

# Wordpress Comment, Referrer and Ghost Spam: How to Track Down Spammers

Don Tai [dontai.com/wp/](http://dontai.com/wp/)  
October 15 2016

# Talking Points

- Overview: Comment, Referrer, and Ghost Spam
- Why is Spam Bad
- Tools Used:
  - Akismet plugin, reCapcha plugin
  - Learn: Raw access log
  - Search: Whois.com: public IP information
  - Learn: CIDR IP notation
- Demo: trace WP comment spam to access log, ban
  - Dual IP Spam: How to trick akismet spam filter
- Hierarchy of Site Security
- Demo: Referrer Spam/Bad Bot Behaviour: Identify, ban
- Google Analytics and Ghost Spam

# Overview of Website of Spam

1. Comment Spam: Hits your site
  - where: Admin > comments > spam folder
  - where: access log
  - results in Google Search if not managed
2. Referrer Spam: Hits your site, not in WP Admin
  - where: access log
  - see it in Google Analytics
3. Ghost Spam: Spammer does not visit your site
  - where: not in WP Admin or access log
  - see it in Google Analytics

# Why Spam is Bad

- **Why Kill Spam**
  - Clutters your site, unwanted links, unprofessional look
- **Why prevent Spam**
  - spend less time deleting comment spam
  - skews Google Search and Analytics
  - wastes bandwidth, server resources
- **Site Security Concerns**
  - security risk: spammers try to crack your security, site, plugins

# Tools Used

- Akismet plugin, reCapcha plugin
  - Isolates spam from site, does not stop it
- Learn: Raw access log
- Search: Whois.com: public IP information
- Learn: CIDR IP notation
  - Classless Inter-Domain Routing
  - 192.16.1.0 – 192.168.1.255 > 192.168.1.0/24
  - 192.16.0.0 – 192.168.255.255 > 192.168.1.0/16

# Raw Access Log

- What is it, where to find yours?
  - Important web site forensic tool: daily, cumulative monthly
  - Available for Shared service, ISP: cpanel
  - Not available from wordpress.com
- Download, unzip, import access log into spreadsheet
- The columns of the access log
  - Ip/host name, date-time, action done, result code, bytes transferred, referrer, user agent
  - Ex: Don, yesterday evening, drive to Chinese store to buy moon cake, success, gas used/moon cake cost, came from home, Honda Fit
- How do I use it?

