CHAPTER XI

Security Activism

Security activism is similar to penetration/intrusion testing in that the effort is to improve security. Security activism goes beyond mere testing of security, however, to gathering intelligence on crackers and to launch offensive attacks to disrupt online criminal enterprises. This type of reaction could also be perceived as a form of counterattack or hackback. One example, as will be explored in this chapter, is the activist community involved in taking down a botnet.

11.1 Security Activism in Context

Security activism is a curious beast. I often ask people how they would feel about the off-line equivalent, looking at escalating scenarios. First, I ask how they feel about someone walking about the perimeter of their house, on public land, and letting the owner know of open windows, unsecure doors, and other aspects that lend a house less secure. I ask the same question about someone doing this walking on their property to take notes. Things then escalate to someone stepping inside of the house without authorization, through an open door, to observe security defects, then reporting to the owner. Lastly, I cite someone entering the house without permission through an open window, and once inside fixing the security flaws as an act of kindness before exiting. In many ways the above scenarios reflect the work

of how many ethical hackers view cyber security: they are passionate about exposing risks, and protecting and defending systems.

11.2 Case Studies

The case studies look at early security activism against spammers and then move to botnet removal communities. Finally, a case study that looks at how some ethical hackers exposed security flaws and fixed these flaws without authorization is considered.

11.2.1 Spamhaus Project

The Spamhaus Project, a global organization of volunteer guardians in the computer industry, composes blacklists of some of the worst spam propagators, this to aid ISPs and businesses to better filter spam. The company E360insight.com sued the Spamhaus Project in a US district court in Illinois, alleging it was a legally operating a direct-marketing company and should not be blacklisted as a spam provider. Spamhaus did not file a response and did not appear before the court. As such, the arguments presented before the court were unilateral, such that the court issued a default judgment.[1] The court ordered Spamhaus to pay US$11.7 million, to post a notice that E360 was not a spammer, and ordered that the Spamhaus Internet address be removed from the Internet Corporation for Assigned Names and Numbers (ICANN). Spamhaus ignored the ruling, did not pay the money, and did not post a notice on its website that E360 was not a spammer, nor did ICANN remove the Spamhaus website from its root server. In a similar situation, the anti-virus and anti-spyware company Symantec was taken to court in California by a firm that it defines and reports as a spyware company. Hotbar.com claims that the classification of its software as spyware is in violation of trade libel laws and constitutes interference with contract. The suit was reported as settled, with Symantec agreeing to classify Hotbar as "low risk."[2]

11.2.2 Spam Fighter

The US court decision of *Sierra v. Ritz*[3] involved unauthorized use of a DNS zone transfer. Zone transfers are, generally speaking, open-access public information. They provide data about all of the machines within a domain. Without zone transfer, you would literally have to type in an IP (internet protocol) address every time you went to a website—it is one factor contributing to the convenience of

the Internet. The information may be retrieved by the use of "host command" with the "I" option. Zone transfers contain public information to varying degrees, depending on the protocols used by an organization. Zone transfers may be disabled to the greater public with only trusted machines and senior administrators having access on a "need to know" basis. This is a form of limited authorized public access. In Sierra's case, the zone transfer was more widely available in the sense that the system allowed zone transfers to everyone, thereby publicizing potentially private data. There would be no way for a person accessing the zone transfer in the latter context to know whether Sierra was truly allowing shared access or whether it was merely a misconfiguration. From a technical perspective, this is a situation of authorized access to the information found in the zone transfer. From a legal perspective, the judge ruled that access was unauthorized, with emphasis placed on the defendant's intention to obtain and divulge information found in the zone transfer.[4] David Ritz is a well-known anti-spammer. There has been debate as to whether Sierra has facilitated spam in the past. Neither of these two issues appeared to weigh into the decision. While *Sierra v. Ritz* is a civil suit, Ritz was criminally charged with unauthorized access to a computer in North Dakota. Although the charges were later dropped, Ritz lost the civil suit and the court reasoned that "Ritz's behaviour in conducting a zone transfer was unauthorized within the meaning of the North Dakota Computer Crime Law."

