State of Spam & Phishing
A Monthly Report

Confidence in a connected world.

symantec.

February 2010 Report #38

The earthquake in Haiti drove up the volume of scam and phishing messages in January 2010 as spammers used the tragic event for their benefit. Both scam and phishing categories doubled as in percentage of all spam in January 2010 compared to December 2009. With 419-Nigerian spam becoming more prevalent again, the total of scam and phishing messages came in at 21 percent of all spam, which is the highest level recorded since the inception of this report.

hƴƟŚĞ ăŜŀăƨƴƚƒ ăǇŀŶ ŦŴƨƴƟƩ ăǇŀŶŶŜŴă ďăŜŘ ƟŚĞ ďǇǑƨŶƛƴƎ ±ŀƒŜƴƟƛƴŜŵă 5ŀè ĸƨƭƦŘŀè Ɵƨ ăŜƴŘ Øŀ Ŵƛπ ƨďă ƟèǇŜă ƨŦ ǇŴƨŘďǑƟ ăǇŀŶ ŀƴŘ Ŷŀƒø ŀŴŜ϶ 9ØŜƴ øƛƟĸ ƟŚĞ ±ŀƒŜƴƟƛƴŜŵă 5ŀè ǇŴƨŘďǑƟ ăǇŀŶ ǇďăĸƩ ƛƟ was not enough to make up for Christmas-related product spam as the product category decreased by 7 percentage points in January 2010.

Phishing attacks are getting more and more targeted in nature and are focused on attacking major brands rather than being mass attacks. Symantec observed a 25 percent decrease from the previous month in all phishing attacks. The decline in phishing attacks was primarily due to a decrease in the volume of phishing toolkit attacks. It would be important to note that phishing attacks are measured based upon the number of new active phishing sites whereas phishing email messages (spam) are a delivery mechanism to reach phishing sites. In January, 14 percent of phishing URLs were generated using phishing toolkits, a decrease of 50 percent from the previous month. A 16 percent decrease was observed in non-English phishing sites as well. More than 95 Web hosting services were used, which accounted for 13 percent of all phishing attacks, a decrease of 12 percent in total Web host URLs when compared to the previous month.

The following spam and phishing trends are highlighted in the February 2010 report:

- No Sympathy From Spammers
- Spam Calendar of Events
- CNNIC Clamps Down
- Will the Trend Continue?
- January 2010: Spam Subject Line Analysis
- Adult Phishing Scams

