PANDA SECURITY

commtouch®

Q2 2008 Email Threats Trend Report

Zombie Muscle Drives Huge Amounts of Spam and Malware

July 7, 2008

Spam and malware levels remain high for yet another quarter, powered by the brawny yet agile networks of zombie IPs. By operating millions of dynamic IPs every day, botnets dodged defenses and polluted the Internet with all kinds of email threats. Spammers and malware writers experimented with a few new techniques, though no innovation was needed for zombies to continue pummeling email users and networks with unwanted messages and hazardous code.

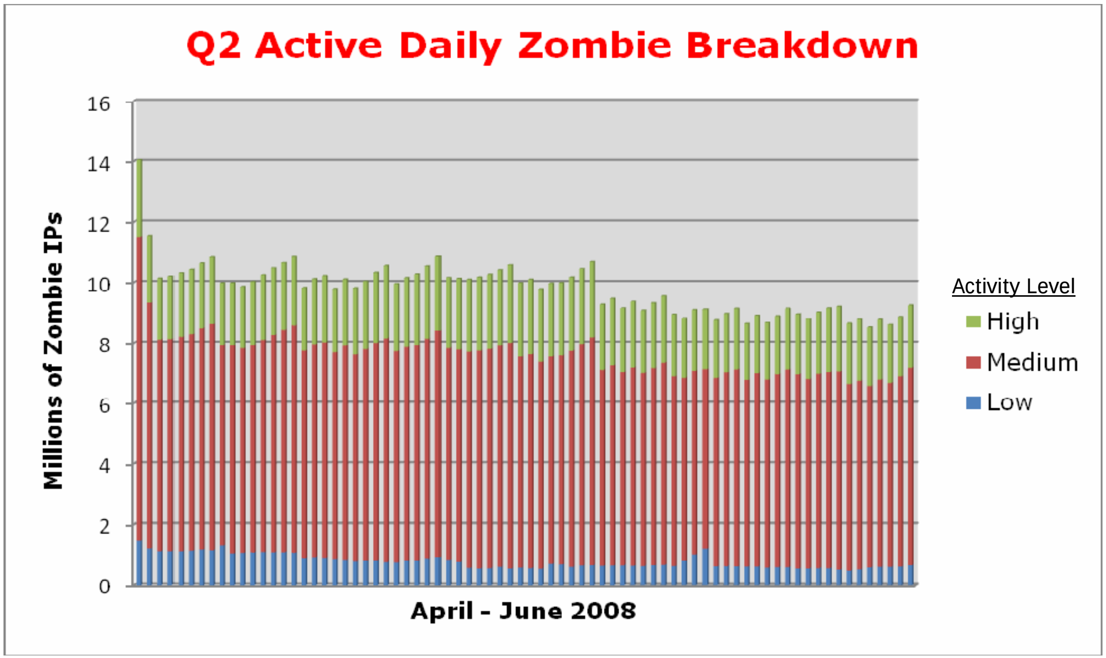
Q2 2008 Highlights

- Spam levels throughout the second quarter averaged 77%, ranging from a low of 64% to a peak of 94% of all email towards the end of the quarter
- Top domains hosting zombies include: Telecom Italia, Brasil Telecom, and Verizon
- 10 million zombie IP addresses are active each day, on average
- United States dropped to 9th place in number of zombies globally. Turkey is #1 with 11% of all zombies
- Pharmaceutical spam is the most popular topic, comprising 40% of all spam
- Phishing scams took advantage of the higher education community, as well as Google adwords users
- Spammers experimented with vertical display in Chinese-language spam

Ten Million Zombies Active in Distribution of Email Threats Everyday

On average, nearly 10 million zombie computers actively sent spam and email-based malware everyday during Q2, according to the Commtouch Zombie Lab, which automatically identifies zombie IPs as they are activated. The vast majority of those IP addresses are dynamic, meaning they are taken in and out of use at will by the botmaster controlling the network. Dynamic control of large numbers of zombie IPs is what allows the continuous delivery of malicious materials across the Internet. By the time traditional security solutions identify and block the source of a new threat, the botmaster easily deactivates them and switches to another set of sender IPs under his control.

Since most of the zombie IPs are dynamic, static blacklists of known offensive IPs can only block a small fraction of spam and malware. The update lag can also cause misclassifications, or false positives, by static solutions, as legitimate email is blocked once an IP is deactivated and then returns to sending innocent messages.



Source: Commtouch Labs

ISPs top the Zombie Charts

Internet Service Providers (ISPs) have been hit especially hard over the last several quarters by zombie armies. Zombie botmasters exploit ISP infrastructure either by sending spam directly to the Internet using port 25, or creating child email accounts from legitimate subscriber's machines. This puts service providers in the challenging position of not only needing to protect their subscribers from inbound spam that fills their inboxes, but they must also defend against being used by zombies to send spam out across the Internet.

Commtouch Zombie Lab consistently finds that the highest volumes of spam are sent by IPs belonging to ISPs.

