ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΟΝΤΕΛΟΠΟΙΗΣΗ ΤΩΝ ΕΝΕΡΓΕΙΩΝ ΕΞΑΠΑΤΗΣΗΣ ΧΡΗΣΤΩΝ ΔΙΑΔΙΚΤΥΟΥ ΜΕΣΩ ΤΗΣ ΥΠΗΡΕΣΙΑΣ EMAIL ΚΑΙ ΔΗΜΙΟΥΡΓΙΑ ΙΣΤΟΤΟΠΟΥ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

ΜΠΟΥΡΗΣ ΦΩΤΙΟΣ, ΜΑΛΛΙΟΣ ΣΩΤΗΡΙΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΡ. ΠΙΕΡΡΑΚΕΑΣ ΧΡΗΣΤΟΣ

ΠΑΤΡΑ 2019

ΠΡΟΛΟΓΟΣ

Το διαδίκτυο, η μεγαλύτερη δεξαμενή πληροφοριών στο κόσμο καθίσταται σταδιακά αναπόσπαστο κομμάτι της καθημερινής ζωής, ενώ είναι ανοιχτό τόσο στους καλόβουλους όσο και στους κακόβουλους επισκέπτες. Ο πληθυσμός του Internet, αν και έχει δεχτεί κατά καιρούς πολλές παραβιάσεις και παρενοχλήσεις όσον αφορά την ασφάλεια των συστημάτων και την κλοπή δεδομένων, δεν έχει υιοθετήσει μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν τη δικτυακή ασφάλεια, με αποτέλεσμα ολοένα και περισσότεροι χρήστες να βρίσκονται σε σύγχυση. Μαζί με την ανάπτυξη του Διαδικτύου και του ηλεκτρονικού ταχυδρομείου, σημειώθηκε δραματική αύξηση των ανεπιθύμητων μηνυμάτων τα τελευταία χρόνια. Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται καθημερινά από εκατομμύρια ανθρώπους, για να επικοινωνούν σε όλο τον κόσμο και αποτελεί μια κρίσιμη εφαρμογή για πολλές επιχειρήσεις. Τα ανεπιθύμητα μηνύματα, αποτελούν ένα από τα ταχέως αναπτυσσόμενα και δαπανηρά προβλήματα που συνδέονται με το Διαδίκτυο σήμερα. Ωστόσο, είναι εκπληκτικό το γεγονός ότι παρά την αυξανόμενη ανάπτυξη των υπηρεσιών και τεχνολογιών κατά της ανεπιθύμητης αλληλογραφίας, ο αριθμός των ανεπιθύμητων μηνυμάτων εξακολουθεί να αυξάνεται με ταχύ ρυθμό. Ο αυξανόμενος όγκος ανεπιθύμητης αλληλογραφίας έχει καταστεί σοβαρή απειλή όχι μόνο για το διαδίκτυο, αλλά και για την κοινωνία. Επηρεάζει όλους τους σημαντικούς τομείς της βιομηχανίας μέρα με τη μέρα με κατάχρηση των διαπιστευτηρίων χρήστη. Το ηλεκτρονικό ταχυδρομείο έχει γίνει ένα ισχυρό εργαλείο που προορίζεται για την ανταλλαγή ιδεών και πληροφοριών, καθώς και για την εμπορική και κοινωνική ζωή των χρηστών. Το ηλεκτρονικό «ψάρεμα» (Phishing) είναι μια μορφή ηλεκτρονικής δόλιας δραστηριότητας στην οποία ο εισβολέας σκοπεύει να κλέψει τις ευαίσθητες πληροφορίες ενός θύματος, όπως έναν κωδικό e-banking ή έναν αριθμό πιστωτικής κάρτας. Με συνδυασμό τεχνικών πλαστογράφησης και social engineering, τα θύματα εξαπατούνται και παρέχουν τέτοιες πληροφορίες.

ΠΕΡΙΛΗΨΗ

Το διαδίκτυο λίγα χρόνια πριν αποτελούσε ένα περιορισμένο δίκτυο, συνήθως μεταξύ πανεπιστημιακών και στρατιωτικών μονάδων. Με την πάροδο των ετών σημειώθηκε τεράστια ανάπτυξη και εξάπλωση του διαδικτύου σε πολλούς τομείς της καθημερινότητάς μας, με αποτέλεσμα τον εκθετικό πολλαπλασιασμό γενικής μετατροπής των δεδομένων πάσης φύσεως σε ψηφιακή ηλεκτρονική μορφή. Αντίστοιχα όμως παρατηρείται ανάπτυξη και εξάπλωση σε παγκόσμια κλίμακα όσον αφορά την υποκλοπή των προσωπικών δεδομένων, μέσω του ηλεκτρονικού "ψαρέματος" το οποίο αποτελεί το κύριο αντικείμενο της παρούσας εργασίας.

ABSTRACT

The internet a few years ago was a limited network, usually between university and military units. Over the years there has been tremendous growth and deployment of the Internet in many areas of our daily lives, resulting in exponential multiplication of generic conversion of data of any kind into digital electronic form. However, there is a worldwide development and spread of personal data interception, caused by electronic "phishing" witch is the main consept of the present work.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Διαδίκτυο, υποκλοπή προσωπικών δεδομένων, ψηφιακή ηλεκτρονική μορφή, ηλεκτρονικό "ψάρεμα"

KEYWORDS

Internet, personal data interception, digital electronic form, electronic "phishing"

Πίνακας περιεχομένων

ΑΠΟΔΟΣΗ ΟΡΩΝ

Hacker : άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους

Phishing : ηλεκτρονική απάτη

Phishers: άτομο που προσπαθεί να εξαπατήσει ανθρώπους ώστε, να δώσουν πληροφορίες μέσω του Διαδικτύου ή μέσω ηλεκτρονικού ταχυδρομείου.

Malware : κακόβουλο λογισμικό

Botnet : Εκτελούνται από συσκευές που μπορούν να συνδεθούν στο διαδίκτυο. Μπορούν να χρησιμοποιηθούν για την εκτέλεση κατανεμημένης επίθεσης άρνησης.

ΕΙΣΑΓΩΓΗ

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 εμφάνιση 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 ως hackers, βρίσκουν πρόσφορο έδαφος για να δράσουν έχοντας ως απώτερο σκοπό την απόσπαση χρηματικού ποσού.

Οι σύγχρονοι hackers έχουν από καιρό συνειδητοποιήσει ότι ο ευκολότερος τρόπος να παραδώσουν τα εργαλεία επίθεσης τους είναι να επικεντρωθούν στο «εσωτερικό» του οργανισμού. Η μόλυνση ενός χρήστη με κακόβουλο λογισμικό μπορεί να δώσει στους εισβολείς οτιδήποτε χρειάζονται για να ξεκινήσουν μια πολύ πιο σημαντική διείσδυση σε ένα δίκτυο οργανισμού, να κλέψουν τα διαπιστευτήρια, να διαταράξουν κρίσιμες διαδικασίες ή να κρυπτογραφήσουν τα δεδομένα και να τα καταστήσουν απρόσιτα έως ότου ικανοποιηθούν οι απαιτήσεις τους.

Το ηλεκτρονικό «ψάρεμα», ή αλλιώς phishing θεωρείται ένας διαδικτυακός τρόπος εξαπάτησης των χρηστών του διαδικτύου. Συγκεκριμένα αυτή η ηλεκτρονική δραστηριότητα δημιουργεί μηνύματα με την μορφή email με σκοπό να παραπλανήσει τους χρήστες. Αυτό γίνεται γιατί οι ιστοσελίδες και τα ηλεκτρονικά εργαλεία δεν είναι σωστά προστατευμένα .Η συγκεκριμένη μορφή εμφανίστηκε την δεκαετία του 90’. Μέσα σε αυτά τα χρόνια κατάφερε να εξελιχθεί με διάφορες μορφές. Η ηλεκτρονική μορφή των μηνυμάτων στην αρχή φαίνεται αξιόπιστη, με αποτέλεσμα πολλοί χρήστες να παραπλανούνται. Μόνο οι hackers μπορούν να τα ανιχνεύσουν μέσω ειδικών προγραμμάτων. Το πρόβλημα που δημιουργείται είναι ότι ο χρήστης δεν μπορεί να αντιληφθεί τι γίνεται και οι απάτες αυτές δεν συμβαίνουν μόνο σε καθημερινούς χρήστες αλλά και σε οργανισμούς, σύμφωνα με την Global Corporate IT Security Risks. Στην συγκεκριμένη έρευνα συμμετείχαν πολλά στελέχη επιχειρήσεων και οργανισμών από όλη την Ελλάδα και διαπιστώθηκαν ότι το 69% των Ελλήνων στελεχών δέχτηκαν επιθέσεις από ιούς και το 46% των επιχειρήσεων ηλεκτρονικού "ψαρέματος".

Ο στόχος του phising, είναι να αποσπάσει προσωπικά στοιχεία του χρήστη ή και πληροφορίες μέσα από εφαρμογές συμπλήρωσης πλατφόρμας. Πληροφορίες όπως το ονοματεπώνυμό του, τηλέφωνο, διεύθυνση, email κλπ (Gruber, T. R. 1993)

Μια πλήρης επίθεση phishing περιλαμβάνει τρεις ρόλους. Πρώτον, οι αποστολείς στέλνουν ένα μεγάλο αριθμό ψευδών μηνυμάτων ηλεκτρονικού ταχυδρομείου (συνήθως μέσω των botnet), οι οποίοι κατευθύνουν τους χρήστες σε ψευδείς ιστοτόπους. Δεύτερον, οι συλλέκτες δημιουργούν ψευδείς ιστοτόπους, οι οποίοι προτρέπουν στους χρήστες να παρέχουν εμπιστευτικές πληροφορίες. Τέλος, οι cashers χρησιμοποιούν τις εμπιστευτικές πληροφορίες για την επίτευξη του στόχου τους. (Lance James, 2005)

Οι hackers έχουν συνήθως οικονομικούς σκοπούς, για αυτό το λόγο στοχεύουν στις περισσότερες περιπτώσεις σε τραπεζικούς λογαριασμούς, ή λογαριασμούς στους οποίους οι χρήστες εμπιστεύονται τα προσωπικά τους δεδομένα για να κάνουν συναλλαγές. Σε άλλες περιπτώσεις, το phishing γίνεται εργαλείο για spamming, προώθηση κακόβουλου λογισμικού ή διαφημιστικά (Singh, D., et al., 2011)

Εικόνα 1.

1. Γενική επισκόπηση

Οι επιθέσεις από ιούς και phising πραγματοποιούνται είτε με την αποστολή μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου για τη συμπλήρωση προσωπικών δεδομένων σε μια τράπεζα, είτε με την αναφορά ότι ο χρήστης έχει κέρδίσει κάποιο δώρο και θα πρέπει να συμπληρώσει τα προσωπικά του στοιχεία για να το παραλάβει. Ένας τρόπος απάτης είναι μέσω της εφαρμογής ebay. Ο χρήστης μπορεί να παραπλανηθεί για κάποια προσφορά και οι hackers να προσπαθήσουν να μάθουν τα προσωπικά του στοιχεία. Στις μέρες μας έχουν διαπιστωθεί πολλά κρούσματα και δυστυχώς αυξάνονται αντι να λιγοστέψουν. Οι εισβολείς συνήθως χρησιμοποιούν διάφορες τακτικές για να εξαπατήσουν το χρήστη και να εισάγει τα προσωπικά του στοιχεία. Η ασφάλεια, ήταν ένα μεγάλο θέμα στον τομέα της τεχνολογίας των ηλεκτρονικών υπολογιστών από τις αρχές της δεκαετίας του '50. Αρκετές μέθοδοι κρυπτογράφησης και ελέγχου πρόσβασης χρησιμοποιηθήκαν για την προστασία των κωδικών κλπ., όπου αργότερα αναπτύχτηκαν στη δεκαετία του 1960.

Την Δεκαετία του '80 μια τεχνική ηλεκτρονικού "ψαρέματος" περιγράφηκε λεπτομερώς σε ένα έντυπο και παρουσίαση που υποβλήθηκε στο διεθνές συνέδριο χρηστών της Hewlett Packard του 1987.

Το 1996, ο όρος «phishing» χρησιμοποιήθηκε για πρώτη φορά όταν κάποιοι hackers έκλεψαν την America Online, έχοντας πρόσβαση στους κωδικούς των χρηστών της. Επιπλέον, το 1997, η πρώτη δημοσίευση των μέσων ενημέρωσης προειδοποιεί τους πελάτες για μια νέα απειλή που λέγεται phishing, και η AOL μείωσε την άμεση πρόσβασή της για τους Ρώσους χρήστες εξαιτίας του αυξημένου επιπέδου απάτης.

Το 2001 το e-gold έγινε το πρώτο θύμα μεταξύ των χρηματοπιστωτικών ιδρυμάτων. (Malisa, L., et al. 2015) Οι hackers άρχισαν να χρησιμοποιούν μηνύματα spam για να διαδώσουν το δίκτυό τους.

Η πρώτη γνωστή επίθεση ηλεκτρονικού "ψαρέματος" κατά μιας τράπεζας λιανικού εμπορίου αναφέρθηκε από τον The Banker τον Σεπτέμβριο του 2003.

Εκτιμάται ότι από το Μάιο του 2004 έως το Μάιο του 2005, περίπου 1,2 εκατομμύρια χρήστες υπολογιστών στις Ηνωμένες Πολιτείες υπέστησαν ζημίες που προκλήθηκαν από το ηλεκτρονικό «ψάρεμα», συνολικού ύψους περίπου 929 εκατομμυρίων δολαρίων ΗΠΑ. Οι επιχειρήσεις των Ηνωμένων Πολιτειών χάνουν περίπου 2 δισεκατομμύρια δολάρια ΗΠΑ ετησίως καθώς οι πελάτες τους γίνονται θύματα.

Το 2005, η Τράπεζα της Αμερικής έχασε 1.2 εκατομμύρια ονόματα χρηστών και τους αριθμούς κοινωνικής ασφάλισης SSN "Social security number" των πελατών τους. Στο Ηνωμένο Βασίλειο, οι απώλειες από την ηλεκτρονική τραπεζική απάτη, κυρίως από το ηλεκτρονικό «ψάρεμα», σχεδόν διπλασιάστηκαν σε 23,2 εκατομμύρια λύρες το 2005 από 12,2 εκατομμύρια λύρες το 2004, ενώ ένας στους 20 χρηστές ηλεκτρονικών υπολογιστών ισχυρίστηκε ότι έχει πέσει θύμα phishing.

Περίπου το ήμισυ των κλοπών phishing το 2006 πραγματοποιήθηκαν από ομάδες που λειτουργούν μέσω του ρωσικού επιχειρηματικού δικτύου που εδρεύει στην Αγία Πετρούπολη.

Οι τράπεζες διαφώνησαν με τους πελάτες για τις απώλειες phishing. Η στάση που υιοθέτησε ο βρετανικός τραπεζικός οργανισμός APACS είναι ότι "οι πελάτες πρέπει επίσης να λαμβάνουν προφυλάξεις, έτσι ώστε να μην είναι ευάλωτοι στον εγκληματία". Ομοίως, όταν η πρώτη εμφάνιση επιθέσεων phishing έπληξε τον τραπεζικό τομέα της Ιρλανδικής Δημοκρατίας το Σεπτέμβριο του 2006, η Τράπεζα της Ιρλανδίας αρνήθηκε αρχικά να καλύψει τις ζημίες που υπέστησαν οι πελάτες της, παρόλο που οι ζημίες ύψους 113.000 ευρώ είχαν καλυφθεί.

Οι Phishers απευθύνθηκαν στους πελάτες των τραπεζών και στις υπηρεσίες πληρωμών μέσω διαδικτύου. Τα μηνύματα ηλεκτρονικού ταχυδρομείου, υποτιθέμενα από την υπηρεσία εσωτερικών εσόδων, χρησιμοποιήθηκαν για την συλλογή ευαίσθητων δεδομένων από τους φορολογούμενους των ΗΠΑ. Ενώ τα πρώτα τέτοια παραδείγματα στάλθηκαν αδιάκριτα με την προσδοκία ότι μερικά θα γίνουν δεκτά από μια συγκεκριμένη τράπεζα ή υπηρεσία, πρόσφατες έρευνες έχουν δείξει ότι οι phishers μπορούν καταρχήν να καθορίσουν ποιες τράπεζες χρησιμοποιούν τα δυνητικά θύματα και να στοχεύσουν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου ανάλογα.

Οι ιστότοποι κοινωνικής δικτύωσης είναι ο πρωταρχικός στόχος του phishing, καθώς τα προσωπικά στοιχεία σε τέτοιους ιστοτόπους μπορούν να χρησιμοποιηθούν στην κλοπή ταυτότητας. Στα τέλη του 2006, ένας ιός τύπου worm ανέλαβε σελίδες στο MySpace και άλλαξε συνδέσμους σε απευθείας σύνδεση σε ιστοσελίδες που σχεδιάστηκαν για να κλέψουν στοιχεία σύνδεσης. Τα πειράματα δείχνουν ποσοστό επιτυχίας πάνω από 70% για επιθέσεις ηλεκτρονικού "ψαρέματος" στα κοινωνικά δίκτυα.

3,6 εκατομμύρια χρήστες έχασαν 3,2 δισεκατομμύρια δολάρια το δωδεκάμηνο που έληξε τον Αύγουστο του 2007. Η Microsoft υποστηρίζει ότι αυτές οι εκτιμήσεις είναι υπερβολικές και θέτουν την ετήσια απώλεια phishing στις ΗΠΑ στα 60 εκατομμύρια δολάρια.

Οι εισβολείς που μπήκαν στη βάση δεδομένων της TD Ameritrade και πήραν 6,3 εκατομμύρια διευθύνσεις ηλεκτρονικού ταχυδρομείου (αν και δεν μπόρεσαν να λάβουν αριθμούς κοινωνικής ασφάλισης, αριθμούς λογαριασμών, ονόματα, διευθύνσεις, ημερομηνίες γέννησης, αριθμούς τηλεφώνου και εμπορική δραστηριότητα) , έτσι ξεκίνησαν μια επίθεσης δόλιου phishing.

Το 2008 ο ιστότοπος κοινής χρήσης αρχείων RapidShare έγινε στόχος από το ηλεκτρονικό «ψάρεμα» για την απόκτηση ενός λογαριασμού premium, ο οποίος αφαιρεί τα ανώτατα όρια ταχύτητας στα αρχεία λήψεων, την αυτόματη κατάργηση των μεταφορτώσεων, την αναμονή των λήψεων και τους χρόνους μεταξύ των μεταφορτώσεων.

Τον Ιανουάριο του 2009, μια επίθεση ηλεκτρονικού "ψαρέματος" (phishing) οδήγησε σε μη εξουσιοδοτημένες μεταφορές χρημάτων ύψους 1,9 εκατομμυρίων δολαρίων στις ΗΠΑ μέσω των λογαριασμών ηλεκτρονικής τραπεζικής της Experi-Metal.

Το 3ο τρίμηνο του 2009, η ομάδα εργασίας για την καταπολέμηση του ηλεκτρονικού "ψαρέματος" ανέφερε ότι έλαβε 115.370 αναφορές για ηλεκτρονικό «ψάρεμα» από καταναλωτές. Οι ΗΠΑ και η Κίνα φιλοξενούν περισσότερα από το 25% των σελίδων phishing.

Τον Μάρτιο του 2011, το προσωπικό της RSA έπεσε θύμα phishing, οδηγώντας στα βασικά κλειδιά για όλες τις μάρκες ασφάλειας RSA SecureID που κλέφθηκαν και στη συνέχεια χρησιμοποιήθηκαν για να διαρρήξουν τους προμηθευτές των αμυντικών υπηρεσιών των ΗΠΑ.

Η κινεζική εκστρατεία phishing στόχευσε τους λογαριασμούς Gmail των αξιωματούχων των κυβερνήσεων και των στρατιωτικών δυνάμεων των Ηνωμένων Πολιτειών και της Νότιας Κορέας, καθώς και κινέζων πολιτικών ακτιβιστών. Η κινεζική κυβέρνηση αρνήθηκε τις κατηγορίες για συμμετοχή σε επιθέσεις στον κυβερνοχώρο από τα σύνορά της, αλλά υπάρχουν στοιχεία ότι ο κινεζικός στρατός βοήθησε στην κωδικοποίηση του λογισμικού των επιθέσεων.

Τον Αύγουστο του 2013, η διαφημιστική υπηρεσία Outbrain υπέστη επίθεση spearphishing και η SEA τοποθέτησε ανακατευθύνσεις στις ιστοσελίδες του The Washington Post, Time και CNN.

Τον Οκτώβριο του 2013, μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονταν από την American Express αποστέλλονταν σε άγνωστο αριθμό αποδεκτών. Μια απλή αλλαγή DNS θα μπορούσε να γίνει για να αποτρέψει αυτό το πλαστογραφημένο ηλεκτρονικό ταχυδρομείο,

αλλά η American Express δεν κατάφερε να την κάνει.

Μέχρι το Δεκέμβριο του 2013, το Cryptolocker ransomware μόλυνε 250.000 προσωπικούς υπολογιστές, στοχεύοντας πρώτα τις επιχειρήσεις χρησιμοποιώντας ένα συνημμένο αρχείο που ισχυρίστηκε ότι είναι ένα παράπονο πελάτη και αργότερα στόχευσε το ευρύ κοινό χρησιμοποιώντας έναν σύνδεσμο σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου σχετικά με ένα πρόβλημα εκκαθάρισης μιας επιταγής. Το ransomware κλείδωσε αρχεία στον υπολογιστή και ζήτησε από τον ιδιοκτήτη να κάνει μια πληρωμή σε αντάλλαγμα για το κλειδί για να τα ξεκλειδώσει και να αποκρυπτογραφήσει τα αρχεία. Σύμφωνα με την Dell SecureWorks, το 0,4% ή περισσότερο των μολυσμένων πιθανώς συμφώνησε να παραχωρήσει τα λύτρα.

Τον Ιανουάριο του 2014, το Seculert Research Lab εντόπισε μια νέα στοχοθετημένη επίθεση που χρησιμοποίησε το Xtreme RAT. Αυτή η επίθεση χρησιμοποίησε ηλεκτρονικά μηνύματα "phishing" για να στοχεύσει ισραηλινούς οργανισμούς και να αναπτύξει ένα κομμάτι προηγμένου κακόβουλου λογισμικού.

Σύμφωνα με την έκθεση της Microsoft Safer Security Index το 2014, οι ζημίες που προκλήθηκαν από το ηλεκτρονικό «ψάρεμα» ήταν περίπου 5 δισεκατομμύρια δολάρια.

Η Google αναφέρει ότι μεταξύ των ετών 2014 και 2015, τον αριθμός των κακόβουλων ιστοσελίδων που αυξήθηκε από περίπου 24.864 σε 33.571.

Εικόνα 2.

Ο Charles H. Eccleston δήλωσε ένοχος για μια προσπάθεια μη εξουσιοδοτημένης πρόσβασης και σκόπιμης βλάβης σε έναν προστατευμένο υπολογιστή στην απόπειρα Cyber Attack Spear-Phishing στις 15 Ιανουαρίου 2015, όταν προσπάθησε να μολύνει υπολογιστές 80 υπάλληλους του υπουργείου ενέργειας.

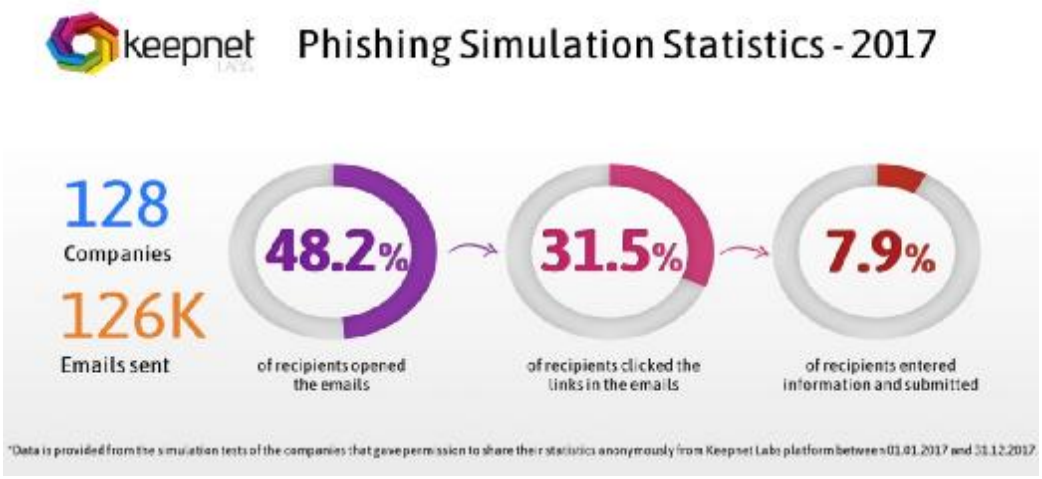
Έως το 2016, οι αμερικανικές επιχειρήσεις υπέστησαν μισό δισεκατομμύριο δολάρια σε απώλειες από επιθέσεις phishing με μέσο κόστος στα 1,6 εκατομμύρια δολάρια ετησίως. Αυτοί οι αριθμοί δηλώνουν τις ανησυχητικές αποδείξεις ότι μόνο με ένα κλικ μπορούν να δημιουργηθούν σημαντικές οικονομικές επιπτώσεις και κακή φήμη στο εμπορικό σήμα μιας εταιρίας. Οι μελέτες δείχνουν, πως το 30% των μηνυμάτων του ηλεκτρονικού "ψαρέματος" κατατάσσονται σταθερά ως κορυφαίος φορέας απάτης.

Το Φεβρουάριο, η αυστριακή εταιρεία αεροναυπηγικής FACC AG υπέστη εξαπάτηση ύψους 42 εκατομμυρίων ευρώ (47 εκατομμύρια δολάρια) μέσω επίθεσης BEC και στη συνέχεια κατέλυσε τόσο τον CFO όσο και τον διευθύνοντα σύμβουλο.

Το 2017, το 76% των οργανώσεων αντιμετώπισαν επιθέσεις phishing. Σχεδόν οι μισοί από τους επαγγελματίες της ασφάλειας πληροφοριών που συμμετείχαν στην έρευνα ανέφεραν ότι το ποσοστό επιθέσεων αυξήθηκε από το 2016.

Σύμφωνα με έρευνα του Keepnet Labs, το 2017 το 48,2% των μηνυμάτων ηλεκτρονικού "ψαρέματος" ανοίχτηκαν από τους παραλήπτες. Το 31,5% συνέχισε να κάνει κλικ στο κακόβουλο συνημμένο αρχείο ή σύνδεσμο και το 7,9% έδωσε τις πληροφορίες και έτσι επέτρεψε την επίθεση να επιτύχει.

Εικόνα 3.



Το Μάιο του 2018, η ιδιωτική εταιρεία Block.one που ανέπτυξε την πλατφόρμα EOS.IO δέχθηκε επίθεση από hacker. Οι hackers επιτέθηκαν στο σύστημα υποστήριξης ηλεκτρονικού ταχυδρομείου Block.One που χρησιμοποιήθηκε και απέστειλε μηνύματα ηλεκτρονικού "ψαρέματος" με βάση τις επαφές ηλεκτρονικού ταχυδρομείου. Το ηλεκτρονικό μήνυμα "ψαρέματος" περιελάμβανε μια υπερ-σύνδεση και κατευθύνει τους χρήστες σε μια σελίδα που υπέκλεψε τα κλειδιά τους.

Εικόνα 4.

Total number of unique phishing reports (campaigns) received, according to APWG[74]

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244	173063
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787	268126
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683	327814
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187	335965
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897	412392
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020	313517
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979	284445
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195	320081
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489	491399
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765	704178
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421	194499	105233	80548	1413978
2016	99384	229315	229265	121028	96490	98006	93160	66166	69925	51153	64324	95555	1313771
2017	96148	100932	121860	87453	93285	92657	99024	99172	98012	61322	86547	85744	1122156
2018	89250	89010	84444	91054	82547	90882	93078	89323	88156				

"APWG Phishing Attack Trends Reports". Retrieved October 20, 2018.

Στο παραπάνω σχήμα καταγράφονται τα σύνολα των αναφορών για επιθέσεις phishing για κάθε μήνα από το έτος 2005 έως το 2018 καθώς και τα σύνολά τους για κάθε χρονιά.

