6 Δεκεμβρίου 2020

Πώς θα καταλάβω αν κάποιος με παρακολουθεί μέσω web κάμερας;

/ Επιστήμες, Τέχνες & Πολιτισμός

Από τον Παντελή Ταμπακόπουλο,

Στις μέρες μας, εν μέσω καραντίνας, η χρήση των καμερών είναι πιο συχνή και σε αρκετές περιπτώσεις επιβαλλόμενη, κυρίως λόγω της τηλεργασίας. Παρά το ότι υπάρχουν χαρακτηριστικά σημάδια παρακολούθησης όπως το «πάγωμα» του υπολογιστή ή του κινητού τηλεφώνου, η εμφάνιση άγνωστων προγραμμάτων στη συσκευή που “επιβραδύνουν” σημαντικά τη δουλειά της ή ακόμη και η αυθόρμητη ενεργοποίησή της κάμερας (αν και πολλές φορές ενδέχεται να μην είναι αναμμένη η φωτεινή ένδειξη λειτουργίας της, ενώ θα καταγράφει τι συμβαίνει γύρω), γίνεται ολοένα και πιο δύσκολο να καταλάβετε αν σας παρακολουθεί κάποιος μέσω της web κάμερας του υπολογιστή, του κινητού ή ακόμη και της Smart TV σας.

Πως όμως μπορούν οι κυβερνοεγκληματίες να αποκτήσουν πρόσβαση στην κάμερα σας; Χρησιμοποιώντας, ως επί το πλείστον, μεθόδους εξαπάτησης phishing αλλά και άλλες αναγνωρίσιμες τεχνικές, για να εγκαταστήσουν εργαλεία απομακρυσμένης πρόσβασης, μέσω των οποίων αποκτούν την πρόσβαση. Το κακόβουλο λογισμικό γνωστό και ως RAT (Remote Access Tool) όχι μόνο επιτρέπει στους κυβερνοεγκληματίες να «βλέπουν» μέσα από τις κάμερες των συσκευών που έχουν παραβιαστεί, αλλά υπάρχει και μία κατηγορία εγκληματιών γνωστή ως «Ratters», οι οποίοι πωλούν πρόσβαση σε αυτές μέσω ιστότοπων στο Dark Web.

Εάν ανησυχείτε ότι κάποιος μπορεί να χρησιμοποιήσει την web κάμερα σας για να σας κατασκοπεύσει, δεν είστε οι μόνοι. Μερικά χρόνια πριν, εμφανίστηκε μια φωτογραφία του Mark Zuckerberg η οποία έδειχνε το laptop του στο παρασκήνιο,

όπου φαίνονταν ότι πάνω στην κάμερα, είχε κολλήσει ένα μικρό κομμάτι ταινίας. Η εικόνα προκάλεσε πολλή συζήτηση εκείνη την εποχή διότι ενώ ο συγκεκριμένος είναι το αφεντικό μιας εκ των μεγαλύτερων τεχνολογικών εταιρειών παγκοσμίως (Facebook), η οποία διαθέτει από τις καλύτερες τεχνολογικές υπηρεσίες υποστήριξης στον κόσμο, ανησυχούσε για τυχόν εισβολείς μέσω της κάμερας του.

Το να κολλήσετε, ένα αυτοκόλλητο πάνω στην κάμερα σας είναι ένας τρόπος για να προφυλαχτείτε από αυτές τις επιθέσεις, αλλά δεν σας εξασφαλίζει 100%, διότι οι περισσότερες κάμερες καταγράφουν και ήχο.

Αλλά πώς μπορείτε να καταλάβετε εάν η web κάμερα σας έχει παραβιαστεί; Λοιπόν, υπάρχουν μερικά σημάδια που πρέπει να προσέξετε.

