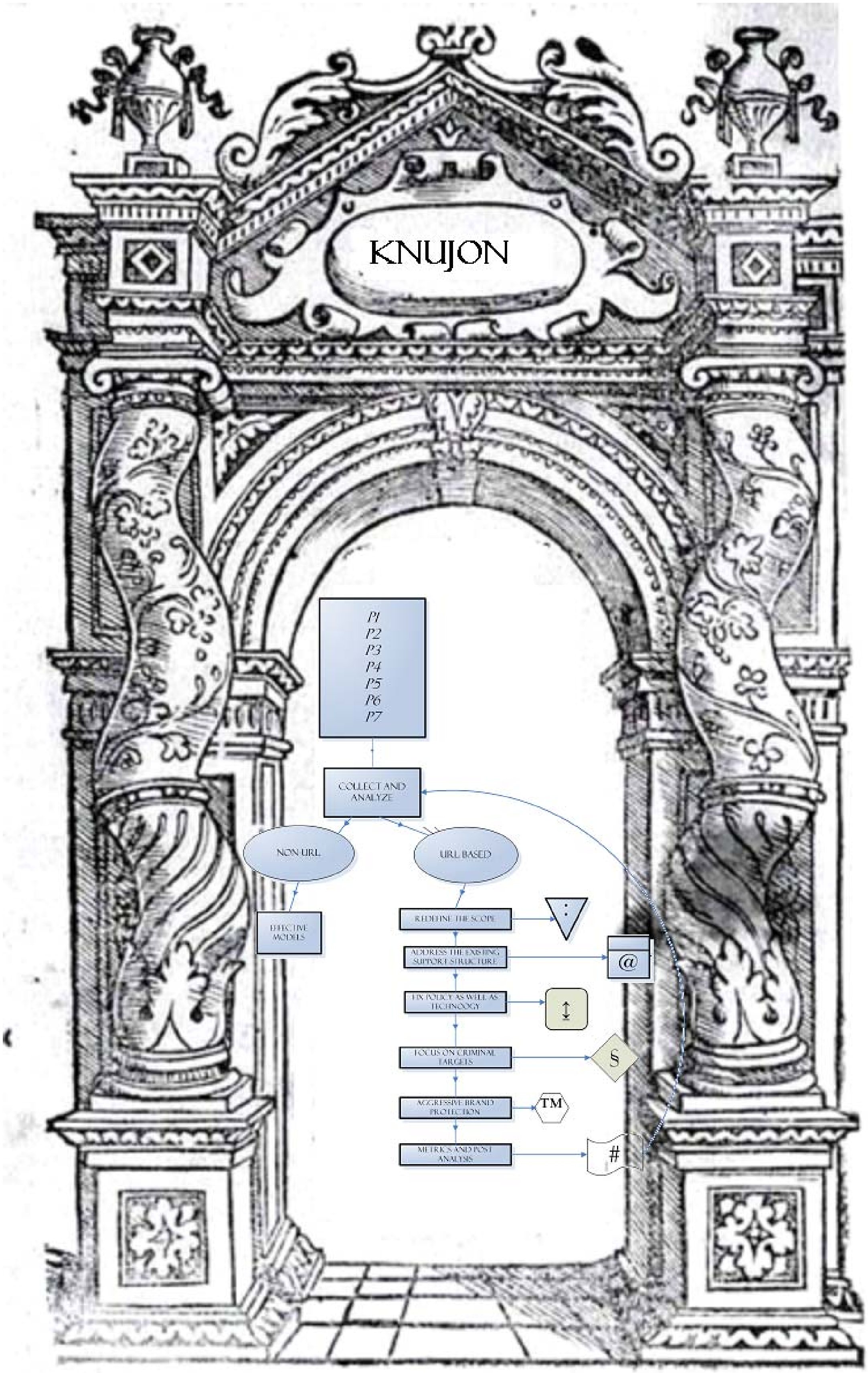
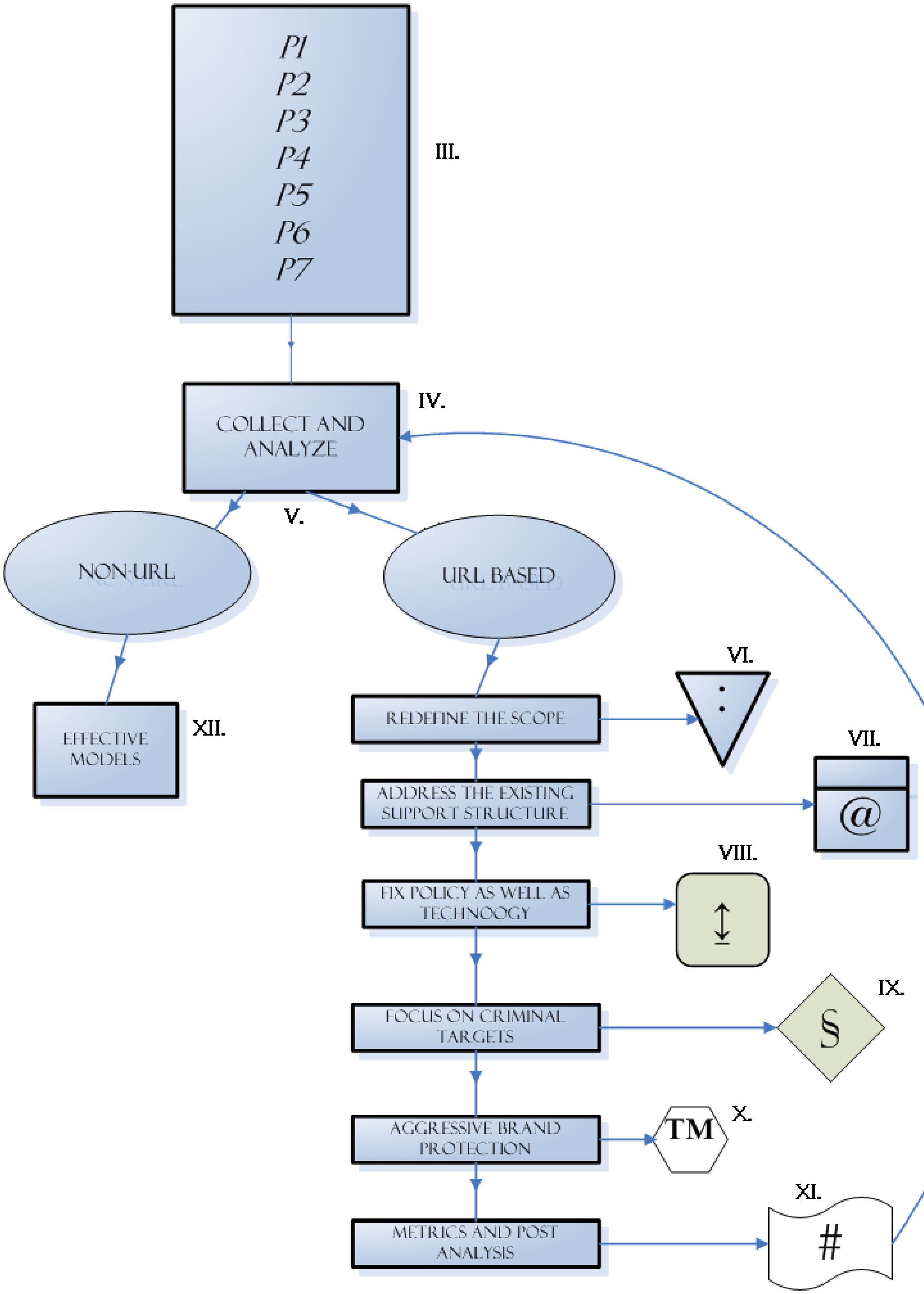
KNUJON