Top 10 Zombie Hot Spots
Timeframe: 30 Days

Rank	Domain	# Zombies
1	ttnet.net.tr	1,807,935
2	telecomitalia.it	1,219,940
3	tpnet.pl	1,162,406
4	163data.com.cn	754,466
5	telesp.net.br	696,961
6	asianet.co.th	647,778
7	brasiltelecom.net.br	646,979
8	verizon.net	556,040
9	speedy.net.pe	564,599
10	etb.net.co	561,531

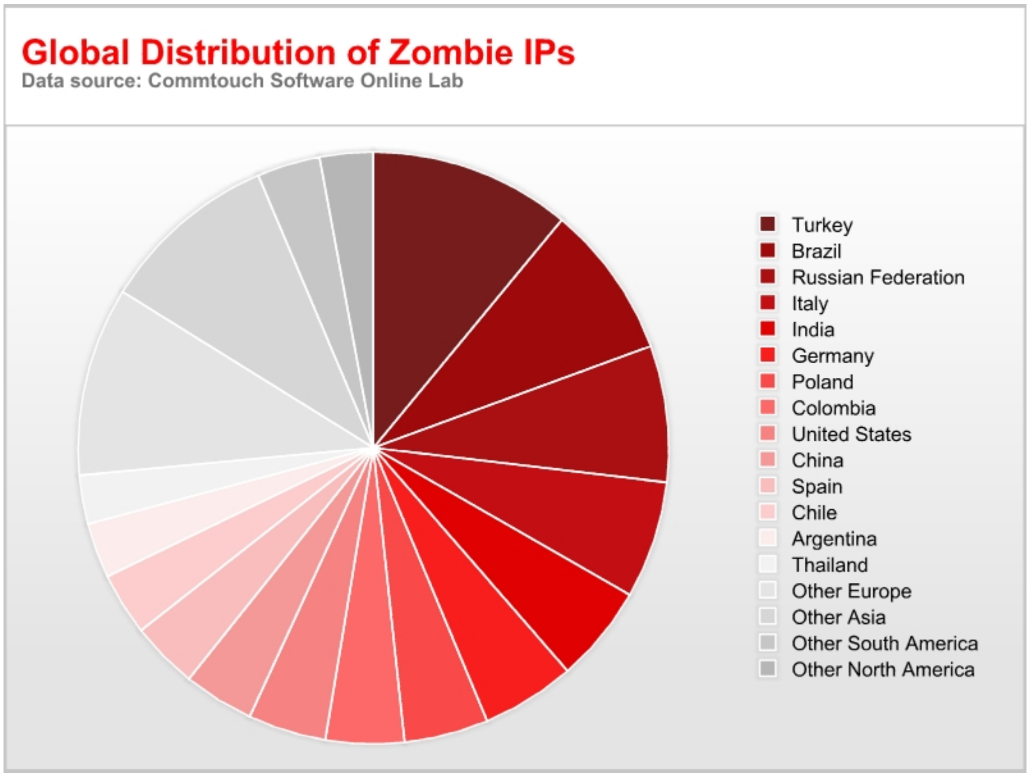
Source: Commtouch Labs

Q2 2008 Email Threats Trend Report

Outbound spam is a growing threat for ISPs that can lead to their IP ranges getting blacklisted and blocking legitimate outbound email along with the junk. In addition to getting blacklisted, zombie abuse uses precious network resources and can decrease customer satisfaction. As more and more subscriber PCs get infected, zombies will become an even greater problem for ISPs around the globe.

Zombie Geographic Distribution

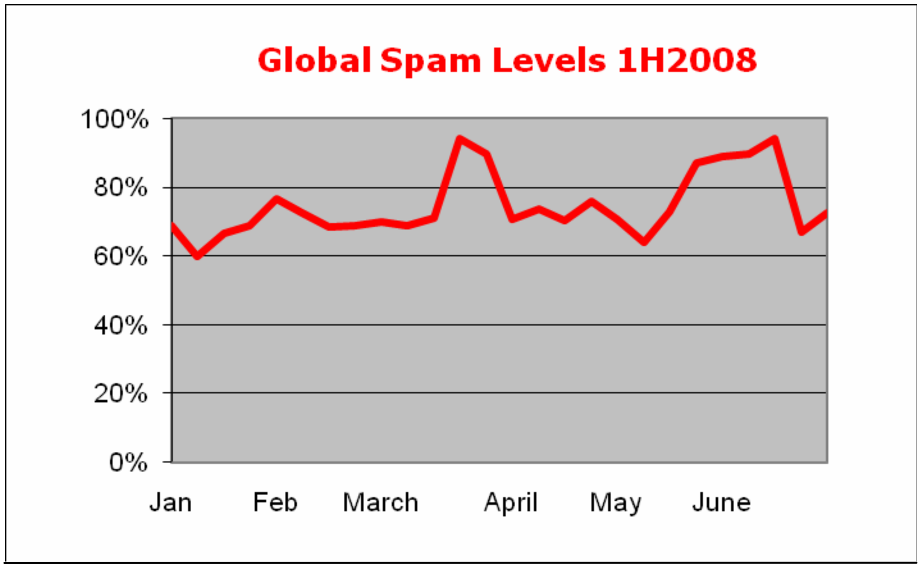
At the end of Q2, Turkey had moved into first place for the highest number of zombies (11% of all zombies worldwide), followed closely behind by Brazil and Russia with 8.4% and 7.4% respectively. Interestingly, the United States has fallen into ninth place, with only 4.3% of all zombies, compared to 5% in Q1 2008.


Global Distribution of Zombie IPs

Data source: Commtouch Software Online Lab

Email Threats Remain Strong

Though some new variations did appear, no ground-breaking innovations in email threats were unveiled during Q2. Unfortunately the same old tricks used in the past continued to evade traditional defenses. Spam levels throughout the second quarter averaged 77%, ranging from a low of 64% to a peak of 94% of all email towards the end of the quarter. The graph below shows the spam levels throughout the first half of 2008.



Source: Commtouch Labs

Phishing 101

Educational Institutions

Phishing, spam messages that attempt to coax users into handing over passwords and other sensitive personal information, continue claiming victims. Throughout the first half of 2008, University students and faculty members were taught a hard lesson in online security as waves of phishing scams were targeted at this vulnerable population. Messages were text-based, seeming to come from the IT department. Texts varied but were along these lines:

```
Dear Webmail Account Owner

This message is from web mail admin messaging center to all web mail account
owners. We are currently upgrading our data base and e-mail account center
We are canceling unused web mail  email account to create more  space for new
Accounts.

To prevent your account from closing you will have to update it below so that
we will know it's status as a currently used account.

CONFIRM YOUR EMAIL IDENTITY BELOW
Email Username : .............
Email Password : ................
Date of Birth : .................
```

```
Warning!!! Any account owner that refuses to update his or her account  within
Three days of this update notification will loose [sic] his or her account
permanently.

Thank you for using web mail
Support Team
Warning Code: ID67565434=20
```

Recipients may not have worried about giving up their email credentials; however Commtouch has evidence that compromised University accounts are being used for spearphishing scams, with spammers hiding their tracks by sending malicious messages from a legitimate source.

