ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (ΜΕΣΟΛΟΓΓΙ)

Πτυχιακή εργασία

Ψηφιακός εγκληματίας (Hacker)

Σπυρόπουλος Χρήστος

Επιβλέπων καθηγητής κ. Χρήστος Τσουραμάνης

ΜΕΣΟΛΟΓΓΙ 2016

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Στη σημερινή εποχή της ραγδαίας τεχνολογικής εξέλιξης παρατηρείται αυξανόμενη εισχώρηση νέων τεχνολογιών στην παγκόσμια κοινωνία καθώς και οι μεταβολές που επιφέρει σε καθημερινές δραστηριότητες, τον τρόπο ψυχαγωγίας και σκέψης. Παράλληλα όμως, οι νέες αυτές συνθήκες δημιούργησαν πρόσφορο έδαφος για την ανάδειξη νέων μορφών εγκληματικότητας και παράνομες συμπεριφορές γνωστές ως Ψηφιακό Έγκλημα και αυτοί που το διαπράττουν Ψηφιακοί Εγκληματίες. Η νέα κατηγορία αυτή λειτουργεί χρησιμοποιώντας τους ηλεκτρονικούς υπολογιστές, όπου ανακαλύπτει νέους τρόπους για κλοπή στοιχείων, χρημάτων, δημιουργία κακόβουλων λογισμικών και απόκτηση παράνομης πρόσβασης σε απόρρητα στοιχεία. Σαν αποτέλεσμα διευκολύνεται το έργο των εγκληματιών και το διογκώνεται το έγκλημα.

1.1 Ιστορική Αναδρομή

Αρχικά, ο όρος «**χάκερ**» σήμαινε στα αγγλικά το δημιουργό ενός επίπλου ή ξύλινου αντικειμένου με τη βοήθεια τσεκουριού. Η ιστορία των χάκερς ξεκινάει το 1960 από σπουδαστές του πανεπιστημίου του MIT. Οι υπολογιστές την εποχή εκείνη ήταν mainframes τα οποία ήταν κλειδωμένα σε δωμάτια με ελεγχόμενη θερμοκρασία. Το κόστος λειτουργίας τους ήταν απαγορευτικό και οι ερευνητές είχαν στη διάθεση τους περιορισμένο χρόνο εργασίας. Κάποιοι από αυτούς, δημιούργησαν τα πρώτα hacks, προγράμματα για να ενισχύσουν την απόδοσή. Αρκετές φορές τα hacks ήταν καλύτερα από τα αρχικά προγράμματα. Ένα από τα μεγαλύτερα hacks της ιστορίας έγινε το 1969, όταν δύο υπάλληλοι της Bell έφτιαξαν προγράμματα για να ενισχύσουν την ταχύτητα των υπολογιστών. Το hack αυτό το πήρε το ονόμα UNIX και σήμερα αποτελεί ένα ευρέως γνωστό λειτουργικό σύστημα. Τη δεκαετία του 1970, χάκερς χρησιμοποίησαν το χρόνο τους για την εξερεύνηση των δυνατοτήτων των ανερχόμενων τεχνολογιών. Το 1971 ο John Draper, ένας βετεράνος του Βιετνάμ, και στον οποίο δόθηκε το ψευδώνυμο Captain Crunch, συνελήφθηκε για παράνομη συμπεριφορά. Τότε δημιουργήθηκε ένα κοινωνικό κίνημα από το

περιοδικό YIPL/TAP (Youth International Party Line/Technical Assistance Program) το οποίο βοηθούσε χάκερς να κάνουν δωρεάν υπεραστικές κλήσεις. Στη συνέχεια, δύο μέλη του Homebrew Computer Club της Καλιφόρνιας, οι Steve Jobs και Steve Wozniak, δημιούργησαν τα «blueboxes», συσκευές με τις οποίες συνήθιζαν να «κάνουν Hack» σε τηλεφωνικές συσκευές. Το 1978, οι Randy Sousa και Ward Christiansen δημιούργησαν το πρώτο BBS (Bulletin Board System) για Hackers που λειτουργεί μέχρι και σήμερα. Το 1983, συνελήφθησαν οι χάκερς με ψευδώνυμο 414 από το FBI. Αυτοί είχαν εισβάλει σε 60 υπολογιστές διάφορων ερευνητικών κέντρων συμπεριλαμβανομένων των Memorial Sloan-Kettering Cancer Center και Alamos National Laboratory. Την ίδια εποχή η ταινία "War Games" έριξε φως στο τούνελ του hacking και προειδοποίησε το κοινό για τις ικανότητες των χάκερς. Οι ίδιοι οι χάκερς πήραν ποικίλα μηνύματα από την ταινία. Το 1984 αποτέλεσε την αρχή του Μεγάλου Πολέμου κατά των χάκερς. Δημιουργήθηκε η ομάδα Legion of Doom, μέλη των οποίων αποσπάστηκαν και δημιούργησαν τους Masters of Deception. Από το 1990 και για δύο χρόνια, οι δύο ομάδες βρισκόντουσαν σε συνεχή διαμάχη μεταξύ τους μέχρι που έλιξε όταν το FBI συνέλαβε τις ομάδες. Στο τέλος της δεκαετίας του '80 ιδρύθηκε ο πρώτος νόμος για τους ηλεκτρονικούς υπολογιστές στο Κογκρέσο της Αμερικής. Ο Robert Morris 1988 εισέβαλε σε 6.000 υπολογιστές και κέρδισε τον "τίτλο" του πρώτου hacker που τιμωρήθηκε από τον νόμο, με 10.000 δολάρια πρόστιμο και ατέλειωτες ώρες κοινωνικού έργου. Στη συνέχεια, ακολούθησαν ο Kevin Mitnick και κάποια μέλη των Legion of Doom. Τα αισθήματα του κοινού για τους χάκερς άλλαξαν. Οι χάκερς δεν ήταν πια οι εκκεντρικοί που ήθελαν μόνο να εμπλουτίσουν το πηγάδι των γνώσεων τους. Η οικονομία που στηριζόταν στο δίκτυο χρειαζόταν προστασία και οι χάκερς χαρακτηρίστηκαν ως εγκληματίες. Τη δεκαετία του 1990, αυξήθηκαν οι κλοπές μέσω internet από τους χάκερς. Χαρακτηριστικό γεγονός ήταν ότι το 2000, σε τρεις ημέρες χάκερς κατάφεραν να εμποδίσουν τη πρόσβαση σε ιστοσελίδες όπως οιYahoo!, Amazon.com, Buy.com, eBay και CNN.com υπερφορτώνοντας το σύστημα. Ακολούθησαν επιθέσεις κατά κυβερνήσεων, κλεψίτυπα αντίγραφα λογισμικού αλλά και δημιουργία ηλεκτρονικών ιών από χάκερς ανά τον κόσμο.

Βιβλιογραφία

http://www.sptimes.com/Hackers/history.hacking.html

Ιστορία των Hackers:
https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81

1.2 Εισφορά Της Εργασίας

Ξεκινώντας από την εισαγωγή, ο αναγνώστης ενημερωνεται για την ιστορική εξέλιξη των ψηφιακών εγκληματιών. Από το 1971 και την συνεχή εξέλιξή τους, ο αναγνώστης μαθαίνει για στον κόσμο των Hacker και συγκεκριμένα για γνωστές ηλεκτρονικές τραπεζικές και τηλεπικοινωνιακές απάτες όπως επίσης, και γνωστές απειλές κρατικών φορέων. Ο ορισμός του ηλεκτρονικού εγκλήματος και τα χαρακτηριστικά του όσο και των μορφών του δίνουν μία σφαιρική εικόνα και βοηθούν στην καλύτερη κατανόηση του θέματος.

Πέρα από την γενική προσέγγιση του θέματος, στην εργασία περιγράφονται αναλυτικά κατηγορίες και είδη των ψηφιακών εγκληματιών, οι όροι **cracking** και **hacking**, καθώς και τα κίνητρα που κρύβονται και τα μέσα που χρησιμοποιούνται πίσω από τις επιθέσεις ψηφιακών εγκληματιών. Καθημερινοί χρήστες του διαδικτύου και των υπολογιστών, επωφελούνται επιπλέον από την συνεισφορά της εργασίας σε αυτό το κομμάτι καθώς αναφέρονται τρόποι προστασίας και τρόποι αντιμετώπισης από τους ψηφιακούς εγκληματίες. Τέλος, οι καταναλωτές και οι επιχειρήσεις που χρησιμοποιούν το διαδίκτυο για τις καθημερινές τραπεζικές τους συναλλαγές μπορούν να πληροφορηθούν για τους κινδύνους που αντιμετωπίζουν και για τα μέσα με τα οποία μπορούν να προφυλαχτούν.

1.3. Δομή εργασίας

Η πτυχιακή εργασία αυτή παρουσιάζει τις πτυχές του ψηφιακού εγκληματία και του ψηφιακού εγκλήματος. Επίσης, περιλαμβάνει λόγους, εργαλεία και κίνητρα που διαπράττονται τα ψηφιακά εγκλήματα και τρόποι αντιμετώπισής τους.

Αρχικά, στο πρώτο κεφάλαιο, ο αναγνώστης μαθαίνει την ιστορία των ψηφιακών εγκλημάτων και ο τρόπος που αντιμετωπίστηκαν.

Στο δεύτερο κεφάλαιο, δίνεται ο ορισμός του ψηφιακού εγκληματία όπως επίσης οι κατηγορίες, τα είδη και τα χαρακτηριστικά τους αντίστοιχα.

Στα επόμενα δύο κεφάλαια περιγράφονται τα κίνητρα, τα εργαλεία καθώς και τρόποι αντιμετώπισης κατά των ψηφιακών εγκληματιών.

Συγκεκριμένα, στο τρίτο κεφάλαιο περιγράφονται οι τρόποι, τα εργαλεία και τα κίνητρα που έχουν οι ψηφιακοί εγκληματίες συμπεριλαμβανομένων παράνομη πρόσβαση, κλοπή πληροφοριών, διακίνηση πορνογραφικού υλικού καθώς και καταστροφή λειτουργικών συστημάτων με τη χρήση κακόβουλων λογισμικών.

Στο τέταρτο κεφάλαιο δίνονται πληροφορίες σχετικά με την ελληνική Αστυνομία και τη συμβολή της στην αντιμετώπιση του ψηφιακού εγκλήματος καθώς και μέτρα και συμβουλές που μπορούν να αξιοποιήσουν μεγάλη πληθώρα χρηστών του διαδικτύου από απλούς χρήστες μέχρι και επιχειρήσεις.

Στο πέμπτο κεφάλαιο παρουσιάζεται η προσπάθεια που καταβάλουν οι εταιρίες για την παροχή της καλύτερης δυνατής προστασίας μέσω της διοργάνωσης διαγωνισμών. Μέσω μιας τέτοιου είδους εκδήλωσης οι εταιρίες μαθαίνουν τις αδυναμίες των προϊόντων τους.

Η εργασία ολοκληρώνεται με σύνοψη όλων των παραπάνω και το λόγο που είναι δύσκολη η σύλληψη των ψηφιακών εγκληματιών καθώς και η αντιμετώπισή τους καθώς επίσης δίνονται πληροφορίες σχετικά με τη λήψη μέτρων για την αντιμετώπισή τους.

ΚΕΦΑΛΑΙΟ 2

Ψηφιακός Εγκληματίας (Hacker)

2.1 Ορισμός Ψηφιακού Εγκληματία (HACKER)

Ακριβής ορισμός του όρου hacker (hacking) δεν υπάρχει. Για κάποιους ο hacker είναι κάποιος που περνάει το μεγαλύτερο μέρος της ζωής του μπροστά από έναν υπολογιστή προσπαθώντας να εισβάλει χωρίς εξουσιοδότηση σε άλλους υπολογιστές ή δίκτυα υπολογιστών, να προκαλέσει καταστροφές, να "σπάσει" κωδικούς, να κλέψει πολύτιμα δεδομένα, κλπ. Για άλλους είναι ένας πανέξυπνος άνθρωπος που χρησιμοποιεί τις γνώσεις του για την παροχή προστασίας σε σύστημα υπολογιστών.

