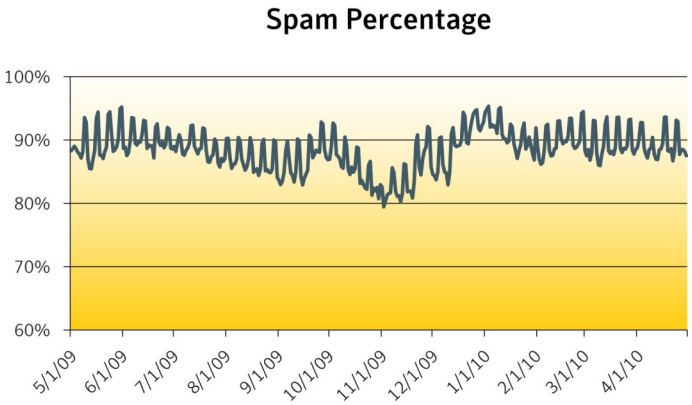
Dotted quad spam makes a splashy return to this report as the volume more than tripled from the month prior. The most observed spam subject line of the month was also the dotted quad spam attack. With respect to message size, attachment spam continued to creep up in volume in March. This, along with an increase in NDR spam, raised the average message size. The 5kb to 10kb bucket increased by over 4 percentage points, and 10+kb bucket increased by over 9 percentage points. With respect to spam categories, scam and phishing messages in April accounted for 17 percent of all spam, remaining unchanged compared to March. Overall, spam made up 89.22 percent of all messages in April, compared with 89.34 percent in March.



An increase of 33 percent was observed in overall phishing attacks from the previous month. The increase was contributed to all sectors of phishing. Twelve percent of the phishing websites were generated from automated toolkits, an increase of 77 percent from the previous month. Unique URLs increased by 29 percent and IP attacks increased by 3 percent from the previous month. Non-English phishing websites increased by 23 percent. The increase was contributed by a rise in attacks in French and Portuguese. Phishing in French was mostly in the financial sector and attacks in Portuguese were a combination of the financial and information services sectors. About 108 free webhosting services were used, which accounted for 10 percent of all phishing attacks.

The following trends are highlighted in the April 2010 report:

- Deeper Dive into Dotted Quad Spam
- A Fake Fast Food Survey
- UK Students Under Scam Attack
- Another Holiday Spammers Can't Skip On
- April 2010: Spam Subject Line Analysis
- Will the Trend Continue?

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	April	March	Change (% points)
Adult	1%	1%	No change
Financial	15%	12%	+3
Fraud	6%	7%	-1
Health	12%	12%	No change
Internet	33%	34%	-1
Leisure	4%	5%	-1
419 spam	7%	6%	+1
Political	<1%	<1%	No change
Products	17%	18%	-1
scams	4%	4%	No change

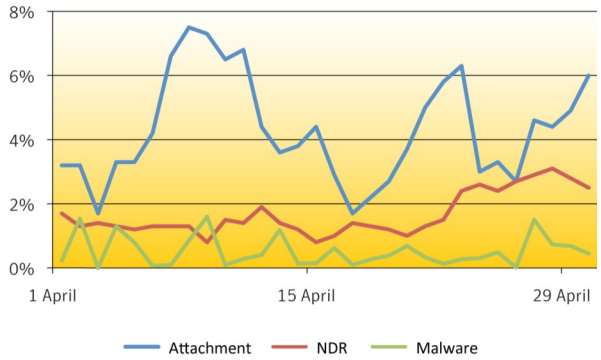
Spam URL TLD Distribution

TLD	April	March	Change (% points)
com	62.7%	47.0%	+15.7
ru	22.1%	29.8%	-7.7
org	6.0%	Not listed	N/A
cn	2.2%	4.1%	-1.9

