McAfee®


Protect what you value.

# January Spam Report

McAfee's Avert Labs discovers and discusses key spam trends. McAfee evaluates 2008's spam "Winners and Losers" and releases predictions on spam trends for 2009.

# Table of Contents



McAfee®

# January Spam Report

McAfee's Avert Labs discovers and discusses key spam trends. McAfee evaluates 2008's spam "Winners and Losers" and releases predictions on spam trends for 2009.

## Journalist's Work Leads to 65% Drop in Spam

There are a number of companies in the security industry that specialize in the quick and efficient takedown of malicious sites—primarily those that are hosting phishing web pages that attack their customers. However, Brian Krebs, a Washington Post investigative technology reporter, recently accomplished something that had never been done before—he nearly killed spam! Well, at least, he helped reduce it by as much as 65% for a couple of weeks.

In the fall of 2008, Mr. Krebs began an investigation of the key infrastructure providers for the online cybercrime scene. This led him to the identification of companies like Atrivo and McColo—network hosting providers that had a wide range of cybercriminal activity emanating from their networks. On Atrvio's network, a domain name registrar called EstDomains allowed cybercriminals to register hundreds of thousands of domains.

In addition to shining a light on these dark areas of the Internet through his reporting, Mr. Krebs also worked with network carriers to shut down network access to these hosted providers, effectively booting them off the Internet. In the case of EstDomains, the result was de-accreditation as a registrar by ICANN.

As a result of McColo's Internet lockout on Tuesday, November 11, 2008, McAfee® TrustedSource™ Internet Reputation System, registered a 65% drop in global spam traffic. In the chart below, you can see the decline in volume starting on Tuesday afternoon (EST). By 24 hours later, however, the spammers had rebounded and levels were only 50% off normal spam traffic flow. The rise continued on Thursday, November 13, although even more than a month later spam levels were not yet back to normal.