Ένας ορισμός που θα μπορούσε να φανεί αντιπροσωπευτικός είναι ο παρακάτω:

Ως hacker αναφέρεται το άτομο το οποίο διαθέτει εξειδικευμένες γνώσεις να εισβάλλει και να διαχειρίζεται με εκπληκτική ευκολία διάφορα πληροφοριακά και υπολογιστικά συστήματα, χωρίς απαραίτητα να τα καταστρέφει ή να δημιουργεί προβλήματα σε αυτά.

Οι hackers είναι συνήθως λάτρης των υπολογιστών, του προγραμματισμού και του σχεδιασμού πληροφοριακών συστημάτων. Οι περισσότεροι έχουν την τάση να ασχολούνται με άλλες επιστήμες που δεν συνδέονται άμεσα με τους υπολογιστές και να δεξιότητες σε αυτά σε σπουδαίο επίπεδο. Αξιοσημείωτο είναι ότι οι hackers συνήθως δρουν με καλές προθέσεις και όχι κακόβουλες όπως θεωρούν αρκετοί. Προσπαθούν να ανακαλύψουν νέα πράγματα μέσω της απασχόλησης αυτής και αποκτήσουν περισσότερες γνώσεις. Επιπλέον, υποστηρίζει και πιστεύει σε μία κουλτούρα των hackers που είχε "δημιουργηθεί" παλαιότερα, κατά την εμφάνιση των πρώτων πληροφοριακών συστημάτων. Όπως έχει διατυπωθεί από τον **Eric Steven Raymond** (προγραμματιστής, συγγραφέας και υποστηρικτής του κινήματος Open Source Software, υπάρχει

άνθρωποι που αυτοαποκαλούνται hackers, αλλά δεν είναι. Αυτοί είναι άνθρωποι (κυρίως έφηβοι) που βρίσκουν διασκεδαστικό το να εισβάλλουν σε υπολογιστές και να παραβιάζουν το σύστημα του τηλεφώνου άνευ λόγου και αιτίας. Αυτοί ονομάζονται Crackers και δεν υπάρχει αντιπαλότητα και πολλές διαφορές με τους Hackers. Οι Hackers πιστεύουν πως οι crackers είναι αργόσχολοι, ανεύθυνοι, και όχι πολύ έξυπνοι, αφού το ότι έχεις εξειδικευμένες γνώσεις στους ηλεκτρονικά συστήματα δεν σε κάνει hacker. Πολλοί δημοσιογράφοι και συγγραφείς συγχέουν τις ομάδες αυτές με αποτέλεσμα να παρουσιάζουν τους crackers ως hackers αλλά και το αντίθετο. Η βασική διαφορά είναι αυτή: **Οι hackers χτίζουν πράγματα, οι crackers τα σπάνε**.

2.2 Έννοιες Cracking και Hacking

Η μορφή αυτή του Ηλεκτρονικού Εγκλήματος αφορά την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, με παράνομους τρόπους και δόλιους σκοπούς. Ο Ψηφιακός εγκληματίας χωρίζεται σε δύο κατηγορίες ανάλογα με τον τρόπο εισβολής και το σκοπό που προσπαθεί να επιτύχει. Οι κατηγορίες αυτές είναι το hacking και cracking.

Hackers χαρακτηρίζονται τα άτομα που έχουν εξειδικευμένες γνώσεις και ικανότητες στη διαχειρηση υπολογιστικών συστημάτων. Συνήθως είναι προγραμματιστές, σχεδιαστές συστημάτων και ακόμα και αν δεν ασχολούνται επαγγελματικά, δουλεύουν είτε μόνοι τους είτε σε ομάδες. Οι Hackers είναι σε θέση να εντοπίσουν αδυναμίες σε λογισμικά και λειτουργικά συστήματα καθώς και να συνεργαστούν για την επίλυση προβλημάτων υπολογιστών. Σαν απότερο σκοπό έχουν την ικανοποίηση που αποκτούν από την παράκαμψη συστημάτων ασφαλείας και την πρόσληψη τους από τον αντίστοιχο οργανισμό που εντόπισαν το εκάστοτε πρόβλημα και βοήθησαν στην επίλυση του. Οι Hackers πιστεύουν ότι προσφέρουν κοινωνικό έργο καθώς δεν έχουν κακό σκοπό αλλά αντίθετα βοηθούν την κοινωνία.

Crackers, από την άλλη, είναι άτομα τα οποία χαρακτηρίζονται ως κακόβουλοι hackers καθώς η εισβολή τους στα υπολογιστικά συστήματα έχει στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, δημιουργία κακόβουλων λογισμικών, παραβίαση κωδικών ασφαλείας, παύση της προστασίας των προγραμμάτων κάνοντας εφικτή την παράνομη αντιγραφή τους. Οι ενέργειες αυτές έχουν σκοπό την αποκόμοιση οικονομικών οφελών και πληροφοριών όπως π.χ. μεταφορά χρημάτων από λογαριασμό σε λογαριασμό και κλοπή κωδικών πιστωτικής κάρτας.

Το πρόβλημα με το cracking είναι ότι δεν εντοπίζεται σε επιθέσεις που γίνονται σε δημόσιες υπηρεσίες ή οργανισμούς επειδή εντοπίζεται εύκολα ο εισβολέας. Αντίθετα, γίνοται πολλές ύπουλες επιθέσεις με σκοπό την τροποποίηση πληροφοριών όπως η αντιγραφή ολόκληρων δικτυακών τόπων, μεγαλοεπιχειρήσεων που κάνουν πωλήσεις μέσω διαδικτύου, μεγάλων οργανισμών, δημόσιων υπηρεσιών και εξαπάτηση ανυποψίαστων χρηστών του διαδικτύου.

Ένας μεγάλος αριθμός hackers τίνει σε εγκληματικές συμπεριφορές. Εισβάλουν σε τραπεζικά συστήματα και καταστήματα ηλεκτρονικού εμπορίου υποκλέπτοντας διάφορες πληροφορίες όπως κωδικούς πιστωτικών καρτών και πολλές φορές μπαίνουν σε κρατικά συστήματα για εκμετάλλευση πληροφοριών ή την χρήση ιών για πρόκληση ζημιάς σε προγράμματα και συστήματα. Οι hackers γενικά παραβιάζουν το νόμο για να αποκομίσουν κάποιο όφελος, είτε είναι χρηματικό είτε όχι. Πλέον, η παρακικρή εισβολή σε ένα δίκτυο υπολογιστών χωρίς να έχει κάποια επίπτωση στο σύστημα διώκεται ποινικά.

Βασικός επίσης παράγοντας αυτής τη συμπεριφοράς είναι το γεγονός ότι πλέον καταρρίπτεται η ιδέα της βιομηχανίας ασφαλείας υπολογιστών η οποία θέλει να έχει πλήρη έλεγχο πληροφοριών για δικούς της σκοπούς. Η βιομηχανία αυτή είναι δυσαρεστημένη με hackers που αποκαλύπτουν κρατικά και εταιρικά λάθη και καθώς την αναγκάζουν να επενδύσει τεράστια χρηματικά ποσά σε αγορά και δημιουργία νέων προγραμμάτων ασφαλείας πιο ανθεκτικών των προηγουμένων για να μπορέσουν να αμυνθούν από μελλοντικές επιθέσεις.

2.3 Κατηγορίες των Hacker

Τα τελευταία χρόνια, οι **Hackers** έχουν αποκτήσει κακή φήμη έχουν χαρακτηριστεί από την κοινωνία ως εγκληματίες. Χωρίζονται σε κατηγορίες ανάλογα με τις ηθικές τους αρχές. Χαρακτηριστικοί όροι που χρησιμοποιούνται για τους **hackers** είναι **Crackers** και **Black Hats**. Ο όρος κράκερ χρησιμοποιείται για να διακρίνει αυτούς που αποκτούν παράνομη πρόσβαση σε υπολογιστικά συστήματα στα οποία προκαλούν σοβαρές ζημιές.

Οι όροι B**lack/White/Gray hats** αναφέρονται στις ομάδες των hacker ανάλογα με τις ηθικές τους αρχές. Ο όρος black hats χαρακτηρίζει τα άτομα εκείνα που έχουν μεγάλη εξειδίκευση στους υπολογιστές αλλά χρησιμοποιούν τις ικανότητές τους με μη ηθικούς τρόπους.

Ενδιάμεσα στους Black και White Hats υπάρχουν οι Gray Hats. Οι **Gray hat** χρησιμοποιούν τις γνώσεις τους στους υπολογιστές εθελοντικά με σκοπό τη διερεύνηση και την προσπάθεια να τιμωρήσουν τους εγκληματίες του κυβερνοχώρου. Επίσης, χαρακτηρίστηκαν και ως «hacktιβιστές (hacktivists)», δηλαδή άτομα που χρησιμοποιούν τους υπολογιστές για μεταφορά πολιτικών μηνυμάτων.

White Hats

Οι hackers όμως δεν είναι όλοι κακόβουλοι καθώς υπάρχουν και άνθρωποι που εισβάλλουν σε κάποιο σύστημα για να βρούν τα τρωτά σημεία. Οι hackers αυτοί είναι γνωστοί ως **White hats**. Οι white hats είναι hackers που χρησιμοποιούν τις δεξιότητές τους με ηθικό σκοπό. Συνήθως είναι οι υπάλληλοι εταιρειών, οι οποίοι έχουν ειδική άδεια να επιτίθενται στα δίκτυα και τα συστήματα της ίδιας τους της εταιρείας για την ανακάλυψη αδύναμων σημείων στο σύστημα ασφάλειας της. Επίσης white hats, είναι και οι πράκτορες μυστικών υπηρεσιών που χρησιμοποιούν τις ικανότητές τους για τη διερεύνηση και την επίλυση εγκλημάτων καθώς για την εξυπηρέτηση του κράτους. Χρησιμοποιούν τις γνώσεις τους με τέτοιο τρόπο, ώστε να επωφεληθούν άλλοι άνθρωποι ή υπηρεσίες. Οι White Hats πιστεύουν:

Α) Οι πληροφορίες πρέπει να είναι ελεύθερες στον καθένα.

Β) Έχουν έλλειψη εμπιστοσύνης στην εξουσία-προώθηση αποκέντρωσης.

Γ) Οι hackers πρέπει να κρίνονται με βάσει την ικανότητά τους και όχι με κριτήρια όπως πτυχία, ηλικία, φυλή κλπ.

Δ) Μπορεί να δημιουργηθεί τέχνη και ομορφία στον υπολογιστή.

Ε) Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο.

Οι White hackers έχοντας αυτά τα ιδανικά αποτελούν ένα πυρήνα ατόμων, τα οποία εναντιώνονται στις σύγχρονες τάσεις που θέλουν τη διαχείριση των πληροφοριών αποκλειστικά από το σύστημα και την επιβολή περιορισμών στην κυκλοφορία τους από τους απλούς πολίτες. Πολλοί hackers επιδιώκουν την αναγνώριση σαν ένα αξιέπαινο πολιτισμικό αρχέτυπο. Τα κίνητρα των hackers αυτών είναι η έμφυτη ανάγκη των ατόμων αυτών για γνώση. Επιδιώκουν πρόσβαση σε δεδομένα και δίκτυα για να μάθουν.

