ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Firmware

ΠΑΝΤΕΛΕΗΜΩΝ ΠΡΩΙΟΣ
ice18390023
6ο Εξάμηνο
ice18390023@uniwa.gr

Τμήμα ΑΣΦ09

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

Υπεύθυνοι καθηγητές

ΛΙΜΝΙΩΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ
ΙΩΑΝΝΑ ΚΑΝΤΖΑΒΕΛΟΥ

Τμήμα Μηχανικών και Πληροφορικής Υπολογιστών
14 Ιουνίου 2021

Περιεχόμενα

Κατάλογος σχημάτων

1 Τι είναι το firmware

Το firmware στα ελληνικά μεταφράζεται ως υλικολογισμικό και είναι το λογισμικό το οποίο υπάρχει στις ηλεκτρονικές συσκευές [5]. Το firmware είναι προγραμματισμένο σε γλώσσα μηχανής ή συμβολική γλώσσα. Θεωρητικά, μόνο οι εταιρίες κατασκευής γνωρίζουν και ποιο συγκεκριμένα ο κατασκευαστής γνωρίζει τις δυνατότητες και τα χαρακτηριστικά της συσκευής με αποτέλεσμα να μην μπορεί κάποιος άλλος να το προγραμματίσει εκτός από τον ίδιο. Εν ολίγοις, το firmware είναι ο κώδικας του υλικού για να φέρει εις πέρας τις επιθυμητές λειτουργίες, οι οποίες έχουν προγραμματιστεί από τον κατασκευαστεί ώστε να εκτελεί το hardware.

Σχήμα 1.1: ROM BIOS firmware on a Baby AT motherboard (source wikipedia)

2 Επίθεση firmware

Με αυτήν την επίθεση, ο επιτιθέμενος μαζεύει διαφορές πληροφορίες για το υλικό των συσκευών του στόχου, όπως

- έκδοση (version)
- ρυθμίσεις (configuration)

και διάφορες άλλες ευαίσθητες πληροφορίες, με σκοπό τον εντοπισμό ευπαθιών του firmware μέσα από αναζήτηση στο διαδίκτυο ή με την βοήθεια του γνωστού εργαλείου metasploit. Κυριότερα γίνεται με επίθεση στον πυρήνα (kernel) ή με φυσική επίθεση (physical attack) στο υλικό [2].

3 Επιτυχημένη επίθεση firmware

Τον Μάιο του 2020, ο ερευνητής υπεύθυνος ασφαλείας Björn Ruytenberg του πανεπιστημίου τεχνολογίας του Εδιμβούργου στην Ολλανδία, ανακοίνωσε την ανακάλυψη του Thunderspy, μια σειρά ευπαθιών στην τεχνολογία Thunderbolt. Η επίθεση αυτή άλλαζε το επίπεδο ασφαλείας στην διεπαφή της Thunderbolt θύρας του υπολογιστή με αποτέλεσμα την κλοπή δεδομένων ακόμα και αν ο δίσκος ήταν κρυπτογραφημένος [3].

Όπως αναφέρει, η επίθεση Thunderspy είναι πλήρως κρυφή διότι δεν υπάρχει κάποιο phishing link ή κακόβουλος κομμάτι hardware όπου ο επιτιθέμενος ξεγελά το θύμα ώστε να το χρησιμοποιήσει. Το μόνο που χρειάζεται ο επιτιθέμενος είναι 5 λεπτά με τον υπολογιστή, ένα κατσαβίδι και μία θύρα [4].

4 Αποτροπή επιθέσεων firmware

Η επιθέσεις firmware είναι ποίο δύσκολες να εντοπισθούν και να αποφευχθούν διότι είναι σε χαμηλό επίπεδο. Το κυριότερο πρόβλημα που συμβαίνουν αυτές οι επιθέσεις είναι πως οι εταιρίες δεν υπολογίζουν στο budget τους την ανάπτυξη ασφαλέστερων firmware. Ένας ακόμα σημαντικός παράγοντας, είναι πως οι χρήστες δεν συνειδητοποιούν πως υπάρχει νέο firmware update ή δεν γνωρίζουν την ύπαρξη του ή ακόμα δεν ξέρουν πως να το κάνουν χωρίς να φοβούνται πως θα καταστρέψουν κάτι με το περίεργο gui interface όπως του BIOS. Η τρόποι αποφυγής τέτοιων επιθέσεων είναι οι εξής [1]

- Ανανέωση στην τελευταία έκδοση firmware σε όλες τις συσκευές
- Προσοχή με προγράμματα malware
- Στην αγορά hardware αναζητήστε υπολογιστές και εξυπηρετητές με firmware security
- Η ασφάλεια του firmware πρέπει να είναι προτεραιότητα όπως και τα υπόλοιπα updates

5 Συμπεράσματα

Το firmware είναι μια δύσκολη αλλά πανίσχυρη επίθεση διότι αν ο επιτιθέμενος την φέρει εις πέρας, τότε θα είναι ο βασιλιάς του συστήματος. Είναι μια ιδιαίτερη επίθεση, η οποία χρειάζεται υπερβολική αφοσίωση, αναζήτηση και πολύπλευρη γνώση για να επιτευχθεί από κάποιον. Το ποίο σημαντικό είναι πως οι χρήστες δεν γνωρίζουν για το firmware ή το firmware update ή ακόμα μπορεί και να φοβούνται να δοκιμάσουν να αναβαθμίσουν κάτι σε ένα gui περιβάλλων το οποίο δεν πολύ καταλαβαίνουν. Αυτό έχει ως αποτέλεσμα να έχουν κάποια έκδοση με γνωστές ευπάθειες έτσι ώστε να γίνονται εύκολος στόχος. Ωστόσο, σε επίπεδο εταιρίας οι υπεύθυνοι γνωρίζουν προφανώς κάποιες από τις ευπάθειες αυτές αλλά δεν κάνουν αναβάθμιση επειδή δεν προβλέπεται από τα budget των εταιριών.

Αναφορές

[1] Nathan Drager. Firmware attack prevantion. https://quantumpcs.net/firmware-attacks-are-up/.

[2] Richard Gall. Firmware attacks. https://blog.macrium.com/what-are-firmware-attacks-and-why-are-they-growing-90e54cb0eda2.

[3] Aryeh Goretsky. Thunderspy attack. https://www.welivesecurity.com/2020/07/30/thunderspy-attacks-what-they-are-whos-at-greatest-risk-how-to-stay-safe/.

[4] Björn Ruytenberg. Breaking Thunderbolt Protocol Security: Vulnerability Report, 2020. Public version.

[5] Wikipedia. Firmware. https://en.wikipedia.org/wiki/Firmware.