|  |  |
| --- | --- |
| **νήσια ηλεκτρονικά εγκλήματα**

|  |
| --- |
| **ΓΝΗΣΙΑ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΛΗΜΑΤΑ**Σε αυτά συμπεριλαμβάνονται οι κακόβουλες εισβολές στα δίκτυα, (hacking).Συμπεριλαμβάνονται επίσης οι επιθέσεις άρνησης εξυπηρέτησης, το κακόβουλο λογισμικό, η ανεπιθύμητη αλληλογραφία (spamming), οι επιθέσεις σε δικτυακούς τόπους, η πειρατεία ονομάτων χώρου, το ψάρεμα (phishing) και πειρατεία λογισμικού.https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcRVHFnsQw1A2CDy9YQYS7YaRt3jbnhwwAjDBQVBgiWCqn9cwIQTiQ1.**HACKING** Η Χωρίς Νόμιμη Εξουσιοδότηση Είσοδος σε Η/Υ(hacking ή cracking):Το hacking είναι πλέον το έγκλημα του 21ου αιώνα και βρίσκεται σε κάθε διαδικτυακό έγκλημα. Οι hackers αποσκοπούν στην πρόσβαση ξένων υπολογιστών ή συστημάτων υπολογιστών με στόχο την διαχείριση αυτών εξ’ αποστάσεως. Εισβάλλουν στο διαδίκτυο με πρόσβαση σε συστήματα, αποκτώντας γνώσεις για την ασφάλεια του και τις αδυναμίες του, κάτι το οποίο καθιστά ακόμη πιο εύκολη την επίθεση του στόχου.Ανάλογα με τα δικαιώματα που αποκτά ο εισβολέας στο σύστημα, διακρίνονται δύο κατηγορίες: α) στην πλήρη διείσδυση με δικαιώματα διαχειριστή συστήματος, όπου σε αυτή τη περίπτωση ο επιτιθέμενος μπορεί να παρέμβει κάνοντας σοβαρές αλλαγές, και β) στην διείσδυση με δικαιώματα απλού χρηστή συστήματος.Ποιες είναι όμως οι πιο συνήθεις τεχνικές hacking;Η εκμετάλλευση των **cookies**: Σε κάθε ηλεκτρονικό υπολογιστή τοποθετούνται μικρά αρχεία (cookies) από διάφορες τοποθεσίες του διαδικτύου που επισκέπτεται ο χρηστής. Τα cookies είναι ένα είδος αρχείων τα οποία δημιουργούνται και αποθηκεύονται στον σκληρό δίσκο του υπολογιστή από τα Web sites που επισκέπτονται οι χρήστες στο internet με απώτερο σκοπό την αναγνώριση τους από τα ίδια τα Websites την επόμενη φορά που θα τα επισκεφθούν. Yποτίθεται ότι εξυπηρετούν χρήσιμους σκοπούς για τους χρήστες του διαδικτύου, καθώς συγκεντρώνουν πληροφορίες  σχετικά με τις καταναλωτικές τους συνήθειες, τις οποίες μπορούν να αξιοποιήσουν sites μεγάλων εταιρειών για να εξειδικεύσουν έτσι ή και να βελτιώσουν τα προϊόντα ή τις υπηρεσίες τους. Παρ’όλα αυτά, η σημαντικότερη χρήση των cookies είναι η  παρακολούθηση και η καταγραφή των κινήσεων των χρηστών στο internet, συνήθως τις καταναλωτικές, τις προτιμήσεις στα site που επισκέπτονται, το χρόνο που μένουν σε αυτά, τις φορές που τα επισκέπτονται κ.τ.λ. Τα cookies αποτελούν ένα από τα πιο αμφιλεγόμενα θέματα του διαδικτύου καθώς έχουν να κάνουν με τα προσωπικά δεδομένα και το προσωπικό απόρρητο των χρηστών του.Σε αυτά τα αρχεία λοιπόν, ένας hacker εκμεταλλευόμενος κάποια ευπάθεια του ηλεκτρονικού συστήματος, έχει τη δυνατότητα να βρει όνομα χρηστή, κωδικούς πρόσβασης για μια υπηρεσία κ.α. Ανίχνευση δικτυακών υπηρεσιών συστημάτων: Στην περίπτωση αυτή οι εισβολείς προσπαθούν να συγκεντρώσουν πληροφορίες για το σύστημα – στόχο. Αυτό το πετυχαίνουν στέλνοντας ερωτήματα σε διακομιστές σχετικά με τις παρεχόμενες υπηρεσίες και το επίπεδο ασφαλείας. Αυτή είναι η τεχνική σάρωσης των θυρών (port scanning). Οι πληροφορίες που λαμβάνουν είναι σημαντικές αφού έτσι ο επιτιθέμενος μπορεί πλέον να εισβάλει στο σύστημα εκμεταλλευόμενος τις ευπάθειές του λειτουργικού συστήματος ή άλλων παρεχόμενων υπηρεσιών. Μέσω αυτών των πληροφοριών μπορεί να βρει και λογαριασμούς οι όποιοι δεν προστατεύονται με κωδικούς πρόσβασης, κάνοντας το στόχο ευκολότερο. Ανιχνευτές δικτυακών πακέτων: Η ανίχνευση δικτυακών πακέτων πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers τα οποία παρέχουν τη δυνατότητα εντοπισμού όλων των πακέτων που υπάρχουν στο διαδίκτυο. Σε περίπτωση που τα πακέτα αυτά δεν είναι κρυπτογραφημένα η απόσπαση των πληροφοριών είναι εύκολη. Ο hacker μπορεί να έχει πληροφορίες όπως είναι οι κωδικοί πρόσβασης, ο αριθμός πιστωτικών καρτών και άλλων που βρίσκονται στο διαδίκτυο.