Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλειας Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Μελέτη Ανίχνευσης Δημιουργίας και Αντιμετώπισης των Hoax Email

Νικόλαος Παπαπολύζος

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Νοέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλειας Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Μελέτη Ανίχνευσης Δημιουργίας και Αντιμετώπισης των Hoax Email

Νικόλαος Παπαπολύζος

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια και Προστασία Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Νοέμβριος 2019

Περίληψη

Τα Hoax Emails είναι μηνύματα απάτης ηλεκτρονικού ταχυδρομείου που αποστέλλονται από εγκληματίες του κυβερνοχώρου με σκοπό να εξαπατήσουν ανυποψίαστους χρήστες. Χρήστες του διαδικτύου που έχουν γίνει θύματα από επιθέσεις των hoax email , μπορεί να αποκαλύψουν ευαίσθητα δεδομένα τους , όπου αυτό μπορεί να προκαλέσει υποκλοπή προσωπικών δεδομένων , διαδικτυακό εκβιασμό ή ακόμα και υποκλοπή μεγάλων χρηματικών ποσών.

Με εκτιμώμενη ζημία 3,86 εκατομμυρίων δολαρίων για το έτος 2019 τα ηλεκτρονικά μηνύματα hoax αποτελούν σημαντική απειλή για το τοπίο της ασφάλειας στον κυβερνοχώρο (Retruster LTD, 2019).

Για να αντιμετωπιστεί το πρόβλημα, οι ερευνητές και οι εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο προσπαθούν να δημιουργήσουν αυτοματοποιημένα συστήματα φιλτραρίσματος προκειμένου να ανιχνεύσουν και να αφαιρέσουν τα μηνύματα ηλεκτρονικού ταχυδρομείου πριν φτάσουν στα θύματά τους. Ως απάντηση, οι κυβερνοεγκληματίες χρησιμοποιούν μια ποικιλία εξελιγμένων μεθόδων και τεχνικών ώστε να κάνουν τα ηλεκτρονικά τους μηνύματα εξαπάτησης , να διακρίνονται ως νόμιμα μηνύματα ιστού. Κατά συνέπεια, τα εξαιρετικά πειστικά ηλεκτρονικά μηνύματα μπορούν να παρακάμψουν τα υπάρχοντα συστήματα φιλτραρίσματος, στοχεύοντας χρήστες του διαδικτύου με καταστροφικές συνέπειες.

Η αποτελεσματική ανίχνευση μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ένα ανεπίλυτο πρόβλημα μεγάλης σημασίας και το ερευνητικό ερώτημα που τίθεται είναι εάν μπορούμε να δημιουργήσουμε έναν αλγόριθμο εντοπισμού των hoax email. Συνεπώς η μεταπτυχιακή διατριβή εστιάζει στην ανίχνευση και αντιμετώπιση των hoax email, με χρήση αλγορίθμου αυτόματου εντοπισμού σύμφωνα με τα λεκτικά χαρακτηριστικά. Ο τρόπος της λειτουργίας του αλγορίθμου βασίζεται στον εντοπισμό και στην αναγνώριση , των υψηλής συχνότητας εμφανιζόμενων λέξεων απο hoax email. Για την λειτουργία του αλγορίθμου χρησιμοποιήθηκαν απο το διαδίκτυο, δύο λίστες λέξεων. Η πρώτη λίστα περιείχε hoax λέξεις (Badwords.txt) ενώ η δεύτερη stopwords, δηλαδή απλές λέξεις (Whitelist.txt). Επίσης χρησιμοποιήθηκαν απο το διαδίκτυο τρία e-mail Dataset, εκ των οποίων το ένα απο αυτά περιελάμβανε clean emails (Clean.txt) ενώ τα άλλα 2 (Fraud1.txt & Fraud2.txt) hoax emails. Ο αλγόριθμος δημιουργεί μία λίστα DirtyWords, η οποία εντοπίζει ύποπτες λέξεις “hoax” στα παραπάνω Dataset της οποίας τα αποτελέσματα συγκρίνονται με αυτά της λίστας Badword ώστε να ελεγχθεί η απόδοση της DirtyWords.

Η υλοποίηση του αλγορίθμου πραγματοποιήθηκε σε περιβάλλον προσομοίωσης με χρήση γλώσσας προγραμματισμού Python3.7.

Για την αξιολόγηση του συστήματος, πραγματοποιήθηκε σύγκριση, χρησιμοποιώντας τα δεδομένα που προκύπτουν απο τη λίστα Badwords με τα δεδομένα που προκύπτουν απο την λίστα του δημιουργηθέντος συστήματος DirtyWords, στην οποία περιέχονται συχνά εμφανιζόμενες λέξεις απο hoax email. Τα αποτελέσματα των πειραμάτων με τη μέθοδο του αλγορίθμου υποδεικνύουν λιγότερα false negatives με περισσότερα true positives, καθώς το σύστημα που κατασκευάστηκε DirtyWords έχει κατά μέσο όρο 33% υψηλότερο ποσοστό ακρίβειας, στον εντοπισμό ενός Hoax email, απο ότι της λίστας Badwords που χρησιμοποιήθηκε απο το διαδίκτυο για τους ελέγχους. Αυτό σημαίνει ότι για ένα Hoax email που θα εισέλθει στο σύστημα, η πιθανότητα να μην αναγνωριστεί ως "hoax" είναι μικρότερη αντί της Badwords λίστας. Αντίστοιχα, όσο αφορά τον εντοπισμό ενός Clean email, το σύστημα παρουσίασε 1,2% μικρότερο ποσοστό λάθους σε σχέση με την λίστα Badword. Αξίζει να σημειωθεί πως αν και οι δύο λίστες είναι αρκετά επαρκείς στον εντοπισμό των clean emails η λίστα του αλγορίθμου DirtyWords προσεγγίζει με μικρότερο ποσοστό λάθους τον εντοπισμό των clean emails αντί της λίστας Badwords, καθώς έχουμε λιγότερα false negatives. Η πιθανότητα να αναγνωρίσει η DirtyWords ένα clean email ως hoax, είναι μικρότερη αντί της λίστας Badwords. Βάση των ευρημάτων, μπορούμε να αποφανθούμε στο συμπέρασμα ότι το σύστημα το οποίο κατασκευάστηκε μπορεί να χρησιμοποιηθεί επιτυχώς, για την επίλυση του προβλήματος.

Η αποτελεσματική ανίχνευση μηνυμάτων ηλεκτρονικού ταχυδρομείου επηρεάζει το κόστος εξασφάλισης και υλοποίησης ενός ευρύτερου συστήματος ηλεκτρονικής ασφάλειας σε έναν οργανισμό και είναι καθοριστικής σημασίας (N. Sklavos 2006:15, P. Souras 2006:15). Αυτό συνεπάγεται ότι υπάρχουν συστήματα ηλεκτρονικής ασφάλειας ενός οργανισμού που δεν υποστηρίζουν παρόμοια τεχνική, λόγω των αυξημένων οικονομικών πόρων που απαιτούνται, από την προστασία που παρέχεται σε επίπεδο εφαρμογής. Από την άλλη παρόμοια τεχνική θα μπορούσε να είχε ευρεία χρήση σε σύγχρονες εφαρμογές και τεχνολογίες , όπως σε ασύρματες τεχνολογίες 4G (N. Sklavos 2013:58, A. Bikos 2013:58) ή στο IOT (Internet of Things) όπου υπάρχουν πολλά κενά ασφαλείας και ευπάθειες. (S. Zeadally 2019:6, A.K. Das 2019:6, N. Sklavos 2019:6) Μελλοντικά το παρόν σύστημα μπορεί να χρησιμοποιηθεί απο την ακαδημαϊκή κοινότητα ώστε οι επιστήμονες να αναπτύξουν πρακτικά, αποδοτικότερους αλγορίθμους δοκιμάζοντας διάφορους μεθόδους και τεχνικές οι οποίες θα συμβάλλουν στην αποτελεσματικότερη απόδοση του αλγορίθμου.

Summary

Hoax Emails are fraudulent messages which are sent by cybercriminals with the intent to deceive unsuspecting users. Users who are victimized by hoax emails may be tricked into revealing sensitive data with may result in identity theft, cyber extortion or even big financial frauds. With an estimated damage of 3.86 million US dollars for the year 2019, Hoax emails present a significant threat to the cyber security landscape (Retruster Ltd, 2019). To address the problem, researchers and cyber security experts strive to create automated filleting systems in order to detect and remove hoax emails before they reach their victims. As a response, cybercriminals utilize a variety of sophisticated methods and techniques in order to make their hoax emails indistinguishable from legitimate web messages. Consequently, highly convincing hoax emails can still bypass existing filtering systems and target users with catastrophic consequences. The effective detection of hoax emails is an unresolved problem of great significance and the research question that arises is whether we can build a hoax email tracking algorithm. Therefore, the master's thesis focuses on the detection and handling of hoax emails, using an automatic algorithm based on verbal features. The way the algorithm works is based on detection and identification of words which are frequently being used in hoax emails. Two word lists were used for the operation the algorithm. The first list contains “hoax” words (Badwords.txt) and the second "stopwords" clean words (Whitelist.txt). Additionally, three Dataset of e-mails were used, one of which included clean emails (Clean.txt) and the other 2 (Fraud1.txt & Fraud2.txt) hoax emails. The algorithm generates a DirtyWords list, which detects suspicious "hoax" words in the above Datasets whose results are compared with the Badwords list to check the performance of DirtyWords. The algorithm was implemented in a simulation environment using Python3.7 programming language. A comparison was made to evaluate the system, using the data from the Badwords list with the data from the created DirtyWords system, which contains frequently used words from hoax email. The results of the experiments of the algorithm show less false negatives with more true positives, as the system with was developed with the use of DirtyWords list has an average of 33% higher accuracy in detecting a Hoax email when compared to the Badwords list which is currently being used for internet for checks. This means that for a Hoax email which is inserted into the system, the probability of not being recognized as a "hoax" is lower in comparison to the Badwords list. Based on the findings, we can conclude that the system that was built can successfully be used to solve the problem. The effective detection of hoax emails, also affects the cost of securing and implementing a wider cybersecurity system in an organization and is crucial (N. Sklavos 2006: 15; P. Souras 2006: 15). This implies that there are cyber security systems in an organization that do not support such a technique, due to the increased financial resources required, from the protection provided by the application layer. On the other hand, such a technique could be widely used in modern applications and technologies, such as in 4G wireless technologies (N. Sklavos 2013: 58, A. Bikos 2013: 58), or in IOT (Internet of Things) where there are many security gaps and vulnerabilities. (S. Zeadally 2019: 6, AK Das 2019: 6, N. Sklavos 2019: 6) In the future, this system can be used by the academic community to

allow scientists to develop practical, efficient algorithms by testing various methods and techniques that will contribute to the more efficient performance of the algorithm.

Ευχαριστίες

Ευχαριστώ την οικογένειά μου δηλαδή τους φίλους και τα αδέλφια μου Άλκη , Άκη , Μαρία , Ανδριανή , Γιάννη , Γιώργο , Λευτέρη , Αγγελική , Φωτεινή , Φάνη , Γιώργο , Ελένη και Γιώργο, που με στήριξαν στη προσπάθειά μου και τους εύχομαι ολόψυχα πάντα να έχουν κάθε ευλογία και επιτυχία στη ζωή τους.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Τα μηνύματα απάτης ηλεκτρονικού ταχυδρομείου (Hoax Emails) είναι παραπλανητικά και αληθοφανή μηνύματα που αποστέλλονται απο κυβερνοεγκληματίες προς λογαριασμούς χρηστών ηλεκτρονικού ταχυδρομείου και αποτελούν μία σημαντική απειλή για το τοπίο της κυβερνοασφάλειας στο διαδίκτυο. Οι κυβερνοεγκληματίες κατά την σύνθεση και την αποστολή των hoax email , προς τους λογαριασμούς χρηστών , ακολουθούν διάφορους μεθόδους και τεχνικές ώστε τα μηνύματα αυτά , να μην ανιχνεύονται ως μηνύματα ηλεκτρονικής απάτης , απο τα συστήματα αναγνώρισης ή απο τους χρήστες ηλεκτρονικού ταχυδρομείου.

Η δυσκολία αναγνώρισης των μηνυμάτων απάτης στο διαδίκτυο αποτελεί και το μεγαλύτερο πρόβλημα όσο αφορά την αποτελεσματική αντιμετώπιση του φαινομένου. Ένα μη ανιχνεύσιμο hoax email μπορεί να υποβάλλει το χρήστη σε υποκλοπή των προσωπικών δεδομένων, παραβίαση του συστήματος , παραβίαση του λογαριασμού ηλεκτρονικού ταχυδρομείου , υποκλοπή μεγάλου χρηματικού ποσού. Η ζημία που αποφέρεται απο ένα hoax email , εκτός από ατομικό επίπεδο , κρίνεται και σε συλλογικό (ομάδα χρηστών ηλεκτρονικού ταχυδρομείου) που ανήκουν σε έναν οργανισμό ή μια εταιρεία και αποτελούν το εργατικό δυναμικό , όπου εκεί οι απώλειες δύναται να είναι ακόμη μεγαλύτερες.

Οι έλεγχοι τηλεμετρίας της Symantec για το έτος 2018 σύμφωνα με την έκθεση που δημοσιεύτηκε στο διαδίκτυο , ανέδειξε ότι οι υπάλληλοι οργανισμών ήταν πιο πιθανό να πληγούν από απειλές μέσω ηλεκτρονικού ταχυδρομείου συμπεριλαμβανομένων των ανεπιθύμητων μηνυμάτων (spam), του ηλεκτρονικού "ψαρέματος" (phishing) και του κακόβουλου κώδικα ηλεκτρονικού ταχυδρομείου (malware). Διαπιστώθηκε ακόμα , ότι τα επίπεδα ανεπιθύμητης αλληλογραφίας συνέχισαν να αυξάνονται το 2018, όπως έκαναν κάθε χρόνο από το 2015, με το 55% των μηνυμάτων ηλεκτρονικού ταχυδρομείου που ελήφθησαν το 2018 να κατηγοριοποιούνται ως ανεπιθύμητα. Αντίστοιχοι έλεγχοι τηλεμετρίας που πραγματοποιήθηκαν για το ίδιο έτος απο την Kaspersky Lab ανέδειξαν ότι το 30,01% των χρηστών υπολογιστή , είχε υποστεί μία τουλάχιστον διαδικτυακή επίθεση τύπου Malware κατά τη διάρκεια του έτους.

Λόγω της σημαντικότητας που χρήζει η ανίχνευση και η αντιμετώπιση των μηνυμάτων ηλεκτρονικής απάτης το ερευνητικό ερώτημα που προκύπτει , είναι αν μπορούμε να κατασκευάσουμε έναν αλγόριθμο εντοπισμού των hoax email.
Συνεπώς η μεταπτυχιακή διατριβή εστιάζει στην ανίχνευση και αντιμετώπιση των hoax email, με χρήση αλγορίθμου αυτόματου εντοπισμού σύμφωνα με τα λεκτικά χαρακτηριστικά. Η τρόπος λειτουργίας του αλγορίθμου βασίζεται στον εντοπισμό και στην αναγνώριση των υψηλής συχνότητας εμφανιζόμενων λέξεων των hoax email.
Για την λειτουργία του αλγορίθμου χρησιμοποιήθηκαν απο το διαδίκτυο , δύο λίστες

λέξεων. Η πρώτη λίστα περιείχε ύποπτες λέξεις hoax (Badwords.txt) ενώ η δεύτερη μη ύποπτες λέξεις (Whitelist.txt.). Επίσης χρησιμοποιήθηκαν απο το διαδίκτυο τρία πραγματικά e-mail Dataset , εκ των οποίων το ένα απο αυτά περιελάμβανε clean emails (Clean.txt) ενώ τα άλλα 2 (Fraud1.txt & Fraud2.txt) hoax emails.
Ο αλγόριθμος δημιουργεί μία λίστα DirtyWords[] , η οποία εντοπίζει ύποπτες λέξεις "hoax" στα παραπάνω Dataset του οποίου τα αποτελέσματα συγκρίνονται με τη λίστα Badword με στόχο τον έλεγχο της απόδοσης της DirtyWords[] λίστας.
Η υλοποίηση του αλγορίθμου πραγματοποιήθηκε σε περιβάλλον προσομοίωσης με τη χρήση γλώσσας προγραμματισμού Python 3.7.

Για την αξιολόγηση του συστήματος, πραγματοποιήθηκε σύγκριση χρησιμοποιώντας τα δεδομένα που προκύπτουν απο τη λίστα Badwords[] με τα δεδομένα που προκύπτουν απο την λίστα του δημιουργηθέντος συστήματος DirtyWords[] , στην οποία περιέχονται συχνά εμφανιζόμενες λέξεις απο hoax email.

Τα αποτελέσματα των πειραμάτων με τη μέθοδο του αλγορίθμου υποδεικνύουν λιγότερα false negatives με περισσότερα true positives , καθώς το σύστημα που κατασκευάστηκε DirtyWords[] έχει κατά μέσο όρο 33% υψηλότερο ποσοστό ακρίβειας , στον εντοπισμό ενός Hoax email , απο ότι της λίστας Badwords[] που χρησιμοποιήθηκε απο το διαδίκτυο για τους ελέγχους. Αυτό σημαίνει ότι για ένα Hoax email που θα εισέλθει στο σύστημα , η πιθανότητα να μην αναγνωριστεί ως "hoax" είναι μικρότερη αντί της Badwords λίστας. Αντίστοιχα , όσο αφορά τον εντοπισμό ενός Clean email , το σύστημα παρουσίασε 1,2% μικρότερο ποσοστό λάθους σε σχέση με την λίστα Badword.

Αξίζει να σημειωθεί πως αν και οι δύο λίστες είναι αρκετά επαρκείς στον εντοπισμό των clean emails η λίστα του αλγορίθμου DirtyWords[] λίστα προσεγγίζει με μικρότερο ποσοστό λάθους τον εντοπισμό των clean emails έναντι της λίστας Badwords, καθώς έχουμε λιγότερα false positives. Αυτό συνεπάγεται ότι η πιθανότητα να αναγνωρίσει η DirtyWords[] λίστα ένα Clean email ως Hoax email είναι μικρότερη αντί της λίστας Badwords.

Βάση των ευρημάτων , μπορούμε να αποφανθούμε στο συμπέρασμα ότι το σύστημα το οποίο κατασκευάστηκε μπορεί να χρησιμοποιηθεί επιτυχώς , για την επίλυση του προβλήματος. Η αποτελεσματική ανίχνευση μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ένα ανεπίλυτο πρόβλημα μεγάλης σημασίας , το οποίο επηρεάζει και το κόστος ενός ευρύτερου συστήματος. Αυτό συνεπάγεται ότι υπάρχουν συστήματα που δεν υποστηρίζουν παρόμοια τεχνική λόγω των πόρων που δεν διαθέτουν. Από την άλλη παρόμοιες τεχνικές έχουν ευρεία χρήση σε σύγχρονες εφαρμογές που όμως έχουν πολύ περιορισμένους πόρους.

Μελλοντικά το παρόν σύστημα μπορεί να χρησιμοποιηθεί απο την ακαδημαϊκή κοινότητα και να επιτρέψει τους επιστήμονες να αναπτύξουν πρακτικά , αποδοτικότερους αλγορίθμους δοκιμάζοντας διάφορους μεθόδους και τεχνικές οι οποίες θα συμβάλλουν ουσιαστικά στην αποτελεσματικότερη απόδοση του αλγορίθμου.

Κεφάλαιο 2
Hoax Emails

Εισαγωγικά

Το ηλεκτρονικό ταχυδρομείο είναι παντού. Εδώ και 40 χρόνια περίπου , έχει γίνει ένα από το πιο διαδεδομένα μέσα ηλεκτρονικής επικοινωνίας στις τεχνολογίες διαδικτύου , με απόδειξη τα δισεκατομμύρια μηνύματα που αποστέλλονται καθημερινά. Με αυτό το επίπεδο δημοτικότητας έρχονται και τα αντίστοιχα μερίδια των κινδύνων. Απο τους διάφορους φορείς απειλής, κανένα άλλο μέσο διανομής κακόβουλου κώδικα δεν πλησιάζει τόσο όσο το ηλεκτρονικό ταχυδρομείο. Το ηλεκτρονικό ταχυδρομείο για τους εισβολείς είναι από μακράν η πιο δημοφιλής μέθοδος στην εξάπλωση κακόβουλου κώδικα μέσω του διαδικτύου.

Τι είναι τα Hoax Email

Η απάτη στο διαδίκτυο είναι η χρήση υπηρεσιών Internet ή λογισμικού με πρόσβαση στο Διαδίκτυο για την εξαπάτηση των θυμάτων ή για την κατά τα άλλα εκμετάλλευση τους. Τα μηνύματα απάτης ηλεκτρονικού ταχυδρομείου (Hoax Emails) είναι παραπλανητικά μηνύματα που αποστέλλονται απο κυβερνοεγκληματίες προς λογαριασμούς χρηστών ηλεκτρονικού ταχυδρομείου. Ανήκουν στη κατηγορία των απειλητικών ηλεκτρονικών μηνυμάτων για τη κυβερνοασφάλεια στο ηλεκτρονικό ταχυδρομείο. Τα μηνύματα αυτά έχουν υποστεί πλαστογράφηση, και παραποίηση, με στόχο την υποκλοπή χρηματικών ποσών , και προσωπικών δεδομένων απο τους παραλήπτες τους.

Οι επιτιθέμενοι που συντάσσουν τα μηνύματα αυτά και τα διαδίδουν στο Διαδίκτυο, υποκλέπτουν εκατομμύρια δολάρια ετησίως από θύματα και συνεχίζουν να είναι η μάστιγα του κυβερνοχώρου με διάφορες μεθόδους και τεχνικές που ακολουθούν , ώστε να μην γίνονται αντιληπτοί.

2.1 Επιπτώσεις των Hoax Email τα τελευταία χρόνια

Το 2017 ο μη κερδοσκοπικός οργανισμός “Save the Children” , με έδρα τις Η.Π.Α., ο οποίος στηρίζει τα παιδιά σε όλο τον κόσμο και προσφέρει φιλανθρωπικές υπηρεσίες χρηματοδοτήσεις και χορηγίες , δημοσιοποιήθηκε από το Αμερικάνικο ειδησεογραφικό πρακτορείο Boston Globe στις 14 Δεκεμβρίου του τρέχοντος έτους, ότι τον Απρίλιο του 2017 , χάκερς εξαπάτησαν μέσω ηλεκτρονικού ταχυδρομείου , υπάλληλο της “Save the Children” με στόχο να καταθέσει χρηματικό ποσό της τάξης των 997.400 δολαρίων σε τραπεζικό λογαριασμό της Ιαπωνίας. Ο επιτιθέμενος κατάφερε να αποκτήσει πρόσβαση στον λογαριασμό ηλεκτρονικού ταχυδρομείου του υπαλλήλου και από εκεί έκτοτε, έστειλνε ψεύτικα τιμολόγια και άλλα έγγραφα που αποσκοπούσαν στο να εξαπατήσουν

την οργάνωση και να κατατεθούν τα χρήματα. (Muncaster 2018)

Το 2018 λίγο μετά την έναρξη των χειμερινών Ολυμπιακών Αγώνων στο Pyeongchang της Κορέας , τα συστήματα τηλεμετρίας απο επώνυμες εταιρείες παροχής αντιϊικών υπηρεσιών που έχουν στόχο την ασφαλή λειτουργία συστημάτων και περιήγησης στο διαδίκτυο , εξέλαβαν περιστατικά αναφορών για επιθέσεις κακόβουλων προγραμμάτων σε υποδομές που σχετίζονταν με τους χώρους των παιχνιδιών.

Ο διαδικτυακός "ολυμπιακός καταστροφέας" (olympic destroyer) ένας κακόβουλος κώδικας malware, που διοχετεύθηκε μέσω του ηλεκτρονικού ταχυδρομείου, έκλεισε τις οθόνες απεικόνισης των κεντρικών συστημάτων της διοργάνωσης , απενεργοποίησε το Wi-Fi και κατέστρεψε την ιστοσελίδα της διοργανώτριας αρχής , εμποδίζοντας τους επισκέπτες να εκτυπώσουν εισιτήρια.
Η επίθεση επηρέασε επίσης και γειτονικούς, γεωγραφικά οργανισμούς της περιοχής , απενεργοποιώντας για παράδειγμα τις πύλες του σκι και των λιφτ του σκι , πολλών χιονοδρομικών κέντρων της Νότιας Κορέας.

Το National Cybersecurity and Communications Integration Center (NCCIC) στις 19/06/2018 εξέδωσε ανακοίνωση μέσα απο τον επίσημο ιστότοπό του η οποία ανέφερε: "Ο olympic destroyer μολύνει νέα θύματα στην Ευρώπη απο τον Μάιο και τον Ιούνιο του 2018. Οι επιτιθέμενοι οργανισμοί , αναφέρονται ως χρηματοπιστωτικά ιδρύματα της Ρωσίας , εγκαταστάσεις πρόληψης βιολογικών και χημικών απειλών στην Ευρώπη και την Ουκρανία. Το κακόβουλο πρόγραμμα διανέμεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου με τη μέθοδο ηλεκτρονικού "ψαρέματος" και κακόβουλων συνημμένων αρχείων (NCCIC 2018).

Η κοινωνική μηχανική (Social Engineering) παραμένει ένα σημαντικό εργαλείο για τις επιθέσεις στο οπλοστάσιο των cyber attackers κάθε είδους.
Οι επιτιθέμενοι εκμεταλλευόμενοι σημαντικά γεγονότα που αφορούν τον αθλητισμό τη πολιτική και γενικότερα πολιτικά δρώμενα , βρίσκουν πάντα ευκαιρίες για να κερδίσουν χρήματα. Το 2018 το παγκόσμιο κύπελλο της FIFA, πριν ξεκινήσει η εκδήλωση, οι κυβερνοεγκληματίες άρχισαν να δημιουργούν ιστότοπους ηλεκτρονικού "ψαρέματος" (phishing) και να στέλνουν μηνύματα που αφορούσαν τα θέματα του παγκοσμίου κυπέλλου ποδοσφαίρου. Αυτά τα μηνύματα ηλεκτρονικού "ψαρέματος" περιελάμβαναν ειδοποιήσεις για μια ψεύτικη νίκη λοταρίας ή ένα μήνυμα που προσφέρει εισιτήρια σε έναν από τους αγώνες.
Τα μηνύματα με τα πειστικά εταιρικά λογότυπα που περιείχαν έδειχαν να προέρχονταν απο νόμιμους ιστότοπους συνεργατών της διοργάνωσης , ενώ παρείχαν έναν "αέρα" νομιμότητας και αξιοπιστίας όσο αφορά το περιβάλλον του περιεχομένου τους. Το καλά δημιουργημένο και σχεδιασμένο περιεχόμενο των σελίδων που παρέπεμπαν τα μηνύματα ηλεκτρονικής απάτης , (με πιστοποιητικά SSL) εξαπάτησε πάρα πολλούς παραλήπτες οι οποίοι προκειμένου να αγοράσουν εισιτήρια , τελικά κατέθεταν τα ποσά σε λογαριασμούς κατάθεσης των επιτιθέμενων και όχι στους λογαριασμούς της καθ' αυτής διοργάνωσης. (Chebyshev 2018 , Emm 2018)

Ο ιδρυτής και διευθύνων σύμβουλος Patrick Peterson της ACID (Agari Cyber Intelligence Division) σημειώνει μέσω της έκθεσης Q2 (ACID_29/04/19) ότι οι επιθέσεις τύπου "account takeover" για τη παραβίαση λογαριασμών χρηστών του ηλεκτρονικού ταχυδρομείου , έχει εντοπιστεί από το FBI, να είναι συνεχώς μια νέα αυξανόμενη απειλή για το τρέχον έτος. Αυτό συμβαίνει όταν ένας επιτιθέμενος θα διεισδύσει στον λογαριασμό του ηλεκτρονικού ταχυδρομείου για να γνωρίσει τα προσωπικά στοιχεία

του θύματος (είδος εργασίας , περιοχή διαμονής, τραπεζικούς λογαριασμούς κ.α.). Για την "account takeover" επίθεση οι χάκερς το 2019 στοχεύουν όλο και περισσότερο σε κτηματομεσίτες , κλέβοντας μεγάλα τραπεζικά εμβάσματα απο πωλήσεις σπιτιών. (Peterson 2019)

Στατιστικά

Κατά το 2017 η έρευνα της Symantec αναφέρει ότι κατά μέσο όρο, ένας στους εννέα ηλεκτρονικούς λογαριασμούς χρηστών αντιμετώπισαν κακόβουλο πρόγραμμα ηλεκτρονικού ταχυδρομείου κατά το πρώτο εξάμηνο του 2017. Ο κακόβουλος κώδικας δεν αποτελεί τη μόνη απειλή που χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο. Με τη μεγάλη τους εξάρτηση από την κοινωνική μηχανική και την επείγουσα φύση τους, οι απάτες ηλεκτρονικού ταχυδρομείου τύπου Business email Compromise BEC Scam είναι μια από τις πιο ισχυρές επιθέσεις ηλεκτρονικού ταχυδρομείου.

