ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΨΗΦΙΑΚΗ ΚΑΙΝΟΤΟΜΙΑ ΚΑΙ ΔΙΟΙΚΗΣΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιθέσεις παραβίασης ασφάλειας στο Διαδίκτυο των Πραγμάτων και τεχνικές αντιμετώπισής τους

Ιωάννα Φ. Αντωνοπούλου

Επιβλέπων: Ιωάννης Σταματίου, Καθηγητής

ΠΑΤΡΑ 2022

Η παρούσα εργασία είναι αφιερωμένη στην οικογένειά μου.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία πραγματοποιήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος Σπουδών: «Ψηφιακή Καινοτομία και Διοίκηση» του Τμήματος Διοικητικής Επιστήμης και Τεχνολογίας του Πανεπιστημίου Πατρών. Η εργασία αποτελεί μια βιβλιογραφική προσέγγιση και σχετίζεται με την ανάλυση κυβερνοεπιθέσεων σε διάφορους φορείς της οικονομίας και της κοινωνίας. Στην εργασία αναλύονται τόσο οι τρόποι επίθεσης όσο και οι τρόποι άμυνας των επιθέσεων αυτών και εξάγονται χρήσιμα συμπεράσματα για την αποφυγή τέτοιου είδους επιθέσεων στο μέλλον.

Η εργασία αποτελείται από πέντε κεφάλαια όπου το κάθε ένα από αυτά αποτελεί και μια ξεχωριστή περίπτωση κυβερνοεπίθεσης και ένα ξεχωριστό κεφάλαιο συμπερασμάτων. Το πρώτο κεφάλαιο αναφέρετε σε κεβερνοεπίθεση σε αυτοκίνητο τύπου Jeep Cherokee. Στην περίπτωση αυτή αναλύεται πώς ο εισβολέας μπορεί να επιτεθεί μέσω του συστήματος infotainment του αυτοκινήτου και πως είναι δυνατό να προκαλέσει αλλαγές στη λειτουργία του αυτοκινήτου με πρόκληση ατυχημάτων. Επίσης περιγράφονται οι δυνατότητες αντιμετώπισης των επιθέσεων αυτών, όπως για παράδειγμα μέσω στατικής ανάλυσης SAST ή IAST. Στο δεύτερο κεφάλαιο γίνεται αναφορά σε μια παρουσίαση που πραγματοποιήθηκε στο Defcon του Μαϊάμι των ΗΠΑ, ένα από τα πιο μεγάλα συνέδρια για χάκερς, το 2015. Η παρουσίαση αυτή αφορούσε ένα πραγματικό γεγονός διαδικτυακής επίθεσης σε συστήματα ελέγχου κυκλοφορίας. Το τρίτο κεφάλαιο αναφέρετε σε φορείς υγείας. Σε αυτό περιγράφονται ευρήματα από την έρευνα, που τονίζουν τις κύριες ανησυχίες σχετικά με την ασφάλεια και την αρχιτεκτονική συστημάτων εμφυτεύσιμων καρδιακών συσκευών. Συνεχίζοντας στο τέταρτο κεφάλαιο η εργασία αναφέρετε πάλι στον τομέα της υγείας και συγκεκριμένα σε μια πραγματική ανάλυση ασφάλειας σε τρία νοσοκομεία με παραβιασμένα ενδονοσοκομειακά ιατρικά IOT συστήματα. Οι επιθέσεις αυτές χαρακτηρίζονται στη βιβλιογραφία ως MEDJACK, ή "αεροπειρατεία ιατρικών συσκευών". Στο επόμενο κεφάλαιο, κεφάλαιο πέντε, αναλύονται τα θέματα των κυβερνοεπιθέσεων σε βιομηχανικές μονάδες διανομής ηλεκτρικής ενέργειας καθώς και τρόποι αντιμετώπισής τους. Τέλος στο κεφάλαιο έξι ακολουθούν τα συμπεράσματα και οι μελλοντικές προοπτικές της εργασίας.

Από την παρούσα εργασία εξήχθησαν τα κάτωθι κύρια συμπεράσματα. Όσον αφορά την επίθεση του πρώτου κεφαλαίου διαπιστώθηκε ότι εύκολα προσβάλετε το σύστημα διαχείρισης πληροφορίας (Infotainment system) ενός αυτοκινήτου, όμως υπάρχουν και προτεινόμενοι τρόποι αντιμετώπισης αυτού. Στην επίθεση του δεύτερου κεφαλαίου φάνηκε η σπουδαιότητα ελέγχου των συστημάτων ελέγχου της κυκλοφορίας, διότι αυτά μπορούν να προσβληθούν πολύ εύκολα. Προτείνονται τρόποι αντιμετώπισης των εισβολέων. Σαν κύριο συμπέρασμα του τρίτου κεφαλαίου είναι ότι η αντιμετώπιση αυτού του είδους των επιθέσεων, απαιτεί την ομαδοποίηση

των ευρημάτων από τους προμηθευτές για την πιο δόκιμη αντιμετώπιση των εισβολέων. Ένα από τα κύρια συμπεράσματα του τέταρτου κεφαλαίου είναι ότι οι εισβολείς έχουν αναπτύξει προηγμένα κακόβουλα λογισμικά προκειμένου να εισβάλουν στα πληροφοριακά συστήματα νοσοκομειακών μονάδων. Ένας από τους κύριους τρόπους αντιμετώπισης τέτοιου είδους επιθέσεων προτείνεται η απομόνωση των ιατρικών συσκευών μέσα σε ένα ασφαλές δίκτυο και προστασία αυτού με ένα εσωτερικό τείχος προστασίας που θα επιτρέπει την πρόσβαση μόνο σε συγκεκριμένες υπηρεσίες και διευθύνσεις IP. Τέλος στο πέμπτο κεφάλαιο το κύριο συμπέρασμα που διεξήχθη είναι ότι πρέπει να λαμβάνετε υπόψη η προηγούμενη αλληλουχία των γεγονότων που έλαβε χώρα από τον επιτιθέμενο προτού διεξάγει την επίθεση.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Διαδίκτυο των Πραγμάτων (IoT), Κυβερνοεπίθεση, Κυβερνοασφάλεια

ABSTRACT

The present work was carried out in the framework of the Postgraduate Program: "Digital Innovation and Management" of the Department of Management Science and Technology of the University of Patras. The work is a bibliographic approach and is related to the analysis of cyber attacks in various sectors of the economy and society. The paper analyzes both the ways of attack and the ways of defending these attacks and draws useful conclusions to avoid such attacks in the future.

The work consists of five chapters where each of them is a separate case of cyber attack and a separate chapter of conclusions. The first chapter deals with a cyber attack on a Jeep Cherokee. In this case it is analyzed how the intruder can attack through the infotainment system of the car and how it is possible to cause changes in the operation of the car by causing accidents. It also describes how to deal with these attacks, such as through static analysis (SAST) or IAST. The second chapter refers to a presentation held at Defcon in Miami, USA, one of the largest conferences for hackers, in 2015. This presentation was about a real cyber attack on traffic control systems. The third chapter refers to health care providers. It describes research findings that highlight major concerns about the safety and architecture of implantable cardiac device systems. Continuing in the fourth chapter, the work refers again to the field of health and specifically to a real safety analysis in three hospitals with violated in-hospital medical IOT systems. These attacks are described in the literature as MEDJACK, or "medical device hijacking". The next chapter, chapter five, analyzes the issues of cyber attacks on industrial power distribution units and ways to deal with them. Finally in chapter six follow the conclusions and future perspectives of the work.

The following main conclusions were drawn from the present work. Regarding the attack of the first chapter, it was found that you easily attack the information management system (Infotainment system) of a car, but there are also suggested ways to deal with it. The attack on the second chapter showed the importance of controlling traffic control systems, because they can be attacked very easily. Ways to deal with intruders are suggested. The main conclusion of the third chapter is that dealing with this type of attack, requires the grouping of findings by suppliers for the most tried and tested treatment of intruders. One of the main conclusions of the fourth chapter is that intruders have developed advanced malware in order to invade hospital information systems. One of the main ways to deal with such attacks is to isolate medical devices within a secure network and protect it with an internal firewall that will only allow access to specific services and IP addresses. Finally in the fifth chapter the main conclusion reached is that you must take into account the previous sequence of events that took place by the attacker before carrying out the attack.

KEY WORDS: Internet of Thinks, Cyberattack, Cyber Security.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ 1

1. ΕΛΕΓΧΟΣ ΑΥΤΟΚΙΝΗΤΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ, ΜΕ ΚΑΤΑΧΡΗΣΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ INFOTAINMENT 3

1.1 ΕΙΣΑΓΩΓΗ 3

1.2 ΑΙΤΙΟΛΟΓΗΣΗ ΕΠΙΛΟΓΗΣ 4

1.3 ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΟΣΥΣΤΗΜΑΤΑ ΤΟΥ ΑΥΤΟΚΙΝΗΤΟΥ 6

1.3.1 Προσαρμοστικός έλεγχος οδήγησης (Adaptive Cruise Control) (ACC) 7

1.3.2 Προειδοποίηση πρόσκρουσης εμπροσθοπορείας (Forward Collision Warning Plus) (FCW+) 7

1.3.3 Προειδοποίηση Αλλαγής Λωρίδας (Lane Departure Warning) (LDW+) 7

1.3.4 Σύστημα υποβοήθησης στάθμευσης (Park Assist System) (PAM) 8

1.4 ΠΙΘΑΝΑ ΣΥΣΤΗΜΑΤΑ ΤΟΥ JEEP CHEROKEE 2014 ΕΥΑΛΩΤΑ ΕΠΙΘΕΣΕΩΝ 8

1.4.1 Παθητικό αντικλεπτικό σύστημα (Passive Anti-Theft System) (PATS) 8

1.4.2 Σύστημα παρακολούθησης πίεσης ελαστικών (Tire Pressure Monitoring System) (TPMS) 9

1.4.3 Απομακρυσμένη είσοδος/εκκίνηση χωρίς κλειδί (Remote Keyless Entry/Start) (RKE) 9

1.4.4 Bluetooth 10

1.4.5 Σύστημα ραδιοφωνικών δεδομένων (Radio Data System) 10

1.4.6 Wi-Fi 11

1.4.7 Τηλεματική / εφαρμογές διαδικτύου (Telematics/Internet/Apps) 11

1.5 ΜΗ ΔΙΑΣΥΝΔΕΔΕΜΕΝΟ ΣΥΣΤΗΜΑ (UCONNECT SYSTEM) 11

1.5.1 Περιβάλλον πλατφόρμας QNX και αξιοπιστία αυτοκινήτου 12

1.5.2 Κρυπτογράφηση 13

1.5.3 Ανοιχτή θύρα (Open port) 14

1.6 ΜΗ ΔΙΑΣΥΝΔΕΔΕΜΕΝΑ ΣΥΣΤΗΜΑ ΕΥΑΛΩΤΑ ΕΠΙΘΕΣΕΩΝ (UCONNECT ATTACK PAYLOADS) 14

1.6.1 Το παγκόσμιο σύστημα εντοπισμού θέσης (Global Positioning System(GPS)) 14

1.6.2 HVAC 14

1.6.3 Ένταση ραδιοφώνου (Radio Volume) 14

1.6.4 Μπάσα (Bass) 15

1.6.5 Ραδιοφωνικός Σταθμός (FM) 15

1.6.6 Απεικόνιση (Display) 15

1.6.7 Κομβία (Knobs) 15

1.7 ΟΛΟΚΛΗΡΗ Η ΑΛΥΣΙΔΑ ΕΝΕΡΓΕΙΩΝ ΤΗΣ ΕΠΙΘΕΣΗΣ 15

1.8 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ – ΠΡΟΛΗΨΗΣ ΕΠΙΘΕΣΕΩΝ 17

1.8.1 Στατική ανάλυση (SAST) για κυβερνοασφάλεια αυτοκινήτου 17

1.8.2 IAST για την ασφάλεια στον κυβερνοχώρο αυτοκινήτων 18

1.8.3 SCA για ασφάλεια στον κυβερνοχώρο αυτοκινήτων 18

1.9 ΣΥΜΠΕΡΑΣΜΑ 19

2. ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΗΣ ΡΑΔΙΟΕΠΙΚΟΙΝΩΝΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΕΛΕΓΧΟΥ ΤΗΣ ΚΥΚΛΟΦΟΡΙΑΣ ΓΙΑ ΤΟΝ ΕΛΕΓΧΟ ΤΟΥΣ 20

2.1 ΓΕΝΙΚΑ 20

2.2 ΤΟ ΔΙΚΤΥΟ ΤΩΝ ΑΙΣΘΗΤΗΡΩΝ ΣΤΗΝ ΟΥΑΣΙΓΚΤΟΝ 21

2.3 ΟΙ ΑΙΣΘΗΤΗΡΕΣ ΚΑΙ Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥΣ 22

2.4 ΕΥΠΑΘΕΙΕΣ ΣΥΣΤΗΜΑΤΟΣ ΚΥΚΛΟΦΟΡΙΑΣ 26

2.5 ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΛΕΓΧΟΥ 27

2.6 ΒΑΡΥΤΗΤΑ ΕΠΙΘΕΣΕΩΝ 28

2.7 ΤΡΟΠΟΙ ΕΚΔΗΛΩΣΗΣ ΕΠΙΘΕΣΕΩΝ 28

2.8 ΣΥΜΠΕΡΑΣΜΑΤΑ 29

3. ΕΚΜΕΤΑΛΛΕΥΣΗ ΙΔΙΟΚΤΗΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΔΙΚΤΥΟΥ ΓΙΑ ΤΟΝ ΕΛΕΓΧΟ ΒΗΜΑΤΟΔΟΤΗ 30

3.1 ΓΕΝΙΚΑ 30

3.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΤΟΥ ΟΙΚΟΣΥΣΤΗΜΑΤΟΣ 31

3.3 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ 34

3.4 ΕΥΡΗΜΑΤΑ 35

3.5 ΔΥΝΑΤΟΤΗΤΑ ΑΠΟΚΤΗΣΗΣ ΤΩΝ ΥΠΟ ΠΡΟΜΗΘΕΙΑ ΥΠΟΣΥΣΤΗΜΑΤΩΝ ΑΠΟ ΔΗΜΟΣΙΟΥΣ ΦΟΡΕΙΣ 36

3.6 ΕΥΑΛΩΤΑ-ΤΡΩΤΑ ΣΗΜΕΙΑ ΣΤΟ ΟΙΚΟΣΥΣΤΗΜΑ ΤΩΝ ΕΜΦΥΤΕΥΣΙΜΩΝ ΚΑΡΔΙΑΚΩΝ ΣΥΣΚΕΥΩΝ 36

3.6.1 Εμπορικοί μικροεπεξεργαστές άμεσα διαθέσιμοι (στο ράφι) 36

3.6.2 Διεπαφές εντοπισμού σφαλμάτων σε ενσωματωμένη συσκευή 37

3.6.3 Κρυπτογραφημένο υλικολογισμικό 38

3.6.4 Εμποτισμένες -κρυφές συσκευές και επαφές για επανέλεγχο 38

3.6.5 Χρήση συναρτήσεων λειτουργίας τύπου ASCII και αντιμετώπιση λογισμικού 38
3.6.6 Χρήση βιβλιοθηκών τρίτων 39
3.6.7 Χαρτογράφηση της εικόνας του υλικολογισμικού σε προστατευμένη μνήμη 39
3.6.8 Εξωτερικές συνδέσεις με USB (Universal Serial Bus) 40
3.6.9 Κωδικοποιημένα διαπιστευτήρια και δεδομένα υποδομής 40
3.6.10 Ενεργοποίηση ραδιοσυχνοτήτων (RF) 41
3.6.11 Απομακρυσμένη ενημέρωση υλικολογισμικού 41
3.6.12 Ψηφιακά υπογεγραμμένο υλικολογισμικό 41
3.6.13 Αφαιρούμενα μέσα/σκληροί δίσκοι 41
3.6.14 Κρυπτογράφηση 41
3.6.15 Μη κρυπτογραφημένα δεδομένα ασθενών 42
3.6.16 Αυθεντικοποίηση για τη διενέργεια προγραμματισμού 42
3.6.17 Εφαρμογές προγραμματισμού ιατρών 42
3.6.18 Διπλή χρήση ραδιοεξοπλισμού για συσκευή οικιακής παρακολούθησης και προγραμματιστή ιατρών 43
3.6.19 Λευκή λίστα εντολών 43
3.6.20 Παγκόσμιο διακριτικό ελέγχου ταυτότητας 43
3.7 ΣΥΝΟΨΗ ΤΩΝ ΕΥΡΗΜΑΤΩΝ 43
3.8 ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΕΛΕΓΧΩΝ ΑΣΦΑΛΕΙΑΣ 44
3.9 ΣΥΜΠΕΡΑΣΜΑΤΑ 45
4. ΠΡΑΓΜΑΤΙΚΗ ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ ΤΡΙΩΝ ΝΟΣΟΚΟΜΕΙΩΝ ΜΕ ΠΑΡΑΒΙΑΣΜΕΝΑ ΕΝΔΟΝΟΣΟΚΟΜΕΙΑΚΑ ΙΑΤΡΙΚΑ ΙΟΤ ΣΥΣΤΗΜΑΤΑ 46
4.1 ΓΕΝΙΚΑ 46
4.2 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ - ΝΟΣΟΚΟΜΕΙΟ #1 49
4.2.1 *Επισκόπηση* 49
4.2.2 Ανάπτυξη και Ανάλυση 50
4.3 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ - ΝΟΣΟΚΟΜΕΙΟ #2 51
4.3.1 Επισκόπηση 52
4.3.2 *Ανάπτυξη και Ανάλυση* 52
4.4 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ - ΝΟΣΟΚΟΜΕΙΟ #3 55
4.4.1 Επισκόπηση 55
4.4.2 Ανάπτυξη και Ανάλυση 56

4.5 ΚΑΤΑΝΟΗΣΗ ΤΟΥ MEDJACK.2 57

4.6 ΣΥΜΠΕΡΑΣΜΑΤΑ 57

4.7 ΣΥΣΤΑΣΕΙΣ 59

4.8 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ -ΣΥΣΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΜΥΝΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ 60

5. ΕΠΙΘΕΣΕΙΣ ΣΤΟ ΕΞΥΠΝΟ ΔΙΚΤΥΟ ΜΕΤΑΦΟΡΑΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ ΤΗΣ ΟΥΚΡΑΝΙΑΣ 62

5.1 ΕΙΣΑΓΩΓΗ 62

5.2 ΤΕΧΝΙΚΕΣ ΕΠΙΤΙΘΕΜΕΝΟΥ ΚΑΙ ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ 63

5.3 ΧΑΡΤΟΓΡΑΦΗΣΗ ΤΗΣ ΑΛΥΣΙΔΑΣ ΚΥΒΕΡΝΟ-ΘΑΝΑΤΟΥ (ICS CYBER KILL CHAIN) 68

5.4 ΜΑΘΗΜΑΤΑ ΑΜΥΝΑΣ - ΠΑΘΗΤΙΚΗ ΚΑΙ ΕΝΕΡΓΗΤΙΚΗ ΑΜΥΝΑ 68

5.4.1 Το φαινόμενο του Spear Phishing 69

5.4.2 Κλοπή διαπιστευτηρίων 71

5.4.3 Διείσδυση δεδομένων 72

5.4.4 Πρόσβαση VPN 73

5.4.5 Απομακρυσμένη πρόσβαση στο σταθμό εργασίας 74

5.4.6 Έλεγχος και λειτουργία 75

5.4.7 Επιπτώσεις σε εργαλεία και τεχνολογία 76

5.4.8 Ανταπόκριση και αποκατάσταση 78

5.5 ΣΥΣΤΑΣΕΙΣ 80

5.5.1 Αρχιτεκτονική 80

5.5.2 Παθητική άμυνα 80

5.5.3 Ενεργός άμυνα 81

5.6 ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ 82

5.6.1 Επιπτώσεις για τους υπερασπιστές 82

5.6.2 Συμπεράσματα 83

6. ΣΥΜΠΕΡΑΣΜΑΤΑ 85

ΒΙΒΛΙΟΓΡΑΦΙΑ 88

ΕΙΣΑΓΩΓΗ

Στις αρχές του 21ου αιώνα, οι τεράστιες πρόοδοι στον τομέα της επιστήμης των υπολογιστών και των συναφών τομέων, όπως η τεχνητή νοημοσύνη, η εικονική πραγματικότητα, η ρομποτική και ο ψηφιακός σχεδιασμός οδήγησαν σε μια νέα βιομηχανική επανάσταση, συγκεκριμένα την 4η βιομηχανική επανάσταση που στοχεύει στην επίτευξη προηγμένης αυτοματοποίησης των υπαρχουσών βιομηχανικών κατασκευών που χρησιμοποιούν σύγχρονη έξυπνη τεχνολογία. Με παρόμοιο τρόπο με τις τρεις πρώτες βιομηχανικές επαναστάσεις, οι οποίες θεωρούνται ως αποτέλεσμα σημαντικών τεχνολογικών επιτευγμάτων όπως η μηχανοποίηση, η ηλεκτρική ενέργεια και η τεχνολογία της πληροφορίας, η 4η βιομηχανική επανάσταση είναι μια έννοια στενά συνδεδεμένη με διάφορες τεχνολογίες, όπως το Internet of Things (IoT) , Big Data, data mining και cloud computing και οδηγεί σε σημαντικό μετασχηματισμό και αναβάθμιση των παραδοσιακών βιομηχανιών παραγωγής. Παράλληλα όμως με την πρόοδο μέσω της 4ης βιομηχανικής επανάστασης δημιουργήθηκε η ανάγκη για διασφάλιση της μεταφερόμενης πληροφορίας μεταξύ των διαφόρων συστημάτων.

Η παρούσα εργασία αποτελεί μια βιβλιογραφική ανασκόπηση σε επιθέσεις παραβίασης ασφάλειας στο Διαδίκτυο των Πραγμάτων, οι οποίες πραγματοποιήθηκαν σε προηγμένα συστήματα και υπηρεσίες τόσο σε οικονομικούς όσο και σε κοινωνικούς φορείς. Η επιλογή ήταν τέτοια των επιθέσεων που αναλύθηκαν έτσι ώστε να αντιπροσωπεύουν κυρίαρχες δράσεις της καθημερινής ζωής οι οποίες είναι ευάλωτες σε επιθέσεις, αλλά πολύ διδακτικές για τον ερευνητή του μέλλοντος.

Οι στόχοι της διπλωματικής είναι: α) η κατανόηση μέρους διαδικτυακών επιθέσεων, β) οι τρόποι με τους οποίους πραγματοποιήθηκαν, γ) οι συνέπιες που αυτές μπορεί να έχουν τόσο την οικονομική όσο και στην κοινωνική ζωή και δ) να μελετηθούν ενδελεχώς και να αναφερθούν οι τρόποι αντιμετώπισης αυτών που είναι γνωστοί ως σήμερα. Έτσι λοιπόν σκοπεύουμε να δώσουμε τα παραπάνω με τη μεγαλύτερη δυνατή κατανόηση, ώστε στο τέλος με τα συνολικά συμπεράσματα καθώς και τη μελλοντική έρευνα να δείξουμε πως αυτά συνδέονται με τη ψηφιακή καινοτομία και διοίκηση.

Για να πραγματοποιηθούν αυτά τα οποία περιγράφουμε στις παραπάνω παραγράφους εξετάστηκε η τρέχουσα στάθμη της βιβλιογραφίας από την οποία έλαβα υλικό για τις επιθέσεις. Έτσι σύμφωνα με τους C. Miller and C. Valasek παρουσιάστηκε διαδικτυακή επίθεση στο αυτοκίνητο Jeep Cherokee, όπου αναλυθήκαν τα αίτια, τα αποτελέσματα και οι τρόποι αντιμετώπισης. Συνεχίζοντας, ο Cerrudo στο συνέδριο στο Defcon του Μαϊάμι των ΗΠΑ παρουσίασε ένα πραγματικό γεγονός διαδικτυακής επίθεσης σε συστήματα

ελέγχου κυκλοφορίας. Εν συνεχεία, οι Rios and J. Butts στην τεχνική τους αναφορά στο WhiteScope το 2017, παρείχαν στοιχεία για το εμφυτεύσιμο οικοσύστημα καρδιακών συσκευών. Τα ερευνητικά εργαστήρια TrapX δημοσίευσαν το 2015 μια έκθεση σχετικά με την ανακάλυψη και ανάλυση τριών στοχευμένων επιθέσεων σε νοσοκομεία. Τέλος τα περιοδικά E-ISAC και SANS παρέχουν πληροφορίες σχετικά με επιθέσεις που πραγματοποιήθηκαν το 2015 σε Ουκρανικές εταιρείες διανομής ηλεκτρικής ενέργειας.

Η εργασία δεν είναι ερευνητική ως εκ τούτου δεν υπάρχει προτεινόμενη μεθοδολογία στην ανάπτυξη του προβλήματος. Ωστόσο γράψαμε παραπάνω επιχειρήθηκε στα πλαίσια της ανασκόπησης μια μεθοδολογική προσέγγιση για κάθε μία εκ των επιθέσεων, όπου φαίνεται ο τρόπος επίθεσης, οι συνέπειες και οι τρόποι αντιμετώπισής τους.

Η εργασία αποτελείται από πέντε κεφάλαια όπου το κάθε ένα από αυτά αποτελεί και μια ξεχωριστή περίπτωση κυβερνοεπίθεσης και ένα ξεχωριστό κεφάλαιο συμπερασμάτων. Το πρώτο κεφάλαιο αναφέρεται σε κεβερνοεπίθεση σε αυτοκίνητο τύπου Jeep Cherokee. Στην περίπτωση αυτή αναλύεται πώς ο εισβολέας μπορεί να επιτεθεί μέσω του συστήματος infotainment του αυτοκινήτου και πως είναι δυνατό να προκαλέσει αλλαγές στη λειτουργία του αυτοκινήτου με πρόκληση ατυχημάτων. Επίσης περιγράφονται οι δυνατότητες αντιμετώπισης των επιθέσεων αυτών, όπως για παράδειγμα μέσω στατικής ανάλυσης SAST ή IAST. Στο δεύτερο κεφάλαιο γίνεται αναφορά σε μια παρουσίαση που πραγματοποιήθηκε στο Defcon του Μαϊάμι των ΗΠΑ, ένα από τα πιο μεγάλα συνέδρια για χάκερς, το 2015. Η παρουσίαση αυτή αφορούσε ένα πραγματικό γεγονός διαδικτυακής επίθεσης σε συστήματα ελέγχου κυκλοφορίας. Το τρίτο κεφάλαιο αναφέρετε σε φορείς υγείας. Σε αυτό περιγράφονται ευρήματα από την έρευνα, που τονίζουν τις κύριες ανησυχίες σχετικά με την ασφάλεια και την αρχιτεκτονική συστημάτων εμφυτεύσιμων καρδιακών συσκευών. Συνεχίζοντας στο τέταρτο κεφάλαιο η εργασία αναφέρεται πάλι στον τομέα της υγείας και συγκεκριμένα σε μια πραγματική ανάλυση ασφάλειας σε τρία νοσοκομεία με παραβιασμένα ενδονοσοκομειακά ιατρικά IOT συστήματα. Οι επιθέσεις αυτές χαρακτηρίζονται στη βιβλιογραφία ως MEDJACK, ή "αεροπειρατεία ιατρικών συσκευών". Στο επόμενο κεφάλαιο, κεφάλαιο πέντε, αναλύονται τα θέματα των κυβερνοεπιθέσεων σε βιομηχανικές μονάδες διανομής ηλεκτρικής ενέργειας καθώς και τρόποι αντιμετώπισής τους. Τέλος στο κεφάλαιο έξι ακολουθούν τα συμπεράσματα και οι μελλοντικές προοπτικές της εργασίας.

1. ΕΛΕΓΧΟΣ ΑΥΤΟΚΙΝΗΤΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ, ΜΕ ΚΑΤΑΧΡΗΣΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ INFOTAINMENT

1.1 ΕΙΣΑΓΩΓΗ

Στα 80 χρόνια μαζικής παραγωγής, το επιβατικό αυτοκίνητο παρέμενε επιφανειακά στατικό: ένας μόνο βενζινοκινητήρας εσωτερικής καύσης, τέσσερις τροχοί και τη γνωστή διεπαφή χρήστη τιμονιού, γκαζιού, αλλαγής ταχυτήτων και φρένου. Ωστόσο, τις τελευταίες δύο δεκαετίες τα υποκείμενα συστήματα ελέγχου έχουν αλλάξει δραματικά. Το σημερινό αυτοκίνητο δεν είναι απλώς μια μηχανική συσκευή, αλλά περιέχει και πλειάδα ηλεκτρονικών υπολογιστικών συστημάτων. Αυτοί οι υπολογιστές συντονίζουν και παρακολουθούν αισθητήρες και εξαρτήματα, τον οδηγό και φυσικά τους επιβάτες. Πράγματι, μια πρόσφατη έρευνα υποδηλώνει ότι ένα τυπικό πολυτελές sedan σήμερα περιέχει πάνω από 100 MB δυαδικού κώδικα σε 50-70 ανεξάρτητους υπολογιστές - Electronic Control Units (ECUs) οι οποίοι επικοινωνούν με ένα ή περισσότερα κοινόχρηστα οχήματα π.χ. λεωφορεία ενός δημοτικού δικτύου συγκοινωνίας (Charette, 2009), (Emaus, 2005).

Ενώ η αυτοκινητοβιομηχανία πάντα θεωρούσε υψηλής ασφάλειας τα συστήματα πέδησης και τα συστήματα των κλειδαριών, δεν είναι σαφές εάν οι κατασκευαστές οχημάτων έχουν προβλέψει στα σχέδιά τους την πιθανότητα προσβολής συστημάτων των αυτοκινήτων τους από αντιπάλους- εξωτερικές πηγές.

Πράγματι, φαίνεται να είναι πιθανό ότι αυτός ο αυξανόμενος βαθμός ελέγχου από λογισμικά, παρακολουθείται επίσης, από μια αντίστοιχη σειρά πιθανών απειλών. Συνδυάζοντας αυτό το ζήτημα, η επιφάνεια επίθεσης για τα σύγχρονα αυτοκίνητα αυξάνεται ραγδαία καθώς οι πιο εξελιγμένες υπηρεσίες και επικοινωνιακά χαρακτηριστικά ενσωματώνονται σε οχήματα.

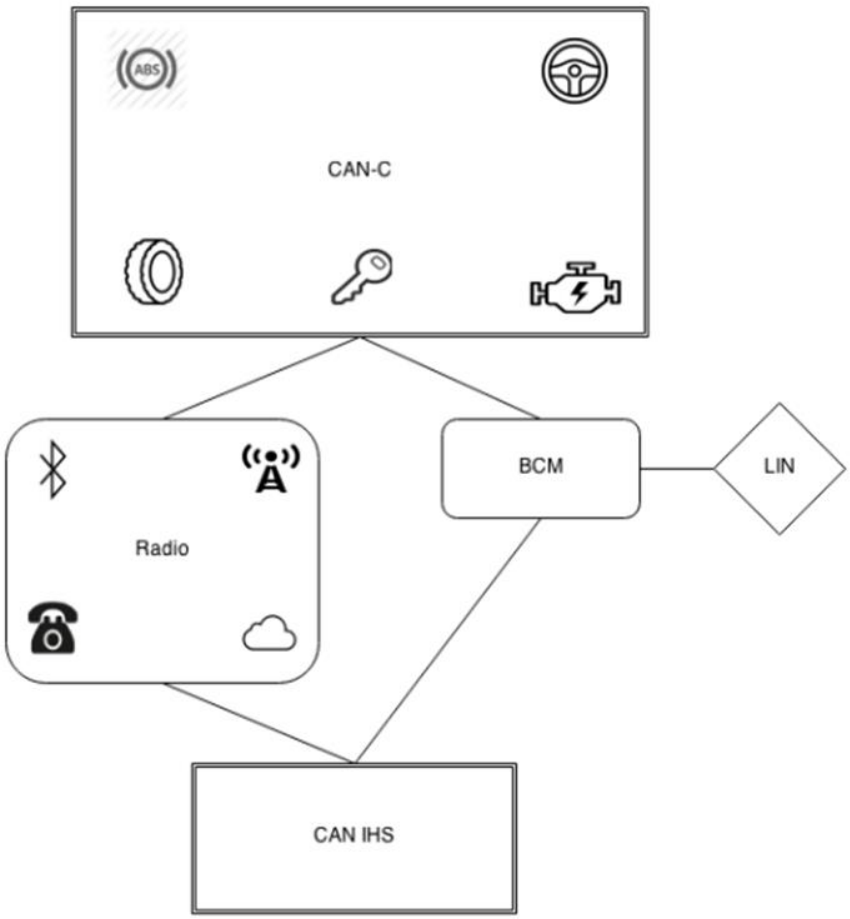
Στις Ηνωμένες Πολιτείες, η ομοσπονδιακή απόφαση για διαγνωστική σφαλμάτων κατά την οδήγηση (On-Board Diagnostics (OBD-II)), σε ουσιαστικά όλα τα σύγχρονα οχήματα, παρέχει άμεση και τυπική πρόσβαση σε εσωτερικά δίκτυα ελέγχου αυτοκίνησης. Τα συστήματα αναβάθμισης χρήστη, όπως οι συσκευές αναπαραγωγής ήχου, συνδέονται συνήθως με τα ίδια εσωτερικά δίκτυα, όπως και μια ποικιλία ασύρματων συσκευών μικρής εμβέλειας (Bluetooth, αισθητήρες ασύρματης πίεσης ελαστικών κλπ.). Τα συστήματα τηλεματικής, για παράδειγμα του OnStar της GeneralMotors (GM), έχουν προστιθέμενη αξία καθώς παρέχουν αυτόματη απόκριση σε σύγκρουση, απομακρυσμένα διαγνωστικά μηνύματα και ανάκτηση πληροφορίας για τυχόν κλεμμένα οχήματα, μέσω ασύρματου συνδέσμου μεγάλης εμβέλειας.

Προς το παρόν, αυτά τα τηλεματικά συστήματα ενσωματώνουν εσωτερικά υποσυστήματα αυτοκινήτων με ένα απομακρυσμένο κέντρο εντολών μέσω μιας κυψελοειδούς σύνδεσης ευρείας περιοχής συχνοτήτων. Κάποιοι ερευνητές, το έχουν προχωρήσει ακόμα περισσότερο προτείνοντας ένα μοντέλο «αυτοκίνητο ως πλατφόρμα». Η Hughes Telematics έχει περιγράψει σχέδια για την ανάπτυξη ενός "App Store" για εφαρμογές αυτοκινήτων (Mollman, 2009), ενώ η Ford ανακοίνωσε ότι θα ανοίξει το τηλεματικό σύστημα Sync ως πλατφόρμα για εφαρμογές στην αυτοκίνηση (Goodwin, 2009). Τέλος, τα προτεινόμενα μελλοντικά συστήματα επικοινωνίας από όχημα σε όχημα (V2V) και από όχημα σε υποδομή (V2X) (“Cooperative intersection collision avoidance system” 2008), (“Vehicle safety communications” 2008), (“Vehicle safety communications 2005), (“Intersection collision avoidance” 2007) θα διευρύνουν ακόμη περισσότερο την επιφάνεια επιθέσεων.

1.2 ΑΙΤΙΟΛΟΓΗΣΗ ΕΠΙΛΟΓΗΣ

Το Jeep Cherokee του 2014 επιλέχθηκε από τους ερευνητές Dr. Charlie Miller και Chris Valasek επειδή πίστευαν ότι θα τους έδινε την καλύτερη ευκαιρία να αποδείξουν με επιτυχία ότι ένας απομακρυσμένος έλεγχος ενός οχήματος θα μπορούσε να οδηγήσει σε αποστολή μηνυμάτων, όπου θα μπορούσαν να εισβάλουν στην ιδιωτικότητα του οδηγού και να εκτελέσουν φυσικές ενέργειες για λογαριασμό του εισβολέα. Όπως επισήμαναν σε προηγούμενη έρευνά τους (http://illmatics.com/remote%20attack%20surfaces.pdf), αυτό το όχημα φαινόταν να παρουσιάζει λιγότερα πιθανά εμπόδια για έναν επιτιθέμενο. Αυτό δεν σημαίνει ότι τα οχήματα άλλων κατασκευαστών ή τύπων δεν μπορούν να προσβληθούν, επιθυμώντας να δείξουν ότι το Cherokee ήταν η καλύτερη επιλογή. Ακόμα ένας σημαντικός λόγος ήταν ότι, το εν λόγω Jeep εμπίπτει και στους οικονομικούς περιορισμούς, σε περίπτωση που προστίθενται όλα τα τεχνολογικά χαρακτηριστικά που απαιτούν για τη έρευνα τους οι συγγραφείς (Dr. Charlie Miller και Chris Valasek) του εν λόγω άρθρου.

Η αρχιτεκτονική του μοντέλου Jeep Cherokee του 2014, ήταν πολύ ενδιαφέρουσα για τους παραπάνω ερευνητές λόγω του γεγονότος ότι η κεντρική μονάδα (Ραδιόφωνο) συνδέεται και με τα δύο πρωτόκολλα τύπου λεωφορείου CAN (Controller area network Bus), που έχουν εφαρμοστεί στο όχημα (Σχήμα 1).



Σχήμα 1: Διάγραμμα αρχιτεκτονικής Jeep Cherokee 2014 (Miller C. and Valasek C., 2015)

Υπέθεσαν ότι εάν το Ραδιόφωνο μπορούσε να παραβιαστεί, τότε θα είχαν πρόσβαση στην κεντρική μονάδα ελέγχου (Electronic Central Unit-ECU) και στα ηλεκτρονικά δίκτυα CAN-IHS και CAN-C, γεγονός που σημαίνει ότι θα μπορούσαν να αποσταλούν μηνύματα σε όλες τις ECU που ελέγχουν τα φυσικά χαρακτηριστικά λειτουργίας του οχήματος.

Ο απομακρυσμένος έλεγχος της κεντρικής μονάδας δεν οδηγεί άμεσα στην πρόσβαση στα πρωτόκολλα CAN, και θα ήταν δε απαραίτητα περαιτέρω στάδια ελέγχου. Με όσα είναι γνωστά, δεν υπάρχουν αρχιτεκτονικοί περιορισμοί πρωτοκόλλων CAN, όπως π.χ. το σύστημα διεύθυνσης που είναι τοποθετημένο σε ένα ξεχωριστό πρωτόκολλο CAN. Εάν μπορούν να σταλούν μηνύματα από την κεντρική μονάδα, θα είναι δυνατόν να αποσταλούν σε κάθε ECU του πρωτοκόλλου CAN.

CAN C Bus
1. ABS MODULE - ANTI-LOCK BRAKES
2. AHLM MODULE - HEADLAMP LEVELING
3. ACC MODULE - ADAPTIVE CRUISE CONTROL
4. **BCM MODULE - BODY CONTROL**
5. CCB CONNECTOR - STAR CAN C BODY
6. CCIP CONNECTOR - STAR CAN C IP
7. **DLC DATA LINK CONNECTOR**
8. DTCM MODULE - DRIVETRAIN CONTROL
9. EPB MODULE - ELECTRONIC PARKING BRAKE
10. EPS MODULE - ELECTRIC POWER STEERING
11. ESM MODULE - ELECTRONIC SHIFT
12. FFCM CAMERA - FORWARD FACING
13. IPC CLUSTER
14. OCM MODULE - OCCUPANT CLASSIFICATION
15. ORC MODULE - OCCUPANT RESTRAINT CONTROLLER
16. PAM MODULE - PARK ASSIST
17. PCM MODULE - POWERTRAIN CONTROL (2.4L)
18. **RADIO MODULE - RADIO**
19. RFH MODULE - RADIO FREQUENCY HUB
20. SCM MODULE - STEERING CONTROL
21. SCLM MODULE - STEERING COLUMN LOCK
22. TCM MODULE - TRANSMISSION CONTROL

CAN IHS Bus
1. AMP AMPLIFIER - RADIO
2. **BCM MODULE - BODY CONTROL**
3. CCB CONNECTOR - STAR CAN IHS BODY
4. CCIP CONNECTOR - STAR CAN IHS IP
5. DDM MODULE - DOOR DRIVER
6. DLC DATA LINK CONNECTOR
7. EDM MODULE - EXTERNAL DISC
8. HSM MODULE - HEATED SEATS
9. HVAC MODULE - A/C HEATER
10. ICS MODULE - INTEGRATED CENTER STACK SWITCH
11. IPC MODULE - CLUSTER
12. LBSS SENSOR - BLIND SPOT LEFT REAR
13. MSM MODULE - MEMORY SEAT DRIVER
14. PDM MODULE - DOOR PASSENGER
15. PLGM MODULE - POWER LIFTGATE
16. **RADIO MODULE - RADIO (Not a Bridge)**
17. RBSS SENSOR - BLIND SPOT RIGHT REAR

Πίνακας 1: Επεξήγηση συμβόλων (Miller C. and Valasek C., 2015)

1.3 ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΥΠΟΣΥΣΤΗΜΑΤΑ ΤΟΥ ΑΥΤΟΚΙΝΗΤΟΥ

Κυβερνοφυσικά Χαρακτηριστικά (Cyber Physical Features)

Αυτή η ενότητα περιγράφει τα συστήματα που χρησιμοποιήθηκαν στο Jeep Cherokee του 2014 για υποβοηθούμενη οδήγηση. Αυτές οι τεχνολογίες είναι ιδιαίτερα ενδιαφέρουσες καθώς παρόμοια συστήματα, είχαν χρησιμοποιηθεί προηγουμένως σε επιθέσεις για να αποκτήσουν πρόσβαση σε φυσικά χαρακτηριστικά λειτουργίας του αυτοκινήτου (http://illmatics.com/content.zip). Οι τεχνολογικές εξελίξεις αυξάνουν την ασφάλεια του οδηγού και του περιβάλλοντός του, παρέχουν όμως και την ευκαιρία σε έναν εισβολέα να τα χρησιμοποιήσει ως μέσο ελέγχου του οχήματος.

