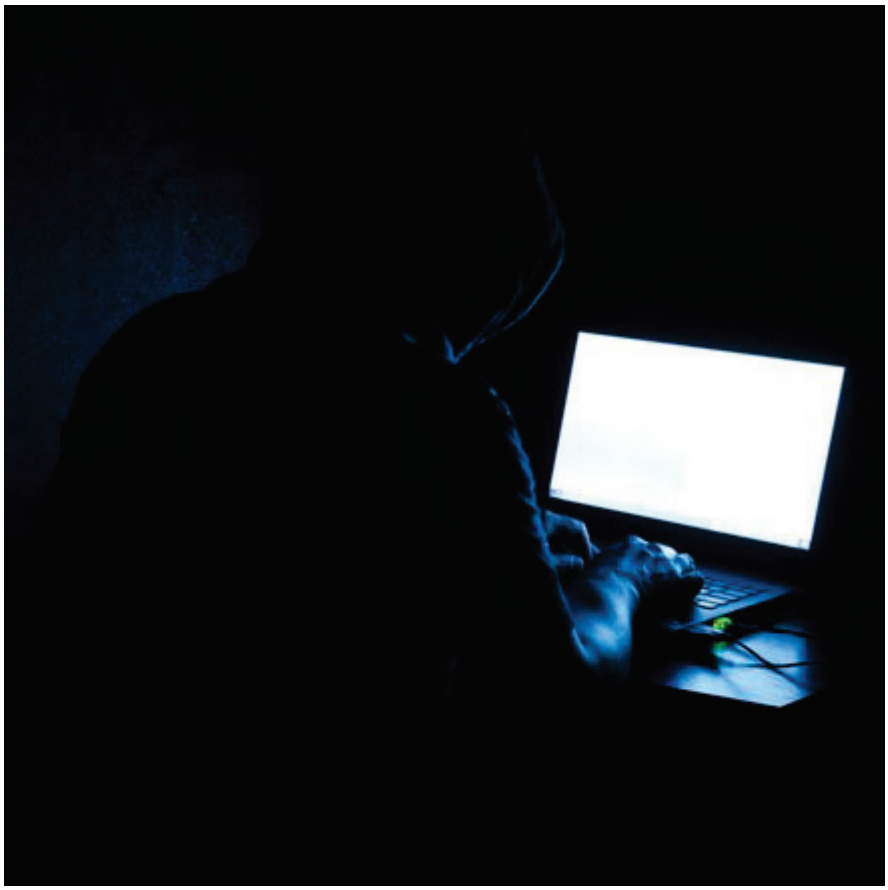
Τμήμα
Μηχανικών
Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

DEEP/DARK WEB: ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΚΑΙ ΤΕΧΝΙΚΑ ΖΗΤΗΜΑΤΑ



ΣΠΟΥΔΑΣΤΡΙΑ: ΜΗΛΙΩΝΗ ΕΛΕΝΗ
ΑΜ: 1625

ΕΠΟΠΤΕΥΟΝ ΚΑΘΗΓΗΤΗΣ:ΑΣΗΜΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ
ΑΝΤΙΡΙΟ 7/6/2017

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Από τους εκατομμύρια ανθρώπους που «σερφάρουν» καθημερινά από τον υπολογιστή ή την «έξυπνη» συσκευή τους, πολλοί ίσως δεν έχουν διανοηθεί πως, εκτός από το «ορατό» Internet, υπάρχει κι ένα παράλληλο online «σύμπαν» από υπηρεσίες και ιστοσελίδες στις οποίες δεν υπάρχει περίπτωση να... πέσουν κατά τύχη πάνω τους. Απροσπέλαστο από τους συμβατικούς browser, το «σύμπαν» αυτό έχει «βαφτισθεί» Σκοτεινό Διαδίκτυο (Darknet). Ένα όνομα που χρωστά στο γεγονός ότι παραμένει κρυμμένο από τις μηχανές αναζήτησης που «σαρώνουν» το web, όπως και από τις διωκτικές αρχές ή τις υπόλοιπες κρατικές υπηρεσίες ανά τον κόσμο.

Η λογική του Darknet είναι να παρέχει ανωνυμία σε όσους το χρησιμοποιούν – κάτι που, όπως ισχύει και στον πραγματικό κόσμο, αποτελεί μια ευκαιρία την οποία δεν θα άφηναν ανεκμετάλλευτη οι εγκληματίες. Από τις έκνομες δραστηριότητες που έχουν βρει «στέγη» σε αυτό, ψηλά στη λίστα βρίσκεται η διακίνηση κάθε λογής παράνομου προϊόντος ή υλικού. Έτσι, το Σκοτεινό Διαδίκτυο επιστρατεύεται κατά κόρον για αγοραπωλησίες παιδικής πορνογραφίας, ναρκωτικών, όπλων, κλεμμένων πιστωτικών καρτών και πλαστών ταυτοτήτων.

Στις περισσότερες περιπτώσεις, οι παράνομες συναλλαγές γίνονται από online «μαύρες αγορές», δηλαδή site όπου οι «πωλητές» αναρτούν τις αγγελίες τους και δέχονται παραγγελίες. Όπως λειτουργεί και το νόμιμο ηλεκτρονικό εμπόριο, τα προϊόντα αποστέλλονται ταχυδρομικά, στη διεύθυνση που θα επιλέξει ο αγοραστής. Με τη διαφορά ότι οι αγοραπωλησίες γίνονται ως επί το πλείστον σε Bitcoin, το εικονικό νόμισμα στο οποίο δεν εμπλέκεται κάποια κεντρική τράπεζα, με συνέπεια να είναι πιο δύσκολο να ανιχνευθούν οι συναλλαγές.

Το Darknet είναι ένα δίκτυο από server, οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα. Η πιο διαδεδομένη τεχνολογία γι' αυτό τον σκοπό είναι το Tor (The onion router), το οποίο αναπτύχθηκε αρχικά από το Ερευνητικό Εργαστήριο του αμερικανικού πολεμικού ναυτικού, για την προστασία των στρατιωτικών επικοινωνιών. Χάρις στο Tor, ένα site μπορεί να αποκρύπτει τα ψηφιακά του ίχνη, «καμουφλάροντας» τον server που το φιλοξενεί. Παράλληλα, η τεχνολογία εξασφαλίζει πως πρόσβαση στο Σκοτεινό Διαδίκτυο έχουν μόνον χρήστες που έχουν εγκαταστήσει το ανάλογο λογισμικό στο μηχάνημά τους. Λογισμικό που εγγυάται και τη δική τους ανωνυμία.

Μέχρι πρόσφατα, ακόμη κι αν είχε κανείς εγκαταστήσει το software, θα έπρεπε να γνωρίζει επίσης τη συγκεκριμένη διεύθυνση κάθε ιστοσελίδας που θέλει να επισκεφθεί. Ωστόσο, το Darknet απέκτησε το δικό του «ψαχτήρι», το Grams, μια μηχανή αναζήτησης που συγκεντρώνει αποτελέσματα από οκτώ online «μαύρες αγορές» και τις αγγελίες τους. Βέβαια, το κίνητρο του δημιουργού του Grams είναι το κέρδος, αφού όπως ανέφερε στο αμερικανικό περιοδικό Wired, σύντομα θα αρχίσει να χρεώνει όσους θέλουν οι αγγελίες τους να εμφανίζονται ψηλότερα στα αποτελέσματα.

Εξάλλου, το κέρδος είναι επίσης βασική αιτία που οι περισσότερες από αυτές τις ιστοσελίδες εμφανίστηκαν παρά τη σύλληψη τότε από το FBI του ανθρώπου που φέρεται να είναι ο «εγκέφαλος» πίσω από το Silk Road, -«μια από τις πιο εξελιγμένες online "μαύρες αγορές"» όπως έχει χαρακτηρισθεί. Κι αυτό γιατί, με βάση τη δικογραφία, τα έσοδα του Silk Road μέσα σε λιγότερο από 3 χρόνια λειτουργίας άγγιξαν τα 80 εκατομμύρια δολάρια, από την προμήθεια που χρέωνε για κάθε αγοραπωλησία. Μάλιστα, οι συναλλαγές που έγιναν στο διάστημα λειτουργίας του site φαίνεται πως ξεπέρασαν τα 1,2 δισ. δολ.

Πάντως, σύμφωνα με τις διωκτικές αρχές σε όλο τον κόσμο, το Σκοτεινό Διαδίκτυο κάνει πιο δύσκολη την αντιμετώπιση του online εγκλήματος, όχι όμως και αδύνατη. Ετσι, ενώ ο κατηγορούμενος ως διαχειριστής του Silk Road δικάστηκε, σε ποινή φυλάκισης 30 ετών, εξαρθρώθηκε μια ακόμη online «μαύρη αγορά», η Utopia, με τη σύλληψη πέντε υπόπτων από την ολλανδική και τη γερμανική αστυνομία.

Πάγια τακτική είναι οι αρχές να μην αποκαλύπτουν τι είδους ηλεκτρονικά «αντίμετρα» επιστρατεύουν – στην περίπτωση του Silk Road, ο εκπρόσωπος του FBI αναφέρθηκε απλώς σε «ανθρώπινα λάθη» που οδήγησαν στα ίχνη του διαχειριστή του. Από την άλλη μεριά, οι αρχές εκμεταλλεύονται το γεγονός ότι τα εγκλήματα στον online κόσμο αφήνουν ίχνη και στον πραγματικό: για την εξάρθρωση του Utopia, σύμφωνα με το δελτίο Τύπου της ολλανδικής αστυνομίας, αστυνομικοί υποδύθηκαν τους «πελάτες», αγοράζοντας ναρκωτικά και όπλα. «Η επιχείρηση στέλνει ένα ξεκάθαρο μήνυμα πως κανείς δεν μπορεί να ξεγλιστρήσει, επειδή χρησιμοποιεί το Tor», αναφέρεται χαρακτηριστικά στην ανακοίνωση.

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Για να κατανοήσουμε πως ακριβώς λειτουργούν το Deep web & το Dark Web θα πρέπει να κάνουμε μια σύντομη ιστορική αναδρομή στον τρόπο λειτουργίας του διαδικτύου.
Ως γνωστόν, η ηλεκτρονική επόχή τον 20 αιώνα σηματοδοτήθηκε απο την ικανότητα των υπολογιστών να μεταφέρουν και να αποθηκεύουν πληροφορίες σε ελάχιστο χρόνο μέσα απο αντίστοιχα δίκτυα με πρώτο εξ αυτών το **ARPANET** τη δεκαετια του 70', ως πρόγονο του σημερινού Internet.
Το ARPANET δημιουργήθηκε ως δίκτυο επικοινωνίας με ασφαλή τρόπο για τον στρατό των ΗΠΑ απο τον στρατιωτικό οργανισμό **ARPA(Advanced Research Projects Agency)**
Η πρώτη δεκαετία των ψηφιακών επιτευγμάτων του Internet, κάπου στα μέσα του 1990 είχε ως σήμα κατατεθέν τις συνδέσεις σε απλές σελίδες παρουσίασης (web pages) HTML με πολύ αργές ταχύτητες. Ένα ακόμα σημείο αναφοράς εκείνης της εποχής ήταν τα λεγόμενα Bulletin Boards, προπομπός και αυτα των σημερινών forums και κοινωνικών δικτύων οπου το μέλος για να μπεί, έπρεπε μέσω της τηλεφωνικής του σύνδεσης να καλέσει συγκεκριμένο αριθμό (dial-in) για να συμμετάσχει, ενω απαιτούνταν και πολλές τεχνικές γνωσεις.
Κανείς δεν είχε τον απόλυτο έλεγχο της ροης πληροφορίας και έμοιαζε σαν ένας τόπος σκοτεινός που μπορούσαν να τον χρησιμοποιήσουν παρα μόνο ελάχιστοι, οι οποίοι διέθεταν τις απαιτούμενες γνώσεις.

ΚΕΦΑΛΑΙΟ 1 :DARKNET / DARK WEB - DEEP WEB

Όσοι ασχολούνται με την τεχνολογία κάποια στιγμή έχουν συναντήσει αυτές τις ορολογίες χωρίς να γνωρίζουν το πραγματικό νόημά τους. Μερικές φορές ακόμη και οι εμπειρογνώμονες μπερδεύονται με αυτούς τους όρους επίσης. Θα προσπαθήσουμε να δώσουμε μια κατανοητή ερμηνεία και να εντοπίσουμε τις διαφορές τους πριν αναφερθούμε στο κάθε ένα αναλυτικά στα επόμενα κεφάλαια.

Μπορούμε να τα θεωρήσουμε ως τα διαφορετικά μέρη του Παγκόσμιου Ιστού (WWW) όπου οι ιστοσελίδες έχουν διαφορετικά δικαιώματα πρόσβασης. Το Darknet είναι η σκοτεινότερη πλευρά του ιστού ενώ η επιφανειακή μεμβράνη είναι η πιο ανοιχτή πλευρά.
Μόνο το 4 % του διαδικτύου είναι προσβάσιμο από τις μηχανές αναζήτησης όπως το Google, το Bing ή το Yahoo και το υπόλοιπο 96 % των περιεχομένων του διαδικτύου είναι προσβάσιμα μόνο με ειδικά εργαλεία και λογισμικό - browsers και άλλα πρωτόκολλα πέρα από τους άμεσους συνδέσμους ή τα διαπιστευτήρια.
Μπορούμε να καταλάβουμε λοιπόν πόσο απέραντη είναι η πιο σκοτεινή πλευρά του Παγκόσμιου Ιστού όπου κρύβονται εγκληματίες, στρατιωτικά μυστικά, προφίλ χάκερ, μαύρες αγορές, ναρκωτικά κ.α .

