UNRAVELING ANONYMOUS INTERNET CRIMINAL NETWORKS: LESSONS FROM A CYBER DEFENSE TEAM

Gina Vega
Salem State University
Benjamin Ngugi
Suffolk University

The Cyber Defenders

September, 2010. The mood in the big barn in Vermont was solemn. Bob and Garth Bruen, the cyber defense team, sat at their desks, each lost in thought about the decision they needed to make. They had just won their first Herculean battle in the fight to unravel an Internet criminal network. They had forced eNom, one of the biggest domain name registrars, to remove several illicit pharmaceutical domains; however, they were worried that the network would grow another of its ugly heads, just like the Hydra of Greek myth. They knew that this was just the beginning of the war against cybercrime. There were many more battles waiting to be fought and many more criminal organizations that needed to be dealt with. They were not sure that they were fully equipped to deal with the increasing security threats from criminals like the ones they had just ousted. They needed to orchestrate more resources in terms of volunteers and money needed for a full blown war against cybercrime. They had mostly supported the effort to fight cybercrime by taking time away from their paid consulting to do this work *pro bono* but more was now required. There was so much to think about… The silence was broken only by the humming of Bob's computer servers. They now needed to address the question: How could they make more significant inroads in the fight against cybercrime? What direction was likely to have the greatest impact? They looked back at growth of Internet crime and the long, complex path to the end of the current battle.

Growth of Internet Crime

The twenty years from 1990-2010 have witnessed an unprecedented growth of computers. As predicted by Gordon Moore (co-founder of Intel), computer speeds have doubled approximately every eighteen months, CPU prices continued to drop and network speeds had also been increasing [Moore, 1965]. The Internet has grown in tandem with the growth of computers to unprecedented levels. For example in North America "344 million citizens, which is 77 percent of the total North American population, use the Internet" [Internet World Stats, 2010]. The flip side of all this progress is growth of Internet crime. For example cybercrime in the US grew by 22.3 percent between 2008 and 2009 [Federal Bureau of Investigation and Internet Crime Complaint Center, 2010]. Further increasing amounts of the malicious activity is shifting to emerging economies with China, Brazil, India and Russia within the top ten countries [Symantec, 2010].

Bob and Garth's Mission

Bob Bruen had worked in computer security for years, managing systems and networks at MIT. MIT, like most large, prestigious institutions was frequently under cyber attack, and this gave Bob firsthand exposure to virtual criminals. In the early 2000s, Garth Bruen, Bob's son, was working for the Commonwealth of Massachusetts and was frustrated with the inundation of spam his department was receiving. How many times could he receive the Nigerian Prince letter (known in the industry as Scam 419) without reacting? He decided to fight back against the spam criminal networks using an old, underutilized approach, and Bob helped him get started. The method he used was simple:

1. Look in the spam email for the name of the spamming site;

2. Use the WHOIS tool to check the owner of the site. (WHOIS was a program that asked a domain name to identify its owner and returned that identification to the person who sent the query).

3. Report any inaccurate information like a fake email, phone number or address by filing a complaint with ICANN (Internet Corporation for Assigned Names and Numbers). ICANN was an international not-for-profit partnership that coordinated the Internet's domain name system (DNS) to help avoid confusion and ensure that each Internet participant had a unique identifier.

4. ICANN would in turn forward the complaint to the registrar of the site (the organization appointed by ICANN to issue IP addresses to business organizations and the public). The registrar was required by the contract with ICANN to suspend the registrant's domain name unless the latter fixed the problem.

Garth was successful in cutting his spam by 99 percent because most spammers used fake contact information. He was amazed to see the big difference that this simple change made and decided to start writing code to automate this process. In 2003, Garth launched a new organization to fight junk email in earnest. Bob and Garth dreamed of a new world with no email junk, hence decided to name the new organization "KnujOn" (pronounced nu-jon). The name was derived by reversing the letters in the "no junk" dream message (see www.knujon.com) . Garth led the initiative, and Bob built up the facility, wrote and presented papers at conferences, and handled the large amount of positive feedback and publicity they received. He often received invitations after a speaking engagement to speak elsewhere, and the project grew. Bob's friends introduced Garth to the different government agencies involved in the Internet. Garth was passionate about cleaning up the problem, Bob helped him, and they were successful. They had a strong sense of justice, ethics and social responsibility. They sincerely believed that the only way to get the Internet cleaned was for someone to decide to take it on and follow through. They would be the cyber defenders who could do it, as an adjunct to their for-profit technology security consulting.