Dylan Morss
Executive Editor
Antispam Engineering

David Cowings
Executive Editor
Security Response

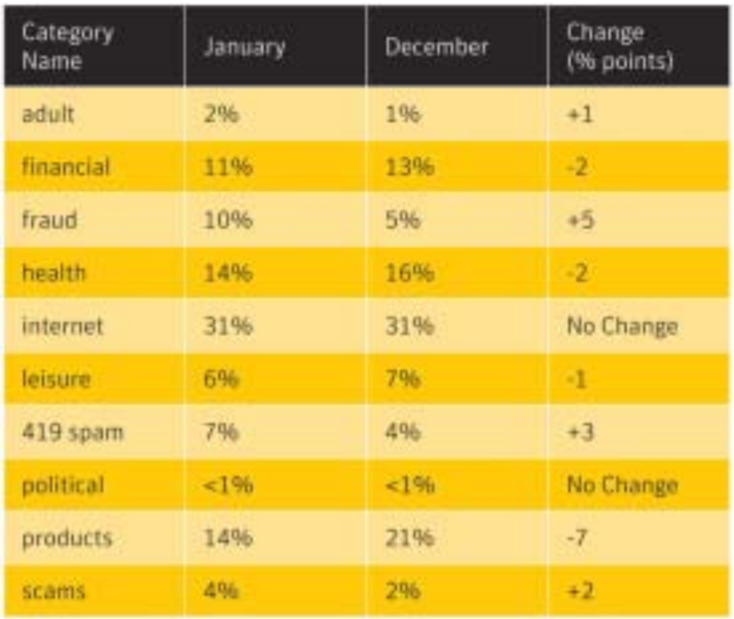
Eric Park
Editor
Antispam Engineering

Mathew Maniyara
Editor
Security Response

Sagar Desai
PR contact
sagar_desai@symantec.com

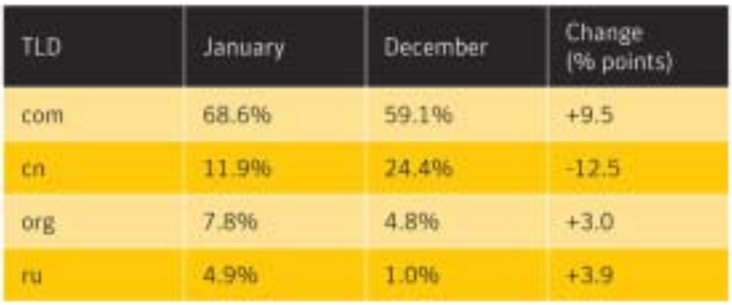
Metrics Digest

Global Spam Categories



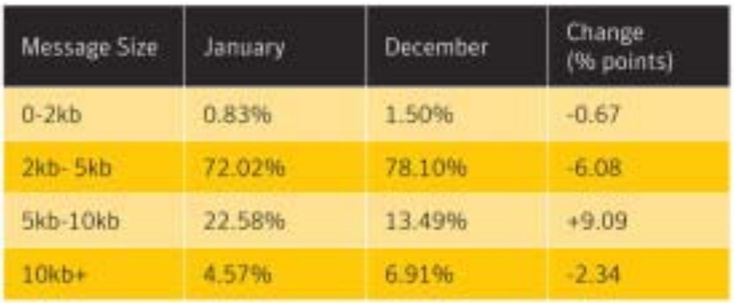
Category Name	January	December	Change (% points)
adult	2%	1%	+1
financial	11%	13%	-2
fraud	10%	5%	+5
health	14%	16%	-2
internet	31%	31%	No Change
leisure	6%	7%	-1
419 spam	7%	4%	+3
political	<1%	<1%	No Change
products	14%	21%	-7
scams	4%	2%	+2

Spam URL TLD Distribution



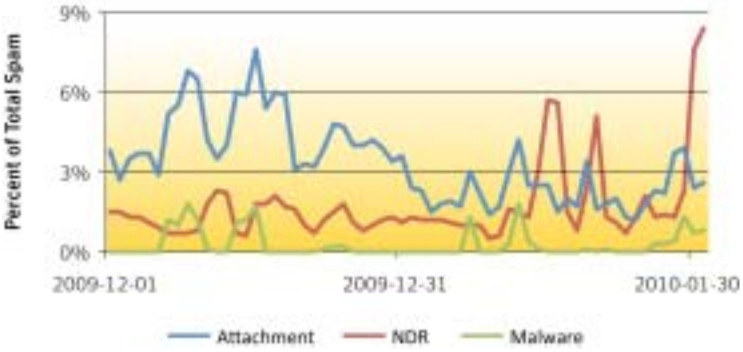
TLD	January	December	Change (% points)
com	68.6%	59.1%	+9.5
cn	11.9%	24.4%	-12.5
org	7.8%	4.8%	+3.0
ru	4.9%	1.0%	+3.9

Average Spam Message Size



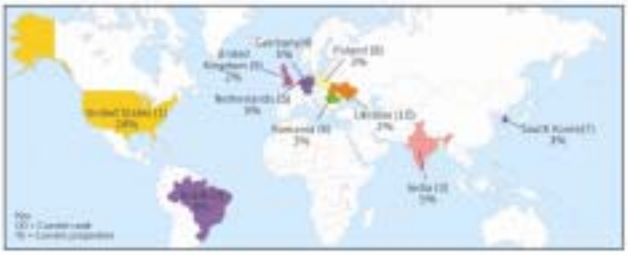
Message Size	January	December	Change (% points)
0-2kb	0.83%	1.50%	-0.67
2kb- 5kb	72.02%	78.10%	-6.08
5kb-10kb	22.58%	13.49%	+9.09
10kb+	4.57%	6.91%	-2.34

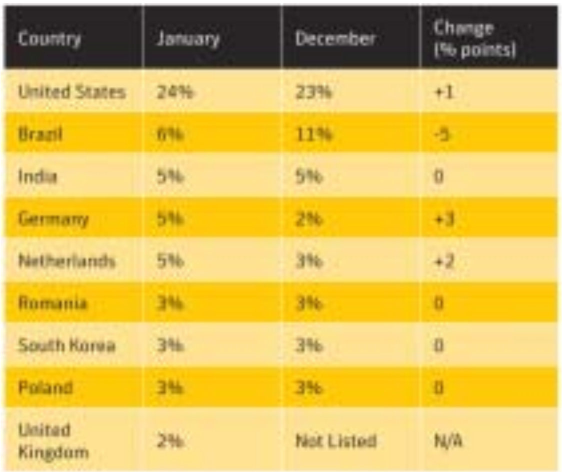
Spam Attack Vectors



Metrics Digest

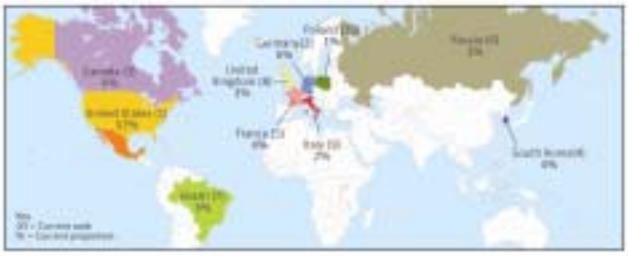
Spam Regions of Origin

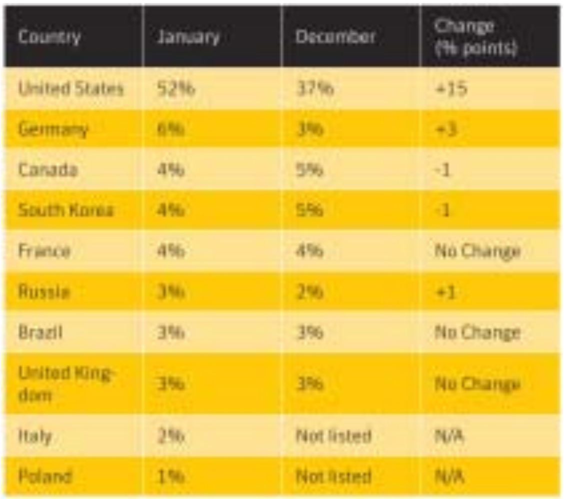




Country	January	December	Change (% points)
United States	24%	23%	+1
Brazil	6%	11%	-5
India	5%	5%	0
Germany	5%	2%	+3
Netherlands	5%	3%	+2
Romania	3%	3%	0
South Korea	3%	3%	0
Poland	3%	3%	0
United Kingdom	2%	Not Listed	N/A

