

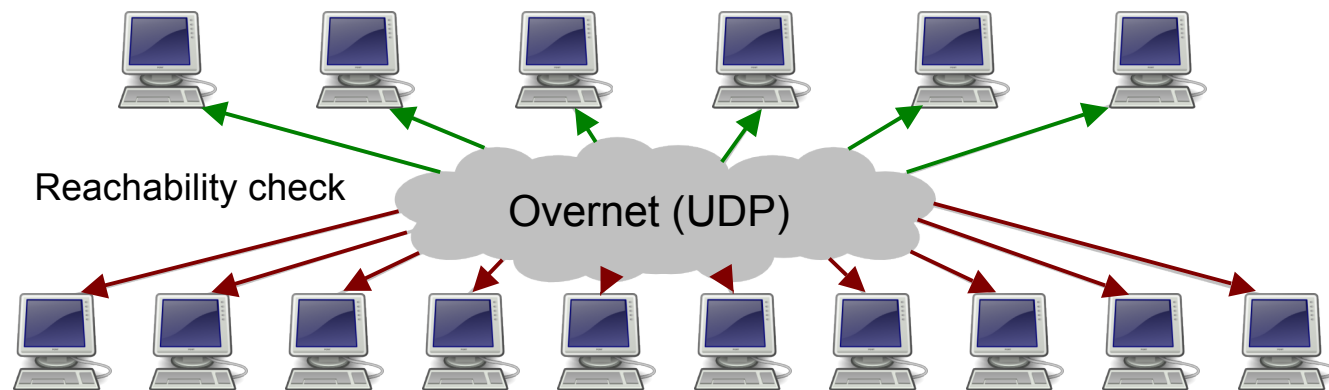
# Welcome to Storm!



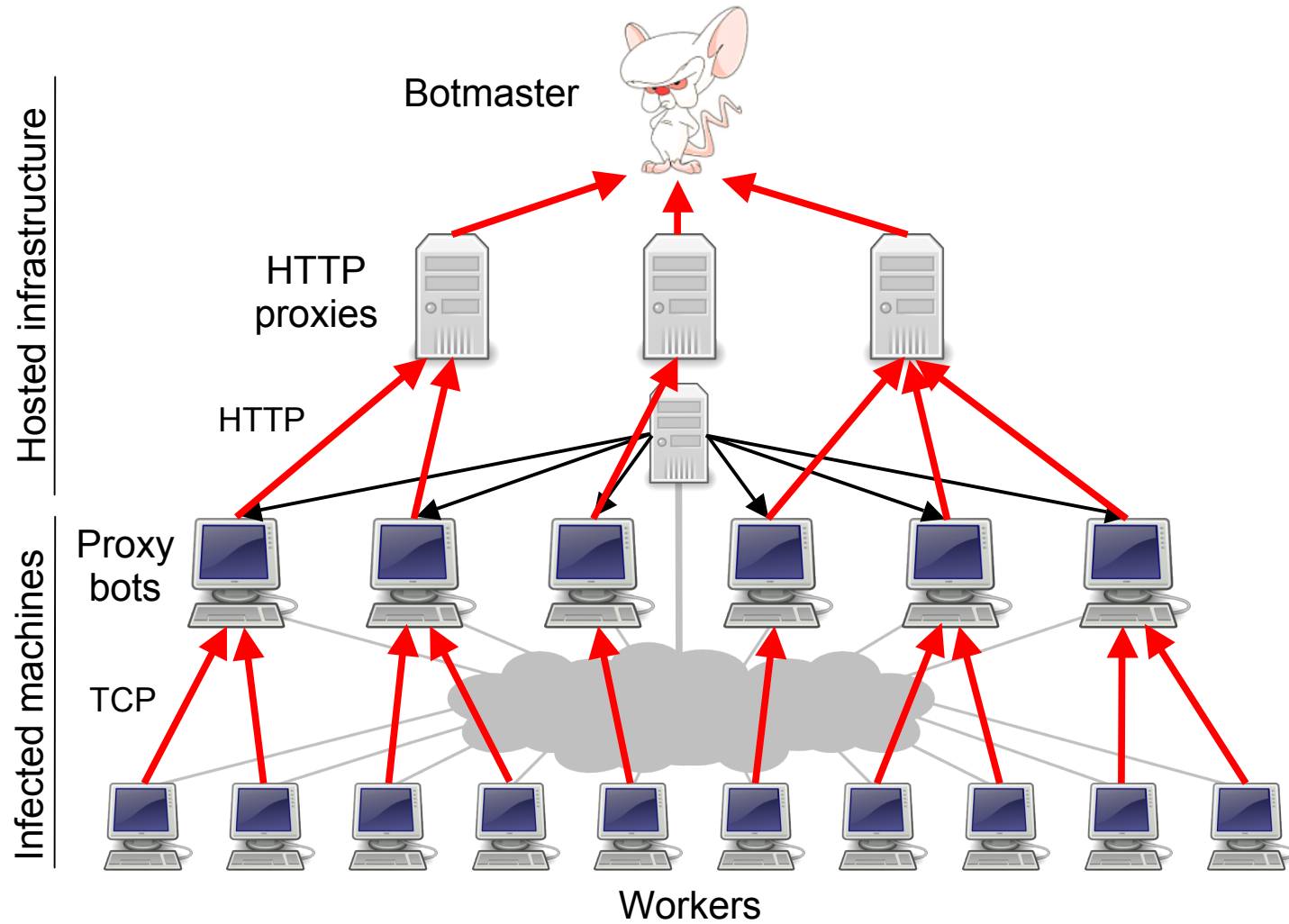
Would you like to be one of our newest bots?  
Just read your postcard!

