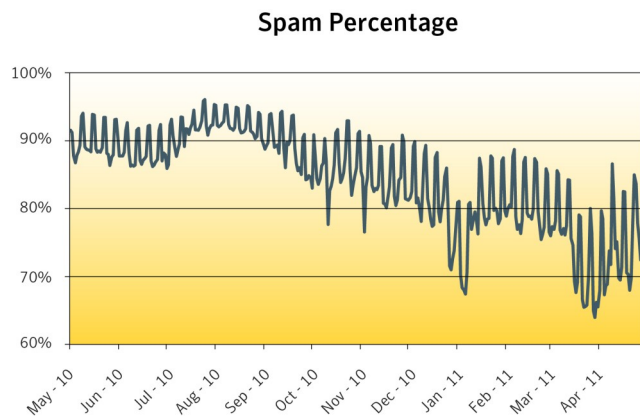


The unexpected raid and resulting death of Osama Bin Laden shocked the world. As always, spammers were quick to jump on this headline, and send a variety of spam messages leveraging the event. The “Fallout from the Death of Osama Bin Laden” section includes samples of some of the spam monitored in different languages.



The effect of the Rustock shutdown from the previous month continued this month.

After falling 27.43 percent in March, the average daily spam volume fell another 5.35 percent in April. Compared to a year ago, it is down 65.42 percent. Overall, spam made up 74.81 percent of all messages in April, compared with 74.68 percent in March. Going back a year, the percentage of spam was 89.22 percent in April 2010.

The overall phishing landscape increased by 15.61 percent this month. Automated toolkits and unique domains increased in comparison to the previous month. Phishing websites created by automated toolkits increased by about 26.19 percent, while unique URLs increased by 12.29 percent. Phishing websites with IP domains (for e.g. domains like <http://255.255.255.255>) also increased slightly by about 5.48 percent, and webhosting services comprised 12 percent of all phishing, an increase of 10.3 percent from the previous month. The number of non-English phishing sites saw an increase of 16.23 percent. Among non-English phishing sites Portuguese, Italian and Spanish were the highest in April.

The following trends are highlighted in the May 2011 report:

- Fallout from the Death of Osama Bin Laden
- Spammer Wishes You Happy Mother’s Day
- Let the Games Begin!
- Free Coins for Online FIFA Players
- April 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	April	March	Change (% points)
Adult	2%	<1%	+2
Financial	7%	7%	No change
Fraud	4%	4%	No change
Health	5%	4%	+1
Internet	51%	52%	-1
Leisure	11%	10%	+1
419 spam	6%	8%	-2
Political	<1%	<1%	No change
Products	11%	12%	-1
scams	2%	2%	No change

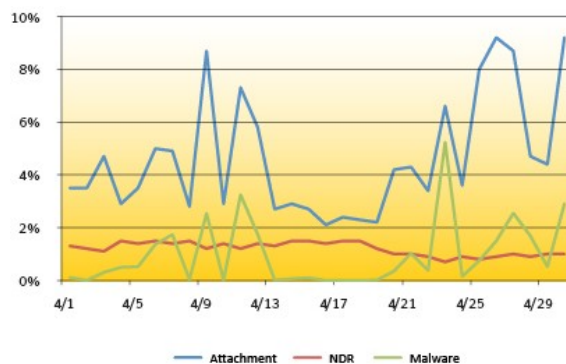
Spam URL TLD Distribution

TLD	April	March	Change (% points)
com	55.0%	50.0%	+5.0
info	18.5%	15.7%	+2.8
ru	10.1%	18.9%	-8.8
net	6.9%	5.7%	+1.2

Average Spam Message Size

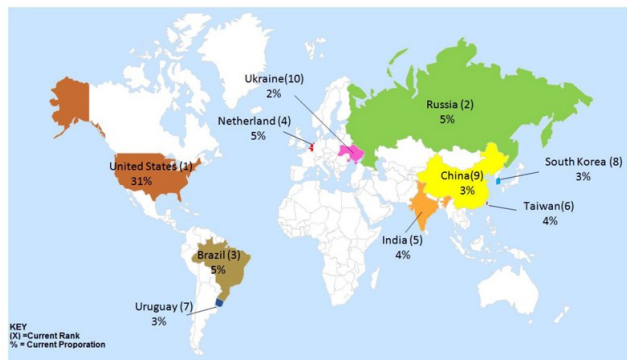
Message Size	April	March	Change (% points)
0-2kb	1.30%	1.99%	-0.69
2kb-5kb	68.29%	68.28%	+0.01
5kb-10kb	16.18%	15.49%	+0.69
10kb+	14.23%	14.24%	-0.01