**Πλάστες διευθύνσεις**: Ο ρόλος των hackers σε αυτήν τη τεχνική είναι η παρέμβαση τους σε επικεφαλίδες πακέτων μέσα σε ένα δίκτυο, τις οποίες τροποποιούν ώστε το μήνυμα να φαίνεται ότι προήλθε από αξιόπιστη πηγή. Μέσω αυτών των πλαστών διευθύνσεων εισβάλλουν αβίαστα σε δικτυακές υπηρεσίες.**Επιθέσεις σε επίπεδο εφαρμογής**: Οι επιθέσεις εστιάζονται στις αδυναμίες – ευπάθειες των δικτυακών εφαρμογών. Οι φυλλομετρητές συχνά παρουσιάζουν προβλήματα στην ασφάλεια τους.Γενικά η μορφή αυτή του Ηλεκτρονικού Εγκλήματος έχει να κάνει με την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα, με παράνομους σκοπούς.Αυτούς τους «εγκληματίες του Κυβερνοχώρου» μπορούμε να τους διακρίνουμε σε δύο κατηγορίες ανάλογα με τον τρόπο διείσδυσης και το επιδιωκόμενο αποτέλεσμα :στους hackers και στους crackers (criminal hackers) .Με τον όρο hackers χαρακτηρίζονται εκείνα τα άτομα που έχουν εξειδικευμένες τεχνικές γνώσεις για τους υπολογιστές γενικότερα αλλά έχουν και προχωρημένες γνώσεις προγραμματισμού, μπορούν να εντοπίσουν αδυναμίες σε συστήματα υπολογιστών και να συνεργάζονται για την επίλυση των προβλημάτων των υπολογιστών, χωρίς να προξενούν ζημιά με απώτερο σκοπό για κάποιους από αυτούς την αμοιβή τους ή ακόμα και την πρόσληψη τους από τον οργανισμό που εντόπισαν οποιοδήποτε πρόβλημα και βοήθησαν στην επίλυση του . Οι ίδιοι θεωρούν ότι προσφέρουν κοινωνικό έργο καθώς η παράνομη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε υπολογιστικά συστήματα δεν γίνεται με σκοπό την δολιοφθορά ή την καταστροφή, την υποκλοπή ή την κατασκοπεία αλλά κυρίως την προσωπική τους ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ. Οι hackers εμφανίστηκαν για πρώτη φορά στα τηλεπικοινωνιακά δρώμενα τη δεκαετία του 1970 στις Η.Π.Α.Οι crackers , από την άλλη μεριά, είναι εκείνα τα άτομα τα οποία τα χαρακτηρίζουν ως κακόβουλους hackers αφού η παράνομη εισβολή τους στα υπολογιστικά συστήματα γίνεται με στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την άρση της προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους, τις ενέργειες εκείνες που θα τους αποκομίσουν οικονομικά οφέλη, για παράδειγμα μεταφορά σε προσωπικό λογαριασμό τραπέζης μεγάλων χρηματικών ποσών από υποκλοπή αριθμού πιστωτικής κάρτας. Η ουσία του προβλήματος του cracking δεν εντοπίζεται σε επιθέσεις που γίνονται στην αρχική ιστοσελίδα (Home Page) του δικτυακού τόπου μιας δημόσιας υπηρεσίας ή ενός μεγάλου οργανισμού, κάτι που είναι πολύ εύκολο να γίνει αντιληπτό, αλλά στις ύπουλες επιθέσεις. Στη τροποποίηση, δηλαδή, χωρίς να γίνει αντιληπτό σημαντικών δεδομένων που τηρούνται από δημόσιες υπηρεσίες, όπως για παράδειγμα η αλλαγή της σειράς επιτυχίας σε έναν διαγωνισμό, στη πιστή αντιγραφή ολόκληρων διαδικτυακών τόπων μεγάλων εταιρειών που κάνουν πωλήσεις μέσω διαδικτύου ή και μεγάλων οργανισμών ή δημόσιων υπηρεσιών και στην εξαπάτηση ανυποψίαστων χρηστών των διαδικτυακών τόπων.**2.