Bizarre and unusual uses of DNS

Rule 53: If you can think of it, someone's done it in the DNS

Peter Lowe
Principal Security Researcher | DNSFilter
whoami

- Peter Lowe
- Principal Security Researcher at DNSFilter
- We provide protective DNS services for companies
- So I spend a lot of time thinking about DNS and malware techniques
- Worked in DNS security for around 3 years now, 27 years in tech
- You *might* know me from my blocklist for ads and trackers at pgl.yoyo.org
- Ask me about DNS Abuse
- Terrible, absolutely terrible, at slides

- https://twitter.com/pgl
Potential Titles

- How I Learned To Stop Worrying And Love DNS
- The things people do with DNS
- 20 Wacky DNS Tricks - #5 will SHOCK YOU
- DNS Museum*
- Went with something descriptive in the end
What

DNS in 2 minutes

● DNS is an always available, highly resilient, incredibly fast, fundamental part of the internet.

● ... so of course people have done some interesting things with it.

● "Questions" are sent to resolvers, which return "answers" - the records you're looking for. These are normally domains.

● It's often called the "phone book of the internet" - you look up a domain and get records back about it (not just IPs, but TXT records, MX records, etc.)

● This makes it a general records system.
Why

Not my fault

- It's John Todd's fault really
- This became a Twitter thread
- DNS Abuse SIG work - first.org/global/sigs/dns
- Rule 34 implies that thinking of something brings it into existence...
- ... so let's not suggest anything too out there
Caveats

And notes

- Most not around anymore
- Thought I'd have more time for this talk
- Links at the end
- No really, I'm terrible at slides, I hate doing them
Traceroutes

OK, so maybe not 100% DNS…
From Ryan Werber at beagle.net in Feb 11th 2013

Down because of DDoS
IPv6 versions popped up

Gone but not forgotten

Traceroutes

Star Wars
Traceroutes

hand.bb0.nl

Interesting extension using IPv6 - apparently there's more if you increase hops
Traceroutes

Sebastian Haas' "fakert" that creates a TUN device

IP range routed to where the fakert is running

@_sehaas on Twitter
By Ambrose Chua

To the tune of "American Pie"
Traceroutes

bad.horse

From Dr Horrible's Sing-Along

Bonus: cert chain from signed.bad.horse
Traceroutes

bad.horse
Traceroutes

Christmas

Ho

Ho

Ho
Tools and Toys
Tools and Toys

Calculator

Sadly not around anymore

There's a reverse Polish calculator out there as well

```bash
dig @dns.postel.org 2.8.add.calc.postel.org +short 0.10.0.0

dig @dns.postel.org 8.2.sub.calc.postel.org +short 0.6.0.0

dig @dns.postel.org 2.8.mul.calc.postel.org +short 0.16.0.0

dig @dns.postel.org 8.2.div.calc.postel.org +short 0.4.0.0
```
Tools and Toys

"My IP"

```
[pgl-macbook-pro:pgl]~ $ host -t txt o-o.myaddr.l.google.com ns1.google.com
Using domain server:
Name: ns1.google.com
Address: 216.239.32.10#53
Aliases:
o-o.myaddr.l.google.com descriptive text "77.97.197.133"
```

```
[pgl-macbook-pro:pgl]~ $ dig myip.opendns.com @resolver1.opendns.com +short
77.97.197.133
```
Tools and Toys

"My IP"

THE RUMORS ARE TRUE. GOOGLE WILL BE SHUTTING DOWN PLUS—ALONG WITH HANGOUTS, PHOTOS, VOICE, DOCS, DRIVE, MAPS, GMAIL, CHROME, ANDROID, AND SEARCH—TO FOCUS ON OUR CORE PROJECT:

THE 8.8.8.8 DNS SERVER.
Tools and Toys

IP to ASN

```
"15169 | 8.8.8.0/24 | US | arin | 1992-12-01"

[pgl-macbook-pro:pgl]$: dig +short 1.1.1.1.peer.asn.cymru.com TXT
"1103 2914 3257 7195 | 1.1.1.0/24 | AU | apnic | 2011-08-11"

"23969 | 1.0.128.0/17 | TH | apnic | 2011-04-08"
"23969 | 1.0.128.0/18 | TH | apnic | 2011-04-08"
"23969 | 1.0.160.0/18 | TH | apnic | 2011-04-08"
"23969 | 1.0.168.0/24 | TH | apnic | 2011-04-08"
```

From Team Cymru - similar to Whois but faster
Tools and Toys

Postcodes

```bash
[pgl-macbook-pro:pgl]~ $ host -t LOC kt112ra.find.me.uk
kt112ra.find.me.uk location 51 19 42.141 N 0 23 56.076 W 0.00m 0.00m 0.00m 0.00m
```

```bash
[pgl-macbook-pro:pgl]~ $ dig PASSAU.zipde.jpmens.net TXT
;; ;<><> DiO 9.10.6 <<<>> PASSAU.zipde.jpmens.net TXT
;; ; global options: +cmd
;; ; Got answer:
;; ;>>>HEADER<< opcode: QUERY, status: NOERROR, id: 2488
;; ; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; ; OPT PSEUDOSECTION:
;; ; EDNS: version: 0, flags:;; udp: 512
;; ; QUESTION SECTION:
;PASSAU.zipde.jpmens.net. IN TXT
;; ; ANSWER SECTION:
PASSAU.zipde.jpmens.net. 604800 IN TXT "94836"
PASSAU.zipde.jpmens.net. 604800 IN TXT "94834"
PASSAU.zipde.jpmens.net. 604800 IN TXT "94832"
```
Tools and Toys

dns.toys

Currency conversion (forex)

dig 100USD-INR.fx @dns.toys

dig 50CAD-AUD.fx @dns.toys

$Value$FromCurrency-$ToCurrency. Daily rates are from exchangerate.host.

Number to words

dig 987654321.words @dns.toys

Convert numbers to English words.

World time

dig mumbai.time @dns.toys

dig newyork.time @dns.toys

dig paris/fr.time @dns.toys

Pass city names without spaces suffixed with .time optionally.

IP echo

dig ip @dns.toys

Echo your IP address.

Usable CIDR Range

dig 10.0.0.0/24.cldr @dns.toys

dig 2001:db8::/108.cldr @dns.toys

Parse CIDR notation to find out first and last usable IP address in the subnet.

From Kailash Nadh, CTO of Zerodha
From Sebastian Haas:

Mockapetris himself wasn't involved in the geocache. "Mockapetris_1876" is just a hint to DNS and RFC 1876 ;)
The cache is maintained by me.
To solve the complete riddle you have to execute multiple queries (TXT, AAAA, PTR, LOC). You can find the solution in the screenshot.
Tools and Toys

Text adventure

By Craig Mayhew, @craigmayhew

Uses round robin DNS for chance-based actions
Tunneling
Tunneling

General idea

DNS Tunneling works by abusing DNS records to traffic data in and out of a network. In principle, every type of record can be used, but the speed of the connection differs by the amount of data that can be stored in a single record. Below are some obvious ones:

- **TXT records** allow free-form data and can even include spaces. You can as such store information in it encoded with base64, allowing 220 bytes of data per record. TXT records are intended for "generic" use within the DNS framework. Users can place whichever data in it, as long as it meets the protocol requirements: a maximum length of 255 octets according to RFC 1035. In the recent past, TXT records had virtually been deprecated, which would have enabled highly security conscious environments to discard them at the enterprise DNS server. Today however, they have regained use as the carrier of the antispam-related SPF record.
- **CNAME records** allow only the characters A through Z, digits 0-9 and the hyphen. As such you require base32 encoding and are limited to about 110 bytes per record.
- **EDNS0 messages** can be larger than the 512 byte maximum for UDP DNS, and can carry a 1280 byte payload by default. OzyManDNS uses a 768 byte payload for stability.
- **A and MX records** can be used as well, but with more limitations. These cannot store all types of data.

