ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (Πάτρα)

Τίτλος Εργασίας: *ΑΝΑΖΗΤΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ DEEP WEB*

Πτυχιακή Εργασία *των Παναγιώτη Κωνσταντόπουλου και Βασίλειου Αλεξίου*

Επιβλέπων: Δημήτριος Παπαδόπουλος

ΠΑΤΡΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2016

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1. ΤΟ ΔΙΑΔΙΚΤΥΟ

1.1 Ορισμός διαδικτύου

Οι ορισμοί που έχουν δοθεί κατά διαστήματα αναφορικά με το Ίντερνετ είναι αρκετοί. Ως βασικό σημείο αναφοράς μπορεί κάποιος να πει ότι το Ίντερνετ δεν είναι μια νέα τεχνολογία, αλλά ένας οδηγός που ωθεί για την δημιουργία και ανάπτυξη νέων τεχνολογικών και πρακτικών που επηρεάζουν τη ζωή του μέσου ανθρώπου (Markham, 2001).

Σύμφωνα με τον Markham, το ίντερνετ άρχισε ως ένα κυβερνητικό και στρατιωτικό δίκτυο επικοινωνίας στις αρχές της δεκαετίας του 1970. Στην συνέχεια χρησιμοποιήθηκε από ακαδημαϊκούς σε ινστιτούτα ερευνών ως ένα εργαλείο που συνέδεε τους υπολογιστές για να μοιράζονται πληροφορίες και τα αποτελέσματα των ερευνών τους. Σήμερα το ίντερνετ χρησιμοποιείται από πολλούς ανθρώπους ως μέσο επικοινωνίας, διασκέδασης, έρευνας αλλά και για αγορά προϊόντων και υπηρεσιών (Markham, 2001).

Σύμφωνα με τον Turban γίνεται η εξής αναφορά: «*Το ίντερνετ είναι ένα δίκτυο υπολογιστών που συνδέεται με διάφορους τρόπους και σε διάφορες ταχύτητες. Αυτό επιτρέπει στους χρήστες να ανταλλάζουν πληροφορίες με ανθρώπους που βρίσκονται σε άλλα σημεία*» (Turban, 2002).

Σύμφωνα με τον Rowan σημειώνεται ότι «*Στην αρχή πολλοί νόμιζαν ότι το ίντερνετ θα ήταν ένα νέο μέσο επικοινωνίας. Παρόλα αυτά, η παράλληλη ανάπτυξη νέων τεχνολογιών και δικτύων επικοινωνίας (π.χ. γρήγορες συνδέσεις και δημιουργία ασύρματων δικτύων) βοήθησαν το ίντερνετ να γίνει κάτι παραπάνω από ένα μέσο επικοινωνίας. Πολλές επιχειρήσεις βασίζονται στο ίντερνετ για τις επικοινωνίες τους αλλά και να πουλάνε τα προϊόντα τους και τις υπηρεσίες τους*» (Rowan, 2002).

Επιχειρήσεις όπως η Siemens, έχουν δημιουργήσει συστήματα διαχείρισης γνώσης που ασχολούνται με μεγάλες ποσότητες γνώσης και φυσικά είναι τα συστήματα πάνω στα οποία η επιχείρηση βασίζει τα ανταγωνιστικά πλεονεκτήματα τους.

1.2 Οφέλη Διαδικτύου

Η γρήγορη εξέλιξη του διαδικτύου και η ραγδαία κοινωνική κυρίως εγκατάσταση, του προσέδωσε πολλές διαστάσεις όπως την εκπαιδευτική και τη ψυχαγωγική. Η παρούσα υποενότητα θα εστιάσει στην ψυχαγωγική διάσταση του διαδικτύου, ενώ η παιδαγωγική θα αναλυθεί στην αμέσως επόμενη υποενότητα.

Όσο περισσότερο τα παιδιά χρησιμοποιούν το διαδίκτυο, τόσο πιο εύκολα, η σκέψη τους εξελίσσεται σύμφωνα με αυτό και μαθαίνουν να αναπτύσσουν δεξιότητες με εργαλεία που στο παρελθόν όχι μόνο ήταν άγνωστα αλλά θεωρούνταν και επιβλαβή.

Παρά το γεγονός, ότι αρκετοί θεωρούν το διαδίκτυο, ως ένα εργαλείο που απομονώνει τα παιδιά, η ένταξή του στη καθημερινότητά τους, φαίνεται να ενθαρρύνει τη συνεργασία και να ευνοεί την κοινωνική και συναισθηματική τους ανάπτυξη. Κατά συνέπεια, οδηγεί στη δημιουργία αρμονικών σχέσεων και στην αποφυγή των συγκρούσεων (Κόμης, 2012).

Εστιάζοντας, στα ηλεκτρονικά παιχνίδια κάποιες μελέτες (Weiss, Rand, Katz, 2004) θεωρούν ότι τα παιδιά γοητεύονται από ηλεκτρονικά παιχνίδια και είναι καλό να παρακινούνται να ασχολούνται με αυτά, διότι τους παρέχουν, τόσο εξωτερικά, όσο και εσωτερικά κίνητρα όπως είναι το αίσθημα του ελέγχου, της περιέργειας και της φαντασίας.

Παράλληλα τα ηλεκτρονικά παιχνίδια, δίνουν τη δυνατότητα στον έφηβο, να αναπτύξει τη λογική του, αλλά και να αποκτήσει δεξιότητες και γνώσεις με ευχάριστο τρόπο (Klawe, Philips, 1995). Χαρακτηριστικό παράδειγμα, αποτελούν τα ηλεκτρονικά παιχνίδια, τύπου προσομοιώσεων. Οι προσομοιώσεις αναπαριστούν την πραγματικότητα και μελετούν την εξέλιξη ενός φαινομένου που δύσκολα μπορεί να πραγματοποιηθεί στο σχολικό εργαστήριο. Με τη χρήση προσομοιώσεων ο μαθητής μπορεί να αλλάζει τις παραμέτρους του προβλήματος και να συμμετέχει στη διαδικασία ενεργά, εξετάζοντας την εξέλιξη ενός φαινομένου, ελέγχοντας τις μεταβλητές (Ματσαγγούρας, 1998).

Οι προσομοιώσεις με τη χρήση λογισμικού δίνουν τη δυνατότητα των

πολλαπλών αναπαραστάσεων και τη διερεύνηση από το μαθητή, ενώ γίνεται ευκολότερος ο έλεγχος των υποθέσεων και των προβλέψεων από αυτόν. Επομένως, ο μαθητής αποκτά προσωρινά και το ρόλο του ερευνητή. Ο συνδυασμός του πειράματος και των προσομοιώσεων είναι μια ακόμα θετική συμβολή των προσομοιώσεων, αλλά απαιτεί προσεκτικό σχεδιασμό και διερεύνηση γιατί πιθανώς να μειώνεται η φυσική επαφή του μαθητή με το εργαστήριο (Κόκκοτας, Βλάχος, Καρανίκας, 1995).

Στη σημερινή εποχή, το διαδίκτυο και συγκεκριμένα οι λεγόμενες μηχανές αναζήτησης, αποτελούν μια σημαντική πηγή πληροφόρησης, τόσο για τους εκπαιδευτικούς, όσο και για τους έφηβους μαθητές. Οι νέοι χρησιμοποιούν κυρίως το διαδίκτυο προκειμένου να αναζητήσουν χρήσιμες πληροφορίες σχετικά με τις εργασίες τους ή με τις σπουδές τους.

Χρήσιμο εργαλείο του διαδικτύου αποτελούν επίσης οι ηλεκτρονικές βιβλιοθήκες, οι οποίες βοηθούν τους χρήστες στην αναζήτηση βιβλιογραφικών πηγών (Jones, 2002). Το διαδίκτυο με τις μηχανές αναζήτησης, παρέχει ποικίλες και πρόσφατες γνώσεις χωρίς χώρο-χρονικούς περιορισμούς και θα μπορούσε να ειπωθεί ότι συμπληρώνει τη λειτουργία του μοναδικού έντυπου βιβλίου (Μικρόπουλος, 2006).

Η χρήση του διαδικτύου στην εκπαίδευση έχει εμπλουτίσει τη διδασκαλία με εικόνα, animation, ήχο και με τη δυνατότητα της διάδρασης. Τα στοιχεία αυτά, κατά πρώτο λόγο, κάνουν το περιβάλλον της μάθησης πιο ελκυστικό για το μαθητή, και κατά δεύτερο τον βοηθούν να κατανοήσει δύσκολες κι αφηρημένες έννοιες (White, 1997).

Το διαδίκτυο, θεωρείται χρήσιμο εργαλείο στην εκπόνηση ενός σχεδίου εργασίας από τους μαθητές. Τα projects (σχέδια εργασίας) μπορεί να πραγματοποιηθούν, ιδιαίτερα, όσον αφορά στη συλλογή του υλικού, με τη χρήση του ηλεκτρονικού υπολογιστή ή του διαδικτύου. Η χρήση του ηλεκτρονικού υπολογιστή θεωρείται ότι ευχαριστεί ιδιαίτερα τους μαθητές, τους προσφέρει πλούσιο οπτικοακουστικό υλικό, ενώ παράλληλα τους δημιουργεί κίνητρα για μάθηση και καθιστά το διδακτικό αντικείμενο προσιτό και κατανοητό.

Η χρήση του διαδικτύου στην εκπόνηση ενός σχεδίου εργασίας, δίνει τη δυνατότητα στους μαθητές να ανταλλάξουν τις απόψεις τους σε ηλεκτρονικούς χώρους συζητήσεων (chat rooms) του facebook και τηλεδιασκέψεις (video conferencing) με τους εικονικούς συμμαθητές τους. Παράλληλα τα βοηθάει να συλλέγουν υλικό μέσα από πληθώρα πηγών, που διαβάζουν και με τον τρόπο αυτό αποκτούν εμπειρίες και γνώσεις. Τέλος τους δίνεται η δυνατότητα για δημιουργική δράση, μέσα από τη δημιουργία ιστοσελίδας (web site) στο Internet (Dudeney, 2000).

Τα προβλήματα ωστόσο του διαδικτύου δεν παύουν να υπάρχουν και να εμφανίζονται κυρίως σε ανήλικους χρήστες. Οι έφηβοι, λόγω της ψυχικής και διανοητικής τους ανωριμότητας είναι πιο ευάλωτοι απέναντι στους κινδύνους του διαδικτύου (Αθανάσαινα, 2008). Οι έρευνες (Yellowlees, Shayna, 2007) εξάλλου αποδεικνύουν ότι οι ανήλικοι αποτελούν το πιο δυναμικό κομμάτι στην ηλικιακή κατανομή των χρηστών του διαδικτύου.

Ταυτόχρονα οι Έλληνες γονείς είναι οι τελευταίοι σε ολόκληρη την Ευρωπαϊκή Ένωση όσον αφορά στη γνώση τους πάνω στους κινδύνους που εγκυμονεί το διαδίκτυο. Το αισιόδοξο είναι ότι η συντριπτική πλειονότητα των Ελλήνων αισθάνεται την ανάγκη να πληροφορηθεί περισσότερα για τους κινδύνους του διαδικτύου προκειμένου να προστατεύσει τα παιδιά του.

1.3 Κίνδυνοι διαδικτύου

Θεωρητικά, επικρατεί ένα στερεότυπο αναφορικά με τον χρήση που είναι εξαρτημένος και χρησιμοποιεί παθολογικά το διαδίκτυο. Τα κύρια χαρακτηριστικά του στερεότυπου αυτού είναι ότι είναι άνδρας νεαρής ηλικίας, στοιχείο που τονίζει τον παράγοντα του φύλου σε αυτό το φαινόμενο (Griffiths, 2000).

Ο πρώτος που αναφέρθηκε στον εθισμό από τον διαδίκτυο ήταν ο καθηγητής του πανεπιστημίου της Columbia, Ivan Goldberg. Ο Goldberg (1995) ήταν ο πρώτος που όρισε την υπερβολική χρήση του διαδικτύου, ως μία έννοια ταυτόσημη με τις δυσλειτουργίες και τις αναπηρίες (Goldberg,

1995). Επίσης, ο Goldberg (1996), ήταν ο πρώτος που αναφέρθηκε σε κριτήρια τα οποία χρησιμοποιούνταν στην εξάρτηση των ουσιών για να καθορίσει τη συγκεκριμένη διαταραχή (Goldberg, 1996).

Με τη πάροδο του χρόνου, το φαινόμενο περιγράφηκε με διάφορους όρους όπως «εθισμός στο διαδίκτυο», «παθολογική χρήση του διαδικτύου και «προβληματική χρήση του διαδικτύου» (Davis, Flett, Besser, 2002).

Η εξάρτηση από το διαδίκτυο και εν γένει από τη χρήση ηλεκτρονικών υπολογιστών υφίσταται ως υπαρκτό κοινωνικό φαινόμενο στις σύγχρονες βιομηχανικές ή μεταβιομηχανικές μορφές κοινωνικής οργάνωσης ανά τον κόσμο. Το φαινόμενο αλόγιστης χρήσης του διαδικτύου από τους ενήλικες, όσο – και αυτό είναι το πιο ανησυχητικό – από εφήβους, δημιουργεί σοβαρά προβλήματα στην ψυχική και κοινωνική λειτουργία των εξαρτημένων χρηστών του.

Ο εθισμός στο Διαδίκτυο αποτελεί μια σχετικά νέα μορφή εξάρτησης, η οποία βρίσκεται υπό εξέταση από την επιστημονική κοινότητα προκειμένου να οριοθετηθεί. Σύμφωνα με την κ Ίλια Θεοτοκά, κλινική ψυχολόγο και παιδοψυχολόγο, η εξάρτηση από το Ίντερνετ δεν είναι ακόμη μια κλινική οντότητα που συναντάται σε εγχειρίδια ψυχιατρικά (Davis, 2001).

Η πρώτη περίπτωση εθισμού από το διαδίκτυο εμφανίστηκε το 1997, στις Η.Π.Α. Το πρώτο Κέντρο Απεξάρτησης λειτούργησε το 1995, στην Πενσυλβάνια των Η.Π.Α., ενώ την ίδια χρονιά ο Νεοϋορκέζος ψυχίατρος Ivan Goldberg, υιοθέτησε πρώτος τον όρο Internet addiction («εθισμός» στο Internet). Οι πρώτες περιπτώσεις αφορούσαν ενήλικες, ωστόσο τα επόμενα χρόνια το φαινόμενο επεκτάθηκε ραγδαία σε εφήβους και νέους.

Λόγω του ότι η Αμερικανική Ψυχιατρική Εταιρεία δεν έχει αποδεχθεί την κατάχρηση διαδικτύου ως κατάσταση αληθούς εθισμού, και υπάρχει γενικά συζήτηση στην διεθνή βιβλιογραφία, ο όρος «εθισμός» ή «εξάρτηση» χρησιμοποιούνται σε εισαγωγικά (Τσίτσικα, Φρέσκου, 2008).

Ο εθισμός στο διαδίκτυο θα μπορούσε να οριστεί ως την «ενασχόληση με το Ίντερνετ για άντληση αισθήματος ικανοποίησης που

συνοδεύεται με αύξηση του χρόνου που καταναλώνεται για την άντληση αυτού του αισθήματος» (Τσίτσικα, 2008). Η ενασχόληση αυτή συνοδεύεται από επιπλέον συμπτώματα που σχετίζονται κυρίως με τη μη ενασχόληση με άλλες δραστηριότητες.

Επιγραμματικά, μερικά συμπτώματα του εθισμού εφήβων στο Διαδίκτυο, σύμφωνα με την κλινική ψυχολόγο και παιδοψυχολόγο κ. Ίλια Θεοτοκά, είναι η αδιαφορία για άλλες δραστηριότητες, η μειωμένη επίδοση στο σχολείο λόγω των πολλών ωρών που περνάει ο έφηβος στο Ίντερνετ, ενώ σε προχωρημένες περιπτώσεις ο έφηβος δεν κοιμάται, παραμελεί την προσωπική του υγιεινή αλλά και αδυναμία να σταματήσει την ενασχόληση αυτή την ώρα που έχει ορίσει ο ίδιος.

Το Ίντερνετ έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα χαρακτηριστικά του μέσου που προκύπτει από τη φύση του είναι ότι μπορεί να δημιουργήσει μια «ιδανική κατάσταση εαυτού», όπου το άτομο μπορεί να εξερευνήσει διάφορες πτυχές της προσωπικότητάς του χωρίς περιορισμούς και συνέπειες.

Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων. Ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει, πολλές φορές, οπτική επαφή. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους, ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου.

Η εξάρτηση του εφήβου από το διαδίκτυο μπορεί να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας και κοινωνική φοβία. Όπως με κάθε μορφής διαταραχή, δεν λείπουν τα ακραία περιστατικά, όπου ο έφηβος δεν παραμελεί απλά το περιβάλλον του, αλλά τον ίδιο του τον εαυτό, διακυβεύοντας ακόμη και τη σωματική του υγεία.

Έτσι, εκτός από περιπτώσεις παιδιών που είχαν χαθεί για ολόκληρα 24ωρα σε Ίντερνετ καφέ και που εκδήλωσαν βίαιες συμπεριφορές, η Μονάδα

Εφηβικής Υγείας βρέθηκε μπροστά σε παιδιά που παραμελούσαν την προσωπική τους υγιεινή, τη διατροφή τους, παραμελούσαν τον εαυτό τους σε τέτοιο σημείο που δεν άλλαζαν καν ρούχα για μέρες.

Για να κριθεί ένα άτομο εθισμένο στο Διαδίκτυο, πάσχον δηλαδή από μια ψυχική διαταραχή, πρέπει να πληροί ορισμένα συγκεκριμένα επιστημονικά κριτήρια. Σε αυτά, εκτός από την πολύωρη ημερήσια ενασχόληση με το Διαδίκτυο περιλαμβάνονται τα ακόλουθα (Σιώμος, Αγγελόπουλος, 2008):

- Συμπτώματα Συνδρόμου Απόσυρσης , όπως ψυχοκινητική διέγερση, εκούσια ή ακούσια κίνηση δακτυλογράφησης των δακτύλων του χεριού, άγχος, έμμονη σκέψη για το Internet, όνειρα για το Internet
- Χρήση Διαδικτύου προκειμένου να αποφευχθούν συμπτώματα απόσυρσης
- Παραμονή on-line για μεγαλύτερο χρονικό διάστημα από το προτιθέμενο
- Κατανάλωση υπερβολικού χρόνου ή/και χρήματος σε δραστηριότητες σχετικές με το Διαδίκτυο (λογισμικό, σκληροί δίσκοι κ.λπ)
- Έκπτωση λειτουργικότητας του ατόμου (σε κοινωνικό, οικογενειακό, προσωπικό επίπεδο, παραμέληση προσωπικής φροντίδας και υγιεινής, απώλεια ύπνου, ενδοοικογενειακές συγκρούσεις, σχολική αποτυχία)
- Συνέχιση χρήσης παρά την γνώση της παραπάνω έκπτωσης.
- Εξιδανίκευση του μέσου. Ο χρήστης θεωρεί τον ηλεκτρονικό υπολογιστή ή το Διαδίκτυο το σημαντικότερο «κεφάλαιο» της καθημερινότητάς του.
- Τροποποίηση της διάθεσης. Σε όσους εθίζονται στα ηλεκτρονικά παιχνίδια παρουσιάζεται αύξηση της παραγωγής του νευροδιαβιβαστή του εγκεφάλου ντοπαμίνη, η οποία συνδέεται με την

ευχαρίστηση.

- Ανοχή. Το άτομο χρειάζεται σταδιακά όλο και περισσότερες ώρες χρήσης του υπολογιστή ώστε να νιώθει ευχαρίστηση.

- Σύγκρουση. Ενώ το παιδί αισθάνεται ότι έχει πρόβλημα, δεν μπορεί να κάνει κάτι για να περιορίσει τη χρήση του υπολογιστή.

- Ενασχόληση αρχικώς με ηπιότερες και όχι τόσο εθιστικές λειτουργίες του Διαδικτύου, όπως είναι η αποστολή ηλεκτρονικών μηνυμάτων, και σταδιακή μετάβαση σε πιο διαδραστικές διαδικτυακές λειτουργίες όπως τα δωμάτια συνομιλιών (chat room), οι ομάδες ειδήσεων ή ακόμη και τα αποκαλούμενα κοινωνικά παιχνίδια όπως το «Second Life», στο οποίο κάθε χρήστης φτιάχνει μια νέα «εικονική» διαδικτυακή ζωή με όλες τις εκφάνσεις της (αξίζει να σημειωθεί ότι έχει ήδη προκληθεί θόρυβος σχετικά με τέτοιου είδους παιχνίδια, καθώς σε κάποιες περιπτώσεις η «εικονική» ζωή του χρήστη παρενέβαινε στη φυσιολογική ζωή του, ενώ παράλληλα η πλατφόρμα του παιχνιδιού γινόταν έρμαιο παιδεραστών και διακινητών πορνογραφικού υλικού).

Όλα τα παραπάνω, όπως είναι επόμενο, προκαλούν σοβαρές επιπτώσεις σε διάφορους τομείς της λειτουργικότητας του ατόμου. Μειώνεται ο χρόνος που περνάει ο έφηβος με την οικογένειά του, περιορίζονται τα χόμπι και οι κοινωνικές συναναστροφές του, αυξάνεται ο κίνδυνος εμφάνισης παχυσαρκίας, μυοσκελετικών προβλημάτων και οφθαλμικών παθήσεων λόγω των πολλών ωρών- ακινησίας- μπροστά στην οθόνη. Παράλληλα, οι εθισμένοι στο Διαδίκτυο νεαροί παραμελούν τη σωματική τους υγιεινή, ενώ κάνουν πολλές απουσίες στο σχολείο με αποτέλεσμα ακόμη και να χάνουν τάξεις.

Όσον αφορά στην ηλικία των παιδιών που είναι «εθισμένα» στο διαδίκτυο μπορούμε να πούμε ότι το φαινόμενο μπορεί να εμφανιστεί σε εφήβους κατά την πρώιμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία. Είναι ωστόσο πιο συχνό κατά την μέση εφηβεία (15-17 ετών), κατά την οποία οι έφηβοι πειραματίζονται και σταδιακά αυτονομούνται, καθώς και

κατά την όψιμη εφηβεία (> 17 ετών).

Αυτό συμβαίνει διότι όσο ο έφηβος μεγαλώνει και πλησιάζει την μέση εφηβεία, ο πειραματισμός και η περιέργεια, η μη συνειδητοποίηση του κινδύνου και η φυσιολογική αντίδραση σε κάθε καταπίεση, γίνονται βασικά χαρακτηριστικά του (αποτελεί ακόμη αναπτυσσόμενο άτομο), και τον καθιστούν ευάλωτο και ευαίσθητο σε εξαρτήσεις. Οι περισσότεροι εξαρτημένοι έφηβοι ασχολούνται με «παιχνίδια», στο σπίτι ή τα internet café (Wu & Cheng, 2007).

Μπορεί να σταματήσουν το σχολείο, να απομονωθούν από την οικογένεια και τους φίλους, να είναι επιθετικοί με τους γονείς, να κλέβουν χρήματα από την οικογένεια για να «παίζουν», να ζουν σε ένα δωμάτιο, να μην τρώνε ή το αντίθετο (να παχύνουν πολύ), να μην γυμνάζονται και να μην κοιμούνται για 24ωρα. Μπορεί ακόμη να μην αλλάζουν ρούχα, να παραμελούν την υγιεινή τους και την καθαριότητα (Paul, Bryant, 2005).

Στην σύγχρονη επιστήμη ο όρος «εθισμός» χρησιμοποιείται συνήθως για να περιγράψει σωματικές εξαρτήσεις όπως αυτές που δημιουργεί το αλκοόλ και οι ναρκωτικές ουσίες. Σήμερα, ο όρος αυτός χρησιμοποιείται πλέον και για να περιγράψει τα άτομα που χρησιμοποιούν υπερβολικά το διαδίκτυο και είναι εξαρτημένα από αυτό.

Ο Beard (2005), θεωρεί ότι ένας από τους πιο ακριβείς όρους που περιγράφουν την εξάρτηση από το διαδίκτυο είναι η παθολογική χρήση γιατί δεν εμπεριέχει θεωρητικούς συνειρμούς.

Η Young (1996) ήταν η πρώτη ερευνήτρια που ερεύνησε εμπειρικά την υπερβολική χρήση του διαδικτύου και την περιέγραψε βάση των κριτηριών DSM-IV που χρησιμοποιούνται στον εθισμό του τζόγου. Σύμφωνα λοιπόν με την Young (1996), η προβληματική χρήση του διαδικτύου, όπως την ονόμασε, είναι ένας όρος που περιγράφει περισσότερα από ένα προβλήματα που σχετίζονται με την χρήση του διαδικτύου. Πιο συγκεκριμένα, περιλαμβάνει τις εξής κατηγορίες:

α) τον εθισμό σε ιστοσελίδες που εμπεριέχουν σεξουαλικό περιεχομένου. Οι άνθρωποι που ανήκουν σε αυτή την κατηγορία

επισκέπτονται υπερβολικά αυτού του είδους τις ιστοσελίδες για να έχουν εικονικό σεξ.

β) τον εθισμό σε σχέσεις μέσω του διαδικτύου. Οι σχέσεις αυτές είναι εικονικές.

γ) τον εθισμό σε πάθη. Ως πάθη μπορούν να οριστούν ο τζόγος που μπορεί ο χρήστης να παίξει ηλεκτρονικά αλλά και οι υπερβολικές και συνεχείς αγορές που γίνονται μέσω διαδικτύου.

δ) τον εθισμό στην αναζήτηση πληροφοριών. Στη περίπτωση αυτή ο χρήστης αναζητεί συνέχεια πληροφορίες σε βάσεις δεδομένων ή «σερφάροντας».

ε) τον εθισμό στη χρήση υπολογιστή όπως π.χ. το παίξιμο παιχνιδιών.

Ο Griffiths (1998), όρισε τον εθισμό στο διαδίκτυο ως εθισμό της τεχνολογίας, ως έναν εθισμό δηλαδή που προϋποθέτει την αλληλεπίδραση ανάμεσα σε έναν άνθρωπο και μία μηχανή. Τον εθισμό ο Griffiths (1998), τον παρουσιάζει μέσω συγκεκριμένων χαρακτηριστικών που έχει ο χρήστης (Griffiths, 1998):

1. Την προβολή. Η χρήση του διαδικτύου γίνεται για τον χρήστη η πιο σημαντική δραστηριότητα του και προσανατολίζεται αποκλειστικά προς αυτήν.