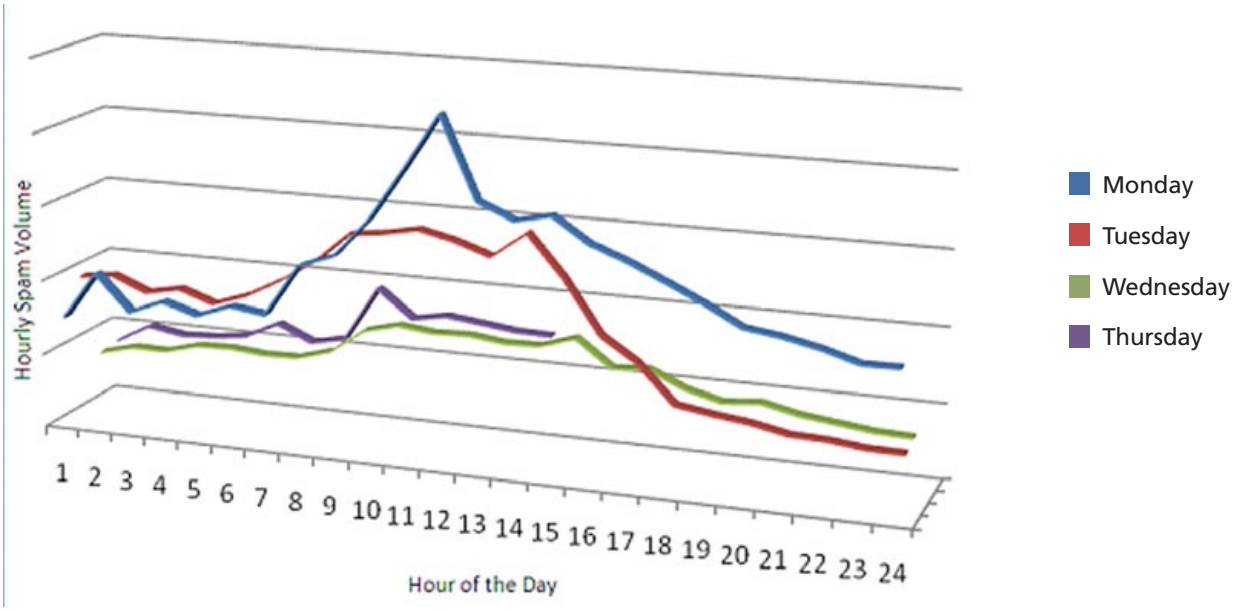


*Figure 1: Decrease in spam volume after McColo's Internet lockout*

The reason for this decrease was due to the large number of command and control spam servers (C&Cs) located on McColo's networks taken offline. These servers were the ones that controlled millions of compromised PCs (zombies) that were responsible for the majority of spam sent worldwide. When these servers went offline, the zombies effectively lost the connection to their "brain" and were no longer commanded to send out spam.

Reports indicate that the Internet connection to McColo was briefly re-enabled during the weekend after they were shut off, in order to see what would happen. Spammers took advantage of this to re-establish connectivity with the botnets and tell them to look elsewhere for their command and control. This has allowed them to restart the idle botnet networks and begin spamming again.

Current spam levels have shown a significant increase in the last few weeks but are still 40% less than levels prior to the McColo takedown. Historically, the month of December is when spam volume records are set. Before the takedown, we were on our way to seeing a new spam volume record. So the effect of the takedown is significant in many ways, and we should rejoice for this holiday blessing. However, spam volume slowly climbs each week, and we expect as the command and control servers get new homes that junk email will return to previous levels in due time.

## Political Spam Aftermath

The political spamming that gave us so much amusement during the U.S. election (and by the way the spammers predictions were correct with an Obama victory) was connected to the McColo hosting company. After the brief shutdown of McColo, the volume of political spam dropped substantially.


*Figure 2: Volume of political spam nearly disappeared with McColo's shutdown (source: TrustedSource)*

Before the shutdown there was still a lot of McCain spam, as we discussed in our last report. However, as the spam has started to return, the McCain associations have not. Current spam headlines do contain "Obama" but the new president's name does not appear to be a focus of the spammers at this time.


*Figure 3: IRS Tax related spam email*

## The Season for Tax Relief Junk Email

With tax season fast approaching, we've been keeping an eye out for tax scams. In 2008, we saw tax scams used for "spear phishing" as well as for general malware distribution This year we are seeing full corporate fronts that lure people in and convince them to expose their financial information. Until we have a tax system that doesn't involve the collection of personal data, this will remain a very exploitable vector for criminals.

With the improving professionalism in scam corporate fronts, they are likely to be very effective this year, unless consumers and enterprises are protected by a web security product or service that employs a reputation system. Here are examples (See Figure 3 and 4).

McAfee Avert Labs has released a document covering the evolving nature of threats that are targeting the browser:

*http://www.securecomputing.com/pdf/WebBrowsersNov08.pdf.*

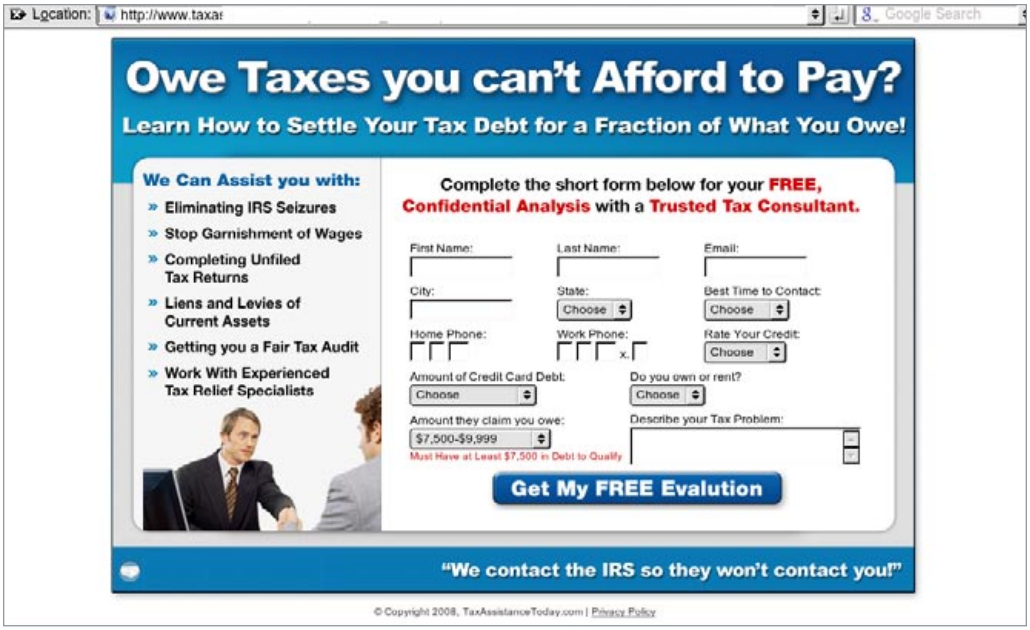


*Figure 4: IRS Tax scam website*

## The End of Domain Tasting

Domain tasting is the systematic abuse of ICANN's five-day "grace period" that allows an individual to register a domain name and return it for a full refund within five days. For years, many online advertisers, and some registrars and spammers have been taking advantage of this policy to register hundreds of thousands of domains on a daily basis, try them out for a few days, and then return them back to the registry for a full refund.

Some registrars have built new businesses by having a continuous "float" of millions of domains in their portfolio that are exchanged daily for ones that can result in better search engine placement and generate more advertising revenue.

After much pressure and debate, ICANN's board adopted a recommendation by the GNSO (Generic Names Supporting Organization) Council that applies limits on the impact and scale of domain tasting. After three months of this policy, we can see the results in Figure 5.

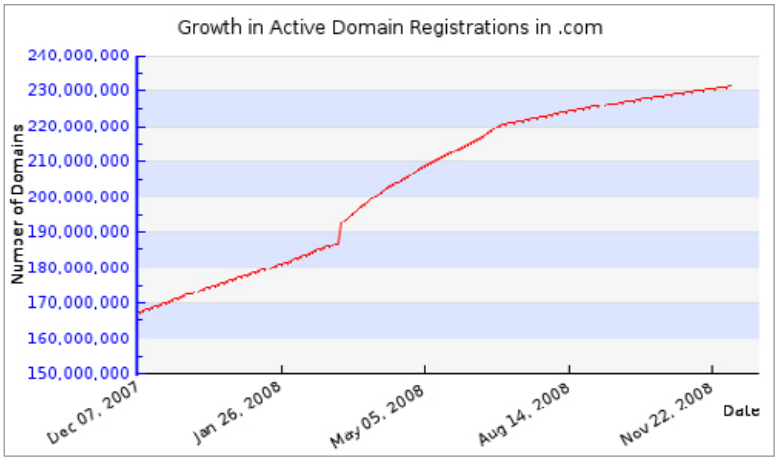


*Figure 5: Daily number of domain registrations within .com registry*

Note the rapid decline in the slope of the graph that begins in late June. ICANN reported that Add Grace Period (AGP) deletes are down by 84% since June[1]. This means that there are now fewer daily registrations of profane or malicious domains and more, in general, available for legitimate use.

However, it's important to realize that this measure is only a temporary short-term solution that the ICANN board has put in place until a permanent consensus on domain tasting can be achieved in the community. The proposal for the permanent change is now available for public comment and we encourage everyone to give ICANN feedback[2] on this practice and the proposed policy change.

1 http://www.icann.org/en/announcements/announcement-13nov08-en.htm
2 http://www.icann.org/en/announcements/announcement-20oct08-en.htm

## With the Increase in Unemployment, Diploma Spam Rises Proportionally

After the spam decrease in November due to the McColo shutdown, botnets have been busy reorienting their command and control. All spam types have increased, but the kind of spam that is associated with the global economic issues has been most apparent.

Knowing more people are out of work has given spammers a juicy new group to target: the unemployed. The most obvious spam reaction to the economic headlines has been the increase of junk messages advertising diplomas and advanced schooling.

