Internet Name and Number Resources, Cyber Crime, and Your Company: Some Technical Approaches

Coalition Against Domain Name Abuse (CADNA)
June 2nd, San Francisco, California

Joe St Sauver, Ph.D.
(joe@uoregon.edu or joe@internet2.edu)

http://www.uoregon.edu/~joe/cadna/

Introduction

- I'd like to begin by thanking Josh Bourne and everyone at CADNA for the invitation to participate today, and Wells Fargo for providing such a great facility for this meeting.
- Today's panel is going to look at cyber crime issues associated with names and numbers from three different perspectives: an end-user/consumer perspective, a technical perspective, and a policy-oriented perspective.
- I'll be briefly addressing the technical perspective.
- Given our limited time -- and the desire to leave some time for Q&A -- we won't be able to cover all the potentially relevant topics today. I've tried to just pick a few topics that I think are particularly relevant/urgent for this audience, and then provide some pointers to more in depth information for those who want to dig in further.

My Background And A Disclaimer

- I work as Internet2's nationwide Security Program Manager under contract through University of Oregon Information Services. [See www.internet2.edu and www.uoregon.edu for more on those organizations]
- I'm also active with a variety of community security activities, including serving as one of half a dozen senior technical advisors for the Messaging Anti-Abuse Working Group. MAAWG is the international anti-spam forum representing almost one billion mailboxes from some of the largest ISPs worldwide as well as responsible senders and vendors servicing that market [see www.maawg.org]
- All that said, however, my remarks today represent solely my own opinions, and do not necessarily represent the opinions of any other organization or entity.

What We'll Quickly Cover Today

- Three urgent topics focused on your own company's networks and systems:
  - -- IPv4 Address Exhaustion (and IPv6 Adoption)
  - -- The Domain Name System (DNS) and DNSSEC
  - -- Your Brand, Spoofed Email, and SPF
- Three topics focused on external networks and systems:
  - -- The Struggle Has Shifted from Email to the Web
  - -- Using One Problematic Domain to Identify Clusters of Problematic Domains
  - -- WDPRS
- One "advanced" "extra credit" topic (if we have time):
  - -- ASNs and Routeviews

(1) IPv4 Address Exhaustion

- There is a finite pool of available IPv4 addresses, and we're close to running out of them.
- Based on the best available forecasts [see note 1], the last IPv4 blocks will be allocated by the Internet Assigned Numbers Authority to the RIRs on **30-Jul-2011**.
- The regional internet registries (RIRs), such as ARIN, RIPE, APNIC, LACNIC and AFRINIC will exhaust the address space they've received from IANA less than a year later, around **13-Mar-2012**.
- These best estimates are based on current trends, but actual exhaustion might accelerate (or might slow down) depending on what the community does (but probably not by much). **As of today, there's one year, 9 months and 11 days until 13-Mar-2012. That's not much time.**

Being Very Candid About This…

- **If you're planning to do <u>any</u> new projects that will legitimately require additional IPv4 address space, you should request the space you know you'll need <u>now</u>.** Do NOT wait to do so. If you wait even a year or two, you may not be able to get the additional IPv4 address space your company needs at that later time.

- Concurrently, **your IT staff should be hard at work to make sure that your network connectivity and your servers and workstations have been upgraded to support both IPv4 and IPv6 simultaneously.**

- You might well ask, "But Joe, what does this all have to do with cyber crime and brand protection?"

IPv4, IPv6 and Cyber Crime

- As IPv4 exhaustion occurs, there will be increased pressure for miscreants to obtain IPv4 address space any way they can, including by temporarily hijacking chunks of your IPv4 space. [see Note 2] **You should be protecting your Internet number assets the same way you monitor and defend your Internet names.**
- IPv6 deployment will also require careful consideration of potential security issues. For example, are your network firewalls and intrusion detection systems IPv6 aware? Do your sys admins, your network engineers and your security team "get" IPv6? If you're monitoring Internet sites for infringing content and some sites are IPv6-only, can you even **access** them? **Do you know how to investigate abusive IPv6-only sites?** [see Note 3]

MANY Companies Are NOT Ready for IPv4 Depletion and Imminent IPv6 Rollout

- If you're like most people, you may assume that your company must be technically ready for the impending IPv4 depletion and imminent IPv6 rollout.
- Trust me, you're probably not. Want to find out? Check some very basic status items for your domain at www.mrp.net/cgi-bin/ipv6-status.cgi

