TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Toomas Esko 162754IABM

DNS-PÕHISTE KONTROLL- JA ANDMEVAHETUSKANALITE TUVASTAMINE

Magistritöö

Juhendaja: Innar Liiv
PhD

Tallinn 2020

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Toomas Esko

12.05.2020

Annotatsioon

Käesoleva magistritöö teemaks on DNS-põhiste kontroll- ja andmevahetuskanalite tuvastamine DNS serveri logiandmete põhjal. Töö eesmärgiks on luua metoodika, mis võimaldab eristada DNS protokolli väärkasutust legitiimsetest päringutest, on lihtsasti juurutatav ja tagab sealjuures madala valepositiivsete tuvastuste arvu.

Probleemi lahendamiseks analüüsis autor erinevates publikatsioonides kirjeldatud DNS väärkasutuse tuvastamise meetodeid, hindas nende sobivust ja rakendatavust vastavalt näidisandmestiku omapäradele ning testis välja valitud meetodite täpsust näidisandmestikul. Kuna ükski meetod iseseisvalt ei saavutanud soovitud täpsust, siis täiendavalt eksperimenteeriti erinevate meetodite kombinatsioone.

Näidisandmestikuna kasutati ca 3000 arvutitöökohaga ettevõtte DNS serverite logiandmeid, mis olid kogutud kahe nädalase perioodi jooksul. Erinevate kontroll- ja andmevahetuskanalite stsenaariumite loomiseks käivitati testkeskkonnas tarkvarad dnscat2, FrameworkPOS, iodine, OilRig ja Poison Frog ning nende logiandmed lisati näidisandmestikule.

Töö käigus loodud metoodika võimaldab tuvastada kõik käsitletud DNS protokolli väärkasutuse stsenaariumid valepositiivsete tuvastuste osakaaluga 0,44%. Kõige raskemini tuvastatava stsenaariumi kõrvale jätmisel langes valepositiivsete tuvastuste osakaal 0,04%ni.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 40 leheküljel, 6 peatükki, 7 joonist, 18 tabelit.

Abstract

Detection of DNS based control and data channels

The topic of this master's thesis is detecting DNS based control and data channels based on DNS server logs. The purpose of this research is to develop methodology that enables to differentiate between DNS protocol abuse and legitimate queries, can be easily deployed and has a low false positive rate.

To solve this task, the author analyzed DNS abuse detection methods described in different publications, evaluated their suitability and applicability for the sample data and tested the accuracy of some chosen methods on the sample data. As none of the chosen methods achieved the desired accuracy, different method combinations were also tested.

DNS server logs collected over a two week period from a company with about 3000 workstations were used as sample data. Software applications dnscat2, FrameworkPOS, iodine, OilRig and Poison Frog were run in the isolated test environment to simulate different control and data exchange channels and the logs were added to the sample data.

The methodology presented in this thesis enables to detect all the considered DNS protocol abuse scenarios with a false positive rate of 0,44%. Leaving aside the scenario which is most difficult to detect, the false positive rate achieved is as low as 0,04%.

The thesis is in Estonian and contains 40 pages of text, 6 chapters, 7 figures, 18 tables.

Lühendite ja mõistete sõnastik

DNS	*Domain Name System*, hierarhiline detsentraliseeritud süsteem, mis võimaldab IP-aadresside asemel kasutada domeeninimesid
Epoch ajatempel	Unixi epoch ajast 01.01.1970 00:00:00UTC möödunud sekundite arv
IANA	*Internet Assigned Numbers Authority*, organistatsioon, mis korraldab domeeninimede süsteemi juurtsooni haldust
IP-aadress	IP-võrku ühendatud seadme identifikaator
Rekursiivne DNS server	Server, mis sooritab nimelahendusi rekursiivselt alustades juurtsoonist
SPF	*Sender Policy Framework*, e-kirjade võltsimise tuvastamist võimaldav meetod
SQL	*Structured Query Language*, enimkasutatav relatsiooniliste andmebaaside päringukeel
Sisuedastusvõrk	*Content Delivery Network*, piirkonniti laiali paigutatud puhverserverite võrk kindlate omadustega ja kiirusega teenuse tagamiseks
VPN	*Virtual Private Network*, virtuaalne privaatvõrk, mis potentsiaalselt ebaturvalisi kanaleid kasutades ühendab kahte või enamat otspunkti

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Käesoleva töö teemaks on DNS-põhiste kontroll- ja andmevahetuskanalite tuvastamine. Eksperimentidega luuakase erinevad DNS väärkasutuse stsenaariumid ja peale saadud tulemuste lisamist näidisandmestikule hinnatakse erinevate tuvastusvõimaluste efektiivsust.

1.1 Taust

Ettevõtted panustavad küberturvalisusele suuri summasid, ent sellele vaatamata toimub turbeintsidente, sealhulgas teenusetõkestusi ja andmevarguseid. Kui esimeste puhul on kahju suurus küllaltki kiiresti ja selgepiiriliselt määratletav, siis andmevargustega on keerulisem, kuna sageli võtab andmevarguse tuvastamine kaua aega ning näiteks mainekahjul võib olla väga pikaajaline mõju.

DNS on informatsiooni edastamise paindlikkuse ja ülimalt laia leviku tõttu väga hea kanal märkamatuks andmevarguseks. Hierarhiline ülesehitus, kus reeglina iga tase on erineva osapoole kontrolli all, loob ideaalse võimaluse protokolli väärkasutuseks. Antud valdkonda on viimase kümnendi jooksul küllaltki põhjalikult uuritud, kuid liialt vähe tähelepanu on pööratud DNS-põhist andmevahetust kasutavale pahavarale.

1.2 Probleem

DNS on hierarhiline süsteem, kus reeglina iga tase on erineva osapoole kontrolli all. See võimaldab DNS serveri haldajal andmetega manipuleerida ja protokolli väärkasutamist viisil, kus päringute ja vastuste struktuur on spetsifikatsiooniga vastavuses. See omakorda muudab väärkasutamise tuvastamise keeruliseks ja niimoodi on võimalik DNS-põhiste kontroll- ja andmevahetuskanalite abil märkamatult mööduda (ettevõtte) tulemüürist ja teistest turvameetmetest. Peamised kasutuskohad on pahavara kontrollkanal või andmevargus, vähemal määral ka tavaline VPN ühendus.

1.3 Eesmärk

Töö eesmärgiks on luua metoodika, mis võimaldab eristada DNS protokolli väärkasutust legitiimsetest päringutest, on lihtsasti juurutatav ja tagab sealjuures madala valepositiivsete tuvastuste arvu. Eriline rõhk on pahavara kontrollkanalitel ja spetsiifilise andmevarguse andmevahetuskanalitel, kuna nende poolt algatatud DNS päringute arv on märkimisväärselt väiksem võrreldes DNS protokolli põhise VPN ühendusega ning on seetõttu märkimisväärselt keerulisem tuvastada.

1.4 Ülevaade tööst

Töö teine peatükk annab ülevaate DNS-põhistest kontroll- ja andmevahetuskanalitest ning nende toimimisest, DNS päringute ja vastuste omadustest, teemaga seotud varasematest uurimustöödest ning antud valdkonnas eksisteerivatest kommertslahendustest.

Kolmas peatükk kirjeldab töö metoodilist olemust, annab ülevaate töös kasutatud DNS päringuid iseloomustavatest omadustest, kontroll- ja andmevahetuskanalite tuvastamise meetoditest ja näidisandmestikust.

Neljandas peatükis sisaldub DNS-põhist andmevahetust kasutavate tarkvarade ja testkeskkonna kirjeldus ning testkeskkonnas analüüsistsenaariumite loomiseks läbiviidud eksperimentide ülevaade ja tulemused.

Viiendas peatükis analüüsib autor erinevate DNS-põhiste kontroll- ja andmekanalite tuvastamise võimaluste efektiivsust.

Viimane peatükk esitab kokkuvõtvalt töö tulemused.

2 Teoreetiline taust ja seotud initsiatiivid

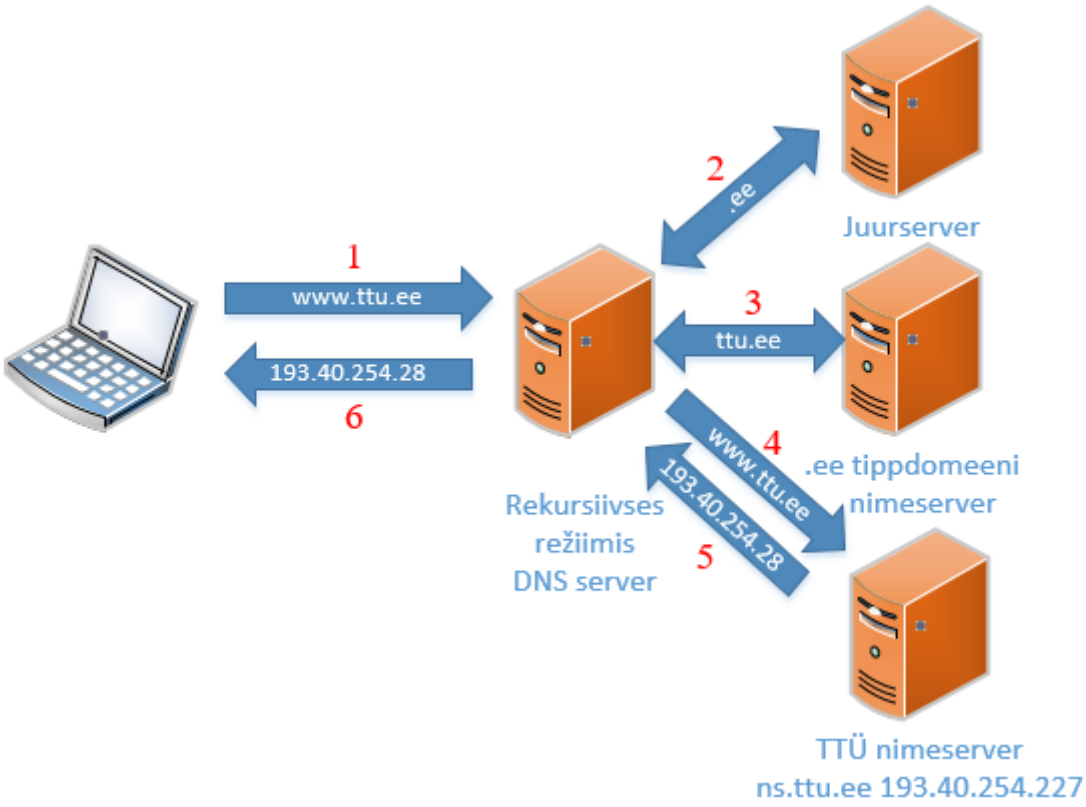
Käesolev peatükk annab ülevaate DNS-põhistest kontroll- ja andmevahetuskanalitest ning nende toimimisest, DNS päringute omadustest, teemaga seotud uurimustöödest ja kommertslahendustest.

2.1 DNS-põhiste kontroll- ja andmevahetuskanalite ülevaade

DNS on arvutivõrkude kriitiline protokoll ja teenus, mille peamine eesmärk on võimaldada IP-aadresside asemel kasutada domeeninimesid, kuna viimaseid on inimestel tunduvalt lihtsam meeles pidada. DNS hõlmab endas üle 30 kirjetüübi, enimkasutatav on neist A-tüüpi kirje, mis kirjeldab vastavuse domeeninime ja IPv4-aadressi vahel, IPv6-aadressi puhul täidab sama rolli AAAA-tüüpi kirje. [1] SPF (*Sender Policy Framework*) tarvis kasutatakse TXT-tüüpi kirjeid, mis andmetüübilt sarnanevad sõnega ja võivad olla kuni 255 tähemärki pikad [2].

DNS on hierarhiline süsteem, kus reeglina iga tase on erineva osapoole kontrolli all. Nimelahendus käib samm-sammult ja algab tippdomeenist (näiteks „.ee“). Tippdomeenide kirjeid hoitakse juurtsoonis, mida teenindavad DNS juurserverid. Juurserverilt saadud vastus sisaldab konkreetse tippdomeeni nimeserverite aadresse, kuhu edastatakse 2. taseme domeeni päring (näiteks „.ttu“). Saadud vastus sisaldab 2. taseme domeeni nimeserverite aadresse, mis omakorda hoiavad kirjeid konkreetse 2. taseme domeeni alamdomeenide ja võrgunimede kohta. [1] Kuna 2. (ja madalama) taseme domeeni teenindavate nimeserverite valik on domeeni registreerinud füüsilise või juriidilise isiku kontrolli all, siis on võimalik kasutada modifitseeritud tarkvaraga DNS serverteenust ja päringutele antavate vastustega manipuleerida. DNS-põhiste kontroll- ja andmevahetuskanalite puhul kapseldatakse järgmine OSI raammudeli [1] rakenduskihi protokoll või edastatav informatsioon DNS päringutesse ja vastustesse, seega on neid kanaleid käesolevas töös ja mujal kirjanduses lihtsustatult ka DNS tunneliteks nimetatud. DNS tunnelite tuvastamise teeb keerukaks asjaolu, et päringute ja vastuste struktuur on spetsifikatsiooniga vastavuses. Joonisel 1 on lihtsustatud näide, kus tööjaamast saadeti

DNS päring sisuga „www.ttu.ee“, kuidas antud päring liikus DNS serverite hierarhiat mööda Tallinna Tehnikaülikooli nimeserverini ning kuidas viimane andis vastuseks IP-aadressi 193.40.254.28.



Joonis 1. DNS päringu lihtsustatud näide

Lihtsustatud näide DNS-põhist andmevahetust kasutavast pahavarast on järgmine: päringu sisu „www.ttu.ee“ asendatakse väärtusega „krediitkaardi-number.ttu.ee“, joonisel kujutatud ahel jääb samaks ning päring (ja selles sisalduv informatsioon) jõuab endiselt TTÜ nimeserverini. Viimane võib vastata TXT-tüüpi kirjega, et kinnitada informatsiooni kättesaamist ning anda pahavarale järgmiseid juhiseid.