The pair cared intensely about keeping illegal activities off the Internet. They feared the Internet could be used as a weapon to make it easy for any business (or individual) to do something wrong and hide it. (See Exhibit 1 for stakeholder information). Anything you could do was transmitted around the planet in a few seconds. The Internet was a rapid and broad communication, a many-to-many medium, unlike radio and TV, which were one-to-many…And, by the same token, criminal elements could hide right in plain sight because they lived with the same privacy protections as the rest of us. Bob and Garth tried to figure out how they could "out" the Internet criminals while protecting the Internet innocent and set up a not-for-profit organization to lead the process (see www.knujon.org).

ICANN, Law Enforcement Agencies, and Protection of the Internet

Bob and Garth started familiarizing themselves with ICANN working protocols. If a person wanted to establish a website, the first step was to check the availability of the preferred domain name with one of the registrars. The registrar would provide the domain name rights to the purchaser if the domain name was available. The domain name and associated IP address was an entry in the Domain Name Server. Appointed registrars had to sign a contract called an RAA (Registrar Accreditation Agreement) with ICANN specifying the rules and regulations to be followed by the registrar in assigning and withdrawing domains [ICANN, 2011].

However, some of the Internet players were creating problems, beginning with criminal networks that were trashing the Internet with spam. According to a Symantec report, 90 percent of all email was spam [Whitney, 2009]. Spam was followed by other criminal activities like selling of counterfeit pharmaceuticals drugs, pornography and identity theft. The structure of the Internet made it very difficult to catch the perpetrators. US law enforcement agencies like the police and the FBI (Federal Bureau of Investigations) had tried shutting down these sites. However, new websites selling the same illegal goods would crop up soon thereafter. Domains that originated spam were often terminated quickly, but name servers received a fresh group of domain names nearly as quickly as the others were closed. The law enforcement agencies also tracked down the sites' owners, but their trails would disappear into other countries where such activities were either not illegal or not a priority.

The problem was complicated further because the criminal networks were hiding their identities. The owner of any domain could normally be identified by querying the identity of the owner using the "WHOIS" tool. This provision gave the public and the law enforcement agencies the ability to verify the owners of the domains that they were dealing with. However, criminals were using privacy anonymity schemes to hide their identification names and remain anonymous to the authorities. This was done most frequently by using the "WhoisGuard" service [WhoisGuard.com, 2011]. This replaced the identity and contact details of the actual owner of a domain with those of the WhoisGuard service provider. As a result, all the customers of such a service, numbering in the thousands, would have the same generic provider's identity as a proxy name placeholder. This gave the criminal networks a cover from which they could execute their criminal activities while remaining anonymous and unaccountable to the public, contrary to the original intention of Internet administration. This practice was protected under the concept of net neutrality, a policy whereby all users were entitled to participate fully in the Internet without restrictions as to content or sites, among other things, and this generated huge debate. Please refer to [Berners-Lee, 2006] for one side of the debate and to [The Editors, 2010] for the other side.

The law enforcement agencies simply could not keep up with the criminals. They were poorly equipped and outnumbered. On the other side, the criminal networks were well financed [Broadhurst, 2006] and were constantly changing names and the mode of operation. This made them a moving target for the law enforcement agencies.

It also seemed that ICANN, the institution that was responsible for monitoring the technical side of the Internet, including identifying legitimate and illicit transactions was unable to control the criminals either. By contract with ICANN, any US registrar was required to repossess a domain name from anyone who was committing a crime. However, ICANN was a standard setter and not involved in actual Internet governance [Johnson and Crawford, 2011].Thus, criminals were able to set up operations within the legitimate infrastructure with very little resistance from other operators—and none from within the legitimate infrastructure itself.

“Outing” the Criminal Networks

The Bruens felt that something had to be done or the criminals would take complete and irrevocable control of the Internet. They brainstormed and struggled for months to find a practical solution. They realized that the various Internet crimes like spam, rogue pharmaceutical sales, identity fraud, online pornography, gambling etc shared several common characteristics. First, spam was used to advertize the different crimes to unsuspecting consumers. Second, the criminal networks would constantly change their domain names (websites) to keep ahead of the law enforcement agencies. What was needed was a versatile strategy that could be reused with the different Internet crimes. This suggested that the strategy needed to leverage some common characteristics. Then it occurred to them that there was one single, but very important, key that others were ignoring, and this key might help with any of the cybercrimes in unraveling the criminal networks.

