Project KnujOn

Garth Bruen http://www.knujon.com
Dr. Robert Bruen http://www.coldrain.net

This white paper is intended to present the KnujOn Project(knujon.com) and Internet security related issues. It is not overly technical but does contain telecommunications, Internet, security, law enforcement, and business concepts as well as current economic and global affairs that require a diverse background to be fully appreciated. However, KnujOn itself is meant to be accessible to all interested parties. Our goal is to help as many people and communities as possible. KnujOn is an effort to combat email abuse and Internet fraud in creative ways that bring all interested parties to the table. The paper has three main sections: 1. An overview of the problem, 2. Why other methods have failed, and 3. a review of Project KnujOn.

I. Problem

Anyone reading this is probably somewhat familiar with the issue. The problem as it stands today is that 90% of all email traffic is spam (1). Employees in the U.S. spend about 100 hours each year dealing with spam, a daily loss of $130 million to our workforce (2). The loss of productivity on the company side is estimated at $712 Per Employee, and $71 billion to all U.S. businesses annually (3). But this is not only about the email. In fact, we assert that it has less to do with the email than other issues we are about to discuss.

Spam works. It is that simple, and that is why we continue to see it. The chances of getting caught, prosecuted and punished are miniscule in comparison to the potential wealth. According to a Consumer Reports survey 650,000 people purchased at least one item sold through a spam advertisement in a single month (4) If the average spam "unit" is $75,that is $48,750,000 per month or $585,000,000 per year. While the majority of Internet users may be blocking and deleting spam, the remainder keeps the spammers employed.

The threat is escalating. Cybercriminals are launching massive Distributed Denial of Service attacks (DDoS) against anti-spam services. Worms have been designed to specifically attack anti-virus software companies (and specific people). DDoS and hacking attacks have been used against law enforcement networks as revenge and are growing.

Beyond threats on the Internet itself, cybercrime is playing out in the real world, as well. Malaysian media pirates have threatened police and Customs Service dogs (bounties have been placed on specific animals). Recently, an imprisoned spammer tried to hire a hit man to kill the family of a witness. Journalists investigating counterfeit product networks in many countries have been murdered. The criminal threat is much more aggressive than ever before. Targeted attempts to intimidate and disrupt enforcement for the purpose of protecting lucrative criminal operations are commonplace. As the spam money grows, so will the physical threats.

Compounding these threats are enforcement agencies that claim a lack of technical resources and personnel, with the current investigators facing insurmountable backlogs of data. Add to this the prospect of cyber attacks between nations becoming commonplace and we are all in for a rough new century. KnujOn is interested in the problem and what is driving it.

Illicit Products and Traffic

Before 1990, global illicit traffic represented a small, flat percentage of worldwide commerce. Since the birth of the Internet, the traffic in counterfeit, stolen, and pirated goods has doubled and continues to grow

at a shocking rate. Illicit traffic is now a $600 Billion industry(5) The underground economy is booming. While many factors contribute to this increase, dangerous junk products and fraud are reaching previously untapped victims through spam and fake websites. The extent of this problem shows up in other sectors. For example, 210,000 American manufacturing workers could be added to the economy if parts were made legally (6). The E.U. figures 100,000 jobs are lost annually because of product counterfeiting (7). If the knockoff network were a single company, it would be twice the size of Wal-Mart (8). If counterfeiting, smuggling, and piracy were a single industry, it would be the world's largest (9). German authorities seized $1.6 billion in pirated goods in 2006, which was a 500% increase from 2005 (10). U.S. Customs and Border Protection reported an 83% increase in counterfeit good seizures in 2006 (11). England claimed a 45% increase in fake drug traffic in 2005 (12). Interpol has noted a steady 10-year surge in intellectual property crime (13). The International AntiCounterfeiting Coalition claims a ten thousand percent increase in recent decades (14).

Those familiar with the fight against spam know about fake pills, pirated software and counterfeit watches, but the other items being forged and trafficked are shocking. Cigarettes, with twice the carcinogens; alcohol, with ethanol and other poisons; tea leaves, dried with truck exhaust; weed killer, that kills crops too; shampoo, with fecal matter ("shampoop"?); brake pads, made from pressed sawdust; surge protectors, that explode. There are many more examples, too extensive to be listed here (15).

Between the spam and the junk products, each item sold through a spam site has a sordid pedigree. To begin with, the manufacture of counterfeit items is often done with forced, child, prison or under-compensated labor. The illegal factories are themselves not inspected and pose serious health, safety and environmental threats. In order to operate these illegal factories government officials must be bribed or coerced. The products themselves often represent trademark, copyright, and intellectual property infringements. These fake goods must be smuggled out of countries of orgin with the contraband often being carried on the persons of human mules, some of whom are trafficked and sold into slavery. No taxes or tariffs are being paid on these shipments and the profits must be moved by money launderers. Profits from this traffic often go to fund bloody conflicts in developing countries as well as terrorism and criminal activity. In the process of ordering one fake watch from a spam advertisement, we contribute to an enormous criminal network. Some cynics may believe that this is just how the developing world competes with the industrial world, but the poorest people in this cycle do not benefit from it and the enduring government corruption holds them back further (16).

Software Piracy

Considering that the use of pirated software is estimated at 50% worldwide and that some developing countries have nearly 90% piracy rates there is a secondary threat looming. With private citizens, small business and even some governments purchasing and downloading pirated software there is a potential for a "big hack". The person who is the source of pirated software can insert whatever they want into that installation bundle. The consumer of pirated software probably does not know their new office package contains pre-configured malware. Pirated tax return software is a goldmine for hackers and identity thieves. Tax returns can contain social security numbers, bank account numbers, salary figures, mother's maiden names, home owner information, job descriptions, addresses and phone numbers. AutoCAD is expensive technical drafting software commonly featured in software pirate spam. A small company concerned about its bottom line might be tempted to buy pirated AutoCAD. Defense contractors may be clean of pirated software, but what about their subcontractors, and subcontractor's subcontractors? This is not conjecture. Malware has already been inserted into popular business applications and even installed on devices at the factory before the consumer even logs on. Countries that are known sources for pirated software are also known for spying on companies in the U.S., U.K., Europe and other industrial countries. It is not always clear who is doing the spying, it could be corrupt government elements or gangs. It could be a combination of both or it could be with the full authority of a rogue government. In China, Wo Shing Wo, San Yee On, and the 14K crime organizations are all reportedly involved in media piracy as well as human smuggling. Authorities in China often claim that Chinese Americans run these gangs. Obviously, this is a problem that is much more complex than publicly acknowledged or understood.

Fake Prescription Drugs and Easy Access

Deaths from painkiller overdoses have exceeded those from heroin and cocaine in recent years. In 2005 drug poisonings were second only to automobile accidents for unintended deaths (17). Counterfeit drug investigations by the FDA have increased 10 times since 2000(18). Steroids are much easier for young athletes to obtain and even licensed pharmacists and physicians have been implicated in high-profile scams. This has been the most common type of spam observed by KnujOn and it has moved beyond the erectile dysfunction drugs and now includes cancer, blood pressure, heart, arthritis, and diabetes medication as well as anti-depressants and psychotropics. KnujOn has been presented in a variety of venues and we are almost always approached by an attendee who has purchased substandard medication on the Internet or at least knows someone who has.

Drugs are complex chemicals that change the way a human body works. Taking physicians and pharmacists out of the chain can lead to a host of disastrous results. For example, some male prostate drugs are extremely toxic to pregnant women. Surely pharmacists and physicians will ensure that patients are aware of this, but the spammer will not and there is no legal recourse for the victim.

Vacation Scams

Customers pay for a trip and do not receive anything. The company sends tickets or vouchers, but the airline/hotel does not honor them. Customers are charged extra (and often large) fees when presenting vouchers. One fare is promised but a different one is charged. The company agrees to a schedule, but the dates are then changed by the company. Customers are promised a specific airline/hotel, but different services appear on the voucher(s). There is nothing new here, except that the threat has moved to the Internet.

