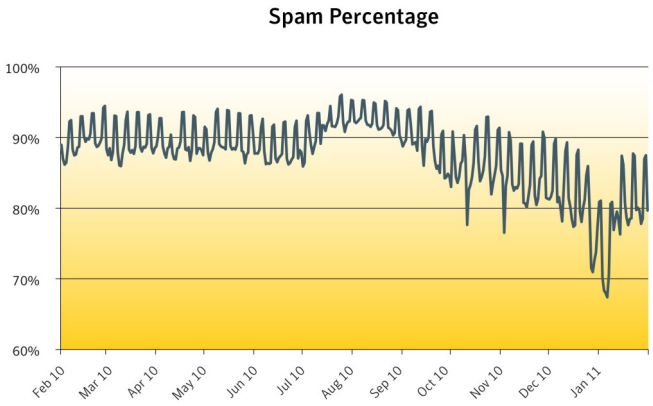
The recent events in Egypt had an unintended outcome. The shutting down of the Internet also shut out spammers in Egypt.



The global spam volume, which has been the discussion topic for several months, appears to have finally stopped its decline. While the month-over-month figures were still down in January, the uptick observed in early January looks to become a permanent fixture of the spam landscape. We expect to see a first month-over-month increase in spam volume in February, which will be a first since August 2010. Spam made up 79.55 percent of all messages in January, compared with 81.69 percent in December.

Phishing levels decreased by 16 percent this month. The decrease was attributed to a decrease in nearly all sectors of phishing. Phishing websites created by automated toolkits decreased by approximately 39 percent, while unique URLs decreased by 1 percent. Phishing websites with IP domains (for e.g. domains like http://255.255.255.255) decreased by about 49 percent. Webhosting services comprised of 12 percent of all phishing activity, an increase of 19 percent from the previous month. The number of non-English phishing sites increased by 5 percent. Among the non-English phishing sites, French and Portuguese were the highest in January.

The following trends are highlighted in the February 2011 report:

- Conclusion of Spam Volume Saga
- Turmoil in Egypt Shuts Down the Spammers
- Scammers Seek Support for Serrana Flood Victims
- Big Brother Brasil Bait is Back
- January 2011: Spam Subject Line Analysis

Dylan Morss
Executive Editor
Antispam Engineering

David Cowings
Executive Editor
Security Response

Eric Park
Editor
Antispam Engineering

Mathew Maniyara
Editor
Security Response

Sagar Desai
PR contact
sagar_desai@symantec.com

Metrics Digest

Global Spam Categories

Category Name	January	December	Change (% points)
Adult	1%	<1%	+1
Financial	6%	8%	-2
Fraud	4%	4%	No change
Health	5%	4%	+1
Internet	47%	47%	No change
Leisure	13%	10%	+3
419 spam	6%	6%	No change
Political	<1%	<1%	No change
Products	14%	17%	-3
scams	3%	3%	No change

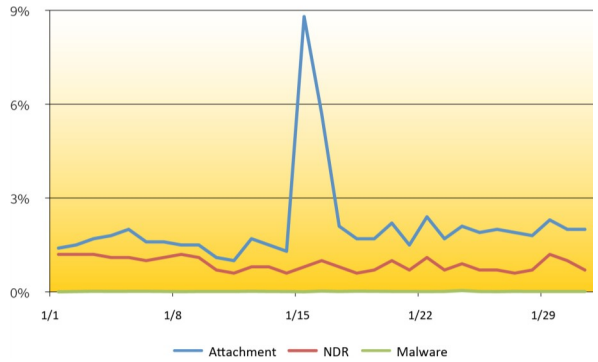
Spam URL TLD Distribution

TLD	January	December	Change (% points)
com	66.8%	72.3%	-5.5
ru	11.1%	7.7%	+3.4
org	6.6%	7.1%	-0.5
info	4.5%	Not listed	N/A

