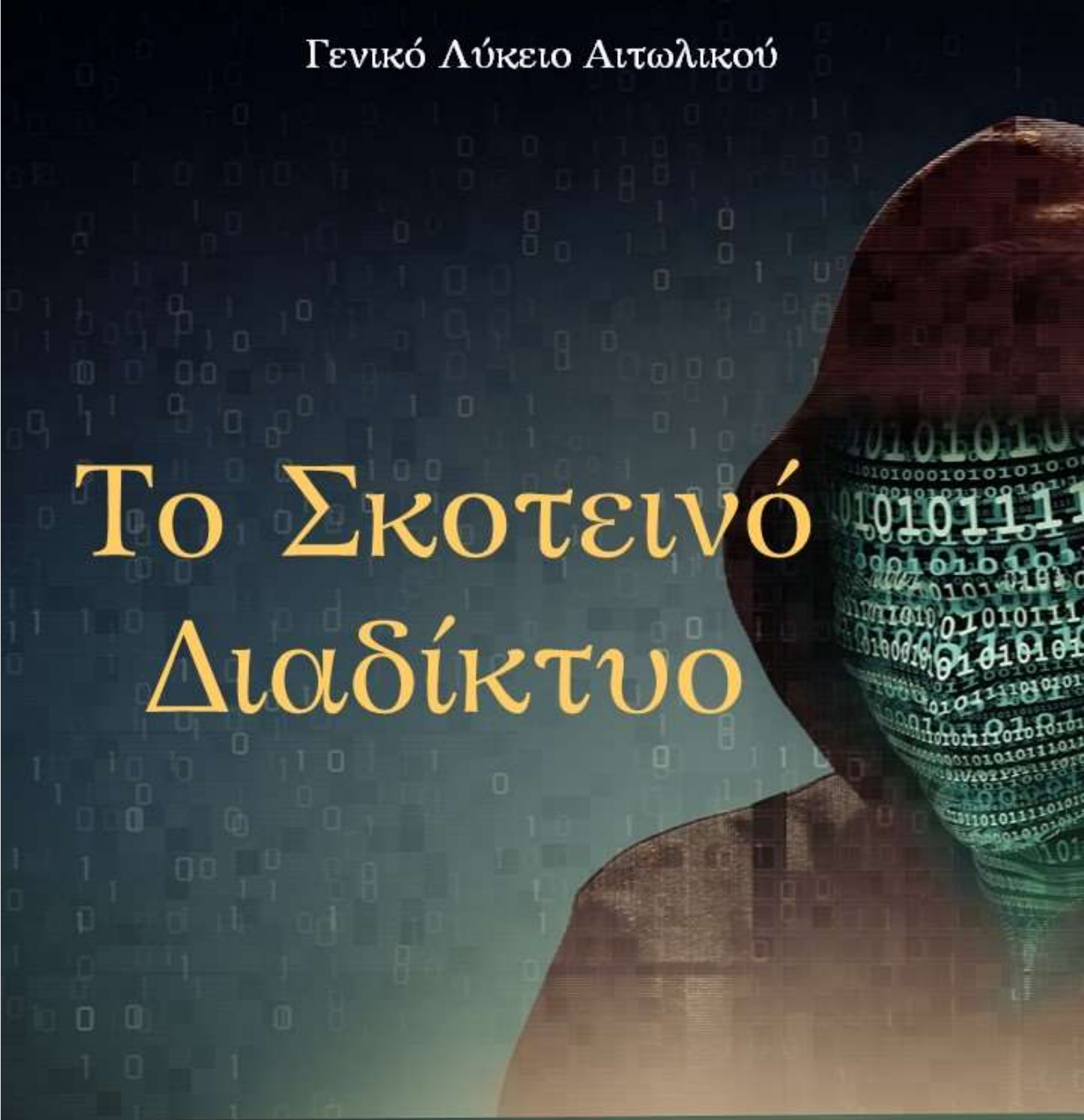
Γενικό Λύκειο Αιτωλικού

Το Σκοτεινό Διαδίκτυο



Ερευνητική Εργασία του τμήματος Α3
Α' Τετράμηνο 2018-2019
Υπεύθυνος Καθηγητής: Σαπουντζάκης Πέτρος

Αιτωλικό, Ιανουάριος 2019

Σχετικά με την εργασία

Η παρούσα ερευνητική εργασία αποτελεί προϊόν έρευνας που διεξήγαγε το τμήμα Α3 του Γενικού Λυκείου Αιτωλικού κατά τη διάρκεια του Α' Τετραμήνου του σχολικού έτους 2018-2019. Στην έρευνα συμμετείχαν οι κάτωθι μαθητές:

Ποριτσάνου Παρασκευή

Πουρνάρα Δανάη Μαρία

Πουρνάρας Νικόλαος

Ράπτης Αθανάσιος

Σκεπετάρη Φρειδερίκη

Σκόνδρα Νικολέτα

Στάμου Σπυριδούλα Μαρία

Ταμπακόπουλος Ανδρέας

Τρόκα Μαρία

Τσαντίλα Παναγιώτα

Τσίρκας Παναγιώτης

Τσοκάντας Γεώργιος

Φαράντος Γεώργιος

Φίλη Ουρανία

Φλώρος Ιωάννης

Φλώρου Μιχαηλία Παρασκευή

Φλώρου Περσεφόνη Ελένη

Χατζίου Αουρέλα

Χρυσοπούλου Ελένη

Επιβλέπων καθηγητής: Σαπουντζάκης Πέτρος

Περιεχόμενα

Κεφάλαιο 1ο: Web - Deep Web - Dark Web

Ιστορία του Παγκόσμιου Ιστού

Ο Τιμ Μπέρνερς Λι έγραψε το World Wide Web στο δεύτερο εξάμηνο του 1990 σε έναν υπολογιστή Next, κατά τη διάρκεια της εργασίας του στο CERN. Το πρώτο επιτυχές build ολοκληρώθηκε στις 25 Δεκεμβρίου 1990 και άλλα διαδοχικά build κυκλοφόρησαν μεταξύ του Μπέρνερς Λι και τους συναδέλφους του πριν διατεθεί στο ίντερνετ , τον Αύγουστο του 1991. Μέχρι τότε, ήταν αρκετοί άλλοι που συμμετείχαν στο έργο, συμπεριλαμβανομένου τον Bernd Pollerman, Poverty Cailliau, Jean - Francois Croff και ο μεταπτυχιακός φοιτητής Nicola Pellow, ο οποίος έγραψε το line - mode browser .

Αυτό που οδήγησε τον Λι στην εφεύρεση του Παγκόσμιου Ιστού ήταν το όραμα του για έναν κόσμο που ο καθένας άνθρωπος θα μπορούσε να ανταλλάσσει πληροφορίες, ιδέες και άλλα, άμεσα προσβάσιμες από τους υπόλοιπους. Το σημείο στο οποίο έδωσε πιο πολύ βάρος ήταν η μη ιεράρχηση των διασυνδεδεμένων στοιχείων. Οραματίστηκε κάθε στοιχείο του, κάθε κόμβο του ιστού αυτού ίσο ως προς την προσβασιμότητα με τα υπόλοιπα.

Το επιφανειακό Web (surface web)

Ο όρος ιστός επιφανείας, surface Web, αντιπροσωπεύει εκείνο το τμήμα του παγκόσμιου ιστού που είναι διαθέσιμο στο κοινό αναζητήσιμο με κοινές μηχανές αναζήτησης. Είναι το αντίθετο του βαθέος ιστού.

Στο επιφανειακό Web (surface web) συναντάμε τις ιστοσελίδες που επισκεπτόμαστε καθημερινά όπως το youtube ,τη wikipedia , το facebook ,το instagram , κ.λ. Συνολικά υπάρχουν περίπου 14.5 δισεκατομμύρια σελίδες. Το επιφανειακό web είναι προσβάσιμο σε οποιονδήποτε χρησιμοποιεί το internet και δεν υπάρχουν κρυφές ιστοσελίδες, ιστοσελίδες που είναι κρυφές υπάρχουν μόνο στο deep web. Μπορείς να μπεις στις σελίδες του surface web με όλες τις μηχανές αναζήτησης.

Ο βαθύς Ιστός (Deep web)

Το **deep web** είναι ένας διαδικτυακός ιστός, που εκεί εκατομμύρια χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες. Μπορεί να χρησιμοποιείται ειτε για θετικούς είτε για αρνητικούς σκοπούς. Οι περισσότερες πληροφορίες του **deep web** είναι θαμμένες μεσα σε ιστοτόπους και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Το **deep web** είναι αρκετά μεγαλύτερο από το επιφανειακό *web*. Το **dark web** δεν είναι το **deep web**, είναι μόνο ένα μέρος του **deep web**. Το **dark web** είναι τα βαθύτερα τμήματα του **deep web** που απαιτούν εξαιρετικά εξειδικευμένα εργαλεία ή εξοπλισμό για την πρόσβαση. Βρίσκεται στο βαθύτερο σημείο και οι ιδιοκτήτες του ιστότοπου έχουν περισσότερους λόγους για να κρατήσουν το περιεχόμενο τους κρυφο.
Το Deep web είναι τεράστιο και αναλογεί στο 90% ένω το Dark web αντιπροσωπεύει μόνο το 0,01%. Το Deep web δεν μπορεί να ευρετιριάσει βαθύ περιεχόμενο στον παγκόσμιο ιστό. Το Dark web είναι συχνα διαθέσιμο στο κοινό απλά πρέπει να γνωρίζεις πώς να το βρεις.

Κατηγορίες δεδομένων που εντοπίζονται στο Deep Web

1) Δυναμικό περιεχόμενο:Είναι σελίδες στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες στις οποίες συμπληρώνει στοιχεία.

2) Μη συνδεδεμένο περιεχόμενο:Είναι σελίδες που δεν συνδέονται με άλλες σελίδες.Έτσι τα crawlers που χρησιμοποιούν οι μηχανές αναζήτησης δεν βρίσκουν αποτελέσματα.

3) Περιεχόμενο περιορισμένης πρόσβασης: Είναι ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους (π.χ Robots Exclusion Standards,CAPTCHAS και άλλα)

4) Private Web : ιστοσελίδες που χρειάζεται να κάνετε login με username και password.

5) Contextual Web : είναι οι σελίδες εκείνες που το περιεχόμενο τους προσαρμοζεται ανάλογα με τον τρόπο που έχεις κάνει πρόσβαση σε αυτό.

6) Scripted content :σελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από javascript και περιεχόμενο που κατεβάζετε από Web servers μέσω Flash.

7) Non-HTML/text content :περιεχόμενο κειμένου που είναι κωδικοποιημένο σε αρχεία multimedia ή συγκεκριμένα formats που δεν μπορούν να διαβάσουν οι μηχανές αναζήτησης.

8) Οτιδήποτε δεν ακολουθεί το πρότυπο HTTP.

Όλες αυτές οι κατηγορίες δεδομένων βρίσκονται εκεί καθώς στο deep Web η περιήγηση δεν γίνεται όπως σε μια κοινή μηχανή αναζήτησης αλλα με πιο περιπολικό τρόπο.

Μερικά από τα τμήματα που αποτελούν το Deep Web είναι:

Ο Βαθύς Ιστός είναι το κομμάτι του διαδικτύου το οποίο δεν ευρετηριοποιείται από τις γνωστές μηχανές αναζήτησης. Ενώ αυτό ακούγεται περίπλοκο, στην πραγματικότητα είναι αρκετά απλό.Για παράδειγμα, τα προσωπικά μας email δεν εμφανίζονται στις μηχανές αναζήτησης, ειδάλλως ο καθένας θα είχε πρόσβαση με μια απλή αναζήτηση στο Google. Άρα, ο προσωπικός μας λογαριασμός email ανήκει πρακτικά στο Deep Web.Το ίδιο ισχύει για το προσωπικό μας e-banking, τις ρυθμίσεις του λογαριασμού μας στα social media, το διαχειριστικό περιβάλλον αν έχουμε ένα δικό μας site, κλπ.

Back-end Dashboard: Ειναι το περιβαλλον διαχειρισης μιας ιστοσελίδας.Λεγεται και wp-admin ή dashboard(λανθασμενα).Το backend δεν ειναι ποτέ ορατό στους χρηστες. Ουσιαστικα ειναι ο εγκεφαλος καθε εφαρμογης.Το front-end αλληλεπιδρα με το back-end.Ενας προγραμματιστης στο back-end κανει τα εξης:Δημιουργει νεο περιεχομενο,διαχειρίζεται τους χρηστες του,διαμορφωνει τις επιλογες ιστοτοπου και συντηρει τις εργασιες(εργασιες με κωδικα που διεπουν διασυνδεση με βαση δεδομενων οπως ηλεκτρονικα καταστηματα συνδεοντας πληρωμες μεσω διαδικτυου-online αγορες).Αρα, οπως συμπεραινουμε μια online αγορα,μια διεργασια σε μια ιστοσελιδα,μια εγγραφη σε ενα newsletter ή η αποστολη στοιχειων μεσω μιας φορμας επικοινωνιας ειναι ολα απο ενα backend κωδικα φτιαγμενο απο τους προγραμματιστες υπευθυνο να συντελει καθε μια λειτουργια.

Το Dark Web

Το **Dark Web**, σκοτεινό διαδίκτυο, είναι ένας **ανώνυμος διαδικτυακός ιστός**, όπου εκεί άγνωστοι-ανώνυμοι χρήστες έχουν πρόσβαση σε κρυφές υπηρεσίες. Το Dark Web χρησιμοποιείται είτε για καλούς είτε για κακούς σκοπούς. Χαρακτηριστικα στοιχεία του σκοτεινού διαδικτύου, είναι τα διάφορα fora ή σκοτεινα δίκτυα το οποία είναι κρυμμένα βαθιά στο διαδίκτυο. Τα δίκτυα F2F είναι, δύο χαρακτηριστικοί τύποι των σκοτεινών δικτύων και χρησιμοποιούνται για ανταλλαγές αρχείων με σύνδεση peer-to-peer.
Συχνά, ο περισσότερος κόσμος συνδέει το **Deep Web** με το **Dark Web** πράγμα που είναι λάθος καθώς το **Dark Web** ειναι ενα μίκρο υποσύνολο του **Deep Web.**

Διαφορες Deep Web με Dark Web:

1. Το **deep web** περιέχει δεδομένα που δεν είναι ορατά από τις μηχανές αναζήτησης όπως τα email μας,και οι ρυθμίσεις των social media,ενώ το **dark web** περιέχει σελιδες με πολύ παρανομο και επικινδυνο περιεχόμενο.
2. Τα δεδομένα του **deep web** εξακολουθούν να είναι προσβάσιμα σε εμας αν χρησιμοποιήσουμε ενα pin ή ακόμα και τα εισερχόμενα του gmail μας ενω του **dark web** είναι πολύ καλά κρυμμένα.
3. Τέλος, η πρόσβαση στο **deep web** δεν είναι επικίνδυνη ενώ, η πρόσβαση στο **dark** ίσως προκαλέσει πολλούς κινδύνους.

Μύθοι για το Dark Web

Αρκετοί χρήστες, λόγω ελλιπούς ενημέρωσης, συνδέουν τους όρους Deep Web και Dark Web θεωρώντας πως αναφέρονται στο ίδιο πράγμα. Στην πραγματικότητα, το Dark Web ή Darknet είναι ένα πολύ μικρό υποσύνολο του Deep Web.

Ένας άλλος μύθος είναι πως το Dark Web χρησιμοποιείτε μόνο για παράνομη δραστηριότητα και ότι περιέχει επικίνδυνο περιεχόμενο.

Το Dark Web είναι οποιοδήποτε δίκτυο στον παγκόσμιο ιστό, στο οποίο μπορούμε να έχουμε πρόσβαση με ειδικό λογαριασμό. Ακριβώς αυτό το επίπεδο ανωνυμίας είναι ο λόγος που αρκετοί καταφεύγουν στη χρήση του για να αποφύγουν την λογοκρισία.

Κάποιοι άλλοι όμως εκμεταλλευόμενοι αυτη την “προστασία”, χρησιμοποιούν το Dark Web για κάθε είδους παράνομη δραστηριότητα.

Το Dark Web δεν είναι απαραίτητα ένας σκοτεινος κόσμος γεμάτος κινδύνους. Σε αυτό μπορούμε να βρούμε πολλές ασφαλείς σελίδες και μάλιστα με αυθεντικό περιεχόμενο.

Κεφάλαιο 2ο: Κακόβουλες δραστηριότητες στο Dark Web

Η Τρομοκρατία στο Dark Web

Η πληροφορική της τρομοκρατίας ορίζεται ως η εφαρμογή προηγμένων μεθοδολογιών και τεχνικές σύντηξης και ανάλυσης πληροφοριών για την απόκτηση ,ολοκλήρωση ,ενσωμάτωση , επεξεργασία,ανάλυση και την διαχείριση της ποικιλομορφίας των πληροφοριών που σχετίζονται με την ασφάλεια .αυτές οι τεχνικές προέρχονται από κλάδους όπως η πληροφορική,οι στατιστικές,τα μαθηματικά ,τη γλωσσολογία,τις κοινωνικές επιστήμες και την δημόσια τάξη .Επειδή η μελέτη της τρομοκρατίας περιλαμβάνει άφθονες ποσότητες πληροφοριών από πολλές πηγές ,τύπους δεδομένων και γλώσσες ,τεχνικές σύντηξης και ανάλυσης πληροφοριών,όπως η εξόρυξη δεδομένων και η επεξεργασία βίντεο και φωτογραφιών παίζουν βασικούς ρόλους στην μελλοντική πρόληψη, ανίχνευση και αποκατάσταση την τρομοκρατιας μέσω διαδικτύου. Η βιβλιογραφία σ αυτή την αναδυόμενη περιοχή είναι κατακερματισμένη και εστιασμένη σε συγκεκριμένους τομείς.

Οι τρομοκράτες δημιουργούν ιστοσελίδες στο ίντερνετ και μεταφέρουν τις γνώσεις τους σε άλλους τρομοκράτες. Επίσης εκμεταλλεύονται τις δυνατότητες των online πλατφόρμων όπως το facebook , το youtube, το instagram κ.α. για να επικοινωνούν. Επιπλέον στο surface web υπάρχουν εκατοντάδες σελίδες που παρέχουν εγχειρίδια για το πως να φτιάξει κάποιος εκρηκτικά όπλα.
Κάποια στιγμή ένας τζιχαντιστής ανέβασε στον επιφανειακό ιστό υλικό που μπορούν να χρησιμοποιούν οι τρομοκράτες. Αργότερα και άλλοι τζιχαντιστές ανέβαζαν επιπλέον υλικό στο surface web και δημιούργησαν την 'wikipedia of terror' η οποία ήταν προσβάσιμη από όλους ,ακόμα και από την αστυνομία και έτσι μπορουσαν να τους πιάσουν. Έτσι μετέφεραν την ιστοσελίδα στο Dark Web όπου τα πάντα είναι ανώνυμα.