Μία επίθεση phishing στηρίζεται σε τρεις βασικούς παράγοντες: την έλλειψη γνώσεων του θύματος, την έλλειψη προσοχής του θύματος και την εικονική εξαπάτηση. Ο μέσος άνθρωπος ξέρει να χειρίζεται τις βασικές λειτουργίες του υπολογιστή και του διαδικτύου χωρίς να γνωρίζει την διαδικασία με την οποία αυτό λειτουργεί. Έτσι δεν μπορεί να αναγνωρίσει τα ίχνη του phishing, όπως είναι μια παραλλαγμένη διεύθυνση email, ή το διαφορετικό URL. Ταυτόχρονα, λόγω της άγνοιας του κινδύνου, αμελεί τη χρήση προγραμμάτων anti-phishing. Ακόμα και σε περιπτώσεις που ο χρήστης έχει τις κατάλληλες γνώσεις για να ανιχνεύσει τα κακόβουλα στοιχεία, πολλές φορές δεν θα προσέξει τα σημάδια, αφού μπορεί να είναι αφηρημένος ή απασχολημένος με κάτι άλλο. (Garera, S. 2007)

Σε μη αξιόπιστες ιστοσελίδες δημοπρασιών ενδέχεται να γίνονται πλειστηριασμοί ανύπαρκτων αντικειμένων. Τα θύματα πληρώνουν προκαταβολές και διαδικαστικά έξοδα, ωστόσο δεν παραλαμβάνουν ποτέ το αντικείμενο για το οποίο πλειοδότησαν. Δημιουργώντας ψεύτικες αγγελίες θέσεων εργασίας που μοιάζουν με αληθινές, όπου συχνά δημοσιεύοντάς τις σε νόμιμες ιστοσελίδες εύρεσης εργασίας, οι hackers ελπίζουν να παραπλανήσουν τους πρόθυμους και ανυποψίαστους χρήστες που αναζητούν εργασία και να τους πείσουν να στείλουν τα προσωπικά τους στοιχεία. Αυτές οι ψεύτικες αγγελίες εύρεσης εργασίας γίνονται όλο και πιο κομψές και συχνά χρησιμοποιούν πειστικά εταιρικά λογότυπα και φρασεολογία.

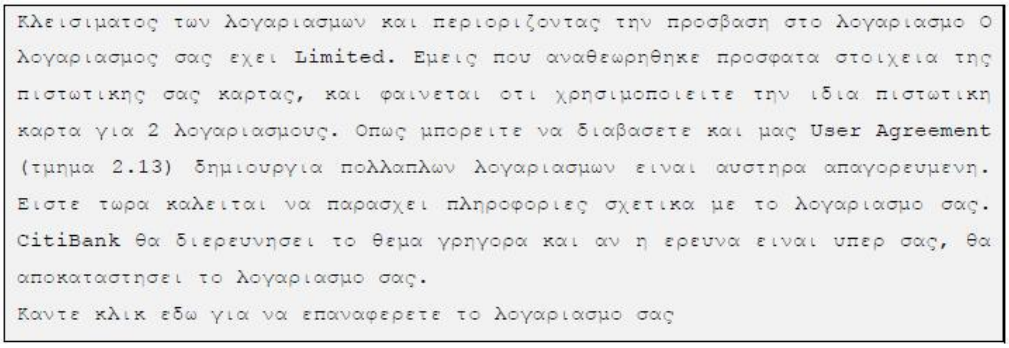
Εκτός από τη σάρωση προσωπικών ιστοσελίδων και τη δημοσίευση ανακοινώσεων σε δημόσιες ιστοσελίδες, οι hackers συχνά εμφανίζονται ως γραφεία εργασίας που διαθέτουν ευκαιρίες απασχόλησης και στέλνουν ανεπιθύμητη αλληλογραφία (ή spam) σε πιθανούς υποψηφίους. (Gaddis S.,2011)

Μια άλλη γνωστή τακτική των hackers είναι η πλαστογράφηση πολλών web sites. Ορισμένες απάτες ηλεκτρονικού "ψαρέματος" χρησιμοποιούν εντολές JavaScript για να αλλάξουν τη γραμμή διευθύνσεων ενός ιστοτόπου. Αυτό γίνεται είτε τοποθετώντας μια εικόνα νόμιμης διεύθυνσης URL στη γραμμή διευθύνσεων είτε κλείνοντας την αρχική γραμμή και ανοίγοντας μια νέα με τη νόμιμη διεύθυνση URL.

Ένας εισβολέας μπορεί επίσης να χρησιμοποιήσει ελαττώματα αξιόπιστων ιστοτόπων κατά του θύματος. Αυτοί οι τύποι επιθέσεων (γνωστοί ως δέσμες ενεργειών μεταξύ ιστοτόπων) είναι ιδιαίτερα προβληματικοί, διότι κατευθύνουν τον χρήστη να συνδεθεί στην ιστοσελίδα της τράπεζάς του ή της υπηρεσίας του, όπου τα στοιχεία από τη διεύθυνση ιστού έως τα πιστοποιητικά ασφαλείας, εμφανίζονται σωστά. Στην πραγματικότητα, ο σύνδεσμος προς τον ιστότοπο δημιουργείται για να πραγματοποιήσει την επίθεση, καθιστώντας πολύ δύσκολο να εντοπιστεί χωρίς ειδικές γνώσεις.

Στην Ελλάδα, οι επιθέσεις αυτού του είδους υπάρχουν αλλά όχι σε τόσο μεγάλο βαθμό λόγω της δυσκολίας που παρουσιάζει η ελληνική γλώσσα. Ωστόσο όμως, έχουν συμβεί τέτοιου είδους επιθέσεις. Ένα από τα παραδείγματα επιθέσεων phishing είναι ένα μήνυμα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι στάλθηκε από την City bank στους πελάτες της και όπως φαίνεται στην παρακάτω εικόνα εμπεριείχε το εξής μήνυμα:

Εικόνα 5.


Κλεισιματος των λογαριασμων και περιοριζοντας την προσβαση στο λογαριασμο Ο λογαριασμος σας εχει **Limited.** Εμεις που αναθεωρηθηκε προσφατα στοιχεια της πιστωτικης σας καρτας, και φαινεται οτι χρησιμοποιειτε την ιδια πιστωτικη καρτα για 2 λογαριασμους. Οπως μπορειτε να διαβασετε και μας **User Agreement** (τμημα 2.13) δημιουργια πολλαπλων λογαριασμων ειναι αυστηρα απαγορευμενη. Ειστε τωρα καλειται να παρασχει πληροφοριες σχετικα με το λογαριασμο σας. **CitiBank** θα διερευνησει το θεμα γρηγορα και αν η ερευνα ειναι υπερ σας, θα αποκαταστησει το λογαριασμο σας.
Καντε κλικ εδω για να επαναφερετε το λογαριασμο σας

Όπως μπορεί να παρατηρηθεί το συγκεκριμένο μήνυμα δεν είναι σωστά συνταγμένο πράγμα που σημαίνει ότι οι εισβολείς πιθανόν το μετέφρασαν στον αυτόματο μεταφραστή. Επίσης, αυτό το μήνυμα στάλθηκε και σε χρήστες οι οποίοι δεν ήταν πελάτες της συγκεκριμένης τράπεζας με σκοπό να εξαπατήσουν περισσότερους χρήστες.

Στην επόμενη εικόνα παρατηρείται άλλο ένα phising mail που έλαβε ένας χρήστης και το οποίο επίσης δεν είναι σωστά συνταγμένο και εμπεριέχει και ορθογραφικά λάθη.

Εικόνα 6.

Αγαπητε πελατη
Μπορειτε εχουν βραβευθει με κουπονι για 100 eur.
Δωροεπιταγη code: 11245325932
για να συλλεξουμε παρακαλω συνδεθειτε και να εισαγετε το κωδικο κουπονιου παραπανω.
Παρακαλω επιτρεψτε 3-5 μερες για μεταποιηση.
Copyright © winbank 2008

Τέλος, άλλο ένα παράδειγμα επίθεσης phishing είναι ένα ηλεκτρονικό μήνυμα που στάλθηκε από την υποτιθέμενη Alpha bank και εμπεριείχε το εξής:

Εικόνα 7.

"Αγαπητέ πελάτη της Ιντερνέτ-Τράπεζας!
Επειδή η κατάσταση με Online - Τράπεζες στη χώρα μας είναι σήμερα πολύ δύσκολη, η κυβέρνηση της Ελλάδας παρακάλησέ μας να κάνουμε τον έλεγχο για όλους τους Online - λογαριασμούς της δηκής ! μας τράπεζας να μάθουμε αν υπάρχουν "λογαριασμοί μιας μέρας", τους οποίους χρησημοποιούν οι εγκληματίες για να αποπλύνονται τα κλεμμένα λεφτά. Δια ταυτα σας παρακαλούμε πολύ &eigm! a;σβαρά να συμ& pi;λπρώσετε το ερωτηματολόγιο της επιβεβαιώσεις λόγαριασμού στη επίσημη μας Ιντερμετ-σελήδα.
Οι λογαριασμοί, που δε θα επιβεβαιωθούν ως της 27.11.05, θα παγώνονται για ακαθόριστο καιρό πριν γίνει φανερό πως ακριβώς έχουν δημιουργηθεί και εκμετολευθεί. Ο έλεγχος αυτος είν&alph! a;ι επίκαιρος οχι μόνο για ιδιωτικούς μας πελάτες, αλλα για όλους σας.
ΝΑ ΣΥΜΠΛΗΡΩΣΩ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ
Σας ζητούμε συγνώμη για τις ενοχλήσεις που προκύπτει απο τη διαταγή της παρούσες εκδήλωσης και ελπίζουμε για την κατανόηση και την βοήθειά σας.
Με σεβασμό,

Υπηρεσία ασφάλειας
Τράπεζα Alpha Bank"

Σύμφωνα με τις παραπάνω εικόνες παρατηρούμε ότι ο χρήστης έχει να συμπληρώσει ένα ερωτηματολόγιο. Ωστόσο παρατηρείται ότι αυτός που το δημιούργησε δεν πρόσεξε τα ορθογραφικά λάθη και την ασυνταξία του κειμένου. Επομένως οι χρήστες όταν διαβάζουν οποιοδήποτε μήνυμα τους σταλθεί πρέπει να προσέχουν την κάθε λεπτομέρεια του κειμένου, και να είναι συγκεντρωμένοι και καχύποπτοι πριν απαντήσουν.

2. Κατηγορίες phishing

Το ηλεκτρονικό «ψάρεμα» έχει εξαπλωθεί πέρα από τα μηνύματα ηλεκτρονικού ταχυδρομείου και συμπεριλαμβάνει VOIP, SMS, instant messaging, κοινωνική δικτύωση ιστότοπων, ακόμη και παιχνίδια. Διάφορες τεχνικές αναπτύσσονται για επιθέσεις phishing διαμορφώνοντας τις λιγότερο ύποπτες. Το spoofing μιας ηλεκτρονικής διεύθυνσης χρησιμοποιείται για να δημιουργεί ψευδείς μηνύματα ηλεκτρονικού ταχυδρομείου για την πλαστογραφία, ώστε να φαίνεται πως έχει σταλθεί από τους νόμιμους αποστολείς, με αποτέλεσμα οι παραλήπτες να είναι πιθανότερο να πιστεύουν στο μήνυμα και να λαμβάνουν μέτρα σύμφωνα με τις οδηγίες του. Το web spoofing κάνει τις πλαστές ιστοσελίδες να μοιάζουν με νόμιμες, έτσι ώστε οι χρήστες να εισάγουν μυστικές πληροφορίες σε αυτό, όπως και το Pharming που προσελκύει το ενδιαφέρον των πλαστών ιστοτόπων. Επίσης κακόβουλα προγράμματα εγκαθίστανται σε υπολογιστές των θυμάτων για να συλλέγουν πληροφορίες απευθείας ή να βοηθούν άλλες τεχνικές π.χ. PDF έγγραφα, τα οποία υποστηρίζουν scripting και φόρμες συμπλήρωσης που χρησιμοποιούνται επίσης για την συλλογή πληροφοριών.

2.1. Τεχνικές phishing

- **Email Spoofing**

Το Email spoofing, είναι μια κοινή τεχνική phishing στην οποία αποστέλλεται ένα ψευδές μήνυμα ηλεκτρονικού ταχυδρομείου, που ισχυρίζεται ότι προέρχεται από μία έγκυρη πηγή ενώ πραγματικά αποστέλλεται από μία άλλη με αλλοιωμένη τη διεύθυνση αποστολέα και άλλα τμήματα της κεφαλίδας του ηλεκτρονικού ταχυδρομείου, προκειμένου να εξαπατηθούν οι παραλήπτες. (Markus Jakobsson & Steven Myers, 2007)

Τα spoofed μηνύματα ηλεκτρονικού ταχυδρομείου εμφανίζονται συνήθως από έναν ιστότοπο ή ένα οικονομικό ίδρυμα που ο παραλήπτης μπορεί να έχει συναλλαγές, έτσι ώστε ένας ανυποψίαστος παραλήπτης πιθανότατα να λάβει δράση σύμφωνα με τις οδηγίες από τα περιεχόμενα του μηνύματος, όπως:

I. απαντήστε στο email με τον αριθμό της πιστωτικής σας κάρτας
II. κάντε κλικ στον σύνδεσμο με την ετικέτα "view my statement" και εισαγάγετε τον κωδικό πρόσβασης όταν η ιστοσελίδα σας το ζητάει

III. ανοίξτε μια προσαρτημένη φόρμα PDF και εισαγάγετε πληροφορίες στη φόρμα "Αποστολή φαινομένου ηλεκτρονικού ταχυδρομείου"

- **Clone Phishing**

Σε αυτόν τον τύπο phishing δημιουργείται ένα κλωνοποιημένο μήνυμα ηλεκτρονικού ταχυδρομείου. Αυτό γίνεται παίρνοντας πληροφορίες, όπως το περιεχόμενο και οι παραλήπτες, από ένα νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου που είχε παραδοθεί προηγουμένως. Τότε στέλνει το ίδιο μήνυμα ηλεκτρονικού ταχυδρομείου με συνδέσμους που έχουν αντικατασταθεί από κακόβουλα links. Επίσης πλαστογραφεί τη διεύθυνση του αποστολέα έτσι ώστε το μήνυμα ηλεκτρονικού ταχυδρομείου να φαίνεται να είναι από τον αρχικό αποστολέα. Τέλος το μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να ισχυριστεί ότι είναι μια νέα αποστολή του πρωτοτύπου ή μια ενημερωμένη έκδοση ως στρατηγική παγίδευσης.

- **Spear Phishing**

Το spear phishing στοχεύει σε μια συγκεκριμένη ομάδα. Έτσι, αντί να εξαπολύσουν χιλιάδες μηνύματα ηλεκτρονικού ταχυδρομείου τυχαία, οι hackers στοχεύουν σε επιλεγμένες ομάδες ανθρώπων με κάτι κοινό, όπως άτομα που εργάζονται στον ίδιο οργανισμό.

Το spear phishing χρησιμοποιείται επίσης ενάντια σε στόχους υψηλού επιπέδου, σε ένα είδος επίθεσης που ονομάζεται “whaling” (φαλαινοθηρία).

Για παράδειγμα, το 2008, αρκετοί διευθύνοντες σύμβουλοι των Η.Π.Α. έλαβαν μια ψεύτικη κλήτευση μαζί με ένα συνημμένο μήνυμα που θα εγκαθιστούσε ένα κακόβουλο λογισμικό όταν προβαλλόταν. Ως θύματα των επιθέσεων spear phishing στα τέλη του 2010 και στις αρχές του 2011 περιλαμβάνονται το γραφείο του Αυστραλιανού πρωθυπουργού, η καναδική κυβέρνηση, η υπηρεσία αλληλογραφίας "Epsilon", το HB Gary Federal και το "Oak Ridge National Laboratory".

- **Κακόβουλα Links**

Οι περισσότερες μέθοδοι phishing χρησιμοποιούν κάποια μορφή τεχνικής εξαπάτησης που έχει σχεδιαστεί για να δημιουργούν έναν σύνδεσμο σε ένα email, όπου φαίνεται να ανήκουν στον πλαστογραφημένο οργανισμό. Οι τροποποιημένες διευθύνσεις URL ή η χρήση υποτομέων είναι κοινά κόλπα που χρησιμοποιούνται από phishers. Ένα άλλο κοινό κόλπο

είναι να κάνει το κείμενο που εμφανίζεται για ένα σύνδεσμο να υποδεικνύει έναν αξιόπιστο προορισμό, όταν ο σύνδεσμος πηγαίνει στην τοποθεσία του phisher. Πολλοί clients του ηλεκτρονικού ταχυδρομείου και προγράμματα περιήγησης ιστού θα εμφανίζουν τη διεύθυνση URL προορισμού μιας σύνδεσης στη γραμμή κατάστασης, όταν θα μετακινείται ο κέρσορας του ποντικιού πάνω από αυτήν. Αυτή η συμπεριφορά, μπορεί σε ορισμένες περιπτώσεις να παραμεριστεί από το phisher. Οι ισοδύναμες εφαρμογές για κινητά γενικά δεν έχουν αυτή τη λειτουργία προεπισκόπησης.

Τα διεθνοποιημένα ονόματα τομέα (IDN) μπορούν να αξιοποιηθούν μέσω αλλοίωσης ή ομογραφικών επιθέσεων, για τη δημιουργία διευθύνσεων ιστού οπτικά πανομοιότυπων με έναν νόμιμο ιστότοπο, οι οποίες οδηγούν σε κακόβουλη έκδοση. Οι Phishers έχουν επωφεληθεί από παρόμοιο κίνδυνο, χρησιμοποιώντας ανοικτούς ανακατευθυντές διευθύνσεων URL στις ιστοσελίδες αξιόπιστων οργανισμών για τη συγκάλυψη κακόβουλων διευθύνσεων URL με έναν αξιόπιστο τομέα. Ακόμη και τα ψηφιακά πιστοποιητικά δεν επιλύουν αυτό το πρόβλημα επειδή είναι πολύ πιθανό ένας phisher να αγοράσει ένα έγκυρο πιστοποιητικό και στη συνέχεια να αλλάξει περιεχόμενο για να παραβιάσει έναν γνήσιο ιστότοπο ή για να φιλοξενήσει τον ιστότοπο του phishing χωρίς SSL.

- **Phishing μέσω εγγράφων PDF**

Η μορφή φορητού εγγράφου της Adobe είναι η πιο δημοφιλής και αξιόπιστη μορφή περιγραφής εγγράφων. Αυτό καθιστά τα έγγραφα PDF πιο ευάλωτα σε απειλές ηλεκτρονικού "ψαρέματος", λόγω της φορητότητάς και διαλειτουργικότητας τους σε πολλαπλές πλατφόρμες. Εκτός από την ισχυρή μορφή εγγράφων, το PDF είναι μία ολοκληρωμένη γλώσσα προγραμματισμού που είναι αφιερωμένη στη δημιουργία και τη χειραγώγηση εγγράφων με δυνατά χαρακτηριστικά εκτέλεσης. Ορισμένες κρίσιμες λειτουργίες μιας γλώσσας PDF θα μπορούσαν να χρησιμοποιηθούν κατά λάθος από ένα εισβολέα ή έναν hacker για να σχεδιάσει ένα έγγραφο PDF προς το δικό του πλεονέκτημα και να εξαγάγει τις επιθυμητές πληροφορίες από το θύμα, δημιουργώντας έτσι μια νέα παγκόσμια απειλή. Αυτές οι δυνητικά επικίνδυνες λειτουργίες περιλαμβάνουν το OpenAction και το SubmitForm.

Αν και η Adobe έχει εφαρμόσει ορισμένους μηχανισμούς ασφαλείας στα Adobe Reader και Adobe Acrobat για να ειδοποιήσουν τον χρήστη σε περίπτωση (πιθανώς) κακόβουλων προσπαθειών, αυτά τα μέτρα συναγερμού είναι απλά πλαίσια μηνυμάτων, που ζητούν από τον χρήστη να επιτρέψει ή να αποκλείσει μια ενέργεια. Δυστυχώς, ένα τέτοιο μήνυμα παραμελείται συχνά από τους χρήστες και είναι δυνατόν να παρακάμψουν αυτούς τους

μηχανισμούς ασφαλείας τροποποιώντας τα αρχεία RdLang32.FRA και AcroRd32.dll με κακόβουλο λογισμικό. (Gundeep Singh Bindra, 2011)

- **Voice Phishing**

Αυτός ο τύπος ηλεκτρονικού "ψαρέματος" αναφέρεται σε μηνύματα που ισχυρίζονται ότι προέρχονται από μια τράπεζα ζητώντας από τους χρήστες να καλέσουν ένα τηλεφωνικό αριθμό σχετικά με προβλήματα στους τραπεζικούς τους λογαριασμούς. Ο παραδοσιακός τηλεφωνικός εξοπλισμός Voice over IP, έχει συγκεκριμένες γραμμές, με αποτέλεσμα να είναι πιο εύκολο να διαμορφωθεί από τον εισβολέα. Οπότε αποτελεί εύκολο στόχο για μια καλή επιλογή επίθεσης. Όταν ο αριθμός του τηλεφώνου που ανήκει στο hacker και παρέχεται από μια υπηρεσία VoIP καλείται, οι φωνητικές εντολές λένε στον καλούντα να εισάγει τους αριθμούς λογαριασμού και τον κωδικό PIN. Αυτό καλείται ID spoofing, το οποίο δεν απαγορεύεται από το νόμο και μπορεί να χρησιμοποιηθεί έτσι ώστε η κλήση να φαίνεται να προέρχεται από μια αξιόπιστη πηγή.

- **Pharming**

Το Pharming είναι ένας τύπος επίθεσης που αποσκοπεί στην ανακατεύθυνση του trace σε έναν ψεύτικο host του Διαδικτύου. Υπάρχουν διάφορες μέθοδοι για επιθέσεις pharming, μεταξύ των οποίων το "DNS cache poisoning" είναι η πιο κοινή. Υπάρχουν τεχνικές pharming σε μικρότερο πεδίο, όπως ο τοπικός υπολογιστής ή ένα οικιακό δίκτυο, που μπορεί να παραμείνει απαρατήρητο για μεγαλύτερο χρονικό διάστημα.

Το αρχείο Hosts είναι ένα κείμενο σε έναν τοπικό υπολογιστή, που περιέχει αντιστοιχίσεις μεταξύ κεντρικού υπολογιστή και IP. Αυτό βρίσκεται στο "/ etc / hosts σε συστήματα UNIX ή % WINDIR% \system32\drivers\etc\HOSTS" σε συστήματα Windows. Το TCP/IP stack διαβουλεύεται με αυτό πριν από την αναζήτηση του DNS. Αυτό το αρχείο θα μπορούσε να γραφτεί από κακόβουλο λογισμικό για pharming.

Σε περιοχές του κόσμου που το Διαδίκτυο είναι περιορισμένο, μερικοί άνθρωποι έχουν λύσεις που ισχυρίζονται ότι παρέχουν απεριόριστη πρόσβαση στο Διαδίκτυο. Αυτές οι λύσεις συνήθως παρέχονται ως λογισμικό VPN, διακομιστή μεσολάβησης ή υλικό router. Που θα μπορούσαν να πληρώνονται ή να είναι δωρεάν. Ένας ανέντιμος πάροχος θα μπορούσε να προσφέρει μια λύση με pharming, και οι χρήστες όταν αναζητούν πρόσβαση χωρίς λογοκρισία να καταλήξουν να επισκεφτούν πλαστές ιστοσελίδες χωρίς να το καταλάβουν.

- **Η δηλητηρίαση DNS και DNS cache**

Το σύστημα domain name (DNS) είναι ένα κρίσιμο κομμάτι της υποδομής του Internet. Σχεδιασμένο ως διανεμημένο σύστημα, το DNS δημοσιεύει μια ιεραρχική βάση δεδομένων με μια ιεραρχία ονομάτων διακομιστών. Για να βελτιωθεί η απόδοση, οι πελάτες επικοινωνούν με τοπικούς ανιχνευτές DNS που διατηρούνται από τοπικούς ISPs, από τους οποίους μπορούν να αποθηκευτούν οι εγγραφές από το cache των διακομιστών ονομάτων. Οι πελάτες, οι διαχωριστές και οι διακομιστές ονομάτων μιλούν μεταξύ τους μέσω της θύρας UDP 53. (Beichuan Zhang).

Το DNS είναι κρίσιμο για την ασφάλεια του Διαδικτύου. Τα SPF, DKIM και Sender ID, βασίζονται στο DNS. Αν το DNS έχει αλλοιωθεί με πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου, μπορεί να διαρρεύσουν πλαστές υπογραφές και αντίμετρα. Το διαδικτυακό spoofing μπορεί επίσης να πραγματοποιηθεί κάνοντας το DNS να απαντήσει με τη διεύθυνση του επιτιθέμενου διακομιστή.

Η δηλητηρίαση της προσωρινής μνήμης DNS επιχειρεί να τροφοδοτήσει την προσωρινή μνήμη των τοπικών ανιχνευτών DNS με εσφαλμένες εγγραφές. Αυτό είναι δυνατό επειδή το DNS τρέχει μέσω του πρωτοκόλλου UDP και είναι εύκολο να παραβιάσει τη διεύθυνση προέλευσης ενός UDP Πακέτου. Η κεφαλίδα πακέτου DNS περιέχει ένα αναγνωριστικό ερωτημάτων 16 bit, το οποίο είναι σχετικά σύντομο έτσι ώστε η επίθεση να είναι εφικτή. Η επέκταση ασφαλείας συστήματος ονόματος τομέα ή Domain Name System Security Extension (DNSSEC) (D. Eastlake 3rd, 1999) είναι μια επέκταση του DNS που παρέχει τρεις ξεχωριστές υπηρεσίες: διανομή κλειδιών, έλεγχο προέλευσης δεδομένων και αυθεντικοποίηση συναλλαγής και αιτήματος. Η δηλητηρίαση από τη μνήμη cache είναι δεν είναι πλέον δυνατή, επειδή ο εισβολέας δεν μπορεί να παράγει μια σωστή υπογραφή χωρίς να γνωρίζει το ιδιωτικό κλειδί του domain.

- **Κλοπή του domain**

Μια πιο προηγμένη επίθεση pharming είναι το domain hijacking. Στο domain hijacking, διαμορφώνετε η καταγραφή αντιπροσώπευσης του domain στον καταχωρητή, αλλάζοντας τον ελεγκτή του διακομιστή ονομάτων από έναν hacker, έτσι ώστε όλη η μεταφορά να μπορεί να ανακατευθυνθεί παγκοσμίως. Η Baidu, η μεγαλύτερη μηχανή αναζήτησης στην Κίνα, δέχθηκε επίθεση από τον ιρανικό κυβερνο - στρατό το 2010. (Owen Fletcher & Robert McMillan, 2010)

- Οι εισβολείς συζήτησαν την τεχνική υποστήριξης του Register.com, του καταχωρητή domain του baidu.com, για να αλλάξει τη διεύθυνση ηλεκτρονικού ταχυδρομείου. Η αλλαγή εγκρίθηκε χωρίς προσεκτική επαλήθευση.
- Ο κωδικός πρόσβασης του λογαριασμού επαναφέρθηκε με τη νέα διεύθυνση ηλεκτρονικού ταχυδρομείου.
- Το αρχείο εξουσιοδότησης άλλαξε σε ένα διακομιστή ονομάτων που ελεγχόταν από τους εισβολείς.
- Εκατομμύρια χρήστες ανακατευθύνθηκαν στο διακομιστή των εισβολέων.

Ένας hacker θα μπορούσε επίσης να χρησιμοποιήσει παρόμοιες τεχνικές για να αποκτήσει τον έλεγχο ενός domain. Η δηλητηρίαση της προσωρινής μνήμης DNS και η πειρατεία του domain είναι αποτελεσματική σε μεγάλο εύρος, επομένως θα πρέπει να εντοπίζεται και να διορθώνετε άμεσα.

Ø 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 hacker εκμεταλλεύεται τον 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. Επίσης, ένας εισβολέας πιθανόν να παρακολουθεί μία συζήτηση μέσω προγραμμάτων sniffing.

Ø Μέσα κοινωνικής δικτύωσης (chat, facebook)

Το chat στο διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται "δωμάτιο επικοινωνίας" (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Ένα παράδειγμα, είναι η χρήση των "chat rooms" για παραπλάνηση ανηλίκων. Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές επειδή βρίσκεται στον φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός internet cafe, μπορεί να μετατρέψει αυτό τον τρόπο της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του

διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο.

Συχνά απάτες phishing συμβαίνουν και στις μηχανές αναζήτησης, τις οποίες επισκέπτεται ο χρήστης συνήθως για κάποια οικονομική αγορά προϊόντων ή υπηρεσιών. Οι hackers εκμεταλλευόμενοι αυτής της αγοραστικής τάσης, 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 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.