2.2 DNS päringute ja vastuste omadused

Varem läbiviidud uurimustööd ja eksperimendid on keskendunud järgmistele DNS päringute ja vastuste omadustele:

1. domeeninime entroopia [3], [4], [5], [6], [7]
2. domeeninime (päringu) pikkus [3], [6], [7]
3. päringu kirjetüüp (A, AAAA, TXT jms) [3], [4], [5]
4. liikluse maht 2. taseme domeeni kohta [5], [7]
5. unikaalsete alamdomeenide arv 2. taseme domeeni kohta [3], [8]
6. päring saadetakse avalikule DNS serverile [5]
7. domeeni nimekirjete ajalugu [5]
8. liikluse maht kliendi (IP-aadressi) kohta [5]
9. NXDOMAIN vastuste arv [5]
10. päringu ja vastuse suuruse suhe [5]
11. päringu suurus [4]
12. päringud, mille ei järgne võrguliiklust [5]
13. päringus esinevad sõnad [3]
14. päringus esinevate suur- ja väiketähtede ning numbrite jaotus [6]
15. päringute ajaline intervall [4]
16. päringute arv ühe kliendi (IP-aadressi) kohta [5]
17. spetsiifilised signatuurid [5]
18. unikaalsete päringute maht [3]

2.3 Seotud uurimustööd

Antud teemat on käsitletud mitmes uurimustöös, ühed viimased ja silmapaistvamad neist kasutavad binaarse klassifikatsiooni ja masinõppe meetodeid. Esimesel juhul uuriti ainult DNS-põhiseid andmevahetuskanaleid, teisel juhul kaasati ka pahavara, mille tuvastamine on keerukam.

DNS päringute ja vastuste omadustel põhinev binaarne klassifikatsioon

Binaarne klassifikatsioon põhineb neljal DNS päringute ja vastuste omadusel: päringute ajaline intervall, päringu suurus, domeeninime entroopia ja päringu kirje tüüp. Uuriti nelja DNS tunneli tarkvara: dns2tcp, dnscat2, iodine ja OzymanDNS. Analüüsi kaasati 1000

legitiimset päringu-vastuse paari ja iga tunneli tarkvara poolt genereeritud 1000 päringu-vastuse paari. Andmestik kattis tunnise vahemiku, mille jooksul legitiimne liiklus sisaldas 70-80% A-tüüpi kirjeid ja 8-10% AAAA-tüüpi kirjeid. DNS tunneli tarkvarad kasutasid suurema kanali läbilaske huvides teistsuguseid kirjete tüüpe. Eksperimendi käigus saavutati DNS tunnelite tuvastamise 99,98% positiivne ennustusvõime ja 99.93% täielikkus. Järeldati, et tunnelite tuvastamisel on oluline vaid päringu suurus, vastuse suurus ei ole. [4]

Masinõpe

Masinõppe meetodi puhul kaasati järgmised DNS päringute ja vastuste omadused: entroopia, päringu kirje tüüp, unikaalsete päringute arv ja unikaalsete päringute maht 2. taseme domeeni kohta, keskmine päringu pikkus ja pikim päringus sisalduv sõna. Uuriti nelja DNS-põhist andmeedastust kasutavat tarkvara: iodine, dns2tcp, FrameworkPOS ja Backdoor.Win32.Denis. Meetodi loomisel välistati statistiliste omaduste (näiteks sagedused, keskmised) kasutamine - nii on õpetatud mudel kasutatav igasuguse suurusega keskkonnas. Meetod põhineb kahel eeldusel:

1. tunnelite andmevahetus on legitiimsete päringutega võrreldes anomaalne - päringute ja vastuste ajaline kestvus on suurem, päringute sisu on kodeeritud ja unikaalsete päringute arv on suur,
2. pahavara kasutab ainult ühte 2. taseme domeeni.

Meetod tuvastas kõikide uuritud tarkvarade päringud ja andis samal ajal väga madala valepositiivsete tuvastuste osakaalu – peale kahepäevast õppeperioodi kuni üks uus domeen ööpäevas. [3] Masinõppega DNS tunnelite tuvastamist on eksperimenteeritud ka varem, kuid mitte nii heade tulemustega [9], [10].

2.4 Kommertslahendused

DNS-põhist andmeedastust kasutavad tarkvarad eksisteerivad juba üle kümnendi, seega on turul mitmeid kommertslahendusi, mis sellist protokolli väärkasutamist tuvastada ja blokeerida suudavad.

Dokumentatsiooni põhjal on kõige täiuslikum Palo Alto tulemüüri operatsioonisüsteemi PAN-OS sisse ehitatud tuvastusmehhanism, mis analüüsib päringute arvu, entroopiat ja päringu DNS tunneli mustritele vastavust [11]. DNS tunnelite tuvastamine on toetatud ka

tööjaamadesse ja serveritesse paigaldatava pahavaratõrje poolt, kuid täpsemaid toimemehhanisme pole avaldatud [12].

Cisco Umbrella DNS tunnelite tuvastamise lahendus põhineb reaalajas heuristikal, signatuuridel ning kodeeritud andmete ja ebahariliku kirjetüübi kasutuse tuvastamisel [13]. Tuvastamise võimekust pakuvad ka Comodo [14] ja Check Point [15], kuid nende puhul pole täpsemaid tuvastusmehhanisme avaldatud.

3 Metoodika

Käesolev peatükk kirjeldab näidisandmestiku analüüsimisel kasutatud DNS päringute omadusi, DNS tunnelite tuvastamise meetodeid, näidisandmestiku omadusi ja näidisandmestiku analüüsi protsessi.

3.1 DNS päringuid iseloomustavad omadused

DNS päringute omaduste valikul lähtuti nende efektiivsusest varasemate uurimustööde korral ning näidisandmestiku eripärast. Analüüsi käigus uuriti järgmisi omadusi:

1. domeeninime entroopia,
2. domeeninime pikkus,
3. unikaalsete alamdomeenide arv 2. taseme domeeni kohta,
4. päringute arv ühe kliendi (IP-aadressi) kohta,
5. päringus esinevate alamdomeenide arv.

Lisaks valitutele on teistes uurimustöödes sageli kasutatud päringu kirjetüüpi ja päringu-vastuse paari, kuid käesolevas töös polnud see võimalik, kuna logihaldussüsteem ei võimalda DNS serveritest vastava informatsiooni kogumist.

Domeeninime entroopia

Kõige levinumaks DNS tunnelite tuvastusmeetmeks läbi aegade on domeeninime sõne entroopia. Reeglina kasutatakse Shannoni entroopiat, mis on sisuliselt informatsiooni hulga mõõt [16]. Järelikult peab informatsiooni hulga suurenedes suurenema ka entroopia. DNS päringu ja vastuse ajaline viide on tavapärase võrguliiklusega võrreldes suur, seega efektiivse DNS tunneli puhul tuleb ühte päringu-vastuse paari mahutada võimalikult palju informatsiooni.

Legitiimsed päringud sisaldavad sageli madala entroopiaga inimkeelseid sõnu, sest madalama informatsiooni hulga tõttu on inimestel neid lihtsam meeles pidada [17]. Oluliseks erandiks on sisuedastusvõrgud, mis kasutavad koormuse juhtimiseks [18] programmiliselt koostatud domeeninimesid ja sarnanevad niimoodi pahavara käitumismustritele [19].

Domeeninime pikkus

Domeeninime pikkus on samuti antud teemal erinevates uurimustöödes palju kajastamist leidnud ja efektiivseks osutunud. Nagu selgitatud domeeninime entroopia kirjelduses, siis efektiivse DNS tunneli jaoks peab olema ühte päringusse (või vastusesse) mahutatud võimalikult palju informatsiooni, mis omakorda suurendab päringu pikkust.

Unikaalsete alamdomeenide arv 2. taseme domeeni kohta

DNS päringuga (ja vastusega) on võimalik dünaamiliselt informatsiooni edastada ainult 3. ja madalama taseme alamdomeenide sõnedega. See omakorda tähendab, et kui muutub edastatav informatsioon, siis muutub ka päringu sisu. Suur arv unikaalseid alamdomeene on otsene märk, et domeeniga on seotud mahukas andmevahetus.

Päringute arv ühe kliendi (IP-aadressi) kohta

Arvutivõrgus olevatel seadmetel on reeglina kindlad käitumismustrid. Ühelt kliendilt (IP-aadressilt) kindla ajavahemiku jooksul saabunud päringute arvu mitmekordistumine määratud ajaaknas võib olla märk DNS tunneli kasutamisest.

Päringus esinevate alamdomeenide arv

Päringus esinevate alamdomeenide arvu pole autorile teadaolevalt varem DNS tunnelite tuvastamiseks edukalt kasutatud. Uue alamdomeeni tekkimiseks on vaja päringusse lisada punkt, sõltuvalt tarkvara lähtekoodist ja andmete kodeerimisest võib see olla vägagi triviaalne ülesanne – see on ka tõenäoline seletus, miks antud lähenemine pole kajastamist leidnud. Siiski on antud võimalust käesolevas töös uuritud.

3.2 Kontroll- ja andmevahetuskanalite tuvastamise meetodid

Käesolevas töös kasutatud kontroll- ja andmevahetuskanalite tuvastamise meetodid jagunevad kaheks:

1. olekuta – järelduste tegemine üksiku päringu omaduste põhjal,
2. olekupõhised – järelduste tegemine päringute kogumi ja nende omaduste põhjal.

Olekuta tuvastusmeetodi kasutatavateks päringu atribuutideks on epoch-i ajatempel, domeeninimi ja päringu sooritanud seadme IP-aadress. Olekuta tuvastusmeetodi eeliseks on kiirus, kuna meetod suudab otsuse langetada ühe päringu põhjal ja ei ole vajalik oodata

järgmiste päringute saabumist. Vaadeldes ühte päringut eraldiseisvalt ei oma tähtsust päringu sooritamise aeg ega päringu sooritanud seadme IP-aadress, seega ainsaks kasutatavaks atribuudiks on domeeninimi.

Olekupõhised tuvastusmeetodid põhinevad päringute kogumi statistilistel omadustel ja eeldavad tuvastusmehhanismilt teatud oleku säilitamist, näiteks konkreetse 2. taseme domeeni alamdomeenide arvu üle arvestuse pidamist. Olekupõhiste tuvastusmeetodite eeliseks on võimalus hinnata arvutivõrgu käitumismustrit pikema perioodi jooksul, näiteks alamdomeenide arvu mitmekordistumine kindlas ajaaknas võib olla märk aktiivsest DNS tunnelist.

Kumbki meetod eraldiseisvalt ei andnud soovitud tulemus, seega on täiendavalt kasutatud mõlema meetodi kombinatsioone.

3.3 Näidisandmestiku kirjeldus

Näidisandmestik on kogutud umbes 3000 arvutitöökohaga ettevõtte võrgust 14 päevase perioodi vältel. Selles sisaldub kokku 75993134 unikaalset kirjet, maht avatekstina 3,68 gigabaiti. Lihtsamaks töötlemiseks grupeeriti kirjed 14sse faili, igas faili 24 tunnise perioodi kirjed. Esimese kirje ajatempel on 1552824001 (17. märts 2019 12:00:01), viimase kirje ajatempel on 1554033600 (31. märts 2019 12:00:00).

Kirjete struktuur on järgmine: päringu aeg (epoch ajatempel), päringu sooritanud seadme IP aadress, päritud domeeninimi. Näidiskirjetena on esitatud iga faili esimene rida:

1552824001 10.12.25.171 pool.ntp.org
1552910400 10.0.24.152 i.ytimg.com
1552996801 10.0.29.54 _sip._udp.proxy.elion.ee
1553083200 10.0.209.111 nimbus.bitdefender.net
1553169601 10.12.1.57 cdn.samsungcloudsolution.com
1553256000 192.168.133.65 elb-fra-amz.nimbus.bitdefender.net
1553342401 10.0.210.58 vsd53.mycdn.me
1553428800 10.0.210.53 v20.vortex-win.data.microsoft.com
1553515201 10.0.42.15 nimbus.bitdefender.net
1553601600 10.0.210.58 ocsp.pki.goog
1553688001 10.0.26.147 files.acrobat.com

1553774400 10.0.29.146 v20.vortex-win.data.microsoft.com

1553860801 10.0.22.51 outlook.office365.com

1553947200 10.10.1.51 nexus.officeapps.live.com

Märkimisväärse osa mahust moodustasid sisemiste ressursside päringud, kuid kuna need domeenid on ettevõtte kontrolli all, siis pole nendega võimalik DNS tunneleid luua ning need eemaldati näidisandmestikust koos teiste ettevõttele kuuluvate domeenidega (unikaalsete kirjete arv kajastab seisu peale kirjeldatud tegevust). Autorile teadaolevalt ei sisalda näidisandmestik DNS tunneleid või muud sarnasele DNS protokolli väärkasutusele viitavaid päringuid.

4 Eksperimendid

Eksperimentide peatükis on kirjeldatud testkeskkond, analüüsiks kasutatud andmebaas, eksperimentide näidisandmestikule lisamise protseduur ning loetletud DNS-põhist andmeedastust kasutavad ja analüüsistsenaariumite loomiseks valitud tarkvarad.

4.1 Testkeskkond

Testkeskkonnas pole samad tingimused, mis internetis - latentsus on märkimisväärselt väiksem ja sisuliselt puudub paketikadu. Samas on testkeskkonnal eeliseid – ei tekitata asjatut koormust avalikele nimeserveritele ning eksperimentidega saadud tulemused on korratavad ja võrreldavad. Avalikke nimeservereid kasutades sõltuvad tulemused nii nimeserverite koormusest kui ka serverite ja kliendi omavahelisest andmesidekanali ribalaiusest ja latentsusest. Samas on madal latentsus ka puuduseks, kuna seab piirangud päringute ajaliste omaduste uurimisele.

Testkeskkond koosneb kolmest virtuaalmasinast: DNS tunneli klient, DNS tunneli server ja sisevõrgu DNS server. Viimane on konfigureeritud rekursiivsesse režiimi, kus päringut ei edastata mitte mõnele järgmisele DNS serverile, vaid nimelahendus toimub juurservereid kasutades samm-sammult alustades tippdomeeni ning lõpetades konkreetse (alam)domeeni nimeserverile päringu saatmisega. DNS tunnelite tarvis on kasutusel domeen nimega „domeen.tld“. Kuna „tld“ tippdomeeni ei eksisteeri, siis juurserver annaks päringule vastuse „NXDOMAIN“, mis tähendab, et domeeni ei eksisteeri. Antud olukorra vältimiseks on sisevõrgu DNS serveris tehtud seadistus, kus kõik „domeen.tld“ päringud edastatakse DNS tunneli serverisse.