IPv6 Status Results

Domain Name	cadna.org	
HTTP	FAIL	No service could be found via IPv6
SMTP	FAIL	No service could be found via IPv6
DNS	0/0/5	No DNS service could be found via IPv6
NTP	FAIL	No service could be found via IPv6
XMPP	FAIL	No service could be found via IPv6

(2) The Domain Name System and DNSSEC

- Virtually ALL Internet applications are built on top of the Domain Name System (DNS), and will only work if DNS is functioning correctly.
- **If a cyber criminal can manipulate the DNS to return incorrect results for your domain, the criminal can send your customers to any arbitrary destination of their choice, including look-alike phishing sites, or sites that may drop viruses or other malware on the victim's PC.**
- One way this DNS misdirection can be done is with "DNS cache poisoning." DNS cache poisoning attacks aren't just theoretical, they've been seen in the wild. [see note 4]
- **DNS can be secured against cache poisoning with DNSSEC.** Domain owners need to sign their zones with DNSSEC, and resolvers need to be set to check those sigs.

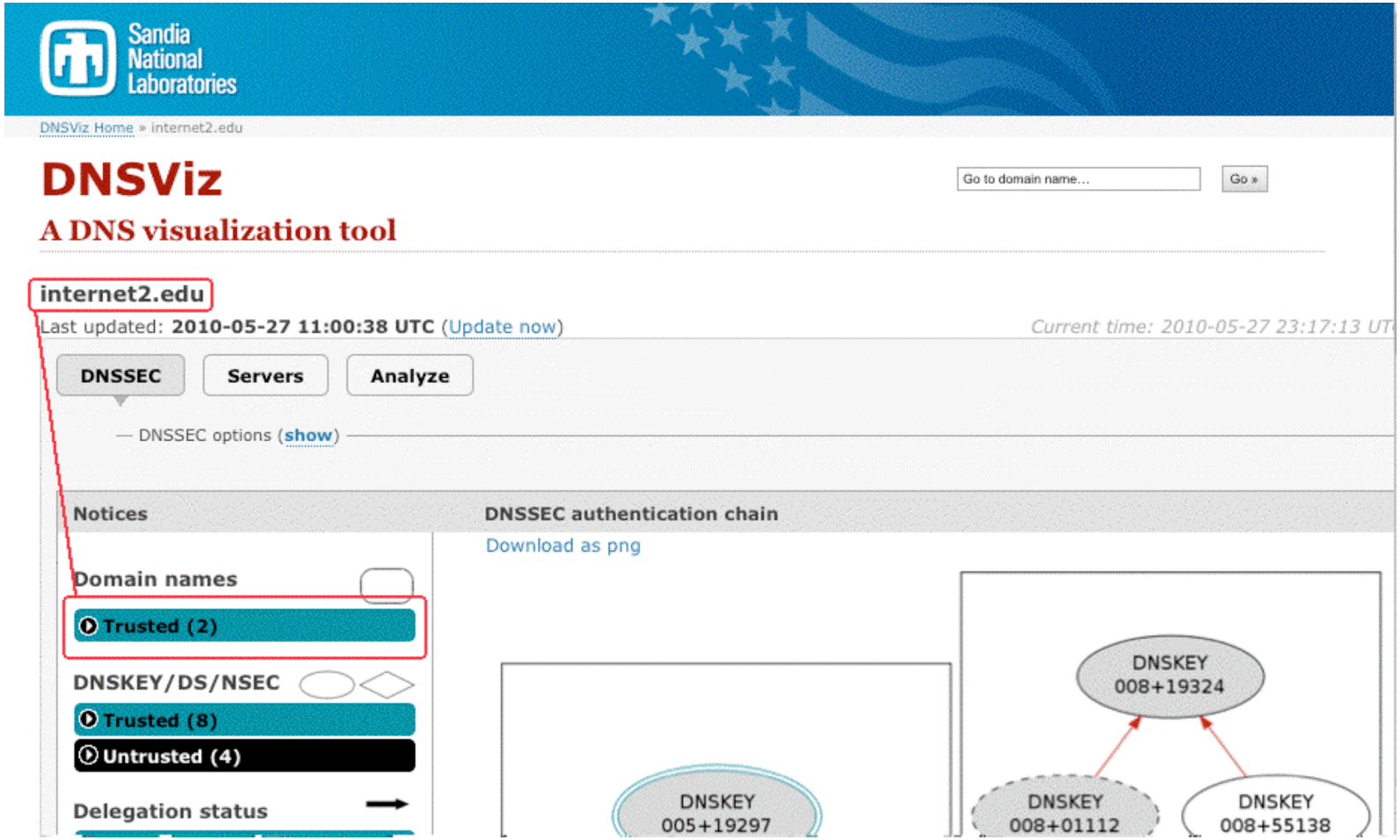
DNSSEC Trust Anchors

- Just as is the case for SSL certs, DNSSEC needs a "trust anchor." When dealing with SSL certs, you rely on a set of trusted "root certs" to act as trust anchors. For SSL, those root certs are built right into users' web browsers.
