1. Επιθέσεις DoS και DDoS

Μία επίθεση *Άρνησης Παροχής Υπηρεσιών* (*Denial of Service, DoS*) είναι μια επίθεση που αποσκοπεί στο να αποκόψει νόμιμους χρήστες του διαδικτύου από ένα δικτυακό πόρο είτε προσωρινά ή για μεγάλο χρονικό διάστημα. Μία επίθεση *DoS* έχει αφετηρία έναν υπολογιστή και πλημμυρίζει το θύμα με πολύ μεγάλο όγκο κίνησης, στοχεύοντας στην κατασπατάληση των πόρων του (επεξεργαστής, φυσική μνήμη, κτλ.). Το θύμα απασχολείται με ανούσιες εργασίες, αφού καλείται να επεξεργαστεί όλα τα μηνύματα που δέχεται από τον επιτιθέμενο και αδυνατεί να εξυπηρετήσει τους πελάτες του, απαντώντας στα μηνύματά τους.

Εικόνα 1. Επίθεση *DoS*

Συνεπώς, οι επιθέσεις *DoS* δε συνίστανται στην εγκατάσταση *κακόβουλου κώδικα* (*malware*) στο θύμα, αλλά στην εκμετάλλευση τρωτών σημείων των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται και στην αδύναμη υποδομή του θύματος (περιορισμένη φυσική μνήμη, επεξεργαστική ισχύς, κλπ).

Εικόνα 2. Επίθεση *DDoS*

Όταν η επίθεση δεν έχει σημείο εκκίνησης έναν υπολογιστή, αλλά πολλούς υπολογιστές, που βρίσκονται κατανεμημένοι σε διαφορετικά σημεία του διαδικτύου και προχωρούν σε συντονισμένη επίθεση, ονομάζεται *Κατανεμημένη Επίθεση DoS* (*Distributed DoS, DDoS*). Αξιοποιώντας τη δύναμη μεγάλου αριθμού υπολογιστών, μια επίθεση *DDoS* είναι πάρα πολύ δυνατότερη από μία απλή επίθεση *DoS* και μπορεί να στοχεύει στην κατασπατάληση του *εύρους ζώνης* (*bandwidth*) των ζεύξεων του δικτύου του θύματος, αλλά και στην ταχύτερη εξάντληση των πόρων του.

2. Συνέπειες και Κίνητρα Επιθέσεων DoS/DDoS

Οι συνέπειες μιας επιτυχημένης επίθεσης *DoS*/*DDoS* είναι πολύ μεγάλες για τον οργανισμό που διαχειρίζεται το θύμα και αφορούν στους παρακάτω τομείς:

- ***Απώλεια εσόδων*:** Πολλές επιχειρήσεις σήμερα λειτουργούν ηλεκτρονικά. Τα έσοδά τους στηρίζονται αποκλειστικά στις αγορές που πραγματοποιούν online οι χρήστες. Οι επιχειρήσεις αυτές έχουν ολοκληρωτική απώλεια εσόδων σε μια επίθεση *DDoS*.
- ***Απώλεια παραγωγικότητας*:** Η εργασία στις σύγχρονες επιχειρήσεις απαιτεί την πρόσβαση των εργαζομένων στο διαδίκτυο, σε απομακρυσμένους εξυπηρετητές, σε *υπηρεσίες συννέφου* (*cloud*) και άλλες σημαντικές δικτυακές υπηρεσίες. Έτσι, σε μια *DDoS*, οι υπάλληλοι μιας επιχείρισης αδυνατούν να εργαστούν σωστά και πλήττεται η παραγωγικότητα της επιχείρισης.
- ***Οικονομική επιβάρυνση*:** Πολλοί οργανισμοί επενδύουν μεγάλα χρηματικά ποσά στην πρόληψη τέτοιων επιθέσεων (ειδικό λογισμικό, σύμβουλοι, εταιρείες που παρέχουν υπηρεσίες ασφάλειας έναντι σε επιθέσεις *DDoS*).
- ***Αποζημιώσεις σε πελάτες*:** Οι επιχειρήσεις υπογράφουν με τους πελάτες τους *Συμφωνίες Εγγύησης Επιπέδου Υπηρεσιών* (*Service Level Agreements*, *SLA*s) που οφείλουν να τηρούν. Σε μια επίθεση *DDoS* παραβιάζουν τις εγγυήσεις τους και οι πελάτες τους μπορεί να απαιτήσουν αποζημιώσεις.
- ***Πλήγμα στην εικόνα της επιχείρισης*:** Η αδυναμία της επιχείρισης να εγγυηθεί τις υπηρεσίες της οδηγεί στην απώλεια της εμπιστοσύνης των πελατών τους.

