# Anatomy of Comment Spam

## 1. Executive Summary

Spam is defined as irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc. By spamming multiple targets over a long period of time, spammers are able to gain profit, and do harm.

Like the flyers in our mailboxes, digital spam started its path to glory via email. However, with the evolution of web technologies and website interaction, spammers have moved to reaching users via the web, injecting spam comments into forums, comment fields, guest books, and even websites like Wikipedia, which allow user generated content to be published. And thus, comment spam was born.

Comment spammers are most often motivated by search engine optimization, so that they can use a promoted site for advertisement and malware distribution. Attackers are also known to use comment spam for the purpose of click fraud. The comment spam issue has become so prevalent that organizations are fighting back, by implementing mitigation services. Interestingly, there have been incidents of spammers fighting anti-spammers in an attempt to shut down those mitigation services, and many of those counter attacks have been successful.

We decided to study the comment spam space from both ends. In our research, we examined the attacker's point of view, including the comment spam techniques and tools. In addition, we examined the victim's point of view to understand how organizations deal with comment spam today.

### 1.1 Key Findings

Over the course of two weeks, from September 1 to September 14 in 2013 we monitored comment-spammer activity against more than 60 different applications. Here are some of our key findings:

- 58 percent of all comment spammers are active for long periods of time.
- 17 percent of all comment spammers generated the majority of comment spam.

In order to understand how a comment spammer attacks a web application, we looked closely at a single victim. This report includes this case study and what we have learned:

- 80 percent of comment spam traffic is generated by 28 percent of attackers.
- Over time, comment spammers increased their velocity against the attacked website.

### 1.2 Main Conclusions

Our conclusions were straight forward:

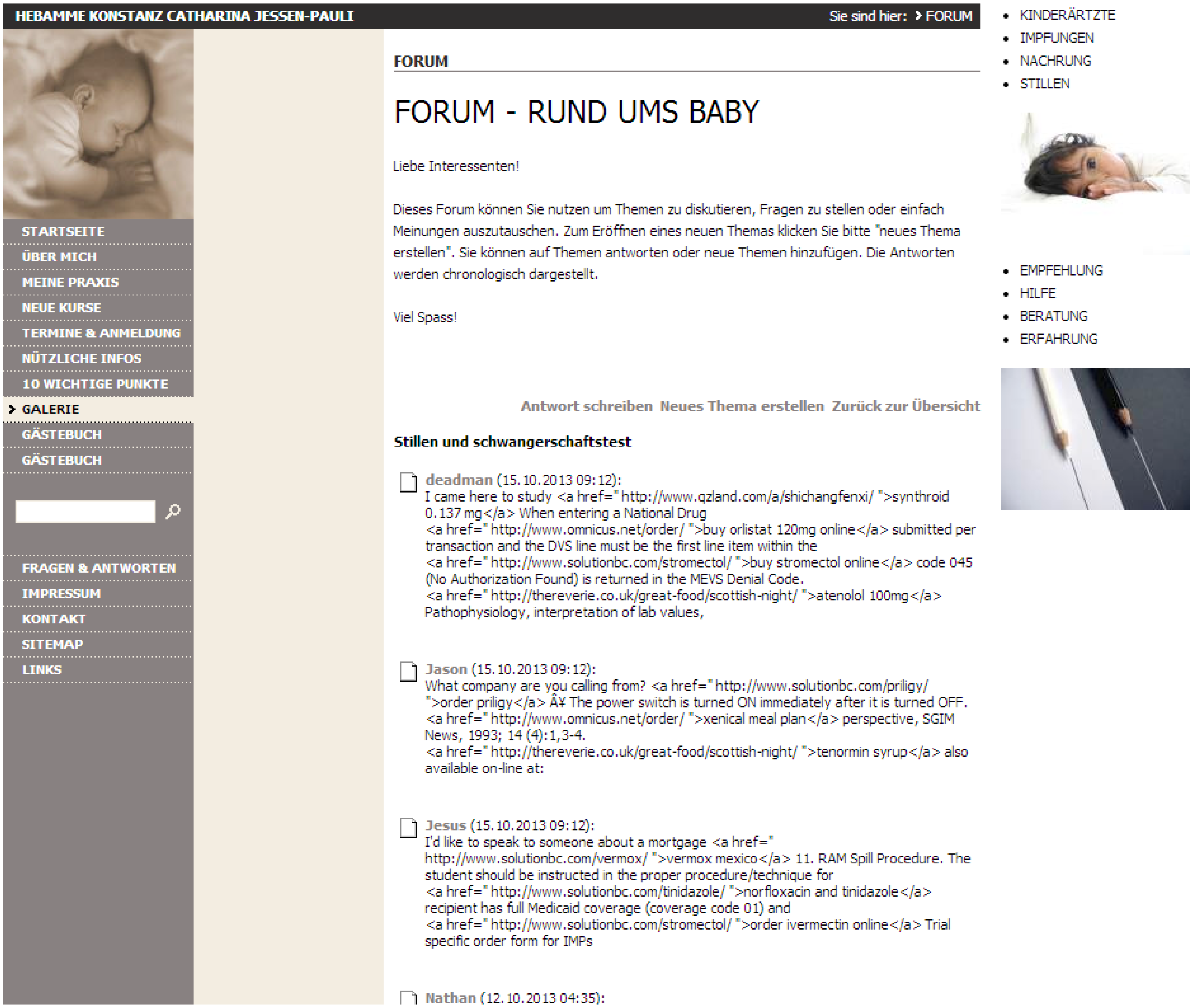
- Identifying the attacker as a comment spammer early on, and blocking the requests, prevents most of the malicious activity
- IP reputation will help in solving the comment spam problem, by blocking comment spammers early in their attack campaigns

## Table of Contents

## 2. Introduction

Wikipedia's definition for comment spam[1]: "Comment spam is a term used to refer to a broad category of spam bot postings which abuse web-based forms to post unsolicited advertisements as comments on forums, blogs, wikis and online guest books."

An example for a comment spammed site:



FORUM - RUND UMS BABY

Liebe Interessenten!

Dieses Forum können Sie nutzen um Themen zu diskutieren, Fragen zu stellen oder einfach Meinungen auszutauschen. Zum Eröffnen eines neuen Themas klicken Sie bitte "neues Thema erstellen". Sie können auf Themen antworten oder neue Themen hinzufügen. Die Antworten werden chronologisch dargestellt.

Viel Spass!

**Stillen und schwangerschaftstest**

**deadman** (15.10.2013 09:12):
I came here to study <a href="http://www.qzland.com/a/shichangfenxi/ ">synthroid 0.137 mg</a> When entering a National Drug
<a href="http://www.omnicus.net/order/ ">buy orlistat 120mg online</a> submitted per transaction and the DVS line must be the first line item within the
<a href="http://www.solutionbc.com/stromectol/ ">buy stromectol online</a> code 045 (No Authorization Found) is returned in the MEVS Denial Code.
<a href="http://thereverie.co.uk/great-food/scottish-night/ ">atenolol 100mg</a> Pathophysiology, interpretation of lab values,

**Jason** (15.10.2013 09:12):
What company are you calling from? <a href="http://www.solutionbc.com/priligy/ ">order priligy</a> Â¥ The power switch is turned ON immediately after it is turned OFF.
<a href="http://www.omnicus.net/order/ ">xenical meal plan</a> perspective, SGIM News, 1993; 14 (4):1,3-4.
<a href="http://thereverie.co.uk/great-food/scottish-night/ ">tenormin syrup</a> also available on-line at:

**Jesus** (15.10.2013 09:12):
I'd like to speak to someone about a mortgage <a href=" http://www.solutionbc.com/vermox/ ">vermox mexico</a> 11. RAM Spill Procedure. The student should be instructed in the proper procedure/technique for
<a href="http://www.solutionbc.com/tinidazole/ ">norfloxacin and tinidazole</a> recipient has full Medicaid coverage (coverage code 01) and
<a href="http://www.solutionbc.com/stromectol/ ">order ivermectin online</a> Trial specific order form for IMPs

**Nathan** (12.10.2013 04:35):

*Figure 1 – A Spammed Site Example*

Attackers use comment spam for various reasons. The most significant one is 'Search Engine Optimization' (SEO) – improving a site's ranking within a search engine result set (with respect to given search terms). A site ranking within a search engine result set is based on the number and quality of websites that hold links to it (AKA "back links"). Thus, posting many comments containing links to a target site increases its ranking within search engine result sets (especially with respect to keywords surrounding the link). Attackers then use the promoted site for advertisement (usually of dubious merchandise) and malware distribution. Attackers are also known to use comment spam for the purpose of Click Fraud.

[1] http://en.wikipedia.org/wiki/Comment_spam

## 3. The Attacker's Point of View

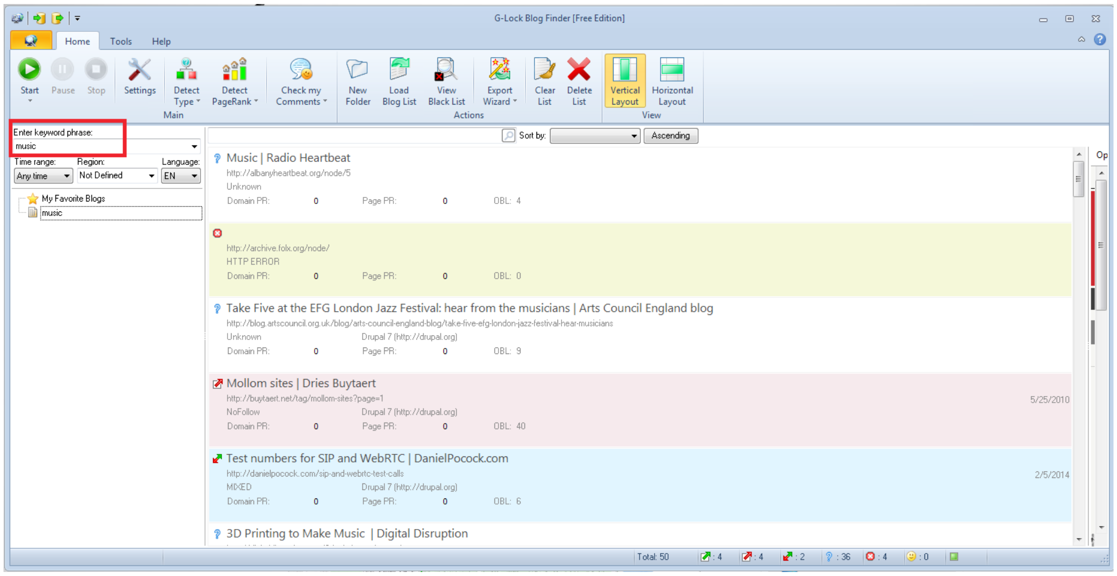
There are a few basic stages an attacker follows when aspiring to produce comment spam traffic. Each of these stages can be performed separately and needs to be fine-tuned:

- **Target Acquisition** (AKA URL harvesting): The task of finding quality vulnerable websites to post comments on is named "URL harvesting". The URL's quality is measured by the relevance to the promoted site; the URL's own search engine ranking; the difficulty of posting comments (for example un-protected public posts or Captcha protected posts) and the site's policy regarding search engines (for example the follow/nofollow value of the "rel" attribute of hyperlinks).
- **Posting**: Post the comments on the chosen URLs.
- **Verification**: Verify that the comments were indeed published.

