1 Αυγούστου 2017

Τι Είναι η Επίθεση DDoS Και Πώς Ρίχνει Μεγάλα Site

/ Επιστήμες, Τέχνες & Πολιτισμός / Πολυμέσα - Multimedia

Αν κάποιο γνωστό διεθνές site που επισκέπτεστε δείχνει να δυσλειτουργεί ή να

έχει πέσει εντελώς για κάποιες ώρες, είναι πολύ πιθανό ο ένοχος να είναι μια επίθεση DDoS. Σύμφωνα με τη Verisign, 50 εκατομμύρια σχετικά κρούσματα καταγράφονται ετησίως, τα οποία καταφέρνουν να γονατίσουν ακόμα και τα μεγαλύτερα site. Δείτε τι είναι η επίθεση DDoS και τι την καθιστά τόσο επικίνδυνη.

Τι είναι η επίθεση DDos και DoS
Τα DDoS και DoS είναι συντομογραφίες της φράσης (Distributed) Denial of Service. Στα Ελληνικά μεταφράζεται ως "Κατανεμημένη Επίθεση Άρνησης Εξυπηρέτησης".

Μια επίθεση DDoS έχει σαν στόχο ένα σύστημα, συνήθως έναν server ή ένα ολόκληρο κέντρο δεδομένων (datacenter). Η επίθεση "βομβαρδίζει" το σύστημα με ένα τεράστιο όγκο δεδομένων από διαφορετικές πηγές.

Το σύστημα, στην προσπάθειά του να ανταποκριθεί, καταλήγει να εξαντλήσει τους πόρους του, όπως CPU, RAM, κτλ, με αποτέλεσμα να υπερφορτώνεται και στο τέλος να καταρρεύσει.

Μία "επίθεση DDoS" στην οποία έχουμε συμμετέχει άθελά μας
Για να το κάνουμε κατανοητό, ας δούμε ένα απλό παράδειγμα που έχουμε ζήσει οι περισσότεροι από εμάς.

Έχετε παρατηρήσει πως την Πρωτοχρονιά, με το που θα αλλάξει ο χρόνος, ή αμέσως μετά την Ανάσταση το Πάσχα, για μερικά λεπτά είναι δύσκολο να κάνουμε μια κλήση ή ακόμα και να στείλουμε sms με το κινητό?

Αυτό συμβαίνει γιατί υπερβολικά μεγάλος αριθμός συνδρομητών προσπαθεί να χρησιμοποιήσει το δίκτυο ταυτόχρονα. Το ίδιο ισχύει και σε περιπτώσεις μια εκτεταμένης φυσικής καταστροφής, όπως πχ σε ένα σεισμό.

Σε κανονικές συνθήκες, μόνο ένα ποσοστό των χρηστών χρειάζεται ταυτόχρονα πρόσβαση στο δίκτυο ανά πάσα στιγμή.

Έτσι, σχεδόν κανένα μεγάλο δίκτυο, είτε πρόκειται για δίκτυο κινητής τηλεφωνίας ή για ιστοσελίδα, δεν είναι σχεδιασμένο ώστε να υποστηρίξει όλους τους χρήστες ταυτόχρονα. Θα ήταν τεράστια σπατάλη πόρων.

Μια κακόβουλη υπερφόρτωση
Κάτι αντίστοιχο συμβαίνει σε μια επίθεση DDoS/DoS, αν και για εντελώς διαφορετικά αίτια. Σε αυτή την περίπτωση, δεν είναι πραγματικοί χρήστες που μπλοκάρουν ένα δίκτυο ή ένα server. Πρόκειται για αυτοματοποιημένες ενέργειες μέσω software.

Οι ενέργειες αυτές δεν έχουν σκοπό να αξιοποιήσουν τον server, αλλά να τον

μπλοκάρουν. Έτσι, εμποδίζουν τους πραγματικούς χρήστες από το να έχουν πρόσβαση στο δίκτυο.

Μάλιστα, επειδή οι ενέργειες έχουν σκοπό να μπλοκάρουν, χρησιμοποιούν μεγαλύτερο όγκο δεδομένων σε σχέση με έναν απλό χρήστη.

