Slutrapport Projekt "Robust DNS"

September 2024

Nästan all användning av Internet börjar med att man hittar en tjänst med hjälp av DNS. Tyvärr använder även skadliga programvaror som malware, virus och ransomware DNS för sina egna syften. Det är svårt att hitta spår av dessa skadliga hotaktörer i loggar från en enskild DNS-resolver då mönster som avslöjar en hotaktör framträder först när data från flera källor samlas. Genom att samla data från en större mängd användare i realtid kan man generera en helhetsbild, och kan därigenom snabbt fånga förändringar i beteende samt skapa effektiva motåtgärder.

Emellertid kommer en sådan samling av data innehålla information som avslöjar hur enskilda individer använder internet vilket självklart är starkt integritetskränkande. Utmaningen är alltså att skapa en lösning som låter oss hitta hotaktörer samtidigt som den enskildes integritet skyddas.

Projektet "Robust DNS" har skapat ett system som på ett unikt och effektivt sätt söker efter avvikande mönster och händelser i DNS utan att individens integritet kränks. Systemet heter "DNS TAPIR" och är ett distribuerat system där data samlas från många aktörer. Nya data jämförs kontinuerligt mot ett etablerat normalläge och avvikelser av snabbare karaktär fångas upp av att unika händelser skickas direkt när de uppstår – oftast med en reaktionstid på under minuten. Ett stort och brett dataunderlag är nödvändigt för att upprätthålla information om ett normalläge, något systemet självt gör över tid. Systemet är från början konstruerat med inbyggt dataskydd (*privacy by design*) specifikt för att göra det tryggt att dela med sig av sina DNS-data utan att kränka individers rätt till privatliv.

Flera stora namnkunniga operatörer i Sverige har följt utvecklingen och är positiva till att pröva systemet i produktion. En uppsättning data som inkluderar alla, en allmänning i dataform, är också något både operatörer och användare lättare accepterar när data är fritt från känsliga uppgifter.

Resultaten från DNS TAPIR är i sig intressanta och en del observationer kan göras direkt, men verkligt värde uppnås först när informationen kombineras med andra typer av data kopplade till samma fenomen, exempelvis informationsläckage och cyberhot. Ett antal säkerhetsföretag har visat stort intresse då de ser den data som systemet producerar som ett unikt tillskott i detta avseende – data de har svårt att få tillgång till själva på annat sätt.

Alternativa lösningar finns men är i samtliga fall utvecklade av kommersiella leverantörer som i flera fall använder detta data för andra syften. Ofta är det svårt för dem att få tillgång till tillräckligt bred datamängd, samtidigt som data man samlar in blir inlåst hos leverantören. Detta sker dels av kommersiella skäl men oftast för att kunna hantera juridiskt ansvar om de samlar integritetskänsligt data. Dessa får därför inte en samlad bild av aktivitet i Sverige och kan inte leda till samma reaktionsförmåga som ett nationellt genomförande av DNS TAPIR har potential att uppnå.

Demonstrationer av programvaran (*proof of concept*) som utvecklats i fas 1 visar tydligt att alla delmoment fungerar — hela vägen från insamling via analys till återkoppling och åtgärd.

Bakgrund

Projektet “Robust DNS” har som syfte att utveckla ett innovativt och öppet system som baserat på data från DNS-frågor från användares aktiviteter i t.ex. mobilappar, webbläsare och IoT-system analysera data och skapa en reaktionsförmåga som kan stoppa destruktiva förlopp, som till exempel ett virus som snabbt sprider sig eller ransomware. Systemet utvecklas i öppen källkod för granskning och byggande av en internationell community. Parallellt jobbas med att förbereda för en nationell installation i Sverige med syftet att stärka förmågan att skydda svenska användare av Internet. Ett sådant system kräver samverkan mellan en stor mängd operatörer av DNS-tjänster för att få tillräcklig mängd data för analys och snabb reaktion.

Projektets första fas är färdigställd och vi har uppnått, och i vissa hänseenden överträffat, de resultat vi hoppats på.

