Τ.Ε.Ι. ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ (ΠΑΡΑΡΤΗΜΑΤΟΣ ΑΜΑΛΙΑΔΑΣ)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ:

ΕΠΙΔΗΜΙΟΛΟΓΙΚΑ ΜΟΝΤΕΛΑ
ΜΟΝΤΕΛΑ ΔΙΑΔΟΣΗΣ ΙΟΜΟΡΦΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ

ΕΠΙΜΕΛΕΙΑ ΑΠΟ ΤΙΣ ΦΟΙΤΗΤΡΙΕΣ:

ΚΗΡΥΚΟΥ ΠΑΝΑΓΙΩΤΑ
ΚΥΠΡΙΑΔΟΥ ΣΤΑΥΡΟΥΛΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ ΤΗΣ ΠΑΡΟΥΣΑΣ ΕΡΓΑΣΙΑΣ:

ΚΥΡΙΑ ΝΙΚΟΛΟΠΟΥΛΟΥ ΕΙΡΗΝΗ

ΑΜΑΛΙΑΔΑ 2011

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΕΥΧΑΡΙΣΤΙΕΣ

Θερμές ευχαριστίες θα θέλαμε να δώσουμε στην καθηγήτρια μας Κα. Νικολοπούλου Ειρήνη για την συνεχόμενη επίβλεψη, την καθοδήγηση, καθώς και τις πολύτιμες συμβουλές που μας παρείχε οι οποίες μας οδήγησαν στην καλύτερη κατανόηση της επιστήμης της επιδημιολογίας μα και στο πέρας της παρούσας εργασίας.

Επίσης θα θέλαμε να εκφράσουμε την ευγνωμοσύνη μας σε όλους τους καθηγητές μας από το ΑΤΕΙ Αμαλιάδος για τις πολύτιμες γνώσεις που κατάφεραν να μας μεταδώσουν όλα αυτά τα χρόνια των σπουδών μας καθώς επίσης και τις οικογένειες μας για την υποστήριξη και τη βοήθεια που μας προσέφεραν είτε οικονομικά είτε με τη ψυχολογική τους υποστήριξη.

ΠΕΡΙΛΗΨΗ

Στη παρούσα εργασία το θέμα μελέτης της είναι τα επιδημιολογικά μοντέλα και τα μοντέλα διάδοσης ιομορφικού λογισμικού.

Στη πτυχιακή μας γίνεται η παρουσίαση του κακόβουλου λογισμικού κατηγοριοποιώντας το και μελετάμε τις τεχνικές διάδοσής του, τον τρόπο λειτουργίας του, τις στρατηγικές αντιμετώπισης του καθώς και τις τεχνικές ανίχνευσης και καταστολής του. Κάνουμε σύγκριση μεταξύ του βιολογικού ιού με τον ιό των υπολογιστών και παρουσιάζουμε μερικά από τα επικρατέστερα μοντέλα διάδοσης ιομορφικού λογισμικού καθώς επίσης και τα αντίστοιχα επιδημιολογικά μοντέλα διάδοσης βιολογικών ιών θέλοντας να σας δείξουμε έτσι τον άμεσο συσχετισμό τους.

Επίσης παρουσιάζουμε αναλυτικά το PSDIR μοντέλο διάδοσης καθώς και τα αποτελέσματα που έχουνε προκύψει από τις προσομοιώσεις αυτού.

Σκοπός του παρόντος συγγράμματος είναι η επικέντρωση στην μελέτη των επιδημιολογικών μοντέλων διάδοσης ιομορφικού λογισμικού καθώς και στο τρόπο εξάπλωσης, αναγνώρισης, πρόληψης και αντιμετώπισης του κακόβουλου λογισμικού.

ABSTRACT

The subject of the study for this specific dissertation is the epidemiological models and the models of spreading virus-like software.

The dissertation is concentrating primarily on the malware presentation by categorizing it and proceeds to the study of its propagation techniques, the methods of its operation, the strategies available in order to tackle it, as well as, the techniques of its detection and suppression. Furthermore, the authors of this dissertation investigate further the comparison between the biological virus and the computer virus and they present some of the prevailing models of spreading virus-like software as well as those of epidemiological models of biological viruses' spreading in order to indicate their direct correlation.

They also present in detail the PSDIR transfer model and the results which outcome from its simulations. Scope of this assignment is the focus on the study of the epidemiological models of spreading virus-like software as well as the methods of spreading, recognizing, preventing and combating malicious software.

ΕΙΣΑΓΩΓΗ

Κανένας άνθρωπος δεν μπορεί πλέον να αμφισβητήσει το γεγονός ότι ζούμε σε μια εποχή που όλα τα πράγματα γύρω μας συσχετίζονται με την τεχνολογία. Ερχόμαστε σε επαφή καθημερινά μαζί της μιας και μας έχει γίνει απαραίτητη. Με τη χρήση τεχνολογιών μειώνεται ο χρόνος των εργασιών μας και έτσι μας διευκολύνει σίγουρα στη περαίωση αυτών. Πλέον σε όλες τις επιχειρήσεις καθώς και σε κάθε σπίτι συναντούμε μέσα τουλάχιστον ένα κουτί με λειτουργικό που εκτελεί εντολές, όπου και ονομάζεται υπολογιστής και αποτελεί από μόνος του, για το σημαντικό του έργο, αντικείμενο μελέτης και έρευνας.

Στο τρέχον σύγγραμμα θα επικεντρωθούμε στην μελέτη των επιδημιολογικών μοντέλων διάδοσης ιομορφικού λογισμικού καθώς και στο τρόπο εξάπλωσης, αναγνώρισης, πρόληψης και αντιμετώπισης του κακόβουλου λογισμικού .

Τα επιδημιολογικά μοντέλα έχουν χρησιμοποιηθεί παραδοσιακά για την κατανόηση αλλά και τη πρόβλεψη των ξεσπασμάτων των ιών στους ανθρώπινους [1] ή ζωικούς πληθυσμούς. Τα ίδια πρότυπα ισχύουν όμως και στην ανάλυση των επιδημιών των υπολογιστών [2].

Οι ομοιότητες που παρουσιάζουν μεταξύ τους οι βιολογικοί ιοί και οι ιοί των υπολογιστών είναι πολλές [3]. Οι βιολογικοί ιοί (ζωντανοί οργανισμοί) και οι ιοί των υπολογιστών βρίσκονται μέσα στον οικοδεσπότη τους και μπορούν να αναπαραχτούν μόνο όταν είναι μέσα σε αυτόν.

Επιπλέον, οι βιολογικοί ιοί εισέρχονται στον οικοδεσπότη τους παθητικά όπως μετά από μια εισπνοή ή μέσω άμεσης επαφής κτλ. Κατά αντιστοιχία και οι ιοί των υπολογιστών εισέρχονται παθητικά στον οικοδεσπότη τους όπως με την τοποθέτηση ενός μολυσμένου USB, ή σκληρού δίσκου ή. με το άνοιγμα ενός μολυσμένου ηλεκτρονικού ταχυδρομείου κτλ.

Άλλο ένα κοινό σημείο μεταξύ τους είναι ότι τόσο οι βιολογικοί ιοί όσο και οι ιοί των υπολογιστών θα πρέπει να βρίσκονται στον κατάλληλο οικοδεσπότη για να δράσουν. Έτσι ένας ιός για σκύλους δεν μπορεί να κάνει έναν άνθρωπο άρρωστο, Ομοίως όμως ένας ιός για MAC δεν μπορεί να μολύνει έναν υπολογιστή που τρέχει Linux.

Ομοιότητες επίσης συναντάμε και στις συνέπειες από τους ιούς όπου οι βιολογικοί παράγονται σε βάρος του οικοδεσπότη προκαλώντας του αδυναμία, πόνο

ή ακόμα και θάνατο. Ομοίως και οι ιοί των υπολογιστών επιβραδύνουν τη λειτουργία του υπολογιστή ή παραλλάσουν αρχεία ή ακόμα και τα καταστρέφουν.

Όσον αφορά τη διάδοσή τους και εκεί συναντάμε ομοιότητες. Τα δικτυακά σκουλήκια διαδίδονται χωρίς καμία αλληλεπίδραση των χρηστών όπως και οι κοινωνικά διαβιβαζόμενες ασθένειες όπως η γρίπη, οι οποίες έχουν τη δυνατότητα να μολύνουν ευπαθείς ομάδες.

Επίσης υπάρχουν και οι επιδημίες των υπολογιστών που μοιάζουν με τις σεξουαλικές ασθένειες. Η διάδοσή τους σχετίζεται με συγκεκριμένες πρακτικές συμπεριφοράς όπως για παράδειγμα οι λογικές βόμβες που είναι όπως το HIV, επειδή ενεργοποιείται σε άλλη ημερομηνία από αυτής της μόλυνσης.

Παρατηρώντας κανείς αυτές τις συσχετίσεις οι οποίες σε μεγάλο βαθμό επηρεάζουν τη διάδοση των ιών και κατά επέκταση τη μοντελοποίηση τους, είναι εύκολο να αντιληφθεί κανείς γιατί η επιδημιολογία η οποία αφορά κυρίως βιολογικούς οργανισμούς, αποδεικνύεται χρήσιμη για την αντιμετώπιση της εξάπλωσης του κακόβουλου λογισμικού.

Οι επιδημίες επηρέασαν και συνέχισαν να επηρεάζουν διαχρονικά την ανθρωπότητα [4] και προκάλεσαν αλλαγές έως και ανατροπές στο τρόπο ζωής των ανθρώπων. Γι αυτό και οι άνθρωποι λόγω της σοβαρότητας των συνεπειών αυτών ασχολήθηκαν από πολύ νωρίς με το κλάδο της επιδημιολογίας την οποία έθεσε ως αυτόνομο επιστημονικό κλάδο ο Ιπποκράτης το 400 π.Χ.

Στην επιδημιολογία έδωσε καινούργιο ενδιαφέρον και ώθηση το έργο του John Graunt, "Φυσικές και Πολιτικές παρατηρήσεις σχετικά με τους ρυθμούς θνησιμότητας", [5]. Κατόπιν ακολούθησαν πολλοί επιστήμονες όπως ο Daniel Bernoulli, Lowell Reed ,Ronald Ross και ο Wade Hampton Frost οι οποίοι συνδύασαν την επιδημιολογία με τα μαθηματικά, δημιουργώντας έτσι ένα καινούργιο επιστημονικό κλάδο την Μαθηματική Επιδημιολογία.

Η μεγαλύτερη συμβολή προήλθε από τους William Ogilvy Kermack και Anderson Gray Mckendrick, [6] οι οποίοι παρουσίασαν το Γενικό Επιδημιολογικό Μοντέλο (General Epidemic Model.).

Το βασικό πλεονέκτημα του γενικού επιδημιολογικού μοντέλου είναι ότι μπορεί να περιγράψει την εξέλιξη μιας επιδημίας με την χρήση διαφορετικών εξισώσεων. Η μαθηματική επιδημιολογία άκμασε τη τελευταία δεκαετία και μπόρεσε να συμπεριλάβει και άλλες πολλές παραμέτρους δημιουργώντας ακριβέστερα μοντέλα

για πολλές από τις ασθένειες που εμφανίζουν ιδιαιτερότητες στον τρόπο εξάπλωσης ή στον πληθυσμό που μολύνουν [7,8,9,10,11].

Το γενικό επιδημιολογικό μοντέλο το οποίο είναι γνωστό και ως SIR (Susceptible-Infective-Recovered) μπορεί με τις κατάλληλες υποθέσεις να περιγράψει με ακρίβεια την εξάπλωση του κακόβουλου λογισμικού.

Ο πρώτος που χρησιμοποίησε τα επιδημιολογικά μοντέλα του McKendrick σε αυτόν τον τομέα ήταν ο Kephart [2,12,13,14] ο οποίος δημιούργησε τον κλάδο της επιδημιολογίας των υπολογιστών. Την εποχή που ο Kephart δούλεψε πάνω σε αυτόν τον κλάδο βέβαια δεν είχαμε τόσο μεγάλη απειλή από την εξάπλωση του κακόβουλου λογισμικού λόγω του πρωτόγονου τρόπου εξάπλωσης των ιών που τότε βασίζονταν στην ανταλλαγή δισκετών.

Οι έρευνες για το κακόβουλο λογισμικό είχαν επικεντρωθεί στην ανάλυση του επιζήμιου κώδικα και ήταν αρκετές για εκείνη την εποχή. Η εξέλιξη της επιδημιολογίας των υπολογιστών εμφανίστηκε να επικρατεί μετά το 2000 όταν εμφανίστηκαν περισσότεροι τρόποι εξάπλωσης κακόβουλου λογισμικού όπως για παράδειγμα τα δικτυακά σκουλήκια [15,16,17,18] και τότε ήταν εμφανές ότι οι υπάρχοντες τρόποι προστασίας δεν επαρκούσαν.

Ο Staniford [19] μελέτησε τις δυναμικές εξάπλωσης του κακόβουλου λογισμικού με βάση την επιδημιολογία δίνοντας νέα εξέλιξη σε αυτό το χώρο όπου βασίζονταν στο Γενικό Επιδημιολογικό Μοντέλο.

INTRODUCTION

Nobody can now dispute the fact that we live in an era where all things around us are related to technology. We come into daily contact with it since it has become necessary.

By using technology we reduce the time needed for our tasks and enable us to complete them. Nowadays, in every company and organization and in every home we encounter at least a box with an operating system that performs orders which is called computer and that alone, for its important job, consists a subject of study and research.

In the current task we will focus on the study of the epidemiological models of spreading virus-like software as well as the methods of spreading, recognizing, preventing and combating malicious software.

Epidemiological models have traditionally been used for understanding and anticipating the outbreak of the viruses in human [1] or animal populations. The same standards apply, however, in the analysis of epidemics of computers [2].

There are numerous similarities between biological and computer viruses [3]. Biological viruses (living organisms) and computer viruses are located inside their host and can be reproduced only inside it.

In addition, biological viruses enter the host passively, such as, for instance, after an inhalation or by direct contact, etc. In correspondence, computer viruses enter their host passively such as, for example, by putting an infected USB, or a hard disk or the opening of an infected e-mail, etc.

Another common point between them is that both biological and computer viruses must be located in an appropriate host to act. So, a virus for dogs cannot make a person sick, in the same way a virus for the MAC cannot infect a computer running Linux.

We also encounter similarities on the effects from the viruses where the biological are produced against the host causing weakness, pain or even death. Likewise, computer viruses slow down the operation of the computer or change files or even destroy them.

As far as their spread is concerned, we also find similarities. The Web worms are spread without any interaction by users, as well as socially transmitted diseases such as the flu, which are able to infect vulnerable groups.

There are also computer viruses which are similar to sexual diseases. These are associated with specific behavioral practices such as logic bombs, like HIV, because they are activated on another date from that of their contamination.

By observing these correlations which greatly influence the spread of viruses and additionally their modeling, it is easy for someone to understand the reason why the epidemiology, which is mainly about biological organisms, is proved to be useful for facing the spread of malicious software.

Epidemics have influenced and continued to influence humankind over time [4] and caused changes and turnovers on the way of people's life. This is why people, because of the seriousness of these consequences, were involved very early with the epidemiology branch, which has been set as a separate branch by Hippocrates in 400 BC.

John Graunt's research, "Natural and Political observations on mortality rates" [5] gave to the epidemiology a new interest and boost. After that, many scientists followed, such as Daniel Bernoulli, Lowell Reed, Ronald Ross and Wade Hampton Frost who combined the epidemiology with mathematics, and they created the new scientific branch of Mathematical Epidemiology. The largest contribution came from William Ogilvy Kermack and Anderson Gray Mckendrick, [6] who presented the General Epidemiological Model (General Epidemic Model).

The main advantage of the general epidemiological model is that it can describe the development of an epidemic by using different equations. The mathematical epidemiology flourished during the last decade and could include many other parameters, by creating more accurate models for many of the diseases which appear special features in the way of spreading or the population which is infected [7,8,9,10,11].

The general epidemiological model which is known as SIR (Susceptible-Infective-Recovered) may, with the appropriate assumptions, describe the spread of malicious software accurately.

The first person who used McKendrick's epidemiological model in this era was Kephart [2,12,13,14] who created the field of epidemiology of computers. At the time when Kephart worked on this subject, of course we did not have such a large threat from the spread of malicious software because of the primitive way of spreading the viruses, which was then based on the exchange of floppy disks.

Investigations on the malicious software which had focused on the analysis of harmful code were enough for those times. The development of the epidemiology of computers appeared to prevail after 2000 when more ways of spreading malicious software appeared, such as the Web worms [15,16,17,18] and then it was evident that the existing methods of protection were not sufficient.

Staniford [19] studied the dynamics of spreading malicious software based on epidemiology, giving new development in this area which was based on the General Epidemiological model.

ΚΕΦΑΛΑΙΟ 1

1.1 ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ ΤΩΝ ΔΙΚΤΥΩΝ

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Το δίκτυο των υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο ή περισσότερους υπολογιστές ή ανεξάρτητες περιφερειακές συσκευές [20]. Δύο υπολογιστές θεωρούνται διασυνδεμένοι όταν μπορούν να ανταλλάξουν μεταξύ τους πληροφορίες.

ΣΚΟΠΟΣ ΤΩΝ ΔΙΚΤΥΩΝ

Τα δίκτυα δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής (αρχεία, δεδομένα, προγράμματα).

Πόροι του συστήματος μπορούν να είναι είτε το υλικό (hardware) π.χ. (υπολογιστές, εκτυπωτές, σκληροί δίσκοι) είτε το λογισμικό (software) π.χ. (προγράμματα εφαρμογών, υπηρεσίες, εφαρμογές).

Τα προγράμματα, τα δεδομένα και οι συσκευές π.χ. (σκληροί δίσκοι, εκτυπωτές) είναι διαθέσιμα σε οποιονδήποτε είναι συνδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση. Με τον τρόπο αυτό επιτυγχάνεται η εξοικονόμηση των χρημάτων, η αύξηση της απόδοσης του συστήματος, ο κεντρικός έλεγχος και η εύκολη επεκτασιμότητα.

Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων.

Επιπλέον ανεξάρτητα της τεχνολογίας, ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετική θέση.

ΠΡΩΤΟΚΟΛΛΟ ΔΙΚΤΥΩΝ

Το πρωτόκολλο των δικτύων είναι ένα σύνολο από κανόνες που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου και είναι υπεύθυνο για το πώς διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών.

Το Internet δεν είναι ένα απλό δίκτυο, αλλά ένα διαδίκτυο. Χρειάζεται επομένως ένα σύνολο από κανόνες που να καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα (όπως π.χ. τα δίκτυα ευρείας περιοχής, τα τοπικά δίκτυα, τα αστικά δίκτυα).

1.2 ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο άρχισε σε πειραματικό στάδιο στα τέλη της δεκαετίας του 1960 από την Advanced Research Agency (ARPA) του Αμερικανικού Υπουργείου Αμύνης.

Το 1969 το πειραματικό δίκτυο είχε 4 online κόμβους συνδεδεμένους με κυκλώματα των 56 kbps. Η τεχνολογία αυτή αποδείχτηκε αξιόπιστη και οδήγησε σε δύο δίκτυα στρατιωτικά το MINET της Ευρώπης και το MILNET της ΗΠΑ. Ακολούθησαν αρκετές ακόμη μελέτες και προσπάθειες πειραματικών δικτύων μέχρι και την ίδρυση του Διαδικτύου όπως και είναι γνωστό στις μέρες μας.

Το διαδίκτυο είναι παγκοσμίας κλίμακας δίκτυο (World Wide Web), το οποίο συνδέει ετερογενή, ως προς τη τεχνολογία υλοποίησης και πρωτόκολλα επικοινωνίας δίκτυα.

Στη συνήθη περίπτωση συνδέονται τα τοπικά δίκτυα (Local Area Networks) που επικοινωνούν μεταξύ τους με το γνωστό πρωτόκολλο TCP/IP. Το IP πρωτόκολλο αναλαμβάνει τη διασύνδεση ετερογενών δικτύων και τη διευθυνσιοδότηση των κόμβων διασύνδεσης (Network Layer στο μοντέλο ISO/OSI), ενώ το TCP πρωτόκολλο αφορά στην αξιόπιστη μεταφορά της πληροφορίας μεταξύ των κόμβων (Transport Layer στο μοντέλο ISO/OSI).

Κατά τον σχεδιασμό του IP (Internet Protocol-Διαδικτυακό Πρωτόκολλο), στόχος ήταν η δημιουργία ενός πρωτοκόλλου που θα διασύνδεε ετερογενή δίκτυα με τέτοιο τρόπο ώστε οι υπολογιστές να είναι μοναδικά σχεδιασμένοι, να μπορούν να ανταλλάσουν δεδομένα με κοινή μορφοποίηση και να μεταδίδουν δεδομένα χωρίς να

γνωρίζουν στοιχεία για τη δομή και τη μορφή των δικτύων που ανήκουν οι παραλήπτες. Αρχικά τα δίκτυα που διασυνδέθηκαν αφορούσαν πανεπιστήμια ή ερευνητικά κέντρα και για αυτό το λόγο ποτέ δεν τέθηκε θέμα ασφάλειας στο σχεδιασμό του πρωτοκόλλου.

Όμως με τη τεράστια εξάπλωση του διαδικτύου αναγκαστικά εμφανίστηκε το ζήτημα της ασφάλειας καθώς και οι τρόποι αντιμετώπισής της.

Παραδείγματα αυτής της διαπίστωσης είναι το πρωτόκολλο Secure Sockets Layer (SSL) που λειτουργεί στο επίπεδο μεταφοράς και το πρωτόκολλο HTTP που λειτουργεί στο επίπεδο της εφαρμογής.

Παρά τις όποιες επιτυχημένες προσπάθειες το πρόβλημα παραμένει. Αυτό συμβαίνει γιατί ακόμα και αν χρησιμοποιείτε προστασία στο επίπεδο εφαρμογής υπάρχει αρκετή πληροφορία στην επικεφαλίδα του πακέτου, στο οποίο ενσωματώνονται τα δεδομένα και για αυτό παραμένουν ευάλωτα στις επιθέσεις. Με τη χρήση προγραμμάτων ανάλυσης της δικτυακής κυκλοφορίας (sniffers) είναι δυνατό να αποκαλυφθούν οι διεργασίες και τα συστήματα που ανταλλάσουν πληροφορίες.

Θα πρέπει να προστεθεί επίσης ότι το κόστος προστασίας από κάθε εφαρμογή ξεχωριστά είναι υψηλότερο σε σχέση με την παροχή της ασφάλειας.

Οι περισσότερες εταιρείες, οργανισμοί, ιδιώτες που συμμετέχουν στο Διαδίκτυο, παρόλα αυτά φαίνονται να έχουν ένα αίσθημα ασφάλειας αγνοώντας τους ανυπολόγιστους κινδύνους που παραμονεύουν. Πιστεύουν πως η εκάστοτε ιστοσελίδα δεν αποτελεί στόχο και ότι έχουνε ληφθεί τα απαραίτητα μέτρα. Δεν υπολογίζουν όμως πως η τεχνολογία μεταβάλλεται με την πάροδο του χρόνου και τα εργαλεία των εισβολέων προσαρμόζονται ανάλογα. Επιπροσθέτως η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών δεν είναι εφικτή καθώς το μεγαλύτερο μέρος των δεδομένων που διακινείτε δεν είναι κρυπτογραφημένο. Με αυτόν τον τρόπο μια ιστοσελίδα μπορεί να πέσει θύμα μιας επίθεσης συλλέγοντας πληροφορίες για αυτή με διάφορα εργαλεία όπως ένα packet sniffer.

Επιπλέον ένας ακόμα παράγοντας που πρέπει να ληφθεί υπόψη στην επιδείνωση του προβλήματος είναι η ραγδαία ανάπτυξη των υπηρεσιών πάνω από το Διαδίκτυο με τη χρήση των πολύπλοκων εφαρμογών. Έτσι η επιλογή του λειτουργικού συστήματος του εκάστοτε εξοπλισμού θα πρέπει να γίνεται με γνώμονα και την ασφάλεια και όχι μόνο την επίδοση, την ταχύτητα, την ευκολία χρήσης ,την

τιμή την διαχείριση ή την υποστήριξη. Συνήθως η αρχική διαμόρφωση του λειτουργικού που προσφέρει ο κατασκευαστής είναι ακατάλληλη για τη διασφάλιση της ασφάλειας, πόσο μάλλον για την ενίσχυσή της.

Γίνεται τέλος σαφής η ανάγκη τόσο για εξειδικευμένα δικτυακά πρωτόκολλα ασφαλείας, όσο και για εξειδικευμένο προσωπικό που θα συντηρούν την ασφάλεια ενός διαδικτυακού τόπου.

1.3 ΤΑ ΤΡΩΤΑ ΣΗΜΕΙΑ

Με τον όρο τρωτό σημείο εννοούμε ένα αδύναμο σημείο που εκμεταλλεύεται κάποιος που θέλει να βρει ένα τρόπο να εισβάλει χωρίς εξουσιοδότηση σε ένα υπολογιστικό/δικτυακό σύστημα. Όταν με τη χρήση του τρωτού σημείου γίνει εισβολή, τότε μιλάμε για περιστατικό παραβίασης της ασφάλειας. Τα τρωτά σημεία οφείλονται σε σχεδιαστικά και κατασκευαστικά λάθη, αλλά και άλλους παράγοντες που αναλύουμε παρακάτω [21,22,23,24].

1) Ελαττώματα στο λογισμικό ή στο σχεδιασμό πρωτοκόλλων

Μέσω των πρωτοκόλλων προσδιορίζονται οι κανόνες και οι μέθοδοι, με τις οποίες μπορούν να επικοινωνήσουν μεταξύ τους οι υπολογιστές. Αν υπάρχει σχεδιαστικό σφάλμα στο πρωτόκολλο, υπάρχει μεγάλη πιθανότητα να εξελίχθη σε τρωτό σημείο, ασχέτως με την ποιότητα υλοποίησης του πρωτόκολλου.

Όταν σχεδιάζετε το λογισμικό χωρίς να περιλαμβάνετε η ασφάλεια του στις αρχικές προδιαγραφές, ενδέχεται το τμήμα που προστίθεται εκ των υστερών για την προστασία των χρηστών, να μην έχει την αναμενόμενη αλληλεπίδραση και να προκύπτουν νέα τρωτά σημεία.

2) Αδυναμίες στην υλοποίηση του λογισμικού ή του πρωτοκόλλου

Το λογισμικό μπορεί να περιέχει ευάλωτα σημεία, επειδή δεν βρεθήκαν πριν την τελική του έκδοση και έτσι οι εισβολείς του να μπορούν να αναζητήσουν ελαττώματα, (τρωτά σημεία) με ειδικά εργαλεία. Μερικές περιπτώσεις ευάλωτων σημείων θα μπορούσαν να είναι ο ελλιπείς έλεγχος του λειτουργικού συστήματος, η ανυπαρξία των ελέγχων για την αντιμετώπιση των εσωτερικών λαθών.

Κάνοντας χρήση αδυναμιών λοιπόν στο λογισμικό οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε πόρους χωρίς να χρειάζονται την απαραίτητη εξουσιοδότηση από το σύστημα με χρήση κάποιων κακόβουλων λογισμικών.

Παραδείγματος χάριν, ένα πρωτόκολλο για ηλεκτρονικό ταχυδρομείο μπορεί να υλοποιηθεί με τέτοιο τρόπο που να επιτρέπει την σύνδεση στο mail port του συστήματος που θα γίνει η επίθεση και να ζητήσει να εκτελέσει κάποιες συγκεκριμένες εντολές .Ο εισβολέας μπορεί να γράψει στο πεδίο «κάτι άλλο», αντί τη σωστή διεύθυνση, με τις συγκεκριμένες εντολές και να ζητήσει το password file του συστήματος δίχως να χρειάζεται καν λογαριασμός σε αυτό.

3) Αδυναμίες στη διαμόρφωση των συστημάτων και δικτύων

Σε αυτήν την περίπτωση τα τρωτά σημεία προέρχονται από τον τρόπο που εγκαθίστανται και χρησιμοποιούνται από τα πρωτόκολλα ή το λογισμικό. Συνήθως εγκαθίστανται με προκαθορισμένες παραμέτρους που οι εισβολείς μπορούν να εκμεταλλευτούν.

Οι διαχειριστές των συστημάτων και οι χρήστες μπορεί να μην αλλάξουν τις προκαθορισμένες παραμέτρους με αποτέλεσμα το σύστημα να εμφανίζει τρωτά σημεία.

Οι παράμετροι εγκατάστασης είναι προκαθορισμένοι, γεγονός που οι εισβολείς το γνωρίζουν και το εκμεταλλεύονται.

4) Ομοιογένεια των υπολογιστικών συστημάτων

Ένας ακόμα λόγος που συνεισφέρει στην μεγιστοποίηση του προβλήματος της παραβίασης της ασφάλειας των υπολογιστικών συστημάτων και των δικτύων, είναι το γεγονός ότι όλοι σήμερα τρέχουμε τα ίδια λειτουργικά συστήματα και χρησιμοποιούμε τους ίδιους τύπους δικτύων.

Πριν δύο δεκαετίες υπήρχαν διαφορετικά είδη υπολογιστών, λειτουργικών και δικτύων. Είχαμε τα minis, τα mainframes και τα PC’s όλα με μία μεγάλη ποικιλία διαφορετικών λειτουργικών συστημάτων και υποστηριζόμενων δικτυακών πρωτοκόλλων.

Ένας τύπος για παράδειγμα ενός εχθρικού κώδικα (malicious code) θα μπορούσε να επιτεθεί και να επηρεάσει μόνο ένα περιορισμένο πληθυσμό υπολογιστικών συστημάτων και αυτό εξαιτίας της διαφορετικότητας που υπήρχε.

Σήμερα όμως τα πράγματα έχουν αλλάξει. Η λεγόμενη επανάσταση των υπολογιστών έχει επιφέρει μία τεράστια συνένωση σε ότι αφορά τις πλατφόρμες και τους τύπους των δικτύων και των πρωτοκόλλων. Φαίνεται ότι όλα λειτουργούν με βάση τα Windows ή το Unix και χρησιμοποιούν το πρωτόκολλο TCP/IP για να επικοινωνούν.

Τι μπορεί όμως να σημαίνει αυτό; Ένα ομογενοποιημένο υπολογιστικό περιβάλλον αποτελεί εύφορο έδαφος ειδικά για malicious code. Επειδή το υπολογιστικό μας 'οικοσύστημα' έχει μικρή ποικιλία, ένας και μόνο τύπος ενός malicious code θα μπορούσε να έχει τεράστιο αντίκτυπο στο υπολογιστικό μας σύστημα.

5) Συνδυασμός δεδομένων και εντολών

Ένας από τους κύριους λόγους όπου οι ιοί έχουν γνωρίσει τεράστια ανάπτυξη αποτελεί ο τρόπος με τον οποίο οι υπολογιστές συνδυάζουν διάφορα είδη πληροφοριών. Δύο πολύ γενικές κατηγορίες περιεχομένων είναι: τα δεδομένα και οι εκτελέσιμες εντολές. Τα δεδομένα είναι αναγνώσιμα αλλά όχι και εκτελέσιμα. Ο υπολογιστής εκτελεί πράξεις πάνω σε αυτού του είδους τα περιεχόμενα.

Από την άλλη μεριά οι εκτελέσιμες εντολές 'λένε' στον υπολογιστή ενός χρήστη να προβεί σε κάποια ενέργεια, (το τι να κάνει δηλαδή). Αν μπορούσαμε να κρατήσουμε αυτούς τους δύο τύπους πληροφοριών χωριστά τότε δεν θα είχαμε και τόσο μεγάλο πρόβλημα με τον εχθρικό κώδικα (malicious code).

Συνδυάζοντας τα δεδομένα και τις εκτελέσιμες εντολές, οποιοσδήποτε τύπος πληροφοριών στο σύστημά μας θα μπορούσε να περιέχει εχθρικό κώδικα. Ο εισβολέας περιμένει την ευκαιρία κάποιος χρήστης να το τρέξει και να πάρει τον έλεγχο του συστήματος.

6) Ανάγκη για συνδεσιμότητα

Όλοι οι υπολογιστές συνδέονται μεταξύ τους είτε το θέλουμε είτε όχι εφόσον έχουμε εγκλωβιστεί σε ένα μικρό αριθμό από πρωτόκολλα και λειτουργικά συστήματα, τα οποία έχουμε εμείς μειώσει και ακριβώς τότε απαιτούμε και μεγαλύτερη συνδεσιμότητα.

7) Η κακή χρήση του ηλεκτρονικού ταχυδρομείου

Το ηλεκτρονικό ταχυδρομείο αποτελεί μία από τις πιο διαδεδομένες και χρησιμοποιούμενες υπηρεσίες του διαδικτύου. Είναι το κύριο μέσο επικοινωνίας μεταξύ των χρηστών και αποτελεί ένα από τα βασικά εργαλεία μιας εταιρείας ή ενός οργανισμού.

Αποτελεί όμως και τον κύριο εκπρόσωπο μέσω του οποίου διαδίδεται κακόβουλο λογισμικό με τη μορφή επισυναπτόμενων αρχείων. Ο χρήστης ανοίγει τα αρχεία που δέχεται χωρίς να τα ελέγχει με αποτέλεσμα να μολύνεται το σύστημα. Η μη σωστή χρήση του αποτελεί ένα τρωτό σημείο το οποίο μπορεί να οδηγήσει στη παραβίαση της ασφάλειας του δικτύου.

1.4. ΣΥΝΗΘΙΣΜΕΝΕΣ ΑΠΕΙΛΕΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Αποκάλυψη των συνθηματικών

Τα συνθηματικά είναι ένας από τους πιο διαδεδομένους τρόπους για να αναγνωρίζεται ένας χρήστης από το σύστημα. Παρά την ευρεία τους διάδοση και πολύχρονη χρήση, υπάρχει μια σειρά από ζητήματα που σχετίζονται με τη χρήση και την αποτελεσματικότητά τους.

Τα συνθηματικά μπορεί να αποκαλυφθούν [26] είτε μέσω της εξαντλητικής αναζήτησης όπως για παράδειγμα δοκιμή όλων των πιθανών συνδυασμών του κωδικού, είτε με χρήση λιστών με συχνά χρησιμοποιημένα συνθηματικά, είτε με αξιοποίηση προκαθορισμένων συνθηματικών, καθώς και με πληθώρα άλλων μεθόδων.

Οι επιθέσεις που αφορούν αποκάλυψη συνθηματικών διευκολύνονται από τους γρήγορους υπολογιστές και τα γρήγορα δίκτυα.

Πλοήγηση

Ένας νόμιμος χρήστης ενός συστήματος ή ένας εισβολέας που έχει αποκτήσει πρόσβαση στο σύστημα ψάχνει σε αυτό για να βρει πληροφορίες που θα του δώσουν περισσότερα προνόμια. Η αναζήτηση μπορεί να γίνεται σε σελίδες μνήμης ή σε απροστάτευτα αρχεία κτλ.

Αυτό το εκμεταλλεύονται μετά κάποιοι κακόβουλοι χρήστες προκειμένου να αποκτήσουν πρόσβαση στο σύστημα και να το κάνουν δικό τους.

Επίσης συχνό είναι και το φαινόμενο όπου χρήστες επισκέπτονται σελίδες με πορνογραφικό περιεχόμενο με αποτέλεσμα στις περισσότερες των περιπτώσεων να εγκαθίσταται εν αγνοία του χρήστη ένας dialer που κάνει κλήσεις σε απομακρυσμένες περιοχές. Ο λογαριασμός τηλεφώνου που θα πρέπει να πληρώσεις μετά είναι αρκετά αυξημένος.

Αντιποίηση ή μεταμφίεση

Ένα παράδειγμα προγραμμάτων από μεταμφιέσεις είναι διάφοροι ιστότοποι που προσποιούνται ότι είναι οι τράπεζες συνήθως στέλνοντας email στους ανυποψίαστους χρήστες για να μπορέσουν να συγκεντρώσουν πληροφορίες με σκοπό να τις χρησιμοποιήσουν προς όφελος τους.

Οι χρήστες λοιπόν χωρίς να έχουν ιδέα για το τι κρύβεται από πίσω εισάγουν τους κωδικούς πρόσβασης τους το όποιο αντί να τους συνδέει τους καταγράφει τους κωδικούς τους σε μια βάση ώστε να τους βρει ο δημιουργός του.

Στη περίπτωση αυτή ο χρήστης πιστεύει ότι αλληλεπιδρά με μια οντότητα [40] (δηλ. πρόγραμμα, υπηρεσία, χρήστη). Στην πραγματικότητα όμως δεν αλληλεπιδρά με αυτήν αλλά με κάποια άλλη που προσποιείται ότι είναι η πραγματική.

Road apple

Road Apple είναι μία τεχνική που χρησιμοποιείται συχνά από τους hackers. Αυτό που κάνουν είναι να τοποθετούν σε μία δισκέτα ή σε ένα CD ένα κακόβουλο πρόγραμμα, να της δίνουν ένα κατάλληλο όνομα και να την αφήνουν τυχαία πάνω σε ένα γραφείο με την ελπίδα ότι κάποιος θα την χρησιμοποιήσει.

Η επίθεση αυτή βασίζεται στην περιέργεια του θύματος. Παράδειγμα μίας τέτοιας επίθεσης είναι το εξής: Κάποιος βρίσκει από το διαδίκτυο το λογότυπο μίας εταιρείας, δημιουργεί βάσει αυτού μία ετικέτα που κινεί την περιέργεια (πχ. Μισθοί υπαλλήλων) και το αφήνει σε κάποιο γραφείο της εταιρείας.

Εάν κάποιος περίεργος υπάλληλος την χρησιμοποιήσει, τότε ο υπολογιστής του θα μολυνθεί με κακόβουλο λογισμικό.

Εφαρμογές instant messaging

Οι χρήστες χρησιμοποιούν αυτές τις εφαρμογές προκειμένου να έρθουν σε επικοινωνία με φίλους, να στείλουν ή να δεχθούν αρχεία, μηνύματα.

Στις εφαρμογές αυτές οι εισβολείς προσπαθούν να ξεγελάσουν τα προγράμματα που φιλτράρουν τις πληροφορίες που εισέρχονται και εξέρχονται από ένα δίκτυο και να περάσουν δεδομένα που μπορεί να περιέχουν κακόβουλο λογισμικό. Ωστόσο οι χρήστες δεν συνειδητοποιούν τους κινδύνους που κρύβουν αυτές οι εφαρμογές και την πιθανή καταστροφή που μπορεί να επιφέρουν.

Ποτέ δεν μπορούμε να είμαστε σίγουροι για το ποιος είναι στο άλλο άκρο της γραμμής. Μπορεί πράγματι να είναι κάποιος φίλος μας όπως όμως μπορεί να είναι και ένας κακόβουλος χρήστης. Οι περισσότερες από αυτές τις εφαρμογές περιέχουν τρωτά σημεία, τα οποία μπορούν να εκμεταλλευτούν οι κακόβουλοι χρήστες και να προκαλέσουν σοβαρά προβλήματα στο σταθμό εργασίας μας.

Αυτό γίνεται γιατί ένα αρχείο που θα πάρουμε μπορεί να είναι μολυσμένο και έτσι θα οδηγήσει με τη σειρά του τη μόλυνση του συστήματος και του δικτύου γενικότερα.

Downloading από άγνωστες και επισφαλείς τοποθεσίες

Το κατέβασμα αρχείων από άγνωστες και επισφαλείς τοποθεσίες με ταυτόχρονη χρησιμοποίηση των συστημάτων και του δικτύου μιας εταιρείας ή ενός οργανισμού, μπορεί να οδηγήσει σε επιβλαβή αποτελέσματα: Μπορεί να οδηγηθούν σε καταστάσεις στις οποίες αρχεία και δεδομένα χάνονται, καταστρέφονται ή ακόμα και σε μερικές περιπτώσεις παραποιούνται.

Αυτό αποτελεί σήμερα ένα συχνό φαινόμενο, καθώς πολλές φορές οι χρήστες κατεβάζουν από το διαδίκτυο αρχεία χωρίς να δίνουν τη κατάλληλη προσοχή.

Έλλειψη χρήσης-ενημέρωση προγραμμάτων προστασίας.

Πολλοί από τους χρήστες δεν εγκαθιστούν προγράμματα προστασίας (antivirus) από το κακόβουλο λογισμικό ή κάποιο τείχος προστασίας (firewall), με αποτέλεσμα να μολύνονται από κάποιο ιό ή να παραβιάζεται η ασφάλεια του συστήματος τους από κάποιο επίδοξο hacker. Αυτό μπορεί να οδηγήσει στη συνέχεια στη παραβίαση της ασφάλειας ολόκληρου του δικτύου που χρησιμοποιεί ο χρήστης.

Αξιοποίηση προγραμματιστικών σφαλμάτων

Σε πολλές περιπτώσεις, προγραμματιστικά σφάλματα σε εφαρμογές ή σε λειτουργικά συστήματα επιτρέπουν σε επίδοξους εισβολείς να υποβαθμίσουν την ασφάλεια των υπολογιστικών συστημάτων.

