SPAM- A Mail to Kill

- Preface 2
- What is Spam 2
- Genesis of "SPAM" 2
- Cost of Spam 3
  - Burden on Shared Resources 3
  - Burden on Private Resources 3
  - Staggering Number of Victims 5
  - Unwanted Legal Liability 5
  - Assault of Family-and-Friends 5
  - Spam as Scams 6
- Seamless Solution 6
- Summary 7
- About Cyberoam 7

"An inefficient business (one that cannot bear the cost of its own activities) is dangerous to the economy, because to function, it must spread the cost of its activities across a large number of victims." - Ronald Coace, Nobel Laureate (Economics)

"Spam is the same thing lots and lots of times." - Henry Neeman

Any business that needs to send Spam emails to survive is not a viable business.

Preface

Spam is a Big problem because it is symptomatic of inefficient, parasitical businesses. The Nobel Prize winning economist Ronald Coace in what is now known as the Coace Theorem postulated that an inefficient business (one that cannot bear the cost of its own activities) is dangerous to the economy, because to function, it must spread the cost of its activities across a large number of victims. We will here discuss the impact of Spam. We will also briefly look at the ways to mitigate it. threat gains importance over the actual intrusion.

What is Spam

The term Spam refers to unsolicited, unwanted, inappropriate bulk email, Usenet postings and MUD/IRC monologs. For the purposes of this discussion, we will use the term Spam primarily in reference to email, which is what it is generally understood to mean when used in connection with the Internet. Spam is often referred to as Unsolicited Bulk Mail (UBM), Excessive Multi-Posting (EMP), Unsolicited Commercial email (UCE), spam mail, bulk email or just junk mail.

To draw a line between Spam and legitimate email or spam free bulk email is not as obvious as it may seem. To some, any and all email that does not come from an approved source is Spam. According to Mail Abuse Prevention System (MAPS) www.mailabuse.org, spam has a certain number of characteristics.

An electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

This definition of Spam goes on to say that whether the email is relevant, or whether the benefit to the sender is disproportionate is up to the recipient and not open to discussion. If this is the case, then Spam isn't Spam until the recipient decides it is. However, point (2) above really only makes sense when interpreted in the context of bulk email sent to subscribers. As often as not, the first email you ever send to someone has not been "authorized" since you have never exchanged emails before.

The generally accepted principle for Spam to really be Spam, it has to be bulk email. This definition is reinforced by Henry Neeman's "Why Spam is Bad" where he explains to a particularly dense group of spammers, entirely in single syllable words that "Spam is the same thing lots and lots of times."

Genesis of "SPAM"

The prevailing theory is that the term refers to a classic skit by Monty Python's Flying Circus. In the skit a couple in a restaurant tries in vain to order something that does not have SPAM in it. As the waitress lists endless dishes, all of them containing increasing amounts of SPAM, a group of Vikings in the corner begin to sing "spam, spam, spam, spam…" until all useful information is drowned out. But where did the connection between unwanted SPAM and unwanted Spam come from?

It did not start with email. The term has it roots, in relation to the Internet, in the late 1980s or early 1990s in Multi-User Dungeons (MUD) and Multi-User Shared Hallucinations (MUSH). MUDs and MUSHes are online, real-time, interactive, text-based virtual environments. According to one source, a MUSH user programmed a macro key to type "spam spam spam…" in a MUSH until his connection was terminated by a Sysem Administrator. He was subsequently referred to as "the !*%@ who spammed us" by other members. From MUDs and MUSHes the term Spam began to be used to describe Excessive Multi-Posting (EMP) on Usenet groups.

The very first Spam email was sent on 1 May 1978 by a Digital Equipment Corp. sales rep advertising a computer equipment demonstration. An attempt was made to send this email to all of the Arpanet users on the west coast of the US. Remember that Arpanet was a military project and commercial use was not acceptable. At the time, there was no such thing as an email Spam filter to stop Spam mail because there was no Spam.

