CHAPTER V

Select Ethical-Hacking Incidences: Anonymous

One of the most well-known ethical-hacking "groups" is Anonymous. The word group here is arguably used incorrectly as Anonymous is more like an umbrella name or a movement for a plethora of smaller groups and operations. In addition to performing denial-of-service attacks, members of some of the smaller groups participate in more sophisticated forms of hacktivism that require a higher range of computer skills. Instances of these more sophisticated attacks include the release of names and details of the Mexican drug cartel, Los Zetas, the names and details of individuals who use child-pornography sites, and the capturing of secret documents held by governments around the world—some of these documents are then given and released by WikiLeaks.

Hacktivism is not limited to attacking information systems and retrieving documents. It also extends to finding technical solutions to mobilize people. At the height of the Egyptian e-revolution the major Internet-service providers and mobile-phone companies, under government direction, shut down the Internet, flipping the so-called Internet kill switch, preventing people from using the Internet and mobile phones. This, in turn, affected people's ability to mobilize. Anonymous worked around the clock to ensure that images from the revolution were still sent to international media.

This chapter takes selected notable ethical-hacking incidences from the quantitative work in chapter 3 and breaks down incident

by group, target, date, source, motivation, type of attack, whether any other groups have claimed responsibility, damage caused, and additional important information. This chapter will only explore incidences by Anonymous. The following chapter addresses select incidences for CCC, CyberBerkut, LulzSec, and others. Again, some of the incidences from the last chapter, this chapter, and the proceeding chapter will be explored in great detail from technical, political, criminological, and policy perspectives based on their classification in chapters 7 through 9.

ANONYMOUS

Anonymous—Operation Titstorm

ITEM	NOTES
Target:	Australian Government/Kevin Rudd
Date:	February 10, 2010
Source:	P. Martin, "Australian Government Website Hacked in Protest," *Technorati*, February 10, 2010, available at http://technorati.com/politics/article/australian-government-website-hacked-in-protest/ (last accessed February 11, 2010). "Operation Titstorm—Anonymous Wants Their Small Boobs" (February 12, 2010), available at http://www.youtube.com/watch?v=FdPmbiK4JGY. "Anonymous Message to the Australian Government" (February 14, 2010), available at http://www.youtube.com/watch?v=yK1nsGFsvbo.
Motivation:	Protest Internet filtering
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	No
Damage caused:	Kevin Rudd's website defaced with the words "Operation Titstorm" for an unspecified period of time
Additional important information:	N/A

Anonymous—ACS:Law

ITEM	NOTES
Target:	ACS
Date:	September 21, 2010
Source:	Wecanchangetheworld, "4Chan Hacks Anti Piracy Lawfirm, Leaks Porn Downloaders' Names," *Buzzfeed*, November 29, 2010, available at http://www.buzzfeed.com/wecanchangetheworld/4chan-hacks-anti-piracy-lawfirm-leaks-porn-downlo-1q36 (last accessed November 21, 2011). Enigmax, "New 4chan DDoS Targets Hated Anti-Piracy Law Firm," *Torrent Freak*, September 22, 2010, available at https://torrentfreak.com/new-4chan-ddos-targets-hated-anti-piracy-law-firm-100922/.
Motivation:	Operation: Payback- Protesting anti-piracy actions by large corporate entities
Type of attack:	DDoS, unauthorized access, data leak
Any other groups claiming responsibility:	No
Damage caused:	Published company emails and 5,300 names of people accused of illegally downloading "pr0n"
Additional important information:	N/A

Anonymous—PayPal

ITEM	NOTES
Target:	PayPal
Date:	December 6–9, 2010
Source:	J. Leyden, "Anonymous attacks PayPal in 'Operation Avenge Assange,'" *The Register*, December 6, 2010, available at http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/. M. Raman, "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14," *International Business Times*, July 20, 2011, available at https://www.ibtimes.com/fbi-cracks-down-anonymous-over-paypal-hacking-arrests-14-300225 (last accessed July 21, 2011).

	US Department of Justice, Office of Public Affairs, "Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks" (press release, July 19, 2011), available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed November 10, 2011). "Anonymous—Antisec—OP PayPal" (July 27, 2011), available at http://www.youtube.com/watch?v=aa-h0HHp908.
Motivation:	Operation Avenge Assange—retaliation for blocking WikiLeaks donations
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	It was reported that the attack lasted about eight hours and resulted in numerous disruptions. Little is known of what these disruptions entailed.
Additional important information:	Fourteen alleged members of Anonymous charged for intentional damage to protected computers, which carries a maximum penalty of ten years' (five for conspiracy) imprisonment and a $250,000 fine. The individuals named in the San Jose indictment are: Christopher Wayne Cooper, aka "Anthrophobic"; Joshua John Covelli, aka "Absolem" and "Toxic"; Keith Wilson Downey; Mercedes Renee Haefer, aka "No" and "MMMM"; Donald Husband, aka "Ananon"; Vincent Charles Kershaw, aka "Trivette," "Triv" and "Reaper"; Ethan Miles; James C. Murphy; Drew Alan Phillips, aka "Drew010"; Jeffrey Puglisi, aka "Jeffer," "Jefferp" and "Ji"; Daniel Sullivan; Tracy Ann Valenzuela; and Christopher Quang Vo. One individual's name was withheld by the court.

Anonymous—WikiLeaks revenge

ITEM	NOTES
Target:	MasterCard, Visa, Swedish prosecutor's office, Sara Palin's website
Date:	December 8–9, 2010
Source:	*The Australian*, "Wikileaks Complaint Against Visa" (July 5, 2011) https://www.theaustralian.com.au/news/world/wikileaks-complainst-against-visa/news-story/e5f38c1f5317f64cf0e73ca21921fa1c

	"Anonymous attack on MasterCard, discussed on 4 News" (December 8, 2010), available at http://www.youtube.com/watch?v=i4HKk5yB8fU.
Motivation:	Retaliation for blocking funding to WikiLeaks—Operation Avenge Assange
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	• MasterCard's main site was down for seven hours on December 8. • Visa's site was down for two hours on December 9. • Sara Palin's site was down for six minutes; additionally, her and her husband's bank accounts were disrupted. • Swedish prosecutor's office website was taken off-line for an unspecified period of time.
Additional important information:	Wikileaks lodged a complaint with the European Commission regarding the actions of Visa and Master Card for banning payment to Julian Assange's legal fund (The Australian)

Anonymous—Sony (PS3)

ITEM	NOTES
Target:	Sony
Date:	April 4, 2011
Source:	J. Mick, "Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit," *Daily Tech*, April 4, 2011, available at http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm. M. Raman, "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14," *International Business Times*, July 20, 2011, available at https://www.ibtimes.com/fbi-cracks-down-anonymous-over-paypal-hacking-arrests-14-300225 (last accessed July 21, 2011). "We are Anonymous—Sony hacked" (April 28, 2011), available at http://www.youtube.com/watch?v=370bq3VS5WU.