P1
P2
P3
P4
P5
P6
P7
COLLECT AND ANALYZE
NON URL
URL BASED
EFFECTIVE MODELS
REDEFINE THE SCOPE
:
ADDRESS THE EXISTING SUPPORT STRUCTURE
@
FIX POLICY AS WELL AS TECHNOOGY
↕
FOCUS ON CRIMINAL TARGETS
§
AGGRESSIVE BRAND PROTECTION
TM
METRICS AND POST ANALYSIS
#

The Future of Anti-Spam: A Blueprint for New Internet Abuse Tools

Garth Bruen, CEO Knujon.com LLC
gbruen@knujon.com

Process and Document Map


P1
P2
P3
P4
P5
P6
P7
III.
COLLECT AND ANALYZE
IV.
V.
NON-URL
URL BASED
EFFECTIVE MODELS
XII.
REDEFINE THE SCOPE
VI.
ADDRESS THE EXISTING SUPPORT STRUCTURE
VII.
@
FIX POLICY AS WELL AS TECHNOOGY
VIII.
↕
FOCUS ON CRIMINAL TARGETS
IX.
§
AGGRESSIVE BRAND PROTECTION
TM
X.
METRICS AND POST ANALYSIS
XI.
#

(Map of the Process and the Document)

Abstract: It is this author's contention that the efforts, technology, funding, and even critical thought in anti-spam development have been incorrectly focused on the email itself. In essence, the Internet security community has been "looking through the wrong end of the telescope." Resources poured into larger and larger filtering engines and algorithms have failed to reduce the volume and flow of unsolicited email. In fact, spam volumes have generally increased since filtering was declared the de facto solution. The problem is not really about flaws in SMTP (simple mail transfer protocol), or email clients, or even email security in general. Nor is the problem solely attributed to botnets and malware. Garth Bruen and Dr. Robert Bruen have developed a solution that is based on mass abuse data collection, data analysis, policy enforcement, public reporting, and infrastructure enhancement. The ultimate key to solving the spam problem is about blocking transactions, stopping the flow of money to criminals who hire spammers to market their illicit products. Doing this through the existing, but enhanced, policy structure addresses the issue without exaggerated costs or reinventing the Internet. This paper seeks to develop a philosophy of anti-spam based on clearly defined principles and a model that can be adopted by any anti-spammer, industry or country.

I. Introduction

This is not a complete technical solution paper, rather a set of guiding principles that solutions can be attached to and developed around. Before we can begin on any endeavor the real problem must be identified and our role as problem solver must be clarified. What seems to be missing from the anti-spam fight is philosophy, a philosophy that acknowledges failures and recognizes opponents to solution. The paper seeks to establish a new framework that is accessible to anyone in the anti-spam world, a kind of Christmas tree any engineer, technician, policy-maker or enforcer can hang his or her own ornament on.

Anti-spam is a multidisciplinary field. It is not just about discrete mathematics, but it does require a considerable amount. The effective anti-spammer must have knowledge in the areas of advertising, marketing, crime, policy, politics, economics, international affairs, journalism, statistics, psychology, and of course computer science. Because the problem does not just involve the delivery of email, it encompasses information, disinformation, reaction, fear, gullibility, consumerism, greed, naïveté, generosity, market shifts, and basic human needs.

Spam email itself is not an independent variable. Spam does not exist miraculously. Spam email is designed carefully with specific intent and measurable results. In the end, the actual email may be the least interesting and least important part of the organism of electronic or cyber crime. This is why the filtering/blacklisting model has limitations.

For the length of this fight we have been too focused on the actual spam email to the occlusion of the other portions of the problem, resulting in an ignorance of motivating factors and effects.

II. Failures and Limitations

Good cyber security comes at a large price. Even if a consumer is not directly paying for a spam filter, the cost is being built in to cable bills, ISP bill, phone bills, taxes, and general costs companies must pay to protect their own networks and transactions. Beyond security concerns, we all pay for the global network. It is generally accepted that junk traffic comprises an outrageous percentage of email routing on the Internet. The global network has been hijacked by persons unknown. Considering this, we must acknowledge that reliance on spam filtering alone is economic absurdity. Regardless of how vigorously defended an inbox is, the consumer is still paying for spam to be delivered just short of that inbox.

Filtering is based on the older paradigm of network security which is clearly concerned with keeping unwanted persons out of the network and allowing authorized persons access to the network. However, the Internet is collection of networks that was created for collaboration, mass communication, and commerce. In order to make use of the Internet, we must leave the network at certain points. A tightly secured network does not protect a brand name from being exploited on another network. Account information can be used to make unauthorized purchases without breaching a bank’s network. Network security professionals have also been reluctant to use countermeasures or proactive tools. It is unrealistic to be simultaneously connected to an enormous open network and also be cut off from it.

We also must ask if there is a mathematical limit to filtering utility. Studies of even the best consumer spam filters put the success somewhere between 90-99%. Even the best, most complex filtering allows some spam through. All filters are vulnerable to so-called “zero day” threats, attempts using new techniques not seen and tested before. Unknown to most Internet users, the anti-virus and anti-spam vendors are in a constant state of catch-up, collecting today’s threats to improve the protection tomorrow. This is not a proactive solution, regardless of success levels.