I ansökan definierades målen för fas ett enligt följande:

1. ***Utveckla en arkitektur*** *för datainsamling och dataanalys med bibehållen integritet för slutanvändaren med syfte att möta moderna cyberhot.*
2. ***Ta fram en specifikation*** *av en decentraliserad DNS-resolverfunktion med stöd för moderna protokoll och standarder samt stöd för produktion av anonymiserad insamling av DNS-resolverdata.*
3. *Genomföra* ***implementationen av en demonstrator*** *(proof-of-concept, PoC) gentemot denna specifikation. I detta steg integreras resultaten från steg 1 och 2 ovan.*
4. ***Förbereda för en implementering*** *i större skala i samverkan med landets ledande operatörer. Denna fas ska kunna påbörjas Q1 2024 och förutsätter annan finansiering. Denna fas ska även samordnas med ansökan om EU-medel under 2023.*

Som sammanfattning av den större rapporten kan vi konstatera att vi kommit bra i mål på punkterna 1-3 och en bit på vägen i punkt 4.

DNS roll gällande mitigering av cyberhot

På en mycket hög nivå kan ”cyberhot” klassificeras som flera typer av attacker:

- Hot som nyttjar Internet för att störa driften av en specifik tjänst eller entitet
- Hot som syftar till att störa användandet av Internet generellt inom ett område, och därmed störa Internetbaserade tjänster i det området.

I båda fallen är det vanligt att se att DNS används eller missbrukas av angriparen. För att kunna lindra effekterna av sådana aktiviteter så är medvetenhet om aktiviteten det första målet. Eftersom DNS ofta existerar någonstans på angriparens väg till målet, så är DNS-observationer på nationell skala ett av de mest precisa verktygen som går att använda för detektion. Ett stort problem är att det inte finns någon tradition av att på ett integritetssäkert vis dela denna typ av information mellan operatörer. För att kunna göra än

mer effektiva analyser än man kan göra idag behövs en stor mängd DNS-data, vilket i Sverige förutsätter att data delas på nationell nivå.

Projektet “Robust DNS” har en unik position att från ett svenskt perspektiv möta denna brist.

Övergripande funktion

Programvaran som utvecklas inom projektet heter “DNS TAPIR” och finns tillgänglig som öppen källkod. I den centrala delen av systemet behandlas inte någon information som kan identifiera en enskild individ.. Detta medför att systemet har ett starkt skydd för personlig integritet och det medför också att det inte går att agera (filtrera, spärra) på användarnivå i DNS TAPIR. Den totala insamlade datamängden och behandlingen av denna i realtid visar förändringar av en egenskap som föranleder en reaktion. I systemet benämner vi en sådan förändring en *observation*. Observationer distribueras till alla ingående operatörer och varje operatör beslutar själva hur deras TAPIR Edge-installation ska agera på observationer från TAPIR Core. Det finns alltså ingen central styrning – *alla policybeslut är lokala.*

Ett exempel på en observation kan vara ett virus som kommunicerar med en central tjänst. DNS TAPIR kommer kunna se förändringar i frågemönster och skicka ut en observation med attribut relaterade till förändringarna, exempelvis snabbt ökande, låg rank (måttet på en domäns popularitet eller vikt, vilket används t.ex för sökmotorer) eller bibehållen ökad trafikvolym. Om dessa attribut är tillräckliga för att operatören skall filtrera trafiken skulle virusets förmåga att sprida sig och orsaka skada, via till exempel ransomware, minska betydligt. Andra aktörer som får data från DNS TAPIR och har tillgång till andra typer av data kan korrelera dessa och då också reagera för att förhindra en pågående infektion eller attack.

Alla delmoment som krävs för att skapa den kedja som beskrivs ovan, från incident till reaktion i DNS-resolvern, är implementerade och demonstrerade, och utgörs av följande steg:

- Användare surfar som vanligt och deras system sänder löpande frågor till en DNS-resolver (som är standard och oförändrad av DNS TAPIR)
- Data om frågor skickas från DNS-resolvern till TAPIR Edge som där processas med hänsyn till integritet, informationsvärde och liknande. Resulterande avidentifierade data skickas från TAPIR Edge till TAPIR Core
- TAPIR Core bearbetar inkommande data och om det finns information av intresse, skapas observationer med attribut relaterade till eventuella förändringar, avvikelser från norm, och så vidare.
- TAPIR Core publicerar observationer till alla medverkande parter
- TAPIR Edge lyssnar på dessa observationer, och om tillräcklig verkshöjd uppnås (enligt Edge-operatören), beslutar om en åtgärd för DNS-svaret på den relevanta frågan
- DNS-resolvern får uppdaterad information från TAPIR Edge om hur den skall hantera den relevanta frågan
- Användare får nu t.ex felkod vid surfning till en spärrad adress