Motivation:	Retaliation for Sony taking legal action against George Hotz, a coder who wrote a tool that, Raman reported, "allows *homebrew* software to run on the PlayStation 3 (PS3)." The tool allows for the use of third-party software on the consoles.
Type of attack:	DDoS, data theft, unauthorized access.
Any other groups claiming responsibility:	LulzSec
Damage caused:	PS3 online capabilities were disrupted for almost a month.
Additional important information:	Compromised personal data of 77 million users worldwide; it is considered the largest breach of its kind to date.

Anonymous—Westboro Baptist Church

ITEM	NOTES
Target:	Westboro Baptist Church—church/organization
Date:	February, 2011
Source:	E-Li, "Anti-Gay Website Hacked by Anonymous," *lezbelib.over-blog.com*, June 4, 2011, available at http://lezbelib.over-blog.com/article-anti-gay-website-hacked-by-anonymous-75636306.html (last accessed June 5, 2011). "Anonymous v. Westboro Baptists" (February 22, 2011), available at http://www.youtube.com/watch?v=jUcW_8Ya32Q. "Anonymous Hacks Westboro Baptist Church During LIVE" (February 24, 2011), available at http://www.youtube.com/watch?v=OZJwSjor4hM. "Anonymous Members Allegedly Unmasked, Involved in Westboro Baptist Church Hacking Incident" (June 21, 2011), available at http://www.youtube.com/watch?v=QBExfh1oZCs.
Motivation:	Protesting homophobia; to retaliate for publicity church garnered in claiming prior Anonymous threats, which Anonymous denied
Type of attack:	Unspecified. Likely DDoS
Any other groups claiming responsibility:	No

Damage caused:	Took down a number of anti-gay websites for an unspecified period of time.
Additional important information:	The Westboro Baptist Church is the headquarters of campaign called "God Hates Fags," blaming the death of US soldiers on an acceptance of homosexuality by the United States, for example. Li reported that, in acknowledging the hack, Anonymous sent a message to the church that ended with "God hates fags: Assumption. Anonymous hates leeches: Fact."

Anonymous—Interpol attack

ITEM	NOTES
Target:	Interpol
Date:	28/3/12
Source:	B. Quinn, "Interpol Website Suffers 'Anonymous Cyber-Attack,'" *Guardian*, March 29, 2012, available at http://www.guardian.co.uk/technology/2012/feb/29/interpol-website-cyber-attack
Motivation:	Anonymous brought done a number of websites including the Interpol website in retaliation for arrest of twenty-five suspected members of Anonymous during Operation Unmask. Operation Unmask was part of a police operation where members of Anonymous were arrested for planned coordinated attacks against Columbia's defense ministry and presidential website.
Type of attack:	DDoS (suspected)
Any other groups claiming responsibility:	No
Damage caused:	Website off-line for a brief period
Additional important information:	N/A

Anonymous—Combined Systems (Bahraini contractor)

ITEM	NOTES
Target:	Combined Systems and Bahraini Government Website
Date:	February 14, 2012
Source:	D. Rushe, "Anonymous Sends Unhappy Valentine's Day Greetings," *Guardian*, February 14, 2012, available at http://www.guardian.co.uk/world/us-news-blog/2012/feb/14/anonymous-hacking-valentines-day-nasdaq
Motivation:	Response to alleged weapons sales of Combined Systems to the Bahraini Government, used in the suppression of anti-government protests
Type of attack:	DDoS (suspected)
Any other groups claiming responsibility:	Unknown
Damage caused:	Combined Systems and Bahraini Government Websites taken off-line
Additional important information:	Demonstrates (at least a segment of) Anonymous support for the Bahraini Uprising/Arab Spring

Anonymous—Nasdaq OMX—"Operation Digital Tornado"

ITEM	NOTES
Target:	Nasdaq OMX
Date:	February 14, 2012
Source:	D. Rushe, "Anonymous Sends Unhappy Valentine's Day Greetings," *Guardian*, February 14, 2012, available at http://www.guardian.co.uk/world/us-news-blog/2012/feb/14/anonymous-hacking-valentines-day-nasdaq.
Motivation:	"We are the 99%" protest against perceived corporate greed
Type of attack:	DDoS (suspected)
Any other groups claiming responsibility:	Handle "L0NGwave99"; may or may not be a member of Anonymous
Damage caused:	"Intermittent Service Disruption" to Nasdaq OMX website
Additional important information:	N/A

Anonymous—Puckett & Faraj law firm

ITEM	NOTES
Target:	Puckett & Faraj law firm (US Marine Frank Wuterich's defence lawyers)
Date:	February 6, 2012
Source:	D. Rushe, "Anonymous Publishes Trove of Emails from Haditha Marine Law Firm," *Guardian*, February 7, 2012, available at http://www.guardian.co.uk/technology/2012/feb/06/anonymous-haditha-killings
Motivation:	Protest against the firm defending Wuterich, a US Marine who pled guilty to a "dereliction of duty," but served no jail time, relative to the massacre of twenty-four unarmed Iraqi civilians by Marines in Haditha
Type of attack:	Unauthorized access—black-hat hacking
Any other groups claiming responsibility:	No
Damage caused:	"Trove" of emails leaked onto "The Pirate Bay" website. Excerpts ere also posted on Pastebin, the anonymous Internet posting site.
Additional important information:	Interesting that Anonymous attacked a law firm, and, seemingly too, notions of the innocence until proven guilty and defendants' rights. "In other emails released by Anonymous, members of the firm appear to worry that hack may 'completely destroy the Law Firm'" (Rushe).

Anonymous—London Metropolitan Police/FBI

ITEM	NOTES
Target:	London Metropolitan Police/FBI
Date:	Late January/early February 2012
Source:	J. Halliday, and C. Arthur, "Anonymous' Release of Met and FBI Call Puts Hacker Group Back Centre Stage," *Guardian*, February 3, 2012, available at http://www.guardian.co.uk/technology/2012/feb/03/anonymous-hack-met-fbi-call
Motivation:	Proof of ability to infiltrate two country's top investigative bodies. Also protest over arrest of LulzSec members.
Type of attack:	Unauthorized access

Any other groups claiming responsibility:	No
Damage caused:	Eighteen-minute inter-agency conference call from January 17, 2012, leaked in late January/early February 2012
Additional important information:	"The call reveals British police and the FBI discussing the delay of court proceedings against two alleged members of the LulzSec hacking group, which attacked a number of sites in 2011 including the US Congress and UK Serious Organised Crime Agency" (Halliday and Arthur).

