Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**«Ασφάλεια πρωτοκόλλου DNS over https/tls»** **«DNS over https/tls security»**
Ονοματεπώνυμο Φοιτητή	**ΠΑΥΛΟΣ ΑΛΙΜΠΑΛΗΣ**
Πατρώνυμο	**ΝΙΚΟΛΑΟΣ**
Αριθμός Μητρώου	**ΜΠΚΣΑ/18002**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **Δεκέμβριος 2020**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης Επίκουρος Καθηγητής	Μαρία Βίρβου Καθηγήτρια	Ευθύμιος Αλέπης Αναπληρωτής Καθηγητής

Αφιερώνεται στην αγαπημένη μου φίλη Αλεξία ,

που πίστεψε σε εμένα από την αρχή

και ήταν πάντα δίπλα μου…

ΠΕΡΙΛΗΨΗ

Το αντικείμενο έρευνας της παρούσας μεταπτυχιακής διατριβής είναι το σύστημα dns over https και πώς μπορούμε να εξάγουμε πληροφορίες από αυτό που θα μας βοηθήσουν να αυξήσουμε την ασφάλεια.

Αρχικά, η ανάγκη υλοποίησης του DNS προήλθε από την «αδυναμία» του ανθρώπινου εγκεφάλου να απομνημονεύει πολλά και μεγάλα νούμερα. Κάθε υπολογιστής που συνδέεται σε ένα δίκτυο έχει μια ip διεύθυνση η οποία αποτελείται από έναν αριθμό μήκους 32 bit (και με το πρωτόκολλο ipv6 128 bit). Ένας υπολογιστής είναι πολύ εύκολο να απομνημονεύει τέτοιου μήκους διευθύνσεις κάτι που δεν ισχύει για έναν άνθρωπο. Έτσι γεννήθηκε η ιδέα για ένα πρωτόκολλο το οποίο θα αντιστοιχίζει ip διευθύνσεις που είναι εύκολες να διαβαστούν από έναν ηλεκτρονικό υπολογιστή σε ονόματα, που είναι πιο εύκολο να τα θυμάται ο ανθρώπινος εγκέφαλος. Έτσι το σύστημα ονοματοδοσίας στο διαδίκτυο έγινε ένα σημαντικό και αναπόσπαστο κομμάτι της καθημερινής μας διαδικτυακής δραστηριότητας. Κάθε φορά που πλοηγούμαστε στο διαδίκτυο, στέλνουμε ένα email και γενικότερα χρησιμοποιούμε υπηρεσίες διαδικτύου το πρωτόκολλο αυτό αναλαμβάνει να αντιστοιχίσει ip διευθύνσεις με ονόματα για να σταλούν τα πακέτα των υπηρεσιών που ζητάμε στο σωστό παραλήπτη.

Η δομή της εργασίας έχει ως ακολούθως:

- Στο πρώτο κεφάλαιο θα γίνει μια εισαγωγή στο σύστημα ονοματοδοσίας στο διαδίκτυο και θα περιγραφεί ο τρόπος λειτουργίας του.
- Στο δεύτερο κεφάλαιο θα γίνει μια εισαγωγή σε βασικές έννοιες σχετικά με θέματα ασφαλείας και συγκεκριμένα σε επιθέσεις στο πρωτόκολλο dns.
- Στο τρίτο κεφάλαιο θα γίνει ανάλυση του τρόπου λειτουργίας του dns over https.
- Στο τέταρτο κεφάλαιο θα αναλύσουμε με ποιους τρόπους μπορούμε να αναγνωρίσουμε και να επιβλέψουμε κίνηση DNS over HTTPS σε ένα δίκτυο.
- Στο πέμπτο κεφάλαιο θα γίνει μια παρουσίαση του αποκεντρωμένου μοντέλου διαχείρισης του DNS.
- Στο έκτο κεφάλαιο θα παρουσιαστούν τα συμπεράσματα που προέκυψαν από την έρευνα που πραγματοποιήθηκε.

ABSTRACT

The subject of this master's thesis is the dns over https system and how we can extract information from it that will help us increase security.

Initially, the need to implement DNS protocol came from the "inability" of the human brain to memorize large numbers. Each computer connected to a network has an ip address which consists of a 32 bit length number (and 128 bit with the ipv6 protocol). A computer is very easy to memorize such length addresses which is not true for a human being. This gave rise to the idea of a protocol that would assign ip addresses that are easy to read from a computer into names that are easier for the human brain to remember. So the domain name system has become an important and integral part of our daily internet activity. Each time we navigate the Internet, we send an email and generally use Internet services this protocol undertakes to assign ip addresses into domain names and send the required packages to the correct recipient.

The structure of this thesis is as follows:

- The first chapter will introduce the domain name system protocol and will describe how it works.
- The second chapter will introduce some basic concepts about security issues and in particular attack vectors on the dns protocol.
- The third chapter will analyze how dns over https works.
- The fourth chapter will analyze effective ways for DNS over HTTPS monitoring
- The fifth chapter will introduce decentralized blockchain-based DNS
- The sixth chapter will present the conclusions drawn from the research carried out.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Το πρωτόκολλο DNS, αν και σημαντικό και αναπόσπαστο κομμάτι της καθημερινής διαδικτυακής μας δραστηριότητας, είναι κατανοητό από λίγους επαγγελματίες της πληροφορικής σε σχέση με τη σπουδαιότητά του. Ακόμα και επαγγελματίες στο χώρο του security που έχουν επιφορτιστεί με το έργο της προστασίας ενός οργανισμού συχνά δεν έχουν πλήρη επίγνωση των ευπαθειών που έχει το πρωτόκολλο. Πολύ σημαντικό ρόλο σε αυτό παίζει ότι συνήθως οι επαγγελματίες της πληροφορικής ρυθμίζουν μια φορά αυτό το πρωτόκολλο και μετά το «ξεχνάνε» για πολύ καιρό, εφόσον λειτουργεί απροβλημάτιστα. Είναι πολύ λίγες οι φορές που θα χρειαστεί να αλλάξουν κάτι στο configuration μιας dns υποδομής και έτσι σπάνια ελέγχονται οι ρυθμίσεις του και σε κάποιες περιπτώσεις, δεν υπάρχει και η τεχνογνωσία για να γίνει κάτι τέτοιο διότι πολλοί οργανισμοί έχουν αναθέσει τη ρύθμιση και συντήρηση τέτοιων υποδομών σε άτομα που δεν έχουν την κατάλληλη τεχνογνωσία για τη συγκεκριμένη εργασία.

Σαν πρωτόκολλο χωρίς καμία μορφή κρυπτογράφησης, το dns έγινε ένας από τους πιο συχνούς στόχους κακόβουλων επιθέσεων καθώς τα δεδομένα που ανταλλάσσονται μεταξύ server και client είναι σε plain text. Έτσι οι κακόβουλοι χρήστες μπορούν με διάφορες τεχνικές να «χτυπήσουν» σε κάποιο από τα ευάλωτα σημεία του πρωτοκόλλου. Κάποιες από αυτές τις τεχικές είναι το Domain hijacking, DNS flood attack, Distributed Reflection Denial of Service, Cache poisoning, DNS tunneling, DNS hijack attack, NXDOMAIN attack, Phantom domain attack κτλ. Στις μέρες μας τα περισσότερα λογισμικά ασφαλείας χρησιμοποιούν το dns για να ελέγξουν την κίνηση του δικτύου και να προλάβουν ή να ανακαλύψουν επιθέσεις από κακόβουλους χρήστες και γενικότερα η κίνηση που παράγει το dns στο δίκτυο χρησιμοποιείται και αναλύεται για διάφορους σκοπούς, όπως από antivirus για την αποτροπή επισκέψεων σε κακόβουλες ip διευθύνσεις ή ακόμα και για παρακολούθηση της κίνησης απλών χρηστών για διαφημιστικούς ή και κακόβουλους σκοπούς.

Αυτή η ευάλωτη αρχιτεκτονική του πρωτοκόλλου σε θέματα ασφαλείας αλλά και σε θέματα ιδιωτικότητας, έκανε τους επιστήμονες και τους ερευνητές της πληροφορικής να αναζητήσουν εναλλακτικές λύσεις σε σχέση με την αρχική αρχιτεκτονική. Καινούρια πρωτόκολλα όπως το DNSCrypt, DNS over HTTPS, DNS over TLS and DNSSEC έκαναν την εμφάνισή τους για να ενισχύσουν την ιδιωτικότητα και την ασφάλεια του διαδικτύου. Στην παρούσα εργασία θα εμβαθύνουμε στο πρωτόκολλο DNS over HTTPS στον τομέα της ασφάλειας πρωτίστως και δευτερευόντως στον τομέα της ιδιωτικότητας. Πιο αναλυτικά, στο πρώτο κεφάλαιο θα γίνει μια λεπτομερής ανάλυση του πρωτοκόλλου dns και θα περιγραφεί λεπτομερώς πως λειτουργεί και ποια δεδομένα ανταλλάσσονται κατά τη διάρκεια της επικοινωνίας του εξυπηρετητή με τον πελάτη. Στο δεύτερο κεφάλαιο θα γίνει μια εισαγωγή σε βασικές έννοιες σχετικές με θέματα

ασφαλείας και συγκεκριμένα θα αναπτυχθούν οι επιθέσεις που αναφέρθηκαν παραπάνω κατά του πρωτοκόλλου αλλά και ζητήματα ιδιωτικότητας των χρηστών του διαδικτύου. Στο τρίτο κεφάλαιο θα γίνει εμβάθυνση στο πρωτόκολλου DNS over HTTPS και θα αναλύσουμε διεξοδικά θέματα ασφαλείας και θέματα ιδιωτικότητας.

ΚΕΦΑΛΑΙΟ 1. Το σύστημα DNS

1.1 Ιστορικό

Η συνεχής εξέλιξη του διαδικτύου γέννησε την ανάγκη ενός συστήματος όπου κάποιου είδους δομή θα φιλοξενούσε μια λίστα με τα ονόματα των κεντρικών υπολογιστών της εποχής. Πριν την καθιέρωση του συστήματος dns, το αρχείο hosts.txt αντίστοιχα σε κάθε λειτουργικό έπαιζε το ρόλο της βάσης δεδομένων και ήταν υπεύθυνο για τη ονοματοδοσία των κεντρικών υπολογιστών. Συγκεκριμένα το αρχείο hosts.txt «γεννήθηκε» το Δεκέμβριο του 1973 με το πρότυπο RFC 592 όπου και καθιερώθηκε η πρώτη επίσημη σύμβασης ονοματοδοσίας στην οποία επιτρέπονταν μόνο αριθμοί, γράμματα και παύλες. Με την συγκέντρωση και των 81 ονομάτων της εποχής και την εισαγωγή τους στο αρχείο hosts μπορούσαν οι διαχειριστές του δικτύου να το κατεβάσουν μέσω ftp και να το αποθηκεύσουν κατάλληλα ανάλογα με το λειτουργικό σύστημα που χρησιμοποιούσαν. Αυτό το αρχείο ήταν το μοναδικό που ήταν διαθέσιμο έτσι ώστε όλοι να έχουν το ίδιο και για την ιστορία, το πρώτο αρχείο hosts.txt έγινε διαθέσιμο δημόσια την 25 Μαρτίου 1974.

Καθώς το πρώτο διαδίκτυο (ARPANET) του κόσμου άρχισε να γίνεται όλο και πιο δημοφιλές, η ανάγκη να προσθέτουμε όλο και περισσότερους servers που θα διαχειρίζονταν την αποστολή αλληλογραφίας γινόταν συνεχώς μεγαλύτερη. Μαζί με αυτή την αυξανόμενη ανάγκη για hardware, έπρεπε να ενημερώνουμε συνεχώς το αρχείο hosts.txt με τα νέα ονόματα και να το διανείμουμε στους διαχειριστές των δικτύων για να το ενημερώσουν και αυτοί με τη σειρά τους. Η αρχική ιδέα για τη δομή αυτών των ονομάτων ήταν να έχει κάθε τομέας το δικό του hostname. Για παράδειγμα, εάν μια εταιρεία είχε όνομα company και είχε γραφεία στην Αθήνα τότε έπρεπε να δημιουργηθεί ξεχωριστό όνομα για τα γραφεία αυτά. Η διεύθυνση ηλεκτρονικού ταχυδρομείου των γραφείων της Αθήνας θα ήταν για παράδειγμα info@companyath και όχι info@company. Αυτή η δομή δημιούργησε μεγάλη σύγχυση, καθώς αν δεν ήσουν σίγουρος σε ποιο γραφείο του οργανισμού ανήκε το άτομο που θες να επικοινωνήσεις το email ήταν πιθανόν να μην έβρισκε τον παραλήπτη του. Με την πάροδο του χρόνου αυτή η δομή άλλαξε και από address@host έγινε address@hostname.company.domain

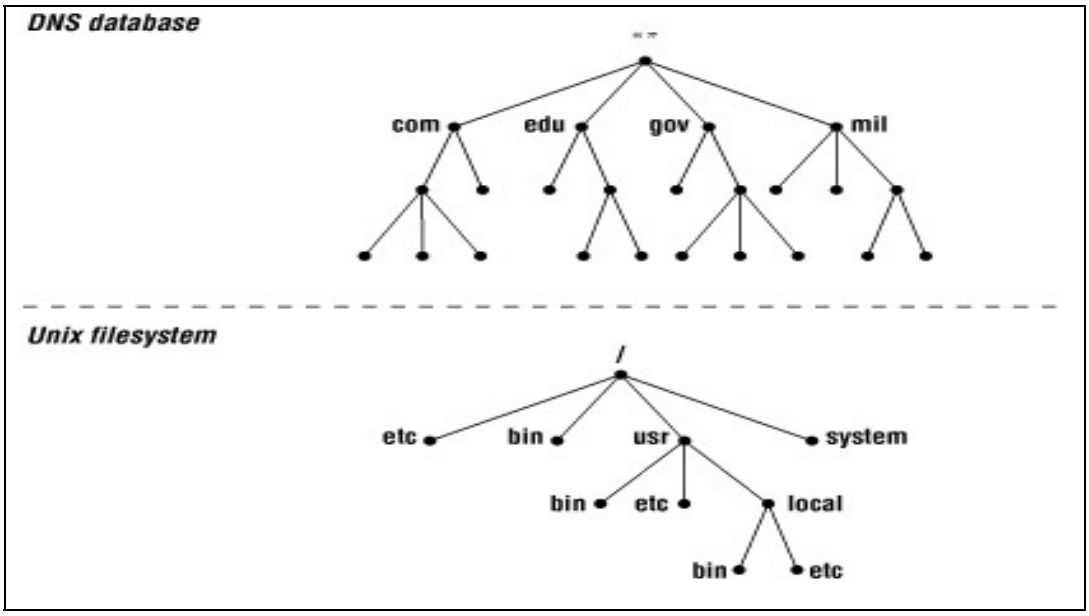
λύνοντας προσωρινά αυτά τα προβλήματα και εισάγοντας για πρώτη φορά τον όρο «Internet Domain Names» κάνοντας έτσι πιο εύκολη τη διαχείριση των ονομάτων και λύνοντας έτσι τα χέρια των διαχειριστών των δικτύων. Το 1982 έγινε δημόσια διαθέσιμος ο πρώτος hostname server που αρχικά χρησιμοποιήθηκε για να μοιραστούν πληροφορίες σχετικά με Δίκτυα, πύλες και κεντρικούς υπολογιστές, αλλά τελικά χρησιμοποίησε την ίδια μορφή των domain queries που θα χρησιμοποιήσουμε στη συνέχεια της εξέλιξης. Όλα αυτά τα προβλήματα ξεκίνησαν μια συζήτηση για να δημιουργηθεί ένα πιο έξυπνο και πιο πρακτικό σύστημα ονοματοδοσίας και τον Οκτώβριο του 1984 διατέθηκε δημόσια το πρότυπο RFC 920 με τις απαιτήσεις για την υλοποίηση του DNS ARPANET και ποια βήματα θα έπρεπε να γίνουν στη συνέχεια. Το πρότυπο περιείχε και τα πρώτα TLD τα οποία ήταν .GOV, .MIL, .EDU, .COM, .ORG καθώς και τα domain των χωρών με δύο γράμματα.

Το καινούριο αυτό πρότυπο υιοθετήθηκε και εφαρμόστηκε πολύ γρήγορα και το πρώτο domain που κατοχυρώθηκε στην ιστορία του διαδικτύου ήταν το nordu.net την 1 Ιανουαρίου 1985. Παράλληλα, το Αμερικανικό Defense Information Systems Agency που ήλεγχε το arpanet ανέθεσε τη συντήρηση της υποδομής στο Stanford Research Institute και έτσι γεννήθηκε η πρώτη DNS υποδομή όπως την ξέρουμε σήμερα.

1.2 Domain namespace

Στην ουσία το dns είναι μία κατανεμημένη βάση δεδομένων. Αυτή η δομή μας επιτρέπει να ελέγχουμε τμήματα της βάσης μας ενώ τα δεδομένα μας είναι διαθέσιμα σε ολόκληρο το δίκτυο μέσω της αρχιτεκτονικής server-client. Η ταχύτητα με την οποία ανταποκρίνεται το σύστημά μας εξασφαλίζεται με τεχνικές caching, όπως θα συζητήσουμε στο δεύτερο κεφάλαιο της εργασίας.

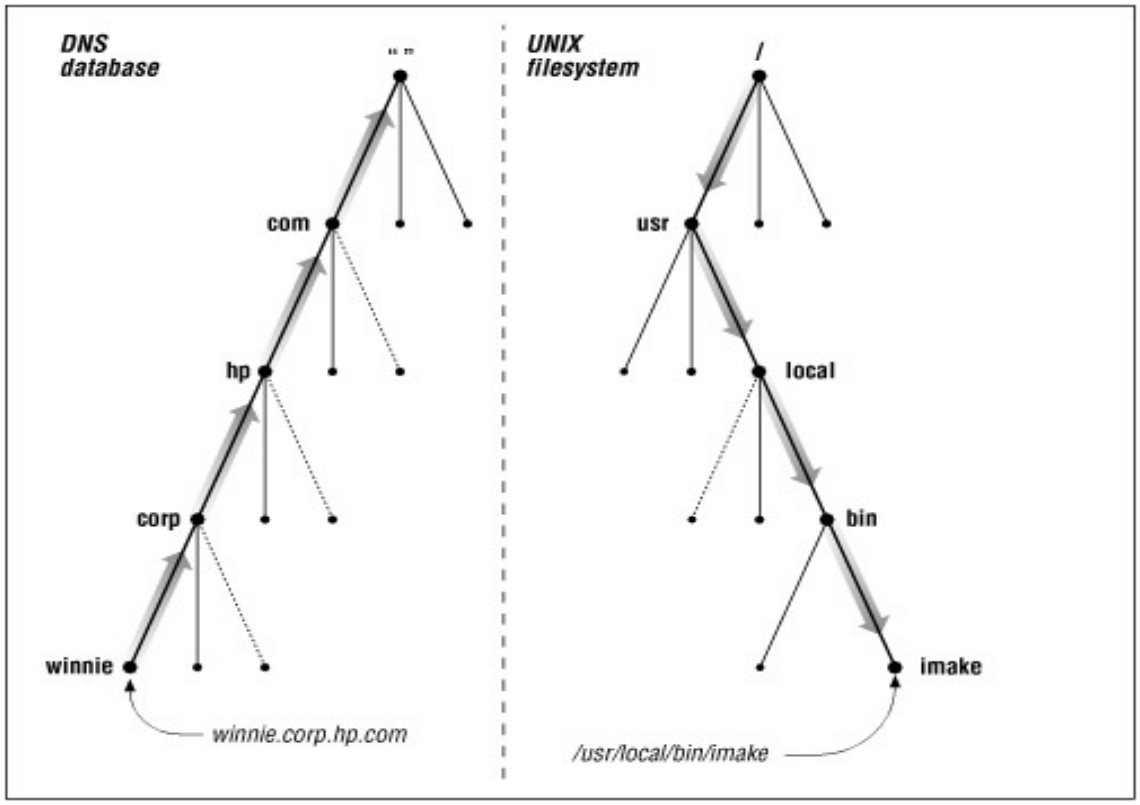
Η δομή της βάσης δεδομένων του συστήματος dns είναι παρόμοια με τη δομή του συστήματος αρχείων του unix και απεικονίζεται στην εικόνα 1.1 σαν ένα δέντρο με την κορυφή να είναι η ρίζα *(root) της βάσης. Κάθε κόμβος στο δέντρο έχει μια ετικέτα η οποία προσδιορίζει τον κόμβο σε σχέση με τον γονέα του.



Εικόνα 1.1 Η βάση δεδομένων DNS σε σχέση με το unix filesystem

Κάθε κόμβος επίσης είναι η ρίζα κάθε υποδένδρου κάτω από αυτόν και όλα αυτά τα υποδένδρα απεικονίζουν τμήματα της συνολικής βάσης δεδομένων. Για παράδειγμα, ένα domain name είναι η κορυφή του υποδένδρου που σχηματίζεται με αυτό σαν κορυφή και κάθε subdomain είναι παιδί του.

Κάθε domain έχει ένα μοναδικό όνομα με το οποίο τοποθετείται στη βάση δεδομένων. Για παράδειγμα, ένα domain name είναι η ακολουθία των ετικετών κάθε από τον κόμβο που είναι ο root για το υποδένδρο που σχηματίζει μέχρι τη ρίζα του, με τις ετικέτες να χωρίζονται με κουκίδες (.) Κάτι αντίστοιχο γίνεται και με το filesystem του unix, με τη διαφορά ότι το path διαβάζεται από την ρίζα μέχρι την μέχρι τον τελευταίο κόμβο του δένδρου και όχι αντίθετα όπως τα domain names. Στην εικόνα 1.2 φαίνονται παραδείγματα domain name και unix filesystem.



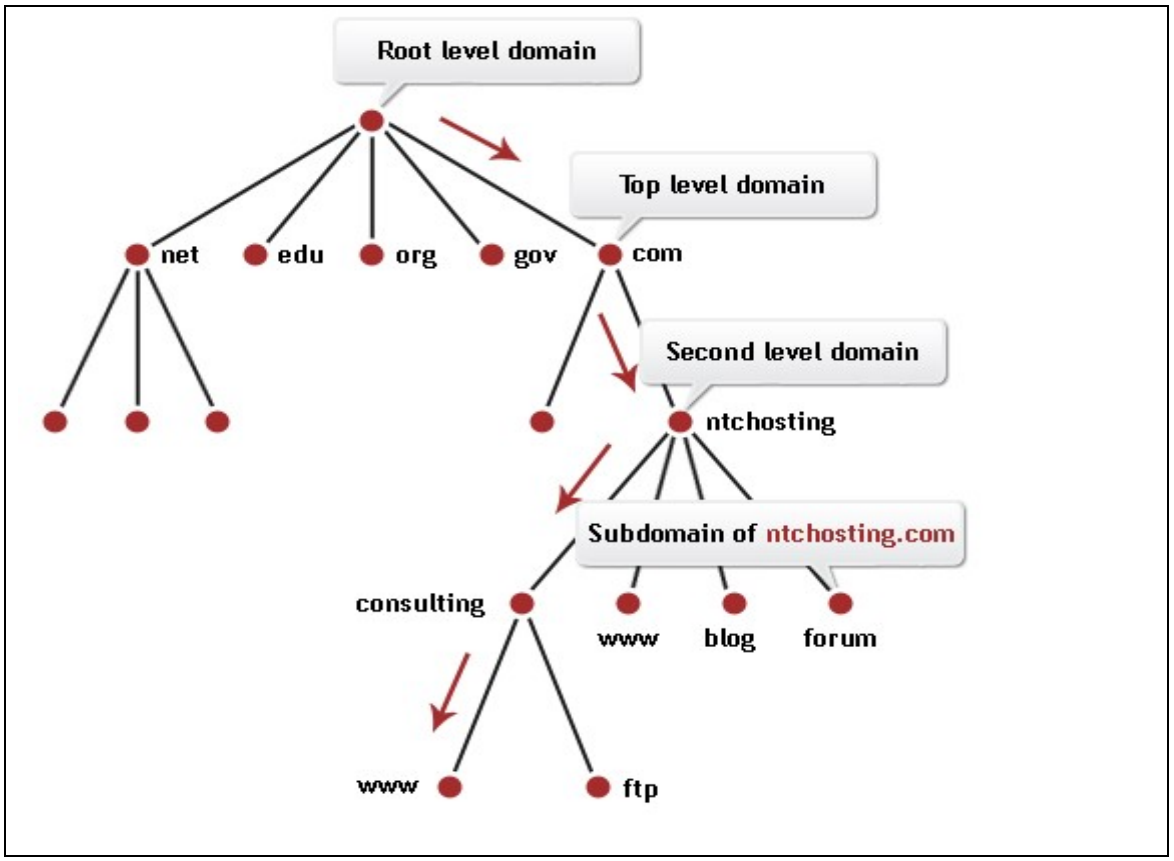
Εικόνα 1.2 Κατασκευή ονομάτων στο dns και στο unix filesystem

Τα domains χρησιμοποιούνται ως ευρετήρια στη βάση. Ένα υποδένδρο ενός domain name μπορεί να περιέχει πληροφορίες για hosts και για subdomains που τα domain τους είναι μέσα στο υποδένδρο με κορυφή το αρχικό domain. Βέβαια τα hosts μπορούν να δείχνουν και σε άλλα domain διότι πολλά διαφορετικά domain μπορούν να δείχνουν στην ίδια ip. Αυτό επιτυγχάνεται με έναν απλό pointer από το host προς το domain name που δείχνει.

