Wars Within

It's not just spam anymore

Orlando Padilla
xbud@g0thead.com

Last modified: 09/19/06

0.1 Abstract

In this paper I will uncover the information exchange of what may be classified as one of the highest money making schemes coordinated by 'organized crime'. I will elaborate on information gathered from a third party individual directly involved in all aspects of the scheme at play. I will provide a detailed explanation of this market's origin, followed by a brief description of some of the actions strategically performed by these individuals in order to ensure their success. Finally, I will elaborate on real world examples of how a single person can be labeled a spammer, malware author, cracker, and an entrepreneur gone thief. For the purposes of avoiding any legal matters, and unwanted media, I will refrain from mentioning the names of any individuals and corporations who are involved in the schemes described in this paper.

Disclaimer: This document is written with an educational interest and I cannot be held liable for any outcome of the information released.

Thanks: #vax, Shannon and Katelynn

0.2 Introduction

It is inherently obvious to anyone who owns a computer that the Internet has changed the world around us in a significant number of ways. From an uncountable number of careers to a world-wide open market, it drastically affected everything around us. Don't worry though, I will not bore you with another "The future will look like this ... " article. For that, I will refer to you a great book by Michio Kaku called *Visions* that is remarkably accurate considering it was written in the mid 90's. But anyway, why am I restating the obvious? To allow myself to focus on one not so obvious division of an existing market developed by a corporation that had previously filed for bankruptcy. I will elaborate on how it "innovated" one particular market and how that change resulted in a ripple of disaster and greed. The market is real estate and my focus is on mortgage leads [1]. I will begin by explaining what mortgage leads are, why they are worth writing a paper about and how

[1] The idea of finding, selling and stealing leads is anything but new, in fact Hollywood made a movie based entirely on the importance of sales leads titled 'Boiler Room' starring Giovanni Ribisi, Ben Affleck and Vin Diesel [Boiler]. The movie illustrates a perfect example of the significance of even one major lead

certain individuals have made millions off of them. I will then discuss the roles of the connected individuals and how they continue to work when trust is the single point of failure. My decision to write this article is nothing more than informational, I have no intentions of ruining the lives of the people who make a living from what I am about to discuss. In fact, it is to my knowledge not much of a secret at all but I found it fascinating and wish to share my experiences with anyone willing to listen.

0.3 Guidance

As I was growing up, my parents discouraged me from working while attending school. They made a genuine attempt to provide for me the support that I needed so that I could focus exclusively on my academics. Their reasoning for this was simple - *Once you start making money, you'll forget what is important in life and will simply want to follow this path.* As you read through this paper, ask yourself how true this actually is.

Financial gain drives every market around the world, and quite honestly there are very few things the world as a whole has not yet done for money. To quantify what my parents' believe, I will describe how the lives of the people involved vary from the lives they once lived, and from the lives of a person working a nine-to-five job.

0.4 The Entity

Mortgage leads, referred to as leads from this point on, are nothing more than a selective set of criteria consisting of the following:

```
First Name
Last Name
Phone
City
State
Zip
Email
Loan Type
Loan Amount
```

`Affiliate ID`
`Domain Ref.`
`Date`

Each lead must contain at least the above criteria with the exception of perhaps Affiliate ID and Domain Reference to be worth anything to a buyer. Furthermore, the more reliable a set of leads is, the more it is worth to a buyer. A buyer? You ask. Well, financing firms are indirectly involved in this scheme; finance firms take the information you sold to them, and follow up with the people allegedly interested in buying, refinancing or applying for a home loan.

0.4.1 Background

To fully understand who is selling the collected information and to elaborate on who is buying the information listed above, I'll introduce hypothetical `Corporation A` to play the role of the real company. Corp. A is a mortgage firm on the fall, not only are they on the verge of closing shop but they have already filed for Chapter 11 bankruptcy and are out of viable options for recovery. As a last resort they decide to offer money in exchange for possible loan application candidate *leads*. This quickly gained momentum as the Internet was a prime place for accumulating such information. The plan eventually imploded, but before diving into what the outcome was, I'll elaborate on how this truly became its own market.

0.4.2 Numbers

Initially each collector[2] averaged about `200` leads per sale which drove just enough profits to keep the company afloat. A lead was first bought at a flat rate of `10` US dollars which at an average of `200` per sale the profit for the collector was a comfortable `2,000` US dollars. On the flip side of things, Corp. A was successfully conducting business averaging about `10` sales for every `100` leads they bought. With these numbers consistently coming through Corp. A made a profit of about `10,000` US dollars for every successful sale. A little math illustrates the return on investment ratio:

[2]The term collector in this paper in its loosest sense is a name given to an individual who collects mortgage leads for the purpose of attaining a profit.