Anonymous—MasterCard

ITEM	NOTES
Target:	MasterCard
Date:	June 28, 2011
Source:	J. Bergen, "Anonymous hacktivists take down MasterCard.com again in support of WikiLeaks," *Geek*, June 28, 2011, available at http://www.geek.com/articles/news/anonymous-hacktivists-take-down-mastercard-com-again-in-support-of-wikileaks-20110628/ (last accessed June 29, 2011). C. Fernandez, "Second WikiLeaks payback vs. MasterCard: LulzSec or Anonymous?," *International Business Times*, June 29, 2011, available at http://www.ibtimes.com.au/second-wikileaks-payback-vs-mastercard-lulzsec-or-anonymous-1283014 (last accessed June 30, 2011).
Motivation:	Protest WikiLeaks defunding
Type of attack:	DDoS
Any other groups claiming responsibility:	LulzSec—alluded to in reports, not formally claimed
Damage caused:	The MasterCard site was reportedly down for two hours
Additional important information:	N/A

Anonymous—Turkish Internet filter

ITEM	NOTES
Target:	Turkish government
Date:	July 2011
Source:	C. Zakalwe, "Turkish Government Websites Hacked in Protest at Internet Censorship" *Stop Turkey—BlogSpot* (July 7, 2011), available at http://stopturkey.blogspot.com/2011/07/turkish-government-websites-hacked-in.html
Motivation:	Protest Internet filtering
Type of attack:	Unauthorized access, data theft, data leak, defacement
Any other groups claiming responsibility:	No
Damage caused:	Anonymous claimed to have stolen data from over a hundred Turkish websites and defaced seventy-four government websites for an unspecified period of time. Unspecified what was done with the stolen data.
Additional important information:	N/A

Anonymous—Operation AntiSec

ITEM	NOTES
Target:	Law enforcement, Intelligence Agencies and Government Departments Globally—Eg. Scotland, United Kingdom, Arizona, California. …
Date:	August 1, 2011
Source:	L. Constantin, "AntiSec Hackers Hit 77 Law Enforcement Websites," *Softpedia*, August 1, 2011, available at http://news.softpedia.com/news/AntiSec-Hackers-Hit-77-Law-Enforcement-Websites-214555.shtml "Operation AntiSec" (June 2011-September 2012) available at https://everipedia.org/wiki/lang_en/Operation_AntiSec/
Motivation:	Retaliation for law-enforcement personnel's actions against protesters and arrests relating to the PayPal hack
Type of attack:	Unauthorized access, data theft, data modification, and data leak.

Any other groups claiming responsibility:	As the operation involved multiple hacking incidences, several groups participated including LulzSec, Anonymous, AntiSec NL, LulzSec Brazil, RedHack and other individual handler names
Damage caused:	Claim to have stolen 5–10 GB of data, including personal info on 7,000 officers.
Additional important information:	Anonymous also claimed to have stolen inmate info from prison services, which they are redacting. They threatened to publicize informant information—the publication of such information would be problematic. There were over 30 hacking incidences all under the banner of AntiSec involving retrieval of confidential information, the shutdown of websites but mostly the publication of information, many of which was protected by privacy laws.

Anonymous—Neo-Nazi websites

ITEM	NOTES
Target:	Neo-Nazi websites
Date:	August 8, 2011
Source:	M. Kumar, "Anonymous Hackers hack neo-Nazis websites & leak personal info of 16,000 Finns," *Hacker News*, November 8, 2011, available at http://thehackernews.com/2011/11/anonymous-hackers-hack-neo-nazis.html
Motivation:	As per *Hacker News*, "an apparent desire to shame the Finnish government into improving data security"
Type of attack:	Unauthorized access, defacement, data leak
Any other groups claiming responsibility:	No
Damage caused:	Released user information on 16,000 members
Additional important information:	N/A

Anonymous—Operation Free Condor

ITEM	NOTES
Target:	Quayaquil City Homepage (Ecuador)
Date:	August 8, 2011
Source:	T. Lara, "Hackers Attack Government Website in Ecuador to Protest President's Policies Against Freedom of Expression" on Knight Center for Journalism in the Americas, *Journalism in the Americas Blog* (August 10, 2011), available at http://knightcenter.utexas.edu/blog/hackers-attack-news-website-ecuador
Motivation:	Protest government measures against freedom of expression
Type of attack:	Sabotage and defacement. Site down for unspecified length of time
Any other groups claiming responsibility:	No
Damage caused:	Details of 45,000 police officers published, government threatened
Additional important information:	YouTube video was originally posted at this link (no longer available), http://www.youtube.com/watch?feature=player_embedded&v=ieC3gM5d_JM Another website (link unknown) attacked during same operation. Website based in Francisco de Orellana in eastern Ecuador.

Anonymous—BART

ITEM	NOTES
Target:	San Francisco's Bay Area Rapid Transit (BART)
Date:	August 15, 2011
Source:	L. Romney, "Bart drafts new policy on disruption of cellphone service," *LA Times*, October 19, 2011, available at http://latimesblogs.latimes.com/lanow/2011/10/bart-outlines-cell-phone-service-disruption-policy.html (last accessed October 20, 2011). E. Limer, "Anonymous follows through on BART hack, organizes protest," *Geekosystems*, August 15, 2011, available at http://www.geekosystem.com/anon-hacks-bart/.

	X. Jardin, "Anonymous hacks BART after wireless shutdown; protests planned for Monday," *Boing Boing*, August 14, 2011, available at http://boingboing.net/2011/08/14/anonymous-hacks-bart-after-wireless-shutdown-protests-planned-for-monday.html. "Website for BART customers hacked by Anonymous" (ABC News [US], August 15, 2011), available at http://www.youtube.com/watch?v=DjFSq-aTMm8&feature=related.
Motivation:	Perceived breach of first amendment rights—restricting freedom of speech by disabling telecommunications services
Type of attack:	Unauthorized access, modification of data, website defaced, release of personal information
Any other groups claiming responsibility:	No
Damage caused:	Defaced myBART website, leaked info on myBART user database which also included non-BART employees. Also "assured" non-BART employees that "the only information that will be abused from this database is that of BART employees."
Additional important information:	Undifferentiated/disorganized release of information. Though they claimed only BART employees would be abused, Anonymous made no distinction which employees may or may not have even been involved in cellphone disruption. Circumstances would include the alleged "destruction of district property.

Anonymous—OpIndependencia

ITEM	NOTES
Target:	Mexican government
Date:	September 15, 2011
Source:	E. Comley, "Hackers target Mexico government websites," Reuters, September 15, 2011, available at http://www.reuters.com/article/2011/09/15/us-mexico-hackers-idUSTRE78E7AC20110915 (last accessed September 18, 2011).

	M. Kumar, "Operation OpIndependencia: Anonymous hit Mexican government official websites," *Hacker News*, September 16, 2011, available at http://thehackernews.com/2011/09/operation-opindependencia-anonymous-hit.html (last accessed September 30, 2011).
Motivation:	Unknown
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Government websites off-line for a number of hours.
Additional important information:	N/A

Anonymous—RevoluSec

ITEM	NOTES
Target:	Syrian government websites
Date:	September 26, 2011
Source:	*Jerusalem Post*, "Online activists hack into Syrian government websites," September 26, 2011, available at https://www.jpost.com/Middle-East/Online-activists-hack-into-Syrian-government-websites (last accessed September 27, 2011). Anonymous—Operation Syria (September 12, 2011), available at http://www.youtube.com/watch?v=MGfF1ixk7S0. "Activists deface Syrian official websites" (Al Jazeera English, September 26, 2011), available at http://www.youtube.com/watch?v=qX30M6gakQ4.
Motivation:	Protesting level of government monitoring and injuries/deaths of protesters
Type of attack:	Unauthorized access, modification of data, defacement
Any other groups claiming responsibility:	No

Damage caused:	Caricatures of President Bashar Assaad were posted on defaced websites, as were protest messages, along with an interactive map of those reportedly killed during protests. Sites remained defaced for an unspecified period of time.
Additional important information:	N/A

