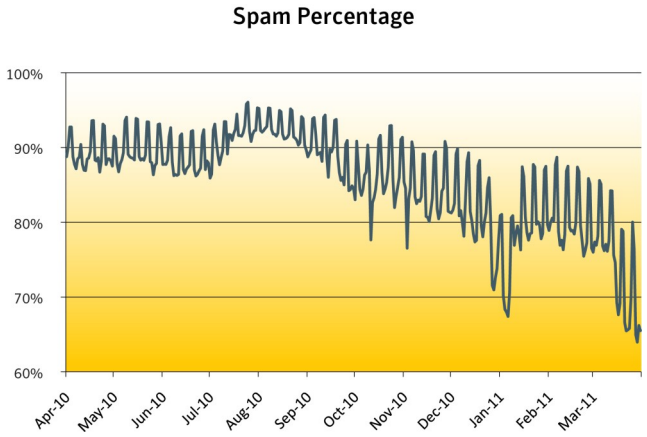
State of Spam & Phishing
A Monthly Report

April 2011 **Report #52**

Rustock is the hot topic of the spam threat landscape once again. After falling asleep for about two weeks a few months ago, Rustock was shut down on March 16, 2011. Rustock's shutdown had dramatic impact on the global spam volume. After increasing 8.7 percent last month, the average daily spam volume fell 27.43 percent in March. This drop in overall volume was paired with overall spam percentage. Meanwhile, spammers continued to take advantage of the earthquake in Japan to send spam, scam, malware, and phishing attacks.



Overall, spam made up 74.68 percent of all messages in March, compared with 80.65 percent in February.

The overall phishing landscape decreased by 22.71 percent this month. Automated toolkit and unique domains decreased as compared to the previous month. Phishing websites created by automated toolkits decreased by about 41.54 percent. Unique URLs decreased by 14.02 percent and phishing websites with IP domains (for e.g. domains like http://255.255.255.255) decreased by about 30.94 percent. Webhosting services comprised of 13 percent of all phishing, a decrease of 22.31 percent from the previous month. The number of non-English phishing sites saw a huge decrease by 58.22 percent. Among non-English phishing sites Portuguese, Italian and Spanish were the highest in March.

The following trends are highlighted in the April 2011 report:

- Rustock Shutdown
- Spammers' Take on the Earthquake in Japan
- Phishers Have No Mercy for Japan
- Fake Donations for New Zealand Earthquake Victims
- March 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	March	February	Change (% points)
Adult	<1%	<1%	No change
Financial	7%	5%	+2
Fraud	4%	4%	No change
Health	4%	6%	-2
Internet	52%	50%	+2
Leisure	10%	8%	+2
419 spam	8%	11%	-3
Political	<1%	<1%	No change
Products	12%	12%	No change
scams	2%	3%	-1

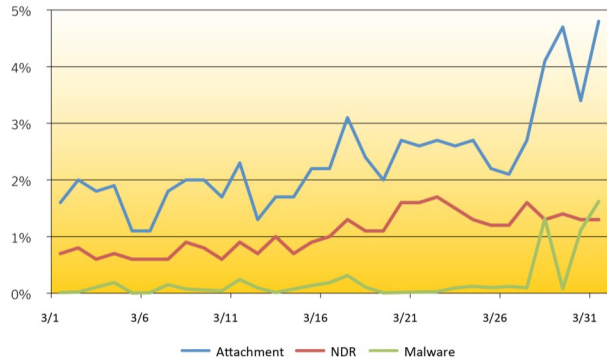
Spam URL TLD Distribution

TLD	March	February	Change (% points)
com	50.0%	56.9%	-6.9
ru	18.9%	18.1%	+0.8
info	15.7%	9.8%	+5.9
net	5.7%	3.9%	+1.8

Average Spam Message Size

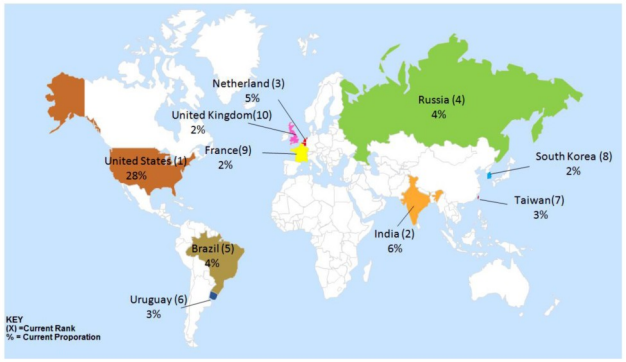
Message Size	March	February	Change (% points)
0-2kb	1.99%	1.81%	+0.18
2kb-5kb	68.28%	72.32%	-4.04
5kb-10kb	15.49%	16.10%	-0.61
10kb+	14.24%	9.77%	+4.47