Στόχος τους επίσης, όπως λένε και οι ίδιοι, είναι η ανακάλυψη των αδυναμιών σε δίκτυα και υπολογιστικά προγράμματα, έτσι ώστε να εξασφαλισθεί η κατά το δυνατότερον ασφαλέστερη πλοήγηση στο διαδίκτυο μέσω της βελτίωσης προγραμμάτων άμυνας των υπολογιστών και τη διόρθωση λαθών σε λειτουργικά συστήματα.Αυτό φαίνεται ξεκάθαρα στη διακύρηξη του Nomad Mobile Research Centre,ένα δίκτυο hacker που εργάζεται για την ασφάλεια των υπολογιστών,δηλαδή την αντιστροφή της εφαρμοσμένης μηχανικής: «Στόχος μας είναι να υποχρεώσουμε τις εμπορικές εταιρίες λογισμικού να διορθώνουν τα προϊόντα τους και να προσφέρουμε εναλλακτικές επιλογές. Όλα τα hacks/cracks γίνονται με σκοπό να προβληθεί η ιδέα οτι δεν μπορείς να εξασφαλίσεις ένα σύστημα για πολύ χρόνο.».

Γι' αυτούς το hacking εκτός από μία πρόκληση συχνά αποτελεί και το αγαπημένο τους παιχνίδι. Όπως δηλώνει και ο Κέβιν Μίτνικ, ένας από τους θρυλικότερους hackers: «Βρίσκοντας διάφορους τρόπους να παραβιάζω τα συστήματα ασφαλείας απλώς περνούσα καλά,είχε πλάκα.». Το εικονικό περιβάλλον προσφέρει μία αίσθηση ασφαλείας, καθώς ο νεαρός κατορθώνει από την ασφάλεια του δωματίου του σαν super ήρωας να υπερπηδήσει τα εμπόδια αρκετά πιό μορφωμένων και μεγαλυτέρων σε ηλικία προγραμματιστών και να τους εμπαίξει.

Η κοινωνία των hacker είναι κυριαρχούμενη από έφηβους και κυρίως αγόρια και γι' αυτό έχει μία ανδροκρατούμενη κουλτούρα. Μολονότι οι γυναίκες είναι σήμερα μία ανερχόμενη δύναμη στο χώρο, αντιμετωπίζουν ακόμη προκατάληψη.

Black Hats/Crackers

Πολλοί hackers σήμερα είναι κακοήθεις και άπληστοι. Ταλαντούχοι και ικανοί συχνά βρίσκουν δουλειά στη Μαφία, τα κολομβιανά καρτέλ ναρκωτικών, τα τρομοκρατικά δίκτυα και γενικά το οργανωμένο έγκλημα.

Τα κίνητρα των crackers αυτών είναι ευτελή, επηρεασμένα από το πάθος για χρήμα και δύναμη μέχρι το βανδαλισμό και την καταστροφή συστημάτων είναι η αυτοπροβολή και η αίσθηση εξουσιασμού των λιγότερο καταρτισμένων και των αδαών. Είναι άτομα τα οποία διαθέτουν χαλαρούς ηθικούς φραγμούς λόγω ελλιπούς παιδείας καθώς, όπως υποστηρίζει και ο Larry Martin, οι γονείς, ο τύπος και οι καθηγητές δεν αντιλαμβάνονται την υποχρέωσή τους να συμβάλουν στην ανάπτυξη ηθικών αρχών σχετικά με τους υπολογιστές. Είναι τεχνολογικά αναλφάβητοι και συνεπώς οι πολιτισμικές νόρμες υστερούν ως προς τις εξελίξεις της τεχνολογίας και τις εξαρτήσεις της κοινωνικής ζωής από αυτές. Ο Bloombecker δηλώνει σχετικά: «Ατυχώς, τόσο για την κοινωνία όσο και γι' αυτούς που χρειάζονται καθοδήγηση δεν υπάρχει κάποιο δεδομένο καθεστώς στην κοινότητα των ηλεκτρονικών υπολογιστών που να ορίζει πότε ακριβώς το παιχνίδι έχει βγεί εκτός ελέγχου...». Σημαντικό ρόλο στην ηθική ανεπάρκεια που εμφανίζουν οι νέοι hackers είναι κατά τον Brian Harvey το νεαρό της ηλικίας τους που δεν τους επιτρέπει μία ανεπτυγμένη αίσθηση ηθικής, ώστε να έχουν πλήρη αντίληψη για το πότε οι ενέργειές τους είναι βλαπτικές για τους συνανθρώπους τους. Αλλά και μέσα από τα μάτια ενός hacker, του Chris Goggans, μέλος μίας ομάδας που στιγμάτισε τη δεκαετία του 90' με τη δράση της, τους Legion Of Doom, βλέπουμε οτι η νέα γενιά δεν του εμπνέει εμπιστοσύνη. Αναφέρει οτι με τον καιρό τα άτομα έγιναν πιό αντικοινωνικά και καθώς πέρναγαν τα χρόνια χάθηκε αυτο το αίσθημα συναδελφικότητας που επικρατούσε στους κύκλους των hackers. Οι άνθρωποι άρχισαν να μαζεύουν μανιωδώς πληροφορίες για τον εαυτό τους και να καταδίδουν για εκδίκηση.Το hacking έπαψε να είναι πιά διασκεδαστικό.Έγινε μια διαδικασία πρωτόγονη και διψασμένη για δύναμη σε ατομικό επιπεδο. Αυτό έχει τις ρίζες του και στην αθρόα αύξηση των επίδοξων hacker που αλλοίωσαν το αίσθημα κοινότητας μεταξύ των παλαιών και λόγω πλήθους έχασε σε νόημα και η διανομή δεδομένων και πληροφοριών αλλά και η εκπαίδευση νέων από τους παλαιοτέρους.

Πρόβλημα επίσης αποτελεί κατά τον Spafford η αντίληψη του υπολογιστή ως μηχάνημα με λειτουργία αδιάφορη με την κοινωνική

και καθημερινή λειτουργία των ανθρώπων και τις αξίες τους. Η θέαση του ως κάτι αριθμητικο το απογυμνώνει από κάθε ηθικό προβληματισμό καθώς αποτυγχάνουμε να κατανοήσουμε οτι οι υπολογιστές είναι εργαλεία τα παράγωγα των οποίων αφορούν και επηρεάζουν τους ανθρώπους.

Τα τελευταία δεδομένα συντελούν στη διαμόρφωση μίας εικόνας για το ηθικό υπόβαθρο ή μάλλον την ανυπαρξία ενός τέτοιου όσον αφορά στους crackers, ώστε να δικαιολογηθεί η πορεία που καταλήγουν να ακολουθούν.Στη συνέχεια θα εξετάσουμε τις αιτίες της εγκληματοποίησης του κοινωνικού αυτού φαινομένου αλλά και θα καταγράψουμε τις τάσεις της κοινής γνώμης απέναντι του.

Gray Hats

Στο ενδιάμεσο των white hats και black hats βρίσκονται οι gray hats. **Gray hat hackers** αποτελούνται από εθελοντές hacker, δηλαδή, τα άτομα αυτά που χρησιμοποιούν τους υπολογιστές για τη διερεύνηση και την προσπάθεια να τιμωρήσουν τους υποτιθέμενους εγκληματίες του κυβερνοχώρου. Επίσης, χαρακτηρίστηκαν και ως «hacktivists», δηλαδή τα άτομα που χρησιμοποιούν τους υπολογιστές και το διαδίκτυο για να μεταφέρουν πολιτικά μηνύματα.

Ακτιβισμός είναι η αντίδραση σε μία κατεστημένη αρνητική κατάσταση με ενέργειες όπως πορείες, καθιστικές διαμαρτυρίες, καταλήψεις. Η Τζ. Μαρκέτου υποστηρίζει και ο χακτιβισμός είναι ένα τέτοιο είδος πολιτικού ακτιβισμού, ένα σύνολο προτάσεων για αντίσταση και κριτικό διάλογο. Συνεπώς, ο χακτιβισμός αποτελεί μία μεταφορά του ακτιβισμού της πραγματικής ζωής σε ένα εικονικό επίπεδο έκφρασης, το διαδίκτυο, και υποδεικνύει πώς ο άνθρωπος μαθαίνει να χειρίζεται ψηφιακά πλέον τις δυνατότητες που του προσφέρονται και πώς μαθαίνει να σκέφτεται και να λειτουργεί στα πλαίσια της περιρρέουσας ηλεκτρονικής κουλτούρας.

Ο χακτιβισμός δεν είναι μία τυπική αντίδραση μόνο αλλά έχει μετατραπεί σε μία μορφή καλλιτεχνικής έκφρασης με πολιτικά και κοινωνικά μηνύματα. Όπως δηλώνει και η Τζ. Μαρκέτου, πολλοί καλλιτέχνες πιστεύουν οτι δημιουργικότητα δεν είναι να δημιουργείς κάτι καινούριο μόνο, αλλά να χρησιμοποιείς ό,τι ήδη υπάρχει. Ο χακτιβιστής διαδικτυακός καλλιτέχνης αντί να παράγει

φυσικά αντικείμενα,οργανώνει και αποδομεί το σύστημα με σκοπό την αφύπνιση του χρήστη. Στα πλαίσια της ελευθερίας δεδομένων στο NET, η τέχνη δε νοείται να είναι διαθέσιμη επί πληρωμή.

Old School Hackers

Οι old school hackers είναι δημιουργούν προγραμμάτα για την ανάλυση/σχεδιασμό συστημάτων. Δεν έχουν κακές προθέσεις και σέβονται σημαντικά το απόρρητο των πληροφοριών. Είναι της "παλιάς σχολής" όπως αναφέρει το όνομά τους και βασίζονται στις μεθόδους και τρόπους των πρώτων hackers.

Script Kiddies ή Cyber Punks

Ως script kiddies χαρακτηρίζονται άνθρωποι, με ελάχιστες έως και μηδαμινές γνώσεις περί προγραμματισμού και πληροφοριακών συστημάτων που χρησιμοποιούν έτοιμα εργαλεία hacking που βρίσκουν στο internet. Συνήθως τα χρησιμοποιούν για κακούς σκοπούς και δεν ενδιαφέρονται για τον τρόπο κατασκευής τους. Οι Cyber punks είναι αυτοί που υπερηφανεύονται για τις γνώσεις και τις πράξεις τους, συνήθως χρησιμοποιώντας λογισμικά άλλων. Στόχος τους είναι η διασκέδαση τους και κάνουν απάτες με τηλεπικοινωνίες, παραμορφώνουν ιστοσελίδες, κλέβουν στοιχεία από πιστωτικές κάρτες και στέλνουν ανεπιθύμητα μηνύματα (spamming).

Professional Criminals ή Crackers

Αυτοί ανήκουν στους εγκληματίες που έχουν στόχο το χρήμα και την καταστροφή πληροφοριακών συστημάτων. Πολλές φορές λειτουργούν και ως κατάσκοποι σε στρατιωτικό και βιομηχανικό τομέ ή και σε τρομοκρατικές ομάδες.

Coders ή Virus Writers

Τα άτομα που ανήκουν σε αυτήν την κατηγορία έχουν άριστες γνώσεις προγραμματισμού και κατασκευάζουν επιβλαβές λογισμικό για τον υπολογιστή. Τις περισσότερες φορές δεν τα χρησιμοποιούν οι ίδιοι αλλά τα προμηθεύουν σε τρίτους.

2.4 Είδη Ψηφιακών Εγκληματιών (Hacker)

Η πρώτη γενιά hackers αποτελείται από μέλη πανεπιστημιακών ομάδων των τεχνολογικών πανεπιστημίων MIT και Stanford. Αυτοί οι επιστήμονες ζούσαν εργαζόμενοι στα εργαστήριά τους και ανέπτυξαν τις πρώτες μεθόδους προγραμματισμού την περίοδο 1950-1960 για την Αμερικανική κυβέρνηση.

Η δεύτερη γενιά αποτελείται από εμπορικά προσανατολισμένους επιστήμονες που ως σκοπό είχαν την ευρεία διάδοση της πληροφορικής τεχνολογίας στις μάζες. Ηταν αυτοί που δημιούργησαν τους πρώτους υπολογιστές. Επιπλέον στόχος της νέας γενιάς αυτής ήταν η μελέτη και ο πειραματισμός για τη βελτίωση της αλληλεπίδρασης ανθρώπου με υπολογιστή, παραδειγματικό επίτευγμα της οποίας ήταν το γνωστό και απαραίτητο σήμερα «ποντίκι».