Μολυσμένα αφαιρούμενα μέσα

Τα αφαιρούμενα μέσα μεταφοράς όπως είναι για παράδειγμα τα CD (οπτικοί δίσκοι), οι σκληροί δίσκοι, οι USB συσκευές μεταφοράς δεδομένων ή άλλα παρόμοια μέσα θεωρούνται σαν μία πιθανή πηγή μόλυνσης και υποκλοπής σημαντικών δεδομένων.

Τα διάφορα είδη κακόβουλου λογισμικού χρησιμοποιούν τέτοια μέσα προκειμένου να διαδίδονται και να προκαλούν κινδύνους σχετικά με την εγκατάσταση ενός τέτοιου μέσου σε ένα σταθμό εργασίας.

Συχνά παρατηρείται το φαινόμενο κάποιος χρήστης να εγκαθιστά ένα τέτοιο μέσο το οποίο έχει κάποια αρχεία μολυσμένα, με αποτέλεσμα να μολύνεται το σύστημα και να περνά αυτό και στο υπόλοιπο δίκτυο. Απαραιτήτος θα πρέπει να γίνετε έλεγχος π.χ. μέσω κάποιου antivirus πριν το άνοιγμα αυτών.

Καταπακτή (trapbors)

Πρόκειται για τροποποιήσεις συστημάτων που παρέχουν πρόσβαση στο σύστημα χωρίς ιδιαίτερες επιπτώσεις. Μολονότι συνήθως εγκαθίστανται από τους εισβολείς μετά από μια επιτυχημένη επίθεση και μια μελλοντική χρήση, δεν είναι σπάνια η περίπτωση να εγκατασταθούν και από τους ίδιους τους κατασκευαστές ως << δίοδοι ταχείας πρόσβασης >> για την περίπτωση που κάτι πάει στραβά.

Διάσημα προγράμματα αυτής της κατηγορίας είναι οι τροποποιημένες εκδόσεις του login που επιτρέπουν είσοδο με δικαιώματα σε συγκεκριμένα user names καθώς και το back office σε περιβάλλον pc που δίνει σε απομακρυσμένους χρηστές δικαιώματα διαχειρίσεις στον δικό μας υπολογιστή.

Πλαστογράφηση

Πρόκειται για τη μη εξουσιοδοτημένη τροποποίηση δεδομένων με αποτέλεσμα την δημιουργία πλαστογραφημένων εκδόσεων τους. Η τροποποίηση μπορεί να γίνει είτε στα αποθηκευμένα δεδομένα με αποτέλεσμα τη μόνιμη παραποίηση τους, είτε στα δεδομένα όταν αυτά μεταδίδονται μέσω δικτύου.

Παρεμπόδιση παροχής υπηρεσιών

Η υποβάθμιση της άξιας ενός υπολογιστικού συστήματος μπορεί να επέλθει χωρίς κάποια φυσική καταστροφή ή φθορά δεδομένων, αλλά επίσης και με την ανάθεση σε αυτό ενός ιδιαίτερα επαχθούς έργου που να εξαντλεί τους πόρους του, καθιστώντας το ανίκανο να προσφέρει το έργο που του έχει ανατεθεί. Έτσι ένας

εξυπηρετητής ηλεκτρονικού ταχυδρομείου μπορεί να καταστεί «άσχετος» αν του ανατεθεί να διακινήσει 50.000 μηνύματα των 200Mbytes έκαστο, καθώς σίγουρα θα εξαντληθεί ο αποθηκευτικός του χώρος. Επίσης ένας εξυπηρετητής www θα είναι επίσης «άχρηστος» αν «βομβαρδισθεί» με δυσανάλογο προς τις προδιαγραφές του αριθμό αιτήσεων.

Η παρεμπόδιση παροχής υπηρεσιών συνίσταται, συνήθως στην υποβολή πολλών αιτήσεων που η κάθε μια είναι μεμονωμένα «νομότυπη», αλλά συνδυάστηκα έχουν άσχημα αποτελέσματα. Η παρεμπόδιση παροχής υπηρεσιών αποσκοπεί στη στέρηση από τους νόμιμους χρηστές την δυνατότητα τους να εξυπηρετηθούν από το υπολογιστικό σύστημα.

Μη ηθελημένη καταστροφή

Ένας χρήστης μπορεί να πραγματοποιήσει ατυχείς ενέργειες π.χ. να διαγράψει ένα (χρήσιμο) αρχείο ή να σβήσει ένα σύνολο εγγράφων από μια βάση δεδομένων. Ως ενέργειες που υποβαθμίζουν την αξία του συστήματος τα περιστατικά αυτά πρέπει να καλύπτονται από τους μηχανισμούς ασφάλειας.

Μολονότι προφανώς δεν είναι δυνατόν να στερήσουμε από τους χρηστές τα βασικά τους προνομία για να αποτραπούν οι ατυχείς ενέργειες, πρέπει στο σχέδιο ασφάλειας να μεριμνούμε για μεθόδους αντιμετώπισης των περιστατικών αυτών .

Παρά την πληθώρα των δυνατών επιθέσεων στην ασφάλεια και τις σημαντικές συνέπειες που μπορεί αυτές να έχουν, πολλές φορές οι επιθέσεις αυτές δεν αναφέρονται στους υπευθύνους, στην διοίκηση ή σε κατάλληλους φορείς στο internet

ΟΙ ΛΟΓΟΙ ΜΗ ΑΝΑΦΟΡΑΣ ΕΙΝΑΙ ΚΥΡΙΩΣ ΟΙ ΑΚΟΛΟΥΘΟΙ [24]:

1) Η αναφορά ενός προβλήματος δίνει ιδέες σε άλλους επίδοξους εισβολείς. Έτσι εάν διαρρεύσει μια πληροφορία ότι «ο τάδε υπολογιστής έχει μια αδυναμία σ' αυτήν την υπηρεσία», αρκετοί εισβολείς μπορεί να προσπαθήσουν να εκμεταλλευτούν το συγκεκριμένο κενό ή να εντοπίσουν και αλλά.

2) Η αρνητική δημοσιότητα διώχνει πελάτες και δυσαρεστεί τους μετόχους. Για παράδειγμα, αν μια τράπεζα ανακοινώσει ότι κάποιος «έσπασε» το διαδικτυακό σύστημα εξυπηρέτησης πελατών, οι καταθέτες της τράπεζας θα είναι πολύ διστακτικοί στο να αξιοποιήσουν την υπηρεσία αυτήν, ενώ οι μέτοχοι στην Σοφοκλέους πιθανόν να μπουν στην κόκκινη ζώνη.

3) Πολλές φορές η σημασία ενός συμβάντος υποβαθμίζεται και δεν τίθεται στις πραγματικές της διαστάσεις, που πιθανώς αυτό γίνεται λόγω άγνοιας των ενδεχόμενων συνεπειών. Η μη αναφορά των περιστατικών πάντως δίνει την ψευδαίσθηση ότι «όλα πάνε καλά» και έτσι δεν βοηθά στην δημιουργία (ή αναμόρφωση) και εφαρμογή ενός καλύτερου σχεδίου ασφάλειας.

Κακόβουλο λογισμικό

Η κατηγορία αυτή αποτελεί στην εργασία μας ένα κεφάλαιο από μόνο του μελέτης οπότε και θα αναφερθούμε αργότερα με πολύ λεπτομέρεια στο κακόβουλο λογισμικό.

1.5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως μπορούμε να διαπιστώσουμε από όλα τα παραπάνω, το κρίσιμο στοιχείο σε καθένα από αυτά είναι ο χρήστης. Μπορούμε να πούμε αποτελεί το τρωτό σημείο του διαδικτύου. Αυτός είναι ο πιο υπεύθυνος για τις ενέργειες που εκτελεί στο σύστημα και κατ' επέκταση στο διαδίκτυο.

Και επειδή σε καμία περίπτωση δεν μπορούμε να εξαλείψουμε το χρήστη, αυτό που μπορούμε και πρέπει να κάνουμε είναι να του παρέχουμε τα κατάλληλα εφόδια ώστε να συνειδητοποιήσει τους κινδύνους που απορρέουν από κάθε ενέργειά του στο διαδίκτυο. Να συνειδητοποιήσει δηλαδή ότι κάθε πράξη του πιθανώς μπορεί να έχει και κάποιο αρνητικό αποτέλεσμα, άρα θα πρέπει να σκέφτεται τις ενέργειες που κάνει πριν εξαπατηθεί με τους προαναφερθείσας τρόπους.

ΚΕΦΑΛΑΙΟ 2

2.1 ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι χρήστες σε ένα δικτυακό περιβάλλον δέχονται υπηρεσίες και αποθηκεύουν ή ανταλλάσσουν πληροφορίες δημιουργώντας έτσι από πλευρά ασφαλείας την εξασφάλιση των απαιτήσεων με εμπιστευτικότητα ακεραιότητα και διαθεσιμότητα των δεδομένων και των υπηρεσιών.

Να σημειώσουμε όμως πως για να είναι δυνατή η επίτευξη αυτών των στόχων θα πρέπει να εξασφαλισθούν κάποιες συνιστώσες [24,72]:

1) Θα πρέπει να γίνεται διακρίβωση ταυτότητας (χρηστών - συστημάτων), έτσι ώστε το σύστημα να είναι βέβαιο για τη ταυτότητα του χρήστη με τον οποίο έρχεται σε επαφή και από την άλλη πλευρά ο χρήστης να είναι βέβαιος ότι έχει συνδεθεί με το σύστημα που επιθυμεί.

2) Είναι απαραίτητο να υπάρχουν αξιόπιστοι μηχανισμοί έλεγχου εξουσιοδότησης/προσπέλασης, έτσι ώστε να εξασφαλίζεται ότι τα κατάλληλα δικαιώματα έχουν δοθεί στους κατάλληλους χρήστες και ότι ο καθένας χρήστης ο οποίος χρησιμοποιεί το σύστημα δεν μπορεί να υπερβεί τα προνόμια των δικαιωμάτων του.

3) Είναι χρήσιμο να γίνονται αποτελεσματικοί έλεγχοι των δικαιωμάτων του κάθε χρήστη προκειμένου να αντιμετωπίζονται οι περιπτώσεις όπου τα δικαιώματα που τους έχουνε παραχωρηθεί για κάποιους συγκεκριμένους λόγους εξασφαλίζονται και δεν χρησιμοποιούνται και δεν τα χρησιμοποιούν για άλλο σκοπό.

4) Είναι αναγκαίο να υπάρχουν άψογα πρωτόκολλα, λειτουργικά και εφαρμογές τα οποία είναι τα εργαλεία που θα επιτρέψουν την εφαρμογή των πολιτικών ασφαλείας.

2.2 ΤΕΧΝΙΚΕΣ ΔΙΑΣΦΑΛΙΣΕΙΣ

Οι τεχνικές διασφαλίσεις [27] αποσκοπούν στο να εξασφαλίσουν ότι ένα σύστημα είναι ασφαλές ή στην ανάδειξη και έγκαιρη διόρθωση των τρωτών σημείων του συστήματος, πριν αυτά γίνουν αντικείμενο εκμετάλλευσης από εισβολείς.

Η πρώτη προσέγγιση η όποια συνίσταται από τους μηχανικούς λογισμικού, είναι η υιοθέτηση καλών προγραμματιστικών και πρακτικών, καθώς και εκτεταμένες δοκιμές του προϊόντος λογισμικού. Η προσέγγιση αυτή δεν είναι αποτελεσματική καθώς τα προϊόντα λογισμικού που κυκλοφορούν στην αγορά θεωρητικά τουλάχιστον έχουν αναπτυχτεί σωστά και ελέχθη διεξοδικά, χωρίς αυτό να αποτρέπει την ύπαρξη προβλημάτων ασφάλειας.

Μια δεύτερη προσέγγιση είναι η ανάλυση του συστήματος για εντοπισμό πιθανών αδυναμιών. Εδώ γίνετε συλλογή από γνώστες αδυναμίες και τεχνικές εκμετάλλευσής τους, ώστε να εντοπιστούν οι αδυναμίες έγκαιρα και να διορθωθούν από το προσωπικό ασφάλειας πριν τις εντοπίσουν και τις εκμεταλλευτούν οι εισβολείς. Μια τέτοια δοκιμή θα δείξει ενδεχόμενος την ύπαρξη αδυναμιών αλλά ωστόσο δεν εγγυάται την απουσία τους.

Και η τρίτη προσέγγιση είναι η προσπάθεια πρόληψης ή ανίχνευσης των προσπαθειών για εκμεταλλεύσεις των αδυναμιών των συστημάτων.
Προκειμένου να αντιμετωπισθούν τα ζητήματα αυτά είναι δυνατόν να υιοθετηθούν στατικές ή δυναμικές μέθοδοι, όπως συνοψίζεται στον πίνακα:

	Ανάλυση (στατική μέθοδος)	**Ανίχνευση επιβολή πολιτικών (δυναμική μέθοδος)**
Προγραμματιστικά σφάλματα	Ανάλυση πρωτογενούς κώδικα για ανίχνευση σφαλμάτων	Παρακολούθηση συμπεριφοράς και επιβολή ασφαλών προτύπων για τα προγράμματα
Σφάλματα ολοκλήρωσης	Ανάλυση διαμόρφωσης συστήματος για εντοπισμό αδυναμιών	Ανάλυση διαμόρφωσης συστήματος για εντοπισμό αδυναμιών

ΠΙΝΑΚΑΣ 1. ΣΤΑΤΙΚΟΙ ΚΑΙ ΔΥΝΑΜΙΚΟΙ ΜΕΘΟΔΟΙ

Η ανάλυση του πρωτογενούς κώδικα για ανίχνευση σφαλμάτων (security audit) είναι μία διαδικασία όπου ειδικοί περί την ασφάλεια αναλύουν γραμμή προς γραμμή τον πρωτογενή κώδικα των συστημάτων για εντοπισμό πιθανών ευπαθειών.

Δεδομένου όμως ότι η ανάλυση γίνεται από ανθρώπους πάντα υπάρχει ο κίνδυνος σφάλματα να «ξεφύγουν» και έτσι προϊόντα που έχουν περάσει από πολλαπλές αναλύσεις ασφάλειας κώδικα διαπιστώθηκε στο τέλος ότι έχουν προβλήματα ασφάλειας.

2.3 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ (INTRUSION DETECTION SYSTEMS IDS).

Το IDS [21,29,30] είναι software ή hardware συστήματα τα οποία αυτοματοποιούν τη διαδικασία παρακολούθησης όλων των events που συμβαίνουν σε ένα υπολογιστικό σύστημα ή σε ένα δίκτυο αναλύοντας τα σε βάθος για την ανακάλυψη τυχών προβλημάτων ασφαλείας. Εισβολές (intrusions), προέρχονται είτε από επιτιθέμενους που έχουν πρόσβαση σε εσωτερικά συστήματα μέσω του internet, είτε από εσωτερικούς χρήστες των συστημάτων που προσπαθούν να αποκτήσουν παραπάνω προνόμια από όσα έχουν, είτε από εσωτερικούς χρήστες που χρησιμοποιούν με λανθασμένο τρόπο τα προνόμια που τους έχουν δοθεί.

2.3.1 ΣΚΟΠΟΣ ΤΩΝ IDS

Δύο είναι βασικοί σκοποί των συστημάτων intrusion detection [29,30,]

1. **Ανακάλυψη των στοιχείων του επιτιθεμένου (Accountability)**

Η φράση που χαρακτηρίζει το σκοπό αυτόν είναι ¨θεωρούμε ικανός να αντιμετωπίσω περιστατικά παραβίασης της ασφαλείας του δικτύου όσο γνωρίζω ποιος είναι υπεύθυνος για τα περιστατικά αυτά¨. Η ανακάλυψη των στοιχείων του επιτιθέμενου είναι αρκετά δύσκολη υπόθεση στις περιπτώσεις των δικτύων TCP/IP, όπου οι επιτιθέμενοι μπορούν να τροποποιήσουν την πραγματική διεύθυνση προέλευσης των πακέτων που στέλνουν στο δίκτυο. Γενικά θεωρείται δύσκολο να επιτευχθεί αυτός ο σκοπός όταν δεν υπάρχουν μηχανισμοί πιστοποίησης και αναγνώρισης των χρηστών.

2. **Response**

Με την έννοια response εννοούμε την ικανότητα αναγνώρισης ενός event ως δείγμα επίθεσης ως προς το εσωτερικό δίκτυο και την άμεση αντίδραση των συστημάτων έτσι ώστε να ελαχιστοποιηθεί ο κίνδυνος εμφάνισης νέων προβλημάτων. Η χαρακτηριστική φράση που συνδέεται με αυτόν τον σκοπό είναι η εξής: “Δεν μας ενδιαφέρει η προέλευση της επίθεσης από την στιγμή που υπάρχει η δυνατότητα αναγνώρισης και μπλοκαρίσματός της.”

2.4 IPSEC

Η IEFT γνώριζε για χρόνια ότι η ασφάλεια στο Διαδίκτυο ήταν ανεπαρκής. Μετά την τεράστια εξάπλωση που γνώρισε το Διαδίκτυο και τη σημασία που απέκτησε στον τομέα των επιχειρήσεων και του ηλεκτρονικού εμπορίου η ασφάλεια έγινε μία από τις πιο απαιτητικές ανάγκες.

Για να καλύψει τις ανάγκες αυτές η IEFT δημιούργησε το IP Security Working Group [31] με στόχο να σχεδιάσει μια αρχιτεκτονική ασφαλείας και τα αντίστοιχα πρωτόκολλα.

Η προσθήκη της ασφάλειας δεν ήταν εύκολη υπόθεση επειδή είχε ξεσπάσει ένας πόλεμος σχετικά με το σημείο που θα έπρεπε να τοποθετηθεί. Οι περισσότεροι ειδικοί στην ασφάλεια θεωρούν ότι για να υπάρχει πραγματικά ασφάλεια η κρυπτογράφηση και οι έλεγχοι ακεραιότητας θα πρέπει να γίνονται παντού. Δηλαδή η διεργασία προέλευσης θα κρυπτογραφεί ή και θα προστατεύει την ακεραιότητα των δεδομένων, και μετά θα τα στέλνει στη διεργασία προορισμού όπου θα αποκρυπτογραφούνται ή και θα επαληθεύονται.

Οποιεσδήποτε τροποποιήσεις γίνουν ανάμεσα σε αυτές τις διεργασίες θα μπορούν να εντοπιστούν. Το πρόβλημα με αυτή τη προσέγγιση είναι ότι απαιτεί την αλλαγή όλων των εφαρμογών ώστε να ασχολούνται με την ασφάλεια.

Η αντίθετη άποψη είναι ότι οι χρήστες δεν κατανοούν την ασφάλεια και δεν θα είναι σε θέση να τη χρησιμοποιήσουν σωστά και ότι κανείς δεν θέλει να τροποποίηση τα υπάρχοντα προγράμματα με κανένα τρόπο, έτσι το επίπεδο του δικτύου θα πρέπει

να πιστοποιεί την ταυτότητα ή και να κρυπτογραφεί τα πακέτα χωρίς να αναμιγνύεται ο χρήστης.

Μετά από χρόνια έντονων μαχών, αυτή η προσέγγιση απέκτησε αρκετή υποστήριξη ώστε να ορίζει ένα πρότυπο ασφαλείας επιπέδου δικτύου. Το αποτέλεσμα αυτού του πολέμου ήταν μια σχεδίαση που ονομάζεται IPSec.

2.5 ΤΟΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (FIREWALLS)

Η σύνδεση ενός συστήματος στο διαδίκτυο δίνει τη δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Η δυνατότητα αυτή δεν είναι πάντα επιθυμητή αφού οι εμπιστευτικές πληροφορίες που βρίσκονται στον υπολογιστή μας μπορεί να διαρρεύσουν.

Έτσι για να υπάρχει ένα είδος διαχωρισμού ανάμεσα στο intranet του οργανισμού και το internet, υπάρχει μια ομάδα συστημάτων που δημιουργεί ένα τοίχος προστασίας ανάμεσα στα δυο δίκτυα.

Η χρήση του firewalls συμβάλει στην ενίσχυση της ασφάλειας αλλά δεν την εγγυάται. Ο σωστός σχεδιασμός της παραμέτρου και της διαμόρφωσης των συστημάτων είναι απαραίτητος για την σωστή λειτουργία τους. [25,32,33].

FIREWALL	
ΜΠΟΡΕΙ ΝΑ ΠΡΟΣΦΕΡΕΙ	***ΔΕΝ ΜΠΟΡΕΙ ΝΑ ΠΡΟΣΤΑΤΕΨΕΙ***
Ένα σημείο εφαρμογής των αποφάσεων που αφορούν την ασφάλεια.	Από νεωτερικούς χρηστές που σκοπεύουν να επιτεθούν.
Ένα μέσο για τη πολιτική ασφάλειας	Συνδέσεις που δεν περνούν από αυτό
Ένα τρόπο καταγράφεις της δικτυακής κίνησης	Εντελώς νέους τύπους απειλών επιθέσεων
Ένα φράγμα σε ανεπιθύμητες επιθέσεις	Από ιούς αποδοτικά
	Από λάθη στην διαμόρφωση

ΠΙΝΑΚΑΣ 2 FIREWALL

Παρόλα αυτά έχουμε μεγαλύτερη ασφάλεια στο δίκτυο με την χρήση firewall. Όταν μιλάμε για ασφάλεια θα πρέπει να λάβουμε υπόψη μας το βαθμό πολυπλοκότητας του συστήματος μας, την ευκολία χρήσης και το κόστος που απαιτείτε για την προστασία.

Επειδή το firewall αλληλεπιδρά με το internet χρειάζεται ιδιαίτερη προσοχή στη εγκατάσταση του και στη σωστή διαμόρφωση του.

Το τοίχος προστασίας είναι ένας μηχανισμός [34] που χρησιμοποιούμε για να ελέγχει την πρόσβαση από και προς το δίκτυο με σκοπό τη προστασία του συστήματος μας.

Με την χρήση του περιορίζετε η επικοινωνία ανάμεσα στο προστατευμένο δίκτυο (intranet, υπολογιστής μας) καθώς και σε ένα άλλο οποιοδήποτε δίκτυο. Δηλαδή λειτούργει ως μια πύλη από την όποια παίρνουν όλοι από και προς το εξωτερικό δίκτυο. Θα μπορούσαμε να το παρομοιάσουμε σαν ένα τοίχος ανάμεσα σε ένα εσωτερικό δίκτυο και ένα εξωτερικό.

Είναι αυτό που ελέγχει τις πύλες από τις οποίες θα περάσει η συγκεκριμένη πληροφορία. Το ποιο δύσκολο κομμάτι στην υλοποίηση του είναι η εύρεση κριτηρίων που θα προσδιορίσουν ποια πακέτα επιτρέπονται να περάσουν στο εσωτερικό του δικτύου και ποια όχι.

.

ΚΕΦΑΛΑΙΟ 3

3.1 ΕΧΘΡΙΚΟΣ ΚΩΔΙΚΑΣ (HOSTILE CODE)

Εχθρικό κώδικα (Hostile Code) ονομάζουμε: ένα σύνολο από εντολές που τρέχουν σε ένα σύστημα-υπολογιστή και τον αναγκάζουν να εκτελεί αυτά που θέλει ο εισβολέας.

Ο εχθρικός κώδικας μπορεί να τοποθετηθεί-υλοποιηθεί σε οποιαδήποτε γλώσσα υπολογιστή με μόνο περιορισμό τη φαντασία του εισβολέα και η οποία στις περισσότερες περιπτώσεις τείνει να είναι μεγάλη. Οι εισβολείς έχουν αλλάξει μία μεγάλη ποικιλία από γλώσσες υπολογιστή, προγράμματα καθώς και άλλα σύνολα εντολών προκειμένου να δημιουργήσουν malicious code.

Γενικά, όταν ο εχθρικός κώδικας τοποθετείται στον υπολογιστή ενός χρήστη, το γεγονός αυτό και μόνο δίνει στον εισβολέα σημαντικά δικαιώματα όσον αφορά στον έλεγχο του συστήματος αυτού του χρήστη. Ο κώδικας λοιπόν αυτός μπορεί να δράσει σαν ένας κατάσκοπος που επιτρέπει στον εισβολέα να κάνει πράξη τα σχέδιά του.

Αν ένας εισβολέας λοιπόν μπορεί να εγκαταστήσει εχθρικό κώδικα στον υπολογιστή μας ή να μας ξεγελάσει ώστε να κατεβάσουμε ένα πρόγραμμα που έχει μολυνθεί, τότε ο υπολογιστής μας δρα σαν μια μαριονέτα στα χέρια του εισβολέα που εκτελεί τις εντολές του. Την ίδια στιγμή το σύστημά μας παύει να εκτελεί τις δικές μας εντολές.

3.2 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ (MALICIOUS SOFTWARE).

Το κακόβουλο λογισμικό [24] είναι οποιοσδήποτε κώδικας που προστίθεται, αλλάζεται, ή αφαιρείται από ένα σύστημα λογισμικού προκειμένου να προκληθεί σκόπιμα ζημιά ή να παραβιαστεί η προοριζόμενη λειτουργία του συστήματος χωρίς τη συγκατάθεση του ιδιοκτήτη. (Με τον όρο παραβίαση εννοούμε την απόπειρα παραβίασης της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας του συστήματος.)

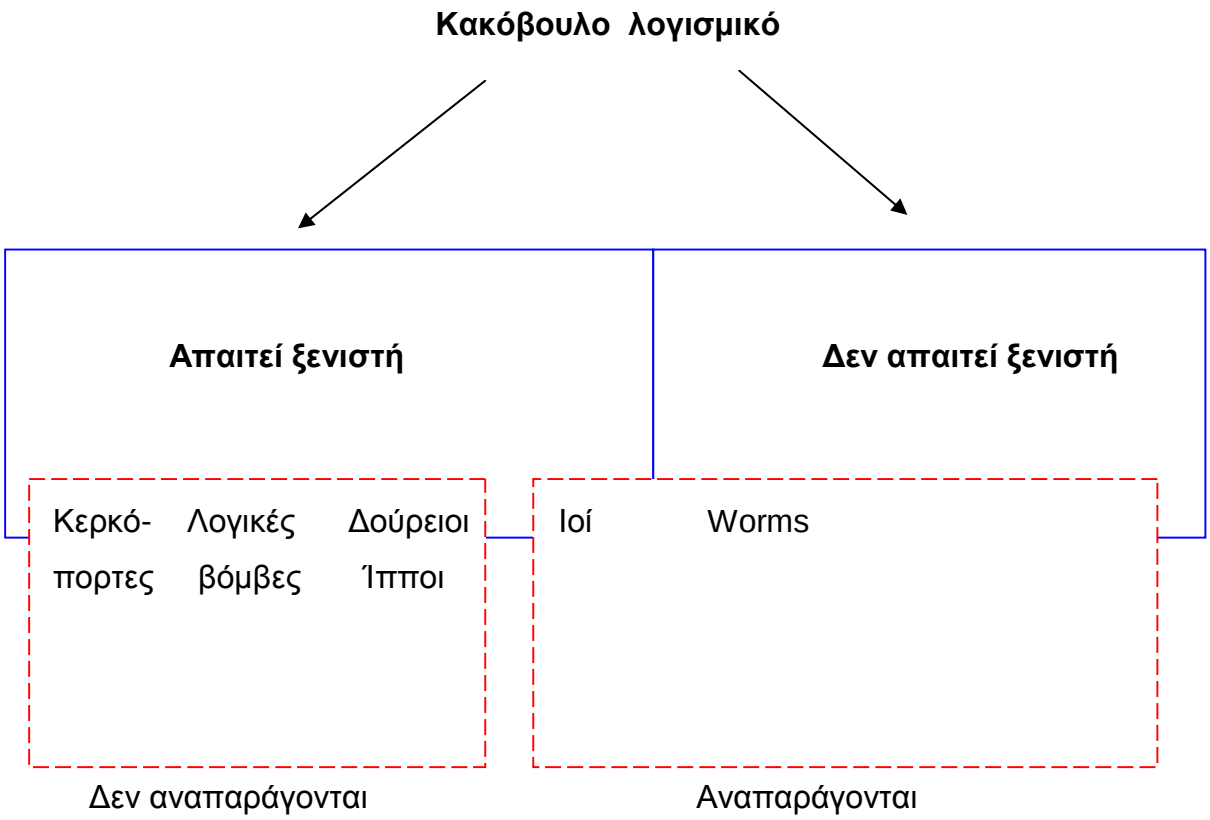
Το Κακόβουλο λογισμικό είναι ένας γενικός όρος που χρησιμοποιείται από τους επαγγελματίες της πληροφορικής και σημαίνει μια ποικιλία μορφών εχθρικού κώδικα του προγράμματος. Όμως οι απλοί χρήστες λανθασμένα βέβαια

χρησιμοποιούν τον όρο "ιός" ως catch-all φράση για να συμπεριλάβει όλα τα είδη κακόβουλου λογισμικού.

Δυστυχώς για εμάς και κυρίως για αυτούς που ασχολούνται με την ασφάλεια των υπολογιστικών συστημάτων και δικτύων, σήμερα συναντάμε μία μεγάλη ποικιλία από κακόβουλο λογισμικό, τα είδη του οποίου θα αναφέρουμε και αναλύσουμε στις αμέσως επόμενες παραγράφους.

3.3 ΕΙΔΗ ΑΠΕΙΛΩΝ

Τα είδη απειλών με τα οποία θα ασχοληθούμε σε αυτό το κεφάλαιο και που μας ενδιαφέρει ο τρόπος με τον οποίο διαδίδονται και αντιμετωπίζονται, είναι αυτά που καλούμε σήμερα κακόβουλο λογισμικό, μαζί με τις διάφορες παραλλαγές αυτού που συναντούμε.



ΣΧΗΜΑ 1 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ –ΑΠΑΙΤΕΙ ΞΕΝΙΣΤΗ- ΔΕΝ ΑΠΑΙΤΕΙ ΞΕΝΙΣΤΗ.

Επίσης το κακόβουλο λογισμικό χωρίζεται σε δυο κατηγορίες.
Στο παρακάτω σχήμα μπορούμε να δούμε τι περιλαμβάνει η κάθε κατηγορία:

ΠΙΝΑΚΑΣ 3 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ – ΙΟΜΟΡΦΙΚΟ - ΜΗ ΙΟΜΟΡΦΙΚΟ

ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ				
Ιομορφικό Κακόβουλο Λογισμικό	**Μη Ιομορφικό Κακόβουλο Λογισμικό**			
Ιοί	Δούρειος Ίππος	Λογικές Βόμβες	Κερκόπορτες ή Πίσω Πόρτες	Worms

3.4 ΔΙΑΦΟΡΕΣ ΙΟΜΟΡΦΙΚΟΥ ΜΕ ΜΗ ΙΟΜΟΡΦΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ

Το ιομορφικό λογισμικό έχει χαμηλή πιθανότητα μόνιμης ζημιάς στο σύστημα μας καθώς και στοχευμένης απόπειρας επίθεσης. Επίσης έχει χαμηλή δυσκολία εντοπισμού και ο μηχανισμός αναπαραγωγής του γίνετε χωρίς την ανθρωπινή παρέμβαση.

Ενώ το μη ιομορφικό λογισμικό έχει υψηλότερη πιθανότητα ζημιάς στο σύστημα μας καθώς και στοχευμένης απόπειρας επίθεσης, ο μηχανισμός αναπαραγωγής του χρειάζεται ανθρώπινη παρέμβαση και η δυσκολία εντοπισμού του είναι πολύ πιο δύσκολη από το ιομορφικό λογισμικό.

	Ιομορφικό Κακόβουλο Λογισμικό	**Μη Ιομορφικό Κακόβουλο Λογισμικό**
Μόνιμη ζημιά στο σύστημα	Χαμηλή πιθανότητα	Υψηλή πιθανότητα
Μηχανισμός αναπαραγωγής	Αναπαραγωγή χωρίς ανθρώπινη παρέμβαση	Αναπαραγωγή με ανθρώπινη παρέμβαση
Δυσκολία εντοπισμού	Χαμηλή	Υψηλή
Στοχευμένη απόπειρα επίθεσης	Χαμηλή πιθανότητα	Υψηλή πιθανότητα

ΠΙΝΑΚΑΣ 4 ΔΙΑΦΟΡΕΣ ΙΟΜΟΡΦΙΚΟΥ ΜΕ ΜΗ ΙΟΜΟΡΦΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ

3.5 ΙΟΣ (VIRUS)

Ο ιός είναι ένας κώδικας υπολογιστή, ο οποίος μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη.

Ο ιός προσπαθεί να διαδοθεί από υπολογιστή σε υπολογιστή παραδείγματος μέσω του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB σε ένα κεντρικό πρόγραμμα. Μπορεί να προκαλέσει ζημιές στο υλικό, το λογισμικό ή τα δεδομένα.

Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και τα τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα.

Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το ηλεκτρονικό ταχυδρομείο, την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων τους είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές μάλιστα φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου τους.

Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημιά αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη με την μορφή κειμένου, βίντεου, ή ηχητικών μηνυμάτων μερικές φορές αρκετά χιουμοριστικών.

Όμως, ακόμη και αυτοί οι "καλάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη των υπολογιστών.

Καταρχάς καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να

οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων.

Σύμφωνα με τη θεωρητική ανάλυση του Cohen, ο μόνος σίγουρος τρόπος για να εμποδίσουμε τη διάδοση μιας μόλυνσης που οφείλεται σε έναν ιό είναι να απαγορεύσουμε την ύπαρξη διαμοιράσιμων πόρων και τη ροή πληροφορίας στο σύστημα μας. Τότε όμως στην ουσία θα καταλήξουμε να έχουμε ένα σύστημα που δεν λειτουργεί.

Αφού πρώτα εγκατασταθεί σε ένα υπολογιστικό σύστημα, ο ιός αποκτά, προσωρινά, τον έλεγχο του λειτουργικού συστήματος. Όταν συμβεί αυτό, οποτεδήποτε ο μολυσμένος υπολογιστής έρθει σε επαφή με μη μολυσμένο πρόγραμμα, το πρόγραμμα αυτό μολύνεται με την εισαγωγή στον κώδικά του ενός αντιγράφου του ιού.

Είναι φανερό ότι με τη διαδικασία αυτή η μόλυνση μπορεί να διαδοθεί από υπολογιστή σε υπολογιστή μέσω ανυποψίαστων χρηστών που είτε ανταλλάσσουν δισκέτες είτε προγράμματα μέσω δικτύου.

Το περιβάλλον του δικτύου μάλιστα, με τη δυνατότητα που παρέχει στους χρήστες για προσπέλαση εφαρμογών και υπηρεσιών του συστήματος που βρίσκονται σε απόμακρους υπολογιστές, αποτελεί ιδεώδες περιβάλλον για τη διάδοση των ιών.

Ένας ιός μπορεί να κάνει οτιδήποτε σε οποιοδήποτε πρόγραμμα και εκτελείται κρυφά, όταν εκτελείται το πρόγραμμα – φορέας.

Από τη στιγμή που εκτελείται ένας ιός, μπορεί να επιτελέσει οποιαδήποτε λειτουργία, όπως,(π.χ. διαγραφή αρχείων και προγραμμάτων.) Ένα από τα κύρια χαρακτηριστικά των ιών είναι η αδυναμία τους να σταθούν σαν αυτόνομα εκτελέσιμα.

3.5.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ - ΟΙ ΠΡΩΤΟΙ ΙΟΙ

Υπάρχουν πολλές και διαφορετικές απόψεις για το πότε ακριβώς δημιουργήθηκε καθώς και για το ποιος ήταν ο πρώτος ιός. Είναι ωστόσο γνωστό ότι οι Univac 1108 και IBM 360/370 [38] είχαν δεχθεί ιούς (συγκεκριμένα τους "Pervanting Animal" και "Christmas tree") οπότε μπορούμε να πούμε σχεδόν σίγουρα πως ο πρώτος ιός δημιουργήθηκε κάπου στις αρχές του 1970 (παρόλο που ο όρος «ιός» ήρθε πολύ αργότερα -πιθανόν το 1983 από τον Fred Cohen.

Τη περίοδο εκείνη (τέλη του 1960 με αρχές του 1970) έκαναν περιοδικά την εμφάνιση τους διάφορα προγράμματα με την ονομασία Rabbit, τα οποία κλωνοποιούσαν τον εαυτό τους και καταλάμβαναν πόρους του συστήματος μειώνοντας κατά συνέπεια την παραγωγικότητα του.

Αυτά πιθανότατα δεν αντιγράφονταν από σύστημα σε σύστημα και ήταν αυστηρά τοπικά φαινόμενα (λάθη ή φάρσες από τους προγραμματιστές συστημάτων που συντηρούσαν αυτούς τους υπολογιστές.) Το πρώτο περιστατικό που θα μπορούσε να ονομαστεί «επιδημία ενός ιού υπολογιστών» συνέβη στον Univac 1108 και ήταν ο "Pervading Animal" ο οποίος συγχωνευόταν στο τέλος εκτελέσιμων αρχείων.

Το πρώτο πρόγραμμα καταπολέμησης ιών (antivirus) ήρθε στις αρχές της δεκαετίας του '70 όταν μετά την εμφάνιση του ιού Creeper (τα συστήματα στα οποία είχε εισχωρήσει τύπωναν το μήνυμα: " I' M THE CREEPER: CATCH ME IF YOU CAN.")

Το 1981 κάνει την εμφάνιση του ο elkcloner (ο οποίος δημιουργήθηκε από έναν 15χρονο μαθητή) που δρούσε στους Apple II υπολογιστές, ενώ ο πρώτος ιός για IBM-Pc ήρθε το 1986, ο λεγόμενος Brain vírus [38] που προκάλεσε πανδημία.

Ο τελευταίος ο οποίος σύμφωνα με τα λεγόμενα των δημιουργών του (δύο αδέλφια από το Πακιστάν) είχε σαν σκοπό την μέτρηση της «πειρατείας» στην χώρα τους, εξαπλώθηκε στιγμιαία σε ολόκληρο τον κόσμο και ήταν ο πρώτος που είχε stealth ικανότητες.

1987-1990	Εμφάνιση των πρώτων ιών που μεταδίδονταν με τη βοήθεια των δισκετών (μέσω της περιοχής εκκίνησης των δισκετών)
1990-1995	Άρχισαν να μεταδίδονται οι ιοί με τη βοήθεια των αρχείων.
1995-1998	Εμφάνιση των πρώτων ιών μακρο-εντολών που μεταδίδονταν με τα έγγραφα κειμένου.
1998-2001	Εμφάνιση των πρώτων ιών που μεταδίδονταν με τα μηνύματα του ηλεκτρονικού ταχυδρομείου.
2001 - …	Κατακόρυφη αύξηση των ιών που μεταδίδονταν μέσω του διαδικτύου.

ΠΙΝΑΚΑΣ 5 Η ΕΞΕΛΙΞΗ ΤΩΝ ΙΩΝ

3.5.2 Ο ΚΥΚΛΟΣ ΖΩΗΣ ΕΝΟΣ ΙΟΥ

1. Δημιουργία του ιού. Παλιότερα απαιτούνταν μεγάλες τεχνικές γνώσεις για την δημιουργία ιών, σήμερα όμως η δημιουργία τους αποτελεί μια σχετικά εύκολη υπόθεση .

2. Αναπαραγωγή του ιού. Ένας καλός ιός προκείμενου να μην γίνει αντιληπτός δεν προκαλεί καταστροφές αμέσως μόλις εγκατασταθεί σε κάποιο μηχάνημα αλλά φροντίζει για την αποστολή του σε άλλα μηχανήματα, αναβάλλοντας το καταστροφικό του έργο για αργότερα.

3. Πρόκληση καταστροφών. Ο ιός αρχίζει το καταστροφικό του έργο και προκαλεί διάφορες ζημιές στο υλικό και το λογισμικό του συστήματος που μολύνουν.

4. Αναγνώριση. Οι εταιρείες και οι οργανισμοί παρακολούθησης ιών (π.χ. International Computer Security Association) αναγνωρίζουν την ύπαρξη των νέων ίων που κυκλοφορήσαν.

5. Αντιμετώπιση. Οι εταιρείες παραγωγής λογισμικού καταπολέμησης των ιών, ενσωματώνουν στα προϊόντα τους τη δυνατότητα αναγνώρισης και εξουδετέρωσης του ιού.

6. Εξάλειψη. Με την πάροδο του χρόνου και τη διάδοση νέων εκδόσεων του antivirus software ο ιός γίνεται όλο και πιο σπάνιος, ενώ σε μερικές περιπτώσεις μπορεί να εξαφανιστεί εντελώς.

7. Αναγέννηση. Ένα σημαντικό ποσοστό των νέων ιών αποτελεί στην πραγματικότητα ανακύκλωση μέρους του κώδικα άλλων παλαιότερων. Έτσι, ακόμη και αν ένας ιός έχει καταπολεμηθεί στην αρχική του μορφή, νέες μεταλλάξεις του μπορούν να κυκλοφορούν για πολλά χρόνια.

