Στοιχεία Δικαίου της Πληροφορίας
Εαρινό εξάμηνο 2022
Καθ. Ευαγγελία Βαγενά

Κριτική μελέτη του Dark Web

Μελάς Παναγιώτης - 3190118
Τσατσαμπά Αντωνία-Μαρία - 3150182

Περιεχόμενα

Συντομογραφίες

ΧΘΔ: Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ

ΕΣΔΑ: Ευρωπαϊκή σύμβαση δικαιωμάτων του ανθρώπου

ΠΚ: Ποινικός Κώδικας

Εισαγωγή

Εδώ και αρκετά χρόνια έχουμε περάσει στην λεγόμενη «ψηφιακή εποχή» ή «εποχή της πληροφορίας». Με την δημιουργία του διαδικτύου, υπολογιστές που εκπροσωπούν ανθρώπους από όλο τον κόσμο, επικοινωνούν μεταξύ τους και έχουν πρόσβαση σε κοινά δεδομένα, ιστοσελίδες, (social) media, ιστοσελίδες ηλεκτρονικών αγορών και φορολογικές φόρμες ή επίσημα γραφειοκρατικά έγγραφα.

Το γεγονός ότι η πληροφορία του διαδικτύου είναι –δίχως βλάβη της γενικότητας- άπειρη, είναι ευρέως γνωστό, και οι χρήστες του παγκόσμιου ιστού έχουν πρόσβαση σε ένα τεράστιο όγκο δεδομένων και υπηρεσιών. Ποια είναι όμως τα πραγματικά όρια του διαδικτύου και σε τι ποσοστό μπορεί ο μέσος χρήστης να αποκτήσει πρόσβαση και να εξερευνήσει τις υπηρεσίες του διαδικτύου χωρίς να θέσει τον εαυτό του ή αλλους σε κίνδυνο;

Για τον μέσο χρήστη, διαδίκτυο είναι οι ιστότοποι και τα δεδομένα άμεσα προσβάσιμα από μαζικές και μεγάλες μηχανές αναζήτησης όπως η Google, το Yahoo και το Bing. Στην πραγματικότητα όμως αυτά είναι μόνο ένα πολύ μικρό μέρος του διαδικτύου και μόνο η επιφάνεια, σε μια θάλασσα, που όποιος θέλει και μπορεί να εξερευνήσει, έχει τεράστιο βάθος.

Το Dark Web (Σκοτεινός Ιστός) αποτελεί θέμα ενδιαφέροντος για πάρα πολλούς ανθρώπους που χρησιμοποιούν το διαδίκτυο, καθώς το τι πραγματικά συμβαίνει μέσα σε αυτό είναι στα όρια του "αστικού θρύλου", δεδομένου ότι η πρόσβαση είναι εξαιρετικά δύσκολη και συχνά οδηγεί σε παράνομους δρόμους.

1.1 To Dark web

Σύμφωνα με την Finklea(2017), συχνά υπάρχει η παρανόηση ότι το Διαδίκτυο και ο Παγκόσμιος Ιστός (web) είναι συνώνυμα, όμως δεν είναι. Αντίθετα, ο ιστός είναι ένα τμήμα του Διαδικτύου και ένα μέσο μέσω του οποίου μπορούν να προσπελαστούν πληροφορίες.

Στην προσπάθεια κατανόησης της έννοιας του ιστού, ορισμένοι μπορεί να θεωρήσουν ότι αποτελείται αποκλειστικά από τους διαδικτυακούς τόπους που είναι προσβάσιμοι μέσω μιας συνηθισμένης μηχανής αναζήτησης όπως η Google. Ωστόσο, αυτό το περιεχόμενο - γνωστό ως "επιφανειακός ιστός” (surface web)- είναι μόνο ένα τμήμα του ιστού. Ο βαθύς ιστός (deep web) αναφέρεται σε μια κατηγορία περιεχομένου που, για

διάφορους τεχνικούς λόγους, δεν είναι δυνατόν να προσπελαστεί από τις κλασικές μηχανές αναζήτησης(τεχνικά θέματα που αφορούν κυρίως το indexing στα search engines).

Οι πληροφορίες στο Deep Web περιλαμβάνουν περιεχόμενο από ιδιωτικά intranets (εσωτερικά δίκτυα όπως αυτά των επιχειρήσεων, των κυβερνήσεων οργανισμών ή πανεπιστημίων), εμπορικές βάσεις δεδομένων όπως η Lexis Nexis ή η Westlaw, ή ιστότοπους που παράγουν περιεχόμενο μέσω ερωτημάτων αναζήτησης (queries) ή φορμών. Πηγαίνοντας ακόμη πιο βαθιά στον ιστό, ο σκοτεινός ιστός (dark web) είναι ο τμήμα του Deep Web που έχει αποκρυφτεί σκόπιμα. Ο σκοτεινός ιστός είναι ένας ευρύτερος όρος που περιγράφει τους κρυμμένους ιστότοπους στο διαδίκτυο, στους οποίους οι χρήστες δεν μπορούν να αποκτήσουν πρόσβαση χωρίς τη χρήση κάποιου ειδικού λογισμικού. Το περιεχόμενο αυτών των ιστότοπων είναι προσβάσιμο, όμως οι εκδότες αυτών των ιστότοπων αποκρύπτονται.