Η τρίτη γενιά αποτελείται από τους προγραμματιστές που δημιούργησαν τις βασικές δομές στις οποίες στηρίχθηκε η δημιουργία των ηλεκτρονικών παιχνιδιών. Η γενιά αυτή αντιλαμβάνεται πλήρως τις οικονομικές δυνατότητες του συγκεκριμένου τομέα και εργάζεται σκληρά για να ανταποκριθεί στη ζήτηση που δημιουργείτε από την χρήση προσωπικού ηλεκτρονικού υπολογιστή αλλά και τη δημιουργία νέων αναγκών.

Η τέταρτη γενιά είναι αυτή που συγκρότησε την hacker κοινότητα. Στις προηγούμενες γενιές υπήρχε μια προσήλωση στην επίτευξη μίας εκλαίκευσης του νέου μέσου και κυρίως μία χρήση αυτού βασισμένη σε ανάγκες και δεδομένα της καθημερινότητας, η νέα αυτή γενιά εμφάνισε μια αναρχική τάση όχι σύνθεσης νέων δεδομένων και προγραμμάτων, αλλά αντίθετα μία αποδομητική και μια ενδοσκοπική εξερευνητική ενέργεια, που εξελίχθηκε στη σημερινή μορφή hacking.

Η γενιά αυτή αποδέχεται γενικά τις ηθικές αρχές αλλά παράλληλα αποτελεί ένα σύνολο που έχει γεννηθεί και κοινωνικοποιηθεί σε ένα υπάρχον πληροφορικό περιβάλλον, το οποίο αποτελείται από άτομα που ζούν σε διαφορετικά μήκη και πλάτη του κόσμου και έχουν αναπόφευκτα ποικίλες ιδιοσυγκρασίες και ήθη. Η εκρηκτική εξέλιξη του διαδικτύου δημιούργησε ένα νέο κοινωνικό μόρφωμα, όπου αναπόφευκτα διάφορες συμπεριφορές αποκτούν μία νέα σημασία, όταν πραγματώνονται εκτός εργαστηρίων και επηρεάζουν την ανθρώπινη καθημερινότητα πλέον.

Βιβλιογραφία

Ορισμός των Hackers:
https://sites.google.com/site/projecths12/hacking

WhiteHats, Black Hats, Grey Hats:
http://webcache.googleusercontent.com/search?q=cache:http://www.theartofcrime.gr/artofcrime/assets/hackers.doc&gws_rd=cr&ei=_8E4V4KECurO6ATR3ZfoAw

Oldschool Hackers, Script Kiddies/Cyber Punks, Professional Criminals/Crackers
https://sites.google.com/site/projecths12/hacking/kategories

Είδη Ψηφιακών Εγκλημάτιών:
http://webcache.googleusercontent.com/search?q=cache:http://www.theartofcrime.gr/artofcrime/assets/hackers.doc&gws_rd=cr&ei=_8E4V4KECurO6ATR3ZfoAw

ΚΕΦΑΛΙΟ 3

Μεθοδολογία επιθέσεων και σκοπός Ψηφιακών Εγκληματιών

Η μεθοδολογία των ψηφιακών επιθέσεων καθορίζεται από το σκοπό τους. Συγκεκριμένα, οι ψηφιακοί εγκληματίες χρησιμοποιούν τα πιο κατάλληλα μέσα για να επιτύχουν το σκοπό τους. Ένας hacker για να εισβάλλει σε ένα πληροφοριακό σύστημα, πρέπει αρχικά να συλλέξει πληροφορίες γύρω από αυτό. Η συγκέντρωση αυτών των στοιχείων είναι γνωστή ως information gathering και διευκολύνει το έργο του τόσο όσον αφορά την είσοδο του στο σύστημα όσο και την απόκρυψη της ταυτότητάς του. Ο hacker έχει εξασκηθεί για να μπορεί με ευκολία να συλλέγει τις κατάλληλες πληροφορίες που του είναι απαραίτητες όπως διευθύνσεις, πληροφορίες για τους διαχειριστές του συστήματος, κλπ. Για την είσοδο του hacker στο σύστημα, πραγματοποιούνται διάφορες μέθοδοι επιθέσεων οι οποίες στοχεύουν στην εκμετάλλευση των πιθανών σημείων ευπάθειάς του. Μέθοδοι που χρησιμοποιούν είναι:

3.1 Παράνομη πρόσβαση σε Η/Υ.

Η δραστηριότητα αυτή είναι γνωστή σε όλους σαν **Hacking.** Η συγκεκριμένη εγκληματική συμπεριφορά αφορά μόνο την

παράνομη πρόσβαση σε λειτουργικά συστήματα υπολογιστών. Η τέλεσή της γίνεται με την παραβίαση των μέτρων ασφαλείας που είχε λάβει ο ιδιοκτήτης τους και ανεξάρτητα από τους λόγους για τους οποίους την επιχειρεί ο δράστης. Τα θύματα στόχοι μπορεί να είναι από καθημερινούς πολίτες μέχρι επιχειρήσεις ή οργανισμούς.

3.2 Κλοπή, παραποίηση ή καταστροφή αρχείων Η/Υ

Ένας ψηφιακός εγκληματίας που εισχωρεί σε ένα σύστημα υπολογιστών έχει τη δυνατότητα να κλέψει, να τροποποιήσει και πολλές φορές να καταστρέψει αρχεία ή και προγράμματα που υπάρχουν στο σύστημα. Αν κάποιος επιτεθεί σε μια εταιρία η ζημιά που μπορεί να προκληθεί είναι τεράστια. Τα στοιχεία μισθοδοσίας των υπαλλήλων, μελλοντικά πλάνα και σχέδια, ακόμα και στοιχεία πελατών διατρέχουν κίνδυνο καθώς η παραποίησή τους, κλοπή ή καταστροφή μπορεί να αποβεί μοιραία όχι μόνο για την ίδια την εταιρία αλλά και για όσους συναναστρέφονται μαζί της.

3.3 Αρνηση παροχής υπηρεσιών (Denial of service attack-DoS)

Denial of Service (DoS) και Distributed Denial of Service (DDoS), είναι μέθοδοι επιθέσεων που κάνουν μια διαδικτυακή υπηρεσία ή έναν server να υπολειτουργεί, δηλαδή να αδυνατεί να εξυπηρετήσει τις απαιτήσεις του εκάστοτε χρήστη. Μια DoS επίθεση λειτουργεί ως εξής: Ένας ή και περισσότεροι υπολογιστές αποστέλλουν ένα μεγάλο πλήθος δεδομένων στο αντίστοιχο Server ή Ιστοσελίδα με αποτέλεσμα να υπερφορτώσει ή να προκαλέσει επανεκκίνηση. Με λίγα λόγια προσπαθεί να "γεμίσει" τη μνήμη του συστήματος με απαιτήσεις (requests) τις οποίες το σύστημα δεν μπορεί να διαχειριστεί/εκτελέσει. Σε μία DdoS επίθεση, ο hacker, προσπαθεί να αποκτήσει πρόσβαση σε πολλούς υπολογιστές και να

πάρει τον έλεγχο τους. Σαν επακόλουθο της επιτυχίας του, χρησιμοποιεί αυτούς να εκτελέσει μια επίθεση DoS στο επιθυμητό στόχο.

3.4 Διασπορά κακόβουλων λογισμικών/προγραμμάτων (malware)

Οι **ιοί (viruses)** και τα Σκουλήκια (Worms) είναι προγράμματα Η/Υ που έχει δημιουργηθεί με σκοπό τη μόλυνση προγραμμάτων και αρχείων. Δύο πολύ γνωστοί ιοί είναι Packet Sniffer και Trojan Horse.

Συγκεκριμένα, τα **Σκουλήκια (Worms) και** οι **Ιοί (Viruses)**, είναι κακόβουλα προγράμματα διαφορετικά μεταξύ τους και από τους Δούρειους Ίππους. Παρ' όλα αυτά, πολλοί αναφέρονται σε αυτά συνήθως με τον όρο "ιός". Τα σκουλήκια εξαπλώνονται από υπολογιστή σε υπολογιστή χωρίς να απαιτείται ανθρώπινη ενέργεια, λαμβάνοντας πληροφορίες για τον τρόπο μεταφοράς των αρχείων. Όταν ένα σκουλήκι εισβάλει σε ένα δίκτυο, αρχίζει να πολλαπλασιάζονται αντιγράφοντας τον εαυτό του συνεχώς, χρησιμοποιώντας μεγάλο μέρος του σύστημα και σαν αποτέλεσμα αυτό καταρρέει. Το διάσημο σκουλήκι Blaster Worm μπορούσε να εισχωρήσει στο σύστημα και να λειτουργεί ως backdoor λογισμικό.

Ένας ιός (virus) "κολλάει" σε ένα αρχείο ή πρόγραμμα, συνήθως με επέκταση *.exe. Επίσης, έχει τη δυνατότητα να μεταφέρεται από σύστημα σε σύστημα, αφήνοντας "μολυσμένα αρχεία" πίσω του. Σε αντίθεση με τα σκουλήκια (worms), ο ιός είναι εξαρτώμενος από ανθρώπινη ενέργεια, για παράδειγμα, ένας ιός μπορεί να υπάρχει σε ένα σύστημα αδρανής μέχρι ο χρήστης να του δώσει εντολή. Έτσι οι χρήστες, ανυποψίαστοι, εξαπλώνουν τον ιό.

Ο **Packet Sniffer**, ή αλλιώς **Packet Analyzer**, είναι λογισμικό που χρησιμοποιείται για να υποκλέψει πληροφορίες από τα πακέτα δεδομένων που εισάγει και εξάγει ένα δίκτυο υπολογιστών. Τα packet sniffers παρακολουθούν την κίνηση των πακέτων πληροφοριών, παίρνουν από το καθένα από αυτά πληροφορίες και τέλος, αν χρειάζεται, αποκρυπτογραφούν τα δεδομένα τους δίνοντας τις πληροφορίες στον hacker.

Ο Δούρειος Ίππος (Trojan Horse), είναι λογισμικό που έχει τη δυνατότητα να κρύβεται μέσα σε κάποιο άλλο καλόβουλο λογισμικό ώστε να γίνεται πολύ δύσκολα αντιληπτό από το σύστημα ασφαλείας. Έτσι, όταν ο ανυποψίαστος χρήστης του συστήματος χρησιμοποιήσει το πρόγραμμα ξεκινά χωρίς να το ξέρει να παρέχει πληροφορίες στον Hacker, όπως για παράδειγμα usernames, passwords, e-mais, κλπ. Ο διασημότερος δούρειος ίππος είναι ο Black Orifice. Δημιουργήθηκε από την hacking team Cult of the Dead Cow και μπορεί να προσφέρει πρόσβαση και έλεγχο σε κάθε προσωπικό υπολογιστή που λειτουργεί με Windows 95/98 και επόμενα, εκμεταλλευόμενο μία ευπάθεια σε ένα πρόγραμμα για αποστολή e-mail. Ο όρος προέρχεται από την ομώνυμη κατασκευή που χρησιμοποιήθηκε στην ελληνική μυθολογία.