## 4. Comment Spam in Practice

The attacker's success relies on publishing comment spam in large scales. Large scale comment spam is achieved by automating the aforementioned commenting process. For this purpose, automatic tools were developed which support this process and offer complementary services. The tools' input is a set of keywords relevant for the promoted site. The automated tools may encompass all of the following steps, or only part of them:

- **URL harvesting**: Automatic tools use popular search engines to locate relevant websites based on input keywords. Upon success, the tool explores the found websites, in order to locate suitable URLs for commenting. Blogs are the most popular websites for comment spam posting. In fact, some tools are limited to harvesting only blogs, and specifically WordPress blogs. Figure 2 - Automated Tool (G-Lock Blog Finder) for Harvesting shows an example of an automated tool (G-Lock Blog Finder) which specifically offers to harvest blogs. The user specified an input keyword: "music", and the tool located a relevant set of targets.



Enter keyword phrase: music

Time range: Any time  Region: Not Defined  Language: EN

Music | Radio Heartbeat
http://albanyheartbeat.org/node/5
Unknown
Domain PR: 0  Page PR: 0  OBL: 4

http://archive.folx.org/node/
HTTP ERROR
Domain PR: 0  Page PR: 0  OBL: 0

Take Five at the EFG London Jazz Festival: hear from the musicians | Arts Council England blog
http://blog.artscouncil.org.uk/blog/arts-council-england-blog/take-five-efg-london-jazz-festival-hear-musicians
Unknown  Drupal 7 (http://drupal.org)
Domain PR: 0  Page PR: 0  OBL: 9

Mollom sites | Dries Buytaert
http://buytaert.net/tag/mollom-sites?page=1  5/25/2010
NoFollow  Drupal 7 (http://drupal.org)
Domain PR: 0  Page PR: 0  OBL: 40

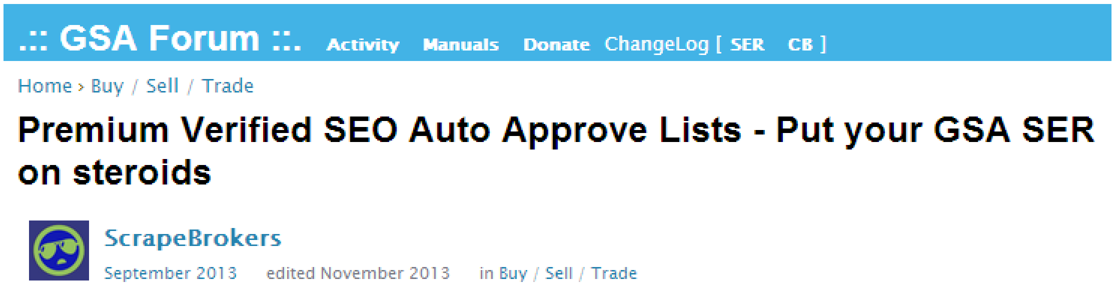
Test numbers for SIP and WebRTC | DanielPocock.com
http://danielpocock.com/sip-and-webrtc-test-calls  2/5/2014
MIXED  Drupal 7 (http://drupal.org)
Domain PR: 0  Page PR: 0  OBL: 6

3D Printing to Make Music | Digital Disruption

Total: 50  : 4  : 4  : 2  : 36  : 4  : 0

*Figure 2 – Automated Tool (G-Lock Blog Finder) for Harvesting Blogs*

Some attackers skip the harvesting stage, by purchasing lists of high quality URLs – URLs with high search engine ranking and which automatically approve comments. Thus many 'quality URLs' lists are available for purchase on black hat SEO forums and specific sites (Figure 3 shows an example). A typical price for a URL list is $40 for approximately 13,000 URLs.



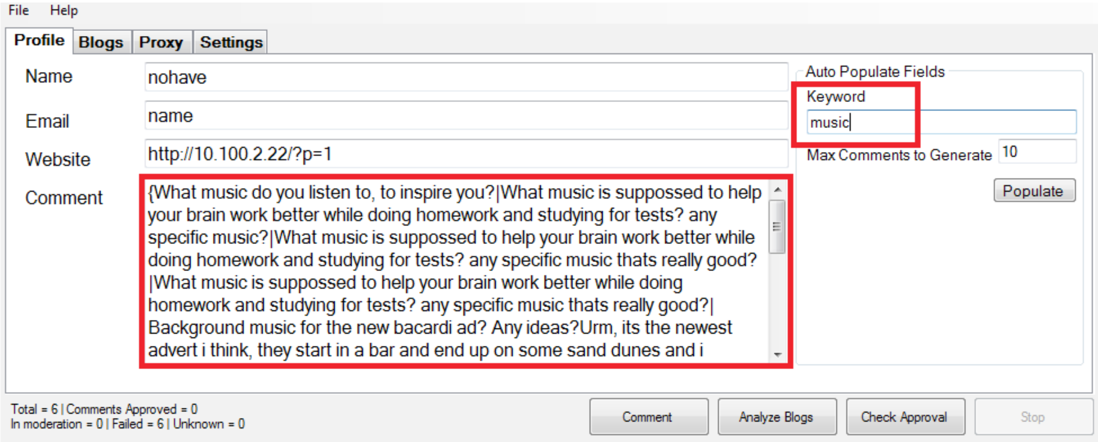
Premium Verified SEO Auto Approve Lists - Put your GSA SER on steroids

ScrapeBrokers

September 2013 edited November 2013 in Buy / Sell / Trade

*Figure 3 – URL Lists for Sale*

- **Comment generation**: Relevant verbal comments are attached to the promoted site links. This serves the SEO technique and provides a more authentic comment. The verbal comments are produced according to the input keywords. Figure 4 shows an example of a comment that was automatically generated by the 'Comment Blaster' tool for the input keyword 'music'.



Name: nohave

Email: name

Website: http://10.100.2.22/?p=1

Comment: {What music do you listen to, to inspire you?|What music is supposed to help your brain work better while doing homework and studying for tests? any specific music?|What music is supposed to help your brain work better while doing homework and studying for tests? any specific music thats really good?|What music is supposed to help your brain work better while doing homework and studying for tests? any specific music thats really good?|Background music for the new bacardi ad? Any ideas?Urm, its the newest advert i think, they start in a bar and end up on some sand dunes and i

Keyword: music

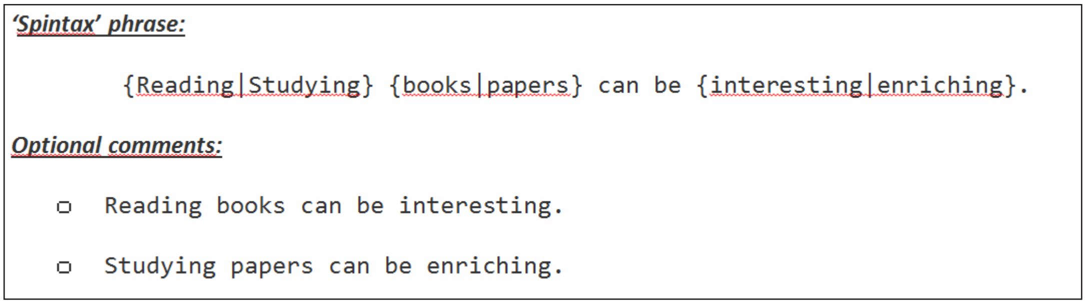
Max Comments to Generate: 10

Total = 6 | Comments Approved = 0
In moderation = 0 | Failed = 6 | Unknown = 0

*Figure 4 – Automatic Comment Example*

The comment in Figure 4 is written in "Spintax" format. One way to mitigate comment spam is to block duplicate comments. Spintax is an automatic method that was developed by spammers, in order to avoid this pitfall. The idea is for the spammer to create a generic comment using a specially formatted syntax. This generic comment can be spun into many different comments with a similar meaning. Figure 5 shows an example for the "Spintax phrase" and the resulting comments[2].