In April 1994, the Phoenix law firm, Canter and Siegel, advertised their services by posting a message to several thousand newsgroups. This was probably the first automated large scale commercial use of Spam, and was the incident that popularized the term, which up until then had been exclusively part of the arcane vocabulary of Multi-User Dungeons.

Spam is going to increase 35% per year and by 2007 it will be 99% of all email.
- NetworkWorld

Some very large email servers have been shut down due to Spam overload for extended periods.

Spam is the electronic equivalent of junk mail. People send Spam in order to sell products and services or to promote an email scam. Some Spam is purely ideological, sent by purveyors of thought. The bulk of Spam is intended, however, to draw traffic to web sites or to sell sex and money making schemes.

Unlike junk mail in your physical mailbox, Spam does not abate if it is unsuccessful. When marketing departments send junk mail at considerable expense, without success, they generally cease, or try a different sales pitch. Spam on the other hand can be entirely unsuccessful, but the large number of wannabe spammers waiting in the wings ensures that we will continue to receive lots of it.

The Coace Theorem of inefficient business cuts close to home where Spam is concerned. Any business that needs to send Spam emails to survive is not a viable business. The benefit to the spammer is disproportionate to the cost borne by the spammer, which is next to nil. More importantly, the cost of Spam removal to the victims is totally disproportionate to the benefit to the spammer. In a free market economy such a grossly inefficient process should cease when property rights are enforced (i.e. the cost is borne by the party who incurs them).

Cost of Spam

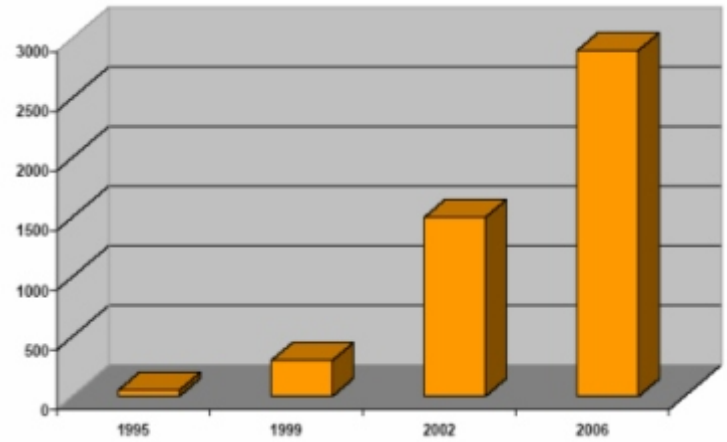
In a free market economy a grossly inefficient process Spam, should cease when property rights are enforced (i.e. the cost is borne by the party who incurs them). However, Spam is a big problem because property rights are difficult or impossible to enforce which makes it hard to get rid of Spam. From the 1800s through the mid 1960s industrials considered it their right to produce and pollute with impunity. It took over two decades of lobbying to move government and industry to another point of view. Yet these were reasonable businesses, with physical assets in the countries of their victims and subject to their legal systems. Consider the spammers in contrast. Any physical assets they may have are irrelevant to their activity, which incidentally, has no borders. They are not subject to the legal systems of their victims. If they become subject to legislation attempting to stop Spam they can find a more favorable environment in another country.

Burden on Shared Resources

Spam is a big problem because of the shared resources it consumes. Internet Service Providers (ISPs) allow you to surf the Internet, and deliver your email to your email software usually for a flat monthly fee. They must, in turn, purchase bandwidth and additional servers to manage email. Spam however, increases their need for bandwidth, and increases the load on their email servers with no added revenue to compensate. The added cost must be passed on to the customers, the victims of spammers trespassing on their private cyber-property. Some very large email servers have been shut down due to Spam overload for extended periods. One leading ISP processes about 30 million email messages a day, 30% of which are Spam.

The problem of Spam has reached proportions where it threatens the viability of email and of the Internet itself. According to research firm IDC, by 2006 the number of e-mails exchanged every day will exceed 36 billion worldwide. Estimates for the percentage of e-mail messages that can be classified as spam are approximately 40%.