Χρ. Ε. Τσουραμάνης & Μαρ. Ευγ. Καρολή (2010) Οικονομία και Εγκληματικότητα

3.5 Spam – Phishing

Spam είναι ο όρος που χρησιμοποιούμε για να περιγράψουμε τη μαζική αποστολή μηνυμάτων, συνήθως διαφημιστικών. Οι spammers είναι συνήθως εύκολο να ανακαλυφθούν λόγο του ότι παίρνουν τις διευθύνσεις από τους καταλόγους εταιρειών με ηλεκτρονικά

καταστήματα ή χρησιμοποιούν λογισμικά είδους harvester (σαρώνει το διαδίκτυο και συλλέγει διευθύνσεις).
Το phishing είναι μια νέα μέθοδος ψηφιακού εγκλήματος, που σκοπεύει στην εξαπάτηση των καταναλωτών και συγκεκριμένα την οικονομική απολαβή ή την υποκλοπή πληροφοριών. Σε συνεργασία με spammers, οι phishers εμφανίζονται ως εκπρόσωποι εταιρειών αποσπόντας από τα θύματά αριθμούς λογαριασμών, κωδικούς πιστωτικών καρτών κ.λ.π. Η μέθοδος αυτή πήρε το όνομα της το 1996 από hackers που έκλεβαν πληροφορίες και χρήματα με αυτή τη μέθοδο. Η πρώτη αναφορά για το phishing έγινε στο newsgroup hackers γνωστό ως alt.2600 τον Ιανουάριο του 1996 και η πρώτη αναφορά στα μέσων ενημέρωσης το Μάρτιο του 1997.

(http://ikee.lib.auth.gr/record/115622/files/ptuxiaki.pdf)

3.6 Παιδική Πορνογραφία

Η παιδική πορνογραφία τα τελευταία χρόνια έχει αυξηθεί σημαντικά. Σύμφωνα με ειδικούς η αύξηση αυτή οφείλεται σε ψυχολογικούς και κοινωνικούς παράγοντες κυρίως. Σημαντικό να αναφερθεί είναι ότι η παιδική πορνογραφία έχει τεράστιο τζίρο για τους ασχολούμενους με αυτή που φτάνει τα 3 δισ.εκ. ευρώ το χρόνο σε παγκόσμια κλίμακα.

Η πορνογραφία είναι καταπάτηση της ανθρώπινης αξιοπρέπειας. Αυτό που συγκλονίζει περισσότερο είναι ότι οι δράστες σε ανακρίσεις και μαρτυρίες που έχουν δώσει είναι ότι υποστηρίζουν ότι πέρα από τα χρήματα το κάνουν και για την <αδυναμία> τους προς στα νεαρής ηλικίας παιδικά κορμιά. Γενικά, παιδική πορνογραφία θεωρείται οποιαδήποτε αντιπροσώπευση ενός παιδιού σε σεξουαλικές δραστηριότητες.

Χρ. Ε. Τσουραμάνης & Μαρ. Ευγ. Καρολή (2010) Οικονομία και Εγκληματικότητα

3.7 Παράνομη διακίνηση προγραμμάτων

Η παράνομη ενέργεια αυτή η οποία ουσιαστικά συνιστά κλοπή λογισμικού γίνεται από τους ψηφιακούς δράστες με σκοπό να χρησιμοποιήσει το συγκεκριμένο πρόγραμμα μόνο ένας ή πολλοί που αργότερα πιθανόν να το πουλήσουν σε τρίτους. Το αντίστοιχο πρόγραμμα ο δράστης αποκτά μέσω (downloading) στο δικό του Η/Υ από το αντίστοιχο site που θα το προμηθευτεί.

Χρ. Ε. Τσουραμάνης & Μαρ. Ευγ. Καρολή (2010) Οικονομία και Εγκληματικότητα

3.8 Βιομηχανική, κρατική και πολιτική κατασκοπεία

Επιχειρήσεις, κυβερνήσεις και πολιτικές οργανώσεις, προσπαθούν να ανακαλύψουν εκ των προτέρων τις κινήσεις των ανταγωνιστών/αντιπάλων τους. Η χρήση νέων τεχνολογιών τους προσφέρει διευκόλυνση στην ανακάλυψη αυτών των πληροφοριών. Πολλές επιχειρήσεις επιδιώκουν να αποκτήσουν πληροφορίες για τρόπο προϊόντων των ανταγωνιστών τους και συμβόλαια που έχουν υπογράψει με τρίτους και πολλές φορές ψάχνουν τις στρατηγικές marketing που χρησιμοποιούν οι άλλες εταιρίες για δικό τους όφελος.

Χρ. Ε. Τσουραμάνης & Μαρ. Ευγ. Καρολή (2010) Οικονομία και Εγκληματικότητα

ΚΕΦΑΛΑΙΟ 4

Μέτρα αντιμετώπισης κατά του Hacking

Η αντιμετώπιση των ψηφιακών εγκλημάτιών γίνεται με τη λήψη μέτρων που βασίζονται στην ψηφιακή τεχνολογία. Συγκεκριμένα, μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς λογαριασμούς είναι συχνότατοι και άλλες μορφές ψηφιακών εγκλημάτων είναι συχνές και παραμονεύουν σε κάθε γωνία.

4.1 Αντιμετώπιση εισβολής με ψηφιακή τεχνολογία

Για την προστασία ενός υπολογιστικού συστήματος από κακόβουλο λογισμικό είναι απαραίτητη η εγκατάσταση προγραμμάτων **antivirus**. Τα antivirus προστατεύουν το σύστημα μας όχι μόνο από τους ιούς που περιέχονται στη βάση δεδομένων

του, αλλά και καινούργιους που τυχόν εμφανιστούν καθώς πολλά έχουν μηχανισμούς αναβάθμισης της βάσης δεδομένων τους, ενσωματωμένους. Επίσης, ελέγχουν αρχεία και μηνύματα ηλεκτρονικής αλληλογραφίας του χρήστη, ώστε να εντοπίζουν τυχόν ιό πριν αυτός μολύνει το υπολογιστικό σύστημα. Γι' αυτό, τα προγράμματα τέτοιας λειτουργίας είναι καλό να παραμένουν ανοιχτά συνέχεια.

Η **ενημέρωση του λειτουργικού συστήματος** με τα τελευταία patches, services packs κ.τ.λ. (π.χ. Windows Update) είναι απαραίτητη ώστε να διασφαλίζεται η ομαλή λειτουργία του και η βελτίωση της προστασία του υπολογιστή. Επίσης για την προστασία ενός υπολογιστικού συστήματος χρειάζεται συχνή εγκατάσταση των τελευταίων ενημερώσεων του web browser καθώς πρέπει να αφαιρεθούν η δυνατότητα αποθήκευσης των cookies, να ενεργοποιηθεί η εμπλοκή αναδυόμενων παραθύρων, να γίνεται συχνή εκκαθάριση του ιστορικού και των προσωρινών αρχείων του browser και να απενεργοποιηθούν τα πρόσθετα (Add-On και Plugins) που δεν χρησιμοποιούνται.

Εγκατάσταση **firewalls (τείχη προστασίας)** για την αποτροπή Spam αν και η προστασία τους είναι σχετική λόγο έλλειψης τροποποίησης ρυθμίσεων.

4.2 Ελληνική Νομοθεσία και οι αδυναμίες της

Η ελληνική νομοθεσία καλύπτει τα ψηφιακά εγκλήματα στο βαθμό που εντάσσονται στα άρθρα (370Β, 370Γ, 386Α) του Ν. 1805/88.

Στην ελληνική νομοθεσία δεν υπάρχουν νόμοι που να αναφέρονται αποκλειστικά σε θέματα Διαδικτύου. Γι' αυτό το λόγο η Ελλάδα σε συνεργασία με άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, προσπαθεί να καλύψει τα κενά στην αδυναμία της.

Ο ανωτέρω νόμος και οι διεθνείς συνεργασίες πολλές φορές δεν επαρκούν για την κάλυψη όλων των περιπτώσεων. Το βέβαιον είναι ότι, τα κράτη προσπαθούν να αντιμετωπίσουν αυτό το θέμα με τον καλύτερο δυνατό τρόπο.

Όπως αναφέρει ο **Προϊστάμενος του Τμήματος Ηλεκτρονικού Εγκλήματος της Δ/νσης Ασφάλειας Αττικής, Αστυνόμος Α΄ κ. Εμμανουήλ Σφακιανάκης,** οι αδυναμίες δεν υπάρχουν μόνο στην Ελλάδα αλλά και σε όλες τις χώρες λόγο της ταχύτατης εξέλιξης του ψηφιακού εγκλήματος δημιουργώντας προβλήματα στην οριοθέτηση των πράξεων που πρέπει να διώκονται ποινικά. Οι συγγραφείς των νόμων χρειάζονται διαρκή ενημέρωση για τις εξελίξεις του διαδικτύου και άμεση ανταπόκριση στα νέα δεδομένα.

Η νομοθεσία στην Ελλάδα έχει ως εξής:

1. Άρθρο 370Β

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον 3 μηνών. Ως απόρρητα θεωρούνται κι εκείνα που ο νόμιμος κάτοχός τους από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.
2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.
3. Αν πρόκειται για στρατιωτικό ή διαπλαστικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παρ. 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.
4. Οι πράξεις που προβλέπονται στις παρ.1 και 2 διώκονται ύστερα από έγκληση.

2. Άρθρο 370Γ

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ευρώ. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.
4. Οι πράξεις των παρ. 1 έως 3 διώκονται ύστερα από έγκληση.

3.Αρθρο 386Α
Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα.

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414

4.3 Αντιμετώπιση και Συμβουλές για παιδία, ενήλικους και γονείς.

Οι ψηφιακοί εγκληματίες είναι ένα κρίσιμο θέμα που απασχολεί τακτικά την αστυνομία καθώς τα εγκλήματα που έρχονται με αυτούς είναι πολλές φορές δύσκολο να εξιχνιαστούν.

Η αστυνομία καταβάλει μεγάλες προσπάθειες στην αντιμετώπιση των ψηφιακών εγκληματιών. Ο χρόνος για την ανακάλυψη των ψηφιακών εγκληματιών που καταβάλλεται είναι τεράστιος από ένα μήνα έως και δύο χρόνια καθώς αν ο αντίστοιχος εγκληματίας αντιληφθεί την καταδίωξή του αρχίζει να παίρνει απαραίτητα μέτρα προστασίας. Επίσης, το έγκλημα στον Κυβερνοχώρο είναι γρήγορο στη φύση του, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές είναι αργά για να γίνει κάτι.

Παρ' όλα αυτά, το ελληνικό κράτος δημιούργησε το τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος ως ένα από τα μέτρα για την αντιμετώπισή του.

Καθημερινά γίνονται καταγγελίες από πολίτες θύματα που παραβιάστηκαν προσωπικά τους δεδομένα ή αντιλήφθηκαν ύποπτες συμπεριφορές. Για την καλύτερη προστασία μας είναι καλό να γνωρίζουμε τους κινδύνους που διατρέχουμε όχι μόνο εμείς αλλά και τα παιδιά και οδηγίες για την αντιμετώπισή τους.

Κίνδυνοι για τα παιδιά

- Τα παιδιά μπορούν να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο.
- Τα παιδιά μπορούν να έρθουν σε επαφή με αγνώστους που μπορούν να τα βλάψουν.
- Τα παιδιά υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο Διαδίκτυο.
- Τα παιδιά μπορούν να εθιστούν στη χρήση του Διαδικτύου και έτσι κινδυνεύουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις, τα παιχνίδια τους με φίλους.

Συμβουλές για τα παιδιά

- Εξηγείτε στους γονείς σας τις εμπειρίες σας κατά την περιπλάνησή σας στο Διαδίκτυο.
- Πάντα να μιλάτε στους γονείς σας ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρήκατε στο Διαδίκτυο και σας ανησυχούν ή σας φοβίζουν.
- Διαφυλάσσετε τις προσωπικές σας πληροφορίες. Ποτέ μην δίνετε το όνομα σας, την διεύθυνση σας, την διεύθυνση και το όνομα του σχολείου σας, το τηλέφωνο σας, φωτογραφίες σας σε αγνώστους που συναντάτε στο Διαδίκτυο ακόμη και αν σας το ζητήσουν.
- Κρατάτε τον κωδικό εισόδου στον υπολογιστή σας μυστικό. Είναι σαν το κλειδί του σπιτιού σας που δεν θα το δανείζετε σε κανέναν.
- Μόνο με την άδεια και την παρουσία των γονιών σας μπορείτε να συμφωνήσετε να συναντήσετε κάποιον/κάποια που γνωρίσατε στο Διαδίκτυο.
- Προσέχετε όταν μιλάτε διαμέσου chatroom ή e-mail. Διακόψτε τη συνομιλία όταν κάποιοι σας κάνουν να νιώθετε άβολα.