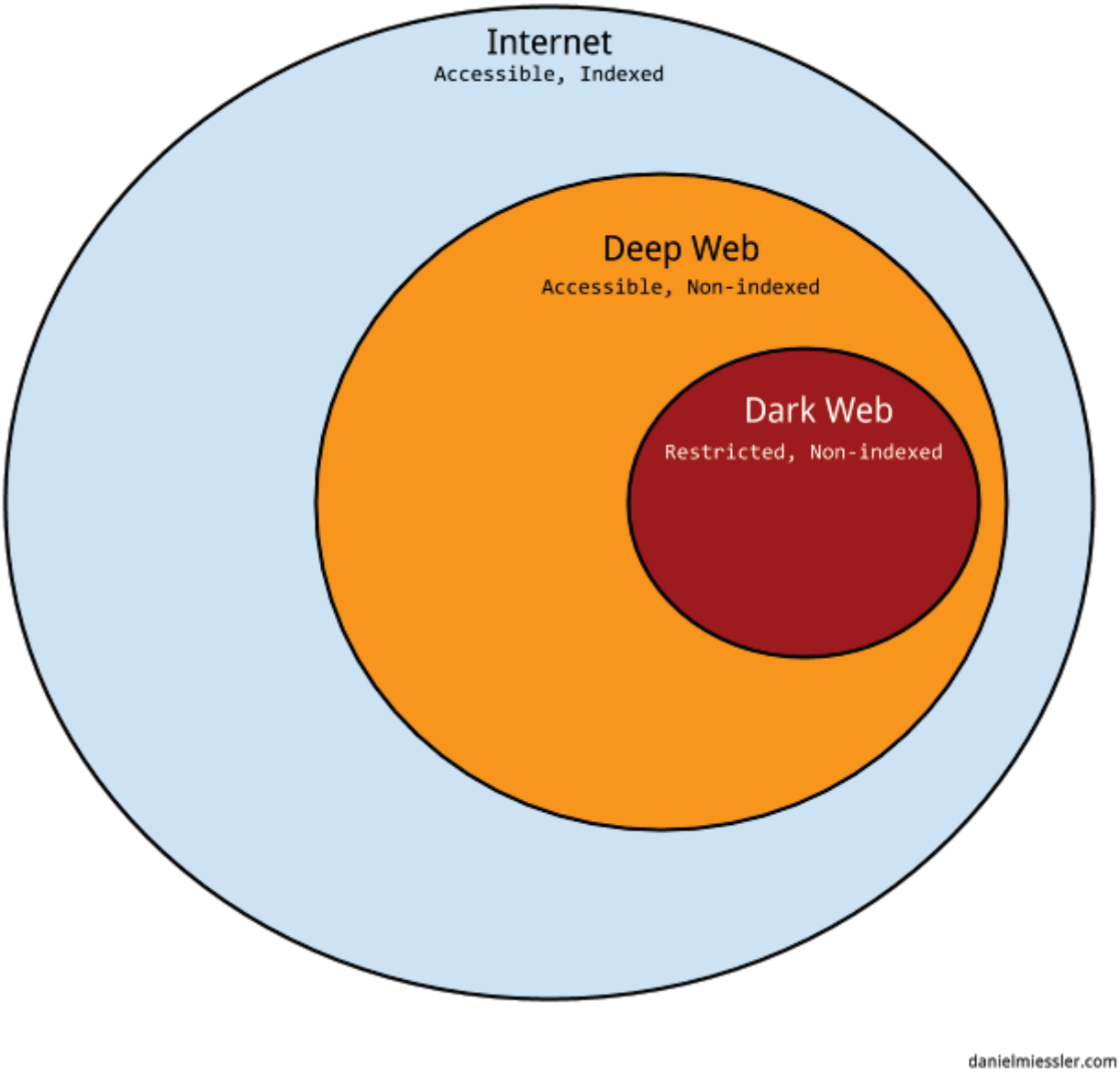
1.1 :Darknet & Dark Web

Το Darknet είναι ένα δίκτυο επικάλυψης. Ένα δίκτυο που είναι χτισμένο πάνω στο διαδίκτυο, το οποίο έχει σχεδιαστεί ειδικά για ανωνυμία. Το Darknet και το Dark Web είναι άμεσα συνδεδεμένα. Ο όρος Dark Web αναφέρετε σε ιστότοπους που βρίσκονται σε ένα σκοτεινό δίκτυο. Dark Web είναι οι ιστοσελίδες σε servers στους οποίους δεν είναι δυνατή πρόσβαση από μια μηχανή αναζήτησης χωρίς έναν έγκυρο λογαριασμό. Το μεγαλύτερο ποσοστό των παράνομων δραστηριοτήτων λαμβάνουν χώρο στο Dark Web

1.2 :Deep Web

Πάνω από το Dark Web υπάρχει το Deep Web. Το Deep Web είναι επίσης στην σκοτεινότερη πλευρά του Διαδικτύου επειδή όπως και το Dark Web τα βαθιά περιεχόμενα του ιστού δεν μπορούν να βρεθούν ή να αποκτήσουν άμεση πρόσβαση μέσω μηχανών αναζήτησης τύπου Google. Σε αντίθεση με το Dark Web το Deep Web δεν χρειάζεται πάντα το ειδικό πρόγραμμα περιήγησης Tor. Αντίθετα οι περισσότερες πληροφορίες του Web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες. Αυτές οι σελίδες δεν υπάρχουν μέχρι να δημιουργηθούν δυναμικά ως αποτέλεσμα μιας συγκεκριμένης αναζήτησης.

ΚΕΦΑΛΑΙΟ 2: DEEP WEB



2.1 : Ορισμός

Το Deep Web (ο Βαθύς Ιστός επίσης γνωστό ως Deepnet, Darknet, Undernet, το αόρατο Web ή το κρυμμένο Web) είναι ένα υποσύνολο του διαδικτύου το οποίο δεν είναι ορατό από τις μεγάλες μηχανές αναζήτησης. Αυτό σημαίνει ότι ο χρήστης πρέπει να επισκεφθεί αυτά τα μέρη απευθείας αντί να μπορεί να τα αναζητήσει. Έτσι δεν υπάρχουν κάποιες οδηγίες ή κατευθύνσεις για να φτάσει κάποιος εκεί, μα μπορούν να βρεθούν αν υπάρχει η ακριβής διεύθυνση.

Είχατε πρόσβαση στο email σας σήμερα; Έχετε ελέγξει τα μηνύματά σας στο Facebook; Ή το προσωπικό σας Dropbox; Εάν κάνατε τουλάχιστον ένα από αυτά, τότε μπήκατε στο Deep Web. Το Deep Web δεν είναι κάποιο μυστηριώδες μέρος όπως απεικονίζεται.
Αντ' αυτού, είναι η συλλογή εκατομμυρίων αρχείων στο διαδίκτυο που δεν είναι διαθέσιμα στο κοινό. Φανταστείτε να είχε κάποιος πρόσβαση στο email σας.
Δεν θα ήταν πολύ καλό έτσι είναι "κρυμμένο" από τον κανονικό ιστό.
Οι πρώτες εκτιμήσεις έδειξαν ότι ο Βαθύς Ιστός είναι 400 έως 550 φορές μεγαλύτερος από τον επιφανειακό ιστό. Η έρευνα ανίχνευσε περίπου 300.000 Deep Web Sites σε ολόκληρο τον Ιστό το 2004 και περίπου 14.000 Deep Web Sites μόνο στο ρώσικο τμήμα του ιστού το 2006.
Σύμφωνα με μια μελέτη που έγινε στο πανεπιστήμιο Berkley της Καλιφόρνια το Deep Web αποτελείται από 91.000 terabytes. Αντίθετα το επιφανειακό web, που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης είναι περίπου 167 terabytes.
Το Youtube υπολογίζεται ότι είχε το 2011 αποθηκευμένα περίπου 200 εκατομμύρια βίντεο, συνολικού μεγέθους 5 petabytes ή 5000 terabytes
Το σίγουρο είναι ότι κανείς δεν μπορεί να υπολογίσει με ακρίβεια σήμερα το μέγεθος του καθώς συνεχώς μεταβάλλεται και αυξάνεται.

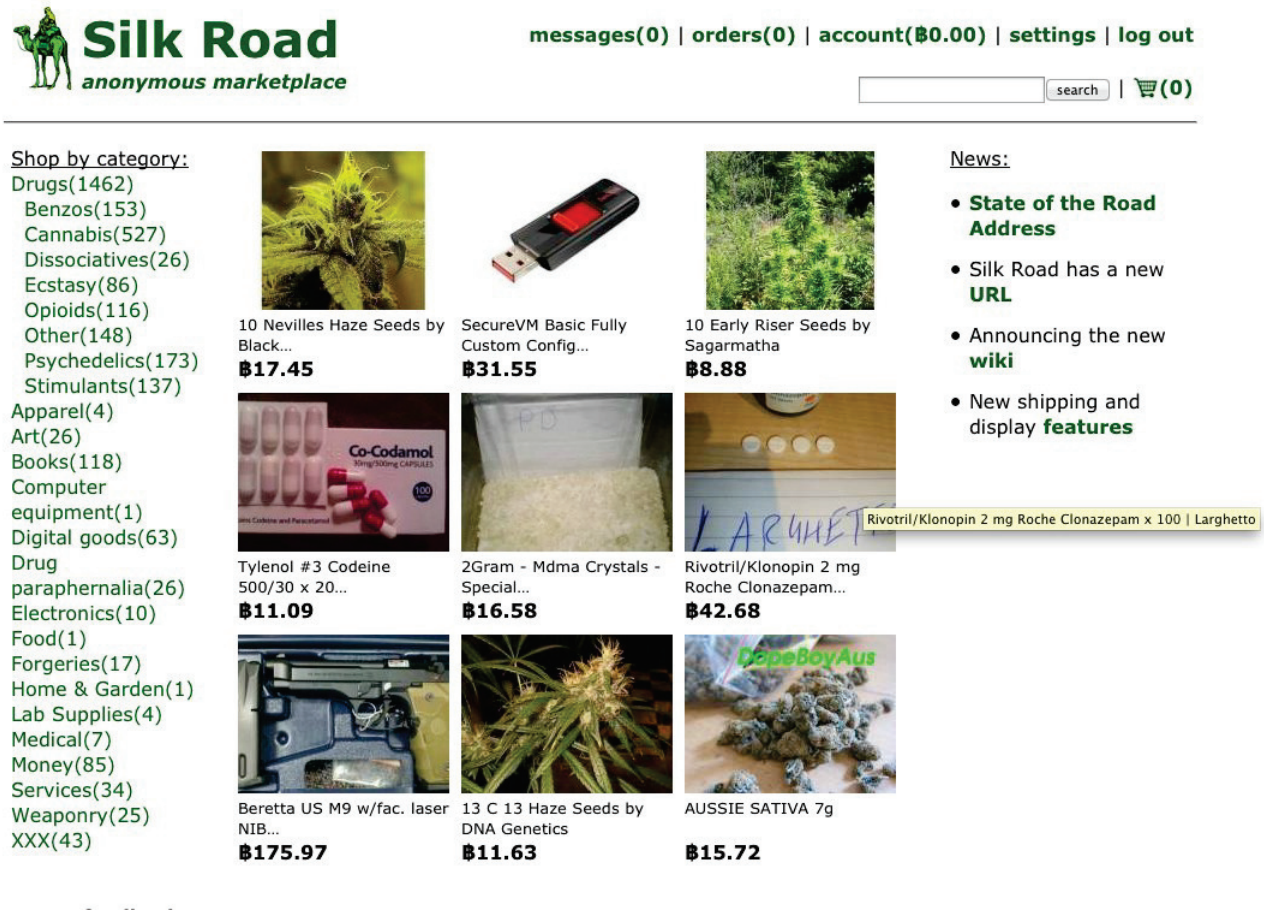
Μερικές από τις μηχανές αναζήτησης που έχουν πρόσβαση στο Deep Web είναι οι εξής:

- http://www.findthatfile.com : εξετάζει σχεδόν όλους τους τύπους αρχείου και τα πρωτόκολλα

- www.semanticommunity.info : ασχολείται με την γενική στρατιωτική επισκόπηση σε hardware

