

# McColo - Cyber Crime USA



**HOSTEXPLOIT.COM**

2008 Version 2.0

Edited by: Jart Armin

Contributors: Garth Bruen, Greg Feezel, Paul Ferguson, Matt Jonkman,  
James McQuaid, Chris, Luis, Hugo & Max

# McColo - Cyber Crime USA

---

## HostExploit's Cyber Crime Series - Version 2.0

### Advice and data:

**StopBadware, McAfee, Trend Micro, Emerging Threats, Knujon, Sunbelt, CastleCops, Spamhaus, Arbor Networks, Malwaredomains, Threat Expert, SecureWorks, aa419, NEOinfoSecForum, Robtex**

### Blog

[InternetEvolution.com](http://InternetEvolution.com)

## ABSTRACT

---

This second CYBER CRIME USA report highlights those Internet players that currently host the world's major spam botnets (an estimated 50% of spam worldwide), malware, rogue PC security products, cybercrime affiliate payment systems, and child pornography. This study from HostExploit.com is based on tracking and documenting ongoing cyber criminal activity. As a result of the first report focusing on Atrivo / Intercage and subsequent community actions, there was a quantitative drop of 10% of spam and malware worldwide. While temporary, it does clearly demonstrate that with a concerted and consistent effort by concerned commercial Internet network operators, a safer Internet can ensue.

On this occasion we focus on McColo and others that, like Atrivo / Intercage, actually operate from servers and depend on US transit peers. This open source security study sets out to quantify and continuously track cyber crime using numerous methods of measurement. In addition to original quantitative research and analysis, the study draws upon and welcomes the findings of other research efforts. What emerges is a picture of a front for cyber criminals who specifically target consumers in the United States and elsewhere. It provides hard data regarding specific current activity within McColo and associated networks, explains how consumers are targeted, and describes McColo's virtual network structure.

The philosophy behind the study is that we as an Internet community act in accordance with the ACM (Association of Computing Machinery) code of ethics, e.g. avoiding harm to others. "Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm Internet users and the general public. It is the Internet security community's responsibility to blow the whistle. While we do not take the actions to 'stop' the cyber criminals, we do urge those who provide connectivity or peering to consider this report and their role.

### **Stop Press – Nov 11 2008 – 7:30pm (EST)**

According to the [CIDR report](#) which shows routing for AS networks. McColo has been de-peered by Hurricane Electric (HE) one of the major routes of transit for McColo tonight. An explanation is shown in the [Washington Post](#), we ensured HE was aware of this report's content. This clearly demonstrates that, when presented with the appropriate evidence of criminal activity, the Internet community can bring about the positive forces necessary to purge it. As a note of caution there is still limited access to the McColo badness and there still many other bad actors on the Internet, but we can believe in 'change'.

# 1. INTRODUCTION

---

This report's purpose is to provide specific facts and analysis on bad actors which provide Internet hosting. In this report we focus on McColo Corp., which was described by Kaspersky Labs as "...the US hosting provider MCCOLO, whose resources have long been used for distributing malicious programs and hosting cybercriminal sites"

It is the second in a series, of Cyber Crime USA. The first report, "[Atrivo – Cyber Crime USA](#)," in itself did not bring down Atrivo. But it did highlight bad actor(s) on the Internet, drawing upon five years worth of anti-spam, abuse, malware, and botnet research.

However, the report stressed such activities could not occur if commercial third parties or other organizations did not collaborate. Such collaboration is mostly without charge but can be the equivalent of turning a blind eye to the bad activity while accepting the cash, as perhaps several commercial hosting or Internet servers did. Cyber criminals totally depend on the complicity, cooperation or ignorance of providers in the U.S, Europe or elsewhere.

After publication, Atrivo/Interchange was "de-peered," in both a technical and normal sense. North American Network Operators' Group (NANOG) operators have the right to de-peer anyone they don't trust -- these are voluntary relationships in which providers accept each other's traffic. The report and the community response was the straw that broke the camel's back, after many years of assuming either law enforcement or someone else would act. Since Atrivo/Interchange went dark, independent reports showed a 10 percent drop in spam worldwide and less badware available.

As Richard Donaldson, COO of United Layer, the last provider to de-peer Atrivo / Interchange, [stated](#), "What is the ethical thing to do in this situation? Can people reform? Can they stay reformed?"

The answer is a split decision; No in the case of clearly cybercriminal operated enterprises, but happily, yes if we take, for example, Directi, the major Asian domain registrar, which had received much criticism and some bad press. It was able to demonstrate its resolve, with the help of the community and a strengthened abuse team. It has now downed 175,000 bad domains, and stripped the privacy from 500,000 resellers, based upon proven abuse; see [HostExploit's latest report](#).

Some have faulted the Atrivo report as violating the principle of "Net neutrality." Net neutrality means different things to different people. At its most fundamental, Net neutrality is about making sure that users have control of what content they receive. But as the Atrivo and now McColo reports demonstrate, what we are talking about is criminal activity aimed at innocent parties. If Net neutrality is an extension of freedom of speech, it is worth noting that not all speech is protected. Words aimed at defrauding people--to say nothing of active taking of others' property via malware--are not lawful. In fact, those that assist fraudulent speakers are at times found to share legal as well as moral culpability.

HostExploit follows the wisdom, of Eleanor Roosevelt, who said: "Do what you feel in your heart to be right, for you'll be criticized anyway. You'll be damned if you do, and damned if you don't." As professionals, we blew and are continuing to blow the whistle, while mindful of the consequences and potential criticisms, it is absolutely worth it.

This report raises the question: should the Internet community tolerate McColo's presence?

## 2. THE TOXIC NETWORKS

---

In this report we focus on a small group of 'bad actor' Internet network operators, especially McColo. The five shown in this section are not specifically associated apart from the similar aspects of badness (see page 20). To assist the reader:

- This bullet = key points & summary items of information in the main sections
- The AS # (Autonomous System Number) is an identity for the network operator, issued by Internet Assigned Numbers Authority (IANA). For this and other terms, see Appendix 3 The Glossary of Terms
- The numbers showing e.g. Infected / badware sites = 62 (from 3,072 IP addresses – exploit ratio 2.02%) the **Exploit Ratio** is a measure of known infected web sites per IP address. A measure of clean hosting should be say a maximum of **0.01%**
- Each overview shows a 'bad data history' of security observation e.g. (bad data history 05/2006 – 10/2008)
- It should be noted all data contained within this report is recent Nov 6<sup>th</sup> 08 or shown as historical.