ΕΠΙΘΕΣΕΙΣ ΑΡΝΗΣΗΣ ΕΞΥΠΗΡΕΤΗΣΗΣ**Οι επιθέσεις άρνησης εξυπηρέτησης έχουν ως στόχο την εισβολή σε ένα υπολογιστικό σύστημα με σκοπό την εξάντληση πόρων αυτού έτσι ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Γενικότερα οι επιθέσεις αυτές έχουν σαν στόχο την παρεμπόδιση μετάδοσης δεδομένων στο δίκτυο, την παρεμπόδιση σύνδεσης σε υπηρεσίες, την αλλοίωση ποιότητας μιας υπηρεσίας που προσφέρεται στον χρήστη. Οι επιθέσεις άρνησης μπορούν να πραγματωθούν με τεχνικές όπως είναι οι τεχνικές επιθέσεις, SYN Flood Attacks, UDP Flood Attacks, ICMP Flood Attacks, Teardropattacks, Ping of death, port flooding, OOB Attacks, Fragmentation, Smurf Attacks, Fraggle Attacks και PapasmurfAttacks. Οι πιο σημαντικές τεχνικές επιθέσεων είναι οι SYN Flood Attacks, Ping of death, Fragmentation.Η εκτέλεση της επίθεσης άρνησης μπορεί να συνοψιστεί σε τέσσερα βασικά βήματα. Στο πρώτο βήμα ο εισβολέας εγκαθιστά το πρόγραμμα απομακρυσμένης διαχείρισης σε ηλεκτρονικούς υπολογιστές που διαθέτουν ευρυζωνικές συνδέσεις στο διαδίκτυο και στην πορεία γίνεται απόπειρα σύνδεσης με αυτούς τους υπολογιστές. Στο δεύτερο βήμα ο επιτιθέμενος δίνει εντολή στο πρόγραμμα να αποστείλει ping. Το ping είναι μια δικτυακή εφαρμογή μέσω της οποίας διαπιστώνεται αν μια διεύθυνση είναι προσβάσιμη. Ο υπολογιστής του δράστη λειτουργεί ως zombie, δηλαδή ο συγκεκριμένος υπολογιστής επιτρέπει στον επιτιθέμενο να το διαχειρίζεται από απόσταση. Στην τρίτη φάση πλέον έχουμε την ανταπόκριση του υπολογιστή – θύμα, ο όποιος απαντάει στα ping χωρίς όμως να μπορεί να πετύχει κάποια σύνδεση με τον υπολογιστή - zombie. Όσο ο υπολογιστής - θύμα περιμένει απάντηση, ο υπολογιστής - zombie συνεχίζει να στέλνει νέα ping. Το αποτέλεσμα είναι η άρνηση εξυπηρέτησης, δηλαδή οι πόροι του θύματος εξαντλούνται από την πληθώρα αιτημάτων κι έτσι είναι αδύνατη η προσφορά άλλων υπηρεσιών.**3.ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ**Το κακόβουλο λογισμικό είναι ίσως ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του διαδικτύου. Η διασπορά του κακόβουλου κώδικα έχει σκοπό να διεισδύσει σε έναν ηλεκτρονικό υπολογιστή με σκοπό να του προκαλέσει ζημιά διαγράφοντας ή αλλοιώνοντας δεδομένα και προγράμματα, υποκλέπτοντας δεδομένα ή παρεμποδίζοντας τη λειτουργία ενός συστήματος.Συμφωνά με τον Sinrod ο κακόβουλος κώδικας διακρίνεται στους ιούς, στα σκουλήκια και στους δούρειους ίππους. Οι ιοί είναι ο πιο συνήθης κακόβουλος κώδικας. Ένας ιός δεν είναι τίποτα περισσότερο από ένα πρόγραμμα που τοποθετείται σε σημεία τέτοια ώστε να μην γίνεται αντιληπτός εκτελώντας την επίθεση του. Το πρόγραμμα αυτό είναι μια σειρά από εντολές που εκτελούν κακόβουλες ενέργειες σε έναν υπολογιστή. Σημαντικό είναι, όπως αναφέρθηκε και προηγουμένως, να εγκατασταθεί σε τέτοια θέση στον υπολογιστή – θύμα ώστε να μην γίνει αντιληπτό από το χρηστή. Ο χρηστής επομένως άθελα του γίνεται φορέας του ιού που θα μεταδώσει σε άλλον υπολογιστή. Έτσι επιδιώκεται η συνέχειά του ενώ παράλληλα προκαλεί ζημιές και αλλοιώσεις σε κάθε υπολογιστικό σύστημα. Η ζημιά που κάνει ένας ιός μπορεί να κυμαίνεται από την εμφάνιση ενός ενοχλητικού μηνύματος στην οθόνη του υπολογιστή μέχρι και την διαγραφή όλων των δεδομένων του σκληρού δίσκου του υπολογιστή που έχει μολύνει. Ο συνηθέστερος τρόπος μόλυνσης ενός υπολογιστή είναι μέσω e-mail με απατηλά μηνύματα από άγνωστο, τις περισσότερες φορές, αποστολέα που περιέχουν ένα συνημμένο αρχείο με το πρόγραμμα του ιού, το οποίο εκτελείται αυτόματα και μολύνει τον υπολογιστή του χρήστη. Γνωστοί ιοί υπολογιστών που άφησαν εποχή είναι ο Melissa, o Michelangelo, o I Love You, oBlaster κ.