Ένας υπολογιστής που συμμετέχει σε μια επίθεση DDoS μπορεί να προξενεί επιβάρυνση ίση με εκατοντάδες ή χιλιάδες κανονικούς χρήστες.

Οι επιθέσεις DDoS και DoS αναφέρονται ουσιαστικά στο ίδιο πράγμα, με μοναδική διαφορά την κλίμακα.

Η επίθεση DoS είναι ένα μικρής κλίμακας κρούσμα, συνήθως από ένα σύστημα-θύτη προς ένα σύστημα-θύμα.

Στις DDoS επιθέσεις η κλίμακα είναι σαφώς μεγαλύτερη, αφού βασίζονται μέχρι και σε εκατοντάδες χιλιάδες συσκευές. Αρκετά μεγάλες επιθέσεις DDoS και μπορούν να ρίξουν ολόκληρα κέντρα δεδομένων με πολλαπλούς server.

Μια σύντομη ιστορία

Οι πρώτες DoS επιθέσεις παρατηρήθηκαν κατά τη δεκαετία του ’90 και εκμεταλλεύονταν απλώς bugs και αδυναμίες λογισμικού. Είχαν στόχο να βγάλουν εκτός λειτουργίας μεμονωμένους server και υπηρεσίες.

Τα τελευταία 20 χρόνια, αυτού του είδους οι ενέργειες έχουν εξελιχθεί σε σημαντικό βαθμό. Σε αυτό βοήθησαν προηγμένα εργαλεία δικτύωσης, καθώς και το μειωμένο κόστος υπηρεσιών που μπορούν να χρησιμοποιηθούν σε μια επίθεση DDoS.

Θύματα τέτοιων επιθέσεων έχουν πέσει μεγάλες εταιρείες, από τις αρχές του 2000 μέχρι και σήμερα, όπως CNN, Amazon, Yahoo, eBay, Sony, Facebook, Twitter, ακόμα και το site του FBI, μεταξύ άλλων.

Ιστορικά, η μεγαλύτερη επίθεση DDoS που έχει καταγραφεί μέχρι στιγμής, έγινε στις 21 Οκτωβρίου 2016.

Θύμα ήταν η εταιρία Dyn, η οποία ελέγχει το μεγαλύτερο μέρος των υποδομών DNS (Domain Name System) του διαδικτύου. Το κρούσμα αυτό είχε επίπτωση σε αμέτρητες ιστοσελίδες διεθνώς, οι οποίες βασίζονταν στους DNS servers της Dyn.

Ο όγκος δεδομένων που κατάφεραν να γονατίσουν τους server πιθανόν να ξεπέρασε τα 1,2Tbps (Terabit per second, τρισεκατομμύρια bit ανά δευτερόλεπτο).

Αυτό το μέγεθος ήταν εφικτό με τη χρήση ενός botnet με το όνομα Mirai.

Botnet: το κυριότερο όπλο για την εξαπόλυση μιας επίθεσης DDoS

Όσο κι αν ακούγεται περίεργο, μια επίθεση DDoS λειτουργεί με την ίδια βασική αρχή όπως η φορολογία και η φιλανθρωπία.

Τι είναι πιο εύκολο? Ένας άνθρωπος να δωρίσει 1.000.000 ευρώ, ή 1.000.000 άνθρωποι να δώσουν από 1 ευρώ?

Αν κάποιοι θέλουν να επιτεθούν σε έναν μεγάλο server, δεν αρκεί να στέλνουν αιτήματα από πέντε ή δέκα υπολογιστές ταυτόχρονα. Χρειάζονται χιλιάδες ή και εκατοντάδες χιλιάδες υπολογιστές. Στις μέρες μας, αυτό είναι εφικτό με τη χρήση ενός botnet.

Η λογική του botnet είναι απλή. Πρώτα, ένα κακόβουλο λογισμικό τύπου trojan μολύνει έναν αριθμό από υπολογιστές. Το trojan μπορεί να προέρχεται από μολυσμένα συνημμένα στο email, σπασμένα προγράμματα, μολυσμένες ιστοσελίδες, ή από οπουδήποτε αλλού.

