Έρευνα αποκαλύπτει τις τακτικές των χάκερς: Ψηφιακοί εγκληματίες χρησιμοποιούν τις επιθέσεις DDoS ως προπέτασμα καπνού για άλλες επιθέσεις εναντίον επιχειρήσεων

Οι Κατανεμημένες Επιθέσεις Άρνησης Εξυπηρέτησης (Distributed Denial of Service – DDoS) χρησιμοποιούνται μερικές φορές από εγκληματίες του κυβερνοχώρου για να αποσπάσουν την προσοχή των επιχειρήσεων, ενώ παράλληλα οι χάκερς τρυπώνουν κρυφά από την «πίσω πόρτα», όπως έδειξε σχετική έρευνα της Kaspersky Lab και της B2B International. Περισσότερες από τις μισές επιχειρήσεις που ερωτήθηκαν (56%) είναι πεπεισμένες ότι οι DDoS έχουν χρησιμοποιηθεί ως προπέτασμα καπνού για άλλα είδη ψηφιακών εγκλημάτων, ενώ από τις επιχειρήσεις που απάντησαν, η μεγάλη πλειοψηφία (87%) ανέφερε ότι είχε πέσει επίσης θύμα μιας στοχευμένης επίθεσης.

Η Έρευνα Kaspersky Lab IT Security Risks 2016 έδειξε ότι σε αρκετές επιχειρήσεις που έχουν πέσει θύμα ψηφιακής εγκληματικότητας οι DDoS έχουν υπάρξει μέρος των τακτικών της επίθεσης (29%). Για παράδειγμα, ένα ανησυχητικό 26% των επιχειρήσεων που έχουν υποστεί απώλεια δεδομένων, ως αποτέλεσμα μιας στοχευμένης επίθεσης, υπέδειξε τις DDoS ως έναν από τους συμβάλλοντες φορείς. Συνολικά, το 56% των

εκπροσώπων των επιχειρήσεων που συμμετείχαν στην έρευνα πίστευαν ότι οι επιθέσεις DDoS που είχαν υποστεί οι εταιρείες τους ήταν προπέτασμα καπνού ή δόλωμα για άλλες εγκληματικές δραστηριότητες.

Ο Kirill Ilganaev, επικεφαλής του τμήματος Kaspersky DDoS Protection, εξήγησε γιατί οι επιθέσεις DDoS μπορεί να χρησιμοποιούνται από τους ψηφιακούς εγκληματίες ως μέρος της τακτικής τους. *«Οι επιθέσεις DDoS εμποδίζουν μια εταιρεία από την άσκηση των συνηθισμένων δραστηριοτήτων της θέτοντας είτε δημόσιες είτε εσωτερικές υπηρεσίες σε κατάσταση αναμονής. Αυτό είναι προφανώς ένα πραγματικό πρόβλημα για τις επιχειρήσεις και συχνά εργάζεται όλη η ομάδα του τμήματος Πληροφορικής με στόχο να επιδιορθωθεί το όποιο πρόβλημα. Οι επιθέσεις DDoS μπορεί επομένως να χρησιμοποιηθούν όχι μόνο ως ένας εύκολος τρόπος για να σταματήσει η δραστηριότητα μιας εταιρείας, αλλά και ως δόλωμα προκειμένου να αποσπάσουν την προσοχή του IT προσωπικού από μια άλλη εισβολή που λαμβάνει χώρα μέσω άλλων διαύλων».*

Η έρευνα διαπίστωσε ότι όταν οι επιθέσεις DDoS έχουν χρησιμοποιηθεί από ψηφιακούς εγκληματίες ως προπέτασμα καπνού, οι επιχειρήσεις αντιμετώπισαν ταυτόχρονα άλλες απειλές, όπως ζημίες και exploits μέσω φορητών συσκευών (81%), μέσω ενεργειών άλλων οργανισμών (78%), phishing απάτης (75%), ή ακόμη και κακόβουλης δραστηριότητας εναντίον του προσωπικού της εταιρείας (75%). Η πλειοψηφία (87%) είχε πέσει επίσης θύμα στοχευμένων επιθέσεων.

Όπως αναφέρει ο κος. Ilganaev, *«Η έρευνα μας δείχνει ότι οι επιθέσεις DDoS είναι συχνά ευθυγραμμισμένες με άλλες απειλές. Ως εκ τούτου, οι επιχειρήσεις πρέπει να γνωρίζουν το πλήρες τοπίο των απειλών και να έτοιμες να αντιμετωπίσουν πολλαπλές μορφές εγκληματικής δραστηριότητας ανά πάσα στιγμή. Σε αντίθετη περίπτωση, αυτό θα μπορούσε να αυξήσει τις παράπλευρες απώλειες, επιπλέον από τις ήδη σημαντικές απώλειες που προκλήθηκαν από το χρόνο διακοπής και τις επακόλουθες επιπτώσεις στη φήμη. Οι επιχειρήσεις πρέπει να χρησιμοποιούν*

μια αξιόπιστη υπηρεσία προστασίας από επιθέσεις DDoS για να μειώσουν τον σχετικό κίνδυνο και για να βοηθήσουν το προσωπικό να επικεντρώνει τις προσπάθειές του στην προστασία της επιχείρησης από τυχόν απειλές που μπορεί να κρύβονται ως αποτέλεσμα».

Για να βοηθήσει τις επιχειρήσεις να διατηρήσουν τον έλεγχο επάνω στην αυξανόμενη απειλή που αποτελούν οι επιθέσεις DDoS και όλα αυτά που φέρνουν μαζί τους, η λύση Kaspersky DDoS Protection παρέχει πλήρη και ολοκληρωμένη προστασία, για την υπεράσπιση των επιχειρήσεων σε κάθε στάδιο μιας απόπειρας επίθεσης.

* Η Έρευνα Corporate IT Security Risks πραγματοποιείται ετησίως από την Kaspersky Lab σε συνεργασία με την B2B International. Το 2016, περισσότεροι από 4.000 εκπρόσωποι μικρών, μεσαίων (50-999) και μεγάλων επιχειρήσεων (1000+) από 25 χώρες κλήθηκαν να εκφράσουν τις απόψεις τους σχετικά με την ασφάλεια του τομέα της Πληροφορικής και πραγματικά περιστατικά που κλήθηκαν να αντιμετωπίσουν.