Αυτή η περίπλοκη δομή που υιοθετήθηκε για την ιεραρχική βάση δεδομένων του dns μας λύνει πολλά από τα προβλήματα που είχαμε με την αρχική δομή στα πρώτα χρόνια της ονοματοδοσίας με το hosts.txt. Με αυτή τη δομή αποφεύγουμε τυχόν συγκρούσεις στα ονόματα των domains και συγχρόνως εξασφαλίζουμε ότι κάθε domain έχει μοναδικό όνομα έτσι ώστε ο εκάστοτε ιδιοκτήτης του κάθε ονόματος να μπορεί να διαχειρίζεται hosts και subdomains σύμφωνα με τις ανάγκες του.

Αυτή τη θεωρητική δομή που έχουμε αναφέρει έως τώρα θα την ονομάσουμε domain namespace, που στην ουσία είναι μια κατανεμημένη βάση δεδομένων σε δενδρική μορφή με μία ρίζα (root) στην κορυφή του και ευρετηριασμένη με βάση το domain name, όπου κάθε domain

name είναι ένα μονοπάτι σε αυτό το δένδρο και έχει όριο σε βάθος τα 127 επίπεδα.



Εικόνα 1.3 Ιεραρχική δομή του DNS namespace

1.3 Internet domain namespace

Μέχρι τώρα έχουμε μιλήσει μόνο για τη θεωρητική δομή του domain namespace. Για να μπορούμε να καταλάβουμε όμως τη δομή όλων αυτών των ονομάτων που βλέπουμε καθημερινά στην πλοήγησή μας στο διαδίκτυο, πρέπει να εμβαθύνουμε λίγο στον τρόπο με τον οποίο φτιάχνονται αυτά και να μάθουμε ποιους άγραφους κανόνες ακολουθούμε στα domain των υψηλότερων επιπέδων.

Top-Level Domains

Τα αρχικά top-level domains που χώρισαν το internet domain namespace ήταν τα εξής:

- com
  Πήρε την ονομασία του από το commercial και ήταν πιο πολύ για οργανισμούς όπως η IBM, η Microsoft κτλ
- edu
  Για εκπαιδευτικούς οργανισμούς
- gov
  Για κυβερνητικούς οργανισμούς
- mil
  Για στρατιωτικούς οργανισμούς
- org
  Για μη κερδοσκοπικούς οργανισμούς
- net
  Για οργανισμούς που παρείχαν δικτυακές υποδομές
- int
  Για διεθνείς οργανισμούς

Country code Top-Level Domains

Η διεθνοποίηση του διαδικτύου έφερε την ανάγκη για περισσότερα domains. Έτσι οι αρμόδιοι αποφάσισαν να επιτρέψουν και άλλα top-level domain names, αυτή τη φορά με βάση τη γεωγραφική θέση. Για παράδειγμα η Ελλάδα είχε gr, η Γαλλία fr και ούτω καθεξής.

Καινούρια Top-Level Domains

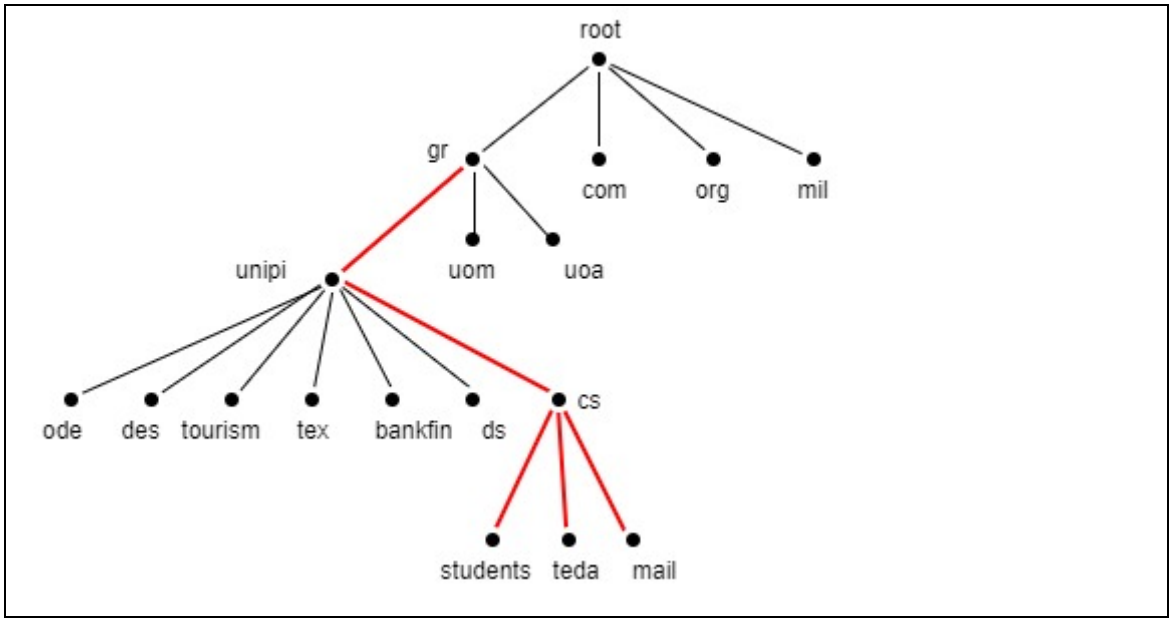
Η αυξανόμενη ζήτηση διεθνώς και η μεγάλη εξάπλωση του διαδικτύου σε όλο τον κόσμο έφερε ακόμα μεγαλύτερη ανάγκη για περισσότερο «domain space» με αποτέλεσμα το 2000 ο οργανισμός που διαχειρίζεται το DNS (ICAAN) να δημιουργήσει 7 καινούρια top-level domains που θα χρησιμοποιούνταν για συγκεκριμένους σκοπούς. Αυτά ήταν εξής:

- aero
  Για την αεροναυτική βιομηχανία
- biz
- coop
- info

- museum
- Για τα μουσεία
- name
  Για ιδιώτες
- pro
  Για επαγγελματίες

Από τότε ο ICAAN έχει εγκρίνει πολλά καινούρια top-level domain τα οποία σήμερα αριθμούν μερικές εκατοντάδες.

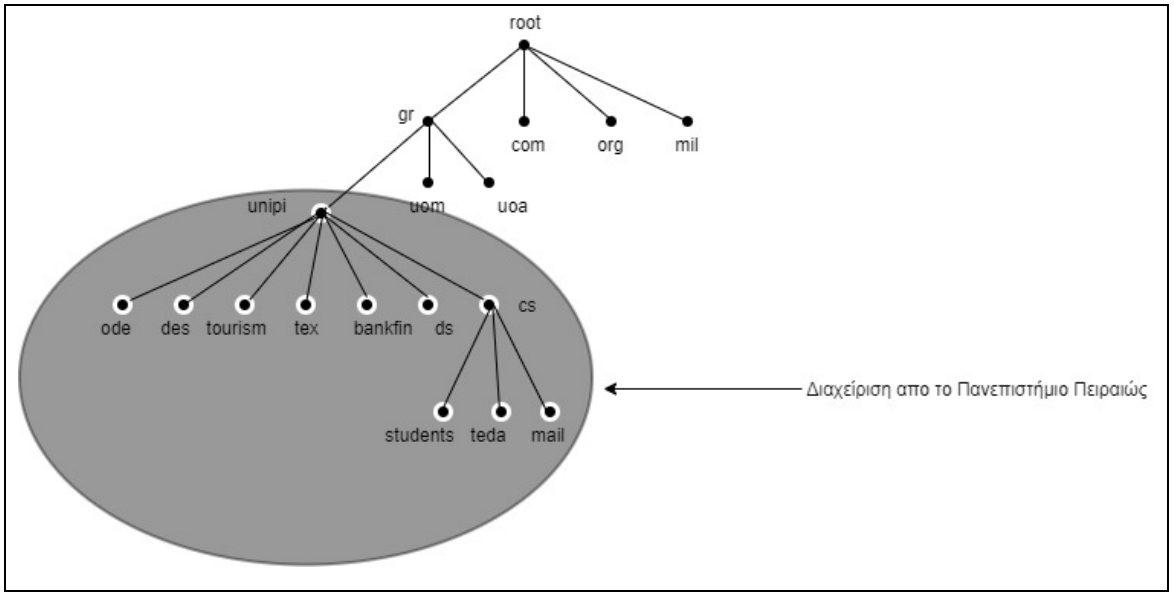
Τώρα που ξέρουμε τη δομή του domain namespace και τι είναι τα top-level domain, μπορούμε να καταλάβουμε τι ακριβώς είναι ένα domain name όταν το βλέπουμε. Για παράδειγμα, ας προσπαθήσουμε να καταλάβουμε το domain students.cs.unipi.gr Ξέρουμε το top-level domain που είναι το gr. Μετά το gr ακολουθεί το unipi το οποίο είναι το domain name του επόμενου επιπέδου για το πανεπιστήμιο Πειραιά. Στην συνέχεια ακολουθεί το subdomain cs το οποίο είναι το αναγνωριστικό για το τμήμα της πληροφορικής (computer science) και τέλος είναι το students όπου είναι ο host που φιλοξενεί της υπηρεσίες του πανεπιστήμιου προς τους φοιτητές της πληροφορικής.



Εικόνα 1.4 Ενδεικτικό μονοπάτι των subdomains του cs.unipi.gr

1.4 Αποκεντρωμένη διαχείριση

Ένας από τους πρώτους στόχους που είχε το σύστημα dns ήταν να καταφέρει να έχει μια αποκεντρωμένη διαχείριση των domains που εισάγονταν ή υπήρχαν ήδη στη βάση δεδομένων. Αυτό το κατάφερε μέσω ενός συστήματος εξουσιοδοτήσεων. Δηλαδή αυτός που κατοχύρωνε ένα domain είχε την εξουσιοδότηση του οργανισμού διαχείρισης τους συστήματος να το διαχειρίζεται πλήρως και όπως νομίζει αυτός. Ακριβώς με την ίδια λογική, αυτός που κατοχύρωνε ένα domain μπορούσε να δώσει εξουσιοδότηση σε τρίτους να διαχειρίζονται τα subdomain του οργανισμού. Για παράδειγμα, το πανεπιστήμιο Πειραιώς έχει κατοχυρώσει το domain unipi.gr και του έχει δοθεί εξουσιοδότηση να το διαχειρίζεται. Ακριβώς με τον ίδιο τρόπο το subdomain cs.unipi.gr έχει δοθεί στο τμήμα πληροφορικής του πανεπιστημίου Πειραιώς και το διαχειρίζεται πλήρως. Με τη σειρά του το τμήμα πληροφορικής έχει δώσει εξουσιοδότηση για τα subdomains του cs.unipi.gr (πχ το students.cs.unipi.gr, το teda.cs.unipi.gr κτλ) σε τρίτους να τα διαχειρίζονται αυτοί. Έτσι η διαχείριση του συστήματος αποκεντρώθηκε με αποτέλεσμα να γίνει πιο εύκολη η συντήρηση και η ενημέρωση του συστήματος dns.

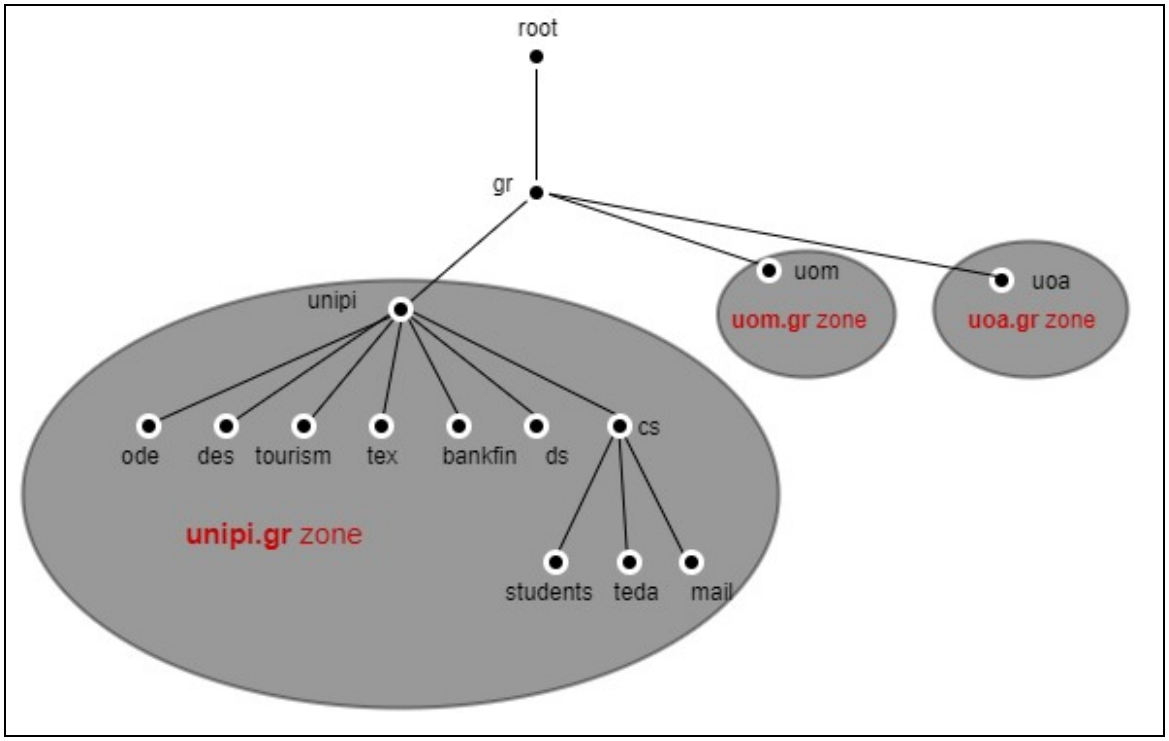


Εικόνα 1.5 Το domain namespace του unipi.gr

1.5 Nameservers και ζώνες

Οι δομές που αποθηκεύουν πληροφορίες σχετικά με το domain namespace λέγονται nameservers. Οι nameservers γενικά αποθηκεύουν πληροφορίες για κομμάτια του domain namespace, τα οποία ονομάζονται ζώνες. Στην ουσία οι nameservers έχουν την δυνατότητα να αλλάζουν πληροφορίες για τη ζώνη όπου έχουν εξουσιοδότηση ή ακόμα και για πολλές ζώνες ταυτόχρονα.

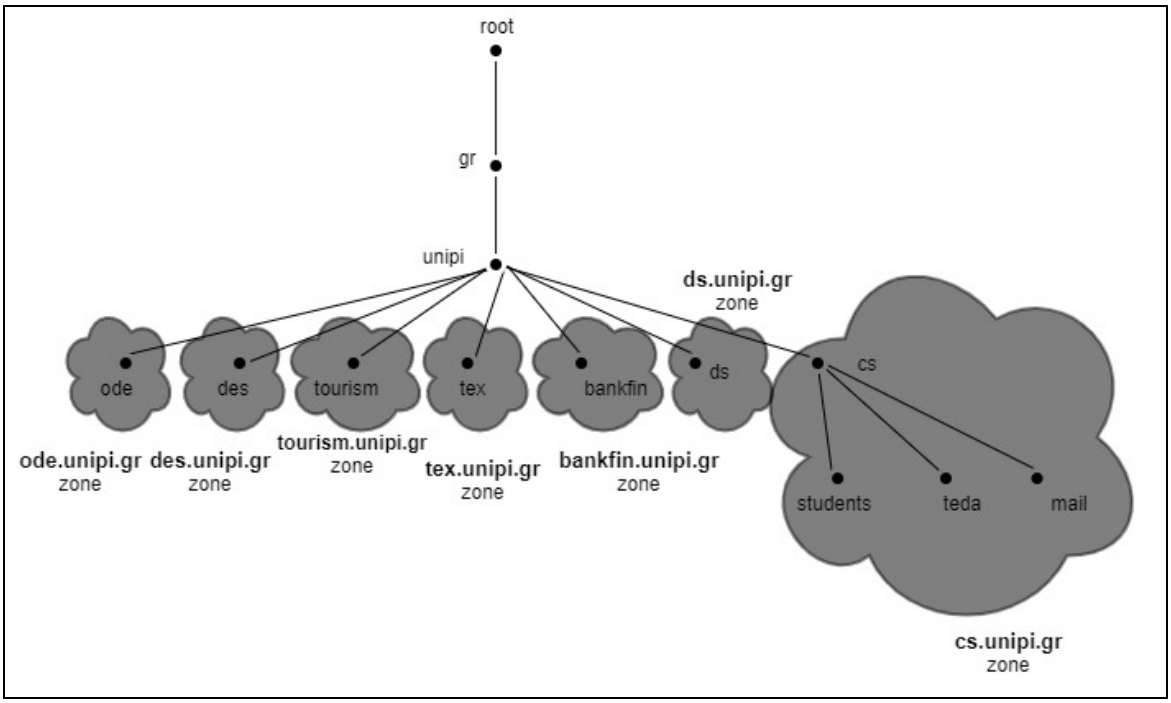
Υπάρχει όμως μια σημαντική διαφορά μεταξύ domain και ζώνης. Όλα τα top-level domain και φυσικά τα επόμενα domain από το δεύτερο επίπεδο και κάτω , όπως το unipi.gr, είναι χωρισμένα σε μικρότερες ομάδες με σκοπό την καλύτερη διαχείρισή τους. Αυτές οι ομάδες ονομάζονται ζώνες. Για παράδειγμα το domain unipi.gr είναι μία ζώνη, το domain uoa.gr είναι άλλη ζώνη και το domain uom.gr είναι μία ξεχωριστή ζώνη και αυτό. Στο επίπεδο των top-level domain υπάρχει η ζώνη του gr domain. Φυσικά με τη λογική των εξουσιοδοτήσεων που εξηγήσαμε στην προηγούμενη παράγραφο ο οργανισμός που κατέχει το gr domain έχει δώσει εξουσιοδότηση στο Πανεπιστήμιο Πειραιά για να διαχειρίζεται το unipi.gr , ειδάλλως θα έπρεπε ο ίδιος να αναλάβει τη διαχείριση του unipi.gr και των subdomain που έχει. Άρα η ζώνη του gr domain κυρίως περιέχει πληροφορίες σχετικά με τις εξουσιοδοτήσεις των subdomain του (του unipi.gr, uom.gr, uoa.gr κτλ) .



Εικόνα 1.6 Οι ζώνες των subdomains του gr domain

Το subdomain του gr domain, unipi.gr, είναι χωρισμένο σε αρκετές ζώνες μέσω των εξουσιοδοτήσεων. Δηλαδή υπάρχουν οι ζώνες του ode, des, tex, tourism, bankfin, ds, cs και ίσως και άλλες, όπου κάθε ζώνη διαχειρίζεται από κάθε τμήμα του Πανεπιστημίου Πειραιώς και μπορεί να έχει εντελώς ξεχωριστούς nameservers η κάθε μία. Άρα κάθε ζώνη περιέχει όλα domain names τα οποία περιέχονται μέσα στο ίδιο domain namespace, εκτός από τα subdomain τα οποία έχουν εξουσιοδότηση τρίτοι να τα διαχειρίζονται. Για παράδειγμα, η ζώνη του gr domain περιέχει όλα τα subdomain που δεν έχουν εξουσιοδοτηθεί σε κάποιον τρίτο, και subdomain όπως είναι το unipi.gr έχουν τη δικιά τους ζώνη. Με τη σειρά του, η ζώνη του domain unipi.gr περιέχει όλα τα subdomain που δεν έχουν εξουσιοδοτηθεί σε κάποιον τρίτο και ούτω καθεξής.

Πλέον, μπορεί να είναι ξεκάθαρο γιατί οι nameservers περιέχουν πληροφορίες για ζώνες και όχι για domains. Ένα domain μπορεί να περιέχει περισσότερες πληροφορίες απ' ότι χρειάζεται ο nameserver διότι μπορεί να περιέχει πληροφορίες για εξουσιοδοτήσεις σε τρίτους, κάτι που ο nameserver δεν χρειάζεται να ξέρει.



Εικόνα 1.7 Οι ζώνες των subdomains του unipi.gr domain

Ο τρόπος με τον οποίο λειτουργούν οι εξουσιοδοτήσεις και οι nameservers για τα subdomains του domain που έχουμε στην κατοχή μας είναι ο εξής. Έστω ότι είμαστε διαχειριστές του domain unipi.gr. Με τη σειρά μας δίνουμε εξουσιοδότηση στη τμήμα Πληροφορικής να διαχειρίζεται το subdomain cs.unipi.gr, στο τμήμα Ψηφιακών Συστημάτων να διαχειρίζεται το ds.unipi.gr, στο τμήμα Οργάνωσης και Διοίκησης Επιχειρήσεων να διαχειρίζεται το ode.unipi.gr και ούτω καθεξής. Άρα έχουμε δώσει εξουσιοδότηση σε τρίτους να διαχειρίζονται μέρος του domain unipi.gr. Ουσιαστικά όμως, αυτό που γίνεται είναι η ανάθεση της διαχείρισης των subdomain σε διαφορετικούς nameserver από τους δικούς μας. Τα δεδομένα που είναι αποθηκευμένα στη ζώνη του unipi.gr έχουν απλά έναν pointer που δείχνει προς τους nameservers που έχουν εξουσιοδοτηθεί από εμάς για το κάθε subdomain και τελικά κάθε ερώτημα προς τους nameservers του unipi.gr για κάποιο από τα subdomain που έχουν παραχωρηθεί θα επιστραφεί με τη σωστή λίστα των nameserver που πρέπει να ρωτήσει για να επικοινωνήσει με κάποιο από αυτά.

1.6 Τύποι των nameserver

Το πρωτόκολλο DNS δύο τύπους nameserver, τον primary master και τον secondary master. Ο primary master nameserver μιας ζώνης διαβάζει τα δεδομένα που αφορούν τη ζώνη του από ένα αρχείο που βρίσκεται στον ίδιο host. Αντιθέτως, ο secondary master nameserver συλλέγει τα δεδομένα που αφορούν τη ζώνη του από άλλον nameserver ο οποίος είναι εξουσιοδοτημένος να έχει πληροφορίες για αυτή, τον master server του. Συνήθως αυτός ο master server είναι ο primary master, αλλά αυτό δεν είναι απαραίτητο. Μπορεί να είναι κάποιος άλλος secondary από τον οποίο φορτώνει δεδομένα για τη ζώνη του. Ο τρόπος λειτουργίας του secondary είναι ότι όταν ξεκινά επικοινωνεί με τον master nameserver και σε περίπτωση που τα δεδομένα που αφορούν τη ζώνη έχουν αλλάξει, τα φορτώνει ξανά έτσι ώστε να είναι ενημερωμένος.

Και οι δύο server, και ο primary και ο secondary έχουν εξουσιοδοτηθεί για τη ζώνη τους και το πρωτόκολλο DNS μας παρέχει δύο τύπους nameserver για να κάνει τη διαχείριση πιο εύκολη, καθώς και για λόγους απόδοσης, διαμοιρασμού του φόρτου και για λόγους διαθεσιμότητας της υπηρεσίας. Ο τρόπος με τον οποίο χρησιμοποιούμε τους nameservers δεν μας περιορίζει, καθώς ένας nameserver μπορεί να χρησιμοποιηθεί για παραπάνω από μία ζώνες ή μπορεί ακόμα να είναι primary σε μία και secondary σε άλλη.

1.7 Αρχεία δεδομένων ζωνών

Τα αρχεία από τα οποία οι primary master servers φορτώνουν τα δεδομένα για κάθε ζώνη για την οποία έχουν εξουσιοδοτηθεί λέγονται zone datafiles. Τα αρχεία αυτά που υπάρχουν στους primary nameservers, γίνονται backup από τους secondary nameservers και κάθε φορά που κάνει restart ο ίδιος ή η υπηρεσία που διαχειρίζεται τα zone datafiles τα ζητάει από τον master έτσι ώστε να ελέγξει αν έχει γίνει κάποια αλλαγή. Τα datafiles περιέχουν εγγραφές που περιγράφουν τη ζώνη που αναφέρονται, δηλαδή όλους τους hosts της ζώνης και πληροφορίες για τυχόν εξουσιοδοτήσεις που έχουν γίνει για τα subdomains του domain namespace.