(Or even easier: just wait 5 seconds!)

# The Storm botnet



# The Storm botnet



September 6th, 2007

# Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

**Categories:** [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox.....](#)

**Tags:** [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



**150** TalkBacks

ADD YOUR OPINION



SHARE



PRINT



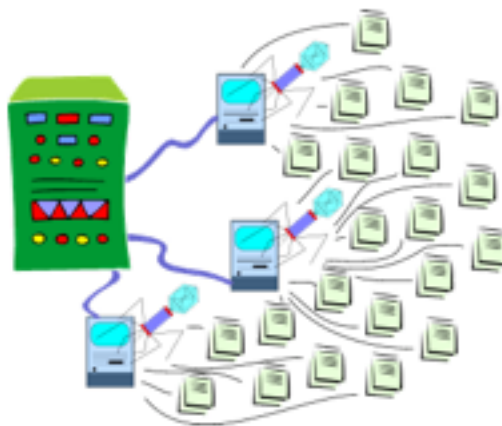
E-MAIL



WORTHWHILE?

**+97**

115 VOTES



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

“

*The [Storm] botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet, and is estimated to be capable of executing more instructions per second than some of the world's top supercomputers. However, it is not a completely accurate comparison, according to security analyst James Turner, who said that comparing a botnet to a supercomputer is like comparing an army of snipers to a nuclear weapon*

“

*The [Storm] botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet, and is estimated to be capable of executing more instructions per second than some of the world's top supercomputers. However, it is not a completely accurate comparison, according to security analyst James Turner, who said that comparing a botnet to a supercomputer is like comparing an army of snipers to a nuclear weapon*

If that made you catch your breath a bit, read on...

“

*At certain points in time, the Storm worm used to spread the botnet has attempted to release hundreds or thousands of versions of itself onto the Internet, in a concentrated attempt to overwhelm the defenses of anti-virus and malware security firms. According to Joshua Corman, an IBM security researcher, "This is the first time that I can remember ever seeing researchers who were actually afraid of investigating an exploit."*

Storm generates OIDs using its own PRNG given by the recurrence:

$$I_{i+1} = (a \cdot I_i + b \bmod 2^{32}) \bmod m$$

with  $a = 1664525$ ,  $b = 1013904223$ ,  $m = 32767$ , and the initial value  $I_0$  is based on the system clock. The generator appears to be based on a well-known linear congruential PRNG described in the *Numerical Recipes*

Location	Hallmarks
Germany	Random OIDs with lower 10 bytes constant. Floods the Storm network aggressively with thousands of fake node IPs.
Iran	Random OIDs biased to upper half of space (first bit always set).
Sweden	Random OIDs biased to upper half of space (first bit always set). Does not appear in routing tables of any other peers.
France	One fixed OID, relatively passive crawler, appears to just be sampling Storm.
East Coast, US	257 OIDs evenly distributed in ID space behind one IP, port number used as upper two bytes of the OID.
East Coast, US	Uniform random OIDs, both a Storm implementation and crawler behind the same IP, does not report other peers.
West Coast, US	Random OIDs biased to upper half of space 100:1. Does not report IPs in response to queries.

