ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ ΚΑΙ ΣΥΝΑΛΛΑΓΕΣ: ΤΕΧΝΟΛΟΓΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Διπλωματική Εργασία
της
Φωστηροπούλου Ηρακλείας

Θεσσαλονίκη, 31/10/2014

ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ ΚΑΙ ΣΥΝΑΛΛΑΓΕΣ: ΤΕΧΝΟΛΟΓΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Φωστηροπούλου Ηρακλεία
Πτυχίο Μηχανικών Πληροφορικής και Τηλεπικοινωνιών Τ.Ε., Τ.Ε.Ι. Λάρισας, 2011

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Χρήστος Κ. Γεωργιάδης
Αναπληρωτής Καθηγητής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

Γεωργιάδης Χρήστος Βλαχοπούλου Μάρω Στειακάκης Εμμανουήλ

……. …….. ……

Φωστηροπούλου Ηρακλεία

……...

ΠΕΡΙΛΗΨΗ

Σκοπός της εργασίας είναι η εξαντλητική καταγραφή όλων των σχετικά πρόσφατων πηγών που σχετίζονται με την οικονομική και τεχνολογική πρόκληση που επιφέρει η εξέλιξη

της τεχνολογίας της πληροφορίας στο κομμάτι των έξυπνων συσκευών. Επίσης, η κριτική προσέγγιση τόσο των εμπλεκόμενων τεχνολογιών όσο και των οικονομικών επιπτώσεων σε χώρες της Ε.Ε. (ή ακόμη και σε ΗΠΑ, Κίνα κ.ά.). Επιπλέον, από οικολογικής πλευράς, ειδικότερη αναφορά αποσκοπεί στη διερεύνηση-μελέτη οικονομικών και τεχνολογικών στοιχείων που εμπλέκονται με την ανακύκλωση των κινητών συσκευών.

Οι στόχοι της εργασίας είναι: α) η ανακάλυψη των τελευταίων τάσεων περί των εφαρμογών, τεχνικών εξαπάτησης και κακόβουλου λογισμικού που κυκλοφορούν για τις κινητές συσκευές σε παγκόσμιο επίπεδο, β) ο εντοπισμός των κατάλληλων εφαρμογών που προορίζονται για προσωπική ή επαγγελματική χρήση, η ικανότητα αντίληψης των τρόπων εξαπάτησης που αφορούν είτε προσωπικά δεδομένα είτε χρεώσεις καθώς και η εκμάθηση τρόπων αντιμετώπισης τυχόν επιθέσεων κακόβουλου λογισμικού στο λειτουργικό σύστημα ενός κινητού τηλεφώνου ,γ) η ικανότητα αντίληψης της ψυχολογίας και του τρόπου σκέψης του κακόβουλου χρήστη.

Από περιβαλλοντικής πλευράς ορίζονται ως στόχοι η πληροφόρηση σχετικά με την επιβάρυνση που μπορεί να έχουν όλα τα παραπάνω στη φύση, η ευαισθητοποίηση ως προς την «πράσινη» χρήση κινητών συσκευών και τέλος η συμμετοχή και προώθηση της παγκόσμιας καμπάνιας ανακύκλωσης κινητών τηλεφώνων.

Η εργασία στηρίζεται πάνω στη μελέτη επιστημονικών άρθρων, ερευνών και διατριβών καθώς και σε εμπεριστατωμένα περιστατικά – περιπτώσεις υποκλοπών και εξαπατήσεων του κοινού, τα οποία βοηθούν στην ανάλυση ζωντανών παραδειγμάτων προς αποφυγή.

Οι μέθοδοι που χρησιμοποιήθηκαν για τη συγκέντρωση του υλικού ήταν κυρίως η αναζήτηση στο διαδίκτυο καθώς και η μελέτη συγγραμμάτων σε δημόσιες βιβλιοθήκες.

Τέλος, τα αποτελέσματα της έρευνας δείχνουν ότι ο -κακόβουλος- πληθυσμός (δημιουργοί κακόβουλου λογισμικού) όλο και αυξάνεται σε παγκόσμιο επίπεδο και μάλιστα με ιδιαίτερα γρήγορο ρυθμό. Από τους παραδοσιακούς Η/Υ οι επιτήδειοι στοχεύουν πλέον έντονα στις έξυπνες συσκευές. Από την άλλη μεριά κοινό και εταιρίες φαίνεται να πέφτουν ουκ ολίγες φορές θύματα, μιας και δεν υπάρχει το κατάλληλο υπόβαθρο γνώσης θεμάτων ασφαλείας. Η εξαπάτηση βέβαια είναι κάτι το αναπόφευκτο, ειδικά όταν μιλάμε για μεγάλους οργανισμούς οι οποίοι λειτουργούν με χιλιάδες ηλεκτρονικά μέσα.

Λέξεις κλειδιά: Έξυπνες συσκευές ; κακόβουλο λογισμικό ; συναλλαγές ; ανακύκλωση κινητών συσκευών.

Abstract

The purpose of this report is to set down all the relatively recent sources, which are associated with the economic and technological challenge, that comes as a result from the development of mobile phone technology. In addition, the critical approach of both the involved technologies and economical effects in countries of European Union (or even U.S.A., China, etc). Furthermore, from an ecological point of view a more specific reference aim at an investigation of economical an technological elements that are involved in the recycling of mobile devices.

The goals of this report are: i) the study of the last trends of applications, techniques deceptions and installation malware, ii) the recognition of the - applications which are appropriate for personal or professional use, - ways of deception of personal data (overcharges, unauthorized banking dealings and possible malware attacks at the operating mobile system) and - threats and their treatment, iii) the understanding of the logic of hackers' thinking.

As far as the environmental side is concerned, the goals are the information about mobile recycling, the consciousness as far as the "green" use of mobile phone is concerned and the development of thinking in accordance with the global campaign of recycling of mobile phones.

The report is based on study of scientific articles, researches and projects as well as on incidents and cases of unauthorized deception of banking and financial dealing that helps in the analysis of live examples to avoid.

The methods of gathering data were mostly the research on the internet as well as the study of books in public libraries.

Finally, according to the results the number of hackers is more and more growing up with a rapid rhythm. This comes as a result of the fact that in the end the earnings are outrageous. That is the reason that there is a deepening turn from the traditional PC malware to mobile malware. On the other hand, public seems to be tricked many times as there is no knowledge of mobile security, especially when we talk about enterprises which use a extended net of PC and mobile devices. However, the only certain thing is that in last case, the advantages are much more disadvantages.

Key-words: smart devices ; malware ; transactions ; recycling of mobile devices

ΠΡΟΛΟΓΟΣ – ΕΥΧΑΡΙΣΤΙΕΣ

Στο σημείο αυτό θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της εργασίας μου κ. Χρήστο Γεωργιάδη για τη στήριξή του ιδιαίτερα στο κομμάτι της ανεύρεσης πηγών καθώς και για την κατανόησή του σε θέματα πρακτικής φύσεως. Επίσης, θα ήθελα να ευχαριστήσω και τα μέλη της επιτροπής αξιολόγησης της εργασίας μου τα οποία αφιέρωσαν χρόνο προκειμένου να εξετάσουν μεταξύ πολλών και τη δική μου προσπάθεια.

Τέλος ένα μεγάλο ευχαριστώ στην οικογένεια και τους φίλους μου που όλον αυτόν τον καιρό βίωναν την αγωνία μου καθώς και στους εργοδότες μου Λ. Κουμπουλίδη και Φ. Κύρτσιου οι οποίοι έδειξαν πολλές φορές κατανόηση σε περιόδους που χρειάστηκε να απουσιάσω από την δουλειά λόγω της διπλωματικής μου εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1ο: Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Η εργασία διαπραγματεύεται τις οικονομικές και τεχνολογικές επιπτώσεις που επιφέρει η χρήση των κινητών συσκευών σε επιχειρήσεις – οργανισμούς και άτομα. Με άλλα λόγια, στην εργασία γίνεται ανάλυση όλων των παραγόντων που σχετίζονται με την εξέλιξη της αγοράς των έξυπνων συσκευών και τις συνέπειες που έχει η εξέλιξη αυτή στη λογική των επιτήδειων χάκερ.

Πιο συγκεκριμένα, μία προσπάθεια να καταμεριστεί ο όγκος της εργασίας σε επιμέρους κομμάτια θα κατέληγε αρχικά στο κομμάτι σχετικά με θέματα που αφορούν στις εφαρμογές κινητών συσκευών, οι οποίες συχνά αποτελούν τον κύριο παράγοντα που συντελεί στην αγορά τους. Έπειτα, ένα άλλο κομμάτι είναι οι κρυμμένες χρεώσεις που συχνά υπάρχουν ως υπηρεσίες στους λογαριασμούς των χρηστών χωρίς αυτοί να το αντιλαμβάνονται και οι υποκλοπές που λαμβάνουν χώρα κατόπιν δράσης επιτήδειων χάκερ και αφορούν στις οικονομικές τους συναλλαγές. Σχετικά ζητήματα είναι αυτά τα οποία έχουν να κάνουν με το κακόβουλο λογισμικό, τους τρόπους με τους οποίους ενεργεί και τις συνέπειες τις οποίες μπορεί να επιφέρει στο κοινό. Στην πορεία, αναλύεται η σχέση μεταξύ των επιχειρήσεων – οργανισμών και των έξυπνων συσκευών, όσων αφορά στην πολλαπλή τους χρήση από τους υπαλλήλους, οι συνέπειες που φέρει αυτή η χρήση και οι τρόποι αντιμετώπισης προβλημάτων – συμβουλές για τις επιχειρήσεις. Ένα ακόμη σημαντικό σημείο είναι η ασφάλεια και η γνώση θεμάτων ασφαλείας από το κοινό καθώς και οι φόβοι των χρηστών απέναντι σε ηλεκτρονικές απειλές. Τέλος, σημαντικό κομμάτι της εργασίας αποτελεί η καταγραφή των επιπτώσεων που έχει στο περιβάλλον η συνεχώς αυξανόμενη παραγωγή κινητών συσκευών καθώς και η ανάλυση των τρόπων με τους οποίους θα επιτευχθεί συλλογικά η ανακύκλωση των κινητών συσκευών.

1.2 Σκοπός – Στόχοι

Εστιάζοντας πρωτίστως στην οικονομική και τεχνολογική πρόκληση που επιφέρει η εξέλιξη της τεχνολογίας της πληροφορίας στο κομμάτι των έξυπνων συσκευών, σκοπός της εργασίας είναι η εξαντλητική παράθεση όλων των σχετικά πρόσφατων πηγών και η κριτική προσέγγιση τόσο των εμπλεκόμενων τεχνολογιών όσο και των οικονομικών επιπτώσεων σε χώρες της Ε.Ε. (ή ακόμη και σε ΗΠΑ, Κίνα κ.ά.). Επιπλέον, προσεγγίζοντας το θέμα από οικολογικής πλευράς, δεδομένης της αυξανόμενης τάσης του κοινού για εναλλαγή των κινητών συσκευών ανά τακτά χρονικά διαστήματα, ειδικότερη αναφορά αποτελεί η διερεύνηση-μελέτη οικονομικών και τεχνολογικών στοιχείων που εμπλέκονται στην ανακύκλωση των κινητών συσκευών.

Οι στόχοι της εργασίας είναι:

α) η ανακάλυψη των τελευταίων τάσεων περί των εφαρμογών, τεχνικών εξαπάτησης και κακόβουλου λογισμικού που κυκλοφορούν για τις κινητές συσκευές σε παγκόσμιο επίπεδο,

β) ο εντοπισμός των κατάλληλων εφαρμογών που προορίζονται για προσωπική ή επαγγελματική χρήση, η ικανότητα αντίληψης των τρόπων εξαπάτησης που αφορούν είτε προσωπικά δεδομένα είτε χρεώσεις καθώς και η εκμάθηση τρόπων αντιμετώπισης τυχόν επιθέσεων κακόβουλου λογισμικού στο λειτουργικό σύστημα ενός κινητού τηλεφώνου,

γ) η ικανότητα αντίληψης της ψυχολογίας και του τρόπου σκέψης του κακόβουλου χρήστη.

Από περιβαλλοντικής πλευράς ορίζονται ως στόχοι η πληροφόρηση σχετικά με την επιβάρυνση που μπορεί να έχουν όλα τα παραπάνω στη φύση, η ευαισθητοποίηση ως προς την «πράσινη» χρήση κινητών συσκευών και τέλος η συμμετοχή και προώθηση της παγκόσμιας καμπάνιας ανακύκλωσης κινητών τηλεφώνων.

1.3 Συνεισφορά

Η συγκέντρωση του υλικού το οποίο προέρχεται από έρευνες, επιστημονικά άρθρα και διατριβές και το οποίο σχετίζεται με τις οικονομικές προκλήσεις και επιπτώσεις της χρήσης των κινητών συσκευών από το κοινό αλλά και από μεγάλους οργανισμούς και φορείς, η ταξινόμηση των επί μέρους θεμάτων που προκύπτουν από την ανωτέρω γενική εικόνα, η παρουσίαση στατιστικών στοιχείων περί της επικρατούσας κατάστασης επί του θέματος καθώς και η αναφορά των οικονομικών στοιχείων από την ανακύκλωση κινητών τηλεφώνων, αποτελεί τη συνεισφορά της συγκεκριμένης διπλωματικής εργασίας. Επίσης, συνεισφέρει σε ένα βαθμό στην ευαισθητοποίηση του κοινού (είτε πρόκειται για μεμονωμένα άτομα είτε για μεγάλες επιχειρήσεις) στα ζητήματα ασφάλειας των έξυπνων συσκευών.

1.4 Ειδικοί όροι κακόβουλου λογισμικού:

- Collects Device Data-συγκεντρώνει πληροφορίες οι οποίες είναι ακριβείς ως προς τη λειτουργικότητα της συσκευής, όπως IMEI, IMSI, λειτουργικό σύστημα, και δεδομένα εγκατάστασης του κινητού.
- Spies on User-συγκεντρώνει σκόπιμα πληροφορίες από τη συσκευή (π.χ. από το ημερολόγιο του τηλεφώνου, ή τα μηνύματα sms που ανταλλάσει ο χρήστης) για να συνεχίσει να παρακολουθεί το χρήστη και έπειτα στέλνει τις πληροφορίες σε μια απαμακρυσμένη πηγή.
- Sends Premium SMS-στέλνει μηνύματα SMS σε premium rate αριθμούς τα οποία

χρεώνονται στον λογαριασμό κινητού του χρήστη.

- Downloader-μπορεί να κατεβάσει στην εκτεθειμένη συσκευή λογισμικά που εμπεριέχουν ρίσκο.
- Back door-ανοίγει μια πίσω πόρτα στην εκτεθειμένη συσκευή, επιτρέποντας στους επιτιθέμενους να δρουν αυθαίρετα.
- Tracks Location-συγκεντρώνει πληροφορίες GPS από τη συσκευή ειδικά για να εντοπίσει την τοποθεσία του χρήστη.
- Modifies Settings-αλλάζει τις ρυθμίσεις εγκατάστασης στην εκτεθειμένη συσκευή.
- Steals Media-κλέβει πολυμέσα, όπως εικόνες, και τις στέλνει σε μια απομακρυσμένη πηγή.
- Elevates Privileges-επιχειρεί να αποκτήσει προνόμια πέρα από τα δεδομένα (laid out) όταν εγκαθιστά μια επικίνδυνη εφαρμογή.
- Banking Trojan-καταγράφει τη συσκευή με την οποία ο χρήστης κάνει συναλλαγές banking, συγκεντρώνοντας τις ευαίσθητες λεπτομέρειες για περαιτέρω κακόβουλες δραστηριότητες.
- SEO Poisoning-στέλνει ανά διαστήματα τον browser του χρήστη σε προκαθορισμένες URLs βοηθώντας έτσι στις ταξινομήσεις της έρευνα του κακόβουλου λογισμικού.

1.5 Διάρθρωση της μελέτης

Μελετώντας κατά κύριο λόγο, πλην εξαιρέσεων που αναφέρονται κατά την έκταση της εργασίας, τη συμπεριφορά της μερίδας των ανθρώπων που βάση της «Ψηφιακής διαχωριστικής γραμμής» (όπως αποκαλείται το φαινόμενο της δυσανάλογης επίδρασης της πληροφορίας και των τεχνολογιών της επικοινωνίας σε διαφορετικές ομάδες Β.2.11) έχουν πρόσβαση στο διαδίκτυο και Η/Υ η διάρθρωση της εργασίας έχει ως εξής. Το κεφάλαιο 2 αναφέρεται στο διαδίκτυο και τις εφαρμογές τις οποίες επιλέγουν και εγκαθιστούν οι χρήστες στις κινητές τους συσκευές. Στο κεφάλαιο 3 αναφέρονται οι τρόποι με τους οποίους οι εταιρίες χρεώνουν τους χρήστες πολλές φορές εν αγνοία τους με επιπλέον χρεώσεις καθώς και η σχέση κινητών συσκευών με τις συναλλαγές των χρηστών. Στο κεφάλαιο 4 γίνεται μία εκτενής αναφορά περί του κακόβουλου λογισμικού που συχνά αποτελεί το μέσο από το οποίο πλουτίζουν πολλοί άνθρωποι παγκοσμίως. Το κεφάλαιο 5 αναφέρεται στη σχέση των επιχειρήσεων – οργανισμών με τα κινητά τηλέφωνα, τη χρήση αυτών από τους υπαλλήλους και τους τρόπους με τους οποίους παραβιάζεται η ασφάλεια των ηλεκτρονικών μέσων των επιχειρήσεων. Έπειτα στο κεφάλαιο 6 αναλύεται η επίγνωση της ασφάλειας των κινητών συσκευών σε παγκόσμιο επίπεδο καθώς και οι ύποπτες κινήσεις τις οποίες θα πρέπει να προσέχει ή αποφεύγει κανείς προκειμένου να διατηρεί ασφαλές το λειτουργικό σύστημα του κινητού του τηλεφώνου. Τέλος στο κεφάλαιο 7 παρουσιάζεται η επικρατούσα κατάσταση

όσων αφορά στην ανακύκλωση των κινητών συσκευών στην Ελλάδα αλλά και σε παγκόσμιο επίπεδο.

ΚΕΦΑΛΑΙΟ 2ο: INTERNET ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΤΙΣ ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ

2.1 Εισαγωγή: Περιεχόμενο και εφαρμογές mobile internet

Σύμφωνα με μία έρευνα του τμήματος Μηχανικών Διοίκησης του Πολυτεχνείου του Μιλάνο και του μεταπτυχιακού προγράμματος Μηχανικών Παραγωγής επίσης του Πολυτεχνείου του Μιλάνο [Β.2.4], που διεξήχθη τον Ιούνιο του 2012, η αγορά του mobile internet αρχίζει το 2011 να αναπτύσσεται ξανά, μετά από τρία χρόνια αδράνειας, ακολουθώντας μια αλλαγή προτύπου, από τα παραδοσιακά κανάλια προμήθειας (πύλες Wap, μαζικά SMS, κτλ.) σε νέα κανάλια βασιζόμενα σε καταστήματα mobile internet και εφαρμογών για κινητά.

Συγκεκριμένα, η αγορά αναπτύχθηκε κατά 4% το 2011, αγγίζοντας τα 530 εκατομμύρια ευρώ, ενώ μια αύξηση πάνω από 15% σημειώθηκε το 2012. Η αγορά του mobile internet είναι μια αγορά πληρωμένου περιεχομένου (για αυτό εξάλλου χρειάζεται κανείς να γνωρίζει πώς να διαγράφει, αξιολογεί και να αναφέρει ένα πρόβλημα [Β.1.19]), σε αντίθεση με το διαδίκτυο το οποίο χρησιμοποιούμε στα PC. Σχεδόν το 90% των εσόδων προήλθε, στην πραγματικότητα, από την πώληση του mobile internet και των εφαρμογών στον πελάτη και το υπόλοιπο 10% από διαφημίσεις.

Η συνεχής αύξηση προήλθε κυρίως από τα παιχνίδια (+44%), τα οποία προωθούνταν στα κινητά μέσα από ηλεκτρονικά καταστήματα εφαρμογών και πύλες εταιριών τηλεπικοινωνίας. Η μουσική και τα βίντεο αναπτύσσονταν επίσης με ικανοποιητικούς ρυθμούς (+39% και +30%, αντίστοιχα), αν και εξακολουθούσαν να έχουν περιορισμένο αντίκτυπο στη συνολική αγορά. Τα πλεονεκτήματα της πλοήγησης και οι εφαρμογές του ελεγχόμενου παιχνιδιού με χρηματικά κέρδη αναπτύσσονταν επίσης καλά. Ωστόσο, το «παραδοσιακό» περιεχόμενο όπως διασκεδαστικά sms, logos και ringtones και υπηρεσίες διαδραστικών πολυμέσων (televoting, κτλ.) συνέχιζαν να μειώνονται.

Από άποψη τεχνολογικής πλατφόρμας, τα downloads από καταστήματα εφαρμογών επέδειξαν την πιο εντυπωσιακή αλλαγή: +89%. Σχεδόν όλες οι άλλες πλατφόρμες βρίσκονταν σε ύφεση (ιδιαίτερα τα SMS και τα MMS).

Παρόλα αυτά, οι εταιρίες που προσέφεραν τη δυνατότητα της πώλησης περιεχομένου και πίστωσης έπειτα στο λογαριασμό του χρήση, συνέχισαν να διοικούν το 89% της αγοράς. Όσων αφορά στη διαφήμιση σε κινητά, βέβαια, σημαντική ανάπτυξη της τάξης του 50% καταγράφηκε το 2011, αγγίζοντας τα 56 εκατομμύρια ευρώ ενώ η ανοδική αυτή τάση συνεχίστηκε.

Τέλος, σύμφωνα επίσης με την έρευνα των φοιτητών του Πολυτεχνείου του Μιλάνο [Β.2.4], σχετικά με τις φόρμες της διαφήμισης, πρέπει να αναφερθεί ότι έχουν γίνει μεγάλες επενδύσεις στην κλασσική διαφήμιση που παρουσιάζεται σε εφαρμογές και ιστοσελίδες για κινητά, καθώς και στη διαφήμιση του τύπου -δίνω τη λέξη κλειδί και μου εμφανίζει ό,τι σχετικό-. Η Google και η Adnetworks παρείχαν ένα δυνατό κίνητρο προς αυτήν την κατεύθυνση. Από την άλλη, η διαφήμιση βασιζόμενη σε μηνύματα SMS συνέχισε να αναπτύσσεται το 2012, παρά το γεγονός ότι σταμάτησε να αντιπροσωπεύει το μεγαλύτερο μερίδιο των επενδύσεων.

2.2 Μια πιο ενδελεχής ματιά στο κατάστημα εφαρμογών

Μέσω της έρευνας που διεξήχθη από το Πολυτεχνείου του Μιλάνο [Β.2.4], θα εστιάσουμε την προσοχή μας στο πιο καινοτόμο στοιχείο της αγοράς, τις εφαρμογές για κινητές συσκευές που διατίθενται προς download στα ηλεκτρονικά καταστήματα εφαρμογών. Οι εφαρμογές αυτές –όπως αναφέρθηκε προηγουμένως- σχεδόν διπλασιάστηκαν το 2011. Συνολικά όλη αυτή η “αγορά” των εφαρμογών για κινητά υπολογίζεται ότι τον Ιούνιο του 2012 άξιζε τα 75 εκατομμύρια ευρώ: η πλειοψηφία των χρημάτων αυτών σε ποσοστό 85% προέρχεται από ποσά που πληρώνει το κοινό για μια εφαρμογή, ενώ τα έσοδα που προέρχονται από in-app billing (υπηρεσία κατά την οποία πωλούνται ψηφιακές καινοτομίες μέσω των εφαρμογών) παίζουν επίσης σημαντικό ρόλο.

Ως σήμερα, η αγορά κυριαρχείται ακόμη από την Apple. Παρόλο που το λειτουργικό σύστημα της Google (Android) ξεπέρασε την Apple το 2011 όσων αφορά στη διάδοση συσκευών, οι εφαρμογές που ήταν διαθέσιμες στο Google Play (κατάστημα εφαρμογών της Google) το 2011 δεν παρουσίασαν σημαντική εξέλιξη ακόμη και ένα χρόνο μετά. Γενικώς, και στις δύο πλευρές υπάρχουν ακόμη σημαντικές ελλείψεις σε επίπεδο χρήσης και ικανότητας για φτάσουμε σε σημείο να κοστολογούμε τις εφαρμογές. Για την Google, αυτό οφείλεται κυρίως στην έλλειψη κατοχυρωμένου συστήματος πληρωμής στον κόσμο της Android. Γι' αυτό το λόγο, η διάδοση ενός καναλιού πληρωμής βασιζόμενου σε πίστωση τηλεφώνου θα μπορούσε να παρέχει ένα σημαντικό κίνητρο στο κατάστημα εφαρμογών της Android.

Μια εικόνα των πιο πετυχημένων εφαρμογών προκύπτει κατά τη συγγραφή της 10ης κατά σειρά αναφοράς του τμήματος Μηχανικών Διοίκησης του Πολυτεχνείου του Μιλάνο και του μεταπτυχιακού προγράμματος Μηχανικών Παραγωγής επίσης του Πολυτεχνείου του Μιλάνο σχετικά με το ίντερνετ στα κινητά και τις εφαρμογές του, η οποία έλαβε χώρα τον Ιούνιο του 2012 και στην οποία εξετάσθηκαν περιοδικά 50 ταξινομημένες εφαρμογές που διατίθενται στο κατάστημα εφαρμογών της Apple και στο Google Play. Η ανάλυση ταυτοποίησε αρκετά σημαντικά ευρήματα:

- Τα παιχνίδια ήταν η κορυφαία κατηγορία και στην Apple και στη Google με ποσοστό χρήσης πάνω από 50%. Οι καινοτόμες ωφέλειες είχαν τη δεύτερη θέση και στα δύο καταστήματα, ενώ η «πληροφορία μέσω πολυμέσων» ήταν στην τρίτη θέση στο κατάστημα Apple και η πλοήγηση στην αντίστοιχη θέση στο Google Play.
- Όσων αφορά στο είδος των εταιριών που εμφανίζονταν στην ταξινόμηση, οι εταιρίες προϊόντων λογισμικού κυριάρχησαν και στην Apple και στην Android.
- Το ποσοστό των Ιταλικών εταιριών στις ταξινομήσεις ήταν αρκετά περιορισμένο- ανάμεσα στο 10%-20% στο κατάστημα εφαρμογών της Apple, ανάλογα με τη χρονική περίοδο, κι ακόμη χαμηλότερο (πιο κάτω από 10%) στο Google Play.
- Ως τον Ιούνιο του 2012 που διεξήχθη η έρευνα, ο καθημερινός μέσος δείκτης τζίρου για εφαρμογές στο App Store ήταν σχεδόν διπλάσιος από αυτόν στο Google Play (11% έναντι 6%)
- Σχετικά με το μοντέλο εσόδων και στα δύο καταστήματα η αναλογία δωρεάν εφαρμογών με in-app billing μεγάλωσε πολύ σημαντικά (ενδεικτικά έφτασε το 49% στο Apple Store το Μάιο του 2012 σε σύγκριση με 17% που ήταν 12 μήνες πριν).

2.3 Εστιάζοντας στους κατασκευαστές εφαρμογών

Σύμφωνα με μία έρευνα η οποία διεξήχθη το Μάιο του 2012 και η οποία κατεγράφη από το τμήμα Μηχανικών Διοίκησης του Πολυτεχνείου του Μιλάνο και το μεταπτυχιακό πρόγραμμα Μηχανικών Παραγωγής επίσης του Πολυτεχνείου του Μιλάνο [B.2.4] κατά τη συγγραφή της 10ης κατά σειρά αναφοράς σχετικά με το ίντερνετ στα κινητά και τις εφαρμογές του τον Ιούνιο του 2012, σε σύνολο σχεδόν 200 Ιταλών κατασκευαστών εφαρμογών (εταιρίες λογισμικού, web agencies, ανεξάρτητοι κατασκευαστές λογισμικού, κτλ.), οι μισοί από αυτούς συνήθιζαν να αναπτύσσουν λογισμικό σε περιβάλλοντα B2c(business-to-consumer) και B2b(business-to-business), περίπου το 1/4 αυτών μόνο σε B2b και σχεδόν το 1/3 αποκλειστικά σε B2c. Είναι ενδιαφέρον το ότι πάνω από το 1/4 των ερωτηθέντων ήταν ανεξάρτητοι κατασκευαστές λογισμικού (single individuals).

Το πρώτο εύρημα που προέκυψε ήταν ότι μια πολύ σημαντική αναλογία διαθέσιμου περιεχομένου ήταν υποτιμημένη, τόσο που οι κατασκευαστές δεν μπορούσαν ακόμη και να ανακτήσουν το κόστος ανάπτυξης της. Στην πραγματικότητα, σχεδόν το 50% των ερωτηθέντων κατασκευαστών της έρευνας διεκδίκησαν από τις B2c εφαρμογές συνολικά κέρδη λιγότερα από 1.000 ευρώ, σε σύγκριση με το 7% που κέρδισαν περισσότερα από 50.000 ευρώ. Επίσης, πάνω από το 25% διεκδίκησε από 1.000 έως 10.000 ευρώ ετησίως και τελικά το 14% από 10.000 έως 50.000 ευρώ.

Παρόλα αυτά, στην πορεία της έρευνας πολλοί ανεξάρτητοι κατασκευαστές και εταιρίες λογισμικού υποστήριξαν ότι έχοντας συλλάβει την ιδέα του πως να στήσουν ένα κατάστημα εφαρμογών κατάφεραν χειροπιαστά αποτελέσματα από το λανσάρισμα των εφαρμογών τους (με έσοδα αρκετών χιλιάδων ευρώ ανά μήνα), κυρίως μέσω εκπτώσεων και/ή της τακτικής in-app billing, κοινώς της τακτικής 2+1 δώρο.

Επιστρέφοντας στα αποτελέσματα της έρευνας, παρατηρείτε ότι σχεδόν στις μισές περιπτώσεις, τα έσοδα προέρχονταν από το εξωτερικό, οπότε δεδομένου του ότι τα καταστήματα εφαρμογών, λειτουργούν ορθά, μπορούν να ανοίξουν την πόρτα σε ενδιαφέρουσες ευκαιρίες στην παγκόσμια αγορά.

Τέλος, σύμφωνα με την ανωτέρω έρευνα η κύρια πλατφόρμα για Εφαρμογές B2c είναι η Apple (51%)· παρόλα αυτά το ποσοστό που υποδεικνύει την Android είναι επίσης σημαντικό (38%). Άλλες πλατφόρμες είναι περιθωριοποιημένες, με το 7% να αντιπροσωπεύει περιβάλλοντα ανάπτυξης cross-platform (που βασίζονται σε πολλαπλές πλατφόρμες).

2.4 Η οπτική γωνία του καταναλωτή

Η έρευνα του Πολυτεχνείου του Μιλάνο [Β.2.4] στο κομμάτι της συνεργασίας με την ιταλική εταιρία στατιστικής ονόματι Doxa, συμπεριλαμβάνει 910 χρήστες εφαρμογών και παρουσιάζει τη συμπεριφορά του καταναλωτή σε ό,τι αφορά τις εφαρμογές για κινητά και tablets.

Μερικά από τα αποτελέσματα συνοψίζονται παρακάτω:

- για τους χρήστες λογισμικού της Apple, το 31% των ερωτηθέντων έχουν λιγότερες από 5 εφαρμογές, 34% έχουν από 6 έως 20, και 35% έχουν περισσότερες από 21. Για χρήστες iPhone αυτές οι εκτιμήσεις αλλάζουν, αντίστοιχα σε: 13%, 29%, και 58%.
- Πάνω από το 1/4 των εφαρμογών που κατεβαίνουν χρησιμοποιούνται μόνο μια ή δύο φορές.
- Οι πιο συχνά χρησιμοποιούμενες κατηγορίες εφαρμογών είναι αυτές της κοινωνικής δικτύωσης και κοινοποίησης, της κινητικότητας/ταξιδιών, των παροχών/ωφελειών και τέλος, τα παιχνίδια/διασκέδαση και τα νέα.
- Οι κύριοι οδηγοί όταν επιλέγεται μια εφαρμογή είναι: η δωρεάν διαθεσιμότητα/τιμή και το να ικανοποιεί μια συγκεκριμένη απαίτηση. Ακολουθεί η γνώμη των φίλων και των γνωστών και τέλος η κατάταξη του καταστήματος.
- Οι βασικοί λόγοι για να αγοραστεί μια εφαρμογή είναι: η λογική τιμή, η διάθεση δωρεάν εναλλακτικών λύσεων και το ενδιαφέρον στο περιεχόμενο.
- Η προθυμία να πληρώσει ο χρήστης για μια εφαρμογή ποικίλει πολύ στους χρήστες iPhone και στην υπόλοιπη αγορά: για παράδειγμα το 54% των χρηστών Android δηλώνουν ότι κατεβάζουν μόνο δωρεάν εφαρμογές, έναντι του 27% των χρηστών της Apple που δηλώνουν το ίδιο πράγμα.

2.5 Τρέχουσες τάσεις και μελλοντικά σενάρια

Σε ένα άρθρο του Geoff Riley που αναρτήθηκε στις 26/09/2013 στην ιστοσελίδα tutor2.net ο αρθρογράφος αναφέρεται σε μία έρευνα που πραγματοποιήθηκε και δημοσιεύτηκε από το Ανθρώπινο Δυναμικό του τομέα Κοινωνίας και Επικοινωνιών του Ινστιτούτου της Vodafone με τίτλο «Mobile phones - the impact on the economy, society and our personal lives», βασισμένη σε ευρήματα πολλών πηγών, συμπεριλαμβανομένων μεταξύ άλλων συνεντεύξεις από 10 κορυφαίους ακαδημαϊκούς ερευνητές και επιστήμονες της Vodafone από όλον τον κόσμο. Από την έρευνα αυτή προέκυψαν τα εξής:

Οι κινητές τεχνολογίες συνεισφέρουν σημαντικά στην οικονομική ανάπτυξη του ΑΕΠ μιας χώρας με το προβλεπόμενο φάσμα ανάπτυξης να κυμαίνεται μεταξύ του 1,8% για το Ηνωμένο Βασίλειο και του 24,9% για την Αίγυπτο από το 2010-2020, συγκριτικά με το ΑΕΠ των εν λόγω χωρών κατά το 2011. Φυσικά η επίδραση αναμένεται πολύ μεγαλύτερη για τις αναπτυσσόμενες χώρες [Β.4.Η.19]

Υπάρχουν πολλοί παράγοντες που θα μπορούσαν να αντικρούσουν την τάση ανάπτυξης της αγοράς των εφαρμογών για κινητά τα επόμενα χρόνια. Παρουσιάζονται παρακάτω συνοπτικά οι παράγοντες που σύμφωνα με τη μελέτη του Πολυτεχνείου του Μιλάνο [Β.2.4], θα μπορούσαν να αποτελέσουν -κλειδί- σε μελλοντικές εξελίξεις.

