Monthly Spam Report, April 2008

Contributors

Kelly Conley
Manager ESG
Symantec Security Response

Sammy Chu
Security Response Technician
Symantec Security Response

Shravan Shashikant
Pr. Business Intelligence Analyst
Antispam Engineering

Charles Adams
Sr. Business Intelligence Analyst
Antispam Engineering

Rui Brito
Sr. Business Intelligence Analyst
Antispam Engineering

Jessica Lin
Security Response Analyst
Symantec Security Response

Dylan Morss
Manager
Antispam Engineering

Kevin X Yu
Security Response Lead
Symantec Security Response

Joe Krug
Pr. Business Intelligence Analyst
Antispam Engineering

Robert Vivas
Sr Security Response Lead
Symantec Security Response

Amanda Grady
Customer Response Analyst
Antispam Engineering

Niall O’ Reilly
Security Response Analyst
Symantec Security Response
Monthly Spam Landscape

Despite recent high profile spam litigation, including “Spam King” Robert Soloway’s guilty plea and the Virginia Supreme Court’s decision to uphold its conviction of Jeremy Jaynes, the spam menace continued in March 2008 averaging 81% of all email, and peaking at all-time highs of nearly 88%. The United States also continued its dominance as the prominent country of origin for spam emails, accounting for nearly one quarter of all spam distribution.

Highlights from this month included:

- **Spammers Bounce Back.** In what should be considered a wake-up call to mail transfer agent (MTA) administrators, spammers are taking advantage of the generosity of MTA programs and using the practice of backscatter to forge sending email addresses and bounce massive volumes of emails around the globe until they’re received into inboxes.

- **EMEA Spammers Get Social.** Spammers in select EMEA regions have been heavily promoting social networking sites—one example reached more than two million Symantec customers.

- **Spammers Offer Virus, Not Tax Day Refund.** As the clock ticks down to April 15, Symantec has observed an increase in malicious spam messages spoofing the IRS or popular programs like TurboTax.

- **Attachment Spam Makes a Weak Attempt at Comeback.** While pharmaceutical spam is always a popular angle coming in all shapes and sizes, spammers reverted back to the tactic of using attachments—Zip files in this particular case. While Zip files are often used to evade spam filters, this was a weak attempt accounting for only .5% of all spam attacks in March.

- **‘419 Spammers’ Aim for 2010 South African World Cup.** In the latest twist on the infamous 419 Nigerian Spam Scam, spammers are now informing recipients they’ve won $2 million in promotion of the 2010 South African World Cup. All they must do is provide personally identifiable information to process the funds.

- **Hall of Shame: Phone Sex Sells.** For two months in a row, Chinese spammers have recognized the ‘sex sells’ cliché, this time pointing to a phone sex service.
Percentages of Email Identified as Spam

**Defined:**

Worldwide Internet Mail Gateway Spam Percentage represents the number of messages that were processed and classified as spam versus the total number of messages processed when scanned at the mail gateway. This metric represents SMTP layer filtering and does not include the volumes of email detected at the network layer.

A trend line has been added to demonstrate a 7-day moving average.
Global Spam Categories

**Defined:**
Spam category data is collected from classifications on messages passing through the Symantec Probe Network.

**Global Category Count Last 30 Days**

- Financial: 15%
- Adult: 9%
- Fraud: 6%
- Scams: 10%
- Health: 11%
- Internet: 20%
- Leisure: 7%
- Products: 22%
Category Definitions

• **Product Email attacks** offering or advertising general goods and services. Examples: devices, investigation services, clothing, makeup

• **Adult Email attacks** containing or referring to products or services intended for persons above the age of 18, often offensive or inappropriate. Examples: porn, personal ads, relationship advice

• **Financial Email attacks** that contain references or offers related to money, the stock market or other financial “opportunities.” Examples: investments, credit reports, real estate, loans

• **Scams Email attacks** recognized as fraudulent, intentionally misleading, or known to result in fraudulent activity on the part of the sender. Examples: Nigerian investment, pyramid schemes, chain letters

• **Health Email attacks** offering or advertising health-related products and services. Examples: pharmaceuticals, medical treatments, herbal remedies

• **Fraud Email attacks** that appear to be from a well-known company, but are not. Also known as “brand spoofing” or “phishing,” these messages are often used to trick users into revealing personal information such as email address, financial information and passwords. Examples: account notification, credit card verification, billing updates

• **Leisure Email attacks** offering or advertising prizes, awards, or discounted leisure activities. Examples: vacation offers, online casinos, games

• **Internet Email attacks** specifically offering or advertising Internet or computer-related goods and services. Examples: web hosting, web design, spamware

• **Political Messages** advertising a political candidate’s campaign, offers to donate money to a political party or political cause, offers for products related to a political figure/campaign, etc. Examples: political party, elections, donations
Countries of Origin

Defined:
Country of origin represents the percentage of spam messages reported coming from certain countries in the last 30 days.