Table 2: Other parties participating in the “encrypted” Storm network on April 4, 2008.



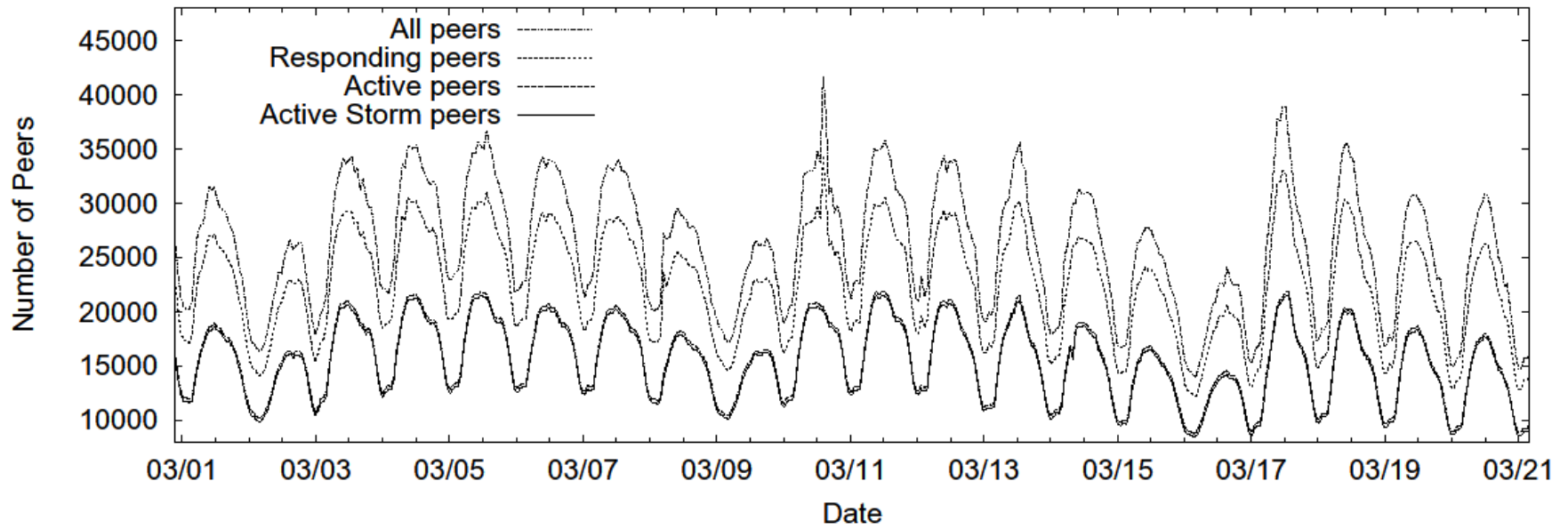
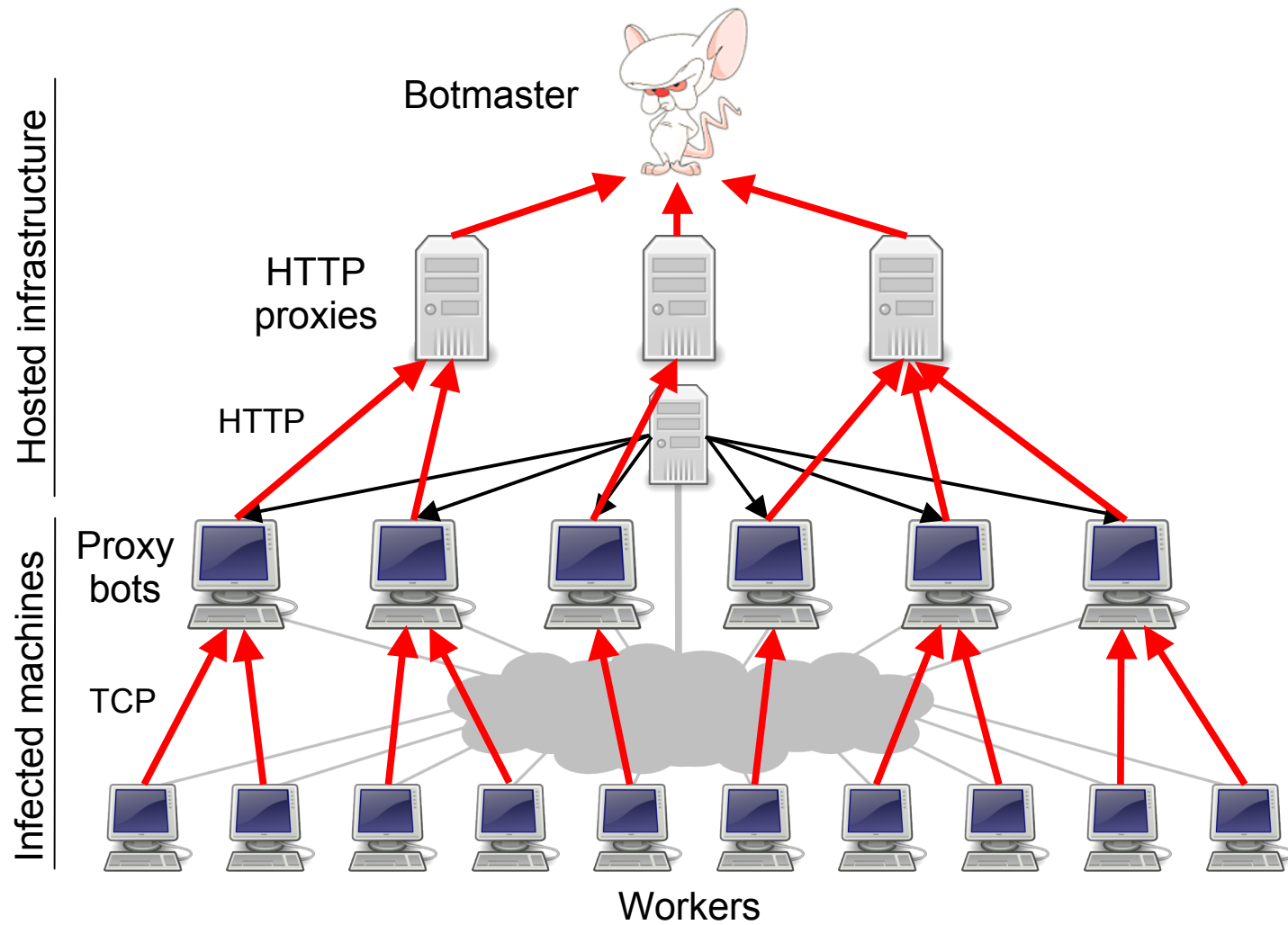