- *Το μοντέλο χρήσης και διανομής του περιεχομένου.* Το πρώτο σημαντικό θέμα περιλαμβάνει τα σχετικά βάρη των διαφορετικών καναλιών διανομής του περιεχομένου και των εφαρμογών. Υπάρχουν ποικίλοι παράγοντες που θα μπορούσαν να παίξουν σημαντικό ρόλο σε αυτό το κομμάτι. Πρώτα είναι η ταχύτητα με την οποία διαδίδονται οι εφαρμογές HTML5 και Web (ως το 2012, λίγες από τις πιο διαδεδομένες ιστοσελίδες είχαν site βασισμένο σε HTML5). Δεύτερον είναι το επίπεδο διάχυσης και η αποτελεσματικότητα του περιβάλλοντος των πολυπλατφόρμων. Μια τρίτη πτυχή έχει σχέση με την ανάπτυξη νέων αγορών στην Ιταλία, όπως αντίστοιχα υπάρχει το κατάστημα της Amazon στις ΗΠΑ.
- *Ο ρόλος των ποικίλων λειτουργικών συστημάτων.* Μια άλλη αβεβαιότητα σχετίζεται με την επιρροή των ποικίλων λειτουργικών συστημάτων, με ιδιαίτερη προσοχή στο ρόλο που παίζουν η Microsoft και η Nokia, μαζί με την Apple και την Google.
- *Οι κανόνες της αγοράς.* Οι κανόνες της αγοράς σε σχέση με την προστασία του καταναλωτή θα παίξουν ένα σημαντικό ρόλο: για παράδειγμα, ένας νέος κανόνας διαχείρισης της ιδιωτικής ζωής, ή του μεγάλου όγκου δεδομένων θα έχει αντίκτυπο στη διαφάνεια και τη διαύγεια της επικοινωνίας του καταναλωτή.
- *Ανταγωνισμός πολύ-συσκευών.* Ένα τελικό σημείο βρίσκεται εκεί όπου τα tablets αντικαθιστούν ως μια εναλλακτική λύση τα κινητά και τα smartphones, για πρόσβαση σε περιεχόμενο και εφαρμογές για κινητές συσκευές. Ο γενικός ανταγωνισμός για μερίδιο στο πορτοφόλι του καταναλωτή και μερίδιο στο χρόνο του καταναλωτή, θα μπορούσε να εκτοξευτεί ακολουθώντας επίσης την αυξανόμενη διάδοση των προσφορών, οι οποίες καθιστούν δυνατό το να αποκτήσουμε πρόσβαση του ίδιου περιεχόμενου από πολλαπλές συσκευές (χωρίς να χρειάζεται να κάνουμε διπλότυπες αγορές για κάθε συσκευή).

2.6 Η αγορά υπηρεσιών τηλεπικοινωνίας: μόνο το ίντερνετ για κινητά αναπτύσσεται

Σύμφωνα πάλι με την 10η κατά σειρά αναφορά του τμήματος Μηχανικών Διοίκησης του Πολυτεχνείου του Μιλάνο και του μεταπτυχιακού προγράμματος Μηχανικών Παραγωγής επίσης του Πολυτεχνείου του Μιλάνο, τα έσοδα από τις υπηρεσίες τηλεπικοινωνίας για κινητά μειώθηκαν κατά 6% το 2011, σημειώνοντας μια ακόμη πιο σημαντική μείωση από τη μείωση της προηγούμενης χρονιάς του 3%.

Όπως συμβαίνει για χρόνια, η προς τα κάτω τάση είναι το αποτέλεσμα δυο αντίθετων δυναμικών: μια συνεχόμενη μείωση σε φωνητικές υπηρεσίες (-10%) και υγιείς ανάπτυξη σε υπηρεσίες δεδομένων (+5%).

Η μείωση στα έσοδα των φωνητικών υπηρεσιών δεν οφείλεται σε μείωση της ανάγκης επικοινωνίας, αλλά μπορεί να ερμηνευτεί ως μια περαιτέρω μείωση των μονάδων ανά λεπτό (ως αποτέλεσμα της ανταγωνιστικής πίεσης και των διαφόρων άλλων προσφορών) και βέβαια λόγω της νομοθεσίας η οποία οδηγεί σε σταδιακή μείωση των τιμών και των μάξιμουμ δασμών περιήγησης. Αν τα έξοδα του χρήστη σε φωνητικές υπηρεσίες μειωθούν κατά 8%, τα έσοδα από τερματισμό κάποιας υπηρεσίας πέφτουν ως και 18%.

Όσων αφορά στις υπηρεσίες δεδομένων, οι δυναμικές ποικίλουν πολύ:

- ✓ Το P2p messaging παρέμεινε λίγο ή πολύ σταθερό το 2011, με μια ελαφριά μείωση στο ποσοστό του συνόλου της υπηρεσίας των δεδομένων. Ο λόγος γι' αυτήν την κατάσταση σχετίζεται με μια σταθερή πτώση στις τιμές μονάδας, ενόψει μιας αύξησης του όγκου της επικοινωνίας.
- ✓ Η συνδεσιμότητα PC Data, (η οποία περιλαμβάνει έσοδα internet key και new tablet), παρά το γεγονός ότι η χρήση της συνεχίζει να αναπτύσσεται, καθυστερεί εξαιτίας του κορεσμού της αγοράς μετά από χρόνια σημαντικής ανάπτυξης.
- ✓ Το mobile internet (δηλαδή η συνδεσιμότητα δεδομένων από κινητά/smartphones) αυξήθηκε κατά 52% και λόγω αυτού παρατηρήθηκε επίσης μία αύξηση σε ποσοστό 14% στα συνολικά έσοδα των υπηρεσιών δεδομένων.
- ✓ Τα έσοδα που προέρχονται από την πώληση περιεχομένου για κινητά, το οποίο περιεχόμενο διαχειρίζονται εταιρίες λογισμικού συνεχίζουν να μειώνονται(-3%) όπως και τα έσοδα από τη διαφήμιση σε κινητά όταν αυτό αποτελεί αρμοδιότητα των εταιριών τηλεπικοινωνίας.

Ενδεικτικά στοιχεία για το 2011 δίνει η αναφορά του Πολυτεχνείου του Μιλάνο [Β.2.4] σχετικά με το mobile internet και τις εφαρμογές του που πραγματοποιήθηκε τον Ιούνιο του 2012. Τα αρχικά δεδομένα για το 2012 επιβεβαιώνουν, ως επί το πλείστον, τις τάσεις που παρατηρήθηκαν το 2011:

- Οι φωνητικές υπηρεσίες συνέχισαν να πέφτουν με παρόμοιες τάσεις σε σχέση με εκείνες που είδαμε τα περασμένα χρόνια.
- Το messaging αναμένεται να πέσει ελαφρώς εξαιτίας μιας μείωσης στους μέσους δείκτες μονάδας και στην αυξανόμενη χρήση προγραμμάτων ανταλλαγής άμεσων μηνυμάτων·
- Δεν σημειώθηκαν σημαντικές αλλαγές στη συνδεσιμότητα Pc Data το 2012, πλην μιας ανάπτυξης που έλαβε χώρα το 2013 χάρη στην έλευση της συνδεσιμότητας LTE·
- Ένα επιπλέον άλμα μπροστά, παρόμοιο με εκείνο που έγινε το 2011, συνέβη και το 2012 για το mobile internet.·
- Όσων αφορά στο πληρωμένο περιεχόμενο, αναμένεται η ανάπτυξη και για περιεχόμενο το οποίο διαχειρίζονται εταιρίες τηλεπικοινωνιών (μέσω πίστωσης στο λογαριασμό του τηλεφώνου)·
- Τέλος, η διαφήμιση σε κινητά παρέμεινε σταθερή και αυξήθηκε ελαφρώς κατά το 2012

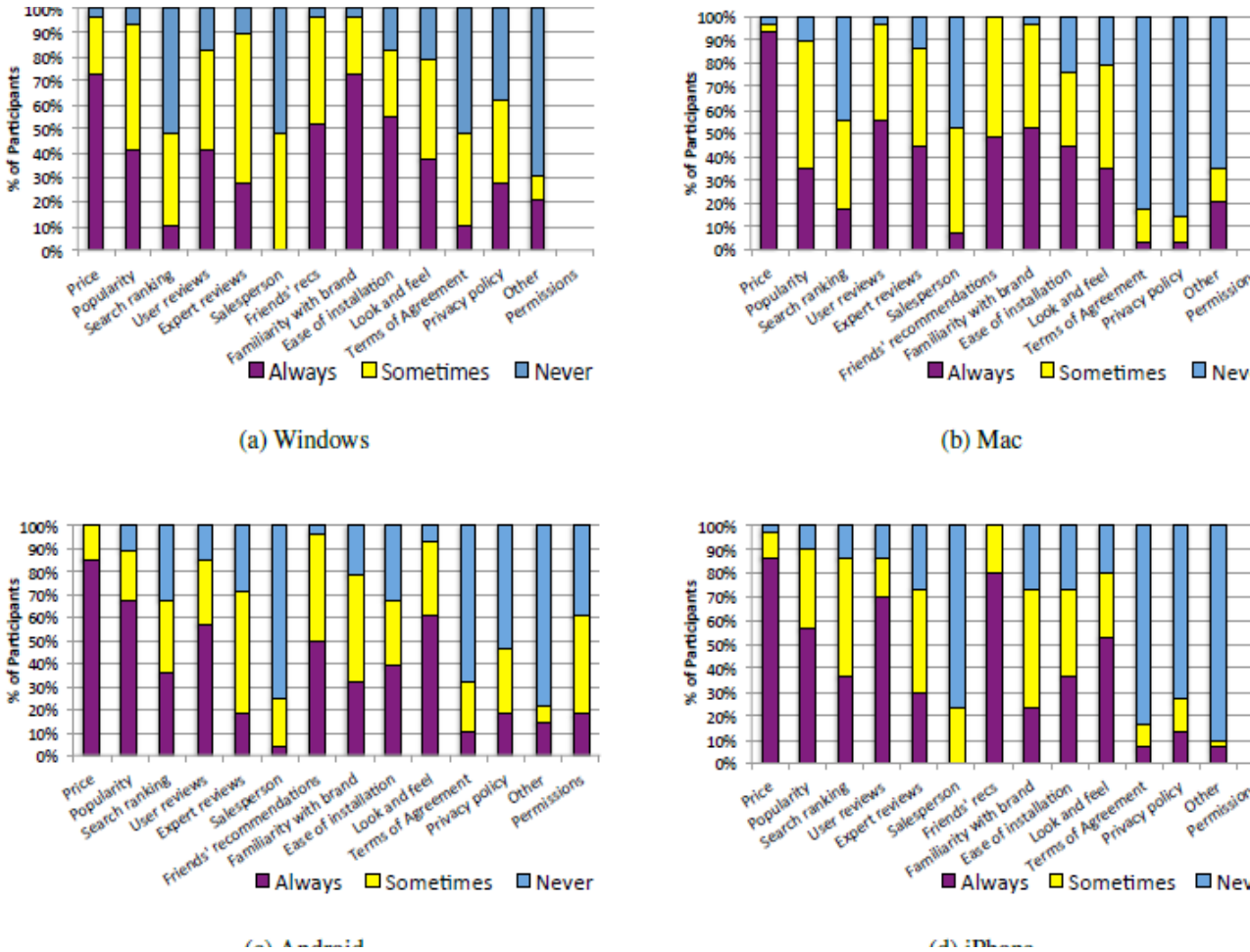
Το 2011 και κατά τους πρώτους μήνες του 2012 σημειώθηκε μια σημαντική περίοδος για τους διαχειριστές των τηλεπικοινωνιών για κινητά διότι τέθηκαν οι βάσεις για τις προκλήσεις των επόμενων χρόνων. Ενδεικτικά:

- Η δημοπρασία αδειών για τις συχνότητες LTE network, που ήταν μια εκροή σχεδόν 4 δισεκατομμυρίων ευρώ από 4 Ιταλούς Διαχειριστές κινητών συσκευών.
- Το λανσάρισμα σημαντικών διενεργειών του διαχειριστή σε σχετικά θέματα όπως η πληρωμή από κινητό και η διαφήμιση σε κινητό,
- Μια μεγάλη ώθηση προς τη χρήση τηλεφωνικής πίστωσης για νέο περιεχόμενο και υπηρεσίες που βασίζονται στο πρότυπο του mobile internet και των εφαρμογών για κινητά.
- Η προώθηση αρχικών πειραμάτων για NFC (επικοινωνία κοντινού πεδίου)·
- Η προώθηση υπηρεσιών “Cloud”, που αποτελεί ένα νέο ανταγωνιστικό μέτωπο.
- Η προώθηση ομάδων εργασίας που θα ορίσουν στην ευρωπαϊκή κοινότητα τους κανόνες της μελλοντικής διοίκηση του ίντερνετ σε σχέση με την δικτυακή ουδετερότητα.

2.7 Παράγοντες εγκατάστασης

Μόλις ο χρήστης ανακαλύψει μια εφαρμογή, πρέπει να αποφασίσει αν θα την εγκαταστήσει. Επιπλέον κρίνεται απαραίτητο να γνωρίζει πότε μία εφαρμογή διαγράφεται και τον τρόπο διαγραφής της. Σύμφωνα με μία έρευνα των εργαστηρίων Berkley Intel του πανεπιστημίου της Καλιφόρνια, η οποία πραγματοποιήθηκε από τους Erika Chin, Adrienne Porter Felt, Vyas Sekar, David Wagner, με τίτλο, «Measuring User Confidence in Smartphone Security and Privacy»[B.2.5], και διεξήχθη ενδεικτικά με 50 χρήστες στις Η.Π.Α., οι παράγοντες που επηρεάζουν την απόφαση εγκατάστασης ή απόρριψης μιας εφαρμογής είναι οι εξής: τιμή, δημοτικότητα, έρευνα κατηγορίας, κριτικές χρηστών, κριτικές ειδικών, πωλητής, συστάσεις φίλων, οικειότητα με τη φίρμα, ευκολία εγκατάστασης, γραφικά, όροι συμφωνίας, πολιτικές ιδιωτικότητας και τέλος, άδειες.

Η εικόνα 1.1 αναφέρει δεδομένα από τις σύντομες ασκήσεις στις οποίες οι συμμετέχοντες ταξινόμησαν ένα σύνολο παραγόντων εγκατάστασης (π.χ. τιμή, φίρμα, screenshots) ως παράγοντες που -πάντα λαμβάνουν υπόψη-, -μερικές φορές λαμβάνουν υπόψη- ή -ποτέ/σπάνια λαμβάνουν υπόψη- κατά τη διάρκεια της εγκατάστασης.



Εικόνα 1.1: Η σχετική σημασία διαφόρων παραγόντων που λαμβάνονται υπ' όψιν

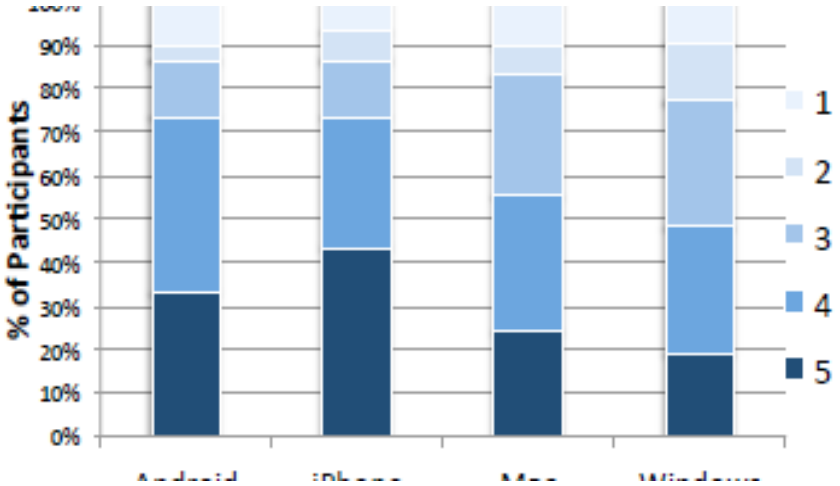
από τους χρήστες καθώς εγκαθιστούν μια εφαρμογή σε (α) Windows, β) Mac, (γ) Android, (δ) iPhone. Οι παράγοντες είναι με τη σειρά οι: τιμή, δημοτικότητα, έρευνα κατηγορίας, κριτικές χρηστών, κριτικές ειδικών, πωλητής, συστάσεις φίλων, οικειότητα με τη φίρμα, ευκολία εγκατάστασης, γραφικά, όροι συμφωνίας, πολιτικές ιδιωτικότητας, άλλα και τέλος, άδειες.

Βάσει της έρευνας ζητήθηκε επίσης από τους συμμετέχοντες να κατατάξουν τους παράγοντες από τον περισσότερο στο λιγότερο σημαντικό. Η τιμή, η δημοτικότητα και οι συστάσεις από φίλους και οικογένεια είναι οι τρεις παράγοντες με το μεγαλύτερο αριθμό συμμετεχόντων που -πάντα- ή -μερικές φορές- λαμβάνουν υπ' όψιν. Συνολικά, οι συμμετέχοντες είναι πιο πιθανό να δοκιμάσουν δωρεάν εφαρμογές από άγνωστους σχεδιαστές λογισμικού στα κινητά τους τηλέφωνα, με ένα μεγαλύτερο κίνδυνο ασφαλείας στα κινητά σε σχέση με στις παραδοσιακές συσκευές laptop.

Κάποιοι παράγοντες ίσως κάνουν τους συμμετέχοντες περισσότερο ή λιγότερο ευάλωτους στο κακόβουλο λογισμικό. Για παράδειγμα ένας χρήστης που διαβάζει τις πολιτικές ιδιωτικότητας και τις κριτικές των χρηστών και εγκαθιστά εφαρμογές από έμπιστες φίρμες ίσως είναι λιγότερο πιθανό να αντιμετωπίσει κακόβουλο λογισμικό ή grayware. Η ανάλυσή αυτή για τους παράγοντες εγκατάστασης, παρέχει επίσης βαθιά γνώση για το αν οι χρήστες λαμβάνουν υπόψη τους υπάρχοντες δείκτες ασφαλείας (π.χ. όρους συμφωνίας, πολιτικές ιδιωτικότητας, και άδειες Android).

Κριτικές: Οι κριτικές των χρηστών είναι ένας τρόπος να εδραιωθεί η εμπιστοσύνη της ασφάλειας και της ποιότητας μιας εφαρμογής, ακόμη και αν οι κριτικές μεμονωμένων χρηστών αυτές καθαυτές δεν είναι πάντα αξιόπιστες. Περισσότερο από το 80% των συμμετεχόντων στην έρευνα ανέφεραν ότι οι κριτικές των χρηστών επηρεάζουν 'πάντα' ή 'μερικές φορές' τις αποφάσεις τους για την εγκατάσταση, ασχέτως της πλατφόρμας. Λόγω της ενσωμάτωσης των κριτικών των χρηστών σε επίσημες αγορές για κινητά, οι ερευνητές υπέθεσαν ότι οι κριτικές των χρηστών θα ήταν πιο σημαντικές για αποφάσεις των χρηστών για εγκατάσταση εφαρμογών σε κινητά από ότι στα laptop. Όμως, αυτό δεν ισχύει. Σύγκριναν τις κριτικές των χρηστών για τις επιλογές εγκατάστασης στα κινητά χρησιμοποιώντας ένα τεστ τυχαίας ανακατάταξης και δε βρήκαν σημαντική διαφορά. Αντίθετα, οι απαντήσεις των συμμετεχόντων για τα laptop έδειξαν ότι το κοινό ενδιαφέρεται αρκετά να αναζητήσει κριτικές ακόμη κι αν δεν είναι ευρέως κοινοποιούμενες.

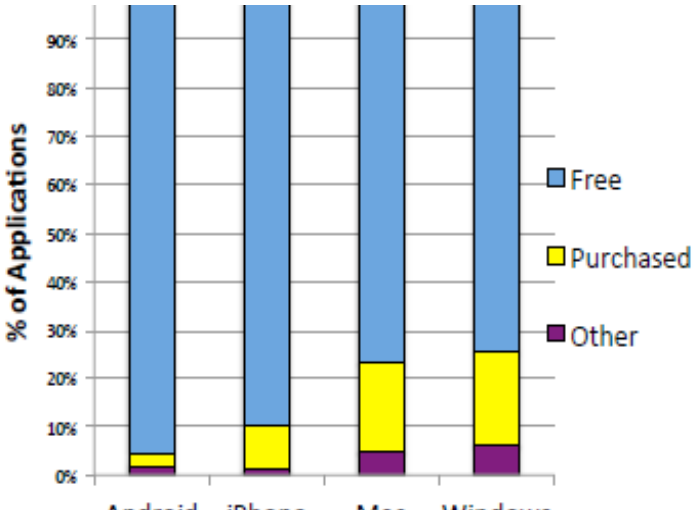
Φίρμα: Το όνομα της φίρμας μιας εφαρμογής (εταιρεία που δημιούργησε το λογισμικό) μπορεί να λειτουργήσει ως σήμα ασφαλείας· οι γνωστές εφαρμογές είναι λιγότερο πιθανό να εμπεριέχουν κακόβουλο κώδικα grayware. Υποθετικά οι συμμετέχοντες θα ήταν πιο ήσυχοι για την επωνυμία της εφαρμογής που επρόκειτο να εγκαταστήσουν στα laptop τους από ότι στα κινητά τους επειδή οι φίρμες για laptop τείνουν να εδραιωθούν και να γίνουν γνωστές. Για να το τεκμηριώσουν αυτό οι συγγραφείς της έρευνας, ρώτησαν τους συμμετέχοντες πόσο πρόθυμοι θα ήταν να δοκιμάσουν μια εφαρμογή από μια μη οικεία φίρμα ή εταιρεία. Το ρώτησαν αυτό δύο φορές: μια για κινητά τηλέφωνα, και μια για laptops. Η εικόνα 1.2 δείχνει τις απαντήσεις των συμμετεχόντων, οι οποίες είναι σε μια κλίμακα από το 1 (λιγότερο πιθανό να δοκιμάσουν μια μη οικεία φίρμα) ως το 5 (περισσότερο πιθανό να δοκιμάσουν μια μη οικεία φίρμα). Προκύπτει ότι οι συμμετέχοντες είναι περισσότερο πρόθυμοι να δοκιμάσουν εφαρμογές από μη οικείες φίρμες σε κινητές συσκευές παρά σε laptops. Οι απαντήσεις ήταν σχεδόν φυσιολογικά διανεμημένες. Αυτό το αποτέλεσμα είναι σύμφωνο με τις κατατάξεις παραγόντων της εικόνας 1.1, όπου η οικειότητα με τη φίρμα ήταν κυρίως στην κατηγορία 'μερικές φορές' για πλατφόρμες κινητών.



Εικόνα 1.2: Η προθυμία των συμμετεχόντων να δοκιμάσουν εφαρμογές από μη οικείες φίρμες, σε κλίμακα από 1 (λιγότερο πιθανό) ως 5 (περισσότερο πιθανό)

Τιμή: οι συγγραφείς της ανωτέρω έρευνας υπέθεσαν ότι οι χρήστες θα ήταν λιγότερο πιθανό να πληρώσουν χρήματα για εφαρμογές για κινητά από ότι για εφαρμογές για laptop. Για να δοκιμάσουν αυτήν την υπόθεση, ρώτησαν τους συμμετέχοντες αν κάθε εφαρμογή τους ήταν δωρεάν ή πληρωμένη. Το Σχήμα 6 δείχνει τα αποτελέσματα, οι 'λοιπές'

καταχωρήσεις για Windows και Mac είναι πρωτίστως εφαρμογές που πήγαιναν μαζί με περιφερειακά ή προμηθεύονταν από εργοδότες. Βρέθηκε λοιπόν ότι οι συμμετέχοντες έχουν πολύ περισσότερες δωρεάν εφαρμογές στα τηλέφωνά τους από ότι στα laptop τους. Οι ερευνητές παρατήρησαν επίσης ότι οι συμμετέχοντες με Android τηλέφωνα έχουν ένα μεγαλύτερο ποσοστό δωρεάν εφαρμογών από ότι συμμετέχοντες με iPhones, το οποίο είναι σύμφωνο και με αναφορές της βιομηχανίας.



Εικόνα 1.3: Το ποσοστό εφαρμογών που ήταν δωρεάν ή επί πληρωμή

Ιδιωτικότητα: Πολιτικές ιδιωτικότητας, και όροι συμφωνίας είναι ξεκάθαρα στους δείκτες ιδιωτικότητας. Λίγοι συμμετέχοντες τους λαμβάνουν υπόψη πριν εγκαταστήσουν εφαρμογές για κινητά τηλέφωνα. Απροσδόκητα, το 60% των συμμετεχόντων με τηλέφωνα Android αναφέρουν ότι λαμβάνουν υπόψη τους τις άδειες ‘μερικές φορές’ ή ‘πάντα’. Αυτά τα αποτελέσματα δείχνουν ότι οι συμμετέχοντες βασίζονται σε άλλους δείκτες εμπιστοσύνης (π.χ. συστάσεις και κριτικές) αντί γι’ αυτούς τους ξεκάθαρους αλλά δυσνόητους δείκτες ασφαλείας και ιδιωτικότητας.

ΚΕΦΑΛΑΙΟ 3ο: ΚΡΥΜΜΕΝΕΣ ΧΡΕΩΣΕΙΣ ΚΑΙ ΥΠΕΡΧΡΕΩΣΕΙΣ – ΤΡΑΠΕΖΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΚΑΙ ΚΙΝΗΤΑ

3.1.1 Εισαγωγή (Κρυμμένες χρεώσεις και υπερχρεώσεις)

Σύμφωνα με κάποια άρθρα που δημοσιεύτηκαν σε ιστοσελίδες τεχνολογικού περιεχομένου όπως αυτό που αναρτήθηκε στις 6/9/12 από την κα. Katia Moskovitch, ρεπόρτερ της τεχνολογίας στο BBC News, καθώς και αυτό που αναρτήθηκε στο SC MAGAZINE στις 3/10/2011 από τον ίδιο τον εκδότη του περιοδικού κ. Dan Kaplan, σημειώνεται “άνθιση” των εφαρμογών για κινητές συσκευές και μάλιστα μέσα σε σχετικά μικρό χρονικό διάστημα. Δυστυχώς όμως τα πράγματα δεν είναι τόσο ονειρεμένα όσο θα θέλαμε να τα φανταστούμε. Ξεκινώντας από τις κρυμμένες χρεώσεις στα κινητά διαπιστώνει κανείς για ποιο λόγο τελικά δεν πάνε όλα κατ' ευχήν για τους πελάτες και χρήστες κινητών τηλεφώνων παγκοσμίως.

Πολλοί χρήστες κινητών τηλεφώνων δεν κατανοούν πλήρως για ποιες υπηρεσίες πληρώνουν μέχρι που τους έρχεται ο λογαριασμός. Τις περισσότερες φορές αυτοί που πέφτουν θύματα της ανωτέρω παγίδας είναι εκείνοι που χρησιμοποιούν το κινητό τους μόνο για κλήσεις (ούτε καν για αποστολή και παράδοση μηνυμάτων), δεν είναι ακόλουθοι της τεχνολογίας και βέβαια το κινητό τους δεν είναι smartphone. Επίσης θύματα πέφτουν πολλοί έφηβοι οι οποίοι μπορεί να κάνουν κλικ για παράδειγμα σε μια διαφήμιση που υπόσχεται δωρεάν ringtones και να καταλήξουν με μηνιαία χρέωση στο λογαριασμό τους. Ακόμη στην κατηγορία των θυμάτων αυτών ανήκουν και αυτοί οι οποίοι μεταπηδούν από ένα απλό κινητό τηλέφωνο σε ένα smartphone καθώς επίσης και οι πελάτες οι οποίοι εμπιστεύονται “τρίτες” εταιρίες διαμεσολάβησης πέφτοντας θύματα υπερχρεώσεων.

Τέλος, θύματα των χρεώσεων – υποκλοπών θεωρούνται και οι χρήστες οι οποίοι δελεάζονται από δωρεάν downloads, σχεδιασμένα να μοιάζουν με αυθεντικές εφαρμογές ενώ από πίσω, οι εφαρμογές αυτές δουλεύουν για να κλέβουν χρήματα μέσω κρυμμένων συναλλαγών.

3.1.2 Κρυμμένες χρεώσεις και υπερχρεώσεις σε Ρωσία, Ηνωμένο Βασίλειο και Η.Π.Α.

Σύμφωνα με το ανωτέρω άρθρο της κας. Katia Moskovitch, στη Ρωσία, το φαινόμενο των κρυμμένων χρεώσεων έχει πάρει μεγάλες διαστάσεις με τις κορυφαίες εταιρίες τηλεφωνίας, στις οποίες κατά βάσει οφείλεται το φαινόμενο των "φουσκωμένων" λογαριασμών, να αρνούνται να σχολιάσουν.

Επιπλέον, στο Ηνωμένο Βασίλειο η βιομηχανία ανίχνευσης λαθών και ηλεκτρονικών ενημερώσεων με την επωνυμία Phoneplus, έχει ένα σύστημα αποστολής μαζικών ενημερώσεων για να καθιστά ξεκάθαρο όταν οι πελάτες έχουν πρόσβαση σε συνδρομητικές υπηρεσίες υψηλού κόστους, ότι κατανοούν το πλήρες κόστος της υπηρεσίας. Σύμφωνα με έρευνες οι έφηβοι είναι ιδιαίτερα επιρρεπής στο να κάνουν κλικ σε μια υπηρεσία που υπόσχεται να είναι δωρεάν, όπως μοντέρνα ringtones, αν και δε διαβάζουν τους όρους και τις συμφωνίες, μέχρι που οι γονείς τους ανακαλύπτουν μια ογκώδη χρέωση στο μηνιαίο τους λογαριασμό. Η PhonePlus έχει ιδρύσει έναν ιστότοπο που ονομάζεται PhoneBrain για να εκπαιδεύσει νέους ανθρώπους σχετικά με τις πιθανές παγίδες στις οποίες μπορεί να «πέσει» κανείς έχοντας στην κατοχή του ένα κινητό τηλέφωνο.

Από την άλλη μεριά του Ατλαντικού (ΗΠΑ) οι υπερχρεώσεις είναι ένα μεγάλο θέμα επίσης, με «τρίτες» εταιρείες- συνεργάτες να χρεώνουν τους πελάτες για υπηρεσίες μη εξουσιοδοτημένες. Οι πελάτες καταλήγουν να πληρώνουν για υπηρεσίες στις οποίες δε γράφτηκαν ποτέ, από ήχους κλήσης, ημερήσιο ωροσκόπιο και λήψη μουσικής, ως μαθήματα γιόγκα και προγράμματα δίαιτας. Οι υπερχρεώσεις στα σταθερά τηλέφωνα επηρεάζουν 15 με 20 εκατομμύρια νοικοκυριά της Αμερικής, λέει η αντίστοιχη με τα ελληνικά δεδομένα Αμερικανική Γεν. Γραμματεία Προστασίας του Καταναλωτή, ενώ από το 2012 και έκτοτε πραγματοποιούνται απάτες και στα κινητά τηλέφωνα. Σύμφωνα με μια έρευνα της Αμερικανικής Συγκλήτου που ολοκληρώθηκε το 2011, οι υπερχρεώσεις κοστίζουν στους Αμερικανούς πελάτες περίπου 2 δισεκατομμύρια δολάρια το χρόνο, και μόνο ένας στους 20 συνειδητοποιεί ότι έχει εξαπατηθεί.

3.1.3 Περιπτώσεις θυμάτων κρυμμένων χρεώσεων και υπερχρεώσεων

Στο άρθρο της στην ιστοσελίδα BBC News Technology η κα. Katia Moskovitch, αναφέρει ενδεικτικά την περίπτωση μιας πελάτισσας Ρωσικής εταιρίας τηλεφωνίας η οποία κάλεσε τον αριθμό του κινητού τηλεφώνου του συζύγου της και άκουσε μουσική αντί του συνηθισμένο ήχου αναμονής. Το ίδιο συνέβη και με τον σύζυγό της. Αυτό που δε γνώριζαν είναι ότι αυτή η υπηρεσία τους κόστιζε, ακόμη και αν κανείς τους δε θυμάται να γράφτηκε ως συνδρομητής σε αυτήν. Μόνο όταν η εν λόγω κυρία κάλεσε την εταιρεία κινητής τηλεφωνίας, η οποία τύχαινε να είναι και ο μεγαλύτερος διαχειριστής κινητής τηλεφωνίας στη Ρωσία, ανακάλυψε ότι χρεώνεται για αυτό: 42 ρούβλια ($ 1,30) το μήνα. Όταν παραπονέθηκε ότι ποτέ δεν αγόρασε αυτήν την υπηρεσία, ο εκπρόσωπος της εξυπηρέτησης πελατών της

απάντησε ήρεμα πως ναι, την είχε αγοράσει. Προκύπτει πως αμέσως μετά την υπογραφή του συμβολαίου της, της έστειλαν ένα μήνυμα, ενημερώνοντάς τη πως είχε προστεθεί αυτή η μουσική στο λογαριασμό της και ότι ήταν δωρεάν για τον πρώτο μήνα, όμως μετά από αυτό θα συνεχιζόταν αυτόματα η όλη παροχή με μηνιαία χρέωση οπότε για να το σταματήσει έπρεπε να τους τηλεφωνήσει και να την ακυρώσει.