Mortgage Fraud and Phishing

There were 600 cases of mortgage fraud in 2004 and 21,971 in 2005 totaling over $1 Billion in losses(FBI)(19). While the FBI reports that mortgage fraud cases are increasing, convictions, seizures, and recovered funds are declining. Some mortgage spams are just phishing/ID Theft attempts, others are “referrals”. Reverse Mortgages, “Teaser” ARMs, and “flipping” schemes are conducted by skilled industry insiders. Targets are often elderly or people on a fixed income. The increase in foreclosures has become a burden on the market generally and has played out recently on the national stage with heated debates about government buyouts of bad loans.

Phishing has evolved into multi-prong threats that combine viruses and ID theft. Hackers post exposed accounts for auction. Changes in the banking industry may provide a false sense of security (two-factor guidelines). The weakest point in any system will always be the people. Banks can lock down on-line transactions but deceived customers and employees will still hand money over to crooks. Access is often a target and not simply money, any increase in illicit traffic profits increases demand for more money laundering.

Market Manipulation

Spammers have successfully manipulated stock prices for their gain and other investor’s loss. Studies at Harvard, Oxford and Purdue have confirmed the viability of manipulating penny stocks for big gain (20). Penny Stocks (Pink sheets, OTCBB) are used because their small value does not require as much oversight or registration. Spammers use software similar to CAPTCHA to create stock touting images
In 2006/2007 KnujOn noted that there was a “Polish epicenter” of stock junk. The bulk of stock spam examined by Knujon originated on Polish networks. Secondary sources were countries bordering Poland. Tertiary sources were countries with large Polish communities. Around the same time we released these

results the SEC started targeting a Latvian-Russian gang. This points to an "organic" nature of malware while illustrating that reporting followed by proper analysis can lead to meaningful action.

Spam that is not email

Our belief that the spam problem is not primarily about email is enhanced by the existence and prevalence of non-email spam. Junk faxes existed long before the Internet and continue to be a growing threat. Advertisements for junk products and services continue to appear stapled to telephone poles, the only difference is that they now have websites. The post office still dutifully delivers snail junk mail with deceptive prize winnings, predatory mortgages, and outright fraud. Will fixing email stop brochures and menus from being placed on car windshields? No, this is a much more complex issue.

On the Internet itself the spammers have many tools at their disposal besides email. Search Stacking has been researched in detail at KnujOn (21). Basically, cybercriminals establish websites loaded with credit card and banking related keywords that are found by search engines and block out the real sites. Wiki, blog and forum spam are a continuous annoyance. Social networking sites are burdened with predators and junk postings. Even iTunes allows non-music files like text and PDF to be posted. Even if email itself were scrapped as a tool tomorrow, spam would still be here in some other medium.

Other Threats

Not every type of spam is covered above. We also have deposit scams, sometimes called "Nigerian/419" or Advance Fee Scams. These present a unique problem for cybercops because there is rarely a website involved and the perpetrators hide in unstable countries and behind deep levels of anonymity. Victims of this kind of fraud have been kidnapped or murdered while trying to retrieve their money overseas. Degree or diploma mills are an old business, but pose a serious secondary threat because people use these fake degrees to obtain jobs and as identity fraud in more complex schemes. Gambling spam is prevalent because, although on-line gambling has been made illegal in the U.S., international web-based casinos still attract American customers. Pornography spam was the flagship Internet lure and remains a way to trick people in exposing PCs to viruses. The sex trade is alive and well on the Internet and bold emails promise in lurid detail the services being offered. Spam has also been used in various political attacks and is a looming threat for the U.S. 2008 presidential election. Hoax and urban legend emails seem soft compared to the criminal spam today, but they demonstrated the public's gullibility in the 1990's and provided spammers with a foundation to work on today.

Direct email is a favorite starting point for industrial espionage. Spies collect "gray material" on companies and researchers and then use carefully crafted emails to open communication and pretend to be colleagues and graduate students. Threats can be foreign intelligence, foreign companies, domestic competitors, activists, and people with a grudge. Commonly held beliefs about spam and phishing, that they are purely the province of criminals and hackers, allow foreign intelligence services the opportunity to be "lost in the crowd." U.S. National Counterintelligence Executive Joel Brenner recently said that foreign intelligence services are "eating our lunch" (meaning U.S. intelligence).

The new Internet economy has made way for some smaller countries to engage in the dangerous practice of selling their very sovereignty to spammers, electronic fraud and illicit business. Some nations have loaned their name and legal authority to fake banks, allowed their telephone systems to be hijacked by confidence scams, and their country domain extensions to be used by spammers in addition to harboring smugglers, pirates, and counterfeit factories. If one compares the treasury balance of the world's most impoverished countries with the amount of money being made by spammers there is a vast gap. To see how wealthy criminals are in a position to *own* counties, consider the influence Osama bin Laden has had in Afghanistan. The smaller, poorer and more overlooked the county, the more likely it will become a haven for unsavory characters. The threats in coming years will emerge from places only mapmakers have heard of. For example, the top level domain .CD is emerging as a phisher favorite. .CD is the domain extension for The Democratic Republic of the Congo(DRC) which is not the same as the Republic of the Congo. The

DRC, formerly Zaire, has been in a state of political upheaval since the late 1990's. It is unlikely that the ordinary consumer will be aware of the complex history and confusing conditions that would allow clever criminals to take advantage of troubled countries.

As for virus emails, there has been some criticism that encouraging people to report junk email will spread viruses, especially if the email needs to be opened for forwarding. Reports that come to KnujOn are scanned before processing and we often report back to members if we find viruses in their submissions. Existing email functions and enhanced tools that allow submissions without opening are emphasized. Unfortunately, malware epidemics are not often discovered until the infection has already spread ("in the wild"). If email users reported possible virus emails to services like CastleCops MIRT instead of deleting the email a widespread infection could be averted.

II. Failures

The Failure of Filtering

Anti-Spam Software "Doesn't Work." This was the conclusion drawn by a recent Brockmann and Co. study(22) and asserted by KnujOn as early as 2003. In short, email users are frustrated by filters that trash good email and allow bad email to slip through. To be clear, the developers of filtering software are brilliant people and their products filter correctly an overwhelming percentage of the time, but it is the wrong solution for the wrong fight. This is looking through the wrong end of the telescope.

The Economic Nonsense of Spam Filtering

Not only does filtering not work, but it makes no money sense. If we accept the overwhelming evidence that 90% or more of Internet traffic is junk, then the criminals have clearly hijacked the global network. What is the Internet? It is a collection of private networks, commercial cable and public phone systems. Who pays for the maintenance of this network? We all do. Through taxes, access fees and overhead passed to the consumer. So the consumer is more or less supporting the spam network. How much does that end up costing? In the United States it could be as high as $1.5 Billion per month or $18 Billion per year. This figure does not include the amount of money spent on filtering, or the lost work hours, or money spent on chasing e-crooks, only the estimated cost of transmitting the spam. Based on the average household paying $30 per month for access, even if you have a virus scan and filtering software and receive no spam in your inbox, you are still paying $27 per month to guarantee that it gets delivered just short of your mailbox. Since the spammers are hijacking machines with malware, their costs are zero. The estimate is based on 55,544,208 households with net access (an outdated 2000 census) with only 10% of paid fees or taxes going to support traffic that is wanted. The estimate is possibly lower than the true cost (which is difficult to truly quantify), and this is only the United States. The global cost is probably much higher.

Block and Delete Strategy Ignores the Issue

Relying on blockers and filters makes the problem worse. Organizations and personal email users are blocking/filtering billions of junk emails every day. This is to the advantage of spammers as it allows them to target the most vulnerable users who do not have filtering software or technical savvy. Besides helping the junk emailers and identity thieves find their target audience, we are restricting our own use of email. Too much attention is paid to the email and the spammer. The spammer is a mercenary criminal. He is not really concerned with what is being sold in junk email and is not the real engine behind the scheme. Spammers do not have warehouses full of fake pills and knockoff handbags. Spam, transaction sites, shipping, and supply are all distinct operations. It is possible that the parties never meet face to face and that discussions and mentoring occur in chat rooms. Spamming skills are easy to pick up and share, and there are even spamming "kits" available for sale/download. In this model, blocking spam or even arresting and jailing a single spammer is of little consequence to the larger fight.