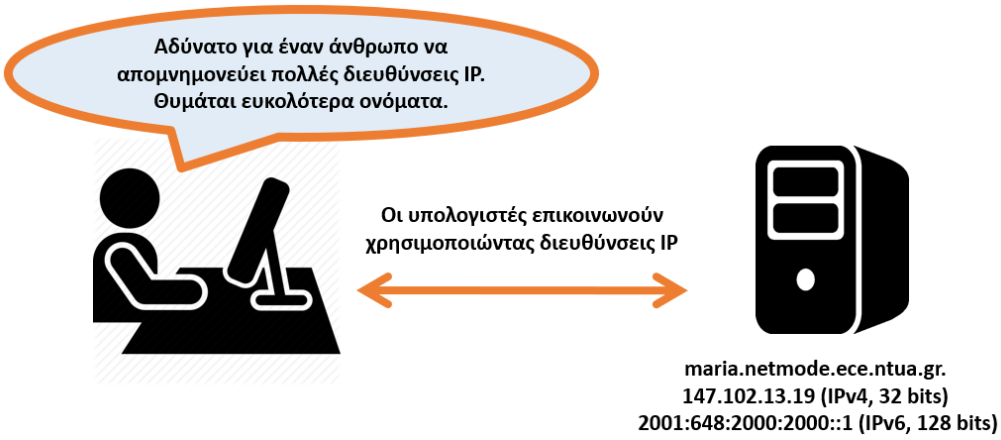
Τα κίνητρα τέτοιων επιθέσεων μπορεί να αναζητηθούν στους παρακάτω σκοπούς:

- ***Ακτιβισμός* (*hacktivism*):** Ακτιβιστές του διαδικτύου μπορούν να χρησιμοποιήσουν τις επιθέσεις *DDoS* ως μέσο για να διαμαρτυρηθούν για κάποιο κοινωνικό ή πολιτικό ζήτημα.
- ***Πνευματική πρόκληση*:** Ο επιτιθέμενος εκτελεί επιθέσεις για να πειραματιστεί και να αποκτήσει εμπειρία ή για να γίνει το επίκεντρο της προσοχής, κερδίζοντας έτσι φήμη στην κοινότητα των ανθρώπων που επιδίδονται σε επιθέσεις *DDoS*.
- ***Οικονομική ζημιά*:** Ο επιτιθέμενος θέλει να προκαλέσει οικονομική ζημιά σε μια επιχείρηση και εξαπολύει επίθεση *DDoS* εναντίον της.
- ***Ηλεκτρονικός πόλεμος* (*cyberwarfare*):** Κατά τη διάρκεια ενός πολέμου, μία χώρα μπορεί να εξαπολύσει επίθεση *DDoS* εναντίον μιας αντίπαλης χώρας για να παραλύσει βασικές υπηρεσίες της.
- ***Αντιπερισπασμός*:** μία επίθεση *DDoS* μπορεί να χρησιμοποιηθεί για να τραβήξει την προσοχή μακριά από κάποια άλλη κακόβουλη δραστηριότητα.