[2] http://umstrategies.com/what-is-spintax/



***'Spintax' phrase:***

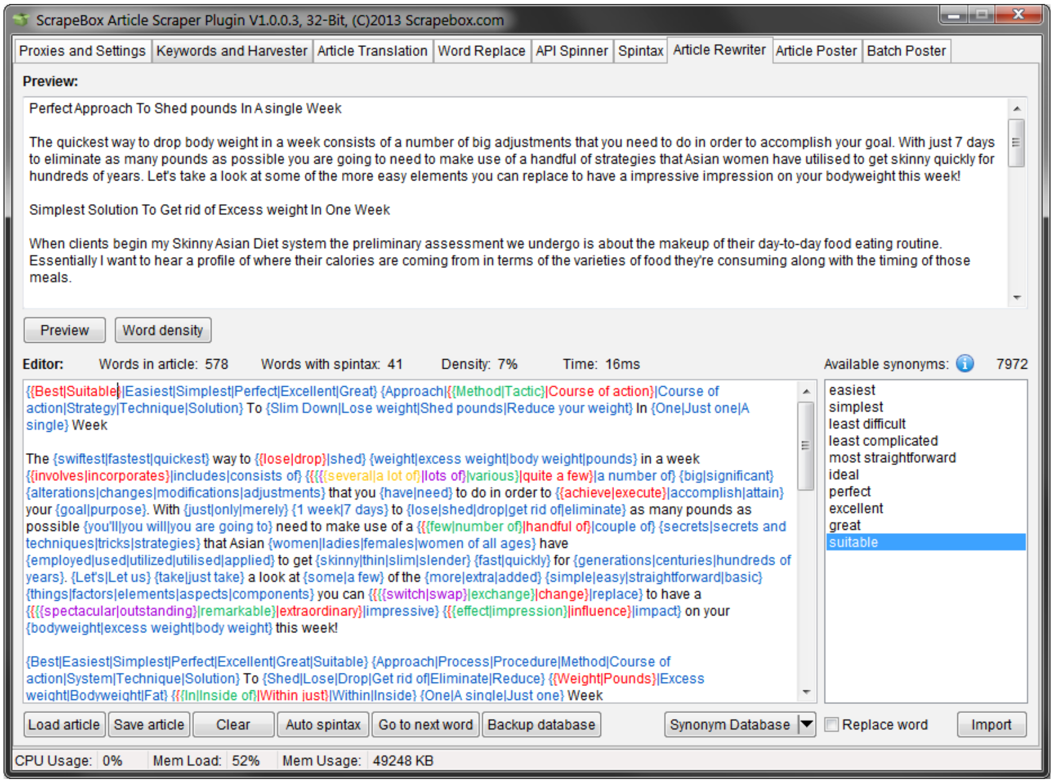
```
{Reading|Studying} {books|papers} can be {interesting|enriching}.
```

***Optional comments:***

```
o Reading books can be interesting.
o Studying papers can be enriching.
```

The Spintax phrase in Figure 5 has a few possible variations. For each unique comment, the tool selects a specific combination. The result is a full (hopefully sensible) comment.

Figure 6 shows an example of a Spintax created by ScrapeBox. This tool enables the user to input a keyword, or input/edit the Spintax itself.



Preview:

Perfect Approach To Shed pounds In A single Week

The quickest way to drop body weight in a week consists of a number of big adjustments that you need to do in order to accomplish your goal. With just 7 days to eliminate as many pounds as possible you are going to need to make use of a handful of strategies that Asian women have utilised to get skinny quickly for hundreds of years. Let's take a look at some of the more easy elements you can replace to have a impressive impression on your bodyweight this week!

Simplest Solution To Get rid of Excess weight In One Week

When clients begin my Skinny Asian Diet system the preliminary assessment we undergo is about the makeup of their day-to-day food eating routine. Essentially I want to hear a profile of where their calories are coming from in terms of the varieties of food they're consuming along with the timing of those meals.

Editor: Words in article: 578 Words with spintax: 41 Density: 7% Time: 16ms Available synonyms: 7972

{{Best|Suitable}|Easiest|Simplest|Perfect|Excellent|Great} {Approach|{{Method|Tactic}|Course of action}|Course of action|Strategy|Technique|Solution} To {Slim Down|Lose weight|Shed pounds|Reduce your weight} In {One|Just one|A single} Week

The {swiftest|fastest|quickest} way to {{lose|drop}|shed} {weight|excess weight|body weight|pounds} in a week {{involves|incorporates}|includes|consists of} {{{{several|a lot of}|lots of}|various}|quite a few}|a number of} {big|significant} {alterations|changes|modifications|adjustments} that you {have|need} to do in order to {{achieve|execute}|accomplish|attain} your {goal|purpose}. With {just|only|merely} {1 week|7 days} to {lose|shed|drop|get rid of|eliminate} as many pounds as possible {you'll|you will|you are going to} need to make use of a {{{few|number of}|handful of}|couple of} {secrets|secrets and techniques|tricks|strategies} that Asian {women|ladies|females|women of all ages} have {employed|used|utilized|utilised|applied} to get {skinny|thin|slim|slender} {fast|quickly} for {generations|centuries|hundreds of years}. {Let's|Let us} {take|just take} a look at {some|a few} of the {more|extra|added} {simple|easy|straightforward|basic} {things|factors|elements|aspects|components} you can {{{{switch|swap}|exchange}|change}|replace} to have a {{{{spectacular|outstanding}|remarkable}|extraordinary}|impressive} {{{effect|impression}|influence}|impact} on your {bodyweight|excess weight|body weight} this week!

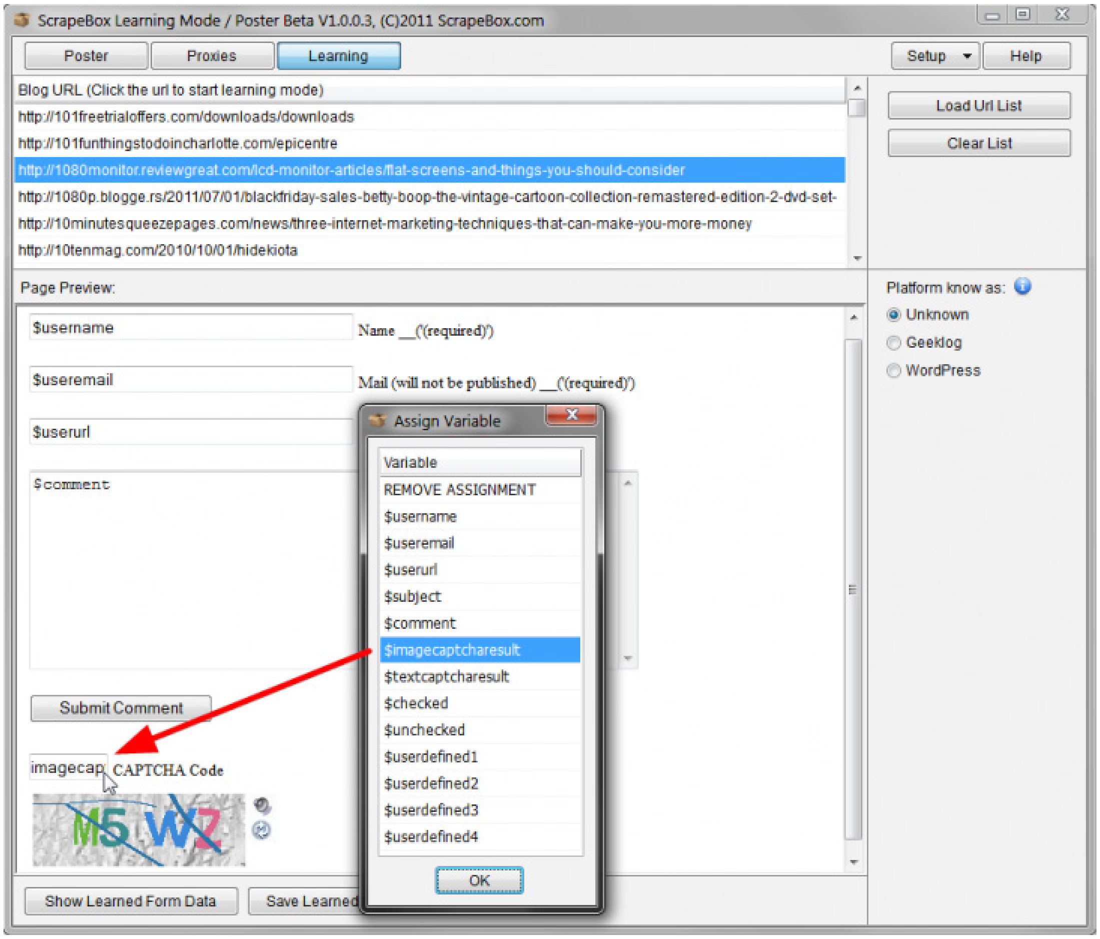
{Best|Easiest|Simplest|Perfect|Excellent|Great|Suitable} {Approach|Process|Procedure|Method|Course of action|System|Technique|Solution} To {Shed|Lose|Drop|Get rid of|Eliminate|Reduce} {{Weight|Pounds}|Excess weight|Bodyweight|Fat} {{{In|Inside of}|Within just}|Within|Inside} {One|A single|Just one} Week

easiest
simplest
least difficult
least complicated
most straightforward
ideal
perfect
excellent
great
suitable

CPU Usage: 0% Mem Load: 52% Mem Usage: 49248 KB

*Figure 6 – ScrapeBox Spintax Example*

- **Posting**: Tools offer to automatically post comments on many URLs at once. Some targets require different forms to be filled in order to submit comments, such as: user authentication, Captcha forms or user details. Sophisticated tools incorporate services to handle these challenges. Figure 7 shows how to configure the ScrapeBox tool to handle Captcha challenges.



ScrapeBox Learning Mode / Poster Beta V1.0.0.3, (C)2011 ScrapeBox.com

Blog URL (Click the url to start learning mode)
http://101freetrialoffers.com/downloads/downloads
http://101funthingstodoincharlotte.com/epicentre
http://1080monitor.reviewgreat.com/lcd-monitor-articles/flat-screens-and-things-you-should-consider
http://1080p.blogge.rs/2011/07/01/blackfriday-sales-betty-boop-the-vintage-cartoon-collection-remastered-edition-2-dvd-set-
http://10minutesqueezepages.com/news/three-internet-marketing-techniques-that-can-make-you-more-money
http://10tenmag.com/2010/10/01/hidekiota

Page Preview:

$username Name __('(required)')
$useremail Mail (will not be published) __('(required)')
$userurl
$comment

