

# Whose Internet Is It, Anyway?



Blackhat DC 2010  
Andrew Fried, ISC, SURBL  
Richard Cox, Spamhaus  
Ben Butler, GoDaddy



# How we use the Internet



- Web Surfing
- Email
- Social Networking  
(Facebook, MySpace, Twitter)
- Word Processing,  
Spreadsheets, Powerpoint
- VoIP



# What the bad guys attack



- Web Surfing
- Email
- Social Networking (Facebook, MySpace, Twitter)
- Word Processing, Spreadsheets, Powerpoint
- VoIP



# Who “owns” the Internet

- Internet consists of tens of thousands of independently owned and operated networks
- Various networks are connected via telecoms, ISPs, and backbone providers
- Private peering arrangement between providers
- Public peering points that connect the ISPs and Providers

**No one entity owns the Internet!**

**No one entity is in charge of the Internet.**



# Your email, Your inbox

**Subject:** possible fraudulent transaction and/or collusion with your VISA card

Dear VISA card holder,

A recent review of your transaction history determined that your card was used at an ATM located in Guam, but for security reasons the requested transaction was refused. You need to complete the VISA Card Holder Form. You can do this by clicking the link below:

<http://sessionidE0WIGZT1Z.cforms.visa.com/secureapps/vdir/cholderform.php?ref=87246604936107283808320562509325871294865306269561489911261467696265&email=>

VISA Cards Support

ID: YZDYDOND00EJ9Y5JSG9S2Z66XT3W5EM1IDU4



# Your email, Your inbox

**From:** Wachovia <usp@ppla.com>  
**Date:** Wed, 27 Jan 2010 10:39:41 -0500  
**To:** <undisclosed-recipients:;>  
**Subject:** New Alert Message



**WACHOVIA**

## UNAUTHORIZED ACCESS TO YOUR WACHOVIA ONLINE BANK ACCOUNT

Dear Wachovia Customer,

We recently have determined that different computers have logged in your **Wachovia Online Banking account**, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us. If this is not completed by **January 28, 2010**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner. In order to confirm your Online Bank records, we may require some specific information from you.

- To restore your account, please follow the link below:

<https://onlineservices.wachovia.com/auth/AuthService>

Thank you for using Wachovia Online Service.

The Wachovia Bank Team.



# Your email, Your inbox

**From:** Western union® [mailto:infor@westernunion.com]  
**Sent:** Wednesday, January 27, 2010 3:23 PM  
**Subject:** Important aknowledgement from Western union® money transfer

**Dear Sir/Madam**

There is an issue with the Western Union Money Transfer in the amount of \$500,000.00 (Five Hundred Thousand United State Dollar) directed in "Automated Teller Machine" (ATM)Card at the owner of this email address. The International Monetary Fund contacted us for your compemsation a couple of hours ago due to your allocated security code.They choose to send it to an email address instead of a name. We are unable to complete your ATM delivery to an email address, so we require some more information in order to complete this Delivery .

- **Full Name:**
- **Full Contact Address:**
- **Mobile Phone Number:**
- **Occupation:**
- **Sex:**
- **Marital Status:**
- **Age:**

In order to effect this delivery, please email via Western Union Automated Teller Machine (ATM) Department:- westernunion\_atmcard2009@upmail.us  
As soon as this information is received,your ATM card Will be delivered to your doorstep through a Diplomatic Courier Company and the tracking number will be sent to you to enable you track it down before its arrival in your country.  
NOTE:You are required to reconfirm your Full name,House address where the Automated Teller Machine will be sent.

Your valid telephone number is also needed for easy communication.

The Management Of Western Union Money Transfer, Dispatched This Day Sincerely,

Mr. Mark Greg. www.western union.com

Western Union®

Welcome to Western Union - Send Money Worldwide

**Registered © 2008 - 2009 Western Union Money Transfer All Right Reserved**



# Your email, Your inbox

Subject: [BMW Automobile Award Programmed](#)  
To:  
Date: Saturday, January 23, 2010, 7:36 PM

BMW Automobile Award  
Programmed  
Your Email Address Has Won You A Car and a cash prize of  
750,000GBP  
In the BMW Automobile Promotion Held in United Kingdom.  
To claim your prize Contact David Brown.  
Email: [bmwawareness@bmwdealernet.com](mailto:bmwawareness@bmwdealernet.com)  
Telephone Number:+ +447024038675  
1 Name,  
2 Address:  
3 Mobile No:  
4 Age:  
5 Sex:  
6 Occupation:  
7 Country:  
All mail should go to [bmwawareness@bmwdealernet.com](mailto:bmwawareness@bmwdealernet.com)  
Regards,  
Bmw Promo Team.  
Phone No: +447024038675





# Your email, Your inbox

**Subject:** IRS REFUND Notification - Please Read This!

 **Internal Revenue Service**  
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive 546.47\$ tax refund under section 501(c) (19) of the Internal Revenue Code. Please submit the [Tax Refund Request Form](#) and allow us 3-9 days to process it.