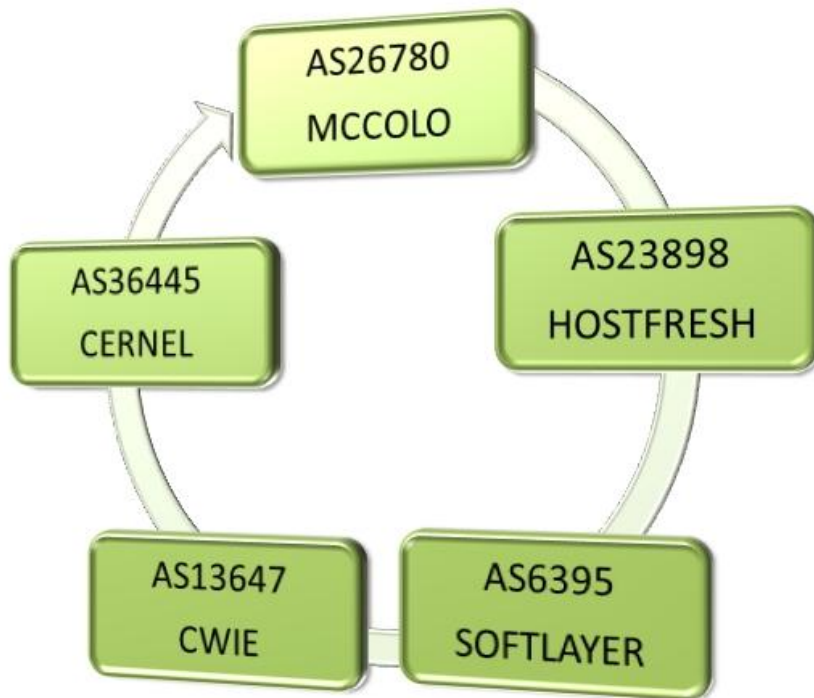


Figure 1 – THE TOXIC NETWORKS - HostExploit.com v2.0 2008

AS26780  
MCCOLO

## 2 a - McCOLO

Serving & Hosting: Botnet infrastructure, Spam, Mal Links, Malware warehousing, Rogues & Fakes, & Illegal Content (child pornography).

Overview of current badness instances (bad data history 05/2006 – 10/2008):

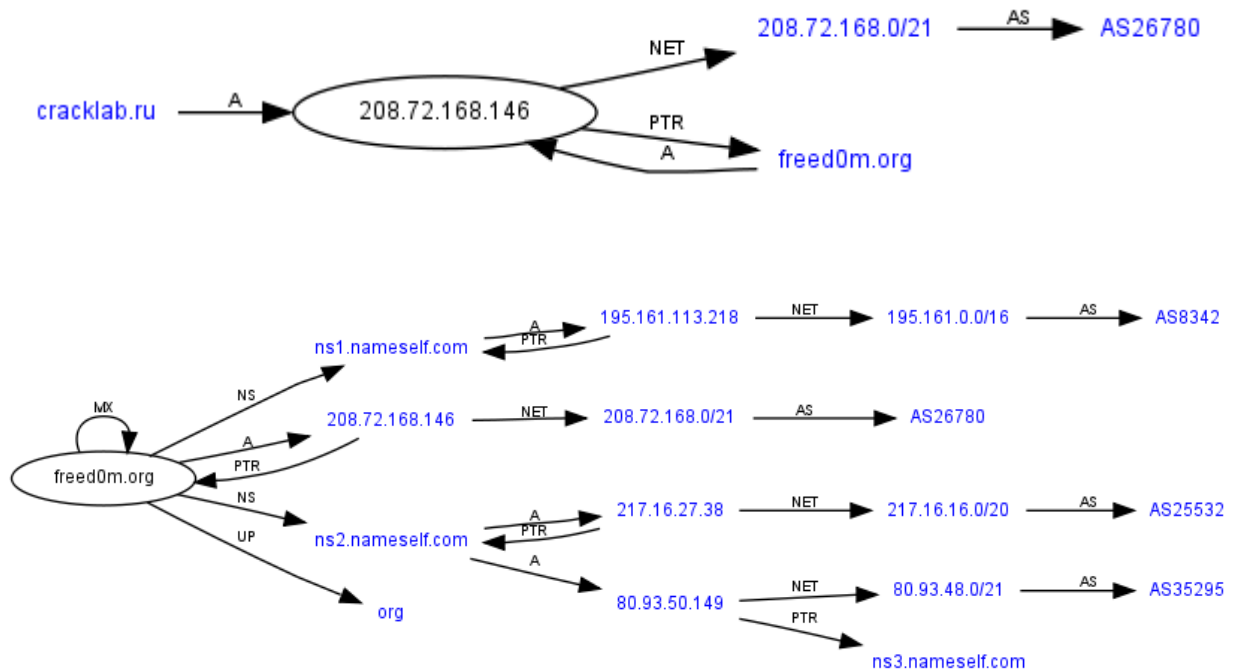
- HE Pharm & spam = 172
- HE Botnet C&C = 24
- HE Mal Links = 969
- HE Rogues & Malware = 64
- HE Infected / badware sites = 62 (from 3,072 IP addresses – exploit ratio 2.02%)
- HE Illegal content = 40 locations & payment systems

## Rustock - Cracklab / Freed0m & McColo

Rustock advisory May 08 - rootkit named NTLDRBOT (ref: [SysInternals Forum](#)) authored by Cracklab.ru / Freed0m.org 208.72.168.146 Hosted by McColo & co-hosted name servers by:

- HE AS8342 RTCOMM Autonomous System Moscow, Ru
- HE AS35295 PETERHOST, Ru

The following two figures diagrammatically show the relationship of Internet servers;



## Rustock and All That – Virus List

“The hallmarks of the IFrameBiz group have tended to be domains in the .biz zone and filenames in the loadadv\*.exe format.

The group can be traced back to Russia, where most of its members reside. In the early stages of its existence the group extensively used hosting resources in St. Petersburg. It is also known to have collaborated with the infamous RBN (Russia Business Network), which many experts also associate with the city.

The IFrameBiz botnet is actively used to distribute new malicious programs. Customers pay for a time period during which their Trojans will be distributed via the botnet. Then the Trojans are downloaded to victim computers. It is common for the same downloader (e.g., Tibs) to install several Trojans from different customers. The service is in demand, and customers think nothing of their requests being fulfilled at the same time as several other client orders.

To perform this task, the botnet connects to a server at [208.66.194.215](http://208.66.194.215) and receives message templates from it. The IP address belongs to the US hosting provider **MCCOLO**, whose resources have long been used for distributing malicious programs and hosting cybercriminal sites.” Ref: [Kaspersky / Virus List](#)

Currently McColo hosts C&C (command and control) servers for some of the biggest botnets - Rustock, Srizbi, Pushdo/Cutwail, Ozdok/Mega-D and Ghag all have part or all of their master control servers hosted by McColo. When Atrivo was de-peered, the world saw a brief drop in the output of spam. If McColo were ever to suffer the same fate, worldwide spam output would probably be cut in half (ref – [Joe Stewart – Secureworks](#)) - ([ref Srizbi – McAfee](#))

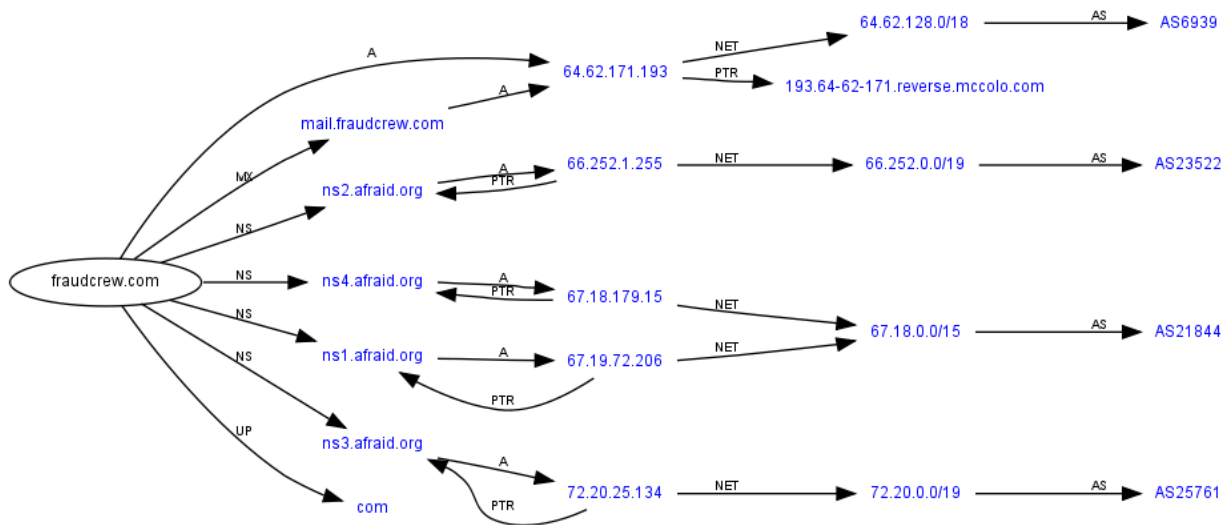
## FraudCrew & McColo

FraudCrew = CoolWebSearch hijackers – Sunbelt & [SiteAdvisor](#)