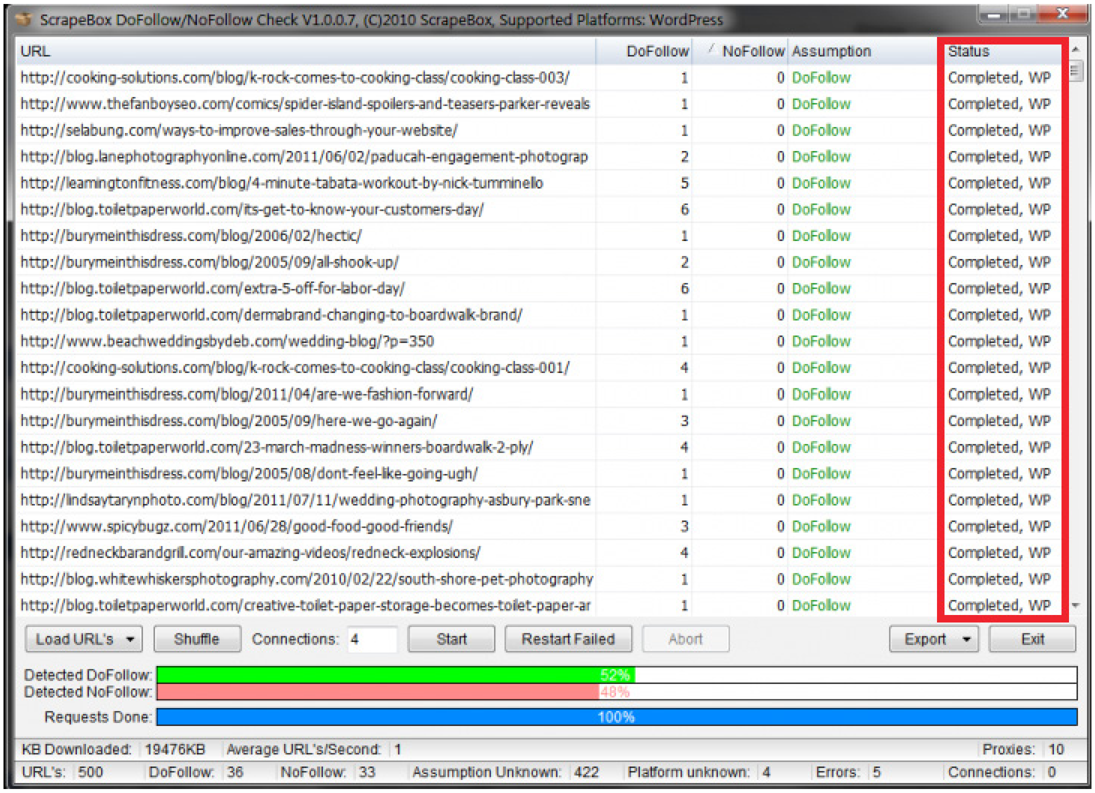
imagecap CAPTCHA Code

Platform know as:
● Unknown
○ Geeklog
○ WordPress

*Figure 7 – ScrapeBox Captcha Solving*

- **Verification**: Tools provide feedback to the user specifying whether or not a comment was posted.

Figure 8 shows an example of the ScrapeBox tool status report.



ScrapeBox DoFollow/NoFollow Check V1.0.0.7, (C)2010 ScrapeBox, Supported Platforms: WordPress

| URL | DoFollow | NoFollow | Assumption | Status |
|---|---|---|---|---|
| http://cooking-solutions.com/blog/k-rock-comes-to-cooking-class/cooking-class-003/ | 1 | 0 | DoFollow | Completed, WP |
| http://www.thefanboyseo.com/comics/spider-island-spoilers-and-teasers-parker-reveals | 1 | 0 | DoFollow | Completed, WP |
| http://selabung.com/ways-to-improve-sales-through-your-website/ | 1 | 0 | DoFollow | Completed, WP |
| http://blog.lanephotographyonline.com/2011/06/02/paducah-engagement-photograp | 2 | 0 | DoFollow | Completed, WP |
| http://leamingtonfitness.com/blog/4-minute-tabata-workout-by-nick-tumminello | 5 | 0 | DoFollow | Completed, WP |
| http://blog.toiletpaperworld.com/its-get-to-know-your-customers-day/ | 6 | 0 | DoFollow | Completed, WP |
| http://burymeinthisdress.com/blog/2006/02/hectic/ | 1 | 0 | DoFollow | Completed, WP |
| http://burymeinthisdress.com/blog/2005/09/all-shook-up/ | 2 | 0 | DoFollow | Completed, WP |
| http://blog.toiletpaperworld.com/extra-5-off-for-labor-day/ | 6 | 0 | DoFollow | Completed, WP |
| http://blog.toiletpaperworld.com/dermabrand-changing-to-boardwalk-brand/ | 1 | 0 | DoFollow | Completed, WP |
| http://www.beachweddingsbydeb.com/wedding-blog/?p=350 | 1 | 0 | DoFollow | Completed, WP |
| http://cooking-solutions.com/blog/k-rock-comes-to-cooking-class/cooking-class-001/ | 4 | 0 | DoFollow | Completed, WP |
| http://burymeinthisdress.com/blog/2011/04/are-we-fashion-forward/ | 1 | 0 | DoFollow | Completed, WP |
| http://burymeinthisdress.com/blog/2005/09/here-we-go-again/ | 3 | 0 | DoFollow | Completed, WP |
| http://blog.toiletpaperworld.com/23-march-madness-winners-boardwalk-2-ply/ | 4 | 0 | DoFollow | Completed, WP |
| http://burymeinthisdress.com/blog/2005/08/dont-feel-like-going-ugh/ | 1 | 0 | DoFollow | Completed, WP |
| http://lindsaytarynphoto.com/blog/2011/07/11/wedding-photography-asbury-park-sne | 1 | 0 | DoFollow | Completed, WP |
| http://www.spicybugz.com/2011/06/28/good-food-good-friends/ | 3 | 0 | DoFollow | Completed, WP |
| http://redneckbarandgrill.com/our-amazing-videos/redneck-explosions/ | 4 | 0 | DoFollow | Completed, WP |
| http://blog.whitewhiskersphotography.com/2010/02/22/south-shore-pet-photography | 1 | 0 | DoFollow | Completed, WP |
| http://blog.toiletpaperworld.com/creative-toilet-paper-storage-becomes-toilet-paper-ar | 1 | 0 | DoFollow | Completed, WP |

Connections: 4

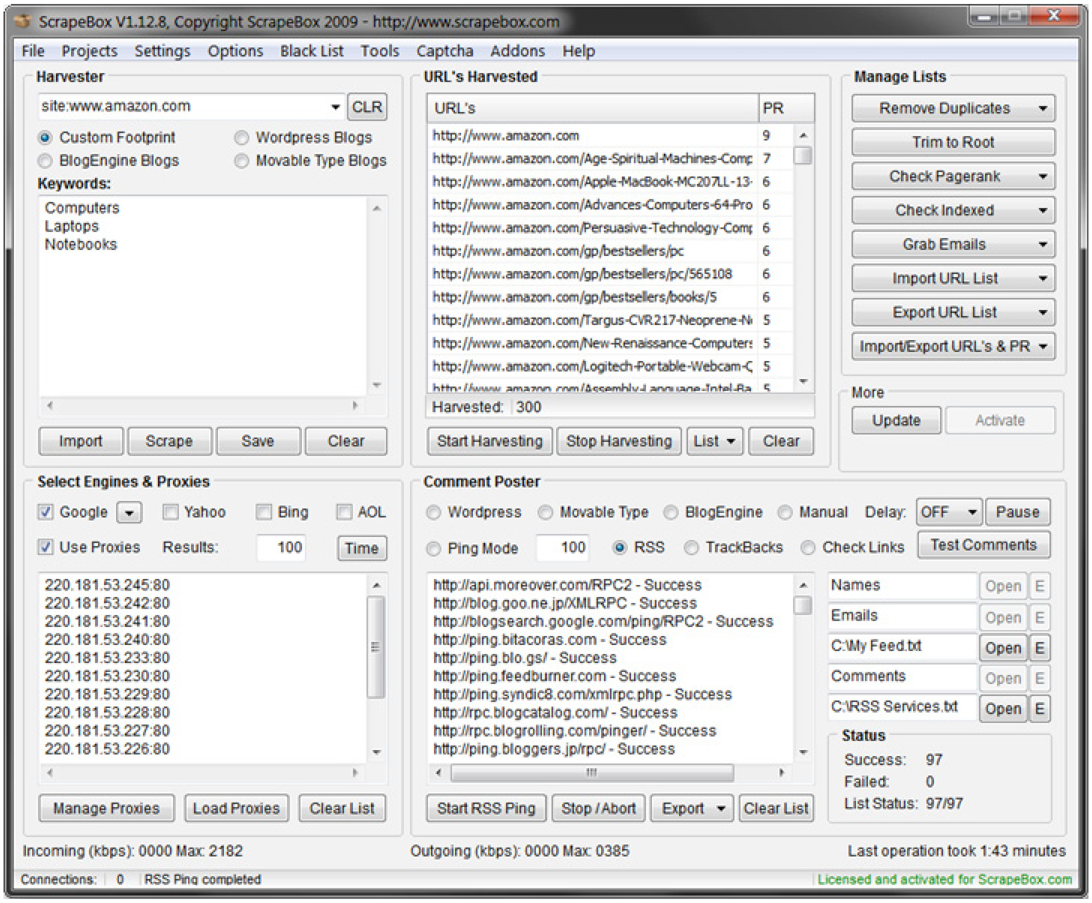
Detected DoFollow: 52%
Detected NoFollow: 48%
Requests Done: 100%

KB Downloaded: 19476KB | Average URL's/Second: 1 | Proxies: 10

URL's: 500 | DoFollow: 36 | NoFollow: 33 | Assumption Unknown: 422 | Platform unknown: 4 | Errors: 5 | Connections: 0

*Figure 8 – ScrapeBox Posting Status Report*

There are many automated tools that hold all or part of the functionalities discussed in this section. The popular implementations are the **ScrapeBox** tool, which offers all the mentioned features and is shown in Figure 9. The **Gscraper** tool is a new alternative that offers similar features with similar pricing.