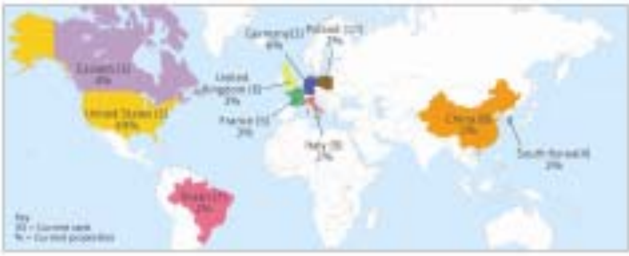
Geo-Location of Phishing Lures

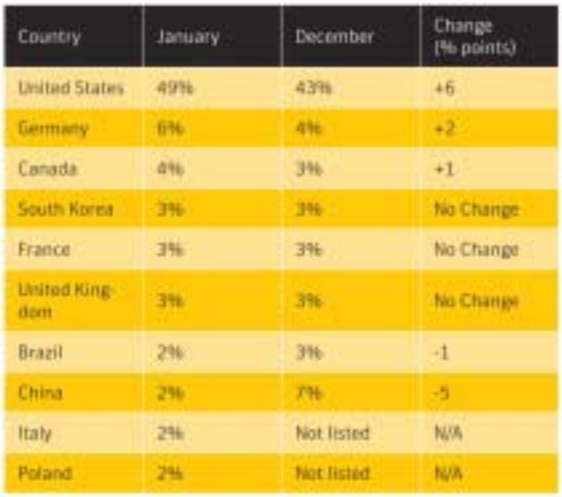




Country	January	December	Change (% points)
United States	52%	37%	+15
Germany	6%	3%	+3
Canada	4%	5%	-1
South Korea	4%	5%	-1
France	4%	4%	No Change
Russia	3%	2%	+1
Brazil	3%	3%	No Change
United Kingdom	3%	3%	No Change
Italy	2%	Not listed	N/A
Poland	1%	Not listed	N/A

Geo-Location of Phishing Hosts

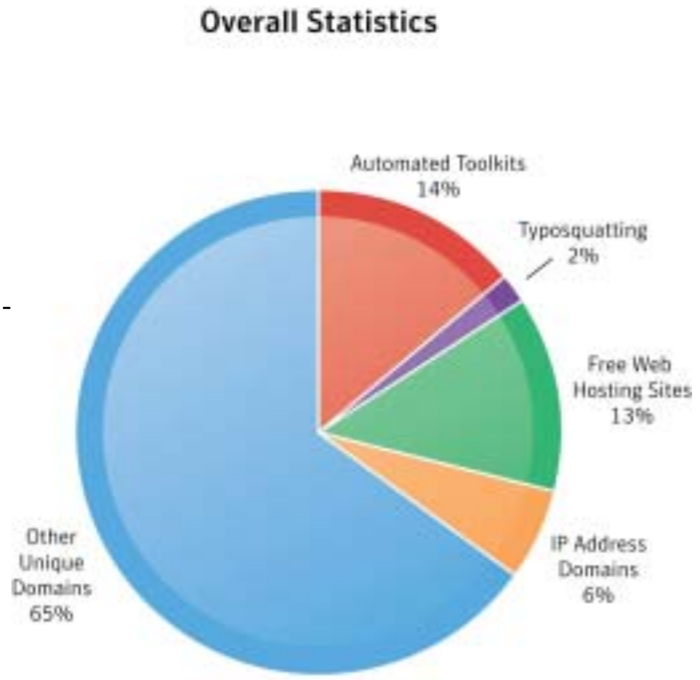




Country	January	December	Change (% points)
United States	49%	43%	+6
Germany	6%	4%	+2
Canada	4%	3%	+1
South Korea	3%	3%	No Change
France	3%	3%	No Change
United Kingdom	3%	3%	No Change
Brazil	2%	3%	-1
China	2%	7%	-5
Italy	2%	Not listed	N/A
Poland	2%	Not listed	N/A

