Υπερδιπλασιάστηκε το κακόβουλο λογισμικό με στόχο «έξυπνες» συσκευές το 2017

Ο συνολικός αριθμός δειγμάτων κακόβουλου λογισμικού με στόχο «έξυπνες» συσκευές έχει ξεπεράσει τις 7.000, με περισσότερα από τα μισά δείγματα να κάνουν την εμφάνισή τους το 2017 σύμφωνα με τους ερευνητές της Kaspersky Lab. Με περισσότερες από 6 δισεκατομμύρια «έξυπνες» συσκευές να χρησιμοποιούνται σε ολόκληρο τον κόσμο, οι άνθρωποι κινδυνεύουν ολοένα και περισσότερο από το κακόβουλο λογισμικό που στοχεύει τη συνδεδεμένη ζωή τους.

Οι «έξυπνες» συσκευές – όπως τα smartwatches, οι smart TVs, τα routers και οι φωτογραφικές μηχανές – συνδέονται μεταξύ τους και δημιουργούν το φαινόμενο του αναπτυσσόμενου Internet of Things (IoT), ένα δίκτυο συσκευών εξοπλισμένων με ενσωματωμένη τεχνολογία που τους επιτρέπει να αλληλοεπιδρούν μεταξύ τους ή με το εξωτερικό περιβάλλον. Λόγω του μεγάλου αριθμού και της ποικιλίας των συσκευών, το IoT έχει γίνει ένας ελκυστικός στόχος για τους ψηφιακούς εγκληματίες. Με την επιτυχή παραβίαση συσκευών IoT, οι εγκληματίες είναι σε θέση να κατασκοπεύουν τους ανθρώπους, να τους εκβιάζουν και ακόμη και να τους καταστήσουν διακριτικά συνεργάτες τους στο έγκλημα. Και ακόμα χειρότερα, botnets όπως το Mirai και το Hajime έδειξαν ότι η απειλή αυτή είναι σε άνοδο.

Οι ειδικοί της Kaspersky Lab πραγματοποιήσαν έρευνες για κακόβουλο λογισμικό με στόχο το IoT με σκοπό να εξετάσουν πόσο

σοβαρός είναι ο κίνδυνος. Έχουν δημιουργήσει honeypots – τεχνητά δίκτυα, τα οποία προσομοιώνουν τα δίκτυα διαφόρων συσκευών IoT (routers, συνδεδεμένες κάμερες κλπ.) για να παρατηρούν τα κακόβουλα προγράμματα που προσπαθούν να επιτεθούν στις εικονικές τους συσκευές. Δεν χρειάστηκε να περιμένουν πολύ, καθώς μεγάλες επιθέσεις με γνωστά και άγνωστα κακόβουλα δείγματα ξεκίνησαν σχεδόν αμέσως μετά την εγκατάσταση του honeypot.

Οι περισσότερες από τις επιθέσεις που καταγράφηκαν από τους ειδικούς της εταιρείας στόχευαν σε ψηφιακές συσκευές εγγραφής βίντεο ή IP κάμερες (63%) και το 20% των επιθέσεων είχε ως στόχο συσκευές δικτύου, συμπεριλαμβανομένων routers και DSL modems, κλπ. Περίπου το 1% των στόχων ήταν οι πιο συνηθισμένες συσκευές, όπως οι εκτυπωτές και οι «έξυπνες» οικιακές συσκευές.

Η Κίνα (17%), το Βιετνάμ (15%) και η Ρωσία (8%) εμφανίστηκαν ως οι 3 κορυφαίες χώρες που δέχτηκαν επιθέσεις σε συσκευές IoT, καθεμία από τις οποίες παρουσιάζει μεγάλο αριθμό «μολυσμένων» μηχανών. Ακολουθούν η Βραζιλία, η Τουρκία και η Ταϊβάν με7%.

Μέχρι σήμερα, κατά τη διάρκεια αυτού του συνεχιζόμενου πειράματος, οι ερευνητές κατάφεραν να συλλέξουν πληροφορίες για περισσότερα από 7.000 δείγματα κακόβουλου λογισμικού που έχουν σχεδιαστεί ειδικά για την παραβίαση συνδεδεμένων συσκευών.