Kasutatud virtuaalmasinad ja nende parameetrid on esitatud tabelis 1. Iga tunneli tarkvara testimiseks oli kasutusel omaette komplekt virtuaalmasinaid. Ühesuguste baasseadistuste tagamiseks on kõik virtuaalmasinad loodud mallidest.

Tabel 1. Testkeskkonna virtuaalmasinate parameetrid

Virtuaalmasina eesmärk	**Operatsioonisüsteem**	**IP-aadress**
DNS tunneli klient	Windows 10	10.0.0.4
DNS tunneli server	Debian 9	10.0.0.3
DNS server	Windows Server 2019	10.0.0.2

Peamisteks DNS tunnelite tuvastamise ajenditeks on vältida andmevargusi ja suhtlust pahavara juhtserveritega. Esimesega kaasneb reeglina suur andmevoog ettevõtte võrgust väljapoole, teisel juhul on edastatavaid andmeid märksa vähem - selle alusel on valitud ka testkeskkonna tunnelis edastatavad andmed, milleks on Eesti Keele Instituudi kodulehelt pärinevad tekstikorpused ja Linuxi */dev/random* virtuaalseadme väljund. Andmeülekande suund on DNS tunneli kliendi perspektiivist ehk allalaadimisel liikusid andmed kliendi suunas ja üleslaadimisel serveri suunas. Kokkuvõtlikult on andmefailide omadused kirjeldatud tabelis 2.

Tabel 2. Testkeskkonna andmefailide kirjeldus

Allikas	**Failinimi**	**Suurus**	**Tegevus**
EKI	1.txt	203 baiti	Allalaadimine
EKI	2.txt	707 baiti	Allalaadimine
EKI	3.txt	203 baiti	Üleslaadimine
EKI	4.txt	3,16 kilobaiti	Üleslaadimine
EKI	5.txt	1425 kilobaiti	Üleslaadimine
/dev/random	6.dat	2000 kilobaiti	Üleslaadimine
/dev/random	7.dat	2000 kilobaiti	Allalaadimine

Faili ülekannet alustati 10 sekundit peale DNS tunneli käivitumist ja tunnel suleti 5 sekundit peale faili ülekande lõppu. Protsessi korrati sarnaselt kõikide failidega iga DNS tunneli tarkvaraga ning erinevate tunneli seadistustega. Peale igat faili ülekannet kontrolliti failide terviklust räside võrdlemisega.

Testkeskkonnas kogutud andmed lisati näidisandmestikule viisil, kus päringute omavahelised ajad jäid muutumatuks, kuid oli võimalik valida, mis ajahetkel tunnel aktiveerub. Antud protsessi on pikemalt kirjeldatud peatükis „4.4 Testkeskkonna tulemuste lisamine näidisandmestikule“.

4.2 DNS protokolli kontroll- või andmevahetuskanalina kasutavad tarkvarad

Käesolevas peatükis on ülevaade tarkvaradest, mis kasutavad DNS protokolli kontroll- või andmevahetuskanalina. Nimekiri ei ole täielik, eksisteerib täiendavaid hobikorras loodud tarkvaraarendusprojekte ja ka pahavara osas on nimekiri ajas täienev.

DeNiSe on programmeerimiskeeles Python kirjutatud rakendus, mis võimaldab edastada TCP pakette DNS protokolli abil. Viimane versioon pärineb aastast 2006. [20]

dns2tcp on kirjutatud Olivier Dembour ja Nicolas Collignon poolt C programmeerimiskeeles Linuxi platvormile, lisaks on klient Windows platvormile. Viimane versioon pärineb aastast 2012. [21]

DNScapy on kirjutatud Pierre Bienaime poolt ja võimaldab luua SSH ühenduse kasutades DNS protokolli andmevahetuskanalina. Viimane versioon pärineb aastast 2011. [22]

DNScat esmaversioon valmis aastal 2004 ja tarkvara autoriks on Tadeusz Pietraszek. Programmeerimiskeeleks on Java ja toetatud on UNIXi-laadsed süsteemid. Viimane versioon pärineb aastast 2005. [23]

DNScat nime kannab ka teine tarkvara, mille autor on Ron Bowes. Toetatud on Linux, Mac OS ja Windows platvormid. Viimane versioon pärineb aastast 2010. [24]

dnscat2 on 2010. aastal valminud DNScat tarkvara edasiarendus sama autori poolt. Viimane versioon valmis aastal 2016, kuid hiljem on tehtud mitmeid kooditäiendusi. [25]

fraud-bridge on kirjutatud C programmeerimiskeeles ja toetatud on Linux platvorm. Viimane versioon pärineb aastast 2013. [26]

Hexify on ettevõtte Infoblox, Inc. poolt arvutivõrkude turbetestimiseks arendatud tööriist. Viimane versioon pärineb aastast 2016. [27]

Heyoka autoriteks on Alberto Revelli ja Nico Leidecker. Tarkvara on kirjutatud C programmeerimiskeeles ja toetatud on Windows platvorm. Viimane versioon pärineb aastast 2012. [28]

iodine autoriteks on Bjorn Andersson ja Erik Ekman. Tarkvara on kirjutatud C programmeerimiskeeles ja toetatud on Linux, Mac OS ja Windows platvormid. Esmaversioon pärineb aastast 2010, viimane versioon aastast 2018 ning peale seda on tehtud mitmeid kooditäiendusi. [29]

NSTX autoriteks on Florian Heinz ja Julien Oster was released in 2000. Toetatud on Linux platvorm. Viimane versioon pärineb aastast 2002. [30]

OzymanDNS autoriks on Dan Kaminsky. Tarkvara on kirjutatud Perl programmeerimiskeeles ja võimaldab luua SSH ühenduse kasutades DNS protokolli andmevahetuskanalina. Viimane versioon pärineb aastast 2004. [31]

psudp autoriks on Kenton Born. Tarkvara üritab märkamatuks jäämise eesmärgil modifitseerida legitiimseid DNS päringuid. Viimane versioon pärineb aastast 2010. [32]

SplitBrain on modifitseeritud versioon tarkvarast OzymanDNS. Viimane versioon pärineb aastast 2008. [33]

Squeeza autoriteks on Marco Slaviero ja Haroon Meer. Tegu on SQL andmebaaside ründamiseks loodud tarkvaraga, mis kasutab ühe andmevahetuskanalina DNS protokolli. Viimane versioon pärineb aastast 2008. [34]

tcp-over-dns on kirjutatud Java programmeerimiskeeles ja toetatud on Linux, Solaris ja Windows platvormid. Viimane versioon pärineb aastast 2008. [35]

TUNS autoriks on Lucas Nussbaum ja tarkvara on kirjutatud Ruby programmeerimiskeeles. Viimane versioon pärineb aastast 2009. [36]

Your Freedom on VPN teenus, mis muuhulgas võimaldab andmevahetuskanalina kasutada DNS protokolli. Tarkvara viimane versioon pärineb aastast 2019. [37]

DNS-põhiseid kontroll- ja andmevahetuskanaleid kasutavad järgmised pahavarad:

1. OilRig [38]
2. DNS_TXT_Pwnage [38]
3. DNSMessenger [38]
4. Feederbot [39]
5. Moto [27]
6. Morto [27]
7. FrameworkPOS [27]
8. PlugX [27]
9. Win32.Zbot.chas/Unruy.H [27]
10. Win32.Mufanom.vha [27]
11. Win32.AutoTsifiri.n [27]
12. Win32.Hiloti [27]

4.3 Analüüsistsenaariumite loomiseks kasutatud tarkvarad

Analüüsistsenaariumite loomiseks kasutatud DNS tunneli tarkvarade valikul lähtuti järgmistest tingimustest:

1. tarkvara töötab isoleeritud testkeskkonnas,
2. tarkvara peab töötama Windows platvormil,
3. tarkvara viimane versioon pole vanem kui kolm aastat.

Pahavarade puhul kasutati neid näidiseid, mis olid autorile kättesaadavad. Nendeks olid FrameworkPOS, OilRig ja Poison Frog. Kõigi kolme näol on tegu pahavaradega, mis kasutavad DNS päringuid kontrollkanalina ja peale tarkvara käivitamist üritavad luua ühendust juhtserveriga.

4.3.1 dnscat2

dnscat2 võimaldab andmeid edastada nii avatekstina kui ka krüpteeritult. Tabelis 3 on esitatud mõlemat võimalust iseloomustavad tulemused kõikide ülekantud failide kaupa. Andmefaili nime järel sulgudes on failiga tehtud toiming (AL ehk allalaadimine, ÜL ehk üleslaadimine).

Tabel 3. dnscat2 failiülekande tulemused

	Päringute arv			**Entroopia**		
Andmefail	**Avatekst**	**Krüpteeritud**	**Erinevus %**	**Avatekst**	**Krüpteeritud**	**Erinevus %**
1.txt (AL)	27	33	22,22	4,0572	4,0676	0,26
2.txt (AL)	36	41	13,89	3,9206	4,0941	4,43
3.txt (ÜL)	28	29	3,57	3,8416	4,0771	6,13
4.txt (ÜL)	55	61	10,91	3,8029	4,1151	8,21
5.txt (ÜL)	14065	15314	8,88	3,7072	4,1288	11,37
6.dat (ÜL)	19507	21316	9,27	4,1287	4,1285	0,00
7.dat (AL)	19679	21330	8,39	3,9734	4,0767	2,60

Krüpteeritud andmetega tunneli puhul on päringute arvu kasv kõikide failidega tehtud toimingute lõikes 11,02%, entroopia suurenes keskmiselt 4,71%. Väikseim entroopia väärtusega 3,7072 oli faili 5.txt avatekstina üleslaadimisel.

4.3.2 iodone

iodine ei paku andmete krüpteerimise funktsionaalsust, seega kui tunnelit kasutav rakendus andmeid ei krüpteeri, siis edastatakse need avatekstina. Parameetriga „–M“ saab määrata päritavate domeeninimede maksimaalse pikkuse (vaikimisi 255 sümbolit). Antud piiramine muudab tunneli stabiilsemaks, minimaalne kasutatav väärtus on vastavalt dokumentatsioonile ligikaudu 100. [29]

Tabelis 4 on esitatud iodine tunneleid iseloomustavad tulemused kõikide ülekantud failide kaupa vastavalt parameetri „-M“ väärtustele. Andmefaili nime järel sulgudes on failiga tehtud toiming (AL ehk allalaadimine, ÜL ehk üleslaadimine).

Tabel 4. iodine failiülekande tulemused

Andmefail	Päringute arv			Entroopia		
	-M 255	**-M 100**	**Erinevus %**	**-M 255**	**-M 100**	**Erinevus %**
1.txt (AL)	24	31	29,17	4,3363	4,3536	0,40
2.txt (AL)	24	32	33,33	4,3014	4,4480	3,41
3.txt (ÜL)	23	31	34,78	4,3654	4,3669	0,03
4.txt (ÜL)	35	68	94,29	4,9361	4,9652	0,59
5.txt (ÜL)	7172	20010	179,00	5,6234	5,3650	-4,59
6.dat (ÜL)	14351	-	-	5,7541	-	-
7.dat (AL)	3941	3925	-0,41	4,2700	4,3919	2,85

Domeeninime pikkuse piiramisega on päringute arvu kasv kõikide failidega tehtud toimingute lõikes 61,69%, entroopia suurenes keskmiselt 0,45%. Erandiks on andmefaili 5.txt üleslaadimine, kus entroopia kahanes 4,59%. Parameetri „-M“ väärtuse 100 korral andmefaili 6.dat üleslaadimine ebaõnnestus.

4.3.3 FrameworkPOS pahavara

FrameworkPoS on põhjalikult dokumenteeritud pahavara, mis ründab kassasüsteeme ja mida on kasutatud vähemalt ühe suure andmevarguse läbiviimisel. Tarkvara autor(id) on pahavara parendamist jätkanud ning sellest eksisteerib mitu erinevat versiooni. [40]

Antud tarkvaral puuduvad parameetrid ja see ei võimaldanud failide ülekannet, seega jälgiti, kuidas pahavara üritab luua ühendust juhtserveriga. Sessiooni kestuseks oli 15 minutit, mille jooksul sooritas tarkvara 10 päringut. FrameworkPOS puhul on realiseeritud mehhanism, mille tõttu ei sooritata samas arvutis teistkordsel käivitamisel enam DNS päringuid ja protsess lõpetab töö kohe peale käivitamist. Tõenäoliselt on tegu katsega vältida analüüsi niinimetatud liivakasti keskkonna poolt – tegu on pahavarade puhul tavapärase käitumismustriga.

4.3.4 OilRig rühmituse pahavara

OilRig arvatakse olevat Iraanist pärinev kuritegelik rühmitus, kelle sihtmärgid on peamiselt Lähis-Idas ja tegutseb alates aastast 2014. Rühmitus on rünnanud ohvreid mitmetest valdkondadest, sealhulgas valitsusi, pangandust, energiasektorit,

keemiatööstust ja telekommunikatsioonieттevõtteid. [41] Mitmed rühmituse loodud tööriistad kasutavad kontrollkanalina DNS-põhist andmeedastust [38].

Sarnaselt FrameworkPOS-le puuduvad ka antud tarkvaral parameetrid ja see ei võimaldanud failide ülekannet. Jälgiti, kuidas pahavara üritab luua ühendust juhtserveriga. Peale käivitamist sooritas pahavara 7 päringut teise taseme domeeni withyourface[.]com alamdomeenide poole ning kuna DNS serveri vastuseks oli „NXDOMAIN“, siis lõpetas pahavara protsess peale seitsme vastuseta jäänud DNS päringu saatmist töö. Loodi kolm komplekti näidisandmeid: pahavara käivitati ühe korra, pahavara käivitati tsüklis 10 korda ja pahavara käivitati tsüklis 100 korda. Logitud DNS päringute arvud olid vastavalt 7, 70 ja 696.

