated to them follows.

Anonymous has been labeled by the United States Attorney's Office as a "hacking group," (United States Department of Justice, United States Attorney's Office, Central District of California, 2011; U.S. DOJ, USAO, Northern District of California, 2011a) and "loose confederation of computer hackers" (U.S. DOJ, USAO, Southern District of California, 2011), and by the FBI as a "hacktivist group," (Cybersecurity: Responding to the; U.S. DOJ, Federal Bureau of Investigation, 2011), and as a "collective of computer hackers and other individuals located throughout the world that conduct cyber attacks, including the dissemination of confidential information stolen from victims' computers, against individuals and entities they perceive to be hostile to its interests" (U.S. DOJ, F.B.I., Los Angeles Division, 2011). The United States District Court of Northern California described Anonymous in a grand jury indictment as "an online collective of individuals that was associated with collaborative hacking attacks motivated by political and social goals, often referred to as 'hacktivism'" (United States v. Collins et al., 2011). The United States Department of Homeland Security labeled Anonymous as a "loosely organized hacking collective" (United States Department of Homeland Security, 2011c), a "hacktivist collective" (U.S. DHS, 2011d), a "hacking group" (U.S. DHS, 2011b), and as a "hacker collective" that seeks uses the "...the internet to recruit and train new personnel, conduct reconnaissance on potential targets, exploit vulnerabilities found in information systems, deny access to resources, alter information presented by organizations, and steal sensitive information" (U.S. DHS, 2011a).

LulzSec, just like Anonymous, has been called a “computer hacking group” by the F.B.I. and United States Attorney’s Office on multiple occasions (U.S. DOJ, F.B.I., Los Angeles Division, 2011; U.S. DOJ, USAO, Northern District of California, 2011b; U.S. DOJ, USAO, District of New Jersey). The Department of Homeland Security has referred to them as a “hactivist collective” whose membership is composed of “former anonymous members who use hacker tools to hijack or deface websites as a political statement” (U.S. DHS, 2011d). LulzSec has also been referred to as a “known cyber known cyber terrorism group” by the Arizona Department of Public Safety (Arizona Department of Public Safety, 2011a).

AntiSec has also been labeled by the Arizona Department of Public Safety as a “cyber-terrorism group,” just as LulzSec had been (Arizona Department of Public Safety, 2011b). A United States Attorney’s Office press release specifically linked AntiSec to Anonymous and LulzSec by stating that:

...in publicizing the Stratfor hack, members of AntiSec reaffirmed their connection to Anonymous and other related groups, including LulzSec. For example, AntiSec members published a document with links to the stolen Stratfor data entitled: ‘Anonymous LulzXmas rooting you proud’ on a file sharing website.

(U.S. DOJ, USAO, Southern District of California, 2011).

The Department of Homeland Security has stated that AntiSec is “designed to demonstrate the weakness of general internet security” and has been successful in the “compromise of sensitive by unclassified law enforcement and intelligence data” (U.S. DHS, 2011d).

The most clear cut example of the United States labeling these groups comes from the events of a single day in which all groups were simultaneously labeled together. On March 6th, 2012, the United States Department of Justice unsealed indictments for six members of Anonymous, LulzSec, and AntiSec. In the press releases and court documents released, Anonymous was referred to as a “loose confederation of computer hackers” (U.S. DOJ, USAO, Southern District of New York, 2012) whose indicted members engaged in “a deliberate campaign of online destruction, intimidation, and criminality, as part of which they have carried out cyber attacks against businesses and government entities in the United State and throughout the world” (United States v. O’Cearrbhail, 2011; United States v. Ackroyd et al., 2011; United States v. Hammond) and in “‘operations’ – that is, coordinated efforts that included cyber attacks – against individuals and entities that were perceived to be hostile to Anonymous and its members interests” (United States v. Monsegur, 2011). Much like Anonymous, an indictment alleged that LulzSec engaged in “acts online destruction and criminality” and were known to “announce their hacks and issue written ‘press releases’ about them; mock their victims; solicit donations; and publically disclose confidential information they had stolen through their cyber attacks”(United States v. Ackroyd, 2011).

Anonymous was described explicitly in the indictment of Hector Xavier Monsegur (also known as LulzSec leader *Sabu*) as:

A collective of computer hackers and other individuals located in the United States and elsewhere that undertook ‘operations’ -- that is, coordinated efforts that included cyber attacks -- against individuals and entities that were perceived to be hostile to Anonymous and its members' interests. These attacks included, among

other things, the theft and later dissemination of confidential information from computer systems and the defacement of internet websites. These attacks also included attacks against websites, known as ‘denial of service’ or ‘DoS’ attacks, which involved the use of computers to bombard a victim's website with bogus requests for information, causing the website to temporarily cease functioning. (United States v. Monsegur, 2011).

When synthesized together these statements show that several terms and descriptions for Anonymous, LulzSec, and AntiSec have been used by the United States government. Although wide ranging and not bound to unified terminology, the government has clearly condemned these groups’ actions of hacking, hacktivism, and information dissemination which the government has alleged were conducted with malicious and politically opposing intent. As with the issue between cyber-terrorism and hacktivism, it is important that these groups are viewed and label appropriately in order for government understanding and operations to combat to them to be effective.

CHAPTER III

HISTORY

Anonymous has a long and storied history. Formed during 2003 from the image message board community of 4chan, the group exists without a centralized leadership structure and operates under the premise that anyone can be a member of Anonymous simply by conducting acts in its name. Anonymous activities are frequently publicized by several different prominent Twitter accounts such as AnonymousIRC (<http://twitter.com/anonymousirc>), YourAnonNews (<http://twitter.com/youranonnews>), and AnonOps (<http://twitter.com/anonops>). Compiling the history of events and publications from Anonymous and all the various sects within the organization into a historical compendium would be a project in itself. Two recent works, Cole Stryker's *Epic Win for Anonymous: How 4Chan's Army Conquered the Web* (2011) and Parmy Olson's *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (2012) are the most comprehensive publicized works detailing the history of Anonymous and also include in-depth histories for LulzSec and AntiSec.

This section, a historical review, is mostly limited to LulzSec and AntiSec. LulzSec, an Internet hacktivist group, formed and began operations during the spring of 2011 and unlike Anonymous adhered to an organized leadership structure. At the helm of the LulzSec operation was a person known by the Internet moniker Sabu who led core members: Topiary, operator of the group's public relations; Kayla, operator of a large

botnet; T-Flow, operator of the group's website and computer programmer; Avunit, and Pwnsauce (Poeter, 2011; Halliday, 2011a). A message produced by the group (See Appendix G) mentioned and confirmed further associations with Joepie91, Neuron, Storm, Trollpoll, Voodoo , and m_nerva, an associate turned adversary who leaked LulzSec chat room logs to The Guardian (Gallagher & Arthur, 2011; LulzSec, 2011m). Additionally linked persons included: Ryan Cleary of Wickford, Essex, United Kingdom who assisted LulzSec and operated the chat servers used by the group (Dodd, Halliday, & Arthur, 2011); Anarchaos, who participated in the Stratfor hack (United States v. Hammond, 2012), Recursion, who participated in LulzSec activities against Sony (Geuss, 2012); and Palladium, who participated in the interception of a conference call between the FBI and London's Metropolitan Police (United States v. O'Cearrbhail, 2012).

The group operated for a brief two month stint during 2011 from the beginning of May to the end of June with a brief and temporary reprise in July. In that time LulzSec gained an immense amount of media coverage and attention by the United States government. Towards the end of their hacking spree LulzSec helped to establish the AntiSec movement with collaboration from Anonymous. AntiSec, motivated by the same goals and desires as LulzSec and Anonymous, took off in its own right and became very active in publishing hacks.

LulzSec and AntiSec released a majority of their releases on BitTorrent file sharing website The Pirate Bay. The release for each *operation*, or hack/vulnerability exploit conducted by these groups, contained a press release that detailed the organization attacked, information accessed and released, and motivation for doing so under a cleverly worded title. Official releases by these groups have been released on The Pirate Bay

under user accounts LulzSec (<http://thepiratebay.se/user/LulzSec>) and AntiSecurity (<http://thepiratebay.se/user/AntiSecurity>). LulzSec was very vocal about group activities and maintained a Twitter account (<http://twitter.com/LulzSec>) used to broadcast messages and to interact with the public. The group also maintained a website (<http://www.lulzsecurity.com>; no longer operational) which they protected from other hackers and DoS/DDoS attacks utilizing services provided by CloudFlare, a company that provides protection from attacks and optimizes global rerouting for their user's websites (Anderson, 2011; CloudFlare, 2011).

LulzSec's first notable actions occurred during early May, 2011. On May 6th, *The X-Factor*, a television show produced by the Fox Broadcasting Company, had its computer network hacked into and a database of contestants stolen by the group. The information obtained was released the following day on LulzSec's The Pirate Bay account titled as *X-Factor Leaked Contestants Database* (see Appendix A). The accompanying press release 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 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! (LulzSec, 2011r).

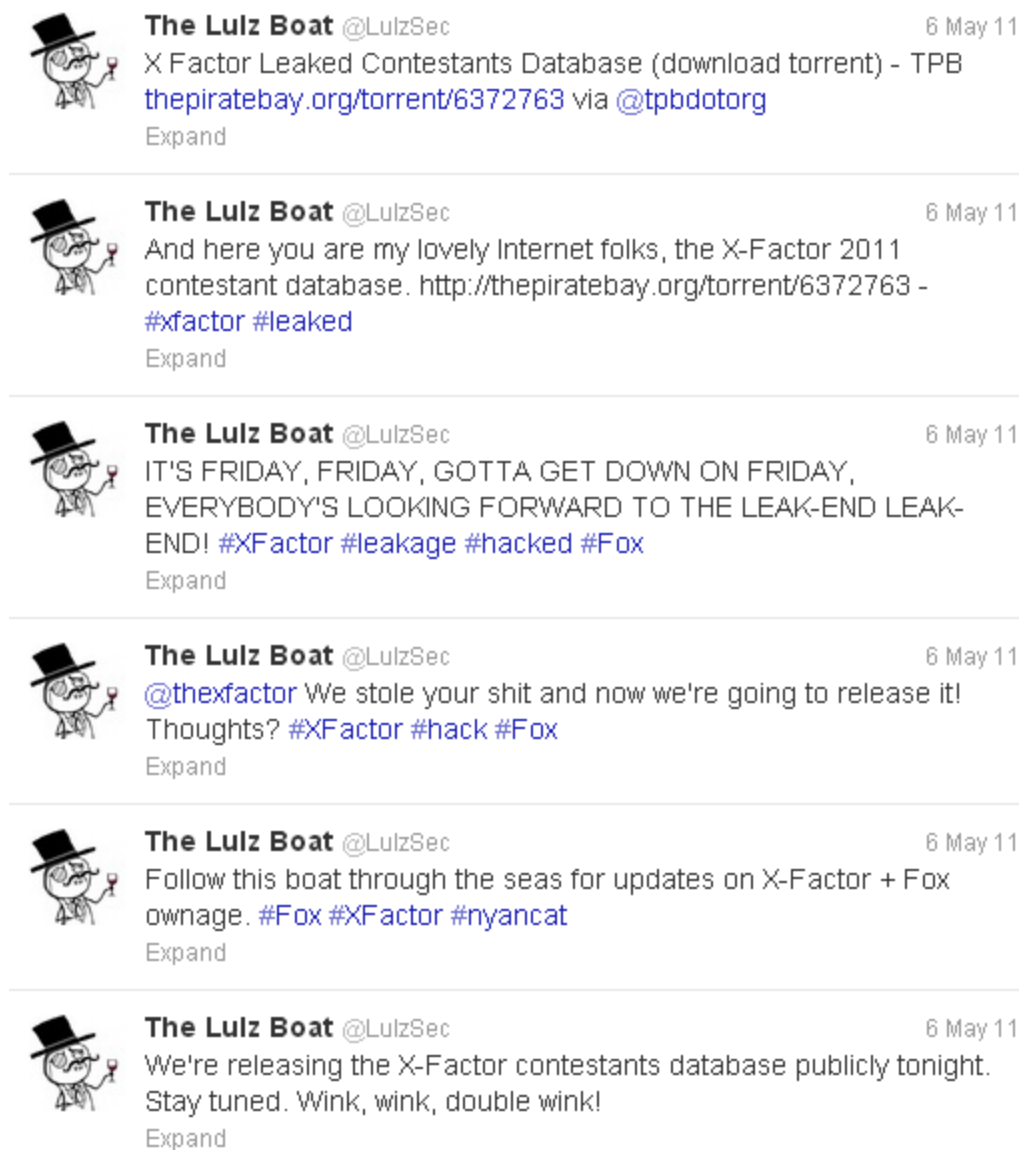


Figure 1. LulzSec Twitter post describing the group's first actions against the Fox media corporation. Posted on May 6th, 2011. Retrieved from <http://twitter.com/LulzSec>.

LulzSec's attack on Fox was not limited to the X-Factor television show as the network's primary website (<http://www.fox.com>) was hacked into by the group days after the initial X-Factor incident. An untitled May 11th pastebin post by LulzSec (see Appendix B) explained the Fox.com hack which stole similar information as their first:

Dear Fox.com,

We don't like you very much. As such, we cordially invite you to kiss our hand-crafted crescent fresh asses.

....

Well now we're leaking some more of your junk. We invite the Internet to ravage the following list of emails and passwords (from a database within Fox.com) - Facebook, MySpace, PayPal, whatever you can get your hands on. Take from them everything. Remember to proxy up, or tunnel like a pro!

.... (LulzSec, 2011q).

LulzSec announced on May 12th they were developing a website to host their hacks and leaks; the website was subsequently launched as www.lulzsecurity.com and was in operation until the group's demise. On May 13th a press statement titled *[LulzSec] Fox.com leakage phase 0/1/2/3* was released by the group to Pastebin that consolidated the previous Fox attacks with two further ones (see Appendix C):

Phase 0 - 73,000 X-Factor contestants leakage:

Phase 1 - 363 Fox.com email/password combinations leakage: (thank you for the mirror, anapnea.net <3 (@anapnea on twitter))

Phase 2 - Fox.com internal PHP fucktard security workings + additional login information (mostly hashed but lots of it):

Phase 3 - !! NEW !! OH MAH GAAAAWD NEW !! finishing taunt - Fox failed to provide us with candy, so we're tossing these additional 44 email/password combinations from Fox.com overboard:

.....

ENJOY AND DON'T FORGET TO BRUSH YOUR TEETH BECAUSE IT'S VERY IMPORTANT

Follow us on twitter, we're owning the FBI next! @LulzSec (LulzSec, 2011c).

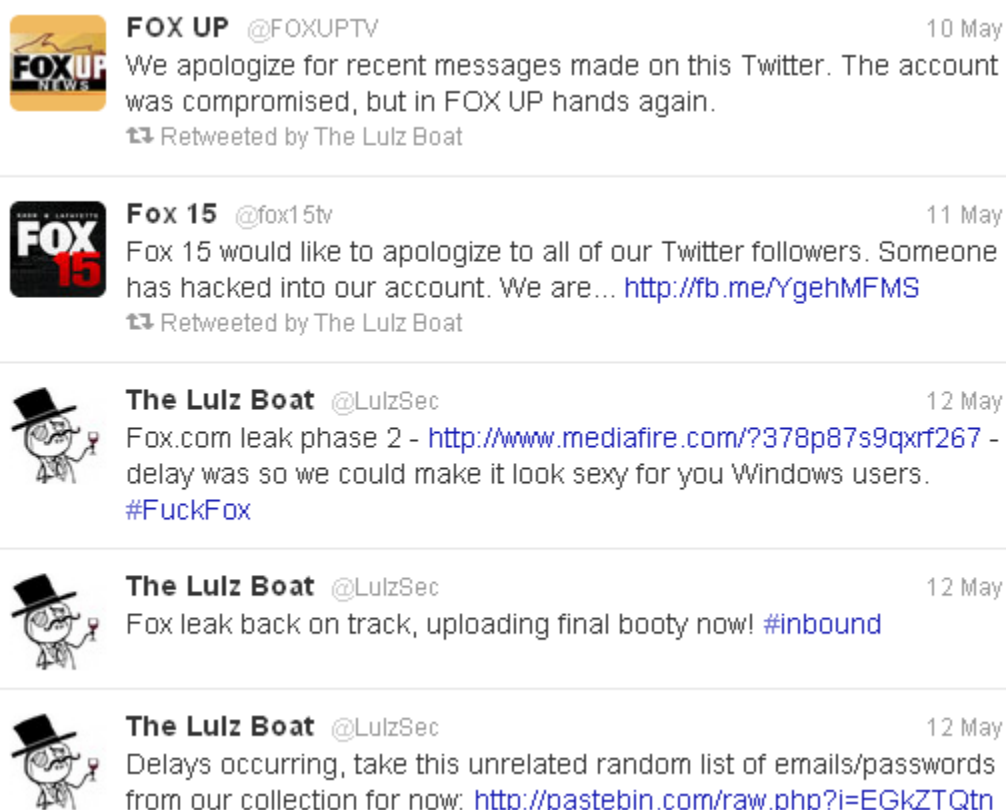


Figure 2. LulzSec Twitter post describing additional actions against the Fox media corporation. Posted on May 12th, 2011

On May 15th, LulzSec released a database for over 3,100 British ATM devices to pastebin titled *[ATM leak] ~LulzSec* (see Appendix D).. No motivation for the release was given by LulzSec other than it was a “leak of pointless ATM information” list (LulzSec, 2011b).

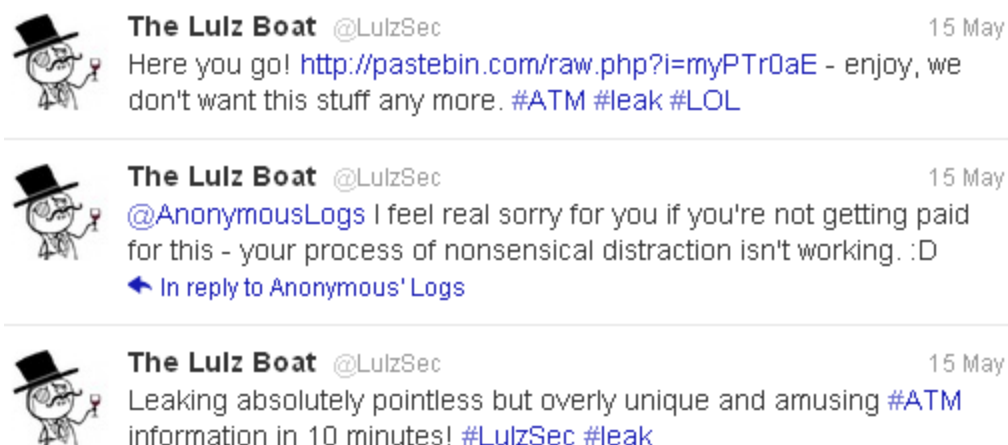


Figure 3. LulzSec Twitter post describing British ATM information.

Posted on May 15th, 2011

The following week, on May 23rd, LulzSec hacked the Japanese division of Sony Music Corporation and released two large SQL databases retrieved from the website. LulzSec did so for the purpose of the group wanting “to embarrass Sony some more” and alluded to other Sony hacks when they mockingly asked “Can this be hack 8? 7 and a half?!” (LulzSec, 2011j). The press release was posted to Pastebin as *LulzSec hates Sony too* (see Appendix E). Sony, at the time, had been experiencing intrusions into its network from other hackers (Bilton & Stelter, 2011) and just not from LulzSec.

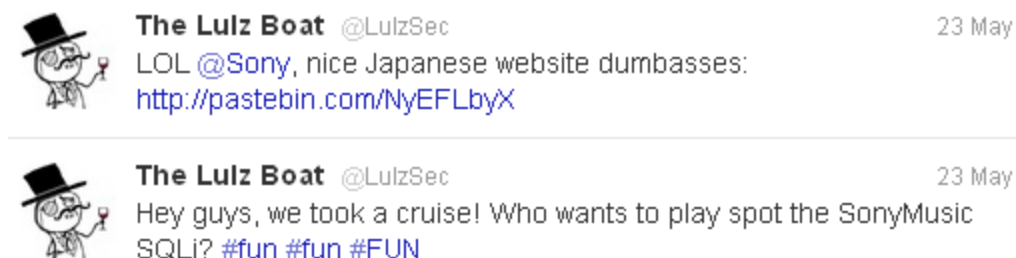


Figure 4. LulzSec Twitter post describing the Sony hack. Posted May 23rd, 2011.

LulzSec, the following week on May 30th, hacked into and defaced the Public Broadcasting Company's (PBS) website. The attack on PBS was in retaliation for a documentary PBS had aired on Julian Assange which LulzSec deemed to be an unjust and critical view of him. LulzSec announced they had "just finished watching WikiSecrets and were less than impressed. We decided to sail our Lulz Boat over to the PBS servers for further... perusing" (LulzSec, 2011i). Included in the website defacement was a fake news story that rapper Tupac Shakur was alive and well in New Zealand and his hideout had also housed fellow deceased and rival rapper The Notorious B.I.G.. Shakur was famously gunned down and murdered in Las Vegas in September, 1996 during a drive-by shooting. The attack on PBS also included an assortment of staff website passwords as well as a detailed listing of staff personnel. The leak was published to Pastebin as *LulzSec Hack PBS.ORG* (see Appendix F).


The Rundown
A BLOG OF NEWS AND INSIGHT
RSS FEED

« PREVIOUS ENTRY
BLOG MAIN

TUPAC -- May 29, 2011 at 11:30 PM EDT

Tupac still alive in New Zealand

BY: PBS WEB TECH

 Like 3.9k

Prominent rapper Tupac has been found alive and well in a small resort in New Zealand, locals report. The small town - unnamed due to security risks - allegedly housed Tupac and Biggie Smalls (another rapper) for several years. One local, David File, recently passed away, leaving evidence and reports of Tupac's visit in a diary, which he requested be shipped to his family in the United States.

"We were amazed to see what David left behind," said one of sisters, Jasmine, aged 31. "We thought it best to let the world know as we feel this doesn't deserve to be kept secret."

David, aged 28, was recently the victim of a hit-and-run by local known gangsters. Having suffered several bullet wounds on his way home from work, David was announced dead at the scene. Police found the diary in a bedside drawer.











"Naturally we didn't read the diary," one officer states. "We merely noted the request to have it sent to a US address, which we did to honor the wishes of David."

Officials have closed down routes into the town and will not speculate as to whether Tupac or Biggie have been transported to another region or country. Local townsfolk refuse to comment on exactly how long or why the rappers were being sheltered; one man simply says "we don't talk about that here."

The family of David File have since requested that more action be taken to arrest those responsible for the shooting. "David was a lovely, innocent boy" reported his mother. "When he moved to New Zealand, he'd never been happier."

His brother Jason requested that one part of David's diary be made public in an attempt to decipher it. "Near the end," Jason says, "there's a line that reads "yank up as a vital obituary", which we've so far been unable to comperhend."

ENTRIES FROM ...

BLOGS WE READ

NEWS

The Two-Way

Figure 5. Image of the false story posted by LulzSec to the PBS website. Posted on

May 30th, 2011. Retrieved from <http://freze.it/5S>.



Figure 6. LulzSec Twitter post describing actions against PBS. Posted May 30th, 2011.

June, 2011 was by far the most active and prolific month for the group. The group's activities and hackings which occurred during the month launched them to new levels of infamy and brought a change in course to attacking websites of governments and law enforcement agencies while still continuing to attack corporations. On June 2nd, LulzSec hacked into a website operated by Sony Pictures (www.SonyPictures.com) and claimed to gain details and information to over one million user accounts. Information included "passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts" (LulzSec, 2011). Information obtained was released as the group's second The Pirate Bay release; titled as *Sownage* (see Appendix H). Websites for Sony BMG Belgium and Sony BMG Netherlands were also compromised and had account databases released. LulzSec claimed they achieved entry into Sony's website using a relatively simple method, SQL injection, and lauded the public for

allowing Sony to store personal details sans accountable and proper methods for securing such sensitive data.

The following day, June 3rd, 2011, as part of a campaign known as *Fuck FBI Friday*, LulzSec released information for nearly 180 user accounts associated with Infragard's Atlanta chapter. Infragard is a private non-profit organization affiliated with FBI, facilitating as a link between the FBI and the private sector for sharing and analyzing intelligence pertaining to matters of national security (Infragard, 2012). On June 5th the release was posted to The Pirate Bay as *Fuck FBI Friday*, *ç* (*FFF*) (see Appendix I).



Figure 7. LulzSec Twitter post describing actions against the FBI. Posted June 3rd, 2011.

LulzSec had apparently been holding onto account information related to the Infragard attack for weeks before it was released, as roughly three weeks prior on May 14th, LulzSec taunted that they had account information for 178 accounts for an FBI associate's website.

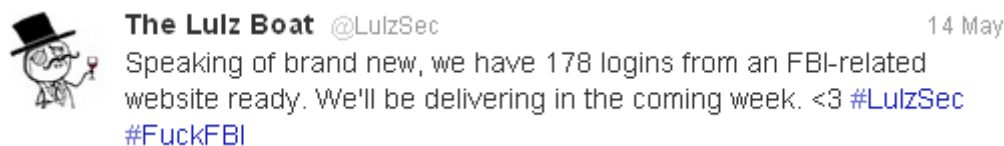


Figure 8. LulzSec Twitter post describing previous actions against the FBI.

Posted May 14th, 2011.

LulzSec claimed they were motivated by recent announcement that NATO and “Barrack Osama-Llama 24th-century Obama” were to classify “hacking as an act of war” in the press release announcing the Infragard hack (LulzSec, 2011f). Days prior, the Obama administration released a report titled *International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World* detailing how the Pentagon and NATO would consider intrusion and attacks of their computer networks to be acts of war (White House, 2011). Using information from the hacked accounts, LulzSec delved into the life and dealings of Karim Hijazi, owner of networking security and FBI/Infragard associated company Unveillance. Hijazi was accused of questionable business tactics and lauded for activities which LulzSec deemed to contradict the company’s white-hat ethical stance. LulzSec believed Hijazi “compromised his entire company and the personal lives of his colleagues, then attempted to silence us with promises of financial gain and mutual benefits” (LulzSec, 2011n). Unveillance and LulzSec publically bantered back and forth; Unveillance released a statement in response to LulzSec’s attack which was replied to by LulzSec in an additional pastebin post (see Appendix J). On the same day as the initial announcement of the Infragard hack, LulzSec also posted the server configuration for Nintendo’s website and posted to Twitter that

they were not anti-Nintendo, as the hack was “for the lulz”, as in for laughs, and was a warm up for an upcoming Fuck FBI Friday hack.



Figure 9. LulzSec Twitter post describing actions against Nintendo.

Posted June 3rd, 2011.

On June 4th, 2011, the LulzSec twitter account posted an announcement serving as the first declaration of what would become known as the Operation Anti Security movement, known by its shorthand *AntiSec*.



Figure 10. LulzSec Twitter post describing the AntiSec movement. Posted June 4th, 2011.

LulzSec, on June 6th, attacked Sony once again in two separate incidences and released source code belonging to the Sony Computer Entertainment Developer Network and data relating to the network mapping of Sony BMG. Information obtained from the hack was posted to The Pirate Bay as *Sownage 2* and contained 54 megabytes of information (see Appendix K). LulzSec stated they wished to “Hack Sony 5 Times” and taunted the company with a tally of “That’s hackers 16, Sony 0. Your move!” (LulzSec, 2011p).

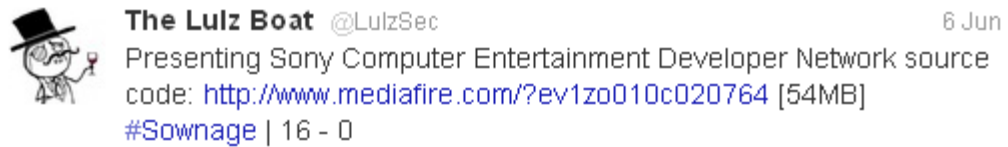


Figure 11. LulzSec Twitter post describing actions against the Sony corporation.

Posted June 6th, 2011.

On June 9th the United Kingdom’s National Health Service (NHS) was notified by LulzSec that their website was unsecure and the group had hacked into it and retrieved administrator account information. A recent drive on the Internet started by Alice Pyne, a 15 year old battling Hodgkin's lymphoma, asking people to register to a bone marrow database prompted LulzSec to notify the NHS of the vulnerability.

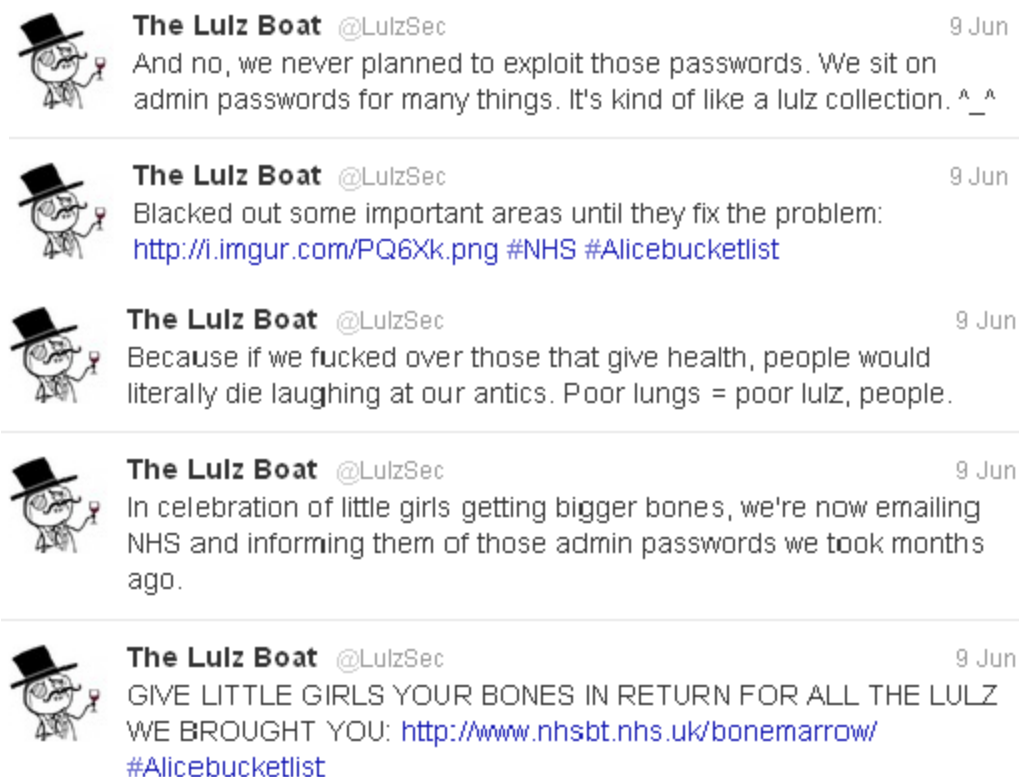


Figure 12. LulzSec Twitter post describing actions against the United Kingdom's National Health Service. Posted June 9th, 2011.

