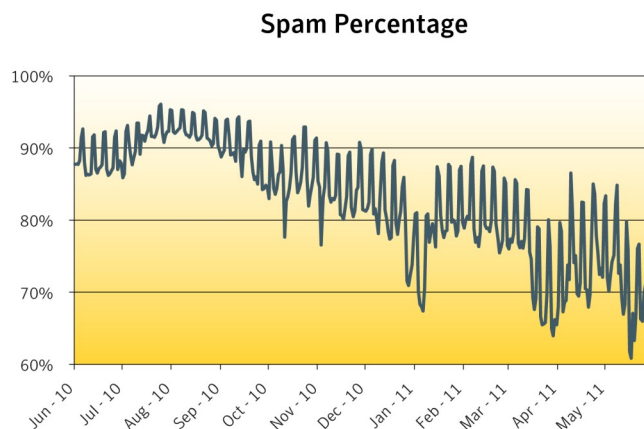




The effect of recent botnet shutdowns continue to have dramatic effects on overall spam volume. After falling 5.35 percent in April, average daily spam volume fell another 10.02 percent in May. Compared to the same period a year ago, it is down 70.65 percent. Overall, spam made up 72.14 percent of all messages in May, compared with 74.81 percent in April. For a longer term perspective, spam percentage was 89.81 percent in May 2010.



However, this does not mean that spammers are dead. This month's report highlights online pharmacy spam using two different angles: a spoof of an online video sharing service and Wikipedia. Also, May spam subject line analysis shows that adult spam continue to flourish.

The overall phishing landscape increased by 6.67 percent this month. Automated toolkits and unique domains increased as compared to the previous month. Phishing websites created by automated toolkits increased by 24.82 percent. Unique URLs increased slightly by 0.26 percent. Phishing websites with IP domains (for e.g. domains like <http://255.255.255.255>) increased by 14.93 percent. Webhosting services comprised 9 percent of all phishing, a decrease of 17.66 percent from the previous month. The number of non-English phishing sites saw an increase of 17.73 percent. Among non-English phishing sites, Portuguese, French, Italian and Spanish were the highest in May.

The following trends are highlighted in the June 2011 report:

- Clicking to Watch Videos Leads to Pharmacy Spam
- Wiki for Everything, Even for Spam
- Phishers Return for Tax Returns
- Fake Donations Continue to Haunt Japan
- May 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

Pamela Reese
PR contact
pamela_reese@symantec.com



Metrics Digest

Global Spam Categories

Category Name	May	April	Change (% points)
Adult	<1%	2%	-2
Financial	9%	7%	+2
Fraud	4%	4%	No change
Health	5%	5%	No change
Internet	57%	51%	+6
Leisure	4%	11%	-7
419 spam	5%	6%	-1
Political	<1%	<1%	No change
Products	14%	11%	+3
scams	1%	2%	-1

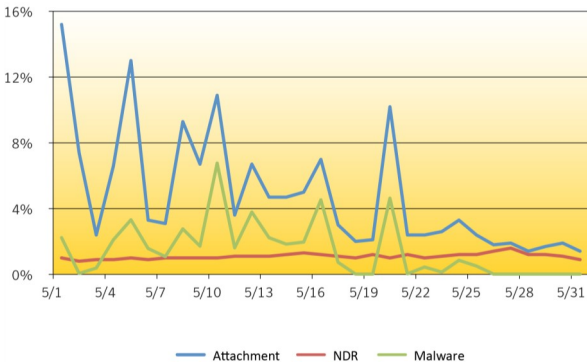
Spam URL TLD Distribution

TLD	May	April	Change (% points)
com	53.4%	55.0%	-1.6
ru	19.2%	10.1%	+9.1
info	14.9%	18.5%	-3.6
net	5.5%	6.9%	-1.4

Average Spam Message Size

Message Size	May	April	Change (% points)
0kb-5kb	62.33%	69.59%	-7.26
5kb-10kb	24.23%	16.18%	+8.05
10kb+	13.44%	14.23%	-0.79