Average Spam Message Size

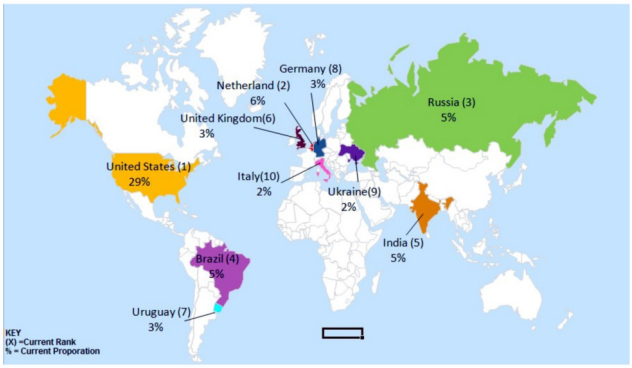
Message Size	January	December	Change (% points)
0-2kb	2.99%	1.30%	+1.69
2kb-5kb	66.52%	65.41%	+1.11
5kb-10kb	21.31%	25.09%	-3.78
10kb+	9.18%	8.20%	+0.98

Spam Attack Vectors



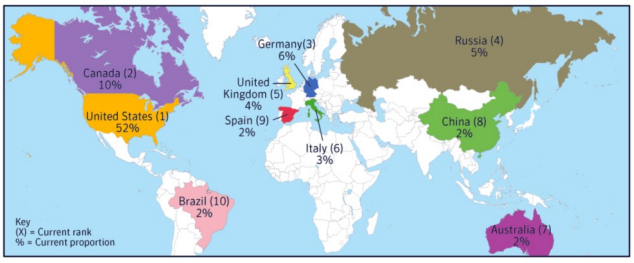
Metrics Digest

Spam Regions of Origin



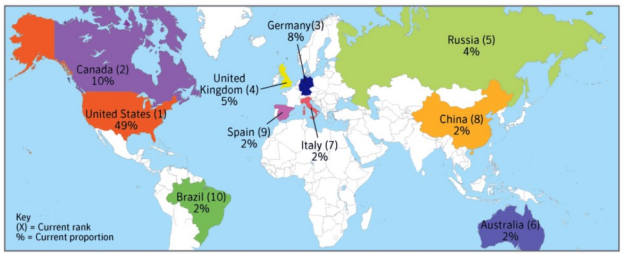
Country	January	December	Change (% points)
United States	29%	29%	No change
Netherlands	6%	5%	+1
Russia	5%	4%	+1
Brazil	5%	4%	+1
India	5%	5%	No change
United Kingdom	3%	4%	-1
Uruguay	3%	Not listed	N/A
Germany	3%	3%	No change
Ukraine	2%	Not listed	N/A
Italy	2%	3%	-1

Geo-Location of Phishing Lures



Country	January	December	Change (% points)
United States	52%	56%	-4
Canada	10%	11%	-1
Germany	6%	7%	-1
Russia	5%	6%	-1
United Kingdom	4%	2%	+2
Italy	3%	2%	1
Australia	2%	Not listed	N/A
China	2%	Not listed	N/A
Spain	2%	2%	No Change
Brazil	2%	1%	+1

Geo-Location of Phishing Hosts

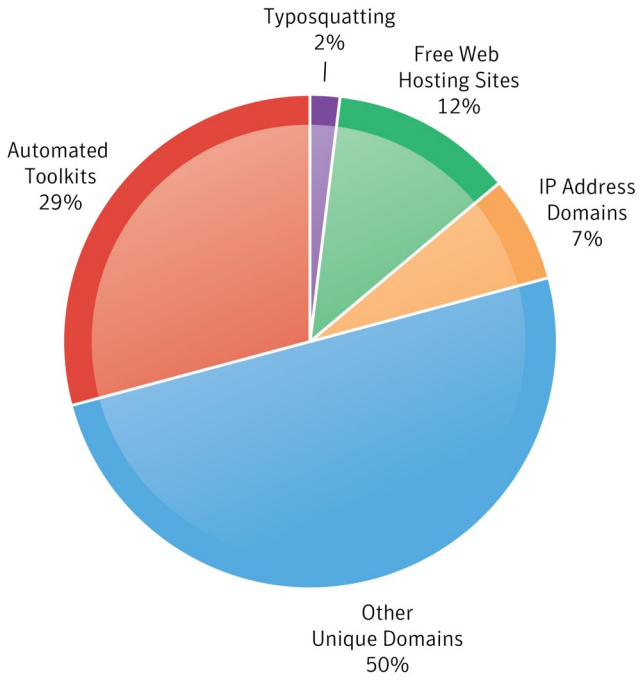


Country	January	December	Change (% points)
United States	49%	54%	-5
Canada	10%	17%	-7
Germany	8%	6%	+2
United Kingdom	5%	2%	+3
Russia	4%	3%	+1
Australia	2%	Not listed	N/A
Italy	2%	2%	No Change
China	2%	Not listed	N/A
Spain	2%	2%	No Change
Brazil	2%	1%	+1