Anonymous—New York Stock Exchange, Operation Icarus

ITEM	NOTES
Target:	New York Stock Exchange
Date:	October 4–10, 2011
Source:	D. Grant, "NYSE Hacked! Is The Anonymous Infrastructure Crumbling?," *New York Observer*, October 10, 2011, available at http://www.observer.com/2011/10/nyse-remains-unhacked-is-the-anonymous-infrastructure-crumbling-video/ (last accessed October 10, 2011). P. Chiaramonte and J. Winter, "Hacker Group Anonymous Threatens to Attack Stock Exchange," Fox News, October 4, 2011, available at http://www.foxnews.com/scitech/2011/10/04/hacker-group-anonymous-threatens-to-attack-stock-exchange/ (last accessed October 4, 2011). "Operation Invade Wall Street—A Message to the Media" (October 2, 2011), available at http://www.youtube.com/watch?v=lsLuYnEyFLw.
Motivation:	Occupy Wall Street protest
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	New York Stock Exchange off-line for two minutes
Additional important information:	Conflicting information over whether the attack was successful or whether it occurred at all. Anonymous claims that they did not perform this protest, and that it was a clever plot by law enforcement to accuse the group. There is too much conflicting information to know one way or another.

Anonymous/TeaMp0isoN

ITEM	NOTES
Target:	Oakland City Police
Date:	October 28, 2011
Source:	K. Fogarty, "Hackers come out of shadows to attack police, support Occupy protests," *IT World*, October 28, 2011, available at http://www.itworld.com/security/217561/hackers-come-out-shadows-attack-police-support-occupy-protests. "Anonymous Message to the Oakland Police Department and City of Oakland" (January 31, 2012), available at http://www.youtube.com/watch?v=SzDuSaf55ek.
Motivation:	Retaliation against police injuring a protester
Type of attack:	DDoS, SQL injection, unauthorized access, modification of data, website defaced, release of personal information
Any other groups claiming responsibility:	TeaMp0isoN—did not claim responsibility, but engaged in aspects of the protests
Damage caused:	Anonymous took the main Oakland Police Department website off-line for a number of hours, infiltrated a local government security server, and posted personal information of officers and information on the structure of the servers. TeaMp0isoN released a list of police-department websites vulnerable to MS-Access SQL injections, along with encouragements to participate in protest.
Additional important information:	No indication of collaboration between Anonymous and TeaMp0isoN

Anonymous—Operation Darknet

ITEM	NOTES
Target:	Those in possession of child pornography and child-pornography websites on the Dark Net
Date:	November 3, 2011
Source:	M. Liebowitz, "Anonymous releases IP addresses of alleged child porn viewers," NBC News, November 3, 2011, available at http://www.nbcnews.com/id/45147364/ns/technology_and_sciencesecurity/t/anonymous-releases-ip-addresses-alleged-child-porn-viewers/#.XAAS7S1L1PM (last accessed November 4, 2011).

	RT, "Anonymous busts Internet pedophiles," November 3, 2011, available at http://rt.com/usa/news/anonymous-child-tor-porn-513/ (last accessed November 15, 2011). QMI Agency, "Hacktivist group shuts down child porn sites," *Canoe Technology*, October 24, 2011, available at http://technology.canoe.ca/2011/10/24/18871656.html (last accessed October 25, 2011).
Motivation:	Expose those who are "ruining Tor for the majority of legitimate users." Lay ground work for investigations into child pornography.
Type of attack:	Spyware, brute-force attack, social engineering/phishing, release of identifying information of active child-pornography site visitors and those in possession of child pornography, and unauthorized access.
Any other groups claiming responsibility:	No
Damage caused:	No reported damage. Reputational damage to those identifiable; however, it is up to law enforcement to identify alleged paedophiles.
Additional important information:	Those identified as having child pornography claim that an add-on was accidentally created with Mozilla's permission through a browser update such that the child pornography was uploaded by someone else. This is seemingly unsubstantiated. No differentiation between those who have child pornography on their computer and whether this is known to users.

Anonymous—Operation Rainbow Dark

ITEM	NOTES
Target:	Rainbow Medical Associates, Dr. Carlo Musso
Date:	November 4, 2011
Source:	S. Seltzer, "For-Profit Company Oversaw Davis's Execution, Had Prompted Complaint for Illegal Purchase of Lethal Injection Drugs," *Alternet*, August 22, 2011, available at http://www.alternet.org/newsandviews/article/670237/for-profit_company_oversaw_davis%27s_execution,_had_prompted_complaint_for_illegal_purchase_of_lethal_injection_drugs/.

	AnonNews, "Operation Rainbow Dark," previously available at http://anonnews.org/?p=press&a=item&i=1162 (last accessed January 5, 2012).
Motivation:	Retaliation for execution of Troy Davis and the alleged use of illegally imported drugs for execution
Type of attack:	Possible unauthorized access, modification of data, website defacement, release of personal information
Any other groups claiming responsibility:	No
Damage caused:	Operation is unsubstantiated
Additional important information:	Same Anonymous post that something would be done pasted into various blogs and Anonymous-related sites. No indication that they followed through with threat.

Anonymous—OpCartel

ITEM	NOTES
Target:	Alleged associates of Los Zetas drug cartel in Mexico—corrupt law enforcement, those involved in managing and participating in Los Zetas operations
Date:	November 5, 2011
Source:	N. Mandell, "Anonymous hacker group threatens Mexican drug cartel Zetas in online video," *New York Daily News*, October 31, 2011, available at http://www.nydailynews.com/news/world/anonymous-hacker-group-threatens-mexican-drug-cartel-zetas-online-video-article-1.969859#ixzz1d4sAfvE6 (last accessed November 1, 2011)
Motivation:	Retaliation for alleged kidnapping of an Anonymous activist. General threat posed by criminal organizations.
Type of attack:	DDoS attack. Unauthorized access to communications. Threatened release of personal information of those involved in cartel operations.
Any other groups claiming responsibility:	No
Damage caused:	If information is released (or even if not released), more likely to pose a threat to Anonymous members depending on the nature and importance the Zetas cartel places on the information. The cartel may retaliate on the basis of publicity alone.

Additional important information:	Current reports indicate conflicting rumours whether "Opcartel" will go ahead. Little belief that Anonymous has the ability to do any kind of damage. Interesting note—"Anonymous likely won't be able to turn up more information than the U.S. government already has, but they are able to publicize more information than the U.S. government can." Stratfor, *Dispatch: Anonymous' Online Tactics Against Mexican Cartels* (November 1, 2011), available at https://worldview.stratfor.com/article/dispatch-anonymous-online-tactics-against-mexican-cartels#ixzz1cj0LSuso. UPDATE—No attack occurred: Pastebin, *OPCartel Proceeds* (November 3, 2011), available at http://pastebin.com/XZRpjUZq.

