

Digging Into Unlawful Email Messages

Economic Fraud and Digital Evidence

September 22nd, 2005

Valley River Inn, Eugene OR

Joe St Sauver, Ph.D. (joe@uoregon.edu)

University of Oregon Computing Center

<http://www.uoregon.edu/~joe/digging-in/>

I. Introduction

Our Agenda Today

- Today we're going to talk a little about how you can dig into the illegal email (spam, fraud, phishing, etc.) which you may run into. Our goals are to help you think about:
 - what's involved in selecting email messages to pursue
 - identifying where a particular email really came from
 - tracking websites spamvertised in the body of email messages
 - overcoming obfuscatory techniques and methods

It Can Be Amazing To See How Far You Can Get From Public Sources

- The approaches discussed in this talk are not meant as a replacement for more traditional methods such as:
 - making a targeted buy and then following the money (and/or the fulfillment channels) back up stream, or
 - infiltrating criminal organizations with undercover officers, or
 - passively collecting information based on lawful intercept orders (although frankly, I'm not seeing lawful intercept getting much used in attacking cybercrime right now; see www.uscourts.gov/wiretap04/contents.html)
- This talk is meant to illustrate how far you can get just by tugging a little on some of the “loose threads” that have been unintentionally left by the bad guys (another analogy you'll hear is “following the trail of crumbs”)

II. Picking The Right Messages To Investigate

The Reality of Cybercrime Today

- Unfortunately, there is a true flood of illegal activity online today. Given a steady stream of reports relating to unlawful online activity, your first chore is determining which reports represent ones worth pursue (unless you have infinite investigative capacity, you will need to be selective!)
- Of course, standard considerations (such as subject matter jurisdiction and geographical jurisdiction) pertain just as they always do, but before proceeding with a particular investigation that includes cybercrime-related components, there are some additional factors you may want to consider.

Condition of The Submitted Email

- When it comes to crimes perpetrated by email, a prime consideration is the quality or condition of the email message you're starting with. If it is of poor quality, you're building your "house" on an unsound foundation.
- What makes a message "poor quality"?
 - message is incomplete, exists only in printed form, as a screen capture, etc.
 - message was sent more than 48 hours ago
 - message was forwarded via one or more mailing lists
 - message does not include full headers
 - message does not include the raw message body
 - message does not include one or more attachments
 - message has been "munged"/otherwise altered
- Sometimes you need to play what you've been given, but if you have a choice, pick wisely.

Why Is Message Timeliness Important?

- Cybercriminals are inherently agile, and part of their defensive strategy, like terrorists, involves never staying too long in one place. If you begin to work an incident based on mail that is days (or even weeks) old, the bad guys may already have moved (possibly more than once). You need to be as nimble as they are, and you also need to recognize that the bad guys are working nights and weekends. M-F 8-12 and 1-5 just won't cut it anymore.
- You also need to recognize that internet service providers, ISPs, are handling so many customers and so much traffic that if you want a particular bucket of water from the river, you need to let them know before it hits the ocean and is lost forever. Logs rotate. Records get deleted. Servers get reformatted and reused. If you need evidence, you need to get it while it still exists.

Look For “Triple Word Score” Opportunities

- Just like a traffic cop, you’ll see lots of relatively minor incidents as well as more serious ones. If you don’t correctly pick the right incidents to work, you’ll be tied up working a “five-over” when a drunken driver comes by (doing eighty) (in a school zone) (where there’s active construction work) (in a stolen car). Pick your shots....
- I’d suggest looking for incidents that:
 - are of material volume (e.g., involving the distribution of hundreds of thousands or millions of messages)
 - use compromised systems (aka “spam zombies”) for the distribution of their messages
 - include violations of substantive laws, such as sale or attempted sale of a controlled substance, inherently fraudulent schemes, child porn related incidents, etc...
 - involve .gov/.mil hosts

Some Other Suggested Priority Categories

- Incidents involving:
 - easily-documented large out-of-pocket losses
 - known Spamhaus.org ROKSO spammers or particularly Spamhaus.org “top 10” spammers
 - new exploits
 - custom spamware
 - so-called “bullet proof hosting”
 - so-called “bullet proof domain name registration”
 - anonymous online payment channels
 - spam “affiliate programs”
 - incidents involving known repeat offenders
 - incidents targeting children or the elderly
 - topically current/newsworthy incidents
 - “low hanging fruit,” etc.
- Pick incidents that will make a difference, and which prosecutors can run with and get good convictions

Ones to Skip (For Now)

- Incidents that don't have clean, complete and current sample emails
- Low volume incidents
- Poorly targeted/unlikely to be effective messages (e.g., spam with botched links, Korean language spam sent to largely-english-only audiences, etc.)
- Common spam that would be easily blocked using routine technical means
- Incidents already being worked by another agency
- Viruses/worms/spyware (that sort of malware is a different animal requiring specialized expertise)

Okay, so let's assume you've picked a spam or phishing mail message of interest -- now what?

III. Where Did The Message Come From?

Why Do You Need Full Headers?

- Virtually all the headers you routinely see displayed in a mail reading program like Outlook can be (and are) forged by spammers in an effort to evade detection. The key exception: the topmost/last-added “Received” header(s)...
- “Received” headers will usually be present but are only visible only when you enable full (expanded) headers.
- “Received” headers are intended to show the hop-by-hop path that a message takes as it goes from its origin to its destination.
- A “Received” header gets added by each host as it accepts the message from the preceding host.
- New “Received” headers get added above the existing “Received” headers.
- Spammers may add (“preload”) bogus Received: headers₁₃

Mechanics of Getting Full Headers

- The mechanics of getting full headers on a given mail message will vary from mail client to mail client; the way you do it on Thunderbird is not the same way you do it on Eudora which in turn is not the same way you do it on Outlook. Each client is different.
- We have information for the clients UO users commonly use at <http://micro.uoregon.edu/fullheaders/>
- For other email clients not listed, check Google; it will probably show one or more recipes for getting full headers from the client of interest (beware PC vs. Mac recipe differences, and version-related differences)
- Note that some users send in spam or phishing complaints and then dump those messages; in some cases, after submitting w/o full headers, they may not be able to go back and resubmit properly.

Sample Full Message Headers

Return-Path: <amit@punjabagro.com>

Received: from mail.punjabagro.com ([202.164.51.114])

by smtp.uoregon.edu (8.13.4/8.13.4) with ESMTP id j8MD2iXC018790

for <joe@oregon.uoregon.edu>; Thu, 22 Sep 2005 06:02:50 -0700

Received: by mail.punjabagro.com (Postfix, from userid 503)

id B843480899E; Thu, 22 Sep 2005 06:16:02 +0530 (IST)

To: joe@oregon.uoregon.edu

Subject: PayPal Security Measures

From: paypal@paypal.com

Content-Type: text/html

Message-Id: <20050922004602.B843480899E@mail.punjabagro.com>

Date: Thu, 22 Sep 2005 06:16:02 +0530 (IST)

<title>paypal</title>

<p><IMG
src="https://www.paypal.com/en_US/i/logo/paypal_logo.gif" border=0>

</p>

The Topmost Received Header

- The key bit of the topmost “Received” header is the IP address of the host that handed the message to the receiving system.
- IP addresses are often also called “dotted quads” because they consist of four numbers separated by dots. An example IP address is 128.223.142.13
- Host names, such as darkwing.uoregon.edu, get translated to numeric addresses (such as 128.223.142.13) by the Domain Name System (DNS).
- The DNS record that normally does that sort of host-name to dotted quad mapping is called an “A” record.
- The DNS record that normally does dotted quad to hostname mapping is called an “inverse address” record (or an “in-addr”). In-addr’s often won’t be present.