αΟι βασικότεροι ιοί είναι οι:**File-infectors ή parasitic viruses**: ο ιός αυτός ενεργεί μολύνοντας ένα εκτελέσιμο πρόγραμμα, στο όποιο προσθέτουν το κακόβουλο κώδικα. Μολύνει αρχεία με επεκτάσεις .com, .exe, .sys, .old. Boot Sector Virus: ο ιός αυτός προσβάλει εκτελέσιμο κώδικα συστήματος, τον οποίο εντοπίζει σε συσκευές βοηθητικής μνήμης, στον τομέα εκκίνησης ή στο MBR (Master Boot Record) του δίσκου.Ο Boot Sector Virus ενεργεί μολύνοντας κάθε δίσκο ή δισκέτα που θα χρησιμοποιηθεί από τον υπολογιστή.**Multi-partite viruses**: Δρουν συνδυάζοντας επιμέρους χαρακτηριστικά των δύο παραπάνω κατηγοριών. Έχουν τη δυνατότητα να μολύνουν εκτελέσιμα αρχεία αλλά και τομείς εκκίνησης. Companion viruses: ο ιός εκμεταλλεύεται μια ευπάθεια του λειτουργικού συστήματος DOS. Μεταδίδεται με αποσπώμενα αποθηκευτικά μέσα και πολλές φόρες το αρχείο αυτό παραμένει κρυφό στη μνήμη του υπολογιστή.**Ιοί Link και Flash Bios**: οι link δε μολύνουν το πρόγραμμα καθ’ αυτό αλλά δρουν τροποποιώντας το αρχείο FAT (fileallocation table). Αυτό έχει ως αποτέλεσμα να αλλάζει ο σύνδεσμος που δείχνει προς ένα πρόγραμμα του υπολογιστή με τρόπο ώστε να «δείχνει» στο σημείο που βρίσκεται ο ιός και να εκτελείται αυτός αντί για το πρόγραμμα. Οι Flash Bios αντικαθιστούν το λογισμικό BIOS στην μητρική πλακέτα με απρόβλεπτες συνέπειες, όπως αδυναμία εκκίνησης του υπολογιστή.**Macro viruses**: οι ιοί αυτοί βρίσκονται σε αρχεία προγράμματος αυτοματισμού γραφείου. Τα σκουλήκια είναι παρόμοια με τους ιούς μονό που πολλαπλασιάζονται χωρίς κάποια συγκεκριμένη ενέργεια από το χρηστή. Η διάδοσή τους γίνεται μέσω διαδικτύου χωρίς να χρειάζεται να επισυναφτούν σε κάποιο αρχείο. Αυτά μπορούν να τροποποιήσουν ή να διαγράψουν αρχεία ενός υπολογιστή και στη συνέχεια στέλνουν αντίγραφα του εαυτού τους σε υποψήφια θύματα. Από τα πιο καταστροφικά σκουλήκια ήταν το Code Red II που μόλυνε σε 14 ώρες 359.000 υπολογιστές προκαλώντας ζημία που ξεπερνούσε τα δύο δις. δολάρια.Στη κατηγορία του κακόβουλου λογισμικού περιλαμβάνονται επίσης οι **Δούρειοι ίπποι, Adware,Spyware,** **Dialers** ( Dialers είναι εκείνα τα προγράμματα που καλούν τηλεφωνικούς αριθμούς για την πρόσβαση σε ορισμένες υπηρεσίες υψηλής χρέωσης) οι λογικές και ωρολογιακές βόμβες, οι φάρσες και οι τεχνικές απόκρυψης ιών. Αναλυτικότερα, στον τρωικό πόλεμο ο Οδυσσέας κατάφερε να εξαπατήσει τους Τρώες με τον Δούρειο Ίππο. Αυτό που έκανε ήταν να «δωρίσει» στους Τρώες τον Δούρειο Ίππο για να έχουν καλή τύχη. Οι Τρώες πέρασαν τον Ίππο μέσα από τα τείχη και τότε εμφανίστηκαν οι έλληνες μέσα από αυτόν ξεκινώντας την άλωση της πόλης. Έτσι λοιπόν δίνουμε αυτή την ονομασία και στο κακόβουλο λογισμικό αφού κι αυτό φαινομενικά είναι ένα «αθώο» πρόγραμμα το όποιο κρύβει λειτουργίες που δεν είναι εύκολο να εντοπιστούν από το χρηστή. Τα προγράμματα αυτά φορτώνονται στο σκληρό δίσκο του υπολογιστή. Ο επιτιθέμενος με αυτό τον τρόπο καταφέρνει τον εξ αποστάσεως έλεγχο του συστήματος και μπορεί έτσι να συλλέξει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή ακόμα και να εξαπολύσει άρνηση εξυπηρέτησης. Τα Ad-ware και Spyware είναι προγράμματα που περιέχουν κακόβουλο κώδικα και θεωρούνται υποκατηγορία των Δούρειων Ίππων. Χρησιμοποιούνται για την διαφημιστική προώθηση συγκεκριμένων δικτυακών τόπων και προϊόντων που προσφέρονται μέσω του διαδικτύου. Σε περίπτωση που η λειτουργία τους ορίζεται στους ορούς χρήσης που αποδέχεται ο χρηστής, δεν χαρακτηρίζεται ως κακόβουλο λογισμικό. Τα Ad-ware και Spyware συνεργάζονται για τη δημιουργία προφίλ χρηστών με σκοπό την αποστολή στοχευόμενων διαφημίσεων αλλά μπορούν να προκαλέσουν και ανεπιθύμητα αποτελέσματα όπως είναι η καταστροφή αρχείων, οι αποσυντονισμοί του συστήματος και η επιβράδυνση της περιήγησης στο διαδίκτυο και της εν γένει λειτουργίας του υπολογιστή.