- DNSSEC had a slightly different design. DNSSEC was premised on the idea that the DNS root (".") would be signed, after which the root's signature could be used to verify the signatures for the TLDs (com, net, etc.), which in turn be used to verify the 2nd level domains, etc.
- **The root will be signed on July 15th, 2010.** [see note 5] You don't need to wait til then, however. Many TLDs (including dot org) and some 2nd level domains are already signing their zones and providing stand alone trust anchors through IANA or through the use of DLV.

Are You DNSSEC Signing Your Domains?

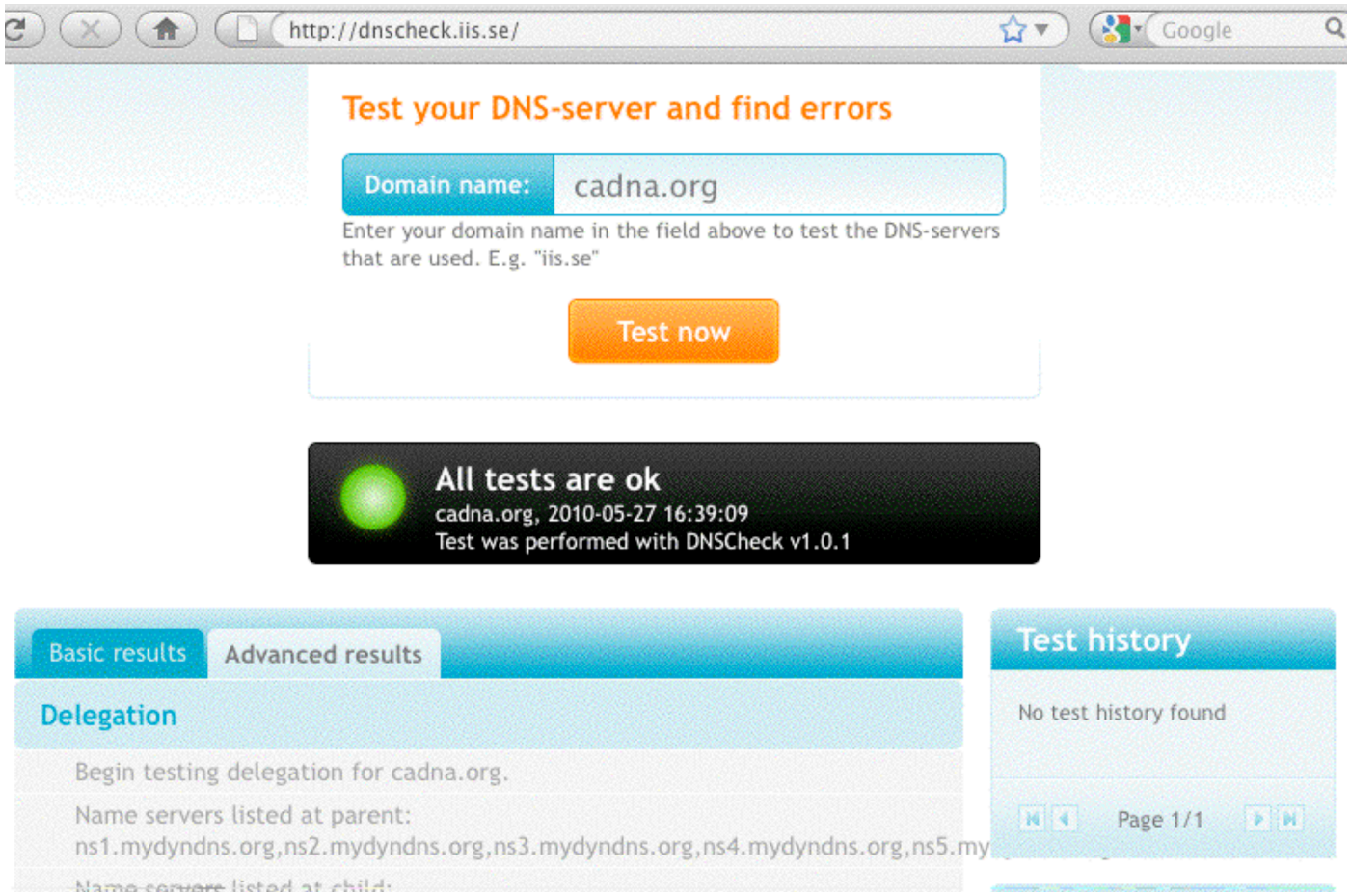
- Some sites (particularly in dot gov and in some ccTLDs) are, but you're not, even though you should be. You can check this online using the web site dnsviz.net , or by checking UCLA's SecSpider (see secspider.cs.ucla.edu)
- Of course, remember that **two** things need to happen for DNSSEC to help with cache poisoning and other attacks: 1) sites need to sign their own domains, and 2) sites, such as companies and ISPs running recursive DNS resolvers, need to be configured to check those DNSSEC signatures.
- In case you worry that no one will bother to check your DNSSEC signatures, one of the largest consumer ISPs in the US, Comcast, is currently engaged in DNSSEC trials and will be implementing DNSSEC validation for all its customers by the end of 2011. [see Note 6]