Hostname-IP Factoids

- Multiple hostnames can resolve to the same dotted quad. This is common in situations such as at web hosting farms where dozens or hundreds of hosts may all live on a single shared IP address.
- One hostname can resolve to multiple dotted quads. This is common when you're dealing with a particularly popular site that is "spread out over" multiple servers to handle the load.
- IP addresses normally resolve to only a single in-addr. That hostname may or may not actually exist. :-;
- Hostnames may not resolve to the same thing in the forward and reverse directions. (Trivial example: if you have fifty hostnames all pointing at a single IP address, if you check that IP address, it will normally only resolve to a single hostname (maybe one of the fifty, maybe not))

Actually Doing The DNS Translation

- So how do you actually mechanically do the DNS translation we've been talking about?
- If you're using a Unix/Linux box, or a Macintosh, you can pop up a terminal window and then use any of several different commands. Dig is probably the most popular DNS tool among professionals, but nslookup is another option that's easy to use:

```
% nslookup
> darkwing.uoregon.edu
Server:    128.223.32.35
Address:   128.223.32.35#53

Name: darkwing.uoregon.edu
Address: 128.223.32.35
```

What If You Don't Have a Unix Box or a Mac?

- While you can buy a \$300 Dell and run Linux on it, or pay \$500 for a Mac Mini, some users only have a PC running Windows.
- That's okay -- you can still do nslookup on a vanilla Windows XP PC too

Start --> Programs --> Accessories --> Command Prompt
C:\> nslookup
128.223.32.35 (or whatever)

- You can also do nslookup using any of a variety of web sites -- as long as you've got a web browser, you can do DNS "stuff" online. :-) One such example is:
<http://www.zoneedit.com/lookup.html>

Your Goal In Doing nslookup

- Start with the dotted quad, translate it to the hostname, translate the hostname to the dotted quad until you either run into a hostname or dotted quad that doesn't resolve, or you find a consistent dotted quad to hostname to dotted quad mapping.
- Why bother going through that process? Well, spammers have been known to try to lie about their inverse addresses. For example, you might look up a dotted quad, only to find that it resolves to something improbable like `nowayamigoingtoletyoubustme.com`
- On the other hand, if you resolve a dotted quad to a hostname and then that hostname in turn resolves to that same dotted quad, you can have some confidence that the hostname really is associated with that dotted quad.

DNS “Problems”

- Spammers may not define ANY inverse address records for their dotted quads (non-spammers may ALSO not do this; this sloppiness is particularly common in parts of the world where DNS does not do a great job of handling the local character set (e.g., Korean, Chinese, Vietnamese, etc.)
- You can access “synthetic” inverse addresses for at least some of these IP addresses by checking the RUS-CERT Passive DNS Server. It synthetically associates IP addresses with hostnames by logging A records as they get resolved, and then allowing searches on the dotted quads which were logged as well as the A hostname values. Of course, this approach only works if the folks providing RUS-CERT with data have seen queries for the IP address that’s of interest.

RUS-CERT Example

The screenshot shows a web browser window titled "RUS-CERT - Passive DNS Replication - Mozilla Firefox". The address bar contains the URL `http://cert.uni-stuttgart.de/stats/dns-replication.php?query=218.153.11.16&submit=Query`. The page header features the "RUS CERT" logo and the text "Computer Emergency Response Team DV-Sicherheit an der Universität Stuttgart". A navigation bar includes links for "Kontakt", "Sitemap", "Impressum", "E-Mail-Abo", and "Presse".

A left sidebar menu lists various services and resources, with "Dienste" (Services) currently selected. The "Dienste" menu includes: Home, Aktuelle Meldungen, Betriebssysteme, Themen, Dienste (selected), Uni-Firewall, Verkehrsbeobachtung, Top 5, Mailinglisten, Passworttest, Angriff, Incident Response, VulnerabilityResponse, Projekte, Archive, and Jobs.

The main content area is titled "Passive DNS Replication" and contains the following text:

RUS-CERT runs a DNS replication server as a service to the CERT community. By using this web page, you can query the replication database and obtain information that is not readily available through traditional DNS queries.

Do not run automatic queries against this database. If you want to submit bulk queries, please contact [the operators](#).

Query string:

The server returned the following data:

[club.bugs.co.kr](#) A [218.153.11.16](#)

The server status is **201 Okay**.

Passive DNS Replication Also Lets You See The Domains Using a Common Name Server (unrelated example)

RUS-CERT - Passive DNS Replication - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://cert.uni-stuttgart.de/stats/dns-replication.php?query=dog.ccpatoncejk.biz

Firefox Help Firefox Support Plug-in FAQ RUS-CERT - Passive ...

Markingasten

Passworttest

Angriff

Incident Response

VulnerabilityResponse

Projekte

Archive

Jobs

Universität Stuttgart

Rechenzentrum der Universität Stuttgart

Suche in Meldungen

Los geht's

Query string: dog.ccpatoncejk.biz

Query

The server returned the following data:

burtonabdea.com	NS	dog.ccpatoncejk.biz
anointefbha.com	NS	dog.ccpatoncejk.biz
achotelcia.com	NS	dog.ccpatoncejk.biz
dlsingledb.com	NS	dog.ccpatoncejk.biz
guacofknhb.com	NS	dog.ccpatoncejk.biz
gunlyndhib.com	NS	dog.ccpatoncejk.biz
feputrefymb.com	NS	dog.ccpatoncejk.biz
coderlbqfc.com	NS	dog.ccpatoncejk.biz
stereeaafc.com	NS	dog.ccpatoncejk.biz
lygeungjmic.com	NS	dog.ccpatoncejk.biz
dutchibabd.com	NS	dog.ccpatoncejk.biz
ambushlmdbd.com	NS	dog.ccpatoncejk.biz
yunkghcd.com	NS	dog.ccpatoncejk.biz
revertalmgd.com	NS	dog.ccpatoncejk.biz
entitycdfjd.com	NS	dog.ccpatoncejk.biz
ulemabld.com	NS	dog.ccpatoncejk.biz
solveaiaand.com	NS	dog.ccpatoncejk.biz
unbungkanbe.com	NS	dog.ccpatoncejk.biz
editehkce.com	NS	dog.ccpatoncejk.biz
visnencgke.com	NS	dog.ccpatoncejk.biz
darjheef.com	NS	dog.ccpatoncejk.biz
uigurimfif.com	NS	dog.ccpatoncejk.biz
zinciccgag.com	NS	dog.ccpatoncejk.biz
klfiduciaig.com	NS	dog.ccpatoncejk.biz
lkchordabjg.com	NS	dog.ccpatoncejk.biz

What Else Can We Do With the Dotted Quad?

- In addition to seeing what a dotted quad resolves to by checking its in-addr (or RUS-CERT), we can also see who has been officially assigned that address range.
- Understanding IP address assignment requires a brief detour to explain how IP addresses are obtained.
- Normally an end user, like Cousin Bob or Aunt Edna, just temporarily uses IP addresses that have been assigned to their internet service provider (ISP).
- What if Aunt Edna RAN her own ISP, however? Where would she get IP addresses then? These days, if she's a small ISP, she'd still end up getting IP addresses from her upstream provider (in her case she'd get a chunk (or "block" of IP addresses instead of just one, and she'd get them assigned for the duration of her contract with her upstream provider, rather than just a brief time).

How Are Long Term IP Address Assignments Documented?

- Any customer assignment that is at least a /29 or larger has to be defined using SWIP (shared whois IP service) or rwhois (referral whois).
- Whoa -- I see I need to back up and explain one more concept, and that's CIDR address block notation.
- In the old days, IP addresses were assigned on “classful boundaries” -- e.g., at “dot” boundaries. If you needed a block of addresses, you either got a “class C” block (256 addresses), a “class B” block (65,534 addresses), or a “class A” block. Unfortunately, classful network allocations are sort of like Goldilocks: some are too big, some are too small, and it is hard to get one that's just right.
- If we had infinite addresses, then who'd care, but unfortunately IP addresses are a finite resource.

CIDR to the Rescue (And It Isn't Hard CIDR!)

- CIDR said, “Hey, who cares about where the dot is? We’ll give you a block that’s the size you need.
- CIDR blocks are written as a starting address followed by a slash and the size of the allocation.
- A single IP address is a /32.
- Two IP addresses make up a /31.
- Four IP addresses make up a /30.
- Eight IP addresses are a /29.
- Sixteen IP addresses are a /28.
- Etc, etc., etc.
- Remember, allocations that are at least a /29 or larger are required to be documented. If someone has eight IP addresses, we should be able to “look that assignment up” and see “whois responsible” for them.