Forecast Spam Messages Sent(Billions)



The volume of spam is set to double by 2006

A company with 500 knowledge workers earning an average of $60,000 per year each spending almost five seconds per mail, deleting Spam would experience an added burden of $107,708.33 per year.

Email is a business tool. Anything sent from a corporate email address is effectively written on company's letterhead electronically, making the company accountable for it.

A company with 10,000 employees loses more than $13 million worth of productivity each year because of spam internally generated and distributed. - Gartner

Burden on Private Resources

According to NetworkWorld, Spam is going to increase 35% per year and by 2007 it will be 99% of all email. The biggest expense by many times (in some cases an order of magnitude) is lost productivity.

Spam is a big problem because of the private resources it consumes. Many business people spend up to fifteen minutes per day reading and deleting their Spam emails.

A company with 500 knowledge workers earning an average of $60,000 per year each spending almost five seconds per mail, deleting Spam would experience an added burden of $107,708.33 per year.

This cost would be passed on to Internet users and non-users alike as they purchase products from this company at their local department store.

Company	
Number of employees with email	500
Average annual salary	$60,000
Average spam per day per employee	25
Seconds to identify and delete each spam	4.4
Cost	
Total salary lost daily	$458.33
Total salary lost monthly	$8,975.69
Total salary lost annually	$107,708.33
Productivity	
Total time lost daily	15.28 hours
Total time lost monthly	37.40 work days
Total time lost annually	448 work days

*Based on 220 day work year

Staggering Number of Victims

Spam is a big problem because of number of victims it involves. In May 2002, the Korea Times reported that unsolicited e-mail costs Korean Internet users and ISPs $2.25 billion a year. In just one day, nearly 900 million spam e-mails were sent to Korean e-mail subscribers, while the number of spam e-mail circulating in that country now exceeds 340 billion messages annually. That's around 21 spam e-mails every single day for every man, woman, and child in Korea.

IT resource consumption costs include not only network bandwidth and disk storage, but also the cost of dealing with spam related inquiries. If spam in your organization represents 40% of all incoming messages, that translates to 40% more processing and storage capacity that your email system will be required to sustain.

Unwanted Legal Liability

Spam is a big problem because it is an unwanted legal liability when it contains sexual or otherwise questionable content. This type of email is easily forwarded to people inside and outside the organization. Email is a business tool. Anything sent from a corporate email address is effectively written on electronic company letterhead.

As a result, any views, quotes, or discussions made via company email can be representative of the company and legally binding. In a survey by Strategic Surveys International of Fortune 500 companies, Chevron Corporation and Morgan Stanley Dean Witter have both settled multimillion-dollar sexual harassment lawsuits as a result of internally circulated emails that contained offensive content.

To make matters worse, if an employee forwards a joke or personal "friends and family" junk e-mail, they put their employer at risk if someone who receives it outside of the company is offended by its content. This is the new face of Spam.

If spam in your organization represents 40% of all incoming messages, that translates to 40% more processing and storage capacity that your email system will be required to sustain.

Assault of Family-and-Friends

A new form of spam is taking its toll on networks. Described by research firm Gartner as "friendly fire," the amount of e-mail sent to employees by their family and friends is on the increase. As users become more familiar and comfortable with creating and sending graphic images, these emails are increasingly made up of bandwidth-hogging files including MPEGs, gifs, BMPs and mp3s.

As a result, many workplaces are inundated with unnecessary personal e-mails with large attachments. These include family photos, home videos, cartoons, jokes, electronic greetings and a host of other electronic files. Although the senders mean well, the employer's networks and servers pay the price. Not to mention any loss in productivity as employees view and forward these files.

According to a survey conducted by Market Facts' e.Nation, every single week employees receive up to 30 chain letters, jokes, video clips or similar junk e-mail messages from someone they know. This means many American workers have to deal with more than 1,500 pieces of junk e-mail each year from friends, family and colleagues. This also means that traditional spam, the much-reviled commercial e-mail sent by strangers, won't even reach the proportion of "friendly" junk e-mail until 2006. According to Gartner, a company with 10,000 employees loses more than $13 million worth of productivity each year because of spam internally generated and distributed.

