VIRCOM
freedom of e-expression

Why Spammers Spam

A Foray Into the World of Spammers

www.vircom.com

Table of Contents

Vircom Inc., 460 St. Catherine St. West, Suite 600, Montreal, QC, Canada, H3B 1A7
Vircom Europe S.A., 16 Place de l'Université, B-1348 Louvain-la-Neuve, Belgium

For more information, visit our Website at http://www.vircom.com or contact us at:
Vircom Inc. : +1 (514) 845-1666 (EST)
Vircom Europe : +32 (10) 48.35.04 (CET)

Introduction

Spammers come from every walk of life, every country worldwide and every socio-economic condition.

A spammers work is one of contradiction; they work in a secretive environment, constantly straddling the fence between legal and illegal, moral and immoral. For this report, Vircom acquired the assistance of three active spammers, all of whom have varying degrees of experience and success as spammers.

Our goal for this paper was not to criticize or judge what these people do or how they conduct their business. Instead, we wanted to gain a unique window on the world of spamming; to shed the cloak of mystery regarding who spammers really are...

...and Why Spammers Spam.

How we created this report

In order to gain the participants' full co-operation, certain conditions were required:

1. Vircom was not to reveal the real nor the online names of the spammers who participated.
2. Vircom was not to specify the names of the product or services the spammers have marketed.
3. Vircom was not to reveal any personal details regarding the spammers without their agreement.
4. No response was to be altered by Vircom in any way.

How we met the spammers

Because they operate on the fringes of legality, it is difficult to contact and communicate with spammers. In general, the spamming community is not a close-knit group. Spammers prefer to work solo or in small groups known as 'spam gangs'.

For this study, Vircom took a direct approach and posted messages on a known spammer's website, asking for experienced persons to participate in a discussion about spamming. As a result of this request, we made contact with several people, including one of our participants, who introduced us to members of her spam gang. At no time did we, at Vircom, disguise our identity. The spammers we spoke with were all aware that Vircom is an email filtering solution provider.

Spammer terminology

Our spammers refer to their occupation in many different terms: *online marketers*, *bulk e-mail marketers*, *e-mail marketers*, *vertical marketers*, *crap peddlers*, *mail bombers*, *junk e-mailers* and *porn hawkers*. To prevent any confusion, we will refer to our participants as *spammers* and to the act sending unsolicited bulk commercial e-mails as *spamming*.

For more information, visit Vircom's website for a **Glossary of Spam Terminolgy**.

Visual codes

To facilitate readability, this document uses visual marks to help the reader track spammer comments and quotes from spam experts. The following is a legend of the marks used in this study:

Legend

Acknowledgements

Expert analysis

This analysis would not have been possible without the contributions of Michael D. Osterman.

Michael D. Osterman, *President and Founder*
Osterman Research Inc.
www.ostermanresearch.com

Spammers

Vircom would like to thank Virginia, Matt and Thomas for allowing us into their inner-circle and sharing some of their experiences. Their assistance in this study was invaluable.

Virginia

Virginia is a 22 year old university student from the northeastern United States and a a relative "rookie in the spam game". Virginia started spamming to earn extra money and to pay for her tuition and housing. Taking an analytical approach to her work, Virginia views her spamming in terms of "campaigns" and has created her unique artistic approach to spamming.

Matt

Matt is a 32 year old part-time spammer. He lives in California and has been spamming for a few years. He is contracted by several adult sites to find new customers, as well as cater its existing customer base with special offers and promotions.

Thomas

Thomas is the seasoned spamming veteran amongst our three participants. He is in his early 30's and has been spamming, part-time, for over 5 years. His years of experience have given him a unique view of the industry and its effects on business and consumers.

Starting up

How did you get involved in spamming?