Figure 2: Estimates of the size of the Storm botnet using different notions of liveness over the first three weeks of March 2008. Note that the  $y$ -axis does not begin at zero to better separate the curves.

# The Storm botnet





# GooHost.ru

Reliable and quality hosting

Тел.: +7(495) **542-39-87**, icq: 418396204

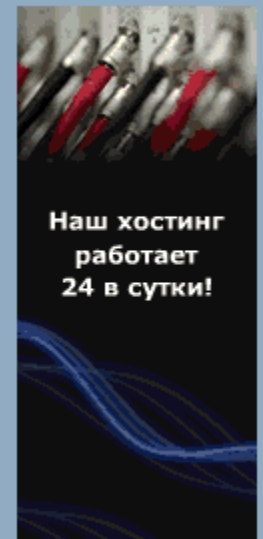
## Menu

- Hosting Plans
- Email Mailing
- Website Design
- FAQ
- Dedicated server
- Domain Registration
- Payment
- Contact

## Hosting Plans

We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.

We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.



Наш хостинг  
работает  
24 в сутки!

**Obuzoustoychivy hosting** is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

<u>MINI PLAN</u>	
Volume disc	400 MB
Domains	1
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	4 000 rub. / 1 month.

<u>STARTER PLAN</u>	
Volume disc	500 mb
Domains	3
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	5 000 rub. / 1 month.

<u>BUSINESS PLAN</u>	
Volume disc	1000 mb
Domains	7
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	7 000 rub. / 1 month.