Anonymous—Israeli Government

ITEM	NOTES
Target:	Israel government, security-services websites
Date:	November 5, 2011
Source:	A. Pfeffer, and O. Yaron, "Israel government, security services websites down in suspected cyber-attack," *Haaretz*, November 6, 2011, available at http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042 (last accessed November 7, 2011). "An open letter from Anonymous to the Government of Israel" (November 4, 2011), available at http://www.youtube.com/watch?v=QNxi2lV0UM0.
Motivation:	Retaliation for intercepted Gaza flotilla
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Websites off-line for an unspecified amount of time, including that of the Israel Defence Force, Mossad, and the Shin Bet security services, in addition to a number of government portals and ministries.
Additional important information:	N/A

Anonymous—Operation #TMX

ITEM	NOTES
Target:	Toronto Stock Exchange
Date:	November 7, 2011
Source:	J. Errett, "Expecting Anonymous at #TMX" *Now Toronto*, November 7, 2011, available at http://www.nowtoronto.com/news/webjam.cfm?content=183319 (last accessed November 8, 2011)
Motivation:	Part of the Occupy movement; economy disparity, social inequality
Type of attack:	None—likely attempted DDoS
Any other groups claiming responsibility:	No
Damage caused:	None
Additional important information:	No confirmed reports of an attack

Anonymous—Operation Brotherhood Shutdown

ITEM	NOTES
Target:	Muslim Brotherhood websites
Date:	November 11, 2011
Source:	M. Kumar, "Operation Brotherhood Shutdown: Multiple Sites taken down by Anonymous Hackers," *Hacker News*, November 12, 2011, available at http://thehackernews.com/2011/11/operation-brotherhood-shutdown-by.html (last accessed November 13, 2011). "Anonymous—Operation Brotherhood Shutdown" (November 7, 2011), available at http://www.youtube.com/watch?v=ZnPTBLbazAo. "Anonymous—The Aftermath of Operation Brotherhood Shutdown" (November 12, 2011), available at http://www.youtube.com/watch?v=bBe9co3l9wI&feature=related.
Motivation:	"The Muslim Brotherhood has become a threat to the revolution Egyptians had fought for"
Type of attack:	DDoS

Any other groups claiming responsibility:	No
Damage caused:	Four websites were temporarily taken down by an attack of approximately 380,000 hits per second. Down time unspecified.
Additional important information:	N/A

Anonymous (Finland)—Operation Green Rights

ITEM	NOTES
Target:	Talvivaara
Date:	November 12, 2011
Source:	E. Kovacs, "Anonymous Turns Green and Goes After Polluters," *Softpedia*, November 15, 2011, available at http://news.softpedia.com/news/Anonymous-Turns-Green-and-Goes-After-Polluters-234681.shtml
Motivation:	Environmental destruction from waste water resulting in contamination of surrounding flora and fauna
Type of attack:	Unknown; most likely a series of DDoS attacks
Any other groups claiming responsibility:	No
Damage caused:	None as of yet
Additional important information:	N/A

Anonymous vs. Anonymous?

ITEM	NOTES
Target:	Anon Ops
Date:	November 16, 2011
Source:	E. Kovacs, "Anonymous Attacks Anonymous for Being Trolls," *Softpedia*, November 16, 2011, available at http://news.softpedia.com/news/Anonymous-Attacks-Anonymous-For-Being-Trolls-234949.shtml (last accessed November 18, 2011)

Motivation:	"Anonymous claims that those behind AnonOps are blind with power and instead of fighting corruption and internet censorship by welcoming newcomers, they treat them with disrespect and arrogance"
Type of attack:	Zero-day attack
Any other groups claiming responsibility:	No
Damage caused:	Shut down servers used by AnonOps
Additional important information:	Example of infighting and disunity inside Anonymous

Anonymous—Venezuelan Government Hacks

ITEM	NOTES
Target:	Venezuelan Government websites
Date:	Various, 2011
Source:	J. Wyss, "Political hackers are one of Latin America's newest headaches," *Miami Herald*, November 3, 2011, available at http://www.miamiherald.com/2011/10/31/2481360/political-hackers-are-one-of-latin.html
Motivation:	Anti-government protests
Type of attack:	Website hack
Any other groups claiming responsibility:	Reportedly affiliated with Anonymous
Damage caused:	Government websites defaced
Additional important information:	Two hundred attacks in 2011, a large number considering the country's "slow internet connections." Interesting to note the attack on a leftist government, in contrast with the centrist/centre-right governments of other attacks.

Anonymous—US Congress

ITEM	NOTES
Target:	US Congress
Date:	November 17, 2011
Source:	E. Kovacs, "Anonymous Threatens Congress Over SOPA," *Softpedia*, November 17, 2011, available at http://news.softpedia.com/news/Anonymous-Threatens-Congress-Over-SOPA-235201.shtml. "Anonymous—A Message to Congress on SOPA you will not infringe on our rights" (November 18, 2011), available at http://www.youtube.com/watch?v=9rbyk0h3yeg.
Motivation:	Opposition to the proposed Stop Online Piracy Act; claims the proposed legislation would represent a breach of constitutional rights. Fear that the act may have wider implications than what the title indicates.
Type of attack:	None yet. Probably DDoS.
Any other groups claiming responsibility:	No
Damage caused:	None
Additional important information:	N/A

Anonymous—Operation Weeks Payment (Brazilian banks)

ITEM	NOTES
Target:	Brazilian banks
Date:	January 2012
Source:	F. Bajak, "Anonymous Hackers Claim They Were Infiltrated," *Bellingham Herald*, February 29, 2012, available at http://bellinghamherald.com/2012/02/29/2415830/anonymous-hackers-claim-they-were.html. S. McCaskill, "Anonymous Targets Vatican Website," *Tech Week Europe*, March 8, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-targets-vatican-website-65797.
Motivation:	Protest against "widespread inequality"

Type of attack:	DDoS attacks
Any other groups claiming responsibility:	No
Damage caused:	Websites crashed, defaced
Additional important information:	Nine Brazilian banks were targeted

Anonymous—Polish Government

ITEM	NOTES
Target:	Polish government websites
Date:	January 21–22, 2012
Source:	T. Jowitt, "Anonymous Attacks Polish Websites for ACTA Support," *Tech Week Europe*, January 26, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-attacks-polish-websites-for-acta-support-56450
Motivation:	In response to Poland's support for the proposed multinational Anti-Counterfeiting Trade Agreement (ACTA; not in force)
Type of attack:	DDoS
Any other groups claiming responsibility:	@AnonymousWiki (possibly linked to Anonymous)
Damage caused:	Polish government websites taken off-line
Additional important information:	ACTA protests follow earlier Stop Online Piracy Act (a controversial law proposed in the United States) protests.

