Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών Τμήμα Μηχανικών Πληροφορικής

Πτυχιακή Εργασία

Τίτλος: Internet Of Things Security

Νίκος Τζουνάκος (ΑΜ: 2841)

Επιβλέπων καθηγητής: Φυσαράκης Κωνσταντίνος

Ευχαριστίες

Καταρχάς θα ήθελα να εκφράσω τις αληθινές μου ευχαριστίες για τους γονείς μου και τους φίλους μου που με στήριξαν σε όλες τις φάσεις της ζωής μου και για τη γιαγιά μου για όλη τη βοήθεια τόσο ψυχολογική όσο και οικονομική, που μου προσέφερε όλα αυτά τα χρόνια.

30/9/2017

Νίκος Τζουνάκος

Abstract

Internet of Things represents a general concept for the ability of network devices to sense and collect data from the world around us, and then share that data across the Internet where it can be processed and utilized for various interesting purposes.

Some applications that may be useful are receiving warnings on your phone or wearable device when IoT networks detect some physical danger is detected nearby, self-parking automobiles, automatic ordering of groceries and other home supplies. All kinds of ordinary household gadgets can be modified to work in an IoT system. Wi-Fi network adapters, motion sensors, cameras, microphones and other instrumentation can be embedded in these devices to enable them for work in the Internet of Things

Internet of Things immediately triggers questions around the privacy of personal data. Whether real-time information about our physical location or updates about our weight and blood pressure that may be accessible by our health care providers, having new kinds and more detailed data about ourselves streaming over wireless networks and potentially around the world is an obvious concern.

In the Internet of Things there are many different aspects of security that manufacturers should take into consideration before starting to produce their devices and each of these aspects has different needs in security.

Σύνοψη

Το Internet of Things αντιπροσωπεύει την ιδέα ότι οι συσκευές του δικτύου θα μπορούν να γνωρίζουν και να συλλέγουν δεδομένα από τον κόσμο γύρω μας και στη συνέχεια θα μοιράζονται αυτά τα δεδομένα στο Ίντερνετ όπου μπορούν να επεξεργαστούν για διάφορους σκοπούς.

Μερικές από τις χρήσεις που θα μπορούσαν να μας χρησιμεύσουν είναι να λαμβάνουμε ειδοποιήσεις στο κινητό τηλέφωνο όταν το δίκτυο του IoT εντοπίσει φυσικό κίνδυνο κοντά του, συσκευές που επιτρέπουν σε ένα αυτοκίνητο να παρκάρει μόνο του, αυτόματη παραγγελία τροφίμων για το σπίτι όταν είναι ανάγκη κ.α. Όλων των ειδών τα gadget μπορούν να ρυθμιστούν για να δουλεύουν με ένα IoT σύστημα. Wifi network adapters, αισθητήρες κίνησης, κάμερες, μικρόφωνα.

Με το Internet of Things όμως γεννιούνται και πολλά ερωτήματα γύρω από την ιδιωτικότατα και τα προσωπικά δεδομένα. Αν οι πληροφορίες πραγματικού χρόνου της φυσικής μας τοποθεσίας, για το βάρος ή άλλα στατιστικά υγείας που θα πρέπει να είναι διαθέσιμα στους παρόχους υπηρεσιών υγείας τα οποία ταξιδεύουν μέσο των ασύρματων δικτύων είναι όντως ασφαλή.

Στο Internet of Things υπάρχουν πολλοί τομείς της ασφάλειας που πρέπει να λάβουν υπόψιν οι εταιρίες πριν προχωρήσουν στην κατασκευή των συσκευών τους και η κάθε μία έχει διαφορετικές ανάγκες.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Λίστα Πινάκων

Περίληψη

Σκοπός της πτυχιακής είναι η μελέτη της ασφάλειας του Internet of Things (Ίντερνετ των πραγμάτων) από το φυσικό επίπεδο, το επίπεδο δικτύου, μέχρι και το επίπεδο λογισμικού. Για το λόγο αυτόν μελετήθηκαν οι πιθανοί εισβολείς που μπορεί να υπάρχουν πίσω από μία τέτοια επίθεση καθώς και τα κίνητρά τους, καθώς επίσης και οι πιο γνωστές περιοχές που μπορούν να δεχτούν μία τέτοια επίθεση στο IoT σύμφωνα με τα πρότυπα του OWASP.
Πιο συγκεκριμένα σε κάθε περιοχή εξετάστηκαν και όλες οι αντίστοιχες επιθέσεις που μπορούν να πραγματοποιηθούν, καθώς επίσης και τη λογική πίσω από αυτές ούτως ώστε να μπορεί και κάποιος που έχει πληροφορηθεί να λάβει τα ανάλογα αντιμέτρα για να τις αποτρέψει.
Τέλος παρουσιάζεται το εργαλείο Shodan όπου μπορεί να δείξει πόσο ευάλωτες είναι οι συσκευές IoT στις μέρες μας και πόσο λίγη έμφαση δίνεται στο κομμάτι της ασφάλειας, μαζί με αρκετές περιπτώσεις πραγματικών επιθέσεων, όπου για τα θύματα ήταν καίριας σημασίας.

Κίνητρο για την Διεξαγωγή της Εργασίας

Είναι πολύ εύκολο κάποιος να τοποθετήσει μία κάμερα ασφαλείας στο σπίτι του, ή ένα θερμοστάση όπου θα ελέγχεται απομακρυσμένα ή ακόμα και μία συσκευή για την παρακολούθηση της υγείας ενός ηλικιωμένου μέσα στο σπίτι. Αλλά λίγες είναι οι φορές όπου κάποιος γνωρίζει όντως τις συνέπειες που μπορεί να προέρθουν από μία τέτοια συσκευή αν ο ίδιος δε δώσει την απαραίτητη προσοχή στην ασφάλειά της για την ομαλή λειτουργία της, το οποίο μπορεί να είναι τόσο απλό όσο το να αλλάξει απλά τις προεπιλεγμένες ρυθμίσεις της για το όνομα χρήστη και τον κωδικό της συσκευής.

Σκοπός και Στόχοι Εργασίας

Ο σκοπός και οι στόχοι της εργασίας είναι να πληροφορίσει κάποιον απλό ιδιώτη που απλά χρησιμοποιεί κάποια συσκευή IoT, για τον κίνδυνο που διατρέχει. Και για άτομα που ασχολούνται με την ασφάλεια των εν λόγω συσκευών να διευρύνουν την αντίληψή τους για τους τομείς όπου μπορεί μία τέτοια συσκευή να δεχτεί μία επίθεση.

Δομή Εργασίας

Στο **πρώτο** κεφάλαιο παρουσιάζονται οι λόγοι που η ασφάλεια στο IoT είναι σημαντική και γίνονται κατανοητοί οι κίνδυνοι που μπορεί να διατρέχει κάποιος.

Στο **δεύτερο** κεφάλαιο παρουσάζονται τα είδη των επιθέσεων.

Στο **τρίτο** κεφάλαιο παρουσιάζονται ποιοί ενδέχεται να είναι οι επιτηθέμενοι και ποιά είναι τα κίνητρά τους.

Στο **τέταρτο** κεφάλαιο παρτουσιάζονται οι περιοχές επίθεσης σε ένα σύστημα IoT καθώς και η λίστα που προτείνεται από το OWASP project.

Στο **πέμπτο** κεφάλαιο παρουσιάζονται πιο αναλύτικά οι κίνδυνοι στο μηχανισμό του update.

Στο **έκτο** κεφάλαιο παρουσιάζεται η ασφάλεια στο Interface του χρήστη.

Στο **έβδομο** κεφάλαιο παρουσιάζεται η ασφάλεια στο δίκτυο του IoT.

Στο **όγδωο** κεφάλαιο είναι αναλυτικά η ασφάλεια στο φυσικό επίπεδο.

Στο **ένατο** παρουσιάζεται το εργαλείο Shodan και πως μπορεί κάποιος να το χρησιμοποιήσει, χωρίς να έχει ιδιαίτερες γνώσεις πάνω στην ασφάλεια.

Στο **δέκατο** κεφάλαιο παρουσιάζονται κάποιες δημοσιευμένες επιθέσεις πάνω στο IoT και τα αποτελέσματα που έφεραν.

Εισαγωγή

Τι είναι το IoT

Το IoT μπορεί να είναι ένα επίκαιρο θέμα στη βιομηχανία αλλά δεν είναι μία καινούρια έννοια. Στις αρχές του 2000 ο Kevin Ashton είχε φτιάξει τις βάσεις γι αυτό που θα μπορούσε να γίνει Internet of Things στα εργαστήρια του MIT. Ο Ashton ήταν ένας από τους πρωτοπόρους που αντιλήφθηκε αυτή την έννοια καθώς έψαχνε τρόπους η εταιρία Procter & Gamble θα μπορούσε να βελτιώσει τη δουλειά της συνδέοντας RFID πληροφορίες στο Internet. Η ιδέα ήταν απλή και πολύ ισχυρή. Αν όλα τα αντικείμενα στην καθημερινή ζωή εξοπλιζόντουσαν με αναγνωριστηκά και ασύρματη σύνδεση, θα μπορούσαν να επικοινωνούν μεταξύ τους και να διαχειρίζονται από τους υπολογιστές. Σε ένα άρθρο το 1999 ο Ashton γράφει:

"Αν είχαμε υπολογιστές που γνώριζαν όλες τις πληροφορίες για όλα τα πράγματα –χρησιμοποιώντας δεδομένα που μάζευαν οι ίδιοι χωρίς τη δική μας βοήθεια- θα είμασταν σε θέση να παρακολουθούμε και να μετράμε τα πάντα και το κόστος να μειωθεί σιμαντικά. Θα γνωρίζαμε πότε κάτι χρειαζόταν αντικατάσταση, επιδιόρθωση και πότε ήταν καινούρια ή είχαν περάσει τη μέγιστη απόδοσή τους. Χρειάζεται οι υπολογιστές να έχουν τη δική τους εξουσιοδότηση στο θέμα της συλλογής πληροφοριών, ώστε να μπορούν να δουν, να ακούσουν και να μυρίσουν τον κόσμο μόνοι τους. Η RFID τεχνολογία και οι αισθητήρες επιτρέπουν στους υπολογιστές να παρατηρήσουν, να αναγνωρίσουν και να καταλάβουν τον κόσμο χωρίς την ανάγκη για παρέμβαση του ανθρώπου"

Εκείνη τη στιγμή αυτό το όραμα απαιτούσε μεγάλες τεχνολογικές βελτιώσεις. Στο κάτω κάτω πως θα συνδέονταν τα πάντα πάνω στον πλανήτη; Τι είδους ασύρματης τεχνολογίας μπορεί να χτιστεί σε αυτές τις συσκευές; Τι αλλαγές θα έπρεπε να γίνουν στην ήδη υπάρχουσα υποδομή για να υποστηριχτούν δισεκατομμύρια καινούριες συσκευές; Τι θα τροφοδοτούσε αυτές τις συσκευές; Και άλλες πολλές παρόμοιες ερωτήσεις υπήρχαν το 1999.

Σήμερα πολλά από αυτά τα εμπόδια έχουν λυθεί. Το μέγεθος και το κόστος των ασύρματων τεχνολογιών έχει πέσει τρομερά. Το IPv6 επιτρέπει την ανάθεση διευθύνσεων επικοινωνίας σε δισεκατομμύρια συσκευές. Οι ηλεκτρονικές εταιρίες χρίζουν Wi-Fi τεχνολογίες που συνδέονται με μεγάλο εύρος συσκευών. Κάλυψη δεδομένων κινητής τηλεφωνίας έχει βελτιωθεί σιμαντικά με πολλά δίκτυα να προσφέρουν ευρυζωνικές ταχύτητες. Παρόλο που δεν είναι τέλεια, η τεχνολογία των μπαταριών έχει βελτιωθεί και η ηλιακή επαναφόρτιση έχει τοποθετηθεί σε αρκετές συσκευές. Υπάρχουν δισεκατομμύρια αντικείμενα που θα συνδέονται στο διαδίκτυο τα επόμενα χρόνια, εκτιμάται πάνω από 50 δισεκατομμύρια συσκευές μέχρι το 2020.

Το IoT περιγράφει ένα σύστημα όπου τα αντικείμενα στο φυσικό κόσμο με τους σένσορες που διαθέτουν, είναι συνδεδεμένα στο Ιντερνετ μέσω ασύρματων και ενσύρματων συνδέσεων. Αυτοί οι σένσορες μπορούν να χρησιμοποιήσουν διάφορους τύπους από τοπικές συνδέσεις όπως RFID, NFC, Bluetooth και Wi-Fi. Το Internet of Things θα μπορεί:

- **Να συνδέει μηχανικά και ζωντανά αντικείμενα.** Έχουν ξεκινήσει δοκιμές για την ανάπτυξη του δικτύου του Internet of Things όπου συνδέονται βιομηχανικός εξοπλισμός. Σήμερα η πρόκληση για το IoT είναι να επεκταθεί ούτως ώστε να συνδέονται τα πάντα από το βιομηχανικό εξοπλισμό μέχρι τα καθημερινά αντικείμενα, μπορεί επίσης και να περιλαμβάνει ζωντανούς οργανισμούς όπως φυτά, εκτρεφόμενα ζώα και ανθρώπους.
- **Να χρησιμοποιήσει αισθητήρες για τη συλλογή πληροφοριών.** Τα φυσικά αντικείμενα τα οποία συνδέονται θα έχουν στην κατοχή τους ένα η περισσότερους αισθητήρες. Κάθε ένας από αυτούς θα καταγράφει μία συγκεκριμένη κατάσταση όπως, τοποθεσία, κίνηση, θερμοκρασία κ.α. Στο IoT αυτοί οι αισθητήρες θα συνδέονται μεταξύ τους και σε συστήματα όπου μπορούν να

καταλάβουν και να παρουσιάσουν από τους αισθητήρες. Αυτοί οι αισθητήρες θα παρέχουν καινούριες πληροφορίες στα συστήματα μίας εταιρίας και στους ανθρώπους.

- **Να αλλάζουν τα είδη των αντικειμένων που επικοινωνούν μέσα από ένα IP δίκτυο.** Το IoT επιτρέπει σε αντικείμενα να μοιράζονται πληροφορίες για την κατάστασή τους και το περιβάλλον τους με ανθρώπους, συστήματα λογισμικού και μηχανήματα. Αυτή η πληροφορία μπορεί να μεταδοθεί σε πραγματικό χρόνο. Αυτό σημαίνει ότι κάθε τι θα έχει μία ηλεκτρονική ταυτότητα και μία σύνδεση, έτσι θα είναι δυνατή η αναγνώριση, η καταγραφή και η επικοινωνία με τα αντικείμενα.

Τα δεδομένα στο IoT διαφέρουν από το παραδοσιακό μοντέλο που υπάρχει μέχρι τώρα. Τα δεδομένα μπορούν να είναι μικρά σε μέγεθος και γρήγορα στη μετάδοση. Ο αριθμός των συσκευών, των κόμβων που είναι συνδεδεμένα στο δίκτυο είναι επίσης μεγαλύτερος στο IoT από ότι στο παραδοσιακό δίκτυο. Η επικοινωνία μηχανή-με-μηχανή θα επιτρέψει στις επιχειρήσεις να αυτοματοποιήσουν κάποιες διαδικασίες χωρίς να εξαρτόνται από ένα κεντρικό cloud. Όλο αυτό παρουσιάζει μεγάλες ευκαιρίες για τη συλλογή δεδομένων, αλλά και μεγάλες προκλήσεις από τη μεριά του σχεδιασμού του δικτύου και της ασφάλειας. (1) (2)

Χαρακτηριστικά του IoT

Το κέρδος από τις επιχειρήσεις μέσα από το IoT δημιουργείται από τις πληροφορίες που συλλέγονται μέσο των IoT συσκευών οι οποίες περνάνε μέσα από πέντε φάσεις: Αρχικά η **φάση της δημιουργίας,** όπου οι συσκευές ή οι αισθητήρες συλλέγουν πληροφορίες από το φυσικό περιβάλλον γύρω τους. Τα δεδομένα από τις συνδεδεμένες έξυπνες συσκευές μπορούν να χρησιμοποιηθούν για να δημιουργήσουν πληροφορίες που μπορούν να βοηθήσουν τις επιχειρίσεις, τους πελάτες και τους συνεργάτες. Δεύτερη η **φάση της επικοινωνίας,** όπου τα δεδομένα και τα γεγονότα που παράγονται στέλνονται μέσω του δικτύου στον επιθυμητό προορισμό. Τρίτη **η φάση αθροίσματος,** όπου τα δεδομένα που συλλέχθηκαν συγκεντρώνονται στις καθε αυτές συσκευές. Τέταρτη **η φάση ανάλυσης,** όπου τα δεδομένα που υπάρχουν περνάνε από εκλεπτυσμένη ανάλυση και παράγονται βασικά υποδείγματα, ελέγχου και βελτιστοποιούνται οι διαδικασίες και τελευταία **η φάση πραγματοποίησης** όπου κατάλληλες ενέργεις πραγματοποιούνται βασισμένες στις πληροφορίες που έχουν μαζευτεί. Το IoT είναι ένα περίπλοκο σύστημα με ένα μεγάλο αριθμό χαρακτηριστικών, τα οποία διαφέρουν από ένα τομέα σε ένα άλλο. Μερικά βασικά από αυτά είναι:

1. **Εξυπνάδα**
   Το IoT έρχεται με μία πληθώρα από αλγορίθμους στο λογισμικό που το κάνει έξυπνο. Η έξυπνη νοημοσύνη στο IoT ενισχύει τις δυνατότητες που διευκολύνουν τα πράγματα να ανταποκριθούν με ένα έξυπνο τρόπο σε μία ιδαίτερη κατάσταση και τα υποστηρίζει στην πραγματοποίηση συγκεκριμένων στόχων. Παρά την όλη δημοτικότητα των έξυπνων τεχνολογιών, η νοημοσύνη στο IoT είναι μόνο ένα μέσο για την αλληλεπίδραση μεταξύ των συσκευών, ενώ ο χρήστης με τις μηχανές αλληλεπιδράνε μέσω των κανονικών μεθόδων εισαγωγής δεδομένων και το γραφικό περιβάλλον διεπαφής χρήστη.
2. **Συνδεσιμότητα**
   Η συνδεσιμότητα ενισχύει το Intrnet of Things με το να ενώνει καθημερινά αντικείμενα. Η συδεσιμότητα σε αυτά τα αντικείμενα είναι ζωτικής σημασίας επειδή επιτρέπει τη συλλογή πληροφοριών μέσα στο δίκτυο του IoT και επιτρέπει την πρόσβαση και τη συμβατότητα στα

πράγματα. Με αυτή τη δυνατότητα μία νές ευκαιρίες δημιουργούνται για το Internet of Things.

3. **Δυναμική Φύση**
   Η κύρια δραστηριότητα του Internet of Things είναι να μαζέυει δεδομένα από το περιβάλλον του και αυτό επιτυγχάνεται με τις δυναμικές αλλαγές που συμβαίνουν στις συσκευές του. Η κατάσταση αυτών των συσκευών αλλάζει δυναμικά, για παράδειγμα κατάσταση ύπνου και κατάσταση επαγρύπνησης, συνδεδεμένο και αποσυνδεμένο, καθώς επίσης και διάφορα χαρακτηριστικά όπως θερμοκρασία, τοποθεσία και ταχύτητα. Επιπλέον από την κατάσταση των συσκευών αλλάζει και το πλήθος τους δυναμικά με τους ανθρώπους, το μέρος και την ώρα.
4. **Μεγάλη κλίμακα**
   Ο αριθμός των συσκευών που χρειάζονται διαχείριση και επικοινωνούν μεταξύ τους είναι πολύ μεγαλύτερος από αυτόν που υπάρχει μέχρι τώρα στο τρέχον Internet. Η διαχείριση των δεδομένων που παράγεται από αυτές τις συσκευές γίνεται πολύ πιο σιμαντική.
5. **Τεχνολογία αισθητήρων**
   Το IoT δε θα μπορούσε να υπάρχει χωρίς αισθητήρες οι οποίοι θα εντοπίζουν ή θα μετράνε τις αλλαγές στο περιβάλλον για να δημιουργήσουν δεδομένα τα οποία να αναφέρουν την κατάστασή τους ή ακόμα και να επιδράσουν με το περιβάλλον. Η τεχολογία αισθητήρων παρέχει τα μέσα για να δημιουργηθούν ικανότητες που κατοπτρίζουν πραγματική επίγνωση του φυσικού κόσμου και των ανθρώπων σε αυτόν. Αυτή η τεχνολογία είναι απλά η αναλογική είσοδος από το φυσικό κόσμο, αλλά μπορεί να παρέχει μία βαθιά κατανόηση για τον γύρω μας κόσμο.
6. **Ανομοιογένεια**
   Η ανομοιογένεια στο Internet of Things είναι είναι ένα πολύ βασικό χαρακτηριστικό. Οι συσκευές στο IoT χρησιμοποιούν διαφορετικό hardware και μπορούν να αλληλεπιδρούν με άλλες συσκευές ή πλατφόρμες μέσω διαφορετικών δικτύων. Η IoT αρχητεκτονική πρέπει να υποστηρίζει απευθείας σύνδεση μεταξύ ανομοιγενών δικτύων. Τα βασικά χαρακτηριστικά για τη σχεδίαση των ανομοιογενών πραγμάτων και των περιβάλλοντών τους είναι η κλιμάκωση, επεκτασιμότητα και η διαλειτουργικότητα.
7. **Ασφάλεια**
   Οι IoT συσκευές είναι εκφύσεων ευπαθείς στις απειλές ασφάλειας. Καθώς κερδίζουμε τόση αποτελεσματικότητα και πλεονεκτήματα από το IoT, θα ήταν πολύ λάθος να ξεχάσουμε τα θέματα ασφαλείας που σχετίζονται με αυτό. Υπάρχουν πολλά ζητήσματα ασφαλείας που σχετίζονται με το IoT. Είναι πολύ σιμαντικό να ασφαλίσουμε τα τελικά σημεία, τα δίκτυα και τα δεδομένα που μεταφέρονται μέσα σε αυτό.

Υπάρχει μία πληθόρα τεχνολογιών που σχετίζονται με το Internet of Things η οποία διευκολύνει στην επιτυχή λειτουργία του. Οι IoT τεχνολογίες κατέχουν τα παραπάνω χαρακτηριστικά τα οποία υποστηρίζουν τις ανθρώπινες δραστηριότητες. Επιπλέον ενισχύουν τις ικανότητες του IoT δικτύου με την αμοιβαία συνεργασία καθώς λαμβάνουν μέρος στο συνολικό σύστημα. (2) (3) (5)

Ασφάλεια στο IoT

Γιατί η ασφάλεια στο IoT είναι τόσο σημαντική

Είκοσι χρόνια πριν ένα τηλέφωνο δε θα μπορούσε να κλέψει των κωδικό από το email ή να πάρει ένα αντίγραφο από τα δακτυλικά αποτυπόματα. Σήμερα όπου το Internet of Things συνδέει ψηφιακά συσκευές που χρησιμοποιούμε στην καθημερινότητά μας όπως σπίτια, γραφεία, αυτοκίνητα, ακόμα και τα ίδια μας τα σώματα. Με την έλευση του IPv6 και μία μεγάλη ανάπτυξη των Wi-Fi, το IoT μεγαλώνει με πολύ γρήγορους ρυθμούς.

Το καλό είναι ότι μπορούμε να κάνουμε πράγματα που ποτέ πριν δεν είχαμε φανταστεί, αλλά μαζί με αυτό έρχεται και το μειονέκτημα ότι λόγου της μεγάλης του εξάπλωσης και ευχρηστίας του έχει γίνει ένας πολύ ελκυστικός στόχος για τους εγκληματίες του κυβερνοχώρου. Περισσότερες συνδεδεμένες συσκευές σημαίνει περισσότεροι τομείς για επίθεση και περισσότερες ευκαιρίες για να γίνουμε στόχος των χάκερς και είναι ένα φαινόμενο που πρέπει να του δωθεί μεγάλη σημασία για να προλάβουμε μία καταστροφή τέτοιου είδους.

Οι IoT ευπάθειες ανοίγουν καινούριες ευκαιρίες για τους χάκερς. Μερικές από αυτές τις τρομακτικές ευπάθειες που έχουν βρεθεί στις IoT συσκευές έχουν δημιουργήσει την ανάγκη αυτά τα θέματα να ληφθούν γρήγορα υπόψιν.

Τον προηγούμενο χρόνο οι ερευνητές βρήκαν κρίσιμες ευπάθειες σε ένα μεγάλο εύρος συσκευών όπου η χρήση τους ήταν για την παρακολούθηση μωρών η οποία μπορεί να εκμεταλευτεί από επιτηθέμενους για να διαράξουν αισχρές δραστηριότητες.

Σε μία άλλη έρευνα αποδείχτηκε ότι τα αυτοκίνητα που συνδέονταν στο Internet μπορούσαν να τεθούν σε κίνδυνο και οι χάκερς να πραγματοποιήσουν πολλές κακόβουλες επιθέσεις όπως το να πάρουν υπό τον έλεγχό τους το σύστημα ψυχαγωγίας, να ξεκλειδώσουν πόρτες ή ακόμα και να σταματήσουν τη λειτουργία του αμαξιού καθώς αυτό ήταν σε κίνηση.