3.5.3 ΚΑΛΟΙ ΙΟΙ

Ένα θέμα που έχει προβληματίσει τους επιστήμονες του κλάδους είναι το αν κάποιο πρόγραμμα που έχει όλα τα χαρακτηριστικά του ιού μπορεί να χρησιμοποιηθεί για καλό σκοπό. Όπως χαρακτηριστικά μας λένε οι επιστήμονες αυτό συμβαίνει σε πολλές περιπτώσεις.

Ως παραδείγματα ¨καλών¨ ιών έχουμε να σας αναφέρουμε τα παρακάτω:

1. Ο ¨αντιβιοτικός¨ ιός, ο οποίος μπορεί να ανιχνεύσει και να σκοτώσει τους κακούς ιούς.
2. Ο ιός ¨συμπιεστής¨, που εντοπίζει τα αρχεία που χρησιμοποιούμε πιο σπάνια και τα συμπιέζει.
3. Ο ιός ¨κρυπτογράφος¨, ο οποίος εγκαθίσταται στον σκληρό δίσκο και τον κρυπτογραφεί βάση ενός συνθηματικού που του δίνει ο χρήστης και αυτό γίνεται προκειμένου να κρατήσει τα αρχεία να είναι αθέατα από τα αδιάκριτα βλέμματα.
4. Ο ιός ¨συντηρητής¨ που είναι υπεύθυνος στο να συντηρεί κάποιες λειτουργίες στο σύστημα. π.χ. διαγραφή προσωρινών αρχείων.

Όπως και να έχει όμως σε κάθε περίπτωση, η τοποθέτηση μας πάνω στο ζήτημα ύπαρξης καλών ιών θα πρέπει να είναι αρνητική και αυτό γιατί συντρέχουν τόσο τεχνικοί λόγοι, όσο και ψυχολογικά ζητήματα.

3.5.4 ΟΙ ΙΟΙ ΣΥΝΗΘΩΣ ΔΙΑΙΡΟΥΝΤΑΙ ΣΕ ΔΥΟ ΒΑΣΙΚΕΣ ΣΥΝΙΣΤΩΣΕΣ :

1. το Μηχανισμό Διάδοσης

2. το «Ωφέλιμο Φορτίο» τους.

ΜΗΧΑΝΙΣΜΟΣ ΔΙΑΔΟΣΗΣ

Ο μηχανισμός διάδοσης, είναι ο τρόπος με τον οποίο ο ιός εξαπλώνεται. Κατά τις πρώτες μέρες της εμφάνισής τους, οι ιοί μεταδίδονταν κυρίως μέσω δισκετών ή άλλων παρόμοιων αποθηκευτικών μέσων.

Σήμερα, με την επανάσταση που έφερε το internet, τόσο οι ιοί, όσο και τα σκουλήκια (τα οποία θα αναλύσουμε παρακάτω) μεταδίδονται με πολύ γρήγορο ρυθμό, εξαιτίας τόσο των υψηλών ταχυτήτων, όσο και της υψηλής διασύνδεσης των κόμβων του διαδικτύου.

ΩΦΕΛΙΜΟ ΦΟΡΤΙΟ

Το ωφέλιμο φορτίο αφορά στο τι κάνει ο ιός όταν εκτελεστεί, χωρίς να έχει σχέση με τη διάδοση. Μερικοί ιοί απλά μολύνουν και διαδίδονται χωρίς να προκαλούν βλάβη στο σύστημα. Άλλοι πάλι κάνουν «αθώα» πράγματα, όπως να ζητούν κάποιο cookie, ενώ άλλοι προκαλούν σοβαρές ζημιές στο σύστημα που μολύνουν.

Μερικοί ιοί για να ξεκινήσουν την εκτέλεσή τους απαιτούν κάποιο συγκεκριμένο ερέθισμα. Το καλύτερο για έναν ιό είναι να έχει κάποιον μηχανισμό που θα του παρέχει κάποιο ερέθισμα για να αρχίσει να εκτελεί το ωφέλιμο φορτίο του, παρά να αρχίζει την εκτέλεσή του αμέσως μόλις μολύνει κάποιο μηχάνημα για να μην γίνεται εύκολα αντιληπτός και να μην μειωθεί ο ρυθμός εξάπλωσης του.

3.5.5 ΚΑΤΗΓΟΡΙΕΣ ΙΩΝ

Σε γενικές γραμμές υπάρχουν ποικίλοι τρόποι για να κατηγοριοποιήσει κανείς τους ιούς. Ενδεικτικά βλέπουμε μερικές κατηγορίες ιών παρακάτω [39]:

1. Boot sector
2. Macro Viruses
3. Polymorphic Viruses
4. Parasitic
5. Memory-resident

1. Boot sector ιοί γενικά χαρακτηριστικά

Οι boot sector ιοί [38,40] μπορούν να μολύνουν ή να αντικαθιστούν με τον δικό τους κώδικα, τόσο το DOS boot sector όσο και το Master Boot Record (MBR).Το MBR είναι ένα μικρό πρόγραμμα που τρέχει κάθε φορά που ανοίγει ο υπολογιστής, το οποίο έχει στον έλεγχο του το boot sequence και καθορίζει από ποιο partition θα

κάνει εκκίνηση (boot) ο υπολογιστής. Γενικά το MBR βρίσκεται στο πρώτο τομέα (sector) του σκληρού δίσκου.

Γίνεται εύκολα αντιληπτό ότι από τη στιγμή που το MBR εκτελείται κάθε φορά που ανοίγει ο υπολογιστής, η μόλυνση του από έναν ιό είναι άκρως επικίνδυνη. Από τη στιγμή που θα μολυνθεί ο κώδικας εκκίνησης του δίσκου, ο ιός θα φορτώνεται στη μνήμη σε κάθε άνοιγμα του υπολογιστή.

Από τη μνήμη ο boot sector ιός μπορεί να μολύνει κάθε δίσκο που διαβάζεται από το σύστημα. Οι ιοί αυτοί μπορούν να προκαλέσουν μία ποικιλία προβλημάτων ανάκτησης δεδομένων ή και στοιχείων εκκίνησης. Σε κάποιες περιπτώσεις μάλιστα είναι δυνατόν να προκληθεί απώλεια δεδομένων και μάλιστα από ολόκληρα κομμάτια του δίσκου.

Επίσης πολύ συχνά ο υπολογιστής γίνεται ξαφνικά ασταθής, αποτυγχάνει να ξεκινήσει, ή δεν μπορεί να εντοπίσει τον σκληρό δίσκο. Σε τέτοιες περιπτώσεις μηνύματα λάθους όπως: "Invalid system disk" είναι συχνό φαινόμενο.

Η μετάδοση αυτού του είδους ιομορφικού λογισμικού γινόταν συνήθως από μολυσμένα floppy disks.Σήμερα η μετάδοση τους γίνεται κατά βάση μέσω δικτύων (και του Διαδικτύου φυσικά) από downloads αρχείων ή και από μολυσμένα emails. Στις περισσότερες των περιπτώσεων όλοι οι δίσκοι (με ενεργοποιημένη την εγγραφή στη μνήμη) σε έναν μολυσμένο υπολογιστή θα "κωλύσουν" τον ιό.

Τρόποι αντιμετώπισης – αντίμετρα

Ένα μεγάλο πρόβλημα με τους ιούς αυτούς είναι η απομάκρυνση τους, και αυτό γιατί συχνά είναι δύσκολο για ένα antivirus πρόγραμμα να καθαρίσει το MBR την ώρα που εκτελείται το λειτουργικό σύστημα. Γενικά η πρόληψη είναι θέμα επαγρύπνησης και αποφυγής επαφής με άγνωστους δίσκους. Πέρα από τα γενικά αντίμετρα που θα αναλυθούν στη συνέχεια υπάρχουν κάποιοι τρόποι για να μειώσουμε την πιθανότητα μόλυνσης από έναν boot sector ιό [40]. Καταρχάς είναι δυνατόν να γίνουν κάποιες ρυθμίσεις στο CMOS (complementary metal oxide semiconductor) ώστε να μην είναι δυνατή η εγγραφή στον boot τομέα του σκληρού δίσκου. Αυτό αν και μπορεί να βοηθήσει κάπως, είναι πιθανόν να δημιουργήσει προβλήματα (πχ όταν θελήσουμε να ξανά εγκαταστήσουμε το λειτουργικό μας σύστημα). Ακόμη είναι καλό οι διάφοροι removable δίσκοι που χρησιμοποιούμε να

είναι κλειδωμένοι (write protected) και να τους χρησιμοποιούμε μόνο σε υπολογιστές που έχουμε βεβαιωθεί ότι είναι ασφαλείς.

2. Macro viruses γενικά χαρακτηριστικά

Γενικά οι μακροεντολές μπορούν να χρησιμοποιηθούν σε προγράμματα όπως το word και το excel, για να αυτοματοποιήσουν σύνθετους η επαναλαμβανομένους στόχους.

Μόλις γραφτούν, ορίζετε σε αυτές ένας συνδυασμός πλήκτρων, ή κάποιο κουμπί από την εργαλειοθήκη που θα ενεργοποιεί την μακροεντολή. Οι μακροεντολές αποθηκεύονται σαν μια σειρά οδηγιών σε μια γλωσσά όπως η VISUAL BASIC.

Από τη στιγμή που καταγράφει μια μακροεντολή ο χρήστης μπορεί να την επεξεργαστεί ή ακόμα και να προσθέσει πιο περιπλοκές εντολές που δεν είναι κανονικά εγγράψιμες. Αυτό δίνει την δυνατότητα στον έμπειρο χρηστή όχι μόνο να αυτοματοποιήσει λειτουργίες μέσα στο πρόγραμμα αλλά και να εκτελεί βασικές εντολές του συστήματος όπως διαγραφή, μετονομασία, ή αλλαγή των ιδιοτήτων των αρχείων. Ένας μακροιός χρησιμοποιεί την δύναμη και την λειτουργικότητα των μακροεντολών για να δημιουργήσει αντίγραφα του εαυτού του και για να διαδοθεί.

Όταν ένας χρήστης λαμβάνει και ανοίγει ένα αρχείο που περιέχει μακροιούς, αυτός ο ιός είτε θα εκτελεστεί αυτόματα είτε από τον συνδυασμό κάποιον πλήκτρων ή από την εκτέλεση κάποιας εντολής από το menu επιλογών ή και το πάτημα κάποιου κουμπιού μιας εργαλειοθήκης κ.τ.λ.

Στην συνεχεία ο ιός θα αντιγραφτεί στο σύστημα. Ο μακροιός θα είναι παρόν πλέον στα αρχεία που θα ανοίγει ο χρήστης και θα μπορεί να μεταδοθεί με πολλούς διαφορετικούς τρόπους.

Μερικά πολύ επικίνδυνα πράγματα που μπορεί να κάνει ένας τέτοιος ιός είναι να διαγράψει-τροποποιήσει τα περιεχόμενα ενός κειμένου ή να αλλάξει τις ρυθμίσεις του word κ.τ.λ.

Θεωρητικά ένας μακροϊός μπορεί να γραφτεί για οποιοδήποτε πρόγραμμα που αποθηκεύει μακροεντολές σε μορφή που μπορεί να ανοιχτεί και να επεξεργαστεί χρησιμοποιώντας μια γλώσσα όπως η word basic και visual basic.

Στην πράξη ωστόσο οι περισσότεροι που έχουν βρεθεί αφορούν κυρίως το word και το excel. Μια άλλη ενδιαφέρουσα ιδιότητα των μακροϊών είναι ότι μπορούν ενδεχομένως να διαδίδονται σε διαφορετικές πλατφόρμες όπως από MAC σε PC.

Οι διάφοροι ιοί που προσπαθούν να προκαλέσουν ζημιά σε ένα μέρος του συστήματος του χρηστή έξω από το word δεν θα είναι σε θέση να κάνουν το ίδιο και σε διαφορετική πλατφόρμα.

Συνοψίζοντας δηλαδή ένα μακροϊό που διαδίδετε και μπορεί να προκαλεί βλάβες σε ένα σύστημα, μπορεί να διαδίδεται σε κάποιον άλλο, αλλά να μην προκαλεί κάποια βλάβη. Υπάρχει δηλαδή η δυνατότητα ένας μακροϊός να εντοπίζει σε ποιο σύστημα τρέχει και να αλλάζει την συμπεριφορά του ανάλογα. Όμως κάτι τέτοιο δεν είναι σύνηθες.

Τρόποι αντιμετώπισης- αντίμετρα

Όταν τον Αύγουστο του 1995 έκανε την εμφάνιση του ο πρώτος μακροιός στην πραγματικότητα δεν ήταν ο πρώτος, αφού κάποιες εταιρείες αντιβιοτικών είχαν πειραματικά δημιουργήσει ιούς που μεταδίδονταν από ένα κείμενο στο άλλο, ωστόσο σχεδόν κανείς δεν ενδιαφέρθηκε για αυτό το μάλλον αποτυχημένο πείραμα και έτσι η αντιική ικανότητα βρέθηκε απροετοίμαστη.

Αξιοσημείωτο μάλιστα είναι ότι αν παρατηρούσε κανείς την τότε βιβλιογραφία σε σχέση με τους ιούς θα έβλεπε ότι στην ερώτηση, αν μπορεί ένα κείμενο να περιέχει κάποιον ιό, η απάντηση ήταν απλή: ΟΧΙ.

Έτσι η πρώτη βιαστική αντιμετώπιση της επιδημίας μακροϊών που προέκυψε ήταν η δημιουργία άλλων ιών που μεταδίδονταν από κείμενο σε κείμενο και έσβηναν τις κακόβουλες μακροεντολές.

Οι τρόποι για την ανίχνευση των μακροϊών πλέον ποικίλουν. Ένας πολύ απλός είναι με την ανίχνευση του ονόματος του ιού. Επίσης επειδή ένα μεγάλο μέρος των νέων ιών που κυκλοφορούν είναι ουσιαστικά "αλλαγμένες" εκδόσεις παλιών, είναι δυνατόν να γίνεται η ανίχνευση με βάση το βασικό σώμα ενός ιού.

3. Πολυμορφικοί ιοί γενικά χαρακτηριστικά

Πολυμορφικός ιός είναι αυτός που παράγει μία μεγάλη ποικιλία από διαφορετικά αντίγραφα του εαυτού του [42] (τα οποία είναι λειτουργικά.) Η στρατηγική υποθέτει ότι το αντιϊικό πρόγραμμα δεν θα μπορέσει να εντοπίσει όλα τα διαφορετικά στιγμιότυπα

του ιού. Ένας τρόπος για την αποφυγή ανίχνευσης είναι η κρυπτογράφηση του εαυτού του με ένα μεταβλητό κλειδί.

Κάποιοι πιο εξελιγμένοι πολυμορφικοί ιοί ωστόσο αλλάζουν τις ακολουθίες οδηγιών μέσα στις μεταβλητές τους με το να παραβάλουν τις οδηγίες κρυπτογράφησης με "θορυβώδη" οδηγίες με το να εναλλάσσουν αμοιβαία ανεξάρτητες οδηγίες, ή ακόμα και με τη χρησιμοποίηση ποικίλων συχνοτήτων οδηγιών με πανομοιότυπα net effects.

Μια από τις πιο εξελιγμένες μορφές πολυμορφισμού που χρησιμοποιείται είναι η Dark Angels Multiple Encryptor (dame), που εμφανίζεται με μία μορφή object module (άλλες γεννήτριες πολυμορφικότητας είναι οι: MTE, TPE, NED κ.α).

Με τη βοήθεια της, οποιοσδήποτε ιός μπορεί να γίνει πολυμορφικός με το να προσθέσει συγκεκριμένες κλήσεις στον assembly κώδικα του και συνδέοντας τον με την DAME γεννήτρια τυχαίων αριθμών.

Η εμφάνιση των πολυμορφικών ιών μετέτρεψε την επιστήμη της ανίχνευσης των ιών σε ένα εξαιρετικά δύσκολο και ακριβό εγχείρημα. Αυτό δεν σημαίνει ότι απαραίτητα οι πολυμορφικοί ιοί είναι οι πιο καταστροφικοί (υπάρχουν απλοί ιοί που μπορούν να σβήσουν όλα τα δεδομένα από τον σκληρό δίσκο (format) ή να δημιουργήσουν μεγάλα προβλήματα στο BIOS).

Το πιο μεγάλο πλεονέκτημα τους είναι η δυσκολία εντοπισμού τους. Η απλή πρόσθεση όλο και περισσότερων συμβολοσειρών (strings) αναζήτησης σε απλούς ανιχνευτές είναι προφανές ότι δεν μπορεί πάντα να επιλύσει επαρκώς το πρόβλημα αφού πλέον είναι δυνατόν να μην υπάρχει ένα συγκεκριμένο strings από bytes που να ταυτοποιεί τον ιό.

Τρόποι αντιμετώπισης – αντίμετρα

Οι τρόποι που χρησιμοποιούνται από τα διάφορα antivirus προγράμματα για την ανίχνευση πολυμορφικών ιών ποικίλουν. Οι συνηθέστεροι είναι [42]: Scan Strings Variable Scan Strings Cryptanalysis Generic Decryptor Heuristic analysis
Το απλό scan string (αναζήτηση συμβολοσειράς) είναι η ανίχνευση για συγκεκριμένες ακολουθίες από bytes. Πχ. το scan string που είναι της μορφής: aa ?? bb ?? cc μπορεί να εντοπίσει ιούς μόνο της μορφής: aa xx bb xx cc.

Το Variable Scan string (μεταβλητή αναζήτηση συμβολοσειράς) είναι μία βελτίωση του παραπάνω που λειτουργεί με δυναμικό τρόπο. Πχ. το scan string που είναι της μορφής: aa * bb * cc μπορεί να εντοπίζει ιούς των μορφών: aa xx xx bb xx xx xx xx cc ή aa bb xx xx xx cc κτλ.

Η κρυπτανάλυση λειτουργεί με το να εντοπίζει ένα μέρος από το σώμα του ιού, να εκτελεί μία βασική κρυπτανάλυση πάνω σε αυτό και τελικά εάν είναι επιτυχής να τον εντοπίζει.

Ο γενικός Αποκρυπτογράφος (Generic Decryptor) λειτουργεί με το να προσομοιώνει οδηγίες σε έναν πολυμορφικό αποκρυπτογράφο με σκοπό να αναγκάσει τον ιό να αποκρυπτογραφηθεί μόνος του και στην συνέχεια τον εντοπίζει με μία απλή αναζήτηση συμβολοσειράς.

Η Heuristic analysis (ευρυστική ανάλυση) (από τα πιο δυνατά όπλα των antivirus προγραμμάτων) αναζητούν αντιφατικότητες μεταξύ του κώδικα που αναλύεται και του κώδικα που πρέπει να έχει κανονικά ένα πρόγραμμα.

4. Παρασιτικός

Ο παραδοσιακός αλλά και πιο διαδεδομένος τύπος ιού. Οι ιοί αυτοί προσαρτώνται σε εκτελέσιμα αρχεία και αναπαράγονται, όταν εκτελεστεί το μολυσμένο πρόγραμμα, βρίσκοντας και άλλα εκτελέσιμα αρχεία για να μολύνουν.

5. Παραμένοντες στη μνήμη

Οι ιοί αυτοί εγκαθίστανται στην κύρια μνήμη ως τμήματα προγραμμάτων που παραμένουν στη μνήμη. Από τη στιγμή της εγκατάστασης τους, οι ιοί αυτοί μολύνουν κάθε πρόγραμμα που εκτελείται.

(Για τα αντίμετρα των κατηγοριών 4, 5 δεν έχουμε να αναφέρουμε κάτι επιπρόσθετο από αυτά που θα σας αναλύσουμε παρακάτω στην ενότητα της προστασίας του κακόβουλου λογισμικού.)

3.5.6 ΤΕΧΝΙΚΕΣ ΙΟΥ ΜΟΛΥΝΩΝΤΑΣ ΕΝΑ ΕΚΤΕΛΕΣΙΜΟ.

1. **companion infection τεχνική:**

Σύμφωνα με την μέθοδο αυτή η οποία θεωρείτε και η πιο απλή ο ιός βρίσκεται μαζί με ένα εκτελέσιμο αρχείο και το μόνο που κάνει είναι να ονομάζει τον εαυτό του με το ίδιο όνομα του αρχικού του προγράμματος. Έτσι λοιπόν όταν ο χρηστής ζητά να εκτελέσει το αρχικό πρόγραμμα το λειτουργικό σύστημα εκτελεί και τον ιό.

Στα συστήματα με λειτουργικό Windows ένας τρόπος για να υλοποιηθεί η παραπάνω μέθοδος, είναι σε .EXE αρχεία να δώσει κάποιος στον ιό το ίδιο βασικό όνομα όπως έχει το αρχικό πρόγραμμα αλλά και να χρησιμοποιήσει κατάληξη .COM αντί .EXE που είναι το αρχικό. Αυτό μπορούμε να το δούμε στο παρακάτω παράδειγμα:

Συνήθως όταν ο χρηστής θέλει να εκτελέσει ένα αρχείο EXE πληκτρολογεί μονό το όνομα χωρίς την κατάληξη. Στην περίπτωση αυτήν τα Windows δίνουν προτεραιότητα σε αρχεία .COM που έχουνε το όνομα αυτό και όχι στα .EXE τα οποία εκτελούνται μετά αν δεν βρεθεί αρχείο με κατάληξη .COM.

Για να κρύψουν την ύπαρξή τους, οι ιοί που χρησιμοποιούν αυτή τη τεχνική συνήθως αναθέτουν ένα κρυφό χαρακτηριστικό στο COM αρχείο, μειώνοντας έτσι την πιθανότητα ο χρήστης του συστήματος να το ανακαλύψει στον κατάλογο αρχείων. Τα αρχεία με κρυφό χαρακτηριστικό εξ' ορισμού δεν εμφανίζονται στον κατάλογο των αρχείων.

Για να εξασφαλίσουν ότι το θύμα δεν θα καταλάβει τίποτα, εκτελούν το κανονικό πρόγραμμα μετά από την εκτέλεση του κώδικα του ιού.

Σήμερα τα περισσότερα προγράμματα Windows δεν εκτελούνται πλέον από την γραμμή εκτέλεσης εντολών με αποτέλεσμα η μέθοδος αυτή να μην είναι αρκετά αποτελεσματική.

2. **Η τεχνική της αντιγραφής (overwriting infection):**

Ο ιός που χρησιμοποιεί αυτή τη τεχνική αντικαθιστά ένα μέρος του κώδικα του αρχικού προγράμματος. Ένας τρόπος για να το καταφέρει αυτό είναι με το να ανοίξει

το πρόγραμμα για εγγραφή, όπως θα έκανε με ένα συνηθισμένο αρχείο και να αντιγράψει ένα αντίγραφο του εαυτού του μέσα στο αρχείο αυτό.

Αυτό έχει ως αποτέλεσμα ότι όταν ο χρήστης προσπαθήσει να εκτελέσει το πρόγραμμα, το λειτουργικό σύστημα θα εκτελέσει τον κώδικα του ιού αντί αυτού.

Ο χρήστης μετά από αυτό μπορεί να καταλάβει ότι κάτι δεν πήγε καλά αλλά τότε θα είναι αργά αφού ο ιός έχει ενεργοποιηθεί ήδη

3. Η τεχνική εισαγωγής του κώδικα στην αρχή του προγράμματος (prepending technique):

Εδώ ο ιός προσθέτει τον κώδικά του στην αρχή του προγράμματος που θέλει να μολύνει. Όταν ένα πρόγραμμα μολυσμένο με ένα τέτοιο ιό εκτελεστεί, τότε το λειτουργικό σύστημα εκτελεί πρώτα τον κώδικα του ιού μιας και βρίσκεται στην αρχή του προγράμματος.

Στις περισσότερες περιπτώσεις ο ιός περνά τον έλεγχο στον ξενιστή του ώστε ο χρήστης να μην καταλάβει εύκολα την παρουσία του .

4. Η τεχνική εισαγωγής του κώδικα στο τέλος του προγράμματος (appending technique):

Ο ιός προσθέτει τον κώδικά του στο τέλος του προγράμματος. Για να εκτελεστούν αυτοί οι ιοί είναι απαραίτητο να αλλάξουν την αρχή του προγράμματος που έχουν μολύνει ώστε να δημιουργήσει ένα άλμα μέσα στον κώδικά του και να δείχνει αυτό στο μέρος εκείνο που βρίσκεται ο κώδικας του ιού.

Όταν ο ιός εκτελέσει το μέρος του επαναφέρει τον έλεγχο στο αρχικό πρόγραμμα. Η μέθοδος αυτή όπως και η προηγούμενη δεν καταστρέφει το πρόγραμμα ξενιστή. Ο ιός αυτός μπορεί να μολύνει και να διαδοθεί και μέσα από αρχεία εγγράφων.

Μερικά προγράμματα-εφαρμογές που υποστηρίζουν μάκρο-εντολές εσωτερικά σε έγγραφα με σκοπό τον εμπλουτισμό της εφαρμογής με νέες δυνατότητες, την αλληλεπίδραση με το χρήστη ή ακόμα και την αυτοματοποίηση κάποιων διαδικασιών είναι: το Microsoft Office, το WordPerfect Office, το Star Office, το AutoCAD.

Για παράδειγμα το Microsoft Word είναι μακράν το πιο δημοφιλές πρόγραμμα και η εφαρμογή του υποστηρίζει τις μακρό-εντολές. Από αυτά λοιπόν εύκολα καταλαβαίνουμε ότι τα αρχεία αυτά είναι πιθανοί και ταυτόχρονα αρκετά ελκυστικοί στόχοι για ιούς που βασίζονται σε μακροεντολές.

Ένας χρήστης είτε είναι κακόβουλος είτε όχι μπορεί να εισάγει μακροεντολές σε ένα αρχείο κειμένου ή σε κάποιο άλλο έγγραφο χρησιμοποιώντας για παράδειγμα τον editor της Visual Basic. Ο ιός ο οποίος προσκολλάται σε ένα τέτοιο αρχείο θα πρέπει να διασφαλίσει ότι ο κώδικάς του θα εκτελεστεί από τον χρήστη. Σε άλλη περίπτωση ο ιός δεν μπορεί τότε να 'τρέξει'.

Για να πετύχουν το στόχο οι ιοί περικλείουν υπορουτίνες με ονόματα που έχουν ιδιαίτερη σημασία για το Microsoft Word ή για τις άλλες εφαρμογές. Για παράδειγμα αν ένα αρχείο-έγγραφο περιέχει μια υπορουτίνα που καλείτε Document_Open( ), τότε το Microsoft Word θα πάει να εκτελέσει αυτή την υπορουτίνα μόλις ο χρήστης ανοίξει αυτό το έγγραφο.

Ένας άλλος δημοφιλής στόχος είναι η υπορουτίνα που ονομάζεται Document_Close και η οποία εκτελείται όταν το έγγραφο κλείνει/τερματίζεται. Υπάρχουν και άλλες ρουτίνες τις οποίες οι ιοί χρησιμοποιούν προκειμένου να ενεργοποιηθούν.

ΜΕΡΙΚΕΣ ΑΠΟ ΤΙΣ ΠΙΟ ΓΝΩΣΤΕΣ ΚΑΙ ΠΕΡΙΣΣΟΤΕΡΟ ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΕΣ ΥΠΟΡΟΥΤΙΝΕΣ ΕΙΝΑΙ ΟΙ ΠΑΡΑΚΑΤΩ:

AutoExec → Η συνάρτηση αυτή εκτελείται όταν κάποιος χρήστης ξεκινά το Word.

FileExit → Οι ρουτίνες αυτές εκτελούνται όταν έχουμε το κλείσιμο ενός εγγράφου.

AutoExit → Η συνάρτηση αυτή ενεργοποιείται όταν έχουμε τον τερματισμό της εφαρμογής του Word από ένα χρήστη.

AutoOpen → Οι ρουτίνες αυτές εκτελούνται όταν κάποιος χρήστης ανοίγει ένα έγγραφο.

AutoNew → Οι συναρτήσεις χρησιμοποιούνται όταν κάποιος χρήστης δημιουργεί ένα έγγραφο.

FileSave → Αυτή η συνάρτηση χρησιμοποιείται όταν ένας χρήστης ¨ σώζει¨ ένα έγγραφο για μελλοντική χρήση.

3.6 ΔΟΥΡΕΙΟΣ ΙΠΠΟΣ (TROJAN HORSE)

Ο δούρειος ίππος (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Ο όρος αυτός που χρησιμοποιούμε για αυτά τα προγράμματα προέρχεται από την ελληνική ιστορία, όπου οι Έλληνες χρησιμοποιώντας το Δούρειο ίππο μπορέσανε και κατακτήσανε την Τροία. Ανάλογη λοιπόν είναι και η λειτουργία αυτών των προγραμμάτων σήμερα.

Η τακτική που χρησιμοποιούν οι δούρειοι ίπποι είναι παρόμοια με την τακτική που χρησιμοποίησε ο Οδυσσέας, όπου και από εκεί πήρε και αυτήν την ονομασία. Μια άλλη εκδοχή βέβαια όπου μπορεί να ονομάστηκε έτσι ήταν όταν για πρώτη φορά χρησιμοποιήθηκε ο όρος αυτός από τον Κεν Τόμσον στην ομιλία του κατά την τελετή απονομής τον βραβείων μιας και παρατήρησε ότι είναι δυνατόν να προστεθεί κακόβουλος κώδικας στην εντολή Loginc του unix για την υποκλοπή των κωδικών πρόσβασης. Αυτή του την ανακάλυψη όπως και προαναφέραμε την ονόμασε δούρειο ίππο .

Συγκεκριμένα, κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Για παράδειγμα θα μπορούσαμε να σας πούμε είναι κάποιο νέο παιχνίδι δωρεάν στο διαδίκτυο, κάποιο τραγούδι σε mp3, κάποιο εξιδανικευμένο πρόγραμμα πορνογραφικού υλικού ή κάποιο άλλο πρόγραμμα αρκετά δελεαστικό ώστε να το κατεβάσουν οι χρήστες.

Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως το αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου

προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

Ένα παράδειγμα είναι ένα πρόγραμμα που καταγράφει usernames και passwords, το οποίο αρχικά τυπώνει ένα φαινομενικά νόμιμο παράθυρο για την εισαγωγή αυτών των στοιχείων και περιμένει μέχρι ο χρήστης να εισάγει κάποια στοιχεία. Όταν αυτό συμβαίνει, τότε τα καταγράφει και τα στέλνει στο δημιουργό του και συγχρόνως παράγει ένα μήνυμα στο χρήστη ότι ο κωδικός είναι λάθος, πριν τρέξει το πραγματικό πρόγραμμα εισαγωγής στο σύστημα. Ο χρήστης τότε νομίζει ότι έκανε λάθος και επανεισάγει τα στοιχεία του, χωρίς να γνωρίζει τι έγινε π.χ. στο Facebook.

Ένα ακόμα παράδειγμα του Δούρειου Ίππου είναι η απενεργοποίηση του ήχου του μόντεμ και εν συνεχεία τη κλήση κάποιου διεθνούς αριθμού με ιδιαίτερο υψηλό κόστος. Συνήθως επιλέγονται μακρινές χώρες (π.χ. Μολδαβία κτλ.) όπου επιλέγετε κάποιος πολύ ακριβός παροχέας διαδικτύου, ώστε ο χρήστης να μην αντιληφθεί κάτι ύποπτο και να συνεχίζει να δουλεύει για ώρες.

3.6.1 ΤΥΠΟΙ ΔΟΥΡΕΙΩΝ ΙΠΠΩΝ

Υπάρχουν δύο είδη δούρειων ίππων:

Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία διάφοροι hackers μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για παράδειγμα διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων (peer-to-peer), προγράμματα ανακοίνωσης καιρικών συνθηκών.

Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Οι τύποι δούρειων ίππων μπορούν να διαχωριστούν περαιτέρω στις εξής κατηγορίες ανάλογα με τις συνέπειες που έχουν στον μολυσμένο υπολογιστή π.χ. Μερικές από τις επιπτώσεις εκτέλεσης ενός δούρειου ίππου είναι για παράδειγμα η διαγραφή αρχείων στον μολυσμένο υπολογιστή, η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές, το ανοιγόκλειμα του οδηγού CD-ROM, η παρακολούθηση των

κινήσεων του χρήστη για την απόκτηση των κωδικών του σε τράπεζες, η απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, η επανεκκίνηση του υπολογιστή, η απενεργοποίηση προγραμμάτων firewall ή αντιϊοικών και πολλά άλλα.

3.7 ΛΟΓΙΚΕΣ ΒΟΜΒΕΣ (LOGIC BOMB)

Οι λογικές βόμβες δε μπορούν να αναπαραχθούν και άρα να αυξήσουν το πληθυσμό τους. Μπορούν να είναι είτε αυτόνομα προγράμματα είτε να έχουν εισέλθει σε ένα κώδικα.

Χαρακτηριστικό τους είναι ότι μπορούν και κρύβονται καλά ανάμεσα σε εκατομμύρια γραμμές κώδικα ενός νόμιμου προγράμματος, γεγονός που κάνει πολύ δύσκολο τον εντοπισμό τους.

Οι ιοί και τα σκουλήκια, συχνά περιέχουν λογικές βόμβες που εκτελούν ένα συγκεκριμένο ωφέλιμο φορτίο, σε προκαθορισμένο χρόνο ή όταν κάποια άλλη προϋπόθεση αυτή πληρείται.

Αυτή η τεχνική μπορεί να χρησιμοποιηθεί από έναν ιό ή ένα σκουλήκι για να αποκτήσει δύναμη και να εξαπλωθεί πριν από τον εντοπισμό του.

Το λεγόμενο **logic bomb** αποτελείται από δύο μέρη:

1) Το ωφέλιμο φορτίο, που είναι μία ενέργεια που θα εκτελεστεί και που είναι κακόβουλη και από το ερέθισμα.

2) Μία δυαδική συνθήκη η οποία αξιολογείται και αν ισχύει τότε εκτελείται το ωφέλιμο φορτίο. Το τι θα είναι αυτό το ερέθισμα που περιορίζεται μόνο από τη φαντασία του δημιουργού του μπορεί να βασίζεται πχ στην ημερομηνία, στην έκδοση του λειτουργικού κ.α.

3.8 ΠΙΣΩ ΠΟΡΤΕΣ (BACKDOORS) Η ΚΕΡΚΟΠΟΡΤΕΣ

Backdoor είναι ένα πρόγραμμα το οποίο επιτρέπει σε ένα κακόβουλο χρήστη να προσπεράσει συνηθισμένα μέτρα ασφαλείας σε ένα σύστημα και να αποκτήσει πρόσβαση σε αυτό με τους δικούς του όρους όμως.

Ο βασικός στόχος λοιπόν ενός backdoor είναι να παρέχει πρόσβαση σε ένα σύστημα παρακάμπτοντας όμως κάποια συνηθισμένα μέτρα ασφάλειας. Θα πρέπει

να τονίσουμε ότι οι λεγόμενες αυτές πίσω πόρτες μπορούν να τοποθετηθούν είτε σε ένα κομμάτι νόμιμου κώδικα ή να σταθούν σαν αυτόνομα προγράμματα. Δεν μπορούν όμως να διαδοθούν όπως οι ιοί και τα σκουλήκια με αποτέλεσμα να μην αυξάνουν και τον πληθυσμό τους.

Η εγκατάσταση των backdoors

Μια περίπτωση είναι ο ίδιος ο χρήστης να το έχει τοποθετήσει έχοντας αποκτήσει πρόσβαση στο σύστημα με άλλες μεθόδους όπως η εκμετάλλευση κάποιων τρωτών σημείων ή από λάθη τα οποία υπήρχαν στη διαμόρφωση του συστήματος από το διαχειριστή. Επίσης μπορεί κάποιος να εγκαταστήσει ένα τέτοιο πρόγραμμα χρησιμοποιώντας αυτοματοποιημένα προγράμματα όπως είναι οι ιοί και τα worms. Μία ακόμα μέθοδος είναι αυτή που ο χρήστης του συστήματος εγκαθιστά ο ίδιος το backdoor χωρίς να το γνωρίζει.

3.9 WORMS

Ένα worm [43,44,45] είναι ένα αυτό-αναπαραγόμενο πρόγραμμα ηλεκτρονικού υπολογιστή το όποιο χρησιμοποιεί το διαδίκτυο για να στείλει αντίγραφα του εαυτού του σε άλλους υπολογιστές στο δίκτυο χωρίς να είναι αναγκαία κάποια παρέμβαση από τον χρηστή.

Σε αντίθεση με τους ιούς, δεν χρειάζεται να προσκολλάτε σε ένα υπάρχον πρόγραμμα. Τα worm σχεδόν πάντα προκαλούν βλάβες στο δίκτυο, έστω και μόνο από την κατανάλωση εύρους ζώνης, σε αντίθεση με τους ιούς που σχεδόν πάντα καταστρέφουν ή τροποποιούν τα αρχεία στον υπολογιστή που έχουν στοχεύσει.

Η ονομασία των worm προέρχεται από ένα επιστημονικής φαντασίας μυθιστόρημα με τίτλο The Shockwave Rider το όποιο δημοσιεύτηκε το 1975 απο τον John Brunner .

Οι ερευνητές John F Shock και John Hupp της Xerox PARC ήταν οι πρώτοι που χρησιμοποίησαν αυτό το όνομα σε ένα έγγραφο που δημοσίευσαν το 1982 και έκτοτε έχει υιοθετηθεί ευρέως. Επίσης ήταν και οι δυο πρώτοι ερευνητές που υλοποίησαν ένα worm το 1978.

Οι Shoch και Hupp κατασκεύαζαν αρχικά ένα worm με σκοπό να εντοπίζει τους αδρανείς επεξεργαστές στο δίκτυο και να τους αναθέτει εργασίες, ανακατανέμοντας

με αυτό τον τρόπο το φορτίο επεξεργασίας, οδηγώντας στην βελτίωση της κατανομής της χρησιμοποίησης των CPU του δικτύου .

Ένα άλλο στοιχειό που διέθετε τον εν λόγο λογισμικό, ήταν ότι ήταν αυτοπεριορισμένο, έτσι ώστε να μην είναι δυνατή η περεταίρω εξάπλωση του στο διαδίκτυο. Τα worm χρησιμοποιούν το Internet ως μέσο διάδοσής τους (emails, mirc chat κ.ά.).

Όπως οι ιοί, έτσι και τα σκουλήκια, τροποποιούν τη φυσιολογική λειτουργία των μηχανημάτων που μολύνουν. Τα σκουλήκια, συνήθως, εγκαθιστούν τους εαυτούς τους στα μολυσμένα μηχανήματα και κατόπιν αρχίζουν την εκτέλεσή τους. Κατά την εκτέλεσή τους χρησιμοποιούν τους πόρους του μολυσμένου μηχανήματος, όπως άλλωστε και οποιοδήποτε φυσιολογικό πρόγραμμα.

Παρόλα αυτά, αρκετά σκουλήκια κρύβουν την ύπαρξή τους εγκαθιστώντας λογισμικό ή rootkits, ώστε να κρυφτούν αποτελεσματικά, ενώ άλλα χρησιμοποιούν ακόμη και ρουτίνες του πυρήνα για να το πετύχουν αυτό.

3.9.1 ΒΑΣΙΚΕΣ ΔΙΑΦΟΡΕΣ ΜΕΤΑΞΥ ΤΩΝ ΙΩΝ ΚΑΙ ΤΩΝ ΣΚΟΥΛΗΚΙΩΝ:

1) Σε αντίθεση με τους ιούς, τα σκουλήκια έχουν τη δυνατότητα να μεταδίδονται αυτόνομα από σύστημα σε σύστημα μέσω του δικτύου, χωρίς να χρειάζονται τη βοήθεια άλλου λογισμικού.

2) Ένα σκουλήκι είναι ένα ενεργό σύστημα διανομής, το οποίο ελέγχει και χρησιμοποιεί το δίκτυο για να φτάσει στο σύστημα στόχο. Αντίθετα, ένας ιός είναι ένα στατικό μέσο, το οποίο δεν μπορεί να ελέγξει και να κάνει χρήση του συστήματος διανομής, δηλ. του δικτύου.

3) Σε αρκετές περιπτώσεις, οι διάφοροι κόμβοι του δικτύου του σκουληκιού (τα μηχανήματα που έχουν μολυνθεί από το σκουλήκι) μπορούν να ανταλλάξουν πληροφορία μεταξύ τους ή με κάποιον κεντρικό κόμβο. Αντίθετα οι ιοί δεν έχουν τη δυνατότητα να επικοινωνήσουν με εξωτερικά συστήματα.

3.9.2 PAYLOAD

Πολλά σκουλήκια έχουν δημιουργηθεί με σκοπό την εξάπλωση τους χωρίς να προσπαθούν να τροποποιήσουν τα συστήματα που διέρχονται. Ωστόσο, όπως έδειξαν τα σκουλήκια Morris και Mydoon [27,46] η διαδικτυακή κίνηση έχει και άλλες ακούσιες συνέπειες που μπορεί συχνά να προκαλέσουν σημαντικές διαταραχές. Αυτό οφείλετε στο payload (φορτίο) που φέρουν τα worms το όποιο είναι ένα κώδικας σχεδιασμένος να κάνει κάτι περισσότερο από το να εξαπλώνετε, όπως είναι η διαγραφή αρχείων σε έναν υπολογιστή (π.χ. explore ZIP worm), η κρυπτογράφηση αρχείων σε cryptoviral extortion επίθεση ή η αποστολή εγγράφων μέσω e-mail.