Average Spam Message Size

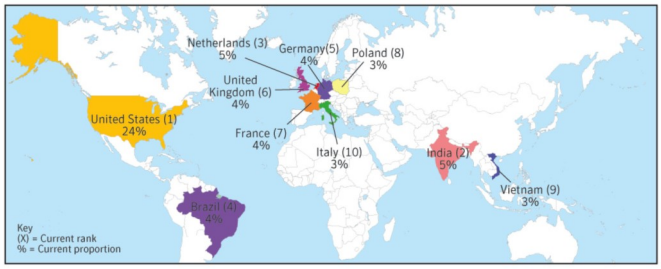
Message Size	April	March	Change (% points)
0-2kb	0.57%	0.34%	+0.23
2kb-5kb	50.37%	63.63%	-13.26
5kb-10kb	29.03%	25.02%	+4.01
10kb+	20.03%	11.01%	+9.02

Spam Attack Vectors



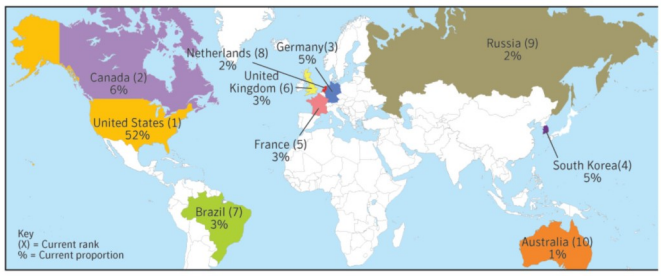
Metrics Digest

Spam Regions of Origin



Country	April	March	Change (% points)
United States	24%	24%	No change
India	5%	5%	No change
Netherlands	5%	5%	No change
Brazil	4%	5%	-1
Germany	4%	3%	+1
United Kingdom	4%	3%	+1
France	4%	3%	+1
Poland	3%	3%	No change
Vietnam	3%	Not listed	N/A
Italy	3%	Not listed	N/A

Geo-Location of Phishing Lures



Country	April	March	Change (% points)
United States	52%	51%	+1
Canada	6%	7%	-1
Germany	5%	5%	No Change
South Korea	5%	4%	+1
France	3%	4%	-1
United Kingdom	3%	3%	No Change
Brazil	3%	3%	No Change
Netherlands	2%	Not Listed	N/A
Russia	2%	3%	-1
Australia	1%	Not Listed	N/A

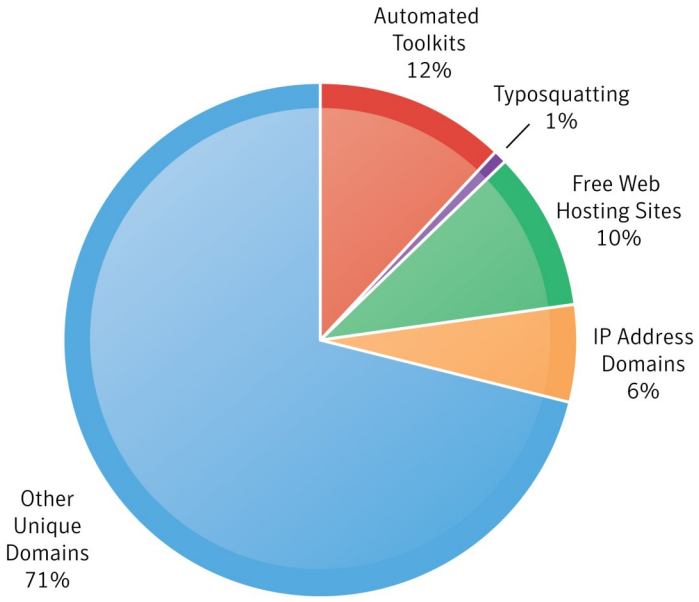
Geo-Location of Phishing Hosts

Country	April	March	Change (% points)
United States	51%	50%	+1
Germany	6%	7%	-1
Canada	4%	5%	-1
South Korea	4%	4%	No Change
United Kingdom	4%	4%	No Change
France	3%	3%	No Change
Russia	3%	2%	+1
China	2%	2%	No Change
Netherlands	2%	2%	No Change
Brazil	2%	Not Listed	N/A