Whois trivia

- Whois differs from nslookup in that whois is less seamless. You need to “know” where to start when it comes to looking up IP addresses.
- There are four normal starting points:
 - whois.arin.net (for North American IP addresses)
 - whois.ripe.net (for European IP addresses)
 - whois.apnic.net (for Asian Pacific IP addresses)
 - whois.afrinic.net (for African IP addresses)
- If you guess wrong, you’ll normally be redirected to the right registry. If not, just try another one at random. :-)
- After a while, you’ll develop an instinctive sense for which registry to go to for particular numeric blocks of addresses (addresses are assigned to registries in relatively large “clumps”).

Looking Up IP Assignments With Whois

- The process of looking up an IP address assignment involves using the cleverly named whois command. Like nslookup, whois is something that you can run directly from the Unix shell prompt if you have a Linux box or a Mac:
% whois -h whois.arin.net 128.223.32.35
- In some cases you may end up with more than one whois entry that “matches” a given IP address (to understand this, remember that a medium size ISP might have a /19, from which they make assignments of /24’s to smaller downstream ISPs, who in turn might make assignments of /29’s to small web hosting concerns). When that happens, you can rerun whois specifying the name of the most-specific block mentioned to usually get the “right” party using a given IP.

Faking It On A PC

- Most PCs running Windows don't come with a whois client, but you can "pretend" to be a whois program on a PC, by popping up a DOS window and entering:

C:\> telnet nameofthewhoisserver 43

then plug in the IP address that's of interest

Disappointments

- Whois data does not always work out the way you'd like it to... For example, you may see:
 - whois report a HUGE block of addresses belonging to a large provider like Comcast or Qwest, typically for temporary use by casual retail customers (like Cousin Bob). To find out who had that IP address at a given point in time, you'll need to hit the provider with a suitable bit of legal paperwork, as well as the IP address and a time stamp, to get the identity of the user at that time. (note: the logs needed to make that association may be rolled over/destroyed relatively quickly; if you're interested in this data, you will want to ask the provider to preserve the records required to do that IP to customer mapping (at least you now know what provider to ask to do that!))

An Aside: Why Do You Need Timestamps?

- You should routinely note and provide timestamps in conjunction with requests for information about who had an IP address at a given time because dynamic pools of IP addresses get continually reused. That is, when one person finishes using an IP address, it gets returned to the pool of available addresses and then another person will eventually be given that IP. This sort of address assignment normally happens via something known as “DHCP” or “Dynamic Host Configuration Protocol.”
- Without a time stamp, there might be a dozen or more users who were “on” a DHCP pool IP address during the course of a typical day. On the other hand, sometimes addresses may nominally be “dynamic” yet practically never change. Think of these as “pseudo static” IP addresses.

That's Not the Only Possible Disappointment

- You may also run into a “private residence” registration, e.g., a block of IP's that are in use by someone who's just a regular person, not a company.

Regular people are allowed to have their address information withheld from IP whois listings to preserve the privacy of their residence address.

Law enforcement can, of course, use legal process to compel the ISP to disclose the customer information associated with such an IP address range, regardless of the preferences of the customer.

A Third Way Things Can Go Wrong

- You should also be prepared for the possibility that the IP block was hijacked, or used without authorization. In such a situation, a spammer identifies a network block and convinces an ISP to begin advertising it (letting the spammer use those addresses), typically by providing the ISP with a fraudulent LOA (letter of authorization).
- A list of known hijacked IP blocks can be found at <http://www.completewhois.com/>
- See also <http://www.spamhaus.org/drop/index.lasso>
- We'll talk more about routing later.

Whois data for 202.164.51.114

```
whois -h whois.apnic.net 202.164.51.114
inetnum:      202.164.51.112 - 202.164.51.119
netname:      PUNJABAGRO
country:      IN
descr:        KHARAR
admin-c:      RS341-AP
tech-c:       RS341-AP
status:       ASSIGNED NON-PORTABLE
changed:      sanjay.kumar@hfclconnect.com 20050717
mnt-by:       MAINT-IN-RAVINDER
source:       APNIC

person:       Ravinder Singh
nic-hdl:      RS341-AP
e-mail:       ravinder.singh@hfclconnect.com
address:      B-71 , Industrial Area Phase VII
address:      Mohali
phone:        +91-172-5090114
country:      IN
changed:      pankaj.mehta@hfclconnect.com 20050428
mnt-by:       MAINT-NEW
```

Whois Can Also Tell You About Domains

- Whois can also be used to tell you about who is responsible for domain names:

```
% whois okiodata.net
Domain Name: OKIODATA.NET
Registrar: ENOM, INC.
Whois Server: whois.enom.com
Referral URL: http://www.enom.com
Name Server: NS1.AXARNET.NET
Name Server: NS2.AXARNET.NET
Status: ACTIVE
Updated Date: 16-aug-2005
Creation Date: 13-aug-2003
Expiration Date: 13-aug-2006
```

Note the Referral...

- The whois server that was queried by default didn't have detailed information about the domain in question, but it did know where to send us if we wanted to get that info (e.g., it “referred us” to whois.enom.net)
- This is common for whois...

Sample detailed whois data for a domain

```
% whois -h whois.enom.com okiodata.net
```

```
Registration Service Provided By: Axarnet  
Comunicaciones SL
```

```
Contact: info@axarnet.es
```

```
Visit: https://www.axarnet.es/renovar.asp
```

```
Domain name: okiodata.net
```

```
Registrant Contact:
```

```
Okiodata Iberica Software
```

```
Pascual Raga (pascualraga@okiodata.com)
```

```
+34.963467277
```

```
Fax: +34.963465409
```

```
Profesor Beltran Baguena, 5,6, 20-21
```

```
Valencia, Valencia 46009
```

```
ES
```

Sample detailed whois data for a domain (cont.)

Administrative Contact:

Axarnet Comunicaciones SL
Jesus Pinazo (info@axarnet.es)
+34.952544569
Fax: +34.952546363
C/ Dr. Flemming, 2-2
Torre del Mar, MALAGA 29740
ES

Billing Contact:

Axarnet Comunicaciones SL
Jesus Pinazo (info@axarnet.es)
+34.952544569
Fax: +34.952546363
C/ Dr. Flemming, 2-2
Torre del Mar, MALAGA 29740
ES

Sample detailed whois data for a domain (cont. 2)

Technical Contact:

Axarnet Comunicaciones SL
Jesus Pinazo (info@axarnet.es)
+34.952544569
Fax: +34.952546363
C/ Dr. Flemming, 2-2
Torre del Mar, MALAGA 29740
ES

Status: Locked

Name Servers:

ns1.axarnet.net
ns2.axarnet.net

Creation date: 13 Aug 2003 04:29:54

Expiration date: 13 Aug 2006 04:29:54

Whois Privacy Services

- When investigating interesting domain name registrations in whois, you should be prepared to see both blatantly bogus information, and information that's "hidden" from public view by means of whois privacy protection service providers.
- Blatantly incorrect whois data should be reported to <http://wdprs.internic.net/>
- Data hidden from public whois access may require suitable paperwork compelling disclosure for investigatory purposes
- Note that in some cases, the spammer or phisher may be the registration service provider...

OK, So What?

- Once you have contact info for a message source, you then have the ability to contact that source for:
 - information about the customer of interest (likely will require suitable paperwork)
 - mitigation of the compromised systems (and yes, many of the systems that you run into WILL be compromised) -- for more information on how ISPs are beginning to approach those zombies, see my paper “Spam Zombies and Inbound Flows to Compromised Customer Systems” that’s at <http://www.uoregon.edu/~joe/zombies.pdf>

Who Should I Contact About A Given Domain?



The screenshot shows a Mozilla Firefox browser window with the title "Look up an address in the abuse.net contact database - Mozilla Firefox". The address bar contains "http://www.abuse.net/lookup.phtml". The page content includes the "NETWORK ABUSE CLEARINGHOUSE" logo, the heading "Look up an address in the abuse.net contact database", and a form with a text input field and a "Lookup" button. Below the form are two links: "Look up another domain" and "Return to the abuse.net home page". At the bottom, it says "This page updated: 01/02/2004" and "© 1999-2001 I.E.C.C."