Ένα πολύ συνηθισμένο payload για σκουλήκια είναι η εγκατάσταση μιας κερκόπορτας στον μολυσμένο υπολογιστή για να επιτρέψει την δημιουργία ενός “zombie” υπολογιστή , ο όποιος βρίσκεται υπό τον έλεγχο του σχεδιαστή του worm.

Δίκτυα με τέτοιους υπολογιστές zombie συχνά αναφέρονται ως botnets και χρησιμοποιούνται από τους σχεδιαστές των λογισμικών για την αποστολή e-mail junk ή για την παραλογή της διεύθυνσης του δικτυακού τόπου. Γι’ αυτό το λόγο οι spammers [47] θεωρούνται ως μια πηγή χρηματοδοτήσεις για την δημιουργία τέτοιων worms, ενώ αρκετοί δημιουργοί τους, έχουν συλληφθεί για την πώληση καταλογών με διευθύνσεις IP μολυσμένων μηχανημάτων, ενώ άλλοι προσπαθούν να εκβιάσουν εταιρείες υπό την απειλή Dos επιθέσεων.

Οι κερκόπορτες μπορούν να αξιοποιηθούν και από αλλά κακόβουλα προγράμματα, συμπεριλαμβανόμενων και των σκουληκιών. Χαρακτηριστικό παράδειγμα αυτού αποτελεί το doomjuice, το όποιο εξαπλώθηκε χρησιμοποιώντας την κερκόπορτα που είχε ανοίξει το Mydoom.

3.9.3 WORM ΜΕ ΚΑΛΗ ΠΡΟΘΕΣΗ

Αρχίζοντας με την πρώτη έρευνα για τα worm στο Xerox PARC, υπήρξαν προσπάθειες να δημιουργηθούν χρήσιμα σκουλήκια. Η οικογένεια των σκουληκιών Nachi, για παράδειγμα, προσπάθησε να κατεβάσει και να εγκαταστήσει patches από το δικτυακό τόπο της Microsoft με σκοπό την επιδιόρθωση των τρωτών σημείων.

Στην πράξη, παρόλο που μπορούν να κάνουν τα συστήματα αυτά πιο ασφαλή καθώς και να σκοτώνουν ορισμένους ιούς την ίδια ημέρα [5], σαν αντιστάθμισμα δημιουργούν σημαντική κίνηση δικτύου, προκαλούν την επανεκκίνηση του

υπολογιστή κατά τη διάρκεια της ενημέρωσης του κώδικα και όλα αυτά γίνονται χωρίς τη συγκατάθεση του ιδιοκτήτη του υπολογιστή ή του χρήστη.

Η πλειονότητα των ειδικών σε θέματα ασφάλειας θεωρούν όλα τα σκουλήκια ως κακόβουλα προγράμματα, ανεξαρτήτως του φορτίου ή των ενδεχομένως καλών προθέσεων των δημιουργών τους.

3.9.4 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΕΠΙΚΙΝΔΥΝΑ ΣΚΟΥΛΗΚΙΑ

Τα worm εξαπλώνονται εκμεταλλευόμενα τα τρωτά σημεία των λειτουργικών συστημάτων . Όλες οι κατασκευάστριες αντιβιοτικών παρέχουν τακτικές ενημερώσεις ασφάλειας και εφόσον αυτές έχουν εγκατασταθεί σε ένα υπολογιστή, τότε η πλειοψηφία των σκουληκιών δεν είναι σε θέση να εξαπλωθεί από αυτόν.

Εάν μια κατασκευάστρια είναι ενημερωμένη για ένα θέμα ευπάθειας αλλά δεν έχει ακόμα κυκλοφορήσει ένα patch για την ενημερωμένη έκδοση ασφάλειας, είναι πιθανή μια έκθεση μηδενικής ημέρας.

Θα πρέπει να είμαστε δύσπιστοι όσον αφορά το άνοιγμα απρόσμενης ηλεκτρονικής αλληλογραφίας και δεν θα πρέπει να τρέχουμε συνημμένα αρχεία ή προγράμματα, ή να επισκεπτόμαστε δικτυακούς τόπους που συνδέονται με τέτοιου είδους μηνύματα. Όπως και με το I Love you [39] τύπου worm, αλλά και με την παράλληλη ανάπτυξη και αυξημένη αποδοτικότητα των επιθέσεων τύπου phishing, εξακολουθεί να είναι δυνατόν να παραπλανηθεί ο τελικός χρηστή θέτοντας σε λειτουργιά ένα κακόβουλο κώδικα.

Ως μετρό πρόληψης για αυτού του είδους τις απειλές συνίσταται η χρήση Anti-virus και anti-spyware λογισμικών, τα όποια θα πρέπει να ενημερώνονται σε καθημερινή βάση, ενώ θα πρέπει να εκτελείται μια πλήρης σάρωση του τερματικού τουλάχιστον μια φορά την εβδομάδα. Φυσικά τα αποτελέσματα αυτά μπορούν να βελτιωθούν σημαντικά με την παράλληλη χρήση ενός τείχους προστασίας.

3.10. ΕΙΣΑΓΩΓΗ ROOTKITS

Ένας στους πέντε υπολογιστές έχει rootkits. Η επίθεση των rootkits συνεχίζεται με εντατικούς ρυθμούς, σύμφωνα με στοιχεία που αποκαλύπτονται από μια νέα έρευνα της εταιρείας Prevx [35] (www.prevx.com).

Σε διάστημα δύο μηνών ελέγχθηκαν με τη βοήθεια του λογισμικού Prevx csi της εταιρείας περισσότερα από 725.000 Pc και ενώ το ποσοστό των υπολογιστών

που είχαν εγκατεστημένο κάποιο rootkit [39] ήταν στο 15,6% σε αντίστοιχη μέτρηση τον Οκτώβριο (2008), αυξήθηκε στο 22% στις αρχές του Δεκεμβρίου.

Τα κακόβουλα rootkits μπορούν να επιτρέψουν σε έναν επιτιθέμενο εισβολέα να παρακολουθεί, να καταγράφει και να μεταφέρει πληροφορίες από έναν υπολογιστή εξ' αποστάσεως.

Παρ' όλο που δεν πρόκειται για μια καινούργια απειλή, η Prevx ισχυρίζεται ότι : "Η άνοδος των rootkits έχει ξεκινήσει", καθώς χρησιμοποιούνται ολοένα και πιο συχνά από όσους δημιουργούν κακόβουλο κώδικα για να έχουν πρόσβαση σε άλλους υπολογιστές χωρίς να εντοπίζονται.

Ακόμη, η Prevx τονίζει ότι ο εντοπισμός και η απομάκρυνση των rootkits είναι κάτι που ξεπερνά κατά πολύ τις δυνατότητες των παραδοσιακών προγραμμάτων antivirus και antispyware που αποκαλούνται security suites.

3.10.1 ΤΟ ROOTKIT

Τα rootkit [23,36,37] είναι προγράμματα ή συνδυασμός διαφόρων προγραμμάτων σχεδιασμένα με σκοπό να λάβουν τον πλήρη έλεγχο της λειτουργίας των υπολογιστών, χωρίς την άδεια από τους χειριστές τους.

Αυτό είναι δυνατό χωρίς κατά ανάγκη να υπάρχει πρόσβαση στο υλικό καθώς στοχεύουν στην λήψη ελέγχου του λειτουργικού συστήματος που εκτελείται στο υλικό.

Συνήθως τα rootkits επισκιάζουν την παρουσία τους μέσα από την καταστροφή των προτύπων μηχανισμών ασφαλείας των λειτουργιών συστημάτων, ενώ συχνά είναι και Trojan καταφέρνοντας έτσι να ξεγελάσουν τους χρήστες κάνοντας τους να πιστέψουν ότι είναι ασφαλής η εκτέλεση τους στο σύστημα.

Τεχνικές που χρησιμοποιούνται για να επιτευχθεί αυτό περιλαμβάνουν την απόκρυψη εκτελούμενων προγραμμάτων από προγράμματα παρακολούθησης, ή την απόκρυψη αρχείων ή δεδομένων του συστήματος από το λειτουργικό σύστημα.

Τα rootkits αρχικά έβρισκαν εφαρμογή σε έκτακτες καταστάσεις όπου έθεταν υπό έλεγχο συστήματα που δεν ανταποκρινόντουσαν, αλλά τα τελευταία χρόνια έχουν χρησιμοποιηθεί σε μεγάλο βαθμό ως κακόβουλα προγράμματα τα οποία και χρησιμοποιούνται για να βοηθήσουν τους εισβολείς να αποκτήσουν πρόσβαση σε συστήματα όπως τα Microsoft windows, Linux καθώς και δρουν συνήθως τροποποιώντας συνιστώσες των λειτουργικών συστημάτων ή εγκαθίστανται ως

οδηγοί ή λειτουργίες του πυρήνα ανάλογα με τις εσωτερικές λεπτομέρειες των μηχανισμών του εκάστοτε λειτουργικού συστήματος .

3.11 SPYWARE

Το spyware [27,48,49,50,51] είναι λογισμικό υπολογιστή το οποίο εγκαθίσταται με άγνοια του χρήστη με στόχο να σταματήσει ή να λάβει το μερικό έλεγχο της αλληλεπίδρασης του χρήστη με τον υπολογιστή.

Μια συνηθισμένη λειτουργία τους είναι να κατακλύζουν τους προσβεβλημένους υπολογιστές με pop-up διαφημίσεις. Η λειτουργικότητά τους παρόλα αυτά ξεπερνά κατά πολύ την απλή παρακολούθηση της συμπεριφοράς των χρηστών, καθώς είναι ικανά να συλλέξουν διάφορα είδη προσωπικών πληροφοριών όπως είναι οι συνήθειες που έχουν οι χρήστες κατά τη πλοήγηση τους στο διαδίκτυο, τους δικτυακούς τόπους που επισκέπτονται αλλά και η παρέμβαση τους στον έλεγχο του χρήστη εγκαθιστώντας επιπρόσθετο λογισμικό, ανακατευθύνοντας την λειτουργία των φυλλομετρητών και προσπελάζοντας ιστοσελίδες που μπορούν να προσβάλουν τον υπολογιστή με πολύ πιο επικίνδυνους ιούς.

Επιπρόσθετα είναι ικανά ακόμα και να αλλάξουν τις ρυθμίσεις του υπολογιστή προκαλώντας έτσι μείωση της ταχύτητας των συνδέσεων, σε διαφορετικές homepages στους περιηγητές καθώς και στην απώλεια των συνδέσεων αλλά και των προγραμμάτων.

3.11.1 ΙΣΤΟΡΙΑ ΚΑΙ ΕΞΕΛΙΞΗ SPYWARE

Η πρώτη καταγεγραμμένη χρήση του όρου spyware ήταν στις 16 Οκτωβρίου 1995 σε μια δημοσίευση η οποία γελοιοποιούσε το επιχειρησιακό μοντέλο της Microsoft.

Ενώ αρχικά ο όρος αυτός παρέπεμπε σε υλικό το οποίο χρησιμοποιούταν για κατασκοπευτικούς σκοπούς, στις αρχές του 2000 ο ιδρυτής των ZONE LABS, GREGOR FREUND, έκανε χρήση αυτού του όρου σε μία συνέντευξη τύπου για το τοίχος προστασίας του ZoneAlarm .

3.11.2 ΜΕΣΑ ΕΝΝΟΜΗΣ ΠΡΟΣΤΑΣΙΑΣ ΚΑΙ ΠΡΟΛΗΨΗΣ ΑΠΟ ΤΑ SPYWARE

Δεδομένου της ραγδαίας εξάπλωσης των spyware, μια σειρά από τεχνικές έχουν αναπτυχθεί, για να μετριάσουν αυτό το πρόβλημα. Αυτές περιλαμβάνουν τόσο προγράμματα σχεδιασμένα για την αφαίρεση ή το μπλοκάρισμα αυτών, όσο και διάφορες πρακτικές που πρέπει να υιοθετήσουν οι χρήστες για να μειώσουν την πιθανότητα να προσβληθεί ο υπολογιστής τους από spyware.

Στη πράξη παρόλο την δεδομένη ανάπτυξη μηχανισμών και διαδικασιών αφαίρεσης τους τα spyware εξακολουθούν να αποτελούν ένα σημαντικό πρόβλημα. Όταν ένας μεγάλος αριθμός από spyware έχει προσβάλει έναν υπολογιστή, η μόνη δυνατή λύση είναι η δημιουργία αντιγράφων ασφαλείας των δεδομένων του χρήστη και ακολούθως η επανεγκατάσταση του λειτουργικού συστήματος.

Εν γένη δύο είναι οι βασικοί τρόποι με τους οποίους τα anti-spyware προγράμματα είναι σε θέση να καταπολεμήσουν τα spyware [59]:

1) Μπορούν να παρέχουν προστασία σε πραγματικό χρόνο αποτρέποντας έτσι την εγκατάσταση κατασκοπευτικού λογισμικού στους υπολογιστές. Αυτού του είδους η προστασία κατά των spyware λειτουργεί με τον ίδιο ακριβώς τρόπο που λειτουργούν και τα antivirus προγράμματα δηλαδή ανιχνεύει όλη την εισερχόμενη κίνηση του δικτύου για τυχόν ύπαρξη κατασκοπευτικού λογισμικού και μπλοκάρει όλες τις πιθανές απειλές που εντοπίζει.
2) Ένας δεύτερος τρόπος λειτουργίας για τα anti-spyware προγράμματα είναι να χρησιμοποιούνται αποκλειστικά για τον εντοπισμό και την απομάκρυνση spyware λογισμικού που έχει ήδη εγκατασταθεί στον υπολογιστή. Αυτό το είδος της προστασίας είναι συνήθως πολύ πιο εύκολη στη χρήση και αρκετά πιο δημοφιλής, ενώ παράλληλα παρέχει στους χρήστες την δυνατότητα να προγραμματίζουν σε καθημερινό, εβδομαδιαίο ή και σε μηνιαίο επίπεδο, περιοδικές σαρώσεις του υπολογιστή με σκοπό την ανίχνευση και εξόντωση spyware λογισμικού που τυχών να έχει εγκατασταθεί σε αυτόν.

Όπως σε όλα τα λογισμικά προστασίας από malware έτσι και στα anti-spyware είναι επιτακτική η συχνή ενημέρωση της βάσης δεδομένων με τις νέες απειλές. Έτσι όταν υπάρξουν νέες απειλές οι προγραμματιστές τις εξετάζουν και τις αναλύουν δημιουργώντας στην συνέχεια υπογραφές ή ορισμούς που επιτρέπουν στο λογισμικό να τις ανιχνεύει και να τις εξαλείφει.

Ωστόσο δεν στηρίζονται όλα τα προγράμματα στην ενημέρωση της βάσης. Κάποια προγράμματα στηρίζονται εν μέρει. (Windows Defender) και άλλα εξολοκλήρου (WinPatrol) στην παρατήρηση του ιστορικού.

Ουσιαστικά αυτό που κάνουν είναι να παρατηρούν τις ρυθμίσεις των παραμέτρων όπως είναι οι ρυθμίσεις του περιηγητή ή ορισμένα τμήματα του μητρώου των Windows και αναφέρουν οποιαδήποτε αλλαγή στον χρήστη χωρίς να παρέχουν κρίση ή κάποια προτροπή.

Η έλλειψη αυτή οφείλεται στο γεγονός ότι δεν στηρίζονται στην ενημέρωση της βάσης με τα spyware όπου και θα τους επέτρεπε να εντοπίσουν νέες απειλές και άρα δεν είναι εφικτή η παροχή κάποιας σύστασης. Έτσι ο χρήστης μένει να αποφασίσει "τι ήταν αυτό που μόλις έκανε και ποία είναι η κατάλληλη αλλαγή της ρύθμισης".

Το Spynet προσπαθεί να δώσει λύση σε αυτό το πρόβλημα μέσω της δημιουργίας μιας κοινότητας που διαμοιράζεται πληροφορίες βοηθώντας τόσο τους χρήστες που μπορούν να κοιτάξουν αποφάσεις που έχουν ήδη ληφθεί από άλλους, όσο και τους αναλυτές που μπορούν να εντοπίσουν spyware τα οποία εξαπλώνεται γοργά.

Ένα άλλο δημοφιλές εργαλείο κατάργησης κατασκοπευτικού λογισμικού που χρησιμοποιείται από χρήστες με κάποιο βαθμό εμπειρίας είναι το HijackThis, το οποίο σαρώνει ορισμένες περιοχές του λειτουργικού συστήματος των Windows που συχνά εντοπίζονται spyware και παρουσιάζει μια λίστα με αντικείμενα τα οποία θα πρέπει να διαγραφούν χειροκίνητα.

Συνήθως μια καλή πρακτική για να αυξηθούν οι πιθανότητες αφαίρεσης επίμονων spyware είναι η εκκίνηση του μολυσμένου υπολογιστή σε ασφαλή λειτουργία. Ωστόσο μία νέα γενιά spyware(Look2Me από την NicTechNetworks) έχει αρχίσει να κρύβεται στο εσωτερικό των κρίσιμων διεργασιών του συστήματος εκκινώντας έτσι ακόμα και σε safe mode. Καθώς δεν υπάρχει καμία διαδικασία για να τερματιστεί και είναι δυσκολότερο να εντοπιστούν και να καταργηθούν και μερικές φορές δεν αφήνουν κανένα ίχνος υπογραφής στον δίσκο.

Ένα άλλο εξίσου ανησυχητικό στοιχείο είναι ότι παρουσιάζουν συγκεκριμένα αντίμετρα κατά γνωστών αντικατασκοπευτικών λογισμικών εμποδίζοντας τα να τρέχουν ή ακόμη και αποκαθιστώντας τα. Ένα χαρακτηριστικό παράδειγμα ενός spyware που χρησιμοποιεί αυτές τις μεθόδους είναι το Gromozon το οποίο χρησιμοποιεί εναλλακτικές ροές δεδομένων για να κρυφτεί.

Προκειμένου να αποτραπεί ή τουλάχιστον να περιοριστεί η πιθανή προσβολή από spyware, έχουν αναπτυχθεί αρκετές χρήσιμες πρακτικές πέρα από την εγκατάσταση anti-spyware προγραμμάτων.

Ξεκινώντας, μια καλή πρακτική είναι η εγκατάσταση ενός διαφορετικού περιηγητή από τον I.E όπως είναι ο Mozilla Firefox ή ο Opera. Αν και στην πράξη κανένας περιηγητής δεν είναι απόλυτα ασφαλής, για λόγους που έχουμε ήδη αναφέρει, ένας υπολογιστής ο οποίος έχει τον IE έχει τις περισσότερες πιθανότητες να προσβληθεί από spyware.

3.12 ADWARE

Το adware [27] είναι λογισμικό με λειτουργίες διαφήμισης οι οποίες ενσωματώνονται ή ομαδοποιούνται μαζί με ένα πρόγραμμα. Όπως εύκολα γίνετε αντιληπτό αυτού του είδους το λογισμικό έχει σαν απώτερο σκοπό την αποφορά χρημάτων στους συγγραφείς τους (λόγω των διαφημίσεων) παρακινώντας τους έτσι κατά αυτό τον τρόπο να συνεχίσουν να αναβαθμίζουν και να αναπτύσσουν νέο λογισμικό.

Μία άλλη δυνατότητα των adware είναι ότι μπορούν να κατεβάζουν και να εγκαθιστούν στον υπολογιστή PUPs (Potentially unwanted programs, ένας όρος που αναφέρεται σε λογισμικό που πιθανόν δεν θέλουμε να εγκατασταθεί χωρίς ωστόσο να είναι τόσο ενοχλητικό όσο είναι τα Spyware).

3.13 ΤΑ ΠΙΟ ΔΗΜΟΦΙΛΗΣ ΠΑΡΑΔΕΙΓΜΑΤΑ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ:

Ο ΙΟΣ MELISSA

Ο ιός Melissa [27] έκανε την εμφάνιση του την Παρασκευή 26 Μαρτίου 1999 και μπόρεσε να διαδοθεί σε ολόκληρο τον κόσμο μέσα σε μερικές ώρες κάτι που δεν είχε ξανασυμβεί ποτέ έως εκείνη την περίοδο.

Αυτός ο ιός εξαπλώθηκε με το να στέλνει αυτόματα σε email τον εαυτό του από τον ένα χρήστη στον άλλο. Όταν ο ιός ενεργοποιήθηκε τροποποιούσε τα έγγραφα του χρήστη παρεμβάλλοντας κάποια σχόλια από μια γνωστή τηλεοπτική εκπομπή (“the Simpsons”).

Ανησυχητικό ήταν το γεγονός ότι μπορούσε να στείλει και εμπιστευτικές πληροφορίες ενός χρήστη σε έναν άλλο.

Ο ιός “ χτύπησε ” μεγάλους οργανισμούς όπως η Microsoft και η Intel. Η Microsoft μάλιστα αναγκάστηκε να κλείσει τελείως το σύστημα του ηλεκτρονικού ταχυδρομείου της για να σταματήσει την περεταίρω εξάπλωση του ιού.

Ο Melissa αρχικά μεταδόθηκε σε φόρουμ συζητήσεων (alt.sex) Ο ιός εστάλη στους χρήστες με το όνομα List.Doc που περιείχε κωδικούς πρόσβασης από ιστοσελίδες που είχαν χαρακτηριστεί X-rated (σεξουαλικού περιεχομένου).

Όταν κάποιος άνοιγε το αρχείο, ο μακρό ιός εκτελείτο και έστελνε το list.doc με email σε 50 άτομα από το address book του χρήστη.
Το email είχε τη μορφή :

From: (name of infected user)
Subject: Important Message From (name of infected user)
To: (50 names from alias list)
Here is that document you asked for…don’t show anyone else ;-)
(Attachment: LIST.DOC)

Ο Melissa ενεργοποιούταν αν εκτελούνταν τα λεπτά από το ρολόι του συστήματος και συμπίπταν με την ημερομηνία. (π.χ. 15:30 στις 5 Ιανουαρίου)

ΠΑΡΑΣΚΕΥΗ ΚΑΙ 13-ΙΣΤΡΑΗΛ

Το υπολογιστικό Κέντρο του Εβραϊκού Πανεπιστημίου της Ιερουσαλήμ μολύνθηκε από έναν ιό που προσέβαλε ibm-pcs. Ο ιός αντέγραφε τον εαυτό του σε όλα τα προγράμματα που έτρεχαν στο μολυσμένο υπολογιστή. Παρόλα αυτά, υπήρχε ένα προφανές λάθος, καθώς ένα ήδη μολυσμένο πρόγραμμα θα μπορούσε να ξαναμολυνθεί από τον ιό. Σταδιακά, αυτό προκαλούσε την ανεξέλικτη αύξηση του

μεγέθους των προγραμμάτων, με αποτέλεσμα να μη χωρούν στη μνήμη του υπολογιστή.

Όταν τελικά απομονώθηκε ο ιός, ανακαλύφθηκε ότι ήταν προγραμματισμένος να ενεργοποιηθεί Παρασκευή και 13.Πολλοί πιστεύουν ότι στόχος ήταν η Παρασκευή, 13 Μαΐου 1988 η 40η επέτειος του Ισραήλ. Αν ο ιός είχε ενεργοποιηθεί, όλα τα μολυσμένα προγράμματα θα είχαν διαγραφεί από το δίσκο.

Ο ΙΟΣ MONKEY

Ο ιός monkey είναι ένας boot sector ιός που προσβάλλει το Master Boot Record: (MBR) του σκληρού δίσκου (αλλά και το boot sector των δισκετών). Εμφανίστηκε το 1991 στο Edmonton του Καναδά και γρήγορα διαδόθηκε στις ΗΠΑ, στην Αυστραλία και την Μεγάλη Βρετανία. Ο monkey είναι εκτός των άλλων stealth ιός [41], από τη στιγμή που καταφέρει να εξαπλωθεί στη μνήμη και δεν μπορεί να εντοπιστεί στον σκληρό δίσκο ή σε κάποια δισκέτα.

Η απομάκρυνση του παρακωλύεται περαιτέρω από το γεγονός ότι δεν υπάρχει πρόσβαση στον σκληρά δίσκο αν προσπαθήσουμε να επανακινήσουμε το σύστημα χρησιμοποιώντας κάποια δισκέτα εκκίνησης αφού λαμβάνουμε μηνύματα του τύπου: "Invalid drive specification"

Ο τρόπος διάδοσης του είναι να προσπαθήσουμε να κάνουμε boot το σύστημα με μία δισκέτα που είναι μολυσμένη. Σε αυτή τη περίπτωση αυτό που θα συμβεί είναι ότι θα προσπαθήσει το σύστημα να ξεκινήσει, διαβάζοντας την δισκέτα (για να δει εάν είναι boot δισκέτα) και θα τυπώσει το κλασικό μήνυμα: "No system disk” ή “disc error”) Από τη στιγμή αυτή ο ιός έχει εισβάλει στον υπολογιστή πρώτα στο MBR και έπειτα στη μνήμη.

Αυτό που συμβαίνει σε ένα σύστημα που έχει μολυνθεί από τον ιό πρακτικά είναι ότι όλο το σύστημα και η διαθέσιμη μνήμη μειώνεται κατά 1,024 bytes. Η εκκαθάριση τελικά του ιού μπορεί να γίνει είτε με την χρήση κάποιου antivirus προγράμματος (αναγκαστικά μέσω κάποιας δισκέτας εκκίνησης) είτε με τη χρήση εργαλείων fdisk (όπως πχ το Norton Disk Doctor) που μπορούν να ξαναφτιάξουν (να κάνουν"rebuild") το Master Boot Sector.

Επίσης είναι δυνατόν να επαναφέρουμε τις αρχικές ρυθμίσεις του πρωτότυπου Master Boot Record και του partition table εάν έχει γίνει backup πριν την μόλυνση.

Ο ΙΟΣ NYB (H B1)

Ο ιός NYB (New York boot) είναι ένας τυπικός Boot sector ιός, (εμφανίστηκε κάπου στα τέλη του 1994), ο οποίος μολύνει όπως και ο monkey μόνο αν προσπαθήσουμε να κάνουμε εκκίνηση ενός συστήματος με μία μολυσμένη δισκέτα. Εκείνη τη στιγμή ο ιός περνάει στο Main Boot Record και στη συνέχεια "κατοικεί" στην high dos μνήμη σε κάθε επανεκκίνηση του υπολογιστή. Ο NYB είναι και αυτός ένας stealth ιός οπότε οι διάφορες αλλαγές στο MBR δεν είναι ορατές.

Κάθε φορά που έχουμε πρόσβαση στη δισκέτα υπάρχει μεγάλη πιθανότητα να ενεργοποιηθεί ο ιός. Τότε υπάρχει η περίπτωση να καταστραφεί η κεφαλή της δισκέτας (και επομένως και η ίδια η δισκέτα). Τέλος ενδιαφέρον έχει ότι από τους περισσότερους μελετητές των ιών "ξέφυγε" ένας άλλος τρόπος ενεργοποίησης του. Έτσι το σύστημα μπορεί συντριβή εάν επιχειρηθεί εγγραφή όταν το ρολόι του υπολογιστή έχει όλα τα πεδία μηδέν (όταν δηλαδή είναι μεσάνυχτα).

I LOVE YOU

Στις 4 Μαΐου του 2000 εμφανίστηκε το σκουλήκι των ερωτικών γραμμάτων το λεγόμενο I LOVE YOU [27]. Το σκουλήκι αυτό ήταν ένα πρόγραμμα σε VBScript, το οποίο εξαπλωνόταν με διάφορους τρόπους. Στις 5μ.μ της 8^{ης} Μαΐου 2000 το συντονιστικό κέντρο του cert είχε λάβει αναφορές από 650 και πλέον ιστοσελίδες για περισσότερα από 500.000 <<μολυσμένα>> συστήματα.

Επιπλέον, υπήρξαν αρκετές αναφορές από ιστοσελίδες που είχαν υποστεί σοβαρές ζημιές στο δίκτυο τους λόγω αυξημένης κίνησης τόσο στο ηλεκτρονικό ταχυδρομείο, όσο και σε διαδικτυακά αρχεία που προερχόταν από το I love you.

Το σκουλήκι εισέβαλε στο εκάστοτε σύστημα τόσο από το ηλεκτρονικό ταχυδρομείο, όσο και από άλλες διαδικτυακές δραστηριότητες, όπως Windows File Sharing, irc, usenet news και πιθανόν από ιστοσελίδες.

Όταν εκτελούταν ο κώδικας I love you προσπαθούσε να στείλει αντίγραφα του εαυτού του σε όλες τις ηλεκτρονικές διευθύνσεις που ήταν καταχωρημένες στο Microsoft outlook. Το μήνυμα που στελνόταν είχε τα εξής χαρακτηριστικά:

Ένα συνημμένο αρχείο με το όνομα ”LOVE-LETTER-FOR-YOU.TXT.VBS”
Θέμα: I LOVE YOU
Το περιεχόμενο του μηνύματος ήτανε ήταν: <<Παρακαλώ κοιτάξτε το συνημμένο ΕΡΩΤΙΚΟ ΜΗΝΥΜΑ που σας στέλνω>>.

Ο ΙΟΣ CONCEPT

Εμφανίστηκε το 1995 και είχε σαν στόχο το Microsoft Word (windows). Ο ιός αυτός εκτελείτε κάθε φορά που ανοίγει ένα μολυσμένο έγγραφο και προσπαθεί να μολύνει το NORMAL.DOD.

Αν εντοπίσει κάποια από τις μακρό εντολές payload ή file save as υποθέτει ότι ο ιός υπάρχει ήδη όποτε σταματήσει την λειτουργιά του. Αν όμως δεν βρει τις παραπάνω εντολές τότε αρχίζει να γραφεί τις κακόβουλες εντολές και εμφανίζει ένα μικρό μήνυμα στη οθόνη: Το μήνυμα αυτό εμφανίζεται μόνο κατά την αρχική μόλυνση του NORMAL.DOT. Από τη στιγμή αυτή ο ιός περνάει σε κάθε κείμενο που δημιουργήθηκε με την Save As εντολή.

PAKISTANI-BRAIN VIRUS

Ένας από τους πιο γνωστούς ιούς στον κόσμο των IBM-PCS υπήρξε ο Pakistani (Πακιστανός) ή Brain (Εγκέφαλος) ιός [38]. Θεωρείται ο πρώτος ιός που προσέβαλε Η/Υ εκτός εργαστηρίου.

Σύμφωνα με την Ann Webster του Ακαδημαϊκού Υπολογιστικού Κέντρου του Πανεπιστημίου του Delaware, Newark η πρώτη αναφορά χρονολογείται στις 22 Οκτώβρη του 1987. Είχε εντοπιστεί και σε άλλες τοποθεσίες στο χώρο του Πανεπιστημίου μία ή δύο μέρες νωρίτερα.

Ονομάστηκε BRAIN (Εγκέφαλος), διότι ονόμαζε έτσι όποια δισκέτα προσέβαλε. Μετά την αρχική ανάλυση του ιού βρέθηκαν δύο ονόματα, Basit και

Admjad και η διεύθυνση τους ήταν στο LEHORE, Πακιστάν. Έτσι ο BRAIN απέκτησε το όνομα PAKISTANI (Πακιστανός).

Όταν, λοιπόν μία «μολυσμένη» δισκέτα εισερχόταν σε κάποιον υπολογιστή, ο ιός έφτιαχνε αντίγραφα του εαυτού του στις υψηλότερες θέσεις μνήμης και άλλαζε το μέγεθος της μνήμης που έβλεπε το σύστημα τροποποιώντας το interrupt vector (διάνυσμα διακοπής) A2H με σκοπό να προστατέψει το αντίγραφο που είχε φτιάξει.

Επίσης τροποποιούσε και το interrupt vector 13H ώστε να δείχνει στον κώδικα του στις υψηλές θέσεις μνήμης και το 6H (αχρησιμοποίητο από τις υπάρχουσες εκδόσεις του DOS) ώστε να δείχνει στο interrupt vector 13H.

Η «μολυσμένη δισκέτα περιλάμβανε ένα μήνυμα και μέρος του κώδικα του ιού στον τομέα (sector) εκκίνησης. Ο υπόλοιπος κώδικας και ένα αντίγραφο του αρχικού τομέα εκκίνησης (boot sector) της δισκέτας περιλαμβανόταν σε τρεις ομάδες (clusters) (ή έξι τομείς - sector), τις οποίες ο ιός ονόμαζε «χαλασμένες» στο FAT.

Με τον ιό στις υψηλές θέσεις μνήμης ήταν αδύνατο να διαβαστεί ο μολυσμένος τομέας εκκίνησης. Αν γινόταν κάποια προσπάθεια να διαβαστεί ο τομέας εκκίνησης, τότε ο Πακιστανός κατεύθυνε την αίτηση ανάγνωσης στον αρχικό τομέα εκκίνησης που αποθήκευε σε κάποια από τις «χαλασμένες» ομάδες.

Ο μόνος τρόπος να αναγνωστεί το μήνυμα του Εγκεφάλου που βρισκόταν στον τομέα εκκίνησης ήταν να εκκινήσεις το σύστημα με μία μη «μολυσμένη» δισκέτα και να τοποθετήσεις τη «μολυσμένη» δισκέτα στην κεφαλή (drive).

Η ΧΡΙΣΤΟΥΓΕΝΝΙΑΤΙΚΗ ΚΑΡΤΑ ΤΗΣ IBM

Ο ιός Χριστουγεννιάτικη Κάρτα της IBM δεν ήταν ακριβώς ένας ιός και δε μόλυνε μεμονωμένα υπολογιστικά συστήματα. Είχε όμως τρομακτικά αποτελέσματα στο ηλεκτρονικό ταχυδρομείο της IBM κατά τη διάρκεια του Δεκεμβρίου του 1987.

Το πρόγραμμα του ιού ήταν ένα ηλεκτρονικό μήνυμα (email), το οποίο δημιουργήθηκε στην Ευρώπη. Το μήνυμα εμφάνιζε μια Χριστουγεννιάτικη κάρτα στην οθόνη του αποδέκτη, ενώ έστελνε αντίγραφα του εαυτού του σε όλες τις διευθύνσεις email του <<βιβλίου διευθύνσεών του>>.

Το μήνυμα σύντομα διέσχισε τον Ατλαντικό Ωκεανό και διείσδυσε σε άλλα δίκτυα email συμπεριλαμβανομένου και του παγκόσμιου δικτύου της IBM. Κατόπιν, τα δίκτυα email γέμισαν από αντίγραφα της Χριστουγεννιάτικης κάρτας μπαίνοντας

τελικά σε κατάσταση αναμονής. Χρειάστηκαν από μία μέχρι τρεις μέρες για να «καθαρίσουν» τα δίκτυα από το μήνυμα της Χριστουγεννιάτικης κάρτας.

SOBIG

Ο ιός με την κωδική ονομασία “ SoBig” προκάλεσε πολύ μεγάλα προβλήματα στους χρήστες των υπολογιστών σε όλο των τον κόσμο. Ο ιός χτυπά τους υπολογιστές και διαδίδεται μέσω του ηλεκτρονικού ταχυδρομείου. Ενεργοποιείται με το άνοιγμα ενός αρχείου που έρχεται συνημμένο σε ένα email το οποίο αναφέρει ότι πρόκειται για ένα αρχείο προστασίας οθόνης ή ρυθμίσεων.

Η εταιρεία ασφαλείας υπολογιστών MessageLabs ανακοίνωσε ότι μέσα σε μια μόνο ημέρα εντόπισε ένα εκατομμύριο αντίγραφα του Sobig που μεταδίδεται μέσω του ηλεκτρονικού ταχυδρομείου και έχει ήδη μολύνει χιλιάδες υπολογιστές σε 150 περίπου χώρες.

Ο ιός αλλάζει τακτικά την περιγραφή του στο θέμα του ηλεκτρονικού μηνύματος και το όνομα του συννημένου αρχείου και όσοι μολύνονται από τον ιό, λαμβάνουν αρκετά αντίγραφα του, με μηνύματα που μοιάζουν μεταξύ τους.

Ο MVF ΙΟΣ

Ο MVF είναι ένας πολυμορφικός ιός που εμφανίστηκε το 1992 στη Ρωσία και έχει σαν στόχο τα .COM αρχεία.(συμπεριλαμβανομένου του comand.com). Από τη στιγμή που ένα μολυσμένο πρόγραμμα εκτελεστεί ο MVF εγκαθίσταται στην μνήμη ως TSR, (Terminate and stay recident).Από τη στiγμή που βρίσκεται ο ιός στη μνήμη θα μολύνει κάθε .COM πρόγραμμα που εκτελείται.

ΕΙΣΒΟΛΗ ΣΤΗ MICROSOFT

Το Φθινόπωρο του 2000 έγινε ένα σοβαρό περιστατικό εισβολής στο δίκτυο της Microsoft. Χωρίς να έχουν γνωστοποιηθεί πολλά για την υπόθεση και το είδος της προσπέλασης που είχαν αποκτήσει οι εισβολείς είναι σίγουρο πως η φήμη της εταιρείας είχε δεχτεί κάποιο πλήγμα.

Η επίθεση φαίνεται πως ξεκίνησε από τον υπολογιστή στο σπίτι ενός υπαλλήλου που συνδεόταν με το δίκτυο της εταιρείας. Από εκεί, λοιπόν, ένας Δούρειος ίππος με όνομα Qaz μεταφέρθηκε στο εσωτερικό του δικτύου και μεταδόθηκε μέσω του ηλεκτρονικού ταχυδρομείου και αυτόματης αντιγραφής του μέσω διαμοιρασμένων φακέλων, αλλάζοντας τη γνωστή εφαρμογή Notepad με τον εαυτό του.

Με την ενεργοποίηση του Quaz.trojan ψάχνει για την εφαρμογή Notepad.exe και αντιγράφει τον εαυτό του στη θέση του μετονομάζοντας το αυθεντικό σε note.exe. Κάθε φορά κάποιος που τρέχει το μεταλλαγμένο notepad.exe εκτελείται και το Note exe, ώστε ο χρήστης να μην διαπιστώνει κάποιο πρόβλημα. Κατόπιν ψάχνει στο δίκτυο για να μολύνει και άλλα αντίγραφα του Notepad.exe. Από τη στιγμή που μολύνει ένα σταθμό, στέλνει με email στο hacker την IP διεύθυνσή του.

Η ΕΠΙΘΕΣΗ ΤΩΝ ΟΛΛΑΝΔΩΝ HACKERS

Την 1^{η} Απριλίου του 1990 ξεκίνησε η προσπάθεια εισβολής στο domain.mil (Αμερικανικός Στρατός) και διήρκεσε σχεδόν δύο χρόνια. Το CERT /CC αναφέρεται ως το πιο μακροχρόνιο περιστατικό και είχε προσβάλει 383 sites, ένα εκ των οποίων ήταν ελληνικό. Η εν λόγω επίθεση εκτυλισσόταν κατά τη διάρκεια του Περσικού πολέμου και ορισμένες από τις προεκτάσεις της μπορούσαν να είχαν επιπτώσεις στην αποστολή.

Οι Hackers εισέβαλαν σε 34 αμερικάνικα στρατιωτικά sites στο ίντερνετ, συμπεριλαμβανομένων και sites που συμμετείχαν στην επιχείρηση «Desert Storm/Shield>>. Αναζήτησαν λέξεις όπως <<πυρηνικά>>, <<όπλα>>, <<πύραυλοι>> και βρήκαν πληροφορίες για την ακριβή θέση των αμερικανικών στρατευμάτων, τον τύπο των όπλων τους, τις δυνατότητες των πυραύλων Patriot και τις κινήσεις των αμερικανικών πλοίων.

Ο Jim Christy, ένας από τους υπεύθυνους του προγράμματος για την ανακάλυψη εγκλημάτων σε θέματα πολέμου των πληροφοριών, του γραφείου της αμερικανικής αεροπορίας αναφέρει ότι οι επιθέσεις αφορούσαν και συστήματα τροφοδοσίας των στρατευμάτων στον Κόλπο. Χαρακτηριστικά είχε δηλώσει στο ABCNews: “θα μπορούσαν ενώ για πυρομαχικά να έχουν στείλει και οδοντόβουρτσες”.

Οι hackers συγκέντρωσαν μέρος της πληροφορίας τους σε χώρο των υπολογιστικών συστημάτων στο Bowling Green University και στο University of Chicago. Οι εισβολείς επιχείρησαν ακόμη και να πουλήσουν πληροφορίες στους Ιρακινούς κατά τη διάρκεια του πολέμου.

Η πληροφορία μεταδόθηκε μέσω του BBC, που πήρε τη πληροφορία από κυβερνητικούς αξιωματούχους του Ιράκ αλλά ο Σαντάμ Χουσεΐν αρνήθηκε τη προσφορά των hackers γιατί θεώρησε ότι ήτανε παγίδα.

