Monthly Spam Landscape

Few people in the industry are celebrating spam's 30th birthday during the beginning of May this year, however the email menace has afforded us an opportunity to review just how prominent it has become. During the month of April, 80% of all email was spam, with that number jumping as high as 87% at times.

Highlights from the report include:

– NDR Spam Bounces Away...For Now
– Spammers “Google” the Google Brand
– Spammer’s Who’s Who Network
– Spear Phishing for a Subpoena
– Resist the Calendar Invite From Spammers
– Spammers: The New Movie Casting Agents
– IRS Phishing Tricks You into ‘Biting’ the Bait
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.

Email Internet Spam Percentage

The trend line demonstrates 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: 17%
- Scams: 12%
- Products: 23%
- Leisure: 10%
- Internet: 16%
- Health: 9%
- Fraud: 7%
- Adult: 6%

Total: 100%
Category Definitions

Products
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
Regions of Origin

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

**Region of Origin**

![Bar chart showing regions of origin](chart.png)
NDR Spam Bounces Away...For Now

As reported in the April State of Spam report, Symantec observed an increase in the number of NDR (Non Delivery Report) bounce messages sent in response to spam with forged headers. Spammers are taking advantage of systems that will return full message copies with delivery failure reports, out of office messages, and mail box quota messages. The format of these messages has been changing, indicating that there is a deliberate attempt to use known systems to bounce spam instead of using the first sent message attempt to deliver the payload. NDR spam averaged at 2.7% of spam in March and 3.7% in April. However, as April came to a close, NDR spam accounted for less than 2% of all spam.

Percentage NDR Spam
Spammers “Google” the Google Brand

For some time, spammers have used reputable brands to try and deliver spam and phishing messages to end-users. In the last year, Google has become a favorite target for some spammers. In November 2007, Symantec reported the emergence of a technique where spammers manipulated Google’s advanced search query and the “I’m feeling lucky” option to direct users to a spam site. In February 2008, Symantec reported that spammers had manipulated parameters in Google URLs used for AdSense and redirected unsuspecting end-users to a spam website. In April 2008 phishing emails purporting to come from the Google AdWords service have emerged. Google AdWords is a service that allows advertisers to intelligibly connect with individuals who search using Google. In the Google AdWords phishing samples that have emerged, the end-user is encouraged to click on a link to update their billing information and/or renew their account. The link in these phishing emails leads to a fraudulent website where personal information is requested and harvested.

As security companies and the Internet community pay more attention to the reputation of websites and email senders, spammers are doing their best to hide behind well-established and reputable brands like Google.
Spammers Who’s Who Network

One of the side effects stemming from the growth of personal and professional networking sites is the increase in unsolicited emails that operate under the guise of connecting business professionals with their peers. In the example below, the recipient is invited to join an organization which it claims recognizes “men and women who have achieved success in their respective fields.” The recipient is asked to join the “inner circle” and is encouraged to supply the network with their professional history by clicking on a URL which brings the user to a registration page. The page requests personal information that could be used for identity theft and could fuel future spam attacks.

Subject: your who's who profile

April 25th, 2008

Welcome to our Inner Circle.

We are eager to consult with you. Our referral based program enables you to be reached by hundreds and thousands of professionals and your peers with the purpose of doing business with you.

Our organization recognizes men and women who have achieved success in their respective fields: [REDACTED]

WHO’S WHO is used as an outstanding professional resource throughout the World, providing a forum for consulting, exposure and credibility.

Visit us at the address below and acquaint us with your History.

http://www.[REDACTED]

We look forward to your reply.

Very truly yours,

George Malone

P.S. We are proud to invite you to our consortium.
Spear Phishing for a Subpoena

While spear phishing is not a particularly new security trend, it is a trend that has received some prominence recently. Spear phishing is different than other types of phishing attacks because it targets specific people and organizations. In a recent example observed by Symantec in April 2008, certain organizations received a spear phishing attack that claimed to come from a United States District Court. It stated that the recipient was, “HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.” A fraudulent link in the email instructed the recipient to: “Please download the entire document on this matter (follow this link) and print it for your record.” However, if the recipient attempted to download the document they also installed a keystroke logging trojan.

![Image of a subpoena document]
Resist the Calendar Invite From Spammers

In April 2008 Symantec observed the emergence of calendar spam. The email in question was sent with a meeting or calendar invitation attached. This type of spam did not reach high volumes in April, and the samples observed by Symantec were generally related to 419 or Nigerian spam. 419 spam is named after an article in the Nigerian Criminal Code that deals with fraud. Calendar spam messages, while low in number, show the lengths that some spammers are willing to go to for spam.
Spammers: The New Movie Casting Agents

Do you want to be a movie extra? As shown in the examples below, spammers are looking for their own American Idol by soliciting end-users to provide their mailing address to obtain information on how to become an extra in a movie.

If a recipient clicks on of the URLs in the message it will redirect the Web browser to a spammer’s website. The main objective of the spammer’s message is to harvest personal contact information.
IRS Phishing Tricks you Into ‘Biting’ the Bait

Remember the IRS phish of the past few months? You know the ones - end-users being given refunds if they but enter their credit card information into non-IRS sites.

Our May report has shown us an interesting twist. This time, instead of the refund link taking you to a site to steal your credentials, the link takes you to a popular web-based game in which you incarnate a vampire. The vampire gains more power every time end-users click on his link. It’s a rough, dark world out there… be warned.

Sample:

We are pleased to inform you that upon reviewing your fiscal activity, we have determined that you are eligible to receive a tax refund of $372.31

To access the online form for your tax refund, please follow this link:

http://s8.bitefight.ro/c.php?uid=34952

Your Individual Taxpayer Identification Number: 217 XX 3569

Because this letter could help resolve any questions regarding your exempt status, you should keep it in your permanent records.

If you distribute funds to other organizations, your records must show whether they are exempt under section 497 (c) (12). In cases where the recipient organization is not exempt under section 497 (c) (12), you must have evidence the funds will be used for section 497 (c) (12) purposes.

If you distribute fund to individuals, you should keep case histories showing the recipient’s name and address; the purpose of the award; the manner of section; and the relationship of the recipient to any of your officers, directors, trustees, members, or major contributors.

Sincerely,
Natasha Morgen
Director, Tax Refunds Department

While this IRS fraud won’t steal your credentials or break your bank, it’s still not the tax refund you’ve been waiting for. But don’t worry Symantec’s taking the ‘bite’ out of this one…
Beware of the Spammer Bearing Instant Messenger Gifts.

A new and interesting spam attack was spotted this month. The attack purportedly 'gifts' the spammed recipient with the opportunity to scan through their messenger buddy list and highlight who they would like removed from it.

Instant messaging services are a regularly used medium for social interactions. A growing number of today’s consumers and businesses are conversing online rather than over the phone, or in person. So finding out that you’ve been removed from an acquaintance’s friends list can tell you a lot about yourself, and your “acquaintance.”

The recipient is invited to click on a URL, which notifies them who has blocked their name on instant messenger. It asks the recipient to provide their username and password. The most interesting aspect of this type of spam is the theft of usernames and passwords, as many people use the same username and password across the Internet.