Ο προγραμματιστής λογισμικού Satoshi Nakamoto εισήγαγε το Bitcoin το 2008. Τώρα οι τρομοκράτες μέσω του Dark web συγκεντρώνουν χρήματα για την δικιά τους πορεία δέχοντας δωρεές bitcoin και με την σειρά τους τα χρησιμοποιούν για αγορές όπλων από το dark web μαύρες αγορές. Ένα έγγραφο PDF δημοσιεύθηκε ηλεκτρονικά με ψευδώνυμο wa sadaqat aljahad που σημαίνει Bitcoin και η φιλανθρωπία του βίαιου φυσικού αγωνα στην πραγματικότητα είναι ένας οδηγός για την χρήση του Dark web για μυστικές μεταφορές χρημάτων.

Υπάρχουν στοιχεία ότι οι τρομοκράτες χρησιμοποιούν τα κανάλια του dark web για να βρουν χρήματα. Το γραφείο τεχνικής υποστήριξης (CTTSO) εντοπίζει και αναπτύσσει αντιτρομοκρατικές ικανότητες. Ένα σημείωμα CTTSO στις 2 Ιανουαρίου 2014 προειδοποίησαν ότι η εισαγωγή του εικονικού νομίσματος θα διαμορφώσει τη χρηματοδότηση. Το Ιανουαρίου 2015 ανακλήθηκε το S2T είναι μια εταιρία που βασίζεται στη Σιγκαπούρη, ανακάλυψαν στοιχεία ότι οι τρομοκρατική ομάδα σχετίζεται με το Ισλαμικό κράτος και λειτουργεί στο Ισραήλ Αμερική και προσελκύει bitcoin ως μέρος των προσπαθειών συγκεντρώσεις χρημάτων.
Οι τρομοκράτες χρησιμοποιούν ηλεκτρονικές πλατφόρμες για να επικοινωνούν μεταξύ τους, με τους οπαδούς τους, με τα μέσα μαζικής ενημέρωσης (ΜΜΕ) και το ευρύ κοινό. Ωστόσο, οι επικοινωνίες τους μπορεί να οδηγήσουν σε αναγνώριση και σύλληψη. Έτσι βρίσκουν το **Dark Web** και άλλα σκοτεινά κανάλια (dark channels) ως ασφαλέστερες λύσεις. Πρόσφατα, οι ISIS και άλλες ομάδες τζιχάντ έχουν χρησιμοποιήσει νέες εφαρμογές στο διαδίκτυο που επιτρέπουν χρήστες να μεταδίδουν τα μηνύματα τους σε απεριόριστο αριθμό μελών μέσω κρυπτογραφημένων τηλεφωνικών εφαρμογών όπως το τηλεγράφημα. Το τηλεγράφημα είναι τόσο σίγουρο για την ασφάλειά του που προσέφερε δύο φορές $300.000 ανταμοιβή για το πρώτο άτομο που θα μπορούσε να "σπάσει" την κρυπτογράφηση του.

Καταπολέμηση της τρομοκρατίας στο Dark Web

Οι τρομοκράτες χρησιμοποιούν ηλεκτρονικές πλατφόρμες για να επικοινωνούν μεταξύ τους αλλά και με τους οπαδούς τους ωστόσο πολλές φορές αυτές οι επικοινωνίες τους οδηγούν στην σύλληψη.Έτσι βλέπουν το Dark web και άλλα σκοτεινά κανάλια ως τα ασφαλέστερα σημεία για να πουλήσουν κάτι.Οι τζιχαντιστές έχουν χρησιμοποιήσει νέες εφαρμογές όπου επιτρέπουν στους χρήστες να ανταλλάσουν μηνύματα μέσω κάποιων κρυπτογραφημένων εφαρμογών για κινητά οπως το TELEGRAM κλπ.Στην συνέχεια οι Ρώσοι αδερφοί Durov συνέχισαν να δημιουργούν το TELEGRAM το 2013.Αυτή η εφαρμογή είναι τόσο σίγουρη για την ασφάλειά της που προσφέρει 300.000£ για αυτόν που θα μπορέσει να σπάσει την εφαρμογή.Το TELEGRAM έχει έδρα το Βερολίνο και κυκλοφόρησε για πρώτη φορά το 2013 σε iPhone και δύο μήνες αργότερα σε Android.Οι ισλαμιστές προσελκύστηκαν απο την υπερηφάνεια του Telegram για την παροχή μιας "μυστικής συνομιλίας" εγκατάσταση η οποία κρυπτογραφεί σε μεγάλο βαθμό τα μηνύματα που ανταλλάσουν οι χρήστες μεταξύ τους με ένα μοναδικό κλειδί για να μπορέσουν να αποφύγουν πιθανές εισβολές απο hackers ή απο κυβερνητικούς οργανισμούς.

Αρχικά, το Internet είναι διαθέσιμο απο το 1990, όμως το Dark Web έκανε την εμφάνισή του τα τελευταία χρόνια. Η μυστικότητα του και η ταυτόχρονη έλλειψη χρήσης βοηθητικής μεθοδολογίας καθιστούν δύσκολη την μελέτη και καταπολέμηση της τρομοκρατίας στο Dark Web.Έτσι λοιπόν, το IBM Internet Security System δημοσίευσε το 2015 άρθρο και παρέθεσε καθαρά στοιχεία τα οποία έδειχναν οτι οι διαδικτυακές επιθέσεις προέρχονται από το Dark Web χρησιμοποιώντας TOR και έδωσε την ώθηση για να τις καταπολεμήσουμε. Στην συνέχεια, το πανεπιστήμιο της Arizona έκανε ένα project για το Dark Web με στόχο την μελέτη και κατανόηση της διεθνούς τρομοκρατίας μέσω Internet.Ωστόσο, τα αυξημένα ποσοστά της τρομοκρατίας στο DW οδήγησαν το DARPA στο να πιστεύει οτι η απάντηση στην τρομοκρατία μπορεί να δωθεί από το MEMEX ,δηλαδή ενα λογισμικό που επιτρέπει την καλύτερη καταλογράφηση των site του DW. Το DARPA ελπίζει οτι το MEMEX θα διαπερνά το DW.Επίσης, το NSA μέσω ενός προγράμματος μπορούσε να μάθει την ταυτότητα των χρηστών του TOR τα οποία είναι όλα υπό την επιτήρηση του. Τέλος, δύο ειδικοί στην διερεύνηση του DW επεσήμαναν τρόπους για την καταπολέμηση της τρομοκρατίας στο Internet :

1. χαρτογράφηση των κρυμμένων συσκευών.
2. παρακολούθηση των δεδομένων του πελάτη για συνδέσεις σε μη φυσιολογικά πεδία.
3. παρακολούθηση κρυμμένων συσκευών από νέα sites.

Οι Michael Chertoff και Tobby Simon προτείνουν τις ακόλουθες προσπάθειες για την παρακολούθηση του Dark Web:

1. Χαρτογράφηση του καταλόγου κρυφών υπηρεσιών
2. Παρακολούθηση δεδομένων πελατών με αναζήτη συνδέσεων σε μη τυποποιημένους τομείς.
3. Παρακολούθηση του κοινωνικού ιστότοπου για ανταλλαγή μηνυμάτων με νέα μηνύματα Dark Web
4. Κρυφή παρακολούθηση υπηρεσίας νέων χώρων για συνεχή ή μεταγενέστερη ανάλυση.
5. Σημασιολογική ανάλυση για την παρακολούθηση των μελλοντικών παράνομων δραστηριοτήτων και των κακόβουλων παραγόντων.
6. Προφίλ αγοράς για τη συλλογή πληροφοριών σχετικά με τους πωλητές, τους χρήστες και τα είδη καλών ανταλλαγών.

Πληρωμένοι δολοφόνοι μέσω Dark Web

Η πληρωμή δολοφόνων στο Dark web ειναι πολύ εύκολη, ευκολότερη και απο την αγοραπωλησία ναρκωτικών και παιδική πορνογραφία. Κάθε άτομο μπορεί να μισθώσει ενα δολοφόνο

απο την ανεση του σπιτιου του με ενα κουμπι. Σε αυτο βοηθα το Deep Web (δηλαδη ενα πλεγμα κρυπτογραφημενων ιστοτοπων γνωστο και ως Tor) το οποιο δινει την δυνατοτητα στους χρήστες να περιηγουνται στο ιντερνετ με πληρη ανωνυμια και κατω απο την μυτη τησ αστυνομίας. Μερικοι hitmen(δολοφονοι) δινουν την ευκαιρια στους πελατες τους να ποντα-ρουν για το ποια χρονικη περιοδο θα πεθανει το θυμα βαζοντας τα λεφτα μεσα σε μια πισίνα. Πληρωνοντας ενα δολοφονο εχεις την δυνατοτητα να σκοτώσεις απο την πρωην συζυγο σου, ενα δικηγορο, εναν ανθρωπο της γειτονιας μεχρι και εναν μικρο πολιτικο.

Οπως και στο Silk Road ετσι και εδω οι συναλλαγες γινονται με bitcoin.Ο πιο δημοφιλης ιστοτοπος ειναι το MailOnline οπου εκει μπορει να δολοφονουν για την αμερικη με $10.000 και για την Ευρωπη με $12.000. Μερικοι δολοφονοι που μιλησαν αναφερουν πως δεν ξερουν τιποτα για τους πελατες τους και πως απλως δινουν τον καλυτερο εαυτο τους για να ολο-κληρωσουν την αποστολη που τους ανατεθηκε.Αλλοι αναφερουν πως αν πληρωθουν καλα μπορουν να κανουν τα ΠΑΝΤΑ και πως τισ περισσοτερεσ φορεσ η δολοφονια ειναι λανθα-σμενη κατι , ομως , που δεν τους ενδιαφέρει.Τελος επισημαίνουν πως οι δολοφονιες που κανουν ειναι για καλο σκοπο και οι μονο κακοι σκοποι που υπαρχουν στον κοσμο ειναι οι εκτρωσεις παίδων και η ενοχλητικη μουσικη του Justin Bieber.

Υπαρχει ενας ιστοτοπος που δίνει τη δυνατότητα στους πελάτες να πληρωνουν υψηλά ποσά για να παρακολουθήσουν κατακτημένους τρομοκράτες ISIS που βασανίζονται και στη συνέχεια δολοφονούνται. Ακομα εχουν γινει αναφορες για χωρους στους οποιους πωλούν ανθρώπινα όργανα και ο αγοραστής μπορεί να κανει συλλογη με αυτα τα οποια προερχονται απο αναπτυσσομενες χωρες (τριτοκοσμικες). Τελος υπαρχουν ορισμενοι ιστοτοποι που προσφέρουν πρόσβαση σε αγώνες Gladiator πραγματικης βίας μέχρι το θάνατο, ακομα και ζωντανή ροή βασανιστηρίων.

Κυβερνοεπιθέσεις στο Dark Web

Είναι γνωστό ότι ανάμεσα στους όρους «Cybercrime» και «Hacking» υπάρχουν κάποιες ουσιώδεις διαφορές.
Αρχικά ο όρος «Hacker» χρησιμοποιείται για να οριστεί ένα πρόσωπο το οποίο έχει προσπαθήσει να κλέψει και να καταστρέψει κάποια δεδομένα τα οποία δεν του ανήκουν . Αυτό το καταφέρνει αφού εισχωρεί σε διαφορετικά συστήματα των ηλεκτρονικών υπολογιστών . Η Αστυνομία θεωρεί ότι όλα τα εγκλήματα που γίνονται μέσω υπολογιστή. Ο ορος “hacker” αρχικα ειχε θετική σημασία γιατί είναι ο άνθρωπος που προγραμματίζει με ευκολία τους ηλεκτρονικούς υπολογιστές,ωστοσο αργοτερα αποκτησε αρνητικη σημασια καθως σημαινει οτι ειναι καποιος εγκληματιας του κυβερνοχωρου. Για το Cybercrime δεν υπάρχει ακριβής ορισμός. Το έγκλημα αυτό μπορεί να περιλαμβάνει την χρήση υπολογιστών αλλά μπορεί να είναι και ένα έγκλημα μέσω της τεχνολογίας. Κάποιοι εγκληματίες του ποινικού δικαίου δίνουμε μεγάλη σημασία στο νομικιστικο πλαίσιο όπως ο wall που χρησιμοποίησε τις κατηγορίες του ποινικού νόμου για την δημιουργία κατηγοριών εγκλημάτων στον κυβερνοχώρο.

Πολλές κλοπές αρχείων στρατιωτικών και κυβερνητικών υπολογιστών συχνά καταλήγουν σε κυβερνοεπιθέσεις που οφείλονται στα **Botnets**. Γενικά ενα **Botnet** είναι μια συλλογή πολλών **Bot** ή **Drone** που με την σειρά τους περιέχουν χιλιάδες μολυσμένους υπολογιστές.συχνά αυτοί οι μολυσμένοι υπολογιστές αποτελούνται απο **ιους** φτιαγμενους να φαίνονται ακίνδυνους μέχρι να χρησιμοποιηθούν από τους δημιουργούς τους ή απο τα γνωστά **Network-bound worms** που έχουν κατασκευαστεί εξαρχής να εκμεταλλεύονται υπηρεσίες δικτύου συνήθως σε ταχύτερο χρόνο διάδοσης απο αυτο των ιων.Ετσι οι πλέον τώρα μολυσμένοι υπολογιστές χρησιμοποιούνται συνήθως χωρίς την συναίνεση των κατόχων τους ως μια στρατιά αγνώστων χρηστών (συνήθως κακοποιών) για τις κακόβουλες πράξεις τους.ενώ η ευρεία βάση των bots δίνει στους ιδιοκτήτες των botnet **(botmaster ή bot herder)** ανήκουστη εξουσία και πηγή να αποκτήσουν ταυτότητες αλλά και να διεξάγουν ψηφιακό πόλεμο.

Το Shadowserver Foundation ειναι μια μη κερδοσκοπική ομάδα επαγγελματιών εθελοντών ασφαλείας με αποστολή να συλλέγουν πληροφορίες από την σκοτεινοτερη πλευρα του διαδικτύου. Εντοπίζουν τις απειλές και τις εξετάζουν προσεκτικά, και αν είναι απαραίτητο ζητάνε και την βοήθεια των αρμόδιων αρχών. Επίσης ανιχνεύουν και παρακολουθούν χιλιάδες botnets.

Botnets: Ένα botnet είναι μια στρατιά από υπολογιστές, όλοι τους μολυσμένοι με το ίδιο κακόβουλο λογισμικό, που δίνει στον επικεφαλή την δυνατότητα να διαχειρίζεται από μακρια αυτούς τους υπολογιστές (χωρίς οι ιδιοκτήτες τους να το γνωρίζουν) με σκοπό να τους εντάξει κρυφά για τους σκοπούς του. Το χρησιμοποιει για να τραβήξει στοιχεία όπως αριθμούς πιστωτικών καρτών, διαπιστευτήρια για τραπεζικούς λογαριασμούς ή για να τα χρησιμοποιήσει για να ξεκινήσει επιθέσεις εναντίον web sites, καθώς και για να στείλει και άλλα κακόβουλα προγράμματα σε θύματα ή για να τα χρησιμοποιήσει για να κάνει απάτη με κλικς πάνω σε διαφημίσεις.

Honeypots: Είναι ένας πόρος δικτύου που είναι ευάλωτος και έχει τρωτά σημεία ασφαλείας με σκοπό την προσέλκυση κυβερνοεπιθέσεων. Έτσι το χρησιμοποιουν για την ανίχνευση απειλών κατά της ασφάλειας και την κατανόηση των κινήτρων των επιτιθέμενων για την συλλογή κακόβουλου λογισμικού. Ακόμη χρησιμοποιούν παγίδες ηλεκτρονικου ταχυδρομείου και κάτι σαν ενεργές αράχνες θα λέγαμε, τα οποία είναι συστήματα με τα οποία το Crowle ψάχνει ιστοσελίδες που ασχολούνται με το drive - by - downloads. Έτσι ανακαλυπτονται νέες τεχνολογίες για να αναζητήσουμε κακόβουλα αρχεία που διαβιβαζονται ως "δούρειοι ίπποι' σε δημοφιλείς πλατφόρμες.

Έχοντας τοποθετήσει Honeypots σε δυκτια - κλειδιά σε όλο τον κόσμο και συλλέγοντας κακόβουλα προγράμματα από γνωστούς κακόβουλους ιστότοπους συγκεντρωνουν ολα τα κακόβουλα προγράμματα για επεξεργασία και ανάλυση ενεργών Sandbox (εκτελούν δείγματα κακόβουλου λογισμικού σε ένα εικονικό περιβάλλον Windows έτσι οι κλήσεις που πραγματοποιούνται στο API των Windows καταγράφονται σε λεπτομερή αναφορά) και τα σαρώνουν με μηχανισμούς προστασίας από ιούς όπως AVC, PANDA, MCAFEE ANTI-VA, F-SECURE κτλ

Η ανάλυση sandbox είναι μια τεχνική που επιτρέπει σε έναν χρήστη κακόβουλου λογισμικού να εκτελεί ενεργά έναν αναξιόπιστο κακόβουλο κώδικα σε ένα προσεκτικά ελεγχόμενο περιβάλλον. Όλες οι έξοδοι sandbox αναλύονται για κάθε σχετικό στατιστικό λογισμικό κακόβουλου λογισμικού.Το πρωταρχικό μας ενδιαφέρων είναι αν το δείγμα κακόβουλου λογισμικού παρήγαγε ή όχι οποιαδήποτε κίνηση στο δίκτυο, συμπεριλαμβανομένων των πρωτοκόλλων IRC που χρησιμοποιούνται από την πλειοψηφία των κακόβουλων προγραμμάτων που σχετίζονται με το botnet.

Όλοι οι διακομιστές IRC που έχουν πρόσβαση κατά την ανάλυση του sandbox θεωρούνται κακόβουλοι και επομένως παρακολουθούνται στενά. Συνδέουμε και παρακολουθούμε τα πρόσφατα εγκατεστημένα δίκτυα IRC. Τα αρχεία καταγραφής IRC αναλύονται με ένα σύστημα υπογραφής που ταιριάζει με τα υποδήματα, όπου τα συμβάντα και οι εντολές ταξινομούνται ανά τυπο, οι εξαγομενες πληροφορίες τελικά διαδίδονται σε αναφορές σε διάφορα μέρη ανά τον κόσμο.

Ένα βασικό κίνητρο για τη μελέτη ήταν να αυξήσουμε τη γνώση μας σχετικά με την εγκληματικότητα του botnet και τη γενική κατάσταση της απειλής του botnet.