1.8 Resolvers

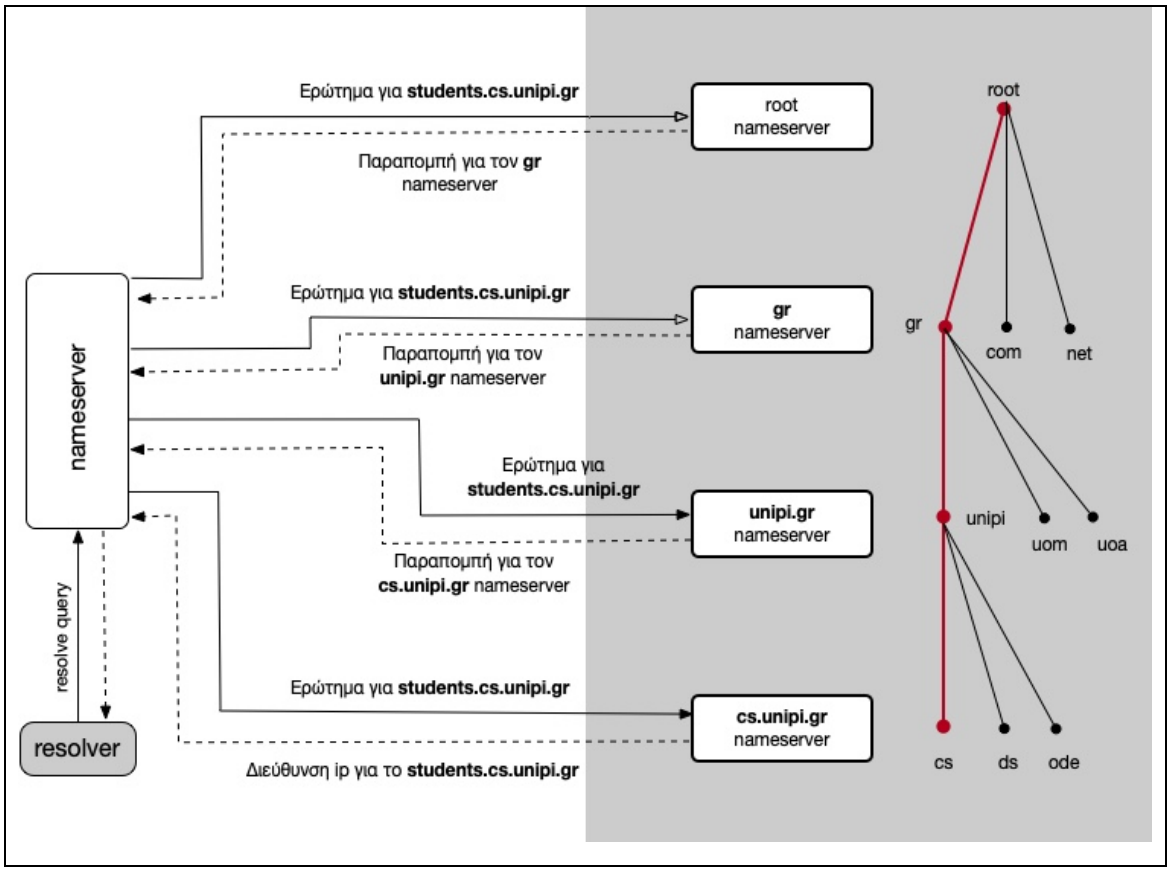
Οι resolvers είναι οι clients που έχουν πρόσβαση στους nameservers και χρησιμοποιούνται από προγράμματα τα οποία χρειάζονται πληροφορίες για ένα domain namespace. Οι υπηρεσίες που προσφέρουν οι resolvers είναι οι εξής:

- Κάνουν ερωτήματα στους nameservers
- Ερμηνεύουν τις απαντήσεις που παίρνουν από τον nameserver
- Επιστρέφουν τις πληροφορίες που παίρνουν από τον nameserver στο πρόγραμμα που τις ζήτησε

Προγράμματα όπως το ftp και το ssh χρησιμοποιούν resolvers για να πάρουν πληροφορίες από τους nameservers. Τέλος, οι resolvers βασίζονται αποκλειστικά στους nameservers για το αν θα πάρουν τις σωστές πληροφορίες.

1.9 DNS Address resolution

Η αντιστοίχιση ενός domain name με μία διεύθυνση ip είναι μια διαδικασία γνωστή ως Name-Address resolution. Ο resolver που αναλύσαμε στην προηγούμενη παράγραφο εκτελεί αυτή τη λειτουργία με τη βοήθεια των nameserver. Οι nameserver με τη σειρά τους το μόνο που χρειάζονται για να βρουν την απάντηση που θα δώσουν στο resolver είναι το domain name και τη διεύθυνση των root nameserver του domain. Η πληροφορία αυτή είναι πολύ εύκολο να βρεθεί, λόγω της δενδροειδούς δομής δεδομένων του domain namespace.



Εικόνα 1.8 Address resolution του domain students.cs.unipi.gr

Πριν μιλήσουμε για τους δύο τύπους του address resolution, θα αναφερθούμε στους root nameservers. Οι root nameservers έχουν την πληροφορία πού είναι οι εξουσιοδοτημένοι nameservers για κάθε ένα από τα top-level domains ή για κάθε μία από τις top-level ζώνες, για να είμαστε πιο ακριβείς. Όταν ένας resolver θέλει πληροφορία για ένα domain name, ο root nameserver μας δίνει το όνομα και τη διεύθυνση των nameserver που έχουν εξουσιοδοτηθεί για το top-level domain του domain που του δώσαμε. Στη συνέχεια, οι top-level nameserver μας δίνουν πληροφορίες για τους second-level nameserver που έχουν εξουσιοδοτηθεί για το second-level domain που αναζητάμε. Αυτοί οι nameserver μπορούν να δώσουν την πληροφορία για το όνομα και τη διεύθυνση του host που δείχνουν ή μπορεί και να μας δώσει έναν third-level nameserver σε περίπτωση που ένα subdomain του domain που ψάχνουμε έχει

εξουσιοδοτηθεί σε άλλον nameserver. Αυτή η διαδικασία θα γίνεται μέχρι να μας επιστραφεί μια διεύθυνση για το domain που ψάχνουμε ή να μας επιστραφεί ότι το domain που ψάχνουμε δεν αντιστοιχεί σε κάποιον host. Οι root nameservers είναι 13 σε ολόκληρο τον κόσμο μέχρι αυτή τη στιγμή και είναι ζωτικής σημασίας για την διαδικασία του dns address resolution.

1.10 Resolution types

Υπάρχουν δύο τύποι resolution, η επαναληπτική και η αναδρομική. Στην αναδρομική διαδικασία το πρόγραμμα παράγει ένα ερώτημα dns και το προωθεί στον resolver και αναμένει απάντηση. Ο resolver με τη σειρά του προωθεί το ερώτημα στον τοπικό dns server. Εάν αυτός γνωρίζει τη διεύθυνση ip για το domain που αναζητούμε, την επιστρέφει στον resolver. Εάν δε την γνωρίζει, τότε προωθεί το ερώτημα στον root nameserver. Ο root nameserver με τη σειρά του προωθεί το ερώτημα στον top-level domain nameserver. Εάν αυτός γνωρίζει την αντιστοιχία, τότε στέλνει την απάντηση πίσω στο root nameserver και αυτός με τη σειρά του στον dns server που στάλθηκε αρχικά η ερώτηση. Εάν δεν γνωρίζει, τότε θα πρέπει να έχει πληροφορίες για την διεύθυνση ip του τοπικού dns server του προορισμού. Ο τοπικός dns server με τη σειρά του ξέρει τη διεύθυνση ip του host που φιλοξενεί το domain που αναζητούμε και με τη σειρά του στέλνει πίσω στον top-level domain server την απάντηση ο οποίος με τη σειρά του τη στέλνει στον root server και τέλος αυτός τη στέλνει στον τοπικό dns server όπου αυτός την δίνει στον παραλήπτη.

Η επαναληπτική διαδικασία διαφέρει λίγο από την αναδρομική. Σε αυτό το resolution, ο nameserver δίνει την πιο σωστή απάντηση που ήδη ξέρει σε αυτόν που κάνει το ερώτημα χωρίς να κάνει περαιτέρω ερωτήματα σε άλλους servers. Σε περίπτωση που δεν ξέρει την απάντηση, επιστρέφει σε αυτόν που κάνει το ερώτημα τον μια λίστα με nameservers που έχει καταχωρημένους στα δεδομένα του και από εκεί και πέρα είναι δουλειά του resolver για το τι ερωτήματα θα κάνει στη συνέχεια μέχρι να γίνει το resolution του domain name.

Τέλος, να αναφέρουμε ενδεικτικά ότι η επιλογή του root nameserver (από τους 13 που υπάρχουν) όπου θα κάνουμε τα ερωτήματά μας, γίνεται συνήθως με βάση το χρόνο απάντησης στα ερωτήματα που κάνουμε. Δηλαδή το λογισμικό που χειρίζεται αυτά τα ερωτήματα θα τα στείλει σε όλους τους εξουσιοδοτημένους nameservers για τη ζώνη που ανήκει το domain που ψάχνουμε και με βάση το πόσο γρήγορα θα γυρίσει η απάντηση διαλέγει τον κοντινότερο root nameserver για να του στείλει τα ερωτήματά του.

1.11 Μηχανισμός προσωρινής αποθήκευσης (caching)

Ολόκληρη η διαδικασία του name-address resolution, αν και από την περιγραφή της φαίνεται αρκετά περίπλοκη και χρονοβόρα, στην πραγματικότητα είναι αρκετά γρήγορη. Το κύριο τεχνικό χαρακτηριστικό που την κάνει τόσο γρήγορη είναι η τεχνική caching.

Σε κάθε ερώτημα που κάνει ο nameserver για να γίνει resolve ένα domain σε μια διεύθυνση, αποκτά πρόσβαση σε πληροφορίες που του στέλνουν άλλοι servers σχετικά με το domain namespace. Κάθε φορά που τον παραπέμπουν σε μια λίστα από nameservers, μαθαίνει ότι αυτοί οι nameserver είναι εξουσιοδοτημένοι για μία ή περισσότερες ζώνες και φυσικά μαθαίνει τις διευθύνσεις τους. Στο τέλος του resolution process και αφού έχει βρει τη διεύθυνση του domain που έψαχνε, αποθηκεύει τις πληροφορίες που έχει συγκεντρώσει σχετικά με τους nameservers που παραπέμφθηκε και τις διευθύνσεις του με σκοπό να τις χρησιμοποιήσει σε μελλοντικά ερωτήματα.

Οι nameserver αποθηκεύουν αυτές τις πληροφορίες σε μια δομή προσωρινής μνήμης για να κάνουν τα ερωτήματα πιο γρήγορα. Την επόμενη φορά που ο resolver θα κάνει ένα ερώτημα στον nameserver σχετικά με ένα domain, αν ξέρει την απάντηση από την προσωρινή του μνήμη θα το επιστρέψει κατευθείαν ως απάντηση στον resolver. Εάν δεν ξέρει την διεύθυνση του domain αλλά ξέρει τον nameserver που είναι εξουσιοδοτημένος για αυτό το domain, θα τον ρωτήσει απευθείας και θα επιστρέψει την απάντηση στον resolver.

Για παράδειγμα, ας πούμε ότι θέλουμε να κάνουμε resolve την διεύθυνση του cs.unipi.gr. Κατά τη διάρκεια της διαδικασίας ο domain nameserver κρατάει στην προσωρινή του μνήμη τα ονόματα και τις διευθύνσεις των nameserver του cs.unipi.gr και του unipi.gr και φυσικά την διεύθυνση ip του cs.unipi.gr. Σε περίπτωση που ο resolver κάνει ένα ερώτημα στον DNS για την διεύθυνση students.cs.unipi.gr τότε ο τοπικός nameserver μπορεί να παρακάμψει το ερώτημα που κανονικά θα έκανε στον root nameserver και να κάνει ερώτημα απευθείας στον cs.unipi.gr nameserver τον οποίο είχε αποθηκεύσει στην προσωρινή του μνήμη από προηγούμενο ερώτημα. Σε περίπτωση που είχαμε επισκεφθεί ξανά το students.cs.unipi.gr, ο τοπικός dns θα είχε αποθηκεύσει τη διεύθυνσή του και έτσι θα επέστρεφε στον resolver απευθείας την ip του domain.

Όπως καταλαβαίνουμε, τα δεδομένα της προσωρινής μνήμης δεν μπορούν να παραμείνουν για πάντα στο server μας. Εάν γίνει αυτό, αλλαγές που γίνονται στους εξουσιοδοτημένους nameservers δεν θα γίνουν ποτέ γνωστές σε όλο το δίκτυο. Ο χρόνος τον οποίο αυτά τα δεδομένα υπάρχουν και χρησιμοποιούνται από το server είναι συγκεκριμένος και ορίζεται από τον διαχειριστή της εκάστοτε ζώνης. Μετά από αυτό το χρονικό διάστημα, τα προσωρινά

δεδομένα διαγράφονται και σε κάθε ερώτημα γίνεται η γνωστή διαδικασία του name-address resolution και φυσικά η προσωρινή μνήμη ξαναδημιουργείται.

Ένας ακόμα πολύ σημαντικός λόγος που έχει υλοποιηθεί αυτή τεχνική, εκτός από την ανάγκη να γίνεται πιο γρήγορα το name-address resolution, είναι να αποσυμφορήσουμε τους κεντρικούς nameservers και φυσικά τους root nameserver. Φανταστείτε πόσα ερωτήματα θα έπρεπε να απαντήσουν οι root nameservers κάθε μέρα. Πιθανόν δισεκατομμύρια. Ακόμα και οι top-level domains nameserver θα έπρεπε να απαντούν σε αρκετά εκατομμύρια αιτήματα καθημερινά. Με την τεχνική αυτή μειώνεται σημαντικά ο φόρτος των κεντρικών nameserver και φυσικά και ο φόρτος του δικτύου.

ΚΕΦΑΛΑΙΟ 2. Επιθέσεις κατά του συστήματος DNS

2.1 Εισαγωγή

Το DNS έχει γίνει πλέον ένας από τους πιο κοινούς στόχους επιθέσεων. Είναι ένα από τα πιο παλιά και απαραίτητα πρωτόκολλα του διαδικτύου και όλες οι συσκευές που συνδέονται με το διαδίκτυο το χρησιμοποιούν με αποτέλεσμα να είναι ένας ελκυστικός στόχος για τους επιτιθέμενους. Μια λίστα με παραβιάσεις ασφαλείας που έγιναν με επιθέσεις κατά υποδομών DNS ή που εκμεταλλεύτηκαν κενά ασφαλείας στο πρωτόκολλο θα μπορούσε να γεμίσει αρκετά βιβλία.

Κατά καιρούς έχουν γίνει πολλές μεγάλες επιθέσεις με στόχο το DNS. Το 1996 ο Eugene Kashpureff εκμεταλλεύτηκε μια αδυναμία του πρωτοκόλλου μέσω της τεχνικής cache poisoning και ανακατεύθυνε την κίνηση του ιστότοπου του InterNIC στον δικό του. Τον Ιανουάριο του 2001 όλοι οι ιστότοποι της Microsoft έγιναν απρόσιτοι για περίπου μια ημέρα λόγω επίθεσης στους nameserver της. Τον Ιούνιο του 2008 μια ομάδα Τούρκων ακτιβιστών μέσω της τεχνικής του social engineering έπεισαν τους οργανισμούς ICAAN και IANA να τους δώσουν την εξουσιοδότηση των domain icann.org και iana.org. Το 2010 η εταιρεία Verisign, η οποία διαχειρίζεται τα .com και .net domains, καθώς και τους root nameservers για άλλα top-level domains και country code top-level domains, έγινε στόχος πολλαπλών επιθέσεων με αποτέλεσμα να γίνουν απρόσιτα πολλά domain κατά τη διάρκειά της. Το 2013 μια ομάδα ακτιβιστών με το όνομα anonymous προσπάθησαν μέσω της τεχνικής του dns amplification να πλήξουν τους 13 root nameservers με στόχο να προκαλέσουν ένα internet blackout παγκοσμίως, κάτι που τελικά δεν το κατάφεραν.

Πλέον, λόγω της νευραλγικότητας της υπηρεσίας, οι εταιρείες που διαχειρίζονται το dns έχουν εστιάσει περισσότερο στην ασφάλεια της υπηρεσίας, πλην όμως η φύση του πρωτοκόλλου το κάνει ευπαθές σε ένα μεγάλο εύρος επιθέσεων.

2.2 Γενικές επιθέσεις κατά της υπηρεσίας DNS

Αυτές οι επιθέσεις στοχεύουν συνήθως στις υποδομές του DNS, είτε κάνοντας την υπηρεσία μη διαθέσιμη είτε αλλάζοντας τις απαντήσεις που παρέχει η υπηρεσία.

Network floods

Όπως κάθε άλλος server, έτσι και οι dns server είναι ευάλωτοι σε επιθέσεις μέσω δικτύου. Υπάρχουν πολλοί τρόποι όπου οι επιτιθέμενοι μπορούν να κατευθύνουν ένα πολύ μεγάλο αριθμό κίνησης δικτύου προς ένα dns server, κάνοντας την υπηρεσία μη διαθέσιμη στους υπόλοιπους χρήστες που ζητούν πληροφορίες από αυτόν.

Ευπάθειες λογισμικού

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν ευπάθειες στο λογισμικό των dns server ή ευπάθειες του λειτουργικού συστήματος που τρέχουν και έτσι με διάφορες τεχνικές να προσπελάσουν τα μέτρα ασφαλείας και είτε να δημιουργήσουν δικές τους εγγραφές στην βάση δεδομένων του dns server είτε να κρασάρουν το server και να καταστεί μη διαθέσιμος.

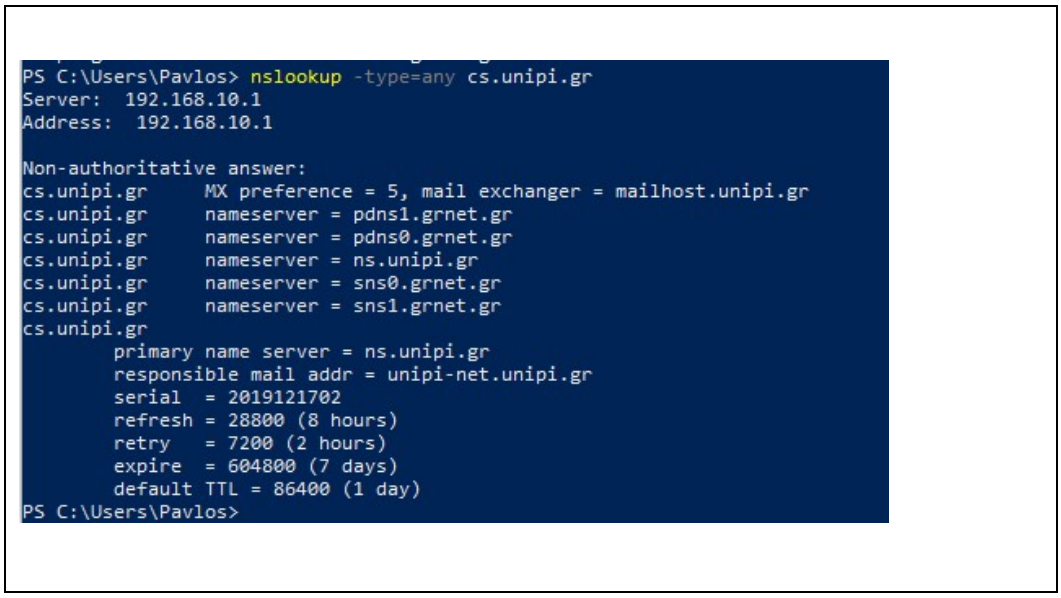
2.3 DDoS Attacks

Υπάρχουν πολλοί τύποι επιθέσεων άρνησης της υπηρεσίας (distributed denial of service) τις οποίες βλέπουμε καθημερινά. Στην περίπτωση του dns αυτές οι επιθέσεις έχουν κυρίως δύο στόχους. Να πάρουν την διαχείριση του dns server ή να τον καταστήσουν μη διαθέσιμο. Οι δύο κύριες μεθοδολογίες τέτοιων επιθέσεων είναι το amplification και το reflection. Αυτές οι επιθέσεις έχουν διαφορετικές τεχνικές και τακτικές, πολλές φορές όμως συνδυάζονται για να παράγουν καλύτερα αποτελέσματα στους επιτιθέμενους.

Amplification

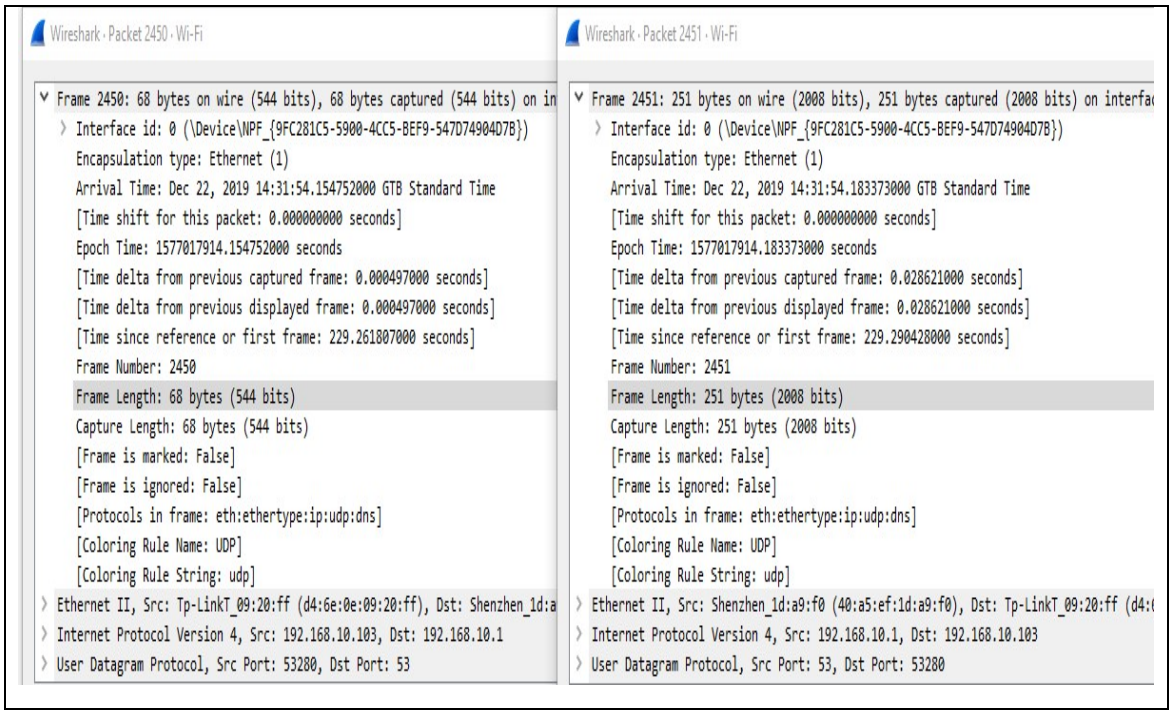
Η επίθεση τύπου amplification είναι μια τεχνική όπου ένα μικρό ερώτημα μπορεί να παράξει μια πολύ μεγάλη απάντηση. Τροφοδοτώντας το server με πολλά επαναλαμβανόμενα τέτοια μικρά ερωτήματα, τον αναγκάζουμε να παράξει μεγάλες απαντήσεις με αποτέλεσμα ακόμα και ένας μικρός υπολογιστής να μπορεί να υπερφορτώσει το dns server που είναι πολύ απασχολημένος να απαντά σε αυτά τα ερωτήματα και έτσι δεν μπορεί να απαντήσει στα

υπόλοιπα ερωτήματα που του κάνουν. Ένα παράδειγμα είναι το εξής. Κάνουμε ένα dns ερώτημα στο unipi.gr/ANY.



Εικόνα 2.1 DNS query για το domain cs.unipi.gr

Με το wireshark βλέπουμε ότι η ερώτηση είναι μήκους 68 byte ενώ η απάντηση έχει μήκος 251 bytes. Είναι δηλαδή περίπου 4 φορές μεγαλύτερη. Υπάρχουν περιπτώσεις που ο dns server μπορεί να επιστρέψει και 100 φορές μεγαλύτερη απάντηση. Σε περίπτωση που ένας επιτιθέμενος δημιουργήσει ένα ρομπότ που κάνει περίπου 10.000 ερωτήσεις το λεπτό με μία σύνδεση 24 Mbps και η απάντηση είναι 251 bytes όπως είδαμε πιο πάνω, τότε ο DNS server θα πρέπει να απαντά με 2,5 Mb το δευτερόλεπτο σε κάθε bot. Φανταστείτε να έχουμε ένα botnet με 100 bots που κάνουν το ίδιο πράγμα. Τότε ο server θα πρέπει να απαντά με 250 Mb το δευτερόλεπτο. Όπως καταλαβαίνετε, ο server θα απαντά μόνο σε αυτά τα request και δεν θα είναι δυνατό να απαντήσει σε νόμιμα ερωτήματα από άλλους clients.