1.3.1 Προσαρμοστικός έλεγχος οδήγησης (Adaptive Cruise Control) (ACC)

Το Jeep του 2014 που χρησιμοποιήθηκε στις δοκιμές είχε Adaptive Cruise Control (ACC), το οποίο είναι μια τεχνολογία που βοηθά τον οδηγό να διατηρεί τη σωστή απόσταση μεταξύ των αυτοκινήτων. Ουσιαστικά, διασφαλίζει ότι εάν το cruise control είναι ενεργοποιημένο και ένα όχημα επιβραδύνει μπροστά του, τότε το Jeep θα ενεργοποιήσει τα φρένα με την κατάλληλη πίεση για να αποφύγει σύγκρουση και θα συνεχίσει με την ίδια ταχύτητα, αφού το εμπόδιο απομακρυνθεί από το δρόμο ή βρίσκεται σε ασφαλή απόσταση. Το ACC μπορεί να επιβραδύνει το όχημα σε πλήρη στάση εάν το όχημα μπροστά του σταματήσει.

1.3.2 Προειδοποίηση πρόσκρουσης εμπροσθοπορείας (Forward Collision Warning Plus) (FCW+)

Όπως και το ACC, το FCW+ εμποδίζει το Jeep να συγκρουστεί με αντικείμενα μπροστά του. Σε αντίθεση με το ACC, το FCW+ είναι πάντα ενεργοποιημένο εκτός εάν είναι απενεργοποιημένο ρητά, προσφέροντας στην οδήγηση το πρόσθετο όφελος από το υποβοηθούμενο φρενάρισμα σε περίπτωση αναμενόμενης σύγκρουσης. Για παράδειγμα, αν ο οδηγός ελέγχει το Twitter στο τηλέφωνό του, αντί να παρακολουθεί το δρόμο, και το όχημα μπροστά του σταματήσει απότομα, το FCW+ θα στείλει μια ηχητική προειδοποίηση και θα πατήσει τα φρένα για λογαριασμό του οδηγού.

1.3.3 Προειδοποίηση Αλλαγής Λωρίδας (Lane Departure Warning) (LDW+)

Το LDW+ είναι ένα άλλο χαρακτηριστικό που χρησιμοποιείται για τη διασφάλιση της ασφάλειας του οδηγού κατά την οδήγηση στον αυτοκινητόδρομο. Το LDW+, όταν είναι ενεργοποιημένο, εξετάζει τις διαγραμμίσεις του δρόμου προσπαθώντας να διαγνώσει εάν το Jeep εκτελεί μετακινήσεις σε άλλες λωρίδες, με την προοπτική να αποτρέψει τυχόν σύγκρουση. Εάν δε, εντοπίσει ότι το Jeep φεύγει από την τρέχουσα λωρίδα κίνησής του, θα ρυθμίσει το τιμόνι για να κρατήσει το όχημα μέσα την τρέχουσα λωρίδα.

1.3.4 Σύστημα υποβοήθησης στάθμευσης (Park Assist System) (PAM)

Ένα από τα χαρακτηριστικά λειτουργίας που εισήλθαν τα τελευταία χρόνια στα περισσότερα αυτοκίνητα, είναι το σύστημα υποβοήθησης στάθμευσης. Το PAM του Jeep επιτρέπει στον οδηγό να παρκάρει σχεδόν αβίαστα το αυτοκίνητο υπό διάφορα σενάρια παρκαρίσματος, όπως π.χ. η παράλληλη στάθμευση, η επιστροφή σε έναν χώρο, κλπ. Οι ερευνητές θεώρησαν ότι αυτό ήταν το ευκολότερο σημείο εισόδου για τον έλεγχο του τιμονιού στα σύγχρονα οχήματα, με κατάλληλα πρωτόκολλα CAN (http://illmatics.com/content.zip).

1.4 ΠΙΘΑΝΑ ΣΥΣΤΗΜΑΤΑ ΤΟΥ JEEP CHEROKEE 2014 ΕΥΑΛΩΤΑ ΕΠΙΘΕΣΕΩΝ

Επιφάνεια απομακρυσμένης επίθεσης

Ο παρακάτω πίνακας δείχνει τα πιθανά σημεία εισόδου για έναν εισβολέα. Ενώ πολλοί άνθρωποι σκέφτονται μόνο αυτά τα στοιχεία όσον αφορά την τρέχουσα τεχνολογία, κάποιος με τη νοοτροπία ενός επιτιθέμενου θεωρεί κάθε κομμάτι τεχνολογίας που αλληλοεπιδρά με τον έξω κόσμο ένα πιθανό σημείο εισόδου επίθεσης (Πίνακας 2).

Entry Point	ECU	Bus
RKE	RFHM	CAN C
TPMS	RFHM	CAN C
Bluetooth	Radio	CAN C, CAN IHS
FM/AM/XM	Radio	CAN C, CAN IHS
Cellular	Radio	CAN C, CAN IHS
Internet / Apps	Radio	CAN C, CAN IHS

Πίνακας 2: Σημεία εισόδου επίθεσης (Miller C. and Valasek C., 2015)

1.4.1 Παθητικό αντικλεπτικό σύστημα (Passive Anti-Theft System) (PATS)

Για πολλά σύγχρονα αυτοκίνητα, υπάρχει ένα μικρό τσιπ στο κλειδί ανάφλεξης που επικοινωνεί με αισθητήρες στο όχημα. Για το Jeep, αυτός ο αισθητήρας συνδέεται απευθείας στη μονάδα διανομέα ραδιοσυχνοτήτων (RFHM). Όταν πατηθεί το κουμπί ανάφλεξης, ο ενσωματωμένος υπολογιστής στέλνει ένα σήμα RF που λαμβάνεται από το αναμεταδότη στο κλειδί. Στη συνέχεια, ο αναμεταδότης επιστρέφει ένα μοναδικό σήμα RF στον υπολογιστή του οχήματος, δίνοντάς του επιβεβαίωση για να ξεκινήσει και να συνεχίσει. Όλα αυτά συμβαίνουν σε λιγότερο από ένα δευτερόλεπτο. Εάν ο

ενσωματωμένος υπολογιστής δεν λάβει τον σωστό κωδικό αναγνώρισης, ορισμένα εξαρτήματα, όπως η αντλία καυσίμου και υπό συνθήκες η μίζα, θα παραμείνουν απενεργοποιημένα.

Όσον αφορά τις απομακρυσμένες επιθέσεις, αυτή η επιφάνεια επίθεσης είναι πολύ μικρή.

1.4.2 Σύστημα παρακολούθησης πίεσης ελαστικών (Tire Pressure Monitoring System) (TPMS)

Κάθε ελαστικό διαθέτει αισθητήρα πίεσης που μετρά συνεχώς την πίεση του ελαστικού και μεταδίδει σε πραγματικό χρόνο δεδομένα στην ECU. Στο Jeep, ο αισθητήρας λήψης είναι συνδεδεμένος στο RFHM.

Είναι δυνατό να εκτελεστούν κάποιες ενέργειες έναντι του TPMS, όπως για παράδειγμα το αυτοκίνητο να «σκεφτεί» αν αντιμετωπίζει πρόβλημα ελαστικών ή προβλήματα με το σύστημα TPMS εν γένει. Επιπλέον, οι ερευνητές έχουν δείξει (http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf) ότι είναι πιθανό να καταστραφεί από απόσταση η ECU, σε ορισμένες περιπτώσεις. Σχετικά με τις πιθανότητες εκτέλεσης του κώδικα του TPMS, φαίνεται ότι η επιφάνεια επίθεσης είναι μάλλον μικρή, αλλά το απομακρυσμένο περιβάλλον ελέγχου δείχνει ότι τα δεδομένα επεξεργάζονται με μη ασφαλή τρόπο.

1.4.3 Απομακρυσμένη είσοδος/εκκίνηση χωρίς κλειδί (Remote Keyless Entry/Start) (RKE)

Τα πλήκτρα, ή η απομακρυσμένη είσοδος χωρίς κλειδί (RKE), περιέχουν ραδιοφωνικό πομπό μικρής εμβέλειας που επικοινωνεί με την ECU στο όχημα. Ο ραδιοφωνικός πομπός στέλνει δεδομένα που περιέχουν πληροφορίες ταυτοποίησης από τα οποία η ECU μπορεί να καθορίσει εάν το κλειδί είναι έγκυρο και στη συνέχεια να κλειδώσει, να ξεκλειδώσει και να θέσει σε λειτουργία το όχημα. Στο Jeep, πάλι η RFHM λαμβάνει αυτές τις πληροφορίες.

Όσον αφορά την απομακρυσμένη εκτέλεση κώδικα, η επιφάνεια επίθεσης είναι αρκετά μικρή. Το RFHM πρέπει να έχει υλικολογισμικό κατάλληλο για τον χειρισμό σήματος RF, κρυπτογράφηση/αποκρυπτογράφηση κώδικα, λογική για τον προσδιορισμό δεδομένων από το πλήκτρο, και να προγραμματιστεί για επιπλέον/αντικατάσταση πλήκτρων. Η απομακρυσμένη εκτέλεση κώδικα μπορεί να είναι μια πιθανή είσοδος επίθεσης ωστόσο η εύρεση και η εκμετάλλευση μιας ευπάθειας για απομακρυσμένη εκτέλεση κώδικα στο RKE φαίνεται να είναι απίθανη ή πολύ περιορισμένη.

1.4.4 Bluetooth

Τα περισσότερα οχήματα έχουν τη δυνατότητα συγχρονισμού μιας συσκευής μέσω Bluetooth. Αυτή η δυνατότητα αντιπροσωπεύει ένα απομακρυσμένο σήμα ορισμένης πολυπλοκότητας που επεξεργάζεται μια ECU. Στο Τζιπ, το Bluetooth αναγνωρίζεται και επεξεργάζεται από το Ραδιόφωνο (γνωστό και ως κεντρική μονάδα). Αυτό επιτρέπει στο αυτοκίνητο να έχει πρόσβαση στο βιβλίο διευθύνσεων του τηλεφώνου, να πραγματοποιεί τηλεφωνικές κλήσεις, να αναπαράγει μουσική, να στέλνει μηνύματα SMS από το τηλέφωνο και άλλες λειτουργίες.

Σε αντίθεση με τα άλλα σήματα μέχρι τώρα, το σύνολο σημάτων του Bluetooth είναι αρκετά μεγάλο και αντιπροσωπεύει μια σημαντική επιφάνεια επίθεσης που είχε τρωτά σημεία στο παρελθόν (http://www.f-secure.com/vulnerabilities/SA201106648). Υπάρχουν γενικά δύο σενάρια επίθεσης που περιλαμβάνουν σήματα από Bluetooth. Η πρώτη επίθεση περιλαμβάνει μια μη συζευγμένη συσκευή. Αυτή η επίθεση είναι η πιο επικίνδυνη από οποιαδήποτε άλλη καθώς ο εισβολέας μπορεί να αποκτήσει πρόσβαση στον κώδικα ελέγχου. Η δεύτερη επίθεση μπορεί να λάβει χώρα μετά τη σύζευξη του Bluetooth με άλλες συσκευές, η οποία όμως αποτελεί μικρότερη απειλή, καθώς μπορεί να υπάρχει και κάποια αλληλεπίδραση των χρηστών, π.χ. ενός επιβάτη του οχήματος. Προηγουμένως, οι ερευνητές είχαν δείξει απομακρυσμένο έλεγχο ενός οχήματος μέσω της διεπαφής του Bluetooth (http://www.autosec.org/pubs/cars-usenixsec2011.pdf). Ερευνητές από το Codenomicon έχουν εντοπίσει πολλά ατυχήματα σε κοινούς δέκτες Bluetooth σε αυτοκίνητα (http://www.ars2000.com/Codenomicon_wp_Fuzzing.pdf).

1.4.5 Σύστημα ραδιοφωνικών δεδομένων (Radio Data System)

Το ραδιόφωνο δεν λαμβάνει μόνο ηχητικά σήματα, αλλά και άλλου είδους δεδομένα. Στο Τζιπ, το Ραδιόφωνο έχει πολλές τέτοιες απομακρυσμένες εισόδους, όπως GPS, ραδιόφωνο AM/FM και δορυφορικό ραδιόφωνο. Ως επί το πλείστων, αυτά τα σήματα απλώς μετατρέπονται σε έξοδο ήχου και δεν αντιπροσωπεύουν σημαντική ανάλυση δεδομένων, πράγμα που σημαίνει ότι είναι πιθανόν να μην περιέχουν εκμεταλλεύσιμα τρωτά σημεία. Μια πιθανή εξαίρεση είναι πιθανό να είναι τα δεδομένα του ραδιοφώνου, δεδομένα του συστήματος τα οποία χρησιμοποιούνται για την αποστολή δεδομένων μαζί με αναλογικά σήματα FM ή το αντίστοιχο δορυφορικό ραδιόφωνο. Αυτό συνήθως το αντιλαμβάνονται οι χρήστες όταν τα ραδιόφωνα δείχνουν τα ονόματα των σταθμών, τον τίτλο του τραγουδιού κλπ. Σε αυτήν την περίπτωση, τα δεδομένα πρέπει να επεξεργαστούν, δημιουργώντας κατάλληλο χώρο για μια πιθανή ευπάθεια ασφαλείας.

1.4.6 Wi-Fi

Ορισμένα αυτοκίνητα με σύνδεση στο Διαδίκτυο μέσω κινητής τηλεφωνίας μοιράζονται στην πραγματικότητα αυτές τις συνδέσεις με τους επιβάτες ενεργώντας σαν Wi-Fi hotspot. Στο Jeep, αυτό είναι ένα χαρακτηριστικό που πρέπει να αγοράζεται ανά χρήση, για παράδειγμα για μία ημέρα ή και έως ένα μήνα. Μια παρατήρηση που έγινε ήταν ότι το σύστημα Wi-Fi θα μπορούσε να αξιολογηθεί από άτομα χωρίς προηγμένη γνώση συστημάτων αυτοκινήτων. Οι μεθοδολογίες αξιολόγησης της ασφάλειας των Wi-Fi's υπάρχουν εδώ και χρόνια και η παραβίαση σημείων πρόσβασης έχουν συχνά τεκμηριωθεί πρόσφατα (https://labs.integrity.pt/articles/from-0-day-to-exploit-buffer-overflow-in-belkin-n750-cve-2014- 1635/).

1.4.7 Τηλεματική / εφαρμογές διαδικτύου (Telematics/Internet/Apps)

Πολλά σύγχρονα αυτοκίνητα περιέχουν ένα κυψελοειδές ραδιόφωνο, το οποίο γενικά αναφέρεται ως τηλεματικό σύστημα, το οποίο χρησιμοποιείται για σύνδεση στο όχημα σε δίκτυο κινητής τηλεφωνίας, για παράδειγμα OnStar της General Motors(GM). Η τηλεματική μπορεί επίσης να χρησιμοποιηθεί για την ανάκτηση δεδομένων, όπως πληροφορίες για την κυκλοφορία ή τις καιρικές συνθήκες.

Αυτό αποτελεί αιχμή των επιθέσεων σε αυτοκίνητα αφού το εύρος είναι αρκετά ευρύ. Ακόμα κι αν μια μονάδα τηλεματικής δεν βρίσκεται απευθείας στο πρωτόκολλο CAN, έχει τη δυνατότητα απομακρυσμένης μεταφοράς δεδομένων/φωνής, μέσω του μικροφώνου, σε άλλη τοποθεσία. Ερευνητές εκμεταλλεύονταν εξ αποστάσεως μια τηλεματική μονάδα αυτοκινήτου χωρίς αλληλεπίδραση χρήστη (http://www.autosec.org/pubs/cars-usenixsec2011.pdf). Στο Jeep, όλα αυτά τα χαρακτηριστικά ελέγχονται από το Ραδιόφωνο, το οποίο βρίσκεται τόσο στο πρωτοκόλλο τύπου λεωφορείο (CAN - Interior High Speed - CAN-IHS) όσο και στο αντίστοιχο CAN-C.

Τα τηλεματικά, το Διαδίκτυο, το ραδιόφωνο και οι εφαρμογές ανήκουν όλα στο σύστημα Harman Uconnect που υπάρχει στο Jeep Cherokee του 2014. Το σύστημα Uconnect περιγράφεται λεπτομερέστερα παρακάτω. Η λειτουργικότητα που σχετίζεται με το «infotainment» βρίσκεται σε μία μονάδα, το Uconnect system.

1.5 ΜΗ ΔΙΑΣΥΝΔΕΔΕΜΕΝΟ ΣΥΣΤΗΜΑ (UCONNECT SYSTEM)

Το Uconnect ομαδοποιεί λειτουργίες συνδεσιμότητας, ψυχαγωγίας και πλοήγησης. Βασίζεται στην οθόνη αφής, και είναι σχετικά εύκολο στη χρήση.

Το Jeep Cherokee του 2014 χρησιμοποιεί το ραδιόφωνο Uconnect 8.4AN/RA4 που κατασκευάζεται από την εταιρεία Harman Kardon ως μοναδική πηγή για ψυχαγωγία,

σύνδεση Wi-Fi, πλοήγηση, εφαρμογές και κυψελοειδείς επικοινωνίες (http://www.driveuconnect.com/system/2014/ramtrucks/ram_1500/8-4an-ra4/). Η κύρια λειτουργικότητα σχεδιάστηκε από την Texas Instruments OMAP-DM3730, σε ένα τσιπ (http://www.allpar.com/corporate/tech/uconnect.html), το οποίο είναι κοινό σε αρκετά αυτοκίνητα. Αυτά τα συστήματα Harman Uconnect διατίθενται σε διάφορα οχήματα της Fiat Chrysler Automotive, συμπεριλαμβανομένων των οχημάτων από την Chrysler, Dodge, Jeep και Ram. Όπως αναφέρεται στη βιβλιογραφία τα συστήματα Harman Uconnect είναι πιθανό, να διατίθενται και σε άλλους τύπους αυτοκινήτων.

Η μονάδα κεφαλής Uconnect περιέχει επίσης έναν μικροελεγκτή και λογισμικό που του επιτρέπει να επικοινωνεί με άλλες ηλεκτρονικές μονάδες στο όχημα μέσω του διαύλου δεδομένων CAN-IHS. Σε οχήματα εξοπλισμένα με πρόσβαση Uconnect, το σύστημα χρησιμοποιεί επίσης και ηλεκτρονικό μήνυμα επικοινωνίας με άλλες ηλεκτρονικές μονάδες του οχήματος μέσω του διαύλου δεδομένων CAN-C.

Το σύστημα Harman Uconnect δεν περιορίζεται στο Jeep Cherokee και είναι αρκετά συνηθισμένο στη σειρά αυτοκινήτων Chrysler Fiat όπως προαναφέρθηκε, και μάλιστα φαίνεται να κάνει την εμφάνισή του και στη Ferrari όπου παράγεται στην Καλιφόρνια των ΗΠΑ (http://forums.motortrend.com/70/8102478/the-general-forum/ferrari-california-navigation-chrysler-uconnect/index.html). Αυτό σημαίνει ότι ενώ οι κυβερνοφυσικές αναφορές αυτού του εγγράφου περιορίζονται σε ένα Jeep Cherokee του 2014, οι ευπάθειες στο σύστημα Uconnect και οι πληροφορίες είναι σχετικές με κάθε όχημα που περιλαμβάνει το εν λόγω σύστημα. Επομένως ο αριθμός των ευάλωτων οχημάτων στο δρόμο μπορούμε να πούμε ότι αυξάνεται δραματικά.

1.5.1 Περιβάλλον πλατφόρμας QNX και αξιοπιστία αυτοκινήτου

Η πλατφόρμα QNX για infotainment είναι ένα αποδεδειγμένα, πλήρως εξοπλισμένο πακέτο λογισμικού που έχει σχεδιαστεί για να βοηθήσει τους κατασκευαστές αυτοκινήτων να δημιουργήσουν γραφικά πλούσια, συνδεδεμένα συστήματα infotainment που ενσωματώνουν κορυφαίες τεχνολογίες αυτοκινήτων.

Το QNX παρέχει μια ασφαλή και αξιόπιστη βάση. Η πλατφόρμα ενσωματώνει μια συλλογή τεχνολογίας μέσω λογισμικού QNX για τη διαχείριση πολυμέσων, εφαρμογών ιστού, ενσωμάτωσης ομιλίας, συνδεσιμότητας smartphone, Bluetooth και ακουστικής επεξεργασίας για κλήσεις hands-free. Η πλατφόρμα υποστηρίζεται από την αυτοκινητοβιομηχανία και είναι κατασκευασμένη με αρθρωτή και επεκτάσιμη αρχιτεκτονική. Αυτή η αρθρωτότητα διευκολύνει τυχόν προσαρμογές που απαιτούνται στο λογισμικό για την προσθήκη νέων δυνατοτήτων και την αντικατάσταση υπαρχουσών τεχνολογιών.

Το σύστημα Uconnect στο Jeep Cherokee του 2014 τρέχει το λειτουργικό σύστημα QNX σε έναν ARM 32-bit επεξεργαστή, ο οποίος φαίνεται να είναι μια κοινή εγκατάσταση για συστήματα ψυχαγωγίας αυτοκινήτων. Το εργαλείο ISO που χρησιμοποιείται για ενημερώσεις και η επανεγκατάσταση του λειτουργικού συστήματος μπορεί να μεταφορτωθεί πολύ εύκολα από το Διαδίκτυο (http://www.driveuconnect.com/software-update/). Επίσης, μέσω εξωτερικής μνήμης (NAND) που χρησιμοποιείται στη μονάδα Uconnect, περιέχονται πολλά διαφορετικά συστήματα και τύποι αρχείων που εξυπηρετούν διάφορους σκοπούς (http://www.qnx.com/developers/docs/6.3.0SP3/ide_en/user_guide/builder.html), όπως π.χ. η αναβάθμιση του λογισμικού QNX, η βελτίωση χωρητικότητας μνήμης, κτλ.

1.5.2 Κρυπτογράφηση

Η προεπιλεγμένη μέθοδος κρυπτογράφησης Wi-Fi είναι μέσω του πρωτοκόλλου WPA2 με έναν τυχαίο κωδικό πρόσβασης που περιέχει τουλάχιστον 8 αλφαριθμητικούς χαρακτήρες. Λόγω της τρέχουσας ισχύος του WPA2 και του αριθμού των πιθανών κωδικών πρόσβασης, αυτή θεωρείται μια αρκετά ασφαλής ρύθμιση, η οποία θέτει το ερώτημα, πώς αποκτά πρόσβαση ένας εισβολέας σε αυτό το δίκτυο;

Μια από τις ευκολότερες, αλλά λιγότερο πιθανές δυνατότητες, είναι ότι ο χρήστης έχει επιλέξει ενσύρματο ισοδύναμο απόρρητο-Wired Equivalent Privacy(WEP) ή καθόλου κρυπτογράφηση καθώς και οι δύο είναι διαθέσιμες επιλογές. Σε κάθε περίπτωση, ο επιτιθέμενος θα είχε σχετικά μικρό πρόβλημα να κερδίσει πρόσβαση στο σημείο ασύρματης πρόσβασης είτε σπάζοντας τον κωδικό πρόσβασης του WEP (http://www.qnx.com/developers/docs/660/index.jsp?topic=%2Fcom.qnx.doc.neutrino.sys_arch%2Ftopic%2Ffsys_ETFS.html), είτε απλώς συνδεόμενος στο σημείο πρόσβασης.

Ένα άλλο σενάριο επίθεσης υπάρχει εάν ο εισβολέας έχει ήδη παραβιάσει μια συσκευή που συνδέεται στο Wi-Fi hotspot στο αυτοκίνητο, όπως φορητό υπολογιστή ή κινητό τηλέφωνο. Το γεγονός ότι ο ιδιοκτήτης πληρώνει για αυτή την υπηρεσία σημαίνει ότι πιθανότατα έχει τηλέφωνο ή άλλη συσκευή που συνδέονται τακτικά με το ασύρματο δίκτυο. Σε αυτήν την περίπτωση, εάν ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε μία από αυτές τις συσκευές, θα έχει ήδη συνδεθεί στο ασύρματο δίκτυο του αυτοκινήτου.

Ωστόσο, ακόμη και στην περίπτωση που ο χρήστης έχει την προεπιλεγμένη ρύθμιση Προστατευμένη Πρόσβαση Wi-Fi II (WPA2), παραμένει ακόμα δυνατή για τον εισβολέα να έχει πρόσβαση στο δίκτυο σχετικά εύκολα.

1.5.3 Ανοιχτή θύρα (Open port)

Μία από τις πιο προφανείς μεθόδους εκτίμησης του σημείου πρόσβασης Wi-Fi ήταν η σάρωση θύρας της προεπιλεγμένης πύλης και ο έλεγχος αν υπάρχουν ανοιχτές θύρες. Από την εξέταση του Jeep , αποδείχθηκε ότι ήταν αρκετές θύρες ανοιχτές. Μετά από τον έλεγχο αρκετών θυρών αποδείχθηκε ότι η θύρα 6667 που σχετίζεται με το πρωτόκολλό D-BUS ήταν η πιο ευάλωτη σε επίθεση (Miller C. , Valasek C. 2015)

1.6 ΜΗ ΔΙΑΣΥΝΔΕΔΕΜΕΝΑ ΣΥΣΤΗΜΑ ΕΥΑΛΩΤΑ ΕΠΙΘΕΣΕΩΝ (UCONNECT ATTACK PAYLOADS)

Αυτή η ενότητα καλύπτει διάφορα σενάρια προγραμματισμού με γλώσσα ανοιχτού κώδικα (LUA) που μπορούν να χρησιμοποιηθούν για να επηρεάσουν τα εσωτερικά χαρακτηριστικά λειτουργίας του οχήματος και τη λειτουργία του ραδιοφώνου και προγραμματίζονται στο τσιπ OMAP. Για παράδειγμα αναφέρουμε την αύξηση της έντασης ή την αποτροπή ανταπόκρισης ορισμένων κομβίων ελέγχου (π.χ. την ρύθμιση της έντασης του ήχου).

Οι δέσμες ενεργειών μπορούν να δώσουν μια ιδέα για το τι μπορεί να συμβεί στο όχημα από ένα απομακρυσμένο κέλυφος ελέγχου και πρόσβαση στο λειτουργικό σύστημα Uconnect. Παρακάτω θα περιγράψουμε τα υποσυστήματα του Uconnect.

1.6.1 Το παγκόσμιο σύστημα εντοπισμού θέσης (Global Positioning System(GPS))

Η κεντρική μονάδα ελέγχου έχει τη δυνατότητα να αναζητήσει και να ανακτήσει τις συντεταγμένες GPS του Jeep, είτε μέσω του ασύρματου μόντεμ της Sierra ή του Wi-Fi. Αυτές οι τιμές μπορούν επίσης να ανακτηθούν χρησιμοποιώντας μη πιστοποιημένο δίαυλο επικοινωνίας D-bus μέσω της θύρας 6667, με αποτέλεσμα τη δυνατότητα παρακολούθησης αυθαίρετων οχημάτων.

1.6.2 HVAC

Η κεντρική μονάδα μπορεί να ελέγξει τη θέρμανση και τον κλιματισμό του οχήματος. Ένας κώδικας θα ρυθμίσει το ανεμιστήρα σε αυθαίρετη ταχύτητα.

1.6.3 Ένταση ραδιοφώνου (Radio Volume)

Μία από τις κύριες λειτουργίες του συστήματος Uconnect είναι ο έλεγχος του ραδιοφώνου. Ένας εισβολέας που θέλει να ρυθμίσει π.χ. την ένταση σε μια αυθαίρετη τιμή μπορεί εύκολα να το πράξει.

1.6.4 Μπάσα (Bass)

Μερικές φορές όταν τον ανέβασμα του μπάσου είναι η μόνη επιλογή, οι επιτιθέμενοι μπορούν να εκτελέσουν ενέργειες για να προσαρμόσουν ανάλογα τα επίπεδα μέσω κατάλληλων κωδίκων.

1.6.5 Ραδιοφωνικός Σταθμός (FM)

Η επιλογή ενός κατάλληλου ραδιοφωνικού σταθμού στα FM μπορεί να είναι ένα από τα πιο σημαντικά χαρακτηριστικά απόλαυσης κάθε ταξιδιού. Η αλλαγή του σταθμού είναι επίσης διαθέσιμη μέσω προγραμματισμού ενεργειών από ανοιχτούς κώδικες(LUA).

1.6.6 Απεικόνιση (Display)

Υπάρχουν διάφοροι τρόποι για να αλλάξει η κατάσταση της οθόνης Uconnect, όπως να την απενεργοποιηθεί εντελώς ή να δείχνει την εφεδρική κάμερα.

Μπορεί επίσης να αλλάξει η οθόνη αυτής της μονάδας για να εμφανιστεί μια εικόνα. Η εικόνα πρέπει να είναι μέσα τις σωστές διαστάσεις και μορφή (png). Στη συνέχεια, η εικόνα πρέπει να τοποθετηθεί κάπου στο φάκελο των αρχείων. Μόνο τότε μπορείτε να πείτε στην κεφαλή να εμφανίσει την εικόνα.

1.6.7 Κομβία (Knobs)

Μια από τις πιο ενδιαφέρουσες επίσης ανακαλύψεις ήταν η ικανότητα να καταστρέψεις μια υπηρεσία που θα αναιρούσε το φυσικό έλεγχο των κομβίων που χρησιμοποιούνται για το ραδιόφωνο, όπως η ένταση ή το ψάξιμο των σταθμών. Καταστρέφοντας την κύρια υπηρεσία D-Bus, μπορεί να σταματήσουν να αποκρίνονται όλα τα χειριστήρια που χρησιμοποιούνται για το ραδιόφωνο. Αυτή η επίθεση μπορεί να είναι ιδιαίτερα ενοχλητική ειδικά μετά την εκτέλεση αρκετών και άλλων λειτουργιών, όπως μετατροπή του μπάσου και της έντασης στα μέγιστα επίπεδα.

1.7 ΟΛΟΚΛΗΡΗ Η ΑΛΥΣΙΔΑ ΕΝΕΡΓΕΙΩΝ ΤΗΣ ΕΠΙΘΕΣΗΣ

Μέχρι αυτό το σημείο, έχουμε συζητήσει πολλές πτυχές για τον τρόπο επίθεσης από απόσταση του Jeep και παρόμοιων οχημάτων. Υπάρχουν αρκετές πληροφορίες μέχρι στιγμής για να πραγματοποιηθεί μια πλήρης επίθεση. Παρακάτω συνοψίζουμε πώς θα λειτουργούσε η αλυσίδα επιθέσεων από την αρχή μέχρι το τέλος.

1. **Προσδιορισμός στόχου**

Απαιτείται η διεύθυνση διαδικτυακού πρωτοκόλλου (IP) του οχήματος.

2. **Εκμετάλλευση του τσιπ *OMAP* της κεντρικής μονάδας**

Όταν γνωστοποιηθεί η διεύθυνση IP ενός ευάλωτου οχήματος, είναι δυνατό να εκτελεστεί κώδικας χρησιμοποιώντας τη μέθοδο εκτέλεσης της υπηρεσία D-Bus. Το πιο εύκολο

πράγμα που μπορεί να γίνει είναι να μεταφορτωθεί ένα δημόσιο κλειδί SSH[1], σαν αρχείο διαμόρφωσης και, στη συνέχεια, να εκκινήσει η υπηρεσία SSH.

3. Έλεγχος συστήματος αποσύνδεσης

Εάν το μόνο που απαιτείται είναι να ελέγχει το ραδιόφωνο, το HVAC, να λαμβάνετε το GPS ή άλλες επιθέσεις που δεν σχετίζονται με CAN, τότε χρειάζονται μόνο οι ενέργειες μέσω LUA. Στην πραγματικότητα, το μεγαλύτερο μέρος της λειτουργικότητας μπορεί να γίνει χρησιμοποιώντας το D-Bus χωρίς να εκτελείτε πραγματικός κώδικας, απλά χρησιμοποιώντας τις παρεχόμενες υπηρεσίες D-Bus.

4. Εξωτερικός προγραμματισμός του v850[2] με τροποποιημένο υλικολογισμικό

Υπάρχει ένα τροποποιημένο υλικολογισμικό v850 και είναι δυνατόν να ακολουθηθούν οδηγίες για να λειτουργήσει το v850 με το τροποποιημένο υλικολογισμικό. Αυτό απαιτεί αυτόματη επανεκκίνηση του συστήματος, η οποία ενδέχεται να ειδοποιήσει τον οδηγό ότι κάτι συμβαίνει. Αν δεν υλοποιηθεί αυτό το βήμα υπάρχει περίπτωση να αστοχήσει η κεφαλή και θα πρέπει να αντικατασταθεί.

5. Εκτέλεση κυβερνοφυσικών ενεργειών

Χρησιμοποιώντας το τροποποιημένο υλικολογισμικό, στέλνονται τα κατάλληλα μηνύματα CAN για να συμβούν φυσικά γεγονότα στο όχημα στέλνοντας μηνύματα από το τσιπ OMAP στο τροποποιημένο υλικολογισμικό του μικροεπεξεργαστή V850 χρησιμοποιώντας το πρωτόκολλο SPI (http://illmatics.com/content.zip).

---

[1] Το SSH, επίσης γνωστό ως Secure Shell ή Secure Socket Shell, είναι ένα πρωτόκολλο δικτύου που δίνει στους χρήστες, ιδιαίτερα στους διαχειριστές συστήματος, έναν ασφαλή τρόπο πρόσβασης σε έναν υπολογιστή μέσω ενός μη ασφαλούς δικτύου. Εκτός από την παροχή ασφαλών υπηρεσιών δικτύου, η SSH αναφέρεται στη σουίτα των υπηρεσιών κοινής ωφέλειας που εφαρμόζουν το πρωτόκολλο SSH. Η Secure Shell παρέχει ισχυρό έλεγχο ταυτότητας κωδικού πρόσβασης και έλεγχο ταυτότητας δημόσιου κλειδιού, καθώς και κρυπτογραφημένες επικοινωνίες δεδομένων μεταξύ δύο υπολογιστών που συνδέονται μέσω ανοιχτού δικτύου, όπως το Διαδίκτυο. Εκτός από την παροχή ισχυρής κρυπτογράφησης, το SSH χρησιμοποιείται ευρέως από τους διαχειριστές δικτύου για τη διαχείριση συστημάτων και εφαρμογών εξ αποστάσεως, επιτρέποντάς τους να συνδεθούν σε έναν άλλο υπολογιστή μέσω δικτύου, να εκτελέσουν εντολές και να μετακινήσουν αρχεία από τον έναν υπολογιστή στον άλλο.

[2] Το V850 είναι μια αρχιτεκτονική CPU RISC 32-bit που παράγεται από την Renesas Electronics για ενσωματωμένους μικροελεγκτές. Σχεδιάστηκε από την NEC ως αντικατάσταση της προηγούμενης οικογένειας NEC V60 και παρουσιάστηκε λίγο πριν η NEC πουλήσει τα σχέδιά της στη Renesas στις αρχές της δεκαετίας του 1990.

1.8 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ – ΠΡΟΛΗΨΗΣ ΕΠΙΘΕΣΕΩΝ

Τα συστήματα ελέγχου των αυτοκινήτων εγκαθίστανται σήμερα ως δίκτυα ενσωματωμένων υπολογιστών, μερικοί από τους οποίους έχουν συνδεσιμότητα με τον παγκόσμιο ιστό. Οι παραδοσιακές λύσεις ασφάλειας αυτοκινήτων, όπως ο συναγερμός, η είσοδος χωρίς κλειδί κ.λπ., αποτυγχάνουν να προστατεύσουν το αυτοκίνητο ως κυβερνοφυσικό σύστημα.

Οι αυτοκινητοβιομηχανίες και οι προμηθευτές τους πρέπει επίσης να εξετάσουν τι σημαίνει το συνδεδεμένο όχημα για την προστασία της ιδιωτικής ζωής και της ασφάλειας των καταναλωτών. Καθώς περισσότερα συνδεδεμένα οχήματα κυκλοφορούν στους δρόμους, τα τρωτά σημεία του λογισμικού γίνονται προσβάσιμα σε κακόβουλους χάκερ που χρησιμοποιούν δίκτυα κινητής τηλεφωνίας, Wi-Fi και φυσικές συνδέσεις για την εκμετάλλευσή τους. Η μη αντιμετώπιση αυτών των κινδύνων μπορεί να είναι ένα δαπανηρό λάθος, συμπεριλαμβανομένου του αντίκτυπου που μπορεί να έχουν στην εμπιστοσύνη των καταναλωτών, την προσωπική ιδιωτικότητα και τη φήμη της επωνυμίας της κατασκευάστριας εταιρείας. Ερευνητές διαπίστωσαν ότι οι τεχνολογίες με τον μεγαλύτερο κίνδυνο είναι οι τεχνολογίες ραδιοσυχνοτήτων(RF) (όπως Wi-Fi και Bluetooth), η τηλεματική και τα αυτόνομα οχήματα. Αυτό υποδηλώνει ότι τα μη κρίσιμα συστήματα και η συνδεσιμότητα είναι τα πιο ευάλωτα για επιθέσεις και θα πρέπει να είναι το κύριο επίκεντρο των προσπαθειών κυβερνοασφάλειας (https://www.synopsys.com/glossary/what-is-connected-car-cyber-security.html#2).

Όπως αναφέρετε στη βιβλιογραφία σημειώνεται στο TechSpective (https://techspective.net/2017/08/16/safety-security-open-source-automotive-industry/), "Οι κατασκευαστές οχημάτων πρέπει να υιοθετήσουν μια προσέγγιση στην κυβερνοασφάλεια που να αντιμετωπίζει όχι μόνο προφανείς επιθέσεις στο λογισμικό του αυτοκινήτου τους, αλλά και τις κρυφές ευπάθειες που θα μπορούσαν να εισαχθούν από εξαρτήματα ανοιχτού κώδικα [ή τρίτων] σε αυτό το λογισμικό.

1.8.1 Στατική ανάλυση (SAST) για κυβερνοασφάλεια αυτοκινήτου

Η στατική ανάλυση (SAST) είναι ένα βασικό εργαλείο για τους προγραμματιστές λογισμικού στην αυτοκινητοβιομηχανία για τον εντοπισμό σφαλμάτων ασφαλείας-όπως η λογική SQL, η δέσμη ενεργειών μεταξύ ιστοτόπων και οι υπερχειλίσεις χώρων δεδομένων (buffer)-στον κώδικα τους.

Το SAST, γνωστό και ως δοκιμή λευκού κουτιού, σαρώνει μια εφαρμογή πριν καταρτιστεί ο κώδικας.

Δεδομένου ότι δεν απαιτείται η εκτέλεση μιας εφαρμογής ή η εκτέλεση κώδικα, το SAST μπορεί να λάβει χώρα νωρίς στον κύκλο ζωής ανάπτυξης ενός λογισμικού (SDLC). Το SAST βοηθά τους προγραμματιστές να εντοπίσουν τρωτά σημεία στα αρχικά στάδια της ανάπτυξης και να επιλύσουν γρήγορα ζητήματα χωρίς να σπάσουν τις δομές του κώδικα ή να μεταβιβάσουν τα ευάλωτα σημεία στην τελική κυκλοφορία της εν λόγω εφαρμογής.

1.8.2 IAST για την ασφάλεια στον κυβερνοχώρο αυτοκινήτων

Οι διαδραστικές λύσεις δοκιμών ασφαλείας εφαρμογών (IAST) βοηθούν τους οργανισμούς αυτοκινήτων να εντοπίζουν και να διαχειρίζονται κινδύνους ασφαλείας που σχετίζονται με ευπάθειες οι οποίες ανακαλύπτονται κατά την εκτέλεση εφαρμογών, χρησιμοποιώντας τεχνικές δυναμικού ελέγχου (συχνά αναφέρονται ως δοκιμές χρόνου εκτέλεσης). Ορισμένες λύσεις IAST ενσωματώνουν εργαλεία ανάλυσης και σύνθεσης λογισμικού (SCA) για την αντιμετώπιση γνωστών τρωτών σημείων σε στοιχεία και πλαίσια ανοιχτού κώδικα.

Το IAST πραγματοποιείται γενικά κατά τη διάρκεια του σταδίου δοκιμής/QA του κύκλου ζωής ανάπτυξης του λογισμικού (SDLC). Το IAST επηρεάζει αποτελεσματικά τις δοκιμές του κώδικα, και έτσι τα προβλήματα ανιχνεύονται νωρίτερα στον κύκλο ανάπτυξης, μειώνοντας το κόστος αποκατάστασης και τις καθυστερήσεις. Πολλά εργαλεία IAST μπορούν να ενσωματωθούν σε εργαλεία συνεχούς ολοκλήρωσης (CI) και παράλληλα συνεχούς ανάπτυξης (CD). Η τελευταία γενιά εργαλείων IAST επιστρέφει αποτελέσματα μόλις επανεπεξεργαστεί ο τροποποιημένος κώδικας και επανεξεταστεί η εφαρμογή που εκτελείται, βοηθώντας έτσι τους προγραμματιστές να εντοπίσουν ευπάθειες ακόμα νωρίτερα στη διαδικασία ανάπτυξης του κώδικα.