Οι επιθέσεις αυτές φαίνεται να μην είναι πια σπάνιες, με περίπου 8.000 επιχειρήσεις να αναφέρουν επιθέσεις σε ένα συγκεκριμένο μήνα ενώ κατά μέσο όρο, μια στοχευμένη οργάνωση έχει αποστέλλει 5 μηνύματα ηλεκτρονικού ταχυδρομείου BEC κάθε μήνα σε κάθε μία απο αυτές. Τα Spam email εξακολουθούν να αντιπροσωπεύουν ένα τεράστιο ποσοστό της κίνησης του ηλεκτρονικού ταχυδρομείου, αυξάνοντας στο 54% τη χρήση του ηλεκτρονικού ταχυδρομείου κατά το πρώτο εξάμηνο του 2017, αφού το ποσοστό είχε φτάσει στα χαμηλότερα επίπεδα τα τελευταία δύο χρόνια. (Nahorney 2017)

Η Symantec αναφέρει επίσης ότι το 2018, υπάλληλοι μικρών οργανισμών ήταν πιο πιθανό να πληγούν από απειλές ηλεκτρονικού ταχυδρομείου συμπεριλαμβανομένων των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam), του ηλεκτρονικού "ψαρέματος" (phishing) και του ηλεκτρονικού ταχυδρομείου (malware) ενώ διαπιστώθη κε ακόμα , ότι τα επίπεδα ανεπιθύμητης αλληλογραφίας συνέχισαν να αυξάνονται το 2018, όπως έκαναν κάθε χρόνο από το 2015, με το 55% των μηνυμάτων ηλεκτρονικού ταχυδρομείου που ελήφθησαν απο το έτος 2018 να κατηγοριοποιούνται ως ανεπιθύμητα (Symantec 2019)

Σύμφωνα με την Kaspersky για το έτος 2018 μόλις το 30,01% των χρηστών υπολογιστή , είχε υποστεί μία τουλάχιστον διαδικτυακή επίθεση τύπου Malware κατά τη διάρκεια του έτους. (Kaspersky 2018)

Προβλέψεις για το 2020

Για το 2020 η McAfee προβλέπει μέσω της έκθεσης Mobile Threat Report στο Mobile World Congress (MWC) που πραγματοποιήθηκε φέτος , ότι σχετικά με τις επιθέσεις κακόβουλου λογισμικού που έπονται για το τρέχον έτος , αναφέρει ότι διανύουμε την εποχή του “year of everywhere malware.” Λόγος είναι ο αριθμός των απειλών που αυξάνεται εκθετικά καθημερινά μέσω του Internet of Things(IoT) των gadgets και των κινητών συσκευών. Ήδη πρώτη αύξηση των απειλών παρατηρήθηκε να αυξάνεται γρήγορα απο το 2018. (George 2019)

Για το τρέχον έτος αντίστοιχο περιεχόμενο έκθεσης φαίνεται να δημοσίευσε και η Malwarebytes. Γίνεται αναφορά επίσης για το πρόβλημα των botnet που προκύπτει μέσω του IoT καθώς ήδη απο το 2ο εξάμηνο του 2018, αρκετά χιλιάδες MikroTik routers παραβιάστηκαν για να συνεισφέρουν ως συσκευές εξυπηρέτησης κατά το “coin mining”. Οι παραβιάσεις μεγάλης κλίμακας δρομολογητών και συσκευών του IoT αποτελεί μεγάλο

πρόβλημα , καθώς είναι πολύ πιο δύσκολο να αποτραπούν σε σχέση με τους υπολογιστές. Ακόμη και μόνο η επιδιόρθωση δεν διορθώνει το πρόβλημα, εάν η συσκευή είναι μολυσμένη. (Malwarebytes Labs 2018)

2.2 Ανίχνευση των Hoax Email

Παρακάτω παρουσιάζονται στοιχεία που συντελούν στην αναγνώριση και ανίχνευση μηνυμάτων ηλεκτρονικής απάτης στο διαδίκτυο.

Χαρακτηριστικά των Hoax Email

Η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα δεν συμφωνεί με τη διεύθυνση ιστότοπου του νόμιμου και έμπιστου οργανισμού ή εταιρείας.
Το μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται από μια εντελώς διαφορετική διεύθυνση ή απο έναν εξυπηρετητή που παρέχει δωρεάν λογαριασμούς και υπηρεσίες ηλεκτρονικού ταχυδρομείου.

Το μήνυμα ηλεκτρονικού ταχυδρομείου δεν απευθύνεται προσωπικά στο σωστό όνομα του παραλήπτη , αλλά χρησιμοποιεί ουδέτερο χαιρετισμό σε τρίτο πρόσωπο.

Υπάρχει στο μήνυμα η αίσθηση της επείγουσας ανάγκης. Για παράδειγμα, η απειλή , του ότι εάν δεν ενεργήσει άμεσα ο παραλήπτης , στις οδηγίες που καταγράφει ο επιτιθέμενος , τίθεται πρόβλημα ασφάλειας και υπάρχει ο κίνδυνος απενεργοποίησης του λογαριασμού του παραλήπτη.
Στο μήνυμα περιλαμβάνεται ένας παραπλανητικός σύνδεσμος ιστότοπου , που πρέπει να ανοίξει ο παραλήπτης. Αυτοί οι ιστότοποι μοιάζουν πολύ με τη σωστή διεύθυνση του οργανισμού ή της εταιρείας , αλλά υπάρχει διαφορά ελάχιστων χαρακτήρων που δεν είναι αντιληπτό εύκολα αν δεν το ελέγξει ο παραλήπτης του μηνύματος ενδελεχώς.
Το περιεχόμενο του μηνύματος εστιάζει στη καταχώρηση προσωπικών στοιχείων μέσω συμπλήρωσης μιας φόρμας , όπως όνομα χρήστη, κωδικό πρόσβασης ή τραπεζικά στοιχεία.
Το ηλεκτρονικό μήνυμα περιέχει συντακτικά ορθογραφικά και γραμματικά σφάλματα.
Δεν αναμένεται ο παραλήπτης να λάβει ένα μήνυμα ηλεκτρονικού ταχυδρομείου από την εταιρεία που φαίνεται να την έχει στείλει.
Το όλο περιεχόμενο του μηνύματος ηλεκτρονικού ταχυδρομείου εστιάζεται σε μια εικόνα και όχι σε κείμενο. Η εικόνα περιέχει μια ενσωματωμένη υπερσύνδεση σε μια πλαστή τοποθεσία. (NFCCRC 2016)

2.3 Βασικοί μέθοδοι επίθεσης των Hoax Email

Τα υψηλής δημοτικότητας ηλεκτρονικά μηνύματα απάτης , περιλαμβάνουν μεθόδους όπως:

Business E-Mail Compromise (BEC)

Μια εξελιγμένη απάτη που εστιάζει σε επιχειρήσεις οι οποίες συνεργάζονται με αλλοδαπούς προμηθευτές και γενικότερα σε εταιρείες που εκτελούν τακτικά καταθέσεις ή μεταφορές χρημάτων μέσω διαδικτύου σε προμηθευτές πελάτες ή διάφορους φορείς.

Data Breach

Την υποκλοπή και διαρροή ευαίσθητων προσωπικών δεδομένων από μια ασφαλή τοποθεσία σε ένα μη αξιόπιστο περιβάλλον. Η παραβίαση των δεδομένων μπορεί να εμφανιστεί σε προσωπικό και , μαζικό επίπεδο όπως επιχειρήσεις , εταιρείες, οργανισμούς, μια ευρύτερη ομάδα χρηστών του διαδικτύου η οποία περιλαμβάνει ευαίσθητες, προστατευμένες ή εμπιστευτικές πληροφορίες που αντιγράφονται, μεταδίδονται, προβάλλονται, υποκλέπτονται ή χρησιμοποιούνται από μη εξουσιοδοτημένα άτομα για να το πράξουν στο διαδίκτυο.

E-Mail Account Compromise (EAC)

Την απάτη ηλεκτρονικού ταχυδρομείου που στοχεύει στο ευρύ κοινό και τους επαγγελματίες που σχετίζονται με το κοινό αυτό. Δηλαδή , αυτού του είδους η ηλεκτρονική απάτη δεν περιορίζεται αναγκαστικά σε, χρηματοπιστωτικούς και δανειστικούς οργανισμούς, εταιρείες κτηματομεσιτικών και δικηγορικά γραφεία (όπως η BEC). Οι δράστες της μεθόδου EAC χρησιμοποιούν παραβιασμένους λογαριασμούς ηλεκτρονικού ταχυδρομείου για να ζητήσουν πληρωμές σε ύποπτες για το διαδίκτυο , γεωγραφικές τοποθεσίες χωρών.

Malware / Scareware

Το κακόβουλο λογισμικό που περιέχεται σε μηνύματα ηλεκτρονικού ταχυδρομείου , και προορίζεται να βλάψει ή να απενεργοποιήσει τους υπολογιστές και τα συστήματα των υπολογιστών. Μερικές φορές αυτές οι τακτικές των επιτιθέμενων , χρησιμοποιούνται για να ζητήσουν οικονομικά κεφάλαια από τα υποψήφια θύματα.

Phishing/Spoofing

Τους μεθόδους απάτης που εστιάζουν σε πλαστά και παραποιημένα ηλεκτρονικά έγγραφα τα οποία διανέμονται μέσω ηλεκτρονικού ταχυδρομείου. Η μέθοδος “Spoofing” αναφέρεται στη διάδοση ηλεκτρονικής αλληλογραφίας, όπου ο αποστολέας υποδύεται την πραγματική πηγή του μηνύματος, ενώ δεν είναι. Η μέθοδος απάτης ηλεκτρονικού "ψαρέματος" (phishing), η οποία αναφέρεται επίσης και ως “vishing”, “smishing”, ή “pharming” χρησιμοποιείται συχνά σε συνδυασμό με ένα πλαστογραφημένο ηλεκτρονικό έγγραφο. Είναι η δράση δηλαδή της αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου που ισχυρίζεται ότι είναι η νόμιμη πηγή του μηνύματος (π.χ. επιχείρηση) με σκοπό να εξαπατήσει τον ανυποψίαστο παραλήπτη ώστε να αποκαλύψει προσωπικές, ευαίσθητες πληροφορίες του, όπως κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών και πληροφορίες τραπεζικού λογαριασμού. Αυτό συμβαίνει αφού ο χρήστης επισκεφθεί έναν συγκεκριμένο ιστότοπο που το μήνυμα τον προτρέπει. Ο ιστότοπος κατ επέκταση που επισκέπτεται ο παραλήπτης , δεν είναι γνήσιος , αλλά τείνει να ομοιάζει με το πραγματικό. Το περιβάλλον του ιστότοπου είναι πλήρως διαχειρίσιμο απο τον επιτιθέμενο, δίνοντάς του τη δυνατότητα να αποθηκεύει οποιαδήποτε πληροφορία ο χρήστης καταχωρήσει.

Ransomware:

Τη μορφή κακόβουλου λογισμικού που στοχεύει σε αδυναμίες τόσο του ανθρώπινου παράγοντα (ανθρώπινο λάθος , ελλειπή τεχνική κατάρτιση), όσο και στις τεχνικές

ευπάθειες συστημάτων οργανισμών και μεμονωμένων δικτύων. Η μέθοδος Ransomware διοχετεύεται συχνά μέσω του ηλεκτρονικού ταχυδρομείου με το μέθοδο "phishing" στους τελικούς χρήστες, με αποτέλεσμα την ταχεία κρυπτογράφηση ευαίσθητων αρχείων και πληροφοριών σε ένα εσωτερικό εταιρικό δίκτυο. Όταν ο οργανισμός-θύμα, διαπιστώνει ότι δεν είναι πλέον σε θέση να έχει πρόσβαση στα δεδομένα του, ο δράστης του κυβερνοχώρου απαιτεί απο το θύμα της επίθεσης , την καταβολή χρηματικού ποσού , σε εικονικό νόμισμα του διαδικτύου, (bitcoin), ώστε να ανακτήσει την πρόσβαση στα δεδομένα του ξανά το θύμα. (FBI 2017)

2.4 Βασικοί τύποι Hoax Email

1. Government Maneuver

Αυτός ο τύπος μηνύματος ηλεκτρονικού ταχυδρομείου φαίνεται να προέρχεται από έναν ομοσπονδιακό οργανισμό, όπως το FBI, και προσπαθεί να τρομάξει τον παραλήπτη για την δημοσιοποίηση και την καταχώρηση των πληροφοριών του σε μία φόρμα συμπλήρωσης. Συνήθως το περιεχόμενο αυτών των μηνυμάτων είναι: "Η ασφάλειά σας έχει απορριφθεί λόγω ελλιπών πληροφοριών. Κάντε κλικ εδώ για να δώσετε τα στοιχεία σας ή επειδή έχετε κατεβάσει παράνομα αρχεία, η πρόσβαση στο Internet σας θα ακυρωθεί μέχρι να καταχωρίσετε τις απαιτούμενες πληροφορίες στην παρακάτω φόρμα".

2. Friend Tactic

Το μήνυμα αναφέρει ότι ένας φίλος του παραλήπτη βρίσκεται σε ξένη χώρα και χρειάζεται τη βοήθειά του. Έτσι , είναι θεμιτό πριν ο παραλήπτης καταθέσει οποιοδήποτε ποσό σε κάποιον γνωστό του , να επικοινωνήσει πρώτα τηλεφωνικά με τον ίδιο για μια επαλήθευση της κατάθεσης. Η λίστα επαφών του ηλεκτρονικού ταχυδρομείου του παραλήπτη πιθανότατα παραβιάστηκε απο τον επιτιθέμενο ο οποίος και υποδύεται τον φίλο του παραλήπτη.

3. Billing Problem

Η ανίχνευση αυτής της τακτικής ηλεκτρονικού ψαρέματος είναι δύσκολη επειδή φαίνεται αρκετά νόμιμη. Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου δηλώνει ότι ένα στοιχείο που αγόρασε ο παραλήπτης ηλεκτρονικά δεν μπορεί να του αποσταλεί επειδή η πιστωτική κάρτα έληξε (ή η διεύθυνση χρέωσης δεν ήταν σωστή κ.λπ.). Εάν επιλέξει τον σύνδεσμο που του παρέχεται στο μήνυμα , το link θα τον οδηγήσει σε έναν όμοιο με πραγματικό ιστότοπο , για να καταχωρήσει εν συνεχεία , -όπου του ζητείται- προσωπικές πληροφορίες , κωδικούς ή να κάνει ηλεκτρονικές πληρωμές με εμβάσματα σε τραπεζικούς λογαριασμούς κλπ.

4. Expiration Date

Αυτός ο τύπος μηνύματος ηλεκτρονικού ταχυδρομείου εξηγεί ψευδώς ότι ο λογαριασμός με το όνομα της εταιρείας πρόκειται να λήξει και πρέπει να συνδεθεί το συντομότερο δυνατό, ώστε να αποφευχθεί η απώλεια όλων των δεδομένων του χρήστη. Σε αρκετά εμφανές σημείο του μηνύματος , υπάρχει ένας σύνδεσμος ο οποίος οδηγεί και πάλι σε μια σελίδα σύνδεσης για την καταχώρηση προσωπικών δεδομένων και στοιχείων απο πλευράς χρήστη.

5. Virus or Compromised Account Scare

Αυτοί οι τύποι μηνυμάτων ηλεκτρονικού ταχυδρομείου δηλώνουν ότι ο υπολογιστής του χρήστη έχει μολυνθεί απο ιό ή ότι ένας από τους λογαριασμούς του χρήστη έχει παραβιαστεί. Έτσι ο επιτιθέμενος , καθοδηγεί το θύμα να ακολουθήσει έναν σύνδεσμο και εν συνεχεία να κάνει λήψη ενός συνημμένου αρχείου, με στόχο (υποτίθεται) , να αποφευχθεί τυχόν οικονομική απώλεια ή απώλεια δεδομένων απο το χρήστη. Το κατέβασμα και άνοιγμα του αρχείου απο μεριάς του χρήστη , θα δώσει στον επιτιθέμενο πλήρη πρόσβαση στο σύστημα του χρήστη.

6. Contest Winner

Ο χρήστης λαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου που ισχυρίζονται ότι ο παραλήπτης έχει κερδίσει κάποια διάκριση , κάποιο δώρο ή είναι δικαιούχος κληρονομιάς από συγγενή που δεν γνώριζε ποτέ. Το 99,9% αυτών των μηνυμάτων , είναι ψευδή. Οι οδηγίες που παρέχονται στο περιεχόμενο του μηνύματος οδηγούν το θύμα να κάνει κλικ σε ένα σύνδεσμο ώστε κατά συνέπεια, σε μία φόρμα συμπλήρωσης στοιχείων μετά , ο χρήστης να εισαγάγει προσωπικές πληροφορίες του (διεύθυνση τηλέφωνο κωδικούς) για την αποστολή βραβείων.

7. Friendly Bank

Η τράπεζα μπορεί να προσφέρει ειδοποιήσεις για τις κινήσεις λογαριασμών ακόμα και μέσω ηλεκτρονικού ταχυδρομείου , όταν αποσύρονται ορισμένα ποσά από τους λογαριασμούς των πελατών της. Αυτή η μέθοδος τύπου Hoax εξαπατά τους χρήστες του ηλεκτρονικού ταχυδρομείου , με μια ψευδή ειδοποίηση λογαριασμού που δηλώνει ότι έχει αφαιρεθεί ποσό από το λογαριασμό του χρήστη, που υπερβαίνει το ανώτατο όριο. Έτσι αν ο παραλήπτης του μηνύματος έχει ερωτήσεις σχετικά με αυτή την ανάληψη ποσού , απο το τραπεζικό του λογαριασμό (που πιθανώς θα έχει), αναδεικνύει το περιεχόμενο του μηνύματος, έναν σύνδεσμο που αν επιλεγεί απο το χρήστη , τον οδηγεί σε μια φόρμα συμπλήρωσης , όπου ζητούνται προς καταχώρηση ο αριθμός του τραπεζικού του λογαριασμού "για λόγους επαλήθευσης" και διάφορα άλλα προσωπικά στοιχεία. Θα πρέπει λοιπόν ο χρήστης αντί να κάνει κλικ στον σύνδεσμο του μηνύματος , να επικοινωνήσει τηλεφωνικά με το τμήμα εξυπηρέτησης πελατών της τράπεζας, για επαλήθευση της αυθεντικότητας του μηνύματος , ή αν διαπιστωθεί διαδικτυακή απάτη , την αναφορά του συμβάντος.

8. Victim

Το περιεχόμενο του μηνύματος εστιάζει σε κατηγορίες κατά του παραλήπτη απο έναν πελάτη ο οποίος είναι δυσαρεστημένος απο την αγορά ενός προϊόντος που του στάλθηκε. Αυτός ο τύπος ηλεκτρονικού ταχυδρομείου ηλεκτρονικού "ψαρέματος" λειτουργεί ως ο θυμωμένος και δυσαρεστημένος πελάτης, ο οποίος υποτίθεται ότι έστειλε χρήματα προς το χρήστη του ηλεκτρονικού ταχυδρομείου για ένα προϊόν που του στάλθηκε απο το παραλήπτη του μηνύματος. Το email ολοκληρώνεται με την απειλή ότι ο αποστολέας θα ενημερώσει τις αρχές εάν ο παραλήπτης του μηνύματος δεν απαντήσει άμεσα στον αποστολέα.

9. Tax Communication

Επειδή ο κάθε ένας φορολογούμενος έχει ετήσιους φόρους να υποβάλει και να δηλώσει στον αρμόδιο φορέα, αυτός είναι ο λόγος για τον οποίο η απόπειρα ηλεκτρονικού "ψαρέματος" είναι τόσο δημοφιλής Το μήνυμα δηλώνει ότι οι παραλήπτης του μηνύματος δικαιούται να λάβει επιστροφή φόρου ή ότι έχει επιλεγεί για έλεγχο. Στη συνέχεια, το μήνυμα ζητά απο το παραλήπτη να υποβάλει μέσα απο μια φόρμα συμπλήρωσης , αίτημα επιστροφής φόρου.

10. Checkup

Ο αποστολέας του μηνύματος ισχυρίζεται ότι πάντα με την υπογραφή ενός νόμιμου κατοχυρωμένου brand μίας εταιρείας , η εταιρεία διεξάγει μια διαδικασία ρουτίνας όσο αφορά την ασφάλεια των προσωπικών δεδομένων των πελατών της και ζητά απο τους πελάτες να κάνουν επαλήθευση των στοιχείων τους μέσα απο μια φόρμα συμπλήρωσης. Αυτή η απάτη είναι ιδιαίτερα αποτελεσματική αν ο πελάτης τυχαίνει να είναι πραγματικός πελάτης της εν λόγο εταιρείας. (Ellis 2019)

Γνωστότεροι τύποι Hoax Email 2018 – 2019

Airbnb Scam

Αυτή η απάτη εκμεταλλεύεται τους ταξιδιώτες που νοικιάζουν ένα διαμέρισμα ή ένα σπίτι μέσω της Airbnb, παρουσιάζοντας ψεύτικα σπίτια στην περιοχή και κατευθύνοντας τον ενοικιαστή σε έναν πλαστό ή "ψεύτικο" ιστότοπο για να ολοκληρώσει την συμπληρώνοντας φόρμες καταχώρησης στοιχείων. Οι απατεώνες συχνά θα εξαπατήσουν ακόμη και πραγματικούς ιδιοκτήτες, οι οποίοι δεν γνωρίζουν ότι η περιουσία τους παραβιάζεται απο κυβερνοεγκληματίες. Αποτέλεσμα αυτού είναι ότι τα πιθανά θύματα , ταξιδιώτες ή τουρίστες να καταλήγουν να πληρώνουν χρήματα για ένα ακίνητο που είτε δεν υπάρχει είτε δεν είναι διαθέσιμο.

Amazon Fake Order Cancellation Emails

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου λαμβάνεται απο το χρήστη , σχετικά με μια ακύρωση ηλεκτρονικής παραγγελίας του , μέσω της Amazon. Το μήνυμα προτρέπει το χρήστη να κάνει κλικ σε διάφορους συνδέσμους που περιέχονται σε αυτό, ώστε ο χρήστης να κάνει λήψη κακόβουλου λογισμικού στη συσκευή του ή να ανοίξει έναν ιστότοπο που θα τον οδηγήσει σε μία σελίδα του επιτιθέμενου και η οποία θα μοιάζει με της Amazon. Ο παραλήπτης τέτοιου μηνύματος ηλεκτρονικού ταχυδρομείου αν πρόσφατα είχε πραγματοποιήσει μια παραγγελία μέσω της Amazon, θεμιτό θα ήταν να μεταβεί στη σελίδα της Amazon για να ελέγξει την κατάσταση της παραγγελίας του.

Apple Care Scam

Αυτός ο νέος τύπος απάτης που απευθύνεται σε κατόχους smartphone της Apple , χρησιμοποιεί ηλεκτρονικά μηνύματα ηλεκτρονικού "ψαρέματος" (phishing) για να στείλει τους χρήστες της Apple σε έναν ψεύτικο δικτυακό τόπο της Apple. Οι χρήστες iPhone λαμβάνουν μια αναδυόμενη εικόνα ενός πλαισίου διαλόγου συστήματος που λέει στους χρήστες ότι το τηλέφωνό τους έχει "κλειδωθεί για παράνομη δραστηριότητα". Όταν οι χρήστες κάνουν κλικ στον σύνδεσμο, οι απατεώνες τους εγγράφουν σε μια δόλια "υπηρεσία διαχείρισης κινητών συσκευών" που επιτρέπει στους απατεώνες να στέλνουν εφαρμογές κακόβουλου λογισμικού σε iPhone.

Cryptocurrency Scams

Καθώς η τιμή και η δημοτικότητα του Bitcoin και άλλων κυβερνο-νομισμάτων ανέβηκαν στα ύψη στα τέλη του 2017, οι απατεώνες προσπάθησαν με ανυπομονησία να εκμεταλλευτούν την συνεχώς αυξανόμενη δημοτικότητα στο κυβερνοχώρο και να επωφεληθούν απο υποκλοπές μεγάλων χρηματικών ποσών. Το ιαπωνικό χρηματιστήριο Bitcoin Coin check παραβιάστηκε απο επιτιθέμενους τον Ιανουάριο του 2018 και οι επιτιθέμενοι κατάφεραν να υπεξαιρέσουν περισσότερα από 500 εκατομμύρια δολάρια. Παραβίασαν τους λογαριασμούς συναλλαγών του Ιαπωνικού χρηματιστηρίου με αποτέλεσμα τα ηλεκτρονικά νομίσματα να κατατίθενται σε λογαριασμούς επιτιθέμενων. Αυτό το γεγονός του 2018 συντέλεσε ώστε το Facebook και το Instagram να έχουν απαγορεύσει τις διαφημίσεις για ορισμένα bitcoin, για αρχικές προσφορές νομισμάτων (ICO) και για κάποια άλλα προϊόντα που σχετίζονται με την κρυπτο-οικονομία στο κυβερνοχώρο, λόγω των παραπλανητικών πρακτικών που ακολουθούνταν απο επίδοξους επιτιθέμενους. Αρκετές διαφημίσεις οδηγούσαν τα υποψήφια θύματα σε τοποθεσίες όπως το Prodeum, όπου σκοπός των επιτιθέμενων ήταν να υποκλέπτουν εμβάσματα , απο οικονομικές καταθέσεις πελατών.

Death Threat Hoax

Η ομοσπονδία του FBI προειδοποίησε τους χρήστες του διαδικτύου, σχετικά με αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου που εμπεριέχουν ηλεκτρονικά συμβόλαια θανάτου , και απειλούν τη ζωή του παραλήπτη , ότι είναι αναληθή και αποτελούν μια νέα μορφή απειλής για το ηλεκτρονικό έγκλημα στο ηλεκτρονικό ταχυδρομείο. Το FBI συστήνει ο χρήστης να μη στέλνει χρηματικά ποσά σε κάποιον που δεν γνωρίζει και δεν έχει λόγο να εμπιστευτεί απο το διαδίκτυο. Επίσης αναφέρει να μην παρέχει τα προσωπικά δεδομένα και στοιχεία του ο χρήστης , συμπεριλαμβανομένου και του τραπεζικού του λογαριασμού, για χρήση τρίτων . Τέλος επισημαίνει ότι για την αντιμετώπιση του φαινομένου είναι αρκετό, να μην υπάρξει καμία είδους επαφή ή μορφή επικοινωνίας, με τον αποστολέα του μηνύματος ο οποίος ζητάει πληρωμή μέσω νομίσματος bitcoin ή προπληρωμένης κάρτας. (McCabe 2017)

Fake Bank Apps

Οι επιτιθέμενοι προσομοιώνουν τις εφαρμογές κίνησης των τραπεζικών συναλλαγών των τραπεζών ώστε τελικά να καταθέτουν τα υποψήφια θύματά τους εμβάσματα στους δικούς τους λογαριασμούς ώστε να υποκλέψουν μεγάλα χρηματικά ποσά . Έρευνα της Avast, διαπίστωσε ότι ένας στους τρεις χρήστες σε όλο τον κόσμο πίστευε λανθασμένα ότι το προσομοιωμένο application mobile banking ήταν η αυθεντική εφαρμογή , θέτοντας οι χρήστες της εφαρμογής τα χρηματοοικονομικά τους δεδομένα σε κίνδυνο. Οι επιτιθέμενοι υποκλέπτουν συνήθως τη πελατειακή βάση δεδομένων απο μεγάλες τράπεζες ώστε να προσπαθήσουν εν συνεχεία να παραβιάσουν τις αξιόπιστες εφαρμογές e-banking και να συλλέξουν προσωπικές πληροφορίες.