Μία άλλη περίπτωση αφορά σε έναν 20χρονο χάκερ ο οποίος, σύμφωνα με μία είδηση της ιστοσελίδα του BBC που δημοσιεύτηκε στις 18/10/2012, συνελήφθει στη Βόρεια Γαλλία επειδή διέδωσε έναν ιό μέσω εφαρμογής smartphone, εξαπατώντας χιλιάδες θύματα. Υπολογίζεται ότι έκλεψε μικρά ποσά από 17.000 ανθρώπους συγκεντρώνοντας περίπου 500.000 ευρώ (405.000 λίρες) κατά το 2011. Δουλεύοντας από το σπίτι των γονέων του στη νότια Γαλλία, δελέαζε τα θύματά του με δωρεάν downloads, σχεδιασμένα να μοιάζουν με αυθεντικές εφαρμογές. Μόλις οι ψεύτικες εφαρμογές εγκαθίσταντο, στέλνονταν γραπτό μήνυμα εν αγνοία του χρήστη σε ένα premium rate αριθμό που είχε οριστεί από τον κακόβουλο χρήστη. Ο συγκεκριμένος επίσης χειρίζονταν προγράμματα που περιείχαν κακόβουλο κώδικα και εφόσον κανείς τα κατέβαζε έστελναν στον χάκερ τους κωδικούς για ιστοσελίδες παιχνιδιών και τζόγου στις οποίες τα θύματα ήταν συνδρομητές.

3.2.1 Εισαγωγή (Τραπεζικές συναλλαγές και κινητά)

Τα τελευταία χρόνια, με την ανάπτυξη του προηγμένου λογισμικού για κινητές συσκευές, οι χρήστες συνηθίζουν να χρησιμοποιούν την κινητή τους συσκευή μεταξύ άλλων και για να κάνουν τις τραπεζικές τους συναλλαγές. Το e-banking δεν είναι μέθοδος πληρωμής, πρακτικά είναι το ηλεκτρονικό κατάστημα μιας τράπεζας [Β.1.1]. Σύμφωνα με το άρθρο του κ. John Leyden που δημοσιεύτηκε στις 7/12/2012 στην ιστοσελίδα τεχνολογικών νέων και απόψεων «The register» με τους Η/Υ και τις κινητές συσκευές εκτεθειμένες, οι εισβολείς μπορούν να ανακόπτουν και να κλέβουν όλα τα θύματα που κάνουν online συναλλαγές, ενώ τα θύματα συνεχίζουν σε πολλές περιπτώσεις να μην λαμβάνουν μέτρα. Συμπεριλαμβανομένου και του κλειδιού, ολοκληρώνοντας τη συναλλαγή, το μήνυμα της τράπεζας προς τους πελάτες εμπεριέχει τον αριθμό αυθεντικοποίησης της συναλλαγής (TAN). Με τον αριθμό λογαριασμού, τον κωδικό και το TAN, οι εισβολείς είναι ικανοί να μεταφέρουν λαθραία χρήματα από τους λογαριασμούς των θυμάτων, ενώ τα θύματα μένουν με την εντύπωση ότι η συναλλαγή τους ολοκληρώθηκε επιτυχώς.

Εικόνα 3.1: Οι προσωπικές πληροφορίες στα κινητά προσελκύουν τους εγκληματίες [B.4.H.21]

Πολλοί πελάτες επίσης ρίχνουν το φταίξιμο στις τράπεζες, ισχυριζόμενοι ότι κακώς δίνουν τέτοιες δυνατότητες και φυσικά ότι δεν θα έπρεπε τα πράγματα να εκσυγχρονιστούν κατ' αυτό τον τρόπο. Φυσικά αυτό είναι εντελώς λάθος. Όπως αναφέρει και ο S.A. Bilal Malick και ο S. Sumathi σε μία παρουσίαση τους που αναρτήθηκε στις 23/01/2013 στην ιστοσελίδα slideshare.net με τίτλο «Electronic and mobile banking», όλα εξαρτώνται από τον χρήστη. Εάν οι χρήστες χρησιμοποιούμε το mobile banking σωστά, θα μας φανεί ιδιαίτερα χρήσιμο. Εξάλλου οι απαιτήσεις προπορεύονται του επιπέδου ασφαλείας ενώ οι πρακτικές που εφαρμόζονται για τη διαχείριση ενός τραπεζικού συστήματος αντικαθίστανται από τεχνολογικά εργαλεία. Φτάνει να δούμε μερικά από τα φαινόμενα που φανερώνουν την αλληλοσύνδεση μιας τράπεζας με την τεχνολογία [B.2.8]:

- Προστασία των δεδομένων και της υποδομής.
- Επιπρόσθετη αξία στο προφίλ.
- Εντοπισμός απατών.
- Σχέδια στρατηγικής για την τεχνολογία της πληροφορίας.
- Καλύτερη αξιοποίηση των πληροφοριών.
- Αλλαγές στη διαχείριση.
- Προσαρμογή της τεχνολογίας πάνω στα εκάστοτε δεδομένα.
- Βελτίωση στην ποιότητα της τεχνολογίας.
- Προσέγγιση, ανάπτυξη και διατήρηση επαγγελματικών μεθόδων της τεχνολογίας της πληροφορίας.

Επιπλέον, με τη συσχέτιση μεταξύ της τεχνολογίας και των τραπεζών οι επιχειρήσεις που πλέον έχουν τη δυνατότητα να διαχειρίζονται τους τραπεζικούς τους λογαριασμούς μέσω κάποιας κινητής συσκευής σημειώνουν, α)βελτίωση στην εξυπηρέτηση, β)μείωση του κόστους της επιχείρησης, γ)αύξηση των μετοχών της επιχείρησης στην αγορά, δ)αύξηση της αξίας της επιχείρησης. Και παρ' όλο που αυτό το πακέτο κοστίζει ανεξάρτητα για το αν μιλάμε για μικρή ή μεγάλη επιχείρηση σίγουρα επιτελείται μια σπουδαία προσδοκία της τράπεζας.

3.2.2 Θέματα Ασφάλειας και Λειτουργίας

Σύμφωνα με την σύνοψη μιας έρευνα του Dr. Kevin Streff στο Dakota State University η οποία δημοσιεύθηκε στις 02-04-2010 και τιτλοφορείται ως «An Overview of Mobile Banking Threats» κάποια θέματα ασφαλείας και λειτουργίας που σχετίζονται με τις κορυφαίες τεχνολογικές εφαρμογές των τραπεζών είναι τα παρακάτω:

- Θέματα ασφαλείας του Banking για κινητά:

- Πιστοποίηση.
- Άρνηση υπηρεσίας.
- Χαμένο και κλεμμένο τηλέφωνο.
- Ψάρεμα, μέσω των τηλεφωνικών κλήσεων και των αποστολών sms για Vishing ή SMiShing.
- Μπλοκάρισμα (cracking) και κλωνοποίηση του τηλέφωνου.
- Ευαίσθητα δεδομένα, υπογραφές, υποκλοπές κίνησης κρυπτογράφησης,
- Κακόβουλη διαμεσολάβηση, Man-in-the-Middle, και Διοχέτευση παράνομων (Redirecting) Μηνύματων.
- Ιοί και Κακόβουλο Λογισμικό.

- Η πιστοποίηση της αυθεντικότητας σε mobile banking γίνεται με τα παρακάτω:

- Χρήση αριθμού κινητού.
- Ονόματα χρηστών και κωδικοί.
- Κωδικοί μίας φοράς.
- Αριθμοί PIN.
- Βιομετρήσεις.
    - Αναγνώριση Προσώπου.
    - Ανάλυση πληκτρολόγησης.

- Αναγνώριση γραφικού χαρακτήρα.
- Αναγνώριση ομιλητή.
- Αξιοποίηση υπηρεσίας.

➢ Πιστοποίηση εκτός ζώνης.

- Τρόποι με τους οποίους προφυλάσσουμε τα ευαίσθητα δεδομένα:

➢ Περιορισμένη χρήση
➢ AES (Προηγμένα πρότυπα κρυπτογράφησης- advanced Encryption Standars).
➢ HTTPS (Ασφαλής δικτυακές συνδέσεις - **HTTPS** (Hypertext Transfer Protocol Secure)
➢ SSL (Ασφαλής μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο -**Secure Sockets Layer**).
➢ Αλγόριθμος κρυπτογράφησης Blowfish.

- Ιοί και κακόβουλο λογισμικό.

➢ Κρύβονται πίσω ακόμη και από SMS, MMS, HTTP και email αρχεία.
➢ Doombot: είναι ένας Δούρειος ίππος που διαφθείρει συσκευές στο λειτουργικό των οποίων υπάρχει.
➢ Symbian.
➢ Commwarrior: χρησιμοποιεί τα MMS και το Bluetooth για να εξαπλώσει κακόβουλο
➢ λογισμικό από συσκευή σε συσκευή.
➢ «Φινλανδία»: όταν ένα ασήμαντο ξέσπασμα κακόβουλου λογισμικού για κινητά διαχέεται από συσκευή Bluetooth σε συσκευή Bluetooth σε έναν αγώνα ποδοσφαίρου.

3.2.3 Περιπτώσεις και παραδείγματα υποκλοπών με Eurograbber

Μία περίπτωση που χρήζει ιδιαίτερης προσοχής και μελέτης είναι αυτή της κλοπής 36.000.000 ευρώ (47.000.000 δολαρίων) από ευρωπαϊκή τράπεζα με τη βοήθεια κακόβουλου λογισμικού κινητών συσκευών.

Σύμφωνα με μία είδηση που δημοσιεύτηκε στις 7-12-2012 στην ιστοσελίδα zbnet.com από τη δημοσιογράφο Charlie Osborne, βάση μιας εργασίας που κυκλοφόρησε από την CheckPoint (εταιρία λογισμικού) χάκερς, οι οποίοι δούλευαν στην ανατολική Ευρώπη μπόρεσαν συστηματικά να κλέψουν περίπου 47.000.000 δολάρια με τη χρήση ενός κακόβουλου λογισμικού τύπου Δούρειου ίππου το οποίο εισχωρούσε στις έξυπνες συσκευές. Η «επιδρομή» αυτή χρισμένη από το Eurograbber (κακόβουλο λογισμικό που βασίζεται στις συνήθειες και τις προτιμήσεις του κάθε χρήστη του διαδικτύου και επιτίθεται αναλόγως), είναι

μία παραλλαγή που βασίζεται στα κακόβουλα λογισμικά για online banking (το Zeus και Zitmo).

Σύμφωνα με την CheckPoint, οι επιτήδειοι ανέκοπταν μικρά μηνύματα που περιείχαν στοιχεία χρηστών μοντέλων Blackberry και Android και αφού επεξεργάζονταν στέλνονταν πίσω με ιδιαίτερο τρόπο. Υπολογίζεται ότι κατ' αυτόν τον τρόπο έχουν κλαπεί ποσά από 500-250.000 ευρώ από περισσότερους από 30.000 πελάτες τραπεζών.

Το Eurograbber χτυπά σε πολλαπλά στάδια. Αφού κάνετε κλικ, χωρίς να γνωρίζετε, σε ένα ψαρωτικό email – που πιθανόν να οδηγεί σε μια κακόβουλη ιστοσελίδα – το trojan κατεβαίνει στον υπολογιστή σας. Έτσι όταν ένας πελάτης συνδέεται στον τραπεζικό του λογαριασμό η online banking συνεδρία υποκλέπτεται και ο κακόβουλος javascript κώδικας μπαίνει στην προσωπική σελίδα banking. Τότε ο πελάτης ειδοποιείται για μία δήθεν "αναβάθμιση της ασφάλειας" και του δίνεται η συμβουλή να κάνει κλικ σε έναν επισυναπτόμενο σύνδεσμο που του στέλνεται μέσω ενός sms στον αριθμό του κινητού του τηλεφώνου. Αυτό το στάδιο προκαλεί ένα download στο κινητό του πελάτη μιας κακόβουλης εφαρμογής παραλλαγής του Zitmo για διάφορα λειτουργικά συστήματα, κυρίως Android, Blackberry και Windows και τελικά ο πελάτης λαμβάνει "κωδικό επιβεβαίωσης" που πρέπει να εισάγει μέσω του Η/Υ στην ήδη μολυσμένη – εμπλουτισμένη με κακόβουλο κώδικα σελίδα. Αφού εισαχθεί ο «κωδικός επιβεβαίωσης», ένα παραθυράκι της javascript ενημερώνει τον πελάτη της τράπεζας ότι η δήθεν αναβάθμιση ασφαλείας έχει ολοκληρωθεί ενώ αυτό στην πραγματικότητα σημαίνει ότι το trojan έχει ενεργοποιηθεί.

Οι τράπεζες στην Ευρώπη συχνά χρησιμοποιούν "TAN" (transaction authorization number) για να αποτρέψουν αθέμιτες online συναλλαγές, κάτι σαν τους αριθμούς PIN απλά χρησιμοποιούνται μία μόνο φορά, προσφέρουν επιπλέον ασφάλεια στις τραπεζικές συναλλαγές με τον ίδιο τρόπο που και το PayPal (ασφαλής πύλη ηλεκτρονικών πληρωμών) απαιτεί να εισάγεις ένα κλειδί που στέλνεται με SMS στο κινητό σου, πριν αποκτήσεις πρόσβαση στον online λογαριασμό σου. Η επιτηδευμένη επίθεση του Eurograbber trojan αφού εγκατασταθεί παρακολουθώντας την δραστηριότητα banking του χρήστη, παρακάμπτει αυτήν την επικύρωση της διπλο-ασφαλείας και ανακόπτει το SMS ώστε τελικά να μεταφέρει αθόρυβα χρήματα έξω από τον τραπεζικό λογαριασμό.

Ενδιαφέρον παρουσιάζει το ότι σύμφωνα με την CheckPoint δεν υπάρχει καμία ένδειξη αυτών των ενεργειών στις καταστάσεις (λογαριασμού) που μπορεί να δει ο χρήστης μέσω του ιστού, καθώς το trojan ανακόπτει το SMS επιβεβαίωσης και ουσιαστικά διαδραματίζεται μια αθόρυβη παρασκηνιακή απειλή, που ενεργεί μέχρι να είναι πολύ αργά.

Για να αποτρέπεται ωστόσο η έκθεση σε τρίτους, μόνο ένα μικρό ποσοστό τραπεζικού ισολογισμού μπορεί να μεταφέρεται κάθε φορά.

Για να εκτελέσει αυτού του είδους τις επιθέσεις, ο Eurograbber μεταβιβάζει την τραπεζική δραστηριότητα σε μια ομάδα ανθρώπων οι οποίοι αθόρυβα ολοκληρώνουν όποια συναλλαγή θέλουν.

Η υποδομή ενός server request-response δημιουργήθηκε με Βάσεις Δεδομένων SQL οι οποίες συνδέονταν μεταξύ τους με διαφορετικά domain names και επιπλέον ένα στρώμα proxy server χρησιμοποιείται για να αποτρέπει την ανίχνευση πληροφοριών από τρίτους.

Ο trojan Eurograbber παρ' όλο που στοχεύει σε Android και Blackberry smartphones βρέθηκε επίσης και με παραλλαγές σχεδιασμένες για windows μοντέλα. Σύμφωνα με την CheckPoint, έχουν επηρεαστεί από το εν λόγω κακόβουλο λογισμικό όχι μόνο απλοί χρήστες αλλά και ολόκληρες επιχειρήσεις.

Οι επιθέσεις ξεκίνησαν στη Γαλλία, και σύντομα παρατηρήθηκαν κι άλλες στις ακτές της Γερμανίας, Ισπανίας και Ολλανδίας. Περιπτώσεις καταγράφηκαν μέχρι τα τέλη του 2012 μόνο στην Ευρώπη, όμως στην πορεία το trojan εξαπλώθηκε και εκτός Ευρωπαϊκής Ένωσης.

ΚΕΦΑΛΑΙΟ 4ο: ΕΚΤΕΝΗΣ ΜΕΛΕΤΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ

4.1 Εισαγωγή

Κατόπιν, της προσέγγισης των τεχνολογικών και οικονομικών προκλήσεων των κινητών συσκευών μέσω των κρυμμένων χρεώσεων και των τραπεζικών συναλλαγών ήρθε η στιγμή να μελετήσουμε εκτενέστερα ένα μεγάλο, ίσως το μεγαλύτερο, κεφάλαιο οικονομικής πρόκλησης που αφορά στα κινητά και το οποίο λέγεται -κακόβουλο λογισμικό-.

Σύμφωνα με μία ανάλυση της Symantec.com που πραγματοποιήθηκε για να μελετηθεί η τάση των απειλών που αφορούν στα κινητά τηλέφωνα κατά το 2011, από τότε που έφτασαν στα χέρια των πελατών τα πρώτα smartphones, οι εικασίες για απειλές και ηλεκτρονικά εγκλήματα (εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχει καθ' οποιονδήποτε τρόπο ηλεκτρονική συσκευή[Β.1.2]), που θα στόχευαν αυτές τις συσκευές αφθονούσαν. Ενώ οι απειλές ήταν ειδικά στοχευμένες για τα πρώτα smartphones που ήταν βασισμένα σε λειτουργικά συστήματα Symbian και Palm, καμία από αυτές δεν εξαπλώθηκε και μάλιστα πολλές από αυτές παρέμειναν απλά μια ιδέα. Με την αναπτυσσόμενη κίνηση σε smartphones και tablets, και την αυξανόμενη συνδεσιμότητα και ικανότητά τους υπάρχει μια αντίστοιχη αύξηση στην προσοχή τόσο από τους κατασκευαστές απειλητικού λογισμικού όσο και από τους ερευνητές ασφαλείας.

Καθώς ο αριθμός των άμεσων απειλών σε κινητές συσκευές παραμένει σχετικά χαμηλός σε σχέση με τις απειλές που στοχεύουν σε PC, έχουν υπάρξει νέες εξελίξεις στον τομέα. Όπως λέει και ο Ondrej Vlcek «οι συγγραφείς του κακόβουλου λογισμικού για Η/Υ ξεκίνησαν να εργάζονται σε γκαράζ, ενώ οι συγγραφείς του κακόβουλου λογισμικού για

κινητά σε γραφεία» [Β.4.Η.21], εννοώντας ότι οι πρώτοι ενασχολήθηκαν με τη συγκεκριμένη συγγραφή αρχικά βλέποντάς την ως χόμπυ ενώ οι δεύτεροι εξ' αρχής ως πηγή κέρδους. Και εφόσον τα πρώτα κακόβουλα λογισμικά για κινητά αρχίζουν να προσδίδουν έσοδα στους συγγραφείς τους, συνέχεια αναπτύσσονται νέα τέτοια λογισμικά, αφού και ο κόσμος χρησιμοποιεί όλο και περισσότερο τις κινητές συσκευές για ευαίσθητες συναλλαγές όπως αγορές και online banking.

Όσο για τους σταθερούς υπολογιστές, η εκμετάλλευση μιας αδυναμίας μπορεί να γίνει η αιτία λόγω της οποίας ο κακόβουλος κωδικός θα εγκατασταθεί σε μια κινητή συσκευή.

4.2 Ανάπτυξη του κακόβουλου λογισμικού: Ποσοστά και αριθμοί ανά χρονικές στιγμές

Σύμφωνα με το άρθρο του Dan Kaplan, αποκλειστικού εκδότη του περιοδικού SC Magazine), το οποίο φέρει τον τίτλο «Beyond Theory: Malware mobile» και το οποίο αναρτήθηκε και στο διαδίκτυο στις 3/10/2011, το κακόβουλο λογισμικό για κινητά, που συχνά εξαπλώνεται μέσω εφαρμογών, αυξάνεται επιτηδευμένα. Έτσι προβλέπεται από μυριάδες καταγραφές ότι το 2010 και 2011 θα σημειωνόταν μια απότομη αύξηση στον αριθμό του κακόβουλου λογισμικού που στοχεύει σε κινητές συσκευές. Σύμφωνα με μία αναφορά της MacAfee που δημοσιεύθηκε το Φεβρουάριο του 2011, ο αριθμός των νέων κακόβουλων λογισμικών για ποικίλα κινητά ήταν στο σύνολο 55.000 το 2010 με μια αρκετά μεγάλη αύξηση της τάξης του 46% σε σύγκριση με το 2009. Ολοφάνερα, η απειλή σημείωσε μεγάλη αύξηση από το 2004, όταν στάλθηκε για έλεγχο το 1ο κακόβουλο λογισμικό για κινητά, γνωστό ως Campir, σε εταιρείες παροχής ηλεκτρονικής ασφάλειας για κακόβουλα λογισμικά. Το σκουλήκι, που δημιουργήθηκε για κινητά με χαρακτηριστικά λειτουργικού συστήματος Symbian, δεν ήταν κάτι απλό κι ακίνδυνο (ήταν σχεδιασμένο να εμφανίζει τη λέξη "Caribe" στην οθόνη των τηλεφώνων και να εξαπλώνεται σε άλλες συσκευές μέσω Bluetooth). Απεναντίας, η άφιξή του αποδείχτηκε προφητική 2 χρόνια αργότερα, το 2006, όταν στο εργαστήριο της Kaspersky ταυτοποιήθηκε με αυτό το πρώτο κακόβουλο λογισμικό σχεδιασμένο να κλέβει χρήματα- ήταν ένας ιός που στόχευε σε συσκευές που «τρέχουν» java. Ο ιός Dubbed RedBrowser, έστελνε γραπτά μηνύματα σε premium rate αριθμούς, χωρίς να το συνειδητοποιεί ο χρήστης.

Προχωρώντας στο 2011, φαίνεται ότι το κρίσιμο σημείο πλησιάζει. Σύμφωνα με τον Νίλσεν, ο αριθμός των έξυπνων συσκευών όπως iPhone, Blackberry και Android στις ΗΠΑ, αναμένεται να ξεπεράσει αυτόν των συμβατικών τηλεφώνων. Αυτή η σταθερή άνοδος από τις εύχρηστες συσκευές που παρέχουν πέραν της κλήσης και των γραπτών μηνυμάτων σε κινητά με λειτουργία που μοιάζει με αυτήν ενός παραδοσιακού υπολογιστή και κάποιες ακόμα δυνατότητες έχει φυσικά κεντρίσει το ενδιαφέρον της κοινότητας που ασχολείται με το κακόβουλο λογισμικό. Έπειτα από δοκιμές που διήρκησαν χρόνια και επηρέασαν βαθύτατα τους χρήστες κινητών τηλεφώνων παγκοσμίως, οι εγκληματίες του διαδικτύου τώρα ανασκουμπώνονται και ετοιμάζουν τα προϊόντα ώστε να μοιάζουν σε αυτά τα οποία τα θύματα είναι συνηθισμένα να βλέπουν στους υπολογιστές τους.

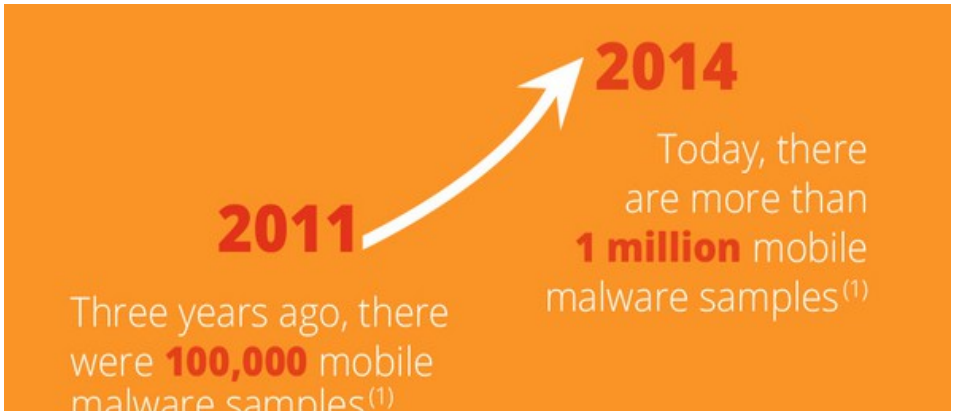
Τα smartphones έχουν όλα τα χαρακτηριστικά που θα περίμενε κανείς να έχει ένας παραδοσιακός Η/Υ. Είναι ικανά και πολυσύνθετα, ενώ διαθέτουν λειτουργικά συστήματα και εφαρμογές που υπερλειτουργούν. Οι χάκερς έχουν γράψει τον περισσότερο κώδικα κακόβουλου λογισμικού για κινητές συσκευές Symbian και Windows επειδή είναι οι παλιότερες και περισσότερο μελετημένες συσκευές. Όμως όλο αυτό φαίνεται να αλλάζει.

Σύμφωνα με μία έρευνα της εταιρίας δικτύων Juniper, που δημοσιεύθηκε το Μάιο του 2011, δείγματα κακόβουλου λογισμικού στοχεύουν σε Google Android συσκευές, με μία αυξανόμενη τάση της τάξεως του 400% από τον Ιούνιο του 2010 έως τον Ιανουάριο του 2011. Αυτό δεν εκπλήσσει. Εξάλλου, τα ποσοστά κέρδους της αγοράς υπαγορεύουν το κακόβουλο λογισμικό. Μια σειρά ερευνών που διεξήχθησαν από τον Nielsen από το Φεβρουάριο ως το Μάρτιο του 2011 έδειξε ότι το 31% των πελατών που σχεδίαζαν να αγοράσουν ένα νέο smartphone, προτίμησαν Android, σε σύγκριση με το 30% που θα επέλεγαν iPhone και το 11% που θα προτιμούσαν ένα BlackBerry. Ένα 20% δεν ήταν σίγουροι τι θα αγόραζαν. Συγκρίνοντας όλες τις εταιρίες, ενώ τα BlackBerry θεωρούνται η -χρυσή σταθερά- για την ασφάλεια των επιχειρήσεων παγκοσμίως, λόγω των ικανοτήτων που προσφέρουν σε θέματα μάνατζμεντ και κρυπτογράφησης, πολλοί εργαζόμενοι προτιμούν τα κουδούνια και τις σφυρίχτρες που παρέχουν η Android και η iPhone.

Πολλοί ειδικοί συμφωνούν ότι αυτό που κάνει την πλατφόρμα Android να αποτελεί πρόσφορο στόχο επιθέσεων σε σχέση με άλλα λειτουργικά συστήματα κινητών είναι η όλο και μεγαλύτερη επέκταση των εφαρμογών της στην αγορά. Σύμφωνα με την εταιρία προστασίας λογισμικού Lookout ο αριθμός των διαθέσιμων εφαρμογών στην αγορά Android ανέβηκε κατά 127% από τον Αύγουστο του 2010 μέχρι το Φεβρουάριο του 2011, ενώ το κατάστημα εφαρμογών της Apple αυξήθηκε κατά 44%. Τα τελευταία νούμερα δείχνουν ότι η αγορά Android περιέχει σχεδόν 300.000 εφαρμογές για download. Το πρόβλημα είναι ότι σε ορισμένες περιπτώσεις οι εφαρμογές αυτές είναι από τη φύση τους -κακές-, προσαρμοσμένες να εγκαθιστούν κακόβουλο λογισμικό στο κινητό ή να αποκτούν πρόσβαση σε ευαίσθητες πληροφορίες. «Είναι το πως πλασάρει κανείς το προϊόν του, ο βασικός παράγοντας που ανεβάζει τις συσκευές τηλέφωνων» σύμφωνα με τον Chris Wysopal, συνιδρυτή και επικεφαλή της ομάδας εργασίας μιας εταιρίας ασφάλειας εφαρμογών, ονόματι Veracode. Τα Android, συνεχίζουν με πιο ανοιχτό μοντέλο τακτικής, και επιτρέπουν προγραμματιστές να κατοχυρώνουν τα δικαιώματα των εφαρμογών που έχουν δημιουργήσει με την υπογραφή τους και έπειτα να διαθέτουν τις εφαρμογές για downloading στην αγορά. Ενώ οι φορείς ασφάλειας παραδέχονται ότι τη μερίδα του λέοντος για τα κακόβουλα λογισμικά την έχουν τα πιο επικερδή περιβάλλοντα Η/Υ, αυτό δεν έχει σταματήσει τους συγγραφείς από το να μοστράρουν τους κωδικούς τους με αποτέλεσμα να μπορεί να διεισδύει ο καθένας σε περιβάλλοντα περιήγησης. Και βέβαια τα κακόβουλα λογισμικά υπό

αυτές τις συνθήκες κάνουν πολύ εύκολα τη δουλειά τους δεδομένου ότι το 85% των χρηστών smartphone δεν χρησιμοποιούν anti-virus.

Οι εφαρμογές της Rogue (εταιρία προστασίας λογισμικού) από την άλλη μεριά, αναπτύσσονται επιτηδευμένα. Τον Αύγουστο του 2010 σύμφωνα με την Juniper, ο πρώτος Δούρειος ίππος για Android εμφανίστηκε με τη μορφή μιας εφαρμογής η οποία μιμούνταν ένα media player και έστελνε γραπτά μηνύματα σε ρώσικους premium rate αριθμούς, χρεώνοντας 6 δολάρια το μήνυμα. Με τον ερχομό του 2011, έγινε γρήγορα φανερό ότι οι συγγραφείς κακόβουλου λογισμικού γίνονταν γρήγορα επικίνδυνοι. Ένας δούρειος ίππος για Android, το ονομαζόμενο Geinimi, περιείχε δυνατότητες σύνδεσης με κακόβουλο δίκτυο botnet. Τρεις μήνες αργότερα, η Google αναγκάστηκε να αποσύρει περισσότερες από 50 εφαρμογές Android από την αγορά επειδή περιείχαν κακόβουλο λογισμικό γνωστό ως “DroidDream”, το οποίο ήταν ικανό να αποκτά πρόσβαση στην -ρίζα-, συλλέγοντας δεδομένα και εγκαθιστώντας επιπλέον κακόβουλο κωδικό.



Εικόνα 4.1: Το κακόβουλο λογισμικό για κινητά από το 2011 έως το 2014 [Β.4.Η.21]

Τέλος, η επιχείρηση του κακόβουλου λογισμικού είναι ακόμη σε εξελισσόμενο στάδιο και οι επιτήδειοι σκέπτονται ακόμα πιο μοντέλο κακόβουλου λογισμικού θα τους επιφέρει περισσότερο έσοδα σύμφωνα και με τον Kevin Mahaffey, επικεφαλή της ομάδας εργασίας της Lookout, ενώ σύμφωνα με ένα άρθρο του Ondrej Vlcek στο blog της avast που αναρτήθηκε στις 09/09/2014 υπολογίζεται ότι το 2018 οι απειλές για κινητά τηλέφωνα θα φτάσουν σε μέγεθος σπουδαιότητας τις απειλές για Η/Υ [Β.4.Η.21]

4.3 Υπερβολικά πολλά προνόμια

Σύμφωνα με ένα άλλο άρθρο επίσης του κ. Dan Kaplan το οποίο αναρτήθηκε στο SC Magazine στις 2/1/2012 και φέρει τίτλο «Focusing on mobile malware», άλλες κυρίαρχες ύπουλες εφαρμογές είναι αυτές στις οποίες αναφέρονται οι ειδικοί με τη λέξη “greynets”. Είναι εκείνα τα προγράμματα που δεν είναι απαραίτητα κακόβουλα, όμως απαιτούν περιττές

άδειες- όπως πρόσβαση στο hardware, στις ρυθμίσεις και τα δεδομένα του χρήστη- για να εκτελέσουν τις λειτουργίες τους. Αυτό επιτρέπει τη διαρροή μυστικών δεδομένων. Στην πραγματικότητα, μία αναφορά από 5 ερευνητές, του τμήματος της Ηλεκτρονικής Μηχανολογίας του πανεπιστημίου της Καλιφόρνια αποκάλυψε ότι το 1/3 από τις 940 εφαρμογές που εξετάσθηκαν ζητούν υπερβολικά πολλά προνόμια.

Η έρευνα ακόμη λέει ότι οι προγραμματιστές, στις περισσότερες περιπτώσεις, δεν σκαρώνουν κάτι το κακόβουλο απλά αποτυγχάνουν στο να επιτρέπουν λιγότερα προνόμια. Υπάρχουν και μερικές εφαρμογές, τα λεγόμενα spyware (λογισμικό κατασκοπείας) τα οποία ζητούν άδεια εισαγωγής στο σύστημα δήθεν για να εντοπίσουν ύποπτα στοιχεία απάτης.

Οι χρήστες θα πρέπει να είναι προσεκτικοί με όλες τις εφαρμογές που εγκαθιστούν στο κινητό τους και πρέπει να είναι σίγουροι ότι καταλαβαίνουν γιατί ένα πρόγραμμα απαιτεί άδεια εισαγωγής στη διαχείριση του συστήματος, λέει ο Chris Wysopal (ειδικός στην ασφάλεια συστημάτων). Δυστυχώς, οι περισσότεροι άνθρωποι δε δίνουν πολύ σημασία σε αυτό- απλά θέλουν την εφαρμογή. Για παράδειγμα, τον περασμένο Ιούλιο, η Citigroup, αναγκάστηκε να κυκλοφορήσει μια αναβάθμιση στη διατραπεζική της εφαρμογή διότι ανακάλυψε ότι η προηγούμενη έκδοση, εν αγνοία των χρηστών αποθήκευε χρηστικές πληροφορίες λογαριασμού σε ένα κρυμμένο αρχείο στις συσκευές. Ακόμη και εφαρμογές που θεωρούνται στάνταρ στα κινητά μπορεί να είναι μερικές φορές ευάλωτες. Υπάρχει επίσης και το ενδεχόμενο του jail breaking, όπως αναφέρει και ο Paul Ducklin σε ένα ηλεκτρονικό άρθρο του που αναρτήθηκε στις 22/08/2014 στην ιστοσελίδα nakedsecurity.sophos.com με τίτλο «Apple iOS malware gets onto 75,000 iPhones, steals ad clicks», κατά το οποίο οι χρήστες, συχνά με σκεπτικό ειρωνείας και προκειμένου να αποκτήσουν την ελευθερία που επιθυμούν κατά τη χρήση για παράδειγμα του iPhone ή του iPad τους, απορρίπτουν τους ελέγχους ασφαλείας που πραγματοποιεί την χρονική στιγμή download μιας εφαρμογής η Apple. Το αποτέλεσμα είναι να ανακόπτεται η επιλογή αποδοχής ή απόρριψης των διαφόρων εφαρμογών που κατεβάζει ο χρήστης από το διαδίκτυο και έτσι ανεξέλεγκτα να επιτρέπεται η είσοδος μεταξύ άλλων και μολυσμένων εφαρμογών στο σύστημα [Β.4.Η.20]. Γερμανοί ερευνητές το Μάιο του 2011, ανακάλυψαν ότι το ημερολόγιο και οι εφαρμογές της Android έχουν ένα ελάττωμα το οποίο θα μπορούσε να επιτρέψει τον επιτιθέμενο μέσω δημοσίων δικτύων Wi-Fi, να κρυφακούει και να υποκλέπτει πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν ανά πάσα ώρα για την πρόσβαση σε προσωπικά δεδομένα.