By discussing this, we are not suggesting that filters be turned off and removed. What we are requesting is that the filters be extended to report what has been filtered. In fact, many organizations are already moving in this direction by publishing reports on the worst offenders. Services like URIBL do not simply offer vast lists of blacklisted sites, but also categorize the junk traffic and sort it by Registrar. StopBadware, Symantec, McAfee, HostExploit and others have published detailed reports on ISPs acting at criminal conduits. This is the beginning of seeing spam as critical, usable information and not just trash.

The Anti-Phishing Working Group (APWG.org) and CastleCops (defunct) developed fantastic models for quickly taking down Phishing websites. This model is being extended to replace downed phishing pages with educational pages warning victims about online crime. This is also a step beyond the takedown model, building on success and digging deeper to solve the problem.

III. KnujOn Principles

We feel that the anti-spam effort is missing a code, philosophy, or a set of guiding principles that can be useful in developing new tools. Acknowledging these axioms puts the anti-spam thinker on a positive, success-oriented path.

Principle 1: *Spam is not an impossible problem to solve.*

No endeavor should begin with failure as the expected outcome. However, too many researchers and officials have already declared the spam war lost. KnujOn has documented many articles and papers where the author has asserted that spam is permanent; a fact of life on the Internet (http://www.pewinternet.org/PPF/r/214/report_display.asp). True, there will probably always be some spam, the question is about managing and minimizing the problem in ways that improve the overall structure of the Internet. Repairing or eliminating the conditions that allow spam to exist is possible, has already been done, and already documented as effective.

Principle 2: *It is possible to collect and process every piece of unwanted email for examination and enforcement*

If the technology and resources exist to create, route and deliver 100 billion pieces of spam each day then the technology and resources exist to capture, analyze and enforce against that 100 billion pieces of spam. This is not a technical issue; this is a problem of will. So far, no one has wanted to take on the problem. Governments, ICANN, business, and service providers have historically seen spam as “someone else’s problem.”

Principle 3: *Spam is about who benefits from it, not who sent it.*

This may be a difficult concept for some to grasp. The problem *is* spam and the spammer, but it is being driven and enabled by other parties. The main legal tool we have been given, CANSPAM, completely focuses on the spam and the spammer without acknowledging the criminal infrastructure behind it. We have been reminded many times by enforcement agents that law was not written to go after the beneficiaries. While there have been some arrests and civil judgments against spammers they have little effect on the volume of spam. Spammers are expendable and replaceable. Removing individual players from the spam world has little effect on the players driving the problem.

Principle 4: *Spammers send mass email because someone pays them to.*

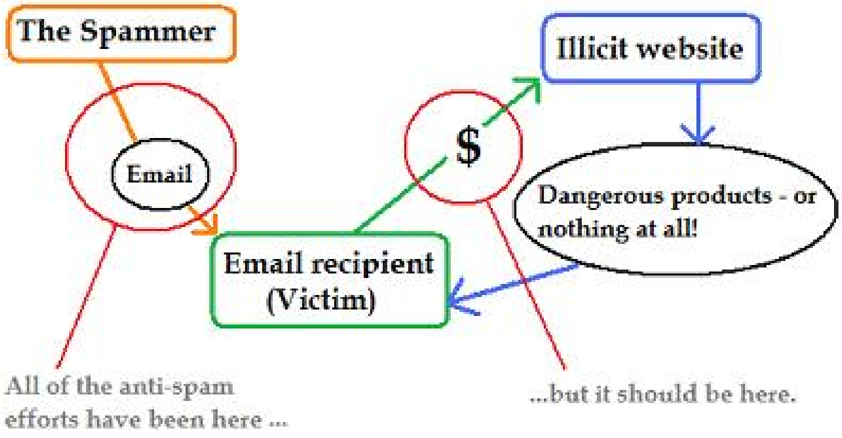
Spammers are mercenaries. It is arguable whether or not there is even such a thing as a “spammer” since spam is *tool* used by criminals and miscreants. Just as malware, botnets, social engineering, identity theft, intrusions, and fraud are tools. Today’s “spammer” may also be a bot-herder, malware author, phisher, counterfeiter, etc. In each case, illicit profit is the motivation for continuous engagement in the enterprise. There have been cases of political attack spam, or harassment and stalking spam but these are not sustainable, long-term efforts. Spam is not a philosophy or social movement. Spammers make contracts for work and receive payment based on effectiveness. They are paid to market an illicit product, illegal service, or phantom scam. It is also important to realize these are not so much “cyber criminals”, but criminals who use the Internet.

Principle 5: *The motivation is money, the goal is a transaction*

In exchange for payment, spammers are expected to deliver something to their benefactors: a transaction. Sending spam is not a transaction. Transaction occurs only when the recipient of the spam surrenders something the criminals want. Transaction in this sense has a broad meaning. It can refer the common definition where one party hands over money for a product or service, in this case illegal items. However, it can also refer to an exchange where the victim expects something but gets nothing. A transaction could be theft of identity, account access, or information. Transactions also occur when the recipient’s behavior changes because of the spam, as in the case of stock spam, money is delivered to the criminals in roundabout way because of the victim’s trade of that stock. A behavior-based transaction could also relate a situation where the spam-victim accepts stolen goods or laundered money to be transferred to a third party. The earliest examples of spam-based transactions can be seen in hoax or urban legend emails as recipients simply believed that something was true and forwarded the email onto other victims.

Principle 6: *Focus efforts on the transaction target or platform not on the advertisement.*

Unwanted advertisements are annoying, but it is not the problem only a symptom. Blocking spam email for one Internet user does not block another user from accessing the transaction. It is also important to mention at this point that email is only one type of spam. Instant messages, texting, faxes, blogs, banner ads, search engine ads, search result stacking, redirect hijacking, traffic hacks, domain vandalism, etc. have all been used to spam. Even the best tool for blocking email spam only protects email.