Fortnite Scam

Η μεγάλη ανταπόκριση που βρίσκει το διαδικτυακό παιχνίδι "Fortinite" στο κυβερνοχώρο (περισσότεροι από 125 εκατομμύρια παίκτες σε όλο τον κόσμο) οδηγεί τους επιτιθέμενους να εστιάζουν σε έναν νέο τύπο σύνθεσης Hoax email ο οποίος οδηγεί τους παίκτες του παιχνιδιού , στο να ανοίγουν συνημμένα αρχεία , μηνυμάτων απάτης τα οποία υπόσχονται ότι περιέχουν κωδικούς προσφορών για την αύξηση των

δυνατοτήτων του παιχνιδιού. Η Epic Games (κατασκευάστρια εταιρεία του Fortinite) επιστεί τη προσοχή στους παίκτες του παιχνιδιού , ότι αυτός ο τύπος Hoax email μπορεί να έχει ως αποτέλεσμα την υποκλοπή λογαριασμού χρήστη του παιχνιδιού , εν συνεχεία τη λήψη κακόβουλου λογισμικού σε μια απο τις συσκευές του χρήστη και τέλος την υποκλοπή χρηματικού ποσού.

Instagram Fake Ads

Σκοπός τους επιτιθέμενου είναι να παρακινήσει το υποψήφιο θύμα να αγοράσει μέσω ενός μηνύματος απάτης , ένα ανύπαρκτο προϊόν, το οποίο προέρχεται απο μία ψεύτικη διαφήμιση του Instagram. Λόγω του μεγάλου όγκου των διαφημίσεων στα μέσα κοινωνικής δικτύωσης οι χρήστες κάποιες φορές δυσκολεύονται να διακρίνουν τα αυθεντικά απο τα ψεύτικα προϊόντα συμπεριλαμβανομένων και των διαφημίσεων. Οι επιτιθέμενοι συχνά δημοσιεύουν ψεύτικες διαφημίσεις για να παρακινήσουν τους χρήστες των κοινωνικών μέσων δικτύωσης να αγοράσουν ένα προϊόν , με κίνητρο την πολύ χαμηλή τιμή του προϊόντος (τιμή προσφοράς).

Netflix Scam

Η δημοφιλής υπηρεσία streaming (συνεχούς ροής) της Netflix , έχει ξεκινήσει να γίνεται στόχος απο επιτιθέμενους με τη σύνθεση ενός νέου τύπου μηνύματος απάτης. Με τη μέθοδο phishing , αναγράφεται στο θέμα του μηνύματος ότι "η πληρωμή απορρίφθηκε". Αν κάποιος παραλήπτης είναι συνδρομητής στην υπηρεσία της Netflix ένα τέτοιο θέμα μηνύματος σίγουρα θα του επιστήσει τη προσοχή. Το περιεχόμενο του ίδιου μηνύματος προτρέπει το χρήστη να ανοίξει έναν ιστότοπο , και μέσω μιας φόρμας που συμπληρώνει τα προσωπικά του στοιχεία, καταχωρεί και τα στοιχεία της πιστωτικής του κάρτας , τα οποία εν συνεχεία υποκλέπτονται απο τους κυβερνοεγκληματίες.

Porting Scams

Αυτός ο τύπος απάτης αναφέρεται στη μέθοδο που ακολουθούν οι κυβερνοεγκληματίες ώστε να υποκλέψουν προσωπικά στοιχεία του θύματος , μέσω κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Απώτερος σκοπός τους είναι να καταφέρουν να έχουν εξουσιοδοτημένη πρόσβαση στο κινητό τηλέφωνο του θύματος , με στόχο να μπορούν να πραγματοποιούν συναλλαγές σε τραπεζικούς λογαριασμούς. Απαραίτητη προϋπόθεση γι αυτούς είναι να έχουν στη κατοχή τους , τους κωδικούς επιβεβαίωσης e-banking οι οποίοι στέλνονται στη συσκευή με sms text απο τη τράπεζα. Οι κυβερνοεγκληματίες αφού ξεκινήσουν με τη συλλογή των προσωπικών στοιχείων του υποψηφίου θύματος όπως ονοματεπώνυμο , αριθμός τηλεφώνου, διεύθυνση , αριθμός κοινωνικής ασφάλισης και ημερομηνία γέννησης στη συνέχεια, επικοινωνούν με τον πάροχο κινητής τηλεφωνίας και δηλώνουν κλοπή της τηλεφωνικής συσκευής για τον συγκεκριμένο αριθμό και ζητούν την μεταφορά του αριθμού σε άλλο πάροχο κινητής τηλεφωνίας αλλά και συσκευής. Μόλις ο αριθμός του θύματος μεταφερθεί στο νέο πάροχο και στη νέα συσκευή, οι επιτιθέμενοι μπορούν στη συνέχεια να ξεκινήσουν αναλήψεις απο τραπεζικούς λογαριασμούς του θύματος αφού κάθε κίνηση απαιτεί πρόσθετη εξουσιοδότηση (μέσω κωδικών επιβεβαίωσης που στέλνονται απο την τράπεζα στη καινούργια συσκευή μέσω του παρόχου κινητής τηλεφωνίας). (Tatham 2018)

2.5 Αντιμετώπιση των Hoax Email

Μέτρα πρόληψης για την αντιμετώπιση των Hoax Email

Ο παραλήπτης των μηνυμάτων δεν θα πρέπει να ανοίγει κάποιο συνημμένο μήνυμα ή σύνδεσμο που δεν είναι αξιόπιστο εφόσον αυτό μπορεί να έχει κάποιο ιό, ο οποίος με την σειρά του θα πλήξει την λειτουργία του συστήματος. Είναι προτιμότερη η αποθήκευση ολόκληρου του μηνύματος και ο έλεγχός του να γίνει από το αρμόδιο τμήμα IT.

Για την εξασφάλιση της προστασίας να γίνεται ο έλεγχος της διεύθυνσης URL των ιστότοπων και των συνδέσμων. Θα μπορούσε κάποιος να διακρίνει τις αξιόπιστες σελίδες από τις ιστοσελίδες απάτης αφού οι πρώτες χρησιμοποιούν σαφείς διευθύνσεις όπως ενώ οι δεύτερες κάνουν χρήση ειδικών χαρακτήρων όπως = j & q = & esrc = s & source = web & "7 . (IATA 2019)

Ο χρήστης δεν θα πρέπει να ανοίγει απο το περιεχόμενο των μηνυμάτων συνδέσμους εικόνων , συνημμένα αρχεία ή εικόνες. Παράλληλα, δεν θα πρέπει σε καμία περίπτωση να απαντήσει στον αποστολέα.

Σε περίπτωση που ο χρήστης πραγματοποιεί μια νόμιμη συναλλαγή με μια εταιρεία που έχει ήδη αναφερθεί στο ηλεκτρονικό ταχυδρομείο ως “εταιρεία ηλεκτρονικού ψαρέματος” , προτείνεται να επικοινωνήσει με την επιχείρηση σχετικά με την αποστολή του ηλεκτρονικού μηνύματος, ώστε να ληφθούν τα απαραίτητα μέτρα απο τη μεριά της εταιρείας.

Αναφορικά με το προφίλ των επίμονων επιθέσεων απο εισβολείς, συνήθως προσποιούνται πως είναι κυβερνητικοί υπάλληλοι, μέλη οικογενειών, φιλανθρωπιών ή εταιρειών με τις οποίες συνεργάζεται ο χρήστης προκειμένου να κερδίσουν την εμπιστοσύνη του. Για αυτό το λόγο είναι σημαντικό να μη αποστέλλει χρήματα και να μην δίνει προσωπικά στοιχεία, οποιασδήποτε μορφής , είτε μέσω κειμένου , είτε μέσω τηλεφωνικής κλήσης είτε μέσω ηλεκτρονικού ταχυδρομείου.

Προτείνεται για μεγαλύτερη ασφάλεια να γίνεται και αναζήτηση στο διαδίκτυο μιας εταιρείας ή ενός τίτλου προϊόντος σε συνδυασμό με λέξεις κλειδιά ώστε να διασφαλιστεί η γνησιότητα του προϊόντος και η επαλήθευση της ταυτότητας του αποστολέα. Είναι απαραίτητο ο παραλήπτης του ηλεκτρονικού μηνύματος να είναι επιφυλακτικός ακόμη και αν μπορεί να δει την ταυτότητα του αποστολέα. Είναι πιθανό το όνομα, ο αριθμός και λοιπές πληροφορίες να είναι ψευδείς. Ο χρήστης θα πρέπει να διακόψει την επικοινωνία σε περίπτωση που του ζητηθούν χρήματα ή προσωπικά στοιχεία. Σε περίπτωση που κρίνει ότι η επικοινωνία δεν είναι προϊόν απάτης , μπορεί να επικοινωνήσει με τον αποστολέα σε μια πιστοποιημένη και γνήσια διεύθυνση του διαδικτύου.

Ο χρήστης δεν θα πρέπει να πληρώνει εκ των προτέρων σε περιπτώσεις που μπορεί να αφορούν ελάφρυνση χρεών, προσφορές δανείων, υποθήκες και εργασία.

Επίσης, είναι πιθανό να εξαπατηθεί κάποιος με το πρόσχημα πως κέρδισε κάποιο βραβείο και να του ζητηθεί να πληρώσει κάποιο φόρο.

Απαιτούμενη προσοχή πρέπει να δοθεί και όσον αφορά τον τρόπο πληρωμής, παρόλο που οι πιστωτικές κάρτες έχουν σημαντική προστασία κατά των περιστατικών απάτης στο διαδίκτυο. Θα πρέπει ο χρήστης να προσέξει υπηρεσίες μέσω των οποίων δεν είναι

δυνατή η επιστροφή των χρημάτων (WesternUnion, MoneyGram). Ακόμη, υπάρχει κίνδυνος στις επαναφορτιζόμενες κάρτες (MoneyPak ή Reloadit) και στις κάρτες δώρων όπως iTunes και Google Play. Εξάλλου, αν πρόκειται για κυβερνητικές εταιρείες ή αξιόπιστες εταιρείες δεν θα ζητηθούν οι συγκεκριμένοι μέθοδοι πληρωμής.

Είναι πολύ βοηθητική η επικοινωνία με κάποιο πρόσωπο εμπιστοσύνης σε περίπτωση που το άτομο υποψιαστεί πως πρόκειται για μήνυμα ηλεκτρονικής απάτης ιδιαίτερα όσον αφορά χρηματικές πληρωμές και αποστολή προσωπικών στοιχείων. Καλό θα ήταν ο παραλήπτης του μηνύματος να αναζητήσει στο διαδίκτυο πληροφορίες σχετικές με το μήνυμα που του έχει αποσταλλεί ή να συμβουλευτεί κάποιον ειδικό της ασφάλειας δικτύου.

Ο χρήστης χρειάζεται να κρατάει επιφυλακτική στάση όσον αφορά τις δοκιμαστικές προσφορές. Υπάρχει πιθανότητα κάποιος με την εγγραφή του σε κάποια προσφορά (δωρεάν δοκιμής) , να έχει υποστεί μηνιαία χρέωση, για την υπηρεσία μέχρι την ακύρωσή της. Για αυτό απαιτείται έρευνα σχετικά με την εταιρεία, τη γνώση της πολιτικής ακύρωσης και την αναζήτηση τυχόν μηνιαίων χρεώσεων που δεν αναγνωρίζει.

Αν υπάρχει κάποια απειλή σε ένα λογαριασμό του ηλεκτρονικού του ταχυδρομείου τότε απειλούνται και όλοι οι υπόλοιποι που συνδέονται στο ίδιο δίκτυο.

Ο χρήστης δεν θα πρέπει να ανοίγει συνημμένα αρχεία από άγνωστες πηγές. Παράλληλα, δεν θα πρέπει να εκτελεί προγράμματα συνημμένα σε μηνύματα του ηλεκτρονικού ταχυδρομείου από άγνωστους παραλήπτες. Με αυτούς τους τρόπους κάποιος επιτιθέμενος είναι δυνατόν να αποκτήσει πρόσβαση στους λογαριασμούς του ηλεκτρονικού του ταχυδρομείου. Οι τρόποι αυτοί είναι βοηθητικοί για προστασία από ιούς και κακόβουλα λογισμικά όπως τα “Key Logger” (καταγραφείς κωδικών) που αναζητούν τα στοιχεία πρόσβασης που πληκτρολογεί ο χρήστης στις εκάστοτε φόρμες.

Τέλος, πρόσβαση στο λογαριασμό κάποιου χρήστη ηλεκτρονικού ταχυδρομείου θα μπορούσαν να έχουν οι επιτιθέμενοι σε περίπτωση σύνδεσης του χρήστη σε ανοιχτό, δημόσιο δίκτυο Wi-fi. Συνεπώς για τους επιτιθέμενους θα ήταν ορατή η σύνδεση του θύματος στο ηλεκτρονικό ταχυδρομείο καθώς θα ήταν ορατές και κάποιες ηλεκτρονικές πληρωμές. Χρειάζεται προσοχή λοιπόν, στις συνδέσεις σε ανοιχτά δίχτυα. Για μεγαλύτερη ασφάλεια είναι αναγκαίο ο χρήστης όχι μόνο να αποσυνδεθεί από το ηλεκτρονικό ταχυδρομείο αλλά και να κλείσει την καρτέλα του προγράμματος περιήγησης.

Ο χρήστης χρειάζεται να είναι προσεχτικός με διαφημίσεις προσφοράς προϊόντων , που αφορούν στην ασφάλεια του συστήματός του. Υπάρχουν στο διαδίκτυο διαφημίσεις για “download-able” προγράμματα αντι-ικής προστασίας , προστασίας malware και anti-spyware τα οποία κατά την εγκατάστασή τους περιέχουν spyware ή κάποιο κακόβουλο κώδικα. Το λογισμικό υποκλοπής spyware , αφενός συγκεντρώνει πληροφορίες του χρήστη χωρίς τη συγκατάθεση του και αφετέρου προβάλλει ανεπιθύμητες διαφημίσεις στο πρόγραμμα περιήγησης.

Είναι ωφέλιμο να υπάρχει πολιτική αντιμετώπισης όσο αφορά τα ηλεκτρονικά μηνύματα

απάτης , είτε από τον οργανισμό ή τις εταιρείες και να έχει ενημερωθεί το προσωπικό για τις αντίστοιχες ενέργειες σε περίπτωση περιστατικού κακόβουλης ηλεκτρονικής επίθεσης.

Επίσης, οι εταιρείες θα πρέπει να εκκινήσουν διαδικασίες ελέγχου δύο και τριών ατόμων, ώστε ένα άτομο να μην μπορεί να πραγματοποιήσει νέα πληρωμή για λογιαριασμό της εταιρείας χωρίς την συγκατάθεση των άλλων δύο ατόμων ώστε να επαληθεύουν την αυθεντικότητα της πληρωμής. (IATA 2019)

2.6 Προστασία απο Hoax Email

Μέτρα Προστασίας για την αντιμετώπιση των Hoax Email

Είναι σημαντικό ο χρήστης να αναφέρει την ηλεκτρονική απάτη προωθώντας το ηλεκτρονικό μήνυμα στην αρμόδια αρχή κατά του ηλεκτρονικού εγκλήματος να αποκλείσει τον αποστολέα και να διαγράψει το ηλεκτρονικό μήνυμα από τον υπολογιστή του.

Θεμιτό είναι , να μην γίνονται αποδεκτά , τα αιτήματα συνδέσεων μέσω επαγγελματικών μέσων δικτύωσης , απο λογαριασμούς χρηστών που ο χρήστης δεν γνωρίζει. Ακόμα και αν αυτοί οι χρήστες έχουν κοινές επαφές με τον παραλήπτη του αιτήματος .

Επιπρόσθετα, είναι αξιοσημείωτος ο κίνδυνος που υφίσταται ο λογαριασμός χρήστη ηλεκτρονικού ταχυδρομείου απο τα online παιχνίδια στον υπολογιστή καθώς κατά την εγγραφή του χρήστη στον εξυπηρετητή του παιχνιδιού , ζητούνται στοιχεία προς καταχώρηση , κωδικοί πρόσβασης , άλλες διευθύνσεις email, κ.α.) Οι επιτιθέμενοι έχουν την δυνατότητα ακόμα και αν κάποιος χρήστης προσέξει κατά την εγγραφή του σε έναν εξυπηρετητή παιχνιδιού , να εισβάλλουν στον υπολογιστή του , μέσω ευπάθειας που βρίσκεται στην ασφάλεια του online παιχνιδιού , γι αυτό είναι σημαντικό ο χρήστης να απενεργοποιεί τα Flash ή τα Java Scripts αν δεν του είναι χρήσιμα απο τα προγράμματα περιήγησης του διαδικτύου.

Για προστασία από τις κακόβουλες επιθέσεις στο ηλεκτρονικό ταχυδρομείο προτείνεται η συχνή αλλαγή των κωδικών και η αποφυγή της χρήσης του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς (προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου, ηλεκτρονικό ταχυδρομείο εργασίας κτλ.).

Στα μηνύματα ηλεκτρονικής απάτης που συνθέτουν οι επιτιθέμενοι, μπορούν να παραποιούν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου του αποστολέα , ώστε να είναι όμοιες με πραγματικές και έμπιστες . Μια προσεκτικότερη όμως εξέταση της διεύθυνσης , θα μπορούσε να φανερώσει αν πρόκειται τελικά για ασφαλή πηγή ή όχι.

Για παράδειγμα, το iatabsp1@gmail.com δεν είναι μια γνήσια διεύθυνση που ανήκει στην IATA. Είναι χρήσιμο απο το παραλήπτη του μηνύματος να ελεγχθούν τυχόν λάθη σε γραμματική και ορθογραφία αφού στις περισσότερες περιπτώσεις τα κακόβουλα μηνύματα συχνά μεταφράζονται από διαφορετικές γλώσσες και υπάρχει πιθανότητα συντακτικών ορθογραφικών και εννοιολογικών λαθών στο μήνυμα.

Προτείνεται στον παραλήπτη ενός κακόβουλου μηνύματος , να αποκλείει τον αποστολέα, και να διαγράφει το μήνυμα. Επίσης αν είναι εφικτό ακόμα και την διακοπή χρήσης της συγκεκριμένης διεύθυνσης ηλεκτρονικού ταχυδρομείου.

Ο χρήστης είναι πολύ σημαντικό να έχει ενεργοποιημένο το τείχος προστασίας και ενημερωμένο το λειτουργικό του συστήματός του Επίσης προτείνεται η χρήση ενός φίλτρου ανεπιθύμητης αλληλογραφίας στο ηλεκτρονικό ταχυδρομείο. Είναι σημαντικό ο χρήστης να εκπαιδευτεί να αναγνωρίζει την ανεπιθύμητη αλληλογραφία, ακόμη και αν φαινομενικά είναι αξιόπιστη. Ιδιαίτερη σημασία , έχει και η ενεργοποίηση προγράμματος anti-malware για το σύστημα του χρήστη

Για μεμονωμένους υπολογιστές προτείνεται η χρήση του τείχους προστασίας λογισμικού, ενώ για δικτυακούς υπολογιστές οι δρομολογητές υλικού.

Επιπρόσθετα, είναι σημαντικό ο χρήστης να εγκαταστήσει και να ενημερώσει το λογισμικό προστασίας από ιούς, το οποίο είναι σχεδιασμένο για την αποτροπή την ενσωμάτωσης προγραμμάτων κακόβουλου λογισμικού στον υπολογιστή. Το λογισμικό προστασίας από ιούς ανιχνεύει , αφοπλίζει και αφαιρεί τον κακόβουλο κώδικα. Ο ιός θα μπορούσε να μολύνει τον υπολογιστή χωρίς αυτό να γίνει αντιληπτό από τον χρήστη.

Για την προστασία του ηλεκτρονικού ταχυδρομείου ο χρήστης μπορεί να εγκαταστήσει λογισμικό Anti-spyware το οποίο πρέπει να είναι συνεχώς ενημερωμένο αν και η πλειονότητα αυτών των λογισμικών έχουν την δυνατότητα της αυτόματης ενημέρωσης.

Με την ανάπτυξη συνδέσεων Internet υψηλής ταχύτητας, πολλοί επιλέγουν να εγκαταλείπουν τους υπολογιστές σε λειτουργία ώστε να διεκπεραιώνουν τα συστήματά τους διάφορες online λειτουργίες. Το μειονέκτημα είναι ότι αυτή η τακτική κάνει τα συστήματα των χρηστών πιο ευπαθή.

Ο λόγος είναι ότι πέρα από την προστασία που προσδίδει το τείχος προστασίας, το οποίο έχει σχεδιαστεί για να αποτρέψει ανεπιθύμητες επιθέσεις, η απενεργοποίηση του υπολογιστή αποκόπτει αποτελεσματικά τη πιθανή σύνδεση ενός εισβολέα - είτε είναι spyware είτε είναι botnet τα οποία χρησιμοποιούν πόρους του υπολογιστή , ώστε να προσεγγίζουν άλλους ανεπιθύμητους χρήστες στο σύστημα. (FBI 2018)

Κεφάλαιο 3
Δημιουργία Hoax Email

Τεχνικές Δημιουργίας Hoax Email

Ο επιτιθέμενος χρησιμοποιεί μια τεχνική που επιτρέπει το όνομα του πραγματικού αποστολέα να είναι καλυμμένο έτσι ώστε το μήνυμα ηλεκτρονικού ταχυδρομείου να φαίνεται ότι έχει σταλθεί από μια έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου. Στις περιπτώσεις αυτές, ο επιτιθέμενος ζητά από τον παραλήπτη εγγράφως και μέσα στο μήνυμα , να απαντήσει το θύμα , σε μια άλλη διεύθυνση ηλεκτρονικού ταχυδρομείου και όχι στη πραγματική. Επίσης ο επιτιθέμενος μπορεί να χρησιμοποιεί πλαστά έγγραφα που φέρουν επίσημα λογότυπα εταιρειών πιθανότατα αντιγραμμένα από την επίσημη ιστοσελίδα της εκάστοτε εταιρείας. Αυτά τα έγγραφα φαίνονται νόμιμα τιμολόγια και μπορούν εύκολα να ξεγελάσουν το θύμα. Το περιεχόμενο του μηνύματος του επιτιθέμενου μπορεί να προτείνει στο θύμα να ανοίξει έναν σύνδεσμο. Αφού λοιπόν το θύμα επιλέξει τον σύνδεσμο και τον ανοίξει μεταφέρεται σε έναν ψεύτικο ιστότοπο του εισβολέα (όπου μοιάζει με τον κανονικό). Στη συνέχεια ζητούνται από το θύμα τα προς καταχώρηση στοιχεία σύνδεσής του , έτσι ώστε ο επιτιθέμενος να υποκλέψει τα διαπιστευτήρια σύνδεσης του θύματος και να έχει πρόσβαση στο λογαριασμό του. (IATA 2019)

Περιγραφή συχνών Τύπων Hoax Email

Παρακάτω περιγράφονται συχνοί τύποι μηνυμάτων διαδικτυακής ηλεκτρονικής απάτης. Αναλύεται ο τρόπος λειτουργίας τους , οι επιπτώσεις που προκαλούν , ο τρόπος ανίχνευσής τους , καθώς και με ποιο τρόπο επιτυγχάνεται η πρόληψη και η προστασία από τα μηνύματα αυτά.

3.1 Malware

Τι είναι Malware

Το κακόβουλο λογισμικό "malware ", αναφέρεται σε ένα είδος προγράμματος υπολογιστή που έχει σχεδιαστεί για να μολύνει έναν υπολογιστή χρήστη και να τον βλάψει με πολλούς τρόπους. Το κακόβουλο λογισμικό μπορεί να μολύνει υπολογιστές και συσκευές με διάφορους τρόπους και έρχεται σε διάφορες μορφές, Έρχεται σε μια ευρεία ποικιλία

απο μορφές, συμπεριλαμβανομένων των ιών, των σκουληκιών, των προγραμμάτων Δούρειου ίππου, του λογισμικού υποκλοπής spyware, του ransomware και του λογισμικού botnet - τα οποία μπορούν να θέσουν σε κίνδυνο τον υπολογιστή αλλά και τα προσωπικά δεδομένα των χρηστών.
Η επίσκεψη σε μολυσμένους ιστότοπους, το άνοιγμα συνημμένων ηλεκτρονικών μηνυμάτων και η εισαγωγή αφαιρούμενων μονάδων δίσκου είναι μερικοί από τους συνήθεις τρόπους με τους οποίους εξαπλώνεται το κακόβουλο λογισμικό. (Kaspersky 2018)

3.1.1 Επιπτώσεις Επιθέσεων Malware

Οι επιτιθέμενοι απλώς στέλνουν ένα μήνυμα ανεπιθύμητης αλληλογραφίας σε έναν στόχο ή μια ομάδα στόχων και δεν χρειάζεται να βασίζονται σε έμμεσες μεθόδους όπου ο στόχος ενδέχεται να μην επισκεφτεί έναν μολυσμένο ιστότοπο ή να μην κάνει κλικ σε μια κακόβουλη διαφήμιση banner. Πρόκειται για ένα άμεσο κανάλι προς έναν τελικό χρήστη, ο οποίος, αν μπορεί να πειστεί να ανοίξει ένα συνημμένο ή να κάνει κλικ σε ένα σύνδεσμο του ηλεκτρονικού ταχυδρομείου, μπορεί να παρακάμψει δικτυακά επίπεδα ασφαλείας του εισβολέα κερδίζοντας με αυτό τον τρόπο ο εισβολέας στον επιδιωκόμενο στόχο πρόσβαση εύκολα άμεσα και γρήγορα. Τα αποτελέσματα επιτυχημένων επιθέσεων κακόβουλου λογισμικού μπορεί να κυμαίνονται από το κλείσιμο του υπολογιστή , την απόκτηση και πρόσβαση σε κωδικούς , τη πρόσβαση σε πληροφορίες λογαριασμού μέχρι και την υποκλοπή προσωπικών στοιχείων.

Αυτή η άμεση πρόσβαση στον επιδιωκόμενο στόχο είναι και ο μόνος λόγος όπου οι επιχειρήσεις θα πρέπει να λαμβάνουν σοβαρά υπόψιν τους τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Οι επιχειρήσεις γίνονται στόχοι τακτικά από κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. (ESET 2019)

Πρόσφατα ο Olympic Destroyer (ο ολυμπιακός καταστροφέας) που διακινείται στο διαδίκτυο μέσω malware , αυτό που κάνει είναι ότι εάν οι παραλήπτες ανοίξουν το συνημμένο αρχείο και ενεργοποιήσουν τη λειτουργία των μακροεντολών, ο olympic destroyer εγκαθίσταται στο απομακρυσμένο σύστημα του θύματος εκτελώντας ένα σύνολο εντολών στο σύστημα του θύματος.

Μέρος απο τις λειτουργείες του olympic destroyer είναι επίσης και να παραβιάζει τους λογαριασμούς διαχείρισης του ηλεκτρονικού υπολογιστή , να υποκλέπτει κωδικούς πρόσβασης που είναι αποθηκευμένοι σε προγράμματα περιήγησης ιστού, όπως Internet Explorer, Chrome και Firefox. Μόλις αποκτηθούν αυτοί οι κωδικοί πρόσβασης από το σύστημα προορισμού, χρησιμοποιούνται από τους επιτιθέμενους.