Όσο αφόρα στους dialers αποτελούν υποκατηγορία των Spyware. Είναι μικρά προγράμματα κι έχουν τη δυνατότητα να αποσυνδέουν της τηλεφωνική γραμμή από το internet και να συνδέονται με άλλες κλήσεις μεγαλύτερης χρέωσης. Επομένως το αποτέλεσμα αυτής της λειτουργίας είναι ο πλουτισμός συγκεκριμένων κατόχων δικτυακών τόπων από τα τεράστια αυτά ποσά. Οι dialers κρύβονται σε συγκεκριμένες ιστοσελίδες οι οποίες πιθανόν περιέχουν πειρατικό λογισμικό ή οποιοδήποτε άλλο αμφιλεγόμενο λογισμικό. Η λογική βόμβα είναι ένα πρόγραμμα που ενεργοποιείται με ένα συγκεκριμένο γεγονός. Το πρόγραμμα αυτό μπορεί να σταματήσει τη λειτουργία του υπολογιστή και να απελευθερώσει έναν ιό διαγράφοντας αρχεία και προκαλώντας γενικότερες ζημιές. Το εν λόγω πρόγραμμα ενεργοποιείται είτε από το χρηστή, είτε σε χρόνο και ημερομηνία που έχει εκ των προτέρων προγραμματισθεί, όπως συμβαίνει και με τις ωρολογιακές βόμβες.Οι φάρσες ίσως να μην ανήκουν στο κακόβουλο λογισμικό αλλά είναι κακόβουλη η πρόθεση του επιτιθέμενου, αφού το μόνο που καταφέρνει είναι να προκαλέσει πανικό στο χρήστη προειδοποιώντας τον για έναν ιό που δεν υπάρχει. Ο χρηστής ωστόσο στην προσπάθεια του να προστατέψει τα δεδομένα του καταφεύγει στη διαγραφή αυτών.Για την προστασία του χρηστή από τους ιούς εταιρείες αντιβιοτικού λογισμικού προσφέρουν το αντίστοιχο λογισμικό για την αντιμετώπιση τους. Ωστόσο, οι αόρατοι ιοί (stealth) προβλέποντας αυτές τις κινήσεις, παραμένουν ενεργοί, κάνοντας τις καταστροφικές λειτουργίες τους χωρίς να μπορούν να εντοπιστούν από το εκάστοτε αντιβιοτικό λογισμικό. Οι πολυμορφικοί ιοί (Polymorphic, self-mutating) παράγουν αντίγραφα του εαυτού τους, διαφορετικά μεταξύ τους αλλά το ίδιο καταστροφικά. Τα αντίγραφα δημιουργούν ένα «θόρυβο» με αποτέλεσμα να μην εντοπίζονται από τα antivirus.**4.SPAMMING**Με τον όρο spam εννοούμε την απρόκλητη, εμπορική και μαζική αποστολή μεγάλου αριθμού ηλεκτρονικών μηνυμάτων, τα οποία απευθύνονται σε ένα σύνολο χρηστών του διαδικτύου, χωρίς αυτοί να έχουν ζητήσει ή να επιθυμούν κάτι τέτοιο και χωρίς να έχουν συνειδητά προκαλέσει την επικοινωνία με τον αποστολέα των μηνυμάτων. Τα μηνύματα των spam e-mails είναι συνήθως ενημερωτικού ή διαφημιστικού περιεχομένου για προϊόντα και υπηρεσίες αμφίβολης ποιότητας. Οι εταιρείες που στέλνουν μαζικά διαφημιστικά e-mails αποκαλούνται spammers και μερικές από αυτές διακινούν το 90% των spam emails. Επίσης, έχουν την δυνατότητα να στείλουν εκατομμύρια e-mails με μια κίνηση ενώ οι εταιρείες που διαφημίζονται μέσω τέτοιων μηνυμάτων πληρώνουν βάσει συμφωνίας κάποια ποσά για κάθε παραγγελία που δέχονται. Η εύρεση των διευθύνσεων είναι μια σχετικά εύκολη διαδικασία αφού οι spammers παίρνουν τις διευθύνσεις από καταλόγους εταιρειών που διατηρούν ηλεκτρονικά καταστήματα ή χρησιμοποιούν λογισμικό τύπου harvester, που σαρώνει όλο το διαδίκτυο και συλλέγει διευθύνσεις από καταλόγους, από δωμάτια συζητήσεων κλπ. Επομένως μια τέτοια εφαρμογή είναι επόμενο να έχει και την αρνητική της λειτουργία εννοώντας πως είναι μια άριστη ευκαιρία για επιθέσεις.**5.