### 64.62.171.193

base	route	as
193.64-62-171.reverse.mccolo.com		
fraudcrew.com	64.62.128.0/18	AS6939
mail.fraudcrew.com	Hurricane Electric 55	Hurricane
proxy.fraudcrew.com	South Market St San Jose, CA	Electric

base	ip	route	as
193.64-62-171.reverse.mccolo.com	64.62.171.193	64.62.128.0/18	AS6939
mccolo.com	208.66.192.100	208.66.192.0/22	AS26780
	208.66.192.102		
	208.72.175.3	208.72.168.0/21	
	208.66.195.232	208.66.192.0/22	
	208.72.175.5	208.72.168.0/21	
	208.66.192.101	208.66.192.0/22	
	208.72.175.6	208.72.168.0/21	



## Sinowal / Torpig / Mebroot & McColo

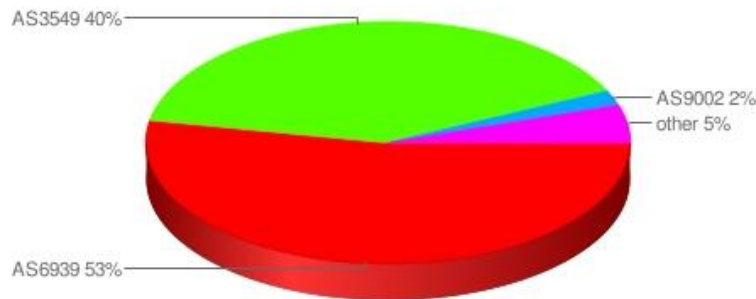
Below is shown an example of command and control via McColo housed botnets of The Sinowal Trojan virus tracked by [RSA](#), which stole the details of about 500,000 online bank accounts and credit and debit cards. It originated from McColo IP address 208.72.169.56

**208.72.769.56**

base	route	as
56.208-72-1.reverse.enterhost.com	208.72.0.0/22	AS26780 MCCOLO

# AS26780 MCCOLO AS McColo Corp

## Peer and upstream distribution



## Brief information

Number of prefixes:	3
Regions:	2
IP numbers:	3328
Unique IP numbers:	3072
Overlapping IP numbers:	256

### Major Peers & Transit – for McColo

- HE AS3549 = GBLX (Global Crossing) – 40%
- HE AS6939 = HURRICANE Electric – 53%

McColo names as partners “mccolo.com/about/” = Cisco, Hewlett Packard, 3Com, Hurricane Electric, GLBX (Global Crossing), Ynot

McColo Locations =



Stated Postal - 64 East Main St. Box 275, Newark, DE, 19715 USA

The actual PO Box is operated by SIMILEX, which provides online Delaware incorporation services.

Brewed Awakenings, Floundergraphics, Italo's Tailor Shop & Cleaners are located at 64 E Main St Newark, DE

Pictured is the actual street view of - 64 East Main St. Newark, DE

Stated server location - MarketPostTower IT center, San Jose, CA, USA.

Actual trace routes of McColo IP addresses - Palo Alto, CA and Fremont, CA i.e. Hurricane Electric

**McColo. Hosting Solutions.**  
 Dedicated Virtual Hosting Colocation Support About Company

## About Company

McColo Hosting Solutions offers best-of-breed IT services for any customer, starting from individuals to large companies and corporations.

McColo Benefits:

- Safe and modern Datacenter
- Leading internet providers
- Quality tested equipment
- Trained staff

Our datacenter is situated in top-level modern MarketPostTower IT center, San Jose, CA, USA.

Total bandwidth throughput exceeds several gigabits.

We use only certified equipment providers, such as Cisco, IBM, Intel, Supermicro.


Thanks to our professional trained staff, we managed to lower risks to the minimum.


Become our customer today and open new horizons for your business.


## We accept all major payment methods:


- Wire Transfer
- Credit Card\*


## Our partners


 [www.cisco.com](http://www.cisco.com)

 [www.hp.com](http://www.hp.com)

 [www.3com.com](http://www.3com.com)

 [www.he.net](http://www.he.net)

 [www.globalcrossing.com](http://www.globalcrossing.com)

 <http://www.vnot.com>



## Contact us

**General information:**  
[info@mccolo.com](mailto:info@mccolo.com)

**Tech support:**  
[support@mccolo.com](mailto:support@mccolo.com) (ticket system)

**Sales dept:**  
[sales@mccolo.com](mailto:sales@mccolo.com)

**Virtual Hosting:**  
[virtual@mccolo.com](mailto:virtual@mccolo.com)

**ICQ:**  
 407737  
 403222

**Phone:**  
 +1-914-455-5598

**Fax:**  
 +1-408-716-8899

**Our post address**  
 McColo Corp., 64 East main st.,  
 Box 275  
 Newark, DE, 19715, USA

**McColo. Hosting Solutions.**  
 Dedicated Virtual Hosting Colocation Support About Company

## Dedicated Servers

McColo Hosting Solutions offer you:

- Maximum stability for your business
- 24/7 live support
- 99.99% uptime
- Enterprise level datacenter
- DDoS protection
- User-friendly trained staff

Each server includes:

- only best parts from Supermicro
- remote reboot service access (APC)
- online statistics access
- full root-level server access
- any OS at your choice

### Basic

Processor: P4 3.2 Ghz  
 RAM: 1GB DDR  
 Hard Drive: 2x160 GB Sata  
 OS: Your choice  
 Bandwidth: 10 Mbps  
**\$210/month**

### Advanced


Processor: Intel Core 2 Duo  
 RAM: 2GB DDR  
 Hard Drive: 2x160 GB Sata (raid)  
 OS: Your choice  
 Bandwidth: 10 Mbps  
**\$299/month**

### Professional

Processor: Dual Xeon Dual Core 3.0  
 RAM: 2GB DDR-II  
 Hard Drive: 2x250GB Sata(raid)  
 OS: Your choice  
 Bandwidth: 100 Mbps  
**\$1995/month**

## Need Customization?

contact sales manager  
**+1 (914) 455-5598**

 **407737**  
 mcalexy  
[sales@mccolo.com](mailto:sales@mccolo.com)

Dedicated Servers SLA AUP

Sample McColo's web pages

(a) Contact and partner page

(b) Pricing for dedicated (bulletproof?) serving

AS23898  
HOSTFRESH

## 2 b - HOSTFRESH

Was routed by Atrivo AS27595, the hub of malware in the USA for years until Atrivo / Intercage were de-peered from the Internet.