Top Ten Countries of Origin
Spam Regions of Origin

Defined:
Region of origin represents the percentage of spam messages reported coming from certain regions in the last 30 days.

![Chart showing spam regions of origin]

- EMEA: 45%
- APJ: 25%
- NAM: 17%
- LAM: 13%
Spammers Bounce Back

There has been an increase in bounce messages due to recent spam attacks not reaching the recipient listed in the To: header. Although many of the originating IP addresses are from across the globe, the content of the original spam messages is in Russian. Each wave of messages contains images as well as text that change regularly, usually once or twice a day. This mail is being scattered across the Internet via the tried and true practice of backscatter.

Backscatter occurs when spammers forge sending email addresses and insert them into the From: header of their spam messages. For example, have you ever seen spam from yourself to yourself? It’s the same principle. Quite often spammers are also either forging the recipient or To: header as well, or just testing out lists of email addresses to verify existence. Either way, the sent email will end up going somewhere, anywhere, but not returned to the spammer. The availability of email processing programs that will send back full messages to the apparent sender of an email creates a spam attack vector that is used time and again by spammers.

Spammers take advantage of MTA programs, which can be configured to send back not only a list of failed recipient addresses, and an explanation why each address failed, but also a copy of the original message in its entirety. Spammers can then bounce their messages around the Internet until they end up in someone’s spam folder, or worse, inbox. Since many users want to know if they have accidentally misspelled their friends’ email addresses by getting a failed recipient message, these bounced messages will often go unblocked due to configurations of antispam filters.

This is what the spammer sends:

This is what you get:
Spammers Get Social

The rise of social networking Web sites has drawn many Internet users to join in hopes of interacting with friends and acquaintances. In the EMEA region in March, two social networking spam attacks were observed.

In the example below, the message written in French is crafted to look like a message from a friend, inviting the recipient to visit “my personal page.”

Date: 26 March 2008 09:43
To: xxx
Subject: Salut!

Salut ! Ca va ?
Dis moi j’ai découvert ce site... www.bahu.com
S’rieux tu devrais venir dessus ... Ya tous les étudiants de France et Belgique !!!!
Sur ma page perso, j’ai mes photos, ma zik, mes vidéos, mes amis, mes clubs…
Alors rejoins-moi vite dessus !!

@toute
Spammers Offer Virus, Not Tax Day Refund

As first reported in the February Symantec State of Spam report, spammers continue to disguise themselves as the IRS, dangling an offer of a tax refund to unwitting recipients. The email offers a refund once you input your credit card information into their site—a site that does not bear the IRS URL. The site is fraudulent and nothing more than a collection tool for credit card and other personal information. As the April 15 Tax Day approaches in the US, Symantec has observed some additional spam trends regarding the tax season with the spam messages being of a more sinister type, directing recipients to download a virus.

In one example, the spammer indicates that a new law requires you to download tax software. There is no existing law stating that you need a computer to complete your tax returns. If that wasn’t enough of a red flag, the site that you actually download the “software” from is not a government site. Instead, it is merely an IP address.

In the body of the message, the URL does appear to be a legitimate government site being “irs.gov/softwareupdate.” However, when you click it, you are redirected to the IP address hosting the virus. Upon going to the official IRS site (irs.gov) and manually typing in irs.gov/softwareupdate, the “The requested page does not exist. Please check your URL.” error message is displayed.

At first glance, this message does appear to be legit, at least on the surface, carrying legitimate-looking “From” and “Subject” lines, as well as a seemingly credible link referencing the IRS:

From: "IRS"
Subject: IRS Notice @.net

Dear Tax Payer,
As part of new requirements from the IRS, all U.S. Citizens are required by law to update their computers with new tax software.
To begin the update, please visit irs.gov/softwareupdate and click "Open" when asked to begin the download.
After doing so, no further action is required on your part.
Thank you for your cooperation.
Sincerely,
IRS.GOV
Another example is utilizing the popular tax software, TurboTax. Here the spammer is also advising the recipient to download software updates to comply with new IRS requirements. The first red flag would be the “From” line which does not look like it originates from the business as it contains a “.cn” domain.