On June 10th, LulzSec took down an Islamic jihadist website, hacked into and released a database of 26,000 accounts belonging to a pornography website, and released identification for the owners of the Endgame Systems and Prolexic companies. LulzSec used their attack on the Islamic jihadist website to taunt the hacking skills of a computer hacker known as th3j35t3r, an adversary of the group who attacks and brings down Islamic Jihadist websites (see Figure 15).



Figure 13. LulzSec Twitter post describing actions against Endgame Systems and Prolexic. Posted June 10th, 2011.



Figure 14. LulzSec Twitter post describing actions of releasing user account information for various pornography websites. Posted June 10th, 2011.



Figure 15. LulzSec Twitter post describing actions against an Islamic jihadist website.

Posted June 10th, 2011.

On June 13th, LulzSec hacked into computer gamer development and publishing company Bethesda Softworks and parent company ZeniMax Media. LulzSec released the information taken from the company's servers – sans 200,000 user accounts for the online computer game Brink, as LulzSec said they were a fan of Bethesda's productions and were anticipating the release of a computer game they were working on (LulzSec, 2011d). Additionally, at the end of the press release was a surprise statement that LulzSec had hacked into the United States Senate website (www.senate.gov) and was releasing information obtained from the Senate's public facing server. A BitTorrent file containing the data released on The Pirate Bay as *Bethesda Internal Data* sans information extracted from the senate website (see Appendix L). The same press release was also posted on Pastebin which additionally included the senate.gov website information (see Appendix M).



Figure 16. LulzSec Twitter post describing the announcement for accessing the leak information for the group’s actions against the Bethesda software company and the United States Senate website. Posted June 13th, 2011.



Figure 17. LulzSec Twitter post describing actions against the Bethesda software company. Posted June 13th, 2011.

The following day, June 14th, was deemed as *Titanic Takeover Tuesday* by LulzSec. They committed a distributed denial of service (DDoS) act against and took down the servers for online computer games Eve, Minecraft, and League of Legends. Also taken down were websites belonging to videogame magazine The Escapist and the IT computer security company Finfisher. LulzSec attacked Finfisher’s website because they believe that the company sold “monitoring software to the government or some shit like that” (Bright, 2010).



Figure 18. LulzSec Twitter post describing actions for the group’s Titanic Takeover Tuesday. Posted on June 14th, 2011.

On June 16th, as was done with the Senate’s website, LulzSec attacked and brought down the CIA’s public facing website. The group also released a trove of 62,000 email accounts with user names and passwords (see Figure 20). In celebration for LulzSec’s 1000th post to Twitter, a manifesto was posted to Pastebin that addressed the group’s motivations and philosophies with a glimpse of the future to come (see Appendix N). Several statements outlining LulzSec’s beliefs of committing acts based around the concept of for the lulz were included, such as “This is the lulz lizard era, where we do things just because we find it entertaining. Watching someone’s Facebook picture turn into a penis and seeing their sister’s shocked response is priceless”, “Most of you reading this love the idea of wrecking someone else’s online experience anonymously”, and “This is the Internet, where we screw each other over for a jolt of satisfaction” (LulzSec, 2011g).



Figure 19. LulzSec Twitter post describing the takedown of the CIA's website.

Posted June 15th, 2011.



Figure 20. LulzSec Twitter post detailing information for user accounts. Posted June

16th, 2011.

Following the attack on the CIA's website, LulzSec attacked and took down a computer hacking community message board, denied they were at odds and battling with Anonymous, and rejected hacker typology classifications.



Figure 21. LulzSec Twitter post describing the group's relationship with Anonymous.

Posted June 17th, 2011.



Figure 22. LulzSec Twitter post regarding taking down a hacking forum. Posted June 17th, 2011.



Figure 23. LulzSec Twitter post describing the group's beliefs on hacker typology. Posted June 18th, 2011.

On June 19th, LulzSec officially launched Operation Anti Security in collaboration with Anonymous. Much like Anonymous, no membership requirements or initiation existed to join the AntiSec movement. Anyone who carried out hacktivist activities against targets and leaked stolen information were encouraged to do so under the banner of AntiSec. AntiSec was officially announced on Twitter and with a post on Pastebin titled *Operation Anti-Security* (see Appendix O) that stated:

Welcome to Operation Anti-Security (#AntiSec) - we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.

....

Top priority is to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments. If they try to censor our progress, we will obliterate the censor with cannonfire anointed with lizard blood (LulzSec, 2011k).

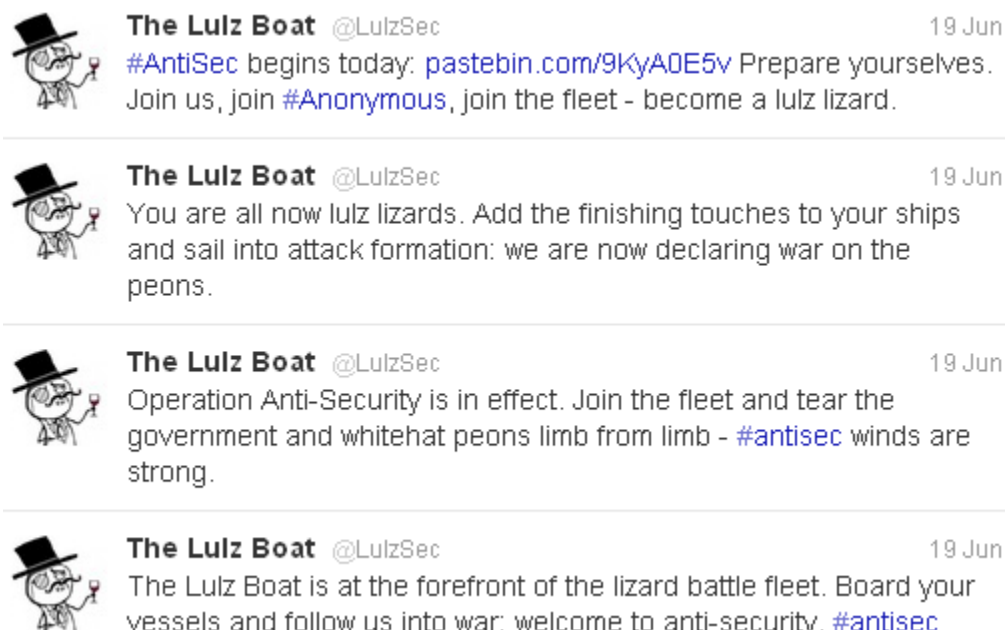


Figure 24. LulzSec Twitter post proclaiming the start of the AntiSec movement. Posted June 19th, 2011.

LulzSec also claimed on June 19th that they had once more hacked into InfraGard; this time into the Connecticut chapter. Hundreds of accounts were compromised as a result of the attack. LulzSec, in a surprising move, did not publically leak the breached account details. The Infragard Connecticut website was taken down as a precautionary measure and the FBI commented that they were aware of the hack (Satter, 2011).



Figure 25. LulzSec Twitter post describing actions against the FBI.

Posted June 19th, 2011

LulzSec’s next action and the first formally conducted under the AntiSec banner occurred on June 20th when the United Kingdom’s Serious Organized Crime Agency’s website was taken down with a DDoS attack



Figure 26. LulzSec Twitter post describing actions against the United Kingdom’s Serious Organized Crime Agency. Posted June 20th, 2011.

On June 21st, a post was made on pastebin claiming LulzSec had stolen the 2011 census data from the United Kingdom’s Office for National Statistics (see Appendix P) which contained the “records of every single citizen who gave their records to the security-illiterate UK government...” (LulzSec, 2011h). The claim was false however, as

the act was not carried out by LulzSec and involvement with it was adamantly denied on Twitter (see Figure 27).

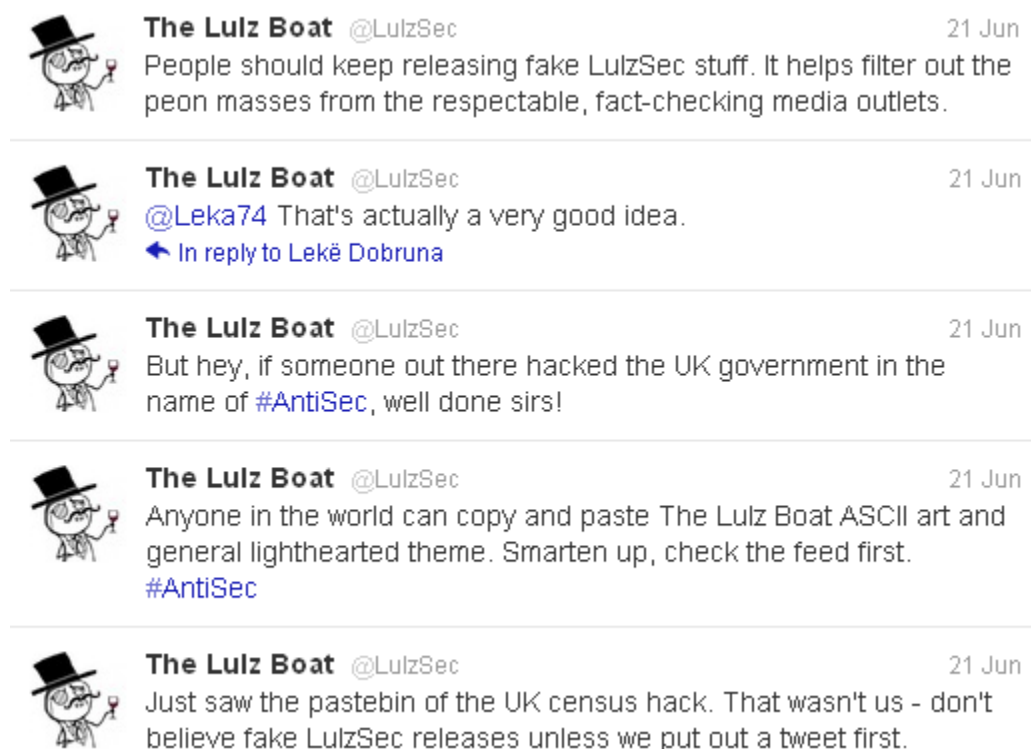


Figure 27. LulzSec Twitter post debunking a false LulzSec release.

Posted June 21st, 2011.

Additionally, on June 21st, the first arrest of an alleged LulzSec participant was made when the London Metropolitan Police arrested Ryan Cleary, 19, of Wickford, Essex. Cleary was charged under the Computer Misuse Act for participation in LulzSec's attack on the Serious Organized Crime Agency, and earlier attacks conducted during 2010 against Britain's International Federation of the Phonographic Industry and the British Phonographic Industry (Dodd & Halliday, 2011). The London Metropolitan Police issued a press release statement on their website which was later removed. In

response to the arrest, LulzSec issued a statement that Cleary was a mere associate of the group who ran their chat servers and was not an official LulzSec member (see Figure 28).



Figure 28. LulzSec Twitter post in response to Ryan Cleary's arrest.

Posted on June 21st, 2011.

In the midst of the event, LulzSec also released the purported real life identity of former member m_nerva in a press released titled Snitches getting various snitches (see Appendix Q). LulzSec did so because the group believed m_nerva "...tried to snitch on us" and that "...we just did your job for you with great ease," hoping the FBI would investigate him for his participation "in hacking the game of 'Deux Ex' and was/is involved in countless other cybercrimes (AntiSec, 2011o).

Two days later, on June, 23rd, LulzSec hacked into the computer network of the Arizona Department of Public Safety. Information retrieved from the agency's email servers was released on The Pirate Bay as *Chinga La Migra* (see Appendix R). In the accompanying press release LulzSec mentioned they were motivated to conduct the hack in protest of "SB1070 and the racial profiling anti-immigrant police state that is Arizona" (LulzSec, 2011e). Contained within release were "private intelligence bulletins, training manuals, personal email correspondence, names, phone numbers, addresses and passwords" relating to the Arizona Department of Public Safety and the agency's officers. The following day the Arizona Department of Public Safety released a press release which acknowledge the breach of security and labeled LulzSec as a "cyber-terrorist organization" (Arizona Department of Public Safety, 2012a).



Figure 29. LulzSec Twitter post describing the Chinga La Migra operation. Posted on June 23rd, 2011.

The following day, on June 24th, The Guardian posted a log of an IRC chatroom channel utilized by LulzSec from May 31st through June 4th, 2011 (Arthur & Gallagher, 2011). The logs proved to be an intrusive, yet informative insight into the group's operations, methods, motivations, and members. It is believed former member m_nerva was the leak's supplier – a claim addressed by LulzSec via a Pastebin post made just days prior (see Appendix Q).

On June 25th, in an unexpected move, LulzSec announced the end of its hacking spree on Pastebin in a post titled *50 Days of Lulz* (see Appendix S). Included in the final release were internal documents belonging to the AOL & ATT corporations. LulzSec encouraged hackers wishing to follow in its footsteps to do so under the AntiSec banner on Twitter. The release was subsequently removed from The Pirate Bay by the website's administrators as one of the files within the torrent was purportedly infected with a virus

(McAleavey, 2011). LulzSec claimed the file was already infected when taken from the AT&T server and that it was not their doing (Ernesto, 2011). The final press release from LulzSec stated:

Friends around the globe,

We are Lulz Security, and this is our final release, as today marks something meaningful to us. 50 days ago, we set sail with our humble ship on an uneasy and brutal ocean: the Internet. The hate machine, the love machine, the machine powered by many machines. We are all part of it, helping it grow, and helping it grow on us.

For the past 50 days we've been disrupting and exposing corporations, governments, often the general population itself, and quite possibly everything in between, just because we could. All to selflessly entertain others - vanity, fame, recognition, all of these things are shadowed by our desire for that which we all love. The raw, uninterrupted, chaotic thrill of entertainment and anarchy. It's what we all crave, even the seemingly lifeless politicians and emotionless, middle-aged self-titled failures. You are not failures. You have not blown away. You can get what you want and you are worth having it, believe in yourself.

....

Again, behind the mask, behind the insanity and mayhem, we truly believe in the AntiSec movement. We believe in it so strongly that we brought it back, much to the dismay of those looking for more anarchic lulz. We hope, wish, even beg, that

the movement manifests itself into a revolution that can continue on without us. The support we've gathered for it in such a short space of time is truly overwhelming, and not to mention humbling. Please don't stop. Together, united, we can stomp down our common oppressors and imbue ourselves with the power and freedom we deserve.

.....(LulzSec, 2011a).

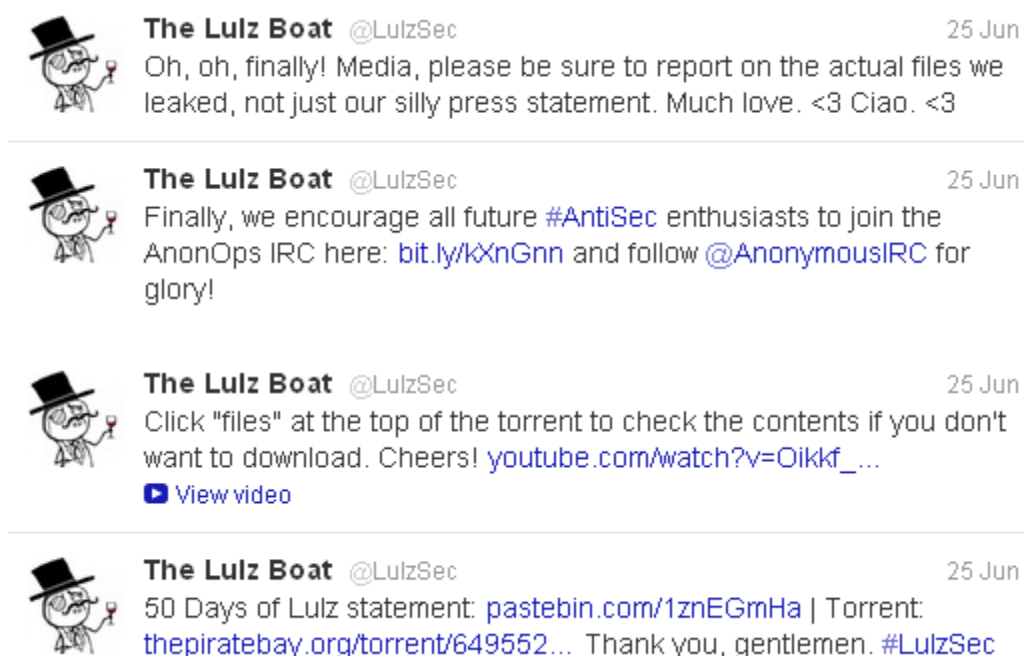


Figure 30. LulzSec Twitter post describing the 50 Days of Lulz release. Posted on June 25th, 2011.

June 28th marked the proper introduction and start of AntiSec. The movement's first official release of hacked data was posted on The Pirate Bay as *antisec01* (see Appendix T) and included information obtained from the governments of Zimbabwe and

Brazil, the Universal Music Group, and Viacom. The accompanying press release stated that AntiSec obtained and released the information because:

....Thus, the introductory #AntiSec release (dubbed AntiSec-001) does not contain the type of data that a typical Lulz Lizard can just abuse mindlessly. Instead, we provide material that is primarily against corrupt Governments (in our world this is all Governments) and corrupt companies. And keep in mind: #AntiSec vessels have a very large cache of valuable goods aboard; the crews are currently working hard to sort the loot in a way that even the lousy media sailboats are able to just grab it and sail away for the horizon. You will hear from us very soon.

.....(AntiSec, 2011e).

On June 29th AntiSec took responsibility for an additional Arizona Department of Public Safety hack known as *Chinga La Migra II* (see Appendix U). The attack was a continuation of the previous attack on the agency and was carried out for the same reasons; AntiSec hackers viewed the Arizona Department of Public Safety as an agency contributing to LulzSec's claim that legislation in Arizona was "pro-censorship" and contributed to "racial-profiling police state laws" (AntiSec, 2011g).

On July 1st, AntiSec further hacked Arizona law enforcement and hacked into the Arizona Fraternal Order of Police's website and released the data as *Chinga La Migra III* (see Appendix V). The release contained personal information for over "1,200 officer's usernames, passwords, and email addresses" and included "racist email chain emails" (AntiSec, 2011h). LulzSec published a strong and condemning message to the law enforcement community with the release:

Let this third and crushing blow against Arizona police send a strong message to the ruling class around the world. You will no longer be able to operate your campaign of terror against immigrants and working people in secrecy: we will find you, expose you, and knock you off the internet. Many lulz have been had while we purposefully strung you along slowly and painfully for the past two weeks. We know exactly what we're doing, so think twice before considering crossing us (AntiSec, 2011h).

On July 7th AntiSec released *Turkish Takedown Thursday* (see Appendix W) on The Pirate Bay. AntiSec hackers attacked the Turkish government and released information on nearly 100 government websites while hacking into and defacing 74 of them, replacing their “content with a better message” (AntiSec, 2011u). The following day, July 8th, AntiSec released the second installment of the Fuck FBI Friday campaign, titled *Fuck FBI Friday II: IRCFederal* (see Appendix X). IRC Federal was attacked because of the company’s contracts to provide technical support to the United States Army, United States Navy, the FBI, NASA, and the Department of Justice. Included in the release of the emails were “various contracts, development schematics, and internal documents for various government institutions” (AntiSec, 2011l). On July 11th, AntiSec released *Military Meltdown Monday: Mangling Booz Allen Hamilton* (see Appendix Y) on The Pirate Bay. Booz Hamilton was attacked by AntiSec for holding contracts with the United States government for projects relating to homeland security and defense. The release contained information for nearly “90,000 military email accounts”, “the complete sldump”, and “4gb of source code” (AntiSec, 2011q). Included as a secondary part of

the release were taunts and information relating to Anonymous' battle with the HBGary corporation which had attempted to uncover identities of the group's leadership structure.

On July 18th, LulzSec made a brief reprise and announced they had hacked into *The Sun*, a British tabloid newspaper published by News Corporation, a previous target of LulzSec. Over 4 gigabytes of information was retrieved. LulzSec, however, decided to not release any of the material obtained due to *The Sun's* ongoing legal issues (Ball & Arthur, 2011).



Figure 31. LulzSec Twitter post describing the attack on *The Sun* newspaper.

Posted June 18th, 2011.

On July 19th, the FBI carried out a multistate sweep of suspected Anonymous members and arrested 16 people in ten states, including California, New York, Florida

and New Jersey. Fourteen of the arrested were indicted for Anonymous' attack on PayPal, one for involvement with LulzSec's attack on Infragard, and one involvement with LulzSec's release of AT&T internal documents (Sengupta, 2011). The London Metropolitan police carried out a raid with information provided by the FBI on the same day and arrested a 16 year-old male in southern London (Harris, 2011). It was widely believed the London arrest was that of LulzSec member T-Flow; the first arrest of an official member of LulzSec. Eight days later, on the 27th, AntiSec released a memo on Pastebin titled *A message to PayPal, its customers, and our friends* (see Appendix Z) addressing the arrests, as well as condemning the activities of Internet payment company PayPal. Within the press release, LulzSec commented on the FBI's arrest of the Anonymous members and lambasted the agency for its "willingness to arrest and threaten those who are involved in ethical, modern cyber operations" (AntiSec, 2011a). LulzSec stressed the difference between committing DDoS attacks versus infected botnet attacks and believed the same punishment for the former, which they called "adding one's voice to a chorus and digital sit-in", is unjustified when compared to the later. The problem with PayPal, as they stated, was the company "continues to withhold funds from WikiLeaks, a beacon of truth in these dark times." The PayPal and WikiLeaks conflict was addressed 8 months earlier in December, 2010, with Anonymous' *Operation Avenge Assange*.

Following the FBI arrests of Anonymous members, on July 27th, 2011, the second member of LulzSec was arrested when Jake Davis of the United Kingdom's Shetland Islands, known as Topiary, was arrested by the London Metropolitan police. Davis was believed to be LulzSec's spokesperson and to have operated the group's press

operations (Ball, 2012). After Davis' arrest on the 27th, the Twitter account belonging to LulzSec became inactive. On July 29th, AntiSec released the third part of the Fuck FBI Friday campaign, titled *Fuck FBI Friday III: ManTech* (see Appendix AA). Included in the release was 400 megabytes of documentation belonging to NATO and ManTech, a firm contracted by the FBI to handle their cyber security. The release was intended to embarrass the FBI for how ManTech "are wasting the tax payer's money" and so the "public can see for themselves how their tax money is being spent" (AntiSec, 2011m).

On August 8th, AntiSec released *Shooting Sheriff's Saturday* on The Pirate Bay (see Appendix BB). The release contained "over 10 gigabytes of information" of "hundreds of private email spools, password information, address and social security numbers, credit card numbers, snitch information, training files, and more" (AntiSec, 2011s). AntiSec did so because they believed "that not only will dropping this info demonstrate the inherently corrupt nature of law enforcement using their own words, as well as result in possibly humiliation, firings, and possible charges against several officers, but that it will also disrupt and sabotage their ability to communicate and terrorize communities."

On August 10th, AntiSec posted *Corrupt Brazil (Satiagraha)* to The Pirate Bay (see Appendix CC). The release, which contained over 4.7 gigabytes of data, was proclaimed as "a cache of evidence revealing government coverup of a corruption investigation involving the CIA, the Brazilian telecom industry, and multiple US corporations" (AntiSec, 2011i).

On August, 22nd, AntiSec posted the fourth installment of the Fuck FBI Friday's campaign to The Pirate Bay as *Fuck FBI Friday IV: Vanguard Defense Industries* (see Appendix DD) which contained information retrieved from Vanguard Defense Industries:

For #FuckFBIFriday, we are releasing 1GB of private emails and documents belonging to Vanguard Defense Industries(VDI), a defense contractor that sells arms to law enforcement, military, and private corporations. The emails belong to Senior Vice President of VDI Richard T. Garcia, who has previously worked as Assistant Director to the Los Angeles FBI office as well as the Global Security Manager for Shell Oil Corporation. This leak contains internal meeting notes and contracts, schematics, non-disclosure agreements, personal information about other VDI employees, and several dozen "counter-terrorism" documents classified as "law enforcement sensitive" and "for official use only."

.....

We are doing this not only to cause embarrassment and disruption to Vanguard Defense Industries, but to send a strong message to the hacker community. White hat sellouts, law enforcement collaborators, and military contractors beware: we're coming for your mail spools, bash history files, and confidential documents (AntiSec, 2011n).

On September 2nd, AntiSec released *Texas Takedown Thursday: Chinga La Migra IV* to The Pirate Bay (see Appendix EE). AntiSec attacked and hacked into several police departments within Texas. The attack was conducted in retaliation for the arrest of 16 anonymous members and Topiary during July, 2011. Texas was targeted specifically

as AntiSec claimed “they continue to harass immigrants and use border patrol operations as a cover for their backwards racist prejudice” and because “the notoriously racist police state of Texas recently passed SB 9 and 'Secure Communities' anti-immigration laws” (AntiSec, 2011t). Three gigabytes of emails were released.

On September 22nd, the FBI arrested Cody Kretsinger of Phoenix, Arizona, believed to be LulzSec member Recursion, after a federal grand jury indicted him for conspiracy and the unauthorized impairment of a protected computer in relation to June’s *Sownage* hack. Kretsinger plead guilty on April, 5th 2012, to each charge (Geuss, 2012). The FBI said the following in a press release detailing the arrest:

From approximately May 27, 2011, through June 2, 2011, the computer systems of Sony Pictures Entertainment were compromised by a group known as ‘LulzSec,’ or ‘Lulz Security,’ whose members anonymously claimed responsibility on LulzSec’s website. Kretsinger, also known by the moniker “recursion,” is believed to be a current or former member of LulzSec. The extent of damage caused by the compromise at Sony Pictures is under investigation (United States Department of Justice, Federal Bureau of Investigation, Los Angeles Division, (2011).

On November 18th, AntiSec released *Fuck FBI Friday V: IACIS Cybercrime Investigators Owned* on The Pirate Bay as part of the Fuck FBI Friday campaign (see Appendix FF). The hacked was carried out by accessing the email account belonging to Fred Baclagan, a “Special Agent Supervisor of the CA Department of Justice in charge of computer crime investigation” (AntiSec, 2011o). Within his email they found “the IACIS.com internal email list archives (2005-2011) which detail the methods and tactics

cybercrime units use to gather electronic evidence, conduct investigations and make arrests.” AntiSec said they were “leaking over 38,000 private emails which contain detailed computer forensics techniques, investigation protocols as well as highly embarrassing personal information.” As a result of the hack, over 500 megabytes of information, including personal identification such as names, addresses, phone numbers, email addresses and password, and social security numbers was released belonging to the International Association of Chiefs of Police were released.

On the same day as *Fuck FBI Friday V*, November 18th, LulzSec additionally released *International Association of Chiefs of Police Owned on The Pirate Bay* (see Appendix GG). LulzSec hacked into the Internal Association of Chiefs of Police and released the 16,000 person membership roster which included personally identify information, hacked into the Boston Police Patrolmen’s Association website and released information belonging to 1,000 members, hacked into several websites belonging to police departments within Alabama and released information for over 1,000 of their officers, and attacked the Matrix Group, a company that creates websites for government agencies. The attacks were once again conducted in support for the arrested Anonymous members and against the Boston Police Department specifically for their clamp down and “unprovoked mass arrests and brutality” (AntiSec, 2011p) of Boston’s chapter of the Occupy Wall Street protestors.

The next major campaign initiated by AntiSec, titled *LulzXmas* (see Appendix HH and Appendix II) occurred around Christmas 2011, during which AntiSec created havoc for several online websites and organizations. Beginning with Stratfor, a private intelligence organization, AntiSec hackers gained access to their website on December

24th and obtained information on over 860,000 user's email accounts and over 75,000 credit card accounts (AntiSec, 2011c). Supporters of AntiSec were told of "Joy in the form of over \$500,00 expropriated from the bigshot clients of Stratfor" (AntiSec, 2011b) as a *LulzXmas* gift from the group. AntiSec also retrieved the internal email spools from the company. Stratfor, as noted by the hackers, had stored all their client information on their servers unencrypted. The information for these accounts was released over a period of a few days and the credit card account numbers were used fraudulently to make nearly \$700,000 in donations to non-profit groups supported by Anonymous (United States v. Hammond, 2012). In addition to information retrieved from Stratfor, the company's public front facing website was defaced¹ and embedded with a YouTube Christmas themed video titled *Anonymous' LulzXmas*². Emails retrieved from Stratfor were released by WikiLeaks beginning in February 2012 as the *Global Intelligence Files* and proved to be an embarrassing look into Stratfor's internal operations.

On December 29th as part of *LulzXmas*, AntiSec hacked into the website of SpecialForces.com, an online supplier for law enforcement and military supplies, and released information for 14,000 user accounts and 8,000 credit card account numbers for people who maintained accounts with the business (see Appendix JJ). AntiSec did mention the business encrypted their user's accounts information, unlike Stratfor, but was able to find the encryption keys and subsequently retrieve the data. Motivation for the attack was the often repeated general sentiment of disdain for law enforcement in general by Antisec:

¹ An archive/mirror of Stratfor's defaced website exists at <http://zone-h.org/mirror/id/16416728>

² The video can be accessed at <http://www.youtube.com/watch?v=BdQoSWtYpHE>

.... Continuing the week long celebration of wreaking utter havoc on global financial systems, militaries, and governments, we are announcing our next target: the online piggie supply store SpecialForces.com. Their customer base is comprised primarily of military and law enforcement affiliated individuals, who have for too long enjoyed purchasing tactical combat equipment from their slick and “professional” looking website. What’s that, officer? You get a kick out of pepper-spraying peaceful protesters in public parks? You like to recreationally taser kids? You have a fetish for putting people in plastic zip ties?

We had to contain our laughter when we saw these two "hacker proof" logos plastered on the SpecialForces.com website: "Scanned by GoDaddy.com: secured website" and "McAfee SECURE sites help keep you safe from identity theft, credit card fraud, spyware, spam, viruses, and online scams.” Despite the almighty powers of GoDaddy and McAfee's logos and some reassuring words, SpecialForces.com was just no match for our hella wicked black hat voodoo. We have just one question before we continue: You mad, officer? (AntiSec, 2011c).

Beginning with New Year’s Day in 2012, AntiSec hacked into the California State Law Enforcement Association (CSLEA) and into the New York State Association of Chiefs of Police (NYACP) and posted the leak to Pastebin as *CSLEA Hacked/Defaced or some rubbish, happy new year* (see Appendix KK) . For the CSLEA, AntiSec obtained internal email spools and a forum database and publically released the information. They also took down several websites associated and hosted by CSLEA.

Most everybody already knows that we don't like police very much. Shit, just about everybody hates them, everybody except for the rich and powerful who

depend on their protection. But which state got the most blood on their hands?

Well we already owned pigs in Texas and Arizona, and many many others; guess its time to ride on the California police.

....