4.3.5 Poison Frog pahavara

Poison Frog tarkvara peamine funktsionaalsus on vastavalt juhtserveri korraldustele failide alla- ja üleslaadimine ning Powershell skriptide käivitamine. Tarkvara loob ajastatud töö ja käivitab end iga kümne minuti tagant. Igal käivitumisel sooritatakse DNS päring, mis annab juhtserverile pahavara käivitumisest märku ja seejärel päritakse serverilt järgmisi korraldusi. Juhtserveri antud käsud täidetakse ja tulemus saadetakse juhtserverile tagasi. [42]

Sarnaselt teistele pahavaradele puudusid ka Poison Frog puhul parameetreid ja failide ülekannet ei toimunud. Jälgiti, kuidas pahavara üritab luua ühendust juhtserveriga, sessiooni kestuseks oli 15 minutit. Päriti domeeni myleftheart[.]com ja selle alamdomeene, kokku sooritas pahavara 55 DNS päringut.

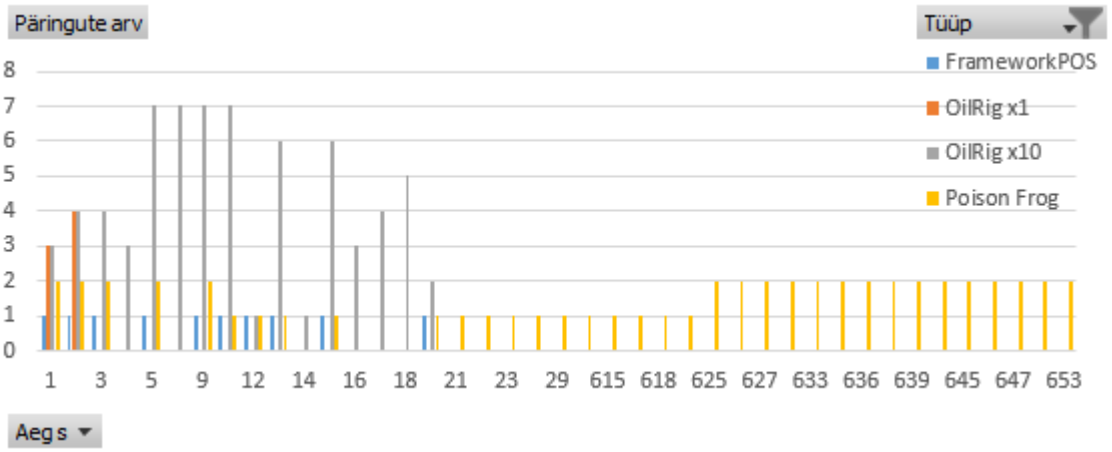
4.3.6 FrameworkPOS, OilRig ja Poison Frog tulemuste kokkuvõte

FrameworkPOS, OilRig ja Poison Frog käivitamise parameetrid (tegu pole pahavara protsessile antud parameetritega), sooritatud DNS päringute arvud ja keskmine entroopia on esitatud tabelis 5.

Tabel 5. FrameworkPOS, OilRig ja Poison Frog tulemuste kokkuvõte

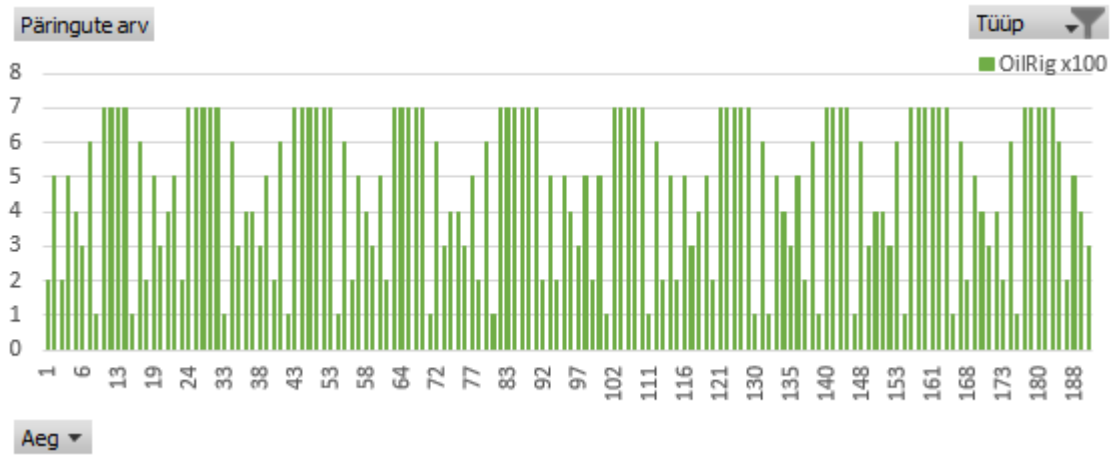
Tüüp	**Parameetrid**	**Päringute arv**	**Keskmine entroopia**
FrameworkPOS	15 min sessioon	10	4,4296
OilRig	Tsükkel 1x	7	4,5139
OilRig	Tsükkel 10x	70	4,5269
OilRig	Tsükkel 100x	696	4,6273
Poison Frog	15 min sessioon	55	4,1357

Päringute ajaline jaotus on kujutatud joonisel 2. Enamus pahavarasid sooritas DNS päringuid ainult esimese 20 sekundi jooksul. Erandiks oli Poison Frog, mis sooritas suurema osa päringuid peale 10 minutilist jõudeolekut.



Joonis 2. FrameworkPOS, OilRig ja Poison Frog päringute ajaline jaotus

OilRig sooritas 100 kordse tsüklina käivitades märkimiseväärselt rohkem DNS päringuid ja seega on loetavuse huvides antud päringute ajaline jaotus kujutatud eraldi joonisel 3.



Joonis 3. OilRig 100-kordse tsükli päringute ajaline jaotus

4.4 Testkeskkonna tulemuste lisamine näidisandmestikule

Testkeskkonnas kogutud andmed lisati näidisandmestikule skriptiga, mis võimaldas valida tunneli aktiveerumise aja, kuid seejuures jäi muutumatuks päringute omavaheline ajaline nihe. Tulemused lisati näidisandmestikule kahe erineva IP-aadressiga:

1. kasutati unikaalset IP-aadressi 10.0.0.4, mida näidisandmestikus ei esinenud,
2. kasutati IP-aadressi 192.168.136.171, mille DNS päringute arv langes kokku kogu näidisandmestiku päringute arvu mediaaniga IP-aadressi kohta.

Unikaalne IP-aadress võimaldab analüüsi ajal keskenduda ainult DNS-põhisele andmeedastusele, samas kui mediaan annab parema pildi nii-öelda „keskmisest“ arvutivõrgu seadmest. Keskmise päringute arvu asemel valiti mediaan seetõttu, et on süsteeme, mis sooritavad DNS nimepäringuid minimaalselt, näiteks kommutaatorid ja marsruuterid, samas on ka süsteeme, mis sooritavad väga palju päringuid, näiteks tulemüürid, kus reeglibaasis kasutatakse domeeninimesid – tulemüür peab sooritama nimelahendusi, et välja selgitada domeeninimele vastav IP-aadress. Minimaalne päringute arv IP-aadressi kohta oli 1, maksimaalne 15496380, mediaan 5895 ja keskmine 13149 päringut.

4.5 Andmebaasi kirjeldus

Andmete kiire analüüsi võimaldamiseks lisati need andmebaasi. Andmed indekseeriti ja need olid erinevate kriteeriumite alusel väga kiiresti otsitavad, samuti võimaldab andmebaasimootor mitmete agregeerimis- ja analüütiliste funktsioonide kasutamist.

DNS päringud on antud töös jaotatud vastavalt päringu sooritamise eesmärgile või päringu sooritanud tarkvarale järgmisteks tüüpideks:

1. dnscat2
2. dnslog
3. FrameworkPOS
4. iodine
5. OilRig
6. Poison Frog

Näidisandmestikus olnud kirjetel oli kolm atribuuti: päringu sooritamise epoch ajatempel, päritud domeeninimi ja päringu sooritanud seadme IP aadress. Need kolm atribuuti olid andmebaasi kirje lisamisel kohustuslikud – nende atribuutide puudumisel oleks olnud tegu vigase kirjega näidisandmestikus. Analüüsi lihtsustamiseks tekitati mitmeid liiasusega veerge, näiteks jaotati domeeninimi iga taseme alamdomeeni kaupa eraldi veergudesse. Indeksid lisati SQL päringutes sagedamini kasutatavatele veergudele. Andmebaasitabeli olemite omaduste detailne kirjeldus on esitatud lisas 1.

Näidisandmestikus sisaldus suurel hulgal kirjeid, mille analüüsi kaasamine oleks andnud valed tulemused. Enamuse neist moodustas spetsiifilise iseloomuga võrguseadmete või teenuste poolt sooritatud päringud, samuti esines märkimisväärsel hulgal päringuid, mis ei sisaldanud avalikku tippdomeeni. Analüüsi lihtsustamiseks lisati tabelisse veerg *skip*, mis võimaldab ühe SQL päringu tingimusega neid kirjed analüüsil mitte kasutada. Veeru *skip* väärtused ja nende kirjeldused on esitatud tabelis 6. Mitteavalike domeenide välistamiseks kasutati IANA tippdomeenide loendit [43].

Tabel 6. Tabeli *skip* väärtused koos kirjeldusega

Veeru skip väärtus	**Kirjeldus**	**Päringute arv**
0	Kirje kaasatakse analüüsimiseks	60498800
1	Päring ei sisalda avalikku tippdomeeni	321734
2	IP aadress(id), mille päringuid ei analüüsita	13365896
3	Päring ei sisalda avalikku tippdomeeni ja päringu sooritas seade, mille päringuid ei analüüsita	2130484

5 Analüüs

Näidisandmestiku ja testkeskkonna tulemuste liitmisel saadud andmestiku analüüsil kasutati olekuta ja olekupõhiseid tuvastusmeetodeid. Esimesel juhul on järelduste tegemine võimalik üksiku päringu omaduste põhjal, teisel juhul vaadeldakse päringute kogumit ja nende omadusi.

5.1 Olekuta tuvastusmeetodid

Olekuta tuvastusmeetodite puhul vaadeldi järgmisi omadusi: entroopia, päringus esinevate alamdomeenide arv ja domeeninime pikkus (sealhulgas alamdomeenide pikkus ilma 1. ja 2. taseme domeenita).

5.1.1 Entroopia

Entroopia arvutatakse päringus oleva täispika domeeninime sõne põhjal. Tabelis 7 on vastavalt erinevatele parameetrile esitatud iga tüübi minimaalne, keskmine ja maksimaalne entroopia. Iga tüübi puhul on esile toodud kõige väiksem keskmine entroopia.

Tabel 7. Päringute entroopia väärtused vastavalt tüübile ja parameetritele

Päringu tüüp	**Andmefail**	**Parameetrid**	**Entroopia**		
			Minimaalne	**Keskmine**	**Maksimaalne**
dnscat2	1.txt	Krüpteeritud	3,8216	4,0676	4,2334
dnscat2	1.txt	Avatekst	3,3930	4,0572	4,2542
dnscat2	2.txt	Krüpteeritud	3,8915	4,0941	4,2356
dnscat2	2.txt	Avatekst	3,2421	3,9206	4,1852
dnscat2	3.txt	Krüpteeritud	3,9046	4,0771	4,2225
dnscat2	3.txt	Avatekst	3,0806	3,8416	4,0473
dnscat2	4.txt	Krüpteeritud	3,8098	4,1151	4,2969
dnscat2	4.txt	Avatekst	3,2224	3,8029	4,1163
dnscat2	5.txt	Krüpteeritud	3,9777	4,1288	4,2633
dnscat2	5.txt	Avatekst	3,1468	**3,7072**	4,2373
dnscat2	6.dat	Krüpteeritud	3,9105	4,1285	4,2502
dnscat2	6.dat	Avatekst	3,4048	4,1287	4,2373
dnscat2	7.dat	Krüpteeritud	3,6199	4,0767	4,3413
dnscat2	7.dat	Avatekst	3,2371	3,9734	4,3492
FrameworkPOS		15 min sessioon	4,3726	**4,4296**	4,4865
iodine	1.txt	-m 1130	3,3816	4,3363	5,7887
iodine	1.txt	-m 1130 -M 100	3,3006	4,3536	5,7582
iodine	2.txt	-m 1130	3,3372	4,3014	5,8263
iodine	2.txt	-m 1130 -M 100	3,3211	4,4480	5,7752
iodine	3.txt	-m 1130	3,3816	4,3654	5,8262
iodine	3.txt	-m 1130 -M 100	3,3006	4,3669	5,7856
iodine	4.txt	-m 1130	3,3816	4,9361	5,8862
iodine	4.txt	-m 1130 -M 100	3,3372	4,9652	5,7856
iodine	5.txt	-m 1130	3,3372	5,6234	5,9218
iodine	5.txt	-m 1130 -M 100	3,2608	5,3650	5,7752
iodine	6.dat	-m 1130	3,1953	5,7541	5,9356
iodine	7.dat	-m 1130	3,2158	**4,2700**	5,8515
iodine	7.dat	-m 1130 -M 100	3,0708	4,3919	5,7752
OilRig		Tsükkel 1x	4,4267	**4,5139**	4,7077
OilRig		Tsükkel 10x	4,3374	4,5269	4,7170
OilRig		Tsükkel 100x	4,4613	4,6273	4,8982
Poison Frog		15 min sessioon	3,5069	**4,1357**	4,3964

Kõige väiksem keskmine entroopia iga tunneli tüübi puhul:

1. dnscat2 - 3,7072
2. FrameworkPOS - 4,4296
3. iodine - 4,2700
4. OilRig - 4,5139
5. Poison Frog - 4,1357

Tabelis 8 on esitatud tingimustele vastavate päringute osakaal tüüpide lõikes erinevate entroopia väärtuste korral. Parameetritega tüüpide korral on valitud kõige madalama entroopia andnud seadistus – dnscat2 puhul andmefaili 5.txt edastamine avatekstina, iodine puhul andmefaili 7.dat edastamine parameetri „-M“ vaikeväärtuse korral ja OilRig pahavara puhul ühekordne käivitamine.