Yours faithfully,  
Sarah Hall Ingram, Commissioner

**This notification has been sent by the Internal Revenue Service, a bureau of the Department of the Treasury.**



# Your email, Your inbox

**Subject:** Tax Refund



After the last annual calculations of your fiscal activity we have determined that you are eligible to receive 439.42\$ tax refund under section 501(c) (25) of the Internal Revenue Code. Please submit the [Tax Refund Request Form](#) and allow us 3-9 days to process it.

Yours faithfully,  
Sarah Hall Ingram, Commissioner

This notification has been sent by the Internal Revenue Service, a bureau of the Department of the Treasury.



# Your email, Your inbox

from ebay Member: user173 <test@test.com> ☆  
subject You've received a question about eBay item #:220507397590  
to undisclosed-recipients; ☆

reply forward archive junk dele  
1/20/10 6:00  
other actions



eBay sent this message from **user173** (Elodia William).  
Your registered name is included to show this message originated from eBay. [Learn more.](#)

## Question about item -Respond Now



Do not respond to the sender if this message requests that you complete the transaction outside of eBay. This type of offer is against eBay policy, may be fraudulent, and is not covered by buyer protection programs. [Learn more.](#)

Dear member,

I'd would like to know how much to start shipping charges for Miami (FL) and if pickup is available for this auction.

Thanks in advance and wait for your answer, when you are available.

Regard's.

- user173

**Respond Now**

*Responses will not include your email address.*

### Item and user details

Item number: 220507397590  
Item URL: [cgi.ebay.com/ws/eBaySAPI.dll?ViewItem&item=220507397590&sspageName=ADME:B:AAQ:1](http://cgi.ebay.com/ws/eBaySAPI.dll?ViewItem&item=220507397590&sspageName=ADME:B:AAQ:1)  
End date: Thursday, Jan 22, 2010 13:02:12 PDT  
From User: **user173** ( 6245 ★ ) **Power Seller**  
**99.7% Positive Feedback**  
Member since Nov-22-02 in United States  
Activity with user173 (last 90 days): I have bid on 0 items from **user173**.

This message was sent when the listing was active. **user173** is a potential buyer.

### Marketplace Safety Tip

Second Chance Offer emails with the subject of "message from eBay Member" are fake. Real [Second Chance Offers](#) come directly from eBay and also appear in [My Messages](#) with a subject stating "eBay Second Chance Offer for Item...".

Never pay for your eBay item using instant case wire transfer services through [Western Union](#) or [MoneyGram](#). These payment methods are unsafe when paying someone you don't know. [Learn more](#) about sending payments.

Is this email inappropriate? Does it violate [eBay policy](#)? Help protect the Community by [reporting it](#).

Learn how you can protect yourself from spoof (fake) emails at:  
<http://pages.ebay.com/education/spoof/tutorial>

This eBay notice was sent on behalf of another eBay member through the eBay platform and in accordance with our Privacy Policy. If you would like to receive this email in text format, change your [notification preferences](#).

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.

Privacy Policy: <http://pages.ebay.com/help/policies/privacy-policy.html>

User Agreement: <http://pages.ebay.com/help/policies/user-agreement.html>

Copyright © 2008-2007 eBay, Inc. All Rights Reserved.  
Designated trademarks and brands are the property of their respective owners.  
eBay and the eBay logo are registered trademarks or trademarks of eBay, Inc.  
eBay is located at 2145 Hamilton Avenue, San Jose, CA 95125.



# Your email, Your inbox

e→cards  
from Hallmark

## A Friend has sent you a Hallmark E-Card.

If you recognize this name, click the link to see your E-Card.