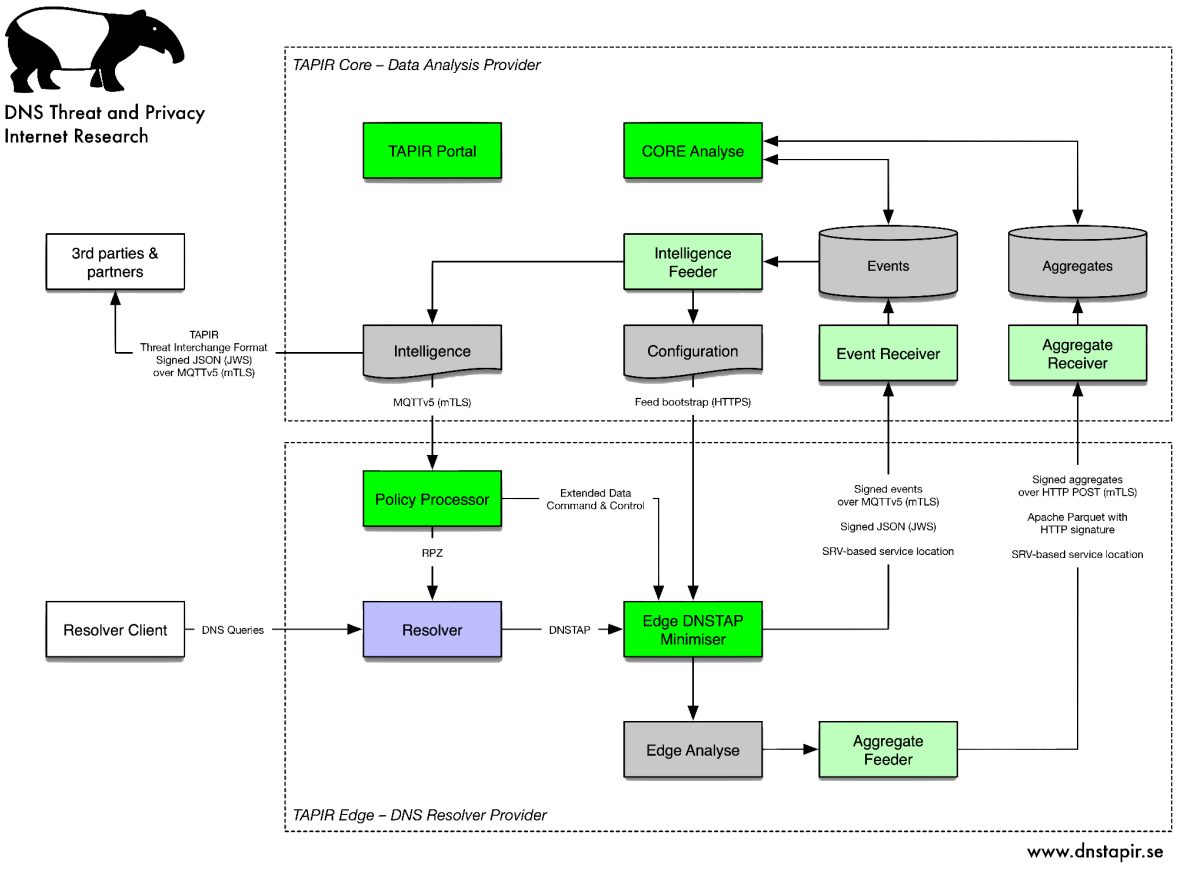
Systemkonstruktion

Projektet har utvecklat en innovativ systemkonstruktion med en central tjänst (TAPIR Core) som samlar in data från ett antal distribuerade tjänster hos resolver-operatörer (TAPIR Edge).

