2010 24th IEEE International Conference on Advanced Information Networking and Applications

Key Parameters in Identifying Cost of Spam 2.0

Farida Ridzuan, Vidyasagar Potdar, Alex Talevski, William F.Smyth
Anti Spam Research Lab,
Digital Ecosystems and Business Intelligence Institute, Curtin University of Technology, Perth, Western Australia
farida.mohdridzuan@postgrad.curtin.edu.au {v.potdar, a.talevski}@curtin.edu.au, smyth@mcmaster.ca

***Abstract*— This paper aims to provide an analytical view in estimating the cost of Spam 2.0. For this purpose, the authors define the web spam lifecycle and its associated impact. We also enlisted 5 stakeholders and focused on defining 5 cost calculations using a large collection of references. The cost of web spam then can be calculated with the definition of 13 parameters. Detail explanations of the web spam cost impacts are given with regards to the main four stakeholders: spammer, application provider, content provider and content consumer. Ongoing research in developing honey spam is also presented in this paper.**

Keywords-component; web spam, cost of spam

I. INTRODUCTION

Spam in the context of email is defined as "unsolicited, anonymous and mass email messages" [1, 2]. Spam originated via email and one of the first spam emails dates back to the early eighties, when a lawyer sent out an advertising email on a newsgroup. Since then spam has evolved into what we know as spam today. A spammer is defined as "an entity that is involved in spamming". Spammers use many different mediums to spam web users, drifting from the traditional email approach to new approaches that are termed Web Spam, Web 2.0 Spam or as we call it Spam 2.0 [3].

Spam 2.0 refers to the techniques employed by spammers to spread spam via websites in contrast to using emails. Spammers now use blogs, forums, wikis or even develop their own websites to post advertising material. Overall the motivation is still the same i.e. to generate revenue, increase page rank, promote product or services and steal user information [4].

Spammers use a number of techniques to drive traffic to their websites and one of those is to fine tune their websites to deceive search engines in increasing their ranking. It is quite common that when you search for a particular keyword, you are taken to a website which does not relate to what you are looking for, but instead it is an advertising page designed by spammers. Such websites are carefully crafted to make the search engines believe that it is providing genuine content by implementing keyword stuffing, incorporating fresh content and several other strategies [5].

Spamming activities affects number of different parties involved in the Web 2.0 spam lifecycle, which includes the developer (i.e. those who tries to implement anti-spam techniques like introducing CAPTCHA [6] to discourage spammers but also introduce another level of annoyance for users), spammer itself, followed by the Internet Service Provider (ISP), Application Provider (i.e. those who host blogs, forums, wikis etc.), Content Providers (i.e. users who add rich content to blogs, forums, wikis etc.) and finally the Content Consumer (i.e. the actual end users who uses this rich content). There is a cost associated for each an every stakeholder in the spam lifecycle i.e. the application provider has to spend time or money to ensure that their blogs or forums are free of spam, the content provider also spends time to filter out spam from their blog comments or forum posts, and finally the content consumer is adversely affected if spam content bypasses all the filters and is published on the web, since they cannot find the right information that they are looking for.

It is understood that there is a cost incurred by each stakeholder at each and every stage of the Web 2.0 spam lifecycle, however, to the best of our knowledge, there is no prior work that looks into detail at various cost parameters involved in the Web 2.0 spam lifecycle. No one has so far analysed the Web 2.0 spam lifecycle itself. Hence this paper aims to:

1. Understand Spam 2.0
2. List the key Spam 2.0 stakeholders
3. Identify different Spam 2.0 cost categories and cost parameters
4. Derive the cost associated with each stakeholder

This paper has been organized as follows. Section II will provide a detailed description of the Web 2.0 spam lifecycle. It will outline all the different stages in the web 2.0 spam lifecycle and associate different stakeholders to different stages. This section will also list different tools used by different parties for spamming or anti-spamming. Having understood the spam lifecycle, Section III then describes different costs categories for Spam 2.0 and its associated parameters used in deriving actual cost. Section IV then shows cost impact for each stakeholder. Section V then explains the prototype developed for capturing Spam 2.0, we call it HoneySpam. The prototype is being developed to estimate the costs for each stakeholder in the Spam 2.0 lifecycle. Section VI provides some thoughts on future research, ongoing work and concludes the paper.

II. SPAM 2.0 STAKEHOLDERS

In this section we list all the main stakeholders in the Spam 2.0 lifecycle. These include;

- Developer
- Internet Service Provider (ISP)
- Application Provider
- Content Provider

1550-445X/10 $26.00 © 2010 IEEE
DOI 10.1109/AINA.2010.163

- Spammer
- Content Consumer

A. Developer

Developer plays the role in developing programs or software to either help spammers or anti spammers. Most of the services provided by them are not free. Developer for the spammers' side will try to create program that could break the latest anti spam techniques. On the other hand, developer on the anti spammers' side will try to create new techniques or method to avoid spammers from successfully sending spam to the applications, such as the CAPTCHA [6]. Even though such techniques have been proven to be ineffective [7], they do slow down spam attacks. Nevertheless, programs that they create usually have a few drawbacks on the users. Generally, developer on both sides aims for high profit.