"I was looking for a part-time job, something that would help me pay the bills and not occupy a lot of time. I was suffering from starving student syndrome big time… My friend mentioned doing this in passing to me, and the more I thought the more the job appealed to me. At first it seemed almost too good to be true, I had pretty much all of the hardware I needed all I had to do was invest in a new internet provider, and buy a list of e-mail addresses. I started up for pretty much nothing and turned a profit on the first day!"

Matt started spamming as a result of his affinity for hacking and computer security. Matt currently works in the computer industry in the Silicon-Valley, and uses his work experience to hone his spamming techniques.

"I have always been interested in the what's of computing, what makes the anti-spam filters work, and then how I can bypass them. After a while I realized that I could make a few dollars from this."

Thomas worked for a large multi-national corporation as a manager in IT for seven years before getting laid off in early 2002. As his own boss, spamming offered Thomas the freedom to pursue other goals while earning money. Currently he is only spamming part time, and has since taken on another full time job in the IT industry.

"I fell into it, because it was so cheap to start up, and I had plenty of time to spend with my kids."

All of our spammers agree that one of the main reasons they began spamming was because it had an extremely low start-up cost. Most spammers can get started for under $1,500.00 and may earn back their initial investment within a few days.

Making money

How do spammers make money?

Spammers can earn money by using a number of different methods:

- Sending spam to sell their product
- Harvesting e-mail addresses
- Joining affiliate programs

Sending Spam to sell their product: Some spammers earn money by selling their own products or services. The types of commodities can include pirated software or pornographic material. In general, a spammer looks for a product that is easy to distribute to their customers.

Harvesting e-mail addresses: Spammers build lists consisting of millions of names and sell them to other spammers. A spammer will pay a premium for lists that are categorized geographically and for authenticated "clean" lists (the e-mail addresses have been validated).

Affiliate Programs: This is the most common type of spamming activity. Under an affiliate program, spammers are hired by companies who pay them based upon either:

1. The amount of leads they bring to the site (click-through rate)
2. The sales generated from the spam (commission)

How much money do you make from your activities?

"It varies but I have made as little as $150 per campaign or as much as $2,000.00. It depends on the product, timing and my creativity."

For Virginia, a campaign consists of an e-mail burst of approximately 5-days. Virginia explains that the 5-day period allows her to distribute the mail at least once or twice to the 40 million recipients in her database. In addition she estimates that she has a 5-day window during which to trick certain spam filters before a fix is introduced and released into the stream.

"That is pretty tough to know, it varies wildly. I calculated that I earned around $1,200.00 per week last year. The most I earned in a week was $6,500.00, and the least was $1.00, so I have done the gambit.

What type of products or services do you sell?

Like the majority of spammers, all of our participants work strictly through affiliate programs. They are paid either directly by the company they are representing or through intermediaries.

"I have strict rules regarding the types of products that I market. I will not market porn or stuff like that. I have been very successful with the low-carb diet plans. It is after Christmas and everyone wants to lose weight. I started this campaign the week another report made the rounds saying that obesity was a bigger killer than tobacco.

My current campaign involves discount travel. So far it has been quite successful because of all the students going on spring break and people suffering from winter doldrums."

"I have an exclusive contract with several adult sites, they have me advertise specials or other offers to its current list of subscribers and also to promote these sites to others."

Matt works for an affiliate that manages 12 different adult sites. Part of Matt's work is to promote all of the different sites to registered subscribers as well as any other person contained within his database of e-mail users. Matt is paid a commission for new subscribers and spends the majority of his time trying to solicit new customers to his affiliate.

"I have peddled everything from diet pills to porn. I usually get the biggest response from porn… skin sells, unfortunately."

How do you obtain your contracts?

"I work with a close knit group, who look out for each others' interests. All of my campaigns were a direct result of contracts that I got from the group."

"I get most of my contracts through word-of-mouth. I don't work in an industry where you can really advertise yourself. Between friends and satisfied customers, I am almost always assured a contract."

Organization

Is the spammer community a close-knit group?