Στην πραγματικότητα, το πρώτο εξάμηνο του 2017, περισσότερο από το 11% των χρηστών είχαν τουλάχιστον ένα κακόβουλο μήνυμα ηλεκτρονικού ταχυδρομείου που τους στάλθηκε. Αυτός είναι ένας στους εννέα χρήστες ηλεκτρονικού ταχυδρομείου. Ο αριθμός αυτός παρουσίασε ανοδική πορεία καθώς προχώρησε το έτος.
Τον Ιανουάριο, μόνο ένας στους 12 χρήστες (8,6%) έλαβε κάποιο κακόβουλο μήνυμα ηλεκτρονικού ταχυδρομείου από αυτούς. Μέχρι τον Μάιο, ο αριθμός αυτός είχε ανέβει σε περισσότερους από έναν στους επτά (15%) και παρέμεινε σε αυτό το επίπεδο μέχρι τον Ιούνιο. Ωστόσο, ανεξάρτητα από το ποσοστό , χρειάζεται μόνο ένας χρήστης να πέσει θύμα μιας επίθεσης και η δικτυακή ασφάλεια επιτυχώς έχει παραβιαστεί

Τρόποι Ανίχνευσης Malware

Η προσωπική επαγρύπνηση είναι το πρώτο επίπεδο προστασίας από κακόβουλο λογισμικό, αλλά η προσοχή απλά δεν αρκεί. Επειδή η ασφάλεια των επιχειρήσεων δεν είναι τέλεια, μερικές φορές οι λήψεις μηνυμάτων από νόμιμους ιστότοπους μπορεί μερικές φορές να έχουν συνημμένο κακόβουλο λογισμικό. Αυτό σημαίνει ότι ακόμη και ο πιο συνετός χρήστης κινδυνεύει.

Επειδή οι διανομείς κακόβουλων προγραμμάτων αλλάζουν πάντοτε τις μεθόδους τους, το αποτελεσματικό λογισμικό αντιμετώπισης malware χρησιμοποιεί πολλαπλές μεθόδους ανίχνευσης.

Κάποιες απο τις μεθόδους ανίχνευσης περιλαμβάνουν: ανίχνευση γνωστού κακόβουλου λογισμικού απο συστήματα που βασίζονται στη φήμη της επικινδυνότητας κακόβουλων γνωστών προγραμμάτων , την ανίχνευση ύποπτης συμπεριφοράς, τον έλεγχο του πηγαίου κώδικα του κακόβουλου λογισμικού, την εκτέλεσή του σε προστατευμένο περιβάλλον. Αυτός είναι ο λόγος για τον οποίο υπολογιστές, καθώς και συσκευές όπως τα tablet και τα smartphones, χρειάζονται λογισμικό anti-malware, το οποίο πρέπει επίσης να ενημερώνεται και τακτικά για την καταπολέμηση των προαναφερθέντων απειλών.

Τεχνικές Δημιουργίας Malware

Οι προγραμματιστές κακόβουλου λογισμικού χρησιμοποιούν συχνά την λεγόμενη "κοινωνική μηχανική" για να εξαπατήσουν τους χρήστες ώστε να μολύνουν τους ηλεκτρονικούς υπολογιστές τους.

Για παράδειγμα, οι χρήστες μπορούν να ξεγελαστούν από προγράμματα ηλεκτρονικού "ψαρέματος" (phishing) που παραδίδουν προσβληθέντα από ιούς συνημμένα αρχεία ή οδηγούν σε ψεύτικους ιστότοπους με σκοπό να φαίνονται νόμιμοι.

Ένας από τους πιο δημοφιλείς τρόπους για την εξάπλωση κακόβουλου λογισμικού είναι μέσω ηλεκτρονικού ταχυδρομείου, το οποίο μήνυμα μπορεί να είναι συγκαλυμμένο , ώστε να φαίνεται σαν να προέρχεται από μια γνωστή εταιρεία όπως μια τράπεζα ή ένα προσωπικό ηλεκτρονικό μήνυμα από έναν φίλο.

Διανομή Κακόβουλου Λογισμικού Malware

Η συντριπτική πλειοψηφία , των κακόβουλων ηλεκτρονικών μηνυμάτων , επιχειρεί να προσελκύσει τον χρήστη μέσω κοινωνικά διαμορφωμένων θεματικών γραμμών ή και θεματικών μηνυμάτων για να εξαπατήσει τον χρήστη να ανοίξει ένα κακόβουλο συνημμένο.

Η κορυφαία και συχνή θεματολογία των παραπλανητικών μηνυμάτων επικεντρώνονται γύρω από ενημερωτικά έγγραφα , δελτία όπως νέα νομοσχέδια , λογαριασμοί πληρωμών , αρχεία pdf και αναφορές αποστολής δεμάτων.

Υπάρχουν γενικά δύο τρόποι με τους οποίους διανέμεται κακόβουλος κώδικας απο ένα μήνυμα ηλεκτρονικού ταχυδρομείου: Είτε με μια διεύθυνση URL στο περιεχόμενο του μηνύματος είτε με ένα συνημμένο ηλεκτρονικού ταχυδρομείου.

Τυπικό Infection Process ενός email Malware

1 Ένας εισβολέας στέλνει ένα τυπικό email, μεταμφιεσμένο ως ένα Τιμολόγιο , ή Δελτίο παράδοσης ή σκαναρισμένο έγγραφο.

2. Το email περιέχει ένα συνημμένο αρχείο , συνήθως ένα αρχείο JavaScript (JS) ή ένα αρχείο office που περιέχει μακροεντολές.

3. Όταν το αρχείο θα εκκινηθεί απο το χρήστη, το ίδιο το αρχείο:

α) ή θα προτρέψει το χρήστη να εκτελέσει μια μακροεντολή.
β) ή θα εκκινήσει το PowerShell για να κατεβάσει ο χρήστης το payload και να το εκτελέσει.

4. Το payload είναι συνήθως ransomware, αλλά μπορεί επίσης να είναι ή ένας Infostealer Snifula ένα Trojan horse που κλέβει πληροφορίες απο τον υπολογιστή που έχει μολυνθεί κάνοντας τον υπολογιστή να εκτελεί αρχεία από το Internet.
Με τα χρόνια, για να βελτιώσουν τις πιθανότητές να παραδώσουν το κακόβουλο λογισμικό τους, οι επιτιθέμενοι στα θύματά τους , ενώ αρχικά κινούνταν στη διανομή (και μη ενδεχόμενη εκτέλεση) του payload στο παραλήπτη ,πλέον προτιμούν την ενσωμάτωση προγραμμάτων λήψης στα μηνύματά τους.

Γενικά , τα προγράμματα λήψης είναι μικρού μεγέθους προγράμματα scripts (Java ή VBS) που, όταν εκτελούνται, μπορούν να κάνουν λήψη περαιτέρω αρχείων.
Κατά το πρώτο εξάμηνο του 2017, το 53,3% των κακόβουλων συνημμένων ήταν script ή αρχεία Office φορτωμένα με macro-εντολές , τα οποία έχουν σχεδιαστεί , για τη λήψη περαιτέρω κακόβουλου λογισμικού , όταν αυτά εκτελούνται από το χρήστη.

Η δημοτικότητα των προγραμμάτων λήψης οφείλεται σε απλούς λόγους:

Η λήψη ενός payload ξεχωρίζει απο τη διαδικασία απόκτησης και εκτέλεσης κακόβουλου φορτίου από το ηλεκτρονικό ταχυδρομείο. Μόλις ξεκινήσει η δέσμη ενεργειών, όλη η κίνηση του δικτύου για να λάβει το payload διαχωρίζεται τελείως από τα πρωτόκολλα ηλεκτρονικού ταχυδρομείου και επομένως από τις ηλεκτρονικές προστασίες. Το ηλεκτρονικό ταχυδρομείο μπορεί να παραδώσει το πρόγραμμα λήψης επιτυχώς , αλλά το πρόγραμμα λήψης θα ολοκληρώσει το βασικότερο σκέλος της επίθεσης στο θύμα.

Ο server μπορεί να ελέγξει την IP του προγράμματος λήψης και να στείλει local payloads, ή και όχι (αν ο προσβεβλημένος υπολογιστής δεν πληρεί ορισμένα κριτήρια).

Ο εισβολέας μπορεί να αλλάξει γρήγορα το τελικό payload σε περίπτωση που εντοπιστεί απο προγράμματα προστασίας. Όσοι χρήστες προσβάλλονται από το πρόγραμμα λήψης του εισβολέα θα λάβουν ένα νέο και μη ανιχνευμένο payload (απο τα προγράμματα προστασίας) , αυξάνοντας ο εισβολέας αφενός τον αριθμό των μολύνσεων στο σύστημα του θύματος και αφετέρου τη ποσοστιαία πιθανότητα να προσβληθεί με ιό το σύστημα του θύματος επιτυχώς. (Unuchek 2017 , Sinitsyn 2017 , Parinov 2017 , Liskin 2017) , (Price 2017) , (Symantec 2017).

3.1.2 Προστασία από Malware

Η προστασία απο τα malware χρησιμεύει γιατί η επίσκεψη σε μολυσμένους ιστότοπους, το άνοιγμα συνημμένων ηλεκτρονικών μηνυμάτων και η εισαγωγή αφαιρούμενων μονάδων δίσκου είναι μερικοί από τους συνήθεις τρόπους με τους οποίους εξαπλώνεται το κακόβουλο λογισμικό.

Η προσωπική επαγρύπνηση και τα εργαλεία προστασίας είναι οι τρόποι με τους οποίους προστατευόμαστε απο τα malware.

Μηνύματα ηλεκτρονικού ταχυδρομείου που ζητούν απο το χρήστη να δώσει κωδικούς πρόσβασης ή μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από φίλους, επιχειρήσεις ή ιδιώτες αλλά έχουν μόνο ένα γραπτό μήνυμα ακολουθούμενο από μια σύνδεση ιστότοπου πιθανότατα πρόκεινται για malware.

Η προστασία από κακόβουλο λογισμικό παρέχει το δεύτερο βασικό επίπεδο προστασίας για τον υπολογιστή ή το δίκτυό μας.
Ένα ισχυρό πακέτο λογισμικού εντοπισμού ιών είναι το κύριο συστατικό των τεχνολογικών αμυντικών που πρέπει να διαθέτει κάθε προσωπικό και επιχειρησιακό σύστημα υπολογιστών.

Η καλά σχεδιασμένη προστασία από ιούς έχει πολλά χαρακτηριστικά. Ελέγχει κάθε νέο πρόγραμμα που έχει ληφθεί για να βεβαιωθεί ότι δεν είναι κακόβουλο λογισμικό.
Ελέγχει περιοδικά τον υπολογιστή για να ανιχνεύσει όπως και να απεγκαταστήσει οποιοδήποτε κακόβουλο λογισμικό μπορεί να έχει εγκατασταθεί. Ενημερώνεται τακτικά για να αναγνωρίζει τις τελευταίες απειλές.

Η καλή προστασία από ιούς μπορεί επίσης να αναγνωρίσει – όπως και να προειδοποιήσει - ακόμη και για παλαιότερες άγνωστες απειλές κακόβουλου λογισμικού, με βάση τεχνικά χαρακτηριστικά (όπως η απόπειρα «απόκρυψης» τμημάτων κώδικα των αρχείων σε έναν σύστημα υπολογιστή) που είναι χαρακτηριστικό του κακόβουλου λογισμικού.

Επιπλέον, το ισχυρό λογισμικό εντοπισμού ιών εντοπίζει και προειδοποιεί για ύποπτες ιστοσελίδες, ειδικά εκείνες που μπορεί να σχεδιάζονται για "phishing" με στόχο οι χρήστες να εισάγουν κωδικούς πρόσβασης ή αριθμούς λογαριασμών. Η ισχυρή προστασία κακόβουλων προγραμμάτων προστατεύει ειδικά λογαριασμούς τραπεζών χρηστών.

Αυτά τα εργαλεία προστασίας , προστατεύουν τις πληροφορίες των λογαριασμών και μπορούν επίσης να παρέχουν εργαλεία διαχείρισης κωδικών πρόσβασης, έτσι ώστε αν ξεχαστούν κωδικοί πρόσβασης των λογαριασμών αυτών, μέσα απο ασφαλές περιβάλλον να πραγματοποιείται η ανάκτησή τους , χωρίς να γίνεται παραβίαση της διαδικασίας και άρα η υποκλοπή αυτών.

Ένας συνδυασμός προσωπικής ευαισθητοποίησης και καλά σχεδιασμένων εργαλείων προστασίας θα καταστήσει τον υπολογιστή ασφαλέστερο . (Kaspersky 2019)

3.4 Bec Scam

Τι είναι Bec Scam

Οι κυβερνοεγκληματίες στο κυβερνοχώρο εξαπολύουν τις επιθέσεις τους με τέτοιο τρόπο όπως λειτουργεί κάθε επιχειρηματίας στο χώρο των επιχειρήσεων: θέλουν το μέγιστο κέρδος με ελάχιστη επένδυση. Μια πρόσφατη τάση μεταξύ των επιτιθέμενων ώστε να εκπληρώσουν αυτό το στόχο είναι η επίθεση τύπου Business Email Compromise (BEC), γνωστή και ως "CEO Fraud". Αυτός ο τύπος απάτης είναι πολύ κερδοφόρος δεδομένου αν η μία επίθεση είναι επιτυχής τότε είναι ιδιαίτερα αποδοτική και επικερδής για τους επιτιθέμενους. Η επίθεση αυτή απευθύνεται σε επιχειρήσεις που συνεργάζονται με ξένους προμηθευτές και επιχειρήσεις που εκτελούν τακτικά πληρωμές μέσω τραπεζικών εμβασμάτων στο διαδίκτυο. Οι επιθέσεις τύπου BEC εξελίσσονται καθημερινά για να παίρνουν διάφορες μορφές.

Συνήθως ο επιτιθέμενος , μιμείται ένα στέλεχος της εταιρείας όταν επιτίθεται , και ζητάει επείγουσα μεταφορά χρημάτων απο υπάλληλο του τμήματος λογιστηρίου σε κάποιον λογαριασμό.

Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται συχνά σε έναν υπάλληλο της εταιρείας ή, σε ορισμένες περιπτώσεις, απευθείας σε μια τράπεζα που κατέχει τους λογαριασμούς της στοχευόμενης εταιρείας με στόχο να πραγματοποιήσει κατάθεση ή ανάληψη ποσών. Τα μηνύματα αυτά έχουν τον “αέρα” συνήθως του “επείγοντος” και αποστέλλονται λίγο πριν στο τέλος της εργάσιμης μέρας για την εταιρεία , ώστε να προβεί ο παραλήπτης το συντομότερο δυνατό σε καταθέσεις ή μεταφορές ποσών τραπεζικών λογαριασμών.

3.4.1 Επιπτώσεις επιθέσεων Bec Scam

Σύμφωνα με πρόσφατη ανάλυση του FBI, απώλειες ύψους 5 δισεκατομμυρίων δολαρίων σημειώθηκαν μεταξύ του τέλους του 2013 και του τέλους του 2016. Δεν πρόκειται μόνο για μεγάλες επιχειρήσεις, καθώς οι επιχειρήσεις όλων των μεγεθών έχουν αναφέρει απόπειρες επιθέσεων τέτοιου είδους. Το 2017, περίπου 8.000 επιχειρήσεις στοχοποιήθηκαν συνολικά με απάτες τύπου BEC σε ένα μόνο μήνα. Κατά μέσο όρο, αποστέλλονταν 5,2 BEC μηνύματα ηλεκτρονικού ταχυδρομείου σε έναν οργανισμό για κάθε μήνα.

Το σενάριο

Ένας υπάλληλος εργάζεται σε μια επιχείρηση ως λογιστής της εταιρείας. Είναι σχεδόν 5:00 μ.μ. την Παρασκευή, πριν από ένα τριήμερο Σαββατοκύριακο και είναι ο τελευταίος που έχει απομείνει απο το τμήμα με στόχο να διεκπεραιώσει και τις τελευταίες του αρμοδιότητες. Ένας εισβολέας που κατάφερε επιτυχώς να παραβιάσει το λογαριασμό του εταιρικού ηλεκτρονικού ταχυδρομείου ενός απο τα σημαντικά στελέχη της εταιρείας , στέλνει απο το λογαριασμό του , ένα μήνυμα με θέμα "ΕΠΕΙΓΟΝ" προς το λογιστή της εταιρείας. Διαβάζοντας το περιεχόμενο του μηνύματος ο λογιστής , βλέπει το στέλεχος της εταιρείας να τον ρωτάει , αν βρίσκεται ακόμα στο γραφείο του (παρόλο που είναι ώρα μη εργάσιμη και οι περισσότεροι από τους εργαζόμενους απουσιάζουν). Ο λογιστής φυσικά, απαντάει ότι βρίσκεται , και ρωτάει τι θα μπορούσε να κάνει για να βοηθήσει το προϊστάμενό του. Μετά απο πολύ μικρό χρονικό διάστημα , λαμβάνει ο

λογιστής ένα μήνυμα ηλεκτρονικού ταχυδρομείου απο το στέλεχος της εταιρείας , του οποίου το περιεχόμενο , εμφανίζεται να έχει συνταχθεί βιαστικά, με λάθη ορθογραφίας και μορφοποίησης, ώστε να φαίνεται ότι το στέλεχος βιάζεται να το συντάξει γρήγορα. Το περιεχόμενο του μηνύματος , περιγράφει ότι επειδή , δεν έχει καταβληθεί ακόμη , η πληρωμή για τον κύριο προμηθευτή της εταιρείας , ο προμηθευτής απειλεί να παρακρατήσει τις απαραίτητες προμήθειες αν δεν πραγματοποιηθεί η εξόφληση αμέσως σε κάποιον λογαριασμό του. Αυτό θα μπορούσε να επηρεάσει τα σχέδια παραγωγής και ανάπτυξης της εταιρείας.
Έτσι το στέλεχος περιλαμβάνει στο μήνυμα λεπτομέρειες σχετικά με το οφειλόμενο ποσό, τους τραπεζικούς λογαριασμούς του προμηθευτή για πληρωμή , και ρωτά τον λογιστή , αν μπορεί να ξεκινήσει μια τραπεζική μεταφορά αμέσως, πριν κλείσουν οι τράπεζες για Σαββατοκύριακο.

Τύποι Bec Scam

CEO fraud

Η πιο διαδεδομένη απάτη τύπου BEC είναι αυτή του Διευθύνοντος Συμβούλου της εταιρείας. Σε αυτή τη μορφής επίθεση, ο επιτιθέμενος έχει παραβιάσει επιτυχώς τη διεύθυνση του ηλεκτρονικού ταχυδρομείου του CEO. Ο εισβολέας υποδυόμενος τον CEO θα στείλει έπειτα οδηγίες ηλεκτρονικού ταχυδρομείου στους υπαλλήλους ή στην οικονομική υπηρεσία που θα καθοδηγεί τη μεταφορά κεφαλαίων για την άμεση πληρωμή ενός λογαριασμού. Το σίγουρο σε αυτές τις περιπτώσεις είναι ότι πάντα θα υπάρχει η επισημότητα στο μήνυμα ηλεκτρονικού ταχυδρομείου που θα τονίζει την ανάγκη της επείγουσας δράσης απο μεριάς του παραλήπτη.

Bogus invoice scam

Η απάτη των εσφαλμένων τιμολογίων. Στο πλαίσιο αυτής της δραστηριότητας BEC ο κυβερνοεγκληματίας αφού παραβιάσει τους διευθυντικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου και τους λογαριασμούς υπαλλήλων που ασχολούνται με το εκτελεστικό κομμάτι , της αποπληρωμής των οικονομικών υποχρεώσεων της εταιρείας, ο ίδιος , θα εξετάσει για τυχόν λογαριασμούς που πληρώνονται σύντομα και συχνά. Έπειτα επικοινωνεί με το τμήμα οικονομικών και με εντολή του , τα αρμόδια όργανα αλλάζουν τα στοιχεία των τραπεζικών λογαριασμών. Αυτό σημαίνει ότι μόλις πληρωθεί ο λογαριασμός καταβάλλεται στον τραπεζικό λογαριασμό του εισβολέα χωρίς να γνωρίζει κανείς τι έχει προηγηθεί.

Account Compromise

Παραβίαση λογαριασμού. Ένας λογαριασμός ηλεκτρονικού ταχυδρομείου ενός υπαλλήλου εντός του οργανισμού έχει παραβιαστεί και στη συνέχεια χρησιμοποιείται για την υποβολή αιτημάτων προς πληρωμή τιμολογίων προς διάφορους λογαριασμούς. Τα μηνύματα ηλεκτρονικού ταχυδρομείου αποστέλλονται σε πολλούς προμηθευτές που βρίσκονται στη λίστα επαφών της επιχείρησης.

Attorney Impersonation

Η απάτη του φερόμενου ως δικηγόρου. Σε αυτή τη φάση επίθεσης τύπου BEC , ο εισβολέας θα επικοινωνήσει μέσω ηλεκτρονικού ταχυδρομείου με τους εργαζόμενους

της εταιρείας , ή με τους διευθυντές της , υποδυόμενος τον δικηγόρο ή τον αντιπρόσωπο δικηγορικού γραφείου , όπου ισχυρίζεται ότι χειρίζεται εμπιστευτικά ευαίσθητα και κρίσιμα θέματα για την ασφάλεια της εταιρείας. Αυτή η επικοινωνία γίνεται , συνήθως είτε μέσω τηλεφώνου είτε μέσω ηλεκτρονικού ταχυδρομείου, ώστε να πιέσει ο εισβολέας τον παραλήπτη , να ενεργήσει γρήγορα ή κρυφά κατά το χειρισμό της μεταφοράς χρημάτων.

Data Theft

Η υποκλοπή πληροφοριών . Αυτού του είδους η επίθεση , αναφέρεται ως η παραβίαση των λογαριασμών ηλεκτρονικού ταχυδρομείου των υπαλλήλων μιας εταιρείας , που σχετίζονται με τη διαχείριση κρίσιμων θεμάτων για την εξέλιξη της εταιρείας. Η παραβίαση αυτών των λογαριασμών δεν γίνεται απο τον εισβολέα , για να πραγματοποιηθούν μεταφορές κεφαλαίων , αλλά για υποκλέψουν προσωπικές πληροφορίες , όπως προσωπικά στοιχεία υπαλλήλων και στελεχών. (Benhayon 2017)
Πέρα από τις τραπεζικές μεταφορές μία από τη πιο ενδιαφέρουσα εξέλιξη στις επιθέσεις τύπου BEC είναι οι επιθέσεις στις οποίες οι απατεώνες προσπαθούν να αποκτήσουν προσωπικά στοιχεία απο τα θύματα , σε αντίθεση με την άμεση κλοπή χρημάτων.

Σε μια οργανωμένη επίθεση BEC στις αρχές του 2017 στην Αμερική, οι εισβολείς επικεντρώνονταν στο να υποδύονται τους εργαζομένους , της φορολογικής υπηρεσίας στην οποία οι φορολογούμενοι κατέθεταν τη φορολογική δήλωσή τους. Οι εισβολείς , απο όλο τον οργανισμό (αφού τον παραβίασαν) συγκέντρωναν ευαίσθητες πληροφορίες (προσωπικά δεδομένα) απο όλους τους φορολογούμενους με στόχο , την υποκλοπή των προσωπικών δεδομένων , για μελλοντικές περαιτέρω επιθέσεις σε Αμερικανούς πολίτες.

Τεχνικές Δημιουργίας Bec Scam

Οι εισβολείς θα χρησιμοποιήσουν αρκετά απλές, αλλά αποτελεσματικές τεχνικές ώστε να αποφευχθεί η οποιαδήποτε υποψία απο μεριάς του θύματος ότι πρόκειται για επίθεση τύπου BEC. Έτσι θα εξασφαλίσουν ότι τα θύματά τους θα ενεργήσουν όσο πιο γρήγορα γίνεται χωρίς δεύτερη σκέψη ή περαιτέρω επαλήθευση.

Μέσω της τεχνικής Spoofing ή typosquatting , οι επιτιθέμενοι συχνά παραποιούν τα domains (τομείς) των διευθύνσεων αποστολής των μηνυμάτων τους , ώστε να μοιάζουν με επίσημες διευθύνσεις ηλεκτρονικού ταχυδρομείου οργανισμών που σκοπεύουν να στοχεύσουν. Αυτοί οι τομείς μπορεί να έχουν έναν ή δύο χαρακτήρες παραπάνω απο ότι θα έπρεπε ή να είναι αντιστραμμένοι, όπως για παράδειγμα αντί να είναι "amce_inc.com" για τη νόμιμη επιχείρηση, να είναι "acme_inc.com".

Σε άλλες, (σπάνια περιπτώσεις), οι εισβολείς μπορούν να χρησιμοποιήσουν διαφορετικό domain ή απλώς να προσθέσουν λέξεις κατά τη διαμόρφωση του domain αποστολέα , όπως για παράδειγμα "acme_inc_sales.com".

Οι επιτιθέμενοι χρησιμοποιούν έναν τόνο επείγουσας ανάγκης στα μηνύματά τους, ζητώντας έτσι απο τα υποψήφια θύματά τους να διεκπεραιώσουν οποιαδήποτε αίτημά τους το συντομότερο δυνατό.

Δηλώνουν στα ηλεκτρονικά μηνύματα απάτης , ότι ο Διευθύνων Σύμβουλος ή ο

Οικονομικός Διευθυντής της εταιρείας βρίσκονται σε μια κρίσιμη συνάντηση και ότι δεν μπορούν να διακόψουν , για την έγκριση του αιτήματος που ο εισβολέας αιτείται.

Οι επιτιθέμενοι σε άλλη περίπτωση , χρησιμοποιούν μια συσκευή για να γράψει το ηλεκτρονικό ταχυδρομείο, τη φημισμένη και συχνά χρησιμοποιούμενη φράση για παράδειγμα "αποστέλλεται από το iPad μου", αντί της εταιρικής υπογραφής του ηλεκτρονικού ταχυδρομείου. Αυτό το τέχνασμα που χρησιμοποιείται αρκετά συχνά , είναι ιδιαίτερα αποτελεσματικό, επειδή υπονοείται ότι το μήνυμα ηλεκτρονικού ταχυδρομείου αποστέλλεται από μια κινητή συσκευή του αποστολέα, αποφεύγοντας σε οποιαδήποτε γλώσσα, τα ορθογραφικά λάθη ή την νόμιμη υπογραφή ηλεκτρονικού ταχυδρομείου, τα οποία συνήθως ενεργοποιούν την αναγνώριση μηνυμάτων ηλεκτρονικού "ψαρέματος" (phishing) απο διάφορα φίλτρα προγραμμάτων. Αυτή η τεχνική βοηθά επίσης τον επιτιθέμενο να ενισχύσει στο μήνυμά του την αίσθηση του επείγοντος και του κρίσιμου αιτήματος προς διεκπεραίωση απο τον παραλήπτη , καθώς σε διαφορετική περίπτωση ο αποστολέας θα μπορούσε να μεταβεί στο γραφείο του. Οι επίδοξοι εισβολείς χρησιμοποιούν τεχνικές κοινωνικής μηχανικής για να μάθουν πότε τα στελέχη μεταβαίνουν στο χώρο της εργασίας, καθιστώντας την απάτη τους πιο αξιόπιστη στο θύμα τους.

Επίσης οι κυβερνοεγκληματίες προκειμένου να βεβαιωθούν ότι δεν θα κινήσουν υποψίες στα υποψήφια θύματά τους , ζητούν νόμιμα ποσά κατά τις μεταφορές χρημάτων σε τραπεζικούς λογαριασμούς, προκειμένου να αποφευχθεί η αμφιβολία στην αυθεντικότητα του μηνύματος.