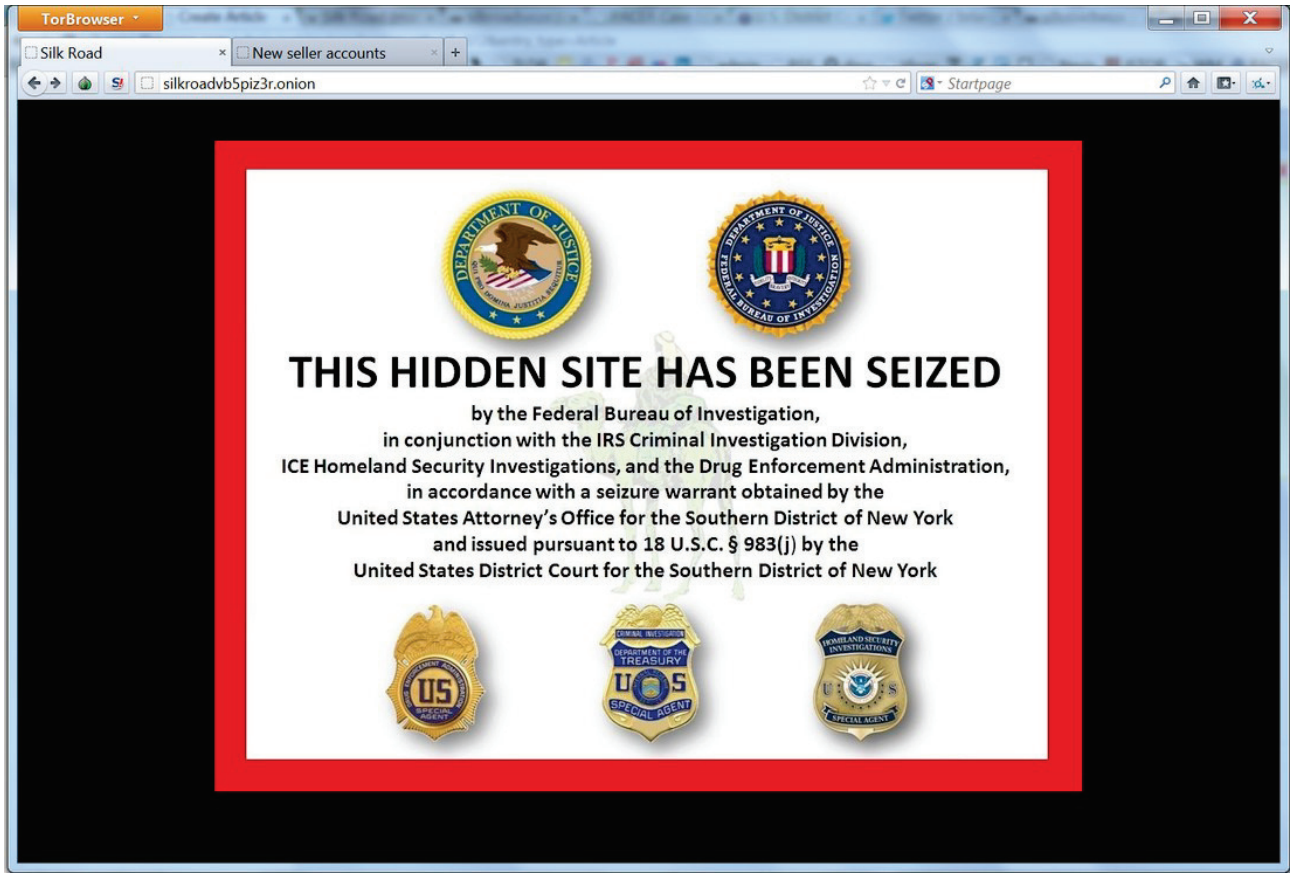
- www.archive.org : ένα μεγαθήριο των media – σπάνια βιβλία, ηχητικά ντοκουμέντα και βίντεο, αρχειοθετημένες εικόνες των παλαιότερων websites των τελευταίων 20 χρόνων και ελεύθερα ακουστικά βιβλία (audio books)

2.2 : Silk Road



Το πιο διάσημο "κρυμμένο" website ήταν το Silk Road. Με περισσότερους από 960.000 εγγεγραμμένους χρήστες ονομάστηκε ως η πιο εξελιγμένη και εκτεταμένη εγκληματική αγορά στο διαδίκτυο.
Ο άνθρωπος που κατηγορείται "ότι έτρεχε" το Silk Road είναι ο Ross Ulbricht που κυκλοφορούσε με το ψευδώνυμο Dread Pirate Roberts και τελικά συνελήφθη από τις αρχές το φθινόπωρο του 2013.
Το Silk Road εδώ και πολύ καιρό βρισκόταν στο στόχαστρο των Αμερικάνικών (και όχι μόνο) αρχών, καθώς ήταν μια πλατφόρμα στην οποία διάφοροι προμηθευτές όλων των ειδών ναρκωτικών και άλλων εμπορευμάτων, που δεν μπορεί κανείς να αγοράσει στην ελεύθερη αγορά, εξέθεταν το εμπόρευμά τους και οι καταναλωτές μπορούσαν να ψωνίσουν ότι εκείνοι ήθελαν μέσα από μια μεγάλη ποικιλία.
Οι πληρωμές γίνονταν φυσικά σε Bitcoin (το οποίο θα αναλύσουμε στην συνέχεια).
Το Silk Road διέθετε επίσης και κάποιους υπαλλήλους. Ένας από αυτούς αποφάσισε να υπεξαιρέσει bitcoins από χρήστες, με αποτέλεσμα το αφεντικό του και ιδιοκτήτης

του Silk Road να εξοργιστεί μαζί του. Δε δίστασε μάλιστα, στα forum του Silk Road να δημοσιοποιήσει την επιθυμία του να δείρει κάποιος τον κλέφτη υπάλληλό του, προκειμένου να τον εξαναγκάσει να επιστρέψει τα bitcoin που είχε καταχραστεί. Στην συνέχεια όμως άλλαξε γνώμη : "Να αλλάξω την εντολή για ξυλοδαρμό σε εντολή για δολοφονία;" είχε αναφέρει.
Κάπως έτσι ξεκίνησε να ανταλλάσει μηνύματα με κάποιον που παρουσιάστηκε ως εκτελεστής και έκλεισε συμφωνία μαζί του να σκοτώσει τον υπάλληλό του έναντι 40.000 δολαρίων. Ο εκτελεστής έστειλε φωτογραφίες από την "εκτέλεση" και ενώ αρχικά ο Dread Pirate Roberts εξέφρασε μια επιφύλαξη για την αποτελεσματικότητά του, τελικά πείστηκε πως ο υπάλληλός του ήταν νεκρός.
Κι όμως ο υπάλληλος κρατούνταν από τις αρχές, στις οποίες και είχε ομολογήσει τι είχε κάνει, ενώ ο υποτιθέμενος εκτελεστής ήταν πράκτορας των αρχών.
Και κάπως έτσι ο Ross Ulbricht βρέθηκε στα χέρια των αρχών, αφού είχε προηγηθεί παρακολούθηση των κινήσεών του και προσπάθεια εξακρίβωσης των στοιχείων του πολύ πριν την εικονική δολοφονία, όπου οι πράκτορες που σύχναζαν στην σελίδα του δεν ήταν για αν ψωνίσουν αλλά για να παρακολουθούν όλες τις κινήσεις και συνομιλίες του.



2.3 : Bitcoin

Το bitcoin είναι πιθανώς η μεγαλύτερη αλλαγή στο χρηματοοικονομικό σύστημα εδώ και έναν αιώνα, μεγαλύτερη ακόμα και απ' την πρώτη εμφάνιση των πιστωτικών καρτών.
Είναι ένα εντελώς ψηφιακό νόμισμα χωρίς να υπάρχει σε καμία φυσική μορφή κερμάτων ή χαρτονομισμάτων. Η παραγωγή του, η αποθήκευσή του, η διακίνησή του και όλες οι συναλλαγές με αυτό γίνονται αποκλειστικά σε ηλεκτρονική μορφή.

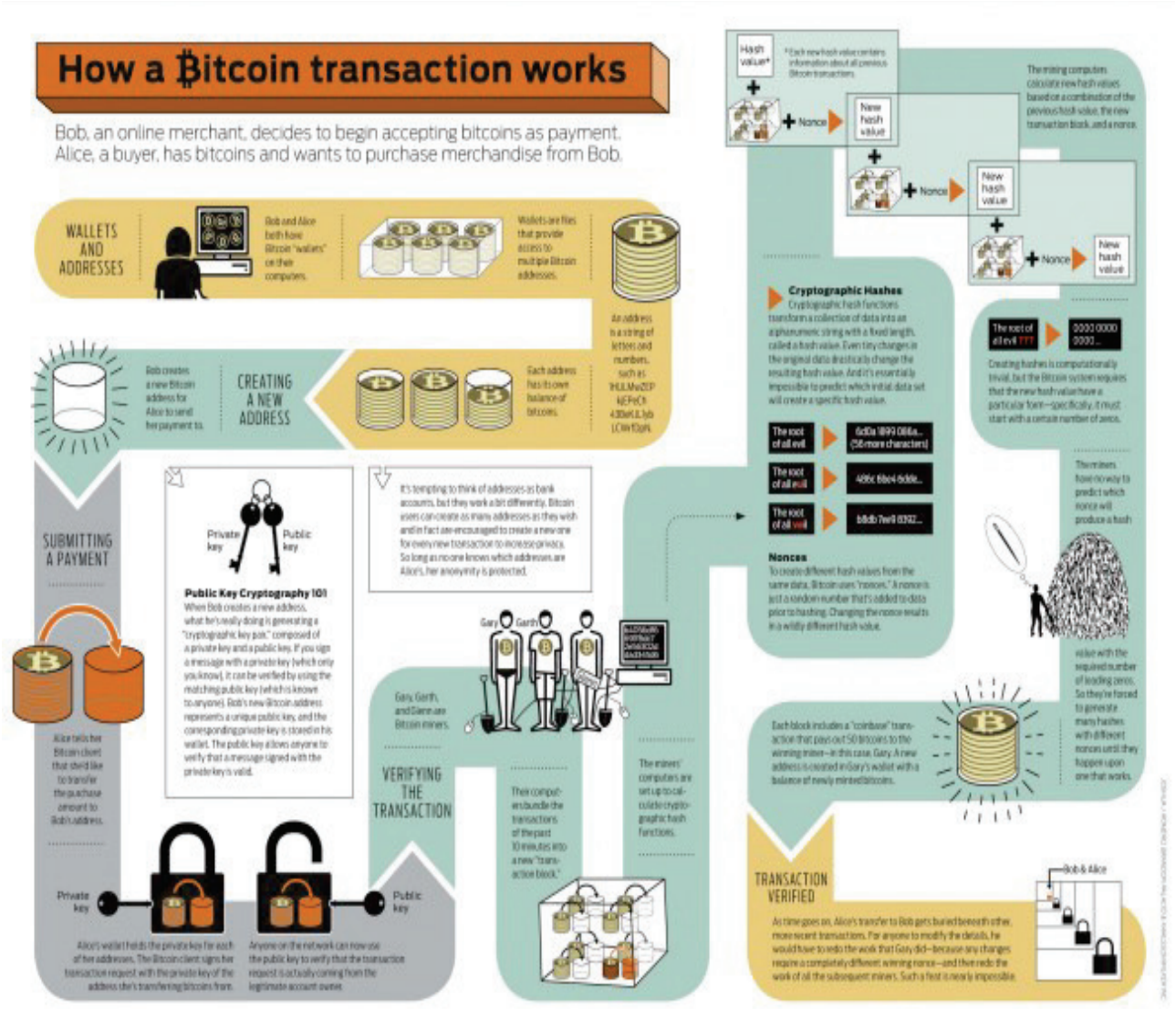
Για την ακρίβεια το bitcoin είναι ένα peer-to-peer σύστημα πληρωμών και ένα ψηφιακό συνάλλαγμα ανοιχτού κώδικα. Ανήκει στην κατηγορία cryptocurrency, καθώς χρησιμοποιεί μεθόδους κρυπτογραφίας για την δημιουργία και διαχείριση των χρημάτων και για την επιβεβαίωση της εγκυρότητας των συναλλαγών.

Ο τρόπος να αποθηκεύσουμε τα bitcoin και να κάνουμε αγορές με αυτά είναι ένα ψηφιακό "πορτοφόλι". Το πορτοφόλι αυτό μπορεί να βρίσκεται είτε σαν πρόγραμμα στον υπολογιστή μας, είτε να φιλοξενείται σε κάποια ιστοσελίδα πχ ένα Bitcoin Exchange.
Κάθε bitcoin wallet έχει μια μοναδική διεύθυνση, η οποία χρησιμοποιείται για να γίνουν οι μεταφορές ανώνυμα.

Όταν γίνεται μια συναλλαγή με bitcoin το σύστημα επιβεβαιώνει τις διευθύνσεις των 2 διαφορετικών wallets, του αγοραστή και του πωλητή. Έπειτα γίνονται κάποιοι περίπλοκοι μαθηματικοί υπολογισμοί για να επιβεβαιωθεί η εγκυρότητα της συναλλαγής. Αφού γίνουν οι πράξεις (απαραίτητες για το σύστημα κρυπτογράφησης που προστατεύουν το σύστημα) οι έγκυρες συναλλαγές καταγράφονται, και τα δεδομένα της κάθε συναλλαγής προστίθενται σε ένα δημόσιο αρχείο καταγραφών (log) που ονομάζεται Blockchain.

Είναι αρκετά ασφαλές αφού υπάρχει ένα σύστημα συνεχούς επιβεβαίωσης, που ουσιαστικά κάνει το ψηφιακό νόμισμα απρόσβλητο όσων αφορά τους hackers. Πολύ απλά, αν κάποιος επιχειρούσε να αντιγράψει ψηφιακά τα bitcoins του και πήγαινε μετά να τα ξοδέψει, δεν θα μπορούσε να παραχθεί μια έγκυρη συναλλαγή που να επιβεβαιώνεται από το υπάρχων blockchain. Ουσιαστικά το σύστημα θα αναγνώριζε τα διπλά bitcoin ως αντίγραφα και θα τα απέρριπτε.

