SPAM and its impact

[1]Rajesh Pokhriyal, [2]Vikas Kumar Jain, [3]Rajesh Patil, [4]Rajveer Singh Rajawat, [3]Jatin Nagpal
[1]Manager, [2] Sr. Manager, [3]Manager, [4] Dy. Manager, [5] Dy.Manager
[1]Data Center,
[1]Railtel Corporation, Gurugram, India

Abstract: In the age of web-based email and effective spam filters, it's easy to forget the sheer volume of unsolicited mails that are circulated around the web. There are hundreds of billions of spam messages sent out across the web daily, representing more than 97% of all email sent. All that spam takes a lot of computer power and consumes internet bandwidth to get to the inbox. SPAM increases the carbon footprint and the consumes ample amount of people's precious time in reading the spam mail, filtering them out. Hence impacting the productivity and profit of enterprises. Many techniques are used in combination to block the number of spam.

IndexTerms **– SPAM, carbon footprint, Greenhouse gas, ISP, Spammers, botnet, spoofing**

1. INTRODUCTION

Email provides us with a way to reach out to our near and dear once instantaneously. This innovation has changed the way people communicate. But technology comes with its disadvantages and unforeseen drawbacks – spam being a major. Spam is unwanted email sent out in bulk to an non-selective recipient list. Typically, spam is sent for commercial purposes or with malintent. It can be sent in massive volume by botnets, networks of infected computers called spammers. Spam emails cause everybody vexation from time to time. There isn't much that's more annoying than unwanted emails trying to sell you products you don't want and requests to transfer money to your bank account when all you want to know is whether your friends and family have been in touch.

Various report has revealed that it's not just people's time that is being wasted by the millions of spam emails landing in people's inboxes every day; Spam email has a considerable carbon footprint.

2. IMPACT OF SPAM

2.1 SPAM CONTRIBUTES TO A LOSS OF PRODUCTIVITY AND PROFIT.

In traditional business cost of printing and postage when sending out commercial mails to their target audiences is incurred by senders not the receivers of these communications. This direct-mail concept works in reverse when it comes to spam. It costs virtually nothing for spammers to send out large bulk mailings to tens of thousands of unwilling recipients. Shockingly enough, only 1 in 25,000 spam recipients need to buy a product or service through spam advertising for it to be profitable. These kinds of numbers would never work in direct-mail traditional advertising scenarios.

As per reports spam accounts for an estimated 70% of global emails – which is approximately 14.5 billion emails per day Spam costs the global economy close to $20 billion every year in lost productivity while spammers as a whole make about $200 million per year. Spam email is equal to a genuine waste of employees' time. On an average, employees take about 16 seconds to go through and delete each spam email If the business doesn't have a spam-filtering service, then up to 70% of an employee's incoming emails per day could be spam messages. So, 70 % of (x) incoming emails times 16 seconds times the number of employees in your business would equal to X wasted man hours per day. Bottom line is that spam being a continuous process the time wasted per mail gradually adds up over days, weeks, months, years. Enterprises could insidiously thousands of dollars every year because of the inefficiency resulting from spam.

2.2 SPAM POSES LEGAL RISKS

Statistics show that sexually explicit, pornographic content is on the rise with spam tactics; in fact, pornographic spam has doubled in the recent years and is now the fastest-growing category of unsolicited mail. Two things could happen if your employees receive pornographic spam at work:

- Enterprises can land in legal suits if incredibly offended, employees file complaints of sexual harassment and a hostile work environment -- even if your business is not the source of this spam. If your business is alerted about the pornographic spam and doesn't take action to block it, employees will have grounds for legal action against the business. The headaches and stress, not to mention the fines, fees, and damage settlements, that result from losing a lawsuit like this could be a serious professional setback.

- Pornographic spam presents an opportunity for an employee to open the email message and absorb the explicit images and content contained therein during valuable work hours. Overall production and well-being of the company is hampered when malicious content is received as spam.

2.3 SPAM CONTAINS VARIOUS MALWARE THREATS

In our current digital age, spam is no longer just annoying but harmless to computer, computer network(s), or servers(s). A large number of spam messages purport to come from legitimate enterprises, financial institutions, legal authorities, or personal friends and family. Typically written with bad grammar and spelling, these messages encourage you to click on a link or download a file, through which malicious software can find its way onto your computer.

Malicious spam also uses threats to get you to click on a link or email attachment. So, if someone comes across such an email that has characteristics, recognize it for what it is and simply delete it. At the very least, exercise extra caution before you go ahead and click on an email link or open an email attachment. Note: .exe files are notorious for carrying malware.

Spammers utilize malware primarily for stealing sensitive information, e.g. social security numbers, credit card numbers, passwords, and other confidential data pertaining to your bank accounts. The reason here is fairly straightforward. These cyber thieves want to use these financial details to drain your bank accounts or commit credit card fraud under your name.