Tabel 8. Päringute osakaal vastavalt entroopia väärtusele

Tüüp/Entroopia	**3,7072**	**4,1357**	**4,2700**	**4,4296**	**4,5139**
dnscat2	48,67%	0,01%	0,00%	0,00%	0,00%
dnslog	23,99%	3,21%	2,55%	1,82%	1,48%
FrameworkPOS	100,00%	100,00%	100,00%	50,00%	0,00%
iodine	73,56%	34,08%	34,03%	34,03%	34,03%
OilRig	100,00%	100,00%	100,00%	85,71%	28,57%
Poison Frog	81,82%	72,73%	63,64%	0,00%	0,00%

Entroopia väärtus 3,7072 välistab märkimisväärse osa dnslog tüüpi päringutest, samas on teiste tüüpide puhul kaasatud päringute osakaal suur. Järgmise entroopia väärtuse korral langeb dnscat2 tüüpi päringute tuvastuse osakaal sisuliselt olematuks, seega ei võimalda 4,1357 ja kõrgemad entroopia väärtused enam kõikide tüüpide DNS tunnelite päringuid tuvastada.

Päringute osakaalust ülevaatlikum on 2. taseme domeeni arv, mis mingile entroopia väärtusele vastab. Selline jaotus on esitatud tabelis 9.

Tabel 9. 2. taseme domeeni arv vastavalt entroopia väärtusele

Minimaalne entroopia	**Päringute arv**	**2. taseme domeenide arv**	**Osakaal kõikidest 2. taseme domeenidest**
0,0000	60174748	112247	100,00%
3,7072	14432990	12663	11,28%
4,1357	1933062	567	0,51%
4,2700	1531634	267	0,24%
4,4296	1094028	125	0,11%
4,5139	889745	82	0,07%

Tabelite 8 ja 9 põhjal selgub, et minimaalse entroopia väärtuse 3,7072 puhul on 2. taseme domeenide arvu vähenemine märkimisväärselt suurem, kui antud tingimusele vastavate päringute osas. Siiski on antud tingimusele vastavate 2. taseme domeenide arv 12663 liialt suur, et seda hallata usaldusväärsete domeenide nimekirjaga. Usaldusväärsete domeenide nimekiri koosneks domeenidest, mis on küll tuvastustingimustele vastavad, kuid jäetakse tulemustesse kaasamata nende antud nimekirja kuulumise tõttu. Entroopia väärtuse 4,1357 korral ei oleks usaldusväärsete domeenide nimekirja haldamine enam liialt ajamahukas, kuid kiiresti hakkab vähenema DNS tunneli päringute tingimusele vastavus ning dnscat2 tüüpi päringud ja 2. taseme domeenid võivad jääda tuvastamata. Kokkuvõtlikult võib väita, et entroopia võimaldab edukalt välistada suure hulga dnslog tüüpi kirjeid ning seda on mõistlik kasutada edasise analüüsi käigus.

5.1.2 Päringus esinevate alamdomeenide arv

DNS päringut iseloomustab selles sisalduvate alamdomeenide arv. 1. taseme domeen ehk tippdomeen, 2. taseme domeen, mida füüsilised ja juriidilised isikud tavapäraselt registreerivad ja millele järgnevad 3. ja madalama taseme domeenid. 3. tasemest alates võib tegu olla seadme võrgunime või alamdomeeniga, kuid antud töös läbi viidud analüüsi puhul ei oma see tähtsust.

Alamdomeeni tasemete minimaalne, keskmine ja maksimaalne arv erinevate päringutüüpide lõikes on esitatud tabelis 10.

Tabel 10. Alamdomeenide arv päringu tüüpide lõikes

Päringu tüüp	**Minimaalne**	**Keskmine**	**Maksimaalne**
dnslog	2	3	13
dnscat2	3	4	6
FrameworkPOS	3	6	10
iodine	3	4	7
OilRig	3	3	3
Poison Frog	2	2	3

Päringute protsentuaalne jaotus vastavalt alamdomeenide arvule on esitatud tabelis 11. Tabelist on välja jäetud alamdomeenide 12-13 osakaalu kajastavad veerud, kuna nende puhul oli päringute hulk ümardatult 0%.

Tabel 11. Päringute protsentuaalne jaotus vastavalt alamdomeenide

Päringu tüüp	**Alamdomeenide arv / %**								
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
dnslog	1,87	**65,16**	20,78	10,88	0,83	0,44	0,03	0,01	0,00
dnscat2	0,00	37,01	0,03	0,01	**62,96**	0,00	0,00	0,00	0,00
FrameworkPOS	0,00	**50,00**	0,00	0,00	0,00	0,00	0,00	0,00	**50,00**
iodine	0,00	15,21	**44,53**	4,11	0,67	35,48	0,00	0,00	0,00
OilRig	0,00	**100,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Poison Frog	18,18	**81,82**	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Ainult pikkus ei võimalda erinevaid päringute tüüpe eristada, seega on järgnevalt uuritud alamdomeenide arvu ja päringu sõne entroopia kombinatsioone. Minimaalsele entroopia väärtusele 3,7072 vastav jaotus on esitatud tabelis 12.

Tabel 12. Alamdomeenide arv entroopia väärtuse 3,7072 korral

Päringu tüüp	**Alamdomeenide arv / %**								
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
dnslog	0,07	37,24	**37,83**	20,48	2,54	1,68	0,11	0,04	0,00
dnscat2	0,00	39,45	0,03	0,01	**60,52**	0,00	0,00	0,00	0,00
FrameworkPOS	0,00	**50,00**	0,00	0,00	0,00	0,00	0,00	0,00	**50,00**
iodine	0,00	11,23	**46,62**	4,30	0,70	37,14	0,00	0,00	0,00
OilRig	0,00	**100,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Poison Frog	0,00	**100,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Tabelist 12 selgub, et legitiimsete päringute puhul suurenes enim esinevate alamdomeenide tase ühe võrra, teiste päringute puhul jäi protsentuaalne jaotus sisuliselt samaks.

Tabelis 13 on esitatud unikaalsete domeenide protsentuaalne jaotus vastavalt alamdomeenide tasemele:

Tabel 13. Unikaalsete domeenide jaotus vastavalt alamdomeenide tasemele

Päringu tüüp	**Alamdomeenide arv / %**									
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**12**
dnslog	0,00	37,01	0,03	0,01	**62,96**	0,00	0,00	0,00	0,00	0,00
dnscat2	17,69	**44,84**	26,46	9,82	0,66	0,20	0,28	0,02	0,00	0,01
FrameworkPOS	0,00	**50,00**	0,00	0,00	0,00	0,00	0,00	0,00	**50,00**	0,00
iodine	0,00	15,20	**44,54**	4,11	0,67	35,49	0,00	0,00	0,00	0,00
OilRig	0,00	**100,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Poison Frog	10,00	**90,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Tabelis 14 on esitatud unikaalsete domeenide protsentuaalne jaotus vastavalt alamdomeenide tasemele, kui entroopia on vähemalt 3,7072.

Tabel 14. Unikaalsete domeenide jaotus vastavalt alamdomeenide tasemele entroopia 3,7072 korral

Päringu tüüp	**Alamdomeenide arv / %**									
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**12**
dnslog	0,00	39,45	0,03	0,01	**60,52**	0,00	0,00	0,00	0,00	0,00
dnscat2	1,69	24,42	**50,41**	21,37	1,15	0,24	0,63	0,05	0,01	0,02
FrameworkPOS	0,00	**50,00**	0,00	0,00	0,00	0,00	0,00	0,00	**50,00**	0,00
iodine	0,00	11,23	**46,62**	4,30	0,70	37,14	0,00	0,00	0,00	0,00
OilRig	0,00	**100,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Poison Frog	0,00	**100,00**	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Peatükis esitatud tabelites olevate andmete põhjal selgus, et päringus esinevate alamdomeenide arv ei võimalda päringu tüüpide eristamist ning seda pole otstarbekas edasises analüüsis kasutada.

5.1.3 Domeeninime pikkus

DNS tunnelite puhul on eesmärgiks edastada informatsiooni – mida rohkem viimast on, seda pikemaks kujuneb ka domeeninimi. Alternatiiv on suurendada päringute arvu, kuid see lisab märkimisväärse viite, seega tunnel on seda efektiivsem, mida rohkem informatsiooni ühe päringu sisse suudetakse kodeerida. Tabelis 15 on esitatud päringutes sisaldunud sõnede pikkust kirjeldavad üldised väärtused tüüpide lõikes.

Tabel 15. Päringu sõnede pikkus

Päringu tüüp	**Minimaalne**	**Keskmine**	**Maksimaalne**
dnscat2	29	162	236
dnslog	4	22	227
FrameworkPOS	45	88	131
iodine	17	144	252
OilRig	36	39	42
Poison Frog	15	33	41

Tunnelite päringu keskmine pikkus on suurem, kui tavapärastel päringutel. Võttes minimaalseks domeeninime pikkuseks 33 ja lisades sellele minimaalse entroopia 3,7072, tuvastatakse kõikide tunnelite puhul üle 75% päringutest, dnslog puhul on tingimustele vastavate päringute osakaal 7,51% ja 2. taseme domeenide arv 1450. Viimane on autori hinnangul liiga suur, et seda lubatud domeenide nimekirjaga hallata.

Domeeninime puhul on informatsiooni edastamise seisukohast staatilised osad tippdomeen ja 2. taseme alamdomeen, seega DNS tunnelite puhul jääb edastatav informatsioon kolmanda ja madalama taseme alamdomeenidesse. Staatilise olemuse tõttu võib teha eelduse, et analüüsi seisukohast pole tippdomeen ja 2. taseme alamdomeen olulised. Küll aga on DNS päringusse võimalikult suure hulga informatsiooni mahutamiseks otstarbekas hoida 2. taseme domeen võimalikult lühike.

Neljanda ja madalama taseme domeene esineb ainult dsncat2, FrameworkPOS ja iodine puhul, kuid seda ei saa analüüsi käigus eelduseks võtta, kuna uute alamdomeenide tekkimiseks on vaja DNS päringusse lisada täiendavaid punkte – sõltuvalt tarkvara lähtekoodist ja andmete kodeerimisest võib see olla vägagi triviaalne ülesanne. Seetõttu tuleb vaadelda kõiki kolmanda ja madalama taseme päringuid. Kolmanda ja madalama taseme domeenide päringute pikkust iseloomustavad omadused on kirjeldatud tabelis 16.

Tabel 16. Kolmanda ja madalama taseme domeenide päringute pikkus

Päringu tüüp	**Minimaalne**	**Keskmine**	**Maksimaalne**
dnscat2	18	149	222
dnslog	0	9	215
FrameworkPOS	2	41	81
iodine	6	131	237
OilRig	19	22	25
Poison Frog	0	17	25

Kõige lühem keskmine sõne pikkus kogu päringu lõikes oli dnslog tüübi puhul väärtusega 22, mis kolmanda ja madalama taseme domeenide puhul vähenes 59,1% võrra väärtusele 9. Järgnes Poison Frog, mille puhul oli vastav väärtus 33 ja vähenemine 48,5% väärtusele 17. Ülejäänud tüüpide puhul oli kolmanda ja madala taseme päringu keskmise sõne vähemine järgmine: dnscat2 8%, FrameworkPOS 53,4%, iodine 9% ja OilRig 43,6%.

Kõige suurem vähenemine oli dnslog tüüpi päringute puhul, mis kinnitab, et DNS tunnelite efektiivsuse suurendamiseks on mõistlik hoida 1. ja 2. taseme domeen võimalikult lühike, edastatavat informatsiooni kannavad madalama taseme alamdomeenid.

Tabelis 17 on esitatud tingimustele vastavate päringute osakaal, kui 3. ja madalama taseme domeeninimede pikkus on minimaalselt 17.

Tabel 17. Minimaalselt 17 märgise pikkusega päringute osakaal

Päringu tüüp	**Ilma entroopiata**	**Minimaalne entroopia 3,7072**
dnscat2	100,00	93,31
dnslog	12,00	11,10
FrameworkPOS	50,00	50,00
iodine	88,51	88,51
OilRig	100,00	100,00
Poison Frog	81,82	81,82

Täispika domeeninime korral ja minimaalse entroopia nõudega oli tingimustele vastavate päringute osakaal dnslog tüübi puhul 7,51%. Tingimustele vastavate päringute osakaal küll tõusis märkimisväärselt, samas 2. taseme domeenide arv vähenes väärtuseni 1431. Viimane väärtus on endiselt liiga kõrge lubatud nimekirjadega haldamiseks, kuid sellele vaatamata on nimekirje pikkus küllaltki efektiivne päringu tüüpide eristamiseks.

5.2 Olekupõhised tuvastusmeetodid

Olekupõhiste tuvastusmeetodite puhul vaadeldi järgmisi omadusi: päringute arv ühe kliendi (IP-aadressi) kohta ja unikaalsete alamdomeenide arv 2. taseme domeeni kohta.

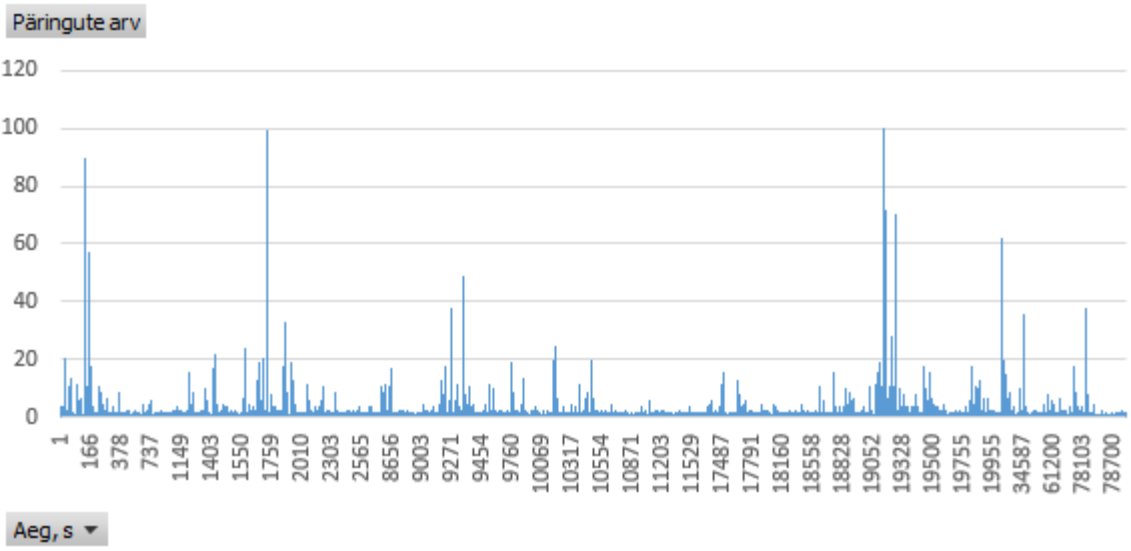
5.2.1 Päringute arv ühe kliendi (IP-aadressi) kohta

Analüüsi puhul uuriti ainult IP-aadressilt 192.168.136.171 sooritatud päringuid, kuna antud seadme sooritatud päringud vastavad nii-öelda „keskmisele“ võrguseadmele. Päringu tüübi dnscat2 puhul vaadeldi ainult failide avatekstina edastamisel tehtud päringuid, kuna nende hulk on väiksem ja seega ka tuvastamine keerukam. Andmefaili 1.txt puhul oli kõige vähem päringuid, 3-4 tekitasid samas suurusjärgus päringute arvu,

märkimisväärselt suurem päringute arv oli andmefailide 5.txt, 6.dat ja 7.dat korral. Saamaks hinnangut nii väga väikse kui ka suurema päringute arvu kohta on vaadeldud andmefailide 1.txt ja5.txt edastamisel tehtud päringuid.