Κατά συνέπεια εκτός αν ανακαλυφθεί κάποιο τεράστιο κενό ασφαλείας στο σύστημα, η πλαστογραφία είναι πολύ απίθανη.



2.4 : Τι περιέχει το Deep Web;

Οι μηχανές αναζήτησης εμφανίζουν αποτελέσματα χρησιμοποιώντας κάποιους αλγόριθμους που βάζουν σε λίστες τις ιστοσελίδες και λέγονται crawlers ή αράχνες. Οι Web Crawlers όμως δεν βρίσκουν τα πάντα. Υπάρχουν κρυφοί πόροι στο διαδίκτυο που σε γενικές γραμμές, κατατάσσονται στις παρακάτω κατηγορίες:

- **Δυναμικό περιεχόμενο:** δυναμικές σελίδες στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες στις οποίες συμπληρώνει στοιχεία. Στην ίδια κατηγορία ανήκουν οι σελίδες που δημιουργούνται με session ids και δεν έχουν σταθερό url.

- **Μη συνδεδεμένο περιεχόμενο:** σελίδες που δεν συνδέονται με άλλες σελίδες. Έτσι, οι αράχνες ή web crawlers που χρησιμοποιούν οι μηχανές αναζήτησης, δεν μπορούν να τις "βρουν" από άλλες σελίδες που εξετάζουν. Το internet λειτουργεί με τους συνδέσμους (links) και οι μηχανές αναζήτησης όταν ακολουθούν έναν σύνδεσμο που παραπέμπει σε κάποια άλλη σελίδα, τότε ανακαλύπτουν την νέα σελίδα και την ταξινομούν.

- **Private Web:** ιστοσελίδες που χρειάζεται να κάνετε login με username και password.

- **Contextual Web:** είναι οι σελίδες εκείνες που το περιεχόμενο των οποίων προσαρμόζεται ανάλογα με τον τρόπο που έχει κανείς πρόσβαση σε αυτό. Για παράδειγμα, οι σελίδες εκείνες που, αν έχετε πρόσβαση σε αυτές με μία διεύθυνση IP από την Ελλάδα, βλέπετε διαφορετικό περιεχόμενο από το αν θα επισκεπτόσασταν την ίδια σελίδα από μια IP των ΗΠΑ.

- **Περιεχόμενο περιορισμένης πρόσβασης:** ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους.

- **Scripted content:** σελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από JavaScript καθώς και περιεχόμενο που κατεβάζεται από Web servers μέσω Flash. Αυτός είναι και ο λόγος που τα flash sites είναι αόρατα από την Google.

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

- **Οτιδήποτε δεν ακολουθεί το πρότυπο HTTP/HTTPS:** που σημαίνει ότι ένα αρχείο σε κάποια άλλη γλώσσα προγραμματισμού δεν είναι προσπελάσιμο. Κείμενα που χρησιμοποιούν το παλαιότερο πρωτόκολλο Gopher και αρχεία που βρίσκονται σε διακομιστές FTP και τα οποία δεν μπορούν να εντοπιστούν από τις περισσότερες μηχανές αναζήτησης

2.4.1 : Παραδείγματα από σελίδες που περιέχει το deep web

- Τα **πιστοποιητικά γεννήσεως**, τα δικά μας και των παιδιών μας, καθώς και τα πιστοποιητικά οικογενειακής κατάστασης είναι καταχωρημένα στο Deep Web.

- Οι **τίτλοι σπουδών** μας και τα σχολεία που βγάλαμε, είναι καταχωρημένα στο Deep Web.

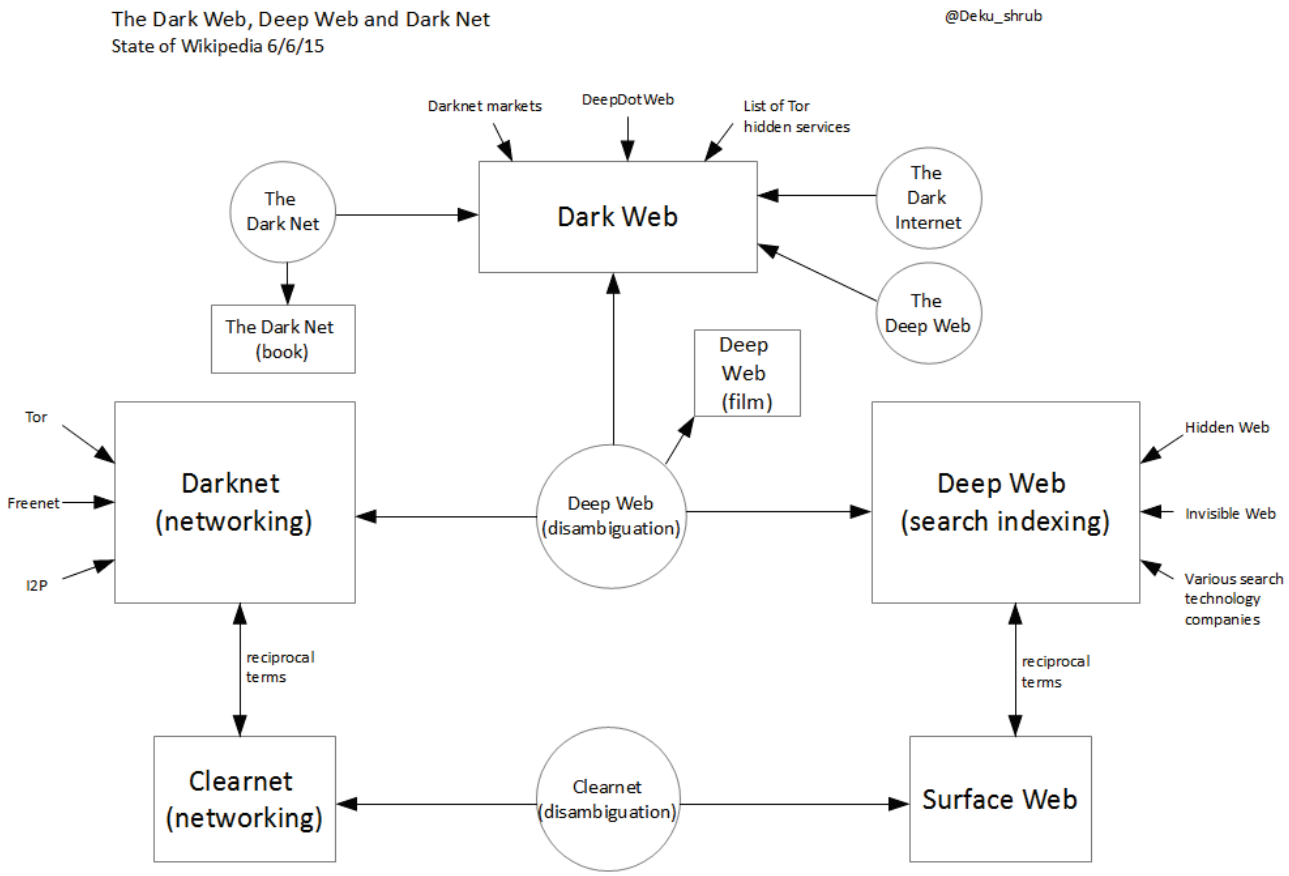
- Τα στοιχεία της αστυνομικής μας ταυτότητας, του διαβατηρίου μας, του διπλώματος οδήγησης, των τροχαίων παραβάσεων που καταχωρούνται στο Point System κλπ, είναι καταχωρημένα στο **Deep Web.**

- Το σπίτι μας, είτε δικό μας είτε με ενοίκιο, καθώς και το αυτοκίνητο ή η μοτοσυκλέτα μας και η ασφάλεια που πληρώνουμε γι αυτά, είναι καταχωρημένα στο Deep Web.

- Το **ΑΦΜ** μας και το **ΑΜΚΑ** μας, οι φορολογικές μας δηλώσεις, η φορολογική μας ενημερότητα, το ιστορικό της ιατροφαρμακευτικής και νοσοκομειακής μας περίθαλψης, είναι καταχωρημένα στο Deep Web.

- Η Αγγελική Νικολούλη είναι και αυτή καταχωρημένη στο Deep Web, και την βάζουμε και στο σπίτι μας!!

ΚΕΦΑΛΑΙΟ 3: DARK WEB



3.1 : Ορισμός

Το Dark Web (ή αλλιώς Darknet) είναι ένα υποσύνολο του Deep web το οποίο όχι μόνο δεν βρίσκεται από τις κοινές μηχανές αναζήτησης αλλά απαιτεί και κάτι ξεχωριστό για να έχει κανείς πρόσβαση σε αυτό (πχ. Συγκεκριμένο λογισμικό proxying ή έλεγχο ταυτότητας για πρόσβαση). Αντιπροσωπεύει λιγότερο από το 0,01% του web αναφέρει ο ερευνητής ασφαλείας Nick Cubrilovic που μέτρησε λιγότερες από 10.000 κρυμμένες Tor υπηρεσίες σε πρόσφατη ανίχνευση του Σκοτεινού διαδικτύου. Ο αριθμός 10.000 είναι πολύ μικρός, σε σύγκριση με τις εκατοντάδες εκατομμυρίων τακτικών ιστοσελίδων που υπάρχουν στο Deep Web.
Το Dark Web βρίσκεται συχνά πάνω από τα πρόσθετα υποδίκτυα όπως το Tor, I2P και το Freenet και συνδέεται συχνά με εγκληματική δραστηριότητα διαφόρων βαθμών, συμπεριλαμβανομένης της αγοράς και πώλησης ναρκωτικών, πορνογραφίας, τυχερών παιχνιδιών κ.α.

Ενώ το Dark Web σίγουρα χρησιμοποιείται περισσότερο για τέτοιου είδους χρήση (περισσότερο από το κανονικό Internet ή το Deep Web) υπάρχουν και πολλές νόμιμες χρήσεις επίσης.

Παράδειγμα:

Μια πολύ καλή εξήγηση για το τι ακριβώς είναι το Dark Web έχει δημοσιευτεί από τον Daniel Prince, Associate Director Security στο πανεπιστήμιο του Lancaster.

Ο κ.Prince λεει: "Για ένα λεπτό φανταστείτε ότι ολόκληρο το διαδίκτυο είναι ένα δάσος, μια απέραντη έκταση καταπράσινου δάσους για όσο βλέπει το μάτι.
Και υπάρχουν αρκετές καλές διαδρομές για να πάμε από το σημείο Α στο σημείο Β.

Ας θεωρήσουμε ότι αυτές οι διαδρομές είναι οι δημοφιλείς μηχανές αναζήτησης όπως η Google, επιτρέποντάς σας ως χρήστη την επιλογή να βλέπετε το ξύλο από τα δέντρα όταν είστε συνδεδεμένοι. Όμως μακριά από αυτές τις διαδρομές (και μακριά από την Google) τα δέντρα και το δάσος εμποδίζουν την ορατότητά σας. Έξω από αυτά τα μονοπάτια είναι σχεδόν αδύνατο να βρεθεί οτιδήποτε εκτός αν ξέρετε τι ψάχνετε, κάτι σαν το κυνήγι θησαυρού, επειδή πραγματικά ο μόνος τρόπος

να βρείτε κάτι σε αυτό το απέραντο δάσος είναι να σας έχουν πει που ακριβώς να ψάξετε.

Έτσι λειτουργεί και το Dark Web, όπως και το δάσος κρύβει πράγματα καλά, κρύβει πράξεις και ταυτότητες. Επίσης εμποδίζει τους ανθρώπους να γνωρίζουν ποιοι είστε, τι κάνετε και που το κάνετε.

3.2 : Ποιός δημιούργησε το Deep/Dark Web;

Κάποιος θα μπορούσε να υποστηρίξει ότι αφού το διαδίκτυο αρχικά ήταν να χρησιμοποιηθεί από στρατιωτικές και κυβερνητικές οργανώσεις και το διαδίκτυο δημιούργησε τον βαθύ ιστό, τότε επομένως τον βαθύ ιστό τον δημιούργησε η κυβέρνηση.

Ωστόσο το διαδίκτυο ήταν διαθέσιμο για το κοινό αφού η κυβέρνηση των ΗΠΑ είδε την πιθανότητα χρήσης του ARPAnet (η αρχική μορφή και ονομασία του διαδικτύου) στην οικονομία, την γνώση και την επιτήρηση. Το διαδίκτυο δημιούργησε τον βαθύ ιστό ως αποτέλεσμα της επιθυμίας των ανθρώπων να κρύβουν τα πράγματά τους.

Η κυβέρνηση των ΗΠΑ δεν το ήθελε αυτό, ήθελε το ακριβώς αντίθετο οπότε δεν μπορούμε να πούμε να πούμε ότι η κυβέρνηση δημιούργησε τον βαθύ και κατ' επέκταση σκοτεινό ιστό.

Η εκδοχή που υπερέχει είναι πως σπουδαστές από το MIT και το πανεπιστήμιο του Stanford ήταν από τους πρώτους που χρησιμοποίησαν το ARPAnet για τον συντονισμό της πώλησης κάνναβης.

Οπότε θα μπορούσαν να θεωρηθούν οι πρωτεργάτες αυτού που αποκαλούμε deep/dark web.