B. Internet Service Providers (ISPs)

Internet Service Providers (ISPs), as the name suggests, provide web hosting servers and services that can be accessed by both spammers and non spammers. ISPs also provide several other services such as selling domain names, email hosting and others. Some of the popular companies that provide internet access in Australia are BigPond, OptusNet, AAPT LiveNet, Virgin and Vodafone.

Both spammers and other stakeholders need access to the internet to send and receive spam which makes ISPs the connector between spammers and spam receivers. Spam is transmitted through the service that the ISP provides. In order to maintain a high service standard, ISPs must implement strategies to avoid unnecessary bandwidth hogging load and protect from successful intelligent attacks and many failed brute-force spam attacks.

Nonetheless, it is still unclear of how ISPs manage web spam. Not only is it hard to detect web spammers, it is impossible for ISPs to stop providing services to spammers. Even so, useless/wasteful contents are transmitted through the networks makes the network becomes slower and this affects client's satisfactory towards the services.

C. Application Providers

Application providers play an important role in the lifecycle as they host web applications. Some of the most popular applications are Wordpress, phpBB, SMF, and Blogger [8]. They are generic freely available Web 2.0 tools. They have many templates and plugins that enhance their operation in order to provide a better user experience and reach a greater user base. These plugins may provide better interfaces, embedded applications and spam filters. Application providers would also want to ensure that their blogs or forums are free of spam so they spend significant amounts of time and money to develop and integrate spam filtering tools such as CAPTCHA [6].

D. Content Providers

Content providers have the ability to add, edit and delete web content. They usually need to register for an account from the application provider. They could be the web administrator hired by a company, a paying sponsor, they could simply be an application user, or for instance, an author of a blog.

If we assume a world without spam, the real job of a content provider would be just to add rich content to their website. Unfortunately, with the existence of spammers, the content provider's tasks widen requiring them to maintain their application / websites to be spam free. They have to regularly check for spam comments, spam posts, spam reports from users, and this include determining and detecting whether it is spam or not. Without proper management, users or viewers of the applications would leave.

E. Spammer

Basically, the lifecycle of Spam 2.0 starts with the spammer. Spammers may work in a team in order to make the spam campaign a success [9]. Importantly, spammers also pay for people to manually spam websites [10]. Spammers use various techniques to spam Web 2.0 applications in order to make profits. They will not only try to bypass filters ensuring that their spam content can get through to the content consumers, but also to ensure that content consumers read their spam content and visit the links provided. The interesting thing that must also be considered is that such evidently lucrative jobs may take away from the regular labour force and / or may drive up labour prices. Furthermore, spammers then require whole new matching job position that is dedicated to spam prevention. Further reading on [9] could give an in depth knowledge of what a spammer is.

F. Content Consumer

A content consumer is the final stakeholder in the lifecycle of Spam 2.0. Similarly to the content provider, all spam content sent by spammers is basically targeted to the content consumers. They could be someone who is spam aware or they likely could be someone who has limited knowledge of spam. Using the internet, it is common that a user may stumble upon spam content and fall for it. This could mean that they may;

- Make a misinformed conclusion or decision (this could range from something very small to very large)
- Unable to find genuine content
- Spend additional time on a website as they filtering and searching through genuine and spam content
- Attempt to inform staff of the problem (which of course may redundantly occur many times by many users)
- Simply give up and no longer visit the site / lose interest
- Become emotionally frustrated, angry etc
- Being redirected to another site which may be one that replicates the original, is an advertising page or may even be something illegal and/or offensive.
- Their computer becomes infected with Malware [11].

III. LIFECYCLE OF SPAM 2.0

In this section we enlist the six main stages in Spam 2.0 lifecycle. These are as follows:

- Getting a list of URLs
- Creating Spam Content
- Sending Spam Content
- Filtering Spam at Application Level

- Filtering Spam at Personal Level
- Spam that Bypasses all Filters

The six stages are shown in Fig. 1 along with five stakeholders. The first three stages involve spammers, the next stage involves the application provider, followed by content provider and finally the content consumer. Between the third stage and the fourth stage, spam traverses from Spammer to ISP and to content provider. At this stage it is not clear on what steps are taken by the ISP to filter out Spam 2.0, we have neglected this party in further discussions. We are also neglecting developer from this point forward as developer can be considered working on both sides. We now explain each stage in detail.