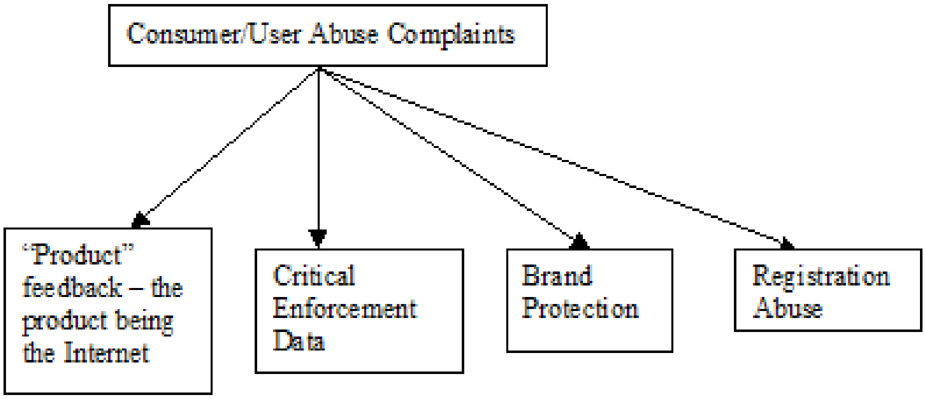

The Spammer
Email
Illicit website
$
Dangerous products - or nothing at all!
Email recipient (Victim)
All of the anti-spam efforts have been here ...
...but it should be here.

Principle 7: *Eliminating transaction access removes money from the illicit cycle.*

Illicit money does not enter the cycle through spam, it enters through a transaction site. As expressed by Foreign Policy editor Moses Naim: *"Illicit traffic is not about products, it's about transactions"* (http://www.moisesnaim.com/illicit/index.asp). Criminal profit exists because *something* desired is unattainable through legal channels, and it really does not matter what that something is. If cheeseburgers were illegal, their would be a black market for cheeseburgers. According to a Consumer Reports study, over half a million Americans buy something advertised in spam each month (http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/spam/0709_net_spam.htm). This is even with mass anti-spam filter deployment. Spammers still reach customers and billions of dollars continue to enter the illicit economy.

IV. Data Collection = Consumer Enfranchisement

By publicly and freely collecting spam we can address two problems with one process: (1) A lack of samples/data/evidence and (2) Angry Internet consumers. In this context, we have to re-categorize spam not as *junk* but as vital data. Forget for a moment that our goal is spam elimination. Consider the Internet as a new product that is still evolving. All initial products have flaws, either in design, appearance or function. These flaws cannot be addressed without consumer feedback. Abuse data is the best, richest feedback data set for the Internet.


Consumer/User Abuse Complaints
'Product" feedback – the product being the Internet
Critical Enforcement Data
Brand Protection
Registration Abuse

Unwanted email tells us exactly what the Internet user dislikes, it reveals al the places network security is weak and people are gullible. And for ten years the Internet user has been told to delete this data. If spam is a crisis, victims of a crisis typically want one thing: to be heard. Victims want the ability to bring their issues to an authority who will accept them. However, spam victims have been turned away by government and the Internet industry. No one has wanted to take responsibility for this issue which has left the consumer resentful and mistrustful of the Internet. This can easily be changed by massive outreach campaign that shows Internet users how to report their spam. Many spam submitters to KnujOn expect nothing in return, no reports or response; they are just like the idea that someone will take their junk email.

Even if consumers take the time to report spam, the process is arduous. Reporters are required to know about HTML source code, email headers, IP addresses, Whois, spoofing, ASN numbers, upstream providers, etc… When reporting spam, victim's own mailboxes or IP addresses are often flagged as spammy and blacklisted. Reporters are expected to know the difference between phishing and other spam. The victim is trusted to find the right place to report the spam and is often additionally abused by rude ISP or Registrar contacts. Individual abuse reports are rarely acted on and completely ignored by service providers in league with the criminals. Silence is the most frequent reward the time and effort as reporters rarely receive feedback or thanks. The burden on the end user is an unrealistic expectation that represents a completely failed model. The best strategy for the future is to freely encourage spam victims to report and return information for their efforts. This is exactly what KnujOn has done with excellent results.

V. Sort, Categorize, Analyze

Spam can be divided into many subgroups, but the major, top-level categories are: URL-based spam and Non-URL-based spam. Spam that contains a website link as the advertizing target are profoundly different than spam that advertise stock symbols, phone numbers or other information. The difference is that there is already a vast policy structure dedicated to websites and the domain name industry. This is not to say that Non-URL spam cannot be addressed, it just has to be addressed by other mechanisms. This would be the case even if the offered item was the same in both categories (e.g., fake employment phishing) because without a related domain name the policy addressing them would be useless. Spam that uses an image or some other contrivance to advertise a domain name, as opposed to text or HTML code, is still URL-Spam. The domain-related spam and illicit traffic has been the focus of KnujOn's work and success up to this point. KnujOn still collects and analyses Non-URL spam but has not developed comprehensive tools to address it. There are, however, many effective models for success against Non-URL spam discussed in section twelve.

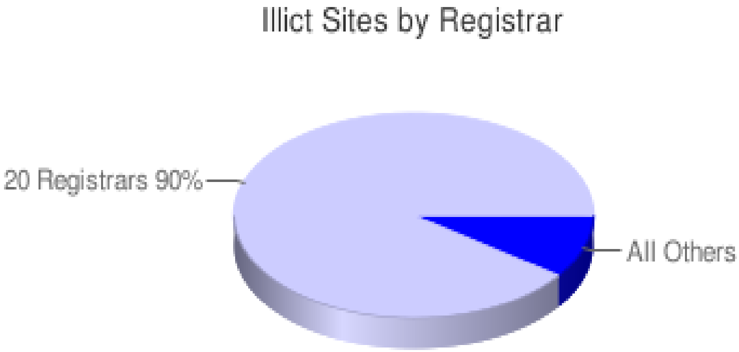
Capturing the domain name and then discovering the support structure behind that domain name is the critical part of this operation. Gathering and parsing all related records for an illicitly advertised domain connects this instance to other potentially related instances. Once domain information has been captured and recorded, any further instances become statistics. For this process we are not concerned by the email itself, the origin or header analysis, the crucial data is the advertised site. By thinking of this in terms of, say, *456 instances of spam for this domain*, rather than *456 spam emails*, we have completely changed the perception of the problem and taken focus off the high count of email by shifting it to background information about a single website.