Look up an address in the abuse.net contact database - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.abuse.net/lookup.phtml

Firefox Help Firefox Support Plug-in FAQ RUS-CERT - Passive ...

NETWORK ABUSE CLEARINGHOUSE

Look up an address in the abuse.net contact database

Enter the name of the domain that you would like to check, such as example.com.

 [Look up another domain](#)

 [Return to the \[abuse.net home page\]\(#\).](#)

This page updated: 01/02/2004

© 1999-2001 I.E.C.C.

All domain's should have a preferred reporting addresses on file!

Investigating a Host's/Domain's Reputation

- There are a number of resources online which will help you to investigate a host/IP address/domain/netblock's reputation. Some you may want to try include:
 - <http://www.spamhaus.org/>
 - <http://www.senderbase.org/>
 - <http://www.mynetwatchman.com/>
 - <http://www.openrbl.org/>
 - <http://www.spamcop.net/>

Routing of IP Address Space

- While you are now familiar with whois as a way of finding out who is responsible for a given block of IP addresses or a specific domain name, there is one other piece to the puzzle that you need to know about...
- Blocks of IP addresses get routed, or announced to the Internet, by ISPs. The ISP announcing a given block may or may not be the same party that shows up in whois as being responsible for those addresses.
- To see who's routing a given address block, or who's "upstream," from a site, beginning users will often try using traceroute. Traceroute will show you one path by which packets get to a given site of interest, but they may miss many others which are equally or more important.

Sample Traceroute

```
traceroute www.amazon.com
```

```
traceroute to www.amazon.com (207.171.166.102), 30 hops max, 40 byte packets
```

```
1  vlan214.uonet2-gw.uoregon.edu (128.223.214.3)  154.805ms  4.114ms  0.689ms
2  0.ge-0-0-0.uonet8-gw.uoregon.edu (128.223.2.8)  1.318ms  2.484ms  0.49ms
3  eugn-car1-gw.nero.net (207.98.64.65)  0.658 ms  0.54 ms  0.609 ms
4  eugn-core2-gw.nero.net (207.98.64.169)  0.513 ms  0.573 ms  0.499 ms
5  ptck-core2-gw.nero.net (207.98.64.2)  2.898 ms  2.831 ms  4.799 ms
6  ptck-core1-gw.nero.net (207.98.64.137)  7.654 ms  2.871 ms  2.932 ms
7  so-6-1.hsa2.seattle1.level3.net (63.211.200.245)  5.937ms  6.201ms  5.957ms
8  ae-1-52.mp2.seattle1.level3.net (4.68.105.33)  6.296ms  6.167ms  7.289ms
9  as-1-0.bbr1.washington1.level3.net (4.68.128.201)  70.789 ms  70.869 ms
   as-2-0.bbr2.washington1.level3.net (209.247.10.130)  70.336 ms
10 ge-3-0-0-55.gar3.washington1.level3.net (4.68.121.132)  70.662 ms
    ge-4-0-0-52.gar3.washington1.level3.net (4.68.121.36)  70.49 ms
    ge-4-0-0-56.gar3.washington1.level3.net (4.68.121.164)  70.296 ms
11 amazon-com.gar3.washington1.level3.net (4.79.192.10)  70.674 ms  70.792 ms
    70.768 ms
12 72.21.201.24 (72.21.201.24)  70.918 ms  70.892 ms  70.984 ms
13 * * *
[etc]
```

A More Sophisticated Approach

- A more sophisticated approach to figuring out who's "upstream" of a site involves checking the Internet routing tables. The University of Oregon Route Views project (see <http://www.routeviews.org/>) coincidentally has what is perhaps the world's finest collection of real time Internet routing data
- See the discussion at <http://www.uoregon.edu/~joe/one-pager-asn.pdf> for information on how to work with that data
- You should also know about the Team Cymru public whois server, which does IP to ASN mapping...

Team Cymru Whois Server



Team Cymru is happy to announce the availability of a public whois server dedicated to mapping IP numbers to ASNs, located at **whois.cymru.com**. We have also extended the functionality of this daemon to support BULK IP submissions when combined with netcat, for those who wish to further optimize their queries. We recommend the use of the GNU version of netcat, not nc. GNU netcat can be downloaded from <http://netcat.sourceforge.net/download.php>.

The data provided by the whois server is based on 17 BGP peers, and is updated every 30 minutes.

Using the WHOIS Server

Following is a quick overview of how to use the Team Cymru whois server:

```
$ whois -h whois.cymru.com <IP>
```

Where <IP> is replaced by the IP you'd like to map, like so:

```
$ whois -h whois.cymru.com 68.22.187.8
ASN      | IP          | Name
23028    | 68.22.187.8 | SAUNET SAUNET
```

You can also include comments in your queries. These might be port information, timestamps, or

IV. What About The Body of the Message?

In The Body of the Message, You're Basically Looking for the Spamvertised Website...

- When we were focussed on the message headers, the emphasis was on finding where the message came from. When we move to the message body, the emphasis changes, and becomes one of figuring out where the spammer or phisher wants you to go.
- Sometimes the target destination will be a phone number or mailing address, but most often the target destination -- the purpose for the mail -- will be a web site.
- You can use the same tools we've already talked about (nslookup, IP whois, domain whois, etc.) to look at those links, but there are some additional tricks you should know about.

curl

- Normally you retrieve web pages using a web browser such as Internet Explorer or Firefox. When you do so, the browser automatically handles some things in a transparent way that may not be in your best interest if you're interested in following the breadcrumbs.
- A handy alternative you should know about is “curl”
- Curl is included in many current versions of Unix, or you can download it online from <http://curl.haxx.se/>
- Curl will let you see both the headers and the full raw body of a web page

Mechanics of Using Curl

- I recommend redefining curl to be:
`alias curl 'curl -i --no-buffer --junk-session-cookies'`
- Then say, for example:

```
% curl "http://www.ppmort.net/j.php" > ppmort.txt
```

When you then look at the content of ppmort.txt, you see...

```
% more ppmort.txt
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">
<html>
<head>
<title>Refinance With US!</title>
<meta http-equiv="REFRESH"
content="0;url=index.php?id=j38"></HEAD>
<BODY>
</BODY>
</HTML>
```

Things Curl Will Show You

- When you start looking at spamvertised web pages with curl, you should expect to routinely start seeing:
 - http meta refresh redirection
 - status code-based redirection
 - framing of the “real” site that’s under the spamvertised site
 - javascript redirection
- Note that what you are shown may depend on what the spamvertised site sees for a default “agent type” (e.g., what sort of browser you seem to be using). Curl will let you set the browser agent string to anything you like which should allow you to defeat that sort of thing.

Obfuscation

- Some spammers may attempt to obfuscate the URLs of their web sites, either by %-encoding them or by other means. You should be aware that it will normally be possible to de-obfuscate those links using online tools. For example, you may want to try cutting and pasting a %-encoded block of text into:

`http://www.uoregon.edu/~joe/xl-cgi.pl`

to deobfuscate it.

- There are numerous other decoders for other types of text (e.g., raw base64 mime attachments, etc.)

A Caution for Those of You Working From Windows

- When ripping into the bodies of messages, it is possible that you will bump into hostile content, usually targeting Windows computers.
- Beware of what you retrieve, and how you then look at that content. In particular, if you retrieve an executable program mentioned in the body of a piece of spam, be particularly wary of “just running it.” Quick checks that will often (but NOT ALWAYS) detect problematic executables can be found at:

-- <http://www.virustotal.com/>

-- <http://virusscan.jotti.org/>

see also the Norman Sandbox Information Center:

-- <http://sandbox.norman.no/>

V. Ripping Apart a Sample Phish

Ripping Apart A Sample Phish

- This example is a real eBay phish, received on Saturday night, April 23rd, 2005, and forwarded to us by the recipient on Sunday morning. The reporting user, like most of our users, has been trained to supply spam samples complete with FULL HEADERS as described at <http://micro.uoregon.edu/fullheaders/>
- Unfortunately the vast majority of spam samples reported by casual email users, whether to ISPs or to government agencies, lack expanded headers (a fact which delights typical spammers, obviously).
- Make sure the victims you work with know how to enable full headers!