1.8.3 SCA για ασφάλεια στον κυβερνοχώρο αυτοκινήτων

Με την αύξηση της χρήσης ανοιχτού κώδικα, ειδικά από τρίτους προμηθευτές, οι κατασκευαστές αυτοκινήτων πρέπει να διασφαλίσουν ότι η ανάλυση σύνθεσης λογισμικού (SCA) αποτελεί μέρος των εργαλείων ασφαλείας και εφαρμογών τους. Οι έλεγχοι του συνολικού κώδικα δείχνουν σταθερά στοιχεία ανοικτού κώδικα που συνθέτουν έως και το 25% οποιασδήποτε εφαρμογής αυτοκινήτου. Όπως σημείωσε η Forrester Research (https://www.synopsys.com/glossary/what-is-connected-car-cyber-security.html#2) σε μια έκθεση του 2017, "Δυστυχώς, πολλά από αυτά τα στοιχεία ανοιχτού κώδικα έχουν περιορισμούς από τις συμφωνίες άδειας χρήσης τους και μπορεί κάθε ένα από τα αιτήματα λήψης ανοιχτού κώδικα να αφορά ένα στοιχείο με γνωστή ευπάθεια."

Με την προσθήκη μιας λύσης SCA, οι αυτοκινητοβιομηχανίες μπορούν να προσαρμόσουν αποτελεσματικά τη χρήση ανοιχτού κώδικα στον συνολικό κώδικά τους, είτε προέρχεται από εσωτερικές ομάδες ανάπτυξης είτε από εξωτερικούς προμηθευτές ανίχνευσης τρωτών σημείων σε στοιχεία ανοιχτού κώδικα.

Για πιο ασφαλή οχήματα, ο Montoya (https://www.computerworld.com/article/2951489/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html) πιστεύει ότι οι κατασκευαστές πρέπει τελικά να βρουν έναν τρόπο να απομονώσουν τις λειτουργίες οδήγησης από τα συστήματα infotainment.

Ο Άλεν (https://www.computerworld.com/article/2951489/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html) συμφώνησε ότι οι εκτεταμένες επιθέσεις σε οχήματα δεν είναι πιθανό να συμβούν στο μέλλον, επειδή θα υπάρχουν ελάχιστα οικονομικά κίνητρα για αυτούς και θα απαιτούσαν πολλή δουλειά.

Η ασφάλεια των οχημάτων από ασύρματες παραβιάσεις έχει μικρότερη σχέση με ένα τείχος προστασίας και περισσότερο με την αναγνώριση μιας επίθεσης που συμβαίνει.

Ο Μίλερ (https://www.computerworld.com/article/2951489/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html) συμφώνησε και είπε: «Πρέπει να πάρετε μια πολυεπίπεδη προσέγγιση, όπως κάνετε στην ασφάλεια των επιχειρήσεων. Το πρωτόκολλο CAN bus είναι πολύ απλό. Τα μηνύματα σε αυτό είναι πολύ προβλέψιμα, αλλά όταν αρχίζω να στέλνω μηνύματα για να προκαλέσω επιθέσεις, αυτά τα μηνύματα είναι πολύ ξεκάθαρα. Οι κατασκευαστές αυτοκινήτων θα μπορούσαν να αναβαθμίσουν το λογισμικό για να εντοπίσουν κακόβουλα μηνύματα CAN, δίνοντας εντολή σε κρίσιμα συστήματα, όπως τα φρένα ή το σύστημα μετάδοσης ώστε να τα αγνοήσουν».

1.9 ΣΥΜΠΕΡΑΣΜΑ

Η Εργασία των Miller και Valasek ήταν το αποκορύφωμα τριών ετών έρευνας για την ασφάλεια των αυτοκινήτων. Αποδείχθηκε ότι μια απομακρυσμένη επίθεση μπορεί να πραγματοποιηθεί εναντίον πολλών οχημάτων όπως π.χ της Fiat-Chrysler. Ο αριθμός των ευάλωτων οχημάτων ήταν εκατοντάδες χιλιάδες και ανάγκασε 1,4 εκατομμύρια οχήματα σε ανάκληση από την FCA καθώς και αλλαγές στο δίκτυο μεταφορέων Sprint.

Αυτή η απομακρυσμένη επίθεση θα μπορούσε να πραγματοποιηθεί έναντι οχημάτων που βρίσκονται οπουδήποτε στις Ηνωμένες Πολιτείες και δεν απαιτούν τροποποιήσεις στο όχημα ή φυσική αλληλεπίδραση από τον επιτιθέμενο ή τον οδηγό.

Ως αποτέλεσμα της απομακρυσμένης επίθεσης, ορισμένα φυσικά συστήματα όπως το τιμόνι και το φρενάρισμα επηρεάζονται άμεσα. Οι Miller και Valasek παρείχαν αυτήν την

έρευνα με την ελπίδα ότι μπορούν να δημιουργηθούν πιο ασφαλή οχήματα στο μέλλον, έτσι ώστε οι οδηγοί να μπορούν να εμπιστευτούν ότι είναι ασφαλείς από κυβερνοεπίθεση κατά την οδήγηση.

Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν από τους κατασκευαστές, τους προμηθευτές και τους ερευνητές ασφάλειας για να συνεχίσουν εξετάζοντας το Jeep Cherokee και άλλα οχήματα σε μια συνολική προσπάθεια να εξασφαλίσουμε σύγχρονα ασφαλή αυτοκίνητα.

2. ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΗΣ ΡΑΔΙΟΕΠΙΚΟΙΝΩΝΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΕΛΕΓΧΟΥ ΤΗΣ ΚΥΚΛΟΦΟΡΙΑΣ ΓΙΑ ΤΟΝ ΕΛΕΓΧΟ ΤΟΥΣ

2.1 ΓΕΝΙΚΑ

Το κεφάλαιο αυτό αναφέρεται σε μια παρουσίαση που πραγματοποιήθηκε στο Defcon του Μαϊάμι των ΗΠΑ, ένα από τα πιο μεγάλα συνέδρια για χάκερς, το 2015 (https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf), (https://www.youtube.com/watch?v=_j9lELCSZQw).

Ο Cerrudo, ένας Αργεντίνος ερευνητής και Haker, παρουσίασε ένα πραγματικό γεγονός διαδικτυακής επίθεσης σε συστήματα ελέγχου κυκλοφορίας. Ο Cerrudo κατοικεί σε μια μικρή πόλη του τρίτου κόσμου, μακριά από τα προβλήματα μεγαλουπόλεων και δουλεύει το λογισμικό του σε Ms Office, Oracle, SQL Server, κτλ.

Ο Cerrudo, ξεκινώντας την ομιλία του, αναφέρθηκε στο θέμα που είναι η εκμετάλλευση των συστημάτων ελέγχου της κυκλοφορίας οχημάτων στις ΗΠΑ. Αναφέρθηκε σε καινοτόμα συστήματα που χρησιμοποίησε προκειμένου να παρουσιάσει το πρόβλημα.

Τα συστήματα ελέγχου κυκλοφορίας αποτελούνται από πολλές διαφορετικές συσκευές όπως κάμερες , συλλέκτες δεδομένων, συστήματα ανάγνωσης δεδομένων, κεραίες κτλ.

Ανέφερε πως σήματα ραδιοσυχνοτήτων και συλλέκτες δεδομένων, χρησιμοποιούνται στο Λονδίνο από του υπουργείο συγκοινωνιών του UK, για ασύρματη διαχείριση και έλεγχο της κυκλοφορίας σε διάφορους δρόμους.

Ο Cerrudo ανέφερε ότι ήταν κάτι καινούργιο αυτό και του κέντρισε το ενδιαφέρον. Έτσι ζήτησε από τους διάφορους προμηθευτές των συσκευών, πληροφορίες (από παρουσιάσεις αυτών, από διάφορα άλλα άρθρα στον τύπο κτλ) για την τεχνολογία αυτών, προκειμένου να διαπιστώσει αν η τεχνολογία αυτή είναι ευρέως γνωστή.

Διαπίστωσε ότι ήταν πάρα πολύ καλά συστήματα για ασύρματο έλεγχο της κυκλοφορίας, αλλά και για εκμετάλλευση από τη άλλη πλευρά.

Όσο αφορά τα ασύρματα συστήματα ελέγχου κυκλοφορίας, οι ΗΠΑ ήταν πρώτες σε αριθμό, μετά το Ηνωμένο Βασίλειο και Τρίτη έρχεται η Αυστραλία και ακολουθούν ο Καναδάς, η Γαλλία, η Γερμανία και η Κίνα. Περίπου 250 πελάτες σε όλο τον κόσμο χρησιμοποιούν τα συστήματα αυτά.

Έχουν τοποθετηθεί παγκοσμίως 500.000 περίπου τέτοια συστήματα ελέγχου κυκλοφορίας, τα περισσότερα από αυτά στις ΗΠΑ.

2.2 ΤΟ ΔΙΚΤΥΟ ΤΩΝ ΑΙΣΘΗΤΗΡΩΝ ΣΤΗΝ ΟΥΑΣΙΓΚΤΟΝ

Στην Ουάσιγκτον υπάρχουν πλέον των 1300 ασύρματων αισθητήρων για τον έλεγχο της κυκλοφορίας (Εικόνα 1).

Εικόνα 1: Το δίκτυο των 1300 ασύρματων αισθητήρων στην Ουάσιγκτον (https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

Ερευνώντας τις σελίδες των εγχειρίδιων των αισθητήρων ο Cerrudo βρήκε ότι μια και μόνο σελίδα αναφέρονταν σε θέματα ασφαλείας από τις 100 περίπου σελίδες εκάστου εγχειριδίου.

Στις ΗΠΑ οι αισθητήρες αγοράζονται από τις πολιτείες ή από τη κεντρική κυβέρνηση, μέσω αντιπρόσωπων των κατασκευαστών τους.

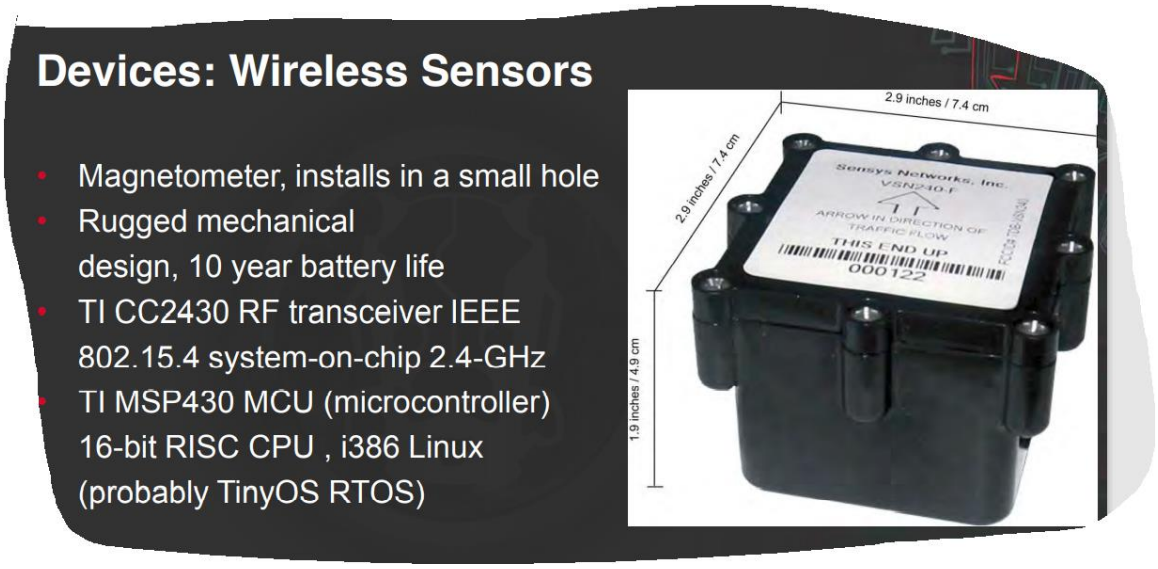
Στα παρακάτω σχήματα φαίνονται οι αισθητήρες και οι συσκευές που χρησιμοποιούνται για τον έλεγχο της κυκλοφορίας.

Ο Cerrudo πρότεινε, και ο ίδιος πιστοποίησε τους αισθητήρες με δοκιμές που πραγματοποίησε, όσο αναφορά τη ποιότητά τους και την ορθότητα της πληροφορίας που διαχειρίζονται. Συνήθως όπως ανέφερε, για κάθε αισθητήρα υπάρχει ένα σημείο πρόσβασης (ACCESS POINT). Επίσης στα διάφορα πειράματα που έκανε , οι αισθητήρες ταξίδεψαν από την Αργεντινή στο Πουέρτο Ρίκο, στις ΗΠΑ και πάλι στη Αργεντινή χωρίς τεχνικά πρόβλημα λόγω μεταφοράς.

2.3 ΟΙ ΑΙΣΘΗΤΗΡΕΣ ΚΑΙ Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥΣ

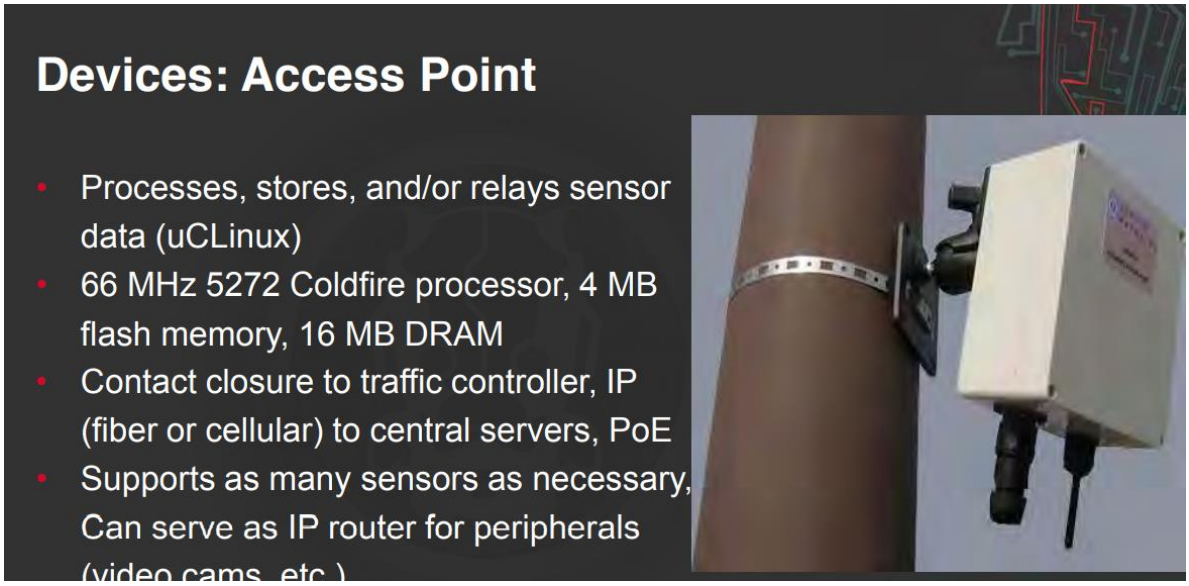
Ο Cerrudo χρησιμοποίησε ασύρματους αισθητήρες όπως φαίνεται στη παρακάτω εικόνα 2.

Τα μαγνητόμετρα όπως χαρακτηριστικά ανέφερε, μετρούν τις αλλαγές του μαγνητικού πεδίου στην ατμόσφαιρα. Έτσι, όποιο αυτοκίνητο διέρχεται κοντά από τον αισθητήρα, αλλάζει το μαγνητικό πεδίο στην ατμόσφαιρα και ανιχνεύεται.



Εικόνα 2: Ασύρματος αισθητήρας
(https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

Επίσης υπάρχουν και σημεία πρόσβασης με τα τεχνικά χαρακτηριστικά που φαίνονται στην Εικόνα 3.

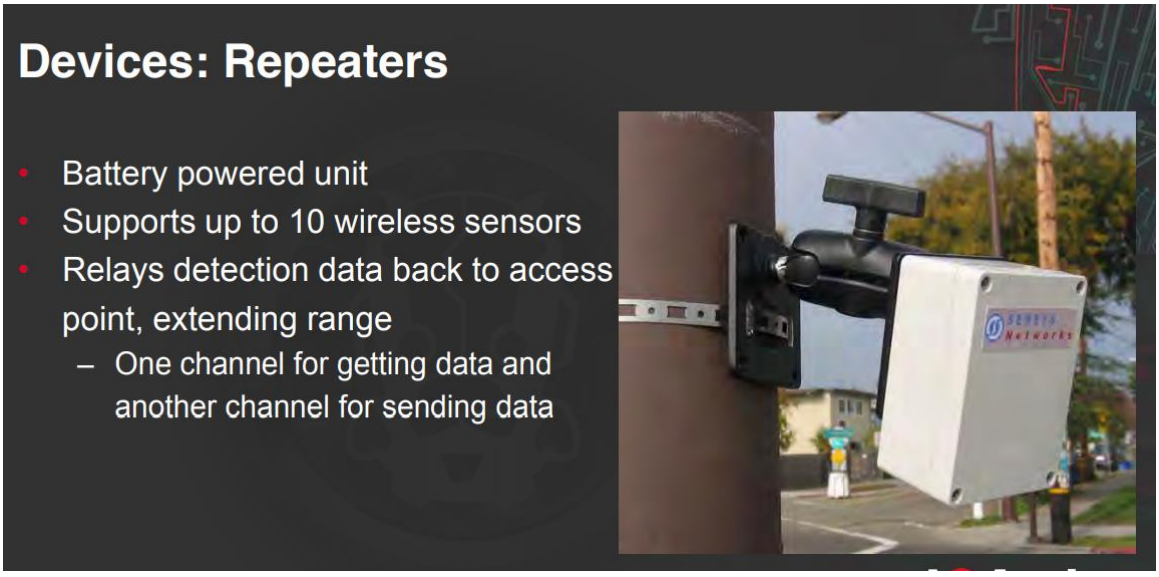


Εικόνα 3: Σημεία πρόσβασης
(https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

Τα σημεία πρόσβασης, υποστηρίζουν όσους αισθητήρες απαιτούνται για τον έλεγχο και λειτουργούν ως IP router, για τις περιφερειακές συσκευές, όπως π.χ βιντεοκάμερες.

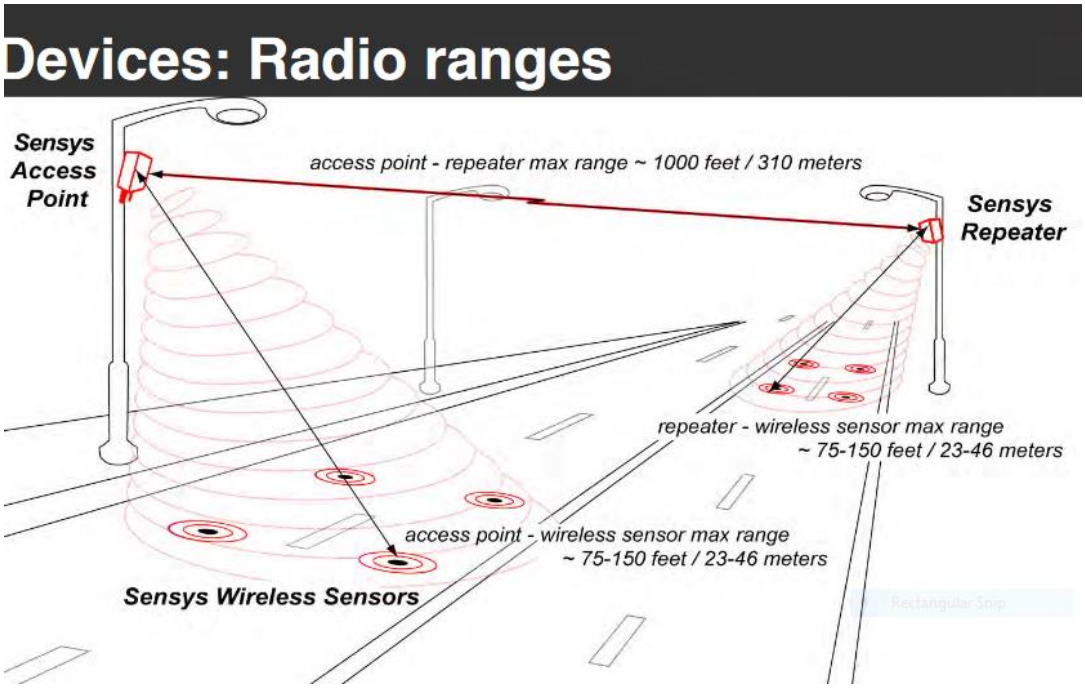
Επίσης συσκευές όπως οι επαναλήπτες πληροφορίας(repeaters), εικόνα 4, οι οποίοι υποστηρίζουν μέχρι 10 αισθητήρες και στέλνουν τα δεδομένα πίσω στο σημείο πρόσβασης (access point).

Συνήθως έχουν ένα κανάλι για την λαμβάνουσα πληροφορία και ένα για την μεταδιδόμενη.



Εικόνα 4: Επαναλήπτες πληροφορίας
(https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

Στην παρακάτω εικόνα εικονίζεται συνολικά το δίκτυο και η τοποθέτηση των αισθητήρων για τον έλεγχο της κυκλοφορίας. Φαίνονται οι επαναλήπτες και οι ασύρματες διατάξεις των αισθητήρων τοποθετημένες σε απόσταση 75-150ft (ποδών) από τους επαναλήπτες (Εικόνα 5) .



Εικόνα 5: Συνολικό δίκτυο ελέγχου κυκλοφορίας
(https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

Η διέλευση των αυτοκινήτων διεγείρει τους αισθητήρες και το παραγόμενο σήμα μεταφέρεται στα σημεία πρόσβασης (access points). Το έκαστο διερχόμενο αυτοκίνητο γίνεται η διεπαφή μεταξύ του παραγόμενου από τη διέλευση σήματος και σημείων ελέγχου της κυκλοφορίας όπως είναι τα φώτα ρύθμισης της κυκλοφορίας. Είναι επίσης δυνατόν να ελεγχθεί πόσο γρήγορα ένα αυτοκίνητο μπορεί από τα φωτά ρύθμισης κυκλοφορίας να περάσει στο δρόμο ταχείας κυκλοφορίας. Επίσης υπάρχουν αισθητήρες που εντοπίζουν πόσα αυτοκίνητα είναι σταματημένα στα φώτα ελέγχου και πόσα πλησιάζουν στο σημείο αυτό.

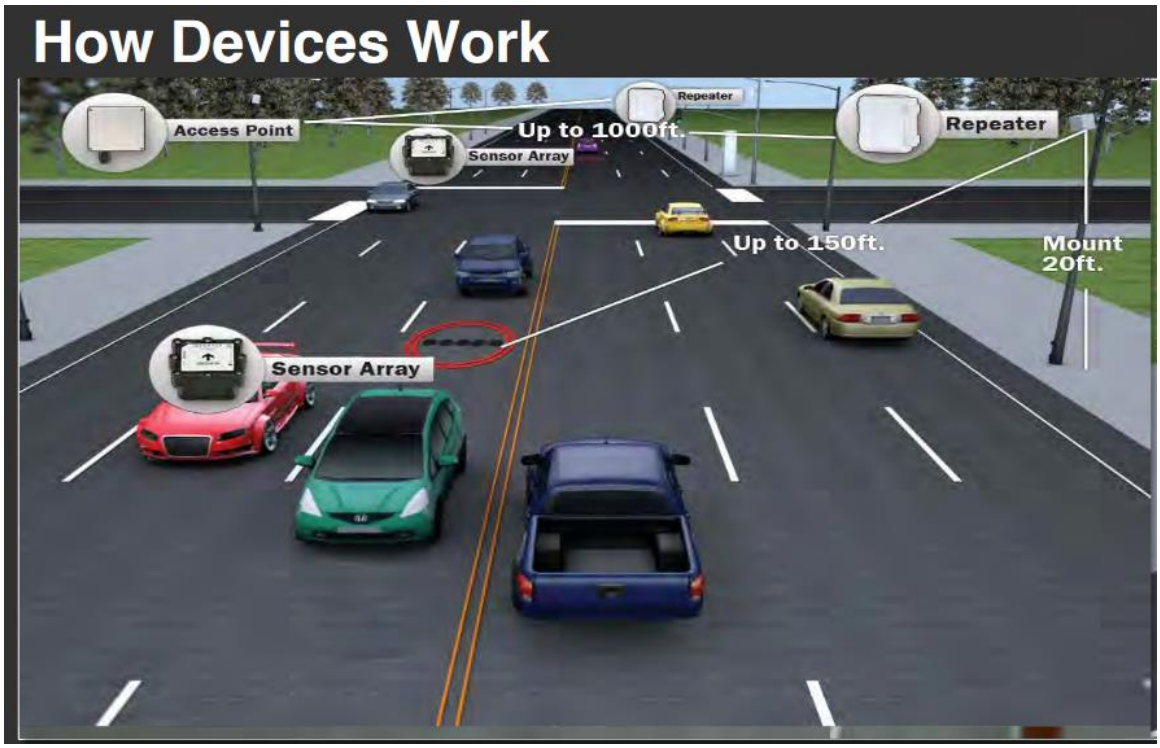
Σε δρόμους ταχείας κυκλοφορίας υπάρχουν τοποθετημένοι πιο πολύ αισθητήρες οι οποίοι ελέγχουν τον αριθμό και την ταχύτητα των αυτοκινήτων που κινούνται στο δρόμο αυτό, ρυθμίζοντας με αυτό τον τρόπο την κυκλοφορία.

Επίσης, υπάρχουν τοποθετημένοι αισθητήρες στις διασταυρώσεις, οπότε με βάση τον αριθμό των αυτοκινήτων που εντοπίζεται, σε στάση, σε κάθε κατεύθυνση, μέσω των

σημάτων από τους αισθητήρες και την επεξεργασία τους, δύναται και πάλι να ρυθμιστεί η κυκλοφορία, ρυθμίζοντας για παράδειγμα τον χρόνο λειτουργίας του πράσινου φωτός.

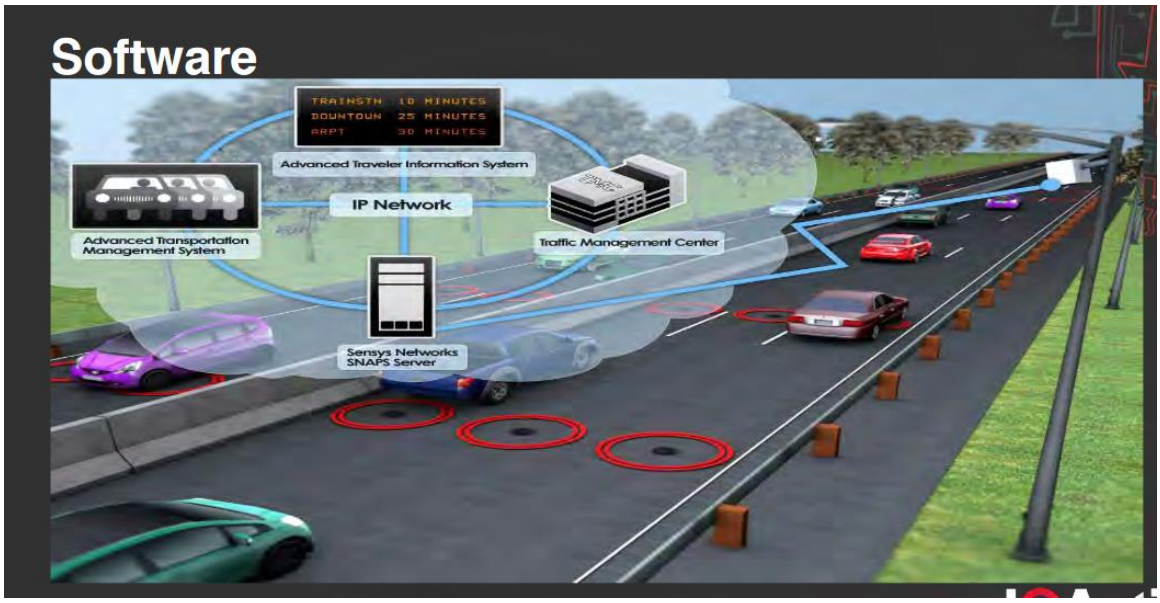
Στις διασταυρώσεις επίσης μπορεί να υπάρχει διαφορετική προσέγγιση τα βραδιά, όπως μπορεί να ρυθμιστεί το άνοιγμα και το σβήσιμο της λειτουργίας του πορτοκαλί φωτός ή να ρυθμιστεί το κόκκινο με συνεχόμενη λειτουργία αν σε άλλο σημείο υπάρχει αναμμένο συνεχώς το πράσινο.

Επίσης, το δίκτυο των αισθητήρων, εικόνα 6, μπορεί να ελέγξει το χρόνο ταξιδιού, ελέγχοντας το περίγραμμα ενός αυτοκίνητου σε δύο διαφορετικά σημεία, μέσω της αλλαγής του μαγνητικού πεδίου. Με αυτό τον τρόπο ελέγχεται και η ταχύτητα καθώς και ο χρόνος που απομένει μέχρι τον επόμενο προορισμό ή τον τελικό προορισμό.



Εικόνα 6: Έλεγχος κυκλοφορίας σε φώτα ελέγχου και σε διασταύρωση
(https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

Τα πρόγραμμα ελέγχου (software), όπως φαίνεται στην εικόνα 7, μπορεί να στηρίζεται στα Windows ή και σε άλλα λειτουργικά συστήματα και λαμβάνει τις πληροφορίες από τους αισθητήρες, επεξεργάζεται την πληροφορία και δίνει τη πληροφορία όπως την περιγράψαμε πιο πάνω για κάθε περίπτωση ελέγχου, σε όλες τις απαιτούμενες συσκευές. Επίσης μπορεί και να ανανεώνεται τακτικά.



Εικόνα 7: Συσκευές και αισθητήρες για τον έλεγχο κυκλοφορίας (https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

2.4 ΕΥΠΑΘΕΙΕΣ ΣΥΣΤΗΜΑΤΟΣ ΚΥΚΛΟΦΟΡΙΑΣ

Παρακάτω αναφέρονται οι ευπάθειες που μπορεί να εμφανιστούν σε ένα σύστημα ελέγχου κυκλοφορίας:

• ***Όλη η ασύρματη επικοινωνία μπορεί να είναι Χωρίς κρυπτογράφηση***

Πιθανοί Ισχυρισμοί προμηθευτών: «Ασφάλεια: Οι ραδιοφωνικές εκπομπές SNP δεν φέρουν ποτέ εντολές, μόνο δεδομένα που μεταδίδουν.

Επομένως, ενώ οι ράδιο επικοινωνίες (RF) ενδέχεται να υπόκεινται σε τοπική παρέμβαση, δεν υπάρχει δυνατότητα ενσωμάτωσης κακόβουλων οδηγιών σε μια συσκευή δικτύου ή σε ένα σύστημα κυκλοφορίας ανάντη .

Η επιλογή κρυπτογράφησης των πληροφοριών αφαιρείται αρκετά νωρίς στον κύκλο ζωής του προϊόντος με βάση την ανατροφοδότηση από τον έκαστο πελάτη.

• ***Χωρίς έλεγχο ταυτότητας***

Είναι δυνατόν να υπάρχει πρόσβαση στους αισθητήρες και τους επαναλήπτες από οποιονδήποτε, συμπεριλαμβανομένων και των ενημερώσεων υλικολογισμικού.

Το AP δεν πιστοποιεί αισθητήρες, απλώς εμπιστεύεται πλήρως τα ασύρματα δεδομένα

Οι ενημερώσεις υλικολογισμικού δεν είναι ούτε κρυπτογραφημένες ούτε υπογεγραμμένες. Οποιοσδήποτε μπορεί να τροποποιήσει το υλικολογισμικό και να ενημερώσει αισθητήρες και επαναλήπτες.

Ισχυρισμοί προμηθευτών: Κρυπτογραφούμε/υπογράφουμε υλικολογισμικό σε τυχόν νεότερες εκδόσεις αισθητήρων.

2.5 ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΛΕΓΧΟΥ

Αναφέρουμε παρακάτω τα βασικά πρωτόκολλα επικοινωνίας, Εικόνα 8, που χρησιμοποιήθηκαν.

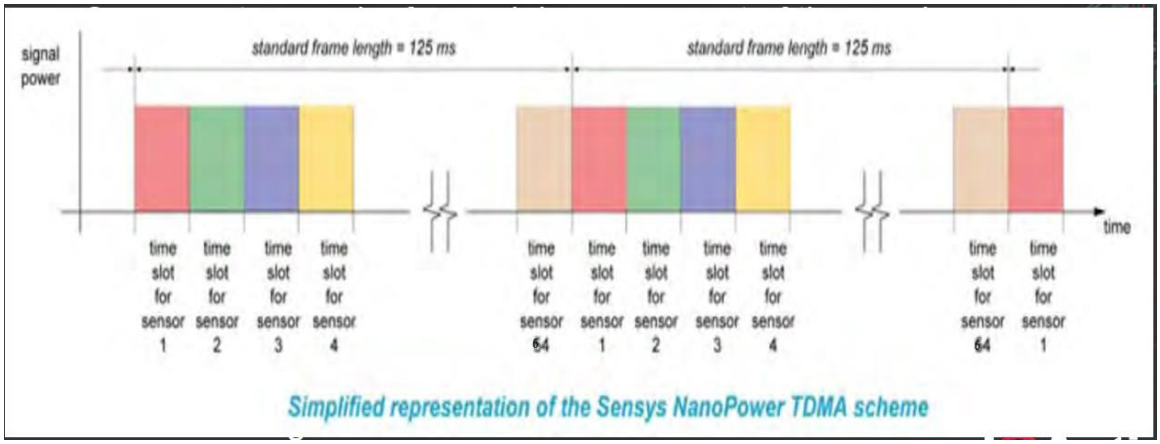
Έτσι αναφέρουμε για παράδειγμα:

Το πρωτόκολλο της IEEE 802.15.4 PHY, που χρησιμοποιείται από το ZigBee και άλλα ασύρματα συστήματα. Ταχύτητα δεδομένων 250 kbps, 16 κανάλια συχνότητας στο ISM των 2,4 GHz εύρος ζώνης (band).

Επίσης, το πρωτόκολλο Sensys NanoPower (SNP) το οποίο χρησιμοποιεί πάνω από τα 802.15.4 PHY ως πρωτόκολλο πρόσβασης πολυμέσων (MAC). Το επίπεδο MAC βασίζεται σε TDMA και χρησιμοποιεί παρόμοιες με αυτές IEEE 802.15.4 MAC επίπεδο.

Η πολλαπλή πρόσβαση διαίρεσης χρόνου (TDMA) είναι μια μέθοδος πρόσβασης καναλιού για κοινόχρηστα μεσαία δίκτυα. Επιτρέπει σε πολλούς χρήστες να μοιράζονται το ίδιο κανάλι συχνότητας διαιρώντας το σήμα σε διαφορετικές χρονικές θυρίδες. Οι χρήστες μεταδίδουν διαδοχικά, ο ένας μετά τον άλλον, ο καθένας χρησιμοποιώντας τη δική του χρονική υποδοχή**.**

Περισσότερα δεδομένα για τα πρωτόκολλα μπορεί να βρει κάποιος στο https://www.youtube.com/watch?v=_j9lELCSZQw.



Εικόνα 8: Απλοποιημένη αναπαράσταση του πρωτοκόλλου SensysNanopower TDMA(https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf)

2.6 ΒΑΡΥΤΗΤΑ ΕΠΙΘΕΣΕΩΝ

Πάνω από 200.000 αισθητήρες και επαναλήπτες σε όλο τον κόσμο θα μπορούσαν να σχετίζονται και ίσως να είναι σταθερά τοποθετημένοι για τον έλεγχο της κυκλοφορίας , όπως για παράδειγμα αισθητήρες για:

Έλεγχο κυκλοφοριακής συμφόρησης σε διασταυρώσεις, σε ράμπες και αυτοκινητόδρομους – ή την στάση στο πράσινο χρώμα (όταν υπερβαίνεται ο μέγιστος χρόνος του πράσινου), το κόκκινο χρώμα και τη διάρκειά του, η λάθος οθόνη του ορίου ταχύτητας κ.λπ.

Επίσης μπορεί να δοθεί από τους αισθητήρες πληροφορία για ατυχήματα, ακόμη και θανατηφόρα από αυτοκινητιστικά δυστυχήματα ή ακόμα μπορεί να αποκλείσουν την κυκλοφορία για τη ευκολότερη διέλευση ασθενοφόρων, πυροσβεστικής, αυτοκίνητων της αστυνομίας κ.λπ, σε περίπτωση ατυχήματος.

Η εθνική υπηρεσία για τους εθνικούς αυτοκινητόδρομους των ΗΠΑ (US DOT Federal Highway Administration) αναφέρει ότι: «… Οι δυσλειτουργίες των αισθητήρων και οι σχετικές βλάβες των σημάτων τους αυξάνουν τον χρόνο ελέγχου και οδηγούν σε καθυστέρηση των οδηγών, σε επιπλέον κόστη συντήρησης, και πιθανά ατυχήματα.

2.7 ΤΡΟΠΟΙ ΕΚΔΗΛΩΣΗΣ ΕΠΙΘΕΣΕΩΝ

Αναφέρουμε παρακάτω τους τρόπους με τους οποίους εκδηλώνονται οι επιθέσεις στα συστήματα ελέγχου κυκλοφορίας:

Με απενεργοποίηση των αισθητήρων/επαναληπτών, με αλλαγή διαμόρφωσης ή υλικολογισμικό, θέτοντας τους αισθητήρες/επαναλήπτες προσωρινά (ίσως και μόνιμα) σε αχρησία αλλάζοντας το υλικολογισμικό τους.

Επίσης, μπορούν να τροφοδοτήσουν τους αισθητήρες με ψεύτικη πληροφορία, όπως μη αληθή δεδομένα εντοπισμού κίνησης, με πολλές ανιχνεύσεις αυτοκινήτων ακόμα και όταν δεν υπάρχει κίνηση. Επιπλέον, μέσω απενεργοποίησης των αισθητήρων/επαναληπτών, είναι δυνατόν να μην στέλνονται δεδομένα ανίχνευσης σε περιπτώσεις δρόμων όπου πραγματικά υπάρχει μεγάλη κυκλοφορία.

Με ενημέρωση κακόβουλου υλικολογισμικού εσφαλμένου αισθητήρα. Θα μπορούσε να συμβεί επίσης συντονισμός ενός αισθητήρα με κακόβουλο υλικολογισμικό, με πιθανότητα να αναπαραχθεί και σε άλλους αισθητήρες. Είναι αδύνατο να γνωρίζει κάποιος, εάν υπάρχουν ήδη παραβιασμένοι αισθητήρες δεδομένου ότι η έκδοση του υλικολογισμικού επιστρέφεται ως πληροφορία από το ίδιο το υλικολογισμικό.

Μπορούν επίσης τα συστήματα αυτά να χρησιμοποιηθούν από την Εθνική υπηρεσία ασφαλείας των ΗΠΑ, την Κυβέρνηση, τις Ειδικές Δυνάμεις ή και τρομοκράτες ακόμα κλπ. για αντίστοιχες κυβερνοεπιθέσεις. Οι αισθητήρες είναι δυνατόν να εντοπίσουν άτομα σε πραγματικό χρόνο, να χακάρουν τα smartphones τους και να χρησιμοποιηθούν για τυχόν επίθεση. Χρησιμοποιούν δεδομένα αναγνώρισης αισθητήρα αυτοκινήτου για να ενεργοποιήσουν διάφορες καταστάσεις, όπως π.χ. βομβιστικούς μηχανισμούς σε αυτοκίνητο.

2.8 ΣΥΜΠΕΡΑΣΜΑΤΑ

Από την παρουσίαση του Cerudo, μπορούν να εξαχθούν τα κάτωθι συμπεράσματα:

• Οποιοσδήποτε άνθρωπος του τρίτου κόσμου μπορεί εύκολα να αγοράσει συσκευές που παράγονται και χρησιμοποιούνται από τις ΗΠΑ, να τις χακάρει και στη συνέχεια να επιτεθεί στις ΗΠΑ.

• Οποιοσδήποτε μπορεί να δημιουργήσει μια συσκευή 100$ για να προκαλέσει προβλήματα στην κυκλοφορία στις σημαντικότερες πόλεις στις ΗΠΑ και άλλες μεγάλες πόλεις στον κόσμο.

• Οι τεχνολογίες που σχετίζονται με τις κρίσιμες υποδομές θα πρέπει να είναι σωστές και να ελέγχονται για να βεβαιωθεί ότι είναι ασφαλείς πριν από τη χρήση.

• Οι έξυπνες πόλεις δεν είναι τόσο έξυπνες όταν τα δεδομένα που χειρίζονται διάφορα συστήματά τους είναι ευκόλως προσβάσιμα και ευάλωτα.

• Ο κυβερνοπόλεμος τελικά είναι μια σχετικά φθηνή διαδικασία.

3. ΕΚΜΕΤΑΛΛΕΥΣΗ ΙΔΙΟΚΤΗΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΔΙΚΤΥΟΥ ΓΙΑ ΤΟΝ ΕΛΕΓΧΟ ΒΗΜΑΤΟΔΟΤΗ

3.1 ΓΕΝΙΚΑ

Με βάση τις πρόσφατες ανησυχίες και γεγονότα ασφαλείας, ο WhiteScope (είναι κυρίαρχος, ανεξάρτητος πάροχος εκπαίδευσης ειδικών και επαγγελματικών υπηρεσιών ασφαλείας) εκτέλεσε μια εξαντλητική αξιολόγηση ασφάλειας στο εμφυτεύσιμο οικοσύστημα καρδιακών συσκευών. Το παρόν κεφάλαιο περιγράφει ευρήματα από την έρευνα, που τονίζουν τις κύριες ανησυχίες σχετικά με την ασφάλεια και την αρχιτεκτονική του οικοσυστήματος των εμφυτεύσιμων καρδιακών συσκευών και τις αλληλεξαρτήσεις τους.