Εξετάζοντας το περιεχόμενο των ηλεκτρονικών μηνυμάτων απάτης τύπου BEC, γενικά το κυρίαρχο μοτίβο που παρατηρείται στις υποκείμενες γραμμές τείνει να φέρει μια αίσθηση επείγουσας ανάγκης, απαιτώντας άμεση ανταπόκριση και δράση απο το θύμα, με την ελπίδα ότι ο παραλήπτης θα εξαναγκαστεί να ενεργήσει γρήγορα χωρίς να σκεφτεί πάρα πολύ, για το ποιος είναι ο αποστολέας του μηνύματος και ποιο είναι το αίτημα προς διεκπεραίωση. (Fraud Watch International 2016)

3.4.2 Προστασία από Bec Scam

Εκπαίδευση του προσωπικού για την αναγνώριση μηνυμάτων απο επιθέσεις τύπου BEC.

Στενή παρακολούθηση των διευθύνσεων ηλεκτρονικού ταχυδρομείου της εισερχόμενης αλληλογραφίας , ώστε να αποφευχθούν τυχόν φαινόμενα της εξαπάτησης από τη πλαστογράφηση των διευθύνσεων.

Είναι αναγκαία η αμφισβήτηση μηνυμάτων ηλεκτρονικού ταχυδρομείου , που αιτούνται σε αυτά γρήγορες ενέργειες, ανεξάρτητα από το αν φαίνονται ύποπτα ή όχι. Ειδικότερα εάν στο μήνυμα δεν προβλέπονται να ακολουθούνται οι κανονικές διαδικασίες.

Πριν απο οποιαδήποτε συναλλαγή πρέπει να πραγματοποιείται τηλεφωνική κλήση προς τα εμπλεκόμενα μέρη για επαλήθευση της ταυτότητας του νόμιμου επιχειρηματικού εταίρου ή προμηθευτή.

Επαλήθευση δύο ή περισσότερων επιπέδων πριν την κατάθεση τραπεζικών εμβασμάτων σε λογαριασμούς.

Ενέργειες θύματος σε περίπτωση επιτυχούς επίθεσης Bec Scam

Απόδειξη μιας επιτυχημένης επίθεσης τύπου BEC είναι όταν εμφανίζονται στην αναφορά της πιστωτικής έκθεσης του θύματος αναίτιες κινήσεις στο τραπεζικό λογαριασμό του ή να μην εκτελούνται πάγιες εντολές προς τη τράπεζα , αυτό θα μπορούσε να σημαίνει ότι έχει παραβιαστεί ο τραπεζικός λογαριασμός και όλα τα προσωπικά στοιχεία του θύματος απο τον εισβολέα.

Εάν το θύμα έχει ήδη απαντήσει σε μια επίθεση τύπου BEC , πρέπει να γίνει τερματισμός αμέσως οποιασδήποτε περαιτέρω επικοινωνίας.

Γίνεται επικοινωνία με τη τράπεζα για ακύρωση όλων των συχνών επαναλαμβανόμενων πληρωμών.

Επίσης για το συμβάν πρέπει να ενημερώνονται επίσης και οι αρμόδιες αρχές κατά του ηλεκτρονικού και οικονομικού εγκλήματος.

3.5 Phishing

Τι είναι Phishing

Το ηλεκτρονικό "ψάρεμα" (phishing) είναι η πλαστογράφηση ιστότοπων ή μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποσκοπούν στην εξαπάτηση των χρηστών με στόχο να υποκλαπούν από τον χρήστη , ευαίσθητες πληροφορίες του, όπως διαπιστευτήρια, προσωπικά στοιχεία , στοιχεία λογαριασμών.
Είναι μια από τις σοβαρές απειλές για την ασφάλεια στο Διαδίκτυο.
Καθώς η προσβασιμότητα στο Διαδίκτυο συνεχίζει να αυξάνεται και καθώς η επιτήδευση των επιθέσεων ηλεκτρονικού "ψαρέματος" εξακολουθεί να βελτιώνεται , οι χρήστες του διαδικτύου κάθε ηλικίας είναι όλο και πιο ευάλωτοι σε απειλές τύπου phishing.

3.5.1 Επιπτώσεις Επιθέσεων Phishing

Ένα θύμα αν υποπέσει σε μια απόπειρα ηλεκτρονικού "ψαρέματος" μπορεί να οδηγηθεί σε απώλεια οικονομικών πόρων, υποκλοπή προσωπικών δεδομένων και παραβίαση του συστήματός του.

Τα εμπορικά σήματα και νόμιμα λογότυπα εταιρειών επίσης , γίνονται συχνά στόχος απο επιτιθέμενους , όταν εκκινήσουν κάποια καμπάνια phishing στο διαδίκτυο.
Παρόλο που οι επιθέσεις ηλεκτρονικού "ψαρέματος" απευθύνονται κατά κύριο λόγο σε συγκεκριμένες ομάδες χρηστών , τελικά φαίνεται ότι τα θύματα απο επιθέσεις απάτης ηλεκτρονικού ταχυδρομείου , να ανέρχονται αθέλητα και αναπόφευκτα σε μεγαλύτερη μερίδα χρηστών του διαδικτύου.

Οι phishers πριν ξεκινήσουν μια επίθεση, συνήθως πρέπει να αντιγράψουν και να κατευθύνουν τις επιθέσεις τους μέσα απο ένα εμπορικό σήμα μίας εταιρείας ή ενός οργανισμού. Οι επιτιθέμενοι συνήθως δημιουργούν μια κακόβουλη σελίδα προορισμού για το χρήστη , που μοιάζει πολύ με την ιστοσελίδα μιας αξιόπιστης μάρκας , ενός γνωστού brand. Αυτό καθιστά ευκολότερο να πείσει τα θύματα-πιθανούς πελάτες του brand της εταιρείας να ανταποκριθούν σε μια παρότρυνση της σελίδας , προς μια διαδραστική ενέργεια από τη πλευρά του χρήστη. Συχνό παράδειγμα , η συμπλήρωση μιας φόρμας ή λήψη ενός συνημμένου αρχείου. Όταν εκκινείται μια καμπάνια phishing

απο κυβερνοεγκληματίες με το brand μιας εταιρείας αυτός ο τύπος δημοσιότητας μπορεί να βλάψει την εικόνα του brand , αφήνοντας την εντύπωση ότι οι ιστοσελίδες της δεν είναι ασφαλείς για επισκεψιμότητα απο τους χρήστες του διαδικτύου. Μερικοί πελάτες ενδέχεται να καταλήξουν να αποφεύγουν πλέον τους νόμιμους ιστότοπους της εταιρείας, ώστε να μην καταλήξουν απροσδόκητα σε μια ψεύτικη ιστοσελίδα και γίνουν θύματα ηλεκτρονικής απάτης. Αυτοί οι άνθρωποι μπορούν να χάσουν την εμπιστοσύνη τους στο εμπορικό σήμα και ενδεχομένως να εγκαταλείψουν την εταιρεία για έναν ανταγωνιστή της. Ακόμα χειρότερα, εάν καταστούν θύματα (πχ . υποστούν υποκλοπή προσωπικών δεδομένων), ενδέχεται να υποβάλουν αγωγή. Η άλλη περίπτωση είναι αυτή που τα δεδομένα του πελάτη , καλύπτονται από κανονισμούς προστασίας δεδομένων, οπότε στην εταιρεία επιβάλλονται μεγάλα πρόστιμα για μη συμμόρφωση με τους νέους κανονισμούς του GDPR. (DI 2017)

3.5.2 Πρόληψη και Αντιμετώπιση από επιθέσεις τύπου Phishing

Συχνότεροι εμφανιζόμενοι τύποι phishing είναι οι παρακάτω:

1. Email phishing scams

Μια απάτη "ηλεκτρονικού ψαρέματος" στο ηλεκτρονικό ταχυδρομείο είναι ένα μήνυμα απάτης ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από πρόσωπο ή μια εταιρεία που είναι γνωστή στο θύμα. Προσπαθεί να συλλέξει παράνομα προσωπικά δεδομένα από το υποψήφιο θύμα-παραλήπτη. Ένα μήνυμα ηλεκτρονικού "ψαρέματος" περιλαμβάνει συνήθως τουλάχιστον έναν σύνδεσμο με έναν ψεύτικο ιστότοπο, σχεδιασμένο να μιμείται τον ιστότοπο μιας νόμιμης επιχείρησης.

Πρόληψη και Αντιμετώπιση :

Ο χρήστης δεν θα πρέπει να επιλέγει συνδέσμους του μηνύματος ή να ανοίγει τα συνημμένα αρχεία στο ύποπτο μήνυμα , ηλεκτρονικού ταχυδρομείου. Είναι θεμιτό να ανοίγει ένα πρόγραμμα περιήγησης ιστού και να μεταβαίνει στον εν λόγω ιστότοπο πληκτρολογώντας τον στη γραμμή διευθύνσεων του προγράμματος περιήγησης. Η εγρήγορση και η προσωπική επαγρύπνηση για το χρήστη πρέπει να είναι μεγάλη καθώς οι «phishers» είναι γνωστό ότι χρησιμοποιούν πραγματικά λογότυπα εταιρειών στα μηνύματα απάτης που στέλνουν προς τους χρήστες του διαδικτύου ώστε να φαίνονται νόμιμα. Χρησιμοποιούν επίσης ψευδείς διευθύνσεις αποστολής , ηλεκτρονικού ταχυδρομείου, οι οποίες είναι παρόμοιες με την πραγματική διεύθυνση της εταιρείας. Ωστόσο, η διεύθυνση e-mail αποστολής ενδέχεται να έχει ορθογραφικά λάθη ή να προέρχεται από πλαστογραφημένο domain.

2. Vishing scams

Το V-ishing είναι οι επιθέσεις phishing μέσω VOIP (Voice Over IP). Είναι μια τηλεφωνική απάτη στην οποία τα υποψήφια θύματα , χρήστες της υπηρεσίας , εξαπατώνται από εισβολείς ώστε , να παραδώσουν πολύτιμες προσωπικές πληροφορίες τους στους επιτιθέμενους.

Πρόληψη και Αντιμετώπιση:

Δεν πρέπει οι χρήστες του διαδικτύου να δίνουν προσωπικές πληροφορίες μέσω τηλεφώνου. Σε περίπτωση αποκάλυψης της απάτης απο το θύμα, θα πρέπει να διακοπεί

οποιαδήποτε είδους επικοινωνία υπάρχει με τον εισβολέα . Αν , υπάρχουν υπόνοιες ότι μια επικοινωνία μέσω τηλεφώνου είναι ύποπτη για απάτη , θα πρέπει ο χρήστης να αναζητήσει τον τηλεφωνικό αριθμό της επιχείρησης στον επίσημο και νόμιμο ιστότοπό της και να καλέσει άμεσα για να βεβαιωθεί ότι πρόκειται για νόμιμη επικοινωνία. Ποτέ δεν θα πρέπει ο χρήστης να καλέσει τον αριθμό που τον κάλεσε.

3. Tech support cold call scams

Είναι ένα τέχνασμα επίδοξου εισβολέα , ο οποίος αφού επικοινωνήσει με ένα υποψήφιο θύμα , ισχυρίζεται ότι είναι αντιπρόσωπος μιας αξιόπιστης εταιρείας η οποία παρέχει υπηρεσίες ασφάλειας δικτύου στους πελάτες της.
Ενημερώνει το θύμα ότι η εν λόγω εταιρεία εντόπισε κακόβουλο λογισμικό στο σύστημα του θύματος. Έτσι οι κυβερνοεγκληματίες προσποιούνται ότι προσφέρουν μια λύση, κάνοντας τον χρήστη να εγκαταστήσει έναν τύπο λογισμικού απομακρυσμένης διαχείρισης συστήματος. Αυτό επιτρέπει στον εισβολέα να έχει πρόσβαση στον υπολογιστή , για να εγκαταστήσει κακόβουλο λογισμικό απομακρυσμένα στο σύστημα του θύματος. Εκτός από την προσπάθεια εγκατάστασης κακόβουλου λογισμικού στο σύστημα του χρήστη, οι κυβερνοεγκληματίες εν συνεχεία ζητούν πρόσθετες ώρες εργασίας απο το θύμα, ώστε να "διορθώσουν" περεταίρω προβλήματα ασφαλείας του συστήματος που εντόπισαν.

Πρόληψη και Αντιμετώπιση:

Εάν κάποιος προσπαθεί να επικοινωνήσει είτε τηλεφωνικά , είτε μέσω ηλεκτρονικού ταχυδρομείου , για να προτείνει σε κάποιον χρήστη του διαδικτύου , να εργαστεί για λογαριασμό μιας συγκεκριμένης και γνωστής εταιρείας, θεμιτό είναι , ο χρήστης , αφού πρώτα αναζητήσει τον τηλεφωνικό αριθμό που τον κάλεσε , να του αναφέρει ότι θα τον καλέσει ξανά για επιβεβαίωση. Δεν πρέπει ποτέ να επιτρέπεται η απομακρυσμένη πρόσβαση στον υπολογιστή απο τρίτους.

4. Pop-up warning scams

Αναδυόμενες διαφημίσεις , εμφανίζονται συνήθως όταν κάποιος χρήστης ενώ πραγματοποιεί μία περιήγηση στο διαδίκτυο βλέπει στην οθόνη του να προβάλλονται γραφικά παράθυρα με διαφημίσεις. Συνήθως, το περιεχόμενο απο τα αναδυόμενα μηνύματα διαφημίσεων σχετίζονται με το περιεχόμενο του ιστότοπου , που ανοίγεται εκείνη τη στιγμή αυτόματα στο πρόγραμμα περιήγησης. Τα παράθυρα αυτά μπορεί να είναι τρομερά ενοχλητικά, καθιστώντας δύσκολο για τον χρήστη να κλείσει το αναδυόμενο παράθυρο. Οι διαφημίσεις αυτές , ενδέχεται να εμφανίζουν ένα μήνυμα , που δηλώνει στο χρήστη , ότι ο υπολογιστής του έχει μολυνθεί από κακόβουλο λογισμικό , και προσφέρεται στο χρήστη , ένας αριθμός τηλεφώνου ή e-mail για επικοινωνία με την αρμόδια εταιρεία που μπορεί να αποκαταστήσει και να επιλύσει άμεσα το πρόβλημα του κακόβουλου εγκατεστημένου λογισμικού.
Ακόμα είναι εφικτό (πιο συχνά) να κοινοποιείται απο τη διαφήμιση ένας σύνδεσμος , απο τον οποίο ο χρήστης μπορεί να κατεβάσει σχετικό λογισμικό για το καθαρισμό του συστήματός του απο το υποτιθέμενο κακόβουλο λογισμικό που είναι εγκατεστημένο στον υπολογιστή του. Συνήθως , οι κυβερνοεγκληματίες κάνουν τα αναδυόμενα παράθυρα να μοιάζουν με αυτά , που προέρχονται απο έμπιστες και αξιόπιστες εταιρείες που παρέχουν επαγγελματικές υπηρεσίες, όσο αφορά την ασφάλεια συστημάτων και ασφαλούς περιήγησης στο διαδίκτυο.

Πρόληψη και Αντιμετώπιση:

Ο χρήστης θα πρέπει να εξετάζει προσεκτικά το μήνυμα της διαφήμισης. Πρέπει να αναζητεί εμφανή στοιχεία ηλεκτρονικής απάτης, όπως ορθογραφικά λάθη, αντιεπαγγελματική απεικόνιση στοιχείων κακή σύνταξη κειμένου και εννοιολογικά λάθη (πολλά απο τα κείμενα αυτά είναι μεταφρασμένα αυτόματα απο άλλη γλώσσα). Χρειάζεται απο το χρήστη , προσοχή και προσωπική επαγρύπνηση όταν υπάρχει η αμφιβολία, για την αυθεντικότητα του αναδυόμενου στοιχείου διαφήμισης. Ο χρήστης θα πρέπει να εκκινήσει το λογισμικό προστασίας ιών και να πραγματοποιήσει σάρωση για ιούς , σε όλο το σύστημά του καθώς η διαφήμιση , μπορεί να είναι αποτέλεσμα ενός malware που εγκαταστάθηκε στον υπολογιστή. (Norton 2019)

Κεφάλαιο 4
Περιγραφή του Προβλήματος

Σε αυτό το κεφάλαιο αρχικά, παρουσιάζεται μια περιγραφή του θέματος της μεταπτυχιακής διατριβής και ακολουθεί ο ορισμός της συγκεκριμένης πτυχής του προβλήματος που η έρευνα προσπαθεί να επιλύσει.

Τα μηνύματα απάτης ηλεκτρονικού ταχυδρομείου είναι παραπλανητικά και αληθοφανή μηνύματα που αποστέλλονται απο κυβερνοεγκληματίες προς λογαριασμούς χρηστών ηλεκτρονικού ταχυδρομείου και αποτελούν μία σημαντική απειλή για το τοπίο της κυβερνοασφάλειας στο διαδίκτυο. Οι κυβερνοεγκληματίες κατά την σύνθεση και την αποστολή των hoax email, προς τους λογαριασμούς χρηστών, ακολουθούν διάφορους μεθόδους και τεχνικές ώστε τα μηνύματα αυτά, να μην ανιχνεύονται ως μηνύματα απάτης, απο τα συστήματα αναγνώρισης ή από τους καθαυτούς χρήστες του ηλεκτρονικού ταχυδρομείου. Η δυσκολία αναγνώρισης των μηνυμάτων απάτης από τα συστήματα του διαδικτύου ή από τους χρήστες της ηλεκτρονικής αλληλογραφίας αποτελεί και το μεγαλύτερο πρόβλημα όσο αφορά την αποτελεσματική αντιμετώπιση και εξάλειψη του φαινομένου. Ένα μη ανιχνεύσιμο ή εντοπίσιμο hoax email μπορεί να οδηγήσει το χρήστη στο να δημοσιοποιήσει ευαίσθητα προσωπικά του δεδομένα στο διαδίκτυο. Αυτό έχει ως αποτέλεσμα τα δεδομένα του χρήστη να διαρρεύσουν και έτσι να υποστεί υποκλοπή των προσωπικών στοιχείων του, παραβίαση του συστήματός του, παραβίαση του λογαριασμού ηλεκτρονικού ταχυδρομείου του, διαδικτυακό εκφοβισμό ή εκβιασμό ακόμα και υποκλοπή μεγάλου χρηματικού ποσού.

Είναι πολύ σημαντικό να αναφερθεί ότι οι μεγάλες οικονομικές απώλειες , σε συνδυασμό με την ηθική βλάβη στην οποία επέρχονται τα θύματα από διαδικτυακές απάτες ηλεκτρονικού ταχυδρομείου, μπορούν να συντελέσουν ακόμα και στην απώλεια ανθρώπινης ζωής. Εκατομμύρια ανυποψίαστοι χρήστες ηλεκτρονικής αλληλογραφίας γίνονται καθημερινά θύματα απάτης στο διαδίκτυο.

Το κατάλληλο γνωσιακό υπόβαθρο , όπως η πληροφόρηση των χρηστών σχετικά με τις νέες ηλεκτρονικές απειλές του διαδικτύου , αλλά και εκπαίδευση των χρηστών όσο αφορά τα μέτρα προστασίας από επιθέσεις του ηλεκτρονικού ταχυδρομείου , μπορούν να συντελέσουν στο να περιοριστεί αρκετά ένα μεγάλο μέρος από τον αριθμό των ανυποψίαστων χρηστών που συχνά γίνονται θύματα από τέτοιου είδους διαδικτυακές επιθέσεις. Η άγνοια των χρηστών γύρω από τα hoax email δεν αποτελεί σίγουρα καθόλου καλό σύμμαχο για την εξάλειψη του φαινομένου που τα τελευταία χρόνια αρχίζει ολοένα να παίρνει διαστάσεις και να γίνεται όλο και μεγαλύτερο σύμφωνα με τις παγκόσμιες τηλεμετρικές στατιστικές εταιρειών που ειδικεύονται στην ασφάλεια του διαδικτύου.
Η ραγδαία αύξηση του φαινομένου τα τελευταία χρόνια οφείλεται στο ότι οι συνεχώς αποτελεσματικότερες και περισσότερο εξελιγμένες επιθέσεις των κυβερνοεγκληματιών

του διαδικτύου στο ηλεκτρονικό ταχυδρομείο κάνουν τις επιθέσεις τους να είναι περισσότερο από κάθε άλλη φορά επιτυχής. Οι κυβερνοεγκληματίες μπροστά στα συστήματα και τις εφαρμογές που φιλτράρουν τα hoax email , οι ίδιοι χρησιμοποιούν μια ποικιλία περισσότερο εξελιγμένων μεθόδων και τεχνικών ώστε να κάνουν τα ηλεκτρονικά τους μηνύματα εξαπάτησης , να διακρίνονται ως νόμιμα μηνύματα ιστού. Κατά συνέπεια, τα εξαιρετικά πειστικά ηλεκτρονικά μηνύματα μπορούν να παρακάμψουν τα υπάρχοντα συστήματα φιλτραρίσματος, στοχεύοντας χρήστες του διαδικτύου , φυσικά με καταστροφικές συνέπειες.

Ένα μη ανιχνεύσιμο και εντοπίσιμο hoax email , εκτός από ατομικό επίπεδο , επιφέρει επιπτώσεις και σε συλλογικό. Μία επιτυχημένη επίθεση απο hoax email σε μία ομάδα χρηστών ηλεκτρονικού ταχυδρομείου , οι οποίοι ανήκουν σε έναν οργανισμό ή μια εταιρεία και αποτελούν το εργατικό δυναμικό , θα προκαλούσε ισχυρό πλήγμα στο κύρος και τη φήμη της εταιρείας ή του οργανισμού. Αυτό συμβαίνει για το λόγο , ότι αν μια εταιρεία , πέσει θύμα επίθεσης από hoax email επιτυχώς, αυτό θα σήμαινε πιθανόν τη κλοπή , δημοσιοποίηση και διάθεση των ευαίσθητων προσωπικών δεδομένων της εταιρείας προς τρίτους , ενδεχομένως στους ανταγωνιστές της. Αυτό επιφέρει ισχυρό πλήγμα στα οικονομικά αποθέματα της εταιρείας και μπορεί να οδηγήσει ακόμα και στη διακοπή της λειτουργίας της.

Έτσι λοιπόν σύμφωνα με τα παραπάνω επειδή τα hoax email είναι ένα πρόβλημα που χρήζει επίλυσης, η ανάπτυξη ενός λογισμικού προσομοίωσης για την αναγνώριση των Hoax email , κρίνεται αναγκαία. Η εφαρμογή που υλοποιήθηκε στη παρούσα μεταπτυχιακή διατριβή έχει ως κύριο στόχο , την αυτόματη αναγνώριση των hoax email με βάση τις λέξεις που εμφανίζονται σε αυτά.

Η αποτελεσματική ανίχνευση μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ένα ανεπίλυτο πρόβλημα μεγάλης σημασίας , το οποίο επηρεάζει και το κόστος ενός ευρύτερου συστήματος όσο αφορά την ασφάλεια του ηλεκτρονικού ταχυδρομείου.
Αυτό συνεπάγεται ότι υπάρχουν συστήματα που δεν υποστηρίζουν παρόμοια τεχνική λόγω των πόρων που αυτά δεν διαθέτουν. Από την άλλη πλευρά παρόμοιες τεχνικές έχουν ευρεία χρήση σε σύγχρονες εφαρμογές που όμως έχουν πολύ περιορισμένους πόρους.

Έχοντας ως βάση αυτό το λογισμικό προσομοίωσης, μελλοντικά οι ερευνητές , η επιστημονική ομάδα και η ακαδημαϊκή κοινότητα θα μπορούν περαιτέρω , να εξετάσουν τη λειτουργία ενός αλγορίθμου εντοπισμού hoax email , σε ένα ελεγχόμενο περιβάλλον με κατάλληλους πόρους και επαρκής υποδομές.
Αυτό θα επιτρέψει στους επιστήμονες να αναπτύξουν πρακτικά , αποδοτικότερους αλγορίθμους δοκιμάζοντας διάφορους μεθόδους και τεχνικές οι οποίες θα συμβάλλουν ουσιαστικά στην αποτελεσματικότερη αναγνώριση μηνυμάτων ηλεκτρονικής απάτης , στο ηλεκτρονικό ταχυδρομείο.

Με βάση τα τεχνικά χαρακτηριστικά και την δράση των hoax emails στο διαδίκτυο, το πρόβλημα το οποίο η παρούσα μεταπτυχιακή διατριβή εστιάζει να λύσει , μπορεί να συνοψιστεί στο ακόλουθο ερευνητικό ερώτημα:

Μπορούμε να αναγνωρίσουμε και να εκμεταλλευτούμε τα λεκτικά χαρακτηριστικά των hoax emails ώστε να κατασκευάσουμε έναν αλγόριθμο αυτόματου εντοπισμού ;

Κεφάλαιο 5
Περιγραφή του Συστήματος

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο αρχικά παρουσιάζεται στην υποενότητα 5.2 μια γενική περιγραφή του συστήματος. Έπειτα στην υποενότητα 5.3 γίνεται αναφορά της γενικής περιγραφής υλοποίησης του συστήματος. Στην συνέχεια στην υποενότητα 5.4 γίνεται αναλυτική περιγραφή των βημάτων υλοποίησης του συστήματος.
Στην υποενότητα 5.5 επισημαίνεται η μεθοδολογία και ο τρόπος υλοποίησης του συστήματος, στην υποενότητα 5.6 απεικονίζονται τα γραφήματα από τα ευρήματα των τιμών του συστήματος , ενώ στην υποενότητα 5.7 παρουσιάζονται τα αποτελέσματα και τα συμπεράσματα του συστήματος που υλοποιήθηκε.

5.2 Γενική Περιγραφή του Συστήματος

Η προσομοίωση του αλγορίθμου , υλοποιεί ένα σύστημα , που αναγνωρίζει μηνύματα απάτης ηλεκτρονικού ταχυδρομείου αλλά και μηνύματα ασφαλή ηλεκτρονικού ταχυδρομείου.

Η αναγνώριση των μηνυμάτων απάτης , βασίζεται σε μία λίστα λέξεων (Dirtywords[]), η οποία ενημερώνεται δυναμικά από τον αλγόριθμο. Κατά την προσομοίωση , η λίστα Dirtywords[] , “μαθαίνει”, λέξεις που χρησιμοποιούνται συχνά σε μηνύματα ηλεκτρονικής απάτης. Στη συνέχεια χρησιμοποιείται από τον αλγόριθμο μία λίστα λέξεων Badwords[] η οποία περιέχει αντίστοιχα, ύποπτες λέξεις που χρησιμοποιούνται σε hoax emails.

Το περιεχόμενο της λίστας Badwords[] , προέρχεται από το διαδίκτυο , από έτοιμες και ενημερωμένες λίστες λέξεων (“triggerwords”), οι οποίες χρησιμοποιούνται συνήθως σε μηνύματα ηλεκτρονικού ταχυδρομείου τύπου hoax.

Στον αλγόριθμο , η χρήση της λίστας διαδικτύου Badwords[] , γίνεται με στόχο , την σύγκριση των ποσοστών επιτυχίας, στην αναγνώριση των hoax email αλλά και των ασφαλών email αντίστοιχα , από τις 2 λίστες Dirtywords[] και Badwords[].

Με τη μέθοδο αυτή του αλγορίθμου μπορούμε να αποφανθούμε αν το σύστημα που υλοποιήθηκε (λίστα Dirtywords[]) είναι αποδοτικότερο από τη λίστα Badwords[].
Τα ευρήματα από τη σύγκριση των τιμών των 2 λιστών ,οδηγούν στο συμπέρασμα ότι το υλοποιημένο σύστημα , παρουσιάζει λιγότερα false negatives και περισσότερα true positives.

Αυτό συμβαίνει καθώς το σύστημα που δημιουργεί ο αλγόριθμος (DirtyWords[]) στον εντοπισμό ενός Hoax email έχει κατά μέσο όρο 33% υψηλότερο ποσοστό ακρίβειας , απο ότι η λίστα Badwords[] που χρησιμοποιήθηκε απο το διαδίκτυο για τους ελέγχους καθώς για ένα hoax email που θα εισέλθει στο σύστημα , η πιθανότητα να μην αναγνωριστεί ως "hoax" είναι μικρότερη αντί της Badwords[] λίστας.