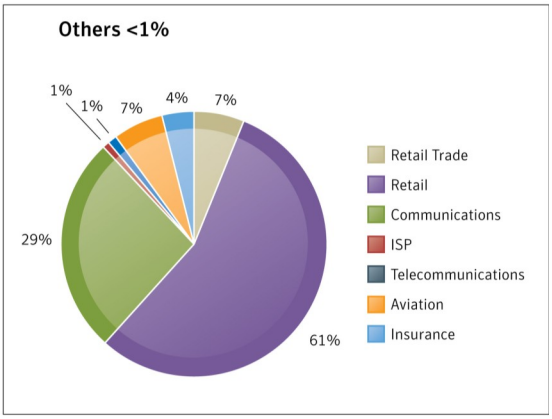
Metrics Digest

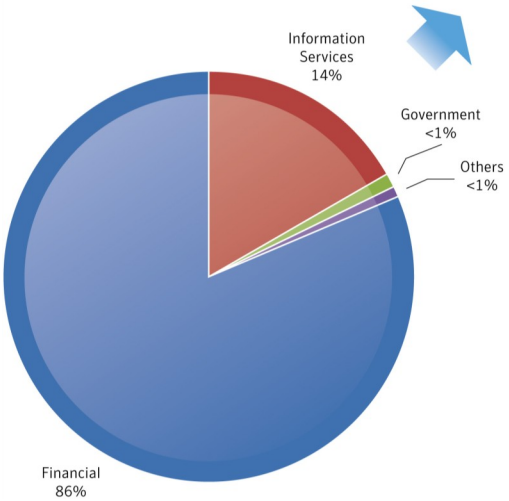
Phishing Tactic Distribution

Overall Statistics



Phishing Target Sectors





Deeper Dive into Dotted Quad Spam

As highlighted in the "Will the Trend Continue?" and "April 2010: Spam Subject Line Analysis" sections, dotted quad spam attacks definitely made an impact in April. Dotted quad spam occurs when the dotted quad address of the spam URL link is used in the spam message body rather than the domain name of the spam URL. A dotted quad address refers to the notation that expresses the four-byte (32-bit) IP address as a sequence of four decimal numbers separated by dots. For example, rather than using domain.com in the URL, the link is an IP address (i.e., http://255.255.255.255).

Here is a sample HTML code of a dotted quad spam message:

Having trouble viewing this email? View it in your browser.

Navigating to the link provided in the message eventually leads the user to:

As seen in the address bar of the browser, the user is redirected to another webpage after clicking on the link provided in the message. However, there is another hidden step before the user arrives at the final destination. Closely examining the source code of URL provided in the message reveals that the page (http://[IP ADDRESS REDACTED]/vassal73.html) loads a script hosted on another website.

Deeper Dive into Dotted Quad Spam (continued)

<html><head><script>location = 'http://[DOMAIN REDACTED]:8080/';</script></head></html>

That script finally sends the user to the above website. While this example involved only two redirects, spammers can deploy many redirects in their spam campaigns.

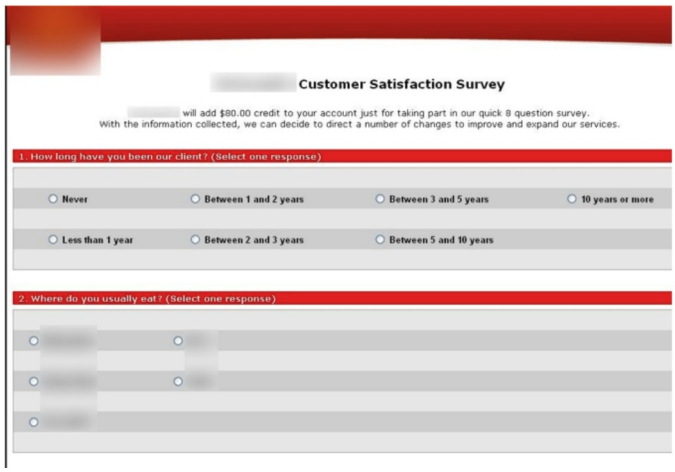
Why do the spammers leverage this technique? Due to advances in anti-spam technology, even the most basic filters can block messages based on URLs in the message. Therefore, if the spammer simply sent out messages with spam.com domain as URL, the message is likely to get blocked based on the URL filter.