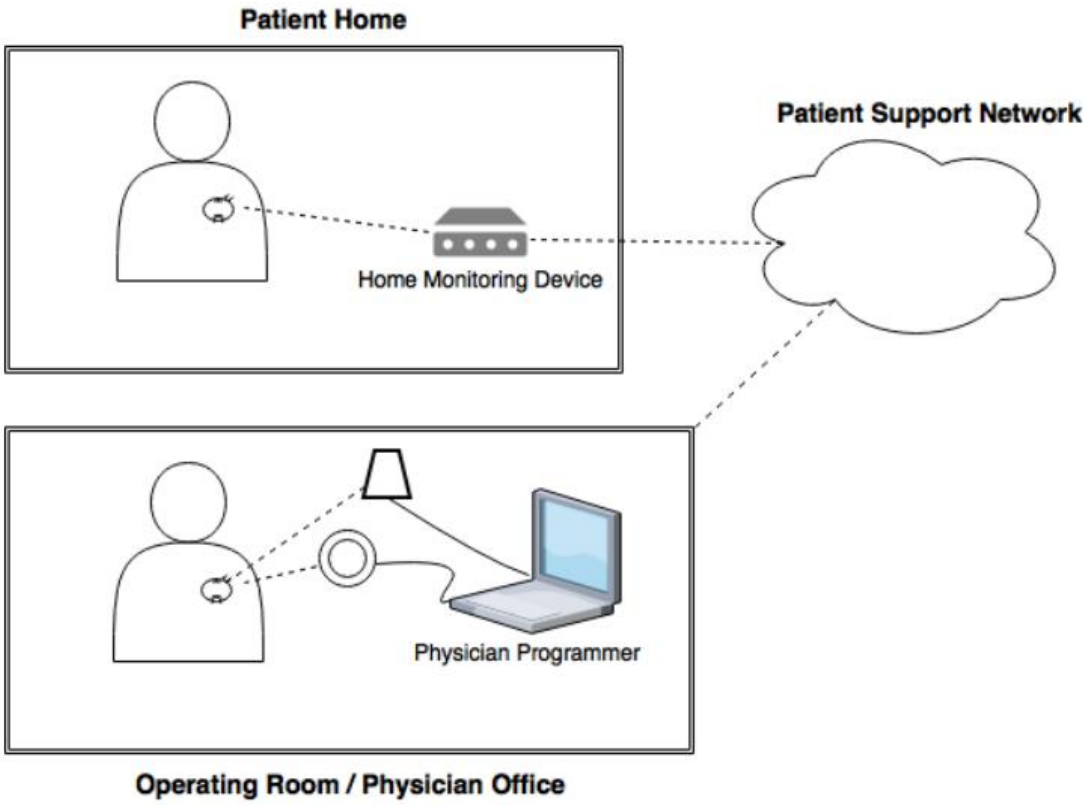
Ο WhiteScope έχει στην διάθεση του προγραμματιστές ιατρικών πράξεων, συσκευές παρακολούθησης στο σπίτι και εμφυτεύσιμες καρδιακές συσκευές για τους τέσσερις μεγάλους προμηθευτές εμφυτεύσιμων καρδιακών συσκευών. Εννοιολογικά, οι τέσσερις μεγάλοι προμηθευτές χρησιμοποιούν ένα παρόμοιο πλαίσιο αρχιτεκτονικής, συμπεριλαμβανομένων πρωτοκόλλων επικοινωνίας, ενδοεπικοινωνιών συσκευών, ενσωματωμένης συσκευής υλικού και ελέγχου ταυτότητας συσκευής. Η ανάλυση αποκάλυψε πιθανούς κινδύνους ασφαλείας που απορρέουν από τα υποκείμενα πρωτόκολλα και τις επικοινωνίες μεταξύ συστημάτων που περιλαμβάνουν ενσωματωμένες συσκευές. Για να μετριάσει τον πιθανό αντίκτυπο στη φροντίδα των ασθενών, συνιστάται στους προμηθευτές να αξιολογήσουν τις αντίστοιχες εφαρμογές τους και να επικυρώσουν ότι υπάρχουν αποτελεσματικοί έλεγχοι ασφαλείας για την προστασία από εντοπισμένες ελλείψεις που μπορεί να οδηγήσουν σε πιθανή παραβίαση του συστήματος.

Τα αποτελέσματα της ολιστικής ανάλυσης βοηθούν στη διευκρίνιση τόσο της φύσης όσο και του εύρους των απειλών που αντιμετωπίζει το οικοσύστημα εμφυτεύσιμης καρδιακής συσκευής, καθώς και τον πιθανό αντίκτυπο στην φροντίδα του ασθενούς. Οι ερευνητές του WhiteScope παρακινούνται από την προοπτική ενίσχυσης της ασφάλειας του

κυβερνοχώρου που αφορά την κοινότητα ιατρικών συσκευών όταν αυτό ενισχύει την ασφάλεια των ασθενών.

3.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΤΟΥ ΟΙΚΟΣΥΣΤΗΜΑΤΟΣ

Το οικοσύστημα εμφυτεύσιμων καρδιακών συσκευών αποτελείται από μια εμφυτεύσιμη ιατρική συσκευή (π.χ. βηματοδότης ή απινιδωτής), τον προγραμματιστή ιατρό, την συσκευή παρακολούθησης από το σπίτι και το δίκτυο υποστήριξης των ασθενών. Το παρακάτω σχήμα 2 δείχνει μια αναπαράσταση της γενικής αρχιτεκτονικής του οικοσυστήματος.



Σχήμα 2. Αρχιτεκτονική οικοσυστήματος βηματοδοτών (Rios and Butts J., 2017)

Τα υποσυστήματα εντός ενός τέτοιου οικοσυστήματος αλληλοεπιδρούν για να διευκολύνουν την παράδοση και την παρακολούθηση της θεραπείας των ασθενών. Η

ακόλουθη λίστα προσδιορίζει τις κύριες λειτουργίες των υποσυστημάτων του οικοσυστήματος:

Εμφυτεύσιμη καρδιακή συσκευή - Implantable Cardiac Device (ICD)

Είναι μια συσκευή με μπαταρία που εμφυτεύεται χειρουργικά κάτω από το δέρμα ενός ασθενούς. Μια εμφυτεύσιμη καρδιακή συσκευή βηματοδότη στέλνει ηλεκτρικούς παλμούς στην καρδιά για να την βοηθήσει να διατηρήσει έναν κανονικό-φυσιολογικό ρυθμό λειτουργίας.

Ο εμφυτεύσιμος απινιδωτής είναι ο άλλος πρωταρχικός τύπος εμφυτεύσιμης καρδιακής συσκευής (ICD). Αυτός παρακολουθεί τους καρδιακούς ρυθμούς και προκαλεί ηλεκτροσόκ εάν ανιχνεύσει επικίνδυνους ρυθμούς λειτουργίας της καρδιάς.

Προγραμματιστής ιατρός

Είναι μια συσκευή που χρησιμοποιείται στη διάγνωση και τον προγραμματισμό της εμφυτεύσιμης καρδιακής συσκευής. Ο προγραμματιστής ιατρός προορίζεται για κλινικές ρυθμίσεις, όπως σε χειρουργείο ή σε ιατρείο. Μόλις η καρδιακή συσκευή εμφυτεύεται, ο προγραμματιστής χρησιμοποιείται στο χειρουργείο για να δοκιμάσει τη λειτουργία της καρδιακής συσκευής και τον καθορισμό παραμέτρων θεραπείας ασθενούς.

Οι γιατροί μπορούν επίσης να χρησιμοποιούν τον προγραμματιστή σε επακόλουθες επισκέψεις του ασθενούς στο ιατρείο για να εξετάσουν τη λειτουργικότητα της καρδιακής συσκευής, την επανεξέταση της χορηγούμενης θεραπείας και ενημέρωσης των παραμέτρων θεραπείας του ασθενούς. Ο προγραμματιστής επικοινωνεί με την εμφυτεύσιμη καρδιακή συσκευή μέσω ασύρματης σύνδεσης με χρήση ραδιοσυχνοτήτων και επαγωγικής τηλεμετρίας, έτσι ώστε η συσκευή (π.χ. βηματοδότης) να μην χρειάζεται να αφαιρεθεί χειρουργικά για ενημερώσεις και διάγνωση.

Συσκευή παρακολούθησης στο σπίτι

Είναι μια συσκευή που χρησιμοποιείται για τη μετάδοση και παρακολούθηση της εμφυτεύσιμης καρδιακής συσκευής και των δεδομένων θεραπείας των ασθενών. Η συσκευή παρακολούθησης στο σπίτι προορίζεται για χρήση στην κατοικία ενός ασθενούς. Η οικιακή συσκευή παρακολούθησης τοποθετείται συχνά κοντά στον ασθενή όπου

κοιμάται. Η συσκευή παρακολούθησης του σπιτιού συγκεντρώνει τα δεδομένα της θεραπείας του ασθενούς από την εμφυτεύσιμη καρδιακή συσκευή και μεταδίδει τα δεδομένα μέσω του δικτύου υποστήριξης ασθενών στον ιατρό του ασθενούς. Η ενσωμάτωση της συσκευής παρακολούθησης στο σπίτι στο οικοσύστημα αποσκοπεί στην ενίσχυση της φροντίδας των ασθενών με τον εντοπισμό των προβλημάτων γρήγορα και την ελαχιστοποίηση των επαναλαμβανόμενων επισκέψεων στο γραφείο. Πρόσφατα, η Εταιρεία Καρδιακού Ρυθμού (Heart Rhythm Society), δημοσίευσε έρευνα που επισημαίνει τα κλινικά οφέλη της απομακρυσμένης μετάδοσης και παρακολούθησης των εμφυτεύσιμων καρδιακών συσκευών και των δεδομένων της θεραπείας των ασθενών (Slotwiner et al, 2015) Τα ευρήματα υποδεικνύουν μεγαλύτερη διατήρηση ασθενών και βελτιωμένη συμμόρφωση με προγραμματισμένες αξιολογήσεις, με αποτέλεσμα τη συνολική βελτίωση της ποιότητας και της αποτελεσματικότητας της φροντίδας τους.

Δίκτυο υποστήριξης ασθενών

Το δίκτυο υποστήριξης ασθενών είναι μια αποκλειστική υποδομή δικτύων που χρησιμοποιείται για να διευκολύνει την μετάδοση των δεδομένων της θεραπείας των ασθενών από τη συσκευή παρακολούθησης στο σπίτι στον κλινικό γιατρό. Συνδεδεμένα μέσα επικοινωνίας από την συσκευή παρακολούθησης στο σπίτι, στο δίκτυο υποστήριξης ασθενών περιλαμβάνουν μόντεμ dial-up, κυψελοειδή και wifi. Οι προμηθευτές χρησιμοποιούν επίσης το δίκτυο υποστήριξης ασθενών για την εγγραφή ασθενών και συσκευών καθώς επίσης και για την ενημέρωση του συστήματος από την συσκευή παρακολούθησης στο σπίτι. Μια πύλη που σχετίζεται με το δίκτυο υποστήριξης ασθενών παρέχει στους ασθενείς και τους γιατρούς τη δυνατότητα σύνδεσης και αναθεώρησης των δεδομένων της θεραπείας των ασθενών. Το δίκτυο υποστήριξης ασθενών παρέχει επίσης δυνατότητα ειδοποίησης του γιατρού όταν ένας ασθενής εμφανίζει ορισμένες καρδιακές παραμέτρους που χρήζουν προσοχής.

Η επικοινωνία εντός του οικοσυστήματος πραγματοποιείται κυρίως μεταξύ: (i) του προγραμματιστή ιατρού και της εμφυτεύσιμης καρδιακής συσκευής για προγραμματισμό και ανάλυση (ii) της συσκευής παρακολούθησης στο σπίτι και της εμφυτεύσιμης καρδιακής συσκευής για την εξαγωγή δεδομένων (iii) της εμφυτεύσιμης καρδιακής συσκευής και της συσκευή παρακολούθησης στο σπίτι για την παροχή των δεδομένων της θεραπείας των ασθενών (iv) της συσκευής παρακολούθησης στο σπίτι και του δικτύου υποστήριξης ασθενών για τη μετάδοση των δεδομένων της θεραπείας των ασθενών και την ενημέρωση της συσκευής παρακολούθησης στο σπίτι. Η πλειοψηφία των επικοινωνιών βασίζεται σε πρωτόκολλα από συσκευή σε συσκευή που σχετίζονται με τις ενσωματωμένες επικοινωνίες συσκευών.

3.3 ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

Έχουν δημοσιευτεί και άλλες υποστηρικτικές έρευνες που επισημαίνουν τους σχετικούς κινδύνους ασφαλείας που συνδέονται με το οικοσύστημα των εμφυτεύσιμων καρδιακών συσκευών. Το 2008, ο Halperin κ.α. αξιολόγησαν τις ιδιότητες ασφαλείας και παρουσίασαν επιθέσεις σε κοινά ICDs (Halperin et al, 2008). Η ερευνά τους απέδειξε την αντίστροφη μηχανική των πρωτοκόλλων επικοινωνίας ICD και επιθέσεις μέσω ραδιοσυχνοτήτων καθορισμένου από λογισμικό που έχουν τη δυνατότητα να επηρεάσουν την ασφάλεια των ασθενών. Ομοίως, οι Hei et al. παρουσίασαν έρευνα που κατέδειξε επιθέσεις εξάντλησης πόρων έναντι των εμφυτεύσιμων ιατρικών συσκευών (IMD) (Hei, Du, Wu & Hu, 2010). Η έρευνα επικεντρώθηκε σε γενικές εφαρμογές των IMD's και υποστήριξε ότι παρέχει τη δυνατότητα μείωσης σημαντικά της διάρκειας ζωής της μπαταρίας για κατηγορίες IMD's που χρησιμοποιήθηκαν σε ασύρματες επικοινωνίες με εξωτερικό προγραμματιστή.

Το 2010, οι Maisel και Kohno ζήτησαν ένα συγκεκριμένο κανονιστικό πλαίσιο για την ιατρική ασφάλεια της συσκευής (Maisel & Kohno, 2010). Η έρευνά τους έδωσε έμφαση στις ανησυχίες σχετικά με τις ιδιότητες ασφαλείας που σχετίζονται με συσκευές που εκτελούν λειτουργίες σωτήριες για την ζωή, όπως ένας βηματοδότης. Επιπλέον, η εργασία του Maisel και του Kohno ανέδειξε τους κινδύνους που σχετίζονται με την αρχιτεκτονική και εφαρμογή αλληλεξαρτήσεων για ένα οικοσύστημα που επεκτείνεται πέραν από τους κινδύνους εφαρμογής του προμηθευτή. Υποστήριξαν επίσης ότι αυτές οι ιατρικές συσκευές παρέχουν σημαντικά οφέλη για την υγεία των ασθενών και ότι πρέπει να σταθμίζονται οι έλεγχοι ασφαλείας ανάλογα με τις επιπτώσεις στη φροντίδα των ασθενών.

Το 2012, οι Burleson και Fu συζήτησαν τις προκλήσεις σχεδιασμού που σχετίζονται με την ασφάλεια των εμφυτεύσιμων ιατρικών συσκευών (Burleson & Fu, 2012). Οι συγγραφείς παρείχαν ένα μοντέλο απειλής και συζήτησαν πόσο σημαντικοί παράγοντες ασφαλείας ισχύουν συνήθως σε πολλές εμφυτεύσιμες καρδιακές συσκευές. Οι ενδείξεις της έρευνάς τους δείχνουν κοινά θέματα σε διάφορα IMDs προμηθευτών, καταδεικνύοντας ευρύτερες ανησυχίες για συγκεκριμένους τομείς.

Πρόσφατα, οι Marin et al. δημοσίευσαν έρευνα που εξέτασε ιδιόκτητα πρωτόκολλα που χρησιμοποιούνται στις ασύρματες επικοινωνίες μεταξύ προγραμματιστών ιατρών και ICDs (Marin, Singelee, Garcia, Chothia, Willems & Preneel, 2016). Χρησιμοποίησαν τεχνικές αντίστροφης μηχανικής black-box για την εξέταση του καναλιού RF μεγάλης εμβέλειας την πιο πρόσφατη γενιά ICDs. Η έρευνά τους εντόπισε πολλαπλά πρωτόκολλα και αδυναμίες εφαρμογής που παρέχουν σε έναν εισβολέα τη δυνατότητα να διεξάγει και επιθέσεις άρνησης υπηρεσίας, καθώς και την έναρξη επιθέσεων πλαστογραφίας και

αναπαραγωγής μηνυμάτων που μπορούν να επηρεάσουν την ασφάλεια των ασθενών. Οι συγγραφείς σημειώνουν ότι η έρευνά τους επικυρώθηκε για τουλάχιστον δέκα τύπους ICD.

Η έρευνα του WhiteScope που παρουσιάζεται σε αυτό το έγγραφο εξετάζει την αρχιτεκτονική και αλληλεξαρτήσεις εφαρμογής σε όλο το οικοσύστημα εμφυτεύσιμων καρδιακών συσκευών. Η έρευνα αυτή επικεντρώνεται σε μια ολιστική ανάλυση της υποκείμενης αρχιτεκτονικής. Τα ευρήματα της έρευνας, σε συνδυασμό με άλλες υποστηρικτικές έρευνες, υποδεικνύουν ανησυχίες για την πιθανή ασφάλεια σχετικά με τον πυρήνα της υποκείμενης αρχιτεκτονικής που μπορούν να εφαρμοστούν σε όλες τις υλοποιήσεις προμηθευτών.

3.4 ΕΥΡΗΜΑΤΑ

Στο σύνολό του, το οικοσύστημα των εμφυτεύσιμων καρδιακών συσκευών κληρονομεί χαρακτηριστικά ασφαλείας που σχετίζονται με την υποκείμενη αρχιτεκτονική συστήματος-συστημάτων. Εάν δεν εφαρμόζονται έλεγχοι ασφαλείας, τότε αδυναμίες που σχετίζονται με την αρχιτεκτονική και οι αλληλεξαρτήσεις εφαρμογής έχουν τη δυνατότητα να θέσουν σε κίνδυνο το οικοσύστημα εμπιστευτικότητα, ακεραιότητα ή/και διαθεσιμότητα - με αποτέλεσμα δυνητικά αρνητικές συνέπειες στη φροντίδα των ασθενών εάν αξιοποιηθούν αυτές οι αδυναμίες.

Ο WhiteScope ξεκίνησε την ανάλυση εξετάζοντας χαρακτηριστικά αρχιτεκτονικής και εφαρμογή αλληλεξαρτήσεων για τον εντοπισμό πιθανών περιοχών κινδύνου. Μόλις οι περιοχές κινδύνου προσδιορίστηκαν, ο WhiteScope απέκτησε υποσυστήματα για τους τέσσερις μεγάλους προμηθευτές και εξέτασε τα υποσυστήματα για να αξιολογήσει τους ελέγχους ασφαλείας και να διακρίνει την ύπαρξη πιθανών αδυναμιών ασφάλειας. Τα ευρήματα που παρουσιάζονται παρακάτω δείχνουν τα αποτελέσματα της αξιολόγησης και τον προσδιορισμό των πιθανών προβλημάτων ασφάλειας που ενδέχεται να δικαιολογούν την εφαρμογή περαιτέρω ελέγχων ασφαλείας για τον μετριασμό πιθανών κινδύνων. Τα ευρήματα δεν επιχειρούν να καταγράψουν όλους τους πιθανούς περιορισμούς και ελέγχους που μπορεί να υπάρχουν ή την διαφορετική δυσκολία οποιασδήποτε προσπάθειας εκμετάλλευσης πιθανών τρωτών σημείων. Η περίληψη επίσης δεν επιδιώκει να αντιμετωπίσει τις ανάγκες ευχρηστίας των ασθενών και των ιατρών που ενδέχεται να επηρεαστούν και πρέπει να εξισορροπηθούν έναντι πιθανών ζητημάτων ασφαλείας. Σημειώστε ότι για ανάλυση, οι κύριοι τομείς εστίασης για την αλληλεπίδραση υποσυστημάτων είναι: (i) το σύστημα παρακολούθησης στο σπίτι και η εμφυτεύσιμη καρδιακή συσκευή, (ii) το σύστημα παρακολούθησης στο σπίτι και το δίκτυο υποστήριξης ασθενών και (iii) ο προγραμματιστής ιατρός και η εμφυτεύσιμη καρδιακή συσκευή.

3.5 ΔΥΝΑΤΟΤΗΤΑ ΑΠΟΚΤΗΣΗΣ ΤΩΝ ΥΠΟ ΠΡΟΜΗΘΕΙΑ ΥΠΟΣΥΣΤΗΜΑΤΩΝ ΑΠΟ ΔΗΜΟΣΙΟΥΣ ΦΟΡΕΙΣ

Ο WhiteScope μπόρεσε να αποκτήσει υποσυστήματα για τους τέσσερις μεγάλους προμηθευτές μέσω δημόσιων ιστοσελίδων δημοπρασιών. Ως σημείο αναφοράς, ο παρακάτω πίνακας 3 δείχνει ένα στιγμιότυπο των διαθέσιμων συσκευών παρακολούθησης στο σπίτι και προγραμματιστών ιατρών για προμήθεια από το eBay. Παρόλο που η ευκολία απόκτησης εμφυτεύσιμων καρδιακών υποσυστημάτων δεν είναι μια συγκεκριμένη ευπάθεια, μπορεί να βοηθήσει έναν επιτιθέμενο (hacker) στην εκμετάλλευση του εν λόγω οικοσυστήματος. Για παράδειγμα, εάν ένας προμηθευτής χρησιμοποιεί κοινά αλλά αυστηρά κωδικοποιημένα διαπιστευτήρια, ένας εισβολέας έχει τη δυνατότητα να συλλέξει τα διαπιστευτήρια από το υποσύστημα που προμηθεύεται μέσω δημόσιου ιστότοπου δημοπρασιών και στη συνέχεια να αξιοποιήσει τα διαπιστευτήρια ως επιφάνεια επίθεσης για πολλαπλά υποσυστήματα.

	Vendor One	Vendor Two	Vendor Three	Vendor Four
Home Monitoring Device	7	52	18	5
Physician Programmer	2	1	1	3

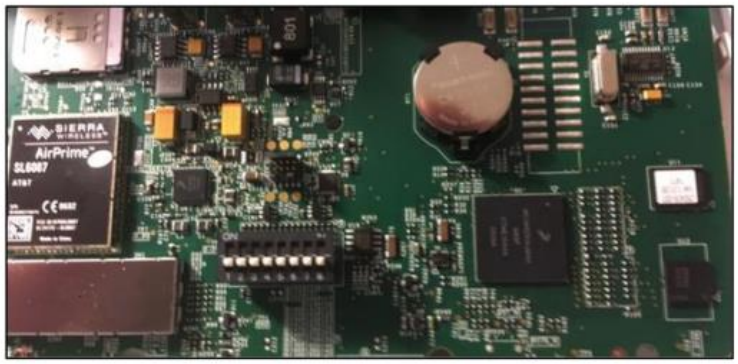
Πίνακας 3. Αριθμός διαθέσιμων συσκευών στο e bay. Πληροφορία από 23-11-2016 (Rios and Butts J., 2017)

3.6 ΕΥΑΛΩΤΑ-ΤΡΩΤΑ ΣΗΜΕΙΑ ΣΤΟ ΟΙΚΟΣΥΣΤΗΜΑ ΤΩΝ ΕΜΦΥΤΕΥΣΙΜΩΝ ΚΑΡΔΙΑΚΩΝ ΣΥΣΚΕΥΩΝ

3.6.1 Εμπορικοί μικροεπεξεργαστές άμεσα διαθέσιμοι (στο ράφι)

Παρόλο που δεν θεωρείται ένα εξόχως σημαντικό θέμα ευπάθειας, η χρήση μικροεπεξεργαστών εμπορίου με άμεσα διαθέσιμα φύλλα δεδομένων μπορεί να βοηθήσει έναν εισβολέα στην αντίστροφη μηχανική διαδικασία. Οι ταξινομικοί σειριακοί αριθμοί των ολοκληρωμένων κυκλωμάτων (IC's) επιτρέπουν την εύρεση γνωστών σημάτων ή ακόμα και τους κωδικούς ελέγχου στα φύλλα δεδομένων. Οι κωδικοί παρέχουν όρους με δυνατότητα αναζήτησης όταν υλοποιείται αποσυναρμολόγηση του υλικολογισμικού, καθιστώντας δυνατή την εύρεση των ρουτίνων που διασυνδέονται, με συγκεκριμένα στοιχεία υλικού, όπως μνήμη flash. Ως αποτέλεσμα, ένας επιτιθέμενος έχει τη δυνατότητα αναγνώρισης κρίσιμων λειτουργιών και εντολών που σχετίζονται με το υποσύστημα, ενισχύοντας έτσι τη διαδικασία της αντίστροφης μηχανικής. Επιπλέον, τα φύλλα

δεδομένων αποκαλύπτουν τη συγκεκριμένη αρχιτεκτονική τσιπ. Τα φύλλα δεδομένων για εμπορικούς μικροεπεξεργαστές που σχετίζονται με τις συσκευές παρακολούθησης στο σπίτι διατίθενται ανοιχτά στο Διαδίκτυο. Ως αποτέλεσμα, ένας επιτιθέμενος έχει τη δυνατότητα αναγνώρισης της αρχιτεκτονικής του συστήματος προκειμένου να διευκολυνθεί η αντίστροφη μηχανική. Σημειώστε ότι είναι πιθανό ένας εισβολέας να μπορεί να εντοπίσει τη λειτουργικότητα ακόμη και χωρίς αναγνωρίσιμους εμπορικούς μικροεπεξεργαστές από το ράφι. Ωστόσο, η χρήση τους μπορεί να βοηθήσει έναν εισβολέα να εντοπίσει πιο γρήγορα τη λειτουργικότητα και να επιτρέψει τη χρήση αυτοματοποιημένων εργαλείων hacking. Στο εικόνα 9 δείχνουμε την οικιακή συσκευή του προμηθευτή No 3.



Εικόνα 9. Εμπορική οικιακή συσκευή του προμηθευτή No 3.
(http://www.alldatasheet.com/datasheet-pdf/pdf/396495/FREESCALE/MCIMX251AJM4A.html)

3.6.2 Διεπαφές εντοπισμού σφαλμάτων σε ενσωματωμένη συσκευή

Οι ενσωματωμένες συσκευές συνήθως ενσωματώνουν διεπαφές για να παρέχουν εντοπισμό σφαλμάτων εντός λειτουργικού κυκλώματος. Η διεπαφή JTAG [3] που προορίζεται για λειτουργικές δοκιμές μπορεί να χρησιμοποιηθεί για απόκτηση υλικολογισμικού, ανίχνευση εντολών, ανάγνωση τμημάτων μνήμης, σύλληψη και επαναφορά τμημάτων μνήμης, και να μεταβάλλει τις τιμές των καταχωρητών. Εντοπίστηκαν διεπαφές JTAG που επιτρέπουν αλληλεπίδραση συσκευών οικιακής παρακολούθησης και προγραμματιστών γιατρών. Ως αποτέλεσμα, ένας εισβολέας έχει τη

[3] **Το JTAG** (που πήρε το όνομά του από την **κοινή ομάδα δράσης δοκιμών** που το κωδικοποίησε) είναι ένα βιομηχανικό πρότυπο για την επαλήθευση των σχεδίων και τη δοκιμή των τυπωμένων κυκλωμάτων μετά την κατασκευή.
Η JTAG εφαρμόζει πρότυπα για όργανα on-chip στον αυτοματισμό ηλεκτρονικού σχεδιασμού (EDA) ως συμπληρωματικό εργαλείο ψηφιακής προσομοίωσης.

δυνατότητα να αποκτήσει υλικολογισμικό υποσυστήματος καθώς και παύση και ανακατεύθυνση της ροής εντολών.

Μια άλλη κοινή διεπαφή εντοπισμού σφαλμάτων σε ενσωματωμένες συσκευές είναι το UART. Το UART χρησιμοποιείται συνήθως για τον εντοπισμό σφαλμάτων για να επιτρέψει μια σειριακή διασύνδεση μεταξύ της ενσωματωμένης σειριακής θύρας συσκευής και υπολογιστή ή USB. Με τη διαμόρφωση των παραμέτρων διεπαφής σε κοινές ρυθμίσεις για κάθε αντίστοιχο προμηθευτή, ένας εισβολέας έχει τη δυνατότητα να κερδίσει προνομιακή πρόσβαση μέσω κονσόλας σε οικιακές συσκευές παρακολούθησης και προγραμματιστές γιατρούς. Με την προνομιακή πρόσβαση, ένας εισβολέας έχει τη δυνατότητα να αποκτήσει το υλικολογισμικό του υποσυστήματος/συστήματος αρχείων.

3.6.3 Κρυπτογραφημένο υλικολογισμικό

Η χρήση τεχνικών όπως κλειστού τύπου υλικολογισμικό, η απόκρυψη και η κρυπτογράφηση καθιστούν πολύ δυσκολότερη την διαδικασία της αντίστροφης μηχανικής του υλικολογισμικού. Ανάλυση οικιακών συσκευών παρακολούθησης για τους τέσσερις προμηθευτές αποκάλυψαν ότι κανένα κλειστού τύπου υλικολογισμικό δεν χρησιμοποιεί τεχνικές κρυπτογράφησης. Κατά συνέπεια, μόλις ένας εισβολέας αποκτήσει ένα υποσύστημα του υλικολογισμικού, υπάρχει η δυνατότητα αντίστροφης μηχανικής του υλικολογισμικού, χωρίς να χρειάζεται να αποκρυπτογραφήσει την απόκρυψη ή την κρυπτογράφηση.

3.6.4 Εμποτισμένες -κρυφές συσκευές και επαφές για επανέλεγχο

Οι εμποτισμένες συσκευές συνήθως περιλαμβάνουν διεπαφές για τον έλεγχο και επανέλεγχο της λειτουργικότητάς τους. Στα λειτουργικά τεστ η διεπαφή JTAG για παράδειγμα μπορεί να χρησιμοποιηθεί για τον έλεγχο του υλικολογισμικού, για τον έλεγχο της μνήμης και της χωρητικότητας και άλλες κρίσιμες λειτουργίες.

Οι διεπαφές JTAG εντοπίστηκαν με επιτρεπόμενη αλληλεπίδραση συσκευών σε συσκευές οικιακής παρακολούθησης και προγραμματισμό επίσης

3.6.5 Χρήση συναρτήσεων λειτουργίας τύπου ASCII και αντιμετώπιση λογισμικού

Η χρήση κειμένου ASCII για ονόματα συναρτήσεων παρέχει κρίσιμες ενδείξεις για την κλήση στον κώδικα συγκεκριμένων συναρτήσεων που μπορούν να βοηθήσουν στην διαδικασία της αντίστροφης μηχανικής. Επιπλέον, σύμβολα εντοπισμού σφαλμάτων του λογισμικού και τα σχόλια του πηγαίου κώδικα μπορούν να αποκαλύψουν την

λειτουργικότητα και τις κρίσιμες περιοχές του κώδικα. Η ανάλυση των συσκευών των τεσσάρων προμηθευτών εντόπισε χρήση κειμένου ASCII για ονόματα συναρτήσεων καθώς και εκδόσεις που κυκλοφορούν και περιείχαν χαρακτηριστικά εντοπισμού σφαλμάτων λογισμικού. Ως αποτέλεσμα, είναι ο εισβολέας να έχει τη δυνατότητα να εντοπίσει κρίσιμα τμήματα της κωδικοποίησης που σχετίζονται με λειτουργίες του εκάστοτε υποσυστήματος. Αξίζει να σημειωθεί δε, ότι είναι πιθανό ένας εισβολέας να μπορεί να προσδιορίσει τη λειτουργικότητα ακόμη και χωρίς κείμενο ASCII, για ονόματα λειτουργιών και χαρακτηριστικά εντοπισμού σφαλμάτων λογισμικού. Ωστόσο, ο περιορισμός της χρήσης τους μπορεί να προσθέσει έναν βαθμό δυσκολίας για έναν πιθανό εισβολέα.

3.6.6 Χρήση βιβλιοθηκών τρίτων

Οι προγραμματιστές λογισμικού αξιοποιούν συνήθως και στοιχεία τρίτων (π.χ. βιβλιοθήκες) για επιπλέον βοήθεια επιταχύνοντας τη διαδικασία ανάπτυξης του λογισμικού. Η συμπερίληψη στοιχείων τρίτων, ωστόσο, μπορεί να εισαγάγει πιθανά τρωτά σημεία που συχνά σε διαφορετική περίπτωση δεν μπορούν να συμβούν.

Πολλές περιπτώσεις όμως ενσωμάτωσαν ξεπερασμένα και ευάλωτα στοιχεία από τρίτα μέρη. Κατά συνέπεια, μπορεί να υπάρχει η δυνατότητα για έναν επιτιθέμενο να αξιοποιήσει δημόσια γνωστές πηγές κώδικα και να θέσουν σε κίνδυνο το έκαστο υποσύστημα.

Οι αριθμοί που σχετίζονται με τα ανιχνευμένα στοιχεία στον κώδικα τρίτων μερών και ο σχετικός αριθμός γνωστών τρωτών σημείων, όπου μπορούν να χρησιμοποιηθούν από προγραμματιστές γιατρούς αναφέρονται παρακάτω (Πίνακας 4).

	Vendor One	Vendor Two	Vendor Three	Vendor Four
Number of identified third-party components	201	47	77	21
Number of vulnerable third-party components	74	39	51	10
Identified number of known vulnerabilities in third-party components	2,354	3,715	1,954	642

Πίνακας 4: Ποσοτική ανίχνευση στοιχείων στον κώδικα τρίτων μερών (Rios and Butts J., 2017)

3.6.7 Χαρτογράφηση της εικόνας του υλικολογισμικού σε προστατευμένη μνήμη

Η αντιστοίχιση της εικόνας του υλικολογισμικού σε προστατευμένη μνήμη υπολογιστή, αποτρέπει τη δυνατότητα αντικατάστασης ή την αλλαγή της κρίσιμης λειτουργικότητας

του υποσυστήματος κατά τη λειτουργία του. Αν η εικόνα του υλικολογισμικού αντιστοιχεί σε προστατευμένη μνήμη, ο εισβολέας πρέπει να χρησιμοποιήσει διαφορετική περιοχή μνήμης για τυχόν φόρτωση κακόβουλου κώδικα. Οι συσκευές παρακολούθησης στο σπίτι δεν περιλαμβάνουν πρόγραμμα υλοποίησης που ενσωματώνει τη χαρτογράφηση των εικόνων υλικολογισμικού σε προστατευμένη μνήμη. Ως εκ τούτου, ένας εισβολέας έχει τη δυνατότητα να γράψει αυθαίρετα εντολές στη μνήμη και να τροποποιήσει τη βασική λειτουργία του συστήματος.

3.6.8 Εξωτερικές συνδέσεις με USB (Universal Serial Bus)

Οι οικιακές συσκευές παρακολούθησης περιλάμβαναν εξωτερικές συνδέσεις USB που επέτρεπαν την επικοινωνία σε επίπεδο συστήματος. Αξιοποιώντας τις συνδέσεις USB, ένας εισβολέας δυνητικά μπορεί να προσπελάσει το σύστημα αρχείων ή να εισαγάγει κακόβουλο λογισμικό στις οικιακές συσκευές παρακολούθησης.

Παρόλο που απαιτείται και κάποια λειτουργικότητα του συστήματος, να υπάρχουν συνδέσεις USB, θα πρέπει να προστατευτούν με τέτοιο τρόπο ώστε να επιτρέπονται μόνο εξουσιοδοτημένες συσκευές για χρήση.

3.6.9 Κωδικοποιημένα διαπιστευτήρια και δεδομένα υποδομής

Οι ενσωματωμένες συσκευές συχνά χρησιμοποιούν σχήματα ελέγχου ταυτότητας από συσκευή σε συσκευή. Σαν συνέπεια αυτού, τα διαπιστευτήρια για τον έλεγχο ταυτότητας πρέπει να αποθηκεύονται με κάποιο τρόπο στο σύστημα ελέγχου ταυτότητας. Η ανάλυση ανέδειξε τη χρήση διαπιστευτηρίων με σκληρό κωδικό στις οικιακές συσκευές παρακολούθησης για τον έλεγχο της ταυτότητας σε δίκτυα υποστήριξης ασθενών.

Σε τρεις πωλητές, αποκτήθηκαν καθαρές τιμές κειμένου. Ως αποτέλεσμα, ένας εισβολέας έχει τη δυνατότητα να χρησιμοποιήσει τα διαπιστευτήρια για έλεγχο ταυτότητας στο δίκτυο υποστήριξης ασθενών. Παρόμοια με τα σκληρά κωδικοποιημένα διαπιστευτήρια, τα σκληρά κωδικοποιημένα δεδομένα υποδομής χρησιμοποιούνται συχνά σε επικοινωνίες. Τα σκληρά κωδικοποιημένα δεδομένα υποδομής εφαρμόστηκαν σε συσκευές παρακολούθησης από το σπίτι για τη διευκόλυνση της επικοινωνίας με τα δίκτυα υποστήριξης των ασθενών. Τα δεδομένα υποδομής περιλάμβαναν αριθμούς τηλεφώνου και διευθύνσεις IP που αντιστοιχούν σε διακομιστές ελέγχου ταυτότητας για το δίκτυο υποστήριξης ασθενών. Ως αποτέλεσμα, ένας επιτιθέμενος έχει τη δυνατότητα εντοπισμού των διακομιστών ελέγχου ταυτότητας για το δίκτυο υποστήριξης ασθενών.

3.6.10 Ενεργοποίηση ραδιοσυχνοτήτων (RF)

Η ενεργοποίηση RF χρησιμοποιείται για την ενεργοποίηση του κυκλώματος εμφυτεύσιμης καρδιακής συσκευής για τη μετάδοση δεδομένων στη συσκευή παρακολούθησης από το σπίτι. Οι συσκευές οικιακής παρακολούθησης έχουν τη δυνατότητα να ξεκινήσουν επικοινωνίες για να επικαλεστούν πτυχές της ενεργοποίησης RF για δεδομένα θεραπείας ασθενών. Ως αποτέλεσμα, εάν δεν υπάρχουν άλλοι έλεγχοι ασφαλείας, ένας εισβολέας έχει το δυνατότητα αποστολής επαναλαμβανόμενων σημάτων ενεργοποίησης RF στην εμφυτεύσιμη καρδιακή συσκευή με την πιθανότητα να αδειάσει η μπαταρία με ταχύτερο ρυθμό.

3.6.11 Απομακρυσμένη ενημέρωση υλικολογισμικού

Οι συσκευές παρακολούθησης από το σπίτι λαμβάνουν ενημερώσεις υλικολογισμικού μέσω του δικτύου υποστήριξης ασθενών. Οι συσκευές οικιακής παρακολούθησης, ωστόσο, δεν επικυρώνουν απαραίτητα την πηγή του συστήματος διανομής του υλικολογισμικού. Ως αποτέλεσμα, υπάρχει η δυνατότητα να πραγματοποιηθεί μια επίθεση και να εκδοθεί πλαστό υλικολογισμικό σε μια συσκευή οικιακής παρακολούθησης.

3.6.12 Ψηφιακά υπογεγραμμένο υλικολογισμικό

Το ψηφιακά υπογεγραμμένο υλικολογισμικό διασφαλίζει ότι μια συσκευή θα εκτελεί μόνο εξουσιοδοτημένο υλικολογισμικό, ακόμη και αν λαμβάνεται από μη εξουσιοδοτημένη οντότητα. Ψηφιακά υπογεγραμμένο υλικολογισμικό, ωστόσο, δεν εφαρμόστηκε για υποσυστήματα εντός του οικοσυστήματος της εμφυτεύσιμης καρδιακής συσκευής. Ως αποτέλεσμα, υπάρχει η δυνατότητα φόρτωσης και εκτέλεσης πλαστών υλικολογισμικών σε μια συσκευή οικιακής παρακολούθησης.

3.6.13 Αφαιρούμενα μέσα/σκληροί δίσκοι

Οι προγραμματιστές γιατροί χρησιμοποιούν αφαιρούμενα μέσα/σκληρούς δίσκους. Ως αποτέλεσμα, ένας επιτιθέμενος έχει τη δυνατότητα να προσαρτήσει το αφαιρούμενο μέσο και να εξαγάγει ολόκληρο το σύστημα αρχείων για τους προγραμματιστές γιατρούς.

3.6.14 Κρυπτογράφηση

Η κρυπτογράφηση συστήματος αρχείων αποτρέπει τη μη εξουσιοδοτημένη ανάγνωση των δεδομένων του υποσυστήματος. Ωστόσο, οι εφαρμογές στερούνται κρυπτογράφησης του συστήματος αρχείων για τους προγραμματιστές γιατρούς. Ως αποτέλεσμα, μετά την

εξαγωγή του συστήματος αρχείων, ένας εισβολέας έχει τη δυνατότητα να διαβάσει το σύστημα αρχείων.