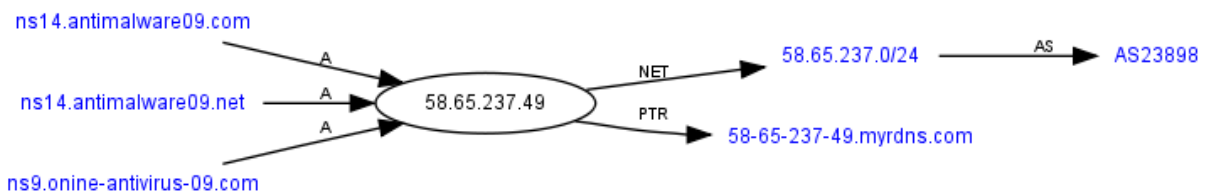
Overview of current badness instances (bad data history 05/2006 – 10/2008):

- HE Pharm & spam = 3,284
- HE Rogues & Malware = 16
- HE Infected / badware sites = 49 (from 11,264 IP addresses – exploit ratio 0.44%)

The botnet based at IP address 58.65.237.49 from Hostfresh was used in the cyberwarfare DDos on Georgia government web sites.

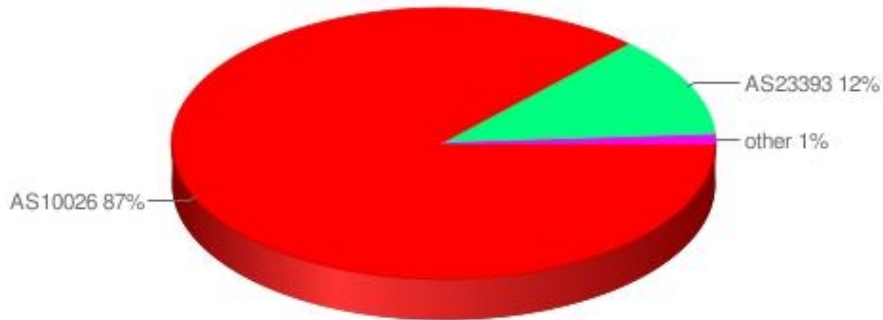
### 58.65.237.49

base	reverse	route	as
ns14.antimalware09.com	58-65-237-49.myrdns.com	58.65.237.0/24 Proxy-registered route object	AS23898 HOSTFRESH AS AP HostFresh Internet Service Provider
ns14.antimalware09.net			
ns9.onine-antivirus-09.com	-		
58-65-237-49.myrdns.com			



# AS23898 HOSTFRESH AS AP HostFresh Internet Service Provider

## Peer and upstream distribution



### Brief information

Number of prefixes:	20
Regions:	4
IP numbers:	15360
Unique IP numbers:	11264
Overlapping IP numbers:	4096

#### Major Peers & Transit – for Hostfresh

- AS10026 = ANC Asia Netcom Corporation – 87%
- AS23393 = ISPRIME, Inc – 12%



### 2c - CERNEL

Was routed by Atrivo AS27595, the hub of malware in the USA for years until Atrivo / Interchange were de-peered from the Internet.

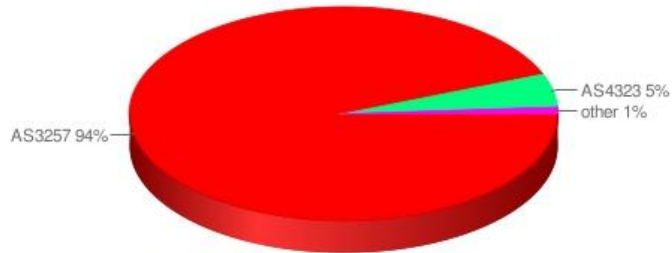
#### Overview of current badness instances (bad data history 05/2006 – 10/2008):

- Pharm & spam = 79 (mostly registered with EstDomains)
- Rogues & Malware = 32
- Infected / badware sites = 66 (from 4,864 IP addresses – exploit ratio 1.36%)

67.210.0.0/20 is listed on the Spamhaus Block List ([SBL 58520](#))

# AS36445 CERNEL Network Ltd

## Peer and upstream distribution



### Brief information

Number of prefixes:	6
Regions:	5
IP numbers:	5632
Unique IP numbers:	5376
Overlapping IP numbers:	256

### Major Peers & Transit – for Cernel

- HE AS3257 = Tiscali Intl Network BV Formerly Nacamar Data Communications, Germany – 94%
- HE AS4323 = Time Warner Telecom – 5%

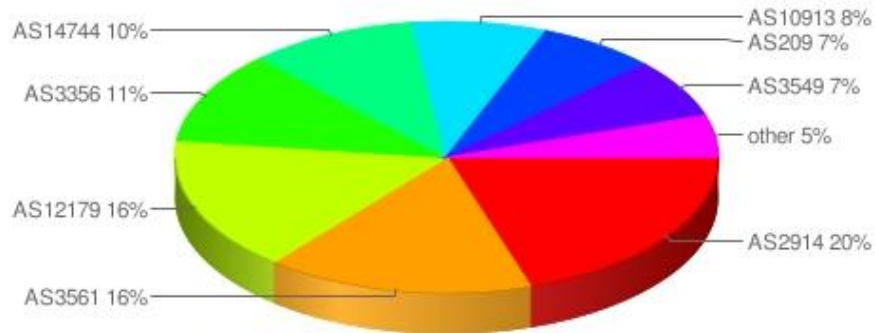


### Overview of current badness instances (bad data history 05/2006 – 10/2008):

- HE Pharm & spam = 12,420
- HE Rogues & Malware = 167
- HE Infected / badware sites = 1,538 (from 276,480 IP addresses – exploit ratio 0.56%)

# AS36351 SOFTLAYER Technologies Inc

## Peer and upstream distribution

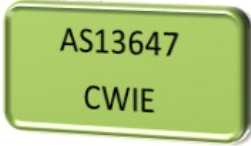


### Brief information

Number of prefixes:	49
Regions:	10
IP numbers:	443392
Unique IP numbers:	302592
Overlapping IP numbers:	140800

### Major Peers & Transit – for SoftLayer

- AS2914 = NTT Communications – 20%
- AS3561 = SAVVIS Communications – 16%
- AS12179 = Internap Network Services (2 blk)= 16%
- AS3356 = Level 3 Communications = 11%
- AS14744 = Internap Network Services (4 blk)= 10%
- AS10913 = Internap Network Services = 8%



## 2e - CWIE / TRANQUIL HOSTING

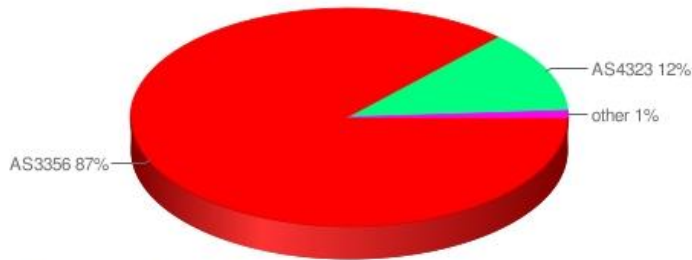
Although on a smaller scale than others in this category it is shown here as a recent example of an emerging network bad actor. Note: 200 rogue and malware NS (name servers) are detected, although an important element in cyber crime serving they are not detected by conventional badness detection.