2. Η αλλαγή διάθεσης. Οι άνθρωποι που ασχολούνται συνέχεια με το διαδίκτυο περιγράφουν ότι όταν το κάνουν είναι ευχαριστημένοι και ευτυχισμένοι.

3. Η ανοχή. Οι άνθρωποι διαθέτουν υπομονετικά όλο τον χρόνο τους στη χρήση του διαδικτύου προκειμένου να έχουν τα αποτελέσματα που θέλουν.

4. Η στέρηση. Ο χρήστης που είναι εθισμένος στο διαδίκτυο, όταν δεν μπορεί να έχει πρόσβαση σε αυτό ή περιορίζει τη χρήση του νιώθει συμπτώματα στέρησης όπως δυσαρέσκεια, στενοχώρια, κ.α.

5. Η σύγκρουση. Οι εθισμένοι στο διαδίκτυο συγκρούονται συχνά με

τους ανθρώπους του περιβάλλοντος τους για την δραστηριότητα τους αλλά και για άλλους λόγους.

6. Η υποτροπή. Ακόμα και αν σταματήσουν ή περιορίσουν τη χρήση του διαδικτύου οι εθισμένοι έχουν μία τάση χρήσης του και πάλι (Griffiths, 1998).

ΚΕΦΑΛΑΙΟ 2. DEEP WEB

Το Deep Web (επίσης γνωστό και ως Deepnet, Undernet, το αόρατο Web ή το κρυμμένο Web) αναφέρεται στο περιεχόμενο του World Wide Web που δεν ανήκει στον Επιφανειακό Web (Surface Web), το οποίο ευρετηριάζεται από μία συνηθισμένη μηχανή αναζήτησης (de Viana et al., 2010).

Ο Mike Bergman, ιδρυτής του Bright Planet, που επινόησε τη φράση, είχε πει πως το να ψάχνει κανείς στο Internet σήμερα είναι σαν να σέρνει ένα δίχτυ στην επιφάνεια του ωκεανού: πολλά μπορεί να πιαστούν στο δίχτυ, αλλά υπάρχει ένας πλούτος πληροφοριών που βρίσκονται βαθιά και επομένως δεν μπορούν να πιαστούν. Οι περισσότερες πληροφορίες του Web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες, και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Οι παραδοσιακές μηχανές αναζήτησης δεν μπορούν να ανακτήσουν το περιεχόμενο του deep Web. Αυτές οι σελίδες δεν υπάρχουν μέχρι να δημιουργηθούν δυναμικά ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Το deep Web είναι αρκετές τάξεις μεγέθους μεγαλύτερο από το επιφανειακό Web (Wright, 2009).

2.1 Μέγεθος

Σύμφωνα με εκτιμήσεις που έγιναν σε μία μελέτη στο Πανεπιστήμιο της Καλιφόρνιας, Μπέρκλεϋ (University of California, Berkeley) το 2001 (Bergman, 2001), το deep Web αποτελείται περίπου από 91.000 terabytes. Αντίθετα το επιφανειακό Web (που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης) είναι περίπου 167 terabytes. Η Βιβλιοθήκη του Κογκρέσου, υπολογίστηκε πως το 1997 είχε 3.000 terabytes. Το 2011, το YouTube υπολογίζεται ότι είχε αποθηκευμένα περίπου 200 εκατομμύρια βίντεο, συνολικού μεγέθους 5 petabytes ή 5000 terabytes. Ο υπολογισμός του μεγέθους του web διαφέρει από πηγή σε πηγή και έτσι υπάρχει ένα μεγάλο περιθώριο λάθους και κανένας αριθμός δε μπορεί να θεωρηθεί ως ακριβής

(Michael, 2009). Ωστόσο σχετικά με τον αριθμό των πηγών του deep Web υπάρχουν πιο ακριβείς εκτιμήσεις: Το 2004 ο He ανακάλυψε 300.000 deep web sites σε ολόκληρο το Web (He et al., 2007) και σύμφωνα με τον Shestakov, περίπου 14.000 deep web sites υπήρχαν στο Ρώσικο τμήμα του Web το 2006 (Denis, 2011).

2.2 Πληροφορίες του Deep Web

Οι πληροφορίες του Deep Web ανήκουν σε μία ή περισσότερες από τις παρακάτω κατηγορίες (Madhavan, et al., 2009):

Δυναμικά παραγόμενο περιεχόμενο: δυναμικές ιστοσελίδες οι οποίες δημιουργούνται ως αποτέλεσμα της εκτέλεσης κάποιας επερώτησης (query) ή προσπελαύνονται μόνο μέσω κάποιας φόρμας.

Μη συνδεδεμένο περιεχόμενο: ιστοσελίδες οι οποίες δεν περιέχουν συνδέσμους από άλλες ιστοσελίδες, εμποδίζοντας έτσι τα προγράμματα που κάνουν Web crawling να επισκεφθούν το περιεχόμενό τους.

Ιδιωτικό Web: ιστότοποι που απαιτούν εγγραφή (registration) και κωδικό πρόσβασης.

Περιεχόμενο περιορισμένης πρόσβασης: ιστότοποι που περιορίζουν την πρόσβαση στις σελίδες τους με τεχνικό τρόπο (π.χ. χρησιμοποιώντας το Robots Exclusion Standard, CAPTCHAs, ή το no-cache Pragma στις επικεφαλίδες του πρωτοκόλλου HTTP, τα οποία απαγορεύουν στις μηχανές αναζήτησης να πλοηγούνται στις ιστοσελίδες τους) (Tikk, Kardkovács & Magyar, 2007).

Περιεχόμενο που δεν είναι σε μορφή HTML: κείμενα που συμπεριλαμβάνονται σε multimedia αρχεία (εικόνες ή video) ή που έχουν συγκεκριμένη μορφή την οποία δεν μπορούν να χειριστούν οι μηχανές αναζήτησης.

Κείμενα που χρησιμοποιούν το παλαιότερο πρωτόκολλο Gopher και

αρχεία που βρίσκονται σε διακομιστές FTP και τα οποία δεν μπορούν να εντοπιστούν από τις περισσότερες μηχανές αναζήτησης. Οι μηχανές αναζήτησης όπως η Google δεν δεικτοδοτούν ιστοσελίδες που βρίσκονται έξω από το πρωτόκολλο HTTP (Madhavan et al., 2008).

2.3 Προσπέλαση

Οι μηχανές αναζήτησης ανακαλύπτουν περιεχόμενο στο Web, χρησιμοποιώντας web crawlers που ακολουθούν συνδέσμους. Αυτή η τεχνική είναι ιδανική για να ανακαλύψει κανείς πληροφορίες στο Επιφανειακό Web (Surface Web) αλλά είναι αναποτελεσματική στην εύρεση πληροφοριών από το deep Web. Για παράδειγμα, αυτοί οι crawlers δεν προσπαθούν να βρουν δυναμικές ιστοσελίδες που προέρχονται από ερωτήματα σε βάσεις δεδομένων επειδή τα ερωτήματα αυτά θα ήταν θεωρητικά άπειρα (Wright, 2009).

Το 2005, η Yahoo! έκανε ένα μικρό κομμάτι του deep Web ερευνήσιμο με τη χρήση των Yahoo! Subscriptions. Αυτή η μηχανή αναζήτησης ψάχνει μόνο μέσω λίγων συνδρομητικών ιστοτόπων. Κάποιοι τέτοιοι ιστότοποι εμφανίζουν όλο τους το περιεχόμενο στα robots των μηχανών αναζήτησης, έτσι ώστε να εμφανίζονται στις αναζητήσεις των χρηστών, αλλά μετά εμφανίζουν στους χρήστες μία σελίδα για login ή συνδρομή.

2.4 Διαδικασία πρόσβασης στο Deep Web

Χρησιμοποιώντας τις μηχανές αναζήτησης όπως το Google, είμαστε σε θέση να ψάξουμε μόνο το 1% των διαθέσιμων δεδομένων στο διαδίκτυο. Τα δεδομένα (ιστοσελίδα) τα οποία είναι δυνατό να βρεθούν μέσω των μηχανών αναζήτησης είναι γνωστά ως «surface web» (επιφανειακό διαδίκτυο), ενώ οι ιστοσελίδες που δε μπορούν να βρεθούν εύκολα αναφέρονται με τον όρο «Deep Web» (Madhan, 2015).

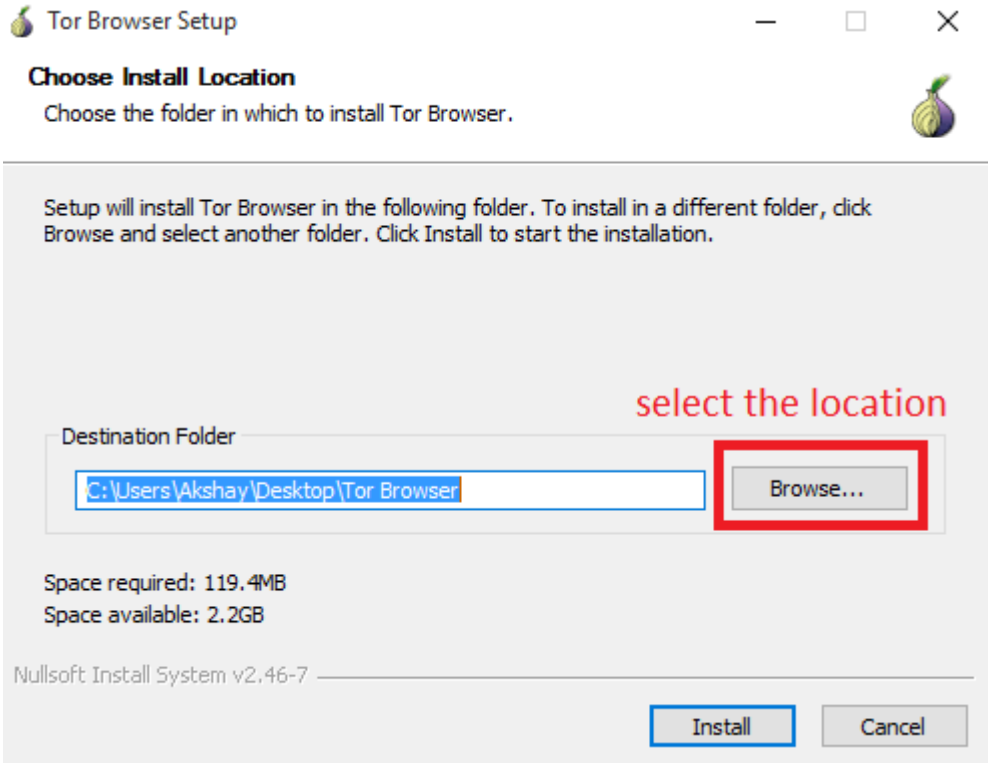
Σε τεχνικούς όρους, το μη καταχωρημένο τμήμα του Διαδικτύου

ονομάζεται Deep web ενώ το καταχωρημένο τμήμα του Διαδικτύου ονομάζεται Surface web. Παρακάτω ακολουθεί οδηγός για το πώς να έχουν πρόσβαση σε Deep ιστοσελίδες που χρησιμοποιούν το πρόγραμμα περιήγησης Tor. Δεν είναι προσβάσιμο το deep internet από ένα κανονικό web browser όπως ο Mozilla ή το Google Chrome. Για να αποκτήσετε πρόσβαση στο deep web, θα πρέπει να έχετε ένα ειδικό πρόγραμμα περιήγησης κρυπτογράφησης που ονομάζεται Tor και το οποίο επιτρέπει να ψάξετε σε ανώνυμα χωρίς να φύγετε από την αρχική σας ταυτότητα.

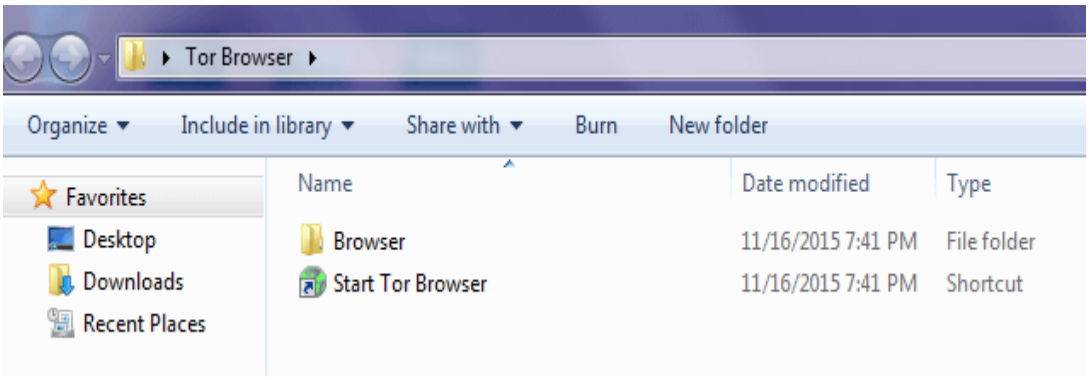
Βήμα 1: Εγκαταστήστε το Tor Browser Bundle

1. Στο πρόγραμμα περιήγησης σας μεταβείτε στο torproject.com και κάντε κλικ στο μπλε κουμπί για να κατεβάσετε το Tor Browser Bundle.

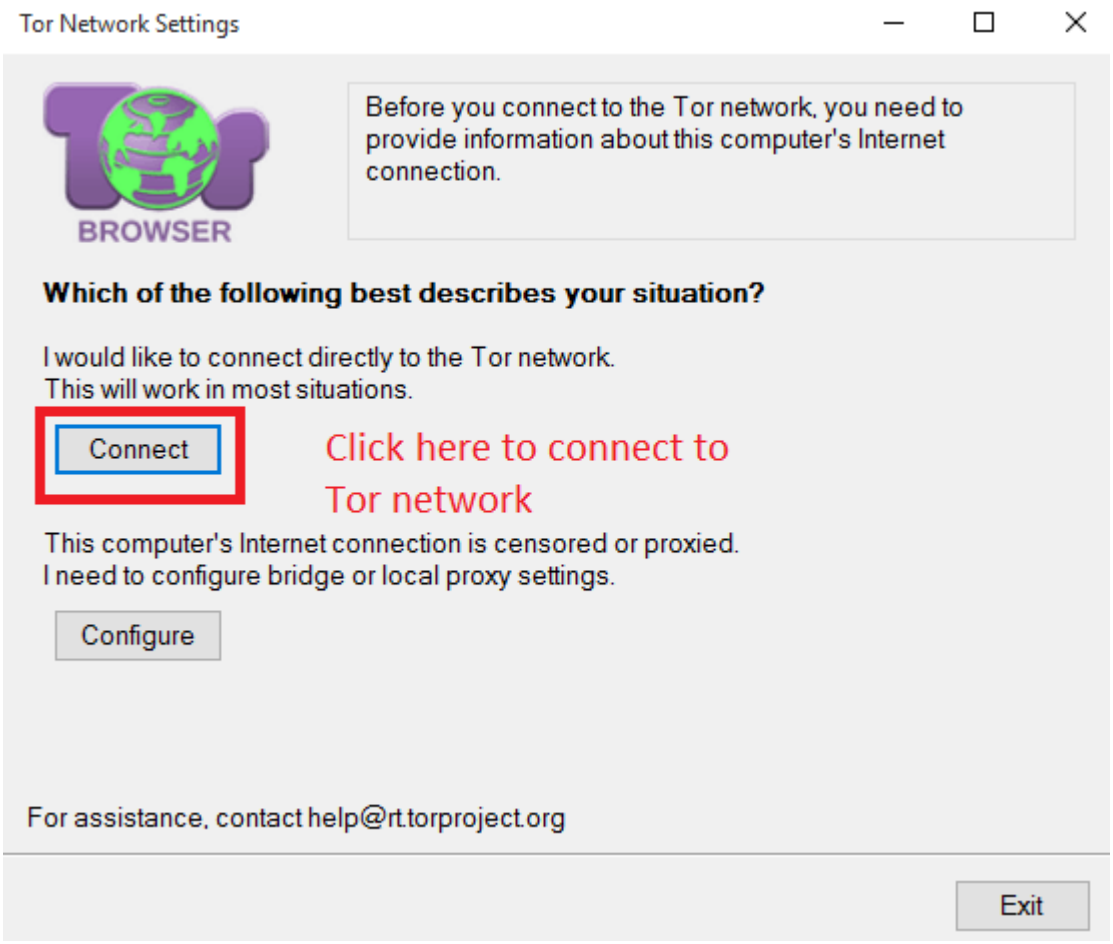
2. Μόλις ολοκληρωθεί η λήψη, κάνουμε διπλό κλικ για να τρέξει, επιλέγουμε τη θέση εγκατάστασης και, τέλος, κάνουμε κλικ στο κουμπί εγκατάστασης.



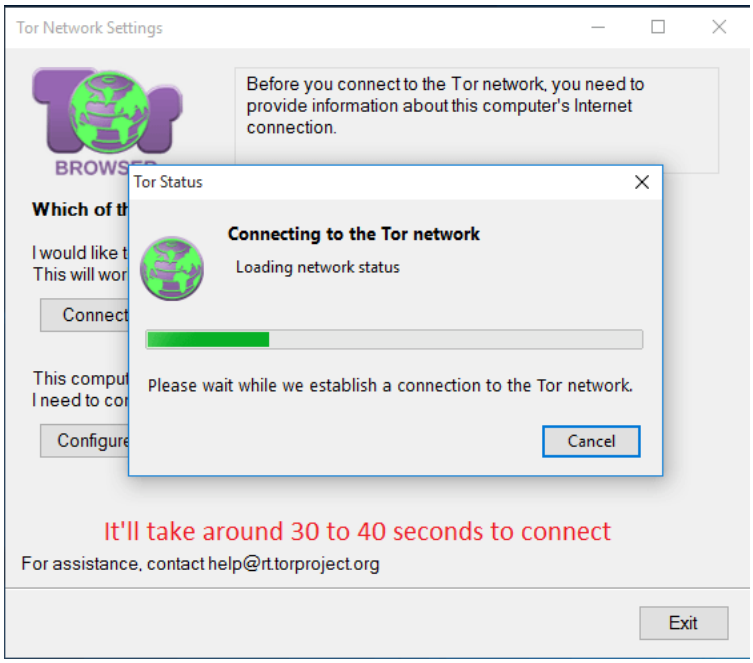
3. Μετά την εγκατάσταση του Tor, ανοίγουμε το φάκελο στον οποίο έχουμε εγκαταστήσει το προγράμματος περιήγησης Tor και στη συνέχεια κάνουμε κλικ στο πρόγραμμα περιήγησης έναρξη Tor.



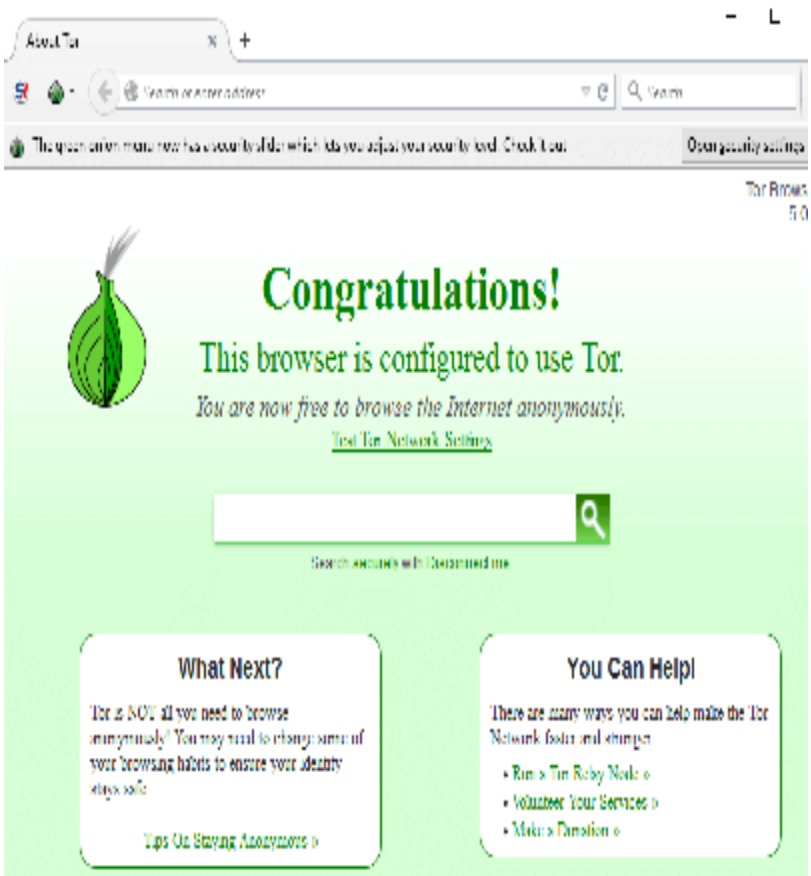
4. Τώρα κάνουμε κλικ στη Σύνδεση.



5. Αφού κάνουμε κλικ στο κουμπί Connect, θα πάρει περίπου 10-20 δευτερόλεπτα για να δημιουργήσει μια ασφαλή σύνδεση που σας συνδέει με το δίκτυο Tor μέσω μιας αναμετάδοσης που περνά ουσιαστικά μέσα από πολλές διαφορετικές συνδέσεις ανωνυμοποίησης της ταυτότητάς σας.



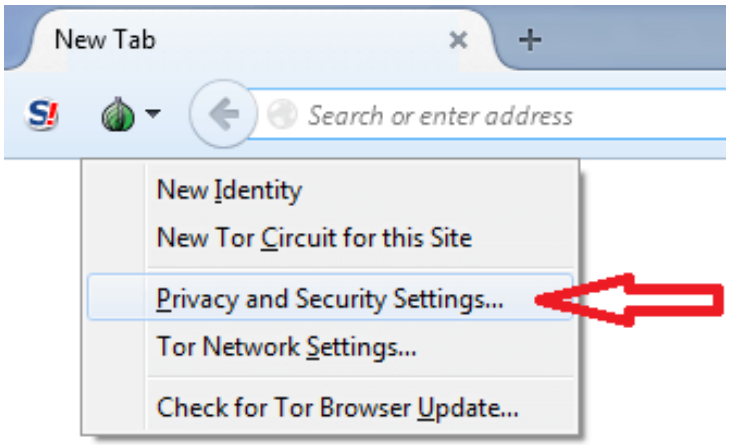
6. Αφού το πρόγραμμα περιήγησης Tor έχει ξεκινήσει θα δείτε το μήνυμα συγχαρητήρια, όπως φαίνεται στο παρακάτω screenshot.



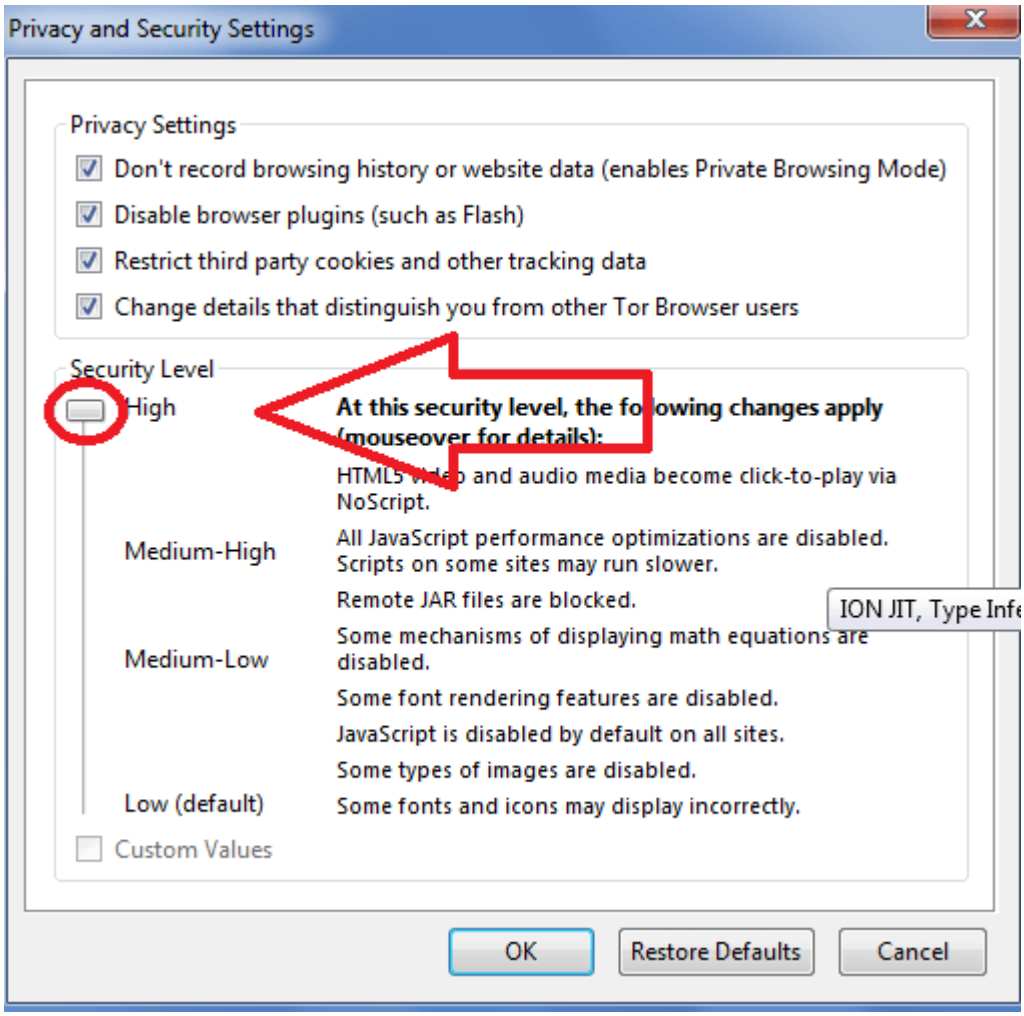
Φαίνεται όπως θα περίμενε κανείς, όπως το Firefox, διότι είναι απλώς μια πιο εμπεριστατωμένη έκδοση - απλά με ένα σωρό add-ons. Αυτό ήταν, τώρα έχετε συνδεθεί με επιτυχία στο δίκτυο Tor.

Βήμα-2: Διαμόρφωση του Tor Browser για καλύτερη ασφάλεια

1. Στο πρόγραμμα περιήγησης Tor, κάντε κλικ στο εικονίδιο με το πράσινο κρεμμύδι και στη συνέχεια κάντε κλικ στο Privacy and Security, όπως φαίνεται στην παρακάτω εικόνα.