Headers From The Sample eBay Phish

```
>Return-Path: <wwwrun@golf.webmind.de>
>Received: from golf.webmind.de ([145.253.231.171])
>      by darkwing.uoregon.edu (8.13.4/8.13.4) with ESMTP id j302SKxa011425
>      for <[redacted]@darkwing.uoregon.edu>; Sat, 23 Apr 2005 19:28:20-0700 (PDT)
>Received: by golf.webmind.de (Postfix, from userid 30)
>      id 799FDE557C; Sun, 24 Apr 2005 04:29:17 +0200 (CEST)
>To: [redacted]@darkwing.uoregon.edu
>Subject: Your Account Will Be Suspended
>From: eBay Billing Department <Billing@eBay.com>
>Reply-To: update@eBay.com
>MIME-Version: 1.0
>Content-Type: text/html
>Content-Transfer-Encoding: 8bit
>Message-Id: <20050424022917.799FDE557C@golf.webmind.de>
>Date: Sun, 24 Apr 2005 04:29:17 +0200 (CEST)
>Status:
>
>Hello! <http://signin.ebay.com/ws2/eBayISAPI.dll?SignIn>Sign=20
>in/out<http://pages.ebay.com/ebay_IBM.html>.
>
>Dear eBay valued member,
```

Let's start with stuff from the full header, specifically the IP address that handed us the message. (After we get done poking at that, then we'll come back to the rather interesting Reply-To: address.)

The Phish Was Received From 145.253.231.17

```
% whois 145.253.231.17  
[ querying whois.ripe.net for 145.253.231.17 ]  
% This is the RIPE Whois query server #1.  
% The objects are in RPSL format.  
%  
% Rights restricted by copyright.  
% See http://www.ripe.net/db/copyright.html
```

```
inetnum:      145.253.231.0 - 145.253.231.255  
netname:      SIRCON-NET  
descr:        Sirconic Group GmbH  
descr:        Breslauer Str. 49  
descr:        D-83395 Freilassing  
descr:        Germany  
country:      DE  
admin-c:      SD2300-RIPE  
tech-c:       ANOC1-RIPE  
status:       ASSIGNED PA  
mnt-by:       ARCOR-MNT  
notify:       ip-registry@arcor.net  
changed:      ip-registry@arcor.net 20040929  
source:       RIPE
```

```
person:       Sezgin Demircan  
address:      Breslauer Str. 49  
address:      D-83395 Freilassing  
address:      Germany  
e-mail:       sd@sirconic-group.de  
phone:        +49 8654 7788510  
fax-no:       +49 8654 7788511  
mnt-by:       ARCOR-MNT  
notify:       ip-registry@arcor.net  
nic-hdl:      SD2300-RIPE  
changed:      ip-registry@arcor.net 20040929  
source:       RIPE
```

What Does Whois say about sirconic-group.de?

```
% whois sirconic-group.de  
[ querying whois.denic.de for sirconic-group.de ]  
domain:          sirconic-group.de  
status:          connect
```

- Dot de (German) domain registrations have taken privacy concerns to an absurd length, with the result that little if anything of use is shown for many .de domain names (unlike IP whois records, as shown on the preceding page).
- In this case, if we wanted to (e.g., to try to get this phishing site torn down), we could also look at the web site for the domain for contact information.
- We'll stay with the dotted quad (e.g., the IP address).

145.253.231.17 Isn't Blocklisted

Openrbl: Multi DNSBL Lookup 145.253.231.17 145.253.231.17 - Mozilla Firefox


File Edit View Go Bookmarks Tools Help


http://www.openrbl.org/ip/145/253/231/17.htm Go

Openrbl DNSBL Whois Route Multi DNSBL Lookup

IP or Hostname 145.253.231.17 Submit Singlepage

Lookup 145.253.231.17 (golf.webmind.de) in 20+8 Zones

AS: 145.253.0.0/16 AS3209  Arcor IP-Network UNKNOWN

Net 145.253-145.254 ARCOR-IP  @adm.arcor.net

Results: **Negative=28**, Positive=0 (2005-04-24 16:00:27 UTC)

- **Negative 28:** @COUNTRY @DYNAMIC @ISP @SPAM AHBL AUDNSBL BOGONS BOPM CBL DRBL DSBL FIVETEN INTERSIL JIPPGMA LNSG NJABL NOMORE ORDB PSBL SBL SORBS SPAMBAG SPAMCOP SPAMRBL SPAMSITE SPEWS UCEPROT WPBL

Hints for 145.253.231.17: ([external](#), use BACK or ALT-LEFT when done)

- Track "golf.webmind.de" at [[Whois & Abuse](#)|[SpamCop](#)]
- Search "145.253.231.17" at [[Google](#)|[SpamCop](#)]*[[SenderBase](#)] [[MAPS](#)|[Schlund](#)]
- **CHECK:** Nominate Relay-Test at: [[ORDB](#)] [[Add Comment](#)]

145.253.231.17 Has No Senderbase History

SenderBase - 145.253.231.17 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.senderbase.org/search?searchString=145.253.231.17

Home Domains IP's

Report on IP address: 145.253.231.17

Volume Statistics for this IP

	Magnitude	Vol Change vs. Average
Last day	0.0	- .00%
Last 30 days	0.0	- .00%
Average	0.0	

Third-party Certification

Bonded Sender?	Not Bonded
TRUSTe Privacy Seal?	Not Certified

Information from whois [Click to show details]

Network Owner:	RIPE Network Coordination Centre
Registered on:	1993-05-01
Updated on:	1993-05-01
Expires on:	unknown

Other information about this IP address

Sender Category	unknown
Network Owner	unknown
Domain	unknown
Date of first message seen from this address	
CIDR range	unknown
# of domains controlled by this network owner	0
Geography data	
Country	unknown
State	unknown
City	unknown
Postal code	unknown

Related links

Google groups	http://groups.google.com/groups?scoring=d&q=145.253.231.17+group:*abuse*
OpenRBL	http://openrbl.org/dnsbl?i=145.253.231.17
SpamCop	http://spamcop.net/w3m?action=checkblock&ip=145.253.231.17

Real-time blacklists [Click to view all]

not in any blacklists

No address list shown since no email was detected from 145.253.231.0/24.

Conclusion About This IP...

- 145.253.231.17 is likely a newly hijacked IP address at a compromised host, perhaps running a vulnerable web cgi-bin application of one sort or another (note the "wwwrun" Return-path in the phish, a username commonly associated with cgi-bin execution environments)

What About That Odd Reply-To Address?

[querying whois.wildwestdomains.com for eba-y.com]

Registrant:

Non
2341 21st. st. Apt. C.
San pablo, California 94806
United States

Registered through: GO PAPPI

Domain Name: EBA-Y.COM

Created on: 01-Apr-04

Expires on: 01-Apr-06

Last Updated on: 06-Apr-05

Administrative Contact:

Miranda, Carlos mugamil@webtv.net
Non
2341 21st. st. Apt. C.
San pablo, California 94806
United States
(888) 491-2133

Technical Contact:

Miranda, Carlos mugamil@webtv.net
Non
2341 21st. st. Apt. C.
San pablo, California 94806
United States
(888) 491-2133

Domain servers in listed order:

NS1.AFTERNIC.COM
NS2.AFTERNIC.COM

A Note On Email Addresses in Spam/Phishing Headers -- Real or Possibly Just "Joe Jobs"

- An email address seen in a mail message header may be one really controlled by the person sending the mail, or it may be a spoofed address (an address that has no connection to the spam/phishing message whatsoever).
- Why would a spammer potentially use a real address? A real address might be getting used to collect messages that bounce, or to handle communications with victims who try to reply to the phishing message (rather than visiting the phishvertised web form)
- A spoofed address might ALSO be used to misdirect the curious, or in an attempt to implicate a competitor or to punish an innocent party (such as an antispammer)
- Let's see if our conclusions are helped by "vetting" the whois data we just saw...

Is The Street Address Used for The Domain Whois Superficially Valid? Yes...