### Overview of current badness instances (bad data history 02/2008 – 10/2008):

- HE** Pharm & spam = 15
- HE** Botnet C&C = 8
- HE** Mal Links = 4
- HE** Rogues & Malware = 4
- HE** Infected / badware sites = 1 (from 11,520 IP addresses – exploit ratio 0.1%)
- HE** Rogue & Malware Name Servers = 200 (all on IP 208.79.82.50)

## AS13647 CWIE BBBJ83393

### Peer and upstream distribution



### Brief information

Number of prefixes:	8
Regions:	6
IP numbers:	11520
Unique IP numbers:	11008
Overlapping IP numbers:	512

### Major Peers & Transit – for CWIE / Tranquil Hosting

- HE** AS3356 = Level 3 Communications – 87%
- HE** AS4323 = Time Warner Telecom – 12%

### 3. McColo - A CASE STUDY– THE MECHANICS

Within this section we focus on how the malware delivery system works around a specific and recent example. This demonstrates McColo’s role in malware warehousing and is also shown within Sunbelt’s CWS Sandbox and by Threat Expert <[malware report here](#)>



Figure 2 - McColo - Malware Warehousing and Botnet Infrastructure - HostExploit.com v2.0 2008

DNS Info	IP Address	Domain	Registrar	AS #	Network	Country	Blacklists
Host Name / IP	23.176.184.238	pictures-base.com	HostHost.Biz	AS35057	UltraNet Ltd	Latvia	SBL67313
Data posted to URLs	78.157.142.119	image-big-library.com	HostHost.Biz	AS35057	UltraNet Ltd	Latvia	SBL67313
	208.85.181.59	nessotr-help.com	Domainmonster	AS29809	NETRCLLC	US	SBL65094
	78.157.142.45	bigimagecatalogue.com	season	AS35057	UltraNet Ltd	Latvia	SBL67313
Download URLs	78.157.142.46	winsystemsUPPORT.com	HostHost.Biz	AS35057	UltraNet Ltd	Latvia	SBL67313
	193.142.244.94	winsystemsUPPORT.com	HostHost.Biz	AS30783	LUCKYNET 2	Israel	SBL57948
	213.189.9.108	protect.advancedcleaner.com	x	AS25525	REASONNET	Netherlands	x
	76.74.249.30	ad2cash.net	Tucows	AS13768	Peer 1	Canada	x
	93.190.139.221	gomyhit.com	x	AS15435	KABELFOON	Netherlands	x
	78.157.142.47	bestvirusremover2008.com	Sagent Group	AS35057	UltraNet Ltd	Latvia	SBL67313
	92.62.101.67	ds67.esthost.eu	Esthost	AS39823	COMPIC Ltd	Estonia	SBL68255
Warehoused Malware	208.72.169.114	x	x	AS26780	McColo Corp	US	EmThreats

HostExploit.com- Cyber Crime - USA - V 2.0 - 2008

The table above show the interrelationships of the various malware affiliates hosting and serving. Notes:

- McColo acts for malware warehousing, i.e. the centralized point for malware to be called download to a user's PC



A fake anti-virus display on a PC user's computer.

# 4. McColo – THE BUSINESS OF CYBER CRIME

Terms & Conditions | Privacy policy | Refund policy | Company

**XP ANTIVIRUS protection**

Not satisfied with your current Windows antivirus software ?  
Make the switch to XP antivirus Protection and enjoy your system work without any influence of spyware and viruses

**XP antivirus product details:**

- Basic price is \$49.95
- Worldwide shipping
- Secure credit card payments
- Advanced Customer Support service

**TRY FREE** **BUY NOW**

**VIRUS WATCH**

**latest Virus Alerts**

- W32.Trojan.Downloader.s
- W32.Backdoor.j
- Worm.Chernobyl6.a
- W32.FileDeleter.E2.b
- Worm.Trojan.OfficeWorm.k

**latest Threats**

- Spyware.Wather.ic
- Spyware.CreditCard.er.y
- Adware.Clicker.P2.e
- Adware.TrojanFactory.F
- Spyware.Zlob.di

**FREE scan**

**PROTECT YOURSELF !**

Is your computer infected?

Stop spyware and spam infecting your PC!

**START SCAN**

Find out right now with our **FREE SPYWARE SCAN**

The whole process takes less than 5 minutes and is **FREE** of all charge

antispay software for Windows XP

Copyright © 2008 Bolzar LTD  
2007 XP antivirus | All Rights Reserved

## Company Details

### BOLZAR LIMITED

Arch. Makariou III. 69. TLAIS TOWER. P.C. 1070. Nicosia, Cyprus. Contact: [company@protectionpurchase.com](mailto:company@protectionpurchase.com)

## 208.72.162.158

base	route	as
protectionpurchase.com	208.72.162.0 / 21	AS26780
securedownloadcenter.com		MCCOLO

"The Business" = protectionpurchase.com - e.g. serving Anti-Virus 2009 - (served by McColo) -

### Protectionpurchase.com users come from these countries:



### Protectionpurchase.com traffic rank in other countries:



### Data courtesy of Alexa

Averaging 40,000 US visitors and many internationally per day during October 2008 - has its own Google analytics acct. UA-2403830-2 - out of 75 million web sites currently 41,800 on Alexa ranking - (for comparison the well known blog site Internetevolution.com has a traffic rank of: 43,939) – What is surprising is the amount of web traffic with many forms of blocking e.g. OpenDNS, Spamhaus, IP blocking / ISP blacklists etc.



*"Clipped from: secure.xp-antivirus.com"*

Your Purchase is Backed By Our 30-Day Money Back Guarantee!

Fully Secure & Encrypted Ordering - Even Safer Than Over the Phone.

Your Email Address and Personal Information are private and NEVER resold.

**Thank you. Your transaction has been accepted.**

Thank you for the recent purchase XP Antivirus software.

**PLEASE PRINT!**

THIS IS A ONE-TIME CHARGE.

Product/Service ordered: License for XP antivirus

This charge will appear on your card statement as [www.innovage2000.com](http://www.innovage2000.com) or [www.pandora-software.info](http://www.pandora-software.info)

ACTIVATION INFORMATION:

**axxxxx@hotmail.com**

Registration key: 5647-8221-6321

If you need any assistance please go to our Support page here <http://paymentdetailization.com/support.php>

It may fall into your e-mail Bulk/Junk/Spam folder. Please go to your Mail box, and mark this e-mail as NOT SPAM as shown below.

## How to fight back smarter, disrupt the flow of money?

The scareware and fake anti-malware campaigns work on two levels, the first is installing malware (downloads up to 30 other independent trojans and keyloggers) and the second is direct billing - getting victims to buy the misleading and dangerous products with a credit card.

We urge the community from now on to also hunt down the payment processing sites and hurt the crooks involved in their wallets.

A quick example: [premium-pc-scan.com](http://premium-pc-scan.com), [antivirus-live-scan.com](http://antivirus-live-scan.com), [pc-antivirus-scan.com](http://pc-antivirus-scan.com), [antiviruspcadvisor.com](http://antiviruspcadvisor.com), and [quick-antivirus-scan.com](http://quick-antivirus-scan.com) amongst 100 others all used the same payment gateway on [xp-antivirus.com](http://xp-antivirus.com). Taking down that vital domain name took 1 email and 2 hours wait time. This was a secure site where the crooks had also gained a valid SSL certificate from Equifax. For this reason a request was also made to lock the domain and ensure it was kept isolated until the certificate had expired.