TAPIR Core kan dela sina observationer med tredje part, som kan använda dessa tillsammans med andra typer av datakällor. Det är tekniskt möjligt i TAPIR Core att också dela observationer med andra Core (TAPIR federation). *TAPIR Edge* är den programvara som ska köras hos operatörer av DNS-resolvrar, och som bearbetar data kommande från och skickade till resolvern.

DNS TAPIR innehåller också implementationen av en systemkonstruktionen som identifierar de olika parterna och integritetsskyddar data under transport mellan TAPIR Edge och Core.

En översikt av systemkonstruktionen återfinns i figuren nedan. Notera att inte alla delar är implementerade, då fokus var att leverera en fungerande *övergripande funktion* enligt ovan.



Specifikation

Vi har utvecklat specifikationer för samtliga delar av plattformen. Detta inkluderar protokoll-specifikationer för datautbyte och kommunikation samt datastrukturer för lagring och analys. Dessa finns öppet tillgängliga på projektets Github instans, och fortsatt utveckling sker inom ramen för Open Source-projektet.

Projektet har också författat ett dokument som beskriver integritetsskyddet för plattformen, ett så kallat whitepaper. Detta har publicerats öppet på vår webbplats och distribuerats för att stimulera granskning och återkoppling[1].

Förberedelser för implementation

Vi har löpande fört en dialog med flera aktörer, bland annat Internetoperatörer och analysföretag för att förstå hur en implementation kan integreras i deras driftsmiljö. Dessa aktörer är intresserade av en utökad testverksamhet i en kommande fas.

Operatörerna har i dialogen framfört att man har ett stort tryck från olika kommersiella aktörer att implementera *liknande system där frågor som integritet och lokal kontroll av policies inte fått prioritet.* Intresset för en gemensam lösning där integritetsfrågorna beaktas är stor och man har även framfört intresse av att aktivt delta i Open Source-projektet. Dialog med dessa operatörer kommer att fortsätta.

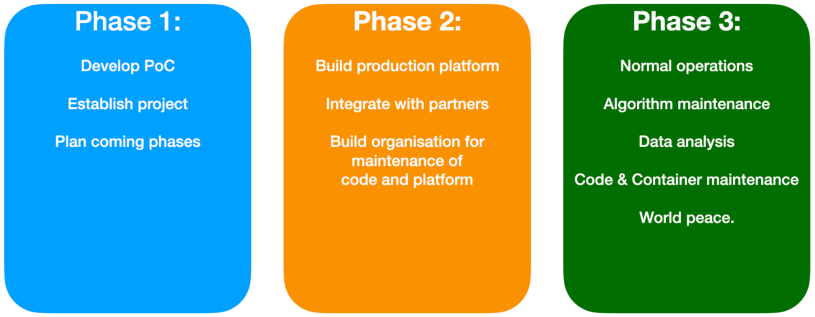
I dialog med både operatörer och analysföretag har det framkommit ett behov av att köra en parallell TAPIR Core, där data från interna nätverk kan analyseras separat. Vi har i fas ett inte fokuserat på att hitta en systemkonstruktion för detta, men behovet är så starkt att det bör ingå i vidare arbete i kommande faser av projektet.

Fortsatt arbete med att färdigställa plattformen för drift, utveckla erfarenhet av drift i en testverksamhet och hitta former för innovation och vidareutveckling av analysfunktioner är en del av en fas två av projektet. Denna fas beskrivs i ett separat dokument som kan erhållas på förfrågan. Fas tre är en produktionsfas där projektets programvara går i drift och vidare arbete sker parallellt i det öppna källkods-projektet och en tänkt driftsorganisation.

Så här beskrevs de olika faserna på ett tidigt stadium i projektet:

[1] https://www.dnstapir.se/info_mgmt/tapir_info_mgmt.sv

DNStapir project phases



Status för DNS TAPIR-plattformen

All kod har utvecklats på Github och har släppts med en öppen källkodslicens (BSD-licens). Det borgar för detaljerad granskning och möjligen också för samverkan med andra aktörer i utveckling av plattformen. Det är centralt med transparens för att uppnå tillräckligt förtroende för att plattformen gör det den säger att den gör och endast detta.