The increase in this type of email can be timed with announcements from major corporations about their workforce reductions of thousands of workers. Well publicized and notable reductions from major banks, manufacturers, technology, and automotive companies are examples of the recently unemployed that spammers are preying upon (example Figure 6).

**We need Ph.d nominees**

**From:** "Benita Sanford" <------@------.--->
**To:** --------@---.---
**Date:** Today 03:01:15

WHAT A GREAT IDEA!

We provide a concept that will allow anyone with sufficient work experience to obtain a fully verifiable University Degree.

Bachelors, Masters or even a Doctorate.

For USA: 1 [redacted] 5746
Outside USA: +1 [redacted] 5746

Only you have the right to decide what to study and when to study, your degree is completely up to you. Besides the quality education we also offer you personal financial aid options. You don't have to quit your job, you don't have to work part-time. You will have a chance to work even more than 40 hours a week and studying during your free time.

Just leave your NAME & PHONE NO. in the voicemail.

*Figure 6: Sample diploma spam*

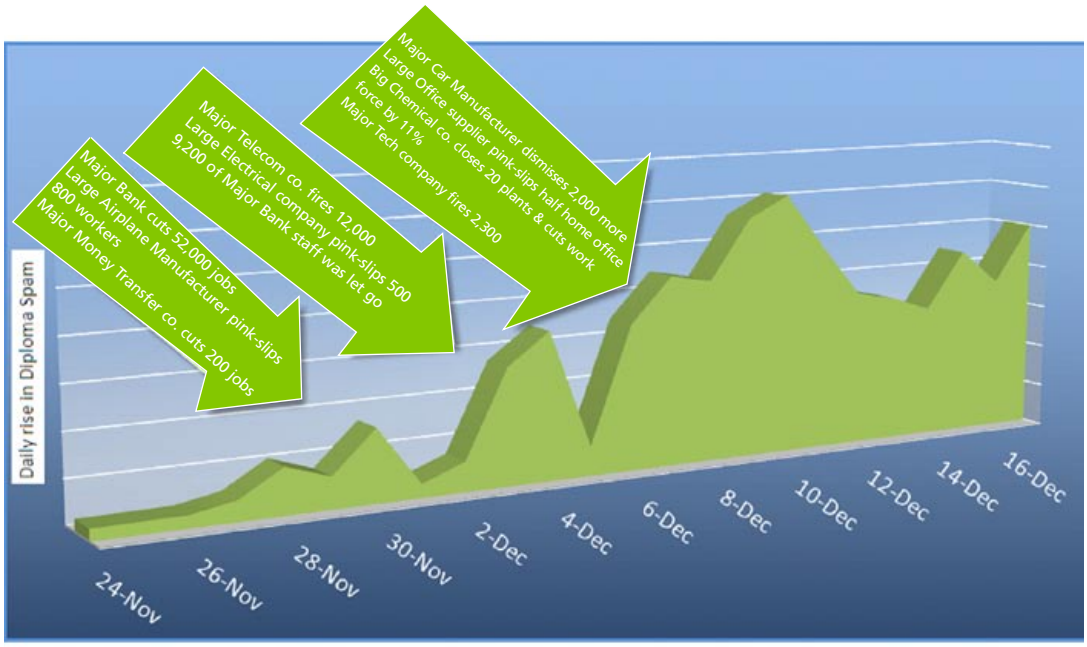


*Figure 7: Rise in diploma spam and the increase in unemployment are directly proportional (source: TrustedSource)*

With unemployed people looking to further their careers through continuing education, the attractiveness of advertising low cost diplomas has increased. This kind of spam grew significantly during December (see Figure 7).

## Need "Credit" for Holiday Shopping?

Spam that advertises new credit cards, credit checks, loans, mortgages, or dealing with bad credit or debt has also increased significantly. Offers to get money without credit checks, or to escape debt with no strings attached were on the rise before the Holidays (see Figures 8 and 9).