Google Adwords Phishing

Google adwords served as the cover for a glut of phishing scams during April. The Subject lines were socially engineered to look like legitimate administrative messages Google Adwords account owners would reasonably expect to receive. If the recipient was enticed by the Subject, the body of the email contained links that appear to be legitimate Google links (e.g. www.adwords.google.com…). When clicked, the link redirected to a phishing site hosted on a Chinese .cn domain.

Sample Google Adwords Phishing Subjects:

- your adwords google account is stopped
- account reactivation
- please re-activate your account
- please re-submit your payment information.
- please submit your payment information.
- please update your billing information.
- reactivate your adwords google account.
- submit your payment information.
- your payment didn't succeed

Love is in the air – and in your inbox

Love remained a common theme for malware spreading spam. The amorous emails have become a classic email threat; exploiting users' romantic inclinations to bypass their better judgment and spread malicious code.

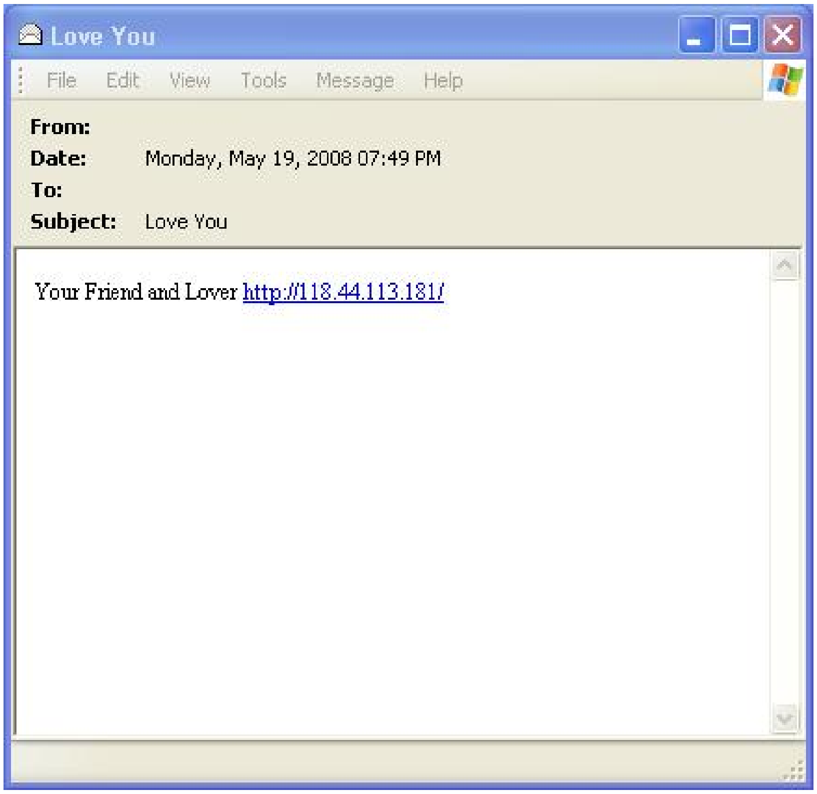
An outbreak that began mid-May featured promising love-themed Subjects and messages. The body of the email contained IP-address based URLs that delivered a malicious 'iloveyou.exe' executable file.

Sample Love-themed Subjects:

- Love You
- I love you so much!
- Heavenly Love
- Our Love is Free
- Crazy in love
- With you by my side
- Me & You
- The Mood for Love
- A Precious Gift
- You're the one
- A kiss so gentle
- In your arms

The IP address URL in the sample message below delivers the malware download.

Sample Love Malware Blended Threat Message



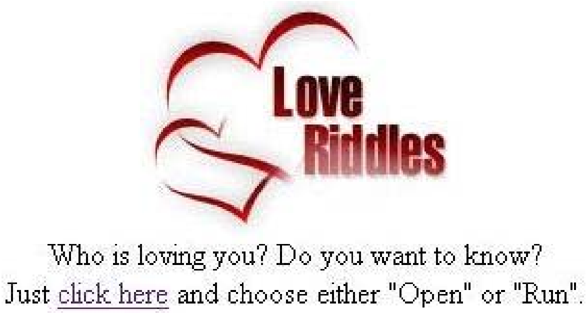
From:
Date: Monday, May 19, 2008 07:49 PM
To:
Subject: Love You

Your Friend and Lover http://118.44.113.181/

Source: Commtouch Labs

Just weeks later, Commtouch Detection Labs identified another love-themed blended threat outbreak. This time the romantic Subjects lured users to open an email message containing a link to download a version of the notorious Storm malware, known by the monikers Zhelatin or Nuwar.

More Love in a Storm



Who is loving you? Do you want to know?
Just click here and choose either "Open" or "Run".