# Access Log: Columns

	A	B	C	D	E	F	G
1	192-227-161-54-host.colocrossing.com	[12/Sep/2016:06:00:24	GET /wp/2009/03/14/squirrel-acrobatics/ HTTP/1.1	403	637	http://dontai.com/wp/2009/03/14/squirrel-acroba	Mozilla/5.0 (Windows; U; Window
2	crawl811.us.archive.org	[12/Sep/2016:06:00:35	GET /wp/wp-json/oembed/1.0/embed?url=http%3A%2F	200	2559	http://dontai.com/wp/2012/02/21/interview-quest	Mozilla/5.0 (compatible; special
3	185.158.135.134	[12/Sep/2016:06:01:24	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41429	http://dontai.com/	Mozilla/5.0 (Windows NT 6.1; WC
4	185.158.135.134	[12/Sep/2016:06:01:26	GET /wp/wp-login.php HTTP/1.0	200	2566	http://dontai.com/	Opera/9.80 (Windows NT 6.2; Wi
5	185.158.135.134	[12/Sep/2016:06:01:27	GET /wp/wp-login.php HTTP/1.0	200	2566	http://dontai.com/wp/wp-login.php	Opera/9.80 (Windows NT 6.2; Wi
6	185.158.135.134	[12/Sep/2016:06:01:27	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41429	http://dontai.com/	Opera/9.80 (Windows NT 6.2; Wi
7	185.158.135.134	[12/Sep/2016:06:02:44	POST /wp/wp-comments-post.php HTTP/1.1	302	-	http://dontai.com/wp/2012/07/08/ripstik-mechani	Opera/9.80 (Windows NT 6.2; Wi
8	185.158.135.134	[12/Sep/2016:06:02:45	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41600	http://dontai.com/wp/wp-comments-post.php	Opera/9.80 (Windows NT 6.2; Wi
9	185.158.135.134	[12/Sep/2016:06:02:47	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41428	-	Opera/9.80 (Windows NT 6.2; Wi
10	114.72.198.172	[12/Sep/2016:06:03:01	GET /wp/wp-content/uploads/2013/03/winter-snow-4-6	200	###	https://www.bing.com/	Mozilla/5.0 (Windows NT 10.0; W
11	b110076.yse.yahoo.net	[12/Sep/2016:06:03:30	GET /wp/tag/durometer/ HTTP/1.1	200	22787	-	Mozilla/5.0 (compatible; Yahoo! S
12	baiduspider-180-76-15-161.crawl.baidu	[12/Sep/2016:06:03:34	GET /wp/tag/t-testing-fvds-ru/ HTTP/1.1	200	23255	-	Mozilla/5.0 (compatible; Baidusp
13	crawl-66-249-65-58.googlebot.com	[11/Sep/2016:16:54:26	GET /wp/wp-content/themes/default-enhanced/images	200	33810	-	Googlebot-Image/1.0
14	b110076.yse.yahoo.net	[11/Sep/2016:16:54:41	GET /wp/tag/tetra-pack/ HTTP/1.1	200	22755	-	Mozilla/5.0 (compatible; Yahoo! S
15	86-125-223-230.rdsnet.ro	[11/Sep/2016:16:55:14	GET /wp/2009/03/09/female-cochineal-beetle-and-your	200	54786	http://dontai.com/wp/2009/03/09/female-cochine	Mozilla/4.0 (compatible; MSIE 8.
16	86-125-223-230.rdsnet.ro	[11/Sep/2016:16:55:23	POST /wp/wp-comments-post.php HTTP/1.1	302	-	http://dontai.com	Mozilla/4.0 (compatible; MSIE 8.
17	b110076.yse.yahoo.net	[11/Sep/2016:16:55:29	GET /wp/?p=3057&buy-deltasone-no-prescription HTT	301	-	-	Mozilla/5.0 (compatible; Yahoo! S
18	b110076.yse.yahoo.net	[11/Sep/2016:16:55:36	GET /wp/2010/09/21/jiucal-growing-at-our-front-doorste	200	27677	-	Mozilla/5.0 (compatible; Yahoo! S
19	ec2-54-175-100-106.compute-1.amazo	[11/Sep/2016:16:55:57	GET /wp/2010/08/22/inexpensive-rola-bola-lots-of-fun	403	637	-	Mozilla/5.0 (Windows NT 6.0; WC
20	157.55.39.248	[16/Sep/2016:22:01:28	GET /wp/tag/china/page/8/ HTTP/1.1	200	51409	-	Mozilla/5.0 (compatible; bingbot/
21	205.234.203.78	[16/Sep/2016:22:01:45	GET /wp/2015/05/04/ubuntu-14-04-and-android-studio	200	47999	http://dontai.com/wp/2015/05/04/ubuntu-14-04-a	Mozilla/5.0 (Windows; U; Window
22	205.234.203.78	[16/Sep/2016:22:01:48	POST /wp/wp-comments-post.php HTTP/1.1	302	-	http://dontai.com	Mozilla/5.0 (Windows; U; Window
23	180.76.15.24	[16/Sep/2016:22:01:51	GET /wp/category/retail/page/5/ HTTP/1.1	200	49357	-	Mozilla/5.0 (compatible; Baidusp
24							
25							
26							
27							
28							
29							
30							
31							
32							

# Demo: WP Comment Spam

- Find a spam entry in Admin > comments > Spam
  - Find identical spam transaction in access log
  - Check log for dual IP spammer
  - Search Whois.com, find their IP range
  - Ban ip using htaccess, WP-Ban
    - Ban as little as possible, but enough
- # Digital Energy UK 185.158.132.0 – 185.158.135.255  
deny from 185.158.135.0/24 86.125.223.0/24



- Dashboard
- Posts
- Media
- Links
- Pages
- Comments 71**
- Appearance
- Plugins
- Users
- Tools
- Settings
- Insights
- Collapse menu

# Comments

Screen Options Help

All (793) | Pending (71) | Approved (722) | Spam (3) | Trash (0)

Search Comments

Bulk Actions Apply All comment types Filter Empty Spam 3 items

<input type="checkbox"/>	Author	Comment	In Response To	Submitted On
<input type="checkbox"/>	<b>Virtual Reality Games in Los Angeles</b> <a href="#">service-ok.svyaznoy.ru/bitrix/rk.php?goto=http://...</a> x <a href="#">manuelaannand@gmx.de</a> 185.158.135.134	It's an awesome post in favor of all the web people; they will obtain advantage from it I am sure.	<b>Ripstik Mechanical Maintenance: Overview</b> <a href="#">View Post</a> 2	2016/09/12 at 5:02 am
<input type="checkbox"/>	<b>Fast Weight Loss</b> <a href="#">tinyurl.com/mgl7gpb</a> x <a href="#">Vandeman@gmail.com</a> 86.125.223.230	The Zune concentrates on being a Portable Media Player. Not a web browser. Not a game machine. Maybe in the future it'll do even better in those areas, but for now it's a fantastic way to organize and listen to your music and videos, and is without peer in that regard. The iPod's strengths are its web browsing and apps. If those sound more compelling, perhaps it is your best choice.	<b>Female Cochineal Beetle and your Food</b> <a href="#">View Post</a> 18 3	2016/09/11 at 3:55 pm
<input type="checkbox"/>	<b>www.resourceaddictio</b>	Check if you have a throid disorder.	<b>Heat Rash</b>	2016/09/11 at