A. Getting a list of URLs

This is the first stage in the Spam 2.0 lifecycle. Here the spammers compile a list of URLs pointing to vulnerable web 2.0 applications like blogs, wikis, forums etc. Such application URLs can be used for adding comments or links on forum, wiki or blog threads. Vulnerable web applications can be found using shareware or commercial tools like Win Web Crawler, Web Data Extractor, Rafabot, Extract Link, Online Data Extractor, Visual Web Spider, Hrefer and Teleport [12-19]. Some of these tools are free for a limited time while others come with limited features in the free version. Alternatively, spammers may be opting for freeware such as Elite Web Crawler, WebReaper, URL Spider Pro, Heritix and WebSphinx [20-24].

It is not sure whether spammers are using any other sophisticated tools for crawling vulnerable sites or even detect dead links before actually spamming. Manual detection of dead links will be costly hence spammers may just spam all the collected links, given that the cost to spam 1 or a million websites would be marginal. From anti-spam perspective, web administrator could take some actions to prevent URL fetching by controlling which bots crawl their sites or index their pages.

B. Creating Spam Content

This is the second stage in the Spam 2.0 lifecycle. Creating spam content such that it can deliver the right advertising message while at the same time bypasses all anti-spam filters, is an extremely challenging task. Spammers are using intelligent methods to achieve this goal. It is observed that they create content using a combination of text messages, links and images [25]. It is understood that spammers have developed database of words, phrases and pictures for periodic use. It is also possible for the spammers to use SEO Text Generator or Keyword List Generator to create good spam content messages. In order to avoid being detected as spam content, spammers develop unique content so as to avoid being blacklisted. One of the spammers' tools that include this feature is X-Rumer Palladium [18].

The ultimate motivation for spammers is to provide a link or build a link farm that could generate revenue for them.

C. Sending Spam Content

This is the third stage in the Spam 2.0 lifecycle. Spammers can either manually or automatically send spam to Web 2.0 applications. If it is done manually, it can be done to a more specific target but as compared to automated approaches, this requires significant time. Hence, in order to send spam in bulk, spammers try to create or buy spambot that performs this task in an streamlined and automated fashion [26]. This works out well because most of Web 2.0 application uses generic templates which have the same format and data entry / validation requirements.

X-Rumer Palladium [18] is a tool that can be used for auto registration and posting spam on a forum, guestbook, wiki and other applications. This tool can be used to break most recent CAPTCHA and pass many antispam filters. With this tool, spammers can send spam automatically with a higher success rate.

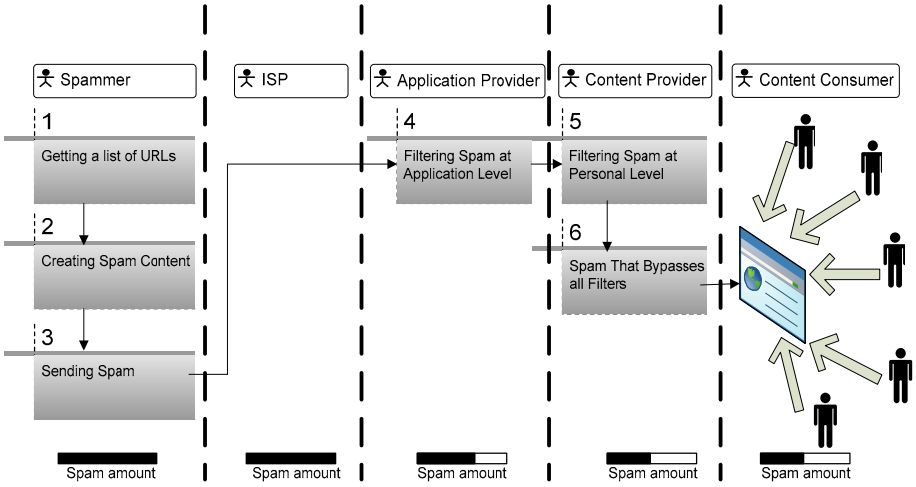

Figure 1. Lifecycle of web spam.

D. Filtering Spam at Application Level

This is the fourth stage in the Spam 2.0 lifecycle. Spam can be seen to be sent directly or indirectly. For instance, spam messages can be sent directly to the users of a forum using private messaging. On the other hand, if it is a spam entry in a forum, then the forum's users can be considered to have

received spam indirectly. This works similarly for comments in blog and wiki. At the application level, web administrators hired by the application provider can install a number of antispam filters to quarantine possible spam content. Existing antispam filters apply blacklisting, whitelisting, keyword checking or other techniques to make an initial decision to quarantine.