Spam Attack Vectors



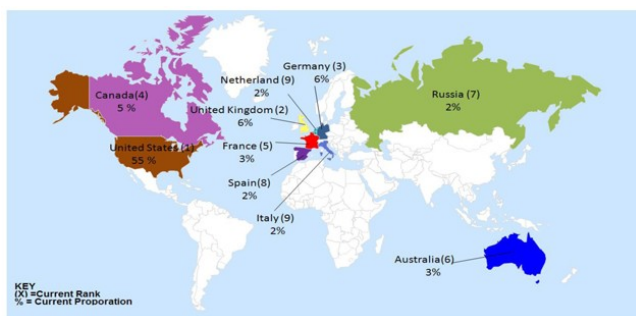
Metrics Digest

Spam Regions of Origin



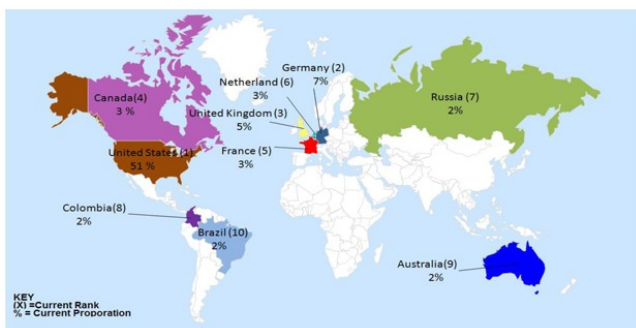
Country	April	March	Change (% points)
United States	31%	28%	+3
Russia	5%	4%	+1
Brazil	5%	4%	+1
Netherlands	5%	5%	No change
India	4%	6%	-2
Taiwan	4%	3%	+1
Uruguay	3%	3%	No change
South Korea	3%	2%	+1
China	3%	Not listed	N/A
Ukraine	2%	Not listed	N/A

Geo-Location of Phishing Lures



Country	April	March	Change (% points)
United States	55%	50%	+5
United Kingdom	6%	4%	+1
Germany	6%	5%	+1
Canada	5%	3%	+2
France	3%	2%	+1
Australia	3%	Not Listed	N/A
Russia	2%	2%	No Change
Spain	2%	2%	No Change
Netherlands	2%	7%	-5
Italy	2%	Not Listed	N/A

Geo-Location of Phishing Hosts

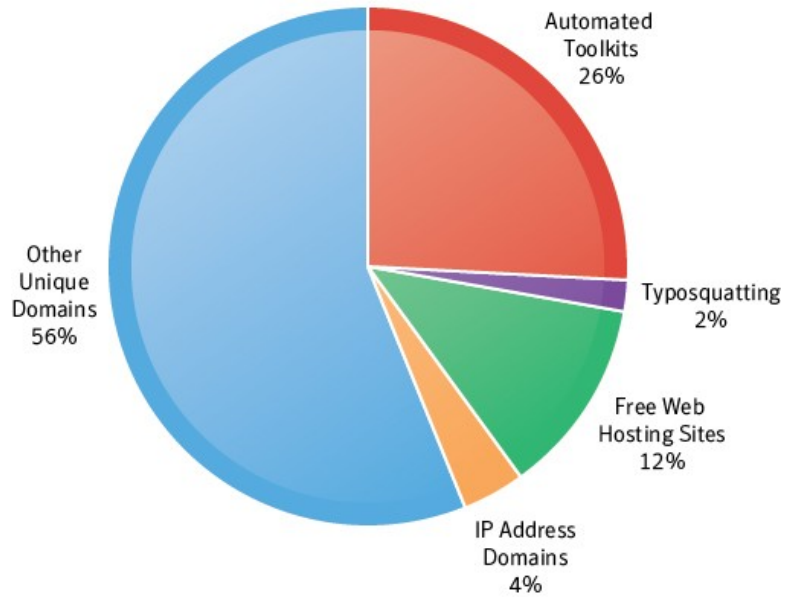


Country	April	March	Change (% points)
United States	51%	49%	+3
Germany	7%	6%	+1
United Kingdom	5%	4%	+1
Canada	3%	6%	-3
France	3%	3%	No Change
Netherlands	3%	3%	No Change
Russia	2%	3%	-1
Colombia	2%	Not Listed	N/A
Australia	2%	Not Listed	N/A
Brazil	2%	2%	No Change