So we went ahead and owned the California State Law Enforcement Association (CSLEA.COM), defacing their website and giving out live backdoors. We dumped a few of their mail spools and forum databases, and we did get a few laughs out of reading years of their private email correspondence (such as CSLEA's Legislative and Police Liason Coby Pizzotti's convos with his girlfriend who calls him "doodle"). But what we were really after was their membership rosters, which included the cleartext password to 2500 of their members, guaranteeing the ownage of many more California pigs to come (AntiSec, 2011j).

For the NYACP, information was released that revealed personal details for chiefs of police of various departments statewide as well as internal email spools. The New York City Police Department's response and handling of Occupy Wall Street was listed as motivation for the hack:

For our next owning we bring you multiple law enforcement targets in the state of New York, who has been on our crosshairs for some time due to their brutal repression of Occupy Wall Street.

.....

We're dropping the md5-hashed passwords and residential addresses for over 300 Police Chiefs in the state of New York. We are also sharing several private mail spools of a few NY police chiefs. While most of the contents of these emails

involve boring day to day office work and blonde joke chain emails, there were also treasure troves of embarrassing personal information as well as several "For Official Use Only" and "Law Enforcement Sensitive" documents discussing police methods to combat protesters (AntiSec, 2011j).

AntiSec maintained a relatively quiet profile during January. On February 3rd, AntiSec reappeared with a full day's worth of activities with *Fuck FBI Friday VI*. The website belonging to the Puckett and Faraj law firm was hacked into and defaced (see Appendix LL). AntiSec also retrieved and released to the public over 3 gigabytes of internal emails. Motivation for the attack was due to the law firm representing Staff Sgt. Frank Wuterich, a United States marine involved in the November, 2005 Haditha, Iraq massacre (AntiSec, 2012r). AntiSec additionally hacked into and defaced the Boston PD's website (see Appendix MM) and embedded the music video to the KRS-One song "Sound of Da Police" in further protest of the Boston Police Department's continued crack down of Occupy Wall Street protestors (AntiSec, 2012f). The Syracuse Police Department's website was also attacked and taken offline (Dowty, 2012). The most notable part of *Fuck FBI Friday VI* (see Appendix LL) was the interception of a FBI Conference Call to counterparts with the London Metropolitan Police that discussed recent developments for government investigations into Anonymous and LulzSec; such as the Ryan Clearly and Jack Davis court proceeding. The conversation, 18 minutes in length, was recorded by AntiSec and released on YouTube.

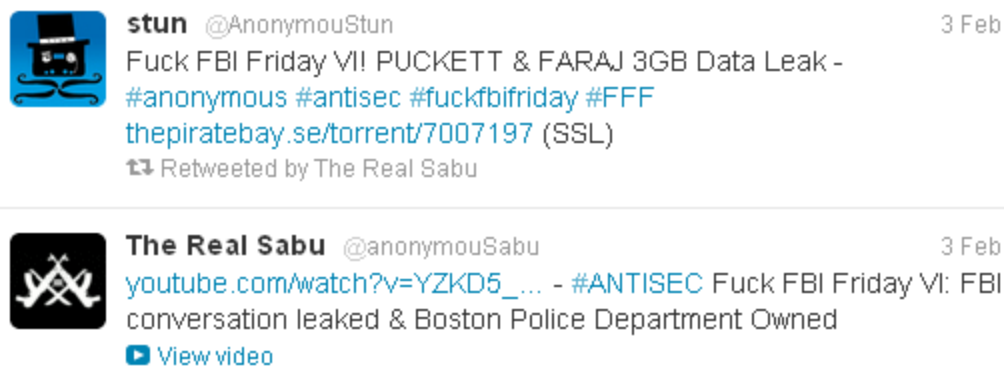


Figure 32. LulzSec’s leader Sabu and an Anonymous member Twitter posts describing the Fuck FBI Friday VI release. Retrieved from http://twitter.com/anonymouSabu_

Posted on February 3rd, 2012.

During February, AntiSec and Anonymous attacked the United States’ Federal Trade Commission (FTC) as well as international police agency Interpol. On February 17th, AntiSec hacked into the FTC’s website and posted information to Pastebin as *FTC JACKHAMMERBUTTRAEPD BY ANONYMOUS ANTISEC* (see Appendix NN). AntiSec mocked the FTC as the “Fuctarded Troglodyte Clusterfuck” and took down the websites of several and associated agencies and organizations (AntiSec, 2012k). Eleven days later, on the 28th, Anonymous initiated a DDoS attack and brought down Interpol’s website (see Figure 33).



Figure 33. Anonymous Twitter post describing the group’s action against Interpol.

Retrieved from <http://twitter.com/youranonnews>. Posted on February 28th, 2012.

On March 6th the United States Department of Justice struck the core membership of LulzSec and the AntiSec movement when a series of indictments and criminal charges were unsealed and subsequently arrested those involved. The indicted, listed by their real name and alias, were Hector Xavier Monsegur or Sabu (United States v. Monsegur, 2011); Ryan Ackroyd or Kayla, Jake Davis or Topiary, Jeremy Hammond or Anarchaos/sup_g, Darren Martyn or Pwnsauce (United States v. Ackroyd, 2012); and Donncha O'Cearrbhail or Palladium (United States v. O'Cearrbhail, 2012).

Unexpectedly, Hector Xavier Monesgur (Sabu) of New York City, leader and infamous front man of LulzSec, had been in cooperation with the United States government as an informant since shortly after the first attacks carried out by the group upon his arrest on June 7th, of 2011. Charged with twelve counts related to his crimes, Monsegur was arraigned on August 5th, 2011 and plead guilty on August 15th, 2011. His indictment and related court transcripts were sealed to prevent public knowledge of his arrest. Monsegur's role as an FBI information was described by United States Assistant Attorney Jim Pastore during an arraignment hearing as "since literally the day he was arrested, the defendant has been cooperating with the government proactively" (United States v. John Doe, 2011). Monsegur's continued participation with Anonymous, LulzSec, and AntiSec and the FBI's subsequent surveillance was instrumental for the investigation and arrest of the other charged persons.

Jeremy Hammond (Anarchaos/sup_g) of Chicago, was arrested for his involvement in the December, 2010 hack of Strategic Forecasting, Inc., also known as Stratfor. The March 6th unsealed complaint against him include three counts for his association with the crimes: one of Conspiracy to Commit Computer Hacking, one of

Computer Hacking, and one of Conspiracy to Commit Access Device Fraud. The document revealed the an informant known as *CW-1* (believed to be Monsegur) provided Hammond a server that was accessible by the FBI to help facilitate the Stratfor hack (United States v. Jeremy Hammond, 2011). Hammond and his associates retrieved information from 860,000 Stratfor subscribers and 60,000 credit card numbers which were used for over \$700,000 in fraudulent charges (U.S. DOJ, USAO, Southern District of New York, 2012).

Ryan Ackroyd (Kayla) and Jake Davis (Topiary) of the United Kingdom, and Darren Martyn (Pwnsauce) and Donncha O’Cearrbhail (Palladium) of Ireland, were jointly indicted for crimes associated with LulzSec’s hacking spree and were each charged with two counts (United States v. Ackroyd et al., 2012). In May, 2012, a superseding revision to March’s indictment was released and further included Hammond for involvement with AntiSec’s Arizona Department of Public Safety hacks (United States v. Ackroyd, David, Martyn, O’Cearrbhail, and Hammond, 2012). O’Cearrbhail’s charges were further complicated by a separately filed complaint amending his charges to include one count for his involvement in the interception of a FBI and London Metropolitan Police conference call (United States v. O’Cearrbhail, 2012).

Hammond pleaded not-guilty to his charges in May, 2012 (Bray, 2012). During June, 2012, a United States’ grand jury indicted Ryan Cleary for his involvement in Anonymous and LulzSec hacking activities from April to June 2011 (United States v. Cleary, 2012) and Cleary and Davis plead guilty while Ackroyd plead not guilty to separate charges filed in their native United Kingdom for hacking activities related to LulzSec (Associated Press, 2012). It was believed that Cleary would likely not face

extradition to the United States due to the United Kingdom's prosecution of similar charges (Arthur, 2012). In August, 2012, Monsegur was granted a six month reprieve from sentencing in August, 2012 due to his continued cooperation with the FBI (Singel, 2012) and Raynaldo Rivera of Tempe, Arizona, known as LulzSec hacker Neuron, was arrested on charges relating to the group's Sony hackings of May and June, 2011 (U.S. DOJ, F.B.I., Los Angeles Division, 2012). Rivera pleaded guilty to the charges in October, 2012 (United v. Rivera, 2012).

CHAPTER IV

PROBLEM AND RESEARCH QUESTIONS

A new phenomenon is on the rise: the formation of Internet-based organizations and movements that obtain confidential and classified data and subsequently release the information to the general public. It is important to understand these groups' motivations in order to avoid their classification into erroneous categories. To classify hacktivism as cyber-terrorism is problematic, as the two are motivated for entirely different reasons and intend for their activities to have entirely different consequences. If the recent rise in hacktivism and leaking organizations indicate a trend, then the United States government will be required to address issues of confidential and classified data release and dissemination in an effective and appropriate manner for years to come. As a result, it is necessary to understand these groups' motivations and proper typology.

This study pertains specifically to Anonymous, LulzSec, and the AntiSec movement. A research study could be conducted on any of these groups individually. A decision to analyze the three together was made based on how interconnected these groups have become. Anonymous and LulzSec are separate entities but have ties to each other with previous and crossover memberships and mutual support and solidarity. The de-facto leader of LulzSec, Sabu, posted as AnonymouSabu on Twitter (<http://twitter.com/anonymouSabu/>) until his March, 2012 arrest. LulzSec helped to start

the AntiSec movement which Anonymous has regularly contributed to with their involvement in the Fuck FBI Fridays campaign.

Additionally, all groups have supported or contributed to the WikiLeaks organization whose main agenda is to disseminate confidential government data. During December 2010, WikiLeaks had their means of financial support, Internet based donations, revoked by Amazon, MasterCard, Visa, and PayPal. In response, Anonymous launched *Operation Payback* (also known as Operation Avenge Assange) shortly after. A year later, in December 2011, Jeremy Hammond of Anonymous and the AntiSec movement hacked into Stratfor, a private global intelligence gathering and analysis company. Information retrieved by the Anonymous hack, in the form of five million emails, was released by WikiLeaks starting in February, 2012 as the *Global Intelligence Files*. LulzSec's defacement of the PBS website was motivated by their condemnation of a documentary the company had aired profiling the founder of WikiLeaks. In summary, the acts in which these groups engage their targets, their methods, and their associations vary, but ultimately they execute the same action and possess the same goal– the dissemination of confidential and classified information.

Anonymous, LulzSec, and AntiSec explain the motivation engaging in their activities in their own words via press releases which are published with their data releases. Statements contained within these press releases can be analyzed to determine a more accurate analysis of motivation for these groups' actions as opposed to simply observing the outcomes of the releases. These documents will serve as the data to be researched.

United States federal and state government agencies have published reports or made statements relating to the rationale, motivation, and ideology of these organizations. These reports and studies have discussed the repercussions relating to the releases and have report on the results of these groups' action. A lack of scientific research exists for analysis conducted on the statements made by the groups; no in-depth analysis of the content of press releases and statements released and made by them has been conducted. This can partly be attributed to the fact it was not until 2011 that Anonymous had a break out year as far as serious politically motivated hacktivist activities and LulzSec and AntiSec formed and began operations.

This thesis will answer the following research goals pertaining to these groups: first, determine motivation the hacktivist operations of Anonymous, LulzSec, and AntiSec during the period from March 2011 to March 2012 which engaged in seemingly anti-government and law enforcement behavior that released classified and confidential data; and second, determine whether these groups are accurately described and profiled by United States federal and state government agencies. Outcomes developed by this research will contribute to the knowledge base for studies relating to government and hacktivism that will become more relevant as governments become more reliant on computer and the Internet with each passing day.

CHAPTER V

METHODOLOGY

The methodology for this study follows a mixed-method approach developed by Srnka and Koeszegi (2007) that takes into account both qualitative and quantitative data. Mixed-method designs make use of the respective strengths of both qualitative and quantitative data, and by using the two, it is possible for researchers to discover results that may have not surfaced had only one method been considered. Due to the lack of application surrounding mixed-methods designs, Srnka and Koeszegi (2007) have developed a blueprint for researchers seeking to utilize mixed-method designs in research.

Two separate types of mixed-method designs exist with each type further divided into two subtypes. First, two-study research is an analysis conducted of combined data collected from separate qualitative and quantitative studies. Sequential design, a subtype, is used when research begins with a qualitative data set to develop a theory which is further explored in a companion study utilizing quantitative data. The second subtype, concurrent design, combines the results of separate non-related concurrent studies utilizing either qualitative or quantitative data (Srnka & Koeszegi, 2007).

The second type of mixed methods design, integrated design, utilizes both qualitative and quantitative data simultaneously within the analysis phase of a singular study. Necessary to conduct integrated design research is a method to transform

qualitative data into quantitative and vice-versa within the same study so that the data may be synthesized for further analysis. Two distinct subtypes of integrated design research exist – elaboration and generalization – with each performing data transformation in a separate order. In the elaboration design subtype, quantitative data becomes qualitative and the addressed research questions are examined from a different perspective which may allow for new theories to be developed. In generalization designs, qualitative data is transformed into quantitative data to further explain new theories as well as create a data set of generalizable results which can be further analyzed quantitatively. Precise documentation of the process and methods involved in conducting the research is required so future researchers can replicate the process used to transform the qualitative data into quantitative as well as the derived theoretical and quantitative (Srnska & Koeszegi, 2007).

The research design developed by Srnska and Koeszegi (2007) is based on the generalization integrated mixed-method design. Developed as a five stage guide, the blueprint is designed with the generalized results as the product with several measures for maintaining scientific validity and reliability of the project's analysis. The methodology for this study thesis follows the model outlined by Srnska and Koeszegi (2007) with slight modifications tailored for the specifics of this research. The following subtitles for each stage are shown exactly as they appear in the blueprint article (Srnska & Koeszegi, 2007). The explanation and example for each stage were combined and summarized in order to create the following stage descriptions.

Stages 1 & 2: Data Sourcing and Transcription – Creating the Basis for Qualitative Analysis

In Stage One, the researcher collects the data necessary to conduct the study. In Stage Two, if needed, the data are to be recorded in written form so that it may later be coded (i.e. transcribing audio interviews into text or translating recorded data from one language to another). These stages pose minimal work for the researcher if the data already exists in text or written form. When the data have been obtained and processed it must be checked for overall consistency. Qualitative material to be used by the following stages will exist at the end of Stage One and Two.

Stage 3: Unitization – Choosing the Unit of Analysis and Dividing the Material into Coding Units

Stage Three divides the qualitative data from Stage One and Two into manageable units that will subsequently be analyzed. The method and unitization form of the data is dependent on the type collected and used for the research. Short-form data, such as brief statements or sentences, can be broken up directly into the individual units. Data existing in longer form requires analysis to determine the best method of unitization, such as broken up by sentence, groups of sentences, or some other units that best represents the data. Srnka and Koeszegi (2007) propose that the best method for data unitization is to categorize the data into *thought units* which convey a singular idea. Thought units may exist as a complete sentence, a verb-object sequence, a single word, a symbol or a sign, punctuation marks, or a similar signifier that represents the data (p. 36).

Two coders should independently perform the unitization process. Outcomes derived from the unitization phase must be subjected to two cross-checks for inter-coder

reliability: one to compare number of units identified and one to compare the textual consistency of the units. The check for number of units identified is conducted by utilizing the Guetzkow's U calculation to assess the amount of disagreement between coders (p. 42). The formula is represented as: $U = (O1-O2) / (O1 + O2)$. The U which represents the reliability of the unitizing process between the two coders is determined by subtracting the amount of units identified by coder one ($O1$) with the amount identified by coder two ($O2$) and then dividing by the total amount (sum) of the two (Guetzkow, 1950). High conformance (100%) between the coders for the total amount of units identified is represented by the roman numeral 0.

The textual consistency check is conducted to compare the textual conformance of the content for the units identified by the two coders (Srnska & Koeszegi, p. 42. 2007). Srnska and Koeszegi's (2007) blueprint article lacks the exact method utilized for this check and the following method is based upon correspondence with Dr. K.J. Srnska, co-author of the article. Individual thought units, as determined by coder one ($O1$) and coder two ($O2$), are exported into Microsoft Excel and placed within their own cells, in a descending order by row, into column A for $O1$ and column B for $O2$. Microsoft Excel's =IF function is then used to compare the values of the cells within a row belonging to coder one in column A and coder two in column B. Equal value (the same unit chosen) is indicated by the roman numeral 1 and a false value (different unit chosen) is indicated by the roman numeral 0. The formula is calculated and results are displayed in column C. The amount of agreement is totaled and divided by the total number of units to create a percentage of agreement; a high agreement percentage indicates the coders were

relatively consistent during the coding process. The Excel formula is represented as =IF(A1=B1,1,0) (K.J. Srnka, personal communication, June 14, 2012).

After conducting the inter-coder reliability consistency check, the researcher must scrutinize the findings and determine if a second round of unitization will increase the percentage of agreement between coders. If another cycle is required the coders should work together to further refine how individual units are chosen. Codeable units, which are used in Stage Five, are produced by the completion of Stage Three's unitization process (p. 59).

For this research coder one will unitize all data and by doing so will create a master list to be used by both coders during Stages Four and Five. A master list of units will ensure the consistency and reliability of data to be further analyzed as it is imperative for the validity of the research for each coder to unitize same unitized master list. Separate lists of thought units as unitized by coder one and two would causes serious errors for validity during the subsequent categorization phase. Coder two will unitize a random sample of 25% of the data unitized by coder one; these are the data which will be subjected to the above inter-coder reliability checks.

Stage 4: Categorization – Developing a Scheme of Categories Relevant to the Research Problem

Categories must be created in order for the ideas and themes unitized within the data to be grouped together to address the research's purpose. Srnka and Koeszegi have several suggestions for category creations. First, all of the unitized data should be utilized for categorization development in order to have an encompassing view/analysis of the researched phenomenon and to avoid selection bias of data which may be skipped. For

cases in which an extraordinary or large amount of data exists, the researcher should create a balanced random sub-sample of the data and document the method employed to do so. Second, a deductive-inductive procedure should be used to identify categories. Deductive categories are those derived from the existing knowledge base and literature and inductive categories are those derived from the specific data and research phenomena at hand. Third, categories should be detailed, precise, and distinct enough to promote high reliability of valid coding, but not to the point in which the complexity of coding may causes issues for inter-coder reliability. Fourth, hierarchical category schemes or main categories encompassing subcategories may be developed. Hierarchical schemes allow for the relationship between categories to be represented and a higher reliability of data coding due to the precision of the distinct main and subcategories (p. 37).

Once coding categories are developed, an initial phase of application (applying codes to the units) should be conducted by the coders. The initial coding application will allow for the researcher to become aware of any systematic inconsistencies in regards to the types of categories devised when applying the categories to the units. Problematic categories should be further refined once identified, such as developing them into new categories, modifying the idea they represent, or removing them altogether. All though units must be able to be assigned to a category. Once categories are revised, the application phase should be conducted once again to further identify any problematic categories which may have developed as a result of the initial refinement. This stage should be repeated until the researcher feels comfortable the categories have evolved into a coding hierarchy that accurately assesses all of the data (p. 43).

Coding must then be compared for inter-coder consistency. Srnka and Koeszegi suggest two checks; calculating Cohen's Kappa for intercoder reliability, and devising a matrix to determine intercoder-consistency of assigned categories to units as well as the difference in assigned categories to units between the varying categories (p. 44).

Stage 5: Coding – Assigning Category Codes to Text Units

In the coding stage, the categories created in Stage Four are applied to the units created in Stage Three. Categories should have definitions and anchor-examples developed in order for the reliability of coding within the entire set of data to remain constant. Stage Five differs from Stage Four's initial coding application in that all categories are now created and refined in order for all thought units to be placed into one.

CHAPTER VI

ANALYSIS

Stage 1 & 2: Data Sourcing and Transcription

LulzSec, AntiSec, and Anonymous often release their retrieved data on the Internet as BitTorrent files. BitTorrent is type of computer file format and distribution method that allows for a large amount of information to be split up into numerous pieces of data known as *packets*. The packets can then be downloaded simultaneously from different users worldwide who are connected to the Internet with the same BitTorrent file active. The Pirate Bay (<http://thepiratebay.org>), a BitTorrent file indexing websites, serves as the main distribution source for these groups operations which release data. LulzSec (<http://thepiratebay.org/user/lulzsec>) and AntiSec (<http://thepiratebay.org/user/antisecurity>) both maintained accounts on the website. The Pirate Bay was the 72nd most trafficked website for both overall in the world and as well as for Internet traffic within the United States³ as of June 4th, 2012.

In addition to using BitTorrent files these groups often use Pastebin (<http://www.pastebin.com>), a website which allows users to upload text documents anonymously to the Internet. Documents hosted on Pastebin are viewable and accessible by anyone. Several statements and press releases produced by an innumerable amount of hacker and hacktivists groups are hosted on the website. Statements by Anonymous,

³ Web traffic statistics for The Pirate Bay can be accessed at <http://www.alexa.com/siteinfo/thepiratebay.se>

LulzSec, and AntiSec hosted on Pastebin are often posted as responses to the media and other hacker groups and/or as non-official or smaller scale releases.

Two methods to obtain the press releases hosted on The Pirate Bay and ready them for analysis were possible. The first method involved downloading the actual BitTorrent files off of The Pirate Bay. A BitTorrent software client on the receiving-end user's computer can identify and separate individual files enclosed within the BitTorrent file. In order to avoid the repercussions of participating in the possession and dissemination of the classified or hacked data within the rest of the BitTorrent files the press releases contained within the BitTorrent files could be singled out and downloaded. All other files within the BitTorrent files would not have been downloaded.

A decision was made to avoid obtaining the press releases in this manner after careful consideration for obtaining the press releases using the other possible method. For all releases hosted on The Pirate Bay the press release can be viewed directly from the website's page that displays information relating to the BitTorrent file. The user who uploads the file to The Pirate Bay has the option to write a description available for viewing by anyone accessing the page in order to download the file. Descriptions for BitTorrent files uploaded to The Pirate Bay by these groups use the same text as the press release file located within the BitTorrent file, and the majority of these BitTorrent file descriptions already have sensitive information redacted for the version of the press release presented on the website. Obtaining the press releases this way avoided compromising any integrity that would be lost by modifying them from the way they existed within the BitTorrent files.

The text of each press release hosted on The Pirate Bay was copied into a text editor, formatted to maintain the same formatting as published on The Pirate Bay, and then saved as a .txt file. This method allowed for skipping the download of a release's packaged BitTorrent file and then specifically downloading only the press release, only to further modify the press release for sensitive data. Documents hosted on Pastebin were downloaded as a .txt file via an option included on the website and renamed to correspond with the document's title. These documents were then modified to remove personally identifying sensitive information such as names, addresses, telephone numbers, email addresses, emails, as well as sensitive information relating to the computer networks of these groups' targets. For cases in which it was found, the information was redacted and replaced with *[Sensitive/Personal Information Redacted]*. The documents formatting and redaction of sensitive data were the only modifications done to the documents during Stage One and are the versions located in the Appendix section of this thesis.

The press releases follow the same format; text-based artwork (ASCII) at the top which identifies the group and associated imagery, a code-name for the specific release or operation, followed by information identifying data contained within the release and statements describing actions (such as hacking into a computer system and retrieving emails and documents), motivation (such as responding to a government or government agency), intended consequences and repercussions, future warnings and threats, and bragging rights.

The entirety of the obtained press releases referenced in the History section of this thesis were thoroughly examined in order to determine which ones were suitable for analysis. All major operations conducted by these groups (those published to The Pirate Bay) were included. Selected other related hacktivist and hacker related activities posted to Pastebin serving as correspondence for non-official operations were included for analysis and were addressed on a case by case basis. Documented here after is the initial list of press releases and the step by step scrutiny process that determined the final list.

A total of forty documents were obtained from Anonymous, AntiSec, and LulzSec: 19 press releases from The Pirate Bay (6 from the LulzSec and 13 from the AntiSec accounts), 19 documents from Pastebin, and 2 additional press releases saved from website defacements. These documents are titled by either the name of the release as uploaded to The Pirate Bay or name of the document as uploaded to Pastebin. Listed additionally is the date the document was posted to the Internet, the URL from which it was accessed, and in some cases a further explanation of the document's history or method of acquisition. All press releases are listed in chronological order with the exception of the first. An example precedes the list in order to explain the provided information.

- #. Release/Document Title
 - a. URL retrieved from
 - b. Date
 - c. Additional information (if needed).
- 1. X Factor Leaked Contestants Database
 - a. http://thepiratebay.se/torrent/6372763/X_Factor_Leaked_Contestants_Database
 - b. 05/07/2011
- 2. Untitled [Fox Hack]

- a. <http://pastebin.com/DsafwNZz>
 - b. 05/11/2011
3. [LulzSec] Fox.com leakage phase 0/1/2/3
 - a. <http://pastebin.com/Q2xTKU2s>
 - b. 05/13/2011
4. [ATM leak] ~LulzSec
 - a. <http://pastebin.com/myPTr0aE>
 - b. 05/15/2011
5. LulzSec hates Sony too
 - a. <http://pastebin.com/NyEFLbyX>
 - b. 05/23/2011
6. LulzSec Hack PBS.ORG
 - a. <http://pastebin.com/B3gmw5NS>
 - b. 05/30/2011
7. Re: "LulzSec Exposed"
 - a. <http://pastebin.com/yut4P6qN>
 - b. 06/06/2011
8. Sownage
 - a. <http://thepiratebay.se/torrent/6443601/Sownage>
 - a. 06/02/2011
9. Fuck FBI Fridayâ,,ç (FFF)
 - a. [http://thepiratebay.se/torrent/6446763/Fuck_FBI_FridayA_a__A__\(FFF\)](http://thepiratebay.se/torrent/6446763/Fuck_FBI_FridayA_a__A__(FFF))
 - b. 06/05/2011
10. RE: Unveillance
 - a. <http://pastebin.com/AjVd0L9E>
 - b. 06/04/2011
11. Sownage 2
 - a. http://thepiratebay.se/torrent/6449737/Sownage_2
 - b. 06/06/2011
12. Bethesda Internal Data
 - a. http://thepiratebay.se/torrent/6467131/Bethesda_internal_data
 - b. 06/13/2011
13. LulzSec versus Bethesda & Senate.gov
 - a. <http://pastebin.com/i5M0LB58>
 - b. 06/13/2011
14. LulzSec - 1000th tweet statement
 - a. <http://pastebin.com/HZtH523f>
 - b. 06/17/2011
15. Operation Anti-Security
 - a. <http://pastebin.com/9KyA0E5v>
 - b. 06/19/2011
16. LulzSec 2011 census released
 - a. <http://pastebin.com/K1nerhk0>
 - b. 06/20/2011

17. Snitches getting various stitches
 - a. <http://pastebin.com/MBEsm5XQ>
 - b. 06/21/2011
18. Chinga La Migra
 - a. http://thepiratebay.se/torrent/6490796/Chinga_La_Migra
 - b. 06/24/2011
19. 50 Days of Lulz
 - a. <http://pastebin.com/1znEGmHa>
 - b. 06/25/2011
 - c. 50 Days of Lulz was initially posted to The Pirate Bay as a BitTorrent file which included this press release. It was later removed by The Pirate Bay moderators as it reportedly contained a virus. The press release was also posted to Pastebin which is the version used here.
20. Antisec01
 - a. <http://thepiratebay.se/torrent/6502765>
 - b. 6/29/2011
21. Chinga La Migra II
 - a. http://thepiratebay.se/torrent/6504060/Chinga_La_Migra_II
 - b. 6/29/2011
22. Chinga La Migra III
 - a. http://thepiratebay.se/torrent/6508513/Chinga_La_Migra_III
 - b. 7/01/2011
23. Turkish Takedown Thursday
 - a. http://thepiratebay.se/torrent/6521231/Turkish_Takedown_Thursday
 - b. 7/04/2011
24. Fuck FBI Friday II: IRC Federal
 - a. http://thepiratebay.se/torrent/6525567/Fuck_FBI_Friday_II__IRCFederal
 - b. 7/08/ 2011
25. Military Meltdown Monday: Mangling Booz Allen Hamilton
 - a. <http://thepiratebay.se/torrent/6533009>
 - b. 7/11/2011
26. A message to PayPal, its customers, and our friends.txt
 - a. <http://pastebin.com/LAykd1es>
 - b. 07/27/2011
27. Fuck FBI Friday III: ManTech Mayhem
 - a. http://thepiratebay.se/torrent/6571301/Fuck_FBI_Friday_III__ManTech
 - b. 7/29/2011
28. Shooting Sheriffs Saturday
 - a. http://thepiratebay.se/torrent/6587214/Shooting_Sheriffs_Saturday
 - b. 8/06/2011
29. Corrupt Brazil (Satiagraha)
 - a. [http://thepiratebay.se/torrent/6593891/Corrupt_Brazil_\(Satiagraha\)](http://thepiratebay.se/torrent/6593891/Corrupt_Brazil_(Satiagraha))
 - b. 8/10/2011

- c. This press release also contained a Portuguese translation which was skipped over for analysis.
- 30. Fuck FBI Friday IV – Vanguard Defense Industries
 - a. http://thepiratebay.se/torrent/6615674/Fuck_FBI_Friday_IV__Vanguard_Defense_Industries
 - b. 8/19/2011
- 31. Texas Takedown Thursday: Chinga La Migra IV
 - a. http://thepiratebay.se/torrent/6647306/Texas_Takedown_Thursday__Chinga_La_Migra_IV
 - b. 9/02/2011
- 32. Fuck FBI Friday V: IACS Cybercrime Investigators Owned
 - a. http://thepiratebay.se/torrent/6827936/Fuck_FBI_Friday_V__IACIS_Cybercrime_Investigators_Owned
 - b. 11/18/2011
- 33. International Association of Chiefs of Police Owned
 - a. http://thepiratebay.se/torrent/6828076/International_Association_of_Chiefs_of_Police_Owned
 - b. 11/18/2011
- 34. AntiSec teaser 12/26
 - a. <http://pastebin.com/q5kXd7Fd>
 - b. 12/26/2011
- 35. AntiSec teaser 12/29 (legit)
 - a. <http://pastebin.com/f7jYf5Wd>
 - b. 12/29/2011
- 36. AntiSec teaser 12/29
 - a. <http://pastebin.com/QSX0XYiD>
 - b. 12/29/2011
- 37. CSLEA Hacked/Defaced or some rubbish, happy new year.
 - a. <http://pastebin.com/gZ9pm207>
 - b. 12/31/2011
- 38. Puckett & Faraj Lawfirm – Hadidtha
 - a. <http://zone-h.org/mirror/id/16859533>
 - b. 02/03/2012
 - c. The Puckett & Faraj law firm was hacked into and defaced by Anonymous and AntiSec hackers. The contents of the defacement serve as a press release similar to other AntiSec press releases. The link provided is an archive for how the website looked on February 2rd, 2012. A portion of this press release was used as the contents for #39 and was deleted in order to avoid having the same information analyzed twice.
- 39. Boston Police Department Defacement
 - a. <http://zone-h.org/mirror/id/16859089>
 - b. 02/03/2012
 - c. Just as with the Puckett & Faraj lawfirm, the Boston Police Department’s website was hacked into and defaced. The contents of the defacement serve as

a press release similar to other AntiSec press releases. The link provided is an archive for how the website looked on February 2rd, 2012. The entirety of this press release was also included within #38.