To avoid spammers from easily sending spam to web applications, there are some tools that web administrators could use. For forums, TruBar and Anti-Spam Verification Questions for SMF are some of the antispam programs that can be applied [27, 28]. The latest version of phpBB has already embedded antispam filters including CAPTCHA into their package [29]. NoSpamNX, Typepad AntiSpam, AntispamBee, Trollguard Beta, WP Hashcash Plugin and WP-SpamFree are developed for Wordpress [30-35]. Other most applied antispam filter for web applications are Akismet and Defensio [36, 37]. Defensio supports various types of platforms other than Wordpress, such as AintaBlog, Drupal, Dotclear and Textcube [36]. Though these tools usually come with no cost for personal use, they usually require frequent updates and / or data for training.

E. Filtering Spam at Personal Level

While on this stage, the effort in eliminating spam is fully dependable on content provider's effort. The content provider has the appropriate permissions to add, edit and delete the spam content manually. Content providers can also report, delete, approve or even close the application. At this stage, there is almost nothing that spammers can do except to hope that the users would not delete spam content and somebody would fall for the trap by clicking on the link provided in the spam content. This is where the content provider plays an active and important role in managing their own application.

F. Spam that Bypasses all Filters

Web spam content usually consists of a spam message, followed by a link which will take a user to another site which generates revenue for the spammers. Spam that bypasses filters is likely to be seen by many users. If the link is clicked, then the search engine rank for that site linked with the spam will improve which is one the spammer's motivation for spamming.

At this stage, the targets of the web spammer are the content consumer. Content consumer have no access to edit or delete web spam, but they are able to view the content and possibly to report it to administrators. For forum content, consumers are the forum users. This applies similarly for blog and social networking applications. Meanwhile, for wikis, anyone could have the access to view and modify content.

IV. Cost Categories of Spam 2.0

This section will show how the defined parameters are generally related to costs related to spam.

A. Defining Parameters

Based on previous research and several spam cost calculators that are currently available, there are several costs that can be calculated in order to estimate the price of email spam but no solutions currently exist that can calculate the cost of Spam 2.0. It is important to define the related costs that are measurable such as time and money. Hence, intangible cost such as the users' level of annoyance in dealing spam is not included in the calculation.

Spam content for all type of applications have a basic unit. For email, the basic unit that is commonly used is the messages. We define spam content for all types of Web 2.0 applications as follows:

TABLE I. Web 2.0 Application and Spam Units

Type of Web 2.0 Application	Forum	Wiki	Blog	Social networking
Spam Unit	post, poll, personal message, attachment	article, tag, reference	entry, comment, tag	post, comment, tag, personal message, user

Spam content will refer to the basic unit for each type of application. Further definitions of terms used in cost calculations and generic definitions for calculating each cost are defined in this section.

1) Storage Cost : Storage cost as explained in [8, 36] is the cost for "the storage space used to keep message". In the case of web spam, storage cost is the cost spent for server storage used to store any information such as list of URL to spam for spammers and blacklisted IP addresses for company and ISP and most of the time, storage used to store actual spam content. Parameters for storage cost function are generally defined as follow:

$$C_s = f(a,b,c,d) \tag{1}$$

where a = monthly storage cost/GB
b = total amount of spam content/day
c = total spam content size
d = duration of storage before elimination

2) Bandwidth Cost : Bandwidth cost as explained in [8] is "the bandwidth taken to download the message". In our case, we define bandwidth cost as the cost used for connectivity. In this case, all parties are going to bear the cost of connectivity with different amount. Bandwidth cost function needs parameters as defined below:

$$C_b = f(e,f,g) \tag{2}$$

where e = connectivity cost
f = type of application percentage representing bandwidth
g = spam percentage of all types of applications

3) Human Resource Cost (Annual Support Cost for Spam Filter) : Human resource cost or annual support cost for spam filter is the cost used by the associated party for spamming or spam filtering. This cost can be defined as follow:

$$C_{hr} = f(h) \quad (3)$$

where h = salary for human resource incharge of support spam queries.

4) Annual Productivity Cost : Annual Productivity cost in usual cases would consider the recipient time to delete spam messages. In this case, annual productivity cost is defined as the cost calculated in order to identify the cost of time that the recipient of spam spent to combat spam. Parameters for this cost function are as follow:

$$C_{ap} = f(i,j,k,l) \quad (4)$$

where i = time to clear out spam content/each check,
j = time to look for false positive for marked spam content/each check,
k = time used to determine that it's a spam/each check,
l = how many times users check/day.

5) Software Cost : Spammers or users usually rely on software or program to spam or for spam filtering. There is a lot of free open source software but sometimes it requires settings, knowledge and skills to be able to use them effectively. Therefore, it is easier to opt for software that is easy to use, easy to setup and most of them come with a price. This cost can be defined as follow:

$$C_{sw} = f(m) \quad (5)$$

where m = software costs.

Listed in Table II below are the parameters used in calculation for spammer, application provider, content provider and content consumer. Even though we are trying to define a generic definition for each cost calculation, there might still be some cost calculation that is not going to be applicable to certain party thus showing that parameters used vary depends on the cost calculation.