Spam Attack Vectors



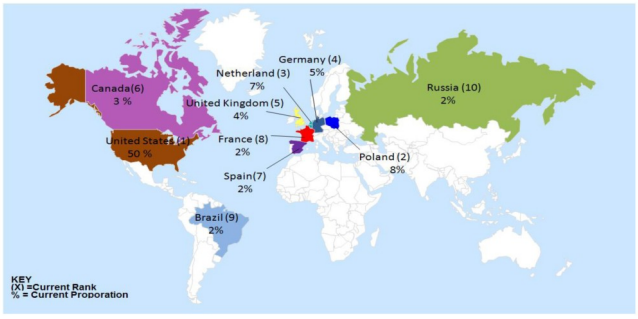
Metrics Digest

Spam Regions of Origin



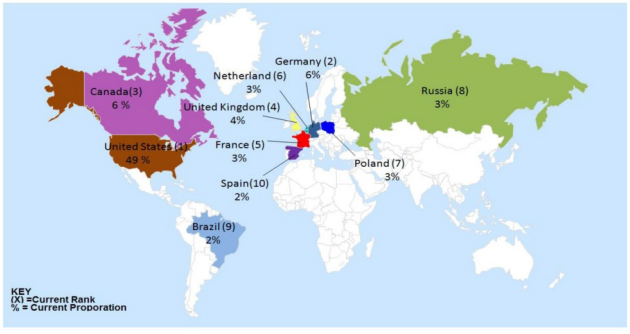
Country	March	February	Change (% points)
United States	28%	28%	No change
India	6%	5%	+1
Netherlands	5%	5%	No change
Russia	4%	4%	No change
Brazil	4%	4%	No change
Uruguay	3%	3%	No change
Taiwan	3%	Not listed	N/A
South Korea	2%	Not listed	N/A
France	2%	2%	No change
United Kingdom	2%	3%	-1

Geo-Location of Phishing Lures



Country	March	February	Change (% points)
United States	50%	52%	-2
Poland	8%	Not listed	N/A
Netherlands	7%	5%	+2
Germany	5%	3%	+2
United Kingdom	4%	4%	No Change
Canada	3%	7%	-4
Spain	2%	Not listed	N/A
France	2%	1%	+1
Brazil	2%	Not listed	N/A
Russia	2%	2%	No Change

Geo-Location of Phishing Hosts

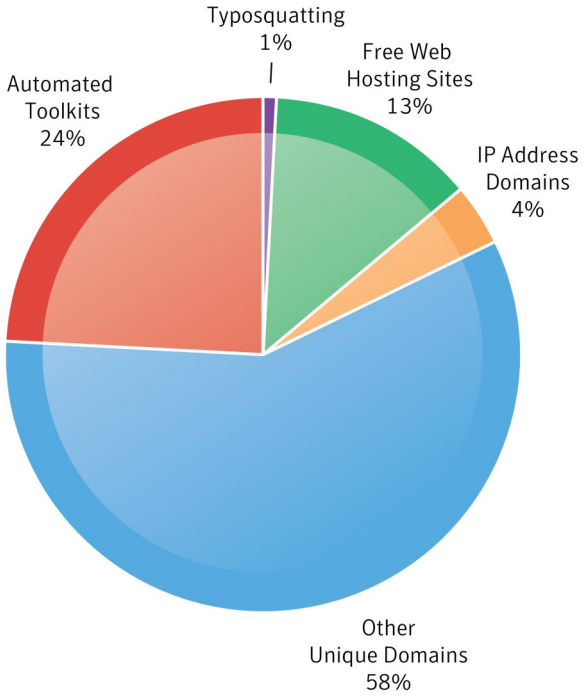


Country	March	February	Change (% points)
United States	49%	49%	No Change
Germany	6%	6%	No Change
Canada	6%	2%	+4
United Kingdom	4%	5%	-1
France	3%	2%	+1
Netherlands	3%	2%	+1
Poland	3%	Not Listed	N/A
Russia	3%	4%	-1
Brazil	2%	3%	-1
Spain	2%	Not Listed	N/A