40. FTC JACKHAMMERBUTTRAEPD BY ANONYMOUS ANTISEC

- a. <http://pastebin.com/2qfEqS1p>
- b. 2/17/2012

The following press releases were removed for analysis with explanations provided for the reason why the particular document was deemed insufficient. These documents were either too short and/or lacked enough content to be useful for analysis to contribute to this research, or served as replies to claims by other hackers and/or adversaries and did not explain hacktivist related activities. All releases posted to The Pirate Bay were included as these releases are considered to be official.

2. Untitled [Fox Hack]
 - a. This document is not useful due to brevity and/or lack of statements.
3. [LulzSec] Fox.com leakage phase 0/1/2/3
 - a. This document is not useful due to brevity and/or lack of statements.
4. [ATM leak] ~LulzSec
 - a. This document is not useful due to brevity and/or lack of statements.
5. LulzSec hates Sony too
 - a. This document is not useful due to brevity and/or lack of statements.
7. Re: "LulzSec Exposed"
 - a. This document served as response to claims that the identities for LulzSec members were revealed in June, 2011, and was not related to a statement or data release of LulzSec, AntiSec, or Anonymous.
10. RE: Unveillance
 - a. This document served as a response to statements by Unveillance, a company that was part of LulzSec's attack on Infragard Atlanta, and was not related to a statement or data release of LulzSec, AntiSec, or Anonymous.
13. LulzSec versus Bethesda & Senate.gov
 - a. This document, posted to Pastebin, is a slight variation of LulzSec's Bethesda data release found on The Pirate Bay, and for all purposes is the same document.
14. LulzSec 2011 census released
 - a. This document, posted to Pastebin, was refuted by LulzSec as an imposter release.
17. Snitches getting various stitches

- a. This document was posted by LulzSec to reveal the identities of former associates and was not related to a statement or data release of LulzSec, AntiSec, or Anonymous.

The press releases left for further analysis were:

1. X Factor Leaked Contestants Database
6. LulzSec Hack PBS.ORG
8. Sownage
9. Fuck FBI Fridayâ,,ç (FFF)
11. Sownage 2
12. Bethesda Internal Data
14. LulzSec - 1000th tweet statement
15. Operation Anti-Security
18. Chinga La Migra
19. 50 Days of Lulz
20. Antisec01
21. Chinga La Migra II
22. Chinga La Migra III
23. Turkish Takedown Thursday
24. Fuck FBI Friday II: IRC Federal
25. Military Meltdown Monday: Mangling Booz Allen Hamilton
26. A message to PayPal, its customers, and our friends.txt
27. Fuck FBI Friday III: ManTech Mayhem
28. Shooting Sheriffs Saturday
29. Corrupt Brazil (Satiagraha)
30. Fuck FBI Friday IV – Vanguard Defense Industries
31. Texas Takedown Thursday: Chinga La Migra IV
32. Fuck FBI Friday V: IACS Cybercrime Investigators Owned
33. International Association of Chiefs of Police Owned
34. AntiSec teaser 12/26
35. AntiSec teaser 12/29 (legit)
36. AntiSec teaser 12/29
37. CSLEA Hacked/Defaced or some rubbish, happy new year.
38. Puckett & Faraj Lawfirm – Hadidtha
39. Boston Police Department Defacement
40. FTC JACKHAMMERBUTTRAEPD BY ANONYMOUS ANTISEC

Stage 3: Unitization

All data contained within the press releases were unitized as thought units (Srnlka & Koeszegi, p. 57, 2007) by coder one in order to create a master list to be used for the categorization phase by both coder one and two. A random subsample of 25% of the press releases was created within the SPSS computer program to be unitized by coder two for Stage Three's intercoder consistency check. The press releases taken from the list for analysis created at the end of Stage Two were entered into a column in descending order, and after running random selection calculation, were selected for inclusion as indicated by the roman numeral 1, or not selected and therefore not subjected for inclusion as indicated by the roman numeral 0. This set of press releases (# 9, 12, 14, 15, 24, 34, 36 and 40) were given to coder two to be unitized separately and then compared to coder one's unitization in order to determine inter-coder reliability of the thought units.

Unitization of the data was conducted within a basic text editor. The press releases' content was broken up into individual thought units with each identified thought unit placed into its own individual line of text. ASCII art and related text at the top of the press releases serving as introductions and data at the end such as server configurations and network maps were unitized as single thought units. These files were then imported into Microsoft Excel and each thought unit was placed into its own cell in descending order. The press releases unitized by both coders were subjected to two checks for intercoder reliability: one to determine the consistency for the number of thought units identified by the coders, and one to determine the textual consistency of these units.

Guetzkow's U , the check for intercoder consistency of thought units identified between the coders, was conducted for each individual press release as well for all press releases combined. The overall consistency of thought units identified among all press releases unitized by both coders combined equated to a U of 0.0458 (see Table 1), indicating a high level of conformance between the two coders.

The check for the textual consistency was conducted within Microsoft Excel using the IF=Then formula and is explained fully within the Methodology section of this research. Each cell was modified to remove spaces as the cell's first character and any ending punctuation in order to improve the percentage of agreement for the check. Cases in which text was unitized at differencing points within a sentence and included extraneous spaces or differing punctuation marks are included as part of the IF=Then check and will be indicated as a false agreement even though the thought units are the same with the exception of an extra space, punctuation mark, etc. The unitization results were additionally spot checked and were manually corrected as needed. As was done with the check for intercoder reliability of the amount of thought units identified, the textual consistency check was done for each individual press release and for all the press releases combined as whole. Overall, coder one and two were found to have an 81.88% agreement for textual content of the unitized press releases (see Table 1).

Table 1: Intercoder Consistency Comparisons

Press Release #	Thought Units Identified by Coder One (O1)	Thought Units Identified by Coder Two (O2)	% Of Textual Agreement	U =
9	50	48	90.00%	0.0204
12	35	30	80.00%	0.0769
14	94	90	89.36%	0.0217
15	45	42	84.44%	0.0345
24	37	36	91.67%	0.0137
34	82	69	75.61%	0.0861
36	96	85	70.53%	0.0608
40	98	90	73.47%	0.0426
Total	537	490	81.88%	0.0458

Stage 4: Categorization

The master list of all unitized press releases was then next subjected to the categorization phase. A hierarchy of categories (Table 2) to be applied to the thought units in order to describe them was created based upon the themes and concepts identified and discussed within the Literature Review chapter. After the creation of the hierarchy list, a refinement process occurred in which the list evolved several times to a state that best described the data necessary to address this research's goal. Table 3 shows an example of how the categories were applied to the thought units within Microsoft Excel using drop down lists in the next column.

Table 2: Final Category Hierarchy Scheme

Actor Motivation	Hacktivist	Motivation: Anti Government
		Motivation: Anti Police
		Motivation: Anti Corporation
		Motivation: Anti Banks
		Motivation: Anti Military
		Motivation: Anti Politics
		Motivation: Anti FBI / CIA
		Motivation: Anti Media
		Motivation: Pro Investigative Journalism
		Motivation: Electronic Civil Disobedience
	Black Hat	Motivation: Financial Gain
		Motivation: Malicious Intent
		Motivation: Mayhem
	Grey Hat	Motivation: Anti White Hat
		Motivation: Curious
	White Hat	Motivation: For the Lulz
		Motivation: Improved Internet Security
	Cyber Terrorist	Motivation: Improved Database Security
		Motivation: Kill Harm or Maim
	Expansionist	Motivation: Anti Internet Legislation
Motivation: Pro Expansionist View		
Instrumentalist	Motivation: Pro Instrumentalist View	
	Motivation: Bradley Manning	
Miscellaneous	Motivation: Anti 1%	
	Motivation: Anti Sony	
	Motivation: OWS Support	
	Motivation: OWS Support	
Committed Act	Data Stolen	Stolen: Personal Emails
		Stolen: Institutional emails
		Stolen: Personally identifiable information
		Stolen: Internal Documents
		Stolen: Credit Card Numbers
		Stolen: Computer Database
		Stolen: Bank Account Numbers
		Stolen: User Accounts and Passwords

Table 2: Final Category Hierarchy Scheme – Continued

	Hacker Act	Act: Chat Logs Posted
		Act: Website Defacement
		Act: Website Intrusion
		Act: Data Wiped
		Act: Network Take Over
		Act: Website Offline
		Act: Server Intrusion
		Act: Sever Map/Configuration
		Act: Restraint
		Other: Not Relevant to Study
Other	Other: ASCII Intro	
	Other: Press Release Title Intro	
	Other: Greeting/Farewell Statements	
	Other: URL Link	
	Other: Non Text Characters	
	Other: Twitter/IRC/BitCoin Addresses	
	Other: Database Example	
	Other: Email Example	
	Other: Server Configuration Example	
	Other: LulzSec/Anonymous/AntiSec Signature/Motto	
	Other: Quote/Lyrics/Poem	
	Other: Information on Leak Access	
Statements	Statement: LulzSec Lingo about LulzSec	
	Statement: Taunt	
	Statement: Account Security	
	Statement: Describing Stolen Data	
	Statement: Naming the act's specific target/victim	
	Statement: Describing Poor Network Security	
	Statement: Describing how hack achieved	
	Statement: Support for Target	
	Statement: Computer Security Procedure	
	Statement: Increased Support	
	Statement: Increased Enemies	
	Statement: LulzSec/AntiSec/Anonymous Support	
	Statement: Incitement to Action	

Table 3: Example of Assigning Thought Units a Category

<pre> () () () () () / . () () / () () / ()) () () () () / / () () () () () () () () () () () () () () () () () () () "We did it for the lulz" ~LulzSec </pre>	Other: ASCII Intro
Hello, good day, and how are you? Splendid!	Other: Greeting/Farewell Statements
We're LulzSec,	Other: Greeting/Farewell Statements
a small team of lulzy individuals who feel the drabness of the cyber community is a burden on what matters: fun.	Motivation: For the Lulz
Considering fun is now restricted to Friday,	Motivation: For the Lulz
where we look forward to the weekend, weekend,	Motivation: For the Lulz
we have now taken it upon ourselves to spread fun, fun, fun, throughout the entire calender year.	Motivation: For the Lulz

Stage 5: Coding

After all thought units were assigned a category by both coder one and coder two, Cohen's Kappa was calculated within SPSS to check the intercoder reliability between coder one and coder two for the categories assigned to thought units at the lowest hierarchy level; $K= 0.818$ ($p < 0.00$). The K value of .818 coincides with the highest tier of agreement ("almost perfect") between two coders according to the widely cited scale developed by Landis and Koch (1977). The intercoder consistency-matrix (Table 4) cross-tabulated the categories assigned to the thought units at the middle hierarchy level with the exception for the highest level hierarchy for the categories of other and statements. The lowest level of agreement occurred within the motivation categories of

grey hat hacker and miscellaneous. For the grey hat hacker motivation category, the finding can most likely be attributed to a certain level of ambiguity when it came to the boundaries between grey, white, and black hat hackers and a lack of mutual understanding between coder one and coder two regarding these boundaries, as well as a relatively small amount of occurrences (16 and 22). For the miscellaneous motivation category, once again there were a relatively a small amount of occurrences (10 and 12), and even though there were 8 units of agreement, the percentage was skewed by the lack of occurrences. Neither coder one or coder two assigned the motivation categories of cyber terrorist or instrumentalist to a thought unit, and as a result of the way division is included in the formula for calculating the percentage of agreement, the percentage of agreement between the coder shows zero percent even though the actual agreement between the two coders is 100%.

Table 4: Intercoder Consistency-Matrix

Coder 1/ Coder 2	Hacktivist	Black Hat	Grey Hat	White Hat	Cyber Terrorist	Expansionist	Instrumentalist	Misc.	Data Stolen	Hacker Act	Other	Statements	Total
Hacktivist	46	1	0	0	0	0	0	2	3	0	2	1	55
Black Hat	0	26	2	0	0	0	0	0	0	0	4	1	33
Grey Hat	0	5	12	0	0	0	0	0	0	0	5	0	22
White Hat	0	0	0	4	0	0	0	0	0	0	0	1	5
Cyber Terrorist	0	0	0	0	0	0	0	0	0	0	0	0	0
Expansionist	2	0	0	0	0	40	0	0	0	0	0	0	42
Instrumentalist	0	0	0	0	0	0	0	0	0	0	0	0	0
Miscellaneous	0	0	0	0	0	0	0	8	1	0	0	1	10
Data Stolen	0	0	0	0	0	0	0	0	38	1	0	1	40
Hacker Act	0	0	0	0	0	0	0	0	2	24	0	2	28
Other	3	0	2	0	0	1	0	1	0	0	100	8	115
Statements	1	0	0	1	0	0	0	1	0	4	7	173	187
Total	52	32	16	5	0	41	0	12	44	29	118	188	537
Agreement	75%	67%	46%	67%	0%	93%	0%	57%	83%	73%	75%	86%	

Analysis of Final Output

In total there were 2,136 thought units which received a category. The following tables are based upon the categories assigned only by coder one to all press releases.

Tables include groupings at various levels and categories and are individually explained.

All tables include the frequency of the category and the percentage that frequency represents of the table as a whole.

Table 5: High and Mid Level Categories Frequencies

Category	Frequency	Percent
Statements	625	29.3%
Other	440	20.6%
Motivation: Hactivist	437	20.5%
Act: Data Stolen	241	11.3%
Motivation: Black Hat	115	5.4%
Act: Hacker Act	113	5.3%
Motivation: Expansionist	67	3.1%
Motivation: Miscellaneous	50	2.3%
Motivation: Grey Hat	42	2.0%
Motivation: White Hat	6	0.3%
Motivation: Cyber Terrorist	0	0.0%
Motivation: Instrumentalist	0	0.0%
Total	2136	100.0%

Table 5 contains the frequencies for the middle level of the coding hierarchy with the exception of the high levels for the categories of Statements and Other due to these categories containing only a high and low level for category coding. The highest percentage of categories were Statements (29.3%; 625 units) followed by Other (20.6%;

440). These two categories make up a combined 49.9% of the data and combined contain 25 out of 69 low level categories. The following categories, by order of highest occurrence, are those for units describing hacktivist motivation (20.5%), hacker acts of stealing computer data (11.3%), black hat hacker motivation (5.4%), and statements describing hacking activities (5.3%), for a combined 42.5% of the data. The remaining 7.6% belongs to the categories for motivation of Expansionists, Miscellaneous motivation, Grey Hat hackers, and White Hat hackers. There were no occurrences for the motivation categories of Cyber Terrorism or Instrumentalism.

Table 6: Hacktivist Motivation Category Frequencies

Category	Frequency	Percent
Motivation: Anti Police	175	40.0%
Motivation: Anti Government	103	23.6%
Motivation: Anti Corporation	58	13.3%
Motivation: Electronic Civil Disobedience	32	7.3%
Motivation: Anti Military	24	5.5%
Motivation: Anti FBI / CIA	24	5.5%
Motivation: Anti Banks	10	2.3%
Motivation: Anti Media	6	1.4%
Motivation: Anti Politics	4	0.9%
Motivation: Pro Investigative Journalism	1	0.2%
Total	437	100%

Table 6 contains the frequencies for the Hacktivist Motivation category tier. The highest percentage of categories describing thought units was Anti Police (40%; 175),

followed by Anti Hovernment (23.6%; 103). These two categories make up a combined 63.6% of the data. The following motivation categories, by order of highest occurrence, were Anti Corporation (13.3%; 58), Electronic Civil Disobedience (7.3%; 32), Anti Military (5.5%; 24), and Anti FBI/CIA (5.5%; 24) for a combined 31.6% of the data. The remaining categories of Anti Banks, Anti media, Anti Politics, and Pro Investigative Journalism combine for the remaining 4.8%.

Table 7: Remaining Actor Motivation Categories Frequencies

Category	Frequency	Percent
Motivation: Anti White Hat	75	26.8%
Motivation: For the Lulz	40	14.3%
Motivation: Pro Expansionist View	35	12.5%
Motivation: Anti Internet Legislation	32	11.4%
Motivation: Malicious Intent	24	8.6%
Motivation: Mayhem	16	5.7%
Motivation: Bradley Manning	15	5.4%
Motivation: Anti 1%	13	4.6%
Motivation: Anti Sony	11	3.9%
Motivation: OWS Support	11	3.9%
Motivation: Improved Database Security	4	1.4%
Motivation: Curious	2	0.7%
Motivation: Improved Internet Security	2	0.7%
Motivation: Financial Gain	0	0%
Motivation: Kill Harm or Maim	0	0%
Motivation: Pro Instrumentalist View	0	0%
Total	280	100%

Table 7 contains the frequencies for the remaining actor motivation categories for Black, Grey, and White Hat Hackers; Expansionists and Instrumentalists; Cyber Terrorists, those motivated by Bradley Manning and WikiLeaks; opposition to the Sony Corporation; those who acted in support of Occupy Wall Street; and those who were specifically against the 1% as made known by Occupy Wall Street. Most notably, Cyber Terrorism and Instrumentalist motivation is nonexistent; there were zero instances of the two categories within the data. The highest percentage of categories describing thought units was Black Hat Hackers motivation against White Hat Hackers (26.8%; 75), followed by Grey Hat hackers' motivation of for the lulz (14.3%; 40), Pro Expansionism motivation (12.5%; 35), and Expansionist motivation against Internet legislation (11.4%; 32). These four categories make up a combined 65% of the data. Occupy Wall Street support and motivation against the 1% combined for a total of 8.5%. The four categories within Black Hat Hacker motivation category (Anti White Hat, Malicious Intent, Mayhem, and Financial Gain) total 41.1% of the data, the largest actor category for the table. The two Grey Hat Hacker categories of For the Lulz and Curious total 20%. The White Hat Hacker motivation categories of Improved Database Security and Improved Internet Security combine to represent 2.1%.

Figure 24 shows the frequencies for the motivation statement categories for the isolated hacker actor categories of Black Hat Hacker, Grey Hat Hacker, and White Hat Hacker. The biggest motivation factor was black hat hackers resentment for white hat hackers followed by grey hat hackers motivation of for the lulz. Black hat hacker motivation of Malicious Intent and Mayhem were the next two largest categories, and the black hat hacker motivation of for Financial Gain occurred zero times. Pro white hat

hacker beliefs of hacking to improve database and Internet security occurred, albeit a small amount.

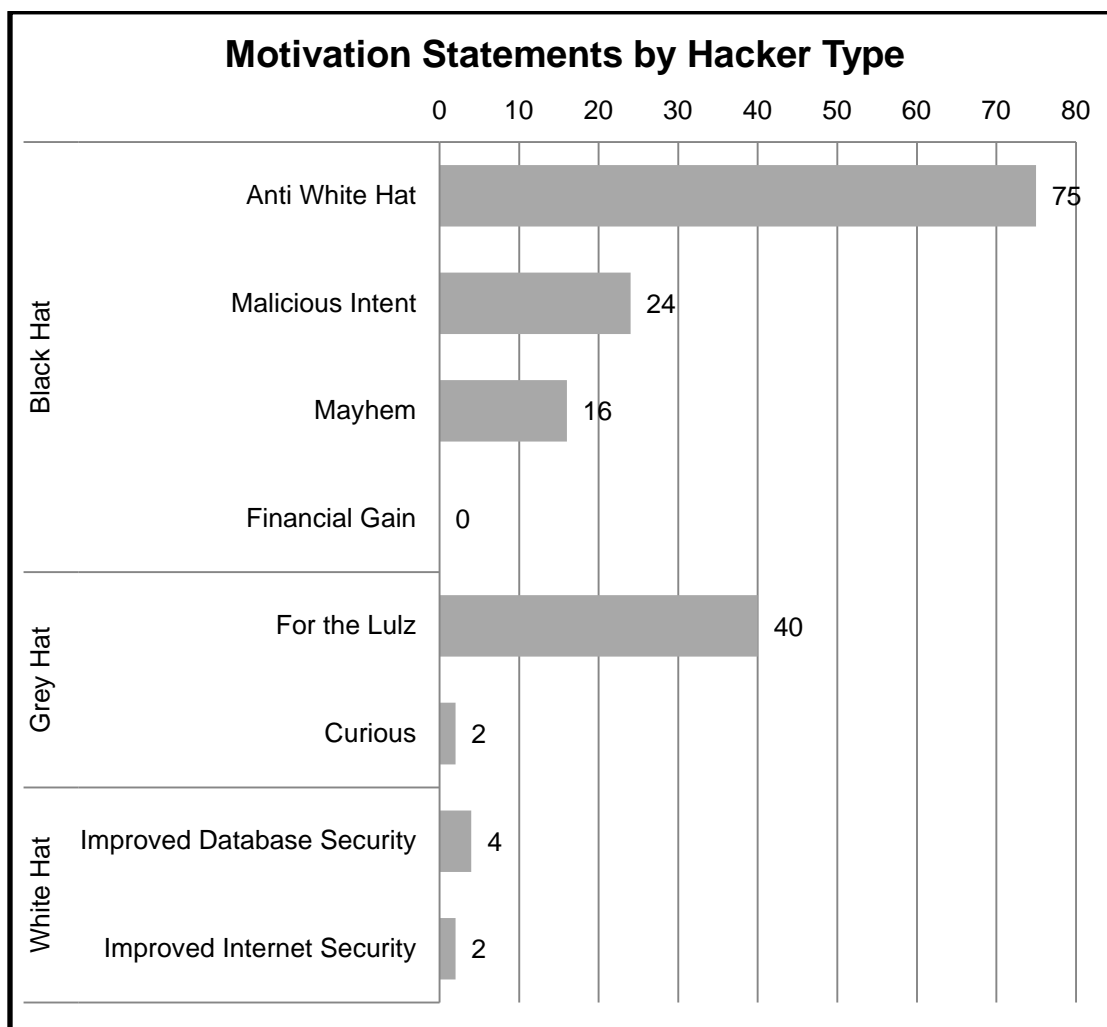


Figure 34. Graph for Motivation Categories by Hacker Type

Table 8 contains the frequencies for the type of information/data which was stolen or retrieved. Most frequently taken were institutional Internal Documents (30.3%; 73), followed by Personally Identifiable Information (27.8%; 67) and stolen User Account and Passwords (19.9; 48). These three categories make up 78% of the data. The following

types of information/data stolen, by order of highest occurrence were Personal Emails (7.1%,17); Databases (5.4%; 13); Institutional Emails (5.0%; 12); Credit Card Numbers (4.1%; 10); and a singular occurrence of stolen Bank Account Numbers (0.4%; 1), totaling the remaining 22% of the information/data stolen.

Table 8: Data Stolen Category Frequencies

Category	Frequency	Percent
Stolen: Internal Documents	73	30.3%
Stolen: Personally Identifiable Information	67	27.8%
Stolen: User Accounts and Passwords	48	19.9%
Stolen: Personal Emails	17	7.1%
Stolen: Computer Database	13	5.4%
Stolen: Institutional Emails	12	5.0%
Stolen: Credit Card Numbers	10	4.1%
Stolen: Bank Account Numbers	1	0.4%
Total	241	100%

Table 9 contains the frequencies for the types of hacker related activities and acts committed. Acts most frequently committed or mentioned by these groups were Website Defacements (26.5%; 30), Server Intrusions (23.9%; 27) and deleting/wiping data (17.7%; 20). These three categories make up 68.1% of the data. There were 9 (8%) occurrences of these groups stealing data and subsequently restraining from releasing it online due to some type of perceived solidarity with the persons associated with stolen information/data. Knocking websites offline, an often mentioned activity attributed to these groups, accounted for only 5.3% of the committed acts.

Table 9: Hacker Act Category Frequencies

Category	Frequency	Percent
Act: Website Defacement	30	26.5%
Act: Server Intrusion	27	23.9%
Act: Data Wiped	20	17.7%
Act: Sever Map/Configuration	9	8.0%
Act: Restraint	9	8.0%
Act: Website Offline	6	5.3%
Act: Network Take Over	5	4.4%
Act: Website Intrusion	4	3.5%
Act: Chat Logs Posted	3	2.7%
Total	113	100%

Table 10 contains frequencies for the type of statements made by these groups. Taunting was the overwhelming type of statement (38.9%; 243), followed by the specific naming out the group's current or previous victim (18.2%, 114) and descriptions of the information/data stolen (11.5%; 72). These three categories make up 68.6% of the hacking related activities committed by these groups. Statements inciting fellow hackers and hacktivists to action accounted for 8% of the statements. Descriptions of how targets of these groups had poor network security, account security, and computer security procedures, and descriptions for how the hacks were conducted combine to represent 9.7% of the statements.

Table 10: Statements Category Frequencies

Category	Frequency	Percent
Statement: Taunt	243	38.9%
Statement: Naming the act's specific target/victim	114	18.2%
Statement: Describing Stolen Data	72	11.5%
Statement: Incitement to Action	50	8.0%
Statement: LulzSec Lingo about LulzSec	47	7.5%
Statement: Describing Poor Network Security	32	5.1%
Statement: LulzSec/AntiSec/Anonymous Support	22	3.5%
Statement: Describing how hack achieved	14	2.2%
Statement: Increased Support	10	1.6%
Statement: Account Security	9	1.4%
Statement: Computer Security Procedure	6	1.0%
Statement: Support for Target	5	0.8%
Statement: Increased Enemies	1	0.2%
Total	625	100%

Table 11 describes information which was captured but has no particular relevance for this research's goals. Thought units which were unable to be sufficiently described by any of the categories were categorized as Not Relevant to Study and accounted for 28.6% of the Other category and 5.9% (126 of 2,136 thought units) of the research's entire data set. There were 60 occurrences relating to information for how to access the information/data published by these groups and 31 ASCII artwork introduction headers. Quotes, song lyrics, and/or poetry occurred 10 times. Examples of retrieved emails, sever configurations, or computer databases retrieved occurred 14 times.

Table 11: Other Category Frequencies

Category	Frequency	Percent
Other: Not Relevant to Study	126	28.6%
Other: Non Text Characters	63	14.3%
Other: Information on Leak Access	60	13.6%
Other: Greeting/Farewell Statements	53	12.0%
Other: ASCII Intro	31	7.0%
Other: LulzSec/Anonymous/AntiSec Signature/Motto	28	6.4%
Other: Press Release Title Intro	25	5.7%
Other: URL Link	22	5.0%
Other: Quote/Lyrics/Poem	10	2.3%
Other: Twitter/IRC/BitCoin Addresses	8	1.8%
Other: Email Example	6	1.4%
Other: Server Configuration Example	5	1.1%
Other: Database Example	3	0.7%
Total	440	100%

CHAPTER VII

DISCUSSION

Research Questions

The first research goal was to determine motivation for the hacktivist operations of Anonymous, LulzSec, and AntiSec during the period from March 2011 to March 2012 which engaged in seemingly anti-government and law enforcement behavior that released classified and confidential data. The analysis of these groups' press releases indicates they were primarily motivated by the hacktivist and black hat hacker ideology of anti police, government, white hat hacker, and corporate sentiment. These four categories, out of twenty six, combine for over 50% of all of the motivational statements made within the press releases which were analyzed. These groups were also motivated for the lulz, or that is, for the purpose of humor, entertainment, and committing their activities simply for the sake of doing so. They were also aligned with pro-expansionist views and have taken a stance and act out against Internet related legislation by engaging in hacktivist activities.

The second research goal was to determine whether these groups have been accurately described and profiled by United States federal and state agencies. The Department of Homeland Security, Department of Justice, United States Attorney's Office, and the Federal Bureau of Investigation were correct in the various labels they assigned to these groups which mostly referred to them as hacktivist and/or hacking

organizations. The FBI's statement that Anonymous was a "collective of computer hackers and other individuals located throughout the world that conduct cyber attacks, including the dissemination of confidential information stolen from victims' computers, against individuals and entities they perceive to be hostile to its interests," (U.S. DOJ, F.B.I., Los Angeles Division, 2011) and the United States District Court of Northern California grand jury indictment of an Anonymous member that referred to the group as "an online collective of individuals that was associated with collaborative hacking attacks motivated by political and social goals, often referred to as 'hacktivism'" (United States v. Collins et al., 2011) serve as examples of the United States government making accurate assessments. These hacktivist organizations can be studied, analyzed and defended against in a more effective manner when labeled accurately. The Arizona Department of Public Safety incorrectly proclaimed AntiSec and LulzSec as cyber terrorist organizations in response to the Chinga La Migra hacktivist activities against the agency. The agency's actions were a hastily made reaction out of spurn for these groups' actions with failure to fully comprehend and analyze those who had attacked them.

Expansionists and Instrumentalists

Instrumentalists are those persons and organizations who believe the Internet should exist within the confines of law. To instrumentalists, the Internet is seen as an instrument or a tool which is beneficial to people but one that it must adhere and be contained within modern society's laws and structure. Opposite to the belief of instrumentalists are the expansionists who vision the Internet differently. Expansionists believe the Internet represents a paradigm shift for the way people are involved in government and the flow and access to information. They believe capabilities provided

by the Internet are so powerful that the Internet can open up governments to the benefit of all people worldwide, and eventually governments will have to redefine and restructure due to the power which will be placed within the hands of the people. In other words, expansionists believe government will have to conform to the Internet and not the Internet being required to conform to governments as instrumentalists believe.

Expansionists see themselves as the foot soldiers in the Internet's war for the spread of information and instrumentalists see themselves as the gatekeepers for information not meant to be spread across systems. They believe governments, corporations, and other powerful institutions are actors of the instrumentalist side and seek to control the information expansionists believe may be used to empower citizens across the world.

These two groups have been engaged in a conflict for decades and hacktivist groups can be seen as the new armies of the expansionist front.

Tavani's (2005) concept of Internet ethical expansionism and traditionalism and Sterner (2011) and Hwang's (2010) related concepts of Internet expansionism and instrumentalism can be associated to the expansionist beliefs held by Anonymous, AntiSec, LulzSec, and possibly by hacktivist collectives and movements as a whole. Expansionists, both ethical as in Tavani's work and informational as in the case with hacktivist groups, believe the existing framework and social structures of government and law is incapable of handling the change in information and ethics associated with the advancement of the Internet. Instrumentalists, both informational and ethical, believe otherwise; that the existing framework is capable of dealing with same issues within the the confines of how government and law is already structured.

Hackers and Hacktivism

A comparison between the original definitions for computer hackers and the more currently accepted definitions reveals a noticeable evolution of terminology and meaning. A clear disdain for the current perception of hackers and hacking is articulated in the Jargon File's 8th definition of hacker which flat out rejects today's commonly accepted view of hackers as those who engage in malicious activities. The hacktivist and hacking activities taken by these groups are in direct contrast with the accepted hacker ethics of the original hackers and hackers operating within the 1980s as discussed by Levy (2010).

