DNS Blocking Revisited…

… because things have changed over the last 13 years.

Overview

- The DNS, the Internet and the world have evolved over 13 years.
- 13 years ago:
  - Occupy Wall Street protests begin in the United States
  - Minecraft was released
  - European sovereign debt crisis
  - Chile's Puyehue volcano erupts
  - India wins the Cricket World Cup
  - Samoa only had 364 days
  - “Somebody That I Used to Know” - Gotye
  - Liechtenstein becomes the 26th member state of the Schengen Area.
- We are seeing a spike in Gvmnt mandated DNS blocking.
  - Probably can’t stop this, but we might be able to minimize the damage.

Overview of what changed…

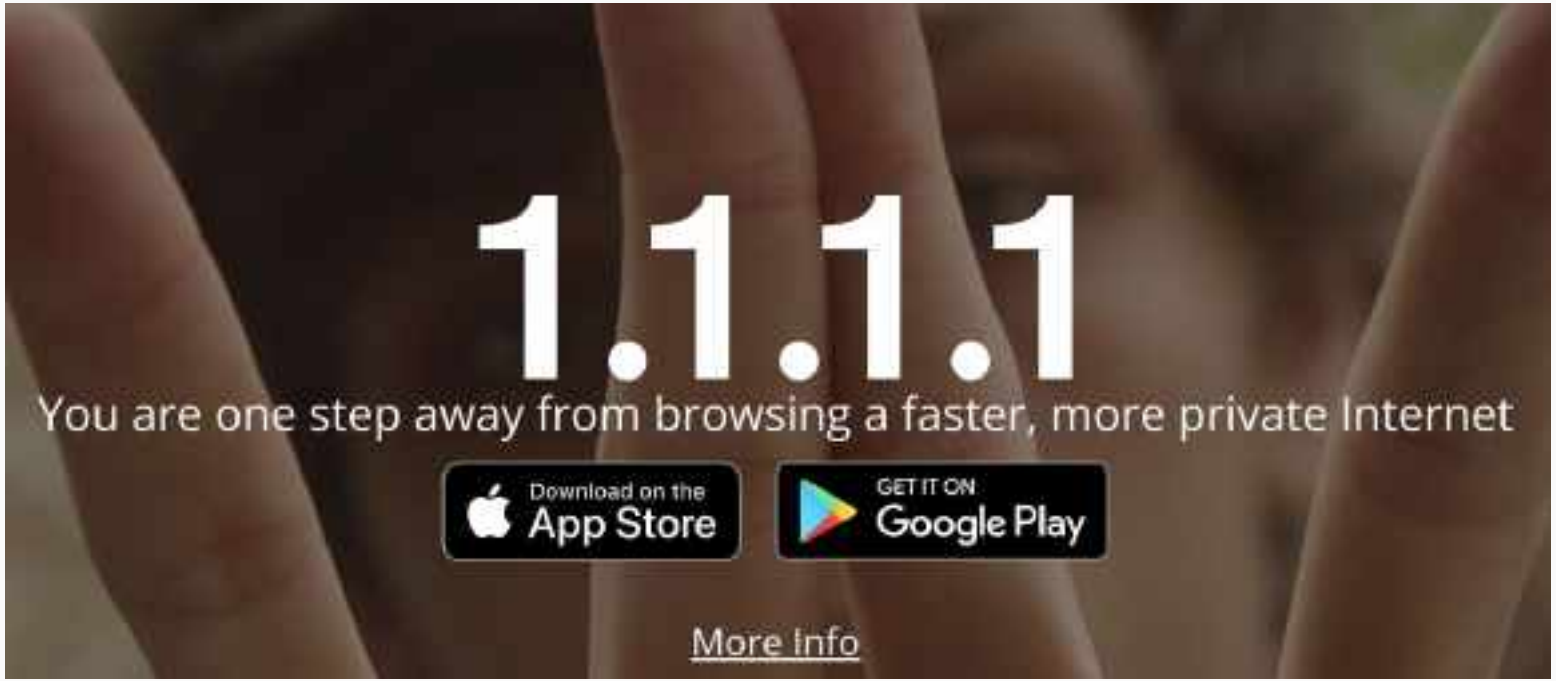
1. VPNs are much more common
2. DoH / DoQ
3. Many more, and much better known Public Resolvers
4. Extended DNS Error
5. Increased deployment of DNSSEC
6. Much simpler to deploy resolvers

1. VPNs are much more common

- Companies like NordVPN, SurfShark, Private Internet Access, etc. sponsor many videos, etc.
  - One click install.
- In addition to tunneling the traffic to endpoints outside the country, they also often include their own resolvers.

  Whenever you connect to any NordVPN server, you automatically connect to NordVPN’s private DNS servers, which prevents DNS leaks during your VPN connection and offers a fast DNS query processing.