Vi har installerat en publik DNS-resolver som implementerar TAPIR Edge, och har användare bland SNUS och ISOC-SE:s medlemmar. Det finns också ett flertal testscript som belastar servern med frågor. Tack vare samverkan med Torbjörn Eklöv, Nordlo AB, som har kört tester mot denna resolver, så har vi lyckats lösa ett antal problem med bland annat stora frågevolymer. Torbjörn går dagligen igenom alla domäner inom se-zonen, vilket gett ett bra svenskt underlag att jobba från.

Status för ingående komponenter

TAPIR Edge

TAPIR Edge är samlingsnamnet för de komponenter som skall köras av resolver-operatören i anslutning till sin resolver. Implementerade funktioner är datainsamling och minimering (EDM) och resolverns policyhantering (POP).

Resolver (extern mjukvara)

Den resolver som använts i utvecklingen av TAPIR Edge har utsatts för ständiga påfrestningar av både interna och externa testare i syfte att skapa trafikvolymer liknande de man kan se hos en internetleverantör. Endast standardprotokoll har använts för att interagera med resolvern för att undvika inlåsning till en specifik produkt, så att godtycklig resolver som implementerar DNSTAP och RPZ skall kunna användas.

TAPIR EDM (Edge DNSTAP Minimiser)

- Körs kontinuerligt och samlar in DNS-händelser via DNSTAP.

- Gör pseudonymisering av IP-adresser tillhörande DNS-klient eller DNS-server. Detta sker antingen via Crypto-PAn kryptering (pseudonymisering) eller hashning till en HyperLogLog (HLL) datastruktur (stokastisk kardinalitetsapproximation).
- Upptäcker när det sker uppslag mot domäner den inte känner till sedan tidigare och skapar då händelser (*events*) på meddelandebuss (MQTT).
- Lagrar domäner den agerat på lokalt för kontinuerlig funktion även om processen startas om.
- För domäner som kategoriserats som välkända sammanställs resultatet till räknare som periodvis skrivs ut till Parquet-filer och levereras signerat in till TAPIR Core.
- Applikationen exponerar mätvärden och profileringsdata för att ha underlag till förbättringar av koden.
- Applikationen loggar vad den gör via strukturerad JSON.
- Koden har grundläggande tester för viktiga funktioner.

TAPIR POP (Policy Processor)

- Tar emot observationer från TAPIR Core på meddelandebussen (MQTT).
- Implementerar beslutsregler för hur observationer och andra datakällor skall användas i policybeslut för spärr och liknande.
- Underhåller och tillhandahåller minimerade listor formaterade för att resolvern skall konsumera dem.
- Underhåller filter för klassificering i EDM, såsom kända domännamn och liknande.

TAPIR EDGE Stack

En samling scripts och multipla Docker-containers för att förenkla och möjliggöra test och installation av en komplett TAPIR Edge-plattform, inklusive en resolver.

TAPIR Core

Kod som utvecklats för TAPIR Core är ett antal stödjande komponenter för hantering av meddelanden, lagring av inkommande data och administration av säkerhetsfunktioner och konton. Utöver detta finns en analys-modul bestående av en plattform för produktion av kontinuerliga analyser och en dynamisk arbetsmiljö för löpande explorativ dataanalys och utveckling av nya algoritmer.

Analysfunktionen implementeras med standardverktyg för dataanalys, såsom Apache Spark, Jupyter Hub, samt ett antal moduler till dessa, som alla är tillgängliga som öppen källkod. Kod för analys utvecklas löpande i programspråket Python, där arbetet i huvudsak sker i Jupyter Notebooks. Några exempel på Notebooks som använts under utvecklingen är publicerade, som beskriver hur man får tillgång till data och publicerar observationer. Produktion av kontinuerliga analysprocesser görs för närvarande också i Jupyter Notebooks, men skall normalt sett ske i ett mer processorienterat verktyg.

Analys har i fas 1 fokuserat på att säkerställa att insamlade data är meningsfulla och användbara, att samtliga led i systemet hanterar dem korrekt utan förvanskning och att validera aggregerade trafikdata. Genom att generera och identifiera avvikelser i testdata utifrån valda metoder och algoritmer så har både datamodeller och infrastruktur testats, utvecklats och stabiliserats. Kommunikation mellan komponenterna (EDM, POP, Analyse)

har anpassats, verifierats och felsökts genom att kontinuerligt presentera trafikdata och meddelande-flöden till och från Core.