For comparison to a more recent ethical code for hackers, several tenets of Mizrach's (1997) ethical framework describing those operating during the mid 1990s were violated by Anonymous, AntiSec, and LulzSec. Acts such as stealing personally identifiable information and bank account numbers and disseminating the information on the Internet would be considered gross violations of the hacker ethics discussed by Mizrach. However, many of the acts which Mizrach believed to be against the ethical code adhered to by hackers during the mid 1990s are now common place within the hacking community. Mizrach's code of ethics may no longer accurately represent acceptable actions within the hacking culture and may be outdated.

Cyber Terrorism and Policy Implications

If governments, police forces, corporations, and other institutional forces are to keep their data secured it is important they understand the motivation behind actors seeking and attempting to retrieve it. In order to repel attacks from hacktivist organizations these institutions must be fully aware of the parties in which they are

defending themselves against. Zero occasions of cyber terrorism motivation or acts were discovered within this research. Labeling groups as cyber terrorists when they are in fact hacktivist organizations is problematic as these groups do not seek to kill, harm, or physically maim those they oppose. Opposition to the government and police does not necessarily equate to labeling these groups as those who justify the use physically violent means for accomplishing actions in support of their beliefs.

However, as there certainly are groups which are cyberterroristic in nature, Anonymous, AntiSec, and LulzSec are not. Even though only a singular instance of a government agency (Arizona Department of Public Safety) applying the cyber terrorism label incorrectly to these groups was discovered, a dangerous precedent was set if other government agencies are to follow in their footsteps. Government agencies which find themselves as the targets of suspected hacktivist related acts should carefully assess those attacking them in order to develop the most appropriate response.

Studies and literature that define cyber terrorism, such as Talihärm's (2010), as acts facilitated through the use of computers or technology with the intent to cause outcomes comparable to actual physical acts of terrorism, such as to injure or maim, and to cause fear, panic, or hysteria promote a more well defined and accurate usage of the term. Cases in which the definition of cyber terrorism includes the use of politically motivated hacks or computer actions, but without intent of physical harm and the threats most typically associated with traditional terrorism do not accurately portray cyber-terrorism and are flawed.

CHAPTER VIII

CONCLUSION

The Press releases analyzed cannot be considered as valid resources due to an unforeseen revelation which took place during the course of this study. Research for this study began during the summer of 2011 shortly after the conclusion of LulzSec's hacking spree. Several months later, in March, 2012, it was revealed that LulzSec's leader Sabu had been arrested shortly after the start of the group's hacking activities and had been acting as an FBI informant. It cannot be determined and is unknown whether the FBI influenced the activities of LulzSec as a result of the agency's relationship with Sabu, and if so, the extent in which the agency was involved. This research for this study had progressed too far by the time the arrest was announced to alter or make significant changes to the project. As a result, it must be assumed the integrity of the press releases which were gather for analysis was compromised.

The press releases also span three separate but highly intertwined entities (Anonymous, AntiSec, and LulzSec) and due to the anonymity of these groups and lack of a proclaimed authorship it is very likely they were authored by different persons with differing and varied opinions. LulzSec's press releases have been assumed to be penned by Topiary; a singular author. Anonymous and AntiSec, on the other hand, are leaderless organizations in which there is no one central figure guiding activities and beliefs. The

combination of press releases from all three groups has lead to a highly probability that the inclusion of multiple authors into this research's data occurred.

As a result of Sabu's involvement with the FBI and the combination of press releases authored by different persons this research can serve as a guide and method for how similar press releases can be analyzed for future projects studying similar groups. Future researchers should attempt to collect and verify press releases authored by the same person or same group in order to increase validity of findings. This research, as well as future studies, could have benefited from a more highly refined hierarchy of categories, especially within the categories of Other and its lower level categories.

This research set forth to explore the intertwined hacktivist organizations AntiSec, Anonymous, and LulzSec hacktivist organizations. It profiled hacker classifications, cyber terrorists, and the expansionist and instrumentalists Internet stances and summarized the profiles given to AntiSec, Anonymous, and LulzSec by United States federal and state government agencies. Two research questions were explored: one seeking to explain these groups motivation for their actions, and the other seeking to determine if these groups have been accurately portrayed and reported on. The questions were examined by transforming qualitative data existing in the form of the press releases released by the groups describing their hacking related activities into quantitative data to be analyzed. Analysis of the data found these groups to be primarily motivated by anti police, government, corporate, and white hacker sentiment and that they have been, for the most part, accurately portrayed by government agencies. Issues arose that compromised the integrity of the the press releases chosen for analysis, and as a result, the data and results of the thesis relating to Anonymous, AntiSec, and LulzSec as a whole

must be deemed invalidated. This research now serves as an example of how similar groups and other press releases published by them can be analyzed for future studies.

APPENDIX

Appendix A: X Factor Leaked Contestants Database

```
( ) ( )( )( ) ( _ )/. |( )( ) / )( )/ )
)( _ )( )( ) ( _ / / _ ( _ ))( )( \ \ ) )( ( _
( _ )( _ )( _ )( _ ) ( _ )( _ ) ( _ / ( _ ) \ )
      "We did it for the lulz" ~LulzSec
```

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 calendar 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!

Host settings:

MySQL version: (5.1.47-log) running on 10.96.57.102 (www.fox.com)

Date: 22.04.2011 15:50:02

Database: "xfactorreg"

Sample:

```
id | firstname | lastname | dob | phone | email | auditiontype |
numberofperformers | location | optin_1 | optin_2 | gender | zip |
timestamp
```

[Sensitive/Personal Information Redacted]

Appendix B: Untitled [Fox Hack]

```
#####
## OFFICIAL LULZSEC MEMO OF JUSTICE ##
#####
```

```
tl;dr http://i.imgur.com/TkI54.png
password list below
```

Dear Fox.com,

We don't like you very much. As such, we cordially invite you to kiss our hand-crafted crescent fresh asses.

Remember that time we leaked all your X-Factor contestants?
http://thepiratebay.org/torrent/6372763/X_Factor_Leaked_Contestants_Database

Well now we're leaking some more of your junk. We invite the Internet to ravage the following list of emails and passwords (from a database within Fox.com) - Facebook, MySpace, PayPal, whatever you can get your hands on. Take from them everything. Remember to proxy up, or tunnel like a pro!

Follow us on twitter; we're owning more things next week. Kisses!

All the best,

LulzSec
twitter.com/LulzSec

```
-----
-----
--raped material goes below the shiny dashes oh god they're so shiny--
-----
-----
```

[Sensitive/Personal Information Redacted]

Hello again, fellow Internet crusaders! As you know by now, we're LulzSec, a small team of GOD-FEARING NUNS. We're here to tell you that the following hacking is evil and should be frowned upon:

Phase 0 - 73,000 X-Factor contestants leakage:
http://thepiratebay.org/torrent/6372763/X_Factor_Leaked_Contestants_Database

Phase 1 - 363 Fox.com email/password combinations leakage:
<http://mirror.anapnea.net/lulzsec-fox.txt> (thank you for the mirror, anapnea.net <3 (@anapnea on twitter))

Phase 2 - Fox.com internal PHP fucktard security workings + additional login information (mostly hashed but lots of it): <http://www.mediafire.com/?4p611mqabal88xw>

Phase 3 - !! NEW !! OH MAH GAAAAWD NEW !! finishing taunt - Fox failed to provide us with candy, so we're tossing these additional 44 email/password combinations from Fox.com overboard:

[Sensitive/Personal Information Redacted]

ENJOY AND DON'T FORGET TO BRUSH YOUR TEETH BECAUSE IT'S VERY IMPORTANT
Follow us on twitter, we're owning the FBI next! @LulzSec

Lulz won't hurt anymore,
it's an open smile on a friendly shore.

Yes LULZ! Welcome aboard: it's LULZ!

```
----- The Prototype Lulz Boat -----
<kraken>      _~
<kraken>    _~ )_)_~
<kraken>    )_))_))_
<kraken>    _!_!_!_
<kraken>    \_____t/
<kraken> ~~~~~~
<BottleOfRum> that's no mighty boat
<BottleOfRum> that's a toy boat
<kraken> :o
```

```
MACHINE ID | MACHINE COMPANY OWNER | ADDRESS 1 | ADDRESS 2 | CITY |
POSTCODE | MACHINE CHARGE | MACHINE TYPE | LATITUDE | LONGITUDE
```

Appendix E: LulzSec hates Sony too

@LulzSec was here you sexy bastards!

This isn't a 1337 h4x0r, we just want to embarrass Sony some more.
Can this be hack number 8? 7 and a half?!

Stupid Sony, so very stupid:

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>

(two other databases hosted on this boxxy box, go for them if you want)

example of the tasty but not very exciting innards:
table || columns

[Sensitive/Personal Information Redacted]

MySQL root passwords: <http://pastehtml.com/view/avetoiqfz.html>
All stations and passwords: <http://pastehtml.com/view/avetuy7rz.html>
All press passwords: <http://pastehtml.com/view/aveul972n.html>
Frontline logins: <http://pastehtml.com/view/avewarfsf.html>
SQL database leaked: <http://pastehtml.com/view/avex64zdb.html>
Network map disclosure: <http://pastebin.com/pHShw0qN>
Staffers/admins: <http://pastehtml.com/view/avf0xtvun.html>

Tupac story cache: <http://freze.it/5S>
Deface cache: <http://freze.it/lulz>

Appendix G: Re: "LulzSec Exposed"

Dear Internets,

Herro! Recently some of you may have seen "LulzSec exposed" logs floating around. We'd like the time to say this: LOL. Those logs are primarily from a channel called #pure-elite, which is /not/ the LulzSec core chatting channel. #pure-elite is where we gather potential backup/subcrew research and development battle fleet members, i.e. we were using that channel only to recruit talent for side-operations.

Note that people such as joepie91/Neuron/Storm/trollpoll/voodoo are not involved with LulzSec, they just hang out with us in that channel. Also, "ev0", who was allegedly arrested (?) was never a part of LulzSec or in fact the subcrew. We don't even know who he is.

Despite the fact that we're laughing heartily right now, we do take care of our subcrew, and as such the person who leaked those logs (m_nerva) has been completely hacked inside and out. We have all his online accounts, all his personal information, all the illegal things he's done on record. We destroyed him so hard that he sat there apologizing to us all night on IRC for what he did. His mother probably spanked him after we wrecked his home connection. Uh-oh, m_nerva!

Our core chatting channel remains unaffected. Our core LulzSec team is at full strength. The Lulz Boat sails stronger than ever, nice try though.

TL;DR we are too sexy to be sunk, hacking continues as usual, u mad bros?

<http://lulzsecurity.com/>
twitter.com/LulzSec

This is an embarrassment to Sony; the SQLi link is provided in our file contents, and we invite anyone with the balls to check for themselves that what we say is true. You may even want to plunder those 3.5 million coupons while you can.

Included in our collection are databases from Sony BMG Belgium & Netherlands. These also contain varied assortments of Sony user and staffer information.

Follow our sexy asses on twitter to hear about our upcoming website. Ciao! ^_^

Naturally we were just stringing him along to further expose the corruption of whitehats. Please find enclosed Karim's full contact details and a log of him talking to us through IRC. Also, enjoy 924 of his internal company emails - we have his personal gmail too, unreleased.

We call upon journalists and other writers to delve through the emails carefully, as we have uncovered an operation orchestrated by Unveillance and others to control and assess Libyan cyberspace through malicious means: the U.S. government is funding the CSFI to attack Libya's cyber infrastructure. You will find the emails of all 23 people involved in the emails.

Unveillance was also involved in a scheme where they paid an Indian registrar \$2000 to receive 100 domains a month that may be deemed as botnet C&Cs. Shameful ploys by supposed "whitehats".

We accept your threats, NATO. Game on, losers.

Now we are all sons of bitches,

Lulz Security

How to open the lulzy emails:

- Sail over here: <http://www.mozillamessaging.com/thunderbird/>
- Get this thing that changes filetypes:
<http://www.bulkrenameutility.co.uk/Download.php>
- Grab your booty (the email files) and change their extension to ".eml" using the above tool
- copy/drag into your Thunderbird sailing vessel

Happy plundering!

Appendix J: RE: Unveillance

RE: <http://www.unveillance.com/latest-news/unveillance-official-statement/> - whitehat morons

From: <http://lulzsecurity.com/> - masters of the seven proxseas

Dear Karim & Unveillance,

Greetings morons. We're writing in response to your recent press statement, which, while blatantly trying to hide your incompetence, attempts to paint an ill-conceived picture on The Lulz Boat. To clarify, we were never going to extort anything from you. We were simply going to pressure you into a position where you could be willing to give us money for our silence, and then expose you publicly.

Ironically, despite the fact that you A) claimed that you wouldn't do something like that, and B) foolishly got outsmarted yet again, we'd like to point out something that you did do: attempt to cooperate with mystery hackers in order to radically, and illegally, boost your company from the ground.

Karim, founder of Unveillance, attempted from the start to work with us for his own gain, and he even offered us payment for certain "tasks". These tasks, hardly subtle at this point, were those of a malicious nature; destroying Karim's competitors through insider info and holes Karim would supply us.

Karim also wanted us to help track "enemy" botnets and "enemy" botnet trackers. All in return for our silence and "mutual gain".

While it's normal for him to try and cover up this embarrassment by putting all the focus back on us, we can, again, see past this primitive social engineering. Karim compromised his entire company and the personal lives of his colleagues, then attempted to silence us with promises of financial gain and mutual benefits.

We don't need cleverly-crafted media spinning to cover up anything, we say it how it is, nice and loud: Karim is a giant fuckwit that used the same password for all of his online accounts and all accounts linked to a company he owns. Then he tried to bargain with hackers so his company wouldn't crumble.

Try harder, Karim. We're too smart for your silly games.

To everyone else: stay safe, secure yourself, the Internet is a playground for people like us. We love you.

After mapping their internal network and thoroughly pillaging all of their servers, we grabbed all their source code and database passwords, which we proceeded to shift silently back to our storage deck.

Please find enclosed everything we took, excluding one thing - 200,000+ Brink users. We actually like this company and would like for them to speed up the production of Skyrim, so we'll give them one less thing to worry about. You're welcome! :D

Please keep making awesome games, guys, and you should totally add an official LulzSec top hat to new releases.

But anyway, bwahahaha... >:]

See also:

Senate.gov internal data - lulzsecurity.com/releases/senate.gov.txt

delicious. As of late, certain inferior sailing boats have discovered flaws in Brink (brinkthegame.com), thinking themselves exciting and new.

Too late. The Lulz Boat controls this ocean, chumps.

Some weeks ago, we smashed into Brink with our heavy artillery Lulz Cannons and decided to switch to ninja mode. From our LFI entry point, we acquired command execution via local file inclusion of enemy fleet Apache vessel. We then found that the HTTPD had SSH auth keys, which let our ship SSH into other servers. See where this is going?

We then switched to root ammunition rounds.
And we rooted... and rooted... and rooted...

After mapping their internal network and thoroughly pillaging all of their servers, we grabbed all their source code and database passwords, which we proceeded to shift silently back to our storage deck.

Please find enclosed everything we took, excluding one thing - 200,000+ Brink users. We actually like this company and would like for them to speed up the production of Skyrim, so we'll give them one less thing to worry about. You're welcome! :D

Please keep making awesome games, guys, and you should totally add an official LulzSec top hat to new releases.

But anyway, bwahahaha... >:]

LINKS:

http://thepiratebay.org/torrent/6467131/Bethesda_internal_data

BONUS ROUND! SENATE.GOV!

<http://lulzsecurity.com/releases/senate.gov.txt>

Appendix N: LulzSec - 1000th tweet statement

Dear Internets,

This is Lulz Security, better known as those evil bastards from twitter. We just hit 1000 tweets, and as such we thought it best to have a little chit-chat with our friends (and foes).

For the past month and a bit, we've been causing mayhem and chaos throughout the Internet, attacking several targets including PBS, Sony, Fox, porn websites, FBI, CIA, the U.S. government, Sony some more, online gaming servers (by request of callers, not by our own choice), Sony again, and of course our good friend Sony.

While we've gained many, many supporters, we do have a mass of enemies, albeit mainly gamers. The main anti-LulzSec argument suggests that we're going to bring down more Internet laws by continuing our public shenanigans, and that our actions are causing clowns with pens to write new rules for you. But what if we just hadn't released anything? What if we were silent? That would mean we would be secretly inside FBI affiliates right now, inside PBS, inside Sony... watching... abusing...

Do you think every hacker announces everything they've hacked? We certainly haven't, and we're damn sure others are playing the silent game. Do you feel safe with your Facebook accounts, your Google Mail accounts, your Skype accounts? What makes you think a hacker isn't silently sitting inside all of these right now, sniping out individual people, or perhaps selling them off? You are a peon to these people. A toy. A string of characters with a value.

This is what you should be fearful of, not us releasing things publicly, but the fact that someone hasn't released something publicly. We're sitting on 200,000 Brink users right now that we never gave out. It might make you feel safe knowing we told you, so that Brink users may change their passwords. What if we hadn't told you? No one would be aware of this theft, and we'd have a fresh 200,000 peons to abuse, completely unaware of a breach.

Yes, yes, there's always the argument that releasing everything in full is just as evil, what with accounts being stolen and abused, but welcome to 2011. This is the lulz lizard era, where we do things just because we find it entertaining. Watching someone's Facebook picture turn into a penis and seeing their sister's shocked response is priceless. Receiving angry emails from the man you just sent 10 dildos to because he can't secure his Amazon password is priceless. You find it funny to watch havoc unfold, and we find it funny to cause it. We release personal data so that equally evil people can entertain us with what they do with it.

Most of you reading this love the idea of wrecking someone else's online experience anonymously. It's appealing and unique, there are no two account hijackings that are the same, no two suddenly enraged girlfriends with the same expression when you admit to killing

prostitutes from her boyfriend's recently stolen MSN account, and there's certainly no limit to the lulz lizardry that we all partake in on some level.

And that's all there is to it, that's what appeals to our Internet generation. We're attracted to fast-changing scenarios, we can't stand repetitiveness, and we want our shot of entertainment or we just go and browse something else, like an unimpressed zombie. Nyan-nyan-nyan-nyan-nyan-nyan-nyan, anyway...

Nobody is truly causing the Internet to slip one way or the other, it's an inevitable outcome for us humans. We find, we nom nom nom, we move onto something else that's yummiier. We've been entertaining you 1000 times with 140 characters or less, and we'll continue creating things that are exciting and new until we're brought to justice, which we might well be. But you know, we just don't give a living fuck at this point - you'll forget about us in 3 months' time when there's a new scandal to gawk at, or a new shiny thing to click on via your 2D light-filled rectangle. People who can make things work better within this rectangle have power over others; the whitehats who charge \$10,000 for something we could teach you how to do over the course of a weekend, providing you aren't mentally disabled.

This is the Internet, where we screw each other over for a jolt of satisfaction. There are peons and lulz lizards; trolls and victims. There's losers that post shit they think matters, and other losers telling them their shit does not matter. In this situation, we are both of these parties, because we're fully aware that every single person that reached this final sentence just wasted a few moments of their time.

Thank you, bitches.

Lulz Security

Appendix O: Operation Anti-Security

Salutations Lulz Lizards,

As we're aware, the government and whitehat security terrorists across the world continue to dominate and control our Internet ocean. Sitting pretty on cargo bays full of corrupt booty, they think it's acceptable to condition and enslave all vessels in sight. Our Lulz Lizard battle fleet is now declaring immediate and unremitting war on the freedom-snatching moderators of 2011.

Welcome to Operation Anti-Security (#AntiSec) - we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.

Whether you're sailing with us or against us, whether you hold past grudges or a burning desire to sink our lone ship, we invite you to join the rebellion. Together we can defend ourselves so that our privacy is not overrun by profiteering gluttons. Your hat can be white, gray or black, your skin and race are not important. If you're aware of the corruption, expose it now, in the name of Anti-Security.

Top priority is to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments. If they try to censor our progress, we will obliterate the censor with cannonfire anointed with lizard blood.

It's now or never. Come aboard, we're expecting you...

History begins today.

Lulz Security,
<http://LulzSecurity.com/>

Support: <http://www.mithral.com/~beberg/manifesto.html>
Support: <http://www.youtube.com/user/thejuicemedia>
Support: <http://wikileaks.ch/>
Support: <http://anonyops.com/>

Myself and the rest of my Lulz shipmates will then embark upon a trip to ThePirateBay with our beautiful records for your viewing pleasure!

Ahoy! Bwahahaha... >:]

Cap'n Pierre "Lulz" Dubois

LINKS:

http://thepiratebay.org/torrent/6467131/Bethesda_internal_data

BONUS ROUND! SENATE.GOV!

<http://lulzsecurity.com/releases/senate.gov.txt>

Appendix Q: Snitches getting various stitches

Hi FBI & other law enforcement clowns,

LulzSec here with some juicy gossip.

This is [Sensitive/Personal Information Redacted], also known as "[redacted]" in the "#pure-elite" IRC logs you no doubt have enjoyed. He was involved in the hacking of the game "Dues Ex" and was/is involved in countless other cybercrimes.

Also, he tried to snitch on us. Therefore we just did your job for you with great ease.

This moron is trying to flee the country in order to avoid serious punishment. Hunt him down:

SNITCH: [Sensitive/Personal Information Redacted]
 EXPOSED: YES
 AIM: [Sensitive/Personal Information Redacted]
 Last known IP: [Sensitive/Personal Information Redacted]
 Location: [Sensitive/Personal Information Redacted]
 Name: [Sensitive/Personal Information Redacted]

This is also the name of one of his associates, Michael, or "Hann". He's also wanted for some pretty heavy stuff:

PIC: [Sensitive/Personal Information Redacted]
 Name: [Sensitive/Personal Information Redacted]
 DOB: [Sensitive/Personal Information Redacted]
 Aliases: [Sensitive/Personal Information Redacted]
 Address: [Sensitive/Personal Information Redacted]
 Phone: [Sensitive/Personal Information Redacted]
 Google Voice Number: [Sensitive/Personal Information Redacted]
 AIM: [Sensitive/Personal Information Redacted]
 IRC: [Sensitive/Personal Information Redacted]

These goons begged us for mercy after they apologized to us all night for leaking some of our affiliates' logs. There is no mercy on The Lulz Boat.

Snitches get stitches,

Lulz Security

[Sensitive/Personal Information Redacted]

While we are responsible for everything that The Lulz Boat is, we are not tied to this identity permanently. Behind this jolly visage of rainbows and top hats, we are people. People with a preference for music, a preference for food; we have varying taste in clothes and television, we are just like you. Even Hitler and Osama Bin Laden had these unique variations and style, and isn't that interesting to know? The mediocre painter turned supervillain liked cats more than we did.

Again, behind the mask, behind the insanity and mayhem, we truly believe in the AntiSec movement. We believe in it so strongly that we brought it back, much to the dismay of those looking for more anarchic lulz. We hope, wish, even beg, that the movement manifests itself into a revolution that can continue on without us. The support we've gathered for it in such a short space of time is truly overwhelming, and not to mention humbling. Please don't stop. Together, united, we can stomp down our common oppressors and imbue ourselves with the power and freedom we deserve.

So with those last thoughts, 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

Our mayhem: <http://lulzsecurity.com/releases/>
Our chaos: <http://thepiratebay.org/user/LulzSec/>
Our final release:
http://thepiratebay.org/torrent/6495523/50_Days_of_Lulz

Please make mirrors of material on the website, because we're not renewing the hosting. Goodbye. <3

to the department, they punished him and pushed him out of the police force. We welcome Wilson's attempts to expose his racist administrators and so we won't be releasing his info.

Yes we're aware that putting the pigs on blast puts risks their safety, those poor defenseless police officers who lock people up for decades, who get away with brutality and torture, who discriminate against people of color, who make and break their own laws as they see fit. We are making sure they experience just a taste of the same kind of violence and terror they dish out on an every day basis. Our advice to you is to quit while you still can and turn on your commanding officers before you end up in our cross hairs next, because we're not stopping until every prisoner is freed and every prison is burned to the ground.

To other hackers: it's time to set aside our differences and join the antiseccular popular front against the corrupt governments, corporations, militaries, and law enforcement of the world. We promise you much more bounty to come guaranteed to bring smiles to the faces of all those who have hated the police. Unite and fight, for the flames of revolution burn bright!

```
/*  
the files  
*/
```

[Sensitive/Personal Information Redacted]

kastamonudh.gov.tr
 korgandh.gov.tr
 kovancilardh.gov.tr
 kursunludh.gov.tr
 kursunluuh.gov.tr
 mackadh.gov.tr
 menemendh.gov.tr
 niksardh.gov.tr
 ofdevlethastanesi.gov.tr
 ordudogum.gov.tr
 ortakoydevlethastanesi.gov.tr
 pazardh53.gov.tr
 rize82yildh.gov.tr
 rizeagizdissagligi.gov.tr
 samandagdh.gov.tr
 samsunghh.gov.tr
 sandiklidevlethastanesi.gov.tr
 sarikayadh.gov.tr
 sefaatlidevlethastanesi.gov.tr
 sorgundevlethastanesi.gov.tr
 sungurludevlethastanesi.gov.tr
 tatvandogumevi.gov.tr
 tavasdh.gov.tr
 tireboludh.gov.tr
 tonyadevlethastanesi.gov.tr
 torbalidh.gov.tr
 toruldh.gov.tr
 trabzonadsm.gov.tr
 trbdogum-cocuk.gov.tr
 tuzlucadh.gov.tr
 unyedevlethastanesi.gov.tr
 uzumludevlet.gov.tr
 vezirkoprudh.gov.tr
 yusufelidh.gov.tr
 zeynepkamil.gov.tr

May the winds be always with you, sail strong my friends!

#antisecc

Appendix X: Fuck FBI Friday II: IRC Federal

```
#####
### #ANTISEC LAYING NUCLEAR WASTE TO MILITARY AND WHITE HAT BOXES SINCE 2011 ###
# FOR OFFICIAL UNDERGROUND USE ONLY # FUCK LOIC & LOIC-KIDS # FUCK BARRETBROWN #
#####
```

```

 _ |  |  | _ |  |  | _ |  |  | _ |  |  | _ |  |  | _ |  |  |
/ |  |  | \ |  |  | / |  |  | \ |  |  | \ |  |  | \ |  |  |
| |  |  | | |  |  | | |  |  | | |  |  | | |  |  | | |  |  |
\ |  |  | / |  |  | \ |  |  | / |  |  | \ |  |  | \ |  |  |
 _ |  |  | _ |  |  | _ |  |  | _ |  |  | _ |  |  |
#anonymous
#whiteh8
#antiseC

```

```
#####
          roses are red, violets are blue,
          we hate whitehats, and you do too!
#####
```

Today we release the owngage of another government-contracted IT company, IRC Federal. They brag about their multi-million dollar partnership with the FBI, Army, Navy, NASA, and the Department of Justice, selling out their "skills" to the US empire. So we laid nuclear waste to their systems, owning their pathetic windows box, dropping their databases and private emails, and defaced their professional looking website.

In their emails we found various contracts, development schematics, and internal documents for various government institutions including a proposal for the FBI to develop a "Special Identities Modernization (SIM) Project" to "reduce terrorist and criminal activity by protecting all records associated with trusted individuals and revealing the identities of those individuals who may pose serious risk to the United States and its allies". We also found fingerprinting contracts for the DOJ, biometrics development for the military, and strategy contracts for the "National Nuclear Security Administration Nuclear Weapons Complex".

Additionally we found login info to various VPNs and several Department of Energy login access panels that we are dumping *live* complete with some URLs to live ASP file browser and upload backdoors - let's see how long it takes for them to remove it (don't worry we'll keep putting it back up until they pull the box ;D)

Before we begin the drop, a personal message to the employees of IRC Federal:

If you place any value on freedom, then stop working for the oligarchy and start working against it. Stop aiding the corporations and a government which uses unethical means to corner vast amounts of wealth and proceed to flagrantly abuse their power. Together, we have the power to change this world for the better.

â€œHe who passively accepts evil is as much involved in it as he who helps to perpetuate it.â€ â€”Martin Luther King, Jr.

Props to our black hat and antiseC comrades: bantown, dikline, h0no, phrack high council, ~el8 and all you kick-ass motherfuckers we've never even heard of. Thank you.

* Melissa Hathaway, Current Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils

Now let's check out what these guys have been doing:

* Questionable involvement in the U.S. government's SWIFT surveillance program; acting as auditors of a government program, when that contractor is heavily involved with those same agencies on other contracts. Beyond that, the implication was also made that Booz Allen may be complicit in a program (electronic surveillance of SWIFT) that may be deemed illegal by the EC.

<http://www.aclu.org/national-security/booz-allens-extensive-ties-government-raise-more-questions-about-swift-surveillance>

<https://www.privacyinternational.org/article/pi-and-aclu-show-swift-auditor-has-extensive-ties-us-government>

* Through investigation of Booz Allen employees, Tim Shorrock of Democracy Now! asserts that there is a sort of revolving-door conflict of interest between Booz Allen and the U.S. government, and between multiple other contractors and the U.S. government in general. Regarding Booz Allen, Shorrock referred to such people as John M. McConnell, R. James Woolsey, Jr., and James R. Clapper, all of whom have gone back and forth between government and industry (Booz Allen in particular), and who may present the appearance that certain government contractors receive undue or unlawful business from the government, and that certain government contractors may exert undue or unlawful influence on government. Shorrock further relates that Booz Allen was a sub-contractor with two programs at the U.S. National Security Agency (NSA), called Trailblazer and Pioneer Groundbreaker.

<http://www.democracynow.org/article.pl?sid=07/01/12/151224>

If you haven't heard about Pioneer Groundbreaker, we recommend the following Wikipedia article:

"The NSA warrantless surveillance controversy (AKA "Warrantless Wiretapping") concerns surveillance of persons within the United States during the collection of foreign intelligence by the U.S. National Security Agency (NSA) as part of the war on terror."

http://en.wikipedia.org/wiki/Pioneer_Groundbreaker

* A June 28, 2007 Washington Post article related how a U.S. Department of Homeland Security contract with Booz Allen increased from \$2 million to more than \$70 million through two no-bid contracts, one occurring after the DHS's legal office had advised DHS not to continue the contract until after a review. A Government Accountability Office (GAO) report on the contract characterized it as not well-planned and lacking any measure for assuring valuable work to be completed.

<http://www.washingtonpost.com/wp-dyn/content/article/2007/06/27/AR2007062702988.html>

* Known as PISCES (Personal Identification Secure Comparison and Evaluation System), the "terrorist interdiction system" matches passengers inbound for the United States against facial images, fingerprints and biographical information at airports in high-risk countries. A high-speed data network permits U.S. authorities to be informed of problems with inbound passengers. Although PISCES was operational in the months prior to September 11, it apparently failed to detect any of the terrorists involved in the attack.