Κεφάλαιο 3ο: Θετικές ή τουλάχιστον ουδέτερες δραστηριότητες στο Dark Web

Η ελεύθερη δημοσιογραφία στο Dark Web

Πόσο πραγματικά ελεύθερη μπορεί να είναι η δημοσιογραφία στον επιφανειακό ιστό όταν ο ίδιος ο Edward Snowden μας αποκάλυψε πως όλα παρακολουθούνται; Για να μπορέσουν κάποιοι δημοσιογράφοι, ακτιβιστές, μυστικοί πράκτορες, στρατιωτικοί και ερευνητές να εκφραστούν ελεύθερα ,να πουν τις απόψεις τους, χρησιμοποιούν το Dark Web το οποίο τους εξασφαλίζει την ανωνυμία τους. Η ανωνυμία αυτή στο επαναστατικό αυτό νέο μέσο έκφρασης, οδηγεί σε άρθρα πιο αληθή και ειλικρινά (οδηγεί εξίσου και σε ψευδείς ειδήσεις). Σε άρθρα που μπορούν να εκθέσουν και την αντίθετη άποψη, σε άρθρα που μπορεί μεν να προκαλέσουν αλλά θα πρέπει να ακουστούν εξίσου. Στο Dark Web δεν έχει πρόσβαση η κυβέρνηση έτσι ώστε να μην υπάρχει λογοκρισία . Οι δημοσιογράφοι χρησιμοποιούν το σκοτεινό διαδίκτυο για να επικοινωνούν με πηγές ανώνυμα ή για να αποθηκεύουν ευαίσθητα έγγραφα. Επίσης χρησιμοποιώντας το dark web μοιράζονται πληροφορίες και λαμβάνουν ευαίσθητα έγγραφα από ανώνυμους . Για παράδειγμα η New York Times έχει ένα ασφαλές κιβώτιο κλειδιών στο σκοτεινό διαδίκτυο όπου οι άνθρωποι μπορούν να στέλνουν αρχεία ανώνυμα για τις χώρες όπου η χρήση του διαδικτύου είναι περιορισμένη.

Έλλειψη λογοκρισίας στο Dark Web

Επειδή στο σκοτεινό διαδίκτυο υπάρχει ανωνυμία αρκετοί άνθρωποι το χρησιμοποιούν για να αποφύγουν την λογοκρισία .

Με ποιον τρόπο ένα άρθρο μπορεί να είναι διαφορετικό στο Dark Web ;
Ένα άρθρο στο dark web δεν δέχεται λογοκρισία από κανέναν και κανείς δεν μπορεί να το διαγράψει επειδή έχει παράνομο ή προσβλητικό περιεχόμενο

Για ποιο λόγο πιθανόν να μην μπορεί να δημοσιευθεί στο επιφανειακό Web ;
Ο λόγος που το ίδιο άρθρο δεν θα μπορούσε να δημοσιευθεί στον επιφανειακό ιστό είναι διότι όλα αυτά που δημοσιεύονται εκεί δέχονται λογοκρισία.

ΛΟΓΟΚΡΙΣΊΑ είναι ο έλεγχος που ασκείται από κάποια εξουσία στις διάφορες εκφάνσεις του λόγου (κυρίως στα ΜΜΕ) και της τέχνης με απώτερο στόχο την παρεμπόδιση ανταλλαγής πληροφοριών, ιδεών και απόψεων, οι οποίες είναι αντίθετες προς τις αρχές της εξουσίας.

Λογοκρισία στην Κίνα: Στην Κίνα υπάρχουν πάνω από 2 εκατομμύρια εργαζόμενοι στην βιομηχανία ελέγχου πληροφοριών οι οποίοι παρεμποδίζουν την εξάπλωση επιβλαβών υλικών στο διαδίκτυο. Πολλά θέματα απλά δεν εμφανίζονται όταν παγκόσμιο ιστό τα οποία έχουν θέμα τον κομμουνισμό, τις βίαιες ενέργειες του κράτους και την πολιτική ηγεσία της Κίνας κ.α. .Πρόσφατα μπλόκαραν το winnie το αρκουδάκι επειδή είχε ομοιότητες με τον πρόεδρο της δημοκρατίας της Κίνας.Επίσης γεγονότα όπως η σφαγή του 1989 έχουν μετατραπεί σε εικόνες χαμογελαστών τουριστών. Εάν κάποιος πολίτης στην Κίνα πιαστεί να επισκέπτεται ή να ψάχνει για ένα απαγορευμένο θέμα πάρα πολλές φορές, μπορεί να περιμένει μια επίσκεψη από έναν αστυνομικό. Η ποινή για τέτοιες πράξεις δεν είναι σχεδόν ανύπαρκτη. Η πλειοψηφία του κινεζικού λαού υποστηρίζει τον έλεγχο του διαδικτύου από την κυβέρνησή τους.

Διακίνηση λογοκριμένων βιβλίων στο Dark Web

Λογοκριμένα βιβλία είναι τα βιβλία τα οποία έχουν απαγορευτεί σε μια χώρα ή παγκοσμίως και δεν επιτρέπεται να πωληθούν.

Στο ***Dark Web*** υπάρχουν λογοκριμένα βιβλία με διεστραμμένα θέματα ή απλά βιβλια που απαγορεύονται για πολιτικούς λόγους. Τα βιβλία αυτά είναι ακατάλληλα και έχουν απαγορευτεί για πολιτικά θέματα, επειδη χρησιμοποιούν άσχημη γλωσσα, για θρησκευτικούς λόγους, επειδή είναι βίαια, διότι είναι υπέρ όλων των σεξουαλικών προτιμήσεων, είναι πολύ καταθλιπτικά, ή είναι χυδαία.
Επίσης πουθενά δεν μπορούν να δημοσιευθούν τα πάντα. Στης Ηνωμένες Πολιτείες παρα την αντίθεση της Αμερικανικής βιβλιοθήκης τα βιβλία απαγορεύονται στα σχολεία και δημόσιες βιβλιοθήκες.

Έκφραση ελεύθερης άποψης στο Dark Web

Wikis: Το wiki είναι μία διαδικτυακή εφαρμογή, η οποία επιτρέπει στους χρήστες της να προσθέτουν, να τροποποιούν ή να διαγράφουν το περιεχόμενό της σε συνεργασία με τους άλλους.Το wiki είναι ένα είδος συστήματος διαχείρισης περιεχομένου, διαφέρει από ένα ιστολόγιο ή περισσότερα άλλα τέτοια συστήματα καθώς το περιεχόμενο δημιουργείται χωρίς κάποιον ορισμένο ιδιοκτήτη.
Διάσημο wiki είναι το wikileaks.Το WikiLeaks είναι διεθνής μη κερδοσκοπικός οργανισμός ΜΜΕ ο οποίος δημοσιεύει έγγραφα από ανώνυμες πηγές και διαρροές, που υπό άλλες συνθήκες δεν θα έβλεπαν το φως της δημοσιότητας.
Υπάρχει ένα wiki το οποίο αποτελεί τον πυρήνα του DW και είναι το Hidden wiki. Πρόκειται για μία συλλογή από αρκετά wikis στα οποία έχεις πρόσβαση μόνο μέσω της χρήσης TOR. Ο καθένας που κάνει εγγραφή σε ένα wiki μπορεί να εκδίδει ελεύθερα πληροφορίες και απόψεις.Ωστόσο, τίποτα δεν σταματάει τους χάκερς στο να ποστάρουν οτι θέλουν.Όποιος διαφωνεί με τις πληροφορίες ενός wiki μπορεί να τις διορθώσει και να εκθέσει τις δικές του απόψεις ελεύθερα και ανώνυμα. Όταν έχεις πρόσβαση στο Hidden Wiki βρίσκεις πληθώρα από συνδέσμους που έχουν δημιουργήσει οι ίδιοι οι χρήστες και πληροφορίες που έχουν παράνομο περιεχόμενο καθώς δεν υπάρχει λογοκρισία.

Αποκάλυψη μυστικών – διαρροές απόρρητων εγγράφων μέσω Dark Web

whistleblower

- είναι αυτός που εκθέτει κάθε μορφή πληροφορίας που θεωρείται παράνομη, ανήθικη ή δεν είναι σύμφωνη με τους κανονισμούς ενός οργανισμού.

Οι μάρτυρες δημοσίου συμφέροντος ξεσκεπάζουν πληροφορίες είτε εσωτερικά είτε εξωτερικά. Εσωτερικά, μπορούν να κάνουν γνωστές τις καταγγελίες μέσα στον οργανισμό και σε όσους δουλεύουν σε αυτό. Ωστόσο μπορούν να καταγγείλουν και εξωτερικά, δηλαδή να φέρουν στο φως απόρρητες πληροφορίες μέσω ενός τρίτου μέρους, εκτός από τον κατηγορούμενο οργανισμό. Επιπλέον, μπορούν να φτάσουν και να δώσουν στοιχεία στα Μέσα Μαζικής Ενημέρωσης, την κυβέρνηση, τις δυνάμεις επιβολής του νόμου ή σε όσους έχουν σχέση με τον κατηγορούμενο οργανισμό.

το whistleblowing είναι μια μορφή πολιτικής ανυπακοής και σκοπεύει να προστατεύσει το κοινό από τις παραβιάσεις της κυβέρνησης.

Τσέλσι Μάνινγκ
Ο άνθρωπος που έφερε στο φως τα μυστικά του πολέμου στο Αφγανιστάν

Στεφανί Ζιμπώ
Η γυναίκα που αποκάλυψε τις παράνομες πρακτικές της UBS

Αντουάν Ντελτούρ
Ο άνθρωπος που αποκάλυψε τα LuxLeaks

Edward Snowden

Ο Edward Joseph Snowden είναι Αμερικανός επαγγελματίας υπολογιστών, πρώην υπάλληλος της Κεντρικής Υπηρεσίας Πληροφοριών (CIA) και πρώην εργολάβος της κυβέρνησης των Ηνωμένων Πολιτειών ο οποίος αντιγράφει και διαρρέει διαβαθμισμένες πληροφορίες από την Εθνική Υπηρεσία Ασφαλείας (NSA) εξουσιοδότηση.Οι αποκαλύψεις του αποκάλυψαν πολυάριθμα προγράμματα παγκόσμιας παρακολούθησης , πολλά από τα οποία διοικούν οι NSA και η Five Eyes Intelligence Alliance με τη συνεργασία των εταιρειών τηλεπικοινωνιών και των ευρωπαϊκών κυβερνήσεων.

Ο Edward Snowden αποχώρησε από το γυμνάσιο και σπούδασε ηλεκτρονικούς υπολογιστές στο κοινοτικό κολλέγιο Anne Arundel στο Arnold, Maryland .Μεταξύ των καθηκόντων του στο κολέγιο της κοινότητας, ο Snowden πέρασε τέσσερις μήνες από τον Μάιο έως τον Σεπτέμβριο του 2004 σε ειδική εκπαίδευση στα στρατιωτικά αποθέματα, αλλά δεν ολοκλήρωσε την εκπαίδευσή του. Ο Snowden δήλωσε στο *The Guardian* ότι απελευθερώθηκε από το στρατό όταν «έσπασε τα δύο πόδια του σε ένα ατύχημα κατά τη διάρκεια της εκπαίδευσης». Ωστόσο, μια μη ταξινομημένη έκθεση που δημοσιεύθηκε στις 15 Σεπτεμβρίου 2016 από την Επιτροπή Πληροφοριών του Σώματος αρνείται τον ισχυρισμό του, δηλώνοντας: έχουν εγκαταλείψει το στρατό βασική εκπαίδευση λόγω των σπασμένων ποδιών, όταν στην πραγματικότητα εξέπληξε εξαιτίας των ναρθήκων. "

Ο Edward Snowden το 2013 διέρρευσε άκρως απόρρητες πληροφορίες σχετικά με τις δραστηριότητες επιτήρησης των NSA.Κατά τη διάρκεια των ετών εργασίας του στον τομέα των τεχνολογιών πληροφορικής, ο Snowden είχε παρατηρήσει την μεγάλη εμβέλεια της καθημερινής εποπτείας της NSA. Ενώ εργάστηκε για τον Booz Allen, ο Snowden άρχισε να αντιγράφει τα άκρως απόρρητα έγγραφα NSA, δημιουργώντας ένα φάκελο για τις πρακτικές που βρήκε διεισδυτική και ενοχλητική. Τα έγγραφα περιείχαν τεράστιες πληροφορίες σχετικά με τις εγχώριες πρακτικές επιτήρησης της ΕΑΑ.
Αφού είχε συντάξει ένα μεγάλο κατάστημα εγγράφων, Σνόουντεν είπε NSA προϊστάμενό του ότι χρειάζεται άδεια απουσίας για λόγους υγείας, δηλώνοντας ότι είχε διαγνωστεί με επιληψία. Στις 20 Μαΐου 2013, ο Snowden πήρε πτήση στο Χονγκ Κονγκ της Κίνας, όπου παρέμεινε καθώς οργάνωσε μια παράνομη συνάντηση με δημοσιογράφους από τη βρετανική έκδοση *The Guardian* καθώς και τη σκηνοθέτιδα Laura Poitras.Στις 5 Ιουνίου, *ο Guardian* κυκλοφόρησε μυστικά έγγραφα που ελήφθησαν από το Snowden. Στα έγγραφα αυτά, το Ελεγκτικό Συνέδριο Εξωτερικών Πληροφοριών εφάρμοσε μια εντολή που απαιτούσε από την Verizon να παρέχει πληροφορίες στην ΕΑΑ σε "συνεχή, καθημερινή βάση" που απορρίφθηκε από τις τηλεφωνικές δραστηριότητες των αμερικανών πελατών της. Την επόμενη μέρα, το *The Guardian* και το *The Washington Post* κυκλοφόρησαν πληροφορίες σχετικά με το PRISM, ένα πρόγραμμα NSA που

επιτρέπει τη συλλογή πληροφοριών σε πραγματικό χρόνο ηλεκτρονικά. Ακολούθησε πλημμύρα πληροφοριών και ακολούθησε τόσο η εσωτερική όσο και η διεθνής συζήτηση.

"Είμαι πρόθυμος να θυσιάσω [την προηγούμενη ζωή μου] επειδή δεν μπορώ με καλή συνείδηση να επιτρέψω στην αμερικανική κυβέρνηση να καταστρέψει την ιδιωτικότητα, την ελευθερία του Διαδικτύου και τις βασικές ελευθερίες για τους ανθρώπους σε όλο τον κόσμο με αυτήν την τεράστια μηχανή επιτήρησης που κρύβουν κρυφά" Ανέφερε ο Snowden σε συνεντεύξεις που έδωσε από την αίθουσα του ξενοδοχείου του Χονγκ Κονγκ.

Το περιστατικό από τις αποκαλύψεις του συνεχίστηκε να εξελίσσεται τους επόμενους μήνες, συμπεριλαμβανομένης μιας νομικής μάχης για τη συλλογή δεδομένων τηλεφώνου από την NSA. Ο Πρόεδρος Ομπάμα προσπάθησε να πρεμήσει τους φόβους σχετικά με την κατασκοπεία της κυβέρνησης τον Ιανουάριο του 2014, διατάσσοντας τον γενικό εισαγγελέα Eric Holder να αναθεωρήσει τα προγράμματα επιτήρησης της χώρας.

Ο Snowden παρέμεινε κρυμμένος για λίγο περισσότερο από ένα μήνα. Αρχικά είχε προγραμματιστεί να μετακομίσει στον Ισημερινό για άσυλο, αλλά, όταν έκανε ενδιάμεση στάση, κατέρρευσε σε ρωσικό αεροδρόμιο για ένα μήνα, όταν το διαβατήριο του ακυρώθηκε από την αμερικανική κυβέρνηση. Η ρωσική κυβέρνηση αρνήθηκε τα αμερικανικά αιτήματα να εκδώσει το Snowden. Τον Νοέμβριο του 2013, το αίτημα του Snowden προς την κυβέρνηση των ΗΠΑ για επιείκεια απορρίφθηκε.

Διοργάνωση συλλαλητηρίων μέσω Dark Web

Πολλοί άνθρωποι πιστεύουν πως το Dark Web περιέχει μόνο παράνομο υλικό και ανθρώπους ψυχολογικά ασταθείς που το χρησιμοποιούν ομως αυτό είναι λάθος καθώς το μεγαλύτερο μέρος του χρησιμοποιείται από φυσιολογικούς ανθρώπους που φοβούνται να εκφράσουν την άποψή τους ή ανθρώπους που θέλουν να κατακρίνουν κάτι χωρίς το φόβο της εμπλοκής τους ,άλλους για την διοργάνωση διαδηλώσεων ενώ πολλοί το χρησιμοποιούν για άντληση ή διάδοση πληροφοριών οπως οι μάρτυρες σε ενα συμβάν ή οι δημοσιογράφοι ψάχνοντας ένα καλό θέμα για την έρευνά τους.ειδικότερα η οργάνωση συλλαλητηρίων μέσω dark web είναι ένα σύνηθες φαινόμενο ιδίως στις κρυφές διαδηλώσεις καθώς είναι απαραίτητο να το μάθει ο κόσμος χωρίς την επέμβαση των πολιτικών ή άλλων παραγόντων που ίσως αποτρέψουν αυτή την ενέργεια.

Συλλαλητήριο Μουμπάρακ στην Αίγυπτο

Η υπηρεσία-σύμβολο τρόμου της εποχής Μουμπάρακ ζητείται να καταστραφεί, για το λόγο του ότι, υπήρξαν αποδείξεις για κατασκοπεία και βασανιστήρια από την αιγυπτιακή υπηρεσία ασφαλείας.

Πρόκειται για τη γνωστή ως «κρατική ασφάλεια», ένα όργανο για το οποίο υπήρξαν φήμες ότι ακολούθησε σε πράξεις κατάχρησης εξουσίας και ότι βοηθησε το καθεστώς Μουμπάρακ.

Ενεργοί πολίτες, ακτιβιστές οπως ονομαζονταν, εισέβαλαν στις εγκαταστάσεις και στα αρχεία της υπηρεσίας και δημοσιευσαν στο Διαδίκτυο βίντεο και έγγραφα, τα οποία περιλαμβάνουν εικόνες από ένα δωμάτιο που παρουσιάζεται ως αίθουσα βασανιστηρίων. Στο πάτωμα της αίθουσας υπάρχουν σημάδια από αίμα και είναι εξοπλισμένο με αλυσίδες και φακέλους. Μάλιστα, πολλοί Αιγύπτιοι, ήδη πίστευαν ότι επί πολλά χρόνια παρακολουθούνταν λεπτομερώς από μυστικούς πράκτορες.

Βίντεο που επίσης αναρτήθηκαν δείχνουν ακτιβιστές να εξετάζουν κάτι που φαίνεται να είναι σαν ένα μεταλλικό πλαίσιο σχεδιασμένο να θέτει τους κρατούμενους σε στάση που να πιέζονται και να έχουν ένα όπλο αναισθητοποίησης, που μοιάζει με κινητό τηλέφωνο.