4.4 Η τάση του κέρδους από τη μόλυνση λογισμικού κινητών συσκευών

Σύμφωνα με την ιστοσελίδα bgr.com και το άρθρο του Zach Epstein που δημοσιεύτηκε στις 14/12/2011, το 2012, οι δημιουργοί κακόβουλου λογισμικού συνέχισαν να κλέβουν χρήματα απευθείας από τους πελάτες αποκτώντας πρόσβαση στο σύστημα του

κινητού τους τηλεφώνου, μέσω μηνυμάτων και τηλεφωνικών κλήσεων. Κατά το 2011 η Lookout αναγνώρισε το GGTracker, ένα κακόβουλο λογισμικό που κλέβει χρήματα από πελάτες και ταυτοποίησε το RuFraud, ένα άλλο κακόβουλο λογισμικό για κινητά τύπου trojan, που στόχευε σε χρήστες της ανατολικής Ευρώπης.

Botnets. Ως σήμερα η Lookout σημειώνει ότι τα botnets εξελίσσονται. Οι συγγραφείς κακόβουλου λογισμικού θα μπορούσαν κρυφά να εντάξουν χιλιάδες κινητές συσκευές σε εκτεταμένα δίκτυα που μοιάζουν με botnet ώστε να διαμερίζουν τις λειτουργίες τους, να κλέβουν ιδιωτικές πληροφορίες και να εγκαθιστούν άλλο κακόβουλο λογισμικό. Το DroidDream και το Geimini είναι παραδείγματα Botnets.

Ευάλωτα τηλέφωνα. Λόγω του ότι είναι δύσκολο να αναβαθμίσει κανείς το λογισμικό ενός κινητού τηλεφώνου και λόγω της ευαισθησίας του σαν εργαλείο, οι συγγραφείς κακόβουλου λογισμικού συνεχίζουν να εκμεταλλεύονται iOS and Android OS με ρυθμό μεγαλύτερο από αυτόν με τον οποίο θα μπορούσαμε να αντιμετωπίσουμε.

Τάσεις διαμερισμού του κακόβουλου λογισμικού σε ένα λειτουργικό σύστημα κινητού τηλεφώνου. Οι δημιουργοί κακόβουλου λογισμικού αναπτύσσουν εργαλεία που καθιστούν ικανή την εξάπλωση κακόβουλων εφαρμογών. Η Lookout έχει συναντήσει περιστατικά κατά τα οποία ορισμένες μολυσμένες εφαρμογές πακεταρίστηκαν από τον ίδιο προγραμματιστή μέσα σε λίγα δευτερόλεπτα – πιο γρήγορα από ότι θα μπορούσε να κάνει κανείς χειροκίνητα- έτσι τα μέσα για το repacking μάλλον ήδη υπάρχουν.

Επιθέσεις Browser. Όσων αφορά στις επιθέσεις Browser, στο παρελθόν, οι συγγραφείς κακόβουλου λογισμικού προσπάθησαν να αποκομίσουν κέρδη με το διαμερισμό της διαδικασίας μόλυνσης του λειτουργικού συστήματος μιας συσκευής με mail, γραπτά μηνύματα και ύπουλες ιστοσελίδες. Ακόμη και οι συσκευές iOS είχαν γίνει στόχος από ιστοσελίδες σχεδιασμένες για jailbreak. Το 2012, σύμφωνα με τη Lookout σημειώθηκε μια συνεχόμενη αύξηση στο “ψάρεμα” κινητών συσκευών και στα μηνύματα τα οποία είναι συνδεδεμένα και προέρχονται από ιστοσελίδες που εγκαθιστούν κακόβουλο λογισμικό αυτόματα.

Malvertising. Το Malvertising (διαφημίσεις, που φαίνονται αυθεντικές, ενώ συνδέονται με άλλες -κακές- ιστοσελίδες) θα συνεχίσει να αυξάνεται. Δεδομένου ότι αυτή η μέθοδος ήταν επιτυχής με Δούρειους ίππους όπως ο GGTracker, πλέον κι άλλοι συγγραφείς κακόβουλου λογισμικού σκοπεύουν να εφαρμόσουν παρόμοιες τακτικές διανομής.

4.5 Κορυφαίος στόχος: το Android

Σε ένα άρθρο του Joanie M. Wexler, αναλυτή της τεχνολογίας, το οποίο αναρτήθηκε στην ιστοσελίδα webtutorials.com επισημαίνονται τα παρακάτω. Το Android λειτουργικό σύστημα της Google κυκλοφορεί τώρα περίπου στα μισά από τα smartphones παγκοσμίως. Δεδομένου του bring-your-own-device, είναι μη ρεαλιστικό να σκεφτόμαστε ότι μπορούμε να κρατήσουμε συσκευές βασισμένες στο Android έξω από την ομάδα. Ωστόσο, το ηλεκτρονικό κατάστημα εφαρμογών της εταιρίας που προσφέρει περισσότερες από 300.000 εφαρμογές, υπέφερε από αρκετές επιθέσεις ιδιαίτερα διαδεδομένου κακόβουλου λογισμικού κατά το 2011, αναγκάζοντας την Google να αχρηστέψει μερικές εφαρμογές που προσβλήθηκαν.

Μερικοί λόγοι με τους οποίους επεξηγεί ο Joanie M. Wexler την αδυναμία (ευαισθησία της Android) είναι οι εξής:

- είναι “ανοιχτό”. Παρ' όλο που οι ανοιχτές πλατφόρμες ευνοούν τη δημιουργικότητα και οδηγούν σε επιλογές ανάλογες των εφαρμογών για την υποστήριξη του hardware, το μειονέκτημα είναι ότι πολλοί άνθρωποι μπορούν να ανακαλύψουν μέχρι εσχάτως το λειτουργικό σύστημα, σε σημείο που να μπορούν και να το εκμεταλλευτούν (σκεφτείτε τα Windows).
- Χαμηλό επίπεδο αυστηρότητας στον έλεγχο εφαρμογών που πωλούνται στην αγορά της Google Android. Αυτό διευκολύνει τους κακόβουλους να μπουν στο κατάστημα. Υπάρχουν επίσης εναλλακτικά καταστήματα εφαρμογών Android, όχι επισήμως υποστηριζόμενα από την Google, και μερικά έχουν συμπεριλάβει ανασυσκευασμένες εκδοχές νόμιμων εφαρμογών που περιλαμβάνουν adware ή και trojans.
- Η όλο και αυξανόμενη ευρεία υιοθέτηση από το κοινό, οδηγεί τους χάκερς στην Android όπως οι αρκούδες στο μέλι.

Η Symantec σε ένα άρθρο που δημοσιεύτηκε το 2012 στο κομμάτι «Threats activity trends» της ιστοσελίδας της σχετικά με την αύξηση των κινδύνων του Android, αναφέρει ότι η κατηγορία των δούρειων ίππων που ανιχνεύτηκαν σε κινητά Android, ονόματι Opfake, που στοχεύει στην Ανατολική Ευρώπη, είναι ένα καλό παράδειγμα απειλής. Αυτή η απειλή γράφτηκε αρχικά για τηλέφωνα που διέθεταν λειτουργικά συστήματα Windows Mobile/Symbian/JAVAME. Παρόμοια πειράματα έγιναν στην Κίνα όπου εμφανίστηκαν νέες απειλές οι Android.Adsms και Android.Stiniter. Και οι δυο ήταν αρχικά απειλές για Symbian πριν οι συγγραφείς τους στοχεύσουν προς τα Android. Αναμένουμε ότι αυτή η τάση θα αυξηθεί, ειδικά όταν πρόκειται για απειλές που πέραν του βασικού δικτύου στοχεύουν και σε θυγατρικά υποδίκτυα.

4.6 Στρατόπεδο της Apple

Στο ίδιο άρθρο του Joanie M. Wexler, αναλυτή της τεχνολογίας, το οποίο αναρτήθηκε στην ιστοσελίδα webtutorials.com που αναφέρθηκε ανωτέρω επισημαίνεται επίσης ότι η πλατφόρμα iOS της Apple έχει υπάρξει πιο ασφαλής λόγω του κλειστού οικοσυστήματός της. Όμως η τσιγκουνιά της Apple με την χαμηλού επιπέδου διεπαφή της με τον χρήστη σημαίνει ότι οι προγραμματιστές του iOS δεν μπορούν εύκολα να καταλάβουν αν μία συσκευή της Apple έχει πέσει θύμα jailbroken (δηλαδή αν το λειτουργικό της σύστημα έχει προσπελαστεί από κάποιον τρίτο με άσχημες προθέσεις) ή ακόμα εάν η ίδια η συσκευή έχει αποκτήσει πρόσβαση σε άλλες εφαρμογές, για να μπορέσουν τελικά να αναγνωρίσουν το ύποπτο κακόβουλο λογισμικό.

Και παρά τη στενή αστυνόμευση της Apple για το τι μπαίνει στο κατάστημα εφαρμογών της, μερικές ρωγμές εμφανίστηκαν στην πορεία. Για παράδειγμα, περίπου στα τέλη του 2012 γνωστοποιήθηκε ότι το κατάστημα εφαρμογών της Apple πούλησε εφαρμογές όπως το PATH train, οι οποίες μεταδίδουν ένα πλήρες βιβλίο διευθύνσεων του χρήστη σε απομονωμένο server για κατοπινή επεξεργασία χωρίς άδεια - παρ' όλο που το να συλλέγει κανείς δεδομένα επαφών χωρίς τη συναίνεση του χρήστη αποτελεί παραβίαση την κατευθυντήριας γραμμής της Apple.

Ενώ η Apple γενικά κάνει καλή δουλειά κρατώντας υπό έλεγχο τις εισβολές, τέτοια περιστατικά θα μπορούσαν να κλονίσουν την εμπιστοσύνη της βιομηχανίας, λόγω της ανικανότητας της Apple να βρει έναν τρόπο ασφάλειας πριν επιτύχουν την εκμετάλλευση των πελατών της οι χάκερς, παρακινούμενοι από οικονομικό όφελος.

4.7 Παλιά κόλπα που μεταφέρονται σε νέες πλατφόρμες

Στο ίδιο άρθρο της Symantec που δημοσιεύτηκε το 2012 στο κομμάτι «Threats activity trends» της ιστοσελίδας της σχετικά με την αύξηση των κινδύνων του Android αναφέρεται ακόμη ότι η διακίνηση μηνυμάτων σε premium rate αριθμούς ήταν πάντα πρόβλημα όσων αφορά στις απειλές σε κινητά, ειδικά στην Ανατολική Ευρώπη, όπου οι επιτήδειοι ενεργούσαν σχεδόν αμέσως από τη στιγμή που ο χρήστης εγκαθιστούσε την έκδοση της Java για κινητές συσκευές. Δε θα πρέπει να προκαλεί έκπληξη το γεγονός ότι οι συγγραφείς κώδικα οι οποίοι επηρεάζουν αυτήν την κερδοφόρα πηγή εισοδήματος κάνουν μια αλλαγή - προσαρμογή στις νεότερες, δημοφιλείς πλατφόρμες.

Οι δημιουργοί των απειλών για κινητά γίνονται πιο στρατηγικοί και θαρραλέοι στις προσπάθειές τους. Ένα καλό παράδειγμα αυτού του γεγονότος είναι οι απόπειρες να περιπλέξουν την απεγκατάσταση μιας μόλυνσης. Μια τέτοια στρατηγική που χρησιμοποιείται είναι ο κατακερματισμός των κακόβουλων πακέτων εν ώρα εργασίας. Η ιδέα είναι απλή, αντί να έχουν ένα φορτίο να κουβαλάει ολόκληρο το κακόβουλο περιεχόμενο σπάνε την απειλή σε ξεχωριστές download μονάδες. Τα μικρότερα κομμάτια είναι πιο εύκολο να κρυφτούν, φαίνονται να είναι αβλαβείς ενημερώσεις και έτσι περιπλέκουν τη διαδικασία κατάργησης που

υπάρχει ως επιλογή από τον πάροχο υπηρεσιών, την αγορά κτλ. Στις περισσότερες περιπτώσεις απάτης και αποστολής μηνύματος σε premium rate αριθμούς οι επιτήδειοι, και/ή καλούντες δεν ακολουθούν κάποια συγκεκριμένη πολιτική. Για να δουλέψουν εξαρτώνται πολύ από το λεγόμενο social engineering, το οποίο είναι εργαλείο για τους συγγραφείς κακόβουλου λογισμικού για κινητά (εξαπατά και εκμεταλλεύεται άκρως εμπιστευτικά δεδομένα του χρήστη).

Παρόλα αυτά, η αποστολή μαζικών μηνυμάτων υπάρχει πολλά χρόνια τώρα και σαν μέθοδος μπορεί να έχει πίσω της επενδύσεις που εφαρμόζονται γρήγορα από εγκληματίες.

Μια άλλη ενδιαφέρουσα τάση που παρατήρησε η Symantec είναι η χρήση της μεθόδου in-app promotion που εφαρμόζουν οι επιτήδειοι προτρέποντας τον χρήστη να κατεβάζει επικίνδυνες εφαρμογές. Μια τέτοια εφαρμογή απαιτεί από τον χρήστη να κατεβάσει την εφαρμογή που επιθυμεί από μη εξουσιοδοτημένους browsers ή από ένα κατάστημα εφαρμογών που δεν είναι όμως εξουσιοδοτημένο από τον δημιουργό της εφαρμογής.

Παρόλο που απαιτείται έγκριση του χρήστη για να εγκατασταθούν επιπλέον εφαρμογές, ο λόγος ανησυχίας εδώ είναι ότι η όλη διαδικασία εμπεριέχει ένα στοιχείο social engineering (εξαπάτησης και εκμετάλλευσης άκρως εμπιστευτικών δεδομένων του χρήστη) και ο τελικός χρήστης υποθέτει ότι αφού η πρώτη εφαρμογή κατέβηκε από το επίσημο κανάλι όποιες επιπλέον εφαρμογές κατεβάζει θα προέρχονται όλες από εκεί και θα είναι αυθεντικές.

Λόγω του αποκαλούμενου θέματος ‘fragmentation hardware’ (της έλλειψης συγχρονισμού και συντονισμού των πολλών εφαρμογών του Android με του hardware), μια δημοφιλής υπηρεσία εκπομπής βίντεο online στις ΗΠΑ είχε αρχικά προωθήσει μια εφαρμογή για τους πελάτες της Android σε περιορισμένη κυκλοφορία, απευθυνόμενη μόνο σε συσκευές που παρείχαν την καλύτερη εμπειρία στο χρήστη. Χάρη στη δημοτικότητα της υπηρεσίας, λίγο μετά την αρχική κυκλοφορία πολλές προσπάθειες έγιναν από διάφορους κατασκευαστές λογισμικού για να εισάγουν ένα ανεπίσημο αντίγραφο της εφαρμογής σε συσκευές που δεν λειτουργούσαν καλά. Ένα κενό στη διαθεσιμότητα για ορισμένες συσκευές σε συνδυασμό με ένα μεγάλο ενδιαφέρον από τους χρήστες στο να αποκτήσουν την εφαρμογή στην Android συσκευή τους δημιούργησε την τέλεια κάλυψη για τον Android.Flicker, ένα παράδειγμα εγχειριδίου ενός υποκλοπέα πληροφοριών που στόχευε σε πληροφορίες λογαριασμού.

Η κακόβουλη εφαρμογή δεν είναι σύνθετη για να την καταλάβουμε. Χωρισμένη σε δύο κύρια μέρη αποτελείται κατά κόρον από μια splash οθόνη ακολουθούμενη από μια οθόνη σύνδεσης όπου βρίσκονται οι πληροφορίες χρήστη και μάλιστα, αναρτημένες σε έναν server. Υπάρχουν πολλαπλές άδειες που απαιτούνται την ώρα της εγκατάστασης, αυτό είναι σημάδι μιας κακόβουλης εφαρμογής. Όμως σε αυτήν την περίπτωση οι άδειες είναι πανομοιότυπες με τις άδειες που απαιτούνται από τη νόμιμη εφαρμογή. Αυτό πιθανόν έγινε από τους κακόβουλους για να δώσουν την ψευδαίσθηση ότι εγκαθίσταται η νόμιμη εφαρμογή.

4.8 Απειλές υποκινούμενες από πολιτικούς σκοπούς

Ο ακτιβισμός δεν απαγορεύεται στα PC όπως αναφέρεται στο άρθρο της Symantec το οποίο αναλύεται ανωτέρω. Το 2011 εμφανίστηκε κακόβουλο λογισμικό χωρίς ιδιαίτερο νομισματικό κέρδος αλλά με στόχο να στείλει ένα μήνυμα. Ένα παράδειγμα: για πολλούς σε όλον τον Αραβικό Κόσμο, η 18η Δεκεμβρίου 2010 σηματοδότησε τη γέννηση αυτής που είναι ευρέως γνωστή ως 'Η Αραβική Άνοιξη'. Ανάμεσα στα πολλά εργαλεία που χρησιμοποιούνται για να συντονίσουν και να πληροφορήσουν την αγορά, η Symantec ανακάλυψε έναν trojan, που έστελνε μαζικά mail και εμπλούτιζε με κακόβουλο υλικό τις συσκευές Android στις οποίες είχε προστεθεί.

Ο trojan είχε προστεθεί σε μια πειρατική έκδοση μιας δημοφιλούς Ισλαμικής εφαρμογής πυξίδας και διανέμονταν μόνο μέσω φόρουμ που επικεντρώνονταν σε θέματα της Μέσης Ανατολής. Η επίσημη έκδοση της εφαρμογής που ήταν διαθέσιμη στην Αγορά Android δε μολύνθηκε. Μετά την εγκατάσταση της πειρατικής εφαρμογής, ο κώδικας στόχευε σε αρχεία επανεκκίνησης, δουλεύοντας αθόρυβα στο παρασκήνιο. Επέλεγε τυχαία ένα σύνδεσμο από μια προκαθορισμένη λίστα με δεκαοκτώ συνδέσμους και έπειτα έστελνε SMS σε κάθε επαφή του βιβλίου διευθύνσεων της μολυσμένης συσκευής, με ένα συνδέσμο που παρέπεμπε σε ένα φόρουμ το οποίο είχε ως θέμα τον Mohamed Bouaziz.

4.9 Τα καταστήματα εφαρμογών - δόλωμα στην εγκατάσταση κακόβουλου λογισμικού

Σύμφωνα με τη Symantec και το κείμενο περί των τάσεων της απειλής για τις κινητές συσκευές που αναρτήθηκε το 2012 στην ιστοσελίδα της με τίτλο «Analysis of mobile threats» με την προβλεπόμενη ανάπτυξη των πωλήσεων smartphones να ξεπερνά αυτήν των συνηθισμένων τηλεφώνων, δεν αποτελεί έκπληξη να δούμε τη ζήτηση για drivers να οδηγεί στην εμφάνιση νέων τόπων αγοράς εφαρμογών, καταστημάτων εφαρμογών και ιστοσελίδων download. Επωφελούμενοι από την αυξανόμενη ζήτηση των drivers, χωρίς την παρουσία επίσημων εξουσιοδοτημένων καταστημάτων, σε ορισμένες περιοχές του πλανήτη ο αριθμός παράνομων αγορών σημειώνει δραματική αύξηση, παρέχοντας ένα τέλειο εκκολαπτήριο και μια μηχανή εξάπλωσης για κακόβουλο λογισμικό.

Σε περιοχές όπως η Κίνα η Symantec έχει παρατηρήσει ότι αυτοί οι πάροχοι υπηρεσιών τείνουν να είναι λίγο πιο τολμηροί και λειτουργούν με αυτό που θα μπορούσε να περιγραφεί καλύτερα ως ρηξικέλευθο χάρισμα. Πέρα από το να έχουν τη συνηθισμένη βιτρίνα εφαρμογής για κινητά, για να ενθαρρύνουν τους τοπικούς συγγραφείς να υποβάλουν πρωτότυπο περιεχόμενο, έχουν μια ισχυρή οπτική παρουσία Web και χρησιμοποιούν αυτήν την παρουσία χρησιμοποιώντας το μερίδιο της διαφήμισης ως νομισματικό κίνητρο. Κατά ειρωνεία, σε μερικές περιπτώσεις φαίνεται ότι ανήκουν σε επίσημες αγορές, θολώνοντας ακόμη περισσότερο τα νερά, βασιζόμενοι σε μη πραγματικό αλλά πειρατικό περιεχόμενο.

Με πωλήσεις περίπου $15 δισεκατομμυρίων το 2011, ο αριθμός των καταστημάτων εφαρμογών στην Κίνα συνέχισε να αναπτύσσεται με δραματικό ρυθμό. Καθώς ο βασικός μηχανισμός εξέτασης του περιεχομένου είναι αδρανής, το πειρατικό ή κακόβουλο περιεχόμενο δεν εντοπίζεται αμέσως και οι διαχειριστές ιστοσελίδων αρνούνται κάθε εγγύηση σε ζημιές που προκύπτουν από τη χρήση κατεβασμένου λογισμικού. Από την οπτική ενός κακόβουλου συγγραφέα, αυτές οι ιστοσελίδες τείνουν να είναι οι ευκολότερες να στοχεύσει κανείς, καθώς οι χρήστες που επισκέπτονται αυτές τις ιστοσελίδες έχουν απενεργοποιήσει τους ελέγχους ασφαλείας της συσκευής τους για να επιτρέπουν την εγκατάσταση μη υπογεγραμμένου λογισμικού. Αυτό λέγεται side loading.

Η Κίνα (ακολουθούμενη στενά από την Ανατολική Ευρώπη) μαστίζεται εδώ και καιρό από απειλές και εφαρμογές μολυσμένες με trojan που στοχεύουν σε πλατφόρμες για κινητά. Απάτες που στέλνουν αθόρυβα SMS σε premium rate αριθμούς έχουν επικρατήσει τόσο πολύ που η Κινεζική κυβέρνηση αναγκάστηκε να θέσει κανονισμούς διευθέτησης για να πάρει αυστηρά μέτρα όχι μόνο εναντίον των δημιουργών αλλά επίσης εναντίον των αδίστακτων που τις προωθούν. Σύμφωνα με το άρθρο 23 του Νομοθετικού Διατάγματος 147, καθιστά παράνομη οποιαδήποτε δραστηριότητα σχετίζεται με τη διασπορά ιών ή άλλου κακόβουλου λογισμικού. Οι κυρώσεις που προβλέπονται για την παραβίαση των παραπάνω διατάξεων, περιλαμβάνουν χρηματικό πρόστιμο, που κυμαίνεται από 5.000 – 15.000 γιεν ανάλογα με τη σοβαρότητα του εγκλήματος [Β.1.2]. Οι αδίστακτοι μάλιστα που προωθούν τις απειλές πωλούν κινητά ήδη μολυσμένα και μάλιστα χορηγώντας εγγυήσεις. Όσο πιο μικρή είναι η εγγύηση, τόσο περισσότερο χρόνο χρειάζεται ένας χρήστης να υποπτευθεί ότι κάτι πάει στραβά.

ΚΕΦΑΛΑΙΟ 5ο: ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ

5.1 Εισαγωγή

Σύμφωνα με μία έρευνα της Symantec σε παγκόσμια κλίμακα σχετικά με τη χρήση των κινητών συσκευών, η οποία δημοσιεύθηκε το 2012 και τιτλοφορείται ως «State of mobility Survey» γίνεται σαφές ότι ο τρόπος με τον οποίο χρησιμοποιούμε το διαδίκτυο ως εργαλείο έχει αλλάξει εντελώς. Τα smartphones χρησιμοποιούνται πλέον από εκατοντάδες εκατομμύρια εργαζόμενους σε όλον τον κόσμο, για να ενημερώνονται για τον τρέχοντα επιχειρηματικό κόσμο 24 ώρες το 24/ωρο. Η Symantec το 2012 ανέλαβε να εκτιμήσει πως οι οργανισμοί ανταπεξέρχονται σε αυτή τη μόδα. Βάσει της έρευνας μιλώντας με 6.275 οργανισμούς μικρούς και μεγάλους σε 43 χώρες από τον Αύγουστο ως το Νοέμβριο του 2011, έχουμε φτάσει σε ένα σημείο καμπής στην επιχειρηματική χρήση των κινητών

συσκευών. Οι περισσότεροι οργανισμοί μπορούν και προσαρμόζονται. Επίσης αναπτύσσουν εφαρμογές και κάνουν ακόμα και σχέδια για εταιρικά καταστήματα εφαρμογών για τους υπαλλήλους τους, απ' όπου θα μπορούν να κατεβάζουν συγκεκριμένο υλικό. Όλα αυτά δείχνουν έναν στόχο, να καλυτερεύσει η εταιρική ευκινησία. Όπως αναφέρουν και οι Alla G. Kravets, Ngoc Duong Bui και Mohammed Al-Ashval στο σύγγραμμά τους με τίτλο «Mobile Security Solution for Enterprise Network», παρά το γεγονός ότι το φαινόμενο που περιγράφεται παραπάνω αυξάνει την αποδοτικότητα στην εργασία και προάγει την απόδοση των εργαζομένων, ωστόσο τίθεται το ζήτημα καταπάτησης της ιδιωτικότητας των δεδομένων και της ασφάλειας των πληροφοριών της εταιρίας [Β.3.2, Β.1.3, Β.1.17, Β.1.8]. Το σημαντικότερο θέμα που απασχολεί όσες επιχειρήσεις δραστηριοποιούνται ηλεκτρονικά και μάλιστα με τη χρήση κινητού τηλεφώνου είναι η ασφάλεια των συναλλαγών τους. Σήμερα ωστόσο, και ευτυχώς για τις επιχειρήσεις αυτές υπάρχουν αρκετές αξιόπιστες τεχνολογίες που μπορούν να εγγυηθούν την ασφάλεια των συναλλαγών[Β.1.5]. Οι επιχειρήσεις χάνουν ένα σημαντικό χρηματικό ποσό σε περιστατικά που σχετίζονται με κινητές συσκευές – μέχρι και 429.000 δολάρια σε περίπτωση μεγάλων επιχειρήσεων. Παρά τα κόστη αυτά όμως, οι οργανισμοί πιστεύουν ότι τα ρίσκα αξίζουν ως προς τα οφέλη και φροντίζουν ώστε να εφαρμόζουν τα απαραίτητα μέτρα ασφαλείας για να ρίχνουν στο ελάχιστον αυτά τα κόστη και να διαφυλάττουν τις εταιρικές πληροφορίες τους.

5.2 M-Commerce

Σύμφωνα με τον Geoffrey Elliott και τον Nigel Phillips και βάση του βιβλίου τους με τίτλο «Mobile Commerce and Wireless Computing Systems» το οποίο εκδόθηκε το 2004, ο ορισμός, τα εμπόδια και οι εφαρμογές του m- commerce αναλύονται ως εξής:

Ορισμός: Ως M-Commerce ορίζονται οι κινητές συσκευές και τα ασύρματα περιβάλλοντα Η/Υ, που είναι απαραίτητα για να παρέχεται συνδεσιμότητα από τη θέση του χρήστη.

Εμπόδια στο m-commerce: Τα εμπόδια του m-commerce, όπως το κόστος των κινητών συσκευών και των υπηρεσιών του κινητού διαδικτύου και η δυσκολία της αποτελεσματικής πρόσβασης και των γρήγορων τηλεπικοινωνιακών δικτύων, όλο και φθίνουν κάθε έτος. Έτσι το κινητό εμπόριο γίνεται όλο και πιο ενδιαφέρον για επιχειρήσεις και για άτομα (και για πολλούς εκπαιδευτές) [Β.1.20].

Εφαρμογές του m-commerce: Οι προσωπικές και επαγγελματικές εφαρμογές των κινητών τηλεπικοινωνιών και των διεισδυτικών υπολογιστικών συστημάτων είναι απεριόριστες. Τέτοια τεχνολογία αρέσει ιδιαίτερα σε επιχειρήσεις με έμψυχο δυναμικό εν κινήσει. Για παράδειγμα, διάφοροι επαγγελματίες όπως αρχιτέκτονες, ασφαλιστές, δημοσιογράφοι και πωλητές, μπορούν να εκτελούν τις δουλειές τους πιο αποτελεσματικά

χρησιμοποιώντας ασύρματες τεχνολογίες και κινητές συσκευές. Αυτό δημιουργεί έναν επαγγελματία εν κινήσει που χρησιμοποιεί τεχνολογία κινητών Η/Υ με διαφορετικούς τρόπους, για να ανταποκριθεί σε συγκεκριμένους στόχους της δουλειάς του.

5.3 Αποτέλεσμα έρευνας για τη σχέση κινητής τηλεφωνίας και εταιριών

Η Symantec ανέλαβε να σφυγμομετρήσει την κατάσταση που επικράτησε στην κινητή τηλεφωνία από τον Αύγουστο ως το Νοέμβριο του 2011. Οι άνθρωποι της Symantec ήρθαν σε επαφή με 6.275 επιχειρήσεις συνολικά, με τον αριθμό των εργαζομένων να κυμαίνεται από 5-πάνω από 5.000. Στις μικρές επιχειρήσεις, οι ερωτηθέντες της έρευνας ήταν οι υπεύθυνοι των Η/Υ, ενώ στις μεγάλες επιχειρήσεις ήταν οι επικεφαλής των τμημάτων τεχνολογίας. Η δημοσκόπηση έχει αξιοπιστία 95% εμπιστοσύνης με +- 1,3% περιθώριο λάθους.

Εύρημα Νο1: Σημείο καμπής στην υιοθέτηση της κινητής τηλεφωνίας. Οι καιροί αλλάζουν για τις επιχειρήσεις, και αυτό φαίνεται ξεκάθαρα από τις κινητές συσκευές. Αυτές οι συσκευές έχουν γίνει βασικά εργαλεία για να κάνει κανείς τη δουλειά του. Οι υπάλληλοι βλέπουν σημαντικά βελτιωμένη παραγωγικότητα όντας σε θέση να έχουν πρόσβαση σε δουλειές της επιχείρησης από οπουδήποτε με τη βοήθεια του κινητού τους τηλεφώνου. Οι οργανισμοί τώρα εφαρμόζουν μία κοινή γραμμή όσων αφορά στις εφαρμογές που είναι προσβάσιμες από κινητές συσκευές- 59% των ερωτηθέντων ανέφεραν ότι αυτό είναι υπόθεση. Στην πραγματικότητα, τώρα που οι κινητές συσκευές αποτελούν εργαλεία όλων, σχεδόν τα 3/4 (71% των επιχειρήσεων) φτάνουν τώρα να εφαρμόσουν ένα εταιρικό "κατάστημα" με κινητές εφαρμογών.

Για να κατανοηθεί καλύτερα γιατί οι οργανισμοί υιοθετούν τη νέα μέθοδο εργασίας μέσω των κινητών συσκευών, ρωτήθηκαν για τα πιο σημαντικά επιχειρησιακά οφέλη που προέρχονται από τα κινητά. Ανέφεραν την αυξημένη αποδοτικότητα, την αυξημένη αποτελεσματικότητα στο χώρο εργασίας και τον μειωμένο χρόνο που απαιτείται για να ολοκληρώσουν τα καθήκοντα τους. Βάζοντάς τα όλα μαζί, όλα αυτά ωφελούν την ευκινησία των επιχειρήσεων τους. Σε πολλούς τομείς της τεχνολογίας, οι προσδοκίες να εφαρμοστεί μια καινοτομία δεν ταιριάζει πάντα με τα αποτελέσματα. Στην περίπτωση των κινητών συσκευών παρ' όλα αυτά, οι προσδοκίες ταίριαξαν περισσότερο με την πραγματικότητα. Για παράδειγμα, περίπου τα 3/4 των επιχειρήσεων προσδοκούσαν να αυξήσουν την αποτελεσματικότητα μέσω της χρήσης των κινητών συσκευών και τελικά και τα 3/4 έπεσαν μέσα στις προσδοκίες τους με αποδείξεις. Αυτά τα αποτελέσματα βγήκανε σε μεγάλο βαθμό αληθινά για τις μικρές και τις μεγάλες επιχειρήσεις, με κύριο στόχο την αποτελεσματικότητα.

Οι μεγάλες επιχειρήσεις ήταν ελαφρώς πιο αισιόδοξες, ενώ οι μικρές είχαν πιο μικρές προσδοκίες. Η κύρια διαφορά ήταν ότι οι μικρότερες επιχειρήσεις ήταν λιγότερο πιθανό να έχουν σχέδια που αφορούν σε εφαρμογές πελατών, ή εταιρικά καταστήματα εφαρμογών σε σχέση με τις μεγάλες επιχειρήσεις.

Η βόρεια Αμερική υστερεί σε σχέση με την επικρατούσα επιχειρηματική τάση στη Λατινική Αμερική, η οποία είναι μπροστά σε τομείς της κοινής εταιρικής γραμμής -εφαρμογές (67% σε σύγκριση με 53% για τη Βόρεια Αμερική) και του σχεδιασμού εταιρικών καταστημάτων εφαρμογών (70% σε σύγκριση με 52%).

Εύρημα 2: Πρωτοβουλίες για κινητές συσκευές που έχουν αντίκτυπο στις πηγές της τεχνολογίας. Σχεδόν οι μισοί οργανισμοί που συμμετείχαν στην έρευνα (48%) θεωρούσαν το κινητό ως κάτι υπερβολικά πρακτικό και η χρήση του είναι απαραίτητη. Στην πραγματικότητα, το 31% των ανθρώπων που εμπλέκονται με την εξέλιξη της τεχνολογίας της πληροφορίας (IT), ασχολούνται και με την εξέλιξη των κινητών συσκευών. Οι κύριες προτεραιότητες αυτού του ποσοστού των ανθρώπων είναι η ασφάλεια, το backup και η αντιμετώπιση προβλημάτων σε χαμένες ή κλεμμένες συσκευές.

Η χρήση του κινητού ταξινομήθηκε καθώς αυτό αποτελεί το μεγάλο ρίσκο της τεχνολογίας της πληροφορίας, ειδικά όταν μιλάμε για οργανισμούς (οι οποίοι αποτελούν έναν από τους τρεις κυριότερους τομείς στους οποίους η χρήση κινητού εμπεριέχει ρίσκο σύμφωνα με το 41% των ερωτηθέντων). Η IT έχει πολλές έννοιες, μεταξύ των οποίων είναι η απώλεια συσκευών, η διαρροή δεδομένων, η μη εξουσιοδοτημένη πρόσβασης σε εταιρικές πηγές καθώς και η μόλυνση από κακόβουλο λογισμικό.