3.6.15 Μη κρυπτογραφημένα δεδομένα ασθενών

Εκτός από ένα μη κρυπτογραφημένο σύστημα αρχείων, η ανάλυση αποκάλυψε ότι δύο προμηθευτές δεν κάνουν κρυπτογράφηση των δεδομένων των ασθενών που είναι αποθηκευμένα στους σκληρούς δίσκους του προγραμματιστή. Για έναν προμηθευτή, τα δεδομένα των ασθενών εντοπίστηκαν στον προγραμματιστή που αποκτήθηκε μέσω της ιστοσελίδας δημόσιων δημοπρασιών. Τα δεδομένα ασθενών περιλάμβαναν ονόματα ασθενών, ιατρούς, αριθμούς τηλεφώνου, αριθμούς κοινωνικής ασφάλισης και δεδομένα θεραπείας. Αυτές οι πληροφορίες αναφέρθηκαν σε ξεχωριστή έκθεση προς αρμόδιους κρατικούς φορείς.

3.6.16 Αυθεντικοποίηση για τη διενέργεια προγραμματισμού

Οι προγραμματιστές γιατροί δεν απαιτούν έλεγχο ταυτότητας (π.χ. όνομα χρήστη/κωδικό πρόσβασης) για τον προγραμματισμό εμφυτεύσιμων καρδιακών συσκευών. Ως αποτέλεσμα, η πρόσβαση σε προγραμματιστή γιατρό παρέχει τη δυνατότητα προγραμματισμού οποιασδήποτε υποστηριζόμενης εμφυτεύσιμης καρδιακής συσκευής. Αυτή η διαπίστωση επαληθεύεται εύκολα ενεργοποιώντας οποιονδήποτε από τους τέσσερις προγραμματιστές γιατρούς. Μόλις ενεργοποιηθεί, το λειτουργικό σύστημα του προγραμματιστή γιατρού είναι φορτωμένο και ο τελικός χρήστης μπορεί εύκολα να εκτελέσει λειτουργίες προγραμματιστή ιατρού.

3.6.17 Εφαρμογές προγραμματισμού ιατρών

Οι προγραμματιστές γιατροί περιέχουν ξεχωριστή εφαρμογή προγραμματισμού για κάθε συγκεκριμένη εμφυτεύσιμη καρδιακή συσκευή. Ως αποτέλεσμα, εάν υλοποιηθεί μια ενημέρωση/έλεγχος ασφαλείας για μια συγκεκριμένη εφαρμογή, θα πρέπει επίσης να επαληθευτεί και να ενημερωθεί για όλες τις άλλες εφαρμογές στους προγραμματιστές γιατρούς. Εάν δεν εφαρμόζεται σε κάθε εφαρμογή εμφυτεύσιμης καρδιακής συσκευής στον προγραμματιστή ιατρό, τότε η ενημέρωση/έλεγχος είναι αποτελεσματική μόνο για την εμφυτεύσιμη καρδιακή συσκευή που σχετίζεται με την εφαρμογή στην οποία εφαρμόζεται η ενημέρωση/έλεγχος ασφαλείας.

3.6.18 Διπλή χρήση ραδιοεξοπλισμού για συσκευή οικιακής παρακολούθησης και προγραμματιστή ιατρών

Οι προγραμματιστές ιατροί χρησιμοποιούν ενσωματωμένο ραδιοκύκλωμα για τη μετάδοση σημάτων προς την εμφυτεύσιμη καρδιακή συσκευή. Η ανάλυση αποκάλυψε ότι το ίδιο υλικό που χρησιμοποιείται στους προγραμματιστές ιατρών χρησιμοποιήθηκε σε αντίστοιχες συσκευές παρακολούθησης από το σπίτι. Ως αποτέλεσμα, ενδέχεται να υπάρχει η δυνατότητα αξιοποίησης της συσκευής παρακολούθησης από το σπίτι για την εκτέλεση των ίδιων λειτουργιών προγραμματισμού με τον προγραμματιστή ιατρό.

3.6.19 Λευκή λίστα εντολών

Η λίστα επιτρεπόμενων εντολών διασφαλίζει ότι μια εμφυτεύσιμη καρδιακή συσκευή επεξεργάζεται μόνο εξουσιοδοτημένες λειτουργίες προγραμματισμού. Διαμόρφωση της εμφυτεύσιμης καρδιακής συσκευής μόνο για να δέχεται εξουσιοδοτημένες λειτουργίες προγραμματισμού μέσω εγκατεστημένης συνεδρίας τηλεμετρίας με ένα προγραμματιστή ιατρού ελαχιστοποιεί τον κίνδυνο ενός εισβολέα να χρησιμοποιεί προσαρμοσμένο υλικό ή να εκμεταλλευτεί τη συσκευή παρακολούθησης από το σπίτι για να προγραμματίσει κακόβουλα την εμφυτεύσιμη συσκευή καρδιάς. Η ανάλυση αποκάλυψε ότι οι εμφυτεύσιμες καρδιακές συσκευές στερούνται την εφαρμογή των εντολών λευκής λίστας. Ως αποτέλεσμα, ένας επιτιθέμενος μπορεί να έχει τη δυνατότητα να παραποιήσει εντολές προγραμματισμού στην εμφυτεύσιμη καρδιακή συσκευή χρησιμοποιώντας προσαρμοσμένο υλικό.

3.6.20 Παγκόσμιο διακριτικό ελέγχου ταυτότητας

Εντοπίστηκαν μόνιμα σημεία ελέγχου ταυτότητας που επέτρεπαν τη σύζευξη οποιασδήποτε υποστηριζόμενης συσκευής παρακολούθησης στο σπίτι με μια εμφυτεύσιμη καρδιακή συσκευή. Κατά συνέπεια, εάν άλλοι έλεγχοι ασφαλείας δεν εφαρμόζονται, ένας εισβολέας μπορεί να έχει τη δυνατότητα να χρησιμοποιήσει το καθολικό διακριτικό ελέγχου ταυτότητας για να παραποιήσει μια συνεδρία με μια εμφυτεύσιμη καρδιακή συσκευή.

3.7 ΣΥΝΟΨΗ ΤΩΝ ΕΥΡΗΜΑΤΩΝ

Στον παρακάτω πίνακα 5 καταδεικνύονται τα πιθανά ζητήματα ασφάλειας που σχετίζονται με την αρχιτεκτονική του οικοσυστήματος της εμφυτεύσιμης καρδιακής συσκευής. Ο πίνακας 5 δείχνει τις αναγνωρισμένες ανησυχίες για την ασφάλεια που αντιστοιχούν στους αξιολογημένους προμηθευτές. Οι περιοχές που εντοπίστηκαν

επισημαίνουν τα θεμελιώδη χαρακτηριστικά της αρχιτεκτονικής του συστήματος που ενδέχεται να δημιουργήσουν ανησυχίες για την ασφάλεια σε όλους τους προμηθευτές.

	Vendor One	Vendor Two	Vendor Three	Vendor Four
Obtainability of vendor subsystems	Verified	Verified	Verified	Verified
Commercial-off-the shelf microprocessors	Verified	Verified	Verified	Verified
Debugging interfaces (JTAG/UART)	Verified	Verified	Verified	Verified
Lack of packed, obfuscated or encrypted firmware	Verified	Verified	Verified	Verified
Use of ASCII text function names	Verified	Verified	Verified	Verified
Presence of software debugging attributes	Verified	Verified	Verified	Verified
Use of third-party libraries	Verified	Verified	Verified	Verified
Lack of protected memory mapping	Verified	Verified	Verified	Verified
External USB connections that allow system-level communications	Verified	Verified	Verified	Not Identified
Hardcoded credentials	Verified	Verified	Verified	Not Identified
Hardcoded infrastructure data (e.g., dial-in phone numbers, IP addresses, server names)	Verified	Verified	Verified	Verified
RF Activation	Verified	Verified	Verified	Verified
Remote firmware update capability	Verified	Verified	Verified	Not Identified
Lack of digitally signed firmware	Verified	Verified	Verified	Verified
Removable media/hard-drive	Verified	Verified	Verified	Verified
Lack of file system encryption	Verified	Verified	Verified	Verified
Storage of unencrypted patient data	Not Identified	Verified	Verified	Not Identified
Lack of authentication to physician programmer prior to conducting implantable cardiac device programming	Verified	Verified	Verified	Verified
Use of individual applications on the physician programmer for each implantable cardiac device	Verified	Verified	Verified	Verified

Πίνακας 5: Ζητήματα ασφάλειας για τους 4 προμηθευτές (Rios and J. Butts, 2017)

Τα ευρήματα αποκαλύπτουν συνοχή σε όλους τους προμηθευτές, τονίζοντας τις αδυναμίες στην αρχιτεκτονική του οικοσυστήματος. Είναι σημαντικό να σημειωθεί ότι οι επιθέσεις που έχουν τη δυνατότητα να επηρεάσουν τη φροντίδα των ασθενών συχνά απαιτούν μια αλυσίδα ενεργειών που παρακάμπτουν πολλαπλούς ελέγχους/αδυναμίες ασφαλείας. Πράγματι, δεν είναι σύνηθες ότι μία αδυναμία ασφάλειας από μόνη της μπορεί να επηρεάσει τη φροντίδα των ασθενών. Για παράδειγμα, εισαγωγή πλαστού υλικολογισμικού για μια οικιακή συσκευή παρακολούθησης θα απαιτούσε από έναν εισβολέα να αποκτήσει το υλικολογισμικό, να ανακατασκευάσει το υλικολογισμικό, να εντοπίσει τη λειτουργικότητα εντός του κώδικα, για να τροποποίηση τον κώδικα με τρόπο που δημιουργεί το επιθυμητό αποτέλεσμα χωρίς να παραβιάζει άλλες λειτουργίες του υποσυστήματος, να επανασυσκευάσει το υλικολογισμικό και να διανείμει το υλικολογισμικό σε συσκευές παρακολούθησης από το σπίτι. Ως εκ τούτου, η αξιολόγηση των ελέγχων ασφαλείας από τους προμηθευτές θα πρέπει να είναι στο πλαίσιο των οφελών της φροντίδας των ασθενών και της ανάλυσης κινδύνου.

3.8 ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΕΛΕΓΧΩΝ ΑΣΦΑΛΕΙΑΣ

Οι έλεγχοι ασφαλείας σχετίζονται με διασφαλίσεις, ειδικά για τον προμηθευτή, που μετριάζουν τους κινδύνους σχετιζόμενους με εγγενείς αδυναμίες στην αρχιτεκτονική του

οικοσυστήματος και αλληλεξαρτήσεις εφαρμογής. Ο WhiteScope συνιστά στους προμηθευτές να εκτελούν μια αξιολόγηση των αντίστοιχων ελέγχων ασφαλείας τους ώστε να διασφαλιστεί η αξιόπιστη εφαρμογή τους. Στην εργασία των (Rios and Butts J., 2017) παρέχεται λίστα ερωτήσεων για να βοηθήσουν τους προμηθευτές στην αξιολόγηση των ελέγχων ασφαλείας έναντι της αναγνωρισμένης αρχιτεκτονικής και εφαρμογής των κινδύνων αλληλεξάρτησης.

3.9 ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο παρόν κεφάλαιο παρατίθενται τα ευρήματα από την ανάλυση που πραγματοποιήθηκε στην αρχιτεκτονική του οικοσυστήματος των συσκευών εμφυτεύσιμης καρδιάς. Αναφέρεται ότι, ο WhiteScope εντόπισε πιθανούς ευάλωτους τομείς για την αρχιτεκτονική των συστημάτων και χρησιμοποίησε συσκευές για την αξιολόγηση των εφαρμογών του συστήματος.

Τα ευρήματα αποκαλύπτουν ότι η εγγενής αρχιτεκτονική και οι αλληλεξαρτήσεις υλοποίησης είναι επιρρεπείς σε κινδύνους ασφάλειας που έχουν τη δυνατότητα να επηρεάσουν τη συνολική εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του οικοσυστήματος.

Τα ευρήματα φαίνεται ότι είναι σχετικώς κοινά σε όλους τους διαφορετικούς προμηθευτές, επισημαίνοντας τους την ανάγκη να διεξάγουν μια ολιστική σε βάθος αξιολόγηση των εφαρμοζόμενων ελέγχων ασφαλείας.

Δεδομένης της ομοιότητας των ευρημάτων σε διαφορετικούς προμηθευτές, ο προσδιορισμός τρωτών σημείων εφαρμογής σε οποιονδήποτε προμηθευτή μπορεί να εκθέσει τις ίδιες ευπάθειες σε άλλους προμηθευτές και πρέπει να εξεταστούν προσεκτικά πριν από τη δημοσιοποίηση.

Διασφαλίζοντας την εφαρμογή των κατάλληλων ελέγχων ασφαλείας, οι προμηθευτές μπορούν να συμβάλουν στην προστασία έναντι πιθανών συμβιβασμών του συστήματος που μπορεί να έχουν επιπτώσεις στη φροντίδα των ασθενών.

4. ΠΡΑΓΜΑΤΙΚΗ ΑΝΑΛΥΣΗ ΑΣΦΑΛΕΙΑΣ ΤΡΙΩΝ ΝΟΣΟΚΟΜΕΙΩΝ ΜΕ ΠΑΡΑΒΙΑΣΜΕΝΑ ΕΝΔΟΝΟΣΟΚΟΜΕΙΑΚΑ ΙΑΤΡΙΚΑ IOT ΣΥΣΤΗΜΑΤΑ

4.1 ΓΕΝΙΚΑ

Τον Μάιο του 2015 τα ερευνητικά εργαστήρια TrapX δημοσίευσαν μια έκθεση σχετικά με την ανακάλυψη και ανάλυση τριών στοχευμένων επιθέσεων σε νοσοκομεία. Η ομάδα των εργαστηρίων TrapX αναφέρθηκε σε αυτό το είδος επιθέσεων ως MEDJACK, ή "αεροπειρατεία ιατρικών συσκευών" (TrapX Investigative Report, 2016).

Στην πρώτη έκθεση τους τα εργαστήρια περιέγραψαν τον τρόπο με τον οποίο οι ιατρικές συσκευές έχουν γίνει βασικός στόχος για τους επιτιθέμενους στα δίκτυα υγειονομικής περίθαλψης. Οι ιατρικές συσκευές είναι ορατά σημεία ευπάθειας και ο πιο δύσκολος τομέας ασφάλειας και αποκατάστασης, ακόμη και μετά τον εντοπισμό μιας παραβίασης. Περιεγράφηκε πώς αυτές οι επίμονες κυβερνοεπιθέσεις απειλούν τις συνολικές λειτουργίες των νοσοκομείων και την ασφάλεια των δεδομένων των ασθενών. Επίσης έγινε περαιτέρω περιγραφή για το πώς γίνονται οι επιθέσεις και, αφού καθιερωθούν, πώς οι επιτιθέμενοι μπορούν να επεκτείνουν τα ερείσματά τους σε αυτά τα παραβιασμένα συστήματα για να παραβιάσουν δυνητικά τα αρχεία ασθενών για μεγάλο χρονικό διάστημα.

Η MEDJACK 2 είναι μια εξέλιξη της αρχικής επίθεσης MEDJACK βασισμένη σε πρωτογενή έρευνα που συγκεντρώθηκε από πρόσφατα περιστατικά τεκμηριωμένη στην πλατφόρμα ασφαλείας TrapX στα τέλη του 2015 και στις αρχές του 2016. Αυτή περιλάμβανε λεπτομερή ανασκόπηση των δεδομένων και σχετικών αναλύσεων με συνεχείς, προηγμένες επιθέσεις σε τρία νέα ιδρύματα υγειονομικής περίθαλψης. Αυτές οι επιθέσεις περιστρέφονταν γύρω από ιατρικές συσκευές που ήταν εγκατεστημένες στα ενσύρματα δίκτυα του νοσοκομείου.

Η MEDJACK 2 αποτελεί μια εξέλιξη των επιθέσεων που καταγράφηκε στην πρώτη έκθεση MEDJACK. Στα τρία νέα νοσοκομεία που μελετήθηκαν βρέθηκε ένα πλήθος από κερκόπορτες και συνδέσεις botnet[4], που λειτουργούσαν υπό τον έλεγχο των επιτιθέμενων.

Είναι εξαιρετικά σημαντικό να σημειωθεί ότι το κακόβουλο λογισμικό που διαδόθηκε από τον/τους επιτιθέμενο/ους δεν εντοπίστηκε ποτέ από κανένα λογισμικό ασφαλείας τελικού σημείου. Συχνά μπορούμε να βρούμε ειδοποιήσεις ασφαλείας τελικών σημείων κατά τη

[4] Ένα botnet είναι ένας αριθμός συσκευών συνδεδεμένων στο Διαδίκτυο, καθεμία από τις οποίες εκτελεί ένα ή περισσότερα bots. Τα botnets μπορούν να χρησιμοποιηθούν για την εκτέλεση επιθέσεων κατανεμημένης άρνησης υπηρεσίας (DDoS), την κλοπή δεδομένων, την αποστολή ανεπιθύμητων μηνυμάτων, και επιτρέπουν στον εισβολέα να έχει πρόσβαση στη συσκευή και τη σύνδεσή της

διάρκεια της δικανικής -εγκληματολογικής μιας έρευνας, αλλά αυτές δεν υπήρχαν στις εν λόγω μελέτες περίπτωσης.

Ένα μοναδικό εύρημα κατά τη διάρκεια της έρευνας ήταν ότι η επίθεση χρησιμοποιούσε μια παλιά παραλλαγή κακόβουλου λογισμικού, όπως μια παραλλαγή του ιού τύπου «σκουλήκι» (worm) MS08-067, της οποίας οι υπογραφές ήταν γνωστές. Τα Windows 7 και οι μεταγενέστερες εκδόσεις είχαν εξαλείψει τα τρωτά σημεία που προσπαθούσε να εκμεταλλευτεί αυτό το «σκουλήκι», έτσι ώστε φαινόταν να μην προκαλεί καμία ανησυχία - ακόμη και αν ανιχνευόταν από άλλες λύσεις ασφαλείας, αφού η συντριπτική πλειοψηφία των σταθμών εργασίας δεν ήταν ευάλωτοι.

Το κακόβουλο λογισμικό που χρησιμοποιήθηκε για αυτή την επίθεση επιλέχθηκε ειδικά για να εκμεταλλευτεί παλαιότερες εκδόσεις των Windows και δεδομένου ότι τα γενικά τελικά σημεία χρησιμοποιούσαν νεότερες εκδόσεις των Windows, δεν θα επηρεάζονταν από την απειλή. Το σημείο αυτό είναι κρίσιμο και εξυπηρετεί δύο κύριους στόχους:

1. Δεδομένου ότι οι νεότερες εκδόσεις των Windows δεν ήταν ευάλωτες, οι σταθμοί εργασίας θα αγνοούσαν την επίθεση, εξαλείφοντας την ανάγκη παρέμβασης οποιουδήποτε λογισμικού ασφαλείας τελικού σημείου. Αυτό εξασφάλιζε ότι ο ιός τύπου σκουλήκι (worm) θα περνούσε απαρατήρητος ενώ αναζητούσε παλαιότερα συστήματα Windows.

2. Τα ιατροτεχνολογικά προϊόντα που χρησιμοποιούνται σε αυτές τις μελέτες περίπτωσης χρησιμοποίησαν παλαιότερες εκδόσεις των Windows που εξακολουθούσαν να είναι ευάλωτες στην απειλή. Αυτό έδωσε στους επιτιθέμενους μεγαλύτερη πιθανότητα να συμβιβαστούν με αυτά τα συστήματα, και δεδομένου ότι οι περισσότερες ιατρικές συσκευές δεν διαθέτουν πρόσθετο λογισμικό ασφαλείας τερματικού σημείου, η επίθεση θα παρέμενε απαρατήρητη.

Προκειμένου να εξασφαλιστεί η επιτυχία, φαίνεται ότι οι επιτιθέμενοι σκόπιμα επανασυσκεύασαν και ενσωμάτωσαν νέα, εξαιρετικά εξελιγμένα εργαλεία και τα καμουφλάρανε μέσα στο «σκουλήκι» MS08-067.

Όταν οι εισβολείς βρέθηκαν μέσα στο δίκτυο, πολλές ιατρικές συσκευές έγιναν εύκολοι στόχοι, από τους οποίους θα μπορούσαν να ξεκινήσουν την καμπάνια τους. Με βάση την εγκληματολογία από αυτές τις περιπτωσιολογικές μελέτες και άλλες, συμπεραίνουμε ότι οι επιτιθέμενοι με τη MEDJACK 2 κινούνται σκόπιμα σε παλιές παραλλαγές των φορέων επίθεσης για να στοχεύσουν ειδικά τις ιατρικές συσκευές γνωρίζοντας ότι δεν έχουν επιπλέον προστασία ασφαλείας.

Από αυτές τις μελέτες περιπτώσεων γίνεται αντιληπτό ότι το κακόβουλο λογισμικό μπόρεσε να εδραιωθεί στα παλαιότερα λειτουργικά συστήματα των ιατρικών συσκευών και να αποφύγει οποιαδήποτε ανίχνευση στα τυπικά τελικά σημεία πληροφορικής ή στις

λύσεις δικτύου. Αυτό επέτρεψε στον επιτιθέμενο να εγκαταστήσει μια κερκόπορτα εντός της επιχείρησης, από την οποία θα μπορούσε να ξεκινήσει την εκστρατεία του και να εξαφανίσει αθόρυβα δεδομένα και ίσως να προκαλέσει σημαντική ζημιά χρησιμοποιώντας μια επίθεση ransomware[5].

Στα τρία νοσοκομεία που επιλέχθηκαν για τις μελέτες περιπτώσεων MEDJACK 2, εγκαταστάθηκε η τεχνολογία TrapX, η οποία επέτρεψε στο να ανακαλυφθούν αυτές οι επιθέσεις μέσα σε μια χρονική περίοδο η οποία κυμαινόταν, λίγο λιγότερο από μία ώρα (μελέτη περίπτωσης #3) έως λίγες ημέρες (μελέτη περίπτωσης #1 και #2). Χρησιμοποιήθηκαν πλήρεις ιατροδικαστικές τεχνικές για να γίνει κατανοητή και να τεκμηριωθεί η αλυσίδα της επίθεσης, να προσδιοριστούν οι τοποθεσίες και οι απειλές της πηγής των εισβολέων, όπου ήταν δυνατόν, και στη συνέχεια να βοηθηθεί ο πελάτης να εξαλείψει τις απειλές και να επιστρέψει στην κανονική λειτουργία.

Τα παρακάτω συστήματα ήταν η πηγή της έντονης δραστηριότητας των επιτιθέμενων:

Νοσοκομείο #1:

Προμηθευτής Α - Σύστημα Ακτινοβολίας Ογκολογίας

Προμηθευτής Α - Σύστημα Linac

Προμηθευτής Β - Ακτινολογικό σύστημα Φλουροσκόπησης (Flouroscopy)

Νοσοκομείο #2:

Προμηθευτής Γ - Σύστημα αρχειοθέτησης εικόνων και επικοινωνίας (picture archive and communication systems) - PACS

Νοσοκομείο #3:

Προμηθευτής Δ - Ακτινογραφία

Παρακάτω παρουσιάζονται συνοπτικά συμπεράσματα και συστάσεις για την ελαχιστοποίηση του κινδύνου που σχετίζεται με μια επίθεση MEDJACK καθώς και την πιο εξελιγμένη επίθεση MEDJACK 2. Παρουσιάζονται ιδέες για τις βέλτιστες πρακτικές σχεδιασμού, υλοποίησης και διαχείρισης ζωής του συστήματος δικτυωμένων ιατρικών συσκευών και των δικτύων υγειονομικής περίθαλψης. Το συμπέρασμα αυτής της έκθεσης ήταν, ότι η συντριπτική πλειοψηφία των ιατρικών συσκευών που βρίσκονται σε ιατρικές

[5] Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που απειλεί να δημοσιεύσει τα προσωπικά δεδομένα του εκάστοτε θύματος ή να εμποδίσει συνεχώς την πρόσβαση σε αυτά, εκτός αν καταβληθούν λύτρα.

εγκαταστάσεις είναι ευάλωτες σε επιθέσεις στον κυβερνοχώρο. Αυτό παραμένει μια σοβαρή κατάσταση, και μια κατάσταση που συνεχίζει να απαιτεί άμεση προσοχή και αποκατάσταση.

4.2 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ - ΝΟΣΟΚΟΜΕΙΟ #1

Προμηθευτής Α - Σύστημα ακτινοβολίας ογκολογίας
Προμηθευτής Α - Σύστημα Linac
Προμηθευτής Β - Ακτινολογικό σύστημα Flouroscopy

4.2.1 *Επισκόπηση*

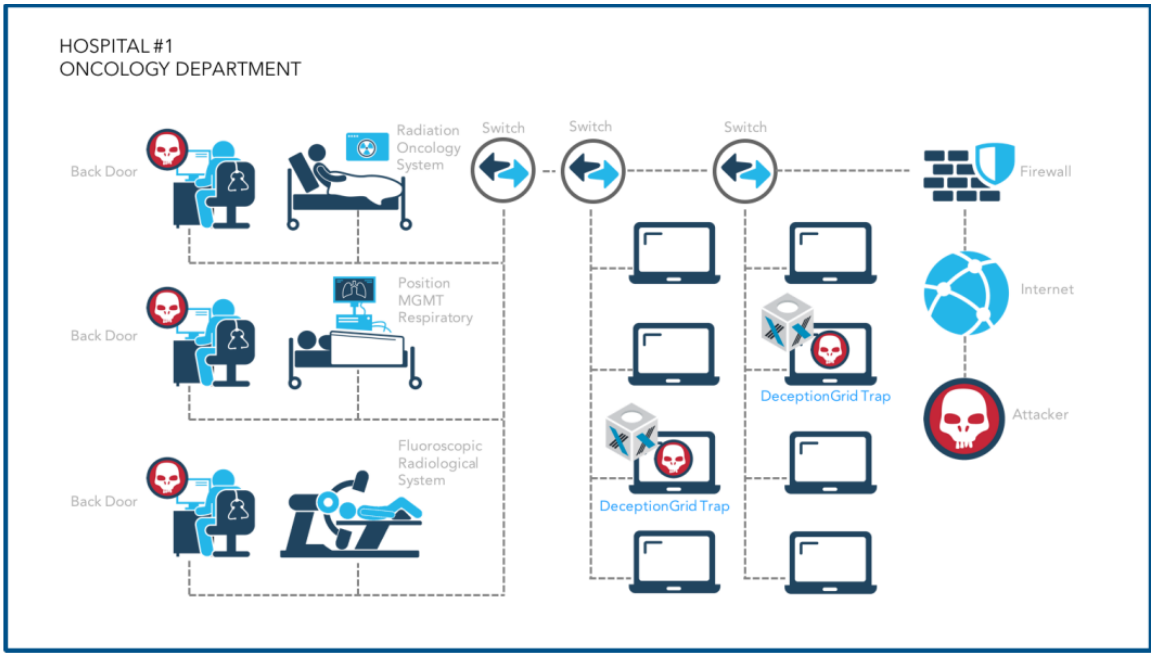
Το συγκεκριμένο νοσοκομείο ήταν μέσα στα 1000 κορυφαία νοσοκομεία παγκοσμίως που αξιολογούσε προηγμένες λύσεις ανίχνευσης απειλών. Είχε ιδιαίτερο ενδιαφέρον για την αξιολόγηση της τεχνολογίας εξαπάτησης και είχε ήδη εφαρμόσει μια τρέχουσα και καλά χρηματοδοτούμενη λύση άμυνας στον κυβερνοχώρο. Το λογισμικό ανίχνευσης εισβολών ήταν κεντρικοποιημένο στο δίκτυο και διέθετε ενημερωμένο λογισμικό προστασίας τελικού σημείου. Είχε ένα εταιρικό τείχος προστασίας νεότερης γενιάς και αρκετά πρόσθετα εσωτερικά τείχη προστασίας.

Οι απαιτήσεις συμμόρφωσης για αυτό το νοσοκομείο περιλάμβαναν την ασφάλιση υγείας και το Νόμο περί φορητότητας και λογοδοσίας (the Health Insurance and Portability and Accountability Act -HIPAA) και την παραβίαση και κοινοποίηση δεδομένων, τις απαιτήσεις διαφόρων κρατών στα οποία είχε εγκαταστάσεις. Ήταν εξαιρετικά ανήσυχοι σχετικά με τον δυνητικό κίνδυνο που προκαλείται στους ασθενείς τους από επιτιθέμενους στον κυβερνοχώρο, στα δεδομένα των ασθενών τους καθώς και στις συνεχιζόμενες δραστηριότητές τους.

Το νοσοκομείο διέθετε μια πολύ ισχυρή ομάδα επιχειρήσεων ασφαλείας. Επίσης είχε προηγουμένως προσλάβει και αρκετές ομάδες για δοκιμές διείσδυσης στο λογισμικό. Η ομάδα ασφάλειας του κέντρου επιχειρήσεων ήταν ξεχωριστή από την ομάδα πληροφορικής και αυτό έδωσε την δυνατότητα καλής εστίασης στη διατήρηση ενός ισχυρού περιβάλλοντος στον κυβερνοχώρο. Χρησιμοποιούσαν την τρέχουσα τεχνολογία τους σύμφωνα με τις βέλτιστες πρακτικές. Προηγούμενες δοκιμές διείσδυσης είχαν επισημάνει ανησυχίες και πιθανά προπύργια επιτιθέμενων εντός των ιατροτεχνολογικών τους συσκευών, αλλά δεν είχαν καμία τεχνολογία εσωτερικά που θα μπορούσε εύκολα να εντοπίσει τις εγκατεστημένες κερκόπορτες των επιτιθέμενων μέσα σε αυτές τις συσκευές.

4.2.2 Ανάπτυξη και Ανάλυση

Η τεχνολογία εξαπάτησης εγκαταστάθηκε σε όλα τα εσωτερικά δίκτυα. Η συγκεκριμένη εγκατάσταση χρησιμοποίησε τις προσομοιωμένες ιατρικές συσκευές. Αυτές οι προσομοιωμένες ιατρικές συσκευές σχεδιάστηκαν για να προσελκύσουν, να παγιδεύσουν και να μπλοκάρουν τα εργαλεία λογισμικού του επιτιθέμενου.



Σχήμα 3: Το τμήμα ογκολογίας του Νοσοκομείου και η λειτουργία του (TrapX Investigative Report, 2016)

Τη δεύτερη ημέρα η DeceptionGrid [6] ειδοποιήθηκε για τη δραστηριότητα του επιτιθέμενου. Ανακαλύφθηκε κακόβουλο λογισμικό να μετακινείται πλευρικά μέσα στο δίκτυο, και όταν βρήκε την προσομοιωμένη ιατρική συσκευή, εισήγαγε κακόβουλο κώδικα στην παγίδα κακόβουλου λογισμικού χρησιμοποιώντας μια τεχνική εκτέλεσης shellcode[7].

[6] Η τεχνολογία εξαπάτησης (deception technology) είναι μια κατηγορία άμυνας ασφάλειας στον κυβερνοχώρο. Τα προϊόντα τεχνολογίας εξαπάτησης μπορούν να ανιχνεύσουν, να αναλύσουν και να υπερασπιστούν ενάντια σε επιθέσεις μηδενικής ημέρας και προηγμένες επιθέσεις, συχνά σε πραγματικό χρόνο.

[7] Επισημαίνουμε ότι στο hacking, ένα shellcode είναι ένα μικρό κομμάτι κώδικα που χρησιμοποιείται ως ωφέλιμο φορτίο στην εκμετάλλευση μιας ευπάθειας λογισμικού. Ονομάζεται "shellcode" επειδή συνήθως ξεκινά ένα κέλυφος εντολών από το οποίο ο εισβολέας μπορεί να ελέγξει τη μηχανή που έχει παραβιαστεί. Επίσης, οποιοδήποτε κομμάτι κώδικα που εκτελεί παρόμοια εργασία μπορεί να ονομαστεί shellcode.

Η ανάλυση επέτρεψε να εντοπιστεί ο επιτιθέμενος μέσω του δικτύου σε μια κερκόπορτα μέσα στην πύλη PC. Πρόκειται για ένα σύστημα ακτινοβολίας στην ογκολογία που εκτελείται σε Windows XP. Το νοσοκομείο δεν είχε καμία προηγούμενη προειδοποίηση ή ένδειξη παραβίασης για το εν λόγω ιατροτεχνολογικό προϊόν.

Εντός τεσσάρων ημερών, δύο επιπλέον ιατρικές συσκευές (παγίδες) που στοχεύουν σε παραβίαση από τον επιτιθέμενο παρήγαγαν ειδοποιήσεις. Κακόβουλο λογισμικό εισήχθη και πάλι με την τεχνική shellcode. Το πιο ενδιαφέρον ήταν ότι αυτό το δίκτυο ήταν ξεχωριστό από εκείνο που σχετιζόταν με τον πρώτο συναγερμό. Έτρεχαν πολλά διαφορετικά προφίλ εξομοίωσης ιατρικών συσκευών και δεν ανιχνεύθηκε κάποια προτίμηση σε αυτή τη συγκεκριμένη επίθεση.

Η ανάλυση επέτρεψε τον εντοπισμό αυτού του επιτιθέμενου μέσω του δικτύου σε μια κερκόπορτα μέσα στο σταθμό εργασίας φθοριοσκοπίας που επίσης εκτελεί Windows XP.

Και τα δύο αυτά συστήματα είναι εξαιρετικά ευαίσθητα και εμπλέκονται στην παροχή κρίσιμων πληροφοριών για τη θεραπεία των ασθενών. Με βάση την ανάλυση που πραγματοποιήθηκε στο αρχικό MEDJACK, μόλις δημιουργηθεί μια κερκόπορτα σε μια ιατρική συσκευή, υπάρχει σημαντική δυνατότητα του επιτιθέμενου να χειραγωγήσει τη συσκευή, τη λειτουργία ή/και τις ενδείξεις της συσκευής και τα δεδομένα της. Πέρα από αυτό το ενδεχόμενο, δεν παρατηρήθηκε απολύτως καμία ένδειξη τέτοιων προθέσεων στην παρούσα μελέτη περίπτωσης και είναι προφανές ότι η όλη δραστηριότητα του επιτιθέμενου είχε ως στόχο την κλοπή των δεδομένων των ασθενών.

Τα εξελιγμένα εργαλεία του επιτιθέμενου ήταν καμουφλαρισμένα μέσα σε έναν ξεπερασμένο κώδικα MS08-067 που χρησιμοποιήθηκε για το αρχικό διάνυσμα διανομής. Το κακόβουλο λογισμικό ήταν στην πραγματικότητα αρκετά εξελιγμένο και ικανό να μετακινείται μεταξύ δικτύων με επιτυχία. Με βάση ένα επαναλαμβανόμενο μοτίβο, οι επιτιθέμενοι σκόπιμα ομαδοποιούν τα εργαλεία τους με τέτοιο τρόπο ώστε να στοχεύσουν σε παλαιότερα Windows XP ή Windows 7 λειτουργικά συστήματα που είναι αρκετά ευάλωτα και δεν διαθέτουν εγκατεστημένη κυβερνοάμυνα. Επιπλέον, το κάνουν αυτό εξαλείφοντας το ενδεχόμενο συναγερμού από τους τυπικούς σταθμούς εργασίας του νοσοκομείου που έχουν εγκαταστήσει ενημερωμένες κυβερνοάμυνες.

4.3 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ - ΝΟΣΟΚΟΜΕΙΟ #2

Προμηθευτής Γ - Σύστημα PACS
Εξυπηρετητές υπολογιστών πολλαπλών προμηθευτών και Μονάδες αποθήκευσης

4.3.1 Επισκόπηση

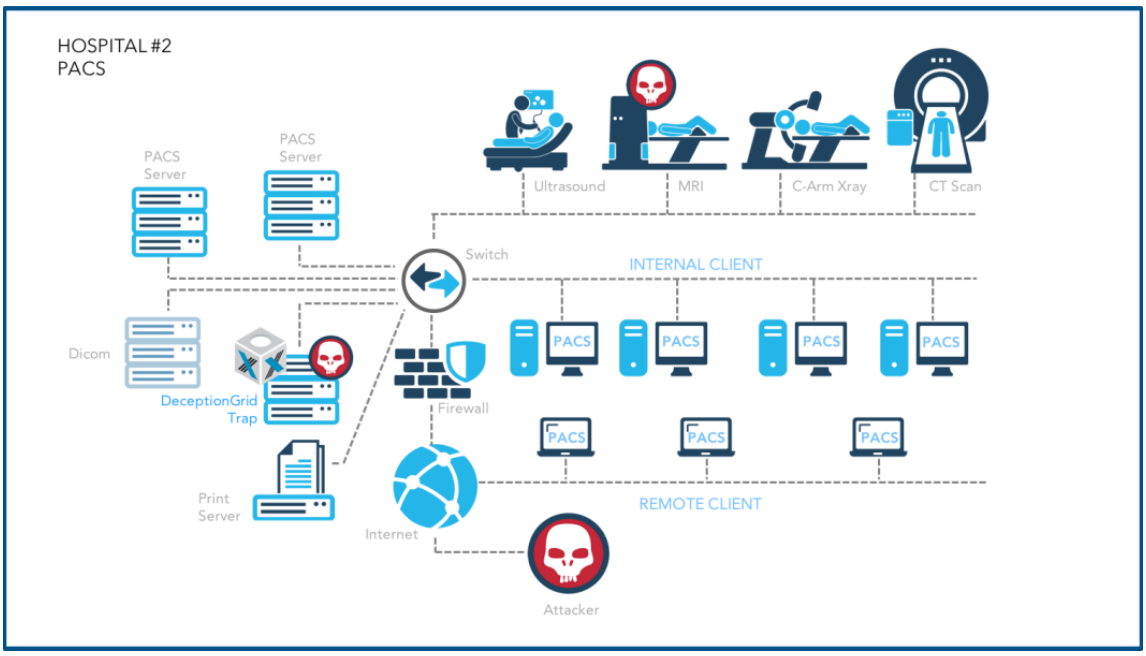
Το συγκεκριμένο νοσοκομείο ήταν μέσα στα 10.000 κορυφαία νοσοκομεία παγκοσμίως. Είχε ιδιαίτερο ενδιαφέρον για την αξιολόγηση της τεχνολογίας εξαπάτησης και της επιθυμητής αυτοματοποιημένης τεχνολογίας που δεν θα τοποθετούσε πρόσθετη επιβάρυνση ή φόρτο εργασίας για την ομάδα πληροφορικής του. Επίσης, στο Νοσοκομείο, είχαν ευαισθησία στον αντίκτυπο που θα είχαν στους υπάρχοντες προϋπολογισμούς τεχνολογίας πληροφοριών που ήταν υπό πίεση. Επιπλέον, είχε λογισμικό ανίχνευσης εισβολών, τείχη προστασίας και εσωτερικά τείχη προστασίας που χώριζαν το δίκτυο σε επιμέρους τμήματα, το καθένα με συγκεκριμένες πολιτικές. Τέλος, περιλάμβανε και μια ασφάλεια τελικού σημείου.

Αυτό το νοσοκομείο ήταν εξαιρετικά ανήσυχο για τον δυνητικό κίνδυνο που προκαλούν οι επιτιθέμενοι στον κυβερνοχώρο στους ασθενείς και στα δεδομένα των ασθενών τους. Είχαν εντοπίσει προηγούμενες προσπάθειες να κλαπούν δεδομένα ασθενών και δεν ήταν σίγουροι ότι είχαν εξαλείψει αυτές τις απειλές.

Το νοσοκομείο διέθετε μια μικρή ομάδα τεχνολογίας πληροφοριών, υπεύθυνη τόσο για τις τυποποιημένες τεχνολογίες υποστήριξης πληροφοριών όσο και για την ασφάλεια στον κυβερνοχώρο. Είχαν ένα σημαντικό ανεκτέλεστο υπόλοιπο εργασιών υποστήριξης για τους εσωτερικούς πελάτες τους και φαινόταν βαριά φορτωμένο και επιβαρυμένο από την ανάλυση ασφαλείας στον κυβερνοχώρο. Ήταν αρκετά αβέβαιοι ως προς το πώς θα μπορούσαν να αντισταθούν καλύτερα στο τρέχον κύμα των προηγμένων επιτιθέμενων.

4.3.2 ***Ανάπτυξη και Ανάλυση***

Το DeceptionGrid εγκαταστάθηκε σε όλα τα εσωτερικά δίκτυα και τους διακομιστές εντός των συστημάτων αρχειοθέτησης εικόνων και επικοινωνίας (picture archive and communication systems – PACS) που παρέχουν αποθήκευση και πρόσβαση σε εικόνες πληροφοριών από μηχανές πολλαπλών πηγών.



Σχήμα 4: Σύστημα πληροφορικής Νοσοκομείου περίπτωσης 2 (TrapX Investigative Report, 2016)

Πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στο PACS περιλαμβάνουν ψηφιακή απεικόνιση και επικοινωνίες στην Ιατρική (Digital Imaging and Communications in Medicine - DICOM), το οποίο είναι ένα πρότυπο για χειρισμό, αποθήκευση, εκτύπωση και διαβίβαση πληροφοριών σε εφαρμογές ιατρικής απεικόνισης. Το DICOM είναι ένα πρωτόκολλο εφαρμογής που χρησιμοποιεί TCP/IP[8] για την επικοινωνία μεταξύ των συστημάτων. Το DICOM χρησιμοποιείται κυρίως για να επιτρέπει σε δύο ή περισσότερες οντότητες που είναι σε θέση να λαμβάνουν δεδομένα εικόνας και ασθενούς σε μορφή DICOM. Το DICOM επίσης επιτρέπει την ενσωμάτωση σαρωτών, διακομιστών, σταθμούς εργασίας, εκτυπωτές και υλικό δικτύου από πολλούς κατασκευαστές σε ένα PACS σύστημα. Το DICOM χρησιμοποιείται κυρίως από νοσοκομεία, χειρουργικά κέντρα (surgi-centers), x-ray/ct-scan/εγκαταστάσεις μαγνητικής τομογραφίας, εγκαταστάσεις ειδικευμένης νοσηλείας, μεγάλα δίκτυα και φορείς γιατρών, και άλλα.