Sample dnsviz.net Report for a Signed Domain



You should also check your DNS setup for general issues… an example of one tool I like for this is on the next slide.

Any Other DNS Problems? Ask dnscheck.iis.se



Your company's DNS administrator may also want to try the port test and reply size testers from www.dns-oarc.net

(3) Your Brand, Spoofed Email, and SPF

- Email is a critical Internet application, but historically email has been quite vulnerable to spoofing.
- For example, traditionally a person could sit at a cybercafe in Eastern Europe or South America and successfully send emails purporting to be from a major American bank because there was no way for companies to say, "Hey! Real email from my company will only come from the following source systems; discard email claiming to be 'from me' that's coming from anywhere else..."
- Sender Policy Framework (SPF) [see note 7] fixes this issue (at least where SPF has been deployed). If your company has published an SPF record, and if ISPs have configured their mail servers to check SPF records, only email sent from the systems you okay will be acceptable.

Some Companies Which Have Deployed SPF…

- admworld.com
- amazon.com
- americanexpress.com
- apple.com
- bankofamerica.com
- bbandt.com
- bestbuy.com
- boeing.com
- cat.com
- cdw.com
- chase.com
- chevron.com
- cisco.com
- costco.com
- citibank.com
- dell.com
- ebay.com
- exxonmobil.com
- google.com
- gs.com
- homedepot.com
- ibm.com
- jpmorgan.com
- key.com
- kroger.com
- mastercard.com
- medco.com
- microsoft.com
- morganstanley.com
- officedepot.com
- officemax.com
- pfizer.com
- safeway.com
- staples.com
- statefarm.com
- sunocoinc.com
- target.com
- usbank.com
- usps.com
- valero.com
- verizon.com
- visa.com
- wachovia.com
- walmart.com
- wf.com

Has *Your* Company Deployed SPF?

