Following the tracks

Understanding snowshoe spam

Image source: wikipedia.org

War on spam…

- Decline of “botnet” driven spam over the past 12 months

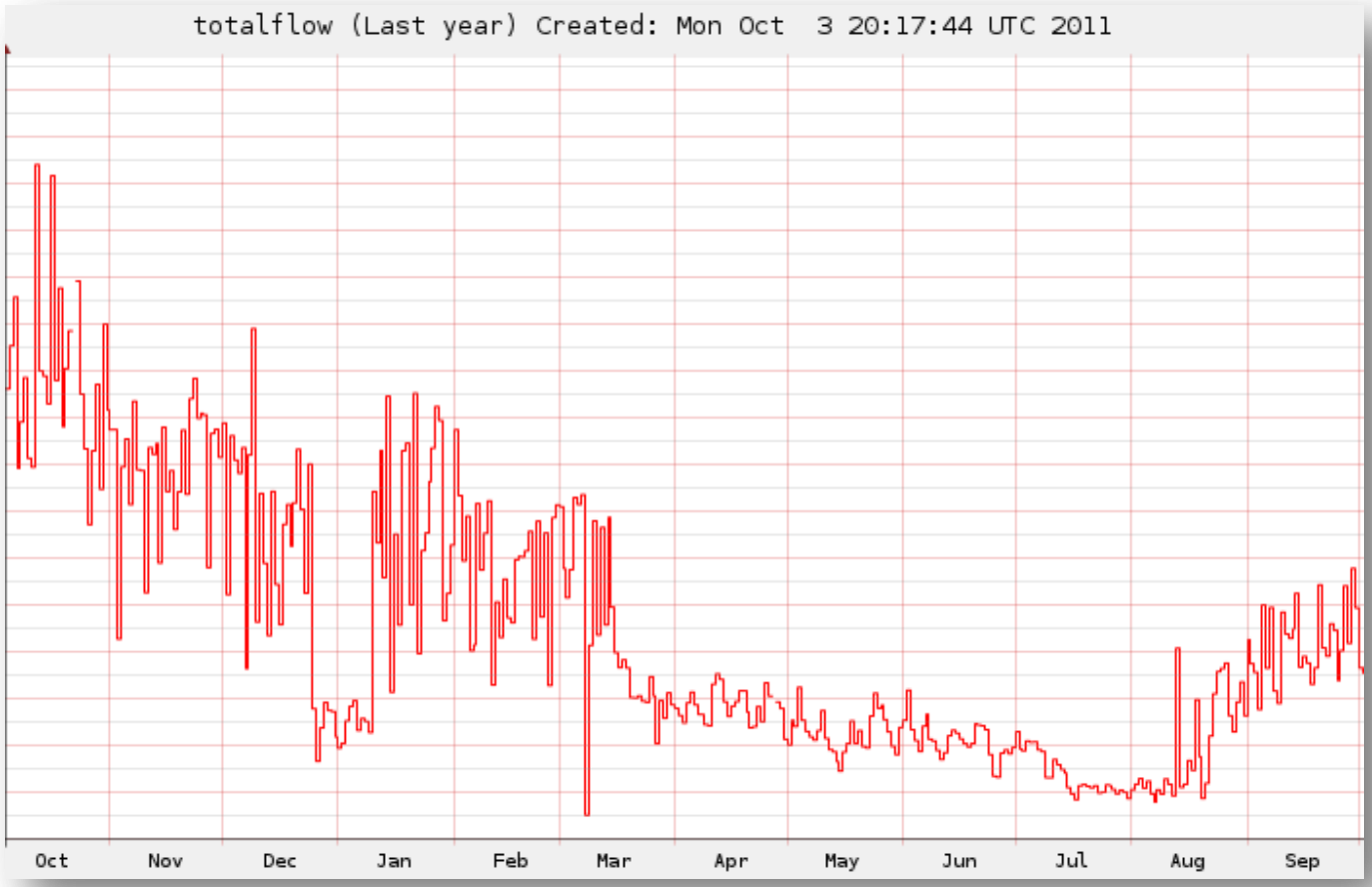


Image source: cbl.abuseat.org

bcove; Our Records Indicate You Have Cash On Hold

--Congratulations Add to contacts
To bcove@hotmail.com

Always show content from www.eyifirio.didifi@www.eyifirio.didifi.ma

bcove@hotmail.com:

Your New $1500 check May Have Been

You've received $900 Cash deposited

AM Payday

You can get a Cash Advance in as little as 1 HOUR*!