Όσο πιο πολλούς υπολογιστές καταφέρει να μολύνει το trojan, τόσο ισχυρότερο είναι το botnet.

Φυσικά, οι κάτοχοι των μολυσμένων υπολογιστών δεν γνωρίζουν πως το σύστημά τους είναι μολυσμένο. Τα trojan που χρησιμοποιούνται για το botnet αποφεύγουν να τραβήξουν την προσοχή, όπως πχ με το να δείχνουν διαφημίσεις ή να καταστρέφουν δεδομένα.

Οι μολυσμένοι υπολογιστές ονομάζονται “zombie”, καθώς το trojan μπορεί να πάρει τον πλήρη έλεγχο του υπολογιστή, όταν χρειαστεί.

Αξίζει να σημειωθεί πως αυτοί που δημιουργούν το botnet και αυτοί που το χρησιμοποιούν δεν είναι απαραίτητα τα ίδια άτομα.

Συχνά μια ομάδα hackers έχει δημιουργήσει ένα botnet και στη συνέχεια νοικιάζει τη χρήση του σε τρίτους.

Από εκεί και πέρα, το botnet μπορεί να κάνει ό,τι θέλει αυτός που το χρησιμοποιεί. Μπορεί να βάλει κάθε υπολογιστή να στέλνει μερικά spam emails, ώστε συνολικά να στέλνονται δεκάδες εκατομμύρια διαφημιστικά μηνύματα από το δίκτυο.

Φυσικά τα botnet δεν περιορίζονται μόνο σε email, μπορούν να στείλουν μηνύματα στο Facebook ή το Twitter, σχόλια σε ιστοσελίδες, ή ότι άλλο χρειάζεται.

Και, για να επανέλθουμε και στο θέμα μας, οι υπολογιστές του botnet μπορούν να εξαπολύσουν μια επίθεση DDoS.

Ειδικά στην επίθεση προς τη Dyn, το botnet Mirai είχε μια καινοτομία. Αντί να μολύνει υπολογιστές, εκμεταλλεύτηκε κενά ασφαλείας σε συσκευές τύπου "Internet of Things".

Οι συσκευές Internet of Things (IoT) είναι κάμερες, θερμοστάτες, μέχρι και ψυγεία που έχουν πρόσβαση στο ίντερνετ.

Το Mirai φέρεται να πήρε τον έλεγχο σε περισσότερες από 150.000 τέτοιες συσκευές και να τις χρησιμοποίησε για την επίθεση.

Για να καταλάβετε τι συμβαίνει σε πραγματικό χρόνο καθ' όλη τη διάρκεια μιας επίθεσης DDoS, δείτε το παρακάτω βίντεο.

Αποτελεί μια γραφική απεικόνιση της επίθεσης που έγινε το 2013 στους download server του VideoLAN, του οργανισμού που αναπτύσσει τον γνωστό Media Player VLC.

Οι χρωματιστές μπάλες αντιπροσωπεύουν τα requests που στέλνονται στον server, ενώ από την άλλη μεριά ο server προσπαθεί να αντεπεξέλθει στην κίνηση αυτή.

Τύποι DDoS επιθέσεων

Οι τύποι των επιθέσεων DDoS είναι πάρα πολλοί, kai δεν μπορούμε να τους αναλύσουμε όλους σε αυτόν τον οδηγό.

Όμως, αυτό που μπορούμε να κάνουμε, είναι να σας παρουσιάσουμε τους τέσσερις βασικότερους τύπους DDoS επιθέσεων, στους οποίους βασίζονται και πολλαπλά άλλα είδη επιθέσεων..

Παρακάτω χρησιμοποιούνται όροι όπως τριπλή χειραψία (SYN, SYN-ACK, ACK), TCP, ICMP κτλ, τους οποίους δε θα αναλύσουμε, αφού για να γίνουν κατανοητοί χρειάζονται ξεχωριστό οδηγό.