1. VPNs are much more common



1. VPNs are much more common

2. DoH / DoQ

- If you can’t see it, you can’t block it…
- DoH encrypts DNS traffic and requires authentication of the server. This mitigates both passive surveillance [RFC7258] and active attacks that attempt to divert DNS traffic to rogue servers … – RFC8484 - DoH

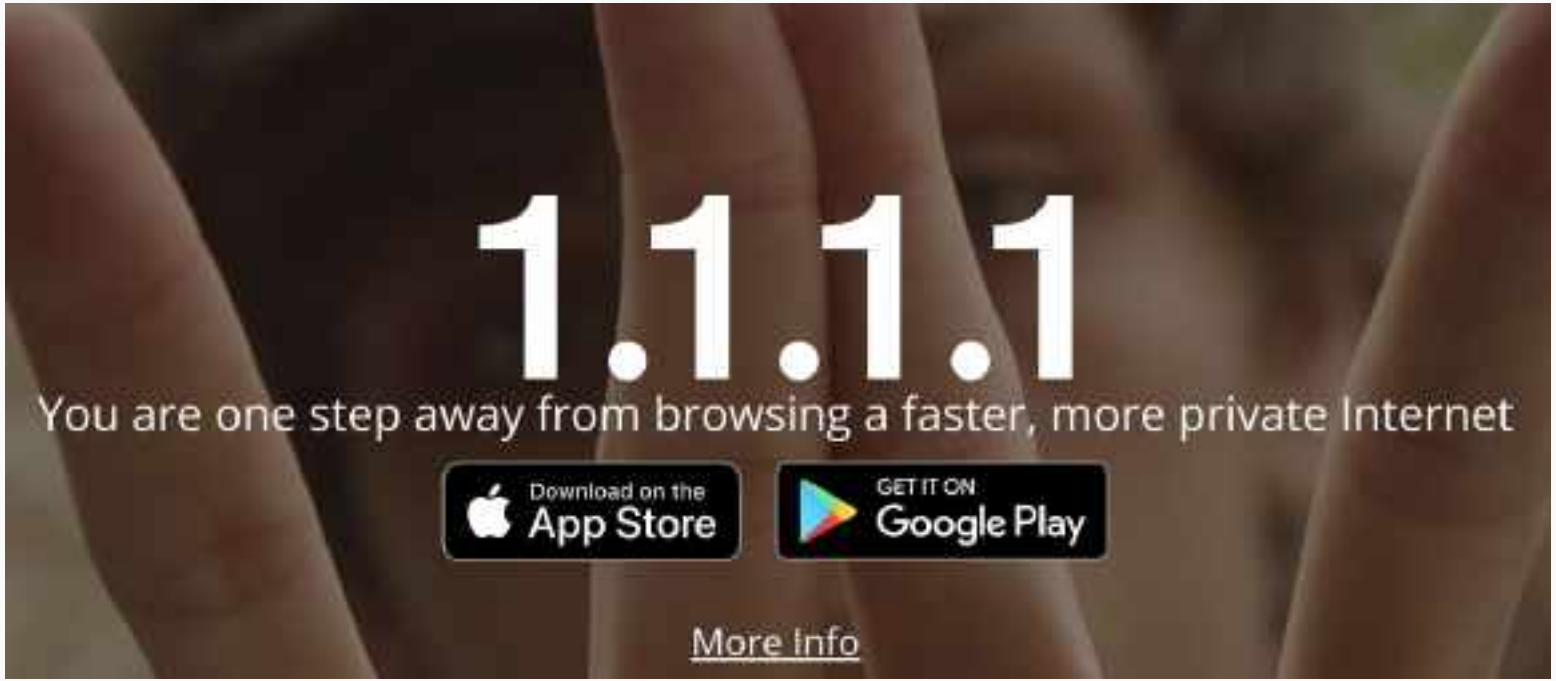
- Encryption provided by TLS eliminates opportunities for eavesdropping and on-path tampering with DNS queries in the network, such as discussed in RFC 7626. –RFC7858 - DoT

3. Many more, and better known Public Resolvers

Notable public DNS service operators [edit]