Virginia and Thomas are part of a loosely formed, 4-member *spam gang*. They share lists, leads, and information regarding affiliates and opportunities. Because Matt is under contract with a group of adult sites, he presently does not belong to a *spam gang*, even though he has worked with Thomas in the past.

"I have met some very smart and talented people who are (spammers). I work a lot with (Thomas) and he has showed me a great deal."

"Not really, it is not like seeing people at the water fountain during smoking breaks. You communicate through e-mails or chat online. I have never personally met a fellow spammer, nor talked to any on the phone."

"Close-knit is not the best way to describe the spammer community. I am pretty aware of all the major players but I can't say that I am close to any. You work in groups because it is a necessity but when it comes down to it, it is every one for themselves."

What are hot topics for you now?

Timing of the spam message is crucial to the success of the spammer's campaign. Affiliates hire spammers at particular times of year to market their product or service knowing that the timing of the spam will ensure higher sales. For example, New Years will see significant increases in spam dedicated towards diet aids, as well as low interest loans to pay off the bills from the holiday season.

"Without a doubt Paris Hilton and Janet Jackson. Sex sells and, as long as you give the consumer a window to peak into the seedier side of celebrities' life, it will continue to sell. Before you would have to go to the video store and sneak behind the curtain to look at the adult films, now it is just a click away."

"Tax software, it is the time of year when people are looking to do their taxes."

Harvesting

How spammers get e-mail addresses

For spammers, the most important work tool is their database of e-mail addresses because these lists are not only used for spamming purposes but sold or exchanged for other lists. Spammers have several weapons in their arsenal to acquire e-mail addresses:

Harvesting software (also known as spiders, bots, robots and crawlers): Spammers and harvesters use these tools to search the internet for e-mail addresses for the purpose of spamming, selling, or swapping. Within a very short period of time, a good e-mail harvester can harvest millions of addresses.

As e-mail harvesters search the internet they look for the @ symbol, an essential part of all email addresses. E-mail harvesters can find addresses from a variety of sources on the internet including:

- Web pages
- Newsgroups and forums
- Compromised mailing lists
- Chat rooms and IRC
- Unsecured opt-in lists
- Corporate web pages
- Web-based surveys
- Web-based order forms

Mailing / Opt-in Lists: Whenever consumers subscribe to a mailing or opt-in list, they run the risk of having their e-mail address compromised by spammers. In certain cases, some legitimate and highly respected companies sell their subscriber lists to other companies, who, in turn, sell them to others.

Opt-out methods: Many spammers will use op-out methods to gather and verify e-mail address list. When consumers respond to unsolicited e-mails by clicking on attached links or replying to opt-out, in many circumstances, they are simply confirming that their e-mail address is valid and accurate for the spammer.

Viruses, Spyware, Malicious Code: Recently, viruses and spyware have beeny by spammers to extract the contents of a computer's address book. Viruses have also been written (Trojans) for the purpose of turning infected systems into relay slaves so that they become platforms to distribute spam.

Dictionary / Phone Book Attacks: A common harvesting tactic that involves automatically requesting likely e-mail addresses to a server by combining letters and numbers in an attempt to find, or validate, active e-mail addresses (e.g. johnsmith@domain.com, john.smith@domain.com, john_smith@domain.com and jsmith@domain.com). Spammers are using this technique less frequently because it results in very poor lists.

Social Engineering: has emerged as an effective tool to validate and harvest e-mail addresses. A spammer sends out millions of e-mails in an attempt to motivate the recipient to respond. The tricks and hoaxes the spammers use vary from the recipient winning a contest to being told that he/she is being charged for an item that was never purchased. No matter what the method is, the goal is the same - to get the recipient to reply and, therefore, validate his/her address.

How do you acquire your e-mail lists?

"I bought my first list from the friend who introduced me to spamming for $100.00; this was a pretty good deal because it had over 15 million names on it. I used this list to swap for more lists, now I have over 40 million names in my database."

