The Athens Affair

Η ΥΠΟΘΕΣΗ

Τα έτη 2004-2005 έλαβε χώρα στην Ελλάδα ένα από τα μεγαλύτερα και σημαντικότερα τηλεπικοινωνιακά σκάνδαλα του κόσμου. Δεκάδες ήταν τα στελέχη και οι προσωπικότητες του Ελληνικού κράτους, και όχι μόνο, που υπέπεσαν στις παρακολουθήσεις της τότε εξαιρετικά έμπειρης ομάδας προγραμματιστών που εισέβαλαν στο τηλεπικοινωνιακό δίκτυο της Vodafone. Η εξέλιξη της υπόθεσης έδειξε πως η αντιμετώπιση των γεγονότων έγινε χωρίς την απαραίτητη σοβαρότητα και πως τα μέτρα ασφαλείας που προϋπήρχαν ήταν ισχνά.

ΤΕΧΝΙΚΑ ΚΑΙ ΔΙΑΔΙΚΑΣΤΙΚΑ ΖΗΤΗΜΑΤΑ

Η επίθεση και παρακολούθηση, μεγάλου αριθμού γραμμών, έγινε με την βοήθεια κακόβουλου λογισμικού το οποίο υιοθετούσε τα χαρακτηριστικά ενός rootkit λογισμικού, που κρύβει ενεργά την παρουσία του από τους διαχειριστές καθώς και από τους ελέγχους του ίδιου του συστήματος. Το πρώτο ζήτημα που προκύπτει είναι η εγκατάσταση του λογισμικού στα κέντρα μεταγωγής (switching centers) με στόχο την δυσλειτουργία του συστήματος υποστήριξης υποκλοπών (wiretapping features) και εν συνεχεία την πρόσβαση και εκμετάλλευση του. Πιο συγκεκριμένα, το κακόβουλο αυτό λογισμικό βρέθηκε εγκατεστημένο σε 4 μεταγωγούς του δικτύου της Vodafone Hellas, όπου δημιουργούσε ένα παράλληλο, αντίγραφο, ρεύμα ψηφιοποιημένων ήχων (parallel streams of digitized voice) το οποίο στην συνέχεια είτε κατέγραφαν είτε αποθήκευαν. Τα μεταγωγικά κέντρα της Vodafone ήταν συνδεδεμένα με τον τηλεπικοινωνιακό υπολογιστή μεταγωγής της Ericsson, AXE, όπου για την υπόθεση αξίζει να σημειωθεί ότι αναπτύχθηκε με την υποστήριξη της Ελληνικής εταιρείας λογισμικού IntraSoft. Ο κεντρικός επεξεργαστής του υπολογιστή αυτού δημιουργεί τις τηλεφωνικές συνδέσεις και ένας διαχειριστικός επεξεργαστής αποτυπώνει αρχεία καταγραφής (log files) στο σύστημα. Επίσης, ο υπολογιστής AXE, περιλαμβάνει ένα σύστημα διαχείρισης υποκλοπών (IMS), το οποίο δεν ήταν εγκατεστημένο στην περίπτωση της Vodafone Hellas, καθώς και ένα σύστημα απομακρυσμένου ελέγχου RMS, το οποίο βοήθησε τους επιτιθέμενους να δημιουργούν αντίγραφα των επικοινωνιών. Ταυτόχρονα, είχαν εγκατασταθεί συστήματα τα οποία απενεργοποιούσαν αρχεία καταγραφής και απέτρεπαν τους διαχειριστές να εντοπίσουν τις ενέργειες του λογισμικού που είχαν προσθέσει και με αυτόν τον τρόπο μπορούσαν να το ενημερώνουν και να το διαχειρίζονται. Για ακόμα περισσότερη μυστικότητα το εγκατεστημένο λογισμικό αποθήκευε τα παρακολουθούμενα νούμερα σε μια δική του εσωτερική μνήμη. Ωστόσο, κατά την διάρκεια μιας ενημέρωσης που συνέπεσε με την προώθηση ορισμένων μηνυμάτων δημιουργήθηκε μια αυτόματη έκθεση αποτυχίας (failure report) και έτσι οι εισβολείς δεν μπορούσαν να κρύψουν τα ίχνη τους από τους διαχειριστές. Από εκείνη την στιγμή και μετά, την επίθεση ανέλαβαν να διαλευκάνουν διάφορα κλιμάκια ασφαλείας και ελέγχου από το ελληνικό κράτος καθώς και από τις εμπλεκόμενες εταιρείες, Vodafone και Ericson. Εκ του αποτελέσματος συμπεραίνουμε πως οι παραπάνω έπραξαν βεβιασμένα βοηθώντας τους επιτιθέμενους να καλύψουν τα ίχνη τους και