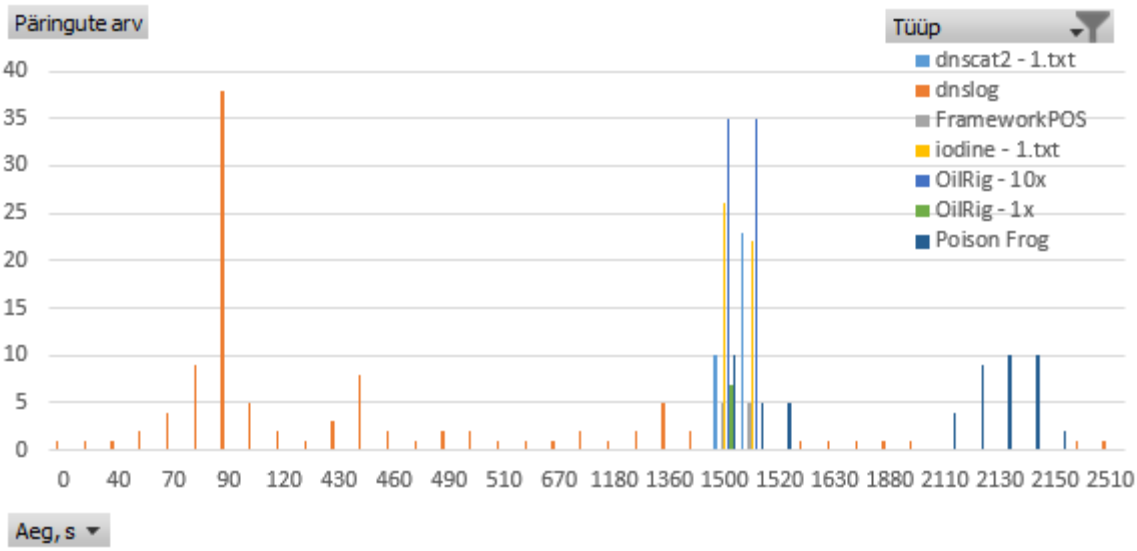
iodine puhul on analüüsitud ainult parameetri "-M" vaikeväärtusega sooritatud päringuid, kuna nende arv oli väiksem ja seega tuvastamine keerukam. iodine puhul oli samuti kõige väiksem päringute arv andmefaili 1.txt puhul. Andmefailide 2.txt, 3.txt ja 4.txt puhul oli päringute arv samas suurusjärgus. Märkimisväärselt suurem oli päringute arv failide 5.txt ja 7.dat puhul (6.dat ülekanne ebaõnnestus). Seega on iodine puhul nii väikse kui ka suurema päringute arvu kohta hinnangu saamiseks vaadeldud andmefailide 1.txt ja 7.dat edastamisel tehtud päringuid.

Joonisel 4 on 192.168.136.171 dnslog tüüpi päringud ühe ööpäeva (kolmapäev) lõikes. Teiste logide põhjal veenduti, et tööpäeva jooksul arvutit kasutati, kuid joonisel kasutaja kohalolu ei väljendu – selle põhjuseks on, et arvutist ei logitud peale tööpäeva lõppu välja ja tööle jäänud protsessid sooritasid endiselt DNS päringuid.



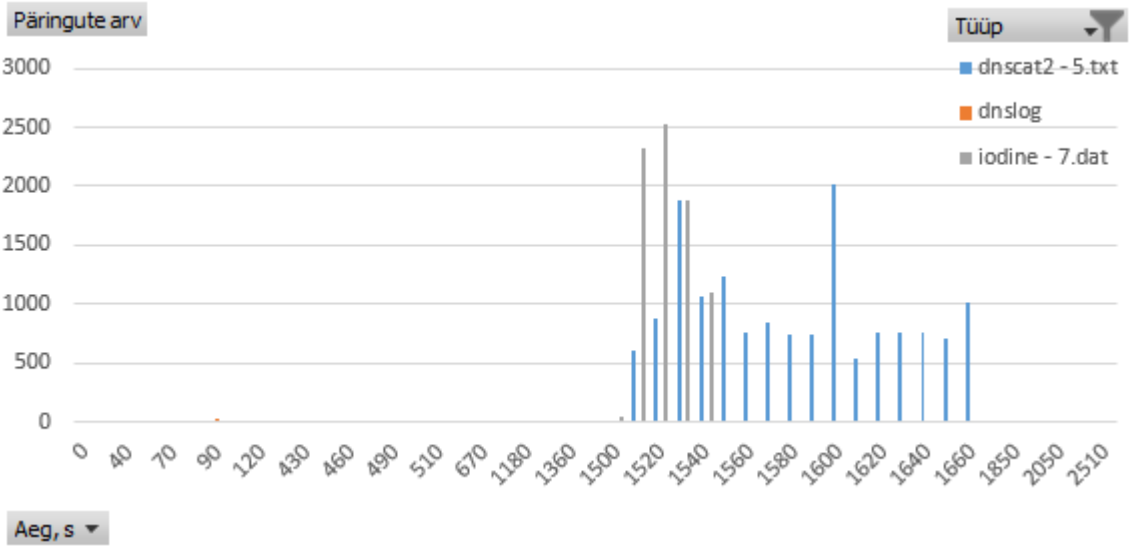
Joonis 4. dnslog tüüpi päringud ühe ööpäeva lõikes

Joonisel 5 on erinevate päringutüüpide lõikes esitatud IP-aadressilt 192.168.136.171 saabunud päringute ajaline jaotus 25 minutit enne ja peale tunnelite tarkvarade käivitamist. Joonisel 4 vastab see väärtusele alates 78253 ehk kellaajale 21:44:13.



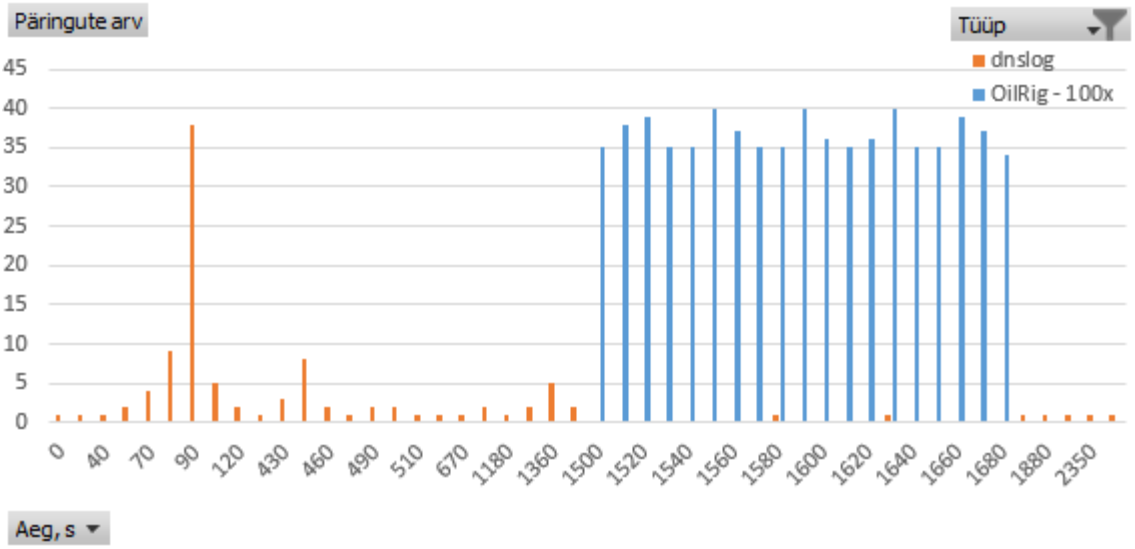
Joonis 5. Väikese päringute arvuga päringutüübid

Joonis 6 vastab muus osas joonise 5 kirjeldusele, kuid kujutatud on suurema päringute arvuga tulemused – dnscat2 puhul faili 5.txt edastamine ja iodine puhul faili 7.dat edastamine, lisatud on ka dnslog tüüpi päringud.



Joonis 6. Suure päringute arvuga päringutüübid

Ka joonis 7 vastab jooniste 5 ja 6 kirjeldusele, kuid sellel on kujutatud OilRig 100 kordse tsüklina käivitamise tulemusel tehtud päringute jaotus koos dnslog tüüpi päringutega.



Joonis 7. OilRig 100-kordse tsükli päringud

Päringute arvu visualiseerimine annab selge märgi, et nii suure päringute arvu varieeruvuse tõttu erinevate tüüpide lõikes pole päringute arv ühe kliendi (IP-aadressi) kohta efektiivne võimalus päringutüüpide eristamiseks.

5.2.2 Unikaalsete alamdomeenide arv 2. taseme domeeni kohta

Vastavalt peatükis „Domeeninime pikkus“ olevale põhjendusele on DNS päringuga võimalik dünaamiliselt informatsiooni edastada ainult 3. ja madalama taseme alamdomeenide sõnedega. See omakorda tähendab, et kui muutub edastatav informatsioon, siis muutub ka päringu sisu – 3. ja olemasolu korral madalama taseme alamdomeenide sõnede väärtus. Teoreetiliselt on võimalik kollisioon ja erineva informatsiooni edastamisel samasuguse päringu sõne teke, kuid näidisandmestiku analüüsimisel kaasnes iga edastatava informatsiooni muudatusega ka unikaalse alamdomeeni tekkimine. Unikaalsete alamdomeenide arv iga 2. taseme domeeni kohta vastavalt tüübile oli järgmine:

1. dnslog – 310607
2. FrameworkPOS – 2
3. Poison Frog – 10

Ülejäänud päringu tüüpide puhul langes unikaalsete alamdomeenide arv kokku päringute arvuga – iga sooritatud päring oli unikaalne.

Unikaalsete alamdomeenide arv on üheks võimaluseks eristada päringu tüüpe, õige ja valepositiivse tuvastuse kriteeriumiks oleks sel juhul unikaalsete alamdomeenide arv. Järjestades 2. taseme domeenid unikaalsete alamdomeenide arvu järgi on võimalik väikse valepositiivsete arvuga tuvastada DNS tunneliga suurte failide edastamist – andmefailide 5.txt, 6.dat ja 7.dat edastamisel olid nii dnscat2 kui ka iodine antud pingejärjestuses esimese 15. seas. Väiksemate andmemahtude korral tõuseb valepositiivsete tuvastuste arv märkimisväärselt, 3.txt edastamine iodine tunneliga oli antud järjestuses 589. kohal, OilRig ühekordse tsükliga 2301. kohal ja FrameworkPOS 24096. kohal. Väljavõte kogu järjestusest on esitatud lisas 2.

Paljude 2. taseme domeenide puhul on nende alamdomeenid ajas muutuvad – neid eemaldatakse ja lisatakse. Eelnevalt oli unikaalsete alamdomeenide leidmisel vaadeldud kogu näidisandmestikku – antud lähenemine ei pruugi olla mõistlik tuvastuste tõepärasuse ja ressursikasutuse osas. Lühendades perioodi samale ööpäevale, mille jooksul kõikide tüüpide päringud tehti, vähenes märkimisväärselt ka valepositiivsete tuvastuste arv. Andmefailide 5.txt, 6.dat ja 7.dat edastamisel olid dnscat2 ja iodine järjestuse alguses, 3.txt edastamine iodine tunneliga 217. kohal, OilRig ühekordse tsükliga 817. kohal ja FrameworkPOS 3428. kohal. Väljavõte kogu järjestusest on esitatud lisas 3.

Täiendavaks võimaluseks DNS tunnelite tuvastamisel on teha eeldus, et antud tüüpi päringuid teevad ainult üksikud seadmed, samas kui legitiimsete päringute puhul on seadmete arv otseses sõltuvuses vaadeldava arvutivõrgu suurusest ja olulisel määral ka seadmete kasutajaskonnast. Välistades 2. taseme domeenid, mille päringuid on sooritanud üle 10 unikaalse seadme (IP-aadressi), jääb järjestuse tipp muutumatuks, 3.txt edastamine iodine tunneliga kerkib 49. kohale, OilRig ühekordse tsükliga 343. kohal ja FrameworkPOS 3183. kohal. Väljavõte kogu järjestusest on esitatud lisas 4. Seega on unikaalsete alamdomeenide arv 2. taseme domeeni kohta efektiivne võimalus päringutüüpide eristamiseks.