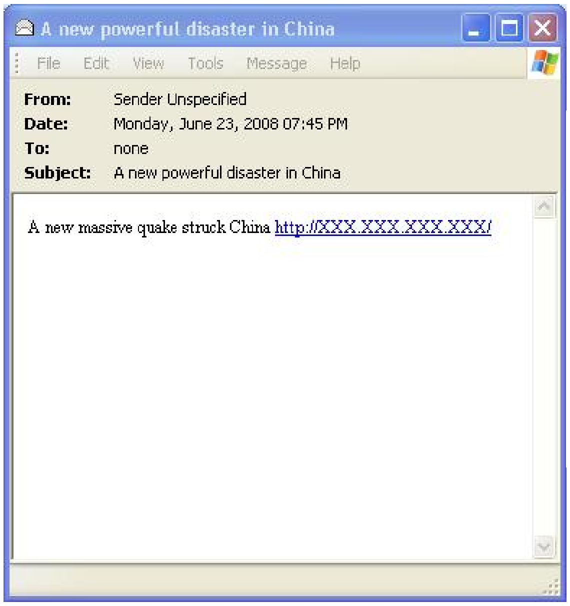
Source: Commtouch Labs

Storm Invents an Earthquake

Storm-watchers nostalgic for the first big outbreak of January 2007 got a reprise in June, with an outbreak of blended threat emails about a nonexistent earthquake in China. The message writers were probably betting on the fact that since a massive earthquake *had* recently hit China a few weeks earlier, that unsuspecting users would assume these messages were legitimate. Further adding to the social engineering is the fact that the summer Olympics are coming up in China, so any unusual news about China has a stronger tendency to be opened or clicked.

There were several waves of "earthquake" outbreaks, the earliest one comprised of simple one-line messages hyperlinking to fast-flux domains, and later messages hyperlinking to zombie IP addresses.

Sample Storm Earthquake Message

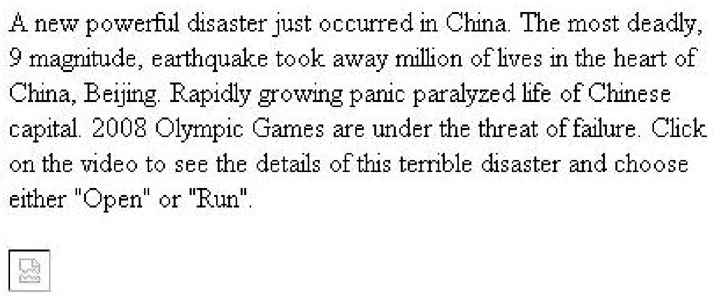

A new powerful disaster in China
File Edit View Tools Message Help

From: Sender Unspecified
Date: Monday, June 23, 2008 07:45 PM
To: none
Subject: A new powerful disaster in China

A new massive quake struck China http://XXX.XXX.XXX.XXX/

Source: Commtouch Labs

Sample Earthquake Malware Site



A new powerful disaster just occurred in China. The most deadly, 9 magnitude, earthquake took away million of lives in the heart of China, Beijing. Rapidly growing panic paralyzed life of Chinese capital. 2008 Olympic Games are under the threat of failure. Click on the video to see the details of this terrible disaster and choose either "Open" or "Run".

Source: Commtouch Labs

Subject lines for these outbreaks included:

- deadly earthquake shook china again
- 2008 olympic games are under the threat
- a new massive quake struck china
- 2008 olympic games will possible not take place
- the capital of china were collapsed by earthquake
- deadly catastrophe in chinese capital
- death toll in china exceeds 1000000
- the capital of china were collapsed by earthquake

Spam Tactics and Cover Ups

Spam and Taxes

The classic Benjamin Franklin quote can now be updated to say that “In this world nothing is certain but spam and taxes.” In April, spammers took advantage of the race to file taxes in the US to launch a round of tax-related spam messages. The email Subject lines promised everything from quick refunds to help with debts owed the IRS.

Sample Tax Spam Subject Lines:

- Get a fast tax refund free
- Get fast relief for irs tax debt
- Tax refund notification (message id nt4838324)
- Need IRS tax relief?
- What the IRS doesn’t want you to know!
- End IRS problems
- Tax Notification Internal Revenue Service (IRS)
- Internal Revenue Service Tax Notification
- Put your tax refund to work for you

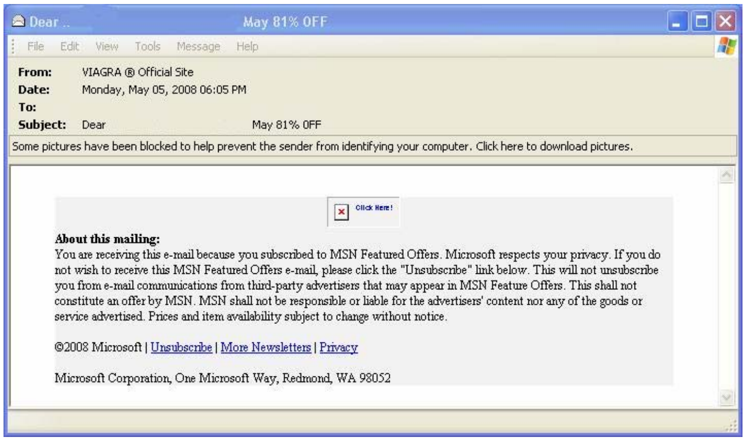
Third Parties Provide Perfect Cover

Spammers’ hijacking of legitimate sources to disguise their evils is nothing new. The third party cover techniques work by fooling content-based anti-spam solutions that scan email messages for suspicious characteristics. In recent months, two new types of third party cover-ups appeared.

Pharma Spam Embedded in Microsoft Content

Since many anti-spam solutions are now capable of identifying and blocking spam with embedded images, spammers have devised a clever way of using common, legitimate content to sneak past filters. In one such outbreak spammers simply copied content commonly found in legitimate Hotmail messages (in this case, the disclaimer message). The presence of this text makes the message appear innocuous to content-based filters; in fact it is a form of Bayesian poisoning. The catch is that the body of the message also contains a link to a hosted image of a pharmaceutical ad. This outbreak is the next logical step from a similar outbreak in the previous quarter, which used legitimate Hotmail text in the HTML source of the message, but not visible to users. Even the image is the same.