[http://www.hallmark.com/ECardWeb/ECV.jsp?a=EG0694272732475M245925860Y&product\\_id=](http://www.hallmark.com/ECardWeb/ECV.jsp?a=EG0694272732475M245925860Y&product_id=)

If this name is not familiar to you and you're concerned about online security, please use the following steps:

1. Visit <http://www.hallmark.com/getecard>
2. Enter your e-mail address in the Original Recipient's E-Mail Address box.
3. Enter EG0694262772475 in the Confirmation Number box.
4. Click Display Greeting.

Want to send an E-Card too ? Visit [www.hallmark.com/ecards](http://www.hallmark.com/ecards)

To view Hallmark's privacy policy or for questions, visit [www.hallmark.com](http://www.hallmark.com), and click the links at the bottom of the page.



# Your email, Your inbox

from PayPal Australia <info@paypal.com.au> ☆  
subject **Your account access has been limited**  
reply-to noreply@paypal.com.au ☆  
to undisclosed-recipients;; ☆

Australia's favourite way to pay online



What is PayPal?  
How does PayPal work?  
How can I contact PayPal?

## Resolution Center: Your account access has been limited.

Dear Customer,

During the regular update and verification process of PayPal Account, we could not verify your current information. Some of the possible reasons for this are:

- Changes in your current contact information;
- Incomplete contact information;

Hence, your access to use this service has been limited.

To restore your Online account please click on the link below, log into your Online Account and follow the instructions on your screen.

<http://www.paypal.com.au/au/>

**Note:** Only submit your information via this secure link.

Do not submit your information via email since this is not a secure way of sending sensitive data.

Thank You. \* Please do not reply to this email, as your reply will not be received. This is an automatic notification of new security messages.  
Code #83945



# Your email, Your inbox

**Subject:** possible fraudulent transaction and/or collusion with your VISA card

Dear VISA card holder,

A recent review of your transaction history determined that your card was used at an ATM located in Guam, but for security reasons the requested transaction was refused. You need to complete the VISA Card Holder Form. You can do this by clicking the link below:

<http://sessionidE0WIGZT1Z.cforms.visa.com/secureapps/vdir/cholderform.php?ref=87246604936107283808320562509325871294865306269561489911261467696265&email=>

VISA Cards Support

ID: YZDYDOND00EJ9Y5JSG9S2Z66XT3W5EM1IDU4



# Your email, Your inbox

**Subject:** official "Underreported Income Notice" to taxpayer

Taxpayer ID: ██████████ -00000456101707US

Tax Type: INCOME TAX

Issue: Unreported/Underreported Income (Fraud Application)

Please review your tax statement on Internal Revenue Service (IRS) website (click on the link below):

[review tax statement for taxpayer id: ██████████ -00000456101707US](#)

Internal Revenue Service



# Your email, Your inbox

from k.Rind <kerryrind1@hotmail.com> ☆

reply forward archive junk delete

subject YOUR PERUSAL

1/23/10 6:21 PM

to undisclosed-recipients:; ☆

other actions ▼

Dear Sir/Madam,

My name is Kerry Rind. I work with a reputable Bank here in the Netherlands. I have Business Proposal of twenty Million Euros (20 Million Euros) for you to handle with me from my bank. I will need you to help me in transferring the above funds from the Netherlands to your country. I need to know if you will be able to handle this with me before I explain to you in details.

Should you be interested please send me your;

- 1, Full names,
- 2, Occupation,
- 3, Private phone number,
- 4, Current residential address

Finally after that I shall furnish you with more information about this project. However I shall be waiting your response and assurance.

Your earliest response to this letter will be appreciated. Do contact me on my email address: [kerryrind@hotmail.com](mailto:kerryrind@hotmail.com).

Kind Regards

Mr. Kerry rind





# Your email, Your inbox

Shopping cart: \$0.00 [Checkout](#) Search:  [GO](#)

[HOME PAGE](#) [FAQ'S](#) [CONTACT US](#) [TESTIMONIALS](#) [ABOUT US](#)



*Exquisite*  
REPLICAS  
YOUR PASS TO THE RICH WORLD



**BUY 3 WATCHES**  
get 50% off one watch

ROLEX OMEGA BREITLING Cartier

*Watches*

- » Rolex Sports Models
- » Rolex Datejusts
- » A Lange & Sohne
- » Aigner
- » Alain Silberstein
- » Audemars Piguet
- » Bell & Ross
- » Breguet
- » Breitling
- » Bvlgari
- » Cartier
- » Chanel