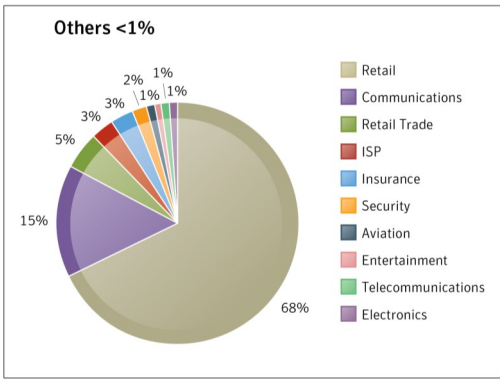
Metrics Digest

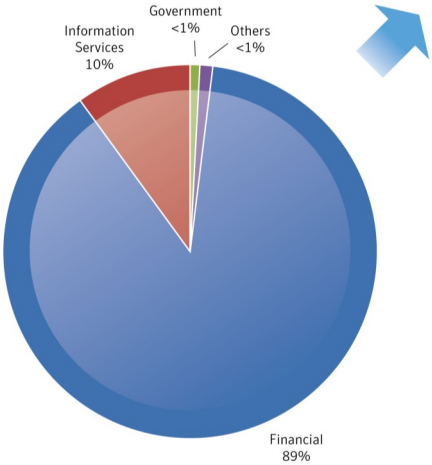
Phishing Tactic Distribution

Overall Statistics



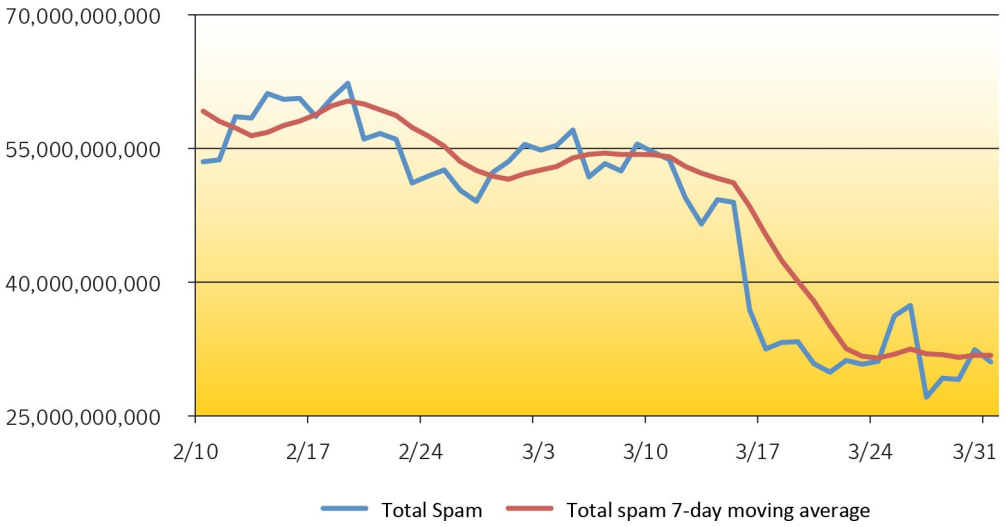
Phishing Target Sectors





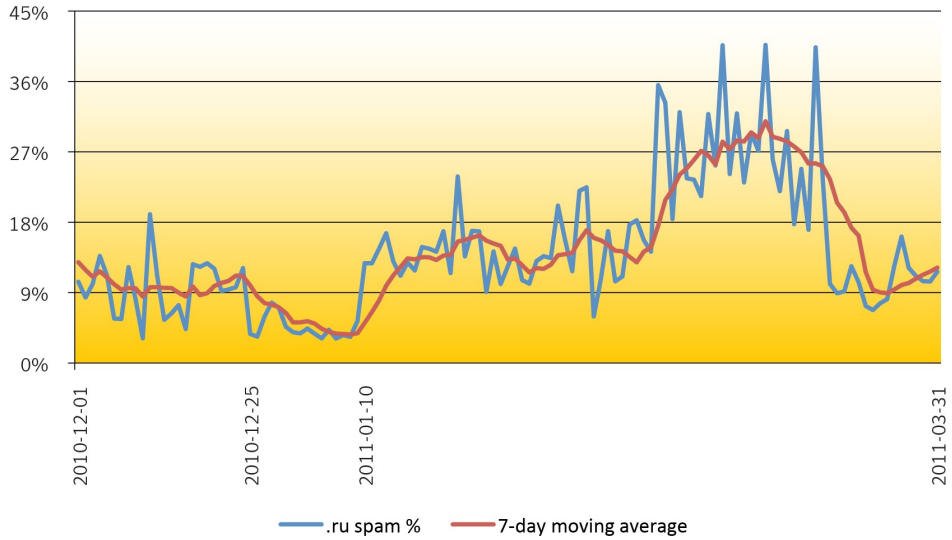
Rustock Shutdown

As Symantec noted in this blog, the global spam volume dropped significantly on March 16, 2011 due to Rustock's shutdown, an action led by the government in collaboration with Microsoft. The global spam volume fell 24.7 percent on March 16th compared to the previous day. On March 17, the volume fell another 11.9 percent. Since then, the volume has continued to stay low.



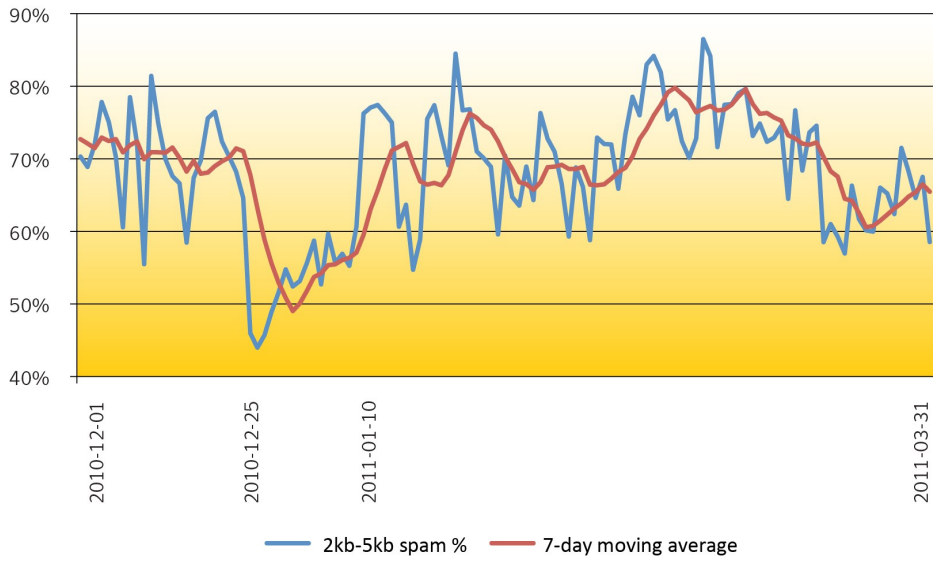
Rustock actually was dormant at the end of 2010. In this blog, Symantec discussed the Rustock botnet disappearing on December 25, 2010, and returning January 10, 2011. With this new shutdown, we now have two time periods to draw correlations in other metrics. As Rustock was one of the most prolific botnets in the world, the effect of its shutdown was seen on metrics other than spam volume.

The chart below shows the percentage of spam with .ru TLD URLs. When Rustock temporarily fell asleep late last year, the percentage of spam with .ru TLD URLs dropped, however, when the botnet came back, .ru TLD URL spam picked up in volume. Then on March 16, the percentage took a deep dive again.