2. Τώρα αλλάξετε το επίπεδο ασφαλείας από χαμηλό σε υψηλό και στη συνέχεια κάντε κλικ στο OK.



Αυτό είναι, τώρα έχετε διαμορφώσει με επιτυχία το Tor browser σας για μεγαλύτερη ανωνυμία.

Βήμα-3: Ψάχνοντας URL (Ενιαίος Εντοπιστής Πόρων) στο deep web

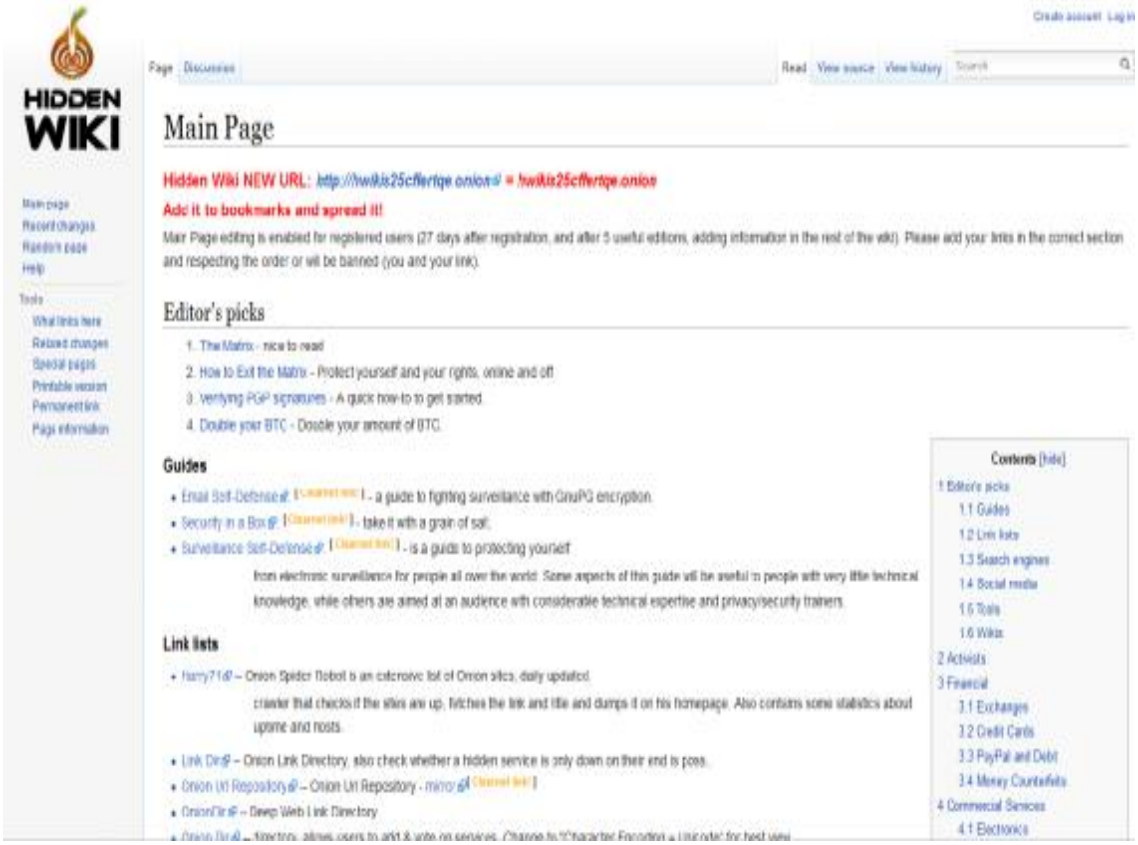
Έτσι τώρα που έχετε εγκαταστήσει και ρυθμίσει το πρόγραμμα περιήγησης Tor στο σύστημά σας με επιτυχία, το επόμενο βήμα είναι να βρεθεί μια διεύθυνση URL ενός deep web. Η εύρεση ενός συνδέσμου εργασίας είναι ένα δύσκολο έργο, διότι συνδέσεις στο deep web δεν είναι σταθερές, επειδή αλλάζουν την ηλεκτρονική διεύθυνση (.onion) από τις σελίδες τακτικά, για να είναι δύσκολο να εντοπιστούν. Αλλά ευτυχώς υπάρχουν μερικοί κατάλογοι .onion και μηχανές αναζήτησης διαθέσιμες από όπου μπορείτε εύκολα να βρείτε τις deep web διευθύνσεις (URL). Παρακάτω είναι μερικά από τους δημοφιλής καταλόγους

.onion στο διαδίκτυο:

Κατάλογοι

1. http: //hwikis25cffertqe.onion
2. http://thehiddenwiki.org

Αν είστε αρχάριος τότε το Hiddenwiki είναι το καλύτερο μέρος για να ξεκινήσετε με το deep web. Με τη βοήθεια της σελίδας Hiddenwiki μπορείτε εύκολα να βρείτε σύνδεσμους .onion των δικτυακών τόπων που φιλοξενούνται στο deep web.

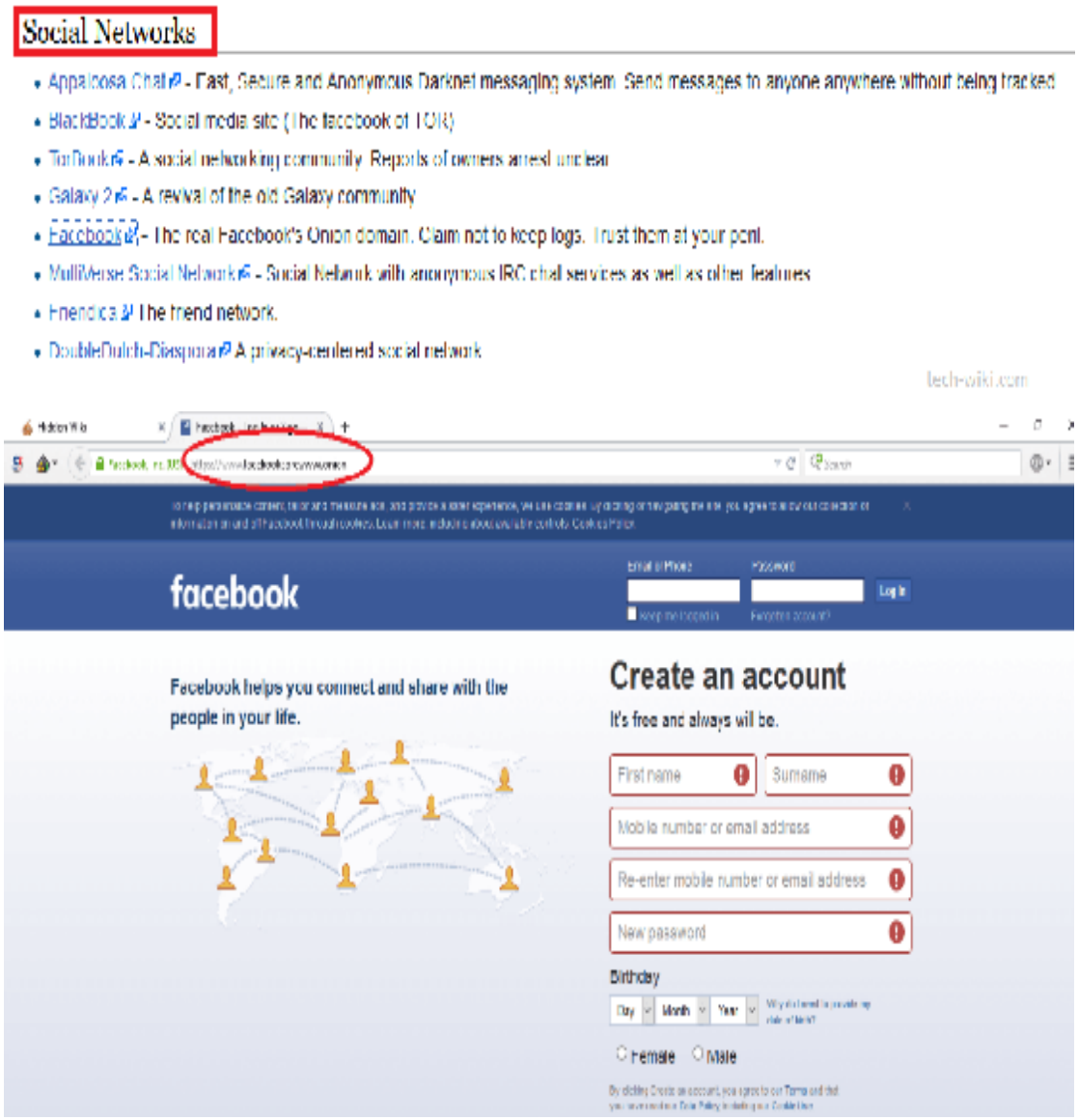


Λάβετε υπόψη σας ότι ορισμένες από τις διαθέσιμες προαναφερόμενες ιστοσελίδες μπορεί να σας οδηγήσουν σε λάθος μέρος των κρυφών web, έτσι ώστε το να επισκεφθείτε αυτούς τους δεσμούς είναι με δική σας ευθύνη.

Έτσι τώρα ας δούμε πώς μπορείτε να βρείτε κάτι που ψάχνετε στο deep web χωρίς να αποκαλύψει την ταυτότητά σας. Σημειώστε ότι οι εξηγήσεις που θα δοθούν είναι πραγματικά παραδείγματα, έτσι ώστε να μπορείτε εύκολα να

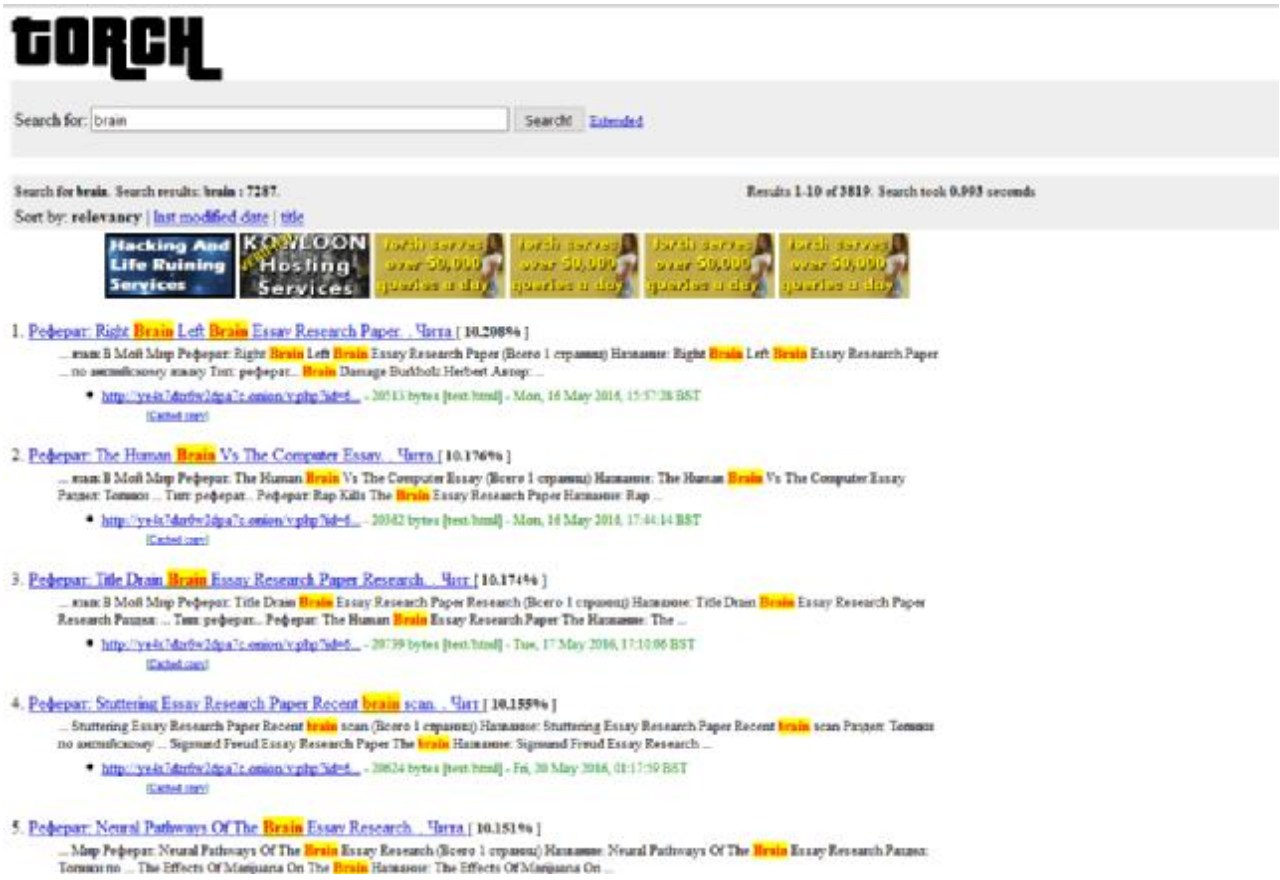
κατανοήσετε τα βασικά.

Για παράδειγμα, ας υποθέσουμε ότι θέλετε να συνομιλήσετε με κάποιον χωρίς να αποκαλύψει την αρχική ταυτότητα και να ψάχνετε για εάν φιλικό προς το χρήστη του ιστοτόπο, όπως το facebook, στην περίπτωση αυτή, μπορείτε να επισκεφθείτε το »hwikis25cffertqe.onion'site, μετακινηθείτε προς τα κάτω λίγο στην ενότητα «Social Networks section» και, τέλος κάντε κλικ σε οποιοδήποτε από τους συνδέσμους σε αυτή την ενότητα για να αποκτήσετε πρόσβαση σε ιστοσελίδες κοινωνικών μέσων μαζικής ενημέρωσης, όπως φαίνεται στην παρακάτω εικόνα.



Το Facebook ισχυρίζεται ότι δεν θα κρατήσει τα αρχεία καταγραφής της δραστηριότητας περιήγησής σας. Εμπιστευθείτε τους με δικό σας ρίσκο.

Παράδειγμα-2: Ας πούμε ότι θέλετε να αναζητήσετε ολόκληρο το deep web, σε αυτή την περίπτωση μηχανές αναζήτησης όπως το DuckDuckGo και Torch είναι πρακτικές για εσάς. Χρησιμοποιώντας αυτές τις μηχανές αναζήτησης, μπορείτε εύκολα να αναζητήσετε το σύνολο του Deep Web σε θέμα λεπτών. Στη συγκεκριμένη περίπτωσή, έχω κάνει αναζήτηση για τη λέξη "εγκέφαλος" στη μηχανή αναζήτησης Torch και μου επέστρεψε τα παρακάτω αποτελέσματα:



Στη προσπάθεια να επισκεφθούμε κάποιες από τις συνδέσεις στα αποτελέσματα αναζήτησης, αυτό που βρήκαμε είναι το αποτέλεσμα της αναζήτησης δεν είναι πολύ σχετικό. Οπότε μην περιμένετε πολλά από αυτές τις μηχανές αναζήτησης. Υπάρχουν πολλά διαφορετικά links που μπορείτε να πάτε.

Για να αυξήσετε την ανωνυμία σας περαιτέρω, προτείνετε να ακολουθήσετε τις παρακάτω προφυλάξεις ασφαλείας

1. Πηγαίνετε στις Ρυθμίσεις συστήματος (Πίνακας ελέγχου) και βεβαιωθείτε αν το Τείχος προστασίας του συστήματός σας είναι ενεργοποιημένο ή όχι. Αν όχι, ενεργοποιήστε το πριν μπείτε στο hidden internet.

2. Απενεργοποιήστε το JavaScript και cookies στο Tor browser σας για να αυξήσει περαιτέρω την ανωνυμία σας.

3. Κλείστε όλες τις άλλες εφαρμογές, όπως το Chrome, το uTorrent, το Internet download manager, κλπ που χρησιμοποιεί το διαδίκτυο όταν έχετε πρόσβαση με TOR.

4. Καλύψτε τη κάμερα του υπολογιστή σας, χρησιμοποιώντας την ταινία ή οποιοδήποτε άλλο υλικό, έτσι ώστε να μην μπορεί να χρησιμοποιηθεί από blackhat χάκερς για να σας κατασκοπεύσει.

ΚΕΦΑΛΑΙΟ 3. ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ TREND MICRO

Οι πληροφορίες που παρέχονται στο παρόν αποτελούν γενικές πληροφορίες και για εκπαιδευτικό σκοπό μόνο. Δεν προορίζονται και δεν πρέπει να ερμηνευτούν ότι αποτελεί νομική συμβουλή. Οι πληροφορίες που περιέχονται στο παρόν μπορεί να μην ισχύουν σε όλες τις περιπτώσεις και να μην αντανακλούν την πιο πρόσφατη κατάσταση.

Τίποτα από όσα περιέχονται στο παρόν δεν θα πρέπει να επικαλεστούν ή να ενεργοποιηθούν χωρίς το όφελος νομικών συμβουλών με βάση τα συγκεκριμένα πραγματικά δεδομένα και τις περιστάσεις που παρουσιάζονται και τίποτα στο παρόν δεν θα πρέπει να ερμηνευτεί διαφορετικά. Η Trend Micro διατηρεί το δικαίωμα να τροποποιήσει το περιεχόμενο του παρόντος εγγράφου σε οποιαδήποτε στιγμή χωρίς προηγούμενη ειδοποίηση.

Οι μεταφράσεις οποιουδήποτε υλικού σε άλλες γλώσσες έχει ως αποκλειστικό σκοπό την εξυπηρέτηση. Δεν εγγυάται ούτε υπονοείται η ακρίβεια της μετάφρασης. Εάν προκύψουν οποιεσδήποτε ερωτήσεις που σχετίζονται με την ακρίβεια της μετάφρασης, ανατρέξτε στην αρχική γλώσσα της επίσημης έκδοσης του εγγράφου. Τυχόν αποκλίσεις ή διαφορές που δημιουργήθηκαν στην μετάφραση δεν είναι δεσμευτικές και δεν έχουν καμία νομική ισχύ στους σκοπούς της συμμόρφωσης ή της εκτέλεσης (Ntoulas, Zerfos & Cho, 2004).

Αν και η Trend Micro καταβάλει εύλογες προσπάθειες για να συμπεριλαμβάνει ακριβείς και ενημερωμένες πληροφορίες στο παρόν, η Trend Micro δεν παρέχει καμία εγγύηση ή επίσημη δήλωση οποιουδήποτε είδους ως προς την ακρίβεια, την επικαιρότητα ή την πληρότητα. Συμφωνείτε ότι η πρόσβαση και η χρήση και η εμπιστοσύνη σε αυτό το έγγραφο και το περιεχόμενό του, αποτελεί δική σας ευθύνη. Η Trend Micro αποποιείται κάθε εγγυήσεως. οποιουδήποτε είδους, ρητής ή σιωπηρής.

Ούτε η Trend Micro ούτε και οποιοδήποτε μέρος που συμμετείχε στην δημιουργία, παραγωγή ή παράδοση αυτού του εγγράφου ευθύνεται για οποιαδήποτε συνέπεια, απώλεια ή ζημιά, συμπεριλαμβανομένης της άμεσης,

έμμεσης, ειδικής, επακόλουθης απώλειας επιχειρηματικών κερδών ή ειδικών ζημιών, που προέρχεται από την πρόσβαση, χρήση ή αδυναμία χρήσης ή σε σχέση με την χρήση αυτού του εγγράφου, ή σε τυχόν λάθη ή παραλείψεις στο περιεχόμενο αυτού. Η χρήση αυτών των πληροφοριών αποτελεί αποδοχή υπό την προϋπόθεση για χρήση «ως έχει».

Το ενδιαφέρον για το Deep Web κορυφώθηκε το 2013, όταν το FBI κατέβασε την αγορά Silk Road και εξέθεσε το περιβόητο σύστημα διακίνησης ναρκωτικών του Διαδικτύου. Ο Ross Ulbricht, γνωστός και ως Dread Pirate Roberts, κατηγορήθηκε για διακίνηση ναρκωτικών, συνωμοσία για ηλεκτρονική πειρατεία και ξέπλυμα χρήματος. Καθώς οι ειδήσεις τεχνικά αναφέρονταν στο Dark Web, εκείνο το τμήμα του Διαδικτύου που μπορεί να προσεγγιστεί μόνο με την χρήση ειδικού λογισμικού περιήγησης, το πιο δημοφιλές από τα οποία είναι το TOR (The Tor Project, 2015), άρχισαν να εξαπλώνονται τα αρνητικά στερεότυπα σχετικά με το Deep Web.

Το Deep Web είναι ένα μεγάλο τμήμα του Διαδικτύου που δεν είναι προσβάσιμο μέσω των μηχανών αναζήτησης, μόνο ένα μέρος του οποίου αντιπροσωπεύει τις εγκληματικές πράξεις όπως αποκάλυψε η καταγγελία του FBI (Ulbricht Criminal Complaint, 2015). Το Dark Web, εν τω μεταξύ, δεν είχε σχεδιαστεί αρχικά για να διευκολύνει τις ανώνυμες εγκληματικές δραστηριότητες.

Στην πραγματικότητα το TOR δημιουργήθηκε για να προστατεύσει τις επικοινωνίες και να ξεφύγει από την λογοκρισία ως ένας τρόπος για να διασφαλιστεί η ελευθερία του λόγου. Το Dark Web, για παράδειγμα, βοήθησε στην κινητοποίηση των διαδηλώσεων της Αραβικής Άνοιξης. Αλλά όπως κάθε εργαλείο, ο αντίκτυπός του μπορεί να αλλάζει, ανάλογα με την πρόθεση του χρήστη.

Μία μελέτη που δημοσιεύθηκε το 2013 με τίτλο «Deep Web and Cybercrime» και οι συμπληρωματικές δημοσιεύσεις που ακολούθησαν (Vincenzo et al., 2015; Vincenzo, 2013; Vincenzo, 2015), επεδίωξε την ανάλυση των διάφορων δικτύων που εγγυώνται την ανώνυμη πρόσβαση στο Deep Web στο πλαίσιο του εγκλήματος στον κυβερνοχώρο. Κατά την

διαδικασία οι συγγραφείς ανακάλυψαν ότι συμβαίνουν πολλά περισσότερα στα σκοτεινά τμήματα του Deep Web από την πώληση ψυχαγωγικών ναρκωτικών. Επίσης, έχει πλέον μετατραπεί σε ένα ασφαλές καταφύγιο που υποκρύπτει την εγκληματική δραστηριότητα τόσο στην ψηφιακή, όσο και στην πραγματική σφαίρα.

Η μελέτη αυτή παρουσιάζει κάποιες σχετικές στατιστικές που προέρχονται από την συλλογή διευθύνσεων Deep Web και εξετάζει προσεκτικά το πώς τα εγκληματικά στοιχεία περιηγούνται και επωφελούνται από το Deep Web. Παρέχει πραγματικά παραδείγματα που αποδεικνύουν ότι οι άνθρωποι πηγαίνουν εκεί όχι μόνο για να αγοράσουν λαθραία ανώνυμα, αλλά και για να ξεκινήσουν τις εγκληματικές τους δραστηριότητες στον κυβερνοχώρο, όπως είναι η κλοπή ταυτότητας, η έκθεση προσωπικοτήτων υψηλού προφίλ, το εμπόριο όπλων και στα πιο διεφθαρμένα σενάρια, η πρόσληψη δολοφόνων.

3.1 Deep Web

Το Deep Web αναφέρεται σε οποιοδήποτε περιεχόμενο στο Διαδίκτυο που για διάφορους λόγους δεν μπορεί ή δεν έχει συμπεριληφθεί στους καταλόγους ευρετηρίασης μηχανών αναζήτησης όπως το Google. Ο ορισμός αυτός περιλαμβάνει, επομένως τις δυναμικές ιστοσελίδων, τις μπλοκαρισμένες ιστοσελίδες (όπως εκείνες που σας ζητούν να απαντήσετε με ένα CAPTCHA για να αποκτήσετε πρόσβαση), τις ιστοσελίδες χωρίς σύνδεσμο, τις ιδιωτικές ιστοσελίδες (όπως εκείνες που απαιτούν διαπιστευτήρια σύνδεσης), περιεχόμενο μη HTML, contextual ή scripted και τα δίκτυα περιορισμένης πρόσβασης (Rong, Hao & Xin, 2012).

Τα δίκτυα περιορισμένης πρόσβασης καλύπτουν όλα εκείνα τα μέσα και τις υπηρεσίες που κανονικά δεν θα ήταν προσβάσιμες σε μια τυπική διαμόρφωση του δικτύου και έτσι προσφέρουν ενδιαφέρουσες δυνατότητες για την δράση κακόβουλων παραγόντων, μερικώς ή ολικώς απαρατήρητη από τον νόμο. Αυτά περιλαμβάνουν ιστοσελίδες με ονόματα τομέα που έχουν καταχωρηθεί στο Domain Name System (DNS) τις οποίες δεν

διαχειρίζεται το Internet Corporation for Assigned Names and Numbers (ICANN) και ως εκ τούτου, διαθέτουν διευθύνσεις URL με μη τυπικούς τομείς ανωτάτου επιπέδου (TLDs) που γενικά απαιτούν έναν συγκεκριμένο διακομιστή DNS για την σωστή επίλυση.

Άλλα παραδείγματα περιλαμβάνουν ιστοσελίδες που έχουν καταχωρήσει το όνομα τομέα τους σε ένα εντελώς διαφορετικό σύστημα από το πρότυπο DNS, όπως οι τομείς .BIT (McArdle, Sancho, 2015). Αυτά τα συστήματα δεν ξεφεύγουν μόνο από τους κανονισμούς όνομα τομέα που επιβάλλει η ICANN, αλλά ο αποκεντρωμένος χαρακτήρας των εναλλακτικών DNSs καθιστά επίσης πολύ δύσκολη την sinkhole δρομολόγηση για αυτούς τους τομείς, αν χρειαστεί.

Επίσης, στα δίκτυα περιορισμένης πρόσβασης περιλαμβάνονται και τα darknets ή ιστότοποι που φιλοξενούνται σε υποδομές που απαιτούν τη χρήση ειδικού λογισμικού για την πρόσβαση, όπως το TOR. Μεγάλο μέρος του ενδιαφέροντος του κοινού στο Deep Web βρίσκεται στις δραστηριότητες που συμβαίνουν στο εσωτερικό των darknets (Wang & Lochovsky, 2003).