Choose an Amount Below or

$300.00

$500.00

$750.00

No Faxing R
qualified a

Bob Need a laptop? Get a new Colours Skin MacBook

Colours Laptop Add to contacts
To Bob

For a Limited Time Only, Get a FREE MacBook

TRY IT, TEST IT, KEEP IT!

For a Limited Time Only get a FREE MacBook
PLUS Colours MacBook Skin by DecalGirl.

Participation required. See Below for Details.

CONTINUE

- 2.26GHz Intel Core 2 Duo
- 2GB DDR3 memory
- 250GB hard drive
- 8x double-layer SuperDrive
- NVIDIA GeForce 9400M graphics

myelectronics-depot.net

To unsubscribe from future advertisements from MyElectronics-Depot.net, go to:
http://MyElectronics-Depot.net/u.cgi?config=6809

123 Click, Inc. P.O. Box 5225 Harrisburg, PA 17110

SUMMARY OF PROGRAM REQUIREMENTS. To receive the reward you must: 1) be a Canadian resident at least 18 years of age or older; 2) register with valid information; 3) complete the following reward offers: 2 Silver offers, 2 Gold offers, and 4 Platinum offers (Available reward offers will vary. Some reward offers require a purchase. Credit card offers may require you to activate the card by making a purchase, transferring a balance or taking a cash advance.) 4) refer 2 unique households that also complete the program requirements; and 5) follow the redemption instructions. All program requirements must be completed within 60 days of the date of registration. Please visit our website to read the complete Terms & Conditions.

MyElectronics-Depot.net is an independent rewards program for consumers and is not affiliated with, sponsored by or endorsed by any of the listed products or retailers. Trademarks, service marks, logos, and/or domain names (including, without limitation, the individual names of products and retailers) are the property of their respective owners.

Copyright © 2011 MyElectronics-Depot.net, a 123 Click, Inc. website.

All rights reserved.

Enroll now at - . University . of . Phoenix.

Classes- Add to contacts
otmail.com

ow content from ntag.mlsop.q4@hopm.wsq5.com

edge with a degree from University of Phoenix
bcove@hotmail.com
iversity of Phoenix - Important - Please Read!

niversity of Phoenix®

a real-world education
real-world faculty.

Create a better future.

With small class sizes, and personalized support, University of Phoenix can help you gain the

ty of Phoenix, we offer higher education that's more than

$1500....Confirmation needed for cash delivery....Click Here!

to contacts

212@fsdsdf.net

nation needed for cash delivery

e Cash
ed FAST!

GET CASH NOW >>

APPLY NOW!

2 Simple Steps
1. Fill out quick application
2. See if you qualify

Bad Credit OK
Security Ensured

Get Up To $1,500!*
Quick Approval

Direct Deposit
Confidential

Fast Advance America is your best resource for quick cash loans. Have Unexpected Bills? No Problem. Need some extra cash for the weekend? No Problem. Get up to $1,500* for whatever you need by filling out this quick, secure application.

FastAdvanceAmerica

If you do not wish to receive these emails, you may at any time unsubscribe by clicking the link here
or by sending a copy of this message to: Sandusky, LLC, 3315 Hwy 50, Silver Springs, Nevada 89429.

You May Qualify For A Grant-Go Back To School

CUSA.University.Directory Add to contacts
To bcove@hotmail.com

Always show content from sus29@contentowners.net

You May Qualify For A Grant - Go Ba

Mothers Go Back To School

Grant Funding May Be Available if you qualify!

Return to School on Your Schedule!

You may qualify for grants and scholarships
or a financial aid package which can help you return to school.

SEE DEGREES NOW

You are receiving this daily newsletter because you
Email was submitted to the cashwithoutinvest.com Newslet
If you do not wish to continue receiving email newsletter
cashwithoutinvest.com Click Stop this email.
To Opt out by postal mail, please include your email ad
Power Segment , 15774 South Lagrange Road,221,Orland Pa

ure correspondence and ads.

f Term Life Coverage for less than $

Protect The Future
Of Your Family With
Life Insurance Today

Free Quote

The future is uncertain, but the fate of your family doesn't have to be. Life insurance allows you the comfort and peace of mind that comes with knowing your loved ones will be taken care of. Termfinder provides life insurance quotes at no cost so that you can find the plan that fits you and the ones you love.

Fill out our short form to get a quote. It's that easy!

Start Now!