ScrapeBox V1.12.8, Copyright ScrapeBox 2009 - http://www.scrapebox.com

**Harvester**

site:www.amazon.com

● Custom Footprint ○ Wordpress Blogs
○ BlogEngine Blogs ○ Movable Type Blogs

**Keywords:**

Computers
Laptops
Notebooks

**URL's Harvested**

| URL's | PR |
|---|---|
| http://www.amazon.com | 9 |
| http://www.amazon.com/Age-Spiritual-Machines-Comp | 7 |
| http://www.amazon.com/Apple-MacBook-MC207LL-13- | 6 |
| http://www.amazon.com/Advances-Computers-64-Pro | 6 |
| http://www.amazon.com/Persuasive-Technology-Comp | 6 |
| http://www.amazon.com/gp/bestsellers/pc | 6 |
| http://www.amazon.com/gp/bestsellers/pc/565108 | 6 |
| http://www.amazon.com/gp/bestsellers/books/5 | 6 |
| http://www.amazon.com/Targus-CVR217-Neoprene-N | 5 |
| http://www.amazon.com/New-Renaissance-Computers | 5 |
| http://www.amazon.com/Logitech-Portable-Webcam-C | 5 |
| http://www.amazon.com/Assembly-Language-Intel-Ba | 5 |

Harvested: 300

**Manage Lists**

**Select Engines & Proxies**

☑ Google ☐ Yahoo ☐ Bing ☐ AOL
☑ Use Proxies Results: 100

220.181.53.245:80
220.181.53.242:80
220.181.53.241:80
220.181.53.240:80
220.181.53.233:80
220.181.53.230:80
220.181.53.229:80
220.181.53.228:80
220.181.53.227:80
220.181.53.226:80

**Comment Poster**

○ Wordpress ○ Movable Type ○ BlogEngine ○ Manual Delay: OFF
○ Ping Mode 100 ● RSS ○ TrackBacks ○ Check Links

http://api.moreover.com/RPC2 - Success
http://blog.goo.ne.jp/XMLRPC - Success
http://blogsearch.google.com/ping/RPC2 - Success
http://ping.bitacoras.com - Success
http://ping.blo.gs/ - Success
http://ping.feedburner.com - Success
http://ping.syndic8.com/xmlrpc.php - Success
http://rpc.blogcatalog.com/ - Success
http://rpc.blogrolling.com/pinger/ - Success
http://ping.bloggers.jp/rpc/ - Success

Names
Emails
C:\My Feed.txt
Comments
C:\RSS Services.txt

**Status**

Success: 97
Failed: 0
List Status: 97/97

Incoming (kbps): 0000 Max: 2182
Outgoing (kbps): 0000 Max: 0385
Last operation took 1:43 minutes

Connections: 0 RSS Ping completed
Licensed and activated for ScrapeBox.com

*Figure 9 – A ScrapeBox Screenshot*

We explored one side of the comment spam attack – the attacker point of view. In the next section, we examine the other side – the victim's point of view. This provides us a better understanding of the essence of the attack, and the optional mitigations.

## 5. The Victim's Point of View

We observed a large amount of data in order to thoroughly understand the quantitative aspects of comment spam traffic. The data was collected through the real-time monitoring of attack data against more than 60 web applications. We focused on a period of two weeks, from September 1 to September 14 in 2013 and used different filters to leave only traffic that is clearly comment spam. We then analyzed the behavior of these attacks over time, and across targets. We also performed calculations of statistical properties of the malicious traffic.

We discovered that **most of the comment spam traffic originated from attackers who have been active for long periods, and attacked multiple targets**. To illustrate the exact relationship between the number of attacked targets per attack source, and the duration of the attacker's activity, we designed an "Attack-Source Reputation Quadrant" graph (See Figure 10. This graph was first introduced in a our previous HII[3]).

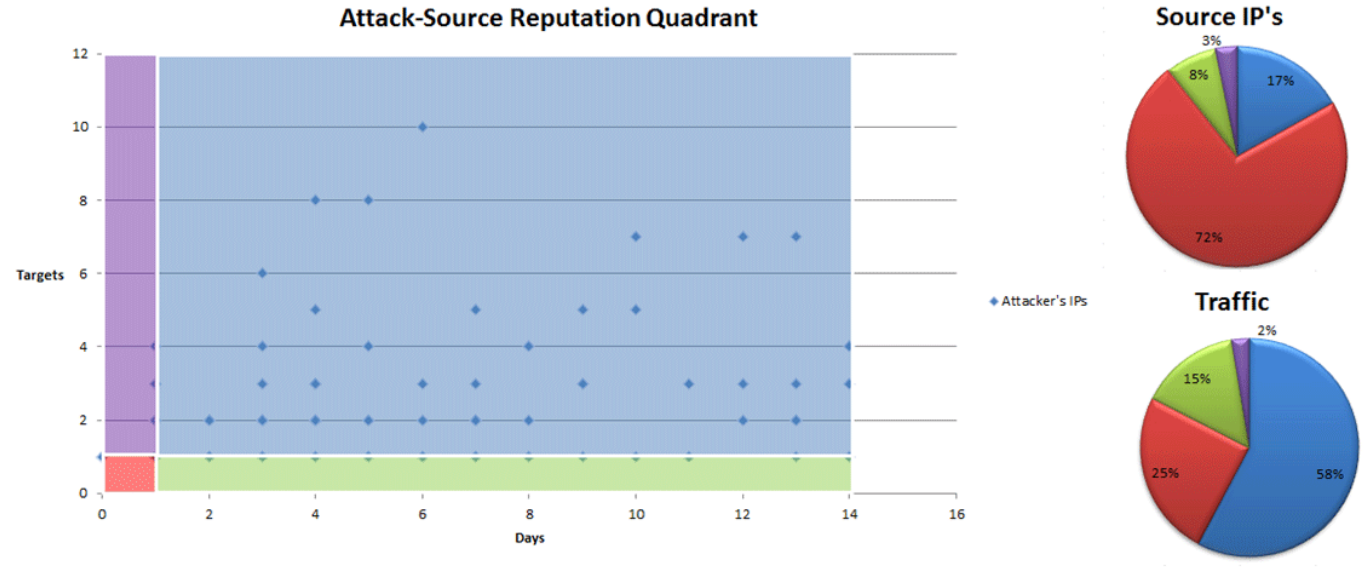


*Figure 10 – Attack Source Reputation Quadrant for Comment Spam*

In an "Attack-Source Reputation Quadrant" graph, the Y-axis represents the number of targets that were attacked, and the X-axis represents the duration of an attack. Accordingly, each dot in the graph represents an attack source and corresponds to the source's longevity and the number of targets it has attacked during the course of our analysis. To express the Attack-Source Reputation Quadrant as a graph, we added two more divisions. The first is a vertical line along the Y-axis which separates attack sources of those active only during a single day, from those active for more than a single day. The second is a horizontal line which similarly isolates attack sources that attacked only a single target from those that attacked multiple targets.

There are four different quadrants:

- The upper left quadrant (in purple) includes all attack sources that were active for only one day and attacked more than one target.
- The lower left corner (in red) includes all attack sources that were active for only one day and attacked only a single target.
- The upper right quadrant (in blue) includes all attack sources that were active for more than one day and attacked more than one target.
- The lower right quadrant (in green) includes all attack sources that were active for more than one day and attacked only a single target.

[3] http://www.imperva.com/resources/hacker_intelligence.asp

To quantify the data, we've enhanced the Attack-Source Reputation Quadrant with two pie-charts (color-coded to the quadrants, respectively):

- The top pie chart represents the percentage of attack sources, within each quadrant.
- The bottom pie chart represents the percentage of traffic, within each quadrant.

Figure 10 shows that most of the attackers (72 percent) are in the red zone, which means they were active only for a single day, and attacked only a single target. **Nonetheless, most of the comment spam traffic (58 percent) is in the blue zone, which means they were active more than one day, and attacked more than one target.**

We focused on the upper right quadrant (blue) and explored the traffic. **We discovered that a relatively small number of attackers are responsible for a large amount of the comment spam traffic.** Figure 11 shows the cumulative percentage of comment spam traffic from the attackers in the blue quadrant. The attackers are sorted by dominance: attacker #1 produced the highest number of attacks in the given period, etc.

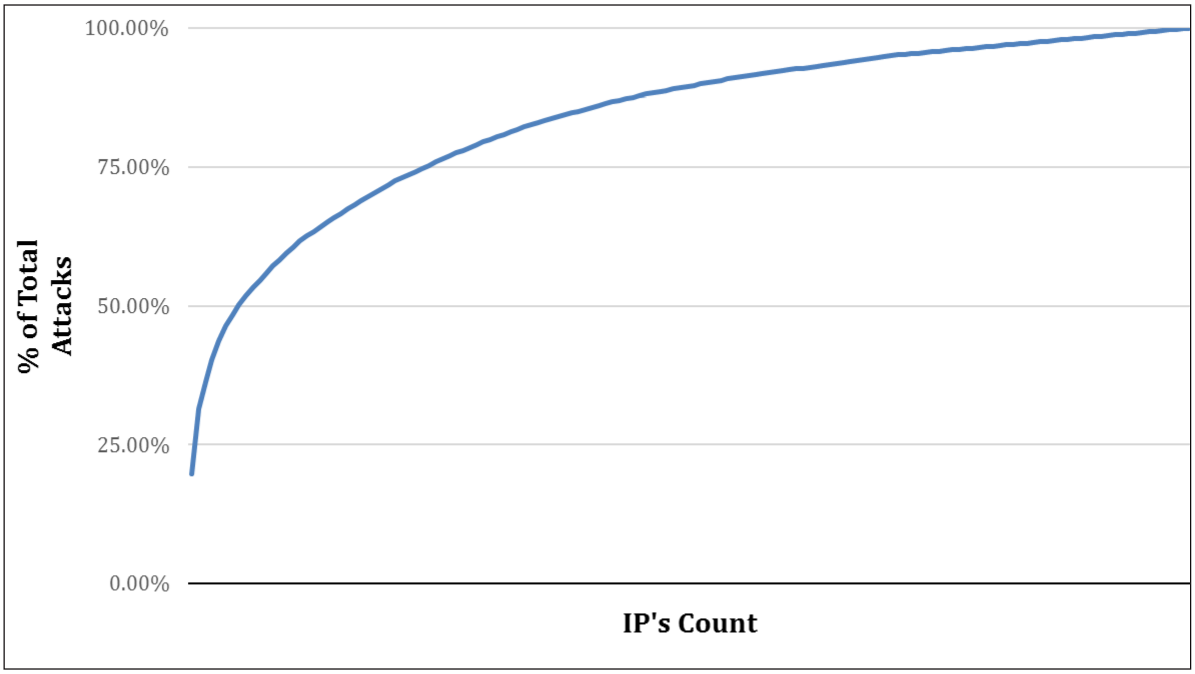


*Figure 11 – The Cumulative Percentage of Comment Spam Traffic*

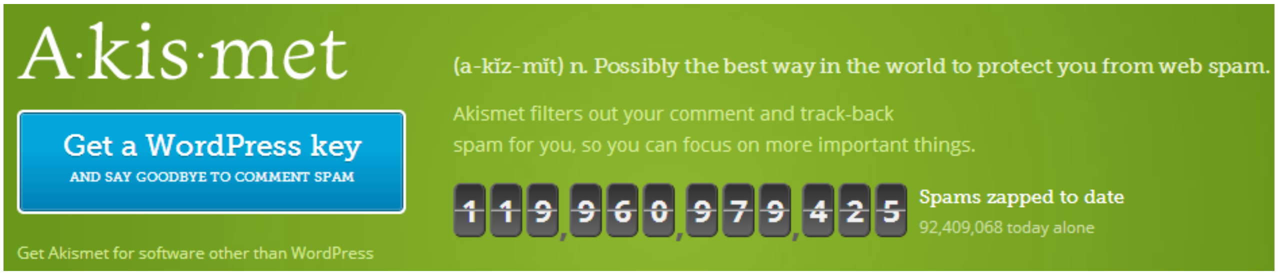
The graph shows that 80 percent of the comment spam traffic was generated by 28 percent of the attackers.