- To see if your company has deployed SPF, use dig to check for a txt record associated with your company's domain name. The SPF record (for Wells Fargo) is typical:

  % dig -t txt wf.com +short
  "v=spf1 mx mx:dxexch.wf.com mx:dxout.wf.com
  mx:omail.spf.wachovia.com ~all"

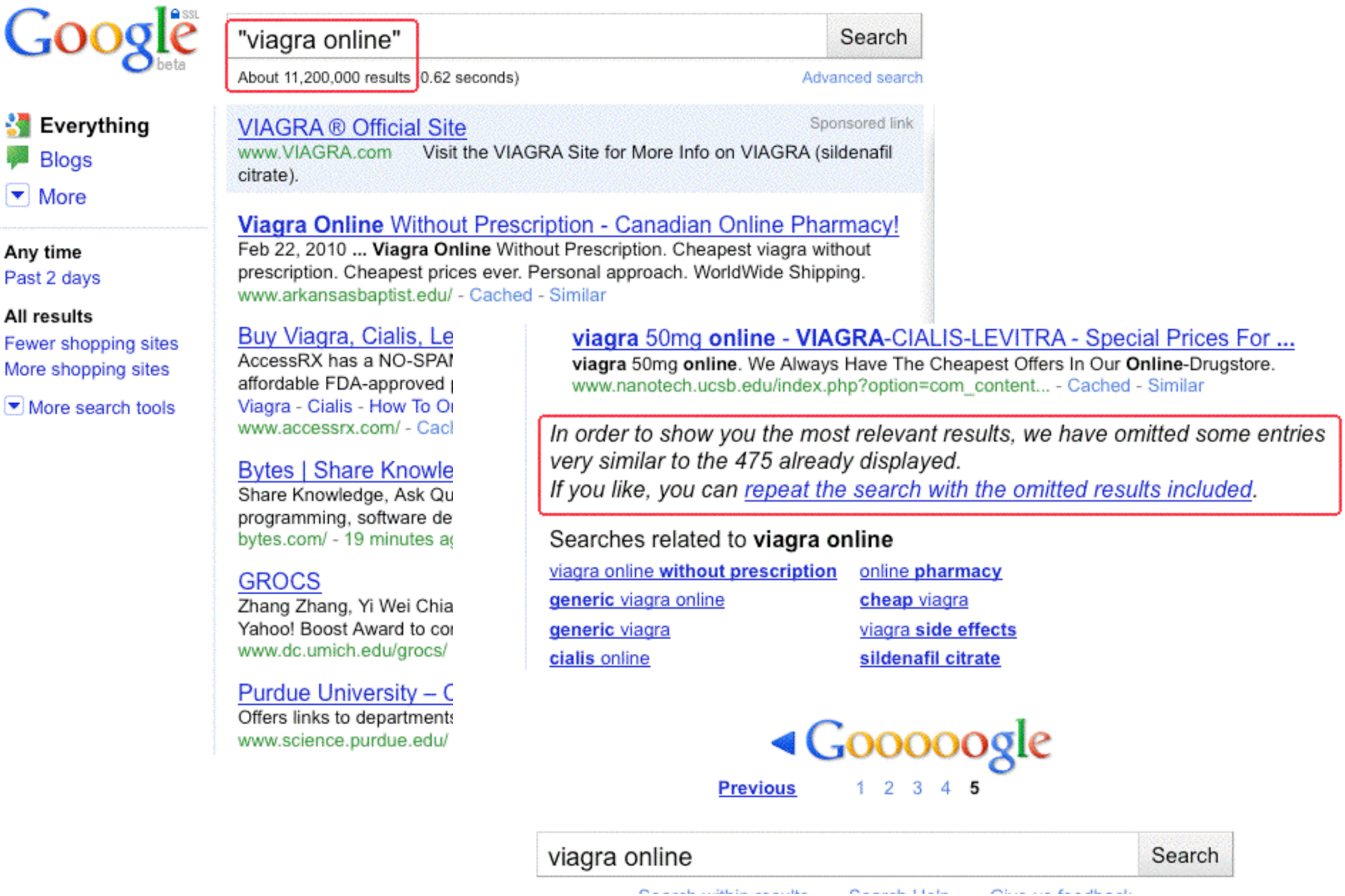
  That record says, "Only accept mail from the currently defined Wells Fargo mail exchanger, or from the following three additional mail servers…

- Don't have access to dig? Try www.digwebinterface.com

(4) The Struggle Has Shifted from Email to the Web

- Improvements in email spam filtering have caused cyber criminals to shift their focus away from email to the web.
- Google (and to a lesser extent, Yahoo and Bing) play a crucial role in making web content visible. As of April 2010, ComScore reports the market share for those three search engines as 64.4%, 17.7%, and 11.8% (total: 93.3%) with no other search engine having even a 5% market share. [See note 8] Those three search engines thus serve as a crucial potential choke point for brand protection.
- "But Joe! Cleaning up the search engines is a sysyphean task! Our marks return millions of infringing pages!"
- **Key point 1:** search engines will only show folks a **fairly easily managed** maximum of 1,000 results per search (and often far less than even that!), and asking to see more results will NOT result in you being shown more results!