The only safest way to deal with all "lucrative" offers Spam, is to deny them an entry into your network.

Spam as Scams

Recognizing that most spam today promotes some form of scam, the Federal Trade Commission

(FTC) has taken an active role in protecting businesses and consumers from the dangers of Spam.

The Commission noticed that much of this spam was a scam frauds, cons, and schemes designed to lure the recipient into a scam. That growth was one of the reasons that prompted the FTC to regularly issue its Dirty Dozen a list of the top 12 spam scams. These scams include almost every conceivable type of fraud including business opportunities, bulk e-mail, chain letters, work-at-home schemes, health and diet scams and investment opportunities. The only safest way to deal with all these "lucrative" offers is to deny them an entry into your network.

An ideal Anti-spam solution should have the least amount of false positives and a high detection rate.

Seamless Solution

Whether you deploy a separate Anti-spam box or a United Threat Management (UTM) solution, at the end of the day, you should get a safe, spam free environment.

You should look for a gateway level solution that allows user-based policy configuration. A user-based Anti-spam solution will provide a system administrator fine granular control over specific scanning and blocking policies for individuals or a group of users. Spam for one person maybe a completely legitimate mail for other.

No solution is foolproof and the Anti-spam technology is still maturing. So the solution should provide a quarantine facility for doubtful mails. The most important criterion of an ideal Anti-spam solution is that it should have the least amount of false positives. If the number of false positives (legitimate mails are mistaken and dealt with as Spam) is high, it will lead to two serious things. First, legitimate mail containing some valuable data might be lost and might to serious business loss. Second, high amount of false positives will force the system administrator to loosen the filtering policies, which will be a self-defeating gesture. Quarantine provides a safety valve, in case of false positives. This will encourage the system administrator to safely tailor fine user-based policies.

The most successful approach is not to rely on just one method of Spam detection, rather combining different methods to achieve the means. Let us have a brief look at them.

Spam filtering may be based either on formal methods or on content analysis and filtering based on artificial intelligence. A formal approach uses lists of known spammer email and IP addresses along with lists of open mail relays used by spammers and formal rules treating message headers.

Lack of proper configuration and control of a Gateway AV mars its performance.

Lists are used to reject letters sent from known open relays or from Internet access providers known as tolerant to spammers. Formal rules are used to recognize messages with typical indicators suggesting spam (such as: no recipient, or too many recipients, sender unknown, etc.)

Content analysis and filtering uses Artificial intelligence (AI) which deals with message contents (text) i.e. message body and subject. To recognize suspicious content, word statistics and collocations, message content fingerprints and other methods are employed. In a nutshell:

1) **Formal** (rule-driven) methods:
   I. **Rules:** Set of formal rules based on the analysis of message headers, size, sender etc
   II.**Real-time Blacklists:** Usage of so-called blacklists that are based on checking message sender IP and e-mail addresses against several conventional real-time blacklists located on the Net.

2) **Content Analysis** (AI) methods:
   I.**Heuristics:** Linguistic heuristics, based on special term databases and "fuzzy" mathematics.
   II.**Signatures:** Linguistic fingerprints of known spam messages employing a "fuzzy" comparison algorithm.

Summary

Spam is a Big problem. It has to be dealt with for the survival of Internet and Email. It has to be dealt with to provide a safe environment in enterprises, universities, governments. Spam should be dealt with so that when a seven year old kid checks his mail account, he does not encounter a pornography spam, waiting to spring on his innocence.

About Cyberoam

Cyberoam Unified Threat Management appliance recently announced the introduction of an advanced version of Intrusion Detection and Prevention solution. Cyberoam's Single Sign-On pinpoints the source of internal threats by the username. This ensures highest levels of security even in Wi-Fi and DHCP environments with dynamic IP allocation. Cyberoam UTM, with its multi-policy capability, allows administrators to configure different user based policies.