Ένας στους 4 ερωτηθέντες αναγνώρισαν ότι οι μεγαλύτεροι κίνδυνοι που αναπτύχθηκαν είναι τα μηνύματα spam, το phishing, και τα κακόβουλα λογισμικά. Για αυτούς τους αισθητούς κινδύνους οι περισσότεροι οργανισμοί έχουν κατά νου μια σειρά από μέτρα ασφαλείας, από λογισμικά antivirus μέχρι και απομακρυσμένη “ακύρωση” συσκευών. Όσων αφορά στην εφαρμογή αυτών των μέτρων, παρ' όλα αυτά, λιγότεροι από τους μισούς οργανισμούς έκαναν αυτά τα βήματα.

Εύρημα 3: Κίνδυνοι για κινητά που επηρεάζουν τους οργανισμούς. Μικρές και μεγάλες επιχειρήσεις βλέπουν βλάβες/ζημιές που σχετίζονται με τη χρήση κινητών συσκευών, να συσσωρεύονται λόγω έλλειψης ασφάλειας. Έχουν υποστεί μια ποικιλία απωλειών, που μετριέται με άμεσα οικονομικά έξοδα, απώλεια δεδομένων και ζημιά στη φήμη ή απώλεια εμπιστοσύνης του πελάτη. Το 2011, το μέσο κόστος αυτών των απωλειών, ήταν ένα εκπληκτικό ποσό της τάξεως των 247.000 δολαρίων συνολικά. Μεγάλες και μικρές επιχειρήσεις υφίστανται περίπου τα ίδια είδη ζημιών όμως σε πολύ διαφορετικό βαθμό – Οι μικρές επιχειρήσεις είχαν ζημιές κατά μέσο όρο 126.000 δολάρια, ενώ οι μεγάλες επιχειρήσεις 429.000 δολάρια. Οι απώλειες ποίκιλαν επίσης ανάλογα με την περιοχή και το μέγεθος της επιχείρησης. Ενδεικτικά κυμαίνονταν από 199.000 δολάρια για μικρές

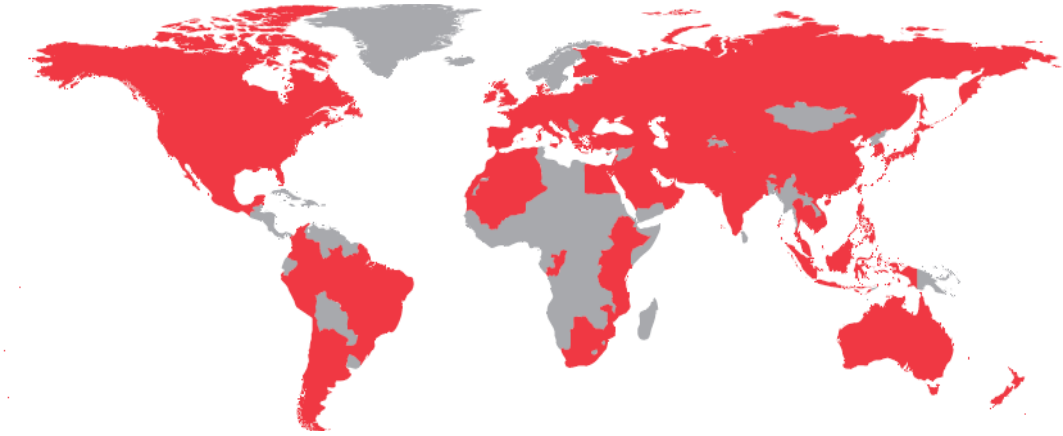
επιχειρήσεις στην Ασία μέχρι και μεγάλες επιχειρήσεις της Λατινικής Αμερικής όπου φτάναμε τα 385.000 δολάρια.

5.4 Διαγράμματα και συμβουλές της VERIZON

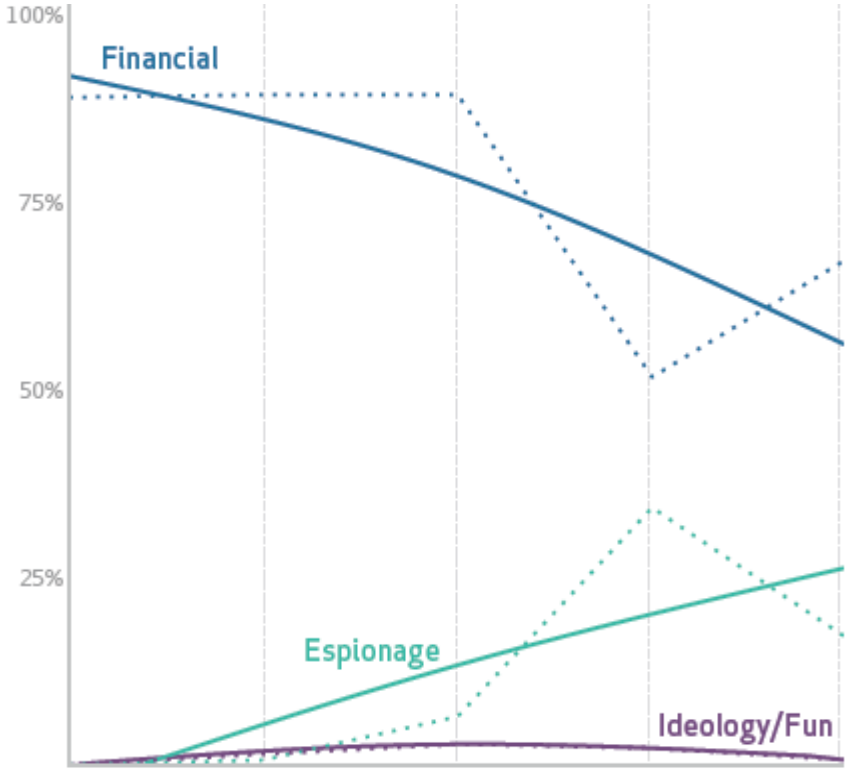
Σε συνέχεια της μελέτης της σχέσης των εταιριών – οργανισμών και των κινητών συσκευών, παρατίθεται η αναφορά της εταιρείας τηλεπικοινωνιών Verizon, η οποία εδρεύει στις Η.Π.Α., για τα ρήγματα και τα περιστατικά που έλαβαν χώρα σε παγκόσμιο επίπεδο σε οργανισμούς και επιχειρήσεις κατά το 2013 [Β.3.Η.3].

Τι θεωρείται όμως ρήγμα και τι περιστατικό;
Βάση της μελέτης της Verizon ισχύουν οι παρακάτω ορισμοί.
Περιστατικό: Ένα γεγονός που θέτει σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα πληροφοριών που σχετίζονται με τα οικονομικά στοιχεία ενός οργανισμού.
Ρήγμα: Ένα περιστατικό που έχει ως αποτέλεσμα την αποκάλυψη ή πιθανή έκθεση δεδομένων του οργανισμού σε ένα μη εξουσιοδοτημένο κοινό.
Παρακάτω με τη βοήθεια διαγραμμάτων – εικόνων φανερώνονται τα ανωτέρω στοιχεία ενώ παρατίθενται και ανάλογες συμβουλές.

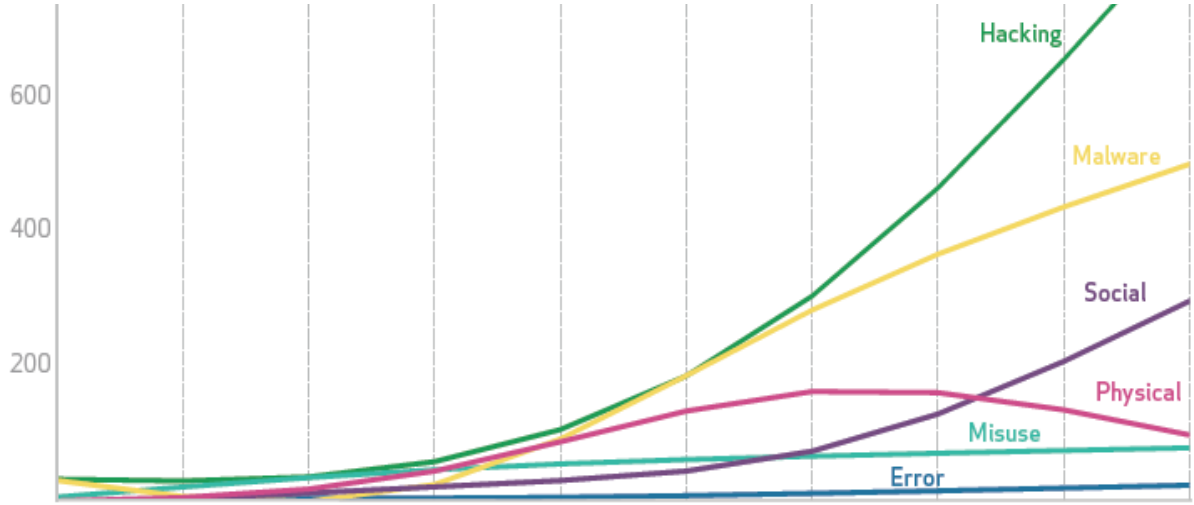
Εικόνα 5.1 : Χώρες όπου εδρεύουν οργανισμοί στους οποίους παρουσιάστηκαν ρήγματα δεδομένων κατά το 2013 (κατά αλφαβητική σειρά).
*Αφγανιστάν, Αλβανία, Αλγερία, Αργεντινή, Αρμενία, Αυστραλία, Αυστρία, Αζερμπαϊτζάν, Αίγυπτος, Αιθιοπία, Βέλγιο, Βοσνία- Ερζεγοβίνη, Βραζιλία, Βουλγαρία, Βιετνάμ, Γαλλία, Γεωργία, Γερμανία, Δανία, Ελλάδα, Ελβετία, Ηνωμένα Αραβικά Εμιράτα, Ηνωμένο Βασίλειο, Ινδία, Ινδονησία, Ιράν, Ιράκ, Ιρλανδία, Ισραήλ, Ισπανία, Ιταλία, Ιαπωνία, Ιορδανία, Καζακστάν, Καμπότζη, Καναδάς, Κατάρ, Κένυα, Κίνα, Κολομβία, Κονγκό, Κορέα, Κουβέϊτ, Κροατία, Κύπρος, Κιργιστάν, Λευκορωσία, Λιθουανία, Λίβανος, Λουξεμβούργο, Μαλαισία, Μπαλί, Μαυριτανία, Μεξικό, Μολδαβία, Μαυροβούνιο, Μαρόκο, Μοζαμβίκη, Μπαχρέϊν, Μποτσουάνα, Μπρουνέϊ, Νεπάλ, Ν. Αφρική, Ν. Ζηλανδία, Ολλανδία, Ομάν, Πακιστάν, Παλαιστίνη, Παρθένοι Νήσοι, Περού, Πολωνία, Πορτογαλία, Σκόπια, Ρουμανία, Ρωσία, Σ. Αραβία, Σιγκαπούρη, Σλοβακία, Σλοβενία, Ταϊβάν, Τανζανία, Ταϋλάνδη, Τουρκία, Τουρκμενιστάν, Τσεχία, Ουγγαρία, Ουγκάντα, Ουκρανία, Ουζμπεκιστάν, Φιλανδία, Φιλιππίνες, Χιλή, Χονγκ Κονγκ.



Εικόνα 5.2: Ποσοστά ρηγμάτων ανά κίνητρο δραστών (οικονομικό όφελος, κατασκοπεία, ιδεολογία)

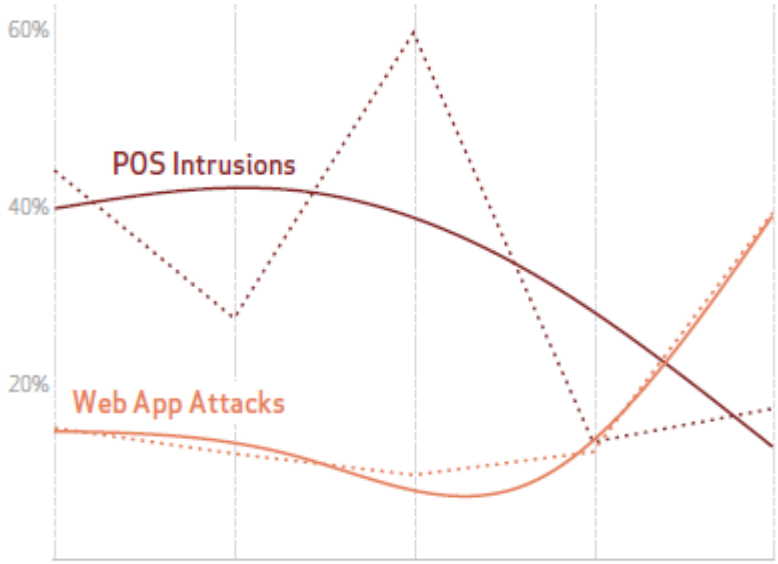


Εικόνα 5.3: Αριθμός ρηγμάτων ανά κατηγορία απειλής (Hacking, Κακόβουλο λογισμικό, κοινωνικά κίνητρα, φυσικοί λόγοι, κακή χρήση δεδομένων, λάθη)

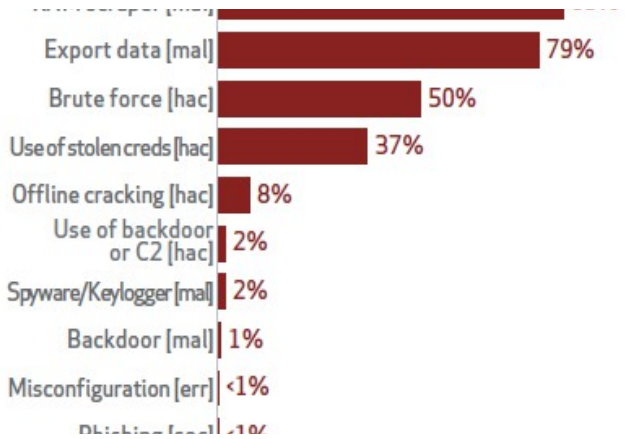


Εισβολές σε μηχανές ταμειακού ελέγχου και επιθέσεις σε δικτυακές εφαρμογές

Εικόνα 5.4: Σύγκριση εισβολών σε λειτουργικά συστήματα και μοτίβο επιθέσεων σε δικτυακές εφαρμογές, κατά τα τελευταία έτη.



Εικόνα 5.5: 10 κορυφαίες απειλές των λειτουργικών συστημάτων (1. RAM Scraper, κακόβουλο λογισμικό-85%, 2. Εξαγωγή δεδομένων, κακόβουλο λογισμικό-79%, 3. Ωμή δύναμη, hacking -50%, 4. Χρήση κλεμμένων διαπιστευτηρίων, hacking-37%, 5. Offline cracking, hacking-8%, 6. Χρήση πίσω πόρτας ή C2, hacking-2%, 7. Spyware/Keylogger, κακόβουλο λογισμικό-2%, 8. πίσω πόρτα, κακόβουλο λογισμικό-1%, 9. κακή εγκατάσταση, Λάθος-<1%, 10. ψάρεμα soc (τσιπάκι)-<1%)



Προτεινόμενες συμβουλές - έλεγχοι για τις ανωτέρω εισβολές προς εταίρους εταιρειών:

- Περιορίστε την απομακρυσμένη πρόσβαση.
  Περιορίστε κάθε απομακρυσμένη πρόσβαση των αντιπροσώπων της εταιρίας στις μηχανές ταμειακού ελέγχου και κάνετε σοβαρές επιχειρηματικές συζητήσεις σχετικά με το πώς και το πότε θα εκτελέσουν τα καθήκοντά τους.
- Δυναμώστε τις πολιτικές κωδικών.
  Σιγουρέψτε απόλυτα ότι όλοι οι κωδικοί που χρησιμοποιούνται για απομακρυσμένη πρόσβαση στις μηχανές ταμειακού ελέγχου δεν είναι εργοστασιακές προεπιλογές, το όνομα του αντιπροσώπου σας, λέξεις λεξικού, ή αλλιώς αδύναμες.
- 'S' is for 'Sale', not 'Social'.
  Μη σερφάρετε στο διαδίκτυο και στο email, μη χρησιμοποιείτε κοινωνικά μέσα δικτύωσης, μην παίζετε παιχνίδια ή κάνετε οποιαδήποτε άλλη δραστηριότητα ειδικά με τα μηχανήματα που συνδέονται με τον ταμειακό έλεγχο.
- Αναπτύξτε AV.
  Εγκαταστήστε και διατηρήστε λογισμικό antivirus στο λειτουργικό σύστημα. Σε τελική ανάλυση: Δυσκολέψτε τους επιτήδειους να συνδεθούν σε μια συσκευή η οποία έχει την πιο στοχευμένη πληροφορία για τους οικονομικά παρακινούμενους εγκληματίες.

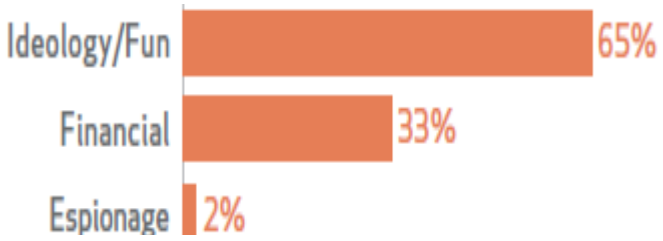
Για μεγάλες εταιρείες:

- Αφήστε τη θεωρία του επίπεδου δικτύου.
  Ελέγξτε τη συνδεσιμότητα ανάμεσα στα καταστήματα και τις κεντρικές τοποθεσίες και διαχωρίστε το περιβάλλον του λειτουργικού σας συστήματος από το εταιρικό δίκτυο.
- Ψάξτε για ύποπτη δικτυακή δραστηριότητα.
  Καταγράψτε τη δικτυακή κίνηση προς και από το δίκτυο του λειτουργικού συστήματος.
- Χρησιμοποιείστε πιστοποίηση δυο παραγόντων.
  Ισχυροί κωδικοί θα απέκοβαν ένα τεράστιο μέρος των επιθέσεων, όμως οι μεγαλύτεροι

οργανισμοί θα πρέπει επίσης να λάβουν υπ' όψιν τους, τους πολλαπλούς παράγοντες για να πιστοποιήσουν τους τρίτους χρήστες και τους εσωτερικούς χρήστες.

Επιθέσεις σε εφαρμογές των εταιριών

Εικόνα 5.6: Κίνητρα δράσης σε Επιθέσεις Δικτυακών Εφαρμογών (Ιδεολογία/Διασκέδαση-65%, Οικονομικά-33%, Κατασκοπία-2%)



Προτεινόμενοι έλεγχοι - συμβουλές

- Αποτυχία μονού κωδικού.
  Για οποιαδήποτε ενέργεια στο διαδίκτυο κάντε επιβεβαίωση που βασίζεται σε κωδικό Παρόλο που ίσως αυτή να απομακρύνει από μια γνωστή ζώνη ασφαλείας, αν θέλετε να υπερασπιστείτε μια δικτυακή εφαρμογή, αναζητήστε εναλλακτικές με αυτή τη μέθοδο επιβεβαίωσης ταυτότητας. Αν είστε πωλητής στο space της δικτυακής εφαρμογής, δοκιμάστε επίσης έναν εναλλακτικό μηχανισμό πιστοποίησης για τους πελάτες σας.
- Ξανασκεφτείτε το CMS (Content Management System).
  Αν είστε αφοσιωμένος σε μια ενεργή πλατφόρμα Joomla, Drupal, Wordpress, κτλ., τότε εφαρμόστε μια αυτόματη διαδικασία τροποποίησης. Αν δεν είναι εφικτό αυτό, τότε αναπτύξτε μια χειροκίνητη διαδικασία και μείνετε σε αυτήν. Αυτό θα πρέπει να ισχύει ιδιαίτερα για τους τρίτους (π.χ. αντιπροσώπους της εταιρίας σας). Ένας άλλος τρόπος για να σιγουρέψετε το σύστημα διαχείρισης περιεχομένου CMS, είναι να λάβετε υπόψη ένα στατικό πλαίσιο CMS. Αντί να δίνεται κωδικό για κάθε αίτημα, το στατικό CMS θα προ-παράγει εκείνες τις δειγματικές σελίδες, απομακρύνοντας την ανάγκη να δίνεται κωδικό στον server για κάθε αίτημα.
- Καταγράψτε εξερχόμενες συνδέσεις.
  Ενώ πολλές από τις επιθέσεις βασίζονται στο bypass πρωτόκολλο του υπάρχοντος τείχους προστασίας (HTTP), άλλες αλλάζουν στον διαδικτυακό server το ρόλο της εταιρίας – θύμα, σε πελάτη. Απροφύλακτα σημεία ωθούν κακόβουλο λογισμικό να συνεχίσει την επίθεση φιλτράροντας εκτεθειμένα δεδομένα ή με το να επιτίθεται σε άλλους κατόπιν εντολής. Για το λόγο, προσπαθήστε να κλειδώσετε την ικανότητα του δικτυακού σας server να το κάνει.
- Επικυρώστε καταχωρήσεις.
  Ο καλύτερος τρόπος για να είστε σίγουροι ότι δε θα εκμεταλλευτούν τη δικτυακή σας

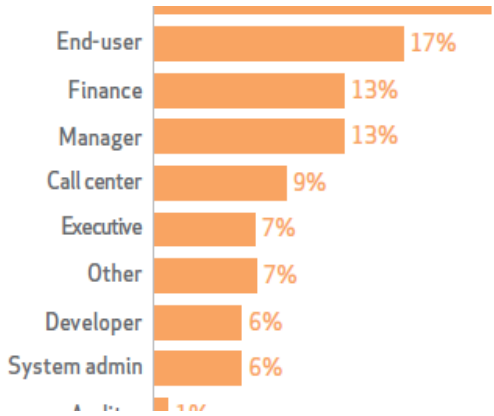
εφαρμογή είναι να αναζητήσετε και να διορθώσετε τις αδυναμίες πριν το κάνουν οι επιτήδειοι. Αν δεν έχετε πρόσβαση στον πηγαίο κωδικό και/ή στους κατασκευαστές λογισμικού, σιγουρέψτε ότι έχετε κάτι (π.χ. ένα συμβόλαιο) για να διορθώσει τα προβλήματα όταν βρεθούν.

- Επιβάλλετε πολιτικές κλειδώματος.

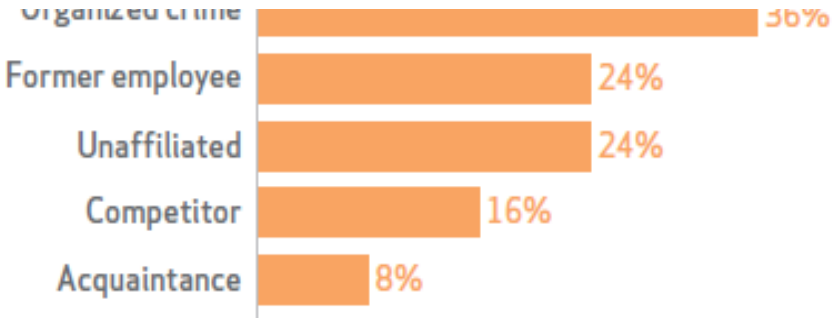
  Η επίθεση ωμής δύναμης δεν είναι η κυρίαρχη μέθοδος σε αυτό το κομμάτι, όμως εξακολουθεί να είναι άξια μνείας. Θεσπίζοντας αντίμετρα, επιβραδύνοντας το ρυθμό των επαναλαμβανόμενων προσπαθειών ή κλειδώνοντας προσωρινά λογαριασμούς με πολλαπλές αποτυχημένες απόπειρες, ο επιτιθέμενος των αποτυχημένων αποπειρών ωμής δύναμης το πιο πιθανό είναι να διαλυθεί και να εξαφανιστεί.

Κακή διαχείριση εσωτερικών παραγόντων και προνομίων

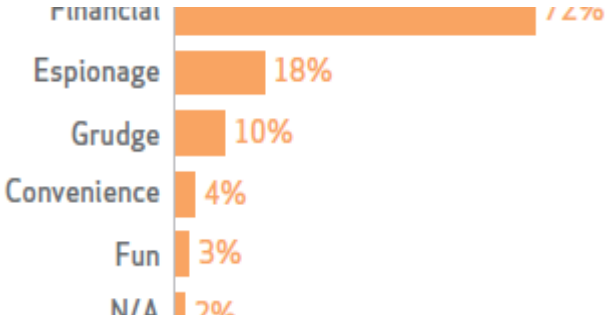
Εικόνα 5.7: οι 10 κορυφαίοι εσωτερικοί δράστες λόγω κακής εσωτερικής χρήσης (ταμείο-23%, τελικός χρήστης-17%, λογιστήριο-13%, διεύθυνση-13%, τηλεφωνικό κέντρο-9%, διοικητικό τμήμα-7%, λοιποί-7%, τμήμα λογισμικού-6%, διαχειριστής συστήματος-6%, ελεγκτής-1%)



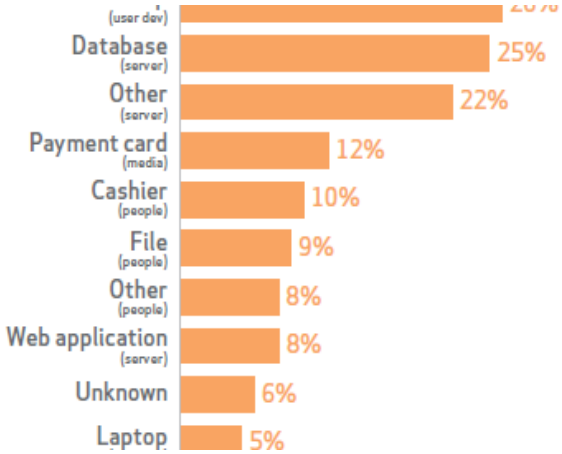
Εικόνα 5.8: Εξωτερικοί δράστες λόγω κακής εσωτερικής χρήσης (οργανωμένο έγκλημα-36%, πρώην υπάλληλος-24%, άγνωστοι-24%, ανταγωνιστής -16%, γνωστοί-8%)



Εικόνα 5.9: κίνητρα εσωτερικής κακής χρήσης (οικονομικά-72%, κατασκοπία-18%, μνησικακία-10%, ευκολία-4%, διασκέδαση-3%, N/A-2%)



Εικόνα 5.10: 10 κορυφαία περιουσιακά στοιχεία εντός των οργανισμών που υπόκειται κακή χρήση (desktop, χρήστης-26%, βάση δεδομένων-25%, server-25%, λοιπά, server-22%, κάρτα πληρωμών, μέσα ενημέρωσης-12%, ταμίας, άνθρωποι-10%, file, άνθρωποι-9%, άλλοι, άνθρωποι-8%, δικτυακή εφαρμογή server-8%, άγνωστο-6%, laptop, χρήστης-5%)



Προτεινόμενοι Έλεγχοι – Συμβουλές:

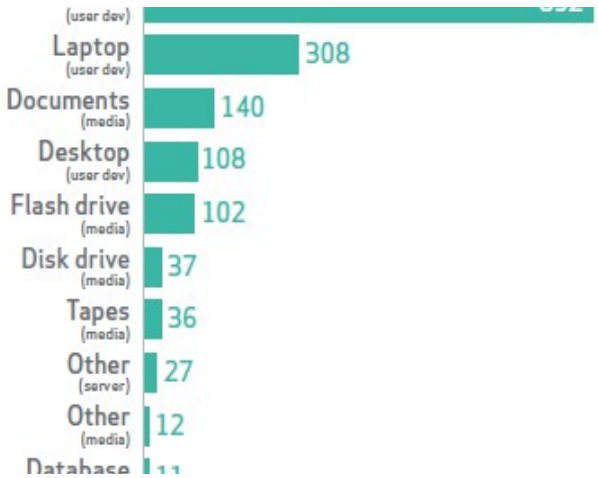
- Να γνωρίζετε τα δεδομένα σας και ποιος έχει πρόσβαση σε αυτά.
  Το πρώτο βήμα για να προστατεύσετε τα δεδομένα σας είναι να γνωρίζετε πού βρίσκονται

και ποιος έχει πρόσβαση σε αυτά. Κάντε ελέγχους για να τα προστατεύετε και να εντοπίσετε κακή χρήση. Δε θα αποτρέψει αποφασισμένους εσωτερικούς επιτήδειους να δράσουν (διότι έχουν ήδη πρόσβαση σε αυτά), όμως υπάρχουν πολλά άλλα οφέλη που δικαιολογούν το να το κάνετε.

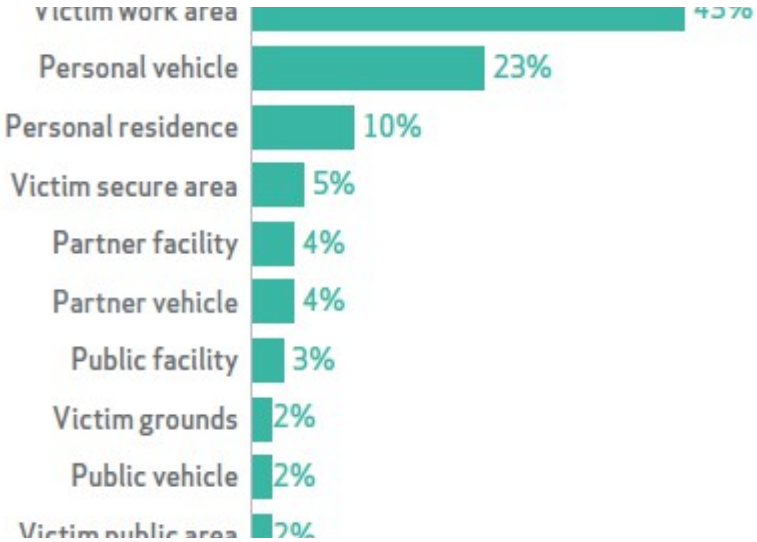
- Ελέγχετε τους λογαριασμούς χρηστών.
  Έχοντας αναγνωρίσει τις θέσεις της εταιρίας από τις οποίες έχει κανείς πρόσβαση σε ευαίσθητα δεδομένα, ελέγξτε τη δραστηριότητα λογαριασμών όταν εκείνοι οι υπάλληλοι οι οποίοι κατέχουν εκείνες τις θέσεις παραιτούνται ή αποδεσμεύονται. Αχρηστεύετε λογαριασμούς χρηστών αμέσως μόλις ένας υπάλληλος φεύγει από την εταιρεία.
- Παρακολουθείτε για διαφυγή πληροφοριών.
  Στις ακραίες περιπτώσεις κακής χρήσης, βλέπουμε δράσεις που διευκολύνουν τη μεταφορά δεδομένων εκτός οργανισμού.
- Δημοσιεύετε αποτελέσματα ελέγχων.
  Από πλευράς επίγνωσης, δημοσιεύετε τακτικά ανώνυμα αποτελέσματα ελέγχων πρόσβασης. Γνωστοποιείτε στους υπαλλήλους ότι υπάρχουν συνέπειες και ότι οι πολιτικές επιβάλλονται. Αυτό μπορεί να λειτουργήσει ως ισχυρό αποτρεπτικό μέσο στην κακή συμπεριφορά.

<u>Φυσική Κλοπή και Απώλεια</u>

Εικόνα 5.11: 10 Κορυφαίοι στόχοι κλοπής/απώλειας (λοιπά, συσκευή χρήστη-892, laptop, συσκευή χρήστη-308, έγγραφα, media-140, desktop, συσκευή χρήστη-108, flash drive, media-102, disk drive, media-37, κασέτες, media-36, λοιπά, server-27, λοιπά, media-12, βάση δεδομένων, server-11)



Εικόνα 5.12: 10 Κορυφαίες τοποθεσίες για κλοπή (περιοχή εργασίας θύματος-43%, προσωπικό όχημα-23%, προσωπική κατοικία-10%, ασφαλής περιοχή θύματος-5%, εταιρικές εγκαταστάσεις-4%, εταιρικό όχημα-4%, δημόσιες εγκαταστάσεις-3%, χώροι θύματος-2%, δημόσιο όχημα-2%, δημόσια περιοχή θύματος-2%)



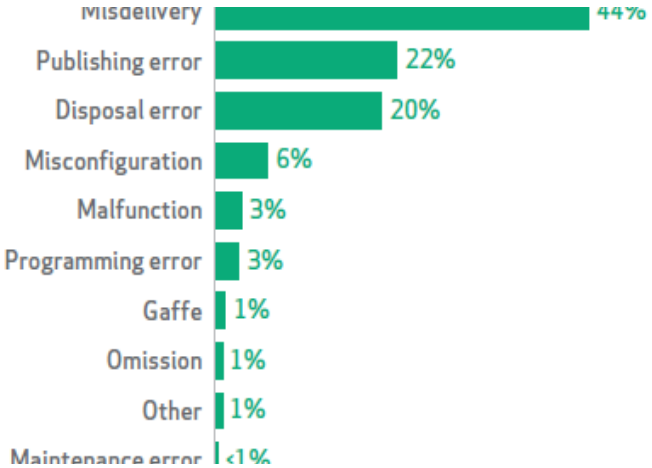
Προτεινόμενοι έλεγχοι – Συμβουλές:

- Κρυπτογραφείστε συσκευές.
  Λαμβάνοντας υπόψη την υψηλή συχνότητα χαμένων περιουσιακών στοιχείων, η κρυπτογράφηση είναι πραγματικά μια λύση. Σίγουρα, τα περιουσιακά στοιχεία εξακολουθούν να λείπουν, όμως τουλάχιστον γλιτώνετε από πολλές στενοχώριες, ντροπή, και πιθανές μηνύσεις.
- Κρατείστε τα μαζί σας.
  Ενθαρρύνετε τους υπαλλήλους να κρατούν τις ευαίσθητες συσκευές στην κατοχή τους και στο οπτικό τους πεδίο κάθε στιγμή.
- Back it up
  Συχνά (και κατά προτίμηση αυτόματα) backups εξυπηρετούν έναν διπλό σκοπό. Διασώζουν αξία μη ανακτήσιμης εργασίας εβδομάδων/μηνών/χρόνων και σας καθιστούν ξανά παραγωγικό σε μια νέα συσκευή σε ελάχιστο χρόνο.
- Κλειδώστε.
  Η πλειοψηφία των κλοπών ήταν έγγραφα παρμένα από το ερμάριο και από κινητές συσκευές (συμπεριλαμβανομένων και των laptops). Μια πιο αποτελεσματική στρατηγική θα ήταν να μεταφέρετε πολύ ευαίσθητα ή πολύτιμα περιουσιακά στοιχεία σε μια ξεχωριστή, ασφαλή περιοχή και να φροντίσετε να παραμείνουν εκεί.
- Χρησιμοποιείτε απωθητική τεχνολογία.
  Ναι, είναι ανορθόδοξο όσων αφορά τις συστάσεις, αλλά ίσως είναι τελικά ένα αποτελεσματικό

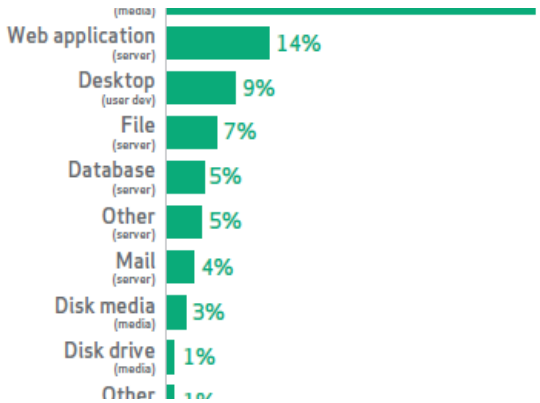
αποτρεπτικό μέσο για τις κλοπές.