Although the criminal networks could afford to change their domain names frequently, the supporting supply chain infrastructure behind the scenes remained intact and stable. For example, the criminal networks needed access to a new supply of domain names as they went through the different metamorphoses, therefore they needed stable domain names providers. They also needed stable payment processors to accept electronic payments transactions, otherwise the expense of registering domains, deploying malware and sending spam would have been in vain. Unraveling illicit traffic was all about identifying backend transactions providers and not about products which could change at any time. The law enforcement agencies failed to overcome the criminal networks because they concentrated on the products instead of the common transactions’ providers. The cyber defenders felt that the best strategy for unraveling the criminal networks was to follow the supporting infrastructure and transactions. For example, they could investigate the source of domain names. They knew that for the criminal networks to acquire domain names they needed access to registrars, and the registrars could not hide.

Testing the Strategy: Unraveling Criminal Internet Pharmacies

KnujOn decided to test its strategy with one line of criminal networks – illicit pharmaceutical drugs. If successful, they would later reuse this strategy on other cybercrimes. Illicit sale of pharmaceuticals became their first target because the amount of money flowing to the criminals was substantial. It was also an easy target because the law was very clear: you had to have a face to face meeting with a physician in order to get a prescription. After the death of an 18-year old athlete and A- student from an overdose of prescription drugs purchased over the Internet, the US Senate mobilized to enact legislation to protect consumers from purchasing controlled substances without a visit to a physician. The resulting Ryan Haight Online Pharmacy Consumer Protection Act [2008] was applicable even if the prescription was to be filled in an online pharmacy. Further, illicit online sale of drugs denied tax revenue to the government, withheld profits from genuine pharmaceutical companies, and exploited the poor by pretending to offer cheaper drugs while in reality their genuineness and efficacy could not be ascertained. Some sites even pretended to be offering cheaper drugs to help the poor from paying unreasonable government taxes on top of the unreasonable profit margins charged by the big pharmaceutical companies but failed to mention the fact that they themselves were in the business to make big illicit profits. Bob and Garth decided to take on one of the most notorious illegal pharmaceutical networks to test their theory. See Exhibit 2 for the law enforcement agencies with a stake in Internet crime.

eNom, the Most Notorious of Them All

They started by analyzing all the registrars and checking for interesting patterns in the registrars' allocation of domain names to the criminal pharmaceutical networks. An independent audit of ICANN registrar adherence to the RAA uncovered a disturbing trend—162 registrars were potentially in breach of their contracts for non-trivial activities. These activities ranged from blocking and manipulating WHOIS access to falsifying applications and knowingly facilitating criminal traffic.

One of the worst offenders was eNom, a domain registrar that had a reputation of providing domains for illegal drug activities. KnujOn had had eNom in its sights for several years, but they had not been successful in shutting them down. According to KnujOn [KnujOn, 2010], eNom became an active facilitator of illicit criminal activity by providing the domains. In December of 2009, eNom received a letter from LegitScript (a private consulting company working with the National Association of Boards of Pharmacy) that described the activities of a "rogue Internet pharmacy" and summarized eNom's own activities in this area, suggesting that they were an accessory to these crimes. Similar letters arrived from pharmacy boards across Canada and from several US states during December 2009 and January 2010. eNom did not respond to any of these accusations.

Bob and Garth were outraged at the flagrant disregard of laws and abuse of Internet freedoms. They concluded that eNom was facilitating illegal drug sales and putting at risk the lives of innocent purchasers. eNom's various pharmaceutical domains were selling not only "lifestyle" drugs like Cialis and Viagra, but also drugs with serious health implications, such as various controlled substances. eNom could not deny its role in this process, as the domains they were registering had suspicious names such as "*noprescriptionpharmacy.biz*" that made clear their violation of dispensing of prescription drugs without a formal prescription. Four thousand rogue Internet pharmacies were operating with impunity under eNom's domains. Even after being made aware of the abuses, eNom permitted the domains to continue operating [Armin, 2010.]

The issue was complicated by the fact that eNom had resellers selling some of its domains coupled with the "WhoisGuard" anonymity service and thus hiding the true ownership of some of the sites. Hiding the domain ownership protected eNom from complaints and from legal recourse. KnujOn believed that eNom was deliberately shirking its responsibilities to customers and putting them at risk.

In June 2010, KnujOn went public with its findings at ICANN's annual meeting in Brussels, Belgium [KnujOn, 2010]. The results were predictable: eNom denied the allegations.