Ελέγξτε την ενδεικτική λυχνία της κάμερας
Οι περισσότερες web κάμερες διαθέτουν ενδεικτική λυχνία, ακόμη και εκείνες που είναι ενσωματωμένες σε φορητούς υπολογιστές. Αυτή η λυχνία ανάβει κατά την λειτουργία της κάμερας. Με μια ποιοτική κάμερα, είναι πραγματικά πολύ δύσκολο για έναν εισβολέα να σας κατασκοπεύσει χωρίς να θέσει σε λειτουργία αυτή την λυχνία. Αν λοιπόν αυτή είναι αναμμένη ενώ η κάμερα δεν είναι σε λειτουργία, υπάρχει μια καλή πιθανότητα να έχετε πέσει θύμα παραβίασης.

Ελέγξτε τα αρχεία σας
Οι περισσότερες παραβιάσεις καμερών βασίζονται στην περιορισμένη γνώση του μέσου χρήστη. Αυτό έχει σαν αποτέλεσμα, πολλοί εγκληματίες που παραβιάζουν Web κάμερες δεν προσπαθούν καν να αποκρύψουν τις δραστηριότητές τους. Οι περισσότεροι χρήστες δεν γνωρίζουν πού αποθηκεύονται τα αρχεία που καταγράφει η κάμερα στο δικό τους σκληρό δίσκο. Μάθετε πού αποθηκεύονται τα αρχεία αυτά (από τις ρυθμίσεις της κάμερας) και ελέγξτε το φάκελο. Εάν π.χ. δείτε έναν αριθμό αρχείων βίντεο που δεν καταγράψατε, πιθανότατα έχετε παραβιαστεί.

Έλεγχος για ύποπτες εφαρμογές
Η πλειοψηφία των ηλεκτρονικών εισβολέων ενεργεί μέσω κακόβουλου λογισμικού. Το κακόβουλο λογισμικό εκτελείται ως διαδικασία στην συσκευή σας χωρίς να το αντιληφθείτε (έως ότου εμφανιστούν εικόνες από την web κάμερα στο Διαδίκτυο). Επειδή μπορεί να είναι δύσκολο για τον μέσο χρήστη να διακρίνει το κακόβουλο λογισμικό από τα άλλα λογισμικά του συστήματος, ο πιο απλός τρόπος είναι αφού επανεκκινήσετε τον υπολογιστή σας και ανοίξετε την διαχείριση εργασιών (Task manager) του συστήματός σας να δείτε τη λίστα των διαδικασιών, προτού φορτώσετε οτιδήποτε άλλο. Όλες οι διεργασίες πρέπει να είναι βασικά αδρανείς (δηλαδή να μην χρησιμοποιούν πόρους επεξεργασίας). Εάν δείτε μια διαδικασία

που εκτελείται, είναι πιθανώς κακόβουλο λογισμικό.

Σάρωση για κακόβουλο λογισμικό
Ένας άλλος τρόπος για να εντοπίσετε και να απαλλαγείτε από τυχόν κακόβουλο λογισμικό είναι να προμηθευτείτε ένα έγκριτο λογισμικό ασφαλείας τύπου Internet Security και να εκτελείτε τακτικά σάρωση του υπολογιστή ή του κινητού σας. Υπάρχουν πολλά διαθέσιμα στην αγορά και ένα αγορασμένο έγκριτο Internet Security διαθέτει τα απαραίτητα εργαλεία εντοπισμού κακόβουλου λογισμικού στις περισσότερες περιπτώσεις. Απλώς βεβαιωθείτε ότι διατηρείτε ενημερωμένο το λογισμικό ασφαλείας σας, επειδή εμφανίζονται συνεχώς νέα κακόβουλα λογισμικά και το λογισμικό σας πρέπει να είναι σε θέση να τα αναγνωρίσει.