8 Reasons Why Content Blocking Does Not Work

1. It does not actually reduce the flow of junk mail . Every study, statistic, news article and expert in the last three years has clearly stated that the junk email problem is getting **worse** (and much worse) since the common institution of filters and content blockers at the ISP, network, and user levels.

2. Junk mail still gets through. Every day a new, clever piece of spam bypasses filters and hits users inboxes.

3. Good mail gets blocked. The following are statements made by on-line companies:

IMPORTANT NOTICE: Some Internet Service Providers may block replies, assuming they are unwanted messages. To ensure that you receive a response to your inquiry, we recommend that you add -------@------.com to your address book. This will also allow you to receive valuable information from ------ such as product updates and special information about ------ products, supplies and accessories.

Internet Service Providers (ISPs) have tightened their definitions of SPAM. As a result, your ISP might categorize an email confirmation from this site as potential spam and filter it into a "Bulk" folder or a predetermined "SPAM" folder you define. If you place an order and do not receive your email confirmation in your Inbox, please check in these areas before contacting customer support.

They are basically saying "we cannot guarantee that our email will be delivered, you have to make an extra effort to dig it out." Where does it end?

4. Legitimate Marketing and Corporate Communication Treated as Spam. Lawful, legitimate companies have a diminished ability to reach potential and current customers. Since it is assumed that all marketing email is illegal junk mail, it is all ignored and deleted. This includes newsletters and catalogs that customers have subscribed to.

5. Filtering does not stop the crimes behind the email. This isn't just about the email. There is a world of fraud behind these emails that needs to be addressed aggressively.

6. Anti-Spam Companies and Service Providers as Censors. "Viagra" and "Valium" are blocked by most filters. What if I work at a pharmacy and I want to send email about these products? What if I want emails with adult content? What if I send email that contains blocked content but I'm not actually selling anything? There has been quite a bit of debate about censorship in the press, television, radio, music, film, and video games but very little concern about the power given to companies that filter email. Privacy alarms sound over credit card databases and telephone records but we thoughtlessly hand over our email to be filtered. Providers have in fact been sued over this issue.

7. Reduces the Value of Email as a Communication Tool. No links, no HTML, no pictures, no spread sheets, no compressed files, no documents. All hold potential for spam and viruses therefore none can be trusted. Email is a perfect universal communication tool and it is being ruined.

8. Creates an Underground Network for Scam Artists. While most of us are blocking and deleting junk email, there are those who are exposed to on-line predators and no one is watching. This is the Pushdown Network. Beneath the protected networks is a wide-open *pushdown* network full of potential victims waiting to be scammed. It's called "pushdown" because we have all created it by pushing down the junk through blocking, filtering, and deleting. While you and I may be protected, those without protection are allowing their PCs to turn into zombie PCs and bringing infected files onto office networks. These people may end up being victims of fraud or identity theft and this affects all of us.

Other failed attempts

In recent years email filters have been distributed globally and the U.S., U.K. and other governments have passed anti-spam laws. Bill Gates said spam would go away by 2006, the media stopped writing about the problem, and many people considered the issue resolved. The problem was not solved, not by a long shot. Why have solutions failed?

Unsubscribe: Legitimate email marketing will usually have an unsubscribe link or opt-out process. Spammers will either: not have the unsubscribe link, a link to another site's unsubscribe, a link that "pretends" to unsubscribe, a link which downloads a virus, or a form that requires a questionable amount of personal information.

Code Verification: Many email services will display a random set of non-ascii (image) letters and numbers(CAPTCHA) for a user to enter in order to verify that a real person is sending email and not a script hacking a mail account. It is a clever concept but does not stop the spammers and instead frustrates legitimate users.

SMTP relay limits: Many mail hosts will limit the amount of mail that can be sent to 500 or 250 emails per day per email address. However, if a spammer has 10 sites with 100 email accounts on each they can send half a million emails per day. This scheme merely prevents legitimate ISPs from being abused.

Filters and Blockers: Most networks use some kind of spam blocker or filter. These programs effectively keep junk mail from reaching mailboxes, but they also block some legitimate mail and allow bad messages to get through. Blocking and filtering do not stop the problem, they only delay it.

Certificate Based Emailing: This may prevent spoofing or header forging, but makes email more complex and expensive. Spammers are not above hacking the system to get around paying.

Hack/DDoS the spammers: Lots of work and also breaks the law.

Sue the spammers: Expensive. Time-consuming. Limited results.

Create Taxed or Fee-based Email Systems: Junk snail mail is a continuing problem even though direct mail marketers have to spend money on postage. Considering how much money spammers seem to be making, this would not be a huge expense for them and would still not protect the consumer from viruses or scams. This also assumes that spammers would not find ways around any payment system.

Pass laws that make spamming illegal: Speeding is illegal, people still do it. It is important to put these rules on paper, but enforcement is extremely difficult because of the size and complexity of the problem. The law alone will not stop them, effective policy enforcement will.

Header Tracing: Services like SpamCop have made titanic efforts to track and shutdown the sending IPs of junk mail, the ordinary email user does not have the knowledge or wherewithal to constantly participate. Folks who take the time to expand and report headers are dedicated to the cause, but most people have bought into the flawed idea of filtering and deleting junk mail. The number and size of botnets is growing,

making the reporting of sender IP less effective. Following the path an email has traveled will only lead you to a victim's PC. Not only that, it is a crap-shoot when it comes to ISP response. Everyone knows spam headers are forged, right? This is exactly what the spammers want consumers to believe. Often when the spammers are tracked down their response is: “We didn’t send it, look at the headers!” The spammers are using the obfuscation to create an umbrella of plausible deniability and we are playing their game by tracing headers.

Major Overhaul of SMTP: Yes, the basic protocols need review and updating to handle unanticipated consequences, but the belief that merely changing the protocol will end illicit traffic on the Internet is a fallacy. As we review below, there are a multitude of non-email spam tools available to the e-criminal.

Blaming the consumer

At the 2007 Spam Summit held by the FTC in Washington, D.C., the results of a spam survey conducted by PEW/INTERNET(Pew Research) (23) were presented. We found the results of this survey troubling since they suggest the public's acceptance of spam is growing. People are just assuming that spam is a part of modern life and nothing can be done to stop it. At KnujOn, we think this is defeatist and we have been working to deal with the problem in creative and unique ways.

It is important to review how the Internet industry has dealt with this problem from the beginning. When spam started to become a problem for email/Internet users it was generally assumed that the user/consumer had done something to bring it on themselves: they purchased pornography, signed-up for questionable websites, etc. (i.e., it's the user's own fault). As spam began to reach people who had never purchased pornography the blame shifted to posting and sharing of email addresses. Users were told not to publicly post their email addresses and be careful who they share them with. Also, user mailboxes became infected. Users with unprotected email programs turned into relays for viruses and address harvesting. Again, the consumer/user is blamed.

Once it was realized that spammers get addresses from a variety of methods, including scripts that generate random or sequential strings, the consumer was told to ignore or delete the spam they receive. Many concerned citizens tried to report phishing attempts to their banks, but the banks told them to delete and ignore. Once again, the burden is on the consumer to deal with it. The problem grew and a new industry of email filtering and blocking software emerged. However, the responsibility is still on the consumer to purchase, maintain, update and upgrade the filtering software. While the algorithms behind these filtering programs are complex, the scheme itself is little more than an enhanced tool for ignoring and deleting.

A year after the widespread deployment of filtering software, spam is still a growth industry. Armies of botnets(zombie PCs) are collections of computers on the Internet that power spam delivery. These zombie PCs are private computers infected with malware and left connected to the Internet usually without the owner knowing. The plague of botnets is again viewed as an end user/consumer problem, because it is the inept public downloading viruses and leaving their connections open that drives spam. Now, the mantra being delivered by these survey results and some other recent media is: "There's nothing we can do, accept it.”