5.3 Olekuta ja olekupõhiste tuvastusmeetodite kombineerimine

Eelneva analüüsi käigus selgus, et entroopia, domeeninime pikkus ja unikaalsete alamdomeenide arv 2. taseme domeeni kohta on küllaltki efektiivsed päringutüüpide eristamiseks, kuid eraldiseisvalt ei paku siiski piisavat täpsust. Nende omaduste

kombineerimisel tulemus paranes, kuid ei olnud autori hinnangul siiski veel vastuvõetav, seega lisati täiendav tingimus, et 3. ja madalama taseme alamdomeenide sõne pikkus oleks minimaalselt 17. Sellisel juhul on 3.txt edastamine iodine tunneliga 39. kohal, OilRig ühekordse tsükliga 46. kohal ja FrameworkPOS 495. kohal. 495 oli ühtlasi kogu järjestuse suurus. Väljavõte järjestusest on esitatud lisas 5. Tabelis 18 on tüüpide kaupa esitatud eelnevalt kirjeldatud tingimustele vastavate päringute arv, kõikide vaadeldud perioodil tehtud päringute arv ning nende protsentuaalne erinevus.

Tabel 18. 5.3 Olekuta ja olekupõhiste tuvastusmeetodite kombineerimise tulemus

		Päringute arv		
Tüüp	**Andmefail / parameetrid**	**Tingimustele vastavad**	**Kokku**	**Erinevus %**
dnscat2	1.txt	26	27	96,30
dnscat2	2.txt	33	36	91,67
dnscat2	3.txt	25	28	89,29
dnscat2	4.txt	41	55	74,55
dnscat2	5.txt	6846	14065	48,67
dnscat2	6.dat	19505	19507	99,99
dnscat2	7.dat	19487	19679	99,02
dnslog		543168	5286118	10,28
FrameworkPOS	15 min sessioon	5	10	50,00
iodine	1.txt	11	24	45,83
iodine	2.txt	11	24	45,83
iodine	3.txt	10	23	43,48
iodine	4.txt	24	35	68,57
iodine	5.txt	6907	7172	96,31
iodine	6.dat	14231	14351	99,16
iodine	7.dat	1343	3941	34,08
OilRig	Tsükkel 1x	7	7	100,00
OilRig	Tsükkel 10x	70	70	100,00
OilRig	Tsükkel 100x	696	696	100,00
Poison Frog	15 min sessioon	45	55	81,82

Tuvastusprotsendid on head kõikide tunneli tüüpide puhul, kuid dnslog tüübi puhul on liialt palju valepositiivseid tuvastusi ja 2. taseme domeene. Viimase vähendamiseks saab rakendada tingimuse, et unikaalsete 3. ja madalama taseme alamdomeenide arv vaadeldavas perioodis peab olema minimaalselt 7. Sellisel juhul jääb küll tuvastamata tunneli tüüp FrameworkPOS, kuid väheneb märkimisväärselt 2. taseme domeenide hulk valepositiivsete tuvastuste osas. Seda enam, et näidisandmestik on staatiline, reaalses keskkonnas on alamdomeenide hulk ajas muutuv ning tingimustele vastavate dnslog tüüpi päringute 2. taseme domeenide hulk kasvab. Usaldusväärsete domeenide nimekiri on vajalik, kuid selle esmane suurusjärk on umbkaudu 50 kirjet.

5.4 Tulemused

Analüüsi tulemusel selgus, et DNS-tunnelite tuvastamise täpsuse ja madala valepositiivsete tuvastuste saavutamiseks tuleb vaadelda järgmisi omadusi:

1. domeeninime entroopia minimaalse väärtusega 3,7072,
2. 3. ja madalama taseme domeeninimede pikkus minimaalselt 17,
3. 2. ja madalama taseme domeeni päringuid on sooritanud alla 10 unikaalse seadme (IP-aadressi),
4. päringud jäävad ajaliselt 24 tunni sisse.

Saadud tulemused järjestada vastavalt unikaalsete alamdomeenide arvule alates kõige suuremast ning valida saadud järjestusest 50 esimest kirjet. Kuna selles järjestuses sisaldub ka legitiimsete päringute domeene, siis on nende välistamiseks vajalik koostada usaldusväärsete domeenide nimekiri, mille haldamine ei ole autori hinnangul liialt ajamahukas. Sellise metoodika puhul on valepositiivsete tuvastuste osakaal 0,04% ja näidisandmestikust jäävad tuvastamata FrameworkPOS tüüpi kirjed. Töö autori seisukoht on, et kui pahavara oleks juhtserveriga ühendust saanud ja teinud rohkem kui kümme päringut kahe unikaalse domeeninimega, siis oleks ka antud päringu tüüpi kirjed tuvastatud. Kaasates tulemustesse ka FrameworkPOS tüüpi kirjed tõuseb valepositiivsete tuvastuste osakaalu 0,44%ni.

Kirjeldatud metoodika on lihtsasti rakendatav mitmete turvatoodete abil, sarnast protsessi on kirjeldatud LogRhythm [44] ja Splunk [45] tarkvarade puhul. Antud näidetes pole DNS päringute omadusi kaasatud nii detailselt, seega täpselt juhendit järgides oleks

tuvastuste osakaal madalam ja/või valepositiivsete tuvastuste arv suurem. Kuigi töömahukam, siis mitte üleliia keerukas alternatiiv on antud metoodika rakenda mõnes vabalt valitud programmeerimiskeeles.

6 Kokkuvõte

Töö eesmärgiks oli luua metoodika, mis võimaldab eristada DNS protokolli väärkasutust legitiimsetest päringutest, on lihtsasti juurutatav ja tagab sealjuures madala valepositiivsete tuvastuste arvu. Eriline rõhk oli pahavara kontrollkanalitel ja spetsiifilise andmevarguse andmevahetuskanalitel, kuna nende tuvastamine on märkimisväärselt keerukam.

Töös uuriti DNS päringute omadusi ja erinevaid DNS väärkasutuse tuvastamise meetodeid ning anti ülevaade DNS väärkasutust võimaldavatest tarkvaradest. DNS väärkasutuse stsenaariumite loomiseks valiti tarkvarad iodine, dnscat2 ning pahavarad FrameworkPOS, OilRig ja Poison Frog. Loetletud tarkvaradega viidi isoleeritud testkeskkonnas läbi mitmeid eksperimente, mis iodine ja dnscat2 puhul hõlmasid erinevate andmefailide ülekannet, pahavarade puhul jälgiti kindla perioodi vältel katseid ühenduda juhtserveriga. Eksperimentide käigus saadud tulemused lisati umbes 3000 arvutitöökohaga ettevõte arvutivõrgust kogutud näidisandmestikule, saadud koondandmestikku kasutati erinevate tuvastusvõimaluste efektiivsuse hindamiseks. Kõige efektiivsemate tuvastusvõimaluste põhjal loodi metoodika, mis kaasab järgmised DNS päringute omadused: domeeninime entroopia, 3. ja madalama taseme domeeninimede pikkus, domeeni nimelahendusi sooritanud klientide arvu ja päringute ajalise kuuluvuse määratud ajaaknasse.

Magistritöö püstitatud eesmärk sai täidetud. Loodud metoodika on lihtsasti rakendatav, tagab kõrge tuvastustäpsuse ja omab madalat valepositiivsete tuvastuste osakaalu väärtusega 0,44%. Kõige raskemini tuvastatava stsenaariumi kõrvale jätmisel langes valepositiivsete tuvastuste osakaal väärtuseni 0,04%.

Kasutatud kirjandus

[1] Charles M. Kozierok (2005). "TCP/IP Guide". No Starch Press

[2] M. Wong (2006). "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1". IETF Administration LLC [https://tools.ietf.org/html/rfc4408]

[3] Asaf Nadler, Avi Aminov, Asaf Shabtai (2018). "Detection of Malicious and Low Throughput Data Exfiltration Over the DNS Protocol"

[4] Jingkun Liu, Shuhao Li, Yongzheng Zhang, Jun Xiao, Peng Chang, Chengwei Peng (2017). "Detecting DNS Tunnel through Binary-Classification Based on Behavior Features". IEEE Trustcom/BigDataSE/ICESS

[5] Greg Farnham (2013). "Detecting DNS Tunneling". SANS Institute Reading Room

[6] Anirban Das, Min-Yi Shen, Madhu Shashanka, Jisheng Wang (2017). "Detection of Exfiltration and Tunneling over DNS". Samsung Research America, Inc

[7] Andreas Berg, Daniel Forsberg (2019). "Identifying DNS-tunneled traffic with predictive models". Department of Computer and Systems Sciences, Stockholm University

[8] Pete Babcock (2013). "Detecting DNS exfiltration of data using HP ArcSight ESM". USAA

[9] E. Cambiaso, M. Aiello, M. Mongelli, G. Papaleo (2016). "Feature transformation and mutual information for dns tunneling analysis". Ubiquitous and Future Networks (ICUFN), 2016 Eighth International Conference on. IEEE

[10] Van Thuan Do, Paal Engelstad, Boning Feng, Thanh van Do (2017). "Detection of DNS tunneling in mobile networks using machine learning".

[11] Palo Alto Networks, Inc. (2020). "PAN-OS® Administrator's Guide, DNS Tunneling Detection". [https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/dns-tunneling-detection]

[12] Palo Alto Networks, Inc. (2020). "Cortex XDR™ Analytics Alert Reference, DNS Tunneling". [https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-analytics-alert-reference/cortex-xdr-analytics-alert-reference/dns-tunneling]

[13] Cisco Systems, Inc. (2019) "Cisco Umbrella, DNS Tunneling".

[14] Comodo Group, Inc. (2020). "Cloud-delivered network security". [https://cdome.comodo.com]

[15] Check Point Software Technologies LTD (2018). "IPS Protection, DNS Tunneling". [https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=protection&threatId=dnstunnel]

[16] Claude Shannon (1948). "A Mathematical Theory of Communication". Bell System Technical Journal

[17] Claude Shannon (1951). "Prediction and entropy of printed english". Bell Labs Technical Journal

[18] Abhijeet Rastogi (2017). "Traffic Steering using RUM DNS". LinkedIn

[19] Palo Alto Networks, Inc. (2019). "Threat Brief: Understanding Domain Generation Algorithms (DGA)" [https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/]

[20] "DeNiSe is a proof of concept for tunneling TCP over DNS in Python" [https://github.com/mdornseif/DeNiSe]

[21] OffSec Services Limited. "dns2tcp Package Description". [https://tools.kali.org/maintaining-access/dns2tcp]

[22] "DNScapy". [https://github.com/FedericoCeratto/dnscapy]

[23] Tadeusz Pietraszek (2004). "DNScat". [http://tadek.pietraszek.org/projects/DNScat/]

[24] Ron Bowes (2015). "Dnscat". [https://wiki.skullsecurity.org/Dnscat]

[25] "dnscat2". [https://github.com/iagox86/dnscat2]

[26] "fraud-bridge". [https://github.com/stealth/fraud-bridge/blob/master/README]

[27] Gianluca Silvestri (2017). "DNS Data Exfiltration". Exclusive Networks Italy

[28] "Heyoka". [http://heyoka.sourceforge.net/]

[29] "iodine". [https://github.com/yarrick/iodine]

[30] "NSTX (IP-over-DNS) HOWTO". [https://thomer.com/howtos/nstx.html]

[31] Dan Kaminsky (2004). "Release!". [https://dankaminsky.com/2004/07/29/51/]

[32] Kenton Born (2010). "PSUDP: A Passive Approach to Network-Wide Covert Communication". Black Hat USA 2010

[33] Andreas Gohr (2008). "DNS Tunneling made easy". [https://www.splitbrain.org/blog/2008-11/02-dns_tunneling_made_simple]

[34] SensePost Pty Ltd. "SQL Injection without the pain of syringes". [https://github.com/sensepost/squeeza]

[35] "tcp-over-dns". [http://analogbit.com/software/tcp-over-dns/]

[36] Lucas Nussbaum (2008). "IP over DNS tunnel". [https://github.com/lnussbaum/tuns]

[37] Applied Wizardry GmbH. "The all-in-one VPN tunneling, firewall & proxy bypassing, anonymization and anti-censorship solution". [https://your-freedom.net/]

[38] Palo Alto Networks, Inc. (2019). "DNS Tunneling in the Wild: Overview of OilRig's DNS Tunneling". [https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/]

[39] Christian J. Dietrich (2011). "Feederbot Botnet Using DNS as Carrier for Command and Control (C2)". [https://chrisdietri.ch/post/feederbot-botnet-using-dns-command-and-control/]

[40] Eric Merritt (2015). "Another Brick in the FrameworkPoS". [https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/another-brick-in-the-frameworkpos/]

[41] The MITRE Corporation (2019). "OilRig". [https://attack.mitre.org/groups/G0049/]

[42] Jonathan Lepore. "Chirp of the PoisonFrog". [https://ironnet.com/blog/chirp-of-the-poisonfrog/]

[43] Internet Assigned Numbers Authority (2020). "tlds-alpha-by-domain.txt". [http://data.iana.org/TLD/tlds-alpha-by-domain.txt]

[44] LogRhythm, Inc. (2014). "Detecting DNS Tunneling". [https://logrhythm.com/blog/detecting-dns-tunneling/]

[45] Steve Jaworski (2016). "Using Splunk to Detect DNS Tunneling". SANS Institute Reading Room