Ελέγξτε την κυκλοφορία του δικτύου σας
Εάν κάποιος χρησιμοποιεί την web κάμερα σας για να σας κατασκοπεύσει, θα πρέπει να στείλει τα δεδομένα αυτά μέσω του οικιακού δρομολογητή (Router) σας. Εάν συνδεθείτε στο δρομολογητή σας ή με ένα απλό πρόγραμμα παρακολούθησης της διακίνησης των δεδομένων σας, μπορείτε να δείτε την ταχύτητα με την οποία στέλνετε και λαμβάνετε δεδομένα. Κλείστε όλες τις εφαρμογές και τα παράθυρα του προγράμματος περιήγησής σας, ώστε να μην χρησιμοποιείτε δεδομένα και εάν εξακολουθούν να περνούν πολλά από το δίκτυο, ίσως κάποιος να έχει παραβιάσει τον υπολογιστή σας. Βέβαια αυτό ίσως να μην οφείλεται στην παραβίαση της κάμερα σας αλλά θα μπορούσατε να είστε μέρος ενός botnet ή να έχετε παραβιαστεί για διαφορετικό λόγο.

Ελέγξτε τις ρυθμίσεις ασφαλείας σας
Ένα ακόμη ενδεικτικό σημάδι ότι η web κάμερα σας έχει παραβιαστεί είναι εάν οι ρυθμίσεις ασφαλείας της είναι λίγο «παράξενες». Ανοίξτε τις ρυθμίσεις της κάμερας και ρίξτε μια ματιά. Εάν δεν μπορείτε να αλλάξετε αυτές τις ρυθμίσεις μόνοι σας, λόγω απώλειας των δικαιωμάτων σας ή εάν το όνομα του λογαριασμού του διαχειριστή έχει αλλάξει, πιθανότατα έχετε παραβιαστεί.

Αποσυνδέστε τις κάμερες σας όταν δεν τις χρησιμοποιείτε
Πολλές φορές, για τις web κάμερες, οι πιο απλές τακτικές είναι οι πιο αποτελεσματικές. Αποσυνδέστε τις εάν μπορείτε, ή αν δεν υπάρχει αυτή η δυνατότητα, κολλήσετε ένα αυτοκόλλητο πάνω στον φακό. Πολλά μοντέρνα μοντέλα καμερών, διαθέτουν μια «ασπίδα προστασίας», συνήθως ένα πλαστικό πώμα, για να μπλοκάρουν το φακό. Αν έχετε παρόμοιο μοντέλο, χρησιμοποιήστε τον όταν η κάμερα δεν χρησιμοποιείται.

Μην ανοίγετε άγνωστους συνδέσμους (links)
Αποτελεί σύνηθες φαινόμενο να λαμβάνουμε, μέσω email ή μέσω μηνυμάτων στα

social media, ακόμη και από φίλους ή συνεργάτες, διάφορους συνδέσμους από video, φωτογραφίες, ακόμη και διαφημιστικές καμπάνιες με δελεαστικές προσφορές. Πολλές από αυτές έχει αποδειχθεί ότι εμπεριέχουν κακόβουλο λογισμικό. Μην τις ανοίγετε εάν δεν έχετε πρώτα επικοινωνήσει με τον αποστολέα και έχετε επιβεβαιώσει την πηγή.

Μια κάμερα συνδεδεμένη ή ενσωματωμένη στον υπολογιστή, στο κινητό ή την Smart TV σας, η οποία είναι συνδεδεμένη στο ίντερνετ, αποτελεί στόχο για τους κυβερνοεγκληματίες, οι οποίοι θα κάνουν το καλύτερο δυνατό για να καταγράψουν το απόρρητο του σπιτιού σας και να σας εκβιάσουν με αυτό ή ακόμη χειρότερα, να το μοιραστούν με άλλα άτομα στο διαδίκτυο. Λαμβάνοντας τα απαραίτητα μέτρα προστασίας, ελαχιστοποιείτε τον κίνδυνο και διαφυλάσσετε τα πολύτιμα προσωπικά δεδομένα σας αλλά και της οικογένειά σας.
Πηγή: csii.gr