Οι μορφές αρχείων στα συστήματα PACS περιλαμβάνουν κυρίως DICOM (ψηφιακή απεικόνιση και επικοινωνίες στην ιατρική) και δεδομένα μη-εικόνας, όπως το PDF, το οποίο μπορεί να ενθυλακωθεί μέσα σε DICOM. Το σύστημα PACS περιελάμβανε φιλμ

[8] Το Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου (Transmission Control Protocol/Internet Protocol (TCP/IP), που αναφέρθηκε παραπάνω είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το διαδίκτυο_αλλά και μεγάλο ποσοστό των εμπορικών δικτύων

ακτίνων X, αξονική τομογραφία (CT) και απεικόνιση μαγνητικού συντονισμού (MRI) μαζί με τους απαραίτητους σταθμούς εργασίας, διακομιστές και αποθήκευση. Σχεδόν κάθε νοσοκομείο διαθέτει τουλάχιστον ένα κεντρικό σύστημα PACS. Εάν ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στο PACS, έχει δίκτυο προς κάθε άλλο πιθανό σύστημα στο νοσοκομείο καθώς και σε πολλές εξωτερικές οντότητες συνδεδεμένες στο δίκτυο.

Μέχρι τη δεύτερη ημέρα μια τεχνολογία τύπου DeceptionGrid PACS είχε ανακαλύψει κακόβουλο λογισμικό, επιτρέποντας να εντοπίζει την προέλευση και τις λεπτομέρειες της επίθεσης. Η προέλευση βρέθηκε να είναι μια συμβιβασμένη ιατρική συσκευή που βρίσκεται σε εντελώς διαφορετικό τμήμα του δικτύου. Το κακόβουλο λογισμικό σε αυτή την παραβιασμένη ιατρική συσκευή έμαθε πού βρίσκονται τα συστήματα PACS, εντοπίστηκαν και επιχείρησε να εκτελέσει επίθεση pass-the-hash [9] για να αποκτήσει πρόσβαση στα συστήματα PACS.

Ευτυχώς αυτή η επίθεση δεν ήταν επιτυχής στο πραγματικό σύστημα PACS, αλλά η παγίδα PACS δέχθηκε την επίθεση, δίνοντας στο κακόβουλο λογισμικό την εντύπωση ότι είχε επιτύχει. Μια pass-the-hash hacking τεχνική επιτρέπει σε έναν εισβολέα να πιστοποιήσει έναν απομακρυσμένο διακομιστή ή υπηρεσία χρησιμοποιώντας τον υποκείμενο κατακερματισμό NTLM (Microsoft NT Lan Manager) τους κωδικούς πρόσβασης ενός ή περισσότερων χρηστών αντί για κωδικούς πρόσβασης απλού κειμένου ως συνήθως απαιτείται. Αυτός ο τύπος επίθεσης είναι σπάνια επιτυχής σε συστήματα που απαιτούν πραγματικό έλεγχο ταυτότητας, αλλά η παγίδα (decoy PACS dydtem) επέτρεψε σε αυτή την επίθεση να πετύχει, συλλαμβάνοντας το κακόβουλο φορτίο, και παρέχοντας πρόσθετες λεπτομέρειες συμβιβασμού.

Η ανάλυση επέτρεψε να εντοπιστεί ο επιτιθέμενος μέσω του δικτύου σε μια κερκόπορτα μέσα στο σύστημα MRI που ξεκίνησε την επίθεση στην παγίδα PACS. Το νοσοκομείο δεν είχε προηγούμενη προειδοποίηση ή ένδειξη συμβιβασμού για αυτό το ιατροτεχνολογικό προϊόν, ή ότι οι διακομιστές του συστήματος PACS δέχονταν επιθέσεις. Αυτή η κερκόπορτα περιλάμβανε ένα σύστημα διοίκησης και ελέγχου διακομιστή σε ένα εξωτερικό botnet.

Παρόλο που η επίθεση χρησιμοποίησε ένα ξεπερασμένο κώδικα τύπου wrapper, διαπιστώθηκε ότι ο κακόβουλος κώδικας ήταν στην πραγματικότητα αρκετά εξελιγμένος και ικανός να μετακινείτε μεταξύ των δικτύων. Το σχεδόν αβλαβές «σκουλήκι» (που αγνοείται από τα συστήματα Windows 7 με επιδιόρθωση, τα Windows 8 πλατφόρμες και σύγχρονα λειτουργικά συστήματα) εκμεταλλεύτηκε μια ευπάθεια στα Windows XP και σε

[9] Μια επίθεση Pass-the-Hash (PtH) είναι μια τεχνική με την οποία ένας εισβολέας συλλαμβάνει έναν κατακερματισμένο κωδικό πρόσβασης και στη συνέχεια απλά το μεταβιβάζει για έλεγχο ταυτότητας και ενδεχομένως έμμεση πρόσβαση σε άλλα δικτυωμένα συστήματα.

εκδόσεις χωρίς patch των windows 7 φορτώνοντας ένα RAT (εργαλείο απομακρυσμένης πρόσβασης) ώστε ο επιτιθέμενος να μπορεί στη συνέχεια να φορτώσει εξαρτήματα εξελιγμένου λογισμικού επίθεσης.

Όπως και στη μελέτη περίπτωσης #1, πιστεύουμε ότι οι επιτιθέμενοι προετοιμάζουν σκόπιμα τα εργαλεία τους με τέτοιο τρόπο ώστε να στοχεύουν ιατρικές συσκευές με παλαιότερα Windows XP, ή έκδοση χωρίς patch του λειτουργικού συστήματος Windows 7, τα οποία είναι αρκετά ευάλωτα και δεν έχουν εγκατεστημένη άμυνα τελικού σημείου. Όπως και πριν, οι επιτιθέμενοι το κάνουν αυτό για να εξαλείψουν την πιθανή ανίχνευση σε επίπεδο λειτουργικού συστήματος από τυποποιημένους νοσοκομειακούς σταθμούς εργασίας (τελικά σημεία) και διακομιστές που διαθέτουν ενημερωμένο λειτουργικό σύστημα καθώς και εγκατεστημένες άμυνες στον κυβερνοχώρο.

Η συγκεκριμένη ιατρική συσκευή εγκαταστάθηκε εντός της επείγουσας περίθαλψης. Για να αποκατασταθεί η επίθεση χρειάστηκαν αρκετές εβδομάδες στο νοσοκομείο. Στο μεταξύ σταμάτησαν τη διεύθυνση πρωτοκόλλου διαδικτύου (IP) του επιτιθέμενου από τη συνέχιση της διοίκησης και τον έλεγχο της συσκευής. Η αποκατάσταση στην περίπτωση αυτή αποτελούταν από μια πρόσφατα κατασκευασμένη συσκευή και επιστρέφοντας την παραβιασμένη συσκευή πίσω στον κατασκευαστή.

4.4 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ - ΝΟΣΟΚΟΜΕΙΟ #3

Προμηθευτής D - Μηχανή ακτινών X

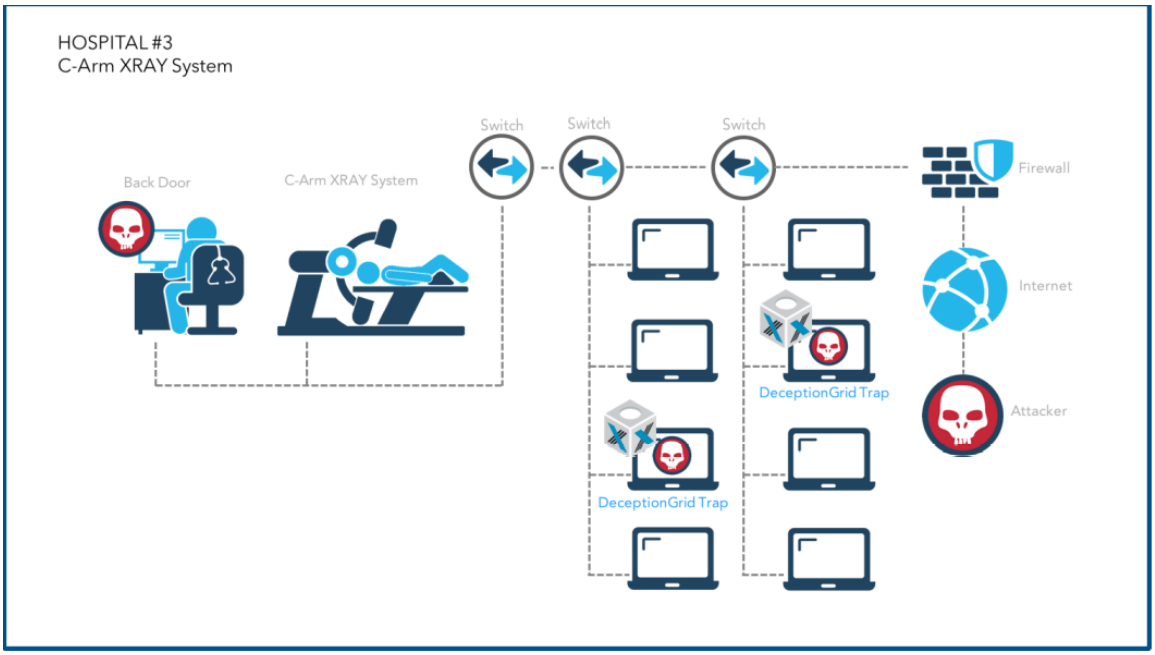
4.4.1 Επισκόπηση

Το συγκεκριμένο νοσοκομείο #3, ήταν επίσης μέσα στα 10.000 κορυφαία νοσοκομεία παγκοσμίως που αξιολογούσε προηγμένες λύσεις ανίχνευσης απειλών. Είχε ενδιαφέρον για την αξιολόγηση της τεχνολογίας εξαπάτησης και είχε ήδη μια χρηματοδοτούμενη αρχιτεκτονική άμυνας στον κυβερνοχώρο. Είχε σύστημα ανίχνευσης εισβολών, τείχη προστασίας και τερματικά σημεία ασφάλειας σε ισχύ.

Το νοσοκομείο διέθετε μια μικρή αλλά ισχυρή ομάδα τεχνολογιών πληροφορικής και ασφάλειας. Είχε σημαντική εμπειρία στον τομέα της ασφάλειας στον κυβερνοχώρο στο παρελθόν και χρησιμοποιούσε την τρέχουσα τεχνολογία σύμφωνα με τις βέλτιστες πρακτικές. Δεν γνώριζε για την παρουσία επιτιθέμενου εντός των δικτύων τους.

4.4.2 Ανάπτυξη και Ανάλυση

Το DeceptionGrid εγκαταστάθηκε σε όλα τα εσωτερικά δίκτυα. Η συγκεκριμένη εγκατάσταση χρησιμοποίησε προσομοιωμένες ιατρικές συσκευές που έχουν σχεδιαστεί να παγιδεύουν και να εμπλέκουν τους επιτιθέμενους, καθώς και τα εργαλεία τους.



Σχήμα 5: Το σύστημα ακτινοσκόπησης C Arm του νοσοκομείου No3 (TrapX Investigative Report, 2016)

Μέσα σε 20 λεπτά το DeceptionGrid ειδοποίησε για πλευρική κίνηση του επιτιθέμενου. Το κακόβουλο λογισμικό μετακινείται πλευρικά μέσα στο δίκτυο και όταν συναντά την προσομοιωμένη ιατρική συσκευή, την προσβάλλει με κακόβουλο λογισμικό.

Η ανάλυση μας επέτρεψε να εντοπίσουμε τον επιτιθέμενο πίσω μέσω του δικτύου σε μια κερκόπορτα μέσα στο εξοπλισμό ακτινών Χ που αποτελούσε εφαρμογή με βάση τα Windows NT 4.0. Το νοσοκομείο δεν είχε προηγούμενη ειδοποίηση ή ένδειξη συμβιβασμού για τη συγκεκριμένη ιατρική συσκευή.

Όπως και στην πρώτη περίπτωση μελέτης, το κακόβουλο λογισμικό ήταν τυλιγμένο μέσα σε ένα παρωχημένο περιτύλιγμα κακόβουλου λογισμικού που αρχικά αναγνωρίστηκε ως networm. Διαπιστώθηκε, για άλλη μια φορά, ότι αυτή η τεχνική καμουφλάριζε μια πολύ πιο εξελιγμένη και στοχευμένη επίθεση

4.5 ΚΑΤΑΝΟΗΣΗ ΤΟΥ MEDJACK.2

Τα εργαλεία έχουν εξελιχθεί για να βοηθήσουν στην κάλυψη παλαιών, εύκολα ανιχνεύσιμων απειλών κακόβουλου λογισμικού ως νέο κακόβουλο λογισμικό μέσω μιας τεχνικής που ονομάζεται επανασυσκευασία. Η πρώτη έκθεση για το MEDJACK στις αρχές του 2015 σημείωσε ότι πολύ βασικές εκδόσεις παλαιού κακόβουλου λογισμικού, όπως το CONFICKER, χρησιμοποιήθηκαν για τη διάδοση της επίθεσης λόγω της ευπάθειας των παλιών ενσωματωμένων λειτουργικών συστημάτων σε ιατρικές συσκευές. Αυτό ήταν παλιό κακόβουλο λογισμικό με παλιές δυνατότητες, αλλά δεδομένου ότι δεν υπήρχε ασφάλεια τελικού σημείου εντός των ιατρικών συσκευών, οι επιθέσεις αυτές εξακολουθούσαν να προκαλούν προβλήματα.

Το MEDJACK.2 αναγνωρίζει ότι οι επιτιθέμενοι έχουν κινηθεί συνειδητά προς την περαιτέρω εκμετάλλευση των ιατρικών συσκευών. Αυτοί οι επιτιθέμενοι έχουν εντείνει τις δραστηριότητές τους και τώρα καμουφλάρουν πολύ εξελιγμένες επιθέσεις μέσα σε αυτά τα παλιά περιτυλίγματα κακόβουλου λογισμικού. Οι παλαιοί κώδικες τύπου wrapper παρακάμπτουν σύγχρονες λύσεις τελικών σημείων καθώς τα στοχευμένα τρωτά σημεία έχουν προ πολλού κλείσει στο επίπεδο του λειτουργικού συστήματος. Έτσι τώρα οι επιτιθέμενοι, χωρίς να δημιουργούν καμία ειδοποίηση, μπορούν να διανέμουν τις πιο εξελιγμένες εργαλειοθήκες τους και να καθιερώσουν κερκόπορτες σε μεγάλα ιδρύματα υγειονομικής περίθαλψης, εντελώς χωρίς προειδοποίηση ή συναγερμό. Επιτιθέμενοι έχουν επενδύσει σημαντική έρευνα και ανάπτυξη σε αυτά τα νέα εργαλεία. Αυτό το προηγμένο κακόβουλο λογισμικό μπορεί πλέον να μεταπηδά πλευρικά σε διάφορα δίκτυα και να εκμεταλλεύεται σχεδόν οποιαδήποτε πληροφορία εντός ενός ιδρύματος υγειονομικής περίθαλψης.

Όλα αυτά καθιστούν τα ιδρύματα υγειονομικής περίθαλψης πιο ευάλωτα. Αυτές οι εκμεταλλεύσεις έχουν τη ρίζα τους σε ιατρικές συσκευές και αποφεύγουν τα περισσότερα λογισμικά κυβερνοάμυνας για μεγάλα χρονικά διαστήματα.

4.6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα δεδομένα που είναι αποθηκευμένα στα δίκτυα υγειονομικής περίθαλψης παραμένουν πρωταρχικός στόχος για τους επιτιθέμενους σε παγκόσμια βάση. Πρόσφατα στοιχεία από την IBM® Security υποδηλώνουν ότι ο τομέας της υγειονομικής περίθαλψης καταλαμβάνει την πρωτιά στις επιθέσεις το 2015, έναντι των χρηματοπιστωτικών υπηρεσιών, οι οποίες ήταν πρώτες το 2014. Οι κινητήριες δυνάμεις για αυτό

περιλαμβάνουν την οικονομική ανταμοιβή και τη σχετική δυσκολία (ή ευκολία) με τις οποίες ένας επιτιθέμενος μπορεί να εκμεταλλευτεί επιτυχώς μια στοχευμένη επιχείρηση. Επίσης, υπάρχει σημαντικό κέρδος από την κλοπή των ιατρικών εγγραφών, οι οποίες έχουν από τις υψηλότερες τιμές στη μαύρη αγορά, που κυμαίνονται από 10 έως 20 δολάρια ανά φάκελο ασθενούς. Όπως ανακαλύφθηκε, τα ιατροτεχνολογικά προϊόντα δεν προστατεύονται καλά από τυποποιημένες πρακτικές άμυνας στον κυβερνοχώρο. Οι λύσεις άμυνας στον κυβερνοχώρο δεν μπορούν να υπερασπιστούν ούτε να αποκαταστήσουν αυτές τις συσκευές.

Οι προϋπολογισμοί άμυνας στον κυβερνοχώρο της υγειονομικής περίθαλψης παραμένουν υπό μεγάλη πίεση και γενικά δεν επαρκούν για να καλύψουν το επίπεδο των επενδύσεων από επιτιθέμενους με κίνητρο. Οι ομάδες άμυνας στον κυβερνοχώρο είναι συχνά οι ίδιες με τις ομάδες υποστήριξης της τεχνολογίας των πληροφοριών, έχοντας έτσι διπλό ρόλο και καθήκον. Είδαν βέβαια κάποιες αυξήσεις στον προϋπολογισμό για να αντιμετωπίσουν τρέχουσες απειλές στο περιβάλλον του κυβερνοχώρου, αλλά και πάλι αυτό δεν ήταν αρκετό για την αντιμετώπιση της πολυπλοκότητας των επιθέσεων.

Αυτές οι δομές κόστους δεν καλύπτουν επαρκώς τις δαπάνες που απαιτούνται για την κάλυψη των σημερινών απειλών στον κυβερνοχώρο.

Οι ομάδες υποστήριξης των κλινικών ιατρών και των διοικητικών τους επικεντρώνονται στη φροντίδα των ασθενών και προγραμματίζονται με ακρίβεια λεπτού κάθε μέρα. Αυτοί αναμένουν ότι οι δικτυακοί και υπολογιστικοί πόροι θα αποδώσουν και δεν θέλουν πραγματικά να συμμετέχουν σε θέματα όπως η ασφάλεια στον κυβερνοχώρο.

Η λειτουργία των γνωστών μολυσμένων συστημάτων συχνά συνεχίζεται για ημέρες μετά την ανακάλυψη της βάσης του επιτιθέμενου καθώς ο αντίκτυπος και ο κίνδυνος για τη φροντίδα των ασθενών ή την εγκατάσταση είναι μεγαλύτερος με τη λήψη αυτών εκτός σύνδεσης. Τα ιδρύματα υγειονομικής περίθαλψης εξαρτώνται από αυτές τις συσκευές σε 24ωρη βάση, 7 ημέρες την εβδομάδα.

Η παρουσία των ιατροτεχνολογικών προϊόντων στα δίκτυα υγειονομικής περίθαλψης δημιουργεί υψηλή ευπάθεια. Αυτές οι ιατρικές συσκευές καταστούν τα δίκτυα αυτά πολύ πιο ευάλωτα σε μια επιτυχημένη κυβερνοεπίθεση. Στις αρχές του 2015 και στα μέσα του 2016 το «παλιρροϊκό κύμα» των ιατρικών συσκευών με βάση τις επιθέσεις είναι εμφανές, ορατό και με σημαντική τάση.

Οι επιπτώσεις του MEDJACK.2 είναι σχεδόν εξουθενωτικές για τον διοικητή ενός νοσοκομείου, ή τα μέλη του διοικητικού συμβουλίου. Πρέπει να προχωρήσουν γρήγορα σε σημαντική αναβάθμιση όσον αφορά στον προϋπολογισμό για την ασφάλεια στον

κυβερνοχώρο, στο προσωπικό και σε εργολάβους όπως οι πάροχοι υπηρεσιών ασφάλειας (MSP/MSSP) προκειμένου να αντιμετωπιστεί αυτή η απειλή.

Είναι πιθανό ότι θα πρέπει να εντοπίζονται και να εξουδετερώνονται συνεχώς επιτιθέμενοι που προσπαθούν να διεισδύσουν στα δίκτυα σε τακτική βάση. Περαιτέρω, για αγορές όπως αυτή των Ηνωμένων Πολιτειών, όπου οι απαιτήσεις συμμόρφωσης με την HIPAA και τις κρατικές απαιτήσεις παραβίασης δεδομένων είναι σημαντικές, η αποτυχία λήψης αυτών των βημάτων μπορεί να υποβάλει ένα ίδρυμα υγειονομικής περίθαλψης σε σημαντικές νομικές κυρώσεις και συναφείς οικονομικούς κινδύνους.

Μόλις ένας επιτιθέμενος δημιουργήσει μια "κερκόπορτα" μέσα σε μια ιατρική συσκευή είναι πολύ δύσκολο να ανιχνευθεί και να αποκατασταθεί. Χρειάζεστε την πλήρη συνεργασία με τον κατασκευαστή της συσκευής. Η ομάδα ασφάλειας στον κυβερνοχώρο δεν μπορεί εύκολα να εντοπίσει κακόβουλο λογισμικό σε ένα σύστημα το οποίο δεν μπορεί να σαρώσει με το τυπικό λογισμικό κυβερνοάμυνας. Η ανίχνευση λογισμικού Botnet λειτουργεί καλύτερα εάν η εξωτερική IP διεύθυνση είναι γνωστό ότι χρησιμοποιείται από επιτιθέμενους. Πέρα από αυτό, μόνο πολύ λίγες επιλεγμένες τεχνολογίες, όπως η τεχνολογία εξαπάτησης, μπορούν να ανιχνεύσουν πλευρική μετακίνηση εντός ενός εσωτερικού δικτύου.

Ακόμη χειρότερα, χωρίς νέες βέλτιστες πρακτικές, ένα αποκαταστημένο, από επίθεση, ιατροτεχνολογικό προϊόν μπορεί να επαναμολύνεται μέσα σε λίγες ώρες από τον ίδιο ιό (σκουλήκι) ο οποίος διαδίδετε από άλλο ιατροτεχνολογικό προϊόν που βρίσκεται εντός του νοσοκομείου.

Συνοπτικά, λόγω της ευρείας διάδοσης του MEDJACK και του εξελιγμένου MEDJACK.2, η μόλυνση από κακόβουλο λογισμικό παραμένει ευρέως διαδεδομένη στα μεγάλα ιδρύματα υγειονομικής περίθαλψης παγκοσμίως. Αυτό περιλαμβάνει νοσοκομεία, πρακτικές γιατρών, ενώσεις ανεξάρτητων πρακτικών γιατρών, υπεύθυνους οργανισμούς περίθαλψης, οργανώσεις ασφάλισης υγειονομικής περίθαλψης, εγκαταστάσεις ειδικευμένης νοσηλείας, χειρουργικά κέντρα και άλλους συναφείς οργανισμούς.

Τα περισσότεροι ιδρύματα δεν μπορούν να ανιχνεύσουν αυτές τις επιθέσεις, μπορεί να αγνοούν την τρέχουσα παραβίαση δεδομένων ή έχουν ανεπαρκής στρατηγικές και χρηματοδότηση για να εντοπίζουν και να απομακρύνουν αυτούς τους επιτιθέμενους.

4.7 ΣΥΣΤΑΣΕΙΣ

Οι φορείς υγείας θα πρέπει να λάβουν υπόψη τους συγκεκριμένες συστάσεις:

Επανεξέταση των προϋπολογισμών και των πρωτοβουλιών για την άμυνα στον κυβερνοχώρο σε επίπεδο μονάδας ή οργανωτικού συμβουλίου. Πρόσκληση ενός ανεξάρτητου εμπειρογνώμονα για την ασφάλεια στον κυβερνοχώρο σε επίπεδο διοικητικού συμβουλίου ώστε να βοηθήσει στην κατανόηση των απαιτούμενων προϋπολογισμών, στα επίπεδα προσωπικού και στις βασικές δραστηριότητες. Εξέταση μια γρήγορης εναλλακτικής λύσης για να την πρόσληψη ενός παρόχου υπηρεσιών ασφάλειας με διαχείριση σε εξωτερική βάση για την ενίσχυση των τρεχουσών δυνατοτήτων άμυνας στον κυβερνοχώρο.

Τα μεγάλα ιδρύματα υγειονομικής περίθαλψης θα πρέπει να επιδιώξουν τις συμβουλές αρμόδιων συμβούλων HIPAA. Δεδομένου του υψηλού κινδύνου παραβίασης δεδομένων που αντιμετωπίζουν τα νοσοκομεία, συνιστάται να προσέλθουν σε εξωτερικούς συμβούλους για τον έλεγχο και την επανεξέταση των προγραμμάτων συμμόρφωσης HIPAA.

Αύξηση των προγραμμάτων εκπαίδευσης των εργαζομένων σχετικά με τη χρήση των συστημάτων τεχνολογίας πληροφοριών υγειονομικής περίθαλψης. Αυτά δεν πρέπει να χρησιμοποιούνται για προσωπικές επικοινωνίες. Το ηλεκτρονικό ταχυδρομείο τα συνημμένα αρχεία και οι σύνδεσμοι (URL) πρέπει να αντιμετωπίζονται με την απαραίτητη υποψία μέχρις αποδείξεως του αντιθέτου. Χρειάζεται μόνο ένα λάθος του υπαλλήλου για να αφήσει τα εργαλεία ενός επιτιθέμενου στην επιχείρηση.

Επανεξέταση των σχεδίων ανάκαμψης από καταστροφές και εξέταση πώς μπορεί να βελτιωθεί η ποιότητα της φροντίδας των ασθενών που επηρεάζονται σε περίπτωση που όλοι οι πόροι της τεχνολογίας πληροφοριών σας (βάσεις δεδομένων ασθενών, συστήματα προγραμματισμού, συστήματα EMR/EHR, συστήματα παραγγελίας διαγνωστικών εργαστηρίων) κατέρρευσαν ή τα δεδομένα είχαν κλειδωθεί εξαιτίας μιας επίθεσης ransomware.

4.8 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ -ΣΥΣΤΑΣΕΙΣ ΓΙΑ ΤΗΝ ΑΜΥΝΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ

Απομόνωση των ιατρικών συσκευών μέσα σε ένα ασφαλές δίκτυο και προστασία αυτού με ένα εσωτερικό τείχος προστασίας που θα επιτρέπει την πρόσβαση μόνο σε συγκεκριμένες υπηρεσίες και διευθύνσεις IP. Εάν είναι δυνατόν και πρακτικά, είναι χρήσιμη η πλήρης απομόνωση των ιατρικών συσκευών μέσα σε ένα δίκτυο που δεν είναι συνδεδεμένο με το εξωτερικό διαδίκτυο.

Εφαρμογή στρατηγικής για την επανεξέταση και την αποκατάσταση των υπαρχουσών ιατρικών συσκευών. Πολλά από αυτά είναι πιθανό να έχουν μολυνθεί και να δημιουργούν κίνδυνο για το ίδρυμα και τους ασθενείς.

Εφαρμογή στρατηγικής για την ταχεία ενσωμάτωση και ανάπτυξη διορθώσεων λογισμικού και υλικού που παρέχονται από τον κατασκευαστή στις ιατρικές συσκευές σας. Αυτά πρέπει να παρακολουθούνται και να ελέγχονται από την ανώτερη διοίκηση και τις ομάδες διασφάλισης ποιότητας.

Εφαρμογή στρατηγικής για την προμήθεια ιατροτεχνολογικών προϊόντων από οποιονδήποτε προμηθευτή μόνο μετά από επανεξέταση με τον κατασκευαστή που επικεντρώνεται στις διαδικασίες ασφαλείας στον κυβερνοχώρο. Διεξαγωγή τριμηνιαίων ανασκοπήσεων με όλους τους κατασκευαστές ιατρικών συσκευών.

Εφαρμογή στρατηγικής για ιατρικές συσκευές που βρίσκονται στο τέλος της ζωής τους. Πολλές ιατρικές συσκευές λειτουργούν για πολλά χρόνια, συχνά έναντι μακράς διάρκειας απόσβεσης στον κύκλο ζωής.

Χρειάζεται απόσυρση αυτών των συσκευών το συντομότερο δυνατό, εάν παρουσιάζουν παλαιότερες αρχιτεκτονικές και δεν έχουν βιώσιμη στρατηγική για την αντιμετώπιση προηγμένων κακόβουλων λογισμικών όπως το MEDJACK. Στη συνέχεια, χρειάζεται αντικατάσταση με νέες συσκευές οι οποίες έχουν την απαραίτητη προστασία από τους κατασκευαστές και μπορούν να συμμορφωθούν με τις απαιτήσεις.

Εφαρμογή στρατηγικής για την ενημέρωση των υφιστάμενων συμβολαίων πώλησης ιατρικών συσκευών για υποστήριξη, συντήρηση και ειδικά για αποκατάσταση κακόβουλου λογισμικού. Εάν αυτές οι νέες υπηρεσίες αυξήσουν τους λειτουργικούς προϋπολογισμούς, πιστεύουμε ότι η πρόσθετη δαπάνη είναι αναγκαία και συνετή. Οι κατασκευαστές ιατρικών συσκευών θα πρέπει να περιλαμβάνουν συγκεκριμένη γλώσσα σχετικά με την ανίχνευση, την αποκατάσταση και ανακαίνιση οποιουδήποτε ιατροτεχνολογικού προϊόντος πωλείται σε ιδρύματα υγειονομικής περίθαλψης τα οποία στη συνέχεια μπορεί να μολυνθούν από κακόβουλο λογισμικό. Οι κατασκευαστές πρέπει να έχουν μια τεκμηριωμένη διαδικασία δοκιμής για να διαπιστωθεί εάν η συσκευή έχει μολυνθεί, και ένα τεκμηριωμένο πρότυπο διαδικασίας αποκατάστασης όταν ένα κακόβουλο λογισμικό και οι κυβερνοεπιτιθέμενοι έχουν διεισδύσει στη συσκευή.

Διαχείριση της πρόσβασης σε ιατρικές συσκευές, ιδίως μέσω θυρών USB. Αποφύγετε να επιτρέψετε σε οποιαδήποτε ιατρική συσκευή να παρέχει θύρες USB για χρήση από το προσωπικό χωρίς πρόσθετη προστασία. Η χρήση νέων memory sticks φαντάζει ως μονόδρομος, διαφορετικά μια ιατρική συσκευή μπορεί να μολύνει άλλες παρόμοιες συσκευές.

Αξιολόγηση και προτίμηση των προμηθευτών ιατρικών συσκευών που χρησιμοποιούν τεχνικές, όπως το ψηφιακά υπογεγραμμένο λογισμικό και κρυπτογράφηση όλων των εσωτερικών δεδομένων με κωδικούς πρόσβασης τους οποίους μπορείτε να τροποποιήσετε και να επαναφέρετε. Η υπογραφή λογισμικού είναι μια μαθηματική τεχνική που χρησιμοποιείται για την επικύρωση της γνησιότητας του λογισμικού. Ορισμένες κατασκευασμένες ιατρικές συσκευές χρησιμοποιούν αυτή την τεχνική για να βοηθούν στην αποτροπή εκτέλεσης μη εξουσιοδοτημένου κώδικα. Η κρυπτογράφηση παρέχει ένα περιθώριο ασφαλείας σε περίπτωση διαρροής δεδομένων ή παραβίασης της συσκευής, τουλάχιστον για ένα χρονικό διάστημα.

Βελτίωση της ικανότητας του χειριστή, ακόμη και όταν μια συσκευή έχει επιλεγεί, ώστε να μπορεί να επιτρέπει στην ομάδα που ασχολείται με την ασφάλεια της πληροφορίας, την αξιολόγηση των προμηθευτών ανεξάρτητα από την αξιολόγηση του τμήματος προμηθειών της εταιρείας. Επιτρέψτε στις ομάδες πληροφορικής να εκτελούν αυστηρότερες δοκιμές ασφαλείας για να ανακαλύψουν τρωτά σημεία και να βοηθήσουν με τη διαχείριση των κατασκευαστών ιατρικών συσκευών. Να τους επιτραπεί να αντιταχθούν στην προμήθεια μια ιατρικής συσκευής που μπορεί να είναι εύκολος και απροστάτευτος στόχος για επιθέσεις τύπου MEDJACK.

Τέλος, η χρησιμοποίηση μιας τεχνολογίας σχεδιασμένης για τον εντοπισμό κακόβουλου λογισμικού και επίμονων φορέων επίθεσης που έχουν ήδη παρακάμψει τις κύριες άμυνες. Η τεχνολογία εξαπάτησης μπορεί να προσφέρει αυτό το πλεονέκτημα στην ομάδα του κέντρου επιχειρήσεων ασφαλείας.

5. ΕΠΙΘΕΣΕΙΣ ΣΤΟ ΕΞΥΠΝΟ ΔΙΚΤΥΟ ΜΕΤΑΦΟΡΑΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ ΤΗΣ ΟΥΚΡΑΝΙΑΣ

5.1 ΕΙΣΑΓΩΓΗ

Στις 23 Δεκεμβρίου 2015, η ουκρανική Kyivoblenergo, μια περιφερειακή εταιρεία διανομής ηλεκτρικής ενέργειας, ανέφερε διακοπές υπηρεσιών προς τους πελάτες της. Οι διακοπές λειτουργίας οφείλονταν στην παράνομη είσοδο τρίτου μέρους στον υπολογιστή της εταιρείας και στα συστήματα SCADA[10]: Ξεκινώντας περίπου στις 3:35 μ.μ. τοπική

[10] Ο όρος **SCADA** (supervisory control and data acquisition) περιγράφει μια κατηγορία συστημάτων βιομηχανικού αυτομάτου ελέγχου και τηλεμετρίας. Το χαρακτηριστικό των συστημάτων SCADA είναι ότι αποτελούνται από τοπικούς ελεγκτές, που ελέγχουν επί μέρους στοιχεία και μονάδες μιας εγκατάστασης, συνδεδεμένους σε ένα κεντρικό Master Station (Κύριο Σταθμό Εργασίας). Ο κεντρικός σταθμός εργασίας μπορεί κατόπιν να επικοινωνεί τα δεδομένα που συλλέγει από την εγκατάσταση σε ένα πλήθος από σταθμούς

ώρα, επτά υποσταθμοί 110 kV και 23 υποσταθμοί 35 kV ήταν αποσυνδεδεμένοι για τρεις ώρες. Μεταγενέστερες δηλώσεις ανέφεραν ότι η επίθεση στον κυβερνοχώρο επηρέασε επιπλέον τμήματα του δικτύου διανομής και ανάγκασε τους χειριστές να στραφούν σε χειροκίνητη λειτουργία (https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid), http://news.finance.ua/ua/news/-/366136/hakery-atakuvaly-prykarpattyaoblenergo-znestrumyvshy-polovynu-regionu-na-6godyn) Η εκδήλωση παρουσιάστηκε και αναλύθηκε από τα ουκρανικά μέσα ενημέρωσης, τα οποία πραγματοποίησαν συνεντεύξεις και διαπίστωσαν ότι ένας ξένος επιτιθέμενος ήλεγχε εξ αποστάσεως το σύστημα διαχείρισης διανομής SCADA (http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html). Οι διακοπές θεωρήθηκε αρχικά ότι επηρέασαν περίπου 80.000 πελάτες, με βάση την ενημέρωση των πελατών από την Kyivoblenergo. Ωστόσο, αργότερα αποκαλύφθηκε ότι τρεις διαφορετικές εταιρείες διανομής δέχθηκαν επίθεση, με αποτέλεσμα να προκληθούν αρκετές διακοπές που προκάλεσαν απώλεια ρεύματος σε περίπου 225.000 πελάτες σε διάφορες περιοχές (http://www.oe.if.ua/showarticle.php?id=3413, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01).

Αμέσως μετά την επίθεση, αξιωματούχοι της ουκρανικής κυβέρνησης ισχυρίστηκαν ότι οι διακοπές προκλήθηκαν από επίθεση στον κυβερνοχώρο και ότι οι ρωσικές υπηρεσίες ασφαλείας ήταν υπεύθυνες για τα περιστατικά (http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html). Μετά από αυτούς τους ισχυρισμούς, οι ερευνητές στην Ουκρανία, καθώς και ιδιωτικές εταιρείες και η κυβέρνηση των ΗΠΑ, πραγματοποίησαν αναλύσεις και προσέφεραν βοήθεια, ώστε να προσδιοριστεί η βασική αιτία της διακοπής (https://www.rbc.ua/rus/news/pravitelstva-ssha-ukrainy-rassmotryat-otchet-1454113214.htm). Τόσο η ομάδα της E-ISAC όσο και η ομάδα ICS της SANS συμμετείχαν σε διάφορες προσπάθειες και αναλύσεις σε σχέση με την υπόθεση αυτή από τις 25 Δεκεμβρίου 2015.

5.2 ΤΕΧΝΙΚΕΣ ΕΠΙΤΙΘΕΜΕΝΟΥ ΚΑΙ ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ

Η άμεση απόδοση της επίθεσης δεν είναι απαραίτητη ώστε να μάθουμε από αυτή. Παραπέρα για να εξετάσουμε στρατηγικές μετριασμού είναι απαραίτητο να χρησιμοποιηθεί το νοητικό μοντέλο του τρόπου λειτουργίας του κυβερνοπαράγοντα για την κατανόηση των δυνατοτήτων και των γενικών προφίλ κατά του οποίου αμύνεται

εργασίας σε τοπικό LAN ή και να μεταδίδει τα δεδομένα της εγκατάστασης σε μακρινά σημεία μέσω κάποιου συστήματος τηλεπικοινωνίας, π.χ. μέσω του ενσύρματου τηλεφωνικού δικτύου ή μέσω κάποιου ασύρματου δικτύου.

κανείς. Το κίνητρο και η πολυπλοκότητα αυτής της επίθεσης στο ηλεκτρικό δίκτυο συνάδει με έναν εξαιρετικά δομημένο και εξοπλισμένο φορέα. Ο δράστης της συγκεκριμένης επίθεσης ήταν προσαρμοστικός και επέδειξε ποικίλες τακτικές και τεχνικές για να ταιριάζουν με τις άμυνες και το περιβάλλον των τριών στόχων που έχουν πληγεί. Το παρόν έγγραφο παρέχει έννοιες μετριασμού που σχετίζονται με την επίθεση και τον τρόπο ανάπτυξης μιας πιο μόνιμης στρατηγικής μετριασμού με την πρόβλεψη μελλοντικών επιθέσεων.

Ικανότητα επιτιθέμενου

Οι επιτιθέμενοι επέδειξαν μια ποικιλία δυνατοτήτων, όπως spear phishing [11] emails, παραλλαγές του κακόβουλου λογισμικού BlackEnergy 3, καθώς και χειραγώγηση εγγράφων του Microsoft Office που περιείχαν το κακόβουλο λογισμικό για να αποκτήσουν έρεισμα στα δίκτυα πληροφορικής (ΤΠ) των εταιρειών ηλεκτρικής ενέργειας, (https://www.sans.org/webcasts/analysis-sandworm-team-ukraine-101597) για να αποκτήσουν ερείσματα και να συλλέξουν διαπιστευτήρια και πληροφορίες και τέλος για να αποκτήσουν πρόσβαση στο δίκτυο των βιομηχανικών συστημάτων ελέγχου-ICS (Industrial Control System). Επιπλέον, οι επιτιθέμενοι έδειξαν εξειδίκευση, όχι μόνο στις υποδομές που συνδέονται με το δίκτυο, όπως τα συστήματα αδιάλειπτης τροφοδοσίας (UPS), αλλά και στη λειτουργία των ICS μέσω του συστήματος εποπτικού ελέγχου, όπως και η αλληλεπίδραση ανθρώπου μηχανής - Human Machine Interface (HMI).

Τέλος, οι αντίπαλοι απέδειξαν την ικανότητα και την προθυμία να στοχεύουν συσκευές πεδίου σε υποσταθμούς, να γράφουν προσαρμοσμένο κακόβουλο υλικολογισμικό και να καθιστούν τις συσκευές, όπως μετατροπείς σειριακού δικτύου σε Ethernet, μη λειτουργικές και μη ανακτήσιμες (http://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046F F6BA00FE8E8A4D857F3.app1?art id=24508688 6&cat id=35109). Σε μια περίπτωση, οι επιτιθέμενοι χρησιμοποίησαν επίσης τηλεφωνικά συστήματα για να δημιουργήσουν χιλιάδες κλήσεις στο τηλεφωνικό κέντρο της εταιρείας ενέργειας, ώστε να αρνείται την πρόσβαση σε πελάτες που αναφέρουν διακοπές. Ωστόσο, η ισχυρότερη ικανότητα των επιτιθέμενων δεν ήταν στην επιλογή των εργαλείων τους ή στην τεχνογνωσία τους, αλλά στην ικανότητά τους να εκτελούν μακροχρόνιες επιχειρήσεις αναγνώρισης που απαιτούνται για την εκμάθηση του περιβάλλοντος και την εκτέλεση μιας εξαιρετικά συγχρονισμένης, πολλαπλών σταδίων επιχείρησης επίθεσης.