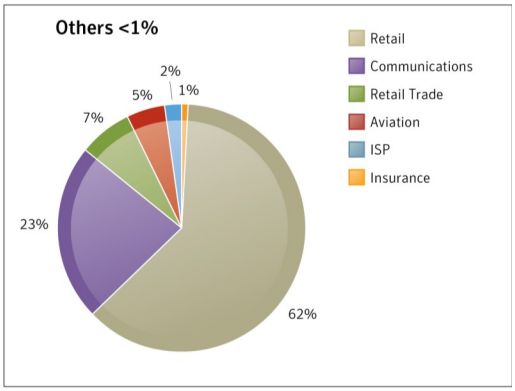
Metrics Digest

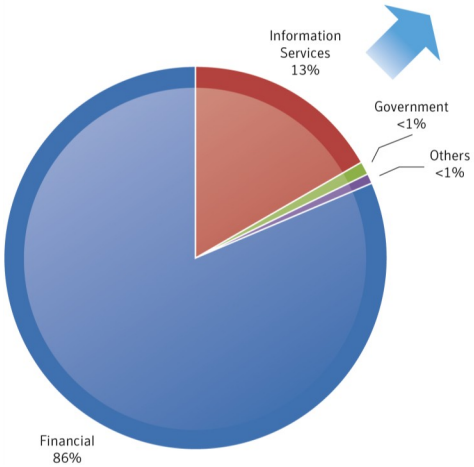
Phishing Tactic Distribution

Overall Statistics



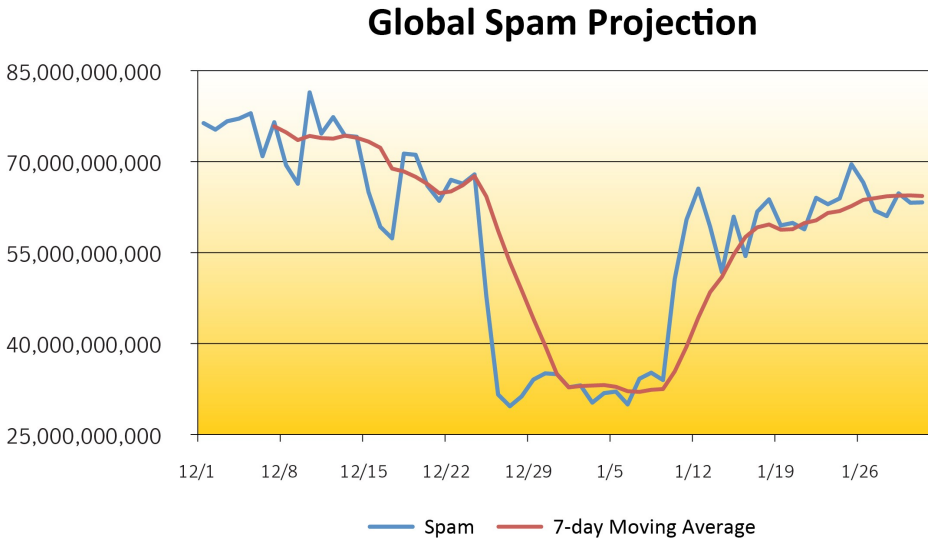
Phishing Target Sectors



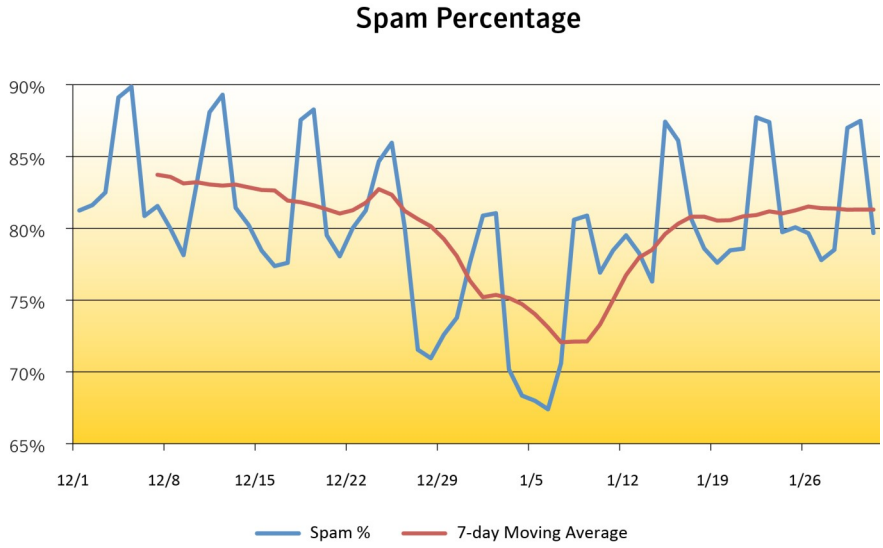


The Closure of Spam Volume Saga

In last month's report, Symantec highlighted the sharp drop in spam around Christmas day and the uptick on January 10th. The chart below shows that the global spam volume continues to rise gradually subsequent to the Rustock botnet returning to action on January 10th.



Despite the uptrend, global spam volume in January 2011 was down 15.7% compared to December 2010. This