Privacy advocates have alleged that the PISCES system is deployed in various countries that are known for human rights abuses (ie Pakistan and Iraq) and that facilitating them with an advanced database system capable of storing biometric details of travelers (often without consent of their own nationals) poses a danger to human rights activists and government opponents.

<http://multinationalmonitor.org/mm2002/02march/march02corp3.html>

```

/*****
***                               BONUS ROUND TWO: ANONYMOUS INTERESTS                               ***
*****/

```

Back in February, as many may recall, Anonymous was challenged by security company HBGary. One month later - after many grandiose claims and several pages of dox on "members" of Anonymous which were factually accurate in no way whatsoever - HBGary and its leadership were busy ruing the day they ever tangled with Anonymous, and Anonymous was busy toasting another epic trolling. And there was much rejoicing. However, celebration soon gave way to fascination, followed by horror, as scandal after scandal radiated from the company's internal files, scandals spanning the government, corporate and financial spheres. This was no mere trolling. Anonymous had uncovered a monster.

One of the more interesting, and sadly overlooked, stories to emerge from HBGary's email server (a fine example to its customers of how NOT to secure their own email systems) was a military project - dubbed Operation Metal Gear by Anonymous for lack of an official title - designed to manipulate social media. The main aims of the project were two fold: Firstly, to allow a lone operator to control multiple false virtual identities, or "sockpuppets". This would allow them to infiltrate discussions groups, online polls, activist forums, etc and attempt to influence discussions or paint a false representation of public opinion using the highly sophisticated sockpuppet software. The second aspect of the project was to destroy the concept of online anonymity, essentially attempting to match various personas and accounts to a single person through recognition shared of writing styles, timing of online posts, and other factors. This, again, would be used presumably against any perceived online opponent or activist.

HBGary Federal was just one of several companies involved in proposing software solutions for this project. Another company involved was Booz Allen Hamilton. Anonymous has been investigating them for some time, and has uncovered all sorts of other shady practices by the company, including potentially illegal surveillance systems, corruption between company and government officials, warrantless wiretapping, and several other questionable surveillance projects. All of this, of course, taking place behind closed doors, free from any public knowledge or scrutiny.

You would think the words "Expect Us" would have been enough to prevent another epic security fail, wouldn't you?

Well, you'd be wrong. And thanks to the gross incompetence at Booz Allen Hamilton probably all military mersonnel of the U.S. will now have to change their passwords.

Let it flow!

```

/*****
***                               INVOICE                               ***
*****/

```

Enclosed is the invoice for our audit of your security systems, as well as the auditor's conclusion.

4 hours of man power: \$40.00
 Network auditing: \$35.00
 Web-app auditing: \$35.00
 Network infiltration*: \$0.00
 Password and SQL dumping**: \$200.00
 Decryption of data***: \$0.00
 Media and press****: \$0.00

Total bill: \$310.00

*Price is based on the amount of effort required.

**Price is based on the amount of badly secured data to be dumped, which in this case was a substantial figure.

***No security in place, no effort for intrusion needed.

****Trolling is our specialty, we provide this service free of charge.

Auditor's closing remarks: Pwned. U mad, bro?

We are Anonymous.

We are Legion.

We are Antisec.

We do not forgive.

We do not forget.

Expect us.

Appendix Z: A message to PayPal, its customers, and our friends

Dear PayPal, its customers, and our friends around the globe,

This is an official communiqué from Anonymous and Lulz Security in the name of AntiSec.

In recent weeks, we've found ourselves outraged at the FBI's willingness to arrest and threaten those who are involved in ethical, modern cyber operations. Law enforcement continues to push its ridiculous rules upon us - Anonymous "suspects" may face a fine of up to 500,000 USD with the addition of 15 years' jailtime, all for taking part in a historical activist movement. Many of the already-apprehended Anons are being charged with taking part in DDoS attacks against corrupt and greedy organizations, such as PayPal.

What the FBI needs to learn is that there is a vast difference between adding one's voice to a chorus and digital sit-in with Low Orbit Ion Cannon, and controlling a large botnet of infected computers. And yet both of these are punishable with exactly the same fine and sentence.

In addition to this horrific law enforcement incompetence, PayPal continues to withhold funds from WikiLeaks, a beacon of truth in these dark times. By simply standing up for ourselves and uniting the people, PayPal still sees it fit to wash its hands of any blame, and instead encourages and assists law enforcement to hunt down participants in the AntiSec movement.

Quite simply, we, the people, are disgusted with these injustices. We will not sit down and let ourselves be trampled upon by any corporation or government. We are not scared of you, and that is something for you to be scared of. We are not the terrorists here: you are.

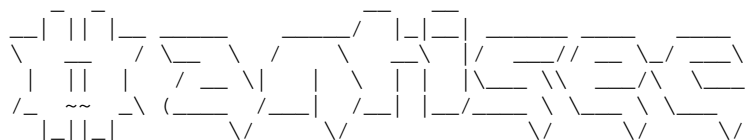
We encourage anyone using PayPal to immediately close their accounts and consider an alternative. The first step to being truly free is not putting one's trust into a company that freezes accounts when it feels like, or when it is pressured by the U.S. government. PayPal's willingness to fold to legislation should be proof enough that they don't deserve the customers they get. They do not deserve your business, and they do not deserve your respect.

Join us in our latest operation against PayPal - tweet pictures of your account closure, tell us on IRC, spread the word. Anonymous has become a powerful channel of information, and unlike the governments of the world, we are here to fight for you. Always.

Signed, your allies,

Lulz Security (unvanned)
Anonymous (unknown)
AntiSec (untouchable)

Appendix AA: Fuck FBI Friday III: ManTech Mayhem



#Anonymous
#AntiSec
#FUCK
#FBI
#FRIDAY

```

/*****
***          FUCK FBI FRIDAY III: ManTech Mayhem          ***
*****/

```

Ahoy thar,

Today is Friday and we will be following the tradition of humiliating our friends from the FBI once again. This time we hit one of their biggest contractors for cyber security: Mantech International Corporation.

What ManTech has to do with the FBI? Well, quite simple: In Summer 2010 the FBI had the glorious idea to outsource their Cybersecurity to ManTech. Value of the contract: 100 Million US-Dollar:

"The FBI is outsourcing cybersecurity to the tune of nearly \$100 million to a Washington-area managed services company. The deal shows a willingness in the federal government to place IT services more and more in the hands of third parties as agencies don't have enough staff on hand to do the job."

<http://www.informationweek.com/news/government/security/226700486>

And this is not the only Cybersecurity contract ManTech won; with a quick internet search you will be able to find lots more. And just a few months back, in March 2011, ManTech received another 9 Million cybersecurity contract from the FBI:

<http://www.euroinvestor.co.uk/news/story.aspx?id=11545467>

Well done, good sirs. You failed epically. Because we pwned ManTech utterly and thoroughly; and we did not need hundreds of millions for it. In fact, we did not require any funds at all, we did it with Lulz.

So we begin by releasing 400MB of internal data from ManTech, this gives some insight on how they are wasting the tax payer's money. Most of the documents in this first batch are related to NATO who, you may recall, made some bold claims regarding Anonymous earlier this year:

"It remains to be seen how much time Anonymous has for pursuing such paths. The longer these attacks persist the more likely countermeasures will be developed, implemented, the groups will be infiltrated and perpetrators persecuted"

<http://www.nato-pa.int/default.asp?SHORTCUT=2443>

Indeed, it remains to be seen. It also remains to be seen how much longer the public will accept how completely incompetent law enforcement agencies are spending their citizens' money to fund even more incompetent federal contractors. Incidentally, apart from the FBI, ManTech International has some other clients:

- * Defense Intelligence Agency,
- * National Geospatial-Intelligence Agency
- * National Reconnaissance Office
- * National Security Agency
- * Department of Homeland Security
- * U.S. Navy, Air Force, Army, Marine Corps
- * Missile Defense Agency and DARPA

- * Department of Justice
- * Department of State
- * Environmental Protection Agency
- * NASA, NATO, state and local governments

Great. It's really good to know that you guys are taking care of protecting the Unites States from so-called cyber threats.

It should also be noted that ManTech, along with HBGary, Palantir, Endgames and others were involved in the now-dubbed Operation MetalGear to manipulate and spy on their citizens using persona management software for social networks:

<http://wiki.echelon2.org/wiki/Mantech>

We are providing these ManTech documents so the public can see for themselves how their tax money is being spent. But don't you worry, the U.S. is a rich country and can afford to waste money, right?

Dear Government and Law Enforcement, we are repeating this message as we have the suspicion you still do not take us seriously: We are not scared anymore and your threats to arrest us are meaningless. We will continue to demonstrate how you fail at about every aspect of cybersecurity while burning hundreds of millions of dollars that you do not even have.

The director of the U.S. Computer Emergency Response Team (CERT), Randy Vickers, already resigned from his post, without proving an explanation. Let us provide you with one: Mr. Vickers realized that he is on the losing side of this war. A war that should never have been started in the first place. Not only because the enemy was vastly underestimated and misjudged completely but even more because it is fought against innocent citizens who simply chose to protest against the grievance of the government. You cannot win this war and the sooner you realize this and call for peace, the sooner we can put an end to this and solve the problems of this world together.

Dear citizens of the U.S. and the world: We are fighting in the name of all the oppressed and betrayed people. In your name we will continue to fire upon these laughable battleships until they are no more. Hold on tight while the seas are rough but we will prevail!

Anonymous
AntiSec

sometimes manipulated and edited in an attempt of embarrass or discredit government agencies and law enforcement. Also in their release, they threaten to publish the names of inmates and confidential informants. Informant and other sensitive data are not kept on the website, and we believe any information that would be released would be false in an attempt to hinder future investigations by law enforcement." - Sheriff John Montgomery (MORE DOX DROPPED)
<http://www.baxterbulletin.com/article/20110801/NEWS01/110801001/BC-Sheriff-Website-hacked?odyssey=tab|topnews|text|FRONTPAGE>

"President of the Missouri Sheriff's Association Steve Cox said he thinks the hackers claim to have more information than they really do. Cox said the group just wants glory and fame." (DOX AND SSN DROPPED)
<http://www.komu.com/news/update-group-hacks-missouri-sheriff-s-association/>

"Sheriff Joe Guy says, "We've not lost any information. There's no, we've not been hacked. I think that's been a fear. No sensitive information is on that website anyway." (DOX AND EMAILS DROPPED AGAIN)
http://wdef.com/news/mcminn_county_sheriffs_department_website/08/2011

////////////////////////////////////
 A week after we defaced and destroyed the websites of over 70 law enforcement agencies, we are releasing a massive amount of confidential information that is sure to embarrass, discredit and incriminate police officers across the US. Over 10GB of information was leaked including hundreds of private email spools, password information, address and social security numbers, credit card numbers, snitch information, training files, and more. We hope that not only will dropping this info demonstrate the inherently corrupt nature of law enforcement using their own words, as well as result in possibly humiliation, firings, and possible charges against several officers, but that it will also disrupt and sabotage their ability to communicate and terrorize communities.

We are doing this in solidarity with Topiary and the Anonymous PayPal LOIC defendants as well as all other political prisoners who are facing the gun of the crooked court system. We stand in support of all those who struggle against the injustices of the state and capitalism using whatever tactics are most effective, even if that means breaking their laws in order to expose their corruption. You may bust a few of us, but we greatly outnumber you, and you can never stop us from continuing to destroy your systems and leak your data.

We have no sympathy for any of the officers or informants who may be endangered by the release of their personal information. For too long they have been using and abusing our personal information, spying on us, arresting us, beating us, and thinking that they can get away with oppressing us in secrecy. Well it's retribution time: we want them to experience just a taste of the kind of misery and suffering they inflict upon us on an everyday basis. Let this serve as a warning to would-be snitches and pigs that your leaders can no longer protect you: give up and turn on your masters now before it's too late.

// A TALE OF TWO OWNINGS

It took less than 24 hours to root BJM's server and copy all their data to our private servers. Soon after, their servers were taken down and a news article came out suggesting they received advance FBI "credible threat" notice of a "hacking plot". At this point it was too late for them because the stolen files were gonna get leaked regardless. However we were surprised and delighted to see that not only did they relaunch a few sites less than a week later, but that their "bigger, faster server that offers more security" carried over our backdoors from their original box. This time we were not going to hesitate to pull the trigger: in less than an hour we rooted their new server and defaced all 70+ domains while their root user was still logged in and active.

We lol'd as we watched the news reports come in, quoting various Sheriffs who denied that they were ever hacked, that any personal information was stolen, that they did not store snitch info on their servers. Many lulz have been had as we taunted the sheriffs by responding to their denials by tweeting teasers exposing their SSNs, passwords, addresses, and private emails. We also took the

liberty to backdoor their online store and capture a few credit card numbers, which were used to make involuntary donations to the ACLU, the EFF, the Bradley Manning Support Network, and more. Despite active FBI investigations and their additional security measures, they could not stop us from owning their servers, stealing their identities, and dropping all their data. Two weeks later only a few of the sites are up with limited functionality as we scared them into removing any dynamic PHP scripts, forcing them to use static HTML content.

A recent DHS bulletin has called us "script kiddies" that lack "any capability to inflict damage to critical infrastructure" yet we continue to get in and out of any system we please, destroying and dropping dox on the mightiest of government systems that are supposed to be protecting their sick nightmare of "law and order". GIVE UP. You are losing the cyberwar, and the attacks against the governments, militaries, and corporations of the world will continue to escalate.

Hackers, join us to make 2011 the year of leaks and revolutions.

//

[*] ORIGINAL DEFAACEMENT: <http://zone-h.org/mirror/id/14515221>
 [*] BROWSE THE LEAK: <http://vv7pabmmyr2vnflf.onion/> (ON TOR)
<http://vv7pabmmyr2vnflf.tor2web.com/> (NOT TOR)
 [*] DONATE BITCOINS: 18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR

The booty contains:

[*] Over 300 mail accounts from 56 law enforcement domains
 [*] Missouri Sheriff account dump (mosheriffs.com)
 7000+ usernames, passwords, home addresses, phones and SSNs
 [*] Online Police Training Academy files
 PDFs, videos, HTML files
 [*] "Report a Crime" snitch list compilation (60+ entries)
 [*] Plesk plaintext server passwords (ftp/ssh, email, cpanel, protected dirs)

//

Satiagraha resultou na prisãfo de muitos investidores, banqueiros e diretores de bancos. A maior figura na investigaãfo foi Daniel Dantas, um banqueiro brasium banqueiro brasileiro e financciador, fundador do Opportunity Asset Management. O grupo que liderou a parceria de setores privados internacionais que resultou na compra de uma parte significativa de empresas de telefonia brasileiras.

Queiroz foi removido da operaãfo por nãfo ter informado seus superiores do envolvimento do Serviãfo Secreto. Ele tambãfo foi investigado por colaborar com o Serviãfo Secreto Brasileiro atravãos do uso de grampos telefãnicos ilegais. Os arquivos completos nunca foram revelados e muitas das informaãfoes nunca foram divulgadas pelo alto nãvel de corrupãfo dentro do Governo do Brasil.

Esses arquivos contãam evidãncias reunidas pela Operaãfo Satiagraha, uma operaãfo que foi fundo na exposiãfo do nãvel de corrupãfo envolvendo o Governo brasileiro e grandes Corporaãfoes, centralizadas em torno de Daniel Dantas e Kröll, uma corporaãfo multinacional que tem ligaãfoes com ex-agentes da CIA , que permaneceram desconhecidas atão hoje.

Apesar de Protãgenes Queiroz ter dito, em uma entrevista ((<http://www.conversaafiada.com.br/audio/2011/08/08/protogenes-identifica-advogado-e-jornalista-da-gravacao/>) apãs tomar conhecimento do vazamento dos documentos obtidos por Anonymous, que havia a possibilidade do envolvimento de opositores do governo na aãfo, numa tentativa de acelerar um golpe de Estado, este nãfo ão o caso e sã mostra que o governo estã; temeroso em relaãfo ao que esses arquivos podem significar.

Esses arquivos foram obtidos pela equipe Anonymous, e estãfo aqui agora para que todo pãblico veja a verdadeira corrupãfo no Brasil. Nãs nãfo apoiamos governos ou partidos. Nãs lutamos pela liberdade, das pessoas e da informaãfo. Estamos divulgando esses arquivos para espalhar a informaãfo e permitir que as pessoas sejam ouvidas e saibam da corrupãfo em seu governo. Nãs os estamos revelando para dar poder ã voz do povo brasileiro. Nãs estamos divulgando para acabar com a corrupãfo que existe, e para libertar aqueles que vãam sendo oprimidos.

Nãs somos Anonymous. Nãs somos Legiãfo. Nãs nãfo esquecemos. Nãs nãfo perdoamos. Nos Aguardem

#####

[*] BitCoin donations to: 18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR

[*] BROWSE THE FILES:

<http://4aclu6ka6s7gz6st.onion/br> (if you are on tor)

<http://4aclu6ka6s7gz6st.tor2web.org/br> (if you aren't on tor)

<http://satiagrahaleaks.org/leaks/> (original HTTP mirror)

#####

Significant files to look at first:

[*] How the Privatization Scheme Works
<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/1805.doc>

[*] People Involved with the operation
<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/1798.doc>

[*] List of Investors
<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/1812.doc>
<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/3744.doc>

[*] Who has money on Oportunity - American banks
<http://4aclu6ka6s7gz6st.tor2web.org/br/948/Export/159348.pdf>

BARCLAYS 5.000.000,00 5,000,000.00
SANTANDER 1.000.000,00 1,000,000.00

MORGAN SWAP (UNIQ 1.550.000,00 1,550,000.00
MORGAN FUTURES (UNIQUE) 4.080.853,53 4,080,853.53
DEUTSCHE BANK NDF 508.127,02 508,127.02
6.303.494,93 6,303,494.93
UBS FUTURES 13.360.555,83 13,360,555.83
UBS DUBLIN 235.336,07 235,336.07
BROWN BROTHERS HARRIMAN 65.769.898,19 65,769,898.19
GOLDMAN & SACHS, INC 1.252.112,88 1,252,112.88
UBS (UNIQUE) 7.552.995,03 7,552,995.03
BROWN BROTHERS HARRIMAN (522,49) (522.49)
BROWN BROTHERS (EURO) 1.160.818,86 1,160,818.86

[*] NAJI Speaks about 50 milion euros, his conections with the Saudi Arabian king, Page 5 on report:

<http://4aclu6ka6s7gz6st.tor2web.org/br/948/Export/158529.doc>

<http://4aclu6ka6s7gz6st.tor2web.org/br/948/Export/160085.wav>

[*] Envolvment with the actual president Dilma R

HUMBERTO e LUIZ EDUARDO says in the dialog information about a possible agreement that is being made between CITIBANK and GRUPO OPPORTUNITY. With the creation of one "Supertele" with the fusion of operations Oi-telemar, telemig, brasiltelecom e amazonia celular, possible with the authorization of the president of republic (viel decret, see that this fusion are ilegal) and the resources BNDS, the necessity of the reunion of President Dilma Russef

[*] Proof of BNDES Involvment (Brazilian Bank of Development)

<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/4117.doc>

[*] Document to the Supreme Court of New York about Brasil Telecom

<http://4aclu6ka6s7gz6st.tor2web.org/br/948/Export/159528.pdf>

<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/2894.wav>

[*] Report of Dantas successfully being contacted by a journalist, and expediting a news article in good favor of him to be written through bribery

<http://4aclu6ka6s7gz6st.tor2web.org/br/758/Export/5850.doc>

Analysis: Humberto JosÃ^ Rocha Braz is with Guilherme Henrique Martins SODRE people DANIEL V. Dantas hired by their companies, for espionage work, influence peddling, "planting" false news in the media and making a false dossier (often the contents of the dossier is reported in the media casting doubt organizations, journalists, or state institutions). DANTAS always talks with them in code, in this case, Dante is afraid that there is some research being conducted against him and asks to leave GOMES (codenamed Luiz Eduardo Greenhalgh)

Defense Industries, but to send a strong message to the hacker community. White hat sellouts, law enforcement collaborators, and military contractors beware: we're coming for your mail spools, bash history files, and confidential documents.

Can't stop, won't stop.

#####

[*] BROWSE THE EMAILS:

<http://4aclu6ka6s7gz6st.onion/vanguard/> <- on tor
<http://4aclu6ka6s7gz6st.tor2web.org/vanguard/> <- not on tor

[*] DONATE BITCOINS TO SUPPORT FUTURE HACKS AND LEAKS:

18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR

#####

Having a slow day behind the desk, filing papers, staring at your colleague's fine posterior? What have you been up to since our last visit? Don't answer that. We already know.

Lewd jokes? Check. Racist chain mails? Check. You lost your radio license? Lulz. Playing on the fears of voters? Check. But we already figured that. Our friends, allies, and vessels are threatened with 10+ years in prison. Yet terrorists like Luis Posada Carilles go free. This hypocritical and paranoid reaction puts us and the citizens you are supposed to protect in the same boat. You call us a national security risk. Yet BATFE guns go directly to drug dealers so they can take out rivals who don't launder money through backrooms of dominant banks. Any press can check court documents from operations like 'Fast and Furious'. Who came up with that one? What you didn't see 'From Dusk 'til Dawn'? Better title. Be more creative next time.

In retaliation for the arrests of dozens of alleged Anonymous suspects, we opened fire on dozens of Texas police departments and stole boatloads of classified police documents and police chief emails across the state. During the San Jose courtdate we defaced and gave out live backdoor and admin access to the website TexasPoliceChiefs.org while allied ships launched ddos attacks upon Justice.gov and other law enforcement websites. For every defendant in the anonymous "conspiracy" we are attacking two top Texas police chiefs, leaking 3GB of their private emails and attachments. Mind you, we don't expect a sane response. Even a few insults would have been better than the way you cowards hide behind protocol, innuendo, and your badge.

For more than a month we have been lurking their emails, law enforcement portals, and records and reporting systems. We leaked a few teasers including access to fbivirtualacademy.edu, several classified documents, voicemail recordings, live passwords, and even some dirty pictures. To continue the fighting spirit of WikiLeaks, we want to share the full Texas collection and expose these bumbling fools and all their secrets to the world.

Thousands of documents are available on tor hidden services / bittorrent and include several dozen FBI, Border Patrol, and counter-terrorism documents classified as "law enforcement sensitive" and "for official use only". The emails also included police records, internal affairs investigations, meeting notes, training materials, officer rosters, security audits, and live password information to government systems. The private chief emails also included several racist and sexist chain email forwards and personal details sure to embarrass, discredit, and incriminate several of these so-called "community leaders".

We are attacking Texas law enforcement as part of "Chinga La Migra" as they continue to harass immigrants and use border patrol operations as a cover for their backwards racist prejudice. The notoriously racist police state of Texas recently passed SB 9 and "Secure Communities" anti-immigration laws. Texas is well known and hated for being full of Minutemen, Tea Party and KKK groups, murdering the most amount of innocent people on death row, and giving us the Bush and Cheney administration. Two months ago on the 1st we attacked the Arizona DPS and defaced several Fraternal Order of Police websites. One month ago we "Shot The Sheriff" and released 10GB of private law enforcement data while defacing dozens of police department websites in several states in the south. A week ago we released private emails belonging to Richard T. Garcia, VP of Texas-based Vanguard Defense Industries, and also a former FBI agent and current Infragard executive board member.

We are doing this in solidarity with the "Anonymous 16" PayPal LOIC defendants, accused LulzSec member Jake Davis "Topiary", protesters arrested during #OpBart actions, Bradley Manning, Stephen Watt, and other hackers and leakers worldwide. We also call for the release of Leonard Peltier, Mumia Abu Jamal, Oscar Lopez Rivera, Troy Davis, the Angola 3, and all others behind bars standing up to state repression. While many of our comrades facing charges and in prison are innocent, there is no such thing as an innocent police officer, and we will continue to directly attack the prison industrial complex by leaking their private data, destroying their systems, and defacing their websites.

We might have respect for these officers if they understood their job and whom they serve. But unlike some that left the force decades ago and rumors abound that they may have joined our ranks, these officers hide behind their badge and use policies to ignore their great responsibility. These officers betrayed the trust citizens have in them by choosing be drones of the system rather than protectors of freedom and the peace of their communities. From the lowest prison guard to the mightiest chief, we will continue to attack the cogs of the police state that protects the interests of the rich and powerful.

Hackers all over the world are uniting to make 2011 the year of hacks and revolutions. Join us, comrades: open fire on governments, law enforcement organizations, white hat, corporate and military targets!

#####

- [*] THE DEFAACEMENT!!
Mirrored at <http://zone-h.org/mirror/id/14841451>
- [*] THE FILES!!

http://vv7pabmmyr2vnflf.onion/tx/	<- on tor
http://vv7pabmmyr2vnflf.tor2web.org/tx/	<- not on tor
- [*] THE TORRENT!!
<http://wikisend.com/download/269976/texsastakedownthursday.torrent>
- [*] DONATE BITCOINS!!
18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR

sure these people are angrily sending out DMCA takedown notices and serving subpoenas as we speak. They call us criminals, script kiddies, and terrorists, but their entire livelihood depends on us, trying desperately to study our techniques and failing miserably at preventing future attacks. See we're cut from an entirely different kind of cloth. Corporate security professionals like Thomas Ryan and Aaron Barr think they're doing something noble by "leaking" the public email discussion lists of Occupy Wall Street and profiling the "leaders" of Anonymous. Wannabe player haters drop shitty dox and leak partial chat logs about other hackers, doing free work for law enforcement. Then you got people like Peiter "Mudge" Zatko who back in the day used to be old school l0pht/cDc only now to sell out to DARPA going around to hacker conventions encouraging others to work for the feds. Let this be a warning to aspiring white hat "hacker" sellouts and police collaborators: stay out the game or get owned and exposed. You want to keep mass arresting and brutalizing the 99%? We'll have to keep owning your boxes and torrenting your mail spools, plastering your personal information all over teh internets.

Hackers, join us and rise up against our common oppressors - the white hats, the 1%'s 'private' police, the corrupt banks and corporations and make 2011 the year of leaks and revolutions!

We are Anti-Security,
 We are the 99%
 We do not forgive.
 We do not forget.
 Expect Us!

#####

[*] Browse the emails using Tor Hidden Services:
<http://ibhg35kgdvn7jvw.onion/cybercrime> <- on tor
<http://ibhg35kgdvn7jvw.tor2web.org/cybercrime> <- not on tor

[*] Download the emails using BitTorrent:
<http://www.thepiratebay.org/user/AntiSecurity>

[*] Donate BitCoins for future leaks!! 18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR

#####

(full release text here: <http://pastebin.com/NwN8ehFW>)

conference starts on the Day of Action Against Police Brutality. They must not have known that all over the world people are in the streets demonstrating discontent with capitalism and the state. They also had no idea that for the past few months black hat hackers have been owning their websites and databases. They should have expected us.

In solidarity with the Occupation Movement and the International Day of Action Against Police Brutality, allied #anonymous and #antisecc vessels took aim at the corrupt bootboys of the 1%: the police. We hacked, defaced, and destroyed several law enforcement targets, leaking over 600MB of private information including internal documents, membership rosters, addresses, passwords, social security numbers, and other confidential data. According to the IACP's development documents, their systems cost several hundred thousand dollars. We are pleased to destroy it all for free, leaking their private info and defacing their websites in one swift blow.

We attacked MatrixGroup.net, a multi-million dollar Washington DC based web development firm, which serves over a hundred government, corporate and association websites. Many lulz have been had as we owned their white hat "\\\"professional\\" intranet, clients and employee wiki portals-- accessing records and passwords, internal communications, company schedules, and development notes for over a hundred clients. We intentionally excluded the unions and other unrelated sites on their servers because, unlike the police and those who support them, we will never betray our working class comrades. We realize our role in the social struggle against capital and against the state, deciding instead to set our sights on the police, military and other government websites hosted by Matrix.

Our lulzboats also took aim at Boston Police in retaliation for the unprovoked mass arrests and brutality experienced by those at Occupy Boston. We hacked the Boston Police Patrolmens' Association (www.bppa.org), releasing full names and the cleartext, user-supplied passwords for a thousand members. Many lulz have been had while perusing their emails and facebook accounts, and we are now sharing their passwords for others so they can join in on the mayhem as well. Let this be a warning to BPD and police everywhere: future acts of aggression against our movements will be met with a vengeance so epic and relentless that your children's children will puke at the sight of swine.

After exhausting both sides of Milli Vanillis' "\\\"Girl You Know It's True\\" tape,

we also decided to attack Alabama law enforcement systems, releasing the names, addresses, and social security numbers for 1000 Birmingham / Jefferson County police officers as well as defacing and destroying the website SherrifOfBaldwin.com. We are attacking Birmingham specifically because of their notorious racial discriminatory practices including the savage beatings and mass arrests endured by civil rights protesters during the 60s. Although we had records of inmates, active warrant names, addresses, charges and social security numbers the thought of releasing them never crossed our mind because we would never betray our brothers and sisters shackled and chained behind prison walls-- our targets are the ones who beat and murder with immunity, the cowardly carcasses and lifeless hosts of power who hide behind a badge.

We are also acting in solidarity with the dozens of alleged "\\\"Anonymous\\" members around the world facing charges for "\\\"hacking,\"\" including the Paypal LOIC defendants in San Jose, Commander X, Recursion, Topiary, Stephen Watt, and more. We are acting in solidarity with the thousands of prisoners in California on Hunger Strike fighting for better living conditions and an end to prolonged solitary confinement. We also call for the IMMEDIATE RELEASE of not only political prisoners (Leonard Peltier, Mumia Abu Jamal, the MOVE 9, the Angola 3, and more) but all prisoners everywhere including all Jon Burge torture survivors still behind bars.

We are attacking the police because they are the vicious boot boys of the 1% whose role in society is to protect the interests and assets of the rich ruling class. They are not part of the 99%-- they are working class traitors who are paid to intimidate, harass, and repress political movements that would possibly

stand a threat to the power structure of the 1%. We have no problem targeting police and releasing their information even if it puts them at risk because we want them to experience just a taste of the brutality and misery they serve us on an everyday basis. We hope those working for the police who have any humanity left refuse their orders and leak the police and their commanding officer's vital secrets and dirt. We must realize that police are no allies of ours and have violently attacked our movements all across the world throughout history.

In Chicago, where the International Association of Chiefs of Police conference is taking place, the CPD has a particularly bloody and ruthless history of brutality and repression of political movements. Throughout the 70s and 80s under Jon Burge (chief detective) and former Mayor Richard M. Daley (prosecuter at the time), dozens of CPD detectives many whom are still on the force tortured hundreds of innocent black men, forcing confessions and giving out decades-long prison sentences for crimes never committed. The CPD also operates notorious "red squad" COINTELPRO operations that attempts to discredit and disrupt revolutionary groups-- including the assassination of Black Panther Party leaders Fred Hampton and Mark Clark. This repression continues today as they beat and arrested over 900 protesters when the second War in Iraq broke out, and just over a year ago dozens of protest organizers were raided by the FBI for alleged affiliation with resistance movements. The CPD just announced a new 'counter-terrorism' operation (taking tips from the NYPD playbook) likely to target protest organizers for the upcoming G8 and NATO conferences in May. Although they try to intimidate us by training over 13,000 riot police for these protests, we believe that they are the truly the frightened ones, and perhaps for good reason: the high profile hacks will continue, and the protests against the 1% are growing every day.