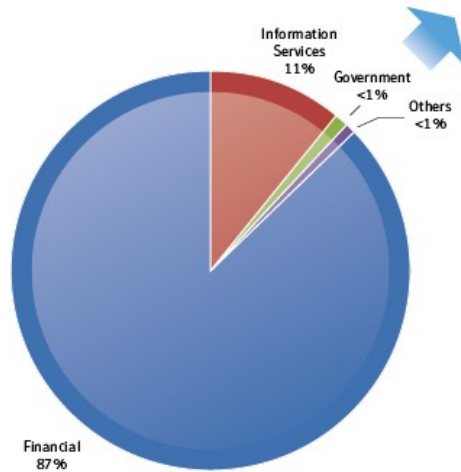
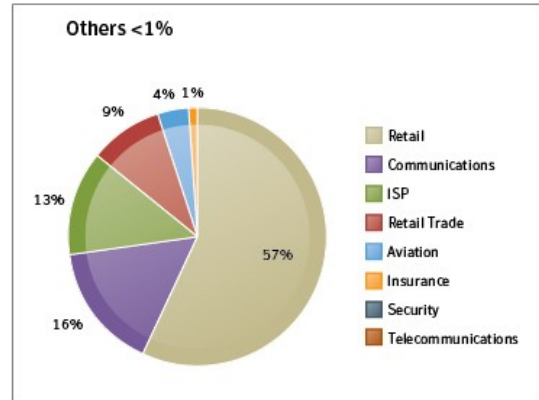
Metrics Digest

Phishing Tactic Distribution

Overall Statistics



Phishing Target Sectors



Fallout from the Death of Osama Bin Laden

Osama Bin Laden was killed by a CIA-led operation at a mansion in Abbottabad, north of Islamabad. News targeting famous/notorious personalities are often used in email scams. In this spam sample, the message is poisoned using the news of Osama's death. The news snippet is glued in an HTML <title> tag which is invisible to the end user. This is most likely due to the fact that the spammer uses legitimate news feed to randomize content in the message.

```
<title>
Osama Bin Laden was killed not by a drone strike, but up close during
a firefight with U.S. troops. He was not living in a cave when he
died, but in a million-dollar mansion with seven-foot walls just 40
miles from the Pakistani capital, where U.S. forces killed him Sunday.
</title>
```

The link provided in the message has nothing to do with the news and directs the user to a promotion site as shown in the image here (right).

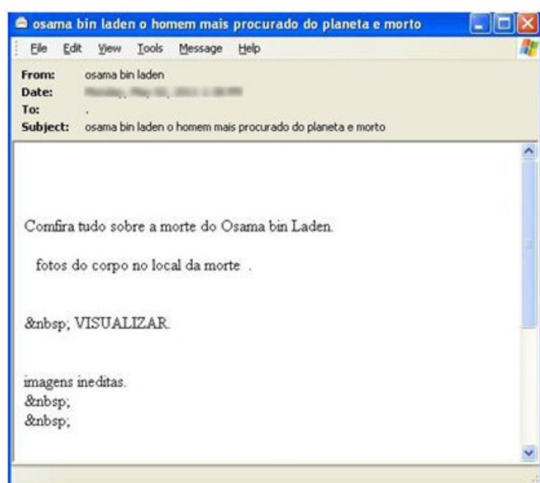


Another spam sample (below) is a typical 419 scam message where the phrase "OSAMA IS DEAD" is used at the end of the subject line "Subject: GOODNEWS FROM ROBERT SWAN MUELLER III (OSAMA IS DEAD)." Internet users may be curious enough to read each and every news item related to the operation carried out against Osama.