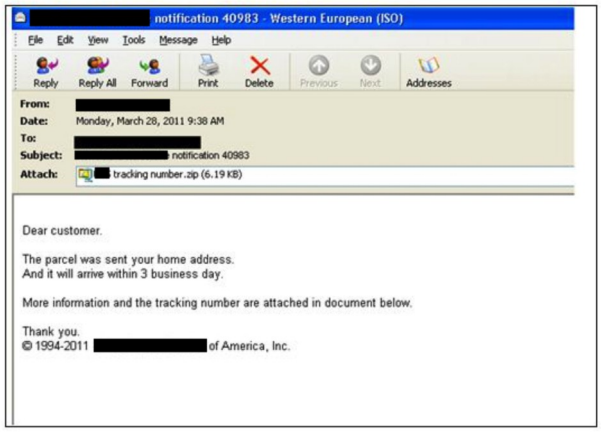


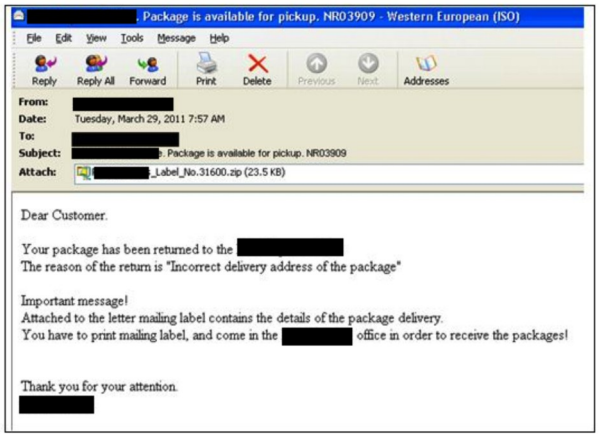
Rustock Shutdown (continued)

A similar trend can be seen in the message size bucket metrics. The chart below shows the percentage of spam message between 2 and 5 kilobytes.



Symantec also observed an increase in zip attachment spam towards the end of March, 2011. All of the observed samples are spoofed to appear as if they are legitimate delivery warnings or notifications from delivery service companies. The message text asks recipients to open the zipped executable file for further details or actions necessary to take delivery of the item.





Once the recipient downloads the compressed file, the following threats are installed (links open to Symantec's Security Response write-up on each threat):

- Trojan.FakeAV
- Backdoor.Cycbot
- Trojan.Sasfis

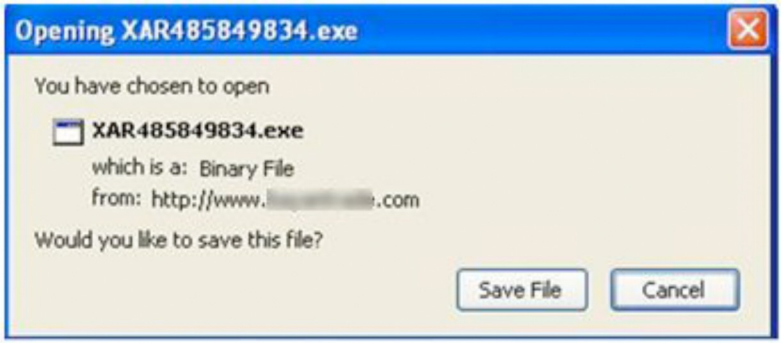
Even though one botnet has been taken down, it appears spammers are trying to rebuild their capacity once again.

Spammers' Take on the Earthquake in Japan

In previous natural disasters like the tsunami in Southeast Asia and the earthquake in Chile, spammers used those tragedies to their advantage by sending out malware, spam, scam, and phishing attacks. This trend continued with the massive earthquake that struck Japan last month.

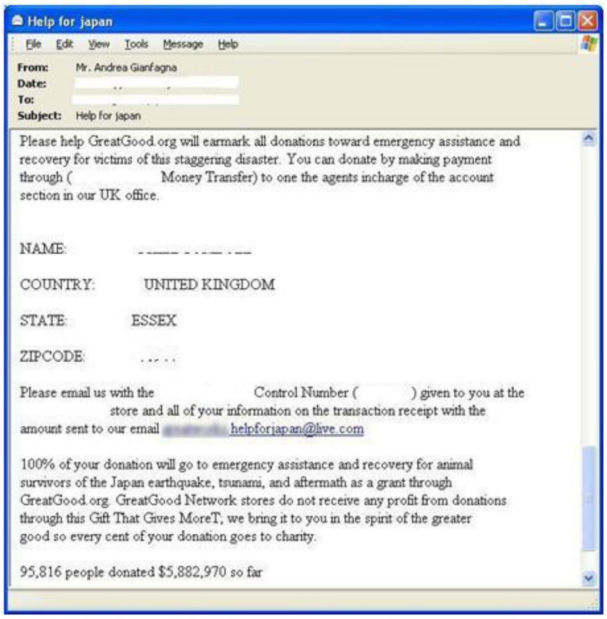
In this first example, the spammer tricks users by embedding what appears to be a video of the disaster.

However, it is just an image with a link that leads to malware. Once the link is opened, the user is asked to download and install an executable file that is malware related to a Brazilian banking Trojan. The link to the image hxxp://xxx.<removed>trade.com/globo.com.html leads the user to download the malware payload from the attacking machine. After it has been successfully installed, the malware gathers the user's Internet banking credentials and other sensitive information.