Το surface web, πρόκειται για το τμήμα του παγκόσμιου ιστού στο οποίο μπορεί να έχει εύκολη πρόσβαση ο καθένας μέσω της χρήσης τυποποιημένων φυλλομετρητών ιστού και μηχανών αναζήτησης. Εδώ εμπεριέχονται όλοι οι γνωστοί δικτυακοί τόποι στους οποίους έχει πρόσβαση το κοινό μέσω παραδοσιακών προγραμμάτων περιήγησης, όπως το Google Chrome, ο Internet Explorer και ο Firefox. Οι ιστότοποι επισημαίνονται συνήθως με χειριστές μητρώου όπως ".com" και ".org" και μπορούν εύκολα να εντοπιστούν με δημοφιλείς μηχανές αναζήτησης.

Ο εντοπισμός ιστοσελίδων επιφανειακού ιστού είναι δυνατός επειδή οι μηχανές αναζήτησης μπορούν να κάνουν indexing τον ιστό μέσω ορατών συνδέσμων (μια διαδικασία που ονομάζεται "crawling" λόγω του ότι η μηχανή αναζήτησης ταξιδεύει στον ιστό σαν αράχνη). Ο επιφανειακός ή ορατός ή ανοιχτός ιστός είναι το περιεχόμενο του Παγκόσμιου Ιστού/World Wide Web (WWW), που είναι διαθέσιμο στους γενικούς χρήστες με καθολική και δωρεάν πρόσβαση. Αποτελεί το "ορατό" επιφανειακό στρώμα. Αν απεικονίσουμε ολόκληρο τον ιστό σαν ένα παγόβουνο, ο ανοιχτός ιστός θα είναι το ανώτερο τμήμα που βρίσκεται πάνω από το νερό. Από στατιστικής άποψης, αυτή η συλλογικότητα ιστοτόπων και δεδομένων αποτελεί λιγότερο από το 5% του συνολικού διαδικτύου (igi-global.com, kaspersky.com).

Το deep web, βρίσκεται κάτω από την επιφάνεια και αντιπροσωπεύει περίπου το 90% όλων των ιστότοπων. Αυτό θα ήταν το μέρος ενός παγόβουνου κάτω από το νερό, πολύ

μεγαλύτερο από τον επιφανειακό ιστό.Ο κρυφός αυτός ιστός είναι τόσο μεγάλος που δεν είναι δυνατό κάποιος να εκτιμήσει με ακρίβεια των αριθμό των σελιδών ή ιστότοπων που είναι ενεργοί ανά πάσα στιγμή.

Όπως αναφέρθηκε, ο βαθύς ιστός περιλαμβάνει κρυφό και ιδιωτικό περιεχόμενο. Δηλαδή, οι μεγάλες μηχανές αναζήτησης μπορούν να έχουν άμεση πρόσβαση μόνο σε ιστοσελίδες –αναλογικά-κοντά στην επιφάνεια. Όλα τα υπόλοιπα, από ακαδημαϊκά περιοδικά μέχρι ιδιωτικές βάσεις δεδομένων ή ακόμα και παράνομο περιεχόμενο, Αν και συχνά υπάρχει σύγχυση μεταξύ των όρων “deep” και “dark” web, μεγάλο μέρος του “deep web” στο σύνολό του είναι απολύτως νόμιμο και ασφαλές. Μερικά από τα μεγαλύτερα τμήματα του deep web περιλαμβάνουν:

-Βάσεις δεδομένων: τόσο δημόσιες όσο και ιδιωτικές προστατευόμενες συλλογές αρχείων που δεν συνδέονται με άλλες περιοχές του διαδικτύου, παρά μόνο για αναζήτηση εντός της ίδιας της βάσης δεδομένων.

-Intranets: εσωτερικά δίκτυα για επιχειρήσεις, κυβερνήσεις και εκπαιδευτικές εγκαταστάσεις που χρησιμοποιούνται για την επικοινωνία και τον έλεγχο πτυχών ιδιωτικά εντός των οργανισμών τους.