Για παράδειγμα, ένα θύμα ίσως κάνει κλικ σε έναν κακόβουλο σύνδεσμο ηλεκτρονικού "ψαρέματος" που αρχίζει με το Facebook. Ένα αναδυόμενο παράθυρο από το Facebook θα ρωτήσει εάν το θύμα θα ήθελε να εξουσιοδοτήσει την εφαρμογή. Αν το θύμα επιλέξει να εγκρίνει την εφαρμογή, θα αποσταλεί ένα "κουπόνι" στον εισβολέα και θα μπορούσαν να εκτεθούν οι προσωπικές ευαίσθητες πληροφορίες του θύματος. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν τη διεύθυνση ηλεκτρονικού ταχυδρομείου, την ημερομηνία γέννησης, τις επαφές και το ιστορικό εργασίας. Σε περίπτωση που το "token" έχει μεγαλύτερο προνόμιο, ο εισβολέας θα μπορούσε να αποκτήσει πιο ευαίσθητες πληροφορίες, συμπεριλαμβανομένης της λίστας γραμματοκιβωτίων, online παρουσίας και φίλων. Ακόμα χειρότερα, ο εισβολέας ενδέχεται να ελέγχει και να χειρίζεται το λογαριασμό του χρήστη. Δεν επιλέγει να εξουσιοδοτήσει την εφαρμογή, αυτός θα εξακολουθεί να ανακατευθύνεται σε έναν ιστότοπο που ελέγχεται από τον εισβολέα, γεγονός που θα μπορούσε να υπονομεύσει περαιτέρω το θύμα.

- **Επιβεβαίωση στοιχείων λογαριασμού**

Ένας κοινός τύπος επίθεσης phishing είναι αυτός της επαλήθευσης στοιχείων λογαριασμού. Συνήθως πρόκειται για ένα email που μοιάζει να προέρχεται από έναν σημαντικό ιστότοπο ηλεκτρονικού εμπορείου ή κοινωνικού δικτύου (όπως το Facebook, το Amazon, η Walmart).

Ενημερώνει ότι υπάρχει κάποιο πρόβλημα σχετικά με το λογαριασμό του παραλήπτη το οποίο πρέπει να διορθωθεί. Το email έχει πολύ πειστικό εταιρικό λογότυπο και μάλιστα μερικές φορές εμπεριέχει τη διεύθυνση της εταιρείας και άλλες τέτοιες πληροφορίες για να εμφανίζεται ως νόμιμο. Επίσης περιλαμβάνει ύποπτους συνδέσμους, που ίσως οδηγήσουν τον χρήστη σε μια ψεύτικη ιστοσελίδα που μοιάζει πολύ με την γνήσια. Ο hacker μπορεί στη συνέχεια να χρησιμοποιήσει τα στοιχεία σύνδεσής του παραλήπτη για να αποκτήσει πρόσβαση στον ιστότοπο για να διαπράξει απάτη.

- **Διαδικτυακός εκφοβισμός**

Ο διαδικτυακός εκφοβισμός μπορεί να λάβει ποικίλες μορφές, για αυτόν τον λόγο αυτό έχει καταστεί μια δυσχερή έννοια μέχρι και σήμερα, στη νομική στοιχειοθέτησή του από τα περισσότερα κράτη. Έτσι ο διαδικτυακός εκφοβισμός μπορεί να εκφραστεί με πρακτικές όπως την απειλή, την παραβίαση προσωπικών δεδομένων, τη συκοφαντική δυσφήμηση, την εξύβριση, την παρενόχληση και άλλα. Τα αγαθά που προσβάλλονται είναι συνήθως τα άυλα αγαθά της προσωπικότητας του ατόμου, της καλής φήμης του, της τιμής και αξιοπρέπειάς του. Για παράδειγμα, αυτό συμβαίνει όταν ένα παιδί ή έφηβος δέχεται απειλές, παρενοχλείται, ταπεινώνεται ή γίνεται στόχος από κάποιο άλλο παιδί ή έφηβο, συνήθως με επαναλαμβανόμενο τρόπο, μέσω της χρήσης των νέων τεχνολογιών, του διαδικτύου ή των κινητών τηλεφώνων. Συγκεκριμένα, ο ηλεκτρονικός εκφοβισμός μπορεί να λάβει χώρα μέσω ηλεκτρονικού ταχυδρομείου, δωματίων συνομιλίας, σελίδων κοινωνικής δικτύωσης, μέσω άλλων ιστοσελίδων σχετικών με ηλεκτρονικά παιχνίδια ή τις υπηρεσιών άμεσης ανταλλαγής μηνυμάτων.

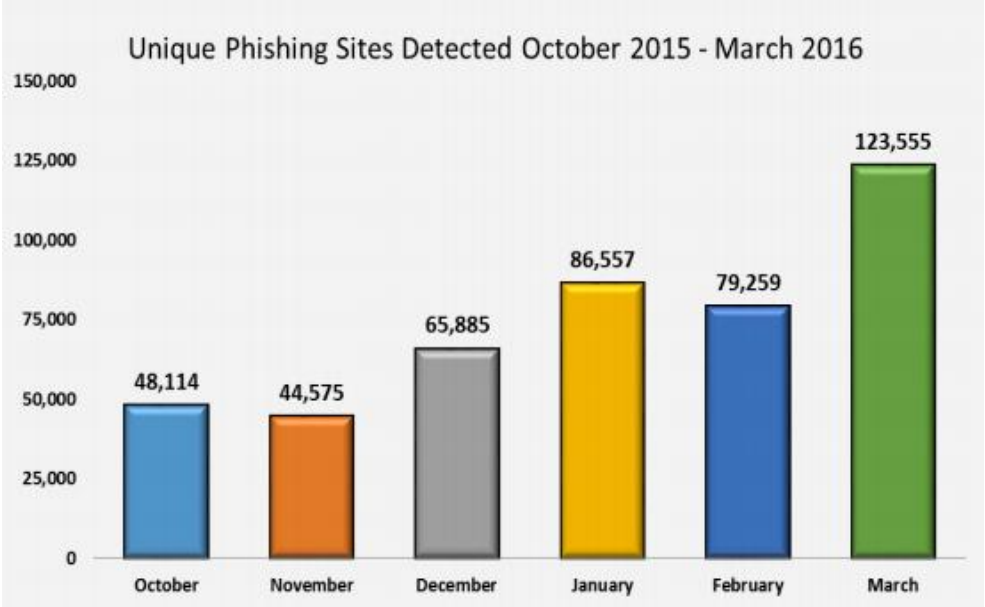
- **Ιστοσελίδες Ηλεκτρονικού "Ψαρέματος"**

Το ηλεκτρονικό εμπόριο αποτελείται κυρίως από τη διανομή, την αγορά, την πώληση, την εμπορία και την εξυπηρέτηση προϊόντων ή υπηρεσιών μέσω ηλεκτρονικών συστημάτων όπως το Διαδίκτυο και άλλα δίκτυα υπολογιστών. Η μεταβαλλόμενη αγορά αντιπροσωπεύει μια τεράστια ευκαιρία για τις επιχειρήσεις να βελτιώσουν τη συνάφεια τους και να επεκτείνουν την αγορά τους στο διαδίκτυο. Υπάρχουν αμέτρητοι διαφορετικοί ιστότοποι ηλεκτρονικού εμπορίου για τους χρήστες, όπου αυτό αυξάνει τις απαιτήσεις των λιανοπωλητών. Μπορεί να είναι αρκετά απλή η δημιουργία ενός ιστοτόπου ηλεκτρονικού εμπορίου, αλλά δεν είναι βέβαιη η επιτυχία του. Υπάρχουν πολλές πτυχές που πρέπει να

λαμβάνονται υπόψη κατά τη λειτουργία και την διαχείριση μιας ιστοσελίδας ηλεκτρονικού εμπορίου.

Ανησυχητική είναι η αύξηση του αριθμού των πλαστών ιστοσελίδων που καταγράφει η τελευταία έκθεση της αμερικανικής κοινοπραξίας Anti-Phishing Working Group (APWG), στην οποία συμμετέχουν τράπεζες, πιστωτικά ιδρύματα και εταιρείες ηλεκτρονικού εμπορίου, με στόχο την καταπολέμηση της ηλεκτρονικής απάτης. Ενώ είναι συνηθισμένο να υπάρχει άνοδος σε περιστατικά ηλεκτρονικού "ψαρέματος" (phishing) σε περιόδους διακοπών, οι ερευνητές της εργασιακής ομάδας ήταν έκπληκτοι για την συγκεκριμένη αύξηση. Η ομάδα παρακολούθησε περισσότερες επιθέσεις ηλεκτρονικού "ψαρέματος" στο πρώτο τετράμηνο του 2016 από ότι σε οποιοδήποτε άλλο διάστημα τριών μηνών από τότε που άρχισε να παρακολουθεί δεδομένα το 2004.

Εικόνα 8.



Οι Ηνωμένες Πολιτείες βρίσκονται στην κορυφή της λίστας με τις χώρες που φιλοξενούν ιστοσελίδες phishing.Οι phishers συχνά διαρρήχνουν ευάλωτα δίκτυα για την παροχή ιστοτόπων ηλεκτρονικού "ψαρέματος" και οι Ηνωμένες Πολιτείες φιλοξενούν μεγάλο αριθμό ιστοσελίδων.

Εικόνα 9.

January		February		March	
United States	75.10%	United States	81.90%	United States	75.62%
Belize	4.79%	United	2.20%	China	4.16%
Netherlands	3.59%	Germany	2.15%	Hong Kong	3.05%
Germany	2.13%	Belgium	1.83%	Netherlands	3.02%
Belgium	1.79%	Netherlands	1.55%	Germany	2.24%
United Kingdom	1.57%	Canada	0.63%	United	1.31%
China	1.46%	Russian	0.59%	Russian	0.75%
Russian Federation	1.28%	Kazakhstan	0.56%	Italy	0.74%
Australia	0.64%	Australia	0.56%	Australia	0.71%
France	0.60%	Chile	0.52%	France	0.56%

Οι πλαστές ιστοσελίδες αποτελούν σημαντικό μέρος αυτής της μεθόδου ηλεκτρονικής απάτης που είναι γνωστή σαν ««ψάρεμα»» (phishing). Οι περισσότερες απόπειρες "ψαρέματος" περιλαμβάνουν την αποστολή παραπλανητικών e-mail σε χρήστες, τα οποία υποτίθεται ότι προέρχονται από κάποιο νόμιμο οργανισμό, μία δημόσια υπηρεσία, μια τράπεζα ή κάποιο ηλεκτρονικό κατάστημα. Στο περιεχόμενο του μηνύματος αναφέρεται πως ο οργανισμός χρειάζεται να επαληθεύσει τα προσωπικά στοιχεία του πελάτη, παραθέτοντας στο e-mail το link με το οποίο ο χρήστης θα μπορέσει να συνδεθεί στην αντίστοιχη ιστοσελίδα. Όμως, αντί για την πραγματική ιστοσελίδα του οργανισμού, ο χρήστης οδηγείται σε ένα πλαστό website, το οποίο μοιάζει απόλυτα με το αυθεντικό. Έτσι, καταχωρώντας ευαίσθητα προσωπικά στοιχεία, ο χρήστης ουσιαστικά τα εκχωρεί στους κυβερνοεγκληματίες, οι οποίοι μπορούν πλέον να τα χρησιμοποιήσουν για να του αποσπάσουν χρηματικά ποσά, προσωπικά στοιχεία ή να εκδώσουν πιστωτικές κάρτες στο όνομά του.

Το 38% των πλαστών ιστοσελίδων μιμούνται τις ιστοσελίδες γνωστών τραπεζών, ενώ στη δεύτερη θέση έρχονται πλαστές ιστοσελίδες που υποτίθεται πως ανήκουν σε γνωστές υπηρεσίες online πληρωμών. Επίσης επισημαίνει πως, παρόλο που πλέον εντοπίζονται πολύ πιο εύκολα απ’ ό,τι στο παρελθόν, και μόνο το γεγονός ότι πολλαπλασιάζονται με τόσο γρήγορο ρυθμό δικαιολογεί το ότι συνεχίζουν να αποτελούν μία πολύ σημαντική απειλή. Αν και οι χώρες προέλευσης των περισσότερων πλαστών site είναι οι ΗΠΑ και ο Καναδάς, περίπου σε ποσοστό 75%, όπου αυτό επισημαίνει ότι και οι καταναλωτές από τις υπόλοιπες χώρες θα πρέπει να είναι ιδιαίτερα προσεκτικοί όταν πρόκειται να καταχωρίσουν ηλεκτρονικά προσωπικά τους δεδομένα.

- **Tabbabbing**

Το Tabbabbing εκμεταλλεύεται την περιήγηση με πολλαπλές ανοιχτές καρτέλες. Αυτή η μέθοδος ανακατευθύνει σιωπηλά τον χρήστη στον ιστότοπο που επηρεάζεται. Αυτή η τεχνική λειτουργεί αντίστροφα με τις περισσότερες τεχνικές ηλεκτρονικού "ψαρέματος" (phishing), επειδή δεν μεταφέρει άμεσα τον χρήστη στη δόλια τοποθεσία, αλλά φορτώνει την ψεύτικη σελίδα σε μία από τις ανοικτές καρτέλες του προγράμματος περιήγησης.

2.2. Κακόβουλα προγράμματα phishing («malware based phishing»)

Εικόνα 10.

Το κακόβουλο λογισμικό είναι ένα κομμάτι λογισμικού που αναπτύσσεται είτε για να βλάψει μια υπολογιστική συσκευή ή για να αποκομίζει οφέλη από αυτήν εις βάρος του χρήστη. (M. Jakobsson & S. Myers, 2007) Το κακόβουλο λογισμικό μπορεί να χρησιμοποιηθεί για τη συλλογή επικίνδυνων πληροφοριών απευθείας ή για να βοηθήσει άλλες τεχνικές ηλεκτρονικού "ψαρέματος". Τα κακόβουλα προγράμματα μπορούν να χρησιμοποιηθούν για την άμεση συλλογή εμπιστευτικών πληροφοριών και την αποστολή τους. Μπορούν να συλλεχθούν πληκτρολογήσεις, στιγμιότυπα οθόνης, περιεχόμενα πρόχειρου και δραστηριότητες του προγράμματος π.χ. κωδικοί πρόσβασης όπου τα γράμματα εμφανίζονται ως αστερίσκοι, που μπορούν εύκολα να διαβαστούν με ένα πρόγραμμα. Το κακόβουλο λογισμικό μπορεί επίσης να εμφανίζει ένα ψεύτικο περιβάλλον χρήστη για να συλλέγει

πληροφορίες. Συγκεντρωμένες πληροφορίες μπορούν να αποστέλλονται αυτόματα στους εισβολείς μέσω ηλεκτρονικού ταχυδρομείου, διακομιστή ftp ή καναλιού IRC.

Το κακόβουλο λογισμικό μπορεί να βοηθήσει και σε άλλες τεχνικές phishing. Στο web spoofing, μπορεί επίσης να εγκαταστήσει το δημόσιο κλειδί CA του hacker στον κατάλογο αξιόπιστων CA του τοπικού υπολογιστή. Όσον αφορά pharming, μπορεί να αλλάξει τους hosts, τις ρυθμίσεις DNS ή ακόμα και να εκτελέσει ARP spoofing σε τοπικό δίκτυο Ethernet. Το κακόβουλο λογισμικό επίσης μπορεί να εισάγει σε έναν υπολογιστή botnets, να στείλει ψευδή μηνύματα ηλεκτρονικού ταχυδρομείου ή να ενεργεί ως διακομιστής πλαστών ιστοτόπων.

Αξιοποιώντας τη δυνατότητα που προσφέρει το διαδίκτυο στους χρήστες του να διαμοιράζονται αρχεία κάθε είδους, κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία στον δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας σύγχρονη επικοινωνία μεταξύ υπολογιστών, γι’ αυτό τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης (peer-to-peer). Η ευρύτατη χρήση της δυνατότητας αυτής του διαδικτύου οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείου (μουσικής, εικόνων, προγραμμάτων), με μηδαμινό κόστος για το χρήστη. Η συγκέντρωση των ταυτόχρονα διασυνδεδεμένων χρηστών σε κάθε τέτοιο πρόγραμμα διαμοιρασμού αρχείων ανέρχεται σε μερικά εκατομμύρια. Δημιουργούνται έτσι μερικές από τις μεγαλύτερες διαδικτυακά πληθυσμιακές κοινότητες, μέσα στις οποίες διακινείται σχεδόν ανεξέλεγκτα κάθε είδους υλικό.

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" (Phishing) αποσκοπούν στην υποκλοπή των στοιχείων σύνδεσης και του κωδικού πρόσβασης ενός ατόμου, ώστε ο εγκληματίας στον κυβερνοχώρο να μπορεί να αναλάβει τον έλεγχο του κοινωνικού δικτύου, του ηλεκτρονικού ταχυδρομείου και των ηλεκτρονικών τραπεζικών λογαριασμών του θύματος. Το 70% των χρηστών του διαδικτύου επιλέγουν τον ίδιο κωδικό πρόσβασης για σχεδόν κάθε υπηρεσία ιστού που χρησιμοποιούν. Αυτός είναι ο λόγος για τον οποίο το ηλεκτρονικό «ψάρεμα» είναι τόσο αποτελεσματικό, χρησιμοποιώντας τα ίδια στοιχεία σύνδεσης, ο εγκληματίας μπορεί να έχει πρόσβαση σε πολλούς ιδιωτικούς λογαριασμούς και να τους διαχειρίζεται.

Μια επίθεση κακόβουλου λογισμικού γίνεται όταν ένα πρόγραμμα "malware" αναλαμβάνει έναν υπολογιστή προκειμένου να διαδώσει το σφάλμα στις συσκευές και τα προφίλ άλλων ανθρώπων. Μπορεί επίσης να μολύνει έναν υπολογιστή και να τον μετατρέψει σε ένα botnet, που σημαίνει ότι ο εγκληματίας στον κυβερνοχώρο μπορεί να ελέγξει τον υπολογιστή και να

τον χρησιμοποιήσει για να στείλει malware σε άλλα botnets, όπως το Rustock, που στέλνει τα περισσότερα μηνύματα spam και συχνά διαφημίζουν φαρμακευτικά προϊόντα ή λογισμικό ασφαλείας, τα οποία οι άνθρωποι πιστεύουν ότι χρειάζονται για να λύσουν ένα ζήτημα ασφάλειας που δεν υπάρχει στην πραγματικότητα.

Σημαντικές απειλές εκδηλώνονται μέσω προγραμμάτων που εκμεταλλεύονται μία ή περισσότερες ευπάθειες των συστατικών μερών της υποδομής της υποστήριξης στα περιβάλλοντα του ηλεκτρονικού εμπορίου. Τέτοια προγράμματα αναφέρονται με τον όρο κακόβουλο λογισμικό (malicious software ή malware). Είναι προγράμματα κατασκευασμένα ειδικά με στόχο την παραβίαση της ασφάλειας του συστήματος. Μια πρώτη κατηγοριοποίηση κακόβουλου λογισμικού διακρίνει αυτό που χρειάζεται ένα πρόγραμμα-φορέα σε αντιδιαστολή με αυτό που λειτουργεί ανεξάρτητα (Κάτσικας, 2001). Έτσι, στην πρώτη κατηγορία ανήκουν τα ουσιαστικά τμήματα προγράμματος που δεν είναι δυνατόν να υπάρξουν μόνα τους, χωρίς κάποιο λογισμικό συστήματος ή κάποιο πρόγραμμα εφαρμογής. Ενώ στη δεύτερη κατηγορία ανήκουν όσα είναι αυτόνομα προγράμματα που μπορούν να εκτελεστούν κάτω από τον έλεγχο του λειτουργικού συστήματος, όπως συμβαίνει στα κανονικά προγράμματα. (Orunsolu, A.A. 2017)

Μια άλλη κατηγοριοποίηση του κακόβουλου λογισμικού διακρίνει το μη αναπαραγόμενο από το αναπαραγόμενο. Η πρώτη κατηγορία περιλαμβάνει τμήματα προγράμματος που ενεργοποιούνται όταν καλείται το πρόγραμμα-φορέας για να εκτελέσει μια συγκεκριμένη λειτουργία. Η δεύτερη κατηγορία περιλαμβάνει τμήματα προγράμματος, αλλά και αυτόνομα προγράμματα που, όταν εκτελούνται, μπορούν να παραγάγουν ένα ή περισσότερα αντίγραφα του εαυτού τους, τα οποία θα ενεργοποιηθούν αργότερα στον ίδιο ή σε κάποιον άλλον υπολογιστή.

Για την εγκατάσταση (μόλυνσης) ενός κακόβουλου λογισμικού σε ένα μηχάνημα, συνήθως απαιτείται η ανθρώπινη συμμετοχή. Η συμμετοχή αυτή μπορεί να είναι άμεση (π.χ. εισαγωγή μίας συσκευής USB, άνοιγμα συνημμένων αλληλογραφίας, προεπισκόπηση μηνυμάτων αλληλογραφίας, ανταλλαγή αρχείων κλπ.), αλλά μπορεί να είναι και έμμεση (π.χ. άρνηση ενημέρωση του λογισμικού ασφαλείας, επιλογή προφανούς κωδικού σύνδεσης κλπ.). Το τμήμα του κώδικα που είναι υπεύθυνο για τις παρενέργειες του λογισμικού καλείται φορτίο (payload).

Το κακόβουλο λογισμικό περιλαμβάνει επιπρόσθετο κώδικα με σκοπό:

I. την αναπαραγωγή του (την εξάπλωση του στο σύστημα που προσβάλλει - «μόλυνση» από το ένα πρόγραμμα του μηχανήματος σε άλλο πρόγραμμα)

II. τη μετάδοσή του (την εξάπλωσή του από το μηχάνημα που μολύνθηκε σε άλλα) (Μάγκος. 2013).

Επίσης όλα τα είδη κακόβουλου λογισμικού δίνουν μεγάλη σημασία στον εντοπισμό της πιο κατάλληλης περιοχής για να εγκατασταθούν. Επιδιώκουν με την εκτέλεσή τους να μην είναι ανιχνεύσιμα, να εγγράφονται στο μητρώο του συστήματος και να δημιουργούν εμπόδια στις διαδικασίες αφαίρεσής τους.

2.2.1. Μορφές κακόβουλου λογισμικού

- Ιός (virus):

Ένα κακόβουλο λογισμικό το οποίο αφού μολύνει ένα μηχάνημα έχει την ικανότητα να αναπαράγεται και να μολύνει και άλλα προγράμματα στο μηχάνημα αυτό. Ο όρος αυτός, δεν είναι τυχαίος, προήλθε από τη βιολογία. Ο βιολογικός ιός είναι ένα πολύ μικρό τμήμα γενετικού κώδικα που μπορεί να καταλάβει τον μηχανισμό αναπαραγωγής ενός υγιούς ζωντανού κυττάρου κάποιου οργανισμού και να τον εξαπατήσει, έτσι ώστε να δημιουργήσει χιλιάδες τέλεια αντίγραφα του εαυτού του. Οι ιοί του υπολογιστή περιέχουν στον κώδικά τους τη «συνταγή» δημιουργίας τέλειων αντιγράφων του εαυτού τους (Κάτσικας, 2001). Μόλις εγκατασταθεί ο ιός, οποτεδήποτε ο μολυσμένος υπολογιστής αν έρθει σε επαφή με μη μολυσμένο πρόγραμμα, το πρόγραμμα αυτό μολύνεται με την εισαγωγή ενός κώδικά αντιγραμμένου ιού.

Εικόνα 11.

- Σκουλήκι (Worm):

Ένα κακόβουλο λογισμικό το οποίο, αφού μολύνει ένα μηχάνημα, έχει την ικανότητα να μεταδίδεται αυτόματα, κάνοντας χρήση της υπάρχουσας δικτυακής υποδομής. Από τη στιγμή που θα ενεργοποιηθεί μέσα σ' ένα σύστημα, το σκουλήκι μπορεί να συμπεριφερθεί ως ιός, ως βακτήριο, να εισαγάγει Δούρειους Ίππους "Trojan Horse" ή να εκτελέσει οποιαδήποτε καταστροφική ενέργεια (Aycock, 2006). Για να αναπαραχθεί ένα σκουλήκι μπορεί να χρησιμοποιήσει την υπηρεσία ηλεκτρονικού ταχυδρομείου (ταχυδρομεί ένα αντίγραφο του εαυτού του σε άλλα συστήματα), την υπηρεσία εκτέλεσης από απόσταση (εκτελεί ένα αντίγραφο του εαυτού του σε κάποιο άλλο σύστημα) ή την υπηρεσία σύνδεσης από απόσταση (συνδέεται με ένα απομακρυσμένο σύστημα ως χρήστης και μετά χρησιμοποιεί εντολές για να αντιγράψει τον εαυτό του από ένα σύστημα σε άλλο).

- Δούρειος Ίππος (Trojan Horse):

Ένα κακόβουλο λογισμικό το οποίο σχετίζεται με το στοιχείο της παραπλάνησης, καθώς συνήθως μεταμφιέζεται σε μια χρήσιμη εφαρμογή, η οποία περιέχει κακόβουλο κώδικα (Μάγκος, 2013) π.χ. ο χρήστης παροτρύνεται να δει μια φωτογραφία, ή να κατεβάσει ένα δωρεάν εργαλείο που ωστόσο περιέχει κακόβουλο κώδικα. Συνήθως, ένας δούρειος ίππος δημιουργεί μια πίσω πόρτα (backdoor) στο σύστημα, στην οποία ο εισβολέας θα μπορέσει αργότερα να συνδεθεί ώστε να διαχειριστεί εξ' αποστάσεως το σύστημα.

Ως πίσω πόρτα (backdoor), ορίζεται κάθε μυστικό σημείο εισόδου σε ένα πρόγραμμα, που εξουσιοδοτεί κάποιον που την γνωρίζει να αποκτήσει δικαιώματα προσπέλασης στο σύστημα, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης. Τις περισσότερες φορές τα trojans δεν αναπαράγονται για αυτόν τον λόγο και δεν χαρακτηρίζονται ως ιοί, όμως χρησιμοποιούνται ως μέσο μεταφοράς για διάφορες μορφές κακόβουλου λογισμικού (spyware, adware, rootkits, ιούς ή σκουλήκια), οπότε εμπίπτουν στην κατηγορία του πολυμερούς "multipartite" κακόβουλου λογισμικού. Η ονομασία παραπέμπει στον Δούρειο Ίππο που χρησιμοποίησαν οι αρχαίοι Έλληνες για να παραπλανήσουν τους Τρώες, κατά τον Τρωικό πόλεμο.

- Spyware Adware:

Ένα κακόβουλο λογισμικό με ανεπτυγμένα χαρακτηριστικά λειτουργιών του Δούρειου Ίππου (κυρίως ως προς τον τρόπο μόλυνσης), με σκοπό την παρακολούθηση - υποκλοπή ευαίσθητων δεδομένων (spyware), ή την αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων (adware). Αναφέρονται στα μέλη της ίδιας κατηγορίας, καθώς συνεργάζονται συνήθως για να πετύχουν τον σκοπό τους (πχ. παρακολούθηση της αγοραστικής συμπεριφοράς κατά την περιήγηση στον παγκόσμιο ιστό και στη συνέχεια εμφάνιση διαφημιστικών μηνυμάτων). Στα ευαίσθητα δεδομένα που στοχεύει το spyware ενδεικτικά περιλαμβάνονται προσωπικά στοιχεία, ονόματα χρήστη, κωδικοί πρόσβασης, κλειδιά, αριθμοί πιστωτικής κάρτας, και λεπτομέρειες συναλλαγών. Η χειρότερη εκδοχή του spyware είναι ως λογισμικό keylogger που υποκλέπτει κάθε χαρακτήρα που πληκτρολογεί ο χρήστης στο παρασκήνιο και τον προωθεί σε τρίτους, πχ. μέσω e-mail. Συνήθως τα spyware συνεργάζονται με λογισμικά adware ή και με διαφημιστικές εταιρείες στο Internet, με σκοπό τη δημιουργία ενός προφίλ χρήστη και την αποστολή στοχευμένων διαφημίσεων. Οι παρενέργειες ενός λογισμικού adware ποικίλουν (Μάγκος, 2013):

1. Με την εμφάνιση ανεπιθύμητων μηνυμάτων στο πρόγραμμα περιήγησης (browser), ή στην επιφάνεια εργασίας (desktop)
2. Με την αλλαγή της αρχικής σελίδας του browser (browser hijacking)
3. Με την αλλαγή της αρχικής σελίδας αναζήτησης στο Web, ανακατεύθυνση (redirection) σε πλαστό δικτυακό τόπο (web spoofing), κλπ.