https://www.daemon.be/maarten/dnstunnel.html
Tunneling

Wikipedia

$ host -t txt foo.wp.dg.cx
foo.wp.dg.cx descriptive text "Foo may refer to: Foo, bar, and baz: metasyntactic variables, \"Foo\", as a nonstandard spelling to indicate a nonstandard pronunciation, Foo Fighters, a post-grunge group formed by Dave Grohl, Foo fighters, a World War II term for various UFOs or mysterio\" \"us aerial phenomena seen in the skies over Europe and the Pacific theatre, Foo, also a known surname or last name of a... http://a.vu/w:Foo"

$ dig +short txt '新疆.wp.dg.cx' | perl -pe's/\{\{d\{1,3\}\}/chr $1/eg'
"Xinjiang (Uyghur: , Shinjiang); \; Postal map spelling: Sinkiang) is an autonomous region (Xinjiang Uyghur Autonomous Region) of the People's Republic of China. It is a large, sparsely populated area (spanning over 1.6 million sq. km) which takes up about one "e sixth of the country's territory. Xinjiang borders the Tibet Autonomous Region to the south and Qinghai and Gansu... http://a.vu/w:Xinjiang"

David Leadbetter
Add TXT records to "publish" a post

By Harshad Sharm - trying to "break coder's block"

---

Tunneling

Blogging

- View latest post:
  ```
  $ dig @127.0.0.1 -p 10053 TXT +short rex.latest
  "# Hello"
  "This is a test."
  ```

- See recent posts:
  ```
  $ dig @127.0.0.1 -p 10053 TXT +short rex.index
  "Latest: rex.latest"
  "Recent:"
  "  rex.hello"
  "  rex.trying.something.silly"
  ```

- Read a specific post:
  ```
  $ dig @127.0.0.1 -p 10053 TXT +short rex.trying.something.silly
  "# Woohoo!"
  "This actually works?!"
  ```
Tunneling

IP over DNS

Erik Eckman - @yarrick on GitHub

IPv4 only inside the tunnel, but server can listen on IPv6

Iodine has the atomic number 53

---

Try it out within your own LAN! Follow these simple steps:

- On your server, run: `./iodined -f 10.0.0.1 test.com`. If you already use the `10.0.0.0` network, use another internal net like `172.16.0.0`.
- Enter a password.
- On the client, run: `./iodine -f -r 192.168.0.1 test.com`. Replace `192.168.0.1` with your server’s ip address.
- Enter the same password.
- Now the client has the tunnel ip `10.0.0.2` and the server has `10.0.0.1`.
- Try pinging each other through the tunnel.
- Done! :)

---
Tunneling

HTTP over DNS

Browsertunnel can send arbitrary strings over DNS by encoding the string in a subdomain, which is forwarded to the browsertunnel server when the browser attempts to recursively resolve the domain.

```
gmr02c.16.0.nbswy3dpea5cs000.tunnel.example.com
```

ID  Size  Offset  Base32-encoded fragment(s)  Top  domain

Longer messages that cannot fit in one domain (253 bytes) are automatically split into multiple queries, which are reassembled and decoded by the server.

```
 ya4iie.40.0.orugs4zanf.zsayjanr.tunnel.example.com
 ya4iie.40.18.xw4z3foiqq.2zltonq.tunnel.example.com
 ya4iie.40.35.wozi0.tunnel.example.com
```
Tunneling

VPN over DNS

"Contains ads"
Tunneling

dnscat2

Iagox86 on GitHub, or "Ron"

Doesn't need a domain

Looks exactly like normal DNS traffic

dnscat2> window -i dns1
New window created: dns1
Starting Dnscat2 DNS server on 0.0.0.0:53531
[domains = skullseclabs.org]...

