

Network Protocols

DNS Intel

*slightly modified public version of another talk

What's in a name?

dns-research01.cti.depaul.edu.

Name hierarchy

- Root (.)
- top-level domain (TLD)
 - country-code (ccTLD), generic (gTLD), special (e.g. .arpa), sponsored (e.g. .aero) and unsponsored (e.g. .com)
- second-level domain (SLD)
 - Note, some SLDs behave like TLDs (e.g. co.uk.)
- Third-level domain and so on...
- Host name is a domain name used as a host name

Domain name registration

- Registrant
 - Authorized user/org with rights to domain name
- Registrar
 - An agent through which you register a name
- Registry
 - Central directory for names in a zone

Typical registration process

- You are interested in tdc375.com
- Visit GoJTK, maybe an accredited .com registrar?
- Put down some \$\$
- Submit various contact info (address, email, phone)
 - Maybe sign up for the privacy service
- Configure name servers for the zone if necessary
- GoJTK sends updates to the registry
 - Both the zone file and whois directory

You query for these names, which one(s) is(are) bad?

*AKA You Can't Judge a Book by Its Cover

- www.depaul.edu
- img179.imageshack.us
- irc.ccpower.net
- tinyurl.com
- [inf-team.by .ru](http://inf-team.by.ru)
- h4x0r.com

Maybe not what you expected

- <http://www.depaul.edu/~jkristof/tmp/pwnd.html>
- <http://img179.imageshack.us/img179/484/rbcacclu1.gif>
- irc.ccpower.net – enough said?
- <http://tinyurl.com/nlepmm> – RFI sploit
- <http://inf-team.by.ru> – BEWARE, javascript-based sploit
- <http://www.h4x0r.com> – the most benign one yet

Whois data questions to ask

- Who is the registrar?
- Address look valid?
- Phone number valid?
- Private registration?
- Interesting name servers?
- How long has it been registered?
- When does it expire?
- Has it been updated recently?

Some interesting response data

- Address of server providing the answer
- The actual answer (RDATA) is very relevant
- The TTL can be relevant
- Sometimes DNS flags are interesting (e.g. RA)
- What can be more interesting than answer data?
 - The history of the name and answer
 - http://www.bfk.de/bfk_dnslogger.html
- Actually, end host queries are real interesting too

DNS Blackhole automation

- Find yourself some DNS blacklists
 - e.g. malwaredomains.com
- Run a local resolver or integrate with `hosts.txt`
 - FYI... running a local resolver is worthwhile
- Answer the “bad” name queries however you want

This is ultimately what you want

```
$ dig @ns1.example.edu 0.0x03x.net
; <<>> DiG 9.3.4 <<>> @ns1.example.edu 00.devoid.us
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12345
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0

;; QUESTION SECTION:
;00.devoid.us.                IN      A

;; ANSWER SECTION:
00.devoid.us.                604800  IN      A      192.0.2.1

;; AUTHORITY SECTION:
00.devoid.us.                604800  IN      NS     localhost.
```

1. Create sink zone

- Easiest to sink all names to one spot
- Generic `/var/named/badnames.zone`, maybe like this:

```
$TTL 1D
@ IN SOA localhost. root ( 2009102800 3H 30M 1W 1D )

    IN NS      localhost.
    IN A       127.0.0.1
    IN AAAA    ::1
    IN TXT     "Inquiries to security@localhost."
```

2. Prepare BIND named config

- Really just need one line in your cache server config:
- A script will periodically update dnsnames.conf
- Put this in master named.conf:

```
include "/var/named/badnames.conf";
```

3. Parse and build config

- Parse source “bad” names list into zone file format
- In a regularly scheduled crontab do something like this:

```
fetch_names
```

```
list2bind badnames.list > /var/named/badnames.conf
```

```
rndc reconfig
```

- Voila, bad names now sunk

DNS Signal Intel

- Since 1.6.7, eggdrop by default has an hourly “beacon”
- An A RR query is made for: uptime.eggheads.org
- This is used to report uptime statistics for the bot
- Do you have any unwanted eggdrop bots on your net?

Prevent MITM attacks

- You may have heard about wpad?
- If not, visit wpad.com and do some net searches
- Are you also aware of isatap?
 - This is a v4 to v6 transition mechanism using tunnels
 - Clients might get a tunnel config from an unfriendly
- Configure wpad and isatap zones in your caching servers
- Get clients to disable use of these names this if possible

Quick stats

- ~3600 wpad queries/month in depaul.edu
 - ~350 unique sources, ~98% are external queriers
- ~18,000 isatap queries/month in depaul.edu
 - ~450 unique sources, > 99% external queriers
- ~300,000/month isatap queries in 9 odd TLDs
 - This is not counting com/net/org
 - ~8000 unique sources
- Note: sources are almost always recursive servers
- Note: wpad TTL = 1 day, isatap NXDOMAIN, ~5 minutes

Ob phish/trademark detector?

- Build a list of known names to monitor
 - e.g. paypal.com, banks, yourorgname
 - Other things too, but maybe too political for our tastes today
- Alert on names that have a low hamming distances
 - e.g. bankofamerita has a hd of 1 with bankofamerica
- Here is the perlmonks code that does it:

```
sub hd { return ($_[0] ^ $_[1]) =~ tr/\001-\255//; }
```

Ob thoughts

- Did you know spam hosts tend to do a lot of MX queries?
- Did you know IRCds tend to do a lot of PTR queries?
- Do you have any port 53 traffic to/from ASN 27595? (**historic**)
- Spamhaus answers maybe good feedback for other stuff?

Ob links

- <http://public.oarci.net/oarc/tools>
- <http://dns.measurement-factory.com/tools/index.html>