•Μην εμπιστεύεστε ότι διαβάζετε στο Διαδίκτυο. Μάθετε να βλέπετε το περιεχόμενο με κριτικό μάτι.

Συμβουλές για τους γονείς

•Κρατήστε τον ηλεκτρονικό υπολογιστή σε χώρους όπως το σαλόνι και όχι σε υπνοδωμάτια. Ασχοληθείτε με τον τρόπο που δουλεύει το Διαδίκτυο και αφιερώστε χρόνο να περιηγηθείτε μαζί με τα παιδιά σας στον Κυβερνοχώρο και μάθετε από αυτά.

•Σιγουρευτείτε ότι τα παιδιά σας είναι ενήμερα, ότι πρέπει να ανησυχούν για αγνώστους που συναντούν μέσω του ηλεκτρονικού υπολογιστή. Όπως ακριβώς είμαστε ανήσυχοι όταν άγνωστοι χτυπάνε την πόρτα του σπιτιού μας, έτσι δεν πρέπει τα παιδιά να δίνουν προσωπικές πληροφορίες για τους εαυτούς τους.

•Να είστε ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα chatrooms (δωμάτια συνομιλίας), χωρίς την επίβλεψη σας. Μην αφήσετε τα παιδιά σας να συναντήσουν κάποιον που γνώρισαν μέσω του Διαδικτύου χωρίς να είστε και εσείς μαζί.

•Ενθαρρύνετε τα παιδιά σας να προτιμούν τις ιστοσελίδες που εσείς θέλετε και όχι αυτές που θεωρείτε ανάρμοστες.

•Εγκαταστήσετε στον υπολογιστή σας κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση σε συγκεκριμένες σελίδες του Διαδικτύου.

•Συζητήστε με τα παιδιά σας για την ασφάλεια του Διαδικτύου. Συζητώντας τους μελλοντικούς κινδύνους μέσω του Διαδικτύου με τα παιδιά χρειάζεται να δείξετε ευαισθησία και έγνοια έτσι ώστε να κατανοήσουν και τα ίδια τους κινδύνους.

•Γνωρίστε ποιους πρέπει να ενημερώσετε και εν ανάγκη να καταγγείλετε σε περίπτωση που συναντήσετε βλαβερό και παράνομο περιεχόμενο στο Διαδίκτυο.

http://www.astynomia.gr/index.phpoption=ozo_content&perform=view&id=1414

Κεφάλαιο 5

Διαγωνισμός για Hackers

Pwn2Own

Το Pwn2Own είναι ένας hacking διαγωνισμός υπολογιστών που διεξάγεται κάθε χρόνο στο CanSecWest συνέδριο για λόγους ασφάλειας και ξεκίνησε το 2007. Οι διαγωνιζόμενοι καλούνται να αξιοποιήσουν ευρέα λογισμικά και φορητές συσκευές με άγνωστες ευπάθειες. Οι νικητές του διαγωνισμού λαμβάνουν τη συσκευή στην οποία λειτούργησαν, ένα χρηματικό έπαθλο και ένα "Masters " σακάκι που απεικονίζει το έτος νίκη τους. Το όνομα « Pwn2Own » προέρχεται από το γεγονός ότι οι διαγωνιζόμενοι πρέπει να « Νικήσουν » ή να κάνουν hack στη συσκευή και όποιος τα καταφέρει την κερδίζει. Ο διαγωνισμός Pwn2Own χρησιμεύει στο να αποδείξει την τρωτότητα των συσκευών και λογισμικού που υπάρχουν σε ευρεία χρήση, ενώ παρέχει επίσης ένα σημείο ελέγχου σχετικά με την πρόοδο που έχει σημειωθεί στον τομέα της ασφάλειας από το προηγούμενο έτος.

Προέλευση: Ο πρώτος διαγωνισμός σχεδιάστηκε και έγινε από την Dragos Ruiu ως ένδειξη απογοήτευσης της προς την Apple λόγο της έλλειψης αναφοράς μηνιαίων σφαλμάτων και ιών, καθώς και στις τηλεοπτικές διαφημίσεις της Apple που προωθούσαν την ασφάλεια που παρείχε. Εκείνη την εποχή, υπήρχε μια ευρέως διαδεδομένη πεποίθηση ότι, παρά τις δημόσιες επιδείξεις των τρωτών σημείων στα προϊόντα της Apple, τα OS X ήταν πιο ασφαλή από όλους τους ανταγωνιστές του. Στις 20 Μαρτίου, περίπου τρεις εβδομάδες πριν διεξαχθεί ο διαγωνισμός στο CanSecWest εκείνο το έτος, η Ruiu ανακοίνωσε τη λίστα των συμμετέχοντων ερευνητών στο διαγωνισμό Pwn2Own. Ο διαγωνισμός περιλάμβανε δύο MacBook Pros που θα ήταν συνδεδεμένα σε δικό τους ασύρματο σημείο πρόσβασης. Κάθε συμμετέχοντας θα μπορούσε να συνδεθεί στο ασύρματο σημείο πρόσβασης και να εκμεταλλευτεί μία από τις συσκευές και αυτός που θα καταφέρει να κάνει hack στην αντίστοιχη συσκευή θα την αποκτούσε. Δεν υπήρχε καμία χρηματική ανταμοιβή. Η Ruiu καθιστούσε σαφές ποιοί περιορισμοί θα υπήρχαν όσον αφορούσε το hacking.

Την πρώτη ημέρα του συνεδρίου, η Ruiu ζήτησε από τον Terri Forslof της Zero Day Initiative (ZDI) να συμμετάσχουν στο διαγωνισμό. Η ZDI έχει ένα πρόγραμμα με το οποίο αγοράζει **zero-day** επιθέσεις, τα αναφέρει στον πωλητή και τα οποία χρησιμοποιεί για να βελτιώσει το δικό του σύστημα ανίχνευσης εισβολής σε δίκτυο, αυξάνοντας την αποτελεσματικότητά του. Τα τρωτά σημεία που πωλούνται στην ZDI, δημοσιοποιούνται αφού πρώτα ο πωλητής έχει εκδώσει νέο **patch** για αυτό. Η Forslof συμφώνησε η ZDI να προσεφερθεί να αγοράσει οποιαδήποτε τυχόν τρωτά σημεία βρεθούν στο διαγωνισμό για την τιμή των $ 10.000.

Διαγωνισμός 2007

Ο πρώτος διαγωνισμός είχε ως στόχο να αναδείξει την αδυναμία του λειτουργικού συστήματος Mac OS X της Apple, δεδομένου ότι, εκείνη την εποχή, υπήρχε μια ευρέως διαδεδομένη πεποίθηση ότι OS X ήταν πολύ πιο ασφαλές από τα ανταγωνιστικά προϊόντα. Ο διαγωνισμός πραγματοποιήθηκε από την Πέμπτη 18 του Απριλίου μέχρι το Σάββατο, 20 Απριλίου 2007.

Κανόνες

Δύο MacBook Pro φορητοί υπολογιστές, ένας 13 "και ένα 15", χρησιμοποιήθηκαν στο συνέδριο στο CanSecWest και συνδεδεμένα σε ένα ξεχωριστό ασύρματο δίκτυο. Μόνο ορισμένοι τύποι επιθέσεων επιτρέπονταν και αυτοί οι περιορισμοί σταδιακά χαλάρωσαν κατά στη διάρκεια τριών ημερών του συνεδρίου.

Ημέρα 1η: Μόνο απομακρυσμένες επιθέσεις. Οι διαγωνιζόμενοι πρέπει να εισβάλουν στο ασύρματο δίκτυο και να εκτελέσουν τις επιθέσεις τους, χωρίς να αλληλεπιδρούν.

Ημέρα 2η: συμπεριλήφθηκαν επιθέσεις σε Browser. Οι διαγωνιζόμενοι θα μπορούσαν να στείλουν ένα σύνδεσμο προς την ηλεκτρονική διεύθυνση του διαγωνισμού, το οποίο κάποιος από τους διοργανωτές θα έμπαινε από τον αντίστοιχο φορητό υπολογιστή του διαγωνισμού.

Ημέρα 3: Περιλαμβάνονται Τοπικές επιθέσεις. Οι διαγωνιζόμενοι θα μπορούν να εισάγουν ένα USB stick ή να προσπαθήσουν να συνδεθούν με τους φορητούς υπολογιστές του διαγωνισμού μέσω Bluetooth.

Για να κερδίσουν το 15 "MacBook Pro, οι διαγωνιζόμενοι θα πρέπει να προχωρήσουν σε περαιτέρω κλιμάκωση των προνομίων τους στον υπολογιστή μετά την απόκτηση πρόσβασης.

Αποτελέσματα

Μετά την ανακοίνωση $ 10.000 ως βραβείο από ZDI και οι φορητοί υπολογιστές δεν είχαν προσβληθεί από τους hackers από την πρώτη ημέρα, ο Shane Macaulay κάλεσε τον πρώην συνάδελφο του Dino Dai Zovi στη Νέα Υόρκη και τον προέτρεψε να διαγωνιστεί την δεύτερη ημέρα. Ξεκινώντας την Πέμπτη το βράδυ, ο Dai Zovi βρήκε και αξιοποίησε μια προηγουμένως άγνωστη ευπάθεια σε μια QuickTime Library που ήταν φορτωμένη στο Safari στις τρεις

εκείνο το βράδυ. Το επόμενο πρωί, ο Dai Zovi αποθήκευσε τον κώδικά του και τον έστειλε στο Macaulay στο συνέδριο στο Βανκούβερ. Η Macaulay ανέβασε τον κώδικα του Dai Zovi σε μια ιστοσελίδα και έστειλε e-mail στους διοργανωτές του διαγωνισμού με αυτό το σύνδεσμο. Όταν έκαναν κλικ από το φορητό υπολογιστή του διαγωνισμού, ο κώδικας του Dai Zovi επέτρεψε στον Shane να αποκτήσει τον έλεγχο του φορητού υπολογιστή, κερδίζοντας τον διαγωνισμό με αντιπρόσωπο τον Dai Zovi. Ως ένα ευχαριστώ για τη βοήθεια να κερδίσει το διαγωνισμό, Ο Dai Zovi επέτρεψε στον Macaulay να κρατήσει το 15 "MacBook Pro. Ο Dai Zovi πούλησε ξεχωριστά την ευπάθεια στην ZDI για το βραβείο $ 10.000.

Διαγωνισμός 2008 Μετά τον επιτυχία του διαγωνισμό το 2007 , ο διαγωνισμός Pwn2Own επεκτάθηκε συμπεριλαμβάνοντας ένα ευρύτερο φάσμα λειτουργικών συστημάτων και browsers. Ο διαγωνισμός θα έβγαζε στο φως τις αδυναμίες των λογισμικών που έχουν ευρεία χρήση από τους καταναλωτές. Η Dragos έκανε το διαγωνισμό καλύτερο με τη βοήθεια μιας ευρείας ομάδας εμπειρογνωμόνων της βιομηχανιών και ο διαγωνισμός χορηγήθηκε από την ZDI, οι οποίοι και πάλι θα προσφέρονταν να αγοράσουν τα τρωτά σημεία μετά επίδειξης τους. Όπως συμβαίνει με όλα τα τρωτά σημεία που αγοράζει η ZDI, οι λεπτομέρειες των τρωτών σημείων που χρησιμοποιούνται στο Pwn2Own θα πρέπει να παρέχονται στους ενδιαφερόμενους πωλητές και να δημοσιεύονται όταν ένα νέο patch δημιουργηθεί. Όλοι οι διαγωνιζόμενοι οι οποίοι με επιτυχία βρήκαν αδυναμίες στη διάρκεια του διαγωνισμού θα μπορούν να πουλήσουν αυτά τα τρωτά σημεία στη ZDI για τα βραβεία των $ 20.000 την πρώτη ημέρα, $ 10.000 τη δεύτερη ημέρα, και $ 5000 την τρίτη ημέρα. Ο διαγωνισμός Pwn2Own πραγματοποιήθηκε από την Πέμπτη, 26 Μαρτίου έως το Σάββατο, 28 του Μαρτίου 2008.