To unsubscribe please go here
or write us at:
P.O. Box 2654
Kirkland, WA 98083

You are receiving this daily newsletter because your
Email was submitted to the suppliesproviders.com Newsletter service.
If you do not wish to continue receiving email newsletters from
suppliesproviders.com Click Stop this email
To Opt out by postal mail, please include your email address:
Commercial Reviewers , 4651 BABCOCK ST NE UNIT 18,106,
PALM BAY,FL,32905

CAN-SPAM Act of 2003

- Functional unsubscribe
- Postal address
- No forged headers
- No sending to harvested addresses
- Send via your own network

Spammer’s Dilemma

CANSPAM
Compliance

Sustainable
Deliverability

CANSPAM?

CANSPAM REQUIREMENTS

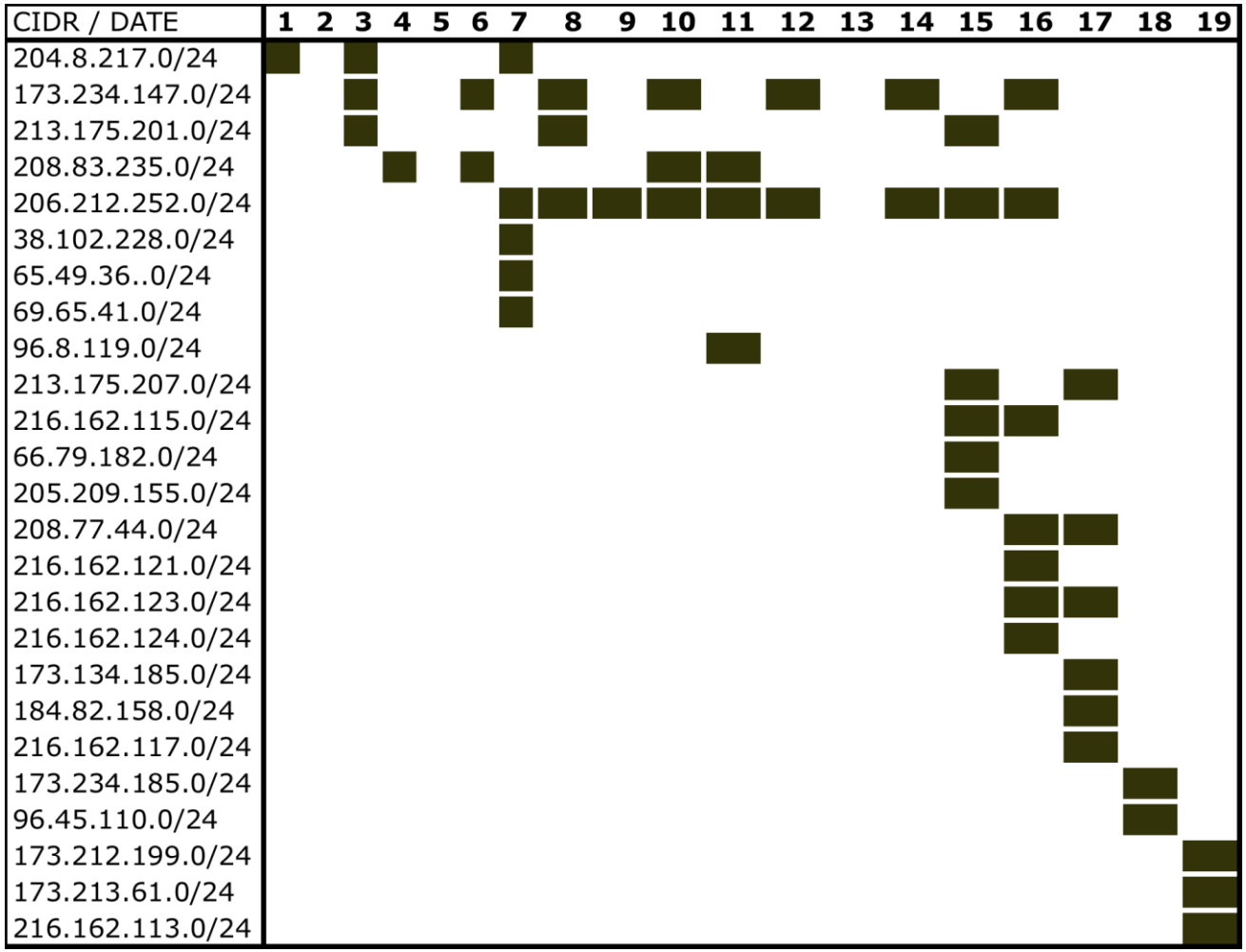
- Functional unsubscribe
- Postal address
- No forged headers
- Send via your own network

COMPLIANCE?