Anonymous—Panda Security

ITEM	NOTES
Target:	Panda Security
Date:	March 6, 2012
Source:	M. Smolaks, "Anonymous Hits Back Over LulzSec Arrests," *Tech Week Europe*, March 7, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-hits-back-over-lulzsec-arrests-65265

Motivation:	Retaliation for arrest of five LulzSec members and the ousting of LulzSec former leader Sabu
Type of attack:	Defaced website, gained access to staff details and shared the information online
Any other groups claiming responsibility:	No
Damage caused:	Thirty-sex defaced websites and the email details of Panda security staff were posted online
Additional important information:	Demonstrates Anonymous and LulzSec interconnection

Anonymous—Vatican (two occasions)

ITEM	NOTES
Target:	Vatican website, Vatican Radio website
Date:	First: March 7, 2012, Second: March 14, 2012
Source:	First: S. McCaskill, "Anonymous Targets Vatican Website," *Tech Week Europe*, March 8, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-targets-vatican-website-65797. Second: M. Kumar, "Vatican Radio Hacked by Anonymous Hackers," *Hacker News*, March 14, 2012, available at http://thehackernews.com/2012/03/vatican-radio-hacked-by-anonymous.html.
Motivation:	First: Protest, "revenge for the 'corruption' of the Roman Catholic Church over the course of its history" (McCaskill). Second: "Anonymous justified its attack by claiming that Vatican Radio is responsible for high cancer rates in a neighborhood near the broadcaster's main transmission facility" (Kumar).
Type of attack:	First: Suspected DDoS Second: Website data compromised
Any other groups claiming responsibility:	No
Damage caused:	First: Vatican website inaccessible Second: Personal data of Vatican Radio journalists, Vatican website hacked

Additional important information:	Second: "The attack is part of the organization's recent declaration of war against religion" (Kumar).

Anonymous—Megaupload protest

ITEM	NOTES
Target:	US Department of Justice, Universal Music, Motion Picture Association of America
Date:	Early/mid-January 2012
Source:	J. Halliday and C. Arthur, "Anonymous' Release of Met and FBI Call Puts Hacker Group Back Centre Stage," *Guardian*, February 3, 2012, available at http://www.guardian.co.uk/technology/2012/feb/03/anonymous-hack-met-fbi-call
Motivation:	Protest over the closure on criminal charges of the Megaupload file-sharing website
Type of attack:	DDoS (suspected)
Any other groups claiming responsibility:	No
Damage caused:	Websites off-line temporarily
Additional important information:	Part of the growing rift between Hollywood and the online pirating community

Anonymous—Leader of NPD Germany

ITEM	NOTES
Target:	Website of NPD Germany party leader
Date:	Early January 2012
Source:	J. Halliday and C. Arthur, "Anonymous's Release of Met and FBI Call Puts Hacker Group Back Centre Stage," *Guardian*, February 3, 2012, available at http://www.guardian.co.uk/technology/2012/feb/03/anonymous-hack-met-fbi-call
Motivation:	Political protest
Type of attack:	DDoS (suspected)
Any other groups claiming responsibility:	No

Damage caused:	Unauthorized access, website off-line temporarily
Additional important information:	N/A

Anonymous—Chinese Government Websites

ITEM	NOTES
Target:	Hundreds of Chinese government websites, including governmental agencies and business enterprises.
Date:	March 30, 2012—April 6, 2012
Source:	J. Burt, "Anonymous Defaces Many Chinese Government Websites," *Tech Week Europe*, April 6, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-defaces-chinese-websites-71791
Motivation:	Response to Chinese government "cracking down on dozens of Websites in the country." Also, pro-democracy social protest.
Type of attack:	DDoS, website defacing
Any other groups claiming responsibility:	No
Damage caused:	Hundreds of government websites defaced, at all levels (local, regional, national)
Additional important information:	Pro-democracy Pastebin message: "All these years, the Chinese Government has subjected their people to unfair laws and unhealthy processes," the message reads. "People, each of you suffers from tyranny of that regime. Fight for justice, fight for freedom, fight for democracy!..." (See E. Protalinski, "Anonymous Hacks Hundreds of Chinese Government Sites" ZDnet, April 4, 2012, available at https://www.zdnet.com/article/anonymous-hacks-hundreds-of-chinese-government-sites/.)

Anonymous—Operation Trial at Home (UK)—UK Home Office Website

ITEM	NOTES
Target:	UK Home Office website
Date:	April 7, 2012
Source:	M. Broersma, "Anonymous Claims Home Office Website Takedown," *Tech Week Europe*, April 8, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-home-office-ddos-71886

Motivation:	"Intended to protest 'draconian surveillance proposals'" (Broersma)
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Website off-line for a brief period
Additional important information:	Promises of more attacks to come. The start of "Operation Trial at Home"

Anonymous—Operation Last Resort

ITEM	NOTES
Target:	US Sentencing Commission's website
Date:	January 25, 2013
Source:	V. Blue, "Feds Stumbling After Anonymous Launches Operation Last Resort," *ZDNet*, January 30, 2013, available at http://www.zdnet.com/feds-stumbling-after-anonymous-launches-operation-last-resort-7000010541/. V. Blue, "Anonymous Hacks US Sentencing Commission and Distributes Files," *ZDNet*, January 26, 2013, available at http://www.zdnet.com/anonymous-hacks-us-sentencing-commission-distributes-files-7000010369/.
Motivation:	To protest the "harsh treatment" by government prosecutors of Internet activist Aaron Swartz. As Blue reported, to call attention to "the federal sentencing guidelines which enable prosecutors to cheat citizens of their constitutionally-guaranteed right to a fair trial."
Type of attack:	Warheads, back door, and defacing
Any other groups claiming responsibility:	No
Damage caused:	Replaced the site's content with a video denouncing the government and praising Swartz. Transformed the ".gov" site into an interactive video game of *Asteroids*. Threatened that de-encryption keys would be publicly released (thus releasing information held on the stolen files) if the US government did not comply with Anonymous's demands for legal reform.

	Left a back door and made it editable in such a way that encourages other hackers to shell the server. In the defacement text, Anonymous also said it placed "multiple warheads" on "compromised systems" on various unnamed websites, and encouraged members to download the encrypted files from ussc.gov that are "primed, armed and quietly distributed to numerous mirrors."
Additional important information:	Commandeered federal websites, threatened to release government information, distributed files, and demanded legal reform. "Anonymous Operation Last Resort Video" (January 26, 2013), available at http://www.youtube.com/watch?v=WaPni5O2YyI.

Anonymous—Operation Trial at Home (UK)—10 Downing Street and Ministry of Justice

ITEM	NOTES
Target:	UK government websites, including 10 Downing Street (official residence of the prime minister) and the Ministry of Justice
Date:	April 7—April 10, 2012
Source:	T. Brewster, "Anonymous Strikes Downing Street and Ministry of Justice," *Tech Week Europe*, April 10, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-government-downing-street-moj-71979
Motivation:	Mixed motivations—protest over UK government's web-surveillance plans, protest over UK's extradition treaty with the United States
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	Three government websites taken down temporarily: 10 Downing Street, Home Office, and Ministry of Justice websites
Additional important information:	Anonymous claimed that they would also attack Government Communications Headquarters (GCHQ)

Anonymous—Operation Ferguson

ITEM	NOTES
Target:	Ferguson Police Department, Ferguson, Missouri Jon Belmar, St. Louis County Police Chief
Date:	August 2014
Source:	D. Hunn, "How computer hackers changed the Ferguson protests', *St. Louis Post-Dispatch*, August 13, 2014, available at http://www.stltoday.com/news/local/crime-and-courts/how-computer-hackers-changed-the-ferguson-protests/article_d81a1da4-ae04-5261-9064-e4c255111c94.html
Motivation:	Police misconduct and its consequences. A doxing attack followed after Anonymous posted a video warning to the Ferguson police, admonishing them for fatally shooting Mike Brown, an unarmed African-American teenager, and vowing revenge if any protesters demonstrating against the police were harmed. Two reasons for the attack: 1) Because Jon Belmar refused to release the name of the officer who shot Mike Brown, and 2) Because Belmar challenged Anonymous, calling their threats hollow.
Type of attack:	Document tracing (doxing)—publishing personally identifiable information. DDoS on the Ferguson Police Department website.
Any other groups claiming responsibility:	No
Damage caused:	Information about Belmar's home address, phone number, and family members and their accounts on social media were all exposed and made public by Anonymous. Photos of Belmar's family members were also made public.
Additional important information:	Anonymous made threats to Belmar that his daughter's personal details, phone number, and home address would be made public in an hour if the name of the officer who shot Mike Brown was not released. However, Anonymous did not disclose the daughter's information, tweeting: "We will save the rest of our energy for the true perpetrator."