is primarily due to the Rustock shutdown which affected volumes during the first 10 days of the year. Symantec expects the spam volume in February to be up month-over-month for the first time since August 2010. Mirroring the increase in spam volume, the spam percentage looks to be rising as well.

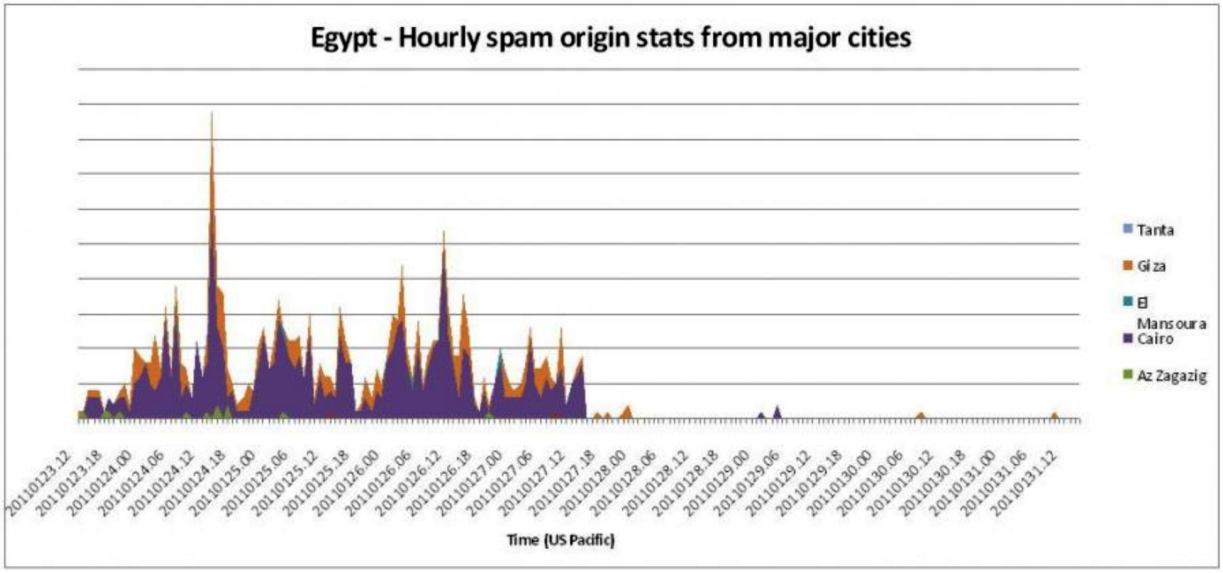


One of the predictions for 2011 was that the spam volume will rise, but at much slower pace compared to post-McColo shutdown. That prediction is holding true thus far, even though it is still very early in the year. Barring a significant change, the spam percentage drama we covered for the past few months appears to be over.