[11] Το **phishing** είναι ένας τύπος κοινωνικής μηχανικής όπου ένας εισβολέας στέλνει ένα δόλιο (π.χ. πλαστό, ψεύτικο ή με άλλο τρόπο παραπλανητικό) μήνυμα που έχει σχεδιαστεί για να εξαπατήσει ένα ανθρώπινο θύμα να αποκαλύψει ευαίσθητες πληροφορίες στον εισβολέα ή να αναπτύξει κακόβουλο λογισμικό στην υποδομή του θύματος όπως ransomware.

Ακολουθεί συγκεντρωτικός κατάλογος των τεχνικών στοιχείων που χρησιμοποιήθηκαν από τους επιτιθέμενους, ο οποίος απεικονίζεται γραφικά στο Σχήμα 6:

-Spear phishing για την απόκτηση πρόσβασης στα επιχειρηματικά δίκτυα του διανομέα ηλεκτρικής ενέργειας

-Προσδιορισμός του λογισμικού BlackEnergy 3 σε κάθε μία από τις επηρεαζόμενες μονάδες παραγωγής ενέργειας

-Κλοπή διαπιστευτηρίων από τα δίκτυα των επιχειρήσεων

-Η χρήση εικονικών ιδιωτικών δικτύων (VPN) για την είσοδο στο δίκτυο ICS

-Η χρήση υφιστάμενων εργαλείων απομακρυσμένης πρόσβασης στο περιβάλλον ή η έκδοση εντολών απευθείας από ένα απομακρυσμένο σταθμό παρόμοιο με HMI χειριστή

-Συσκευές επικοινωνίας σειριακής επικοινωνίας με Ethernet που επηρεάζονται σε επίπεδο υλικολογισμικού (https://www.digitalbond.com/blog/2015/10/30/basecamp-for-serial-converters/)

-Η χρήση ενός τροποποιημένου KillDisk για τη διαγραφή της κύριας εγγραφής εκκίνησης των επηρεαζόμενων συστημάτων του οργανισμού, καθώς και η στοχευμένη διαγραφή ορισμένων αρχείων καταγραφής (http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-mediaorganization)

-Χρήση συστημάτων UPS για τον αντίκτυπο στο συνδεδεμένο φορτίο με προγραμματισμένη διακοπή της υπηρεσίας

-Τηλεφωνική επίθεση άρνησης παροχής υπηρεσιών στο τηλεφωνικό κέντρο

Σχήμα 6 : Ενοποιημένα τεχνικά στοιχεία της επίθεσης στην Ουκρανία (E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016)

Σε διάφορα σημεία της δημόσιας αναφοράς σχετικά με την επίθεση, οργανισμοί ανέφεραν ότι το λογισμικό BlackEnergy 3 και το λογισμικό KillDisk θα μπορούσε να είναι άμεσα υπεύθυνα για τη διακοπή της λειτουργίας. Ένα από τα στοιχεία που επισημάνθηκαν ειδικά για να υποστηριχθεί αυτή η θεωρία ήταν ότι το λογισμικό KillDisk διέγραψε μια διεργασία σε συστήματα Windows που συνδέεται με σειριακή-to-ethernet επικοινωνία (http://www.eset.com/int/about/press/articles/malware/article/eset-finds-connection-between-cyber-espionage-and-electricityoutage-in-ukraine/). Ανεξάρτητα από τον αντίκτυπο του περιβάλλοντος του δικτύου SCADA, ούτε το BlackEnergy 3 ούτε το KillDisk περιείχαν τα απαιτούμενα συστατικά για την πρόκληση της διακοπής λειτουργίας. Οι διακοπές προκλήθηκαν από τη χρήση των συστημάτων ελέγχου και το λογισμικό τους, μέσω άμεσης αλληλεπίδρασης από τον αντίπαλο. Όλα τα άλλα εργαλεία και η τεχνολογία, όπως το BlackEnergy 3 και το KillDisk, χρησιμοποιήθηκαν για να επιτρέψουν την επίθεση ή να καθυστερήσουν τις προσπάθειες αποκατάστασης.

Ευκαιρίες επιτιθέμενου

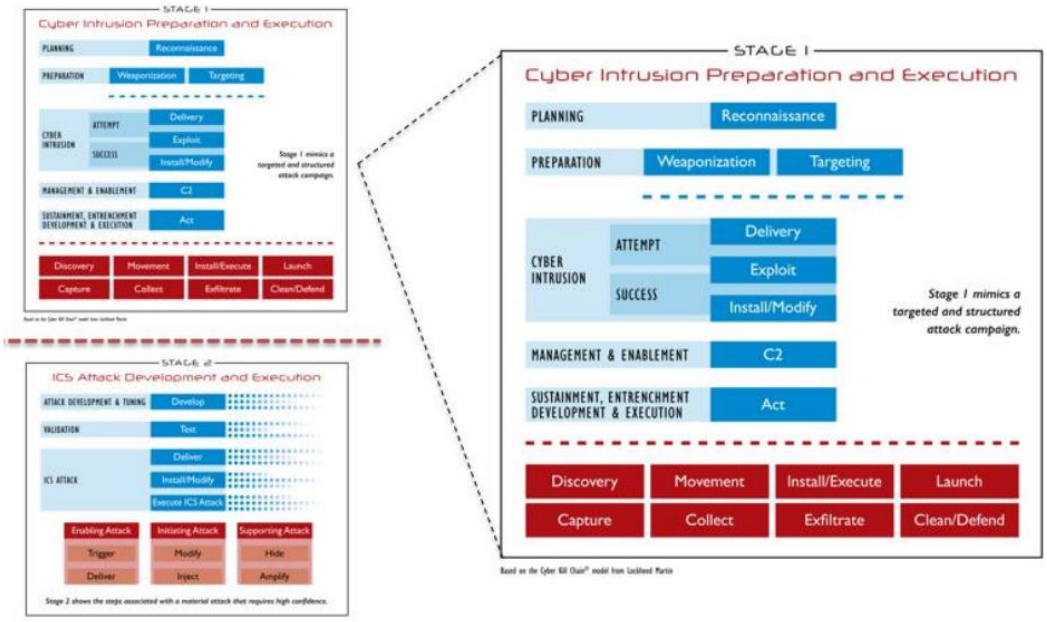
Υπήρχαν πολλαπλές ευκαιρίες για τον αντίπαλο να εκτελέσει την επίθεσή του. Εξωτερικά των εταιρειών διανομής ηλεκτρικής ενέργειας και πριν από την επίθεση, υπήρχε μια πλειάδα πληροφοριών ανοικτού κώδικα, όπως ένας λεπτομερής κατάλογος των τύπων των υποδομών, όπως οι προμηθευτές απομακρυσμένων τερματικών μονάδων και οι εκδόσεις που δημοσιεύονται στο διαδίκτυο από τους προμηθευτές ICS (http://galcomcomp.com/index.php/ru/nashi-proekty/15-proekt3-material-ru). Τα VPN στο ICS από το επιχειρησιακό δίκτυο φαίνεται να μην διαθέτουν έλεγχο ταυτότητας δύο παραγόντων. Επιπλέον, το τείχος προστασίας επέτρεψε στον αντίπαλο να κάνει απομακρυσμένη διαχείριση από το περιβάλλον, χρησιμοποιώντας μια δυνατότητα απομακρυσμένης πρόσβασης που είναι εγγενής στα συστήματα. Επιπλέον, με βάση τις αναφορές των μέσων ενημέρωσης, δεν φαινόταν να υπάρχει η δυνατότητα των κατοίκων να παρακολουθούν συνεχώς το δίκτυο και να αναζητούν ανωμαλίες και απειλές μέσω ενεργητικών μέτρων άμυνας, όπως η παρακολούθηση της ασφάλειας του δικτύου. Αυτά τα τρωτά σημεία παρείχαν στον αντίπαλο την ευκαιρία να παραμείνει στο περιβάλλον για έξι μήνες ή περισσότερο για να διεξάγει αναγνώριση του περιβάλλοντος και στη συνέχεια να εκτελέσει την επίθεση. (http://mobile.reuters.com/article/idUSKCN0VL18E).Με βάση τις λεπτομέρειες που παρέχονται στην έκθεση του DHS, ο αντίπαλος χρησιμοποίησε μια συνεπή προσέγγιση επίθεσης και στους τρεις επηρεαζόμενους στόχους. Ο αντίπαλος χρησιμοποίησε επίσης συνεπείς τακτικές για να επηρεάσει τα ελεγχόμενα στοιχεία του πεδίου και να προκαλέσει ανεπανόρθωτη βλάβη στις συσκευές πεδίου.

Ο λόγος για τον οποίο στοχοποιήθηκαν αυτοί οι διανομείς ηλεκτρικής ενέργειας παραμένει μια ανοιχτή συζήτηση. Με βάση τις δημόσιες αναφορές, είναι άγνωστο αν οι στόχοι επιλέχθηκαν με βάση τις κοινές τεχνολογίες που χρησιμοποιούνται, τις αρχιτεκτονικές των συστημάτων, την αναγνώριση δραστηριοτήτων ή τις περιοχές παροχής υπηρεσιών. Οι εκτιμήσεις για την επιλογή ενός συγκεκριμένου στόχου με βάση τις ευκαιρίες μπορούν να επικεντρωθούν στην αυτοπεποίθηση και την ικανότητα ενός επιτιθέμενου να προκαλέσει επιπτώσεις στο ICS. Ορισμένοι παράγοντες απόφασης θα μπορούσαν να περιλαμβάνουν:

- Στόχοι με κοινά συστήματα και διαμορφώσεις
- Πολλαπλά συστήματα με κοινά κεντρικά σημεία ελέγχου
- Εκτιμήσεις διάρκειας επιπτώσεων ICS (π.χ. μακροπρόθεσμες ή βραχυπρόθεσμες)
- Υπάρχουσες ικανότητες που απαιτούνται για την επίτευξη των επιθυμητών αποτελεσμάτων
- Επίπεδο κινδύνου για να εκτελεστεί η πράξη και να αποκαλυφθεί
- Επίτευξη πρόσβασης και ικανότητα κίνησης και δράσης μέσα στο περιβάλλον του ICS

5.3 ΧΑΡΤΟΓΡΑΦΗΣΗ ΤΗΣ ΑΛΥΣΙΔΑΣ ΚΥΒΕΡΝΟ-ΘΑΝΑΤΟΥ (ICS CYBER KILL CHAIN)

Το ICS Cyber Kill Chain δημοσιεύθηκε από την SANS το 2015 από τους Michael Assante και Robert M. Lee ως προσαρμογή της παραδοσιακής αλυσίδας θανάτου στον κυβερνοχώρο που ανέπτυξαν οι αναλυτές της Lockheed Martin, όπως αυτή εφαρμόζεται στα ICS. Η αλυσίδα θανάτου στον κυβερνοχώρο ICS περιγράφει λεπτομερώς τα βήματα που πρέπει να ακολουθήσει ένας αντίπαλος για να πραγματοποιήσει μια επίθεση υψηλής εμπιστοσύνης στη διαδικασία ή/και στο ICS, προκαλώντας φυσική βλάβη στον εξοπλισμό με προβλέψιμο και ελεγχόμενο τρόπο, όπως φαίνεται στο Σχήμα 7.



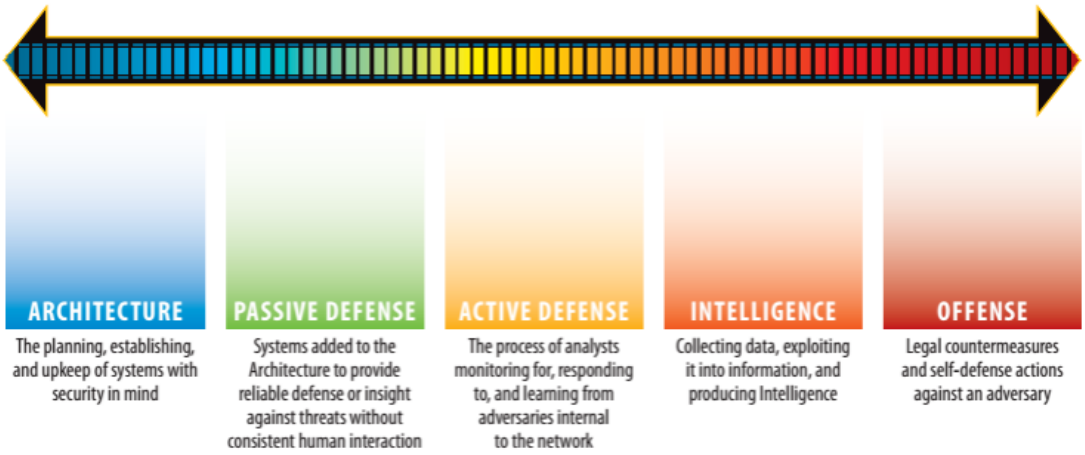
Σχήμα 7: Βήματα για την πραγματοποίηση μιας επίθεσης υψηλής εμπιστοσύνης (E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016)

Περισσότερα στοιχεία ο αναγνώστης θα βρει στην αναφορά: E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016

5.4 ΜΑΘΗΜΑΤΑ ΑΜΥΝΑΣ - ΠΑΘΗΤΙΚΗ ΚΑΙ ΕΝΕΡΓΗΤΙΚΗ ΑΜΥΝΑ

Εξετάστηκαν οι στρατηγικές μετριασμού που παρέχονται μέσω του DHS(Department of Homeland Security's) ICS-CERT Alert(Industrial Control Systems Cyber Emergency Response Team) και εξετάστηκε πώς ο αντίπαλος μπορεί να τροποποιήσει την επόμενη επίθεση με

βάση το μετριασμό που έχει λάβει ο στόχος. Υποστηρίχθηκαν πολλές από τις συστάσεις μετριασμού που έχουν δοθεί μέχρι σήμερα. Ωστόσο, ο αντίπαλος είναι πιθανό να τροποποιήσει την προσέγγιση της επίθεσης σε επόμενες εκστρατείες και αυτές οι στρατηγικές μετριασμού μπορεί να μην είναι επαρκείς. Στην ακόλουθη ενότητα, συζητούνται οι ενέργειες μετριασμού για την επίθεση που πραγματοποιήθηκε για να αντληθούν διδάγματα άμυνας. Επιπλέον, αναλύονται πιθανές μελλοντικές μεθοδολογίες επιτιθέμενων και δίνονται συστάσεις που θα μπορούσαν να διαταράξουν παρόμοιες επιχειρήσεις του αντιπάλου. Τα μέτρα μετριασμού θα επικεντρωθούν σε συστάσεις για την αρχιτεκτονική, την παθητική άμυνα και τις μεθοδολογίες ενεργητικής άμυνας κατά μήκος της κλίμακας ολίσθησης της ασφάλειας στον κυβερνοχώρο, που παρουσιάζεται στο Σχήμα 8 (https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240).



Σχήμα 8: Η ολισθαίνουσα κλίμακα της ασφάλειας στον κυβερνοχώρο (E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016)

5.4.1 Το φαινόμενο του Spear Phishing

Επίθεση στην Ουκρανία

Στην επίθεση, ο αντίπαλος παρέδωσε ένα στοχευμένο μήνυμα ηλεκτρονικού ταχυδρομείου με ένα κακόβουλο συνημμένο που φαινόταν να προέρχεται από μια αξιόπιστη πηγή σε συγκεκριμένα άτομα εντός των οργανισμών. Οι αρχικές συστάσεις μετριασμού θα επικεντρωθούν στην εκπαίδευση ευαισθητοποίησης των τελικών χρηστών και στις συνεχείς δοκιμές phishing. Συχνά γίνονται προσπάθειες για την πρόληψη κακόβουλου λογισμικού από την προτεινόμενη λευκή λίστα εφαρμογών, η οποία μπορεί να είναι αποτελεσματική σε περιβάλλοντα ICS, εάν ο προμηθευτής ICS εγκρίνει την χρήση. Ωστόσο, με βάση τις λεπτομέρειες αυτής της επίθεσης, η λευκή λίστα εφαρμογών θα είχε

περιορισμένο ρόλο ο οποίος θα περιλάμβανε την εκτέλεση των αρχικών μολύνσεων με dropper σε τμήματα δικτύου με μολυσμένους σταθμούς εργασίας (π.χ. χρήστες που έλαβαν και ενεργοποίησαν μολυσμένα spear phish μηνύματα ηλεκτρονικού ταχυδρομείου), όπου η λευκή λίστα εφαρμογών μπορεί να είναι πιο δύσκολο να εφαρμοστεί. Είναι σημαντικό να σημειωθεί ότι η λευκή λίστα εφαρμογών δεν θα είχε αποτρέψει τις επιθέσεις ICS του δεύτερου σταδίου που έπληξαν τις ουκρανικές εταιρείες διανομής ηλεκτρικής ενέργειας. Σε μία τουλάχιστον περίπτωση, ο επιτιθέμενος χρησιμοποίησε έναν απομακρυσμένο αμφίβολης ποιότητας πελάτη και ενέκρινε λειτουργίες απομακρυσμένου διαχειριστή σε επίπεδο λειτουργικού συστήματος για άλλα στοιχεία της επίθεσης.

Η επόμενη επίθεση του οργανισμού μέσω μεγάλης κλίμακας εκστρατειών phishing, χρησιμοποιώντας επιθέσεις water-holing[12] ή διεξάγοντας καμπάνιες άμεσης κλήσης προς τους χρήστες ή το γραφείο βοήθειας. Θα μπορούσαν επίσης να αξιοποιήσουν τεχνικές εκμετάλλευσης που δεν απαιτούν κοινωνική μηχανική του προσωπικού.

Ευκαιρίες για διατάραξη

Ο αντίπαλος είναι πιθανό να τροποποιήσει τις επιθέσεις για να ανταποκριθεί στις αυξήσεις ή στις αλλαγές στις άμυνες του στόχου. Υπερασπιστές χρειάζεται να αναπτύξουν προληπτικές αντιδράσεις στις επιπτώσεις των επιθέσεων. Δεδομένου ότι τα στοιχεία κοινωνικής μηχανικής των επιθέσεων στοχεύουν στο ηλεκτρονικό ταχυδρομείο και στα διαδικτυακά προσβάσιμα περιουσιακά στοιχεία στον κυβερνοχώρο, τα εν λόγω περιουσιακά στοιχεία και τα δίκτυα στα οποία βρίσκονται είναι αναξιόπιστα. Η επικοινωνία με αυτές τις αναξιόπιστες περιοχές θα πρέπει να τμηματοποιείται, να παρακολουθείται και να ελέγχεται. Λειτουργήστε με την παραδοχή ότι το περιβάλλον είναι προσβάσιμο από τον αντίπαλο και εξασφαλίστε ότι υπάρχουν οι κατάλληλες άμυνες για την προστασία των λειτουργιών και του περιβάλλοντος ελέγχου από τα ελεγχόμενα από τον αντίπαλο επιχειρησιακά περιουσιακά στοιχεία στον κυβερνοχώρο (ενώ ορισμένοι οργανισμοί εμπιστεύονται εγγενώς τα επιχειρησιακά τους συστήματα και δίκτυα, είναι αναγκαία η πρόσθετη επιβολή και ο έλεγχος αυτών των συστημάτων). Εξετάστε τη χρήση της τεχνολογίας sandboxing[13] για την αξιολόγηση των εγγράφων και των μηνυμάτων ηλεκτρονικού ταχυδρομείου που εισέρχονται στο δίκτυο, χρησιμοποιώντας συστήματα

[12] Water-holing είναι μια στρατηγική επίθεσης υπολογιστή στην οποία ένας εισβολέας μαντεύει ή παρατηρεί ποιους ιστότοπους χρησιμοποιεί συχνά ένας οργανισμός και μολύνει έναν ή περισσότερους από αυτούς με κακόβουλο λογισμικό. Τελικά, κάποιο μέλος της στοχευμένης ομάδας θα μολυνθεί. Οι αμυχές που αναζητούν συγκεκριμένες πληροφορίες μπορούν να επιτεθούν μόνο σε χρήστες που προέρχονται από μια συγκεκριμένη διεύθυνση IP. Αυτό καθιστά επίσης τα hacks δυσκολότερα στον εντοπισμό και την έρευνα.

[13] Το sandboxing είναι ένας όρος ασφάλειας υπολογιστών που αναφέρεται σε ένα πρόγραμμα που βρίσκεται εκτός από άλλα προγράμματα σε ένα ξεχωριστό περιβάλλον, έτσι ώστε εάν προκύψουν σφάλματα ή ζητήματα ασφάλειας, αυτά τα θέματα δεν θα εξαπλωθούν σε άλλες περιοχές του υπολογιστή. Τα προγράμματα είναι ενεργοποιημένα στη δική τους περιοχή απομόνωσης, όπου μπορούν να εργαστούν χωρίς να θέσουν σε κίνδυνο άλλα προγράμματα.

μεσολάβησης για τον έλεγχο εξερχόμενων και εισερχόμενων μονοπατιών επικοινωνίας και περιορίζοντας τους σταθμούς εργασίας να επικοινωνούν μόνο μέσω των συσκευών μεσολάβησης με την εφαρμογή ελέγχων πρόσβασης στην έξοδο από την περίμετρο.

5.4.2 Κλοπή διαπιστευτηρίων

Επίθεση στην Ουκρανία

Στην επίθεση, ο αντίπαλος φαίνεται να χρησιμοποίησε το λογισμικό BlackEnergy 3 για να εδραιωθεί και να χρησιμοποιήσει συστήματα καταγραφής για την κλοπή διαπιστευτηρίων. Ως αρχική προσέγγιση μετριασμού, συνέστησαν στους οργανισμούς να αποκτήσουν τους κανόνες YARA[14]. Με τη χρήση του εργαλείου YARA, οι οργανισμοί μπορούν να αναζητήσουν μολύνσεις με το κακόβουλο λογισμικό BlackEnergy 3 και, στη συνέχεια να χρησιμοποιήσουν εργαλεία αφαίρεσης κακόβουλου λογισμικού για να εξαλείψουν το κακόβουλο λογισμικό από τα μολυσμένα περιουσιακά στοιχεία. Οι αμυνόμενοι θα πρέπει να έχουν υπόψη τους το χρόνο που χρειάζεται για να εντοπίσουν έναν μολυσμένο υπολογιστή, καθώς ο εισβολέας μπορεί να έχει ήδη μετακινηθεί μέσα στο δίκτυο και εξασφαλίσει πρόσθετες μεθόδους αλληλεπίδρασης και επικοινωνίας με το μολυσμένο δίκτυο. Οι οργανισμοί θα πρέπει να αλλάζουν τους κωδικούς πρόσβασης των χρηστών και των κοινών χρηστών.

Η επόμενη επίθεση

Οι επιτιθέμενοι με μόνιμη πρόσβαση θα χρησιμοποιήσουν απλώς ένα διαφορετικό Trojan απομακρυσμένης πρόσβασης, μια ενημερωμένη έκδοση του κακόβουλου λογισμικού BlackEnergy 3, ή έναν εναλλακτικό τρόπο επιθέσεων με διαπιστευτήρια. Για τον εντοπισμό και τον μετριασμό των κινήσεων των αντιπάλων σε όλο το περιβάλλον και τη χειραγώγηση λογαριασμού, οι προσπάθειες μετριασμού θα πρέπει να επικεντρωθούν στον κατάλογο (π.χ,Active Directory, Domain, eDirectory και LDAP) τμηματοποίησης με μοντέλα εμπιστοσύνης οργανωτικών μονάδων. Αυτή η προσέγγιση θα επέτρεπε την έγκαιρη ανίχνευση και θα απέτρεπε ορισμένες βασικές προσεγγίσεις επιτιθέμενων.

Ευκαιρίες για διατάραξη

[14] **YARA** είναι το όνομα ενός εργαλείου που χρησιμοποιείται κυρίως στην έρευνα και ανίχνευση κακόβουλου λογισμικού. Παρέχει μια προσέγγιση βασισμένη σε κανόνες για τη δημιουργία περιγραφών οικογενειών κακόβουλου λογισμικού με βάση κειμενικά ή δυαδικά μοτίβα. Μια περιγραφή είναι ουσιαστικά ένα όνομα κανόνα YARA, όπου αυτοί οι κανόνες αποτελούνται από σύνολα συμβολοσειρών και μια δυαδική έκφραση

Παρακολούθηση της συμπεριφοράς των λογαριασμών των χρηστών, της επικοινωνίας του δικτύου του συστήματος και της δραστηριότητας σε επίπεδο καταλόγου με έμφαση στον εντοπισμό ανωμαλιών. Εφαρμογή δυνατοτήτων συναγερμού με συναγερμούς διαφορετικού επιπέδου προτεραιότητας με βάση τον κίνδυνο στα συστήματα που σχετίζονται με τους συναγερμούς. Είναι σημαντικό να σημειωθεί ότι το YARA είναι ένα εργαλείο εγκληματολογίας και όχι μια λύση συνεχούς παρακολούθησης.

5.4.3 Διείσδυση δεδομένων

Επίθεση στην Ουκρανία

Αφού οι επιτιθέμενοι απέκτησαν την απαραίτητη ελευθερία κινήσεων και δράσης στην υποδομή της πληροφορικής, ξεκίνησαν εκμεταλλευόμενοι τις απαραίτητες πληροφορίες και ανακαλύπτοντας τους κεντρικούς υπολογιστές και τις συσκευές για να επινοήσουν μια ιδέα επίθεσης προκειμένου να γίνει αντιληπτό από το κατανεμημένο σύστημα διαχείρισης-Distribution Management System (DMS) SCADA, ώστε να ανοίξει τους διακόπτες και να προκαλέσει διακοπή ρεύματος. Ακολούθησαν καταστροφικές επιθέσεις έναντι σταθμών εργασίας, διακομιστών και ενσωματωμένων συσκευών που παρέχουν βιομηχανικές επικοινωνίες στους υποσταθμούς διανομής. Η σύσταση μετριασμού εδώ είναι να γίνει κατανοητό πού υπάρχουν αυτού του είδους οι πληροφορίες στο εσωτερικό του δικτύου της επιχείρησης και των ICS. Η ελαχιστοποίηση του τόπου αποθήκευσης των πληροφοριών και ο έλεγχος της πρόσβασης αποτελούν προτεραιότητα για έναν οργανισμό που εξαρτάται από το ICS.

Η επόμενη επίθεση

Οι επιτιθέμενοι μπορούν να ερευνήσουν βαθύτερα τη διαμόρφωση και τις ρυθμίσεις του ICS ή τον ελεγκτή και τη λογική προστασίας/ασφάλειας. Διασφάλιση για την διατήρηση σε θησαυροφυλάκιο ενός αντιγράφου των γνωστών καλών αρχείων έργου, της λογικής ελέγχου και ασφάλειας και του υλικολογισμικού. Επίσης απαιτείται η χρήση ελεγκτών ακεραιότητας αρχείων για την παρακολούθηση της πρόσβασης ή δειγματοληπτικά φορτωμένα αρχεία για τυχόν αλλαγές.

Ευκαιρίες για διατάραξη

Οι επιτιθέμενοι μπορεί να είναι σε θέση να αναπτύξουν πρόσθετες προσεγγίσεις επίθεσης καθώς έχουν μάθει ένα σύστημα και μπορεί να έχουν κλέψει πληροφορίες που επιτρέπουν την ανάπτυξη ισχυρότερων μελλοντικών επιθέσεων. Οι αμυνόμενοι θα πρέπει να εξετάσουν τις ικανότητες ανίχνευσης και απόκρισης. Οι υπεύθυνοι λήψης αποφάσεων πρέπει να επανεξετάσουν τα σχέδια αποκατάστασής τους για επιθέσεις που έχουν τη

δυνατότητα να διεισδύσουν βαθύτερα στο ICS και να οδηγήσουν σε καταστροφή του εξοπλισμού. Πρέπει να προσδιοριστούν νέες συνδέσεις που εξέρχονται από το περιβάλλον και προηγουμένως αθέατες κρυπτογραφημένες επικοινωνίες. Η παρακολούθηση των δικτύων (Network Security Monitoring - NSM) είναι μια εξαιρετική μέθοδος ενεργητικής άμυνας για τον εντοπισμό της διαρροής και τον τερματισμό της επίθεσης ενός αντιπάλου πριν διαταράξει το ICS.

5.4.4 Πρόσβαση VPN[15]

Επίθεση στην Ουκρανία

Η καθοδήγηση μετριασμού με βάση την προσέγγιση του επιτιθέμενου που χρησιμοποιήθηκε σε αυτή την εκστρατεία συνιστά τη χρήση δύο παραγόντων αυθεντικοποίησης με διακριτικά χρήστη για την ενίσχυση της αυθεντικοποίησης.

Η επόμενη επίθεση

Οι επιτιθέμενοι μπορεί να αρχίσουν να αναζητούν υφιστάμενες υλοποιήσεις VPN από σημείο σε σημείο σε αξιόπιστα δίκτυα τρίτων ή μέσω των συνδέσεων υπαλλήλων απομακρυσμένης υποστήριξης όπου είναι ενεργοποιημένο το split tunneling[16]. Η σύσταση για άμεσο μετριασμό είναι να εφαρμοστούν αξιόπιστα συστήματα κεντρικού υπολογιστή ή ενδιάμεσων συστημάτων με έλεγχο πρόσβασης στο δίκτυο (Network Access Control - NAC). Επιπλέον, θα πρέπει να επιβληθεί μια προσέγγιση διαμόρφωσης VPN που απενεργοποιεί το split tunneling.

Ευκαιρίες για διατάραξη

Η απομακρυσμένη πρόσβαση μέσω αξιόπιστης σύνδεσης είναι επωφελής για έναν επιτιθέμενο. Αναζήτηση κάθε αξιόπιστου μονοπατιού επικοινωνίας, αξιολόγηση του κινδύνου, και εξάλειψη κάθε διαδρομής που δεν έχει εντοπισμένη ανάγκη, και η οποία αντισταθμίζει τον κίνδυνο ύπαρξης μιας διαδρομής επίθεσης. Για τα μονοπάτια επικοινωνίας που πρέπει να παραμείνουν, να εξεταστεί το ενδεχόμενο εφαρμογής της

[15] Το VPN σημαίνει **Virtual Private Network**, δηλαδή εικονικό ιδιωτικό δίκτυο. Πρόκειται για ένα δίκτυο που συνδέει απομακρυσμένες συσκευές μέσω ίντερνετ, διατηρώντας τα χαρακτηριστικά τοπικού δικτύου LAN, όπως την κοινή χρήση αρχείων και τις τοπικές IP. Αυτή η σύνδεση γίνεται με υψηλής ασφάλειας κρυπτογράφηση δεδομένων, που είναι πρακτικά αδύνατον να παραβιαστεί

[16] Η διαχωρισμένη σήραγγα είναι μια λειτουργία VPN που χωρίζει την κυκλοφορία σας στο διαδίκτυο και στέλνει ένα μέρος της μέσω μιας κρυπτογραφημένης σήραγγας εικονικού ιδιωτικού δικτύου (VPN), αλλά δρομολογεί το υπόλοιπο μέσω μιας ξεχωριστής σήραγγας στο ανοιχτό δίκτυο. Συνήθως, η διαχωρισμένη σήραγγα σάς επιτρέπει να επιλέξετε ποιες εφαρμογές θα ασφαλίσετε και ποιες θα μπορούν να συνδεθούν κανονικά.

πρόσβασης των χρηστών με χρόνο χρήσης. Εφαρμογή της δυνατότητας αυτοματοποιημένης αποσύνδεσης αυτών των διαδρομών μετά από καθορισμένο χρονικό διάστημα μετά την πρόσβαση και μια μέθοδο για χειροκίνητη αποσύνδεση αν χρειαστεί. Από την άποψη της παθητικής άμυνας, ο στραγγαλισμός δύναμης σε σημεία στο περιβάλλον ICS, διασφαλίζοντας ότι τα απομακρυσμένα VPN εισέρχονται στο περιβάλλον μέσω ενός αποκλειστικού (**demilitarized zone**) DMZ[17] απομακρυσμένης πρόσβασης. Αυτό διασφαλίζει ότι η κυκλοφορία και οι συνδέσεις μπορούν να παρακολουθούνται από ενεργούς αμυντικούς που χρησιμοποιούν τεχνικές όπως η παρακολούθηση της ασφάλειας του δικτύου για τον εντοπισμό ανωμαλιών στη διάρκεια των συνδέσεων, τον αριθμό των συνδέσεων και την ώρα που αυτές πραγματοποιούνται.

5.4.5 Απομακρυσμένη πρόσβαση στο σταθμό εργασίας

Επίθεση στην Ουκρανία

Με βάση τα στοιχεία που δόθηκαν, οι επιτιθέμενοι χρησιμοποίησαν τους σταθμούς εργασίας των οργανισμών εξ αποστάσεως (ενώ ο επιτιθέμενος ήταν φυσικά απομακρυσμένος, λογικά ήταν τοπικός στον κεντρικό υπολογιστή) για να πραγματοποιήσουν το στάδιο 2 της επίθεσης. Οι συστάσεις μετριασμού επικεντρώνονται στην απενεργοποίηση της απομακρυσμένης πρόσβασης στον κεντρικό υπολογιστή και στο περιμετρικό τείχος προστασίας.

Η επόμενη επίθεση

Οι αντίπαλοι μπορούν να τροποποιήσουν τις προσεγγίσεις επίθεσης για να φορτώσουν πρόσθετα εργαλεία απομακρυσμένης πρόσβασης, να χρησιμοποιήσουν απομακρυσμένες δυνατότητες και επικοινωνίες μέσω εξουσιοδοτημένων επικοινωνιών περιμετρικού τείχους προστασίας. Σε απάντηση σε αυτή την τροποποιημένη προσέγγιση επίθεσης, οι προσπάθειες μετριασμού θα πρέπει να επικεντρωθούν σε τοίχους προστασίας (firewalls) που βασίζονται σε ασφαλείς εφαρμογές του χρήστη και προσπάθειες διαχείρισης ρυθμίσεων για τον εντοπισμό αλλαγών στη λειτουργία ενός περιουσιακού στοιχείου. Εφαρμογή λευκής λίστας, εάν εγκατασταθεί στο HMI χειριστή για να αποτρέψει την εγκατάσταση μη εξουσιοδοτημένου λογισμικού απομακρυσμένης πρόσβασης, δεν θα βοηθούν στην αποτροπή εγκεκριμένου λογισμικού. Επίσης, λάβετε υπόψη ότι συγκεκριμένοι προμηθευτές συστημάτων ελέγχου μπορεί να μην εγκρίνουν το λογισμικό λευκής λίστας.

[17] Στην ασφάλεια των υπολογιστών, μια ζώνη DMZ ή αποστρατικοποιημένη είναι ένα φυσικό ή λογικό υποδίκτυο που περιέχει και εκθέτει τις υπηρεσίες εξωτερικού προσώπου ενός οργανισμού σε ένα μη αξιόπιστο, συνήθως μεγαλύτερο, δίκτυο, όπως το Διαδίκτυο.

Ευκαιρίες για διατάραξη

Καθώς ένας αμυντικός προετοιμάζεται για ένα περιουσιακό στοιχείο στον κυβερνοχώρο εντός ενός αξιόπιστου περιβάλλοντος που μπορεί να παραβιαστεί και να απομακρυνθεί ελέγχεται, πρέπει να εξετάσουν προσεγγίσεις για να μεταβούν γρήγορα σε ένα περιβάλλον συντηρητικών επιχειρήσεων όπου η δυνατότητα έκδοσης σημάτων ελέγχου από μη αξιόπιστα περιουσιακά στοιχεία διακόπτεται. Η σωστή αρχιτεκτονική υπαγορεύει τη δυνατότητα τμηματοποίησης ή απενεργοποίησης δραστηριοτήτων όπως απομακρυσμένες συνδέσεις και περιττές εξερχόμενες επικοινωνίες, ενώ διεξαγωγή ενεργών μηχανισμών άμυνας, όπως η αντιμετώπιση περιστατικών πριν από την αποκατάσταση του επιχειρησιακού ελέγχου, προϋποθέτει ικανότητες σε γνωστά, αξίας, περιουσιακά στοιχεία.

5.4.6 Έλεγχος και λειτουργία

Επίθεση στην Ουκρανία

Καθώς οι επιτιθέμενοι χρησιμοποιούσαν τα HMI του χειριστή, λειτουργούσαν πολυάριθμες τοποθεσίες υπό τον έλεγχο του αποστολέα. Οι προσεγγίσεις μετριασμού για τη συγκεκριμένη δράση θα επικεντρωθούν στη λογική σε επίπεδο εφαρμογής που απαιτεί επιβεβαίωση από τον φορέα εκμετάλλευσης, ή να εφαρμόσει περιορισμούς περιοχής ευθύνης (Area of Responsibility-AoR) που επιτρέπουν σε έναν φορέα εκμετάλλευσης να εκτελεί μόνο ορισμένα στοιχεία ενός συστήματος. Για παράδειγμα: Εάν μια οντότητα εφαρμόσει το AoR σε έναν σταθμό εργασίας χειριστή που παρείχε ανατολικού διακόπτη και έναν δεύτερο σταθμό εργασίας χειριστή που παρείχε τον έλεγχο του δυτικού διακόπτη, τότε ένας αντίπαλος τοποθετημένος σε έναν σταθμό εργασίας θα περιορίζεται στο AoR που επιτρέπεται στον συγκεκριμένο σταθμό εργασίας. Κάποια συστήματα επιτρέπουν την AoR που καθορίζεται από το όνομα χρήστη, την AoR που καθορίζεται από το σταθμό εργασίας ή/και ένα μοντέλο διασταύρωσης που συνδυάζει το όνομα χρήστη και το αναγνωριστικό σταθμού εργασίας στην εξουσιοδότηση AoR. Υπάρχουν διαφοροποιήσεις μεταξύ των συστημάτων των προμηθευτών στον τρόπο με τον οποίο γίνεται ο έλεγχος ταυτότητας στον τοπικό σταθμό εργασίας, στον κατάλογο ή στην εφαρμογή.

Η επόμενη επίθεση

Όταν ένας επιτιθέμενος εντοπίζει έναν σταθμό εργασίας με ελέγχους ασφαλείας εφαρμογών που περιορίζουν τις δυνατότητές του, μπορεί να τροποποιήσει την επίθεσή του ώστε να ελέγχει απευθείας το σύστημα εκδίδοντας ή εισάγοντας εντολές ελέγχου. Οι στρατηγικές μετριασμού αυτής της προσέγγισης θα επικεντρωθούν στην αυθεντικοποίηση της διαδρομής επικοινωνίας ή του πρωτοκόλλου που θα απαιτούσε την έκδοση εντολών από ένα εξουσιοδοτημένο μέσο. Παρακολούθηση συνεδριών επικοινωνίας μεταξύ μπορούν να οδηγήσουν στην έγκαιρη ανίχνευση και διερεύνηση ύποπτων επικοινωνιών.

Ευκαιρίες για διατάραξη

Προετοιμασία για την αντίπαλη αξιοποίηση περιουσιακών στοιχείων στον κυβερνοχώρο ή διαδρομών επικοινωνίας για τον έλεγχο και τη λειτουργία στοιχείων της ένα σύστημα ICS, απαιτεί από τους υπερασπιστές του συστήματος να αναπτύξουν μια προσέγγιση απόκρισης που εξαλείφει ολόκληρα τμήματα των στοιχεία και δίκτυα περιουσιακών στοιχείων στον κυβερνοχώρο σε μια προσπάθεια να εμποδίσουν τον αυτοματοποιημένο έλεγχο και να ενεργοποιήσουν χειροκίνητες λειτουργίες μόνο. Καθώς οι αντίπαλοι μαθαίνουν το περιβάλλον, μπορούν να εκδίδουν δοκιμαστικές εντολές και να αλληλεπιδρούν με το SCADA περιβάλλον, χωρίς την πρόθεση να το διαταράξουν. Για σκοπούς μετριασμού, οι αμυνόμενοι, πρέπει να μιλήσουν με τους φορείς εκμετάλλευσης και να ρωτούν για μη φυσιολογικά περιστατικά και, από την άποψη της παθητικής άμυνας, να διασφαλίσουν ότι τα αρχεία καταγραφής συλλέγονται όχι μόνο από τον κεντρικό υπολογιστή αλλά και από τις εφαρμογές SCADA. Επιπλέον, πρέπει να εφαρμόζουν μια αρχιτεκτονική συγκέντρωσης αρχείων καταγραφής που αναπαράγει αρχεία καταγραφής από περιουσιακά στοιχεία σε ένα σύστημα συσχέτισης καταγραφής. Τέλος, πρέπει οι ενεργοί αμυνόμενοι πρέπει να επανεξετάζουν τακτικά αυτά τα αρχεία καταγραφής σε συνδυασμό με άλλες δραστηριότητες παρακολούθησης σε όλο το ICS για τον εντοπισμό ανωμαλιών.