Στελέχη της υπηρεσίας κατέστρεφαν και έκαιγαν ντοκουμέντα. Αυτές οι πληροφορίες, προκάλεσαν την αντίδραση των μεταρρυθμιστών που πραγματοποίησαν εφόδους, ανησυχώντας ότι καταστρέφονταν αποδείξεις για παραβιάσεις ανθρωπίνων δικαιωμάτων. Από την πλευρά τους, τα στελέχη της υπηρεσίας κατηγόρησαν τους ακτιβιστές ότι έβαλαν φωτιά στα ντοκουμέντα.

Κεφάλαιο 4ο: Τρόποι πρόσβασης στο Dark Web

Το Λογισμικό TOR

Το Tor είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο . Το λογισμικό πελάτη Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση. Η χρήση Tor κάνει δύσκολη την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη συμπεριλαμβανομένου : επισκέψεων σε κάποια ιστοσελίδα , διαδικτυακές αναρτήσεις, προγράμματα άμεσων μηνυμάτων και άλλων μέσων διαδικτυακής επικοινωνίας κι έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητες του. Τέλος, το Tor είναι ελεύθερο λογισμικό πελάτη και η χρήση του είναι δωρεάν.

- Ιστορικά στοιχεία

Μία πρώτη έκδοση του λογισμικού με το δίκτυο δρομολογητών onion να είναι «λειτουργικό και αναπτυσσόμενο» ανακοινώθηκε τον Σεπτέμβρη του 2002. Αρχικά το Tor, το οποίο παρουσιάστηκε από τον Roger Dingledine σε ένα συμπόσιο, χρηματοδοτήθηκε από τις ΗΠΑ, συγκεκριμένα από το ερευνητικό εργαστήριο του ναυτικού. Το Tor υποστηρίχτηκε οικονομικά από το Electronic Frontier Foundation την περίοδο μεταξύ του 2004-2005. Το λογισμικό Tor αναπτύσσεται από το Tor Project , μία μη κυβερνητική οργάνωση που βρίσκεται στις ΗΠΑ από τον Δεκέμβριο του 2006 . Τον Μάρτιο του 2011 το έργο Tor πήρε το βραβείο έργου κοινής ωφέλειας του Free Software Foundation για το 2010 για τον λόγο ότι χρησιμοποιώντας ελεύθερο λογισμικό, το Tor έδωσε την δυνατότητα σε 36 εκατομμύρια ανθρώπους ανά τον κόσμο να απολαύσουν την ελευθερία πρόσβασης και έκφρασης στο διαδίκτυο ενώ τους έδινε τον έλεγχο της ιδιωτικότητας και της ανωνυμίας τους . Το δίκτυο του αποδείχθηκε κρίσιμο σε αντικαθεστωτικά κινήματα στο Ιράν και πρόσφατα στην Αίγυπτο. Επίσης μεγάλο ποσοστό χρηστών προέρχεται από την Κίνα, όπου κυριαρχεί η λογοκρισία στο Διαδίκτυο.

Πώς χρησιμοποιούμε το TOR;

Αρχικά πρέπει να κατεβάσουμε και να εγκαταστήσουμε το πρόγραμμα περιήγησης του TOR το οποίο είναι δωρεάν και μπορείς να το βρείς στην ιστοσελίδα του The Tor Project. Αφού γίνει αυτό, μπορούμε να αλλάξουμε ορισμένες ρυθμίσεις του, π.χ να μην αποθηκεύει το ιστορικό. Χρησιμοποιείται σαν ένα κανονικό πρόγραμμα περιήγησης.

TOR FAQ (frequently asked questions)

1) Τι είναι το exit relay και ποιους κινδύνους διατρέχει ο κάτοχος ενός τέτοιου;

Ένα exit relay είναι το τελευταίο ρελέ που περνάει η κυκλοφορία του Tor προτού να φτάσει στον προορισμό του. Επειδή η κυκλοφορία του Tor περνάει από αυτά τα ρελέ, η διεύθυνση IP του exit relay ερμηνεύεται ως πηγή της κυκλοφορίας. Εάν ένας κακόβουλος χρήστης χρησιμοποιεί το δίκτυο Tor για να κάνει κάτι που μπορεί να είναι απαράδεκτο ή παράνομο παίρνει ο ιδιος την ευθύνη για τις πράξεις του και οχι το Tor. Τα άτομα τα οποία εκτελούν δρομολόγια εξόδου πρέπει να είναι προετοιμασμένα να ασχολούνται με καταγγελίες,ειδοποιήσεις κατάργησης πνευματικών δικαιωμάτων και την δυνατότητα οι διακομιστές τους να προσελκύουν την προσοχή υπηρεσιών επιβολής του νόμου.

2) Μπορούν να μου κάνουν μήνυση αν χρησιμοποιώ το Tor;

Η χρήση του Tor δεν είναι παράνομη αλλά η λήψη υλικού που δεν προστατεύεται από πνευματικά δικαιώματα είναι! Μέχρι στιγμής στις ΗΠΑ κανένας δεν έχει διωχθεί επειδή χρησιμοποιεί Tor. Ωστόσο, κανένας δεν μπορεί να εγγυηθεί ότι δεν θα αντιμετωπίσεις ποτέ νομικά προβλήματα με την χρήση του Tor. Το EFF (διεθνής μη κερδοσκοπική ομάδα ψηφιακών δικαιωμάτων) πιστεύει ότι οι άνθρωποι που χρησιμοποιούν το Tor δεν είναι υπεύθυνοι για την κίνηση που περνάει στο ρελέ εξόδου.

3) Θα πρέπει να χρησιμοποιώ το Tor για παράνομες πράξεις;

Όχι! Το Tor έχει σχεδιαστεί για να εκφράζουν οι άνθρωποι ελεύθερα και ανώνυμα τις απόψεις τους. Δεν είναι ένα εργαλείο για να σπαμε τους νόμους.

4) Μπορώ να καταγγείλω παράνομες πράξεις στους διαχειριστές του TOR;

Οχι! Οι διαχειριστές του TOR δεν είναι οι αρμόδιοι να απαντήσουν σε τεχνικές ερωτήσεις καθώς δεν είναι δικηγόροι ώστε να δίνουν νομικές συμβουλές. Δεν είναι υπεύθυνοι να αποτρεψουν οποία παράνομη δραστηριότητα που συμβεί στο Tor relays. Επίσης, η επικοινωνία με τους διαχειριστές του TOR δεν προστατευεται από κανέναν νόμο οπότε η πολιτεία μπορεί να αποκτήσει όλες τις πληροφορίες που πιθανόν εσύ να τους δώσεις χωρίς να γνωρίζεις!

Μία περιήγηση μέσα στο Dark Web

Μέσω Tor, θα πρέπει να μάθετε πώς να περιηγείστε σε όλο το deep web. Ο ευκολότερος τρόπος να αρχίστε να βρείτε ενδιαφέρουσες τοποθεσίες που μπορούν να έχουν πρόσβαση μόνο μέσω του deep web είναι να ελέγξετε έξω thehiddenwiki.org. Αυτός ο ιστότοπος είναι ένας ανώνυμα διατηρούμενος κατάλογος .onion sites που μπορεί να προβληθεί κατά τη χρήση του προγράμματος περιήγησης Tor.

Διάσημα sites στο Dark Web

Στο Dark Web υπάρχουν πάρα πολλά σάιτ για διάφορα αντικείμενα αυτά είναι μερικά από τα πιο διάσημα σάιτ:

1. Facebook

Το κοινωνικό δίκτυο που φημίζεται για τη συλλογή των δεδομένων των χρηστών του για διαφημιστικούς σκοπούς έχει μια ειδική ιδιωτική έκδοση που μπορεί να προσεγγιστεί μόνο μέσω του Tor.

2. ProPublica

Αυτό είναι ένα σάιτ που έχει σκοπό την ενημέρωση. Εκει καθένας μας μπορεί να διαβάζει διάφορα άρθρα που έχουν σχέση με την πολιτική, τις επιχειρήσεις και για διάφορα άλλα θέματα από ανώνυμους συγγραφείς.

3. DuckDuckGo

Το DuckDuckGo είναι μια πολύ δημοφιλής μηχανή αναζήτησης του Dark Web που δίνει την δυνατότητα στον χρήστη να πλοηγείται σε αυτό με ευκολία και εντελώς ανώνυμα. Το λογότυπο απεικονίζει μια πάπια Που είναι χαρούμενη σημάδι ελευθερίας.

4. Intel Exchange

Ένα από τα πιο διάσημα φόρουμ του Dark Web είναι το Intel Exchange.Σε αυτό το φόρουμ άτομα από κάθε μεριά της γης συζητούν για διάφορα θέματα όπως θεωρίες συνωμοσίας, για εμπόριο λαθραίων εγγράφων και γενικότερα για τα Παγκόσμια γεγονότα. Είναι πολύ ασφαλές αποφεύγει τα Spam και τα Troll επειδή ελέγχει τα μητρώα και επαληθεύει τους λογαριασμού των χρηστών τακτικά.

5. Blockchain

Το Blockchain είναι κάτι σαν εικονικό πορτοφόλι. Εδω οι χρήστες του Dark Web μπορούν να αποθηκεύσουν τα Bitcoin του και να τα χρησιμοποιήσουν για διαδικτυακές αγορές. Αυτό που είναι το περίεργο είναι πως αυτή η ιστοσελίδα διαθέτει επίσημο πιστοποιητικό HTTPS.

6. Hidden Answers

Το Hidden Answers στο Dark Web είναι κάτι αντίστοιχο του Yahoo Answers του Clear Web. Εδώ οι χρήστες του Dark Web μπορούν να ρωτούν για θέματα που αφορούν την περιήγηση σας στο σκοτεινό διαδικτυο π.χ η κλοπή προσωπικών τους δεδομένων, οι απάτες κ.τ.λ

7. MailOnline

Το MailOnline είναι η πιο διάσημη ιστοσελίδα πληρωμένων δολοφόνων. Εκεί άνθρωποι από κάθε μεριά της γης μπορούν να πληρώσουν έναν δολοφόνων με $12.000 για την Ευρώπη και με $10.000 για την Αμερική για να σκοτώσουν εάν άνθρωπο.

8. Silk Road

Το Silk Road ήταν μια διαδικτυακή Μαύρη Αγορά. Η πρόσβαση σε αυτό γινόταν αποκλειστικά μέσω του δικτύου Tor, έτσι ώστε οι χρήστες του να είναι ανώνυμοι και η ταυτότητα τους να παραμένει ασφαλής. Η ιστοσελίδα αυτή πρωτοεμφανίστηκε το 2011. Το Silk Road μερικές φορές συνηθίζονταν να αποκαλείται το Amazonή το eBay των ναρκωτικών.Την 1η Μαΐου του 2013 το Silk Road δέχτηκε επίθεση DDoS, για μικρό χρονικό διάστημα ήταν offline και η πρόσβαση σε αυτό ήταν αδύνατη.

9. SCI-HUB

Το Sci-Hub είναι μια πλατφόρμα που στοχεύει στην απελευθέρωση της επιστημονικής γνώσης στον κοσμο. Ιδρύθηκε από την Alexandra Elbakyan του Καζακστάν το 2011. Φιλοξενεί πάνω από 50 εκατομμύρια ερευνητικά έγγραφα και τα καθιστά διαθέσιμα δωρεάν. Κάτι που είναι βέβαιο ότι θα δώσει ώθηση στην αναζήτηση της ανθρωπότητας για τον τερματισμό των ασθενειών, της ξηρασίας και της πείνας.

10. Secure Drop

Το SecureDrop είναι μια πλατφόρμα λογισμικού ανοιχτού κώδικα για ασφαλή επικοινωνία μεταξύ δημοσιογράφων και πηγών (whistleblowers). [3] Αρχικά σχεδιάστηκε και αναπτύχθηκε από τον Aaron Swartz και τον Kevin Poulsen με το όνομα DeadDrop.

Freenet

Το Freenet είναι μια πλατφόρμα για επικοινωνία ανθεκτική στη λογοκρισία. Χρησιμοποιεί δεδομένα για να διατηρεί και να παραδίδει πληροφορίες και για δημοσίευση και επικοινωνία στον Παγκόσμιο Ιστό χωρίς φόβο λογοκρισίας. Τόσο το Freenet όσο και μερικά από τα εργαλεία του ήταν αρχικά που σχεδιάστηκε από τον Ian Clarke, ο οποίος καθόρισε το στόχο του Freenet να παρέχει ελευθερία λόγου στο Διαδίκτυο με ισχυρή προστασία ανωνυμίας. Το Freenet είναι κάτι που αναπτύσσεται συνεχώς και χρησιμοποιείται σε μεγάλο βαθμό. Οι ιστοσελίδες δεν υπάρχουν από διευθύνσεις αλλά από μοναδικά κλειδιά. Το να δημοσιεύεις στο network είναι η δημιουργία μιας ιστοσελίδας. Το freenet δημιουργεί ένα κλειδί για ιστοσελίδες που βασίζονται στο Digital content . Διάσημες σελίδες μπορεί να δημιουργηθούν όταν αναζητούνται .

Το **Freenet** είναι ένα αυτόνομο δίκτυο, συγκεκριμένα ένα λογισμικό το οποίο έχει να κάνει με ανώνυμες και κρυπτογραφημένες συνδέσεις και έχει συνήθως σκοπό την ανταλλαγή αρχείων (συνήθως σημαντικού περιεχομένου) ανώνυμα, αλλά και την συζήτηση σε φόρουμ χωρίς τον φόβο της λογοκρισίας.

Παρότι έχει αρκετά κοινά με το **Tor**, στο **Freenet** δεν μπορούμε να έχουμε πρόσβαση σε κοινές υπηρεσίες όπως το **Google** ή το **Instagram** καθώς δεν είναι διακομιστής μεσολάβησης αλλά ένας κατανεμημένος χώρος αποθήκευσης.

Οι χρήστες του έχουν λοιπόν την δυνατότητα να αποθηκεύουν αρχεία στο δίσκο άλλου υπολογιστή τα οποία κρυπτογραφούνται και μεταφέρονται μέσω πολλαπλών κόμβων ώστε να είναι πιο δύσκολη η αποκάλυψη των περιεχομένων τους αλλά και η εύρεση του ιδιοκτήτη τους.

Παρόλα τα θετικά που μας προσφέρει το **Freenet**, αποτελεί μερικές φορές κίνδυνο για τους χρήστες του καθώς, ναι μεν υπάρχει η κρυπτογράφηση τον δεδομένων, αλλά ο υπολογιστής είναι συνήθως εκτεθειμένος χωρίς καμία ασφάλεια.

Οι αναφορές για την χρήση του freenet σε αυταρχικά έθνη, είναι δύσκολο να εντοπιστούν εξαιτίας των ίδιων των στόχων του freenet. Μια ομάδα, η Freenet China, εισήγαγε το λογισμικό Freenet σε κινέζους χρήστες, ξεκινώντας από το 2001 και διανέμοντάς την μέσα στην Κίνα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και σε δίσκους μετά τον αποκλεισμό του ιστότοπου της ομάδας από τις κινεζικές αρχές στην ηπειρωτική χώρα. Αναφέρθηκε επίσης, ότι το 2002, η Freenet China είχε αρκετούς αφιερωμένους χρήστες. Τέλος, η κίνηση Freenet είναι αποκλεισμένη στην Κίνα.

TOR vs Freenet vs I2P.

Το Tor (the onion router) είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο διαδίκτυο με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη η τη χρήση της κίνησης από οποιαδήποτε διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κινησης. Η χρήση του κάνει δύσκολη την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη , συμπεριλαμβανομένου επισκέψεων σε κάποια ιστοσελίδα , διαδικτυακές αναρτήσεις , προγράμματα διαδικτυακής επικοινωνίας κι έχει σκοπό να προστατεύσει την ατομική ελευθερία και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητες του.

Μειονεκτήματα και πλεονεκτήματα του TOR :

Αρχικά θεωρείται ότι είναι ταχύτερο και πιο αξιόπιστο μεταξύ των κύριων εναλλακτικών λύσεων (I2P, Freenet). Εχει μεγαλύτερη προσοχή και περισσότερη υποστήριξη. Χαμηλή χρήση μνήμης, έχει εγκριθεί ευρέως και οι επιθέσεις σε αυτόν έχουν πραγματικό παγκόσμιο αντίκτυπο.Κατέχει μεγάλο αριθμό ταλαντούχων προγραμματιστών, μερικοί από τους οποίους χρηματοδοτούνται ακόμη. Στην πραγματικότητα, ο Tor λαμβάνει ένα καλό χρηματικό ποσό για τη συντήρησή του και την ανάπτυξή του. Επίσης το Tor γράφεται στο C(δλδ C είναι μια γλώσσα σύνθετων συστημάτων χαμηλού επιπέδου) . Αυτό σημαίνει ότι ο πελάτης Tor συνήθως τρέχει πιο γρήγορα και με μικρότερο αποτύπωμα. Ο Tor προσπαθεί να επιλύσει ένα πιο δύσκολο πρόβλημα από το I2P ή το Freenet, επειδή αντιμετωπίζει την πρόσβαση στο "δημόσιο" Internet ως κύριο στόχο. Αυτό είναι αναπόφευκτο να δημιουργήσει ενδιαφέροντα ζητήματα και να γράψει έγγραφα σχετικά. Παρόλα αυτά έχει περιορισμένη λειτουργικότητα. Ακόμη και με τη λειτουργία κρυφών υπηρεσιών, ο Tor εξακολουθεί να μην κάνει πολλά παρά μόνο να ενεργεί ως ανώνυμος πληρεξούσιος.

Το δίκτυο είναι πολύ γεμάτο. Η βασική υποδομή του Tor είναι 2.500 έως 3.000 μηχανές δρομολόγησης και έχει περίπου 100.000 έως 200.000 χρήστες καθημερινά.

Το Freenet και το I2P είναι P2P δίκτυα τρίτης γενιάς . Είναι δίκτυα αποκεντρωτικου τύπου και βασίζονται εκτός από την ανωνυμία , στην υψηλή βιωσιμότητα τους στο συνεχή διαμοιρασμό των αρχείων και στην κωδικοποίηση τους έτσι ώστε κανείς να μην μπορέσει ποτέ να αποκτήσει κανένα είδος ελέγχου πάνω σε αυτό .
Είναι γενικά αποδεκτό ότι η χρήση τέτοιων δικτύων ενωνει χρήστες από όλο τον κόσμο λειτουργώντας χωρίς λογοκρισία η απλή δομή, το μηδαμινό κόστος και η αναρχη ροή πληροφοριών είναι τα στοιχεία που καθιστούν τη λειτουργία των δικτύων μοναδική . Οι συμμετέχοντες έχουν τη δυνατότητα να δημιουργήσουν δυναμικά αναπτυσσόμενους χώρους , το περιεχόμενο των οποίων καθορίζεται από τους ίδιους τους χρήστες.