Όταν οι παρενέργειες των spyware ή adware είναι μικρής κλίμακας, αντί του όρου «κακόβουλο λογισμικό» χρησιμοποιείται ο όρος «ανεπιθύμητο λογισμικό» (potentially unwanted programs, PUPs). Ένας άλλος όρος που χρησιμοποιείται είναι "greyware", ακριβώς για να εστιάσει στο ότι πρόκειται για λογισμικό το οποίο, ενώ δεν είναι πάντα πλήρως κακόβουλο, έχει μια ύποπτη ή πιθανώς ανεπιθύμητη πτυχή σε αυτό.

- Rootkit:

Το rootkit είναι ένα κακόβουλο λογισμικό το οποίο λειτουργεί σε πολύ χαμηλό επίπεδο στο λειτουργικό σύστημα, και συνήθως ενσωματώνει λειτουργίες απόκρυψης (stealth) ώστε να παρακάμπτει τους μηχανισμούς πρόληψης και ανίχνευσης. Αξιοποιεί προνόμια Διαχειριστή (Administrator) με σκοπό την απόκρυψη της παρουσίας του στο σύστημα. Ένα λογισμικό rootkit μπορεί να ανήκει σε οποιαδήποτε από τις παραπάνω κατηγορίες, ωστόσο συνήθως ανοίγει πόρτες που θα επιτρέψουν τη μετέπειτα απομακρυσμένη διαχείριση του μηχανήματος από κάποιον τρίτο. Ο κακόβουλος κώδικας τύπου rootkit (ή αλλιώς τύπου stealth), ενσωματώνει λειτουργίες όπως (Μάγκος, 2013):

I. Διαδικασία απόκρυψης (hiding process): αποκρύπτεται μια διαδικασία αφαιρώντας την από τον πίνακα Διαχείρισης Εργασιών (Task Manager), ή υλοποιείται μια διαδικασία ως ένα σύνολο νημάτων (threads), των οποίων η ανίχνευση είναι δύσκολη,
II. απόκρυψη θύρας (port): αποκρύπτεται η λίστα με τις θύρες που θα χρησιμεύσουν ως «πόρτες» για την απομακρυσμένη διαχείριση του συστήματος,
III. απόκρυψη κλειδιού στο μητρώο (registry): χρησιμοποιούνται ονόματα κλειδιών που δεν εγείρουν υποψίες (παραπέμπουν σε «ακίνδυνες» ή χρήσιμες εφαρμογές, πχ. WindowsOS.exe).

- Bot zombie:

Ένα κακόβουλο λογισμικό που παραβιάζει συστήματα υπολογιστών και εγκαθίσταται στα μέλη ενός δικτύου υπολογιστών (botnet) που ελέγχεται εξ΄ αποστάσεως από τρίτους, με σκοπό την πραγματοποίηση Κατανεμημένων Επιθέσεων Άρνησης Υπηρεσιών (Distributed Denial of Service attacks ή DDOS attacks). Επιθέσεις τις οποίες ένας (συνήθως μεγάλος) αριθμός μολυσμένων υπολογιστών συνδέεται στον υπολογιστή μέσω δικτύου προσπαθώντας να τον οδηγήσει σε κατάρρευση, να είναι ανίκανος να λειτουργήσει κανονικά λόγω του υπερβολικού φόρτου εργασίας για τις αποκρίσεις που καλείται να στείλει, καθώς επεξεργάζεται τα πολυπληθή αιτήματα που λαμβάνει.

Οι επιθέσεις άρνησης υπηρεσίας είναι επιθέσεις εναντίον της διαθεσιμότητας (availability) του μηχανήματος. Ο όρος «bot», προέρχεται από την (Τσεχικής προέλευσης) λέξη «robota» και χρησιμοποιείται για να περιγράψει κάθε είδους αυτοματοποιημένη διαδικασία. Ένας υπολογιστής που έχει μολυνθεί από ένα bot συχνά αναφέρεται ως «zombie». Οι υπολογιστές zombies μπορεί να χρησιμοποιηθούν για επιθέσεις τύπου Άρνησης Υπηρεσίας (DOS) σε εξυπηρετητές Web, για την αποστολή μηνυμάτων spam, για την πραγματοποίηση επιθέσεων παραπλάνησης (phishing) κλπ.

- Βακτήρια (bacteria):

Είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία, και ο μοναδικός τους σκοπός είναι να παραπλανούν. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του, ή πιθανόν να δημιουργεί δύο νέα αρχεία, όπου καθένα από αυτά είναι αντίγραφα του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές. Τα βακτήρια αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες (επίθεση τύπου άρνησης υπηρεσίας).

- Λογική βόμβα (logic bomb):

Ένας κώδικας ενσωματωμένος σε κάποιο νόμιμο πρόγραμμα εφαρμογής, ρυθμισμένος να «εκραγεί» όταν εκπληρωθούν κάποιες συγκεκριμένες συνθήκες. Παραδείγματα τέτοιων συνθηκών είναι η έλευση μιας συγκεκριμένης μέρας της εβδομάδας ή μιας ημερομηνίας, η παρουσία/απουσία συγκεκριμένων αρχείων, ή η εκτέλεση της εφαρμογής από ένα συγκεκριμένο χρήστη (Ince, 2009; Κάτσικας, 2001). Από τη στιγμή που θα ενεργοποιηθεί, η

βόμβα μπορεί να τροποποιήσει ή να διαγράψει δεδομένα ακόμα και ολόκληρα αρχεία, να προκαλέσει την διακοπή ενός συστήματος ή να κάνει οποιαδήποτε άλλη ζημιά.

Η διείσδυση του παγκόσμιου Ιστού και των υπηρεσιών του, είχε ως συνέπεια τη δημιουργία και την αλματώδη εξάπλωση νέων και πιο ισχυρών μορφών κακόβουλου λογισμικού.

- Παρασιτικός (parasitic virus)**:**

Ο ποιο παραδοσιακός αλλά και πιο διαδεδομένος τύπος ιού. Προσαρτάται σε εκτελέσιμα αρχεία (πχ. αρχεία .exe ή αρχεία .com) και αναπαράγεται, όταν εκτελεστεί το μολυσμένο πρόγραμμα, βρίσκοντας και άλλα εκτελέσιμα αρχεία για να μολύνει. Όταν εκτελεστεί το μολυσμένο πρόγραμμα, εγκαθίσταται συνήθως ως μέρος του λειτουργικού συστήματος και παραμένει στην κύρια μνήμη του συστήματος (memory-resident), ώστε να «μολύνει» και άλλα προγράμματα που εκτελεί ο χρήστης. Αντιθέτως, υπάρχουν και λιγότερο βλαπτικοί προσωρινοί ιοί στη μνήμη (non memory-resident) οι οποίοι επειδή δεν εγκαθίστανται στην κεντρική μνήμη, όταν εκτελούνται, σαρώνουν το δίσκο μολύνοντας και έπειτα σταματά η δράση τους.

- Τομέα εκκίνησης (boot virus):

Οι ιοί αυτοί μολύνουν τον τομέα εκκίνησης (boot sector) ενός σταθερού ή αφαιρούμενου (removable) αποθηκευτικού μέσου (πχ. του σκληρού δίσκου ή ενός flash drive). Ο τομέας εκκίνησης περιέχει ένα πρόγραμμα μικρού μεγέθους το οποίο το λειτουργικό σύστημα εντοπίζει και «φορτώνει» στην κύρια μνήμη. Τέτοιοι ιοί μπορούν επίσης να μολύνουν την περιοχή MBR (Master Boot Record) που περιέχει τον πίνακα κατατμήσεων του δίσκου, όπου διαδίδονται όταν το σύστημα εκκινήσει από τον δίσκο που περιέχει τον ιό.

- Πολυμερής ή Υβριδικός (multipartite, or hybrid virus):

Συνδυάζει χαρακτηριστικά δύο ή περισσότερων κατηγοριών. Πχ. χαρακτηριστικά ιών του τομέα εκκίνησης και παρασιτικών ιών: ένα μηχάνημα μολύνεται αν χρησιμοποιήσει ένα «μολυσμένο» USB ή αν εκτελέσει ένα μολυσμένο πρόγραμμα. Ο ιός αποτελείται από κώδικα που καλύπτει και τις δύο περιπτώσεις.

οπότε ανάλογα με την περίσταση εκτελείται το αντίστοιχο τμήμα, ενώ αυξάνονται οι πιθανότητες μόλυνσης.

- Ιός συστήματος αρχείων (file system virus):

Ένας τέτοιος ιός (ονόματα σε χρήση είναι link virus, cluster virus, ή FAT virus) δεν συμπεριφέρεται όπως οι παραδοσιακοί ιοί, δηλαδή δε μολύνει τον κώδικα εκτελέσιμων ή άλλων αρχείων. Έχει ωστόσο τη δυνατότητα να παρεμβάλλεται κατά την κλήση ενός προγράμματος και να εκτελεί τον επιβλαβή του κώδικα. Για να το επιτύχει, τροποποιεί τον πίνακα διευθύνσεων που υπάρχει στον σκληρό δίσκο κάθε υπολογιστή, όπου είναι καταχωρημένη η ακριβής θέση (διεύθυνση) του κάθε αρχείου. Το λειτουργικό σύστημα χρησιμοποιεί αυτόν τον πίνακα για να οργανώσει τα αρχεία στον δίσκο κάθε φορά που γίνεται κλήση ενός αρχείου. Ο ιός αλλάζει τον πίνακα διευθύνσεων ώστε όταν ζητείται η εκτέλεση ενός «μολυσμένου» προγράμματος, το λειτουργικό σύστημα παραπέμπεται σε μια άλλη θέση όπου βρίσκεται ο κώδικας του ιού, που στη συνέχεια φορτώνεται στη μνήμη και εκτελείται.

- Μακρο ιός (macro virus):

Προσβάλλει αρχεία δεδομένων (documents ή emails) που περιέχουν μακροεντολές (macros). Οι μακροεντολές είναι κώδικας εντολών, γραμμένος με εξειδικευμένες γλώσσες μακροεντολών (macro languages). Συνήθως είναι σε μορφή γλώσσας συγγραφής σεναρίων (scripting language). Πχ. VBA (Visual Basic for Applications). Χρησιμοποιούνται κυρίως σε προγράμματα εφαρμογών γραφείου (πχ. Word, Excel, PowerPoint, Outlook, Acrobat) για την αυτοματοποίηση ορισμένων λειτουργιών που εκτελεί ο χρήστης (Aycock, 2006).

Οι μακροεντολές επομένως αυτοματοποιούν ένα σύνολο από κακόβουλες ενέργειες. Πχ. όταν σε έναν επεξεργαστή κειμένου εκτελεστεί η μακροεντολή ενός μολυσμένου εγγράφου, ο ιός ενεργοποιείται και απελευθερώνει το καταστροφικό του φορτίο. Αυτός ο τύπος ιών είναι ο κύριος λόγος αύξησης του αριθμού των ιών που εντοπίζονται σε επιχειρηματικά συστήματα. Η δημοτικότητα των εφαρμογών γραφείου, έχει πραγματικά συνεισφέρει στην εξάπλωση αυτού του είδους των ιών. Η επικινδυνότητα του τύπου αυτού οφείλεται κατ' αρχάς στο ότι είναι ανεξάρτητος από πλατφόρμες υλικού. Ο κώδικας που δημιουργείται από

μια γλώσσα συγγραφής σεναρίων, μπορεί να εκτελεστεί σε όλες τις πλατφόρμες: ένας μακρο-ιός μπορεί να εκτελεστεί σε προσωπικό υπολογιστή "PC" και σε ένα "MAC" της APLE.

Το δεύτερο στοιχείο αυξημένης επικινδυνότητας είναι η εύκολη διάδοση (με πιο συνηθισμένη μέθοδο διάδοσης μέσο ηλεκτρονικού ταχυδρομείου). Τέλος, επειδή μολύνουν αρχεία δεδομένων (έγγραφα, emails) και όχι εκτελέσιμα προγράμματα, έχουν περισσότερους στόχους, ενώ η πλειοψηφία της πληροφορίας που εισάγεται σε έναν υπολογιστή είναι σε μορφή τέτοιων αρχείων και όχι σε μορφή εκτελέσιμων προγραμμάτων (Κάτσικας, 2001). Οι περισσότερες μακρο-εντολές ενεργοποιούνται με το αυτόματο άνοιγμα ενός εγγράφου (πχ. λειτουργία auto-open). Για την αναπαραγωγή τους συνήθως οι μακρο-ιοί είναι προγραμματισμένοι να μετατρέπουν τα μολυσμένα έγγραφα σε πρότυπα (templates) ώστε να μολυνθούν όλα τα έγγραφα που θα δημιουργήσει μελλοντικά ο χρήστης.

- Απόκρυψης (stealth virus):

  Ένας ειδικά σχεδιασμένος ιός για να αποφεύγει την ανίχνευση από το αντιβιοτικό λογισμικό. Χρησιμοποιεί τεχνικές που στοχεύουν στην εξαφάνιση των ιχνών του, καθώς και των συμπτωμάτων του, όπου παρόμοιες τεχνικές με αυτές συναντούμε στο κακόβουλο λογισμικό τύπου rootkit. Για αυτό και αρκετές φορές ο όρος stealth virus χρησιμοποιείται ως συνώνυμο του rootkit. Μια συνηθισμένη τακτική απόκρυψης είναι η παρεμβολή στις κλήσεις του αντιβιοτικού λογισμικού προς ένα αρχείο (read request intercepts), ώστε να επιστρέφει στην καθαρή έκδοσή του, ενώ λίγο αργότερα γίνεται η επαναφορά της μολυσμένης έκδοσης του αρχείου.

Μια άλλη ενδεικτική τεχνική απόκρυψης στοχεύει στην υπερπήδηση του έλεγχου ακεραιότητας (integrity checking) που πραγματοποιούν ορισμένα αντιβιοτικά λογισμικά σε όλες τις εφαρμογές του συστήματος (Μάγκος, 2013). Αυτό σημαίνει πως, όταν τροποποιείται ο κώδικας μιας εφαρμογής το αντιβιοτικό λογισμικό ζητάει από τον χρήστη να επιβεβαιώσει την τροποποίηση (πχ. όταν ο χρήστης εγκαθιστά μια επιδιόρθωση, patch, για μια εφαρμογή). Ένας ιός απόκρυψης παραμένει ενεργός στη μνήμη (memory-resident) περιμένοντας την κατάλληλη στιγμή που θα μπορέσει να μολύνει όσα προγράμματα τροποποιούν τον κώδικα

κατόπιν μιας νόμιμης εντολής του χρήστη ή του προγράμματος (πχ. εγκατάσταση μιας αναβάθμισης ή μιας επιδιόρθωσης).

- Πολυμορφικός ιός (polymorphic virus)**:**

  Ο πολυμορφικός ιός μεταλλάσσεται με κάθε μόλυνση (αποτελούμενος από διαφορετικές ακολουθίες ψηφίων), αλλάζοντας την υπογραφή του καθιστώντας έτσι αδύνατη την ανίχνευσή του μέσω αυτής (Virus Bulletin, 2015). Για να πετύχει αυτήν τη διαφοροποίηση, ο ιός μπορεί να εισάγει τυχαίες περιττές εντολές ως θόρυβο ή να αλλάζει τη σειρά εμφάνισης ανεξάρτητων μεταξύ τους εντολών. Όμως, μια πιο αποτελεσματική τακτική είναι να χρησιμοποιήσει κρυπτογράφηση του κώδικά με ένα συμμετρικό κλειδί που συνεχώς αλλάζει (Κάτσικας, 2001).

Πιο συγκεκριμένα, στην τακτική αυτή ένα τμήμα του ιού, που συνήθως ονομάζεται μηχανή μετάλλαξης (mutating engine), δημιουργεί ένα τυχαίο κλειδί κρυπτογράφησης και κρυπτογραφεί τον υπόλοιπο κώδικα του ιού. Το κλειδί αποθηκεύεται μαζί με τον ιό και η μηχανή μετάλλαξης μεταλλάσσεται η ίδια. Όταν κληθεί το μολυσμένο πρόγραμμα, ο ιός χρησιμοποιεί το αποθηκευμένο κλειδί για να αυτοαποκρυπτογραφηθεί. Όταν ο ιός αναπαραχθεί, δημιουργείται νέο κλειδί.

3. Νομοθεσία διαδικτύου σύμφωνα με το phishing

Για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, η ΕΕ έχει εφαρμόσει μια νομοθεσία και έχει υποστηρίξει την επιχειρησιακή συνεργασία, στο πλαίσιο της στρατηγικής της για την ασφάλεια. Η ανακοίνωση "Ανθεκτικότητα, αποτροπή και άμυνα οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ " στηρίζεται και αναπτύσσει περαιτέρω τη στρατηγική της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο.

Το έγκλημα στον κυβερνοχώρο αποτελείται από εγκληματικές πράξεις που διαπράττονται ηλεκτρονικά μέσω δικτύων ηλεκτρονικών επικοινωνιών και συστημάτων πληροφοριών. Είναι ένα πρόβλημα χωρίς περιθώρια που μπορεί να ταξινομηθεί σε τρεις ευρείς ορισμούς:

I. Ειδικά εγκλήματα στο Διαδίκτυο, όπως επιθέσεις κατά των συστημάτων των πληροφοριών ή ηλεκτρονικού "ψαρέματος" (π.χ. ψεύτικες ιστοσελίδες των τραπεζών για την αναζήτηση κωδικών πρόσβασης που επιτρέπουν την πρόσβαση στους τραπεζικούς λογαριασμούς των θυμάτων).

II. Ηλεκτρονική απάτη και πλαστογραφία. Οι απάτες μεγάλης κλίμακας μπορούν να διαπραχθούν σε απευθείας σύνδεση μέσω μέσων όπως η κλοπή ταυτότητας, το ηλεκτρονικό "«ψάρεμα»" (phishing), το spam και ο κακόβουλος κώδικας.

III. Παράνομο περιεχόμενο στο διαδίκτυο, συμπεριλαμβανομένου υλικού σεξουαλικής κακοποίησης παιδιών, προτροπή σε φυλετικό μίσος, προτροπή σε τρομοκρατικές πράξεις και δοξασμό βίας, τρομοκρατία, ρατσισμό και ξενοφοβία.

3.1 Νομοθετικές δράσεις της ΕΕ που συμβάλλουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Το 2001, η απόφαση του πλαισίου για την καταπολέμηση της απάτης και της πλαστογραφίας, μέσων πληρωμής πλην των μετρητών, όριζε τις δόλιες συμπεριφορές που τα κράτη μέλη πρέπει να θεωρούν αξιόποινες πράξεις. Στις 13 Σεπτεμβρίου 2017, η Επιτροπή πρότεινε μια νέα οδηγία που αποσκοπεί στην επικαιροποίηση του ισχύοντος νομικού πλαισίου, την άρση των εμποδίων στην επιχειρησιακή συνεργασία και την ενίσχυση της πρόληψης και της βοήθειας των θυμάτων, προκειμένου να καταστεί πιο αποτελεσματική η καταπολέμηση της απάτης και της πλαστογραφίας των μέσων πληρωμής πλην των μετρητών αποτελεσματικά.

Το 2013 η οδηγία για τις επιθέσεις κατά των συστημάτων πληροφοριών, αποσκοπούσε στην αντιμετώπιση των εκτεταμένων επιθέσεων στον κυβερνοχώρο, απαιτώντας από τα κράτη μέλη να ενισχύσουν τους εθνικούς νόμους στον τομέα της εγκληματικότητας στον κυβερνοχώρο και να εισαγάγουν αυστηρότερες ποινικές κυρώσεις. Το 2017, η Επιτροπή δημοσίευσε μια έκθεση με την οποία αξιολογείται ο βαθμός στον οποίο τα κράτη μέλη έλαβαν τα αναγκαία μέτρα για να συμμορφωθούν με την οδηγία.

Η αποστολή Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος συμπεριλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Δίωξη Ηλεκτρονικού Εγκλήματος, στην εσωτερική της δομή αποτελείται από τέσσερα τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου. Έτσι, στη νέα αναβαθμισμένη δομή της αποτελείται από:

- Το Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων, ασχολείται με τις εγκληματικές πράξεις που διαπράττονται στα μέσα της ηλεκτρονικής επικοινωνίας και ψηφιακής αποθήκευσης ή μέσω αυτών σε ολόκληρη τη χώρα.
- Το Τμήμα Προστασίας Ανηλίκων, ασχολείται με τα εγκλήματα που διαπράττονται με τη χρήση του διαδικτύου και άλλων μέσων ηλεκτρονικής ή ψηφιακής επικοινωνίας και αποθήκευσης.
- Το Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, ασχολείται με τις υποθέσεις παράνομης διείσδυσης σε υπολογιστικά συστήματα και κλοπής, καταστροφής ή παράνομης διακίνησης λογισμικού υλικού, ψηφιακών δεδομένων και οπτικοακουστικών έργων, που τελούνται σε ολόκληρη τη χώρα.
- Το Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών, ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών. (Buku, M.W. and Mazer, R., 2015)

Η ΕΕ προτίθεται να αντιμετωπίσει αυτό το πρόβλημα δημιουργώντας ένα Ευρωπαϊκό κέντρο για την εγκληματικότητα στον κυβερνοχώρο, το οποίο θα προειδοποιεί τις χώρες της ΕΕ για τις σοβαρότερες απειλές και θα επισημαίνει τις αδυναμίες άμυνας των ο online

εγκαταστάσεων. Θα εντοπίζει επίσης τα εγκληματικά δίκτυα και τους πλέον επικίνδυνους εγκληματίες και θα παρέχει υποστήριξη κατά τη διάρκεια σχετικών ερευνών. Το κέντρο αυτό θα συγκεντρώνει πληροφορίες από τον ιδιωτικό τομέα, τη βιομηχανία, την αστυνομία και τον ακαδημαϊκό κόσμο, όπου θα βοηθά τις υπηρεσίες διερεύνησης τέτοιων εγκλημάτων καθώς και τις εισαγγελικές και δικαστικές αρχές. Ο καθένας μπορεί να πέσει θύμα κάποιας μορφής ηλεκτρονικού εγκλήματος: (Chen, C.-M., Guan, D., & Su, Q.-K., 2014)

- κλοπή online ταυτότητας
- απάτη μέσω υπολογιστή
- υποκλοπή πιστωτικής κάρτας
- σεξουαλική εκμετάλλευση παιδιών
- πειρατεία ηλεκτρονικών λογαριασμών
- επιθέσεις σε δημόσια ή ιδιωτικά συστήματα

4. Πρόληψη κατά του ηλεκτρονικού "ψαρέματος"

Εικόνα 12.

Υπάρχει ευρύ φάσμα τεχνικών προσεγγίσεων για την αποτροπή των επιθέσεων ηλεκτρονικού "ψαρέματος" που φτάνουν στους χρήστες ή για την αποτροπή της επιτυχούς καταγραφής ευαίσθητων πληροφοριών.

Η ενημέρωση του κοινού είναι ο καλύτερος τρόπος αντιμετώπισης καθώς η αποτελεσματικότερη αντιμετώπιση του προβλήματος είναι η πρόληψη. Επίσης υπάρχουν και οι τεχνικοί τρόποι αντιμετώπισης όπως:

- Λήψη προγραμμάτων περιήγησης που αναγνωρίζουν τους ιστότοπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα μέσω διαφορετικού URL
- Χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας (Anti-spyware)
- Λήψη προγραμμάτων anti-spam για προστασία email
- Λήψη πρόσθετων (add-ons) για τον εντοπισμό phishing script στις ιστοσελίδες

Ø **Εκπαίδευση χρηστών**

Το ηλεκτρονικό "«ψάρεμα»" εκμεταλλεύεται τις αδυναμίες των ανθρώπων, έτσι ώστε οι τεχνικές λύσεις να μπλοκάρουν μόνο ορισμένες από τις ιστοσελίδες phishing. Δεν έχει σημασία πόσα λογισμικά κρυπτογράφησης, πιστοποίησης ή μηχανισμούς επαλήθευσης ταυτότητας "δύο παραγόντων" έχει ένας οργανισμός αν το άτομο πίσω από το πληκτρολόγιο γίνει θύμα μίας επίθεσης phishing.

Οι άνθρωποι μπορούν να εκπαιδευτούν για να αναγνωρίσουν απόπειρες ηλεκτρονικού phishing και να τις αντιμετωπίσουν μέσω ποικίλων προσεγγίσεων. Αυτή η εκπαίδευση μπορεί να είναι αποτελεσματική, ειδικά όταν η κατάρτιση δίνει έμφαση στην εννοιολογική γνώση και παρέχει άμεση ανατροφοδότηση. Πολλοί οργανισμοί εκτελούν τακτικές προσομοίωσης ηλεκτρονικού "ψαρέματος" στο προσωπικό τους για να μετρήσουν την αποτελεσματικότητα της εκπαίδευσης τους.

Οι χρήστες μπορούν να λάβουν μέτρα για την αποφυγή απόπειρων ηλεκτρονικού "ψαρέματος" τροποποιώντας ελαφρώς τις συνήθειες στην περιήγησή τους. Όταν ένας χρήστης επικοινωνεί με έναν λογαριασμό που χρειάζεται να είναι "επαληθευμένος" είναι μια λογική προφύλαξη να επικοινωνήσει με την εταιρεία από την οποία προήλθε το μήνυμα ηλεκτρονικού ταχυδρομείου, για να ελέγξει εάν είναι νόμιμο. Εναλλακτικά, η διεύθυνση που γνωρίζει το άτομο ότι είναι ο γνήσιος ιστότοπος της εταιρείας που μπορεί να πληκτρολογηθεί στη γραμμή διευθύνσεων του προγράμματος περιήγησης, αντί το άτομο να εμπιστευτεί τους υπερσυνδέσμους στο ύποπτο μήνυμα.

Σχεδόν όλα τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου από εταιρείες προς τους πελάτες τους περιέχουν ένα στοιχείο πληροφοριών που δεν είναι άμεσα διαθέσιμο σε phishers. Ορισμένες εταιρείες, για παράδειγμα το PayPal, απευθύνονται πάντα στους πελάτες τους με το όνομα χρήστη τους στα μηνύματα που στέλνουν, οπότε αν ένα email απευθύνεται στον παραλήπτη με γενικό τρόπο ("Αγαπητέ πελάτη του PayPal"), είναι πιθανό να επιχειρηθεί phishing. Επιπλέον, το PayPal προσφέρει διάφορες μεθόδους για τον προσδιορισμό των spoofed emails και συμβουλεύει τους χρήστες να προωθούν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου στον τομέα spoof@PayPal.com για να διερευνήσουν και να προειδοποιήσουν άλλους πελάτες. Ωστόσο, δεν είναι ασφαλής η υπόθεση ότι μόνο η παρουσία προσωπικών πληροφοριών εγγυάται τη νομιμότητα του μηνύματος και ορισμένες μελέτες έχουν δείξει ότι η παρουσία προσωπικών πληροφοριών δεν επηρεάζει σημαντικά το ποσοστό επιτυχίας των επιθέσεων ηλεκτρονικού "ψαρέματος" και υποδηλώνει ότι οι περισσότεροι άνθρωποι δεν δίνουν προσοχή σε τέτοιες λεπτομέρειες.

Τα μηνύματα ηλεκτρονικού ταχυδρομείου από τράπεζες και εταιρείες πιστωτικών καρτών

περιλαμβάνουν συχνά αριθμούς μερικών λογαριασμών. Ωστόσο, πρόσφατη έρευνα έδειξε ότι το κοινό δεν διακρίνει συνήθως τα πρώτα και τα τελευταία ψηφία ενός αριθμού λογαριασμού αφού τα πρώτα ψηφία είναι συχνά τα ίδια για όλους τους πελάτες ενός χρηματοπιστωτικού ιδρύματος .Μια μελέτη σχετικά με την αποτελεσματικότητα πολλών εκπαιδευτικών υλικών κατά του ηλεκτρονικού "ψαρέματος" υποδηλώνει, ότι η εκπαίδευση μείωσε την τάση των χρηστών να εισάγουν πληροφορίες σε ιστοσελίδες ηλεκτρονικού "ψαρέματος" κατά 40%. ωστόσο, ορισμένα από τα εκπαιδευτικά υλικά μείωσαν ελαφρώς την τάση των συμμετεχόντων να κάνουν κλικ σε νόμιμες συνδέσεις (Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, & Lorrie Cranorand Julie Downs, 2010).

Αυτό οδηγεί στην πεποίθηση ότι είναι ύψιστης σημασίας η εύρεση ενός αποτελεσματικού τρόπου εκπαίδευσης ενός μεγάλου μέρους πληθυσμού. (C. Wilson & D. Argles, 2011) Η πρόκληση έγκειται στο να λάβουν την προσοχή του χρήστη στις συμβουλές ασφάλειας.