The case illustrates how the terms "unauthorized" and "access" do not produce a similar set of shared assumptions in the technical, legal, or ethical fields. A technical researcher may falsely assume that they are operating within safe legal parameters only to discover that such parameters do not translate across fields. The technical researcher would likely assume that he/she is authorized to perform an act where technical protocols and programming convention allow for it. From a legal standpoint, authorization and consent involve a number of factors, including intention, damage, and the bargaining position of affected parties. One commentator on the decision noted that it is the equivalent of, "Mommy, *can* I have a cookie? Sure you can have a cookie, but you *may* not."[5] The case foregrounds a recurring theme: if a user interacts with a server in a way that the protocol does not prohibit but is upsetting to the server's operator, should this be construed as "unauthorized access" as a matter of law?[6] The scope of unauthorized access in computer-fraud statutes is an

old question.[7] Whether or not this would constitute a "hack" is one question, and if it is a "hack," then surely the motives appear to be somewhat ethical.

11.2.3 Botnet Removal Communities

There exists a number of undocumented independent research communities that were (or still are) actively involved with botnet-harm mitigation, interdiction, counterattack, and takedown. This may include attempts by the C&C source to program and reprogram its bots, altering payloads of malicious applications delivered on botnets, and launching a denial-of-service attack on C&C servers.[8] The Offense-in-Depth Initiative (OID) was launched in 2008 as a group-targeted approach to fighting cybercrime. OID is comprised of volunteers who work within smaller subset groups dedicated to botnet countermeasures. Each subgroup specializes in one particular botnet. So, for example, there were the OID-Kraken and OID-Torpig small working groups targeting the Kraken and Torpig botnets. The main goal of the OID teams is to erode the profit model of specific major cybercriminals, while obtaining intelligence for use by law enforcement.[9] Each specialist subgroup divides their roles into reverse-engineer operations specialist, coder, social-engineer linguist, and information warrior. In some instances the same person could fulfil multiple roles, and in other instances the roles are somewhat superficial.

The group's aim was to form small working groups, singling out one botnet or criminal operation, with the purpose of long-term disruption (OID has since disbanded). Other small independent research groups have performed countermeasures for a few weeks or a month, then the countermeasures stop, allowing the criminal operation a chance to regroup and get back to "business as usual."[10] OID's focus was on long-term countermeasures aimed at disrupting the profitability of the botnet operations. Whether a cybercriminal continues operating depends on many factors. OID has singled out three major factors: complexity of the operation, risk of getting caught, and reward/profit of the crime.[11] OID uses methods aimed to increase the complexity of the criminal's organization, forcing them to spend more time, effort, and money into maintaining their criminal operations. For instance, techniques include subverting the C&C or by either increasing or decreasing the size of the botnet. There has been some research done on optimal botnet size for certain types of

activities.[12] Compromised machines can be remediated so that they are no longer part of a botnet. If you remediate enough machines, the size of the botnet becomes untenable for criminal operations. Likewise, if you grow a botnet from 100,000 to 10,000,000 it becomes difficult to effectively manage the botnet without constantly writing new instructions for the C&C. The botnet master ends up spending extraordinary amounts of time and effort to control the bots. Just as one person may only successfully tend to a set amount of sheep or cattle within a set amount of land, an increase in the size of the herd requires more land, water, and labour. Similar to caring for livestock, taking care of botnets is often referred to as "herding" bots.

When a botnet's operations are interrupted, it may create the need for more complex operations in order to adapt to the new environment. In the case of botnets, if the complexity becomes too great for the criminal, more expertise may be needed in the form of hiring a programmer to develop new encryption methods or programs. It is believed that, in turn, this forces the cost of business to rise. It is hoped that if the disruption is continuous and that costs of doing business rise so that profitability will be reduced, then this will correspond with a lower level of criminal activity. There is no evidence to suggest that this has worked to date. Botnet activity remains a growth industry. Nonetheless, this is, or was, the belief of groups such as OID. As stated in the OID mission, it is about long-term disruption. It may be too early to ascertain whether such countermeasures are effective.