Σχετικά με την πρόσβαση στο deep web, ο μέσος άνθρωπος, ήδη, το χρησιμοποιεί καθημερινά. Ο όρος "βαθύς ιστός" αναφέρεται σε όλες τις ιστοσελίδες που δεν είναι αναγνωρίσιμες από τις μηχανές αναζήτησης ή χρειάζονται κάποια διαδικασία εξουσιοδότησης/αυθεντικοποίησης για την προσπέλασή τους. Οι ιστότοποι του deep web μπορεί να είναι κρυμμένοι πίσω από κωδικούς πρόσβασης ή άλλα τείχη ασφαλείας, ενώ άλλοι απλώς λένε στις μηχανές αναζήτησης να μην τις "ανιχνεύουν". Χωρίς ορατούς συνδέσμους, αυτές οι σελίδες είναι πιο κρυφές για διάφορους λόγους.

Στον ευρύτερο βαθύ ιστό, το "κρυμμένο" περιεχόμενό του είναι γενικά πιο καθαρό και ασφαλές. Τα πάντα, από αναρτήσεις σε ιστολόγια υπό αναθεώρηση και εκκρεμείς ανασχεδιασμούς ιστοσελίδων, μέχρι τις σελίδες στις οποίες ένας μέσος χρήστης αποκτά πρόσβαση όταν κάνει τραπεζικές συναλλαγές στο διαδίκτυο, αποτελούν μέρος του deep web. Επιπλέον, αυτά δεν αποτελούν απειλή για τον υπολογιστή ή την γενικότερη ασφάλεια των χρηστών. Οι περισσότερες από αυτές τις σελίδες διατηρούνται κρυμμένες από τον ανοιχτό ιστό για την προστασία των πληροφοριών και της ιδιωτικής ζωής των χρηστών, όπως π.χ: Χρηματοοικονομικοί λογαριασμοί, όπως τραπεζικοί και συνταξιοδοτικοί λογαριασμοί

ηλεκτρονικού ταχυδρομείου και κοινωνικών μηνυμάτων, βάσεις δεδομένων ιδιωτικών επιχειρήσεων, ευαίσθητες πληροφορίες HIPPA, όπως ιατρικά έγγραφα και νομικά αρχεία.

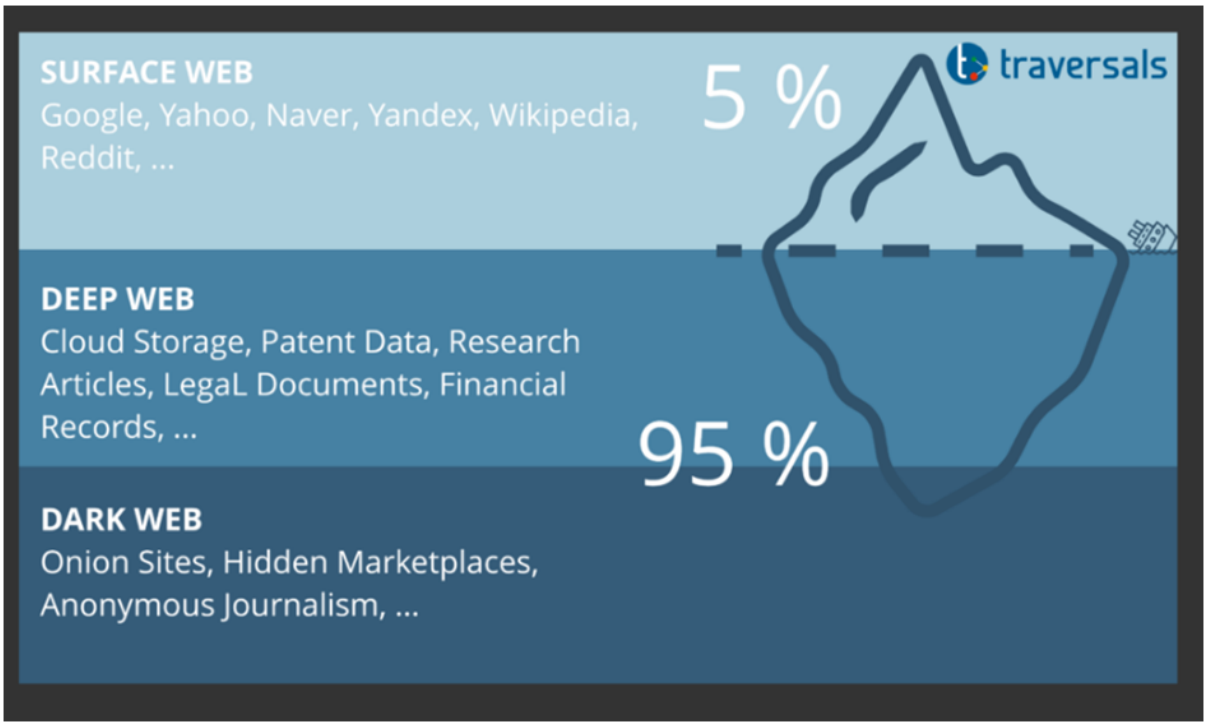
Στο σκοτεινό άκρο ή αναλογικά στον «πάτο» του διαδικτύου στέκεται το πιο επικίνδυνο περιεχόμενο και δραστηριότητες. Σε αυτό το απώτερο άκρο του deep web βρίσκονται ιστότοποι σκοπίμως κρυμμένοι, οι οποίοι θεωρούνται ο "σκοτεινός ιστός" και είναι προσβάσιμοι μόνο από ειδικό λογισμικό ανώνυμου προγράμματος περιήγησης.