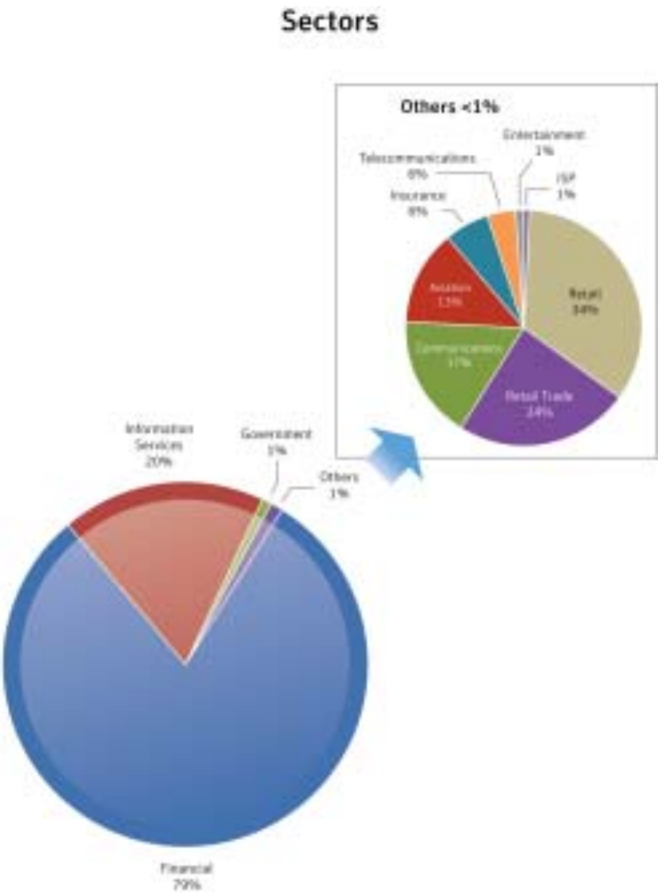
Metrics Digest

Phishing Tactic Distribution



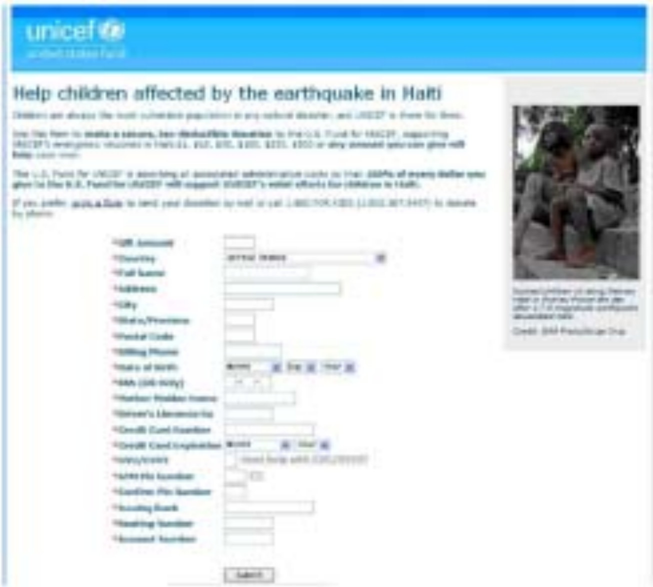
Phishing sites were categorized based upon the domains they leveraged. In January, the total phishing volume decreased significantly by 25 percent. The drop was observed in most sectors including automated toolkit attacks and unique phishing. The sectors that increased from the previous month were typosquatting and IP domains.

Phishing Target Sectors



No Sympathy From Spammers

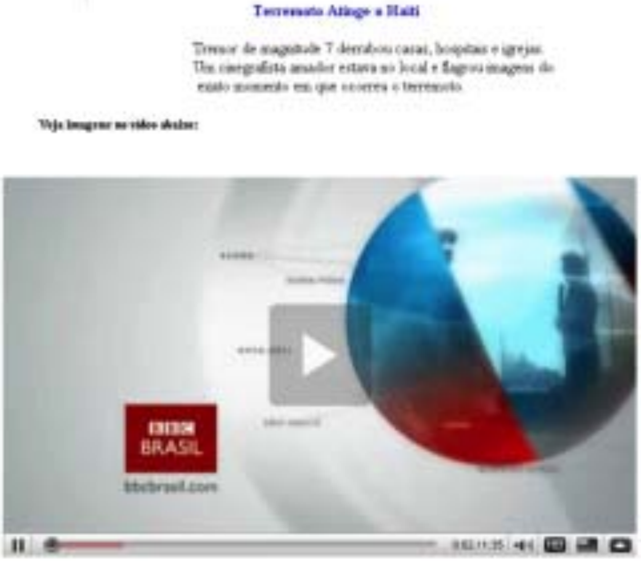
After the tragic earthquake in Haiti on January 12, 2010, relief efforts have poured into the nation from all over the world. Spammers, on the other hand, have taken advantage of this opportunity to send various spam messages related to the tragedy. Symantec researchers have found that spammers usually take advantage of such breaking news events approximately 24-48 hours after the event takes place, and the earthquake in Haiti was no exception.



unicef

Help children affected by the earthquake in Haiti

Spammers started with 419 type spam, asking users to donate money to a charity. When users send their donation, the money disappears into an offshore bank account. Building off of this, spammers began to send phishing messages, pretending to be from a well-known legitimate organization like UNICEF.



Terremoto Atinge o Haiti

Tremor de magnitude 7 derrubou casas, hospitais e igrejas. Um cinegrafista amador estava no local e flagrou imagens do exato momento em que ocorreu o terremoto.