<u>PREMIUM PLAN</u>	
---------------------	--

Professional **Bullet Proof Hosting** -  
**Ultrabulks.com**  
Solid Offshore Hosting BP Server Bulk Email  
Friendly!



 Bulletproof Hosting - Never Get Shut Down Again !



## Reliable Bullet Proof Web Hosting

-Email Marketing Service

### Enter your Domain Name:

www.  .com  [Check Available](#)

.com  .net - Bullet Proof Domain \$100/Year

### Hosting Plans:

#### SILVER PLAN

- [Bullet Proof Hosting A](#)
- 50MB Web Space
- 10GB Monthly Bandwidth
- Static Pages Only
- FTP Account
- 99.8% Uptime
- \$299.95/month

New Price \$**199.95**/month  
[More...](#) --- [Order Now](#)

#### GOLDEN PLAN


- [Bulletproof Hosting B](#)
- 50MB Web Space
- 10GB Monthly Bandwidth
- PHP/CGI/ASP Supported
- FTP Account
- 99.8% Uptime
- \$399.95/month

New Price \$**299.95**/month  
[More...](#) --- [Order Now](#)

 [Bullet Proof Hosting](#)

 [Bullet Proof Domains](#)

 [Bullet Proof Server](#)

 [Reseller](#)

 [BP URL](#)

 [Contact Us](#)

 [Sitemap](#)

### Partners:



[3 Day Free](#)



# Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

### SEARCH THIS BLOG

Go

### RECENT POSTS

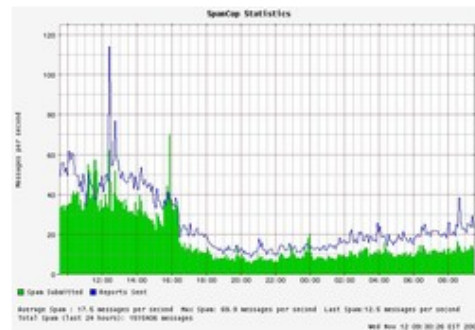
- [E-Banking on a Locked Down PC, Part II](#)
- [ChoicePoint Breach Exposed 13,750 Consumer Records](#)
- [President Obama on Cyber Security Awareness](#)
- [Mozilla Disables Microsoft's Insecure Firefox Add-on](#)
- [PayChoice Suffers Another Data Breach](#)

### Entries By Category

- [Cyber Justice](#)
- [Economy Watch](#)
- [Fraud](#)
- [From the Bunker](#)
- [Latest Warnings](#)
- [Misc.](#)
- [New Patches](#)
- [Piracy](#)
- [Safety Tips](#)

## Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (Note: A link to the full story on McColo's demise is available [here](#).)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic [shows a similar decline](#), from about 40 spam e-



# Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

## SEARCH THIS BLOG

Go

## RECENT POSTS

- [Farewell 2009, and The Washington Post](#)
- [Hackers exploit Adobe Reader flaw via comic strip syndicate](#)
- [Twitter.com hijacked by 'Iranian cyber army'](#)
- [Group IDs hotbeds of Conficker worm outbreaks](#)
- [Hackers target unpatched Adobe Reader, Acrobat flaw](#)

## Entries By Category

- [Cyber Justice](#)
- [Economy Watch](#)
- [Fraud](#)
- [From the Bunker](#)
- [Latest Warnins](#)

## Retail Fraud Rates Plummeted the Night McColo Went Offline

One month after the [shutdown of hosting provider McColo Corp.](#), spam volumes are nearly back to the levels seen prior to the company's take down by its upstream Internet providers. But according to one noted fraud expert, spam wasn't the only thing that may have been routed through the Silicon Valley based host: New evidence found that retail fraud dropped significantly on the same day.

It is unclear whether the decrease in retail fraud is related to the McColo situation, but in speaking with **Ori Eisen**, founder of [41st Parameter](#), he said close to a quarter of a million dollars worth of fraudulent charges that his customers battle every day came to a halt.

Eisen, whose company provides anti-fraud consulting to a number of big retailers and banks, told me at least two of the largest retailers his company serves reported massive declines in fraud rates directly following McColo's termination.

"It stopped completely that night," Eisen said, referring to a drop in fraudulent activity linked to purchases of high-value merchandise with stolen credit and debit cards on Nov. 11, the day McColo was shut down. "Yet, it will come back after [the scammers] erect their new infrastructure."