Το dark web αναφέρεται σε ιστότοπους που δεν μπορούν να γίνουν indexed(η διαδικασία με την οποία μια μηχανή αναζήτησης προσθέτει διαδικτυακό περιεχόμενο στο ευρετήριό της.) και είναι προσβάσιμοι μόνο μέσω εξειδικευμένων προγραμμάτων περιήγησης στο διαδίκτυο. Σημαντικά μικρότερος από τον ήδη συγκριτικά μικροσκοπικό επιφανειακό ιστό, ο σκοτεινός ιστός θεωρείται μέρος του deep web. Χρησιμοποιώντας την εικόνα του ωκεανού και του παγόβουνου, ο σκοτεινός ιστός θα ήταν η κάτω άκρη του βυθισμένου παγόβουνου.

Ο σκοτεινός ιστός, ωστόσο, είναι ένα πολύ κρυφό τμήμα του βαθύ ιστού με το οποίο λίγοι θα αλληλεπιδράσουν ποτέ ή θα το δουν. Η ανάλυση της κατασκευής του dark web αποκαλύπτει μερικά βασικά στρώματα που το καθιστούν ένα ανώνυμο καταφύγιο: Δεν υπάρχει ευρετηρίαση ιστοσελίδων από τις μηχανές αναζήτησης του επιφανειακού ιστού. Η Google και άλλα δημοφιλή εργαλεία αναζήτησης δεν μπορούν να ανακαλύψουν ή να εμφανίσουν αποτελέσματα για σελίδες εντός του σκοτεινού ιστού. Ακόμα, κρύβεται περαιτέρω από διάφορα μέτρα ασφαλείας δικτύου, όπως τείχη προστασίας(firewalls) και κρυπτογράφηση.

Η φήμη του σκοτεινού ιστού έχει συχνά συνδεθεί με εγκληματικές προθέσεις ή παράνομο περιεχόμενο, καθώς και με ιστότοπους "εμπορίας" όπου οι χρήστες μπορούν να αγοράσουν παράνομα αγαθά ή υπηρεσίες. Ωστόσο, νόμιμες δραστηριότητες μπορούν και αυτές να λάβουν μέρος σε αυτό το framework(πλαίσιο) .

Όσον αφορά την ασφάλεια του σκοτεινού ιστού, οι κίνδυνοι του deep web είναι πολύ διαφορετικοί από τους κινδύνους του dark web. Η παράνομη δραστηριότητα στον κυβερνοχώρο ίσως δεν είναι εύκολα ορατή με μια απλή και τυχαία καθημερινή χρήση, αλλά τείνει να είναι πολύ πιο ακραία και απειλητική όταν αναζητείται. (kaspersky.com, traversals.com).



Όταν οι περισσότεροι άνθρωποι μπαίνουν στο διαδίκτυο, το κάνουν μέσω ενός υπολογιστή ή μιας συσκευής που διαθέτει διεύθυνση IP (Internet Protocol) - μια μοναδική διαδικτυακή ταυτότητα.

Η διεύθυνση IP επιτρέπει στα δίκτυα να στέλνουν τις σωστές πληροφορίες στο σωστό μέρος - για παράδειγμα, να διασφαλίζουν ότι ένα μήνυμα ηλεκτρονικού ταχυδρομείου φτάνει στον προορισμό του. Η διαδικτυακή δραστηριότητα ενός ατόμου μπορεί να εντοπιστεί και να παρακολουθηθεί μέσω της διεύθυνσης IP.

Ο "σκοτεινός ιστός" χρησιμοποιεί πολύπλοκα συστήματα που ανωνυμοποιούν την πραγματική διεύθυνση IP ενός χρήστη, καθιστώντας πολύ δύσκολο να εξακριβωθεί ποιους

ιστότοπους έχει επισκεφθεί μια συσκευή. Η πρόσβαση σε αυτόν γίνεται γενικά με τη χρήση ειδικού λογισμικού, κρυφές μηχανές αναζήτησης, με την δημοφιλέστερη να ονομάζεται Tor (The Onion Router).