Topsec Email Security is a highly reliable anti-virus, anti-spam service that will ensure the security of your incoming and outgoing emails. This software consistently filters your inbound emails and blocks spam messages, especially those with malware threats and sexually explicit content.

2.4 ENVIRONMENTAL IMPACT

The McAfee's report of 2009 focused on the energy used by 11 countries including the UK, America, China, Japan, India, France and Germany, uncovered that the energy used to generate, send, store, check and delete spam messages equates over the course of a year to the amount of energy it requires to power 2.4 million US homes. That is the equivalent of 33 billion kWh of electricity. The resulting carbon emissions of using this amount of energy just to deal with spam emails are equal to 3.1 million cars being on the road. It's interesting to note that nearly 80% of the energy consumed by spam is used by people deleting it from their inbox and searching spam boxes for legit email. The world would also be a cleaner place if every email user was protected by spam filters, cutting the total amount of spam related emissions by 75%.

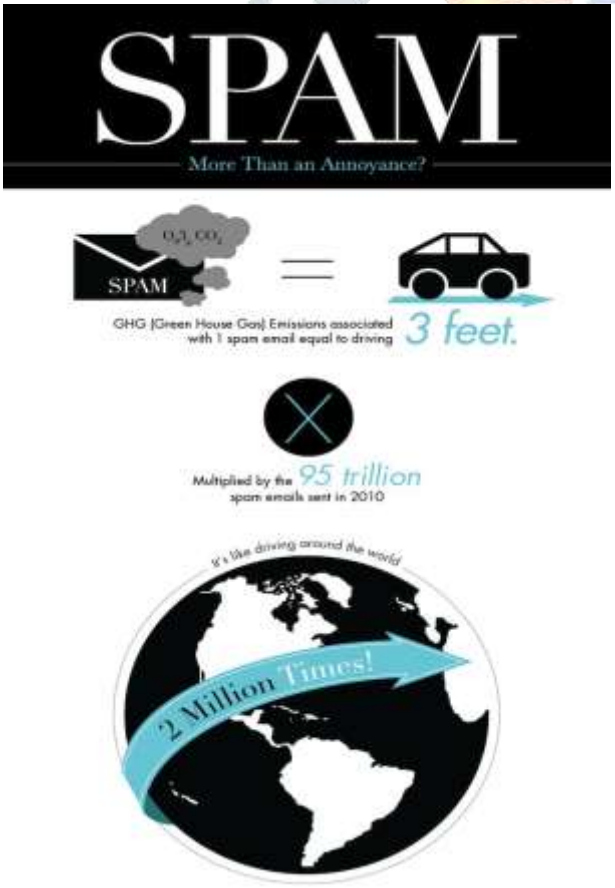

Fig.1 Spam data

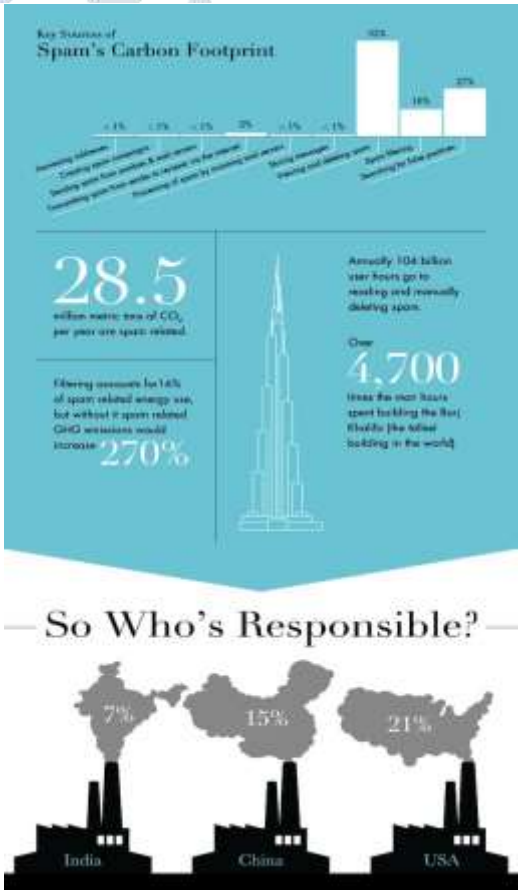

Fig.2 Spam carbon footprint

3. COMMON TYPES OF SPAM

3.1 Commercial advertisements

Whether an email message is spam or a legitimate is subject to the guidelines or laws of the country. When businesses capture your email address, they often subscribe you to their newsletter by default, as a low-cost way to sell their products. Whenever you fill out an online form, look for a checkbox to opt into or out of marketing email. While these emails can be pesky, most are harmless, and by law they must have a visible opt-out or unsubscribe option. If you unsubscribe and continue to receive spam, update your email settings to filter messages from the sender's address out of your inbox.

3.2 Antivirus warnings

Antivirus warnings are a common spam tactic used by spammers. These emails warn you about a computer virus infection and offer a solution--often an antivirus scan--to fix the alleged cyber threat. But taking the bait and clicking the link can grant the hacker access to your system or may download a malicious file.If you suspect that your computer is infected, do not click a random email link. Instead, pursue legitimate cybersecurity software solutions to protect your endpoints.