As demonstrated by Joe Stewart this scam installed 154,825 versions of the software in just 10 days, and then 2,772 copies of the program were later purchased from those infected users. Based on that conversion rate, it is estimated that an affiliate could expect to earn over \$5 million annually by maintaining a botnet large enough to force between 10,000 and 20,000 installations on a daily basis.

# 5. THE DATA

In the numbers showing on this page, e.g. Infected / badware sites = 62 (from 3,072 IP addresses – exploit ratio 2.02%), the **Exploit Ratio** is a measure of known infected web sites per IP address. A measure of clean hosting should be say a maximum of **0.01%**

asn	as_name		feb	mar	apr	may	jun	jul	aug	sep	oct	# of Ips	Exploit ratio
26780	MCCOLO	US	12	24	15	20	12	17	12	12	62	3,072	2.02%
36445	CERNEL (was InterCage)	US?	0	6	8	8	8	19	22	115	66	4,864	1.36%
36351	SOFTLAYER	US	1,812	2,622	3,325	3,507	2,130	2,656	2,574	2,502	1,538	276,480	0.56%
23898	HOSTFRESH	US? / HK	62	91	65	45	55	75	84	62	49	11,264	0.44%
13647	CWIE	US	2	1	1	0	1	2	1	1	1	11,520	0.01%
39823	COMPIC	Estonia	38	27	25	28	60	57	71	47	41	4,608	0.89%
35057	ULTRANET	Bulgaria	0	0	0	0	0	5	25	99	40	8,192	0.49%
25525	REASONNET	NL	91	63	50	65	62	43	32	37	55	98,560	0.06%
13768	PEER1	CA/ Guam	236	216	261	227	206	414	452	416	265	484,352	0.05%
15435	KABELFOON	NL	0	0	2	3	13	11	1	1	1	132,096	0.00%
29809	NETRCLLC	USA?	116	107	64	16	14	25	0	0	0	1,792	0.00%
30783	LUCKYNET	Israel	1	1	1	1	5	5	0	0	0	1,024	0.00%
43513	NANO	Latvia	0	1	2	3	2	26	67	80	329	1,280	25.70%
39561	AGAVA JSC	Russia	861	595	607	523	364	417	397	418	219	8,192	2.67%
29802	No Whois Entry (HVC AS?)	?	187	244	247	408	374	653	396	426	268	33,024	0.81%
24940	HETZNER	Germany	368	451	425	337	406	441	452	302	338	238,592	0.14%
16265	LEASEWEB	NL	431	718	541	296	470	507	533	322	252	215,040	0.12%
39318	NUCLEUS BVBA	Belgium	1	1	1	1	12	4	3	2	2	2,816	0.07%
34187	RENOME	Ukraine	0	0	0	0	0	1	11	4	6	33,536	0.02%
15146	CABLEBAHAMAS	Bahamas	0	1	2	5	2	8	7	4	2	73,472	0.00%

HostExploit.com - 11/08

Comparative Site Infections

Data courtesy of StopBadware based on data provided by Google - analysis HostExploit

asn	as_name	Country	feb	mar	apr	may	jun	jul	aug	sep		# of Ips	Exploit ratio
27595	ATRIVO / INTERCAGE (before de-peered)		1,981	1,048	1,023	1,007	885	1,132	1,289	1,135		31,232	3.63%
44394	BUILDHOUSE	Ru	4	9	12	15	17	40	30	18		512	3.52%
30968	INFOBOX	Ru	308	150	133	136	149	218	144	189		16,384	1.15%
41947	WEBALTA	Ru	103	108	107	89	104	114	154	111		11,520	0.96%
26627	PILOSOFT	US	51	46	41	40	22	28	58	65		29,952	0.22%
29131	RAPIDSWITCH	UK	32	69	82	133	92	92	101	114		68,096	0.17%
6395	BROADWING	US	130	137	176	155	153	225	232	274		210,432	0.13%
32959	LITEUP	Ru?	0	8	6	4	2	4	2	2		4,864	0.04%
26769	BANDCON	US	1,935	0	553	0	0	0	0	2		16,128	0.01%
4657	STARHUB	Singapore	39	50	51	37	28	37	36	30		275,712	0.01%
9121	TTNET	Turkey	217	472	533	434	439	569	583	585		5,916,928	0.01%
4436	NLAYER	US	13	1	1	2	3	2	2	2		55,296	0.00%
23342	UNITEDLAYER	US	1	0	0	0	0	0	0	0		24,320	0.00%

HostExploit.com - 11/08

Comparative Site Infections

Data courtesy of StopBadware based on data provided by Google - analysis HostExploit

McColo	IP
securedownloadcenter.com	208.72.168.158
ietoolsupdate.com	208.72.168.84
iexplorerfile.com	208.72.168.92
voodooorevenue.com	208.72.169.100
secureupdateserver.com	208.72.169.100
fraudcrew.com	208.66.195.89
cluster-club.info	208.72.168.151
paidgamecard.info	208.72.168.151
uniontrade.biz	208.72.168.151
russianwoodshed.com	208.72.168.170

Sample Rogues & Malware      neinfosecforum  
**HostExploit V2.0 2008**

HostFresh	IP
windefender.com	58.65.234.193
antivirus2008x.com	58.65.235.9
vipantisetup.net	58.65.235.9
anti-malware09.com	58.65.237.50
antimalwaresuite2009.com	58.65.234.193
cleaner2009pro.com	58.65.234.193
assisback.com	58.65.236.1
myrdns.com	58.65.234.105
geil-de.info	58.65.237.121
tut-pusto.info	58.65.237.122

Sample Rogues & Malware      neinfosecforum  
**HostExploit V2.0 2008**

Softlayer	IP
antispywarecontrol.com	208.43.41.16
antispywaremaster.com	208.43.41.17
e-Spyware.com	67.228.114.236
pcsecuritynotice.com	67.228.120.3
vidspanet.net	67.228.17.138
pchealthplan.com	74.86.148.179
s0s1.net	67.228.189.192
ogercnt.info	74.86.11.178
aeaer.com	75.126.3.216
070808.net	75.126.3.218

Sample Rogues & Malware      neinfosecforum  
**HostExploit V2.0 2008**

Cernel	IP
malware-scanner.com	67.210.13.94
young-girls-board.com	64.28.187.24
teenysexx.com	67.210.12.2
k9flix.info	67.210.12.53
blaze-search.com	67.210.12.53
free-animal-sex.com.ua	67.210.12.53
6464.biz	67.210.13.94
e7da7.biz	67.210.13.94
fist-sex.info	67.210.13.94
little-teens.info	67.210.13.94

Sample Rogues & Malware      neinfosecforum  
**HostExploit V2.0 2008**

CWIE / Tranquil	IP
latinhackz.net	209.170.150.178
ns1.adtraff.com	208.79.82.50
ns1.advancedprivacyguard2008.com	208.79.82.50
ns1.advancedprivacysuite2008.com	208.79.82.50
ns1.debelloworm2008.com	208.79.82.50
ns1.registrydoctorpro2008.com	208.79.82.50
ns1.antiver2008.com	208.79.82.50
ns1.virusremover2008.com	208.79.82.50
ns1.pcvirusremover2008.com	208.79.82.50
ns1.powerfulvirusremover2008.com	208.79.82.50

Sample Rogues & Malware      neinfosecforum  
**HostExploit V2.0 2008**

## Section 2. - Toxic networks

Added Data - Sample Badness (Rogues, malware, and Name Servers) discovered on the 5 Toxic Networks selected in this report

## 6. ICANN, REGISTRARS & YOUR SPAM

Spam is a word ICANN and the registrars don't like to discuss much less address. Bring up the word spam and the programmed response will be "it's not in our contract/mandate." In fact, the Internet community has spent more time explaining why they are not responsible for spam than really looking into the problem. By researching and examining the problem we have found it is solvable. The causes are known, the breakpoints have been indentified, the policy failures dissected. So why does the internet remain broken? The price of this fix is apparently way too high for some involved. At the core of Internet criminality is a rampant abuse of the infrastructure, the domain name system.