Οι συσκευές όπου φοριούνται μπορούν επίσης να γίνουν απειλή για την ιδιωτικότητα των ατόμων, καθώς οι χάκερς μπορούν να χρησιμοποιήσουν αισθητήρες κίνησης που είναι ενσωματωμένοι στα έξυπνα ρολόγια για να κλέψουν δεδομένα που πληκτρολογεί ο χρήστης ή να συλλέξουν δεδομένα υγείας από τις εφαρμογές που διαθέτει ή από συσκευές που καταγράφουν τέτοια δεδομένα. (4) (6)

Βασικοί στόχοι της ασφάλειας

Για να είμαστε αποτελεσματικοί με την ασφάλεια στο IoT πρέπει να έχουμε υπόψιν μας τους βασικούς στόχους όπως ακολουθούν:

Εμπιστευτικότητα

Η εμπιστευτικότητα είναι σημαντικό χαρακτηριστικό στο IoT, αλλά μπορεί να μην είναι υποχρεωτική σε μερικές περιπτώσεις όπου τα δεδομένα είναι δημόσια. Ωστόσο στις περισσότερες περιπτώσεις τα δεδομένα δεν πρέπει να παρουσιάζονται δημόσια ούτε να έχουν πρόσβαση μη εξουσιοδοτημένοι χρήστες. Για παράδειγμα τα δεδομένα ενός ασθενή, τα προσωπικά δεδομένα επιχειρήσεων ή στρατιωτικά δεδομένα πρέπει να παραμένουν κρυφά από μη εξουσιοδοτημένους χρήστες.

Ακεραιότητα

Για να είναι αξιόπιστες οι IoT συσκευές στους χρήστες πρέπει να παρέχουν ακεραιότητα στις περισσότερες περιπτώσεις. Διαφορετικά συστήματα στο IoT έχουν διαφορετικές απαιτήσεις. Για παράδειγμα ένα σύστημα παρατήρησης του ασθενή με απομακρυσμένη πρόσβαση απαιτεί μεγάλο βαθμό ακεραιότητας στον έλεγχο λαθών που προκαλούνται στην επικοινωνία γιατί μπορεί να στοιχίσει τη ζωές ανθρώπων.

Πιστοποίηση και εξουσιοδότηση

Το πρόβλημα της πιστοποίησης είναι ευρέως διαδεδομένο στο IoT λόγο της ίδιας του της φύσης, είτε πρόκειται για επικοινωνία μεταξύ δύο συσκευών, είτε μεταξύ ανθρώπου και συσκευής, είτε μεταξύ ανθρώπων. Κάθε σύστημα έχει διαφορετικές απαιτήσεις και χρειάζεται διαφορετικές λύσεις για να επιτευχθεί η πιστοποίηση. Κάποια χρειάζονται ένα πολύ δυνατό και έμπιστο μηχανισμό όπως η πρόσβαση σε μία τράπεζα και κάποια άλλα όχι. Η εξουσιοδοτημένη πρόσβαση επιτρέπει μόνο σε εξουσιοδοτημένους χρήστες να εκτελούν συγκεκριμένες ενέργειες στο σύστημα.

Διαθεσιμότητα

Ένας χρήστης μίας συσκευής πρέπει να μπορεί να έχει πρόσβαση στις συσκευές ότι ώρα χρειαστεί. Τα διαφορετικά κομμάτια στο hardware και στο software στις IoT συσκευές πρέπει να μπορούν να είναι διαθέσιμα ακόμα και κάτω από αντίξοες συνθήκες.

Έλεγχος

Ένας συνεχόμενος έλεγχος της ασφάλειας των συσκευών για να δούμε πόσο καλά συμμορφώνονται στα κριτήρια που τους έχουν δοθεί. Λόγο των πολλών bug και ευπαθειών στα περισσότερα συστήματα ο έλεγχος παίζει μεγάλο ρόλο στην εύρεση αδύναμων σημείων που είναι πιθανόν ένας επιτιθέμενος να χρησιμοποιήσει για να θέσει σε κίνδυνο τα δεδομένα.

(5) (8) (9) (10)

Στόχοι ιδιωτικότητας

Η ιδιωτικότητα είναι αυτή που καθορίζει το ποιός θα αλληλεπιδράσει με το περιβάλλον και σε τι βαθμό αυτή η οντότητα θα μοιραστεί αυτές τις πληροφορίες με τις άλλες. Οι κύριοι στόχοι της ιδιωτηκότητας στα IoT είναι:

- Ιδιωτικότητα στις συσκευές: εξαρτάται από τη φυσική ιδιωτικότητα. Οι ευαίσθητες πληροφορίες μπορούν να διαρρεύσουν σε περίπτωση που κλαπεί η συσκευή.
- Ιδιωτικότητα στην επικοινωνία: εξαρτάται από τη διαθεσιμότητα της συσκευής, την ακεραιότητα και την αξιοπιστία. Οι IoT συσκευές πρέπει να επικοινωνούν μόνο όταν είναι ανάγκη για να επιτύχουν την ιδιωτικότητα των δεδομένων.
- Ιδιωτικότητα στο χώρο αποθήκευσης: για να προστατέψεις τα ιδιωτικά δεδομένα στις συσκευές πρέπει να ληφθούν υπόψιν τα ακόλουθα.
  - Τον πιθανό όγκο των δεδομένων που πρόκειται να αποθηκευθούν στις συσκευές.
  - Οι ρυθμίσεις λειτουργίας πρέπει να παρέχουν προστασία στα δεδομένα του χρήστη μετά που θα έχει τελειώσει η λειτουργία της συσκευής, για παράδειγμα τα δεδομένα θα πρέπει να διαγράφονται σε περίπτωση κλοπής της συσκευής.

- Ιδιωτικότητα κατά την επεξεργασία: εξαρτάται από τη συσκευή και από την ακεραιότητα στην επικοινωνία. Τα δεδομένα πρέπει να μη φανερώνονται σε τρίτους χωρίς τη γνώση του ιδιοκτήτη.
- Ιδιωτικότητα στην ταυτότητα: η ταυτότητα κάθε συσκευής πρέπει να μόνο να φανερώνεται σε εξουσιοδοτημένες οντότητες.
- Ιδιωτηκότητα στην τοποθεσία: η γεωγραφική θέση των συσκευών πρέπει να είναι γνώστη μόνο σε εξουσιοδοτημένες οντότητες. (6) (10)

Απειλές, επιθέσεις και ευπάθειες

Ευπάθειες

Οι ευπάθειες είναι αδυναμίες στο σύστημα ή στο σχεδιασμό του οι οποίες αφήνουν ένα επιτιθέμενο να εκτελέσει εντολές, να έχει πρόσβαση σε εξουσιοδοτημένα δεδομένα ή να προκαλέσει επιθέσεις άρνησης εξυπηρέτησης (DoS). Οι ευπάθειες μπορούν να βρεθούν σε πολλές περιοχές σε ένα IoT σύστημα. Πιο συγκεκριμένα μπορεί να είναι αδυναμίες στο hardware ή στο software, αδυναμία στην πολιτική του συστήματος και αδυναμία στους χρήστες που χρησιμοποιούν το σύστημα.

Τα IoT συστήματα είναι βασισμένα σε δύο βασικά συστατικά: Στο hardware και στο software και τα δύο έχουν λάθη σχεδίασης πολύ συχνά. Οι ευπάθειες στο hardware είναι πολύ δύσκολο να εντοπιστούν και ακόμα πιο δύσκολο να διορθωθούν λόγο της συμβατότητας και της προσπάθειας που χρειάζονται για να διορθωθούν. Οι ευπάθειες στο software μπορούν να βρεθούν στα λειτουργικά συστήματα, στο λογισμικό της εφαρμογής και στο λογισμικό ελέγχου όπως πρωτόκολλα επικοινωνίας. Υπάρχουν πολλοί παράγοντες που προκαλούν λάθη σχεδίασης στο λογισμικό όπως ανθρώπινοι παράγοντες και η πολυπλοκότητα του λογισμικού. Οι τεχνικές ευπάθειες συνήθως συμβαίνουν λόγο έλλειψης κατανόησης των απαιτήσεων του project, έλλειψη επικοινωνίας μεταξύ των σχεδιαστών και των χρηστών και έλλειψη γνώσης.

Έκθεση

Η έκθεση είναι ένα πρόβλημα ή λάθος στη ρύθμιση του συστήματος το οποίο επιτρέπει σε ένα επιτιθέμενο να συλλέξει πληροφορίες για το σύστημα. Μία από τις μεγαλύτερες προκλήσεις στα IoT συστήματα είναι η ανθεκτικότητα στην έκθεση ενάντια σε φυσικές επιθέσεις. Στις περισσότερες IoT εφαρμογές, οι συσκευές μένουν απροφύλακτες και είναι τοποθετημένες σε περιοχές όπου ο επιτιθέμενος μπορεί εύκολα να έχει πρόσβαση σε αυτές. Μία τέτοια έκθεση αυξάνει τις πιθανότητες ένας επιτιθέμενος να επέμβει στη συσκευή και να τραβήξει κρυπτογραφημένα μηνύματα, να αλλάξει τον κώδικα ή ακόμα και να αντικαταστήσει τη συσκευή με μία άλλη όπου θα είναι κάτω από τον έλεγχό του.

Απειλές

Η απειλή είναι μία ενέργεια η οποία εκμεταλλεύεται την αδύναμη ασφάλεια σε ένα σύστημα και έχει μία αρνητική επίπτωση σε αυτό. Οι απειλές μπορούν να προέλθουν από δύο βασικές πηγές: τους ανθρώπους και τη φύση. Οι φυσικές απειλές οι σεισμοί, οι ανεμοστρόβιλοι, πλημμύρες, φωτιά και άλλες οι οποίες μπορούν να προκαλέσουν βλάβη στα συστήματα υπολογιστών. Μικρή προστασία μπορεί να εφαρμοστεί εναντίον των φυσικών καταστροφών και είναι δύσκολο κάποιος να τις αποτρέψει από το να συμβούν. Τα σχέδια επαναφοράς όπως το backup και τα σχέδια έκτακτης ανάγκης είναι οι καλύτερες προσεγγίσεις για την ασφάλεια σε τέτοιες περιπτώσεις. Οι απειλές από τους ανθρώπους οι οποίες μπορεί να προέρχονται είτε από κάποιον που έχει πρόσβαση στο σύστημα είτε από κάποιον που δεν έχει έχουν σκοπό να βλάψουν το σύστημα. Οι ανθρώπινες επιθέσεις κατηγοριοποιούνται παρακάτω:

- Μη δομημένες επιθέσεις που κυρίως προέρχονται από μη έμπειρα άτομα τα οποία χρησιμοποιούν ευρέως διαδεδομένα εργαλεία hacking.
- Δομημένες επιθέσεις από ανθρώπους που γνωρίζουν ευπάθειες συστημάτων και μπορούν να καταλάβουν να σχεδιάσουν και να εκμεταλλευτούν κώδικα και scripts.

Καθώς το IoT γίνεται πραγματικότητα και οι πολυάριθμες συσκευές έχουν αρχίσει να μπαίνουν στις ζωές μας, έχει μεγαλώσει και ο αριθμός των επιθέσεων που μπορούν να δεχτούν αυτά τα συστήματα. Δυστυχώς το IoT έρχεται με ένα καινούριο σύνολο επιθέσεων τα οποία μπορούν να επηρεάσουν τα smart-phones, τους προσωπικούς υπολογιστές και σε επέκταση την καθημερινότητά μας. (12) (13) (15)

Επιθέσεις

Οι επιθέσεις είναι δράσεις που συμβαίνουν για να βλάψουν ένα σύστημα ή για να διακόψουν την προγραμματισμένη του λειτουργία, εκμεταλλεύοντας κάποιες ευπάθειες χρησιμοποιώντας διάφορες τεχνικές και εργαλεία. Οι επιτιθέμενοι πραγματοποιούν επιθέσεις για να πετύχουν κάποιους στόχους είτε για προσωπική ευχαρίστηση ή έναντι κάποιας ανταμοιβής. Η ποσότητα της προσπάθειας που καταβάλλεται από τον επιτιθέμενο σχετίζεται με την εμπειρία που έχει, τα μέσα που έχει και το κίνητρο που έχει. Επιτιθέμενοι θεωρούνται όσοι μπορούν να αποτελέσουν απειλή στον ψηφιακό κόσμο. Μπορεί να είναι χάκερς, εγκληματίες η ακόμα και κυβερνήσεις.

Μία επίθεση μπορεί να πάρει διάφορες μορφές, όπως επίθεση στο δίκτυο για την παρακολούθηση της πληροφορίας ή αποκρυπτογράφηση των μηνυμάτων χρησιμοποιώντας κάποια αδυναμία κ.α. Μερικά είδη επιθέσεων είναι:

Α) Φυσικές επιθέσεις: Αυτού του είδους οι επιθέσεις έχουν να κάνουν με τα εξαρτήματα των συσκευών. Λόγο του ότι οι περισσότερες συσκευές είναι σχεδιασμένες για να λειτουργούν σε εξωτερικούς χώρους οι οποίοι συχνά μένουν αφύλακτοι, είναι πολύ εύκολο να πραγματοποιηθούν φυσικές επιθέσεις.

Β) Επιθέσεις αναγνώρισης: Μη εξουσιοδοτημένη χαρτογράφηση του συστήματος, των services ή των ευπαθειών. Μερικά παραδείγματα είναι η σάρωση των network ports, packet sniffers και η ανάλυση της δικτυακής κίνησης.

Γ) Άρνηση υπηρεσιών (DoS): Αυτού του είδους η επίθεση έχει σκοπό να θέσει εκτός λειτουργίας το μηχάνημα το οποίο έχει στόχο. Λόγο της χαμηλής μνήμης, οι περισσότερες συσκευές στο IoT είναι εύκολος στόχος σε τέτοιου είδους επιθέσεις.

Δ) Επιθέσεις πρόσβασης: μη εξουσιοδοτημένοι άνθρωποι παίρνουν πρόσβαση στο δίκτυο ή σε συσκευές στις οποίες δεν έχουν αυτό το δικαίωμα. Υπάρχουν δύο ειδών επιθέσεις πρόσβασης: οι πρώτες είναι οι φυσικές επιθέσεις, όπου ο επιτιθέμενος παίρνει φυσική πρόσβαση στη συσκευή και οι δεύτερες είναι απομακρυσμένης πρόσβασης όπου γίνεται σε συσκευές που χρησιμοποιούν IP.

Ε) Επιθέσεις σε προσωπικά δεδομένα: Η ιδιωτικότητα στο IoT είναι μία ιδιαίτερη πρόκληση λόγο του μεγάλου όγκου δεδομένων μου είναι εύκολα προσβάσιμο μέσω των απομακρυσμένων μηχανισμών πρόσβασης. Οι πιο συνηθισμένες επιθέσεις στα προσωπικά δεδομένα είναι:

- Data mining: επιτρέπει στον επιτιθέμενο να ανακαλύψει πληροφορίες δεν είναι διαθέσιμες σε συγκεκριμένες βάσεις δεδομένων.

- Cyber espionage: χρησιμοποιώντας επιθέσεις cracking και κακόβουλο λογισμικό για να κατασκοπεύσει συγκεκριμένες πληροφορίες για άτιμα, οργανισμούς ή κυβερνήσεις.
- Eavesdropping: ακούγοντας μία συζήτηση μεταξύ δύο άκρων
- Password-based attacks: χρησιμοποιούνται από τον επιτιθέμενο για να πάρει πρόσβαση στο λογαριασμό ενός είδη υπάρχον χρήστη. Τέτοιες επιθέσεις μπορούν να γίνουν με δύο διαφορετικούς τρόπους: 1) επιθέσεις με λεξικό: προσπαθώντας να μαντέψει ένα συνδυασμό από γράμματα και αριθμούς για να βρεθεί ο κωδικός ενός χρήστη. 2) brute force attacks: χρησιμοποιώντας εργαλεία cracking για να δοκιμάσει όλους τους πιθανούς συνδυασμούς κωδικών για ανακαλύψει ένα έγκυρο κωδικό.

Ζ) Διαδικτυακές επιθέσεις: Το Internet και οι έξυπνες συσκευές χρησιμοποιούνται για να εκμεταλλευτούν τους χρήστες και τα δεδομένα για λόγους κλοπής δεδομένων, περιουσίας ή ακόμα και για κλοπή ιδεών.

Η) Καταστρεπτικές επιθέσεις: χρησιμοποιούνται για την καταστροφή της περιουσίας ή ενός συγκεκριμένου ατόμου. Παραδείγματα τέτοιων επιθέσεων είναι η τρομοκρατία και οι επιθέσεις για εκδίκηση.

Θ) Supervisory Control and Data Acquisition (SCADA) Attacks: όπως πολλά TCP/IP συστήματα, έτσι και το SCADA σύστημα είναι ευπαθή σε πολλές δικτυακές επιθέσεις. Μερικές από αυτές είναι: 1) χρησιμοποιώντας επιθέσεις άρνησης εξυπηρέτησης_για να σταματήσει η λειτουργία του συστήματος 2) χρησιμοποιώντας δούρειους ίππους ή ιούς για να πάρουν τον έλεγχο του συστήματος. (7) (15) (18)

Εισβολείς, Κίνητρα και Δυνατότητες

Οι εισβολείς έχουν διαφορετικά κίνητρα και στόχους, μερικά από αυτά μπορεί να είναι το οικονομικό κέρδος, να επηρεάσουν την κοινή γνώμη, για λόγους κατασκοπείας κ.α. Οι δυνατότητες ποικίλουν από απλούς μεμονωμένους επιτιθέμενους μέχρι οργανωμένες ομάδες εγκλήματος.

Οι επιτιθέμενοι επίσης έχουν διαφορετικά επίπεδα από πόρους και δεξιότητες που κάνουν την επιτυχία μιας επίθεσης να διαφέρει. Ένας που είναι ήδη χρήστης έχει πιο πολύ πρόσβαση από κάποιον εξωτερικό. Μερικοί επιτιθέμενοι έχουν διαφορετικό οικονομικό προϋπολογισμό_από κάποιους άλλους. Κάθε επιτιθέμενος επιλέγει ένα στόχο που του είναι οικονομικά εφικτός, μία επίθεση που είναι βασισμένη στο να έχει καλή οικονομική απόδοση βασισμένη στον προϋπολογισμό, στους πόρους και στην εμπειρία. Σε αυτό το κεφάλαιο οι επιτιθέμενοι θα χωριστούν σε κατηγορίες ανάλογα τα χαρακτηριστικά, τα κίνητρα και τους στόχους, τις δυνατότητες και τους πόρους που έχουν. (19) (20)

Σκοπός και κίνητρο μιας επίθεσης

Οι ιστοσελίδες των κυβερνήσεων, τα οικονομικά συστήματα, οι ιστοσελίδες για τα νέα και των μέσων μέσων μαζικής ενημέρωσης και τα δίκτυα του στρατού είναι οι βασικοί στόχοι των κυβερνοεπιθέσεων. Οι αξία αυτών των επιθέσεων είναι δύσκολο να εκτιμηθεί και συνήθως διαφέρει μεταξύ του επιτιθέμενου και του αμυνόμενου. Τα κίνητρα της επίθεσης ποικίλουν από την κλοπή ταυτότητας, κλοπή περιουσίας μέχρι την οικονομική απάτη. Για παράδειγμα το κλέψιμο πληροφοριών πιστωτικών καρτών έχει γίνει χόμπι στις μέρες μας και οι οργανισμοί ηλεκτρονικής τρομοκρατίας που επιτίθενται σε συστήματα των κυβερνήσεων για να δημιουργήσουν πολιτικά ή θρησκευτικά σκάνδαλα.

Κατηγοριοποίηση των πιθανών εισβολέων

Γενικά οι εισβολείς χωρίζονται σε δύο κατηγορίες: εσωτερικούς και εξωτερικούς. Οι εσωτερικοί είναι χρήστες που έχουν δικαιώματα πρόσβασης στο σύστημα είτε με το χρήση ενός account, είτε φυσική πρόσβαση στο δίκτυο. Οι εξωτερικοί εισβολείς είναι άνθρωποι που δεν ανήκουν στο δίκτυο. Ο σκοπός της εισβολής εξαρτάται από τον στόχο που είναι να επιτευχθεί σε κάθε περίπτωση. Ένας μεμονωμένος επιτιθέμενος μπορεί να έχει μικρούς στόχους ενώ οι κατάσκοποι οργανισμών να έχουν μεγαλύτερα κίνητρα. Παρακάτω θα δούμε τους διάφορους τύπους επιτιθέμενων ανάλογα των αριθμό τους, των κινήτρων και τον στόχων που έχουν. (16) (17)

Μεμονωμένοι

Οι μεμονωμένοι hacker είναι επαγγελματίες που δουλεύουν μόνοι τους και έχουν ως στόχο συστήματα με χαμηλή ασφάλεια. Δεν έχουν πολλούς πόρους ούτε μεγάλη εμπειρία από επαγγελματικές ομάδες hacking, οργανισμούς ή κατασκοπικές οργανώσεις. Οι μεμονωμένοι hacker έχουν σχετικά μικρούς στόχους και οι επιθέσεις που κάνουν έχουν μικρή επίπτωση σε σχέση με αυτές των

οργανωμένων ομάδων. Χρησιμοποιούν συχνά επιθέσεις social engineering γιατί συχνά χρειάζεται να μαζέψουν πληροφορίες για το στόχο όπως διεύθυνση, κωδικούς κ.α. Τα δημόσια και τα κοινωνικά δίκτυα είναι τα πιο συχνά μέρη όπου οι χρήστες μπορούν να εξαπατηθούν από τους hackers. Επιπλέον τα λειτουργικά συστήματα που χρησιμοποιούνται στα laptop, PCs και κινητά τηλέφωνα έχουν γνωστές ευπάθειες που συνήθως αυτοί οι hackers εκμεταλεύονται.

Τα οικονομικά ιδρύματα όπως οι τράπεζες είναι στόχοι των μεμονωμένων hacker καθώς ξέρουν ότι αυτού του είδους δικτύων μεταφέρουν οικονομικές συναλλαγές που μπορούν να υποκλέψουν. Η υποκλοπή πιστωτικών καρτών είναι πολύ γνωστή καθώς με την ανάπτυξη του e-commerence είναι πολύ εύκολο να αγοράσεις εμπορεύματα ή υπηρεσίες.

Οι μεμονωμένοι hacker χρησιμοποιούν εργαλεία όπως ιούς, σκουλήκια, sniffers για να εκμεταλλευτούν ένα σύστημα. Σχεδιάζουν επιθέσεις βασισμένες στον εξοπλισμό που έχουν, το περιβάλλον του δικτύου και την ασφάλεια του συστήματος.

Μία κατηγορία των μεμονωμένων hacker είναι οι εσωτερικοί επιτηθέμενοι. Οι εσωτερικοί είναι μεμονωμένοι χρήστες που επιτίθενται στο σύστημα και χρησιμοποιούν πληροφορίες που ήδη γνωρίζουν ή αυξημένα δικαιώματα. Οι εσωτερικοί μπορούν να παρέχουν πολύ σημαντικές πληροφορίες στους εξωτερικούς για να εκμεταλλευτούν ευπάθειες και να πραγματοποιήσουν μία επίθεση. Ξέρουν τα αδύναμα σημεία του συστήματος και πως λειτουργεί όλο το σύστημα. Το προσωπικό όφελος, η εκδίκηση, και το οικονομικό κέρδος μπορούν να είναι τα κίνητρα ενός εσωτερικού επιτιθέμενου. (16) (17) (18)

Οργανωμένες ομάδες

Οι οργανωμένες ομάδες εγκλήματος γίνονται όλο και περισσότερο δημοφιλείς στον τομέα των τηλεπικοινωνιών και της IoT τεχνολογίας. Τα κίνητρα αυτών των ομάδων ποικίλουν. Τυπικά οι στόχοι τους περιλαμβάνουν συγκεκριμένους οργανισμούς για εκδίκηση, κλοπή ή ανταλλαγή πληροφορίας ή οικονομική κατασκοπεία. Περιλαμβάνουν επίσης την πώληση προσωπικής πληροφορίας.

Έχουν αρκετούς πόρους και πολλές επιδεξιότητες. Οι ομάδες εγκληματιών μπορούν να χρησιμοποιήσουν υψηλές μεθόδους και τεχνικές ανάλογα με τους στόχους που έχουν. Είναι πολύ επιδέξιοι στο να δημιουργούν bot nets και κακόβουλο λογισμικό και επιθέσεις άρνησης εξυπηρέτησης. Οι οργανωμένοι εγκληματίες είναι πολύ πιθανόν να έχουν πρόσβαση σε μεγάλα κεφάλαια, που σημαίνει ότι είναι επιδέξιοι hacker επί πληρωμή αν χρειαστεί. Τέτοιοι εγκληματίες επιχειρούν πιο επικίνδυνους στόχους από τους μεμονωμένους επιτιθέμενους και είναι διαθέσιμοι να επενδύσουν σε κερδοφόρες επιθέσεις.