*2009 Brand new models*


SUBMARINER FULL 18K GOLD	SUBMARINER 18K & SS	SUBMARINER SS	ASTRONOMICAL CELESTIAL DOUBLE DIAL
			
Special: \$229.00 Full 18K Gold Blue Dial Blue Bezel... - Men Watch Code: RX333 <a href="#">view similar items</a>	Special: \$229.00 18Kt SS Blue Dial Blue Bezel... - Men Watch Code: RX405 <a href="#">view similar items</a>	Special: \$229.00 All Stainless Black bezel dial... - Men Watch Code: RX406 <a href="#">view similar items</a>	Special: \$229.00 Patek Philippe Astronomical Celestial D... - Men Watch Code: XPA002 <a href="#">view similar items</a>



# Your email, Your inbox

**ULTIMATE  
REPLICA**  
LUXURY AT AN AFFORDABLE PRICE!

[Home](#) | [FAQ's](#) | [Contact Us](#) | [Testimonials](#) | [About Us](#)

 Shopping Cart: \$0.00 **Checkout**

WATCHES

HANDBAGS & WALLET

JEWELRY & ACCESSORIES

  
ROLEX



View Similar

  
BREITLING  
1884



View Similar

LOUIS VUITTON



View Similar

TIFFANY & Co.



View Similar

Get free shipping today



Get 15% Discount On ALL Watches Today!

**New Models**

2010 Hot New Rolex Styles now Instock  
Details >

*Free Shipping*

Save big this holiday season.  
We are offering FREE shipping on all products



**2010 Brand New Models**



# Your email, Your inbox

**Dr. MaXman**  
Max Penis Enlarger Pills



[Home](#) | [Faq](#) | [Testimonials](#) | [Order](#) | [Contact Us](#) | [Privacy Policy](#)

**"Gain 3+ Inches Today"**  
REAL Doctors, REAL Science, REAL Results!

"MaxMan has worked for THOUSANDS of clients"  
- Dr J.C Bowd





# Your email, Your inbox

<<(MAXGENTLEMAN)>>



## Impress Your Partner

With a huge Package

"The ONLY male enlargement pill PROVEN to work in clinical trials – gains of 2-3 inches on average."

- Dr. Richard N. Hoffman

ORDER NOW!



[Home](#) | [Testimonials](#) | [Faqs](#) | [Privacy Policy](#) | [Order Now](#) | [Contact Us](#)





# Your email, Your inbox

Order The Cheapest Medications Now!

http://wholesaledrugs.com/ link:go2mmo.com

Home | Bestsellers | All products | FAQ | Contact us

USD EUR GBP AUD CHF Pharmas Bonus

Your cart: \$0.00 (0 items) Proceed to Checkout

## Canadian Pharmacy

#1 Internet Online Drugstore

- Special Offer
- Free Viagra samples
- 4 pills for every order
- 12 pills for order >\$300

### Product list

For Order more than \$300: 12 VIAGRA PILLS FREE  
For other Orders: 4 VIAGRA PILLS

Product	Price	Details
Viagra + Cialis	\$69.99	10 x Viagra 100 mg, 10 x Cialis 20 mg
Cialis	\$198.40	60 pills 20 mg + 4 Free pills
Viagra	\$229.84	120 pills 100 mg + 4 free pills + free delivery

Search by name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Search:

### Today's bestsellers

Viagra	Our price \$1.15	Accutane	\$0.79
Viagra Professional	Our price \$1.57	Clomid	\$0.58
Viagra Super Active+		Prednisone	\$0.37
Cialis	Our price \$1.99	Doxycycline	\$0.21
Cialis Professional	Our price \$4.17	Zithromax	\$0.51
Cialis Super Active+		Amoxil	\$0.40
Levitra	Our price	Alli	\$1.33
		Strattera	\$0.74
		Lasix	\$0.24
		Prozac	\$0.40
		Nexium	\$0.40
		Cipro	\$0.32
		Lipitor	\$0.35

Scripts Currently Forbidden | <SCRIPT>: 2 | <OBJECT>: 0

Done



## Researcher's "View"

Possible botnets detected: sucipa.vc

Host: sessionidVTKFJX5L8ZY.cforms.visa.com.sucipa.vc

183.87.51.225

189.18.108.77

189.192.53.189

189.194.129.62

189.231.5.193

190.213.161.169

201.43.140.52

201.139.142.208

93.177.185.72

94.55.1.250

94.240.225.56

95.104.39.180

118.33.211.102

123.231.59.214

124.25.235.164



# Researcher's "View"

[uiurluso.cn](http://uiurluso.cn)

