Symantec: Οι συσκευές IoT χρησιμοποιούνται όλο και περισσότερο στις επιθέσεις DDoS

Στις συσκευές-στόχους IoT συμπεριλαμβάνονται οικιακά δίκτυα, routers, modems, συστήματα CCTV, καθώς και βιομηχανικά συστήματα ελέγχου.

Η Symantec, παγκόσμιος ηγέτης ασφάλειας στον κυβερνοχώρο, αποκαλύπτει με νέα έρευνα, που παρουσιάζει πως τα δίκτυα κυβερνοεγκληματιών, εκμεταλλεύονται την ελαστικότητα της ασφάλειας των συσκευών **Internet of Things (IoT)**, με σκοπό την εξάπλωση malware, αλλά και τη δημιουργία zombie networks ή botnets, εν αγνοία των ιδιοκτητών τους.

Η εξειδικευμένη ομάδα Security Response της Symantec, ανακάλυψε ότι οι κυβερνοεγκληματίες , εισβάλουν σε οικιακά δίκτυα, καθώς και σε συνδεδεμένες συσκευές που χρησιμοποιούν καθημερινά οι καταναλωτές, έτσι ώστε να διεξαχθούν επιθέσεις **distributed denial of service (DDoS)**, προς πιο αποδοτικούς για αυτούς στόχους, που συνήθως είναι μεγαλύτερες εταιρείες. Για να πετύχουν το σκοπό τους, χρειάζονται φθηνό bandwidth και το επιτυγχάνουν με τη συρραφή μεταξύ τους, ενός μεγάλου εύρους καταναλωτικών συσκευών, οι οποίες είναι εύκολο να μολυνθούν αφού στερούνται εξελιγμένης ασφάλειας.

Να σημειώσουμε ότι πάνω από το μισό των συνολικών επιθέσεων IoT, προέρχονται από την Κίνα και τις Η.Π.Α. , βάσει της τοποθεσίας των διευθύνσεων των IP οι οποίες «δείχνουν» την αφετηρία των επιθέσεων malware. Επίσης, ένας μεγάλος αριθμός επιθέσεων προέρχεται από τη Γερμανία, την Ολλανδία, τη Ρωσία, την Ουκρανία και το Βιετνάμ. Σε κάποιες περιπτώσεις, οι διευθύνσεις IP χρησιμοποιούνται μέσω proxies, έτσι ώστε οι επιτιθέμενοι να κρύβουν την πραγματική τους τοποθεσία.

Οι περισσότερες επιθέσεις IoT malware, στοχεύουν σε μη προσωπικής χρήσης συσκευές, όπως servers, routers, modems, συσκευές δικτυακής αποθήκευσης (NAS), συστήματα τηλεοράσεων κλειστού κυκλώματος (CCTV), καθώς και βιομηχανικά συστήματα ελέγχου. Πολλά από τα συστήματα αυτά μπορεί να έχουν πρόσβαση στο Internet, αλλά λόγω του λειτουργικού συστήματος και της περιορισμένης ισχύος επεξεργασίας, μπορεί να μη διαθέτουν προηγμένα χαρακτηριστικά ασφάλειας.

Καθώς οι επιτιθέμενοι έχουν πλήρη επίγνωση της ανεπαρκής ασφάλειας του IoT, πολλοί από αυτούς προγραμματίζουν εκ των προτέρων τα malware που δημιουργούν, συμπεριλαμβάνοντας σε αυτά κοινώς χρησιμοποιούμενους κωδικούς πρόσβασης, που επιτρέπουν εύκολα την εισβολή σε αυτές τις συσκευές. Το χαμηλό επίπεδο ασφάλειας σε πολλές συσκευές IoT, τις καθιστούν εύκολους στόχους με τα θύματα συνήθως να μην γνωρίζουν καν ότι έχουν προσβληθεί.

Πρόσθετα ευρήματα από την έρευνα της Symantec περιλαμβάνουν τα εξής:

- Το 2015 ήταν μια χρονιά-ρεκόρ για τις επιθέσεις IoT, με πληθώρα υποθέσεων σε συσκευές οικιακού αυτοματισμού και οικιακών συσκευών ασφαλείας. Ωστόσο, οι επιθέσεις μέχρι σήμερα έχουν δείξει ότι οι επιτιθέμενοι έχουν την τάση να ενδιαφέρονται λιγότερο για το θύμα και η πλειοψηφία να εστιάζει στη συσκευή αυτή καθ αυτή προκειμένου να την προσθέσει σε ένα από τα botnets, τα περισσότερα από τα οποία χρησιμοποιούνται για την εκτέλεση επιθέσεων DDoS.

- Οι συσκευές IoT είναι ο πρωταρχικός στόχος, δεδομένου ότι έχουν σχεδιαστεί έτσι ώστε να συνδέονται και να «ξεχνιούνται» μετά το βασικό set-up.
- Οι πιο συνηθισμένοι κωδικοί πρόσβασης IoT κακόβουλου λογισμικού, χρησιμοποιούνται για να προσπαθήσουν να συνδεθούν σε συσκευές και όπως ήταν αναμενόμενο, ο συνδυασμός είναι «root» και «admin», υποδεικνύοντας ότι οι προεπιλεγμένοι κωδικοί πρόσβασης συχνά δεν αλλάζουν ποτέ!
- Επιθέσεις που προέρχονται από πολλαπλές πλατφόρμες IoT θα τις βλέπουμε πιο συχνά στο μέλλον, καθώς ο αριθμός των ενσωματωμένων συσκευών που συνδέονται στο Internet αυξάνει συνεχώς.

Περισσότερες πληροφορίες σχετικά με την έρευνα της Symantec για το IoT θα βρείτε στο: http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks