3 Δεκεμβρίου 2015

Προ-εγκατεστημένος ιός σε κάμερες της αστυνομίας!

/ Πεμπτουσία

Image not found or type unknown

Φωτ.: Depositphotos

Η iPower Technologies με έδρα τις ΗΠΑ έχει ανακαλύψει ότι οι κάμερες σώματος που πωλούνται από την Martel Electronics έρχονται με προ-εγκατεστημένο τον ιό τύπου Conficker worm (Win32 / Conficker.B!inf). Η συγκεκριμένη γραμμή των καμερών σώματος iPower ελέγχθηκε και είναι η ίδια με εκείνη που πωλείται στις αστυνομικές δυνάμεις των ΗΠΑ, η οποία χρησιμοποιείται από αξιωματικούς που κάνουν περιπολίες στον δρόμο και από τα μέλη της ομάδας SWAT στις επιχειρήσεις τους.

Το μοντέλο, Frontline Body Camera, βρίσκεται στο στήθος ενός αστυνομικού και λειτουργεί καταγράφοντας τις δραστηριότητές του σε βίντεο, τη θέση του, χρησιμοποιώντας ένα GPS tracker και παίρνοντας τακτικά στιγμιότυπα ως εικόνες. Η κάμερα καταγράφει τα δεδομένα σε μια εσωτερική μονάδα, απ” όπου ο αξιωματικός ή οι προϊστάμενοί του μπορούν να το κατεβάσουν σε έναν υπολογιστή

μέσω καλωδίου USB.

Σύμφωνα με τον λογαριασμό της iPower, σε εκείνο το σημείο είναι που εντόπισαν τη μόλυνση. Η IT ομάδα της εταιρείας αξιολογεί μια νέα παρτίδα καμερών σώματος που μόλις είχαν λάβει από την Martel και αφού την άνοιξαν και τη συνέδεσαν με έναν υπολογιστή, ειδοποιήθηκαν από την ασφάλειά τους για την Conficker μόλυνση.

Σχετικά με το κακόβουλο λογισμικό, ο Conficker είναι ένας δεινόσαυρος σε σύγκριση με τις τρέχουσες απειλές. Οι περισσότερες μηχανές antivirus το ανιχνεύουν σήμερα και πολύ λίγες εγκληματικές ομάδες το χρησιμοποιούν εξαιτίας αυτού. Αν τελικά το κάνουν, συνήθως το αναπτύσσουν για να βοηθήσουν τη διάδοση μολύνσεων, μιας και ο Conficker είναι πολύ ικανός στο να εξαπλωθεί γρήγορα σε τοπικά δίκτυα και να απενεργοποιήσει την τοπική προστασία. Επιπλέον, καθώς το ποσοστό ανίχνευσής του είναι υψηλό, ο Conficker μπορεί να είναι πολύ χρήσιμος, ειδικά σήμερα, εξαιτίας των όλο και περισσότερων IoT (Internet of Things) συσκευών.

Δεδομένου ότι σχεδόν καμία συσκευή IoT δεν μπορεί να τρέξει προϊόντα ασφαλείας και συνήθως προγραμματίζονται χωρίς να δίνουν πάρα πολύ προσοχή σε μέτρα αυτοπροστασίας, ο Conficker μπορεί να είναι τόσο αποτελεσματικός το 2015, όπως ήταν το 2008 και το 2009.

Ενώ ο ιός τύπου worm είναι σχεδόν άχρηστος σε προσωπικούς υπολογιστές, επειδή οι ενσωματωμένες ενημερωμένες εκδόσεις ασφαλείας τον περιλαμβάνουν στα Windows εδώ και πολύ καιρό, ο σύγχρονος εξοπλισμός που είναι συνδεδεμένος με το Internet είναι έτοιμος για τη λήψη.

Η iPower είπε ότι επικοινώνησε με την Martel, αλλά δεν έλαβε απάντηση πριν προχωρήσει στη δημοσίευση των ευρημάτων τους μια ημέρα αργότερα. Παρακάτω ακολουθεί ένα βίντεο για του λόγου του αληθές που καταγράφηκε από την ομάδα του iPower.

Πηγή: secnews.gr