Liberation Sans

10



%

0.000

0.000



A7

f(x) Σ =

185.158.135.134

	A	B	C	D	E	
1	192-227-161-54-host.colocrossing.com	[12/Sep/2016:06:00:24	GET /wp/2009/03/14/squirrel-acrobatics/ HTTP/1.1	403	637	http://
2	crawl811.us.archive.org	[12/Sep/2016:06:00:35	GET /wp/wp-json/oembed/1.0/embed?url=http%3A%2F	200	2559	http://
3	185.158.135.134	[12/Sep/2016:06:01:24	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41429	http://
4	185.158.135.134	[12/Sep/2016:06:01:26	GET /wp/wp-login.php HTTP/1.0	200	2566	http://
5	185.158.135.134	[12/Sep/2016:06:01:27	GET /wp/wp-login.php HTTP/1.0	200	2566	http://
6	185.158.135.134	[12/Sep/2016:06:01:27	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41429	http://
7	185.158.135.134	[12/Sep/2016:06:02:44	POST /wp/wp-comments-post.php HTTP/1.1	302	-	http://
8	185.158.135.134	[12/Sep/2016:06:02:45	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41600	http://
9	185.158.135.134	[12/Sep/2016:06:02:47	GET /wp/2012/07/08/ripstik-mechanical-maintenance-c	200	41428	-
10	114.72.198.172	[12/Sep/2016:06:03:01	GET /wp/wp-content/uploads/2013/03/winter-snow-4-60	200	###	https:
11	b110076.yse.yahoo.net	[12/Sep/2016:06:03:30	GET /wp/tag/durometer/ HTTP/1.1	200	22787	-
12	baiduspider-180-76-15-161.crawl.baidu	[12/Sep/2016:06:03:34	GET /wp/tag/t-testing-fvds-ru/ HTTP/1.1	200	23255	-
13	crawl-66-249-65-58.googlebot.com	[11/Sep/2016:16:54:26	GET /wp/wp-content/themes/default-enhanced/images	200	33810	-
14	b110076.yse.yahoo.net	[11/Sep/2016:16:54:41	GET /wp/tag/tetra-pack/ HTTP/1.1	200	22755	-
15	86-125-223-230.rdsnet.ro	[11/Sep/2016:16:55:14	GET /wp/2009/03/09/female-cochineal-beetle-and-your	200	54786	http://
16	86-125-223-230.rdsnet.ro	[11/Sep/2016:16:55:23	POST /wp/wp-comments-post.php HTTP/1.1	302	-	http://
17	b110076.yse.yahoo.net	[11/Sep/2016:16:55:29	GET /wp/?p=3057&buy-deltasone-no-prescription HTTP	301	-	-
18	b110076.yse.yahoo.net	[11/Sep/2016:16:55:36	GET /wp/2010/09/21/jiucai-growing-at-our-front-doorste	200	27677	-
19	ec2-54-175-100-106.compute-1.amazo	[11/Sep/2016:16:55:57	GET /wp/2010/08/22/inexpensive-rola-bola-lots-of-fun/	403	637	-
20	157.55.39.248	[16/Sep/2016:22:01:28	GET /wp/tag/china/page/8/ HTTP/1.1	200	51409	-
21	205.234.203.78	[16/Sep/2016:22:01:45	GET /wp/2015/05/04/ubuntu-14-04-and-android-studio-i	200	47999	http://
22	205.234.203.78	[16/Sep/2016:22:01:48	POST /wp/wp-comments-post.php HTTP/1.1	302	-	http://
23	180.76.15.24	[16/Sep/2016:22:01:51	GET /wp/category/retail/page/5/ HTTP/1.1	200	49357	-
24						
25						
26						
27						
28						




# IP Ban Strategy

- Spammer's Naughty IP: 86.125.223.230
- Immediate Ban: 86.125.223.0/24 (256 addresses in last octet)
- Whois Lookup:
  - 86.125.216.0 - 86.125.223.255
  - netname: RO-RCS-RDS, RCS & RDS Residential
  - Secondary Ban range: 86.125.216.0/21 (1,792 Ips)
- Ban their ISP
  - 86.120.0.0 – 86.127.255.255
  - Third Ban range: 86.120.0.0/13 (462,336 IPs)
  - descr: RDSNET
  - Could try contacting their ISP
- Ballistic Ban Strategy: Find all Ips owned by RO-RCS-RDS, ban them

# WP Admin: IP Dual Comment Spam

WordPress Admin Dashboard for Don Tai (Canada) Blog. Security points: 97/115. User: Howdy, dontai.

regards to this particular topic, forced me to in my view ponder over it out of numerous numerous sides. The just like males and females aren't fascinated until it can be related to Lady gaga! Your individual things spectacular. Continually tackle that!