OID tactics were decided by looking at effectiveness, stealth, ethics, and ability to avoid collateral damage to third parties. Such an approach to tactics is not an official code but represents a rough understanding between members of the group.[13] Ultimately what tactics are used depends on the decisions of the specialist group. While the operations of the OID groups were not openly discussed, many of its operations had involved working with select individuals who worked for computer-security companies. Such companies, unlike OID, often make information on botnet infiltration and countermeasures taken against a botnet available to the public. This was the case with the Kraken botnet, which OID members infiltrated and took down in December of 2008. OID members have not publicly discussed how the botnet was taken down. Researchers with the security corporation TippingPoint, however, have provided publicly

available information about the Kraken botnet and the infiltration process available from their security blog.[14]

Researchers at TippingPoint infiltrated Kraken by starting with a sample of the code provided by the company Offensive Security. The various protocols of the botnet were noted. The C&C instructions were encrypted. Researchers had to reverse engineer the computer code, which entailed decrypting the encryption routes. TippingPoint created a fake server (often referred to as a sinkhole) to redirect Kraken traffic. TippingPoint played a somewhat passive role in that they did not rewrite instructions and send alternative instructions via the C&C. In their words, "we are not talking back to any of the Kraken zombies that are phoning home to us. We are simply listening passively, decrypting the request and recording statistics."[15] As such, they were able to then redirect traffic to their server. Researchers at TippingPoint recorded the list of all uniquely infected IP addresses and applied a reverse DNS lookup to ascertain what types of computers and locations of IP addresses were part of the botnet. The majority of the compromised computers were home broadband users, with compromised devices predominantly based in the United States, Spain, United Kingdom, Colombia, Mexico, Peru, and Chile.[16]

TippingPoint wrote an update code capable of cleaning up the compromised computers of Kraken. They have even provided a video demonstrating their capability of removing the Kraken botnet altogether. TippingPoint researchers have not cleaned up the botnet for ethical and legal reasons, chief being that there is no security-research exemption in criminal law.

11.2.4 Cyber-Security Researcher Y

The identity of this cyber-security ethical hacker remains anonymous. He wants his story to be shared, but not his identity. He discovered a serious critical vulnerability in an organization's system. He identified and developed a correction for the security vulnerability. Instead of notifying the organization of the vulnerability, or asking for money for the information, he chose simply to patch the vulnerability as an act of benevolence. The vulnerability would have otherwise allowed hackers to gain unauthorized access to a variety of data. Curiously, this researcher was in the habit of quietly fixing the vulnerabilities of other's systems. After seeing other researchers charged with criminal offences for the mere discovery of security

vulnerabilities, researcher Y decided to give up such activism. While I cannot say how prevalent this type of security activism is, I can say that I have heard of many hackers who have performed similar deeds.

11.3 Observations

Self-organized security communities recognize that there is great need for action to alleviate the inept legal and regulatory systems in an attempt to reduce cybercrime. When viewed in this light, the work of self-organized communities may be seen by those involved with these communities as "doing justice" where justice has otherwise proven to be non-functioning.

The motto To Do Justice[17] is potentially applicable to both self-help security communities and botnet communities. There is, for example, mounting evidence that eastern European communities have likened Internet crime such as fraud to a legitimate activity—Robin Hood stealing from rich Western countries to give to poor developing ones. Many types of malware and botnets for hire are now distributed with end-user license agreements, and some have even been registered for copyright protection. Conversely, anti-botnet communities have justified breaking the law where required to achieve justice. The motto To Do Justice parallels the actions of many self-organized security communities who are "fighting malware and botnets" under the motto of Doing Justice in the absence of effective regulatory responses to the problems. In fact, regulation may never effectively deal with botnets. The point is, rather, that the perception of the absence of regulation or the presence of ineffective regulation motivates people to take matters into their own hands.

Main targets vary for security activists. In some instances, the target might be simply to gather intelligence in a honeypot. A honeypot is a network that is set up to detect and collect network traffic. A honeypot is often set up to lure cyber attackers, detect malicious software, and may even deflect and protect against such attacks. In other instances, the target may involve actively taking down a botnet, or removing malware from infected websites, or sending information to companies whose security has been compromised, to collecting information and handing it over to law enforcement.

Targets are either performing illegal criminal functions (running a botnet, stealing credit-card information) or they are organizations whose security practices are poor (and often not fully compliant

with security standards). The underlying link between target and motivation is inept security and the ability to exploit vulnerabilities.

Security activists almost always have excellent computer skills. There is no one set of hacker ethos that applies to all hackers, though anecdotal evidence and the opinion of Dreyfus highlights that expert security activists share a common set of ethics that can be best described as responsible engagement.[18] This does not, however, imply that all actions are within the law. Security activism and research is a grey, murky area of the law.