Οι εισβολείς ακόμα και όταν εντοπίστηκαν δεν ήταν δυνατό να συλληφθούν, καθώς εκείνο το καιρό οι επιθέσεις σε υπολογιστές δεν ήταν παράνομες. Το FBI προσπάθησε να παγιδεύσει τον εμπνευστή της ομάδας των hackers,φέρνοντας τον στην Αμερική με πρόφαση μια συνέντευξη για δουλειά από μεγάλη αεροναυπηγική εταιρεία στη Florida, μα εκείνος αθέλητα ειδοποιήθηκε και το αντιλήφθηκε. Εν τέλει δύο από τους Ολλανδούς hackers συλλαμβάνονται και οδηγούνται στη φυλακή για παραποίηση στοιχείων και χρήση της πιστωτικής κάρτας.

ΚΕΦΑΛΑΙΟ 4

4.1 ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Το κακόβουλο λογισμικό είναι ένας ιδιαίτερα καταστροφικός εχθρός της ασφάλειας σε οποιοδήποτε πληροφοριακό σύστημα. Για τον λόγο αυτό είναι απαραίτητο να υπάρχει μια στρατηγική πρόληψης και αντιμετώπισής του. Η στρατηγική αυτή έχει δυο σκέλη το διαδικαστικό που αφορά ενέργειες που πρέπει ή δεν πρέπει να κάνει ο χρήστης ή ο διαχειριστής και το τεχνικό που περιλαμβάνει λογισμικό και τις ρυθμίσεις.

Όσον αφορά το διαδικαστικό σκέλος θα πρέπει η επεξεργασία των δεδομένων μας να γίνετε μόνο με προγράμματα τα όποια είναι ελεγμένα, δεν περιέχουν κακόβουλο λογισμικό και είναι βέβαιο ότι δεν θα μολυνθούν.

Είναι απαραίτητο να αποφεύγουμε την λήψη και εκτέλεση αρχείων που έχουν επισυναφτεί σε ύποπτα μηνύματα από μη αξιόπιστους ιστότοπους ή από newsgroups. Επειδή τα προγράμματα αυτά είναι το κυριότερο μέσο διάδοσης των ιών γι’ αυτό εμείς οι χρηστές πρέπει να αποφεύγουμε την εκτέλεση τους.

Θα πρέπει να κάνουμε συχνή λήψη εφεδρικών αντίγραφων ασφαλείας ανεξάρτητα από τα μετρά που θα πάρουμε για την προστασία και την αποφυγή μόλυνσης του συστήματος μας όπου υπάρχει η περίπτωση το σύστημα μας να μολυνθεί.

Έτσι θα πρέπει να είμαστε σε θέση να αποκαταστήσουμε το σύστημα μας από την μόλυνση γι’ αυτό και πρέπει να τηρούμε τα εφεδρικά αντίγραφα για πολύ καιρό ώστε να είμαστε σε θέση σε περίπτωση μόλυνσης να τα αντικαταστούμε με τα αντίστοιχα “καθαρά.” Όσον αφορά το τεχνικό σκέλος απαγορεύεται η εκκίνηση από μονάδες δισκέτας ,CD, DVD.

Αυτό απαγορεύεται γιατί οι περισσότεροι ιοί τομέων εκκίνησης μολύνουν το σύστημα μας κατά την εκκίνηση από μολυσμένη δισκέτα κ.τ.λ. Γι’ αυτό δεν θα πρέπει να ξεκινάμε τον υπολογιστή με δισκέτα μέσα στην μονάδα , ενώ το BIOS του υπολογιστή μας θα πρέπει να είναι ρυθμισμένο κατάλληλα έτσι ώστε να μην προσπαθεί να κάνει την εκκίνηση από την δισκέτα, DVD, CD.

Είναι απαραίτητο να ρυθμίζουμε τον υπολογιστή μας στο μέγιστο επίπεδο ασφάλειας. Οι ρυθμίσεις αυτές ισχύουν για τα προγράμματα πλοήγησης, ανάγνωση

ηλεκτρονικού ταχυδρόμου και γενικά για όλες την εν δυνάμει πύλες εισόδου κακόβουλου λογισμικού στο σύστημα.

Θα πρέπει να έχουμε εγκατεστημένο και καλά ενημερωμένο κάποιο ειδικό λογισμικό για την αντιμετώπιση κακόβουλου λογισμικού και το όποιο θα αναλύσουμε παρακάτω.

4.2 ΛΟΓΙΣΜΙΚΟ ΠΡΟΣΤΑΣΙΑΣ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ (ANTIVIRUS)

Το Antivirus είναι λογισμικό το οποίο έχει δημιουργηθεί από διάφορες εταιρείες κατασκευής λογισμικού (π.χ. Microsoft).

Υπάρχουν πολλοί προμηθευτές που παράγουν το λογισμικό Antivirus. Όλα τα Antivirus εκτελούν την ίδια λειτουργία με παρόμοιο τρόπο, έτσι η απόφασή μας μπορεί να οδηγηθεί από τις συστάσεις, τα ιδιαίτερα χαρακτηριστικά γνωρίσματα, τη διαθεσιμότητα, ή την τιμή.

Η εγκατάσταση οποιουδήποτε λογισμικού Antivirus, ανεξάρτητα από ποιο επιλέξαμε, αυξάνει το επίπεδο προστασίας του υπολογιστή μας.

Το Antivirus είναι αυτό το οποίο μπορεί να προσδιορίσει και να εμποδίσει πολλούς ιούς προτού να μπορέσουν να μολύνουν τον υπολογιστή μας. Γι’ αυτό θα πρέπει όλοι μας να έχουμε εγκατεστημένο κάποιο Antivirus αλλά δεν αρκεί μόνο αυτό. Το antivirus θα πρέπει να ενημερώνετε όσο πιο συχνά γίνετε.

Επειδή στηρίζεται στις υπογραφές των updates (των νέων ιών) το λογισμικό Antivirus μπορεί μόνο να ανιχνεύσει τους ιούς για τους οποίους έχει ενημερωθεί, έτσι είναι σημαντικό να διατηρείτε ενημερωμένο.

Εφόσον νέοι ιοί δημιουργούνται καθημερινά, οι κατασκευάστριες εταιρείες εντοπίζουν και ενσωματώνουν τις νέες υπόγραφες των νέων ιών στο antivirus τους. Αν και οι λεπτομέρειες μπορούν να ποικίλουν μεταξύ των συσκευασιών, το λογισμικό Antivirus ανιχνεύει τα αρχεία ή τη μνήμη του υπολογιστή μας για αρχεία που μπορούν να αρχίσουν μια μόλυνση.

Τα αρχεία που ψάχνει είναι βασισμένα στις υπογραφές, ή τους ορισμούς, των γνωστών ιών. Θα είμαστε ακόμα “ευαίσθητοι” στους ιούς που κυκλοφορούν προτού το updates του Antivirus.

Έτσι καλύτερα να παίρνουμε και άλλες προφυλάξεις ασφάλειας (π.χ. να μην ανοίγουμε συνημμένα αρχεία από άγνωστες πηγές κ.τ.λ.).

Όταν εγκαταστήσουμε κάποιο από τα Antivirus που κυκλοφορούν στην αγορά, θα πρέπει να ανιχνεύσουμε τον υπολογιστή μας για ιούς γιατί μπορεί να έχουν μολύνει το σύστημα μας ήδη και να μην το γνωρίζουμε .

Οι αυτόματες ανιχνεύσεις που εξαρτώνται από ποιο Antivirus έχουμε μπορεί και είναι σε θέση να ανιχνεύσουν αυτόματα τα συγκεκριμένα αρχεία ή τους καταλόγους και να μας προστατέψουν σε καθορισμένα διαστήματα. Υπάρχει βέβαια και η χειροκίνητη ανίχνευση η οποία είναι επίσης μια καλή ιδέα να ανιχνεύουμε τα αρχεία που λαμβάνουμε από μια εξωτερική πηγή όπως το email,CDs,DVDs κ.λπ. πριν τα ανοίξουμε.

4.3 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ANTIVIRUS ΟΤΑΝ ΕΝΤΟΠΙΖΕΙ ΙΟΥΣ

Υπάρχουν διάφορα Antivirus κάθε ένα από αυτά έχει και την δική του μέθοδο απάντησης όταν εντοπίζει έναν ιό και η απάντηση μπορεί να διαφέρει σύμφωνα με το εάν το λογισμικό εντοπίζει τον ιό κατά τη διάρκεια μιας αυτόματης ή χειροκίνητης ανίχνευσης.

Συνήθως το λογισμικό παράγει ένα πλαίσιο διαλόγου που θα μας προειδοποιήσει ότι έχει βρει έναν ιό και θα ρωτήσει εάν θέλουμε "να καθαρίσει" το αρχείο (για να διαγράψει τον ιό).

Σε άλλες περιπτώσεις, το λογισμικό μπορεί να προσπαθήσει να διαγράψει τον ιό χωρίς να μας ρωτήσει πρώτα. Όταν επιλέγουμε μια συσκευασία Antivirus, θα πρέπει να εξοικειωνόμαστε με τα χαρακτηριστικά γνωρίσματά ώστε να ξέρουμε πως λειτουργεί.

Το καλοκαίρι του 2010 μόλις τελείωσε και τα antivirus για το 2011 έχουν ήδη κυκλοφορήσει. Το Norton 2011 αναμένεται σύντομα, επίσης antivirus θα κυκλοφορήσουν η Trend Micro, η Spyware Doctor και άλλες εταιρείες. Επιπλέον διαθέσιμα είναι το: Bit Defender Antivirus Pro 2011, το Kaspersky Anti-Virus 2011, το Panda Antivirus Pro 2011 και το AntiVirus Webroot Spy Sweeper 2011 και έχουν ήδη περάσει τις δοκιμές.

Αν ψάχνετε να αγοράσετε antivirus, σήμερα, τα αποτελέσματα δείχνουν ότι υπάρχουν ήδη ορισμένες καλές επιλογές που είναι στη διάθεσή σας. Όμως, πολύ λίγα από τα antivirus 2011 είναι δωρεάν και έχουν ήδη κυκλοφορήσει στην αγορά.

Να σημειώσουμε ότι, όπως πάντα, όταν λέμε “antivirus” εννοούμε ένα βοηθητικό πρόγραμμα που προστατεύει από κάθε είδους κακόβουλο λογισμικό όχι μόνο από

τους ιούς. Ένα σωστό antivirus πρέπει να προστατεύει ένα δίκτυο από Trojans, spyware, rootkits, keyloggers, adware, scareware.

4.4 ΕΡΓΑΛΕΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ MALWARE

Το λογισμικό αντιμετώπισης Malware είναι μία πολυσύνθετη κατηγορία λογισμικού που περιλαμβάνει εργαλεία με στόχο [24]:

1)Την ανίχνευση. Τα εργαλεία ανίχνευσης προσδιορίζουν και αναφέρουν αν το σύστημα μας έχει μολυνθεί. Η ανίχνευση μπορεί να γίνεται είτε με ανάλυση των αντικειμένων του συστήματος είτε σε περιοδική βάση ή κατά τη χρησιμοποίηση τους, με παρεμπόδιση των παράνομων ενεργειών ή με ανίχνευση των αναιτιολόγητων αλλαγών.

2)Τον προσδιορισμό της ταυτότητας του κακόβουλου λογισμικού. Αν το σύστημα μας έχει μολυνθεί από ιό, ένα εργαλείο προσδιορισμού ταυτότητας θα μας πληροφορήσει για το ποιος συγκεκριμένος ιός έχει προκαλέσει τη μόλυνση. Ο προσδιορισμός ταυτότητας είναι χρήσιμος αφ' ενός για να μπορέσουμε να αποτιμήσουμε το μέγεθος της ζημιάς και τον πιθανό κίνδυνο που διατρέχουμε, αφ' ετέρου δε για να χαράξουμε τη βέλτιστη στρατηγική επανόρθωσης.

3) Τον καθαρισμό του κακόβουλου λογισμικού. Σε πολλές περιπτώσεις οι αλλαγές που έχουν επιφέρει τα Malware στο σύστημα είναι αντιστρέψιμες με αυτοματοποιημένο τρόπο. Τα εργαλεία καθαρισμού φροντίζουν για την αναίρεση των αλλαγών που έχουν προκληθεί.

4.5 ΕΝΤΟΠΙΣΜΟΣ ΥΠΟΓΡΑΦΩΝ

Η μέθοδος αυτή χρησιμοποιείται κυρίως από εργαλεία εντοπισμού ιών, τα οποία δρουν παράλληλα και ως εργαλεία προσδιορισμού ταυτότητας των ιών, και τα οποία επιχειρούν να ανιχνεύσουν αν υπάρχει ιός προσκολλημένος σε αντικείμενα του δίσκου ή εγκατεστημένος στη μνήμη. Τα εργαλεία αυτά είναι δυνατόν να ελέγχουν τα αντικείμενα σε κάθε πρόσβαση που γίνεται σε αυτά, ή σε περιοδική βάση, π. χ. μία

φορά κάθε εβδομάδα. Με τον όρο «υπογραφή ιού» περιγράφεται μία ακολουθία από bytes τα οποία είναι γνωστό ότι ανήκουν σε ιούς ή οικογένειες ιών.

Μία ακολουθία από bytes που θα χρησιμοποιηθεί ως υπογραφή ενός ιού θα πρέπει να έχει τα εξής δύο χαρακτηριστικά:

1. να υπάρχει σε όλα τα αρχεία που έχουν μολυνθεί από το ιό.

2. να είναι αδύνατον (ή τουλάχιστον σχετικά απίθανο) να εμφανιστεί συγκεκριμένη ακολουθία σε αρχεία που δεν έχουν μολυνθεί από τον ιό.

Οι υπογραφές συλλέγονται από μολυσμένα αντικείμενα, μετά από ανάλυση τους. Μία υπογραφή μπορεί να περιέχει μεταχαρακτήρες, προκειμένου να αντιμετωπίζονται περιπτώσεις όπου συγκεκριμένα bytes μπορούν να αλλάζουν ανάμεσα σε διαφορετικά αντικείμενα που έχουν μολυνθεί από τον ίδιο ιό.

Η υπογραφή μπορεί να συμπληρώνεται από κάποια ένδειξη θέσης εντός του αντικειμένου, π.χ. «τα πρώτα bytes του αντικειμένου» (περίπτωση που θα κάλυπτε τους ιούς που επικαλύπτουν τον εκτελέσιμο κώδικα), «τα τελευταία bytes του αντικειμένου» (π.χ. ιοί που προσκολλώνται στο τέλος και τοποθετούν εντολές άλματος στην αρχή των αντικειμένων) ή «μέσα στα 300 πρώτα bytes του αντικειμένου».

Η παράθεση της ένδειξης θέσης είναι χρήσιμη αφ' ενός διότι μειώνει το πλήθος των bytes που πρέπει να ελεγχθούν για ύπαρξη της υπογραφής, αφ' ετέρου δε διότι μειώνει την πιθανότητα να ανιχνευθεί η υπογραφή σε κάποιο σημείο όπου η παρουσία της δεν υποδηλώνει ύπαρξη ιού. Οι πολυμορφικοί ιοί είναι δύσκολο να ανιχνευθούν μέσω υπογραφών καθώς μεταλλάσσονται τόσο πολύ μεταξύ δύο μολύνσεων που δεν έχουν κάποια σταθερή «υπογραφή». Για τους ιούς αυτούς απαιτείται αλγοριθμική ανίχνευση.

Εντοπισμός υπογραφών – Σύνοψη

Τα θετικά σημεία της τεχνικής εντοπισμού υπογραφών καθώς και των εργαλείων που βασίζονται σ' αυτή είναι τα εξής:

Υπέρ	***Κατά***
Τα καλά συντηρούμενα συστήματα εντοπίζουν άνω του 95% των ιών	Βρίσκουν μόνο τους ιούς που είναι γνωστοί κατά την ανάπτυξη του «πακέτου υπογραφών»
Δοκιμασμένη τεχνολογία με βελτιστοποιημένους αλγορίθμους	Είναι επιρρεπή σε εσφαλμένους προσδιορισμούς ταυτότητας
Απαιτείται ελάχιστη γνώση	Οι χρήστες παρανοούν το ότι δεν ανιχνεύθηκε ο ιός πιστεύοντας ότι σημαίνει ότι δεν υπάρχει ο ιός

(ΠΙΝΑΚΑΣ 6. ΘΕΤΙΚΑ ΚΑΙ ΑΡΝΗΤΙΚΑ ΣΗΜΕΙΑ ΤΗΣ ΤΕΧΝΙΚΗΣ ΤΟΥ ΕΝΤΟΠΙΣΜΟΥ ΤΩΝ ΥΠΟΓΡΑΦΩΝ)

4.6 ΕΠΟΠΤΕΣ ΓΕΝΙΚΟΥ ΣΚΟΠΟΥ

Οι επόπτες γενικού σκοπού [24,28] προστατεύουν το σύστημα από τη διάδοση ιών ή τη δράση των Δούρειων Ίππων αναχαιτίζοντας κακόβουλες ενέργειες. Προκειμένου να αναχαιτισθεί μία κακόβουλη ενέργεια θα πρέπει πρώτα να είναι δυνατόν να διαχωριστούν οι ενέργειες που λαμβάνουν χώρα σε ένα σύστημα σε <<φυσιολογικές>> και <<κακόβουλες>>.

Οι κατασκευαστές των σχετικών εργαλείων μοντελοποιούν τη συμπεριφορά των ιών και των δούρειων ίππων και δημιουργούν κώδικα που προσπαθεί να ανιχνεύσει και να παρεμποδίσει τις ενέργειες αυτές.

Παραδείγματα μοντέλων κακόβουλων συμπεριφορών μπορούμε να παραθέσουμε τα κάτωθι [32]:

1) ένα πρόγραμμα ζητά μνήμη που «αυτονομείται»
2) ένα πρόγραμμα ανοίγει αρχεία συστήματος
3) ένα πρόγραμμα ανοίγει εκτελέσιμα σε άλλους καταλόγους
4) μία μακροεντολή σε ένα έγγραφο διαγράφει αρχεία MP3

Οι ενέργειες αυτές δεν είναι «φυσιολογικές» και δεν είναι πολύ πιθανό να γίνονται από «κανονικά» προγράμματα. Κατά συνέπεια, η εμφάνιση μιας τέτοιας ενέργειας είναι πολύ πιθανό να σηματοδοτεί τη δράση ενός Malware.

Επόπτες γενικού σκοπού – Σύνοψη

Τα θετικά και τα αρνητικά σημεία της τεχνικής των εποπτών γενικού σκοπού καθώς και των εργαλείων που βασίζονται σ' αυτή είναι τα εξής:

Υπέρ	***Κατά***
Αρκετά γενική τεχνική	Είναι δύσχρηστο για τον μέσο χρήστη
Κανονικά λειτουργεί και για άγνωστους ιούς	Παρουσιάζει αρκετές ψευδείς αναφορές ύπαρξης ιών
Μικρή συχνότητα ενημερώσεων	Είναι ευάλωτο σε νέες τεχνικές ιών
	Μπορεί να απενεργοποιηθεί από τους ιούς

ΠΙΝΑΚΑΣ 7. ΘΕΤΙΚΑ ΚΑΙ ΑΡΝΗΤΙΚΑ ΣΗΜΕΙΑ ΤΗΣ ΤΕΧΝΙΚΗΣ ΤΩΝ ΕΠΟΠΤΩΝ ΓΕΝΙΚΟΥ ΣΚΟΠΟΥ.

4.7 ΕΥΡΕΣΤΙΚΗ ΑΝΑΛΥΣΗ ΚΩΔΙΚΑ

Η ευρεστική ανάλυση κώδικα [24,28] έχει ως στόχο να εντοπίζει την ύπαρξη malware σε αντικείμενα του συστήματος μέσω στατικής ανάλυσης του εισερχομένου τους. Σε αντίθεση με την τεχνική εντοπισμού υπογραφών, η ευρεστική ανάλυση κώδικα δεν προσπαθεί να εντοπίσει συγκεκριμένες ακολουθίες από bytes, αλλά κώδικα που μοιάζει με Malware.

Για παράδειγμα, ένα πρόγραμμα που έχει ως πρώτη εντολή του μία εντολή άλματος στο τέλος του αρχείου, όπου υπάρχει αυτοτροποποιούμενος κώδικας που καταλήγει με μία εντολή άλματος στην αρχή, είναι πιθανότατα μολυσμένο από Malware. Οι τεχνικές αυτές καταλήγουν σε εντοπισμό πιθανώς μολυσμένων αρχείων, και για περαιτέρω ενδυνάμωση των συμπερασμάτων πολλές φορές συνδυάζονται με τεχνικές εντοπισμού υπογραφών.

Τα εργαλεία που βασίζονται στην ευρεστική ανάλυση κώδικα είναι συνήθως εύκολα στη χρήση, καθώς δεν απαιτούν ιδιαίτερες ρυθμίσεις, πλην της αρχικής εγκατάστασης τους. Έχουν τη δυνατότητα να ανιχνεύουν άγνωστους ή πολυμορφικούς ιούς, οι οποίοι εμπίπτουν στους ευρεστικούς κανόνες. Από την άλλη πλευρά μπορεί να μην εντοπίσουν όλα τα Malware, αν δεν περιγράφονται από τον κατάλληλο κανόνα, ενδέχεται να αναφέρουν ανύπαρκτα Malware αν κάποιο «νομότυπο» πρόγραμμα ταιριάζει με κάποιον από τους κανόνες του εργαλείου. Τέλος, η λειτουργία τους απαιτεί πολύ επεξεργαστική ισχύ, καθώς η ανάλυση του κώδικα είναι πιο επαχθής υπολογιστικά από την αναζήτηση ακολουθιών bytes.

4.8 ΕΡΓΑΛΕΙΑ ΚΑΘΑΡΙΣΜΟΥ MALWARE

Τα εργαλεία αυτά έχουν ως στόχο να απομακρύνουν το κακόβουλο λογισμικό από το σύστημα μας, επιφέροντας στην αρχική τους μορφή τις αλλαγές που επέφερε η μόλυνση. Προκειμένου να δημιουργήσουν εργαλεία καθαρισμού οι κατασκευαστές λογισμικού αναλύουν την δράση του κακόβουλου λογισμικού και έχουν κατάλληλους αλγορίθμους αναίρεσης, ώστε το σύστημα μας να επανέρθει στη αρχική του κατάσταση πριν την μόλυνση. Αφού λοιπόν αναπτύξουν κατάλληλους αλγορίθμους αναίρεσης, τους ενσωματώνουν στα εργαλεία αντιμετώπισης κακόβουλου λογισμικού.

Η ενσωμάτωση των αλγορίθμων γίνετε είτε μεμονωμένα σε εργαλεία που καθαρίζουν ένα μόνο συγκεκριμένο Malware, είτε κατά ομάδες, οδηγώντας σε εργαλεία καθαρισμού πλειάδων Malware.

Για να λειτουργήσει όμως σωστά ένα εργαλείο καθαρισμού από κακόβουλο λογισμικό θα πρέπει οι αλλαγές που επέφερε το malware να είναι αντιστρέψιμες. Παράδειγμα μιας μη αντιστρέψιμης αλλαγής είναι όταν ένα malware καταστρέφει αντικείμενα, επικαλύπτεται το περιεχόμενό τους με άλλες ακολουθίες bytes χωρίς να αποθηκεύει κάπου το αρχικό περιεχόμενο άρα η αποκατάσταση της αρχικής μορφής του αντικείμενου δεν είναι εφικτή. Θα πρέπει επίσης να προσδιοριστεί σωστά το Malware που έχει μολύνει το σύστημα μας, έτσι ώστε να εφαρμοστεί ο σωστό αλγόριθμος αναιρέσεις.

ΚΕΦΑΛΑΙΟ 5

5.1 Η ΕΠΙΔΗΜΙΟΛΟΓΙΑ ΣΤΗ ΒΙΟΛΟΓΙΑ ΚΑΙ ΣΤΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

Ο όρος ‘επιδημικός’ (epidemic), έχει οριστεί σαν ‘ένα ξέσπασμα μιας μεταδοτικής ασθένειας η οποία εξαπλώνεται ταχύτατα και σε ένα μεγάλο εύρος όσον αφορά τη περιοχή μόλυνσης’ (American heritage Dictionary 2000).

Με ένα παρόμοιο λοιπόν τρόπο, η επιδημιολογία στην επιστήμη των υπολογιστών μπορεί να οριστεί σαν έναν ιό υπολογιστή ή ένα σκουλήκι που διαδίδεται γρήγορα και σε μεγάλο βαθμό μολύνοντας υπολογιστικά συστήματα σε μία περιοχή ή σε ένα πληθυσμό ταυτόχρονα (Symantec 2000).

Η επιδημιολογία στην επιστήμη των υπολογιστών, μελετήθηκε αρχικά από τους Kephart, Chess και White οι οποίοι περιέγραψαν το τρόπο με τον οποίο διαδίδονται τα computer worms/viruses.

Βρήκανε ότι υπάρχουν αρκετές ομοιότητες στο τρόπο που διαδίδεται μία επιδημία εάν το μελετά κάποιος από τη σκοπιά της βιολογίας ή τη σκοπιά της επιστήμης των υπολογιστών.

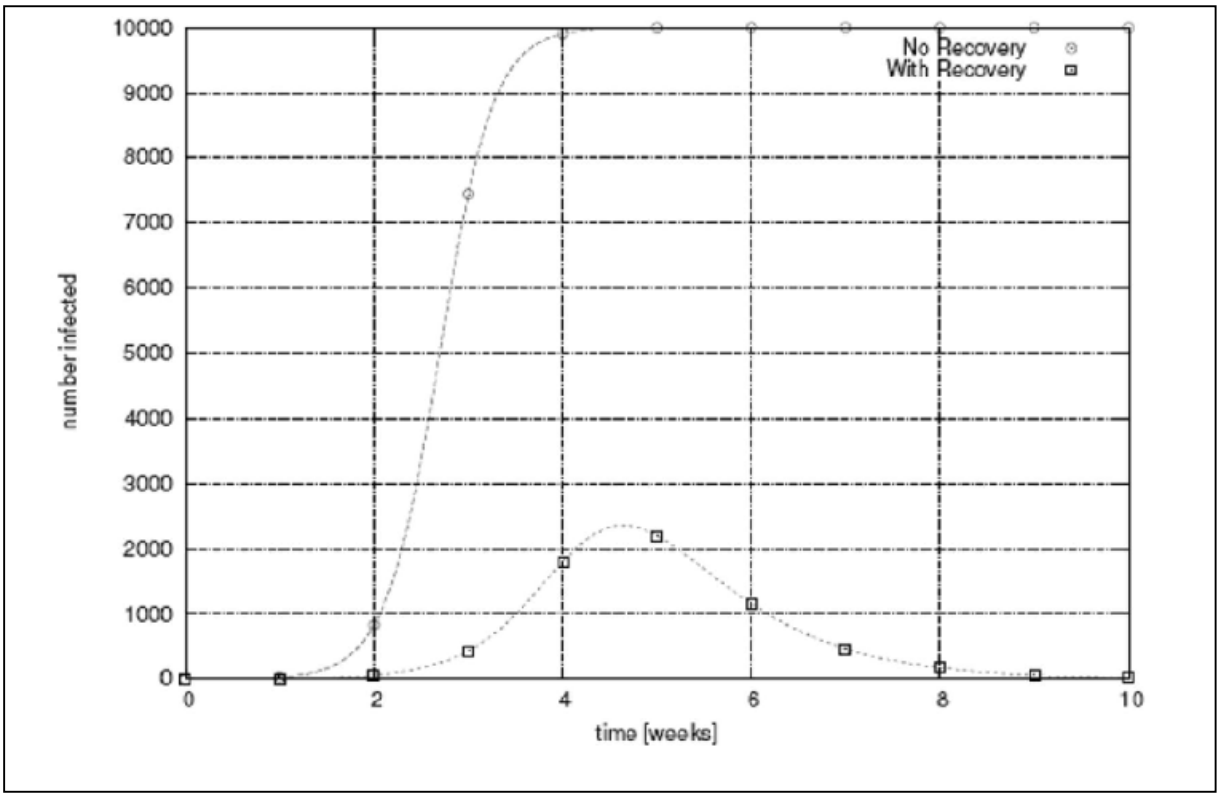
Η επιδημιολογία παρέχει μία μέθοδο για την κατανόηση αλλά και την ανταπόκριση σε μία ασθένεια καθώς αυτή διαδίδεται σε ένα πληθυσμό. Η επιδημιολογία χρησιμοποιεί μαθηματικά μοντέλα για να πολιτικοποιήσει, χαρακτηρίσει και να προβλέψει τη διάδοση και την επίδραση μιας ασθένειας.

Η δημογραφική ανάλυση που συνήθως εφαρμόζεται, χρησιμοποιείται για να καθορίσει τη σχέση αυτή μεταξύ της ασθένειας και του πληθυσμού. Ο ρόλος αυτών που ασχολούνται με την επιδημιολογία είναι να καταστρέψουν ή να βλάψουν αυτή τη σχέση ώστε να προλάβουν τη μόλυνση του πληθυσμού. Με άλλα λόγια ο βασικός στόχος της επιδημιολογίας είναι να εμποδίσει τη διάδοση της ασθένειας και να προλάβει τη πιθανή μελλοντική επανεμφάνιση της.

Η επιδημιολογία στους υπολογιστές λέγεται ψηφιακή επιδημιολογία και εφαρμόζει την βιολογική επιδημιολογία στον κυβερνοχώρο και γενικότερα σε αυτό που ονομάζουμε σήμερα επιστήμη των υπολογιστών.

Οι διαχειριστές δικτύων και συστημάτων, καθώς και οι ερευνητές, αντιλήφθηκαν ότι η ασφάλεια ενός συστήματος εξαρτάται από την ασφάλεια ολόκληρου του πληθυσμού όπου μπορεί να περιλαμβάνει το υποδίκτυο, το πανεπιστήμιο ή το δίκτυο της εταιρείας, ή ακόμη και ολόκληρο το διαδίκτυο. Τεχνικές

από την βιολογική επιδημιολογία προσφέρουν μεθόδους προκειμένου να κατανοήσουμε και να αντιμετωπίσουμε τα θέματα ασφάλειας που απειλούν την υγεία αυτού του πληθυσμού.



ΣΧΗΜΑ 2 ΑΝΑΚΑΜΨΗ ΤΗΣ ΑΣΘΕΝΕΙΑΣ

Αυτό που μπορούμε να παρατηρήσουμε, είναι ότι όταν δεν έχουμε κανένα αντίμετρο, τότε η μόλυνση θα προχωρά μέχρις ότου καλυφθεί ολόκληρος ο πληθυσμός, σε αντίθεση με τη περίπτωση όπου η εφαρμογή κάποιου μέτρου, για παράδειγμα η ανακάλυψη κάποιου εμβολίου, μπορεί και μειώνει δραστικά την εξάπλωση αυτής σε ολόκληρο το πληθυσμό.

Ο ρόλος αυτών που ασχολούνται με την επιδημιολογία είναι να ανακαλύψουν την ασθένεια, ειδικά αυτή που είναι ιδιαίτερα εκδηλωτική και μεταδοτική, όπως δηλαδή αυτή που χαρακτηρίζεται από τη πρώτη καμπύλη στη παραπάνω γραφική παράσταση κατά τα πρώτα στάδια της μόλυνσης και να δημιουργήσουν εκείνα τα αντίμετρα, όπως μία καραντίνα, που αυτή να μειώνει τη διάδοση της μόλυνσης όπως και φαίνεται στη δεύτερη καμπύλη της γραφικής παράστασης.

5.2 ΣΥΓΚΡΙΣΗ ΜΕΤΑΞΥ ΒΙΟΛΟΓΙΚΩΝ ΚΑΙ ΨΗΦΙΑΚΩΝ ΙΩΝ

Τα worms διαδίδονται μεταξύ των δικτύων υπολογιστών με το να εισβάλουν στα συστήματα και μετά να διαδίδονται σε άλλα συστήματα. Αυτή η διαδικασία, μπορεί να παραλληλιστεί με τη διάδοση μιας μολυσματικής ασθένειας στη βιολογία, όπου μια ξένη οντότητα διαδίδεται μέσω του πληθυσμού με το να μολύνει κάποιο άτομο, το οποίο με τη σειρά του μολύνει και άλλα.

Αρχικά οι ομάδες από συσκευές σχηματίζουν ένα δίκτυο ενώ στη βιολογία οι οντότητες σχηματίζουν ένα πληθυσμό.

Κατά δεύτερον η κανονική/φυσιολογική συμπεριφορά μιας οντότητας είναι γνωστή σαν υγεία ενώ σε ένα υπολογιστικό σύστημα αυτό χαρακτηρίζεται σαν κανονική λειτουργία. Ένα τέτοιο σύστημα βρίσκεται σε αντικανονική λειτουργία όταν προκληθεί μια εχθρική απόκλιση από τη κανονική λειτουργία, μια κατάσταση όπου είναι γνωστή σαν ασθένεια στους βιολογικούς οργανισμούς.

Μια βιολογική ασθένεια να σημειώσουμε ότι επιδρά εχθρικά στην υγεία των οντοτήτων όπως και το κακόβουλο λογισμικό και επηρεάζει τη κανονική συμπεριφορά των υπολογιστικών συστημάτων.

Η δε ψηφιακή ασθένεια, στη περίπτωση ενός network stealth worm, μεταδίδεται με βάση τις υπάρχουσες δικτυακές συνδέσεις ενώ σε μία βιολογική ασθένεια, η μόλυνση μπορεί να μεταφέρεται από τον αέρα, το έδαφος ή από άλλους οργανισμούς.

Μια βιολογική ασθένεια και μία οντότητα, μοιράζονται ένα περιβάλλον που χαρακτηρίζεται από τη θερμοκρασία, την υγρασία, τις κοινωνικές αλληλεπιδράσεις, και άλλα παραπλήσια στοιχεία.

Η ύπαρξη τρωτών σημείων, οι τα αντιδραστικά μέτρα άμυνας, το ανοιχτό μοντέλο επικοινωνίας όπως είναι το διαδίκτυο και η έλλειψη ποικιλίας συνθέτουν το περιβάλλον ενός κακόβουλου λογισμικού όμως ένας ζωντανός οργανισμός εμφανίζει κάποιο σύμπτωμα, παρόμοιο με την ανωμαλία σε μία ψηφιακή υπολογιστική συσκευή, όπου και δείχνει μία ασθένεια ή μια αντικανονική λειτουργία.

Μία βιολογική ασθένεια τυπικά προσβάλει ένα πληθυσμό σε ένα διάστημα ημερών και εβδομάδων ή ακόμη και δεκάδων ετών. Στη περίπτωση όμως ενός κακόβουλου λογισμικού, η μόλυνση διαδίδεται σε δευτερόλεπτα, ή και ώρες.

Ακόμα η περίοδος επώασης μιας βιολογικής ασθένειας είναι πολύ μεγαλύτερη από της ψηφιακής ενώ και το μέσο διάδοσης διαφέρει δραστικά.

Η αναγνώριση και ο καθορισμός των παραγόντων μιας ασθένειας προήλθε σαν αποτέλεσμα της αυτοψίας και της μελέτης των δεδομένων. Αυτό είναι ανάλογο με την ανίχνευση και το χαρακτηρισμό του κακόβουλου λογισμικού σε ένα υπολογιστικό σύστημα που έχει αντικανονική λειτουργία.

Η ανάλυση και πρόβλεψη συνέβαλε στη κατανόηση των επιδράσεων και αποτελεσμάτων του κακόβουλου λογισμικού σε ένα σύστημα, όπου είναι παρόμοια με τη πρόγνωση που γίνεται σε ένα βιολογικό οργανισμό που έχει μολυνθεί από μία ασθένεια.

Ο σκοπός της πρόγνωσης είναι τελικά να αναγνωρισθεί η θεραπεία για την ασθένεια προκειμένου ο οργανισμός να επιστρέψει στην υγιή κατάσταση που βρισκόταν. Στο ψηφιακό κόσμο έχουμε τη λεγόμενη αντίδραση προκειμένου να απαλείψουμε το κακόβουλο λογισμικό και το σύστημα να αναρρώσει.

Βιολογικό Παράδειγμα	**Ψηφιακό Παράδειγμα**	**Εξήγηση**
Πληθυσμός	Δίκτυο	Το πλήρες σύνολο των οντοτήτων που είναι υπό εξέταση.
Οργανισμός	Υπολογιστική Συσκευή	Η οντότητα μέσα στο σύνολο που είναι υπό εξέταση.
Ασθένεια	Κακόβουλο λογισμικό ή κακόβουλος χρήστης	Η επιρροή μιας ξένης υπόστασης που επηρεάζει τη κανονική κατάσταση ή συμπεριφορά.
Μέσο Μετάδοσης: αέρας, έδαφος, οργανισμοί, κ.α.	Μέσο Μετάδοσης: δικτυακές συνδέσεις.	Μέθοδος ή μηχανισμός διάδοσης της ασθένειας.
Περιβάλλον: θερμοκρασία, υγρασία, αλληλεπιδράσεις οργανισμών, κ.α.	Περιβάλλον: ύπαρξη τρωτών σημείων, μέτρα άμυνας, κ.α.	Το περιβάλλον όπου η ασθένεια και ο χρήστης συνυπάρχουν.
Ευρωστία	Κανονική λειτουργία	Η κατάσταση κανονικής λειτουργίας και συμπεριφοράς ενός οργανισμού.
Πάθηση/Ασθένεια	Αντικανονική λειτουργία	Εχθρική απόκλιση από τη κανονική λειτουργία ή συμπεριφορά σαν αποτέλεσμα της ασθένειας.
Σύμπτωμα	Ανωμαλία	Σημάδι ή ένδειξη μιας ασθένειας ειδικότερα όταν δείχνει μία εχθρική απόκλιση από τη κανονική λειτουργία ή συμπεριφορά.
Διάγνωση	Ανακάλυψη και χαρακτηρισμός.	Αναγνώριση και καθορισμός της φύσης και αιτίας της ασθένειας μέσα από την αξιολόγηση των χαρακτηριστικών αυτών που νοσούν και διαφόρων άλλων δεδομένων.
Πρόγνωση	Ανάλυση και πρόβλεψη	Πρόβλεψη της πιθανής πορείας μιας ασθένειας και αποτελεσμάτων.
Θεραπεία	Αντίδραση	Παροχή θεραπείας σε μία μολυσμένη οντότητα.

ΠΙΝΑΚΑΣ 8 ΣΥΓΡΙΣΗ ΒΙΟΛΟΓΙΚΩΝ ΚΑΙ ΨΗΦΙΑΚΩΝ ΙΩΝ

ΚΕΦΑΛΑΙΟ 6

6.1 ΑΝΑΓΚΗ ΓΙΑ ΜΟΝΤΕΛΟΠΟΙΗΣΗ

Η Μοντελοποίηση της εξάπλωσης του κακόβουλου λογισμικού παρέχει σημαντικά πλεονεκτήματα στην υλοποίηση των αμυντικών μηχανισμών.

Το κυριότερο όφελος που θα μπορούσαμε να σας πούμε για τη μοντελοποίηση είναι ότι αφήνει τη δημιουργία μιας γενικότερης εποπτικής εικόνας σχετικά με την εξάπλωση των μορφών του κακόβουλου λογισμικού.

Επίσης να προσθέσουμε πως σε πολλές περιπτώσεις είναι δυνατόν, εάν είναι γνωστά κάποια βασικά χαρακτηριστικά κάποιας μορφής κακόβουλου λογισμικού να μπορεί να εκτιμηθεί η επικινδυνότητα του ή γενικά ο αριθμός των ευπαθών στόχων που πρόκειται να πλήξει. Συνήθως βέβαια χρησιμοποιείται για την μετέπειτα μελέτη διάφορων επιδημιών κακόβουλου λογισμικού [18,19] και την ανασύνθεση των γεγονότων που οδήγησαν σε αυτή.

Ακόμα είναι αρκετά συνηθισμένη η χρήση της μοντελοποίησης για την πρόβλεψη της εξάπλωσης και των συνεπειών που είναι πιθανό να έχουν οι νέες μορφές του κακόβουλου λογισμικού [52,53].

6.2 ΕΠΙΔΗΜΙΟΛΟΓΙΚΑ ΜΟΝΤΕΛΑ

Προκειμένου να μοντελοποιηθεί η πρόοδος μιας επιδημίας σε ένα μεγάλο πληθυσμό/δίκτυο υπολογιστών που περιλαμβάνει πολλά διαφορετικά άτομα/υπολογιστές σε διάφορους τομείς, θα πρέπει μια τέτοιου είδους ποικιλομορφία πληθυσμών/δικτύων υπολογιστών να μειωθεί σε μερικά βασικά χαρακτηριστικά που θα είναι σχετικά με την υπό εξέταση μόλυνση.

Παραδείγματος Χάρι, στις περισσότερες ασθένειες παιδικής ηλικίας όπως είναι για παράδειγμα η ανεμοβλογιά που έχει μακρά διάρκεια ανοσίας έχει νόημα να διαιρεθεί ο πληθυσμός σε εκείνους που είναι επιρρεπής στην ασθένεια, σε εκείνους που είναι μολυσμένοι και εκείνους που έχουν περάσει την ασθένεια και έχουν πάθει πλέον ανοσία.