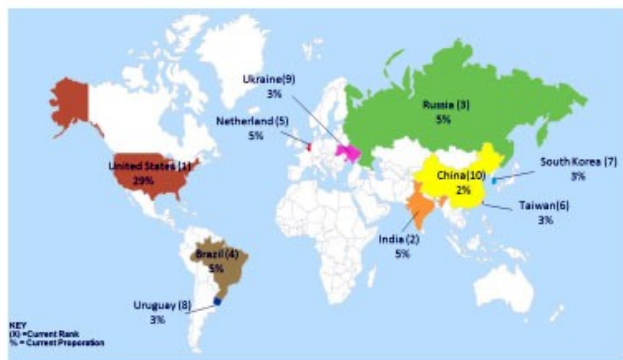
Spam Attack Vectors





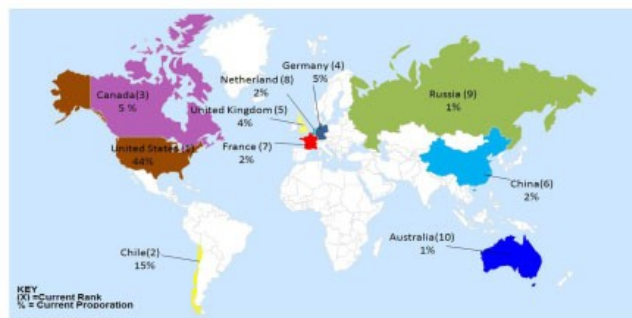
Metrics Digest

Spam Regions of Origin



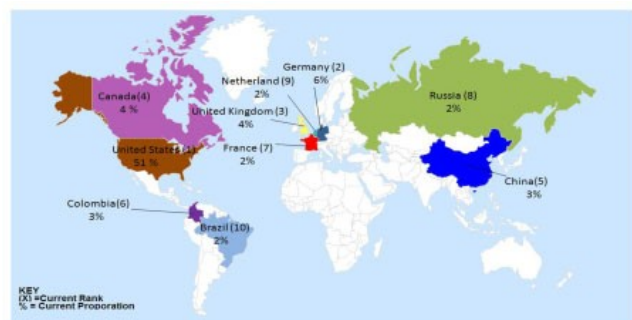
Country	May	April	Change (% points)
United States	29%	31%	-2
India	5%	4%	+1
Russia	5%	5%	No change
Brazil	5%	5%	No change
Netherlands	5%	5%	No change
Taiwan	3%	4%	-1
South Korea	3%	3%	No change
Uruguay	3%	3%	No change
Ukraine	3%	2%	+1
China	2%	3%	-1

Geo-Location of Phishing Lures



Country	May	April	Change (% points)
United States	44%	55%	-11
Chile	15%	Not Listed	N/A
Canada	5%	5%	No change
Germany	5%	6%	-1
United Kingdom	4%	6%	-2
China	2%	Not Listed	N/A
France	2%	3%	-1
Netherlands	2%	2%	No change
Russia	1%	2%	-1
Australia	1%	3%	-2

Geo-Location of Phishing Hosts



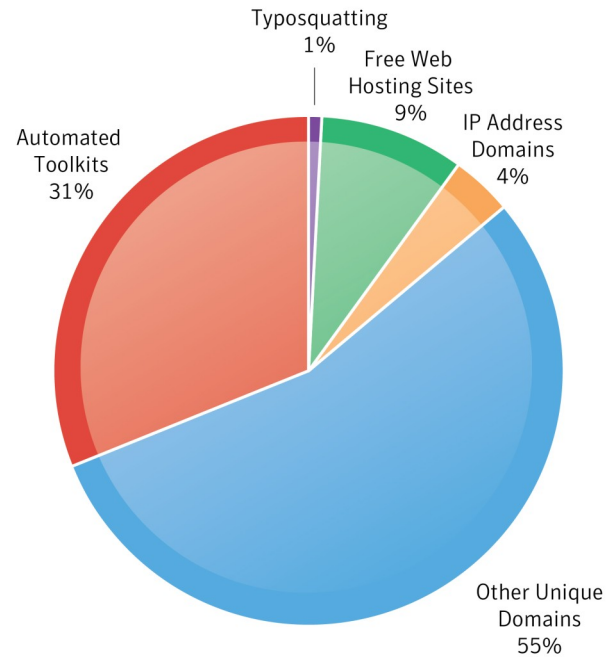
Country	May	April	Change (% points)
United States	51%	51%	No change
Germany	6%	7%	-1
United Kingdom	4%	5%	-1
Canada	4%	3%	+1
China	3%	Not Listed	N/A
Colombia	3%	2%	+1
France	2%	3%	-1
Russia	2%	2%	No change
Netherlands	2%	3%	-1
Brazil	2%	2%	No change