Veja imagens no vídeo abaixo:

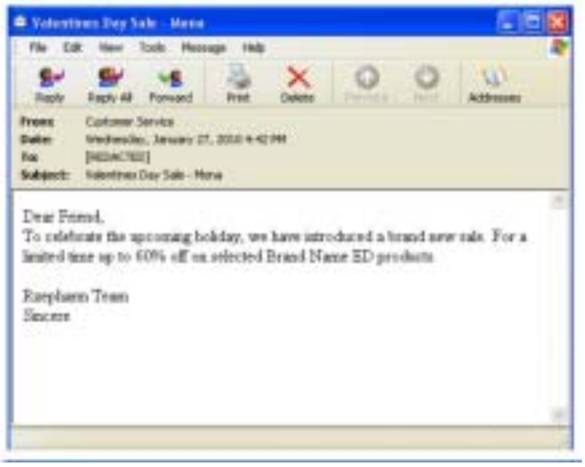
Spammers did not stop there. They also took advantage of this tragedy to deliver malware. In the example (right), users download a Trojan when they click on the link to view the video.

Symantec suggests that users:

- Avoid clicking on suspicious links in e-mail or instant messages as these may be links to spoofed, or fake, Web sites.
- Never fill out forms in messages that ask for personal or financial information or passwords. A reputable charitable organization is unlikely to ask for your personal details via e-mail. When in doubt, contact the organization 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).

Spam Calendar of Events

Even though the holiday season has passed, spammers continue to leverage calendar events, such as major holidays, to lure users into opening their unwanted messages. Symantec re-ăŜl·ǋǑĸŜǋă ĸl·ǾŜ ƻōăŜǋǾŜŘ ǘĸl·ǘ ăLJl·ΥΥŜǋă l·ǋŜ ǝŜǘǘΆyǝ l·ƴŜl·ǋfè ăǘl·ǋǘ ǘƻ ±l·fŜyǘΆyŜǌă 5l·è ōè ăŜyŘπ Άyǝ ăLJl·Υ ΥŜăăl·ǝŜă LJǋƻΥƻǘΆyǝ ŜǾŜǋèǘĸΆyǝ ŦǋƻΥ LJŜǋăƻyl·ƒΆĨŜŘ ǿΆyŜ ǘƻ LJΆffăφ !ă ±l·fŜyǘΆyŜǌă 5l·è is recognized globally, there was also non-English spam observed exploiting the holiday.

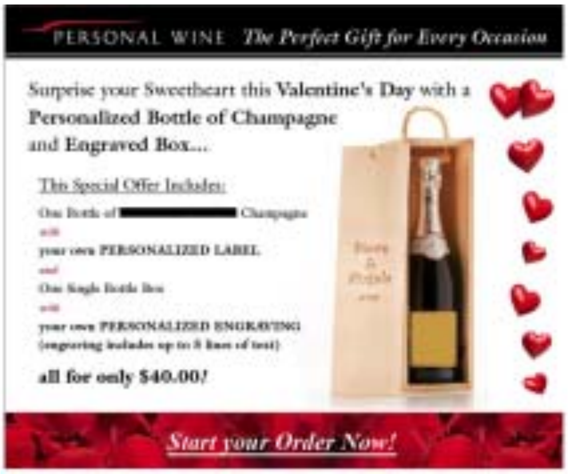

Valentines Day Sale - Mona

File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: Customer Service
Date: Wednesday, January 27, 2010 4:42 PM
To: [REDACTED]
Subject: Valentines Day Sale - Mona

Dear Friend,
To celebrate the upcoming holiday, we have introduced a brand new sale. For a limited time up to 60% off on selected Brand Name ED products

Rxepharm Team
Sincere


PERSONAL WINE *The Perfect Gift for Every Occasion*

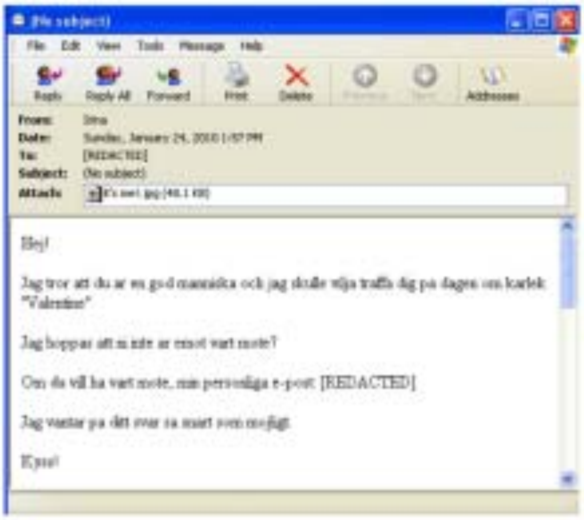
Surprise your Sweetheart this **Valentine's Day** with a **Personalized Bottle of Champagne** and **Engraved Box...**

This Special Offer Includes:

One Bottle of [redacted] Champagne
with
your own PERSONALIZED LABEL
and
One Single Bottle Box
with
your own PERSONALIZED ENGRAVING
(engraving includes up to 8 lines of text)

all for only $40.00!

Start your Order Now!


(No subject)

File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: Irina
Date: Sunday, January 24, 2010 1:57 PM
To: [REDACTED]
Subject: (No subject)
Attach: It's me!.jpg (48.1 KB)

Hej!