Αντίστοιχο παράδειγμα για τους υπολογιστές θα μπορούσαμε να σας αναφέρουμε ένα δίκτυο στο οποίο υπάρχουν υπολογιστές οι οποίοι δεν είναι προστατευμένοι από επιθέσεις του κακόβουλου λογισμικού άρα ανήκουνε στη

κατηγορία των ευπαθών υπολογιστών επίσης, οι υπολογιστές οι οποίοι έχουν ήδη δεχτεί την επίθεση από κάποιον ιό και “νοσούν” άρα ανήκουν στην κατηγορία των μολυσμένων υπολογιστών και τέλος εκείνοι που έχουνε προστασία π.χ. (antivirus, firewalls κτλ.) από το κακόβουλο λογισμικό άρα έχουν πάθει “ανοσία” όταν επιτεθούν από κάποιον ιό.

6.3 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Ο Kephart πραγματοποίησε τη πρώτη ολοκληρωμένη απόπειρα μοντελοποίησης της εξάπλωσης του κακόβουλου λογισμικού στην δεκαετία του 90. Ήταν ο πρώτος που χρησιμοποίησε τα επιδημιολογικά μοντέλα για τη μελέτη της διάδοσης των ιών. Η καινοτομία του αυτή οδήγησε στη δημιουργία του κλάδου της επιδημιολογίας των υπολογιστών.

Τον καιρό όμως που ο Kephart [13] ασχολήθηκε με τη μοντελοποίηση οι ιοί των υπολογιστών αποτελούσαν περισσότερο αντικείμενο επιστημονικής φαντασίας, παρά υπαρκτό πρόβλημα για τους περισσότερους χρήστες και αυτό δυσκόλεψε και αποθάρρυνε την επιστημονική κοινότητα από το να ασχοληθούν εντατικά με το αντικείμενο.

Έπειτα το 2000 ο Code Read και Nimba με τις μεθοδολογίες τους προκάλεσαν το ενδιαφέρον των ερευνητών για να ξαναασχοληθούν με τη μαθηματική μοντελοποίηση της εξάπλωσης του κακόβουλου λογισμικού.

Ακόμα οι εργασίες των Staniford, Weaver και Paxson έδωσαν το έναυσμα για να ξεκινήσει ένας νέος κύκλος έρευνας σε επιδημιολογικά μοντέλα όπου με την υλοποίηση κάποιων αλγορίθμων και συστημάτων περιορίστηκε η διάδοση του κακόβουλου λογισμικού του.

Έπειτα οι Zou και Gong [18] επινόησαν ένα επιδημιολογικό μοντέλο δύο παραγόντων που περιλαμβάνει πιο σύνθετα χαρακτηριστικά από ότι το βασικό επιδημιολογικό μοντέλο ευπαθούς-μολυσμένου πληθυσμού, το οποίο είναι ευρύτερα γνωστό έως S-I (Susceptible-Infected).Συγκεκριμένα, το μοντέλο περιλαμβάνει την αλλαγή της κατάστασης του συστήματος από ευπαθές ή μολυσμένο σε άνοσο κατά την πορεία εξέλιξης του φαινομένου.

Το μοντέλο αυτό αποτελεί μια παραλλαγή του γνωστού μοντέλου SIR (Susceptible- Infected- Removed) και αναμφίβολα, το γεγονός ότι υποστηρίζει τη δυναμική αλλαγή της κατάστασης κατά την διάρκεια εξέλιξης του φαινομένου είναι θετικό καθώς περιγράφει ικανοποιητικά την διαδικασία της αναβάθμισης του λογισμικού που συμβαίνει πάντα σε καταστάσεις αυξημένης κακόβουλης δραστηριότητας.

Οι Zou και Gong έχουν επίσης πραγματοποιήσει έρευνα για την μετάδοση του κακόβουλου λογισμικού μέσω του ηλεκτρονικού ταχυδρομείου και έχουν διατυπώσει τα σχετικά μαθηματικά μοντέλα για να περιγράψουν την παραπάνω διαδικασία.

Μια πιο ολοκληρωμένη και πλήρης μελέτη για την εξάπλωση του λογισμικού έχει γίνει από τον Laveille [54].Ο Laveille προτείνει τροποποιήσεις στο υπάρχον Γενικό Επιδημιολογικό μοντέλο το οποίο ονομάζεται P-S-I-D-R (Progressive-Susceptible-Infected–Removed) και περιλαμβάνει δύο διακριτές περιόδους.

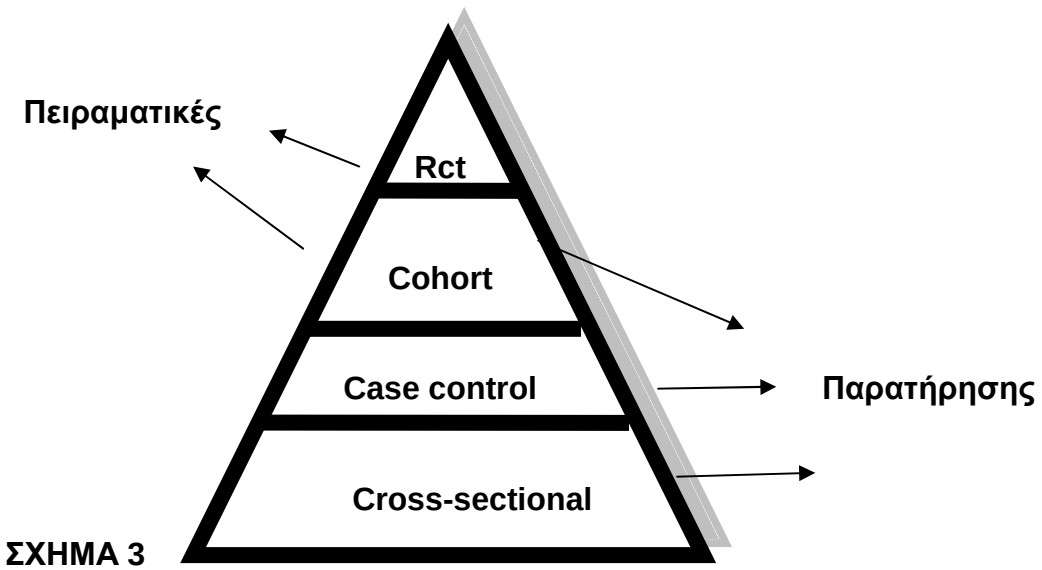
Η πρώτη αφορά τα αρχικά στάδια μιας επιδημίας κακόβουλου λογισμικού, όπου ο ιός ή το δικτυακό σκουλήκι εξαπλώνεται ανεμπόδιστα, είτε γιατί δεν έχει γίνει ακόμα αντιληπτός είτε γιατί δεν υπάρχουν τα κατάλληλα αντίμετρα.

Στην δεύτερη περίοδο, όπου πλέον είναι γνωστή η κακόβουλη δραστηριότητα, μπαίνουν τα περιοριστικά μέτρα σταματώντας την περαιτέρω εξάπλωση τους.

Μπορεί να θεωρηθεί σαν ένας συνδυασμός των επιδημιολογικών μοντέλων S-I και του S-I-R. Συγκεκριμένα κατά τον Laveille το διάστημα που ο ιός δρα λαθραία η εξάπλωση του υπολογίζεται με το επιδημιολογικό μοντέλο S-I. Στην συνέχεια όταν ο ιός γίνει αντιληπτός ακολουθεί το μοντέλο S-I-R.

Ο Boquna και ο Pastor Satorras [8] στην έρευνα τους κατάφεραν να αναδείξουν την σημασία που έχει η χρησιμοποίηση των γράφων ελεύθερης κλίμακας στη μελέτη επιδημικών εξάρσεων. Η δουλειά τους αποτελεί συνέχεια της προγενέστερης προσπάθειας του Pastor-Sattoras με τον Vespignani [55].

ΕΙΔΗ ΕΠΙΔΗΜΙΟΛΟΓΙΚΩΝ ΜΕΛΕΤΩΝ



ΣΧΗΜΑ 3

Στο σχήμα φαίνονται τα 4 βασικά είδη των επιδημιολογικών μελετών διαβαθμισμένες σε μια ιεραρχική πυραμίδα η οποία υποδεικνύει κατά κάποιον τρόπο την ερευνητική δυναμική τους δηλαδή την αποδεικτική δύναμη των αποτελεσμάτων τους.

Στη βάση της πυραμίδας του σχήματος υπάρχουν οι μελέτες συγχρονικού τύπου (Cross-sectional) και οι μελέτες ασθενών-μαρτύρων [56] (Case-control) που ανήκουν στις μελέτες παρατήρησης διότι σε αυτές οι ερευνητές δεν καθορίζουν τις συνθήκες της μελέτης (παράγοντες κινδύνου, χρονικές συνθήκες κτλ.) αλλά απλά παρατηρούν και προσμετρούν τα βίο-ιατρικά φαινόμενα που συμβαίνουν. Οι μελέτες cross sectional λέγονται και μελέτες επιπολασμού.

Ακολουθούν στην ιεραρχική πυραμίδα οι μελέτες κοορτών (cohorts) και επειδή ασχολούνται με τη μέτρηση της επίπτωσης λέγονται και μελέτες επίπτωσης.

Οι μελέτες κοορτών μπορεί να είναι μελέτες παρατήρησης ή και πειραματικές υπό την έννοια ότι οι ερευνητές μπορούν απλά να παρατηρήσουν αλλά και να καθορίσουν επακριβώς τις συνθήκες της μελέτης άρα και να κάνουν μια πειραματική μελέτη.

Στην κορυφή της πυραμίδας βρίσκονται οι τυποποιημένες κλινικές μελέτες ή δοκιμές (Randomized Clinical Trials –RCT) οι οποίες πραγματοποιούνται από τους γιατρούς για να δοκιμάσουν την αποτελεσματικότητα των θεραπευτικών

παρεμβάσεων. Οι συνθήκες στις κλινικές δοκιμές (ομάδες ασθενών, θεραπεία, είδος παρακολούθησης) καθορίζονται απολύτως από τους ερευνητές και για αυτό ανήκουν στις λεγόμενες πειραματικές μελέτες.

6.4 CROSS-SECTIONAL STUDIES (ΕΠΙΠΟΛΑΣΜΟΥ)

Στις μελέτες επιπολασμού (cross sectional) καταγράφεται κατά την διάρκεια μιας εξέτασης (τα άτομα εξετάζονται σε ένα χρονικό σημείο) το βιοϊατρικό φαινόμενο που μας ενδιαφέρει.

Η εξέταση σε μια μοναδική χρονικά φορά, δεν σημαίνει ότι όλοι οι ασθενείς εξετάζονται με μιας, αλλά καθένας μπορεί να εξεταστεί σε διαφορετικό χρόνο όμως μια φορά.

Η μέτρηση των βιοϊατρικών φαινόμενων υπό αυτή την έννοια αποδίδει μια στιγμιαία εικόνα ενός πληθυσμού η οποία μπορεί να αλλάξει όμως στην πορεία του χρόνου. Έτσι οι μελέτες cross sectional έχουν περιορισμένη χρησιμότητα στην απόδοση αιτιολογικών συσχετίσεων μεταξύ αιτιών και νόσου.

Η γνώση όμως των μέτρων επιπολασμού είναι θεμελιώδης στην κλινική ιατρική καθώς δίνει στον κλινικό γιατρό τις γνώσεις για να ξεκινήσει μετά τη λήψη του ιατρικού ιστορικού και την κλινική εξέταση την λογική διεργασία που λέγεται διαφορική διαγνωστική.

Η διαφορική διαγνωστική ξεκινά με ένα κατάλογο δυνητικών διαγνώσεων οι οποίες έχουν μια πιθανότητα να επαληθευθούν με τις κατάλληλες διαγνωστικές εξετάσεις. Οι πιθανότητες αυτές των υπό εξέταση διαγνώσεων αριθμητικώς παριστάνονται από τον επιπολασμό. Έτσι οι διαγνώσεις με την υψηλότερη πιθανότητα, άρα με τον υψηλότερο επιπολασμό, είναι εκείνες που μπορούν να επαληθευθούν στον συγκεκριμένο άρρωστο και εξετάζονται πρώτες.

Ο επιπολασμός στην περίπτωση αυτή καλείται pre test probability (πριν να σταλούν διαγνωστικές εξετάσεις πιθανότητα). Ο επιπολασμός συμβάλλει σημαντικά στην διερεύνηση των διαγνωστικών δυνατοτήτων των διαφόρων εξετάσεων, δοκιμασιών και tests που προγραμματίζουμε για έναν ασθενή.

Ο επιπολασμός καθορίζει την τιμή της θετικής και της αρνητικής διαγνωστικής αξίας (positive and negative predictive value) και επομένως όχι μόνο συμβάλλει στην επιλογή και στην σειρά με την οποία θα παραγγελθούν οι διαγνωστικές εξετάσεις, υπό την έννοια της pre-test probability αλλά και στο κατά πόσο μια θετική ή αρνητική

απάντηση μιας διαγνωστικής εξέτασης, θα σημάνει και το τέλος της διαδικασίας διαφορικής διαγνωστικής, υπό την έννοια της θετικής ή αρνητικής διαγνωστικής αξίας.

Σε αντίθεση με τον επιπολασμό που λέγεται pre-test probability, η θετική διαγνωστική αξία λέγεται post-test probability, γιατί καθορίζει την πιθανότητα μια θετική διαγνωστική εξέταση να είναι όντως αληθινή (δηλαδή ο ασθενής να πάσχει πράγματι από την συγκεκριμένη νόσο).

Παρά την δεδομένη αδυναμία των μελετών επιπολασμού να τεκμηριώσουν σχέσεις αιτίας αποτελέσματος, η παρατήρηση αυξημένου επιπολασμού ενός νοσήματος σε μια ομάδα του πληθυσμού μπορεί να πυροδοτήσει αιτιολογικές σκέψεις και συσχετίσεις οι οποίες να επαληθευθούν με μετέπειτα αρτιότερες μελέτες και συσχετίσεις.

Μια αύξηση ή ελάττωση του επιπολασμού ενός νοσήματος οδηγεί στην εφαρμογή προληπτικών μέτρων ή στην μείωση προϋπαρχόντων.

Οι μελέτες cross-sectional [55]:

1. Μελετούν πληθυσμούς σε μία καθορισμένη χρονική στιγμή. Όπως μια πολιτική δημοσκόπηση.
2. Δίνουν στοιχεία για τον αριθμό των ανθρώπων που έχουν μια συγκεκριμένη ασθένεια σε μια συγκεκριμένη χρονική στιγμή (επιπολασμός).
3. Χρήσιμες για τον καθορισμό της επιβάρυνσης μιας πληθυσμιακής ομάδας από μία ασθένεια.
4. Μπορούν να διερευνήσουν συσχετίσεις με την ασθένεια αλλά δεν έχουν επαρκή σχεδιασμό για την τεκμηρίωση της αιτιολογίας της ασθένειας.

6.5 ΜΕΛΕΤΕΣ ΚΟΟΡΤΩΝ-COHORTS STUDIES

Στην επιδημιολογία ο όρος κοορτή ορίζεται ως την διαδικασία όπου κάθε ομάδα ατόμων σχεδιάζεται να παρακολουθηθεί για μια χρονική περίοδο. Έχει λάβει το όνομα της αλλά και την συνολική φιλοσοφία cohort - κοορτή από την ονομασία του στρατιωτικού σχηματισμού της αρχαίας Ρωμαϊκής Λεγεώνας, κάτι σαν τον δικό μας λόχο. Τα μέλη της κοορτής της Λεγεώνας ήταν άνδρες, ίδιας ηλικίας που παρέμεναν

μαζί στον στρατό έως τα *65* χρόνια τους. Ήταν συνεπώς άτομα περίπου με ίδια χαρακτηριστικά που εκτίθονταν στις ίδιες δυσκολίες και κινδύνους.

Στις επιδημιολογικές μελέτες, τυπικά η κοορτή αποτελείται από άτομα με όμοια χαρακτηριστικά τα οποία επιπλέον έχουν κάτι κοινό το οποίο θέλουμε να εκτιμήσουμε πόσο επιδρά στην εμφάνιση (συχνότητα) ενός νοσήματος. Μετρούμε δηλαδή την επίπτωση ενός νοσήματος ή ενός βιοϊατρικού χαρακτηριστικού και για αυτό λέγονται και μελέτες επίπτωσης.

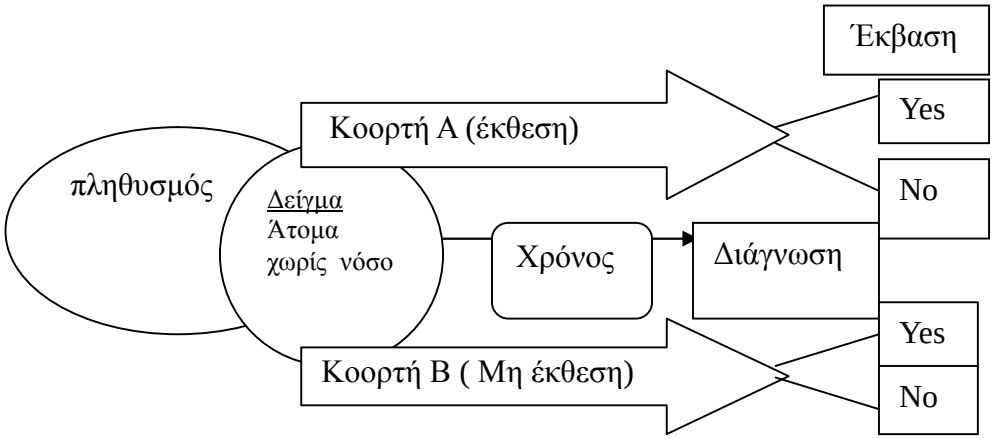
Επιλέγονται 2 κοορτείς με άτομα υγιή και πανομοιότυπα σε όλα τα υπόλοιπα χαρακτηριστικά πλην του γεγονότος, του παράγοντα κινδύνου στον οποίο εκτίθεται μόνο η πρώτη κοορτή. Έτσι μετρώντας την επίπτωση του νοσήματος που μας ενδιαφέρει στις δύο ομάδες μετά την πάροδο του κατάλληλου χρονικού διαστήματος και συγκρίνοντας αυτές, μπορούμε με ασφάλεια να συμπεράνουμε κατά πόσο ο παράγοντας κινδύνου επιδρά στην συχνότητα ενός νοσήματος.

Η έννοια και ο σχεδιασμός των μελετών κοορτών έτσι όπως εκτέθηκε παραπάνω φαίνεται να είναι απλή και ευνόητη αλλά δεν είναι τόσο απλά τα πράγματα καθώς υπάρχουν προβλήματα τα οποία πρέπει να αναλυθούν.

Τα πιο σημαντικά από αυτά είναι: Πως προσμετρούνται οι περιπτώσεις νόσησης ; Ποιος είναι ο πληθυσμός σε κίνδυνο ; Πως καθορίζεται η έκθεση στον παράγοντα κινδύνου ;

Για να αντιληφθούμε αυτές τις δυσκολίες ας δούμε το ακόλουθο παράδειγμα. Ο John Snow προσπάθησε να αναλύσει την επιδημία της χολέρας το 1854 στο Λονδίνο. Στο Λονδίνο εκείνη την εποχή υπήρχαν διάφορες εταιρείες ύδρευσης.

Ο Snow χώρισε τον πληθυσμό σε κίνδυνο, δηλαδή τους κάτοικους του Λονδίνου, σε 2 ομάδες. Σε αυτούς που υδρεύονταν από νερό του Τάμεση που ήταν μολυσμένο με λύματα με εμπλεκόμενες εταιρείες την Sauthwark και την \/auhall (cohort A) και τη δεύτερη ομάδα όπου υδρεύονταν με νερό της εταιρείας Lambeth που αντλούσε νερό από καθαρό μέρος του Τάμεση χωρίς μόλυνση με λύματα (cohort B). Ο Snow εν συνεχεία μέτρησε τους θανάτους από χολέρα μεταξύ των δύο πληθυσμιακών ομάδων.



ΣΧΗΜΑ 4. ΜΕΛΕΤΗ ΚΟΟΡΤΩΝ

Στο σχήμα 4 φαίνονται τα αποτελέσματα του εξαιρετικά έξυπνου επιδημιολογικού σχεδιασμού του Snow.

Πραγματοποίησε μια εξαιρετική μελέτη κοορτών με αποτέλεσμα τα συμπεράσματα του να δώσουν αφορμή να παρθούν μέτρα και να ανακοπεί η επιδημία χολέρας του Λονδίνου το 1854. Δικαίως λοιπόν ο John Snow θεωρείται ο πατέρας της Επιδημιολογίας.

Ο Snow επιθυμούσε να αναλύσει την σχέση της επιδημίας χολέρας με τις υδρευτικές ανάγκες του πληθυσμού του Λονδίνου. Άρα χρειαζόταν άτομα που να μην είναι άρρωστα με χολέρα, να μην έχουν πεθάνει αλλά να βρίσκονται υπό κίνδυνο να νοσήσουν σε εύλογο χρονικό διάστημα.

Αυτός ο κατάλληλος για μελέτη πληθυσμός λέγεται πληθυσμός σε κίνδυνο (population at risk). Το να είναι τα άτομα υγιή από την υπό μελέτη νόσο και εν ζωή μοιάζουν να είναι οι δύο πιο βασικές προϋποθέσεις αυτού που ορίσαμε population at risk.

Διάφορα λοιπόν κριτήρια πρέπει να θεσπίζονται ώστε να επιλέγονται ποια άτομα μπορούν να είναι υποψήφια στο να συμπεριληφθούν στις μελέτες κοορτών και στο πια είναι τα άτομα που ονομάζονται πληθυσμός σε κίνδυνο (population at risk). Τέτοια κριτήρια μπορεί να είναι δημογραφικά, γεωγραφικά κλπ.

Αν και ο πληθυσμός υπό παρακολούθηση στις μελέτες κοορτών (Cohorts) ορίζεται σαν πληθυσμός ελεύθερης νόσου (disease free) αυτό δεν σημαίνει ότι τα άτομα είναι απολύτως υγιή! Ο όρος ελεύθερος νόσου απλώς είναι δηλωτικός του ότι τα άτομα δεν πάσχουν από την νόσο ή την έκβαση της νόσου που μας ενδιαφέρει να εκτιμήσουμε. Αυτό άλλωστε είναι ιδιαίτερα εμφανές στις μελέτες κοορτών προγνωστικών παραγόντων (μελέτες επιβίωσης) όπου τα άτομα με συγκεκριμένη νόσο παρακολουθούνται για να εκτιμηθεί η επίδραση διάφορων προγνωστικών παραγόντων.

6.6 ΣΥΝΩΝΥΜΑ ΚΑΙ ΠΡΟΣΔΙΟΡΙΣΜΟΙ ΤΩΝ ΜΕΛΕΤΩΝ ΚΟΟΡΤΩΝ.

Τέσσερις είναι οι διαφορετικοί προσδιορισμοί που χρησιμοποιούνται στις μελέτες κοορτών [57]:

1) Κοορτής
2) Επίπτωσης
3) Προοπτικές
4) Μακροχρόνιες

Οι 4 αυτοί προσδιορισμοί, αυτού του τύπου των μελετών δίνουν έμφαση σε διαφορετικές πλευρές του σχεδιασμού τους. Ο όρος κοορτή αναφέρεται περισσότερο στις ιδιότητες της ομάδος των ατόμων που θα μελετηθούν και τα χαρακτηριστικά τους τα οποία έχουν αναλυθεί παραπάνω.

Οι μελέτες επίπτωσης μπορεί να λέγονται έτσι διότι προσδιορίζουν και εκτιμούν την επίπτωση. Επίσης ο όρος προοπτικές αναφέρεται έτσι από το γεγονός ότι οι υπό μελέτη ομάδες παρακολουθούνται στην πορεία ενός μελλοντικού χρονικού διαστήματος, ενώ ο όρος μακροχρόνιες προσδιορίζει την μελλοντική μακροχρόνια παρακολούθηση που υφίστανται τα άτομα των μελετών των κοορτών.

6.7 ΜΕΛΕΤΕΣ ΑΣΘΕΝΩΝ-ΜΑΡΤΥΡΩΝ (CASE-CONTROL STUDIES)

Οι μελέτες κοορτών παρουσιάζουν βασικά πλεονεκτήματα όπως [56]:

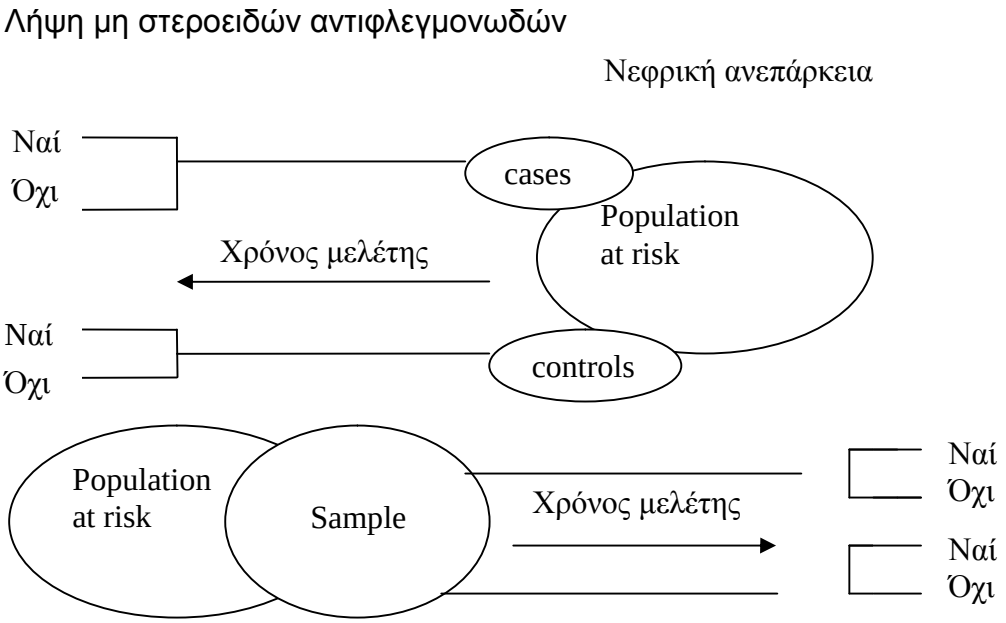
1) Είναι ο μόνος τρόπος για να μετρηθεί απευθείας η επίπτωση.
2) Το μοντέλο της ακολουθεί την κλινική λογική (έκθεση στον κίνδυνο-εκδήλωση της νόσου.)
3) Είναι δυνατή η διερεύνηση της σχέσης του παράγοντα κινδύνου με περισσότερα από ένα νοσήματα.

Έχουν όμως και βασικά μειονεκτήματα. Αυτά είναι:

1. Αναποτελεσματική σε σπάνια νοσήματα (πρέπει να παρακολουθηθούν χιλιάδες άτομα).
2. Οικονομικά πολύ δαπανηρή.
3. Τα αποτελέσματα της δεν είναι γνωστά για πολύ μεγάλο χρονικό διάστημα.
4. Δύσκολη η καταγραφή πολλών παραγόντων μαζί.
5. Πολλές φορές λόγοι ηθικής δεν επιτρέπουν την διεξαγωγή τους (πχ. δεν είναι ηθικό να εκθέσεις ανθρώπους σε κάποιο βλαπτικό παράγοντα προκειμένου να επιβεβαιωθεί μια επίδραση).

Οι μελέτες ασθενών-μαρτύρων αποσκοπούν να εξυπηρετήσουν τους ίδιους σκοπούς με τις μελέτες κοορτών, αλλά πιο γρήγορα και αποτελεσματικά και με πολύ χαμηλότερο κόστος.

Στο ακόλουθο σχήμα συνοψίζεται ο σχεδιασμός των μελετών ασθενών-μαρτύρων με τον σχεδιασμό μελέτης κοορτών. Και στις δύο μελέτες επιχειρείται να διερευνηθεί τυχόν αιτιολογική σχέση μεταξύ παράγοντα κινδύνου (π.χ. τη λήψη μη στεροειδών αντιφλεγμονωδών φαρμάκων και νεφρικής ανεπάρκειας).



ΣΧΗΜΑ 5. ΜΕΛΕΤΗ ΚΟΟΡΤΩΝ ΕΠΑΝΩ ΚΑΙ ΜΕΛΕΤΗ ΑΣΘΕΝΩΝ-ΜΑΡΤΥΡΩΝ ΚΑΤΩ ΓΙΑ ΤΗΝ ΔΙΕΡΕΥΝΗΣΗ ΤΗΣ.

Στο σχήμα 5 βλέπουμε ότι από ένα πληθυσμό σε κίνδυνο αντλούνται 2 κοορτείς. Η μια εκτίθεται στον παράγοντα κινδύνου και η άλλη όχι. Μετά την πάροδο αρκετών ετών επιχειρείται να μετρηθεί η επίπτωση της νεφρικής ανεπάρκειας στις δύο ομάδες. Όμως η νεφρική ανεπάρκεια είναι σπάνια νόσος, έτσι θα πρέπει να παρακολουθηθούν χιλιάδες άτομα σε κάθε κοορτή για να γίνει εφικτό να εκδηλωθούν μερικά περιστατικά νεφρικής ανεπάρκειας.

Αντί αυτού όμως μπορεί να εφαρμοστεί σχεδιασμός μελέτης ασθενών-μαρτύρων. Επομένως ασθενείς με νεφρική ανεπάρκεια (ομάδα ασθενών) συγκρίνετε με μια ομάδα από υγιείς (μάρτυρες) με όλα τα υπόλοιπα παρόμοια.

Στην κάθε ομάδα μετράτε η συχνότητα (έκθεση στον παράγοντα κινδύνου) και συγκρίνετε. Όπως βλέπουμε από το σχήμα η μελέτη κοορτών εξελίσσεται προοπτικά (prospective) ενώ η μελέτη ασθενών-μαρτύρων αντλεί πληροφορίες από το παρελθόν δηλαδή αναδρομικά (retrospective). Οι μελέτες ασθενών-μαρτύρων σε αντίθεση με τις μελέτες κοορτών (προδρομικές) καλούνται και αναδρομικές μελέτες.

Οι μελέτες ασθενών-μαρτύρων έχουν βασικά πλεονεκτήματα όπως:

1) Είναι χρήσιμες για να μελετηθούν προγνωστικοί ή κλινικοί παράγοντες νοσημάτων.
2) Η ανεύρεση των νοσούντων (cases) είναι σχετικά εύκολη ειδικά σε σπάνια νοσήματα κάτι που είναι αδύνατο να γίνει σε cohort design.
3) Δεν χρειάζεται να περιμένουμε πολύ χρόνο για να απαντήσουμε σε τυχόν ερευνητικά κλινικά ερωτήματα όπως συμβαίνει π. χ στη μελέτη των κοορτών.
4) Πολύ συχνή είναι η χρήση τους λόγω της ευκολίας, της ταχύτητας και της μικρής οικονομικής δαπάνης με την οποία μπορεί να μελετηθούν διάφορα κλινικά ερωτήματα.

Απαιτούν όμως και βασικές προυποθέσεις για να γίνει εφικτή η διενέργεια τους όπως:

1) Ύπαρξη ικανού αριθμού ασθενών έτσι ώστε τα όποια συμπεράσματα να μην οφείλονται σε τυχαία πιθανότητα.
2) Ύπαρξη ομάδας ελέγχου (μάρτυρες) που δεν έχουν τη νόσο.
3) Οι δύο ομάδες πρέπει να μοιάζουν σε όλα πλην της νόσου και του παράγοντα κινδύνου ή πρόγνωσης που μελετάται.

6.8 ΠΕΡΙΓΡΑΦΗ ΠΕΡΙΠΤΩΣΗΣ (CASE REPORT) - ΠΕΡΙΓΡΑΦΗ ΣΕΙΡΑΣ ΠΕΡΙΣΤΑΤΙΚΩΝ (CASE SERIES)

Η περιγραφή ενός κλινικού περιστατικού είναι η λεπτομερής παρουσίαση μιας περίπτωσης νοσήματος ή μιας μικρής ομάδας ομοειδών περιπτώσεων που παρουσιάζονται λόγω κάποιου κλινικού χαρακτηριστικού (σπανιότητας, θεραπευτικής ανταπόκρισης). Περίπου το 20-30% των άρθρων που γίνονται παγκοσμίως αφορά τα case reports [58].

Η περιγραφή περίπτωσης είναι χρήσιμη γιατί είναι:

1) Πηγή ερευνητικών υποθέσεων για κάποιο σχετικά σπάνιο περιστατικό.
2) Ενδιαφέρουσα και σχετικώς σπάνια στη κλινική παρουσίαση του νοσήματος.
3) Έχει σχέσεις με πρωτοεμφανιζόμενους παράγοντες κινδύνου.
4) Έχει ιδιόμορφη εξέλιξη και πρόγνωση.

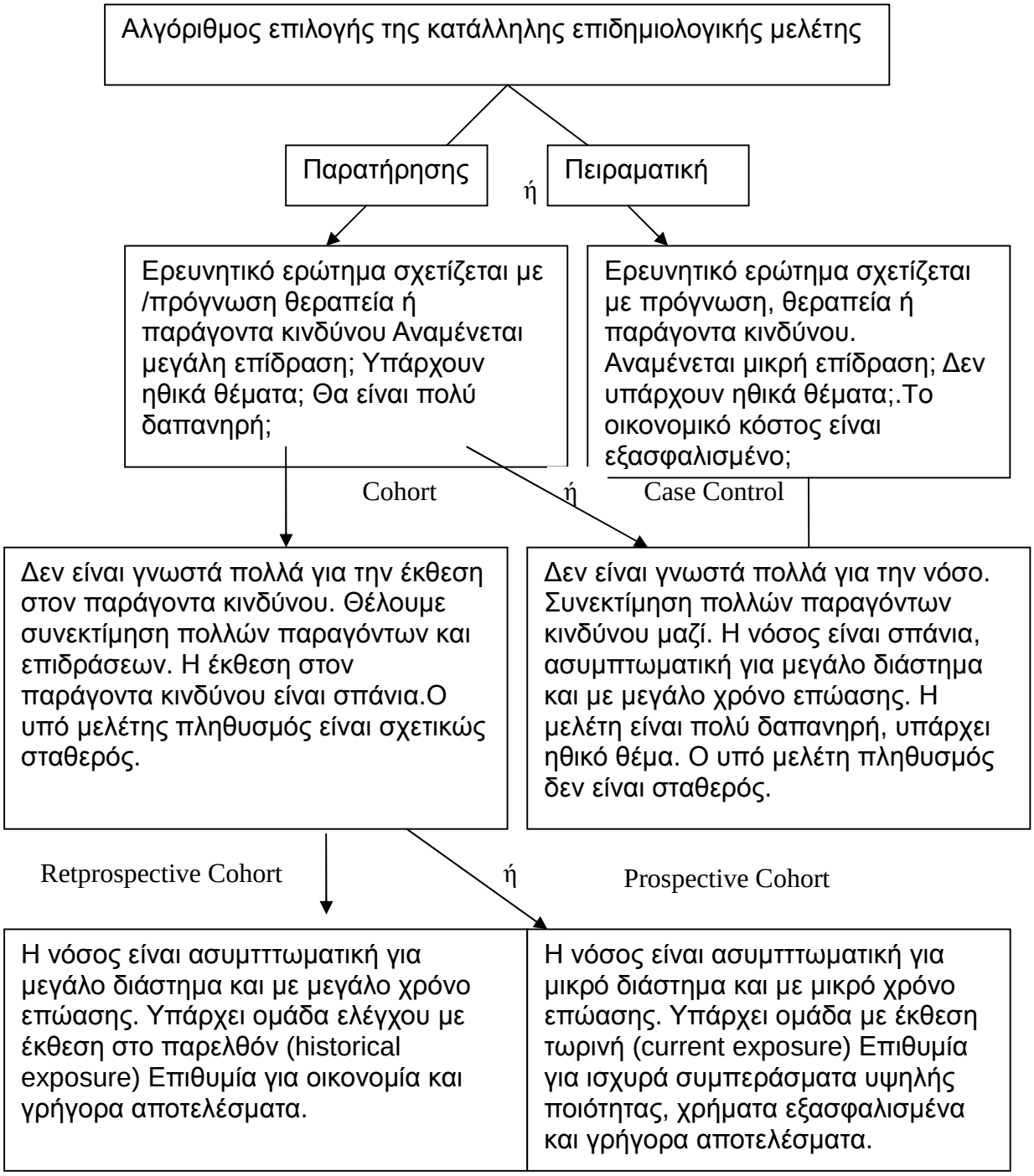
Τα case reports όμως:

1) Δεν χρησιμεύουν στην επαλήθευση διάφορων αιτιολογικών υποθέσεων.
2) Δίνουν την αφορμή για πιο εκτενείς μελέτες ελέγχου των υποθέσεων που τίθενται όπως παθοφυσιολογικοί μηχανισμοί πρόκλησης βλάβης.

Οι επιδημιολογικές μελέτες έχουν διαφορετικούς στόχους ανάλογα με τους διάφορους παράγοντες που εμπλέκονται. Οι μελέτες κλειδιά είναι οι: Σύγχρονες μελέτες ασθενών-μαρτύρων, οι Προοπτικές Τυχαιοποιημένες μελέτες κλινικής παρέμβασης (Πειραματικές).

Κάποιοι σχεδιασμοί μελετών είναι 'καλύτεροι' από κάποιους άλλους για τις ανάγκες του ερευνητικού αντικειμένου και τις συνθήκες που εξασφαλίζονται π.χ. (οικονομικές).

Στο παρακάτω σχήμα συνοψίζεται ένας βοηθητικός αλγόριθμος ενδεικτικός των κριτηρίων που εισέρχονται στην επιλογή του είδους της μελέτης που θα εξασφαλίσει τα καλύτερα αποτελέσματα υπό τις συγκεκριμένες ερευνητικές συνθήκες.



ΣΧΗΜΑ 6 ΑΛΓΟΡΙΘΜΟΣ ΕΠΙΛΟΓΗΣ ΤΗΣ ΚΑΤΑΛΛΗΛΗΣ ΕΠΙΔΗΜΙΟΛΟΓΙΚΗΣ ΜΕΛΕΤΗΣ.

6.9 ΕΠΙΔΗΜΙΟΛΟΓΙΚΑ ΜΟΝΤΕΛΑ

Προκειμένου να μοντελοποιηθεί η πρόοδος μιας επιδημίας σε ένα μεγάλο πληθυσμό που περιλαμβάνει πολλά διαφορετικά άτομα σε διάφορους τομείς, πρέπει μια τέτοια ποικιλομορφία πληθυσμών να μειωθεί σε μερικά βασικά χαρακτηριστικά που είναι σχετικά με την υπό εξέταση μόλυνση. Παραδείγματος χάριν, στις περισσότερες κοινές ασθένειες παιδικής ηλικίας που παρέχουν μακράς διαρκείας ανοσία έχει νόημα για να διαιρεθεί ο πληθυσμός σε εκείνους που είναι επιρρεπείς στην ασθένεια, σε εκείνους που είναι μολυσμένοι και εκείνους που έχουν ανακτήσει και είναι άνοσοι. Αυτές οι υποδιαιρέσεις του πληθυσμού καλούνται διαμερίσματα.

6.9.1 ΤΟ SIR ΜΟΝΤΕΛΟ

Με βάση το μοντέλο αυτό ορίζονται τρία διαμερίσματα, S (για επιρρεπείς), I (για μολυσμένους) και R (για αυτούς που έχουν αναρρώσει) [59]. Τα αρχικά αυτά αντιπροσωπεύουν επίσης τον αριθμό των ανθρώπων σε κάθε διαμέρισμα σε μία συγκεκριμένη χρονική στιγμή. Για να δειχθεί ότι το πλήθος μπορεί να ποικίλει κατά την διάρκεια του χρόνου (ακόμα κι αν ο συνολικός πληθυσμός παραμένει σταθερός), μετατρέπουμε τους ακριβείς αριθμούς σε συναρτήσεις του t (χρόνου): s(t), i(t) και r(t).

Για μια συγκεκριμένη ασθένεια σε έναν συγκεκριμένο πληθυσμό, αυτές οι συναρτήσεις μπορούν να επιλυθούν προκειμένου να προβλεφθούν τα πιθανά ξεσπάσματα και να τεθούν υπό έλεγχο.

6.9.2 ΤΟ SIR ΠΡΟΤΥΠΟ ΕΙΝΑΙ ΔΥΝΑΜΙΚΟ ΥΠΟ ΤΡΕΙΣ ΕΝΝΟΙΕΣ

Όπως υποδεικνύεται από τη μεταβλητή συνάρτηση του t, το μοντέλο είναι δυναμικό δεδομένου ότι οι αριθμοί σε κάθε διαμέρισμα μπορούν να κυμαίνονται κατά τη διάρκεια του χρόνου.

Η σημασία αυτής της δυναμικής πτυχής είναι προφανέστερη σε μια ενδημική ασθένεια με μια μικρή μολυσματική χρονική περίοδο (όπως ήταν η ιλαρά στο Ηνωμένο Βασίλειο πριν από την εισαγωγή ενός εμβολίου το 1968).