Anonymous member, Deric Lostutter—Steubenville High School rape case

ITEM	NOTES
Target:	Steubenville, Ohio
Date:	2012–2013
Source:	K. Baker, "Anonymous outs members of alleged Steubenville High School 'Rape Crew,'" *Jezebel*, December 24, 2012, available at http://jezebel.com/5970975/anonymous-outs-members-of-alleged-steubenville-high-school-rape-crew
Motivation:	Two male sixteen-year-old Steubenville High football players raped a sixteen-year-old girl from West Virginia at a party in Steubenville. The case received national coverage, in part because of the criticism placed upon media outlets, especially on CNN, for their biased coverage of the case, lack of focus on the victim, and sympathy for the rapists. Following the national coverage of the case, Anonymous threatened to reveal the names of other unindicted alleged participants. In December 2012, KnightSec, an offshoot of Anonymous, hacked an unaffiliated website, posting a demand for an apology by school officials and local authorities, who had allegedly covered up the incident in order to protect the athletes and the school's football program.
Type of attack:	Doxing. Lostutter hacked a list of school-board members, cell-phone numbers, and home addresses, and received damning files—internal emails, expense reports, and other incriminating records about the district—which he disseminated online, alleging that more people were involved in the incident.
Any other groups claiming responsibility:	KnightSec, an offshoot of Anonymous
Damage caused:	Personal information made public
Additional important information:	Questionable whether this is ethical hacking or online vigilantism. Lostutter was later indicted under the federal Computer Fraud and Abuse Act. Lostutter's home was raided by the FBI with a warrant targeting his hacking involvement, even though another person acknowledged responsibility for the hack.

Anonymous/WikiLeaks—Stratfor

ITEM	NOTES
Target:	Stratfor (US-based intelligence-gathering firm)
Date:	December 2011–February 2012
Source:	J. Ball, "WikiLeaks Publishes Stratfor Emails Linked to Anonymous Attack," *Guardian*, February 27, 2012, available at http://www.guardian.co.uk/media/2012/feb/27/wikileaks-publishes-stratfor-emails-anonymous
Motivation:	Exposing US military and geopolitical secrets
Type of attack:	Data theft/unauthorized access
Any other groups claiming responsibility:	Collaboration between Anonymous and WikiLeaks
Damage caused:	Personal information and login criteria stolen from user base (300,000 subscribers). Five and a half million emails were accessed, a limited number of which were published online.
Additional important information:	Hacking attack by Anonymous rather than a whistle-blower. WikiLeaks was merely the vehicle in which information was disseminated and promoted. Single-handedly took down the credibility of the otherwise reputable organization.

Anonymous—UK Ministry for Justice and Home Office

ITEM	NOTES
Target:	UK government; websites affected include the Ministry of Justice and the Home Office.
Date:	August 21, 2012
Country:	England
Source:	BBC News, "Anonymous hits UK government websites in Assange protest," August 21, 2012, available at http://www.bbc.com/news/technology-19330592
Motivation:	In retaliation of the United Kingdom's handling of the Julian Assange case
Type of attack:	Anonymous claimed responsibility on Twitter for the denial-of-service attacks that flooded UK government websites, causing disruption and access issues

Damage caused:	Access to websites was denied in brief intervals, no sensitive information was stolen.
Additional important information:	N/A

Anonymous—Scotland Yard

ITEM	NOTES
Target:	Scotland Yard
Date:	October 24, 2012
Country:	England
Source:	BBC News, "Anonymous hacking group target police web forum," October 24, 2012, available at http://www.bbc.com/news/uk-20072981
Motivation:	Retaliation against the police and armed forces for the injustice of the legal system
Type of attack:	Stole identity information, and an attack was undertaken which redirected readers from other police forums to a page showing a video approved by the collective
Damage caused:	Data compromised
Additional important information:	An Internet forum used by police to exchange information and discuss policing issues was "compromised" by hackers from Anonymous. Anonymous obtained the private email addresses of a number of serving and retired officers. Former and current police personnel received in their private email accounts an email containing the subject line "A message to the police and armed forces." It read: "Hello members of our UK police and armed forces, stand with us, not against us. We are not against you, only against the evil system that you defend, and we appeal to your consciences to stop protecting the traitors and banksters, and protect us from them instead."

Anonymous (and LulzSec)—UK GCHQ (Government Communications Headquarters)

ITEM	NOTES
Target:	Hacktivist groups Anonymous and LulzSec
Date:	February 5, 2014
Country:	England
Source:	L. Constantin, "U.K. spy agency attacked hacktivist groups," *Computer World*, February 5, 2014, available at http://www.computerworld.com/article/2487354/cybercrime-hacking/u-k--spy-agency-attacked-hacktivist-groups.html
Motivation:	In retaliation of hacktivist attacks on websites of various companies, organizations and governments
Type of attack:	Denial-of-service and other techniques to disrupt hacktivist groups' online activities and disrupted the hacktivists' communication channels
Damage caused:	Revealed identities of Anonymous and LulzSec hackers
Additional important information:	A unit of the GCHQ, the Joint Threat Research Intelligence Group (JTRIG) collected information on hacktivists and shared it with law-enforcement agencies, such as the US National Security Agency. JTRIG used human-intelligence techniques to gather information about members of Anonymous and LulzSec. JTRIG intelligence-gathering specifically targeted two hackers using the online handles "GZero" and "p0ke." JTRIG used undercover agents in IRC logs to gather the information on the identification of the hacktivists.

Anonymous—Operation DeathEaters

ITEM	NOTES
Target:	UK high-profile paedophilic ring
Date:	November 27, 2014
Source:	K. Baker, "Hacking group Anonymous to target paedophiles using the 'dark web' to carry out child abuse," *Daily Mail*, January 25, 2015, available at http://www.dailymail.co.uk/news/article-2924864/Hacking-group-Anonymous-target-paedophiles.html.

	L. Eleftheriou-Smith, "Anonymous calls for activists to help expose international paedophile networks with 'Operation DeathEaters,'" *Independent*, January 23, 2015, available at http://www.independent.co.uk/news/uk/home-news/anonymous-calls-for-activists-to-help-expose-international-paedophile-networks-with-operation-deatheaters-9998350.html.
Motivation:	Operation Death Eaters is an independent "tribunal" of hackers that have allegedly identified an elite club of paedophiles, including politicians, religious figures, royals, and celebrities, involved in the torture and murder of children
Type of attack:	Unknown
Any other groups claiming responsibility:	No
Damage caused:	Compromising data
Additional important information:	Anonymous released a video and tweeted, urging people to take to the streets of London to protest against the cover up of a "nightmarish" paedophile ring. They made reference to a number of high-profile cases in the United Kingdom, including those of Jimmy Savile, the Elm Guest House, and MP Cyril Smith, and are collecting further data toward proof of similar international rings. This will involve the group setting up a complex database, mapping connections between cases, and presenting it on social media.