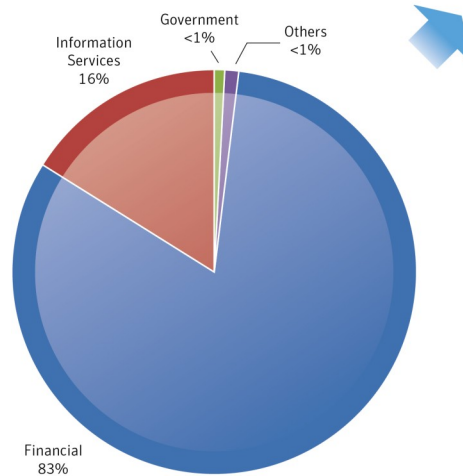
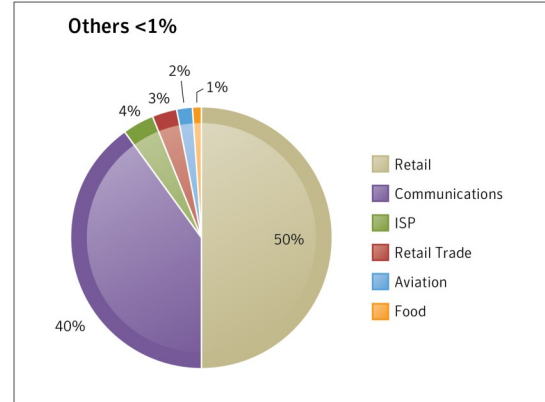
Metrics Digest

Phishing Tactic Distribution

Overall Statistics



Phishing Target Sectors





Clicking to Watch Videos Leads to Pharmacy Spam

Spam messages promoting pharmaceutical products have been perhaps the most commonly seen spam attacks over the past several years. Pharmaceutical products are deceptively marketed through spam emails employing a variety of obfuscation techniques. Symantec saw an increase in pharmacy spam abusing well-known online video sharing site.

Sample From and Subject lines observed in this spam attack are below.

From: [REMOVED] Service <service@[REMOVED].com>

Subject: [REMOVED] Administration sent you a message: Your video on the TOP of [REMOVED]

Subject: [REMOVED] Service sent you a message: Best Unrated Videos To Watch

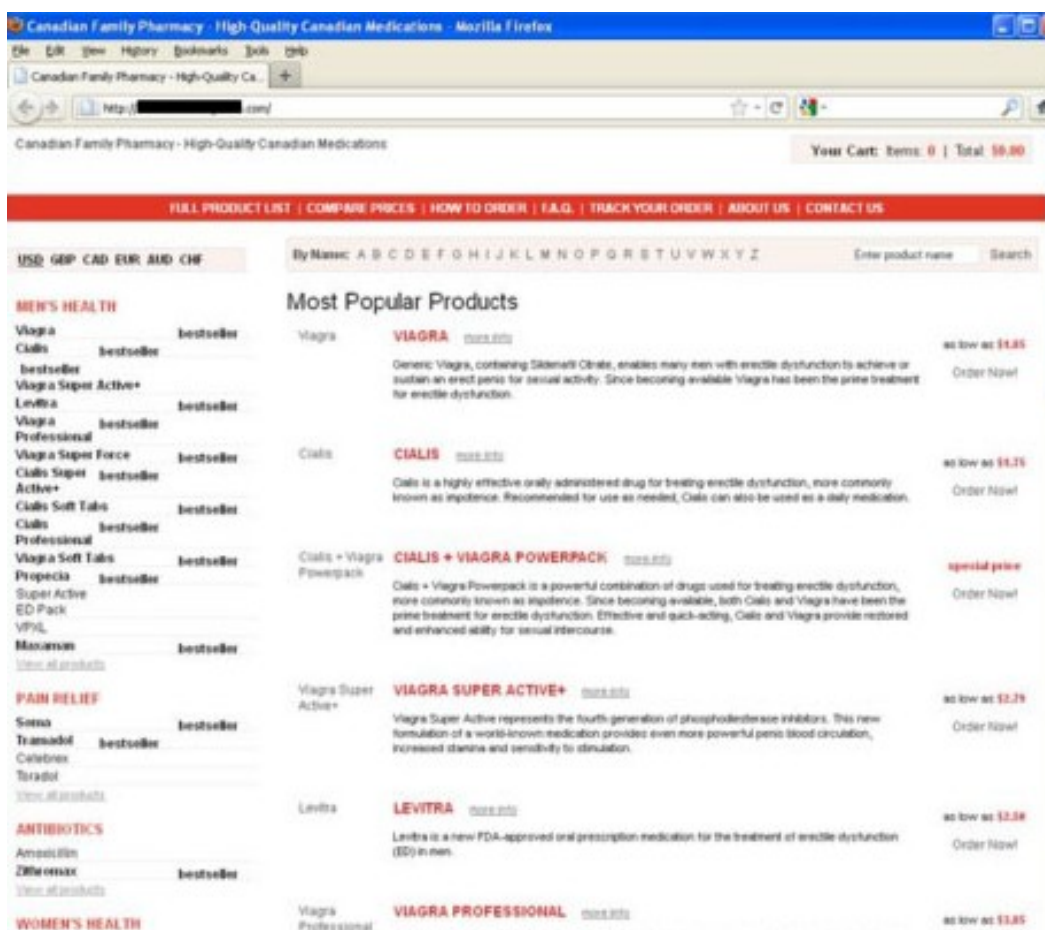
Subject: [REMOVED] Support sent you a message: Your video has been removed due to terms of use violation