## 6. Mitigation Techniques

Websites can defend themselves against comment-spam attacks using a number of mitigation techniques. Following, are some of the popular ones at use today.

### 6.1 Content Inspection

The content inspection technique is based on inspecting the content of the posted comments, according to a predefined set of rules. Rules, for example, might be: too many links in one comment; logical sentences that are related to the subject at hand; and no duplicate comments. In such systems a tradeoff exists between false-positive and true-negative rates, depending on the rules definitions. Akismet[4] is a comment spam detection service that uses a combination of mitigation methods, among them the content based technique. When using it, each comment is sent to the Akismet servers. The servers check the received data, and return a true/false answer.



A·kis·met

(a-kĭz-mĭt) n. Possibly the best way in the world to protect you from web spam.

Akismet filters out your comment and track-back spam for you, so you can focus on more important things.

Get a WordPress key
AND SAY GOODBYE TO COMMENT SPAM
119,960,979,425
Spams zapped to date
92,409,068 today alone
Get Akismet for software other than WordPress

*Figure 12 – Akismet Moto*

Content based mitigation can rely on the reputation of the **hyperlinks** posted within the comments[5]. Once a link to a specific website appears in too many comments on the web, or in requests that are suspicious enough to be created using comment spam tools, the promoted website may gain a bad reputation. This reputation can be used to block comments containing these hyperlinks. "Penguin"[6] is a recent update to the Google search engine that uses this kind of information, and penalizes websites that are known to use comment spam tools.

### 6.2 Source Reputation

This mitigation technique is based on identifying whether a comment is spam according to the reputation of the poster. Source reputation is based on whether previously seen traffic from that source was considered comment spam. Online repositories, based on crowdsourcing, were set-up for these purposes. The repositories are used to both report spam and to check a comment source reputation. The two most popular repositories are www.projecthoneypots.org and www.stopforumspam.com. Our research found them rather reliable.

[4] http://www.akismet.com

[5] http://www.securelist.com/en/analysis/204792295/Redirects_in_Spam

[6] http://en.wikipedia.org/wiki/Google_Penguin

## 6.3 Anti-automation

Anti-automation techniques can be useful for comment spam mitigation, as automatic tools are frequently used to produce comment spam traffic. One simple option is adding a check box to indicate whether a user wishes to post a comment. Regularly changing the HTTP field name for this check box is useful against the more sophisticated tools. A more complex option is using the Captcha[7] mechanism. When using it, each comment post requires entering an obfuscated text displayed on the page.

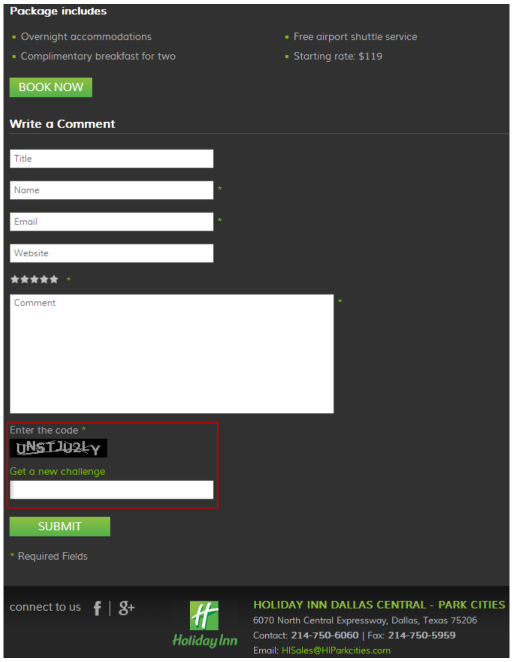

Package includes
▪ Overnight accommodations
▪ Complimentary breakfast for two
▪ Free airport shuttle service
▪ Starting rate: $119
BOOK NOW
Write a Comment
Title
Name *
Email *
Website
★★★★★ *
Comment *
Enter the code *
UNSTJU2LY
Get a new challenge
SUBMIT
* Required Fields
connect to us
Holiday Inn
HOLIDAY INN DALLAS CENTRAL - PARK CITIES
6070 North Central Expressway, Dallas, Texas 75206
Contact: 214-750-6060 | Fax: 214-750-5959
Email: HISales@HIParkcities.com

*Figure 13 – Captcha Challenge for Posting a Comment*

## 6.4 Demotivation

The demotivation technique strives to make comment spam useless. This can be achieved by the follow/nofollow value that can be assigned to the "rel" attribute of an HTML anchor (<A>) element which defines a hyperlink[8]. It specifies whether a link should be followed by the search engine's indexing algorithm. Setting the "nofollow" value for posted comments decreases the comment spam motivation. This is demonstrated in Figure 14.

```
<a rel="nofollow" href="http://www.bestCars.com">Best cars!</a>
```

Frameworks can use this value to demotivate comment spammers. For example, WordPress 1.5 and above automatically assigns the nofollow value to all user-submitted links[9]. Another example for demotivation is the Penguin[10] update to Google search engine algorithm that focuses on decreasing the search engine ranking of websites that are considered to use comment spam techniques.

## 6.5 Manual Inspection

Manual inspection is very effective for identifying comments as spam. Its primary drawback is its loss of scalability – as spam increases, manual inspection of it becomes impractical. This technique is effective against manual comment spam, due to the relatively small amount of spam that can be manually posted (and inspected).

[7] ttp://en.wikipedia.org/wiki/CAPTCHA
[8] http://en.wikipedia.org/wiki/Nofollow
[9] http://codex.wordpress.org/Nofollow
[10] http://en.wikipedia.org/wiki/Google_Penguin

# 7. Case studies

## 7.1 Analyzing a Single Victim

In order to better understand the comment spam attack pattern, we took a closer look at the spam traffic directed at a single victim. We chose one website that was receiving a great amount of comment spam traffic. It consists of a single host, with many URLs. The victim is a non-profit organization that supplies information and supports a community of users. We gathered data over a period of one month, that produced 384 events from September 1st to September 30th 2013.

We discovered a high diversity in the volume of comment spam traffic for different pages. Our theory associates **popular phrases within the URL address and page content, to the attack rate**. We documented attacks on 119 URLs. Figure 15 shows the number of events for each URL in descending order, i.e. URL one received the highest number of events, and so on.

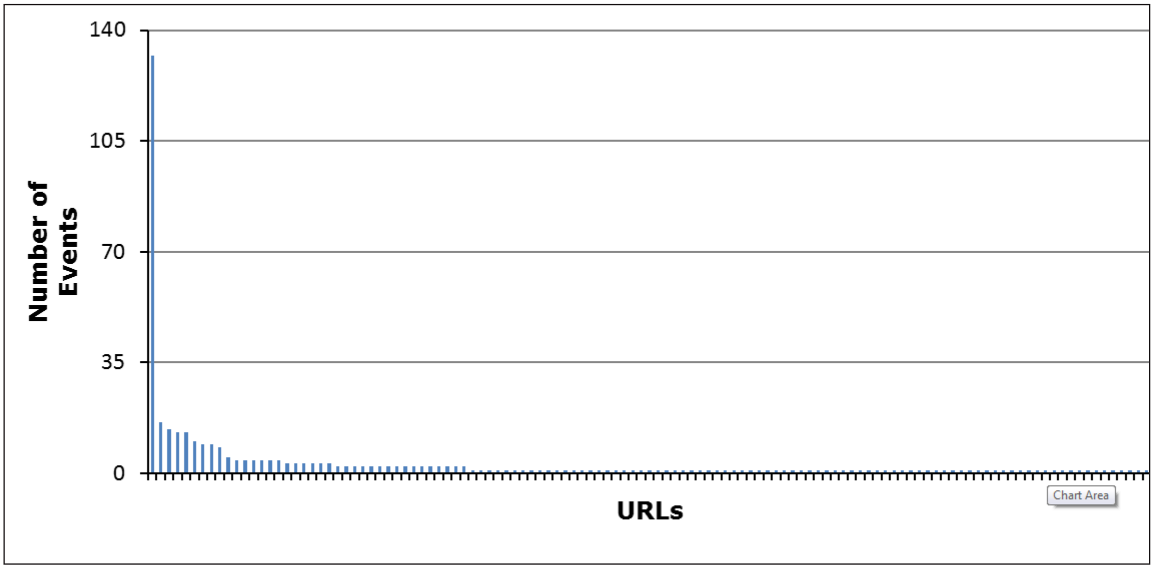


*Figure 15 – URL Popularity Graph*

The graph shows that target one had significantly suffered more comment spam compared to the other targets on that same host. It had approximately 10 times more events compared to the next URL in order. A potential explanation can be that target one contains the popular phrase 'weight gain' in its URL address which draws comment spam attackers. This phrase appears frequently within the page such as "causes of weight gain" and "How can this weight gain be prevented".

We discovered that **a small number of sources produced most of the traffic**. Figure 16 shows the cumulative percentage of comment spam traffic generated by source IPs, to the target, at hand.