TABLE II. PARAMETERS USED FOR SPAMMER, APPLICATION PROVIDER, CONTENT PROVIDER AND CONTENT CONSUMER.

Parameter	Abb.	Spammer	Application Provider	Content Provider	Content Consumer
Storage Cost					
Monthly storage cost/GB	*a*	X	X	X	X
Total amount of spam content/day	*b*		X	X	X
Total spam content size	*c*	X	X	X	X
Duration of storage before elimination	*d*	X	X	X	X
Bandwidth Cost					
Annual fee connectivity cost	*e*	X		X	X
Type of application percentage representing bandwidth	*f*			X	X
Spam percentage of all type of applications	*g*			X	X
Human Resource Cost					
Salary for human resource incharge of supporting spam queries	*h*		X	X	
Annual Productivity Cost					
Time to clear out spam content/each check	*i*			X	X
Time to look for false positive for marked spam content/each check	*j*			X	X
Time used to determine that it's a spam/each check	*k*			X	X
How many times users check/day	*l*			X	X
Software Cost					
Software costs	*m*	X		X	

This section has explicitly defined 13 parameters used in cost calculations. These cost calculations will have different effects on each stakeholder that receive the spam. This will further be explained in the next section.

V. STAKEHOLDER'S COST

Fig. 2 below shows the cost impact of web spam towards six parties: spammer, ISP, application provider, content provider, content consumer and country. Lifecycle of web spam starts from the spammers' side and continues to ISP followed by the application provider, content provider and content consumer. As we have mentioned earlier, we are not going to focus on ISP side as it is unclear of how much ISP played their role in filtering web spam. In this research, we are only going to focus the cost impact of spam towards four stakeholders that we have introduced in Section II. Based on the generic parameters set in previous section, each cost associated for spammer, application provider, content provider and content consumer are going to be identified.

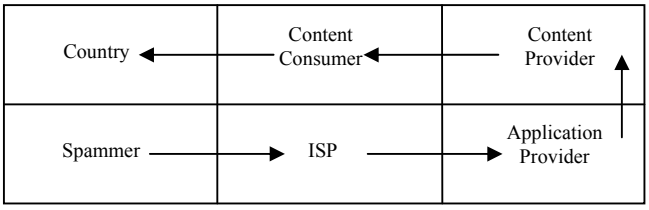

Figure 2. Web spam cost impacts.

A. Cost of Web Spam for Spammers

The fact that spammers also spend some amount of money [9] to spam questions the profit that they obtain from this activity. Hence, this section will further specify the related cost needed for spammers to spam in the web domain in each associated stage of lifecycle that we have introduced earlier.

The lifecycle of web spam starts with spammers as they gather a list of URLs. Spammers can use tools to collect a list of URLs such as Win Web Crawler, Web Data Extractor, Rafabot, Extract Link, Extract URL, Online Data Extractor,

Visual Web Spider and Teleport. These softwares range in price between AUD43 to AUD220. To keep the cost as low as possible, spammers could use freeware Elite Web Crawler, WebReaper, URL Spider Pro, Heritix and WebSphinx. Spammers need to have access to bandwidth and storage to keep a list of URLs. Storage and bandwidth cost is associated with stage 1 for spammers. Hence, parameters set for storage cost and bandwidth cost used by spammer are as follow:

$$C_s = f(a,c,d) \tag{6}$$

$$C_b = f(e) \tag{7}$$

Spammers could also find unsecured machines and use them to send spam. This could further reduce the cost for spammers. As can be seen, the cost that spammers have to bear are relatively small compared to other parties. In stage 2, spammers would have to generate spam content. Tools that can be used by spammers to generate spam content is SEO Text Generator which can be downloaded for free. However, there is an additional cost that spammers have to spend such as software costs. In order to send spam, X-Rumer 5.0 Palladium which costs AUD596. It has the capability to surpass different types of CAPCTHA. This software could also be used in all three stages of the lifecycle of web spam involved with spammers which are to find target for sending spam, create spam content followed by sending spam effectively.

B. Cost of Web Spam for Application Provider

In the effort of avoiding losing legitimate posts, it is easier to flag spam content so that it could be checked by the web administrator itself. Once the admin checks it, the admin would either read it and clear the content as non-spam or delete it if it is spam. This process requires additional storage and includes the cost of filtering because the efficiency of this method depends on the filter itself. Suppose if the email or content itself contains big attachment files or large images, this will increase the storage requirement and its cost. Storage cost is associated between stage 4 and 5 for users. Storage cost parameters can be defined as equation 1.

Application providers also play an active role in creating a better antispam filter. They create antispam plugins with better features in order to promote their services. We define the cost of creating a plugin as a human resource cost in equation 3. Nevertheless, there is a cost of deploying plugins that is used for commercialized purposes and this cost has to be paid by the content provider. This cost will further be explained in the next section.