Μειονεκτήματα και πλεονεκτήματα του I2P:
Μέχρι στιγμής, το I2P είναι το πιο ασφαλές, αφού, πρώτα απ 'όλα, πρέπει να χρησιμοποιήσετε εφαρμογές που έχουν αναπτυχθεί για το I2P. Το μόνο ζήτημα είναι ότι δεν μπορείτε να έχετε πρόσβαση στο διαγραμμένο δίκτυο.Ακόμη ενώ είναι πιο ασφαλές από τα άλλα, καθώς χρησιμοποιεί Java(πειραματικό λογισμικό, που εξακολουθεί να αναπτύσσεται ενεργά και θεωρείται βήτα λογισμικό) δεν έχει τόσους χρήστες οσο ο Tor για αυτό και είναι πιο εύκολο να εντοπιστεί η ταυτότητα του χρήστη. Οι νέοι χρήστες πρέπει να περιμένουν να πάρουν πιο γρήγορες ταχύτητες και δεν είναι ακόμα τόσο γρήγοροι όσο μπορεί να είναι ο Tor. Η υποδοχή του χρήστη δεν είναι ακόμα τόσο φιλική όσο του Tor. Το I2P έχει ένα παρόμοιο μοντέλο με το TOR, αλλά κάθε χρήστης λειτουργεί ως ρελέ. Αυτό αυξάνει την ανωνυμία και την ανυπαρξία. Επιπλέον, οι σήραγγες στο I2P είναι όλες μονόδρομες, επομένως χρειάζεστε δύο συνδέσεις για να μεταδώσετε σε και από έναν ιστότοπο. Αυτό σημαίνει ότι ένας εισβολέας (οποιοσδήποτε προσπαθεί να δει τη χρήση του διαδικτύου σας ή να σας βρει χρειάζεται να σπάσει δύο φορές περισσότερους κόμβους για να ανακτήσει τις πληροφορίες σας.

Μειονεκτήματα και πλεονεκτήματα του Freenet:
Όλο το περιεχόμενο στο Freenet διανέμεται και αποθηκεύεται από την κοινότητα γενικότερα. Αυτό το καθιστά εξαιρετικό για την κοινή χρήση αρχείων. Τα δεδομένα δεν εξαφανίζονται όταν ο αρχικός διακομιστής έχει φύγει. Αυτό κάνει το Freenet πολύ διαφορετικό από το Tor ή το I2P. Δεν μπορείτε να εκτελέσετε ένα φόρουμ στο Freenet, επειδή δεν υπάρχει "διακομιστής ιστού" που μπορείτε να δημοσιεύσετε. Στην πραγματικότητα, δεν μπορείτε να χρησιμοποιήσετε όλες τις γλώσσες του διακομιστή όπως n PHP. Το Freenet έχει μόνο στατικό περιεχόμενο όπως HTML και λήψεις αρχείων. Το Freenet είναι ιδανικό για κοινή χρήση αρχείων και έχει κάποιες ομοιότητες με τον Tor και το I2P, αλλά είναι πραγματικά διαφορετικό .Το μεγάλο πλεονέκτημα του FreeNet σε σχέση με τα άλλα συστήματα P2P είναι ότι αυτό που δημοσιεύετε θα είναι διαθέσιμο ακόμα και αν ο κόμβος σας τεθεί εκτός λειτουργίας. Αυτό συμβαίνει χάρη στην κατανεμημένη αποθήκευση δεδομένων. Τα μειονεκτήματα είναι στις βάσεις των χρηστών, που είναι πολύ μικρότερα και δεν θεωρείται ασφαλές και ταχύ όπως τα άλλα.

Συμπέρασμα: Δεν υπάρχει κανένα δίκτυο ανωνυμίας που να κάνει τα πάντα.Οπότε Tor για την περιήγηση στο διαγραμμένο δίκτυο, το I2P για τους κρυφούς προορισμούς, το freenet για τα κατανεμημένα αρχεία.

Κεφάλαιο 5ο: Ασφάλεια στο Dark Web

VPN (Virtual Private Network)

Το VPN είναι ένα εικονικό, ιδιωτικό δίκτυο, στο οποίο μπορούν να συνδεθούν με κρυπτογραφημένη σύνδεση υψηλής ασφάλειας υπολογιστές από ολόκληρο τον κόσμο. Όπου γίνεται ασφαλή και ανώνυμη πλοήγηση και προστατεύονται οι δραστηριότητες μας, οι σελίδες που μπαίνουμε και τα αρχεία που κατεβάζουμε , ακόμα και οι προσωπικές μας πληροφορίες όπως η διεύθυνση IP. Επίσης, το VPN προσφέρει τη δυνατότητα υπερπήδησης εμποδίων στην πρόσβαση συγκεκριμένων ιστοσελίδων. Π.Χ εάν επιθυμεί κάποιος να επισκεφθεί μια ιστοσελίδα η οποία είναι προσβάσιμη μονάδα στο Αμερικάνικο κοινό , συνδέεται στο internet μέσω του VPN, επιλέγει έναν server που βρίσκεται στις Ηνωμένες Πολιτείες έτσι μπορεί να επισκεφτεί αυτήν την σελίδα.

- Πως λειτουργεί και για ποιους σκοπούς ?

Ο λόγος που δημιουργήθηκε είναι ο στρατός . Δημιουργήθηκε για λόγους ασφαλείας και για να μην μπορεί κανείς να υποκλέψει συνομιλίες και δεδομένα . Σήμερα χρησιμοποιείται από πολλούς χρήστες που επιδιώκουν μια επιπλέον ασφάλεια στη σύνδεσή τους . Η κεντρική ιδέα είναι ότι με το VPN η σύνδεση που γίνεται και βγαίνει στο ίντερνετ δεν ακολουθεί μια τυχαία διαδρομή όπως όλες για να φτάσει στον προορισμό της , αλλά ακολουθεί ένα δικό της ξεχωριστό κανάλι . Με αυτόν τον τρόπο δεν μπορεί κανείς να μπει ανάμεσα και να κλέψει ή να ακούσει πληροφορίες που μεταδίδονται. Ακόμα το VPN χρησιμοποιείται για να κατεβάσουμε ανώνυμα αρχεία και για να παρακαμφθεί η τοπική λογοκρισία.

Η δημιουργία μιας από αυτές τις συνδέσεις δεν είναι δύσκολη . Ο χρήστης απλά συνδέεται πρώτα με το δημόσιο διαδίκτυο μέσω ενός ISP και στη συνέχεια ξενικά μια σύνδεση VPN με τον διακομιστή VPN της εταιρίας χρησιμοποιώντας το λογισμικό του πελάτη. Το λογισμικό πελάτη στον διακομιστή δημιουργεί την ασφαλή σύνδεση και παρέχει στον απομακρυσμένο χρήστη πρόσβαση στο εσωτερικό δίκτυο .

Ο συνδυασμός VPN και TOR προσφέρει την απαραίτητη ασφάλεια για την περιήγηση στο Dark Web;

Όχι πάντα.

1. Μπορεί το VPN να διατηρεί αρχεία καταγραφής των δραστηριοτήτων σου
2. Μπορεί το VPN να χάσει την σύνδεση του χωρίς να το γνωρίζεις και τότε το ISP να βλέπει τις δραστηριότητες σου.
3. Μπορεί να ξεχάσεις πως είσαι συνδεδεμένος στο VPN σου και να χρησιμοποιείσεις το λογαριασμό σου στο google το οποίο κρατάει τα δεδομένα που εισάγονται στο σύστημα τους για πάντα.
4. Μπορεί να μην έχετε μια καινούργια ταυτότητα κάθε φορά που συνδέεστε στο TOR .
5. Μπορεί το VPN να μην κρυπτογραφεί τις πληροφορίες σου.

Μόνο και μόνο επειδή είστε καλυμμένοι από ένα VPN, δεν σημαίνει πως δεν μπορείτε να κάνετε λάθη.

Δωρεάν υπηρεσίες VPN

Ορισμένες υπηρεσίες **VPN** ισχυρίζονται ότι είναι δωρεάν άλλα αυτό μπορεί να σημαίνει περιορισμό στα δεδομένα ή αργή σύνδεση, σε σοβαρές περιπτώσεις μπορεί να υπάρχει κακή κρυπτογράφηση, στοχευμένες διαφημίσεις, αλλά και παραβίαση της ιδιωτικότητας.

Hide.me (free VPN)

Πλεονεκτήματα

●Εγγυημένα ασφάλεια με κρυπτογράφηση OpenVPN
●Αξιοπρεπής ταχύτητα σύνδεσης
●2GB όριο στη χρήση δεδομένων κάθε μήνα
●Ιδανικό για προστασία της ιδιωτικότητας σε δημόσια hotspot ή για το ξεκλείδωμα ορισμένων ιστοτόπων

Μειονεκτήματα

●Περιορισμός στη χρήση δεδομένων

Τα πληρωμένα **VPN** έχουν σημαντικά πλεονεκτήματα με ιδιαίτερα χαμηλό κόστος. Έχουμε πρόσβαση σε εκατοντάδες ή και χιλιάδες server τους οποίους μοιραζόμαστε με πολύ λιγότερους χρήστες. Επίσης, έχουμε τη δυνατότητα να συνδεθούμε σε server που βρίσκονται γεωγραφικά πιο κοντά σε εμάς. Αυτοί οι 2 παράγοντες συμβάλλουν στο να έχουμε πιο σταθερό και πιο γρήγορο **VPN**.

NordVPN (best VPN)

Πλεονεκτήματα

●Συνδέεται με υψηλές ταχύτητες
●Προστασία IP
●Παράκαμψη γεωγραφικών περιορισμών και λογοκριμενων ιστοτόπων
●Εγγύηση επιστροφής χρημάτων 30 ημερών
●Καθημερινή 24ωρη εξυπηρέτηση πελατών

Μειονεκτήματα

●Η πληθώρα από OpenVPN αρχεία μπορεί να μπερδέψει κάποιους
●Υπάρχει έλλειψη διακομιστών στην Αφρική (εκτός από την Νότια Αφρική)

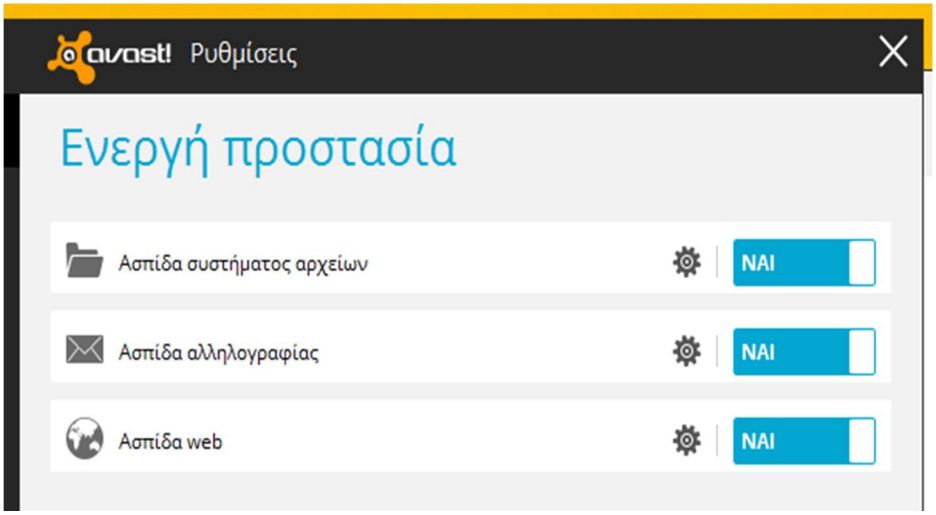
Antivirus

Το Antivirus είναι ένα πρόγραμμα προστασίας ενός υπολογιστή από ένα κακόβουλο λογισμικό.Το πρόγραμμα αυτό ψάχνει τον σκληρό δίσκο και άλλες αποθηκευτικές μονάδες για λογισμικό όπως ιούς και άλλα είδη κακόβουλου λογισμικό τα οποία θα μπορούσαν να βλάψουν τον υπολογιστή. Το Antivirus λοιπόν προσπαθεί να εντοπίζει και να αφαιρεί απο έναν υπολογιστή τον ιό έτσι ώστε να τον χρησιμοποιούμε αρμονικά και χωρίς ιδιαίτερα προβλήματα.

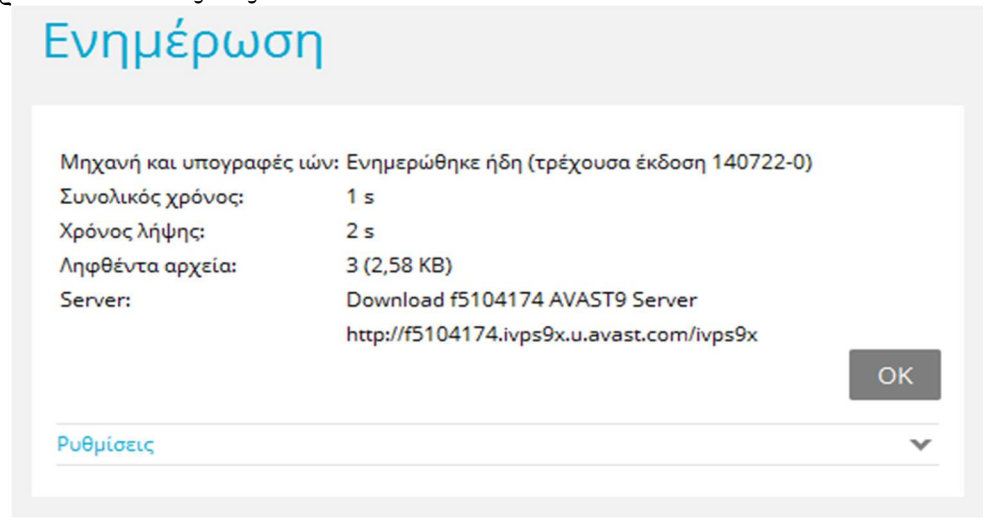
Πώς λειτουργεί το antivirus

- Το antivirus είναι απαραίτητο να ξεκινά αυτόματα μαζί με τα Windows και να παραμένει ενεργό όση ώρα είναι και ο υπολογιστής.

- Κάθε εφαρμογή του είδους έχει μια λειτουργία προστασίας σε πραγματικό χρόνο και ελέγχει οποιοδήποτε αρχείο χρησιμοποιείς. Την λειτουργία αυτή την συναντάμε ως ενεργή προστασία με τα ονόματα real time protection ή με κάποιο παρόμοιο όνομα αναλόγως το antivirus.



Κάθε antivirus διαθέτει μια βάση δεδομένων γεμάτη με χαρακτηριστικά του κώδικα εκατομμυρίων ιών (υπογραφές ιών). Κάθε αρχείο που διαβάζει το πρόγραμμα ουσιαστικά ψάχνει να βρει υπογραφές ιών που το antivirus ήδη γνωρίζει.
Ειναι αναγκαιο το antivirus να είναι συνδεδεμένο στο Internet για να το ενημερώνεις συνεχώς για να μην βρεθεί κάποιος ιός.



Κάθε antivirus διαθέτει έναν έλεγχο όσον αφορά τα heuristics (ελαστικά, υπάρχει κίνδυνος να περάσουν κακόβουλα λογισμικά) των αρχείων. Ουσιαστικά αυτός ο έλεγχος ανιχνεύει υποπτες συμπεριφορές ακόμη και αν δεν ταυτιζεται με τον κωδικό γνωστών κακόβουλων λογισμικών.

Για να ελέγξει ένα antivirus το αρχείο δεν είναι απαραίτητο να το τρέξουμε. Ο έλεγχος από το real time protection γίνεται πάντα όταν ανοίγουμε ένα αρχείο
Υπάρχει ο γρήγορος έλεγχος που ελέγχει αρχεία που ήδη υπάρχουν στην μνήμη και υπάρχει και ο πλήρης έλεγχος που εξετάζει όλα τα αρχεία στον δισκο.

●Δωρεάν Antivirus

+ Το μηδενικό κόστος.
+ Καταναλώνουν λίγους πόρους αφού οι δυνατότητές τους είναι λίγες.
- Συνήθως τα δωρεάν Antivirus προστατεύουν από βασικά malware (κακόβουλο λογισμικό) και ιους.
- Λαμβάνουν updates για νέους ϊούς πιο αργά από τα πληρωτέα.
- Φυσικά δε διαθέτουν Firewall (ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο) και άλλες εξτρά λειτουργίες.

●Επί πληρωμή antivirus

+ Τα AntiVirus επί πληρωμή διατίθενται και σε μορφή «σουϊτας» όπως Internet Security, δηλαδή με εξτρά λειτουργίες όπως Firewall, Ransomware Protection, Προστασία ηλεκτρονικών πληρωμών, AntiSpam κτλ.
+ Το σημαντικότερο είναι το Ransomware protection το οποίο προστατεύει από ϊούς που θέλουν να κρυπτογραφήσουν , δηλαδή να κλειδώσουν τα αρχεία σας ζητώντας «λύτρα» που εαν σας βρεθεί είναι πολυ δυσκολα τα πράγματα...
+ Το Firewall θα σας προστατεύσει από το Ransomware αλλά και πολλών άλλων επιθέσεων.
+ Διαθέτουν πλήρη μενού ρυθμίσεων σε αντίθεση με τα Free
+ Διαθέτουν online υποστήριξη από την εταιρεία και Live chat.
+ Λαμβάνουν updates κάθε λίγες ώρες

AVAST: είναι εντελώς δωρεάν. Το Avast προστατεύει περισσότερα από 220 εκατομμύρια άτομα, επιχειρήσεις και κινητά τηλέφωνα παγκοσμίως.

Kaspersky: Είναι επι πληρωμή.

Τι είναι το firewall.

Το firewall είναι ένα προστατευτικό φράγμα και η δουλειά του είναι παρόμοια με εκείνη ενός φυσικού τείχους προστασίας. Στέκονται μεταξύ του υπολογιστή σας και του υπόλοιπου ψηφιακού κόσμου για να σας κρατήσει προστατευμένους από τις online απειλές. Το Firewall είναι ένα πρόγραμμα λογισμικού ή μπορεί να είναι και ένα κομμάτι του Hardware που προστατεύει τον υπολογιστή σας περιορίζοντας αυτούς που μπορούν να σας στείλουν πληροφορίες. Όλες οι ψηφιακές πληροφορίες που εισέρχονται ή εξέρχονται από ένα δίκτυο περνά μέσα από αυτό το τείχος προστασίας, το οποίο είτε επιτρέπει ή θα τις μπλοκάρει με βάση συγκεκριμένα κριτήρια ασφαλείας.

Η λειτουργία του firewall.

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό

δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίζουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

Πώς προστατεύει τον υπολογιστή το firewall.