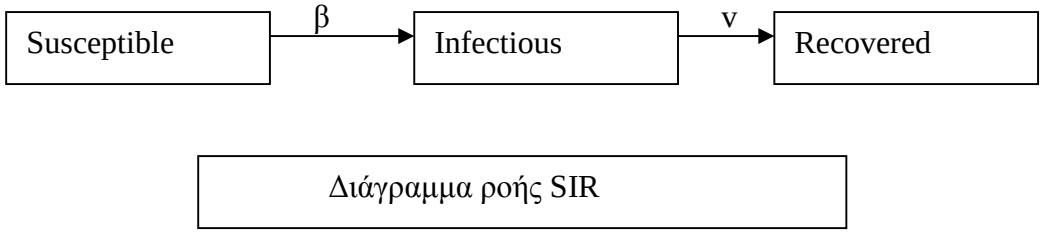
Τέτοιες ασθένειες τείνουν να εμφανίζουν κυκλικά ξεσπάσματα λόγω της μεταβολής του αριθμού των ευπαθών ατόμων (S(t)) κατά τη διάρκεια του χρόνου.

Κατά τη διάρκεια μιας επιδημίας, ο αριθμός των ευπαθών ατόμων μειώνεται γρήγορα δεδομένου ότι περισσότεροι τους μολύνονται και εισάγονται έτσι στα μολυσματικά διαμερίσματα και κατόπιν στα αναρρωμένα διαμερίσματα.

Μια σημαντική παρατήρηση αποτελεί το γεγονός ότι η ασθένεια δεν μπορεί να ξεσπάσει πάλι μέχρι ο αριθμός των ευπαθών ατόμων να επανέλθει (ως αποτέλεσμα των μωρών που γεννιούνται στο διαμέρισμα των ευπαθών).

Το SIR είναι επίσης δυναμικό υπό την έννοια ότι τα άτομα γεννιούνται ευπαθή, και κατόπιν μπορούν να μολυνθούν (μετακίνηση στο μολυσματικό διαμέρισμα) και τελικά να αναρρώσουν (μετακίνηση στο διαμέρισμα αναρρωμένων).

Κατά συνέπεια κάθε μέλος του πληθυσμού κινείται από ευπαθής σε μολυσμένος και μετά αναρρωμένος. Αυτό μπορεί να παρουσιαστεί ως διάγραμμα ροής στο οποίο τα πλαίσια αντιπροσωπεύουν τα διαφορετικά διαμερίσματα και τα βέλη την μετάβαση μεταξύ των διαμερισμάτων [60].



Σχήμα 7 Διάγραμμα ροής SIR

6.9.3 ΡΥΘΜΟΙ ΜΕΤΑΒΑΣΗΣ

Για την πλήρη προδιαγραφή του προτύπου, τα βέλη πρέπει να ονομαστούν με τους ρυθμούς μετάβασης μεταξύ των διαμερισμάτων. Μεταξύ του S και του I, το ποσοστό μετάβασης είναι το β, όπου β είναι ο ρυθμός επαφών, ο οποίος χοντρικά συνυπολογίζει την πιθανότητα να μεταφερθεί η ασθένεια με μια επαφή μεταξύ ενός ευπαθή και ενός μολυσματικού ατόμου.

Μεταξύ του I και του R, ο ρυθμός μετάβασης είναι ο v (ο ρυθμός ανάρρωσης). Εάν η διάρκεια της μόλυνσης είναι *D,* τότε v = 1/D, δεδομένου ότι ένα άτομο αναρρώνει μία και μοναδική φορά σε D χρονικές στιγμές.

Είναι σημαντικό να τονιστεί εδώ ότι υποθέτουμε ότι η μονιμότητα κάθε ατόμου στις επιδημικές καταστάσεις είναι μια τυχαία μεταβλητή με εκθετική κατανομή.

Ποιο σύνθετες και ρεαλιστικές κατανομές (όπως κατανομές Erlang) μπορούν να χρησιμοποιηθούν εξίσου με μερικές τροποποιήσεις.

6.9.4 ΒΙΟ-ΜΑΘΗΜΑΤΙΚΗ ΣΥΜΠΕΡΙΦΟΡΑ ΤΟΥ SIR ΠΡΟΤΥΠΟΥ

1) Το SIR πρότυπο χωρίς ζωτική δυναμική (διαδικασίες γέννησης-θανάτου)

Ένα επιδημικό ξέσπασμα είναι συνήθως πολύ γρηγορότερο από τη ζωτική δυναμική ενός πληθυσμού, επομένως, εάν ο στόχος είναι να μελετηθούν οι άμεσες συνέπειες μιας επιδημίας, μπορεί κανείς να παραμελήσει τις διαδικασίες γέννησης-θανάτου. Σε αυτήν την περίπτωση το SIR [59] σύστημα που περιγράφεται μπορεί να εκφραστεί από το ακόλουθο σύνολο διαφορικών εξισώσεων [61,62,63]

(dS/dt)= - βIS (1)

(dI/dt)= βIS – vI (2)

(dR/dt)= vI (3)

Αυτό το πρότυπο προτάθηκε για πρώτη φορά από τους Kermack και Anderson Gray McKendrick [63], οι οποίοι συνεργάστηκαν με τον βραβευμένο με Νόμπελ και πατέρα της μαθηματικής επιδημιολογίας, Ronald Ross. Αυτό το σύστημα είναι μη γραμμικό, και έτσι δεν παρέχει μια γενική αναλυτική λύση. Παρόλα αυτά, σημαντικά αποτελέσματα μπορούν να παραχθούν αναλυτικά. Βασιζόμενη στην υπόθεση ότι δεν έχουμε θανάτους και άρα ο συνολικός πληθυσμός μας παραμένει σταθερός προκύπτει ότι:

S(t)+I(t)+R(t)= Constant =N< = > (dS/dt)+(dI/dt)+(dR+dt)=0

εκφράζοντας με μαθηματικούς όρους τη σταθερότητα του πληθυσμού N. Σημειωτέων ότι η δυναμική των μολυσματικών κατηγοριών εξαρτάται από την ακόλουθη αναλογία:

Ro=β/v

τον αποκαλούμενο βασικό αριθμό αναπαραγωγής. Κατόπιν με τη διαίρεση της πρώτης διαφορικής εξίσωσης με την τρίτη, το διαχωρισμό των μεταβλητών και την ενσωμάτωση παίρνουμε:

$S(t)=S(0)e^{-R_0(R(t)-R(0))}$

(όπου το S(0) και το R(0) είναι οι αρχικοί αριθμοί, αντίστοιχα, των ευπαθών και αναρρωμένων ατόμων). Κατά συνέπεια, στο όριο, το ποσοστό των αναρρωμένων ατόμων υπακούει την υπερβατική (trancendetal) εξίσωση:

$R_{\infty} = 1-S(0)e^{-o(R_{\infty}-R(0))}$

Η εκτίμηση αυτής της εξίσωσης δείχνει ότι γενικά, στο τέλος μιας επιδημίας, δεν έχουν αναρρώσει όλα τα άτομα, έτσι μερικά πρέπει να παραμείνουν ευάλωτα. Αυτό σημαίνει ότι το τέλος μιας επιδημίας προκαλείται από την πτώση του αριθμού των μολυσμένων ατόμων και όχι από την παντελή έλλειψη ευπαθών ατόμων. Ο ρόλος του βασικού αριθμού αναπαραγωγής είναι εξαιρετικά σημαντικός. Στην συνέχεια, γράφουμε την εξίσωση για τα μολυσμένα άτομα ως εξής:

$dI/dt =(\beta S-v)I$

Είναι σαφές ότι εάν:

$R_o > (1/S)$

Τότε

$(dI/dt(0)) > 0$

Θα υπάρξει ένα κατάλληλο επιδημικό ξέσπασμα με μια αύξηση του πλήθους των μολυσμένων (που μπορεί να φθάσει ένα αξιόλογο μέρος του πληθυσμού). Κατά συνέπεια, είναι σαφές ότι η αναλογία β/v είναι εξαιρετικά σημαντική.
Σημειώστε ότι στο ανωτέρω πρότυπο η συνάρτηση:

F=βI,
μοντελοποιεί το ρυθμό μετάβασης από το διαμέρισμα των ευπαθών ατόμων στο διαμέρισμα των μολυσματικών ατόμων και γι' αυτό το λόγω καλείται δύναμη της μόλυνσης.
Ωστόσο, για τις μεγάλες κατηγορίες μεταδοτικών ασθενειών είναι ρεαλιστικότερο να εξεταστεί μια δύναμη μόλυνσης που δεν εξαρτάται από τον απόλυτο αριθμό των μολυσμένων ατόμων, αλλά από ένα μέρος τους (όσον αφορά *το* συνολικό σταθερό πληθυσμό N):

Ο Capasso και κατόπιν, άλλοι συγγραφείς έχουν προτείνει μη γραμμικές δυνάμεις μόλυνσης για να μοντελοποιήσουν πιο ρεαλιστικά τη διαδικασία μετάδοσης της ασθένειας.

2)Το SIR πρότυπο με ζωτική δυναμική και σταθερό πληθυσμό

Εξετάζοντας έναν πληθυσμό που χαρακτηρίζεται από ένα ρυθμό θανάτων μ και ρυθμό γεννήσεων ίσο με το ρυθμό θανάτου, όπου μια μεταδοτική ασθένεια εξαπλώνεται το μοντέλο [62] είναι:

(dS/dt)=μv-μS-β*(I/N)*S

(dI/dt)= β*(I/N)*S-(μ+v)*I

(dR/dt)=vI-μR

Στο οποίο ισχύει ότι S+I+R=N

Επίσης σε περίπτωση που εισάγουμε ένα ρυθμό αναπαραγωγής αυτός ισούται με:

Ro=(β/μ+v)

6.9.5 ΜΕΤΑΒΛΗΤΟΙ ΡΥΘΜΟΙ ΕΠΑΦΩΝ ΚΑΙ ΠΟΛΥΕΤΕΙΣ Η ΧΑΟΤΙΚΕΣ ΕΠΙΔΗΜΙΕΣ

Είναι ευρέως γνωστό ότι η πιθανότητα να ασθενήσει κανείς δεν είναι σταθερή στην πάροδο του χρόνου. Ακόμα και από την προσωπική μας εμπειρία γνωρίζουμε ότι μερικές ασθένειες είναι συχνότερα παρούσες το χειμώνα, ενώ άλλες το καλοκαίρι. Επιπλέον, όσον αφορά τις ασθένειες της παιδικής ηλικίας, υπάρχει μια ισχυρή επιρροή του σχολικού ημερολογίου σε αυτές, τέτοια ώστε κατά τη διάρκεια των σχολικών διακοπών η πιθανότητα να προσβληθεί κανείς από μια τέτοια ασθένεια να μειώνεται εντυπωσιακά.

Κατά συνέπεια, για πολλές κατηγορίες ασθενειών θα πρέπει να ληφθεί υπόψη μια δύναμη μόλυνσης με περιοδικό (''εποχιακό'') κυμαινόμενο ρυθμό επαφών.

Έτσι το μοντέλο μετασχηματίζεται ως εξής:

$(dI/dt)=\beta(t)* (I/N)*S-(\mu+v)*I$

Η δυναμική της εύκολης ανάρρωσης προκύπτει από την ισότητα R=N-S-I, οδηγώντας σε ένα μη γραμμικό σύνολο διαφορικών εξισώσεων με περιοδικά μεταβαλλόμενες παραμέτρους.

6.9.6 ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΠΡΟΓΡΑΜΜΑΤΩΝ ΜΑΖΙΚΟΥ ΕΜΒΟΛΙΑΣΜΟΥ.

Ο εμβολιασμός των νεογνών με την παρουσία των μεταδοτικών ασθενειών είναι ένας από τους κύριους στόχους για την επάλειψη τους μέσω των μέτρων πρόληψης και εάν είναι δυνατόν, μέσω της καθιέρωσης ενός προγράμματος μαζικού εμβολιασμού. Ας εξετάσουμε μια ασθένεια για την οποία είναι αναγκαίος ο εμβολιασμός των νεογέννητων [74] (με ένα εμβόλιο που προσφέρει ισόβια ανοσία) με ένα ρυθμό :
$P \square (0,1)$:

$(dS/dt)=\mu N(1-P)-\mu S-\beta(I/N)S$
$(dI/dt)= \beta(I/N)S-(\mu+v)I$
$(dV/dt)=\mu NP-\mu V$

όπου το V είναι η κατηγορία των εμβολιασμένων.

Εμβολιασμός και η ορθολογική εξαίρεση.

Οι σύγχρονες κοινωνίες αντιμετωπίζουν μία πρόκληση την "ορθολογική" εξαίρεση, δηλαδή υπάρχει και η οικογενειακή απόφαση που οι γονείς δεν θέλουν να εμβολιαστούν τα παιδιά τους και αυτό έχει ως συνεπεία μια "ορθολογική" σύγκριση μεταξύ του αντιληπτού κινδύνου που διατρέχουν από τη μόλυνση ή αυτών των παρενεργειών που προέρχονται από την επίδραση του εμβολίου.

Προκειμένου να αξιολογηθεί εάν αυτή η συμπεριφορά είναι πραγματικά λογική, δηλαδή εάν μπορεί εξίσου να οδηγήσει στην εξόντωση της ασθένειας, κάποιος μπορεί απλά να υποθέσει ότι ο ρυθμός εμβολιασμού είναι μια αυξανόμενη συνάρτηση των μολυσμένων ανθρώπων [72]:

$P=P(I),P'(I) > 0$

Σε αυτή την περίπτωση η συνθήκη εξόντωσης μετασχηματίζεται:

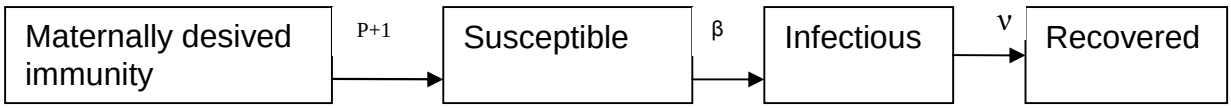
$P(0) \geq P^*$

Δηλαδή ο βασικός ρυθμός εμβολιασμού πρέπει να είναι μεγαλύτερος από το κατώτατο όριο του "υποχρεωτικού" εμβολιασμού. Κατά συνέπεια, η "ορθολογική" απαλλαγή μπορεί να είναι μειωτική δεδομένου ότι είναι βασισμένη μόνο στο τρέχων υψηλό αριθμό συμβάντων λόγω του υψηλού αριθμού εμβολιασμών.

6.9.7 ΤΡΟΠΟΠΟΙΗΣΕΙΣ ΣΤΟ ΒΑΣΙΚΟ SIR ΜΟΝΤΕΛΟ – ΤΟ MSIR ΜΟΝΤΕΛΟ

Για πολλές μολύνσεις, συμπεριλαμβανομένης και της ιλαράς, τα μωρά δεν γεννιούνται στο διαμέρισμα των ευπαθών αλλά είναι άνοσα στην ασθένεια για τους πρώτους μήνες της ζωής τους λόγω της προστασίας από τα μητρικά αντισώματα.

Αυτή η επιπρόσθετη λεπτομέρεια μπορεί να παρουσιαστεί με τη συμπερίληψη μιας κατηγορίας M (για την μητρική παραγόμενη ανοσία) στην αρχή του προτύπου (Σχήμα 8).



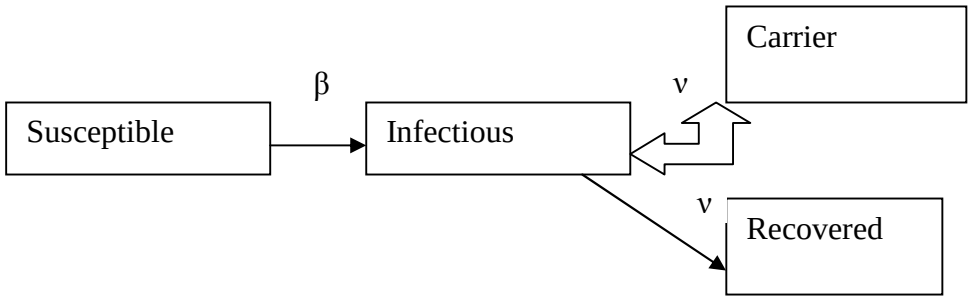
ΣΧΗΜΑ 8. ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ MSIR

6.10 ΚΑΤΑΣΤΑΣΗ ΦΟΡΕΩΝ-ΜΟΝΤΕΛΟ SICR

Μερικοί άνθρωποι που έχουν μια μολυσματική ασθένεια όπως η φυματίωση δεν αναρρώνουν ποτέ εντελώς και συνεχίζουν να φέρνουν τη μόλυνση, χωρίς να επηρεάζονται από την ασθένεια οι ίδιοι.

Έπειτα μπορεί να μετακινηθούν ξανά στο μολυσματικό διαμέρισμα και να υποστούν τα συμπτώματα ή μπορούν να συνεχίσουν να μολύνουν άλλα άτομα χωρίς ωστόσο να υποφέρουν και οι ίδιοι από τα συμπτώματα.

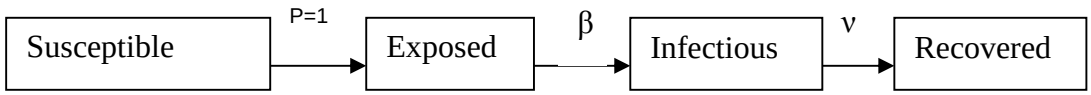
Το διασημότερο παράδειγμα αυτού είναι πιθανώς η Mary Mallon, η οποία μόλυνε 22 ανθρώπους με τον τυφοειδή πυρετό. Το διαμέρισμα των φορέων ονομάζεται C (Σχήμα 9).



ΣΧΗΜΑ 9 ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ SICR ΜΟΝΤΕΛΟΥ

6.11 ΤΟ ΜΟΝΤΕΛΟ SEIR

Για πολλές σημαντικές μολύνσεις υπάρχει μια σημαντική χρονική περίοδος κατά τη διάρκεια της οποίας ενώ το άτομο έχει μολυνθεί δεν είναι ακόμα ο ίδιος μολυσμένος. Κατά τη διάρκεια αυτής της λανθάνουσας περιόδου το άτομο είναι στο διαμέρισμα E (Σχήμα 10).



ΣΧΗΜΑ 10. ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ ΓΙΑ ΤΟ SEIR ΜΟΝΤΕΛΟ

Υποθέτοντας ότι η περίοδος παραμονής στο λανθάνον διαμέρισμα είναι μια τυχαία μεταβλητή με εκθετική κατανομή και παράμετρο α (δηλαδή η μέση λανθάνουσα περίοδος είναι ένα α - 1) και υποθέτοντας επίσης την παρουσία ζωτικής δυναμικής με ρυθμό γεννήσεων ίσο με το ρυθμό των θανάτων, έχουμε το μοντέλο [68]:

$(dS/dt)=\mu N-\mu S-\beta(I/N)S$

$(dE/dt)=\beta(I/N)S-(\mu+\alpha)E$

$(dI/dt)=\alpha E-(\mu+v)I$

$dR/dt=vI-\mu R$

επίσης υποθέτουμε ότι $S+E+I+R= N$

Για αυτό το μοντέλο ο βασικός ρυθμός αναπαραγωγής είναι:

$Ro=(\alpha/(\mu+\alpha))*(\beta/(\mu+v))$

6.12 ΕΠΙΔΗΜΙΟΛΟΓΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

Παρότι η επιδημιολογία αφορά κυρίως βιολογικούς οργανισμούς, η εμπειρία από τις θετικές έρευνες, αποδεικνύεται χρήσιμη για την αντιμετώπιση της εξάπλωσης του κακόβουλου λογισμικού.

Το βασικό πλεονέκτημα του Γενικού Επιδημιολογικού Μοντέλου είναι ότι μπορεί να περιγράψει ικανοποιητικά την εξέλιξη μιας επιδημίας υπολογιστών με τη χρήση των ακόλουθων διαφορικών εξισώσεων:

$$\mathbf{dS/dt = -\beta SI} \quad (1)$$

$$\mathbf{dI/dt = \beta SI - vI} \quad (2)$$

$$\mathbf{dR/dt = vI} \quad (3)$$

Για τους βιολογικούς ιούς όπως και αναφέραμε πιο πάνω **S** είναι ο αριθμός των ευπαθών οργανισμών, **I** ο αριθμός των μολυσμένων μελών ενός πληθυσμού, **R** είναι ο αριθμός των μελών που έχουν αναρρώσει ή βρίσκονται σε καραντίνα ή έχουν αποδημήσει, **β** είναι ο ρυθμός μόλυνσης ανά επαφή (pair wise rate of infection) και **v** ο ρυθμός απομάκρυνσης μολυσμένων μελών.

Οι παραπάνω διαφορικές εξισώσεις για να ισχύουν προϋποθέτουν την ομογενή ανάμιξη του πληθυσμού και ότι ο πληθυσμός είναι σταθερός βάση του τύπου :

$$\mathbf{N=S(t)+I(t)+R(t)} \quad (4)$$

Το Γενικό Επιδημιολογικό Μοντέλο, το οποίο είναι γνωστό και ως **S-I-R**. (Susceptible Infective-Recovered) μπορεί με τις κατάλληλες παραδοχές να περιγράψει με μεγάλη ακρίβεια την εξάπλωση όμως και του κακόβουλου λογισμικού. Ας δούμε κάποιες από τις παραμέτρους που λαμβάνουν χώρα στα επιδημιολογικά μοντέλα με βάση τώρα όχι την επιδημιολογία των βιολογικών ιών αλλά των υπολογιστών:

N : ο συνολικός πληθυσμός. Στην επιδημιολογία υπολογιστών και ειδικότερα στη μελέτη διάδοσης κακόβουλου λογισμικού είναι ο αριθμός των συστημάτων που είναι συνδεδεμένα στο διαδίκτυο.

S : ο αριθμός των ευπαθών συστημάτων. Στην προκειμένη περίπτωση ο αριθμός των υπολογιστών που εκτελούν το λειτουργικό σύστημα ή την εφαρμογή που εμφανίζει το κενό ασφαλείας εκμεταλλεύεται το εξεταζόμενο είδος κακόβουλου λογισμικού. Όσο πιο διαδεδομένο είναι ένα λειτουργικό σύστημα ή μια εφαρμογή τόσο πιθανότερο είναι να προσβληθεί από κάποια μορφή κακόβουλου λογισμικού αν εμφανίσει κάποιο κενό ασφαλείας. Παράλληλα, κατά αυτόν το τρόπο ο ευπαθής πληθυσμός καθίσταται γρηγορότερα μολυσμένος, αποδεικνύοντας ότι η ποικιλομορφία στα πληροφοριακά συστήματα δεν αποτελεί μια περιττή πολυτέλεια, αλλά μια απαραίτητη προφύλαξη.

I: ο αριθμός των μολυσμένων συστημάτων. Στόχος όλων των ερευνητικών προσπαθειών είναι η ελαχιστοποίηση αυτού του συνόλου.

R: ο αριθμός των ανακτημένων ή απομονωμένων μελών. Στην επιδημιολογία των υπολογιστών το R περιλαμβάνει όλα τα συστήματα που είναι επαρκώς προστατευμένα και δεν παρουσιάζουν τα κενά ασφάλειας που αποτελούν τις πύλες εισόδου για το εξεταζόμενο κακόβουλο Λογισμικό.

Η μεγιστοποίηση του R είναι σίγουρα προς το κοινό συμφέρον, αλλά αυτό καθίσταται όλο και δυσκολότερο όσο το χρονικό διάστημα από την κοινοποίηση του κενού ασφαλείας μειώνεται.

Επιπρόσθετα, αν κάποιο δικτυακό σκουλήκι εκμεταλλεύεται κάποιο άγνωστο (ZERO DAY) κενό ασφάλειας, το R μπορεί να αυξηθεί μόνο με την χρήση εξωτερικών μηχανισμών ασφαλείας, όπως τα firewall, τα οποία θα μπορούσαν πιθανώς να ανακόψουν κάποια είδη επιθέσεων.

Από την άλλη πλευρά, υπάρχει και μια δεύτερη όψη του R, καθώς περιλαμβάνει και τα συστήματα τα οποία καταστρέφονται από το κακόβουλο λογισμικό.
Ένα υπερμολυσματικό δικτυακό σκουλήκι είναι αμφίβολο αν θα μπορούσε να διαδοθεί σημαντικά.

β: ο ρυθμός μόλυνσης ανά επαφή. Όσο μεγαλύτερο είναι το β τόσο γρηγορότερα ένα δικτυακό σκουλήκι εξαπλώνεται. Οι συγγραφείς κακόβουλου λογισμικού στην προσπάθεια τους να αυξήσουν το β, χρησιμοποιούν διάφορες τεχνικές.

Χαρακτηριστικά παραδείγματα είναι η ανίχνευση πολλών στόχων ταυτόχρονα με την χρήση νημάτων (threads) όπως στην περίπτωση του δικτυακού σκουληκιού Code Red ή η ενσωμάτωση ολόκληρου του κώδικα του κακόβουλου λογισμικού σε

ένα μόνο πακέτο udp, προκειμένου να αποφευχθούν οι καθυστερήσεις στην δημιουργία των συνδέσεων που εμπεριέχονται στο πρωτόκολλο TCP.

v: ο ρυθμός απομάκρυνσης μολυσμένων κόμβων λόγω ανάρρωσης, απομόνωσης ή θανάτου σε βιολογικούς οργανισμούς. Κατά την διάρκεια μιας επιδημίας κακόβουλου λογισμικού, αν το v λάβει μεγάλη τιμή οι προοπτικές για το περιορισμό του λογισμικού που την προκάλεσε είναι ευοίωνες. Αυτό μπορεί να γίνει, είτε με την έγκυρη μεταφόρτωση και εγκατάσταση διορθωτικού κώδικα, είτε αν το φορτίο του κακόβουλου λογισμικού είναι πολύ καταστροφικό.

6.13 ΚΑΤΑΣΤΑΣΕΙΣ ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΒΡΙΣΚΕΤΑΙ Ο ΥΠΟΛΟΓΙΣΤΗΣ

1. Υγιείς : ούτε μολυσμένος ούτε με ανοσία
2. Μολυσμένος
3. Απομονωμένος: υπολογιστής εκτός δικτύου
4. Ανοσία με ενημερωμένο antivirus
5. Νεκρός: έχει γίνει format

Ένας υγιής υπολογιστής μολύνεται κατά την επικοινωνία του με ένα μολυσμένο ενώ θεωρούμε ότι θεραπεύεται αν έχει γίνει format ή το antivirus που χρησιμοποιεί είναι ενημερωμένο (δηλαδή αν πεθάνει ή αποκτήσει ανοσία). Οι απομονωμένοι υπολογιστές δεν επικοινωνούν με άλλους υπολογιστές και κατ' αυτό τον τρόπο και δεν μπορούν ούτε να μολυνθούν αλλά ούτε και να μολύνουν άλλους υπολογιστές. Έτσι οι παράγοντες που επηρεάζουν την διάδοση της μόλυνσης είναι οι ακόλουθοι [65] :

1) Η πύλη εισόδου του κακόβουλου λογισμικού .
2) Η στρατηγική επιλογής νέων στόχων
3) Η απόσταση επίθεσης. Μέγιστη απόσταση όπου ένας υπολογιστής μπορεί να μολύνει ένα άλλο. Αυτή η απόσταση δεν είναι κατ' ανάγκη χωρική όμως μπορεί π.χ. ένας υπολογιστής να μολύνει μόνο pc που βρίσκονται στο ίδιο δίκτυο με αυτόν ή γειτονικά κτλ.
4) Ο αριθμός επιθέσεων στην μονάδα του χρόνου. Πόσες επιθέσεις δηλαδή μπορεί να κάνει ένας κόμβος κατά την διάρκεια της μέρας.

5) Η αποτελεσματικότητα επίθεσης. Καθορίζει το πόσο πιθανό είναι ένας υγιής κόμβος να μολυνθεί κατά την επικοινωνία του με ένα μολυσμένο.

6) Η περίοδος μόλυνσης. Η χρονική διάρκεια κατά την οποία ένας υπολογιστής παραμένει μολυσμένος.

7) Το αρχικό πλήθος των υγιών- μολυσμένων κόμβων.

8) Η πιθανότητα θανάτου. Είναι η πιθανότητα να γίνει format σε ένα pc μετά από την μόλυνση του.

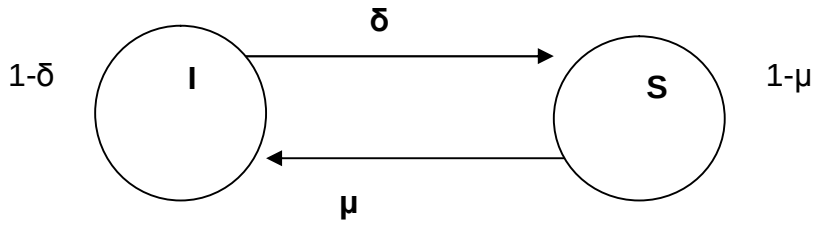
ΕΠΙΠΛΕΟΝ ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΛΗΦΘΟΥΝ ΥΠΟΨΗ ΕΙΝΑΙ ΟΙ ΑΚΟΛΟΥΘΟΙ:

1) Οι ομάδες στις οποίες ανήκουν οι υπολογιστές.
2) Η ενημέρωση του antivirus.
3) Η Απομόνωση του κόμβου ακολουθώντας κάποιες στρατηγικές.

6.14 ΤΟ SIS ΜΟΝΤΕΛΟ ΣΕ ΔΙΚΤΥΑ ΕΛΕΥΘΕΡΗΣ ΚΛΙΜΑΚΑΣ

Το μοντέλο αυτό είναι από τα πιο δημοφιλή μιας και έχει δανειστεί από την επιστήμη της επιδημιολογίας ότι αφορά βιολογικούς ιούς. Σε αυτό το μοντέλο κάθε κόμβος αποτελεί μια ξεχωριστή οντότητα και κάθε ακμή (σύνδεσμος) αναπαριστά μία σύνδεση μέσω της οποίας ο ιός μπορεί να διαδοθεί σε άλλα συστήματα. Κάθε κόμβος μπορεί να βρίσκεται σε μία από τις δύο καταστάσεις: υγιής-ευπαθείς (susceptible) ή μολυσμένος (infected).

Κάθε χρονική στιγμή ένας υγιής κόμβος μπορεί να μολυνθεί με ένα ρυθμό **μ** εφόσον είναι συνδεμένος με έναν ή περισσότερους κόμβους. Αντίστοιχα ένας μολυσμένος κόμβος μπορεί να γίνει ξανά υγιής με ένα ρυθμό **δ** ορίζοντας έτσι ένα ρυθμό διάδοσης του ιού τον οποίο $\lambda=\mu/\delta$ [16]



ΣΧΗΜΑ 11 ΔΙΑΓΡΑΜΜΑ ΡΟΗΣ SIS ΜΟΝΤΕΛΟ

Χωρίς να κάποια γενίκευση μπορούμε να θέσουμε το δ=1 έτσι ώστε το μοντέλο που προκύπτει να αναπαριστά την περίπτωση προγράμματος προστασίας στην οποία όλοι οι μολυσμένοι υπολογιστές γίνονται τελικά υγιείς. Το ζητούμενο λοιπόν σε αυτήν την περίπτωση είναι η εύρεση ενός επιδημικού κατωφλιού λc τέτοιο ώστε για οποιαδήποτε τιμή του λ μεγαλύτερη από αυτό, η διάδοση της μόλυνσης να γίνετε επίμονη ενώ για τιμές του λ μικρότερες αυτού του κατωφλιού η μόλυνση μπορεί να εξασθενεί με εκθετικό ρυθμό.

Στατιστικά δεδομένα εξάπλωσης πραγματικών ιών σε δίκτυα ελεύθερης κλίμακας, (δηλαδή για δίκτυα όπου η πιθανότητα ένας κόμβος να είναι συνδεδεμένος με άλλους n, δίνεται από τον τύπο $P(n)=n^{-k}$ όπου το k κυμαίνεται από 2 έως 3 και οδηγούν στο συμπέρασμα ότι όλοι οι επίμονοι ιοί οδηγούνται σε κορεσμό με πολύ μικρό ποσοστό ανθεκτικότητας επηρεάζοντας μόνο ένα πολύ μικρό ποσοστό επί του συνολικού αριθμού των υπολογιστών. Αυτό το γεγονός έρχεται σε αντιπαράθεση με τις θεωρητικές προβλέψεις (έκτος βέβαια της σπάνιας περίπτωσης όπου όλοι οι ιοί έχουν ρυθμό διάδοσης απειροελάχιστα μεγαλύτερο από την τιμή του κατωφλιού λc).

Το γεγονός αυτό αποδεικνύει ότι παρόλο που το εν λόγο μοντέλο είναι αρκετά διδακτικό δεν επαρκεί για την αναπαράσταση του πραγματικού φαινομένου.

Το ντετερμινιστικό αυτό μοντέλο είναι ομογενές (δηλαδή κάθε κόμβος έχει την ίδια πιθανότητα να θεραπευτεί ή να μεταδώσει την μόλυνση) και προτάθηκε από τον Ross (1915). Ουσιαστικά αυτό που κάνει είναι η δημιουργία μιας καμπύλης (γραφικής παράστασης)όπου προβλέπει τον αφανισμό της επιδημίας οποτεδήποτε ο βασικός ρυθμός αναπαραγωγής (έστω R) είναι μικρότερος της μονάδας, ενώ γίνεται η διατήρηση αυτής αν R>1 οποτεδήποτε η αρχική αναλογία των μολυσμένων κόμβων είναι θετική.

Το στοχαστικό SIS μοντέλο προτάθηκε από τους Weiss και Dishon (1971)[66]. Και ουσιαστικά είναι συνεχούς χρόνου Markov αλυσίδα γεννήσεων, και θανάτων η οποία χρησιμοποιείται για την μοντελοποίηση επιδημιών, την διάδοση των φημών καθώς και για την μοντελοποίηση των χημικών αντιδράσεων.

6.14.1 ΠΑΡΑΛΛΑΓΕΣ

Δεδομένου ενός δικτύου και ενός μοντέλου διάδοσης ιών με ένα αρχικό πλήθος μολυσμένων κόμβων εμείς ενδιαφερόμαστε να ανοσοποιήσουμε το μικρότερο δυνατό πλήθος κόμβων έτσι ώστε στο δίκτυο να είναι συγκρατημένη η διάδοση της μόλυνσης. Σε αυτό το σημείο θα εξετάσουμε 2 διαφορετικούς τύπους μοντέλων το ανεξάρτητο σειριακό μοντέλο Kempe et al [69] και τα SIS μοντέλα (μοντέλα δυναμικής διάδοσης) [70].

Ξεκινώντας με την πρωτοποριακή εργασία των Kermack και McKendric[6] όπου καθιερώνουν την πρώτη στοχαστική θεωρεία διάδοσης των επιδημιών που αποδεικνύουν την ύπαρξη επιδημικού κατωφλιού το οποίο και καθορίζει αν η επιδημία θα εξαπλωθεί ή θα τερματιστεί, ένας μεγάλος αριθμός εργασιών επικεντρώνεται στην παροχή αναλυτικών εκφράσεων για τα επιδημικά κατώφλια, για τα διαφορετικά μοντέλα διάδοσης και για τις διαφορετικές κατηγορίες δικτύων [64].

Σε ομογενή δίκτυα ένας αποτελεσματικός μηχανισμός καταστολής της διάδοσης των επιδημιών είναι η θεραπεία τυχαίων κόμβων στο δίκτυο [68]. Ωστόσο η μέθοδος αυτή είναι ανεπαρκής για δίκτυα ελεύθερης κλίμακας λόγω της ύπαρξης κόμβων με υψηλή συνδεσιμότητα. Παρόλα αυτά ακόμα και γι' αυτά τα δίκτυα μπορεί να αποδειχθεί ότι υπάρχει επιδημικό κατώφλι. Μία καλή πρακτική για την αντιμετώπιση της εξάπλωσης των επιδημιών σε αυτά τα δίκτυα είναι να θεραπεύουμε αυτούς τους κόμβους που παρουσιάζουν υψηλή συνδεσιμότητα έτσι ώστε να οδηγηθούμε σε εξασθένηση της διάδοσης της επιδημίας.

Σε περιπτώσεις όπου η τοπολογία των δικτύων δεν είναι γνωστή ο Cohen [71] έδειξε ότι η ανοσοποίηση τυχαίων ακολουθιών με τυχαίους κόμβους είναι καλύτερη από την ανοσοποίηση τυχαίων κόμβων.

ΚΕΦΑΛΑΙΟ 7

7.1 ΤΟ ΠΡΟΟΔΕΥΤΙΚΟ PSDIR ΜΟΝΤΕΛΟ

Βασιζόμενοι στις ιδέες που αποκομίστηκαν από τα προηγούμενα πρότυπα ένα νέο επιδημιολογικό πρότυπο παρουσιάζεται που μοντελοποιεί τις πραγματικές διαδικασίες που λαμβάνουν χώρα στις επιδημίες των ιών και των υπολογιστών.

Ξεκινώντας εξετάζουμε τα χαρακτηριστικά ενός τυπικού ξεσπάσματος. Στην συνέχεια συμπεριλαμβάνουμε τις πτυχές των πραγματικών ξεσπασμάτων στο PSIDR (προοδευτικό-Ευπαθή-Μολυσμένο-Ανιχνευμένο-Αφαιρεμένο) μοντέλο, με έναν άτυπο τρόπο και έπειτα αναλυτικά.

7.1.1 Η ΧΡΟΝΙΚΗ ΠΟΡΕΙΑ ΕΝΟΣ ΤΕΧΝΟΛΟΓΙΚΟΥ ΞΕΣΠΑΣΜΑΤΟΣ

Φανταστείτε την ακολουθία γεγονότων που συμβαίνουν όταν ένα σκουλήκι προσπαθεί να μολύνει ένα τεχνολογικό δίκτυο.

Για λόγους απλότητας, το εξεταζόμενο δίκτυο εδώ θα είναι το δίκτυο του ηλεκτρονικού ταχυδρομείου μιας μεγάλης εταιρείας.

Μια υπόθεση που θα πρέπει να κάνουμε είναι ότι όλοι οι υπολογιστές στο δίκτυο έχουν κάποιο είδος λογισμικού προστασίας από τους ιούς. Αυτό το λογισμικό μπορεί να ενημερώνεται με κάποια συχνότητα, για παράδειγμα μια φορά την ημέρα έτσι ώστε να σιγουρευτούμε ότι και οι πιο πρόσφατες υπογραφές ιών συμπεριλαμβάνονται στο εν λόγο λογισμικό (ΛΠΥ).

Το πρώτο γεγονός που συμβαίνει είναι η αρχική μόλυνση. Παραδείγματος χάριν, αν ένας υπάλληλος ανοίξει ένα αρχείο (εκτελέσιμο) που έχει επισυναφτεί σε ένα ηλεκτρονικό μήνυμα που στάλθηκε από κάποιον εκτός της επιχείρησης.

Αυτό το πρόγραμμα, μόλις εκτελεσθεί, στέλνεται σε μερικές από τις επαφές του υπαλλήλου (π.χ. στις πρώτες δέκα διευθύνσεις στο βιβλίο διευθύνσεων του).

Εάν κάποιες από τις επαφές είναι στην πραγματικότητα κατάλογοι αλληλογραφίας (κατάλογοι επαφών), τότε το δικτυακό σκουλήκι έχει τη δυνατότητα να μολύνει όλες τις επαφές που απαριθμούνται σε αυτό. Μόλις λάβουν οι άλλοι χρήστες τα σταλμένα μηνύματα ηλεκτρονικού ταχυδρομείου νομίζοντας ότι είναι μήνυμα από τον υπάλληλο, μερικοί από αυτούς μπορεί να το ανοίξουν αμέσως, άλλοι βέβαια όχι αλλά αυτό εξαρτάται με διάφορους παράγοντες (όπως οι προσωπικές συνήθειες, κ.λπ.).

Προτού να μπορέσει το σκουλήκι να καθαριστεί από τους υπολογιστές, πρέπει να ανιχνευθεί πρώτα. Η ανίχνευση θα είναι ιδιαίτερα δύσκολη όταν το σκουλήκι δεν επιβάλλει άμεσα καθόλου ωφέλιμο φορτίο στις μηχανές. Επιπλέον, το λογισμικό προστασίας της εταιρίας θα ανιχνεύσει μόνο τα σκουλήκια για τα οποία έχει τις υπογραφές. Επομένως, μόλις εντοπιστούν μερικά στιγμιότυπα ενός ιού, οι εταιρίες παραγωγής λογισμικών προστασίας θα προσπαθήσουν να εξαγάγουν την υπογραφή των ιών και να την καταστήσουν διαθέσιμη έτσι ώστε όλοι οι υπολογιστές να μπορούν να ενημερώσουν το λογισμικό τους.

Τα πρώτα στιγμιότυπα του σκουληκιού θα γίνουν αντιληπτά για διάφορους λόγους. Σε μερικές περιπτώσεις, η απόδοση του δικτύου μειώνεται επειδή τα διάφορα αντίγραφα του σκουληκιού καταναλώνουν πάρα πολύ εύρος ζώνης (bandwith). Σε άλλες περιπτώσεις, το ωφέλιμο φορτίο το οποίο έχει επιβληθεί δείχνει σαφώς ότι υπάρχει μια μόλυνση.