Demand Media IPO

Initially, KnujOn's struggles with eNom did not seem to produce results. On the contrary, in their efforts to shame them publicly they seemed to have helped eNom acquire new customers by increasing the latter's name recognition. Demand Media, an online media content company purchased eNom and was planning an IPO when KnujOn released its list of Top Ten Worst Registrars in June 2010 [KnujOn, 2010]. Demand Media made a half-hearted blog attempt to discredit the report and filed its IPO intent [U.S. Securities and Exchange Commission, 2010] on August 6, 2010, only to be met with resistance from bloggers everywhere to the tune of well over 300,000 postings a day for several weeks. In the section in the filing statement about risk factors for the future, Demand Media failed to mention the potential downside of eNom's criminal activity.

The pressure on Demand Media continued building with the Security Exchange Commission, and the continuous press coverage made potential investors start paying attention. To add to this pressure, a lawsuit [Sandoval, 2010] was filed alleging that Demand Media was spying against online users using a service called *addthis*. *Addthis* produced zombie cookies, that is, cookies that were regenerated after the end user deleted them without the user's knowledge. This served to further erode Demand Media’s reputation on top of the earlier bad press on eNom omissions.

Further, Kurt Pritz, a senior vice President of ICANN, indicated publicly [McMillan, 2010] that ICANN would ask Demand Media to respond to charges made by KnujOn and repeated by HostExploit (a volunteer-run anti-malware research group). The troubles for Demand Media did not stop there. They got worse when Andrew J. Klein, White House Senior Advisor for Intellectual Property Enforcement called ICANN, Demand Media representatives and other questionable registrars for a meeting to discuss ways of cracking down on companies selling counterfeit drugs.

All the pressure from different quarters eventually forced a change for the better. Just before Labor Day 2010, eNom contacted Legitscript (verification and monitoring service for online pharmacies) and indicated they would start removing verified illicit pharmacy domains. eNom was not the last registrar that needed to conform to the law and good practices, but they were the last of the largest registrars to do so.

Demand Media amended their S-1 filing and stated that eNom had made an arrangement with Legitscript to verify the legitimacy of online pharmacies which had or wanted to have a domain name registered with eNom. Those sites that were not verified lost or would lose their domain name. eNom would be held to strict standards and monitored.

Lessons from the First Battle

The joy in the big barn in Vermont was restrained. Bob and Garth were pleased that they had won the first battle with Demand Media. However, they were under no illusions. They had learned several important lessons: They knew that this was just one of many battles that they had to fight to rid the Internet of criminal networks. And they knew it was going to be risky, on a personal and a professional level.

A significant challenge to law enforcement was the “Wild West” atmosphere of the Internet itself. The laws that governed everyday life were rarely enforced on the Internet. Further, criminal networks were exploiting and hiding behind anonymity tools meant to protect individual consumers. Criminals were thus able to function with impunity, because their confidentiality was protected to the same extent as the consumer’s. In order to protect the customer, the Internet would have to suspend its freedoms of operation. But without freedom of operation, the Internet would not function. And without privacy protection, all consumers were at risk. Was there a way to shift the vicious cycle to a virtuous cycle?

Ironically, the freedoms of operation permitted counter attacks to KnujOn by supporters of "free trade" (illicit drug sales) and others. Garth was the subject of numerous personal attacks on his blog, being accused of being a "busybody" and "in a huff over what is essentially a victim-less 'crime'"[Bruen, 2010]. The hostility on the blog was very much in evidence in many of the postings, but KnujOn's primary weapon was only social shaming, using the very technology that permitted the illicit behavior to try to control it in some way. However, with no formal, legitimate backing Bob and Garth had few options to support pursuing their agenda: encouraging ICANN to issue breach notices to registrars in violation of the RAA forcing overall compliance with WHOIS regulations was all they could do to protect the consumer from Internet fraud. They were worried that they had gone as far as they could go in their fight.

However, they had learned from the first battle that they were not alone. They had learned they could use the Internet to mobilize hundreds of bloggers for a just cause. They knew they could force the law enforcement agencies, and even the White House, to recognize that the criminal networks could bring down the Internet if left unchecked. The war against Internet crime was just beginning, and they were on the front lines. Now, Garth and Bob needed a plan of attack, not just a strong defense. How could they gain the upper hand against the cyber criminals while protecting both privacy rights and anonymity? Was government agency support the key? Would harnessing the power of the social networks be the most effective route? They only thing they were sure of was that going it alone was not the answer.

References

Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.

2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. The authors of the Web pages are responsible for the accuracy of their content.

4. The authors of this article are responsible for the accuracy of the URL and version information.

(2008) Ryan Haight Online Pharmacy Consumer Protection Act of 2008, in *H.R.6353, 110th US Congress*.