We are 99%. We are the working class that makes society function. We are not intimidated by the States attempts to disrupt our resistance through unprovoked arrests and harassments. As the violence of the cops, the courts, the FBI, La Migra, and Homeland Security intensifies, so must our resistance: we will continue to bring the ruckus on the streets and on the internet. We are believers and practitioners of direct action against all governments, militaries, banks, corporations, and police working towards our revolutionary goal: the immediate dissolution of capitalism and the state.

Hackers, join us to make 2011 the year of leaks and revolutions!

"We will destroy laughing, we will set fires laughing, we will kill laughing... and society will fall!!" - Renzo Novatore

 ### OWN & RM ### OWN & RM ### OWN & RM ### OWN & RM ### OWN & RM ###
 #####

- [*] INTERNATIONAL CHIEF OF POLICE TARGETS:
 - * IACP membership rosters (16,000 names, addresses, member numbers, phone numbers, etc)
 - * Databases for all IACP related websites including login/password info
 - * DISCOVERPOLICECAREERS.ORG Internal Documents (250MB of PDFs, DOCs)
 - * POLICEVOLUNTEER.ORG Private Email List 2005-2011 and 340MB of Documents

- [*] BOSTON POLICE PATROLMENS' ASSOCIATION:
 - 1000 full names and cleartext user-supplied passwords.

- [*] ALABAMA POLICE TARGETS:
 - 1000 names, ranks, addresses, phone numbers, and social security numbers for police officers in Birmingham / Jefferson County area, as well as names and passwords associated with SheriffOfBaldwin.com website

- [*] MATRIX GROUP:
 - Full contact database including names, addresses, passwords for hundreds of employees and clients, and internal development notes for intranet and clients portals

#####

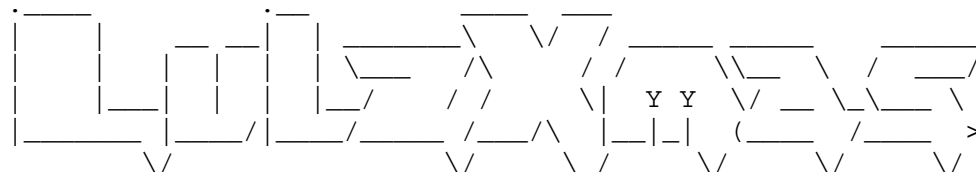
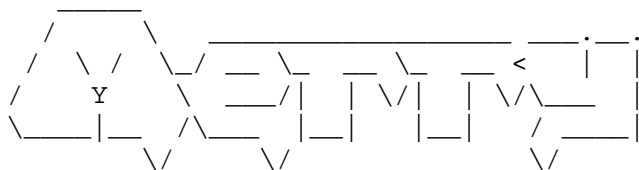
IACP ### OWNED ### IACP ### OWNED ##### IACP ### OWNED ### IACP ### OWNED ###
 #####

CAREERSINPOLICING.COM, CAREERSINPOLICING.ORG, DECP.ORG,
 DISCOVERLAWENFORCEMENT.NET,
 DISCOVERLAWENFORCEMENT.ORG, DISCOVERPOLICE.COM, DISCOVERPOLICE.NET,
 DISCOVERPOLICE.ORG, DISCOVERPOLICECAREERS.COM, DISCOVERPOLICECAREERS.ORG,
 DISCOVERPOLICING.COM, DISCOVERPOLICING.NET, DISCOVERPOLICING.ORG,
 IACP-JOYCE.ORG, IACPRESEARCH.ORG, IACPSOCIALMEDIA.ORG, IACPTRAINING.COM,
 IACPTRAINING.ORG, IDSAFETY.COM, IDSAFETY.ORG, LAWENFORCEMENTCAREERS.ORG,
 LAWENFORCEMENTCHALLENGE.ORG, PATROLVEHICLESAFETY.ORG, POLICECHIEFMAGAZINE.COM,
 POLICECHIEFMAGAZINE.NET, POLICECHIEFMAGAZINE.ORG, POLICECHIEFONLINE.COM,
 POLICECHIEFONLINE.NET, POLICECHIEFONLINE.ORG, POLICEVOLUNTEER.COM,
 POLICEVOLUNTEER.ORG, POLICEVOLUNTEERS.COM, POLICEVOLUNTEERS.ORG, PSLC-IACP.ORG,
 RESPONSETOVICTIMS.COM, RESPONSETOVICTIMS.INFO, RESPONSETOVICTIMS.NET,
 RESPONSETOVICTIMS.ORG, VOLUNTEERINPOLICESERVICE.ORG,
 VOLUNTEERSINPOLICESERVICE.ORG 40 police domains wiped off the internet

#####

(read full release text and hacklog at <http://pastebin.com/aFe0eVsU>)

Appendix HH: AntiSec teaser 12/26



#AntiSec

Greetings Global Pirates,

We truly hope that you've been enjoying the Lulzxmas festivities so far. The gifts that AnonSanta left under the LulzXmas tree are just the beginning. As we speak, his little helpers at the North Pole are readying his battle sleigh of lulz with more goodies to bring you LulzXmas joy all week long. Joy in the form of over \$500,000 being expropriated from the bigshot clients of Stratfor. You didn't think we'd let 2011 end without a BANG, did you?

However, if you are one of the hundreds of thousands of customers of STRATFOR Global [Un]Intelligence, you probably woke up Christmas morning to find heaps of burning coal in your stocking. But don't fret. Take comfort in the fact that at least you're not George Friedman or any of the STRATFOR IT guys right now.

We create chaos. We create mayhem. We curb stomp companies that play fast and loose with their customers' private and sensitive information. We bring pain to greedy whitehats willing to flip for a dime on government payrolls. And don't worry—there's plenty more havoc in store for the rest of the week. So throw a log on the fire, grab some hot chocolate and settle in for a long week of lulz.

Did you have fun looting and plundering from the pocketbooks of the rich and powerful? How about laughing at the reaction of some of their butthurt customers. We LOL'd hard when poor little Cody Sultenfuss, ranch owner and DHS employee, who asked "Why me?" and when Allen Barr, just retired from the Texas Dept. of Banking, exclaimed, "It made me feel terrible. It made my wife feel terrible." Let us not forget dear old Victor Gebilaguin, who posted the following on STRATFOR's Facebook wall in defense of the company: "The hackers ought to be shot then hanged upside down in public."

Well since you feel so strongly about it Victor, we went ahead and ran your card up a bit. Hope you don't mind. Really guys, cry us a river. Then go and fill out our all-purpose Butthurt Form, so we can get back to you promptly. Your feedback is important to us. Thanks.

Interestingly, one thing we noticed in the fallout of this catastrophic hack was that STRATFOR hired not one, but two outside consultants to try to bail their sorry asses out of the hellhole of a grave we dug them. Top identity theft protection? Professional security consultant? We'll see how that works out for you, if you ever dare to put your servers back online again. Until then, we'll be watching and waiting. And laughing, of course.

By the way, now that you have notified your customers of this massive security breach, we might have to pick up the pace of releasing peoples' credit card information.

Accordingly, we'll start the day after Christmas off right by dropping a third of the damn alphabet. How does a drop of 30,000 additional names, credit cards, addresses, phone numbers, and md5 hashed passwords sound? Sounds like a financial calamity to us. And just as the markets in the US are opening after the holiday weekend? Might be trouble.

But wait! That's not all folks. Oh hell n0. Tomorrow, we will be dropping another enormous dump on our next target: the entire customer database from an online military and law enforcement supply store. Bring the pain? Shit, we brought the motherfuckin' ruckus. You really trying to step this this?

Of course, this could all be averted. Have you given our comrade Bradley Manning his holiday feast yet, at a fancy restaurant of his choosing? Better make it happen, captain.

We'll end today's LulzXmas festivities by throwing in 25,000 tickets from the it.STRATFOR.com online support database. It's probably not as controversial as the contents of their private mail spools that we'll be dropping later, but perhaps it will shed some light on just how clueless this company really is when it comes to database security.

Stay tuned ...

###

http://ibhg35kgdvn7jvw.onion/lulzxmas/STRATFOR_full_d_m.txt.gz
https://rapidshare.com/#!/download|44t16|2444489251|STRATFOR_full_d_m.txt.gz|3255|R~7B8842ED6343CEAE67A23C094E131679|0|0
<http://depositfiles.com/files/t0hkk2wif>
<http://www.wupload.com/file/2625986107>
http://www.verzend.be/kx1n5oixnqn1/STRATFOR_full_d_m.txt.gz.html

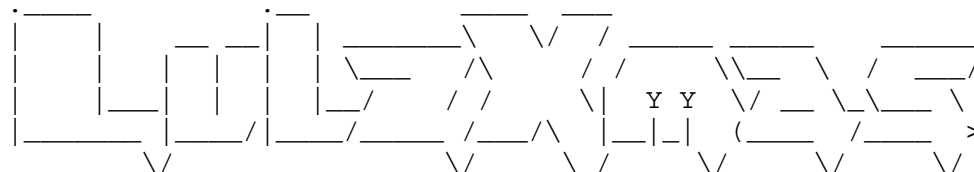
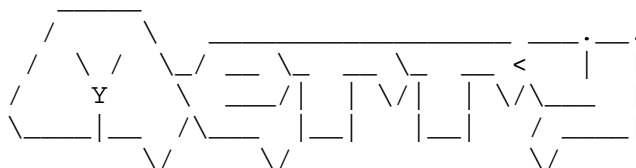
<http://ibhg35kgdvn7jvw.onion/lulzxmas/it.tar.gz>
<http://www.verzend.be/s8v8ccigl2hp/it.tar.gz.html>

<http://www.wupload.com/file/2626086337>
<http://depositfiles.com/files/ifnw3s34a>
<https://rapidshare.com/#!download|418134|3218055206|it.tar.gz|416|R~0|0|0|You%20need%20RapidPro%20to%20download%20more%20files%20from%20your%20IP%20address.%20%288d5611a9%29>

##

SPECIAL NOTICE: We are aware that there has been some confusion as to whether the STRATFOR hack is an "official" Anonymous operation, due to a ridiculous "Emergency Anonymous Press Statement" being circulated, undermining our work while also making baseless accusations that we frequently see perpetrated by agent provocateurs. Whether this is the work of malicious counter-intelligence,, some butthurt pacifists, or stratfor employees themselves is unknown. Unfortunately, some main stream news agencies have picked up on this statement, looking for any reason to highlight and exploit any potential "inner divisions" within Anonymous. However, there has been no such squabble or infighting regarding the STRATFOR target, or any other LulzXmas target for that matter. Anyone can claim to be Anonymous, but because of the inherent decentralized nature of Anonymous, without central top-down leadership, no individual is in a place to speak to the legitimacy of another individual or group's operation. Furthermore, our history of owning high profile targets as Anonymous has been well documented at the #antisecc embassy (<http://ibhg35kgdvn7jvw.onion/>) and is well known and respected within all Anon communities. Case closed.

Appendix II: AntiSec teaser 12/29 (legit)



#AntiSec™ (wtf? we hate copyright...)

> Can I haz candy?
> :3

Greetings Global Pirates! Having fun riding the waves of the Global Financial Meltdown? We sure are.

Did Bradley Manning get his fancy LulzXmas dinner yet?

hm... guess not.

Still trying to lock him up for life?
Still think we're just joking around?
That's OK. The time for talk is over.

So now let's talk... about cocks:
It's time to dump the full 75,000 names, addresses, CCs and md5 hashed passwords to every customer that has ever paid Stratfor. But that's not all: we're also dumping ~860,000 usernames, email addresses, and md5 hashed passwords for everyone who's ever registered on Stratfor's site.

> ...
> WTF?!?!
> Did you say 860,000 accounts????
> Did you notice 50,000 of these email addresses are .mil and .gov?
> fuck men...we're pretty much screwed up now...tin foil hat please here..
> yeah, for the lulz \:D/
> sounds illegal...
* /me phones police
> holy shit, like frontal crash at 180mph!!!

> :P
> lol xD

We almost have sympathy for those poor DHS employees and australian billionaires who had their bank accounts looted by the lulz (orly? i just fapped).

But what did you expect? All our lives we have been robbed blindly and brutalized by corrupted politicians, establishmentarians and government agencies sex shops, and now it's time to take it back.

We call upon all allied battleships, all armies from darkness, to use and abuse these password lists and credit card information to wreak unholy havok upon the systems and personal email accounts of these rich and powerful oppressors. Kill, kitties, kill and burn them down... peacefully. XD XD

Is that it? Oh hell n0.

On New Years Eve, there will be "noise demonstrations" in front of jails and prisons all over the world to show solidarity with those incarcerated.

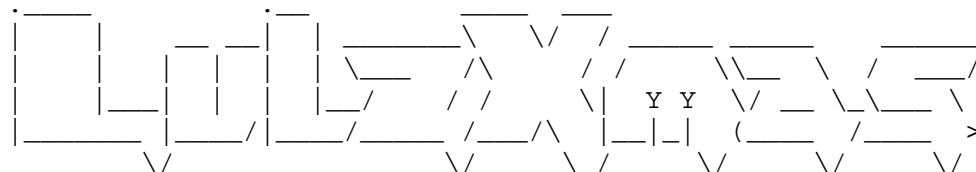
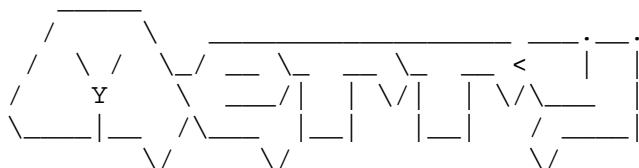
On this date, we will be launching our contributions to project mayhem

by attacking multiple law enforcement targets from coast to coast. That's right: once again we bout to ride on the po po. Problem, officer? umad?

Candiez, pr0n and cookies for LulzXmas:

http://ibhg35kgdvn7jvw.onion/lulzxmas/stratfor_full.tar.gz
<http://depositfiles.com/files/j87arfcpa>
http://www.verzend.be/odmmqjn6320d/stratfor_full.tar.gz.html
<http://www.wupload.com/file/2629492022>
<http://www.megaupload.com/?d=O5P03RXK>
https://rapidshare.com/#!download|877133|3374632512|stratfor_full.tar.gz|53875|R~E33E14C52C8795153D213502698C9141|0|0

Appendix JJ: AntiSec teaser 12/29



#AntiSec

Hall0 all!

>>>> more at >>>
<http://adf.ly/4SOhQ>

or

<http://j.gs/V8G>

 #AntiSec

Greetings fellow global pirates,

The halls are decked with lulz, AnonSanta's battle sleigh is re-filled, and lulz lizards worldwide are awaiting his arrival. Wait no longer, good denizens of the Internet, it's time for another round of the LulzXmas festivities.

But first, tell us, have you enjoyed the complete obliteration of Stratfor live on IRC and Twitter? We have. We also laughed heartily whilst these so-called protectors of private property scrambled desperately to recover the sensitive information of all the customers who they wronged by failing to use proper security precautions. Stratfor's Terms of Service stated, "Security: The personally identifiable information we collect about you is stored in limited access servers. We will maintain safeguards to protect the security of these servers and your personally identifiable

information." Yet Stratfor lazily stored credit card information and corresponding data unencrypted. Is the irony palpable yet?

Continuing the week long celebration of wreaking utter havoc on global financial systems, militaries, and governments, we are announcing our next target: the online piggie supply store SpecialForces.com. Their customer base is comprised primarily of military and law enforcement affiliated individuals, who have for too long enjoyed purchasing tactical combat equipment from their slick and "professional" looking website. What's that, officer? You get a kick out of pepper-spraying peaceful protesters in public parks? You like to recreationally taser kids? You have a fetish for putting people in plastic zip ties?

We had to contain our laughter when we saw these two "hacker proof" logos plastered on the SpecialForces.com website: "Scanned by GoDaddy.com: secured website" and "McAfee SECURE sites help keep you safe from identity theft, credit card fraud, spyware, spam, viruses, and online scams." Despite the almighty powers of GoDaddy and McAfee's logos and some reassuring words, SpecialForces.com was just no match for our hella wicked black hat voodoo. We have just one question before we continue: You mad, officer?

To be fair, at least SpecialForces.com DID store their customers' credit card information using blowfish encryption (unlike the global intelligence and security industry "professionals" at Stratfor, who apparently remain confused as to whether their customers' information was even encrypted or not). Nevertheless, our voodoo prevailed and we were quickly able to break back into the military supplier's server and steal their encryption keys. We then wrote a few simple functions to recover the cleartext passwords, credit card numbers, and expiration dates to all their customers' cards. That's how we roll.

In reality, for the past few months, we have been in possession of approximately 14,000 passwords and 8000 credit cards from SpecialForces.com. Unfortunately a former comrade leaked the password list early, and the full story on this owning will be told in our upcoming zine. Until then, feast upon one hell of a juicy text file.

We'll continue to have ourselves a merry LulzXmas at the expense of capitalist pigs, corrupt public officials and all those third parties who cater to the continued oligarchic elite worldwide. We are your secretaries, your janitors, your babysitters, your IT guys, your bus drivers, your maids, your hard-working, driven and determined fellow humans. We could be sitting next to you in a coffee shop, scanning your goods at a department store or even fixing your busted-ass computer. We are here to stay, and by now, you had better damn well expect us, cause the time for simple "lulz" is long past.

Oh, and by the way: Did Bradley Manning get his fancy holiday meal yet? Might want to hurry up before we hit even more targets.

```

http://ibhg35kgdvn7jvw.onion//lulzxmas/specialforces_full.txt.gz
<- orders/addresses/ccs
http://ibhg35kgdvn7jvw.onion//lulzxmas/specialforces_passwords.txt
<- just the passwords
http://wikisend.com/download/287544/specialforces.tar.gz    <- both
combined

```

[Sensitive/Personal Information Redacted]

We hope you've had a wonderful LulzXmas! For those who missed the past couple of days, have no fear. It's the season of giving and we still have so much to give to the people! Did you ever think that Obama was really, really creepy?

Well..he is!

And we have the documents to prove it.

Our only demand is that the United States Government releases BRADLEY MANNING. If not, you will only receive hell.

FULL COURT CASE: <http://www.filesonic.com/file/4254208425> CASE 7!!!!

Contains: More information leaks on people such as Hilary Clinton, Sarah Palin, and the NFL. Shows how much they have in the bank. Growth Hormones with bribery in the NFL. This leak is the mother load of all leaks. Everything you need to know about the GANGSTER GOVERNMENT running us is in it. The other court cases contain assaults Sarah Palin was involved in assaults against countless people (ie. stabbed some guy in the eye, sexual) (Court Cases: 1, 2, 3, 4, 5, 6, 8) SPREAD LIKE FUCKING HELL.

H0H0h0h0h0h0h0!!!! Merry LulzXmas to everyone and to everyone a good night!!

AND SONY...WE ARE WATCHING YOU. YOU'RE NEXT.

WE ARE ANONYMOUS.
 WE ARE LEGION.
 WE DO NOT FORGIVE.
 WE DO NOT FORGET.

Expect Us.

Appendix KK: CSLEA Hacked/Defaced or some rubbish, happy new year.

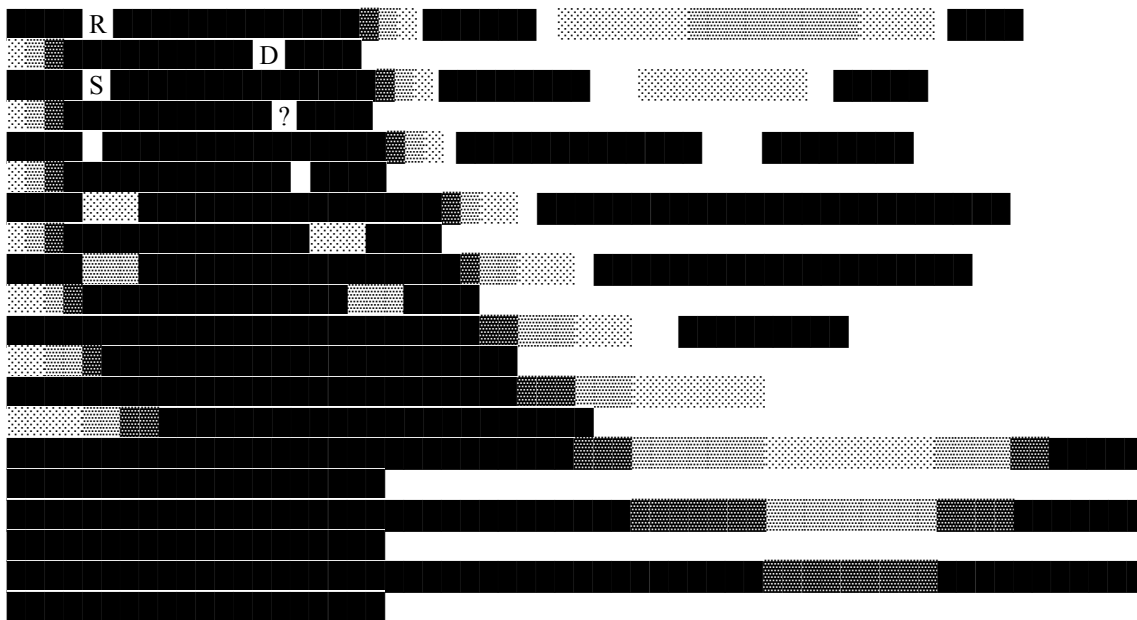
Some more crap hacked, here is a copy paste of the deface:







R
T
S
H
I
P
S
R
?
0
!
J
3
P
K
R
T
O
B
M
L
4
E
Y
M
H
3
M
O
F
O
F
N
I
C
N
E
E
R
W
?
Y
U
E
M
A
A



Hello comrades and thanks for joining us for the final phase of our cross country hacker crime spree, our contribution to pr0j3kt m4yh3m. We're still preparing the torrents, mail spools, as well as our final txt zine release which will surely bring humiliation and embarrassment to many white hats and sysadmins. But this New Years Eve, we bringing yall some party favors to keep you raging all night. Did you remember a month ago when the mayors and piggies across the US conspired to attack protesters in public parks? We sure do, so we have been planning a retaliatory raid of our own. Bring it, NDAA. Bring it, SOPA. We are snipers with one hell of a scope! Takin out a cop or two, they can't cope with us!

west coast - east coast

/*****
 CALIFORNIA LAW ENFORCEMENT ASSOCIATION - DEFACED AND DESTROYED BY
 ANTISEC
 *****/

Soundtrack to the Rev Track: The Coup - Five Million Ways to Kill a CEO
<http://www.youtube.com/watch?v=1Jotps9V4as>

I'm from the land where the Panthers grew
 You know the city and the avenue
 If you the boss we be smabbin through
 And we'll be grabbin' you
 To say "What's up with the revenue?"

Most everybody already knows that we don't like police very much. Shit, just about everybody hates them, everybody except for the rich and powerful who depend on their protection. But which state got the most blood on their hands? Well we already owned pigs in Texas and Arizona, and many many others; guess its time to ride on the California police.

From the murder of Oscar Grant, the repression of the occupation movement, the

assassination of George Jackson in San Quentin prison, the prosecution of our anonymous comrades in San Jose, and the dehumanizing conditions in California jails and prisons today, California police have a notorious history of brutality and therefore have been on our hitlist for a good minute now.

So we went ahead and owned the California State Law Enforcement Association (CSLEA.COM), defacing their website and giving out live backdoors. We dumped a few of their mail spools and forum databases, and we did get a few laughs out of reading years of their private email correspondence (such as CSLEA's Legislative and Police Liason Coby Pizzotti's convos with his girlfriend who calls him "doodle"). But what we were really after was their membership rosters, which included the cleartext password to 2500 of their members, guaranteeing the owmage of many more California pigs to come.

"But wait! Cops are people too! Part of the 99%!" orly? When these soulless traitors voluntarily chose to cross the picket line and side with the bosses and bureaucrats, they burned all bridges with working class. As the bootboys for capitalism they do not protect us, instead choosing to serve the interests and assets of the rich ruling class, the 1%. Many Occupiers are learning what many of us already know about the role of police in society when they violently attacked protesters occupying public parks. Now it's time to turn the table and start firing shots off in the right direction. Problem, officer?

Interestingly, CSLEA members have discussed some of our previous hacks against police targets, raising concern for the security of their own systems. However Ken deliberately made some rather amusing lies as to their security. He repeatedly denied having been hacked up until web hosts at stli.com showed him some of the backdoors and other evidence of having dumped their databases. We were reading their entire email exchange including when they realized that credit card and password information was stored in cleartext. This is about the time Ken changed his email password, but not before receiving a copy of the 'shopper' table which contained all the CCs. Too late, Ken.

In all fairness, they did make an effort to secure their systems after discovery of the breach. They changed a few admin passwords and deleted a few backdoors. Shut mail down for a few days. They also finally decided to set a root mysql password, but we got the new one: "vanguard". We noticed that you got rid of the credit card table, and most of the users in your database. Still haven't figured out how to safely hash passwords though: we really loved your change from 'redd555' to 'blu444'. Clever.

But we still had shell on their servers, and were stealthily checking out the many other websites on the server, while also helping ourselves to thousands of police usernames and passwords (it's how Special Agent Fred Baclagan at the California DOJ Cybercrimes Unit got humiliated last month). For two months, we passed around their private password list amongst our black hat comrades like it was a fat blunt of the dank shit, and now it's time to dump that shit for the world to use and abuse. Did you see that there were hundreds of @doj.ca.gov passwords? Happy new years!!

```

/*****
LIST OF SITES HOSTED BY CSLEA, NOW WIPED OFF THE NET !!!
*****/

```

Association of Conservation Employees (ACE)
Association of Criminalists-DOJ (AC-DOJ)

Association of Deputy Commissioners (ADC)
 Association of Motor Carrier Operations Specialists (AMCOS)
 Association of Motor Vehicle Investigators of California (AMVIC)
 Association of Special Agents-DOJ (ASA-DOJ)
 California Association of Criminal Investigators (CACI)
 California Association of Food and Drug Investigators (CAFDI)
 California Association of Fraud Investigators (CAFI)
 California Association of Regulatory Investigators and Inspectors (CARI)
 California Association of State Investigators (CASI)
 California Organization of Licensing Registration Examiners (COLRE)
 California Association of Law Enforcement Employees (CALEE)
 California Highway Patrol Public Safety Dispatchers Association (CHP-PSDA)
 Fire Marshal and Emergency Services Association (FMESA)
 Hospital Police Association of California (HPAC)
 Resource Protection Peace Officers Association (RPPOA)
 State Employed Fire Fighters Association (SEFFA)

/*****
 OUR FAVORITE SECTION IN ANY GOOD HACKING ZINE - EXPOSING THE CLUELESSNESS
 OF
 WHITE HAT SYSADMINS IN THEIR OWN WORDS. OUR STORY BEGINS IN AUGUST WHEN
 CSLEA
 TAKES NOTICE OF OUR PREVIOUS ATTACKS ON POLICE SYSTEMS. IS ANYONE SAFE?!
 *****/

[Sensitive/Personal Information Redacted]

/*****
 AFTER THE BART AND SHERIFFS HACKS, WEBMASTER KEN FAIR IS ASKED WHETHER
 CSLEA'S
 SYSTEMS ARE SECURE. BUT CAN HIS REASSURING LIES PROVIDE ENOUGH PROTECTION??
 *****/

[Sensitive/Personal Information Redacted]

/*****
 MEMBERSHIP DATA COMPLETELY SEPARATE FROM THE WEBSITE? ALL DATA IS
 ENCRYPTED?
 IF ATTACKED, YOU CAN ALWAYS UNPLUG? SOUNDS LIKE AN AIRTIGHT SECURITY PLAN.
 *****/

[Sensitive/Personal Information Redacted]

/*****
 ARE THEY ON TO US? FALSE ALARM. JUST SOME "FIREWALL SCANS FROM CHINA AND
 RUSSIA"
 *****/

[Sensitive/Personal Information Redacted]

/*****
 LOOKS LIKE THEY DISCOVERED OUR PRIVATE STASH. THE JIG IS UP. JUST ONE LAST
 MESSAGE BEFORE KEN FINALLY DECIDED TO CHANGE HIS EMAIL PASSWORD...

*****/

[Sensitive/Personal Information Redacted]

/*****

LOLOLOL SO MUCH FOR "ENCRYPTED MEMBER DATA". DAMN KEN YOU DID HALF THE WORK

FOR US. AND DESPITE BEING AWARE OF THE BREACH, YOU STILL COULD NOT KEEP US OUT.

ON TO THE NEXT TARGET.... NEW YORK POLICE CHIEFS, OWNED AND EXPOSED !!!

*****/

Soundtrack to the Rev #3: Cop Killer by Ice-T

<http://www.youtube.com/watch?v=p5gRIud57jQ>

I got my black shirt on.
I got my black gloves on.
I got my ski mask on.
This shit's been too long.

I got my twelve gauge sawed off.
I got my headlights turned off.
I'm 'bout to bust some shots off.
I'm 'bout to dust some cops off.

I'm a cop killer, better you than me.
Cop killer, fuck police brutality!
Cop killer, I know your family's grieving, (fuck 'em!)
Cop killer, but tonight we get even, ha ha.

For our next owning we bring you multiple law enforcement targets in the state of New York, who has been on our crosshairs for some time due to their brutal repression of Occupy Wall Street. We also want to bring attention to the 1971 riots at Attica where in response to the murder of George Jackson, convicts took over the prison, demanding humane living conditions. It is in this same spirit of cross-country solidarity that we attacked police targets in NY.

We're dropping the md5-hashed passwords and residential addresses for over 300 Police Chiefs in the state of New York. We are also sharing several private mail spools of a few NY police chiefs. While most of the contents of these emails involve boring day to day office work and blonde joke chain emails, there were also treasure troves of embarrassing personal information as well as several "For Official Use Only" and "Law Enforcement Sensitive" documents discussing police methods to combat protesters.

[Sensitive/Personal Information Redacted]

There were also many parolee/probationers but the thought of betraying our comrades under the gun of the prison industrial complex never crossed our minds. But how about sum moar private police documents?? We dropped these on Bradley Manning's birthday:

* (U//FOUO) Law Enforcement at Risk for Harassment and Identity Theft through 'Doxing' FBI BULLETIN Cyber Intelligence Section

* (U//FOUO) Awareness, Detection, and Mitigation of Cyber Threats and Attacks

- * (U//FOUO) Environmental Extremism: Potential for Increased Criminal Activity
- * (FOUO/LES): LA Intelligence Bulletin: Social Networking in State Prisons"
- * (LES) DEA Intel Brief Gmail Security Features

// THATS ALL FOR NOW KIDDIES! EXPECT A BADASS ZINE AND TORRENT COMING SOON!!!!!!

If you didn't dig it then then you better dig it now. We are calling upon all allied battleships to rise up and make some mayhem. NDAA/PIPA/SOPA for real? The internet is ours for the taking, and we will destroy every corporation and government that attempts to stand in our way.