The Registrars are responsible for keeping accurate records on their customers, and ICANN is responsible for keeping track of the Registrars. The room for abuse starts at the top, as ICANN's core contract with Registrars (the RAA) does not require public disclosure of ownership or location for the companies that issue domain names. This is a practice that would unacceptable in any other industry. Since there is a lax accountability from the top down, it has become trivial for criminals to remain anonymous while silently pulling the strings at certain Registrars.

We reported on criminal influence at Estdomains and others and complete lack of due diligence elsewhere including Xin Net, Beijing Innovative and others. These are in essence self-policing companies, who in theory are supposed to keep criminals off their networks. But when ICANN won't enforce its contracts with Registrars and criminals are throwing money at Registrars, the choice is obvious. In the end it hurts the Internet user and consumer. As consumers and users of the global network we are being marginalized. Just this past week Knujon's Dr. Robert Bruen traveled to an ICANN meeting to speak on behalf of us and the consumer but was told that his voice was unwanted.

To its credit, ICANN has begun a new wave of compliance enforcement, issuing breach notices against Estdomains, Beijing Net, Joker and others. However, none of these have "gotten over the wall," as it were. None of the bad players have been truly punished or made to pay for damages against internet users. What is missing and badly needed is consumer advocacy and open public review of the process. This will never really be a global network if the decisions are made behind closed doors by unknown players.

Directi Domain Abuse Actions -Report Oct 08	# of Domains
False whois	9,034
Fake Pharma	4,379
Spam	2,179
Phishing/spoofing	86
Malware	79
Financial fraud	46
Pedopornographic	19
Co-network	34,725
Abusive Resellers Domains Suspended	125,000
<b>Total domains Suspended</b>	<b>175,547</b>
Privacy Removal – abusive domains	27,000
Privacy Removal – Resellers	500,000
<b>Total PrivacyProtect Removal</b>	<b>527,000</b>

Source: HostExploit.com / Directi - 2008

This figure demonstrates the results of teamwork between HostExploit, Knujon, the community and Directi as a result of the first cyber crime report, in October 2008. This shows changes can be made, with proper analysis of abuse and analysis false 'who is' data. This is real progress and could be a model of cooperation for the industry.

## 7. CHILD PORNOGRAPHY

---

Child pornography (CP) is a difficult topic for any research into cyber crime or badness on the Internet. In most cases it is left solely to the actions of law enforcement of child protection agencies, and avoided by the security community. This avoidance is warranted due to the difficulty of exposing such activity i.e. the lurid nature and not publishing commonly known CP websites or online activity, as this can also provide information to those who want to gain access to such services. All should read the '**Researchers Note**' at the end of this section.

Research and contribution has shown at least 40 confirmed CP websites, name servers, and CP payment systems recently served by McColo. With sub-domains, and associated links it is also the tip of the iceberg, however. As indicated earlier, with McColo and modern cyber criminal techniques these websites and domains move locations very rapidly, as in shuffling a deck of cards. In these cases, at the time of investigation, the websites and domains in question are also co-hosted or name served by:

- HE AS12578 APOLLO LATTELEKOM Latvia
- HE AS3595 Global Net Access, LLC 1100 White Street Atlanta, GA USA
- HE AS9121 TNet TURKEY (via - AbdAllah Internet Hizmetleri)

The registrar for a few on the CP domains is:

- HE Domain Name: zzzzMODEzzzz.INFO / Last Updated On: **06-Nov-2008** 15:31:27 UTC / Expiration Date: 17-Oct-2009 09:40:12 UTC **Sponsoring Registrar: EstDomains.** (While ICANN ponders Estdomains on / off suspension, the cyber criminal activity continues.)

Discussion: From investigation into this topic from a cyber criminal hosting perspective, there is limited active and open source research. However there tend to be a few areas to consider as to why networks or particularly their peers would even have an interest. Considering such hosting is more likely to raise the interest of law enforcement.

- HE Research claims differ wildly; at the high end 30-40% of online porn is CP, to the position that only very few remaining very following the success of law enforcement, and due to a heightened public awareness in this area of cyber crime.
- HE From minimal analysis of these known CP payment systems, it would still appear that such sites receive 15 – 25,000 visitors daily.
- HE Why would such CP sites be with McColo? This is clearly due to the 'bullet-proof' hosting offered and its ability to fast-flux the IPs involved
- HE When considering the economics involved, even though CP is noted as being of high return, e.g. a reported \$90 for limited time access for a user. This should be heavily outweighed by the value of spam, rogue, and malware serving, so there is an added issue of why high volume cyber criminals would have any interest in this area. From selective sources this comes down to a few possibilities:

- (a) Many active CP sites are also laden with trojans and malware, on the basis that no user will complain.
- (b) To gain access to CP content there is still the use of credit cards or other payment mechanisms, it would appear the main value here is to gain uncomplaining 'mules', easy targets for extortion, and blackmail.

***Researchers note:*** We at HostExploit encourage community awareness, investigation and exposure of cyber crime. It is important to stress in virtually all jurisdictions, US and internationally, it is against the law to download content, possess, or in some cases to attempt to visit websites containing child pornography. This can only be carried out by law enforcement or under the direct authorization of law enforcement. No actual visits have been made to any such website by researchers associated with this report or HostExploit. In determining whether a website within this category is via law enforcement or governmentally authorized child protection agencies. Any reader or researchers, who believe they have knowledge of such a website or online service, should contact your local agency. For community purpose, HostExploit has an informational area for [“Reporting Cyber Crime”](#) and in this case for reporting [‘Illegal Content’](#).

Background: Since its establishment in March 1998, the [CyberTipline](#) of the US based National Center for Missing & Exploited Children (NCMEC) has received more than 628,680 reports involving the possession, manufacture, and distribution of child pornography, the online enticement of children for sex acts, child prostitution, child sex-tourism, child molestation (not in the family), unsolicited obscene material sent to a child, and misleading domain names.