Investment —	Average Profit —	Return on Investment
200 x 10 = 2000 —	10,000 x 20 = 200,000 —	200,000 - 2,000 = 198,000

Figure 1: Return on Investment

Based on the collection of an insignificant amount of information, collectors aggressively innovated their collections methods. I will elaborate on what I mean shortly. For now, I will focus on what happened immediately after.

New collection methods drove the lead delivery out of control and soon Corp. A was inundated with so many leads that they had to start turning them down until they figured out how to process the volume. In order to handle the number of leads they were now attaining, they decided to partner with smaller companies and sell them the overflow. Corp. A was now growing exponentially fast, and in a period of roughly five to six years, this simple idea drove Corp. A from bankruptcy to a multi-billion dollar corporation.[3]

People and greed do not mix very well, and as I mentioned, earlier collectors and partners wanted more money, so soon other companies began buying leads from collectors too. I argue that at the time the mortgage industry was large enough for everyone to profit nicely from it, however greedy collectors began selling bogus or non-exclusive leads. This forced mortgage firms to develop a loose classification model for grading the quality of a lead as an addition to the classification of the leads themselves.

Exclusive

An exclusive lead is one that is sold only to one mortgage firm and never again redistributed. The value of these leads was often higher than non-exclusive, or as they decided to term them, *semi-exclusive* leads.

Semi-Exclusive

Yes, semi-exclusive. I honestly cannot define this, as this is an oxymoron itself, but someone somewhere[4] decided to call non-exclusive leads semi-exclusive to allow them to be resold. It's a nice euphemism, though.

The reliability of a bulk set is assessed by the person buying them at the time of sale. The person interested in buying the leads takes a random set

[3]It is actually rumored that at one point in time this company consumed 100% of the mortgage leads ever processed in the United States.

[4]An individual who wishes to stay anonymous informed me of terms commonly used.

Grade	Description
Green	Confirmed Valid Lead
Yellow	Characteristics of a bad lead but enough good to buy
Red	Confirmed Invalid Lead

Figure 2: Weighed Leads

from the bulk he is receiving and personally verifies their validity. A rating is then given depending on the number of missed leads he finds. The grading is different with every person you deal with, but in short a lead is only Green if validated.[5]. A yellow lead is a lead with all information accurate but the candidate was either not home or for some reason was not available. Last, a red lead is a confirmed invalid or bogus lead. A number of things can give away a bad lead, for example *Zip code and State* not matching, or the name given is *John Doe* and the address contains *Elm Street* are probably indications of a bad lead.

0.5 The War

Now that I have indulged you with the whereabouts and importance of a lead, I will discuss how they are obtained. I mentioned above how far an individual would go as a result of greed? Below I describe their actions, which outlines their (at times) unethical behavior and persistence to attain more of the *goods*.

0.5.1 Self Indulgence

When the collector decides to go a straight route (in terms of their industry), they can invest some time and money into setting up an infrastructure to lure potential clients to their web site. They first need to build a site that resembles a loan agency that allows visitors to send their applications to them. Once the collector has a website saving information to a database, he now hires *mailers* or spammers to advertise his website. The average return on spam has been extremely dynamic, and with more advanced filtering mechanisms in place, all a spammer can hope for is more effective evasion

[5]A validated lead is one that is confirmed through the person who's information was sold to begin with *(The loan application candidate)* goes through.

methods. The leads collected through this method are, on average, valued between eight and twelve US dollars per lead only because they are exclusive opt-ins[6] (i.e. no one else should have this information as they obtained it directly from the client). There have been instances when leads are scarse however, and opt-ins sold for over twenty US dollars a lead. Semi-exclusive (or non-exclusive) leads on the other hand are usually half or less than the price of an exclusive lead.

The second method of collection is not as trivial as the first one sounds, although the first is a bit more involved than I actually described. I will elaborate further on what it takes to successfully build the infrastructure described above shortly.

0.5.2 Thievery

Thievery obviously refers to stealing, and to steal, the collector has to choose from an abundance of targets. Essentially, anyone constructing an environment to collect leads themselves is a possible target. Things fall into place fairly easily for a collector wanting to find more targets – recall how collectors use mailers as resources to advertise their websites? This is a pretty viable method for collection however, alternative methods do exist and collectors use any and all possible enumeration methods they can think of. First, lets dive into the details of what collectors looking to construct websites need to do before hiring mailers since this is directly related to the enumeration of targets.