Εικόνα 2.2 Request-response σε ερώτημα dns για το domain unipi.gr

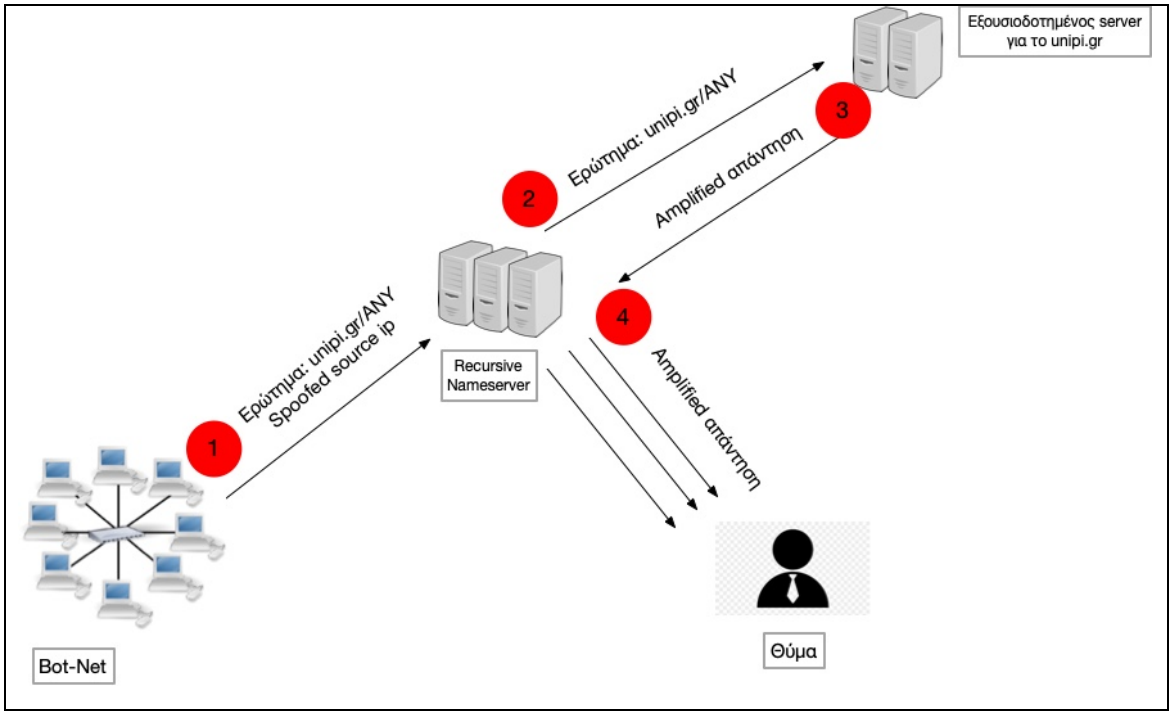
Reflection

Μια επίθεση τύπου reflection στέλνει ερωτήματα τα οποία φαίνονται να έχουν έρθει από το θύμα της επίθεσης. Η απάντηση, που συνήθως είναι amplified και αρκετά μεγάλη ,στέλνεται στο θύμα το οποίο φυσικά ποτέ δεν είχε κάνει το ερώτημα και μπορεί να οδηγήσει σε άρνηση υπηρεσίας εάν αυτές οι απαντήσεις είναι πολλές και δεν μπορεί να ανταπεξέλθει το δίκτυό του. Συγκεκριμένα, ο επιτιθέμενος στέλνει ένα ερώτημα σε έναν αναδρομικό nameserver με αλλαγμένη την διεύθυνση ip. Αυτή η αλλαγμένη ip είναι η ip του θύματος η οποία εμφανίζεται ως source ip. Σε αυτή την περίπτωση, ο nameserver κάνει απλά τη δουλειά του και στέλνει τις απαντήσεις στο θύμα.

Συνδυασμός των δύο επιθέσεων

Ο επιτιθέμενος μπορεί να συνδυάσει τις δύο επιθέσεις αφενός χρησιμοποιώντας την ip του θύματος και αφετέρου στέλνοντας ερωτήματα που έχουν μεγάλες σε μέγεθος απαντήσεις. Με αυτό το τρόπο πραγματοποιεί μια πολύ αποτελεσματική επίθεση με την οποία επιτίθεται σε δύο

θύματα ταυτόχρονα, τον εξουσιοδοτημένο server που παρέχει την επίθεση τύπου amplification και τον επαναληπτικό nameserver που παρέχει την επίθεση τύπου reflection.



Εικόνα 2.3 Συνδυασμός επίθεσης reflection και amplification

Η επίθεση στο παραπάνω σχήμα έχει ως εξής:

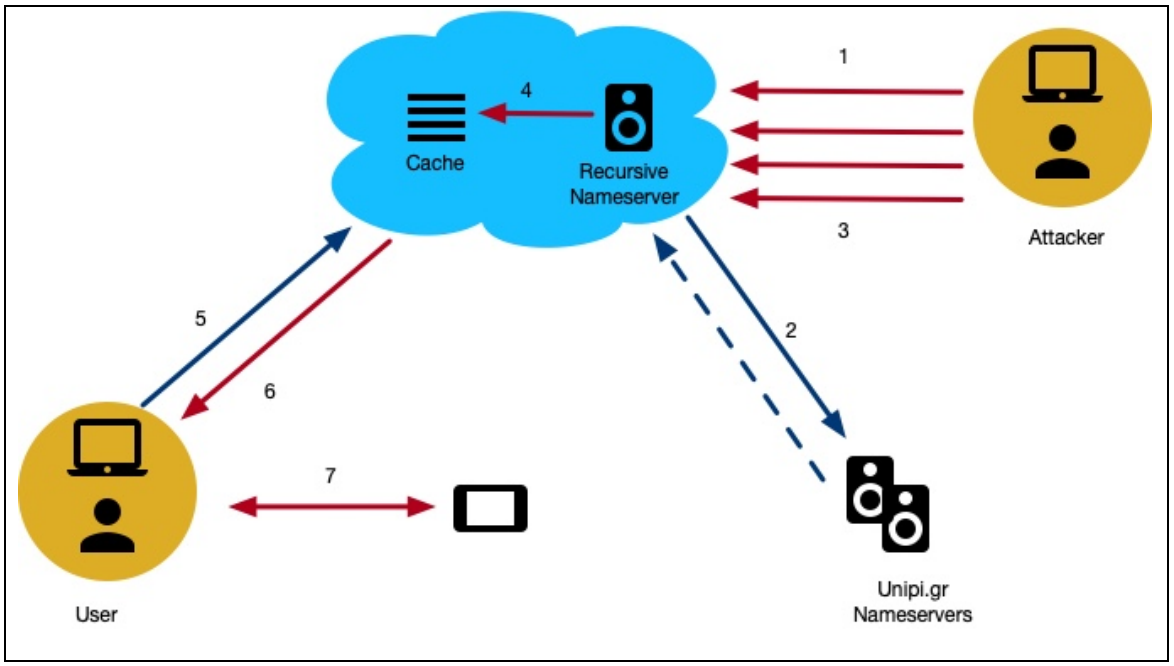
1. Το bot-net που διαχειρίζεται ο επιτιθέμενος στέλνει DNS ερωτήματα με την ip του θύματος στον επαναληπτικό nameserver.
2. Ο επαναληπτικός nameserver ακολουθεί τη διαδικασία που πρέπει και στέλνει το ερώτημα στους άλλους εξουσιοδοτημένους nameservers.
3. Ο επαναληπτικός nameserver λαμβάνει την amplified απάντηση από τους εξουσιοδοτημένους servers.
4. Ο επαναληπτικός nameserver στέλνει την amplified απάντηση στο θύμα, του οποίου η ip φαίνεται ως η source address στο αρχικό ερώτημα.

2.4 Επιθέσεις σε recursive dns servers

Cache poisoning

Αυτή η επίθεση είναι γνωστή ως dns spoofing και έχει ως στόχο να αλλάζει τις απαντήσεις που προέρχονται από την προσωρινή του μνήμη cache, είτε εκμεταλλευόμενοι τις αδυναμίες του πρωτοκόλλου είτε εκμεταλλευόμενοι τις αδυναμίες του λογισμικού. Μια επίθεση τέτοιου τύπου λειτουργεί ως εξής:

1. Ο επιτιθέμενος κάνει ερώτημα σε έναν recursive nameserver για ένα subdomain το οποίο δεν υπάρχει (πχ το mysubdomain.unipi.gr)
2. Ο recursive nameserver δεν έχει την ip του άγνωστου subdomain και έτσι ρωτάει τον nameserver του unipi.gr
3. Πριν προλάβει ο nameserver του unipi.gr να απαντήσει, ο επιτιθέμενος στέλνει πολλές spoofed απαντήσεις οι οποίες φαίνονται να προέρχονται από τον nameserver του unipi.gr . Φυσικά οι spoofed απαντήσεις αντιστοιχίζουν το www.unipi.gr στην ip που ελέγχει ο επιτιθέμενος
4. Ο recursive nameserver δέχεται την απάντηση και καταχωρεί την εγγραφή στην προσωρινή του μνήμη
5. Ένας χρήστης ρωτά τον recursive nameserver για την ip του www.unipi.gr
6. Ο recursive nameserver απαντά στο χρήστη την ip που έχει στην προσωρινή του μνήμη cache
7. Ο χρήστης συνδέεται με τον ιστότοπο που ελέγχεται από τον επιτιθέμενο



Εικόνα 2.4 DNS cache poisoning

NXDOMAIN και Phantom Domain επιθέσεις

Η επίθεση αυτή είναι βασισμένη σε ερωτήματα για domain που είτε δεν υπάρχουν, είτε έχουν φτιαχτεί από τον επιτιθέμενο και αργούν να απαντήσουν ή τελικά δεν απαντούν καθόλου. Στην πρώτη περίπτωση ο επιτιθέμενος στέλνει ερωτήματα στον recursive nameserver για domain που δεν υπάρχουν και γεμίζει η προσωρινή μνήμη cache με αποτελέσματα που δεν έχουν καμία απολύτως πρακτική σημασία με αποτέλεσμα να γίνεται πιο αργός και να καθυστερεί στις απαντήσεις του σε νόμιμα ερωτήματα άλλων nameserver. Στη δεύτερη λόγω ότι τα domain που έχει δημιουργήσει ο επιτιθέμενος καθυστερούν να απαντήσουν ή δεν απαντούν καθόλου ο recursive nameserver καταναλώνει πόρους περιμένοντας τις απαντήσεις που δεν έρχονται ποτέ με αποτέλεσμα να οδηγείτε σε μειωμένη απόδοση.

2.5 Επιθέσεις σε εξουσιοδοτημένους Servers

Reconnaissance

Τα δεδομένα που μας παρέχει ένας dns server είναι by design διαθέσιμα για δημόσια κατανάλωση. Αυτό δίνει την ευκαιρία σε έναν επιτιθέμενο να μάθει περισσότερα σχετικά με το περιβάλλον που τρέχει η υπηρεσία. Η συγκεκριμένη επίθεση δεν πλήττει την διαθεσιμότητα ή την σταθερότητα της υπηρεσίας, είναι όμως μέρος μιας πιο οργανωμένης στρατηγικής επίθεσης. Για παράδειγμα, θα μπορούσαμε να υποθέσουμε ότι αν υπήρχε το subdomain exchange.unipi.gr πιθανόν να έτρεχε το λογισμικό Microsoft exchange και θα μπορούσαμε να οργανώσουμε εξειδικευμένες επιθέσεις σε τυχόν κενά ασφαλείας που έχει εκείνη τη στιγμή.

Μη εξουσιοδοτημένες ενημερώσεις

Οι εξουσιοδοτημένοι nameservers μπορούν να δεχτούν δυναμικές ενημερώσεις, δηλαδή μπορούν να δημιουργήσουν καινούριες dns εγγραφές. Πολλές φορές τη δυνατότητα αυτή μπορούν να την εκμεταλλευτούν επιτιθέμενοι για δημιουργήσουν τις δικές τους εγγραφές στην dns ζώνη.

Επιθέσεις τυχαίων subdomain

Αυτή η επίθεση είναι τύπου DDoS και στόχος της είναι να υπερφορτώσει τον εξουσιοδοτημένο server με αποτέλεσμα να μην μπορεί να απαντήσει σε νόμιμα ερωτήματα που του κάνουν. Συγκριμένα, ο επιτιθέμενος στέλνει πολλά ερωτήματα για subdomain που συνήθως δεν υπάρχουν, καταναλώνοντας έτσι πόρους από το server. Για παράδειγμα, μπορεί να βάλει πολλά bots να κάνουν ερωτήσεις για τυχαία subdomain του domain unipi.gr με αποτέλεσμα ο εξουσιοδοτημένος nameserver του unipi.gr να δέχεται πολλά ερωτήματα τα οποία δεν μπορεί να επεξεργαστεί και να μην απαντά στα υπόλοιπα που δέχεται.

2.6 Άλλες επιθέσεις σε βάρος του DNS

Κακόβουλο λογισμικό

Ο όρος malware προήλθε από τις λέξεις malicious και software. Το κακόβουλο λογισμικό είναι μια κατηγορία λογισμικού σχεδιασμένο με κακόβουλες προθέσεις. Συχνά, το κακόβουλο λογισμικό είναι εγκατεστημένο χωρίς τη συγκατάθεση του χρήστη και λειτουργεί στο παρασκήνιο χωρίς να τραβά την προσοχή.

Αν και το κακόβουλο λογισμικό διανέμεται μέσω web browsers, σαν μέρος διαδικτυακού περιεχομένου, έχει άμεση εξάρτηση από το DNS για την αποτελεσματική διανομή του. Στις

μέρες μας οι επιτιθέμενοι δημιουργούν συστήματα τα οποία καταχωρούν εκατοντάδες οι χιλιάδες domain names και φυσικά με τις κατάλληλες εγγραφές στο dns δείχνουν όλα προς σε web servers οι οποίοι διανέμουν κακόβουλο λογισμικό. Αλλάζοντας συνεχώς αυτά τα ονόματα είναι πολύ δύσκολο να τα παρακολουθήσουμε και να τα μπλοκάρουμε σε επίπεδο DNS.

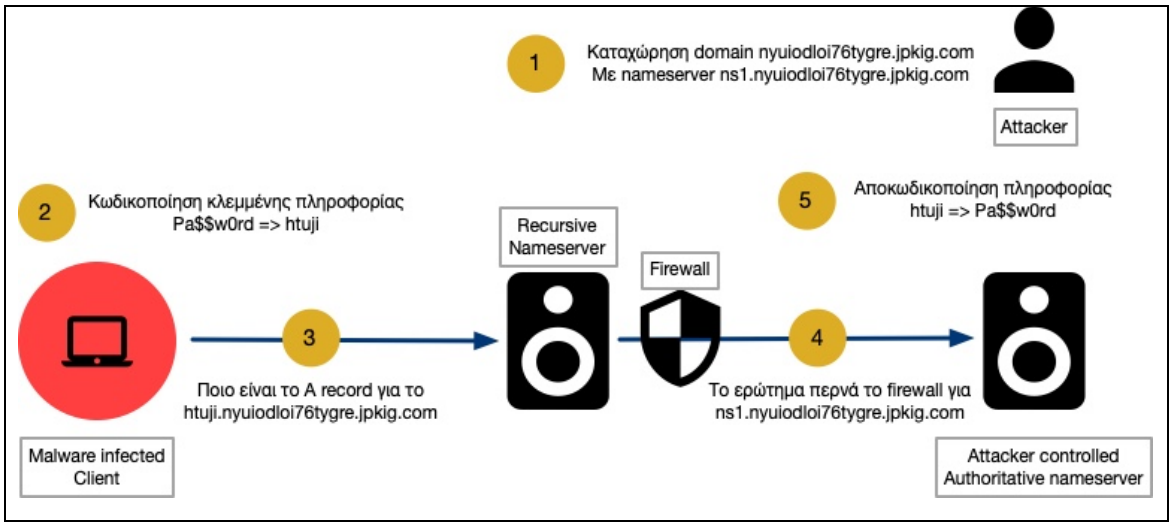
Από τη στιγμή που ένας υπολογιστής έχει μολυνθεί, το κακόβουλο λογισμικό χρησιμοποιεί την υπηρεσία DNS για να βρει μια λίστα από domain names πιθανών “command-and-control servers” μέχρι να βρει έναν διαθέσιμο. Αυτοί οι command-and-control servers είναι servers που ελέγχονται από τους επιτιθέμενους και έχουν τη δυνατότητα να στέλνουν μαζικά εντολές προς τους μολυσμένους υπολογιστές.

Τα κακόβουλα λογισμικά για να υποκλέψουν δεδομένα και να τα μεταφέρουν εκτός δικτύου χρησιμοποιούν μια τεχνική γνωστή ως data exfiltration. Επειδή η τεχνική λειτουργεί μέσω του πρωτοκόλλου DNS, λέγεται και DNS tunneling και θα την αναλύσουμε στην επόμενη παράγραφο.

Data Exfiltration and Tunneling

Οι επιθέσεις DNS tunneling επιτρέπουν στον επιτιθέμενο να διατηρεί ένα κανάλι επικοινωνίας για να μεταφέρει δεδομένα εκτός δικτύου. Η φιλοσοφία του είναι ότι χρησιμοποιεί το DNS για να μπορεί να προσπερνά τα firewall του στόχου. Στην ουσία ο επιτιθέμενος χρησιμοποιεί πρωτόκολλα όπως το shh και το http μέσω του πρωτοκόλλου dns και μεταφέρει δεδομένα χωρίς να τον καταλάβουν τα συστήματα ασφαλείας ή δημιουργεί κίνηση δικτύου πάλι χωρίς να τον καταλάβουν τα συστήματα ασφαλείας.

Ένα κανάλι dns μπορεί να χρησιμοποιηθεί σαν ένα απομακρυσμένο κανάλι για έναν μολυσμένο υπολογιστή. Αυτό επιτρέπει στον επιτιθέμενο να μεταφέρει αρχεία έξω από το δίκτυο, να κατεβάσει καινούριο κώδικα σε υπάρχον κακόβουλο λογισμικό ή απλά να έχει πλήρη έλεγχο στο σύστημα.



Εικόνα 2.5 DNS tunneling

Στο σχήμα 2.5 μπορούμε να δούμε πως λειτουργεί η τεχνική του data exfiltration μέσω του DNS.

1. Ο επιτιθέμενος καταχωρεί ένα domain nyuiodloi76tygrejpkig.com και δημιουργεί τον nameserver ns1.nyuiodloi76tygrejpkig.com
2. Ο μολυσμένος υπολογιστής κωδικοποιεί την κλεμμένη πληροφορία, δηλαδή το αλφαριθμητικό “Pa$$w0rd” στο “htuji”.
3. Ο μολυσμένος υπολογιστής στέλνει ένα ερώτημα dns για το domain με το κωδικοποιημένο αλφαριθμητικό σαν subdomain: htuji. nyuiodloi76tygrejpkig.com.
4. Ο recursive nameserver βρίσκει τον εξουσιοδοτημένο name server ns1.nyuiodloi76tygrejpkig.com και του προωθεί το ερώτημα.
5. Ο επιτιθέμενος αναγνωρίζει το αλφαριθμητικό στο subdomain ως την πληροφορία που έχει κωδικοποιήσει, το “htuji” δηλαδή, και την αποκωδικοποιεί σε “Pa$$w0rd”

Σε αυτό το παράδειγμα δεν είναι απαραίτητο ο μολυσμένος υπολογιστής να λάβει μια απάντηση από τον κακόβουλο server. Στόχος είναι να λάβει την πληροφορία που θέλει και αυτό συμβαίνει. Μπορεί όμως η διαδικασία αυτή να εξελιχθεί με τέτοιο τρόπο έτσι ώστε ο κακόβουλος server να στείλει ένα exploit το οποίο θα τρέξει στον μολυσμένο υπολογιστή.

Η συγκεκριμένη επίθεση είναι πολύ δύσκολο να ανιχνευθεί λόγω των συνεχών αλλαγών στα domain names και της κωδικοποίησης-αποκωδικοποίησης που χρησιμοποιεί ο επιτιθέμενος.

Domain Hijacking και Redirection

Αυτή η επίθεση περιέχει αλλαγές στους dns servers και στον καταχωρητή των ονομάτων με αποτέλεσμα να ανακατευθύνετε η κίνηση από τους νόμιμους διακομιστές σε άλλους προορισμούς.

Συχνά προκαλείτε από διάφορους παράγοντες που έχουν σχέση με την εκμετάλλευση αδυναμιών στο σύστημα του καταχωρητή ονομάτων, αλλά μπορεί να προκληθεί και όταν ο επιτιθέμενος με κάποιο τρόπο έχει πάρει τη διαχείριση των DNS εγγραφών που έχουμε στη κατοχή μας. Από τη στιγμή που ο επιτιθέμενος έχει πάρει τον έλεγχο του domain name, θα προσπαθήσει να το χρησιμοποιήσει για κακόβουλες πράξεις, όπως για παράδειγμα να φτιάξει ένα ψεύτικο σύστημα πληρωμών μέσω κάρτας ή να φτιάξει ένα ακριβές αντίγραφο της πραγματικής ιστοσελίδας με σκοπό να κλέψει πληροφορίες.

ΚΕΦΑΛΑΙΟ 3. DNS Over HTTPS

3.1 Ασφάλεια και ιδιωτικότητα

Τα ερωτήματα του domain name system (DNS) είναι βασικές λειτουργίες των σύγχρονων δικτύων υπολογιστών. Λόγω ότι αυτά τα ερωτήματα στέλνονται σε μη κρυπτογραφημένη μορφή, είναι εύκολο να συγκεντρωθούν από τρίτους με αποτέλεσμα ποιος στέλνει το ερώτημα και ποιο domain επισκέπτεται να είναι δημόσια πληροφορία η οποία συχνά χρησιμοποιείται από εταιρείες για να χτίσουν προφίλ χρηστών που χρησιμοποιούνται σε στοχευμένες διαφημίσεις και μάρκετινγκ. Είναι φανερό λοιπόν ότι υπάρχει έλλειμα ασφάλειας της πληροφορίας που διακινείται και ιδιωτικότητας των ενεργειών του χρήστη.

Ιδιωτικότητα σημαίνει να μην μπορεί να δει κάποιος τρίτος ένα ερώτημα dns κατά τη διαβίβασή του στον dns server, δηλαδή να ελαχιστοποιήσουμε τη δυνατότητα για επιθέσεις του τύπου “man in the middle”. Ένας απλός μηχανισμός για να το κάνουμε αυτό θα ήταν να υλοποιήσουμε μία σύνδεση από σημείο σε σημείο (point-to-point) από τον πελάτη στον εξυπηρετητή dns η οποία φυσικά λόγω της φύσης του διαδικτύου να έχει μια μορφή κωδικοποίησης.

Η ασφάλεια από την άλλη είναι συνυφασμένη με τρία διαφορετικά στοιχεία, κάθε ένα από τα οποία πρέπει να υπάρχει μη εξαρτώμενο από τα υπόλοιπα:

- Η ιδιωτικότητα που αναλύσαμε στην προηγούμενη παράγραφο.
- Η αυθεντικοποίηση με την οποία ο χρήστης ξέρει σε μεγάλο βαθμό ότι επικοινωνεί με τον αναμενόμενο εξυπηρετητή.
- Η ακεραιότητα των δεδομένων με την οποία ο χρήστης ξέρει σε μεγάλο βαθμό ότι τα δεδομένα που στάλθηκαν και ελήφθησαν δεν μπορούν να αλλαχθούν χωρίς να γίνει αντιληπτή αυτή η ενέργεια.

Η ανάγκη για ασφάλεια και ιδιωτικότητα μας έστρεψε προς ήδη δοκιμασμένες λύσεις όπως το πρωτόκολλο https και το 2018 προτάθηκε για πρώτη φορά το πρωτόκολλο DNS over HTTPS μέσω της δημοσίευσης RFC 8484 από τον οργανισμό IETF.

3.2 Λειτουργία πρωτοκόλλου

Σε αυτή την παράγραφο θα γίνει μια σύντομη περιγραφή της λειτουργίας του πρωτοκόλλου. Συγκεκριμένα το πρωτόκολλο DNS over https χρησιμοποιείται για να στείλουμε DNS ερωτήματα και να λάβουμε DNS απαντήσεις μέσω του πρωτοκόλλου HTTP χρησιμοποιώντας https URIs και φυσικά, ασφάλεια TLS για ιδιωτικότητα και ακεραιότητα των δεδομένων που ανταλλάσσονται. Κάθε ζευγάρι ερωτήματος-απάντησης αντιστοιχίζεται σε μία http ανταλλαγή δεδομένων.

1. **Απαιτήσεις πρωτοκόλλου**

   Οι απαιτήσεις του πρωτοκόλλου είναι οι εξής:
   - Το πρωτόκολλο πρέπει να χρησιμοποιεί κανονική σημασιολογία του πρωτοκόλλου http
   - Τα ερωτήματα και οι απαντήσεις πρέπει να είναι αρκετά ευέλικτα έτσι ώστε να αποτυπώνουν πιστά κάθε ερώτημα DNS που θα είχε σταλεί μέσω του πρωτοκόλλου DNS over UDP.
   -Το πρωτόκολλο πρέπει να επιτρέπει την προσθήκη νέων μορφών ερωτήσεων και απαντήσεων DNS.
   - Το πρωτόκολλο πρέπει να διασφαλίζει τη διαλειτουργικότητα καθορίζοντας μια ενιαία μορφή ερωτημάτων και απαντήσεων που είναι υποχρεωτικό να εφαρμοστούν και θα πρέπει να υποστηρίζει μελλοντικές τροποποιήσεις στο πρωτόκολλο DNS.

   1.1. **Μη- απαιτήσεις πρωτοκόλλου**

   -Υποστήριξη του DNS64 για συγκεκριμένα δίκτυα.
   - Υποστήριξη άλλων συμπερασμάτων από plaintext dns ερωτήματα για συγκεκριμένα

δίκτυα.