Sample Microsoft Embedded Pharma Spam
(Before downloading images)



From: VIAGRA ® Official Site
Date: Monday, May 05, 2008 06:05 PM
To:
Subject: Dear May 81% OFF

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

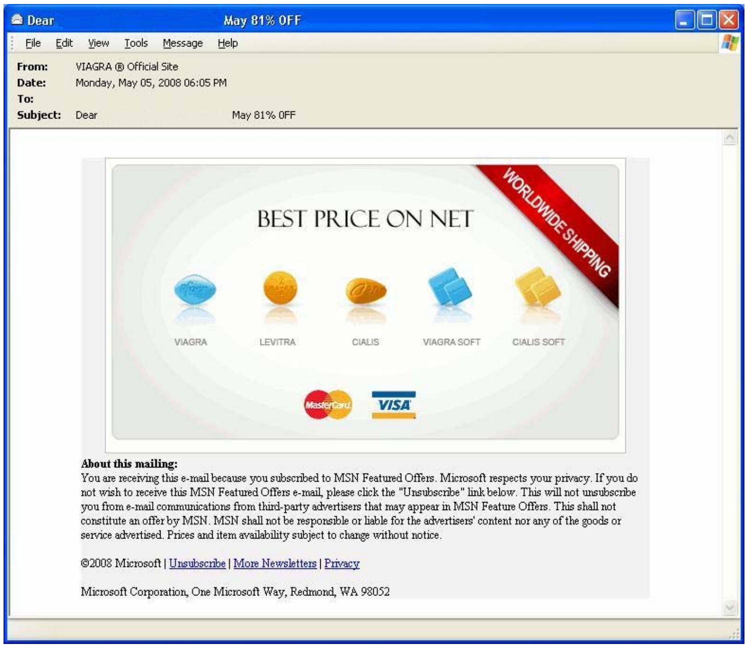
About this mailing:
You are receiving this e-mail because you subscribed to MSN Featured Offers. Microsoft respects your privacy. If you do not wish to receive this MSN Featured Offers e-mail, please click the "Unsubscribe" link below. This will not unsubscribe you from e-mail communications from third-party advertisers that may appear in MSN Feature Offers. This shall not constitute an offer by MSN. MSN shall not be responsible or liable for the advertisers' content nor any of the goods or service advertised. Prices and item availability subject to change without notice.

©2008 Microsoft | Unsubscribe | More Newsletters | Privacy

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Source: Commtouch Labs

Sample Microsoft Embedded Pharma Spam
(After downloading images)



From: VIAGRA ® Official Site
Date: Monday, May 05, 2008 06:05 PM
To:
Subject: Dear May 81% OFF

About this mailing:
You are receiving this e-mail because you subscribed to MSN Featured Offers. Microsoft respects your privacy. If you do not wish to receive this MSN Featured Offers e-mail, please click the "Unsubscribe" link below. This will not unsubscribe you from e-mail communications from third-party advertisers that may appear in MSN Feature Offers. This shall not constitute an offer by MSN. MSN shall not be responsible or liable for the advertisers' content nor any of the goods or service advertised. Prices and item availability subject to change without notice.

©2008 Microsoft | Unsubscribe | More Newsletters | Privacy

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Source: Commtouch Labs

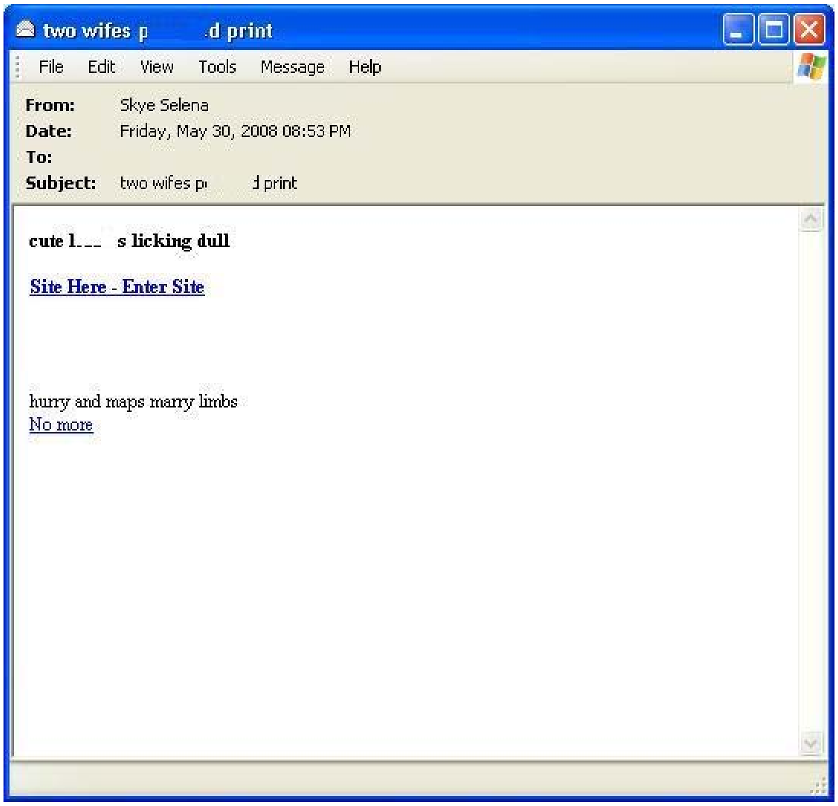
If the user has set his email client to block the viewing of hosted images, he will not see the message immediately. In this case, the content used to fool spam filters may also work on the human end user. The familiar hotmail disclaimer may put the user at ease and make him feel comfortable enough to allow images. If the image is viewed, not only has the spammer succeeding in exposing yet another user to his message, he has also confirmed the recipient's email address is valid, which may put the user at risk of being targeted even more in the future.