Οι διαδικτυακοί τρομοκράτες έχουν ως στόχους στρατιωτικά συστήματα, τράπεζες και συγκεκριμένες εγκαταστάσεις όπως δορυφόρους και τηλεπικοινωνιακά συστήματα τα οποία σχετίζονται με εθνικές πληροφορίες που βασίζονται σε θρησκείες και πολιτικά ενδιαφέροντα. Οι τρομοκρατικές οργανώσεις εξαρτώνται στο διαδίκτυο για να διαδώσουν προπαγάνδα, να αυξήσουν τα κέρδη τους, να μαζέψουν πληροφορία και να επικοινωνούν μεταξύ τους. (19)

Υπηρεσίες πληροφοριών

Οι υπηρεσίες πληροφοριών επιμένουν πολύ στις προσπάθειές τους να εξετάσουν τα στρατιωτικά συστήματα άλλων χωρών για συγκεκριμένους λόγους, για παράδειγμα βιομηχανική κατασκοπεία, πολιτική και στρατιωτική κατασκοπεία. Για να πετύχουν τους στόχους τους απαιτείται ένας μεγάλος αριθμός ειδικών σε πολλούς τομείς.

Τέτοιοι οργανισμοί έχουν οργανωμένες δομές και εκλεπτυσμένες πηγές για να πετύχουν τους στόχους τους. Αυτοί οι οργανισμοί είναι η μεγαλύτερη απειλή στα δίκτυα και απαιτούν στενή παρακολούθηση για να εξασφαλιστεί η ασφάλεια στα κύρια συστήματα κάθε χώρας. (8) (9)

Περιοχές επίθεσης σε συστήματα IoT

Υπάρχουν τρεις βασικές περιοχές επίθεσης, επιθέσεις στα device, επιθέσεις στην επικοινωνία μεταξύ device και master και επιθέσεις στους masters.

Επιθέσεις στα device

Για ένα επιτιθέμενο ένα device μπορεί να είναι ένα ενδιαφέρον στόχος για πολλούς λόγους. Αρχικά γιατί πολλές συσκευές έχουν πρόσβαση στο internet για να κάνουν τη λειτουργία τους. Μία κάμερα ασφαλείας για παράδειγμα μεταδίδει χρήσιμες πληροφορίες για την περιοχή την οποία επιβλέπει.

Οι συσκευές έχουν τη δυνατότητα να διαχειρίζονται πράγματα, όπως να ελέγξουν τη λειτουργία του φωτισμού του σπιτιού ή της επιχείρησης ή ακόμα και κάτι κακόβουλο όπως το κινητό ή να ρυθμίσουν μία ιατρική συσκευή. (21)

Επιθέσεις στην επικοινωνία

Μία συχνή επίθεση είναι η παραποίηση των μηνυμάτων καθώς αυτά μεταφέρονται. Η συχνότητα και η ευαισθησία των δεδομένων που μεταφέρονται σε ένα IoT περιβάλλον κάνει αυτού του είδους τις επιθέσεις ιδιαίτερα επικίνδυνες. Για παράδειγμα οι πληροφορίες που μεταφέρονται για την κατανάλωση ηλεκτρικής ενέργειας από ένα σπίτι προς τον πάροχο του δημιουργούν ένα εύρος επιθέσεων. Για παράδειγμα ένας επιτιθέμενος μπορεί να παρατηρήσει πότε υπήρχε υψηλή κατανάλωση και πότε χαμηλή, για να προγραμματίσει μία φυσική επίθεση στο σπίτι ή να αλλάξει τα δεδομένα που μεταφέρονται προς την εταιρία. (24)

Επίθεση στο Master of Devices

Επιθέσεις ενάντια σε manufacturers, cloud service providers, and IoT solution providers έχουν τη δυνατότητα να προκαλέσουν τη μεγαλύτερη ζημιά. Σε αυτά τα μέρη μαζεύονται μεγάλου όγκου πληροφορίες και ιδιαίτερα ευαίσθητες.

Μία επίθεση σε ένα Master μπορεί επίσης να προκαλέσει ζημιά και σε πολλές συσκευές τις οποίες αυτός διαχειρίζεται. (9) (10)

Λίστα περιοχών επίθεσης

Attack Surface	Vulnerability
Ecosystem (general)	• Interoperability standards • Data governance • System wide failure • Individual stakeholder risks

Ecosystem Access Control	• Implicit trust between components • Enrollment security • Decommissioning system • Lost access procedures
Device Memory	• Cleartext usernames • Cleartext passwords • Third-party credentials • Encryption keys
Device Physical Interfaces	• Firmware extraction • User CLI • Admin CLI • Privilege escalation • Reset to insecure state • Removal of storage media • Tamper resistance • Debug port • Device ID/Serial number exposure
Device Web Interface	• SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Weak passwords • Account lockout • Known default credentials
Device Firmware	• Hardcoded credentials • Sensitive information disclosure • Sensitive URL disclosure • Encryption keys • Encryption (Symmetric, Asymmetric) • Firmware version display and/or last update date • Backdoor accounts • Vulnerable services (web, ssh, tftp, etc.)

	• Security related function API exposure • Firmware downgrade
Device Network Services	• Information disclosure • User CLI • Administrative CLI • Injection • Denial of Service • Unencrypted Services • Poorly implemented encryption • Test/Development Services • Buffer Overflow • UPnP • Vulnerable UDP Services • DoS • Device Firmware OTA update block • Replay attack • Lack of payload verification • Lack of message integrity check
Administrative Interface	• SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Weak passwords • Account lockout • Known default credentials • Security/encryption options • Logging options • Two-factor authentication • Inability to wipe device
Local Data Storage	• Unencrypted data • Data encrypted with discovered keys • Lack of data integrity checks

	• Use of static same enc/dec key
Cloud Web Interface	• SQL injection • Cross-site scripting • Cross-site Request Forgery • Username enumeration • Weak passwords • Account lockout • Known default credentials • Transport encryption • Insecure password recovery mechanism • Two-factor authentication
Third-party Backend APIs	• Unencrypted PII sent • Encrypted PII sent • Device information leaked • Location leaked
Update Mechanism	• Update sent without encryption • Updates not signed • Update location writable • Update verification • Update authentication • Malicious update • Missing update mechanism • No manual update mechanism
Mobile Application	• Implicitly trusted by device or cloud • Username enumeration • Account lockout • Known default credentials • Weak passwords • Insecure data storage • Transport encryption • Insecure password recovery mechanism • Two-factor authentication

Vendor Backend APIs	• Inherent trust of cloud or mobile application • Weak authentication • Weak access controls • Injection attacks • Hidden services
Ecosystem Communication	• Health checks • Heartbeats • Ecosystem commands • Deprovisioning • Pushing updates
Network Traffic	• LAN • LAN to Internet • Short range • Non-standard • Wireless (WiFi, Z-wave, Zigbee, Bluetooth) • Protocol fuzzing
Authentication/Authorization	• Authentication/Authorization related values (session key, token, cookie, etc.) disclosure • Reusing of session key, token, etc. • Device to device authentication • Device to mobile Application authentication • Device to cloud system authentication • Mobile application to cloud system authentication • Web application to cloud system authentication • Lack of dynamic authentication
Privacy	• User data disclosure • User/device location disclosure • Differential privacy
Hardware (Sensors)	• Sensing Environment Manipulation • Tampering (Physically) • Damaging (Physically)

Πίνακας 1 Λίστα περιοχών επίθεσης

Ασφάλεια στο μηχανισμό του Update

Update Sent Without Encryption

Το update μεταφέρεται στο δίκτυο χωρίς τη χρήση TLS ή το αρχείο δεν είναι κρυπτογραφημένο. Ο επιτιθέμενος μπορεί να παρέμβει και να τροποποιήσει το αρχείο πριν φτάσει στον προορισμό του. Έχει τη δυνατότητα είτε να διαβάσει το αρχείο είτε να το παρέμβει στα δεδομένα που μεταφέρει και έτσι να προκαλέσει μία διαφορετική λειτουργία από αυτήν που προοριζόταν.

No Manual Update Mechanism

Δεν υπάρχει η δυνατότητα ο διαχειριστής να κάνει update τη συσκευή κατά βούληση. Αν για κάποιο λόγο το update δεν έχει γίνει ή έχει γίνει κάποια διακοπή ενώ γινόταν, πρέπει να παρέχεται στο διαχειριστή η δυνατότητα να ξανά ξεκινήσει τη διαδικασία από την αρχή. Ένα μεγάλο ποσοστό των update που γίνονται είναι για διορθωθούν κενά που υπάρχουν στην ασφάλεια ενός συστήματος, οπότε κάτι τέτοιο μπορεί να αποδειχτεί εξερετικά επικίνδυνο.

Missing Update Mechanism

Όταν δεν υπάρχει η δυνατότητα να αναβαθμιστεί η συσκευή δεν υπάρχει και η δυνατότητα να καλυφθεί ένα κενό ή μία ευπάθεια που έχει ανακαλυφθεί στη συσκευή. Ακόμα και στα πιο γνωστά και ευρέως χρησιμοποιούμενα συστήματα συνεχώς ανακαλύπτονται κενά στην ασφάλεια, το να υπάρχει ένας μηχανισμός update για να καλύβονται αυτά τα κενά είναι απαραίτητος. (11) (28)

Ασφάλεια στο Interface

Username Enumeration

Ο σκοπός αυτής της επίθεσης είναι να δημιουργήσει ο επιτιθέμενος μία λίστα με έγκυρα usernames αλληλεπιδρώντας με την εφαρμογή, ώστε στη συνέχεια να τα χρησιμοποιήσει για να επιτεθεί στο μηχανισμό του login και να βρει τον κωδικό του χρήστη.

Μία τέτοια επίθεση μπορεί να το επιτευχθεί στέλνοντας στην εφαρμογή λάθος στοιχεία -όνομα χρήστη και κωδικό- και μετά να συγκρίνει τις απαντήσεις που επιστρέφει η εφαρμογή. Αυτό συμβαίνει γιατί οι απαντήσεις που επιστρέφονται από την εφαρμογή για ένα υπαρκτό όνομα είναι διαφορετικές από αυτές που επιστρέφονται για ένα μη υπαρκτό όνομα.

Αρχικά μπορεί κάποιος να εξετάσει την HTTP απάντηση που επιστρέφει ο server:

Δοκιμάζοντας ένα έγκυρο username και password για να δει τι επιστρέφει ο server ως απάντηση. Αυτό γίνεται εύκολα χρησιμοποιώντας ένα web proxy.

Στη συνέχεια μπορεί να δοκιμάσει για ένα έγκυρο username αλλά λάθος κωδικό. Εδώ πρέπει να αποθηκευτεί η απάντηση και το μήνυμα λάθους που επιστρέφεται από το server. Αν υπάρχει κάπου στην απάντηση υπόδειξη ότι ο χρήστης υπάρχει πρέπει να ληφθεί υπόψιν γιατί μπορεί αργότερα να χρησιμοποιειθεί για την εύρεση και άλλων usernames του συστήματος.

Και τέλος δοκιμάζοντας με ένα μη υπαρκτό username.

Οι απαντήσεις της εφαρμογής πρέπει να επιστρέφουν ένα γενικό μήνυμα λάθους που να είναι ίδιο σε όλες τις περιπτώσεις, σε περίπτωση που το μήνυμα διαφέρει πρέπει ο επιτηθέμενος να ψάξει να δει τι προκαλεί αυτή τη διαφορά. Οι απαντήσεις μπορεί να διαφέρουν στα error code, URLS, Web page Titles που επιστρέφουν.

Ένας άλλος τρόπος μπορεί να είναι παρατηρώντας τους τίτλους στις ιστοσελίδες, για παράδειγμα ένας τίτλος θα μπορούσε να είναι “Invalid user” και ένας άλλος “Invalid authentication”.

Ένας άλλος τρόπος αυτής της επίθεσης είναι η εφαρμογή να δημιουργεί η ίδια προβλέψιμα usernames για τους χρήστες. Π.χ. User001, user002 οπότε είναι εύκολο για τον επιτηθέμενο να προβλέψει μία λίστα με έγκυρα usernames.

Weak Passwords

Ο πιο εύκολος και διαδεδομένος τρόπος για την πιστοποίηση του χρήστη είναι με τη χρήση κωδικού. Οι χρήστες για ευκολία προτιμούν να έχουν απλούς κωδικούς, παρά κάτι σύνθετο και πιο ασφαλές.

Για να πραγματοποιηθεί μία brute force επίθεση κωδικού πρέπει πρώτα να εκτιμηθεί το μέγεθος, η περιπλοκότητα, και αν ο κωδικός λήγει μετά από κάποιο χρονικό διάστημα και οι χρήστες υποχρεούνται να δημιουργήσουν καινούριους μετά από αυτό.

Μερικές ερωτήσεις που πρέπει να απαντηθούν κατά τη διάρκεια των δοκιμών:

Ποιοι χαρακτήρες επιτρέπονται και ποιοι απορρίπτονται στον κωδικό? Μικρά κεφαλαία γράμματα, αριθμοί, σύμβολα?

Πόσο συχνά ένας χρήστης μπορεί να αλλάζει τον κωδικό του?

Πότε υποχρεούται ο χρήστης να αλλάζει τον κωδικό του? Μετά από 70 μέρες? Μετά που θα έχει κλειδωθεί το account του από λάθος προσπάθειες?

Πόσο συχνά ο χρήστης μπορεί να ξαναχρησιμοποιήσει τον κωδικό του? Η εφαρμογή κρατάει ιστορικό για τους κωδικούς που έχει χρησιμοποιήσει ένας χρήστης?

Πόσο διαφορετικός πρέπει να είναι ο επόμενος κωδικός από τον προηγούμενο?

Μπορεί ο χρήστης να χρησιμοποιήσει το username του ή άλλα στοιχεία από το account του π.χ. όνομα επώνυμο, στον κωδικό?

Account Lockout

Ο μηχανισμός του Lockout χρησιμοποιείται για να κάνει πιο δύσκολη μία brute force επίθεση στον κωδικό. Οι λογαριασμοί των χρηστών κλειδώνουν μετά από 3 με 5 ανεπιτυχείς προσπάθειες για login και μπορεί να ξεκλειδώσουν μετά από ένα προκαθορισμένο χρονικό διάστημα αυτόματα ή μετά από παρέμβαση του διαχειριστή. Ο μηχανισμός του account lockout απαιτεί μία ισορροπία μεταξύ του να προστατεύονται οι λογαριασμοί από κακόβουλη πρόσβαση και του να μπορούν οι χρήστες να κάνουν login στους λογαριασμούς τους αν κάνουν κάποιο λάθος.

Μετά από μία επιτυχημένη επίθεση brute force ένας κακόβουλος χρήστης μπορεί να έχει πρόσβαση σε:

Εμπιστευτικές πληροφορίες ή δεδομένα: πληροφορίες από το προφίλ του χρήστη, πληροφορίες τραπέζης, προσωπικές πληροφορίες κτλ.

Administration panels: Αυτές οι περιοχές χρησιμοποιούνται από τους διαχειριστές της εφαρμογής για να διαχειρίζονται το περιεχόμενο της web εφαρμογής, να προσθέτουν -αφαιρούν χρήστες, να αναθέτουν διαφορετικά δικαιώματα στους χρήστες κτλ.

Ευκαιρίες για επόμενες επιθέσεις: οι εξουσιοδοτημένες περιοχές που παίρνει πρόσβαση ο επιτιθέμενος μπορεί να περιέχουν ευπάθειας που δεν ήταν ορατές πριν και λειτουργίες που δεν είναι διαθέσιμες στους απλούς χρήστες.

Για να αξιολογήσεις το μηχανισμό του lockout ενάντια σε brute force επιθέσεις, στέλνεις κάποια άκυρα log in με λάθος κωδικό και μετά δοκιμάζεις με τον κανονικό για να διαπιστώσεις αν το account όντως κλειδώθηκε.

Cross-Site scripting (XSS)

Είναι ένα είδος επίθεσης όπου κακόβουλα scripts προσθέτονται σε web sites που ο χρήστης ή η εφαρμογή εμπιστεύονται. Οι επιθέσεις XSS πραγματοποιούνται όταν ο επιτιθέμενος χρησιμοποιεί τη web εφαρμογή για να στείλει κακόβουλο κώδικα, συνήθως σε μορφή script που εκτελεί ο browser, σε ένα διαφορετικό χρήστη. Τέτοια κενά ασφαλείας είναι ευρέως διαδεδομένα και συμβαίνουν οπουδήποτε η είσοδος του χρήστη φαίνεται στη σελίδα χωρίς να πραγματοποιηθεί κάποιος έλεγχος ή encoding.

Ο browser του χρήστη που δέχεται την επίθεση δεν έχει τρόπο να ξέρει ότι το script δεν πρέπει να το εμπιστευτεί και θα εκτελέσει κανονικά το script. Επειδή πιστεύει ότι έχει προέλθει από μία έμπιστη πηγή, το κακόβουλο script μπορεί να έχει πρόσβαση σε cookies, session tokens, και άλλη ευαίσθητη

πληροφορία που διατηρείται μεταξύ του browser και του site. Αυτά τα script μπορούν να ξαναγράψουν τον κώδικα της HTML.

Οι επιθέσεις XSS μπορούν να χωριστούν σε δύο κατηγορίες.

Stored XSS

Stored XSS είναι όταν το κακόβουλο script είναι μόνιμα αποθηκευμένο στο server, όπως σε μία βάση δεδομένων, ένα μήνυμα στο φόρουμ, κτλ. Το θύμα λαμβάνει το script από το server όταν ζητήσει την αποθηκευμένη πληροφορία.

Reflected XSS

Reflected XSS είναι όταν το input του χρήστη ή ένα μέρος του επιστρέφεται στη σελίδα που ζήτησε. Π.χ. Από μήνυμα λάθους ή αποτέλεσμα αναζήτησης κτλ. Όταν ο χρήστης εξαπατηθεί να πατήσει ένα κακόβουλο link, να κάνει submit μία προ δημιουργημένη φόρμα ή απλά να μπει σε κάποιο κακόβουλο site, ο κακόβουλος κώδικας ταξιδεύει στο web site που έχει την ευπάθεια και επιστρέφει πίσω στο browser του χρήστη. Στη συνέχεια ο browser εκτελεί των κώδικα επειδή προήλθε από ένα έμπιστο server.

Είναι δύσκολο να αναγνωριστούν ευπάθειες XSS σε μία εφαρμογή. Ο καλύτερος τρόπος είναι να πραγματοποιηθεί μία ανασκόπηση του κώδικα και να εντοπιστούν όλα τα σημεία όπου η είσοδος του χρήστη από ένα HTTP request μπορεί να εμφανιστεί ως έξοδο σε κάποιο σημείο της εφαρμογής. Μία ποικιλία από HTML tags μπορεί να χρησιμοποιηθεί για να μεταδώσει ένα κακόβουλο JavaScript.

Injection OS commands

Command injection είναι ένα είδος επίθεσης όπου στόχος είναι η εκτέλεση αυθαίρετες εντολές στο λειτουργικό σύστημα μέσα από μία ευπαθείς εφαρμογή. Οι επιθέσεις command injection συμβαίνουν όταν είναι πιθανόν η εφαρμογή να περνάει το input του χρήστη (forms, cookies, HTTP headers etc.) σε ένα system shell. Σε αυτή την περίπτωση ο επιτιθέμενος οι εντολές εκτελούνται με τα δικαιώματα που έχει η εφαρμογή. Αυτές οι επιθέσεις συνήθως συμβαίνουν γιατί δεν υπάρχει επαρκής έλεγχος στην είσοδο του χρήστη.

SQL injection

Η SQL injection είναι μία injection επίθεση όπου ο επιτηθέμενος μπορεί να εκτελέσει κακόβουλες SQL εντολές στη βάση δεδομένων της web εφαρμογής. Αυτή είναι μία από τις πιο παλιές και επικίνδυνες επιθέσεις γιατί μπορεί να επηρέασει κάθε σύστημα που χρησιμοποιεί μία βάση δεδομένων SQL.
Αξιοποιόντας μία τέτοια ευπάθεια, ένας επιτηθέμενος μπορεί να προσπεράσει τους μηχανισμούς authentication and authorization και να ανακτήσει τα δεδομένα ολόκληρης της βάσης δεδομένων. Μπορεί επίσης και να προσθέσει, να τροποποιείσει ή να διαγράψει δεδομένα από τη βάση, επηρεάζοντας έτσι την ακεραιότητα των δεδομένων.
Μπορεί να φτάσει μέχρι το σημείο όπου ο επιτηθέμενος θα έχει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα όπως, τα δεδομένα των πελατών, δεδομένα για τις συναλλαγές, για πνευματική ιδιοκτησία κ.α.

Πώς λειτουργεί μία επιθέση SQL injection

Για να εκτελέσει SQL queries σε μία εφαρμογή, αρχικά ο επιτηθέμενος πρέπει να βρεί σημεία εισόδου μέσα στη web εφαρμογή τα οποία είναι τα ίδια μέρος μέσα σε ένα SQL query. Στη συνέχεια για να μπορεί να συμβεί η επίθεση θα πρέπει η εφαρμογη να προσθέτει την είσοδο του χρήστη απευθείας μέσα σε μία δήλωση SQL. Ο επιτηθέμενος μπορεί να προσθέσει το δικό του κώδικα ο οποίος θα είναι μέρος του SQL query της εφαρμογής και θα εκτελεστεί στη βάση δεδομένων.

Ο ακόλουθος ψευδοκώδικας χρησιμοποιείται για να πιστοποιήσει την ταυτότητα των χρηστών.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd + "'"

# Execute the SQL statement
database.execute(sql)
```

Το παραπάνω script είναι ένα παράδειγμα για την πιστοποίηση των χρηστών χρησιμοποιώντας ένα όνομα χρήστη και ένα κωδικό τα οποία αποθηκεύονται σε μία βάση δεδομένων με όνομα table users και στήλες username και password.

Ο παραπάνω κώδικας είναι ευπαθείς σε επιθέσεις SQL επειδή ο επιτηθέμενος μπορεί να υποβάλλει κακόβουλα δεδομένα με τέτοιο τρόπο ούτως ώστε να αλλάξουν την SQL δήλωση που είναι κανονικά να εκτελεστεί στη βάση δεδομένων του server.

Ένα πολύ απλό παράδειγμα θα ήταν να βάλει στην είσοδο του κωδικού password' OR 1=1, το οποίο θα είχε ως αποτέλεσμα να εκτελεστεί η παρακάτω δήλωση:

```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

Μπορεί επίσης και να βάλει σε σχόλια την υπόλοιπη sql δήλωση για να έχει τον έλεγχο της εκτέλεσης

```
-- MySQL, MSSQL, Oracle, PostgreSQL, SQLite
' OR '1'='1' --
' OR '1'='1' /*
-- MySQL
' OR '1'='1' #
-- Access (using null characters)
' OR '1'='1' %00
' OR '1'='1' %16
```

Αφού εκτελεστούν τα queries, τα αποτελέσματα επιστρέφουν και έχουν ως αποτέλεσμα την παράκαμψη

του μηχανισμού πιστοποίησης. Σε μία τέτοια περίπτωση το πιο πιθανόν είναι η εφαρμογή να δώσει πρόσβαση στον επιτηθέμενο με τον λογαριασμό που θα βρει πρώτο στη βάση δεδομένων, οποίος συνήθως είναι του διαχειριστή του συστήματος.

Τι μπορεί να συμβεί από μία SQL επίθεση.

Η SQL είναι μία γλώσσα που έχει κατασκευαστεί για τη διαχείριση των δεδομένων, οπότε μπορεί να χρησιμοποιηθεί για να έχει πρόσβαση σε αυτά, να τα τροποποιήσει ή και να τα διαγράψει. Σε μερικές περιπτώσεις μία βάση δεδομένων μπορεί να τρέξει και εντολές λειτουργικού συστήματος μέσα από τις εντολές που εκτελεί.

Με βάση τα παραπάνω ένας επιτηθέμενος μπορεί:

- Να παραβιάσει το μηχανισμό πιστοποίησεις της ταυτότητας του χρήστη και να παρουσιαστεί ως κάποιος άλλος
- Μπορεί να έχει πρόσβαση σε εξουσιοδοτημένα δεδομένα
- Μπορεί να τροποποιήσει τα δεδομένα σε μία βάση
- Μπορεί να διαγράψει δεδομένα από μία βάση
- Με τις κατάλληλες προυποθέσεις μπορεί να εκτελέσει εντολές λειτουργικό συστήματος

Two-factor Authentication

Η πιστοποίηση με δύο παράγοντες είναι ένας επιπλέον μηχανισμός που προσθέτει στους λογαριασμούς των χτηστών περισσότερη ασφάλεια. Με τον όρο δύο παράγοντες εννοείται ότι για να έχει κάποιος πρόσβαση απαιτείται κάτι επιπλέον εκτός από τον κωδικό, για παράδειγμα ένα φυσικό αντικείμενο όπως ένα USB stick ή μία κάρτα, ένα κρυφό που είναι γνωστό μόνο στο χρήστη όπως PIN, TAN ή ακόμα και βιομετρικά χαρακτηριστικά όπως δακτυλικά αποτυπώματα, η ίριδα των ματιών ή η χροιά της φωνής.

Οι παράγοντες μπορεί να είναι σε κάποια από τις παρακάτω κατηγορίες:

Παράγοντες γνώσης

Είναι η πιο γνωστή κατηγορία και χρησιμοποιείται ευρέως για την πιστοποίηση των χρηστών, εδώ ο χρήστες καλείται να αποδείξει ότι γνωρίζει μία κρυφή πληροφορία για να μπορέσει να συνδεθεί.
Ο κωδικός είναι μία μυστική λέξη ή μία σειρά από χαρακτήρες που χρησιμοποιούνται για την πιστοποίηση του χρήστη και είναι η πιο γνωστή μέθοδος που χρησιμοποιείται. Γενικά ο κωδικός προβλέπεται να τον γνωρίζει ο χρήστης μνημονικά.