Comment Status	Profile	Text	Post Title	Time
<input type="checkbox"/>	 <a href="http://www.taragupta.in">www.taragupta.in</a> taragupta.in x Neumiller@gmail.com 47.29.14.72	<a href="http://www.taragupta.in">http://www.taragupta.in</a> http://www.taragupta.in I am high class independent <a href="#">Tara Gupta</a> <a href="http://www.taragupta.in">http://www.taragupta.in</a> Delhi escorts model provide 24/7, My name is tara gupta and i am hot sexy delhi escorts call me now.	<a href="#">Ruby Chinese Restaurant: The Good and the Bad</a> View Post	2016/10/07 at 12:09 pm
<input checked="" type="checkbox"/>	 <b>Delhi Escorts</b> taragupta.in x Semenick@gmail.com 47.29.75.55	<a href="http://www.taragupta.in">http://www.taragupta.in</a> http://www.taragupta.in I am high class independent <a href="#">Tara Gupta</a> <a href="http://www.taragupta.in">http://www.taragupta.in</a> Delhi escorts model provide 24/7, My name is tara gupta and i am hot sexy delhi escorts call me now.	<a href="#">Toronto and Ontario Laws on Snow Removal</a> View Post	2016/10/07 at 12:07 pm
<input checked="" type="checkbox"/>	 <a href="http://www.taragupta.in">www.taragupta.in</a> taragupta.in x	<a href="http://www.taragupta.in">http://www.taragupta.in</a> http://www.taragupta.in I am high class independent <a href="#">Tara Gupta</a> <a href="http://www.taragupta.in">http://www.taragupta.in</a> Delhi escorts model provide 24/7, My name is tara gupta and i am hot sexy delhi	<a href="#">Repairing my leaky Suncast Hose Reel</a> View Post	2016/10/07 at 11:09 am

# Access Log: Dual IP Comment Spam

207.46.13.55	[07/Oct/2016:13:07:26	GET /wp/2010/08/18/banning-kite-flying-in-toront	200	42938	-
192.243.55.129	[07/Oct/2016:13:07:32	GET /wp?lumigan-for-sale&p=3707 HTTP/1.1	500	-	-
207.35.163.162	[07/Oct/2016:13:08:22	GET /wp/wp-content/uploads/2012/07/Toronto-E	200	###	<a href="http://www.bing.com/image">http://www.bing.com/image</a>
207.35.163.162	[07/Oct/2016:13:08:22	GET /wp/wp-content/uploads/2012/07/Toronto-E	200	###	<a href="http://www.bing.com/image">http://www.bing.com/image</a>
180.76.15.160	[07/Oct/2016:13:08:28	GET /wp/tag/charter-of-rights/ HTTP/1.1	200	29377	-
66.249.65.56	[07/Oct/2016:13:09:04	GET /wp/2013/10/05/ikea-aventuria-halogen-cei	200	27988	-
203.124.29.64	[07/Oct/2016:13:09:05	GET /wp/wp-content/uploads/2016/02/presto-pr	200	###	-
192.243.55.130	[07/Oct/2016:13:09:06	GET /wp/2010/09/21/looking-for-ryan-wright-mo	500	-	-
47.29.116.88	[07/Oct/2016:13:09:16	GET /wp/2009/10/10/ruby-chinese-restaurant-th	200	36598	<a href="http://dontai.com">http://dontai.com</a>
47.29.14.72	[07/Oct/2016:13:09:20	POST /wp/wp-comments-post.php HTTP/1.1	302	-	<a href="http://dontai.com">http://dontai.com</a>
163.150.129.55	[07/Oct/2016:13:09:21	GET /wp/wp-content/uploads/2009/11/DSC0161	200	###	<a href="https://www.google.com/">https://www.google.com/</a>
47.29.18.198	[07/Oct/2016:13:09:22	GET /wp/2009/10/10/ruby-chinese-restaurant-th	200	36678	<a href="http://dontai.com">http://dontai.com</a>
68.180.229.111	[07/Oct/2016:13:09:49	GET /prettybuttoner/tag/marvel/ HTTP/1.1	200	26249	-
70.28.245.79	[07/Oct/2016:13:09:52	GET /wp/wp-content/uploads/2016/05/briggs-str	403	635	<a href="https://www.google.ca/">https://www.google.ca/</a>
142.26.99.72	[07/Oct/2016:13:10:31	GET /wp/wp-content/uploads/2009/02/missouri	200	62886	<a href="https://www.google.ca/">https://www.google.ca/</a>
180.76.15.145	[07/Oct/2016:13:11:19	GET /wp/2009/09/14/richmond-hill-live-steamer	200	20497	-
14.207.225.206	[07/Oct/2016:13:11:32	GET /wp/wp-content/uploads/2010/10/Ant-color	200	49980	<a href="https://www.google.co.th/">https://www.google.co.th/</a>
47.29.120.14	[07/Oct/2016:13:11:33	GET /wp/2011/05/14/whom-the-gods-wish-to-de	200	25403	<a href="http://dontai.com">http://dontai.com</a>

# Hierarchy of Site Security

- Priority
  - Attempt to break into site: POST /wp-login
  - Look for security loopholes in WP core, plugins, server, odd URLs, other
  - Comment spam
  - Referrer spam
- Secondary
  - Wasting server resources, bandwidth > ISP might shut down your site
  - Content scraping
  - Hotlinking to your images
  - Ghost spam