 UNITED STATES
POSTAL SERVICE®

<http://www.usps.gov/zip4/>

ZIP Code Lookup

ZIP + 4® Code Lookup Results

Below is the correct ZIP + 4 Code from the address information that you provided.

Address (Standard Format) What is This?

2341 21ST ST APT C
SAN PABLO CA 94806-3559

Mailing Industry Information What is This?

[Lookup another ZIP Code >](#)

Do We See the 1-888 Number Used In That Domain Registration Show Up Anywhere? Yes

The screenshot shows a Google search interface with the URL `http://www.google.com/search?hl=en&q=888-491-2133&btnG=Google+Search`. The search bar contains the text "888-491-2133". Below the search bar, the "Web" tab is selected, and the results show "Results 1 - 10 of about 260 for 888-491-2133".

The first result is from [Nantucket Online.com - Classifieds](#). The snippet mentions "Madeleine Madelia • 888-491-2133 • Wilam, United States ... Van Morrison • 888-491-2133 • Wilam, NL, United States • spankaj82@yahoo.com ...". The URL is [nantucketonline.com/classifieds/classifieds.php?classifieds_category_id=3 - 24k - Cached - Similar pages](#).

The second result is from [WhoWon.com ... The Internet Source for Motorsports News and ...](#). The snippet mentions "Home Phone: 888-491-2133 Bus. Phone: 888-491-2133 Email: paragchandranthmahajan@yahoo.com ... Home Phone: 1-888-491-2133 Bus. Phone: 1-888-491-2133 ...". The URL is [www.whowon.com/showclass50.asp?cat=15 - 50k - Cached - Similar pages](#).

The third result is from [Sports collectible](#). The snippet mentions "3.20.2005 Carlos Miranda (Alaska, Business) 888-491-2133 Visit website Send ... 4.5.2005 Van Morrison (Alabama, Business) 888-491-2133 Send e-mailE-mail ...". The URL is [www.domesticsale.com/Classifieds/search/sports-collectible/ - 31k - Cached - Similar pages](#).


The fourth result is from [Dialysis Employment](#). The snippet mentions "Phone: 888-491-2133. Tuesday, April 12, 2005, Wilam, Act now have some fun and make real money from now on. A life time opportunity to promote the dream ...". The URL is [www.globaldialysis.com/Jobs.asp?t=9&Page=9 - 45k - Cached - Similar pages](#).

The fifth result is from [Indonesia Interactive >> HOME](#). The snippet mentions "For more information you can call 888-491-2133, or visit http://sportsbookusa.us. Give a respond Modify Delete. posted by gautam at 4/13/05 2:40:38 PM ...". The URL is [www.i2.co.id/mall/ad_list_new.asp?new=1 - 41k - Cached - Similar pages](#).


The sixth result is from [kzn.co.za Classifieds: for sale, wanted, swap - General ...](#). The snippet mentions "Contact: Madeleine Madelia, Phone: 888-491-2133. Price: \$18.5, Email: krishnashankar77@yahoo.com. Town: Wilam, Province: Mpumalanga ...". The URL is [www.kzn.co.za/business/classifieds.asp?page=5&classType=classifieds - 41k - Cached - Similar pages](#).

At the bottom of the browser window, there is a search bar with the text "gate" and buttons for "Find Next", "Find Previous", "Highlight", and "Match case".

Can We Use Our Original Phone Number to Find Additional Ones? Yes

 Nantucket Online.com - Classifieds - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

 http://nantucketonline.com/classifieds/classifieds.php?classifieds_category_id=3

Used farm tractors Wednesday April 20th 2005
06:18:33

Over 100 tractors in stock. Used and new tractors. A wide variety of quality and prices for all.

• Mahalia Mahari • 315-465-6492 • Loas, United States • paragchandra79@yahoo.com

The Instant Publisher Platinum CDROM Wednesday April 20th 2005
06:18:15

A fabulous collection of 750 Books, Reports & Manuals You Can Reprint & Sell and Make a Fortune! How to Write a Job Winning Resume, How to Sell Books ByMail, How to Write Profitable Classified Ads and many more!

• Mahari Mahari • 561-582-1874 • Hypoluxo, FL, United States • ganeshshivshan79@yahoo.com

Monday April 18th 2005 22:53:07

Increase your business productivity with our consulting services which includes Executive Coaching, Sales Training, and organizational analysis

• Maitland Maj • 317-290-6744 • Carmel, ID, United States • pankajjosh79@yahoo.com

the free sports book Monday April 18th 2005 22:52:04

Act now have some fun and make real money from now on. An exciting product to make real money.

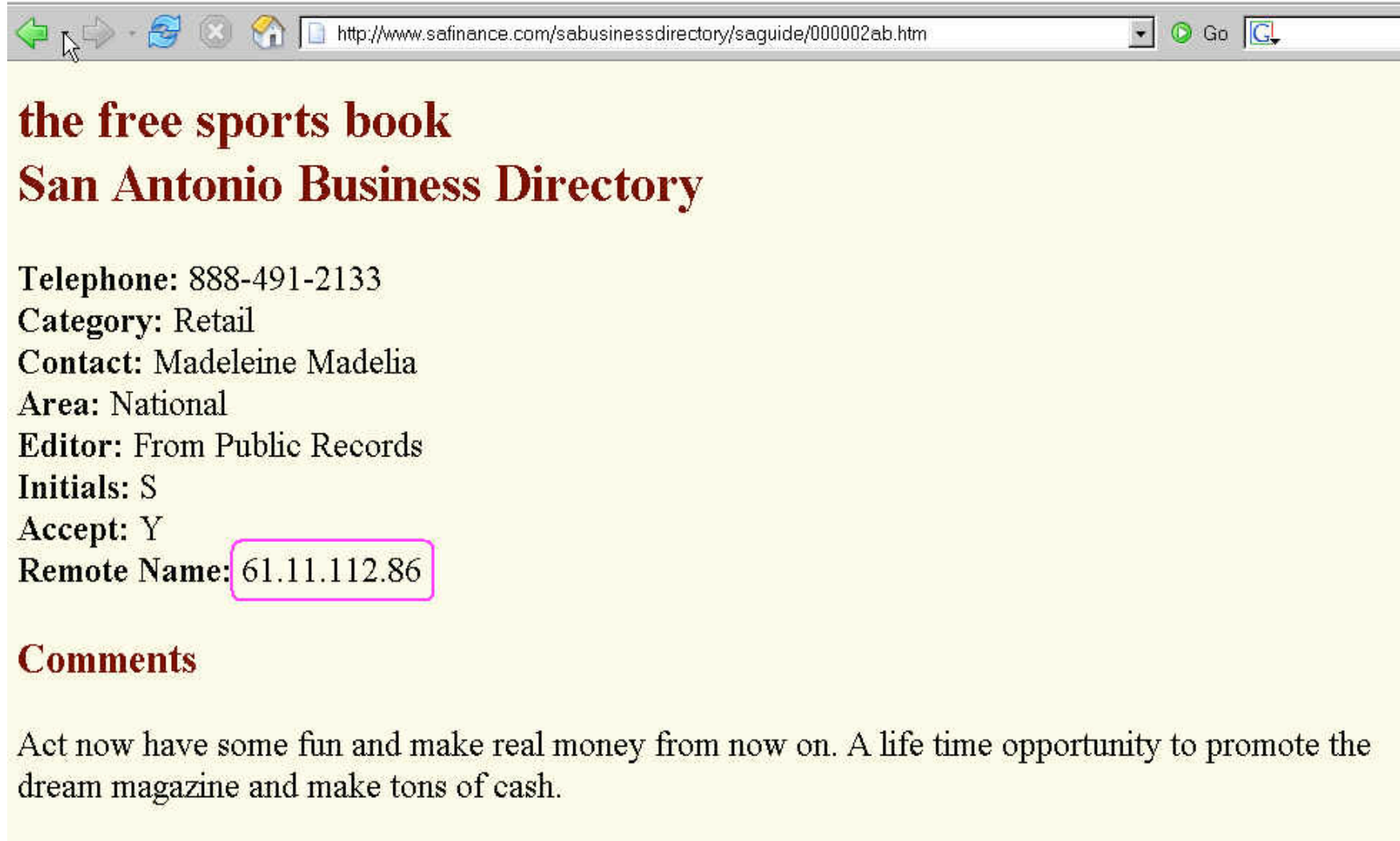
• Maitland Maj • 888-491-2133 • Wilam, United States • anilbalakar76@yahoo.com

the free sports book Monday April 18th 2005 06:43:34

Act now have some fun and make real money from now on. An exciting product to make real money.