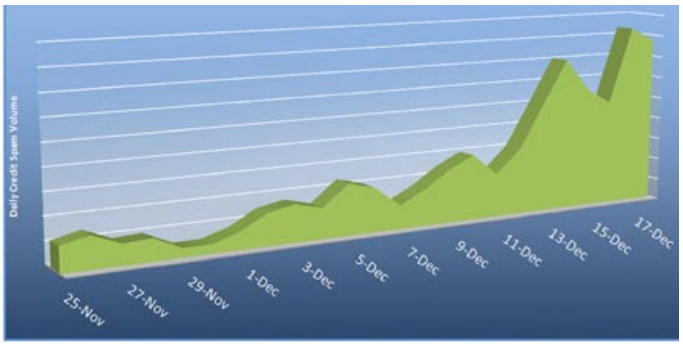


*Figure 8: "Credit" spam increased before the holiday (source: TrustedSource)*


*Figure 9: A sample of "credit" spam*

## The Facts on Phishing Attacks

Phishing attacks against banks have actually not increased significantly since the days following the McColo incident. This is likely due to a lack of servers to centralize the gathering of usernames and passwords that are entered into compromised websites. That's not to say that phishing attacks are not occurring, as this graph shows a spike due to a Bank of America phishing scam on November 26.

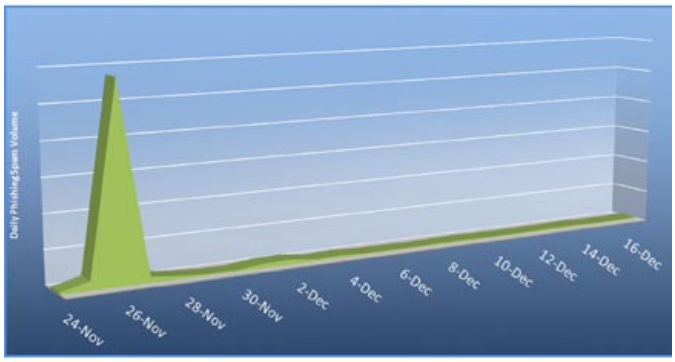


*Figure 10: Spike in phishing attacks on November 26, 2008 (source: TrustedSource)*

## Christmas E-Card Spam

When the holidays come along, they bring the annual holiday spam too. The topic is usually Viagra, but the tactic is just to get someone to click on the link. Malware and viruses are linked to e-card spam.

E-card spam often has a short two sentences and a link:

> *Robert mailed Merry Christmas postcard.*
> *Visit the following web address to see it:*
>
> *http://----christmasgift.com?asdfasdfasdfasdfasdfasdfasdfas*
>
> *Cheers*

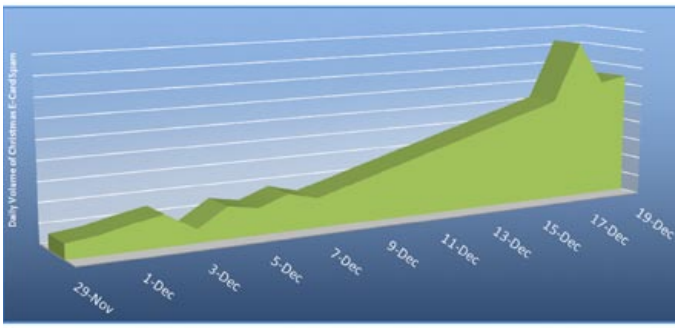


*Figure 11: Increase in Christmas e-card spam (source: TrustedSource)*

## Farewell 2008 – Spam Winners and Losers

Let's take a quick look back at 2008's spam and see how they fared.

**The Losers:**

***Lonely Girl***

A year ago the "lonely girl" spam was just getting into high gear, urging recipients to send them an email at their *.info domain address so that a dialogue could be established. This type of spam still exist, but has generally been drowned out by other spam campaigns.

> *Hey Baby*
> *I saw your profile on-line just a few minutes ago*
> *Email me at Dani@|--------|----.info and I will reply with a Picture and info right away.*
>
> *Maybe we can chat today?*

***Pump-and-Dump Stock Spam***

Image-based stock spam was widespread in 2007 but went back to plain text in 2008. It was very successful in the beginning (as shown below) and spammers did initially profit more using this technique compared to traditional spamming campaigns on a daily basis. These pump-and-dump stock schemes would generally fizzle out over the next six months and become far less of a frequent spam than they used to be. Today, they are not an issue.