Aggregate Receiver

- Tar emot den datastruktur som innehåller de sammanställda räknare som EDM aggregerar, för exempelvis kända domäner, och lagrar dessa i objektlagringen (S3).
- Information om att aggregatet mottagits registreras i en databas med metadata.
- Nya aggregat aviseras via meddelandebussen (MQTT) för analys.

Event Receiver

- Hanterar Events som skickas till TAPIR Core från TAPIR Edge

Analyse

- Fungerande installation av skalbara analysverktyg och gränssnitt för analytiker.
- Läser data skapat av Aggregate Receiver från objektlagring (S3).
- Tar emot Events genererade i TAPIR Edge.
- Kan generera observationer som skickas till TAPIR Edge.
- Kör automatiska processer för att sammanställa och berika data från TAPIR Edge.
- Används för explorativ dataanalys för att utveckla metoder för att identifiera anomalier, ovanlig trafik, eller liknande.
- Funktioner för att presentera analyserade data, exempelvis grafer.

Mål för TAPIR Core

Hot via och mot DNS har dokumenterats av ett antal organisationer, inklusive ICANN[2], First[3], med flera. Just First publicerar en sammanfattning av hot och vilka parter som kan upptäcka, agera och förebygga dem, sammanlagt 21 olika hot och 15 olika aktörer. Av dessa konstaterar man att resolver-operatörer kan upptäcka 17 olika hot, kan agera på 14 och förebygga 6 av dem, och detektering är oftast beroende av DNS-data.

TAPIR Core får i nuläget två distinkt olika data från TAPIR Edge – histogram på kända domäner samt händelser. Exempel på konkreta observationer baserat på händelser, är detektering av ett nytt domännamn. Om ett antal Edge-noder uppfattar samma nya domännamn inom ett begränsat tidsfönster är det en stark indikation på botnet-beteende.

Motsvarande för kända domäner är att skapa en baslinje för domäner över tid, och notera olika typer av avvikelser från denna baslinje. Exempel på avvikelse är en momentant kraftig tillväxttakt eller större periodiska avvikelser från baslinjen. Att en domän är känd är inte likställt med att den är legitim, enbart att den existerat över en längre tid och synts i andra sammanhang. Så hot i formen av phishing/typosquatting, spam, malware, och även botnets, existerar i detta data.

[2] https://www.icann.org/dnsabuse
[3] https://www.first.org/global/sigs/dns/DNS-Abuse-Techniques-Matrix_v1.1.pdf

I och med den infrastruktur som skapats i fas 1 av DNS TAPIR blir det möjligt att analysera och leverera observationer från analysfunktionen i TAPIR Core. Utöver vad som visats i fas 1, finns ett antal analyser som skall prövas på riktiga data i fas 2.

Ytterligare datastrukturer finns definierade, bland annat histogram över domäner som inte är kända och vektoriserade frågeströmmar. Dessa är närmare knutna till frågeställarens identitet, så en förutsättning för att dessa skall kunna skickas till TAPIR Core är en lokal analysfunktion för mer ingående avidentifiering och sammanställning. Histogram används som ovan, medan vektorer är basen för maskininlärning. Dessa kan exempelvis detektera Domain Generation Algorithms[4] (DGA) som används för att gömma en skadlig programvaras styrsystem (Command & Control, C2). Forskning på området ger många färdiga metoder och algoritmer[5], och projektet avser att modifiera dessa till en mer integritetssäker modell.

Mycket av värdet i data som utvinns uppstår när det korreleras med andra data relaterade till samma fenomen. Indikationer observerade i DNS kan stärka bevis för att domäner och IP-adresser man hittar i andra källor, exempelvis Spam, Netflow, etc är skadliga.

Moduler som ej implementerats i fas 1

Fas 1 avsåg att bevisa att analys går att utföra med bevarande av användarens personliga integritet. De delar som inte varit nödvändiga för en fungerande PoC har ej utvecklats, men finns för tydlighet skull dokumenterade i den övergripande systemkonstruktionen.