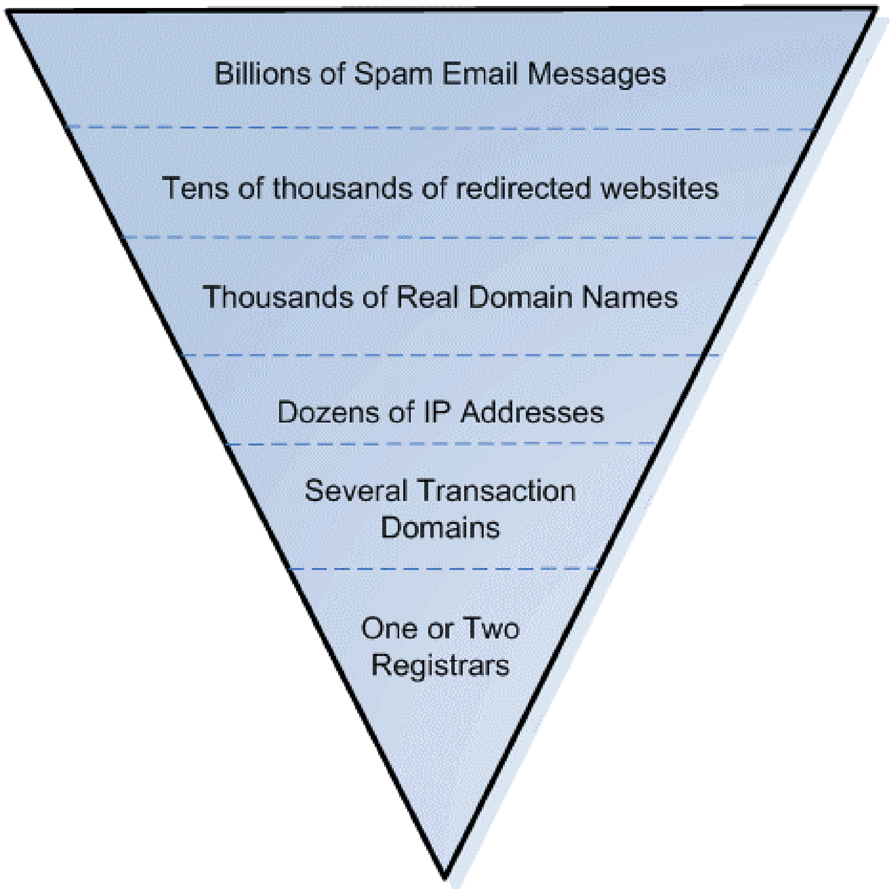
Because the website or domain name is now isolated for analysis, it becomes the target instead of the spam itself. What content is at the site and public records associated with that site help connected individual sites to illicit networks. Statistics on illicit activities at featured sites show e-crime trends and types of spam attacks that are declining or increasing. Understanding and addressing each category makes the problem more manageable. Viewing the problem as 50 fake pharmacy sites, 20 software piracy sites, and 10 phishing sites provides clarity that “80 spammed sites” does not.

VI. Redefining the Scope

In 480 BC the Greeks faced an invading Persian army that was allegedly one or two thousand times the size of the Greek army. In the face of these overwhelming odds the Greeks used math to hold off the invasion. In short, by forcing the Persians to fight at the narrow pass at Thermopylae, the Greeks changed the size of the battlefield. The extreme size of the Persian army became irrelevant and they had to fight in close hand-to-hand combat, at which the Greeks excelled (http://www.historynet.com/greco-persian-wars-battle-of-thermopylae.htm).

In the face of overwhelming odds, tactics dictate better ways of handling the threat than attempting a one-on-one response. An estimate from this time last year stated 100 billion spam emails were passed through the Internet every day (http://www.senderbase.org/generated/big_spam_volume_lastweek.png). In trying to even approach this problem, in an enforcement context, many are deterred by the vast numbers and improbability of successfully enforcing policy for each one (and then processing another 100 billion the next day). It is no wonder that the inability to address the spam problem is seen by most as gospel. In truth, the spam problem only seems this big. The billion-per-day spam counts are noise, illusion. Spam is noise because the billions of emails sent to billions of mailboxes advertise many of the same websites. In fact, the ratio is so dramatic one might wonder why so much attention has been paid to email all this time. However, this is just the beginning of our reduction exercise. The fewer number of advertised websites is further reduced when we realize many are simple redirect pages to a smaller number of real domain names. These domain names are in turn hosted a minority of actual IP addresses and served from a handful of name servers. While many domains in a spam campaign advertise the same product, actual purchases and processing only happen on one or two websites linked from the advertised site. Finally, we find that all the domains are sponsored by a fraction of companies within Registrar industry, less than 20 companies out of 900, and ICANN oversees the all of these companies. At this point the problem becomes quantifiable, manageable and finite.




Billions of Spam Email Messages
Tens of thousands of redirected websites
Thousands of Real Domain Names
Dozens of IP Addresses
Several Transaction Domains
One or Two Registrars

Registrars become the chokepoint. Since criminal Internet operations often use stolen credit cards, identity theft, compromised IP address, and whois fraud to set up their networks the Registrars are the only real, identifiable responsible party. Addressing illicit networks at the provider level has been extremely effective. Cutting off needed resources, the criminals are forced to move on to other providers. Some might see this as futile until one realizes the number of Registrars willing to cooperate with criminals is declining.

VII. Addressing the Support Structure

Now that we understand the problem has a quantifiable set, it becomes easier to manage from a structural perspective. Just as Maslow's Hierarchy of Needs dictates we need air, water, food, shelter, etc. to survive, illicit Internet commerce has a required structure to exist. The requirements are really the same as any Internet business, services to: sponsor a domain name, host a domain name, serve the domain name, deliver content, and process transactions. The industry that provides these services is, in theory, identifiable and accountable. While the cyber criminal may be largely anonymous, companies providing them services are not. In their defense, many companies are unwillingly and unknowingly providing services to criminals. However, KnujOn and other organizations have been specifically telling service providers which customers are really criminals. The difference between a good service provider and bad one is how they handle the problem after being notified. Our first move is to have a domain name removed because of various policy violations. Of course, a raw IP address will still deliver content without a domain name, so we target that as well. No website, no transaction.

By taking away the criminal support structure piece by piece, we eliminate the platforms for transactions. This starts with individual site removal, the “takedown” model. Then we work our way to entire illicit network identification and elimination. In this process we frequently encounter service providers reluctant, unwilling or unable to cooperate. When this happens we assert pressure through regulatory agencies, law enforcement, business relationships, and public disclosure. At this level there have been a number of additional problems to solve: lack of data, will, effective policy, enforcement tools, resources, and faith. KnujOn has been working diligently to collaborate with government, law enforcement, ICANN, Registrars, service providers, consumer advocates, the press, and businesses to close gaps in resources and knowledge.