It is difficult to qualify or quantify perceptions without empirical research. Nonetheless, my observations from my research and with interviews of cyber-security experts is that they are highly skilled individuals who are acutely aware that what they are doing is illegal in many jurisdictions, but that they view their activities as necessary and ethical. For example, university researchers investigating the Torpig botnet invaded the privacy of those individuals whose computers had been compromised in order to gain intelligence about the botnet propagation trends. They did so without consent of the computer owners and in clear violation of the law. Law enforcement was notified of these violations but did not press charges. If anything, they condoned the actions.[19]

As a general proposition, security activists are not deterred by the law; frequently, the law turns a blind eye and thus encourages ethical hacking for these purposes. Security researchers are imperative in any initiative to combat cybercrime. For example, there has yet to be a single takedown of a botnet that did not involve cooperation from a number of entities, including security researchers from specialized security-software companies and universities, ISPs, DNS providers, and often law enforcement—these parties are routinely located in different parts of the world.

There have been few incidents where security activists have been the target of criminal investigations, though there have been many security researchers who have been threatened with criminal sanctions. There have, however, been several instances of civil lawsuits against security activists. Two of these civil (quasi-criminal) cases are discussed below.

Exemption from liability and criminal prosecution has been argued for application to security researchers and for acts that threaten to cross technical and accepted protocols. A resounding question underlies the debate: do the ends justify the means?

Examples might include the recording industry's proposal to hack into users' computers to find infringing material, and cyber-activists placing "Trojan horse" software on child-pornography sites, embedded within digital images, to track and record the contents of offenders' hard drives for evidential purposes. These examples go to the question of intent as well as whether an act may be justified as a social utility for the good of the public, similar to how public-interest exemptions work for the admissibility or otherwise inadmissibility of evidence in court.

For example, if one argues that David Ritz had indeed accessed the zone transfer without authorization, inevitably one must question his motive, intent, and whether such activities were performed in the public interest. Peering into the zone transfer to document illegal spamming activity may indeed be in the public interest. If one successfully concludes that no unauthorized access was performed due to the public nature of the zone transfer and DNS, it seems equally perverse to not consider motive and intent. By way of analogy, if I have equipment to make fake passports, along with a stack of 200 UK passport shells, the trajectory toward the commission of a crime is called into question. Accessing information in the zone transfer for illicit purposes should attract attention, if not a penalty. The implication, however, of criminalizing an act of accessing publicly available information without illicit intent calls into question the utility of "unauthorized access" provisions. The inconsistency of the courts' interpretation of "unauthorized access" makes the use of the provision unpredictable as well as malleable to prosecutorial will. The scope of "unauthorized access" is ripe for reconsideration and debate.

There is no public-interest exemption for computer offences. A public-interest exemption refers to unauthorized access, modification, or impairment where it is in the public interest to break the law. Typically, this might relate to security research, but there are other instances that go beyond mere research which may justify the law being broken. There are reasons to allow for a public-interest exemption, though these reasons are not sufficiently compelling at this point in time as to open up the exemption beyond security research. The idea of a public-interest exemption, however, should be given further consideration by governments.

Notes

1. *E360 Insight, LLC et al v. The Spamhaus Project.*
2. Messmer 2006.
3. The judgment is unreported. A copy of the decision is accessible from private listservs as well as from the webpages of SpamSuite.com. See *Sierra Corporate Design Inc. v. David Ritz.*
4. A detailed analysis of the case can be found on SpamSuite.com available at http://www.spamsuite.com/node/351.
5. Rash 2008.
6. Original idea expressed by Paul Ohm in the CyberProf listserv.
7. Kerr 2003.
8. Smith, B. 2005.
9. Observations from email correspondence with members of the OID Initiative. From 2009–2010.
10. Internet Security Operations and Intelligence (ISOI) is one such group. Members complained of the unfocused, ad hoc short-term approach of ISOI.
11. Observations from founder of OID in listserv correspondence.
12. Li et al. 2009.
13. Observations from Listserv correspondence.
14. TippingPoint 2008.
15. TippingPoint 2008.
16. TippingPoint 2008.
17. Tamanaha 2001.
18. Interview with Dreyfus, December 2010, Sydney, Australia. Chiesa, Ducci, and Ciappi 2009.
19. TrustDefender, "In-Depth Analysis."