Κανόνες

Στο διαγωνισμό του 2008, υπήρχαν τρεις διαφορετικοί στόχοι φορητών υπολογιστών. Ο καθένας είχε την προεπιλεγμένη εγκατάσταση είτε σε Windows Vista Ultimate SP1, OS X 10.5.2 και Ubuntu Linux 7.10. Όπως και στο διαγωνισμό του προηγούμενου έτους, ο Pwn2Own διήρκησε τρεις ημέρες και μόνο ορισμένοι τύποι επιθέσεων επιτράπηκαν ανά ημέρα.

Ημέρα 1: Μόνο απομακρυσμένες επιθέσεις. Οι διαγωνιζόμενοι έπρεπε να ενταχθούν στο ίδιο δίκτυο με τον φορητό υπολογιστή-στόχο και να εκτελέσουν την επίθεση τους, χωρίς αλληλεπίδραση χρήστη και χωρίς έλεγχο ταυτότητας.

Ημέρα 2: Browser και επιθέσεις άμεσων μηνυμάτων συμπεριλήφθηκαν. Οι διαγωνιζόμενοι θα μπορούσαν να στείλουν ένα σύνδεσμο προς τη διεύθυνση e-mail του διαγωνισμού, το οποίο ο διοργανωτής θα έκανε κλικ σε κάποιον από τους φορητούς υπολογιστές του διαγωνισμού. Οι διοργανωτές θα έκαναν εγγραφή στο σύνδεσμο και θα λάμβαναν μηνύματα από τον αντίστοιχο διαγωνιζόμενο.

Ημέρα 3: Περιλαμβάνονται εφαρμογές client τρίτων. Οι διαγωνιζόμενοι θα μπορούσαν να στοχεύσουν δημοφιλή λογισμικό τρίτων, όπως το Adobe Reader και Flash, Sun Java, και Microsoft Silverlight.

Αποτελέσματα

Ο φορητός υπολογιστής που λειτουργούσε σε OS X προσβλήθηκε κατά τη δεύτερη ημέρα του διαγωνισμού λόγο εύρεσης αδυναμίας στον Safari. Η αδυναμία βρέθηκε από τους Charlie Miller, Jake Honoroff και Mark Daniel.

Οι αδυναμίες του φορητού υπολογιστή που εκτελούσε τα Windows Vista SP1 αποκαλύφθηκαν την τρίτη ημέρα του διαγωνισμού μέσω της εκμετάλλευσης του Adobe Flash που συγγράφτηκε από τον Shane Macaulay, τον Alexander Sotirov, και τον Derek Callaway. Μετά το διαγωνισμό, η Adobe αποκάλυψε ότι είχαν ανακαλύψει την ίδια ευπάθεια εσωτερικά και ετοιμαζόταν ένα patch κατά τη διάρκεια της Pwn2Own.

Ο φορητός υπολογιστής που είχε Ubuntu λογισμικό δεν αξιοποιήθηκε.

Διαγωνισμός 2012

Για το 2012 οι κανόνες άλλαξαν σε στυλ διαγωνισμού Capture the Flag. Η νέα μορφή έκανε τον Charlie Miller, ο οποίος ήταν επιτυχής τα δύο τελευταία χρόνια, να μην συμμετάσχει.

Στο Pwn2Own, ο Chrome προσβλήθηκε με επιτυχία για πρώτη φορά. Η VUPEN αρνήθηκε να αποκαλύψει τον τρόπο που ξέφυγε από το sandbox, λέγοντας ότι θα πουλήσει τις πληροφορίες. Ο Internet Explorer 9 για τα Windows 7 προσβλήθηκε με επιτυχία την επόμενη μέρα. Ο Firefox ήταν το τρίτο πρόγραμμα περιήγησης βρέθηκε ευπάθεια μέσω χρήσης του Zero Day Exploit.

Ο Safari για Mac OS X Lion ήταν το μόνο πρόγραμμα περιήγησης που στεκόταν έναντι στο Zero Day Exploit του Pwn2Own . Οι εκδόσεις του Safari που δεν ήταν πλήρως ενημερωμένο και έτρεχε σε Mac OS X Snow Leopard είχαν παραβιαστεί κατά τη διάρκεια του Pwn2Own. Θα πρέπει να σημειωθεί ότι σημαντικές βελτιώσεις ασφάλειας για τα Mac OS X υπήρξαν στο Lion.

Διαμάχη με τη Google

Η Google αποσύρθηκε από τη χορηγία της εκδήλωσης, διότι οι κανόνες του 2012 δεν απαιτούσαν την πλήρη αποκάλυψη της αδυναμίας από τους νικητές, ειδικά όταν αφορά την αποφυγή από ένα sandboxed περιβάλλον και πήραν μέτρα για τυχόν αδυναμίες. Ο Pwn2Own σεβάστηκε την απόφαση, λέγοντας ότι πίστευε ότι κανένας hacker δε θα επιχειρούσε να εισβάλει στον Chrome εάν οι μεθόδοι τους έπρεπε να αποκαλυφθούν. Η Google προσφέρε ένα ξεχωριστό " Pwnium " διαγωνισμό που προσέφερε μέχρι $ 60.000 για να βρεθούν αδυναμίες στον Chrome. Δραστηριότητες εκτός Chrome θα αναφέρονταν αμέσως στον αντίστοιχο κατασκευαστή. Ο Sergey Glazunov και ένας έφηβος που είναι γνωστοί ως « PinkiePie " κέρδισαν $ 60.000 για τα κατορθώματα τους και συγκεκρυμένα που παρέκαμψαν το sandbox ασφαλείας. Η Google εξέδωσε μια αποτύπωση για τους χρήστες του Chrome σε λιγότερο από 24 ώρες μετά τα κατορθώματα στο Pwnium.

Διαγωνισμός 2013

Η Google επέστρεψε ως χορηγός και οι κανόνες άλλαξαν ώστε να απαιτούν την πλήρη αποκάλυψη των αδυναμιών και τις τεχνικές που χρησιμοποιήθηκαν. Τα προγράμματα περιήγησης στο Web των Google Chrome, Internet Explorer και Firefox, μαζί με τα Windows 8 και Java, είχαν τις αδυναμίες στο φως.

Η γαλλική εταιρεία ασφαλείας VUPEN έχει εισβάλει με επιτυχία σε ένα πλήρως ενημερωμένο Internet Explorer 10 του Microsoft Pro Surface εκτελούμενο σε έκδοση 64-bit των Windows 8 και παρακάμφθηκε πλήρως. Η ομάδα VUPEN τότε προχώρησε στο Mozilla Firefox, Adobe Flash, και Oracle Java.

Ο Nils και Jon από τα MWRLabs ήταν επιτυχείς στην εύρεση αδυναμιών του Google Chrome χρησιμοποιώντας WebKit και τα ελαττώματα του πυρήνα των Windows για να παρακάμψει το Chrome sandbox και κέρδισε $ 100.000.

Ο George Hotz έκανε hack στον Adobe Acrobat Reader και ξέφυγε από το sandbox κερδίζοντας $ 70.000. Ο James Forshaw, Joshua Drake, και Ben Murphy ανεξάρτητα εισέβαλαν στον Oracle Java κερδίζοντας $ 20.000 ο καθένας.

Apple Safari στο Mountain Lion δεν παραβιάστηκαν καθώς δεν ομάδες εμφανίστηκαν.

Βιβλιογραφία

1. *Ruiu, Dragos (March 20, 2007). "PWN to OWN (was Re: How Apple orchestrated web attack on researchers)". Retrieved April 1,2012.*
2. **Jump up^** *Naraine, Ryan (February 1, 2007). "Mac Developer mulling OS X equivalent of ZERT". Retrieved April 1, 2012.*
3. **Jump up^** *Orchant, Marc (February 6, 2007). "Cancel or Allow? Good poke at Vista UAC". Retrieved April 1, 2012.*
4. ^ Jump up to: [a] [b] [c] *Naraine, Ryan (March 26, 2007). "How long can a Mac survive the hacker jungle?". Retrieved April 1, 2012.*

5. ^ Jump up to:[a] [b] *"About the Zero Day Initiative"*. Retrieved April 1, 2012.
6. **Jump up^** *Forslof, Terri (May 3, 2007). "Apple issues patch for QuickTime flaw". Retrieved April 1, 2012.*
7. **Jump up^** *"Pwn2Own 2015: The year every web browser went down | ZDNet". ZDNet. Retrieved 2015-11-25.*
8. **Jump up^** *Goodin, Dan (20 April 2007). "Safari zero-day exploit nets $10,000 prize". Vancouver: The Register. Retrieved 10 April 2010.*
9. **Jump up^** *"Apple QTJava toQTPointer() Pointer Arithmetic Memory Overwrite Vulnerability". Retrieved 31 March 2012.*
10. **Jump up^** *Naraine, Ryan (April 23, 2007). "10 questions for MacBook hacker Dino Dai Zovi". ZDNet. Retrieved 16 November 2010.*
11. **Jump up^** *Vaas, Lisa (April 20, 2007). "Mac Hacked Via Safari Browser in Pwn-2-Own Contest". eWeek. Retrieved March 10, 2011.*
12. ^ Jump up to:[a] [b] [c] *Forslof, Terri (March 19, 2008). "CanSecWest PWN to OWN 2008 (updated)". Retrieved April 1, 2012.*
13. ^ Jump up to:[a] [b] [c] *Ruiu, Dragos (March 20, 2008). "CanSecWest 2008 PWN2OWN - Mar 26-28". Retrieved April 1, 2012.*
14. **Jump up^** *"Apple Safari WebKit PCRE Handling Integer Overflow Vulnerability". April 16, 2008. Retrieved April 1, 2012.*
15. **Jump up^** *"PWN to OWN Day Two: First Winner Emerges! (updated)". March 27, 2008. Retrieved April 1, 2012.*
16. **Jump up^** *"Adobe Flash Player DeclareFunction2 Invalid Object Use Vulnerability". April 8, 2008. Retrieved April 1, 2012.*
17. **Jump up^** *"PWN to OWN: Final Day (and another winner!)". March 28, 2008. Retrieved April 1, 2012.*
18. **Jump up^** *Kebbel-Wyen, John (April 4, 2008). "Adobe Product Security Incident Response Team (PSIRT) Blog / CanSecWest 2008 Pwn2Own Contest". Retrieved April 1, 2012.*

19. Pwn2Own 2012 Rules
20. ^ Jump up to:[a] [b] [c] [d] Ryan Naraine, Charlie Miller skipping Pwn2Own as new rules change hacking game, ZDnet, March 7, 2012
21. **Jump up^** Pwn2Own 2012: Google Chrome browser sandbox first to fall,ZDnet, March 7, 2012
22. **Jump up^** IE 9, on most secure Windows yet, next browser to fall at hacker contest, Ars Technica, March 8, 2012
23. **Jump up^** Researchers hack into newest Firefox with zero-day flaw, ZDnet, March 9, 2012
24. **Jump up^** PWN2OWN 2012 rules Archived March 1, 2012, at the Wayback Machine.
25. **Jump up^** PWN2OWN 2012 status Archived June 26, 2012, at theWayback Machine.
26. **Jump up^** Ryan Naraine, CanSecWest Pwnium: Google Chrome hacked with sandbox bypass, ZDnet, March 7, 2012

27. **Jump up^** At hacking contest, Google Chrome falls to third zero-day attack
28. **Jump up^** After the pwnage: Critical Google Chrome hole plugged in 24 hours, Ars Technica
29. **Jump up^** Show off Your Security Skills: Pwn2Own and Pwnium 3, The Chromium Blog, January 28, 2013
30. **Jump up^** http://www.scmagazine.com.au/News/335750,chrome-firefox-ie-10-java-win-8-fall-at-pwn2own-hackfest.aspx
31. **Jump up^**http://www.theregister.co.uk/2013/03/08/pwn2own_contest_cansecwest/

Συμπεράσματα

Έχουν γίνει αντιληπτά πλέον τα πλεονεκτήματα καθώς και τα μειονεκτήματα από την απεριόριστη χρήση των Ηλεκτρονικών Υπολογιστών και τη λειτουργία του Διαδικτύου. Καθημερινά, το διαδίκτυο χρησιμοποιείται για διάφορους σκοπούς είτε καλούς είτε κακούς. Παράλληλα όμως αυτό έδωσε πρόσφορο έδαφος στη δημιουργία του Ψηφιακού Εγκληματία. Ως Ψηφιακός Εγκληματίας θεωρείται πλέον οποιοσδήποτε εισβάλει παράνομα σε κάποιο λειτουργικό σύστημα και οι ανάλογες πράξεις τιμωρούνται από αντίστοιχο νόμο.