ΕΠΙΘΕΣΕΙΣ ΣΕ ΔΙΑΔΙΚΤΥΑΚΟΥΣ ΤΟΠΟΥΣ**Στην κατηγορία των «γνήσιων» ηλεκτρονικών εγκλημάτων εντάσσονται και οι επιθέσεις στους δικτυακούς τόπους που στρέφονται κυρίως σε κυβερνητικούς οργανισμούς και υπηρεσίες. Η επίθεση μπορεί να γίνει στο περιεχόμενο μια σελίδας, το οποίο οι βάνδαλοι θα αλλοιώσουν. Παρόλα αυτά, η παραποίηση αυτή μπορεί να εντοπιστεί και στη συνέχεια να διορθωθεί. Το πρόβλημα είναι πως αν το μέγεθος της παρεμβολής είναι μεγάλο, τότε η διόρθωση θα διαρκέσει τόσο ώστε να χρειαστεί μερικές φόρες ο δικτυακός τόπος να παραμείνει κλειστός.**6.ΠΕΙΡΑΤΕΙΑ ΟΝΟΜΑΤΩΝ ΧΩΡΟΥ**Η συγκεκριμένη «γνήσια» επίθεση ήταν έντονη κυρίως στα πρώτα χρόνια του διαδικτύου, όπου οι εταιρείες δεν είχαν ακόμη κατοχυρώσει διεύθυνση στο διαδίκτυο, κάτι το όποιο πρόλαβαν να πράξουν επιτήδειοι. Έτσι είτε πωλούσαν, έναντι μεγάλου χρηματικού πόσου, τη διεύθυνση στην ενδιαφερόμενη εταιρεία, είτε χρησιμοποιώντας το κύρος του ονόματος της εταιρείας προέβαιναν σε αναρτήσεις προσβλητικού περιεχομένου. Κυβερνοσφετερισμός (cybersquatting) είναι εκείνο το ηλεκτρονικό αδίκημα κατά το οποίο ορισμένοι χρήστες του διαδικτύου κατοχυρώνουν για εμπορικούς σκοπούς Ονόματα Χώρων (Domain Names) που περιέχουν την επωνυμία γνωστών επιχειρήσεων ή σήματα φήμης με αποτέλεσμα να προκαλείται βλάβη στη φήμη των νομίμων δικαιούχων και αποκλεισμός τους από την χρήση του διαδικτύου με την επωνυμία τους ή ακόμα να πληρώνουν υπέρογκα ποσά για την μεταβίβαση της επωνυμίας της ιστοσελίδας.**7.PHISHING**“Το Phishing είναι μια νέα μέθοδος εξαπάτησης των καταναλωτών ενός οργανισμού, συνήθως κερδοσκοπικού, και συνίσταται κυρίως στην απατηλή υφαρπαγή των εμπιστευτικών πληροφοριών των καταναλωτών, όπως προσωπικά ή ευαίσθητα δεδομένα, οικονομικά δεδομένα κλπ, με σκοπό την παράνομη χρήση τους από τον Phisher για την πρόκληση βλάβης ξένης περιουσίας. Με τη βοήθεια κυρίως της απρόσκλητης εμπορικής επικοινωνίας—το γνωστό Spam—ή χρησιμοποιώντας bots2 για την αυτοματοποιημένη στόχευση των υποψήφιων θυμάτων τους ή άλλες παρόμοιες μεθόδους, οι Phishers, εμφανιζόμενοι κυρίως στο διαδίκτυο ως εκπρόσωποι ενός οργανισμού τα χαρακτηριστικά του οποίου έχουν αντιγράψει παράνομα, προβαίνουν σε δόλιες πράξεις ή παραλείψεις με τις οποίες πείθουν τα στοχευμένα θύματά τους, τα οποία ενδέχεται να είναι άδηλα, ν’ αποκαλύψουν ή εισάγουν σε σύστημα ηλεκτρονικών υπολογιστών στοιχεία της ταυτότητάς τους και εμπιστευτικές πληροφορίες με σκοπό να χρησιμοποιήσουν οι Phishers αυτές τις πληροφορίες για να προσπορίσουν στον εαυτό τους ή τρίτον παράνομο περιουσιακό όφελος προξενώντας βλάβη σε περιουσιακά στοιχεία των θυμάτων τους.”(Παπαδόπουλος, 2005)Αυτός ο τρόπος δράσης των εγκληματιών έχει παρατηρηθεί τα τελευταία χρόνια κι έχει σαν σκοπό την απόσπαση πληροφοριών των θυμάτων, με σκοπό την εκμετάλλευσή τους, όπως είναι οι κωδικοί του συστήματος, ο αριθμός πιστωτικών καρτών, κωδικοί πρόσβασης. Ο τρόπος δράσης είναι η εξαπάτηση του θύματος με παραπλανητικά e-mail. Για παράδειγμα, το θύμα θα δεχθεί ένα e-mail από μια ίσως τραπεζική υπηρεσία που θα του ζητήσει την επιβεβαίωση κωδικών στα πλαίσια μιας συντήρησης ή ανασυγκρότησης του συστήματος. Με αυτό τον τρόπο το ίδιο το ανυποψίαστο θύμα επιβεβαιώνει τα προσωπικά στοιχειά και τους κωδικούς στους επιτήδειους.“Η ονομασία Phishing αναφέρεται χρησιμοποιούμενη για πρώτη φορά το 1996 από χάκερς που έκλεβαν ή παράνομα ιδιοποιούνταν τους λογαριασμούς νομίμων χρηστών της εταιρίας America Online (AOL) με παράνομη χρήση κωδικών πρόσβασης που ανήκαν σε ανυποψίαστους χρήστες—συνδρομητές της AOL. Η πρώτη αναφορά στο Διαδίκτυο για το Phishing έγινε σε newsgroup χάκερς γνωστό ως alt.2600 τον Ιανουάριο του 1996, και η πρώτη αναφορά των μέσων ενημέρωσης στο Phishing χρονολογείται τον Μάρτιο του 1997.