Αντίστοιχα για τον εντοπισμό ενός ασφαλούς email η λίστα του συστήματος DirtyWords[] προσεγγίζει με μικρότερο ποσοστό λάθους (από ότι η λίστα Badwords) , κατά 1,2% , έχοντας συνεπώς λιγότερα false positives.
Αυτό συνεπάγεται ότι η πιθανότητα να αναγνωρίσει η DirtyWords[] εσφαλμένα ένα "clean" email ως "hoax" email είναι μικρότερη , αντί της λίστας Badwords[].

5.3 Γενική περιγραφή υλοποίησης του συστήματος

Χρήση προγραμμάτων: Python , PyScripter & pip

Ο αλγόριθμος προγραμματίστηκε σε περιβάλλον προσομοίωσης, με χρήση της γλώσσας προγραμματισμού Python (έκδοσης 3.7.3).
Ο κώδικας κατασκευάστηκε σε περιβάλλον του PyScripter (έκδοσης 3.6.0.0 x 64) ενώ η εγκατάσταση και η διαχείριση πρόσθετων βιβλιοθηκών και πακέτων που δεν αποτελούσαν μέρος των τυπικών βιβλιοθηκών της συγκεκριμένης έκδοσης Python, έγινε από το πρόγραμμα pip που αποτελεί ένα library management tool (έκδοσης 19.1)

Δημιουργία λίστας: DirtyWords[] , Badwords[]

Η λειτουργία του αλγορίθμου βασίζεται στην εκμάθηση και ανίχνευση , λέξεων που χρησιμοποιούνται στα hoax email.
Η προσομοίωση του αλγορίθμου, δημιουργεί μία λίστα DirtyWords[] και μία λίστα Badwords[] για να εντοπίζονται ύποπτες λέξεις, σε hoax emails και στη συνέχεια σε "non-hoax" emails. Στο λογισμικό , τα περιεχόμενα των 2 διαφορετικών λιστών , DirtyWords[] και Badwords[] καταγράφονται και συγκρίνονται. Έτσι το ποσοστό προσέγγισης , όσο αφορά την ακρίβεια στον εντοπισμό ύποπτων λέξεων , των μηνυμάτων ηλεκτρονικού ταχυδρομείου, της λίστας DirtyWords[] προσμετράται και συγκρίνεται με τα αποτελέσματα της λίστας Badwords[].
Με αυτό το τρόπο μπορούμε να αποφανθούμε σε τι ποσοστό η λίστα που δημιουργεί ο αλγόριθμος (DirtyWords[]) προσεγγίζει με ακρίβεια τον εντοπισμό μηνυμάτων απάτης ηλεκτρονικού ταχυδρομείου.

Χρήση αρχείων κειμένου: Whitelist.txt , Badwords.txt

Για την υλοποίηση του αλγορίθμου χρησιμοποιήθηκαν, επίσης και δύο αρχεία κειμένου. Το πρώτο περιείχε λέξεις "hoax" ενώ το δεύτερο "stopwords". Με τον όρο "stopwords" εννοούνται οι λέξεις που χρησιμοποιούνται συνήθως στην καθημερινή χρήση του λόγου. Σπάνια αυτές οι λέξεις εμφανίζονται σε hoax μηνύματα ηλεκτρονικού ταχυδρομείου , καθώς είναι πιθανότερο να εμφανίζονται σε ασφαλή μηνύματα ηλεκτρονικού ταχυδρομείου. Το αρχείο που περιλαμβάνει τις "hoax" λέξεις ορίζεται στον αλγόριθμο ως

Badwords.txt, ενώ το αρχείο που περιλαμβάνει τα “stopwords” ονομάζεται Whitelist.txt. Το περιεχόμενο των αρχείων των λέξεων, ορίστηκε δυναμικά, από πρόσφατες ενημερωμένες λίστες λέξεων του διαδικτύου.

Χρήση τριών email Dataset: Fraud1.txt , Fraud2.txt , Clean.txt

Στον αλγόριθμο το πρώτο Dataset περιλαμβάνει hoax emails και ορίζεται στον αλγόριθμο ως το αρχείο “Fraud1.txt” και χρησιμοποιείται για την δημιουργία της λίστας DirtyWords[]. Το δεύτερο Dataset (Fraud2.txt) περιλαμβάνει και αυτό hoax emails αλλά χρησιμοποιείται για την σύγκριση των αποτελεσμάτων μεταξύ των δύο λιστών DirtyWords[] & Badwords[]. Η σύγκριση γίνεται με βάση το ποσοστό ακρίβειας , όσο αφορά τον εντοπισμό των hoax email. Το τρίτο Dataset περιλαμβάνει ασφαλή μηνύματα ηλεκτρονικού ταχυδρομείου και χρησιμοποιείται και αυτό για την σύγκριση των αποτελεσμάτων μεταξύ των δύο λιστών DirtyWords[] & Badwords[]. Η σύγκριση αυτή αφορά το ποσοστό λάθους να αναγνωριστεί ένα ασφαλές μήνυμα ηλεκτρονικού ταχυδρομείου , ως μήνυμα απάτης.

Ανάδειξη ευρημάτων σε υπολογιστικά φύλλα: Email WEIGHT'S.ods

Κατά την ερευνητική διαδικασία τα αποτελέσματα και των δύο λιστών Badwords[] και DirtyWords[] εξάγονται από το κώδικα σε αρχεία .csv και μέσα από υπολογιστικά φύλλα , τα αποτελέσματα απεικονίζονται και αναλύονται σε γραφήματα με σκοπό αφενός τη σύγκριση των αποτελεσμάτων τους και αφετέρου τον έλεγχο της απόδοσης της λίστας που δημιουργεί ο αλγόριθμος (DirtyWords[]). Για την απεικόνιση των αποτελεσμάτων στα υπολογιστικά φύλλα , χρησιμοποιήθηκαν τα αποτελέσματα των πινάκων από τις παρακάτω λίστες του κώδικα: FMD_array[] , FMB_array[] , RMD_array[] , RMB_array[].

Αποτελέσματα και Συμπεράσματα

Τα αποτελέσματα των πειραμάτων με τη μέθοδο του αλγορίθμου, υποδεικνύουν λιγότερα false negatives με περισσότερα true positives. Αυτό συμβαίνει καθώς το σύστημα που δημιουργεί ο αλγόριθμος (DirtyWords[]) στον εντοπισμό ενός Hoax email έχει κατά μέσο όρο 33% υψηλότερο ποσοστό ακρίβειας , απο ότι η λίστα Badwords[] που χρησιμοποιήθηκε απο το διαδίκτυο για τους ελέγχους. Δηλαδή για ένα hoax email που θα εισέλθει στο σύστημα , η πιθανότητα να μην αναγνωριστεί ως “hoax” είναι μικρότερη αντί της Badwords[] λίστας. Αντίστοιχα , όσο αφορά τον εντοπισμό ενός Clean email , το σύστημα παρουσίασε 1,2% μικρότερο ποσοστό λάθους σε σχέση με την λίστα Badword. Αξίζει εδώ να σημειωθεί πως αν και οι δύο λίστες είναι αρκετά επαρκείς στον εντοπισμό των clean emails η λίστα του αλγορίθμου DirtyWords[] προσεγγίζει με μικρότερο ποσοστό λάθους τον εντοπισμό των clean emails έναντι της λίστας Badwords, καθώς έχουμε λιγότερα false positives. Αυτό συνεπάγεται ότι η πιθανότητα να αναγνωρίσει η DirtyWords[] ένα Clean email ως Hoax email είναι μικρότερη αντί της λίστας Badwords[].

5.4 Αναλυτική περιγραφή βημάτων υλοποίησης του Συστήματος

Η αναλυτική περιγραφή των βημάτων που ακολουθήθηκε κατά την διαδικασία υλοποίησης του συστήματος περιγράφεται παρακάτω.

Δημιουργία Badwords.txt

Ορίστηκε δυναμικά από ιστότοπους του διαδικτύου μια λίστα λέξεων η οποία περιλαμβάνει λέξεις από hoax email (triggerwords) με στόχο τη δημιουργία ενός αρχείου κειμένου με το όνομα Badwords.txt.

Διαδικτυακές πηγές:

https://snov.io/blog/440-spam-trigger-words-to-avoid-in-2019/

https://www.automational.com/spam-trigger-words-to-avoid/

Δημιουργία Whitelist.txt

Ορίστηκε δυναμικά μια λίστα λέξεων από το διαδίκτυο (από διάφορους ιστότοπους) η οποία περιλαμβάνει λέξεις (stopwords) , που δεν χρησιμοποιούνται (συνήθως) σε μηνύματα ηλεκτρονικής απάτης.

Διαδικτυακές πηγές:

https://www.lextek.com/manuals/onix/stopwords1.html

https://countwordsfree.com/stopwords

http://xpo6.com/list-of-english-stop-words/

https://uk.mathworks.com/help/textanalytics/ref/stopwords.html

Δημιουργία Fraud1.txt & Fraud2.txt

Για την δημιουργία του fraud1.txt & Fraud2.txt, χρησιμοποιήθηκε από το διαδίκτυο ένα email Dataset το οποίο περιελάμβανε μηνύματα ηλεκτρονικού ταχυδρομείου. Τα μηνύματα αυτά είναι μια συλλογή ηλεκτρονικών μηνυμάτων hoax, που χρονολογούνται από το 1998 έως το 2007. Στο κάθε αρχείο (Fraud1.txt & Fraud2.txt αντίστοιχα) καταχωρήθηκαν από 126 μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία αναλύονται στο λογισμικό της προσομοίωσης.

Διαδικτυακή πηγή:

https://www.kaggle.com/rtatman/fraudulent-email-corpus

Δημιουργία Clean.txt

Για την δημιουργία του clean.txt χρησιμοποιήθηκε από το διαδίκτυο ένα email Dataset το οποίο περιείχε ασφαλή μηνύματα ηλεκτρονικού ταχυδρομείου.
Από όλο το Dataset επιλέχθηκαν 126 τυχαία μηνύματα ταχυδρομείου προς καταχώρηση στο αρχείο κειμένου clean.txt.

Διαδικτυακή πηγή:

https://www.cs.cmu.edu/~enron/

5.5 Μεθοδολογία υλοποίησης του συστήματος

5.5.1 Κωδικοποίηση email κατά λέξη σε μορφή λίστας

Βήματα:

1.Καταχώρηση των email του fraud1.txt Dataset στο κώδικα.
2.Μετατροπή όλων των αλφαριθμητικών στοιχείων σε πεζούς χαρακτήρες.
3.Αφαίρεση όλων των ειδικών χαρακτήρων κωδικοποίησης και διαστημάτων.

Εισαγωγή:

Αρχικά στο λογισμικό , πρέπει να εισαγάγουμε το fraud email Dataset (fraud1.txt) το οποίο είναι ένα αρχείο κειμένου , που περιέχει μηνύματα ηλεκτρονικής απάτης. Όλα τα περιεχόμενα του αρχείου κειμένου, διαβάζονται μέσα από το λογισμικό και αποθηκεύονται στη λίστα LearningMail[]. Τα περιεχόμενα της λίστας, τροποποιούνται και χρησιμοποιούνται από τη λίστα MessList[] με στόχο την αφαίρεση των ειδικών χαρακτήρων & των κενών διαστημάτων. Η MessList[] αργότερα πρόκειται να χρησιμοποιηθεί στην λίστα AllWords[] με απώτερο σκοπό τη δημιουργία της λίστας του συστήματος DirtyWords[].

Εισαγωγή του fraud1.txt Dataset

Έγινε εισαγωγή του αρχείου στο λογισμικό όπως επίσης έγινε και η αποθήκευση των

περιεχομένων του σε λίστα.

Δημιουργία λίστας LearningMail[]

Η λίστα διαβάζει τα περιεχόμενα του αρχείου κειμένου fraud1.txt.
Επειδή στο αρχείο κειμένου περιέχονται 126 “fraud” emails , τα στοιχεία της λίστας , είναι στο σύνολό τους , 126.
Σε κάθε στοιχείο της λίστας αποθηκεύεται -λέξη προς λέξη- , ολόκληρο το email που διαβάζεται από το αρχείο κειμένου fraud1.txt. Στη πρώτη διάσταση της λίστας αποθηκεύονται όλα τα αλφαριθμητικά που συνιστούν το email , ενώ στη δεύτερη διάσταση , αποθηκεύεται ένας πίνακας αλφαριθμητικών, όπου κάθε αλφαριθμητικό στο σύνολό τους , συνιστούν το email.

Δημιουργία λίστας MessList[]

Η λίστα η οποία είναι μονής διάστασης , διαβάζει ξεχωριστά , το κάθε στοιχείο της λίστας LearningMail[] , αφαιρώντας τους ειδικούς χαρακτήρες και τα κενά διαστήματα από όλα τα αλφαριθμητικά. Τέλος μετατρέπει σε πεζούς χαρακτήρες όλα τα αλφαριθμητικά των στοιχείων της λίστας , και τα αποθηκεύει - ένα προς ένα - σε μία μονοδιάσταση λίστα.

5.5.2 Καταχώρηση προ υπαρχόντων διαδικτυακών λεξικών

Βήματα:

1.Καταχώρηση “hoax” διαδικτυακών λεξικών στο κώδικα.
2.Καταχώρηση των διαδικτυακών λεξικών “stopwords” στο κώδικα.
3.Αποθήκευση διαδικτυακών λεξικών σε λίστες του προγράμματος , Badwords[] & Whitelist[]

Εισαγωγή:

Στο δεύτερο μέρος του λογισμικού θέλουμε το πρόγραμμα να διαβάζει λεξικά , από έτοιμες λίστες λέξεων του διαδικτύου.
Οι λίστες αυτές αφορούν αρχικά λέξεις ύποπτες που αναφέρονται συνήθως σε μηνύματα ηλεκτρονικής απάτης τύπου hoax.
Το περιεχόμενο των λέξεων αυτών αποθηκεύεται στο αρχείο κειμένου Badwords.txt. Ομοίως και το περιεχόμενο των ασφαλών λέξεων από τις έτοιμες λίστες του διαδικτύου αποθηκεύονται αντίστοιχα σε ένα αρχείο κειμένου Whitelist.txt.
Το λογισμικό έπειτα διαβάζει τα δύο αρχεία κειμένου και αποθηκεύει τα περιεχόμενά τους σε δύο λίστες.

Εισαγωγή αρχείων κειμένου Whitelist & Badwords

Εισαγωγή των αρχείων κειμένου Whitelist.txt & Badwords.txt στο λογισμικό και αποθήκευση των περιεχομένων τους στις λίστες Whitelist[] & Badwords[] αντίστοιχα. Εδώ να σημειώσουμε ότι , η λίστα Badwords[] σε επόμενο βήμα διαβάζει emails από 1

fraud email Dataset (fraud2.txt) και από 1 clean email Dataset (clean.txt) όπου τα αποτελέσματά της , συγκρίνονται με τα αποτελέσματα της λίστας Dirtywords[] που υλοποιεί ο αλγόριθμος στο επόμενο βήμα.

Δημιουργία λίστας Badwords[]

Αν και η Python διαθέτει έτοιμες λίστες-συναρτήσεις που περιέχουν λέξεις απο trigger words" ώστε να γίνουν οι κατάλληλοι έλεγχοι (αναγνώρισης των hoax email), η μονοδιάστατη λίστα δημιουργήθηκε παρόλα αυτά με σκοπό την ευελιξία του χρήστη.
Ο λόγος είναι , ότι το αρχείο κειμένου (Badwords.txt) , μπορεί να ενημερώνεται με καινούργιες λέξεις , δυναμικά απο τον χρήστη , και στη συνέχεια , διαβάζεται στο κώδικα από τη λίστα Badwords[] κάνοντας η λίστα , κάθε φορά και τους αντίστοιχους ελέγχους στα μηνύματα ηλεκτρονικού ταχυδρομείου. Κατά την ανάγνωση του αρχείου κειμένου (από τη λίστα) , αφαιρούνται κενά διαστήματα και ειδικοί χαρακτήρες που το κείμενο περιέχει λόγω της κωδικοποίησης του αρχείου ενώ πιθανοί κεφαλαίοι χαρακτήρες από το αρχείο κειμένου μετατρέπονται σε πεζούς.
Στη συνέχεια όλα τα στοιχεία αποθηκεύονται σε μία μονοδιάστατη λίστα με όνομα Badwords[].

Δημιουργία λίστας Whitelist[]

Ομοίως , όπως η λίστα Badwords[] έτσι και η μονοδιάστατη λίστα Whitelist[] , δημιουργείται στο πρόγραμμα για λόγους ευελιξίας από πλευράς χρήστη. Αν και υπάρχουν έτοιμες συναρτήσεις που περιέχουν "stopwords" , για να γίνονται οι κατάλληλοι έλεγχοι στα μηνύματα ηλεκτρονικού ταχυδρομείου, η λίστα δημιουργείται , ώστε οι λέξεις που διαβάζονται από το αντίστοιχο αρχείο κειμένου (Whitelist.txt) να ενημερώνονται από το χρήστη δυναμικά , μέσα στο αρχείο κειμένου.
Η λίστα , διαβάζοντας τα στοιχεία από το αρχείο κειμένου , μετατρέπει κεφαλαίους χαρακτήρες σε πεζούς , όπως επίσης αφαιρεί ειδικούς χαρακτήρες και κενά διαστήματα.

5.5.3 Αναγνώριση , αποθήκευση νεοεμφανιζόμενων triggerword από Hoax emails

Βήματα:

1.Δημιουργία της λίστας DirtyWords[]
2.Μέθοδος ανεύρεσης των "hoax" λέξεων απο τη DirtyWords[] στο fraud1.txt Dataset
3.Έλεγχοι και περιορισμοί στην αποθήκευση των "triggerwords" , από τη DirtyWords[].
4.Καταγραφή συχνότητας εμφάνισης των hoax λέξεων από τη DirtyWords[] λίστα, για δειγματοληψία.

Εισαγωγή:

Στο τρίτο μέρος του λογισμικού θέλουμε το πρόγραμμα να δημιουργήσει τη λίστα του συστήματος DirtyWords[]. Η λίστα αυτή , δεν χρησιμοποιεί από το διαδίκτυο έτοιμες λίστες λέξεων από "triggerwords" όπως η Badwords[] λίστα. Αντιθέτως "μαθαίνει" τις λέξεις που χρησιμοποιούνται σε Hoax emails. Η μεθοδολογία του τρόπου εκμάθησης των "hoax" λέξεων από τη DirtyWords[] λίστα, περιγράφεται παρακάτω στα επόμενα βήματα.

Δημιουργία λίστας AllWords[]

Το λογισμικό αρχικά διαβάζει όλες τις λέξεις που περιέχονται στη λίστα MessList[] (η οποία εμπεριέχει κάθε λέξη του email Dataset fraud1.txt). Στη συνέχεια ο κώδικας ελέγχει αν κάθε λέξη από τη λίστα MessList[] δεν εμπεριέχεται στη λίστα Whitelist[] και αν δεν εμπεριέχεται , είναι υποψήφια προς αποθήκευση στη λίστα AllWords[].
Η λέξη θα αποθηκευτεί τελικά στη λίστα AllWords[], εφόσον –και μόνο- δεν έχει καταχωρηθεί ήδη στη λίστα , πραγματοποιώντας έτσι επιπλέον και έλεγχο, για την αποφυγή των διπλοεγγεγραμμένων καταχωρήσεων. Η μονοδιάστατη λίστα AllWords[] περιέχει 4.040 αλφαριθμητικές καταχωρήσεις και θα χρησιμοποιηθεί παρακάτω για την δημιουργία της λίστας DirtyWords[].

Δημιουργία λίστας DirtyWords[]

Λόγω του μεγάλου πλήθους των αλφαριθμητικών καταχωρήσεων της μονοδιάστατης λίστας AllWords[] , η μονοδιάστατη λίστα DirtyWords θα αποθηκεύσει μόνο, τις “hoax” λέξεις από την AllWords[] λίστα , που έχουν συχνότητα εμφάνισης , μεγαλύτερη από συγκεκριμένη τιμή. Στο κώδικα η τιμή αυτή ορίστηκε να είναι 50.
Άρα η λίστα DirtyWords[] θα περιέχει “hoax” αλφαριθμητικά στοιχεία που έχουν συχνότητα εμφάνισης, στην AllWords[] λίστα πάνω από 50 φορές.
Στο σύνολό της , η μονοδιάστατη λίστα DirtyWords[] αποθηκεύει 67 καταχωρήσεις από “hoax” λέξεις.

Δημιουργία λίστας DirtyCount[]

Η δισδιάστατη λίστα DirtyCount[] αποθηκεύει ως πρώτο στοιχείο της , το “hoax” αλφαριθμητικό στοιχείο της λίστας DirtyWords[] ενώ στη δεύτερη διάσταση αποθηκεύει (αταξινόμητα) και τη συχνότητα εμφάνισης αυτού του στοιχείου, που βρίσκει από τη λίστα AllWords[]

Δημιουργία λίστας SortedCount[]

Η δυσδιάστατη λίστα SortedCount[] ταξινομεί όλα τα στοιχεία της λίστας DirtyCount[] σύμφωνα με τη συχνότητα εμφάνισης των στοιχείων που είναι αποθηκευμένα της DirtyCount[].

5.5.4 Πείραμα Α : Αξιολόγηση του συστήματος σε Dataset με Hoax email

Βήματα:

1.Καταχώρηση του fraud email Dataset (αρχείου fraud2.txt) , στο κώδικα.
2.Μετατροπή όλων των αλφαριθμητικών στοιχείων του αρχείου σε πεζούς χαρακτήρες

3.Αφαίρεση όλων των ειδικών χαρακτήρων κωδικοποίησης και διαστημάτων που περιέχονται στο αρχείο.
4.Έλεγχος όλων των email του αρχείου , απο τις λίστες FMD_array[] & FMB_array[]
5.Καταχώρηση του πλήθους των ανιχνεύσιμων hoax email και των ανιχνεύσιμων "trigger words" για κάθε λίστα
6.Εξαγωγή των ευρημάτων και αποτελεσμάτων , της κάθε λίστας σε .csv αρχεία

Εισαγωγή:

Στο τέταρτο μέρος του λογισμικού θέλουμε το πρόγραμμα να διαβάσει και να αποθηκεύσει όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου από το αρχείο , fraud2.txt. που περιέχει 126 fraud emails. Στη συνέχεια , γίνεται έλεγχος των hoax email από τις λίστες DirtyWords[] και Badwords[].
Στη κάθε λίστα καταχωρείται το πλήθος των "trigger words"και το πλήθος των email που ανιχνεύθηκαν από τις δύο λίστες αντίστοιχα. Οι τιμές αυτές αποθηκεύονται για την κάθε λίστα , στις λίστες HOAX_Score_DIRTY[] & HOAX_Score_BAD[] αντίστοιχα.

Δημιουργία λίστας TestingMail[]

Η δυσδιάστατη λίστα διαβάζει τα περιεχόμενα του αρχείου κειμένου fraud2.txt.
Τα στοιχεία της λίστας , είναι στο σύνολό τους 126. Σε κάθε στοιχείο της λίστας αποθηκεύεται -λέξη προς λέξη- , ολόκληρο το email που διαβάζεται από το αρχείο κειμένου fraud2.txt.
Στη πρώτη διάσταση της λίστας αποθηκεύονται όλα τα αλφαριθμητικά που συνιστούν το email , ενώ στη δεύτερη διάσταση , αποθηκεύεται ένας πίνακας αλφαριθμητικών, όπου κάθε αλφαριθμητικό στο σύνολό τους , συνιστούν το email.

Δημιουργία λίστας HOAX_Score_DIRTY[]

Η μονοδιάστατη λίστα ακεραίων , HOAX_Score_DIRTY[] , αποθηκεύει για κάθε email που διαβάζει από την TestingMail[] λίστα , τον αριθμό της συχνότητας εμφάνισης των "hoax word" που προέρχονται από την λίστα DirtyWords[].

Δημιουργία λίστας HOAX_Score_BAD[]

Η μονοδιάστατη λίστα ακεραίων , HOAX_Score_BAD[] , αποθηκεύει για κάθε email που διαβάζει από την TestingMail[] λίστα , τον αριθμό της συχνότητας εμφάνισης των "hoax word" που προέρχονται από την λίστα Badwords[].

Δημιουργία λίστας FMD_array[]

Η δυσδιάστατη λίστα ακεραίων αριθμών FMD_array[] αποθηκεύει στο πρώτο στοιχείο της , τον αριθμό των "hoax words" που βρέθηκαν από την DirtyWords[] λίστα. Στο δεύτερο στοιχείο της λίστας , αποθηκεύεται ο συνολικός αριθμός των email , στα οποία εντοπίστηκε ο συγκεκριμένος αριθμός από "hoax words".

Δημιουργία λίστας FMB_array[]

Η δυσδιάστατη λίστα ακεραίων αριθμών FMB_array[] αποθηκεύει στο πρώτο στοιχείο της , τον αριθμό των "hoax words" που βρέθηκαν από την Badwords[] λίστα.
Στο δεύτερο στοιχείο της λίστας , αποθηκεύεται ο συνολικός αριθμός των email , στα

οποία εντοπίστηκε ο συγκεκριμένος αριθμός από “hoax words”.

5.5.5 Πείραμα Β : Αξιολόγηση του συστήματος σε Dataset με ασφαλή email

Βήματα:

1.Καταχώρηση των email του clean.txt Dataset στο κώδικα.
2.Μετατροπή όλων των αλφαριθμητικών στοιχείων του αρχείου σε πεζούς χαρακτήρες
3.Αφαίρεση όλων των ειδικών χαρακτήρων κωδικοποίησης και διαστημάτων που περιέχονται στο αρχείο.
4.Έλεγχος όλων των email του αρχείου , απο τις λίστες RMD_array[] & RMB_array[]
5.Καταχώρηση των (εσφαλμένα) ανιχνεύσιμων hoax email και “trigger words” για κάθε λίστα
6.Εξαγωγή των ευρημάτων και αποτελεσμάτων , της κάθε λίστας , σε .csv αρχεία για τον έλεγχο της προσέγγισης

Εισαγωγή:

Στο πέμπτο και τελευταίο μέρος του λογισμικού θέλουμε να εισαχθεί στο πρόγραμμα ένα Dataset από 126 ασφαλή μηνύματα ηλεκτρονικού ταχυδρομείου (clean.txt Dataset). Δύο λίστες REAL_Score_DIRTY[] & REAL_Score_BAD[] διαβάζουν τα ασφαλή μηνύματα ηλεκτρονικού ταχυδρομείου προσπαθώντας να ανιχνεύσουν hoax emails και “trigger words”. Οι ανιχνεύσιμες λέξεις και τα email , αποθηκεύονται στις λίστες RMD_array[] & RMB_array[] αντίστοιχα , με στόχο την εξαγωγή των ευρημάτων σε .csv αρχεία. Η μεθοδολογία αυτή ακολουθείται ώστε να διαπιστωθεί από τα ευρήματα, με τι ποσοστό λάθους προσεγγίζει η λίστα του συστήματος ένα clean email ως hoax συγκριτικά με τη δεύτερη λίστα του αλγορίθμου.

Δημιουργία λίστας CleanMail[]

Η δυσδιάστατη λίστα διαβάζει τα περιεχόμενα του αρχείου κειμένου clean.txt. Τα στοιχεία της λίστας , είναι στο σύνολό τους 126.
Σε κάθε στοιχείο της λίστας αποθηκεύεται -λέξη προς λέξη- , ολόκληρο το email που διαβάζεται από το αρχείο κειμένου clean.txt.
Στη πρώτη διάσταση της λίστας αποθηκεύονται όλα τα αλφαριθμητικά που συνιστούν το email , ενώ στη δεύτερη διάσταση , αποθηκεύεται ένας πίνακας αλφαριθμητικών, όπου κάθε αλφαριθμητικό στο σύνολό τους , συνιστούν το email.