- Yes (mostly), but most recipients do not bother
- Use postal drop boxes to remain anonymous
- Register hundreds or thousands of “throw away” domains
- Lease hundreds of IP addresses from ISPs/Colo/VPS/Cloud

Daily distribution by CIDR

“Limited Trial of the Revolutionary High-Tech Prado Electronic Cigarette!”



Snowshoes!

A closer look…

Sending Behavior

- Statically allocated, dedicated IP addresses
- Paid for by the spammers
- Typically hosted in North America

Top ISPs abused

ISP	Message count	Unique IPs
3dgwebhosting.com	799490	16570
SingleHop	136408	2549
SoftLayer Technologies	106041	1125
Limestone Networks	64787	1119
AccelerateBiz	17457	714
Nobis Technology Group, LLC	55193	697
Network Operations Center	53988	691
FDCservers.net	20460	507
GigeNET	22913	459
Global Net Access, LLC	35996	422
FortressITX	16553	398
LogicWeb	21685	390
Colostore.com	22069	378
iWeb Technologies	65480	306

Financial motivation

- Money is made via a vast array of affiliate programs
- Spammer is the affiliate (publisher)
- Paid via “Cost per Click” or “Cost per Action”

Snowshoe vs “criminal spam”

- Header content

Received: from 789.pizzaperu.com (HELO 789.pizzaperu.com) [65.60.47.236]
by <trap>; <date>
From: "Hybrid Car" <info@pizzaperu.com>
Subject: Go Green Save Green

Received: from duper.varichurm.com (HELO duper.varichurm.com) [64.187.106.21]
by <trap>; <date>
Subject: As A Homeowner This Product Saved_Me_Thousands
From: "Surface_Sealers" <sealsurfaces@varichurm.com>

Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address

Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure

Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
- “Call-to-action”

Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
- “Call-to-action”
- Targeted recipients

Snowshoe vs “criminal spam”

- Header content
- Unsubscribe link and contact address
- Message structure
- “Call-to-action”
- Targeted recipients
- Products advertised

VS Solicited bulk email

- Similar visible content

VS Solicited bulk email

- Similar visible content
- Spam content found in the body

<style type="text/css">

ring breaks at last nights gig. Shop says tama won't replace under warranty and tama won't talk to me.

For the money these are I'm not impressed. Anyone else had similar?

_____
Mapex. Sabian. Iron Cobra. Evans. Gibraltar. DW. Vic Firth.
Reply With Quote
#2
Old 07-06-2011, 12:56 PM
uniin's Avatar
uniin uniin is offline
Silver Member

Join Date: Sep 2010
Location: Blue Mountains, Australia
Posts: 609
Default Re: New iron cobras = useless tama....
are you putting max tension on your springs, and burying the beater into your bass drum (thus creating a lot more tension on your spring)?
[snip]
</style>

