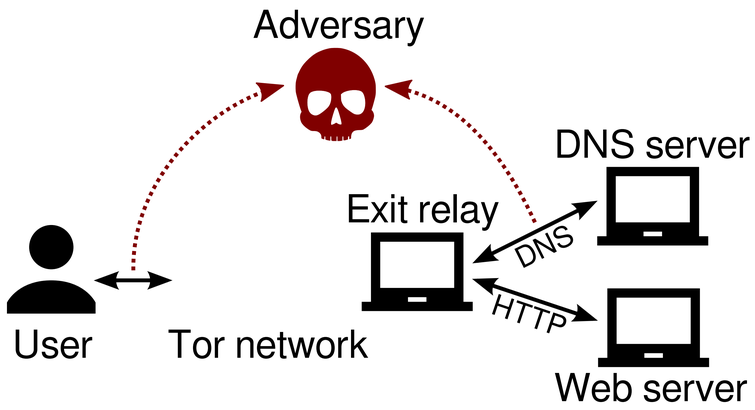
The Impact of DNS on Tor's Anonymity

Benjamin Greschbach* Tobias Pulls* Laura M. Roberts* Philipp Winter* Nick Feamster
KTH Royal Institute of Technology Karlstad University Princeton University Princeton University Princeton University

End-to-end correlation attacks

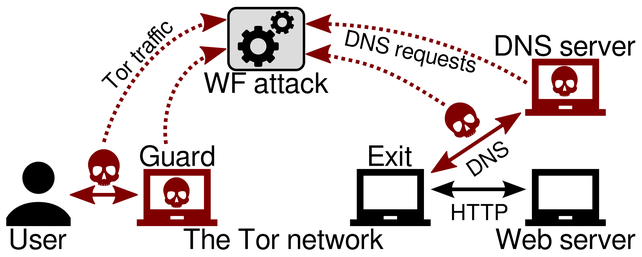
- Adversary seeks to control **both ends** of low-latency anonymity network, like Tor
- Simple techniques like packet counting allow **deanonymization**
- Past work focused on TCP stream between client and server, **ignoring DNS** and its distributed nature



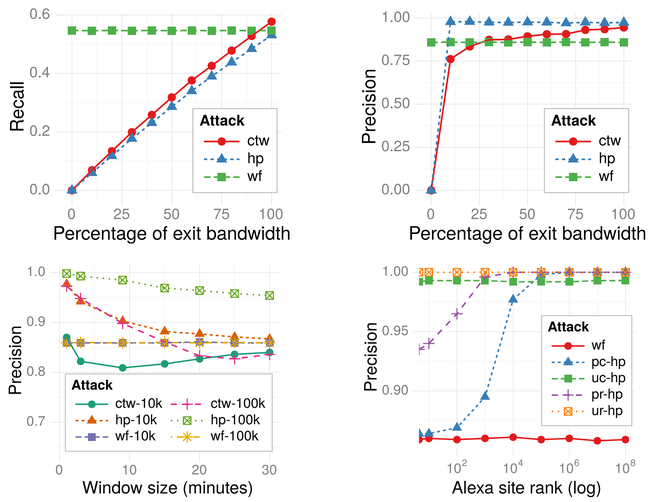
Why is DNS an issue?

- Iterative queries **traverse many paths** in addition to point-to-point TCP connection
- Some third-party resolvers shouldn't learn **what Tor users do**
- Tor's DNS resolution is entirely up to exit relays (**here be dragons**!)

DefecTor attacks

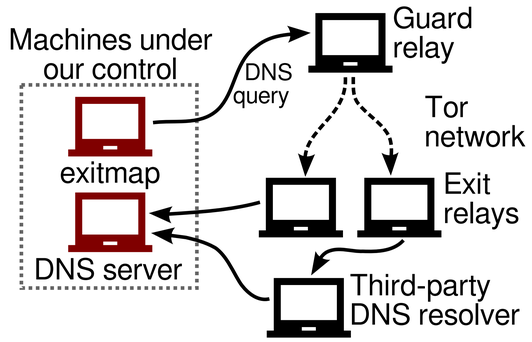


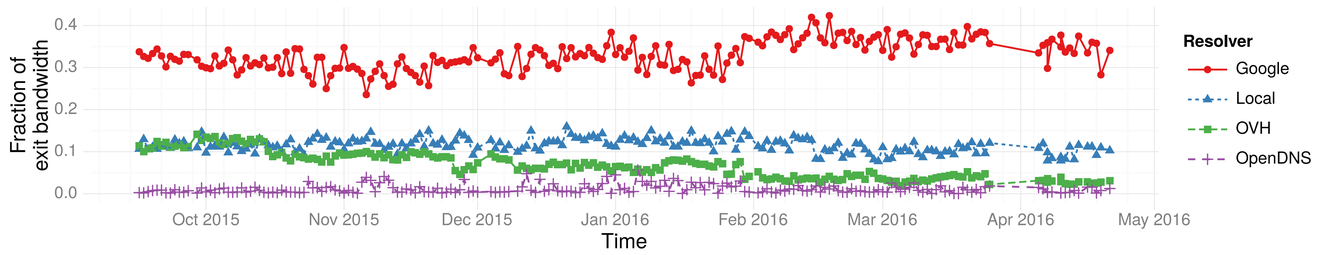
- **D**NS-**e**nhanced **f**ingerprinting and **e**gress **c**orrelation on **Tor** attacks
- Combines a **website fingerprinting** attack on ingress traffic with DNS traffic exiting Tor
- **Perfectly precise** attacks for **unpopular websites** on the Tor network



How Tor exits resolve DNS

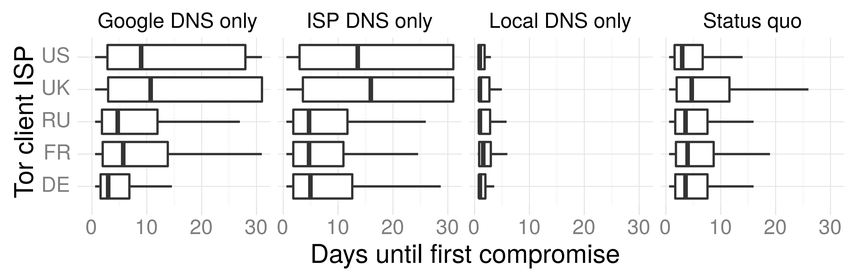
- Each exit either run its own resolver or rely on a **third-party resolver**
- We **mapped DNS queries to exits** from September 2015 to May 2016
- On average, **Google observed 33%** of all DNS requests from the Tor Network





Internet-scale analysis using TorPS

- With RIPE Atlas we achive **previously unprecedented** path coverage for simulating AS-level adversaries
- Exit operators should **avoid public resolvers** such as Google and OpenDNS
- The **location of the Tor client matters** for traffic correlation studies



*All four authors contributed substantially, and share first authorship.

https://nymity.ch/dns-traffic-correlation/