Mixed signals to the public

Consumers are told to delete spam. Consumers are told to report spam. It is certainly easier to check “select all” in bulk or quarantine and delete everything. Reporting spam is difficult. First, the good citizen needs to determine if the email is junk or not. Next, they need to figure out what kind of junk it is and report it to the proper place. In the process ISPs may reject the forwarding of the junk mail, ironic because the ISPs delivered the original email. If the good citizen does manage to report the junk, there is little or no feedback from government or industry. Once and for all we need to retire the idea that deleting emails and ignoring the issue can defeat this problem. Industry and government need to engage the public by sharing more success data and create a sense of partnership. Consumers also need simplified reporting tools.

It is good advice to never buy anything from a company that spams. However, they will still make money from a minority of people and keep spamming everyone. Also legitimate on-line companies sell addresses to spammers, this is a common occurrence in the sales world because mailing lists are very valuable.

It is bad advice to tell users not to post email address on web pages. While spammers do use programs that harvest emails from web pages they also obtain lists from other spammers and send junk to random emails until they get a hit. This strategy also violates the point of the Internet, communication. Legitimate users should not have to self-regulate because of people who refuse to follow the rules.

Computer users have been left, for the most part, to fend for themselves in the world of e-fraud. New users log on to the Internet for the first time every day and they are being counted on to first, determine if something is fraud and second, figure out how and where to report it if it is fraud. This assumes that end users have the time, technical knowledge, consumer savvy, and patience to deal with the problem. Considering that most fraud goes unreported, the few brave souls who try to report junk email are then faced with the task of figuring out how.

Where the Industry is Failing Consumers

Email and Internet users are demanding solutions but the technology market is slow to respond to consumer need. Consider the Napster case. While the music industry focused on the legality of consumers swapping files it completely missed the potentially overwhelming demand for access to music on the Internet. It took several years after this incident for iPod to become a standard for music consumers. Technology is fast, but market thinking is not. This is the case with email. Consumers want better control of their own communications but email software has not changed for the consumer.

Several KnujOn participants have developed their own utiltiies for reporting spam from Thunderbird, Outlook, Yahoo, Gmail, AppleMail and others. These were created by dedicated members, not by big software houses or ISPs. The Internet industry has in many cases made it more difficult for consumers to report junk email while continuing to send confusing messages to the public about security. This would suggest they do want to deal with it or do not know how. Recently, the U.S. Defense Cyber Crime Institute called for "the industry to create tools to help us investigate large volumes of data." The industry has not responded in a meaningful way, and we can see from the examples above, that cybercrime and cyberattacks will continue to be a problem.

KnujOn frequently receives and reviews completely legitimate marketing emails from credit card companies. There are current campaigns that promise banking transactions through mobile devices, combine offers of frequent flyer miles with mortgage applications. Financial products are extremely complex agreements, do the banks really want their customers to base these decisions on an email? KnujOn has also recorded many real credit card offer emails that have phishing characteristics, meaning they spoof URLs or redirect clicking by the customer.

The ability of the communications technology market to create and deliver new products will always be faster than the consumer's ability to fully understand them, and will always be faster than concerned parties to test them for security and safety.

What else is delaying better solutions?

Besides the repeated bad advice of deleting and ignoring spam, there are some other hurdles any improved anti-spam system is going to encounter. One is general fatigue over computer issues. Because computers are now such an integral part of our lives media stories about serious network catastrophes seem like noise. The Y2K hype and subsequent non-event on January 1, 2000 made many people skeptical of dire computer predictions. Books were sold about Y2K and various consultants made lots of money, but now few people discuss the issue and those that do often call it a big hoax. Trying to explain the looming threat of enormous

botnets often taps buried Y2K resentment. For KnujOn the implosion of Blue Security (BlueFrog) had some positive and some negative consequences. The positive was of course increased interest in KnujOn as an alternative. The negative was that anyone who previously considered funding a large-scale anti-spam initiative now finds the idea radioactive.

We also have to lay blame on the media by continuing to encourage people to ignore and delete spam rather than report it, the business community by not properly protecting their brands on-line, and government by not providing feedback to citizens and not adding more processing resources for electronic fraud.

III. KnujOn

KnujOn's thesis stems from 4 basic beliefs. If you do not agree with these principles yet, keep reading. If you still do not believe them at the end of the document, contact us and we will do what we can to convince you.

1. The Spam problem is about more than email.
2. Solutions to spam cannot rely solely on technology.
3. Filtering and deleting spam makes the issue worse.
4. Spam is not an impossible problem to solve.

What KnujOn Is

KnujOn is transforming the "unsolvable" spam problem into a situation that can be understood, managed, minimized and defeated. Spam filtering and blocking isn't working, in fact spam has increased in the last two years, flooding the global network. At KnujOn (http://www,knujon.com) we are providing consumers with a no-nonsense way to report junk mail. In return they receive feedback and action they are not getting from the Internet community. Through persistent policy enforcement, KnujOn is reducing the value of junk email by eliminating the transaction platforms (websites) and increasing the operational costs for the spammers.

We have been soliciting junk email from the public and running it through a process called the Policy Enforcement Engine (Patent Pending). We look at each piece of email and try to determine what the best course of action is. We actually go after the website owners and shut them down through legal, procedural methods. So far our work has led to the shutdown of tens of thousands of sites. We have individual users and small networks feeding us their junk email, many automatically. There are several major areas where our work is having an impact and continues to help:

- Counterfeit or unlicensed prescription drug sales on the Internet
- Traffic in knockoff, diverted, pirated, and stolen merchandise
- Predatory lending in the sub-prime and refinance mortgage industry
- Vacation scams
- Identity theft

In addition to developing an array of technical tools, we work to generate big picture thinking by exploring the complex issues driving spam, illustrating the impact on individual victims as well as the burden on the economy, and by using spam to create a "map" of transnational crime. At KnujOn we challenge beliefs, for example the current assumption that there is too much junk email to process effectively. We empower consumers by accepting junk email submissions from thousands of official and non-official clients as the starting point for our procedures. And we use the current policy structures to address the problem in order to reveal breakpoints and bottlenecks in Internet compliance.

What KnujOn Is Not

It is important to establish that KnujOn is not a firewall, email filtering or blocking system. Nor do we engage in Denial of Service Attacks or Hacking. Our core process does not involve blacklisting or header tracing. While we understand the need and utility of email header tracing, we think this is an unrealistic expectation and burden to place on the consumer. KnujOn is not a version of Blue Frog, SpamCop or Spamhaus. Our efforts have been independent and parallel to these projects.

The Starting Point

We must acknowledge that this is not something that can be eliminated completely; this is rather a problem that must be *managed*. Illicit e-commerce will exist as long as the Internet does. Prostitution, drug abuse and violence have existed in every culture at every stage of history. They cannot be eliminated but they can be reduced and controlled efficiently. We can address the root causes of crime and take particular players off the map but the problems will always resurface elsewhere. The key is recognizing the beginning of a deteriorating situation and addressing it in intelligent ways and not waiting until it has reached a crisis.

Next, it should be accepted that this problem is not primarily about the email. As we have shown above, the email and the sender are the least of our worries. The flood of junk products and fraud are much more serious than the annoyance of spam. Because this is not primarily about email and is not only an Internet problem, we cannot rely solely on the technical tools available.