Ετερόκλητα λάθη

Εικόνα 5.13: 10 Κορυφαίοι παράγοντες απειλών από ετερόκλητα λάθη (λάθος παράδοση-44%, εκδοτικό λάθος-22%, λάθος διάθεσης-20%, κακή εγκατάσταση-6%, κακή λειτουργία-3%, λάθος προγραμματισμού-3%, γκάφα-1%, παράλειψη-1%, άλλο-1%, λάθος συντήρησης-<1%)



Εικόνα 5.14: 10 κορυφαία περιουσιακά στοιχεία που επηρεάστηκαν από ετερόκλητα λάθη (έγγραφα, media-49%, δικτυακές εφαρμογές, server-14%, desktop, συσκευή χρήστη-9%, αρχείο, server-7%, βάση δεδομένων, server-5%, άλλο, server-5%, αλληλογραφία, server-4%, disk media, media-3%, disk drive, media-1%, άλλο, media-1%)



Προτεινόμενοι έλεγχοι - Συμβουλές

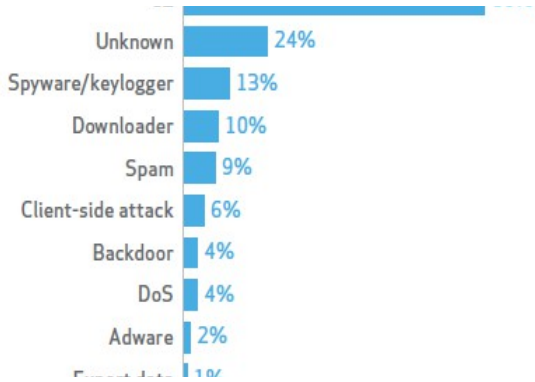
- Κρατήστε το DLP
  Λάβετε υπόψη την εφαρμογή του λογισμικού DLP (πρόληψη απώλειας δεδομένων) για να

μειώσετε τις περιπτώσεις να στέλνονται ευαίσθητα έγγραφα με email. Το DLP μπορεί να αναγνωρίσει πληροφορίες που συμβαδίζουν με μια κοινή μορφή, όπως αριθμοί πιστωτικών καρτών, αριθμοί κοινωνικής ασφάλειας, ή κωδικοί ιατρικών λογαριασμών.

- Ελέγξτε τις αναρτήσεις σας
  Ορίστε και έναν δεύτερο κριτή που να ελέγχει οτιδήποτε αναρτάται στους servers της εταιρείας και να σκανάρει τακτικά τις δημόσιες ιστοσελίδες για το αν έχουν αναρτήσει δεδομένα μη δημόσια και απαγορεύστε δια ροπάλου και αν αποθηκεύονται μη επιμελημένα έγγραφα σε έναν αρχειακό server ο οποίος συνδέεται με έναν διαδικτυακό server.
- Επιβεβαιώστε το σωστό προορισμό
  Όταν στέλνετε μεγάλους ταχυδρομικούς φακέλους, ελέγξτε ένα δείγμα για να σιγουρέψετε ότι οι πληροφορίες στο έγγραφο ταιριάζουν στο όνομα του φάκελου.
- Η τεχνολογία της πληροφορίας δεν παράγει σκουπίδια.
  Κάθε άχρηστη πληροφορία ή πώληση πληροφορίας θα πρέπει να συγχρονίζεται από το τμήμα IT. Εκπαιδεύστε τους χρήστες να σκέφτονται το πέταμα ενός υπολογιστή με τον ίδιο τρόπο που σκέφτονται το πέταμα επικίνδυνων υλικών. ‘Δεν μπορείς να το πετάξεις απλά στα σκουπίδια. Στείλε το στο τμήμα IT για κατάλληλο χειρισμό.’ Ελέγξτε τη διαδικασία απόρριψης παίρνοντας συσκευές ως δείγματα για να επιβεβαιώσετε ότι έχουν καθαριστεί σωστά.

Crimeware

Εικόνα 5.15: 10 κορυφαίες δράσεις Crimeware (C2-86%, άγνωστο-24%, spyware/Keylogger-13%, downloader-10%, spam-9%, client-side attack-6%, backdoor-4%, doS-4%, adware-2%, export data-1%)



Προτεινόμενοι έλεγχοι – Συμβουλές

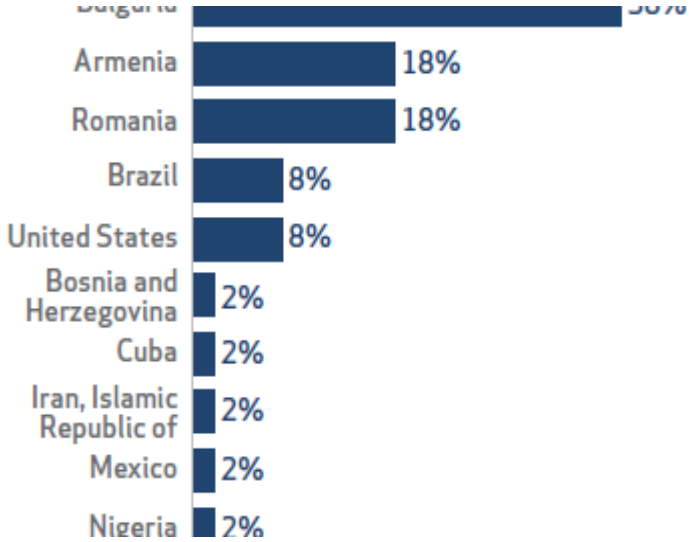
- Διατηρείτε τα προγράμματα περιήγησης ενημερωμένα.
  Το να διατηρείτε ασφαλή τα προγράμματα περιήγησης και να προσθέτετε λειτουργίες

που κρίνονται απαραίτητες θα βοηθήσει να μειώσετε τα περιστατικά crimeware.

- Απενεργοποιήστε την Java στο πρόγραμμα περιήγησης.
- Χρησιμοποιείστε επιβεβαίωση δύο παραγόντων.
  Το crimeware συνδέεται με κλεμμένα διαπιστευτήρια πιο συχνά από οποιοδήποτε άλλο είδος δεδομένων. Αυτό δείχνει το ρόλο κλειδί του crimeware όταν ο σκοπός της επίθεσης είναι η απόκτηση πρόσβασης σε λογαριασμούς του χρήστη. Η διπλή επιβεβαίωση δε θα αποτρέψει την κλοπή διαπιστευτηρίων, όμως θα βοηθήσει στο να αποτραπεί η δόλια επαναχρησιμοποίηση εκείνων των διαπιστευτηρίων.
- Η αλλαγή χρειάζεται.
  Πολλές από τις μεθόδους που χρησιμοποιούνται από το crimeware μπορούν να ανιχνευτούν εύκολα παρακολουθώντας δείκτες-κλειδιά των συστημάτων. Αυτό σημαίνει ότι πρέπει να βελτιώσουμε την ανίχνευση και όχι να επικεντρωνόμαστε απλά στην πρόληψη.

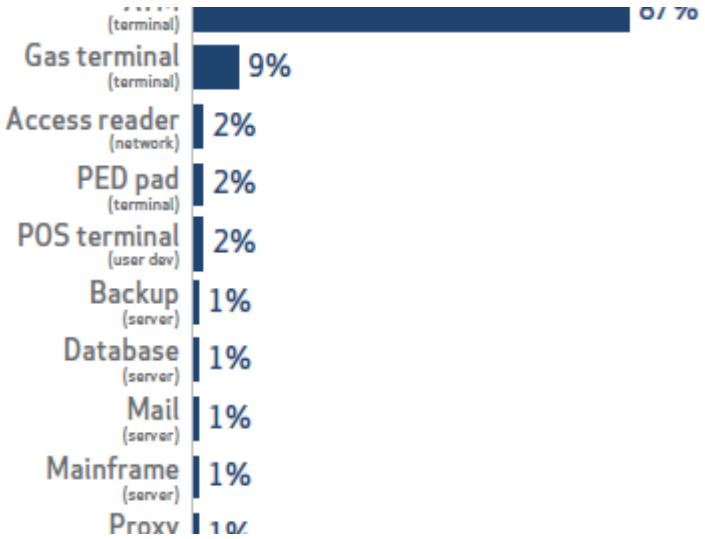
Υποδοχή μηχανημάτων πληρωμής με κάρτα

Εικόνα 5.16: Καταγωγή εξωτερικών δραστών που δρουν με Skimmers (Βουλγαρία-38%, Αρμενία-18%, Ρουμανία-18%, Βραζιλία-8%, Ηνωμένες Πολιτείες-8%, Βοσνία-Ερζεγοβίνη-2%, Κούβα-2%, Ιράν, Ισλαμική Δημοκρατία-2%, Μεξικό-2%, Νιγηρία-2%)



Εικόνα 5.17: Στοιχεία που βασίζονται σε card skimmers (ATM, τερματικό-87%, τερματικό βενζίνης, τερματικό-9%, αναγνώστης πρόσβασης, δίκτυο-2%, PED pad, τερματικό-2%,

τερματικά POS, συσκευή χρήστη-2%, backup, server-1%, βάση δεδομένων, server-1%, ταχυδρομείο, server-1%, mainframe, server-1%, Proxy, server-1%)



Προτεινόμενοι έλεγχοι – Συμβουλές για επιχειρήσεις - οργανισμούς:

- Σχεδιάστε (ή αγοράστε) τερματικά ανθεκτικά στις αλλοιώσεις.
  Ως έμπορος, αυτό πιθανόν δεν είναι κάτι που μπορείτε να κάνετε μόνοι σας, όμως έχετε κατά νου ότι ορισμένα σχέδια είναι πιο επιρρεπή σε συσκευές skimming από ότι άλλα. Πολλά σύγχρονα ATM είναι σχεδιασμένα με αυτή τη λογική· επιλέξτε εκείνα αν είναι δυνατό.
- Κάντε ελέγχους παραβιάσεων.
  Κάντε πράγματα τα οποία καθιστούν εμφανή μια αλλοίωση ή εφαρμόστε πιο περίπλοκες τακτικές όπως η καταγραφή οπτικών ανωμαλιών στα ATM.
- Παρακολουθείστε για αλλοιώσεις.
  Ελέγχετε τακτικά τα τερματικά για σημάδια μη εξουσιοδοτημένης αλλοίωσης. Επίσης εκπαιδεύστε τους υπαλλήλους να αναγνωρίζουν ύποπτη συμπεριφορά από άτομα που προσπαθούν να εγκαταστήσουν skimmers.

Για καταναλωτές:

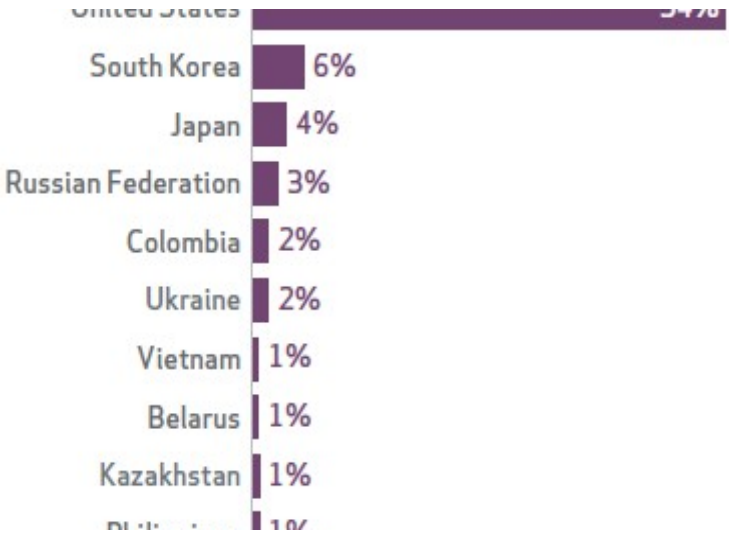
- Προστατεύστε το PIN.
  Όταν εισάγετε το PIN, καλύψτε το χέρι σας για να μπλοκάρετε μικροσκοπικές κάμερες που ίσως σας καταγράφουν.
- Εμπιστευτείτε το ένστικτό σας.
  Αν κάτι φαίνεται εκτός του συνηθισμένου στο ATM ή στην αντλία βενζίνης, κάτι ύποπτο πιθανό να συμβαίνει. Ενώ οι εγκληματίες είναι όλο και πιο ύπουλοι στο να σχεδιάζουν skimmers δύσκολους στην ανίχνευση, ίσως να μπορείτε ακόμη να παρατηρήσετε κάποιο

λάθος, ειδικά αν το τερματικό φαίνεται διαφορετικό από άλλα τριγύρω. Αν ένα από αυτά δεν είναι όπως τα άλλα, μην περνάτε την κάρτα σας!

- Αν δείτε κάτι, πείτε το.
  Αν κάτι σας φαίνεται περίεργο σε ένα τερματικό πληρωμής, φροντίστε να το πείτε στον έμπορο ή την τράπεζα.

Κυβερνο-Κατασκοπία

Εικόνα 5.18: Χώρες θύματα του Cyber-espionage (Ηνωμένες Πολιτείες-54%, Νότια Κορέα-6%, Ιαπωνία-4%, Ρωσική Ομοσπονδία-3%, Κολομβία-2%, Ουκρανία-2%, Βιετνάμ-1%, Λευκορωσία-1%, Καζακστάν-1%, Φιλιππίνες-1%)



Προτεινόμενοι έλεγχοι - Συμβουλές

- Τροποποιείστε όλα τα πράγματα!
  Η εκμετάλλευση των αδυναμιών του προγράμματος περιήγησης, του λειτουργικού συστήματος και άλλου λογισμικού (π.χ. Flash και Java) είναι ένα κοινό αρχικό βήμα για τους επιτιθέμενους προκειμένου να μολύνουν τα συστήματα των τελικών χρηστών. Το να κρατάτε τα πάντα ενημερωμένα θα κάνει αυτό το βήμα πολύ δύσκολο.
- Χρησιμοποιείστε και ενημερώστε το anti-virus (AV).
  Ενώ πολλοί ανακηρύσσουν το AV νεκρό, το να μην το έχετε είναι παρόμοιο με το να ζείτε χωρίς ανοσοποιητικό σύστημα.
- Εκπαιδεύστε τους χρήστες.
  Οπλίστε τους με τη γνώση και τα προσόντα που χρειάζονται για να αναγνωρίσουν και να αναφέρουν πιθανά περιστατικά γρήγορα.
- Μοιράστε το δίκτυό σας.
  Ο καλός καταμερισμός του δικτύου θα κάνει θαύματα για τον περιορισμό ενός

περιστατικού, ειδικά όπου οι δράστες σκοπεύουν να επηρεάσουν την πρόσβαση σε ένα desktop ως εφαλτήριο για ολόκληρο το δίκτυο.

- Κρατείστε καλές «ασφάλειες».
  Κλειδώστε τη δραστηριότητα του συστήματος, του δικτύου και των εφαρμογών. Αυτό δε θα αποτελέσει μόνο μια απαραίτητη βάση για την αντίδραση σε περιστατικά, αλλά πολλά προληπτικά αντίμετρα θα επωφεληθούν επίσης από αυτό.

ΚΕΦΑΛΑΙΟ 6: ΕΠΙΓΝΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

6.1 Εισαγωγή

Η παροχή σε κινητές συσκευές πρόσβασης σε δίκτυο δεν είναι κάτι καινούργιο για τους διαχειριστές της Τεχνολογίας της Πληροφορίας. Πολλά προϊόντα και πολιτικές υπάρχουν προκειμένου να προστατέψουν τα ευαίσθητα δεδομένα και την υποδομή του δικτύου. Παρ' όλα αυτά οι προσπάθειες αυτές δεν είναι πάντοτε επιτυχείς. Σύμφωνα με την αναφορά της Cisco που δημοσιεύτηκε τον Ιούνιο του 2014 με τίτλο «06/2014, «Secure Network Access for Personal Mobile Devices», 7 στους 10 εργαζόμενους παραδέχτηκαν ότι ενσυνείδητα σπάνε σε τακτική βάση τις προκαθορισμένες από την IT πολιτικές προστασίας, ενώ 3 στους 5 δεν θεωρούν αρμοδιότητά τους την ασφάλεια των εταιρικών πληροφοριών και την προστασία των εταιρικών συσκευών. Για αυτό και το 47% των διαχειριστών της Τεχνολογίας της Πληροφορίας κατατάσσουν την αναβάθμιση της ασφάλειας ως κορυφαίο ζήτημα στις αρχές διαμόρφωσης των κινητών συσκευών [Β.2.1]. Το Φεβρουάριο του 2010 πραγματοποιήθηκε μία έρευνα από 4 πανεπιστήμια της Βουδαπέστης με επικεφαλείς τους Iosif Androulidakis και Gorazd Kandus που παρουσιάσθηκε μάλιστα το 2011 στο 6^{ο} Διεθνές Συνέδριο Ψηφιακών Τηλεπικοινωνιών. Το θέμα ήταν η επίγνωση της ασφάλειας που έχουν οι φοιτητές που χειρίζονται κινητά τηλέφωνα τελευταίας τεχνολογίας αλλά και παλαιότερα. Από την ανωτέρω έρευνα προέκυψαν τα παρακάτω στοιχεία. Οι κινητές συσκευές αποτελούν ένα κρίσιμο στοιχείο της ψηφιακής οικονομίας, μια δήλωση κομψότητας και χρήσιμη συσκευή επικοινωνίας και τέλος ένα ζωτικό στοιχείο της καθημερινής ζωής για δισεκατομμύρια ανθρώπους σε όλο τον κόσμο. Οι ενισχυμένες ικανότητες των σύγχρονων κινητών τηλεφώνων τα επιτρέπουν να είναι σχεδόν τόσο ευέλικτα όσο ένας υπολογιστής. Γύρω από αυτά έχει αναπτυχθεί μια μεγάλης αξίας επιχείρηση (λόγω των εφαρμογών που διαθέτουν) με πολλά εργαλεία ψυχαγωγίας (λόγω των παιχνίδιών για κινητά και του m-commerce). Ταυτόχρονα, οι χρήστες αποθηκεύουν και επεξεργάζονται πλέον περισσότερα δεδομένα συμπεριλαμβανομένων και ευαίσθητων πληροφοριών στα τηλέφωνά τους.

Μερικά χρόνια πριν η μόνη έγνοια ενός χρήστη κινητού τηλεφώνου ήταν η ιδιωτικότητα της επικοινωνίας του. Αυτό δεν ισχύει πλέον. Οι χρήστες πρέπει να

προστατεύονται από τη μη εξουσιοδοτημένη πρόσβαση τρίτων στα δεδομένα τους. Εκτός από τα παραδοσιακά μέτρα ασφαλείας όπως τη χρήση PIN (προσωπικός αριθμός αναγνώρισης) και την κρυπτογράφηση φωνής, οι χρήστες πρέπει να παίρνουν επιπλέον μέτρα προστασίας και να ακολουθούν τις νέες πρακτικές. Δυστυχώς, οι χρήστες δεν είναι επαρκώς πληροφορημένοι σχετικά με θέματα ασφαλείας όσων αφορά στις επιλογές των κινητών τους τηλεφώνων και των τεχνικών χαρακτηριστικών αυτών και αποτυγχάνουν να ακολουθήσουν τα σωστά μέτρα και τις ορθές πρακτικές ασφαλείας.

Σύμφωνα τώρα με μία άλλη έρευνα πραγματοποιήθηκε το 2012, στα εργαστήρια του πανεπιστημίου της Καλιφόρνια από τους Erika Chin, Adrienne Porter Felt, Vyas Sekar και David Wagner, ενδεικτικά τα μοντέλα εφαρμογών ασφαλείας στις τέσσερις βασικές ηλεκτρονικές πλατφόρμες έχουν ως εξής:

Windows: Η πλατφόρμα των Windows έχει διαμορφώσει ένα σχετικά εξειδικευμένο οικοσύστημα εφαρμογών, τις οποίες ο χρήστης παίρνει από τρίτους και συχνά από τις ίδιες πηγές π.χ. από online ή φυσικά καταστήματα λιανικής πώλησης. Λόγω του ότι οι εφαρμογές αυτές δεν προέρχονται από το ίδιο το σύστημα αλλά από κάποιον τρίτο, οι χρήστες πρέπει να εγκαθιστούν λογισμικό προστασίας (το οποίο λογισμικό και πάλι το προμηθεύονται από τρίτες πηγές). Αυτό είναι ένα πρόβλημα των **Windows.**

Mac: Αντίθετα, η πλατφόρμα της Mac είθισται γενικά να είναι πιο προστατευμένη στο κακόβουλο λογισμικό, καθώς έχουν υπάρξει λιγότερες καταγεγραμμένες περιπτώσεις επιθέσεων κακόβουλου λογισμικού σε αυτήν. Η Mac έχει επίσης antivirus επιλογές, όμως είναι λιγότερο υιοθετημένες. Παρόμοια με τα Windows, το παραδοσιακό οικοσύστημα εφαρμογών της **Mac** εφοδιάζει εφαρμογές από τρίτες πηγές. Υποκινούμενη από την επιτυχία του καταστήματος των εφαρμογών της για κινητά, η Apple λάνσαρε το κατάστημα εφαρμογών Mac ως μια συγκεντρωμένη αγορά για εφαρμογές desktop. Φαίνεται να είναι αρκετά επιτυχής.

Android: Υπάρχουν αρκετές 'αγορές' για τους χρήστες Android για να κατεβάζουν εφαρμογές, με την αγορά εφαρμογών της Android να είναι η πιο δημοφιλής. Η αγορά Android καλύπτει θέματα ασφαλείας, αν και πρόσφατες αναφορές υπονοούν ότι σκανάρεται για κακόβουλο λογισμικό από την Google (η Google έχει απομακρύνει λογισμικό που βρέθηκε να παραβιάζει τους κανόνες της). Υπάρχουν πολλές καταγεγραμμένες επιθέσεις κακόβουλου λογισμικού στην πλατφόρμα Android. Antivirus εφαρμογές είναι διαθέσιμες για Android, αν και η αποτελεσματικότητά τους αμφισβητήθηκε δημόσια.

iOS: Το κατάστημα εφαρμογών της Apple, είναι αυτόνομο από άποψη εφαρμογών, διατίθεται δηλαδή για αγορά εφαρμογών iPhone. Ενώ οι ακριβείς λεπτομέρειες της διαδικασίας εποπτείας είναι άγνωστες για την Apple, υπάρχει ένδειξη που υποστηρίζει ότι η Apple ελέγχει για παραβιάσεις ασφαλείας. Παρόλο που δεν έχουν υπάρξει αξιοσημείωτα δείγματα κακόβουλου λογισμικού για iPhone, υπάρχουν αρκετές εφαρμογές grayware και

jailbreaking . Για μεγαλύτερη ασφάλεια οι χρήστες αποτρέπονται να αποκτούν πρόσβαση σε περίεργες τοποθεσίες με ειδοποιήσεις.

6.2 Αξιόπιστη κινητή τηλεφωνία

Μία άλλη έρευνα που πραγματοποιήθηκε το 2012 από τους Mariantonietta La Polla, Fabio Martinelli και Daniele Sgandurra για το online περιοδικό IEEE COMMUNICATIONS SURVEYS & TUTORIALS [B.3.H.2] πάλι με κύριο θέμα την ασφάλεια των κινητών συσκευών, απέδειξε ότι η TCG (μία ομάδα που εξετάζει την αξιοπιστία των μηχανημάτων-trusted computing group) έχει εκδόσει ένα σετ προσδιορισμών για να μετράει, αποθηκεύει και να περιγράφει την ακεραιότητα του hardware και του software με τη βοήθεια μιας σειράς αξιόπιστων συναρτήσεων (root-of-trust), οι οποίες είναι το TPM (trusted platform module) και το και το CRTM (Core-Root-of-Trust-Measurement). Σε μια πλατφόρμα TPM, ο πυρήνας CRTM μετρά την αποτελεσματικότητα της δικλείδας ασφαλείας (bootloader) του συστήματος και έπειτα αποθηκεύει τη μετρημένη αξία σε μια από τις πλατφόρμες εγκατάστασης εγγραφών PCRs (Platform Configuration Registers) μέσα στο TPM. Τότε το bootloader φορτώνει την εικόνα του λειτουργικού συστήματος, τη μετράει, την αποθηκεύει με προέκταση PCR, δηλαδή μεθόδου η οποία μπορεί να παρουσιάσει με ακρίβεια στιγμιότυπα, εικόνες του λειτουργικού συστήματος και έπειτα ενεργεί. Με τη σειρά του το λειτουργικό σύστημα μετρά τις φορτωμένες εφαρμογές και αποθηκεύει την ακεραιότητά τους στα PCRs πριν τις εκτελέσει. Σε μια πρόκληση πιστοποίησης από έναν τρίτο, η πλατφόρμα TPM υπογράφει ένα σετ τιμών PCR με ένα κλειδί πιστοποίησης AIK και στέλνει πίσω το αποτέλεσμα. Ο ελεγκτής, τότε, μπορεί να πάρει αποφάσεις σχετικά με την κατάσταση αξιοπιστίας της πλατφόρμας επαληθεύοντας την ακεραιότητα αυτών των τιμών και συγκρίνοντας αυτές με τις αντίστοιχες ιδανικές τιμές.

Υπάρχουν επίσης μοντέλα για πλατφόρμες κινητών τηλεφώνων που εκδόθηκαν από την TCG π.χ. το Mobile Trusted Module (MTM). Το TCG προτείνει να χρησιμοποιούμε το MTM για να αυξήσουμε την ασφάλεια των smartphones παρέχοντας βασικές κρυπτογραφικές ικανότητες, όπως παραγωγή τυχαίων αριθμών, κατακερματισμό, προστατευμένη αποθήκευση ευαίσθητων δεδομένων, ασύμμετρη κρυπτογράφηση και παραγωγή υπογραφών. Με αυτά τα κρυπτογραφικά θεμελιακά στοιχεία μπορούμε να εφαρμόσουμε υπηρεσίες ασφαλείας βασιζόμενες σε hardware, όπως είναι η αυθεντικότητα της συσκευής, η μέτρηση ακεραιότητας, η ασφαλής εκκίνηση (boot), και η απομακρυσμένη πιστοποίηση. Το MTM παρέχει αξιοπιστία για smartphones με τον ίδιο τρόπο όπως και το TPM για Η/Υ. Στη θεωρία, το MTM είναι μια προσαρμογή του TPM για smartphones και συνεπώς η προδιαγραφή του είναι παρόμοια με εκείνη του TPM.

Υπάρχουν δύο διαφορετικά είδη μέτρησης της ακεραιότητας κάθε δυαδικής εφαρμογής: το load-time (φόρτωση χρόνου) και οι δυναμικές μετρήσεις. Το TCG καθορίζει

μόνο τη load-time μέτρηση ακεραιότητας, όταν ένα κομμάτι κωδικού ή δεδομένου μετριέται ή όταν χαρτογραφείται/φορτώνεται στην κύρια μνήμη. Οι δυναμικές μετρήσεις αναφέρονται στη δράση της μέτρησης της ακεραιότητας κρίσιμων εφαρμογών σε τρέχοντα χρόνο, π.χ. τη στιγμή που εκτελούνται οι εφαρμογές. Αφού ένας κωδικός χαρτογραφηθεί στη μνήμη και κατά τη διάρκεια της εκτέλεσής του, είναι πολύ δύσκολο να μετρήσουμε την ακεραιότητα της διαδικασίας, λόγω δυναμικής και μη καθορισμένης συμπεριφοράς τυπικών εφαρμογών (φόρτωση ενεργού κωδικού, λήψη εξωτερικών καταχωρήσεων, καταμερισμός της δυναμικής μνήμης).

Επιπλέον μαζί με την εκκίνηση (boot) και τη μέτρηση της ακεραιότητας του χρόνου φόρτωσης, η προστασία της ακεραιότητας των κινητών συσκευών εγείρει τις ακόλουθες επιπλέον ανάγκες:

- Ασφαλής εκκίνηση: ένα σετ απαραίτητων μηχανισμών βρίσκεται στην πλατφόρμα κινητής συσκευής και παρέχει κρίσιμες και απαραίτητες υπηρεσίες που πρέπει να τρέχουν σε φυσιολογικές καταστάσεις (η ακεραιότητα της κινητής συσκευής πρέπει να επιβεβαιωθεί για να διασφαλίσει την αξιοπιστία της). Εξάλλου, σύμφωνα με την αναφορά της TCG Mobile Phone για την ορθή αρχιτεκτονική των κινητών συσκευών η ασφαλής εκκίνηση (boot) είναι απαραίτητο στοιχείο αξιοπιστίας μιας κινητής συσκευής.
- Αργή και χαμηλού επιπέδου εκκίνηση: τα περισσότερα smartphones είναι ακόμη περιορισμένα σε υπολογιστική δύναμη. Για να βελτιωθεί η δύναμή τους απαιτείται ασφαλής εκκίνηση και μέτρηση της ακεραιότητας του συστήματος ενώ ταυτόχρονα δεν θα πρέπει να υποβαθμίζεται η απόδοση και η εμπειρία του χρήστη.
- Εξασφάλιση της ακεραιότητας του συστήματος: αν και η μέτρηση της ακεραιτότητας δεν είναι πρακτική ούτε στα PC ούτε και στις πλατφόρμες για κινητά, θα έπρεπε να υπάρχει ένας μηχανισμός που να διατηρεί το επίπεδο ακεραιότητας σε κρίσιμες εφαρμογές και πηγές κατά τη διάρκεια λειτουργίας του συστήματος. Το TCG δεν προτείνει κανένα μηχανισμό γι' αυτό το σκοπό.

Ένας ασφαλής τρόπος εκκίνησης ενδείκνυται για μέτρηση της ακεραιότητας των κινητών και μηχανισμούς πιστοποίησης [B.1.21], [B.1.9]. Ο προτεινόμενος μηχανισμός διασφαλίζει ότι μια πλατφόρμα για κινητά μπορεί να πετύχει ασφαλή κατάσταση εκμεταλλευόμενη ένα μοντέλο ροής ακεραιότητας. Η λύση επηρεάζει προεκτάσεις πολιτικής ασφαλείας της Linux (SELinux -Security Enhanced Linux). Το σχέδιο απαιτεί αξιοπιστία, όπως το MTM. Στο βιβλίο τους με τίτλο «Measuring integrity on mobile phone systems» οι D. Muthukumaran, A. Sawani, J. Schiffman, B. M. Jung, και T. Jaeger διαπραγματεύονται την προσπάθεια για προστασία της ακεραιότητα κρίσιμων εφαρμογών από αναξιόπιστη χρηστικότητα και ανάπτυξη μιας μικρής πολιτικής SELinux για να μετρήσουν την ακεραιότητα ενός κινητού τηλεφώνου με προσέγγιση PRIMA (policy-reduced integrity measurement

architecture)[B.1.6]. Η πολιτική SELinux που προκύπτει επιτρέπει το σύστημα του τηλεφώνου να πιστοποιεί και προστατεύει κρίσιμες εφαρμογές από αναξιόπιστο κωδικό, οπότε επιτρέπει στον χρήστη να εγκαθιστά και να τρέχει μόνο αξιόπιστες εφαρμογές με ασφαλή τρόπο: η πολιτική αυτή είναι 90% μικρότερη από ότι μια προτεινόμενη πολιτική αναφοράς SELinux. Στο βιβλίο των A. U. Schmidt, N. Kuntze και M. Kasper με τίτλο «On the Deployment of Mobile Trusted Modules» που εκδόθηκε το 2008, προτείνεται μια πρακτική προσέγγισης σχεδίασης και εφαρμογής μιας αξιόπιστης πλατφόρμας για κινητά. Η προσέγγιση ορίζει μια μέθοδο επιβεβαίωσης των δικαιωμάτων του χρήστη για κάθε συσκευή και τη μετακίνηση των διαπιστευτηρίων του χρήστη ανάμεσα στις συσκευές. Οι O. Aciic¸mez, A. Latifi, J.-P. Seifert και X. Zhang ακόμη, στο βιβλίο τους με τίτλο «A Trusted Mobile Phone Prototype» αναγνωρίζουν τρία ειδικά προβλήματα στον προσδιορισμό του MTM και παρέχουν μερικές πιθανές λύσεις. Η πρώτη αφορά την ανάγκη ισορρόπησης μερικών στόχων όπως η απόδοση και κατανάλωση δύναμης, που έρχονται σε αντίθεση με τα σχέδια του συστήματος. Μια προτεινόμενη λύση εντάσσει μερικά χαρακτηριστικά TPM απευθείας σε έναν επεξεργαστή, σε αντίθεση με μια μονολιθική χρήση όλων των συναρτήσεων σε μια ξεχωριστή μονάδα. Το δεύτερο πρόβλημα είναι το ποιοι κρυπτογραφικοί αλγόριθμοι πρέπει να υποστηρίζουν ένα MTM: μερικοί αλγόριθμοι, όπως ο RSA και ο SHA-1 (αλγόριθμοι κρυπτογραφίας), μπορούν να έχουν είτε κακές αποδόσεις είτε αδυναμίες ασφαλείας. Η προτεινόμενη λύση αφορά σε κρυπτογραφία ελλειπτικής καμπύλης ως εναλλακτική εφικτή λύση. Τέλος, το τρίτο πρόβλημα σχετίζεται με την εφαρμογή κρυπτογραφικών θεμελιακών στοιχείων: οι συγγραφείς προτείνουν μια λύση hardware/software αντίθετα με μια λύση βασιζόμενη μόνο στο hardware, η οποία υποφέρει από φτωχή ευελιξία.