With these subject lines, the spammers have attempted to instill a sense of curiosity among the recipients. The spam messages either state that the recipient's video features as a top video, or that the recipient's particular video has been removed due to a terms-of-use violation. The text, accompanied by URL links in the message body, as in most cases, is the call to action in this spam campaign. The included URLs which appear to link to the video sharing site are in fact spam URLs hosted on a hijacked domains. When clicked, all URLs redirect to a Canadian pharmacy Web page (screenshot below) hosted on a recently created domain owner by the spammer. Some of these domains were found to be registered in Russia and France. The spammer, ironically, has placed a link to report spam which is just another redirect to the same pharmacy Web page.



Clicking to Watch Videos Leads to Pharmacy Spam (continued)



The IP addresses involved in these spam attacks are part of botnets and have been blacklisted for their past involvement in such spam campaigns. It is likely that these messages were sent using multiple botnets to distribute high volume of spam.

Wiki for Everything, Even for Spam

Last year, phishers targeted Wikipedia with a large number of spam emails that directed unsuspecting users to a fraudulent Wikipedia website. Symantec's Global Intelligence Network saw a new spam tactic being used, which targets the Wikipedia name for the promotion of fake pharmaceutical products. The "Subject" line in these attacks has a lot of randomization. The "From" header is either fake or a hijacked ISP account that gives a personalized look to the email.



Wiki for Everything, Even for Spam (continued)

Below are some subject lines that were observed in the spam samples:

Subject: wWIKIp

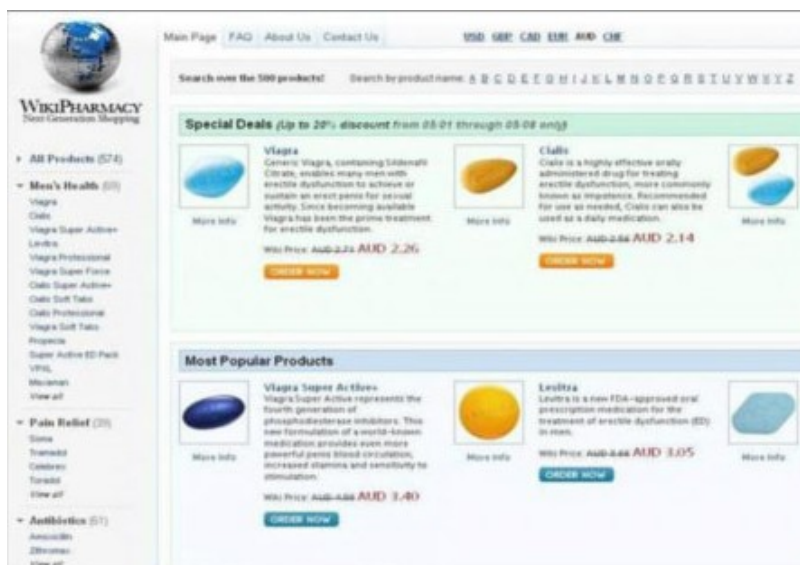
Subject: kWIKIx

Subject: yWIKIg

Subject: hWikiPharmacyl

Subject: oWikiPharmacyp

Subject: uWikiPharmacym



In the image shown above, spammers are promoting pharmacy products at a discounted price using a wiki-style layout. The Web page pretends to be that of “WikiPharmacy”. The volume of spam in this latest attack is quite high. Needless to say is that Wikipedia’s popularity is being exploited here, considering its vast knowledge base and popularity. In this case, users have to be very careful not to enter and personal details on these fake sites.

Here are some of the URL patterns seen in these samples:

http://sucullu.[REMOVED].net/wiki14.html

http://cinar.[REMOVED].org.tr/wiki14.html

http://jmleml.[REMOVED].com/wiki14.html

http://[REMOVED].com.br/wiki15.html

http://[REMOVED].com/wiki15.html

http://web164892.web23.[REMOVED].net/wiki15.html

A careful look at the “Subject” line is sufficient to identify this type of spam. Beware of prowling predators who are waiting to pounce on any opportunity. Please see the Best Practices section of the report for helpful tips in protecting your computer.