1. Αποτρέποντας μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση στον υπολογιστή και στο δικτύου σας.
2. Παρακολουθεί την επικοινωνία μεταξύ του υπολογιστή σας με τους άλλους υπολογιστές στο Internet.
3. Δημιουργεί μια ασπίδα προστασίας που επιτρέπει ή εμποδίζει αυτούς που επιχειρούν να έχουν πρόσβαση στις πληροφορίες του υπολογιστή σας.
4. Σας προειδοποιεί εάν γίνουν προσπάθειες από κάποιους να συνδεθούν στον υπολογιστή σας.
5. Σας προειδοποιεί εάν γίνουν προσπάθειες από κάποια εφαρμογή του υπολογιστή σας να συνδεθεί με άλλους υπολογιστές στο Internet.

Virtual Machine

Το Virtual machine είναι ένα πρόγραμμα που λειτουργεί ως εικονικός υπολογιστής και λειτουργεί με το τρέχον λογισμικό σύστημα και παρέχει εικονικό υλικό στα λειτουργικά συστήματα. Στα Windows τρέχει σαν οποιοδήποτε άλλο πρόγραμμα και στον τελικό χρήστη δίνει την ίδια εμπειρία όπως θα είχε με το λειτουργικό σύστημα υποδοχής. Επίσης το λογισμικό δεν μπορεί να διαφύγει ή να παραβιάσει τον ίδιο τον υπολογιστή και αυτό είναι καλό για την δοκιμή άλλων λειτουργικών συστημάτων.

Οι διαφορές ανάμεσα στο sandbox και το virtual machine είναι οι εξής:

- Το sandbox είναι ένα δοχείο τοποθετημένο γύρω από μια εφαρμογή που εκτελείται μέσα στα Windows ενώ το virtual machine είναι μια εφαρμογή που τρέχει κάτω από τα windows.
- Το sandbox είναι αρκετά ελαφρύ και εύκολο να το εγκαταστήσεις ενώ το virtual machine δεν είναι ελαφρύ χρειάζεται να διαθέσεις χώρο στο δίσκο και πρέπει να επιλέξεις το ποσό της μνήμης RAM που θέλεις να διάθεσης για το VM.
- Η εγκατάσταση ενός VM περιλαμβάνει και την εγκατάσταση ενός λειτουργικού συστήματος από την αρχη.

Η ασφάλεια που μπορεί να προσφέρει το sandbox είναι ότι κάθε κακόβουλο λογισμικό που έχει ληφθεί απορρίπτεται όταν εξέρχεται εφαρμογή και οτιδήποτε δημιουργείται από την εφαρμογή sandbox δεν είναι ορατό έξω από το sandbox και δεν αποθηκεύεται όταν η εφαρμογή εξέρχεται.

- Η ασφάλεια που μπορεί να προσφέρει το virtual machine είναι ότι αν διαγραφεί το vm στον εικονικό σκληρό δίσκο τα πάντα διαγράφονται. Περιλαμβάνει επίσης δικό του σύνολο εικονικών προγραμμάτων οδήγησης συσκευών που συμπεριφέρονται σαν να διασυνδέονται με το πραγματικό υλικό. Επισης όσα συμβαίνουν στο VM μένουν εντός

του VM που σημαίνει ότι οποιαδήποτε λήψεις, εγκαταστάσεις, αλλαγές και ενημερώσεις που αποθηκεύεται ή δημιουργείται στο VM είναι προσβάσιμο μόνο μέσω του VM

JavaScript

Η JavaScript είναι μια γλώσσα προγραμματισμού η οποία, ερμηνεύει εντολές για ηλεκτρονικούς υπολογιστές. Στην αρχή, αποτέλεσε μέρος της υλοποίησης των φυλλομετρητών Ιστού (ένα λογισμικό το οποίο επιτρέπει στο χρήστη του να αλληλεπιδρά με εικόνες, μουσική, κείμενα κ.α.), ώστε τα σενάρια από την πλευρά του πελάτη να μπορούν να έχουν μια επικοινωνία με τον χρήστη, να ανταλλάσσουν δεδομένα που δεν είναι σύγχρονα και να αλλάζουν δυναμικά το περιεχόμενο του εγγράφου που εμφανίζεται.

Είναι μια γλώσσα σεναρίων που βασίζεται στα πρωτότυπα, είναι δυναμική, με ασθενείς τύπους και έχει συναρτήσεις πρώτης τάξης. Είναι επηρεασμένη από τη **C**, μια διαδικαστική γλώσσα προγραμματισμού γενικής χρήσης. Η JavaScript αντιγράφει πολλά ονόματα και συμβάσεις ονοματοδοσίας από τη **Java**, αλλά γενικά οι δύο αυτές γλώσσες δε σχετίζονται και έχουν πολύ διαφορετική σημασιολογία.

Όπως είπαμε λοιπόν και πιο πάνω η **Javascript** ως γλώσσα προγραμματισμού χρησιμοποιείται για την σεναριο ποίηση, δημιουργία διαδραστικών αποτελεσμάτων μέσω των περιηγητών του ιστού επομένως η χρήση της στο tor έχει ως αποτέλεσμα την ευκολότερη εύρεση της διεύθυνσης του υπολογιστή αρα και επομένως την έκθεση του χρήστη παρόλο της ανωνυμίας που προσφέρει το tor.παραδείγματος χάρη αν πάμε σε ένα άλλο site παρακάμπτοντας το tor στον ίδιο υπολογιστή οι δύο αυτές σελίδες με την χρήση του **javascript** ίσως είναι ικανές να συγκρίνουν τις σημειώσεις και να διαπιστώσουν ότι πρόκειται για τον ίδιο χρήστη.

Συνοπτικές οδηγίες για διατήρηση της ανωνυμίας στο Dark Web

1. Χρηση του Tor

Είτε αναζητάτε περιεχόμενο ή υπηρεσίες που δεν περιλαμβάνονται στον κανονικά προσβάσιμο ιστό ή απλως προτιμάτε την ιδιωτικότητα και την ανωνυμία που προσφέρει το δικτυο Tor, η χρήση του όσο το δυνατόν συχνότερα διατηρεί την ταυτότητα σας ασφαλη ενώ είναι online και επίσης βοηθά στη διαφοροποίηση της επισκεψιμότητας στο δίκτυο.

2. Κρυπτογράφηση της αποθήκευσης δεδομένων

Είναι σημαντικό να θυμάστε ότι το Tor είναι χρήσιμο μόνο για την ανωνυμοποίηση της αρχικής τοποθεσίας οποιασδήποτε διαδικτυακής κίνησης που στέλνετε. Το Tor δεν κάνει τίποτα για την προστασία των δεδομένων που υπάρχουν ήδη στον υπολογιστή σας και ο μόνος πραγματικός τρόπος για να διασφαλιστεί η ακεραιότητα αυτών των δεδομένων είναι η χρήση ισχυρού προτύπου κρυπτογραφησης. Το LUKS είναι ένα παράδειγμα προγράμματος υψηλής ποιότητας κρυπτογραφησης που μπορεί να διασφαλίσει την ασφάλεια των προσωπικών σας δεδομένων, ακόμη και αν κάποιος θα έχει πρόσβαση στο μηχάνημα.

3. Μην χρησιμοποιείτε το πραγματικό Email σας

Για να είστε πραγματικά ανώνυμοι online , θα πρέπει να δημιουργήσετε μια ξεχωριστή ταυτότητα που μπορείτε να χρησιμοποιήσετε κατά την πρόσβαση στο δίκτυο Tor. Είναι αδύνατο να αποκρύψετε την πραγματική ταυτότητα σας εάν δώσεις προσωπικα αναγνωρίσιμες πληροφορίες, όπως η πραγματική σας διεύθυνση ηλεκτρονικού ταχυδρομείου. Η ιδιωτική περιήγηση

είναι σχετικά απλή, αλλά μόλις βγάλετε οποιαδήποτε είδος αποτυπωματος πίσω στο ηλεκτρονικό ταχυδρομείο π.χ την εγγραφή ονόματος χρήστη, τη συγγραφή της ρύθμισης κ.λπ. σκεφτείτε πως μπορεί να συνδεθεί σε εσάς με οποιοδήποτε τρόπο. Δημιουργώντας μια εναλλακτική διεύθυνση ηλεκτρονικού ταχυδρομείου που δεν συνδέεται με την πραγματική σας ταυτότητα καθόλου για χρήση όταν επισκέπτεστε ιστότοπους μέσω του δικτύου Tor.

4. Όταν χρησιμοποιούμε το Tor πρέπει να αποφεύγουμε να χρησιμοποιούμε το Google.

Το Google συλλέγει πληροφορίες σχετικά με την περιήγηση των χρηστών και τα δεδομένα αναζήτησης που χρησιμοποιεί για την αύξηση των διαφημιστικών εσόδων. Κατά την αναζήτηση πληροφοριών μέσω του Tor, να χρησιμοποιείτε μηχανές αναζήτησης που δεν καταγράφουν τη διεύθυνση IP σας ή αποθηκεύουν cookies στον υπολογιστή σας. Οι μηχανές αναζήτησης που χρησιμοποιούνται στο Tor περιλαμβάνουν StartString και DuckDuckGo.

5. Διαγράψτε τα cookies και τα τοπικά δεδομένα

Υπάρχουν μερικές επιλογές για να σας βοηθήσουν , (διαθέσιμα πρόσθετα) όπως Self-destruction Cookies που διαγραφουν αυτόματα τα cookies από το μηχάνημα. Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το λειτουργικό σύστημα OS like Tails που διαγράφει αυτόματα όλα τα δεδομένα σύνδεσης όταν κλείσει το λειτουργικό σύστημα.

6. Απενεργοποιήστε το JavaScript, Java και Flash.

Το JavaScript, ειδικότερα, είναι μια ισχυρή γλώσσα δέσμης ενεργειών που μπορεί να χρησιμοποιηθεί για την παρακολουθηση σας με τρόπους που δεν μπορούν να προστατευτούν από το δίκτυο Tor. Τα άλλα ουσιαστικά μεταφέρουν τις πληροφορίες μας στον ιστότοπο σαν να είμαστε εμείς.

7. Μείνετε μακριά από το P2P!

Σημαντικό είναι ότι πολλοί χρήστες που κατεβάζουν torrent αποστέλλουν την πραγματική διεύθυνση IP απευθείας στους ιχνηλάτες και άλλους συναδέλφους.

Κεφάλαιο 6ο: Ψηφιακά νομίσματα: Bitcoin και άλλα

Το Bitcoin

Τα bitcoins είναι μια peer- to- peer ηλεκτρονική μορφή χρήματος η οποία βασίζεται πάνω στις αρχές της κρυπτογραφίας για την διασφάλιση του δικτύου και την επαλήθευση των συναλλαγών. Έτσι όλοι οι χρήστες μπορούν να επιβεβαιώσουν μια συναλλαγή π.χ μεταφορά bitcoins από τον έναν χρήστη στον άλλον χωρίς την ανάγκη κάποιου είδους οργανισμού όπως μια τράπεζα.

Κανείς δεν έχει την ιδιοκτησία των bitcoins όπως και κανείς δεν είναι ιδιοκτήτης του email. Το Bitcoin ελέγχεται από όλους τους χρήστες στον κόσμο που χρησιμοποιούν τα bitcoins. Ενώ οι προγραμματιστές μπορούν να βελτιώσουν το λογισμικό , δεν μπορούν να κάνουν καμία απολύτως αλλαγή στο πρωτόκολλο Bitcoin. Για να διατηρηθεί η συμβατότητα , όλοι οι χρήστες πρέπει να χρησιμοποιούν το λογισμικό που υπακούει στους ίδιους κανόνες. Το Bitcoin μπορεί να λειτουργήσει σωστά μόνο με την πλήρη συναίνεση μεταξύ όλων των χρηστών.

Πότε και από ποιους δημιουργήθηκε το bitcoin ?

Το bitcoin είναι η πρώτη εφαρμογή έννοιας που ονομάζεται «κρυπτονόμισμα», η οποία περιγράφηκε για πρώτη φορά το 1998 από τον Wei Dai στην λίστα αλληλογραφίας cypherpunks υποστηριζοντας την ιδέα μιας νέα μορφής χρήματος η οποία κάνει χρήση κρυπτογραφίας για να ελέγξει τη δημιουργία και της συναλλαγές του, παρά μια αρχή. Οι πρώτες προδιαγραφές του Bitcoin και η απόδειξη της έννοιας του δημοσιεύθηκαν το 2009 από τον Satoshi Nakamoto. Ο Satoshi αποσύρθηκε από το έργο αυτό στα τέλη του 2010 χωρίς να αποκαλύψει πολλά για τον εαυτό του. Από τότε, η κοινότητα του Bitcoin μεγάλωσε εκθετικά με πολλούς προγραμματιστες που ασχολούνται με το Bitcoin. Όταν αποσύρθηκε άφησε την ευθύνη της ανάπτυξης του κώδικα σε μία ομάδα εθελοντών . Η ταυτότητα του ανθρώπου ή των ανθρώπων πίσω από τα bitcoin παραμένει άγνωστη.

Ψηφιακό πορτοφόλι Bitcoin

Ένα πορτοφόλι **bitcoin** είναι ένα πρόγραμμα λογισμικού όπου αποθηκεύονται τα **bitcoins**. Όμως δεν αποθηκεύονται οπουδήποτε, υπάρχει ένα ιδιωτικό κλειδί (μυστικός αριθμος) για κάθε διεύθυνση **bitcoin** που αποθηκεύεται στο πορτοφόλι του ατόμου που κατέχει το υπόλοιπο. Το πορτοφόλι **bitcoin** έρχεται σε πολλές μορφές στην επιφάνεια εργασίας, στο κινητό, στον ιστο και στο υλικό (hardware) είναι οι τέσσερις κύριοι τύποι ψηφιακών πορτοφολιων **bitcoin**.

1 Συνδέστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου με το λογαριασμό για σκοπούς δημιουργίας αντιγράφων ασφαλείας

2 Βάλε την διεύθυνση email σε ένα άλλο άτομο και αυτός μπορεί να σου στείλει χρήματα

3 Καταλάβετε ότι το πορτοφολι σας μπορεί να περιέχει πολλές αναφορές bitcoin. Είναι καλή πρακτική η δημιουργία μιας νέας διεύθυνσης λήψης για κάθε ανώνυμια εισερχόμενης συναλλαγής.

Είναι το Bitcoin ανώνυμο;

Το bitcoin λέγεται πώς οι συναλλαγές του γίνονται με πλήρη ανώνυμοτητα αλλά όλα αυτά είναι πέρα για πέρα λάθος. Ολες οι συναλλαγές καταγράφονται σε ένα blockchain το οποίο καταγράφει κάθε συναλλαγη αλλά και την προέλευση της. Οι συναλλαγές του bitcoin έχουν κάποιες διευθύνσεις οι οποίες λειτουργούν ώς ταυτότητες με αποτέλεσμα να μην είναι τελείως ανώνυμο. Το bitcoin δεν είναι τελείως ανώνυμο ωστόσο μπορούμε να αυξήσουμε την ανώνυμότητα του.

Ειναι το bitcoin εικονικό και άυλο;

Το bitcoin είναι ένα κρυπτονομισμα το οποίο είναι εξίσου εικονικό όπως και μια πιστωτική κάρτα. Χρησιμοποιείται για να πληρώσουμε κάτι online όπως συμβαίνει και με κάθε άλλη μορφή χρημάτων. Ωστόσο υπάρχουν και τα Casascius bitcoin τα οποία υπάρχουν σε φυσική μορφή και μπορούμε να τα χρησιμοποιήσουμε. Όμως πιο βολικός τρόπος είναι η πληρωμή μέσω διαδικτύου. Τέλος, παρότι είναι εικονικά και άυλα τα bitcoin οι άνθρωποι που τα χρησιμοποιούν έχουν κανονικά έλεγχο στα κεφάλαια τους και τα bitcoins δεν μπορούν να εξαφανιστουν έτσι απλά.

Πλεονεκτήματα:

- Επιτρέπει χρήσεις που δεν μπορούσαν να καλυφθούν από τα υπάρχοντα συστήματα πληρωμών.
- Τα bitcoins μεταφέρονται απευθείας από ένα άτομο σε ένα άλλο, μέσω του διαδικτύου, χωρίς να χρειάζεται η διαμεσολάβηση μιας τράπεζας ή μιας εταιρείας χρηματοοικονομικών συναλλαγών.
- Δεν χρειάζεται την άδεια κανενός για να κάνεις τις συναλλαγές σου. Θυμήσου πως ο μισός και πλέον πληθυσμός του πλανήτη είναι αποκλεισμένος από το τραπεζικό σύστημα.
- Οι συναλλαγές σε bitcoin είναι τόσο απλές, όσο η αποστολή ενός email.
- Πληρώνεις μηδενικές ή ελάχιστες προμήθειες για τις συναλλαγές σου.
- Επιτρέπει τις συναλλαγές σε κάθε γωνιά του κόσμου.
- Οι συναλλαγές αυτές γίνονται με τα υψηλότερα στάνταρ ασφάλειας.
- Κανείς δεν μπορεί να αμφισβητήσει την νομιμότητα των συναλλαγών σου.
- Καταργεί το μονοπώλιο των τραπεζών.

Μειονεκτήματα:

- Βαθμός αποδοχής - Πολλοί άνθρωποι δεν είναι ακόμα ενήμεροι για το Bitcoin.
- Αστάθεια - Η συνολική αξία των bitcoins σε κυκλοφορία και ο αριθμός των επιχειρήσεων που χρησιμοποιούν το Bitcoin είναι ακόμα πολύ μικρός σε σύγκριση με αυτό που θα μπορούσε να είναι. Συνεπώς, σχετικά μικρά γεγονότα, συναλλαγές, ή επιχειρηματικές δραστηριότητες μπορούν να επηρεάσουν σημαντικά την τιμή. Θεωρητικά, η αστάθεια αυτή θα μειωθεί καθώς οι αγορές Bitcoin και η τεχνολογία ωριμάζουν. Ποτέ στο παρελθόν δεν έχει δει ο κόσμος ένα νεοσύστατο νόμισμα, οπότε είναι πραγματικά δύσκολο (και συναρπαστικό να φανταστούμε το πώς θα εξελιχθεί.
- Συνεχής εξέλιξη - Το λογισμικό του Bitcoin είναι ακόμα σε έκδοση beta με πολλά ημιτελή χαρακτηριστικά σε ενεργή εξέλιξη. Καινούργια εργαλεία, λειτουργίες και υπηρεσίες εξελίσσονται για να κάνουν το Bitcoin πιο ασφαλές και προσβάσιμο στις μάζες. Μερικές από αυτές δεν είναι ακόμα έτοιμες για όλους. Οι περισσότερες επιχειρήσεις Bitcoin είναι

νέες και δεν προσφέρουν ασφάλεια ακόμα. Γενικότερα, το Bitcoin είναι ακόμα σε διαδικασία ωρίμανσης.