Δημιουργία λίστας REAL_Score_DIRTY[]

Η μονοδιάστατη λίστα ακεραίων , REAL_Score_ DIRTY[] , αποθηκεύει για κάθε email που διαβάζει από την CleanMail[] λίστα (του 3ου Dataset) , τον αριθμό της συχνότητας εμφάνισης των “hoax word” που προέρχονται από την λίστα DirtyWords[].

Δημιουργία λίστας REAL_Score_BAD[]

Η μονοδιάστατη λίστα ακεραίων , REAL_Score_BAD[] , αποθηκεύει για κάθε email που διαβάζει από την CleanMail[] λίστα (του 3ου Dataset) , τον αριθμό της συχνότητας εμφάνισης των “hoax word” που προέρχονται από την λίστα DirtyWords[].

Δημιουργία λίστας RMD_array[]

Η δυσδιάστατη λίστα ακεραίων αριθμών RMD_array[] αποθηκεύει στο πρώτο στοιχείο της, τον αριθμό των “hoax words” που βρέθηκαν από την DirtyWords[] λίστα, στο 3ο Dataset. Στο δεύτερο στοιχείο της λίστας , αποθηκεύεται ο συνολικός αριθμός των email , στα οποία εντοπίστηκε ο συγκεκριμένος αριθμός από “hoax words”.

Δημιουργία λίστας RMB_array[]

Η δυσδιάστατη λίστα ακεραίων αριθμών RMB_array[] αποθηκεύει στο πρώτο στοιχείο της, τον αριθμό των “hoax words” που βρέθηκαν από την Badwords [] λίστα, στο 3ο Dataset. Στο δεύτερο στοιχείο της λίστας , αποθηκεύεται ο συνολικός αριθμός των email , στα οποία εντοπίστηκε ο συγκεκριμένος αριθμός από “hoax words”

5.6 Απεικόνιση Ευρημάτων σε Γραφήματα

Στην ενότητα αυτή παρουσιάζεται η απεικόνιση υπολογιστικών φύλων , για τον υπολογισμό της απόδοσης του αλγορίθμου. Τα αποτελέσματα των ευρημάτων απο τις λίστες FMD_array[] , FMB_array[] , RMD_array[] , RMB_array[] , των οποίων οι τιμές προκύπτουν , από τους ελέγχους που πραγματοποιούν οι 2 λίστες : Badwords[] και DirtyWords[] , στα Hoax email (fraud2.txt) και στα Clean email (clean.txt) αντίστοιχα, εξάγονται και αποθηκεύονται σε .csv αρχεία με στόχο να εισαχθούν σε υπολογιστικά φύλλα ώστε να γίνουν οι κατάλληλες μετρήσεις και συγκρίσεις των τιμών. Οι τιμές από τα ευρήματα των μετρήσεων, αναπαρίστανται σε γραφήματα, στα οποία ελέγχεται και η απόδοση του συστήματος υλοποίησης.

Για τα Hoax Emails

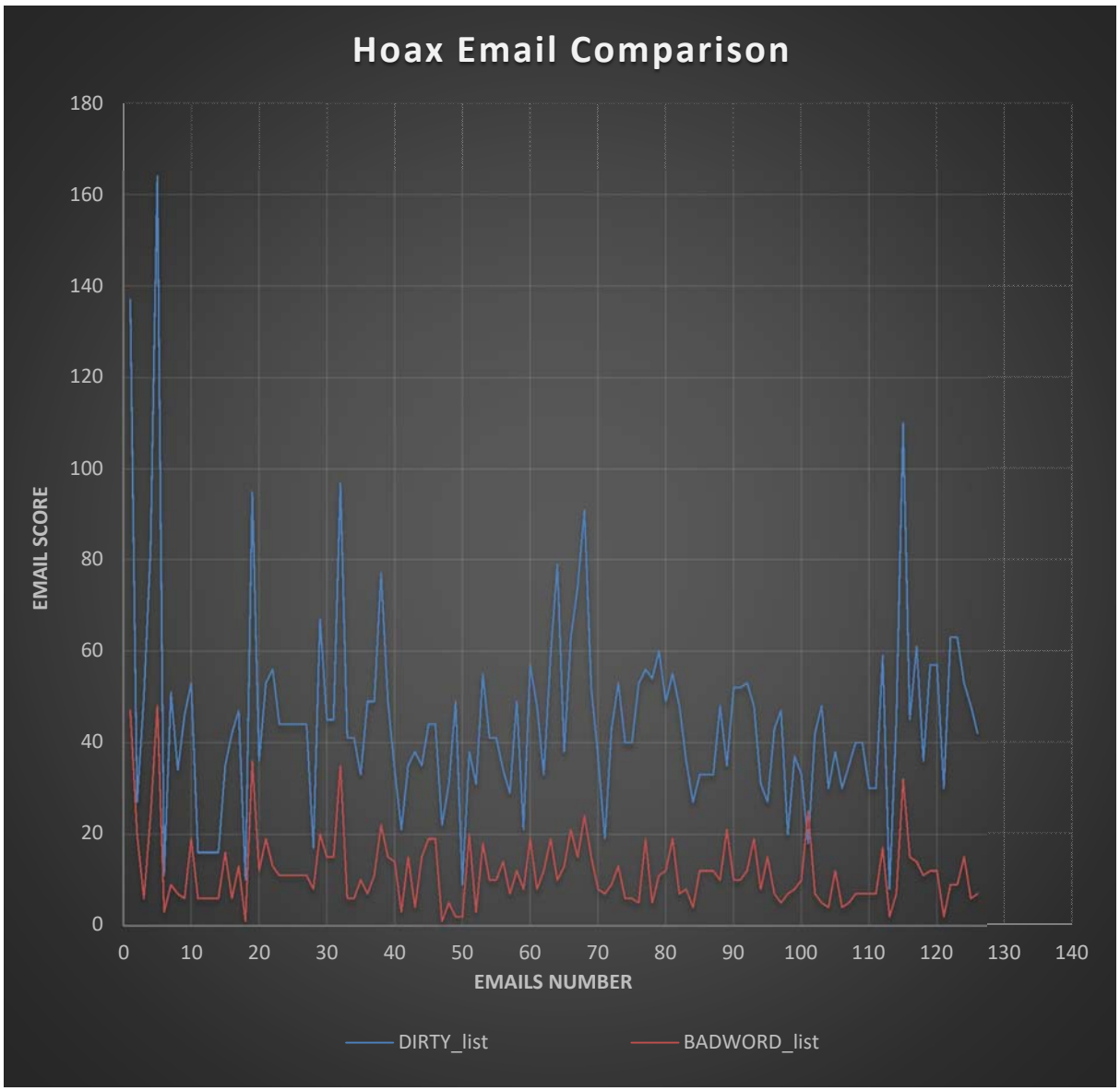
Στο **Διάγραμμα 1** , απεικονίζεται σε γραφική παράσταση το πλήθος των score , που εμφανίζεται από τις λίστες του αλγορίθμου , για ένα πλήθος απο Hoax Email του αρχείου fraud2.txt Dataset. Η DirtyWords[] λίστα παρουσιάζει περισσότερα true positives ενώ η Badwords[] λίστα , παρουσιάζει περισσότερα false negatives.

Αντίστοιχα το παραπάνω φαίνεται και από το **Διάγραμμα 2** όπου αναπαρίσταται το πλήθος των “triggerwords” , που αναγνωρίζει η κάθε λίστα του αλγορίθμου , για κάθε Hoax Email , από το συνολικό δείγμα των 126 Hoax Email του αρχείου fraud2.txt Dataset.

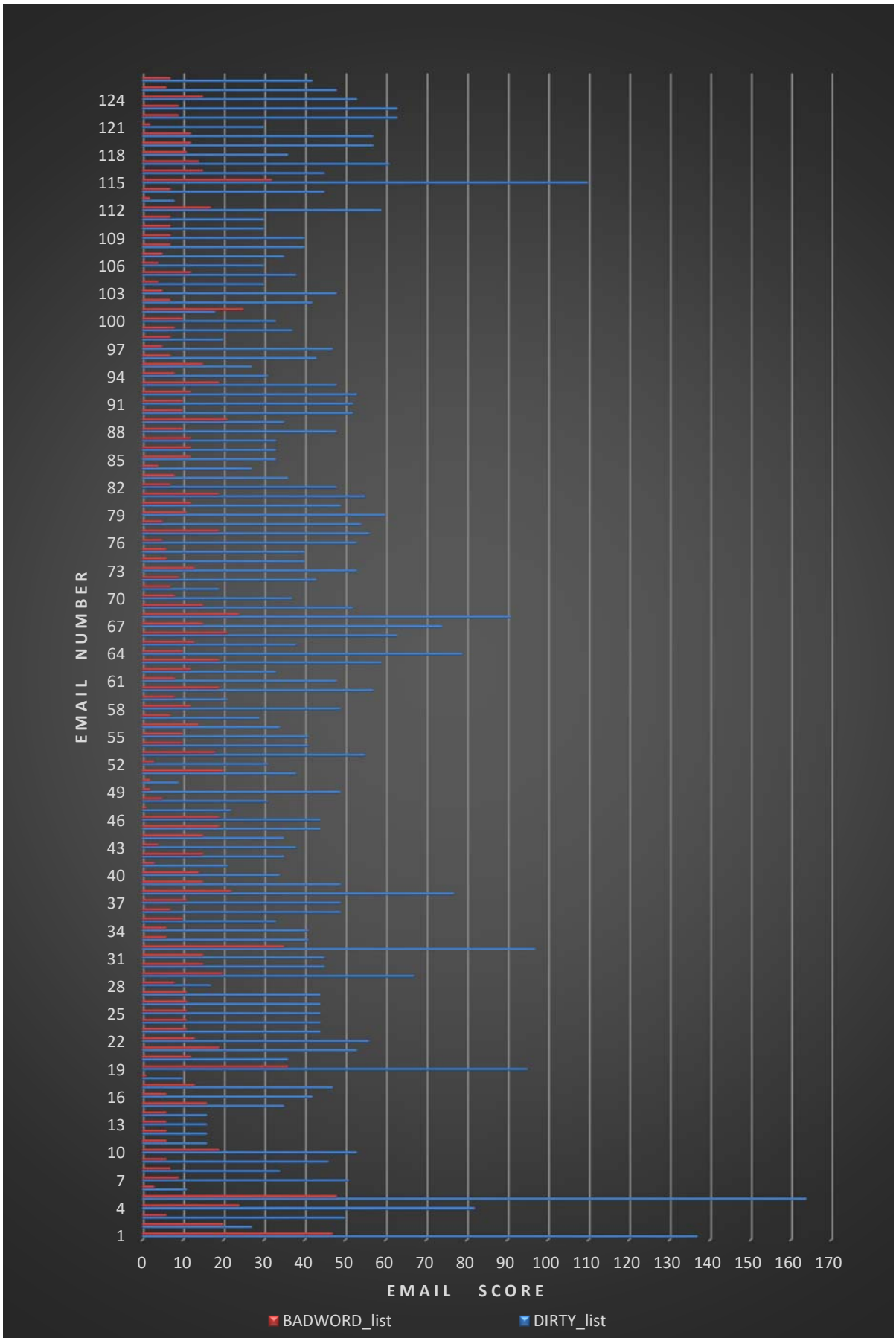
Για τα Clean Emails

Στο **Διάγραμμα 3** , παρατηρούμε το κατά πόσο εσφαλμένα αναγνωρίζει το κάθε Clean Email , από το clean.txt Dataset , ως Hoax η κάθε λίστα του αλγορίθμου. Η DirtyWords[] λίστα παρουσιάζει λιγότερα false negatives, ενώ η Badwords[] λίστα εσφαλμένα παρουσιάζει περισσότερα true positives.

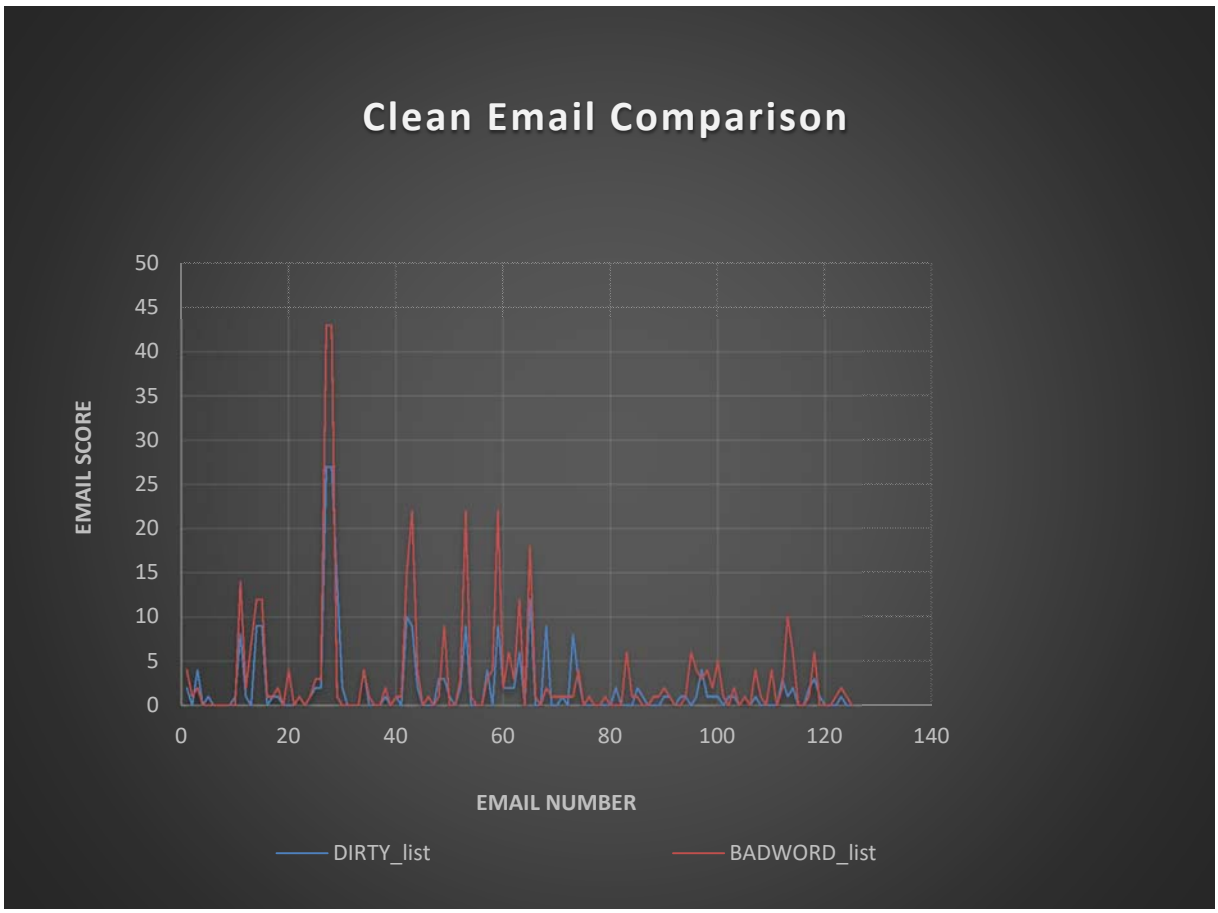
Αντίστοιχα το ίδιο φαίνεται και από το **Διάγραμμα 4** όπου για κάθε Clean Email παρατηρούμε το πλήθος των “triggerwords” , που αναγνωρίζει (εσφαλμένα) η κάθε λίστα του αλγορίθμου. Από το γράφημα φαίνεται , ότι η Badwords[] λίστα αναγνωρίζει εσφαλμένα περισσότερα Clean Email , ως Hoax από ότι η DirtyWords[] λίστα.



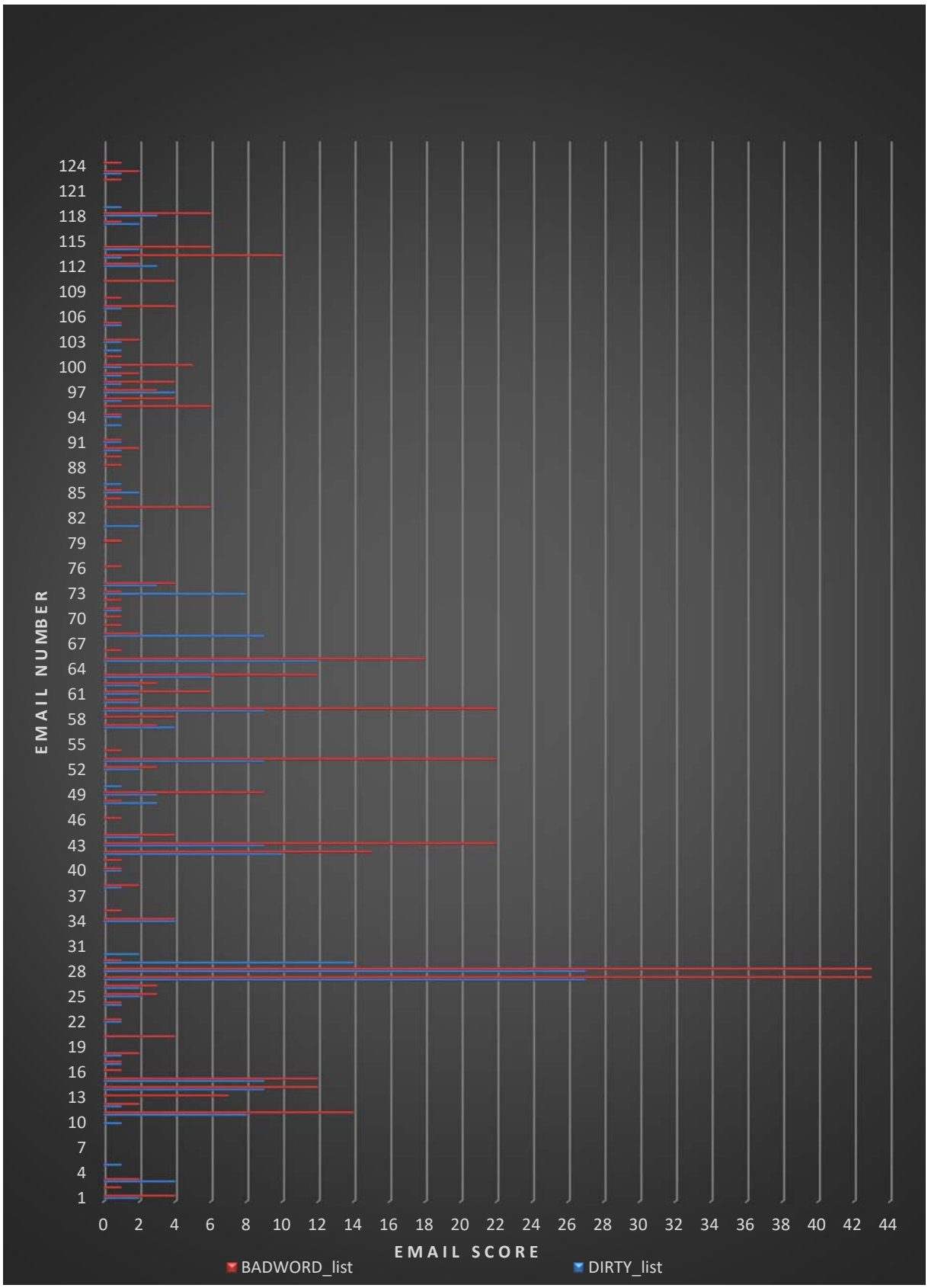
Διάγραμμα 1. Αναπαράσταση του πλήθους των score που εμφανίζονται από τις λίστες του αλγορίθμου , για ένα πλήθος από Hoax Email



Διάγραμμα 2. Αναπαράσταση των συνολικών "triggerwords" , που αναγνωρίζει η κάθε λίστα του αλγορίθμου , για κάθε Hoax Email.



Διάγραμμα 4. Αναπαράσταση των false negatives που φαίνονται στις δύο λίστες του αλγορίθμου για ένα πλήθος από 126 Clean Email.



Διάγραμμα 3. Αναπαρίσταται το ποσοστό λάθους να αναγνωριστεί κάθε Clean Email , του αρχείου Clean.txt email Dataset , ως Hoax Email από τη κάθε λίστα του αλγορίθμου.

Κεφάλαιο 6
Σύνοψη

6.1 Αποτελέσματα Συμπεράσματα

Τα αποτελέσματα των πειραμάτων μας δείχνουν ό,τι το σύστημα που υλοποιεί ο αλγόριθμος DirtyWords[] list εντοπίζει με επιτυχία περισσότερα true positives και λιγότερα false negatives σε σχέση με τη λίστα Badwords[ ] list.

Συγκεκριμένα:

Για τα Hoax Emails όπως φαίνεται στο **Διάγραμμα 1** & στο **Διάγραμμα 2**, από τη σύγκριση των αποτελεσμάτων , των τιμών των δύο λιστών του αλγορίθμου DirtyWords[] list και Badwords[] list , η λίστα του αλγορίθμου DirtyWords[] για κάθε Hoax Email , φαίνεται να παρουσιάζει υψηλότερα score από triggerwords , για το ίδιο δείγμα από Hoax Email σε σχέση με την Badwords[] list.

Εφόσον ο μέσος όρος της διαφοράς των τιμών των δύο λιστών του αλγορίθμου για το τυχαίο δείγμα των 126 Hoax email είναι 33% , συνεπώς μπορούμε να αποφανθούμε ότι το ποσοστό επιτυχίας της λίστας του αλγορίθμου DirtyWords[] list , όσο αφορά την αναγνώριση ενός Hoax Email απο τα 126 Hoax Email , παρουσιάζει υψηλότερο ποσοστό επιτυχίας κατά 33% αντί της Badwords[] list , που παρουσιάζει μικρότερο ποσοστό επιτυχίας στην αναγνώριση ενός Hoax Email.

Το υψηλό ποσοστό επιτυχίας που παρουσιάζει η λίστα του δημιουργηθέντος συστήματος του αλγορίθμου DirtyWords[] , όσο αφορά την αναγνώριση ενός Hoax Email υποδηλώνει ότι έχουμε περισσότερα true positives.

Για τα Clean Emails όπως φαίνεται στο **Διάγραμμα 3** & **Διάγραμμα 4** παρατηρείται ότι κατά μέσο όρο η λίστα του αλγορίθμου DirtyWords[] list , για κάθε Clean Email από τα 126 συνολικά , παρουσιάζει 1.2% λιγότερα score , από ότι η λίστα Badwords[] list. Αυτό σημαίνει ότι η Badwords[] λίστα , υπολογίζει εσφαλμένα ένα Clean Email ως Hoax Email , με μεγαλύτερη πιθανότητα , από ότι η DirtyWords[] list του αλγορίθμου. Συνεπώς αυτό οδηγεί στο συμπέρασμα ότι το υλοποιημένο σύστημα του αλγορίθμου , παρουσιάζει λιγότερα false negatives από ότι η λίστα Badwords[] list.

Σύμφωνα με τα παραπάνω , ένα μήνυμα ηλεκτρονικής απάτης που θα εισέλθει στο σύστημα, η πιθανότητα να μην αναγνωριστεί ως “hoax” είναι μικρότερη , αντί της Badwords[] λίστας. Αν και οι δύο λίστες είναι αρκετά επαρκείς στον εντοπισμό των “clean emails” , η λίστα του αλγορίθμου DirtyWords[] προσεγγίζει με μικρότερο ποσοστό λάθους (από ότι η λίστα Badwords), την αναγνώριση ενός clean email ως Hoax Email (κατά 1,2%) άρα έχουμε λιγότερα false positives. Αυτό συνεπάγεται ότι η πιθανότητα να αναγνωρίσει η DirtyWords[] ένα “clean” email ως “hoax” email είναι μικρότερη αντί της λίστας Badwords[].

Άρα συμπερασματικά , και σύμφωνα με τα παραπάνω αποτελέσματα των πειραμάτων ,

μπορούμε να αποφανθούμε ότι το υλοποιημένο σύστημα , παρουσιάζει λιγότερα false negatives και περισσότερα true positives. Έτσι το σύστημα το οποίο κατασκευάστηκε μπορεί να χρησιμοποιηθεί επιτυχώς, για την επίλυση του προβλήματος.

6.2 Επίλογος

Δεν υπάρχουν εύκολες απαντήσεις στο ερώτημα, για το αν υπάρχει ένα αποτελεσματικό και ολοκληρωμένο σύστημα ασφαλείας που να αποτρέπει επιτυχώς όλες τις επιθέσεις απο hoax emails. Για παράδειγμα, δεν υπάρχει αυτοματοποιημένο σύστημα ή συσκευή δικτύου που να αποτρέπει την εκούσια κατάθεση μεγάλων χρηματικών ποσών σε ύποπτους λογαριασμούς τραπέζης μέσω του διαδικτύου. Αν ένας εισβολέας καταφέρει και εισέλθει στο εσωτερικό δίκτυο μιας εταιρείας ή ενός οργανισμού και υποκλέψει τους λογαριασμούς ηλεκτρονικού ταχυδρομείου των υπαλλήλων και πείσει μέσω hoax email έναν χρήστη, να εκτελέσει μια ενέργεια εμβάσματος, σε τραπεζικό λογαριασμό, τίποτα σε αυτή τη συναλλαγή δεν θα ενεργοποιήσει μια συσκευή δικτύου ώστε να αποτρέψει αυτή την ενέργεια. Η εκπαίδευση των χρηστών του διαδικτύου πάνω σε θέματα της ασφάλειας του ηλεκτρονικού ταχυδρομείου καθώς και η συνεχόμενη ενημέρωσή τους για τις πιο πρόσφατες απειλές στο ηλεκτρονικό ταχυδρομείο, είναι ένας πολύ σημαντικός παράγοντας για την αποτελεσματικότερη αντιμετώπιση των επιθέσεων από hoax emails. Η ευαισθητοποίηση των χρηστών του ηλεκτρονικού ταχυδρομείου, είναι η πρώτη και τελευταία γραμμή άμυνας εναντίον των επιθέσεων από μηνύματα απάτης στο ηλεκτρονικό ταχυδρομείο. Η συνειδητοποίηση είναι καθοριστική, οι εργαζόμενοι στις εταιρείες και στους οργανισμούς πρέπει να εκπαιδεύονται για να ελέγχουν όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου. Πρέπει προσεκτικά να επαληθεύουν και να εξακριβώνουν τα στοιχεία των προμηθευτών. Για μεγάλες μεταφορές χρημάτων, είναι καλή ιδέα για τους υπαλλήλους των εταιρειών, να επιβεβαιώνουν τα αιτήματα εμβασμάτων μέσω προσωπικών ή τηλεφωνικών επικοινωνιών με τα ανώτερα στελέχη της επιχείρησης. Οι κυβερνοεγκληματίες στο διαδίκτυο είναι χρηματοδοτούμενοι, έξυπνοι, συνεργατικοί και καινοτόμοι και πρέπει να εκμεταλλευτούν μόνο μία ευπάθεια για να προκαλέσουν όλεθρο σε έναν χρήστη, οργανισμό ή μια εταιρεία. Το μεγάλο και αυξανόμενο κύμα επιθέσεων από hoax email τα τελευταία χρόνια σηματοδοτεί ότι ο τομέας της ασφάλειας δικτύων χρειάζεται ένα νέο τρόπο προσέγγισης του προβλήματος όπως νέες τεχνολογίες, ολοκληρωμένη και επαρκή κατάρτιση των χρηστών του διαδικτύου με τις ποιο πρόσφατες απειλές, παρέχοντας λύσεις για την αποτελεσματική αντιμετώπιση του φαινομένου.

