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.
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:


VISA Cards Support

ID: YZDYDOND00EJ9Y5JSG9S2Z66XT3W5EM1IDU4
From: Wachovia <usp@ppla.com>
Date: Wed, 27 Jan 2010 10:39:41 -0500
To: <undisclosed-recipients;>;>
Subject: New Alert Message

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.
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 compensation 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

Welcome to Western Union - Send Money Worldwide
Registered © 2008 - 2009 Western Union Money Transfer All Right Reserved
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
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
Regards,
Bmw Promo Team.
Phone No: +447024038675
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.
Subject: Tax Refund

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 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 <user173@eBay.com>
Subject: You've received a question about item: 20107387590

Dear member,

I 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.

Regards,

- user173

Item and user details

<table>
<thead>
<tr>
<th>Item number</th>
<th>20107387590</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item URL</td>
<td>ebay.com/macbookair/12&quot;?item=20107387590&amp;variosname=ADME%2DAAA%2D1</td>
</tr>
<tr>
<td>End date</td>
<td>Thursday, Jan 20, 2010 13:02:32 PST</td>
</tr>
<tr>
<td>From User</td>
<td>user173 (6344) 99.7% Positive Feedback</td>
</tr>
<tr>
<td>From Member</td>
<td>Member since Nov-22-02 in United States</td>
</tr>
</tbody>
</table>

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 cash 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:

This eBay email 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.
User Agreement: https://pages.ebay.com/help/policies/agreement.html

Copyright © 1995-2011 eBay Inc. All Rights Reserved.
Designated trademarks are the property of their respective owners.
eBay and the eBay logo are registered trademarks of eBay Inc.
eBay is located at 334 Hamilton Avenue, San Jose, CA 95110.
A Friend has sent you a Hallmark E-Card.

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

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

2. Enter your e-mail address in the Original Recipient's E-Mail Address box.
3. Enter EG0894262772475 in the Confirmation Number box.
4. Click Display Greeting.

Want to send an E-Card too? Visit www.hallmark.com/ecards

To view Hallmark's privacy policy or for questions, visit 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: no-reply@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.


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 #835645
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: YZDYDONDO0EJ9Y5JSG9S2Z66XT3W5EM1IDU4
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
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.
Kind Regards
Mr. Kerry rind
Your email, Your inbox
Your email, Your inbox

“Gain 3+ Inches Today”
REAL Doctors, REAL Science, REAL Results!

"MaxMan has worked for THOUSANDS of clients"
- Dr J.C Bowd
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
Possible botnets detected: sucipa.vc
Host: sessionidVTKFJX5L8ZY.cforms.visa.com.sucipa.vc

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IP Address</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>183.87.51.225</td>
<td>189.18.108.77</td>
<td>189.192.53.189</td>
</tr>
<tr>
<td>189.194.129.62</td>
<td>189.231.5.193</td>
<td>190.213.161.169</td>
</tr>
<tr>
<td>201.43.140.52</td>
<td>201.139.142.208</td>
<td>93.177.185.72</td>
</tr>
<tr>
<td>94.55.1.250</td>
<td>94.240.225.56</td>
<td>95.104.39.180</td>
</tr>
<tr>
<td>118.33.211.102</td>
<td>123.231.59.214</td>
<td>124.25.235.164</td>
</tr>
</tbody>
</table>
Researcher’s “View”

uiurluso.cn
uivcxwno.cn
uivjvvko.cn
uivkrsuo.cn
uivtyywo.cn
uiwpyvbo.cn
uiwweoco.cn
uiwyhjlo.cn
uixaevjo.cn
uixdjgfh.cn
uixjnrqo.cn
uixxmiho.cn
uiymdmmo.cn
uiyzfkoo.cn
uizghezo.cn
uizmfmwo.cn
ujanxgio.cn
Researchers “View”

URL gets captured in the spamtrap:

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**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>ASN</th>
<th>BGP Netblock</th>
<th>First Seen</th>
<th>Host/Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 15:24:08</td>
<td>0ds45c6wpj.cforms.visa.com.sucipy.vc</td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 14:36:11</td>
<td>alerts.cforms.visa.com.freeimagesonly.be</td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 16:07:17</td>
<td>alerts.cforms.visa.com.sucipa.vc</td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 15:17:23</td>
<td>freeimagesonly.be</td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 16:22:22</td>
<td>g1huwpc6ueux0c5g.cforms.visa.com.jurseda.com.vc</td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 14:37:41</td>
<td>medirams.com</td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>115.176.0.0/15</td>
<td>2010-01-27 14:32:42</td>
<td>reports.cforms.visa.com.freeimagesonly.mobi</td>
</tr>
<tr>
<td>IP Address</td>
<td>Count</td>
<td>Time</td>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>--------</td>
<td>---------------------------------</td>
<td></td>
</tr>
<tr>
<td>115.177.129.136</td>
<td>2510</td>
<td>2010-01-27 15:34:03</td>
<td><a href="http://www.irs.gov.freeimagesonly.co.uk">www.irs.gov.freeimagesonly.co.uk</a></td>
<td></td>
</tr>
</tbody>
</table>
; AUTHORITY SECTION:

<table>
<thead>
<tr>
<th>Domain</th>
<th>TTL</th>
<th>Type</th>
<th>Class</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>iursedq.com.vc</td>
<td>1800</td>
<td>IN</td>
<td>NS</td>
<td>ns1.whiskybrend.net.</td>
</tr>
<tr>
<td>iursedq.com.vc</td>
<td>1800</td>
<td>IN</td>
<td>NS</td>
<td>ns1.nodefront.net.</td>
</tr>
<tr>
<td>iursedq.com.vc</td>
<td>1800</td>
<td>IN</td>
<td>NS</td>
<td>ns2.nodefront.net.</td>
</tr>
<tr>
<td>iursedq.com.vc</td>
<td>1800</td>
<td>IN</td>
<td>NS</td>
<td>ns2.whiskybrend.net.</td>
</tr>
</tbody>
</table>
Ah, more “leads” to chase!

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