Spammers' Take on the Earthquake in Japan (continued)

The scammers have also been exploiting the relief efforts by sending 419 scam emails that have been prevalent ever since the natural disaster took place. In another variation of the Nigerian scam that has been observed recently, the fake message urges people to help the survivors of the earthquake and tsunami while the country is battling a nuclear crisis.


Help for japan

File Edit View Tools Message Help

From: Mr. Andrea Gianfagna
Date:
To:
Subject: Help for japan

Please help GreatGood.org will earmark all donations toward emergency assistance and recovery for victims of this staggering disaster. You can donate by making payment through (Money Transfer) to one the agents incharge of the account section in our UK office.

NAME:

COUNTRY: UNITED KINGDOM

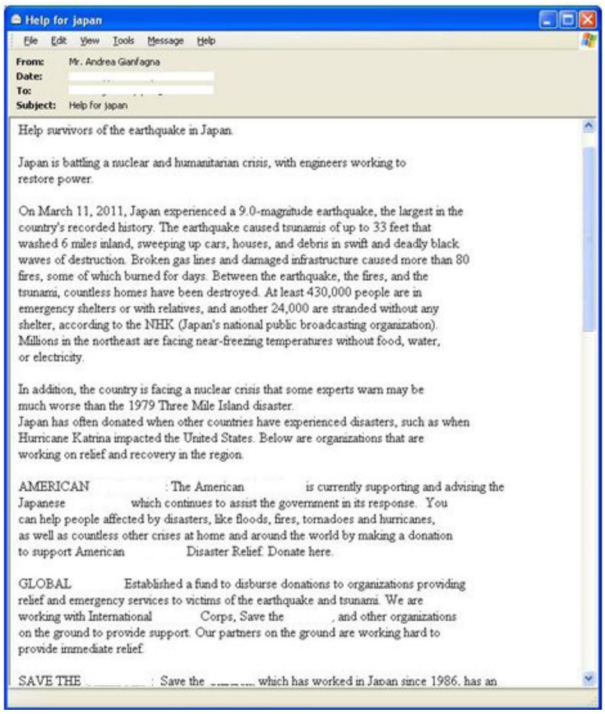
STATE: ESSEX

ZIPCODE:

Please email us with the Control Number ( ) given to you at the store and all of your information on the transaction receipt with the amount sent to our email helpforjapan@live.com

100% of your donation will go to emergency assistance and recovery for animal survivors of the Japan earthquake, tsunami, and aftermath as a grant through GreatGood.org. GreatGood Network stores do not receive any profit from donations through this Gift That Gives MoreT, we bring it to you in the spirit of the greater good so every cent of your donation goes to charity.

95,816 people donated $5,882,970 so far


Help for japan

File Edit View Tools Message Help

From: Mr. Andrea Gianfagna
Date:
To:
Subject: Help for japan

Help survivors of the earthquake in Japan.

Japan is battling a nuclear and humanitarian crisis, with engineers working to restore power.

On March 11, 2011, Japan experienced a 9.0-magnitude earthquake, the largest in the country's recorded history. The earthquake caused tsunamis of up to 33 feet that washed 6 miles inland, sweeping up cars, houses, and debris in swift and deadly black waves of destruction. Broken gas lines and damaged infrastructure caused more than 80 fires, some of which burned for days. Between the earthquake, the fires, and the tsunami, countless homes have been destroyed. At least 430,000 people are in emergency shelters or with relatives, and another 24,000 are stranded without any shelter, according to the NHK (Japan's national public broadcasting organization). Millions in the northeast are facing near-freezing temperatures without food, water, or electricity.

In addition, the country is facing a nuclear crisis that some experts warn may be much worse than the 1979 Three Mile Island disaster.
Japan has often donated when other countries have experienced disasters, such as when Hurricane Katrina impacted the United States. Below are organizations that are working on relief and recovery in the region.

AMERICAN : The American is currently supporting and advising the Japanese which continues to assist the government in its response. You can help people affected by disasters, like floods, fires, tornadoes and hurricanes, as well as countless other crises at home and around the world by making a donation to support American Disaster Relief. Donate here.

GLOBAL Established a fund to disburse donations to organizations providing relief and emergency services to victims of the earthquake and tsunami. We are working with International Corps, Save the , and other organizations on the ground to provide support. Our partners on the ground are working hard to provide immediate relief.