The second red flag is that the URL which the “turbotax.com/update” resolves to does not resolve to the TurboTax official Web site, but instead to an alphanumerically randomized URL consisting of a blank page with a pop-up that asks you to download a suspicious file.

| From: "TurboTax Support"  
| Subject: New TurboTax Update  
| Dear TurboTax User,  
| Due to changes in IRS requirements, we are requiring all TurboTax users to update their software to the current version.  
| The process takes less than 30 seconds, and is done completely in the background.  
| To begin the update, please visit turbotax.com/update and click "Open" when asked to begin the download.  
|  
| After doing so, no further action is required on your part.  
| Thank you for your cooperation regarding this matter.  
| Sincerely,  
| TurboTax Customer Support |

Email users are cautioned to be alert during tax season as spam messages are created to steal personal information or spread viruses. In the above samples, a user should be able to identify that the emails are not legitimate by analyzing them using common sense and a few best practices. Do not download anything from an email on your computer unless you are sure that the email is genuine and comes from some one or some company that you know and trust. Also, be sure to use a mail security technology that offers up-to-date protection against the complete suite of security threats. You can always call a company’s support line from a phone number retrieved on their official site with details of the message and ask them to confirm its validity.
Attachment Spam Makes a Weak Attempt at Comeback

Pharmaceutical spam is often observed in many shapes and sizes and this month arrived in a Zip file. Upon opening the spam attack, a single line of text was revealed such as: “Smart in bed games” and “She wants you more now.” The Zip file contained an HTML page, which revealed information regarding the procurement of pharmaceutical products.

Have the hottest sex ever!
Use Viagra!!!!

http://xxxxx.com

Instant shipping and quality are guaranteed!

While the use of Zip files by spammers to promote their products was intended to evade spam filters, this attack was a low volume attack accounting for less than 0.5% of all spam attacks in March.
'419 Spammers’ Aim for 2010 South African World Cup

Scam emails now account for 10% of all spam emails. Traditionally 419 spammers used the premise of unclaimed riches to lure their victims, but now they have also started using the 2010 South African World Cup as a ruse to entrap their victims. Spammers are requesting email recipients download a Rich Text File (RTF), claiming the attachment file is a winning lottery ticket notification.

Sample attachment below:

| Congratulations your email is among the two lucky winning that won USD$2,000,000.00(Two Million United State Dollars) Each in the just concluded draw held to promote South African 2010 World Cup, sponsored by British American Tobacco Companies South Africa ca. for prize claiming. Call Mr. Mark Thambo on this phone number +27 83 569 8703. or email him on mthambo7@yahoo.it Your winning numbers No: 2,4,17,33,36,45 with bonus No:35. Winning numbers for Wed -Feb-27,2008 draw, visit: http://www.canada.com/findit/lotteries/results.aspx?id=6 And also provide the following information for the processing of your winning fund. NAME: ADDRESS: NATIONALITY: SEX: AGE: PHONE/MOBILE: FAX: OCCUPATION: COMPANY: Your Email Attached to Ticket No: (7Y06ZA) and ballot No: WL02/A) Yours Faithfully, Management. |
Hall of Shame: Phone Sex Sells!

Finally, one of the bizarre spam emails observed this month included a flurry of emails advertising a phone sex line.

```
From: "張雅雯" <a45g9qg975f@xxxx
Subject: 激情的夜□...期盼□的到來...

KzYluEOFSNq3HJPkAnQlb6Vh8I5PJHJCMaaFlrKZGJaR
56535551747654265239066678665967739632978491169

我是辣美眉，想找人聊天□?

喜歡重口味的台灣狼，照過來看□

我最喜歡聊天、唱歌、看電影若□還不錯歡迎來找我！

激情的夜□...期盼□的到來...

請撥打0941530208(每30秒2元)

bWzKPDINlwBES0vfiKP2nxTQ6dU6U3Cuq8KWfVEzB8JjB
7WS7plrZ5cvBzmnjas6vJkUBy57hOKVdv6lIfZDzRDX
7nKQhOTgK3OuiE78UYRpy97jOxPAMZIL88lO0sCrbLfk
FXmUwbaGCcayry71T3aC8uh5VULieAVleEmegfQbuMo

Translation:
From: Zhang Yawen <a45g9qg975f@xxx
Subject: I am waiting for you…

I am hot and sexy, want to talk?

If you are looking for something extreme

I like talking, singing.........

I am waiting for you…

Please call 0941530208($2 per 30 second)