3.3 Email spoofing

Spoofing spam emails masterfully mimic legitimate corporate messages to get you to act. The spammer picks a company victims will trust, such as a bank or an employer, and uses the company's exact formatting and logos.

3.4 Sweepstakes winners

Spammers often send emails claiming that you have won a sweepstake, prize or a lottery. They urge you to respond quickly to collect your prize, and may ask you to click a link or submit some personal information. If you don't recognize the competition, or if the email address seems dubious, don't click any links or reply with any personal details.

3.5 Money scams

Unfortunately, spammers prey on people's goodwill. A common money scam begins with emails asking for help in dire circumstances. The spammer fabricates a story about needing funds for a family emergency or a tragic life event. Some scams, like the Nigerian prince scheme, promise to give you money if you just send your bank account information or pay a small processing fee. Mail recipient should be cautious about providing personal information or sending money.

4. BLOCKING SPAM

Enterprises and ISP's used variety of tools to process and filter incoming email. There is no single way of blocking spam combination of various techniques are used to achieve the objective.

4.1 Anti-Spam Filtering

Spam filter is a program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox. Like other types of filtering programs, a spam filter looks for certain criteria on which it bases judgments.It uses techniques such as Bayesian filters or other heuristic filters, attempt to identify spam through suspicious word patterns or word frequency. There are several different types of spam filters available:

- **Content filters** – review the content within a message to determine if it is spam or not
- **Header filters** – review the email header in search of falsified information
- **General blacklist filters** – stop all emails that come from a blacklisted file of known spammers
- **Rules-based filters** – use user-defined criteria – such as specific senders or specific wording in the subject line or body – to block spam
- **Permission filters** – require anyone sending a message to be pre-approved by the recipient
- **Challenge-response filters** – require anyone sending a message to enter a code in order to gain permission to send email.

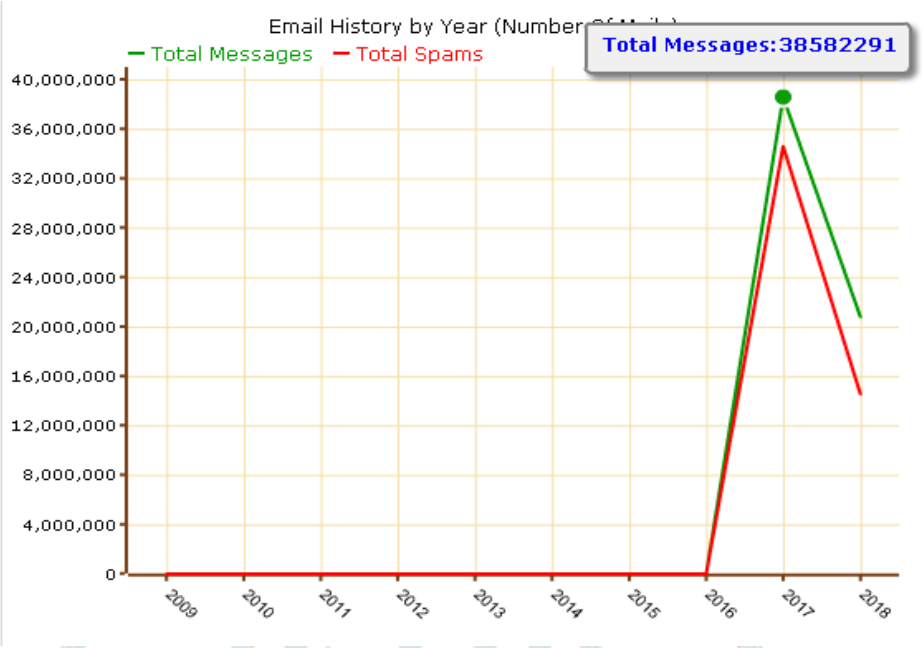

Fig 3. Spam data collected from enterprise
Tool used: Fortmail antispam solution

Year	Total	Spam	Spam %
2017	38582291	34595935	89.7
2018	20752952	14536509	70.0

4.2 Blacklists

Blacklists are databases that contain lists of sender domains and IP addresses of known and suspected spammers. Unfortunately, these blacklists also contain many legitimate email service providers (ESPs) and sender domains.

4.3 Custom Blocking

It is common for ISPs and corporate networks to create their own custom set of criteria for blocking. Many ISPs will use information from blacklists and content filters in a "weighted" system that gives "spam points" for each offensive piece of the message. If the incoming email has spam points above a set threshold it will be tagged as spam and sent straight to the mailbox trash folder, or it may be bounced back to the sender.

REFERENCES

[1] The Book of Spam: A Most Glorious and Definitive Compendium of the World's Favorite Canned Meat Hardcover – August 21, 2007. Dan Armstrong, Dustin Black

[2] Spam - The Cookbook. Marguerite Patten