6.3 Στατιστικά για τις πρακτικές νεαρών ατόμων σε θέματα ασφαλείας

Η έρευνα που διεξήχθη στη Βουδαπέστη [B.2.6] πραγματοποιήθηκε με τη βοήθεια ερωτηματολογίου με τη μορφή πολλαπλών επιλογών (με διανομή αυτοπροσώπως ή με ερωτηματολόγια στο mail [B.1.7], [B.2.10]) σε φοιτητές της Ευρώπης από ηλικίες κυρίως 18-26, περιλαμβάνοντας και νεαρότερα και μεγαλύτερα σε ηλικία άτομα. Το ποσοστό αυτών των ατόμων εκτός των προαναφερόμενων ορίων ήταν 25,5% από 24-26, γιατί αυτές οι ηλικίες είναι πιο δεκτικές σε νέες τεχνολογίες και κατανοούν καλύτερα την τεχνολογική εξέλιξη από μεγαλύτερους σε ηλικία ανθρώπους οι οποίοι χρησιμοποιούν τα κινητά τηλέφωνα κυρίως για κλήσεις ομιλίας.

Η θεμελιώδης ερώτηση της έρευνας ήταν αν οι φοιτητές είναι ενήμεροι σχετικά με το πώς οι επιλογές και τα τεχνικά χαρακτηριστικά των κινητών τους τηλεφώνων επηρεάζουν την ασφάλεια τους και αν λαμβάνουν τα απαραίτητα μέτρα για να μετριάσουν τα ρίσκα. Μόνο το 29,6% πιστεύουν πως είναι πολύ ή πάρα πολύ ενήμεροι, το 42,6% δηλώνει ότι δεν είναι καθόλου ενήμεροι, ενώ ένα ποσοστό 20,4% δηλώνουν ότι δεν είναι και τόσο πολύ.

Χρησιμοποιώντας την απλή φόρμουλα που περιγράψαμε προηγουμένως, ο μέσος όρος της 'γνώσης για την ασφάλεια' ήταν 1,76 στην κλίμακα 0-4 (όπου 0 καθόλου, 4 πάρα πολύ). Συσχετίζοντας επιπλέον τις απαντήσεις των ερωτηθέντων όσων αφορά στον τύπο του λειτουργικού συστήματος που επιλέγουν απεδείχθη ότι οι φοιτητές που έχουν στην κατοχή τους τηλέφωνα χωρίς σύγχρονο λειτουργικό σύστημα έχουν στατιστικά καλύτερη γνώση σε θέματα ασφαλείας από εκείνους που έχουν στην κατοχή τους ένα κινητό με μοντέρνο O/S. Όπως αναμενόταν, οι χρήστες που δε γνωρίζουν τον τύπο του O/S τους ήταν οι λιγότερο ενημερωμένοι για την ασφάλεια.

Συνεχίζοντας με τη γενική ερώτηση σχετικά με το πόσο 'ασφαλείς' αισθάνονται οι χρήστες κινητών τηλεφώνων, η πλειοψηφία (30%) απάντησε 'υψηλά (πολύ)' ακολουθούμενη από 26% 'μέτρια'. Από την άλλη μεριά, περίπου το 27,9% ένιωθαν όχι πάρα πολύ ή καθόλου σίγουροι ότι ήταν ασφαλείς. Το IMEI είναι πολύ σημαντικό γιατί αν ποτέ κλαπεί το τηλέφωνο, ο πάροχος χρησιμοποιώντας αυτόν το σειριακό αριθμό μπορεί να μπλοκάρει αποτελεσματικά την πρόσβαση στο κλεμμένο τηλέφωνο, οπότε κάπως έτσι μετριάζεται το ρίσκο κλοπής. Σχεδόν οι μισοί φοιτητές δε γνωρίζουν καθόλου την ύπαρξή του. Η γνώση αυτού του χαρακτηριστικού θα βοηθούσε πιθανόν το 41,1% αυτών που δυστυχώς τους έχει κλαπεί το τηλέφωνο μια ή περισσότερες φορές. Ομοίως υψηλά ποσοστά σημειώνονται και από άλλες μελέτες [B.2.2], [B.2.7]. Την ίδια στιγμή, το 71% των χρηστών δε γνωρίζουν την ύπαρξη του ειδικού εικονιδίου που ενημερώνει το χρήστη ότι η κρυπτογράφηση του τηλεφώνου του/της έχει απενεργοποιηθεί [B.3.H.1]. Η άγνοια αυτού του εικονιδίου ασφαλείας αφήνει τους χρήστες ευάλωτους στην επίθεση τύπου man-in-the-middle, - όπου ένας διακομιστής παρεμβαίνει στην επικοινωνία δυο πλευρών.

Οι χρήστες, όπως αναμενόταν, χρησιμοποιούν σε ποσοστό σχεδόν 70% τον κωδικό PIN της SIM τους. Το αρνητικό εύρημα είναι ότι μόνο ένα μικρό ποσοστό (24,5%) χρησιμοποιεί κωδικό οθόνης (screen-saver password) ενώ παρόμοια ποσοστά ανθρώπων δε γνωρίζουν αν το τηλέφωνό τους έχει μια τέτοια επιλογή. Αυτό αφήνει το 75% των χρηστών χωρίς κωδικό οθόνης (screen-saver password) και τα τηλέφωνά τους εκτεθειμένα να χειραγωγηθούν από 'κακόβουλα' χέρια. Μια επίθεση μπορεί να συμβεί μέσα σε λίγα λεπτά κατεβάζοντας συγκεκριμένο λογισμικό στο κινητό τηλέφωνο, γι' αυτόν το λόγο δεν είναι αρκετό να προστατεύετε το κινητό μόνο με PIN αλλά επίσης με ένα κωδικό οθόνης (screen-saver password).

Ένας μεγάλος φορέας επίθεσης του παρελθόντος, το Bluetooth, δε φαίνεται να είναι πρόβλημα πια. Μόλις ένας στους πέντε φοιτητές έχει το Bluetooth ανοιχτό και ορατό (αφήνοντας το κινητό ευάλωτο), ενώ το 42,3% των χρηστών το έχει απενεργοποιημένο.

Σε μια ερώτηση που αγγίζει θέματα ευγένειας και ειλικρίνειας, το 44,7% των φοιτητών δανείζουν τα τηλέφωνά τους, όμως μόνο ενώ είναι παρόντες. Αυτός είναι ο σπουδαιότερος παράγοντας που εκθέτει την ασφάλεια του τηλεφώνου ακόμη και αν ο συμμετέχων είναι παρών, γιατί ένα μόνο λεπτό χρειάζεται κάποιος για να εγκαταστήσει κακόβουλο λογισμικό

στο τηλέφωνο. Πάνω σε αυτό το 36,2% των φοιτητών αρνούνται να δανείσουν το τηλέφωνό τους σε καμία περίπτωση όντας καλύτερα ασφαλείς και 'αγενείς' παρά μετανιωμένοι.

Στη συνέχεια, σε μια ερώτηση ασφαλείας και οικονομικής σημασίας, σχεδόν το 60% των συμμετεχόντων δεν κατεβάζει κανένα λογισμικό. Υπάρχει επίσης ένα 13% που κατεβάζει ενεργά ήχους κλήσης ή logos, ένα 16% που δοκιμάζει εφαρμογές και μόνο το 11% παιχνίδια. Είναι επίσης πολύ ενδιαφέρον να σημειώσουμε ότι η μελέτη της ασφάλειας είναι ένας παράγοντας που μας αποτρέπει από το να κάνουμε download [B.1.14]. Αλλά με το να εξοικειωνόμαστε με το download οι χρήστες γινόμαστε πιο ευάλωτοι στη συνήθεια αυτή και στο να χρησιμοποιούμε μη εξουσιοδοτημένο λογισμικό που μπορεί να βλάψει το τηλέφωνό μας. Εδώ είναι που θα μπορούσε να βοηθήσει ένα antivirus για κινητό τηλέφωνο. Στην συγκεκριμένη έρευνα το 19% των χρηστών γνωρίζουν ότι υπάρχει antivirus για κινητό τηλέφωνο αλλά δεν το χρησιμοποιούν, ενώ το 44% δε γνωρίζουν καν την ύπαρξή του. Μόνο ένα 12,3% τελικά χρησιμοποιεί antivirus για κινητό τηλέφωνο. Συγκρινόμενοι με τους χρήστες PC όπου στις μέρες μας όλοι χρησιμοποιούν (τουλάχιστον) ένα antivirus φαίνεται μια ξεκάθαρη έλλειψη εκπαίδευσης ασφαλείας και διαφορετική αντίληψη. Οι οργανισμοί δείχνουν μια αύξηση στη χρήση εργαλείων antivirus για κινητά τηλέφωνα [B.2.3].

Σχετικά με τις ευαίσθητες πληροφορίες τις οποίες συχνά οι χρήστες αποθηκεύουν στα κινητά τους, στη συγκεκριμένη έρευνα, που ας μην ξεχνάμε είχε να κάνει με νέους, το 57% των φοιτητών πανεπιστημίου κρατούν ευαίσθητες πληροφορίες στα κινητά τους τηλέφωνα. Φαίνεται ότι θεωρούν το κινητό τηλέφωνο μια πολύ προσωπική συσκευή και φυλάνε σε αυτό σημαντικές και ευαίσθητες πληροφορίες. Τέτοιου είδους πληροφορίες θα πρέπει να προστατεύονται αλλά πάλι, τα αποτελέσματα από την έρευνα δείχνουν ότι οι χρήστες αποτυγχάνουν να το κάνουν. Οι συνέπειες από ένα ρήγμα δεδομένων τέτοιου είδους θα μπορούσαν να είναι καταστροφικές για τη ζωή του θύματος.

Ένα μάλλον ιδιαίτερα ανησυχητικό εύρημα, το 21,6% των χρηστών διατηρεί κωδικούς αποθηκευμένους σε κοινή θέα στο κινητό τους τηλέφωνο ενώ τουλάχιστον, ένα 22% χρησιμοποιεί κάποιο είδος κρυπτογράφησης (π.χ. ανακάτεμα γραμμάτων). Καθώς οι χρήστες γενικά ακολουθούν την αντίληψη της κρυπτογράφησης σε αυτούς τους αποθηκευμένους κωδικούς, αναμένεται ότι θα μπορούν να κάνουν το ίδιο με ευαίσθητες πληροφορίες (π.χ. φωτογραφίες) που διατηρούνται στο τηλέφωνο, αρκεί να τους παρέχονταν το απαραίτητο λογισμικό. Για μία ακόμη φορά, το ζήτημα καλύτερα σχεδιασμένων interfaces βγαίνει στην επιφάνεια.

Τέλος, εξετάστηκε το ζήτημα του backup. Ένα μεγάλο ποσοστό των συμμετεχόντων που αγγίζει το 47% δεν κάνει ποτέ backup στα δεδομένα του τηλεφώνου του. Τουλάχιστον ένα 53% κάνει backup, ωστόσο η πλειοψηφία (19%) λιγότερο συχνά από μια φορά το μήνα.

Ως κατακλείδα σημειώνεται ότι η ηλεκτρονική ασφάλεια και η εκπαίδευση για ασφάλεια μένει εκτός εκπαιδευτικού συστήματος ενώ οι χρήστες δε γνωρίζουν αν τα τηλέφωνά τους είναι ασφαλή ή όχι. Δεδομένου ότι τα κινητά τηλέφωνα θα μπορούσαν να είναι

ένα κυρίαρχο χαρακτηριστικό της μελλοντικής σχολικής τάξης, η επίγνωση ειδικής ασφάλειας και τα μαθήματα, που παρουσιάζουν τις βασικές κατευθυντήριες γραμμές πάνω σε αυτό το θέμα, θα έπρεπε αναμφίβολα να διδάσκονται στα σχολεία.

6.4 Φόβοι και ανησυχίες κοινού ανεξαρτήτου ηλικίας

Βάση της έρευνας του Πανεπιστημίου της Καλιφόρνια, υπό την επίβλεψη των Erika Chin, Adrienne Porter Felt, Vyas Sekar και David Wagner που πραγματοποιήθηκε το 2012, ζητήθηκε από μια μερίδα ανθρώπων της εκεί κοινωνίας να απαντήσουν σχετικά με τις ανησυχίες τους περί ασφάλειας και ιδιωτικότητας της κινητής τους συσκευής ανάμεσα στους φόβους που αναφέρθηκαν ήταν:

- Η φυσική απώλεια τηλεφώνου (κακή τοποθέτηση και κλοπή)
- Η φυσική ζημιά
- Η απώλεια δεδομένων και (έλλειψη) back up
- Η ένταση του σήματος
- Ο χρόνος ζωής της μπαταρίας
- Η εμπιστοσύνη εφαρμογών

Σε σύνολο 33 ατόμων οι 17 εξέφρασαν ανησυχίες για την απώλεια του κινητού, 11 για ζημιά, και 5 για απώλεια δεδομένων. Πολλοί ωστόσο είναι αυτοί που ανησυχούν για την ασφάλεια και την ιδιωτικότητα και όχι απλά για την αναστάτωση ή τη χρηματική απώλεια του τηλεφώνου τους. Οι αντιδράσεις σε μία περίπτωση απώλειας του κινητού τηλεφώνου των ερωτηθέντων είναι παρόμοιες. Πολλοί υποστηρίζουν ότι εφόσον έχουν πολλές κρίσιμες πληροφορίες εκεί μέσα που αφορούν ακόμη και την πιστωτική τους κάρτα ή και ευαίσθητα προσωπικά δεδομένα, σίγουρα η απώλεια του τηλεφώνου τους θα τους ήταν πλήγμα. Άλλοι εξέφρασαν αμφιβολίες για την αξιοπιστία των εφαρμογών. Πολλοί δεν κατεβάζουν εφαρμογές γιατί δεν αποδέχονται τους όρους ενώ άλλοι γιατί δεν δέχονται το να δίνουν το γεωγραφικό τους στίγμα ανά πάσα ώρα. Επίσης, μερικοί ανησυχούν μην χάσουν την ιδιωτικότητά τους και συχνά δίνουν ψεύτικα στοιχεία π.χ. στη διαδικασία δημιουργίας ενός νέου λογαριασμού e-mail.

Γίνεται λοιπόν αντιληπτό ότι υφίσταται έντονη ανησυχία γα την ασφάλεια της συσκευής αυτής καθεαυτής όπως και για την ασφάλεια και την αξιοπιστία των εφαρμογών που εγκαθίστανται στη συσκευή και σε μερίδες χρηστών οι οποίοι ξεφεύγουν από τα ηλικιακά όρια ενός φοιτητή. Οι κάτοχοι Android και iPhone και ταυτόχρονα ερωτηθέντες της συγκεκριμένης έρευνας φαίνονται εξίσου ανήσυχοι σχετικά με τη φυσική απώλεια του κινητού και τη ζημιά. Ενώ η Apple παρέχει μια υπηρεσία iCloud με επιλογή να εντοπίζει και να κλειδώνει από απόσταση το τηλέφωνο, μέσω της εφαρμογής «βρες το iPhone μου», οι συμμετέχοντες στη συγκεκριμένη έρευνα δεν γνώριζαν για αυτήν την υπηρεσία, η οποία

κυκλοφόρησε τον Οκτώβριο του 2011. Πριν από αυτήν, η iPhone είχε μια υπηρεσία επί πληρωμής ενώ η Android παρέχει επίσης μια υπηρεσία απομακρυσμένου backup η οποία όμως δεν είναι ιδιαίτερα φιλική προς το χρήστη.

6.5 Προτάσεις – Συστάσεις

Κάποιες προτάσεις – συστάσεις των συγγραφέων Erika Chin, Adrienne Porter Felt, Vyas Sekar και David Wagner της ανωτέρω έρευνας για νέες υπηρεσίες και μηχανισμούς που ίσως βελτιώσουν τη συνολική ασφάλεια στα smartphones είναι οι εξής:

Εκπαίδευση χρήστη: Όπως είδαμε προηγουμένως, αρκετές παρανοήσεις σχετικά με την ασφάλεια των πλατφόρμων και τις συνδέσεις των δικτύων αποτρέπουν τους χρήστες από το να κατανοήσουν πλήρως τη χρησιμότητα των smartphones. Το να εκπαιδευτούν οι χρήστες στις ιδιότητες ασφαλείας των διαφόρων μέσων μαζικής ενημέρωσης, τονίζοντας ιδιαίτερα τα οφέλη της κρυπτογράφησης μπορεί να βοηθήσει στο να ξεκαθαρίσουν τέτοιες παρανοήσεις. Εξάλλου σύμφωνα με πολλές εργαστηριακές μελέτες ανάλογα εκπαιδευτικά προγράμματα για τέτοιου είδους γνώση των χρηστών ήταν αποτελεσματικά σε άλλα ευρύτερα πλαίσια ασφαλείας.

Νέοι δείκτες ασφαλείας: Αρκετοί ερωτηθέντες εκφράζουν δυσπιστία στις εφαρμογές τους και πολλοί συμμετέχοντες εγκαθιστούν εφαρμογές από άγνωστους κατασκευαστές λογισμικού χωρίς να λάβουν υπόψη τους υπάρχοντες δείκτες ασφαλείας. Συνεπώς, καλό θα ήταν να οριστούν νέοι δείκτες ασφαλείας σε συγκεντρωμένες αγορές εφαρμογών για smartphones. Οι χρήστες συχνά φτάνουν στις εφαρμογές μέσω περιήγησης, οπότε σε μία τέτοια περίπτωση οι δείκτες ασφαλείας θα μπορούσαν να προστεθούν στο User-Interface(UI) της περιήγησης. Επίσης οι συμμετέχοντες δε λαμβάνουν υπόψη τις φίρμες των smartphones, λόγω του ότι οι πλατφόρμες των smartphones είναι πάρα πολύ καινούργιες για να διαθέτουν εδραιωμένα μοντέλα. Νέοι δείκτες ασφαλείας θα μπορούσαν να βοηθήσουν τους χρήστες smartphones να αναγνωρίσουν ‘αξιόπιστα’ μοντέλα. Το κοινό ακόμη αναφέρει συχνά ότι λαμβάνει υπόψη του τις κριτικές των χρηστών, όμως οι κριτικές των χρηστών δεν είναι πάντα αξιόπιστες. Μια αγορά εφαρμογών θα μπορούσε να θεσπίσει ένα έμπιστο πρόγραμμα κριτικών για να επισημαίνει και να προωθεί αξιόπιστες κριτικές χρηστών.

Διασυνδέσεις χρηστών για ευαίσθητες εφαρμογές: Μεγαλύτερη χρηστικότητα θα μπορούσε να δείξει το δρόμο στο να αυξηθεί το επίπεδο άνεσης των χρηστών με τις ευαίσθητες εφαρμογές. Για παράδειγμα, θα μπορούσαν να βρεθούν τρόποι που θα έκαναν φανερό οπτικά στους χρήστες το γεγονός ότι βρίσκονται σε ασφαλές δίκτυο ή ότι αλληλεπιδρούν με μια ασφαλή ιστοσελίδα. Οι συμμετέχοντες εξέφρασαν επίσης ότι είναι εύκολο να πατήσουν κατά λάθος κάτι που θα μπορούσε να τους κοστίσει χρήματα. Η

αλληλεπίδραση του χρήστη με τέτοιες εφαρμογές μπορεί να βελτιωθεί, με αποτέλεσμα να νιώθουν πιο άνετα όταν χρησιμοποιούν τα τηλέφωνά τους.

Καλύτερες επιλογές backup: Οι χρήστες ανησυχούν για την απώλεια δεδομένων και τη φυσική απώλεια του τηλεφώνου. Πρόσφατες προσπάθειες όπως η iCloud δείχνουν ότι οι ηγέτες της βιομηχανίας αρχίζουν να προσέχουν αυτό το πρόβλημα. Ιδιαίτερα, το λογισμικό backup σήμερα, είναι δύσκολο να συντονιστεί με το μέσο χρήστη. Για παράδειγμα, δεν υπάρχει κανένας κεντρικός μηχανισμός που να καθορίζει το είδος των δεδομένων που υφίστανται backup στην τρέχουσα πλατφόρμα Android. Διαμορφώνοντας τα UI και ρυθμίζοντας καλύτερα κατά την αρχικοποίησή τους τις συνηθέστερες λειτουργίες (όπως η μουσική, το βίντεο, τα μηνύματα, τα email) το κοινό σίγουρα θα ενθαρρυνθεί προς την υιοθέτηση τέτοιων υπηρεσιών.

Καλύτερες υπηρεσίες απομακρυσμένου κλειδώματος: Για να ανταποκριθούν καλύτερα οι εταιρίες στις έγνοιες των χρηστών για την απώλεια και την κλοπή του τηλεφώνου, ασύρματοι φορείς και πωλητές πλατφορμών θα μπορούσαν να παρέχουν επί πληρωμής υπηρεσίες απομακρυσμένου κλειδώματος και απομακρυσμένης διαγραφής. Ενώ υπάρχουν πωλητές AntiVirus που παρέχουν τέτοιες υπηρεσίες (πακέτο με λογισμικό ασφαλείας), το ευρύ κοινό δεν γνωρίζει τη διαθεσιμότητά τους. Εάν γίνει ευρέως γνωστή αυτή η υπηρεσία θα μετριαστούν οι φόβοι των χρηστών σχετικά με το να χάσουν τα τηλέφωνά τους, φόβοι ο οποίοι φαίνεται να περιορίζουν αντίστοιχα και τη δραστηριότητά τους. Άλλες εναλλακτικές για να ασφαλίσουμε τα τηλέφωνα από απώλεια ή κλοπή θα μπορούσαν να είναι ο σχεδιασμός καλύτερων μηχανισμών συνεχούς πιστοποίησης.

6.6 Αυθαίρετες ενέργειες και Τεχνικές εξαπάτησης

Παρακάτω παρατίθενται από τη Symantec.com στο σύνδεσμο της ανάλυσης των απειλών για κινητά (Analysis of Mobile Threats) 5 βασικοί τρόποι αυθαίρετων ενεργειών:

Συλλογή Δεδομένων. Η πιο γνωστή από τις κακές εφαρμογές για κινητά είναι η συλλογή δεδομένων από την εκτεθειμένη συσκευή. Αυτό γίνεται με απώτερο σκοπό να διεξαχθούν περισσότερες κακόβουλες δραστηριότητες, ειδικότερα ό,τι έχει να κάνει με κλέψιμο πληροφοριών με δούρειους ίππους. Κάτι τέτοιο συμπεριλαμβάνει συγκεκριμένες πληροφορίες τόσο για τη συσκευή όσο και για το χρήστη, όπως δεδομένα δομής μέχρι και λεπτομέρειες τραπεζικών συναλλαγών. Αυτή η πληροφορία με τους αριθμούς IMEI και IMSI, χρησιμοποιείται με πολλούς τρόπους αν και δεν είναι τόσο επικίνδυνη, απλά χρησιμοποιείται ως ένας τρόπος αναγνώρισης της συσκευής μοναδικά. Πιο ανησυχητική είναι η συγκέντρωση των δεδομένων που αφορούν στο λογισμικό της συσκευής, (όπως για το τι έκδοση είναι το λειτουργικό της σύστημα (OS) ή τι εγκατεστημένες εφαρμογές έχει), για να συνεχίσουν οι

επιτήδειοι τις επιθέσεις (εκμεταλλευόμενοι ας πούμε μια αδυναμία λογισμικού). Σπανιότερα, αλλά υψίστης σημασίας είναι όταν συγκεντρώνονται πληροφορίες για τα δεδομένα του χρήστη, όπως λεπτομέρειες για τις τραπεζικές συναλλαγές του, προκειμένου να δοκιμάσουν οι επιτήδειοι να κάνουν μη εξουσιοδοτημένες συναλλαγές. Ενώ αυτή η κατηγορία καλύπτει ένα ευρύ φάσμα περιπτώσεων, η διάκριση μεταξύ πληροφοριών συσκευής και δεδομένων χρήστη δίνεται με περισσότερες λεπτομέρειες στις παρακάτω υποκατηγορίες.

Παρακολούθηση του χρήστη. Ο επόμενος πιο κοινός σκοπός των επιτήδειων ήταν να εντοπίσουν την προσωπική συμπεριφορά και τις δράσεις ενός χρήστη. Αυτές οι κινήσεις παίρνουν δεδομένα ειδικά για να κατασκοπεύσουν το άτομο που χρησιμοποιεί το τηλέφωνο. Αυτό γίνεται συγκεντρώνοντας ποικίλα δεδομένα επικοινωνίας, όπως μηνύματα SMS εισερχόμενες και εξερχόμενες κλήσεις και στέλνοντάς τα σε έναν άλλο υπολογιστή ή συσκευή. Σε μερικές περιπτώσεις μπορεί ακόμη και να καταγράφουν τηλεφωνικές κλήσεις. Σε άλλες περιπτώσεις αυτές οι κακόβουλες δράσεις εντοπίζουν συντεταγμένες GPS, κρατώντας ουσιαστικά καρτέλες για την τοποθεσία της συσκευής (και του χρήστη) ανά οποιαδήποτε στιγμή. Το να συγκεντρώνουν φωτογραφίες που τραβήχτηκαν με το τηλέφωνο εμπίπτει επίσης σε αυτήν την κατηγορία.

Αποστολή περιεχόμενου. Η τρίτη μεγαλύτερη ομάδα κακόβουλων μεθόδων είναι οι κακές εφαρμογές που διανέμουν περιεχόμενο. Αυτή η μέθοδος είναι διαφορετική από τις δυο πρώτες κατηγορίες επειδή η άμεση πρόθεσή των επιτήδειων στην περίπτωση αυτή είναι να βγάλουν χρήματα. Οι περισσότερες από αυτές τις κακές δράσεις θα στείλουν ένα γραπτό μήνυμα σε έναν premium αριθμό, του οποίου μηνύματος η χρέωση θα εμφανιστεί τελικά στο λογαριασμό του κινητού του ιδιοκτήτη της συσκευής. Επίσης σε αυτήν την κατηγορία ανήκουν μέθοδοι που ενεργούν ως ρωστήρες email spam, ελεγχόμενοι από τους επιτήδειους, στέλνοντας ανεπιθύμητα emails από διευθύνσεις καταχωρημένες στη συσκευή.

Παραδοσιακές απειλές. Η τέταρτη ομάδα περιέχει περισσότερο παραδοσιακές απειλές, όπως πίσω πόρτες και downloaders. Φαίνεται να αρέσει στους επιτήδειους να μεταφέρουν αυτά τα είδη ρίσκου από τα PCs σε κινητές συσκευές.

Αλλαγή Ρυθμίσεων. Τέλος, υπάρχει ένας μικρός αριθμός κακόβουλων ενεργειών κατά τις οποίες γίνονται αλλαγές στην εγκατάσταση. Με αυτές τις ενέργειες οι επιτήδειοι επιχειρούν να αυξήσουν τα προνόμια ή απλά να τροποποιήσουν ποικίλες ρυθμίσεις στο λειτουργικό σύστημα. Ο σκοπός αυτής της τελικής ομάδας των κακόβουλων ενεργειών φαίνεται να είναι το να εκτελέσουν επιπλέον δράσεις στις εκτεθειμένες συσκευές.

Σε ειδικό σύνδεσμο της ιστοσελίδας της UPS με τίτλο «Μάθετε να αναγνωρίζεται την απάτη» αναλύονται επίσης τεχνικές εξαπάτησης οι οποίες εφαρμόζονται κατά κόρον τα τελευταία χρόνια και είναι οι εξής:

Phishing: Πρόκειται για ιδιαίτερα διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» προσωπικών δεδομένων και ειδικότερα στοιχείων που αφορούν οικονομικές συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας κ.λπ.).

Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name) που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη, η οποία όμως μοιάζει πανομοιότυπη με τη γνήσια.

Σε γενικές γραμμές οι απάτες που είναι γνωστές με τον όρο «scam» αφορούν κάποια συναλλαγή που για να ολοκληρωθεί χρειάζεται κάποια χρήματα από το υποψήφιο θύμα - παραλήπτη του παραπλανητικού μηνύματος. Ωστόσο, το θύμα δεν παραλαμβάνει ποτέ τα προσφερόμενα ανταλλάγματα.

Διεθνή Λαχεία: «Διεθνή» λαχεία αποστέλλουν e-mails, ανακοινώνοντας κέρδη. Στη συνέχεια και αφού τα θύματα έχουν πεισθεί για τα κέρδη, ζητούν απ' αυτούς να καταβάλ-λουν χρήματα για διαδικαστικά έξοδα.

Δημοπρασίες: Σε μη αξιόπιστες ιστοσελίδες δημοπρασιών ενδέχεται να γίνεται πλειστηριασμός ανύπαρκτων αντικειμένων. Τα θύματα πληρώνουν προκαταβολές και διαδικαστικά έξοδα, ωστόσο δεν παραλαμβάνουν ποτέ το αντικείμενο για το οποίο πλειοδότησαν.

Ransomware: Μέσω ηλεκτρονικού ταχυδρομείου το θύμα λαμβάνει μήνυμα με ένα συνημμένο αρχείο ή πρόγραμμα. Μόλις το ανοίξει αρχίζει η διαδικασία κρυπτογράφησης των αρχείων που είναι αποθηκευμένα στον υπολογιστή του. Ως συνέπεια, το θύμα δεν μπορεί να ανοίξει κανένα αρχείο του εκτός από το μήνυμα που του άφησαν οι «scammers» στο οποίο του εξηγούν ότι μόνο αφού πληρώσει ένα συγκεκριμένο ποσό θα του αποσταλεί ο κωδικός πρόσβασης. Πρόκειται ουσιαστικά για απαγωγή των αρχείων του, για την ανάκτηση των οποίων πρέπει να καταβάλλει λύτρα!

Πλαστές επιταγές ή χρηματικές εντολές:

Η δυνατότητα οποιουδήποτε να αγοράζει οτιδήποτε, από οπουδήποτε, οποιαδήποτε ώρα της ημέρας ή της νύχτας, σύμφωνα επίσης με σχετικό σύνδεσμο ενημέρωσης στην ιστοσελίδα της UPS, προσφέρει απίστευτες ευκαιρίες σε όλους μας και στους εικονικούς μας γείτονες σε όλο τον κόσμο. Δυστυχώς, ορισμένοι από αυτούς τους γείτονες δεν σκέφτονται με γνώμονα το δικό μας συμφέρον. Ένας τύπος απάτης είναι η αποστολή πλαστών επιταγών ή χρηματικών εντολών, συνήθως με την υπηρεσία UPS Next Day Air®, είτε ως απάντηση σε μια online διαφήμιση είτε στο πλαίσιο μιας πλαστής προσφοράς εργασίας. Μην υποθέτετε ότι η μέθοδος της παράδοσης προσδίδει νομιμότητα στα περιεχόμενα του δέματος.

Αν λάβατε μια επιταγή ή μια χρηματική εντολή που δεν περιμένατε, θα πρέπει να τη θεωρήσετε πλαστή. Θα πρέπει επίσης να είστε εξαιρετικά επιφυλακτικοί αν λάβετε μια επιταγή ή μια χρηματική εντολή για ποσό μεγαλύτερο από το αναμενόμενο. Μπορεί κάποιος να επικοινωνήσει μαζί σας μέσω e-mail, ζητώντας σας να εξαργυρώσετε ή να καταθέσετε τα χρήματα και να επιστρέψετε τμήμα τους μέσω Western Union ή με άλλη μέθοδο. Ο απατεώνας θα σας πει ότι μπορείτε να κρατήσετε τμήμα των χρημάτων, κάτι που δεν σας συμφέρει αν λάβετε υπόψη σας ότι η αρχική επιταγή είναι πιθανότατα πλαστή. Ακόμα και η

τράπεζα μπορεί αρχικά να θεωρήσει την επιταγή ή τη χρηματική εντολή νομότυπη, με αποτέλεσμα να ανακαλύψει την αλήθεια καθυστερημένα και να σας την επιστρέψει για επιστροφή των χρημάτων που σας κατέβαλε.

ΚΕΦΑΛΑΙΟ 7ο: ΤΟ ΤΕΛΟΣ ΖΩΗΣ ΤΩΝ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

7.1 Εισαγωγή

Σύμφωνα με τη διατριβή των Mohammad Alsheyab και Sigrid Kusch [B.2.9] που φέρει τον τίτλο «End of Life of Electronic Communication Devices in the Context of Strategies to Decouple Resources Use from Economic Growth» και η οποία μάλιστα παρουσιάστηκε στο συνέδριο Διοίκησης των Επιστημών το 2013, οι κινητές συσκευές τηλεπικοινωνιών έχουν γίνει σταθερή αξία στην καθημερινή ζωή του ανθρώπου. Οι γρήγορες αλλαγές στην τεχνολογία και οι ανάγκες που προκύπτουν από την παραγωγή των βιομηχανιών επηρεάζουν τις συνήθειες και τις απαιτήσεις των καταναλωτών. Η τεχνολογία των τηλεπικοινωνιών ξεπερνιέται πολύ γρήγορα και έτσι η ψηφιακή οικονομία, δημιουργώντας μια μόνιμη απαίτηση για τους νεότερους εξοπλισμούς, παράγει ταυτόχρονα όλο και μεγαλύτερες ποσότητες ηλεκτρονικών αποβλήτων. Αυτό οφείλεται σε παράγοντες που σχετίζονται κυρίως και με την περιβαλλοντική εκπαίδευση, ευαισθησία και αντίληψη των ατόμων.

Μερικά από τα απόβλητα αποτελούν εγκληματική παράβαση. Ο τηλεπικοινωνιακός και ψηφιακός εξοπλισμός με τους πόρους και τα δεδομένα του έχει γίνει κρίσιμος και συνεπώς αποτελεί κρίσιμο στοιχείο για την πρόοδο στην οικονομική, επιστημονική και πολιτισμική ζωή. Υπάρχει πολύ λίγη εμπειρική εργασία πάνω στο θέμα, όμως πέρα από την κακή διαχείριση σε βιομηχανικό επίπεδο, η συγκάλυψη και ανωνυμία που παρέχεται από τις τηλεπικοινωνίες φαίνεται να ικανοποιεί ειδικές παρορμήσεις ατόμων [B.1.13]. Αυτό έχει ως αποτέλεσμα όχι μόνο να ελέγχεται κάποιος από κάποιους τρίτους, αλλά και να μελετάται η ψυχολογική του αντίδραση από αυτούς. Ίσως λοιπόν το μπλοκάρισμα και η απενεργοποίηση

των πόρων να συμβάλλουν στην επιτάχυνση της έντασης του ατόμου προκειμένου τελικά να κάνουν κάποιοι τη δουλειά τους εκμεταλλευόμενοι την ψυχολογική δυσλειτουργία του ατόμου.