Υπάρχουν ιστότοποι κατά του ηλεκτρονικού "ψαρέματος" που δημοσιεύουν ακριβή μηνύματα που κυκλοφόρησαν πρόσφατα στο Διαδίκτυο, όπως η FraudWatch International και οι Millersmiles. Τέτοιες τοποθεσίες παρέχουν συχνά συγκεκριμένες λεπτομέρειες σχετικά με τα συγκεκριμένα μηνύματα. Μέχρι το 2007, η υιοθέτηση στρατηγικών κατά του ηλεκτρονικού "ψαρέματος" από τις επιχειρήσεις που χρειάζονται προστασία των προσωπικών και οικονομικών πληροφοριών ήταν χαμηλή. Τώρα υπάρχουν πολλές διαφορετικές τεχνικές για την καταπολέμηση του phishing, συμπεριλαμβανομένης της νομοθεσίας και της τεχνολογίας που δημιουργήθηκαν ειδικά για την προστασία από το ηλεκτρονικό «ψάρεμα». Αυτές οι τεχνικές περιλαμβάνουν βήματα που μπορούν να ληφθούν από άτομα, καθώς και από οργανισμούς.

- **Το μοντέλο πέντε παραγόντων**

Η προσωπικότητα είναι ένα σταθερό πρότυπο για το πώς οι άνθρωποι ανταποκρίνονται στα ερεθίσματα, στο περιβάλλον και τη στάση τους απέναντι σε διαφορετικά γεγονότα. Το μοντέλο πέντε παραγόντων της αξιολόγησης της προσωπικότητας είναι σήμερα ένα από τα πιο διαδεδομένα πολυδιάστατα μέτρα της προσωπικότητας και σκοπός του είναι να ενσαρκώσει την προσωπικότητα σε πέντε ξεχωριστούς παράγοντες που επιτρέπουν μια θεωρητική αντίληψη της προσωπικότητας των ανθρώπων. Αυτές οι διαστάσεις είναι ο νευρωτισμός, η εξωστρέφεια, η δεκτικότητα στην εμπειρία, η συμφωνία και η συνείδηση.

Ένα από τα πιο ευρέως χρησιμοποιούμενα μέτρα αυτού του μοντέλου πέντε παραγόντων αναπτύχθηκε από τους Costa και McCrae και ονομάζεται δοκιμασία NEO-PI FFM.

Πρόκειται για μια σύντομη δοκιμασία 60 ερωτήσεων που επιτρέπει τη σχετικά γρήγορη, αξιόπιστη και ακριβή μέτρηση της προσωπικότητας των συμμετεχόντων σε αυτές τις πέντε κύριες διαστάσεις της προσωπικότητας. Αυτό το μοντέλο θεωρείται ανώτερο από άλλα μοντέλα στη συλλογή των κοινών στοιχείων των χαρακτηριστικών προσωπικότητας και παρέχει μια ακριβή περιγραφή δομής της προσωπικότητας. Μελέτες αποδεικνύουν ότι οι πέντε παράγοντες εκδηλώνονται σε ορισμένα πρότυπα συμπεριφοράς και βρίσκονται σε διαφορετικές ηλικίες, φύλο και φυλετικές ομάδες. Το πλαίσιο έχει προσδιοριστεί ως ένα ισχυρό μοντέλο για την κατανόηση της σχέσης μεταξύ της προσωπικότητας και των διαφόρων ακαδημαϊκών συμπεριφορών.

Ο καθορισμός των παραγόντων προσωπικότητας που συμβάλλουν στην ευπάθεια στις επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing) καθώς και στις απειλές κατά της ιδιωτικής ζωής αποτελεί σημαντικό βήμα για τη βελτίωση της ασφάλειας στο διαδίκτυο. Αυτό μπορεί να βοηθήσει στη δημιουργία προσαρμοσμένων αμυνών για τη μείωση της ευαισθησίας των χρηστών και την προστασία των ατόμων που ενδέχεται να είναι πιο ευάλωτα σε αυτές τις επιθέσεις κατά της ιδιωτικότητας και της ασφάλειας. (D. Querciax and R. Lambiottez and D. Stillwell and M. Kosinskiy and J. Crowcroft,2012)

Ένας ψεύτικος ιστότοπος φαίνεται να είναι παρόμοιος με όλους νόμιμους ιστότοπους σε εμφάνιση και σχεδιασμό. Το μοτίβο διεύθυνσης URL οποιασδήποτε ψεύτικης σελίδας φαίνεται επίσης να είναι παρόμοιο με την πρώτη ματιά. Οι Phishers δοκιμάζουν το καλύτερό τους μοτίβο διευθύνσεων URL σε εμφάνιση, έτσι ώστε όλο και περισσότερα θύματα να προσελκύονται προς την ψεύτικη σελίδα τους χωρίς να γνωρίζουν ότι βρίσκονται υπό επίθεση ηλεκτρονικού "ψαρέματος". Καθώς ολόκληρο το Διαδίκτυο, δεν μπορεί να είναι ελεγχόμενο από την πλευρά του διακομιστή, οι διαθέσιμες λύσεις για την ανίχνευση αυτών των ψεύτικων σελίδων είναι μόνο για την πλευρά του πελάτη. Βάσει αυτών των χαρακτηριστικών, υπάρχουν πολλές λύσεις για την αποφυγή των ιστότοπων ηλεκτρονικού "ψαρέματος", στις ακόλουθες κατηγορίες:

- **Μαύρη λίστα και Λευκή λίστα**

Οι μαύρες λίστες αποτελούνται από διευθύνσεις URL ηλεκτρονικού "ψαρέματος" (phishing) και διευθύνσεις IP που έχουν ανιχνευθεί στο παρελθόν και ενημερώνονται σε συγκεκριμένα χρονικά διαστήματα. Ενώ η λευκή λίστα είναι νόμιμες διευθύνσεις Email ή URL, δεν παρέχει

ασφάλεια κατά όλων των επιθέσεων, καθώς οι νέες διευθύνσεις ή τοποθεσίες δεν μπορούν να ανιχνευθούν. Οι λευκές λίστες χρησιμοποιούνται γενικά για τη μείωση των «false positive» ποσοστών.

Η εφαρμογή API της Google για την ασφαλή περιήγηση, παρέχει τη δυνατότητα στο χρήστη να επαληθεύει εάν μια δεδομένη διεύθυνση URL είναι αποκλεισμένη ή όχι. Η Google παρέχει δύο μαύρες λίστες: "goog-phishshavar" (phishing) και "goog-malware-shavar" (κακόβουλο λογισμικό). Εξουσιοδοτεί τις εφαρμογές της πλευράς του πελάτη να εξετάσουν εάν ένα URL βρίσκεται σε μαύρη λίστα από μια λίστα που ενημερώνεται τακτικά από την Google. Αν και το πρωτόκολλο είναι ακόμα σε πειραματικό στάδιο, διάφοροι φυλλομετρητές το χρησιμοποιούν, όπως το Google Chrome και το Mozilla Firefox.

- **Προγνωστική μαύρη λίστα (phisnet)**

Το PhishNet λύνει το πρόβλημα της ακριβούς αντιστοίχισης (εάν μια διεύθυνση URL είναι ελαφρώς αλλαγμένη έκδοση της μαύρης λίστας, τότε παραμένει μη εντοπισμένη). Παράγει όλες τις πιθανές παραλλαγές ενός δεδομένου URL χρησιμοποιώντας πέντε χαρακτηριστικά:

- Ομοιότητα δομής καταλόγου
- Ομοιότητα διεύθυνσης IP
- Αντικατάσταση συμβολοσειράς
- Ίδια εμπορική ονομασία
- Αυτοματοποιημένη λευκή λίστα

Ο αυτοματοποιημένος κατάλογος λευκής λίστας (AIWL), περιέχει μια λίστα ιστότοπων με ευρετήρια, στα οποία οι χρήστες έχουν καταχωρήσει οποιοδήποτε είδος ευαίσθητων δεδομένων που αναφέρονται ως χαρακτηριστικά διεπαφών χρήστη με έμπιστες συνδέσεις. Το Bayes classifier χρησιμοποιεί ένα διάνυσμα χαρακτηριστικών που βασίζεται σε επιτυχείς ή αποτυχημένες προσπάθειες σύνδεσης και στη συνέχεια κατασκευάζει ένα μοντέλο για τον υπολογισμό της πιθανότητας οποιονδήποτε μελλοντικών προσπαθειών σύνδεσης, με βάση προκαθορισμένα όρια. Οι ευρετικές μέθοδοι αναφέρονται σε σύνολο κανόνων που βασίζεται σε προηγούμενα αποτελέσματα και εμπειρίες, για την επίλυση ενός προβλήματος ή για μαθησιακούς σκοπούς.

- **SPF**

Το Sender Policy Framework (SPF) είναι ένα ανοικτό πρότυπο που καθορίζει μια τεχνική μέθοδο για την πρόληψη της πλαστογράφησης της διεύθυνσης αποστολέα. (Julian Mehnle) Δεδομένου ότι οι περισσότεροι διακομιστές SMTP παρέχουν αμοιβαία διευθυνσιοδότηση TCP στους κεντρικούς υπολογιστές στο Internet, μπορούν να δουν τη διεύθυνση IP του αποστολέα. Το SPFv1 προστατεύει τη διεύθυνση αποστολέα φακέλου, μέσα από την επαλήθευση των διευθύνσεων IP του αποστολέα και εξουσιοδοτεί τον κάτοχο ενός domain να καθορίσει μια λίστα διευθύνσεων IP που επιτρέπεται να στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου από το domain τους και να δημοσιεύουν αυτές τις πληροφορίες στις περιοχές της Ζώνη DNS του domain. Ένας διακομιστής λήψης μπορεί να ρωτήσει το DNS για να ελέγξει αν το μήνυμα προέρχεται από ένα από εκείνες τις διευθύνσεις που έχουν κατατεθεί σε λίστες.

5. Τεχνικές αντιμετώπισης του phishing

Παρά το γεγονός ότι είναι μια από τις παλαιότερες επιθέσεις στον κυβερνοχώρο, το phishing παραμένει τόσο δημοφιλές, επειδή είναι ένα εξαιρετικά αποτελεσματικό μέσο εκμετάλλευσης του πιο αδύναμου συνδέσμου στην ασφάλεια του άνθρωπου. Περεταίρω οι hackers έχουν γίνει πιο εξειδικευμένοι στις τεχνικές τους και οι επιθέσεις ηλεκτρονικού "ψαρέματος" είναι τώρα πολύ στοχοθετημένες, δυναμικές και "υπερμορφικές", καθιστώντας τες όλο και πιο δύσκολες τόσο στον άνθρωπο όσο και στις μηχανές για να τις εντοπίσουν.

Αξίζει να σημειωθεί ότι οι τεχνικές ηλεκτρονικού "ψαρέματος" σε κινητές εφαρμογές μπορούν να γίνουν μέσω ενός προγράμματος περιήγησης στο Web ή χρησιμοποιώντας μια συγκεκριμένη σελίδα σύνδεσης για μια εφαρμογή για κινητά. Η τεχνική κατά του ηλεκτρονικού "ψαρέματος" πρέπει να είναι σε θέση να ανιχνεύει επιθέσεις phishing μέσω προγραμμάτων περιήγησης ή εφαρμογών. Οι μαύρες και οι λευκές λίστες συγκρίνουν την απαιτούμενη διεύθυνση URL με μια λίστα διευθύνσεων URL ηλεκτρονικού "ψαρέματος" (phishing). Προτείνεται μια μέθοδος που βασίζεται στην κατοχή των εγγεγραμμένων χρηστών σε έναν ιστότοπο, ο οποίος αργότερα δημιουργεί έναν μοναδικό κώδικα για κάθε χρήστη. Ο χρήστης καλείται να εισαγάγει μερικά ψηφία του μοναδικού του κωδικού του και ο ιστότοπος πρέπει να απαντήσει με τον πλήρη κωδικό. Ο σωστός κωδικός σημαίνει ότι ο ιστότοπος είναι γνήσιος. Αυτή η μέθοδος απαιτεί από τους χρήστες να εγγραφούν και να θυμούνται τον κώδικα τους για διαφορετικούς ιστοτόπους, έπειτα μόλις τεθεί σε κίνδυνο ο κώδικας, το phishing θα ξεκινήσει εύκολα.

Απαιτείται λεπτομερειακός υπολογισμός για την εξαγωγή κειμένου, εικόνας και χρωμάτων ενός δικτυακού τόπου με την μέθοδο που χρησιμοποιεί για την εξαγωγή του στιγμιότυπου οθόνης για να υπολογίσει τις οπτικές ομοιότητες. Προτείνεται μια μέτρηση που ονομάζεται ποσοστό εξαπάτησης για τον υπολογισμό της ομοιότητας. Η μέθοδος χρησιμοποιείται για τις σύνδεσης των εφαρμογών για κινητά και δεν λειτουργεί για τις συνδέσεις ιστού. Προτείνεται η μέθοδος Bayesian, που βασίζεται στην οικοδόμηση ενός μαθησιακού μοντέλου και στηρίζεται στη συλλογή δεδομένων σχετικά με τα δικαιώματα αλλά και τα βασικά αρχεία καταγραφής. Ωστόσο, το σύστημα αυτό απαιτεί αναβαθμίσεις όσον αφορά τη μνήμη και το σχέδιο ελέγχου του.

- **Ανίχνευση κακόβουλου λογισμικού με προϊόντα ασφάλειας πελατών**

Τα προϊόντα ασφάλειας πελατών είναι ευρέως αναπτυγμένα. Το Microsoft Update ωθεί επίσης το «Malicious Software Removal Tool» μηνιαίως, που είναι ένας ελαφρύς σαρωτής κακόβουλου λογισμικού. Ωστόσο, δεν είναι πάντα αποτελεσματικό. Είναι εύκολο να τροποποιηθεί ένα πρόγραμμα έτσι ώστε να μην περιέχει οποιαδήποτε γνωστή υπογραφή, για να παρακάμψει την ανίχνευση στην οποία βασίζεται. Υπάρχουν επίσης τεχνικές για την παράκαμψη ορισμένων ανιχνεύσεων που βασίζονται στη συμπεριφορά.

Το Avast Free Antivirus, προσφέρει δωρεάν ασφάλεια και προστασία σε πραγματικό χρόνο. Παρέχει έξυπνη ανίχνευση απειλών και ασφάλεια για το δίκτυο, τους κωδικούς και το φυλλομετρητή.

- Μπλοκάρει και εντοπίζει τους ιούς και το κακόβουλο λογισμικό όπως ransomware και άλλες απειλές.
- Παρέχει ασφάλεια του Wi-Fi, εντοπίζει τους εισβολείς και τα κενά ασφαλείας του δικτύου.
- Θωρακίζει τους κωδικούς πρόσβασης κλειδώνοντας τους, σε μία ασφαλή θυρίδα.

Το SUPERAntiSpyware ειδικεύεται σε μοναδικά και κακόβουλα προγράμματα που είναι δύσκολο να εντοπιστούν, εντοπίζοντας και αφαιρώντας περιπτώσεις κακόβουλων απειλών, όπως:

- Malware
- Spyware
- Adware
- Trojans
- Worms
- Keyloggers
- Hijackers
- Rootkits

Ø Προστασία του e-banking

Τα χρηματοπιστωτικά ιδρύματα, είναι οι πιο συνηθισμένοι στόχοι του phishing, που διανέμουν προγράμματα ασφαλείας για προστασία των πελατών τους. Έρχονται συνήθως με τη μορφή προγραμμάτων ή σαν πρόσθετα προγράμματος περιήγησης. Αυτά τα προγράμματα μπορούν να προστατεύσουν τους πελάτες με έναν ή περισσότερους τρόπους:

I. Εφαρμόζουν έναν ασφαλή έλεγχο εισαγωγής κειμένου, έτσι ώστε τα keyloggers να μην μπορούν να παρεμποδίσουν τις πληκτρολογήσεις ή να διαβάσουν περιεχόμενά.

II. Κρυπτογραφούν σημαντικές πληροφορίες στη μνήμη και στο δίκτυο

III. Μπλοκάρουν ή καταργούν γνωστό κακόβουλο λογισμικό

IV. Επαληθεύουν το πιστοποιητικό του οικονομικού ιδρύματος, για να το προστατεύουν από τις επιθέσεις "Man In The Middle"

V. Χρησιμοποιούν tokens ή έξυπνες κάρτες

Μερικοί από αυτούς τους τρόπους προστασίας είναι αρκετά αποτελεσματικοί αλλά όχι τέλειοι:

Όπως σε κάθε άλλο πρόγραμμα, ενδέχεται να υπάρχουν τρωτά σημεία σε αυτά τα προγράμματα ασφαλείας. (luoposhusheng, 2011)

Τα κακόβουλα πρόγραμμα μπορεί να αποκρύψουν τη διεπαφή χρήστη του προγράμματος ασφαλείας και να εμφανίσουν ένα ψεύτικο περιβάλλον εργασίας χρήστη.

- **Ομάδες κατά της απάτης**

Το PhishTank, το οποίο ξεκίνησε τον Οκτώβριο του 2006, είναι ένα συνεργατικό κέντρο εκκαθάρισης δεδομένων και πληροφοριών σχετικά με το ηλεκτρονικό «ψάρεμα» στο διαδίκτυο. Το PhishTank χρησιμοποιεί ένα εξελιγμένο σύστημα ψηφοφορίας που απαιτεί η κοινότητα να ψηφίσει “phish” ή “not phish”, μειώνοντας την πιθανότητα false positives και βελτιώνοντας το συνολικό εύρος και την κάλυψη των δεδομένων ηλεκτρονικού "ψαρέματος". Παρέχει επίσης ένα ανοικτό API για τους προγραμματιστές και για τους ερευνητές να ενσωματώσουν τα δεδομένα κατά του ηλεκτρονικού "ψαρέματος" στις εφαρμογές τους χωρίς χρέωση. Το PhishTank υποστηρίζεται από το OpenDNS, έναν δημόσιο ανιχνευτή DNS. Το OpenDNS χρησιμοποιεί δεδομένα PhishTank για την αποτροπή phishing επιθέσεων στους χρήστες του.

Το 2003 Δημιουργήθηκε η Ομάδα Anti-Phishing Working Group (APWG) είναι μια διεθνής κοινοπραξία που έχει φέρει τις επιχειρήσεις σε επαφή με επιθέσεις ηλεκτρονικού "ψαρέματος", προϊόντα ασφαλείας και εταιρείες παροχής υπηρεσιών, υπηρεσίες επιβολής του

νόμου, κυβερνητικές υπηρεσίες, εμπορικές ενώσεις, οργανισμούς περιφερειακών διεθνών συνθηκών και εταιρειών επικοινωνιών.

Η FraudWatch International, μια ιδιωτική εταιρεία ασφάλειας Internet που ιδρύθηκε το 2003, παρέχει μια ποικιλία προϊόντων και υπηρεσιών κατά του ηλεκτρονικού "ψαρέματος" (phishing) για την προστασία των χρηματικών υπηρεσιών, του ηλεκτρονικού εμπορίου, και των εταιρειών φιλοξενίας στο διαδίκτυο από phishing.

6. Παρουσίαση Ιστότοπου

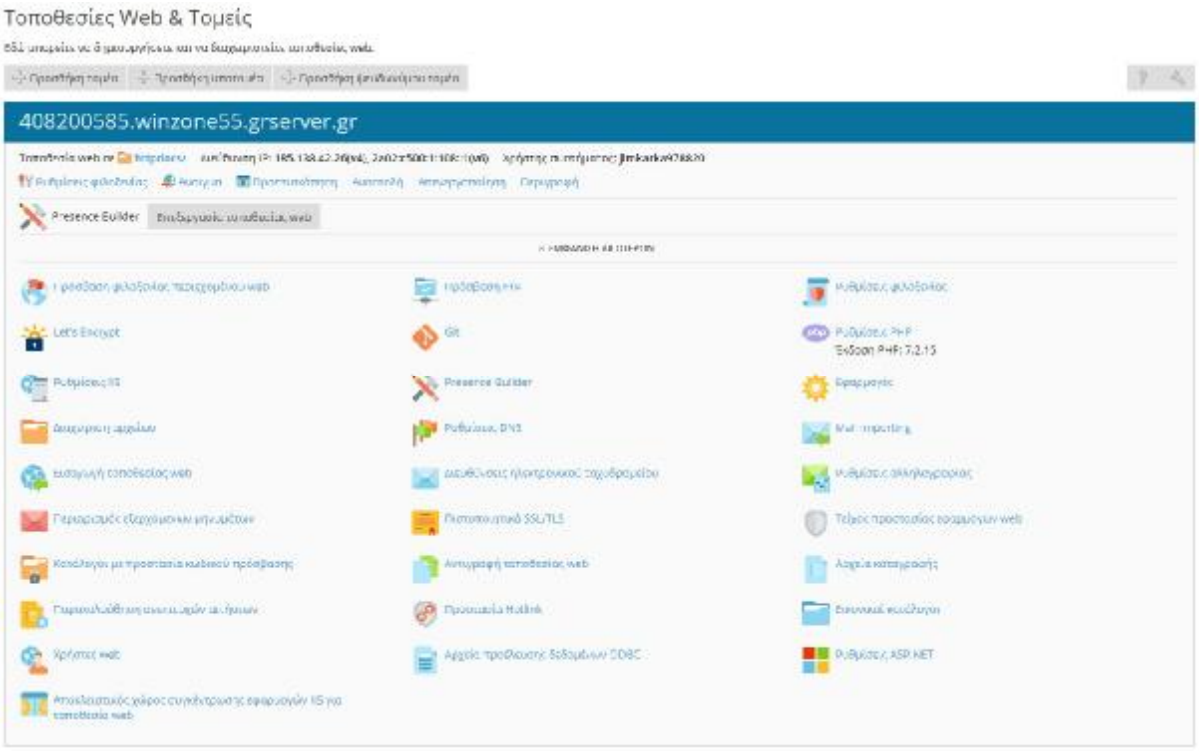
Το Διαδίκτυο διαδραματίζει σημαντικό ρόλο στην επικοινωνία μεταξύ των ανθρώπων και είναι επίσης ένα σημαντικό εταιρικό εργαλείο. Η σημασία του είναι τόσο σημαντική που η παρουσία στο διαδίκτυο θεωρείται στρατηγικό ζήτημα. Όμως, η σημασία της αισθητικής συχνά ξεχνιέται, εφόσον οι προσεγγίσεις που βασίζονται στην επικοινωνία, τη χρηστικότητα και την τεχνική θεωρούνται πιο ρεαλιστικές. Το περιεχόμενο που υπάρχει σε μία ιστοσελίδα είναι υψίστης σημασίας, αλλά για να εξασφαλίσουμε την υπεροχή της, πρέπει να παρουσιάσουμε το περιεχόμενο με τρόπο ελκυστικό, εύχρηστο και όσο πιο δυνατόν πρωτότυπο. Σε αυτό το πλαίσιο υποδεικνύεται η σημασία των αρχών σχεδιασμού των ιστοσελίδων, και συγκεκριμένα στη διάταξη σχεδίασης της σελίδας, έχοντας ως κύρια αναφορά την έννοια της χρηστικότητας.

6.1. Δημιουργία Website

6.1.1. ΔΗΜΙΟΥΡΓΙΑ ΘΕΣΗΣ ΣΤΟΝ SERVER

- Η εικόνα 13 δείχνει την δημιουργία μιας θέσης σε server.

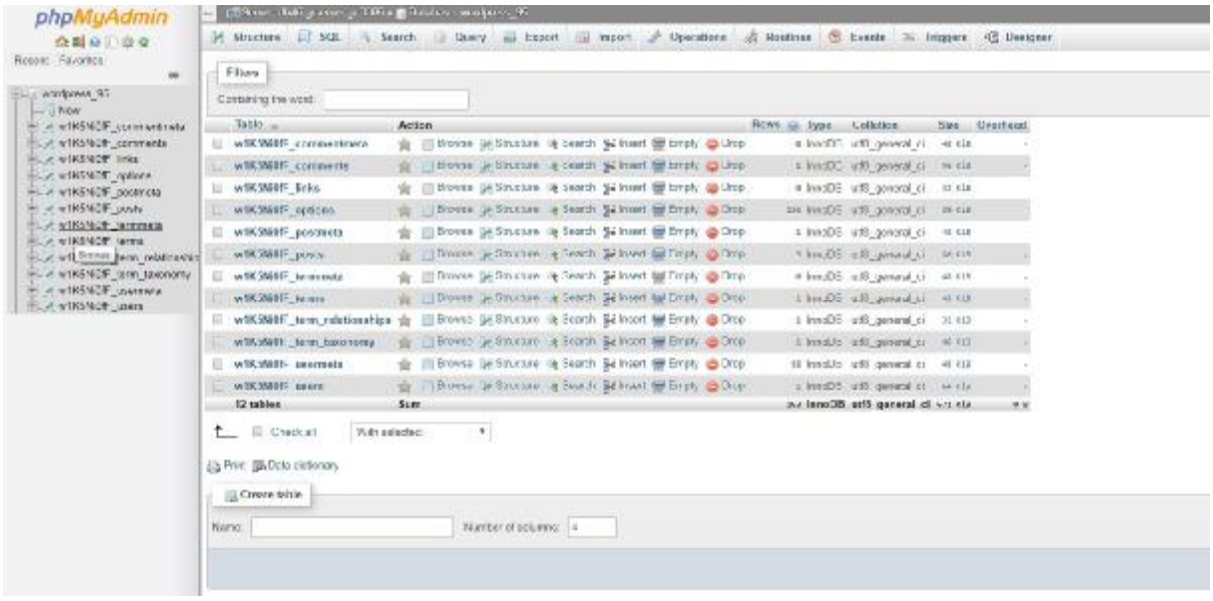
Εικόνα 13. Δημιουργία μιας θέσης σε server



6.1.2. ΔΗΜΙΟΥΡΓΙΑ ΒΑΣΗΣ ΣΤΟ MYSQL

- Η εικόνα 14 δείχνει την δημιουργία μιας Βάσης δεδομένων (MySQL).