- Υποστήριξη μη ασφαλούς HTTP

2. Επιλογή DNS API Server

Πριν χρησιμοποιηθεί ένας DNS API Server για DNS resolution, ο πελάτης πρέπει να είναι σίγουρος ότι χρησιμοποιείται ένας έμπιστος DNS API Server στον οποίο θα στέλνονται τα ερωτήματα.

Ο πελάτης δεν πρέπει να χρησιμοποιεί μη έμπιστους DNS API Server τους οποίους είτε τους βρήκε μόνος του, είτε του προτάθηκαν από τρίτους.

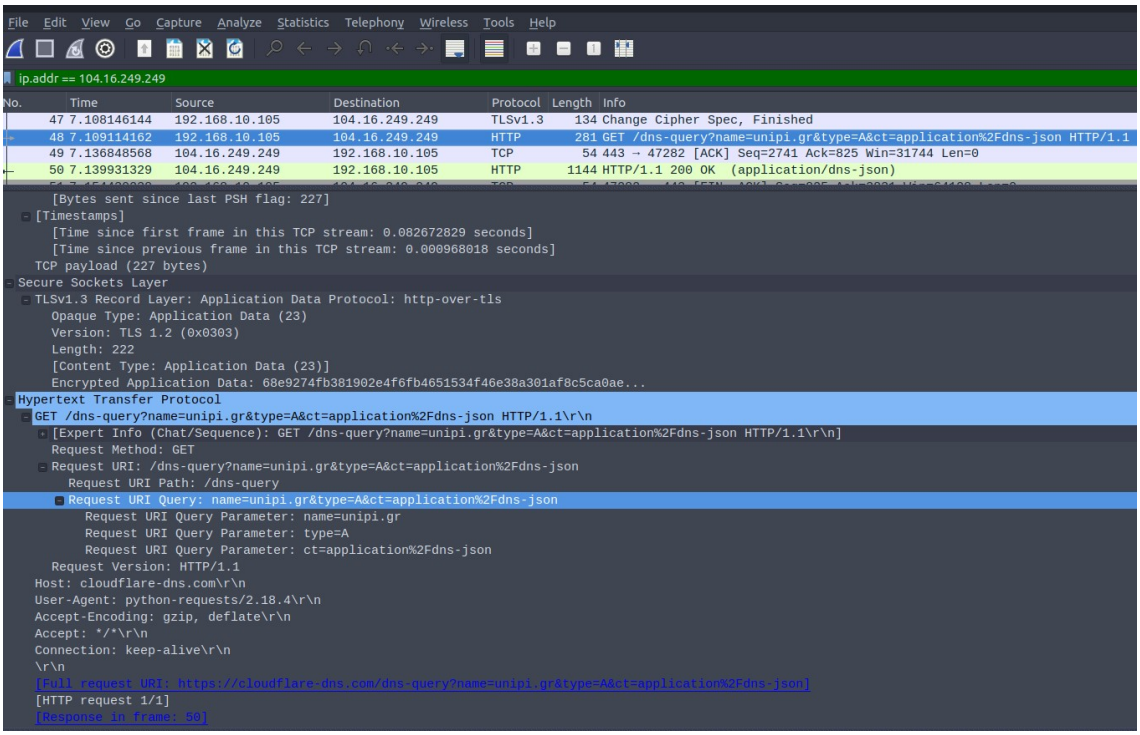
3. Η ανταλλαγή δεδομένων μέσω του πρωτοκόλλου HTTP

3.1. **Το HTTP αίτημα**

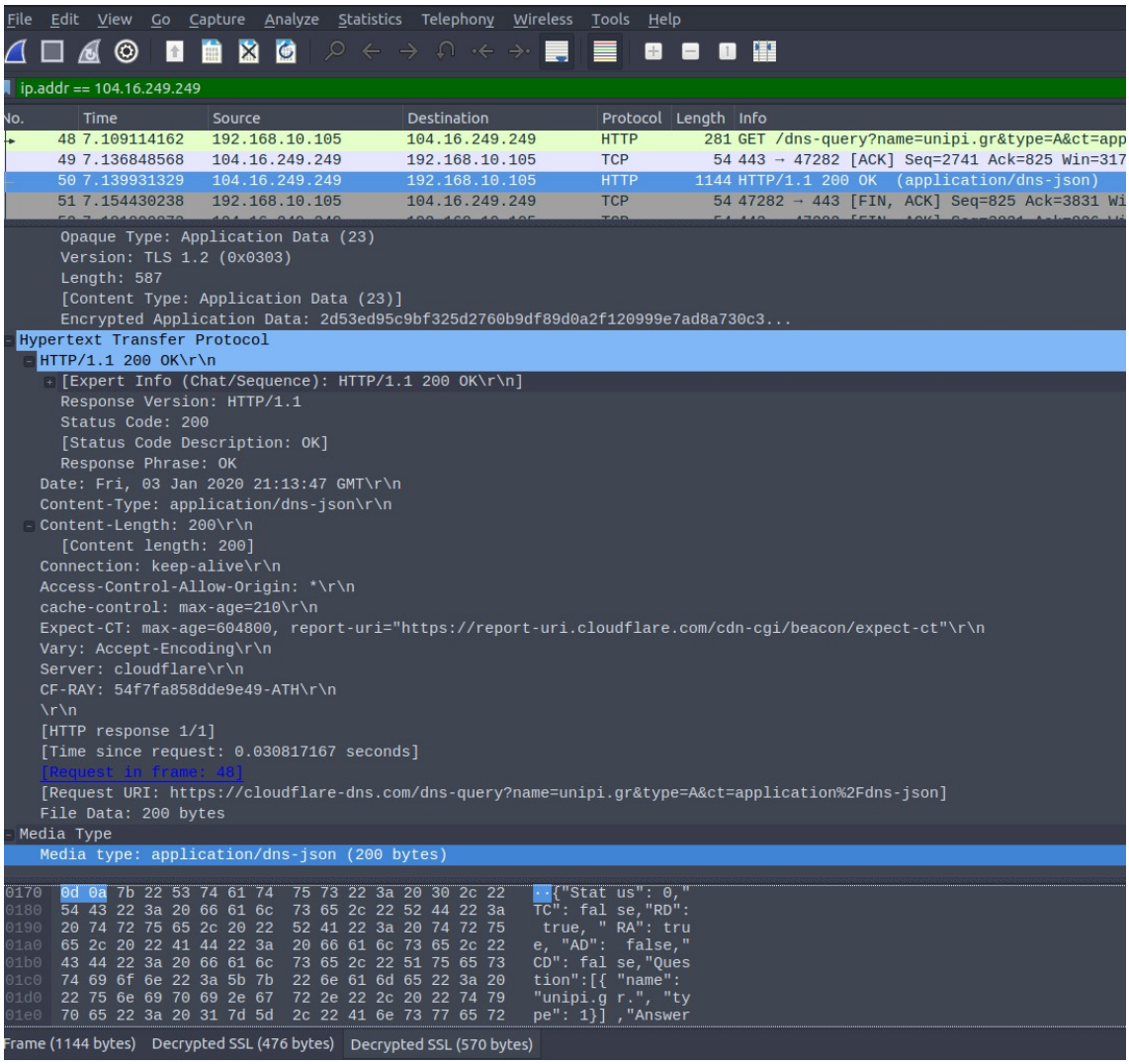
Ο DNS API client κωδικοποιεί ένα ερώτημα DNS σε μία http αίτηση χρησιμοποιώντας είτε την get είτε την post μέθοδο και φυσικά τις υπόλοιπες απαιτήσεις που περιγράψαμε στην προηγούμενη παράγραφο. Ο DNS API server ορίζει το URI που χρησιμοποιείται από την αίτηση μέσω του προτύπου του URI.
Το πρότυπο URI του RFC8484 έχει καθοριστεί χωρίς καμία μεταβλητή όταν η μέθοδος είναι POST, ενώ στη μέθοδο GET έχει καθοριστεί μια μεταβλητή DNS η οποία είναι μέρος του αιτήματος DNS κωδικοποιημένη σύμφωνα με την κωδικοποίηση base64.
Οι DNS API servers πρέπει να υλοποιούν και την POST και την GET μέθοδο.
Όταν χρησιμοποιούμε την μέθοδο POST το ερώτημα DNS περιέχεται ως το body του μηνύματος και ο Content-Type request header υποδηλώνει τον τύπο του μέσου του μηνύματος. Οι αιτήσεις POST είναι μικρότερες από τις ίδιες της μεθόδου GET.
Ο DNS API client πρέπει να περιέχει έναν HTTP "Accept" request header για να υποδηλώνει τι τύπο περιεχομένου μπορεί να καταλάβει στην απάντηση. Ανεξάρτητα από την τιμή του Accept request header , ο πελάτης πρέπει να είναι προετοιμασμένος να επεξεργαστεί “application / dns-message" απαντήσεις αλλά και οποιοδήποτε άλλο τύπο λάβει.
Για να μεγιστοποιήσει τις δυνατότητες για προσωρινή μνήμη, οι DNS API client που χρησιμοποιούν μορφές μέσων οι οποίες περιέχουν DNS ID, όπως το application/dns μήνυμα, πρέπει να χρησιμοποιούν DNS ID αρχίζοντας από το μηδέν. Στη συνέχεια, το πρωτόκολλο http συσχετίζει το αίτημα και την απάντηση, εξαλείφοντας την ανάγκη για αναγνώριση σε μηνύματα τύπου application/dns-message. Η χρήση διαφορετικού DNS IS μπορεί να προκαλέσει το φαινόμενο ίδια ερωτήματα DNS να αποθηκεύονται ως ξεχωριστά στην προσωρινή μνήμη.

3.2. **Η HTTP απάντηση**

Μία HTTP απάντηση με κωδικό 2xx υποδηλώνει μια έγκυρη dns απόκριση στο ερώτημα που έγινε από την HTTP ερώτηση. Μια έγκυρη απάντηση περιέχει τις πετυχημένες αλλά και τις αποτυχημένες απαντήσεις. Για παράδειγμα, μια αποτυχημένη απάντηση DNS για NXDOMAIN θα είναι το μήνυμα σε μια πετυχημένη http απάντηση έστω και αν υπήρξε αποτυχία στο επίπεδο του DNS. Απαντήσεις με αποτυχημένους HTTP κωδικούς κατάστασης δεν περιέχουν απαντήσεις DNS. Κάποιες από τις αποτυχημένες HTTP απαντήσεις μπορεί να σημαίνει ότι ο πελάτης πρέπει να κάνει καινούριο αίτημα για να ικανοποιήσουν την αρχική ερώτηση. Διαφορετικές μορφές απαντήσεων θα παρέχουν περισσότερες ή λιγότερες πληροφορίες από μια DNS απάντηση. Για παράδειγμα, ένας τύπος απάντησης μπορεί να περιέχει πληροφορία από τα bytes της επικεφαλίδας του DNS ενώ μια άλλη μπορεί να μην την περιέχει. Η ποσότητα και ο τύπος της πληροφορίας που δίνει μία μορφή μέσων εξαρτάται αποκλειστικά από την μορφή και δεν ορίζεται σε αυτό το πρωτόκολλο.
Η απάντηση για το "application/dns-message" μπορεί να έχει μία ή περισσότερες EDNS επιλογές όπως ορίζεται στο RFC6891, ανάλογα με τον ορισμό της επέκτασης των επεκτάσεων που δίνονται στο αίτημα DNS.
Κάθε ζευγάρι DNS αίτημα-απάντηση αντιστοιχίζεται σε μία HTTP συναλλαγή. Οι απαντήσεις μπορούν να επεξεργάζονται και να μεταφέρονται σε οποιαδήποτε σειρά χρησιμοποιώντας την multi-streaming λειτουργικότητα του HTTP πρωτοκόλλου.
Ένας DNS API server πρέπει να είναι σε θέση να επεξεργάζεται αιτήματα τύπου application/dns-message. Επίσης, ένας DNS API server πρέπει να απαντά με τον HTTP κωδικό κατάστασης 415 όταν λαμβάνει μία μορφή μέσου που είναι αδύνατο να επεξεργαστεί.



Εικόνα 3.1 Αποκρυπτογραφημένο HTTP αίτημα σε DNS API server

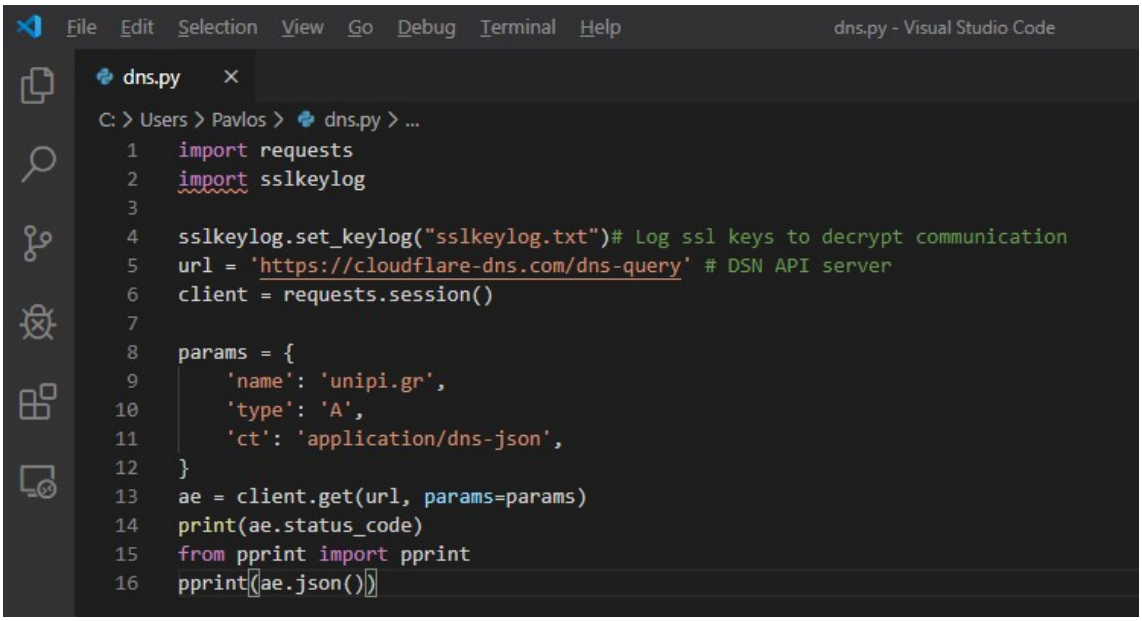


Εικόνα 3.2 Αποκρυπτογραφημένη HTTP απάντηση του DNS API server

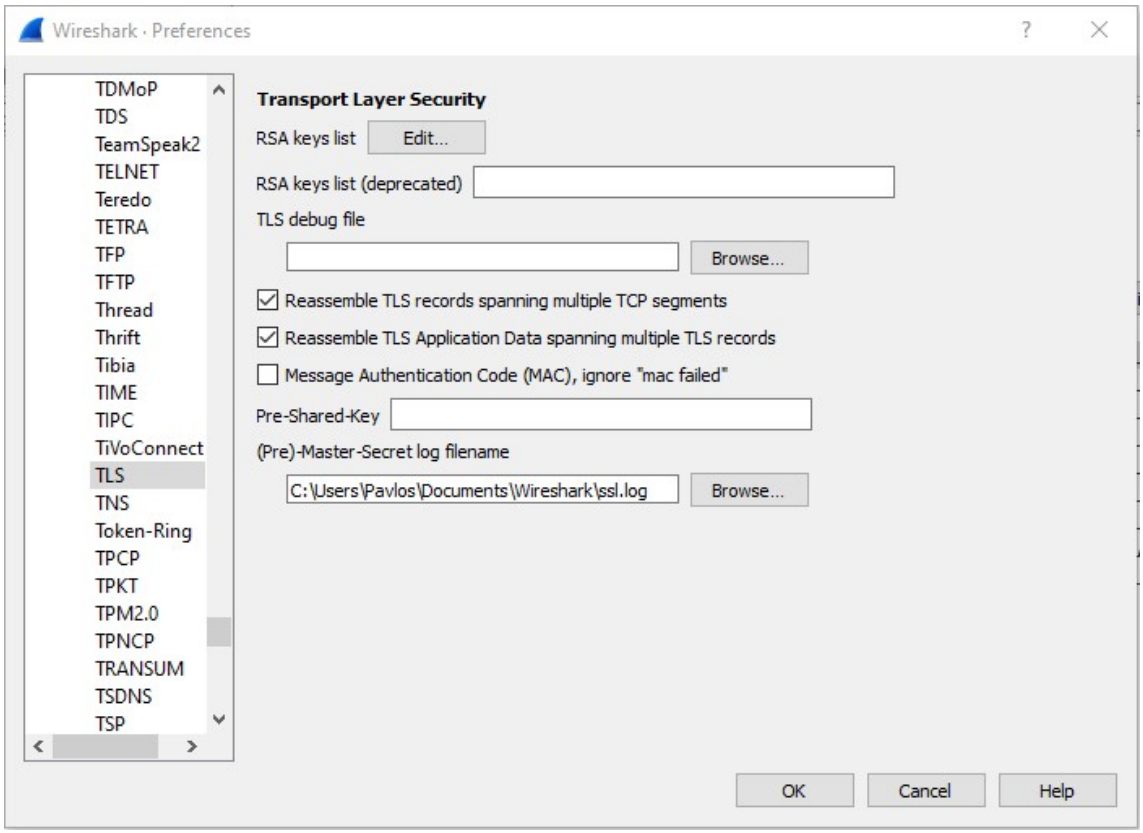
Φτιάχνοντας ένα μικρό πρόγραμμα στην γλώσσα προγραμματισμού python μπορούμε να κάνουμε ένα αίτημα σε έναν DNS API server και να δούμε την απάντηση που μας δίνει. Για να το κάνουμε αυτό, θα αποκρυπτογραφήσουμε την επικοινωνία μεταξύ client και server. Στην αρχή θα αποθηκεύσουμε το κλειδί που ανταλλάσσουν και με τη βοήθεια του wireshark θα καταγράψουμε τα πακέτα που στέλνονται και λαμβάνονται αποκρυπτογραφώντας παράλληλα.

Στην εικόνα 3.1 βλέπουμε το GET request του client προς τον DNS API server και τις παραμέτρους που περνάμε στο uri (name=unipi.gr, type=A, ct=application/dns-json)

όπου name είναι το domain που ψάχνουμε και type είναι ο τύπος της εγγραφής που θέλουμε να μας απαντήσει ο server.
Στην εικόνα 3.2 βλέπουμε την απάντηση του server η οποία είναι 200 bytes και μας δίνει πληροφορίες για το domain που αιτηθήκαμε.



Εικόνα 3.2 Κώδικας σε python αιτήματος πληροφοριών για το domain unipi.gr σε DNS API server



Εικόνα 3.3 Ρύθμιση wireshark για αποκρυπτ/φηση της συνομιλίας client-DNS API server

4. Ενσωμάτωση με το πρωτόκολλο HTTP

4.1. Αλληλεπίδραση με την προσωρινή μνήμη

Μία DNS over HTTPS συναλλαγή μπορεί να περάσει μέσα από μια ιεραρχία προσωρινής μνήμης που περιέχει και HTTP και DNS προσωρινή μνήμη. Αυτά τα αρχεία μπορεί να υπάρχουν μεταξύ του DNS API server και του client ή μόνο στον DNS API client. Η προσωρινή μνήμη του πρωτοκόλλου HTTP είναι γενική σύμφωνα με το σχεδιασμό της και όπως είναι λογικό, δεν καταλαβαίνει το πρωτόκολλο που εξετάζουμε. Ακόμα και αν ο DNS API client έχει τροποποιήσει το σχεδιασμό της προσωρινής του μνήμης έτσι ώστε να καταλαβαίνει τη σημασιολογία του DNS over HTTPS, δεν είναι σίγουρο ότι οι υπόλοιπες τεχνολογίες που παίρνουν μέρος στη συναλλαγή (inline proxies, server-side getaways, content delivery networks) θα το υιοθετήσουν και αυτές.

Ως αποτέλεσμα των παραπάνω, οι DNS API servers πρέπει να είναι προσεκτικοί με τα

http μεταδεδομένα προσωρινής μνήμης που στέλνουν όταν θέλουν να πάρουν απάντηση από αιτήματα με τη μέθοδο GET. Συγκεκριμένα, οι DNS API servers πρέπει να αναθέτουν ένα ρητό χρονικό διάστημα στο οποίο οι DNS API client θα χρησιμοποιούν καινούρια DNS δεδομένα. Αυτή η ανάγκη οφείλεται στο ότι η προσωρινή μνήμη του HTTP είναι σε θέση να χρησιμοποιεί το δικό της χρονικό διάστημα παραμονής των δεδομένων και έχει ως αποτέλεσμα να αναλάβει στην ουσία πόσο τα δεδομένα του DNS θα παραμένουν εκεί, στην ουσία παίρνοντας τον έλεγχο των δεδομένων από τον DNS API server.
Ο χρόνος στον οποίο θα δίνονται “φρέσκα” δεδομένα σε μια DNS over HTTP απάντηση πρέπει να είναι ο μικρότερος TTL στην ενότητα “απάντηση” της DNS απόκρισης. Για παράδειγμα, εάν μια HTTP απόκριση περιέχει τρία RRsets με TTLs των 30,600 και 300, τότε το χρονικό διάστημα του “HTTP freshness” θα είναι 30 δευτερόλεπτα και δεν θα πρέπει να είναι μεγαλύτερο από το μικρότερο TTL στην ενότητα “απάντηση” της DNS απόκρισης. Αυτή η απαίτηση βοηθά να εξασφαλίζετε ότι κανένα από τα RRsets που περιέχονται στην DNS απόκριση σερβίρονται παλαιωμένα από την προσωρινή μνήμη του HTTP. Εάν η DNS απόκριση δεν περιέχει κάποια εγγραφή, και δεν περιέχει SOA εγγραφή στην ενότητα Authority, τότε το “freshness lifetime” δεν πρέπει να είναι μεγαλύτερο από το μικρότερο πεδίο της SOA εγγραφής.
Οι οδηγίες stale-while-revalidate και stale-if-error του Cache-control είναι κατάλληλες σε μια DNS over HTTPS εφαρμογή εφόσον επιτρέπεται από την πολιτική του διακομιστή. Αυτοί οι μηχανισμοί επιτρέπουν σε έναν πελάτη, με την σύνεση του server, να επαναχρησιμοποιήσει μία εγγραφή προσωρινής μνήμης η οποία έχει λήξει χρονικά. Σε αυτή την περίπτωση, ο πελάτης ή επαναχρησιμοποιεί ολόκληρη την εγγραφή ή δεν την χρησιμοποιεί καθόλου.
Οι DNS API servers πρέπει να λαμβάνουν υπόψιν τους την προσωρινή μνήμη όταν δημιουργούν γενικές αποκρίσεις. Για παράδειγμα, εάν ένας DNS API server προσαρμόσει μια απόκριση που προορίζεται για συγκεκριμένο πελάτη με συγκεκριμένα χαρακτηριστικά, δεν επιτρέπεται να χρησιμοποιήσει ξανά αυτή την απόκριση σε έναν άλλο πελάτη. Αυτό επιτυγχάνεται μέσω μιας σειράς τεχνικών HHTP, όπως το Cache-Control max-age of 0, ή χρησιμοποιώντας την επικεφαλίδα Vary response για τη δημιουργία δευτερεύοντος κλειδιού προσωρινής μνήμης.
Οι DNS API clients πρέπει να λαμβάνουν υπόψιν τους την τιμή της επικεφαλίδας Age της απόκρισης όταν υπολογίζουν το DNS TTL μιας απόκρισης. Για παράδειγμα, εάν ένα RRset ληφθεί με ένα DNS TTL με 600, αλλά η επικεφαλίδα Age δείχνει ότι η

απόκριση έχει εισαχθεί στην προσωρινή μνήμη για 250 δευτερόλεπτα, τότε το ο υπολειπόμενος χρόνος ζωής του RRset είναι 350 δευτερόλεπτα.
Οι DNS API clients μπορούν να ζητούν ένα μη αποθηκευμένο στην προσωρινή μνήμη αντίγραφο της απόκρισης χρησιμοποιώντας την οδηγία “no-cache” στο αίτημά τους.
Να σημειωθεί ότι ορισμένοι μηχανισμοί προσωρινής αποθήκευσης μπορεί να μην λάβουν υπόψιν τους αυτές τις οδηγίες, είτε λόγω των ρυθμίσεών τους είτε λόγω ότι αλληλοεπιδρούν με παραδοσιακούς DNS μηχανισμούς προσωρινής αποθήκευσης οι οποίοι δεν υποστηρίζουν τέτοιους μηχανισμούς.

4.2. HTTP/2

Η έκδοση HTTP/2 του πρωτοκόλλου HTTP είναι η ελάχιστη απαιτούμενη έκδοση για την χρησιμοποίηση στο DNS over HTTPS.
Τα μηνύματα στο κλασικό πρωτόκολλο DNS που βασίζεται στο UDP δεν έχουν μια σειρά και έχουν χαμηλή επιβάρυνση. Μια ανταγωνιστική μεταφορά HTTP χρειάζεται να υποστηρίζει αναδιάταξη, παραλληλισμό, προτεραιότητα και συμπίεση επικεφαλίδων για να πετύχουν παρόμοια απόδοση. Αυτά τα χαρακτηριστικά εισήχθησαν στο HTTP με την εισαγωγή της έκδοσης 2. Παλαιότερες εκδόσεις του HTTP είναι σε θέση να ικανοποιούν τις απαιτήσεις του DNS over HTTPS, αλλά μπορεί να οδηγήσουν σε πολύ κακή απόδοση.