SAVE THE : Save the which has worked in Japan since 1986, has an

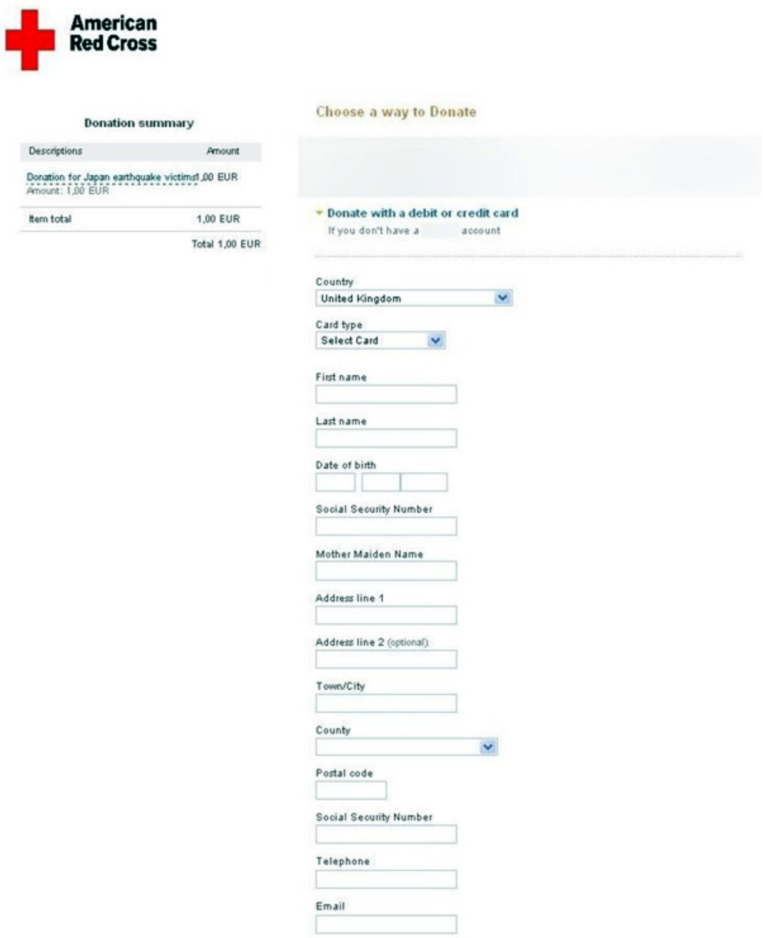
In addition to these messages, there were phishing attempts using the disaster. Please see the next section titled "Phishers Have No Mercy for Japan" for more details.

Symantec recommends that users reach out to the earthquake and tsunami victims through legitimate and secure channels.

Phishers Have No Mercy for Japan

On March 11, 2011, Japan faced its worst nightmare when a massive earthquake struck with a magnitude of 9.0. Nations all over the world are giving their support through aid to Japan. On the other hand, phishers tried to take advantage of this situation to steal and exploit well meaning donors.

Phishers Have No Mercy for Japan (continued)