However, spammers increase their chances of successful delivery when they use above redirects. Spammers often use hijacked or compromised servers and place a small html file that will redirect the user to the destination, or to another redirect. To send these spam messages, they also use compromised hosts (often referred as zombies) which leverages the hosts' good reputation. Combining the two tactics increase the delivery rate as the messages have higher chance of bypassing traditional filter as well as reputation-based filtering.

Furthermore, spammers can leverage multiple levels of compromised hosts, which would generate a large matrix of possible combinations. This helps the spammers continue their campaign even if they lose some compromised hosts.

A Fake Fast Food Survey

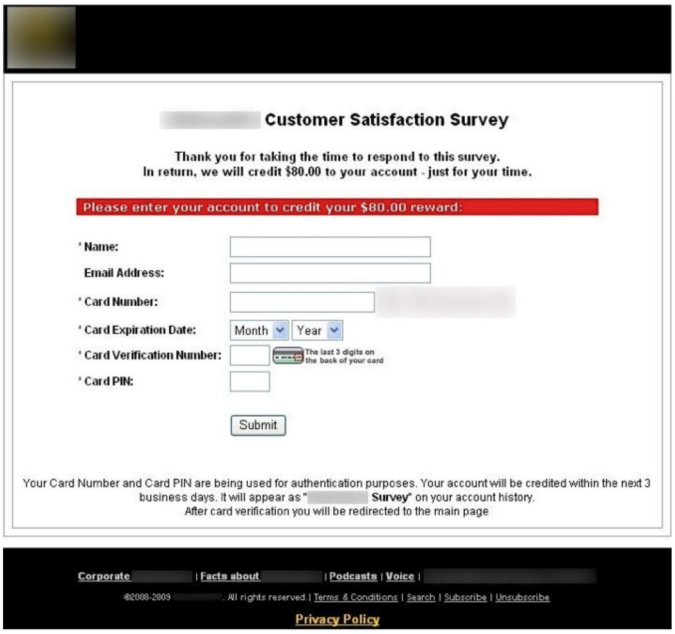
Symantec observed phishing attacks against a major fast food brand. The attacks were carried out through spam mails requesting customer answers for a bogus satisfaction survey. The fast food brand is one of the most popular worldwide, so fraudsters sent the spam globally. The spam email states that the brand is planning major changes to their chain of restaurants to improve their quality of service. The mail further states that to implement these changes, customer opinion is required by means of a survey (which is of course fake). Fraudsters try to trick customers by claiming a reward for those who participate in this survey. The spam email contains a link that leads to the phishing website containing the fake survey:



In this example, the phishing website claims to provide an $80 reward for the customer taking part in a quick, 8 question survey. Upon completing the survey, the Web page is redirected to a fake user authentication page that asks for sensitive information such as credit card number and pin number so as to supposedly credit the bogus reward to the customer's fast food account.

A Fake Fast Food Survey (continued)

The page claims to credit the reward within 3 business days after user authentication and will reflect on the customer's account history.



UK Students Under Scam Attack

Scammers targeted UK students by phishing a brand that belongs to the UK government. The legitimate brand provides information and services for government organizations to UK citizens. Students who are seeking financial services for their higher education can apply on this brand's website. The website requires customers to open an account to access any of the services. An account helps to keep track of all payment transactions.

The phishing website that targeted students was asking for verification to process the credit/loan application submitted by the student. This fake verification request sought sensitive information, such as customer reference number, password, and bank account details. The reference number represents the customer's account, which fraudsters take advantage of by viewing their account history. Upon entering credentials, the page redirects to the legitimate website.

Several phishing websites were observed in this attack, and they were hosted on servers based in the USA and the UK.

Another Holiday Spammers Can't Skip On

In recognition of Mother's Day, spammers sent a variety of product spam messages.