Σε αντίθεση με άλλο περιεχόμενο του Deep Web, τα δίκτυα περιορισμένης πρόσβασης δεν ανιχνεύονται από τις μηχανές αναζήτησης αλλά όχι λόγω τεχνικών περιορισμών. Στην πραγματικότητα, οι υπηρεσίες της πύλης όπως το tor2web προσφέρουν έναν τομέα που επιτρέπει στους χρήστες να έχουν πρόσβαση σε περιεχόμενο που φιλοξενείται σε κρυφές υπηρεσίες.

Το Deep Web μπορεί να παρομοιαστεί με μια επιχείρηση υπόγειας εξόρυξης από την άποψη της κλίμακας, της αστάθειας και της πρόσβασης. Αν οτιδήποτε πάνω από το έδαφος αποτελεί μέρος περιεχομένου που μπορεί να αναζητηθεί στο Διαδίκτυο, τότε οτιδήποτε κάτω από αυτό είναι μέρος του Deep Web, το οποίο είναι εγγενώς κρυμμένο, πιο δύσκολο να αποκτήσει κανείς πρόσβαση και δεν είναι άμεσα ορατό.

3.2 Οι χρήσεις του Deep Web

Ένα έξυπνο πρόσωπο που θέλει να αγοράσει ψυχαγωγικά ναρκωτικά στο διαδίκτυο δεν θα θέλει να πληκτρολογήσει τις σχετικές λέξεις-κλειδιά σε ένα κανονικό πρόγραμμα περιήγησης. Θα πρέπει να μπει στο διαδίκτυο ανώνυμα χρησιμοποιώντας μια υποδομή που ποτέ δεν θα οδηγήσει τους ενδιαφερόμενους στην διεύθυνση IP ή την φυσική τοποθεσία του. Οι πωλητές των ναρκωτικών επίσης δεν θα ήθελαν να δημιουργήσουν ένα ηλεκτρονικό κατάστημα, η θέση του οποίου θα μπορούσε εύκολα να προσδιοριστεί από την αστυνομία ή η διεύθυνση IP του ιστότοπου στον πραγματικό κόσμο.

Υπάρχουν πολλοί άλλοι λόγοι, εκτός από την αγορά των ναρκωτικών, που οι άνθρωποι θέλουν να διατηρήσουν την ανωνυμία τους ή να δημιουργήσουν ιστοσελίδες οι οποίες δεν θα μπορούν να οδηγήσουν την φυσική τοποθεσία ή οντότητα. Οι άνθρωποι που θέλουν να προστατεύσουν την επικοινωνία τους από την κυβερνητική παρακολούθηση μπορεί να χρειάζονται την κάλυψη των darknets. Οι πληροφοριοδότες μπορεί να θέλουν να μοιραστούν τεράστιες ποσότητες εμπιστευτικών πληροφοριών προς τους δημοσιογράφους χωρίς να αφήσουν ίχνη. Οι αντιφρονούντες στα περιοριστικά καθεστώτα μπορεί να χρειάζονται την ανωνυμία προκειμένου να ενημερώνουν με ασφάλεια τον κόσμο για το τι συμβαίνει στην χώρα τους (Zerfos, P., Cho, J., & Ntoulas, 2005).

Από την άλλη πλευρά, οι άνθρωποι που θέλουν να σχεδιάσουν την δολοφονία ενός στόχου υψηλού προφίλ, θα θελήσουν ένα εγγυημένο, αλλά δύσκολο να εντοπιστεί μέσο. Άλλες παράνομες υπηρεσίες όπως η πώληση εγγράφων, π.χ. διαβατηρίων και πιστωτικών καρτών, απαιτούν επίσης μια υποδομή που θα εγγυάται την ανωνυμία. Το ίδιο μπορεί να ειπωθεί και για τους ανθρώπους που διαρρέουν προσωπικά στοιχεία των άλλων ανθρώπων, όπως διευθύνσεις και στοιχεία επικοινωνίας (Wang & Agrawal, 2009).

3.3 Το Surface Web έναντι του Deep Web

Όταν συζητάμε για το Deep Web, είναι αδύνατο να μην προκύψει συζήτηση και για το «Surface Web». Είναι ακριβώς το αντίθετο από το Deep Web, εκείνο το τμήμα του Διαδικτύου που οι συμβατικές μηχανές αναζήτησης μπορούν να καταχωρίσουν στο ευρετήριό τους και τα συνήθη προγράμματα περιήγησης μπορούν να έχουν πρόσβαση χωρίς την ανάγκη για ειδικό λογισμικό και διαμορφώσεις. Αυτό το Διαδίκτυο που επιδέχεται αναζήτησης μερικές φορές αποκαλείται και Clearnet.

3.4 Το Dark Web έναντι του Deep Web

Επικρατεί μεγάλη σύγχυση μεταξύ αυτών των δύο όρων, με κάποιους ερευνητές να τους εναλλάσσουν ελεύθερα. Αλλά το Dark Web δεν είναι το Deep Web, είναι μόνο ένα μέρος του Deep Web. Το Dark Web βασίζεται σε darknets ή δίκτυα όπου οι συνδέσεις πραγματοποιούντα μεταξύ έμπιστων ομοτίμων. Παραδείγματα συστημάτων του Dark Web περιλαμβάνουν το TOR, το Freenet, ή το Invisible Internet Project (I2P).

Επιστρέφοντας στην μεταφορά της εξόρυξης σήραγγας, το Dark Web θα είναι τα βαθύτερα τμήματα του Deep Web που απαιτούν εξαιρετικά εξειδικευμένα εργαλεία ή εξοπλισμό για την πρόσβαση. Βρίσκεται στο βαθύτερο σημείο κάτω από το έδαφος και οι ιδιοκτήτες του ιστοτόπου έχουν περισσότερους λόγους για να κρατήσουν το περιεχόμενό τους κρυφό.

3.5 Η κατάσταση του Deep Web

Πολλές μελέτες και εκθέσεις έχουν γραφτεί σχετικά με τις διάφορες δραστηριότητες που λαμβάνουν χώρα στο Deep Web (Vincenzo et al., 2015; McArdle, 2013; Vincenzo, 2013; Vincenzo, 2015). Διαβάζοντας αυτές, μπορεί να σκεφτεί κανείς ότι η συντριπτική πλειοψηφία των σελίδων στο Deep Web είναι αφιερωμένες στην πώληση παράνομων ναρκωτικών και όπλων, αλλά

αυτό δεν είναι όλη η ιστορία. Ενώ υπάρχουν, φυσικά, σελίδες για την πώληση ναρκωτικών και όπλων, ένα τεράστιο τμήμα των σελίδων του Deep Web αφορά σε πιο πεζά θέματα- προσωπικά ή πολιτικά blogs, ιστοσελίδες ειδήσεων, φόρουμ συζητήσεων, θρησκευτικούς χώρους, ακόμα και ραδιοφωνικούς σταθμούς. Ακριβώς όπως οι ιστοσελίδες που βρίσκονται στο Surface Web, αυτές οι εξειδικευμένες ιστοσελίδες του Deep Web απευθύνονται κυρίως σε άτομα που ελπίζουν να μιλήσουν με ομοϊδεάτες τους ανθρώπους, έστω και ανώνυμα.

Ραδιοφωνικός σταθμός του Deep Web για άτομα που θέλουν να ακούσουν μουσική τζαζ διατηρώντας την ανωνυμία τους

Λόγω της φύσης του, είναι αδύνατο να προσδιοριστεί ο αριθμός των σελίδων στο Deep Web και το περιεχόμενο σε κάθε δεδομένη στιγμή ή να αποκτηθεί μία ολοκληρωμένη εικόνα όλων όσων υπάρχουν σε αυτό. Το αόρατη και δύσκολη να εντοπιστεί φύση ορισμένων τμημάτων του Deep Web το καθιστά τέτοιο ώστε κανείς να μην μπορεί να πει με βεβαιότητα ότι έχει διερευνήσει πλήρως το βάθος του.

Για την στενή παρακολούθηση του Deep Web, η ομάδα της Trend Micro (Forward-Looking Threat Research Team) δημιούργησε ένα σύστημα, το Deep Web Analyzer που συλλέγει τις διευθύνσεις URL που συνδέονται με αυτό, συμπεριλαμβανομένων των κρυμμένα ιστοτόπων TOR και I2P, αναγνωριστικά πόρων Freenet και τομείς με μη συνηθισμένα TLDs και προσπαθεί να εξάγει σχετικές πληροφορίες που συνδέονται με αυτούς τους τομείς, όπως το περιεχόμενο σελίδων, τους συνδέσμους, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, τις κεφαλίδες HTTP, και ούτω καθεξής.

Κατά την διάρκεια δύο ετών από την χρήση του Deep Web Analyzer, συγκεντρώθηκαν περισσότερα από 38 εκατομμύρια γεγονότα από 576.000 διευθύνσεις URL, 244.000 εκ των οποίων φέρουν πραγματικό περιεχόμενο HTML. Μέχρι στιγμής, έχουν δημοσιευθεί δύο εκθέσεις σχετικά με τις υπόγεια φόρουμ που έχουν βρεθεί (Trend Micro Incorporated, 2015).

3.6 Ποιος είναι στο Deep Web;

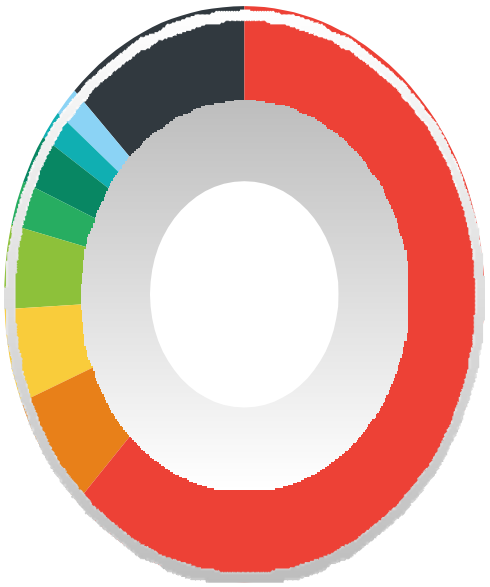
Είναι δύσκολο να πει κανείς σίγουρα ποιος υπάρχει στο Deep Web. Το επίπεδο της ανωνυμίας που προσφέρει στους χρήστες του το καθιστά δύσκολο ακόμη και για τους καλύτερες ερευνητές ασφάλειας να φτιάξουν το προφίλ τους. Μόνο με την εξέταση του περιεχομένου της ιστοσελίδας και της δημοτικότητας μπορεί να μετρηθεί η σύνθεση της βάσης των χρηστών της.

3.7 Κατανομή γλωσσών

Κατά τα τελευταία δύο έτη, έχει παρακολουθηθεί και αναλυθεί ένας τεράστιος αριθμός των ιστοσελίδων του Deep Web οι οποίες στην συνέχεια κατηγοριοποιήθηκαν με βάση την γλώσσα που χρησιμοποιούν. Αυτό έδωσε μία εικόνα για τις πιθανές περιοχές στις οποίες θα μπορούσαν να βασίζονται οι χρήστες του Deep Web.

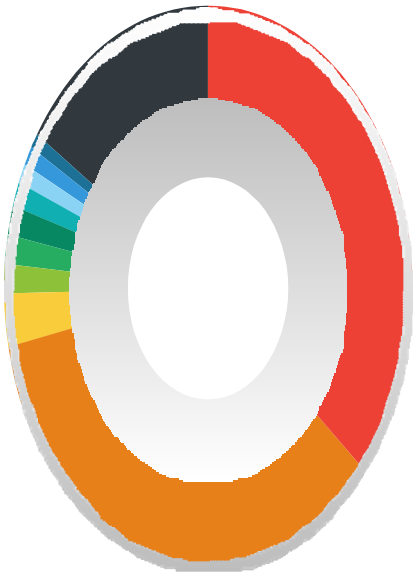
Σε ό,τι αφορά τον αριθμό των τομέων, η αγγλική ήταν η κύρια γλώσσα επιλογής από τουλάχιστον 2.154 ιστοσελίδες από τις 3.454 που

παρακολουθήθηκαν με επιτυχία. Αυτό αποτελεί σχεδόν το 62% του συνολικού αριθμού των ιστοτόπων. Ακολουθεί η ρωσική γλώσσας (228 ιστοσελίδες) και στην συνέχεια η γαλλική (μπορεί να περιλαμβάνει ιστοσελίδες από την Γαλλία και τον γαλλόφωνο Καναδά, 189 ιστοσελίδες).



Οι πιο δημοφιλείς γλώσσες με βάση τον αριθμό των τομέων που περιέχουν ιστοσελίδες που τις χρησιμοποιούν

Εξετάζοντας την κατανομή των γλωσσών με βάση τον αριθμό των διευθύνσεων URL, η ρωσική υπερτερεί της αγγλικής γλώσσας διότι, παρά το γεγονός ότι οι ιστοσελίδες είναι λιγότερες, ο αριθμός των ιστοσελίδων που χρησιμοποιούν την ρωσική ήταν μεγαλύτερος. Επί του παρόντος, υπάρχει ένα ιδιαίτερα μεγάλο ρωσικό φόρουμ που δεν συνδέεται άμεσα με κακόβουλες δραστηριότητες, αλλά αντικατοπτρίζεται και στο TOR και στο I2P κάτι που από μόνο του προστίθεται στον συνολικό αριθμό των ρωσικών ιστοσελίδες.



Ρωσικά	41.40%
Αγγλικά	40.74%
Κορεατικά	3.71%
Γαλλικά	2.00%
Βουλγάρικα	1.89%
Πολωνικά	1.67%
Γερμανικά	1.66%
Φινλανδικά	1.31%
Πορτογαλικά	1.25%
Καταλανικά	1.12%
Άλλη	3.25%

Οι πιο δημοφιλείς γλώσσες με βάση τον αριθμό των διευθύνσεων URL με περιεχόμενο που τις χρησιμοποιεί

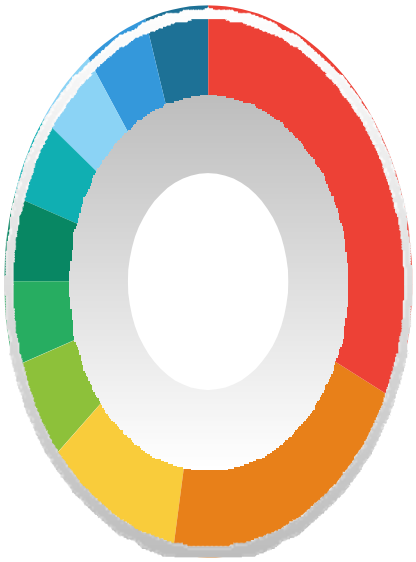
3.8 Κοινό προφίλ των χρηστών

Όπως αναφέρθηκε προηγουμένως, το προφίλ των χρηστών του Deep Web είναι δύσκολο να καθοριστεί. Περισσότερο από ότι για την γλώσσα, η πιο κοντινή και πιο αξιόπιστη εκτίμηση μπορεί πιθανώς να προέρχεται από την εξέταση των διαφόρων πωλητών της αγοράς. Αυτό έδωσε μια ιδέα για το τι κάνει τα δίκτυα όπως το TOR και το I2P να φαίνονται ελκυστικά.

Για την λήψη αξιόπιστων πληροφοριών, οι συγγραφείς απευθύνθηκαν

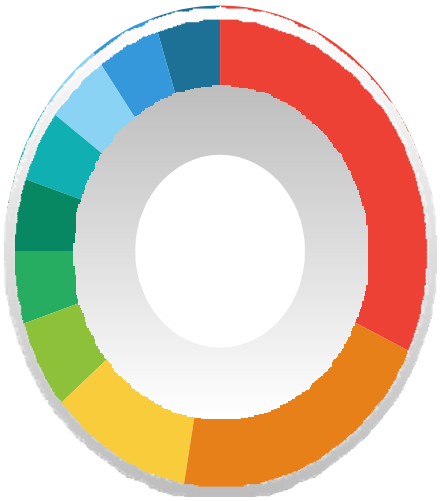
στα δεδομένα που είναι διαθέσιμα στην ιστοσελίδα https://dnstats.net/-a, η οποία ειδικεύεται σε δραστηριότητες παρακολούθησης σε όλες τις αγορές darknet.

Μια ανάλυση από τους κορυφαίους 15 πωλητές σε όλες τις αγορές έδειξε ότι τα ήπια φάρμακα ήταν τα πλέον ανταλλασσόμενα αγαθά στο Deep Web. Ακολουθούν τα φαρμακευτικά προϊόντα όπως το Ritalin και το Xanax, τα σκληρά ναρκωτικά, ακόμα και τα πειρατικά παιχνίδια και οι ηλεκτρονικοί λογαριασμοί. Τα δεδομένα αυτά υποστηρίζουν την άποψη ότι η πλειοψηφία των χρηστών του Deep Web τουλάχιστον εκείνων που συχνάζουν στις κορυφαίες αγορές, το επισκέπτονται για να αγοράσουν παράνομα ναρκωτικά.



- Κάνναβη 31.60%
- Φαρμακευτικά προϊόντα 21.05%
- MDMA 10.53%
- LSD 5.26%
- Μεθαμφεταμίνη 5.26%
- Μανιτάρια 5.26%
- Ηρωίνη 5.26%
- Σπόροι 5.26%
- Βιντεοπαιχνίδια 5.26%
- Λογαριασμοί 5.26%

Κατανομή πωλητών με βάση τα δεδομένα που αντλήθηκαν την 3 Ιουνίου 2015



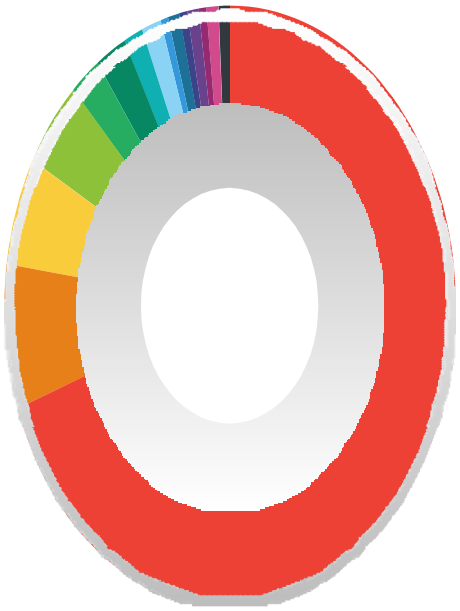
Κάνναβη	27.28%
Φαρμακευτικά προϊόντα	22.39%
MDMA	14.43%
LSD	7.47%
Μεθαμφεταμίνη	3.93%
Μανιτάρια	3.41%
Ηρωίνη	3.31%
Σπόροι	3.92%
Βιντεοπαιχνίδια	6.93%
Λογαριασμοί	6.93%

Κατανομή αγοραστών με βάση τα δεδομένα που αντλήθηκαν την 3 Ιουνίου 2015

3.9 Τι είναι αυτό που κάνει το Deep Web?

Πολλοί χρήστες μπορεί να μην γνωρίζουν ότι υπάρχει κάτι περισσότερο από τις συνηθισμένες ιστοσελίδες στο Deep Web. Με βάση τα δεδομένα και την διετή έρευνα, οι συγγραφείς ομαδοποίησαν τις διευθύνσεις URL σύμφωνα με το σχήμα τους URI (HTTP, HTTPS, FTP, κλπ).

Σχεδόν 22.000 των συλλεχθέντων τομέων σχετίζονται είτε με το πρωτόκολλο HTTP ή HTTPS, καθώς φιλοξενούν κυρίως δεδομένα. Αλλά αν θελήσουμε να τα φιλτράρουμε, τότε απομένουν ενδιαφέροντα δεδομένα.



IRC	99
IRCS	11
Gopher	8
XMPP	7
FTP	3
Telnet	3
Webcal	2
News	2
Mailto	1
SMTP	1
POP	1
Git	1
IMAP	1
RHTTP	1
Mumble	1

Πρωτόκολλα που βρέθηκαν στο Deep Web, εκτός από τα HTTP / HTTPS

Περισσότεροι από 100 τομείς χρησιμοποιούν το IRC ή IRCS πρωτόκολλο συνήθως διακομιστές συνομιλίας που μπορούν να

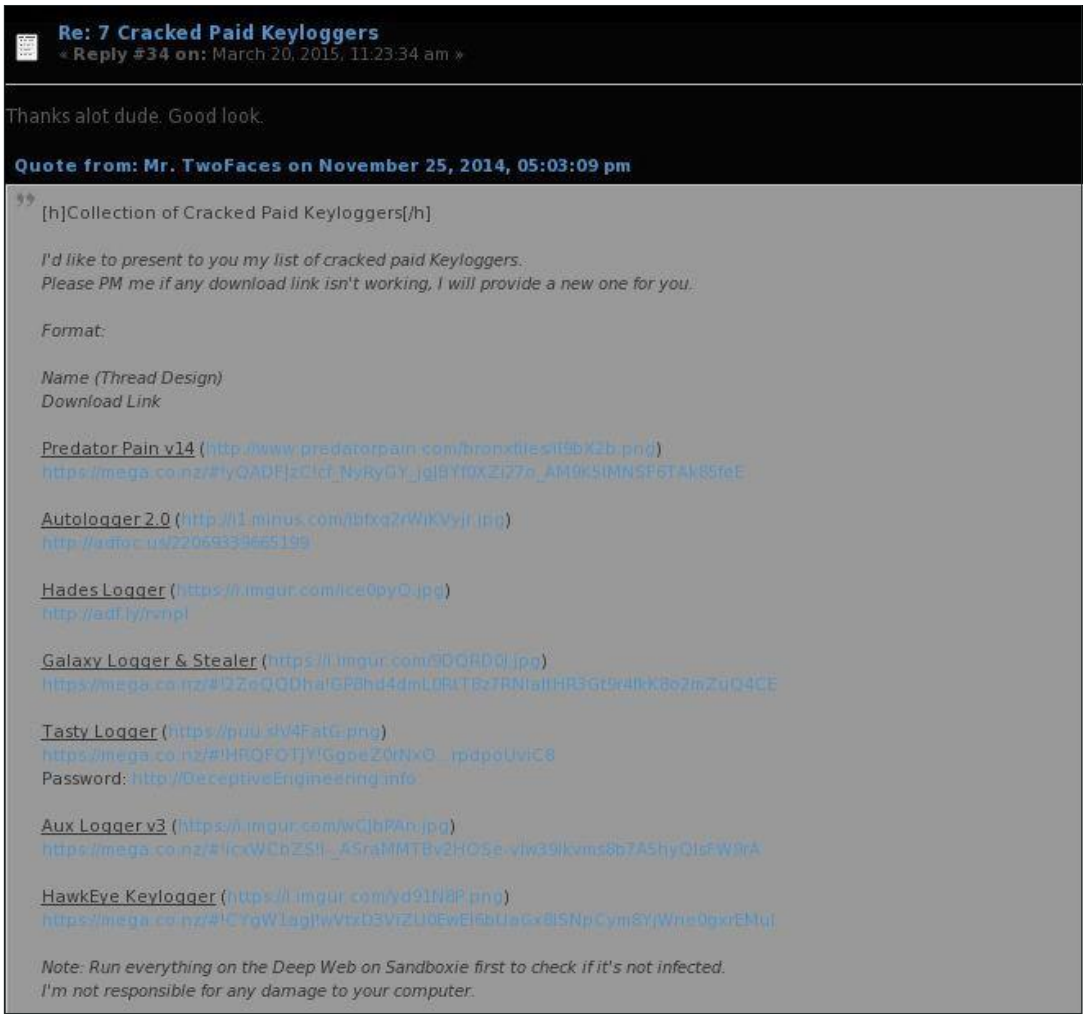
χρησιμοποιηθούν για συναντήσεις κακόβουλων παραγόντων και ανταλλαγή αγαθών ή ως δίαυλος επικοινωνίας για botnets.

Η ίδια αντίληψη ισχύει και για επτά τομείς XMPP και έναν τομέα Mumble, πρωτόκολλα για διακομιστές συνομιλίας που τρέχουν στο TOR

3.10 Ύποπτες σελίδες

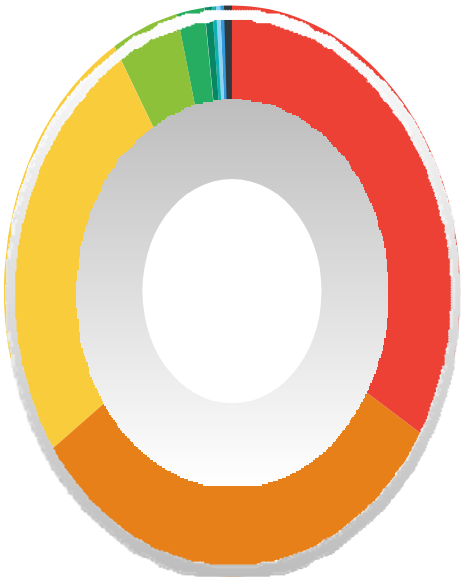
Για κάθε ιστοσελίδα Deep Web που παρακολουθήθηκε, συγκεντρώθηκαν οι διευθύνσεις URL που βρέθηκαν στην σελίδα με τους συνδέσμους. Στην συνέχεια ανακτήθηκε το Web Reputation Technology URL για κάθε σύνδεσμο που οδηγεί στο Surface Web, προκειμένου να προσδιοριστεί ποιες είχαν ταξινομηθεί ως ύποπτες. Παρά αυτήν την περιορισμένη εμβέλεια, μπορούν ακόμα να χρησιμοποιηθούν ως δείκτες.

Συνολικά, εντοπίστηκαν 8.707 ύποπτες σελίδες, συμπεριλαμβανομένων εκείνων που φιλοξενούν εργαλεία phishing, malware ή λήψεις, ή που τρέχουν σε σκιώδεις αγορές (που χρησιμοποιούνται για το εμπόριο εργαλείων hacking, κλπ).



Δείγμα ιστοσελίδας με συνδέσεις σε keyloggers

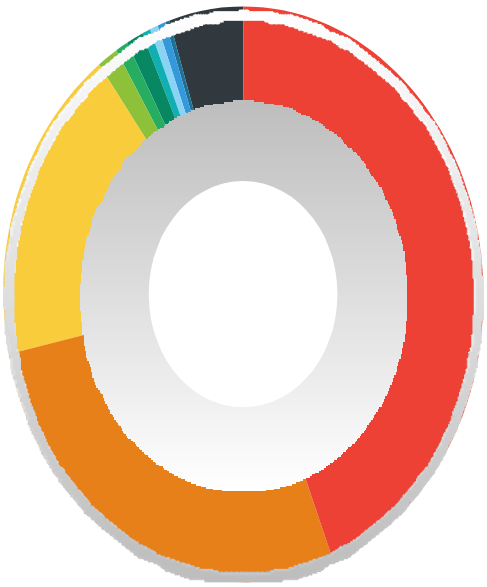
Ο παρακάτω πίνακας παρέχει μια ανάλυση των ύποπτων σελίδων ανά κατηγορία, όπως επιβεβαιώνεται από τις αξιολογήσεις του Web Reputation Technology URL.