3. Το Domain Name System (DNS)

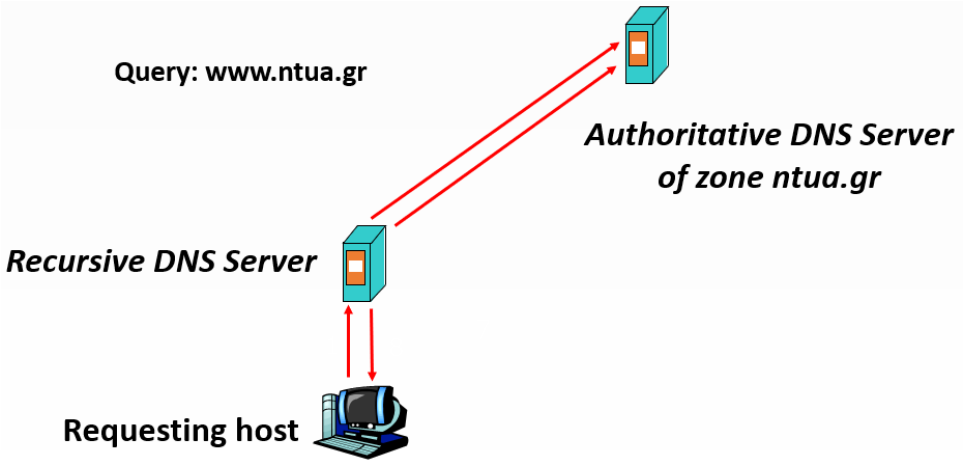
Το *DNS* αποτελεί, ουσιαστικά, την υπηρεσία καταλόγου του δημοσίου διαδικτύου. Όπως ακριβώς, ένας τηλεφωνικός κατάλογος αντιστοιχίζει ονόματα ανθρώπων και τηλεφωνικούς αριθμούς, έτσι και το *DNS* είναι υπεύθυνο για την αντιστοίχιση *ονομάτων υπολογιστών* (*hostnames*) σε *διευθύνσεις IP* (*IP addresses*) και αντίστροφα.

Οποιαδήποτε βλάβη ή απρόσεχτη ρύθμιση στο *DNS* είναι ικανή να παρεμποδίσει την πρόσβαση μεγάλου αριθμού χρηστών στο διαδίκτυο, επιφέροντας σημαντικές ζημιές είτε σε οικονομικό επίπεδο είτε στην αξιοπιστία των διαχειριστών των δικτύων.



Εικόνα 3. Το *DNS*

Στο *DNS*, οι εξυπηρετητές που περιλαμβάνουν τις ακριβείς αντιστοιχήσεις ονομάτων και *διευθύνσεων IP* ονομάζονται *Αρμόδιοι Εξυπηρετητές DNS* (*Authoritative DNS Servers*). Την εύρεση του κατάλληλου *Authoritative DNS Server* πραγματοποιούν οι *Αναδρομικοί Εξυπηρετητές DNS* (*Recursive DNS Servers*), οι οποίοι αναλαμβάνουν να αναζητήσουν τις απαντήσεις σε ερωτήματα χρηστών.