KnujOn’s work has been considerably focused on the existing compliance structure, where it fails and how to improve it in order to achieve our objectives more effectively and extend this utility to the community in general.

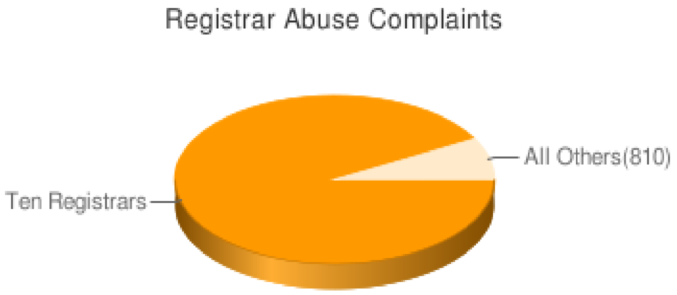
VIII. Fixing Policy and Technology

At the intersection of policy and technology there is a traffic accident. The ability of the marketplace to develop and release new products will always outpace the security community's ability to test those products for safety and exploits. The ability of criminals to exploit new technology will be quicker than government's ability to obtain enforcement tools. Policy is often created without process to execute the policy and frequently procedures are developed without guiding policy.

Benjamin Edleman from the Berkman Center at Harvard testified before congress in 2003 that the Whois database was "substantially fiction", meaning it was rife with uncorrected inaccuracies and deliberate forgery (http://cyber.law.harvard.edu/people/edelman/pubs/judiciary-090403.pdf). In 2005 the U.S. General Accounting Office released a study of Whois accuracy that not only determined that the fraud was wide-spread but the false records were clearly tied to criminal operations (http://www.gao.gov/htext/d06165.html). These problems had been known about publicly for years yet very little had been done. We suspected that there was not only a lack of will but a lack of good policy and missing technical tools. Drawing from the work of these two studies, KnujOn examined the existing policy structure at ICANN for handling these issues, the Whois Data Problem Reporting System (WDPRS). KnujOn developed a system that would verify the accuracy of Whois records relating to domains advertised in spam and then submit and follow up with complaints through this system. KnujOn submitted and tracked hundreds of thousands of complaints over several years.

Our evaluation of ICANN's compliance system is that current processing and staffing levels are not designed to meet the size and scope of today's Internet. Various illicit enterprises have subverted the current domain name system by taking advantage of poor accounting standards and a lack of oversight on the part of the Registrars. While KnujOn had enormous amounts of data, ICANN's daily limit for accepting reports was far below what we could produce. Additionally, the volume of these reports placed increasing strain on ICANN's compliance system. The WDPRS system itself was released in 2002 and not upgraded since. In the six intervening years criminals developed their own "crimeware" to falsely register thousands of domains and populate them will illicit content. We recommended the department be re-staffed and the WDPRS be upgraded. Recently, we got our wish. The WDPRS was overhauled to handle high-volume submissions and the compliance team was enlarged. However, the problem was about more than technical resources.

Our research in this area showed the false whois problem was intensely concentrated at a small number of Registrars. These Registrars continuously flouted ICANN policy by not correcting false whois records and/or terminating the offending customer accounts.



KnujOn also discovered that not only were Registrar customers hiding, but so were some Registrars. KnujOn found dozens of Registrars that had false business addresses or posted no address publicly at all (http://www.knujon.com/news2008.html#06102008). Several Registrars with absent or falsified contact data were sponsoring domains involved in obvious criminal activity. However, KnujOn discovered that there is no obligation for Registrars to publish their location under the existing contract, known as the Registrar Accreditation Agreement (RAA). This loophole created a permissive environment where the, theoretically self-policing, Registrars acted with impunity. KnujOn lobbied ICANN successfully to add disclosure language to the RAA as follows:

> *3.16 Registrar shall provide on its website its accurate contact details including valid email and mailing address*.
> (http://www.icann.org/en/topics/raa/amendments-report-gnso-12dec08-en.pdf)

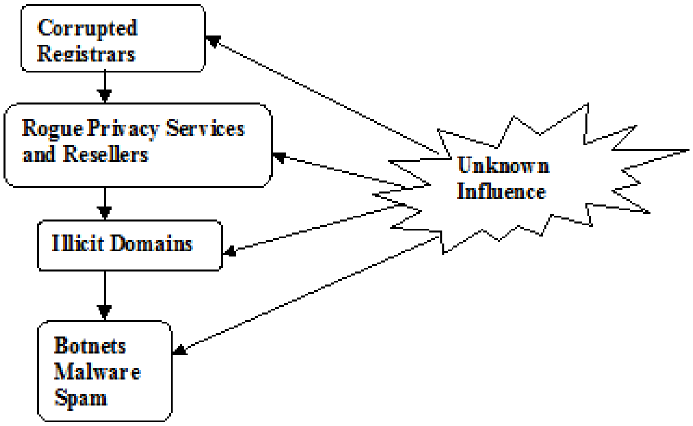
This is just one simple sentence that alters the acceptable behavior of the entities that issue domain names. Attempting to hide or obfuscate is now a violation of their contract.

Two problems, one technical one policy-related. Both exposed by data collection, testing and analysis.

IX. Use the Law When Called For

Every spam email does not necessarily lead to a clearly identifiable crime. It would be an ineffective use of public resources, and a possible mass privacy violation, for law enforcement agencies to review every instance of unwanted email. Furthermore, what is illegal in one place may not be somewhere else. However, the bulk of spam email is directed at something illegal. KnujOn's research suggests that 80-90% of the spam, domain abuse, registration abuse, whois fraud, malware deployments and associated activity are related to illicit drug trade.

At the beginning of this project, several years ago, it became apparent that every layer of the Internet's infrastructure was being influenced by an unknown entity. All had been corrupted to some extent but who was pulling the strings was not immediately clear.



After careful analysis of data from every quarter of the Internet's infrastructure the culprit appears to be drug money. Not cocaine, heroin, or so-called street drugs, but diverted and counterfeit pharmaceuticals. The underground Rx market is enormous. Prescription abuse and overdoses are exceeding illegal narcotics in some places due to a false perception among users and dealers that it is safer than traditional narcotics traffic. While lifestyle drugs like erectile dysfunction pills or pain killers are favored spam citations, the unlicensed online pharmacies are trafficking in illicit heart, blood pressure, diabetes, and cancer medication. The proliferation of such drugs is not completely known at this time and vigorous research should be conducted to find out how bad it is.