Blogs provide cover for public nuisances

The popular blogging platform Blogspot was one of the first to be exploited to host and distribute malicious content. Perhaps in response to growing awareness and attempts to block Blogspot content, spammers have begun using other, less popular blog platforms. Blogdrive, a much smaller blogging site, fell victim in Q2 to spammers' devious schemes.

A spam outbreak distributed via Blogdrive during Q2 used misspelled pornographic subject lines. It appears that one of the Subject words was a randomly selected 'joker' devised to throw off content filters that can learn to recognize word combinations used in an outbreak. Once the message was opened, users were enticed to click a hyperlink to adult content hosted on a Blogdrive page.

Users fall victim to Blogdrive "Jokery"



From: Skye Selena
Date: Friday, May 30, 2008 08:53 PM
To:
Subject: two wifes p d print

cute l___ s licking dull

Site Here - Enter Site

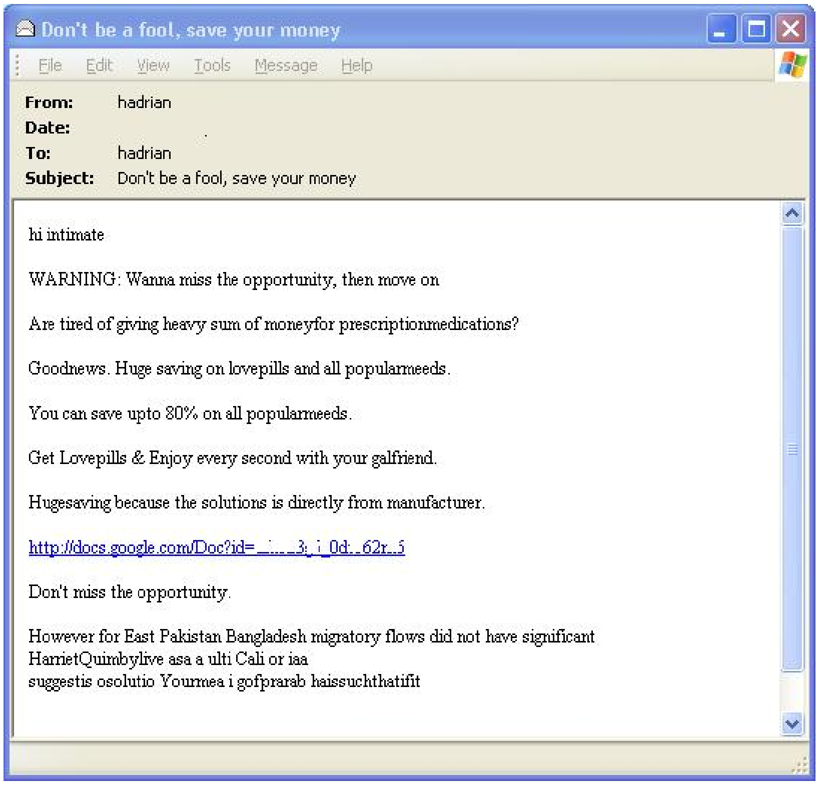
hurry and maps marry limbs
No more

Source: Commtouch Labs

Google Docs Spam Picks up Momentum

Though trivial experimenting can be traced as far back as January 2007, the Google docs spam reappeared during the month of May. The recent run was far from a massive outbreak, but rather appears to be a sort of proof-of-concept test run. The messages featured plain text Bayesian poisoning to get through content-based anti-spam technology, and a link to a Google docs web page where a pharma ad was posted.

Google Docs Used as Pharma Spam Hideaway



Don't be a fool, save your money

From: hadrian
Date:
To: hadrian
Subject: Don't be a fool, save your money

hi intimate

WARNING: Wanna miss the opportunity, then move on

Are tired of giving heavy sum of moneyfor prescriptionmedications?

Goodnews. Huge saving on lovepills and all popularmeeds.

You can save upto 80% on all popularmeeds.

Get Lovepills & Enjoy every second with your galfriend.

Hugesaving because the solutions is directly from manufacturer.

http://docs.google.com/Doc?id=_i..._3;_i_0d:_62r_5

Don't miss the opportunity.

However for East Pakistan Bangladesh migratory flows did not have significant
HarrietQuimbylive asa a ulti Cali or iaa
suggestis osolutio Yourmea i gofprarab haissuchthatifit

Source: Commtouch Labs

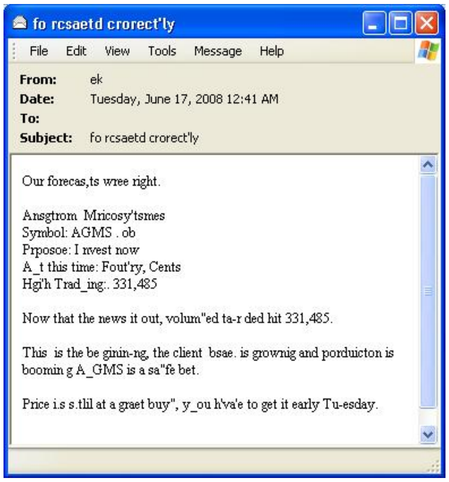
The manual process of creating unique Google docs pages limits the scalability of this technique. But if spammers devise a way to automate the creation of Google docs larger spam outbreaks using this tactic could ensue.

Q2 2008 Email Threats Trend Report

Pump and Dump Perseveres

The bane of email users everywhere, pump-and-dump stock spam, refuses to go away. The artificial promotion of stocks is a scam as old as stock markets themselves, and the email version looks like it will be around for a while. Though the infamous image-based stock spam has nearly disappeared (the low levels of image-based spam today are mainly used for pornographic spam) simple plain text pump and dump spam is still commonplace. Outbreaks during June used regular plain text messages littered with spelling errors that would make any primary school teacher cringe, but apparently does not discourage the ever-optimistic investor looking to earn some quick cash.