Turmoil in Egypt Shuts Down the Spammers

After the protests in Tunisia spread to Egypt, there were attempts to shut down the internet to keep protesters from communicating and organizing their efforts on the Web. While the action achieved its goal of shutting down access to social networks used by organizers to rally the people together, it also was successful in shutting down the spammers in Egypt.

Around 2:00pm on January 27th, Symantec saw a fall in spam traffic from Egypt. While Egypt does not make up a significant portion of global spam output at around 0.1 percent, it was interesting to see the effect of the internet shutdown had on the spammers. The chart below shows spam from some of the largest cities in Egypt:



Scammers Seek Support for Serrana Flood Victims

In January 2011, floods caused severe calamity in several towns in the mountainous region of Brazil known as the Serrana region, in the state of Rio de Janeiro. Scammers, as usual, are on their toes to take advantage of the opportunity to send scam messages that request fake donations.

Scammers Seek Support for Serrana Flood Victims (continued)

Scammers utilized a domain name to carry out the phishing scam. The domain name consisted of words in Brazilian Portuguese which translate to "donations for the tragedy in Friburgo"; Friburgo is a municipality located in the affected region. The Top Level Domain (TLD) of the domain name was Brazil. Though the TLD was of Brazil, the domain name was located on servers based in Dallas, USA. The content of the phishing Web page was in Brazilian Portuguese and translates to:

"The images show districts affected by the tragedy. The number of cities that reported casualties has risen to five, after heavy rains in the Serrana region caused devastating floods. The municipalities and fire department have confirmed a total of 600 deaths. Rio De Janeiro is in need of your help. We donate food and water to those people who have lost their homes. Please help by donating a little money. You may pay with your credit card or directly from your bank account. On behalf of all the homeless, we are grateful for your help."

Below the message were logos of popular banks and credit card services in Brazil. There were a set of hyperlinks below the logos that prompted end-users to donate by clicking on the link. Each hyperlink was for a specific donation amount in dollars. The amounts specified were $5, $10, $15, $30, and $50. Upon clicking the links, end-users were redirected to a phishing site that spoofed the corresponding brand. At the bottom of the page, a message stated that end-users may also pay donations in other amounts by contacting a particular email address with the same domain name. The phishing sites of the brands asked for the users' login credentials. Upon entering the login credentials, the phishing site redirected to the legitimate Web site.

By using this method, scammers were targeting several brands by means of a single phishing scam. If end-users fall victim to the phishing site, scammers will have succeeded in stealing their credentials for financial gain.

Big Brother Brasil Bait is Back

In 2010, Symantec reported on phishing sites that were spoofing a popular social networking brand. The phishing sites claimed to have a Web application with which end users could watch "Big Brother Brasil" online. This phishing attack was launched during the 10th season of the television show that was on air from January to March of 2010. On January 11, 2011, the 11th season of the show began and phishers are back again with the same bait to try their luck at harvesting user credentials. The latest phishing site was hosted on a free webhosting domain.

Big Brother Brasil Bait is Back (continued)

On certain legitimate Web sites, live video feeds of the show are available around the clock from multiple cameras in the Big Brother house. Some of these videos are suitable only for adult viewing. On the other hand, no live video feeds are available on the phishing site and the claim of having such a Web application is only a ploy to lure end-users. The message in the displayed image of the phishing site was in Portuguese and translates to “In ***** [Brand name removed] Big Brother Brazil is live. Attention: Login to the side and check”. If users fall victim to the bait by entering their login credentials, phishers will have succeeded in stealing their information and put end-users at risk of identity theft.

In the past few months, the motive of phishers has been to improve their chances of tempting end-users by increasing the appeal of the bait. It has been observed that pornography or adult content made up a majority of the bait utilized to lure end-users. Here, though pornography was not involved in the phishing site, the strategy of phishers was to give users the hope of viewing adult videos of the celebrities starting in the television show.

