

Internet Hacktivism: Is it Worth the Effort? A Case Study on Anonymous

By: Ryann Quigley and Dr. Scott Ingram

Vocabulary:

Encryption- process of encoding information so third parties cannot read it. Typically in anti-hacking software

Hackers- those who attempt to access information on a computer system without permission of their owners

Hacktivism- a nonviolent way to voice political opinions, promote free speech, and protect human rights, through the proper use of technology and the use of the Internet

Hyperlink- a reference to specific element of data within a document that is followed automatically by computers

Operating System- collection of software that manages hardware within a computer

Mainframe Computers- used by corporations and Governments for critical applications, bulk data processing, resource planning and transaction processing

Microserfs- users of Windows by Microsoft, promoted corporate success

Brief History:

True Hackers- 1950's and 1960's

Hardware Hackers- shrink mainframes for personal use

Game hackers- reverse engineering codes of programs to change purpose of program

phone phreakers- attempt to hack phone systems to make free telephone calls

Personal Computing- connect computers through phone lines

hackers- led to creation of Microsoft's Windows operating system.

Modern Hackers-

Criminal/ Counter-cultural hacking- steal information, utilized by organized crime

Nonviolent/ Hacktivists- voicing political opinions to promote free speech and protect basic

human rights

Motives- Thrill or challenge seekers

Financial

Social change

Types of attacks completed by Anonymous:

distributed Denial-of-Service (DDoS) attack is an overload of a website using a network of computers to attack the targeted website with the use of a program

Virtual Sit-in slow or crash a website by manually overwhelming it with requests for information

Site Defacements- replace the original content of a website with new content that portrays a particular message of a group

Site redirects implement a program that will send the visitors to a new website.

Identification Theft- gains access to classified information and steals it, typically releasing it to the public for shame

History of Anonymous:

• They are a group of nonviolent hackers that are commonly referred to as hacktivists.

• They are loosely organized group. Anonymous has no leader, no hierarchy, no ranks, and no set way of communication.

• They originated on an online image board site, known as 4chan, in 2003.

• Anonymous has been devoted to the prevention of internet censorship and surveillance, and the promotion of equality for genders, sexual orientation and race

Results:

Of 239 total Operations, three were analyzed specifically. #OpRollRedRoll, #OpLastResort, and #Opsreal were the three most prominent. Of the remaining 236, the majority lacked supplemental information or had a plan of attack

Methodology:

Because hacktivism is a very new form of activism, there is minimal research done on the topic. To examine the seven major attacks planned and executed by Anonymous, we must conduct a case study on the hacktivist group. Using newspaper articles, Internet blogs, forums, and Anonymous' webpage AnonNews.org, we will be able to gain information on the group, analyze their attacks and determine how successful they are. Scholarly sources can provide us information focused on hacktivism in general, providing history, key terms and explanations of hacktivism.

These news articles came from reputable and well-known sources. These newspapers include Fox News, Yahoo News, The Huffington Post, International Business Times, NYU Local, The New York Post, BBC News, Daily mail and many others. Some of the smaller sites, such as anonNews.org, CyberWarNews, E-Hacking News, The Daily Beast, and The Hacker News are all lesser known sources, but could arguably be more reliable because they deal exclusively with the cyber community.

Fellow hackers, cyberhacktivists, and general cyber enthusiasts provided Blog posts on Anonymous and hacktivism in general. Sites such as Slashdot, The Hill, ArsTechnica, BetaBeat, AnonymousNews.blog, and Interop all gave detailed information on Anonymous' attacks. Their information would come from message boards; most are aimed for other cyber enthusiasts who are familiar with terms such as DDoS. A message board is typically hosted on a website, the site will have a variety of threads, or topics, and users can respond to each other. BBC published an article giving an overview to message boards in 2012. Message boards allow millions of users around the world to connect. Users have the option to be anonymous or have a username. Anonymous uses the website www.anonnews.org to host their forums. They use these forums to coordinate users on the newest operation.

Online forums run by Anonymous and its members are the main source of information for all of those reporting to the public. AnonNews.org hosts multiple message boards with the manifesto of each planned attack. A typical post contains the intended goal, the target, and sometimes their preferred method of attack. To get a general overview of the effectiveness of Anonymous' attacks, we created a data set that contained every operation hosted by Anonymous in the last three years. When you log onto anonnews.org, you're greeted with a multitude of topics, the most frequent are their upcoming operations. Each operation is connected to a link, allowing you to select that topic. Once the topic is selected, you can read the chronological responses to the original poster. These users can opt to have an identifiable name, which allows other users access to their profiles. These profiles have a history of every submission from the user. Anyone can reply to a comment, engaging in conversation with other users. They also provide links to sources reporting on their actions, and posts of the effects of their operations.

Name	Targets	Goals	Method	Success
#Opsreal	Israeli gvt. Stock market, Finance Ministry	Protesting human rights violations on Gaza	DDoS	Yes, largest losses and significant awareness
#OpLastResort	USSC and DoJ	Disable website, promote 8 th amdt. and reform computer crime laws.	DDoS, Defacement	No, no long term effects.
#OpRollRedRoll	Big Red Football players of Steubenville, OH	Convict the men involved in the gang rape of a young female student	DDoS, Identity	Yes, significant awareness raised

Analysis:

What makes these successful?

- Support base from peers
- Response and retaliation from target
- News coverage and awareness from public
- Embarrassment caused to targets
- Level of damage done to targets
- Completion of goals

Conclusion:

Looking at every attack by Anonymous, it is concluded that they are not successful, although they do have some attacks that are considered successful. With majority of offenses not completed, or having incomplete information, we can only assume they were not successful in completing goals, gaining awareness and change, or costing their targets anything.

Looking more specifically at the three cases, we determined #OpIsrael and the Steubenville Rape successful based on long-term effects of the missions. These all had higher levels of support, similar types of attacks, and the completion of goals set out by Anonymous. In many attacks websites were disabled for a period of days, and Anonymous' efforts even lead to the conviction of two rapists in Steubenville, Ohio. These attacks all had some form of response from the targets, causing embarrassment of the target or causing the target to draw attention to them in attempt react to the attacks.

#OpLastResort is considered ineffective. The lack of response from the targets indicates an unsuccessful attempt from Anonymous to cause major awareness or embarrassment of the target. Although the attack were temporarily successful, they failed to create any long-term effects, such as prolonged website immobilization.