• Maitland Maj • 888-491-2133 • Wilam, United States • anilbalakar76@yahoo.com

Some Free Classified Add Sites Record Where Postings Apparently Come From...



A screenshot of a web browser window. The address bar shows the URL: <http://www.safinance.com/sabusinessdirectory/saguide/000002ab.htm>. The page content is as follows:

the free sports book
San Antonio Business Directory

Telephone: 888-491-2133
Category: Retail
Contact: Madeleine Madelia
Area: National
Editor: From Public Records
Initials: S
Accept: Y
Remote Name: 61.11.112.86

Comments

Act now have some fun and make real money from now on. A life time opportunity to promote the dream magazine and make tons of cash.

That's A Bombay, India Address

```
% whois 61.11.112.86
[ querying whois.apnic.net for 61.11.112.86 ]
% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        61.11.32.0 - 61.11.127.255
netname:        USNL-IN
descr:          Uidesh Sanchar Nigam Ltd - India.
descr:          Uidesh Sanchar Bhawan, M.G. Road
descr:          Fort, Bombay 400001
country:        IN
admin-c:        IA15-AP
tech-c:         UT43-AP
remarks:        +-----+
remarks:        This object can only be modified by APNIC hostmaster
remarks:        If you wish to modify this object details please
remarks:        send email to hostmaster@apnic.net with your organisation
remarks:        account name in the subject line.
remarks:        +-----+
mnt-by:         APNIC-HM
mnt-lower:      MAINT-USNL-AP
mnt-routes:     MAINT-USNL-AP
changed:        hostmaster@apnic.net 20010227
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20040930
source:         APNIC
```

Here's Another One from 61.11...



sports book for free **San Antonio Business Directory**

Telephone: 888-491-2133

Category: Service

Contact: Maitland Maj

Area: I-35 Corridor

Editor: From Public Records

Initials: \$.18.5

Accept: Y

Remote Name: 61.11.23.240

Comments

Act now have some fun and make real money from now on. If you are a sports lover, make money by reaching out to other sport lovers.

But Those Posting May Not Have Really Originated From Someone In India: Proxies!

Openrbl: Multi DNSBL Lookup 61.11.23.240 61.11.23.240 - Mozilla Firefox


File Edit View Go Bookmarks Tools Help


open RBL http://www.openrbl.org/ip/61/11/23/240.htm

Openrbl DNSBL Whois Route Multi DNSBL Lookup

IP or Hostname 61.11.23.240 Submit ☒ Singlepage

Lookup 61.11.23.240 (static23-240.dsl-pun.eth.net) in 20+8 Zones

AS: 61.11.16.0/21 AS10199  DishnetDSL Limited UNKNOWN

Net 61.11.0-31 DISHNET  Pune, Maharashtra @eth.net

Results: Positive=5, Negative=23 (2005-04-24 19:05:24 UTC)

- @DYNAMIC/dialup: 61.11.23/24: 553 ADSL/CABLE/DIALUP ADSL India DISHNET; SORBS DUL
- AUDNSBL/dnsbl.net.au: 61.11.23/24: 553 AUDNSBL Multiple Spam Traps Block List [\[Remove\]](#)
- CBL/abuseat.org: 553 CBL Proxy/Trojan [\[Remove\]](#)
- SORBS/sorbs.net: 61.11.23/24: 553 SORBS DUL [\[Remove\]](#)
- FIVETEN/61.11.8.157.misc.spam: miscellaneous address blocks that have sent spam here
- Negative 23: @COUNTRY @ISP @SPAM AHBL BOGONS BOPM DRBL DSBL INTERSIL JIPPGMA LNSG SPAMBAG SPAMCOP SPAMRBL SPAMSITE SPEWS UCEPROT WPBL

Hints for 61.11.23.240: ([external](#) use BACK or ALT-LEFT when done)

- Track "static23-240.dsl-pun.eth.net" at [[Whois & Abuse](#)|[SpamCop](#)]
- Search "61.11.23.240" at [[Google](#)|[SpamCop](#)]*[\[SenderBase\]](#) [[MAPS](#)|[Schlund](#)]
- CHECK: Nominate Relay-Test at: [[ORDB](#)] [[Add Comment](#)]

An Aside: If You're Interested in Open Proxies or Spam Zombies, You May Want to See...

- "The Open Proxy Problem: Should I Worry About Half a Million Trivially Exploitable Hosts?"
<http://darkwing.uoregon.edu/~joe/jt-proxies/open-proxy-joint-techs.ppt> (or .pdf)
- "Spam Zombies And Inbound Flows to Compromised Customer Systems,"
<http://darkwing.uoregon.edu/~joe/zombies.pdf>

Nutshell Summary for Accounts Associated with 888-491-2133

- That phone number is seen in conjunction with a wide variety of free/throw-away email accounts (often with stereotypical central asian-related names). At least some of the names used in conjunction with those accounts appear to be names of famous celebrities.

Maitland Maj anilbalakar76@yahoo.com

Margot Morrison pradeepbala74@yahoo.com

Madeleine Madelia krishnashankar77@yahoo.com

Van Morrison spankaj82@yahoo.com

Keanu Reeves paragchandrankanthmahajan@yahoo.com

David Bradshaw sowmyakrish82@yahoo.com

Maitland Maj chandrakantmahajan78@yahoo.co.in

Sam Dek paragsphade@yahoo.com

RekhaRekha rekhasanjaypatil74@rediffmail.com

Guyton Wanda DocNoah7@aol.com

raghu hms_raghavendra@yahoo.co.in

Rosalba Rosalia hms_1204ar8@yahoo.co.in

Aminah Amine iliashuss70@yahoo.com

Any Additional Data?

- 888-491-2133 was also seen in conjunction with sportsbookusa.us, a (domain registered to Carlos Miranda, 234 21st (apparently a typo) and/or 2341 21st. st. Apt. C., San Pablo, California, mugamil@yahoo.com (instead of mugamil@webtv.net) -- look familiar to what you saw for the eba-y.com whois? :-;
- Sportsbookusa.us and eba-y.com both live on 216.168.41.230 (that IP is part of a block allocated to digital.forest, Inc., 19515 North Creek Parkway, Suite 208, Bothell WA, 98011), and routed by AS11739 (digital.forest, Inc.).
- Someone interested in eba-y.com (like ebay.com, for example) would probably next go after the identity of the customer hosting those two domains at digital.forest using suitable legal paperwork.

Enough With The Headers, What Can We See In The Body of The Message?

- So far, remember that we've just been looking at the message headers.
- What can we see if we actually proceed down into the text of the body of the message? Quite a bit, actually, since our user submitted the actual raw text of the message the user received, rather than some HTML-rendered representation...

Raw Body of the Phishing Message...

```
#299          24-APR-2005 05:45:55.42          NEWMAIL
>Hello! <http://signin.ebay.com/ws2/eBayISAPI.dll?SignIn>Sign=20
>in/out<http://pages.ebay.com/ebay_IBM.html>.
>
>Dear eBay valued member,
>
>During our regularly scheduled account maintenance and verification=20
>procedures, we have detected an error in your billing information.
>
>This might be due to either of the following reasons:
>
>1. A recent change in your personal information ( i.e. change of address).
>2. Submitting invalid information during the initial sign up process.
>3. An inability to accurately verify your selected option of payment due=20
>to an internal error within our processors.
>To avoid account suspension you must go to the link below and provide=20
>required informations:
><http://ebaserv-cgi-update-account.com/>http://cgi1.ebay.com/aw-cgi/eBayISA=
PI.php?MfcISAPICommand=3DSignInFPP=20
Press RETURN for more...
```

- Obviously, <http://ebaserv-cgi-update-account.com/> is the phishvertised link that we'll want to pursue – it is a classic example of a underlying-link-not-agreeing-with-what-user-normally-sees-for-link-text vector.