Μερικές κρυφές ερωτήσεις όπως «Σε ποιά πόλη γενήθηκες?» είναι παραδείγματα από παράγοντες γνώσεις, τα οποία βέβαια μπορεί να μη είναι και πολύ ασφαλή γιατί μπορεί να τα γνωρίζουν μία μεγάλη γκάμα ανθρώπων ή να είναι εύκολα με μία αναζήτηση.

Possession factors

Οι παράγοντες κατοχής είναι κάτι που μόνο ο χρήστης έχει κια χρησιμοποιούνται και αυτοί πολύ στην πιστοποίηση και έχουν τη λειτουργία ενός κλειδιού. Η βασική αρχή τους είναι ότι το κλειδί περιέχει ένα μυστικό το οποίο το γνωρίζουν μόνο η κλειδαριά και το κλειδί και ακριβώς το ίδιο χρησιμοποιείται και μεταξύ των πληροφοριακών συστημάτων. Ένα security token είναι ένα τέτοιο παράδειγμα.

Disconnected tokens

Αυτού του είδους οι συσκευές δεν έχουν κάποια σύνδεση με τον υπολογιστή του πελάτη. Συνήθως είναι ενσωματωμένες οθόνες που δημιουργούν κάποια στοιχεία για την πιστοποίηση, τα οποία πληκτρολογούνται από το χρήστη.

Connected tokens

Αυτά είναι συσκευές που είναι φυσικά συνδεμένες στον υπολογιστή και μπορούν να μεταφέρουν τα δεδομένα αυτόματα. Υπάρχουν συσκευές διαφόρων ειδών όπως είναι τα card readers.

Inherence factors

Αυτού του είδους σχετίζονται με το χρήστη και είναι συνήθως βιομετρικά χαρακτηριστικά όπως είναι τα δακτυλικά αποτυπώματα, συσκευές για αναγνώριση φωνής κ.α.

(12) (13) (36)

Ασφάλεια στο δίκτυο του IoT

Reconnaissance attacks

Οι επιθέσεις αναγνώρισης μπορεί να είναι ενεργητικές ή παθητικές. Γίνεται μία προσπάθεια από τον επιτηθέμενο για να πάρει πληροφορίες για το σύστημα που έχει ως στόχο ή για το δίκτυο. Η ενεργητική αναγνώριση περιλαμβάνει port scan, OS scan, ενώ η παθητική αναγνώριση είναι κυρίως παρατήρησης τις κίνησης στο δίκτυο ή το σύστημα για να συλέξει πληροφορίες για τις δυνατότητες και ευπάθειες που μπορεί να έχει.

Passive reconnaissance (παθητική αναγνώριση)

Ο επιτηθέμενος ξεκινάει και αναζητάει πληροφορίες στις DNS και whois βάσεις δεδομένων, όταν γνωρίζει το domain που είναι το σύστημα στόχος μπορεί να χρησιμοποιήσει εντολές όπως *nslookup, dig* και *whois* για να πάρει αρκετές πληροφορίες για το στόχο. Τέτοιες πληροφορίες δε σχετίζονται με το μηχάνημα στόχο και απλά φιλοξενούνται στο datacenter του ISP, οπότε με την IP μπορεί να πραγματοποιηθεί active reconnaissance στο μηχάνημα στόχο.

Active reconnaissance (ενεργητική αναγνώριση)

Η ενεργητική αναγνώριση μπορεί να ξεκινήσει με εργαλεία τα οποία στέλνουν πακέτα στον ανακαλυμένο σύστημα. Ένα από αυτά τα εργαλεία μπορεί να είναι το traceroute για να βρει την IP διεύθυνση των router και firewall που προστατεύουν το μηχάνημα στόχο. Σε περιπτώσεις όπου το firewall μπλοκάρει πακέτα UDP, μπορεί να χρησιμοποιηθεί το tcp traceroute εργαλείο για να κάνει το ίδιο είδος αναγνώρισης, όταν ένας επιτηθέμενος έχει όλες τις πληροφορίες μπορεί να χρησιμοποιήσει πιο ειδικά εργαλεία όπως το nmap και το hping για να πραγματοποιήσει μία επίθεση ενεργητικές αναγνώρισης στο στόχο του.

Το Nmap είναι ικανό να εντοπίσει το λειτουργικό σύστημα του στόχου χρησιμοποιώντας TCP fingerprinting. Το TCP fingerprinting χρησιμοποιεί προχωρημένη ανάλυση fingerprinting του TCP stack implementation. Το TCP πακέτο δημιουργείται παραμετροποιώντας κάποια flag και στέλνωντάς το στο απομακρυσμένο μηχάνημα. Το απομακρυσμένο λειτουργικό σύστημα βάση του TCP stack implementation στέλνει μία απάντηση με συγκεκριμένα flag ενεργά ή όχι. Αναλόγος τις απαντήσεις TCP που μαζεύονται για κάθε πακέτο που δημιουργήθηκε πραγματοποιεί μία έξυπνη υπόθεση του λειτουργικού συστήματος από τη βάση δεδομένων που έχει με TCP stack υπογραφές.
Το επόμενο βήμα για τον επιτηθέμενο είναι αν αποκαλύψει ποιά services είναι ενεργοποιημένα στους διαφορετικούς host και θα εκτελέσει ένα port scan με το Nmap. Στη συνέχεια όταν μαζέψει τις πληροφορίες που χρειάζεται θα χρησιμοποιήσει διαφορετικές τεχνικές για να αναγνωρίσει το λογισμικό που δουλεύει πίσω από αυτές τις πόρτες. Για αυτό το σκοπό συνήθως χρησιμοποιούνται τα telnet, ftp ή http client τα οποία μπορούν να συλλέξουν πληροφορίες για τον web server και την έκδοση που χρησιμοποιεί, ποιά plugins είναι σε χρήση κ.α. μετά μπορεί να εκτελέσει πιο ισχυρές επιθέσεις όπως DDoS, buffer-overflow , κάποια exploits κ.α.
Κάποια άλλα εργαλεία που μπορούν να χρησιμοποιηθούν για την ενεργήτική αναγνώριση είναι τα AMAP, Nessus, Scanrand και Paratrace.
(15) (16) (36)

Buffer overflow

Στην επιστήμη των υπολογιστών και στον προγραμματισμό, το buffer overflow είναι μία ανωμαλία όπου ένα πρόγραμμα καθώς γράφει δεδομένα στον buffer, ξεπερνάει τα όρια που είναι διαθέσιμα και γράφει σε γειτονικές θέσεις μνήμης.

Οι buffers είναι θέσεις μνήμης οι οποίες έχουν σκοπό να διατηρίσουν δεδομένα, συχνά όταν μεταφέρονται από ένα τμήμα ενός προγράμματος σε ένα άλλο ή μεταξύ των προγραμμάτων. Τα buffer overflows μπορούν να προκληθούν από την είσοδο του χρήστη. Αν κάποιος υποθέσει ότι οι είσοδοι θα είναι μικρότερες από ένα συγκεκριμένο μέγεθος και ο buffer έχει δημιουργηθεί να έχει αυτό το μέγεθος, αν μία ανώμαλη συναλλαγή παράγει περισσότερα δεδομένα μπορεί αυτά τα δεδομένα να γραφτούν και μετά το τέλος του buffer. Αν τα δεδομένα που θα γραφτούν περεταίρω είναι εκτελέσιμος κώδικας αυτό μπορεί να έχει αποτέλεσμα στην ασταθή λειτουργία του προγράμματος, συμπεριλαμβανομένου σφάλματα στην μνήμη, λάθος αποτελέσματα ή και να διακοπεί η λειτουργία του.

Η εκμετάλευση ενός buffer overflow είναι μία πολύ γνωστή ευπάθεια. Σε πολλά συστήματα η μνήμη ενός προγράμματος ή ενός συστήματος είναι προκαθορισμένη. Στέλνωντας δεδομένα που έχουν σκοπό να δημιουργήσουν ένα buffer overflow, είναι πιθανόν να γραφτεί σε περιοχές της μνήμης όπου είναι γνωστό ότι περιέχουν εκτελέσιμο κώδικα και να τον αντικαταστήσουν με κακόβουλο κώδικα. Οι buffers είναι ευρέως διαδεδομένοι στον κώδικα των λειτουργικών συστημάτων, οπότε είναι εφικτό να πραγματοποιηθούν επιθέσεις που να αυξήσουν τα προκαθορισμένα όρια πρόσβασης στο σύστημα και να παρέχουν πλήρης πρόσβαση στους πόρους του συστήματος.

Το buffer overflow συμβαίνει όταν δεδομένα γραφτούν σε ένα buffer που επίσης ανατρέπουν τιμές στη μνήμη που είναι γειτονικές με αυτές του buffer λόγο του μη επαρκούς ελέγχου που συμβαίνει. Αυτό μπορεί να συμβεί όταν αντιγράφονται δεδομένα από ένα buffer σε ένα άλλο χωρίς πρώτα να ελεγχθούν αν τα δεδομένα χωράνε στο δεύτερο buffer.

Οι τεχνικές για να εκμεταλευτεί κάποιος μία ευπάθεια buffer overflow διαφέρουν ανάλογα την αρχιτεκτονική, το λειτουργικό σύστημα και την περιοχή της μνήμης. Για παράδειγμα μία επίθεση στο *heap* διαφέρει αρκετά από μία επίθεση στο *call stack*.

Stack-based exploitation

Ένας χρήστης μπορεί να εκμεταλλευτεί μία ευπάθεια stack-based buffer overflow για να παραποιήσει τη ροή του προγράμματος για δικό του σκοπό με διάφορους τρόπους όπως:

- Να αντικαθαστήσει μία τοπική μεταβλητή η οποία είναι κοντά στη μνήμη με αυτή του buffer στη στοίβα, με σκοπό να αλλάξει τη συμπεριφορά του προγράμματος.
- Να αντικαθαστήσει τη διεύθυνση επιστροφής στο stack frame. Μόλις επιστρέψει η συνάρτηση, η εκτέλεση θα συνεχιστεί στη διεύθυνση που έχει οριστεί από τον επιτηθέμενο.
- Να αντικαθαστήσει τον pointer μιας συνάρτησης η οποία εκτελείται.
- Να αντιγράψει μία τοπική μεταβλητή ενός διαφορετικού stack frame, η οποία μπορεί να χρησιμοποιηθεί από μία συνάρτηση που κατέχει αυτό το frame αργότερα.

Αν η διεύθυνση η οποία έχει σκοπό ο επιτηθέμενος να παραποιήσει είναι άγνωστη, το να εκμεταλευτεί μία ευπάθεια buffer overflow και να προκαλέσει εκτέλεση απομακρυσμένου κώδικα γίνεται πολύ πιο δύσκολο. Μία τεχνική που χρησιμοποιείται για να εκμεταλευτούν τέτοιες περιπτώσει ονομάζεται “trampolining”. Σε αυτήν την τεχνική ο επιτηθέμενος θα βρει τον pointer του ευπαθή buffer και θα υπολογίσει την τοποθεσία του κώδικα που θα στείλει σχετικά με αυτόν τον pointer. Αργότερα θα χρησιμοποιήσουν αυτόν τον κώδικα για να εκετλέσουν εντολές που είναι ήδη στη μνήμη, οι οποίες με τη σειρά τους θα εξτελέσουν των κώδικα που έχει στείλει ο επιτηθέμενος.

Heap-based exploitation

Ένα buffer overflow που πραγματοποιήται στην περιοχή του heap αναφέρεται και ως heap overflow και μπορεί να εκμεταλευτεί με διαφορετικό τρόπο από το stack-based overflow. Η μνήμη στο heap είναι διανέμεται δυναμικά κατά την εκτέλεση του προγράμματος. Η εκμετάλλευση γίνεται μετατρέποντας αυτά τα δεδομένα με συγκεκριμένο τρόπο ούτως ώστε να προκαλέσουν την εφαρμογή να γράψει πάνω από τις εσωτερικές δομές όπως τους pointers σε μία λίστα. Η τεχνική του heap overflow αντιγράφει πάνω στις δυναμμικές θέσεις μνήμης και χρησιμοποιεί τον pointer του αποτελέσματος για να χρησιμοποιήσει στη συνέχεια τον pointer του προγράμματος.

DDos

Στους υπολογιστές μία επίθεση άρνησης εξυπηρέτησης είναι μία ηλεκτρονική επίθεση όπου ο επιτηθέμενος προσπαθεί να κάνει το μηχάνημα ή το δίκτιο που έχει στόχο, μη διαθέσιμο για τους χρήστες που προορίζεται να είναι διακόπτοντας τις υπηρεσίες που εκτελούνται σε ένα server ο οποίος είναι συνδεμένος στο Internet. Τυπικά αυτή η επίθεση επιτυγχάνεται στέλνοντας ένα μεγάλο αριθμό αιτήσεων στο μηχάνημ-στόχο με σκοπό να υπερφορτωθεί και να το εμποδίσει από το να μπορεί να διαχειριστεί τον τεράστιο όγκο δεδομένων που δημιουργείται και να δεχτεί και νέα αιτήματα από τους χρήστες που κανονικά θα εξυπηρετούσε. Θα μπορούσε να πει κανείς ότι είναι ανάλογο με μία ομάδα ανθρώπων οι οποίοι έχουν μαζευτεί στην είσοδο ενός μαγαζιού και δεν αφήνουν τους πελάτες να περάσουν μέσα.

Τα είδη αυτών των επιθέσεων χαρακτηρίζονται ρητά από τον επιτηθέμενο για να εμποδίσει τους χρήστες μιας υπηρεσίας από το να τη χρησιμοποιήσουν. Σε μία επίθεση άρνησης εξυπηρέτησης, η εισερχόμενη κίνηση που πλυμμηρίζει το στόχο συνήπως προέρχεται από διαφορετικές πηγές ίσως και χιλιάδες αν όχι περισσότερες. Η αποτελεσματικότητα που έχει κάνει αδύνατο να σταματήσει η επίθεση απλά μπολοκάροντας μία μόνο διεύθυνση IP και είναι πολύ δύσκολο να διαχοριστεί ένας κανονικός χρήστης από τον επιτηθέμενο μέσα σε τόσο μεγάλο όγκο δεδομένων. Οι περισσότερες επιθέσεις χρησιμοποιούν πάρα πολλά μηχανήματα και πλαστογραφούν τη διεύθυνση IP αυτών των μηχανημάτων, οπότε είναι πολύ δύσκολο να αναγνωριστεί η πραγματική τοποθεσία των επιτηθέμενων για να μπορέσει να σταματήσει μία τέτοια επίθεση.

Συμπτώματα

Μερικά συμπτώματα των DDos επιθέσεων είναι:

- Πολύ αργή κίνηση του δικτύου
- Κάποιοι πόροι γίνονται μη διαθέσιμοι
- Αδύνατη πρόσβαση σε μερικούς πόρους
- Μεγάλη αύξηση στον αριθμό των spam emails που λαμβάνονται (η επίθεση αυτή λέγεται και e-mail bomb)
- Αποσύνδεση των ασύρματων και των ενσύρματων συνδέσεων
- Μη δυνατή πρόσβαση στα services για μεγάλο χρονικό διάστημα

Αν η επίθεση πραγματοποιηθεί σε μεγάλη κλίμακα, ολόκληρες γεωγραφικές περιοχές μπορεί να χάσουν τη δυνατότητα σύνδεσής τους χωρίς τη γνώση του επιτηθέμενου, από μία λάθος ρύθμιση ή από αδύναμο εξοπλισμό του δικτύου. (17) (16)

Bluetooth

Μερικές ευπάθειες στην τεχνολογία του Bluetooth:

1. Τα κλειδιά για την κρυπτογράφιση είναι στατικά και χρησιμοποιούται τα ίδια σε κάθε επικοινωνία.
2. Το να χρησιμοποιούνται συνεχώς τα ίδια κλειδιά είναι πολύ εύκολο να πραγματοποιηθούν επιθέσεις eavesdropping και spoofing.
3. Οι κωδικοί PIN μπορεί να είναι πολύ μικροί.
4. Η δημιουργία των κωδικών PIN δεν είναι τόσο τυχαία.
5. Τα κλειδιά SSP ECDH είναι στατικά ή πολύ αδύναμα ως προς την πολυπλοκότητα, έτσι είναι πολύ πιθανών ένα σύστημα να πέσει θύμα επιθέσεων MITM.
6. Οι προσπάθειες για την πιστοποίηση του χρήστη δεν έχουν κάποιο όριο, οπότε ένας επιτηθέμενος μπορεί πολύ εύκολα να δοκιμάσει μία πληθόρα από πιθανούς κωδικούς μέχρι να βρει τον σωστό.
7. Η δύναμη της ψευδο-τυχαίας γενήτριας αριθμών (PRNG) δεν είναι γνωστή, η οποία συνήθως δημιουργεί στατικούς ή περιοδικούς αριθμούς οι οποίοι περιορίζουν την αποτελεσματικότητα του μηχανισμού ασφαλείας.
8. Το μέγεθος τους κλειδιού κρυπτογράφησης κυμαίνεται.
9. Σε μερικές περιτπώσεις δεν υπάρχει πιστοποίηση του χρήστη.
10. Οι συσκευές μένουν για πολύ χρονικό διάστημα στη φάση της αναζήτησης και είναι ευπαθή σε επιθέσεις.

Απειλές στο Bluetooth:

Το Bluetooth προσφέρει πολλά πλεονεκτήματα, αλλά έχει και πολλά ρίσκα. Η τεχνολογία Bluetooth και οι συσκευές που σχετίζονται με αυτήν είναι ευάλωτες σε ασύρματες επιθέσεις όπως denial of service, eavesdropping, MITM επιθέσεις, παραποίηση μηνυμάτων. Μερικές από τις πιο γνωστές είναι:

Bluesnarfing. Το bluesnarfing επιτρέπει σε ένα επιτηθέμενο να έχει πρόσβαση σε μία συσκευή που έχει ενεργοποιημένο το Bluetooth εκμεταλεύοντας κενά στο firmware σε πιο παλιές συσκευές. Αυτή η επίθεση προκαλεί μία σύνδεση με μία συσκευή Bluetooth, επιτρέποντας την πρόσβαση σε δεδομένα που είναι αποθηκευμένα στη συκευή συμπεριλαμβανομένου και το IMEI. Το IMEI είναι ένα μοναδικό αναγνωριστικό για κάθε συσκευή όπου ένας επιτηθέμενος μπορεί ενδεχωμένος να χρησιμοποιήσει για να δρομολογήσει όλη την εισερχόμενη κίνηση από τη συσκευή του χρήστη στη συσκευή του επιτηθέμενου.

Bluejacking. Το bluejacking είναι μία επίθεση που διεξάγεται σε συσκευές που έχουν ενεργοποιημένο το Bluetooth, όπως κινητά τηλέφωνα. Ένας επιτηθέμενος προκαλεί bluejacking στέλνωντας μη αναμενόμενα μηνύματα στο χρήστη της Bluetooth συσκευής. Τα μηνύματα κάθε αυτά δεν προκαλούν κάποια βλάβη στη συσκευή του χρήστη, αλλά μπορεί να δελεάσουν το χρήστη να απαντήσει σε αυτά ή και να δημιουργήσει κάποια επαφί στο τηλέφωνό του. Αυτού του είδους οι επιθέσεις αναφέρονται ως spam και phishing επιθέσεις δημιουργημένες για χρήστες e-mail. Το bluejacking μπορεί να προκαλέσει ζημιά όταν ο χρήστης ξεκινάει να απαντήσει σε ένα μήνυμα bluejacking με κακή πρόθεση.

Bluebugging. Το bluebugging εκμεταλεύεται ένα κενό ασφαλείας στο firmware κάποιον παλιών συσκευών Bluetooth για να έχει πρόσβαση στη συσκευή και στη λειτουργία της. Αυτή η επίθεση χρησιμοποιεί τις εντολές τις συσκευής χωρίς τη γνώση του χρήστη, επιτρέποντας έτσι στον επιτηθέμενο

να έχει πρόσβαση σε δεδομένα, μηνύματα και να εκμεταλευτεί όλα τα services που υποστηρίζει η συγκεκριμένη συσκευή.

Denial of Service. Όπως πολλές ασύρματες τεχνολογίες, το Bluetooth είναι ευάλωτο σε επιθέσεις DoS. Μία τέτοια επίθεση καθιστά τη λειτουργία της συκευής μη εφικτή και απορροφά μεγάλα ποσά ενέργειας της μπαταρίας.

Fuzzing Attacks. Οι επιθέσεις Bluetooth fuzzing attacks αποτελούνται από μηνύματα κατασκευασμένα από τον επιτηθέμενο προς τη Bluetooth συσκευή τα οποία έχουν σκοπό να παρατηρήσουν πως αντιδράει η συσκευή σε αυτά τα μηνύματα. Αν η λειτουργία της συσκευής μειωθεί ή σταμματήσει λόγο αυτών των μηνυμάτων, υπάρχει σοβαρό κενό στην ασφάλεια της συσκευής στη στοίβα πρωτοκόλλου.

Secure Simple Pairing Attacks. Ένας μεγάλος αριθμός από τεχνικές επιβάλλουν στη συσκευή να χρησιμοποιήσει SSP και μετά να εκμεταλευτούν την έλειψη προστασίας που υπάρχει στις επιθέσεις Man In The Middle. (34) (35)

Eavesdropping

Το Eavesdropping είναι όταν κάποιος ακούει κρυφά μία ιδιωτική συζήτηση που κάνουν κάποιοι χωρίς να έχει πάρει τη συγκατάθεσή τους και θεωρείται κάτι ανήθικο. Είναι μία επίθεση που μπορεί να πραγματοποιηθεί σε τηλεφωνικές γραμμές, σε email, και σε άλλες μεθόδους όπου χρησιμοποιείται ανταλλαγή άμεσων μηνυμάτων.

Όσο αφορά το δίκτυο υπάρχει ένα επίπεδο δικτύου που στόχο έχει τη συλλογή μικρών πακέτων από το δίκτυο που μεταδίδονται από άλλους και με σκοπό τη συλλογή πληροφοριών μέσα από αυτά. Αυτού του είδους η επίθεση είναι από τις πιο αποτελεσματικές γιατί συνήθως οι πληροφορίες που μεταδίδονται δεν είναι κρυπτογραφημένες. (36)

Unencrypted Services

Σε μία επικοινωνία που δε χρησιμοποιείται κάποια κρυπτογράφηση, είναι πολύ πιο εύκολο για ένα επιτιθέμενο να παρακολουθήσει την κίνηση και να χρησιμοποιήσει Eavesdropping. (18) (19)

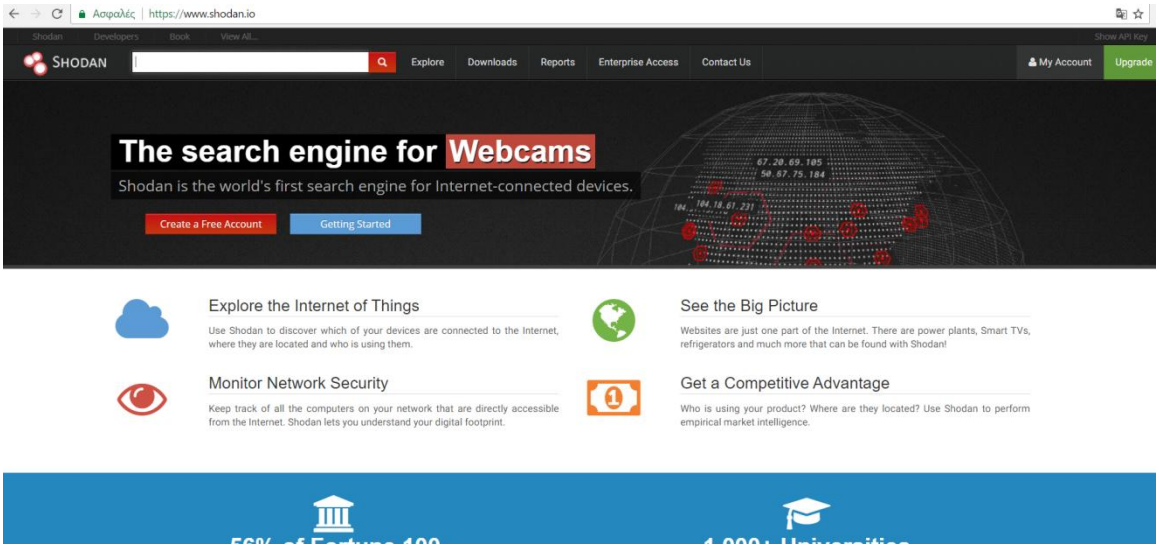
Ασφάλεια στο φυσικό επίπεδο

Η τυποποίηση των μέτρων ασφαλείας για το IoT δεν είναι πρακτική λόγο της μεγάλης πικοιλίας των προϊόντων που υπάρχουν και το κάθε ένα έχει διαφορετικές ανάγκες ασφάλειας. Για παράδειγμα το να ασφαλήσεις ένα θερμοσίφωνα είναι πολύ πιο διαφορετικό από το να ασφαλήσεις μία κάμερα που παρακολουθεί ένα μωρό.
Έτσι και η φυσική ασφάλεια θα πρέπει να εφαρμοστεί διαφορετικά στην ποικιλία των IoT συσκευών. Η φυσική ασφάλεια που θα εφαρμοστεί για ένα έξυπνο αυτοκίνητο θα είναι διαφορετική από αυτή που θα εφαρμοστεί για μία έξυπνη κλειδαριά.
Οι κατασκευαστές των IoT συσκευών, έχουν καταλάβει ότι η επιτυχία των προϊόντων τους εξαρτάται από την ασφάλειά τους, και έχουν ξεκινήσει να συνδιάζουν τη φυσική ασφάλεια με την κυβερνασφάλεια.
Πολλοί κατασκευαστές χρησιμοποιούν ενσωματωμένα μέτρα ασφαλείας και επεκτείνουν την ασφάλεια από τις συσκευές στο cloud ή στις web εφαρμογές που χρησιμοποιούν οι IoT συσκευές τους.
Επιπλέον προσπαθούν να μειώσουν την πρόσβαση που οι IoT συσκευές τους προσφέρουν στους hackers και τους εγκληματίες. Επίσης οι εταιρίες προσπαθούν να ελλαχιστοποιήσουν στις συσκευές τα πιθανά λάθη που μπορεί να προκαλέσουν παραβίαση των δεδομένων. Αυτός ο λόγος τους οδηγεί στο να χτίσουν περισσότερο ασφαλή hardware για τις συσκευές τους και να κωδικοποιήσουν τα τοπικά δεδομένα που αποθηκεύονται σε αυτές.
(20) (21)

Shodan: The World's Most Dangerous Search Engine

Σχεδόν όλοι έχουν χρησιμοποιήσει μηχανές αναζήτησης όπως είναι το Google ή το Bind για να βρουν πληροφορίες στο ίντερνετ. Οι μηχανές αναζήτησης ψάχνουν σε όλο το διαδίκτυο και ταξινομούν τις σελίδες που βρίσκουν ώστε να μπορεί να πραγματοποιηθεί μετά μία αναζήτηση χρησιμοποιώντας κάποιες λέξεις κλειδιά.