Armin, J. (2010.) *Demand Media–eNom: the World's #1 Bad Host and Abusive Registrar. Technical report, HostExploit*.

Berners-Lee, T. (2006) "Net neutrality: This is Serious," http://dig.csail.mit.edu/breadcrumbs/node/144 (June 6th, 2011).

Broadhurst, R. (2006) "Developments in the Global Law Enforcement of Cyber-crime," *Policing: An International Journal of Police Strategies & Management* (29) 3, pp. 408 - 433.

Bruen, G. (2010) "When Registrars Look the Other Way, Drug-Dealers Get Paid," http://www.circleid.com/posts/20100504_when_registrars_look_the_other_way_drug_dealers_get_paid/ (June 13th, 2011).

Federal Bureau of Investigation and Internet Crime Complaint Center (2010) "2009 Internet Crime Report," http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf (November 17th, 2010).

ICANN (2011) "Registrar Accreditation Agreement-2009 Version," http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm (April 1st, 2011).

Internet World Stats (2010) "Internet Usage Statistics-The Internet Big Picture," http://www.internetworldstats.com/stats.htm (November 17th, 2010).

Johnson, D. R. and S. P. Crawford (2011) "What's Wrong with ICANN and How to Fix It," http://www.icannwatch.org/archive/whats_wrong_with_icann.htm (April 1st, 2011).

KnujOn (2010) "KnujOn Internet Security Report: Audit of the gTLD Internet Structure, Evaluation of Contractual Compliance, and Review of Illicit Activity by Registrar," http://www.knujon.com/knujon_audit0610.pdf (June 1st, 2011).

McMillan, R. (2010) ICANN Asks Demand Media for Answers after Report, in *Computer World*.

Moore, G. E. (1965) "Cramming more Components onto Integrated Circuits," *Electronics* (38) 8.

Sandoval, G. (2010) Suit Alleges Disney, Other Top Sites Spied On Users, in *Cnet*.

Symantec (2010) "Symantec Global Internet Security Threat Report: Trends for 2009," http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf (November 15th, 2010).

The Editors (2010) Net Neutrality Is Anti-Consumer, in *National Review Online*.

U.S. Securities and Exchange Commission (2010) "Demand Media IPO Filing Registration Statement," http://www.sec.gov/Archives/edgar/data/1365038/000104746910007151/a2199583zs-1.htm (June 1st, 2011).

Whitney, L. (2009) Report: Spam now 90 percent of all e-mail, in *Cnet*.

WhoisGuard.com (2011) "What is WhoisGuard™?" http://www.whoisguard.com/ (April 1st, 2011).

Exhibit 1 Stakeholders

Stakeholder	**Interest in Internet Security/Privacy**	**Role in Security/Privacy**
ICANN	Mandate to monitor the Internet	Responsible for monitoring but not enforcing Internet technicalities
Registrars	Want security, less concerned with privacy	Issue domain rights to all comers; required to repossess domains from violators but without formal regulations in force
Criminal networks	Want security to operate freely	Completely unregulated activities in the criminal realm
Individual users	Want privacy and also “freedom”	Easily taken advantage of

Exhibit 2 Law Enforcement Agencies with a Stake in Internet Crime

The drug industry was regulated in the US by the federal government. Some of the US agencies that had an interest in illegal Internet pharmaceutical transactions included the Food and Drug Administration (FDA), the Drug Enforcement Administration (DEA), the Department of Homeland Security (DHS), Health and Human Services (HSS), the Department of Commerce (DoC), and the Federal Trade Commission (FTC).

Each of these federal alphabet soup agencies controlled one element of the pharmaceuticals industry, but there was no single entity that coordinated the activities of the individual agencies. Jurisdictional challenges posed many logistical roadblocks for the FDA, the agency with primary responsibility for drug sales, especially for drugs sold through websites originating from other countries where US agencies had no enforcement abilities. This large number of uncoordinated regulators raised several security and privacy concerns in the US and left Internet shoppers at the mercy of the criminals.

AGENCY	INTEREST
FDA	Product regulation to ensure the safety of foods, drugs, biological products, medical devices, cosmetics, and radiation-emitting devices
DEA	Targets drug trafficking within the US
DHS	Protection from cyber attacks on corporate sites, spear phishing, and social media fraud
HSS	Protecting victims of human trafficking and privacy of health records
DoC	Sale of prescription drugs over the Internet in the US
FTC	Mass marketing fraud