Οι επιθέσεις Phishing συνίστανται σ’ ένα μείγμα δόλιας χρήσης τεχνολογικών μέσων αποβλέποντας στην εξαπάτηση των καταναλωτών (technical deceit) και εφαρμοσμένων μηχανιστικών πρακτικών εξαπάτησης (social engineering practices). Σε όλες τις περιπτώσεις επιθέσεων Phishing, ο Phisher υποδύεται τον εκπρόσωπο έμπιστης πηγής πληροφοριών που, δήθεν, σχετίζεται με το θύμα, προκειμένου να πείσει το θύμα να του αποκαλύψει εμπιστευτικές πληροφορίες ή να προβεί σε πράξεις αποκάλυψης της ταυτότητας του θύματος. Συνήθως ο Phisher επικοινωνεί με το υποψήφιο θύμα του και ισχυρίζεται ότι εργάζεται σε τράπεζα ή άλλη εταιρία που μπορεί να σχετίζεται με τον λήπτη της επικοινωνίας δίνοντάς του όλες τις απαραίτητες λεπτομέρειες για την πιστοποίησή του—ονοματεπώνυμο, αριθμός εργαζομένου, τηλέφωνο για επιβεβαίωση των στοιχείων του κλπ. Εν συνεχεία, ο Phisher ενημερώνει τον λήπτη της επικοινωνίας του ότι, δήθεν, η πιστωτική του κάρτα ή ο τραπεζικός λογαριασμός του έχουν καταχωρηθεί σε λίστα παρακολούθησης για ασυνήθιστη συναλλακτική συμπεριφορά. Κατά την επικοινωνία του, ο Phisher επιχειρεί ν’ αλιεύσει, ρωτώντας το θύμα του, κάθε πληροφορία που θα μπορούσε εν συνεχεία να χρησιμοποιήσει για να απαλείψει κάθε αμφιβολία του θύματος για την ταυτότητα του προσώπου με το οποίο επικοινωνεί. Αφού επιτύχει την πλάνη του θύματος αναφορικά με την ταυτότητα του Phisher με παράσταση ψευδών γεγονότων ως αληθινών ή αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, o Phisher οδηγεί το θύμα σε πράξεις περιουσιακής διάθεσης, από τις οποίες άμεσα ή έμμεσα αποκομίζει περιουσιακό όφελος ο Phisher επί ζημία του διαθέτοντος. Η επικοινωνία στις επιθέσεις Phishing μπορεί να διεξαχθεί με ηλεκτρονικό ταχυδρομείο, με χρήση πλαστών διαδικτυακών τόπων, με εργαλεία στιγμιαίας επικοινωνίας, με τηλεφωνική επικοινωνία, και με χρήση παραβιασμένων ως προς την ασφάλειά τους διακομιστές—servers.Οι περισσότερες επιθέσεις Phishing συνήθως γίνονται με χρήση ηλεκτρονικού ταχυδρομείου. Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phishing με ηλεκτρονικό ταχυδρομείο περιλαμβάνουν:1. χρήση ηλεκτρονικής αλληλογραφίας που μοιάζει να έχει σταλεί από έμπιστη πηγή2. χρήση αντίγραφων ηλεκτρονικής αλληλογραφίας στα οποία έχουν γίνει αλλαγές σεπεριεχόμενα URLs και hyperlinks3. χρήση HTML ηλεκτρονικής αλληλογραφίας στην οποία έχουν γίνει αλλαγές σε περιεχόμεναURLs και hyperlinks4. χρήση ιών (viruses) και σκουληκιών (worms) συνημμένων σε ηλεκτρονική αλληλογραφία5. χρήση αντι-spam εργαλείων6. χρήση εξατομικευμένης ηλεκτρονικής αλληλογραφίας7. χρήση ηλεκτρονικής αλληλογραφίας με τροποποιημένη ένδειξη αποστολέα—‘Mail From:’ σε συνδυασμό με χρήση Open Mail Relays διακομιστών για την απόκρυψη της προέλευσης της ηλεκτρονικής αλληλογραφίας.Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phishing με χρήση πλαστών διαδικτυακών τόπων περιλαμβάνουν:1. εισαγωγή παραπλανητικών hyperlinks σε δημοφιλείς διαδικτυακούς τόπους2. χρήση παραπλανητικών γραφικών ή διαφημιστικών πινακίδων (banners κλπ) με σκοπό να δελεάσουν του επισκέπτες του διαδικτυακού τόπου που τα περιέχει για να κάνουν click σ’ αυτά3. χρήση διαδικτυακών bugs ικανών να ιχνηλατήσουν την επισκεψιμότητα και συμπεριφορά των καταναλωτών στο διαδικτυακό τόπο που τα περιέχει4. χρήση pop-ups ή frameless windows για τη μεταμφίεση της αληθινής προέλευσης του ηλεκτρονικού μηνύματος του Phisher5. ενσωμάτωση κακόβουλου λογισμικού κώδικα μέσα σε ιστοσελίδα ή διαδικτυακό τόπο που εκμεταλλεύεται μια γνωστή αδυναμία ασφαλείας των browsers των καταναλωτών και εγκαθιστά στο υπολογιστικό σύστημα των καταναλωτών λογισμικό της επιλογής του Phisher (π.