Ο σκοτεινός ιστός αρχικά χρησιμοποιήθηκε από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών για την ανώνυμη επικοινωνία, όμως πλέον έχει γίνει κόμβος για τους χρήστες που επιθυμούν να παραμείνουν ανώνυμοι σε όλο τον κόσμο. Οι άνθρωποι χρησιμοποιούν το dark web τόσο για νόμιμους όσο και για παράνομους σκοπούς. Όπως ειπώθηκε πάνω η πρόσβαση σε αυτό το κομμάτι του ιστού γίνεται μέσω ειδικού λογισμικού. Χρησιμοποιεί μια τεχνολογία που ονομάζεται "onion routing", η οποία προστατεύει τους χρήστες από την παρακολούθηση και τον εντοπισμό μέσω μιας τυχαίας διαδρομής κρυπτογραφημένων διακομιστών. Όταν οι χρήστες αποκτούν πρόσβαση σε έναν ιστότοπο μέσω του Tor, οι πληροφορίες τους δρομολογούνται μέσω χιλιάδων σημείων αναμετάδοσης που καλύπτουν τα ίχνη του χρήστη και καθιστούν την περιήγησή του πρακτικά αδύνατο να εντοπιστεί.

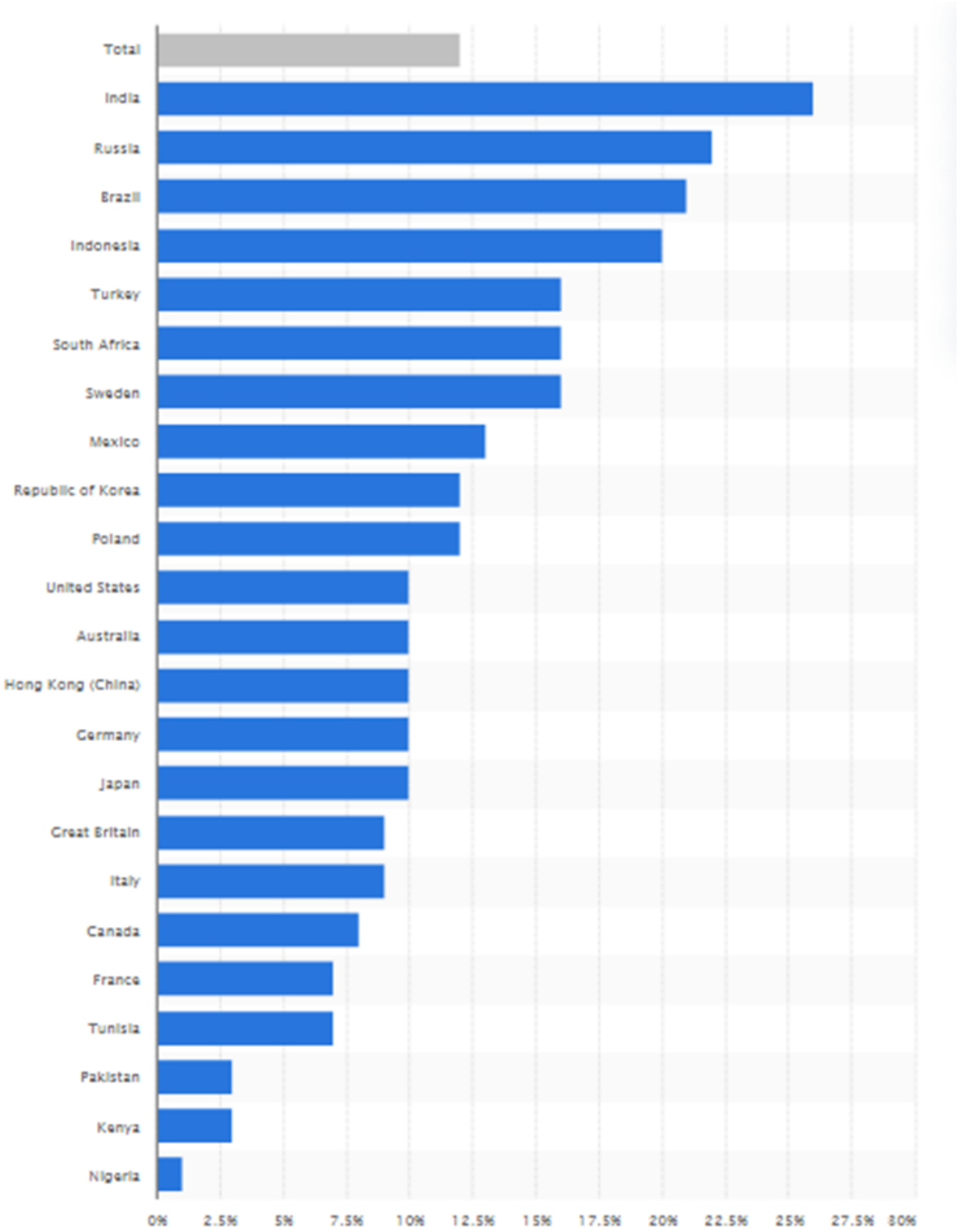
Περίπου 2,5 εκατομμύρια άνθρωποι χρησιμοποιούν το Tor κάθε μέρα. Το ίδιο το Tor δεν είναι ο "σκοτεινός ιστός", αλλά αντίθετα είναι ένας τρόπος περιήγησης τόσο στον ανοιχτό όσο και στον σκοτεινό ιστό χωρίς κανείς να μπορεί να αναγνωρίσει τον χρήστη ή να παρακολουθήσει τη δραστηριότητά του.