# Demo: Referrer Spam/Bad Bot Behaviour

- Look in your Access Log for suspicious referrer entries, ban
  - RewriteCond %{HTTP\_REFERER} ^http://.\*pornogig [OR]
  - RewriteCond %{HTTP\_REFERER} ^http://.\***buttons-for-website** [OR]
  - **Do not go to referrer sites with a browser, you'll get malware**
- Suspicious User Agent: ban
  - RewriteCond %{HTTP\_USER\_AGENT} ^.\*sysomos [NC,OR]
  - RewriteCond %{HTTP\_USER\_AGENT} ^.\*kodomia [NC,OR]
- Look for Bad behaviour, then ban IP
  - Document and Ban
    - larger range provides more protection, more collateral damage (inadvertently ban users near this ip address)
    - smaller range provides less protection, less collateral damage

# Access Log: Referrer Spam

111.47.171.57	[07/Apr/2016:09:32:34	GET /wp/2009/02/09/monster-ne	301	-	<a href="http://businessfields.ru/jokes/45.html">http://businessfields.ru/jokes/45.html</a>	Mozill
111.47.171.57	[07/Apr/2016:09:32:41	GET /reasoned.php HTTP/1.1	200	9410	<a href="http://businessfields.ru/jokes/45.html">http://businessfields.ru/jokes/45.html</a>	Mozill
ec2-52-53-219-173.us-west-1.compute.a	[07/Apr/2016:09:33:32	GET /reasoned.php HTTP/1.1	200	9369	<a href="http://businessfields.ru/jokes/45.html">http://businessfields.ru/jokes/45.html</a>	Mozill
177-2-85-220.3g.brasiltelecom.net.br	[27/Apr/2016:11:26:05	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
177-2-85-220.3g.brasiltelecom.net.br	[27/Apr/2016:11:26:06	GET /root/ HTTP/1.1	200	11242	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
187-13-181-82.user.veloxzone.com.br	[22/Apr/2016:17:07:31	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
187-13-181-82.user.veloxzone.com.br	[22/Apr/2016:17:07:32	GET /root/ HTTP/1.1	200	11228	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
191.249.9.151.dynamic.adsl.gvt.net.br	[18/Apr/2016:12:17:21	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
191.249.9.151.dynamic.adsl.gvt.net.br	[18/Apr/2016:12:17:22	GET /root/ HTTP/1.1	200	41170	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
196.21.236.5	[21/Apr/2016:04:24:47	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
196.21.236.5	[21/Apr/2016:04:24:48	GET /root/ HTTP/1.1	200	40967	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
203.215.117.85	[11/Apr/2016:03:27:06	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
203.215.117.85	[11/Apr/2016:03:27:07	GET /root/ HTTP/1.1	200	42939	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
250.pool92-177-96.dynamic.orange.es	[23/Apr/2016:08:27:11	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
250.pool92-177-96.dynamic.orange.es	[23/Apr/2016:08:27:12	GET /root/ HTTP/1.1	200	41202	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
78-187-162.adsl.cyta.gr	[22/Apr/2016:08:20:40	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
78-187-162.adsl.cyta.gr	[22/Apr/2016:08:20:40	GET /root/ HTTP/1.1	200	41185	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
93-40-201-145.ip40.fastwebnet.it	[25/Apr/2016:14:58:32	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
93-40-201-145.ip40.fastwebnet.it	[25/Apr/2016:14:58:33	GET /root/ HTTP/1.1	200	11242	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
b39f48a8.virtua.com.br	[19/Apr/2016:17:33:35	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
b39f48a8.virtua.com.br	[19/Apr/2016:17:33:35	GET /root/ HTTP/1.1	200	41204	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
porta78.shop-le-biscuit.as28624.oops.ne	[20/Apr/2016:12:05:33	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
porta78.shop-le-biscuit.as28624.oops.ne	[20/Apr/2016:12:05:35	GET /root/ HTTP/1.1	200	41103	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
static-wan-bl3-198-90.rev.webside.pt	[08/Apr/2016:10:48:09	GET / HTTP/1.1	301	231	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
static-wan-bl3-198-90.rev.webside.pt	[08/Apr/2016:10:48:10	GET /root/ HTTP/1.1	200	11558	<a href="http://buttons-for-website.com">http://buttons-for-website.com</a>	Mozill
176-8-91-153-lvv.broadband.kyivstar.net	[21/Apr/2016:15:46:22	GET /wp/tag/awstats/ HTTP/1.1	500	-	<a href="http://buutranelun.wordpress.com">http://buutranelun.wordpress.com</a>	Mozill
107.151.152.210	[05/Apr/2016:03:35:45	GET /reasoned.php HTTP/1.1	200	9334	<a href="http://buycheapsildenafil.net/">http://buycheapsildenafil.net/</a>	Mozill
107.151.152.210	[05/Apr/2016:03:35:45	GET /wp/tag/awstats/ HTTP/1.1	301	-	<a href="http://buycheapsildenafil.net/">http://buycheapsildenafil.net/</a>	Mozill



