
DNS TAPIR
Threat And Privacy
Internet Research
INTERNET STIFTELSEN
NET NOD
SUNET

Välkommen!

- Vi spelar in hela sessionen för publicering på YouTube
- Tack till Internetstiftelsen för tillgång till lokal

Agenda

- Introduktion
  - Olle E. Johansson
- Varför?
  - Mikael Kullberg
- Introduktion till DNS TAPIR
  - Mikael, Ulrika
- Fika
- Demo och teknisk genomgång
  - Ulrika Vincent
- Säkerhetsmekanismer i DNS TAPIR
  - Jakob Schlyter
- Frågor och svar


En innovativ, öppen tjänst
för DNS-analys som
förbättrar svensk
Internetsäkerhet.

Rekursiv DNS får internet att fungera.

Rekursiv DNS tillhandahålls av resolvrar. Dessa drivs av olika aktörer:

De som erbjuder rekursiv DNS *åt andra*

Denna grupp består dels av större **internetoperatörer** som Telia eller Tele2. En privatperson eller ett företag som har Telia som operatör använder då deras resolver – och det är hos Telia som en sådan användares DNS-trafikdata finns.

Dels finns här också **företag som t.ex. Google, Cloudflare och Akamai**. Dessa erbjuder resolvertjänster (till privatpersoner ofta kostnadsfritt), och är ett alternativ som mindre internetoperatörer och företag i Sverige ibland använder sig av.

De som driver rekursiv DNS *åt sig själva*

Denna grupp består av en rad, ofta mindre, aktörer som **myndigheter, universitet, skolor och vissa företag**. Genom att driva egen resolver har de här aktörerna själva tillgång sina användares DNS-trafikdata.

Men. Bedräglig användning av DNS är ett växande problem.

Tre centrala problemområden

1. Förflyttning av bedräglig aktivitet till DNS

DNS har länge setts som ett legitimt protokoll som inte övervakas lika strikt av exempelvis brandväggar. Men i takt med regleringen av områden där cyberhot tidigare rört sig flyttar aktörer sin verksamhet till DNS för att uppnå sina syften.

Ett exempel är web cookies, där ”Cookielagen" reducerade möjligheterna för att spåra användarbeteenden. Detta har medfört en massiv övergång till att istället spåra användare och deras aktiviteter genom att använda DNS som en “sidokanal”.

Grundidén är enkel: koda den användarinformation som skall sparas i ett domännamn (som inte existerar). Ställ en fråga (vilken når egen namnserver) och vips har datat exfiltrerats.

Konsekvens: DNS-infrastrukturen används i allt högre grad på bedrägliga sätt av många aktörer.

2. Fler cyberhot mot användarna via DNS

En internetanvändare kan drabbas av flera klasser av hot där DNS är inblandat:

- **Nätfiske & bedrägerier:** Aktörer tar kontroll över eller dubblerar legitima domännamn för att skapa bedräglig hemsidor, email eller annan kommunikation som kan lura användare på känslig information som lösenord, filer eller personlig info.
- **Spårning & övervakning:** Exploatering av DNS för att spåra användares beteenden och aktiviteter på internet, vilket kan leda till känslig exponering av personlig data eller företagsdata.
- **DDoS-attacker:** Överbelastning av internetbaserade tjänster och -infrastruktur (oftast med hjälp av botnets som genererar stora mängder trafik), vilket gör att användare inte kan nå vissa hemsidor eller tjänster.
- **Dataläckor**: Aktörer använder DNS för att ta sig förbi brandväggar och exfiltrera data utan att bli upptäckta, vilket kan resultera i att känsligt data läcks.

Konsekvens: Ett växande hotbild mot internetanvändare i Sverige, varav en stor del potentiellt kan blockeras via DNS.

3. Ökat beroende av utländska tjänster

På grund av omvärldsläget pågår en förnyad debatt kring det svenska samhällets robusthet.