[uivcxwno.cn](http://uivcxwno.cn)

[uivjvsko.cn](http://uivjvsko.cn)

[uivkrsuo.cn](http://uivkrsuo.cn)

[uivtyywo.cn](http://uivtyywo.cn)

[uiwpyvbo.cn](http://uiwpyvbo.cn)

[uiwweoco.cn](http://uiwweoco.cn)

[uiwyhjlo.cn](http://uiwyhjlo.cn)

[uixaevjo.cn](http://uixaevjo.cn)

[uixdjgfh.cn](http://uixdjgfh.cn)

[uixjnrqo.cn](http://uixjnrqo.cn)

[uixxmiho.cn](http://uixxmiho.cn)

[uiymdmmo.cn](http://uiymdmmo.cn)

[uiyzfkoo.cn](http://uiyzfkoo.cn)

[uizghezo.cn](http://uizghezo.cn)

[uizmfmwwo.cn](http://uizmfmwwo.cn)

[ujanxgio.cn](http://ujanxgio.cn)



## Researchers “View”

URL gets captured in the spamtrap:

[http://alerts.cforms.visa.com.iursedq.com.vc/secureapps/vdir/  
cholderform.php?  
ref=3D224366338567325670281313395621728265132179  
86215473428007364284341942084744511&email=XXXX](http://alerts.cforms.visa.com.iursedq.com.vc/secureapps/vdir/cholderform.php?ref=3D22436633856732567028131339562172826513217986215473428007364284341942084744511&email=XXXX)





# Researcher's View

The chase is on to put the pieces of the puzzle together





# Fake Whois

Created On:27-Jan-2010 20:29:24 UTC

Last Updated On:27-Jan-2010 20:29:24 UTC

Expiration Date:27-Jan-2011 20:29:24 UTC

Sponsoring Registrar:IP Mirror Pte. Ltd. (R116-LRCC)

Registrant Name:Ayenne Applebaum

Registrant Organization:

Registrant Street1:6505 Marissa Circle

Registrant Street2:

Registrant Street3:

Registrant City:Lake Worth

Registrant State/Province:Lake Worth

Registrant Postal Code:58441

Registrant Country:US

Registrant Phone:+1.5613123655



# It's a Fast Flux Domain!

;; ANSWER SECTION:

iursedq.com.vc.	1800	IN	A	115.177.129.136
iursedq.com.vc.	1800	IN	A	116.50.154.197
iursedq.com.vc.	1800	IN	A	118.33.211.102
iursedq.com.vc.	1800	IN	A	189.110.149.105
iursedq.com.vc.	1800	IN	A	189.193.229.197
iursedq.com.vc.	1800	IN	A	189.194.133.9
iursedq.com.vc.	1800	IN	A	189.194.204.79
iursedq.com.vc.	1800	IN	A	190.213.161.169
iursedq.com.vc.	1800	IN	A	200.95.250.127
iursedq.com.vc.	1800	IN	A	201.43.140.52
iursedq.com.vc.	1800	IN	A	201.139.142.208
iursedq.com.vc.	1800	IN	A	211.255.29.30
iursedq.com.vc.	1800	IN	A	69.79.96.70
iursedq.com.vc.	1800	IN	A	114.24.3.17
iursedq.com.vc.	1800	IN	A	114.186.241.236



# View via Passive DNS

Found 115 records

IP Address	ASN	BGP Netblock	First Seen	Host/Domain
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:24:08	<a href="#">0ds45e6wpj.cforms.visa.com.sucipy.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:14:27	<a href="#">28uvidr59n.cforms.visa.com.sucipa.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:36:11	<a href="#">alerts.cforms.visa.com.freeimagesonly.be</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:26:27	<a href="#">alerts.cforms.visa.com.gyueeerf.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:10:36	<a href="#">alerts.cforms.visa.com.iurseda.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:21:56	<a href="#">alerts.cforms.visa.com.iurseda.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:27:06	<a href="#">alerts.cforms.visa.com.iursedq.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:27:40	<a href="#">alerts.cforms.visa.com.iursedz.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:48:48	<a href="#">alerts.cforms.visa.com.sucipa.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:07:17	<a href="#">alerts.cforms.visa.com.sucipa.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:46:41	<a href="#">alerts.cforms.visa.com.sucipy.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:17:23	<a href="#">freeimagesonly.be</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:22:22	<a href="#">g1huwpc6eux0c5g.cforms.visa.com.iurseda.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:37:41	<a href="#">medirams.com</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:32:42	<a href="#">reports.cforms.visa.com.freeimagesonly.mobi</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:17:21	<a href="#">reports.cforms.visa.com.gyueeerh.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:12:55	<a href="#">reports.cforms.visa.com.iursedz.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:22:40	<a href="#">reports.cforms.visa.com.medirams.com</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:47:38	<a href="#">reports.cforms.visa.com.sucipa.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:22:47	<a href="#">reports.cforms.visa.com.sucipe.com.vc</a>