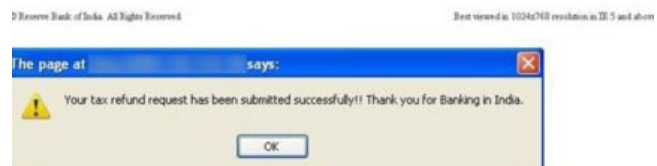
Phishers Return for Tax Returns

The Income Tax Department of India recently announced that the last date for sending income tax returns for AY 2010-2011 has been extended to July 31, 2011. During 2010, phishers had plotted their phishing scams based on the tax return deadline. As the deadline for tax returns of the current financial year approaches, phishers have returned with their stream of phishing sites.

This time, phishers have spoofed the Reserve Bank of India's Web site as a ploy for a tax refund scam. The phishing site attempts to lure users by stating that the bank would take full responsibility for depositing the tax refund to the user's personal bank account. The user is prompted to select the name of the bank and enter their customer ID and password. There is a list of eight banks to choose from. In this way, phishers intend to steal the confidential information of customers of several banks from a single phishing site. The following page asked for credit/debit card number and PIN number. After these details are entered, the phishing site displays a message acknowledging that the request for the tax refund has been submitted successfully. The user is then redirected to the legitimate Web site of Reserve Bank of India. If users fall victim to the phishing site, phishers will have stolen their information for financial gain.

Symantec has been in contact with the Reserve Bank of India. The bank has stated that emails sent in its name to customers have been observed asking for bank account details. The Reserve Bank has clarified that it has not sent any such email and that the Reserve Bank (or any bank) never issues communication asking for bank account details for any purpose. The Reserve Bank has also appealed to members of public to not respond to such email and to not share their bank account details with anyone for any purpose.

The phishing site used a numbered IP domain (for example, domains like `hxxp://255.255.255.255`) hosted on servers based in St Louis, USA. The same IP was used for hosting phishing sites of several other Indian banks. The IP belongs to a Web site of a company that provides roofing for houses. The IP of the company's Web site was compromised to host the phishing sites.





Fake Donations Continue to Haunt Japan

A couple of months ago, Japan was hit by an earthquake of magnitude 9.0. The earthquake and tsunamis that followed caused severe calamity to the country. Phishers soon responded with their [fake donation campaign](#) in the hopes of luring end users. Unfortunately, it seems that the phishers are continuing to use these fake donations as bait in a recent phishing attack we observed.

In a fake donation campaign, phishers spoof the websites of charitable organizations and banks and use those fake sites as bait. This time, they spoofed the German page of a popular payment gateway site with a bogus site that asked for user login credentials. The contents of the page (in German) translated to “Japan needs your help. Support the relief efforts for the earthquake victims. Please donate now.” The message was provided along with a map of Japan that highlighted two cities from the affected region. The first city shown was the one near Japan’s nuclear power plant, Fukushima, and the second was the capital city, Tokyo. The map also showed the epicenter of the earthquake located undersea near the east coast of Japan.

Upon entering their credentials, users are redirected to the legitimate website where they continue their activity, unaware that they have provided their valuable login information to phishers. Because the login credentials in question are for a payment gateway site, the account is linked to users’ money by means of credit cards or bank accounts. If the users have fell victim to the phishing site, phishers will have successfully stolen their personal information for financial gain. The phishing attack was carried out using a toolkit that utilized a single IP address, which resolved to four domain names and was hosted on servers based in France.



May 2011: Spam Subject Line Analysis

#	Total Spam: May 2011 Top Subject Lines	No of Days	Total Spam: April 2011 Top Subject Lines	No of Days
1	Blank Subject line	31	Re: ru girl	24
2	Re: Windows 7, Office 2010, Adobe CS5 ...	16	Blank Subject line	30
3	im online now	31	Re: Windows 7, Office 2010, Adobe CS5 ...	12
4	my new pics :)	31	Save-80%-On-Viagra-Levitra-And-Cialis	14
5	drop me a line	31	Express Delivery system notification	7
6	r u online now?	31	Re:Hi	29
7	hi darling..	31	Re: sale wiagrow	7
8	new email	31	Do you have problem with ErectileDysfunction? ViagraCan help you and make sure it is a unique drug for treatingImpotence.	16
9	found you :)	31	BuyVIAGRA (SildenafilCitrates) Generic Tablets – Online Drugstore. ViagraCan help your ErectileDysfunction	16
10	my hot pics :)	31	Find Out How You Can Start Making \$6487 a Month At HOME	19

In May 2011, adult spam took over the top spam subject line list. Online pharmacy spam subjects, which dominated the list last month, slipped with first one being seen in 16th place.



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.