5.4.7 Επιπτώσεις σε εργαλεία και τεχνολογία

Επίθεση στην Ουκρανία

Οι επιτιθέμενοι χρησιμοποίησαν πολλαπλές προσεγγίσεις για να επηρεάσουν τα εργαλεία επικοινωνίας, την τεχνολογία του χειριστή για προσπάθειες αποκατάστασης λογισμικού, καθώς και υποδομές εγκαταστάσεων που είναι απαραίτητες για πολλές δραστηριότητες των φορέων εκμετάλλευσης. Ως εκ τούτου, οι συστάσεις μετριασμού μεταβάλλονται. Τα στοιχεία στα οποία πρέπει να εστιάσετε είναι:

- Καθιέρωση δυνατοτήτων φιλτραρίσματος και απόκρισης στους παρόχους τηλεπικοινωνιών για ενεργοποίηση κατά τη διάρκεια ενός Telephony Denial of Service (TDoS) σε εξέλιξη επίθεσης
  Η άρνηση παροχής υπηρεσιών τηλεφωνίας (TDoS) είναι ένα είδος επίθεσης άρνησης υπηρεσίας (DoS), στην οποία οι επιτιθέμενοι ξεκινούν μεγάλο όγκο κλήσεων και διατηρούν αυτές τις κλήσεις ενεργές για όσο το δυνατόν περισσότερο κατά του δικτύου προορισμού, αποτρέποντας την είσοδο νόμιμων κλήσεων
- Απενεργοποιήστε την απομακρυσμένη διαχείριση των συσκευών πεδίου όταν δεν απαιτείται.
- Αποσυνδέστε τα συστήματα υποδομής ελέγχου του κτιρίου από το δίκτυο ICS.

- Εξετάστε τον αριθμό των ανταλλακτικών που απαιτούνται για τα ενσωματωμένα συστήματα για την ανάκτηση της απαιτούμενης επικοινωνίας ή ελέγχου/προστασίας.

Η επόμενη επίθεση

Μια επακόλουθη επίθεση μπορεί να προχωρήσει από την κατανάλωση πόρων σε μια πιο άμεση διακοπή της διαδρομής επικοινωνίας που επηρεάζει τις δυνατότητες επικοινωνίας. Για να μετριάσουν αυτή την προσέγγιση, οι υπερασπιστές πρέπει να δημιουργήσουν υποδομή εναλλακτικών επικοινωνιών για βασικές υπηρεσιακές δυνατότητες.

Αφού ένας εισβολέας εντοπίσει αυξημένες απαιτήσεις ασφαλείας για τη διαχείριση συσκευών πεδίου, μπορεί να επιχειρήσει να δημιουργήσει άμεση πρόσβαση σε μια συσκευή πεδίου μέσω ενός τοπικού περιουσιακού στοιχείου με συνδεσιμότητα ή με φυσική παρουσία στο χώρο για τον άμεσο χειρισμό του υλικολογισμικού. Οι στρατηγικές μετριασμού για αυτήν την προσέγγιση της επίθεσης επικεντρώνονται σε ηλεκτρονικούς και φυσικούς ελέγχους πρόσβασης και την ανάπτυξη ικανότητας ταχείας αντίδρασης κατά τη διάρκεια μιας επίθεσης ή ενός συμβάντος.

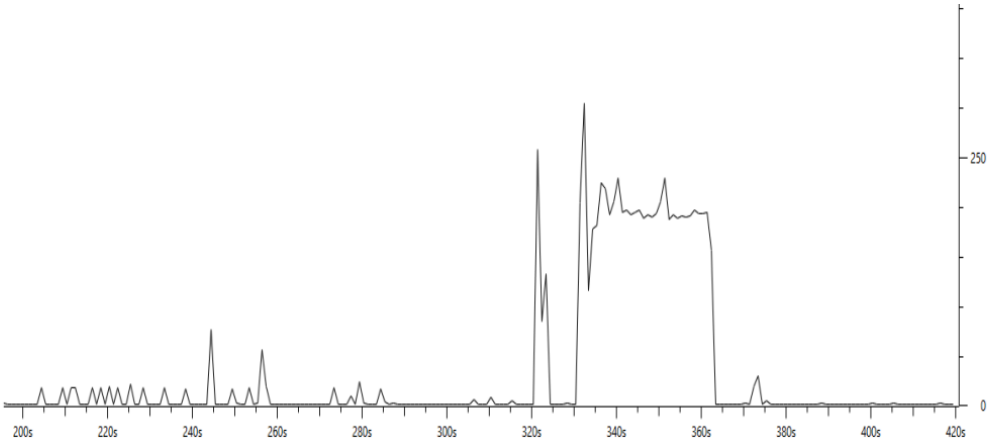
Ευκαιρίες για διατάραξη

Ένας αποφασισμένος αντίπαλος μπορεί να επηρεάσει απομακρυσμένα περιουσιακά στοιχεία είτε ηλεκτρονικά είτε φυσικά. Ένας αμυνόμενος πρέπει να αναπτύξει ισχυρές προσεγγίσεις ανάκαμψης και αποκατάστασης για την αντικατάσταση κρίσιμων για την αποστολή στοιχείων ενεργητικού στον κυβερνοχώρο. Μια επιλογή είναι να βασίζονται στην απογραφή και τη βοήθεια αμοιβαίας βοήθειας από αξιόπιστες ομότιμες οργανώσεις ή/και προμηθευτές. Σε περιπτώσεις όπου συγκεκριμένα περιουσιακά στοιχεία δεν είναι άμεσα ανακτήσιμα, είναι απαραίτητο να αναπτυχθεί η ικανότητα λειτουργίας των μεγαλύτερων συστημάτων με λειτουργικές νησίδες που μπορούν να ανακτηθούν εγκαίρως.

Οι αμυντικοί θα πρέπει να έχουν πρόσβαση και ορατότητα στα ICS για να μπορούν να εντοπίζουν μη φυσιολογική συμπεριφορά γύρω από το πεδίο αλληλεπίδρασης με τη συσκευή. Για παράδειγμα, η μεταφόρτωση υλικολογισμικού εκτός προγραμματισμένου χρόνου διακοπής λειτουργίας θα πρέπει να γίνεται γρήγορα παρατηρήσιμο. Οι τροποποιήσεις του υλικολογισμικού μέσω του δικτύου προκαλούν αιχμές στην κυκλοφορία του δικτύου που οι ενεργοί αμυνόμενοι θα πρέπει να αναζητούν.

Στο Σχήμα 9 φαίνεται ένα παράδειγμα κακόβουλης ενημέρωσης υλικολογισμικού σε μια διακοπή του βιομηχανικού δικτύου. Ακόμα και χωρίς να γνωρίζετε τη βασική γραμμή της

κανονικής δραστηριότητας, την οποία θα πρέπει να έχουν οι αμυνόμενοι, μπορεί να είναι τετριμμένο να εντοπίζονται ενημερώσεις υλικολογισμικού στα δεδομένα δικτύου.



Σχήμα 9: Παράδειγμα κακόβουλης ενημέρωσης υλικολογισμικού σε μια διακοπή του βιομηχανικού δικτύου (https://www.youtube.com/watch?v=yaY3rtA37Uc)

5.4.8 Ανταπόκριση και αποκατάσταση

Επίθεση στην Ουκρανία

Οι κυβερνοεπιθέσεις που πραγματοποιήθηκαν εναντίον τριών ουκρανικών διανομέων ήταν καλά σχεδιασμένες και εξαιρετικά συντονισμένες. Οι επιθέσεις αποτελούνταν από διάφορα κύρια στοιχεία με τμήματα που επέτρεπαν και υποστήριζαν τις επιθέσεις. Οι επιτιθέμενοι ήταν απομακρυσμένοι και αλληλεπιδρούσαν με πολλαπλές τοποθεσίες σε κάθε έναν από τους στόχους τους, ώστε να περιλαμβάνουν κεντρικές και περιφερειακές εγκαταστάσεις. Οι επιχειρήσεις κοινής ωφέλειας διανομής διαθέτουν παραδοσιακά τόσο κεντρικό(α) γραφείο(α) επιχειρήσεων και μηχανικών όσο και έναν αριθμό εγκαταστάσεων υποκαταστημάτων που χρησιμοποιούνται για την υποστήριξη του προσωπικού γραμμής, την ανάγνωση μετρητών, την πληρωμή λογαριασμών και τον κατανεμημένο εποπτικό έλεγχο επιχειρήσεις. Ορισμένοι τύποι επιθέσεων στον κυβερνοχώρο που αποσκοπούν στην κακόβουλη κατάληψη και λειτουργία ενός SCADA DMS μπορεί να εκτελούνται καλύτερα με κατανεμημένο τρόπο στο χαμηλότερο ή το πιο άμεσο επίπεδο (από ένα τοπικό σύστημα αποστολής και SCADA διακομιστή στους υποσταθμούς που παρακολουθούνται και ελέγχονται). Προετοιμασία για μια πολύπλευρη, υψηλού ρυθμού επίθεση δεν είναι εύκολη και απαιτεί προσεκτική αναθεώρηση του σχεδίου, δοκιμές, ολοκληρωμένη άμυνα και επιχειρησιακές ασκήσεις. Δοκιμή των βημάτων για την ταχύτερη αποκοπή ή την αποτροπή της απομακρυσμένης πρόσβασης, για τον ασφαλή διαχωρισμό των ICS από τα

συνδεδεμένα δίκτυα ή για να περιορίσουν και να απομονώσουν ύποπτους κεντρικούς υπολογιστές είναι ζωτικής σημασίας.

Η επόμενη επίθεση

Η επόμενη επίθεση μπορεί σκόπιμα να διαφέρει ως προς την προσέγγισή της για να αποπροσανατολίσει ή να ανατρέψει τα σχέδια του αμυνόμενου και τις προσδοκίες του. Είναι ζωτικής σημασίας οι αμυνόμενοι να ασκούνται και να εκπαιδεύονται έναντι διαφορετικών σεναρίων και να γνωρίζουν ότι οι επιτιθέμενοι είναι συν-προσαρμοστικοί και δημιουργικοί. Επίσης είναι ζωτικής σημασίας η ανάπτυξη ικανοτήτων με γνώμονα την ευελιξία.

Ευκαιρίες για διατάραξη

Το προσωπικό των επιχειρήσεων πρέπει να συμμετέχει στο σχεδιασμό της αποκατάστασης μετά από μια επιτυχή επίθεση στο στάδιο 2 του ICS. Έννοιες που πρέπει να εξεταστούν από την οπτική γωνία των ηλεκτρικών λειτουργιών και της μηχανικής περιλαμβάνουν τα ακόλουθα:

- Ανάλυση έκτακτων περιστατικών στον κυβερνοχώρο: Συνεχής ανάλυση και προετοιμασία του συστήματος για το επόμενο συμβάν.
- Σχεδιασμός αποτυχίας στον κυβερνοχώρο: Μοντελοποίηση και δοκιμή της απόκρισης του συστήματος στον κυβερνοχώρο σε διακοπές λειτουργίας του δικτύου και των περιουσιακών στοιχείων.
- Συντηρητικές επιχειρήσεις στον κυβερνοχώρο: Σκόπιμη εξάλειψη των προγραμματισμένων και μη προγραμματισμένων αλλαγών καθώς και διακοπή των τυχόν δυνητικά επιζήμιων διαδικασιών.
- Απορρόφηση φορτίου στον κυβερνοχώρο: Εξάλειψη των περιττών τμημάτων δικτύου, επικοινωνιών και περιουσιακών στοιχείων στον κυβερνοχώρο που είναι δεν είναι επιχειρησιακά αναγκαία.
- Ανάλυση Βασικών Αιτιών-ν στον Κυβερνοχώρο Cyber Root Cause Analysis (RCA) : Τύπου , ιατροδικαστική ανάλυση RCA για τον προσδιορισμό του τρόπου με τον οποίο συνέβη ένα συμβάν με αντίκτυπο και να διασφαλίσετε ότι θα περιοριστεί.
- Cyber Blackstart: Διαμορφώσεις βάσης περιουσιακών στοιχείων του κυβερνοχώρου και δυνατότητα κατασκευής «καθαρού μετάλλου» για την αποκατάσταση του κυβερνοχώρου του συστήματος σε κατάσταση κρίσιμης υπηρεσίας.
- Αμοιβαία βοήθεια στον κυβερνοχώρο: Δυνατότητα αξιοποίησης των κέντρων ανταλλαγής και ανάλυσης πληροφοριών (information sharing and analysis centers

-ISAC), των ομότιμων υπηρεσιών κοινής ωφέλειας, του νόμου υπηρεσίες επιβολής του νόμου και τις υπηρεσίες πληροφοριών, καθώς και τους εργολάβους και τους προμηθευτές για να ανταποκριθούν σε μεγάλης κλίμακας εκδηλώσεις.

5.5 ΣΥΣΤΑΣΕΙΣ

5.5.1 Αρχιτεκτονική

Συστάσεις:

- Διαχωρίστε σωστά τα δίκτυα μεταξύ τους.
- Διασφαλίστε ότι η καταγραφή είναι ενεργοποιημένη στις συσκευές που την υποστηρίζουν, συμπεριλαμβανομένων τόσο της πληροφορικής όσο και της λειτουργικής τεχνολογίας.
- Διασφάλιση ότι η αρχιτεκτονική του δικτύου, όπως οι μεταγωγείς, διαχειρίζεται και έχει τη δυνατότητα καταγραφής δεδομένων από το περιβάλλον για την υποστήριξη μηχανισμών παθητικής και ενεργητικής άμυνας.
- Δημιουργήστε αντίγραφα ασφαλείας των κρίσιμων προγραμμάτων εγκατάστασης λογισμικού και συμπεριλάβετε έναν ψηφιακό κατακερματισμό MD5 και SHA256 του εγκαταστάτες.
- Συλλογή και φύλαξη εφεδρικών αρχείων έργου από το δίκτυο.
- Δοκιμάστε τα εργαλεία και τις τεχνολογίες που θα χρειαστούν οι παθητικοί και οι ενεργητικοί μηχανισμοί άμυνας (όπως λογισμικό ψηφιακής απεικόνισης) στο περιβάλλον, ώστε να διασφαλιστεί ότι δεν θα επηρεάσει αρνητικά τα συστήματα.
- Ιεράρχηση και επιδιόρθωση γνωστών ευπαθειών με βάση τα πιο κρίσιμα περιουσιακά στοιχεία του οργανισμού.
- Περιορίστε τις απομακρυσμένες συνδέσεις μόνο στο προσωπικό που τις χρειάζεται. Όταν το προσωπικό χρειάζεται απομακρυσμένη πρόσβαση, να διασφαλίζουν ότι, εάν δεν χρειάζονται έλεγχο, δεν έχουν πρόσβαση σε στοιχεία ελέγχου. Χρήση δύο μορφών ελέγχου ταυτότητας στις απομακρυσμένες συνδέσεις.
- Εξετάστε το ενδεχόμενο χρήσης ενός συστήματος παρακολούθησης συμβάντων του συστήματος, διαμορφωμένου και ελεγχόμενου ειδικά για υψηλής αξίας Συστήματα ICS/SCADA.

5.5.2 Παθητική άμυνα

Συστάσεις:

- Η λευκή λίστα εφαρμογών μπορεί να βοηθήσει στον περιορισμό των αρχικών φορέων μόλυνσης των αντιπάλων και θα πρέπει να χρησιμοποιείται όταν δεν είναι πολύ παρεμβατική για τα ICS.
- Τα DMZ και τα κατάλληλα ρυθμισμένα τείχη προστασίας μεταξύ των τμημάτων του δικτύου θα δώσουν ορατότητα στο περιβάλλον και θα επιτρέπουν στους αμυντικούς τον απαιτούμενο χρόνο για τον εντοπισμό εισβολών.
- Δημιουργία ενός κεντρικού σημείου καταγραφής και συγκέντρωσης δεδομένων, ώστε να είναι δυνατή η συλλογή εγκληματολογικών στοιχείων και στη διάθεση των υπερασπιστών.
- Εφαρμογή προτεραιοτήτων πακέτων συναγερμών για μη φυσιολογικά συμβάντα στον κυβερνοχώρο εντός του συστήματος ελέγχου.
- Επιβολή πολιτικής επαναφοράς κωδικού πρόσβασης σε περίπτωση παραβίασης, ειδικά για τα VPN και τα διοικητικά συστήματα στους λογαριασμούς.
- Χρησιμοποιήστε ενημερωμένες τεχνολογίες προστασίας από ιούς ή τεχνολογίες ασφάλειας τελικών σημείων για να επιτρέψετε την άρνηση γνωστού κακόβουλου λογισμικού.
- Διαμορφώστε ένα σύστημα ανίχνευσης εισβολών έτσι ώστε να μπορούν να αναπτυχθούν γρήγορα κανόνες για την αναζήτηση εισβολέων.

5.5.3 Ενεργός άμυνα

Συστάσεις:

- Εκπαιδεύστε τους αμυντικούς να αναζητούν περίεργες επικοινωνίες που εγκαταλείπουν το δικτυακό περιβάλλον, όπως νέες IP επικοινωνίες.
- Παρακολουθήστε την ασφάλεια του δικτύου για τη συνεχή αναζήτηση ανωμαλιών στο δικτυακό περιβάλλον.
- Σχεδιασμός και εκπαίδευση σε σχέδια αντιμετώπισης περιστατικών που περιλαμβάνουν τόσο το προσωπικό του δικτύου πληροφορικής, όσο και το προσωπικό του δικτύου λειτουργικής τεχνολογίας.
- Εξετάστε μοντέλα ενεργού άμυνας για επιχειρήσεις ασφαλείας, όπως ο ενεργός κύκλος άμυνας στον κυβερνοχώρο.
- Διασφαλίστε ότι το προσωπικό που εκτελεί αναλύσεις έχει πρόσβαση σε τεχνολογίες, όπως sandboxes για τη γρήγορη ανάλυση εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου phishing ή περίεργα αρχεία και εξάγετε συμβατούς δείκτες για να αναζητήσετε μολυσμένα συστήματα.
- Χρησιμοποιήστε εργαλεία δημιουργίας αντιγράφων ασφαλείας και ανάκτησης για τη λήψη ψηφιακών εικόνων από μερικά από τα συστήματα του εποπτικού

περιβάλλοντος κάθε 6-12 μήνες. Αυτό θα επιτρέψει μια βασική γραμμή δραστηριότητας που θα κατασκευαστεί και θα καταστήσει τις εικόνες διαθέσιμες για σάρωση με νέους συμβατούς δείκτες, όπως οι νέοι κανόνες YARA για τις αναδυόμενες απειλές.

- Εκπαιδεύστε τους υπερασπιστές στη χρήση εργαλείων όπως το YARA για τη σάρωση ψηφιακών εικόνων και στοιχείων που συλλέγονται από το περιβάλλον αλλά μην κάνετε τις σαρώσεις στο ίδιο το περιβάλλον παραγωγής.

Η καλή αρχιτεκτονική και οι πρακτικές παθητικής άμυνας δημιουργούν ένα υπερασπίσιμο ICS. Η αντιμετώπιση ευέλικτων και επίμονων ανθρώπινων αντιπάλων απαιτεί κατάλληλα εκπαιδευμένους και εξοπλισμένους υπερασπιστές.

5.6 ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

5.6.1 Επιπτώσεις για τους υπερασπιστές

Οι εξ αποστάσεως κυβερνοεπιθέσεις εναντίον των υποδομών ηλεκτρικής ενέργειας της Ουκρανίας ήταν τολμηρές και επιτυχείς. Η κυβερνοεπίθεση ήταν σε μεγάλο βαθμό συγχρονισμένη και ο αντίπαλος ήταν πρόθυμος να λειτουργήσει κακόβουλα ένα σύστημα SCADA για να προκαλέσει διακοπές ρεύματος, ακολουθούμενες από καταστροφικές επιθέσεις για την απενεργοποίηση του SCADA και των επικοινωνιών με το πεδίο. Είναι η πρώτη φορά που ο κόσμος βλέπει αυτού του είδους την επίθεση εναντίον συστημάτων σε κρίσιμες εθνικές υποδομές. Πρόκειται για μια κλιμάκωση σε σχέση με προηγούμενες καταστροφικές επιθέσεις που επηρέασαν γενικής χρήσης υπολογιστές και διακομιστές (π.χ. Saudi Aramco, RasGas, Sands Casino και Sony Pictures). Διασχίστηκαν διάφορες γραμμές στη διεξαγωγή αυτών των επιθέσεων, καθώς οι στόχοι μπορούν να χαρακτηριστούν αποκλειστικά ως μη στρατιωτικές υποδομές. Ιστορικές επιθέσεις, όπως το Stuxnet, το οποίο περιλάμβανε την καταστροφή εξοπλισμού στο περιβάλλον OT (Operational Technology, δηλ. υλικό και λογισμικό που ανιχνεύει ή προκαλεί αλλαγή, μέσω της άμεσης παρακολούθησης ή/και ελέγχου βιομηχανικού εξοπλισμού, περιουσιακών στοιχείων, διαδικασιών και γεγονότων) θα μπορούσε να υποστηριχθεί ότι ομοιάζει με χειρουργική επέμβαση εναντίον στρατιωτικού στόχου.

Οι υπερασπιστές των υποδομών πρέπει να είναι έτοιμοι να αντιμετωπίσουν εξαιρετικά στοχευμένες και κατευθυνόμενες επιθέσεις που περιλαμβάνουν τις δικές τους ICS που χρησιμοποιούνται εναντίον τους, σε συνδυασμό με την ενίσχυση των επιθέσεων για την άρνηση υποδομών επικοινωνίας και μελλοντική χρήση των ICS τους. Τα στοιχεία που αναλύθηκαν στην επίθεση έδειξαν ότι υπήρχε μια συγκεκριμένη ακολουθία στην κακή χρήση των ICS, συμπεριλαμβανομένης της αποτροπής της περαιτέρω χρήσης των ICS από

τους υπερασπιστές για την αποκατάσταση του συστήματος. Αυτό σημαίνει ότι ο επιτιθέμενος "έκαψε τις γέφυρες" πίσω του καταστρέφοντας εξοπλισμό και σβήνοντας συσκευές για να αποτρέψει την αυτοματοποιημένη αποκατάσταση του συστήματος. Οι επιθέσεις υπογραμμίζουν την ανάγκη ανάπτυξης ενεργών κυβερνοαμυντικών συστημάτων.

Αναφορικά με την επίθεση στην Ουκρανία, τίποτα δεν αφορούσε εγγενώς τις ουκρανικές υποδομές. Ο αντίκτυπος μιας παρόμοιας επίθεσης μπορεί να είναι διαφορετικός σε άλλα έθνη, αλλά η μεθοδολογία της επίθεσης, οι Τακτικές, Τεχνικές και Διαδικασίες που παρατηρούνται είναι εφαρμόσιμες σε υποδομές σε όλο τον κόσμο.

5.6.2 Συμπεράσματα

Προσδιορίσαμε πέντε θέματα στα οποία πρέπει να εστιάσουν οι αμυνόμενοι καθώς εξετάζουν τι σημαίνει αυτή η επίθεση για τον οργανισμό τους:

Θέμα 1

Οι υπερασπιστές των ICS, πρέπει να εξετάστε την αλληλουχία των γεγονότων που έλαβαν χώρα από τον αντίπαλο κατά τους μήνες που προηγήθηκαν της 23 Δεκεμβρίου 2015, όταν σχεδιάστηκε και αναπτύχθηκε αυτή η κυβερνοεπιχείρηση με στόχο τις ουκρανικές υποδομές ηλεκτρικής ενέργειας. Η επιχείρηση βασίστηκε σε εισβολές που φαίνεται να προήλθαν από μια ευρύτερη εκστρατεία πρόσβασης που διεξήχθη την άνοιξη του 2015. Σε μια παρατεταμένη όμως εκστρατεία επίθεσης, είναι πιθανό να υπάρχουν πολλές ευκαιρίες να την ανιχνεύσουν και να υπερασπιστούν στην συνέχεια το στοχευμένο σύστημα.

Θέμα 2

Οι κυβερνοεπιθέσεις πραγματοποιήθηκαν με διαφορά λίγων λεπτών η μία από την άλλη εναντίον τριών διανομέων ηλεκτρικής ενέργειας, με αποτέλεσμα διακοπές της ισχύς που επηρέασαν περίπου 225.000 πελάτες για λίγες ώρες. Ενώ ο συνολικός αριθμός των πελατών σε τρία εδάφη υπηρεσιών δεν αθροίζουν σε σημαντικό αριθμό πελατών ή φορτίου σε όλη την Ουκρανία, μπορεί να υπάρχει σημασία στην επιλογή του στόχου ή σε συγκεκριμένα φορτία. Ένα κρίσιμο στοιχείο της συγκεκριμένης επίθεσης ήταν η συντονισμένη φύση που επηρεάζει τρεις οντότητες-στόχους και την πληρότητα της ακολουθίας των γεγονότων του αντιπάλου στην επίτευξη των στόχων του.

Θέμα 3

Οι επιθέσεις στον κυβερνοχώρο χαρακτηρίστηκαν λανθασμένα ως αποκλειστικά συνδεδεμένες με το BlackEnergy 3 και το KillDisk. Το BlackEnergy 3 ήταν απλά ένα εργαλείο που χρησιμοποιήθηκε στο Στάδιο 1 των επιθέσεων και το KillDisk ήταν ένα εργαλείο ενίσχυσης που χρησιμοποιήθηκε στο Στάδιο 2 των επιθέσεων. Το κακόβουλο

λογισμικό BlackEnergy 3 χρησιμοποιήθηκε για να αποκτήσει αρχικά ερείσματα σε πλήθος οργανισμών εντός της Ουκρανίας και όχι μόνο στους τρεις προσβεβλημένους διανομείς. Είναι άγνωστο αν ο αντίπαλος είχε σχεδιάσει να χρησιμοποιήσει αυτή την εκστρατεία πρόσβασης για να επιτρέψει τη λειτουργία τους ή αν η επίτευξη πρόσβασης ήταν το κίνητρο που οδήγησε στην ανάπτυξη μιας ιδέας για την επίθεση στο σύστημα ηλεκτρικής ενέργειας.

Η υπερβολική εστίαση στο συγκεκριμένο κακόβουλο λογισμικό που χρησιμοποιήθηκε σε αυτή την επίθεση τοποθετεί τους υπερασπιστές σε μια νοοτροπία στην οποία απλά περιμένουν καθοδήγηση σχετικά με τα συγκεκριμένα στοιχεία της επίθεσης, ώστε να μπορέσουν να τα εξαλείψουν. Αυτή η επίθεση θα μπορούσε να έχει καταστεί δυνατή με ποικίλες προσεγγίσεις για την απόκτηση πρόσβασης και τη χρήση των υφιστάμενων περιουσιακών στοιχείων εντός ενός στόχου. Ανεξάρτητα από τον αρχικό φορέα επίθεσης, τα εργαλεία και το περιβάλλον ICS χρησιμοποιήθηκαν τελικά για την επίτευξη του επιθυμητού αποτελέσματος και όχι το κακόβουλο λογισμικό BlackEnergy 3.

Θέμα 4

Η ιδέα της επίθεσης έπρεπε να μπορεί να λειτουργήσει σε πολλαπλές υλοποιήσεις SCADA DMS και να στοχεύει σε κοινά ευαίσθητα στοιχεία, όπως η αντικατάσταση αρχείων αποθήκευσης για τους σταθμούς εργασίας με λειτουργικό σύστημα Windows και διακομιστές. Οι επιτιθέμενοι πιθανότατα ανέπτυξαν καταστροφικές τεχνικές αντικατάστασης υλικολογισμικού, αφού ανακάλυψαν προσβάσιμα ενσωματωμένα συστήματα. Υπήρξε πιθανόν ένα σημαντικό ποσό μη παρατηρήσιμων αντιπαραβολικών δοκιμών που πραγματοποιήθηκαν πριν από την εισαγωγή της επίθεσης στο περιβάλλον. Πολλές δυνατότητες επιδείχθηκαν κατά τη διάρκεια αυτής της επίθεσης και όλες παρέχουν συγκεκριμένα διδάγματα που πρέπει να αξιοποιήσουν οι υπερασπιστές.

Θέμα 5

Η ανταλλαγή πληροφοριών είναι το κλειδί για τον εντοπισμό μιας συντονισμένης επίθεσης και την καθοδήγηση της κατάλληλης ενέργειας. Εντός της Ουκρανίας, ένας οργανισμός με την ικανότητα να επιτρέπει την κατάλληλη ανταλλαγή πληροφοριών και θα πρέπει να επιδιώκεται η παροχή καθοδήγησης για την αντιμετώπιση περιστατικών. Στις Ηνωμένες Πολιτείες και σε άλλες χώρες με καθιερωμένους μηχανισμούς ανταλλαγής πληροφοριών, όπως τα ISACs (κέντρα ανταλλαγής και ανάλυσης πληροφοριών), θα πρέπει να επικεντρωθεί στη διατήρηση και τη βελτίωση των πληροφοριών που παρέχουν οι ιδιοκτήτες και οι φορείς εκμετάλλευσης περιουσιακών στοιχείων. Αυτή η αυξημένη ανταλλαγή δεδομένων θα ενισχύσει την ευαισθητοποίηση του τομέα, γεγονός που με τη σειρά του θα οδηγήσει σε έγκαιρη ανίχνευση επιθέσεων και διευκόλυνση της αντιμετώπισης περιστατικών.

Με πολλούς τρόπους, οι ουκρανικοί διανομείς και το προσωπικό τους, καθώς και τα εμπλεκόμενα μέλη της ουκρανικής κυβέρνησης αξίζουν συγχαρητήρια. Αυτή η επίθεση ήταν μια παγκόσμια πρωτοτυπία από πολλές απόψεις και η αντίδραση της Ουκρανίας ήταν εντυπωσιακή .

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η εργασία αποτελεί μια επιλεκτική βιβλιογραφική ανασκόπηση όσον αφορά επιθέσεις παραβίασης ασφάλειας στο Διαδίκτυο των Πραγμάτων και προτάσεις για αντιμετώπιση τους. Η εργασία παρόλο που δεν έχει ερευνητικό χαρακτήρα αναφέρει όσο πιο αναλυτικά γίνεται τη σημασία των συστημάτων ασφαλείας στο Διαδίκτυο των Πραγμάτων και φυσικά τις προτάσεις για αντιμετώπιση τους. Δεδομένου των μεγάλων επενδύσεων που έχουν γίνει, γίνονται και θα συνεχίσουν να γίνονται στον τομέα της κυβερνοασφάλειας η εργασία έχει ιδιαίτερο ενδιαφέρον, διότι προβάλλει τα βασικά σημεία παραβιάσεων ασφαλείας στις επιθέσεις στις οποίες πραγματεύεται. Σε κάθε κεφάλαιο αναφέρονται αναλυτικά τα συμπεράσματα που αφορούν τη συγκεκριμένη επίθεση. Στην παράγραφο αυτή αναφέρουμε τα κυρίαρχα συμπεράσματα. Συνεπώς από τη μελέτη αναφέρονται συμπεράσματα που αφορούν στους τομείς που μελετήθηκαν: α) Τομέας αυτοκίνησης β) υγειονομικός τομέας γ) τομέας ενέργειας.

- Σαν κοινό συμπέρασμα διαπιστώθηκε ότι σε όλους τους τομείς οι επιθέσεις έχουν άμεση οικονομική επίπτωση, είτε σε ιδιώτες είτε σε δημόσιες δομές.

- Όσον αφορά την αυτοκίνηση διαπιστώθηκε ότι το σύστημα διαχείρισης πληροφορίας (Infotainment system) ενός αυτοκινήτου προσβάλετε πολύ εύκολα. Αυτό μπορεί να οδηγήσει σε λάθος πληροφορίες όσον αφορά τη λειτουργία του οχήματος πχ. λάθος εκτίμηση της απόστασης από το προπορευόμενο όχημα, λάθος ενεργοποίηση των φρένων, η αλλαγή ραδιοφωνικών σταθμών ή αυξομείωση της έντασης του ραδιοφώνου χωρίς την παρέμβαση του οδηγού κ.α. Οι αναλύσεις SAST και IAST προτείνονται σαν κύριοι τρόποι αντιμετώπισης των επιθέσεων αυτού του τύπου.

- Όσον αφορά τα συστήματα ελέγχου κυκλοφορίας διαπιστώθηκε ότι είναι δυνατό να παραβιαστούν με πάρα πολύ απλά και φθηνά τεχνικά μέσα, ως αποτέλεσμα τούτου να προκληθεί κυκλοφοριακό χάος ή και ατυχήματα.

- Οι τομείς υγείας επίσης είναι πολύ ελκυστικοί στους διαδικτυακούς εισβολείς. Επίσης συμπεράναμε ότι με πολύ απλά τεχνικά μέσα μπορεί να γίνει εισβολή σε εμφυτεύσιμα καρδιακά συστήματα που αφορούν ασθενείς (ιδιώτες δηλαδή) αλλά και ολόκληρα ενδονοσοκομειακά IoT ιατρικά συστήματα.

- Όσον αφορά τα εμφυτεύσιμα καρδιακά συστήματα και δεδομένης της ομοιότητας των ευρημάτων σε διαφορετικούς προμηθευτές, ο προσδιορισμός κοινών ευάλωτων σημείων στην εφαρμογή της συσκευής, μπορεί να προβάλει τις κοινές αυτές ευπάθειες και να εξεταστούν και κοινοί τρόποι αντιμετώπισης αυτού του είδους των επιθέσεων.

- Όσον αφορά τα νοσοκομεία για την αντιμετώπιση των MEDJACK, όπως διαπιστώθηκε είναι πολύ δύσκολο να ανιχνευθεί και να αντιμετωπιστεί η εισβολή εάν ένας εισβολέας ανιχνεύσει ένα τρωτό σημείο σε μια ιατρική συσκευή. Για τις περιπτώσεις αυτές προτείνετε η πλήρη συνεργασία του νοσοκομείου με τον κατασκευαστή της συσκευής. Σαν μια λύση προτείνετε η διεξαγωγή τριμηνιαίων επιθεωρήσεων από τους κατασκευαστές των ιατρικών συσκευών, η καλύτερη εκπαίδευση του προσωπικού όσον αφορά τα ηλεκτρονικά συστήματα.

- Σχετικά με τα συστήματα ενέργειας γίνεται κατανοητό ότι η πιθανότητα επιθέσεων επηρεάζει τόσο τον οικονομικό όσο και τον κοινωνικό τομέα μια ολόκληρης περιοχής. Οι επιθέσεις αυτού του τύπου είναι συγχρονισμένες και οι εισβολείς μέσω των συστημάτων SCADA μπορούν να προκαλέσουν διακοπές ρεύματος ή και απενεργοποίηση του συστήματος SCADA ενός ενεργειακού σταθμού και των επικοινωνιών αυτού με τους πελάτες του. Οι επιθέσεις στη Ουκρανία ήταν οι πρώτες που έγιναν ευρέως γνωστές στον κόσμο σαν επιθέσεις σε κρίσιμες εθνικές υποδομές. Ως τρόπος αντιμετώπισης ειδικά για την περίπτωση της Ουκρανίας προτάθηκε η δημιουργία ενός οργανισμού ο οποίος επιτρέπει την ανταλλαγή πληροφοριών μεταξύ των ενεργειακών σταθμών, όπου τελικά οδήγησε στην έγκαιρη ανίχνευση επιθέσεων.

ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΜΕΛΛΟΝΤΙΚΕΣ ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ

Στην παράγραφο αυτή επιχειρείται να δοθούν κάποια σημεία όπου οι ερευνητές στην κυβερνοασφάλεια θα μπορούσαν να ασχοληθούν μελλοντικά.

1) Μετεξέλιξη των συστημάτων SAST και IAST.

2)Την μετεξέλιξη των IoT συστημάτων από την 4^{η} Βιομηχανική επανάσταση στην 5^{η} Βιομηχανική επανάσταση.

3) Έρευνα που αφορά το χώρο της κυβερνοασφάλειας στα δίκτυα των εταιρειών λόγω της αυξητικής τάσης της τηλεργασίας εξαιτίας της πανδημίας COVID-19.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Α) Αγγλική

Burleson W. and Fu K., Design Challenges for Secure Implantable Medical Devices, Proceedings of the 49th Annual Design Automation Conference, 2012.

Halperin D., Heydt-Benjamin T., Ramsford B., Clark S., Defend B., Morgan W., Fu K., Kohno T. and Maisel W., Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008.

Hei X., Du X., Wu J. and Hu F., Defending Resource Depletion Attacks on Implantable Medical Devices, Proceedings of the 2010 IEEE Global Telecommunications Conference, 2010.

Maisel W. and Kohno T., Improving the Security and Privacy of Implantable Medical Devices, The New England Journal of Medicine, vol. 362(13), pp. 1164-1166, 2010

Marin E., Singelee D., Garcia F., Chothia T., Willems R., Preneel B., On the (in)Security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them, Proceeding of the Annual Computer Security Applications Conference, 2016.

Miller C. and Valasek C., "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, vol. 2015, 2015

Rios and Butts J. Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies , WhiteScope report, 2017

Slotwiner D., Varma N., Akar J., Annas G., Beardsall M., Fogel R., Galizio N., Glotzer T., Leahy R., Love C., McLean R., Mittal S., Moricheli L., Patton K., Raitt M., Ricci R., Rickard J., Schoenfeld M., Serwer G., Shea J., Varosy P., Verma A. and Yu C., HRS Expert Consensus Statement on Remote Interrogation and Monitoring for Cardiovascular Implantable Electronic Devices, Heart Rhythm Society, Washington, DC, May 23, 2015

TrapX Research, Labs, "Anatomy of Attack: MEDJACK.2 – Hospitals Under Siege," TrapX Investigative Report, 2016

Β) Ιστοσελίδες

Charette R. This car runs on code. Online: http://www.spectrum.ieee.org/feb09/7649, Feb. 2009.

Emaus B. Hitchhiker's Guide to the Automotive Embedded Software Universe, 2005. Keynote Presentation at SEAS'05 Workshop, available at: http://www.inf.ethz.ch/personal/pretscha/events/seas05/bruce_emaus_keynote_050521.pdf.

Goodwin A.. Ford Unveils Open-Source Sync Developer Platform. Online: http://reviews.cnet.com/8301-13746_ 7-10385619-48.html, Oct. 2009

Mollman S. From cars to TVs, apps are spreading to the real world. Online: http://www.cnn.com/2009/TECH/10/08/apps. realworld/, Oct. 2009

CAMP Vehicle Safety Communications 2 Consortium. Cooperative intersection collision avoidance system limited to stop sign and traffic signal violations midterm phase i report, Oct. 2008. Online: http://www.nhtsa.dot.gov/staticfiles/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2008/811048.pdf.

CAMP Vehicle Safety Communications 2 Consortium. Vehicle safety communications — applications first annual report, Sept. 2008. Online: http://www.intellidriveusa.org/ documents/09042008-vsc-a-report.pdf.

CAMP Vehicle Safety Communications Consortium. Vehicle safety communications project task 3 final report, Mar. 2005. Online: http://www.intellidriveusa.org/documents/ vehicle-safety.pdf

Virginia Tech Transportation Institute. Intersection collision avoidance — violation task 5 final report, Apr. 2007. Online: http://www.intellidriveusa.org/documents/ final-report-04-2007.pdf.

http://illmatics.com/remote%20attack%20surfaces.pdf

http://illmatics.com/content.zip

http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf

http://www.f-secure.com/vulnerabilities/SA201106648

http://www.autosec.org/pubs/cars-usenixsec2011.pdf

http://www.ars2000.com/Codenomicon_wp_Fuzzing.pdf

https://labs.integrity.pt/articles/from-0-day-to-exploit-buffer-overflow-in-belkin-n750-cve-2014-1635/

http://www.autosec.org/pubs/cars-usenixsec2011.pdf

http://www.driveuconnect.com/system/2014/ramtrucks/ram_1500/8-4an-ra4/

http://www.allpar.com/corporate/tech/uconnect.html

http://forums.motortrend.com/70/8102478/the-general-forum/ferrari-california-navigation-chrysler-uconnect/index.html

http://www.driveuconnect.com/software-update/

http://www.qnx.com/developers/docs/6.3.0SP3/ide_en/user_guide/builder.html

http://www.qnx.com/developers/docs/660/index.jsp?topic=%2Fcom.qnx.doc.neutrino.sys_arch%2Ftopic%2Ffsys_ETFS.html

https://www.synopsys.com/glossary/what-is-connected-car-cyber-security.html#2

https://techspective.net/2017/08/16/safety-security-open-source-automotive-industry/

https://www.computerworld.com/article/2951489/hacker-hundreds-of-thousands-of-vehicles-are-at-risk-of-attack.html

https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Cesar-Cerrudo-Hacking-Traffic-Control-Systems.pdf

https://www.youtube.com/watch?v=_j9lELCSZQw

https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

http://news.finance.ua/ua/news/-/366136/hakery-atakuvaly-prykarpattyaoblenergo-znestrumyvshy-polovynu-regionu-na-6-godyn

http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

http://www.oe.if.ua/showarticle.php?id=3413

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html

https://www.rbc.ua/rus/news/pravitelstva-ssha-ukrainy-rassmotryat-otchet-1454113214.htm

For a discussion around the history of the BlackEnergy 3 malware and Sandworm team see the SANS ICS webcast with iSight here: https://www.sans.org/webcasts/analysis-sandworm-team-ukraine-101597

http://mpe.kmu.gov.ua/minugol/control/uk/publish/article;jsessionid=CE1C739AA046FF6BA00FE8E8A4D857F3.app1?art id=24508688 6&cat id=35109

To learn about serial to ethernet converters and the types of vulnerabilities that exist to them see DigitalBond's Basecamp report here: https://www.digitalbond.com/blog/2015/10/30/basecamp-for-serial-converters/

http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-mediaorganization

http://www.eset.com/int/about/press/articles/malware/article/eset-finds-connection-between-cyber-espionage-and-electricityoutage-in-ukraine/

http://galcomcomp.com/index.php/ru/nashi-proekty/15-proekt3-material-ru

http://mobile.reuters.com/article/idUSKCN0VL18E

https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

For a good discussion on exploits and malicious firmware updates for industrial ethernet switches see the research by Eireann Leverett, Colin Cassidy, and Robert M. Lee in the DEFCON presentation "Switches Get Stitches" here: https://www.youtube.com/watch?v=yaY3rtA37Uc