Έκθεση της Kaspersky Lab για τις επιθέσεις DDoS το πρώτο τρίμηνο του 2017: Η ηρεμία πριν την καταιγίδα

Το πρώτο τρίμηνο του 2017 επιβεβαιώθηκαν οι προβλέψεις των ειδικών της Kaspersky Lab για την εξέλιξη των επιθέσεων DDoS, σε συνέχεια των αποτελεσμάτων του 2016. Αυτό απιδεικνύει επίσης ότι οι ψηφιακοί εγκληματίες χρειάζονται και εκείνοι ξεκούραση. Παρά την αυξημένη δημοτικότητα των σύνθετων επιθέσεων DDoS που συνεχίστηκαν το πρώτο τετράμηνο, υπήρξε μία αξιοσημείωτη πτώση στον αριθμό των γενικευμένων επιθέσεων και μια αλλαγή στο πως καταμερίζονται ανά χώρα.

Το πρώτο τρίμηνο του 2017, το σύστημα Kaspersky DDoS Intelligence κατέγραψε επιθέσεις DDoS ενάντιων πόρων σε 72 χώρες, ποσοστό το οποίο είναι οκτώ φορές μικρότερο σε σύγκριση με αυτό του τελευταίου τριμήνου του 2016. Η Ολλανδία και το Ηνωμένο Βασίλειο αντικατέστησαν την Ιαπωνία και τη Γαλλία στη λίστα με τις 10 χώρες που παρουσιάζουν τα περισσότερα θύματα επιθέσεων DDoS.

Η Νότια Κορέα παρέμεινε ηγέτης όσον αφορά στον αριθμό των ανιχνευθέντων C&C server. Οι Η.Π.Α ήρθαν δεύτερες σε αυτήν την κατηγορία, ακολουθούμενες από την Ολλανδία, η οποία εκτόπισε την Κίνα από την πρώτη τριάδα για πρώτη φόρα από τότε που ξεκίνησε αυτή η διαδικασία παρακολούθησης. Μάλιστα, η Κίνα έπεσε από τη δεύτερη στην έβδομη θέση. Η Ιαπωνία, η Ουκρανία και η Βουλγαρία δε βρίσκονται πλέον στην πρώτη δεκάδα των χωρών με το μεγαλύτερο αριθμό ανιχνευθέντων C&C server. Αντικαταστάθηκαν από το Χονγκ Κονγκ, τη Ρουμανία και τη Γερμανία.

Επίσης, άλλαξε και η κατανομή ανά λειτουργικό σύστημα το πρώτο τρίμηνο του 2017. Το προηγούμενο τρίμηνο, τα IoT botnets που βασίζονται σε Linux ήταν τα πιο διάσημα, αλλά ξεπεράστηκαν από τα botnets που βασίζονται σε Windows, των οποίων το μερίδιο αυξήθηκε από 25% σε 60% το πρώτο τρίμηνο. Ο αριθμός των TCP, UDP και ICMP επιθέσεων αυξήθηκε σημαντικά, ενώ το μερίδιο των επιθέσεων SYN DDoS και HTTP μειώθηκε από 75% – το τελευταίο τρίμηνο του 2016 – σε 48% το πρώτο τρίμηνο του 2017.

Κατά την περίοδο αναφοράς, δεν καταγράφηκε ούτε μία επίθεση ενισχυτικού τύπου, ενώ ο αριθμός των επιθέσεων που βασίζονται στην κρυπτογράφηση αυξήθηκε. Αυτό συμβαδίζει με τις προβλέψεις των τελευταίων ετών για μία μετατόπιση από τις σύνθετες επιθέσεις DDoS στις πιο απλές αλλά δυνατές επιθέσεις, που είναι δύσκολο να αναγνωριστούν από τα καθιερωμένα συστήματα ασφάλειας.

Συνολικά, το τρίμηνο ήταν σχετικά ήσυχο: ο μεγαλύτερος αριθμός επιθέσεων (994) παρατηρήθηκε στις 18 Φεβρουαρίου. Η μεγαλύτερη επίθεση DDoS στο πρώτο τρίμηνο του 2017 διήρκεσε μόλις 120 ώρες, σημαντικά λιγότερες από τις 292 ώρες του προηγούμενου τριμήνου.

«Υπάρχει συνήθως έντονη πτώση στον αριθμό των επιθέσεων DDoS στις αρχές του έτους, και αυτή η τάση συνεχίζεται εδώ και πέντε χρόνια. Αυτό μπορεί να οφείλεται στο γεγονός ότι οι ψηφιακοί εγκληματίες ή οι πελάτες τους μπορεί να αποφάσισαν να κάνουν ένα διάλειμμα. Ωστόσο, παρά την ήδη γνωστή κάμψη, καταγράψαμε ακόμα περισσότερες επιθέσεις μεταξύ Ιανουαρίου και Μαρτίου του τρέχοντος έτους σε σύγκριση με το πρώτο τρίμηνο του 2016, γεγονός που επιβεβαιώνει το συμπέρασμα ότι ο συνολικός αριθμός των επιθέσεων DDoS αυξάνεται. Τώρα λοιπόν δεν είναι η κατάλληλη στιγμή να χαλαρώσετε τις άμυνές σας. Μάλλον, είναι καλύτερο να φροντίζετε για την προστασία σας προτού οι ψηφιακοί εγκληματίες επιστρέψουν στη συνηθισμένη τους ρουτίνα», σχολιάζει ο Kirill Ilganaev, επικεφαλής του τμήματος Kaspersky DDoS Protection της Kaspersky Lab.

Η λύση Kaspersky DDoS Protection συνδυάζει την εκτεταμένη τεχνογνωσία της Kaspersky Lab για την καταπολέμηση των ψηφιακών απειλών με τις μοναδικές εξελίξεις που αναπτύχθηκαν στο εσωτερικό της εταιρείας. Η λύση προστατεύει από όλους τους τύπους επιθέσεων DDoS, ανεξάρτητα από την πολυπλοκότητα, τη δύναμη ή τη διάρκεια τους.

* Το σύστημα DDoS Intelligence (μέρος της λύσης Kaspersky DDoS Protection) σχεδιάστηκε για να παρακολουθεί και να αναλύει εντολές που αποστέλλονται σε bots από command and control (C&C) servers και δε χρειάζεται να περιμένει μέχρι να «μολυνθούν» οι συσκευές του χρήστη ή να εκτελεστούν οι εντολές του ψηφιακού εγκληματία για να συλλέξει δεδομένα. Είναι σημαντικό να σημειωθεί ότι τα στατιστικά στοιχεία του DDoS Intelligence περιορίζονται στα botnets που ανιχνεύονται και αναλύονται από την Kaspersky Lab.