Επεκτατικές, απαιτητικές και μεγαλύτερης διάρκειας: Η τριμηνιαία έκθεση της Kaspersky Lab για τις επιθέσεις DDoS

Το δεύτερο τρίμηνο του 2017 ήταν η απόδειξη ότι οι μακράς διάρκειας επιθέσεις DDoS ανέλαβαν ξανά δράση. Η μεγαλύτερη επίθεση του τριμήνου ήταν ενεργή για 277 ώρες (περισσότερο από 11 ημέρες) – μέγεθος αυξημένο κατά 131% σε σχέση με το πρώτο τρίμηνο. Αυτό αποτελεί μέχρι στιγμής μέγεθος ρεκόρ για το έτος, όπως αναφέρει η έκθεση των ειδικών της Kaspersky Lab σχετικά με τις botnet επιθέσεις DDoS για το δεύτερο τρίμηνο του 2017.

Η διάρκεια δεν ήταν το μοναδικό χαρακτηριστικό των επιθέσεων DDoS μεταξύ Απριλίου και Ιουνίου. Υπάρχει και μία δραματική αλλαγή στη γεωγραφία των περιστατικών, καθώς το δεύτερο τρίμηνο έχουν δεχτεί επίθεση οργανισμοί με ηλεκτρονικούς πόρους σε 86 χώρες (σε σύγκριση με 72 χώρες το πρώτο τρίμηνο). Οι 10 χώρες που δέχτηκαν τις περισσότερες επιθέσεις ήταν η Κίνα, η Νότια Κορέα, οι ΗΠΑ, το Χονγκ Κονγκ, το Ηνωμένο Βασίλειο, η Ιταλία, η Ολλανδία, ο Καναδάς και η Γαλλία – με την Ιταλία και την Ολλανδία να αντικαθιστούν το Βιετνάμ και τη Δανία.

Οι στόχοι των επιθέσεων DDoS περιλάμβαναν ένα από τα μεγαλύτερα πρακτορεία ειδήσεων, το Al Jazeera, τις ιστοσελίδες

των εφημερίδων Le Monde και Figaro και, σύμφωνα με ισχυρισμούς, τους servers του Skype. Κατά το δεύτερο τρίμηνο του 2017, η αύξηση στις αναλογίες των cryptocurrencies οδήγησε επίσης τους ψηφιακούς εγκληματίες να προσπαθούν να χειραγωγήσουν τις τιμές μέσω των DDoS. Η Bitfinex, το μεγαλύτερο ανταλλακτήριο συναλλαγών Bitcoin, δέχτηκε επίθεση ταυτόχρονα με την έναρξη των συναλλαγών με ένα νέο cryptocurrency, το επονομαζόμενο IOTA token. Νωρίτερα, το ανταλλακτήριο BTC-E ανέφερε επιβράδυνση λόγω ισχυρής επίθεσης DDoS.

Το ενδιαφέρον των διοργανωτών των επιθέσεων DDoS σε μετρητά υπερβαίνει τον χειρισμό των αναλογιών των cryptocurrencies. Η χρήση αυτού του τύπου επίθεσης για να αποσπούν χρήματα μπορεί να είναι επωφελής, όπως δείχνει και η τάση των Ransom DDoS ή RDoS. Οι ψηφιακοί εγκληματίες στέλνουν συνήθως ένα μήνυμα στο θύμα ζητώντας του λύτρα που κυμαίνονται από 5 έως 200 bitcoins. Εάν η εταιρεία αρνείται να πληρώσει, οι επιτιθέμενοι απειλούν να οργανώσουν μια επίθεση DDoS σε έναν κρίσιμο και σημαντικό διαδικτυακό πόρο του θύματος. Τέτοια μηνύματα μπορούν να συνοδεύονται από σύντομης διάρκειας επιθέσεις DDoS για να επιβεβαιώσουν ότι οι απειλές είναι όντως πραγματικές. Στα τέλη Ιουνίου, πραγματοποιήθηκε μια μακράς διάρκειας επίθεση RDoS από την ομάδα Armada Collective, η οποία απαίτησε περίπου 315.000 δολάρια από επτά τράπεζες της Νότιας Κορέας.

Ωστόσο, υπάρχει πάντα κι ένας άλλος τρόπος, ο οποίος έγινε πιο δημοφιλής το τελευταίο τρίμηνο – οι Ransom DDoS χωρίς καθόλου DDoS. Οι απατεώνες στέλνουν απειλητικά μηνύματα σε μεγάλο αριθμό εταιρειών με την ελπίδα ότι κάποιος θα αποφασίσει να είναι ασφαλής παρά να το μετανιώσει αργότερα. Οι επιδείξεις επιθέσεων μπορεί να μην συμβούν ποτέ, αλλά αν μόνο μία εταιρεία αποφασίσει να πληρώσει, αυτό θα φέρει στους ψηφιακούς εγκληματίες κέρδος με ελάχιστη προσπάθεια.

«Σήμερα, δεν είναι μόνο έμπειρες ομάδες hi-tech ψηφιακών εγκληματιών που μπορεί να επιτεθούν με Ransom DDoS. Κάθε απατεώνας που δεν διαθέτει ούτε τις τεχνικές γνώσεις ούτε την

ικανότητα να οργανώσει μια πλήρους κλίμακας επίθεση DDoS μπορεί να αγοράσει μια επίδειξη επίθεσης για σκοπούς εκβιασμού. Οι άνθρωποι αυτοί διαλέγουν ως επί το πλείστον εταιρείες που δεν προστατεύουν τους πόρους τους από τις DDoS με οποιονδήποτε τρόπο και, ως εκ τούτου, μπορούν εύκολα να πεισθούν να πληρώσουν λύτρα με μια απλή επίδειξη», σχολιάζει ο Kirill Ilganaev, Head of Kaspersky DDoS Protection της Kaspersky Lab.

Οι ειδικοί της Kaspersky Lab προειδοποιούν ότι αν μια εταιρεία-θύμα αποφασίσει να πληρώσει, μπορεί να προκαλέσει μακροπρόθεσμη ζημιά εκτός από τις άμεσες νομισματικές απώλειες. Η φήμη του «πληρωτή» εξαπλώνεται γρήγορα μέσω των δικτύων και μπορεί να προκαλέσει περαιτέρω επιθέσεις από άλλους ψηφιακούς εγκληματίες.

Η λύση Kaspersky DDoS Protection συνδυάζει την εκτεταμένη τεχνογνωσία της Kaspersky Lab στην 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 του Kaspersky DDoS Protection) σχεδιάστηκε για να παρακολουθεί και να αναλύει εντολές που αποστέλλονται σε bots από command and control servers (C & C) και δεν χρειάζεται να περιμένει μέχρι να «μολυνθούν» οι συσκευές του χρήστη ή μέχρι να εκτελεστούν οι εντολές συλλογής δεδομένων των ψηφιακών εγκληματιών. Είναι σημαντικό να σημειωθεί ότι τα στατιστικά στοιχεία του DDoS Intelligence περιορίζονται στα botnets που εντοπίστηκαν και αναλύθηκαν από την Kaspersky Lab.