SYN Flood (Κατακλυσμός SYN)

Αυτός ο τύπος επίθεσης στηρίζεται στις βασικές αρχές της λειτουργίας επικοινωνίας δικτύου. Πολυάριθμα αιτήματα σύνδεσης TCP /SYN αποστέλλονται στον server με τέτοιο ρυθμό, που δεν μπορεί να αντιμετωπίσει την επεξεργασία

όλων αυτών.

Ο server, κατά την παραλαβή του πακέτου, δημιουργεί μια σύνδεση για να επικοινωνήσει με τον πελάτη και περιμένει επιβεβαίωση.

Οι επιθέσεις τύπου SYN Flood καταχρώνται αυτόν τον μηχανισμό, και δε στέλνουν ποτέ την επιβεβαίωση που περιμένει ο server.

Με αυτόν τον τρόπο, όλες οι νέες συνδέσεις μειώνονται και οι νόμιμοι χρήστες ουσιαστικά αποκόβονται από την πρόσβαση στον server.

Connection Flood (Κατακλυσμός Συνδέσεων)
Εδώ δημιουργείται ένας τεράστιος αριθμός από κενές συνδέσεις στον server. Ουσιαστικά αποστέλλονται τα πακέτα που χρειάζονται μόνο για την ίδρυση της τριπλής χειραψίας (SYN,SYN-ACK,ACK), χωρίς την μεταφορά των δεδομένων.

Στόχος είναι να δημιουργηθεί ένας μεγάλος αριθμός από πραγματικές συνδέσεις, που προέρχονται από πραγματικές IP, καταβροχθίζοντας τη χωρητικότητα ανεκτέλεστων συνδέσεων στον στοχευμένο server.

UDP Flood (Κατακλυσμός UDP)
Σκοπός αυτής της επίθεσης είναι να εξαντλήσει το bandwidth ή αλλιώς το εύρος ζώνης. Για να το κάνει αυτό, χρησιμοποιεί το πρωτόκολλο δικτύωσης UDP (User Datagram Protocol), μέσω του οποίου στέλνει έναν μεγάλο αριθμό πακέτων.

Συνήθως, τα πακέτα αυτά στέλνονται από διευθύνσεις IP με πλασταγραφημένη πηγή. Έτσι, το bandwidth των συνδέσεων μειώνεται, καθιστώντας τον server μη προσβάσιμο για τους χρήστες.

HTTP Flood (Κατακλυσμός HTTP)
Οι HTTP επιθέσεις έχουν στόχο να υπερφορτώσουν τον server, και τελικώς να εξαντλήσουν τους υλικούς πόρους (hardware) που έχει διαθέσιμους.

Μερικές φορές οδηγούν σε φυσική καταστροφή του υλικού του εξυπηρετητή, λόγω της αδυναμίας αντιμετώπισης της υπερφόρτωσης της CPU και της μνήμης RAM.

Γιατί οι επιθέσεις DDoS είναι τόσο δημοφιλείς?
Μια επίθεση DDoS είναι ταυτόχρονα “εύκολη” και εξαιρετικά αποτελεσματική. Όπως προαναφέραμε, υπάρχουν έτοιμα botnet για όποιον θέλει να μισθώσει τη χρήση τους. Θα βρούμε τέτοιες υπηρεσίες στο Deep Web.

Αυτό σημαίνει πως δεν χρειάζεται κάποιος να είναι ταλαντούχος hacker ή ακόμα και να έχει οποιαδήποτε ειδική γνώση γύρω από τα δίκτυα.

Θεωρητικά, μπορεί κανείς να μισθώσει ένα έτοιμο botnet και μια επίθεση DDoS σαν υπηρεσία, με κόστος που υπολογίζεται σε λίγες χιλιάδες δολάρια.

Βέβαια, το κόστος εξαρτάται από το μέγεθος του botnet, και το απαιτούμενο μέγεθος εξαρτάται από τον στόχο της επίθεσης DDoS.