Φανταστείτε μία μηχανή αναζήτησης που αντί να ψάχνει για ιστοσελίδες, ψάχνει για τα banner από κάθε IP. Με άλλα λόγια όταν συνδέεται σε μία IP διεύθυνση η συσκευή παρέχει κάποιες πληροφορίες γι αυτήν προσδιορίζοντας τον εαυτό της και κάποιες παραμέτρους της. Αυτές οι πληροφορίες μπορεί να είναι πολύ χρήσιμες στην αναζήτηση ευπαθών η μη προστατευμένων συσκευών. Έτσι μπορεί να γίνει αναζήτηση για ένα συγκεκριμένο είδος π.χ. Cisco routers ή για μία συγκεκριμένη περιοχή π.χ. California και ακόμα και συστήματα SCADA. Με τόσες πολλές συσκευές του IoT που κυκλοφορούν χωρίς την απαραίτητη ασφάλεια, τέτοια πληροφορία θα ήταν πολύτιμη στους Hackers.
Μία τέτοια μηχανή υπάρχει. Σχεδιάστηκε το 2009 από τον John Matherly και ονομάζεται Shodan και η διεύθυνσή της είναι www.shodan.io. (22) (23)



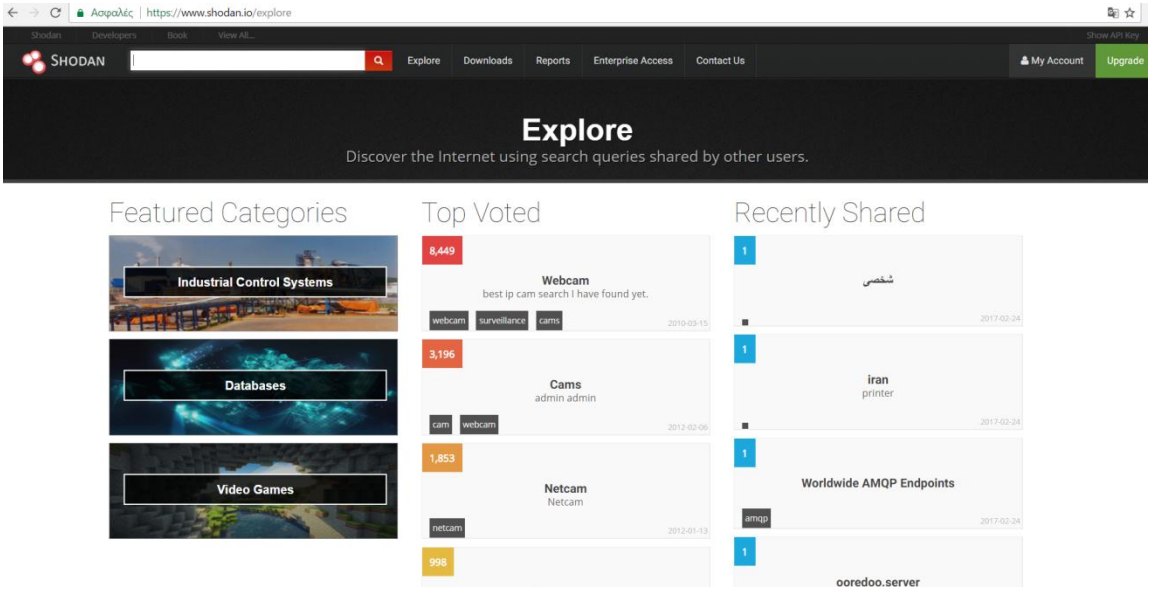
Εικόνα 1 Shodan front page

Στην ουσία το Shodan ψάχνει όλες τις διευθύνσεις IP και προσπαθεί να εξάγει από αυτές τις σχετικές πληροφορίες, χωρίς όμως να γνωρίζει αν οι πληροφορίες που βρήκε είναι ισχύουν κιόλας για την κάθε συσκευή. Μερικές εταιρίες σκόπιμα αλλάζουν το banner τους για να αποφύγουν τους επιτιθέμενους και το Shodan, αλλά είναι πολύ λίγες αυτές.

Χρησιμοποιώντας το Shodan

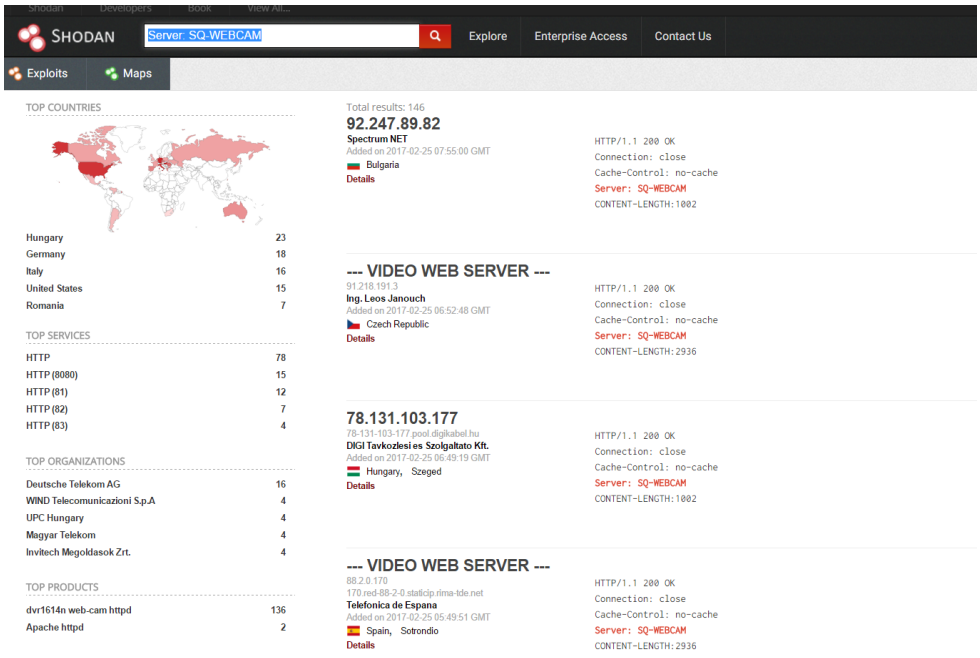
Το πρώτο βήμα για να χρησιμοποιήσεις το Shodan είναι να κάνεις ένα account. Χωρίς εγγραφή οι δυνατότητες είναι πολύ λίγες.

Μερικές από τις πιο συχνές αναζητήσεις είναι στο tab Explore.



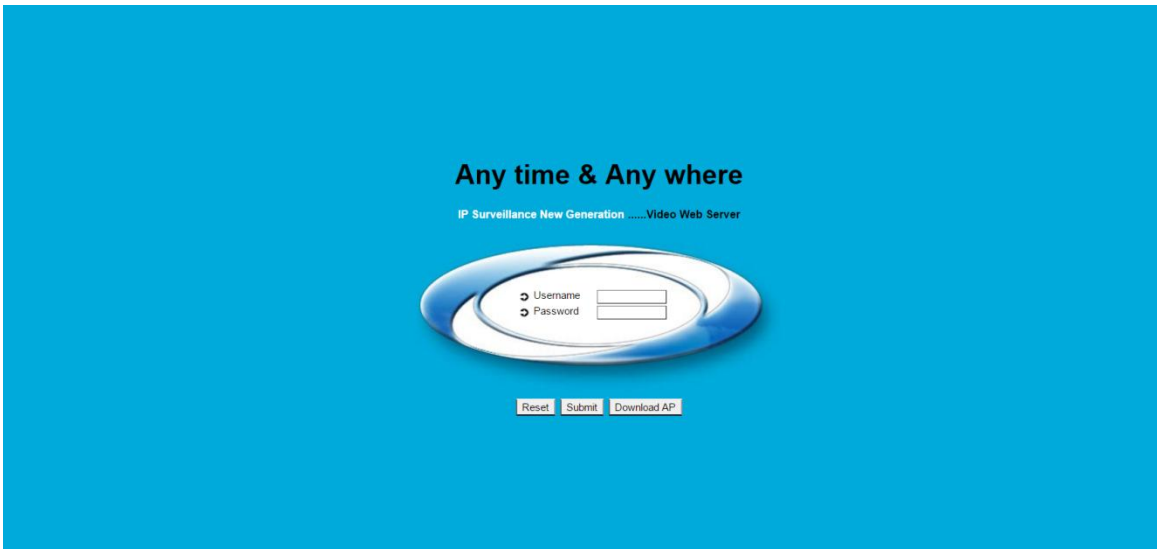
Εικόνα 2 Explore tab

Στην κορυφή των αναζητήσεων στα "Top Voted" είναι το "Webcam". Όταν επιλεγεί το Shodan δημιουργεί μία φράση αναζήτησης η οποία στην προκειμένη περίπτωση είναι "Server: SQ-WEBCAM".



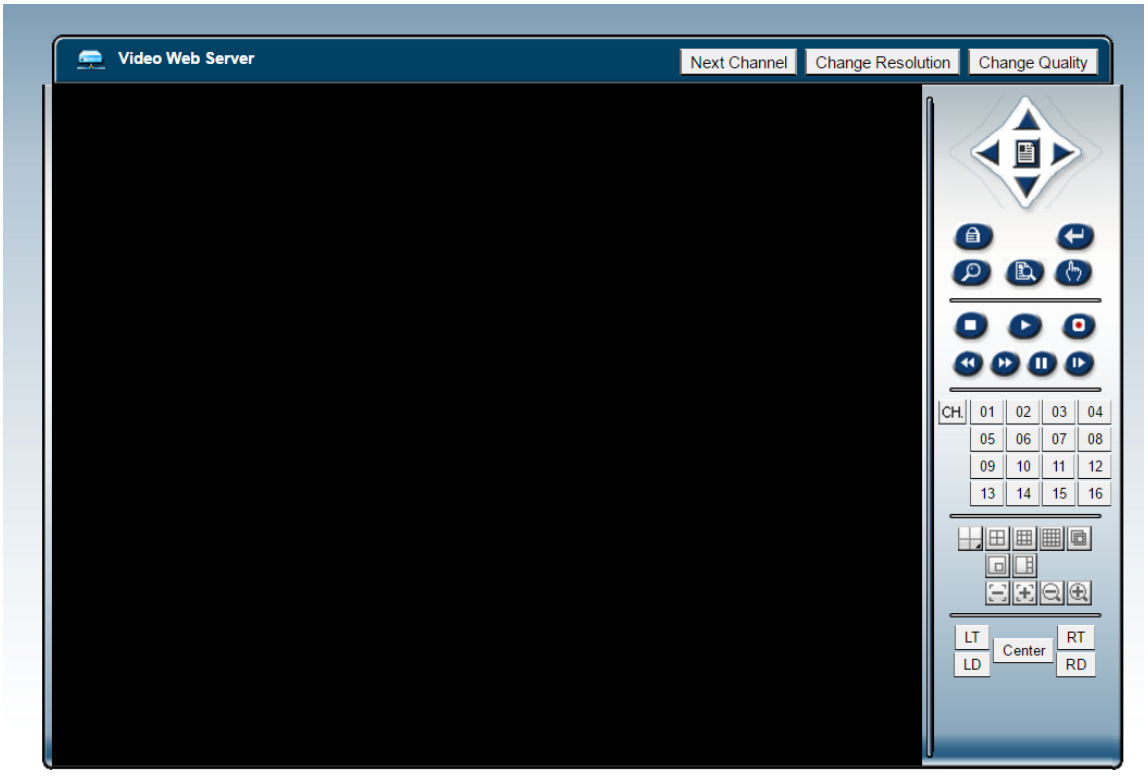
Εικόνα 3 Search: Server: SQ-WEBCAM

Επιλέγοντας σε οποιαδήποτε από αυτές τις καταχωρήσεις θα μας οδηγήσει σε μία συσκευή που είναι συνδεδεμένη στο Internet. Επιλέγοντας μία από αυτές μας εμφανίζει τη login σελίδα για τη συσκευή.



Εικόνα 4 Login promt

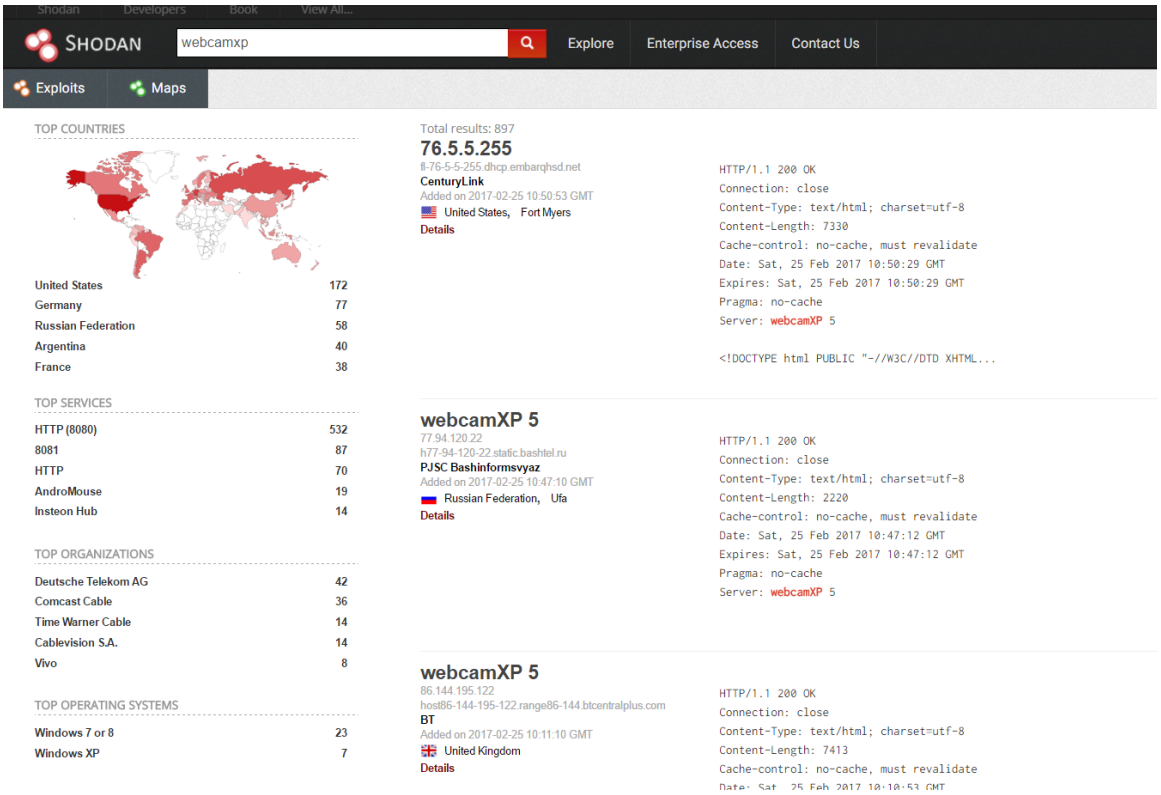
Και χρησιμοποιώντας τα default login/password έχουμε πρόσβαση στο admin panel της συσκευή.



Εικόνα 5 Admin panel

Webcamxp

Μία άλλη γνωστή αναζήτηση για web κάμερες είναι η "Webcamxp". Αυτές οι συγκεκριμένες web κάμερες είναι σχεδόν πάντα απροστάτευτες, οπότε όταν βρεθεί μία είναι πολύ εύκολη η πρόσβαση σε αυτήν. Το shodan με αυτή τη φράση βρίσκει 900 κάμερες.



Εικόνα 6 Search: Webcamxp

Παρακάτω είναι μία φωτογραφία από ένα γραφείο-σπίτι στο τάδε μέρος...

Shodan Search Syntax

Εκτός από τις web cams με το shodan μπορείς να αναζητήσεις πάρα πολλά είδη συσκευών. Το shodan σου επιτρέπει να είσαι πολύ συγκεκριμένος με τις αναζητήσεις σου. Μπορείς για παράδειγμα να βρεις συσκευές με βάση την πόλη, τη χώρα, την IP διεύθυνση ή τη φυσική διεύθυνση χρησιμοποιώντας το CIDR. Μπορείς να είσαι τόσο συγκεκριμένος που να κάνεις αναζήτηση με βάση GPS συντεταγμένες, το hostname, το λειτουργικό σύστημα και την πόρτα.

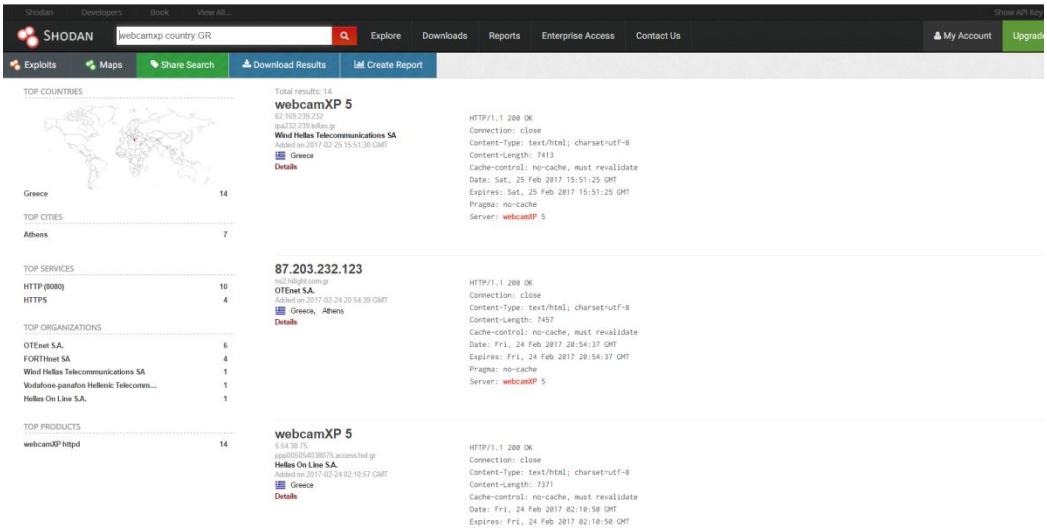
Παρακάτω είναι μερικοί όροι που μπορεί να χρησιμοποιηθούν στις αναζητήσεις με την ακόλουθη σύνταξη:

<keyword>:<value>

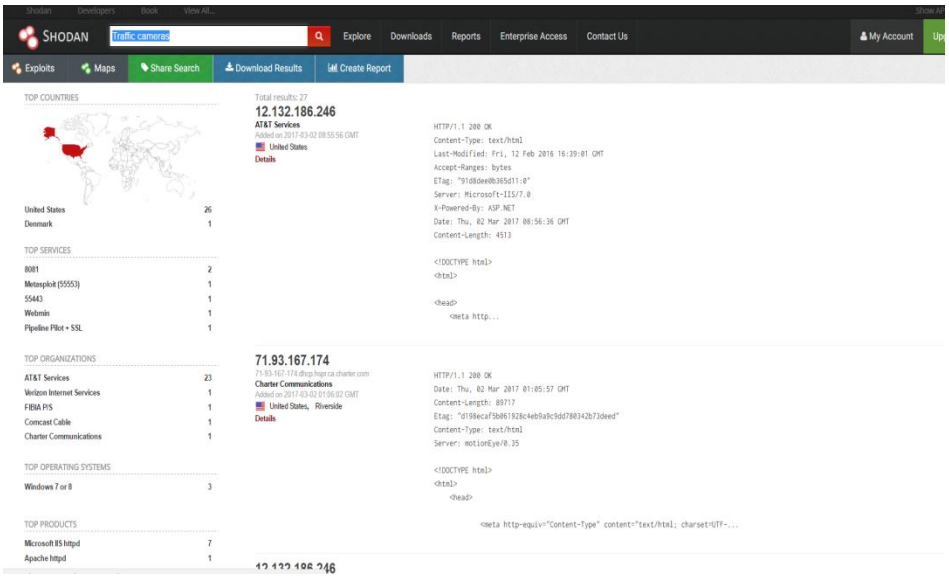
- **city**: βρίσκει συσκευές σε μία συγκεκριμένη πόλη
- **country**: βρίσκει συσκευές σε μία συγκεκριμένη χώρα
- **geo**: μπορείς να χρησιμοποιήσεις συντεταγμένες
- **hostname**: τιμές που αντιστοιχούν στο hostname
- **net**: αναζήτηση με βάση την IP ή το CIDR
- **os**: αναζήτηση με βάση το λειτουργικό σύστημα
- **port**: βρίσκει πόρτες που είναι ανοιχτές
- **before/after**: βρίσκει αποτελέσματα ανάμεσα σε μία χρονική περίοδο

Για παράδειγμα για να ψάξεις webcamxp στην Ελλάδα μπορείς χρησιμοποιήσεις ένα τέτοιο όρο

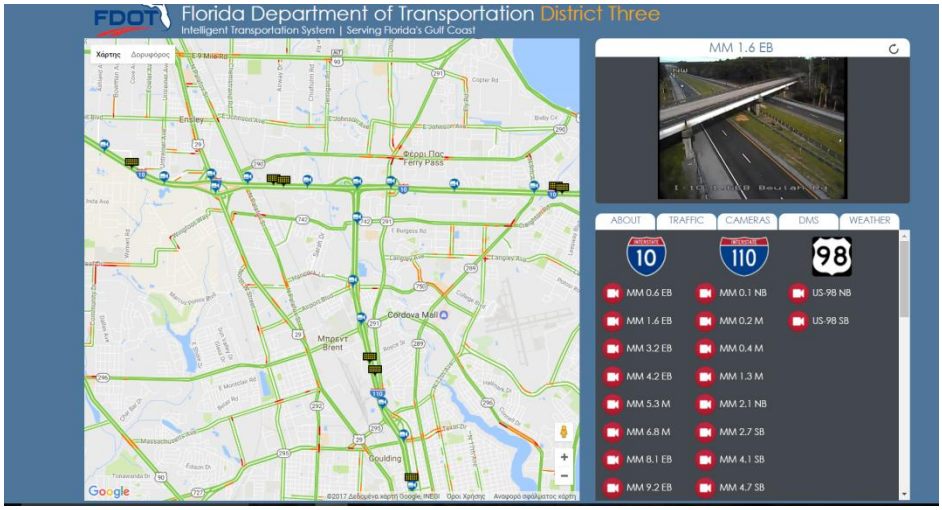
webcamxp country:GR



Εικόνα 7 Webcamxp country:GR

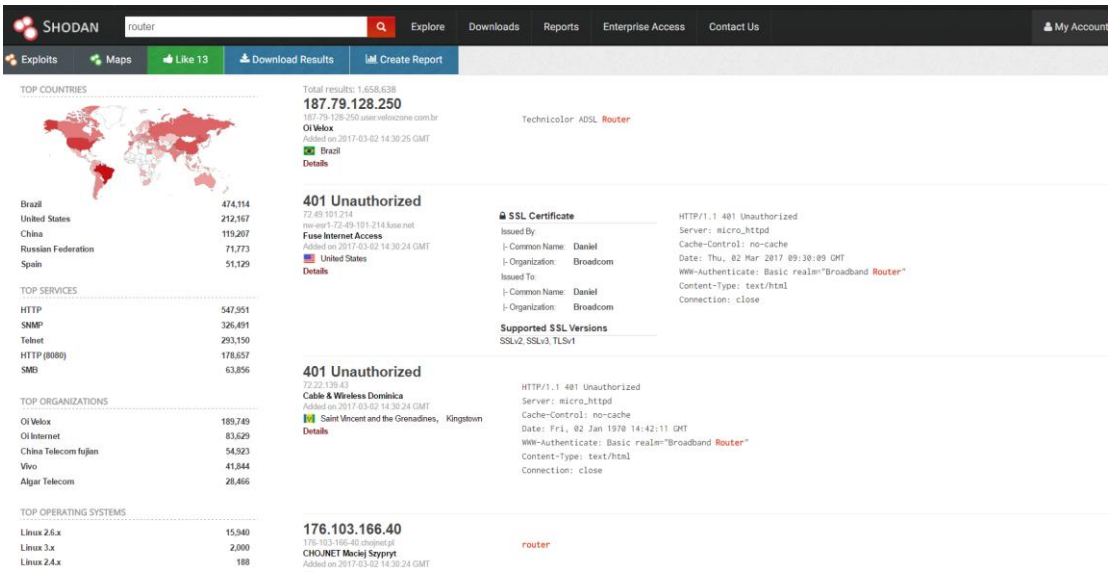


Εικόνα 8 Traffic search



Εικόνα 9 Live traffic

Αναζήτηση για routers, τα περισσότερα είναι χωρίς προστασία ή με τους προεπιλεγμένους κωδικούς και usernames.

