Human-Computer Interaction in Cyber Espionage and Terrorism

Lulzsec: Case Study Part 2

Lulz Security, or Lulzsec, is an offshoot of the hacktivist group Anonymous. A small band of dedicated hackers, they use technology to infiltrate systems and gain sensitive information. Their strategies and process differ extremely from those used en masse by Anonymous, but their basic moral and social structure is basically the same. Anonymous can take credit for far more subtle attacks, setting up protocols for others to protect their right to speak against their own government, for example. Lulzsec on the other hand uses some of the far more blunt instruments Anonymous has become known for, with great success.

The value of Anonymous is that it is a massive crowd-sourced group of potential supporters. A member of Anonymous will point out a problem and another will offer a potential solution. Still another will implement a solution, and still another will make that solution available for everyone to contribute to. This is how Anonymous is capable of such highly concentrated DDoS attacks against large targets. They use something called the Low Orbit Ion Cannon to allow any individual member to simply log on and contribute fire power, in the form of processor space, to overload the servers of a website with repeated requests.

Lulzsec engages in similar types of attacks, but instead of drawing upon an army of willing activists, one member has an army of slave computers that can all be targeted at once. The ethics of such an attack become more questionable when the attacker does not need many voices, or the approval of their peers, to carry out an attack. This lack of accountability is what truly sets Lulzsec apart. They seek to disrupt and destroy, and gain attention for certain causes, but those causes are controversial ones that have not gained the widespread approval that other Anonymous attacks do. In fact, many members of Anonymous argue that Lulzsec goes too far (Knappenberger 2012).

Lulzsec uses a variety of blunt instruments, including DoS attacks using slave computers, to accomplish their goals. They also use more subtle methods, such as SQL injection, where they have to actual find a point of vulnerability in a network system before they can inject malicious code and harvest information. These more subtle tools require quite a bit of “soft” skills to use, such as social engineering. The hackers involved have to locate the most vulnerable points in a network, which can often be the humans using the network. They manipulate these humans into giving them access, and then attack.

There are rumors, from leaked chatlogs, that Lulzsec also used other subtle hacks to exploit vulnerabilities such as XSS and RFI attacks (Poeter, 2011), but many of their attacks are simple and require little skill. For example, the attacks against the Sun Times exploited a known vulnerability to gain access to email information, and also timed a second exploitative attack for a time of IT security maintenance to sneak in under the radar (Arthur, 2011). However, perhaps most disturbing is that we don’t know exactly how many of their attacks were perpetrated. Neither the private companies involved, nor law enforcement officials, have highlighted any security vulnerabilities which were exploited. This seems to be a common response to hacking, as though keeping the secret doors secret will prevent attacks. Arguable, secrecy could simply lead to greater curiosity on the part of other hackers, and greater security measures for those that don’t want to get caught.

There is something to the idea that keeping the vulnerabilities a secret is the only counter-measure. Most of the members of Lulzsec that were arrested, were found because of the activities of Sabu, a member caught and used as a mole for the FBI. Sabu seems to have only been caught because he made a critical error and forgot to log into Tor before posting to Anonymous forums as Sabu one day. Thus, his IP address became traceable and the FBI came calling. If he hadn’t made that one huge, but simple mistake, perhaps none of the hackers involved would have been apprehended. (Arthur, 2013, #2)

The thought that anyone with enough hacking skills cannot be stopped or apprehended, even by government agencies, is a scary one. However, there is something to be said for such protections. Any smart computer user can gain the necessary skills to go undetected, such as using Tor or other IP bouncing programs, and encrypting data. Many believe that average citizens should all automatically have the privacy afforded by these encryption programs, and the fact that they can be used to commit crimes is not an indictment of the tool itself. The question of how to prevent and prosecute actual crime, while also protecting the privacy of average citizens is a difficult one.

Some of the answer lies in how we divide what constitutes crime from merely disruption, protest, and activism. A sit-in at a restaurant counter may be legal, even if done in a large group, but a sit-in at a government building that blocks access is not. Both are forms of disruption and protest. Germany has recently ruled that DoS attacks perpetuated by activists are a form of protected speech, like a digital sit-in (Ball, 2011). Lulzsec was pursued most arduously after they used blunt instrument attacks against the FBI, CIA, Arizona police enforcement, and the UK’s Serious Organized Crime Agency. This is one of the key differences from Anonymous. Anonymous normally does not attack democratic governmental networks, and only disrupts those that have shown some form of censorship or stark removal of citizen freedoms, beyond the silent intrusions of simple monitoring.