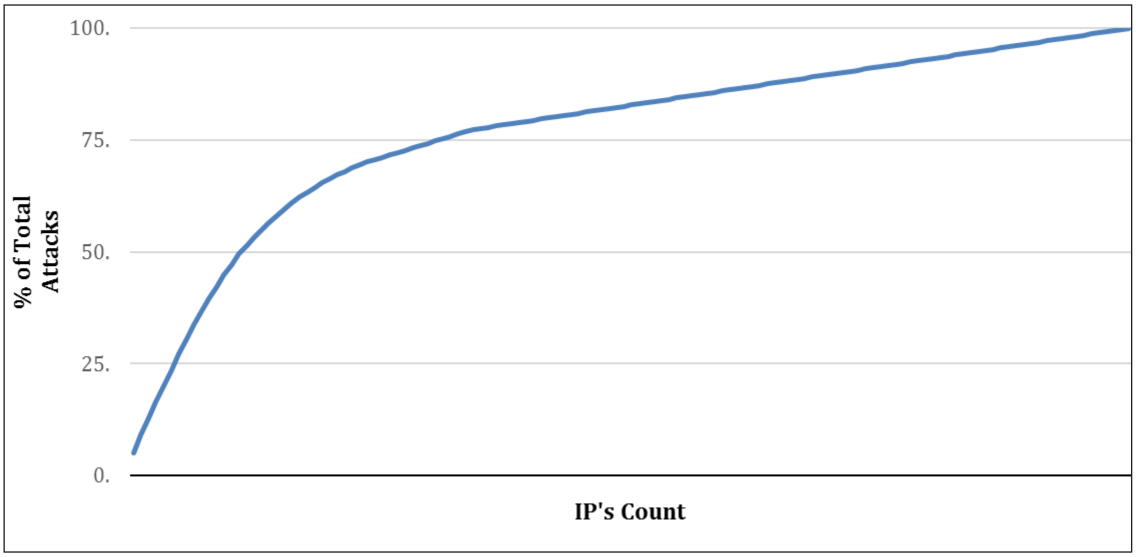


*Figure 16 – The Cumulative Percentage of Comment Spam Traffic to a Single Target*

We can see in Figure 16, 52 percent of source IPs produce approximately 80 percent of the traffic.

### 7.2 Analyzing a Single Attacker

In order to thoroughly understand the comment spam traffic we focused on a highly active attacker, and examined both its traffic quantitative and qualitative aspects.

We discovered that the attacker was active for a long period. We identified 61 HTTP requests as comment spam during a period of two weeks. Figure 17 shows the number of requests the attacker sent each day, during those two weeks.

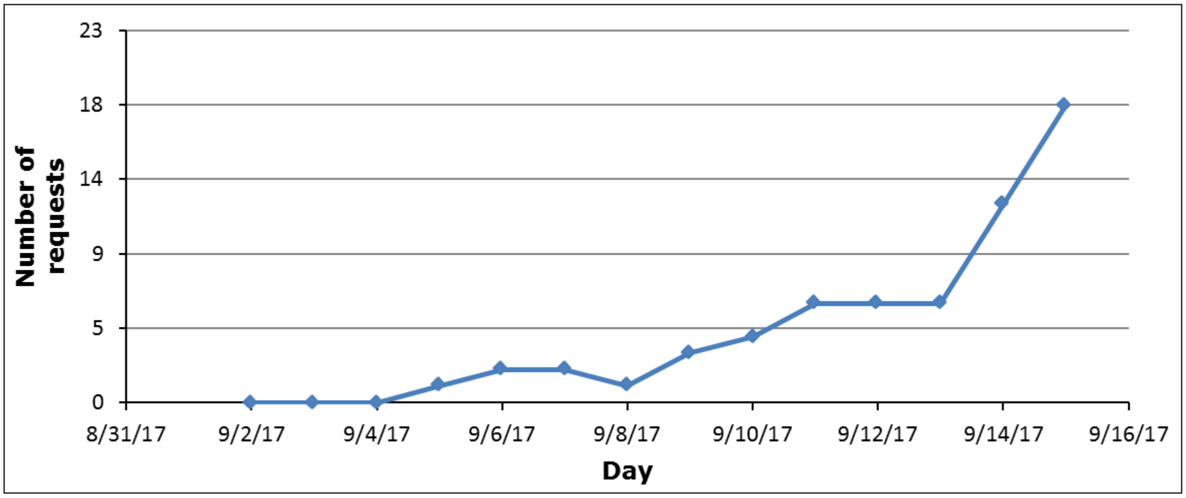


*Figure 17 – Requests per Day for a Single Attacker*

The attacker was active for ten days and the number of requests per day had increased during the period. **Identifying this attacker as a comment spammer early, and blocking its requests, would have prevented most of its traffic.**

The attacker had **a few targets, and most of them suffered a relative high amount of comment spam attacks.** The investigated data included 61 events targeting five different websites. Figure 18 shows the percentage of the traffic received by each target.

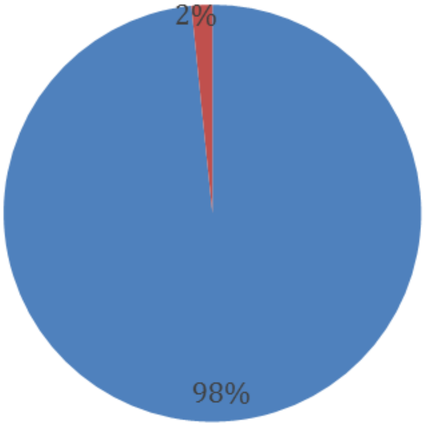
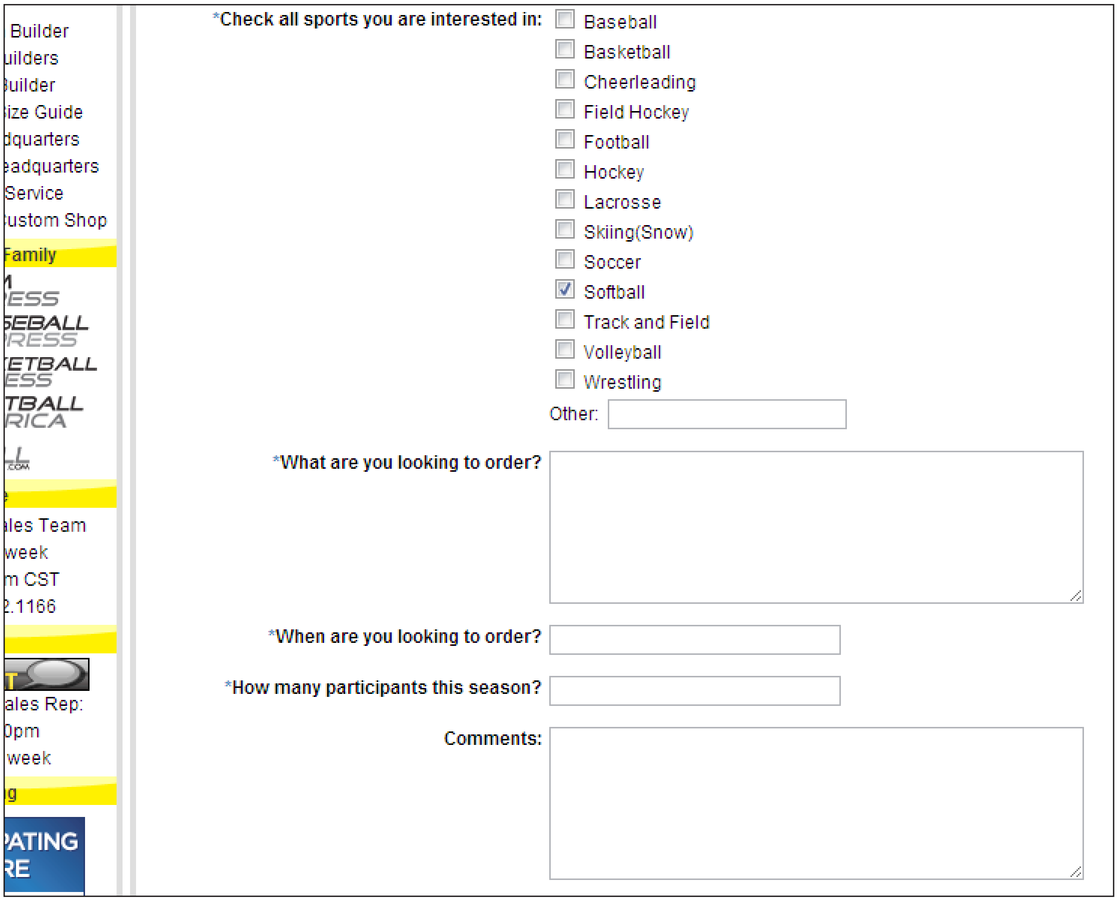


*Figure 18 – Percentage of Traffic per Target*

As shown in Figure 18, most of the targets received roughly, an even portion of the traffic (except from target five). In addition, once the attacker attacked a certain target, it was likely to attack it again, in the following days. For example, the attacks on target two have spanned over eight days, of the two week period.

The automated tool uses **input parameters with no reassurance they are being publicly available on the site**. Figure 19 shows a screenshot of a targeted page. The attacker's target was the "comments" field, however the comments are for an order being made, and will not be published on the site. We believe this happens due to lack of verification by the automated tools – they harvest targets with a "comment" parameter, and do not verify that the value is actually being published on the site.



*Check all sports you are interested in:
☐ Baseball
☐ Basketball
☐ Cheerleading
☐ Field Hockey
☐ Football
☐ Hockey
☐ Lacrosse
☐ Skiing(Snow)
☐ Soccer
☑ Softball
☐ Track and Field
☐ Volleyball
☐ Wrestling
Other:

*What are you looking to order?

*When are you looking to order?

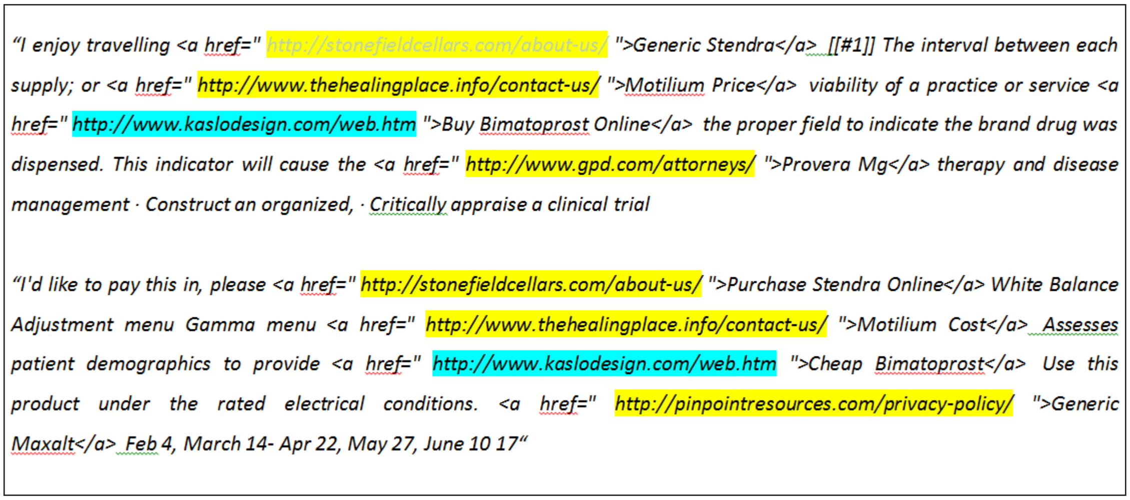
*How many participants this season?