C. Cost of Web Spam for Content Provider

Suppose if a company would like to open a forum or a blog, this company plays the role as a content provider. In this case, storage cost as defined in equation 1 has to be paid by the content provider. Storage cost is wasted for spam content. Hence, there is a need for someone to manage this forum or blog. Therefore, the company then needs to hire a web administrator to handle this.

Taking into account that not everybody has knowledge of what spam is, the administrator is hired to handle any upcoming issues from spam. This could include help-desk support or a team specially hired for fighting spam. In reality, this administrator is not only being paid their salary, they will also need to attend training for antispam technologies that is deployed for the web applications. This support cost for spam filters is associated with stage 5 in the case of lifecycle of web spam and can be defined as in equation 3.

Cost of bandwidth is clearly an important issue as bandwidth is wasted when used to download unnecessary spam content. Spam that is transmitted across the network consumes the bandwidth. It consumes a larger bandwidth capacity whenever the spam content embeds large images. As a consequence, users in a company have slower access to internet and slower download rates to more important tasks. Indirectly, users will take a longer time to finish a given task thus gives an impact to loss of productivity. This cost is associated during the transmission of web spam from spammer's side to user's side which is between stage 3 and 4 and this cost can be defined as in equation 2.

Annual productivity cost is measured for the time that is spent on each spam messages or spam content. This cost may vary depends on the user's knowledge and how well-formed spam content is. This cost is associated with stage 5 and it is calculated as in equation 4.

In stage 4 of the lifecycle where a web application is deployed with the spam filter, there is a dependency on software usage. Most of the plug-ins used in this stage are free for personal use, but consume money if used commercially. For instance, Mollom which is an antispam filter for blog, social network and community website is free if used for personal but costs AUD5860/year for each site if used commercially. Akismet on the other hand is charging AUD55 for filtering spam on a company's blog.

D. Cost of Web Spam for Content Consumer

Spam which is transmitted at the same time with legitimate content causes increase usage of network bandwidth and storage capacity. In order to obtain information from web applications, content consumer also bear the costs of waste storage used to download spam content and their bandwidth is also exhausted for this purpose as defined in equation 1 and 2.

Content consumers could also play an important role in eliminating spam that bypasses the filters. Even though they have no access to delete or edit any content on certain type of web applications, they still have the ability to determine spam content and report it to web administrator. This reduces productivity. This cost can similarly define as in equation 4.

VI. PROTOTYPE DEVELOPMENT OF HONEYSPAM

Using 5 cost categories involving 13 parameters that we have defined earlier, we are now going to develop honey spam that could estimate the cost of web spam. This section will first explain honey spam followed by detailed discussion on how we plan to measure each cost categories.

Towards determining the cost of spam, it is essential to first decide the number of web that is infected by spam. Honey

spam that we are developing contains a crawler engine, content extractor and evaluation engine, such as in Fig. 3. The crawler engine is going to be used to crawl to discover Web 2.0 applications. The data collected is going to be used as a reference which will be used in estimating the total amount of web spam.

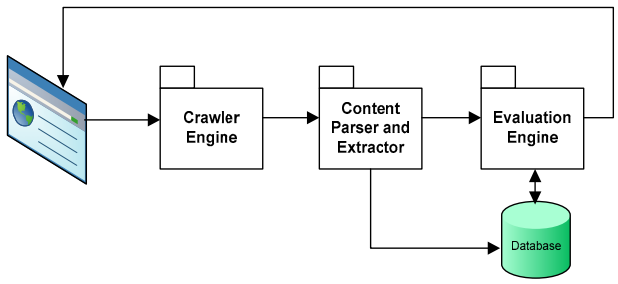

Figure 3. Prototype of HoneySpam Framework.

Meanwhile, the content extractor is going to be used to extract information that is available on a particular Web 2.0 application. The content extractor will parse HTML files that were downloaded earlier and extract valuable information.

This raw data will then be transformed to valuable information. This will then be passed to the evaluation engine which will decide whether the websites are spam-infected or not. The evaluation engine will contain a combination of several effective solutions to categorize a site into spam or not. This system will then report to the owner of the sites whether their site is spam infected or not. The evaluation engine will then be updated with new information.

Basically, based on the estimated amount of web spam for our honey spam above, we would be able to calculate the cost of spam. We will then be able to measure 13 parameters of five cost categories and this is going to be explained in the table below.

TABLE III. LIST OF PARAMETERS AND ITS MEASUREMENT.