(sopa.tulane.edu, thinkuknow.co.uk)

Οι χρήστες έχουν πρόσβαση

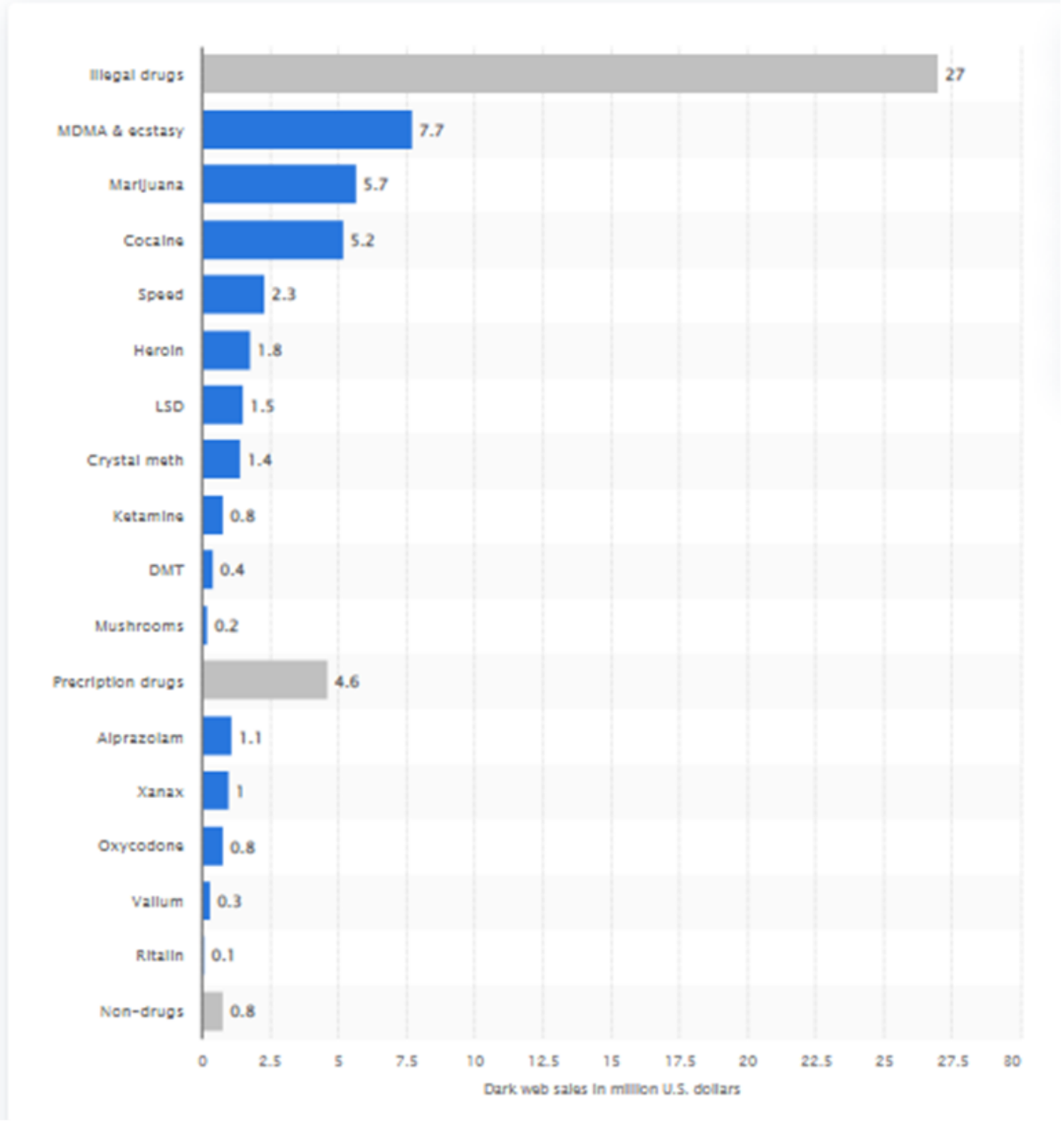
στο Dark Web με την προσδοκία ότι μπορούν να μοιραστούν πληροφορίες ή/και αρχεία με μικρό κίνδυνο. Φυσικά αυτή η ανωνυμία και αδυναμία εντοπισμού χρησιμοποιείται για κάθε είδους παράνομη δραστηριότητα από εμπόριο όπλων και ναρκωτικών, πλαστογράφηση εγγράφων, μέχρι διακίνηση παιδικής πορνογραφίας και υποκίνηση ακραίων πολιτικών ή τρομοκρατικών κινήσεων.