χ. Keyloggers, Screen-grabbers, Back-doors, Trojan Horses, Wabbits, Viruses, Worms, Spyware, Exploits, Rootkits, Dialers, κλπ).6. κατάχρηση προδιαγραφών σχέσεων εμπιστοσύνης δημιουργημένων στα πλαίσια λογισμικών browsing— φυλλομετρητών ιστοσελίδων στο Διαδίκτυο—με σκοπό τη διείσδυση στα υπολογιστικά συστήματα των καταναλωτών και την τοποθέτηση εγκεκριμένων εκτελέσιμων λογισμικών προγραμμάτων—site-authorized scriptable components—στις περιοχές αποθήκευσης δεδομένων των υπολογιστικών συστημάτων των καταναλωτών” (Παπαδόπουλος, 2005)Αποπειρες Phising στις Ελληνικες Τράπεζες1.WinBank – Τράπεζα Πειραιώς2. Citibank Ελλάδος3. EFG Eurobank Ergasias4. Εθνική Τράπεζα της Ελλάδος**8.ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ**Η πειρατεία λογισμικού είναι πλέον ένα αρκετά συχνό φαινόμενο. Με τον όρο πειρατεία εννοούμε την αναπαραγωγή και διακίνηση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται με το νόμο των πνευματικών δικαιωμάτων.Οι εταιρείες παράγωγης λογισμικού στην προσπάθεια τους να αποτρέψουν την πειρατεία εφαρμόζουν τεχνολογικά μετρά όπως είναι η εισαγωγή κωδικών. Δυστυχώς αυτά τα μετρά δεν κατάφεραν να εμποδίσουν τους hackers, οι όποιοι μπορούν να απενεργοποιήσουν – σπάσουν  αυτούς τους κωδικούς (cracking) και να δράσουν ανενόχλητοι στην αντιγραφή αυτών των προγραμμάτων.Η εταιρεία λογισμικού Business Software Alliance πραγματοποιώντας μια ετήσια έρευνα το 2005,δείχνει πως το πρόβλημα της πειρατείας τα τελευταία χρόνια ποσοτικά παρουσιάζει σταθερότητα.Αυτού του είδους η πειρατεία ουσιαστικά συνιστά κλοπή λογισμικού, προγραμμάτων Η/Υ δηλαδή, και γίνεται με σκοπό να χρησιμοποιήσει ο δράστης είτε για τον εαυτό του είτε για να πουλήσει σε τρίτους το συγκεκριμένο πρόγραμμα. Κάθε πρόγραμμα Η/Υ έχει άδεια χρήσης η οποία πιστοποιείται κατά την εγκατάσταση του ή με την έναρξη της λειτουργίας του από συγκεκριμένο κωδικό που δίνεται στο νόμιμο κάτοχο του. Ο δράστης κατά το downloading (κατέβασμα) του προγράμματος από το site της επιχείρησης στην οποία ανήκει η εμπορική του εκμετάλλευση, «σπάει» αυτό το κωδικό καταφέρνοντας έτσι να έχει την πλήρη χρήση του και την δυνατότητα να το χρησιμοποιήσει όπως ο ίδιος επιθυμεί. Η οικονομική ζημιά που υφίσταται το θύμα από την παράνομη κυκλοφορία του προϊόντος είναι τόση όσος και ο αριθμός των πωλήσεων που πραγματοποιούνται με αυτό τον τρόπο.**9.ΥΠΟΚΛΟΠΗ ΑΡΧΕΙΩΝ ΥΠΟΛΟΓΙΣΤΗ**Αποκτώντας πρόσβαση σε ένα δίκτυο ο ψηφιακός εγκληματίας έχει την δυνατότητα να κλέψει, να μεταβάλλει ή να καταστρέψει αρχεία πληροφοριών ή προγραμμάτων και γενικά να κάνει οποιαδήποτε άλλη ενέργεια η οποία θα τα αχρηστέψει, μόνιμα ή προσωρινά, επιφέροντας με τον τρόπο αυτό ανυπολόγιστες οικονομικές ζημιές στα θύματα του. Υπάρχουν ειδικά προγράμματα που δίνουν την δυνατότητα σε ένα χρήστη του internet να τηλεχειρίζεται τον υπολογιστή ενός άλλου χρήστη που είναι ταυτόχρονα συνδεδεμένος στο διαδίκτυο, όταν ο πρώτος καταφέρνει να υποκλέψει την IP διεύθυνση του δευτέρου. Αυτή η δυνατότητα σημαίνει την υποκλοπή αρχείων και προγραμμάτων, την διαγραφή του σκληρού δίσκου του υπολογιστή ή ακόμα και την ενεργοποίηση περιφερειακών συσκευών, όπως για παράδειγμα Web Camera. Η κατασκοπεία είναι μια ανερχόμενη μορφή ηλεκτρονικού εγκλήματος που μπορεί να φύγει από τη σφαίρα της επίθεσης σε μεμονωμένους χρήστες και να λάβει σοβαρότερη έννοια εάν χρησιμοποιηθεί εναντίων κρατών, στρατών κ.τ.λ. |

. |