We also saw related spam attacks in different languages. In this Portuguese spam sample (see next page), the message claims to show unseen footage at the time of Osama's death. It seems that the spammer failed to add the malicious link in the message. Historically we've seen messages such as the one shown below perform malicious activity in the form of downloading binaries and infecting the computer.

Fallout from the Death of Osama Bin Laden (continued)



Subject: osama bin laden the most wanted man on the planet killed
It is confirmed that Osama bin Laden is dead
Photos of dead body.
VIEW
Unseen footage.

Following a historical pattern, we observed more legitimate messages than spam immediately following the death. After 24-48 hours however, we saw more targeted and sophisticated spam attacks leveraging this event. In this example, the spammer spoofed a major news organization and sent a message claiming to show uncensored photos and videos from the raid.



Translation:

Osama bin Laden he is dead (photos and videos shocking), confirmed by U.S. sources - World - [redacted]

Fallout from the Death of Osama Bin Laden (continued)

The phishing site shows an auto-running Bin Laden related video in an iframe and asks the user to click on a link to download a “complete” video. Clicking on that link forces the download of an .exe file that is detected as [Downloader](#):



Symantec’s Global Intelligence Network observed multiple malicious spam samples in a variety of languages including Portuguese, French, and Spanish. The links in this spam email dump download a file named 'Downloader' onto the victim’s machine, which in turn downloads the actual malware. Further analysis of these attacks shows that most of the malicious attacks have originated from Brazil, Europe, and the United States. Below is a list of the subject lines used in these malicious attacks, which refer to videos and photos of Osama Bin Laden:

Subject: Veja Video em que OSAMA BIN Laden aparece segurando jornal com a data de hoje e desmente sua possivel morte relatada por OBAMA .

Subject: FW: Incrive! video Osama Bin Laden sendo morto!

Subject: Video proibido mostra momento da execucao de obama

Subject: Fotos Verdadeiras de Osama Bin Laden Morto!

Subject: See video in which Osama Bin Laden is shown holding a newspaper with today’s date and disprove his possible death reported by OBAMA.

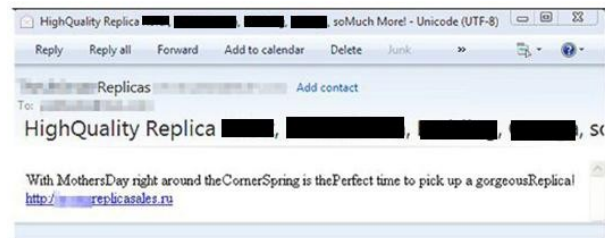
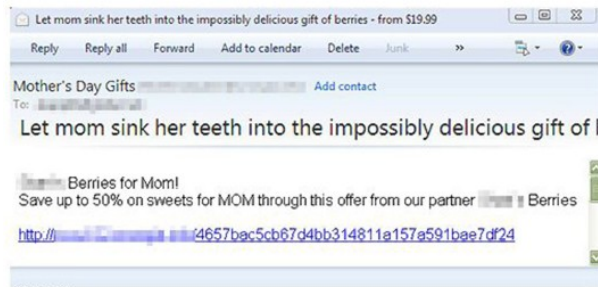
Subject: FW: Incredible video Osama Bin Laden is dead!

Subject: Video shows moment of execution prohibited obama

Subject: True Pictures of Osama Bin Laden Dead!

Spammer Wishes You Happy Mother's Day

Mother's Day has presented spammers with a good opportunity to send massive spam campaigns promoting a variety of products. While there were other headline-grabbing events (like the death of Osama Bin Laden) that spammers could use, they continued to exploit this holiday as well.



Let the Games Begin!

Gone are the days when phishing targeted financial brands alone. Phishers today are eyeing several other sectors to steal users' confidential information. For the past few months, the gaming sector has increasingly been a target for phishers. Symantec is actively keeping track of these phishing sites that spoof gaming brands.

So what's so lucrative about phishing for gaming site credentials? Gaming sites are popular with young generations who are passionate about playing and winning more and more games. Many of these gaming sites have a section for paid members that contain members' exclusive games and added features. The primary motive of phishers is to lure users with the hopes of stealing their credentials to gain access to the members' section. Since these credentials are in high demand, phishers also intend to sell stolen usernames and passwords on the Internet.