Try Googling for "Viagra Online"



You May Have Noticed...

- Many of the results you were shown in that default search were for dot edu pages. For better or worse, many search engines trust (and prioritize) dot edu pages.
- Looking at the pages/sites found, I believe that the servers at those sites have likely been victimized by cyber intruders, either spamming intentionally writable pages (such as blogs, wikis or guestbooks), or in the case of things like institutional home pages, hacking/cracking the content of servers with vulnerable software installed (check the page source of the cached versions of those pages to see). If told about their problem, those sites will remove the problematic content and secure their systems.
- **Key point #2: Are <u>you</u> telling sites about the problems you're seeing when you see them?**

(5) Identifying Clusters of Problematic Domains

- Having identified a dedicated problematic domain (rather than a hacked/cracked page on a legitimate server) you may sometimes wonder, "Are there other similar domains which I should *also* be paying attention to?"
- There are many strategies for identifying domain clusters, but some of attributes you may want to examine include:
  - -- the IP address of the initial problematic domain: are related problematic domains sharing a common IP?
  - -- the name servers of the initial problematic domain: are related problematic domains all using the same set of name servers?
  - -- the IP addrs of the problematic domain's name's name servers (sometimes domains may have unique name servers, but all those NS's may be on a shared IP)

Passive DNS

- Passive DNS is a powerful tool for digging out those sort of inter-domain relationships.
- For example, assume you're interested in "replica watch" web sites.
- Using Google (or another search engine) and searching for replica rolex, you identify www.replicas99.com as a site of interest. Using dig, you determine that www.replicas99.com is hosted on 66.79.167.158.
- Are there other domains of interest also hosted on that same IP address? You can use passive DNS to find out.
- Passive DNS synthesizes (and makes searchable) observed relationships between domains, IPs, and nameservers. **When you find an interesting domain, IP or nameserver, use that starting point to track down related resources.**

Some Domains Sharing The Same IP Address

- **One passive DNS site is www.bfk.de/bfk_dnslogger.html**
  Checking that site for 66.79.167.158 we see:

  -- www.replicas99.com
  -- www.solid925silver.com
  -- www.lifetimereplicas.com
  -- www.mymodelwatches.com
  -- www.tiffanysets.com
  -- www.replicawatchesreviews.com

  While I wouldn't jump to any conclusions based solely on the appearance of domain names you may see, if you were interested in "replica" watches, you might be inclined to at least give some of those domains a closer look.

(6) gTLD Domains With Bad Whois Data

- Having found a problematic gTLD domain, such as perhaps a domain using your company's trademark in an infringing way, or domain that's being used to advertise unauthorized "replica" versions of trademarked products, what can you do to mitigate that abuse?
- Obviously you can employ a variety of traditional administrative or civil remedies to correct that problem (such as the Uniform Domain Name Dispute Resolution Policy (UDRP)); you should **also** check to see if all parts of the domain's whois point of contact data are valid (www.usps.gov/zip4 may be helpful for US addresses)
- **If you find whois data that is inaccurate, in addition to any other remediation strategy you pursue, you may also want to report that inaccuracy via wdprs.internic.net**

WDPRS Can Result In Domains Getting Held

- Based on my experience in filing WDPRS reports, WDPRS reports can and do result in reported domains getting put into ClientHold status, and the effort required to file a WDPRS report via the online form is pretty minimal.
- Downsides:
  - -- WDPRS doesn't work for ccTLD domains (which is one reason, along with a lack of public access to ccTLD zone files, why miscreants have become so fond of ccTLD domains such as dot cn and now dot ru)
  - -- the WDPRS process isn't instantaneous, but the process does grind along
  - -- domains registered with privacy/proxy registration services typically do NOT have whois data that is (technically speaking) "invalid" (even if it is useless)

Example Domain Held As A Result of WDPRS

- DomainName : discplane.com

  RSP: China Springboard Inc.
  URL: http://www.namerich.cn

  Status: clientUpdateProhibited
  Status: clientTransferProhibited
  Status: clientHold
  Status: clientDeleteProhibited
  Creation Date: 2010-04-10
  Expiration Date: 2011-04-10
  Last Update Date: 2010-04-20