Παράρτημα Α
Υλοποίηση Συστήματος

```
import re      # standard library re module for regular expression operations
import csv     # standard library csv module for writing (and reading) values in csv files in Python
import pandas as pd   # Pandas library is needed for writing columns in an excel sheet.

############################ 1st DIRTY DATASET ##############################

LearningMail=[]    #Save to every element of a list the corresponding email and an index for every string
MessList=[]        #Save in a list every element at fraud1.txt dataset so to remove all special chars
Messages1=''   #All mail bodies to a string for usage in LearningMail list (1st Dataset) & TestingMail (2nd Dataset)
Messages='' #All mail bodies to a string for usage at MessList list
#     Fraud     1     Dataset     (the     txt     file)     ,          is     needed     for     making     the     Dirty_List
filepath = "C:/Python37/ERGASIA/fraud1.txt" #Set the name of the file-path included folders
with open(filepath) as fp: # Open the file object stored as a variable called fp
 line=fp.readline() # initialize var line
 FLAG=0
 while line: # while line var is true go inside
   line = fp.readline() # Read every line by calling readline on that file object iteratively in a while loop
   if FLAG==1:
      if 'From r' in line: # If "From r" is in line (a new mail is coming up so)
         FLAG=0
         LearningMail.append(Messages1.lower().split()) # Append a sublist to each element of 2D LearningMail [] with splited string values from buffer Messages with lowercase strings
         Messages1=" " #Initialize string buffer equal to zero. This string buffer is needed to be zero, when a new mail comes up for LearningMail list
```

```
        else:

            #A Test for printing lines in an email. The part of email, which will be saved, starts under the block "From r " --- "Status"

            Messages=Messages+line # string buffer is needed for MessList [] list

            Messages1=Messages1+line  # string buffer is needed for LearningMail [] list. Add readable lines to string buffer which is needed for LearningMail list (1st Dataset). Var is initialized above.


    if FLAG==0:     # at the first time start from this section of code:

        if 'Status: ' in line: # if in line has been found 'Status: '

            FLAG=1   #make the flag equal to one


# MESSLIST a list with lowercase letters and without punctuations. Is made from splited strings, from buffer Messages (at fraud1 emails).


for word in Messages.split():                    # String Messages are splited one by one

    without_punc= re.sub(r'[^\w]','',word)      # then remove special chars

    MessList.append(without_punc.lower()) # Make a sublist of strings with lowercase letters

    #print (MessList)                            # print every string without special chars


# BADWORDS[] LIST MADE FROM THE INTERNET

with open("C:/Python37/ERGASIA/Badwords.txt", "r") as ins: # Open (for reading) the txt file which contains spam words (last updated list from the internet)

    Badwords=[]                                      # Initialize a list which  includes spam words

    for line in ins:                                 # Read the file

     without_punc1= re.sub(r'[\n]','',line)          # Remove special characters from strings of the list

     Badwords.append(without_punc1.lower())   # lowercase strings of the list

#print(Badwords)


# WHITELIST MADE FROM THE INTERNET

with open("C:/Python37/ERGASIA/Whitelist.txt", "r") as ins1: # open (for reading) the txt file which contains non-spam words (last updated list from the internet)

    WhiteList=[]                                     # Initialize a list which  includes non-spam words

    for line in ins1:                                # For every element in the list

     without_punc2= re.sub(r'[\n]','',line)          # Remove special characters from strings of the list

     WhiteList.append(without_punc2.lower())  # lowercase strings of the list

#print(WhiteList)
```

```
# DIRTY WORDS LIST MADE FROM ALLWORDSLIST

ALLWords=[]          # Initialize the list. (In list are contained all strings that are not included in Whitelist)

for item in MessList:              # For every element of MessList

    if item not in ALLWords:       # Avoid duplicate list entries

      if item not in WhiteList[0]:     # If string from MessList is not found at Whitelist

         ALLWords.append(item)         # Append it to AllWords list


DirtyWords=[] # This is the statement of the Dirty_List

DirtyCount=[] # This is a list with a sublist. Every element referred to a spam word and how often this spam word is used (weight)


for item in ALLWords:

 if  MessList.count(item)>50: # Register spam words with a frequent usage of 50times and above

    DirtyWords.append(item)   # Append the elements in the list

    DirtyCount.append([item,MessList.count(item)]) # The list contains an element and a sublist to it , with other 2 elements: The 1st element is the spam word (from the Dirty_List) and the 2nd element referred to the frequent usage of the word

#print("\n\n SPAM WORDS FOUND in 1st Dataset FRAUD1.txt  by Dirty_List: \n\n\n " , DirtyWords , " ")

print("\n\n##########################################################################################################\n")

print("############################    F R E Q U E N T L Y    U S E D    W O R D S    A N A L Y S I S    ########################\n")

print("############################################## F O R     D I R T Y     L I S T ######################################\n")

print("##########################################################################################################\n\n")

# Sort (most used) spam words founded by Dirty_List

SortedCount = sorted(DirtyCount, key=lambda x: x[1],reverse=True) # Copy the Sorted values of DirtyCount list to the SortedCount list

print("MOST USED WORDS BY DIRTY LIST in Fraud1.txt \n\n\n",SortedCount) # print sorted values by frequent usage weight


MFUWtxt = "C:/Python37/ERGASIA/MFUW" #Set the name of the file-path (included folders)

with open(MFUWtxt, "w") as output:  # Open (for writing values) the MFUWtxt.csv file in the existing filepath

   writer = csv.writer(output, lineterminator='\n')  # Usage the writer() method of csv module , for writing values in file .

   writer.writerow(["MFUW (Word)", "MFUW (Weight)"]) # The csv file contains 2 rows: the spam word of Dirty_List , and the value of frequent usage.
```

```
    writer.writerows(SortedCount) # Write values of SortedCount List  into the csv file MFUW.txt


############################## 2nd DIRTY DATASET ############################


# Fraud 2 Dataset (the txt file) , is needed for comparing the results of two lists Count_DIRTY_WORD , Count_BAD_WORD

print("\n\n#########################################################################\n")
print("###################### H O A X    e-M A I L S ######################\n")
print("######################## 2nd  D A T A S E T ########################\n")
print("#########################################################################\n")

TestingMail=[] # this list contains a sublist of all 126 spam emails of the 2nd Dataset

filepath = "C:/Python37/ERGASIA/fraud2.txt" #Set the name of the file-path included folders

with open(filepath) as fp: # Open (for reading) the file object (fraud2.txt) as a variable called fp

  line=fp.readline() # initialize var line

  FLAG=0

  while line:  # while line var is true go inside

   line = fp.readline() # Read every line by calling readline on that file object iteratively in a while loop

   if FLAG==1:
       if 'From r' in line: # If "From r" is in line ( a new mail is coming up so)
           FLAG=0         # make the flag equal to zero ( so later start reading from Status RO line)
           TestingMail.append(Messages1.lower().split()) # Append a sublist to each element of 2D TestingMail[] list with splited string values from buffer Messages with lowercase strings
           Messages1=" " #Initialize string buffer equal to zero. This string buffer is needed to be zero , when a new mail comes up for TestingMail list
```

```
        else:

            #print (line) #A Test for printing lines in an email. The part of email, which will be saved, starts under the block "From r " --- "Status"


            Messages1=Messages1+line # string buffer is needed for TestingMail [] list.  Add readable lines to string buffer which is needed for TestingMail list (2nd Dataset). Var is initialized above.


    if FLAG==0: # at the first time start from this section of code:

        if 'Status: ' in line: # if in line has been found 'Status: '

            FLAG=1 #make the flag equal to one



HOAX_Score_DIRTY=[]  # One-dimensional list containing the number of email "spam frequent usage words (=weight)"  of (126) emails counted by Dirty_List[]

HOAX_Score_BAD=[] # One-dimensional list containing the number of (126) emails counted by Badword[] list


for i in range(len(TestingMail)): # Check all 126 emails (from Dataset2 ) one by one


    Count_DIRTY_WORD=0 # initialize var counter of Dirty_List

    Count_BAD_WORD=0 # initialize var counter of Badword[] list


    for j in range(len(TestingMail[i])):


        if TestingMail[i][j] in DirtyWords: #if a spam word found in TestingMail list from the DirtyWords[] list then:

            #print('>>>>>>>>>>> FOUND',TestingMail[i][j],'---->',DirtyWords.index(TestingMail[i][j])) #a test to print the spam word , and the exact adress of the DirtyWords[] list list

            Count_DIRTY_WORD+=1            #and increase the value of counter by one


        if TestingMail[i][j] in Badwords:  #if a spam word found in TestingMail[]  list from the Badword[] list then:

            #print('>>>>>>>>>>> FOUND',TestingMail[i][j],'---->',Badwords.index(TestingMail[i][j])) # print the spam word , and the exact adress of the Badwords[] list list

            Count_BAD_WORD+=1            #and increase the value of counter by one

    print("\nEmail:",TestingMail.index(TestingMail[i])+1, "\n\n")  # the number of email checked

    print("FOUND",Count_DIRTY_WORD,"words appear in Dirty_List")   # how many spam words appear in this email (from DirtyWords[] list)
```

```
  print("FOUND",Count_BAD_WORD,"words appear in Badword.txt\n") # how many spam words appear in this email (from Badwords[] list)

  print('-----------------------------------')

  HOAX_Score_DIRTY.append(Count_DIRTY_WORD) # This is a 1D list including the number of total spam words (found by DirtyWords[] list) for every email which have been analyzed).

  HOAX_Score_BAD.append(Count_BAD_WORD) # This is a 1D list including the number of total spam words (found by Badwords[] list) for every email which have been analyzed).

  print('-----------------------------------\n')


#####################  ANALYSIS FOR DIRTYWORDS AND  BADWORDS.TXT ####################


print("\n\n#########################################################################################
########################################\n")

print("############################ H O A X   A P P E A R   F R E Q U E N C Y   A N A L Y S I S
#######################\n")

print("############################################### F O R   H O A X   E M A I L S
################################\n")

print("#########################################################################################
####################################\n\n")


print("\n\n TOTAL HOAX EMAILS FOR ANALYSIS:",TestingMail.index(TestingMail[i])+1) # total number of emails that are analyzed via TestingMail list


print('\n\n=======================Count SPAM Words from two
lists============================\n\n')


## this section of code refers to the analysis of spam words found by Dirty list for each email

print('\n\n==========================DIRTY_LIST=================================\n\n')


HOAX_Score_DIRTY.sort() # sort the 1D list according to number of total spam words found in Dirtyword[] (for every email which have been analyzed)

FMD_array=pd.Series(HOAX_Score_DIRTY).value_counts().reset_index().values.tolist() # create a 2D list in which one every element includes 2 values. the 1st is the number of total spam words and the 2nd is the exact number of the referred email (of 126 emails)

FMD_array.sort() # sort the list according to the number of total spam words


print("SORTED TOTAL SCORE APO DIRTYWORD LIST: \n\n",HOAX_Score_DIRTY,"\n") #print values of 1D list includes the number of spam words (found by DirtyWords[] list) for every email analyzed)
```

```
print("\n\nMails and word-scores in FMD_array : \n\n1st element x-x' : (score-words) \n2nd element y-y' : (mail-counter)\n\n",FMD_array)


## Below is shown the Process of writing the relevant values from 2D list (FMD_array list) to a csv file

FMDtxt = "C:/Python37/ERGASIA/FMD_array" #Set the name of the file-path that we want to write (included folders)

with open(FMDtxt, "w") as output: # Open (for writing) the relevant path (included the file object FMD_array) marked as FMD.txt

    writer = csv.writer(output, lineterminator='\n') # When a line ends , write below to the next line

    writer.writerow(["FMD x-x' (score)", " FMD y-y' (counter)"]) # write in file by rows and not by columns. write values under two rows: FMD x-x' (score) & FMD y-y' (counter)

    writer.writerows(FMD_array) #write in csv file , the relevant values from  FMD_array


## this section of code refers to the analysis of spam words found by Badword list for each email

print('\n\n=========================BADWORD.TXT=====================================\n\n')


HOAX_Score_BAD.sort() # sort the list according to number of total spam words found in Badword[] list (for every email analyze)

FMB_array=pd.Series(HOAX_Score_BAD).value_counts().reset_index().values.tolist() # create a 2D list in which one , each element includes 2 values. the 1st is the number of total spam words and the 2nd is the exact number of the referred email (of 126 emails)

FMB_array.sort() # sort the list according to the number of total spam words


print("\nSORTED TOTAL SCORE APO BADWORD.txt: \n\n",HOAX_Score_BAD,"\n") #print values of 1D list includes the number of spam words ( found by Badword[] list) for every email analyzed)

print("\n\nMails and word-scores in FMB_array \n\n1st element x-x' : (score-words) \n2nd element y-y' : (mail-counter)\n\n",FMB_array)


FMBtxt = "C:/Python37/ERGASIA/FMB_array" #Set the name of the file-path that we want to write (included folders)


with open(FMBtxt, "w") as output: # Open (for writing) the relevant path (included the file object FMB_array) marked as FMD.txt

    writer = csv.writer(output, lineterminator='\n') # When a line ends , write below to the next line

    writer.writerow(["FMB x-x' (score)", " FMB y-y' (counter)"]) # write in file by rows and not by columns. write values under two rows: FMD x-x' (score) & FMD y-y' (counter)

    writer.writerows(FMB_array) #write in csv file , the relevant values from  FMD_array


print('\n\n==========Analyze each email , and compare values between DirtyWords[] list and Badwords[] list ==================\n\n')
```

```
for i in range(len(TestingMail)): # For each email in 2nd dataset (Fraud2.txt)

    Count_DIRTY_Mail=0  #  initiallize var counter of Dirtyword[] list
    Count_BAD_Mail=0    #  initiallize var counter of Badword[] list

    for j in range(len(TestingMail[i])):

        if TestingMail[i][j] in DirtyWords: # if a spam word found in TestingMail[]  list from the Dirtyword[] list then:
          Count_DIRTY_Mail+=1           # increase counter value by one

        if TestingMail[i][j] in Badwords:  # if a spam word found in TestingMail[]  list from the Badword[] list then:
          Count_BAD_Mail+=1           # increase counter value by one

    print('Email No: ',i,'--DIRTY=',Count_DIRTY_Mail,'--BAD=',Count_BAD_Mail)

print('++++++++++++++++++++++++++++++++++++++++++++')
```

3o CLEAN DATASET

```
# CLEAN 3rd Dataset (the txt file) , is needed for comparing the results of two lists Count_DIRTY_WORD , Count_BAD_WORD

print("\n\n#############################################################################\n")
print("###################### C L E A N  e-M A I L S ########################\n")
print("######################### 3rd  D A T A S E T ##########################\n")
print("#############################################################################\n")

REAL_Score_DIRTY=[] # One-dimensional list containing the number of (126) emails. we need it to add later the totalnumber spam words found by the DirtyWords[] list for each email
REAL_Score_BAD=[]   # One-dimensional list containing the number of (126) emails. we need it to add later the totalnumber spam words found by the DirtyWords[] list for each email

CleanMail=[] # this list contains a sublist of all 126 spam emails of the 3rd Dataset
```

```
StringBuffer='' #All mail bodies to a string buffer for usage in Cleaning Mail[]  list

filepath = "C:/Python37/ERGASIA/clean.txt"  #Set the name of the file-path included folders

with open(filepath) as fp: # Open the file object stored as a variable called fp

 line=fp.readline() # initialize var line

 FLAG=0

 while line: # while line var is true go inside

   line = fp.readline() # Read every line by calling readline on that file object iteratively in a while loop

   if FLAG==1:

      if '"allen-p' in line:  # If '"allen-p' is in line ( a new mail is coming up so)

         FLAG=0          # make the flag equal to zero ( so later start reading from 'X-FileName' line)

         CleanMail.append(StringBuffer.lower().split()) # Append a sublist to each element of 2D CleanMail[] list  with splited string values from StringBuffer with lowercase strings

         StringBuffer=" "  #Initialize string buffer equal to zero. This string buffer is needed to be zero , when a new mail comes up for CleanMail list


      else:

         #A Test for printing lines in an email. The part of email , which will be saved , starts under the block '"allen-p' --- 'X-FileName'

         StringBuffer=StringBuffer+line  # string buffer is needed for CleanMail [] list. Add readable lines to string buffer which is needed for CleanMail list (3rd Dataset).


   if FLAG==0:                    # at the first time start from this section of code:

      if 'X-FileName' in line:    # if in line has been found 'X-FileName'

         FLAG=1               # make the flag equal to one


for i in range(len(CleanMail)):
```

```
 Count_DIRTY_WORD=0  # initiallize var counter of Dirtyword[] list

 Count_BAD_WORD=0    # initiallize var counter of Badword[] list


 for j in range(len(CleanMail[i])):


     if CleanMail[i][j] in DirtyWords:  #if a spam word found in CleanMail [] list from the DirtyWord[] list  then:

         #print('>>>>>>>>>> FOUND',CleanMail[i][j],'---->',DirtyWords.index(CleanMail[i][j]))   #a test to print the spam word , and the exact address of the DirtyWords[] list

         Count_DIRTY_WORD+=1              #and increase the value of counter by one

     if CleanMail[i][j] in Badwords:         #if a spam word found in CleanMail [] list from the Badword[] list then:

         Count_BAD_WORD+=1            #and increase the value of counter by one

         #print('>>>>>>>>>> FOUND',CleanMail[i][j],'---->',Badwords.index(CleanMail[i][j]))      #a test to print the spam word , and the exact adress of the Badwords[] list


 print("\nEmail:",CleanMail.index(CleanMail[i])+1,"\n\n")       # the number of email checked

 print("FOUND",Count_DIRTY_WORD,"words appear in Dirty_List")    # how many spam words appear in this email (from DirtyWords[] list)

 print("FOUND",Count_BAD_WORD,"words appear in Badword.txt\n")  # how many spam words appear in this email (from Badwords[] list)

 print('-----------------------------------')


 REAL_Score_DIRTY.append(Count_DIRTY_WORD)  # This is a 1D list including the number of total spam words (found by DirtyWords[] list) for each email have been analyzed from CleanMail list).

 REAL_Score_BAD.append(Count_BAD_WORD)    # This is a 1D list including the number of total spam words (found by Badwords[] list) for each email have been analyzed from CleanMail list).


 print('-----------------------------------')


################### ANALYSIS FOR DIRTYWORDS AND  BADWORDS.TXT #################


print("\n\n#########################################################################################\n")

print("############################ H O A X   A P P E A R   F R E Q U E N C Y   A N A L Y S I S ########################\n")

print("############################################## F O R   C L E A N   E M A I L S ##################################\n")

print("#########################################################################################\n\n")
```

```
print("\n\n TOTAL CLEAN EMAILS FOR ANALYSIS: ",CleanMail.index(CleanMail[i])+1)      # total number of emails that are analyzed via TestingMail list


print('\n\n======================Count SPAM Words from two lists============================\n\n')


## this section of code refers to the analysis of spam words found by Dirty list for each email


print('\n\n======================DIRTY_LIST=========================\n\n')


REAL_Score_DIRTY.sort()   # sort the 1D list according to number of total spam words found in DirtyWords[] list (for every email which have been analyzed)

RMD_array=pd.Series(REAL_Score_DIRTY).value_counts().reset_index().values.tolist()  # create a 2D list in which one every element includes 2 values. 1st element is the number of total spam words appear in the email and the 2nd element is how many emails appeared

RMD_array.sort()      # sort the list according to the number of total spam words


print("SORTED TOTAL SCORE APO DIRTYWORD LIST: \n\n",REAL_Score_DIRTY)  #print values of 1D list includes the number of spam words (found by DirtyWords[] list) for every email analyzed)

print("\n\nMails and word-scores in RMD_array : \n\n1st element x-x' : (score-words) \n2nd element y-y' : (mail-counter)\n\n",RMD_array)


# Below is shown the Process of writing the relevant values from 2D list (FMD_array list) to a csv file


RMDtxt = "C:/Python37/ERGASIA/RMD_array"   #Set the name of the file-path that we want to write (included folders)

with open(RMDtxt, "w") as output:    # Open (for writing) the relevant path (included the file object RMD_array) marked as RMDtxt

  writer = csv.writer(output, lineterminator='\n')  # When a line ends , write below to the next line

  writer.writerow(["RMD x-x' (score)", " RMD y-y' (counter)"])  # write in file by rows and not by columns. write values under two rows: RMD x-x' (score) & RMD y-y' (counter)

  writer.writerows(RMD_array)  #write in csv file , the relevant values from  RMD_array


# this section of code reffers to the analysis of spam words found by Badword list for each email


print('\n\n======================BADWORD.TXT============================\n\n')
```

```
REAL_Score_BAD.sort()  # sort the list according to number of total spam words found in Badwords[] list (for every email analyze)

RMB_array=pd.Series(REAL_Score_BAD).value_counts().reset_index().values.tolist()  # create a 2D list in which one , each element includes 2 values. the 1st is the number of total spam words and the 2nd is the exact number of the reffered email (of 126 emails)

RMB_array.sort()      # sort the list according to the number of total spam words


print("\nSORTED TOTAL SCORE APO BADWORD.txt: \n\n",REAL_Score_BAD,"\n")  #print values of 1D list includes the number of spam words ( found by Badwords[] list) for every email analyzed)

print("\n\nMails and word-scores in RMB_array \n\n1st element x-x' : (score-words) \n2nd element y-y' : (mail-counter)\n\n",RMB_array)


RMBtxt = "C:/Python37/ERGASIA/RMB_array" #Set the name of the file-path that we want to write (included folders)

with open(RMBtxt, "w") as output:   # Open (for writing) the relevant path (included the file object RMB_array) marked as RMBtxt

   writer = csv.writer(output, lineterminator='\n') # When a line ends , write below to the next line

   writer.writerow(["RMB x-x' (score)", " RMB y-y' (counter)"])   # write in file by rows and not by columns. write values under two rows: RMB x-x' (score) & RMB y-y' (counter)

   writer.writerows(RMB_array) #write in csv file , the relevant values from  RMB_array



print('\n\n==========Analyze each email , and compare values between DirtyWords[] list and Badwords[] list ==========\n\n')


for i in range(len(CleanMail)):  # For each email in 3rd dataset (Clean.txt)


   Count_DIRTY_Mail=0   # initialize var counter of DirtyWords[] list

   Count_BAD_Mail=0    # initialize var counter of Badword[] list


   for j in range(len(CleanMail[i])):


      if CleanMail[i][j] in DirtyWords:   # if a spam word found in CleanMail[] list from the DirtyWords[] list then:

         Count_DIRTY_Mail+=1          # increase counter value by one


      if CleanMail[i][j] in Badwords:    # if a spam word found in CleanMail[] list from the Badwords[] list then:
```

```
        Count_BAD_Mail+=1            # increase counter value by one


    print('CLEAN Email No: ',i,'--DIRTY=',Count_DIRTY_Mail,'--BAD=',Count_BAD_Mail)


print('+++++++++++++++++++++++++++++++++++++++++++')
```

Βιβλιογραφία

Retruster LTD, (2019) Learn About Phishing Email Statistics For 2019 https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html [Πρόσβαση: 01.12.2019]

Sklavos, N., Souras P., (2006) Economic Models and Approaches in Information Security for Computer Networks. *International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January 2006, pp. 14-20*

Bikos, A., Sklavos, N., (2013 LTE/SAE Security Issues on 4G Wireless Networks. *IEEE Security and Privacy, Issue March/April, Vol. 11, No. 2, pp. 55-62, 2013*

Zeadally, A., Das K., Sklavos N., (2019) Cryptographic Technologies and Protocol Standards for Internet of Things. *Internet of Things: Engineering Cyber Physical Human Systems, Elsevier Science Press, 2019*

Muncaster, P. (2018) Save the Children Hit by $1m BEC Scam. https://www.infosecurity-magazine.com/news/save-the-children-hit-by-1m-bec/ [Πρόσβαση: 29.06.2019]

NCCIC, National Cybersecurity and Communications Integration Center (2018) TROJAN VARIANTS https://www.cyber.nj.gov/threat-profiles/trojan-variants/olympic-destroyer [Πρόσβαση: 14.02.2018]

Emm, D., Chebyshev, V. (2018) Kaspersky Security Bulletin 2018. Top security stories. https://securelist.com/kaspersky-security-bulletin-2018-top-security-stories/89118/ [Πρόσβαση: 03.12.2018]

Peterson, P., ACID, Agari Cyber Intelligence Division (2019) Email Fraud and Identify Deception Trends. https://www.agari.com/email-fraud/ebooks/q2-2019-report.pdf. [Πρόσβαση: 29.04.2019]

Nahorney, B., Symantec, ISTR Internet Security Threat Report (2017) Email Threats. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-email-threats-2017-en.pdf [Πρόσβαση: 20.12.2017]

Symantec, (2019) ISTR Internet Security Threat Report Vol24. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf [Πρόσβαση: 27.03.2019]

Kaspersky, (2018) Kaspersky Security Bulletin 2018 Statistics. https://securelist.com/kaspersky-security-bulletin-2018-statistics/89145/ [Πρόσβαση: 05.12.2018]

George, A, (2019) McAfee says 2019 may be the year where malware is a threat in every device. https://www.digitaltrends.com/computing/mcafee-2019-threat-report-predicts-everywhere-malware/ [Πρόσβαση: 26.02.2019]

Malwarebytes Labs , (2018) Malwarebytes' 2019 security predictions. https://blog.malwarebytes.com/cybercrime/2018/11/malwarebytes-2019-security-predictions/ [Πρόσβαση: 28.11.2018]

NFCCRC, National Fraud & Cyber Crime Reporting Centre (2016) Scam emails. https://www.actionfraud.police.uk/scam-emails [Πρόσβαση: 15.02.2016]

FBI, Federal Bureau of Investigation (2017) Common Fraud Schemes. https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud [Πρόσβαση: 19.06.2017]

Ellis, D., (2019) Top 10 Types Of Phishing Emails. https://www.securitymetrics.com/blog/top-10-types-phishing-emails [Πρόσβαση: 10.10.2019]

McCabe, J., (2017) FBI Warns of Death Threat Email Scams. https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-death-threat-email-scams [Πρόσβαση: 21.12.2017]

Tatham M., (2018) Fraud & Identity Theft. The Ultimate List of the Year's Worst Scam.https://www.experian.com/blogs/ask-experian/the-ultimate-list-of-the-years-worst-scams/ [Πρόσβαση: 01.02.18]

IATA, International Air Transport Association (2019) Email & Website Fraud. Protection. https://www.iata.org/Pages/fraudulent-emails-websites.aspx [Πρόσβαση: 23.08.2019]

IATA, International Air Transport Association (2019) Fraudulent Emails. https://www.iata.org/documents/fraudulent-emails-warning.pdf [Πρόσβαση: 25.08.2019]

FBI, Federal Bureau of Investigation (2018) How to Protect Your Computer. https://www.fbi.gov/scams-and-safety/on-the-internet [Πρόσβαση: 11.11.2018]

Kaspersky, (2018) Learn about malware and how to protect all your devices against it. https://www.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it [Πρόσβαση: 10.12.2018]

ESET, (2019) What is malware? https://www.eset.com/us/antimalware/ [Πρόσβαση: 03.03.2019]

Unuchek, R., Sinitsyn, F., Parinov, D., Liskin, A., (2017) IT threat evolution Q3 2017. Statistics. https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/ [Πρόσβαση: 10.11.2017]

Price, R., (2017) Hackers are using a devilishly clever fake email attachment scam to break into people's accounts.

https://www.businessinsider.com/hackers-fake-email-attachment-scam-spoof-subject-lines-break-into-accounts-2017-1?r=UK [Πρόσβαση: 17.01.2017]

Benhayon, S., (2017) Phishing What is it and could it impact you? https://www.allrisesaynotocyberabuse.com/single-post/phishing-what-is-it-and-could-it-impact-you [Πρόσβαση:26 .12.2017]

Fraud Watch International, (2016) Phishing What is it and could it impact you? https://fraudwatchinternational.com/expert-explanations/what-is-a-bec-scam/ [Πρόσβαση:07.07.2016]

DI , Defence Intelligence (2017) Phishing And Its Impact On Businesses AndEmployees https://defintel.com/blog/index.php/2017/02/phishing-and-its-impact-on-businesses-and-employees.html [Πρόσβαση:23.02.2017]

Norton, (2019) How to help protect against 5 types of phishing scams https://us.norton.com/internetsecurity-online-scams-how-to-protect-against-phishing-scams.html [Πρόσβαση:25.05.2019]