Τι είναι η εξόρυξη του Bitcoin;

Εξόρυξη (mining) είναι η διαδικασία δαπάνης υπολογιστικής ισχύος για να επεξεργαστούν οι συναλλαγές, να ασφαλιστεί το δίκτυο και για να παραμείνουν όλοι στο σύστημα συγχρονισμένοι μαζί.Ειναι το κέντρο δεδομένων του Bitcoin και για να λειτουργήσει χρειάζεται τεράστια υπολογιστική δύναμη.Γι'αυτό το λόγο χρειάζεται τη συνεισφορά τυχαίων υπολογιστών από όλον τον πλανήτη.Αυτή η μέθοδος αναφέρεται ως εξόρυξη (mining) αναλογικά όπως η εξόρυξη χρυσού διότι είναι επίσης ένας μηχανισμός που χρησιμοποιείται στην έκδοση νέων bitcoins. Ωστόσο, σε αντίθεση με την εξόρυξη χρυσού, η εξόρυξη Bitcoin παρέχει μια ανταμοιβή σε αντάλλαγμα των χρήσιμων υπηρεσιών που απαιτούνται για να λειτουργήσει ένα ασφαλές δίκτυο πληρωμών.

Πώς δουλεύει η εξόρυξη του Bitcoin;

- Για να κάνει κάποιος Bitcoin Mining χρειάζεται επεξεργαστική ισχύ. Αρχικά το mining γινόταν κάνοντας χρήση του κεντρικού επεξεργαστή (CPU) ενός ηλεκτρονικού υπολογιστή. Σύντομα όμως παρατηρήθηκε ότι ο κεντρικός επεξεργαστής είναι πολύ πιο αργός σε σχέση με έναν επεξεργαστή γραφικών (GPU).
- Αργότερα τα προγράμματα επεκτάθηκαν και τροποποιήθηκαν ώστε να χρησιμοποιούν τους επεξεργαστές γραφικών για τους σύνθετους υπολογισμούς του Bitcoin Mining. όμως οι σημερινές κάρτες γραφικών έχουν υψηλή κατανάλωση ενέργειας κι αντίστοιχα μεγάλη απαγωγή θερμότητας, δημιουργώντας έτσι σοβαρά προβλήματα για την τροφοδότησή τους αλλά και για την ψύξη τους.
- FPGA Mining: Οι συσκευές FPGA για mining, δημιουργήθηκαν για να έχουν μικρό μέγεθος κι εξαιρετικά μικρή κατανάλωση ενέργειας κι άρα αντίστοιχα μικρή απαγωγή θερμότητας. Πρόκειται συσκευές στο μέγεθος μιας πιστωτικής κάρτας με μεγαλύτερο ύψος, που μπορούν να παράγουν εκατομμύρια hashes σε κάθε δευτερόλεπτο, με καταναλώσεις ενέργειας που ξεκινούν από μόλις μερικά Watt.

Είναι ασφαλές το Bitcoin;

Το πρωτοκολλο και η κρυπτογραφια Bitcoin διαθετει ισχυρη ασφαλεια.Ειναι ισως το μεγαλυτερο διαμοιρασμενο πρότζεκτ της πληροφορικης στον κοσμο.Συνηθως αν γινει ενα λαθος ειναι πιθανον να ευθυνεται ο χρηστης.Στο Bitcoin εχουν βρεθει κενα ασφαλειας τα οποια εχουν επιδιορθωθεί.Η ασφαλεια του Bitcoin εξαρταται απο το ποσο γρηγορα βρισκονται τα προβληματα.Οι χρηστες μπορει κατα λαθος να χασουν τα χρηματα τους να κλαπουν ή να διαγραφουν απο κενα ασφαλειας.Γι αυτο υπαρχουν πρακτικες προστασιας και ασφαλειας εναντι σε κλοπη και απωλεια.Τα τελευταια χρονια αναπτυχθηκαν δυνατοτητες οπως κρυπτογράφηση πορτοφολιου που βοηθουν στην αντιμετωπιση των κενων και στην ασφαλεια του χρηστη.Αλλαγες στο Bitcoin γινονται με την ομοφωνη αποφαση των χρηστων.Τελος λεγεται οτι οι κβαντικοι υπολογιστες(υπολογιστες με τη χρηση της κβαντομηχανικης) μπορουν να παραβιάσουν το Bitcoin και να το χακάρουν.

Το Bitcoin είναι ψηφιακό χρήμα που χρησιμοποιείται κατά τις συναλλαγές μέσω διαδικτύου. Πολλοί χρήστες του έχουν διευκολυνθεί με την ύπαρξή του ενώ άλλοι το εκμεταλλεύονται και

μέσα από αυτό επιχειρούν να πραγματοποιήσουν τις παράνομες συναλλαγές τους.Οι λόγοι που προτιμάται για παράνομους σκοπούς είναι:

- Η υπερβολική ασφάλεια που προσφέρει.με το bitcoin κάνεις ανενόχλητος τις συναλλαγές σου χωρίς την χρήση των προσωπικών σου στοιχείων όπως όνομα,τηλέφωνο και τα λοιπά.
- Η ευκολία της χρήσης του.
- Η εκτέλεση πληρωμών χωρίς την εμπλοκή τρίτων.
- Η μη αναστρέψιμες συναλλαγές.από την στιγμή που γίνει η πληρωμή δεν υπάρχει η δυνατότητα ανταλλάγης.

Εναλλακτικά κρυπτονομίσματα

1. LITECOIN

Litecoins (LTC) είναι αναμφισβήτητα το πιο επιτυχημένο alt-coin. Κυκλοφόρησε το 2011 και είχε κεφαλαιοποίηση αγοράς περίπου 5% από εκείνη του bitcoin.

2. DOGECOIN

Dogecoin (DOGE) εισήχθη το 2013. Το dogecoin είναι ένα fork του litecoin. Η κυρία καινοτομία της έγκειται στη στρατηγική μάρκετινγκ της. Έχει συνδεθεί με το διάσημο doge meme.

Κεφάλαιο 7ο: Πραγματικές ιστορίες στο Dark Web

Wikileaks

Το Wikileaks είναι διεθνής μη κερδοσκοπικός οργανισμός ΜΜΕ ο οποίος δημοσιεύει έγγραφα από ανώνυμες πηγές και διαρροές που υπό άλλες συνθήκες δεν θα έβλεπαν το φως της δημοσιότητας. Ξεκίνησε την λειτουργία του το 2006. Μεσα στον πρώτο χρόνο της λειτουργίας του, ο ιστότοπος ανακοίνωσε πως η βάση δεδομένων του συμπεριλάμβανε πλέον περισσότερα από 1,2 εκατομμύρια έγγραφα .

Ο οργανισμός αυτοπεριγράφεται ως "πνευματικό παιδί " των Κινέζων αντιφρουντών ,καθώς και δημοσιογράφων, μαθηματικών και νεοσύστατων εταιριών τεχνολογίας από τις ΗΠΑ , την Ταϊβάν, την Ευρώπη, την Αυστραλία και την Νότια Αφρική. Δημοσιεύματα εφημερίδων και διαφόρων περιοδικών παρουσιάζουν ως ιδρυτή του οργανισμού αυτού τον Τζούλιαν Ασάντζ, έναν Αυστραλό δημοσιογράφο και ακτιβιστή του Διαδικτύου.

Ο Julian Assange είναι ο άνθρωπος που δημιούργησε το wikileaks. Γεννήθηκε το 1971 (47 χρονών) στην Αυστραλία. Το 2010 δημοσίευσε στο wikileaks απόρρητα έγγραφα της Αμερικής με αποτέλεσμα η Αμερική να τον στοχοποιήσει.Την ίδια περίοδο κατηγορήθηκε από τους σουηδούς για βιασμό και σεξουαλική παρενόχληση αλλά αρνήθηκε τις κατηγορίες λεγοντας πως κατηγορείτε μόνο και μόνο επειδή διέρευσε Αμερικανικά έγγραφα.

Ο Julian παραδόθηκε στην αστυνομία, αλλά αφέθηκε ελεύθερος με εγγύηση μετά από δέκα ημέρες. Αφού δεν μπορούσε να αθωωθεί παραβίασε την εγγύηση του και έφυγε από την χώρα.Το 2012 του παρείχε άσυλο ο Ισημερινός (ή αλλιώς Εκουαδόρ) και από τότε μένει στην πρεσβεία του Εκουαδόρ στο Λονδίνο.

Το 2017 η Σουηδία απέσυρε το ένταλμα σύλληψης του. Παρόλο που είναι ελεύθερος να φυγει πλέον από την πρεσβεία είναι πολύ πιθανό να τον συλλάβουν για την παραβίαση της εγγύησης του.

Το 2018 ο Πρόεδρος του Εκουαδόρ αποκάλυψε ότι είχε ξεκινήσει συνομιλίες με τις βρετανικές αρχές για να αποσύρει το άσυλο του Assange.

Anonymous

Οι Anonymous δεν είναι ένας οργανισμός μπορούν όλοι να συμμετέχουν δεν μπορεί κανείς να σε σταματήσει . Υπάρχει η κρυπτογράφηση για μέγιστη προστασία απορρήτου και χρησιμοποιείς ψευδώνυμο.Επίσεις το λογισμικό που χρησιμοποιεί το anonymous για να ξεκινήσει τις επιθέσεις DDoS λέγεται low orbit ion cannon kai σημαίνει ένα κανόνι χαμηλής τροχιάς . Σήμερα περίπου 100.000 άνθρωποι ανα τον κόσμο είναι anonymous και μόνο ένα μικρό ποσοστό από αυτούς είναι χακερ.

Οι **Anonymous** έχουν πολύ έντονη δράση τώρα τελευταία.
Μερικές από τις επιθέσεις τους:
•Επίθεση «DDoS» (Distributed Denial of Service attack) (Διαμεσολάβηση επίθεσης άρνησης παροχής υπηρεσιών)
•Επίθεση τύπου «deface»: Κάποιος αποκτά πρόσβαση στον διακομιστή του σάιτ και αλλάζει τον κώδικα ιστοσελίδας αναπαράγοντας το δικό του μήνυμα. Αυτό είχαν κάνει στην ιστοσελίδα του ελληνικού υπουργείου Δικαιοσύνης (Στις 3 Φεβρουαρίου 2012) και όταν κάποιος πληκτρολογούσε ένα συγκεκριμένο λινκ θα έβλεπε βίντεο των **Anonymous** με το δικό τους μήνυμα «Justice is coming» (έρχεται η δικαιοσύνη). Οι **Anonymous** χρησιμοποιούν **Dark web** γιατί

μπορούν να παραμείνουν ανώνυμοι αν ξέρουν πως να το λειτουργούν σωστά, πράγμα που σημαίνει ότι μπορούν να κάνουν παράνομες συναλλαγές χωρίς να φοβούνται μην τους πιάσουν.

Exit scams

Το exit scams (απάτη εξόδου) είναι ένα τέχνασμα εμπιστοσύνης όταν για παράδειγμα μια καθιερωμένη επιχείρηση η οποία έχει σταματήσει να στέλνει παραγγελίες αλλά ακόμη λαμβάνει πληρωμή για νέες παραγγελίες.Με αυτόν τον τρόπο οι παραγγελίες δεν αποστέλλονται και έτσι περνάει ένα συγκεκριμένο χρονικό διάστημα μέχρι οι πελάτες να καταλάβουν ότι η παραγγελία τους δεν έγινε μέχρι να εξαφανιστεί η επιχείρηση.

Ashley Madison

Είναι μια καναδική υπηρεσία κοινωνικής δικτύωσης που διατίθεται σε ανθρώπους που είναι παντρεμένοι ή σε σχέσεις.

Ιδρύθηκε το 2002 από τον **Darren Morgenstern**, με το σύνθημα: «**Η ζωή είναι σύντομη. Έχετε μια υπόθεση**».

Στις 15 Ιουλίου χάκερ έκλεψε όλα τα δεδομένα των πελατών της, συμπεριλαμβανομένων των μηνυμάτων ηλεκτρονικού ταχυδρομείου, ονόματα, διευθύνσεις κατοικίας, σεξουαλικές φαντασιώσεις και πιστωτική κάρτα πληροφοριών και απείλησε να δημοσιεύσετε τα δεδομένα στο διαδίκτυο, αν Ashley Madison και οι συνάδελφοι του δεν έκλειναν οριστικά την ιστοσελίδα.

Μέχρι τις 22 Ιουλίου, το πρώτο σύνολο ονομάτων πελατών απελευθερώθηκε από τους χάκερς. Περισσότερες πληροφορίες απελευθερώθηκαν στο dark web στις 20 Αυγούστου 2015.

Στις 28 Αυγούστου 2015, ο Noel Biderman συμφώνησε να παραιτηθεί από τη θέση του γενικού διευθυντή της Avid Life Media Inc.Σύμφωνα με δήλωση της εταιρείας, η αποχώρησή του ήταν "προς το συμφέρον της εταιρείας".

Τον Ιούλιο του 2016, η μητρική εταιρεία Avid Life Media μετονομάστηκε σε Ruby Corp και διόρισε τον Rob Segal ως νέο CEO.Τον ίδιο μήνα, η εταιρεία άλλαξε την υπογραφή της από το «Life is Short. Έχετε μια υπόθεση. Να βρείτε τη στιγμή σας».

Silk Road

Το ***Silk Road*** ήταν μια διαδικτυακή Μαύρη Αγορά που βρισκόταν στο Deep Web . Η πρόσβαση σε αυτό γινόταν αποκλειστικά μέσω του δικτύου Tor, έτσι ώστε οι χρήστες του να είναι ανώνυμοι και η ταυτότητα τους να παραμένει ασφαλής. Η ιστοσελίδα αυτή πρωτοεμφανίστηκε το 2011,. Ο Ross Ulbricht ίδρυσε το Silk Road πριν από 3 περίπου χρόνια, ένα online marketplace που χαρακτηρίστηκε ως το "**Amazon για ναρκωτικά**". Όχι άδικα αν σκεφτεί κανείς ότι πάνω από το 50% των συναλλαγών που γίνονταν αφορούσαν μαριχουάνα και κοκαΐνη. Η αξία των συναλλαγών που πραγματοποιήθηκαν στο Silk Road ανέρχεται στο 1.5 δισεκατομμύρια δολάρια σύμφωνα με το FBI ενώ οι προμήθειες που έπαιρνε το site έφτασαν το ποσό των 80 εκατομμυρίων δολαρίων. Και σε όλα τα παραπάνω χρησιμοποιώ παρελθοντικό χρόνο γιατί πριν από μία εβδομάδα ο Ross Ulbricht συνελήφθη στο San Francisco με πληθώρα κατηγοριών να τον βαραίνουν

- Πώς έγινε γνωστό στις αρχές και μετά από ποια διαδικασία συνελήφθη ο διαχειριστής του?

Ψάχνοντας οι αρχές να εντοπίσουν το ψηφιακό αποτύπωμα του διαχειριστή, πέφτουν πάνω σε μία ανάρτηση σε ένα forum. Ήταν ένα thread με τίτλο «Anonymous market online?» (Ανώνυμη αγορά στο διαδίκτυο;). Ο άνθρωπος που είχε αναλάβει το έργο να εντοπίσει το ψηφιακό αποτύπωμα του διαχειριστή του Silk Road, παρακολουθεί το thread.Το Silk Road διέθετε κάποιους υπαλλήλους ενας από αυτούς, αποφάσισε να υπεξαιρέσει bitcoins από χρήστες . Στα forum του Silk Road, έλεγε πως θα ήθελε να τον δείρει κάποιος και να εξαναγκαστεί να επιστρέψει τα bitcoin που είχε κλέψει. Στη συνέχεια όμως, άλλαξε γνώμη: "Να αλλάξω την εντολή για ξυλοδαρμό, σε εντολή για δολοφονία;».

Κάπως έτσι ξεκίνησε μία συζήτηση, αντάλλαξε μηνύματα με κάποιον που του παρουσιάστηκε ως εκτελεστής και έκλεισε συμφωνία μαζί του να σκοτώσει τον υπάλληλο, έναντι 40 χιλιάδων δολαρίων. Ο εκτελεστής έστειλε φωτογραφίες από την «εκτέλεση» και ενώ ο Dread Pirate Roberts εξέφρασε αρχικά μία επιφύλαξη για την αποτελεσματικότητά του, τελικά πείστηκε πως ο υπάλληλος ήταν νεκρός. Κι όμως. Ο υπάλληλος κρατούνταν από την αστυνομία στην οποία είχε ομολογήσει τι είχε κάνει και ο εκτελεστής ήταν πράκτορας των αρχών. Κάπως έτσι λοιπόν, ο Ross William Ulbricht, βρέθηκε στα χέρια των αμερικανικών αρχών, σε μία ιστορία που θυμίζει ευφάνταστο σενάριο.

- Τι μπορούσε κανείς να αγοράσει εκεί?

Μέχρι τον Απρίλιο του 2013, η ιστοσελίδα είχε 10.000 προϊόντα προς πώληση. Το 70% εξ αυτών ήταν ναρκωτικά που είναι παράνομα στις περισσότερες χώρες. Στο Silk Road κάποιος μπορούσε να βρει 340 διαφορετικές ποικιλίες ναρκωτικών, συμπεριλαμβανομένων της ηρωίνης του LSD, και της κάνναβης.

Οι κανόνες χρήσης της ιστοσελίδας ανέφεραν ότι απαγορεύεται η πώληση «οποιουδήποτε προϊόντος που ο σκοπός του είναι να βλάψει ή να εξαπατήσει.» Σε αυτή την κατηγορία προφανώς περιλαμβάνονταν η παιδική πορνογραφία , κλεμμένες πιστωτικές κάρτες, δολοφονίες και όπλα μαζικής καταστροφής

Εναλλακτικά Silk Roads

Μετά το κλείσιμο του silk road υπήρξε και δεύτερη εκδοχή το silk road (2.0)Η δεύτερη έκδοση τελικά απέτυχε μετά από περίπου ένα χρόνο.Ηταν μια μεγάλη απογοήτευση για τους χρήστες των οποίων τα χρήματα που χάθηκαν από την κατάσχεση. Θεωρείται ως συνέχεια της δεύτερης η τρίτη έκδοση (Silk Road 3.0) θεωρήθηκε απάτη γιατι αναδείχθηκε ως αντίγραφο του αρχικού δρόμου αλλά με πολύ καλύτερη ασφάλεια και μια νέα ομάδα, τα παιδιά που βρίσκονται πίσω από την Crypto Market.

Με το Silk Road 3.0 ως θεμέλιο, δημιουργήθηκε μια νέα αγορά σκοτεινού δικτύου. Ξεκίνησε ως Road Silk 3.1.Αν και έχει τους ίδιους διαχειριστές και σχεδιαστές όπως το Silk Road 3.0 οι προηγούμενες πληροφορίες για το όνομα χρήστη και τον κωδικό πρόσβασης δεν λειτουργούσαν στη νέα τοποθεσία. Πολλοί από τους παλιούς χρήστες το είδαν ως πιθανή απάτη εξόδου. Μετά την εγγραφή, εμφανίζεται μια φόρμα που οι χρήστες πρέπει να συμπληρώσουν ορισμένες πληροφορίες για να επιστρέψουν χρήματα από την προηγούμενη αγορά. Αυτό δείχνει σημάδι αξιοπιστίας και δέσμευσης για τους χρήστες . Οι περισσότεροι από τους διαχειριστές σε αυτή την περίπτωση θα εξαφανιστούν με Bitcoins των χρηστών. Η πρόσβαση δεν παρέχεται αν δεν εγγραφείτε.