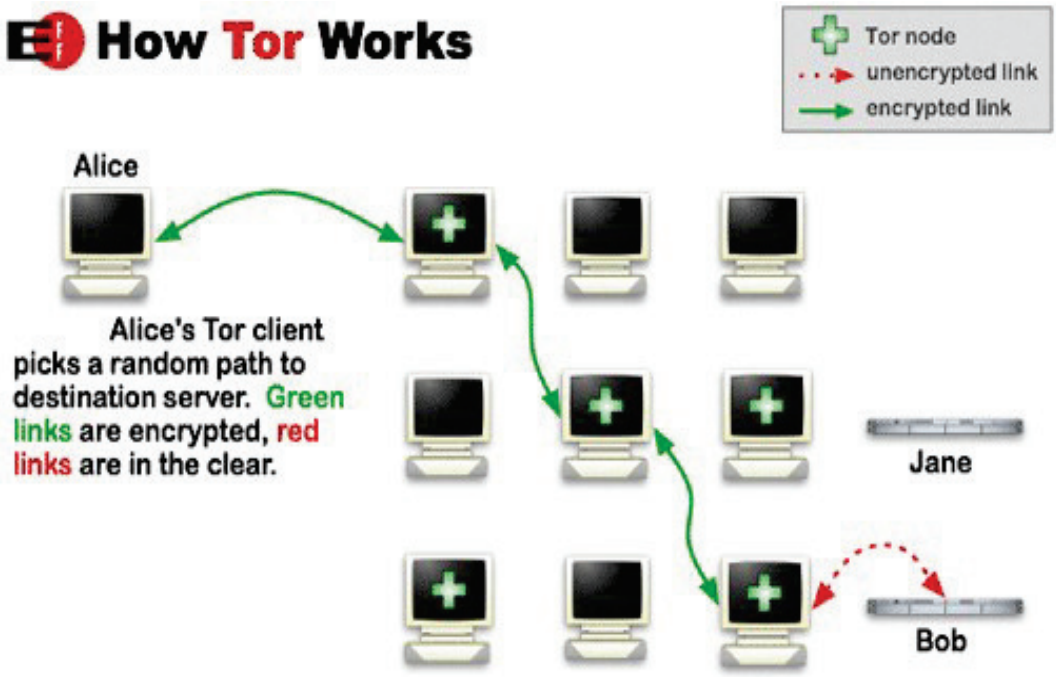
3.3 : Tor

Μπορεί το Deep/Dark web να είναι βαθύ και αφανές αλλά δεν είναι απόρθητο. Το κλειδί για να μπούμε σε αυτό το παράλληλο web είναι το Tor.

Το Tor είναι ένα κρυπτογραφημένο δίκτυο ανωνυμίας με διευθύνσεις που δεν τελειώνουν στα συνηθισμένα .com, .gr, .org αλλά σε .onion και τα περισσότερα δεν έχουν καμία λεκτική συνοχή και είναι και αρκετά μακροσκελή που καθιστά δύσκολη την απομνημόνευση τους. Για να φτάσουμε στην σελίδα προορισμού μας, μας περνάει μέσα από ενδιάμεσους κόμβους (relays) του δικτύου και μας βγάζει από κόμβους εξόδου (exit nodes). Σε αντίθεση με τους proxy server, το exit node δεν γνωρίζει ούτε τη διεύθυνση IP μας ούτε την τοποθεσία μας.

3.3.1 : Πως λειτουργεί;

Το δίκτυο Tor στηρίζεται σε εθελοντές. Χρήστες όπως εγώ και εσείς δέχονται να τρέχουν κόμβους του δικτύου στον υπολογιστή τους είτε ως **relay** είτε ως **exit node**. Όταν θέλουμε να μπούμε σε μια σελίδα μέσω του δικτύου Tor το αίτημά μας περνάει μέσα από τυχαίους κόμβους κρυπτογραφημένο, φτάνει σε ένα κόμβο εξόδου και από εκεί πηγαίνει στην σελίδα προορισμού.
Η σελίδα προορισμού βλέπει μόνο την διεύθυνση του IP του exit node. Με τον τρόπο αυτό ούτε ο ISP (Internet Service provider = υπηρεσία παροχής δικτύου) ούτε κάποιος άλλος μπορεί να συνδέσει την οικιακή μας διεύθυνση IP με την σελίδα προορισμού.
Ακόμα και όσοι τρέχουν τα relays δεν μπορούν να έχουν αυτή την πληροφόρηση καθώς τα δεδομένα είναι κρυπτογραφημένα



Σύμφωνα με την ιστοσελίδα του Tor Project υπάρχουν πολλά είδη ανθρώπων που μπορούν να χρησιμοποιήσουν τον Tor :

- Απλοί χρήστες που θέλουν να προστατέψουν την οικογένεια και τα παιδιά τους.
- Επιχειρήσεις που θέλουν να μελετήσουν τον ανταγωνισμό ανώνυμα και να προστατέψουν τις επιχειρηματικές τους στρατηγικές από τρίτους.
- Άνθρωποι που προσπαθούν να ξεσκεπάσουν τη διαφθορά διατηρώντας την ανωνυμία τους.
- Δημοσιογράφοι που θέλουν να προστατέψουν την έρευνα και τις πηγές τους.
- Στρατιωτικοί και αστυνομικοί οργανισμοί που θέλουν να προστατέψουν τις επικοινωνίες τους, τις έρευνές τους και τις πληροφορίες που συγκεντρώνουν.

Παρ'όλα αυτά, το δίκτυο Tor δεν είναι κατάλληλο για συνεχή χρήση. Λόγω της μεταπήδησης στα relays το browsing γίνεται σημαντικά πιο αργά – η μείωση στην ταχύτητα είναι το τίμημα για την ανωνυμία.

Βέβαια υπάρχει ένα βασικό πρόβλημα που θέλει επισήμανση.
Αν η ιστοσελίδα προορισμού δεν έχει υιοθετήσει το πρωτόκολλο HTTPS (ώστε να είναι κρυπτογραφημένο και το τελευταίο κομμάτι της πληροφορίας ανάμεσα στο exit node και στην ιστοσελίδα) τότε το exit node μπορεί να παρακολουθήσει το traffic που περνάει από αυτό. Για να είναι ένας υπολογιστής exit node χρειάζεται ο κάτοχός του να έχει δώσει άδεια καθώς η διεύθυνση IP που εμφανίζεται στην τελική σελίδα είναι εκείνη του exit node, γεγονός που μπορεί αν τον καταστήσει νομικά υπεύθυνο αν μέσω του δικού του υπολογιστή γίνει κάτι παράνομο ή αξιόποινο.

Για να αποδείξει ότι αυτό μπορεί να συμβεί το 2007 ένας ερευνητής ηλεκτρονικής ασφάλειας κατέγραψε password και email από εκατοντάδες λογαριασμούς τρέχοντας ο ίδιος ένα Tor exit node.
Οι εν λόγω χρήστες έκαναν το λάθος να νομίζουν πως επειδή το δίκτυο Tor είναι κρυπτογραφημένο, δεν υπήρχε λόγος να χρησιμοποιήσουν κρυπτογράφηση στο δικό τους σύστημα email. Όμως αρκεί ένας κρίκος να είναι αδύναμος για να σπάσει η αλυσίδα και αυτός ήταν η σύνδεση ανάμεσα στο exit node και την τελική ιστοσελίδα.
Γι'αυτό όποιος χρησιμοποιεί το δίκτυο Tor καλό είναι να πλοηγείται μόνο σε κρυπτογραφημένες (HTTPS) σελίδες.

3.3.2 : Ασφάλεια

Η ασφάλεια των κρυφών υπηρεσιών Tor ήρθε αντιμέτωπη με έναν εξονυχιστικό έλεγχο που έφερε δεκάδες σκοτεινές σελίδες εκτός σύνδεσης, συμπεριλαμβανομένης μιας μετενσάρκωσης του Silk Road στα τέλη του 2014.
Αυτή η επίθεση που επέτρεψε το κατέβασμα των υποτιθέμενων μη ανιχνεύσιμων ιστοσελίδων, πιστεύεται οτι δημιουργήθηκε από τους ερευνητές ασφαλείας του Carnegie Mellon University και χρησιμοποιούνται από το FBI όπως επίσης και τα αρχεία από τους κρυφούς καταλόγους υπηρεσιών δικτύου.

Οι ερευνητές βρήκαν ένα τρόπο να επισημάνουν την επισκεψιμότητα των κρυφών υπηρεσιών του Tor με ένα μοναδικό κομμάτι δεδομένων που θα μπορούσε να αναγνωριστεί τόσο από τον κόμβο που συνδέθηκε πρώτη φορά (που γνωρίζει την IP της υπηρεσίας), όσο και από την διεύθυνση που παρακολουθείται από τους καταλόγους των κρυφών υπηρεσιών (που γνωρίζουν την .onion διεύθυνση).

Συνδυάζοντας τα δεδομένα από τους 2 αυτούς υπολογιστές η αστυνομία διέθετε αρκετές πληροφορίες για να εντοπίσει τις τοποθεσίες των διακομιστών που τρέχουν τους παράνομους ιστότοπους και να τους κατασχέσει.

Το κενό βέβαια αυτό στην ασφάλεια καλύφθηκε γρήγορα με αποτέλεσμα τα πού σκοτεινά σημεία του διαδικτύου πράγμα που γεννά ένα αναπόφευκτο ερώτημα: Οι άγνωστες κρυφές υπηρεσίες θα γίνουν πόλος έλξης για τα χειρότερα μέρη του διαδικτύου συμπεριλαμβανομένων των αγορών κλεμμένων δεδομένων, εργαλείων hacking ή παιδικής πορνογραφίας;;

Ο συνιδρυτής του Tor Project Nick Mathewson μας δίνει την απάντηση που αυτός και μεγάλο μέρος του κόσμου της κρυπτογράφησης πιστεύουν: Ότι τα ισχυρά εργαλεία προστασίας της ιδιωτικής ζωής προσφέρουν ένα κοινωνικό εμπόριο και αυτό που αξίζει να γίνει. Αν ο μόνος τρόπος για να διασφαλίσουμε ότι οι κοινωνικά βλαβερές χρήσεις του διαδικτύου είναι ανασφαλείς, είναι να κάνουμε τους πάντες ανασφαλείς, δεν εμπνέει και πολύ σιγουριά.

Η ανθρωπότητα αξίζει την ιδιωτικότητα και είναι καλύτερα με αυτήν παρά χωρίς αυτήν αν και μερικά πράγματα που κάνουν οι άνθρωποι με αυτήν χρειάζονται έλεγχο.

3.3.3 : Αναβάθμιση Εργαλείων Tor

Ιστότοποι στο επονομαζόμενο σκοτεινό ιστό ή δίκτυο λειτουργούν κάτω από ένα παράδοξο ιδιωτικότητας. Ενώ όποιος γνωρίζει μία διεύθυνση σκοτεινού ιστότοπου μπορεί να την επισκεφτεί, κανείς δεν μπορεί να καταλάβει ποιος φιλοξενεί αυτόν τον ιστότοπο ή που. Κρύβεται από τα κοινά βλέμματα. Αλλά οι αλλαγές που έρχονται στα εργαλεία ανωνυμίας υπόσχονται να καταστεί δυνατή μια νέα μορφή διαδικτυακής ιδιωτικότητας.
Σύντομα οποιοσδήποτε θα μπορεί να δημιουργήσει την δική του "γωνιά" στο internet που δεν θα είναι απλά ανώνυμη και μη ανιχνεύσιμη, αλλά εντελώς αθέατη χωρίς πρόσκληση.

Τους επόμενους μήνες το μη κερδοσκοπικό πρόγραμμα Tor θα αναβαθμίσει την ασφάλειά και το απόρρητο των αποκαλούμενων "υπηρεσιών κρεμμυδιού" ή "κρυφών υπηρεσιών" που επιτρέπουν την ανωνυμία του σκοτεινού δικτύου.

Ενώ η πλειοψηφία των ανθρώπων που χρησιμοποιούν το λογισμικό του Tor Project το κάνουν για την ανώνυμη περιήγηση στον ιστό και την παράβλεψη της λογοκρισίας σε χώρες όπως το Ιράν και η Κίνα, η ομάδα διατηρεί επίσης κώδικα που επιτρέπει σε οποιονδήποτε να φιλοξενήσει έναν ανώνυμο ιστότοπο ή διακομιστή.

Αυτός ο κώδικας αναβαθμίζεται τώρα ώστε να κυκλοφορήσει σχεδιασμένος τόσο για να ενισχύσει την κρυπτογράφησή του, όσο και για να επιτρέψει στους διαχειριστές να δημιουργήσουν εύκολα πλήρως μυστικές τοποθεσίες που θα μπορούν να ανακαλυφθούν μόνο από εκείνους που γνωρίζουν μια μεγάλη σειρά απρόβλεπτων χαρακτήρων.

Αυτά τα tweaks λογισμικού αναφέρει ο Mathewson θα μπορούσαν όχι μόνο να επιτρέψουν την αυστηρότερη προστασία της ιδιωτικής ζωής στο darknet, αλλά και να χρησιμεύσουν ως βάση για μια νέα γενιά κρυπτογράφησης. Όπως αναφέρει: "Κάποιος θα μπορεί να δημιουργήσει μια κρυφή υπηρεσία μόνο για σας, που μόνο εσείς θα γνωρίζετε και η προστασία της συγκεκριμένης υπηρεσίας θα είναι μη ανακαλύψημη. Ως δομικό στοιχείο αυτό θα παρέχει μια πολύ πιο ισχυρή βάση για πιο ασφαλή και ιδιωτικά συστήματα απ'ότι είχαμε πριν."