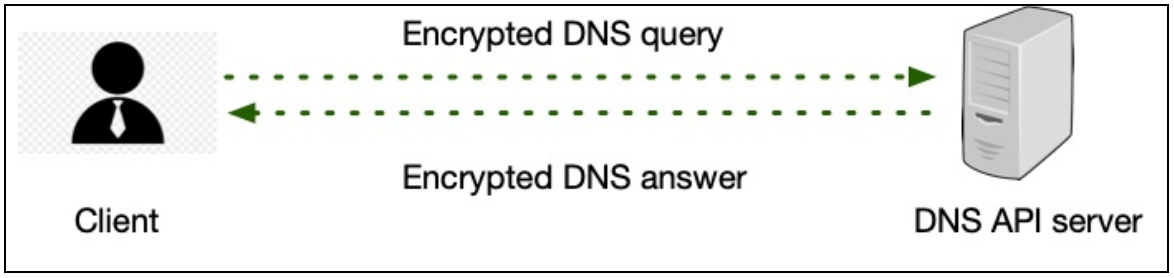
4.3. Server Push

Πριν χρησιμοποιήσουμε τα δεδομένα της DNS over HTTPS απόκρισης για ανάλυση DNS, ο πελάτης πρέπει να βεβαιωθεί ότι η το URI της HTTP αίτησης μπορεί να χρησιμοποιηθεί για το ερώτημα DNS. Για αιτήματα HTTP που ξεκινούν από τον DNS API client αυτό είναι υποχρεωτικό για την επιλογή του URI. Για το HTTP server push πρέπει να ληφθεί επιπλέον μέριμνα για να διασφαλιστεί ότι το εμπλεκόμενο URI είναι αυτό το οποίο ο πελάτης θα είχε κατευθύνει το ερώτημα σε αυτό σε περίπτωση που ο πελάτης είχε ξεκινήσει το αίτημα.

4.4. Διαπραγμάτευση περιεχομένου

Για να μεγιστοποιήσουμε τη διαλειτουργικότητα, οι DNS API clients και οι DNS API servers πρέπει να υποστηρίζουν τον τύπο μέσου "application/dns-message". Άλλοι τύποι μέσων μπορούν να χρησιμοποιηθούν όπως ορίζονται από το HTTP Content Negotiation στο RFC7231. Αυτοί οι τύπου μέσων πρέπει να είναι αρκετά ευέλικτοι για

να μπορούν να εκφράσουν κάθε DNS ερώτημα που κανονικά θα έπρεπε να σταλεί με το DNS over UDP (συμπεριλαμβανομένων ερωτημάτων και αποκρίσεων που χρησιμοποιούν επεκτάσεις DNS, αλλά όχι αυτές που απαιτούν πολλαπλές αποκρίσεις.



Εικόνα 3.4 DNS over HTTPS

3.3 Ευπάθειες πρωτοκόλλου

Το πρωτόκολλο DNS over HTTPS επαφίεται στην ασφάλεια του πρωτοκόλλου HTTP. Αυτό σημαίνει ότι μειώνονται σημαντικά οι amplification επιθέσεις στο κλασικό UDP-based DNS και οι εφαρμογές του πρωτοκόλλου που χρησιμοποιούν HTTP/2 επωφελούνται από την ασφάλεια του TLS που τους παρέχει, από την άλλη όμως κληρονομεί γνωστές ευπάθειες που έχει το πρωτόκολλο HTTP.

Η κρυπτογράφηση σε επίπεδο συνόδου έχει γνωστές αδυναμίες σε σχέση με την ανάλυση της κίνησης οι οποίες μπορεί να είναι ιδιαίτερα έντονες όταν κάνουμε ερωτήματα DNS. Η έκδοση 2 του πρωτοκόλλου HTTP μας δίνει τη δυνατότητα να χρησιμοποιήσουμε συμπίεση και padding στα δεδομένα που ανταλλάσσουμε έτσι ώστε να αυξήσουμε την ασφάλεια από επιθέσεις στο επίπεδο της συνόδου. Ακόμα, οι DNS API servers μπορούν να προσθέσουν padding στις απαντήσεις τους, εφόσον τους ζητηθεί στο DNS ερώτημα.

Η HTTPS σύνδεση μας παρέχει ασφάλεια στη μεταφορά των δεδομένων μεταξύ του DNS API server και του πελάτη, αλλά δεν μας παρέχει την ακεραιότητα των DNS δεδομένων της απάντησης όπως το DNSSEC. Το DNSSEC και το DNS over HTTPS είναι δύο ανεξάρτητα πρωτόκολλα τα οποία μας δίνουν λύσεις σε διαφορετικά προβλήματα. Η χρήση ενός από αυτά δεν μας υπαγορεύει τη χρήση ή τη μη χρήση του άλλου. Είναι στην κρίση του πελάτη αν θέλει να εκτελέσει μια πλήρη επικύρωση των δεδομένων που λαμβάνει με το DNSSEC πρωτόκολλο, ή να εμπιστευθεί τον DNS API server να κάνει ο ίδιος την επικύρωση των δεδομένων μέσω του DNSSEC.

Η αλληλεπίδραση του πρωτοκόλλου με το μηχανισμό προσωρινής μνήμης του HTTP είναι ακόμα μια ευπάθεια για το λόγο ότι μπορεί κάποιος τρίτος να πάρει τον έλεγχο των δεδομένων της προσωρινής μνήμης και να τα παραποιήσει όπως αυτός θέλει. Οι επιπτώσεις στην ασφάλεια είναι ακριβώς ίδιες με άλλα πρωτόκολλα που χρησιμοποιούν το πρωτόκολλο HTTP.

Σε περίπτωση που δεν έχουμε επικύρωση DNSSEC στα δεδομένα DNS που ζητάμε, ο DNS API server μπορεί να μας δώσει μη έγκυρα δεδομένα. Για το λόγο αυτό ο πελάτης δεν πρέπει να χρησιμοποιεί DNS API servers τους οποίους δεν εμπιστεύεται. Αντίθετα, πρέπει να χρησιμοποιεί servers οι οποίοι χρησιμοποιούν ασφαλείς μηχανισμούς. Αυτό δεν εγγυάται την προστασία έναντι μη έγκυρων δεδομένων, αλλά μειώνει αρκετά το ρίσκο.

Ένας πελάτης μπορεί να χρησιμοποιήσει το πρωτόκολλο DNS over HTTPS σαν έναν από τους μηχανισμούς που έχει στη διάθεσή του για να λάβει δεδομένα DNS. Εάν για κάποιο λόγο το πρωτόκολλο HTTP αντιμετωπίσει κάποιο πρόβλημα αφού στείλει ένα ερώτημα DNS, και στη συνέχεια χρησιμοποιήσει αναγκαστικά έναν άλλο μηχανισμό για στείλει το ερώτημά του, μπορεί να αποδυναμωθεί η ιδιωτικότητα και η ακεραιότητα των δεδομένων που λαμβάνονται.

3.4 Μειονεκτήματα και πλεονεκτήματα

Πλεονεκτήματα

- Λόγω της κρυπτογράφησης στο επίπεδο μεταφοράς, το πρωτόκολλο προλαμβάνει επιθέσεις τύπου man in the middle διότι όλα τα ερωτήματα είναι κρυπτογραφημένα.
- Η κρυπτογράφηση μπορεί επίσης να μας πραστατεύσει από επιθέσεις τύπου DNS hijacking, amplification και spoofing
- Μας εγγυάται την εμπιστευτικότητα των DNS ερωτημάτων μας.
- Έχουμε πιο καλό έλεγχο στο τι πληροφορίες μοιραζόμαστε με εταιρείες και κυβερνήσεις σχετικά με τα dns ερωτήματα που κάνουμε.
- Προς το παρών λόγω της centralized φύσης του πρωτοκόλλου, οι χρόνοι απόκρισης των DNS API servers έχουν βελτιωθεί αρκετά.

Όλα αυτά τα πλεονεκτήματα είναι δυνατά λόγω του γεγονότος ότι το domain name resolution δεν απαιτεί ερώτημα στην δημόσια DNS υποδομή για να επιλύσει ένα όνομα χώρου. Αντιθέτως, βασίζεται στην άμεση σύνδεση ανάμεσα στον τελικό χρήστη και τον DNS API server. Αυτό έχει ως αποτέλεσμα να έχουμε καλύτερο έλεγχο στα DNS ερωτήματα που κάνουμε με το πρωτόκολλο να διασφαλίζει ότι μας παρέχει ακριβείς ip διευθύνσεις εξαλείφοντας την ευκαιρία τρίτων να δουν ποιους ιστότοπους επισκεπτόμαστε.

Μειονεκτήματα

- Οι internet service providers κάθε χώρας μπορούν να έχουν ακόμα πρόσβαση και στατιστικά στοιχεία ποιες σελίδες επισκεπτόμαστε απλά διαβάζοντας την destination ip address η οποία είναι μη κρυπτογραφημένη.
- Οι οργανισμοί που χρησιμοποιούν το DNS filtering and monitoring στα συστήματα ασφαλείας τους με σκοπό να μην επιτρέπουν σε χρήστες να επισκέπτονται malware domains ή ιστότοπους μη σχετικούς με την εργασία τους πρέπει να βρουν καινούριους τρόπους να το κάνουν.
- Αποδυναμώνεται η κυβερνοασφάλεια καθώς η συντριπτική πλειοψηφία των λογισμικών ασφαλείας χρησιμοποιούν το DNS για να επιβλέπουν την κίνηση στα δίκτυά τους.
- Συγκεντρώνει την κίνηση DNS σε λίγους DNS API servers, κάτι που έχει αρνητικό αντίκτυπο στην ιδιωτικότητα των χρηστών.
- "Κουβαλάει" τα κενά ασφαλείας του πρωτοκόλλου HTTPS, εφόσον λειτουργεί πάνω σε αυτό.

ΚΕΦΑΛΑΙΟ 4. Επίβλεψη κίνησης DNS over HTTPS

4.1 Εισαγωγή στην επίβλεψη των DNS ερωτημάτων

Η καταγραφή των DNS ερωτημάτων και η ανάλυση των δεδομένων που καταγράφουμε μας βοηθά να καταλάβουμε την δραστηριότητα ενός δικτύου. Η επίβλεψη των ερωτημάτων του DNS έχει σημαντικά πλεονεκτήματα σε σχέση με άλλες μεθόδους επίβλεψης ενός δικτύου. Είναι σχετικά απλό να εφαρμοστεί και απαιτεί ελάχιστες αλλαγές στις ρυθμίσεις στις περισσότερες περιπτώσεις και τα ερωτήματα είναι μη κρυπτογραφημένα τις περισσότερες φορές κάνοντας την διαδικασία της ανάλυσης λιγότερη πολύπλοκη σε σύγκριση με κρυπτογραφημένα πρωτόκολλα.

Λόγω της χρησιμότητας αυτών των δεδομένων, έχουν αναπτυχθεί λογισμικά επίβλεψης των DNS ερωτημάτων τα οποία περιέχουν λειτουργίες επίβλεψης ονομάτων χώρου και σύγκρισή τους με μια λίστα ονομάτων τα οποία θεωρούνται επικίνδυνα ή απλά η πολιτική του οργανισμού απαγορεύει στους υπαλλήλους της να τα επισκέπτονται. Έτσι, εάν πραγματοποιηθεί ένα ερώτημα DNS για domain που περιέχεται στη λίστα, τότε το λογισμικό θα παράξει μια ειδοποίηση ή θα μας γνωστοποιήσει το γεγονός.

Μια βασική ανησυχία για τις λίστες αυτές είναι η αξιολόγηση της αποτελεσματικότητας των πληροφοριών της απειλής από κάθε λογισμικό. Μπορούμε να τις εμπιστευθούμε ότι μπλοκάρουν τις πιο πολλές απειλές κακόβουλου λογισμικού ή τα ποσοστά ανίχνευσης είναι πολύ χαμηλά για να είναι αξιόπιστα; Τέτοιες λίστες κυκλοφορούν ελεύθερες στο διαδίκτυο και ενσωματώνονται σε λογισμικά ασφαλείας, πλην όμως υπάρχουν και λίστες οι οποίες συντηρούνται από εταιρείες που παρέχουν υπηρεσίες ασφάλειας στο διαδίκτυο και δεν δημοσιοποιούν τα περιεχόμενά τους.

4.2 Η συμβολή της επίβλεψης των DNS ερωτημάτων στην ανίχνευση εισβολών

Τα ερωτήματα DNS είναι θεμελιώδους σημασία για την λειτουργία του διαδικτύου. Οι χρήστες χρησιμοποιούν DNS ερωτήματα για να μεταφράσουν ονόματα σε ip διευθύνσεις και τελικά να συνδεθούν στο διακομιστή που έχει αυτή τη μοναδική διεύθυνση ip και γενικότερα χρησιμοποιούνται παγκοσμίως στο διαδίκτυο για τη σύνδεση χρηστών σε έναν διακομιστή.

Οι επιτιθέμενοι έχουν το κίνητρο να χρησιμοποιούν το πρωτόκολλο DNS λόγω της ευελιξίας που προσφέρει. Εάν ένας επιτιθέμενος καθορίσει με μη αυτόματο τρόπο μια διεύθυνση ip σε μια επίθεση, η επίθεση θα είναι αποτελεσματική μόνο όσο η συγκεκριμένη ip είναι προσβάσιμη από το θύμα. Έτσι χρησιμοποιώντας DNS-based επιθέσεις αποκτούν ευελιξία και μπορούν να μετακινούν διακομιστές μεταξύ διαφορετικών ip διευθύνσεων αναγκάζοντας την προσέγγιση του μπλοκαρίσματος των ip διευθύνσεων να μην λειτουργεί ουσιαστικά.

Λόγω της αξίας των δεδομένων των DNS ερωτημάτων, η καταγραφή των ερωτημάτων DNS σε ένα δίκτυο θεωρείτε καλή πρακτική για την ασφάλεια του δικτύου. Όταν η καταγραφή έχει υλοποιηθεί σωστά, τα αρχεία καταγραφής επιτρέπουν σε ειδικούς ερευνητές ψηφιακών μέσων να εξετάσουν ποιες συσκευές δικτύου έκαναν ερωτήματα DNS, για ποιο domain και τι ώρα έγιναν αυτά με αποτέλεσμα αυτά τα αρχεία καταγραφής να μπορούν χρησιμοποιηθούν για την ανίχνευση του σημείου εισόδου και την εξάπλωση μιας επίθεσης στο δίκτυο.

Λόγω της χρησιμότητας αυτών των ερωτημάτων, όπως εξηγήσαμε και στην προηγούμενη παράγραφο, τα λογισμικά ασφαλείας έχουν πάει ένα βήμα παρακάτω στην επίβλεψη των DNS ερωτημάτων σε ένα δίκτυο, αναπτύσσοντας λύσεις που επιβλέπουν τα DNS ερωτήματα σε πραγματικό χρόνο και συγκρίνοντάς τα με λίστες κακόβουλων domain που έχουν στην κατοχή τους. Η ανίχνευση μπορεί να λάβει τη μορφή δημιουργίας μιας ειδοποίησης ή γνωστοποίησης ακριβώς όπως εξηγήσαμε στην προηγούμενη ενότητα.

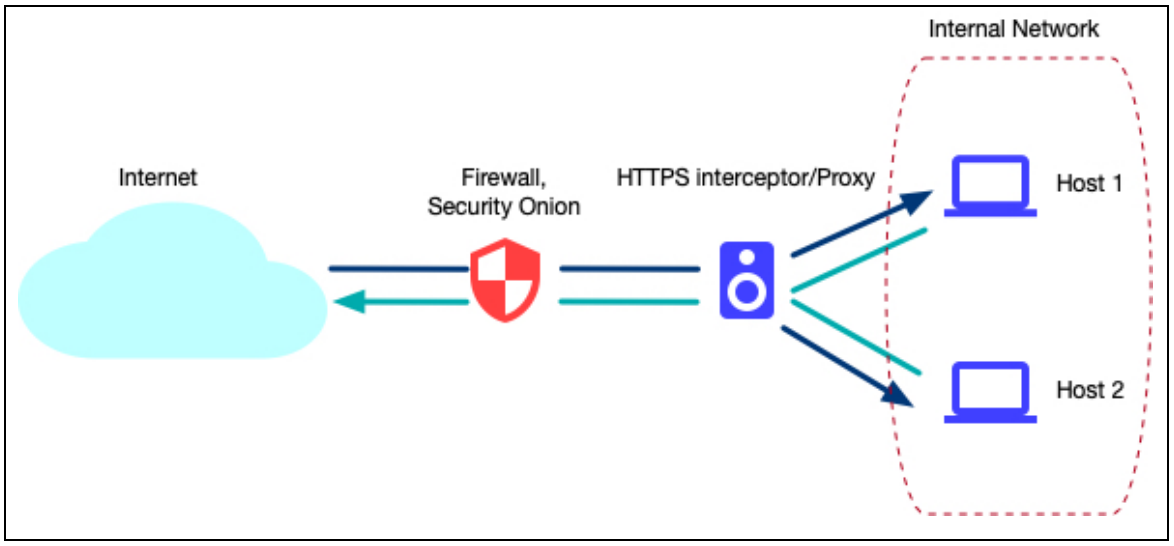
4.3 Δημιουργία εργαστηρίου για δοκιμές

Η παρούσα διατριβή προϋποθέτει να τρέξουμε πολλά τεστ σε ένα περιβάλλον εργαστηρίου με βασική οργάνωση και δικτύωση για να δούμε αρχικά πως το DNS over HTTPS δεν γίνεται αντιληπτό από τα συστήματα ασφαλείας και στη συνέχεια να βρούμε τρόπους να αναγνωρίσουμε και να επιβλέψουμε την κίνηση αυτή έτσι ώστε να κάνουμε πιο ασφαλές το δίκτυό μας.

Το εργαστήριο θα αποτελείται από τα εξής:

- Δύο hosts η οποίοι θα υπάρχουν πίσω από έναν proxy/https interceptor και θα τρέχουν λειτουργικό Kali Linux (θα μπορούσαν να τρέχουν οποιοδήποτε λειτουργικό)
- Έναν HTTPS interceptor/proxy ο οποίος θα έχει δύο διαφορετικούς ρόλους. Θα τρέχει ως proxy για να περνάει η http/https κίνηση του εσωτερικού δικτύου προς το internet και ως https interceptor όπου θα αποκρυπτογραφεί την https κίνηση που παράγει το εσωτερικό δίκτυο προς το internet για να ανιχνεύουμε ερωτήματα DNS over HTTPS.
- Έναν host όπου θα έχει δύο ρόλους, πρώτον να λειτουργεί ως firewall για το δίκτυο και δεύτερον να τρέχει δωρεάν και ανοιχτού κώδικα λογισμικό (η διανομή Linux ονομάζεται Security Onion) για την επίβλεψη των ερωτημάτων dns και της https κίνησης του δικτύου.

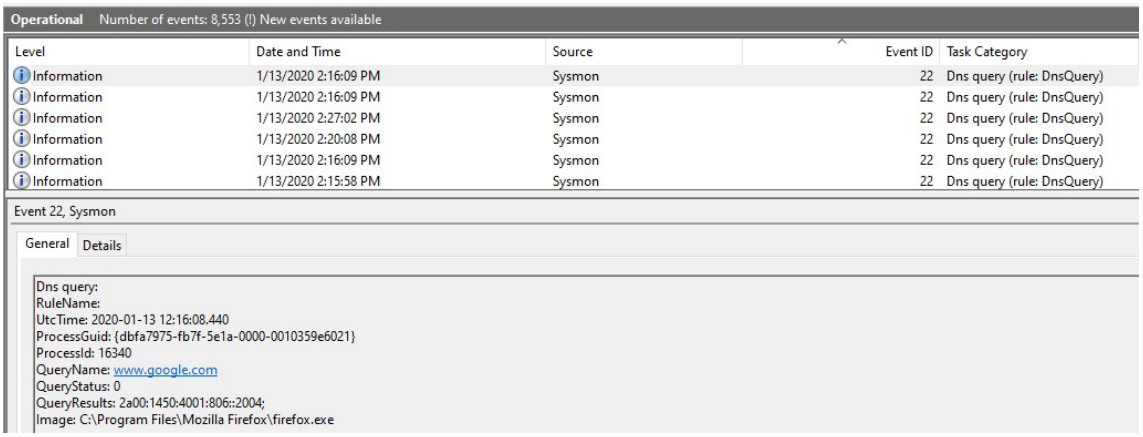
Τα παραπάνω εργαλεία θα χρησιμοποιηθούν για να μπορούμε να επιβλέψουμε την κίνηση του δικτύου μας και να μας βοηθήσουν στο να εξάγουμε τα συμπεράσματά μας.



Εικόνα 4.1 Τοπολογία εργαστηρίου δοκιμών

4.4 Ανίχνευση ερωτημάτων DNS over UDP

Η ανίχνευση των ερωτημάτων DNS που γίνονται μέσω του πρωτοκόλλου UDP είναι πολύ εύκολο να ανιχνευθούν λόγω ότι στέλνονται χωρίς καμία μορφή κρυπτογράφησης. Ένα παράδειγμα επίθεσης που μπορεί να ανιχνευθεί μέσω της επίβλεψης της κίνησης του DNS είναι η κίνηση που δημιουργεί ένα botnet από την command-and-control δραστηριότητά του. Οι command-and-control servers που βρίσκονται στις ip όπου επικοινωνεί το κακόβουλο λογισμικό στέλνουν εντολές στις συσκευές του δικτύου μας με αποτέλεσμα η επίβλεψη των ερωτημάτων dns που πραγματοποιεί να αναγνωρίσει πιθανόν backlisted ip ή domain. Σε περίπτωση που αναγνωριστούν, υπάρχουν κατάλληλες τεχνικές να απαγορεύσουμε αυτά τα ερωτήματα και φυσικά μπορούμε να βρούμε ποιες συσκευές έχουν μολυνθεί στο δίκτυό μας.



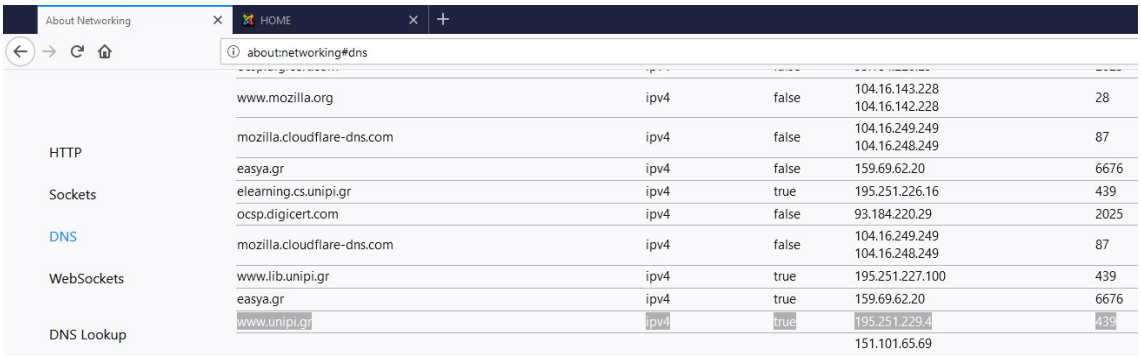
Εικόνα 4.2 Καταγραφή ερωτημάτων DNS μέσω του εργαλείου sysmon

4.5 Μέθοδοι για την ανίχνευση ερωτημάτων DNS over HTTPS

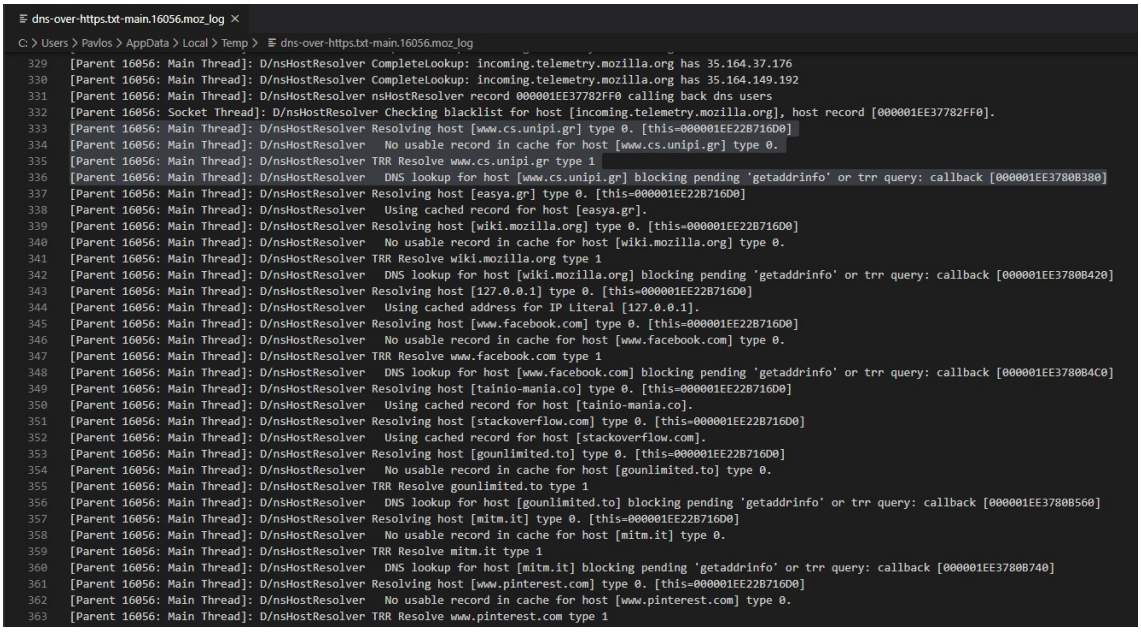
4.5.1 Καταγραφή ερωτημάτων σε επίπεδο εφαρμογής

Σε περίπτωση που μια εφαρμογή μπορεί να τρέξει ερωτήματα DNS μέσω ενός κρυπτογραφημένου καναλιού, η διαμόρφωσή της να αποθηκεύει αυτά τα ερωτήματα σε αρχεία καταγραφής μπορεί να μας δώσει ένα εργαλείο για την ανάλυση και καταγραφή των πληροφοριών αυτών. Οι οργανισμοί που έχουν αυτή τη δυνατότητα αποθηκεύουν τα αρχεία αυτά και τα αναλύουν μέσω ειδικών λογισμικών ασφαλείας (SIEM) ή εργαλείων ανάλυσης αρχείων καταγραφής. Αυτά τα αρχεία επιτρέπουν στον οργανισμό να εξετάζει τη καθημερινή κίνηση του δικτύου της και να βρίσκει ροή πληροφοριών οι οποίες δεν έχουν πληροφορίες DNS που να συνδέονται με αυτές. Δηλαδή μπορούμε να καθορίσουμε ποια εφαρμογή έκανε ένα συγκεκριμένο αίτημα DNS και να ανάλογα με την πολιτική που έχουμε να τη μπλοκάρουμε ως πηγή ασυνήθιστης κίνησης από και προς το δίκτυο μας.