# Google Analytics: Referrer Spam

<input type="checkbox"/>	Source <sup>?</sup>	Acquisition			Behavior
		Sessions <sup>?</sup>	% New Sessions <sup>?</sup>	New Users <sup>?</sup>	Bounce Rate <sup>?</sup> ↓
		2,844 % of Total: 4.80% (59,269)	46.03% Avg for View: 73.47% (-37.35%)	1,309 % of Total: 3.01% (43,542)	26.65% Avg for View: 30.00% (-11.15%)
<input type="checkbox"/>	1. 173.194.44.2	1 (0.04%)	100.00%	1 (0.08%)	100.00%
<input type="checkbox"/>	2. akademie.medio.cz	1 (0.04%)	100.00%	1 (0.08%)	100.00%
<input type="checkbox"/>	3. alexa.com	1 (0.04%)	100.00%	1 (0.08%)	100.00%
<input type="checkbox"/>	4. allmetrics.ru	1 (0.04%)	100.00%	1 (0.08%)	100.00%
<input type="checkbox"/>	5. app.yaware.com.ua	1 (0.04%)	100.00%	1 (0.08%)	100.00%
<input type="checkbox"/>	6. blog.commercialtribe.com	1 (0.04%)	0.00%	0 (0.00%)	100.00%
<input type="checkbox"/>	7. buttons-for-website.com	29 (1.02%)	100.00%	29 (2.22%)	100.00%

# Access Log: User Agents

204.112.53.31	[25/Sep/2016:1	GET /wp/wp-content/uploads/2	200	91944	http://dontai.com/wp/2010/06/03/	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML
204.112.53.31	[25/Sep/2016:1	GET /wp/wp-includes/js/wp-en	200	10414	http://dontai.com/wp/2010/06/03/	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML
204.112.53.31	[25/Sep/2016:1	GET /wp/wp-content/themes/d	200	846	http://dontai.com/wp/wp-content/t	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML
204.112.53.31	[25/Sep/2016:1	GET /favicon.ico HTTP/1.1	200	894	http://dontai.com/wp/2010/06/03/	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML
204.112.53.31	[25/Sep/2016:1	GET /wp/wp-content/themes/d	200	894	http://dontai.com/wp/2010/06/03/	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML
204.12.255.130	[26/Sep/2016:0	GET //wp/wp-login.php HTTP/	500	-	-	-
204.194.29.4	[26/Sep/2016:0	GET /root/comment/reply/58/	200	33243	http://dontai.com/root/comment/re	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gec
204.194.29.4	[26/Sep/2016:0	POST /root/comment/reply/58/	200	33645	http://dontai.com/root/comment/re	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0
204.237.81.150	[25/Sep/2016:2	GET /images/cb125sShemCly	200	###	https://www.google.ca/	Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
204.80.187.229	[25/Sep/2016:1	GET /wp/wp-content/uploads/2	200	###	https://www.bing.com/	Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
205.139.141.54	[25/Sep/2016:0	GET /root/rss.xml HTTP/1.1	500	-	-	Mozilla/5.0 (compatible; Sysomos/1.0; +http://www.sysomos.com/; Sysomos)
205.139.141.54	[25/Sep/2016:1	GET /wp/feed HTTP/1.1	500	-	-	Mozilla/5.0 (compatible; Sysomos/1.0; +http://www.sysomos.com/; Sysomos)
205.139.141.54	[25/Sep/2016:1	GET /wp/feed HTTP/1.1	500	-	-	Mozilla/5.0 (compatible; Sysomos/1.0; +http://www.sysomos.com/; Sysomos)
206.190.34.200	[25/Sep/2016:0	GET /wp/wp-content/uploads/2	200	56682	http://in.images.search.yahoo.cor	YahooCacheSystem: YahooWebServiceClient
206.217.142.135	[25/Sep/2016:1	GET /root/comment/reply/51	403	638	http://dontai.com/	Mozilla/5.0 (X11; Linux i686; rv:17.0) Gecko/20100101 Firefox/17.0
206.217.142.135	[25/Sep/2016:1	GET / HTTP/1.1	403	638	http://dontai.com	Mozilla/5.0 (X11; Linux i686; rv:17.0) Gecko/20100101 Firefox/17.0
206.25.68.217	[25/Sep/2016:0	GET /wp/ HTTP/1.1	500	-	-	GridBot/1.0 crawler@sysomos.com
206.25.68.218	[25/Sep/2016:1	GET /wp/ HTTP/1.1	500	-	-	GridBot/1.0 crawler@sysomos.com
207.102.138.158	[25/Sep/2016:2	GET /prettybuttoner/ HTTP/1.	301	-	http://prettybuttoner.com/	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrc
207.102.138.158	[25/Sep/2016:2	GET /prettybuttoner/ HTTP/1.	200	56255	http://prettybuttoner.com/	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrc
207.182.140.210	[26/Sep/2016:0	GET / HTTP/1.1	301	231	-	M
207.182.140.210	[26/Sep/2016:0	GET /root/ HTTP/1.1	200	11057	http://www.dontai.com/	M
207.182.140.213	[26/Sep/2016:0	GET / HTTP/1.1	301	231	-	Mozilla/5.0 (Windows NT 6.1; Win64; x64; +http://www.komodia.com/newwiki/in
207.182.140.214	[26/Sep/2016:0	GET /root/ HTTP/1.1	200	41190	-	Mozilla/5.0 (Windows NT 6.1; Win64; x64; +http://www.komodia.com/newwiki/in
207.210.45.238	[25/Sep/2016:1	GET /wp/wp-content/uploads/2	200	47125	https://www.google.ca/	Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG SM-G920W8 Build/MMB29K) App
207.210.45.238	[25/Sep/2016:1	GET /wp/wp-content/uploads/2	200	47125	https://www.google.ca/	Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG SM-G920W8 Build/MMB29K) App
207.46.13.0	[25/Sep/2016:1	GET /wp/2012/04/21/xubuntu-	301	-	-	Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
207.46.13.113	[26/Sep/2016:0	GET /wp/2009/12/10/when-you	200	30233	-	Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
207.46.13.113	[26/Sep/2016:0	GET /wp/2009/12/10/when-you	200	30233	-	Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)

