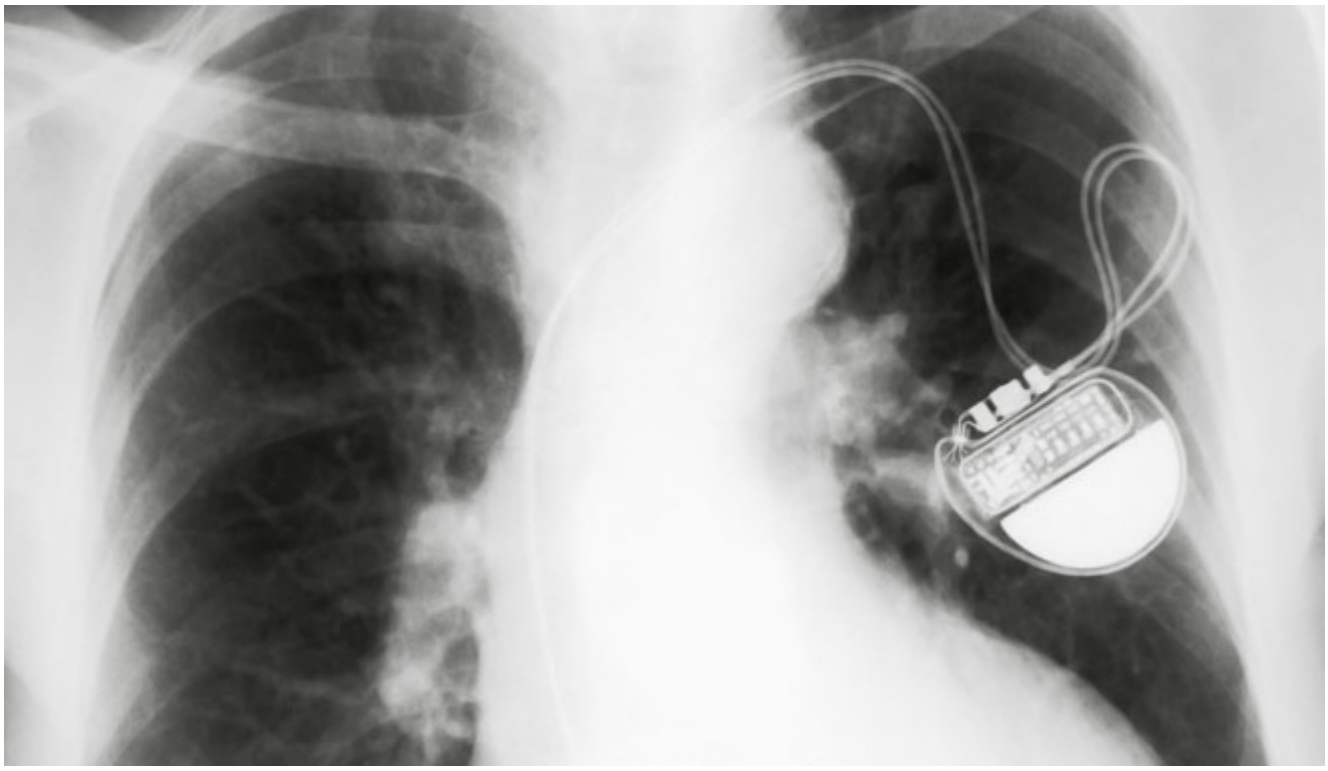
29 Δεκεμβρίου 2015

Ιατρικές συσκευές στην υπηρεσία ηλεκτρονικής απάτης: Ransomware…

/ Πεμπτουσία

Image not found or type unknown



Φανταστείτε έναν ασθενή που έχει βηματοδότη, ξαφνικά να λαμβάνει ένα μήνυμα στο κινητό του που θα λέει: «Θέλετε να συνεχίσετε να χρησιμοποιείτε το βηματοδότη σας; Πληρώστε μας 2 bitcoins.» Αυτό μπορεί να σας φαίνεται παράξενο, αλλά είναι μια κατάσταση που μπορεί να συμβεί στο εγγύς μέλλον.

Ακόμα και τις ιατρικές συσκευές, αυτές που μας βοηθούν να σώσουμε ζωές, μπορούν να εκμεταλλευτούν οι χάκερς, καθώς μπορούν να αντιμετωπίσουν τα ίδια προβλήματα ασφαλείας που αντιμετωπίζουν και οι κανονικοί υπολογιστές, οπότε η μόλυνση με ransomware είναι ένα πιθανό σενάριο!