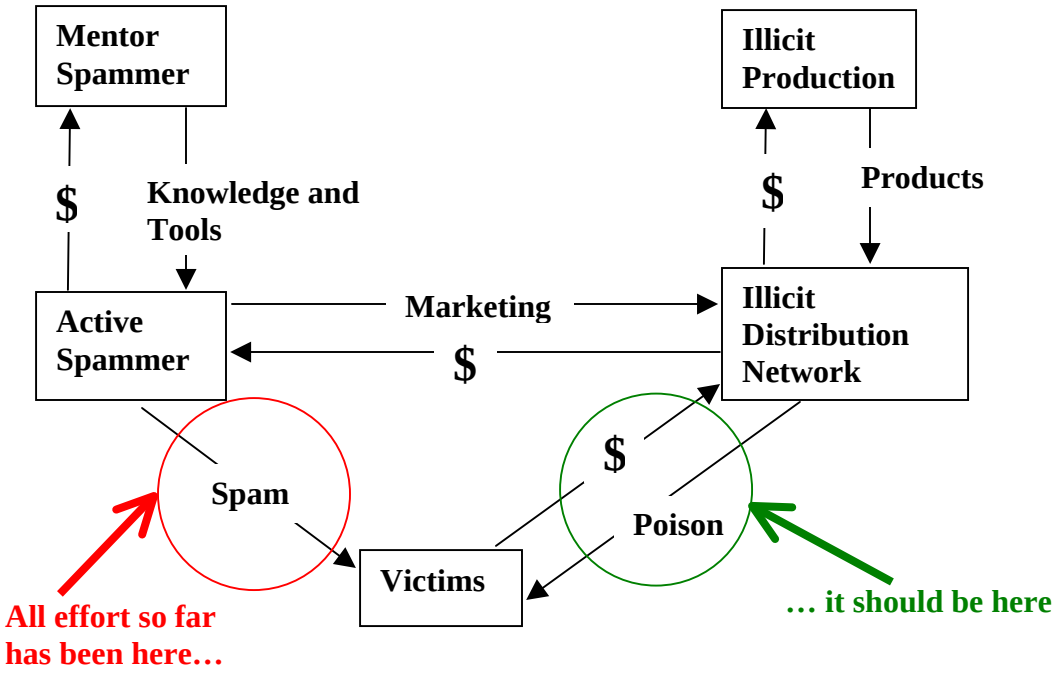
We also want to provide a two-way communication for consumers rather than ignoring their pleas and attempts to report spam. Allowing consumers outlets to express dissatisfaction and frustration is the key to the success of any product. Not only does this help improve the product with feedback data it also averts backlash. Spam filtering is the equivalent of giving someone a gasmask when they complain about the smell of toxic garbage, they can no longer smell the garbage, but they know it is there and their voice has now been muffled.

Consumers have been told that there is too much junk mail to report and process effectively. KnujOn has already proven this false by processing millions of pieces of junk email and providing real results. Our process is not enormous and our current resources are not extensive. We have done this all with smaller code and a tiny budget. Implementing our service on a large scale is underway.

As previously discussed, KnujOn wants to know what drives spam; what and who enables the spammers; who profits from it beyond the spammers; how we all suffer from spam beyond receiving it; what tools are currently available to prevent spam; of those tools, what is working and what isn't; where are the failures and breakpoints; and where our efforts can be maximized.

Targeting the Transaction

Attack the transaction, not the advertisement. Blocking the transaction (at the website) keeps the money from entering the cycle. This will not happen if the spam is deleted. If the spam is reported, there is a better possibility the site will be taken down. Once a connection is made to a victim, they are more likely to be victimized again. So far the effort to combat spam has been narrowly focused on the advertisement, not the transaction. This is a critical error.



Policy and policy enforcement

Policies are easy. Enforcing them is difficult. A teenager can put a sign on his bedroom door that says: "Private property! No Trespassing!" His parents, who own the house or pay the rent, may feel otherwise. A policy is a stated set of rules, procedures, or guidelines that is agreed to, stated or simply implied. Traffic signs are policies. However, without a police force, ticketing system, automobile registration system, collection system, court, jail, and legally granted authority the "policy" of a sign is useless. Early in KnujOn's development an annoyed ISP told this author: "It's not our job to police the Internet." So we tried to find out who was policing the Internet. The sad answer was: no one. The responsibility is poorly distributed, unmonitored, and the results unmeasured. In short, the Internet is full of policies but few are enforced.

If a service provider that hosts or registers websites has a stated "Zero Tolerance Spam Policy," it is meaningless without true definition, procedure and accountability. Our project has included a detailed survey and test of all the levels of Internet abuse compliance and we have a clear picture of who is adhering to policy and who is not. Some are diligent, proactive and above board and act quickly to cooperate with KnujOn. Some are slow and burdened by poor management. Others, sadly, are assisting the cybercriminals and profiting off of the enterprise. Admittedly, many of our goals are not things we have direct control or influence over, but our plan is to provide enough motivation for those that do and will act.

Multi-Tiered Problem and Multi-Tiered Solution

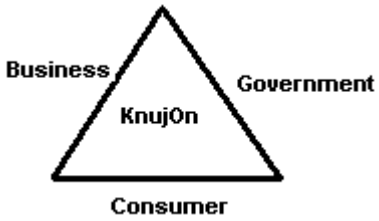
A Multi-Tiered Solution means addressing the issue at every level with the focus of blocking potential transactions. At KnujOn this is about reversing the utility of spam by examining how a single piece of junk mail affects the entire Internet structure and how each of these sectors can be useful in changing its meaning. The end goal is to reduce spam's value as an advertising benefit to the e-crooks and enhance its value as a lead for policy enforcement. We see each email as an opportunity to close a hole that is waiting for a victim to trip into. No website, no transaction. This follows a principle expressed by Moises Naim that "illicit traffic not about products, it's about transactions" (24).

So what is the tier system that needs to be utilized? Starting at the top we have Internet Governance (ICANN and similar organizations). Beneath them are the Registrars who have been granted the authority to issue domain names. Internet Service Providers (ISP) who host websites and email services are another tier. The telecommunications hardware and software industry, which provide the networking tools are again another level. The regulatory and enforcement arms of various governments have oversight and authority when it comes to telecommunications and electronic commerce represent another section. The tier of private enterprise has concern and control over its own intellectual property. News media, educational institutions, and publishers hold sway over public information. Finally, consumers, citizens and email users have enormous untapped power in their participation or non-participation choices. Each of these sections bears some responsibility and influence in the spam problem but none are working together to handle the problem. No single tier can completely address the problem alone and each have at one point denied full responsibility. However, getting these tiers to cooperate is a Herculean task. The solution is to spread out work and enhance the functions that each is best suited for.

This is not always what people want to hear. Our instincts drive us to quick and painless solutions, for this problem none exist. If there was a single responsible party or "silver bullet" it would have been discovered much earlier. KnujOn is not a magic button, it is a long-term plan to change the course of how online criminality and abuse are handled.

The Solution Triangle

This problem cannot be addressed properly without the cooperation and input of consumers, business, and government. Each party holds one piece of the solution that it must share with the other two in order for it to work. The spammers and online criminals benefit from a lack of communication between these three concerned parties. In an improved system consumers would not delete spam email, but rather provide businesses with evidence that their brands are being hijacked and law enforcement with evidence of cybercrime. Businesses would cooperate more with government on investigations, and allow consumers easier avenues for reporting fraud and illicit transactions. Government would also need to partner with business and consumers by providing feedback and including them in enforcement successes. It is a leap of faith for each of these parties, but with KnujOn putting itself in the middle, many potential issues can be defused.



Part of the problem up to this point has been that offered solutions only help one party and inevitably fail because of lack of buy-in from the other two. It is a cliché, but these parties do not always see the use in speaking to each other directly and do not even know how to begin communication.

KnujOn has assumed the first piece of this triangle by engaging email users, accepting spam submissions, returning reports and delivering action. Government has been included through the development of an investigator query engine and a continuous feed of summary reports that speak more clearly than the raw emails. Businesses are being alerted to attempts to hijack their brands in addition to having better spam protection through our core process.

Why is this not a solution square with ISPs and the Internet Community as a fourth side? Having reviewed the problem and reactions from the Internet Community we found a lack of motivation. Whereas consumers, law enforcement, and private enterprise all have reasons to be engaged, the Internet industry stands to lose by committing resources to this effort. Spending money on a true anti-spam solution is a disincentive to companies who want to speed communications and transactions in order to deliver volume

to their customers and increase their market share. Unfortunately, at the moment the Internet Community is not working to the benefit of business, government or consumers on this issue but cooperation between these three parties can improve conditions on the Internet by pushing in persistent and subtle ways.

Where do banks and phishing fit into this arrangement? Phishing is in essence a brand hijacking. The cybercriminals are impersonating banks and for a bank their name is their brand. The reputation and value of a bank is held within its name recognition as a symbol of trust as well as the recorded assets. Unabated financial fraud erodes consumer confidence and brand trust.

What Happens To Submitted Email

The journey of an email submitted to KnujOn is thorough, extensive and recursive. This is step one because the e-crooks are hoping that the email will either: be clicked-through for victimization and deleted, or simply deleted. We process, store, and reprocess everything that is sent. This has allowed us to build up incredible statistical data and keeps the door open for potential follow up in the future.