# Access Log: Login Attempts

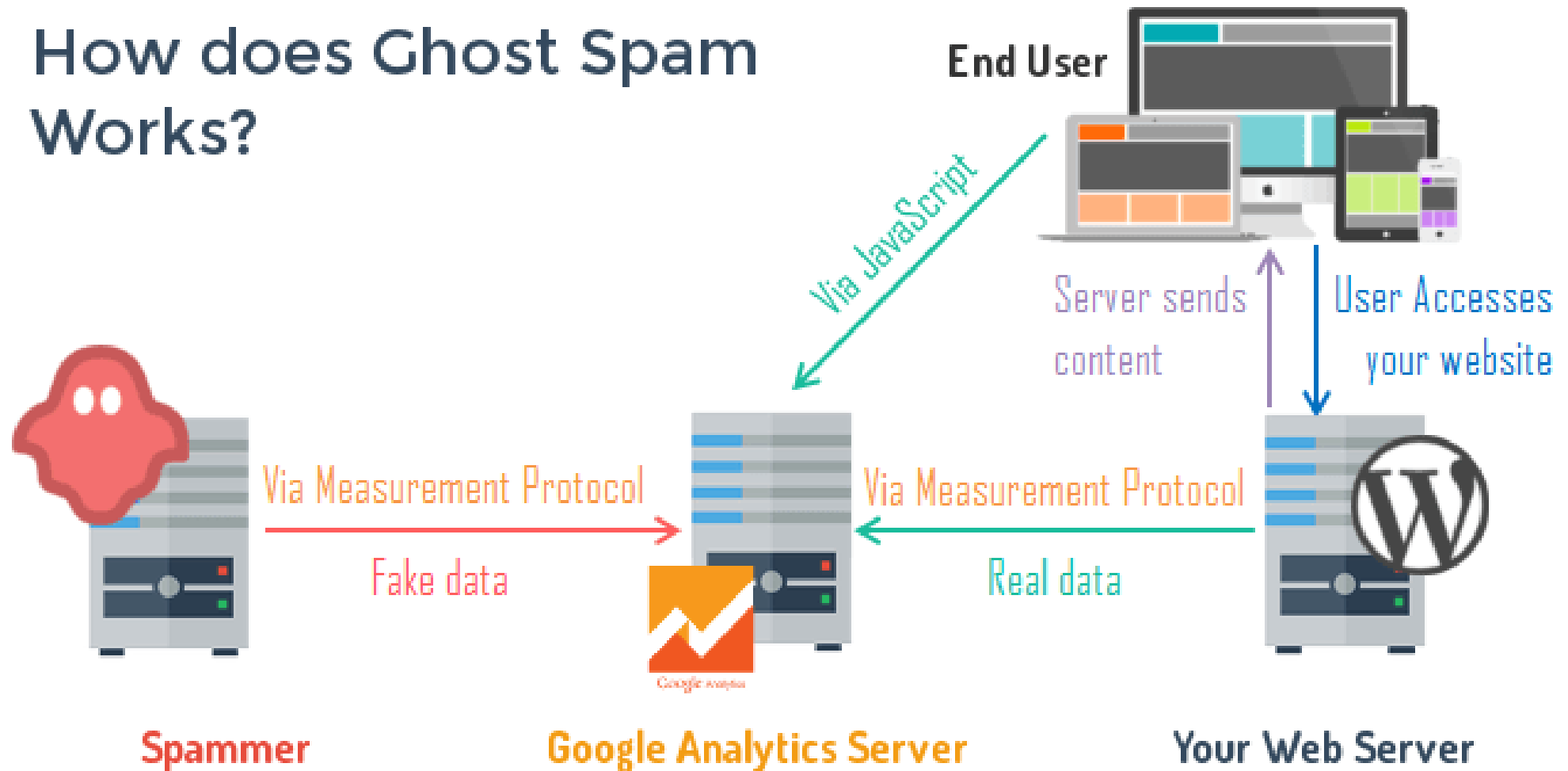
182.71.210.86	[22/Sep/2016:19:56:11	POST /wp/wp-login.php HTTP/1.0	200	3430	-
182.71.210.86	[22/Sep/2016:19:56:13	POST /wp/wp-login.php HTTP/1.0	200	3430	-
182.71.210.86	[22/Sep/2016:19:56:14	POST /wp/wp-login.php HTTP/1.0	200	3430	-
182.71.210.86	[22/Sep/2016:19:56:17	POST /wp/wp-login.php HTTP/1.0	404	-	-
220.178.107.242	[22/Sep/2016:19:56:18	POST /wp/wp-login.php HTTP/1.0	301	-	-
31.214.152.205	[22/Sep/2016:19:57:12	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:14	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:15	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:17	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:18	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:19	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:20	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:21	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:23	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:24	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:26	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:27	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:28	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:29	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:31	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:32	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:33	POST /wp/wp-login.php HTTP/1.0	200	3478	-
31.214.152.205	[22/Sep/2016:19:57:34	POST /wp/wp-login.php HTTP/1.0	200	3478	-
61.190.214.186	[22/Sep/2016:19:56:39	POST /wp/wp-login.php HTTP/1.0	200	3478	-
61.190.214.186	[22/Sep/2016:19:56:41	POST /wp/wp-login.php HTTP/1.0	200	3478	-
61.190.214.186	[22/Sep/2016:19:56:42	POST /wp/wp-login.php HTTP/1.0	200	3478	-
61.190.214.186	[22/Sep/2016:19:56:44	POST /wp/wp-login.php HTTP/1.0	200	3478	-
61.190.214.186	[22/Sep/2016:19:56:46	POST /wp/wp-login.php HTTP/1.0	200	3478	-
61.190.214.186	[22/Sep/2016:19:56:48	POST /wp/wp-login.php HTTP/1.0	200	3478	-