0.5.3 Setting up an Infrastructure

So far all this seems pretty straight forward; they setup a webserver to collect information about the people interested in mortgage loans and the mailers responsible for advertising get a sales commission for leads collected by their spam[7] run. To complete the cycle, the people interested in loans receive an email which sparks their interest and they navigate to the link found in the email. Collectors are usually ambitious and make an eager attempt at

[6] An opt-in is a user who wishes to recieve information regarding the service or product you provide.

[7] Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.[Inside]

keeping their domains, websites, and mailers going round the clock. In the United States it is illegal to spam a person without their consent, and to use spam as advertisement to a website (the loan forms) hosted on a webserver in the US is not too common but they do exist. The easiest thing for a collector to do is to find a hosting provider in a communist country with no regard for the content placed on their servers. The technical term for this type of service is bullet-proof-hosting[8]. The average price for such a service is about `2,500` US dollars a month. An alternative to dishing out large amounts of cash for hosting services is using a bot network[9]. Usually though, bot networks are pretty dynamic and don't fit the necessary requirements to host this type of content. If a collector pays a mailer to spam his site for two or three days and the host goes down the first night (because of an unreliable bot host) a lot is lost and so generally experienced folks tend to pay for reliable hosting.

Often, the businesses providing the bullet-proof-hosting servers are relatively well known, and if they are known so is their allotted IP space. This, in turn, makes finding servers hosting mortgage applications a piece of cake. All one has to do is scan a known IP segment for specific criteria and keep track of those that fit the profile. Once a worthy target list has been collected, the attacks follow. An interesting fact about the individuals involvement in this industry is that nothing either one is doing is really all that legal. This, in fact, allows an attacker to launch whatever type of attack he wants on the victim machine with little to no worry about legal repercussions. Often a collection machine will have several required services open to the Internet, for example: http, ssh, ftp, mysql or mssql and sometimes an administrative web interface. The scope of an attack is unlimited and the number of man hours invested directly reflects on the amount of traffic the victim website attracts. It is even pretty common for certain prowlers to lease a server from the same segment the victim machine is on simply to increase their odds of breaching the host. The following shortly describes common attack practices launched against victim websites.

Brute-force Enumeration

An attacker will attempt to guess login and password pairs on any if not

[8] A bullet-proof-host is a node on a provider's network with extremly loose Terms of Service, often allowing them to spam or host any content they wish. Usually the provider resides in a third world or communist country.

[9] A distributed collection of agents (bots) connected and controlled by a central authority.

all of these services. Usually this kind of attack is not too stealthy, but remember there is little worry - I mean the victim cannot simply pick up the phone and call his lawyer can he?

SQL Injection

If any of the web interfaces are accessible through the site, sql injection attacks are another vector for entry. Although the success ratio of sql injection is now relatively low, there are still some low hanging fruit to find and be assured someone greedy and ambitious enough will find it.

Classic Attacks

With the massively large number of exploits developed and released to the public daily, searching and launching attacks is a frequent action. This sometimes opens up a new market for exploit writers looking to make some quick cash. Collectors can advertise the need for an exploit and place a price on a particular application. There are even online auctions that have been built specifically for this purpose.

Passive / Passive Aggressive

When an attacker decides to lease a machine on the same segment, it is usually because they failed to remotely compromise the victim's machine. As a last resort they can do several things to retrieve the information they are looking for. The attacker can launch an ARP Poisoning attack and sniff all the incoming traffic to the victim machines, an attacker can simply redirect all the client requests to himself and collect the leads himself, or even hope for the victim himself to logon and perform a man-in-the middle attack to passively collect credentials.

0.6 More on The Money

In this section, I will associate the roles described above with the amount of money they can generate. As described earlier, the mailer serves as the core distributor of an advertising campaign. As a company would pay a marketing company for it to advertise its products, a collector pays a mailer to generate leads (e.g advertise and generate revenue). He can also simply take matters into his or her own hands and do the dirty work himself. If a mailer is hired however, to properly track what a mailer collects there is a nifty procedure in place. Each mailer is given a unique ID number and the

link spammed in each email contains the ID number. When a client submits information regarding his loan inquiry, the mailer's ID number is included and the collector now has record of how many leads a mailer is generating.[10]

A single spam run can be as large as two million emails. The time needed to complete a run that big depends on a few key factors - the method used for distribution and the spam software being used. If a decent sized list of proxies is used you can send an average of about forty thousand emails per half hour using Dark Mailer [Inside]. With a little math we can compute that transmitting two million emails would take about twenty-five hours. More over, if I were to shoot low and say that .01 percent of two million emails from a single spam run actually worked, the return for the collector on exclusive leads is about 200 leads per mailer at `10` dollars a lead results to about `2,000` USD. The mailers recieve on average about 8 per referal and can usually track their statistics through a web-based front end tracking their return on time investment in real-time.