Desiring privacy is not an indictment of crime, however, and many of those that legitimately expect privacy, and utilize the appropriate tools to obtain it, are not engaging in any type of crime. For example, a political science professor that studies the social politics behind terrorist attacks, could be subject to strict monitoring because of search history, and could even be searched more regularly at airports because of the types of ideas he searches for. Ideas are not in themselves criminal, but can lead to increased control and monitoring. Someone knowing this may use encryption and server bouncing software to protect their privacy, so that they do not wind up on an FBI watchlist, and subject to scrutiny and increased security. The fault in this case is not with the person reasonably expecting privacy, and using the tools necessary to obtain it, but with a system that denies that privacy.

A person that commits a crime is pursued and prosecuted for that crime, but pre-emptively screening for criminal behavior is a form of profiling, and subject to all manner of biases. One cannot predict that a person is engaged in illegal activity based on their fully legal insistence that they have a right to privacy. And one cannot screen for illegal behavior based on what type of keywords one uses in search history. An organized foreign intelligence with operatives in the US is unlikely to advise operatives to simply google “how to make a bomb” and go to it. The screening process will not find organized terrorists. A person likely to google “how to make a bomb” or “how to DDoS the FBI” is likely a person that is out of means for legitimate, meaningful, legal protest. When legitimate, meaningful protest becomes illegal, protestors simply become criminalized (Ball, 2011).

Lulzsec and other hackers use freely available tools and skills to protect their own privacy, and then use the shade of legitimate privacy to perpetrate security breaches and release information. They are not alone in this. The difference between Lulzsec and many other hacker groups is that they perpetrate these attacks for the attention and publicity, rather than flying under the radar. They seek to show the world what is possible, rather than have the hidden exclusivity of knowledge prevent attacks. Now that it is relatively known that anyone with a certain threshold of skills and information can get away with almost any cyber crime, it seems reasonable to operate under the assumption that one’s data has been compromised unless actively prevented.

Security is now more about how to deal with security breaches that inevitable happen, both on an individual, corporate, and government level, than about prevention. Many organizations run scenarios and actively seek to improve security by encouraging regular breaches and tests of security. (hacker helper article). I think that perhaps libraries need to begin implementing similar systems to ascertain the potential privacy of their information, and assess vulnerabilities. Libraries also need to be on the alert for those that use their public resources to commit cyber crimes anonymously, while still allowing full privacy protections for those everyday citizens.

Some public libraries have fairly strong firewalls and prevent the use of programs that can be used for committing cyber crimes. However, the cost of this denial is that patron privacy is more vulnerable. Those who are aware of the way the government monitors information and communication online are morally entitled to the protections offered by such disreputable services and programs. It is important to strike a balance between preventing potential crime and allowing privacy protections for legally accessing patrons.

Maintaining space for meaningful, effective, and legal protest factors into this as well. Bomb-makers and Lulzsec-type hackers alike are people that run out of options for social disruption. That disruption can take the form of hacktivism, activism through computer disruption. The medium of the internet must maintain some availability for meaningful, legal, disruptive social protest, or illegal disruption becomes the only alternative for protest and social change. Thus, public libraries maintain an important position, as social advocates and shields for both meaningful legal hacktivism and privacy maintenance. As one of the members of Lulzsec said in an interview prior to his arrest “The goal with Anonymous is to brutally cut down the middle of that decision and shout 'NO' to laws we don't agree with. Laws are to be respected when they're fair, not obeyed without question” (Gallagher, 2011).

References:

Arthur, C. (2011, July 19.) How LulzSec hacked the Sun’s website. The Guardian.

Arthur, C. (2013, May 16.) LulzSec: the unanswered questions. The Guardian. <https://www.theguardian.com/technology/2013/may/16/lulzsec-unanswered-questions>

Arthur, C. (2013, May 16.) LulzSec: what they did, who they were and how they were caught. The Guardian. <https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail>

Ball, J. (2011, August 1.) By criminalizing online dissent we put democracy in peril. The Guardian.

Gallagher, R. (2011, July 22.) Inside the LulzSec hacker group. Mail & Guardian

Knappenberger, Brian. 2012. *We are legion: The story of hacktivists.*

Poeter, D. (2011, June 29.) The LulzSec Hacks: How they did them. PCMag. <http://www.pcmag.com/article2/0,2817,2387814,00.asp>