First, we feel it is important to share our collection. While there are criticisms of the FTC and other government agencies' lack of action we feel it is important to partner with them all. While there are skeptics who believe government is ineffective against email abuse and Internet fraud, just accepting junk email reports from citizens is a huge step in the right direction. We are ready to assist any government agency willing to discuss the issue and take the next steps. However, we have been very critical of the fact that government has not engaged the public on this issue and has provided little feedback to concerned citizens who diligently report spam. As we will explain below, even though an organization may not be addressing an issue now, it does not necessarily mean they will not in the future. If citizens stop forwarding spam out of skepticism, we can guarantee that the government agencies will not take action. We also forward these submissions to a host of other anti-spam groups and we are happy to add more to the list. The additional forwarding of submissions is made clear to our participants.

Not all junk email is spam. An aggressive marketing company advertising a completely legal product or service does not see itself in the same light as a criminal group selling counterfeit products and they should not be treated the same way. However, for many consumers getting removed from emailing lists is an exercise in futility. This is where the anti-spammers sometimes lose potential allies and the marketing companies frustrate consumers. At KnujOn we are using varying indicators to measure how different emails should be handled. In the case of legitimate marketing companies we attempt to contact them and negotiate on the client's behalf. For spam that is clearly a campaign for questionable products or services, we follow other routes.

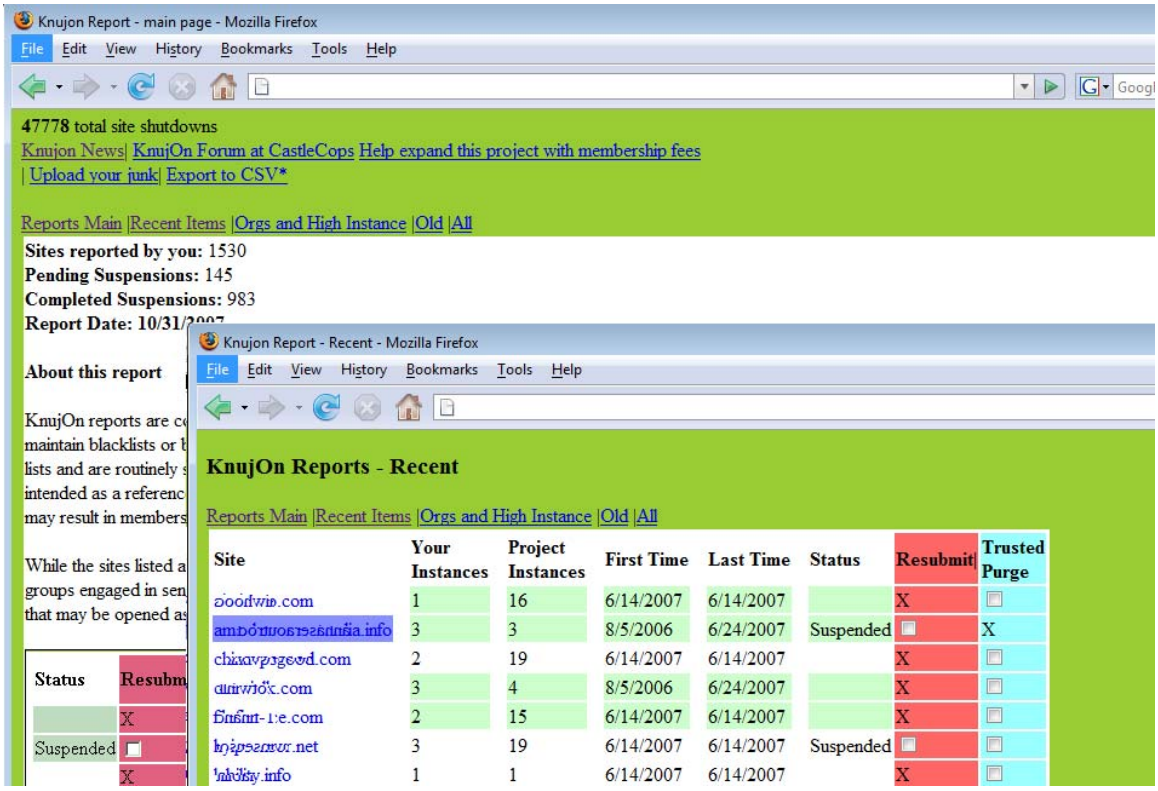
Reported junk email is processed to have the advertised URLs pulled out. This has been made difficult by increasingly obfuscated spam message content, but we are constantly improving our process to deal with this. This is in effect a partial victory because it means the spammers acknowledge that the exposure of their website is a key weakness. These URLs are sorted, categorized and published with details to our members. Our members receive regular updates in the form of interactive reports, which have new features added regularly allowing them the option to extend KnujOn's utility. A more detailed look at the reports is in the next section.

Non-URL email like stock junk, deposit scams and other items are compiled in collections that can be used to present law enforcement with ordered statistical data. Because there is no website to target in these scams they do not fall into the same category as items that generate client reports and enter the Policy Enforcement Engine.

URL junk email that is evaluated to present a more serious threat than aggressive marketing is run through the Policy Enforcement Engine. The KnujOn Policy Enforcement Engine (Patent Pending) looks at each email and attempts to determine the best course of action for handling, based on a complex set of rules discussed in the Declarative Languages section below. Data collected in the process benefits the discovery initiated by other submitted spam and results can produce exponential results.

Interactive Member Reports

We have been releasing improvements and enhancements to our client reports regularly and the example featured may not be current. KnujOn provides the member a view of what is being featured in the junk email they submit to us, how often they get it, when it started, and the current status of the site is. We have features that allow our members to purge sites, which are not real spam sites, and to re-report previously suspended sites. They also have the option of learning more about the site and their owners without actually going to the site and risking exposure to malware. The report may be exported to a flat file that is used by some members to create a personal blacklist. While we in general reject the heavy industry reliance on filtering, this is on a personal level and allows the member to create a smarter personal filter if they wish. From this interface (as well as the general site) members can upload bulk junk email and report image-only junk mail. More features to be added soon will allow users to extend the utility of their reports even further which will enhance the overall results of the project while giving the individual the satisfaction of working against the spammers and their benefactors.



We understand that not everyone is willing to be engaged to this extent and this is acceptable. Some members merely view the reports for reference out of curiosity, but do not use the extended features, while other members are content to not receive reports but still want to participate by submitting junk email to us.

Domain Name Suspensions and Site Shutdowns

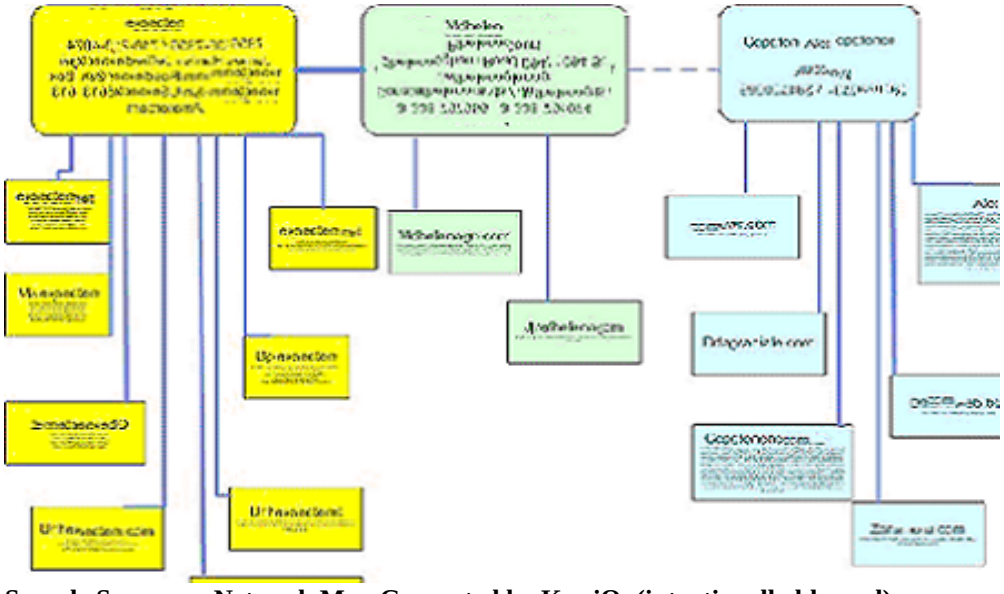
As we have stated repeatedly, removing spam advertised sites from the Internet is key to preventing potential transactions and victimization. Site removal decreases the utility that spam has and reduces returns to those paying the spammers for their work. We ask the question(s): what do the e-crooks need in order to profit and endure? And then how can we limit or remove these tools? What they need more than the email is the website and the ability to transact. Having the biggest billboard on the highway is useless if there is no way to present and deliver the product. The value of removing spam websites or "site