Επιπρόσθετα υπάρχουν και άλλοι τρόποι με τους οποίους ο ένας θα μπορούσε να ανιχνεύσει ένα ξέσπασμα, όπως για παράδειγμα η κατοχή του "ολοήμερου προσωπικού" ή ακόμα και με έλεγχο από τους προμηθευτές των antivirus. Από αυτήν την στιγμή, οι χρήστες γνωρίζουν την απειλή και αρχίζει να διαμορφώνεται ένα σχέδιο για την καταστολή της.

Μόλις είναι διαθέσιμη η απογραφή, οποιοσδήποτε χρήστης συνδεθεί στον υπολογιστή του μπορεί να ενημερώσει αυτόματα το λογισμικό προστασίας του με τη τελευταία υπογραφή.

Δεδομένου ότι όλο και περισσότεροι χρήστες ενσωματώνονται με την νέα υπογραφή, οι ευπαθείς υπολογιστές αποκτούν σταδιακά ανοσία ενάντια στο σκουλήκι, ενώ οι μολυσμένοι υπολογιστές βαθμιαία ανιχνεύονται.

Σε ένα μεγάλο εταιρικό δίκτυο, η χαρακτηριστική αντίδραση όταν βρίσκεται μια μηχανή να είναι μολυσμένη είναι η επίκληση της τεχνικής υποστήριξης για τον πλήρη καθαρισμό. Συνήθως, η πρώτη ενέργεια που λαμβάνει χώρα είναι η απομόνωση του υπολογιστή έτσι ώστε να μην μπορεί να μεταδώσει την μόλυνση.

Δηλαδή ο μολυσμένος υπολογιστής να μεταβαίνει από μία κατάσταση μόλυνσης σε μια κατάσταση μόλυνσης όπου δεν μπορεί να μεταδώσει την μόλυνση (κατάσταση ανιχνευμένης μόλυνσης).

Η διάρκεια αυτής της κατάστασης εξαρτάται τώρα από το πόσο γρήγορα ο ειδικός τεχνικός θα καθαρίσει τον υπολογιστή από την μόλυνση. Μπορεί να πάρει από μερικά λεπτά μέχρι μερικές ώρες (ή ακόμα και ημέρες).

Μόλις καθαριστεί ο υπολογιστής, συνδέεται πάλι στο δίκτυο και είναι ήδη ανοσοποιημένος σε περαιτέρω μολύνσεις επειδή έχει πλέον τη νέα υπογραφή ιών στους ορισμούς του ΛΠΥ του.

Έτσι η μόλυνση εξαλείφεται όταν ανοσοποιούνται όλοι οι υπολογιστές. Στην πράξη βέβαια πάντα υπάρχουν μερικές μολύνσεις λόγω της ελλιπούς ανοσοποίησης ή και επειδή μερικοί χρήστες δεν είναι ενήμεροι σχετικά με την απειλή.

7. 2 ΤΟ PSIDR ΜΟΝΤΕΛΟ.

Σε αυτό το τμήμα, παρουσιάζονται πώς οι προαναφερθείσες πτυχές ενσωματώνονται στο πρότυπο. Σύμφωνα με το προοδευτικό πρότυπο λοιπόν ευπαθούς- μολυσμένου-ανιχνευμένου- αφαιρεμένου μοντέλου, τα επιδημικά γεγονότα στα δίκτυα υπολογιστών μπορούν να διαιρεθούν σε δύο χρονολογικές περιόδους.

Η περίοδος προς την αντίδραση. Στην αρχή, ο πρώτος ιός μολύνει μια μηχανή στο δίκτυο. Για τις επόμενες μερικές μέρες (ή ώρες), ο ιός διαδίδεται ελεύθερα στο δίκτυο χωρίς την παρατήρηση του από τους περισσότερους χρήστες. Με βάση τους όρους του PSIDR, αυτό διαμορφώνεται ως ένα θετικό ποσοστό γέννησης β και καμία θεραπεία. Οι ευπαθείς κόμβοι επομένως μολύνονται με πιθανότητα β εάν έρθουν σε επαφή (δηλ. επικοινωνήσουν) με ένα μολυσμένο κόμβο.

Η περίοδος αντίδρασης. Μετά από κάποιο χρόνο, ο ιός ανιχνεύεται σε μερικούς υπολογιστές και έτσι λαμβάνονται άμεσες ενέργειες για την αποτροπή της περεταίρω εξάπλωσης αλλά και για την θεραπεία των ήδη μολυσμένων κόμβων. Έτσι επίσης εξάγεται και η υπογραφή και περιλαμβάνεται σε ένα ορισμένο ποσοστό των λογισμιών προστασίας των υπολογιστών του δικτύου. Μηχανές που δεν ήταν μολυσμένες γίνονται αυτόματα άνοσες στον ιό, ενώ άλλες που έχουν ήδη μολυνθεί ανιχνεύονται σε ένα ορισμένο ποσοστό.(Ανάλογα με το πόσο συχνά γίνεται η ενημέρωση του ΛΠΥ.) Αυτές οι μηχανές είναι έπειτα απομονωμένες και ανοσοποιημένες ενάντια στην περαιτέρω μόλυνση.

Πάλι, στο πρότυπο PSIDR αυτή η περίοδος διαμορφώνεται με το ίδιο ποσοστό γέννησης όπως πριν, αλλά αυτή τη φορά οι ευπαθείς κόμβοι γίνονται ανοσοποιημένοι

σε ένα ποσοστό μ, και οι μολυσματικοί κόμβοι ανιχνεύονται σε ένα ποσοστό μ και θεραπεύονται έπειτα με ένα ποσοστό δ.

Το ποσοστό μ αντιπροσωπεύει την ταχύτητα της διανομής της υπογραφής Η μόνη λεπτομέρεια που αφήνεται είναι ο χρόνος όταν το σύστημα μεταβαίνει από την προ αντίδρασης περίοδο στην περίοδο αντίδρασης.

Στο πρότυπο PSIDR, αυτό το χρονικό διάστημα αναπαρίσταται από μια παράμετρο π, η οποία μπορεί να πάρει μια αυθαίρετη τιμή. Αυτή η παράμετρος αντιπροσωπεύει το χρονικό διάστημα που μεσολαβεί από την χρονική στιγμή της πρώτης μόλυνσης έως την χρονική στιγμή της έκδοσης της υπογραφής.

7.2.1 ΣΥΝΕΙΣΦΟΡΕΣ ΤΟΥ ΠΡΟΤΥΠΟΥ PSIDR

Όσον αφορά τα πρότυπα SIS, SIR, και SEIR, το πρότυπο PSIDR περιγράφεται καλύτερα ως μια ακολουθία καταστάσεων με ρυθμούς μεταβάσεων μεταξύ αυτών.

Η ακόλουθη περιγραφή δίνει έμφαση σε διάφορους παράγοντες όπου λαμβάνονται υπόψη κατά τη μοντελοποίηση της διάδοσης των ιών σε δίκτυα των υπολογιστών. Οι κύριες συνεισφορές του προτύπου PSIDR στα γενικά επιδημιολογικά πρότυπα είναι:

Μεταβλητότητα του ρυθμού θεραπείας. Αρχικά, κανένας μολυσμένος υπολογιστής δεν θεραπεύεται. Μόνο μετά από μια ορισμένη χρονική περίοδο όπου τα στιγμιότυπα του ιού αρχίζουν να προσδιορίζονται και να απομακρύνονται από τους μολυσμένους οικοδεσπότες τους.

Στο PSIDR πρότυπο, το επιδημικό γεγονός διαιρείται σε δύο χρονολογικές περιόδους αντίστοιχα ως προς την αντίδραση και την περίοδο αντίδρασης. Στην πρώτη περίοδο οι ιοί διαδίδονται με ένα ποσοστό β και δεν απομακρύνονται (οι ρυθμοί ανίχνευσης (μ) και θεραπείας (δ) είναι μηδενική.)

Κατόπιν, σε κάποιο χρόνο που καθορίζετε από την παράμετρο π, το σύστημα μεταπηδά στη δεύτερη περίοδο όπου οι μολυσμένοι οικοδεσπότες μπορούν τώρα να θεραπεύονται (τα ποσοστά ανίχνευσης και θεραπείας παίρνουν αντίστοιχα σταθερές μη μηδενικές τιμές). Τα προηγούμενα επιδημικά πρότυπα δεν υπολόγιζαν αυτό το είδος της μεταβλητότητας του ποσοστού της θεραπείας.

Ευθείες μεταβάσεις από το S στο R. Από την στιγμή που η υπογραφή των ιών είναι διαθέσιμη, οι ευπαθείς υπολογιστές μπορούν να γίνουν άνοσοι χωρίς να

μεταβούν στην μολυσμένη κατάσταση εάν το λογισμικό προστασίας στους ευπαθείς οικοδεσπότες ενημερώνεται πριν προλάβει να τους μολύνει ο ιός.

Στο πρότυπο PSIDR, αυτό αντιπροσωπεύεται από τις πιθανές ευθείες μεταβάσεις από το S στο R κατά τη διάρκεια της περιόδου αντίδρασης. Συγκεκριμένα, σε αυτήν την περίοδο ένας ευπαθής οικοδεσπότης γίνεται αφαιρούμενος σε ένα ποσοστό μ. Οι άμεσες μεταβάσεις όπως αυτή δεν περιλήφθηκαν στα παλαιότερα πρότυπα.

Κατάσταση ανίχνευσης. Σε αυτή την περίοδο, μολυσμένοι (αλλά ακόμα λειτουργικοί) υπολογιστές ανιχνεύονται μόνο όταν ενημερώνεται το λογισμικό με την νέα υπογραφή. Μόλις το ανιχνευθεί, ο χρήστης (ή τεχνικός) το απομονώνει από το δίκτυο και φροντίζει για την αποκατάστασή του.

Στο πρότυπο PSIDR, αυτό μοντελοποιείται με την παρεμβολή μιας νέας καταστάσεις (αποκαλούμενη ¨D¨ για detected) μεταξύ των I και R καταστάσεων. Στην περίοδο αντίδρασης, οι μολυσμένοι υπολογιστές γίνονται ανιχνευμένοι σε ένα ποσοστό μ και ο αφαιρούμενος έπειτα σε ένα ποσοστό δ.

Η κατάσταση D αντιπροσωπεύει την περίοδο όπου ο μολυσμένος υπολογιστής αποκαθίσταται από ένα τεχνικό (ή με άλλα μέσα). Ο συνυπολογισμός αυτού του σταδίου είναι ένα κατάλληλο χαρακτηριστικό του προτύπου PSIDR, το οποίο δεν αναφέρεται σε άλλα πρότυπα.

Σημαντική είναι η επισήμανση ότι τα παραδοσιακά μοντέλα SIS, SIR και το πρότυπο SEIR δεν λαμβάνουν υπόψη τους τις τρεις προαναφερθείσες πτυχές στον απολογισμό.

Στο πρότυπο PSIDR, το επιδημικό γεγονός διαμορφώνεται έτσι σαν ένα S-I σύστημα που γίνεται μετά από χρόνο t=π, ένα S-I-D-R σύστημα με πιθανές μεταβάσεις του τύπου S-R.

Ο λόγος για τον οποίο το πρότυπο καλείται προοδευτικό είναι τώρα σαφής: Είναι λόγω της προόδου (ή της αλλαγής) στη δυναμική του συστήματος.

7.3 ΕΚΤΙΜΗΣΗ ΚΟΣΤΟΥΣ

Ένα πλεονέκτημα του τρέχοντος προτύπου είναι ότι προτείνει ένα φυσικό και αποδοτικό τρόπο εκτίμησης διαφόρων ειδών κόστους σχετιζόμενων με το επιδημικό γεγονός.

Κόστος αποκατάστασης. Το κόστος που σχετίζεται με την αποκατάσταση των υπολογιστών συσχετίζεται και με το χρονικό διάστημα που χρειάζεται για να καθαριστούν οι υπολογιστές καθώς και με το πλήθος αυτόν (δηλαδή το πλήθος των μολυσμένων υπολογιστών που έχουν ανιχνευθεί). Επομένως, αυτό το κόστος μετράται ως το ποσό του αριθμού των ανιχνευμένων υπολογιστών για κάθε χρονική στιγμή .

Κόστος διανομής. Αντιπροσωπεύει το ποσό του δικτύου που επηρεάστηκε σε όλο το ξέσπασμα. Είναι ένα σύνθετο μέτρο του πόσοι υπολογιστές είναι μολυσμένοι και για πόσο καιρό είναι μολυσμένοι. Αποτυπώνονται έτσι πολλές πληροφορίες για το κόστος του ξεσπάσματος. Ομοίως με το κόστος αποκατάστασης, το κόστος διανομής δίνεται από τον τύπο:

$$\text{Κόστος διανομής} = \int I(t)dt \approx \Sigma I(t)$$

Μέγιστος αριθμός μολυσμένων κόμβων. Αυτό είναι επίσης μια ενδιαφέρουσα μεταβλητή δεδομένου ότι δίνει μια ιδέα για τη χειρότερη κατάσταση του συστήματος. Πράγματι, η διάσπαση μπορεί να παραγάγει παρόμοιες τιμές για τα πολύ διαφορετικά επιδημικά γεγονότα, όπου ο μέγιστος αριθμός μολυσμένων κόμβων μπορεί να διαφοροποιηθεί περισσότερο μεταξύ των τύπων των γεγονότων και άρα: .

$$\text{Πλήθος μολυσμένων κόμβων} = \max(I(t))$$

Χρονική διάρκεια μέχρι την ανοσοποίηση. Τα πραγματικά δίκτυα είναι σπάνια και εντελώς ανοσοποιημένα αλλά μπορούν να γίνουν συνήθως άνοσα κυρίως σε ένα σκουλήκι. Κατά συνέπεια, ο χρόνος που μεσολαβεί για να ανοσοποιηθεί το 95% των υπολογιστών του δικτύου υπολογίζεται αντί αυτού: αυτό το επίπεδο το (95%) επιλέγεται κάπως αυθαίρετα με σχέση και τα επίπεδα 90% ή 99% που θα μπορούσαν επίσης να έχουν επιλεχτεί. Μπορεί να είναι συμφέρων να ανοσοποιηθεί το δίκτυο όσο το δυνατόν γρηγορότερα για αυτό και να αποτρέπει οποιοδήποτε

μεγάλο ξέσπασμα. Ο χρόνος που χρειάζεται για την πλήρη ανοσοποίηση μετράται σε συνάρτηση των παραμέτρων διαμόρφωσης.

Εκτός από τη μέτρηση των παραδοσιακών ποσοτήτων, όπως είναι ο αριθμός των ευπαθών ή και το πλήθος των μολυσμένων κόμβων σε κάθε χρονική στιγμή, αυτά τα τέσσερα σε σειρά κόστη μπορούν να μετρηθούν και να χρησιμοποιηθούν για την πρόταση των καλύτερων στρατηγικών αντίδρασης.

Τα πρότυπα SIS, SIR ή SEIR δεν παρέχουν οποιαδήποτε ένδειξη σχετικά με τον καθορισμό του κόστους.

7. 4 ΠΕΡΙΟΡΙΣΜΟΙ ΤΟΥ ΜΟΝΤΕΛΟΥ

Το πρότυπο PSIDR επεκτείνει τα προηγούμενα πρότυπα για να προσφέρει έναν καλύτερο απολογισμό των τεχνολογικών επιδημιών. Εντούτοις, εδώ παρουσιάζονται μερικές πτυχές που δεν υπολογίζει.

1) Μεταβλητότητα του ρυθμού θεραπείας δ. Στην πραγματικότητα, όσο περισσότεροι μολυσμένοι υπολογιστές υπάρχουν τόσο περισσότεροι άνθρωποι ανατίθενται για την καταπολέμησή του. Δηλαδή $\delta \infty I$ (όπου είναι πιθανό να επηρεάσει το χρόνο που απαιτείται για να την απομάκρυνση του ιού). Η ακριβής σχέση μεταξύ του I και δ μπορεί να είναι γραμμική ή μη γραμμική. Το πρότυπο PSDIR μπορεί εύκολα να επεκταθεί με ένα μεταβλητό ρυθμό θεραπείας.
2) Μεταβλητότητα του ρυθμού γεννήσεων β. Στην περίπτωση των αυτόματα μεταδιδόμενων σκουληκιών, ο ρυθμός διάδοσης καθορίζεται εν μέρη από το πόσο γρήγορα το σκουλήκι θα εξετάσει τη νέα διεύθυνση IP. Παραδείγματος χάρι, στην περίπτωση του Codered, το σκουλήκι ήταν προγραμματισμένο να σταματήσει να ψάχνει νέους οικοδεσπότες τα μεσάνυχτα της 20ης Ιουλίου. Άλλα σκουλήκια είχαν επίσης αυτό το χαρακτηριστικό προκαλώντας έτσι μεταβλητότητα του ρυθμού γεννήσεων.
3) Άλλοι περιοδικοί παράγοντες. Μερικά σκουλήκια επιφέρουν ζημιές περιοδικά. Για παράδειγμα, το σκουλήκι Klez.e προκαλούσε καταστροφές μόνο σε μολυσμένους υπολογιστές την 6η μέρα κάθε μονού μήνα π.χ. (Ιανουάριος, Μάρτιος,κτλ.)

7.5 ΠΡΟΣΟΜΟΙΩΣΗ

Αυτό το κεφάλαιο εκθέτει τα διάφορα πειράματα προσομοίωσης που γίνονται με το PSIDR πρότυπο. Ας ανακεφαλαιώσουμε όμως την αλυσίδα των γεγονότων που περιλαμβάνονται στο πρότυπο PSIDR.

Περίοδος προ αντίδρασης (S- >I). Στην αρχή, ένα σκουλήκι μολύνει μια μηχανή στο δίκτυο. Για τις επόμενες μερικές ημέρες (ή ώρες), το σκουλήκι διαδίδεται ελεύθερα στο δίκτυο χωρίς την παρατήρηση του από τους περισσότερους χρήστες.

Περίοδος αντίδρασης (S-I-D-R,S-R). Μετά από κάποιο χρόνο, το σκουλήκι ανιχνεύεται σε μερικούς υπολογιστές και έτσι λαμβάνεται άμεση δράση για την αποτροπή της περαιτέρω εξάπλωσης καθώς και για την θεραπεία των μολυσμένων υπολογιστών. Κατόπιν δημιουργείτε μια υπογραφή σκουληκιών και περιλαμβάνεται σε ένα ορισμένο ποσοστό του πλήθους στο δίκτυο. Υπολογιστές που δεν ήταν μολυσμένοι γίνονται αυτόματα άνοσοι στο σκουλήκι, ενώ οι μολυσμένοι υπολογιστές ανιχνεύονται σε ένα ορισμένο ποσοστό. Αυτές οι μηχανές έπειτα απομονώνονται καθαρίζονται και ανοσοποιούνται ενάντια στη περαιτέρω μόλυνση.

Το PSIDR πρότυπο περιέχει πολλές ελεύθερες παραμέτρους, οδηγώντας έτσι σε πολλές διαφορετικές παραμετροποιήσεις που μπορούν να δοκιμαστούν προκειμένου να επιτευχθεί μια επαρκής κατανόηση του προτύπου.

Εδώ μόνο ένα υποσύνολο των τιμών εξερευνάται για να παρουσιαστεί η βασική δυναμική του προτύπου. Το πρώτο σύνολο των πειραμάτων προορίζεται για να δώσει μια γενική επισκόπηση του προτύπου.

Ο χρόνος που μεσολαβεί μέχρι την αρχική ανίχνευση (π) τίθεται σε διαφορετικές τιμές για την παρουσίαση της επίδρασης αυτού του παράγοντα.

Στο δεύτερο μέρος, οι τιμές για διαφορετικές παραμέτρους όπως ο χρόνος που μεσολαβεί μέχρι την αρχική ανίχνευση (π), ο ρυθμός ανίχνευσης και ανοσοποίησης (μ), και ο ρυθμός θεραπείας (δ) ποικίλουν μεταξύ των προσομοιώσεων.

Η έμφαση δίνεται στην αλληλεπίδραση της ανάμειξης του π και μ, π και δ, και μ και δ παραμέτρων.

Οι τρέχων στρατηγικές για να την αντιμετώπιση των ιών μοντελοποιούνται με αυτές τις παραμέτρους, και ένας από τους κύριους στόχους είναι η αξιολόγηση της αποδοτικότητας αυτών των μεθόδων.

Ένας νέος τρόπος να αντιμετωπιστούν οι επιδημίες είναι να επιβραδυνθεί η διάδοση των ιών [87]. Στο παρόν πλαίσιο, αυτή η στρατηγική μπορεί να εξεταστεί με τη μίμηση πιο αργών ποσοστών γέννησης (β).

Ένα τρίτο σύνολο πειραμάτων ερευνά αυτό το ζήτημα. Μία κατάλληλη μελέτη αυτής της επίδρασης πρέπει να περιλαμβάνει τις προσομοιώσεις των αλληλεπιδράσεων μεταξύ του β και των παραμέτρων π δ, και μ.

Τέλος, συγκρίνεται το SIR πρότυπο με το PSIDR πρότυπο όταν π = 0 με στόχο να παρουσιαστεί η επιρροή των άμεσων μεταβάσεων από το S στο R. (ένα από τα κύρια χαρακτηριστικά γνωρίσματα του PSIDR προτύπου).

Αντίθετα από το SIS πρότυπο, η προσοχή δεν εστιάζεται ρητά στην ύπαρξη ενός πιθανού επιδημιολογικού κατώτατου ορίου.

7.6 ΕΚΤΙΜΗΣΗ ΤΩΝ ΠΑΡΑΜΕΤΡΩΝ

Αντί του υπολογισμού των συγκεκριμένων τιμών για κάθε μια από τις παραμέτρους β δ, μ και π, οι τιμές τους προσεγγίζονται με τον ακόλουθο τρόπο.

1. **Ρυθμός εξάπλωσης**. Δεδομένου ότι τα σκουλήκια διαδίδονται αρκετά γρηγορότερα από ότι ανιχνεύονται ή αφαιρούνται, η τιμή του β πρέπει να είναι υψηλότερη από την ανίχνευση (μ) και του ρυθμού θεραπείας (δ).
2. **Χρόνος αντίδρασης.** Ο αριθμός των χρονικών βημάτων πριν από μια αρχική ανίχνευση (π), δεν περιορίζεται από οποιαδήποτε από τις άλλες παραμέτρους. Κατά συνέπεια και οι τιμές στο διάστημα 0≤π ≤ 20 και επίσης π= 40 χρησιμοποιούνται για την παροχή μιας γενικής εκτίμησης της επίδρασης αυτής της παραμέτρου.
3. **Ρυθμός ανίχνευσης.** Η τιμή του ρυθμού ανίχνευσης είναι μεταξύ του ρυθμού γέννησης και θεραπείας εξαιτίας του γεγονότος ότι είναι μερικώς αυτοματοποιημένος.
4. **Ρυθμός θεραπείας**. Επειδή η θεραπεία απαιτεί τη χειρωνακτική εργασία, είναι μάλλον αργή: Η θεραπεία μερικών ντουζινών υπολογιστών μπορεί να διαρκέσει και ημέρες.

7.7 ΒΕΛΤΙΣΤΕΣ ΣΤΡΑΤΗΓΙΚΕΣ ΕΛΕΓΧΟΥ

Γενικά, είναι προτιμότερο να διατηρείτε ο χρόνος απόκρισης (π) όσο το δυνατόν χαμηλότερος. Αυτό συνεπάγεται ότι οι πρώτες περιπτώσεις δράσης ενός σκουληκιού πρέπει να ανιχνευθούν πραγματικά γρήγορα και να εξαχθεί η υπογραφή του ιού σε πολύ σύντομο χρονικό διάστημα.

Αυτοματοποιημένα συστήματα ασφάλειας είναι ενδεδειγμένα δεδομένου ότι η ταχύτητα δράσης τους σε αυτήν την φάση είναι πολύ μεγαλύτερη από τη χειρωνακτική εργασία.

Εάν το κόστος επισκευής είναι η κύρια ανησυχία, η αύξηση του ρυθμού θεραπείας δ θα το μειώσει αρκετά. Μια αυτοματοποιημένη διαδικασία επιδιόρθωσης θα ήταν πολύ χρήσιμη να μειώσει αυτό το κόστος.

Εάν το κόστος επιβράδυνσης είναι το σημαντικότερο, τότε ο ρυθμός ανίχνευσης (μ) θα πρέπει να αυξηθεί. Δηλαδή το αντιϊκό θα πρέπει να διανεμηθεί γρηγορότερα. Η προσπάθεια να ανοσοποιηθούν οι υπολογιστές που παρουσιάζουν υψηλή συνδεσιμότητα μπορεί επίσης να βοηθήσει στην μείωση της επικράτησης.

Ο χρόνος για την ανοσοποίηση επηρεάζεται από όλους τους παράγοντες ελέγχου π μ και δ δεδομένου ότι συλλαμβάνει την εξέλιξη της ποσότητας των μηχανισμών στο στάδιο της αφαίρεσης. Επομένως, επηρεάζεται από ότι συμβαίνει σε όλες τις προηγούμενες φάσεις (ευπαθής μολυσμένος και ανιχνευμένος).

Οποιαδήποτε βελτίωση στις στρατηγικές ελέγχου θα δημιουργήσει επίδραση στο χρόνο για ανοσοποίηση.

ΚΕΦΑΛΑΙΟ 8

8.1 ΣΥΜΠΕΡΑΣΜΑΤΑ

Λαμβάνοντας υπόψη την εξάρτηση των περισσότερων σύγχρονων κοινωνιών από διάφορες ψηφιακές υποδομές, η ταχεία εξάπλωση του κακόβουλου λογισμικού αποτελεί σημαντικό πρόβλημα. Η ανάπτυξη αλγορίθμων για την βελτίωση της αποτελεσματικότητας των αντιϊοικών προγραμμάτων και των Συστημάτων Ανιχνεύσεως Εισβολέων (Intrusion Detection Systems) είναι χρήσιμη, αλλά όχι και αρκετή για το περιορισμό της ταχείας εξάπλωσης κακόβουλου λογισμικού. Η μικροσκοπική ανάλυση είναι ιδανική για την προστασία μεμονωμένων συστημάτων ή για τον καθαρισμό τους, αν έχουν ήδη μολυνθεί από κάποιο είδος κακόβουλου λογισμικού.

Από την άλλη πλευρά, για την προστασία διαφόρων κρίσιμων τεχνολογικών υποδομών, όπως τα τηλεπικοινωνιακά και πληροφοριακά συστήματα, καθώς και τα συστήματα ελέγχου, απαιτείται μια γενικότερη στρατηγική προσέγγιση. Στην Ιατρική οι μικροβιολόγοι εργάζονται παράλληλα με τους επιδημιολόγους για την έγκαιρη αναγνώριση νέων απειλών, ώστε να προσφέρουν τη βέλτιστη δυνατή προστασία στον ευπαθή πληθυσμό. Σε θέματα επιδημιολογίας υπολογιστών παρόμοιες συνέργειες θα πρέπει να αναπτυχθούν για την προστασία των ψηφιακών υποδομών.

Το πρώτο βήμα για το σχεδιασμό αποτελεσματικών περιοριστικών μέτρων στην εξάπλωση του κακόβουλου λογισμικού είναι η πλήρης και βαθιά κατανόηση του τρόπου και των προτύπων διάδοσης του. Η εφαρμογή επιδημιολογικών μοντέλων στις διάφορες μορφές κακόβουλου λογισμικού μπορεί να περιγράψει με ικανοποιητική ακρίβεια την εξάπλωση του.

Όπως έχει ήδη επισημανθεί, τα μοντέλα αυτά μπορούν να είναι είτε σύνθετα είτε απλά [67]. Τα σύνθετα μοντέλα έχουν το πλεονέκτημα των ρεαλιστικών περιπτώσεων δοκιμής και της παροχής ακριβέστερων προβλέψεων. Εντούτοις, τα απλούστερα μοντέλα μπορούν να οδηγήσουν σε βαθύτερη γνώση και κατανόηση κάτι το οποίο είναι δυσκολότερο να γίνει με ένα σύνθετο πρότυπο.

Παρόλα ταύτα, υπάρχει μία αύξηση της εστίασης στα πρότυπα όπως το SIS, SIR, SEIR.Το πρότυπο PSIDR δείχνει ότι τα πιο σύνθετα πρότυπα μπορούν εύκολα να χτιστούν και να αναλυθούν λεπτομερώς για να παρέχουν καλύτερο χαρακτηρισμό των πραγματικών επιδημιών. Σαν αντάλλαγμα, τα αποτελέσματα για το πρότυπο

PSIDR δίνουν μια καλύτερη κατανόηση των μηχανισμών που θα οδηγήσουν σε έναν αποδοτικό έλεγχο των επιθέσεων από ιούς.

8.2 ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

Ακολουθεί μία λίστα κατευθύνσεων που χρίζουν περεταίρω διερεύνησης

1. Διαφορετικά μεγέθη δικτύων. Οι συγκρίσεις με τα μεγαλύτερα δίκτυα είναι χρήσιμες για την μελέτη των αποτελεσμάτων καθώς και των ιδιοτήτων των διαφορετικών τοπολογιών (κατηγοριών δικτύων). Οι διαφορικές εξισώσεις του Γενικού Επιδημιολογικού Μοντέλου ισχύουν όταν τα εξεταζόμενα συστήματα συνδέονται μεταξύ τους σχηματίζοντας ένα ομογενή γράφο. Σε άλλες τοπολογίες η καμπύλη του ρυθμού εξάπλωσης, παρότι διατηρεί την ίδια μορφή, απαιτεί περισσότερο χρόνο για να προσεγγίσει τα ίδια ποσοστά εξάπλωσης.
2. Δημιουργία μοντέλων που να υποστηρίζουν δίκτυα μεταβλητού μεγέθους όπου θα μπορούν να προσομοιώνουν διαφορετικά μοντέλα διάδοσης του ιού με μεταβλητούς ρυθμούς διάδοσης τόσο της μόλυνσης όσο και της ανίχνευσης αλλά και της θεραπείας.

3. Χρήση διαφορετικών μοντέλων διάδοσης αντιιών. Σε ομογενή δίκτυα ένας αποτελεσματικός μηχανισμός καταστολής της διάδοσης των επιδημιών είναι η θεραπεία τυχαίων κόμβων στο δίκτυο [68]. Ωστόσο η μέθοδος αυτή είναι ανεπαρκής για δίκτυα ελεύθερης κλίμακας λόγω της ύπαρξης κόμβων με υψηλή συνδεσιμότητα. Μία ιδέα που ξεκίνησε από τον Kephart είναι να διαδίδεται η υπογραφή των ιών με τον ίδιο τρόπο που ο ιός διαδίδει στο δίκτυο [73]. Η υπογραφή θα συγχεόταν στον υπολογιστή που άρχισε η μόλυνση και έπειτα θα αφηνόταν να διαδοθεί στους γειτονικούς υπολογιστές. Αυτή η στρατηγική θα είχε το πλεονέκτημα της επίθεσης του ξεσπάσματος στον πυρήνα του.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Murray, J. D. Mathematical Biology, (2nd, corrected edition). Springer Verlag, New York, 1993
2. Kephart, J. Chess, D and White, S. Computers and epidemiology. IEEE Spectrum, 1993.
3. Ludwig, M. Computer Viruses Artificial Life and Evolution , 1993
4. Watts, S. Epidemics and History. Yale University Press,1999
5. Graunt, J. Natural and political Observations made upon the Bills of Mortality. John Martyn, London, 1662.
6. Kermack, W. and McKendrick, A.. A contribution to the mathematical theory of epidemics. Proc. Roy. Soc. Lond., 1927.
7. Allman, E. and Rhodes, J. Mathematical Models in Biology. Cambridge University Press, 2004.
8. Boguna, M and PastorSatorras, R. Exciting spreading in correlated complex networks. Physical Review E, 2002
9. Daley, D. and Gani, J., Epidemic Modelling. Cambridge University Press, 1999.
10. Hethcote, H. The mathematics of infectious diseases. SIAM Review, 2000.
11. Trichopoulos, D..Epidemiology, principles, methods. Scientific Publications Gr. Parisianos, 1982
12. Kephart, J and White, S. Measuring and modeling computer virus prevalence. In Proceedings of the 1999 IEEE Computer Society Symposium on Research in Security and Privacy, 1999.
13. Kephart, J. How topology affects population dynamics. In Proceedings of Artificial Life 3, N EW Mexico, USA, June 1992.
14. Kephart, J. and White, S. Directedgraph epidemiological models of computer viruses. In Proceedings of the 1991 Computer Society Symposium on Research in Security and Privacy, 1991.
15. eEye Digital Security. Code Red II Worm analysis AL 20010804, 2004
16. Leveille, J. 2002 Epidemic spreading in technological networks. Master's thesis, University of Sussex. 2002

17. Moore, D. and Shannon, C. The spread of the codered worm (crv2), 2005
18. Zoo, C. Gong, W. and Towsley, D. Code red worm propagation modeling and analysis. In Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS),Washington DC, USA, 2002
19. Staniford, S. Paxson, V. and Weaver, N. How to 0wn the internet in your spare time. In Proceedings of the 11th USENIX Security Symposium, 2002
20. MILLER, P. and CUMMINS, M.: LAN Technologies Explained, Woburn, MA: Butterworth-Heinemann, 2000.
21. Anderson James P., " Computer Security Threat Monitoring and Surveillance", 1980
22. Gritzalis S. and Spinellis D. Addressing threats and security issues in World Wide Web technology. In Proceeding CMS '97 3rd IFIP TC6/TC11 International joint working Conference on Communications and Multimedia Security, Chapman &Hall, 1997
23. Veiler, R. Professional Rootkits, 2007
24. Κομνηνός Θεόδωρος, Σπυράκης Παύλος, Ασφάλεια δικτύων και Υπολογιστικών Συστημάτων, Ελληνικά Γράμματα, 2002
25. Bellovin, S. Firewall- friendly FTP. RFC 1579, Internet Engineering Task Force, 1994
26. Vacca, J. Internet Security: Secrets , IDG Books Wolrdwide, 1996
27. Erbschloe, M. Trojans, worms and spyware. A computer security professional´s guide to malicious code. Elsevier Butterworth-Heineman, Oxford UK, 2005
28. Pfleeger, C. Security in Computing. PrenticeHall, Inc, Upper Saddle, NJ, USA, 1997
29. Daniel , B Couto, J., Jajodia , S., Popyack, L ., and Ningning, W. "ADAM : Detecting Intrusions by Data Mining," Proceedings of the IEEE Workshop on Information Assurance and Security, 2001
30. Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr Everett F, (Skip), Jr., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit", 2007
31. Doraswamy, N. Harkins, D. "IPSec", 2003

32. Gaynor M. and Brander, S. Firewall enhancement protocol (FEP). (RFP). REC 3093, Internet Engineering Task Force, April 2001
33. Mayer, A. Wool, A. and Ziskind, E. : A firewall analysis engine. In Proceedings of the IEEE Computer Society Symposium on Security and Privacy, 2000
34. Cheswick, W. Bellovin, S. and Rubin, A. Firewalls and Internet Security; Repelling the Wily Hacker. Addison-Wesley, Reading, MA, 2003.
35. Jose Vilches, TechSpot.com, The rise of the rootkits has begun, dec 2007 http://www.techspot.com/news/28244-prevx-the-rise-of-the-rootkits-has-begun.html
36. Altholz, N. and Stevenson , L. Rootkits for Dummies 2006
37. Hoglund, G. and Butler, J. Rootkits: Subverting the Windows Kernel ,2005
38. Cohen, F. A Short Course on Computer Viruses. Wiley Professional Computing. Wiley, Canada, 1994
39. Skoudis, E. Malware, Fighting Malicious Code. Computer Networking and Distributed Systems. Prentice Hall, NJ, USA, sixth edition, 2004.
40. Lin, D “Inexpensive boot sector virus detection and prevention techniques”, 2000
41. Shoch, J. and Hupp, J. The”worm” programs-early experience with a distributed computation.
42. Szor P. and Ferrie, P. Hunting for metamorphic. In Proceedings of the Virus Bulleting Conference, 2001.
43. Arce, I. and Levy, E. An analysis of the slapper worm. IEEE Security & Privacy, 2003
44. Axelsson, S. Visualisation for intrusion detection hooking the worm. In Proceedings of the 8th European Symposium on Research in computer Security. SpringerVerlag, 2003
45. Bailey, M. Cooke, E. Jahanian, F. Watson, D. and Nazario, J. The blaster worm: Then and now, IEEE Security & Privacy, 2005.
46. Spafford, E. The internet worm program: an analysis, 1989
47. Pfleeger , S. and Bloom , G. Canning spam: Proposed solution to unwanted e-mail,
48. Ecker, Clint. Massive spyware-based identity theft ring uncovered. 2005

49. Erbschloe, M. Trojans, worms and spyware. A computer security professional´s guide to malicious code. Elsevier Butterworth- Heineman, Oxford UK, 2005
50. Hower, Eric L. “The Spyware Warrior List of Rogue / Suspect Anti-Spyware Products & Web Sites”, 2005
51. Roberts, Paul F. ”Spyware-Removal Program Tagged as a Trap, 2005
52. Staniford, S. Moore, D. Paxson, V and Weaver, N. The top speed of flash worms In WORM ’04: Proceedings of the 2004 ACM workshop on Rapid malcode, 2004
53. Weaver, N. Paxson, V, and Staniford, S. A worstcase worm. In Proceedings of the Third Annual Workshop on Economics and Information Security, 2004.
54. Leveille, J. Epidemic spreading in technological networks. Hpl2002287, School of Cognitive and Computing Sciences, University of Sussex at Brighton, Bristol, 2002
55. PastorSatorras, R and Vespignani, A. Epidemic spreading in scalefree networks. Physical Review Letters, 2001.
56. Coggon, Rose, and Barker. Epidemiology for the Uninitiated, Chapter 8, “Case –control and cross-sectional studies” , BMJ(British Medical Journal) Publishing, 1997
57. Pildal J, Chan AW, et al. “Comparison of descriptions of allocation concealment in trial protocols and the publihed report: cohort study”, 2005
58. Vandenbroucke, J. In defense of case reports and case series. Ann Intern Med, 2001
59. Kuzntson, Y. and Piccardi, C. Bifurcation analysis of periodic SEIR and SIR epidemic models, Journal of Mathematical biology 1994.
60. Onofrio, A. Manfredi, P. and Salinelli. E. ‘Vaccinating behaviour, information, and the dynamics of SIR vaccine preventable diseases’ Th. Pop. Biol 2007.
61. Bailey, N. The Mathematical Theory of Infectious Diseases (2nd edition Charles Griffin and co. Ltd 1975.
62. Capasso, V. The Mathematical Structure of Epideic Systems; Springer Verlag 1993.
63. Kermack, O McKendrick. A “A Contribution to the Mathematical Theory of Epidemics, 2000

64. Boguna, M. Pastor-Satorras, R Vespignani, A.. Epidemic spreading in complex networks with degree correlations. Statistical Mechanics of complex Networks, 2003
65. Bonfante, G. Kaczmarek, M. and Marion, J. On abstract computer virology from a recursion theoretic perspective. Journal in Computer Virology 2006.
66. Weiss, G. Dishon, M. On the anymptotic behavior of the stochastic and deterministic models of an epidemic.
67. Billings, L. and Schwartz, I. B.. Exciting chaos with noise: unexpected dynamics in epidemic outbreaks. Journal of Mathematical Biology, 2002.
68. Barthelemy, M. Barrat, A Pastor-Satorras, R. and Vespignani, A. Dynamical patterns of epidemic outbreaks in complex heterogeneous network. Journal of Theoretical Biology, 2005.
69. Kempe, D Kleinberg, J. and Tardos, E.. Maximizing the spread of influence through a social network 2003.
70. Pastor R. –Satorras and Vespignani, A.. Epidemics and immunization in scale-free networks. Handbook of Graphs and Networks: From the Genome to the Internet, 2002
71. Cohen, R. Havlin, S. and populations. Phys Rev Lett., 2003.
72. Allen, Julia H. The CERT Guide to System and Network Security Practices,2001
73. Kephart, J. A biologically inspired immune system for computer. In Rodney A. Brooks and Pattie Maes, editors, Artificial Life IV: Proceeding of the Fourth International Workshop on the Synthesis and Simulation of Living Systems, 1994.
74. Onofrio, A. Manfredi, P. and E. Salinelli “Vaccinating behaviour, information and the Dynamics of SIR vacinne preventable diseases” 2007

http://en.wikipedia.org/wiki/Epidemic_model
http://ben-israel.rutgers.edu/711/structure-epidemics.pdf
http://en.wikipedia.org/wiki/Compartmental_models_in_epidemiology
http://www.fordham.edu/images/undergraduate/economics/faculty/si-sis.pdf
http://en.wikipedia.org/wiki/John_Snow_(physician)
http://www.vmsweb.net/attachments/Taming-Lakatos.pdf
http://support.microsoft.com/kb/129972
http://nemertes.lis.upatras.gr/dspace/bitstream/123456789/1594/1/Ergasia
http://www.microsoft.com/hellas/protect/computer/viruses/antivirus.mspx
http://di.ionio.gr/~emagos/Security/Simeioseis-Asfaleia%20Part%20B.pdf