Ενδεικτικά στατιστικά του dark web:



Αυτή η στατιστική παρουσιάζει το ποσοστό των χρηστών του διαδικτύου που έχουν χρησιμοποιήσει τεχνολογίες, όπως το δίκτυο ανωνυμίας Tor, που επιτρέπουν την πρόσβαση στον σκοτεινό ιστό από τον Φεβρουάριο του 2019, ταξινομημένο ανά χώρα. Κατά την περίοδο της έρευνας, το 26% των ερωτηθέντων από την Ινδία δήλωσαν ότι είχαν χρησιμοποιήσει τέτοιες τεχνολογίες.

Πηγή : statista.com



Αυτή η στατιστική παρουσιάζει μια εκτίμηση των πωλήσεων παράνομων ναρκωτικών στο dark web από τον Δεκέμβριο του 2013 έως τον Ιούλιο του 2015. Εκτιμάται ότι τα παράνομα ναρκωτικά απέφεραν 27 εκατομμύρια δολάρια σε αξία πωλήσεων μέσω του dark web, με την κοκαΐνη να αντιπροσωπεύει 5,2 εκατομμύρια δολάρια των παράνομων διαδικτυακών πωλήσεων.

Πηγή : statista.com

Characteristic	Price in U.S. dollars
Bank Details	259.56
Debit Card	250.05
PayPal	42.38
Credit Card	33.88
Western Union	29.44
Moneygram	21.59
Driving License	27.62
Passport	18.45
Proof of Identity	16.52
Amazon	30.36
Best Buy	26.54
eBay	21.66
Nordstrom	13.47

Showing entries 1 to 13 (75 entries in total)
Previous Next

Αυτή η στατιστική παρουσιάζει τη μέση τιμή των κλεμμένων διαπιστευτηρίων στις αγορές του σκοτεινού ιστού από τον Φεβρουάριο του 2019. Η μέση τιμή μιας σύνδεσης λογαριασμού Amazon ήταν 30,36 δολάρια ΗΠΑ. Τα κλεμμένα τραπεζικά στοιχεία είχαν αξία 259,56 δολάρια ΗΠΑ.

Πηγή : statista.com

2. Νομικό πλαίσιο

2.1. Νόμοι

Η διαμόρφωση ενός καθολικού και, συνάμα, πλήρως αποτελεσματικού νομοθετικού πλαισίου σε ένα τόσο περίπλοκο σημείο του διαδικτύου, όσο το Dark Web, αποτελεί δύσκολο έργο.

Πρώτα απ' όλα, αξίζει να σημειωθεί πως η απλή πρόσβαση στο σκοτεινό ιστό δεν αντιτίθεται στην κείμενη νομοθεσία. Το περιεχόμενο το οποίο μπορεί να προσπελάσει ο χρήστης κατά την πλοήγησή του αλλά και οι ενέργειες που μπορεί να διαπράξει εκεί, είναι τα σημεία στα οποία μπορεί να συντελεστεί κάποιο έγκλημα.

Στο έργο του Jardine (2015) καθίσταται σαφές πως η πλήρης απαγόρευση πρόσβαση στο Onion Router (Tor) δεν είναι θεμιτή. Πιο συγκεκριμένα, η εξέλιξη κάθε ανθρώπινης δημιουργίας δύναται να χρησιμοποιηθεί για ωφέλιμους αλλά και επιβλαβείς σκοπούς και εξαρτάται από τον τρόπο χρήσης της, ενώ κάθε ενδεχόμενο "παραθυράκι" μπορεί να εντοπιστεί από κάθε χρήστη.

Επομένως, διαφορετικοί νόμοι σχετίζονται με τις διαφορετικές εγκληματικές πράξεις που απαντώνται στο Dark Web, όσον αφορά τη διάπραξη των εγκλημάτων αυτή καθαυτή.
Αρχικά, η προστασία των προσωπικών δεδομένων του ατόμου αποτελεί θεμελιώδες ανθρώπινο δικαίωμα με βάση τα άρθρα 7 και 8 του ΧΘΔ. Εκτός αυτού, το παραπάνω υποστηρίζεται και από το Συμβούλιο της Ευρώπης βάσει της σύμβασης 108 του 1981 αλλά

και του άρθρου 8 (1950) της ΕΣΔΑ το οποίο προασπίζει τα δικαιώματα περί ιδιωτικής ζωής, κατοικίας και αλληλογραφίας. Επιπροσθέτως, και ο Γενικός Κανονισμός για την προστασία δεδομένων (ΓΚΠΔ) οριοθετεί το πλαίσιο για την προστασία των προσωπικών δεδομένων. Με βάση τα παραπάνω, η παράνομη πρόσβαση σε προσωπικά δεδομένα, καθώς και ο διαμοιρασμός ή οποιαδήποτε άλλη χρήση τους εν αγνοία του ατόμου που αφορούν, αντιβαίνει στο τρέχον νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης. (europarl.europa.eu)