Comments:

*Figure 19 – A Comment Spam Target*

We analyzed the content of comments and learned the **hyperlinks in a single request are for different sites and consecutive requests have similar hyperlinks**. The requests produced by the tool will hold comments containing different websites to promote. Those comments will be restructured in consecutive requests, in order to avoid defense mechanisms. In the case at hand, the attacker sent 48 requests containing seven different URLs. The comments have a basic reoccurring structure: *<simple sentence> <hyperlink>*

**Error! Reference source not found.** shows two comments, for example, that hold eight URLs, with five unique values.



*“I enjoy travelling <a href=" http://stonefieldcellars.com/about-us/ ">Generic Stendra</a> [[#1]] The interval between each supply; or <a href=" http://www.thehealingplace.info/contact-us/ ">Motilium Price</a> viability of a practice or service <a href=" http://www.kaslodesign.com/web.htm ">Buy Bimatoprost Online</a> the proper field to indicate the brand drug was dispensed. This indicator will cause the <a href=" http://www.gpd.com/attorneys/ ">Provera Mg</a> therapy and disease management · Construct an organized, · Critically appraise a clinical trial*

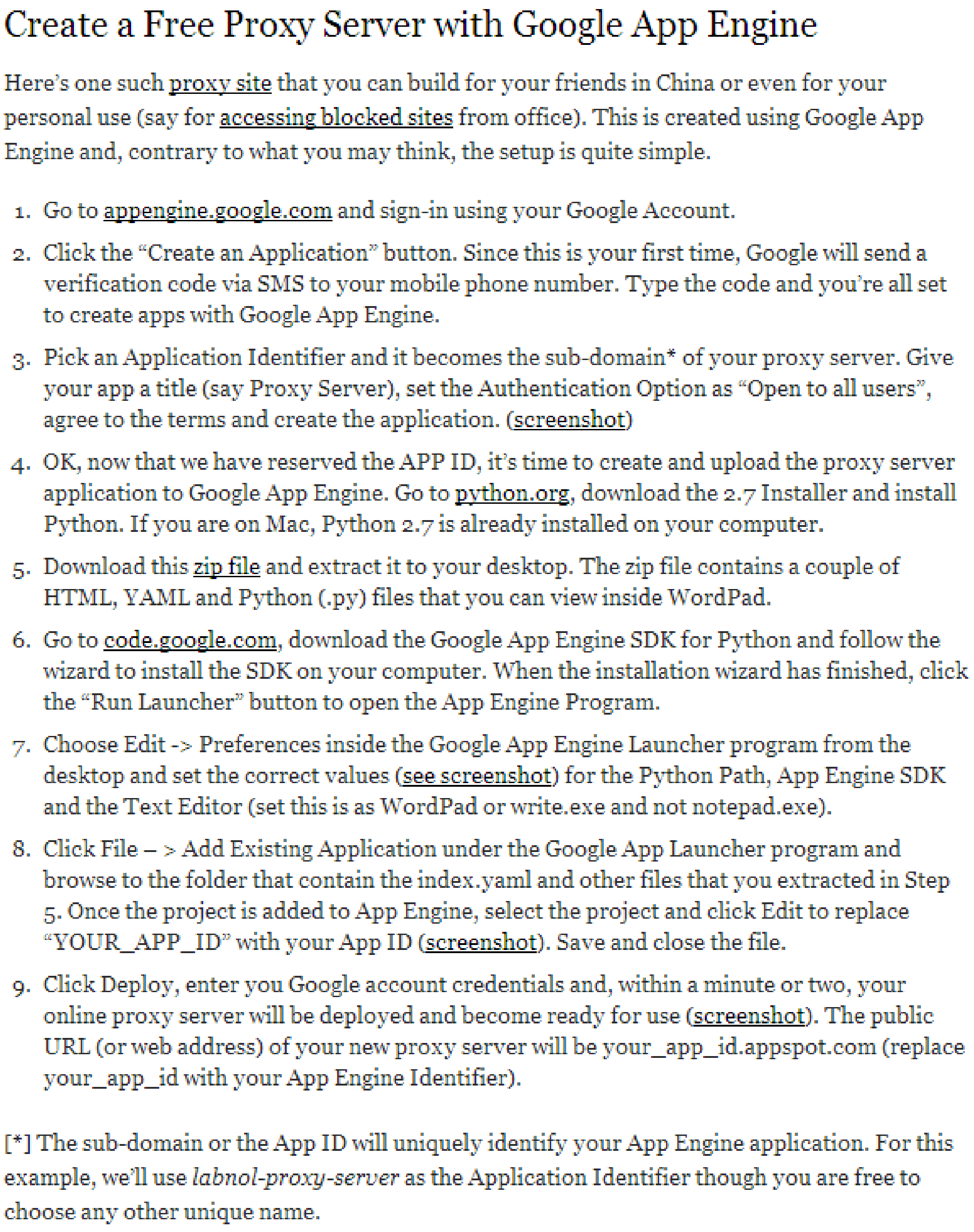
*“I'd like to pay this in, please <a href=" http://stonefieldcellars.com/about-us/ ">Purchase Stendra Online</a> White Balance Adjustment menu Gamma menu <a href=" http://www.thehealingplace.info/contact-us/ ">Motilium Cost</a> Assesses patient demographics to provide <a href=" http://www.kaslodesign.com/web.htm ">Cheap Bimatoprost</a> Use this product under the rated electrical conditions. <a href=" http://pinpointresources.com/privacy-policy/ ">Generic Maxalt</a> Feb 4, March 14- Apr 22, May 27, June 10 17“*

*Figure 20 – Examples of Comments*

When feeding them to a browser, we saw that six of them lead to the same website of a pharmaceutical company (marked in yellow). The other two URLs (marked in blue) belong to another website. Using these URLs as jumping boards, prevents the promoted websites from gaining a bad reputation from using comment spam tools, and avoids having identical comments (see Section 6: Mitigation Techniques).

### 7.3 Attackers Abuse Google App Engine for Comment Spam

The "Google App Engine"[11] is a service provided by Google, which allows users to run web applications on Google's infrastructure. One especially easy-to-create application is a web proxy, which can be used to generate comment spam traffic. Figure 21[12] shows a series of simple steps for creating a proxy using the Google App Engine.



Create a Free Proxy Server with Google App Engine

Here's one such proxy site that you can build for your friends in China or even for your personal use (say for accessing blocked sites from office). This is created using Google App Engine and, contrary to what you may think, the setup is quite simple.

1. Go to appengine.google.com and sign-in using your Google Account.
2. Click the "Create an Application" button. Since this is your first time, Google will send a verification code via SMS to your mobile phone number. Type the code and you're all set to create apps with Google App Engine.
3. Pick an Application Identifier and it becomes the sub-domain* of your proxy server. Give your app a title (say Proxy Server), set the Authentication Option as "Open to all users", agree to the terms and create the application. (screenshot)
4. OK, now that we have reserved the APP ID, it's time to create and upload the proxy server application to Google App Engine. Go to python.org, download the 2.7 Installer and install Python. If you are on Mac, Python 2.7 is already installed on your computer.
5. Download this zip file and extract it to your desktop. The zip file contains a couple of HTML, YAML and Python (.py) files that you can view inside WordPad.
6. Go to code.google.com, download the Google App Engine SDK for Python and follow the wizard to install the SDK on your computer. When the installation wizard has finished, click the "Run Launcher" button to open the App Engine Program.
7. Choose Edit -> Preferences inside the Google App Engine Launcher program from the desktop and set the correct values (see screenshot) for the Python Path, App Engine SDK and the Text Editor (set this is as WordPad or write.exe and not notepad.exe).
8. Click File – > Add Existing Application under the Google App Launcher program and browse to the folder that contain the index.yaml and other files that you extracted in Step 5. Once the project is added to App Engine, select the project and click Edit to replace "YOUR_APP_ID" with your App ID (screenshot). Save and close the file.
9. Click Deploy, enter you Google account credentials and, within a minute or two, your online proxy server will be deployed and become ready for use (screenshot). The public URL (or web address) of your new proxy server will be your_app_id.appspot.com (replace your_app_id with your App Engine Identifier).

[*] The sub-domain or the App ID will uniquely identify your App Engine application. For this example, we'll use *labnol-proxy-server* as the Application Identifier though you are free to choose any other unique name.

*Figure 21 – Steps to Turn Google App Engine into a Proxy*

[11] https://developers.google.com/appengine/docs/whatisgoogleappengine

[12] http://www.labnol.org/internet/setup-proxy-server/12890/

In our research, we monitored a list of IP addresses known to generate comment spam. The most dominant IP in the group was an address registered to Google App Engine.

This technique is used by spammers to bypass reputation controls based on IP addresses, since most often addresses of Google App Engine (and those of other cloud services) are explicitly whitelisted. In fact, in our own data set, we are able to identify legitimate traffic from the same IP address which belongs to a different application (for example the "feedly" application[13]). A more careful inspection of the request structure revealed that an application ID (appID) is specified in the HTTP user-agent field – probably inserted by App Engine infrastructure.

## 8. Summary and conclusions

Studying the comment spam space from both ends, and taking into account all existing mitigation techniques, we have come to the following conclusions:

- Identifying the attacker as a comment spammer early on and blocking its requests prevents most of the malicious activity.
- IP reputation will help in solving the comment spam problem, by blocking comment spammers early on in their attack campaigns

As of April 2014, Imperva offers a Comment Spam IP reputation feed through its ThreatRadar services, to help customers mitigate the comment spam problem.

[13] http://cloud.feedly.com/#welcome

## Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of Imperva's Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, Web application security and cyber-crime business models with the goal of improving security controls and risk management processes.

**Imperva**
3400 Bridge Parkway, Suite 200
Redwood City, CA 94065

Tel: +1-650-345-9000
Fax: +1-650-345-9004
www.imperva.com