"I bought my first list over the net and it was a pretty pathetic one that had made its rounds over and over again, I doubt more than 10% of the addresses were valid. Since then I have used a crawler in the past, but I found it was too much work and I did not like the results I was getting."

Currently, Matt obtains most of his addresses from the affiliates for which he works. These lists have become cash cows because, once he completes his work for the affliates, he uses them for other contracts and sells them to spammers for a profit. The affiliates acquire the lists through registered users.

"Your lists are your livelihood. My lists are even more valuable than most because I have ones that people subscribe to, therefore they are valid and I can cater my messages to their needs."

"I have bought lists in the past, but mainly I trade for them now. The most I ever paid for a list was $899.00. This was a list of 4 million clean (valid) e-mail addresses in Washington, Oregon, California and Nevada. The first time I used this list, I generated over $2,500.00 in commissions".

What is the most time-consuming aspect?

Once a spammer has a list of e-mail addresses, he/she must conceptualize, create and distribute a message that will not only attract the recipient's attention and possibly generate a sale but bypass spam filters that are implemented to eliminate the spam.

"I try to be as creative as possible with the look and the feel of my work. I would love if I could create messages that would read like a print advertisement, but I know better; either it would be too large or a spam filter would catch it."

"Maintaining a database, making sure all of my e-mail addresses are up to date occupies a great deal of time."

"I spend more time on the subject line than on the body of the message. The subject line is what will draw in the customer initially. Testing the message to have it get past spam filters takes a lot of patience because if you cannot get past the spam filter, then you need to figure out why it did not get through."

Spam tricks

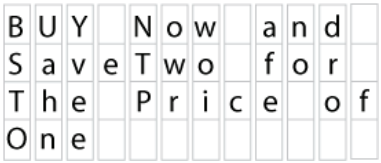
What are some of the techniques that you use?

Our participants were hesitant to reveal the majority of the tricks they use. However, they did talk about some of the techniques that they have used or with which they are familiar.

Technique: Top-to-bottom HTML Coding

"When I create new campaigns, there are 2 crucial factors that I all look at; the flow of the message and will it get past a spam filter. The message itself has to attract the reader and compel them to buy but it must be put in a format that will arrive to its intended receiver. I like using HTML. It is more attractive than just plain text and you can code the tables in such a way as to make them impervious to spam filters. For example coding from top-to-bottom."

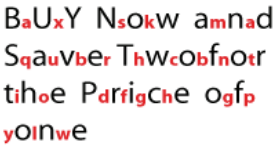
"Using this table involves coding words as individual letters, coded in HTML from top-to-bottom (B S t o) but read from left to right by the recipient. This technique is very difficult for some pam filters to detect because they do not identify individual words like "buy" or "Save". All they read is gibberish."



Virginia also discussed several other techniques that she has come across or used.

Technique: Zero font size

Spammers use the technique of placing 0-font-size letters as spacers between the actual letters of the words. The message is legible to the human eye but most spam filters have difficulty interpreting the content.



NOTE. The zero font size has been illustrated in red here but would normally be invisible to the reader.

Technique: HTML numbers instead of letters

This technique allows the spammer to disguise the message within a series of ASCII codes.

B= &#66 U= &#85 Y= &#89

Technique: Embedded Image

"I have created HTML messages consisting of just an image"

Because the text message is embedded within the image, this technique attempts to trick spam filters by eliminating text as a method for detecting spam.

"I have several great techniques that I am not going to tell you about, but I can say that I can get by any spam filter."

Technique: Added spaces or characters

*This is a simple technique that spammers use to trick spam filters by disguising words. A spammer places a space or character (e.g. - or *) between key words. For example, B U Y or B-U-Y or B*U*Y. Most spam filters will search the body and header of a message looking for certain keywords or phrases.*

Technique: Misspelling

Like placing spaces and adding characters between letters in words, the goal behind this technique is the same; fool the spam filter by making it difficult to distinguish words or phrases.