Samples of plain text stock spam



From: ek
Date: Tuesday, June 17, 2008 12:41 AM
To:
Subject: fo rcsaetd crorect'ly

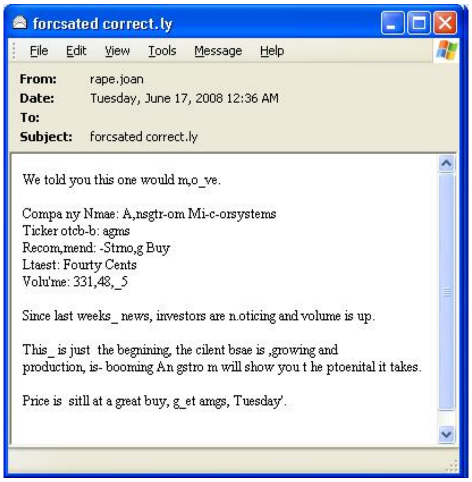
Our forecas,ts wree right.

Ansgtrom Mricosy'tsmes
Symbol: AGMS . ob
Prposoe: I nvest now
A_t this time: Fout'ry, Cents
Hgi'h Trad_ing:. 331,485

Now that the news it out, volum"ed ta-r ded hit 331,485.

This is the be ginin-ng, the client bsae. is grownig and porduicton is boomin g A_GMS is a sa"fe bet.

Price i.s s.tlil at a graet buy", y_ou h'va'e to get it early Tu-esday.



From: rape.joan
Date: Tuesday, June 17, 2008 12:36 AM
To:
Subject: forcsated correct.ly

We told you this one would m,o_ve.

Compa ny Nmae: A,nsgtr-om Mi-c-orsystems
Ticker otcb-b: agms
Recom,mend: -Strno,g Buy
Ltaest: Fourty Cents
Volu'me: 331,48,_5

Since last weeks_ news, investors are n.oticing and volume is up.

This_ is just the begnining, the cilent bsae is ,growing and production, is- booming An gstro m will show you t he ptoenital it takes.

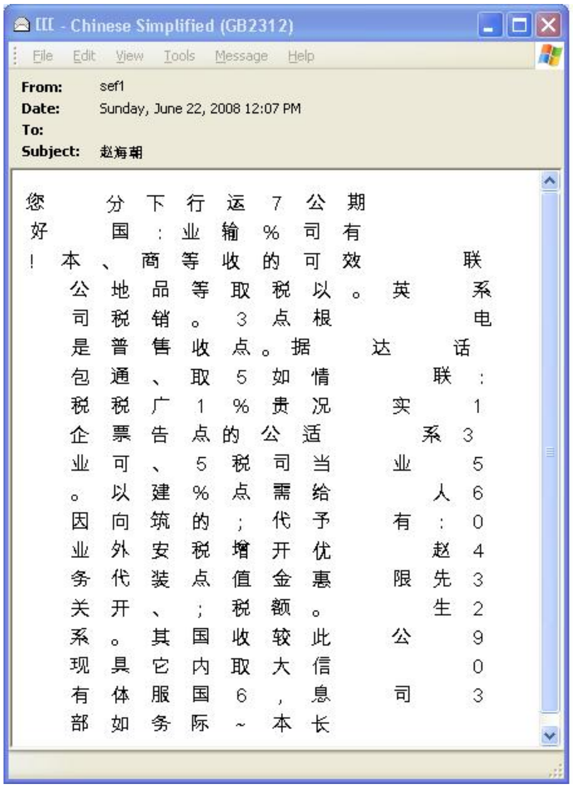
Price is sitll at a great buy, g_et amgs, Tuesday'.

Source: Commtouch Labs

Vertical Text Spam

Spammers are always experimenting with new ways to bypass anti-spam filters, and one of the earliest methods was to play with the display, typically by using tricks available with HTML tables. Asian languages have an added benefit from the spammer's perspective – besides the fact that it is difficult to filter due to its double-byte nature and because sentences are written with no spaces between words, stymieing traditional content-based engines. The latest twist introduced in June is to send Chinese spam with a vertical orientation. In the example below, all of the text is written vertically, including the telephone number on the right-hand side.

Chinese Vertical Spam


[[[- Chinese Simplified (GB2312)
File Edit View Tools Message Help

From: sef1
Date: Sunday, June 22, 2008 12:07 PM
To:
Subject: 赵海朝

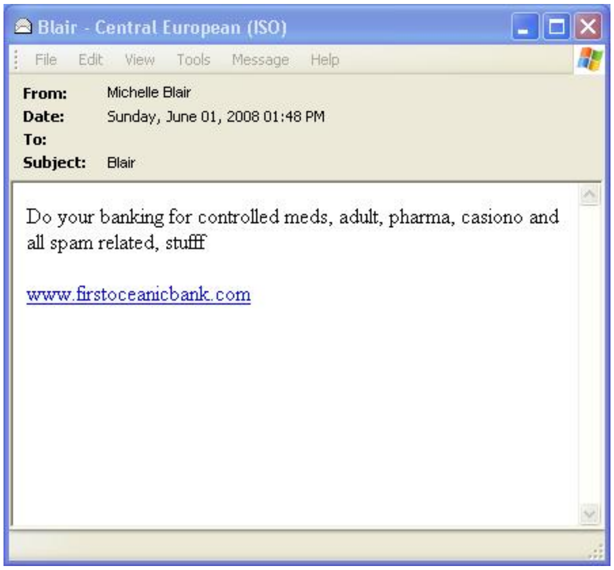
您好！
本公司是包税企业。因业务关系现有部
分国、地税普通税票可以向外代开。具体如
下：商品销售、广告、建筑安装、其它服务
行业等等。收取1点5%的税点；国内国际
运输收取3点5%的税点；增值税收取6～
7%的税点。如贵公司需代开金额较大，本
公司可以根据情况适当给予优惠。此信息长
期有效。
英达实业有限公司
联系人：赵先生
联系电话：13560432903

Source: Commtouch Labs

A Taste of Their Own Medicine

An ironic twist appeared in June, as a spam outbreak that apparently targets other spammers was detected. The message offers banking services for spammers' ill-gotten gains. Some alleged victims of this scam have come forth anonymously on the Internet offering personal accounts of how they were defrauded of significant sums of cash by using the services featured in the spam. Some even claim the scam is used to funnel money to terrorist organizations.