- Webbportal för administration
- PKI-lösning med automatik för anslutning av nya TAPIR Edge instanser
- System- och nätövervakning
- Stöd för installation och driftssättning
- Edge Analyse: Lokal analysmodul i TAPIR Edge

För att skapa ett komplett system, behöver ytterligare funktionalitet utvecklas och befintliga funktioner stabiliseras och göras driftsmässiga.

Samverkan med DNS-samfundet

Vi har gått ut med information i många forum och sammanhang och har inlett en dialog med DNS-användare, integritetskunniga och säkerhetsexperter. Denna dialog har lett till värdefull feedback.

Ett säkerhetsföretag som vill använda TAPIR Core önskar komplettera sina analyser med "*Identifiering av misstänkta Command & Control-domäner för botnets. Hitta indikationer på att specifika företag eller organisationer har blivit infiltrerade, exempelvis exfiltrering av data*".

[4] https://github.com/baderj/domain_generation_algorithms
[5] https://www.sciencedirect.com/science/article/pii/S1319157822000726

Det finns även ett intresse för hur Core fungerar, och andra är intresserade av att använda samma teknik: "*Vi har etablerat förtroende med stora bolag som driver DNS-resolvers men som kanske inte kan tänka sig att skicka upp sina loggar till en för dem okänd part.*".

I dialog med stora Internetoperatörer framkommer ett stort intresse av plattformen och i vissa fall också att delta aktivt i projektet. Införande av Edge-systemet i operatörernas egna driftsmiljöer kommer att kräva att operatören genomför en ordentlig genomsyn av systemet ur olika aspekter samt en försiktig införandeprocess för att bygga upp erfarenhet av drift och operation av de olika modulerna. Det är därför viktigt med en tidig dialog och samverkan för att uppnå en stor täckning av Sveriges DNS-frågor.

Vi har deltagit med presentationer på flera olika möten och konferenser:

- Netnod höstmöte 2023
- Netnod vårmöte 2024
- SAMnet, Stockholm, januari 2024
- Egen konferensdag 2024 på Internetstiftelsen med 90 medverkande
- Sunet-dagarna april 2024
- Nordic Domain Days, Stockholm, maj 2024
- Flera DNS TAPIR AfterWork 2024 på Agicals kontor i Gamla Stan
- Robust Internet Öresund, Malmö, augusti 2024

Nästa presentation av projektet kommer att ske vid:

- Netnod Tech Meeting, oktober 2024

Flera av dessa föredrag har också spelats in och finns på YouTube. Medlemmar i projektet har också presenterat på DNS OARC möten samt deltagit i IETF.

Projektet har också etablerat närvaro på LinkedIn och postat allmän information om vad vi gör i Open Source-delen av projektet. Exempel på information som publicerats:

Länkar:

- Presentation av DNS TAPIR på Netnod meeting 2023 https://youtu.be/E1IsYtUXjYk?si=td5VYDokf-xzUyjO
- LinkedIn: https://www.linkedin.com/company/dnstapir/

Ekonomi

Projektet sökte och beviljades 4,8 miljoner kronor för utveckling av plattformen. Projektet avslutas i månadsskiftet september/oktober 2024.

Utöver de projektdeltagare som finns nämnda i ansökan har ytterligare en konsult anlitats, Ulrika Vincent, Data Scientist från Agical AB.

Av de beviljade bidragen har en stor del gått till utveckling av systemkonstruktion och analysmetoder. Den utveckling som skett av Edge-programvara har i första hand finansierats av partners och utförts av anställd personal. Internetstiftelsen och SUNET har bidragit stort. Netnod har löpande deltagit och försett projektet med infrastruktur som mötestjänster, dokumentarkiv och en DNS-resolver som är tillgänglig på Internet och använts både av projektet och av utomstående som velat bidra med data för analys.

Utvecklingen har skett på Github[6] och en testmiljö har körts på Safespring inom ramen för Vetenskapsrådets avtal.

Rapporten är producerad i samverkan med teamet.

Sollentuna 2024-10-07

Olle E. Johansson
Projektledare, Robust DNS

[6] *https://github.com/dnstapir*