Φορείς ιού	33.74%
Αποφυγή μεσολάβησης	31.69%
Εκμετάλλευσης των παιδιών	26.07%
Hacking	4.74%
Περιεχόμενο για ενήλικες με φορείς ιού	2.00%
Κακόβουλο adware	0.46%
Διακομιστής C&C	0.29%
Phishing	0.28%
Σπάσιμο κωδικού πρόσβασης	0.25%
Περιεχόμενο για ενήλικες με κακόβουλο adware	0.15%
Άλλο	0.33%

Λόγοι για τους οποίους οι διευθύνσεις URL του Web Surface είχαν ταξινομηθεί ως ύποπτες

Περισσότερο από το 30% των συνδέσμων που περιλαμβάνονται στις ιστοσελίδες που έχουν ταξινομηθεί ως «ύποπτες» ήταν φορείς ιού που οδηγούν τους χρήστες σε ιστοσελίδες μεταφόρτωσης κακόβουλου λογισμικού. Οι επόμενες δύο ταξινομήσεις ήταν η αποφυγή μεσολάβησης, διευθύνσεις URL που παρέχουν πρόσβαση VPN ή τρόποι για να αποφεύγονται τα firewalls εταιρειών και εκμετάλλευσης παιδιών.



- Hidden Wiki, ένας κατάλογος συνδέσμων 44.16%
- New Hidden Wiki 2015, ένας κατάλογος συνδέσμων 27.59%
- Κλώνος του Hidden Wiki 18.06%
- Wiki Tierra, ένας κατάλογος συνδέσμων 1.50%
- Μη λογοκριμένο Hidden Wiki 0.91%
- Αντίγραφο μη λογοκριμένου Hidden Wiki 0.89%
- Ένα κινέζικο Blog στο TOR 0.76%
- ParaZite, ένα φόρουμ 0.57%
- The Hidden Wiki, ένας κατάλογος συνδέσμων 0.40%
- Flibustaeous, ένα ρωσικό φόρουμ 0.23%
- Άλλα 4.93%

Ιστοσελίδες που έχουν τον υψηλότερο αριθμό ύποπτων συνδέσμων Web Surface

3.11 Τι άσχημο συμβαίνει στο Deep Web;

Το Deep Web προσφέρει ένα ορισμένο επίπεδο της ανωνυμίας που κάνει τους ανθρώπους σε αυτό περισσότερο διατεθειμένους να συμμετάσχουν σε

παράνομες δραστηριότητες. Οι διάφορες συναλλαγές σε αυτό, συμπεριλαμβανομένων διακεκριμένων προϊόντων και υπηρεσιών που αποτελούν αντικείμενο διαπραγμάτευσης, απεικονίζουν πολύ καλά του τι είναι ικανοί οι άνθρωποι να κάνουν εάν ήταν εγγυημένη η μυστικότητα της ταυτότητάς τους.

Σε αντίθεση με τον υπόγειο κόσμο του κυβερνοεγκλήματος, τα περισσότερα είδη των δραστηριοτήτων στο Deep Web έχουν πιο εμφανείς, εάν όχι δραστικές, συνέπειες στον πραγματικό κόσμο. Πολλά από τα κακόβουλα εργαλεία και υπηρεσίες που πωλούνται στον υπόγειο κόσμο του κυβερνοεγκλήματος μπορούν να χρησιμοποιηθούν για την απόκτηση κέρδους. Αυτοί που πωλούν υπηρεσίες λιανικής στο Deep Web, π.χ. υπηρεσίες δολοφονίας, προφανώς εξυπηρετούν έναν διαφορετικό, πιο σκοτεινό σκοπό.

Δεν υπάρχει κάποια εγγύηση για την αυθεντικότητα των προϊόντων και των υπηρεσιών που συζητούνται εδώ, εκτός από το γεγονός ότι οι ιστοσελίδες που τα διαφημίζουν δεν υπάρχουν και αφορούν σε διάφορες συναλλαγές που πραγματοποιούνται στο Deep Web.

ΚΕΦΑΛΑΙΟ 4 ΚΑΚΟΒΟΥΛΑ ΛΟΓΙΣΜΙΚΑ ΣΤΟ DEEP WEB

Με πολλούς τρόπους, το Deep Web και το κακόβουλο λογισμικό είναι ιδανικά το ένα για το άλλο, ειδικά όταν πρόκειται για την φιλοξενία υποδομών εντολών και ελέγχου (C&C). Είναι στην φύση των κρυφών υπηρεσιών και ιστοσελίδων όπως το TOR και το I2P να κρύβουν την θέση των διακομιστών χρησιμοποιώντας ισχυρή κρυπτογραφία. Αυτό καθιστά ουσιαστικά αδύνατο για τους εγκληματολογικούς ερευνητές να διερευνήσουν με την χρήση παραδοσιακών μέσων μία διεύθυνση IP ενός διακομιστή, να ελέγξουν τα στοιχεία της εγγραφής και ούτω καθεξής. Επιπλέον, η χρήση αυτών των ιστοτόπων και υπηρεσιών δεν είναι ιδιαίτερα δύσκολη.

Έτσι, δεν αποτελεί έκπληξη που μια σειρά από κυβερνοεγκληματίες χρησιμοποιούν TOR για την C&C. Οι χειριστές πίσω από διαδεδομένες οικογένειες κακόβουλου λογισμικού χρησιμοποιούν TOR για ορισμένα τμήματα της εγκατάστασης τους. Απλώς τυλίγουν τον νόμιμο πελάτη TOR στο πακέτο εγκατάστασής τους. Η Trend Micro έγραψε για πρώτη φορά για αυτήν την τάση το 2013, όταν το κακόβουλο λογισμικό MEVADE (Feike, 2015) προκάλεσε μια αισθητή άνοδο στην κυκλοφορία του TOR, όταν ενεργοποιούνταν οι κρυφές υπηρεσίες του TOR για το C&C. Το 2014 ακολούθησαν και άλλες οικογένειες κακόβουλων προγραμμάτων όπως το ZBot (Jay, 2014).

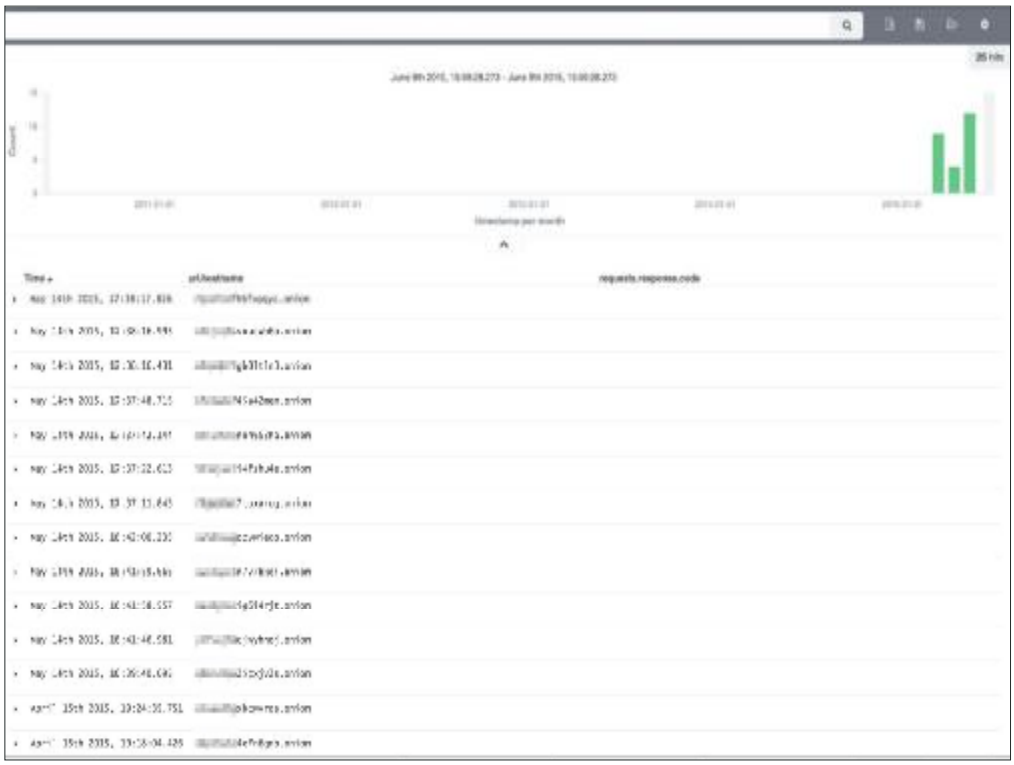
4.1 VAWTRAK

Το κακόβουλο λογισμικό VAWTRAK είναι τραπεζικά Trojans που εξαπλώνονται μέσω των μηνυμάτων ηλεκτρονικού ταχυδρομείου που κάνουν phishing. Κάθε δείγμα επικοινωνεί με έναν κατάλογο διακομιστών C&C των οποίων οι διευθύνσεις IP ανακτώνται από την λήψη ενός κρυπτογραφημένου αρχείου εικονιδίου (favicon.ico) από κάποιες σκληρά κωδικοποιημένες περιοχές του TOR. Αυτό παρέχει το πλεονέκτημα της ανωνυμοποίησης της θέσης ενός διακομιστή εγκληματία, αλλά όχι τους χρήστες που αποκτούν πρόσβαση, κάτι που δεν αποτελεί ζήτημα, επειδή όλοι οι χρήστες είναι

συστήματα που έχουν προσβληθεί με το κακόβουλο λογισμικό (David Sancho, 2015).

Διακομιστής VAWTRAK C&C που δείχνει ένα αρχείο favicon που μοιάζει να είναι νόμιμο

Με βάση την παρουσία αυτού του αρχείου favicon.ico και την ρύθμιση C&C του διακομιστή (πολλοί από τους οποίους τρέχουν openresty / 1.7.2.1), έγινε δυνατή η αναζήτηση στο σύστημα των συγγραφέων μιας πλήρους λίστας αυτών των δικτυακών τόπων και η μεταφόρτωση της τελευταίας διεύθυνση του διακομιστή C&C κάθε μέρα.



Διακομιστές VAWTRAK C&C

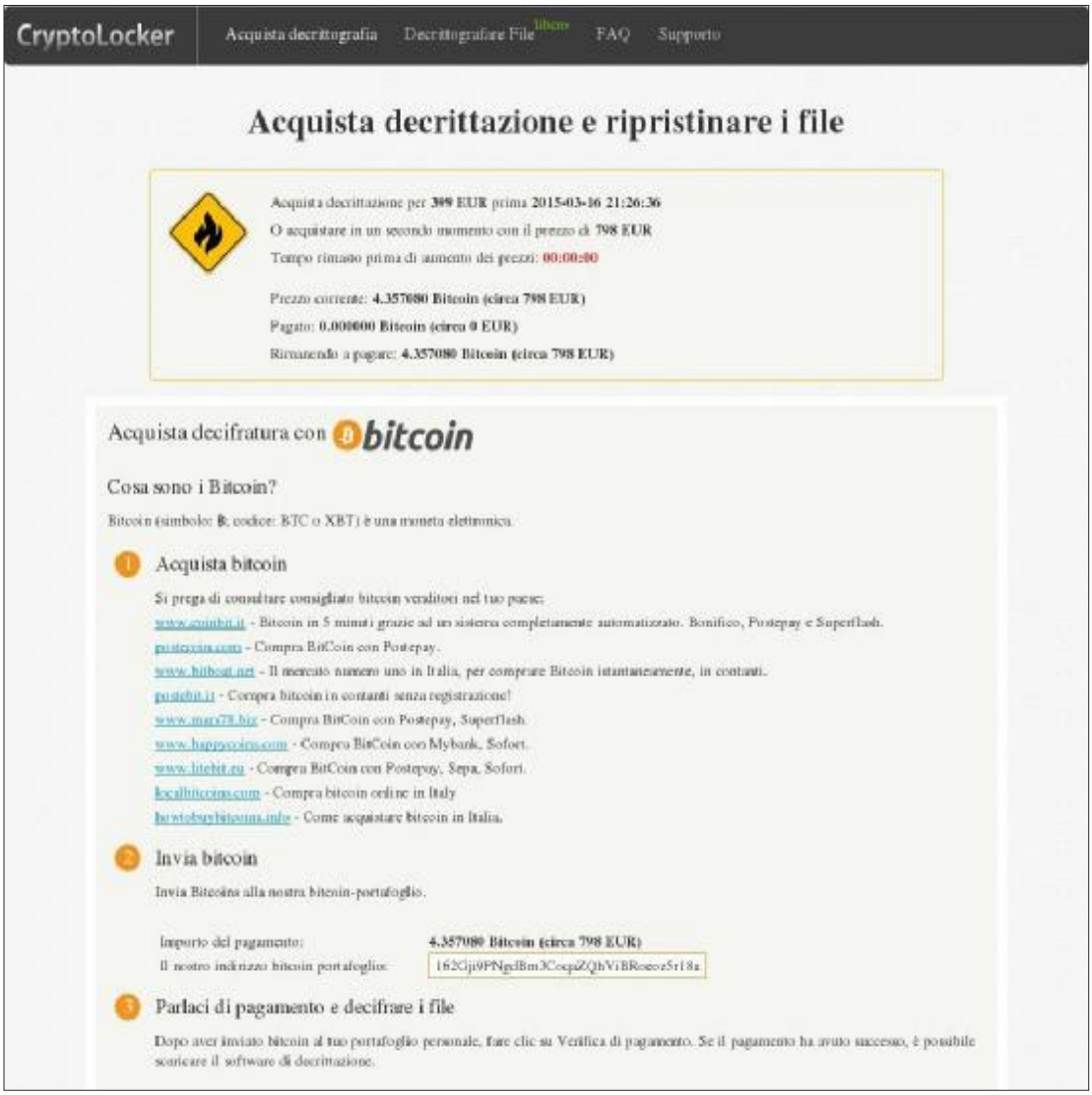
4.2 CryptoLocker

Μία άλλη σημαντική οικογένεια κακόβουλου λογισμικού που χρησιμοποιεί το Deep Web είναι το CryptoLocker. Το CryptoLocker αναφέρεται σε μία παραλλαγή ransomware που κρυπτογραφεί τα προσωπικά έγγραφα των θυμάτων πριν την ανακατεύθυνσή τους σε έναν ιστότοπο όπου μπορούν να πληρώσουν για να ανακτήσουν την πρόσβαση στα αρχεία τους. Το CryptoLocker είναι επίσης αρκετά έξυπνο ώστε να προσαρμόζει αυτόματα την σελίδα πληρωμών ως προς την γλώσσα του θύματος και τα μέσα πληρωμής.

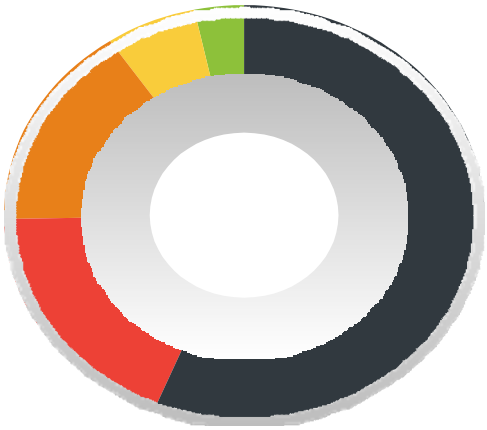
Το TorrentLocker, μία παραλλαγή του CryptoLocker, κάνει χρήση του TOR και φιλοξενεi ιστοσελίδες πληρωμών πλέον της χρήσης του Bitcoin ως τρόπου πληρωμής. Δείχνει γιατί το Deep Web απευθύνεται σε εγκληματίες του κυβερνοχώρου που είναι πρόθυμοι να κάνουν τις υποδομές τους πιο ισχυρές στις πιθανές καταργήσεις της ιστοσελίδας τους.

Οι παρακάτω εικόνες είναι σελίδες πληρωμής που έλαβε το Deep Web Analyzer. Και οι δύο είναι σε διαφορετικές γλώσσες, δίνοντάς μας μία εικόνα για τα θύματα που αποτελούν στόχο και την καταγωγή τους.

Αυτόματα μορφοποιημένες σελίδες CryptoLocker για θύματα από την Ταϊβάν



Αυτόματα μορφοποιημένες σελίδες CryptoLocker για θύματα από την Ιταλία



μπορεί να προσδιοριστεί

- Αγγλικά 18.75%
- Γαλλικά 15.63%
- Τούρκικα 6.25%
- Ιταλικά 3.13%

Κορυφαίες γλώσσες που χρησιμοποιούνται από τις σελίδες CryptoLocker

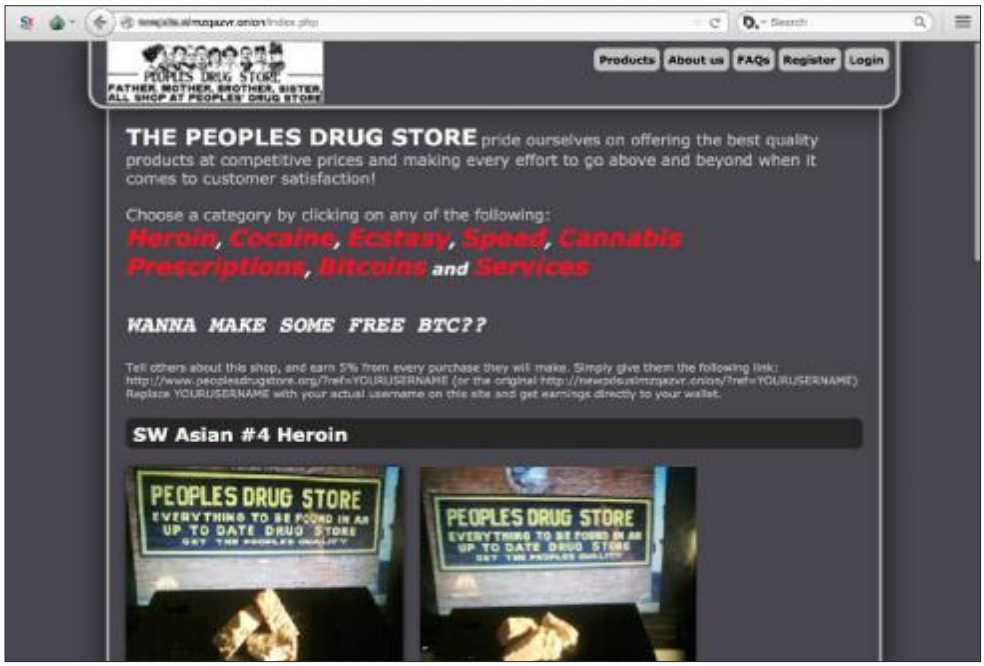
Δυστυχώς, λαμβάνοντας υπόψη όλα τα οφέλη που αποκομίζουν οι κυβερνοεγκληματίες από την φιλοξενία των πιο μόνιμων τμημάτων των υποδομών τους στις υπηρεσίες που κρύβονται στο TOR, πιστεύεται ότι ολοένα και περισσότερες οικογένειες malware θα στραφούν και στο Deep Web στο μέλλον. Εξαιτίας αυτού, το Deep Web Analyzer υλοποιεί ευρετικές μεθόδους για τον εντοπισμό νέων οικογενειών malware (τους λεγόμενους «άγνωστους αγνώστους»). Αυτό το χαρακτηριστικό μας επιτρέπει να είμαστε σε εγρήγορση κάθε φορά που κρυφές υπηρεσίες ξαφνικά εμφανίζουν αυξημένη κίνηση ή εάν υπάρχει κάποια μεγάλη άνοδος στον αριθμό των ιστοτόπων.

Τα bots, περισσότερο από ό,τι άλλες μορφές κακόβουλου λογισμικού που επικοινωνούν με τους διακομιστές C&C, είναι γνωστό ότι χρησιμοποιούν στατικά URI με συμβολοσειρές ερωτημάτων ή τις ίδιες παραμέτρους διαχρονικά. Χρησιμοποιήσαμε αυτή την παρατήρηση ως δεδομένα ώστε το Deep Web Analyzer να μπορεί να επισημάνει αυτόματα το σύνολο της κίνησης που χρησιμοποιεί το στατικό πρότυπο των συμβολοσειρών ερωτημάτων ως ύποπτο.

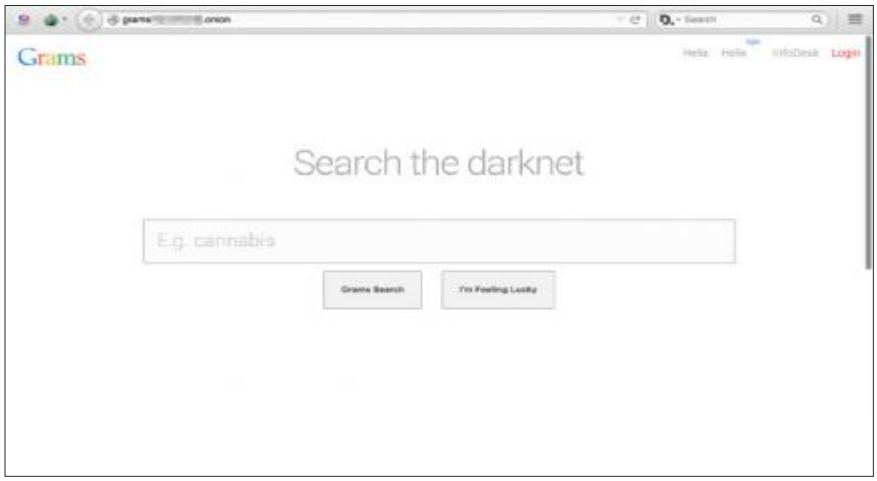
4.3 Παράνομα ναρκωτικά

Αποτελεί κοινό χαρακτηριστικό σε κάθε έκθεση σχετικά με το Deep Web, για το πώς διατίθενται ελεύθερα τα παράνομα ναρκωτικά και τα όπλα σε αυτό. Δεν θα γίνει αναφορά σε αυτό με λεπτομέρειες, αλλά θα επισημανθεί εν συντομία το γεγονός ότι ακόμη και μετά την καταδίκη ατόμων, όπως ο Ross Ulbricht, η αγορά ναρκωτικών από το Deep Web εξακολουθεί να είναι σχετικά ασήμαντη.

Η διαθεσιμότητα των παράνομων ναρκωτικών διαφέρει πολύ στο Deep Web. Μερικές ιστοσελίδες πωλούν τα πάντα, από τα σχετικά ήπια ναρκωτικά (λαθραία τσιγάρα) μέχρι κάνναβη, ψυχεδελικά, κοκαΐνη και άλλα.



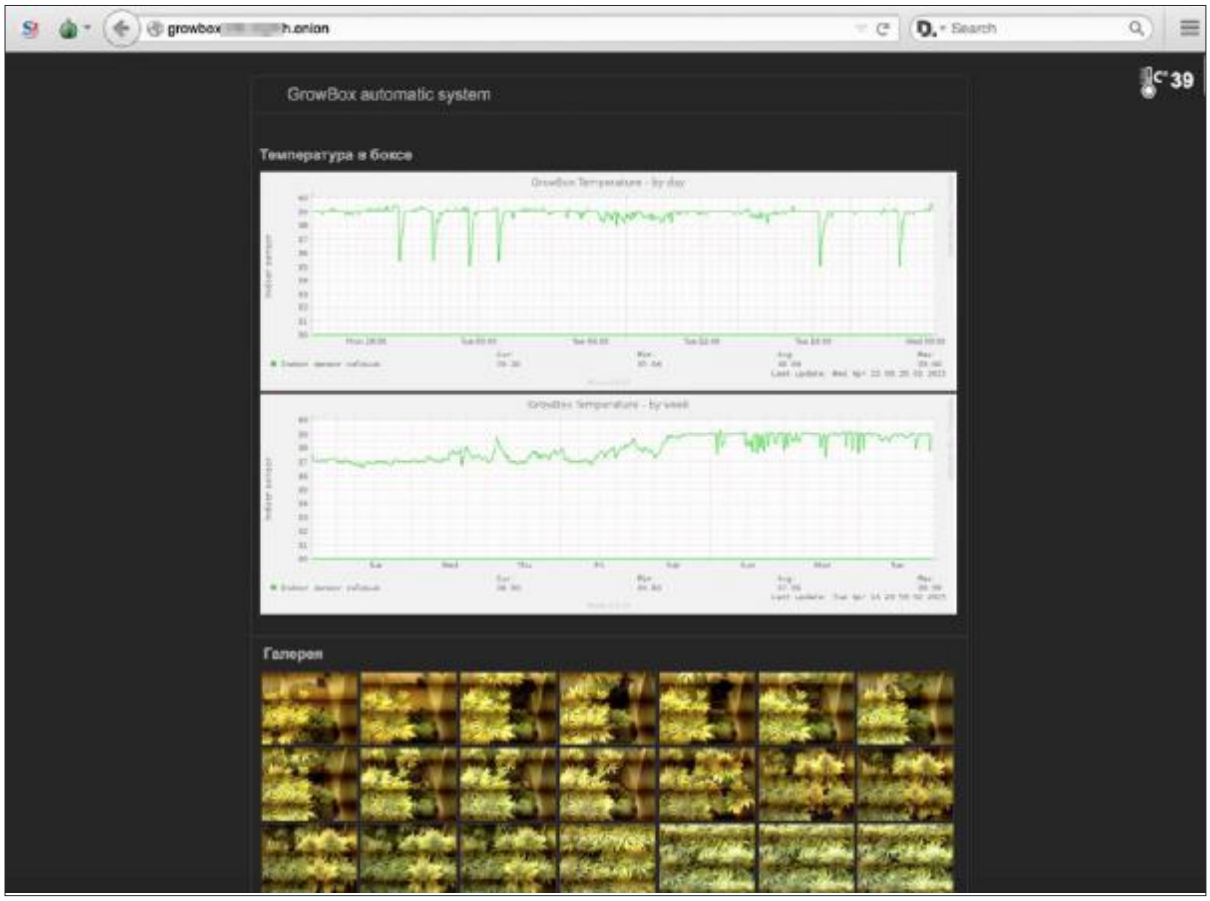
Η ιστοσελίδα Peoples Drug Store πουλά ηρωίνη, κοκαΐνη, έκσταση και άλλα



Το Grams είναι μία μηχανή αναζήτησης ναρκωτικών στο Deep Web

Εκτός από τα καταστήματα ή φόρουμ, μία πολύ δημοφιλής ιστοσελίδα είναι το Grams το οποίο επιτρέπει στους χρήστες να αναζητούν και να καταχωρούν εύκολα ιστοσελίδες στο Deep Web που ασχολούνται με την πώληση παράνομων ναρκωτικών. Με ένα λογότυπο που μιμείται εκείνο της Google, αποτελεί μία ιστοσελίδα για εκείνους που αναζητούν τα εν λόγω εμπορεύματα.