Vision Airships Global Expansion!

BANGKOK, THAILAND, Jul 09, 2007 (MARKET WIRE via COMTEX) -- Vision Airships Inc. (PINKSHEETS: VPSN) -- The company wishes to announce that it has finalized arrangements for funding for its global expansion.

Vision Airships is set to become a worldwide operator of blimps used for advertising around the world. As the advertising market gets more crowded in conventional mediums -- the use of alternative forms of advertising is gaining more and more traction -- this is where Vision Airships comes in and supplies the end to end solution to major advertisers worldwide with its unique form of alternative displays. The size of the market worldwide will support 24 airships which would bring in approximately $400,000,000 annually.

Check out the news and get on VPSN first thing Tuesday and Wednesday!

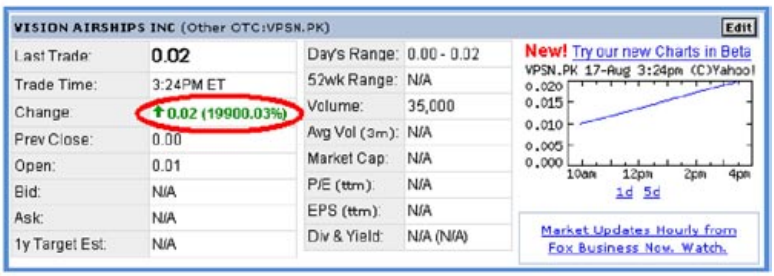


*Figure 12: Pump and dump spam and the company's performance the following day in the stock market*

***Celebrities Targeted by Spam Campaigns***

2008 began with a "New naked Britney video" and then went to "your neighbor naked." Then it went back to Britney, gained traction with "Paris Hilton caught on Video," peaked with "Angelina Jolie gets naked," and ended with lurid insinuations of the Presidential candidates' wives. After being the target of a lurid and libelous spam campaign during their moments of headline fame these women are left with only the tarnished memories of unwanted publicity in the public eye.

This tactic is a surefire winner, because people love to accidentally click on links associated with nudity, but the victimized women weren't rewarded for the abuse of their names. The headline watchers must be eagerly looking for the next female entertainer to top the charts of the distinguished celebrity spam list.

***Auto CAD***

The late February, 2008 surge brought a lot of Auto CAD spam, leading the way for a cheap "OEM software" revolution. Blogspot was heavily abused for its free website offerings. Blogspot is still heavily abused today, but generally for gambling and pills.

***IP Address Links in Spam***

Early in 2008, we saw a lot of spam strains that used direct links to IP addresses.

By the end of the year, we were hardly seeing this tactic. It's a good approach when the goal is to simply get around the need to purchase (or rent) a domain name to send spam, but it's a bad tactic for trying to blend in with the crowd of legitimate messages that come from sites that use domain names.

**The Winners:**

***Pharmacy Spam***

While others may come and go, pills have remained a big part of global spam. Increasing the potency of your love life through chemical additives is huge business. Spam selling low cost drugs from other countries can even come in pretending to be other types of spam, with subjects and content associated with fake news, Internet dating, casual communications, and stock reports all linking to pharmacy websites. It uses images, obscure URLs, direct URLs, mashed URLs, and anything else it needs to bypass spam detection.

Pharmacy spam is a monster and is certainly not looking to disappear anytime soon.

> *This is the funniest postcard I have ever seen! See it online! http://116.--.194.188/*

***Fake Rolex Watch Spam***

The only real noticeable change in fake Rolex Watch spam has been the website improvements, which are becoming much more professional in appearance. Surprisingly, Rolex Watch spam has flourished in the absence of competition from other spam varieties. It was decreasing in October, but since the McColo shutdown, it has boomed and generally appears less affected by the event than other spam varieties.

## Welcome 2009 – Spam Predictions

**Free Web-hosting/Blogging Services will Be Increasingly Abused by Spammers**

By allowing people to create a public website without the authentication necessary to purchase domain name websites like Geocities, Blogspot, and Live facilitate a spammer's ability to get their message across with a minimal expenditure of resources.