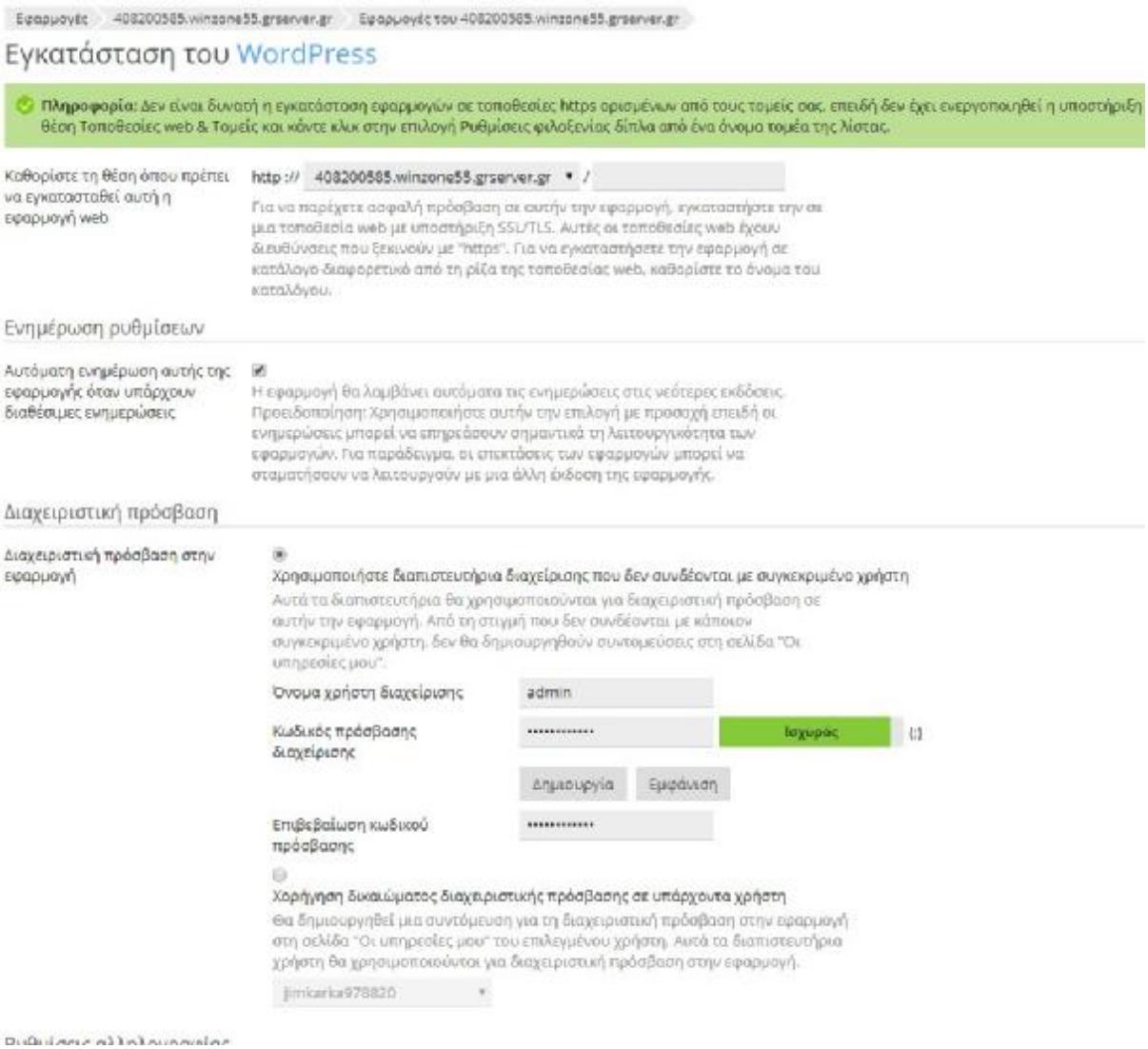
Εικόνα 14. Δημιουργία μιας Βάσης δεδομένων



6.1.3. ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ WORDPRESS

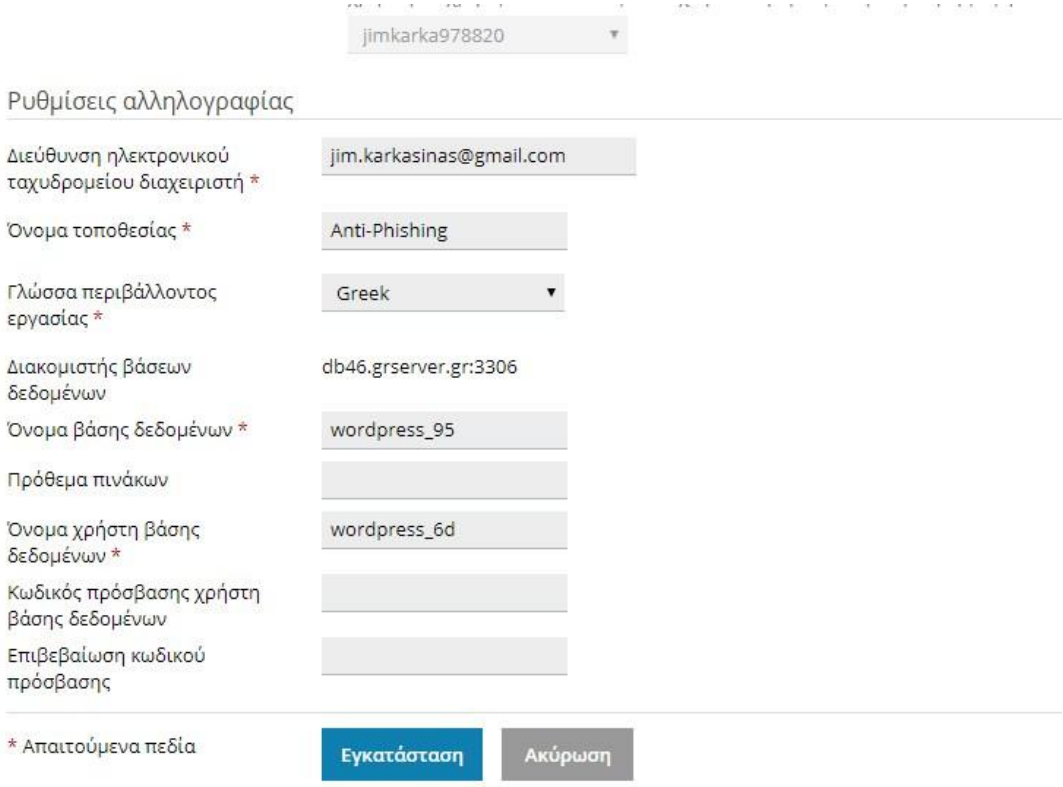
- Στην εικόνα 15 φαίνεται η εγκατάσταση του wordpress στην θέση server "https://408200585.winzone55.grserver.gr", μαζί με την δημιουργία χρήστη / κωδικό διαχειριστή για το wordpress.

Εικόνα 15. Εγκατάσταση του wordpress



- Στην εικόνα 16 παρουσιάζεται η σύνδεση της βάσης δεδομένων του MySQL στην θέση server "https://408200585.winzone55.grserver.gr" και η ονομασία της ιστοσελίδας

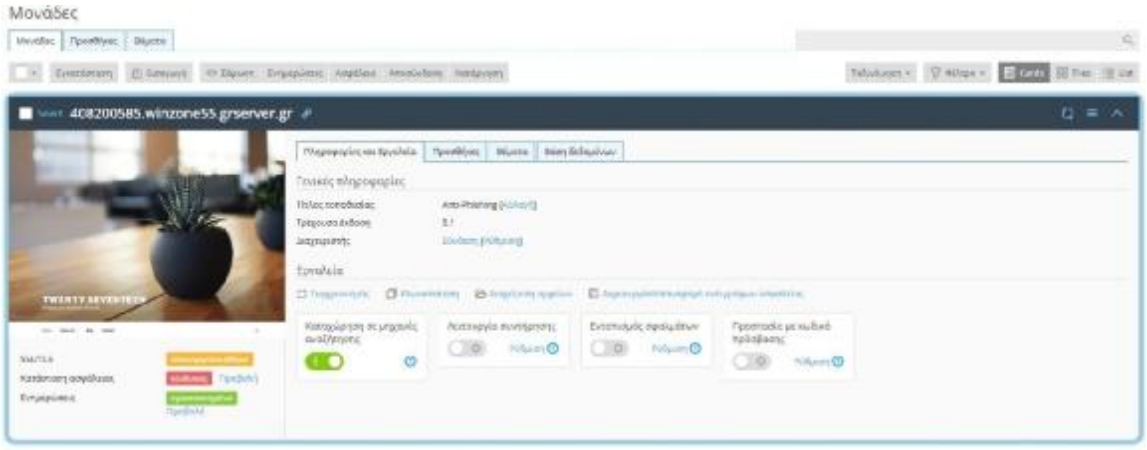
Εικόνα 16. Σύνδεση της βάσης δεδομένων



.

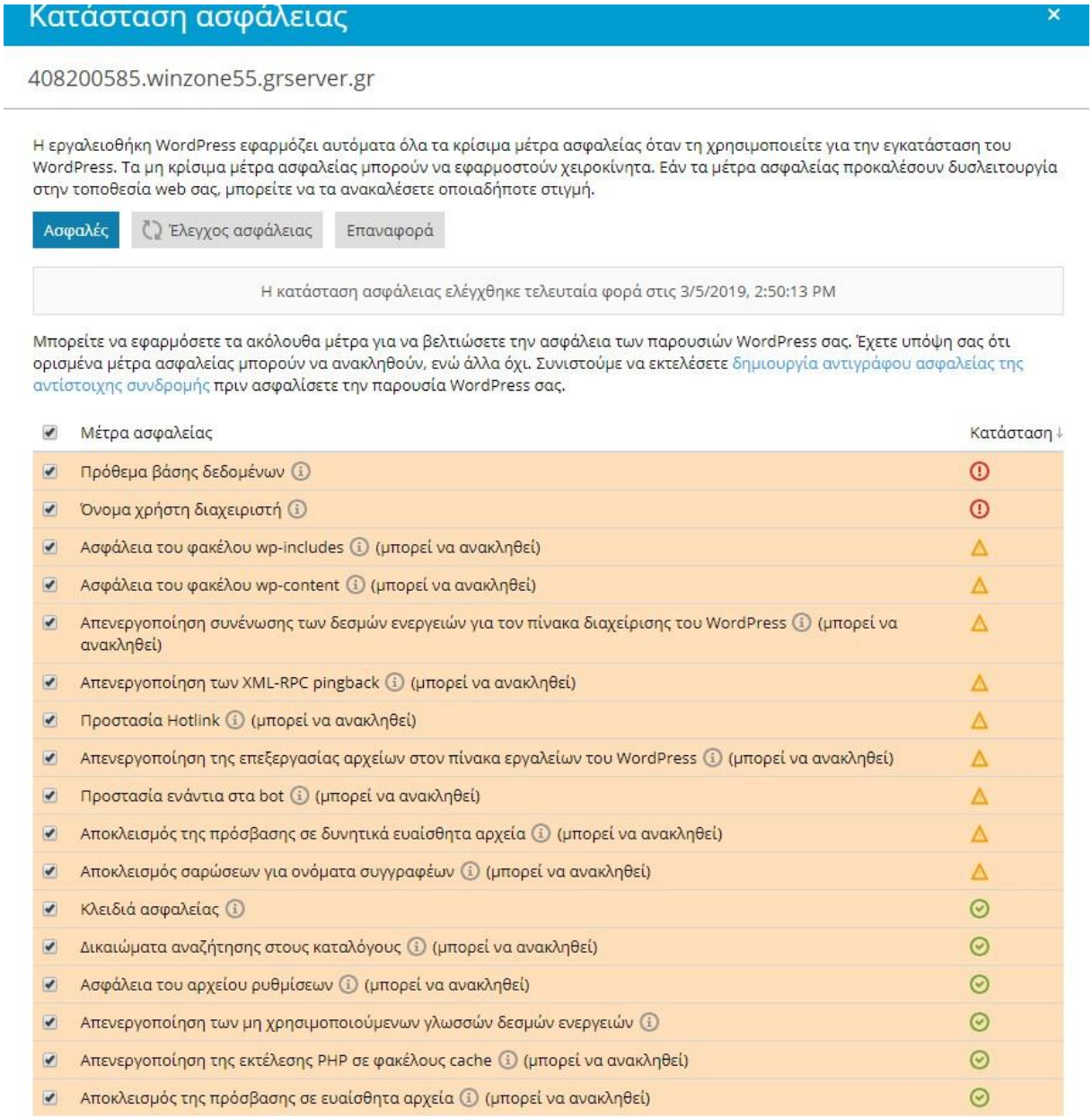
- Στην εικόνα 17 απεικονίζεται η ολοκλήρωση της εγκατάστασης στην θέση "https://408200585.winzone55.grserver.gr".

Εικόνα 17. Ολοκλήρωση της εγκατάστασης



Ø Στην εικόνα 18 ενεργοποιούνται τα μέτρα ασφάλειας (Πρόθεμα βάσης δεδομένων, όνομα χρήστη διαχειριστή, κτλπ.) για την ιστοσελίδα .

Εικόνα 18. Ενεργοποίηση μέτρων ασφάλειας



6.1.4. ΑΓΟΡΑ - ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ TEMPLATE STOIC

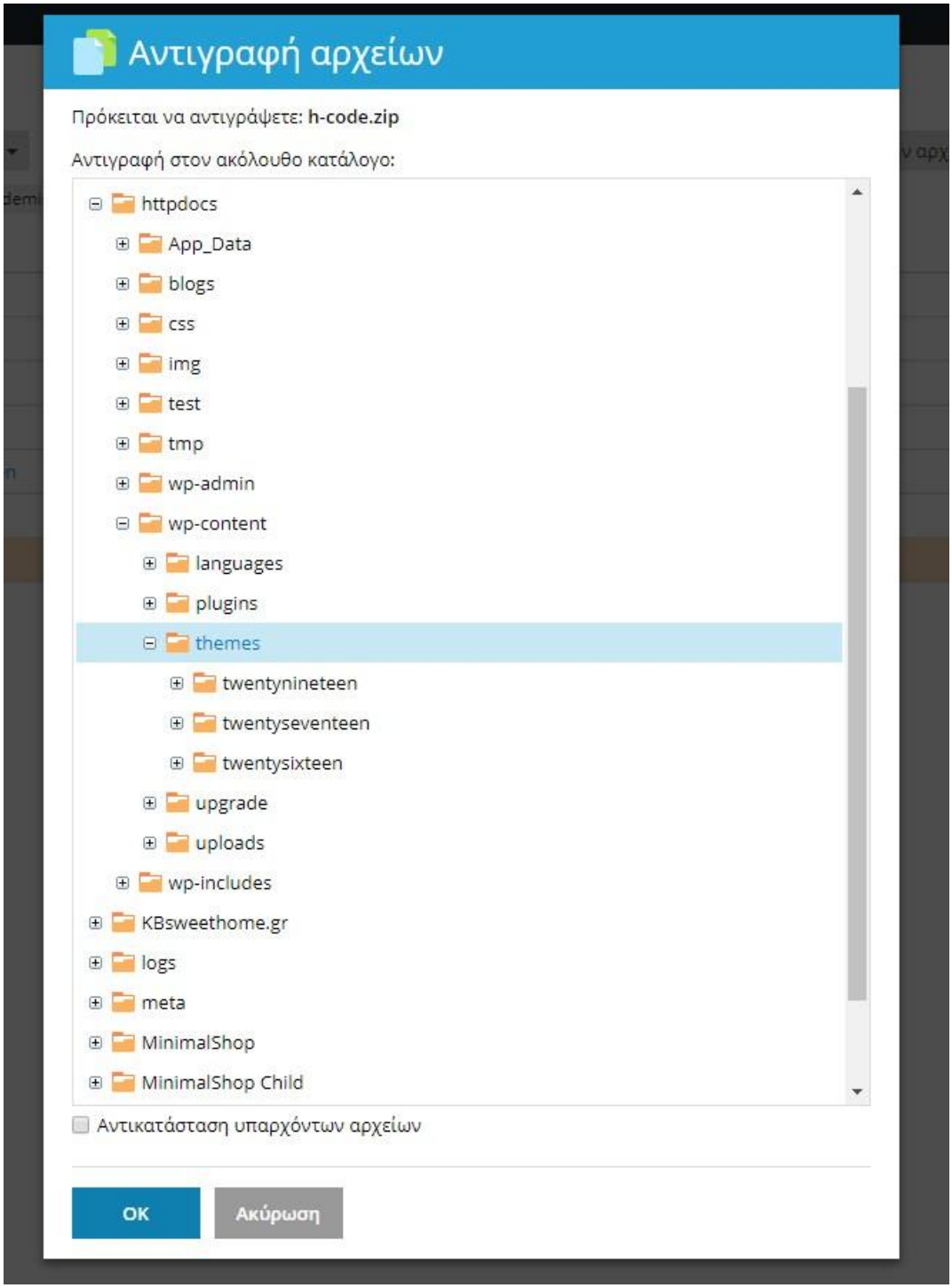
- Στην εικόνα 19 φαίνεται η αγορά του θέματος template (https://themeforest.net/item/stoic-multipurpose-responsive-wordpress-theme/19423429?s_rank=1) ENVATOMARKET

.

Εικόνα 19. Αγορά του θέματος

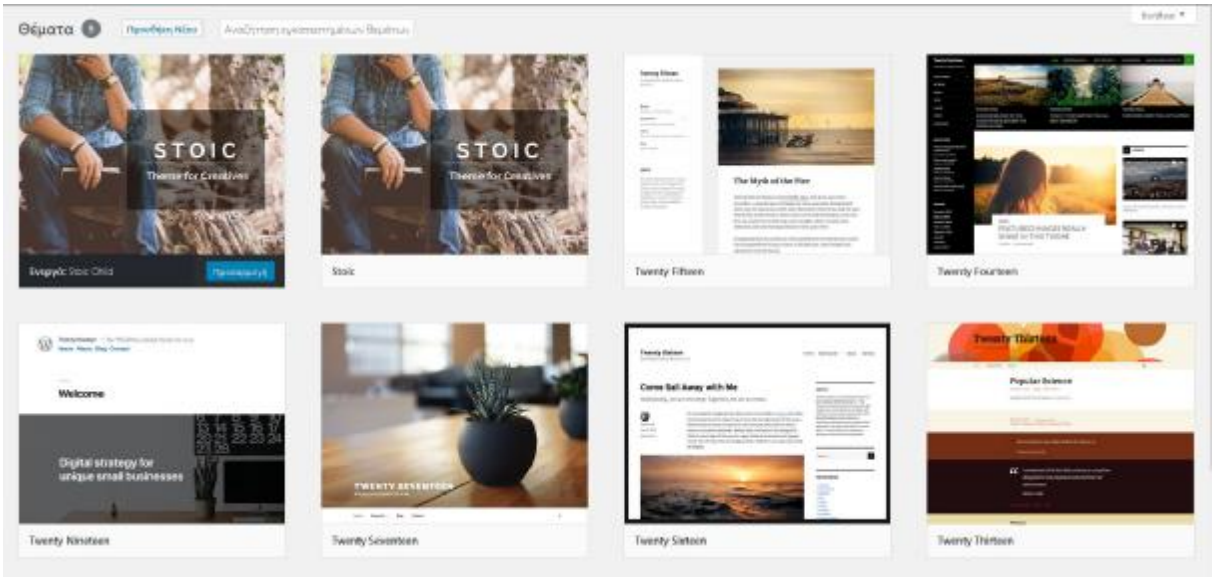
Ø Στην εικόνα 20 απεικονίζεται η αποσυμπίεση στην διαδρομή: https://winzone55.grserver.gr:8443/smb/file-manager/list/htdocs/wordpress/wp-content/themes/stoic

Εικόνα 20. Αποσυμπιέση αρχείων



Ø Στην εικόνα 21 απεικονίζεται η ενεργοποίηση του θέματος (Stoic).

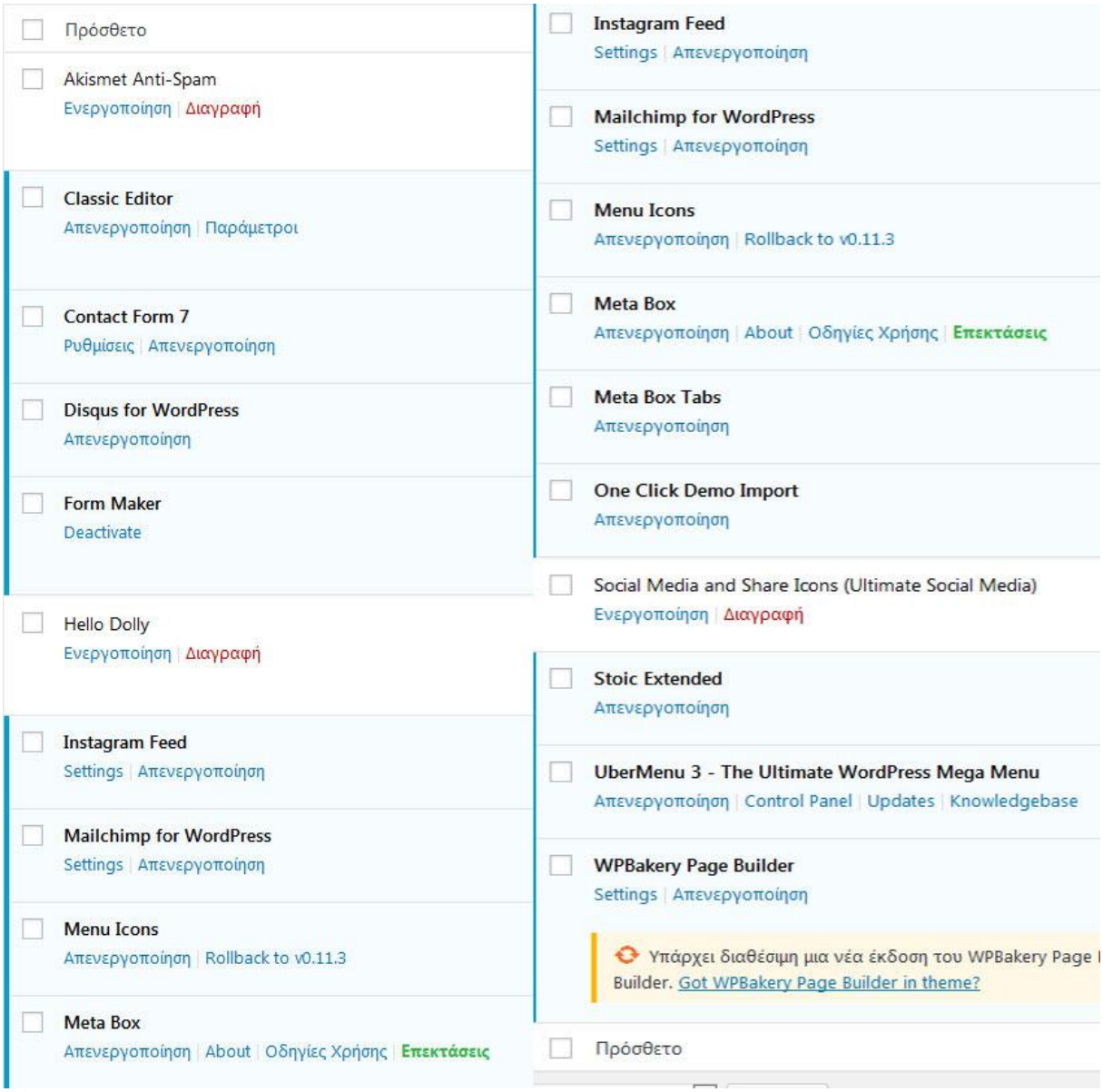
Εικόνα 21. ενεργοποίηση του θέματος



6.1.5 ΕΓΚΑΤΑΣΤΑΣΗ PLUGINS (ΠΡΟΣΘΕΤΑ) ΤΟΥ TEMPLATE (ΘΕΜΑ)

- Στην εικόνα 22 φαίνονται τα εγκατεστημένα και ενεργοποιημένα τα πρόσθετα που χρησιμεύουν στην εμφάνιση και στην λειτουργιά της ιστοσελίδας.

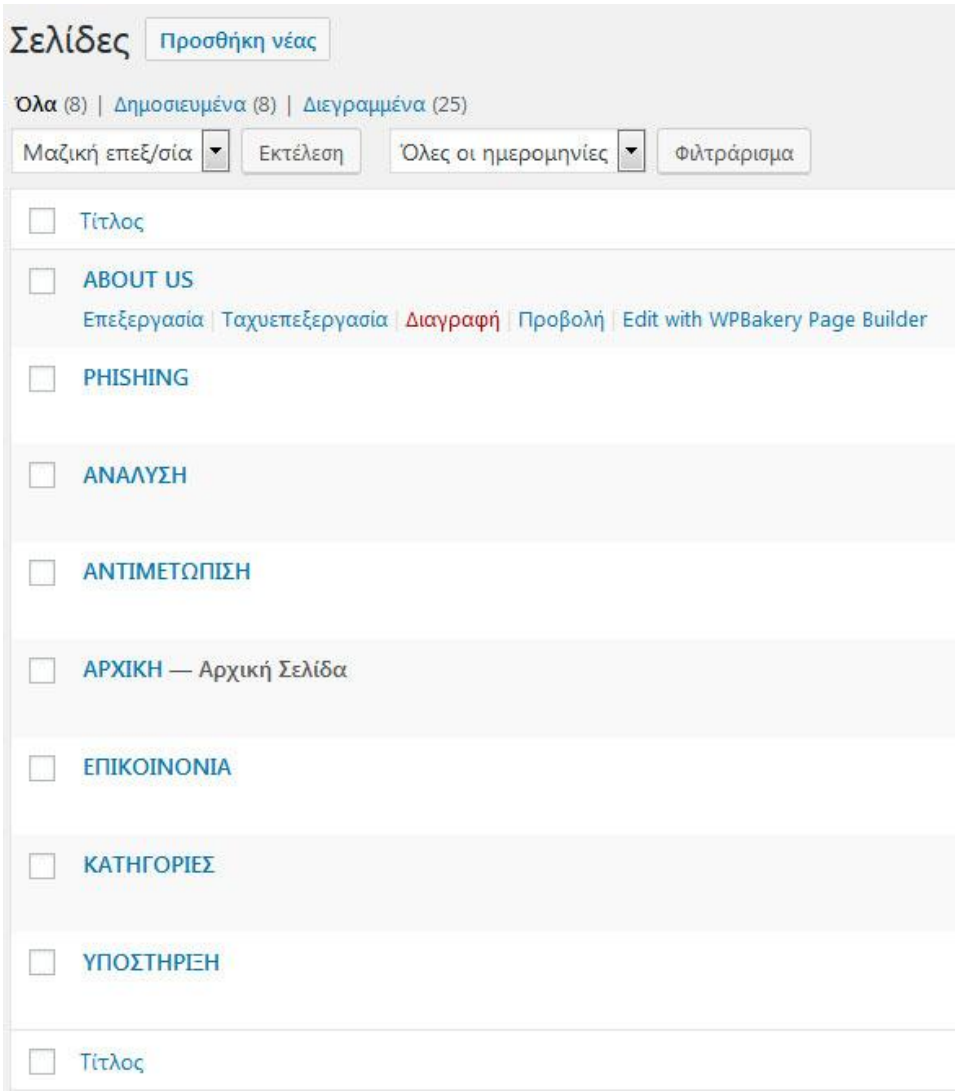
Εικόνα 22.



6.1.6 ΔΗΜΙΟΥΡΓΙΑ 8 ΣΕΛΙΔΩΝ/ΥΠΟΣΕΛΙΔΩΝ & 1 ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ, ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΙ ΔΗΜΟΣΙΕΥΣΗ ΣΕΛΙΔΩΝ

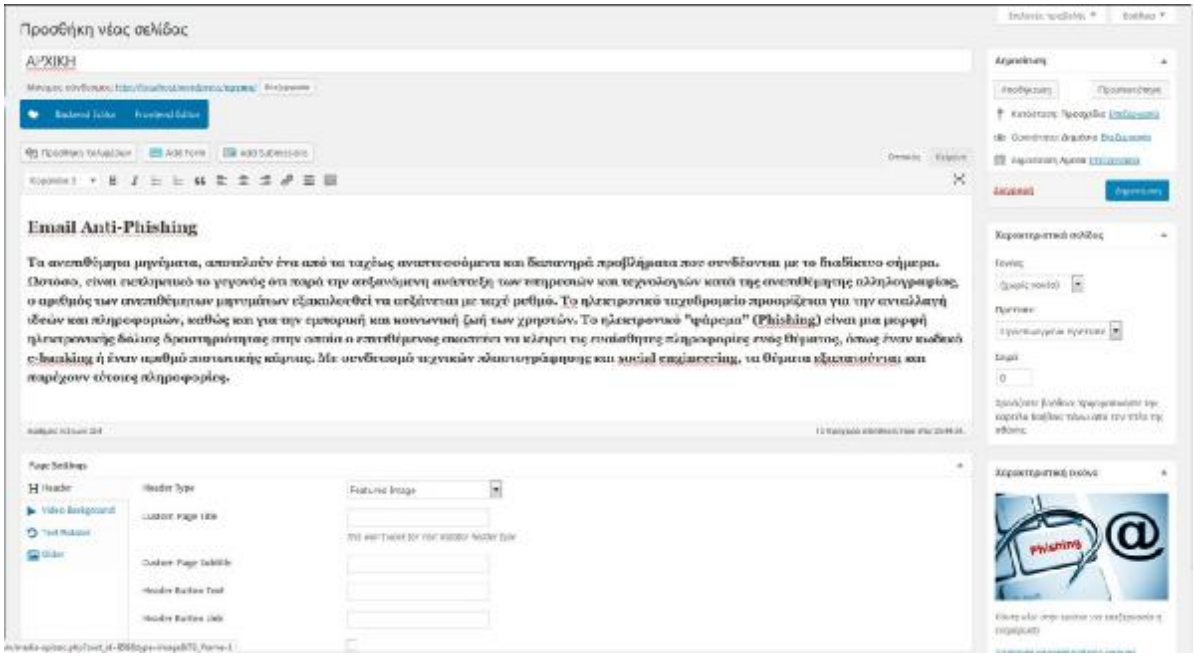
- Στην εικόνα 23 απεικονίζονται οι σελίδες / υποσελίδες που δημιουργήθηκαν για την προσθήκη του περιεχομένου της ιστοσελίδας.