#####

download torrent: <http://thepiratebay.se/user/antisecurity>
 browse on tor hidden services: <http://ibhg35kgdvn7jvw.onion/puckettfaraj>
 follow for teh lulz: <http://twitter.com/#!/anonymousirc>

defaced: <http://www.puckettfaraj.com>
<http://www.militaryselfhelp.net>
<http://www.bpdnews.com>

greetings to our comrades: #codehack and GHS, team redhack in turkey, syrian hackers, all and all allied battleships in this great cyberwar for great justice. keep crackin

#####

[Sensitive/Personal Information Redacted]

chiefingredient.com: you can forget about hosting puckettfaraj.com from now on... we already wiped your shit... we have your mailspools and all your clients... don't make us do this!

[Sensitive/Personal Information Redacted]

#####

BOSTON POLICE DEPARTMENT: OWNING YOU ALL OVER AGAIN FOR THE FIRST TIME
 #####

[Sensitive/Personal Information Redacted]

And just think, as you're reading this statement, we are already sailing into new waters with our allied shiny epic lulzfleet. Don't fret, we've already prepared treasure chests of stolen booty, diamonds and pizzas for our next raid.

We are s(h)itting on hundreds of rooted servers getting ready to drop all your mysql dumps, child pr0n and mail spools (to be honest, fucking too much for us to read on our own, so we swap with all criminal underground allies for sex and 0days). Oh wait, what's that? Your passwords? Addresses? Your precious bank accounts? Even your online dating details?! (yep, We know you're cheating on your...well, we won't get into that here. Yet.)

Yep, we know all about you. All of your little secrets will be laid bare for the world to see. So, how does it feel to be the one spied on?

Oh, eat cock now. Kthxbai. :D

THE UNKNOWN: A Poem

As we know,
There are known knowns.
There are things we know we know.
We also know
There are known unknowns.
That is to say
We know there are some things
We do not know.
But there are also unknown unknowns,
The ones we don't know
We don't know.

D.H.Rumsfeld

(American poet and super-sexy drag queen)

Herp derp derp, so what is ACTA? ACTA is the Anti-Counterfeiting Trade Agreement, a new intellectual property enforcement treaty being negotiated by the US, EU, Switzerland, Japan, Australia, the Republic of Korea, New Zealand, Mexico, Jordan, Morocco, Singapore, the UAE, and Canada.

Why should you care about ACTA? Negotiated in secret and without public input, the treaty will have a *very* broad scope on regulating intellectual property on the Internet and creates new tools targeting "Internet distribution and information technology."

Do you guise just hate all laws that are named with catchy acronyms? No. We just hate ACTA (SOPA too, but you already knew this). ACTA was negotiated in extreme secrecy by the world's top wealthiest and powerful countries - this throws into question the entire act's legitimacy. It raises substantial questions of governmental transparency as well as democratic accountability, with participating leaders deliberately bypassing their constituents by participating in this shady, backroom process.

Because ACTA is an international agreement binding under the general principles of international law, national legislatures would be unable to change domestic copyright law if they eventually feel the ACTA regulations to be too strict. A country would have to literally withdraw from the treaty first, a historical rarity.

There is no doubt that ACTA is more dangerous and detrimental to our rights than SOPA. ACTA will further spread the contagion of stricter copyright enforcement worldwide, at the expense of our essential liberties and basic freedoms of speech, expression and privacy.

TL;DR: ACTA is a downright shitty act. We must kill it. With fire.

can i haz candiez?
:3

WHEREZ TEH HAXLOG!?!?

We are Legion
We do not forgive
We do not forget
Expect Us

[Sensitive/Personal Information Redacted]

// A FEW MORE SHITTY DRUPAL SITES TO ADD TO THE LIST OF ROASTED .GOV SERVERS

[Sensitive/Personal Information Redacted]

YOU STILL WANT TO PASS ACTA? I AINT A KILLER BUT DON'T PUSH ME

LITERATURE CITED

- 2600: The Hacker Quarterly. (1999, January 7). LoU cyberwar press release: international coalition of hackers denounce declaration of war [Press release]. Retrieved from <http://www.2600.com/>
- 2600: The Hacker Quarterly. (2012, April 3). Volume 1 of 2600 now online - drm free - in kindle, nook, and pdf formats. Retrieved from <http://www.2600.com/>
- Anderson, N. (2011). CloudFlare named "tech pioneer" after protecting LulzSec website. *ArsTechnica*. Retrieved from <http://http://arstechnica.com>
- AntiSec (2011a, July 27). A message to PayPal, its customers, and our friends [Press release]. Retrieved from <http://pastebin.com/LAykd1es>
- AntiSec (2011b, December 26). AntiSec teaser 12/26 [Press release]. Retrieved from <http://pastebin.com/q5kXd7Fd>
- AntiSec (2011c, December 29). AntiSec teaser 12/29 [Press release]. Retrieved from <http://pastebin.com/QSX0XYiD>
- AntiSec (2011d, December 29). AntiSec teaser 12/29 (legit) [Press release]. Retrieved from <http://pastebin.com/f7jYf5Wd>
- AntiSec (2011e, June 29). Antisec01 [Press release]. Retrieved from <http://thepiratebay.se/torrent/6502765>
- AntiSec (2012f, February 3). Boston Police Department Defacement [Press release]. Retrieved from <http://zone-h.org/mirror/id/16859089>

AntiSec (2011g, June 29). Chinga La Migra II [Press release]. Retrieved from

http://thepiratebay.se/torrent/6504060/Chinga_La_Migra_II

AntiSec (2011h, July 1). Chinga La Migra III [Press release]. Retrieved from

http://thepiratebay.se/torrent/6508513/Chinga_La_Migra_III

AntiSec (2011i, August 10). Corrupt Brazil (Satiagraha) [Press release]. Retrieved from

[http://thepiratebay.se/torrent/6593891/Corrupt_Brazil_\(Satiagraha\)](http://thepiratebay.se/torrent/6593891/Corrupt_Brazil_(Satiagraha))

AntiSec (2011j, December 31). CSLEA Hacked/Defaced or some rubbish, happy new

year [Press release]. Retrieved from <http://pastebin.com/gZ9pm207>

AntiSec (2012k, February 17). FTC JACKHAMMERBUTTRAEPD BY ANONYMOUS

ANTISEC [Press release]. Retrieved from <http://pastebin.com/2qfEqS1p>

AntiSec (2011l, July 8). Fuck FBI Friday II: IRC Federal [Press release]. Retrieved from

http://thepiratebay.se/torrent/6525567/Fuck_FBI_Friday_II__IRCFederal

AntiSec (2011m, July 29). Fuck FBI Friday III: ManTech Mayhem [Press release].

Retrieved from

http://thepiratebay.se/torrent/6571301/Fuck_FBI_Friday_III__ManTech

AntiSec (2011n, August 19). Fuck FBI Friday IV – Vanguard Defense Industries [Press

release]. Retrieved from

http://thepiratebay.se/torrent/6615674/Fuck_FBI_Friday_IV__Vanguard_Defense_Industries

AntiSec (2011o, November 18). Fuck FBI Friday V: IACS Cybercrime Investigators

Owned [Press release]. Retrieved from

http://thepiratebay.se/torrent/6827936/Fuck_FBI_Friday_V__IACIS_Cybercrime_Investigators_Owned

- AntiSec (2011p, November 18). International Association of Chiefs of Police Owned [Press release]. Retrieved from http://thepiratebay.se/torrent/6828076/International_Association_of_Chiefs_of_Police_Owned
- AntiSec (2011q, July 11). Military Meltdown Monday: Mangling Booz Allen Hamilton [Press release]. Retrieved from <http://thepiratebay.se/torrent/6533009>
- AntiSec (2012r, February 3). Puckett & Faraj Lawfirm – Hadidtha [Press release]. Retrieved from <http://zone-h.org/mirror/id/16859533>
- AntiSec (2011s, August 6). Shooting Sheriffs Saturday [Press release]. Retrieved from http://thepiratebay.se/torrent/6587214/Shooting_Sherriffs_Saturday
- AntiSec (2011t, September 2). Texas Takedown Thursday: Chinga La Migra IV [Press release]. Retrieved from http://thepiratebay.se/torrent/6647306/Texas_Takedown_Thursday__Chinga_La_Migra_IV
- AntiSec (2011u, July 4). Turkish Takedown Thursday [Press release]. Retrieved from http://thepiratebay.se/torrent/6521231/Turkish_Takedown_Thursday
- Arthur, C. (2012, June 15). Alleged LulzSec hacker may escape extradition to US. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Arthur, C., & Gallagher, R. (2011). LulzSec IRC leak: the full record. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Associated Press. (2011, July 22). 4 Dutch Men Suspected of Hacking Attacks Released. *ABC News*. Retrieved from <http://abcnews.go.com/>

- Associated Press. (2012). Two LulzSec hackers plead guilty in Britain. *The New York Times*. Retrieved from <http://www.nytimes.com/>
- Associated Press. (2012, February 28). 25 Suspected Hackers Arrested in International Raids. *The New York Times*. Retrieved from <http://www.nytimes.com/>
- Arizona Department of Public Safety. (2011a). DPS email system compromised [Press release]. Retrieved from <http://www.azdps.gov/Media/News/View/?p=315>
- Arizona Department of Public Safety. (2011b). Arizona Department of Public Safety (DPS) Statement regarding latest Cyber Intrusion [Press release]. Retrieved from <http://www.azdps.gov/Media/News/View/?p=318>
- Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology*, 4(1&2), 643-656.
- Ball, J. (2012). By criminalising online dissent we put democracy in peril. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Ball, J., & Arthur, C. (2011, July 21). LulzSec: we won't public News International emails. *The Guardian*. Retrieved from <http://www.guardian.co.uk>
- Bilton, N., & Stelter, B. (2011). Sony says PlayStation hacker got personal data. *The New York Times*. Retrieved from <http://www.nytimes.com>
- Bray, C. (2012). Chicago Man Pleads Not Guilty to LulzSec Charges [Web log post]. *The Wall Street Journal*. Retrieved from <http://blogs.wsj.com/law/2012/05/14/chicago-man-pleads-not-guilty-to-lulzsec-charges/>
- Brenner, S.W. (2007). "At light speed": attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law & Criminology*, 97(2). Retrieved from <http://home.heinonline.org/>

- Bright, P. (2011, June 14). Titanic Takeover Tuesday: LulzSec's busy day of hacking escapades. Retrieved from <http://www.arstechnica.com>
- Burns, J. F. (2009, July 31). Hacker's Extradition to U.S. More Likely. *The New York Times*. Retrieved from <http://www.nytimes.com/>
- Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers: the science of criminal profiling as applied to the world of hacking*. CRC Press.
- Cisco. (2012, May 30). Cisco Visual Networking Index: Forecast and Methodology, 2011–2016. Retrieved from <http://www.cisco.com/>
- Cisco. (2012, May 30). The Zettabyte Era. Retrieved from <http://www.cisco.com/>
- Cohen, F. (1984). *Computer Viruses - Theory and Experiments*. Retrieved from <http://all.net/books/virus/index.html>
- Coleman, E. G. & Golub, A. (2008). Hacker practice: moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8, 255-277.
doi: 10.1177/1463499608093814
- Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).
- Conway, Maura (2007) Cyberterrorism: hype and reality. In L. Armistead (Ed.), *Information warfare: separating hype from reality* (pp. 73-93). Washington, D.C.: Potomac Books.
- CoudFlare. (2011, June 26). On lulzsec, censorship & cloudflare [Web log post]. Retrieved from <http://blog.cloudflare.com/58611873>
- Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (1984).

Cybersecurity: Responding to the Threat of Cyber Crime and Terrorism: Statement

Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism.

112th Cong. (2011) (testimony of Gordon Snow, Assistant Director of the FBI's Cyber Division). Retrieved from <http://www.fbi.gov/news/testimony/>

Cyberterrorism: Hearing before the Special Oversight Panel on Terrorism of the

Committee on Armed Services, United States House of Representatives, 106th

Cong. (2000) (testimony of Denise Denning). Retrieved from

<http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

DAmico, M. L. (1999, January 13). Hackers spar over cyber war on Iraq, China. *CNN*.

Retrieved from <http://www.cnn.com>

Denning, D. (2001). Activism, hacktivism, and cyberterrorism: the internet as a tool for

influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and*

netwars, the future of terror, crime, and militancy (pp. 239-288). Santa Monica:

Rand Corporation.

Denning, D. (2007). A view of cyberterrorism 5 years later. In K. E. Himma (Ed.),

Internet security: hacking, counterhacking, and society (pp. 123-139). Location:

Jones & Bartlett Publishing

Dodd, V., & Halliday, J. (2011, June 22). Teenager Ryan Clearly charged over lulzsec

hacking. *The Guardian*. Retrieved from <http://www.guardian.co.uk>

Dodd, V., Halliday, J., & Arthur, C. (2011). Hunt for hackers of US government sites

leads to Essex teenager's bedroom. *The Guardian*. Retrieved from

<http://www.guardian.co.uk>

- Dowty, D. (2012). 'Anonymous' hackers shut down Syracuse police website. *The Post-Standard*. Retrieved from <http://www.syracuse.com/news/>
- Electronic Communications Privacy Act, 18 U.S.C. § 2510-22 (1986).
- Ernesto. (2011, June 28). The Pirate Bay Deletes LulzSec Loot [Web log post]. Retrieved from <http://torrentfreak.com/the-pirate-bay-deletes-lulzsec-loot-by-mistake-110628/>
- Gallagher, R., Arthur, C. (2011, June 24). Inside LulzSec: Chatroom logs shine a light on the secretive hackers. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Geuss, M. (2012, April 5). Accused LulzSec member pleads guilty to hacking sony. *ArsTechnica*. Retrieved from <http://www.arstechnica.com>
- Gordon, S., & Ford, R. (2003). Cyberterrorism? [White paper]. Retrieved from the Symantec website at: www.symantec.com
- Graves, K. (2010). *CEH: certified ethical hacker study guide*. (1 ed.). Indianapolis: Sybex.
- Halbert, D. (1997). Discourses of Danger and the Computer Hacker. *The Information Society*, 13, 361-374. doi:10.1080/019722497129061
- Halbert, D. (2006). Discourse of danger and the computer hacker. *The Information Society: An International Journal*, 13(4), 361-374. doi: 10.1080/019722497129061
- Halliday, J. (2011a). LulzSec: the members and the enemies. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Halliday, J. (2011b). Police arrest five over Anonymous WikiLeaks Attacks. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>

- Halliday, J., Arthur, C., & Ball, J. (2011, July 27). LulzSec hacking suspect 'Topiary' arrested. *The Guardian*. Retrieved from <http://www.guardian.co.uk>
- Hampson, N. C.N. (2012). Hactivism, anonymous & a new breed of protest in a networked world. *Boston College International and Comparative Law Review*, 35(2), 511-542. Retried from <http://lawdigitalcommons.bc.edu/iclr/>
- Harmon, A. (1998, October 31). 'Hacktivists' of All Persuasions Take Their Struggle to the Web. *The New York Times*. Retrieved from <http://www.nytimes.com>
- Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2009). *Gray hat hacking: The ethical hackers handbook*. (3rd ed.). New York: McGraw-Hill.
- Harris, P. (2011, July 19). FBI targets Anonymous hacking group in series of raids on homes. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>
- Himma, K.E. (2007). Hacking as politically motivated digital civil disobedience: is hacktivism morally justified?. In K. E. Himma (Ed.), *Internet Security: Hacking, Counterhacking, and Society* (pp. 73-98). Location: Jones & Bartlett Publishing
- Holt, T.J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review*, 28(4), 466-481.
doi:10.1177/0894439309351344
- Hwang, T. (2010). WikiLeaks and the internet's long war. *The Washington Post*. Retrieved from <http://www.washingtonpost.com>
- Infragard. (2012). About Infragard. Retrieved from <http://www.infragard.net/about.php>

Information sharing in the era of WikiLeaks: balancing security and collaboration:

Hearing before the Committee on Homeland Security and Governmental Affairs,

United States Senate. 112th Cong. (2011) (testimony of Patrick Kennedy)

Retrieved from <http://www.state.gov>

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics* ,33(1), 159-174.

Levy, S. (2010). *Hackers: Heroes of the computer revolution*. Sebastopol, CA: O'Reilly Media, Inc.

LulzSec (2011a, June 25). 50 Days of Lulz [Press release]. Retrieved from <http://pastebin.com/1znEGmHa>

LulzSec (2011b, May 15). [ATM leak] ~LulzSec [Press release]. Retrieved from <http://pastebin.com/myPTr0aE>

LulzSec (2011c, May 13). [LulzSec] Fox.com leakage phase 0/1/2/3 [Press release]. Retrieved from <http://pastebin.com/Q2xTKU2s>

LulzSec (2011d, June 13). Bethesda Internal Data [Press release]. Retrieved from http://thepiratebay.se/torrent/6467131/Bethesda_internal_data

LulzSec (2011e, June 24). Chinga La Migra [Press release]. Retrieved from http://thepiratebay.se/torrent/6490796/Chinga_La_Migra

LulzSec (2011f, June 5). Fuck FBI Fridayâ,,ç (FFF) [Press release]. Retrieved from [http://thepiratebay.se/torrent/6446763/Fuck_FBI_FridayA_a__A__\(FFF\)](http://thepiratebay.se/torrent/6446763/Fuck_FBI_FridayA_a__A__(FFF))

LulzSec (2011g, June 17). LulzSec - 1000th tweet statement [Press release]. Retrieved from <http://pastebin.com/HZtH523f>

LulzSec (2011h, June 20). LulzSec 2011 census released [Press release]. Retrieved from

<http://pastebin.com/K1nerhk0>

LulzSec (2011i, May 30). LulzSec Hack PBS.ORG [Press release]. Retrieved from

<http://pastebin.com/B3gmw5NS>

LulzSec (2011j, May 23). LulzSec hates Sony too [Press release]. Retrieved from

<http://pastebin.com/NyEFLbyX>

LulzSec (2011k, June 19). Operation Anti-Security [Press release]. Retrieved from

<http://pastebin.com/9KyA0E5v>

LulzSec (2011l, June 2). Sownage [Press release].

<http://thepiratebay.se/torrent/6443601/Sownage>

LulzSec (2011m, June 6). Re: "LulzSec Exposed" [Press release]. Retrieved from

<http://pastebin.com/yut4P6qN>

LulzSec (2011n, June 4). RE: Unveillance [Press release]. Retrieved from

<http://pastebin.com/AjVd0L9E>

LulzSec (2011o, June 21). Snitches getting various stitches [Press release]. Retrieved

from <http://pastebin.com/MBEsm5XQ>

LulzSec (2011p, June 6). Sownage 2 [Press release]. Retrieved from

http://thepiratebay.se/torrent/6449737/Sownage_2

LulzSec (2011q, May 11). Untitled [Fox Hack] [Press release]. Retrieved from

<http://pastebin.com/DsafwNZz>

LulzSec (2011r, May 7). X Factor Leaked Contestants Database [Press release].

Retrieved from

http://thepiratebay.se/torrent/6372763/X_Factor_Leaked_Contestants_Database

- M.G. (2011, June 3). Once More Unto the Breach [Web log post]. Retrieved from <http://www.economist.com/node/21518659>
- Manach, J. M. (2012, January 31). ‘They searched everywhere for an anonymous mask’ [Web log post]. Retrieved from <http://owni.eu/2012/01/31/dcri-france-anonymous-pierrick-goujon-triskel-greenrights/>
- Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: toward a hacktivist ethic. *Computers and Society*, 30(2), 14-19. doi: 10.1145/572230.572232
- Mansfield-Devine, S. (2011). Hacktivism: assessing the damage. *Network Security*, 2011(8), 5-13. doi: 10.1016/S1353-4858(11)70084-8
- Markoff, J. (2011, October 5). Apple’s Visionary Redefined Digital Age. *The New York Times*. Retrieved from <http://www.nytimes.com/>
- McAfee Labs (2011, December 28). *2011 Threats Predictions*. Retrieved from <http://www.mcafee.com>
- McAleavey, K. (2011, June 27). Warning: original “50 days of lulz” payload is infected [Web log post]. Retrieved from <http://infosecisland.com/blogview/14784-Warning-Original-50-Days-of-Lulz-Payload-is-Infected.html>
- McCracken, E. (2007, December 30). Dial-Tone Phreak. *The New York Times*. Retrieved from <http://www.nytimes.com/>
- McLaurin, J. (2012). Making cyberspace safe for democracy: the challenge posed by denial-of-service attacks. *Yale Law and Policy Review*, 30(1), 211-254.
- Mizrach, S. (1997). Is there a Hacker Ethic for 90s Hackers? Retrieved from <http://www2.fiu.edu/~mizrachs/hackethic.html>
- New York Times Co. v. United States, 403 U.S. 713 (1971)

Official DEF CON FAQ v0.95. Retrieved July, 2012, from

<https://www.defcon.org/html/links/dc-faq/dc-faq.html>

Olson, P. (2012). *We are anonymous: inside the hacker world of lulzsec, anonymous, and the global cyber insurgency*. Little, Brown and Company.

Poeter, R. (2011). Who is LulzSec?. *PC Magazine*. Retrieved from

<http://www.pcmag.com/slideshow/story/266414/who-is-lulzsec>

Raymond, E. (1996). *The new hacker's dictionary*. (3rd ed.). The MIT Press.

Red Hat, Inc. (2011). Red Hat Enterprise Linux 6: Security Guide A Guide to Securing

Red Hat Enterprise Linux (3 ed.). Retrieved from <https://access.redhat.com/>

Ronczkowski, M. (2007). *Terrorism and organized hate crime, intelligence gathering, analysis, and investigations*. CRC Press.

Samuel, A. W. (2004). *Hacktivism and the future of political participation* (Doctoral dissertation, Harvard University). Retrieved from

<http://www.alexandrasamuel.com>

Satter, R. (2011). FBI partner InfraGard hacked, passwords stolen, LulzSec claims credit.

The Huffington Post. Retrieved from <http://www.huffingtonpost.com/>

Sengupta, Somini. (2011). 16 Arrested as F.B.I. Hits the Hacking Group Anonymous.

The New York Times. Retrieved from <http://www.nytimes.com>

Singel, R. (2012). Sabu gets 6-month sentencing delay for continuing to help feds [Web

log post]. *Wired*. Retrieved from <http://www.wired.com/threatlevel/>

Sony Computer Entertainment America LLC v. Hotz et al

- Srnka, K.J., & Koeszegi, S.T. (2007). From words to numbers: how to transform qualitative data into meaningful quantitative results. *Schmalenbach Business Review*, 59, 29-57. Retrieved from <http://www.sbr-online.de>
- Steele, G. (1983). *The hacker's dictionary*. HarperCollins.
- Sterling, B. (1992). The hacker crackdown: law and disorder on the electronic frontier. Retrieved from <http://www.mit.edu/hacker/hacker.html>
- Sterner, E. (2011). WikiLeaks and cyberspace cultures in conflict. Retrieved from the George C. Marshall Institute website: <http://www.marshall.org/pdf/materials/931.pdf>
- Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, Law and Social Change*, 46(4-5), 223-238. doi: 10.1007/s10611-007-9061-9
- Stryker, C. (2011). *Epic win for anonymous: How 4chan's army conquered the web*. (1st ed. ed.). New York: The Overlook Press.
- Talihärm, A.M. (2010). Cyberterrorism: in theory or in practice?. *Defence Against Terrorism Review*, 3(2), 59-73. Retrieved from the Center of Excellence-Defence Against Terrorism website: <http://www.coedat.nato.int/>
- Tavani, H.T. (2005). The impact of the internet on our moral condition: do we need a new framework of ethics?. In R. Cavalier (Ed.), *The Impact of the Internet on our Moral Lives* (pp. 215-237). Albany: SUNY Press.
- The Jargon File 4.4.7. (2012). Retrieved from <http://www.catb.org/~esr/jargon/>
- Tremlett, G. (2011, June 3). Spanish police website knocked offline after hacking suspects arrested. *The Guardian*. Retrieved from <http://www.guardian.co.uk/>

United States Department of Homeland Security, National Cybersecurity and Communications Integration Center. (2011a). Anonymous and associated Hacker Groups developing and deploying New Cyber Attack tools [Bulletin].

United States Department of Homeland Security, National Cybersecurity and Communications Integration Center. (2011b). "Anonymous" and associated hacker groups continue to be successful using rudimentary exploits to attack public and private organizations [Bulletin].

United States Department of Homeland Security, National Cybersecurity and Communications Integration Center. (2011c). "Anonymous" upcoming US operations, impact, and likelihood [Bulletin].

United States Department of Homeland Security, National Cybersecurity and Communications Integration Center. (2011d). Hacktivist group targets U.S. and foreign networks [Bulletin].

United States Department of Justice, Federal Bureau of Investigation. (2011). Anonymous' Participation in "Day of Rage" Protest May Coincide with Cyber Attack [Intelligence bulletin].

United States Department of Justice, Federal Bureau of Investigation, Los Angeles Division. (2011). Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems [Press release]. Retrieved from <http://www.fbi.gov/losangeles/press-releases/>

- United States Department of Justice, Federal Bureau of Investigation, Los Angeles Division. (2012). Second Member of Hacking Group LulzSec Arrested for 2011 Intrusion of Sony Pictures Computer Systems [Press release]. Retrieved from <http://www.fbi.gov/losangeles/press-releases/>
- United States Department of Justice, Office of Public Affairs. (1995). Fugitive Computer Hacker Arrested in North Carolina [Press release]. Retrieved from http://www.justice.gov/opa/pr/Pre_96/February95/89.txt.html
- United States Department of Justice, United States Attorney's Office, District of New Jersey. (2011). Former AT&T Contractor Arrested, Charged With Unauthorized Access Of Servers [Press release]. Retrieved from <http://www.justice.gov/usao/nj/>
- United States Department of Justice, United States Attorney's Office, Central District of California. (2011). Connecticut man allegedly affiliated with anonymous arrested on charges of attacking and shutting down Gene Simmons' website [Press release]. Retrieved from <http://www.justice.gov/usao/cac/>
- United States Department of Justice, United States Attorney's Office, Northern District of California. (2011a). Charges in distributed denial of service attack against Santa Cruz county website [Press release]. Retrieved from <http://www.justice.gov/usao/can/>
- United States Department of Justice, United States Attorney's Office, Northern District of California. (2011b). Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks [Press release]. Retrieved from <http://www.justice.gov/usao/can/>

United States Department of Justice, United States Attorney's Office, Southern District of New York. (2012). Six hackers in the United States and abroad charged for crimes affect over one million victims [Press release]. Retrieved from <http://www.justice.gov/usao/nys/>

United States v. Collins, Cooper, Covelli, Downey, Haefer, Husband, Kershaw, Miles, Murphy, Phillips, Puglisi, Sullivan, Valenzuela, and Vo, Indictment. Cr. 11-004471 (N.D. Ca. 2011). Retrieved from [http://www.justice.gov/usao/can/news/2011/docs/Indictment 7 19 11.pdf](http://www.justice.gov/usao/can/news/2011/docs/Indictment%207%2019%2011.pdf)

United States v. Hector Xavier Monsegur, Information, S1 11 Cr. 666 (LAP) (S.D. N.Y. 2012). Retrieved from <http://www.justice.gov/usao/nys/pressreleases/March12/hackers/monsegurhectorxavierinformation.pdf>

United States v. Donncha O'Cearrbhail, Complaint, 12 Mj. 609(S.D. N.Y. 2012). Retrieved from <http://www.justice.gov/usao/nys/pressreleases/March12/hackers/ocearrbhaildonnchacomplaint.pdf>

United States v. Ryan Ackyord, Jake Davis, Darren Martin, and Donncha O'Cearrbhail, Indictment, 12 Cr. 185 (S.D. N.Y. 2012). Retrieved from <http://www.justice.gov/usao/nys/pressreleases/March12/hackers/ackroydetalindictment.pdf>

United States v. Jeremy Hammond. Complaint. (S.D. N.Y. 2012). Retrieved from <http://www.justice.gov/usao/nys/pressreleases/March12/hackers/hammondjeremycomplaint.pdf>

United States v. Ryan Ackyord, Jake Davis, Darren Martyn, Donncha O'Cearrbhail, and Jeremy Hammond. Indictment. S1 12 Cr. 185 (LAP) (S.D. N.Y. 2012).

United States v. John Doe, 11 Cr. 666 (LAP) (S.D. N.Y. 2011)

- United States v. Ryan Cleary. Indictment. CR12-0561 (C.D. Ca. 2012).
- United States v. I. Lewis Libby, 429 F.Supp.2d 1 (D.D.C. 2006).
- United States v. Manning, Bradley E., PFC (2011).
- United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
- United States v. Riggs, 743 F.Supp. 556 (N.D. Ill. 1980)
- United States v. Rivera, CR No. 12-798-JAK (C.D. Ca. 2012).
- Sony Computer Entertainment America LLC v. Hotz et al., Case 3:11-cv-00167. (N.D. Ca. 2011).
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107 –56, 115 Stat. 272 (2001).
- Verini, J. (2010, November 10). The Great Cyberheist. *The New York Times*. Retrieved from <http://www.nytimes.com>
- Verizon. (2012). The 2012 Data Breach Investigations Report. Retrieved from <http://www.verizonbusiness.com/>
- Weimann, G. (2005). Cyberterrorism: the sum of all fears?. *Studies in Conflict & Terrorism*, 28(2), 129-149. doi: 10.1080/10576100590905110
- White House (2011). International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- Wilson, C. (2003). *Computer attack and cyber terrorism: vulnerabilities and policy issues for congress* (CRS report RL32114).

- Wilson, C. (2005, updated). *Computer attack and cyber terrorism: vulnerabilities and policy issues for congress* (CRS report RL32114).
- Wilson, C., & Rollins, J. (2007) *Terrorist capabilities for cyberattack: overview and policy issues* (CRS report RL33123)
- Woodward, B. (2009, September 21). McChrystal: More Forces or 'Mission Failure'. *The Washington Post*. Retrieved from <http://www.washingtonpost.com/>
- World Internet Usage and Population Statistics. (2012). Retrieved July 18, 2012 from <http://www.Internetworldstats.com/stats.htm>
- Wray, S. (1998). Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics. *Switch New Media Journal*, 4(2). Retrieved from <http://switch.sjsu.edu/web/v4n2/stefan/>
- Young, Y., Zhang, L., & Prybutok, V.R. (2007). Hacking into the minds of hackers. *Information Systems management*, 24(1), 281-287.
doi:10.1080/10580530701585823

VITA

Warren Held was born in Houston, Texas during 1985. He has lived the majority of his life in the Central Texas region; graduating from Austin's Westwood High School in 2004 and from Texas State University-San Marcos in 2008. After a nearly two year break, he re-entered Texas State in 2010 to pursue a master's degree. Warren was a graduate research assistant at the Texas School Safety Center for the majority of his graduate studies.

Permanent Email Address: warrenheld@txstate.edu

This thesis was typed by Warren V. Held.