Ένα botnet 50.000 συσκευών δεν πρόκειται να ρίξει πχ το Facebook, που οι server του μπορούν να ανταπεξέλθουν σε πάνω από 1 δισεκατομμύριο χρήστες online ταυτόχρονα.

Με ένα αρκετά μεγάλο botnet, όμως, και με δεδομένο πως κάθε συσκευή δημιουργεί πολλαπλάσια επιβάρυνση από ένα μεμονωμένο χρήστη, ακόμα και οι μεγαλύτερες ιστοσελίδες μπορούν να γονατίσουν για ένα διάστημα.

Επίσης, οι επιθέσεις αυτές είναι ένας εύκολος τρόπος για να δείξουν οι επιτιθέμενοι τον θυμό και την αποδοκιμασία τους πάνω σε ένα θέμα.

Πολλές φορές χρησιμοποιούν την επίθεση DDoS ως έναν τρόπο για να επικρίνουν πχ την εταιρεία ή την κυβερνητική οργάνωση για την εμφάνιση ανεπιθύμητων πολιτικών ή γεωπολιτικών, οικονομικών ή νομισματικών συμπεριφορών.

Πώς προστατεύονται οι μεγάλες επιχειρήσεις από αυτές τις επιθέσεις

Μια επίθεση DDoS μπορεί να προκαλέσει σημαντικά προβλήματα σε μια εταιρεία. Αυτά είναι κυρίως οικονομικά, καθώς το site τους παύει να λειτουργεί για όσο διαρκεί η επίθεση. Επίσης, το να μην λειτουργεί μια ιστοσελίδα είναι πλήγμα στην αξιοπιστία της.

Γι’ αυτόν τον λόγο, η κάθε εταιρεία πρέπει να λαμβάνει κάποια μέτρα για να προφυλάσσεται από αυτές τις επιθέσεις.

Ο επικρατέστερος τρόπος προστασίας είναι με τη χρήση ειδικευμένων προϊόντων περιμετρικής ασφάλειας δικτύων και δικτυακών εφαρμογών.

Πρόκειται για συστήματα που παρεμβάλλονται μεταξύ των επισκεπτών και των ψηφιακών υπηρεσιών που προσφέρουν οι εταιρείες. Αυτά τα προϊόντα διαθέτουν μηχανισμούς αποτροπής και εντοπισμού για μια επίθεση DDoS, καθώς και αντίμετρα.

Έτσι, μπορούν να διακρίνουν πότε η χρήση της ψηφιακής υπηρεσίας είναι

φυσιολογική και πότε κακόβουλη, εμποδίζοντας τη δεύτερη χωρίς να διαταράσσουν την πρώτη.

Προφανώς κανένα σύστημα προστασίας δεν μπορεί να αποτρέψει κάθε επίθεση ανεξαιρέτως.

Όπως και σε οποιονδήποτε άλλο τομέα που αφορά την ηλεκτρονική ασφάλεια, οι κακόβουλοι χρήστες και οι ερευνητές ασφαλείας εργάζονται ακατάπαυστα, βελτιώνοντας τις αντίστοιχες μεθόδους τους.

Δείτε ζωντανά τις κυριότερες επιθέσεις DDoS αυτή τη στιγμή
Η σελίδα Digital Attack Map παρακολουθεί καθημερινά τις σημαντικότερες επιθέσεις DDoS διεθνώς.

Στις 17 Ιουλίου, που τραβήξαμε το παραπάνω στιγμιότυπο, η πιο σοβαρή επίθεση DDoS ήταν στη Βραζιλία.

Βέβαια, ρίχνοντας μια ματιά στα πιο σημαντικά πρόσφατα κρούσματα…

…βλέπουμε πως η εικόνα κατά τη διάρκεια μιας πραγματικά μεγάλης επίθεσης είναι αρκετά διαφορετική.

Εσείς τι πιστεύετε για την επίθεση DoS/DDoS?
Όπως είναι εμφανές, οι επιθέσεις DDoS είναι ένα αρκετά συχνό φαινόμενο, και συχνά κινούνται από οικονομικά ή και πολιτικά συμφέροντα.

Πηγή: pcsteps.gr