Provider	Privacy policy	DNS over UDP/TCP (Do53)	DNSSEC	DNS over TLS (DoT)	DNS over HTTPS (DoH)	DNS over QUIC (DoQ)	EDNS Padding	DNSCrypt	Hostname	IPv4 addresses	IPv6 addresses	Filters	Remarks
Cloudflare	Yes[16]	Yes	Yes[17]	Yes[18]	Yes[19]	No[20]	Yes	No	one.one.one.one[21] 1dot1dot1dot1.cloudflare-dns.com	1.1.1.1 1.0.0.1	2606:4700:4700::1111 2606:4700:4700::1001	None	
Cloudflare	Yes[16]	Yes	Yes[17]	Yes[18]	Yes[19]	No[20]	Yes	No	security.cloudflare-dns.com	1.1.1.2 1.0.0.2	2606:4700:4700::1112 2606:4700:4700::1002	Malware, Phishing	
Cloudflare	Yes[16]	Yes	Yes[17]	Yes[18]	Yes[19]	No[20]	Yes	No	family.cloudflare-dns.com	1.1.1.3 1.0.0.3	2606:4700:4700::1113 2606:4700:4700::1003	Malware, Phishing, Adult content	
Google	Yes[22]	Yes	Yes	Yes	Yes[23]	No	Yes	No	dns.google[24]	8.8.8.8 8.8.4.4	2001:4860:4860::8888 2001:4860:4860::8844	None	
Quad9	Yes[25][26]	Yes	Yes[27]	Yes[27]	Yes[28]	No	No	Yes[29]	dns.quad9.net	9.9.9.9 149.112.112.112	2620:fe::fe 2620:fe::9	Phishing, malware, and exploit domains	
Quad9	Yes[25][26]	Yes	No[30]	Yes[27]	Yes[30]	No	No	Yes[29]	dns10.quad9.net	9.9.9.10 149.112.112.10	2620:fe::10 2620:fe::fe:10	None	

3. Many more, and better known Public Resolvers



3. Many more, and better known Public Resolvers

4. Extended DNS Error

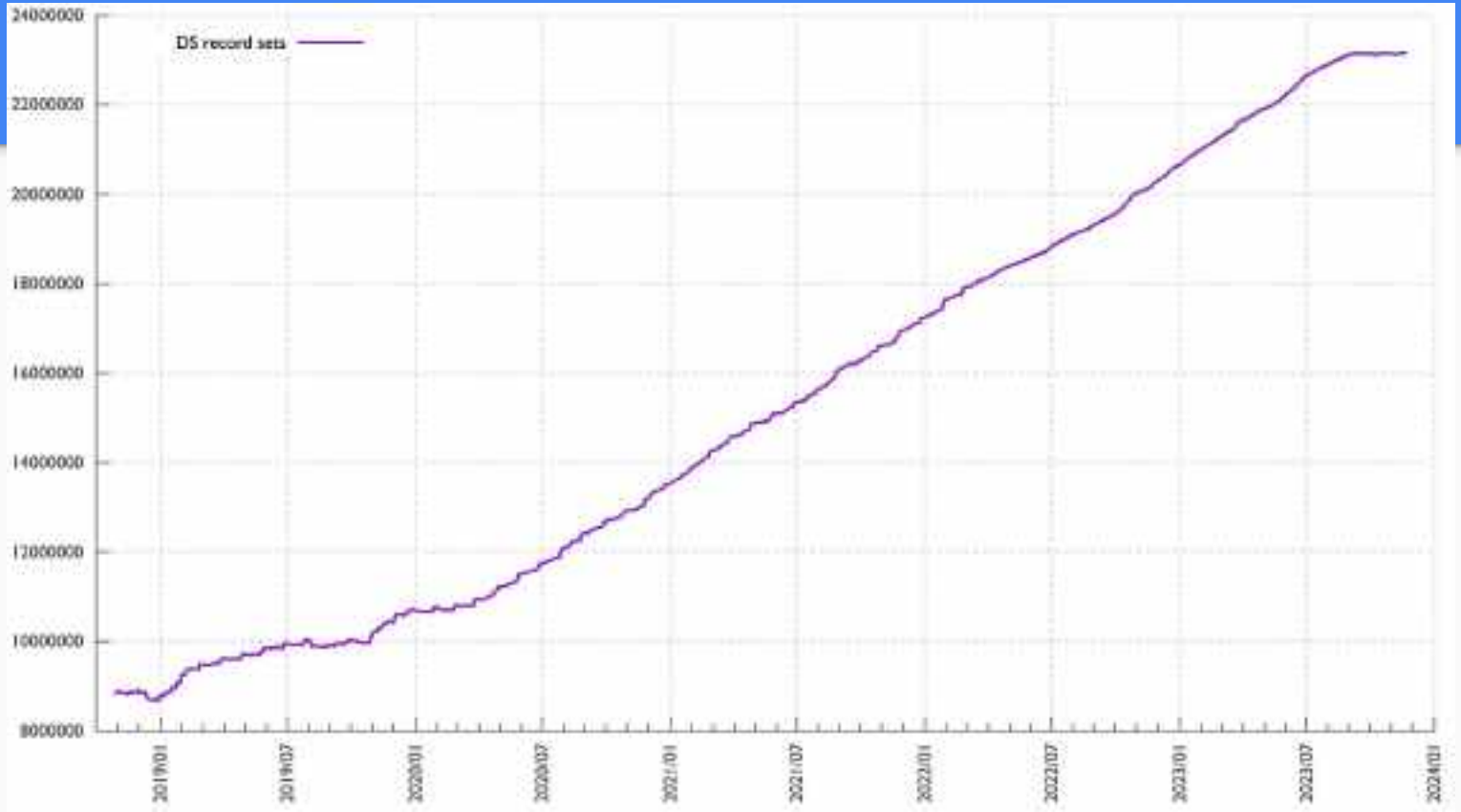
4.16. Extended DNS Error Code 15 - Blocked
The server is unable to respond to the request because the domain is on a blocklist due to an internal security policy imposed by the operator of the server resolving or forwarding the query.