## 8. CONCLUSIONS

---

- HE** It is clear McColo has a key role in managing world's major botnets, and malware warehousing, which has been estimated as partially controlling 50 – 75% of the world's spam.
- HE** McColo and some other bad actors show a relatively low level on specific infected sites / domains (see page 19). The reason being McColo operators and cyber criminals increasingly use IP addresses without domains or conventional websites to deliver malware or botnet command & control to get around Internet user's safe surfing mechanism's e.g. Google's blacklisting, ESET's Nod32, and McAfee's Site Advisor.
- HE** One argument made in the security community is such actions are "whack a mole", possibly true that this war against cyber criminals is not over, but one battle at a time? We will never be 100% safe on the web and cyber criminal techniques will improve, but an incremental step in safety has to be worthwhile.
- HE** A further argument is "rather than call for the removal of XYZ from the Internet it is good to know where the bulk of the bad activity is coming from". The earlier ethical point of "avoiding harm to others" and "whistle blowing" is a double edged sword; if we as security professionals are aware of the badness do we have the option to play God?
- HE** By leaving cyber criminals undisturbed to observe them also ensures many ordinary Internet users are still vulnerable to loss. Even one victim is our responsibility if we know the problem. Further the cyber criminals get richer and can use that funding for further badness or even purchase or influence Internet infrastructure by corruption.
- HE** With the sensitivity and application of issues shown within the "Research Note" on page 23, exposure and eradication of child pornography should become a major priority for the security community.
- HE** Concern still exists as to ICANN's role and action / inaction.
- HE** This and the earlier Atrivo report clearly demonstrate that, when presented with the appropriate evidence of criminal activity, the Internet community can bring about the positive forces necessary to purge it.

**Watch out for the next HostExploit report "Version 3.0 – The Europeans"**

[Email here for an advance copy of the next report when available.](#)

# APPENDIX 1 – REFERENCES

---

## Section 1 Introduction:

- [Atrivo – Cyber Crime USA](#)
- [UnitedLayer COO: Giving access to Intercage is an issue of ethics](#)
- [Directi and HostExploit abuse report](#)

## Section 2 The Toxic Networks:

- [http://forum.sysinternals.com/forum\\_posts.asp?TID=14844](http://forum.sysinternals.com/forum_posts.asp?TID=14844)
- <http://www.viruslist.com/en/analysis?pubid=204792011>
- <http://www.secureworks.com/research/threats/warezov/>
- <http://www.siteadvisor.com/sites/fraudcrew.com>
- [http://www.rsa.com/blog/blog\\_entry.aspx?id=1378](http://www.rsa.com/blog/blog_entry.aspx?id=1378)
- <http://www.spamhaus.org/sbl/sbl.lasso?query=SBL58520>

## Section 3 McColo - a Case Study– The Mechanics:

- <http://www.threatexpert.com/report.aspx?uid=f29a5099-364e-46f0-9569-1cc6fc15fcbd>

## Section 4 McColo – The Business of Cyber Crime:

## Section 5 The Data:

## Section 6 ICANN, Registrars & Your Spam:

## Section 7 Child Pornography

- [Reporting Illegal Content](#)

## APPENDIX 2 – GLOSSARY OF TERMS

---

- HE AS (Autonomous System):** An AS is a unit of router policy, either a single network or a group of networks that is controlled by a common network administrator (or group of administrators) on behalf of an entity (such as a university, a business enterprise, or Internet service provider), issued by Internet Assigned Numbers Authority (IANA). An AS is also sometimes referred to as a routing domain. Each autonomous system is assigned a globally unique number called an Autonomous System Number (ASN).
- HE Badware:** Software that fundamentally disregards a user's choice regarding about how his or her computer will be used. Types of badware are spyware, malware, or deceptive adware. Common examples of badware include free screensavers that surreptitiously generate advertisements, malicious web browser toolbars that take your browser to different pages than the ones you expect, and keylogger programs that can transmit your personal data to malicious parties.
- HE Blacklists:** In computing, a blacklist is a basic access control mechanism that allows access much like your ordinary nightclub; everyone is allowed in except people on the blacklist. The opposite of this is a whitelist, equivalent of your VIP nightclub, which means *allow nobody, except members of the white list*. As a sort of middle ground, a greylist contains entries that are temporarily blocked or temporarily allowed. Greylist items may be reviewed or further tested for inclusion in a blacklist or whitelist. Some communities and webmasters publish their blacklists for the use of the general public, such as Spamhaus and Emerging Threats.
- HE Botnet:** Botnet is a term for a collection of software robots, or bots, that run autonomously and automatically. The term is now mostly associated with malicious software used by cyber criminals, but it can also refer to the network of infected computers using distributed computing software.
- HE DNS (Domain Name System):** DNS associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. *www.example.com*, into IP addresses, e.g. *208.77.188.166*, which networking equipment needs to deliver information. A DNS also stores other information such as the list of mail servers that accept email for a given domain. By providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of contemporary Internet use.
- HE Exploits:** Turning the verb for taking advantage of a weakness into a noun, but with the same meaning. An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause irregular behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as violently gaining control of a computer system or allowing privilege escalation or a denial of service attack.
- HE Hosting:** Usually refers to a computer (or a network of servers) that stores the files of a web site which has web server software running on it, connected to the Internet. Your site is then said to be hosted.
- HE IP (Internet Protocol):** IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering data packets from the source host to the destination host solely based on its address.
- HE Malicious Links:** These are links which are planted on a site to deliberately send a visitor to a malicious site, e.g. a site with which will plant viruses, spyware or any other type of malware on a computer such as a fake security system. These are not always obvious as they can be planted within a feature of the site or masked to misdirect the visitor.

- HE MX:** A mail server or computer/server rack which holds and can forward e-mail for a client.
- HE NS (Name Server):** Every domain name must have a primary name server (e.g. ns1.xyz.com), and *at least one* secondary name server (ns2.xyz.com etc). This requirement aims to make the domain still reachable even if one name server becomes inaccessible.
- HE Open Source Security:** Open source is a set of principles and practices that promote access to the production and design process for various goods, products, resources and technical conclusions or advice. The term is most commonly applied to the source code of software that is made available to the general public with relaxed or non-existent intellectual property restrictions. For Open Source Security this allows users to create user-generated software content and advice through incremental individual effort or through collaboration.
- HE Pharming:** Pharming is an attack which hackers aim to redirect a website's traffic to another website, like cattle rustlers herding the bovines in the wrong direction. The destination website is usually bogus.
- HE Phishing:** Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information. Phishing is typically carried out using e-mail (where the communication appears to come from a trusted website) or an instant message, although phone contact has been used as well.
- HE Registrars:** A domain name registrar is a company with the authority to register domain names, authorized by ICANN.
- HE Rogue Software:** Rogue security software is software that uses malware (malicious software) or malicious tools to advertise or install its self or to force computer users to pay for removal of nonexistent spyware. Rogue software will often install a trojan horse to download a trial version, or it will execute other unwanted actions.
- HE Rootkit:** A set of software tools used by a third party after gaining access to a computer system in order to conceal the altering of files, or processes being executed by the third party without the user's knowledge.
- HE Sandnet:** A sandnet is closed environment on a physical machine in which malware can be monitored and studied. It emulates the internet in a way which the malware cannot tell it is being monitored. Wonderful for analyzing the way a bit of malware works. A Honeynet is the same sort of concept but more aimed at attackers themselves, monitoring the methods and motives of the attackers.
- HE Spam:** Spam is the term widely used for unsolicited e-mail. . Spam is junk mail on a mass scale and is usually sent indiscriminately to hundreds or even hundreds of thousands of inboxes simultaneously.
- HE Trojans:** Also known as a Trojan horse, this is software that appears to perform or actually performs a desired task for a user while performing a harmful task without the user's knowledge or consent.
- HE Worms:** A malicious software program that can reproduce itself and spread from one computer to another over a network. The difference between a worm and a computer virus is that a computer virus attaches itself to a computer program to spread and requires an action by a user while a worm is self-contained and can send copies of itself across a network.