0.7 The Disaster

So far, I've covered in fairly good detail the structure of what was once a falling corporation taking a 180 degree turn and rising straight back up to the top. It is too well known though, that what goes up must come down and twice as fast as it went up.

The core of the problems started out when mailers began to falsify the content of the spam for their collectors. Mailers noticed that the lower the rate they advertised the more traffic they would drive to the collector's website. More traffic indicated a higher collection of leads which resulted in more money. Whether the mailers were aware of the laws before they did what they did is unknown to me but their lies resulted in law suites unfolding from all sides. Unhappy individuals who had been promised a `1.9% - 2.5%` interest rate on a loan began filing law suites against the collectors. This resulted in a fairly large chain of angry partners. The hierarchy below indicates the ripple of disaster that came about.

[10]This method of tracking referrals is well adopted in most spam/advertising related industries online. The majority of spyware and adware vendors leverage this method of tracking to pay their affiliates.

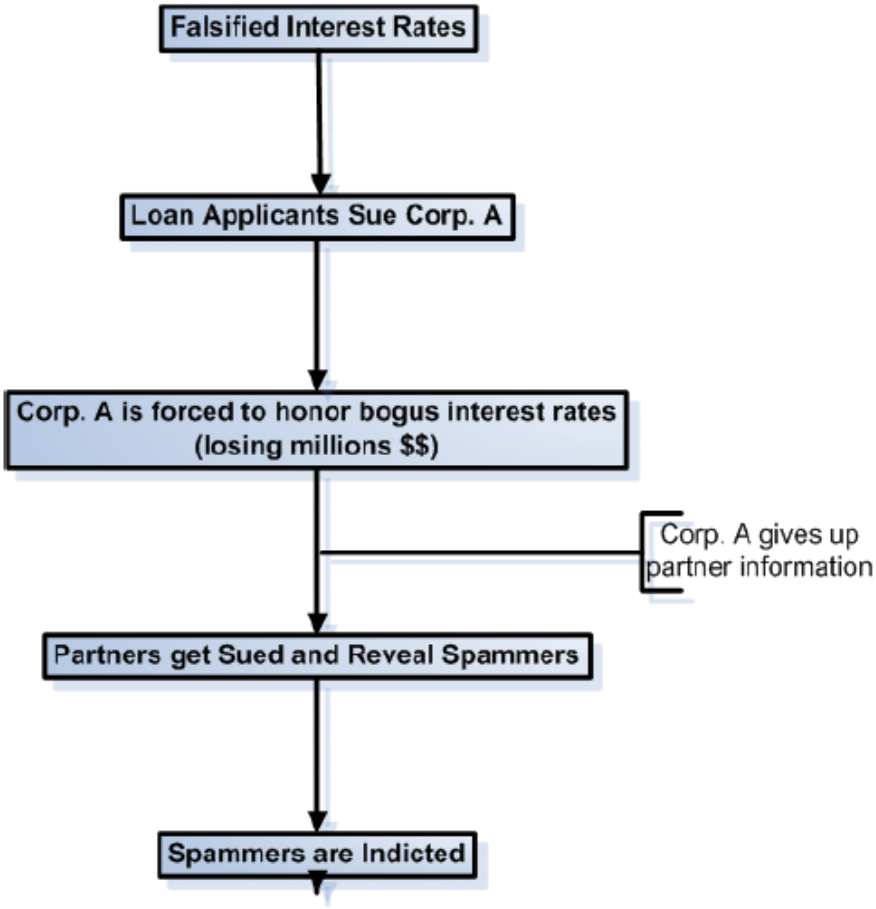

Figure 3: Ripple of Disaster

0.8 Conclusion

It is fair to say that ambition can get the best out of people Indeed, I'm sure these individuals are trying their best to make a profit out of this endeavor. Unfortunately, it is not the most appropriate way to make a living; it does however show that their perception is a bit different. Most of them feel that by staying away from selling drugs and pornography online, they are not hurting anyone and simply taking advantage of a good way to make some money. In retrospect, I agree, but I refuse to condone spam for any reason, it consumes countless corporate man hours and is a general nuisance to anyone who receives email.

Bibliography

[Inside] Spammer-X, "Inside the spam cartel." ⟨http://www.oreilly.com/catalog/1932266860/⟩.

[Boiler] Boiler Room, ⟨http://www.imdb.com/title/tt0181984/⟩.