4.17. Extended DNS Error Code 16 - Censored
The server is unable to respond to the request because the domain is on a blocklist due to an external requirement imposed by an entity other than the operator of the server resolving or forwarding the query. Note that how the imposed policy is applied is irrelevant (in-band DNS filtering, court order, etc.).

4.18. Extended DNS Error Code 17 - Filtered
The server is unable to respond to the request because the domain is on a blocklist as requested by the client. Functionally, this amounts to "you requested that we filter domains like this one."

– RFC8914 - "Extended DNS Errors"

5. Increased deployment of DNSSEC



6. Much simpler to deploy resolvers

To install the DNS Server role as a standalone server, perform the following steps:

PowerShell | GUI

Here's how to install the DNS Server role using the Install-WindowsFeature command.

1. Run PowerShell on your computer in an elevated session.
2. To install the DNS role, run the following command. The installation doesn't require a reboot.

PowerShell — Copy

```
Install-WindowsFeature -Name DNS
```

Risks…

Risks…

- Ineffective
- Collateral damage
- Drives risky behavior
- Additional load / poorly defined behavior.
- Extra-jurisdictional issues.
- Users losing trust in the Internet.
- Trains users to disable or ignore security controls.

Ineffective - the Dancing Hamster problem

Collateral damage…

- Don’t block all of Wikipedia because you disagree who shot first…

Han shot first

Article Talk

From Wikipedia, the free encyclopedia

"**Han shot first**" refers to a controversial change made to a scene in the film *Star Wars* (1977),[a] in which Han Solo (Harrison Ford) is confronted by the bounty hunter Greedo (Paul Blake/Maria De Aragon) in the Mos Eisley cantina. In the original version of this scene, Han shoots Greedo dead. Later versions are edited so that Greedo attempts to fire at Han first. Director George Lucas altered the scene to give Solo more justification for acting in self-defense. Many fans and commentators oppose the change, feeling it weakens Solo's characterization. The controversy is referenced in the 2018 film *Solo: A Star Wars Story*.

Drives risky behavior

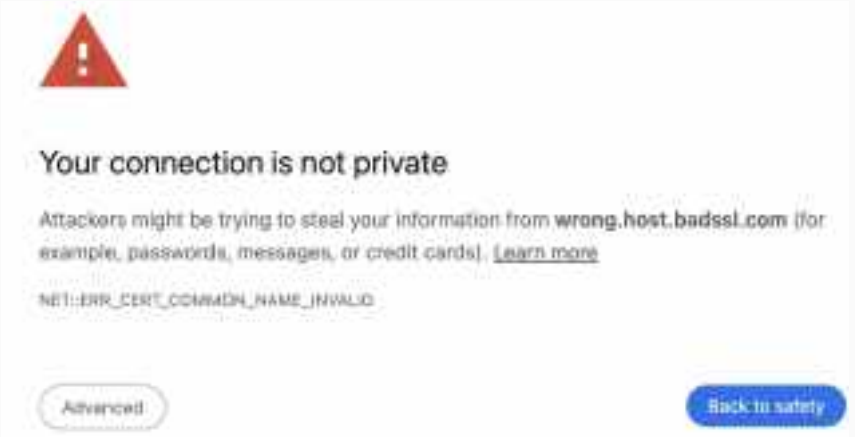
If my government mandates blocking of www.hamsterdance.com I'll:

1. Point my computer at a resolver run by Hax0rs-R-US, who will happily answer for that… and for www.bigbank.com…

2. Point my computer at a resolver operated by [China / Russia / USA / North Korea / England / Iran / {insert your favorite boogie man here }]

Trains users ignore security controls.

- Many of the DNS Blocking solutions involve rewriting answers.
- Results in:
  - 1: DNSSEC failures and
  - 2: TLS failures
- Users gonna click “Proceed anyway…”



Plan…

Reiterate and update advice in SAC050, SAC056

- We still agree with SAC050 (2011) and SAC056 (2012)
  - … mention what all has changed
- Recommend using existing take-down mechanisms (trademark, phishing, CSAM, copyright) to request that the registrar / registry remove the domain. This is the most effective mechanism to ensure that the domain does not resolve.
- If the site is serving malicious content, things like StopBadware
- Keep it short….

Questions?!