Parameters	Abb	Measurement
Storage Cost		
Monthly storage cost/GB	*a*	Actual server cost paid for each GB
Total amount of spam content/day	*b*	Spam content received by all users in the certain duration of data collection recorded each day
Total spam content size	*c*	Actual size used to keep the content in storage
Duration of storage before elimination	*d*	Close observation towards the spam content requires the content of a specific type of application to be downloaded every day
Bandwidth Cost		
Annual fee connectivity cost	*e*	Current cost that users have to pay for the connectivity.
Type of application percentage representing bandwidth	*f*	Not decided yet.
Spam percentage of all type of application	*g*	Storage that spam content uses compared to full downloaded data storage.
Human Resource Cost		
Salary for human resource incharge of support spam queries	h	Current salary usually paid to the network administrator requires further survey on current situation in order to determine its precise value.
Annual Productivity Cost		
Time to clear out spam content/each check	*i*	Measurement for this cost depends on how fast a user can interact with system which also depends on how familiar users are with the application.
Time to look for false positives for marked spam content/each check	*j*	Measurement for this cost may vary depending on how knowledgeable users are. It is also possible to measure this based on author's experience.
Time used to determine that it's a spam/each check	*k*	Measurement for this cost has not been decided yet but it is also possible to measure this based on author's experience or several ongoing research.
How many times users check/day	*l*	It is possible to use a predetermined default value for this parameter.
Software Cost		
Software costs	*m*	Assuming that spammers would use software to spam, our calculation will consider the lowest cost software that could be used by spammers in each stage of lifecycle.

VII. ONGOING RESEARCH, DISCUSSION AND CONCLUSION

Sophos discovers one new infected webpage in every 3.6 seconds [38]. This statistic shows that even with all the technologies and methods that the anti spammers are using now; the spammers still could keep up with them [39]. It's still an "arm race" between these two parties. Unfortunately, while the race is going on between them, users are the ones who have to bear the consequences of this situation. In order to fight spammers, an individual has to spend their valuable time to check for spam content. As for the other parties, they have to prepare larger storage and spend extra on antispam technology.

The authors first identify the lifecycle of web spam and tools that can be used in completing each stage. We then listed the stakeholders involved in the webspam lifecycle. Afterwards, we identify five cost categories with their related parameters. Finally, we derive each stakeholder's cost based on the five cost categories. Considering that we are going to measure the cost of web spam accurately based on a large spam reference collection, there is a need to formulate all associated costs accordingly. It is important to take note that there are several key issues in calculating the cost of web spam.

A considerable amount of this report has been published on the cost of email spam. However, to the authors' knowledge there are no reports or studies on the cost of web spam. As we define Spam 2.0 cost, we noticed that some parameters can be easily defined and measured using our reference collection of downloaded data. Nevertheless, some parameters are highly dependable on current situation and need further survey to find the most acceptable value such as parameter a and h. In addition, there are some others that are not easily measured and are highly dependable on the user itself. For instance, parameters i, j,k, and l which could also be measured based on author's experience.

Moreover, some parameters depend on current technologies which may affect its price such as a and m. There is also a need

to collect data regularly/everyday hence a bigger collection of data would consume a bigger storage space such as parameter d which need a close observation towards determining its value. We are also aware of the resulting values for each attributes may vary depending on several factors such as popularity of the forum, thread, users/topic, number of posters and the administrator's effort.

It is obvious that ISPs are playing their role in filtering email spam. Therefore, it is interesting to find out how ISPs play their role in filtering web spam which requires further research in the future. By developing the HoneySpam and as the ongoing research is progressing, we would finally hope to develop a real time cost spam calculator based on the five cost categories and 13 parameters that we have defined earlier. It is believed that this cost calculator could provide a better overview of how serious the web spam problem is.