Με την πρόοδο της τεχνολογίας ανακαλύπτονται και όλο και περισσότεροι ψηφιακοί εγκληματίες καθώς και νέες μορφές εγκλήματος που οδηγεί στην σύναψη νέων νόμων για την αντιμετώπιση τους. Παράλληλα όμως έχει αποδειχτεί πως όλοι οι Hackers δεν είναι απαραίτητα κακοί και με δόλιους σκοπούς αλλά υπάρχουν και ηθικοί Hackers οι οποίοι χρησιμοποιούν τις γνώσεις τους βοηθώντας στην καταπολέμηση της ψηφιακής εγκληματικότητας. Να εξαλείψουμε τους Ψηφιακούς Εγκληματίες είναι πλέον αδύνατο. Μπορούν να ληφθούν μέτρα και πρέπει να ληφθούν για την καλύτερη αντιμετώπιση τους. Σαν αποτέλεσμα, πολλοί χρήστες του διαδικτύου προσπαθούν να προστατευτούν όσο καλύτερα μπορούν από τυχόν επιθέσεις.

Οι πρώτες μορφές ηλεκτρονικού εγκλήματος εμφανίστηκαν την δεκαετία του '70 στην Αμερική. Οι περισσότερες υποθέσεις περιλαμβάνουν την παράνομη εισβολή σε τηλεφωνικά συστήματα, την υπεξαίρεση μεγάλων χρηματικών ποσών από τράπεζες, την υποκλοπή αριθμών πιστωτικών καρτών και αρχείων μεγάλων εταιρειών και οργανισμών, όπως είναι το FBI, την παράνομη διακίνηση λογισμικού και δημιουργία νέων ιών.

Οι πιο γνωστές και διασκεδαστικές ιστορίες είναι αυτές των hackers, οι οποίοι στην πλειοψηφία ενεργούν είτε για να ικανοποιήσουν την περιέργειά τους είτε για να διασκεδάσουν. Γι' αυτό το λόγο αυτό είναι η μοναδική κατηγορία εγκληματία που είναι αμφιλεγόμενη και πολλές φορές χρήζει της συμπάθειας του κόσμου.

Στην Ελλάδα, οι μορφές ηλεκτρονικών εγκλημάτων που είναι πιο συχνές είναι η παιδική πορνογραφία, το Cracking και hacking, η παράνομη διακίνηση λογισμικού και οι απάτες μέσω πιστωτικών καρτών. Σε αυτά τα εγκλήματα, ειδικά εξειδικευμένοι πολίτες, κυρίως White Hackers) συμβάλουν στην αντιμετώπισή τους.

Από τα βασικότερα προβλήματα του Hacking είναι η ταχύτατη πρόοδός του. Η εξέλιξή του είναι ραγδαία και φέρνει μεγάλες δυσκολίες για την αντιμετώπισή του. Τα κράτη και οι εταιρίες πολλές φορές αδυνατούν να συμβαδίσουν. Αυτό γίνεται λόγο του ότι υπάρχει έλλειψη επαφής με το δράστη, η διεθνής φύση του εγκλήματος καθώς και ο μη καθορισμένος στόχος δυσκολεύουν την αποτροπή του εγκλήματος όπως και σύλληψη του δράστη.

Φυσικά υπάρχουν τρόποι να βρεθούν οι ψηφιακοί εγκληματίες όπως η διεύθυνση IP και ο ηλεκτρονικός υπολογιστής αλλά δεν είναι αρκετά για την αντιμετώπιση του Ψηφιακού Εγκλήματος.

Πολλοί είναι εκείνοι που υποστηρίζουν ότι η σωστή ενημέρωση και προφύλαξη είναι η λύση του προβλήματος. Ειδικότερα όταν πρόκειται για παιδιά και γονείς. Μερικοί τρόποι πρόληψης είναι:

α)επιφύλαξη με τα ηλεκτρονικά mail και ειδικότερα με τα συνημμένα αρχεία που λαμβάνουν

*β)*η εγκατάσταση προγραμμάτων στον υπολογιστή μας που μας προστατεύουν από ιούς και πιθανούς hackers

γ)το κλείσιμο του υπολογιστή όταν δεν χρησιμοποιείται.

Το ηλεκτρονικό και διαδικτυακό έγκλημα αυξάνεται ραγδαία στις μέρες μας λόγω των νέων τεχνολογιών οι οποίες είναι κατανοητές ακόμα και στους απλούς χρήστες. Η έξαρσή του είναι πλέον αντιληπτή. Πολλά είναι τα μέτρα που πρέπει να ληφθούν από τους αρμόδιους και τους κρατικούς φορείς. Αυτό όμως δεν είναι αρκετό. Θα πρέπει και οι ίδιοι οι χρήστες να γνωρίζουν το νόμο και τις συνέπειές του.

Σύνοψη Βιβλιογραφίας

Βιβλιογραφία

Οικονομία και Εγκληματικότητα, Σεπτέμβριος 2010, Χρήστος Ε. Τσουραμάνης, συνεργασία Μαρ. Ευγ. Καρολή

Ηλεκτρονική Βιβλιογραφία

Wikipedia: Χάκερ

https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81

Sites Google

Ορισμός Χάκερ

https://sites.google.com/site/projecths12/hacking

Oldschool Hackers, Script Kiddies/Cyber Punks, Professional Criminals/Crackers
https://sites.google.com/site/projecths12/hacking/kategories

Είδη Ψηφιακών Εγκληματιών:
http://webcache.googleusercontent.com/search?q=cache:http://www.theartofcrime.gr/artofcrime/assets/hackers.doc&gws_rd=cr&ei=_8E4V4KECurO6ATR3ZfoAw

White Hats, Black Hats, Grey Hats:
http://webcache.googleusercontent.com/search?q=cache:http://www.theartofcrime.gr/artofcrime/assets/hackers.doc&gws_rd=cr&ei=_8E4V4KECurO6ATR3ZfoAw

Spam Phishing

http://ikee.lib.auth.gr/record/115622/files/ptuxiaki.pdf

Ελληνική Αστυνομία

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414

Wikipedia: Pwn2Own

https://en.wikipedia.org/wiki/Pwn2Own

Ruiu, Dragos (March 20, 2007). "PWN to OWN (was Re: How Apple orchestrated web attack on researchers)". Retrieved April 1,2012.

Jump up^ *Naraine, Ryan (February 1, 2007). "Mac Developer mulling OS X equivalent of ZERT". Retrieved April 1, 2012.*

Jump up^ *Orchant, Marc (February 6, 2007). "Cancel or Allow? Good poke at Vista UAC". Retrieved April 1, 2012.*

^ Jump up to: *Naraine, Ryan (March 26, 2007). "How long can a Mac survive the hacker jungle?". Retrieved April 1, 2012.*

^ Jump up to: *"About the Zero Day Initiative". Retrieved April 1, 2012.*

Jump up^ *Forslof, Terri (May 3, 2007). "Apple issues patch for QuickTime flaw". Retrieved April 1, 2012.*

Jump up^ *"Pwn2Own 2015: The year every web browser went down | ZDNet". ZDNet. Retrieved 2015-11-25.*

Jump up^ *Goodin, Dan (20 April 2007). "Safari zero-day exploit nets $10,000 prize". Vancouver: The Register. Retrieved 10 April 2010.*

Jump up^ *"Apple QTJava toQTPointer() Pointer Arithmetic Memory Overwrite Vulnerability". Retrieved 31 March 2012.*

Jump up^ *Naraine, Ryan (April 23, 2007). "10 questions for MacBook hacker Dino Dai Zovi". ZDNet. Retrieved 16 November 2010.*

Jump up^ *Vaas, Lisa (April 20, 2007). "Mac Hacked Via Safari Browser in Pwn-2-Own Contest". eWeek. Retrieved March 10, 2011.*

^ Jump up to: *Forslof, Terri (March 19, 2008). "CanSecWest PWN to OWN 2008 (updated)". Retrieved April 1, 2012.*

^ Jump up to: *Ruiu, Dragos (March 20, 2008). "CanSecWest 2008 PWN2OWN - Mar 26-28". Retrieved April 1, 2012.*

Jump up^ *"Apple Safari WebKit PCRE Handling Integer Overflow Vulnerability". April 16, 2008. Retrieved April 1, 2012.*

Jump up^ *"PWN to OWN Day Two: First Winner Emerges! (updated)". March 27, 2008. Retrieved April 1, 2012.*

Jump up^ *"Adobe Flash Player DeclareFunction2 Invalid Object Use Vulnerability". April 8, 2008. Retrieved April 1, 2012.*

Jump up^ *"PWN to OWN: Final Day (and another winner!)". March 28, 2008. Retrieved April 1, 2012.*

Jump up^ *Kebbel-Wyen, John (April 4, 2008). "Adobe Product Security Incident Response Team (PSIRT) Blog / CanSecWest 2008 Pwn2Own Contest". Retrieved April 1, 2012.*

Pwn2Own 2012 Rules

^ Jump up to: [a] [b] [c] [d] Ryan Naraine, Charlie Miller skipping Pwn2Own as new rules change hacking game, ZDnet, March 7, 2012

Jump up^ Pwn2Own 2012: Google Chrome browser sandbox first to fall,ZDnet, March 7, 2012

Jump up^ IE 9, on most secure Windows yet, next browser to fall at hacker contest, Ars Technica, March 8, 2012

Jump up^ Researchers hack into newest Firefox with zero-day flaw, ZDnet, March 9, 2012

Jump up^ PWN2OWN 2012 rules Archived March 1, 2012, at the Wayback Machine.

Jump up^ PWN2OWN 2012 status Archived June 26, 2012, at theWayback Machine.

Jump up^ Ryan Naraine, CanSecWest Pwnium: Google Chrome hacked with sandbox bypass, ZDnet, March 7, 2012

Jump up^ At hacking contest, Google Chrome falls to third zero-day attack

Jump up^ After the pwnage: Critical Google Chrome hole plugged in 24 hours, Ars Technica

Jump up^ Show off Your Security Skills: Pwn2Own and Pwnium 3, The Chromium Blog, January 28, 2013

Jump up^ http://www.scmagazine.com.au/News/335750,chrome-firefox-ie-10-java-win-8-fall-at-pwn2own-hackfest.aspx

Jump up^http://www.theregister.co.uk/2013/03/08/pwn2own_contest_cansecwest/