οδηγήθηκαν σε ενέργειες, όπως η διαγραφή των αρχείων καταγραφής, των βιβλίων επισκεπτών στα κέντρα μεταγωγής καθώς και η διαγραφή των μολυσμένων κομματιών του λογισμικού, που απέτρεπαν την μελλοντική ανάκτηση στοιχείων για έρευνα της υπόθεσης.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Από τα παραπάνω ζητήματα που αναλύθηκαν προκύπτουν ορισμένα μέτρα προστασίας που πιθανόν να είχαν αποτρέψει και την εν λόγω επίθεση. Αρχικά, για την προστασία ενός συστήματος απαιτείται η *φυσική προστασία των συστημάτων* είτε μέσω προσωπικού είτε μέσω συστημάτων καταγραφής και παρακολούθησης. Επιπλέον, τα συστήματα πρέπει να έχουν *ως κεντρικό τους γνώμονα την ασφάλεια και την αξιοπιστία του συστήματος* και όχι το κόστος, όπως αυτό φάνηκε στην υπόθεση της Vodafone. Ταυτόχρονα, *η εγκαθίδρυση αρχών ασφαλείας με εποπτικό ρόλο* θα μπορούσαν να δίνουν συγκεκριμένες οδηγίες σε εταιρείες και οργανισμούς και παράλληλα να διατηρούν ομάδες ελέγχου, αξιολόγησης και ανάκτησης με συγκεκριμένες ευθύνες και αρμοδιότητες. Πιο συγκεκριμένα και όσον αφορά τα τεχνικά θέματα, εταιρείες όπως η Vodafone οφείλουν να εκτελούν *εκτεταμένους ελέγχους συστήματος* με σύγχρονες τεχνικές που περιλαμβάνουν εργαλεία εντοπισμού κακόβουλου λογισμικού και ξεπερνούν τα συστήματα ελέγχου του ίδιου του συστήματος. Επίσης *η αξιοποίηση όλου του πακέτου ενός συστήματος* αποδεικνύεται χρήσιμη επιλογή, όπως για παράδειγμα θα αποτελούσε κρίσιμη επιλογή η προσθήκη του συστήματος IMS από τους τεχνικούς της Vodafone. Για περεταίρω ασφάλεια θα μπορούσαν οι τεχνικοί συντήρησης συστημάτων, όπως και αυτοί της Vodafone, *να αναδρομολογούν ορισμένες διαδικασίες ή πύλες επικοινωνίας* οι οποίες αποτελούν σημείο ορισμού για κακόβουλα λογισμικά καθώς και να χρησιμοποιούν ισχυρούς κρυπτογραφικούς μηχανισμούς σε διάφορα στάδια ώστε να αχρηστεύουν τις προσπάθειες των επιτιθέμενων. Τέλος για να αποφευχθούν επιθέσεις από άτομα που έχουν γνώση του λογισμικού μπορεί οποιαδήποτε εταιρεία σε συνδυασμό με οδηγίες της εταιρείας λογισμικού *να αλλάζει ορισμένες κρίσιμες μεθόδους και διαδικασίες του λογισμικού* ανά τακτά διαστήματα ώστε αυτό να ανανεώνεται και να μην συμφωνεί με τις προδιαγραφές του κακόβουλου λογισμικού. Για παράδειγμα, στην συγκεκριμένη περίπτωση αν οι τεχνικοί είχαν απενεργοποιήσει εξ' ολοκλήρου την δυνατότητα υποκλοπών του συστήματος RMS, εφόσον δεν γινόταν χρήση του, πιθανόν να είχαν δυσκολέψει το έργο των επιτιθέμενων.

ΑΝΙΧΝΕΥΣΗ ΚΑΙ ΑΝΑΚΤΗΣΗ ΠΟΡΩΝ

Εξαιρετικά κρίσιμο ζήτημα η *ορθολογική ανίχνευση και μελέτη των κινήσεων των επιτιθέμενων* καθώς και η ανάκτηση πόρων που αξιοποίησαν ή υπέκλεψαν. Συντονισμένη και καλά σχεδιασμένη ανίχνευση, μπορεί να οδηγήσει στην αποκάλυψη των στοιχείων που αφήνουν οι επιτιθέμενοι. Στο παράδειγμα που αναλύουμε, εάν οι τεχνικοί και οι αρχές δεν είχαν δράσει βεβιασμένα και απερίσκεπτα θα μπορούσαν να είχαν λάβει δράση μέτρα εξερεύνησης και ανίχνευσης μέσω δεδομένων που στην προκειμένη περίπτωση απλώς καταστράφηκαν, όπως αρχεία καταγραφής και κομμάτια κώδικα. Τέλος, ενέργειες ανίχνευσης και καταγραφής θα μπορούσαν να αποτελέσουν η συνεννόηση με τα θύματα, η λειτουργία του ψευδούς δικτύου σε εφεδρικούς υπολογιστές με στόχο την απομόνωση του και την αποκάλυψη των προσώπων που το παρακινούσαν.