Εικόνα 23. Σελίδες / υποσελίδες που δημιουργήθηκαν



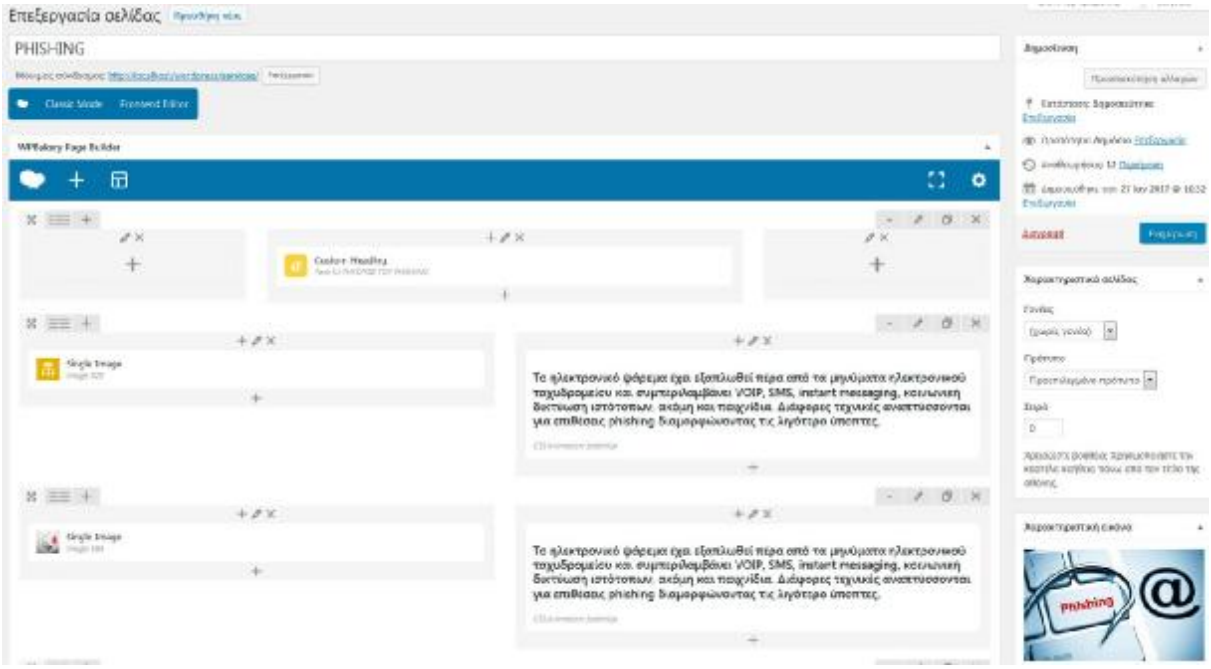
Ø Στην εικόνα 24 φαίνεται η αρχική σελίδα.

Εικόνα 24. Δημιουργία της αρχικής σελίδας



Ø Στην εικόνα 25 παρατηρείται η επεξεργασία μια σελίδας σε λειτουργία "backend editor"

Εικόνα 25.

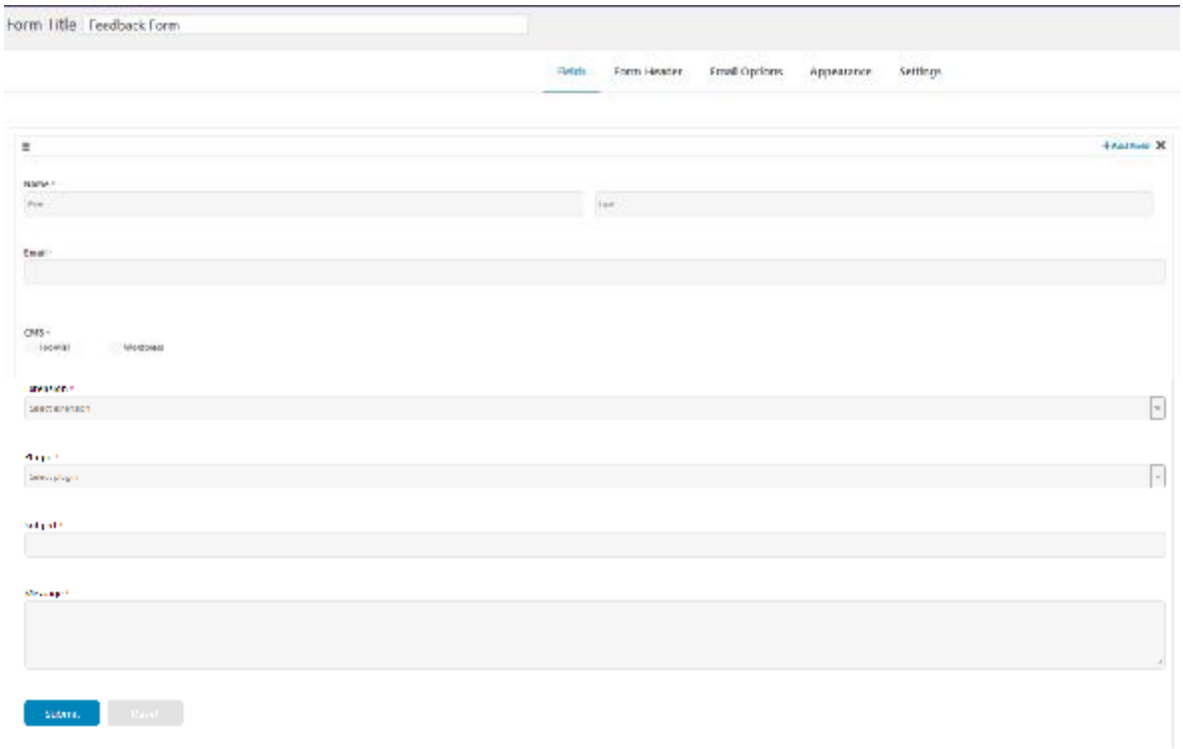


Στην εικόνα 26 παρατηρείται η επεξεργασία μια σελίδας σε λειτουργία προσαρμογής.

Εικόνα 26.

Ø Στην εικόνα 27 απεικονίζεται το ερωτηματολόγιο που χρησιμοποιείται για την συλλογή πληροφοριών των επισκεπτών, για την καλύτερη εξατομίκευση του phishing της ιστοσελίδας.

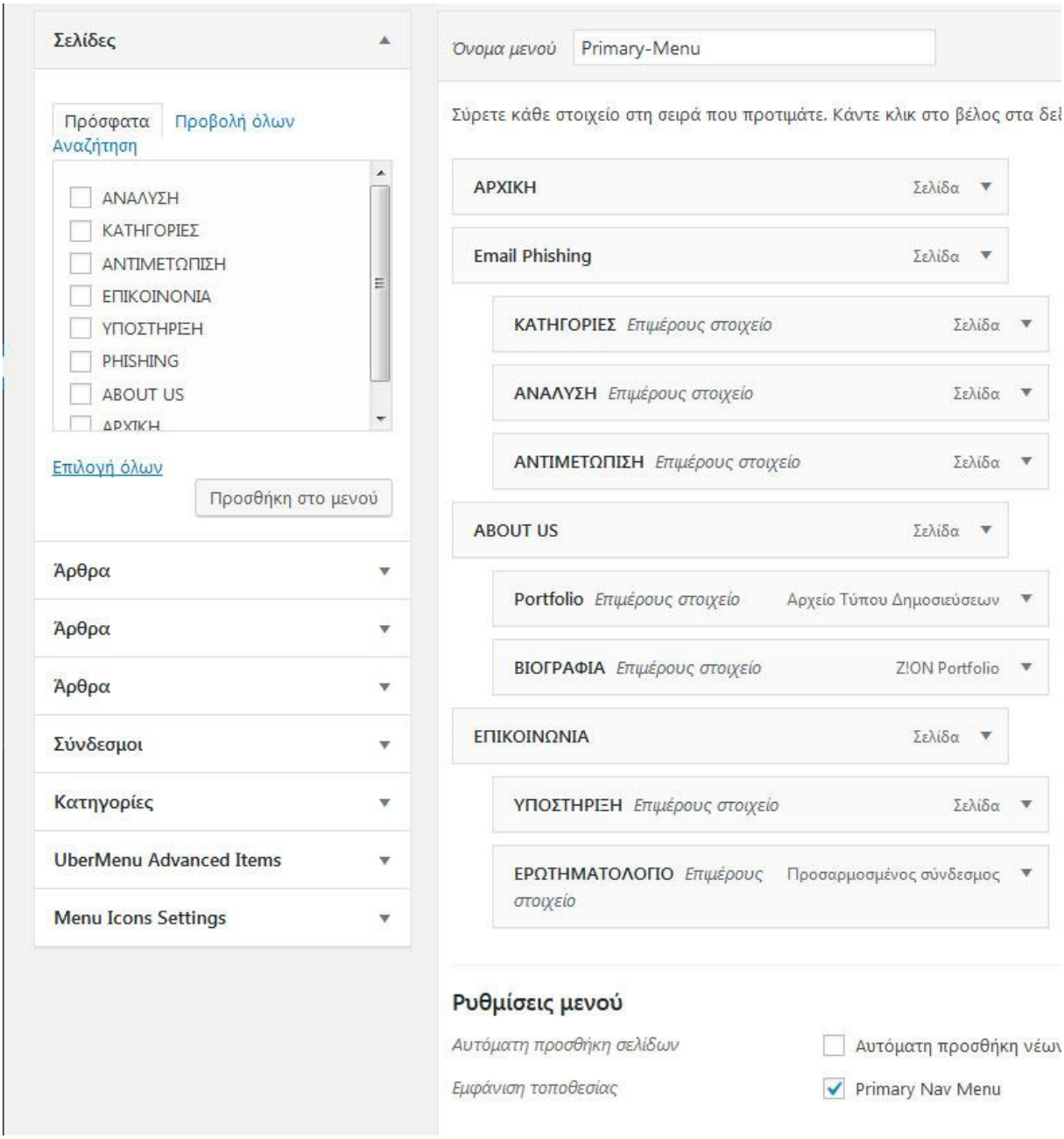
Εικόνα 27. Ερωτηματολόγιο που χρησιμοποιείται για συλλογή πληροφοριών.



6.1.7. ΔΗΜΙΟΥΡΓΙΑ ΜΕΝΟΥ

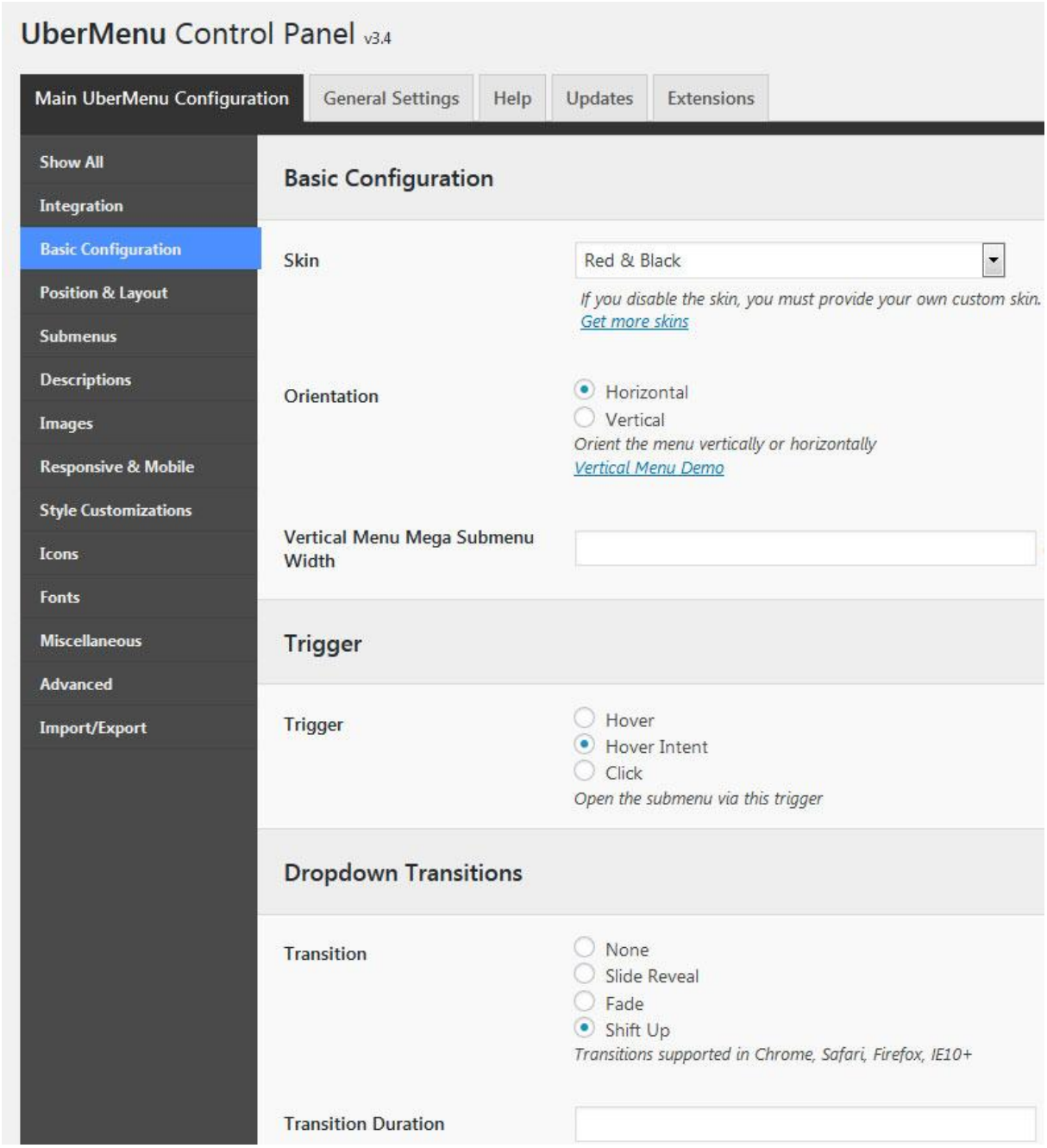
- Στην εικόνα 28 παρατηρείται το μενού που δημιουργήθηκε για την πλοήγηση στο περιεχόμενο της ιστοσελίδας.

Εικόνα 28. Μενού πλοήγησης του περιεχομένου της ιστοσελίδας.



Ø Στην εικόνα 29 φαίνεται η προσαρμογή της εμφάνισης του μενού της ιστοσελίδας.

Εικόνα 29. Προσαρμογή εμφάνισης του μενού



7. Έρευνα

Διεξήχθη μία έρευνα με σκοπό να καταδειχθεί η επίδραση του phishing στους καθημερινούς χρήστες του διαδικτύου. Για την έρευνα αυτή χρησιμοποιήθηκε ένα ερωτηματολόγιο.

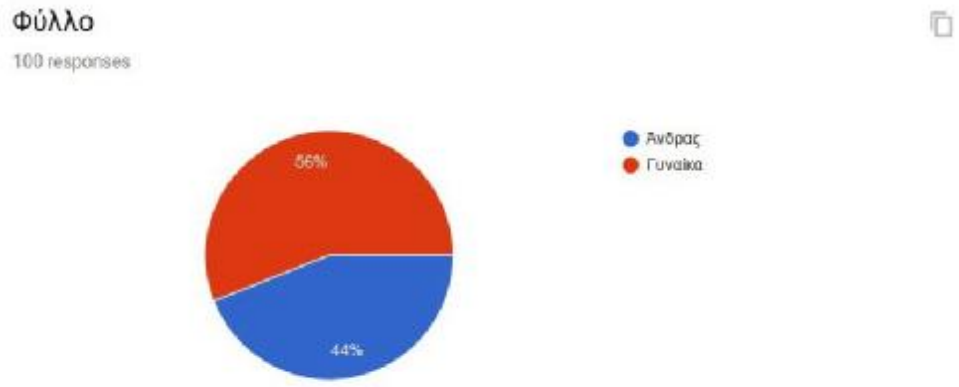
7.1 Υλικό και Μέθοδοι

Η έρευνα απευθύνθηκε σε 100 άτομα. Το ερωτηματολόγιο που δημιουργήθηκε αποστάλθηκε στους χρήστες μέσω της κοινωνικής δικτύωσης. Το σύνολο των ερωτήσεων είναι 15. Οι πρώτες 5 ερωτήσεις αφορούν γενικά δημογραφικά στοιχεία. Ενώ οι υπόλοιπες απευθύνονται στην προσωπική εμπειρία που έχει ο κάθε χρήστης από το phishing και πως το αντιμετώπισε. Τα αποτελέσματα των απαντήσεων καταγράφηκαν και αναλύθηκαν με τη χρήση της περιγραφικής στατιστικής.

7.2 Αποτελέσματα

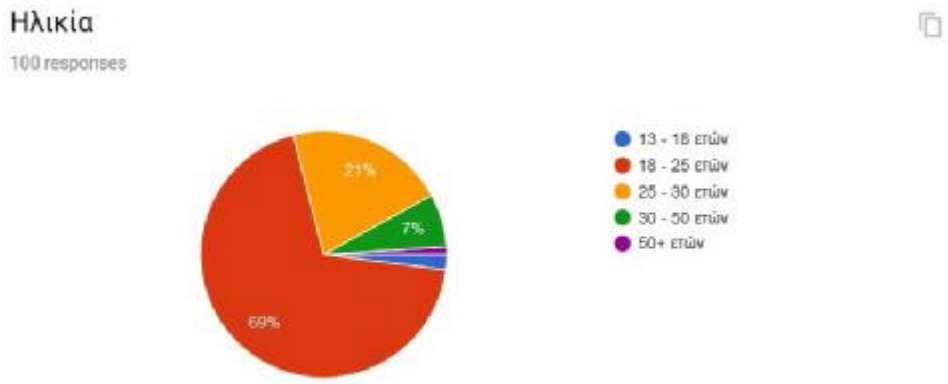
Στην εικόνα 30 φαίνεται ότι οι άνδρες που απάντησαν στην έρευνα είναι το 44% και οι γυναίκες το 56% του συνολικού δείγματος των 100 ατόμων.

Εικόνα 30. Απάντηση ερωτηματολογίου 1.



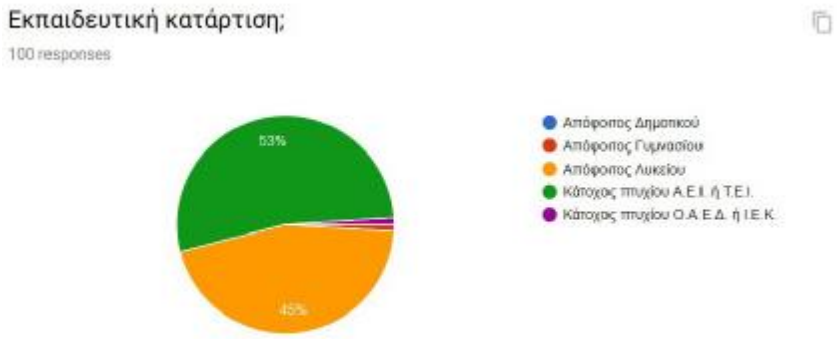
Στην εικόνα 31 φαίνεται ότι το 69% των ατόμων που απάντησαν βρίσκονται σε ηλικία από 18 έως 25 ετών, το 21% είναι άτομα ηλικίας από 25 έως 30 ετών και το 7% είναι άτομα ηλικίας από 30 έως 50 ετών του συνολικού δείγματος των 100 ατόμων.

Εικόνα 31. Απάντηση ερωτηματολογίου 2.



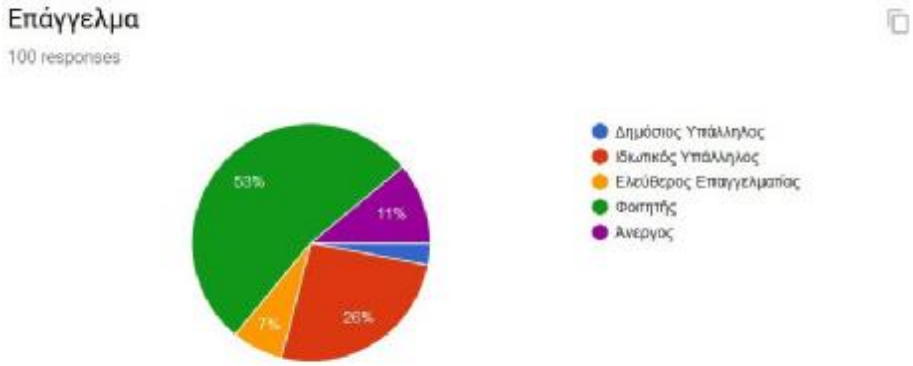
Στην εικόνα 32 φαίνεται ότι σε συνολικό δείγμα 100 ατόμων το 53% είναι κάτοχοι πτυχίου Α.Ε.Ι. ή Τ.Ε.Ι. , ενώ το 45% είναι απόφοιτοι λυκείου.

Εικόνα 32. Απάντηση ερωτηματολογίου 3.



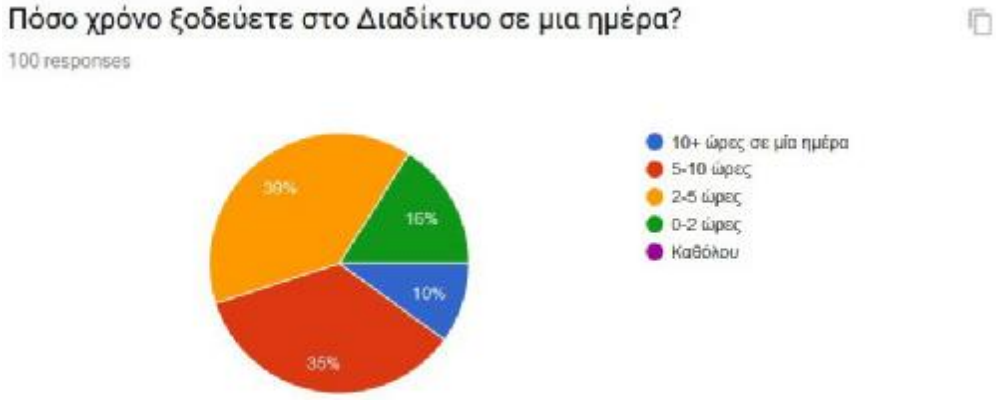
Στην εικόνα 33 φαίνεται ότι σε συνολικό δείγμα 100 ατόμων, το 53% είναι φοιτητές, το 26% είναι ιδιωτικοί υπάλληλη, το 11% είναι άνεργοι και το 7% είναι ελεύθεροι επαγγελματίες.

Εικόνα 33. Απάντηση ερωτηματολογίου 4



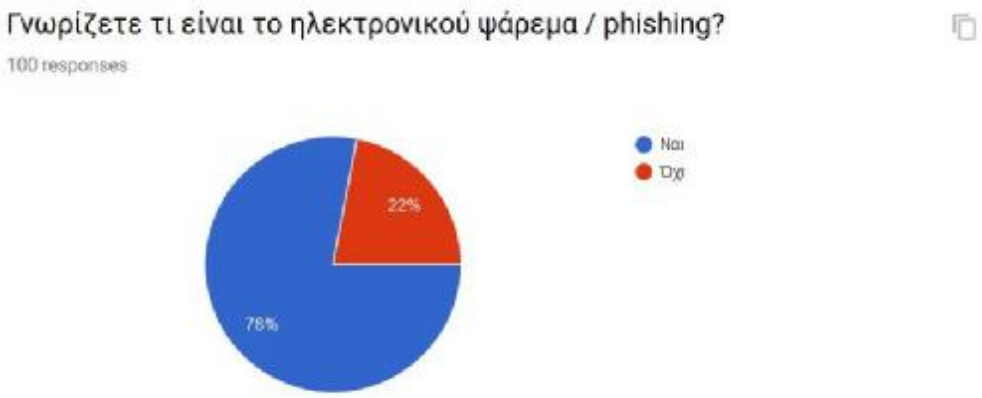
Στην εικόνα 34 φαίνεται ότι σε συνολικό δείγμα 100 ατόμων, το 39% ξοδεύει στο διαδίκτυο 2 έως 5 ώρες την ημέρα, το 35% 5 έως 10 ώρες την ημέρα, το 16% 0 έως 2 ώρες την ημέρα και το 10% περισσότερο από 10 ώρες την ημέρα.

Εικόνα 34. Απάντηση ερωτηματολογίου 5.



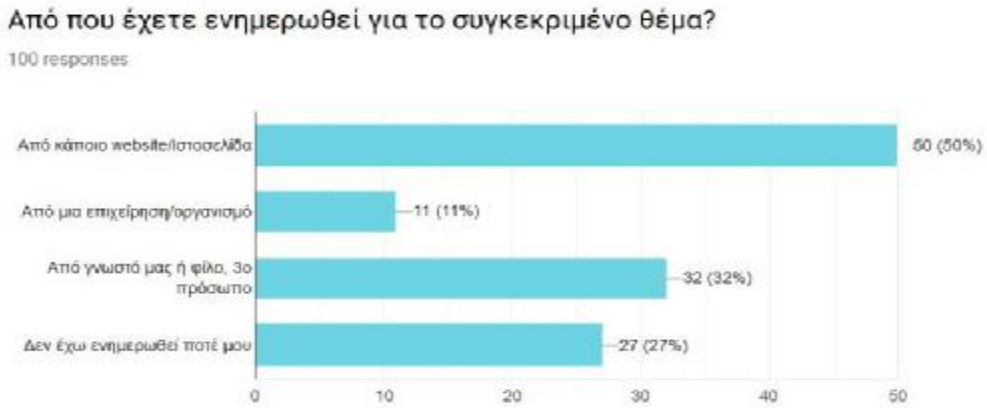
Στην εικόνα 35 παρατηρείται πως το 78% σε δείγμα 100 ατόμων γνωρίζει τί είναι το ηλεκτρονικό ψάρεμα.

Εικόνα 35. Απάντηση ερωτηματολογίου 6.



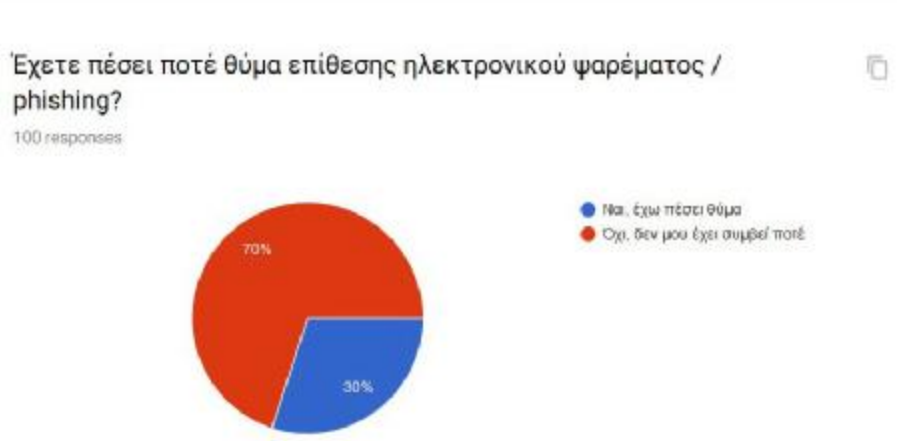
Στην εικόνα 36 φαίνεται πως σε δείγμα 100 ατόμων, το 50% έχει ενημερωθεί για το phishing από κάποιο website, το 32% από κάποιο τρίτο πρόσωπο, το 27% δεν έχει ενημερωθεί ποτέ και το 11% έχει ενημερωθεί από μία επιχείρηση/ οργανισμό.

Εικόνα 36. Απάντηση ερωτηματολογίου 7.



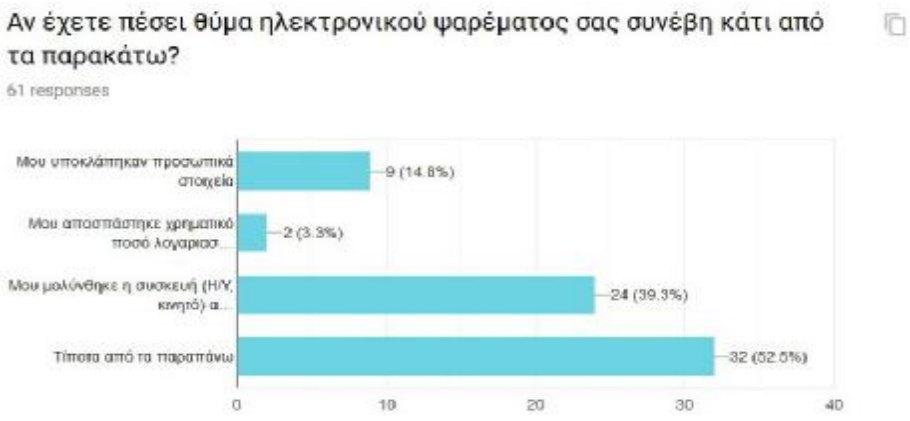
Στην εικόνα 37 παρατηρείται πως σε δείγμα 100 ατόμων το 30% έχει πέσει θύμα κάποιας επίθεσης ηλεκτρονικού ψαρέματος.

Εικόνα 37. Απάντηση ερωτηματολογίου 8.