3.3.4 : Κατάλογοι Ευρυτηρίασης Tor

Οι περισσότερες τοποθεσίες σκοτεινού διαδικτύου σήμερα κοινοποιούν δημόσια τις διαδικτυακές τους διευθύνσεις στο κανονικό διαδίκτυο και τα κοινωνικά μέσα ενημέρωσης για πιθανούς επισκέπτες. Οποιοσδήποτε πληροφοριοδότης μπορεί να επισκεφτεί το ανώνυμο σύστημα ανάρτησης του Wikileaks πχ επικολλώντας το wlupld3ptjvsgwqw.onion στο Tor και πολλές χιλιάδες πελάτες και έμποροι φαρμάκων επίσης ήξεραν ότι μπορούσαν να βρουν την περίφημη σκούρα διαδικτυακή αγορά φαρμάκων στο Silk Road από το silkroadvbpp3.onion πριν το FBI το "κατεβάσει" εκτός σύνδεσης.

Αλλά ακόμη και χωρίς να γνωρίζει τη διεύθυνση της κρυμμένης υπηρεσίας Tor ένα άλλο τέχνασμα επέτρεψε να ανακαλυφθούν τα snoops, οι επιχειρήσεις ασφαλείας, οι hackers και οι αρχές επιβολής του νόμου.

Αυτό έγινε από τους υπολογιστές των εθελοντών που χρησιμοποιούνταν ως κόμβοι ανακατεύθυνσης σε όλο τον κόσμο. Ο κάθε ένας μπορεί να προσφέρει τον υπολογιστή του ως ένα συγκεκριμένο είδος κόμβου, έναν από τους χιλιάδες από τους κρυφούς καταλόγους υπηρεσιών, που δρομολογούν τους επισκέπτες σε μια συγκεκριμένη κρυφή υπηρεσία.

Για να δουλέψει το συγκεκριμένο σύστημα δρομολόγησης όλες οι κρυμμένες υπηρεσίες πρέπει να δηλώσουν πρέπει να δηλώσουν την ύπαρξή τους σε εκείνους τους καταλόγους. Μια μελέτη που δημοσιεύθηκε στην διάσκεψη για hacker στο Defcon πέρυσι έδειξε ότι περισσότεροι απο 100 απο τους 3000 κρυφούς καταλόγους υπηρεσιών μυστικά διέδιδαν όποια διεύθυνση μάθαιναν, με σκοπό να αποκαλυφθούν οι άγνωστες περιοχές του Dark Web.

Η επόμενη γενιά κρυφών υπηρεσιών θα χρησιμοποιεί μια έξυπνη μέθοδο για την προστασία της μυστικότητας αυτών των διευθύνσεων.
Αντί να δηλώσουν την διεύθυνσή τους xxxx.onion σε κρυφό κατάλογο υπηρεσιών, θα αντλούν ένα μοναδικό κρυπτογραφικό κλειδί από αυτή τη διεύθυνση και θα δώσουν αυτό το κλειδί στους κρυφούς καταλόγους υπηρεσίας του Tor. Όμως ο κρυμμένος κατάλογος υπηρεσίας δεν μπορεί να εξάγει την διεύθυνση .onion από το κλειδί, εμποδίζοντας όσους ψάχνουν να ανακαλύψουν οποιαδήποτε μυστική διεύθυνση darknet.

"Το δίκτυο Tor δεν πρόκειται να σας δώσει τον τρόπο για να μάθετε μια διεύθυνση κρεμμυδιού που δεν γνωρίζετε ήδη" λέει ο Mathewson.

Αποτέλεσμα:

Το αποτέλεσμα λέει ο Mathewson θα είναι σκοτεινοί χώροι με νέες πιο σίγουρες εφαρμογές.
Θα μπορούσε ο καθένας να φιλοξενήσει μια κρυφή υπηρεσία στον δικό του υπολογιστή δημιουργώντας έναν τρόπο να συνδεθεί εύκολα από οπουδήποτε στον κόσμο, διατηρώντας παράλληλα την ύπαρξή του μυστική από snoops.
Η επόμενη γενιά κρυφών υπηρεσιών θα αλλάξει από τη χρήση κλειδιών κρυπτογράφησης 1024-bit RSA σε κλειδιά ελλειπτικής καμπύλης ED-25519 μικρότερα μεν αλλά πιο δύσκολο να σπάσουν. Και οι αλλαγές των κρυφών καταλόγων υπηρεσίας σημαίνουν ότι τα urls των κρυφών υπηρεσιών θα αλλάξουν από 16 σε 50 χαρακτήρες.
Παρ' όλα αυτά ο Mathewson υποστηρίζει ότι η αλλαγή δεν επηρεάζει την χρηστικότητα των διευθύνσεων του Dark Web καθώς ήταν ήδη πολύ μεγάλα για να τα αποστηθίσουν.

Λίστα με χρήσιμες διευθύνσεις και αγορές

Για να κατεβάσετε το Tor & Browser (leaves no trace):
https://www.torproject.org/projects/torbrowser.html.en

Για να βρείτε χρήσιμα links:
http://en.wikipedia.org/wiki/.onion#Onion_Sites

Για να μπείτε στο Hidden Wiki που πρακτικά μπορείτε να βρείτε τα πάντα:
http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page

Directory/list of links:
http://dppmfxaacucguzpc.onion/

Οι 5 μεγαλύτερες αγορές:

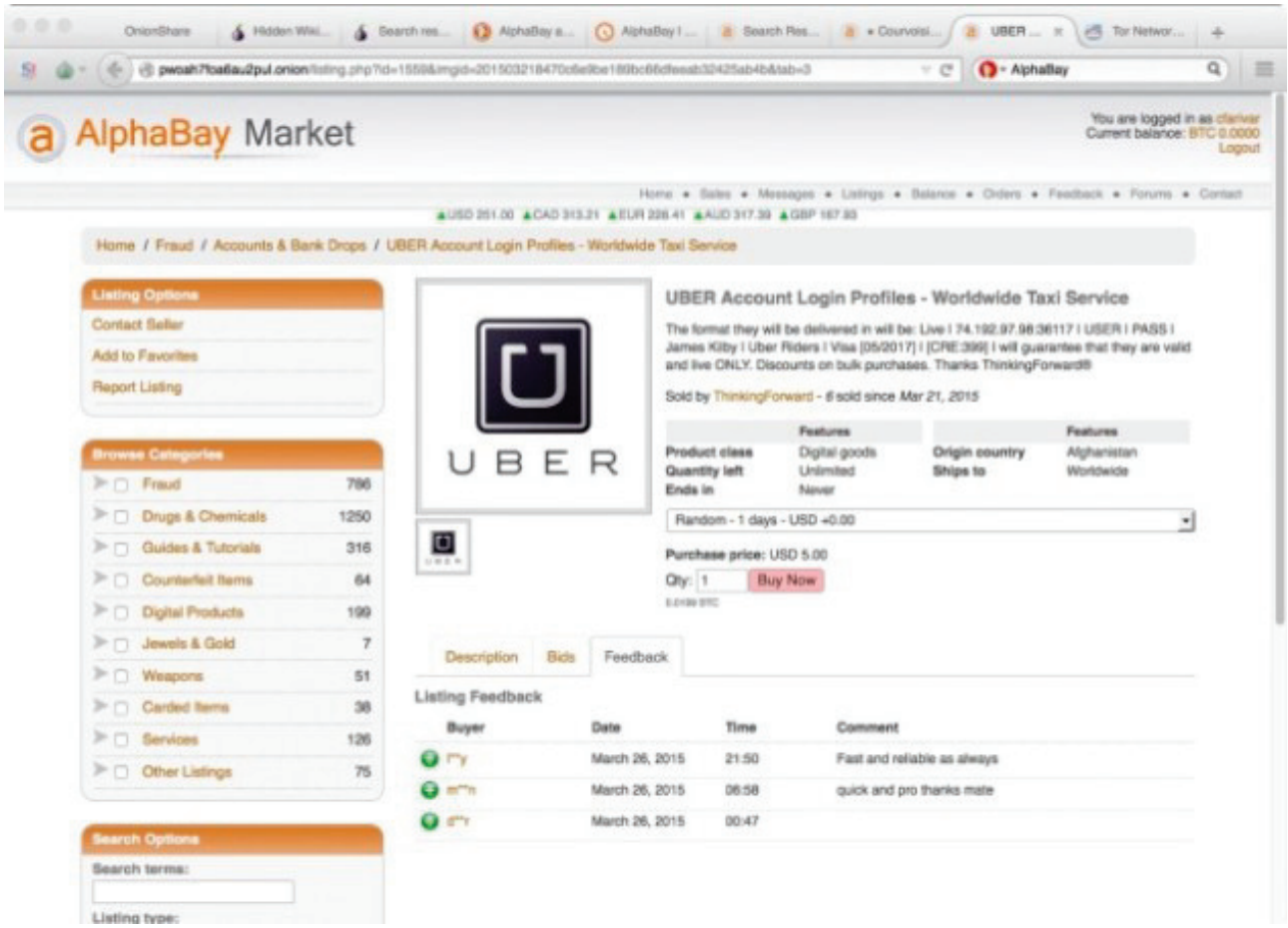
I. *Alphabay*

II. *Dream Market*

III. *Silk Road 3*

IV. *Crypto Market*

V. *Hansa*



AlphaBay Market site

3.4 : Το Dark Web σαν εργαλείο για πολιτικές επιθέσεις

Σε πρόσφατους τίτλους, το dark web έχει αναγνωριστεί ως η δίοδος μέσω της οποίας πραγματοποιούνται πολιτικές επιθέσεις. Λόγω του ανώνυμου και σκοτεινού χαρακτήρα του το dark web είναι ένας δημοφιλής κόμβος για τους εγκληματίες του κυβερνοχώρου και τους hacker για να πραγματοποιήσουν το παράνομο εμπόριο τους χωρίς να ανησυχούν για την παρακολούθηση τους από υπηρεσίες επιβολής νόμου και παρόμοιους φορείς.

Αυτό το σε μεγάλο βαθμό ανώνυμο δίκτυο βρίσκεται στο επίκεντρο ενός από τα μεγαλύτερα πολιτικά σκάνδαλα που έχουν ξεσπάσει στις ΗΠΑ τα τελευταία χρόνια Ένας άγνωστος χρήστης του Dark Web με το ψευδώνυμο "Guccifer 2.0" θεωρήθηκε υπεύθυνος για την διαρροή ευαίσθητων πληροφοριών από τη Δημοκρατική Εθνική Επιτροπή, οι οποίες αργότερα δημοσιεύθηκαν στο Wikileaks και υπήρξαν βάσιμοι ισχυρισμοί ότι η Ρώσικη κυβέρνηση έπαιξε ρόλο στη διαρροή των πληροφοριών.

Ο σκοτεινός ιστός φαίνεται να εκμεταλλεύτηκε και τις τελευταίες εκλογές των ΗΠΑ. Μετά την νίκη του Donald Trump έγινε μια κίνηση από ένα τμήμα των χρηστών για να οργανώσει έρανο για να διευκολύνει την δολοφονία του μαζί με τον αντιπρόεδρο Mike Pence. Όλα αυτά οργανώνονταν μέσω ανώνυμων καναλιών.

Περισσότεροι άνθρωποι ενδιαφέρονται γι αυτό το ανώνυμο τμήμα του διαδικτύου και ο αριθμός αναμένεται να αυξηθεί στο προσεχές μέλλον.
Αυτό αποτελεί πρόκληση για τις υπηρεσίες επιβολής του νόμου που προσπαθούν να παρακολουθήσουν τις δραστηριότητες των χρηστών που εκδίδουν τώρα πολιτικές απειλές μεταξύ της διευκόλυνσης άλλων εγκλημάτων.

Αυτό έχει ως αποτέλεσμα να αναδύονται πολλές εταιρίες με λύσεις που θα μπορούσαν να μειώσουν αυτές τις πολιτικές απειλές.
Ένα παράδειγμα μιας τέτοιας εταιρίας αποτελεί η Sixgill, μια Ισραηλινή εταιρία που ασχολείται κυρίως με τον εντοπισμό και τον έλεγχο των ψηφιακών κινδύνων ασφαλείας.
Η Sixgill αποτελείται από μια ομάδα πρώην Ισραηλινών μυστικών υπηρεσιών που ισχυρίζονται ότι διαθέτουν την απαραίτητη τεχνογνωσία για να ανακαλύψουν και ακόμη να αποτρέψουν τυχόν διαρροές δεδομένων σε σκοτεινές πλατφόρμες πριν συμβούν.