Spammers frequently replace the letter 'l' with the number '1' , the letter 'O' with a '0' (zero) or add foreign language accents to the letters. This method is easy accomplish but is not very effective.

ßÜY NØw and
$avë Two ƒ or
the Þ r1cê of
won

Technique: Hashing

This is a very common technique used by many spammers to attempt to trick spam filters:

A legitimate message is created with the same color (or very similar) for the text and the background (e.g. white on white, black on black). A short spam message is added in a contrasting text color (black text on a white background or white text on a black background). The result is that the recipient only sees the spam message. Example:

It is absolutely impossible to embrace the extent of difference there is between traditional and modern China when you first get out of the airport and ride towards the city. How can I explain this? You're looking through the cab's window, searching for something your eyes can focus on.

Buy Now and
Save Two for
the price of
one

But as you get closer to the center of the city, you start to notice difference after difference, so fast in fact that, before you know it; you're downtown, feeling like you are riding a flying cab in Blade Runner. Speeding along a neon-lit highway between skyscrapers with multiple-story, rainbow-colored advertisements, you ask yourself where the hell can the pagodas, zen garden and tai-chi adepts have gone.

How do you ensure that your messages get through?

"I test on the spam filter in my father's office, if I can get through it, then I can get through most spam filters."

"I use two spam filters, one is open source that I downloaded for free, and the other is an enterprise copy of a commercial filter."

For a spammer, the click-through rate is usually very low, so volume counts. To maximize the amount of messages that get through to their prospective customers, most spammers test on one or more spam filters.

Note that, if a spam message can circumvent one spam filter, this does not mean that it can get through all spam filters. Each spam filter has different capabilities. Some spam filters can only catch 50% or 60% of the spam, while some of the better spam filters catch more than 95% of spam. Vircom's modus solutions are the among the highest at 98.2%.

What do you think of spam filters?

"Spam filters give you a sense of false self-confidence. They can work very well, but when they catch important documents that you need, then they can do a lot of damage."

"There is no doubt that they have made our job more difficult, but I have never come across a spam filter that I could not get around if I tried."

How do you remain undetected by ISPs?

In order to distribute copious amounts of e-mails and remain undetected by Internet Service Providers (ISPs), many spammers use different techniques including sending spam through different ISPs or by hijacking third-party unprotected servers and using them as platforms to spam.

Our participants were reluctant to discuss their methods that they use to distribute spam. Most methods are illegal and none of our participants wanted to incriminate themselves by admitting to any illegal activities.

"I send out short bursts on numerous machines to stay under the ISP wire".

Virginia has used a technique whereby she sends out bursts of 100 messages every 20 seconds from approximately 6 different computers using different ISPs. In a 12-hour time span, she averages over 1.3 million messages.

About Vircom

Montreal-based Vircom is a leading developer of cutting-edge Internet infrastructure and secure messaging solutions for the demanding needs of Internet Service Providers (ISPs) and corporate clients. Vircom's mature modus™ secure email management technology incorporates over 10 years of industry expertise, making it a powerful driving force in the defense against spam and email-borne fraud.

Its award-winning products include email gateway software, a standalone email-gateway appliance and a complete email assurance mail server – all based on its core competence: delivering email assurance technology that protects email assets.

Vircom's state-of-the-art technology manages inbound and outbound email traffic and offers protection from spam, fraud, phishing, viruses, spyware, out-of-policy communications and other email threats. Its flexible design provides the email assurance capabilities necessary to meet today's threats and the essential flexibility and scalability to meet tomorrow's.

Labeled the Best Microsoft® Windows®-based email filtering solution by Network Computing Magazine, modus™ has gained important recognition, among which are a CATA*Alliance* Innovation & Leadership Award and a record-breaking five-award distinction including "Best Software Product" and "Most Innovative Product" from Windows® IT Pro magazine.