Για παράδειγμα, μπορούμε να αποθηκεύσουμε αρχεία καταγραφής των DNS over HTTPS ερωτημάτων στον Mozilla Firefox. Αρκεί να ενεργοποιήσουμε την λειτουργία καταγραφής στην καρτέλα about:networking του Firefox και όλα τα DNS ερωτήματα που γίνονται θα καταγράφονται σε αρχεία της επιλογής μας.



Εικόνα 4.3 Καρτέλα ρυθμίσεων καταγραφής DNS ερωτημάτων του Mozilla Firefox



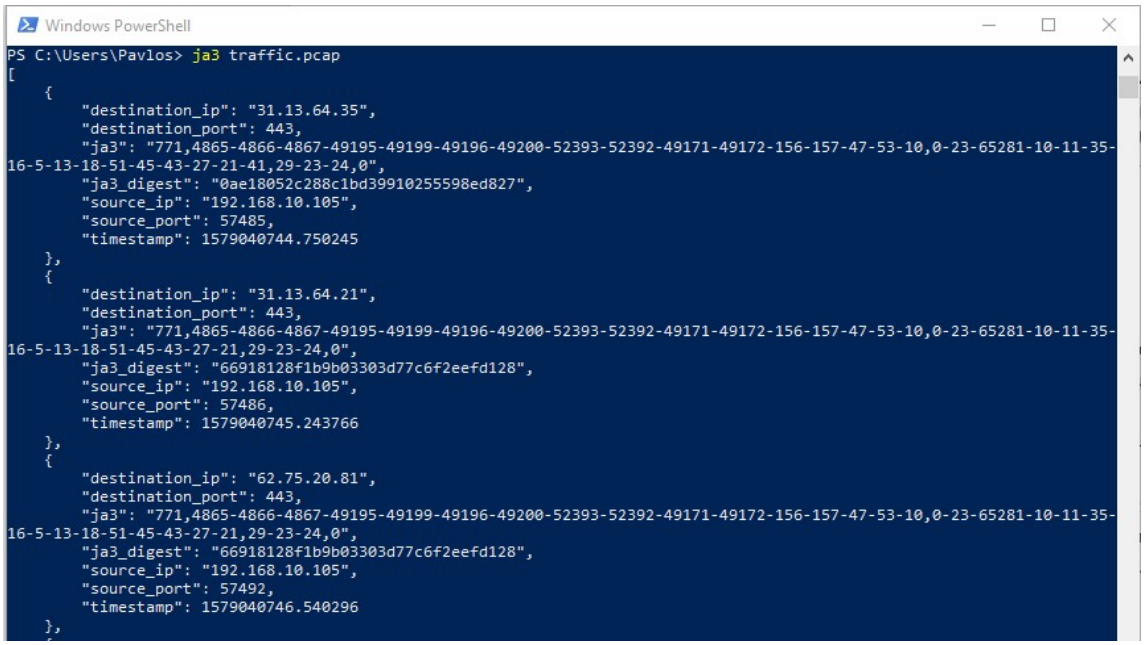
Εικόνα 4.4 Αρχείο καταγραφής DNS over HTTPS ερωτημάτων του Mozilla Firefox

4.5.2 Ψηφιακό αποτύπωμα πρωτοκόλλου TLS (TLS fingerprinting)

Το ψηφιακό αποτύπωμα του πρωτοκόλλου TLS είναι μια τεχνική η οποία συνδέει μια εφαρμογή και/ή μια βιβλιοθήκη TLS με παραμέτρους οι οποίες έχουν εξαχθεί από το TLS ClientHello

χρησιμοποιώντας μια βάση δεδομένων από προσεκτικά επιλεγμένα αποτυπώματα και μπορεί να χρησιμοποιηθεί για την αναγνώριση κακόβουλου λογισμικού, για γενικότερη ορατότητα των κρυπτογραφημένων δεδομένων που κινούνται στο δίκτυό μας και φυσικά για αναγνώριση ερωτημάτων DNS over HTTPS

. Από τις τελευταίες τεχνικές που είναι διαθέσιμες είναι η μέθοδος JA3 η οποία συγκεντρώνει τις δεκαδικές τιμές των bytes στα πεδία SSL Version, Accepted Ciphers, List of Extensions, Elliptic Curves και Elliptic Curve Formats του πακέτου ClientHello και στη συνέχεια ενώνει αυτές τις τιμές στη σειρά χρησιμοποιώντας ένα κόμμα για να χωρίσει κάθε πεδίο και μία παύλα για να χωρίσει κάθε τιμή που υπάρχει σε κάθε πεδίο. Στη συνέχεια, με τη βοήθεια της συνάρτησης κατακερματισμού md5 παράγεται ένα αλφαριθμητικό 32 bit το οποίο είναι το αποτύπωμα JA3. Το JA3S είναι το JA3 από την πλευρά του διακομιστή της SSL/TLS επικοινωνίας και είναι το αποτύπωμα του τρόπου με τον οποίο απαντά ο διακομιστής σε κάθε πελάτη.



Εικόνα 4.5 Υλοποίηση της τεχνικής JA3 σε αρχείο κίνησης δικτύου του wireshark

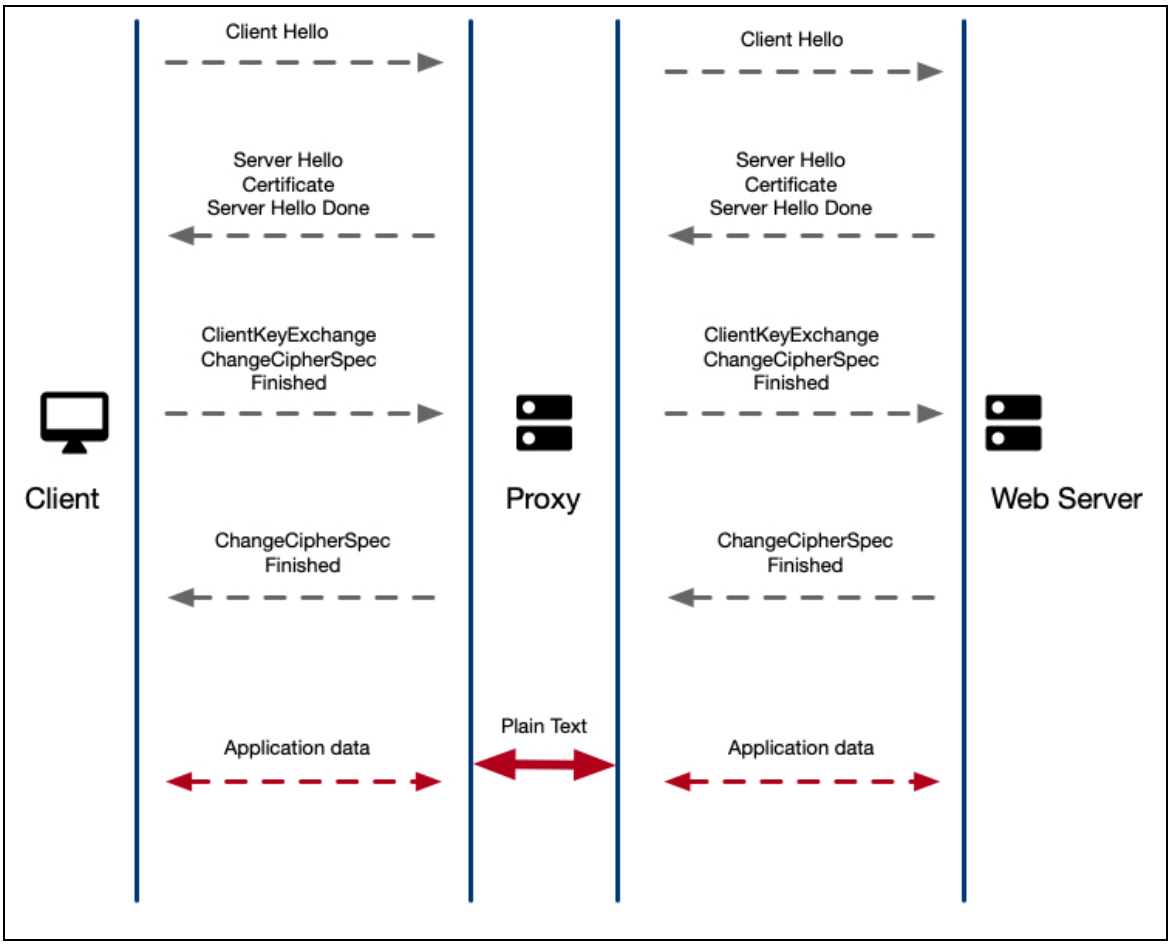
4.5.3 Επιθεώρηση κίνησης SSL/TLS μέσω self-signed certificates

Η επιθεώρηση της κίνησης SSL/TLS σε ένα δίκτυο είναι η διαδικασία όπου παρακολουθούμε την κρυπτογραφημένη διαδικτυακή κίνηση μεταξύ διακομιστή-πελάτη με σκοπό να εξάγουμε, στην περίπτωσή μας, ερωτήματα DNS over HTTPS που έγιναν στο δίκτυο και να τα

αποθηκεύσουμε σε αρχεία καταγραφής για την περαιτέρω ανάλυσή τους από ειδικά λογισμικά ασφάλειας.

Αυτή η διαδικασία μπορεί να γίνει δημιουργώντας self-signed πιστοποιητικά στον client, το οποίο το γνωρίζει και το χρησιμοποιεί και ο proxy, και στήνοντας έναν proxy ο οποίος θα παίξει ουσιαστικά τον ρόλο του man-in-the-middle και θα αποκρυπτογραφεί την SSL κίνηση ανάμεσα στον client και τον server. Ουσιαστικά γίνεται το εξής:

- Όταν προσπαθούμε να συνδεθούμε σε έναν ασφαλή ιστότοπο ο proxy, και όχι ο client, λαμβάνει τα πιστοποιητικά του web server.
- Ο proxy αναλαμβάνει να εγκαταστήσει μια ασφαλή SSL σύνδεση μεταξύ του ιδίου και του web server.
- Έπειτα ο proxy στέλνει ένα ψηφιακό πιστοποιητικό το οποίο φαίνεται να είναι του web server.
- Τέλος, εγκαθίσταται μια ασφαλής σύνδεση μεταξύ του client και του proxy.

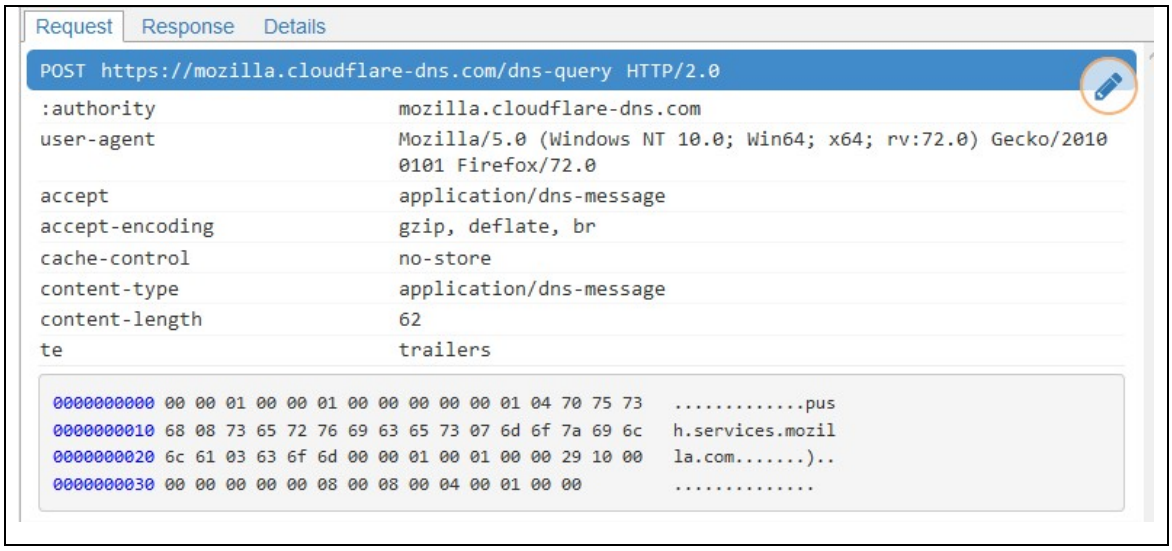


Εικόνα 4.6 Proxy SSL inspection

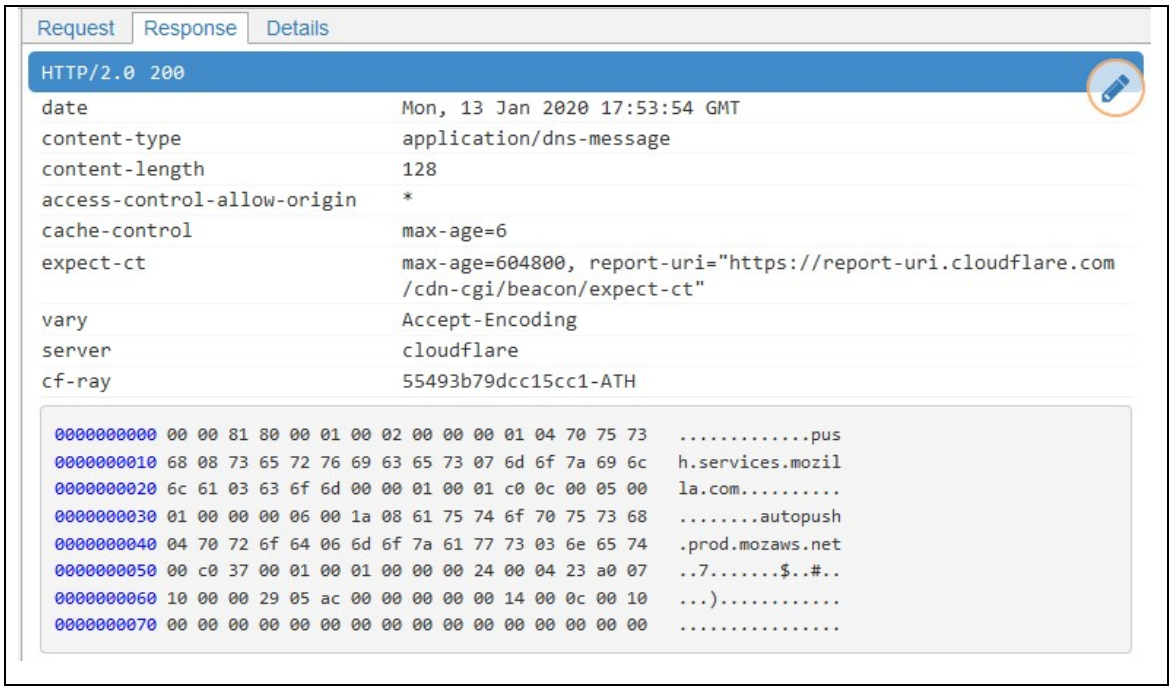
Η διαδικασία που ακολουθήσαμε στο εργαστήριο που φτιάξαμε για τις ανάγκες της παρούσας εργασίας ήταν εξής:

- Εγκαταστήσαμε τον MITMPROXY, έναν δωρεάν και ανοιχτού λογισμικού https proxy στον host που παίζει το ρόλο του HTTPS interceptor.
- Παράξαμε με τη βοήθεια της βιβλιοθήκης openssl ένα self-signed πιστοποιητικό το οποίο το εγκαταστήσαμε στον client και φυσικά στον proxy.
- Ορίσαμε ως proxy του συστήματος το λογισμικό MITMPROXY που εγκαταστήσαμε για να περνάει ολόκληρη η διαδικτυακή κίνηση μέσω αυτού με σκοπό την αποκρυπτογράφησή της.

- Με τη βοήθεια της εντολής mitmdump αποθηκεύσαμε την διαδικτυακή κίνηση σε ένα αρχείο καταγραφής το οποίο θα το εισάγουμε στον host όπου τρέχει το λογισμικό ασφαλείας για περαιτέρω ανάλυση



Εικόνα 4.7 Αποκρυπτογραφημένη αίτηση στον DNS API server



Εικόνα 4.8 Αποκρυπτογραφημένη απόκριση του DNS API server

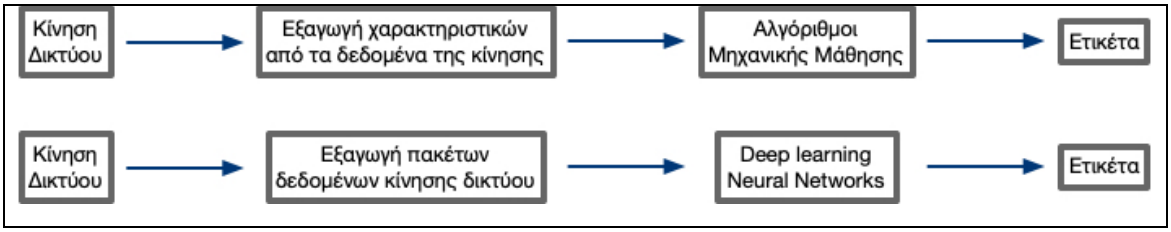
4.5.4 Ταξινόμηση κρυπτογραφημένης κίνησης δικτύου και αναγνώρισης DNS over HTTPS

Οι επαγγελματίες αναλυτές του κλάδου ασφάλειας της πληροφορικής μπορούν να χρησιμοποιήσουν αλγορίθμους μηχανικής μάθησης για να ταξινομήσουν την κρυπτογραφημένη κίνηση στο δίκτυο και να χρησιμοποιήσουν στατιστικά μοτίβα (statistical patterns) για να αναγνωρίσουν την DNS over HTTPS κίνηση χωρίς να χρειαστεί να αποκρυπτογραφήσουν τις κρυπτογραφημένες συνομιλίες.

Για να λειτουργήσουν σωστά αυτοί οι αλγόριθμοι χρειάζονται μεγάλο όγκο δεδομένων με συγκεκριμένα χαρακτηριστικά που αποφασίζουμε εμείς ποια θα είναι. Αυτά τα χαρακτηριστικά μπορεί να προέρχονται από τα πακέτα των δεδομένων που ανταλλάσσονται κατά τη διάρκεια της συνομιλίας ή μπορεί να είναι δεδομένα που έχουμε στη διάθεσή τα οποία χαρακτηρίζουν την κίνηση του δικτύου. Τα δεδομένα των πακέτων εισάγονται σε deep learning αλγορίθμους νευρωνικών δικτύων και μας παράγουν το αποτέλεσμα της ταξινόμησης. Τα δεδομένα της κίνησης του δικτύου χωρίζονται συνήθως σε τρεις κατηγορίες. Η πρώτη είναι τα χαρακτηριστικά της σύνδεσης τα οποία περιγράφουν τη συμπεριφορά της κίνησης και δεν είναι συνδεδεμένα με το κρυπτογραφημένο κομμάτι της. Η δεύτερη είναι τα χαρακτηριστικά της SSL σύνδεσης τα οποία περιγράφουν το SSL handshake και πληροφορίες σχετικά με το κρυπτογραφημένο κομμάτι της σύνδεσης. Το τρίτο είναι τα χαρακτηριστικά του ψηφιακού πιστοποιητικού τα οποία μας περιγράφουν πληροφορίες σχετικά με το πιστοποιητικό που μας δίνει ο webserver κατά τη διάρκεια του SSL handshake. Αυτά τα χαρακτηριστικά μπορούν να συγκεντρωθούν σε ένα αρχείο και να μας βοηθήσουν να φτιάξουμε το μοντέλο πάνω στο οποίο θα τρέξουν αλγόριθμοι μηχανικής μάθησης όπως ο XGBoost, SVM, τα Νευρωνικά Δίκτυα και ο RandomForest. Τέλος, πρέπει να βάλουμε ετικέτες στα δεδομένα μας για το αν η σύνδεση είναι ερώτημα DNS. Μια απλή προσέγγιση θα ήταν να βάλουμε ετικέτα με τον αριθμό 0 αν η σύνδεση δεν είναι ερώτημα DNS και 1 αν είναι.

Το να έχουμε labeled data κάνει την ταξινόμηση πολύ πιο εύκολη διότι έχουμε να λύσουμε ένα πρόβλημα με την τεχνική του supervised learning που συνήθως είναι πιο αποτελεσματική από την unsupervised και έχει μεγαλύτερα ποσοστά επιτυχίας στις προβλέψεις που κάνει. Φυσικά σε πραγματικές εφαρμογές η ετικέτες που έχουμε είναι πιο πολλές και η κίνηση ταξινομείται σε περισσότερες κατηγορίες διότι πρέπει να είμαστε σε θέση να εντοπίζουμε και κακόβουλο λογισμικό, όπως ακόμα πρέπει να λάβουμε υπόψιν ότι και το κακόβουλο λογισμικό

μπορεί να χρησιμοποιεί DNS over HTTPS για τα ερωτήματά του με σκοπό να μην είναι ανιχνεύσιμο από τα λογισμικά ασφαλείας.



Εικόνα 4.9 Διαδικασία ταξινόμησης ερωτημάτων DNS over HTTPS

ΚΕΦΑΛΑΙΟ 5.Αποκεντρωμένη διαχείριση DNS βασιζόμενη στην τεχνολογία Blockchain

5.1 Εισαγωγή

Κατά καιρούς στην επιστήμη των υπολογιστών υπάρχει η εναλλαγή των τάσεων της συγκέντρωσης και της αποκέντρωσης. Ένα χαρακτηριστικό παράδειγμα είναι η εναλλαγή από τον συγκεντρωμένο αποθηκευτικό χώρο στο αποκεντρωμένο cloud που κυριαρχεί τα τελευταία χρόνια. Ακόμα και το internet που είχε σχεδιαστεί να είναι αποκεντρωμένο στην πραγματικότητα διοικείται από πολύ λίγους εταίρους και η ανάγκη για αποκέντρωση γίνεται όλο και μεγαλύτερη. Η ανάγκη αυτή εκδηλώνεται με πολλούς τρόπους και τα τελευταία χρόνια παρατηρούμε όλο και πιο μεγάλη ζήτηση για τη δημιουργία αποκεντρωμένων υπηρεσιών.

Ένα χαρακτηριστικό παράδειγμα είναι η τεχνολογία blockchain η οποία έχει αρχίσει και χρησιμοποιείται σε πολλά και διαφορετικά πεδία της επιστήμης. Η ανάγκη αυτή για αποκεντροποίηση γίνεται προφανής ειδικά σε συστήματα που οι υπηρεσίες τους είναι παραδοσιακά συγκεντρωμένες σε ένα ή σε πολύ λίγα σημεία, όπως το DNS. Όπως είδαμε στα προηγούμενα κεφάλαια, το DNS είναι μια κατανεμημένη βάση δεδομένων με κεντρική διαχείριση δεδομένων, ελεγχόμενη κυρίως από τον οργανισμό ICAAN, ο οποίος ελέγχει τα top-level domains και τη λειτουργία των root servers.