Εικόνα 4. *Recursive & Authoritative DNS Servers*

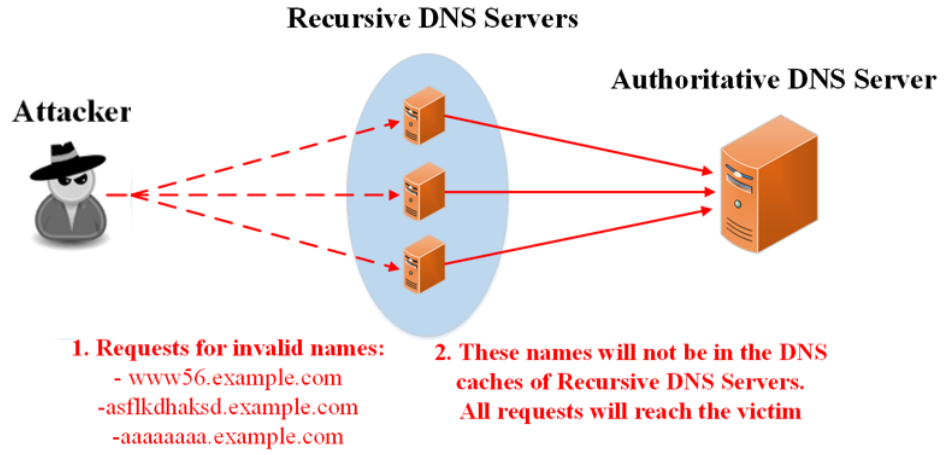
Η διαδικασία αναζήτησης της αντιστοίχισης ενός ονόματος υπολογιστή σε μία *διεύθυνση IP* έχει σημαντική καθυστέρηση και είναι σημαντικό να επαναλαμβάνεται όσο το δυνατόν λιγότερες φορές. Έτσι, είναι επιθυμητό, εάν χρειαστεί ξανά η εγγραφή αυτή σε σύντομο χρονικό διάστημα, νη μην επαναληφθεί η χρονοβόρα διαδικασία αναζήτησής της. Για να καταστεί δυνατό αυτό, ο *Recursive DNS Server* αποθηκεύει τις απαντήσεις στις αναζητήσεις που πραγματοποιεί σε μια *προσωρινή μνήμη* (*DNS cache*) για χρονικό διάστημα που καθορίζεται από μία παράμετρο, η οποία ονομάζεται *Time To Live* (*TTL*). Η τεχνική αυτή ονομάζεται *DNS caching*.

4. DNS Water Torture Attack

Η *DNS Water Torture attack* στοχεύει στην εξάντληση της επεξεργαστικής ισχύος ενός *Authoritative DNS Server*. Ο επιτιθέμενος διατυπώνει έναν πολύ μεγάλο αριθμό από ερωτήματα *DNS* με ονόματα τυχαίας μορφής προς τους διαθέσιμους *Recursive DNS Servers*. Οι *Recursive DNS Servers* προωθούν τα ερωτήματα αυτά στον *Authoritative DNS Server*.

Η δύναμη της επίθεσης εντοπίζεται στο γεγονός ότι όλη η κίνηση του επιτιθέμενου θα καταλήξει στο θύμα, καθώς η τυχαία μορφή των ονομάτων των ερωτημάτων εξασφαλίζει ότι αυτά τα ονόματα δε θα βρίσκονται αποθηκευμένα στην *προσωρινή μνήμη* (*DNS cache*) των *Recursive DNS Servers*. Έτσι, ο επιτιθέμενος μπορεί να στείλει πολύ μεγάλο όγκο κίνησης στο θύμα και να σπαταλήσει πλήρως την επεξεργαστική ισχύ του.

Επειδή τα ονόματα που επιλέγονται στην *DNS Water Torture* παράγονται με τυχαίο τρόπο χαρακτηρίζονται από μεγάλο μήκος, μεγάλος πλήθος συμφώνων και αριθμητικών χαρακτήρων, καθώς και από πολλά συνεχόμενα σύμφωνα. Στα χαρακτηριστικά αυτά βασίζονται οι μηχανισμοί άμυνας σε τέτοιες επιθέσεις.



Εικόνα 5. Επίθεση *DNS Water Torture*

5. Σχετικές με την άσκηση πηγές

- Y. Takeuchi, T. Yoshida, R. Kobayashi, M. Kato and H. Kishimoto, Detection of the DNS Water Torture Attack by Analyzing Features of the Subdomain Names, in Journal of Information Processing, Volume 24, Issue 5, 2016, pp. 793-801
- N. Kostopoulos, A. Pavlidis, M. Dimolianis, D. Kalogeras and Vasilis Maglaris, A Privacy-Preserving Schema for the Detection and Collaborative Mitigation of DNS Water Torture Attacks in Cloud Infrastructures, in the 8th International Conference on Cloud Networking (CloudNet), Coimbra, Portugal, November 2019, pp. 1-6
- Νίκος Κωστόπουλος, Διπλωματική, http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/13571/1/DT2017-0229.pdf