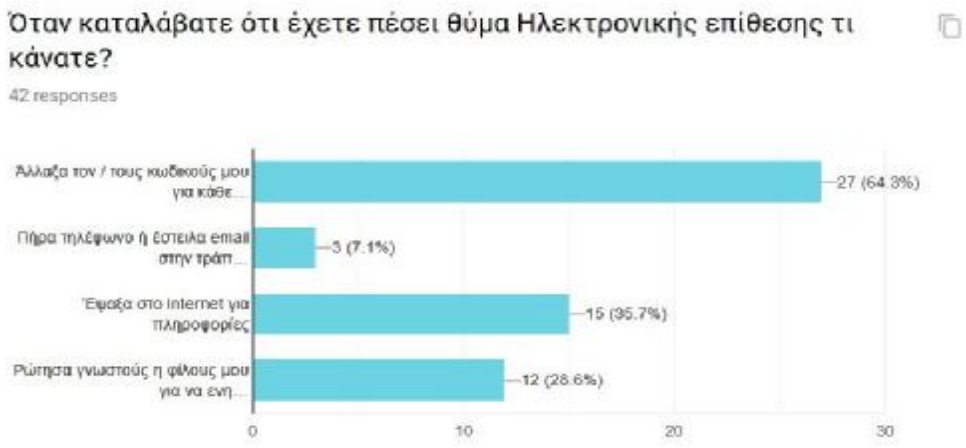
Στην εικόνα 38 φαίνεται πως από τα άτομα που έπεσαν θύμα κάποιας επίθεσης ηλεκτρονικού ψαρέματος παρατηρείται ότι στο 39.3% μολύνθηκε η ηλεκτρονική υπολογιστική συσκευή τους, στο 14.8% υποκλάπηκαν προσωπικά στοιχεία και στο 3.3% αποσπάστηκε χρηματικό ποσό.

Εικόνα 38. Απάντηση ερωτηματολογίου 9.



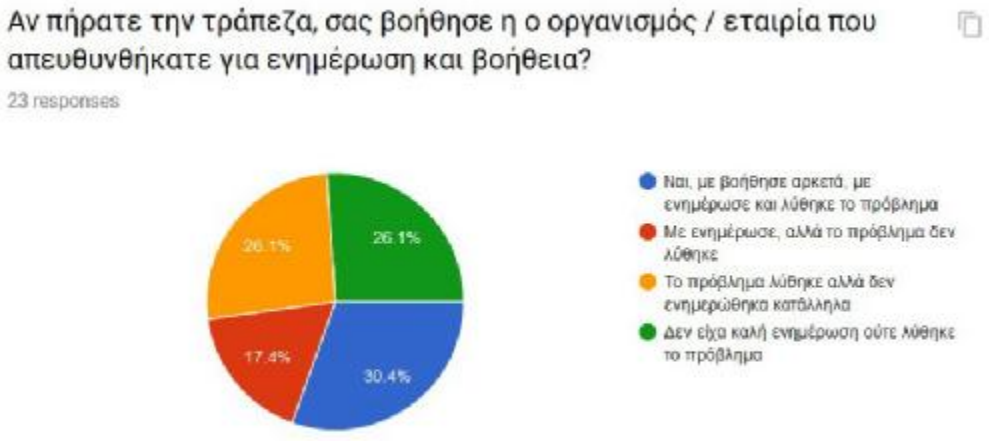
Στην εικόνα 39 φαίνεται ότι από τα άτομα που έπεσαν θύμα κάποιας επίθεσης phishing, μόλις το αντιλήφθηκαν, το 64% άλλαξε τους κωδικούς του, το 35% έψαξε στο internet για πληροφορίες, το 28.6% ζήτησε βοήθεια από κάποιο 3ο πρόσωπο και το 7.1% πήρε τηλέφωνο ή έστειλε e-mail σε κάποιον οργανισμό.

Εικόνα 39. Απάντηση ερωτηματολογίου 10.



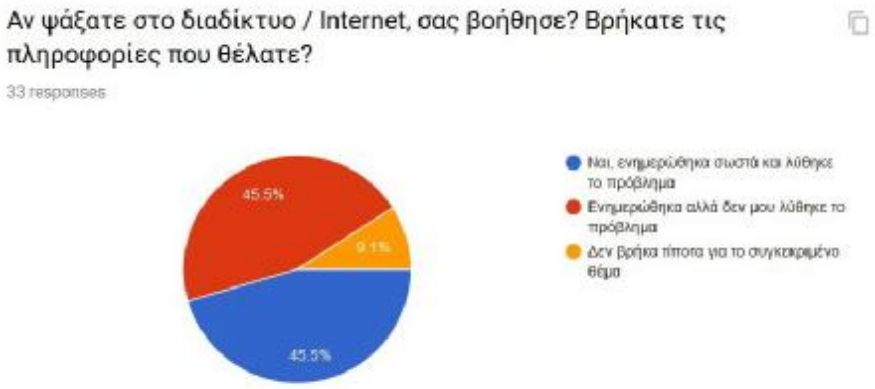
Στην εικόνα 40 φαίνεται ότι το 30% των ατόμων που απευθύνθηκαν σε κάποιον οργανισμό ενημερώθηκε και λύθηκε το πρόβλημά του, το 26,1% δεν ενημερώθηκε ούτε λύθηκε το πρόβλημά του, άλλο ένα 26,1% έλυσε το πρόβλημα αλλά δεν ενημερώθηκε αρκετά και το 17,4% ενημερώθηκε αλλά το πρόβλημα του δεν λύθηκε.

Εικόνα 40. Απάντηση ερωτηματολογίου 11.



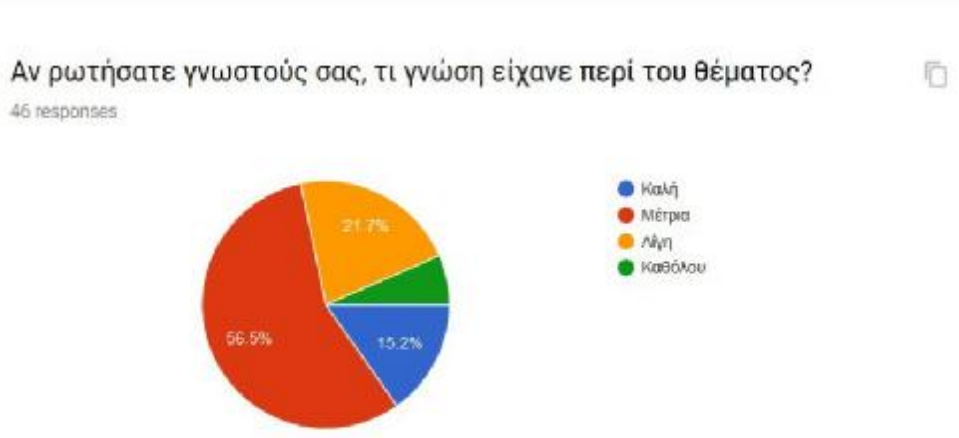
Στην εικόνα 41 φαίνεται πως από τα άτομα που έψαξαν στο διαδίκτυο, το 45.5% ενημερώθηκε και λύθηκε το πρόβλημά του, 45.5% επίσης ενημερώθηκε αλλά δεν λύθηκε το πρόβλημά του, το 9.1 δεν βρήκε πληροφορίες για το συγκεκριμένο θέμα.

Εικόνα 41. Απάντηση ερωτηματολογίου 12.



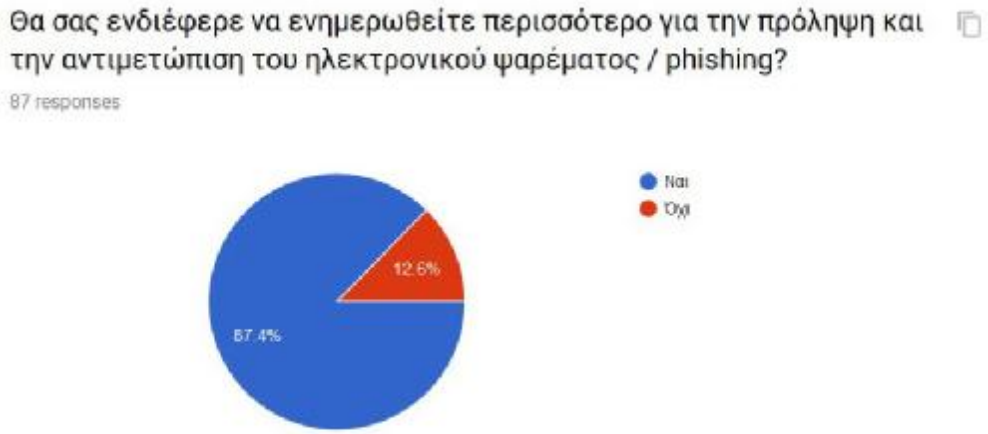
Στην εικόνα 42 παρατηρείται πως για τα άτομα που ρώτησαν γνωστούς τους για πληροφορίες, το 56.5% των τρίτων προσώπων που ερωτήθηκαν είχε μέτρια γνώση, το 21.7% είχε λίγη γνώση και το 15.2 είχε καλή γνώση περί του θέματος.

Εικόνα 42. Απάντηση ερωτηματολογίου 13.



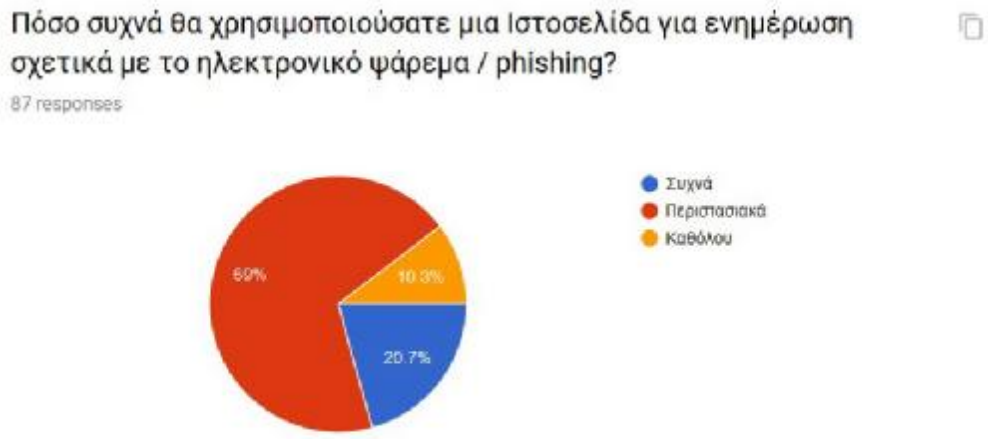
Στην εικόνα 43 φαίνεται πως από το σύνολο των 100 ατόμων το 87.4% θα ήθελε να ενημερωθεί περισσότερο για την πρόληψη και την αντιμετώπιση του ηλεκτρονικού ψαρέματος.

Εικόνα 43. Απάντηση ερωτηματολογίου 14.



Στην εικόνα 44 παρατηρείται πως από τα 100 άτομα που ερωτήθηκαν το 69% θα χρησιμοποιούσε περιστασιακά μια ιστοσελίδα για ενημέρωση σχετικά με το phishing, το 20.7% θα την χρησιμοποιούσε συχνά και το 10.3% καθόλου.

Εικόνα 44. Απάντηση ερωτηματολογίου 15.



ΣΥΜΠΕΡΑΣΜΑ

Το ηλεκτρονικό ««ψάρεμα»» είναι ένας διαδικτυακός τρόπος εξαπάτησης των χρηστών, που λειτουργεί με διάφορους τρόπους και μορφές. Σε αυτήν την εργασία αναλύσαμε διαφορές μεθόδους που χρησιμοποιούνται από hackers για το phising και διαφορετικές τεχνικές πρόληψης και αντιμετώπισης που χρησιμοποιηθήκαν από ερευνητές. Ο κύριος στόχος του phishing είναι η κλοπή χρημάτων μέσω άντλησης προσωπικών δεδομένων. Ως θύματα μιας τέτοιας επίθεσης μπορεί να συμπεριληφθούν απλοί χρήστες, μικρές ή μεγάλες εταιρίες και κρατικοί οργανισμοί. Τα άμεσα ή έμμεσα αποτελέσματα για τα δυνητικά θύματα πιθανόν να είναι καταστροφικά όπως η απώλεια της περιουσίας τους, η δημοσιοποίηση προσωπικών τους στοιχείων καθώς και η μόλυνση της συσκευής τους από κάποιο επιβλαβές λογισμικό. Για την προστασία της ιδιωτικότητας και την ασφάλεια των χρηστών είναι απαραίτητη η ενημέρωση για το phishing, όμως ένας χρήστης ενώ μπορεί να έχει τις απαραίτητες γνώσεις για την ανίχνευση κακόβουλων στοιχείων, ενδεχομένως να μην αντιληφθεί την επίθεση, λόγω έλλειψης προσοχής. Η χρήση προγραμμάτων ασφάλειας πιθανώς να αποτρέψει τους εισβολής από το να προχωρήσουν σε μια κακόβουλη ενέργεια. Υπάρχουν επίσης ομάδες κατά της ηλεκτρονικής απάτης στις οποίες θα μπορούσε να απευθυνθεί ένας χρήστης που θα τον βοηθήσουν να χειριστεί σωστά ένα πρόβλημα τέτοιου είδους.

Σύμφωνα με την έρευνα που διεξήγαμε παρατηρήσαμε ότι, το 78% του δείγματος 100 ατόμων γνωρίζει τί είναι το ηλεκτρονικό ψάρεμα και σε δείγμα 100 ατόμων το 30% έχει πέσει θύμα κάποιας επίθεσης ηλεκτρονικού ψαρέματος. Επίσης με αυτή την έρευνα παρατηρήσαμε ότι, από τα άτομα που έπεσαν θύμα κάποιας επίθεσης ηλεκτρονικού ψαρέματος το 39.3% μολύνθηκε η ηλεκτρονική υπολογιστική συσκευή τους, στο 14.8% υποκλάπηκαν προσωπικά στοιχεία και στο 3.3% αποσπάστηκε χρηματικό ποσό. Επιπλεων από τα άτομα αυτά που έπεσαν θύμα κάποιας επίθεσης phishing, μόλις το αντιλήφθηκαν, το 64% άλλαξε τους κωδικούς του, το 35% έψαξε στο internet για πληροφορίες, το 28.6% ζήτησε βοήθεια από κάποιο 3ο πρόσωπο και το 7.1% πήρε τηλέφωνο ή έστειλε e-mail σε κάποιον οργανισμό. Ενώ παρατηρείται πως από τα 100 άτομα που ερωτήθηκαν, το 69% θα χρησιμοποιούσε περιστασιακά μια ιστοσελίδα για ενημέρωση σχετικά με το phishing, το 20.7% θα την χρησιμοποιούσε συχνά και το 10.3% καθόλου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Aijaz Ahmad, S., et al. (2013) Smartphone: Android vs IOS. The SIJ Transactions on Computer Science Engineering & Its Applications (CSEA), 1, 141-148.
2. Archana, M., et al. (2011) Architecture for the Detection of Phishing in Mobile Internet. International Journal of Computer Science and Information Technologies, 2, 1297-1299.
3. Buku, M.W. and Mazer, R. (2015) Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System. CGAP, Washington, DC.
4. D. Querciax and R. Lambiottez and D. Stillwell and M. Kosinskiy and J. Crowcroft. The personality of popular facebook users. Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW), pages 955–964, 2012.
5. Canova, G., Volkamer, M., Bergmann, C., Borza, R., Reinheimer, B., Stockhardt, S., et al. (2015). Learn to Spot Phishing URLs with the Android NoPhish App. In Information Security Education Across the Curriculum (pp. 87-100): Springer.
6. Cao, Y., Han, W., & Le, Y. Anti-phishing based on automated individual white-list. In Proceedings of the 4th ACM workshop on Digital identity management, 2008 (pp. 51-60): ACM
7. Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. IEEE Security & Privacy, 12(1), 28-38.
8. Carlson, E. L. (2006). Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow.Elder LJ, 14, 423.
9. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. Phishing email detection based on structural properties. In NYS Cyber Security
10. Conference, Albany, New York, 2006 (pp. 1-7)
11. Chandrasekaran, M., Sankaranarayanan, V., & Upadhyaya, S. CUSP: customizable and usable spam filters for detecting phishing emails. In 3rd Annual Symposium on Information Assurance (ASIA'08), Albany, NY., 2008 (pp. 10): Citeseer

12. Chang, J., & Lee, K. (2010). Voice phishing detection technique based on minimum classification error method incorporating codec parameters. Signal Processing, IET, 4(5), 502-509, doi:10.1049/iet-spr.2009.0066.
13. Chen, C.-M., Guan, D., & Su, Q.-K. (2014). Feature set identification for detecting suspicious URLs using Bayesian classification in social networks. Information Sciences, 289, 133-147.
14. Chen, C., Dick, S., & Miller, J. (2010). Detecting visually similar web pages: Application to phishing detection. ACM Transactions on Internet Technology (TOIT), 10(2), 5.
15. Chen, J., & Chuanxiong, G. Online detection and prevention of phishing attacks. In 2006 First International Conference on
16. Communications and Networking in China, 2006 (pp. 1-7): IEEE
17. Cheng, H., Wang, P., & Pu, S. Identify fixed-path phishing attack by STC. In Proceedings of the 8th Annual Collaboration,
18. Electronic messaging, Anti-Abuse and Spam Conference, 2011 (pp. 172-175): ACM
19. Chhabra, S., Aggarwal, A., Benevenuto, F., & Kumaraguru, P. Phi. sh/$ o CiaL: the phishing landscape through short URLs. In the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, Perth, Western Australia, 2011 (pp. 92-101): ACM
20. Choi, H., Zhu, B. B., & Lee, H. (2011). Detecting malicious web links and identifying their attack types. Paper presented at the
21. Proceedings of the 2nd USENIX conference on Web application development, Portland,
22. Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., & Mitchell, J. C. Client-side defense against web-based identity theft. In 11th
23. Annual Network and Distributed System Security Symposium (NDSS'04), San Diego, California, 2004: San Diego, USA
24. Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. Who is tweeting on Twitter: human, bot, or cyborg? In Proceedings of the 26th annual computer security applications conference, Austin, TX, USA, 2010 (pp. 21-30): ACM
25. Chuan, Y., & Haining, W. (2010). BogusBiter: A transparent protection against phishing attacks. ACM Transactions on Internet Technology (TOIT), 10(2), 6.
26. Cova, M., Kruegel, C., & Vigna, G. (2008). There Is No Free Phish: An Analysis of" Free" and Live Phishing Kits. WOOT, 8, 1-8

27. Bottazzi, G. (2015) MP-Shield: A Framework for Phishing Detection in Mobile Devices. IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, 26-28 October 2015, 1977-1983. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.293
28. Gaddis S. Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information. Cyberpsychology, Behavior, and Social Networking, 14:483–488, 9 2011, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3180765/
29. Kumar, N. and Chaudhary, P. (2017) Mobile Phishing Detection using Naive Bayesian Algorithm. International Journal of Computer Science and Network Security, 17, 142-147. Orunsolu, A.A.
30. Luminzu Mudiri, J. (2012) Fraud in Mobile Financial Services. MicroSave, Lucknow.
31. Malisa, L., et al. (2015) Technical Report: Detecting Mobile Application Spoofing Attacks by Leveraging User Visual Similarity Perception.
32. Memon, I.K. and Khan, M.K. (2013) Anti Phishing for Mid-Range Mobile Phones. International Journal of Computer and Communication Engineering, 2, 115-119.
33. Mishra, M., et al. (2012) A Preventive Anti-Phishing Technique using Code Word. International Journal of Computer Science and Information Technologies, 3, 4248-4250
34. Orunsolu, A.A. (2017) A Lightweight Anti-Phishing Technique for Mobile Phone. Acta Informatica Pragensia, 6, 114-123
35. Singh, D., et al. (2011) Telephony Fraud Prevention. US Patent
36. Yenurkar, B. and Zade, S. (2014) An Anti-Phishing Framework with New Validation Scheme Using Visual Cryptography. International Journal of Computer Science and Mobile Computing, 3, 739-744
37. Yoon, J.W., et al. (2010) Hybrid Spam Filtering for Mobile Communication. Computers and Security, 29, 446-459. https://doi.org/10.1016/j.cose.2009.11.003
38. Lance James. Phishing Exposed. Rockland, MA : Syngress, 2005.
39. Wikipedia. Phishing wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Phishing&oldid=484977983,2012.[Online; accessed 2-April-2012]
40. Federal Bureau of Investigation. Spear phishers. http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

41. Markus Jakobsson and Steven Myers. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Inc., 2007.
42. D. Eastlake 3rd. Domain Name System Security Extensions. RFC 2535 (Proposed Standard), March 1999. Obsoleted by RFCs 4033, 4034, 4035, updated by RFCs 2931, 3007, 3008, 3090, 3226, 3445, 3597, 3655, 3658, 3755, 3757, 3845.
43. Owen Fletcher and Robert McMillan. Baidu: Registrar `incredibly' changed our email forhacker. http://www.computerworld.com/s/article/9162118/Baidu_Registrar_incred b%ly_changed_our_e_mail_for_hacker, 2010.
44. Gundeep Singh Bindra. Masquerading as a trustworthy entity through portable document_le (pdf) format. In Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third Inter-national Conference on and 2011 IEEE Third International Confernece on Social Computing (SocialCom), pages 784 {789, Oct 2011.
45. Beichuan Zhang. Domain name system (dns).
46. Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, and Lorrie Cranorand Julie
47. Downs1. Who falls for phish? a demographic analysis of phishing susceptibility and e_ectiveness of interventions. In 28th international conference on Human factors in computing systems, Apr 2010.
48. Wilson C. and Argles D. The _ght against phishing: Technology, the end user and legislation.
49. In Information Society (i-Society), 2011 International Conference on, pages 501 {504, Jun 2011.
50. luoposhusheng. Plaintext disclosure vulnerability of alipay password security control. Hacker Defense, pages 6{8, Nov 2011.
51. Yiru Xu. 67-year-old man swindled 700k from online banking account.
52. http://finance.sina.com.cn/money/bank/guangjiao/20110326/16149598471.sh%tml.
53. Opendns' phishtank.com and anti-phishing working group to share data.
54. http://www.opendns.com/about/announcements/19/.
55. https://blog.barkly.com/phishing-statistics-2016.
56. https://www.keepnetlabs.com/phishing-statistics-2017/
57. https://en.wikipedia.org/wiki/Phishing
58. https://www.duocircle.com/phishing-protection/top-phishing-email-attacks-worldwide-in-2018

59. https://www.scmagazineuk.com/leoni-ag-suffers-34-million-whaling-attack/article/530694/
60. http://resources.infosecinstitute.com/spear-phishing-real-life-examples/#gref [
61. https://www.avast.com/el-gr/index#pc
62. https://www.superantispyware.com/

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Δρ. Γεωργιάδης Χ.Κ. Προβλήματα Ασφάλειας στο Ηλεκτρονικό Εμπόριο. Σημειώσεις μαθήματος, Παν. Θεσσαλίας, 2003.
2. Δρ. Κοτζανικολάου Π. Τεχνολογίες και Πολιτικές Ασφάλειας. Σημειώσεις μαθήματος, 7ο Εξάμηνο. Τμήμα Πληροφορικής, Πανεπιστήμιο Πειραιώς, 2005.

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

- **Φύλλο**

Οι άνδρες που απάντησαν στην έρευνα είναι το 44% και οι γυναίκες το 56% του συνολικού δείγματος των 100 ατόμων.

- **Ηλικία**

Το 69% των ατόμων που απάντησαν βρίσκονται σε ηλικία από 18 έως 25 ετών, το 21% είναι άτομα ηλικίας από 25 έως 30 ετών και το 7% είναι άτομα ηλικίας από 30 έως 50 ετών του συνολικού δείγματος των 100 ατόμων.

- **Εκπαιδευτική κατάρτιση**

Σε συνολικό δείγμα 100 ατόμων το 53% είναι κάτοχοι πτυχίου Α.Ε.Ι. ή Τ.Ε.Ι. , ενώ το 45% είναι απόφοιτοι λυκείου.

- **Επάγγελμα**

Σε συνολικό δείγμα 100 ατόμων, το 53% είναι φοιτητές, το 26% είναι ιδιωτικοί υπάλληλη, το 11% είναι άνεργοι και το 7% είναι ελεύθεροι επαγγελματίες.

- **Πόσο χρόνο ξοδεύετε στο Διαδίκτυο σε μια ημέρα?**

Σε συνολικό δείγμα 100 ατόμων, το 39% ξοδεύει στο διαδίκτυο 2 έως 5 ώρες την ημέρα, το 35% 5 έως 10 ώρες την ημέρα, το 16% 0 έως 2 ώρες την ημέρα και το 10% περισσότερο από 10 ώρες την ημέρα.

- **Γνωρίζετε τι είναι το ηλεκτρονικού ψάρεμα / phishing?**

Το 78% σε δείγμα 100 ατόμων γνωρίζει τί είναι το ηλεκτρονικό ψάρεμα.

- **Από που έχετε ενημερωθεί για το συγκεκριμένο θέμα?**

Σε δείγμα 100 ατόμων, το 50% έχει ενημερωθεί για το phishing από κάποιο website, το 32% από κάποιο τρίτο πρόσωπο, το 27% δεν έχει ενημερωθεί ποτέ και το 11% έχει ενημερωθεί από μία επιχείρηση/ οργανισμό.

- **Έχετε πέσει ποτέ θύμα επίθεσης ηλεκτρονικού ψαρέματος / phishing?**

Σε δείγμα 100 ατόμων το 30% έχει πέσει θύμα κάποιας επίθεσης ηλεκτρονικού ψαρέματος.

- **Αν έχετε πέσει θύμα ηλεκτρονικού ψαρέματος σας συνέβη κάτι από τα παρακάτω?**

Από τα άτομα που έπεσαν θύμα κάποιας επίθεσης ηλεκτρονικού ψαρέματος παρατηρείται ότι στο 39.3% μολύνθηκε η ηλεκτρονική υπολογιστική συσκευή τους, στο 14.8% υποκλάπηκαν προσωπικά στοιχεία και στο 3.3% αποσπάστηκε χρηματικό ποσό.

- **Όταν καταλάβατε ότι έχετε πέσει θύμα Ηλεκτρονικής επίθεσης τι κάνατε?**

Από τα άτομα που έπεσαν θύμα κάποιας επίθεσης phishing, μόλις το αντιλήφθηκαν, το 64% άλλαξε τους κωδικούς του, το 35% έψαξε στο internet για πληροφορίες, το 28.6% ζήτησε βοήθεια από κάποιο 3ο πρόσωπο και το 7.1% πήρε τηλέφωνο ή έστειλε e-mail σε κάποιον οργανισμό.

- **Αν πήρατε την τράπεζα, σας βοήθησε η ο οργανισμός / εταιρία που απευθυνθήκατε για ενημέρωση και βοήθεια?**

Το 30% των ατόμων που απευθύνθηκαν σε κάποιον οργανισμό ενημερώθηκε και λύθηκε το πρόβλημά του, το 26,1% δεν ενημερώθηκε ούτε λύθηκε το πρόβλημά του, άλλο ένα 26,1% έλυσε το πρόβλημα αλλά δεν ενημερώθηκε αρκετά και το 17,4% ενημερώθηκε αλλά το πρόβλημα του δεν λύθηκε.

- **Αν ψάξατε στο διαδίκτυο / Internet, σας βοήθησε? Βρήκατε τις πληροφορίες που θέλατε?**

Από τα άτομα που έψαξαν στο διαδίκτυο, το 45.5% ενημερώθηκε και λύθηκε το πρόβλημά του, 45.5% επίσης ενημερώθηκε αλλά δεν λύθηκε το πρόβλημά του, το 9.1 δεν βρήκε πληροφορίες για το συγκεκριμένο θέμα.

- **Αν ρωτήσατε γνωστούς σας, τι γνώση είχανε περί του θέματος?**

Τα άτομα που ρώτησαν γνωστούς τους για πληροφορίες, το 56.5% των τρίτων προσώπων που ερωτήθηκαν είχε μέτρια γνώση, το 21.7% είχε λίγη γνώση και το 15.2 είχε καλή γνώση περί του θέματος.

- **Θα σας ενδιέφερε να ενημερωθείτε περισσότερο για την πρόληψη και την αντιμετώπιση του ηλεκτρονικού ψαρέματος / phishing?**

Από το σύνολο των 100 ατόμων το 87.4% θα ήθελε να ενημερωθεί περισσότερο για την πρόληψη και την αντιμετώπιση του ηλεκτρονικού ψαρέματος.

- **Πόσο συχνά θα χρησιμοποιούσατε μια Ιστοσελίδα για ενημέρωση σχετικά με το ηλεκτρονικό ψάρεμα / phishing?**

Από τα 100 άτομα που ερωτήθηκαν το 69% θα χρησιμοποιούσε περιστασιακά μια ιστοσελίδα για ενημέρωση σχετικά με το phishing, το 20.7% θα την χρησιμοποιούσε συχνά και το 10.3% καθόλου.