Assuming you have an authoritative DNS server, you can run the client anywhere with the following:
./dnscat2 skullseclabs.org

To talk directly to the server without a domain name, run:
./dnscat2 --dns server=x.x.x.x, port=53531

Of course, you have to figure out <server> yourself! Clients will connect directly on UDP port 53531.

Received: dnscat.9fa8ff1787f26b6d6c716c6376697968657a6d716800 (TXT)
Sending: 9fa8ff1787f26b6d6c716c6376697968657a6d716800
Received: d17cff3e747073776c776d70656b73786f646f616200.skullseclabs.org (MX)
Sending: d17cff3e747073776c776d70656b73786f646f616200.skullseclabs.org
And more
Bigger things

DNS for config

Corey Quinn

Using Route 53 for config management

@quinnypig on Twitter

Episode Summary

Join me as I launch a new series called Whiteboard Confessional that explores how whiteboard architecture diagrams might look pretty but rarely work as designed in production. To kick off the series, we're taking a look at everyone's favorite database, AWS Route 53, while touching upon a number of topics, including what data centers used to look like, the emergence of virtualization and the impact it had, configuration management databases and how they differ from configuration management tools like Chef and Puppet, why using DNS as a configuration management database is inherently an awful idea, how there's always a better solution than whatever you built in your own isolated environment, how just because someone built something doesn't mean they knew what they were doing, and more.

About the Author

Corey is the Chief Cloud Economist at The Duckbill Group, where he specializes in helping companies improve their AWS bills by making them...
Bigger things

Brands

BIMI records

Really just TXT records starting _bimi

https://bimi.agari.com/

With brand indicators, your brand will be integrated into every email.

When customers scan their inboxes, your email will stand out.
"Free, unlimited, unrestricted access to data about every company in the UK*

npm modules, developer docs

Numprotocol.com

NUM technology
Bigger things

Key-value store

Generic service offered to allow people to set and retrieve values

Not sure who's behind this!

DNS Key Value Storage (dnskv.com)

The packet messaging service for true hackers. Simple and free to use.

Too complex? See: simplified tutorial

Structure:

- Suffix all names with this domain
- options.value.key.

Insert:

- value.key.
Bigger things

DNSFS

Ben Cox, benjojo.co.uk
Bigger things

MP3s

One use of DNSFS

---

Ben Cox
@Benjojo12

Replying to @Manawyrm

oh god that actually works. Here is a bash 1 liner:

```
let counter=0; while true; do sleep 1; dig TXT +short $counter.mp3.nodialtone.de @ns1.resellerinterface.de | tr -d ' ' | tr -d '"' | base64 -d; let counter=0; done | vlc
```
Links

https://dnsfilter.com/ - DNSFilter
https://github.com/sehaas/fakert - Sebastian Haas' fakert
https://beaglenetworks.net/post/42707829171/star-wars-traceroute - Star Wars traceroute
https://del.co/wikipedia-dns - Wikipedia over DNS
https://www.youtube.com/watch?v=_y36fG20bA0 - The Day The Router Died
https://www.youtube.com/watch?v=Q03kODVz1Kx - Bad Horse
https://ascinema.org/a/15020 - Christmas traceroute
https://team-cymru.com/community-services/ip-asn-mapping/#dns - IP to ASN mapping
https://www.cambus.net/interesting-dns-hacks/ - few things including the calculator, My IP
https://jpmens.net/2020/10/04/airports-of-the-world/ - Airports
https://github.com/pgl/rule53 - Rule53 list on GitHub
https://twitter.com/pgl/status/140561475500295427 - Twitter thread
Questions?

Principal Museum of DNS Curator
Security Researcher @ DNSFilter

twitter.com/pgl

peter@dnsfilter.com / pgl@yoyo.org