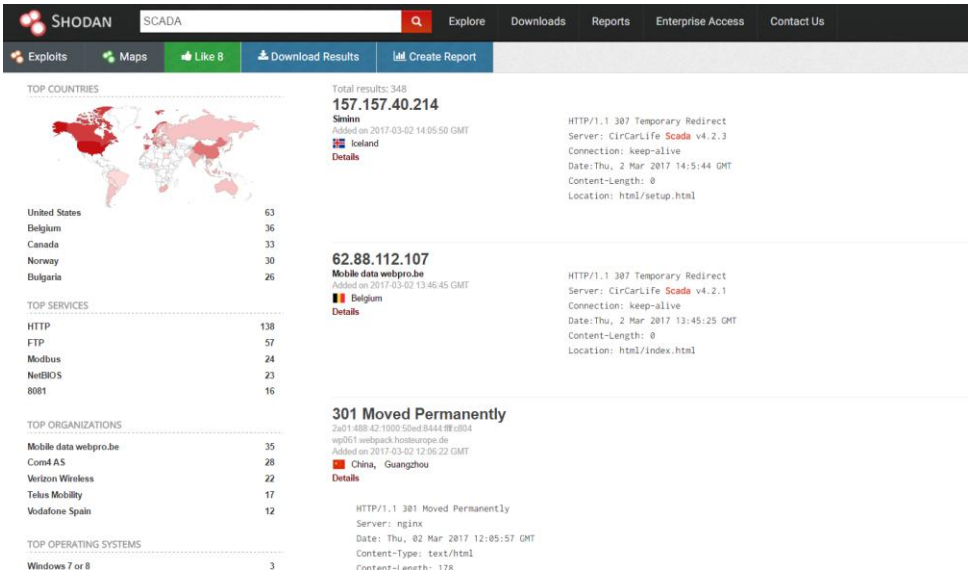


Εικόνα 10 Router search

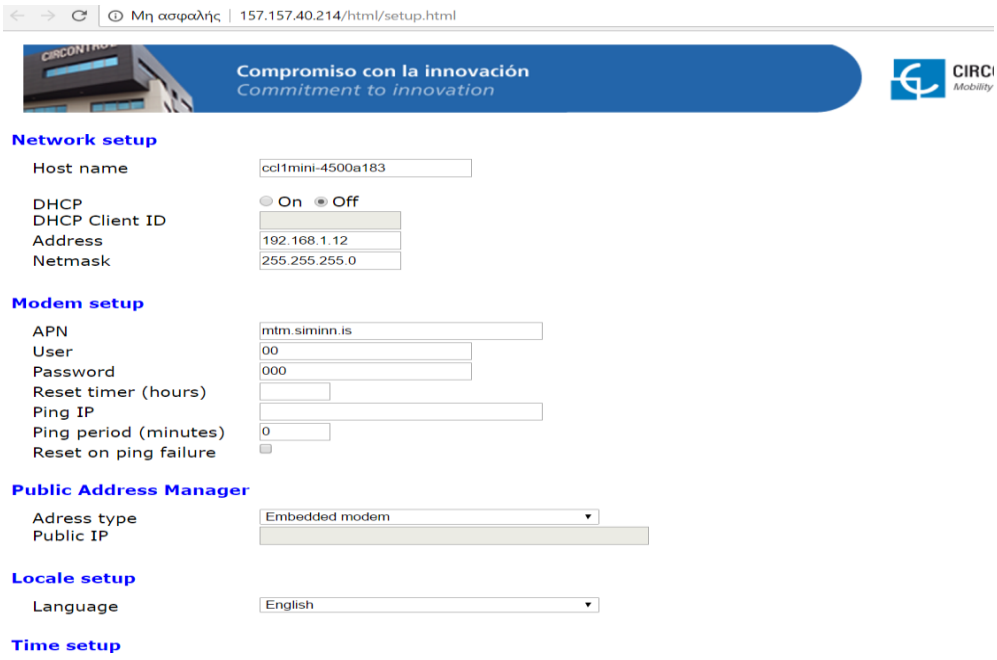
Εικόνα 11 Router details

Μία από τις πιο τρομακτικές χρήσεις του Shodan είναι η εύρεση συστημάτων SCADA (supervisory control and data acquisition) τα οποία έχουν web interface. Τέτοιες συσκευές ρυθμίζουν το ηλεκτρικό δίκτυο, το πότισμα των φητών, εργοστάσια πυρηνικής ενέργειας κ.α.

Τα συστήματα SCADA είναι οι πιο πιθανοί στόχοι σε περιπτώσεις κυβερνο-τρομοκρατίας, όπου οι αντίπαλοι προσπαθούν να απενεργοποιήσουν την υποδομή ο ένας του άλλου και με το να έχει κάποιος πρόσβαση στις ρυθμίσεις της ηλεκτρικής ενέργειας αυτό γίνεται πολύ εύκολα.



Εικόνα 12 Search: SCADA



Εικόνα 13 Open SCADA system

Το Shodan παρόλο που είναι ένα επικίνδυνο εργαλείο, είναι η ζωντανή απόδειξη του τι μπορεί να συμβεί όταν συσκευές με ελλιπή ασφάλεια έρχονται στη ζωή μας. Με μία γρήγορη αναζήτηση μπορεί κάποιος να βρει ευπαθείς web κάμερες από σχολεία μέχρι εργοστάσια μέχρι ιδιωτικές κάμερες για την επίβλεψη μικρών παιδιών.

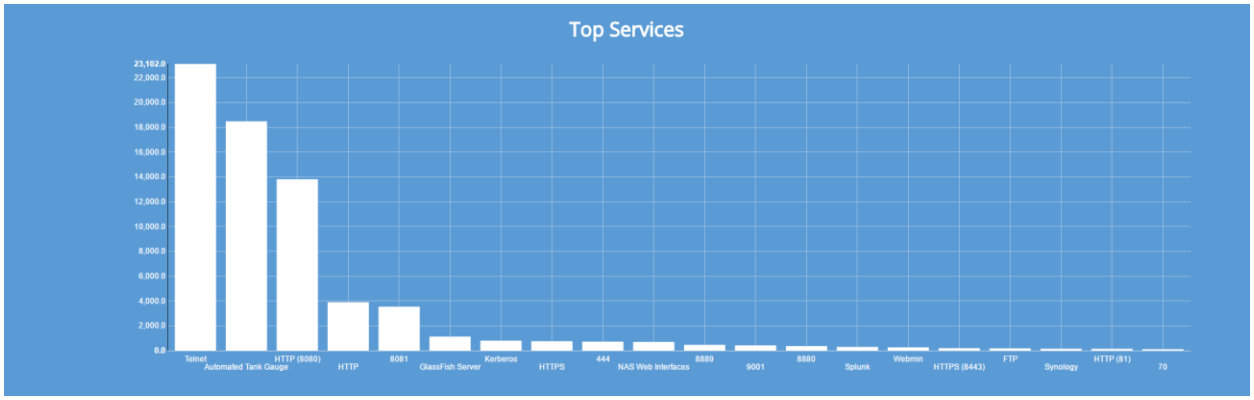
Η έλλειψη ασφάλειας που υπάρχει σε αυτές τις συσκευές, έγκειται στο ότι οι καταναλωτές συχνά για να κάνουν τη δουλειά τους αγοράζουν τις πιο φτηνές συσκευές και αυτό συχνά έχει επίπτωση στην ασφάλειά τους.

(24)

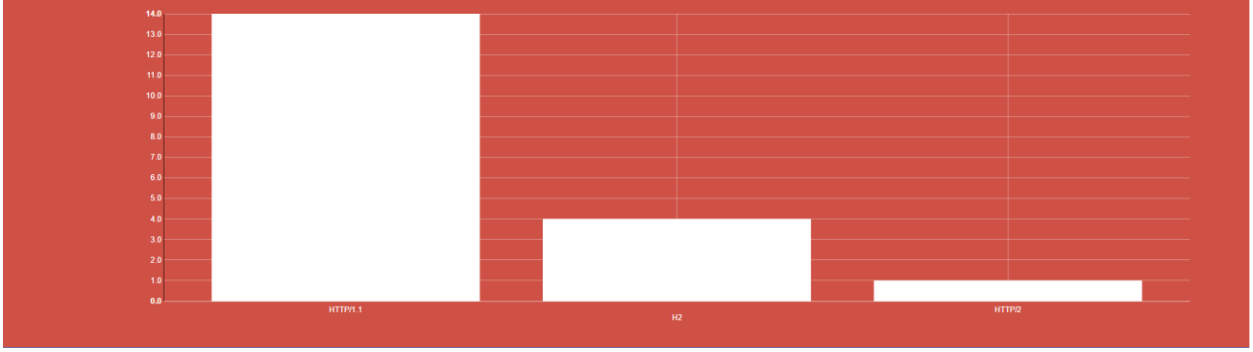
Στατιστικά από έρευνα

Θέλοντας να δείξουμε πόσες συσκευές είναι ευάλωτες στο Internet και πόση λίγη έμφαση δίνεται στο κομμάτι της ασφάλειας, έχουν ετοιμαστεί μερικά στατιστικά χρησιμοποιώντας το εργαλείο Shodan βάζοντας ως λέξεις κλειδιά μερικές από τις πιο γνωστές φράσεις για αναζήτηση.

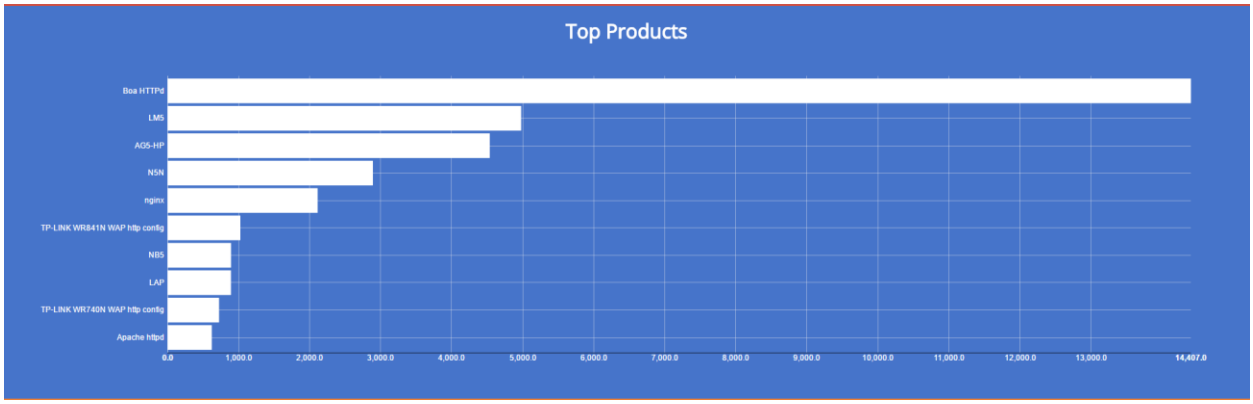
Αναζήτηση για "**default password**"



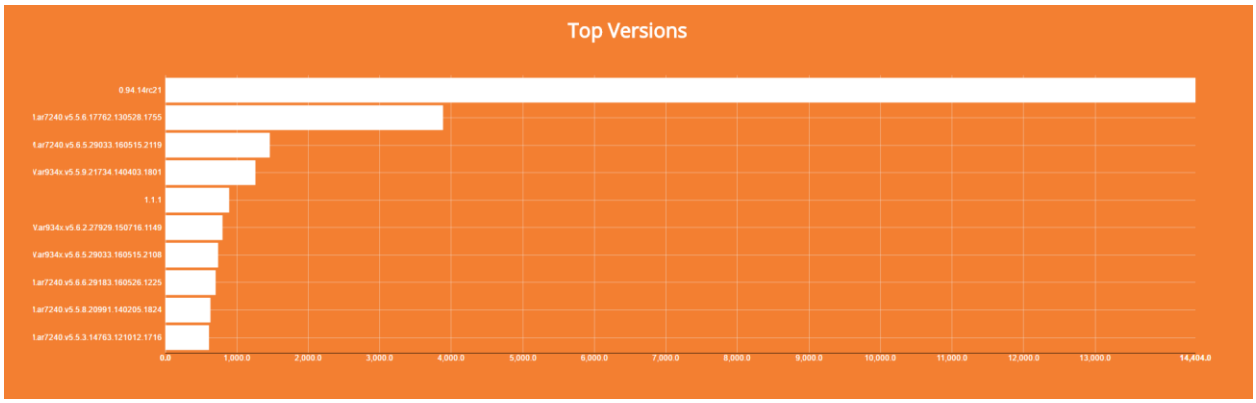
Negotiated HTTP Versions



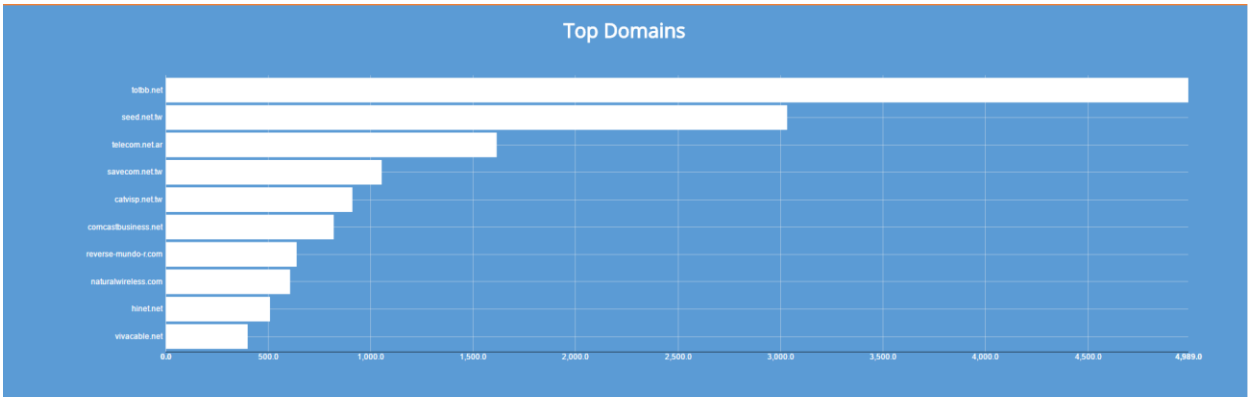
Top Products

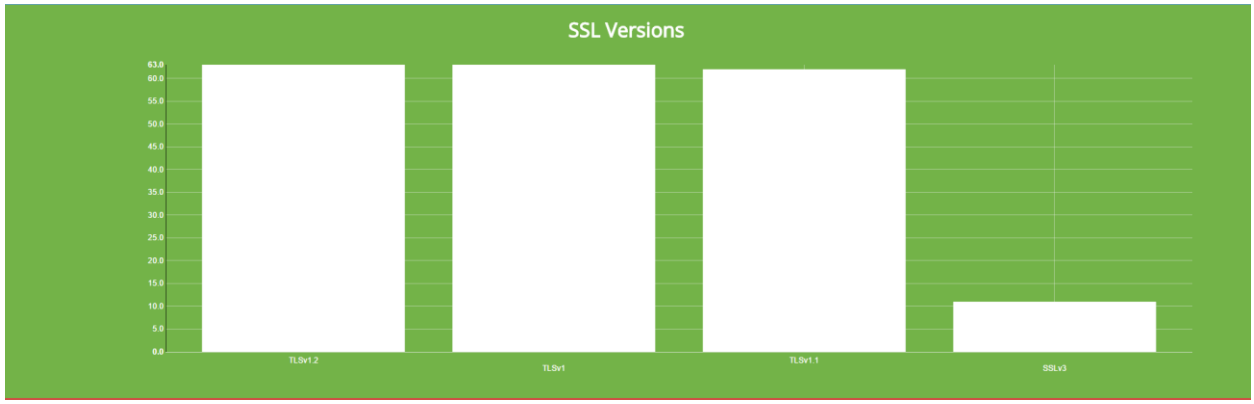


Top Versions



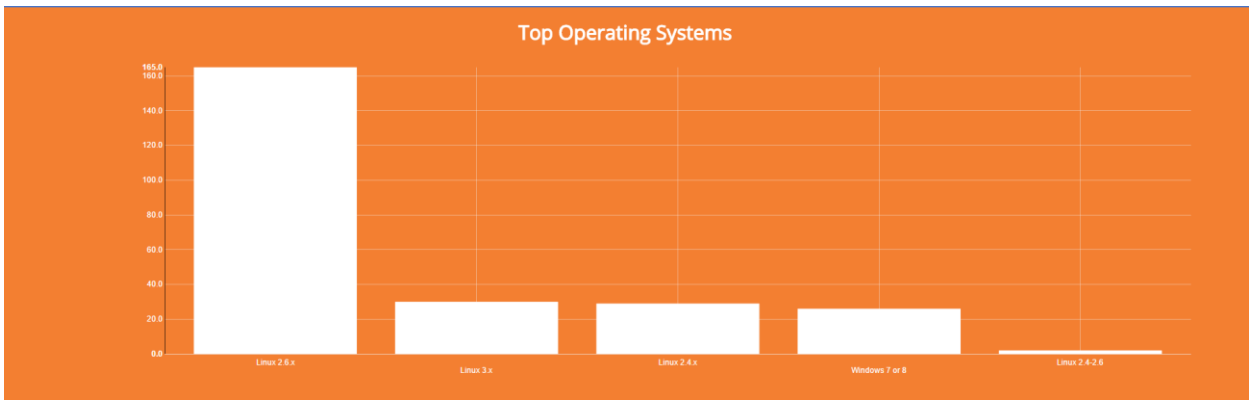
Top Domains



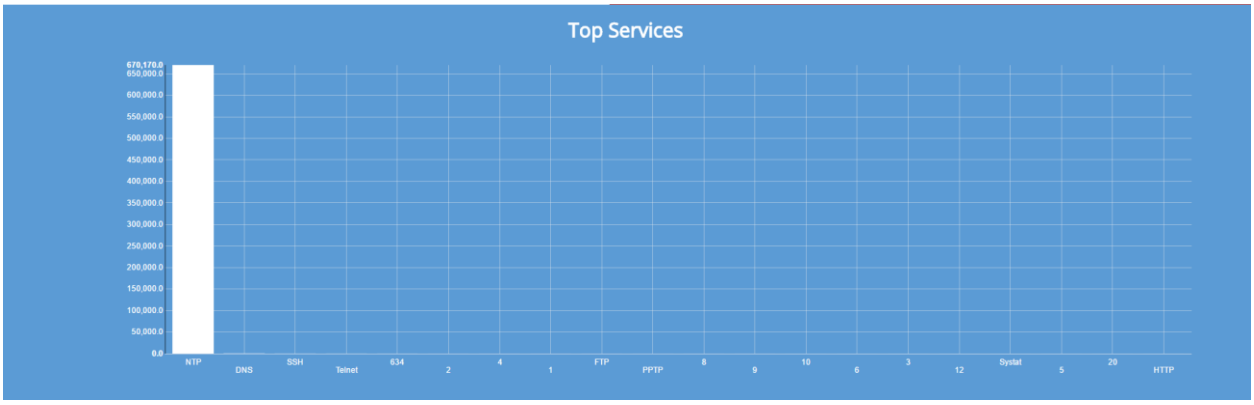

SSL Versions
63.0
60.0
55.0
50.0
45.0
40.0
35.0
30.0
25.0
20.0
15.0
10.0
5.0
0.0
TLSv1.2
TLSv1
TLSv1.1
SSLv3

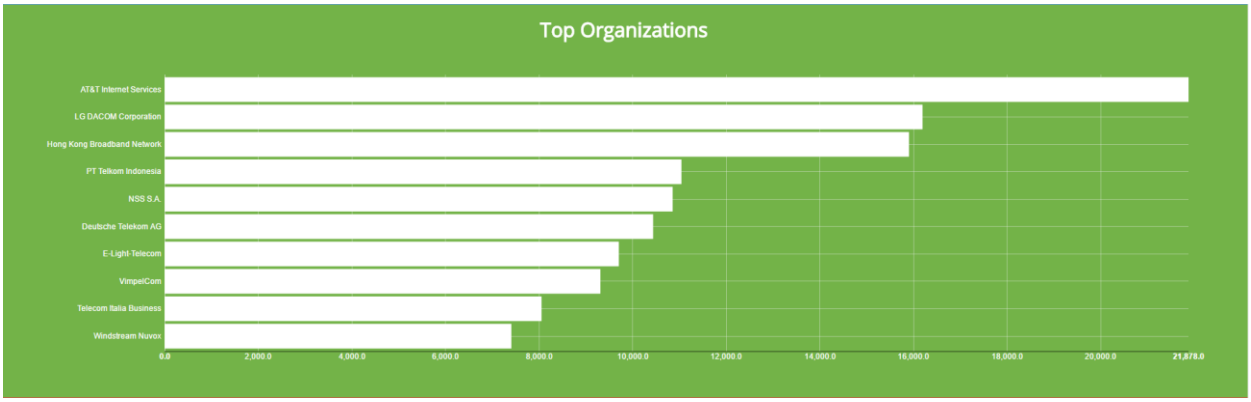

SSL Expired Certificates
50.0
45.0
40.0
35.0
30.0
25.0
20.0
15.0
10.0
5.0
0.0
Not Expired
Expired

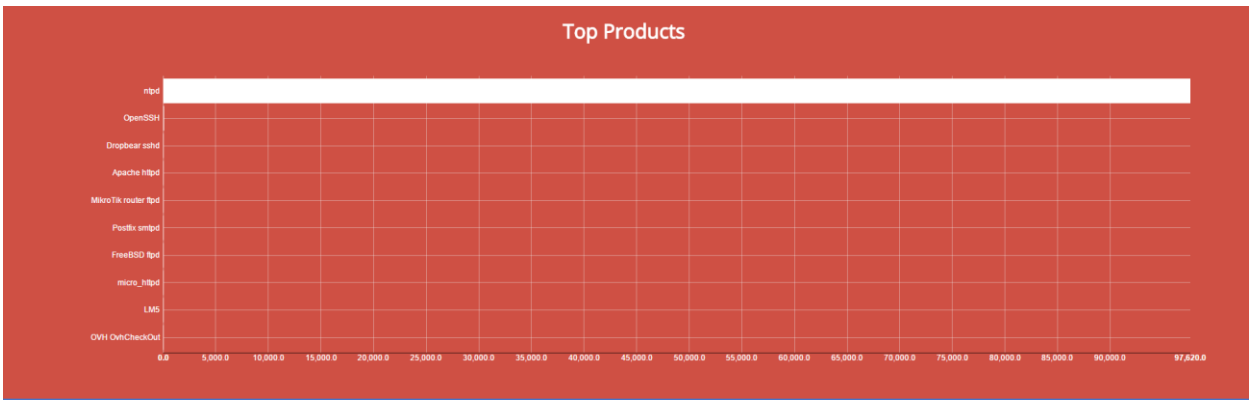

SSL Chain Length
31.0
30.0
28.0
26.0
24.0
22.0
20.0
18.0
16.0
14.0
12.0
10.0
8.0
6.0
4.0
2.0
0.0
2
1
3
4
5

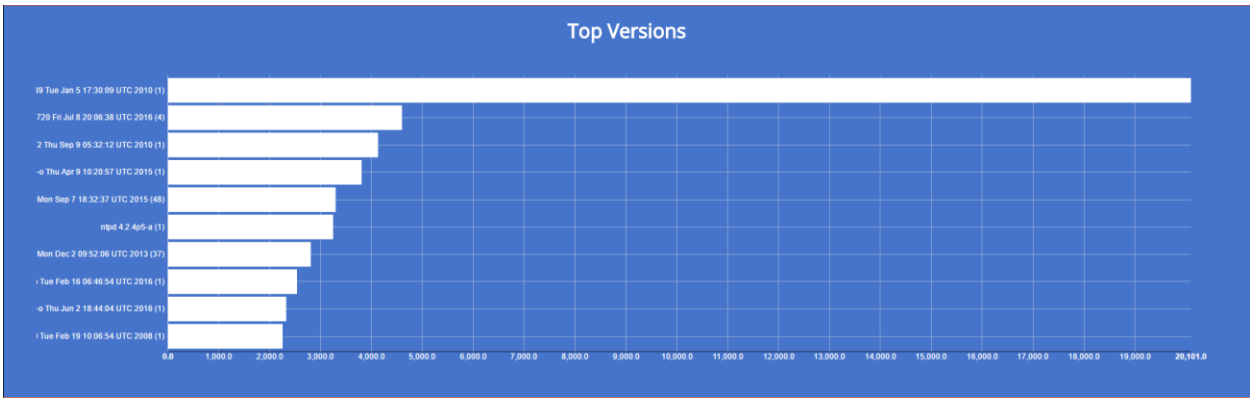

Top Operating Systems
165.0
160.0
140.0
120.0
100.0
80.0
60.0
40.0
20.0
0.0
Linux 2.6.x
Linux 3.x
Linux 2.4.x
Windows 7 or 8
Linux 2.4-2.6

