DNS over HTTPS instead of Platform DNS

- Side-effect to mitigate: DoH bypasses DNS-based parental controls. Need to detect if present, and disable DoH if so.

- One of many heuristics. Others address split horizon, check platform parental controls, etc.
Detecting DNS-based parental controls

- Examining results of looking up existing likely-filtered domains is a really bad idea.
- Use platform DNS to resolve a designated “canary domain”
  - DNS Policy software blocks or modifies result for canary domain
  - Blocked/Modified result indicates platform DNS policy is present
    - Deduce this means to avoid use of application-based DNS
- Multiple canaries can be checked, if needed
How it works: Client
  ○ As part of making DoH the default, Firefox will attempt to resolve the canary domain using platform DNS
  ○ Error result (e.g. NXDOMAIN) or success result with no A or AAAA record -> canary domain positive result -> DoH disabled

How it works: Server/network
  ○ If using parental control software, add canary domain to blocklist
  ○ If using bind9, use Response Policy Zone (RPZ) to specify NXDOMAIN result
  ○ (Trying to make this easy. Changed algorithm based on initial feedback.)
Adoption

- Pi-Hole added support
- Running studies on Canary trigger rate (as well as other DoH heuristics)
  - Initial study results show non-trivial amounts of adoption
  - btw, DoH rollout in US still hasn’t actually started
- Will continue to monitor via telemetry.
- Watching for abuse -- blocking of canary domain above the end-customer level.
Why didn’t you…?

- Wait for standardization?
  - Needed a solution quickly that did not require new versions of other people’s software be developed and deployed
- Flip the logic so DNS lookup success means policy is present?
  - Less likely to be something configurable through parental control solutions
  - NXDOMAIN substitution results in DoH being disabled
Advantages of IETF standardization

- Increased Adoption & usage by apps as well as servers
- Fewer unilateral canaries to check
- Technical benefits: More design freedom and possible reserved TLD usage
- We are interested in working on a candidate for WG adoption, if there is also interest from others.

Thanks!