VS Solicited bulk email

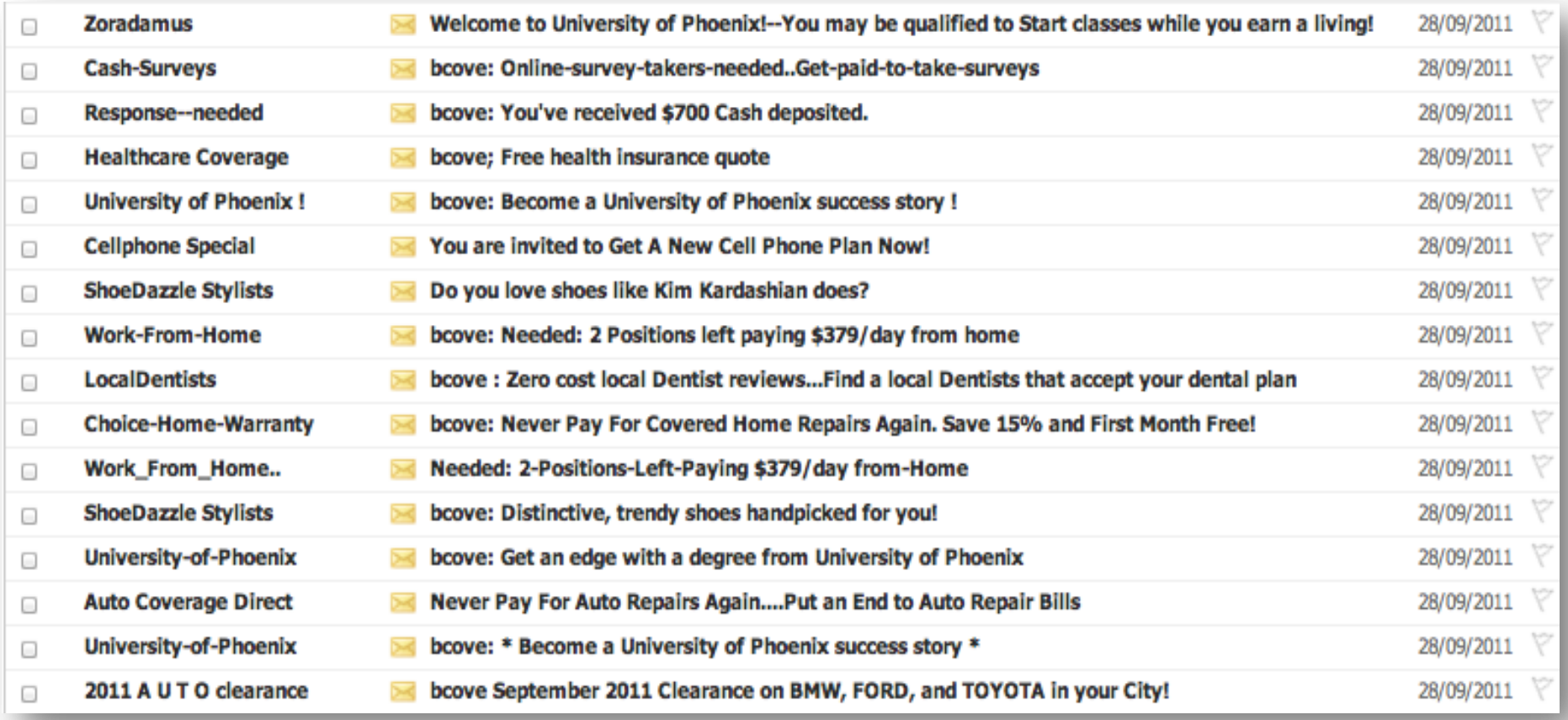
- Similar visible content
- Spam content found in the body
- Domains used

VS Solicited bulk email

- Similar visible content
- Spam content found in the body
- Domains used
- Source and history of IPs used

What makes it a problem

- Volume varies wildly



Zoradamus	Welcome to University of Phoenix!--You may be qualified to Start classes while you earn a living!	28/09/2011
Cash-Surveys	bcove: Online-survey-takers-needed..Get-paid-to-take-surveys	28/09/2011
Response--needed	bcove: You've received $700 Cash deposited.	28/09/2011
Healthcare Coverage	bcove; Free health insurance quote	28/09/2011
University of Phoenix !	bcove: Become a University of Phoenix success story !	28/09/2011
Cellphone Special	You are invited to Get A New Cell Phone Plan Now!	28/09/2011
ShoeDazzle Stylists	Do you love shoes like Kim Kardashian does?	28/09/2011
Work-From-Home	bcove: Needed: 2 Positions left paying $379/day from home	28/09/2011
LocalDentists	bcove : Zero cost local Dentist reviews...Find a local Dentists that accept your dental plan	28/09/2011
Choice-Home-Warranty	bcove: Never Pay For Covered Home Repairs Again. Save 15% and First Month Free!	28/09/2011
Work_From_Home..	Needed: 2-Positions-Left-Paying $379/day from-Home	28/09/2011
ShoeDazzle Stylists	bcove: Distinctive, trendy shoes handpicked for you!	28/09/2011
University-of-Phoenix	bcove: Get an edge with a degree from University of Phoenix	28/09/2011
Auto Coverage Direct	Never Pay For Auto Repairs Again....Put an End to Auto Repair Bills	28/09/2011
University-of-Phoenix	bcove: * Become a University of Phoenix success story *	28/09/2011
2011 A U T O clearance	bcove September 2011 Clearance on BMW, FORD, and TOYOTA in your City!	28/09/2011

What makes it a problem

- Volume varies wildly
- Unsubscribing may not work

What makes it a problem

- Volume varies wildly
- Unsubscribing may not work
- Lack of action response and action by ISPs

What can be done?

- Legislation based on consent (like FISA)
- ISPs must review and take action on abuse complaints
- More coordinated monitoring and abuse reporting
- Draw more attention to the problem

In conclusion

- It’s a growing problem for many people
- It’s still a spam (unsolicited bulk e-mail)
- It’s very different from a criminal spam
- We need to raise awareness and take action

Questions?