# Access Log: Looking for Security Loopholes

50.87.15.217	[17/Sep/2016:11:34:16	POST /xmlrpc-activate.php HTTP/1.1	403
50.87.15.217	[17/Sep/2016:11:34:16	POST /wp-load.php HTTP/1.1	404 -
171.113.86.214	[21/Sep/2016:07:19:08	POST /wp-content/uploads/ftp.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:08	POST /wp-admin/js/edit.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:09	POST /wp-admin/newfile.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:09	POST /wp-content/themes/inline/edit.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:09	POST /wp-includes/css/log.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:10	POST /wp-includes/theme-compat/qiaoqua.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:10	POST /wp-content/themes/light/log.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:19:12	POST /wp-includes/images/wlwlog.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:56	POST /admin.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:57	POST /admin.php/module/action/param1/\${@eval(\$_POST[c]	500 -
171.113.86.214	[21/Sep/2016:07:59:57	POST /admin/admin.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:57	POST /admin/appeal.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:57	POST /admin/Databackup/1.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:58	POST /admin/Databackup/admin.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:58	POST /admin/Databackup/com6.ss.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:58	POST /admin/upclass/ift0_img.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:07:59:59	POST /admin\\Databackup\\admin.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:25	POST /editor/ckeditor/news_bak.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:26	POST /editor/css/office/ban_ner.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:26	POST /editor/images/ban_ner.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:27	POST /Editor/xheditor/emot/default/11.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:35	POST /fckeditor/editor/c_admin.asp HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:35	POST /FCKeditor/Files/file/asp.asp/keio.jpg HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:36	POST /FCKupload/20141112082052.php HTTP/1.1	500 -
171.113.86.214	[21/Sep/2016:08:00:36	POST /fckupload/image/ift0_img.asp HTTP/1.1	500 -

# Google Analytics and Ghost Spam

## How does Ghost Spam Works?



# Future Trends

- Ban Lists for referrer, UA, Ips: easily outdated, can slow down your site
- Spammers will come up with new and wonderful methods
- Look for Spam growth in: Middle East, Africa, S America, SE Asia/Indonesia

# References

- Image: referrer spam:
  - <https://www.optimizesmart.com/geek-guide-removing-referrer-spam-google-analytics/>
- Image: ghost spam
  - <https://moz.com/blog/stop-ghost-spam-in-google-analytics-with-one-filter>
- CIDR:  
[https://en.wikipedia.org/wiki/Classless\\_Inter-Domain\\_Routing](https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

Encourage your friends to publish,  
ban those who harm you

Questions?