Anonymous—#OpHK (Operation Hong Kong)

ITEM	NOTES
Target:	Chinese government websites
Date:	October 7, 2014
Source:	D. Grover, "Anonymous Hackers Threaten Web War Against Hong Kong Police and Government," *International Business Times*, October 2, 2014, available at http://www.ibtimes.co.uk/anonymous-hackers-threaten-web-war-against-hong-kong-police-government-1468220. A. K. Jha, "#OpHK aka Operation Hong Kong: Anonymous hacks Chinese Government website," *Tech Worm*, 2014, available at http://www.techworm.net/2014/10/operation-hong-kong-anonymous-hacks-chinese-government-website.html.

Motivation:	Support for pro-democracy protesters in Hong Kong. While pro-democracy protesters in Hong Kong were protesting on the ground, hacktivists from around the globe joined together online to support the protesters.
Type of attack:	Hacked and defaced Chinese government websites. DDoS
Any other groups claiming responsibility:	In addition to Anonymous, other groups took part in the operation dubbed #OpHK Report suggest that hundreds of Hong Kong–based websites were hacked and defaced under the Operation Hong Kong, while several hundred other were brought down via DDoS attacks by other hacker groups in support of the pro-democracy protests in Hong Kong. Major sites hacked and DDoS attacked include those of the Chinese Ministry of Justice, Ministry of Public Security, and the Hong Kong Police Force.
Damage caused:	A defaced webpage could not be accessed and displayed the message: "We are here to fight against Censorships, Corruptions, Government and against those things that obstruct humans rights. We encountered some problems and issues that we don't want the countries or world want. We are here to help you create a better world. People, we tell you that you are not alone!. This is Kyfx and I am one of the anonymous follower. Peace will not be silenced by fear We are here to expect more." Websites which were defaced, all on October 8, 2014, by Anonymous included: http://www.tielingws.gov.cn/, the website could not be accessed. http://www.bys.gov.cn/index.html, the webpage says "HACKED FUCK THE SYSTEM." http://www.tongcheng.jcy.gov.cn/Xnitro.html, the webpage says "Hacked by Xnitro ErTn and Hacked by Fallaga Team [Don't forget this name]." http://qxj.km.gov.cn/hector.html, the webpage says "Hacked—Cyber Freedom INCEF." The database of www.gyx.gov.cn was also leaked on Pastebin.

Additional important information:	Anonymous tweeted: "In the great tradition of civil disobedience, We, Anonymous, declared war on injustice a few years ago. Once again the Chinese government strikes hard at its own people. At this very moment Chinese police forces are hurting innocent citizens who cry for liberty. Since we are many and we do not fear ANY abusive government or institution in the globe, we also declared war against the Chinese Government, well known for its authoritarian posture. We are only targeting .gov.cn and .gov.hk .mil.cn in opposition to their oppressive ways. We emphatically condemn those attacks against non governmental or non military targets. We stand in solidarity with the citizens of Hong Kong, a Statement released by the Anonymous read."

Anonymous—Operation DestructiveSec/Lulzxmas

ITEM	NOTES
Target:	UK Banks, clothing retailer
Date:	December 2011
Source:	F. Rashid, "Anonymous Beards the Banks to Play Twisted Santa Claus," *Tech Week Europe*, December 21, 2011, available at http://www.techweekeurope.co.uk/news/anonymous-beards-the-banks-to-play-twisted-santa-claus-50922
Motivation:	Robin Hood mentality—rob from the rich, give to the poor
Type of attack:	SQL injection attack
Any other groups claiming responsibility:	Lulzxmas, Anonymous (potentially coordinated)
Damage caused:	About $75,000 stolen from UK Banks, $1.25M in virtual credit cards compromised
Additional important information:	

Anonymous—Operation Charlie Hebdo

ITEM	NOTES
Target:	Al-Qaeda, the Islamic State (ISIS), and terrorist organizations who impair freedom of speech. Threats also made to Turkey, Saudi Arabia, Qatar, and other countries supporting ISIS.
Date:	January 10, 2015
Source:	O. Solon, "Anonymous 'hacktivists' attack ISIS—strike down terrorist propaganda and recruitment sites," *Mirror*, February 9, 2015, available at http://www.mirror.co.uk/news/technology-science/technology/anonymous-hacktivists-attack-isis---5130966. L. Franceschi-Bicchierai, "Anonymous claims first victim in 'Operation Charlie Hebdo,'" *Mashable*, January 11, 2015, available at http://mashable.com/2015/01/10/anonymous-operation-charlie-hebdo/.
Motivation:	The *Charlie Hebdo* shootings in January 2015, and further terrorist attacks in Paris that February, which Anonymous called an attack on freedom of speech and democracy
Type of attack:	DDoS attacks
Any other groups claiming responsibility:	Unknown
Damage caused:	The French-language jihadist website ansar-alhaqq.net was down for more than an hour
Additional important information:	N/A

Anonymous—Support for Hong Kong protestors

ITEM	NOTES
Target:	Thirty Chinese local government websites
Date:	April 10, 2015
Source:	M. Russon, "Anonymous brings down 30 Chinese government websites to support Hong Kong protesters," *International Business Times*, April 13, 2015, available at http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069

Motivation:	To protest the arrest of five hacktivists in October 2014 who were accused of sending additional traffic to a Hong Kong government website during pro-democracy protests
Type of attack:	DDoS
Any other groups claiming responsibility:	No
Damage caused:	The attacked government websites went off-line
Additional important information:	N/A

Anonymous (James Jeffery)—BPAS

ITEM	NOTES
Target:	British Pregnancy Advisory Service (BPAS)
Date:	March 8, 2012
Source:	M. Broersma, "Hacker Pleads Guilty to Abortion Website Attack," *Tech Week Europe*, March 12, 2012, available at http://www.techweekeurope.co.uk/news/hacker-pleads-guilty-to-abortion-website-attack-66295. P. Gallagher, "Abortion Website Hacker Caught," *Guardian*, March 11, 2012, available at http://www.guardian.co.uk/world/2012/mar/11/abortion-website-hacker-caught.
Motivation:	Anti-abortion protest
Type of attack:	Twenty-six thousand attempts to attack BPAS servers during a six-hour period—most likely DDoS
Any other groups claiming responsibility:	Unknown
Damage caused:	Defacement with Anonymous logo and theft of BPAS database of information on those requesting BPAS services
Additional important information:	The normally left/liberal-leaning Anonymous (or one member, Jeffery) attacked a pro-abortion website. Suggests that Anonymous is far less homogeneous in its political stance than previously believed. Jeffery's defacement displayed conservative views on abortion. Jeffery goes by the pseudonym "Pablo Escobar" on Twitter. He was arrested and pled guilty to two offences under the Computer Misuse Act of 1990 (one relating to defacement, one to theft of personal information).