Let the Games Begin! (continued)

The following are some noteworthy statistics of phishing on gaming sites for April 2011:

61 percent of the phishing on gaming sites were hosted on free Web hosting sites.

About 17 percent of the phishing on gaming sites utilized typosquatting domains (Typosquatting refers to the practice of registering domain names that are typo variations of popular Web sites).

There were several phishing sites in non-English languages including Swedish, Spanish, Italian, Russian, Portuguese, Dutch, and French.

Free Coins for Online FIFA Players

In the past couple of months, Symantec observed phishing sites that spoofed online FIFA games. The legitimate game is played by forming a team of footballers purchased with coins. The more games you win with your team, the more coins you gain. The popular and more skilled footballers demand a higher number of coins.

The phishing campaign was launched with fake offers of free coins to lure online FIFA players. One of the phishing sites was purportedly from a player who sympathized with end users who struggle with the game. The phishing site contained a message from this fictitious player which expressed the embarrassment one goes through for having a team of low profile footballers. The message explained that the site would help players generate free coins so that they could form a more expensive team of footballers. The phishing site prompted users to login with their email address and password to gain up to 10,000 free coins per day. The phishing pages featured popular footballers such as Wayne Rooney, Ronaldinho, Frank Lampard, and Xavi, giving the impression that one could buy these players upon generating the free coins. If end users had fallen victim to the phishing site, phishers would have successfully stolen their information for identity theft.

HELLO!

Welcome to the FREE coin generator, the fastest and easiest way to perform miracles upon your opponents and, even better, friends.

All it needs is your EA information to start the stages of transferring the coins over. This may take up to 2 hours transferring to your account, but while you are waiting you could spend it figuring out the best team you could buy!

I was a player who was barely struggling to get good OOLD players and I know what it feels like to be embarrassed about the team you have, so I want to help all those players out there good or bad!

If you think that your team needs that little bit extra or you are just lacking the quality then please feel free to use this website. Any queries or questions feel free to email me on: rooney11@fifa11.com

This is all I can do, so thank you for your time and enjoy the FIFA 11 team we all must wish with your coins.



Please select the options you require for the ultimate FIFA 11 Ultimate Team Experience!

Email (EASPORTS)*

Password (EASPORTS)*

Amount of Coins *




Free 10,000 coins everyday

Sign In

Email:

Password: *

Free Coins for Online FIFA Players (continued)



Free coins
and
duplicated

EA
SPORTS

EA account Email *

EA account Password *

Coins 1-110,000 *

Submit

The following are some noteworthy statistics observed about the phishing attack:

- 89% of the phishing sites were hosted on free web hosting sites.
- 5% used IP domains (for example, domains that look like 255.255.255.255).
- 13% were typosquatting. (Typosquatting refers to the practice of registering domain names that are typo variations of popular Web sites.)
- The country code top level domains (ccTLDs) most utilized was of Tokelau (.tk) and United Kingdom (.uk) with 3% and 0.4% of the phishing attack, respectively.

April 2011: Spam Subject Line Analysis

#	Total Spam: April 2011 Top Subject Lines	No of Days	Total Spam: March 2011 Top Subject Lines	No of Days
1	Re: ru girl	24	Re: ru girl	13
2	<i>Blank Subject line</i>	30	Re: ru girls	11
3	Re: Windows 7, Office 2010, Adobe CS5 ...	12	<i>Blank Subject line</i>	30
4	Save-80%-On-Viagra-Levitra-And-Cialis	14	Re: viagrow	7
5	Express Delivery system notification	7	Re: Windows 7, Office 2010, Adobe CS5 ...	6
6	Re:Hi	29	Save-80%-On-Viagra-Levitra-And-Cialis	19
7	Re: sale viagrow	7	Hi!	30
8	Do you have problem with ErectileDysfunction? ViagraCan help you and make sure it is a unique drug for treatingImpotence.	16	Hi.	30
9	BuyVIAGRA (SildenafilCitrato) Generic Tablets – Online Drugstore. ViagraCan help your ErectileDysfunction	16	Hey!	30
10	Find Out How You Can Start Making \$6487 a Month At HOME	19	Hey.	30

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

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. Deselect 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.