Ενώ το DNS είναι ένα από τα πιο παλιά πρωτόκολλα του internet που εξακολουθούν να λειτουργούν, έχει πολλά μειονεκτήματα που επιβάλλουν την αντικατάστασή του ή τον επανασχεδιασμό του έτσι ώστε να ανταποκρίνεται στις προκλήσεις της εποχής. Τα μειονεκτήματά του και ειδικότερα τις απειλές για την ασφάλεια των χρηστών τα έχουμε αναπτύξει στα προηγούμενα κεφάλαια. Αυτά τα πολύ σοβαρά θέματα οδήγησαν ην επιστημονική κοινότητα και ερευνητές από όλο τον κόσμο να βρουν εναλλακτικές προτάσεις για το domain name system. Χαρακτηριστική είναι η εναλλαγή προς τεχνολογίες όπως το DNS over HTTPS που αναπτύξαμε λεπτομερώς στα προηγούμενα κεφάλαια και το DNS over TLS, ενώ πολλοί αναζητούν λύσεις ακόμα και χωρίς την υποστήριξη του οργανισμού ICAAN, οι οποίες όμως είναι συγκεντρωμένες σε ένα σημείο όπως ακριβώς και το υπάρχον σύστημα.

Μία από τις πιο υποσχόμενες λύσεις για αποκέντρωση των υπηρεσιών DNS είναι η τεχνολογία blockchain η οποία έχει υιοθετηθεί από πολλές αλυσίδες όπως το Ethereum, το Namecoin και από άλλα σχετικά πρωτόκολλα και έχει τραβήξει το ενδιαφέρον πολλών μεγάλων εταιρειών (όπως η Alibaba,η IBM, η Samsung) παρά το ότι είναι πολύ λίγο καιρό στο προσκήνιο. Αυτή η τεχνολογία μας φέρνει αντιμέτωπους με πολλές προκλήσεις σε ένα μεγάλο φάσμα της πληροφορικής και οι ερευνητές έχουν ήδη αρχίσει να ερευνούν τις δυνατότητές της για ένα ασφαλέστερο διαδίκτυο αλλά και τις ευπάθειες που έχει. Όπως είναι αναμενόμενο, οι εγκληματίες του διαδικτύου έχουν ήδη αρχίσει να εκμεταλλεύονται τις αδυναμίες αυτής της τεχνολογίας και επόμενο είναι να γεννηθεί η ανάγκη για την λεπτομερή εξερεύνηση των ευπαθειών που έχουν οι λύσεις βασισμένες στην τεχνολογία blockchain αλλά και τα αποκεντρωμένα συστήματα αποθήκευσης.

Η αποκέντρωση των υπηρεσιών αναμφίβολα μας προσφέρει πολλά οφέλη σχετικά με την ιδιωτικότητα, την ασφάλεια και την διαφάνεια των καθημερινών μας συναλλαγών με το διαδίκτυο, αλλά προσθέτει ένα επίπεδο δυσκολίας παραπάνω στην ανίχνευση μολυσμένων συστημάτων και υπηρεσιών λόγω των κρυπτογραφημένων συνομιλιών αλλά και της έλλειψης γνώσης και εμπειρίας πάνω στην συγκεκριμένη τεχνολογία η οποία φυσικά πρέπει να ωριμάσει πριν αρχίσουμε να την χρησιμοποιούμε καθολικά σε λύσεις και λογισμικά όπου η ασφάλεια και η ιδιωτικότητα είναι αδιαπραγμάτευτες.

5.2 Blockchain-based DNS

Η αρχική ιδέα του πρωτοκόλλου είναι να υλοποιηθεί ένα σύστημα ονοματοδοσίας στο διαδίκτυο το οποίο θα είναι αποκεντρωμένο και κανένας δεν θα μπορεί να το ελέγξει, θα μας προστατεύει από τις ευπάθειες του υπάρχοντος συστήματος που μπορούν να εκμεταλλευθούν οι κακόβουλοι

χρήστες και τέλος να υπάρχει η δυνατότητα για ελεύθερη διακίνηση ιδεών και απόψεων χωρίς τη λογοκρισία των κυβερνήσεων.

Το σύστημα αυτό είναι βασισμένο στην τεχνολογία blockchain, που σημαίνει ότι θα είναι λογισμικό που θα τρέχει σε ένα ευρέως κατανεμημένο δίκτυο υπολογιστών και θεωρητικά δεν θα έχει κανένα σημείο αποτυχίας όπως και δεν θα βασίζεται σε κάποιον οργανισμό που θα μπορούσε να τροποποιήσει ή να σβήσει δεδομένα χωρίς την έγκριση της πλειοψηφίας του δικτύου. Ένα από αυτά τα λογισμικά είναι το Handshake το οποίο είναι μία παραλλαγή του δημοφιλούς λογισμικού bitcoin και όπως το δίκτυο των miners του bitcoin προστατεύει το κρυπτονόμισμα από μη εξουσιοδοτημένες αλλαγές έτσι και το handshake διατηρεί εγγραφές από διαδικτυακά ονόματα τα οποία τα προστατεύει το δίκτυό του. Το handshake αισιοδοξεί να αποκεντρώσει υπηρεσίες όπως το DNS που αποκλειστικός διαχειριστής είναι ο οργανισμός ICAAN με ότι συνεπάγεται αυτό στην ιδιωτικότητα και την ασφάλεια των χρηστών, αλλά και στην δημοκρατικότητα των αποφάσεων που πρέπει να πάρει υπό την πίεση κυρίως των κυβερνήσεων. Επίσης, στους στόχους του είναι να αποκεντρώσει και τις υπηρεσίες έκδοσης ψηφιακών πιστοποιητικών μέσω της τεχνολογίας blockchain που αυτή τη στιγμή τις διαχειρίζονται πολλοί λίγοι οργανισμοί και αν κάποιος κακόβουλος καταφέρει να υποκλέψει πληροφορίες και να εκδίδει πιστοποιητικά στο όνομά τους, τότε ολόκληρη η ασφάλεια του διαδικτύου τίθεται σε κίνδυνο.

Παρόμοιες προσπάθειες έχουν γίνει και στον τομέα του Internet of things με την τεχνολογία blockchain να έχει προταθεί ως μία από τις τεχνολογίες που θα χρησιμοποιούν τα πρωτόκολλα επικοινωνίας. Για παράδειγμα, το DNSLedger είναι ένα σύστημα που χρησιμοποιεί την τεχνολογία blockchain για να εισάγει ένα DNS σύστημα για τις συσκευές του IoT, το BlockONS που σύμφωνα με τους δημιουργούς του προστατεύει το πρωτόκολλο DNS από πολλές και σημαντικές ευπάθειες που έχει μέχρι τώρα και το ConsortiumDNS το οποίο οι δημιουργοί του υποστηρίζουν ότι προστατεύει τους χρήστες από κακόβουλο διαδικτυακό λογισμικό.

Φυσικά η ιδέα χρησιμοποίησης του blockchain για την ονοματοδοσία στο διαδίκτυο έγινε αποδεκτή από την πρώτη μέρα ανακοίνωσής της και προσπάθειες ανάπτυξης τέτοιων συστημάτων άρχισαν από πολύ νωρίς να υλοποιούνται. Το Namecoin, το Ethereum name service, το Blockstack είναι μόνο κάποιες από τις πολλές προσπάθειες για την υλοποίηση του Blockchain-based DNS και πολλές από αυτές έχουν ήδη γίνουν συμβατές με την υπάρχουσα υποδομή DNS με το handshake να έχει ήδη προσθέσει τα 100.000 πιο δημοφιλή domains στην αλυσίδα του.

Τα πλεονεκτήματα μιας τέτοιας εναλλαγής της ονοματοδοσίας στο διαδίκτυο είναι πολλά και πέρα από την ασφάλεια και την ιδιωτικότητα, οι χρήστες μπορούν να επωφεληθούν και από

την ελευθερία που τους προσφέρει ακόμα και στην επιλογή των ονομάτων και των καταλήξεων, πέρα από την ελευθερία του διαδικτυακού λόγου και της λογοκρισίας των εκάστοτε κυβερνήσεων.

5.3 Ασφάλεια και ιδιωτικότητα

Με το υπάρχον σύστημα DNS, η απόκριση του συστήματος μπορεί να σε παραπέμψει σε κακόβουλους ιστότοπους που έχουν ως σκοπό να δώσουν στο χρήστη κακόβουλο λογισμικό να τρέξει στον υπολογιστή του ή να του κλέψει τους κωδικούς εισόδου σε κάποια υπηρεσία. Το DNS over HTTPS όπως εξηγήσαμε στα προηγούμενα κεφάλαια αισιοδοξεί να λύσει αυτό το πρόβλημα, αλλά αυτό δεν είναι αλήθεια. Η λειτουργία του επιτρέπει στις αρχές έκδοσης ψηφιακών πιστοποιητικών (οι οποίες είναι μεγάλες εταιρείες ή κυβερνήσεις) να εγγυηθούν τη νομιμότητα ενός ιστοτόπου. Εάν μία αρχή έκδοσης ψηφιακών πιστοποιητικών πέσει θύμα εγκληματιών του διαδικτύου, κάνει κάποιο λάθος ή ακόμα και να εξυπηρετήσει συμφέροντα κυβερνήσεων μπορεί να εκδώσει ψεύτικα πιστοποιητικά τα οποία δίνουν τη δυνατότητα στους κακόβουλους να διαβάσουν μια κρυπτογραφημένη επικοινωνία. Οι πιο πολλές blockchain-based υπηρεσίες DNS κάνουν τη δουλειά που θα έκανε μια αρχή έκδοσης ψηφιακών πιστοποιητικών με τη διαφορά ότι δεν βασίζονται σε αυτή με αποτέλεσμα να μην μπορεί κανείς να υποκλέψει συνομιλίες όπως ακριβώς δεν μπορεί κανείς να κλέψει τα bitcoin που έχουμε στο λογαριασμό μας και φυσικά, η προστασία αυτή είναι δωρεάν.

Στο θέμα της ιδιωτικότητας των χρηστών, με το υπάρχον σύστημα DNS οι ISP’s και οι διάφοροι ενδιαφερόμενοι που έχουν πρόσβαση στους DNS servers μπορούν να παρακολουθούν ποιους ιστότοπους επισκεπτόμαστε όπως εξηγήσαμε στα προηγούμενα κεφάλαια. Οι λύσεις blockchain-based DNS δεν δημιουργούν κίνηση στο δίκτυο, καθώς τα ερωτήματα DNS γίνονται τοπικά στον υπολογιστή μας.

5.4 Απόδοση του συστήματος

Κάθε αλλαγή που γίνεται στο υπάρχουν σύστημα DNS δεν γίνεται αντιληπτή στο χρήστη για περίπου 24-48 ώρες. Αυτό έχει ως αποτέλεσμα να έχουμε διακοπή κάποιων υπηρεσιών που προσφέρονται από έναν ιστότοπο μέχρι να ενημερωθούν όλοι οι nameservers για την καινούρια διεύθυνση ip ενός domain. Οι εγγραφές που τηρούνται στα συστήματα blockchain-based DNS ανανεώνονται σε πολύ μικρότερο χρονικό διάστημα (μέσο όρο 1 ώρα) με αποτέλεσμα οι χρήστες να βλέπουν άμεσα τις αλλαγές των nameservers.

Η απόδοση των συστημάτων βασισμένων στην τεχνολογία blockchain είναι βελτιωμένη και στο χρόνο που γίνεται resolve ένα domain name. Η αναζήτηση γίνεται τοπικά στον υπολογιστή και χρειάζεται πολύ λίγος χρόνος για να μας επιστρέψει το σύστημα τις πληροφορίες που ζητάμε, σε αντίθεση με το κλασικό σύστημα που κάνει την αναζήτησή του σε servers στο διαδίκτυο.

5.5 Απειλές και ευπάθειες για το σύστημα DNS.

5.5.1 Ευπάθειες της τεχνολογίας blockchain

Όπως και το πρωτόκολλο DNS over HTTPS κληρονομεί τις ευπάθειες του πρωτοκόλλου HTTPS, έτσι και τα blockchain-based DNS συστήματα κληρονομούν τις ευπάθειες του blockchain.

Οι ευπάθειες του blockchain είναι οι εξής:

- Η ευπάθεια του 51%, όπου αν ένας χρήστης καταφέρει να αλλάξει το 51% των εγγραφών της αλυσίδας πριν εισαχθεί άλλη εγγραφή από άλλο χρήστη, τότε μπορεί να αλλάξει τα περιεχόμενα της αλυσίδας προς όφελός του.
- Εάν χαθεί το ιδιωτικό κλειδί του χρήστη τότε δεν μπορεί να ανακτηθεί με κανένα τρόπο. Σε περίπτωση που αυτό το κλειδί κλαπεί, τότε οι πληροφορίες του χρήστη μπορούν να αλλαχθούν χωρίς τη συγκατάθεσή του και είναι πολύ δύσκολο να ανακτήσουμε τις παραποιημένες πληροφορίες.
- Ευπάθειες στα «έξυπνα συμβόλαια» του blockchain που στην ουσία είναι λογισμικό που τρέχει τοπικά στον υπολογιστή του χρήστη και η υλοποίησή του μπορεί να έχει σφάλματα που μπορεί να εκμεταλλευτεί ο επιτιθέμενος.

5.5.2 Κακόβουλο λογισμικό

Τα κακόβουλα λογισμικά που κυκλοφορούν σε οποιαδήποτε μορφή κάνουν χρήση του πρωτοκόλλου DNS για διάφορους λόγους, όπως το να επικοινωνήσουν με τον command and control server ή να κατεβάσουν κώδικα από μια τοποθεσία του διαδικτύου. Η δραστηριότητα αυτή όπως εξηγήσαμε στα προηγούμενα κεφάλαια μπορεί εύκολα να ανιχνευθεί από τα λογισμικά ασφαλείας διακόπτοντας την διαδικτυακή του επικοινωνία και φυσικά δίνοντας την ευκαιρία να ανακαλυφθεί η ύπαρξή του.

Ένα τέχνασμα των δημιουργών κακόβουλων λογισμικών είναι να χρησιμοποιούν blockchain-based DNS για να επικοινωνούν διαδικτυακά μέσω top-level domain όπως EMC, COIN, LIB και BAZAR που είναι διαθέσιμα μόνο μέσω blockchain-based DNS λογισμικών και με αυτό τον τρόπο να κρύβονται πίσω από την τεχνολογία blockchain αφού το resolve του domain που ψάχνουν γίνεται τοπικά στον υπολογιστή του κάθε χρήστη.

5.5.3 Μηχανισμός καταχώρησης domain

Στο υπάρχον σύστημα DNS εάν ένας κακόβουλος χρήστης καταχωρήσει ένα domain το οποίο εξυπηρετεί κακόβουλους σκοπούς, όπως το domain goooogle.com το οποίο έχει ένα γράμμα παραπάνω από τη δημοφιλή μηχανή αναζήτησης, με σκοπό να το χρησιμοποιήσει είτε για να υποκλέψει στοιχεία, είτε για να σπιλώσει τη φήμη της εταιρείας, είτε για οποιοδήποτε κακόβουλο σκοπό, ο οργανισμός που ελέγχει τα domains του top-level domain .com μπορεί να αφαιρέσει την ιδιοκτησία από αυτόν που το καταχώρησε και να το προσθέσει σε μια λίστα όπου δεν επιτρέπεται να καταχωρηθεί από κανέναν.

Σε ένα σύστημα blockchain-based DNS αυτό μπορεί να μην είναι εφικτό, διότι δεν υπάρχει κεντρική διαχείριση που θα λάβει μέτρα μετά την καταχώρηση ενός τέτοιου domain. Φυσικά τέτοια domain μπορούν να καταχωρηθούν και με άλλους τρόπους, όπως για παράδειγμα να αφήσουμε κενά ή να βάλουμε κεφαλαία γράμματα. Τα συστήματα blockchain-based DNS πρέπει να λάβουν σοβαρά υπόψιν τους τέτοιες απειλές και να βρουν λύσεις πριν το λογισμικό γίνει ευρέως διαθέσιμο στους χρήστες του διαδικτύου.

5.5.4 Phissing

Η πρακτική phissing είναι μια από τις πιο διαδεδομένες επιθέσεις στον κυβερνοχώρο με τα ποσοστά επιτυχίας να είναι πολύ υψηλά, ειδικά όταν σχεδιάζονται και εκτελούνται μέσω email. Τα blockchain-based DNS συστήματα μπορούν να καταχωρούν domains που μοιάζουν με τα ευρέως διαδεδομένα με τη διαφορά ότι διαφέρουν στην top-level κατάληξη. Αυτή η τεχνική μπορεί πολύ εύκολα να ξεγελάσει έναν χρήστη ότι το domain που επισκέπτεται είναι το σωστό λόγω ότι τα top-level domains που μπορούν να καταχωρηθούν δεν είναι ευρέως γνωστά στο κοινό, αλλά και για το λόγο ότι μπορεί να έχουν ασφαλή HTTPS σύνδεση χρήστη-διακομιστή μέσω ενός ψηφιακού πιστοποιητικού που φυσικά ξεγελά το χρήστη ότι η επικοινωνία μεταξύ του browser και του server είναι ασφαλής.

5.5.5 Αμετάβλητα δεδομένα

Τα δεδομένα που γράφονται στην αλυσίδα του blockchain, λόγω της αρχιτεκτονικής της τεχνολογίας, δεν μπορούν να διαγραφούν. Αυτό έχει ως αποτέλεσμα δεδομένα που είναι παράνομα και πρέπει να διαγραφούν να παραμένουν αμετάβλητα και διαθέσιμα σε κάθε χρήστη της αλυσίδας. Οι διάφορες υλοποιήσεις της τεχνολογίας πρέπει να λάβουν σοβαρά υπόψιν τους να προσθέσουν τη δυνατότητα διαγραφής κακόβουλου περιεχομένου, καθώς είναι σίγουρο ότι θα χρησιμοποιηθούν από εγκληματίες του διαδικτύου για κακόβουλους σκοπούς.

5.6 Γιατί το blockchain-based DNS θα γίνει το επόμενο βήμα μετά το DNS over HTTPS.

Το κύριο πρόβλημα του DNS over HTTPS είναι η κεντρική διαχείριση του πρωτοκόλλου και η έλλειψη επικύρωσης στα δεδομένα που λαμβάνουμε. Η κεντρική υποδομή του DNS έχει γίνει πλέον στόχος πολλών επιθέσεων και φυσικά είναι πηγή προσωπικών πληροφοριών των μεγάλων εταιρειών που το ελέγχουν. Η υποδομή του αποκεντρωμένου DNS από την άλλη είναι μια ιδανική πλατφόρμα για το πρωτόκολλο διότι εξασφαλίζει την ιδιωτικότητα των χρηστών και την ακεραιότητα των δεδομένων που λαμβάνουν.

Για παράδειγμα, ο ιδιοκτήτης του domain unipi.gr αποθηκεύει τις ψηφιακές υπογραφές του σε ένα δημόσιο blockchain και επιτρέπει σε οποιαδήποτε συσκευή (web browsers, smartphones, συσκευές IoT κτλ) να ελέγξει την αντίστοιχη καταχώρηση στο μπλοκ της αλυσίδας και να βρει τη σωστή υπογραφή. Αυτό επιτρέπει στο στον ιδιοκτήτη του domain να διαχειρίζεται μόνος του τα domains που έχει στην κατοχή του χωρίς να χρειάζεται να πάρει ένα πιστοποιητικό από κάποιον τρίτο οργανισμό. Επιπλέον, αποκεντρώνει πλήρως την εξυπηρέτηση των ερωτημάτων DNS διότι κάθε blockchain server μπορεί να σερβίρει δεδομένα DNS.

Αυτή η νέα τεχνολογία έχει γίνει ευρέως αποδεκτή κυρίως από υποστηρικτές της τεχνολογίας blockchain και γίνονται πολλές προσπάθειες με πλατφόρμες όπως το Namecoin, το Ethereum Name System, το Handshake και άλλα έτσι ώστε να εδραιωθεί και να αντικαταστήσει το μη ασφαλές υπάρχον κεντρικό σύστημα διαχείρισης του DNS.

ΚΕΦΑΛΑΙΟ 6. Συμπεράσματα

Η ιδέα υλοποίησης του DNS ήταν η λύση στα προβλήματα που είχε η ονοματοδοσία στο διαδίκτυο σχετικά με τα hosts.txt αρχεία που αρχικά έκαναν τη δουλειά του σημερινού DNS όπως το ξέρουμε. Η ευρέως διαδεδομένη χρήση του και η ικανότητά του να αντιστοιχίζει

ονόματα χώρου και διευθύνσεις ip για λογαριασμό χρηστών και εφαρμογών το καθιστά ένα κρίσιμο και απαραίτητο πρωτόκολλο για τη λειτουργία του διαδικτύου με την κατανεμημένη διαχείρισή του να είναι ένα από τα πιο δυνατά χαρακτηριστικά του. Η υλοποίηση όμως και οι προδιαγραφές του πρωτοκόλλου αρχικά δεν περιείχαν ασφάλεια με αποτέλεσμα να είναι ευάλωτο σε επιθέσεις που αναλύσαμε στο κεφάλαιο 2 από τις οποίες μπορούν εύκολα να επωφεληθούν κακόβουλοι χρήστες και εγκληματίες του διαδικτύου.

Για να προστεθεί ασφάλεια και να αντιμετωπιστούν αυτές οι απειλές προστέθηκαν χαρακτηριστικά όπως το DNSSEC το οποίο παρέχει έλεγχο ταυτότητας και αυθεντικότητα στα δεδομένα που ανταλλάσσονται και εξασφαλίζει ότι τα δεδομένα DNS προέρχονται από πιστοποιημένη πηγή χωρίς όμως να παρέχεται εμπιστευτικότητα και ακεραιότητα των δεδομένων. Αυτά τα προβλήματα επιχειρεί να λύσει το DNS over HTTPS το οποίο έχει ως στόχο την παροχή εμπιστευτικότητας και ακεραιότητας των δεδομένων DNS και την εξασφάλιση του διαύλου επικοινωνίας μεταξύ του πελάτη DNS και του διακομιστή κουβαλώντας όμως γνωστές ευπάθειες του πρωτοκόλλου HTTP μέσω του οποίου ανταλλάσσει τα δεδομένα DNS. Επίσης, για το λόγο ότι τα δεδομένα ανταλλάσσονται μέσω ασφαλούς καναλιού επικοινωνίας, δημιουργούνται προβλήματα στην επίβλεψη της κίνησης των δικτύων και κατ' επέκταση στην ασφάλειά τους και οι κακόβουλοι χρήστες μπορούν εύκολα να κρύψουν την DNS επικοινωνία που τυχόν παράγουν κακόβουλα λογισμικά. Το πρωτόκολλο DNS over HTTPS λύνει πολλές από τις ευπάθειες ασφαλείας που έχει το DNS αλλά εισάγει προκλήσεις στην αποτελεσματική επίβλεψη των δικτύων καθώς πολλές από τις τεχνικές αναγνώρισης κακόβουλης κίνησης στηρίζονται στην ανάλυση της κίνησης του DNS over UDP και τέλος η διαχείριση των υποδομών μένει αποκλειστικά σε λίγους μεγάλους οργανισμούς με τα όποια προβλήματα ιδιωτικότητας και ασφάλειας μπορούν να προκύψουν.

Τα τελευταία χρόνια όμως έχει εισαχθεί η τεχνολογία blockchain η οποία είναι πολλά υποσχόμενη για την ασφάλεια και την ιδιωτικότητα των χρηστών του διαδικτύου και όχι μόνο. Η τεχνολογία αυτή λύνει προβλήματα ασφάλειας και ιδιωτικότητας που απασχολούν πολλά χρόνια την ερευνητική κοινότητα παγκοσμίως και μπορεί να υλοποιήσει λύσεις οι οποίες θα είναι αποκεντρωμένες και ασφαλείς, όπως το blockchain-based DNS ή η παραγωγή ψηφιακών πιστοποιητικών ακόμα και να σταματήσει επιθέσεις όπως denial-of-service attacks και man-in-the-middle. Το blockchain έχει ήδη μπει στην διαδικτυακή μας ζωή και σε λίγα χρόνια θα κυριαρχεί σε λύσεις που έχουν ως κύριο μέλημά τους την ασφάλεια και μία από αυτές τις λύσεις είναι και το πρωτόκολλο blockchain-based DNS.

ΚΕΦΑΛΑΙΟ 7. Βιβλιογραφία

[1] Associating a DoH Server with a Resolver, https://tools.ietf.org/html/draft-hoffman-resolver-associated-doh-01

[2] Threat Analysis of the Domain Name System (DNS), https://tools.ietf.org/html/rfc3833

[3] Challenges in Effective DNS Query Monitoring, https://www.sans.org/reading-room/whitepapers/dns/challenges-effective-dns-query-monitoring-39215

[4] DNS Queries over HTTPS (DOH), https://tools.ietf.org/html/draft-ietf-doh-dns-over-https-08

[5] A New Needle and Haystack: Detecting DNS over HTTPS Usage, https://www.sans.org/reading-room/whitepapers/dns/needle-haystack-detecting-dns-https-usage-39160

[6] Centralized DNS over HTTPS (DoH) Implementation Issues and Risks, https://tools.ietf.org/id/draft-livingood-doh-implementation-risks-issues-04.txt

[7] Unravelling Ariadne's Thread: Exploring the Threats of Decentralized DNS, https://arxiv.org/pdf/1912.03552.pdf