# View via Passive DNS

<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:29:01	<a href="#">transactions.cforms.visa.com.iursedz.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:20:24	<a href="#">transactions.cforms.visa.com.norytioq.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:33:16	<a href="#">transactions.cforms.visa.com.norytiox.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:45:07	<a href="#">transactions.cforms.visa.com.sucipa.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:35:21	<a href="#">transactions.cforms.visa.com.sucipy.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:34:03	<a href="#">www.irs.gov.freeimagesonly.co.uk</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:34:06	<a href="#">www.irs.gov.freeimagesonly.com</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:47:09	<a href="#">www.irs.gov.gyueeerd.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 15:17:16	<a href="#">www.irs.gov.gyueeerdc.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:24:22	<a href="#">www.irs.gov.gyueeerf.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:11:54	<a href="#">www.irs.gov.gyueeers.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:30:52	<a href="#">www.irs.gov.gyueeeru.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:21:12	<a href="#">www.irs.gov.iursedc.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:40:46	<a href="#">www.irs.gov.iursedz.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 14:27:29	<a href="#">www.irs.gov.iursedz.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:33	<a href="#">www.irs.gov.norytiod.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:33	<a href="#">www.irs.gov.norytiod.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:17	<a href="#">www.irs.gov.norytioq.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:17	<a href="#">www.irs.gov.norytior.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:28	<a href="#">www.irs.gov.norytior.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:08	<a href="#">www.irs.gov.norytiox.com.vc</a>
<a href="#">115.177.129.136</a>	2510	115.176.0.0/15	2010-01-27 16:34:28	<a href="#">www.irs.gov.norytiox.vc</a>



# Nameserver

; AUTHORITY SECTION:

iursedq.com.vc.	1800	IN	NS	<b>ns1.whiskybrend.net.</b>
iursedq.com.vc.	1800	IN	NS	ns1.nodefront.net.
iursedq.com.vc.	1800	IN	NS	ns2.nodefront.net.
iursedq.com.vc.	1800	IN	NS	ns2.whiskybrend.net.



# Ah, more “leads” to chase!

## Found 12 records

IP Address	ASN	BGP Netblock	First Seen	Host/Domain
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-21 09:15:31	<a href="#">ns1.24stophours.com</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-22 06:28:59	<a href="#">ns1.availname.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-18 07:06:20	<a href="#">ns1.disksilver.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-15 09:09:42	<a href="#">ns1.dogsgrem.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-26 05:21:03	<a href="#">ns1.girlfriendsboy.com</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-26 11:47:31	<a href="#">ns1.nodefront.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-19 06:12:41	<a href="#">ns1.pdsproperties.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-15 09:09:42	<a href="#">ns1.platpro-db.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-20 06:07:38	<a href="#">ns1.sorbauto.com</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-20 06:07:38	<a href="#">ns1.theautocompany.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-26 11:54:12	<a href="#">ns1.whiskybrend.net</a>
<a href="#">204.12.229.89</a>	32097	204.12.192.0/18	2010-01-20 09:36:29	<a href="#">ns1.worldkinofest.com</a>



# Threat Mitigation - Zeus



- Estimates of 600,000 victims
- Anti Virus totally ineffective (less than 20% detection rates)
- What can be done, and who should do it?





# Whack a mole approach

## Security Researchers

- Identify Fraudulent Domains
- Identify Associated Nameservers
- Enumerate Address Space

## Internet Service Providers

- Shut down web hosting accounts
- Null route servers
- Remove DNS records
- Lock email accounts
- Preserve evidence for

## Domain Registrars

- Deregister Domains
- Lock accounts
- Remove DNS Glue Records

# Blackhat DC 2010

## Whose Internet Is It, Anyway?