Panama Papers

Πρόκειται για 11 εκατομμύρια έγγραφα, τα οικονομικά και νομικά «Αρχεία του Παναμά», που έχουν να κάνουν με εκατοντάδες υποθέσεις φοροδιαφυγής στον κόσμο, τα οποία είχε στην κατοχή της η δικηγορική εταιρεία Mossack Fonseca, που εδρεύει στον Παναμά. Έχουν προκαλέσει από τον Απρίλιο του 2016 με δημιουργό τους την ICIJ, μεγάλη αναστάτωση σε ηγέτες κρατών και σε εκατομμυριούχους ολόκληρου του πλανήτη, με την τεράστια διαρροή τους. Τα συγκεκριμένα δίκτυα, υποτίθεται ότι αποκαλύπτουν ένα μυστικό δίκτυο, στο οποίο περιλαμβάνονται οι συνεργάτες του Βλαντιμίρ Πούτιν και άλλοι άνδρες στους οποίους οι ΗΠΑ έχουν απαγγείλει κατηγορίες για διαφθορά.Τα έγγραφα δεν έχουν αποδείξει ακόμα απαραίτητα παράνομη δραστηριότητα. Εμπλέκονται σε αυτά άνθρωποι και εταιρίες τις οποίες οι ΗΠΑ έχουν βάλει σε μαύρη λίστα, εξαιτίας εμπορίου ναρκωτικών και συνδέσεων με τρομοκρατίες. Αυτά τα έγγραφα, τα απέκτησε η ICIJ, από μία ανώνυμη πηγή, η οποία τα έδωσε στην γερμανική εφημερίδα Suddeutsche Zeitung.Εξαιτίας όμως της διαρροής των πληροφοριών αυτών σε όλο τον κόσμο υπήρξε μια φοβερή αναστάτωση.Πολλοι άνθρωποι πίστευαν πως τα έγγραφα αυτα είναι αληθινά και ισχύουν πράγματι ενώ άλλοι (ιδίως οι εμπλεκόμενοι σε αυτό το θέμα)υποστήριζαν πως όλα αυτά τα αρχεία βασίζονται σε ένα ψέμα.Πολλές ήταν οι διαμαρτυρίες που έγιναν παγκοσμίως αλλά και οι θεωρίες ύπαρξης συνομωσίας.παρόλα αυτά κάποιες χώρες εξέφρασαν δυσανασχέτηση για το όλο θέμα ενω χώρες όπως η Αγγλία,η Γαλλία κτλ αρχισαν να πραγματοποιούν έρευνες για το όλο θέμα και σε παγκόσμιο επίπεδο άρχισαν οι φόροι να ελεγχονται πιο έντονα.

AlphaBay

Το AlphaBay κυκλοφόρησε επίσημα στις 22 Δεκεμβρίου του 2014 αυξάνοντας πολύ γρήγορα τις τασεις της δημοτικότητας του DarkWeb για την αξιοπιστία του και τα αξιόπιστα πρότυπα λειτουργία του. (14000 νέους χρήστες τις πρώτες 90 ημέρες) Κατά την στιγμή της κατάργησης του είχε πάνω από 400.000 χρήστες.

ΙΔΙΟΚΤΗΤΕΣ : alpha02 και DeSnake
ΔΗΜΙΟΥΡΓΌΣ :Αλεξάντερ Κειζ, γνωστός και ως DeSnake (αυτοκτόνησε στις φυλακές).
ΕΣΟΔΑ : Πανω απο 23 εκατομμύρια δολάρια

Ο ιστότοπος ανέβηκε αφού οι διαχειριστές άλλων αγορών Dark Web διεξήγαγαν περίπλοκες απάτες τα τελευταία χρόνια, ξεφεύγοντας από κλοπές εκατομμυρίων δολαρίων σε Bitcoin.

Το Μάιο του 2015, ο ιστότοπος ανακοίνωσε ένα σύστημα ψηφιακών συμβολαιων και μεσεγγυησης που επετρεπε στους χρήστες να δεσμεύονται και να συμφωνούν να παρέχουν υπηρεσίες στο μέλλον. Οι διαδικτυακές κοινότητες απαιτούσαν δικαιοσύνη για πωλητές των οποίων τα μετρητά είχαν αποθηκευτεί σε λογαριασμούς μεσεγγυησης εν αναμονή της παραγγελίας τους.

Μετα το κλείσιμο του η αντιδραση των χρηστών ήταν άμεση καθώς πίστευαν πως μια απάτη εξοδου 12 εκατομμυρίων με Bitcoin στην πλατφόρμα Evolution από τους διαχειριστές της είχε γίνει με χρήματα χρηστών.

Κεφάλαιο 8ο: Ηθικά ζητήματα για το Dark Web

Παρακάτω καταγράφονται οι απόψεις των μαθητών σχετικά με το αν είναι σωστό να μπαίνουμε στο σκοτεινό Διαδίκτυο ή όχι.

Ομάδα 1

Πιστεύω ότι δεν είναι σωστή η ελεύθερη πρόσβαση στο σκοτεινό διαδίκτυο γιατί ο καθένας μπορεί να το χρησιμοποιήσει για κάποια παράνομη διαδικασία που έχει στο μυαλό του να πραγματοποιήσει χωρίς να εκτεθεί η ταυτότητα του. Μπορεί να το χρησιμοποιήσει για κάποια απλή διαδικασία (κατά κάποιο τρόπο) αλλά και να κάνει κάτι κακό προς το πρόσωπο κάποιου .Άρα πιστεύω ότι δεν πρέπει να το χρησιμοποιεί ελεύθερα οποίος θέλει .
Επιπρόσθετα , από άποψη ηθική , δεν θα έπρεπε να έχει πρόσβαση ο οποιοσδήποτε διότι «πάνε κόντρα» στην κυβέρνηση και στους νόμους. Επιπλέον ο καθένας θα μπορούσε να σχεδιάσει και να οργανώσει τρομοκρατικές επιθέσεις και προπαγάνδες είς βάρος άλλων λαών.

Ομάδα 2

Δεν θεωρώ σωστή την ελεύθερη πρόσβαση στο σκοτεινό διαδίκτυο.
Αρχικά ποτέ δεν μπορείς να είσαι τελείως ασφαλείς και ειδικά για τις ηλικίες κάτω των 18 μπορεί να αποδειχθεί πολύ επικίνδυνο. Επίσης γίνονται πολλές παράνομες ενέργειες όπως πώληση ναρκωτικών, όπλων ή ανθρώπινων μελών. Ακόμα υπάρχει "ενοχλητικό" και ανδιαστικό περιεχόμενο που θα χαραχτεί στο μυαλό σου για πάντα. Παρόλα αυτά εάν το χρησιμοποιείς προσεκτικά και δεν μπαίνεις σε ύποπτες ιστοσελίδες θα είναι χρήσιμο για να βρεις πληροφορίες ή κάτι άλλο.

Ομάδα 3

Η πρόσβαση στο dark web δεν είναι εύκολη. Ωστόσο υπάρχουν άνθρωποι που το χρησιμοποιούν καθημερινά είτε για καλούς σκοπούς είτε για κακούς σκοπούς. Αυτό προσωπικα δεν το θεωρώ σωστό ηθικά διότι όχι μόνο είναι παράνομο αλλά είναι και επικίνδυνο. Άμα σε πιάσουν επειδη δεν είχες καλή κάλυψη θα πας φυλακή. Στο dark web συνήθως μπαίνουν άνθρωποι για να αγοράσουν ναρκωτικά, όπλα, πληροφορίες για ανθρώπους με μεγάλη αξία, ανθρώπους για να σκοτώσουν άλλους ανθρώπους, και πολλά άλλα παράνομα πράγματα.
Το dark web είναι η πιο επικίνδυνη γωνιά στο ίντερνετ. Δεν είναι όσο δύσκολο όσο φαίνεται να μπείς . Επίσης το dark web κάποια άτομα το χρησιμοποιούν και για να αποφύγουν την λογοκρισία και το χρησιμοποιούν και να κάνει; ότι θέλεις χωρίς να ξέρουν ποιος είσαι .

Ομάδα 4

Η ερώτηση ήταν αν είναι σωστό να έχουμε ελεύθερη πρόσβαση στο σκοτεινό διαδίκτυο
Κατα την γνώμη μου δεν πρέπει να έχουμε σε καμία περίπτωση ελεύθερη πρόσβαση στο dark web για πολλούς και διάφορους λόγους. Μπορείς να βρείς μεγάλη ποσότητα ναρκωτικών πολλά ανατριχιαστικά βίντεο αλλά και παράνομα όπλα. Όλα αυτά πιστεύω πως θα σε ταράξουν πολύ ψυχολογικά επομένως μην μπείτε καν στον κόπο να αποκτήσετε πρόσβαση στο σκοτεινό διαδίκτυο. Επιπλέον υπάρχουν πολλά βίντεο από κακοποίηση παιδιών τα οποια βίντεο γίνονται με βάναυσο τρόπο.

Ακούγοντας τις λέξεις Dark Web το πρώτο που μας έρχεται στο μυαλό είναι η παρανομία και όλα όσα συνδέονται με μια παράνομη πράξη. Πράγματι το Dark Web αυτό είναι! Παιδική πορνογραφία, βιασμοι, κακοποίηση ανθρώπων, ναρκωτικά, όπλα, παράνομα λογισμικά κτλ. Τα πάντα μπορείς να βρεις στο Dark Web. Έτσι λοιπόν, από άποψη ηθικής η πρόσβαση μας

σε αυτό δεν είναι σωστή καθώς συνδέεται με κάποια παράνομη πράξη που έχουμε σκοπό να κάνουμε! Ωστόσο, δεν πρέπει να ξεχνάμε ότι το Dark Web σε ορισμένες περιπτώσεις, βασικά ελάχιστες, είναι ωφέλιμο. Για παράδειγμα, αν δεν υπήρχε αυτό δε θα έβγαιναν βίντεο και εικόνες από ένα πόλεμο και έτσι δε θα ανακαλύπταμε την αλήθεια πίσω από τον πόλεμο (πχ πόλεμος Αφγανιστάν). Επίσης, μέσω του Dark Web οργανώνονται συλλαλητήρια και διαδηλώσεις για παγκόσμια θέματα.

Ομάδα 5

Θεωρώ ότι η ελεύθερη πρόσβαση στο dark web ειναι σωστή αρκεί η χρήση να μην βλάπτει τους αλλους και την κοινωνία. Καθώς οι δυνατότητες που σου προσφέρει σε σχέση με το απλο διαδίκτυο ειναι πολλες .Αρχικά δεν υπάρχει έλεγχος σε αυτα που ανεβάζουν ,ας μην ξεχνάμε ότι σε πολλες χωρες υπάρχει λογοκλοπή, έτσι το dark web ειναι ενας καλος τρόπος ενημερώσεις. Ακομα μπορείς να κάνεις συναλλαγές που δεν θα μπορούσες να κανεις δημόσια. Επί πλέον υπάρχει ανωνυμία κι ολα ειναι απρόσωπα. Τελος ειναι πιο ασφαλές σε σχέση με το απλο διαδίκτυο. Όπως λέγανε και οι αρχαίοι μας πρόγονοι όμως, μέτρον άριστον.

Ομάδα 6

Το Dark Web είναι ένα κομμάτι του διαδικτύου. Αυτό έχει ως αποτέλεσμα να είναι ελεύθερο στη χρήση από όλου τους ανθρώπους ,είτε για "σκοτεινά" ζητήματα,είτε όχι.Θα μπορούσαμε να το χαρακτηρίσουμε ως δίκοπο μαχαίρι.Απο την μια πλευρά προσφέρει ένα μεγάλο πλήθος πληροφοριών, την δυνατότητα ανταλλαγής ιδεών χωρίς διακρίσεις(αφού είναι ανώνυμα) και άλλα πολλα που βοηθούν τους ανθρώπους που το χρησιμοποιούν.Απο την άλλη, μερια δίνει την δυνατότητα να πραγματοποιούνται ενέργειες που βλάπτουν τους ανθρώπους, όπως εμπόριο όπλων και ναρκωτικών,παιδική πορνογραφία,μίσθωση δολοφόνων.Είναι ένα σπουδαίο εργαλείο που αν χρησιμοποιηθει σωστα θα μπορέσει να ωφελήσει πολυ την ανθρωποτητα.
Η ελευθερη προσβαση σε αυτο ειναι ενα πολυ σημαντικο θεμα που θα πρέπει να επισημανθεί.Το να μπορει καποιος ανθρωπος να έχει ελεύθερη πρόσβαση σε ενα μεσο ειναι κατι πολυ καλο και κατι που βοηθά και ενισχύει το γενικοτερο πνευμα της δημοκρατιας.Όμως σε αυτη την περιπτωση η ελευθερη προσβαση στο Dark Web ειναι κατι το οποίο μπορεί μεν να βοηθα τους ανθρώπους ,αλλα μπορει και να ειναι αρκετα επιζήμιο όπως προαναφέραμε ήδη.Ετσι πιστεύουμε πως η ελευθερη προσβαση στο Dark Web δεν πρεπει να γινεται, γιατι τα αποτελεσματα της ειναι πολυ επιζήμια και επικινδυνα για τους ανθρωπους.

Ομάδα 7

Το Dark Web ειναι ενα "Σκοτεινό διαδίκτυο" οπου εκει μεσα περιέχεται οτι απαγορευεται ρητα απο τους νομους.Και αυτα ειναι:Ναρκωτικα, οπλα, αριθμους κλεμμενων πιστωτικων καρτων, διαβατηρια, παιδικη πορνογραφια, ξεπλυμα μαυρου χρηματος...Αυτην ειναι η πλευρα του Dark Web...Η μια της πλευρα.Διοτι η δευτερη μπορει να αποδειχθει αρκετα χρησιμη για την ολη ανθρωποτητα.Στα βασικα χαρακτηριστικα του "Σκοτεινου Διαδικτυου" ειναι οτι προασπιζει την ανωνυμια του χρηστη.Οποτε λειτουργει σαν καταφυγιο για τους ανθρωπους που ειναι αντικαθεστωτικοι και η ελευθερια εκφρασης δεν νοειται στην χωρα τους.Αλλωστε μεσα απο το Dark Web ηδη διοργανωθηκαν σημαντιλεγελυλλαλητηρια.Επισης αλλο ενα θετικο που εχει το Dark Web ειναι η δημιουργια ενος οικονομικου προσομοιωτη του ψηφιακου νομισματος Bitcoin οπου αλλαξε ουσιαστικα τα ηδη υπαρχοντα δεδομενα της οικονομιας και μπορει στο κοντινο μελλον να αντικαταστήσει τα σημερινα χρηματα.Αλλωστε οπως ελεγε και ο Ulbricht: "Δημιούργησα εναν οικονομικο προσομοιωτη ωστε οι ανθρωποι να μπορουν να δουν απο πρωτο χερι πως ειναι να ζεις χωρις συστηματικη χρηση βιας"...Και τα καταφερε.
Συνοψίζοντας, το Dark Web ειναι ενα χρησιμο μεσο οπου θα γινοταν πολυ καλυτερο, κατα τη γνωμη μου,αν ολα αυτα τα περιεχομενα που αμαυρωνουν το ονομα αυτου του διαδικτυου

σταματουσαν να υπαρχουν.Τοτε θα ηταν πολυ καλυτερη και ωφελιμη η ελευθερη προσβαση στο Dark Web καθως θα ηταν απαλλαγμενη απο καθε στοιχειο που θα μπορουσε να βλαψει τον ανθρωπο.

Ομάδα 8

Γενικότερα το θέμα του Dark Web στις μέρες μας απασχολεί όλο και περισσότερους ανθρώπους. Η πρόσβαση του ενω δεν είναι παράνομη θα πρέπει να περιορίζεται σε δραστηριότητες που δεν είναι ηθικά λάθος.Κατά την γνώμη μου η ελεύθερη πρόσβαση σε αυτό έχει ωφελήσει πολλούς ανθρώπους ανά τον κόσμο.Εκτός από αυτούς που μπαίνουν στον ιστό για παράνομες ενέργειες έχει ωφελήσει και όσους ψάχνουν έμπιστες πληροφορίες που δεν μπορούν να βρούν στο Surface Web και αυτό μπορεί να βοηθήσει στην δουλειά τους.Ισως πάλι ωφελήσει τους ανθρώπους που θέλουν να γράψουν κάτι σημαντικό με την άνεση της ύπαρξης της ανωνυμίας και επομένως την αποφυγή της έκθεσής τους ή απλά να μάθουν κάτι παραπάνω για ένα θέμα η μια πληροφορία που θα τους ξαφνιάσει.

Παραταύτα η ελεύθερη αυτή πρόσβαση προκαλεί περισσοτερα αρνητικά απότι θετικά και γιαυτό τον λόγο πιστεύω πως η πρόσβαση στο Dark web δεν είναι ηθικά σωστή καθώς μέσα σε αυτό μπορεί να μπλέξεις πολύ εύκολα με παράνομα θέματα και ανθρώπους όπως η αγορά ναρκωτικών,η παιδική πορνογραφία,οι πληρωμένοι δολοφόνοι κ.τ.λ και άθελα σου να βρεθείς αντιμέτωπος με ανθρώπους που είναι ικανοί να σε παρασύρουν.Ετσι παρά τα θετικά που μπορεί να προσφέρει ως ένας ανώνυμος ιστός το Dark Web καλό θα ήταν να αποφεύγεται η χρήση του έτσι ώστε να μην υπάρξει κάποια εμπλοκή με τον νόμο.

Βιβλιογραφία – Ιστογραφία – Πηγές

URLs (διευθύνσεις)

https://www.thesun.co.uk/news/5815189/dark-web-live-torture-hire-hitmen-hackers/

https://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html

http://access-point.gr/cooking-up-a-batch-of-mas-famous-breadsticks/

http://ask-leo.com/whats_the_difference_between_a_sandbox_and_a_virtual_machine.html

https://en.wikipedia.org/wiki/Sandbox_(computer_security)

https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/

https://www.makeuseof.com/tag/virtual-machine-makeuseof-explains/

Βιβλία:

01. Chen, H - Dark Web, Exploring and Data mining the Dark side of the Web

02. Gehl, R - Weaving the Dark Web

03. Henderson, L - Darknet, Guide to Staying Anonymous Online

04. IGI Global - The dark web, breakthroughs in research and practice

05. Masterson, S - Tor Browser Handbook

06. TIME - Cybersecurity, Hacking, the Dark Web

07. CHIP Malaysia - The end of Darknet

08. Gehl, R - Weaving the Dark Web