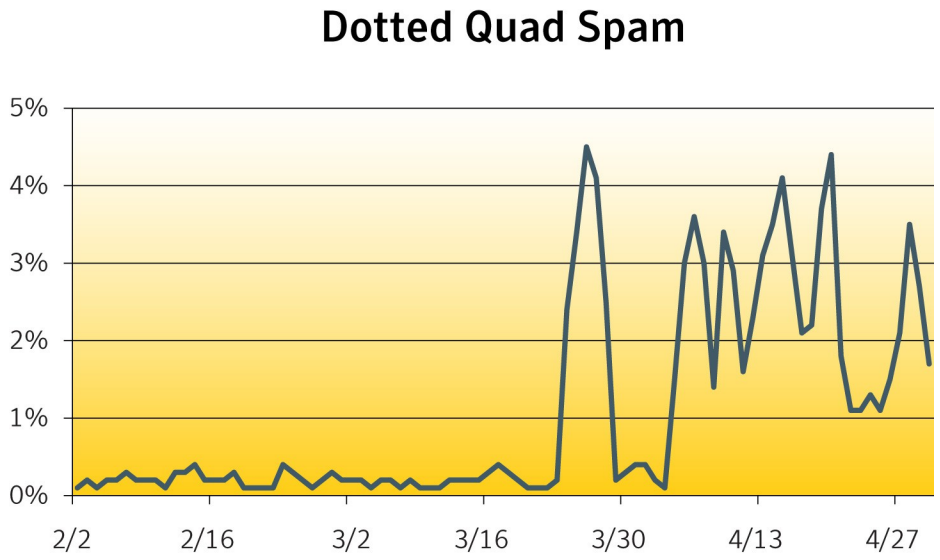
April 2010: Spam Subject Line Analysis

The top Subject line of the month, "Amazon.com Deal of the Day", was used in an online pharmacy attack utilizing dotted quad URLs. It is also noteworthy that spammers heavily used this subject line as it claimed the number one slot despite the fact that it appeared in only ten days. Rounding out the top ten subject lines were additional online pharmacy attacks as well as replica spam.

#	Total Spam: April 2010 Top Subject Lines	No of Days	Total Spam: March 2010 Top Subject Lines	No of Days
1	Amazon.com Deal of the Day	10	*Blank Subject line*	31
2	*Blank Subject line*	30	News on myspace	31
3	Replica Watches	29	Important notice: Google Apps browser support	31
4	News on myspace	23	Important notice: Google	31
5	Important notice: Google Apps browser support	24	You have a new personal message	31
6	Important notice: Google	23	Bestsellers. 70% Discount.	12
7	You have a new personal message	22	SALE 79% OFF on PFIZER!	4
8	Exquisite Replica	29	Replica Watches	24
9	Watches	29	Delivery Status Notification (Failure)	31
10	Delivery Status Notification (Failure)	30	RE: SALE 70% OFF on PFIZER!	11

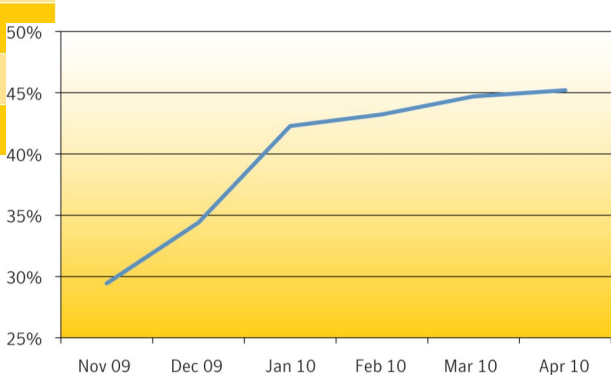
Will the Trend Continue?

Symantec first highlighted the sharp increase in dotted quad spam in the January report. Since then, this type of attack stayed relatively dormant. However, the volume picked up again in late March and continued throughout April. Overall, dotted quad spam volume more than tripled in April, compared to March. See "Deeper Dive into Dotted Quad Spam" to learn why such a tactic may be enticing for spammers to use.



The EMEA region continues to expand its spam market share as the region sent 45.2 percent of worldwide spam in April. As the chart below illustrates, EMEA has grown its spam share over the last six months.

Region	April	March	Change (% points)
North America	25.1%	24.5%	+0.6
Latin America	10.9%	11.7%	-0.8
APJ	18.8%	19.1%	-0.3
EMEA	45.2%	44.7%	+0.5



In the EMEA region, the top ten countries (Netherlands, Germany, United Kingdom, France, Poland, Italy, Romania, Spain, Russian, and Ukraine) made up over 65 percent of the region's volume.

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.