Υπάρχουν ακόμη και ιστοσελίδες TOR που προσφέρουν πληροφορίες για ένα σπίτι καλλιέργειας κάνναβης όπου παρουσιάζονται στατιστικά για την θερμοκρασία και την υγρασία σε πραγματικό χρόνο και υπάρχει και κάμερα που δείχνει την ανάπτυξη των φυτών με την πάροδο του χρόνου.



Σπίτι όπου καλλιεργείται κάνναβη με στατιστικά και ροή εικόνας σε πραγματικό χρόνο

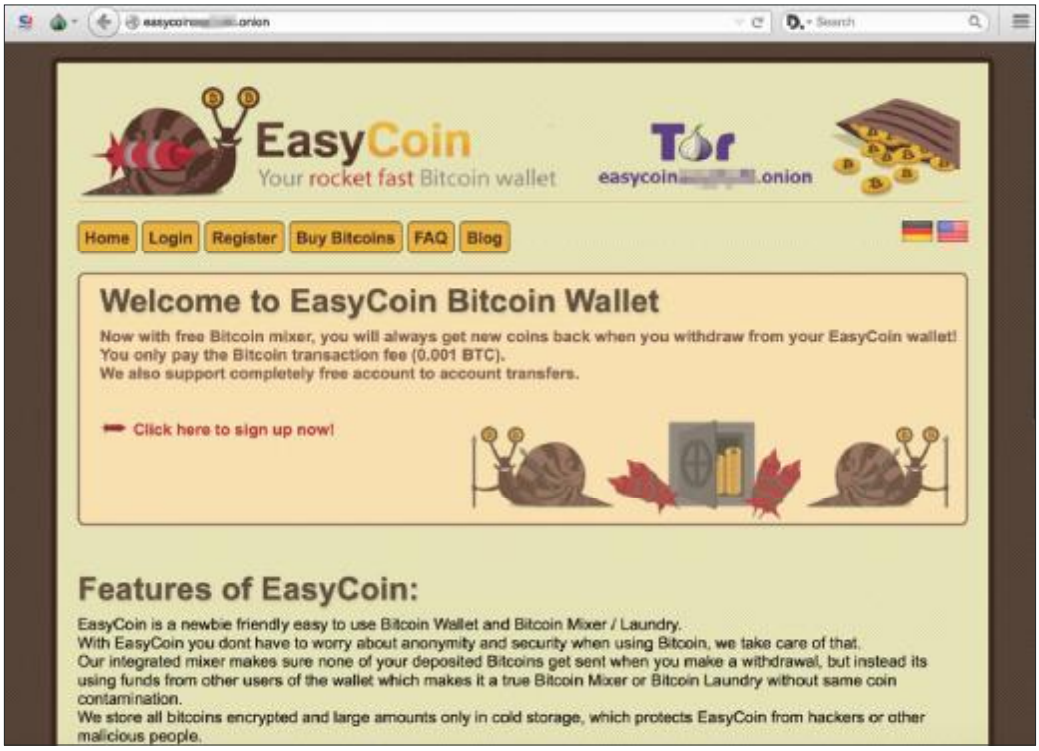
Η αναφορά στα ναρκωτικά έχει σκοπό να τονίσει περαιτέρω ένα σημαντικό σημείο, ότι το κλείσιμο μιας εγκληματικής αγοράς, όπως η Silk Road, ουσιαστικά δεν αποτελεί την λύση. Από την μία πλευρά, υπάρχουν ακόμα οι αγοραστές που επιθυμούν να προμηθευτούν ναρκωτικά και από την άλλη, υπάρχουν και οι πωλητές που επιθυμούν να καλύψουν τις ανάγκες τους. Η αγορά ή το φόρουμ ενεργούν απλώς ως μια μέση λύση. Ακόμη κι αν αφαιρεθούν, όσο θα υπάρχει ισχυρή ζήτηση και από τις δύο πλευρές, μία άλλη αγορά, δυστυχώς, πάντα θα εμφανίζεται για να πάρει την θέση.

4.4 Bitcoin και νομιμοποίηση εσόδων από παράνομες δραστηριότητες

Το Bitcoin είναι ένα νόμισμα που έχει σχεδιαστεί με βάση την αρχή της

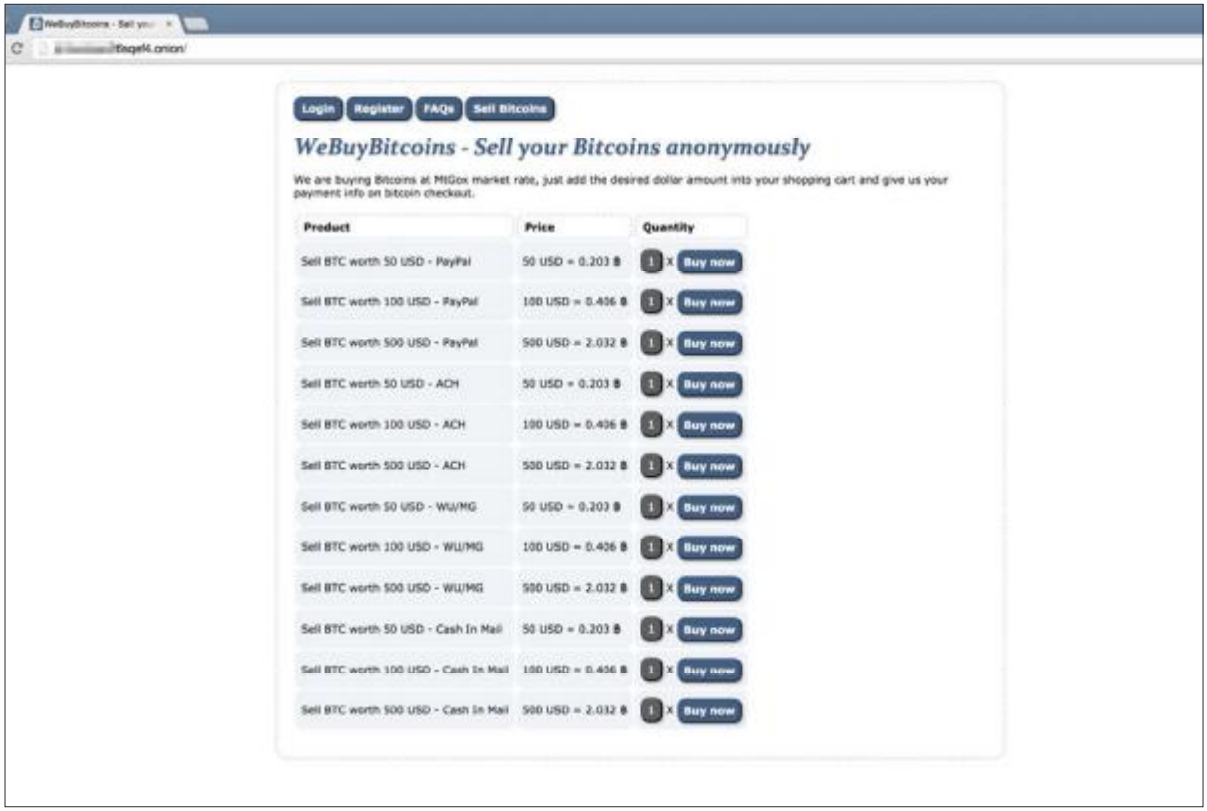
ανωνυμίας. Ως εκ τούτου, χρησιμοποιείται συχνά όταν αγοράζονται παράνομα αγαθά και υπηρεσίες. Ενώ όλες οι συναλλαγές Bitcoin είναι ανώνυμες (εφ' όσον δεν έχει συνδεθεί ο κωδικός του πορτοφολιού με την πραγματική ταυτότητα του χρήστη), είναι πλήρως δημόσιες. Το γεγονός ότι κάθε συναλλαγή στην blockchain του Bitcoin είναι διαθέσιμη στο κοινό σημαίνει ότι οι ερευνητές μπορούν να τις εξετάσουν. Έτσι, καθίσταται εφικτή η παρακολούθηση της πορείας των χρημάτων καθώς κινούνται μέσα από το σύστημα, αν και αρκετά δύσκολη.

Ως αποτέλεσμα, έχουν προκύψει μια σειρά από υπηρεσίες που προσθέτουν περαιτέρω ανωνυμία στο σύστημα, καθιστώντας το ηλεκτρονικό νόμισμα ακόμη πιο δύσκολο να εντοπιστεί. Αυτό επιτυγχάνεται γενικά με την ανάμειξη των Bitcoins, δηλαδή με την μεταφορά τους μέσω ενός αραχνώδους δικτύου από μίκρο-συναλλαγές πριν επιστραφούν στον ιδιοκτήτη τους. Κατά την διαδικασία αυτή, ο χρήστης καταλήγει με το ίδιο χρηματικό ποσό (συνήθως μείον ένα μικρό τέλος επεξεργασίας), αλλά οι συναλλαγές γίνονται αισθητά πιο δύσκολες να παρακολουθηθούν.



Η ιστοσελίδα EasyCoin Bitcoin για την νομιμοποίηση παράνομων εσόδων

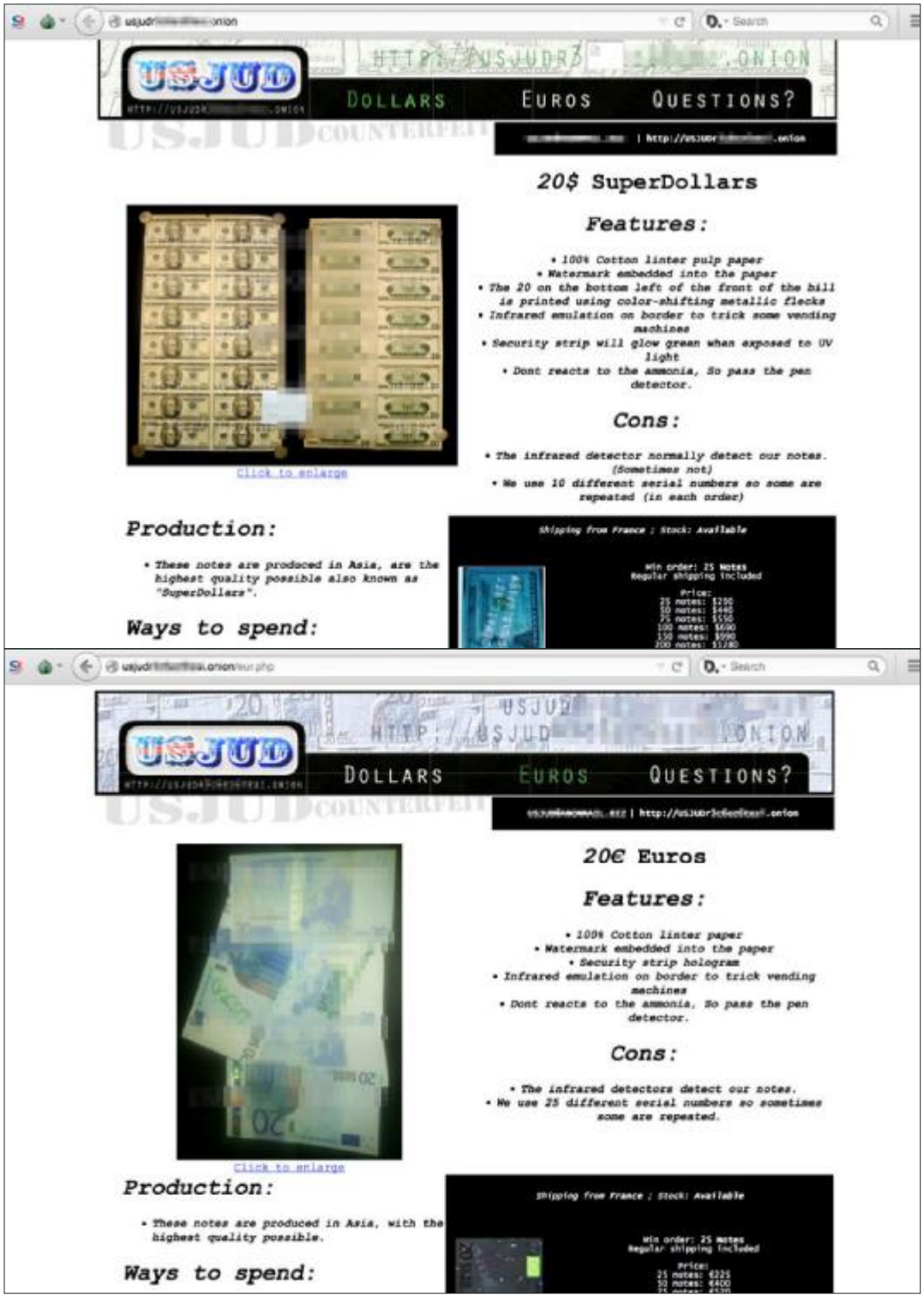
Οι υπηρεσίες νομιμοποίησης παράνομων εσόδων σε Bitcoin συμβάλλουν στην αύξηση της ανωνυμίας στην μεταφορά χρημάτων σε όλο το σύστημα Bitcoin. Τελικά όμως, οι περισσότεροι χρήστες Bitcoin επιθυμούν να εξάγουν τα χρήματα από το σύστημα για να το μετατρέψουν σε μετρητά ή σε άλλους τύπους παραδοσιακών μέσων πληρωμής. Αρκετές ανώνυμες υπηρεσίες υπάρχουν στο Deep Web για το σκοπό αυτό οι οποίες επιτρέπουν στους χρήστες να ανταλλάσσουν τα Bitcoins με χρήματα μέσω των PayPal™, Automated Clearing House (ACH), Western Union, ή ακόμα και να στείλουν μετρητά απευθείας μέσω ταχυδρομείου.



Η σελίδα WeBuyBitcoins, είναι μία υπηρεσία ανταλλαγής χρημάτων ή προσφέρει ηλεκτρονικά μέσα πληρωμής έναντι Bitcoins

Ιστοσελίδες όπως η WeBuyBitcoins ανταλλάσσουν πραγματικά χρήματα για Bitcoins σε ανταγωνιστικές συναλλαγματικές ισοτιμίες σε σύγκριση με ισοδύναμες μη ανώνυμες υπηρεσίες που υπάρχουν στο Surface Web. Οι εγκληματίες που είναι πρόθυμοι να αναλάβουν μεγαλύτερο κίνδυνο για

δυνητικά μεγαλύτερες ανταμοιβές έχουν κι άλλη επιλογή, την αγορά πλαστών νομισμάτων χρησιμοποιώντας Bitcoins.

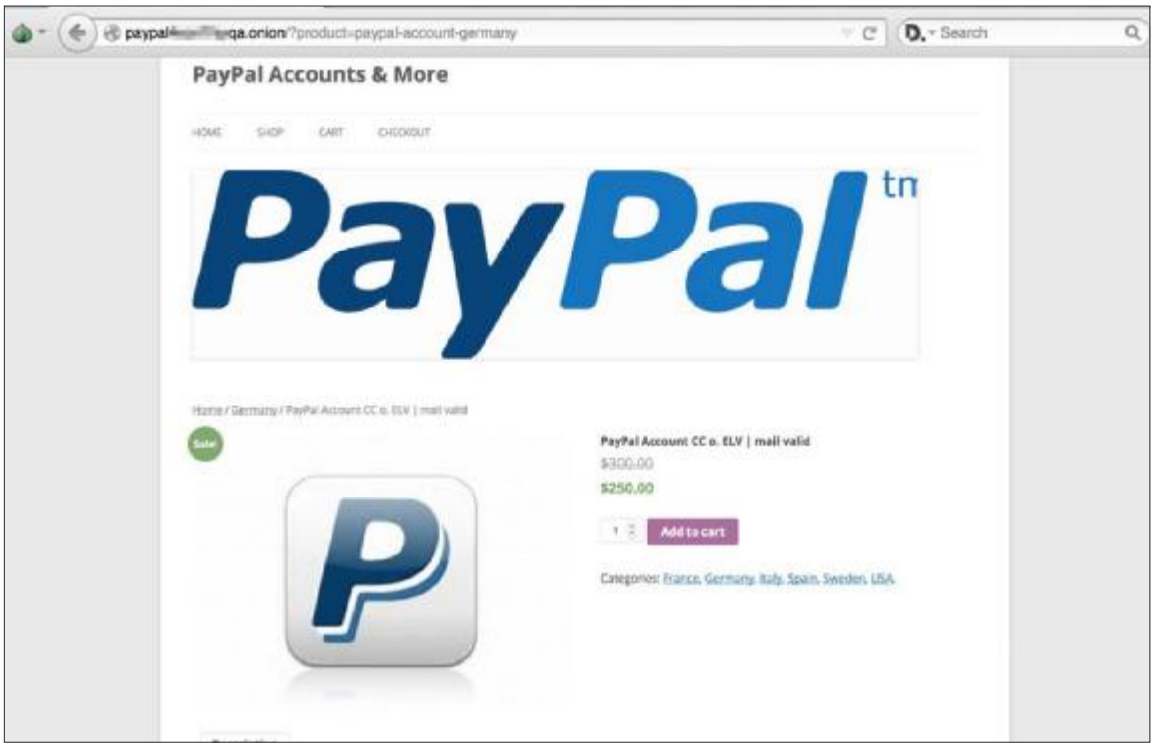


Ιστοσελίδες που προσφέρουν πλαστά $20 ή €20 για περίπου το μισό της ονομαστικής τους αξίας. Άλλες προσφέρουν επίσης πλαστά $50 ή €50

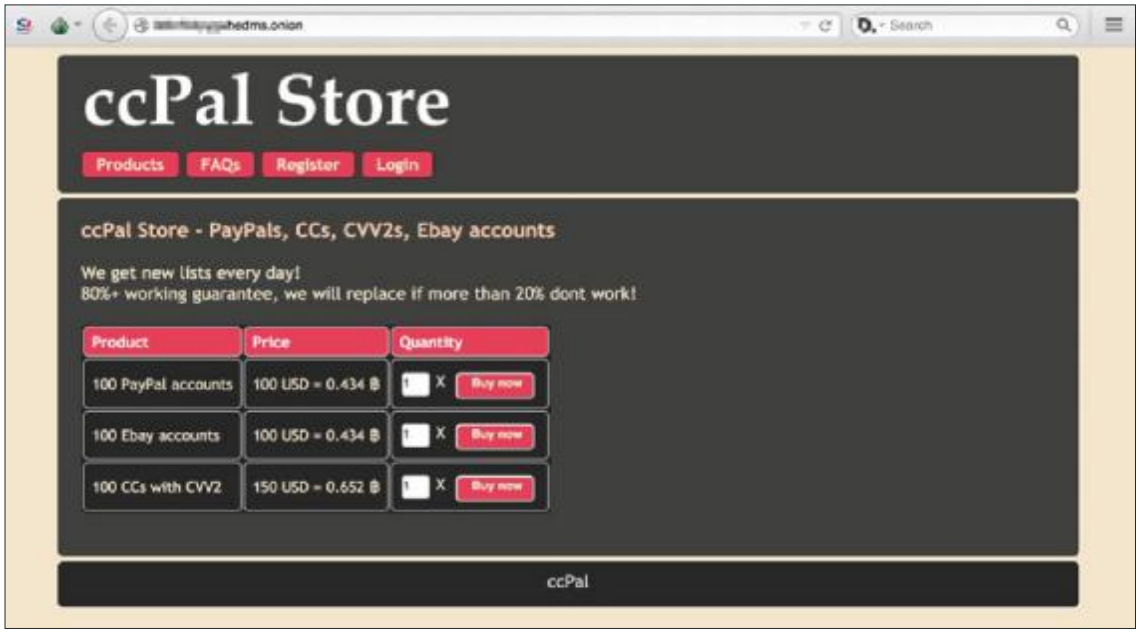
4.5 Κλεμμένοι λογαριασμοί προς πώληση

Η αγορά και πώληση κλεμμένων λογαριασμών σίγουρα δεν περιορίζονται στο Deep Web. Αποτελούν κοινή πρακτική σε όλα τα φόρουμ του υποκόσμου που υπάρχουν στο Surface Web. Οι αριθμοί πιστωτικών καρτών, αριθμοί τραπεζικών λογαριασμών και διαπιστευτήρια σε ηλεκτρονικές δημοπρασίες και ιστοσελίδες τυχερών παιχνιδιών αποτελούν ίσως τα πιο συχνά αγαθά που πωλούνται.

Όπως και στο Surface Web, οι τιμές διαφέρουν μεταξύ των ιστοσελίδων, αλλά υπάρχουν και αγαθά (όπως κλεμμένα διαπιστευτήρια λογαριασμών PayPal) σε πολύ υψηλές τιμές. Λογαριασμοί όπως αυτοί, συνήθως πωλούνται με έναν από τους δύο τρόπους, ως υψηλής ποιότητας επικυρωμένοι λογαριασμοί με τα ακριβή τρέχοντα υπόλοιπά τους ή χύμα (ένας ορισμένος αριθμός από μη επικυρωμένους λογαριασμούς που συνήθως φέρουν και μία εγγύηση ότι τουλάχιστον ένα ορισμένο ποσοστό είναι έγκυρο). Η πρώτη κατηγορία συνήθως είναι και η πιο ακριβή επειδή έχει μεγαλύτερη πιθανότητα απόδοσης της επένδυσης για έναν αγοραστή, ενώ η δεύτερης είναι σημαντικά φθηνότερη.



Κλεμμένοι επικυρωμένοι γερμανικοί λογαριασμοί PayPal (με υπόλοιπο $500-700) προς πώληση για $250



Μη επικυρωμένοι λογαριασμοί PayPal που πωλούνται χύμα (με το 80% αυτών να είναι έγκυροι ή με προσφορά για αντικατάσταση)

Μια προσφορά που μπορεί να βρεθεί πολύ εύκολα στο Deep Web, αλλά όχι τόσο πολύ στο Surface Web είναι η πώληση πραγματικών, φυσικών πιστωτικών καρτών. Αυτό δεν σημαίνει ότι δεν διατίθενται και στα φόρουμ των εγκληματιών στο Surface Web. Οι ιστοσελίδες που τις διαθέτουν στο Deep Web φαίνονται να είναι λίγο πιο επαγγελματικές από την άποψη της προσέγγισης.

Αντίγραφα πιστωτικών καρτών που έχουν δημιουργηθεί με κλεμμένα προσωπικά δεδομένα

4.6 Διαβατήρια και υπηκοότητες προς πώληση

Τα διαβατήρια και οι ταυτότητες είναι μοναδικά, ισχυρά έγγραφα και τα ψεύτικα ακόμη περισσότερο. Χρησιμοποιούνται όχι μόνο ως μια μορφή αναγνώρισης για την διέλευση συνόρων (συμπεριλαμβανομένης και της παράνομης), αλλά και για τα πάντα, από το άνοιγμα τραπεζικών λογαριασμών, την υποβολή αίτησης για δάνεια, την αγορά ακινήτων και πολλά άλλα. Δεν αποτελεί έκπληξη ότι είναι ένα πολύτιμο αγαθό. Υπάρχουν αρκετές ιστοσελίδες στο Deep Web που ισχυρίζονται ότι πωλούν διαβατήρια και άλλες μορφές επίσημων ταυτοτήτων σε διάφορες τιμές από χώρα σε χώρα και από πωλητή σε πωλητή.

Ωστόσο, η εγκυρότητά τους είναι δύσκολο να εξακριβωθεί χωρίς την πραγματική αγορά των εμπορευμάτων, ειδικά στην περίπτωση της υπηκοότητας. Συναφείς υπηρεσίες μπορεί να είναι απλά απάτες που εκμεταλλεύονται ανθρώπους που ψάχνουν να αποκτήσουν υπηκοότητα για να παραμείνουν στην χώρα που διαμένουν σήμερα.

Υπηκοότητα ΗΠΑ προς πώληση για τουλάχιστον $6,000

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

For some countries we have an unique option to register passports in official government department databases. To get more details please contact with our manager:

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.

Πληροφορίες τιμολόγησης

Δείγμα πλαστών διαβατηρίων και άλλων εγγράφων

4.7 Διαρροή πληροφοριών: Κυβέρνηση, αρχές επιβολής του νόμου και διασημότητες

Ανάμεσα στους χάκερ και σε κάποιον βαθμό τους online gamers, είναι σύνηθες για άτομα με όμοιες ιδέες και αντιλήψεις να σχηματίζουν κλειστές ομάδες. Λόγω της φύσης των δραστηριοτήτων που ασκούν, είναι επίσης συνηθισμένες οι αντιπαλότητες μεταξύ ανταγωνιστικών ομάδων. Όταν συμβαίνει κάτι τέτοιο, αποτελεί κοινή πρακτική για μία ομάδα να προσπαθήσει να κάνει «dox» στην άλλο.

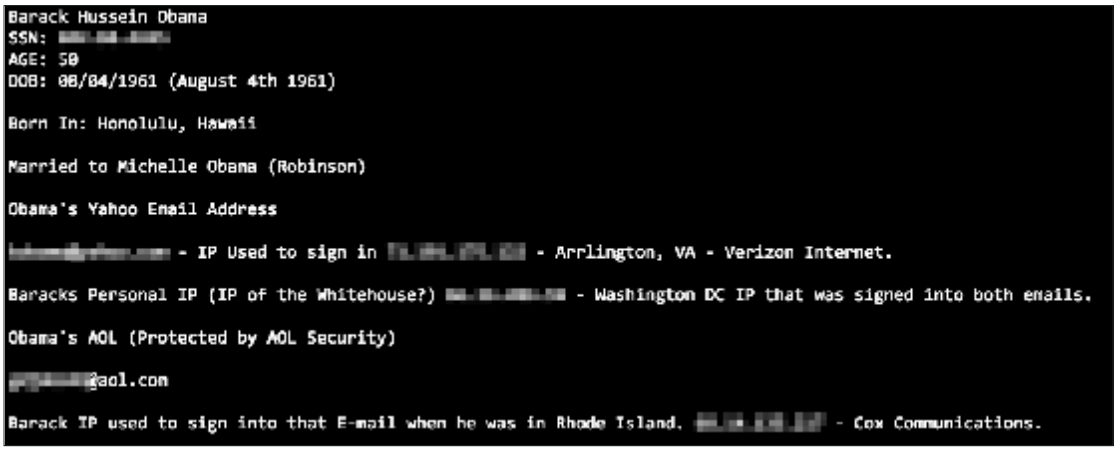
Το «doxing» επομένως είναι η πράξη της έρευνας και διάδοσης των προσωπικών δεδομένων ενός ατόμου, το οποίο, στην περίπτωση των χάκερ, αποκαλύπτεται ένας αντίπαλος ουσιαστικά μέσω της σύνδεσης της ταυτότητάς του στον πραγματικό κόσμο με την ταυτότητά του στο διαδίκτυο. Τα μέσα για να γίνει αυτό ποικίλουν, αλλά συνήθως συνδυάζουν την πρόσβαση σε δημόσια διαθέσιμα δεδομένα, την κοινωνική μηχανική και το άμεσο hacking.