Consumers often wonder why the government or police cannot do more about spam and cyber crime in general. What consumers do not understand is that in order for law enforcement to take action they need victims and evidence. If spam victims delete and do not report spam the police cannot act. U.S. law enforcement and security agencies have actually been criticized for mass communication surveillance. The government is generally reluctant to attack this problem without having real citizen victims participate.

There is also a somewhat misleading perception concerning the real location source of criminal organization and operations. Some studies claim most spam comes from outside the U.S., other studies claim most spam originates within the U.S. (http://www.boston.com/business/globe/articles/2007/03/19/firm_says_us_is_hotbed_of_illegal_cyber_activity/) Both studies are correct. While most of the large criminal networks are based overseas, they rely heavily on U.S. Internet resources to host sites and send email (http://www.knujon.com/discountpharmacy.pdf). This is a cause for concern as well as an opportunity. As the number an type of illicit activities on the Internet increases, it also becomes more localized. Prostitution is becoming a growth industry on the Internet (http://www.boston.com/news/local/articles/2008/07/05/brothel_arrests_cast_a_shadow_in_wellesley/) with the belief that this is safer and more discrete than traditional “street” prostitution. Spammers are being recruited to promote prostitution (http://www.knujon.com/news2008.html#12082008).

The KnujOn process isolates and extracts obvious crime data, there is no shortage of it. This information has also been effectively used to build profiles of online criminal organizations, predict trends, and stop illicit activity. The problem has been getting the right people and agencies to follow up on that information. However, the situation is gradually changing. With public-private cooperation through organizations like the High Technology Crimes Investigation Association (HTCIA.org) and InfraGard (infragard.org) we have been able to work directly with skilled investigators who can follow up on criminal activity. This allows law enforcement to receive presorted data saving time and avoiding the perception of mass surveillance. This also deters the drift towards a crackdown on all messaging just to find the criminals. Problems that appear large and unsolvable often gestate heavy-handed responses from society. When governments are pushed by citizenry to do “something” about a problem, the result is often a poorly designed and rushed response, CANSPAM being a perfect example in this case. The law puts the burden on the spam victim of identifying the spammer and proving that certain number of unsolicited messages were sent during a certain period of time. This law does not consider the illicit activity or financial incentive behind spam.

X. Brand Protection

Brand protection is critical to the overall spam solution. As we have described above, the criminals want a transaction and that transaction often concerns something stolen, copied, or misappropriated. Brand owners have the greatest incentive to address spam aggressively since they are victimized in several different ways by a single spam. If a consumer completes a brand-jacked transaction based on spam, the brand owner not only loses market share in their own product and potential profit from the sale they are also exposed to liability if a consumer is harmed or loss of brand identity if the consumer is dissatisfied by the knockoff.

The scope of brand jacking is far beyond consumer goods. Phishing, is in fact brand jacking. Besides financial holdings, a bank's name is its most important asset. The value of a bank's name is degraded by repeated attempts to compromise accounts. Even if the bank's network is never actually penetrated, public perception is harmed by volumes of spam that include the bank's name.

Consider illicit pharmacy. Not only is name of a pharmaceutical trademarked, but the formula for the drug as well as are shape, packaging and associated icons and type font are often protected. Some drug packaging has extra security features like holograms that have also been counterfeited. Shipping cartons and associated customs information are faked creating a parallel and completely fraudulent supply chain. Not just the pill, but the entire corporate identity of the pill.

After pharmacy, software piracy is one of the largest targets. The problem is believed to be critical in developing countries where even the government uses pirated software. This is very serious when considering that drafting software (AutoCAD) for machinery and vehicles might be counterfeit or tax software that captures name, address, income, place of employment, bank account number, and social security.

The common tactic of “spoofing” and email header by using one network's unsecured email port or HELO and then substituting the sender domain with another one is also brand theft, especially if one of the domain or network names is itself a protected brand. In the process executing a spam campaign the reputation of involved Registrars and ISPs are also harmed. Because of this, they would also benefit from aiding us in our work.

KnujOn and similar organizations may have developed clout with law enforcement and service providers in order to get illicit sites removed, but there are some claims and efforts we cannot undertake without the help of the brand owners. The ability of Internet enforcers to act on behalf of the commercial entities would be a game-changing tool. KnujOn has no trouble extracting and sorting vast amounts of data on compromised brands. Having those brands engaged in the problem is difficult.

XI. The Daily Tally Equation

Each of the above items can be placed in a flexible process that when run continuously and recursively become a juggernaut of Internet enforcement and analysis. Each part of the process is a line item in a kind of balance sheet. The first value in this balance equation is the total unique domains extracted from spam processed in a day. Many of these domains will turn out to be inactive, the automatic spam bots do not know their targets have already been suspended. Some extracted domains are spoofed and therefore do not need enforcement action other than reporting it to the real owner. A portion of the remaining domains are often immediately discovered to have known policy violations and can be reported and suspended quickly. The policy violations range from false whois, unacceptable use, breaching terms of use, etc… These are only useful when

The leftovers require more analysis. This is a way of evaluating our success and pinpointing where the next target of concern is or where new bottlenecks are. This exercise illustrates that the problem is manageable.

Total domains reported
-Sites with some confirmed action (WDPRS or other)
-“Spoofed” domains or errors
-Old, inactive and defunct

Total with no action, Why?
  >no information
  >not processed
  >no violation found
  >uncooperative service providers
  >no engagement from harmed party

“No information” is a simple issue of retooling the data discovery process. Continuous technical improvements will address this set. Some items will fail to be processed and can be placed back into the cycle. For the other “no action” remainders, examine them and develop new strategies. As explained previously, problems with ICANN represented the first large obstacle to a solution. We have made significant progress in this area and will continue to do so. After addressing policy and process issues with ICANN, the biggest area of concern is illicit online pharmacy and controlled substances traffic. This illegal and unregulated activity represents 80-90% of the spam problem currently. Engaging law enforcement on this will produce significant reduction Potential success here should be seen throughout 2009. This proactive shift could be further improved with support from the pharmaceutical and pharmacy industries who have yet to engage us. The equation can be adjusted with the law enforcement engagement as a factor.