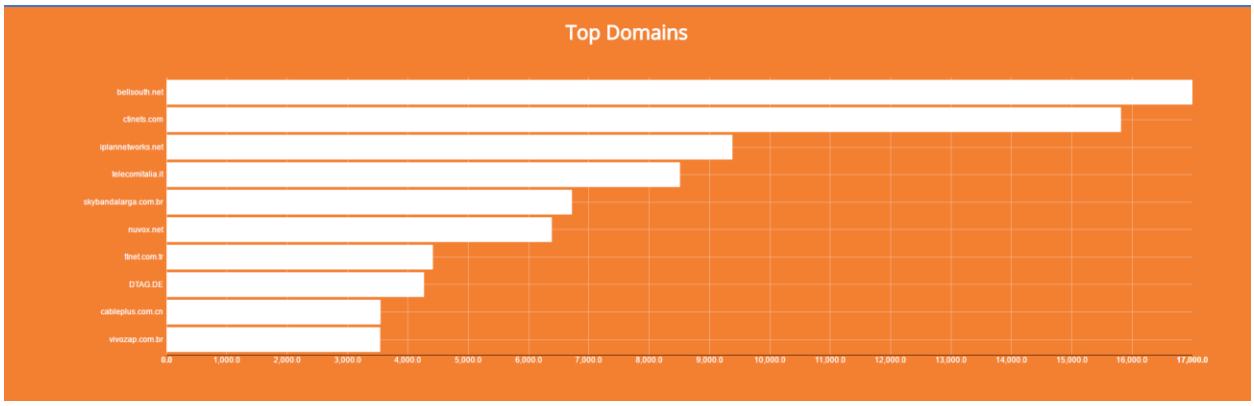
Αναζήτηση για “**ntp**”

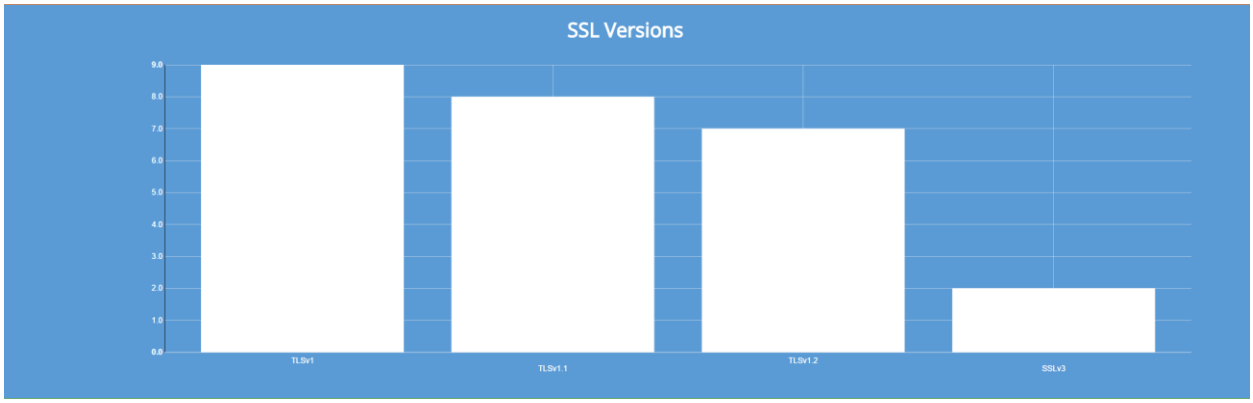


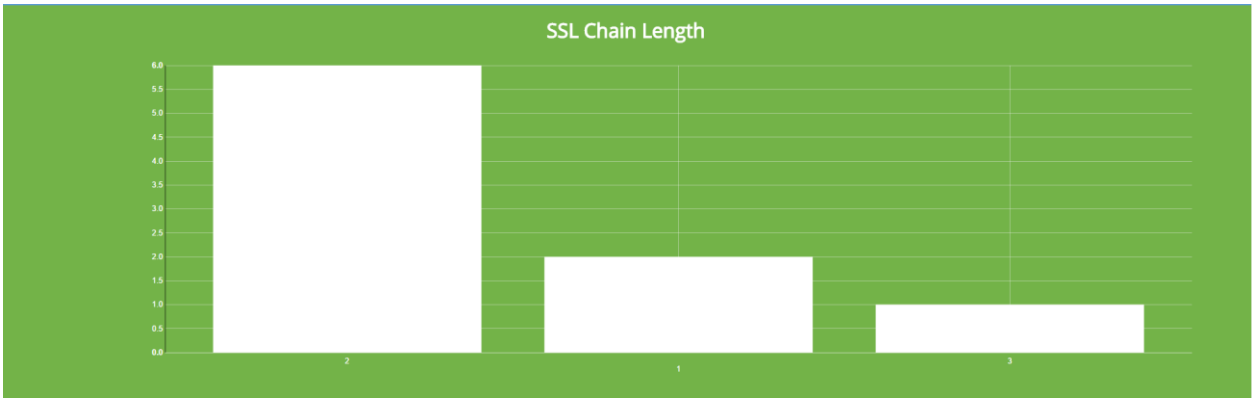


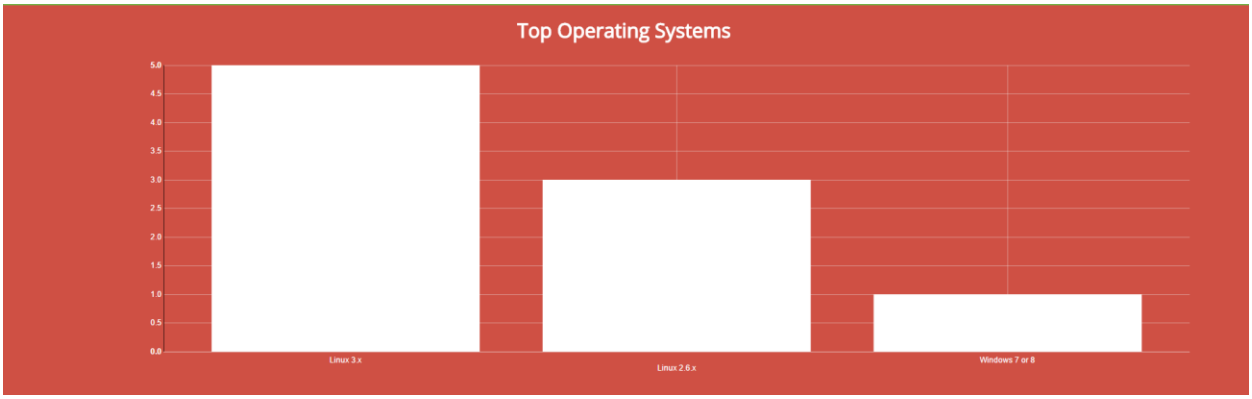



Top Versions
l9 Tue Jan 5 17:30:09 UTC 2010 (1)
720 Fri Jul 8 20:06:38 UTC 2016 (4)
2 Thu Sep 9 05:32:12 UTC 2010 (1)
-o Thu Apr 9 10:20:57 UTC 2015 (1)
Mon Sep 7 18:32:37 UTC 2015 (48)
ntpd 4.2.4p5-a (1)
Mon Dec 2 09:52:06 UTC 2013 (37)
i Tue Feb 16 06:46:54 UTC 2016 (1)
-o Thu Jun 2 18:44:04 UTC 2016 (1)
i Tue Feb 19 10:06:54 UTC 2008 (1)
0.0
1,000.0
2,000.0
3,000.0
4,000.0
5,000.0
6,000.0
7,000.0
8,000.0
9,000.0
10,000.0
11,000.0
12,000.0
13,000.0
14,000.0
15,000.0
16,000.0
17,000.0
18,000.0
19,000.0
20,101.0

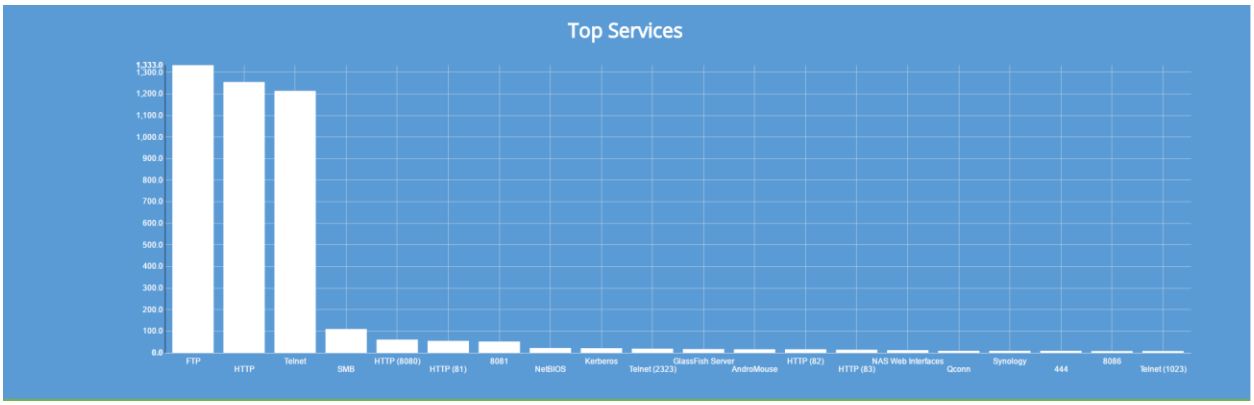

Top Domains
bellsouth.net
cbnets.com
iplannetworks.net
telecomitalia.it
skybandalarga.com.br
nuvox.net
tfnet.com.tr
DTAG.DE
cableplus.com.cn
vivozap.com.br
0.0
1,000.0
2,000.0
3,000.0
4,000.0
5,000.0
6,000.0
7,000.0
8,000.0
9,000.0
10,000.0
11,000.0
12,000.0
13,000.0
14,000.0
15,000.0
16,000.0
17,000.0

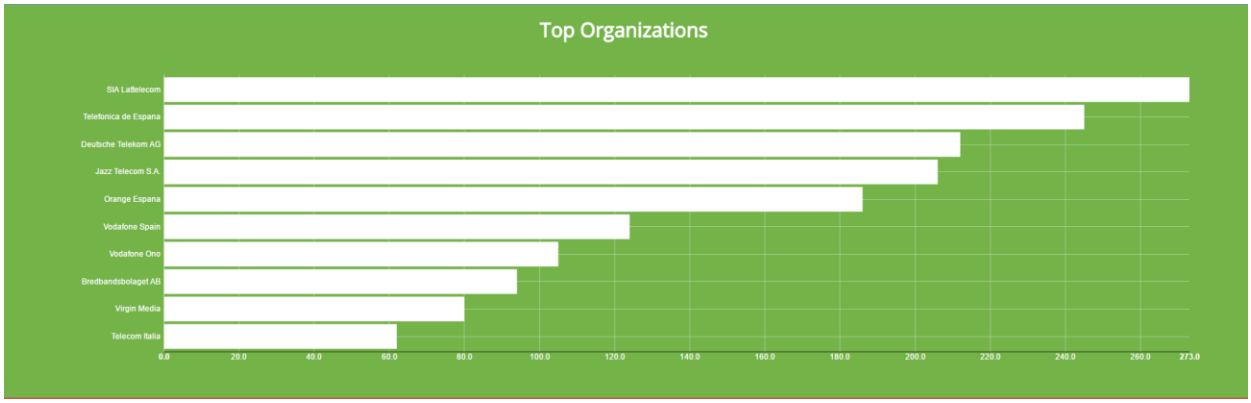

SSL Versions
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
TLSv1
TLSv1.1
TLSv1.2
SSLv3

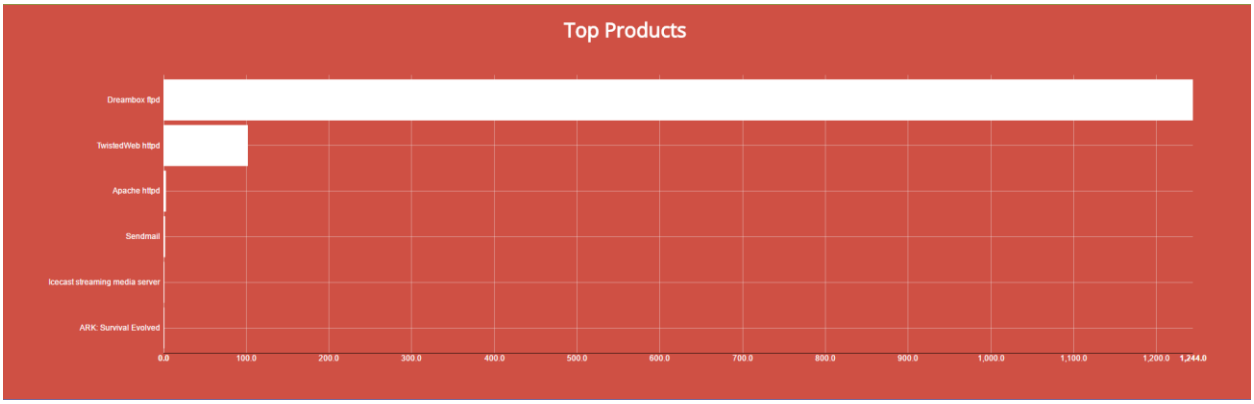

SSL Chain Length
6.0
5.5
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
2
1
3

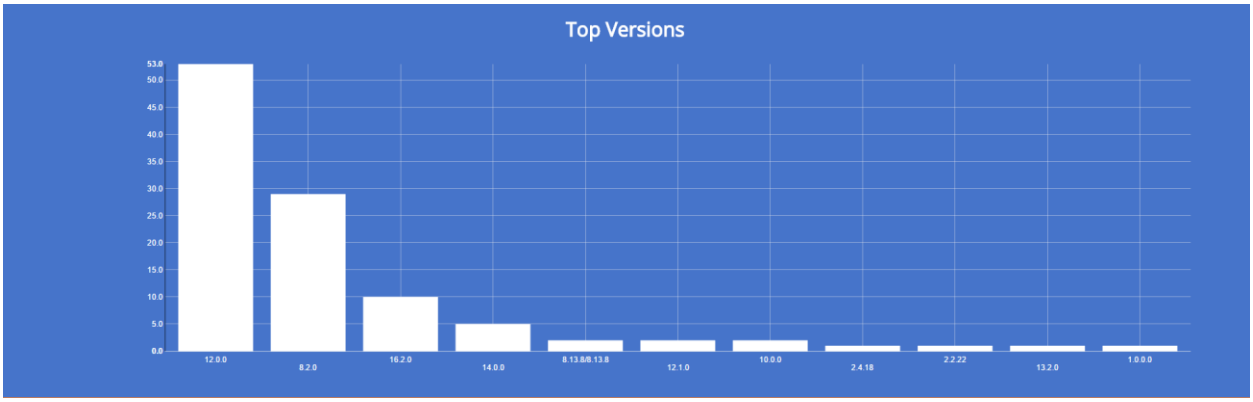

Top Operating Systems
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Linux 3.x
Linux 2.6.x
Windows 7 or 8

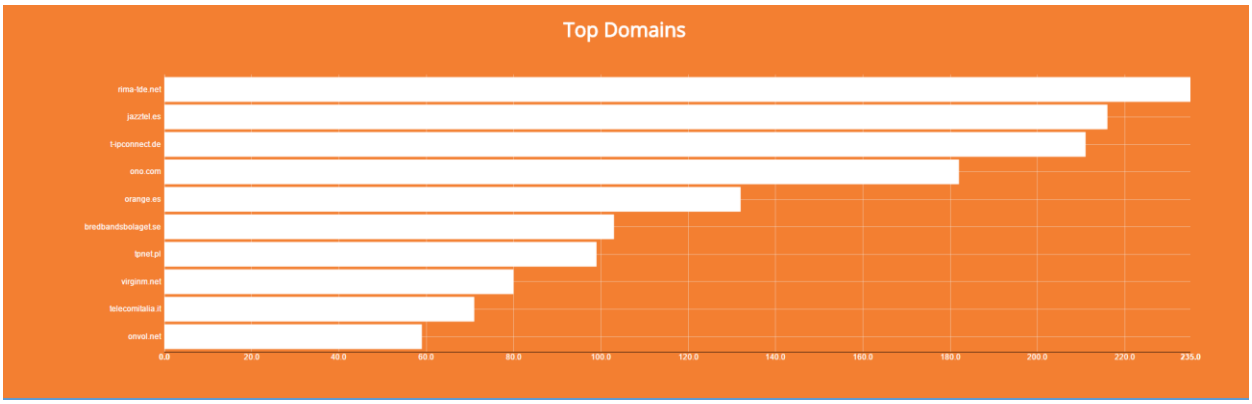
Αναζήτηση για “**dreambox**”

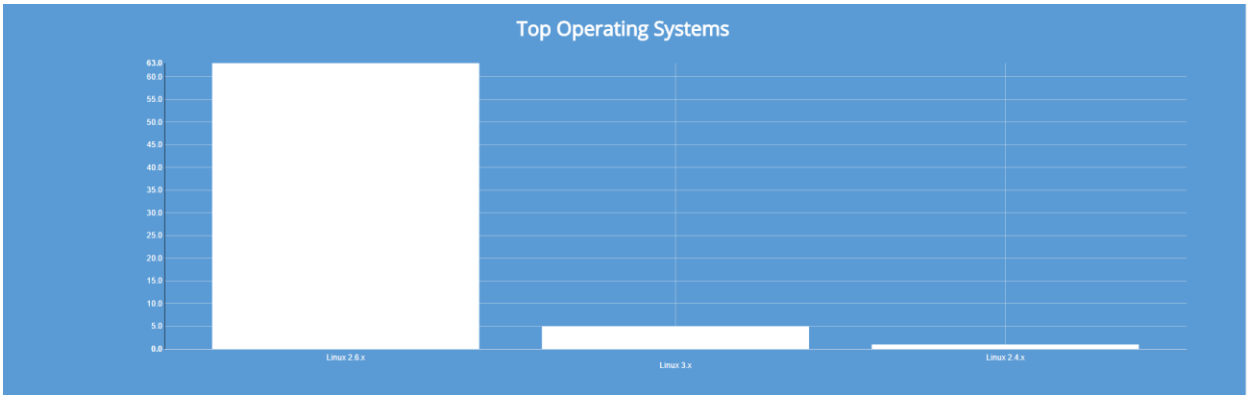





Top Products
Dreambox ftpd
TwistedWeb httpd
Apache httpd
Sendmail
Icecast streaming media server
ARK: Survival Evolved
0.0
100.0
200.0
300.0
400.0
500.0
600.0
700.0
800.0
900.0
1,000.0
1,100.0
1,200.0
1,244.0


Top Versions
53.0
50.0
45.0
40.0
35.0
30.0
25.0
20.0
15.0
10.0
5.0
0.0
12.0.0
8.2.0
16.2.0
14.0.0
8.13.8/8.13.8
12.1.0
10.0.0
2.4.18
2.2.22
13.2.0
1.0.0.0


Top Domains
rima-tde.net
jazztel.es
f-ipconnect.de
ono.com
orange.es
bredbandsbolaget.se
tpnet.pl
virginm.net
telecomitalia.it
onvol.net
0.0
20.0
40.0
60.0
80.0
100.0
120.0
140.0
160.0
180.0
200.0
220.0
235.0


Top Operating Systems
63.0
60.0
55.0
50.0
45.0
40.0
35.0
30.0
25.0
20.0
15.0
10.0
5.0
0.0
Linux 2.6.x
Linux 3.x
Linux 2.4.x

Όπως φαίνεται και από τα στατιστικά είναι εύκολο να διακρίνει κανείς ποιοί οργανισμοί και ποιά προιόντα χρησιμοποιούν περισσότερο τα συγκεκριμένα services, τι έκδοση χρησιμοποιείται στις περισσότερες περιπτώσεις, αν το πιστοποιητικό SSL έχει λήξει, ποιά λειτουργικά συστήματα είναι πιο συνηθισμένα με αυτά τα services κ.α.
Αυτές είναι πληροφορίες που θα ήταν πολύ χρήσιμες για ένα επιτηθέμενο και επίσης δε χρειάζεται να έχει και ιδιαίτερες δεξιότητες για να εκμεταλευτεί τέτοιες ευπάθειες.

Δημοσιευμένα παραδείγματα επιθέσεων στο IoT

Χάκερς επιτέθηκαν στην εταιρία Equifax και έκλεψαν 200.000 λογαριασμούς πιστωτικών καρτών με ένα χτύπημα!

Η Visa και η MasterCard έστειλαν εμπιστευτηκές ειδοποιήσεις σε χρηματοπιστωτικά ιδρύματα στις Ηνωμένες Πολιτείες, προιδοποιώντας τες ότι περισσότερες από 200.000 πιστωτικές κάρτες έχουν κλαπεί σε μία επική παραβίαση δεδομένων που ανακοινώθηκε σε τρία κεντρικά γραφεία της Equifax. Με την πρώτη ματιά, οι ειδοποιήσεις που παρατηρήθηκαν από την KrebsOnSecurity φαίνεται ότι οι χάκερς αρχικά είχαν παραβιάση την Equifax στις αρχές του Νοέμβρη του 2016. Αλλά η Equifax υποστηρίζει ότι οι λογαριασμοί κλάπηκαν όλοι την ίδια στιγμή, όταν οι χάκερς πήραν πρόσβαση στο σύστημα στα μέσα του Μαι του 2017.

Οι δύο εταιρίες Visa και MasterCard συχνά στέλνουν ειδοποιήσεις στους εκδότες καρτών με πληροφορίες για συγκεκριμένες πιστωτικές και χρεωστικές κάρτες οι οποίες μπορεί να έχουν εκτεθεί σε μία πρόσφατη παραβίαση. Αλλά είναι πολύ σπάνιο σε αυτές τις ειδοποιήσεις να αναφέρεται από ποιά εταιρία οι λογαριασμοί έχουν διαρεύσει.

Σε αυτή την περίπτωση όμως οι δύο εταιρίες ήταν ξεκάθαρες, αναφέροντας την Equifax συγκεκριμένα ως την πηγή για την παραβίαση καρτών ηλεκτρονικού εμπορίου.

Σε μία μη δημόσια ειδοποίηση που στάλθηκε αυτή την εβδομάδα σε αρκετές τράπεζες, η Visa έλεγε «η περίοδος έκθεσης» για τις κάρτες που κλάπηκαν από την επίθεση στη Equifax ήταν μεταξύ Νοέμβρη-10-2016 και Ιούλη-6-2017. Μία παρόμοια προιδοποίηση στάλθηκε από τη MasterCard που περιείχε το ίδιο εύρος ημερομηνιών.

Τα δεδομένα που κλάπηκαν συμπεριλαμβάνουν τον αριθμό λογαριασμού της κάρτας, την ημερομινία λήξης και το όνομα του κατόχου της κάρτας. Ένας κακόβουλος μπορεί να χρηστιμοποιήσει αυτές τις πληροφορίες για να διαπράξει απάτη ηλεκτρονικού εμπορίου σε εμπόρους του διαδικτύου.

Είναι πολύ πιθανόν να συμπεράνουμε από τις ειδοποιήσεις που προέρχονται από το 2016, ότι πιθανόν οι εισβολείς κατάφεραν να εγκαταστήσουν λογισμικό το οποίο κατέγραφε τα δεδομένα της κάρτας του πελάτη σε πραγματικό χρόνο καθώς αυτά μεταφέρονταν από μία ιστοσελίδα της Equifax. Βέβαια σύμφωνα με την Equifax, χάκερς κατέβασαν όλα τα δεδομένα με τη μία στα μέσα Μαιου το 2017.

Στην αρχική της αναφορά για την παραβίαση, η Equifax είπε ότι ανακάλυψε την εισβολή στις 29 Ιουλίου το 2017. Η εταιρία είπε ότι οι χάκερς εκμεταλεύτηκαν μία ευπάθεια στο λογισμικό της Web εφαρμογής. Στη συνέχεια προσθέτοντας στην αχική της αναφορά επιβεβαίωσε ότι το σφάλμα στο λογισμικό οφειλόταν σε ένα πακέτο λογισμικού ανοιχτού κώδικα που ονομαζόταν Apache Struts (CVE-2017-5638).

Το ελάττωμα στον Apache βρέθηκε στις 7 του Μαι του 2017, όταν οι εταιρίες της ασφάλειας άρχισαν να προιδοποιούν ότι οι επιτηθέμενοι εκμεταλεύονταν μία “zero-day” ευπάθεια στο Apache Struts. Τα Zero-days είναι κενά ασφαλείας όπου βρίσκουν και εκμεταλεύονται οι χάκερς πριν ο δημιουργός-προμηθευτής του λογισμικού γνωρίζει γι αυτά.

Στις 8 Μαιου η εταιρία Apache είχε δημοσιεύσει μία καινούρια έκδοση του λογισμικού όπου κάλυβε το κενό. Αλλά μέχρι εκείνη τη στιγμή ο κώδικας για να το εκμεταλευτεί κάποιος ήταν ήδη στο

διαδίκτυο, δημιουργώντας έτσι ένα αγώνα μεταξύ των εταιριών που χρειαζόντουσαν την αναβάθμιση στους server τους και στους χάκερς που προσπαθούσαν να την εκμεταλευτούν πριν κλείσει.