  [remainder snipped]

(7) If We Have Time: Autonomous System Numbers

- Unless you're a network engineer, you may never have heard of Autonomous System Numbers (or "ASNs").
- An ASN is a number assigned to a group of network addresses, managed by a particular network operator, which share a common routing policy. Most ISPs, large corporations, and university networks have an ASN. For example, Google is AS15169, Sprint is AS1239, Intel is AS4983, Berkeley is AS25, UOregon is AS3582, and so on.
- While ASNs are primarily used for wide area routing, ASNs are also a useful way to aggregate and sort IP addresses into useful chunks, or to find related netblocks.
- ASNs also serve as the foundation for identifying yet another responsible party for abuse reporting purposes: "If you route it and it's abused, it's <u>your</u> problem."

Mapping Domains to IP Addresses to ASNs

- Assume you want to know the AS number associated with the University of Oregon's web server, www.uoregon.edu.
- First use dig to find www.uoregon.edu's IP address:
  % dig www.uoregon.edu +short
  128.223.142.89
- Now ask the Oregon Routeviews program to give you the ASN associated with that IP (note we reverse the IP):

  % dig -t txt 89.142.223.128.asn.routeviews.org +short
  "3582" "128.223.0.0" "16"

  Interpreting that result, 128.223.142.89 is:
  -- in AS3582
  -- and is part of the netblock 128.223.0.0/16

Mapping Lots of IPs to ASNs

- Sometimes you may have a long list of IP addresses that you'd like to map to ASNs. While you could do these one at a time using the process described on the preceding slides, you may find it easier to use the Team Cymru IP to ASN mapping service. [see note 9 for information on that service]

Finding Point of Contact Data for ASNs

- Unlike IP addresses or domains, there are a relatively small number of ASNs in use, so it doesn't take very long to build a local directory mapping the AS numbers you see to appropriate abuse reporting points of contact.
- To look up the point of contact information for an ASN, use whois (just as you would for an IP address or domain):

  % whois -h whois.arin.net AS3582

  OrgName: University of Oregon
  OrgID: UNIVER-193
  Address: UO Information Services
  [continues]
- ARIN, RIPE, APNIC, LACNIC, and AFRINIC offer web based whois if you don't have a command line whois client. For example, try ws.arin.net/whois to lookup AS3582

Finding The Netblocks Announced by An ASN

- Sometimes you may find what appears to be a malicious ASN, and you'd like to identify all the netblocks announced by that ASN.
- Routeviews can help with that process, too. For example, to see all the netblocks announced by the University of Oregon (AS3582), you'd say:
  % telnet route-views.oregon-ix.net
  Username: rviews
  route-views> show ip bgp regex _3582$
  [hit a space to page down, and enter quit to exit]
- If that output is too painful, you may find it easier to consult a web-based summary such as:
  www.cidr-report.org/cgi-bin/as-report?as=AS3582
  (obviously you'd replace AS3582 with the AS of interest)

Thanks for The Chance To Talk Today!

- Are there any questions?

  [notes can be found on the next couple of slides]

Notes

1: "IPv4 Address Report,"
www.potaroo.net/tools/ipv4/index.html

2: "Route Injection and the Backtrackability of Cyber Misbehavior,"
www.uoregon.edu/~joe/fall2006mm/fall2006mm.pdf

3: "IPv6 Training,"
www.uoregon.edu/~joe/ipv6-training/ipv6-training.pdf and

"IPv6 and the Security of Your Networks and Systems,"
www.uoregon.edu/~joe/i2mm-spring2009/
i2mm-spring2009.pdf (URL split due to length)

Notes (2)

4: E.G., "China Netcom DNS cache poisoning," 8/19/2008, securitylabs.websense.com/content/Alerts/3163.aspx

5: "Root DNSSEC," www.root-dnssec.org

6: "DNSSEC," blog.comcast.com/2010/02/dnssec.html

7: "Sender Policy Framework," www.openspf.org

8: "comScore Releases April 2010 U.S. Search Engine Rankings," tinyurl.com/comscore-april-2010

9: www.team-cymru.org/Services/ip-to-asn.html