Jag tror att du ar en god manniska och jag skulle vilja traffa dig pa dagen om karlek "Valentine"

Jag hoppas att ni inte ar emot vart mote?

Om du vill ha vart mote, min personliga e-post: [REDACTED]

Jag vantar pa ditt svar sa snart som mojligt

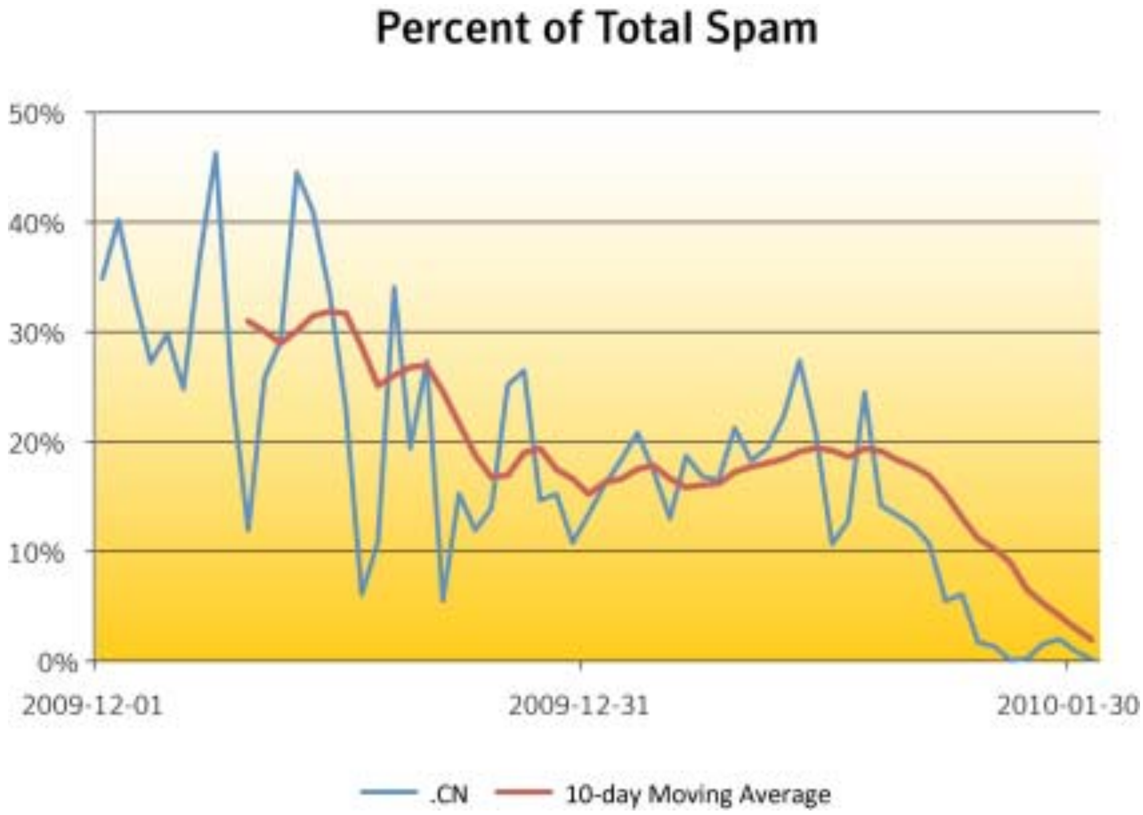
Kyss!

Ly l·ŘŘΆǘΆƻy ǘƻ ±l·fŜyǘΆyŜǌă 5l·è ăLJl·ΥΣ {èΥl·yǘŜǑ ǋŜăŜl·ǋǑĸŜǋă l·yǘΆǑΆLJl·ǘŜ ǘĸl·ǘ ǘĸŜǋŜ Υl·è ōŜ an uptick in phishing messages involving the Internal Revenue Service (IRS). Spammers will be exploiting users as the April 15 deadline for filing taxes approaches. In anticipation of this tax-day spam trend, Symantec advises users to be cautious when opening messages pretending to be from IRS, especially those that claim the recipient owes money or is entitled to a tax refund.

CNNIC Clamps Down

In early January, China Internet Network Information Center (CNNIC) announced the suspension of new overseas .cn domain registrations. CNNIC stated that this suspension will allow them to implement a better procedure to verify registrant information from overseas registrations. This was a follow-up action to a related move in mid-December that required registrants to submit additional paperwork.