takedowns" has been detailed in other research as well (25). It is important to note that KnujOn does not have the authority to terminate websites. Our ability to ensure that websites are suspended or removed relies on cooperation or non-cooperation of those who ultimately control the sites. There are rules for using the Internet, there are rules for operating a for-profit business, and there are rules for selling certain products in the United States and other jurisdictions. Those who benefit from spam campaigns are usually engaged in questionable transactions and generally fail to follow any rules. Suspending domains is a question of showing which rules are being broken in a detailed way to the correct party and then following up constantly. There are many reasons why a website can be terminated, it is a question of figuring out which path is best. For various reasons the details of these methods are not released. While many of these are already discussed and detailed elsewhere, citing which ones are most effective is counterproductive. Handing the entire playbook to the enemy is not a good idea. We also wish to respect the confidentiality requests of parties who have cooperated and opened a dialogue with KnujOn. Site suspensions are not always easy and not always permanent, but KnujOn's persistence and continuous improvement work towards a goal of making this a manageable problem instead of a menace.

Following through with policy enforcement usually results in site suspension, removal of site registration or loss of hosting or network services. But this is not only a single site plan. In many cases when sites are already listed by KnujOn, a processed email may reveal violations at multiple related sites. Spam sites are usually part of a large network, hundreds and thousands sometimes, all controlled by the same person or group. Once enough data is collected by KnujOn it is possible to move against the entire spam network. Afterwards, KnujOn continues to monitor and track every site and spam network since its inception. KnujOn has successfully shutdown spam sites and networks when they resurface months after being suspended initially. It is an ongoing effort, but more participation improves the situation.

Building a Map of Transnational Crime

As we have explained, the motivations and structure of Internet criminal organizations are complex and global. For investigators and researchers this information needs to be presented quickly and remain current. KnujOn has developed tools that allow the structure of groups to be demonstrated and patterns to be evaluated.



Sample Spammer Network Map Generated by KnujOn(intentionally blurred)

While the scope of cybercrime seems massive, KnujOn research illustrates that there is a small but dedicated population involved in spamming and Internet fraud. While the number samples and data KnujOn works from has grown considerably since the project's inception, the number of persons and groups involved in spamming remains relatively unchanged.

Junk email is not the burglary, it's the crowbar. It is not magically generated; there are real flesh and blood criminals behind it making real money. The yearly cost of electronic fraud is in the billions. Law Enforcement, by its own admission, is suffering from a lack of tools and experienced personnel. Part of the KnujOn effort is to present clear and actionable reports for investigators. Query engines and report generators have been developed at KnujOn to provide this crucial data.

Intellectual Property Surveillance

If you are doing business on-line, your brand is being hijacked. It does not matter what kind of industry you are in, someone, somewhere is targeting your web content, name, trademark, copyright, or your network. Commercial enterprises are not adequately protecting their brands online. Many are not protecting them at all. There are numerous ways a company can be ripped off on the web. Product counterfeiting is not only for luxury products, but just about every product under the sun is being counterfeited and sold on the Internet. Brand hijacking is using your trademarks to lure customers to substandard products. The products come from many sources including market diversion that involves re-labeling, repackaging and reissuing expired, damaged or discounted products for full price. Web content is being lifted with impunity, using graphics, photographs, icons, descriptions, product names, code and text to populate illicit sites. Network intrusions are commonplace and used to access resources, send spam, steal funds, and impersonate businesses.

With a huge database of collected fraud emails and a continuous feed of spam that can be researched for brand hijacking we can conduct proactive brand protection on the Internet. KnujOn can take an organization's junk email and process it to better protect your network, limiting your exposure to intrusions and viruses. The idea of monitoring the web for trademark infringements is gaining wide acceptance. Working in concert with our other tools, KnujOn can provide full service to the community.

Game Theory

There are areas of Game Theory that are applicable to email abuse and Internet fraud. This discipline has been useful to us in terms of predicting consumer/user reaction as well as the spammers and using that information to constantly build a better model. Understanding that the rules and players in this game change constantly is critical. *Games* are made up of sets of players and moves. The results of different moves can be defined as payoffs or punishments. In simplest terms, we want to decrease the payoffs for spammers and increase the punishments and this can be done through the creation of extensive trees that map actions and reactions.

In the classic *Prisoner's Dilemma* (25) Game Theory model we have two prisoners tied to a common crime and isolated from each other within police custody. They are each offered the same deal to be released if they testify against their partner. The police offer this deal because the evidence is shaky and they need a confession to keep at least one imprisoned. If both prisoners betray each other neither of them will be released. If both remain silent they will both be released. However, neither prisoner knows what the other is planning to do so they have to evaluate their choice based on four possible outcomes and a lack of information. Either decision can result in incarceration or freedom, but only based on the unknown choice of the other. This is akin to the position email users have been placed in for years. Email users have been making decisions about spam in isolation with a lack of information and yet being expected to make the right choice. Email users have been told not to report spam. Those that want to report spam have difficulty finding how and where to report it. Those that do report spam get little or no feedback and in some cases there have been negative consequences for reporting.

In the *Closed-bag Exchange* (26) game two players exchange goods for money. However, both are in closed bags so one party can hand over an empty bag and walk away with the money. Experienced players always chose to hand over an empty bag. Eventually all players are cynical empty-baggers and no true transactions occur. This is the situation being fostered by spam advertised products and Internet fraud. In this case the spammers are experienced and drawing from a seemingly bottomless well of new player-victims. Commerce wants to foster trust in the Internet and this is a difficult prospect if fraud is ignored.

KnujOn wants to introduce new games that work to consumer advantage. As we have illustrated in the Problem and Failures sections, concerns of the consumer have been left out of the spam discussion and this has played into failed anti-spam efforts. By engaging the consumer we have already solved a big initial problem in the spam fight. Taking spam samples from the public satisfies the two main motivations of those wishing to report: **The Personal /Selfish Motivation**: "Solve MY spam problem"; and **The Group/Altruistic Motivation**: "Solve THE spam problem". These are, in essence, two different problems that do not necessarily have the same solution. These people can be very emotional and dedicated to a fix, but their goals are not the same. Therefore, they may take different paths that result in collective failure. It is important to note that the failed block and filter approach only addresses The Personal/Selfish Motivation.

Our job is to manage effort and expectation to reach a better end. For these two distinct user types we also address varying levels of concern with varying levels of participation: **Engaged/Active** vs. **Unconcerned/Passive**. The Engaged/Active participant submits large volumes of samples, can review detailed reports, make use of the returned data, and take further steps to extend KnujOn's utility. These are the users who ask us: "What else can I do?"; "Why is the process so slow?"; "Can you add this function?". The Unconcerned/Passive user may submit junk email occasionally, not need reports, or simply set up mailbox forwarding rules to submit to KnujOn and be done with it. In this sense "Unconcerned" does not refer to a lack of concern about the problem, but a lack of concern for process and results. For the Engaged/Active participant we have created a *reward* system. The motivation for submitting junk email is an increased number of exposed websites and an increased number of site shutdowns. Some have even referred to the KnujOn statistics as their "score." In effect, the interface is evolving into a kind of game where the player/user may collect inventory and perform certain actions with those objects.