Μια έκθεση που εκδόθηκε από τη Forrester και κυκλοφόρησε πριν από μερικές ημέρες, προβλέπει ότι το 2016 θα αρχίσουμε να βλέπουμε τα ransomware να επωφελούνται από ιατρικές συσκευές. Είναι μια τολμηρή πρόβλεψη από την έκθεση

«Predictions 2016: Cybersecurity Swings To Prevention», αλλά και είναι κάτι που ήδη έχουμε θεωρήσει πιθανό.

Το ICS-ALERT-13-164-01, από το 2013 που έγινε από τους Rios και Terry McCorkle έδειξε ότι 300 ιατρικές συσκευές που χρησιμοποιούν δύσκολους κωδικούς πρόσβασης, οι οποίοι έχουν οριστεί από το εργοστάσιο και που δεν μπορούν να απενεργοποιηθούν ή να τροποποιηθούν, αυτοί οι κωδικοί πρόσβασης διαχωρίζονται στο εγχειρίδιο του κατασκευαστή.

Η αλήθεια είναι ότι η έννοια της ασφάλειας στον κυβερνοχώρο υπάρχει ίσως κατά τα τελευταία 15-25 χρόνια, αλλά πρόκειται για κάτι νέο στον ιατρικό κλάδο, όπως δηλώνει ο Joshua Corman, ιδρυτής του "I Am the Cavalry": «Καθώς κάνουμε αυτή τη δουλειά στον κυβερνοχώρο για 15-25 χρόνια, αυτό είναι το έτος μηδέν ή ένα για αυτούς [τη βιομηχανία υγειονομικής περίθαλψης]» και συνεχίζει «Δεν μπορούμε να τους δώσουμε 15-25 χρόνια για να καλύψουν τη διαφορά, αν και δεν είναι λογικό να φτάσουν στο ίδιο σημείο μέσα σε μια νύχτα... Προσπαθούμε να προσεγγίσουμε το θέμα με ομαδική εργασία και πρεσβευτικές ικανότητες, και όχι ως ένα δάχτυλο που δείχνει, αλλά ως ένα χέρι βοήθειας.»

Το Ransomware είναι μια τεράστια επιχείρηση και οι μεγάλοι προμηθευτές ασφαλείας δηλώνουν ότι το 2015 είχαν μια τεράστια αύξηση στη χρήση ransomware, η οποία τείνει να χρησιμοποιηθεί περισσότερο με τις IoT συσκευές. Μερικούς μήνες πριν, ένας κατάλογος αναπτύχθηκε από την "I Am the Cavalry", που είχε δημιουργηθεί για να μετριάσει την απειλή στα αυτοκίνητα και τώρα σχεδιάζουν τον ίδιο τύπο λίστας, αλλά αυτή τη φορά για τις Ιατρικές Συσκευές.

Υπάρχουν πολλές προκλήσεις, όταν ασχολείσαι με ιατρικές συσκευές, αλλά εδώ έχουμε να κάνουμε με κάτι καινούριο. Ωστόσο, επειδή πολλοί είναι εκείνοι που κατανοούν τον κίνδυνο, είναι βέβαιο ότι πολλοί ερευνητές ασφαλείας θα εστιάσουν την προσοχή τους σε αυτόν τον τομέα.

Πηγή: secnews.gr

Σημείωση: το ransomware είναι ένα είδος κακόβουλου λογισμικού που κλειδώνει την οθόνη του υπολογιστή σας και ζητά κάποιο αντάλλαγμα – λύτρα (ransom=λυτρα), συνήθως ένα χρηματικό ποσό ή κάποιον κωδικό ασφαλείας, προκειμένου να την ξεκλειδώσει. Συνήθως φαίνεται σαν να προέρχεται από κάποιον κρατικό οργανισμό ή άλλη υπηρεσία. Εννοείται ότι σε καμιά περίπτωση δεν πρέπει κανείς να υποκύψει στις απαιτήσεις ενός τέτοιου λογισμικού, αλλά θα πρέπει να αναζητήσει τη λύση σε κάποιο λογισμικό απομάκρυνσής του από τον υπολογιστή.