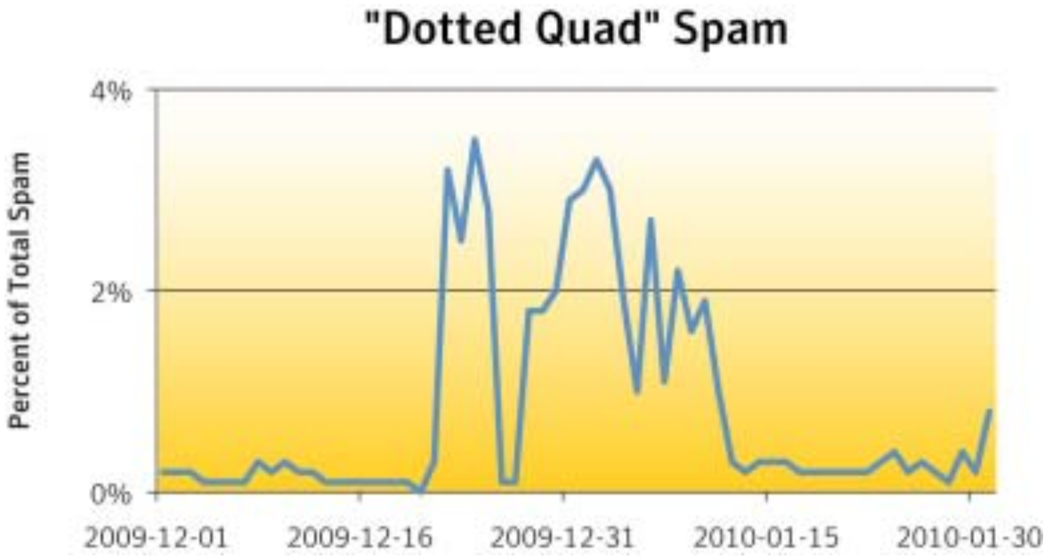
As noted in the Metrics Digest section, spam messages with .cn domain URL dropped by more than half in January, compared to December. Also, the chart below shows precipitous drop towards end of January.



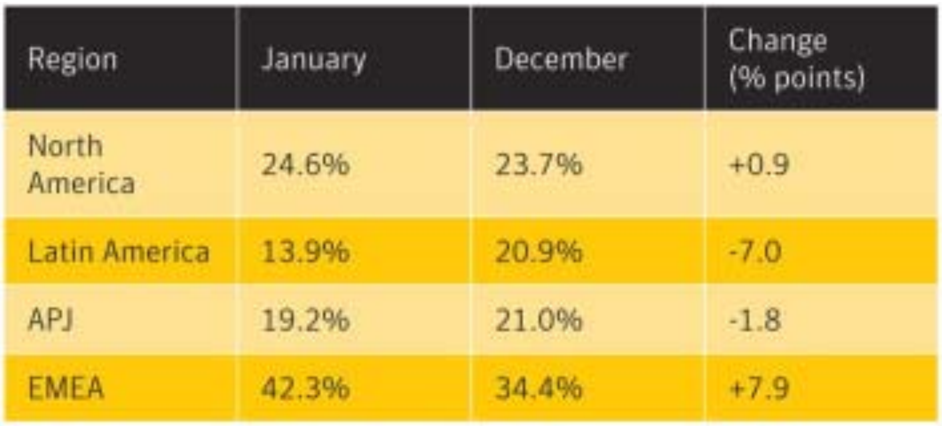
The McColo shutdown in 2008 caused an immediate steep decline in overall spam volume. However, in the subsequent months, spam volumes rose steadily and eventually reached their pre-shutdown levels. As such, it is too early to declare the demise of .cn domain spam. Nevertheless, this shows that certain policies can directly affect the spam threat landscape for the better.

Will the Trend Continue?

hyŜ 2Ŧ ŭĸŜ ĸƛƎĸƒƛƎĸŭă ŦƝ2Ƴ ŭĸŜ Ɯŀyƌŀƚè нлмл ƝŜǕ2Ɲŭ ǿ ŀă άŘ2ŭŭŜŘ ǉƌŀŘέ ăǕǇŀƳǿ ŀă ŭĸŜ ǾƎƒƌƳŜ 2Ŧ this type of spam tripled from the previous month. While the volume continued to increase in January 2010, Symantec researchers did not see a similar rate of increase.



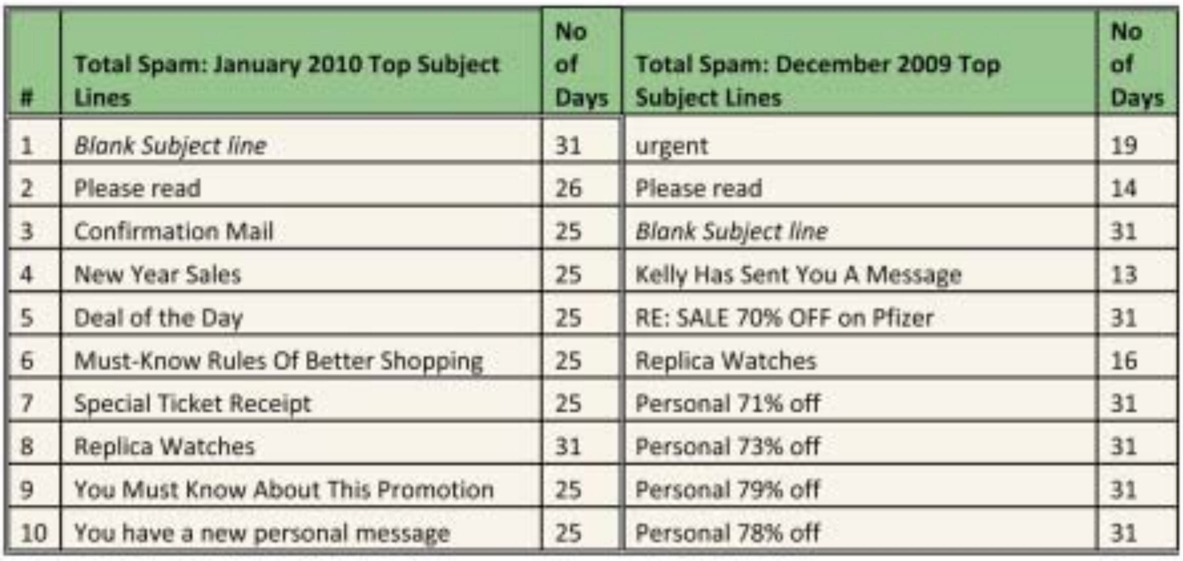
Another pattern highlighted in the last report was the potential reversal of shift in the origin of ăǕǇŀƳ ŀă 9 a 9! ƝŜƎŀƛyŜŘ ŭĸŜ άǎƛyƎέ ŭƛŭƒŜ 2Ŧ ăǕǇŀƳ ƛŭ ƒ2ăŭφ Symantec has observed the continuation of this reversal as the EMEA region sent over 42 percent of spam worldwide, representing a 7.9 percentage point increase from December.