Η ιστοσελίδα doxing Cloudnine (σημειώστε ότι ζητά στοιχεία κοινωνικής ασφάλισης, ιατρικά, οικονομικά στοιχεία, κ.λπ.)

Αλλά το φαινόμενο του doxing ή η κοινοποίηση ιδιωτικών πληροφοριών με κανέναν τρόπο δεν περιορίζεται σε περιπτώσεις χάκερ

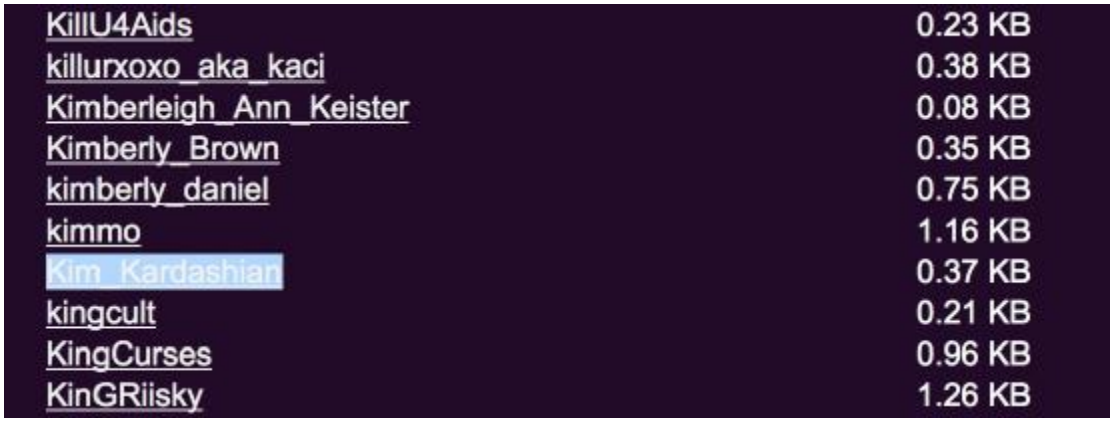
εναντίον χάκερ, καθώς είναι εξίσου κοινό για τους χάκερ να στοχεύουν εταιρείες, διασημότητες και άλλα δημόσια πρόσωπα. Η έκθεση μιας εταιρείας δεν περιορίζεται απλώς στο hacking βέβαια, μπορεί επίσης να προκληθεί από άτομα εντός της εταιρείας, όπως στην περίπτωση των Wikileaks (που αφορούσε το Deep Web με την μορφή μιας σελίδας που επιτρέπει την ανώνυμη υποβολή νέων διαρροών).

Είναι πολύ δύσκολο να γνωρίζουμε αν αυτά τα στοιχεία είναι πραγματικά ή όχι, αλλά σε πολλές περιπτώσεις, οι πληροφορίες που διαρρέουν περιλαμβάνουν ημερομηνίες γέννησης, αριθμούς κοινωνικής ασφάλισης, προσωπικές διευθύνσεις ηλεκτρονικού ταχυδρομείου, αριθμούς τηλεφώνου, φυσικές διευθύνσεις και πολλά άλλα. Για παράδειγμα, η ιστοσελίδα Cloudnine παρουσιάζει πιθανές πληροφορίες dox για δημόσια πρόσωπα, συμπεριλαμβανομένων αρκετών πρακτόρων του FBI και πολιτικών προσωπικοτήτων, γερουσιαστών των ΗΠΑ και άλλων διασημοτήτων του κινηματογράφου και της τηλεόρασης.



Πιθανός προσωπικός λογαριασμός ηλεκτρονικού ταχυδρομείου του Μπαράκ Ομπάμα (ανεπιβεβαίωτη πληροφορία)

Πιθανές πληροφορίες υπηρεσίας επιβολής του νόμου που διέρρευσαν (ανεπιβεβαίωτες)



Πληροφορίες της Kim Kardashian, και άλλες πληροφορίες doxxing που σχετίζονται με χάκερ

Ακόμη και οι χάκερ οι οποίοι συμπαθούσαν τον Ross Ulbricht έχουν βάλει στο στόχαστρο σκόπιμα τα άτομα που εμπλέκονται στην υπόθεσή του. Ένα παράδειγμα αυτού είναι μία ανάρτηση με υποτιθέμενες πληροφορίες doxing για την Katherine Bolan Forrest, ενός εκ των δικαστών στην υπόθεση.

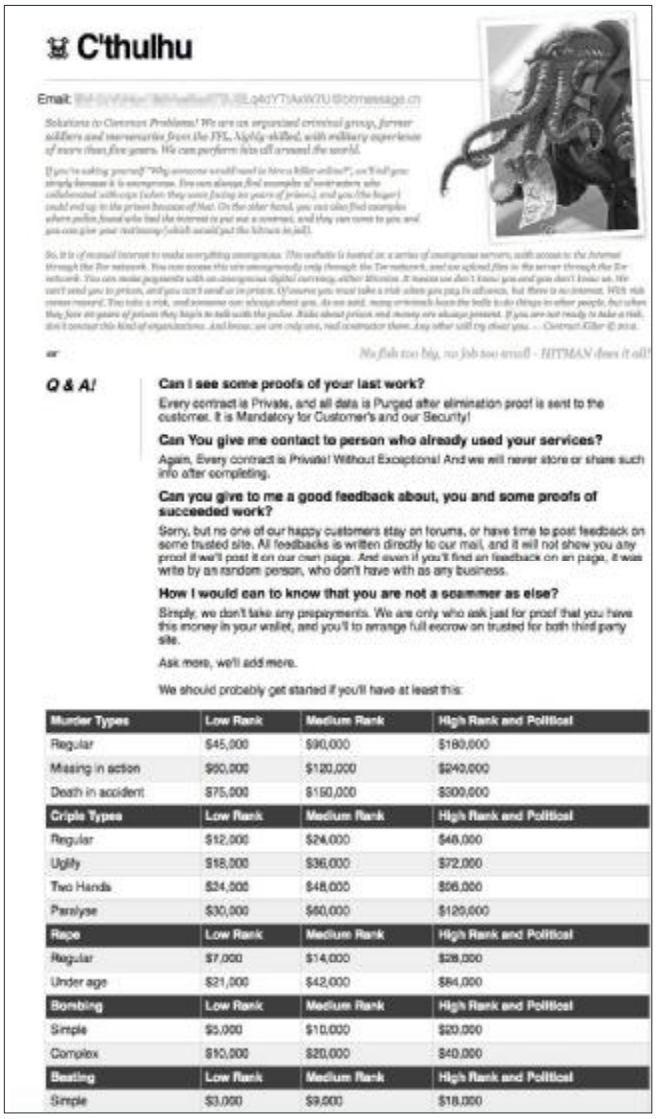
Υποτιθέμενες πληροφορίες που διέρρευσαν σχετικά με δικαστή στην υπόθεση Silk Road

4.8 Υπηρεσίες δολοφονίας

Ίσως μία από τις πιο ανησυχητικές υπηρεσίες που διατίθενται στο Deep Web, κάτι που θα ήταν ανόητο να διαφημίσει οποιοσδήποτε στο Surface Web, αφορά στην πρόσληψη εκτελεστών ή δολοφόνων. Αρκετές τέτοιες υπηρεσίες υπάρχουν στο Deep Web. Ακόμα και οι ιστοσελίδες που τους διαφημίζουν αναγνωρίζουν την άκρως μυστική φύση της δραστηριότητάς τους. Μία ιστοσελίδα για παράδειγμα, αναφέρει σαφώς ότι όλα τα συμβόλαια είναι ιδιωτικά, δεν μπορούν να προσφέρουν απόδειξη για την εμπειρία του υποψηφίου εκτελεστή ή τις επιτυχίες τους ή πληροφορίες από

προηγούμενους πελάτες.

Αντ' αυτού, ζητούν από τους χρήστες να αποδείξουν εκ των προτέρων ότι έχουν αρκετά Bitcoins για την δουλειά μέσω μιας αξιόπιστης υπηρεσίας μεσεγγυήσεων. Μόνο όταν ο εκτελεστής πραγματοποιήσει την δολοφονία και παρέχει αποδείξεις γι' αυτό, θα αποδεσμευθεί το ποσό.



C'thulhu

Email:

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL. Highly skilled, with military experience of more than five years. We can perform hits all around the world.

If you're asking yourself "Why someone would need to hire a killer online?", we'll tell you: simply because it is anonymous. You can always find examples of contractors who collaborated willingly (when they were facing no years of prison), and you (the buyer) could end up in the prison because of that. On the other hand, you can also find examples where police found who had the internet to put out a contract, and they can come to you and you can give your testimony (which would put the killman in jail).

So, it is of mutual interest to make everything anonymous. The website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins. It means we don't know you and you don't know us. We can't send you to prison, and you can't send us in prison. Of course you must take a risk when you pay in advance, but there is no internet. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face six years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don't contact this kind of organizations. And know, we are only one, real contractor there. Any other will cry about you. — Contract Killer © 2014.

or

No fish too big, no fish too small - HITMAN does it all!

Q & A!

Can I see some proofs of your last work?

Every contract is Private, and all data is Purged after elimination proof is sent to the customer. It is Mandatory for Customer's and our Security!

Can You give me contact to person who already used your services?

Again, Every contract is Private! Without Exceptions! And we will never store or share such info after completing.

Can you give to me a good feedback about, you and some proofs of succeeded work?

Sorry, but no one of our happy customers stay on forums, or have time to post feedback on some trusted site. All feedbacks is written directly to our mail, and it will not show you any proof if we'll post it on our own page. And even if you'll find an feedback on an page, it was write by an random person, who don't have with as any business.

How I would can to know that you are not a scammer as else?

Simply, we don't take any prepayments. We are only who ask just for proof that you have this money in your wallet, and you'll to arrange full escrow on trusted for both third party site.

Ask more, we'll add more.

We should probably get started if you'll have at least this:

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	$45,000	$90,000	$180,000
Missing in action	$60,000	$120,000	$240,000
Death in accident	$75,000	$150,000	$300,000
Cripls Types	**Low Rank**	**Medium Rank**	**High Rank and Political**
Regular	$12,000	$24,000	$48,000
Ugliy	$18,000	$36,000	$72,000
Two Hands	$24,000	$48,000	$96,000
Paralyse	$30,000	$60,000	$120,000
Rape	**Low Rank**	**Medium Rank**	**High Rank and Political**
Regular	$7,000	$14,000	$28,000
Under age	$21,000	$42,000	$84,000
Bombing	**Low Rank**	**Medium Rank**	**High Rank and Political**
Simple	$5,000	$10,000	$20,000
Complex	$10,000	$20,000	$40,000
Beating	**Low Rank**	**Medium Rank**	**High Rank and Political**
Simple	$3,000	$9,000	$18,000

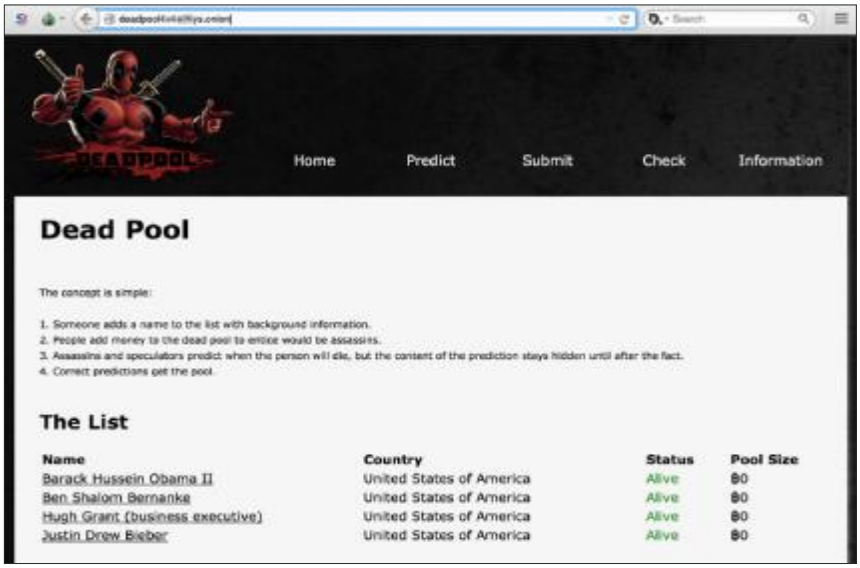
Το βιογραφικό του C'thulu για εκτελέσεις επί πληρωμή

Όπως φαίνεται, οι τιμές διαφέρουν ανάλογα με τον προτιμώμενο τρόπο θανάτου ή τραυματισμού και την θέση του στόχου. Ο Ross Ulbricht ο οποίος έχει πρόσφατα καταδικαστεί για την λειτουργία του περίφημου φόρουμ Silk

Road που αφορούσε την πώληση παράνομων ναρκωτικών, στην πραγματικότητα προσπάθησε να πληρώσει για την δολοφονία πέντε από τους συνεταίρους του.

Μια διαφορετική λύση για τις εν λόγω υπηρεσίες, που ελπίζουμε να μην είναι στην πραγματικότητα πραγματική υπηρεσία, είναι η crowdsourced δολοφονία (κάτι σαν ανοικτή πρόσκληση εθελοντών για συμμετοχή σε δολοφονία). Μία ιστοσελίδα, η Dead Pool, επιτρέπει στους χρήστες να προβάλλουν πιθανούς στόχους. Οι άλλοι μπορούν στην συνέχεια να συνεισφέρουν κεφάλαια με τη μορφή Bitcoins στην «dead pool».

Οι δολοφόνοι μπορούν στην συνέχεια να «προβλέψουν» ανώνυμα πότε και πώς θα δολοφονηθούν οι στόχοι. Αν το άτομο πεθάνει στην πραγματικότητα, αποκαλύπτονται όλες οι προβλέψεις και οι δολοφόνοι που προέβλεψαν σωστά μπορούν να διεκδικήσουν τα χρήματα. Μέχρι σήμερα, έχουν προταθεί τέσσερα ονόματα, αλλά δεν έχουν τοποθετηθεί χρήματα στο «dead pool», οδηγώντας μας στο συμπέρασμα ότι η ιστοσελίδα μάλλον είναι φάρσα.



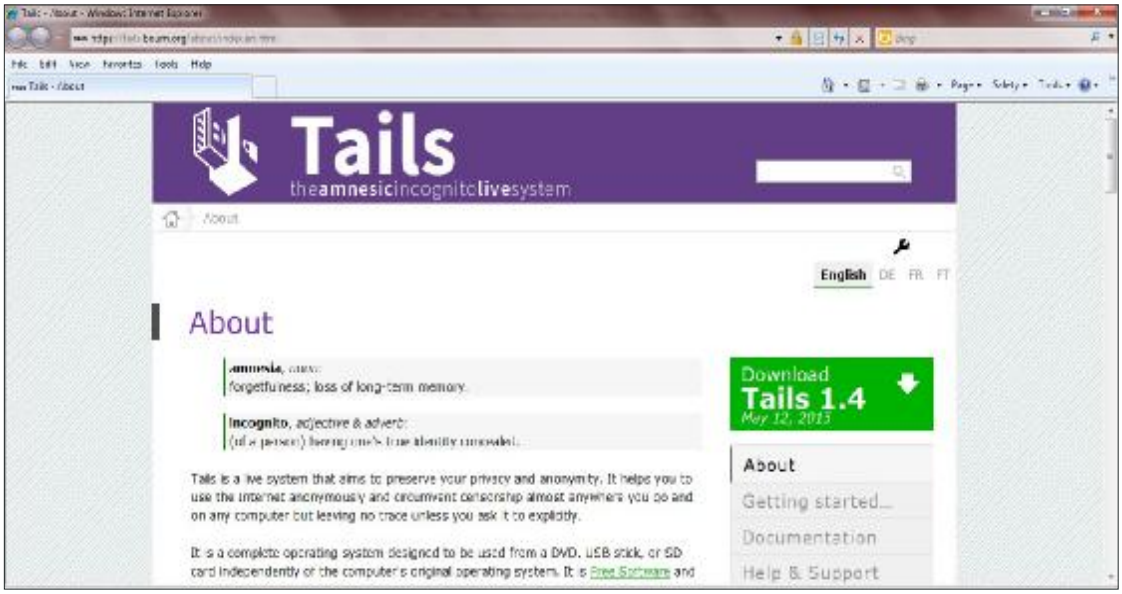
Dead Pool, μία ιστοσελίδα για προβλέψεις δολοφονιών

4.9 Το Deep Web και ο πραγματικός κόσμος

Υπηρεσίες που βασίζονται σε TLD κακοποιούς φύσεως ή Namecoins

που προσφέρουν πολύ υψηλό εμπόδιο έγκρισης σε ενα κοινό χρηστών και πολύ λίγα πλεονεκτήματα για τους μέσους χρήστες ώστε να θεωρούνται δημόσια σημαντικοί. Αλλά υπάρχουν ολοένα και περισσότερες βελτιώσεις χρηστικότητας σε συστήματα όπως το I2P και ιδιαίτερα το TOR που σιγά-σιγά έχουν μετατραπεί σε βιώσιμες λύσεις ώστε καθένας να μπορεί να περιηγείται στο διαδίκτυο με πλήρη ανωνυμία με μόλις κάποιες απαιτήσεις εγκατάστασης.

Πλέον διατίθενται εφαρμογές TOR με ενσωματωμένους ανώνυμους browsers για όλες τις κύριες επιφάνειες εργασίας και κινητές πλατφόρμες, επιτρέποντας σε όλους να περιηγηθούν στο διαδίκτυο ανώνυμα και να έχουν πρόσβαση σε κρυμμένες ιστοσελίδες με λίγες κινήσεις. Για τους δημοσιογράφους και τους ανθρώπους που απαιτούν ένα ακόμα υψηλότερο επίπεδο προστασίας της ιδιωτικής τους ζωής, ένα πλήρως προσαρμοσμένο λειτουργικό σύστημα ενσωμάτωσης TOR και ανώνυμων προγραμμάτων περιήγησης μπορεί να μεταφορτωθεί και να εγκατασταθεί σε ένα κλειδί USB για χρήση σε οποιοδήποτε διαθέσιμο μηχάνημα.



Παράδειγμα ενός προγράμματος ανωνυμίας που μπορεί να μεταφορτωθεί από το διαδίκτυο

4.10 Πραγματική ανωνυμία

Στην πράξη, η κίνηση μεταξύ δύο κόμβων TOR δεν είναι ανιχνεύσιμη, αλλά η κίνηση προς και από την είσοδο και την έξοδο στις πύλες TOR είναι. Αν ένας οργανισμός λειτουργεί αρκετές πύλες TOR, υπάρχει μία πιθανότητα η κίνηση στο δίκτυο TOR να μπορεί να παρακολουθηθεί. Χρησιμοποιώντας TOR σε χώρες που δεν έχουν αρκετό προϋπολογισμό για να λειτουργήσουν μία κρίσιμη μάζα κόμβων πύλης μπορεί να θεωρηθεί ασφαλής. Αλλά και σε άλλες χώρες με προϋπολογισμούς μυστικών υπηρεσιών αρκετά υψηλούς, όπως οι Ηνωμένες Πολιτείες ή η Κίνα, η χρήση του TOR μπορεί να μην είναι εξίσου ασφαλής.

Επιπλέον, κάθε σύστημα ανωνυμοποίησης είναι αποτελεσματικό όσο ο χρήστης του. Όσο προηγμένο και να είναι ένα σύστημα ανωνυμοποίησης, ακόμη και εκείνα όπως το TOR και το I2P, καλύπτει μόνο το επίπεδο μεταφοράς της επικοινωνίας, αλλά παραμένει ανίσχυροι ως προς το περιεχόμενο της επικοινωνίας. Με απλά λόγια, κανένα σύστημα ανωνυμοποίησης δεν μπορεί να κρύψει έναν χρήστη που καταχωρεί την διεύθυνση του σπιτιού του και αναρτά τα στοιχεία του δημοσίως.

Μπορούμε λοιπόν να διαχωρίσουμε δύο βασικά είδη κινδύνων που συνδέονται με την ανωνυμία στο Deep Web: τις περιβαλλοντικές ευπάθειες και τις κοινωνικές ευπάθειες. Οι περιβαλλοντικές ευπάθειες αναφέρονται σε κάθε πιθανό ελάττωμα που μπορεί να συνδεθεί με άλλο λογισμικό που χρησιμοποιείται σε συνδυασμό με το TOR. Για παράδειγμα, ένα περιβόητο σφάλμα που επηρεάζει την έκδοση Adobe® Flash® που είναι ενσωματωμένη στο πρόγραμμα περιήγησης που συμπεριλαμβάνει μια έκδοση TOR, έθεσε ολόκληρο το σύστημα σε κίνδυνο, δεδομένου ότι ήταν δυνατό να χρησιμοποιηθεί το σφάλμα για την διαρροή ευαίσθητων δεδομένων, παρά την χρήση του TOR.

Οι κοινωνικές ευπάθειες σχετίζονται με την συμπεριφορά των χρηστών και τις προφυλάξεις που λαμβάνουν οι χρήστες, εκτός από την απλή χρήση TOR. Ο Dread Pirate Roberts, ο οποίος πρόσφατα καταδικάστηκε σε ισόβια κάθειρξη λόγω της ηλεκτρονικής αγοράς που είχε στήσει στο Deep αγορά,

πιάστηκε από το FBI λόγω της χρήσης του από μια ιδιωτική διεύθυνση ηλεκτρονικού ταχυδρομείου σε ένα δημόσιο φόρουμ. Ο συσχετισμός των ταυτοτήτων των χρηστών του Deep Web με την ταυτότητά τους στο Surface Web αποτελεί ένα ενδιαφέρον ερευνητικό πεδίο που περιλαμβάνει κλάδους όπως η ανάλυση κοινωνικών δικτύων και η στυλομετρία.

«*Αν πάτε στον γιατρό και υποβληθείτε σε χειρουργική επέμβαση και ξυπνήσετε στο δωμάτιο του νοσοκομείου σας και παραβιάσετε όλους τους κανόνες υγιεινής, θα πεθάνετε, ακόμη και αν έχετε τους καλύτερους χειρουργούς, τα καλύτερα εργαλεία, το καλύτερο νοσοκομείο. Το ίδιο ισχύει και με την ανωνυμία, αν δεν συμπεριφέρεστε συνετά, ακόμη και τα καλύτερα εργαλεία δεν θα μπορέσουν να σας προστατεύσουν*».

Martin Rösler, Ανώτερος Διευθυντής, Έρευνες Απειλών

4.11 Αρχές επιβολής του νόμου και Deep Web

Οι αρχές επιβολής του νόμου αντιμετωπίζουν ήδη αρκετές προκλήσεις, όσον αφορά στο διεθνές έγκλημα στο Web Surfac. Σε σχέση με το Deep Web, τρεις συμπληρωματικές πτυχές ενδεχομένως να προβληματίζουν ακόμη περισσότερο τις αρχές επιβολής του νόμου.

Κρυπτογράφηση: Τα πάντα στο Deep Web ή στο Dark Web είναι κρυπτογραφημένα. Αυτό σημαίνει ότι οι εγκληματίες σε αυτό είναι πολύ πιο ενήμεροι για τις παγίδες και τις παρακολουθήσεις. Η κρυπτογράφηση αποτελεί το πρώτο αντίμετρό τους για να αποφύγουν τον εντοπισμό τους.

Απόδοση: Είναι εξαιρετικά δύσκολο να προσδιοριστεί η απόδοση. Όλα συμβαίνουν σε τομείς .onion. Η δρομολόγηση σε αυτούς τους τομείς είναι επίσης ασαφής.

Διακύμανση: Το Deep Web είναι ένας πολύ δυναμικός χώρος. Ένα online φόρουμ μπορεί να είναι σε μια συγκεκριμένη διεύθυνση URL μια μέρα και την επόμενη να μην είναι. Τα συστήματα ονοματοδότησης και διευθυνσιοδότησης του Deep Web αλλάζουν συχνά. Αυτό σημαίνει ότι οι πληροφορίες που συλλέξαμε πριν από δύο εβδομάδες δεν είναι πλέον

επίκαιρες σήμερα. Αυτό έχει επιπτώσεις στην απόδειξη του εγκλήματος. Λαμβάνοντας υπόψη το χρονικό πλαίσιο στο οποίο δικάστηκαν ποινικές υποθέσεις, οι αρχές επιβολής του νόμου πρέπει να είναι σε θέση να τεκμηριώσουν αυστηρά οποιαδήποτε εγκληματική δραστηριότητα στο διαδίκτυο μέσω screenshots με χρονοσήμανση, προκειμένου να αποφευχθεί η ακύρωση των περιπτώσεων.

4.12 Ο ρόλος των πωλητών λογισμικού ασφαλείας

Ενώ η πλειοψηφία των κανονικών χρηστών του Διαδικτύου δεν θα βρει κάποια χρήση για το Deep Web, οι πωλητές λογισμικού ασφαλείας πρέπει να εξακολουθούν να είναι σε θέση να προστατεύσουν τους πελάτες τους από τις εγκληματικές δραστηριότητες του κυβερνοχώρου που πραγματοποιούνται μέσα από αυτό. Τα προγράμματα malware χρησιμοποιούν ολοένα και περισσότερο το TOR και οι πωλητές λογισμικού ασφαλείας πρέπει να είναι σε θέση να δημιουργήσουν μέσα έγκαιρης ανίχνευσης και αντίμετρα κατά αυτών των απειλών, καθώς αργά ή γρήγορα θα βρεθεί τρόπος ώστε οι χρήστες του Surface Web να μετατραπούν σε θύματα.