Declarative Languages

While major pieces of our process are written in standard languages like C++, Perl and VBS, the overall logic of KnujOn makes use of more complex concepts drawn from Prolog and Lisp. These are some of the Declarative Languages often used in Artificial Intelligence theory. These languages differ from standard procedural or imperative programming that has rigid orders, sets of procedures and expected outcomes. Declarative algorithms allow us to expand our rules set and take changing factors into consideration. Because in a single spam message we are dealing with: the content of the message, the context it was sent under, the content of the target site (which may change quickly), the history we may or may not have on this site, and the particular utility of this campaign the best course of action may be different each time a sample is processed. Languages like Prolog allow for the creation of *worlds* of knowledge around a particular object. For example, if we receive a sample email that contains a URL for "RXsite.com" we may deal with it one way if it is the first time we have seen it, and another way if we had seen it many times before. Do we know what the site content is? Do we know if they are part of a known group of spammers? Have we enforced policy against this site previously and was it successful? All of these factors must be considered to maximize the payout referenced in the Game Theory section.

Safer Model

Another KnujOn goal was to develop a better model in the face of cyberattacks. Thus there is no software to download, no live connection needed, and no active process or database on the net. This reduces chance that a client will be tricked into downloading an update from a rogue site or having something on their home computer that can be hacked and linked to the project. All our correspondence with clients is done in plain text and is somewhat infrequent.

Our reporting, processing, and information distribution are all done in different locations. The process itself is compact and highly mobile. A denial of service attack on our sites will not stop the process and will not keep us from communicating with our members. Hacking into one of our websites will reveal nothing beyond what is already publicly posted.

A future plan for KnujOn could create international franchises, knujon.co.uk, knujon.ca, knujon.fr, knujon.de, knujon.co.au, etc. This would take into consideration local laws and customs and create a distributed policy enforcement model that could not be disrupted by denial of service attacks. If one service goes down, users may access another until their own is back online. Unfortunately, in many cybercrime cases, victims have been denied assistance because the perpetrator is in a different country. The global KnujOn network could also act as a referral service to coordinate these efforts better.

Success

Thousands of shutdowns through KnujOn happened because people reported junk email. The SEC has suspended trading of touted penny stocks, pursued many stock-fraud cases, and frozen assets based on citizen tips. The FCC has fined hundreds of companies for sending unsolicited faxes, one company was fined over $700,000 because of victim complaints. Services like APWG and CastleCops(PIRT/MIRT) are coordinating anti-phishing projects that target botnets in the process. All of this is due to consumer participation, cooperation and follow-through.

Next Step for KnujOn

Our primary mission was to convince email users to report, not ignore, spam and we feel we have succeeded in changing many minds. However, KnujOn needs to expand if it is going to have a true effect. New members mean more junk email samples. More samples and participants lead to a greater reach of the project's effect. We also need to appeal to the community as a whole in order to promote the notion that spam should be fought not because of its annoying nature, but because of the serious aftereffects.

Our climb has not been easy. Convincing the media to stop telling people to delete spam has been difficult. Alone we cannot create more cybercrime schools and educate enough professionals. Getting government to publicize successes in enforcement, encourage reporting and expand processing resources is a complex and politicized issue. Encouraging private companies to aggressively protect intellectual property would be a sea change.

The e-fraud problem is a complex, multi-layered issue, which cannot be addressed by blocking, ignoring and deleting email. The Internet and email are tools for communication. These tools should not be restricted because of junk mail and viruses from a minority who refuse to play by the rules. Consumers have a right to know who is collecting their personal information and for what purpose. Government and law enforcement should have the tools and information needed to address serious criminal activity on the Internet. Companies and organizations should not have to restrict email usage with filtering and blocking. Legitimate marketing and e-newsletters should not be characterized as spam as long as they follow acceptable policies. The tools and policies for stopping junk mailers, spammers, phishers, pharmers, virus senders, hackers, and forgers already exist. KnujOn will to continue address e-fraud on the current scale, while actively looking for partners and ways to expand the project.

To contact:

Garth Bruen: g_bruen@knujon.com
Dr. Robert Bruen: b_bruen@knujon.com
For more information: http://www.knujon.com/knujon.html
Press section: http://www.knujon.com/press.html
To join as a client: http://www.knujon.com/register.html
To submit junk samples: http://www.knujon.com/sendusspam.html

References

[1] Brad Stone, “Spam Doubles, Finding New Ways to Deliver Itself” *New York Times.* http://www.nytimes.com/2006/12/06/technology/06spam.html?_r=3&ei=5087%0A&em=&en=4f19ce69cb92bfd1&ex=1165813200&oref=slogin&pagewanted=print&oref=slogin&oref=slogin;
“Spam is back and worse than ever”. http://redtape.msnbc.com/2007/01/spam_is_back_an.html#posts
[2] Paul Roberts, "Study Puts a Price on Spam". http://www.pcworld.com/article/id,111433-page,1/article.html?tk=dn070203X
[3] Thomas Claburn, "Spam Costs $712 Per Employee Annually". http://www.informationweek.com/story/showArticle.jhtml?articleID=198701941&cid=RSSfeed_IWK_News
[4] consumerreports.org, “Spam: Better defenses”. http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/spam/0709_net_spam.htm
[5.] Moises Naim. *Illicit*, p 112; *Art of the Steal* p 19
[6] Frank W. Abagnale. *Art of The Steal*, p 181
[7] Moises Naim. *Illicit*, p 111
[8] Tim Phillips. *Knockoff, The Deadly Trade in Counterfeit Goods* p 3
[9] Tim Phillips. *Knockoff, The Deadly Trade in Counterfeit Goods* p. 3
[10] Moises Naim. *Illicit,* p. 112
[11] Steve Hirsch, “Counterfeit seizures rise 83%”. http://findarticles.com/p/articles/mi_hb5244/is_200701/ai_n20944242
[12] Phil Taylor, “Fake drug sales 'could nearly double by 2010'” http://www.in-pharmatechnologist.com/news/news-ng.asp?n=62488-counterfeit
[13] Moises Naim. *Illicit,* p. 112
[14] http://www.iacc.org/
[15] Tim Phillips. *Knockoff, The Deadly Trade in Counterfeit Goods*, pp. 21, 22, 23, 24, 25, 71, 187, 214; Frank W. Abagnale. *Art of The Steal*, pp. 168, 172, 180; Moises Naim. *Illicit,* pp. 110, 112, 117, 118, 123
[16] *Knockoff, The Deadly Trade in Counterfeit Goods*, p. 4
[17] Mike Stobbe, “CDC Reports Dramatic Rise in Drug Deaths”. http://publicsafety.com/article/article.jsp?id=4879&siteSection=22; Cmdr John Burke, “Prescription-overdose Deaths Surpass Car-accident Deaths”. http://www.pharmacytimes.com/Article.cfm?Menu=1&ID=5059
[18] Joy LePree, “Risky Business”. http://www.manufacturing.net/Counterfeit-Drug-Trade.aspx?menuid=256
[19] “FBI 2006 Mortgage Fraud Report”. http://www.fbi.gov/publications/fraud/mortgage_fraud06.htm
[20] Laura Frieder and Jonathan Zittrain, “Spam Works: Evidence from Stock Touts and Corresponding Market Activity”. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553; Laura Frieder and Jonathan Zittrain, “Raw data and an interface that simulates a tax purchase” http://cyber.law.harvard.edu/stockspam/public/index.php
[21] Garth Bruen, “Search Stacking”. http://www.knujon.com/searchstack.html
[22] Peter Brockmann, Brockmann and Co. “The Spam Index Report: Comparing Technologies”. http://www.brockmann.com/index.php/20070717843/recent-reports/research/abstract-the-spam-index-report-comparing-technologies-july-17-2007.html; John Brodkin, “Anti-spam products ‘don't work’”. http://www.techworld.com/security/news/index.cfm?newsID=9539&pagtype=all
[23] Susannah Fox, “PEW Internet Posts.” http://www.pewinternet.org/PPF/p/1167/pipcomments.asp , http://www.pewinternet.org/PPF/p/1165/pipcomments.asp, http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/071107_sess1.pdf
[24] Moises Naim. *Illicit*, p 240
[25] Tyler More and Richard Clayton. “Examining the Impact of Website Take-down on Phishing”
[26] William Poundstone. *Prisoner's Dilemma*
[27] William Poundstone. *Prisoner's Dilemma*