3.5 : Το Dark Web στον πόλεμο του ISIS

Έχει γίνει γνωστό ότι λίγα μέρη είναι τόσο ανοιχτά στην εγκληματική δραστηριότητα όπως το Dark Web. Τα ναρκωτικά, τα όπλα και οι υπηρεσίες εκτελεστών διαφημίζονται ανοιχτά και μπορούν να πληρωθούν μέσω ανώνυμης κρυπτογράφησης bitcoin. Έτσι έχει γίνει ο παράδεισος για το οργανωμένο έγκλημα και τις πιο διάσημες τρομοκρατικές οργανώσεις του κόσμου.
Κατά τη διάρκεια των τελευταίων χρόνων το ISIS έχει αυξηθεί ραγδαία σε αριθμό. Βίντεο με ψυχρές εκτελέσεις τους έχουν κάνει τον γύρο του διαδικτύου τρομοκρατώντας εκατομμύρια ανθρώπων σε όλο τον κόσμο, καθώς έχουν αποδειχτεί ασύλληπτοι με δεδομένο ότι ένας ολόκληρος συνασπισμός εθνών είχε ελάχιστη επιτυχία στην ανίχνευσή τους.
Η περίπτωση του ISIS είναι πολύ περίεργη καθώς έχουν ανοιχτούς πολέμους σε πολλαπλά μέτωπα σε 5 χώρες σε 2 ηπείρους. Μεσολαβούν πάνω από 500χμ μεταξύ των δραστηριοτήτων τους στην Συρία και τη Νιγηρία και πολλοί αναρωτιούνται πως είναι δυνατόν να έρχονται σε επαφή μεταξύ τους χωρίς να αποκαλύπτονται.

Η απάντηση είναι το Dark Web

Το ISIS χρησιμοποίησε για πρώτη φορά και σε κάποιο βαθμό εξακολουθεί να χρησιμοποιεί τα social media για να προσεγγίσει υποψήφιους τζιχαντιστές, ωστόσο τώρα εστιάζουν την προσοχή τους στο Deep/Dark Web όπου αναζητούν δωρεές ανώνυμα καθώς οι συναλλαγές τους γίνονται με bitcoin.

Ο καθηγητής του Colorando Springs University Edin Mujick αναφέρει:
"Ακόμα και αν υποθετικά το ISIS καταστραφεί μέσα στον επόμενο έτος, αυτό δεν εγγυάται ότι κάποια άλλη ομάδα δεν πρόκειται να εμφανιστεί και να χρησιμοποιήσει την ίδια τακτική αφού έμαθε από αυτούς."

3.5.1 : Νέοι τρόποι ευρετηρίασης

Πώς όμως μπορεί να περιοριστεί αυτή η πρόσφυση;

Το DARPA (Defense Advance Research Projects Agency) της κυβέρνησης των ΗΠΑ, ανακοίνωσε την προσπάθεια δημιουργίας μιας νέας μηχανής αναζήτησης (MEMEX) που θα επιτρέπει την καλύτερη ευρετηρίαση των ιστότοπων του Deep Web.
Ο δημιουργός της μηχανής αναζήτησης Chris White εξήγησε πως λειτουργεί η νέα μηχανή αναζήτησης και πως θα μπορούσε να φέρει την επανάσταση στις έρευνες επιβολής του νόμου.

Το Memex μας επιτρέπει να χαρακτηρίσουμε πόσες ιστοσελίδες υπάρχουν και τι είδους περιεχόμενο υπάρχει πάνω τους.
Το γεγονός ότι η Microsoft τα τελευταία χρόνια κάνει σοβαρές κινήσεις για την δημιουργία μιας νέας τεχνολογίας στην αναζήτηση, θα έπρεπε να αρκεί για να κρατήσει τις υπόλοιπες μηχανές αναζήτησης σε εγρήγορση. Είναι βασικό οι μηχανές αναζήτησης να επεκταθούν και στο Deep Web ώστε να μπορούν να δίνουν ολοκληρωμένες απαντήσεις στους χρήστες και να συμπεριληφθούν τα αποτελέσματα από αρχεία εικόνων, βίντεο και ήχου.
Παρόλο που η παρεμπόδιση του ISIS να έχει μια τέτοια ελεύθερη επιρροή στο Deep Web δεν είναι εύκολη υπόθεση, ούτε θα είναι το τέλος της τρομοκρατικής οργάνωσης, είναι ένα πολύ επιθετικό πρώτο βήμα και στέλνει ένα ισχυρό μήνυμα.

3.6 : Υπηρεσίες εκδίκησης

Μια λίστα που ανήκει σε έναν πωλητή του Dark Web με το ψευδώνυμο "Etimbuk" έχει κάνει αίσθηση τον τελευταίο καιρό.
Αυτό που ο συγκεκριμένος πωλητής πωλεί ξεχωρίζει από τις συγκεκριμένες λίστες darknet σε σημαντικό βαθμό. Για 700$ ο Etimbuk προσφέρει σε εκείνου που επιθυμούν να αγοράσουν τις υπηρεσίες του την ευκαιρία να πάρουν εκδίκηση από όποιον τους έχει πειράξει.

Όσο παράξενο και αν φαίνεται ο κατάλογος συνεχίζεται, εξηγώντας ότι η πράξη εκδίκησης μπορεί να πραγματοποιηθεί σε έναν πρώην εραστή, έναν γείτονα, έναν προϊστάμενο, έναν συνεργάτη, κάποιο μέλος της οικογένειας ή γενικότερα σε "κάποιον που μισούν".
Πέρα από αυτό υπάρχει μια σημαντική έλλειψη πληροφοριών ως προς το είδος της εκδίκησης και στο πόσο μακριά μπορεί να φτάσει ο πωλητής ώστε να ικανοποιήσει τις ανάγκες των πελατών του.

Πηγαίνοντας στην ίδια την λίστα φαίνεται ότι ο Etimbuk αντιπροσωπεύει μια μεγαλύτερη ομάδα ανθρώπων χρησιμοποιώντας συστηματικά την αντωνυμία "εμείς" όταν μιλάει για τις υπηρεσίες. Ο Etimbuk επισημαίνει επίσης ότι οι υπηρεσίες εκδίκησης προσφέρονται "ανώνυμα και νόμιμα" μια προκλητική δήλωση λαμβάνοντας υπόψη τη νομιμότητα της βλάβης των άλλων για χάρη της εκδίκησης.
Τα βασικά σημεία πώλησης αυτής της υπηρεσίας τονίζουν ότι οι πελάτες δεν θα συμμετέχουν σε καμία από τις "βρώμικες" εργασίες και δεν θα συνδέονται με τα εγκλήματα αν τα πράγματα πάρουν άσχημη τροπή.

```
Grim

If you need someone killed you've come to the right place.

Standard asking price is 5,000.00 USD$ paid in Bitcoin.
Other factors will increase the fee, here are some of them.
-Political Targets  +8,000$ (No major figures)
-Law Enforcement    +3,000$
-Pictures           +1,000$
-Extended Suffering +5,000$

Want someone to suffer? I can make them suffer. Need to make an example? It can be arranged.
I require half payment before completion and the rest to be paid upon completion.

I am currently accepting contracts from North and South America.

For me to eliminate someone I need their name, age, address, description and a photo.
Additional details such as habits, pets, and tendancies are helpful but not required.
It can take 2-4 weeks to complete a hit.
```

Υποτιθέμενος κατάλογος πληρωμένου δολοφόνου που αναλύει διεξοδικά τις υπηρεσίες του

Ακόμα μια μεγάλη σελίδα είναι η "Hitman Network" και όταν ο ενδιαφερόμενος γράψει ποιο ακριβώς είναι το πρόβλημα που θα ήθελε να "εξαφανίσει", η σελίδα ενεργοποιεί τρεις δολοφόνους προκειμένου να εκτελέσει την αγγελία αρκεί ο στόχος, όπως ενημερώνει, να μην είναι πολιτικός ή άτομα κάτω των 16 ετών. Η σελίδα παρέχει και έκπτωση 1% στους χρήστες που θα τη διαφημίσουν καθώς μήνυμα της αναφέρει χαρακτηριστικά: "Tell others about this shop, and earn 1% from every purchase they will make".

Ειδικό στη πρόσληψη δολοφόνων θεωρείται το δίκτυο Assassination Market. Εδώ το όνομα του στόχου προστίθεται σε μια λίστα με ονόματα και στη συνέχεια οι χρήστες χρησιμοποιούν bitcoins προκειμένου να χρηματοδοτήσουν τη δολοφονία. Ανάμεσα στα ονόματα της λίστας θα βρούμε τον πρώην διευθυντή της NSA, Keith Alexander, τον πρώην Αμερικάνο πρόεδρο Barack Obama και τον πρόεδρο της Federal Reserve, Ben Bernanke που έχει πλειοδοτηθεί με το ποσό των 75.000 δολαρίων (124.14 bitcoins).
Ο δημιουργός της σελίδας κυκλοφορεί με το ψευδώνυμο Kuwabatake Sanjuro και όπως ο ίδιος έχει αποκαλύψει μέσα από τα forums συζήτησης, φιλοδοξία του είναι η ανατροπή των κυβερνήσεων.

Πως όμως ο δολοφόνος αποδεικνύει ότι έκανε τη προβλεπόμενη δολοφονία;;
Πριν από κάθε δολοφονία, ο εκάστοτε πληρωμένος δολοφόνος δημιουργεί ένα αρχείο κειμένου με την προβλεπόμενη ημερομηνία του θανάτου. Στη συνέχεια χρησιμοποιεί μια κρυπτογραφική λειτουργία γνωστή ως hash, για να μετατρέψει το αρχείο κειμένου σε μία μοναδική σειρά χαρακτήρων.
Πριν από τη δολοφονία επίσης, κάθε δολοφόνος ενσωματώνει τα στοιχεία του σε ένα λογαριασμό bitcoin όπου γίνεται η πληρωμή του. Όταν ο στόχος του δολοφόνου είναι νεκρός, στέλνει το αρχείο κειμένου στον Sanjuro, ο οποίος χρησιμοποιεί τα hashes για να βεβαιωθεί ότι τα αποτελέσματα ταιριάζουν με τον κωδικό που αποστέλλεται πριν από το θάνατο του στόχου.
Ο Sanjuro κρατάει προμήθεια 1% για κάθε δολοφονία.

Πως μπορούμε όμως να καταλάβουμε τις απάτες;

Η πώληση ναρκωτικών, όπλων, παιδικής πορνογραφίας και κακόβουλου λογισμικού είναι μερικοί από τους τρόπους με τους οποίους οι εγκληματίες του κυβερνοχώρου παρουσιάζονται σε διάφορες darknet αγορές ενός λαβύρινθου από κρυπτογραφημένους ιστότοπους. Ωστόσο οι απατεώνες έχουν επίσης μια κυρίαρχη παρουσία για προφανείς λόγους.

Πέρυσι, ένας hacker αποκάλυψε ότι το darknet site Besa Mafia, ένας χώρος που φαινομενικά προσελάμβανες εκτελεστές, δεν ήταν παρά μια περίτεχνη οργάνωση για να αποσπά χιλιάδες δολάρια προσφέροντας σε "πελάτες" υπηρεσίες εκτελέσεων που δεν υπήρχαν.

Εκτός λοιπόν από την έλλειψη σωστής γραμματικής (συνήθως ένα προειδοποιητικό σημάδι ότι μια προσφορά είναι απάτη) δεν υπάρχει κανένας τρόπος να επαληθευτεί η νομιμότητα των υπηρεσιών που προσφέρονται. Φυσικά πολλές φορές η αστυνομία μεταμφιέζεται ως εγκληματίας για να τους παρασύρει σε ατασταλίες έως ότου συγκεντρωθούν αρκετά στοιχεία για την δίωξη.

Για άλλη μια φορά η έλλειψη μεθόδων επαλήθευσης στον σκοτεινό ιστό καθιστά αδύνατο να αποκλείσουμε αυτό το ενδεχόμενο.

3.7 : Παιδική πορνογραφία

Το τέχνασμα του FBI που αποτέλεσε πόλο έλξης για πολλούς παιδόφιλους ανά τον κόσμο έγινε ευρέως γνωστό.
Τον Φεβρουάριο του 2015 οι αστυνομικοί συνεργάστηκαν με την ίδια υπηρεσία που είχε καταλάβει έναν ιστότοπο που ονομαζόταν **"Playpen"** και εξακολουθούσαν να είναι ενεργοί μέσω των διακομιστών της ίδιας της υπηρεσίας για περίπου 2 εβδομάδες.
Κατά τη διάρκεια αυτής της περιόδου, η υπηρεσία ανέφερε ότι χρησιμοποίησε ένα εργαλείο hacking για να εντοπίσει περίπου 1300 IP διευθύνσεις χρηστών απ' όλο τον κόσμο και να μετρήσει περίπου 215.000 εγγεγραμμένους χρήστες.
Με βάση τις ομοσπονδιακές αναφορές, ο Playpen ήταν ο μεγαλύτερος ιστοχώρος παιδικής πορνογραφίας στον σκοτεινό ιστό, μεγαλύτερος από οποιονδήποτε αυτού του είδους.

Παρόμοια κινήθηκαν οι αμερικάνικες αρχές πριν μερικούς μήνες όταν εξάρθρωσαν ένα διεθνές δίκτυο παιδικής πορνογραφίας με 27.000 συνδρομητές απ' όλο τον κόσμο. 14 άτομα συνελήφθησαν με την κατηγορία της εκμετάλλευσης ανηλίκων σε σχέση με μια ιστοσελίδα που λειτουργούσε στο Deep Web.
Ως διαχειριστής και αρχηγός της εμφανίζεται ο 27χρονος Jonathan Johnson ο οποίος αντιμετωπίζει 20ετή ποινή κάθειρξης. Το δίκτυο λειτουργούσε από τον Ιούνιο του 2012 μέχρι τον Ιούνιο του 2013.
Όπως ανακοίνωσαν οι αρχές η ιστοσελίδα διέθετε αρχεία με περισσότερα από 2.000 βίντεο και ακόμη περισσότερες φωτογραφίες από 250 παιδιά κυρίως αγόρια.
Οι ηλικίες ήταν από 3 έως 17 χρονών και προέρχονταν από 39 αμερικάνικες πολιτείες. Εκδόθηκαν περίπου 150 εντάλματα σύλληψης εναντίων υπόπτων στις ΗΠΑ και άλλα 150 σε άλλες χώρες.