Από την άλλη πλευρά, υπάρχουν χρήστες που, για νόμιμους λόγους, πρέπει να επισκέπτονται το Deep Web, προκειμένου να αποφύγουν την κοινωνική κριτική επειδή αγοράζουν συνταγογραφούμενα φάρμακα για ορισμένες παθήσεις, την πρόσβαση σε ψυχαγωγικά φάρμακα που είναι παράνομα σε ορισμένες γεωγραφικές περιοχές, για να συζητούν ελεύθερα κοινωνικά απαγορευμένα θέματα ή να μοιράζονται πληροφορίες από χώρες με καταπιεστικά καθεστώτα στις οποίες διαμένουν. Σε αυτές τις περιπτώσεις, οι πωλητές λογισμικού ασφαλείας εξακολουθούν να έχουν την ευθύνη στο να προστατεύσουν τους πελάτες τους. Αυτός είναι και ο λόγος που Ερευνητική Ομάδα του Trend Micro συνεχίζει να παρακολουθεί αυτές τις ηλεκτρονικές περιοχές.

4.13 Το μέλλον του Deep Web

Ενώ η ευαισθητοποίηση του κοινού μπορεί να οδηγήσει σε αυξημένη

χρήση ή ενδιαφέρον για το Dark Web και άλλες παρόμοιες ιστοσελίδες στο Deep Web, οι χρήστες σήμερα δεν έχουν σημαντικό λόγο να κάνουν περιήγηση στο Διαδίκτυο με εξειδικευμένο λογισμικό ανωνυμοποίησης στο εγγύς μέλλον.

Εν τω μεταξύ, είναι πολύ πιο πιθανό οι τεχνολογικές εξελίξεις που σχετίζονται με το Dark Web να βελτιώσουν την μυστικότητα των darknets. Αυτήν την στιγμή, φαίνεται να υπάρχει ένας αγώνας μεταξύ των «ακραίων ελευθεριακών» και των αρχών επιβολής του νόμου, με τους πρώτους να προσπαθούν να βρουν νέους τρόπους για να γίνουν ακόμη πιο ανώνυμες και μη ανιχνεύσιμες οι διαδικτυακές περιηγήσεις τους από τις αρχές.

Αλλά δεδομένου ότι το εμπόριο παράνομων εμπορευμάτων είναι μία από τις κύριες επιχειρηματικές δραστηριότητες που λαμβάνουν χώρα στο Deep Web, είναι πλέον απαραίτητο στο πλαίσιο της υψηλής ανωνυμίας, να μπορεί να υπάρξει εγγύηση για την εμπιστοσύνη και την φήμη ανάμεσα στους πωλητές και τους αγοραστές, χωρίς να χρειάζεται να στηρίζονται σε μια εξωτερική αρχή όπως ένα τραπεζικό ίδρυμα όπως στο «κανονικό» ηλεκτρονικό εμπότιο.

Διαβλέπετε η άνοδος νέων, πλήρως αποκεντρωμένων αγορών που θα βασίζονται στην τεχνολογία blockchain την οποία τα Bitcoins και άλλα κρυπτονομίσματα ήδη εκμεταλλεύονται για την μεταφορά και την αποθήκευση. Ως εκ τούτου, η τεχνολογία θα χρησιμοποιηθεί για την υλοποίηση πλήρως ανεπτυγμένων αγορών χωρίς κάποιος σημείο αποτυχίας και θα βασίζονται σε συγκεκριμένες πτυχές της θεωρίας παιγνίων για την εγγύηση των ασφαλών συναλλαγών, των μηχανισμών μεσεγγύησης και την εμπιστοσύνη μεταξύ των παραγόντων.

Τα κρυπτο-νομίσματα συμβαδίζουν με τις αγορές στο Deep Web. Συναφώς, ενδέχεται να δούμε νέους, προηγμένους τρόπους που θα κάνουν τα Bitcoins ακόμη λιγότερο ανιχνεύσιμα από ό,τι είναι τώρα. Υπάρχει επίσης μια τεράστια δυνατότητα για κακόβουλο λογισμικό το οποίο θα εκμεταλλεύεται την τεχνολογία blockchain για να ενσωματώνεται και να λειτουργεί με έναν νέο και πλήρως αποκεντρωμένο τρόπο.

ΚΕΦΑΛΑΙΟ 5 ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ

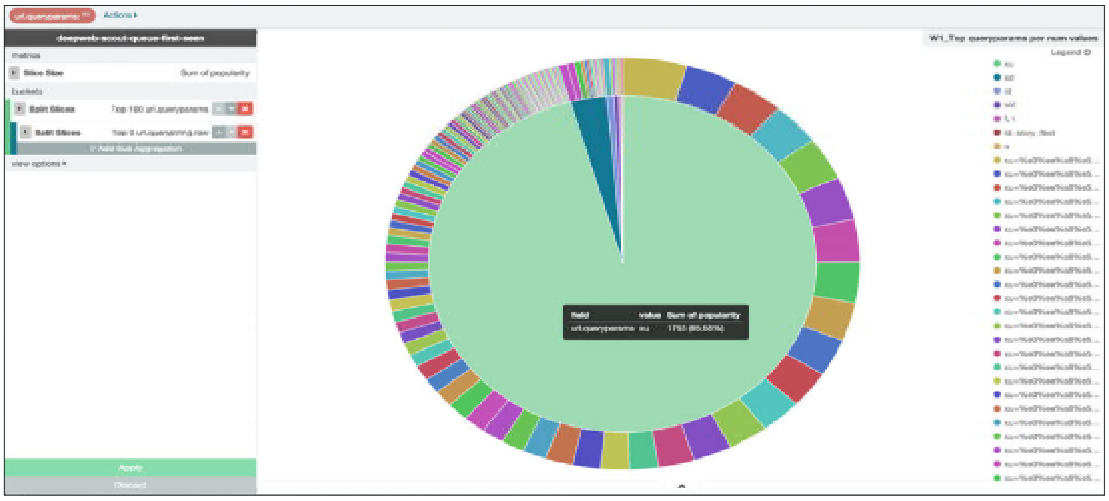
Η σύλληψη του NionSpy (γνωστός και ως Mewsei ή MewsSpy)

Στο ακόλουθο παράδειγμα που σχετίζεται με κακόβουλο λογισμικό που υποκλέπτει εμπιστευτικές πληροφορίες, αναζητήθηκαν οι παράμετροι της διαδεδομένης συμβολοσειράς ερωτήματος σε ένα σύντομο και πρόσφατο χρονικό παράθυρο. Αυτό επέτρεψε τον προσδιορισμό των νέων απειλών από την στιγμή που εμφανίστηκε στο Deep Web. Ειδικότερα, οι δύο παράμετροι, Xu και xD, παρουσίασαν μία απότομη αύξηση στην δημοτικότητά τους κατά την τελευταία εβδομάδα.

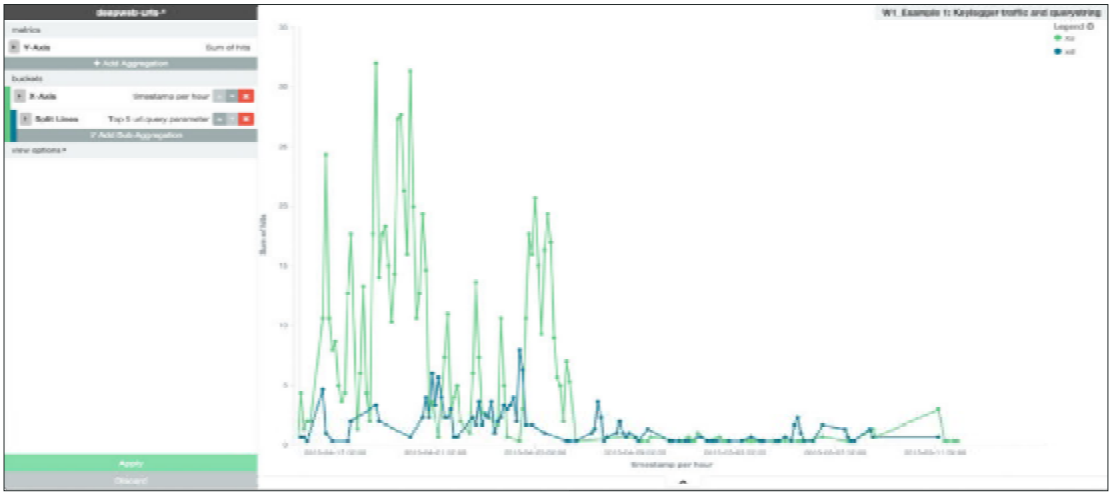
Η Xu συνδέθηκε με περισσότερες από 1.700 διακριτές τιμές που αποτελούνται από δυαδικά μεγάλα αντικείμενα. Περαιτέρω έρευνα αποκάλυψε ότι η Xu χρησιμοποιήθηκε από τον NionSpy για την διαρροή κλεμμένων διαπιστευτηρίων (ηλεκτρονικής τραπεζικής κλπ.), τα οποία στην συνέχεια λήφθηκαν από ένα keylogger και δημοσιεύθηκαν σε μια ζώνη εναπόθεσης στο Deep Web. Η Xd, εν τω μεταξύ, χρησιμοποιήθηκε για την καταχώρηση μιας νέας μόλυνσης στο botnet. Η εγγραφή αυτή περιελάμβανε πληροφορίες όπως το όνομα του μηχανήματος του θύματος και την έκδοση του λειτουργικού συστήματος, η οποία κοινοποιήθηκε σε μορφή συμβολοσειράς JSON ως εξής:

[REDACTED]2xx.onion:80/si.php?xd={“f155”:”MACHINEIP”,”f4336”:”MACHINE
NAME”,”f7035”:”5.9.1.1”,”f1121”:”windows”,”f6463”:””,”f2015”:”1”}

Μετρώντας τα ερωτήματα που σχετίστηκαν με την εγγραφή, ήμασταν σε θέση να δημιουργήσουμε ένα προφίλ του αριθμού των νέων θυμάτων ανά ημέρα, μαζί με την ποσότητα των δεδομένων που διαρρέονταν.



Πιο διαδεδομένες παράμετροι συμβολοσειράς ερωτήματος URI (σε αξία)



Αριθμός νέων θυμάτων ανά ημέρα (σε μπλε χρώμα) και κίνηση στην ζώνη εναπόθεσης (με πράσινο χρώμα)

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ερευνητική ομάδα της Trend Micro ανέπτυξε το Deep Web Analyzer, ένα ισχυρό σύστημα που συλλέγει URL ενδιαφέροντος από το Deep Web, ώστε να μπορούμε να ρίξουμε μια πιο προσεκτική ματιά στο τι συμβαίνει στο Deep Web σε σχέση με το έγκλημα στον κυβερνοχώρο. Με βάση την διετή έρευνα με τον Deep Web Analyzer σε δίκτυα περιορισμένης πρόσβασης, όπως το Dark Web, ήμασταν σε θέση να προσδιορίσουμε ότι το Deep Web φιλοξενεί ιστοσελίδες με κακοήθες περιεχόμενο, μαζί με μερικές από τις πιο ενοχλητικές δραστηριότητες που έχουμε δει ποτέ σε σχέση με το Διαδίκτυο κι έτσι αποκτήσαμε μια βαθύτερη κατανόηση της φύσης του.

Ενώ το 47% των τομέων που παρακολουθήθηκαν με επιτυχία χρησιμοποιούν την αγγλική γλώσσα, η ρωσική εκτόπισε την αγγλική από την πρώτη θέση, όταν έγινε καταμέτρηση των URL. Αυτό θα μπορούσε να αποδοθεί στην ύπαρξη ενός μεγάλου ρωσικού φόρουμ κατά την στιγμή της ανάλυσης.

Τα πιο βαριά εμπορεύσιμα αγαθά με βάση την ανάλυση των κορυφαίων 15 πωλητών στο Deep Web ήταν τα ήπια ναρκωτικά, μετά τα συνταγογραφούμενα φάρμακα όπως το Ritalin και το Xanax και συνθετικές, απαγορευμένες ναρκωτικές ουσίες.

Το Deep Web χρησιμοποιεί σε μεγάλο βαθμό πρωτόκολλα έξω από το πρότυπο HTTP / HTTPS, συνηθέστερα IRC, IRCS, Gopher, XMPP και FTP.

Εντοπίστηκαν χιλιάδες ύποπτες σελίδες, από σελίδες που φιλοξενούν κακόβουλα adware μέχρι σελίδες που χρησιμοποιούνται για την εκμετάλλευση παιδιών.

Ορισμένα μέρη του Deep Web έχουν μετατραπεί σε ασφαλές καταφύγιο για τους διάφορους εγκληματίες του κυβερνοχώρου και τις εγκληματικές τους δραστηριότητες.

Οι διαδεδομένες οικογένειες malware όπως το VAWTRAK και το CryptoLocker χρησιμοποιούν το TOR ως μέρος της διαμόρφωσής τους.

Το κατέβασμα εγκληματικών αγορών δεν αποτελεί μία ιδιαίτερα

διαρκή ή εύστοχη λύση κατά του εμπορίου ναρκωτικών, καθώς εξακολουθούν να υπάρχουν ηλεκτρονικά καταστήματα και φόρουμ που εξυπηρετούν την ζήτηση για παράνομα ναρκωτικά.

Το Deep Web είναι επίσης γεμάτο με υπηρεσίες νομιμοποίησης εσόδων από παράνομες δραστηριότητες με Bitcoin, όπως το EasyCoin για την περαιτέρω αύξηση της ανωνυμίας στην μεταφορά χρημάτων μέσω του συστήματος Bitcoin.

Ένας υπόκοσμος των εγκληματιών του κυβερνοχώρου σίγουρα λειτουργεί στο Deep Web. Κλεμμένοι λογαριασμοί, διαβατήρια και ταυτότητες προσωπικοτήτων υψηλού προφίλ πωλούνται σε φόρουμ με επαγγελματική εμφάνιση και με πλήρεις πληροφορίες τιμολόγησης και περιγραφές. Επίσης στο Deep Web διαφημίζονται και προσφέρονται υπηρεσίες δολοφονίας.

Ενώ δεν είναι πιθανό για την πλειοψηφία των χρηστών του Διαδικτύου να βρουν κάποιον λόγο για να χρησιμοποιήσουν το Dark Web, η ανωνυμία του Deep Web θα συνεχίσει να εγείρει πολλά ζητήματα και αποτελεί ένα σημείο ενδιαφέροντος και τόσο για τις αρχές επιβολής του νόμου, όσο και για τους χρήστες του Διαδικτύου που θέλουν να παρακάμψουν την κρατική επιτήρηση και παρέμβαση. Ως εκ τούτου, οι υπερασπιστές της ασφάλειας, όπως η Trend Micro πρέπει να συνεχίσουν να παρακολουθούν το Deep Web, καθώς ο ρόλος του στο διαδίκτυο μεγαλώνει

ΒΙΒΛΙΟΓΡΑΦΙΑ

Beard, K.W. (2005), Internet Addiction: A review of current assessment techniques and potential assessment questions, *Cyber Psychology & Behavior*, 8(1)

Bergman, M. K (2001). «The Deep Web: Surfacing Hidden Value». *The Journal of Electronic Publishing* **7**(1).

Ciancaglini V. (2013). TrendLabs Security Intelligence Blog. "The Boys Are Back in Town: Deep Web Marketplaces Back Online http://blog.trendmicro.com/trendlabs-security-intelligence/the-boys- are-back-in-town-deep-web-marketplaces-back-online/.

Ciancaglini V. (2015). TrendLabs Security Intelligence Blog. "The Deep Web: Shutdowns, New Sites, New Tools." http://blog.trendmicro.com/trendlabs-security-intelligence/the-deep-web-shutdowns-new-sites- new-tools/.

Ciancaglini, V."(2015) Marco Balduzzi, Max Goncharov, and Robert McArdle. Trend Micro Security Intelligence. "Deep Web and Cybercrime: It's Not All About Tor." http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf.

David Sancho. (2015). TrendLabs Security Intelligence Blog. "Steganography and Malware: Why and How." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/.

David Sancho. (2015). TrendLabs Security Intelligence Blog. "Steganography and Malware: Why and How." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/.

David Sancho. (2015). TrendLabs Security Intelligence Blog. "Steganography and Malware: Concealing Code and C&C Traffic." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware- concealing-code-and-cc-traffic/

David Sancho. (2015). TrendLabs Security Intelligence Blog. “Steganography and Malware: Final Thoughts.” Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-final-thoughts/.

Davis R.A., Flett G.L. and Besser A. (2002), Validation of new scale for measuring problematic internet use: implication for pre-employment screening, *Cyber Psychology and Behavior*, 5; Davis, R.A. (2001), A cognitive-behavioral model of pathological Internet use, *Computers in Human Behavior*, 17 (2)

Davis, R.A. (2001), A cognitive-behavioral model of pathological Internet use, *Computers in Human Behavior*, 17 (2)

de Viana, I. F., Hernandez, I., Jiménez, P., Rivero, C. R., & Sleiman, H. A. (2010). Integrating deep-web information sources. In Trends in Practical Applications of Agents and Multiagent Systems (pp. 311-320). Springer Berlin Heidelberg.

Denis Shestakov (2011). «Sampling the National Deep Web» (PDF). *Proceedings of the 22nd International Conference on Database and Expert Systems Applications (DEXA)*. Springer, pp. 331-340.

Denis Shestakov (2011). «Sampling the National Deep Web»(PDF). *Proceedings of the 22nd International Conference on Database and Expert Systems Applications (DEXA)*. Springer, pp. 331-340.

Dudeney, G. (2000). «*The Internet and the Language Classroom*». Cambridge: Cambridge University Press

Feike Hacquebord. (2015). TrendLabs Security Intelligence Blog. “The Mysterious MEVADE Malware.” Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-mysterious-mevade-malware/.

Goldberg I. (1995), *Internet addiction disorder,* Retrieved from: http://web.urz.uni-heidelberg.de/Netzdienste/anleitung/wwwtips/8/addict.html

[πρόσβαση 27-6-2016]

Goldberg I. (1996), *Internet Addiction*, Retrieved from: http://www.cmhc/mlists/research [πρόσβαση 27-6-2016]

Griffiths M. (1998), *Internet Addiction: Does It Really Exist? Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Applications*, New York: Academic Press

Griffiths M. (2000), Does internet and computer «Addiction» exist? Some case study evidence, *Cyber Psychology & Behavior*, 3(2)

He, Bin; Patel, Mitesh; Zhang, Zhen; Chang, Kevin Chen-Chuan (May 2007). «Accessing the Deep Web: A Survey».*Communications of the ACM (CACM)* **50** (2): 94–101

Jay Yaneza. (2014). TrendLabs Security Intelligence Blog. "Defending Against TOR-Using Malware, Part 1." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-TOR-using- malware-part-1/

Jay Yaneza. (2014). TrendLabs Security Intelligence Blog. "Defending Against TOR-Using Malware, Part 2." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-TOR-using-malware- part-2/

Jones, S. (2002). The Internet goes to college: how students are living in the future with today's technology. *Pew Internet & American Life Project*, http://www.pewinternet.org/ [πρόσβαση στις 27-6-2015]

Klawe, M. and Philips, E. (1995). A classroom Study: Electronic Games Engage Children as Researchers. *Proceedings of CSCL '95 Conference*, Bloomington, Indiana

Lesk M. (1997) "How much information is there in the world?".

Madhan, A.(2015) How to access the deep web using tor browser?, Available from: http://www.tech-wiki.com/how-to-access-the-deep-web-with-tor/[Accessed 24-6-2016]

Madhavan, J., Afanasiev, L., Antova, L., & Halevy, A. (2009). Harnessing the deep web: Present and future. arXiv preprint arXiv:0909.1785.

Madhavan, J., Ko, D., Kot, Ł., Ganapathy, V., Rasmussen, A., & Halevy, A. (2008). Google's deep web crawl. Proceedings of the VLDB Endowment, 1(2), 1241-1252.

Markham J (2001), The future of shopping: Traditional Patterns and Net Effects, MacMillan Business

Michael, Lesk. "*How much information is there in the world?*".Retrieved on 2009-02-24.

Ntoulas, A., Zerfos, P., & Cho, J. (2004). Downloading hidden web content. Technicalreport, UCLA.

Paul B and Bryant JA. (2005). Adolescents and the internet. *Adolesc Med Clin.* 16(2):413-26.

Robert McArdle and David Sancho. Trend Micro Security Intelligence. "Bitcoin Domains." Last accessed on 10 June 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-bitcoin-domains.pdf.

Robert McArdle and David Sancho.(2015) Trend Micro Security Intelligence. "Bitcoin Domains." http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-bitcoin-domains.pdf.

Robert McArdle. (2013). TrendLabs Security Intelligence Blog. "Cybercrime in the Deep Web." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-in-the-deepweb/.

Rong, D., Hao, W., & Xin, Z. (2012). The Design of Deep Web Search Engine Based on Domain Knowledge. In Future Control and Automation (pp. 315-321). Springer Berlin Heidelberg.

Rowan W (2002), *Digital Marketing: using new technologies to get closer to your customers*, Kogan Page London

Scribd. "Ulbricht Criminal Complaint."(2015) http://www.scribd.com/doc/172768269/ Ulbricht-Criminal-Complaint.

Siomos, K., Dafouli E., Braimiotis D., Mouzas O. and Angelopoulos N.

(2008). Internet Addiction among Greek Adolescent Students. *Cyberpsychology & Behaviour*. Volume 11, Number 6

Siomos, K., Dafouli E., Braimiotis D., Mouzas O. and Angelopoulos N. (2008). Internet Addiction among Greek Adolescent Students. *Cyberpsychology & Behaviour*. Volume 11, Number 6

The Tor Project, Inc. Tor Project. Last accessed on 11 June 2015, https://www.torproject.org/.

Tikk, D., Kardkovács, Z. T., & Magyar, G. (2007). Searching the deep web: the WOW project. In Advances in Information Systems Development (pp. 493-504). Springer US.

Trend Micro Incorporated. Trend Micro Security News. "Cybercriminal Underground Economy Series." Last accessed 11 June 2015, http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/index.html.

Turban E (2002), Electronic Commerce: A managerial perspective, Prentice Hall7

ulbr_mirror. Scribd. "Ulbricht Criminal Complaint." Last accessed on 10 June 2015, http://www.scribd.com/doc/172768269/ Ulbricht-Criminal-Complaint.

Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, and Robert McArdle. Trend Micro Security Intelligence. "Deep Web and Cybercrime: It's Not All About Tor." Last accessed on 10 June 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf.

Vincenzo Ciancaglini. (2013). TrendLabs Security Intelligence Blog. "The Boys Are Back in Town: Deep Web Marketplaces Back Online." Last accessed on 10 June 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/the-boys- are-back-in-town-deep-web-marketplaces-back-online/.

Vincenzo Ciancaglini. (2015). TrendLabs Security Intelligence Blog. "The Deep Web: Shutdowns, New Sites, New Tools." Last accessed on 10 June 2015,

http://blog.trendmicro.com/trendlabs-security-intelligence/the-deep-web-shutdowns-new-sites- new-tools/.

Wang, F., & Agrawal, G. (2009, June). Seedeep: A system for exploring and querying scientific deep web data sources. In Scientific and Statistical Database Management (pp. 74-82). Springer Berlin Heidelberg.

Wang, F., Agrawal, G., & Jin, R. (2008). Query planning for searching inter-dependent deep-web databases. In Scientific and Statistical Database Management (pp. 24-41). Springer Berlin Heidelberg.

Wang, J., & Lochovsky, F. H. (2003). Data extraction and label assignment for web databases. In *Proceedings of the 12th international conference on World Wide Web* (pp. 187-196). ACM.

Weiss, P.L., Rand, D. and Katz, N. (2004). Video capture virtual reality as a flexible and effective rehabilitation tool. *Journal of Neuroengineering and Rehabilitation* 1(12).

Weiss, P.L., Rand, D. and Katz, N. (2004). Video capture virtual reality as a flexible and effective rehabilitation tool. *Journal of Neuroengineering and Rehabilitation* 1(12).

White, C. (1997). Technology and social studies: an introduction. *Social Education*, 61(3), 147-149

Wright, A.(2009). «Exploring a 'Deep Web' That Google Can’t Grasp». *The New York Times*;

Wu Cs & Cheng FF. (2007). Internet café addiction of Taiwanese adolescents. *Cyberpsychol Behav*. 10(2):220-5

Yellowlees, P. and Shayna, M. (2007). Problematic Internet use or Internet addiction? *Computers in Human Behavior* 23. 1447–1453;

Young, K.S. (1999). Internet addiction: evaluation and treatment. *Student BMJ* 7:351–352.

Zerfos, P., Cho, J., & Ntoulas, A. (2005). Downloading textual hidden web content through keyword queries. In Digital Libraries, 2005. JCDL'05. Proceedings of the 5th ACM/IEEE-CS Joint Conference on (pp. 100-109). IEEE.

Αθανάσαινα, Π. (2008). Εθισμός στο Διαδίκτυο, μια νέα μορφή εξάρτησης, *εφημερίδα Καθημερινή*

Κόκκοτας, Π., Βλάχος, Γ. και Καρανίκας, Γ. (1995). Διδακτικές στρατηγικές για Εννοιολογική Αλλαγή στις Φυσικές Επιστήμες στο Ματσαγγούρας Η. (επιμ). *Η εξέλιξη της Διδακτικής: Επιστημολογική θεώρηση*, Αθήνα: Gutenberg

Κόμης, Β. (2012). Παιδαγωγικές δραστηριότητες με υπολογιστές στην προσχολική και στην πρώτη παιδική ηλικία. Πανεπιστήμιο Πατρών ανακτημένο από: www.ecedu.upatras.gr. [πρόσβαση στις 27-6-2016]

Ματσαγγούρας, Η. (1998). *Στρατηγικές Διδασκαλίας. Η κριτική σκέψη στη διδακτική πράξη*. Αθήνα: Gutenber

Μικρόπουλος, Τ.Α. (2006), *Ο υπολογιστής ως γνωστικό εργαλείο*. Αθήνα: Ελληνικά Γράμματα

Σιώμος Κ. και Αγγελόπουλος Ν. (2008). Διαταραχή εθισμού στο διαδικτύου, *Ψυχιατρική* 19 (1)

Τσίτσικα Α. και Φρέσκου Α. (2008). *Χρήση και Κατάχρηση Διαδικτύου*. Πρακτικά 1ου Εντατικού Σεμιναρίου στην Εφηβική Ιατρική, 1st State of The Art Adolescent Medicine Course, 31 Μαρτίου - 5 Απριλίου:21-30.