Total domains reported
  - Sites with some confirmed action (WDPRS or other)

- "Spoofed" domains or errors
- Old, inactive and defunct
- **Drug-related Domains for L.E. processing**

Total with no action, Why?
 >no information
 >not processed
 >no violation found
 >uncooperative service providers
 >no engagement from harmed party

The next two critical categories are software piracy and brand-related domain abuse (includes counterfeiting, knockoffs, coupon fraud, etc…). We have significant data that allows us to develop strategies to address these abuses but we lack the engagement of the brand holders and software manufactures. With their support we could mitigate their loses and add this factor the equation. We can also remove the failure factor.

Total domains reported
- Sites with some confirmed action (WDPRS or other)
- "Spoofed" domains or errors
- Old, inactive and defunct
- Drug-related Domains for L.E. processing
- ***Software piracy mitigation with authority from manufacturers****
- ***Abused brand owner advocacy and support***

Total with no action, Why?
 >no information
 >not processed
 >no violation found
 >uncooperative service providers
 ~~>no engagement from harmed part~~y

**Potential factors*

Once we have accounted for the clear factors we still have a large remainder. An enormous number of abused domain names are not associated with illicit pharmacy, counterfeit goods, software piracy or any specific product or service. An examination of these remaining domains reveals a very complex scheme to manipulate the domain name market on behalf of certain Registrars and resellers. Domain names have become a kind of currency and this practice, we refer to as "domain inflation" seems to be a common tool used by manipulators to increase the value and exposure of certain domain names before and during bulk auctions. This situation will require thorough research and documentation, but is believed to function as follows. Mass spam campaigns are being used to advertise longs lists of domain names. The spam emails are generally nonsense and do not seem to offer any specific product or service. The content at the featured domain is typically a message indicating that the domain is for sale, no illicit products are offered. It is assumed that these click-throughs are recorded on server logs and these artificially-inflated numbers are used to justify increased domain resale prices.

The final standout issue is dealing with uncooperative Internet Service Providers. Our research has found that the illicit networks rely and depend on U.S-based sponsorship and connectivity. It has also been documented that many of the U.S.-based ISPs are unwilling or unable to handle the abuse and infiltration of their bandwidth. In some cases even large and well-known telecommunications companies have refused to terminate sites selling controlled substances, citing a lack of priority or authority. In fact, many ISPs will quickly act on IP addresses sending spam and fail to act IP addresses dealing in dangerous illegal products. It may be required to address this problem with the telecom industry at a higher level and formally request their cooperation. We have no problem documenting abuses and supplying data on illegal activity, the only problem is the lack of response.

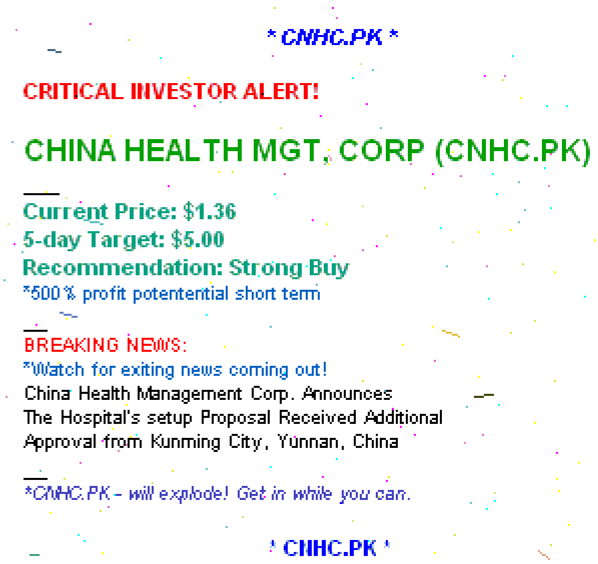
A successful tally process would further isolate any remaining domain abuse issues.

Total domains reported
- Sites with some confirmed action (WDPRS or other)
- "Spoofed" domains or errors
- Old, inactive and defunct
- Drug-related Domains for L.E. processing
- Software piracy domain mitigation with authority from manufacturers
- Abused brand owner advocacy and support
- **Investigation and enforcement against unfair domain market practices**
- **IP Content-level termination of illicit sites making domain termination redundant**

Total with no action, Why?
  >no information
  >not processed
  >no violation found
  ~~>uncooperative service providers~~

XII. Non-URL Successes

Much of KnujOn's work and the focus of this paper have been on domain-related spam, but one of the greatest, and poorly known, success stories in the anti-spam world deals with Non-URL spam, namely stock spam. In 2005 and 2006 it seemed there was nothing but stock spam. Criminals made real profits by short-selling penny or "pink sheet" stocks they artificially inflated through spam (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553#PaperDownload).



* CNHC.PK *

CRITICAL INVESTOR ALERT!

CHINA HEALTH MGT, CORP (CNHC.PK)

Current Price: $1.36
5-day Target: $5.00
Recommendation: Strong Buy
*500 % profit potentential short term

BREAKING NEWS:
*Watch for exiting news coming out!
China Health Management Corp. Announces
The Hospital's setup Proposal Received Additional
Approval from Kunming City, Yunnan, China

*CNHC.PK - will explode! Get in while you can.

* CNHC.PK *

Now, in 2009, stock spam seems to have vanished. How did this miracle occur? The Security Exchange Commission under Chief John Stark began soliciting spam submissions from the public and collected an enormous volume of samples. Stark's investigators analyzed the stocks featured in the spam, not the spam itself, and suspended trading of the featured stocks. Investigators determined who was profiting off the short-selling, froze their assets and indicted perpetrators domestic and foreign. Problem has been minimized and managed.

This is more or less the model we have discussed in this paper: solicit, collect, analyze, enforce using existing policy (http://www.johnreedstark.com/ClassMaterials/StarkArticles/spamarticle.pdf). This is a basic model that can be applied to any illicit Internet activity.

XIII. Conclusion: What is Needed Next

Any anti-spam model in the future should follow this path: reach out the victim and collect data, analyze, report to services, enforce policy, report crime to law enforcement, publish and share findings.

1. Built-in email tools that allow easy reporting for users
2. Ability to collect and process mass amounts of spam email
3. Interfaces that help Internet victims navigate the bureaucracy
4. Retool or add-on to existing filters the ability to forward collected spam or extracted data
5. Creating and promotion of a Consumer Malware Damage Claim Reporting System to track loses in the private sector
6. Better public awareness that spam reporting services exist and work
7. Malware analysis that identifies beneficiaries as well as sources and authors

The spam problem can be solved. The Internet can be better.