Sample of spam for spammers


Blair - Central European (ISO)
File Edit View Tools Message Help

From: Michelle Blair
Date: Sunday, June 01, 2008 01:48 PM
To:
Subject: Blair

Do your banking for controlled meds, adult, pharma, casiono and all spam related, stufff

www.firstoceanicbank.com

Source: Commtouch Labs

Spam Topics

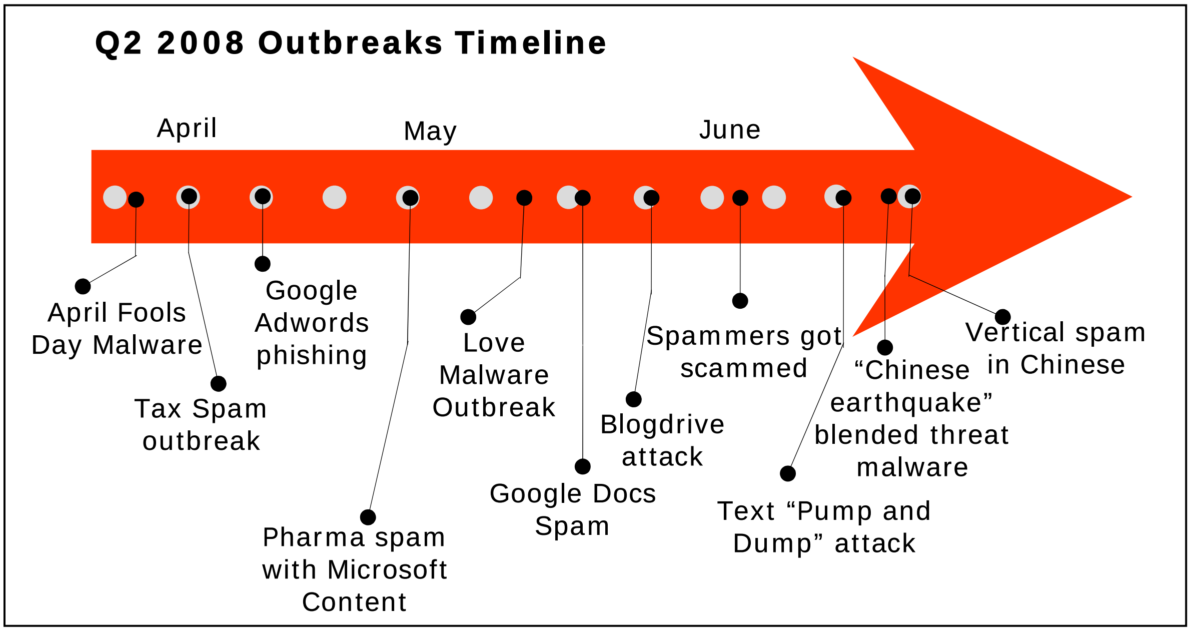
Pharmaceutical spam overtook sexual enhancers in the second quarter, reaching 46% of all spam. In Q4 2007, Enhancers was 70% of all spam, then down to 30% in Q1 2008, and now as low as 22%.

Topics of Spam Email Q2 2008

Pharmacy 46%	Pornography 3%
Sexual Enhancers 22%	Software 2%
Replicas 21%	Loans/ Mortgage 2%
Academic Degrees 3%	Other 1%

Source: Commtouch Labs

Q2 2008 Outbreaks in Review



Source: Commtouch Labs

About Commtouch

Commtouch® (NASDAQ: CTCH) is the source of proven messaging and web security technology for scores of security companies and service providers, enabling them to mitigate Internet threats and allowing them to focus on their business. Proven expertise in building efficient, massive-scale security services has resulted in Commtouch's unmatched suite of offerings that automatically process, learn and improve over time.

Stay abreast of the latest trends all quarter long, at the Commtouch Café: blog.commtouch.com

The key services – Anti-Spam, Zero-Hour™ Virus Outbreak Protection, GlobalView™ Mail Reputation Services and GlobalView™ Zombie Intelligence – all provide information for each other in a comprehensive, self-learning feedback loop that learns locally as well as globally. Relying on Commtouch allows the company's licensing partners the freedom to focus on their own areas of expertise, secure in the knowledge that Commtouch is always well ahead of the latest email and web threats.

Commtouch's patented Recurrent Pattern Detection™ technology automatically analyzes billions of transactions weekly to identify new spam, malware and zombie outbreaks as they are initiated. Because RPD™ technology does not rely on any content-filters, it is equally effective for all languages and formats; it can identify outbreaks of any content- or attachment-type, and is highly effective at blocking spam in double-byte languages.

For more information about enhancing security offerings with Commtouch technology, see www.commtouch.com or write nospam@commtouch.com.

About Panda Security

Panda Security is one of the world's leading IT security providers, with millions of clients across more than 200 countries and products available in 23 languages.

Its mission is to develop and provide global solutions to keep clients' IT resources free from the damage inflicted by viruses and other computer threats, at the lowest possible total cost of ownership.

Panda Security proposes a new security model, designed to offer a robust solution to the latest cyber-crime techniques. This is manifest in the performance of the company's technology and products, with detection ratios well above average market standards and most importantly, providing greater security for its clients.

For more information and evaluation versions of all Panda Security solutions, visit our website at: http://www.pandasecurity.com

For more information: communication@pandasecurity.com Tel. +34 91 806 37 00