Αναβάθμιση, Σεπτ 15, 12¨31 π.μ. Η Visa αναβάθμισε την αναφορά για τις πιστοτικές κάρτες που κλάπηκαν από την Equifax. Τώρα υποστηρίζει ότι μαζί με τα άλλα στοιχεία κλάπηκαν επίσης ο αριθμός κοινωνικής ασφάλισης του κατόχου κάρτας και η διεύθυνση, υποστηρίζοντας ότι οι λογαριασμοί κλάπηκαν από ανθρώπους που είχαν κάνει εγγραφής στο σύστημα για υπηρεσίες ελέγχου πιστώσεων μέσω της Equifax.

Η μεγαλύτερη επίθεση στον κόσμο μεγέθους 1 Tbps DDoS τύπου εκτοξεύτηκε από 152.000 έξυπνες συσκευές που είχαν παραβιαστεί.

Αν κάποιος έχει στην κατοχή του έξυπνες συσκευές που συνδέονται με το διαδίκτυο όπως τηλεώραση, αυτοκίνητο, ψυγείο ή θερμοστάτες μπορεί να είναι ήδη μέρος του botnet που αποτελείται από εκατομμύρια τέτοιες συσκευές οι οποίες χρησιμοποιήθηκαν για να εκτοξεύσουν τη μεγαλύτερη DDoS γνωστή επίθεση μέχρι τώρα, με ταχύτητα αιχμής πάνω από 1Tbps, στην εταιρία OVH που στεγάζεται στη Γαλλία.

Καθώς το Internet of Things και οι συνδεδεμένες συσκευές σε αυτό μεγαλώνουν σταδιακά, συνεχίζονται να μεγαλώνουν οι περιοχές επίθεσης, δίνοντας έτσι στους επιτηθέμενους ένα μεγάλο αριθμό από σημεία εισόδου που μπορούν να επηρεάσουν κάποιον χρήστη με τον ένα ή τον άλλο τρόπο.
Το IoT συχνά αναπτύσεται σε ένα μεγάλο αριθμό από συσκευές μέσα από σπίτια, επιχειρήσεις, νοσοκομεία, ακόμα και ολόκληρες πόλεις, αλλά συχνά χακάρονται και χρησιμοποιούνται ως όπλα για διαδικτυακές επιθέσης λόγο της έλλειψης μέτρων ασφαλείας και της μη επαρκής κρυπτογράφισης.
Ο Octave Klaba, ο ιδρυτής της OVH, αποκάλυψε στο Twitter ότι η εταιρία του χτυπήθηκε από δύο ταυτόχρονες DDoS επιθέσεις που μαζί ξεπερνούσαν το 1 Tbps. Μία φωτογραφία που ανέβασε ο Klaba δείχνει τις πολλαπλές επιθέσεις DDoS που ξεπερνούν τα 100Gbps, συμπεριλαμβανομένου και μίας που έφτανε τα 799Gbps μόνη της, κάνοντας τη τη μεγαλύτερη DDoS επίθεση που έχει καταγραφεί ποτέ.
Σύμφωνα με τον ιδρυτή της OVH, η μαζική επίθεση DDoS πραγματοποιήθηκε από ένα δίκτυο με πάνω από 152.000 IoT συσκευές συμπεριλαμβανομένου και CCTV κάμερες και προσωπικούς μηχανήματα για βίντεο.
Οι IoT συσκευές συνήθως δεν αναμένουν ως προεπιλογή τις αναβαθμίσεις για την ασφάλεια, το οποίο κάνει πολύ πιθανόν για τους επιτηθέμενους να παραβιάσουν αυτές τις συσκευές ανά πάσα ώρα και στιγμή.

61 κωδικοί που τροφοδοτούν το Mirai IoT botnet

Τα προεπιλεγμένα ονόματα χρηστών και οι κωδικοί ήταν πάντα ένα μεγάλο πρόβλημα στην ασφάλεια. Αυτή τη στιγμή η τεράστια ανάπτυξη του Internet of Things έχει κάνει το πρόβλημα μεγαλύτερο.

Τα παρακάτω ονόματα χρηστών και οι κωδικοί χρησιμοποιήθηκαν για να ενεργοποιήσουν το Mirai botnet, το οποίο τροφοδοτείται από την IoT τεχνολογία. Το botnet χρυπάει την Brian Krebs με κίνηση που φτάνει τα 620Gbps, αλλά συνδέεται επίσης και με την DDoS επίθεση κατά της OVH που έφτασε τα 799Gbps.

Το Mirai ψάχνει για συνδέσεις telnet και χρησιμοποιεί τα στοιχεία παρακάτω για να πάρει πρόσβαση στη συσκευή, η οποία μπορεί να είναι μία κάμερα, DVR, ρούτερ ή κάποια άλλη.

Το botnet χρειαζόταν το λιγότερο 2 servers. Όμως ο συγγραφέας του Mirai είπε ότι αυτό το έκανε να δουλέψει με δύο VPS λογαριασμούς, ένα server ως C&C και τρεις άλλους για την εξισορρόπηση της κίνησης.

Στην κορύφωσή του το Mirai είχε σχεδόν 400.000 συσκευές συνδεδεμένες σε αύτο μόνο από συνδέσεις telnet που έψαξε. Μετά την επίθεση στο Brian Krebs, αυτός ο αριθμός έπεσε στις 300.000 γιατί οι ISP εταιρίες προσπάθησαν να διορθώσουν το πρόβλημα.

Μαζί με τον κώδικα του botnet , ο συγγραφέας έδωσε επίσης και οδηγίες για τη διαμόρφωση και τη ρύθμισή του. Οπότε αναμένονται παρόμοια botnets να εμφανιστούν στο διαδίκτυο σύντομα.

USER:	PASS:	USER:	PASS:
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

CSO Online

Πώς το Drone βρίσκει και χακάρει συσκευές του Internet of Things από τον ουρανό.

Οι επιστήμονες της ασφάλειας έχουν ανατπύξει ένα υπτάμενο Drone με ενσωματομένο εργαλείο παρακολούθησης ικανό να καταγράφει δεδομένα από συσκευές που είναι συνδεδεμένες στο διαδίκτυο, γνωστές και ως Internet of Things.

Η εφαρμογή του project ήταν οι ερευνητές να πετάξουν το Drone με το δικό τους σύστημα καταγραφής που είχαν δημιουργήσει ενσωματομένο πάνω από το Aautin του Texas σε πραγματικό χρόνο.

Μέσα σε 18 λεπτά πτήσης το drone βρήκε περίπου 1600 συνδεδεμένες συσκευές, από τις οποίες 453 ήταν κατασκευασμένες από τη Sone και 110 από τη Philips.

Πώς βρέθηκαν οι συσκευές?

Οι ερευνητές εντόπισαν όλες τις έξυπνες συσκευές και δίκτυα που είχαν ενεργοποιημένο το ZigBee. "Όταν οι IoT συσκευές επικοινωνούσαν ασύρματα μέσω του πρωτοκόλλου ZigBee, αυτό το πρωτόκολλο είναι ανοιχτό στο επίπεδο του δικτύου. Οπότε όταν οι συσκευές άρχισαν να συνδέονται και έστελναν beacon αιτήματα, εμείς καταγράφαμε τα δεδομένα βασισμένα σε αυτό." Λέει ο Paul West Jauregui.

Το Zigbee είναι ένα γνωστό πρωτόκολλο που χρησιμοποιείται για την ασύρματη επικοινωνία σε οικιακούς χώρους από την πλειοψηφία των Internet of Things συσκευών σήμερα. Το χρησιμοποιούν εταιρίες όπως Toshiba, Philips, Huawei, Sony, Siemens, Samsung, Motorola, και πολλές άλλες.

Ο Tobias Zillner και ο Sebastian Strobl από την 'Cognosec' έχουν ανακαλύψει μερικά κρίσιμα κενά στην ασφάλεια του ZigBee που επιτρέπουν στους χάκερς να εισβάλουν σε ένα ZigBee δίκτυο και να πάρουν υπό τον έλεγχό τους όλες τις συνδεδεμένες συσκευές σε αυτό, συμπεριλαμβανομένου και κλειδαριές από πόρτες, συστήματα συναγερμού ακόμα και να ελέγξουν τα φώτα.

Αυτή η ευπάθεια στην πραγματικότητα δημιουργείται στον τρόπο όπου το πρωτόκολλο ZigBee διαχειρίζεται τα κλειδιά για την πιστοποίηση των IoT συσκευών και τα προσθέτει στο mesh network, επιτρέποντας στους χάκερς να συλλέξουν τα κλειδιά για την αυθεντικοποίηση.

Το χειρότερο σημείο που επισήμαναν οι ερευνητές ήταν ότι οι χρήστες δε μπορούσαν να κάνουν κάτι για να ασφαλίσουν περισσότερο τις συσκευές τους και από τη στιγμή που το κενό επηρεάζει μία μεγάλη γκάμα από συσκευές, είναι πολύ να προσδιοριστεί πότε οι εταιρίες θα δημιουργήσουν μία διόρθωση.

IoT Botnet ανακάλυψε 120.000 IP κάμερες σε κίνδυνο για επίθεση.

Το Persirai IoT botent, το οποίο στοχεύει IP κάμερες, έρχεται μετά το Mirai και μεγαλώνει τον κίνδυνο των IoT botnets. Οι ερευνητές στο Trend Micro έχουν ανακαλύψει ένα καινούριο Internet of Things botnet το οποίο ανακαλύπτει 120.000 Internet Protocol κάμερες εκτεθημένες για επίθεση.

Το botnet με την επωνυμία Persirai, ανακάλυψε περισσότερα από 1.000 μοντέλα από διαφορετικές IP κάμερες. Το Persirai χτυπάει IoT συσκευές λίγους μήνες μετά το Mirai botnet, το οποίο σπείρει το χάος με το να επιτήθετε σε DVRs και CCTV κάμερες για να εκτοξεύσει μία μαζική DDoS επίθεση το Οκτόμβρη του 2016.

Οι ερευνητές ανακάλυψαν το Persirai όταν βρήκαν 4 command and control σέρβερς και βρήκαν ευπάθειες που σχετίζονταν με αυτούς, εξηγεί ο Jon Clay, υπεύθυνος για τις απειλές στην επικοινωνία στο

Trend Micro.

Κάθως έκαναν ανάλυση στο κακόβουλο λογισμικό, βρήκαν ότι στόχευε IP κάμερες. Χρησιμοποιώντας το εργαλείο Shodan, εντόπισαν περισσότερες από 120.000 συσκευές οι οποίες ήταν εκτεθειμένες στο διαδίκτυο. Οι IP κάμερες είναι ορατοί στόχοι για κακόβουλα λογισμικά που στοχεύουν το IoT γιατί συνήθως χρησιμοποιούν το Universal Plug and Play (UPnP) προτώκολλο που επιτρέπει στις συσκευές να ανοίξουν μία πόρτα στο ρούτερ και να λειτουργήσουν σα σέρβερ.

Η πιο εμαφνή διαφορά ανάμεσα στο Mirai και στο Persirai ήταν ότι το Mirai χρησιμοποιούσε brute-force για να κλέψει τα στοιχεία των χρηστών, ενώ το Persirai χρησιμοποιούσε μία zero-day ευπάθεια η οποία είχε δημοσιευτεί κάποιους μήνες πριν. Οι επιτηθέμενοι που εκμεταλλεύονταν αυτό το κενό μπορούσαν να πάρουν το αρχείο με τους κωδικούς, το οποίο τους έδινε και πρόσβαση στη συσκευή.

Η κάμερα που είχε καταληφθεί από την επίθεση μπορούσε να χρησιμοποιηθεί για να ανακαλύψει και άλλα θύματα, τα οποία μπορούσαν να μολυνθούν από την ίδια zero-day ευπάθεια. Από εκεί και μετά μπορούσαν να συνεχίσουν να κλέβουν αρχεία κωδικών και να εξασφαλίζουν την ικανότητα να εκτελούν εντολές συστήματος και να διαδίδουν τον κακόβουλο κώδικα.

Ο Clay δηλώνει ότι η συγκεκριμένη zero-day ευπάθεια που αφορά το Persirai θα συνεχίσει να είναι μία απειλή. Το λογισμικό διαγράφει τον εαυτό του μόλις μολύνει το μηχάνημα και τρέχει μόνο στη μνήμη. Αυτό κάνει πολύ πιο δύσκολο να εντοπιστεί ο κώδικάς του μόλις φύγει.

“Οι επιτηθέμενοι πίσω από αυτή την ενέργεια είναι πολύ πιθανόν να κυνηγήσουν και άλλες ευπάθειες και να ψάξουν για άλλες συσκευές IoT με παρόμοια κενά ασφαλείας” εξηγεί. Ο επιτηθέμενος μπορεί να φτιάξει ένα μεγαλύτερο ή και ξεχωριστό botnet με αυτές τις συσκευές.

Οι κάτωχοι IP καμερών συμβουλεύονται να μένουν ενημερωμένοι με τις τελευταίες αναβαθμίσεις στην ασφάλεια του λογισμικού τους και να χρησιμοποιούν πιο περίπλοκους κωδικούς για να είναι πιο ισχυροί απέναντι σε μία brute-force επίθεση. Οι περισσότεροι χρήστες δε ξέρουν ότι οι IP κάμερές του είναι εκτεθημένες στο διαδίκτυο και δεν αλλάζουν τον προεπιλεγμένο κωδικό τους, εξηγούν οι ερευνητές. Οι περισσότεροι δε ξέρουν καν εάν η κάμερά τους πραγματοποιεί μία DDoS επίθεση.

Οι κατασκευαστές πρέπει να βελτιώσουν τη διαδικασία πιστοποίησης και να χρησιμοποιήσουν παραπάνω στοιχεία από τον κωδικό, όπως βιομετρικά χαρακτηριστικά ή two-factor authentication για να δυναμώσουν την ασφάλεια των συσκευών τους, δηλώνει ο Clay.

Συμπεράσματα

Το IoT παρουσιάζει μία πληθόρα απειλών που πρέπει να ληφθούν υπόψιν από τους σχεδιαστές ασφαλείας και τους κατασκευαστές. Παρουσιάστηκαν οι τομείς που πρέπει να ληφθούν υπόψιν, καθώς επίσης οι επιτηθέμενοι και τα κίνητρά τους. Σκοπός ήταν να να καλυφθούν όλες οι πλευρές που χρίζουν προσοχή ως προς την ασφάλεια σε ένα IoT σύστημα από το network έως και το φυσικό επίπεδο.
Περισσότερο δώθηκε έμφαση στην ασφάλεια των συσκευών και του λογισμικού σε σχέση με την εμπιστευτηκότητα, την ακεραιότητα και τη διαθεσιμότητα. Οι επιθέσεις από οργανωμένες ομάδες επιτηθέμενων είναι πιο επικίνδυνες από ότι μεμωνομένους χάκερς και ο λόγος είναι ότι οι γνώσεις τους και η εμπειρία τους είναι πολύ μεγαλύτερη.
Το Shodan ως μία μηχανή αναζήτησης IoT συσκευών όπου μπορεί να δείξει πολύ εύκολα την ελλειπή προσοχή στην ασφάλεια αυτών των συσκευών και πόσο εύκολα ένας επιτηθέμενος με πολύ λίγες γνώσει να προκαλέσει ζημιά σε ένα στόχο.
Το Internet of Things είναι πολύ κοντά στο να εφαρμοστεί στην καθημερινότητα από όσο μπορεί κάποιος να φανταστεί. Οι περισσότερες τεχνολογίες που χρειαζόντουσαν έχουν βρεθεί και εφαρμοστεί και μερικοί κατασκευαστές έχουν ήδη εφαρμόσει ένα μικρό κομμάτι του.
Οι κύριοι λόγοι που δεν έχει εφαρμοστεί πλήρως είναι η επίπτωση που θα έχει στο νομικό, ηθικό και στο κομμάτι της ασφάλειας. Οι εργαζόμενοι μπορούν εύκολα να κάνουν κατάχρηση των συσκευών, οι επιτηθέμενοι να πάρουν πρόσβαση σε αυτές, οι εταιρίες μπορεί να μη θέλουν να διαμοιράζονται την πληροφορίας τους και οι υπόλοιποι άνθρωποι να μην τους αρέσει η πλήρης έλλειψη ιδιωτικότητας. Γι αυτούς τους λόγους το IoT μπορεί να καθυστερήσει παραπάνω από ότι χρειάζεται.

Μελλοντική εργασία

Στο μέλλον, θα ήταν χρήσιμο να γίνει μία πιο λεπτομερής μελέτη των “Top IoT Vulnerabilities” από το owasp IoT project, έτσι ώστε να υπάρξει μία καλύτερη εκτίμηση των κινδύνων που αντιμετοπίζουν οι συσκευές και οι χρήστες του IoT. Στις νέες αυτές έρευνες θα πρέπει να χρησιμοποιηθούν διαφορετικά και ειδικά εργαλεία για την κάθε περίπτωση, ούτως ώστε να υπάρχει μεγαλύτερη κατανόηση για την κάθε μία ξεχωριστά. Όπως η ασφάλεια στο Cloud Interface και το Privacy Concerns όπου εξετάζεται αν όλα τα δεδομένα συλλεχθηκαν από την IoT συσκευή και τα Cloud Interfaces, οι συσκευές να συλλέγουν μόνο τα απαραίτητα που χρειάζονται για να εκτελέσουν τη λειτουργία τους, το οποίο έχει επιπτώσεις και στην ασφάλεια και στην ταχύτητα. Τέλος να εξετάζεται ποιός έχει πρόσβαση στα προσωπικά δεδομένα που συλλέγονται.

Βιβλιογραφία

1. **Ad Hoc Networks.** *Internet of things: Vision, applications and research challenges.* 2012.
2. **Akyildiz, I.F.** *Ad Hoc Networks.* 2004.
3. **Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash.** *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications.* 2015.
4. **Security, U.S. Department of Homeland.** *Strategic Principles For Securing The Internet Of Things (IoT).* 2016.
5. **SANS Institute InfoSec Reading Room.** *SANS Institute InfoSec Reading Room, The Art of Reconnaissance.* 2001.
6. **ericsson White paper.** *IoT SECURITY.* 2017.
7. **Gemalto .** *Building a trusted Foundation for the Internet of Things.* 2017.
8. **Køien, Mohamed Abomhara and Geir M.** *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks.* 2015.
9. **Bassi, A., Bauer, M., Fiedler, M., Kramp.** *Enabling Things to Talk.* 2013.
10. **ResearchGate.** *Security of the Internet of Things: Perspectives and challenges.* 2014 .
11. **Lopez research.** *An Introduction to the Internet of Things.* 2013.
12. **Hu, Fei.** *1. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, Fei Hu.* 2016.
13. **Smith, Sean.** *The Internet of Risky Things: Trusting the Devices That Surround Us.* 2014.
14. **Etter, David.** *IoT Security: Practical guide book.* 2016.
15. **Chou, Timothy.** *Precision: Principles, Practices and Solutions for the Internet of Things.* 2016.
16. **Greengard, Samuel.** *The Internet of Things (The MIT Press Essential Knowledge series).* 2015.
17. **Amir Vahid Dastjerdi, Rajkumar Buyya.** *Internet of Things: Principles and Paradigms 1st Edition.* 2015.
18. **Rodrigo Romana, Jianying Zhou.** *On the Features and Challenges of Security & Privacy in Distributed Internet of Things.* 2013.
19. **Luigi Atzori, Antonio Iera.** *The Internet of Things: A survey.* 2010.
20. **Feng Xia, Laurence T.Yang.** *Internet of Things.* 2012.
21. **Gerd Kortuem, Daniel Fitton, Vasughi Sundramoorthy.** *Smart objects as building blocks for the Internet of things.* 2010.
22. **Harald Sundmaeker, Patrick Guillemin, Peter Friess.** *Vision and Challenges for Realising the Internet of Things.* 2010.
23. **Pethuru Raj, Anupama C. Raman.** *The Internet of Things: Enabling Technologies, Platforms, and Use Cases.* 2017.
24. **Luigi Atzori, Antonio Iera, Giacomo Morabito.** *The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization.* 2012.
25. **Dieter Uckelmann, Mark Harrison, Florian Michahelles.** *An Architectural Approach Towards the Future Internet of Things.* 2011.

26. **Dominique Guinard, Student Member, IEEE, Vlad Trifa, Student Member, Stamatis Karnouskos, Senior Member, IEEE, Patrik Spiess, Member, IEEE, Domnic Savio, Member, IEEE.** *Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services.* 2010.
27. **Veracode.** *The Internet of Things: Security Research Study.* 2014.
28. **Procedia Computer Science.** *Security Issues and Challenges for the IoT-based Smart Grid.* 2014.
29. **Tobias Heer, Oscar Garcia-Morchon, Ren´e Hummen.** *Security Challenges in the IP-based Internet of Things.* 2017.
30. **Symantec.** *Insecurity in the Internet of Things.* 2015.
31. **SANS Institute InfoSec Reading Room.** *Securing the Internet of Things Survey.* 2014.
32. **Hancke, Gerhard P., Markantonakis, Konstantinos.** *Radio Frequency Identification and IoT Security.* 2016.
33. **IEC White Paper.** *IoT 2020: Smart and secure IoT platform.* 2016.
34. **Azure, Microsoft.** *Internet of Things security from the ground up.* 2017.
35. **Mandler, B., Barja, J., Mitre Campista, M.E., Cagáňová, D., Chaouchi, H., Zeadally, S., Badra, M., Giordano, S., Fazio, M., Somov, A., Vieriu, R.-L.** *Internet of Things. IoT Infrastructures.* 2015.
36. **FTC Sta Report.** *Internet of Things Privacy & Security in a Connected World.* 2015.
37. **Ma, C. , Weng, J.** *Radio Frequency Identification System Security.* 2013.
38. **Jacob Wurm, Khoa Hoang, Orlando Arias, Ahmad-Reza Sadeghi, Yier Jin.** *Security Analysis on Consumer and Industrial IoT Devices.* 2016.
39. **PubNub.** *A New Approach to IoT Security, 5 Key Requirements to Securing IoT Communications.* 2015.
40. **Bertino, Elisa.** *Data Security and Privacy in the IoT.* 2016.
41. **DIGI.** *IoT DEVICE SECURITY BUILT-IN, NOT BOLT-ON.* 2016.
42. **Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul.** *Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures, Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul.* 2016.
43. **Smart Card Alliance.** *A SMART CARD ALLIANCE INTERNET OF THINGS SECURITY COUNCIL WHITE PAPER.* 2016.
44. **SentryBay.** *IoT Security & Privacy.* 2015.
45. **Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang.** *A Security Framework for the Internet of Things in the Future Internet Architecture.* 2017.
46. **EY.** *Cybersecurity and the Internet of Things.* 2015.
47. **CSA cloud security alliance.** *Security Guidance for Early Adopters of the Internet of Things (IoT).* 2015.
48. **John Mattsson, Göran Selander, Göran AP Eriksson.** *Object Security in Web of Things.* 2016.
49. **Internet of Things Security Foundation.** *establishing principles for Internet of Things security.* 2016.
50. **ARM.** *IOT security.* 2012.
51. **Symantec.** *An Internet of Things Reference Architecture.* 2014.
52. **Tobias Heer, Oscar Garcia-Morchon, Rene Hummen.** *Security Challenges in the IP-based Internet of Things.* 2015.
53. **Verma, Sajal.** *Searching Shodan For Fun And Profit.* 2013.

Websites

https://www.forbes.com/sites/gilpress/2016/09/02/internet-of-things-by-the-numbers-what-new-surveys-found/#2b25ed5b16a0
https://www.linkedin.com/pulse/shodan-search-engine-hackers-beginner-tutorial-yashika-dhir
https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-webcams-across-globe-using-shodan-0154830/
https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerable-targets-using-shodan-the-worlds-most-dangerous-search-engine-0154576/
https://en.wikipedia.org/wiki/Encryption
https://en.wikipedia.org/wiki/Eavesdropping
https://en.wikipedia.org/wiki/Buffer_overflow
https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/
https://www.foreignaffairs.com/articles/2014-10-31/future-cities
https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition
https://www.ft.com/content/7b880aa2-b616-11e5-b147-e5e5bba42e51
http://www.cio.co.uk/opinion/political-debate/internet-of-thieves-3634688/
https://www.technologyreview.com/s/534196/an-internet-of-treacherous-things/
https://www.technologyreview.com/s/545661/finding-insecurity-in-the-internet-of-things/
https://techcrunch.com/2016/05/09/the-internet-of-things-is-security-nightmare-warns-eff/
http://www.federaltimes.com/opinions/2016/02/04/reconciling-risk-and-value-for-the-internet-of-things/
https://www.darkreading.com/vulnerabilities---threats/iot-security-$1-per-thing-to-protect-connected-devices/a/d-id/1323921
https://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys
https://enterprisersproject.com/article/2016/2/internet-hackable-things-why-iot-devices-need-better-security
https://www.helpnetsecurity.com/2015/09/07/end-to-end-encryption-is-key-for-securing-the-internet-of-things/
https://www.nytimes.com/2016/03/03/technology/defense-secretary-takes-position-against-a-data-back-door.html?_r=1
http://www.pbs.org/newshour/updates/your-phone-metadata-is-more-revealing-than-you-think/
http://www.zdnet.com/article/who-really-owns-your-internet-of-things-data/
https://www.theguardian.com/media-network/2015/jun/01/internet-of-things-businesses-data-privacy
http://globalblog.posco.com/posco-looks-to-internet-of-things-iot-for-a-safer-workplace/
https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things
http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things
http://www.networkcomputing.com/network-security/iot-security-worries-it-pros/808058910