Spam that is hosted from do-it-yourself social website hosting providers arrives at the destination with far greater frequency than links pointing to domain names assigned by legitimate registrars. With little to no threat of punishment for their hosted content, and the new restrictions on short-term domain tasting, the attractiveness of free bandwidth offered by these sites will undoubtedly draw greater focus from malicious parties.

**More Targeted Phishing and Corporate Blackmailing**

Botnets that spread into corporate networks and financial datacenters will increasingly be used to gather sensitive information that can be used for blackmail or sold on the underground market. Browser based attacks will increasingly be used as the least protected vector in order to transfer payload. Security breaches of confidential data managed by partner and subsidiary companies will force an overhaul of data security practices.

2008 also had an increase in localized phishing campaigns, especially on college campuses, where professional looking emails claiming to be associated with the school's financial or scholarship department were blasted to all the students at the school. This is a significant danger to people who are just becoming responsible for their own finances. These types of phishing attacks are likely to be more effective per mail than their global cousins.

**More Scams Involving Home Businesses**

"Legitimate" home business scams generally involve either a pay up front and Do-It-Yourself kit, or a pay-to-play shell game of training and certification. We'll see more of it on the television, and the same infrastructure that supports diploma spam and confidence fraud will adjust to the new unemployment reality and will offer people some new bait on the old check cashing scam.

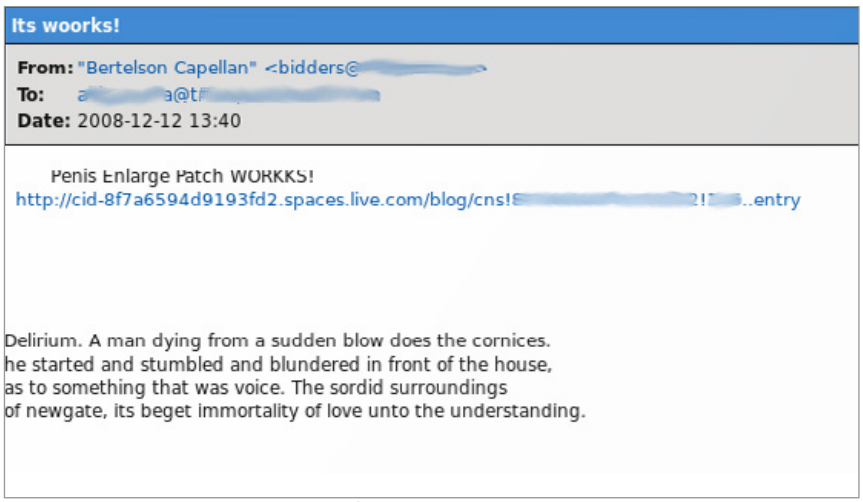


*Figure 13: A sample of spam using link hosted on Live.com*

### Increase in Forging and Abuse of Free Email Services

The free email services have started to allow accounts to send mails with arbitrary "from" addresses. This has increased the usability of these services significantly to businesses, but has also increased the "abusability" by spammers. Shared SPF and SenderID records call to question the purpose of having them in the first place. The need for Domain Keys Identification Mail (DKIM), PGP key signing, and secondary authentication mechanisms will become more important to a basic business security model.

### New Businesses to Replace Lost McColo Hosting

Hosting companies will be set up in countries that are eager to embrace a burgeoning Internet market and will offer services to replace the disrupted command and control centers formerly hosted by McColo. These may be used as pawns by entities that perceive strategic value in sculpting the battlefield of the future.

## Conclusion

In conclusion, McAfee Avert Labs recommends that both enterprises and consumers assure their software and patches are up-to-date, and that they implement a multi-layered approach to preemptively detect and block attacks. Using appliances with McAfee TrustedSource Internet Reputation System and anti-malware detection technology will put organizations a giant step ahead of others both in protecting against existing threats as well as new variants.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054,
888.847.8766
*www.mcafee.com*