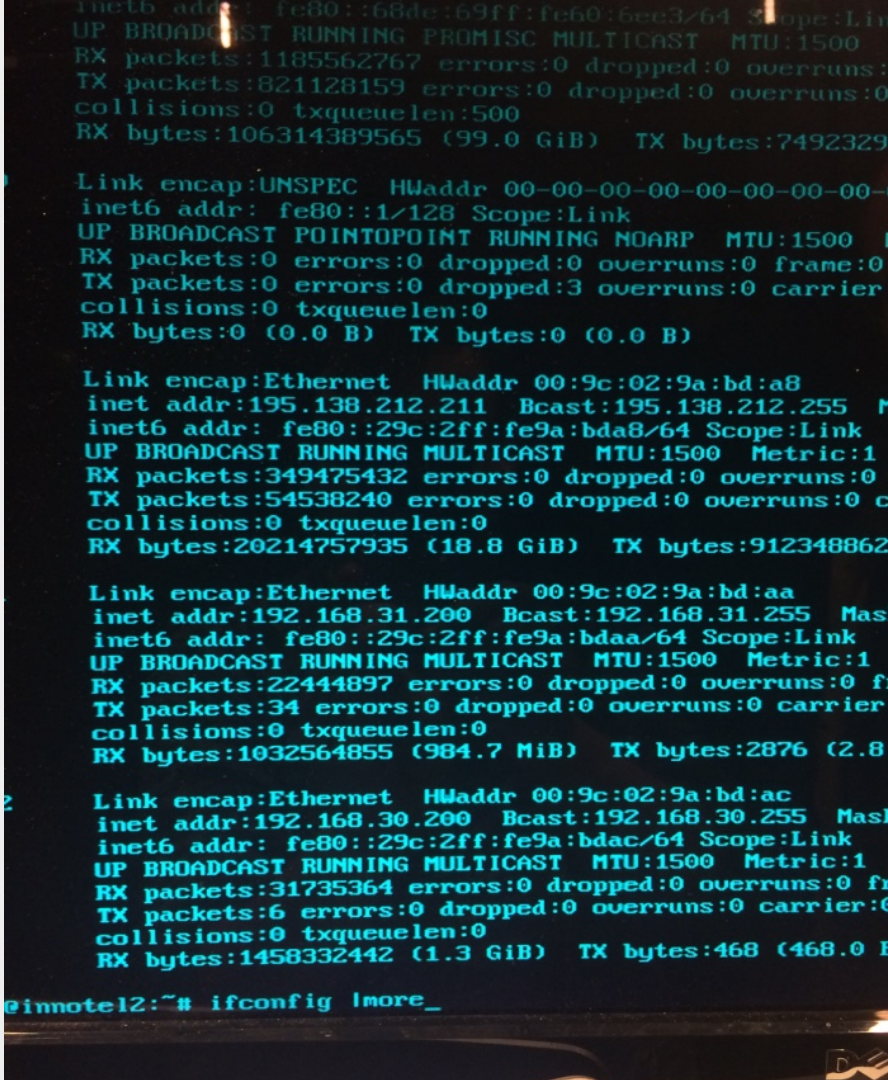
När svenska operatörer använder utländska resolvertjänster som exempelvis Google innebär det att vi i Sverige är beroende av en utländsk aktör för nå svenska internettjänster.

Idag pekar dessutom trenden åt att fler svenska operatörer väljer utländska resolvertjänster för att det är mer resurseffektivt än egen resolverdrift.

Konsekvens: En minskad nationell robusthet för svenskt internet i tider av internationell osäkerhet.

Analys av stora volymer DNS-data som visar vilka frågor användare ställer **skulle kunna bidra till att lösa dessa problem.**

Utmaningen är
att detta frågedata
av integritetsskäl
idag inte delas av
resolveroperatören.



PROBLEM

Problemet har varit att knäcka koden för hur man får tillgång till stora volymer DNS-data **utan att tumma på användarnas integritet.**

Detta möjliggörs nu av DNS TAPIR.

INTERNET STIFTELSEN

DNS TAPIR Threat And Privacy Internet Research

DNS TAPIR är idag en arkitektur och prototyp för ett öppet system för insamling, analys och underlag för blockering av oönskad DNS-trafik som utvecklas i ett samarbete mellan PTS, Internetstiftelsen, Netnod och Sunet.

Tjänsten möjliggör analys av större mängder DNS-data på ett integritetssäkert sätt — och realtidsnära identifiering av säkerhetshot mot internetanvändare.

INTERNET STIFTELSEN NETNOD SUNET

DNS TAPIR vilar på tre grundläggande värderingar:

Samarbete
↳ Win-win

DNS TAPIRs storskalighet bygger på ett samarbete med svenska operatörer där analystjänsten ges tillgång till DNS- data som ”tvättats” från det som gör att en individ kan identifieras.

Det gör att operatörerna inte kompromissar med användarnas integritet. I gengäld får de en mer effektiv och kvalitativ DNS-analys som gynnar deras användare.

Neutralitet
↳ Förtroende

Med Internetstiftelsen som central sponsor får DNS TAPIR den neutrala roll i infrastrukturen som möjliggör att vi kan få både internetoperatörernas och samhällets förtroende.

Det garanterar att data inte missbrukas, att användarintegriteten skyddas och att systemet gynnar samhället som helhet.

Open-source
↳ Transparens

Förtroende etableras genom transparens. DNS TAPIR är därför baserat på öppen källkod och tillämpar full transparens – från systemets funktion till hur data aggregeras för att skydda användarnas integritet.

Vägen framåt för **Robust DNS** och **DNS TAPIR**

INTERNET STIFTELSEN NETNOD SUNET

Fas 1: Proof of concept

Fas 2: Storskalig test, fokus på drift

Fas 3: Drift

Fas 1 är vi klara med.

Vi planerar nu för fas 2 av **Robust DNS**.

Vi har idag resurser för att vidareutveckla **DNS TAPIR på halvfart**

Fas 2 i korthet

Förenkla installation

Förbättra analys med riktiga dataströmmar

Säkerhet

Övervakning, loggning

Administra-tion, konton

Open Source projektet

Export av data till andra system

Organi-sation

Även om fas 1 är klar, jobbar vi envist vidare.

Välkommen att bidra!

info@dnstapir.se www.dnstapir.se