Lisa 1 – Andmebaasitabeli olemite omaduste kirjeldus

Veeru nimi	**Andmetüüp**	**NULL / NOT NULL**	**Indeks**	**Semantika**
id	INTEGER	NOT NULL	Jah	Tabeli primaarvõti
action	NVARCHAR (50)	NULL	Jah	Testfailiga sooritatud toiming – alla- või üleslaadimine
datafile	NVARCHAR (50)	NULL	Jah	DNS andme- või kontrollkanali päringuid sisaldanud andmefaili nimi
domain	NVARCHAR (253)	NOT NULL	Jah	DNS päringus sisaldunud täispikk domeeninimi
domain_lev_cnt	INTEGER	-	Jah	DNS päringus sisaldunud alamdomeenide arv koos tippdomeeniga. Veerul domain põhinev arvutuslik veerg.
domain1	NVARCHAR (253)	NOT NULL	Ei	1. taseme domeen ehk tippdomeen
domain2	NVARCHAR (253)	NOT NULL	Ei	2. taseme domeeni nimi
domain3	NVARCHAR (253)	NULL	Ei	3. taseme domeeni nimi
domain4	NVARCHAR (253)	NULL	Ei	4. taseme domeeni nimi
domain5	NVARCHAR (253)	NULL	Ei	5. taseme domeeni nimi
domain6	NVARCHAR (253)	NULL	Ei	6. taseme domeeni nimi
domain7	NVARCHAR (253)	NULL	Ei	7. taseme domeeni nimi
domain8	NVARCHAR (253)	NULL	Ei	8. taseme domeeni nimi
domain9	NVARCHAR (253)	NULL	Ei	9. taseme domeeni nimi

domain10	NVARCHAR (253)	NULL	Ei	10. taseme domeeni nimi
domain11	NVARCHAR (253)	NULL	Ei	11. taseme domeeni nimi
domain12	NVARCHAR (253)	NULL	Ei	12. taseme domeeni nimi
domain13	NVARCHAR (253)	NULL	Ei	13. taseme domeeni nimi
entropy	DECIMAL (16, 14)	NOT NULL	Jah	Täispika domeeninime (sõne) Shannoni entroopia
ip	NVARCHAR (50)	NOT NULL	Jah	DNS päringu sooritanud seadme IP aadress
len_domain	INTEGER	-	Jah	DNS päringus sisaldunud domeeninime pikkus. Veerul domain põhinev arvutuslik veerg.
len_domain1	INTEGER	-	Jah	1. taseme ehk tippdomeeni pikkus. Veerul domain1 põhinev arvutuslik veerg.
len_domain2	INTEGER	-	Jah	2. taseme alamdomeeni pikkus. Veerul domain2 põhinev arvutuslik veerg.
len_domain3	INTEGER	-	Jah	3. taseme alamdomeeni pikkus. Veerul domain3 põhinev arvutuslik veerg.
len_domain4	INTEGER	-	Jah	4. taseme alamdomeeni pikkus. Veerul domain4 põhinev arvutuslik veerg.
len_domain5	INTEGER	-	Jah	5. taseme alamdomeeni pikkus. Veerul domain5 põhinev arvutuslik veerg.
len_domain6	INTEGER	-	Jah	6. taseme alamdomeeni pikkus. Veerul domain6 põhinev arvutuslik veerg.
len_domain7	INTEGER	-	Jah	7. taseme alamdomeeni pikkus. Veerul domain7 põhinev arvutuslik veerg.
len_domain8	INTEGER	-	Jah	8. taseme alamdomeeni pikkus. Veerul domain8 põhinev arvutuslik veerg.
len_domain9	INTEGER	-	Jah	9. taseme alamdomeeni pikkus. Veerul domain9 põhinev arvutuslik veerg.
len_domain10	INTEGER	-	Jah	10. taseme alamdomeeni pikkus. Veerul domain10 põhinev arvutuslik veerg.
len_domain11	INTEGER	-	Jah	11. taseme alamdomeeni pikkus. Veerul domain11 põhinev arvutuslik veerg.

len_domain12	INTEGER	-	Jah	12. taseme alamdomeeni pikkus. Veerul domain12 põhinev arvutuslik veerg.
len_domain13	INTEGER	-	Jah	13. taseme alamdomeeni pikkus. Veerul domain13 põhinev arvutuslik veerg.
len_subdomains	INTEGER	-	Jah	3. ja madalama taseme alamdomeenide sõne pikkus
logfile	NVARCHAR (50)	NOT NULL	Jah	Legitiimseid DNS päringuid sisaldanud andmefaili nimi
params	NVARCHAR (50)	NULL	Jah	DNS tunneli- või kontrollkanali simuleerimisel kasutatud parameetrid
skip	INTEGER	NOT NULL	Jah	Veerg, mille alusel on võimalik ühe SQL päringu tingimusega kirjeid analüüsi kaasata või välja jätta
targettime	NVARCHAR (50)	NULL	Jah	
time	INTEGER	NOT NULL	Jah	DNS päringu aeg (Unix ajatempel)
type	NVARCHAR (50)	NOT NULL	Jah	Päringu tüüp

Lisa 2 – Unikaalsete alamdomeenide arv 2. taseme domeeni kohta

Jrk nr	Tüüp	Andme-fail	Parameetrid	2. taseme domeen	Alam-domeenide arv
1	dnslog			gstatic.com	43183
2	dnscat2	7.dat	Krüpteeritud	domeen.tld	21330
3	dnscat2	6.dat	Krüpteeritud	domeen.tld	21316
4	iodine	5.txt	-m 1130 -M 100	domeen.tld	20010
5	dnscat2	7.dat	Avatekst	domeen.tld	19679
6	dnscat2	6.dat	Avatekst	domeen.tld	19507
7	dnslog			footprintdns.com	15553
8	dnscat2	5.txt	Krüpteeritud	domeen.tld	15314
9	iodine	6.dat	-m 1130	domeen.tld	14351
10	dnscat2	5.txt	Avatekst	domeen.tld	14065
11	iodine	5.txt	-m 1130	domeen.tld	7172
12	dnslog			dropboxusercontent.com	5616
14	iodine	7.dat	-m 1130	domeen.tld	3941
15	iodine	7.dat	-m 1130 -M 100	domeen.tld	3925
16	dnslog			googlevideo.com	3495
36	OilRig		Tsükkel 100x	withyourface.com	696
37	dnslog			onef.pro	688
194	OilRig		Tsükkel 10x	withyourface.com	70
195	dnslog			fastpic.ru	69
203	iodine	4.txt	-m 1130 -M 100	domeen.tld	68
204	dnslog			bezformata.com	68
227	dnscat2	4.txt	Krüpteeritud	domeen.tld	61
228	dnslog			hpe.com	60
246	dnscat2	4.txt	Avatekst	domeen.tld	55
247	dnslog			europaplus.ru	54
332	dnscat2	2.txt	Krüpteeritud	domeen.tld	41

333	dnslog			salesforce.com	40
366	dnscat2	2.txt	Avatekst	domeen.tld	36
367	dnslog			sendgrid.net	35
382	iodine	4.txt	-m 1130	domeen.tld	35
383	dnslog			tallinn.ee	34
400	dnscat2	1.txt	Krüpteeritud	domeen.tld	33
401	dnslog			gfycat.com	32
415	iodine	2.txt	-m 1130 -M 100	domeen.tld	32
416	dnslog			2gis.com	31
417	iodine	1.txt	-m 1130 -M 100	domeen.tld	31
418	dnslog			me-talk.ru	31
420	iodine	3.txt	-m 1130 -M 100	domeen.tld	31
421	dnslog			7streams.pro	30
458	dnscat2	3.txt	Krüpteeritud	domeen.tld	29
459	dnslog			consensu.org	29
487	dnscat2	3.txt	Avatekst	domeen.tld	28
488	dnslog			ohtuleht.ee	27
493	dnscat2	1.txt	Avatekst	domeen.tld	27
494	dnslog			tartulv.ee	26
572	iodine	1.txt	-m 1130	domeen.tld	24
573	dnslog			at.ua	24
575	iodine	2.txt	-m 1130	domeen.tld	24
576	dnslog			lastpass.com	23
589	iodine	3.txt	-m 1130	domeen.tld	23
590	dnslog			shutterstock.com	22
1446	Poison Frog		15 min sessioon	myleftheart.com	10
1447	dnslog			cloudbeds.com	10
2301	OilRig		Tsükkel 1x	withyourface.com	7
2302	dnslog			blue-tomato.com	7
24096	FrameworkPOS		15 min sessioon	a193-45-3-47-deploy-akamaitechnologies.com	2
24097	dnslog			survata.com	1

Lisa 3 – Unikaalsete alamdomeenide arv 2. taseme domeeni kohta ühe ööpäeva lõikes

Jrk nr	Tüüp	Andme-fail	Parameetrid	2. taseme domeen	Alam-domeenide arv
1	dnscat2	7.dat	Krüpteeritud	domeen.tld	21330
2	dnscat2	6.dat	Krüpteeritud	domeen.tld	21316
3	iodine	5.txt	-m 1130 -M 100	domeen.tld	20010
4	dnscat2	7.dat	Avatekst	domeen.tld	19679
5	dnscat2	6.dat	Avatekst	domeen.tld	19507
6	dnscat2	5.txt	Krüpteeritud	domeen.tld	15314
7	iodine	6.dat	-m 1130	domeen.tld	14351
8	dnscat2	5.txt	Avatekst	domeen.tld	14065
9	iodine	5.txt	-m 1130	domeen.tld	7172
10	iodine	7.dat	-m 1130	domeen.tld	3941
11	iodine	7.dat	-m 1130 -M 100	domeen.tld	3925
12	dnslog			gstatic.com	3673
17	OilRig		Tsükkel 100x	withyourface.com	696
18	dnslog			msn.com	519
78	OilRig		Tsükkel 10x	withyourface.com	70
79	dnslog			adobe.com	69
83	iodine	4.txt	-m 1130 -M 100	domeen.tld	68
84	dnslog			com.au	67
91	dnscat2	4.txt	Krüpteeritud	domeen.tld	61
92	dnslog			onef.pro	60
95	dnscat2	4.txt	Avatekst	domeen.tld	55
96	dnslog			akamai.net	53
128	dnscat2	2.txt	Krüpteeritud	domeen.tld	41
129	dnslog			ipv6test.com	40
141	dnscat2	2.txt	Avatekst	domeen.tld	36
142	dnslog			imgix.net	35
145	iodine	4.txt	-m 1130	domeen.tld	35

146	dnslog			push.world	34
152	dnscat2	1.txt	Krüpteeritud	domeen.tld	33
153	dnslog			svc.ms	32
160	iodine	2.txt	-m 1130 -M 100	domeen.tld	32
161	dnslog			academic.ru	31
162	iodine	1.txt	-m 1130 -M 100	domeen.tld	31
163	iodine	3.txt	-m 1130 -M 100	domeen.tld	31
164	dnslog			tam.by	30
174	dnscat2	3.txt	Krüpteeritud	domeen.tld	29
175	dnslog			trafficmanager.net	29
184	dnscat2	3.txt	Avatekst	domeen.tld	28
185	dnslog			weborama.fr	27
194	dnscat2	1.txt	Avatekst	domeen.tld	27
195	dnslog			espn.com	26
208	iodine	1.txt	-m 1130	domeen.tld	24
209	iodine	2.txt	-m 1130	domeen.tld	24
210	dnslog			kodik-cdn.com	23
217	iodine	3.txt	-m 1130	domeen.tld	23
218	dnslog			t-online.de	22
567	Poison Frog		15 min sessioon	myleftheart.com	10
568	dnslog			businessinsider.com	9
817	OilRig		Tsükkel 1x	withyourface.com	7
818	dnslog			goo.gl	6
3428	FrameworkPOS		15 min sessioon	a193-45-3-47-deploy-akamaitechnologies.com	2
3429	dnslog			survata.com	1

Lisa 4 – Unikaalsete alamdomeenide arv 2. taseme domeeni kohta ühe ööpäeva lõikes IP-aadresside piiranguga

Jrk nr	Tüüp	Andmefail / parameetrid	2. taseme domeen	Alam-domeenide arv	IP aadresside arv
1	dnscat2	7.dat	domeen.tld	19679	1
2	dnscat2	6.dat	domeen.tld	19507	1
3	iodine	6.dat	domeen.tld	14351	1
4	dnscat2	5.txt	domeen.tld	14065	1
5	iodine	5.txt	domeen.tld	7172	1
6	iodine	7.dat	domeen.tld	3941	1
7	OilRig	Tsükkel 100x	withyourface.com	696	1
8	dnslog		gamepedia.com	230	1
14	OilRig	Tsükkel 10x	withyourface.com	70	1
15	dnslog		bezformata.com	68	1
16	dnscat2	4.txt	domeen.tld	55	1
17	dnslog		weeknumber52.com	50	1
23	dnscat2	2.txt	domeen.tld	36	1
24	iodine	4.txt	domeen.tld	35	1
25	dnslog		gov.ua	35	2
33	dnscat2	3.txt	domeen.tld	28	1
34	dnslog		gfycat.com	28	9
40	dnscat2	1.txt	domeen.tld	27	1
41	dnslog		espn.com	27	8
44	iodine	1.txt	domeen.tld	24	1
45	iodine	2.txt	domeen.tld	24	1
46	dnslog		diplotop.ru	24	1
49	iodine	3.txt	domeen.tld	23	1
50	dnslog		globalmarket.com	23	1
181	Poison Frog	15 min sessioon	myleftheart.com	10	1
182	dnslog		fill.ee	10	3
343	OilRig	Tsükkel 1x	withyourface.com	7	1

344	dnslog		vastused.ee	7	1
3183	FrameworkPOS	15 min sessioon	a193-45-3-47-deploy-akamaitechnologies.com	2	1
3184	dnslog		1plus1.video	2	2

Lisa 5 – 5.3 Olekuta ja olekupõhiste tuvastusmeetodite kombineerimise tulemus

Jrk nr	Tüüp	Andmefail / parameetrid	2. taseme domeen	Alam-domeenide arv	IP aadresside arv
1	dnscat2	6.dat	domeen.tld	19505	1
2	dnscat2	7.dat	domeen.tld	19487	1
3	iodine	6.dat	domeen.tld	14231	1
4	iodine	5.txt	domeen.tld	6907	1
5	dnscat2	5.txt	domeen.tld	6846	1
6	iodine	7.dat	domeen.tld	1343	1
7	OilRig	Tsükkel 100x	withyourface.com	696	1
8	dnslog		msn.com	495	8
12	OilRig	Tsükkel 10x	withyourface.com	70	1
13	dnslog		nflxvideo.net	41	3
14	dnscat2	4.txt	domeen.tld	41	1
15	dnscat2	2.txt	domeen.tld	33	1
16	dnslog		cloudfront.net	29	8
18	dnscat2	1.txt	domeen.tld	26	1
19	dnscat2	3.txt	domeen.tld	25	1
20	iodine	4.txt	domeen.tld	24	1
21	dnslog		livetex.ru	22	8
29	iodine	1.txt	domeen.tld	11	1
30	iodine	2.txt	domeen.tld	11	1
31	dnslog		gmx.net	10	1
39	iodine	3.txt	domeen.tld	10	1
40	dnslog		cycleworld.com	9	1
43	Poison Frog	15 min sessioon	myleftheart.com	9	1
44	dnslog		tnt-online.ru	8	3
46	OilRig	Tsükkel 1x	withyourface.com	7	1
47	dnslog		ubembed.com	6	3
495	FrameworkPOS	15 min sessioon	a193-45-3-47-deploy-akamaitechnologies.com	1	1