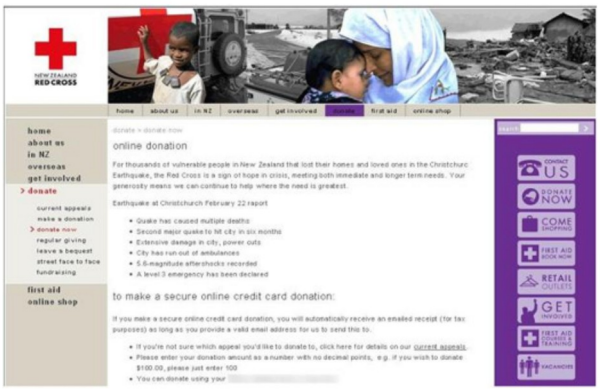


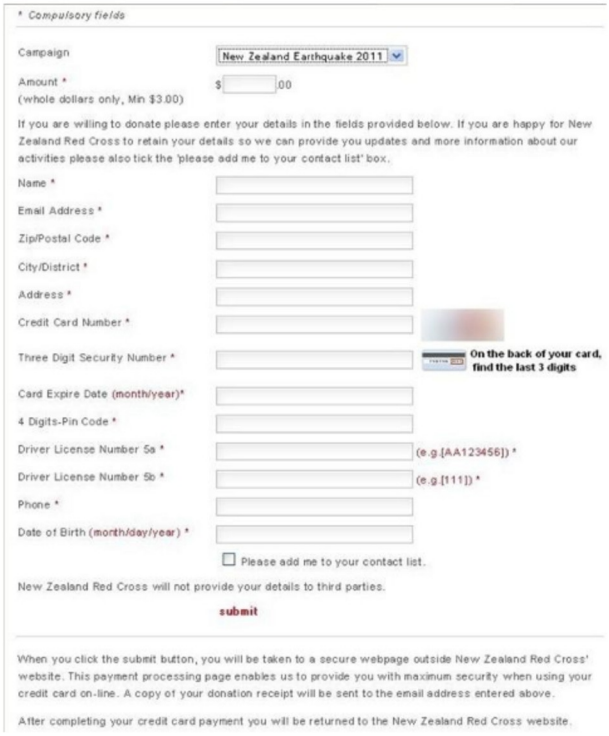
Symantec observed a phishing site that spoofed a popular payment gateway requesting a donation for Japan's earthquake victims. Phishers paid attention to every minute detail to make the page look like the legitimate brand's website. On the top left corner of the page, phishers used the logo of the American Red Cross, a humanitarian organization, to make it appear that the donation would be sent to them. A donation summary was highlighted towards the left of the phishing page that displayed an amount of one euro. A hyperlink, "Donation for Japan earthquake victims", was provided with the donation summary which redirected back to the same phishing page. Phishers fixed the considerably small amount of one euro in the hope that users would be willing to pay the amount without hesitation.

There were two options of payment that users were required to select . The first option was for customers of the brand, prompting them to pay from their account with the brand. The second option was to provide credit or debit card details. The card details asked for included card type, user name, date of birth, social security number, mother's maiden name, postal address, telephone number, and email address. After the required information was entered, the phishing site displayed a "Thank you" message. The phishing site was hosted on servers based in USA. Phishers have been devising strategies by which they can steal user's confidential information for financial gain; fake donations, as this one, have been common bait.

Fake Donations for New Zealand Earthquake Victims

On February 22, 2011, a massive 6.3 magnitude earthquake devastated the New Zealand city of Christchurch. As a result of this, thousands of people in New Zealand lost their homes. Fraudsters, as usual, were seen taking advantage of this by sending spam mails that request donations. In January, phishers had used the same ploy of asking for fake donations for victims of the Serrana floods.





The phishing site spoofed the Red Cross web-site for New Zealand and requested help from end users. First, the phishing site gave details of the earthquake, highlighting the extent of the damage in the city. Second, details on how to make a secure online donation were given. Users were notified that upon making an online donation, the user would receive a re-ceipt by email for tax purposes. There were three credit card services to choose from.

To make the donation, users were required to enter certain confidential information. The first field was a drop down menu from which the user had to select the cause for which the dona-tion would be made. The causes included New Zealand Earthquake 2011, Annual Appeal 2011, Australian Floods Fund, Landmine Appeal, Pacific Disaster Preparedness Fund, and General Fund Appeal.

The confidential information required was email address, postal address, credit card number, three digit security number, card expiration date, four digit PIN code, driver license number, and date of birth. Upon entering the required information, the Web page redirected victims to the legitimate Red Cross website. The phishing site was hosted on servers based in Wien, Aus-tria.

March 2011: Spam Subject Line Analysis

#	Total Spam: March 2011 Top Subject Lines	No of Days	Total Spam: February 2011 Top Subject Lines	No of Days
1	Re: ru girl	13	Find Out How You Can Start Making $6487 a Month At HOME	12
2	Re: ru girls	11	Re:	15
3	*Blank Subject line*	30	Sarah Sent You A Message	11
4	Re: viagrow	7	Save-0n-Cialis-Viagra-And-Many-Other-Meds-N0W	9
5	Re: Windows 7, Office 2010, Adobe CS5 …	6	*Blank Subject line*	15
6	Save-80%-On-Viagra-Levitra-And-Cialis	19	Have Great SEX And Save 80% Valentines Day Special	8
7	Hi!	30	Hookup 2 Night!	8
8	Hi.	30	Guaranteed Quality of Viagra Pills, Fast delivery and Low prices.	5
9	Hey!	30	Trusted Pharmacy >>> Viagra for Sale	5
10	Hey.	30	Viagra for Sale in our FDA Approved Drugstore. Guaranteed Quality of Pills, Fast delivery and Low prices.	6

A combination of online pharmacy, counterfeit software, and adult dating spam messages made up the top ten subject lines list in March, 2011.

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.