Σύμφωνα με τους ειδικούς, ο λόγος πίσω από την άνοδο είναι απλός: το IoT είναι εύθραυστο και εκτεθειμένο απέναντι στους ψηφιακούς εγκληματίες. Η συντριπτική πλειονότητα των «έξυπνων» συσκευών εκτελεί λειτουργικά συστήματα βασισμένα στο Linux, καθιστώντας ευκολότερες τις επιθέσεις σε αυτές, επειδή οι εγκληματίες μπορούν να γράψουν γενικό κακόβουλο κώδικα που στοχεύει ταυτόχρονα σε έναν τεράστιο αριθμό συσκευών.

Αυτό που καθιστά το ζήτημα επικίνδυνο είναι η πιθανή έκτασή του. Σύμφωνα με τους ειδικούς της βιομηχανίας, υπάρχουν ήδη πάνω από 6 δισεκατομμύρια «έξυπνες» συσκευές ανά τον κόσμο. Οι περισσότερες από αυτές δεν διαθέτουν καν λύση ασφάλειας εγκατεστημένη και οι κατασκευαστές τους συνήθως δεν κυκλοφορούν ενημερώσεις ασφάλειας ή νέο firmware. Αυτό σημαίνει ότι υπάρχουν εκατομμύρια δυνητικά ευάλωτες συσκευές – ή ίσως ακόμη και συσκευές που έχουν ήδη παραβιαστεί.

"Το θέμα της ασφάλειας των «έξυπνων» συσκευών είναι σοβαρό και πρέπει να το γνωρίζουμε όλοι. Το περασμένο έτος έδειξε ότι δεν είναι μόνο δυνατή η στόχευση συνδεδεμένων συσκευών, αλλά ότι πρόκειται για μια πραγματική απειλή. Έχουμε δει μια τεράστια αύξηση των δειγμάτων κακόβουλου λογισμικού με στόχο το IoT, αλλά το δυναμικό είναι ακόμα μεγαλύτερο. Προφανώς, ο υψηλός ανταγωνισμός στην αγορά των επιθέσεων DDoS πιέζει τους επιτιθέμενους να αναζητήσουν νέους πόρους που θα τους βοηθήσουν να κάνουν όλο και πιο ισχυρές επιθέσεις. Το botnet Mirai κατέδειξε ότι οι «έξυπνες» συσκευές μπορούν να δώσουν στους ψηφιακούς εγκληματίες αυτό που χρειάζονται, με τον αριθμό των συσκευών που μπορούν να στοχεύσουν πλέον να αγγίζει τα δισεκατομμύρια. Διάφοροι αναλυτές έχουν προβλέψει ότι μέχρι το 2020 αυτό θα μπορούσε να αυξηθεί σε 20-50 δισεκατομμύρια συσκευές», δήλωσε ο Vladimir Kuskov, ειδικός ασφαλείας Kaspersky Lab.

Προκειμένου να προστατεύσετε τις συσκευές σας, οι ειδικοί ασφάλειας της Kaspersky Lab συμβουλεύουν τα εξής:

1. Εάν δεν είναι απολύτως απαραίτητο, μην αποκτήσετε πρόσβαση στη συσκευή σας από εξωτερικό δίκτυο.
2. Απενεργοποιήστε όλες τις υπηρεσίες δικτύου που δεν χρειάζεστε για τη χρήση της συσκευής.
3. ένας στάνταρ ή καθολικός κωδικός πρόσβασης που δεν μπορεί να αλλάξει ή ο προεπιλεγμένος λογαριασμός δεν μπορεί να απενεργοποιηθεί, απενεργοποιήστε τις υπηρεσίες δικτύου στις οποίες χρησιμοποιούνται ή κλείστε την πρόσβαση σε εξωτερικά δίκτυα.

4. Πριν χρησιμοποιήσετε τη συσκευή, αλλάξτε τον προεπιλεγμένο κωδικό πρόσβασης και ορίστε έναν νέο.
5. Αναβαθμίστε τακτικά το firmware της συσκευής στην πιο πρόσφατη έκδοση – αν είναι δυνατόν.

Για περισσότερες πληροφορίες για επιθέσεις σε συσκευές IoT, μπορείτε να διαβάσετε τον ειδικό ιστότοπο Securelist.com.