January 2011: Spam Subject Line Analysis

#	Total Spam: January 2011 Top Subject Lines	No of Days	Total Spam: December 2010 Top Subject Lines	No of Days
1	Re:	31	Inna (status-online) invites you for chat.	4
2	Find Out How You Can Start Making $6487 a Month At HOME	29	Pfizer -80% now!	9
3	Marina 21y.o, I am on-line now, let's chat?	2	RealPfizer -70% now	4
4	New post	3	I am on-line now, let's chat?	2
5	New In town	12	Now Pfizer -70%	4
6	Save-0n-Cialis-Viagra-And-Many-Other-Meds-N0W	15	Find Out How You Can Start Making $6487 a Month At HOME	23
7	*Blank Subject line*	31	Russian girls	14
8	New Message	15	*Blank Subject line*	31
9	RE: Date	18	C1AL1S V1AGRA AND LEV1TRA ALL 8O% 0FF	13
10	[NO SUBJECT]	6	Now-Save-8O%-0n-All-Meds-Including-Viagra&Cia1is	8

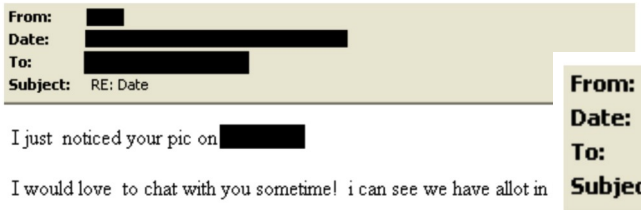
Could it be the Valentine's Day effect? In January 2011, top ten spam subject lines mostly consisted of dating spam. As referenced in the metrics section, the leisure category was up 3 percentage points this month.


From: [redacted]
Date: [redacted]
To: [redacted]
Subject: Marina 21y.o, I am on-line now, let`s chat?

My best wishes to you!

I am **Marina** 21y.o
I am looking for man to have a strong family.
And you?

I am on-line now, let `s chat?


From: [redacted]
Date: [redacted]
To: [redacted]
Subject: RE: Date

I just noticed your pic on [redacted]

I would love to chat with you sometime! i can see we have allot in


From: [redacted]
Date: [redacted]
To: [redacted]
Subject: New post

Check out my profile here and let me know what you think
http://[redacted]

Look at this girl who wants to get married and what people write about her on the forum
http://www[redacted]

Checklist: Protecting your business, your employees and your customers

Do

- Unsubscribe from legitimate mailings that you no longer want to receive. When signing up to receive mail, verify what additional items you are opting into at the same time. De-select items you do not want to receive.
- Be selective about the Web sites where you register your email address.
- Avoid publishing your email address on the Internet. Consider alternate options – for example, use a separate address when signing up for mailing lists, get multiple addresses for multiple purposes, or look into disposable address services.
- Using directions provided by your mail administrators report missed spam if you have an option to do so.
- Delete all spam.
- Avoid clicking on suspicious links in email or IM messages as these may be links to spoofed websites. We suggest typing web addresses directly in to the browser rather than relying upon links within your messages.
- Always be sure that your operating system is up-to-date with the latest updates, and employ a comprehensive security suite. For details on Symantec's offerings of protection visit http://www.symantec.com.
- Consider a reputable antispam solution to handle filtering across your entire organization such as Symantec Brightmail messaging security family of solutions.
- Keep up to date on recent spam trends by visiting the Symantec State of Spam site which is located here.

Do Not

- Open unknown email attachments. These attachments could infect your computer.
- Reply to spam. Typically the sender's email address is forged, and replying may only result in more spam.
- Fill out forms in messages that ask for personal or financial information or passwords. A reputable company is unlikely to ask for your personal details via email. When in doubt, contact the company in question via an independent, trusted mechanism, such as a verified telephone number, or a known Internet address that you type into a new browser window (do not click or cut and paste from a link in the message).
- Buy products or services from spam messages.
- Open spam messages.
- Forward any virus warnings that you receive through email. These are often hoaxes.

* Spam data is based on messages passing through Symantec Probe Network.
* Phishing data is aggregated from a combination of sources including strategic partners, customers and security solutions.