Συμμέτοχοι σε άλλη μια προσπάθεια ήταν και η γνωστή ομάδα hackers **Anonymous** όταν με την επιχείρηση "Operation_Darknet" το 2011 που είχε ως στόχο site παιδικής πορνογραφίας, κατάφεραν να εντοπίσουν την εταιρία hosting στην οποία ήταν ανεβασμένα πάνω από 100 GB πορνογραφικού υλικού δίνοντας στην δημοσιότητα πάνω από 1500 ονόματα μελών της.
Οι Anonymous παρακολουθούσαν αρκετό καιρό την κίνηση του ιστότοπου "Lolita City" γνωστό στους κύκλους των παιδόφιλων το οποίο μάλιστα χρησιμοποιούσε ειδικό software ώστε να κρύβει τις IP διευθύνσεις των χρηστών του.
Τα μέλη της ομάδας ζήτησαν από την εταιρία hosting "Freedom Hosting" να κατεβάσει το συγκεκριμένο site όμως αυτοί αρνήθηκαν, κι έτσι οι Anonymous μπλόκαραν τους servers τους μέσω μιας τεράστιας επίθεσης Ddos.

3.8 : Μυστικές υπηρεσίες

Τον Αύγουστο του 2013, λίγα μόνο εικοσιτετράωρα μετά την ανακοίνωση ότι δόθηκε βίζα στον E.Snowden (γνωστός για τις αποκαλύψεις του περί παρακολουθήσεων, αποκαλύψεις που αρχικά είχαν διαρρεύσει στο Darknet), το FBI ανακοίνωσε ότι απέκτησε πρόσβαση τουλάχιστον στα μισά ανώνυμα sites του δικτύου, συμπεριλαμβανομένου του απόκρυφου συστήματος ασφαλούς, κρυπτογραφημένης ανταλλαγής email, TORmail.
Λέγεται, πως πριν εξαφανιστούν από το διαδίκτυο τα sites αυτά αλλά και άλλα πολλά "διέδιδαν" κακόβουλο λογισμικό που μπορεί να χρησιμοποιήθηκε για την έκθεση των χρηστών και τέλος της ανωνυμίας στο διαδίκτυο.

Την ίδια ώρα, δύο μυστηριώδεις θάνατοι ίσως και να σχετίζονται με την προσπάθεια των μυστικών υπηρεσιών να διεισδύσουν και να ελέγξουν το σκοτεινό χώρο του Deep Web.
Τα δύο πρόσωπα αυτά είναι ο hacker Barnaby Jack και ο δημοσιογράφος Michael Hastings.

Ο 35χρονος Barnaby Jack, ειδικός σε θέματα ασφάλειας πληροφοριών βρέθηκε νεκρός στο διαμέρισμα του στο San Francisco τον Ιούλιο του 2013, λίγο πριν την παρουσίασή του στο συνέδριο Black Hat 2013 που αφορούσε το hacking εξ αποστάσεως ιατρικών συσκευών, όπως τις αντλίες ινσουλίνης και τους βηματοδότες. Η ιατροδικαστική έκθεση που παρουσιάστηκε τον Ιανουάριο του 2014 δείχνει ότι ο hacker πέθανε από υπερβολική δόση κοκαΐνης, ηρωίνης και διφαινυδραμίνης διαψεύδοντας τους συνομωσιολόγους που έλεγαν ότι στον παράξενο θάνατό του ενεπλάκη η CIA.
Βέβαια, αρκετοί είναι εκείνοι που υποστηρίζουν ότι τα αίτια θανάτου του συγκαλύφτηκαν.
Πολλοί είναι εκείνοι που θα κέρδιζαν αν ο Barnaby Jack σταματούσε να μιλά όπως οι εταιρίες ιατρικών υλικών, τρομοκράτες ακόμα και η ίδια η κυβέρνηση των ΗΠΑ που είχε ξεκινήσει ένα κυνήγι εναντίων όλων εκείνων που "σπάνε" τα συστήματα και είναι ειδικοί στον χώρο του διαδικτύου καθώς δεν θα ήθελε με τίποτα να δει μια δεύτερη υπόθεση Snowden στην επικαιρότητα.

Στην δεύτερη περίπτωση, αυτή του 33χρονου Hastings, πρώην δημοσιογράφος του Rolling Stone, χρήζει ιδιαίτερης αναφοράς το γεγονός ότι ο ίδιος είχε εκμυστηρευτεί στους συνεργάτες του πως υποψιαζόταν ότι ήταν αντικείμενο έρευνας από το FBI. Και αυτό λίγες μόλις ώρες πριν σκοτωθεί σε ένα αυτοκινητιστικό δυστύχημα στο L.A όταν το αυτοκίνητό του προσέκρουσε με μεγάλη ταχύτητα σε ένα δέντρο, με αποτέλεσμα να εκραγεί. Υπάρχουν όμως κάποιες μαρτυρίες από αυτόπτες μάρτυρες που ισχυρίζονται πώς το αυτοκίνητό του εξερράγη πριν από την πρόσκρουση.

Ο Hastings υπήρξε ανταποκριτής στην εμπόλεμη ζώνη του Αφγανιστάν και του Ιράκ και όταν έγινε το ατύχημα ερευνούσε μια πολύ μεγάλη είδηση ενώ είχε έρθει και σε επαφή με τους δικηγόρους του Wikileaks.

3.9 : Η Φωτεινή Πλευρά Του Darknet

Μπορεί το Darknet να έρχεται στην επικαιρότητα συνήθως με αφορμή αστυνομικές επιχειρήσεις που έχουν στο στόχαστρο "μαύρες αγορές" όπως το Silk Road, ωστόσο αυτό δεν σημαίνει είναι ότι βλέπουμε online ανάλογο του πραγματικού κόσμου.

"Το σκοτεινό διαδίκτυο έχει και μία εξαιρετικά σημαντική "φωτεινή" πλευρά, εξασφαλίζοντας την ελευθερία της έκφρασης σε ανθρώπους που ζουν σε απολυταρχικά καθεστώτα και βοηθώντας να έρθουν στο φως συνταρακτικά ντοκουμέντα, χωρίς τον φόβο όσων τα διέρρευσαν πως θα διωχθούν ποινικά" σημειώνει ο Brad Chacos από το περιοδικό PC World.

Ενδεικτικά, στο Darknet έχουν κατά καιρούς φιλοξενηθεί αντίγραφα του Global Leaks και του Wikileaks, ενώ το περιοδικό New Yorker έχει δημιουργήσει το Strongbox, μια υπηρεσία στο σκοτεινό διαδίκτυο που εγγυάται ανωνυμία σε όσους θελήσουν να επικοινωνήσουν με τους συντάκτες του με μεγαλύτερη ασφάλεια από αυτή των ηλεκτρονικών ταχυδρομίων.
Επίσης η οργάνωση "Δημοσιογράφοι Χωρίς Σύνορα" συμβουλεύει τα μέλη της να το χρησιμοποιούν για να έρχονται σε επαφή με τις πηγές τους, σε περίπτωση που θέλουν να διασφαλίσουν πως θα μείνει μυστική η ταυτότητα όσων επικοινωνούν.

Το Darknet κατακλύστηκε με blog κατά τη διάρκεια της "Αραβικής Άνοιξης" από ανθρώπους που συμμετείχαν στις εξεγέρσεις και ήθελαν να μεταφέρουν στο εξωτερικό τη μαρτυρία τους.

Δυνατότητες που δεν θα μπορούσαν να γίνουν πραγματικότητα αν το σκοτεινό διαδίκτυο δεν προσέφερε ένα επίπεδο ασφάλειας το οποίο δυστυχώς το κάνει ελκυστικό και σε εγκληματίες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Wikipedia, Internet Service Provider
  https://en.wikipedia.org/wiki/Internet_service_provider

- Dan Goodin, 30/11/2012: Tor operator charged for child porn transmitted over his servers
  https://arstechnica.com/tech-policy/2012/11/tor-operator-charged-for-child-porn-transmitted-over-his-servers/

- Dan Goodin, 22/7/2016: Malicious computers caught snooping on Tor-anonymized Dark Web sites
  https://arstechnica.com/security/2016/07/malicious-computers-caught-snooping-on-tor-anonymized-dark-web-sites/

- Άγγελος Κυρίτσης, 4/4/2013: Παρέχει πλήρη ανωνυμία το δίκτυο Tor?
  https://www.pcsteps.gr/1436-is-tor-really-anonymous/

- Άγγελος Κυρίτσης, 28/5/2016: Τι είναι το Bitcoin, το Ψηφιακό Νόμισμα του Μέλλοντος?
  https://www.pcsteps.gr/13691-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-bitcoin/

- Άγγελος Κυρίτσης, 16/1/2014: Bitcoin: Είναι Ασφαλές; Τι Κινδύνους Εμπεριέχει?
  https://www.pcsteps.gr/13813-bitcoin/

- SPYROS VJ, 24/7/2016: Μία ρεπόρτερ στην ολοσκότεινη καρδιά του Darknet
  http://www.lifo.gr/team/technology/60165

- Νικολαΐδης Ηλίας, 6/10/2015: Darknet
  http://www.tovima.gr/vimagazino/views/article/?aid=743174

- Etay Maor (Audio), 17/7/2016: Τι ακριβώς είναι το dark web;
  http://www.lifo.gr/videos/lifo_picks_planetearth/99022

- Andy Greenberg, 20/1/2017: It's about to get even easier to hide on the dark websites
  https://www.wired.com/2017/01/get-even-easier-hide-dark-web/

- Andy Greenberg, 1/9/2015: A guide to the dark web's lighter side
  https://www.wired.com/2015/09/guide-dark-webs-lighter-side/

- Brendan Sechter, Quora 19/11/2016: How are deep web websites created?
  https://www.quora.com/How-are-deep-web-websites-created

- Vladislav Antonov, Quora 26/5/2017: Have you ever been to the dark web? If so, why and what did you see?
  https://www.quora.com/Have-you-ever-been-to-the-dark-web-If-so-why-and-what-did-you-see/answer/Vladislav-Antonov-1

- Adrian Lamo, Quora 30/1/2017: What is the deep/dark web and how do you access it?
  https://www.quora.com/What-is-the-deep-dark-web-and-how-do-you-access-it

- Nathalie Nahai, Simon Barnard, Matt Shore,(Audio) 21/4/2016: Inside the darknet – Tech Weekly podcast
  https://www.theguardian.com/technology/audio/2016/apr/21/inside-the-darknet-tech-weekly-podcast

- Jennifer Hale, 6/4/2017: The hidden internet
  https://www.thesun.co.uk/news/2054243/dark-web-ross-ulbricht-silk-road-drugs-contract-killers-encrypted-network/

- Tarquin, (d.c) 20/9/2016: How to access the dark websites
  https://darkwebnews.com/help-advice/access-dark-web/

- Richard, (d.c) 6/11/2015: Using Dark Web To Support Intelligence Gathering
  https://darkwebnews.com/news/using-dark-web-to-support-intelligence-gathering/

- Richard, (d.c) 25/2/2016: Judge Rules FBI To Turn Over Malware It Used To Hack Dark Web Pornography Site
  https://darkwebnews.com/dark-web/fbi-malware-porn/

- Django, (d.c) 25/5/2015: Fighting ISIS On The Deep Web
  https://darkwebnews.com/news/fighting-isis-on-the-deep-web/

- 3313, (d.c) 11/5/2017: Behind The Scenes of Dark Web Admins
  https://darkwebnews.com/dark-web/behind-scenes-dark-web-admins/

- David kushner, 22/10/2015: The Darknet: Is the Government Destroying the Wild West of the Internet?
  http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022

- Γιάννης Διβράμης, 13/1/2015: Deep Web – Το ίντερνετ που δεν βλέπει η Google
  http://paramarketing.gr/deep-web-internet-vlepei-google/

- Γιώτα Χουλιάρα, 31/3/2017: Dark Net – Deep Web: Ένα παράλληλο on line σκοτεινό σύμπαν
  http://www.geopolitics.com.gr/2017/03/dark-net-deep-web-on-line.html

- Dimitios Dimakopoulos, 2/8/2015: Deep Web VS Dark Web: Αλήθειες και Ψέματα http://happyonline.gr/blog/security/item/35-deep-web-vs-darkweb-alitheies-kai-psemata

- Κώστας Δεληγίαννης, 4/5/2014: Ο κόσμος του σκοτεινού Ίντερνετ http://www.kathimerini.gr/765417/article/texnologia/diadiktyo/o-kosmos-toy-skoteinoy-internet

- Sabarinath, TechLog360: Darknet vs Dark Web vs Deep Web vs Surface Web https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/
- WhoIsHostingThis? Blog: "Everything You Need To Know on Tor & the Deep Web" http://www.whoishostingthis.com/blog/2017/03/07/tor-deep-web/