Region	January	December	Change (% points)
North America	24.6%	23.7%	+0.9
Latin America	13.9%	20.9%	-7.0
APJ	19.2%	21.0%	-1.8
EMEA	42.3%	34.4%	+7.9

January 2010: Spam Subject Line Analysis

In January 2010, the top ten subject lines used by spammers were dominated by a mixture of Nigerian- type (419) and online pharmacy spam. It is interesting to see that spammers have ǑĶl·ƴƎŜŘ ǘĶŜƛƜ ǘl·ǑǘƛǑǎ ƜŜƎl·ƜŘƛƴƎ ƨƴƫƴŜ ǇĶl·ƜƳl·Ǒè ǎǇǇl·Ƴ϶ {ǳƃƨŜǑǘ ƫƛƴŜǎ ǎǳǑĶ l·ǎ ά a ǳǎǘ-Know wǳƚŜǎ hƑ .ŜǘǘŜƜ {ĶƨǇǇƛƴƎέ l·ƴŘ ά¸ƨǳ a ǳǎǘ Ƴƴƨǿ !ƃƨǳǘ ¢Ķƛǎ tƜƨƳƨǘƛƨƴέ l·ƜŜ ƳƨƜŜ Ǿl·ƎǳŜ ǘĶl·ƴ άw9Ɣ { ! [9 тǅ̂ ȃ hCC ƨƴ tƑƛÎŜƜ϶έ hǘĶŜƜ Ƴƛǎƚ Ŝl·ŘƛƴƎ ǎǳƃƨŜǑǘ ƫƛƴŜǎ ǎǳǑĶ l·ǎ ά/ƨƴƑƛƜƳl·ǘƛƨƴ a l·ƛƫέ l·ƴŘ ά{ǇŜǑƛl·ƫ ¢ƛǑƪŜǘ wŜǑŜƛǇǘέ ǿŜƜŜ l·ƫǎƨ ǳǎŜŘ ƑƨƜ ƨƴƫƴŜ ǇĶl·ƜƳl·Ǒè ǎǇǇl·Ƴ ƳŜǎǎl·ƎŜǎ϶



#	Total Spam: January 2010 Top Subject Lines	No of Days	Total Spam: December 2009 Top Subject Lines	No of Days
1	*Blank Subject line*	31	urgent	19
2	Please read	26	Please read	14
3	Confirmation Mail	25	*Blank Subject line*	31
4	New Year Sales	25	Kelly Has Sent You A Message	13
5	Deal of the Day	25	RE: SALE 70% OFF on Pfizer	31
6	Must-Know Rules Of Better Shopping	25	Replica Watches	16
7	Special Ticket Receipt	25	Personal 71% off	31
8	Replica Watches	31	Personal 73% off	31
9	You Must Know About This Promotion	25	Personal 79% off	31
10	You have a new personal message	25	Personal 78% off	31

Adult Phishing Scams

Symantec observed a new trend in adult oriented phishing. The phishing site states that the end user can obtain free pornography after logging in or signing up. These offers tempt users into entering their credentials in the hopes of obtaining pornography. Upon entering login credentials, the site redirects to a pornographic website that then leads to a fake antivirus website containing malicious code. 92 percent of adult phishing scams were on social networking sites, with the remainder on information services brand. The phishing sites were created using free webhosting services.

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 ς 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 em-ǇƒƋè ŀ ÖƋƳǇǊŜƘŜɯăǶØŜ ăŜŎǳǊǷűè ăǳǷűŜɲ CƋǊ ŘŜűŀǷƒă Ƌɯ {èƳŀɯűŜŎǴă ƋŦŦŜǊǷɯƎă ƋŦ ǇǊƋűŜŎűǷƋɯ ØǷăǷű 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.
- wŜǇƒè űƋ ăǇŀƳɫ ¢èǇǷŎŀƒƒè űƘŜ ăŜɯŘŜǊǎă ŜƳŀǷƒ ŀŘŘǊŜăă Ƿă ŦƋǊƳŜŘƷ ŀɯŘ ǊŜǇƒèǷɯƎ Ƴŀè Ƌɯƒè ǊŜăǳƒű 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.