Οι υπολογιστές και τα κινητά τηλέφωνα είναι αυξανόμενης σημασίας και στις αναπτυσσόμενες χώρες. Στην Αφρική ήδη ο μισός πληθυσμός από το ένα δισεκατομμύριο συνολικά έχουν πρόσβαση σε ένα κινητό τηλέφωνο και στην Ινδία προστίθενται κάθε μήνα 15 εκατομμύρια κινητά τηλέφωνα. Σήμερα τα κινητά τηλέφωνα έχουν γίνει το πανταχού παρόν ηλεκτρονικό προϊόν παγκοσμίως [Β.1.15].

Εθελοντικά δίκτυα ανακύκλωσης μπορούν να συνεισφέρουν σημαντικά στην αντιμετώπιση της αυξανόμενης έλλειψης βασικών μετάλλων που βρίσκονται στα κινητά τηλέφωνα [Β.1.11]. Τα κινητά τηλέφωνα είναι σχετικά μικρότερα σε μέγεθος σε σύγκριση με άλλες ηλεκτρικές συσκευές. Αυτό έχει ως αποτέλεσμα να καταλήγουν βάρος για τις αρχές οι οποίες δεν μπορούν να τα διαχειριστούν με τη συνηθισμένη ροή στέρεων αποβλήτων, ακόμη και όταν οι υπηρεσίες ανακύκλωσης είναι διαθέσιμες. Οι εφαρμογές των υπηρεσιών ανακύκλωσης απαιτούν δημόσια υποστήριξη σε αναπτυσσόμενες χώρες (π.χ. στην Ινδία) [Β.1.16].

Αν ταξινομηθούν ξεχωριστά όλα αυτά τα απόβλητα μπορεί να επεξεργαστούν για να μας προσφέρουν σημαντικά ποσά πολύτιμων πόρων όπως χρυσό. Οι μεγάλες μεταβολές στη σύνθεση των συσκευών είναι μια ειδική πρόκληση. Η προεπεξεργασία επηρεάζει την ανάκτηση μετάλλων όπως ο χρυσός. Αυτή η προεπεξεργασία (που γίνεται χειροκίνητα, μηχανικά ή με συνδυασμένες μεθόδους) σιγουρεύει ότι τα υλικά μπαίνουν στον κατάλληλο δρόμο ανάκτησης. Δεν τίθενται ειδικές προκλήσεις. Μόνο η ποικίλη σύνθεση των συσκευών, η αναγκαιότητα να εγκαταστήσουμε επαρκής υποδομές και οι ποσότητες των ηλεκτρονικών αποβλήτων είναι τα βασικά θέματα που με μελέτη αντιμετωπίζονται. Ο εξοπλισμός επικοινωνιών φαίνεται να είναι το κυρίαρχο ηλεκτρονικό απόβλητο στην Αφρική, σε φτωχότερες περιοχές της Ασίας και στη Λατινική/Νότια Αμερική, αλλά υπάρχει ανάγκη συγκέντρωση περισσότερων και ακριβέστερων στοιχείων [Β.1.10].

Εκτός από το να μπουν σε ανακυκλώσιμα μονοπάτια ή στη χειρότερη περίπτωση να εναπωθετηθούν σε χωματερές, τα κινητά τηλέφωνα συχνά επαναχρησιμοποιούνται. Τα κινητά τηλέφωνα είναι επί του παρόντος ένα από τα λιγοστά ηλεκτρονικά προϊόντα με ελκυστική αγορά επαναχρησιμοποίησης –με συνέπεια όλο και περισσότερα ακουστικά να επαναχρησιμοποιούνται παρά να ανακυκλώνονται.

7.2 Εφαρμογές στην πράξη

Οι ανεπτυγμένες χώρες έχουν ήδη νομοθεσία ηλεκτρονικών αποβλήτων. Σύμφωνα με την έρευνα των Mohammad Alsheyab και Sigrid Kusch έχουν σχετικά ευρείς και λεπτομερείς νόμους που ρυθμίζουν την ανακύκλωση ηλεκτρονικών αποβλήτων, δεν συμπεριλαμβάνουν όμως, όλες τις εντολές της Ευρωπαϊκής Ένωσης για την ανακύκλωση ηλεκτρονικών

αποβλήτων και το νόμο για την ανακύκλωση οικιακών συσκευών της Ιαπωνίας. Στην Κίνα, η ανακύκλωση, η μεταχείριση και η διαχείριση των ηλεκτρονικών αποβλήτων είναι ακόμη σε αρχικό και ερευνητικό στάδιο. Δεν υπάρχουν σχετικοί νόμοι ή κανονισμοί. Τον Ιανουάριο του 2011, η Κίνα επίσημα άρχισε να εφαρμόζει τους κανονισμούς για τη διαχείριση της ανακύκλωσης και τη διάθεση των αποβλήτων ηλεκτρικών συσκευών και ηλεκτρονικών προϊόντων, οι οποίοι σαφώς εγγυούνται το θέμα της ευθύνης, της επίβλεψης των αρχών, τις μεθόδους τιμωρίας κλπ και προτείνουν να εγκαθιδρυθεί ένα εθνικό ίδρυμα για τη μεταχείριση των ηλεκτρονικών αποβλήτων. Παρ' όλα αυτά, λεπτομερής κανόνες για την εφαρμογή των κανονισμών δεν έχουν εκδοθεί και δεν είναι ακόμη ξεκάθαρο πώς οικονομικές ευθύνες θα διευθετηθούν. Η επένδυση σε αρχικά στάδια μεταχείρισης ηλεκτρονικών αποβλήτων και μετέπειτα κόστη στην ανακύκλωση και τη διαχείριση, είναι τεράστια και οι επιχειρήσεις θα τα βγάλουν πέρα δύσκολα χωρίς μία ειδική υποστήριξη από την κυβέρνηση. Συνεπώς και οι παραγωγοί και οι καταναλωτές ηλεκτρονικών προϊόντων είναι υπεύθυνοι για τα αντίστοιχα κόστη ή τέλη που προκαλούνται από την ανακύκλωση ηλεκτρονικών αποβλήτων και την μεταχείριση τους, για να βοηθήσουν και το κράτος στην καλή διαχείριση. Στις αναπτυγμένες χώρες όπως στην Ευρώπη και τις ΗΠΑ όπου χρησιμοποιείται το σύστημα εκτεταμένης ευθύνης παραγωγού, οι παρασκευαστές του ηλεκτρονικού προϊόντος είναι υπεύθυνοι για τη μεταχείριση και την ανακύκλωση ηλεκτρονικών αποβλήτων ενώ οι καταναλωτές μοιράζονται μια σχετικά χαμηλότερη οικονομικά ευθύνη. Αντίθετα, τα κόστη που προκύπτουν στη διαδικασία της μεταχείρισης ηλεκτρονικών αποβλήτων στην Ιαπωνία, κυρίως αναλαμβάνουν οι καταναλωτές. Στην Κίνα, θα ήταν παράλογο να καταμερίσουμε το οικονομικό κόστος μόνο στους παραγωγούς ή μόνο στους καταναλωτές βάσει των ιδιαίτερων συνθηκών της. Οι παραγωγοί επωφελούνται από την πώληση ηλεκτρονικών προϊόντων και οι καταναλωτές από την ωφέλεια της διασκέδασης. Συνεπώς, το κόστος των πεταμένων ηλεκτρονικών προϊόντων πρέπει να μοιραστεί και στους παραγωγούς και στους καταναλωτές.

Από την άλλη μεριά το επίπεδο επίγνωσης και αντίδρασης για τα απόβλητα που παράγονται από ηλεκτρικό και ηλεκτρονικό εξοπλισμό διαφέρει σημαντικά ανάμεσα στις ανεπτυγμένες και τις αναπτυσσόμενες χώρες. Παρ' όλο που τα πλεονεκτήματα της χρήσης των συσκευών κινητών είναι υπεράριθμα, τα μειονεκτήματα αντίστοιχα επίσης υφίστανται. Ακολουθώντας την ανάλυση της δουλειάς που έκανε ο Emmenger et al., υπολογίζεται ότι η παραγωγή μιας συσκευής κινητού τηλεφώνου παράγει περίπου 60 kg CO_2. Είναι άραγε αυτό ευρέως γνωστό; Φτάνει να αναφερθεί ότι στις αναπτυσσόμενες χώρες, προκειμένου να διασώσουν τα μέταλλα που μπορούν να αναμορφωθούν, αυτά τα απόβλητα τα καίνε σε ανοιχτή φωτιά ή τα περιχύνουν με οξύ (Carroll, 2008). Τα απόβλητα που προκύπτουν από αυτή τη διαδικασία είναι προφανώς τοξικά και αποτελούν τεράστιο κίνδυνο για εκείνους που ζουν κοντά. Η εκτίμηση των μοτίβων κατανάλωσης μαζί με την αύξηση του επιπέδου

επίγνωσης είναι οι δύο βασικοί παράγοντες για να αναγνωριστούν τα ηλεκτρονικά απόβλητα ως εκμεταλλεύσιμα υλικά (κάτι που συμβαίνει π.χ. στην Ιορδανία)[Β.3.1].

Η ανακύκλωση των ηλεκτρονικών αποβλήτων στην πράξη σε μια χώρα όπως η Ιορδανία θα απαιτούσε μια σειρά δράσεων όπως:

1) Φορολογία του ηλεκτρονικού εξοπλισμού που εισάγονται στην αγορά κάθε χρόνο.
2) Εκτίμηση του χρόνου ζωής διαφόρων κατηγοριών ηλεκτρονικού εξοπλισμού.
3) Φορολογία των ηλεκτρονικών αποβλήτων που παράγονται ανά χρόνο.
4) Εγκαθίδρυση ενός εθνικού συστήματος συλλογής.
5) Εκτίμηση του ρυθμού συλλογής διαφόρων κατηγοριών ηλεκτρονικών αποβλήτων.
6) Εκτίμηση της πιθανής ανάκτησης διαφόρων συστατικών από τα ηλεκτρονικά απόβλητα.
7) Εγκαθίδρυση βιομηχανικών εγκαταστάσεων για ανακύκλωση και μεταχείριση αποβλήτων μέχρι το στάδιο της ανάκτησης τους.

7.3 Η επικρατούσα κατάσταση στην Ελλάδα

Με το μήνυμα «Ρίξτο στην ανακύκλωση» η εταιρία Vodafone υλοποιεί το πρόγραμμα ανακύκλωσης κινητών τηλεφώνων, μπαταριών και αξεσουάρ, που εφάρμοσε πανελλαδικά για πρώτη χρονιά το 2003, όπως αναφέρεται και στην ιστοσελίδα Vodafone.gr.. Συμπαραστάτες της προσπάθειας αυτής τάσσονται συχνά πολύ Δήμοι της χώρας καθώς και τηλεοπτικοί σταθμοί όπως ο ΣΚΑΪ. Μέχρι σήμερα έχουν προωθηθεί για ανακύκλωση περισσότερα από 600.000 προϊόντα κινητής επικοινωνίας (κινητά τηλέφωνα, φορτιστές και αξεσουάρ), τα οποία έχουν συγκεντρωθεί στους ειδικούς κάδους συλλογής που είναι εγκατεστημένοι:

- σε όλα τα καταστήματα Vodafone και τα κτίρια της εταιρείας
- σε όλα τα Συστήματα του Σώματος Ελλήνων Προσκόπων
- σε εταιρικούς πελάτες

Στο πρόγραμμα ανακύκλωσης κινητών τηλεφώνων, μπαταριών και αξεσουάρ σύμφωνα με τη Vodafone μπορούν να συμμετέχουν όλοι οι φίλοι του περιβάλλοντος, ανεξάρτητα από το δίκτυο επικοινωνίας που χρησιμοποιούν. Το πρόγραμμα περιλαμβάνει ανακύκλωση προϊόντων επικοινωνίας, όπως κινητά τηλέφωνα και σχετικά αξεσουάρ, όπως φορτιστές, hands-free, bluetooth, πρόσοψη και συσκευές σταθερής τηλεφωνίας, φορητούς υπολογιστές και modems, λοιπό εξοπλισμό & αξεσουάρ σταθερής/κινητής επικοινωνίας και internet, καθώς και οικιακές μπαταρίες.

Τα προϊόντα που συγκεντρώνονται παραλαμβάνονται από εξουσιοδοτημένο από το κράτος φορέα εναλλακτικής διαχείρισης, ο οποίος έχει την ευθύνη, σύμφωνα με την εθνική νομοθεσία, για την επαναχρησιμοποίηση, αποσυναρμολόγηση και περαιτέρω χρήση των υλικών για παραγωγή άλλων αντικειμένων. Όλα τα αντικείμενα, αποσυναρμολογούνται στα

επιμέρους υλικά τους και κατόπιν επεξεργασίας τα υλικά αυτά χρησιμοποιούνται για την παραγωγή άλλων αντικειμένων (όπως αντικείμενα οικιακής χρήσης, κώνοι τροχαίας κλπ).

Επίσης, μια άλλη εταιρία ονόματι fonebank προωθεί την ανακύκλωση κινητών με τα εξής κίνητρα μέσω της ιστοσελίδας της:

1) προσφέρει συμβουλές προκειμένου να αποφευχθούν τυχόν λάθη (μη ανάκτηση δεδομένων)
2) επεξηγεί ποια η μεταχείριση των συσκευών έπειτα από την παραλαβή τους από το συνεργείο ανακύκλωσής
3) επεξηγεί αναλυτικά τους λόγους για τους οποίους συμφέρει η ανακύκλωση από οικονομικής αλλά και από περιβαλλοντικής άποψης πληρώνοντας ένα αντίτιμο στον ιδιοκτήτη και το κυριότερο
4) πληρώνει ένα αντίτιμο στον ιδιοκτήτη

Οι παραπάνω συσκευές αποτελούνται από υλικά, όπως πλαστικό και μέταλλα, ενώ οι οικιακές μπαταρίες περιέχουν στοιχεία, τα οποία, αν πεταχτούν στα σκουπίδια, θα καταλήξουν στον υδροφόρο ορίζοντα (δηλαδή στο πόσιμο νερό), επιβαρύνοντας έτσι το περιβάλλον. Για παράδειγμα, στις μπαταρίες νικελίου καδμίου που χρησιμοποιούμε, η ποσότητα του καδμίου που χρησιμοποιούμε, η ποσότητα του καδμίου που περιέχουν, είναι ικανή να μολύνει το 1/3 του νερού μιας πισίνας Ολυμπιακών διαστάσεων.

7.4 Η μεταχείριση των παλαιών συσκευών από τις εταιρίες:

Η fonebank μία από τις εταιρίες που προωθούν το θέμα της ανακύκλωσης στην Ελλάδα αναφέρει χαρακτηριστικά στην ιστοσελίδα της. «Όταν λάβουμε τα άχρηστα για εσάς κινητά για ανακύκλωση, τα επαναχρησιμοποιούμε ή τα ανακυκλώνουμε. Ελέγχεται η κατάσταση του κινητού τηλεφώνου και, αν είναι καλή, στέλνεται σε αναπτυσσόμενες χώρες όπως η Ασία και η Αφρική για επαναχρησιμοποίηση. Πρόκειται για μια πράξη που συμβάλλει στην προστασία του περιβάλλοντος, αφού εξοικονομεί φυσικούς πόρους, ενώ ταυτόχρονα δίνει τη δυνατότητα στους λιγότερο ευνοημένους να έχουν πρόσβαση στην τεχνολογία των κινητών τηλεφώνων. Οι υποδομές σταθερής τηλεφωνίας στις αναπτυσσόμενες χώρες είναι σε κακή κατάσταση, αν όχι ανύπαρκτες, και τα νέα κινητά τηλέφωνα κοστίζουν ακριβά, επομένως η ανακύκλωση βοηθά αυτούς που δεν έχουν την οικονομική δυνατότητα να αγοράσουν καινούριο κινητό.

Τα τηλέφωνα που δεν λειτουργούν και εκείνα που δεν μπορούν να επιδιορθωθούν έχουν σημαντικά και χρήσιμα εξαρτήματα, τα οποία μπορούν να αποσπαστούν και να επαναχρησιμοποιηθούν. Αυτά τα τηλέφωνα υφίστανται μηχανική ή χημική επεξεργασία, αφού έχει επέλθει το τέλος της διάρκειας ζωής τους. Κατά τη μηχανική επεξεργασία το κινητό

αποσυναρμολογείται και τα εξαρτήματά του διαχωρίζονται. Από την άλλη, κατά τη χημική επεξεργασία τα μέταλλα και τα πολύτιμα υλικά, όπως ο χρυσός, το ασήμι και ο λευκόχρυσος ή το πλαστικό, διαχωρίζονται για επαναχρησιμοποίηση».

ΚΕΦΑΛΑΙΟ 8ο: ΕΠΙΛΟΓΟΣ

Η παρούσα διπλωματική εργασία αποτέλεσε μία προσπάθεια καταγραφής όλων των σχετικών/πρόσφατων πηγών και της κριτικής προσέγγισης τόσο των εμπλεκόμενων τεχνολογιών όσο και των οικονομικών επιπτώσεων που φέρει η χρήση των κινητών συσκευών για συναλλαγές σε χώρες της Ε.Ε. (ή ακόμη και σε ΗΠΑ, Κίνα, κ.ά.). Ειδικότερη ενδιαφέρουσα πλευρά αποτέλεσε η διερεύνηση-μελέτη οικονομικών και τεχνολογικών στοιχείων που εμπλέκονται στην ανακύκλωση των κινητών συσκευών.

Η ανάγκη για την αφύπνιση του κοινού που χρησιμοποιεί έξυπνες συσκευές σε προσωπικό ή επαγγελματικό επίπεδο κρίνεται αναγκαία. Δυστυχώς όπως προκύπτει και από την έρευνα οι χρήστες απλών συσκευών είναι περισσότερο συνειδητοποιημένοι ως προς την ασφάλεια σε σχέση με τους χρήστες των έξυπνων συσκευών. Οι κάτοχοι των έξυπνων συσκευών πολλές φορές τυχαίνει να μην γνωρίζουν καν το λειτουργικό σύστημα του κινητού τους αλλά παρ΄ όλα αυτά να έχουν όλες τις τελευταίες εφαρμογές που κυκλοφορούν στην αγορά εγκατεστημένες στη συσκευή τους.

Τα κακόβουλα λογισμικά που κυκλοφορούν στην αγορά και στοχεύουν όλο και περισσότερο στα λειτουργικά συστήματα των έξυπνων συσκευών χρησιμοποιούν ως μέσο για να «εισβάλλουν» στις συσκευές τις εφαρμογές αλλά κυρίως-μικρά- λάθη των χρηστών ή αδυναμίες του λειτουργικού συστήματος. Η ασφάλεια των οικονομικών συναλλαγών των χρηστών (είτε πρόκειται για άτομα, είτε για επιχειρήσεις) αποτελεί καίριο σημείο για συνέχιση της μελέτης των ηλεκτρονικών συσκευών που συνηθίζουμε να αποκαλούμε ως «έξυπνες».

Η περαιτέρω έρευνα και διατριβή στο θέμα αυτό θεωρείται δεδομένη μιας και μεγάλο επιστημονικό μέρος της παγκόσμιας κοινότητας έχει ταχθεί στην καταγραφή και αντιμετώπιση όλων αυτών των προβλημάτων.

8.1 Σύνοψη και συμπεράσματα

Κατά τη μελέτη της συγκεκριμένης εργασίας:

α) ερευνήθηκαν οι τελευταίες τάσεις περί των εφαρμογών, τεχνικών εξαπάτησης και κακόβουλου λογισμικού που κυκλοφορεί για τις κινητές συσκευές σε παγκόσμιο επίπεδο και από περιβαλλοντικής πλευράς την επιβάρυνση που μπορεί να έχουν όλα τα παραπάνω στη φύση,

β) αναγνωρίστηκαν εφαρμογές που ενδεχομένως να χρειαστεί να αγοράσει κάποιος για προσωπική ή επαγγελματική χρήση. Ταυτόχρονα έγινε αντιληπτό με ποιους τρόπους μπορεί να γίνει εξαπάτηση προσωπικών δεδομένων μέσω χρεώσεων και κυρίως μέσω οικονομικών συναλλαγών καθώς επίσης και με ποιον τρόπο αντιμετωπίζονται ως ένα βαθμό επιθέσεις κακόβουλου λογισμικού στο λειτουργικό σύστημα κάποιας κινητής συσκευής σε προσωπικό ή επαγγελματικό επίπεδο.

γ) «αποκωδικοποιήθηκε» ο τρόπος σκέψης και η ψυχολογία του επιτήδειου χρήστη σε βαθμό που να προβλέπεται κάποια ηλεκτρονική απειλή πριν ο κακόβουλος χρήστης μετρήσει κι άλλο θύμα.

Γίνεται αντιληπτό κατόπιν της μελέτης της συγκεκριμένης εργασίας ότι η οικονομική και τεχνολογική πρόκληση που επιφέρει η εξέλιξη της τεχνολογίας της πληροφορίας στο κομμάτι των έξυπνων συσκευών δεν είναι καθόλου εύκολη υπόθεση να αντιμετωπιστεί. Η παράθεση των πηγών και η κριτική προσέγγιση τόσο των εμπλεκόμενων τεχνολογιών όσο και των οικονομικών επιπτώσεων σε χώρες της Ε.Ε. (ή ακόμη και σε ΗΠΑ, Κίνα κ.ά.) φανερώνουν ότι υπάρχει ακόμη πολύς δρόμος και πιθανόν το πρόβλημα των επιτήδειων που στοχεύουν στο ανίδεο κοινό πάντα θα υπάρχει.

Ο δρόμος φαίνεται να είναι ιδιαίτερα μακρύς και δύσκολος ιδιαίτερα στο κομμάτι που έχει να κάνει με το κακόβουλο λογισμικό που στοχεύει σε υποκλοπές. Επιπλέον κάτι εξίσου σημαντικό που όμως και πάλι δε φαίνεται να εκλείπει όσο οι εταιρίες χρησιμοποιούν ηλεκτρονικά μέσα, είναι η επίθεση με σκοπό την απόσπαση δεδομένων και πληροφοριών καθώς και η πρόκληση τεχνικών προβλημάτων στα λειτουργικά συστήματα των μηχανημάτων που ανήκουν σε εταιρίες και οργανισμούς.

Επιπλέον, όσων αφορά στο περιβαλλοντικό κομμάτι της ανακύκλωσης παρ' όλο που γίνονται σημαντικές προσπάθειες να κοινοποιηθεί μια παγκόσμια καμπάνια και να κινητοποιηθούν μαζικά φορείς και κράτη τα αποτελέσματα δεν είναι επαρκή.

8.2 Μελλοντικές επεκτάσεις

Ως συνέχεια της παρούσας έρευνας και έχοντας τέλεια γνώση της τρέχουσας κατάστασης των θεμάτων που διαπραγματεύτηκαν ανωτέρω θα μπορούσε να επεκταθεί κάποιος κυρίως σε θέματα ασφάλειας κακόβουλου λογισμικού σε κινητές συσκευές.

Πιο συγκεκριμένα, από τα ανωτέρω γίνεται αντιληπτό ότι μεγαλύτερη ανάγκη υπάρχει στο κομμάτι της ασφάλειας. Δεδομένου ότι η ασφάλεια αποτελεί το Α και το Ω σε πολλές πτυχές της χρήσης των κινητών συσκευών, μία περαιτέρω έρευνα πάνω στο πως θα αντιμετωπιστούν επιθέσεις, εισβολές, αποκοπές, ζημιές στο λειτουργικό σύστημα μιας κινητής συσκευής, θα ήταν η καλύτερη διαδρομή ενός ερευνητή. Η πορεία του κακόβουλου λογισμικού για Η/Υ θα αποτελέσει φάρο σε μία τέτοια επέκταση μιας και σε αρκετές περιπτώσεις ακολουθείται το ίδιο μοτίβο ως προς τον τρόπο μόλυνσης. Βέβαια υπάρχουν και περιπτώσεις κατά τις οποίες ο τρόπος επίθεσης έχει αλλάξει εντελώς δεδομένης της γνώσης πλέον των επιτήδειων επί των λαθών από προηγούμενη εμπειρία με Η/Υ.

Γενικότερα, η έρευνα σχετικά με την ασφάλεια του λειτουργικού συστήματος μιας έξυπνης συσκευής θα αποτελούσε ό,τι καλύτερο ως απάντηση στις οικονομικές και τεχνολογικές προκλήσεις που επιφέρει η χρήση των κινητών συσκευών σε ατομικό και εταιρικό επίπεδο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Β.1: Πίνακας Αναφορών

[1]. Α.Πασχόπουλος – Π.Σκάλτσας.(2000).*Ηλεκτρονικό Εμπόριο Νέο περιβάλλον Νέα εργαλεία Νέοι ηγέτες*. Εκδ. Κλειδάριθμος

[2]. Κ.Βλαχόπουλος.2007.*Ηλεκτρονικό έγκλημα, Μορφές, Πρόληψη, Αντιμετώπιση*. Νομική Βιβλιοθήκη

[3]. A.Borg.(2011).*Enterprise Mobility Management Goes Global: Mobility Becomes Core IT*.Aberdeen Group

[4]. A.G.Kravets, N. Duong Bui, M. Al-Ashval.(2014).*Mobile Security Solution for Entreprise Network*.Volgograng Russia.Volgograng State

Technical University

[5]. A.Rosen.(2000).*The e-commerce question and answer book*. New York.Amazon, a division of American Management Association Internation

[6]. A. U. Schmidt, N. Kuntze, M. Kasper.(2008). *On the Deployment of Mobile Trusted Modules*.Wireless Communications and Network ing Conference.WCNC 2008 IEEE.pp.3169-3174

[7]. D.A.Dillman.(1999).*Mail and Internet Surveys: The Tailored Design Method*.John Wiley & Sons.2nd edition

[8]. D.Alms.*Understanding Mobility Management: Trends, Priorities and Imperatives*. Visage Mobile

[9]. D. Muthukumaran, A. Sawani, J. Schiffman, B. M. Jung, T. Jaeger.(2008).*Measuring integrity on mobile phone systems*.SACMAT 2008: Proceedings of the 13th ACM symposium on Access control models and technologies. New York.NY.USA.ACM.pp155-164

[10]. F.O. Ongondo, I.D. Williams,T.J. Cherrett.(2011).*How are WEEE doing?A global review of the management of electrical and electronic wastes*.Waste Management. pp 714-730

[11]. F.O. Ongondo,I.D.Williams.(2011).*Mobile phone collection, reuse and recycling in the UK*.Waste Management 31. pp 1307-1315

[12]. G.Elliot – N.Phillips.(2004).*Mobile Commerce and Wireless Computing Systems*. England.Pearson Education Limited

[13]. L. Miller,(2012).*Stalking: Patterns, motives and intervention strategies*.Aggression and Violent Behaviour 17. pp. 495-506

[14]. M. Rahman,H. Imai.(2002).*Security in Wireless Communication*.Wireless Personal Communications. pp.218-228

[15]. O. Aciic¸mez, A. Latifi, J.-P. Seifert, X. Zhang.(2008).*A Trusted Mobile Phone Prototype*.Consumer Communications and Networking Conference.CCNC 2008. 5th IEEE.pp. 1208-1209

[16]. R.K. Kaushal A.K. Nema.(2012).*An analysis of preferences for hazardous substances free products: manufacturing, use and end of life mobile phone*.Waste Management & Research 30, 2012, pp. 1169-1177

[17]. S.Drake.*Embracing Next Generation Mobile Platforms to Solve Business Problems*. Computerworld Inc. IDC

[18]. T. Jaeger, R. Sailer, and U. Shankar.(2006).*PRIMA: policy-reduced integrity measurement architecture*. SACMAT06: Proceedings of the eleventh ACM symposium on Access control models and technologies. New York.NY.USA.ACM.pp.19-28

[19]. Wiley Publishing.(2009). *iPhone for dummies*. 3rd edition, Indianapolis, Indiana

[20]. X.Zhang,O. Aciic¸mez,J.-P. Seifert.(2007).A trusted mobile phone reference architecture via secure kernel.STC '07: Proceedings of the 2007 ACM

workshop on Scalable trusted computing,NewYork, NY,ACM.pp 7-14
[21]. X.Zhang,O.Aciic¸mez,J.-P. Seifert.(2009).*Building Efficient Integrity Measurement and Attestation for Mobile Phone Platforms*.Security and Privacy in Mobile Information and Communication Systems.First International ICST Conference.MobiSec 2009.Turin.Italy.June 3-5, 2009, Revised Selected Papers, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol17,Springer.pp 71-82

Β.2 Εργασίες/ Διατριβές

[1]. Cisco and/or its afillitates.(2014).*Secure Network Access for Personal Mobile Devices*

[2]. CPP.(2010).*Mobile phone theft hotspot.*,CPP survey, http://www.cpp.co.uk.(Διαθέσιμο: 05/05/2013)

[3] Darkreading.(2010).*Survey: 54 Percent Of Organizations Plan To Add Smartphone Antivirus This Year*. Darkreading article. http://www.darkreading.com. (Διαθέσιμο: 05/05/2013]

[4]. Dipartimento d' ignegneria gestionale,MIP – school of management.(2012). *Mobile internet & Apps: is booming*.Polytechnico di Milano

[5]. E.Chin, A. Porter Felt, V. Sekar, D. Wagner.(2012).*Measuring User Confidence in Smartphone Security and Privacy*.University of California.Berkeley Intel Labs

[6]. I.Androulidakis, G.Kandus.(2011). *Mobile Phone Security Awareness and Practices of Students in Budapest.*ICDT 2011: The Sixth International Conference on Digital Telecommunications

[7]. ITwire.(2010).*One-third of Aussies lose mobile phones: survey*.ITwire article, http://www.itwire.com.(Διαθέσιμο: 05/05/2013]

[8]. K. Streff.(2010).*An Overview of Mobile Banking Threats.*The Macroeconomics of Mobile Money.Columbia University.New York.NY

[9]. M.Alsheyab – S. Kusch.(2013).*End of Life of Electronic Communication Devices in the Context of Strategies to Decouple Resources Use from Economic Growth*.Conference of Informatics and Management Sciences

[10]. S. L. Pfleeger, B.A.Kitchenham.(2001).*Principles of Survey Research Part 1: Turning Lemons into Lemonade*.ACM SIGSOFT Software Engineering

[11]. T.A. Lum.(2011).*Mobile goes global The effect of cell phones on economic growth and development, an econometric analysis*.Bucknell University

Β.3 Περιοδικά - Ηλεκτρονικά Περιοδικά

[1]. F.Y. Fraige, L.A. Al-khatib, H.M. Alnawafleh, M.K. Dweirj, P.A.Langston.(2012).*Waste electric and electronic equipment in Jordan: willingness and generation rates*.Journal of Environmental Planning and Management 55 (2).pp. 161-175

[2]. J. Kietzmann, K.Plangger, B.Eaton, K.Heilgenberg, L.Pitt, P.Berthon: Mobility at work: A typology of mobile communities of practice and contextual ambidexterity.Journal of Strategic Information Systems 3 (4)

[H.1]. I. Androulidakis.(2009).*Intercepting Mobile Phones*.Article in «IT Security professional» magazine, Issue 8. pp. 42-28

[H.2]. M. La Polla, F. Martinelli, D. Sgandurra.(2012).*A Survey on Security for Mobile Devices,* IEEE COMMUNICATIONS SURVEYS & TUTORIALS

[H.3]. 50 organizations from around the world.(2014).*2014 data breach investigations report.*Verizon

Β.4 Ιστοσελίδες

[H.1] http://www.theregister.co.uk/2012/12/07/eurograbber_mobile_malware_scam/

[H.2] http://www.scmagazine.com/beyond-theory-mobile-malware/article/211990/

[H.3] http://www.zdnet.com/how-did-european-bank-malware-steal-47-million-7000008481/

[H.4] http://bgr.com/2011/12/14/more-than-1-million-stolen-from-android-users-in-2011-mobile-threats- to-increase-in-2012/

[H.5] http://www.bbc.co.uk/news/world-europe-19994944

[H.6] http://www.bbc.co.uk/news/technology-19402398

[H.7] http://www.webtorials.com/discussions/2012/03/mobile-malware-coming-soon.html

[H.8] http://www.symantec.com/content/en/us/about/media/pdfs/b-state_of_mobility_survey_2012.en-us.pdf

[H.9] http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=analysis_of_mobile_threats

[H.10] http://techtalker.quickanddirtytips.com/dangers-of-unsecured-wifi-hotspots.aspx

[H.11] http://www.ups.com/content/gr/el/resources/ship/fraud_ups_recognize.html

[H.12] https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.thinkmind.org%2Fdownload.php%3Farticleid

%3Dicdt_2011_1_40_20110&ei=_31LUceVJYXuOr_-gfAN&usg=AFQjCNFpkkk-SsTLQXB0TicL7rt7HEUNFA&bvm=bv.44158598,d.ZWU&cad=rja

[H.13] http://www.saferinternet.gr/index.php?objId=Category116&parentobjId=Page2

[H.14] http://www4.gsb.columbia.edu/filemgr?file_id=733516

[H.15] http://www.scmagazineuk.com/focusing-on-mobile-malware/article/247409/

[H.16] http://bgr.com/2011/12/14/more-than-1-million-stolen-from-android-users-in-2011-mobile-threats-to-increase-in-2012/

[H.17] http://skai.gr/

[H.18] http://fonebank.gr/

[H.19] http://www.tutor2u.net/blog/index.php/economics/comments/mobile-phones-the-impact-on-the-economy-society-and-our-personal-lives

[H.20] http://nakedsecurity.sophos.com/2014/08/22/apple-ios-malware-gets-onto-75000-iphones-steals-ad-clicks/

[H.21] http://blog.avast.com/author/vlk/

[H.22] http://www.slideshare.net/bilalmalick1990/electronic-and-mobile-banking