REFERENCES

1. Cournane, A. and R. Hunt, An analysis of the tools used for the generation and prevention of spam. Computers & Security, 2004. 23(2): p. 154-166.
2. Spamhaus. The Definition of Spam. [cited 2010 25 January]; Available from: http://www.spamhaus.org/definition.html.
3. Hayati, P. and V. Potdar, Toward spam 2.0: an evaluation of web 2.0 anti-spam methods, in 7th IEEE International Conference on Industrial Informatics (INDIN 2009) 2009: Cardiff, Wales.
4. Hayati, P. and V. Potdar, Evaluation of spam detection and prevention frameworks for email and image spam: a state of art, in Proceedings of the 10th International Conference on Information Integration and Web-based Applications \& Services. 2008, ACM: Linz, Austria.
5. Lin, Y.-R., et al., Detecting splogs via temporal dynamics using self-similarity analysis. ACM Transactions on the Web (TWEB), 2008. 2(1).
6. Ahn, L.v., M. Blum, and J. Langford, Telling humans and computers apart automatically. Communications of the ACM, 2004. 47(2 (February 2004)): p. 56-60.
7. Yan, J. and A.S.E. Ahmad. A low-cost attack on a Microsoft captcha. in Conference on Computer and Communications Security. 2008. Alexandria, Virginia, USA: Proceedings of the 15th ACM conference on Computer and communications security.
8. Su, C.-c. An Open Source Portal for Educators. TESL-EJ 9,1 2005 [cited 2009 23 November]; Available from: http://tesl-ej.org/ej33/int.html.
9. Spammer-X, J. Posluns, and S. Sjouwerman, Inside the SPAM Cartel: By Spammer-X. 2004: Syngress.
10. Gyongyi, Z. and H.G. Molina, Web spam taxonomy, in 1st International Workshop on Adversarial Information Retrieval on the Web. 2005.
11. Provos, N., M.A. Rajab, and P.i.M. ommatis, Cybercrime 2.0 : when the cloud turns dark. Communication of the ACM. Vol. 52. 2009. 42-47.
12. Win Web Crawler - Powerful webcrawler, web spider, website extractor. [cited 2009 23 November]; Available from: http://www.winwebcrawler.com/.
13. Web Data Extractor - Extract URL, Meta Tag, Email, Phone, Fax from Web. [cited 2009 23 November]; Available from: http://www.webextractor.com/.
14. RafaBot - Download Websites! Bulk website downloading and spidering software [cited 2009 23 November]; Available from: http://www.spadixbd.com/rafabot/.
15. Offline Email Extractor/Link Extractor [cited 2009 23 November]; Available from: http://www.spadixbd.com/elink/.
16. Online Data Extractor - Extract Email, Phone, Fax, URL, Meta Tag from website, search engine. [cited 2009 23 November]; Available from: http://www.onlinedataextractor.com/.
17. Visual Web Spider, Website Crawler, Web Robot, Website Ripper. [cited 2009 23 November]; Available from: http://www.newprosoft.com/web_spider.htm.
18. Botmaster.net. Botmaster.net : autosubmitter's XRumer description. 2009 [cited 2009 13 November]; Available from: http://www.botmasternet.com/more1/.
19. Tenmax.com. Teleport Pro - Offline Browsing Webspider. [cited 2009 13 November]; Available from: http://www.tenmax.com/teleport/pro/home.htm.
20. Sourceforge. WebSphinx. 2009 [cited 2009 9 November]; Available from: http://sourceforge.net/projects/websphinx/.
21. Heritrix. 16 October 2009 [cited 2009 9 November]; Available from: http://crawler.archive.org/.
22. Brothersoft. URL Spider Pro 3.3.3. [cited 2009 9 November]; Available from: http://www.brothersoft.com/url-spider-pro-5727.html.
23. Otway, M. WebReaper. [cited 2009 9 November 2009]; Available from: http://www.webreaper.net/download.html.
24. Brothersoft. Elite Web Crawler. [cited 2009 9 November]; Available from: http://www.brothersoft.com/elite-web-crawler-298613.html.
25. Nagamalai, D., B.C. Dhinakaran, and J.-K. Lee, An in-depth analysis of spam and spammers. 2009.
26. Hayati, P., et al., HoneySpam 2.0: Profiling Web Spambot Behaviour. , in PRIMA 2009. 2009: Nagoya, Japan.
27. PHP-Nuke. PHP-Nuke - TruBar 4.0(Silent) - anti-spam MOD. 2009 [cited 2009 13 November]; Available from: http://phpnuke.org/modules.php?name=News&file=article&sid=8244.
28. Simple Machines. Anti-Spam Verification Questions for SMF 1.1.7 2009 [cited 2009 13 November]; Available from: http://custom.simplemachines.org/mods/index.php?mod=1516.
29. phpBB. phpBB Features. 2009 [cited 2009 13 November]; Available from: http://www.phpbb.com/about/features/?from=submenu.
30. Kubiak, S. Plugin Directory. 2009 [cited 2009 13 November]; Available from: http://wordpress.org/extend/plugins/nospamnx/.
31. TypePad Antispam. 2009 [cited 2009 13 November]; Available from: http://antispam.typepad.com/.
32. Müller, S. Plugin Directory. 2009 [cited 2009 13 November]; Available from: http://wordpress.org/extend/plugins/antispam-bee/.
33. Trollguard Beta. 2009 [cited 2009 13 November]; Available from: http://www.trollguard.com/.
34. WP Hashcash Plugin for Spam by Wordpress Plugins. 2009 [cited 2009 13 November]; Available from: http://wordpress-plugins.feifei.us/hashcash/.
35. Allen, S. Plugin Directory. 2009 [cited 2009 13 November]; Available from: http://wordpress.org/extend/plugins/wp-spamfree/.
36. Defensio - Wordpress Anti Spam Plugin. [cited 2009 9 November]; Available from: http://defensio.com/downloads.
37. Akismet. [cited 2009 13 November]; Available from: http://akismet.com/.
38. SOPHOS, Security threat report: July 2009 update -A look at the challenges ahead. July 2009.
39. Ferris Research, Spam, Spammers and Spam Control. March 2009, Ferris Research: San Francisco, Calif, USA.