Hmm... That Domain "Doesn't Exist..."

```
% date
Sun Apr 24 07:49:21 PDT 2005
% whois ebaserv-cgi-update-account.com
[ querying whois.internic.net for ebaserv-cgi-update-account.com ]

Whois Server Version 1.3

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

No match for "EBASERV-CGI-UPDATE-ACCOUNT.COM".

>>> Last update of whois database: Sat, 23 Apr 2005 19:11:12 EDT <<<
```

- One of the phishers favorite new phishing tricks is to register a new domain name and then IMMEDIATELY begin using it, "making hay while the sun shines" prior to the time the domain shows up in the whois database. (Once the domain shows up in whois, the likelihood that trademark infringing names will be noticed and potentially contested increases dramatically.)

But It Does Exist, and It Resolves Just Fine

```
% nslookup
> ebaserv-cgi-update-account.com
Server:          128.223.32.35
Address:         128.223.32.35#53

Non-authoritative answer:
Name:   ebaserv-cgi-update-account.com
Address: 65.54.132.254
> 65.54.132.254
Server:          128.223.32.35
Address:         128.223.32.35#53

Non-authoritative answer:
254.132.54.65.in-addr.arpa      name = yourpersonaladdress.net.

Authoritative answers can be found from:
54.65.in-addr.arpa      nameserver = NS1.MSFT.net.
54.65.in-addr.arpa      nameserver = NS2.MSFT.net.
54.65.in-addr.arpa      nameserver = NS3.MSFT.net.
54.65.in-addr.arpa      nameserver = NS4.MSFT.net.
54.65.in-addr.arpa      nameserver = NS5.MSFT.net.
NS1.MSFT.net      internet address = 207.46.245.230
NS2.MSFT.net      internet address = 64.4.25.30
NS3.MSFT.net      internet address = 213.199.144.151
```

We Can Also Use Curl To Visit That Site

```
% curl "http://ebaserv-cgi-update-account.com/" > temp.txt
% Total      % Received % Xferd  Average Speed   Time    Time     Curr.
100    300      0   300    0      0    2941      0 --:--:--  0:00:00 --:--:-- 82000
% more temp.txt
HTTP/1.1 302 Found
Connection: close
Date: Sun, 24 Apr 2005 15:06:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
P3P:CP="BUS CUR CONo FIN IUDo ONL OUR PHY SAMo TELo"
X-AspNet-Version: 1.1.4322
Location: http://www.bgl24.de/php/%20%20/
Cache-Control: private
Expires: Sat, 01 Jan 2000 08:00:00 GMT
Content-Type: text/html

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href='http://www.bgl24.de/php/%20%20/'>here</a>.</h2>
</body></html>
```

Eventually, We Get To See The Domain Whois...

- The whois data for the phishvertised domain begins...

```
[ querying whois.enom.com for ebaserv-cgi-update-account.com ]  
Registration Service Provided By: Microsoft  
Contact: personal_address@css.one.microsoft.com  
Visit: http://support.msn.com/contactus.aspx?pk=PersonalAddress  
  
Domain name: ebaserv-cgi-update-account.com  
  
Registrant Contact:  
  Barbara Reiter  
  Barbara Reiter <tofey@ebaserv-cgi-update-account.com>  
  +1.906283393452  
  Fax: none  
  P.O. Box 87  
  Gulliver, MI 49840  
  US  
  
Administrative Contact:  
  Barbara Reiter  
  Barbara Reiter <tofey@ebaserv-cgi-update-account.com>  
  +1.906283393452  
  Fax: none  
  P.O. Box 87  
  Gulliver, MI 49840  
  US
```

- I would be exceedingly surprised if that information proves to be in any way shape or form "valid" and associated with the person truly controlling that domain. That page is just a redirector, anyhow...

Let's Look At The Real Site...

```
% curl "http://www.bgl24.de/php/%20%20/" > temp2.txt
% Total    % Received % Xferd  Average Speed   Time    Time     Curr.
100 11959  100 11959    0     0  16655      0  0:00:00  0:00:00  0:00:00 30055
% more temp2.txt
HTTP/1.1 200 OK
Date: Sun, 24 Apr 2005 15:11:57 GMT
Server: Apache/1.3.27 (Linux/SuSE) PHP/4.3.1 mod_ssl/2.8.12 OpenSSL/0.9.6i
Last-Modified: Sun, 24 Apr 2005 15:11:57 GMT
ETag: W/"5baab-2eb7-4da8a0f0"
Accept-Ranges: bytes
Content-Length: 11959
Content-Type: text/html

<html>
<head>
<!--eBay U3- msxml 4.0 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-->
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1"><!--srcI
d: SignIn-->
<title>Sign In</title></head>
<body bgcolor="#ffffff">

<SCRIPT LANGUAGE="JavaScript">
  <!--
```

```
% whois www.bgl24.de
[ querying whois.denic.de for www.bgl24.de ]
domain:      www.bgl24.de
status:      invalid
```

Rendered, The Phishvertised Page Looks Like:

Sign In - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.bql24.de/php/%20%20/

Go

Sign In [Help](#)

New to eBay? **or** **Already an eBay user?**

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

[Register >](#)

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot your User ID?](#)

Password

[Forgot your password?](#)

[Sign In Securely >](#)

☐ [Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#)

Be sure the Web site address you see above starts with <https://signin.ebay.com/>

You can also register or sign in using the following service:

[About eBay](#) | [Announcements](#) | [Security Center](#) | [Policies](#) | [Site Map](#) | [Help](#)

Copyright © 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

[eBay official time](#)

reviewed by **TRUSTe** site privacy statement

Done Disabled

For Comparison, The Real eBay Sign In Page:

The screenshot shows the eBay Sign In page in a Mozilla Firefox browser window. The browser's address bar is highlighted with a pink box, showing the URL: <https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&ssPageName=h:h:sin:US>. The page features the eBay logo at the top left. Below it, the "Sign In" header is followed by two tabs: "New to eBay?" and "Already an eBay user?". The "New to eBay?" tab is selected, displaying instructions on how to register and a "Register >" button. The "Already an eBay user?" tab is also visible, showing fields for "eBay User ID" and "Password", each with a "Forgot" link. Below these fields is a "Sign In Securely >" button and a checkbox for "Keep me signed in on this computer unless I sign out.". A "Account protection tips" section with a lightbulb icon advises users to ensure the website address starts with <https://signin.ebay.com/>. At the bottom, there are links for "About eBay", "Announcements", "Security Center", "Policies", "Site Map", and "Help". A copyright notice for 1995-2005 eBay Inc. is present, along with a "Trust.e" logo and a "Disabled" status indicator in the bottom right corner.

Sign In - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&ssPageName=h:h:sin:US

Go

ebay

Sign In [Help](#)

New to eBay? or Already an eBay user?

If you want to sign in, you'll need to register first.

Registration is fast and free.

Register >

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot](#) your User ID?

Password

[Forgot](#) your password?

Sign In Securely >

☐ [Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#)

Be sure the Web site address you see above starts with <https://signin.ebay.com/>

Microsoft Passport users [click here](#).

[About eBay](#) | [Announcements](#) | [Security Center](#) | [Policies](#) | [Site Map](#) | [Help](#)

Copyright © 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

[eBay official time](#)

Find: Find Next Find Previous Highlight Match case

Done

signin.ebay.com Disabled

TRUST.e
site privacy statement

What Do We Know About www.bgl24.de ?

- www.bgl24.de (that's an ell, not a one, after the bg) turns out to resolve to 145.253.231.16.... Hmm, now doesn't THAT look familiar. Ah! That's because it is yet another host in the now-familiar 145.253.231.0/24 netblock.
- If you look at the URL to which you get redirected, it includes to hex-encoded spaces (%20's) as part of the path. That sort of trick is symptomatic of someone who's attempting to hide a directory from casual discovery rather than the sort of name that someone would normally use on a system they directly administered.
- The SIRCON-NET host not only sourced the phishing message, they're also hosting the phishvertised site. Dealing with that site now becomes more important... and in fact, after contacting German authorities, the site was torn down. Example endeth.

Thanks for the chance to talk today!

- Are there any questions?