Στη συνέχεια, σύμφωνα με το άρθρο 348Α του ΠΚ (Νόμος 4619/2019), απαγορεύεται η κατοχή, παραγωγή, χρήση, διανομή και κάθε περαιτέρω ενέργεια που αφορά υλικό παιδικής πορνογραφίας, ενώ η μη συμμόρφωση στο νόμο αυτό επιφέρει τις αντίστοιχες ποινικές συνέπειες (πρόστιμο, ποινή φυλάκισης).

Σύμφωνα με το άρθρο 187Α του ΠΚ (Νόμος 4619/2019), τα εγκλήματα κατά της δημόσιας τάξης σε εθνικό ή διεθνές επίπεδο, καθώς και η συμμετοχή σε τρομοκρατικές οργανώσεις τιμωρούνται με φυλάκιση διαρκείας η οποία σχετίζονται με το ρόλο που κατέχει το άτομο σε αυτού του είδους τις οργανώσεις ή πραξεις.

Όσον αφορά το εμπόριο όπλων το οποίο λαμβάνει χώρα στο σκοτεινό ιστό, σύμφωνα με το άρθρο 436 του ΠΚ τιμωρείται είτε με κράτηση είτε με πρόστιμο τόσο η κατοχή και η χρήση όσο και η διακίνηση όπλου.

Για το έγκλημα της εμπορίας ανθρώπων, το άρθρο 323Α του ΠΚ ορίζει τιμωρία με φυλάκιση αλλά και χρηματικό πρόστιμο για τη βίαιη/ εξαναγκαστική απαγωγή, κράτηση, εκμετάλλευση, παράδοση αλλά και παραλαβή ανθρώπου.

Ένα ακόμη ζήτημα που συναντάται στο Dark Web είναι τόσο η πρόσληψη “εκτελεστών” όσο και η διακίνηση υλικού στο οποίο είναι καταγεγραμμένη μια δολοφονία ή άλλο ειδεχθές έγκλημα. Στην πρώτη περίπτωση, με βάση το άρθρο 299 του ΠΚ, η ανθρωποκτονία εκ προθέσεως τιμωρείται με ισόβια κάθειρξη, ενώ η ανθρωποκτονία εν βρασμώ επισύρει ποινή πρόσκαιρης φυλάκισης. Στη δεύτερη περίπτωση, τα όρια δεν είναι εξίσου προσδιορισμένα με σαφήνεια.

Τέλος, η διακίνηση ναρκωτικών ουσιών αποτελεί πράξη παράνομη με βάση το άρθρο 20 του ΠΚ και επιφέρει ποινή φυλάκισης αλλά και χρηματικού προστίμου. Εξαίρεση σε αυτό αποτελούν περιπτώσεις οι οποίες υπόκεινται στα άρθρα 21, 22 και 23 του ΠΚ.

Παρ’ όλα αυτά, σημείο αναφοράς στην επιβολή των παραπάνω αλλά και στη διαδικασία θέσπισης νέων νόμων σχετικά με το ηλεκτρονικό έγκλημα, αποτελεί η φύση του εγκλήματος αυτού. Με άλλα λόγια, η μη χρήση άμεσης βίας μπορεί να οδηγήσει στη φαινομενική υπεραπλούστευση του εγκλήματος, γεγονός το οποίο παραγνωρίζει πως το κυβερνοέγκλημα διαπράττεται σε ένα ευρύτατο περιβάλλον, στο οποίο μπορούν να έχουν

πρόσβαση εκατομμύρια άνθρωποι από όλον τον κόσμο, και μάλιστα σε σημαντικά μικρό χρόνο και μέσω αυτοματοποιημένων διαδικασιών (Βαγιάτη Ε., 2014).

2.2. Σχετικοί φορείς στην Ελλάδα

Σύμφωνα με την ιστοσελίδα kidsatsafety.com, κύριοι αρμόδιοι φορείς που σχετίζονται με την ασφάλεια στο διαδίκτυο αποτελούν:

- Η Δίωξη Ηλεκτρονικού Εγκλήματος (ΔΙΔΗΕ)
- Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)
- Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)
- Το saferinternet4kids, επίσημος εκπρόσωπος του Ευρωπαϊκού δικτύου INSAFE/INHOPE.

3. Αξιοσημείωτες υποθέσεις

Σε αυτό το κεφάλαιο πρόκειται να συζητηθούν τρεις από τις πιο διαβόητες υποθέσεις του Dark Web.

3.1. Peter Scully

Σύμφωνα με το Wikipedia.org, ο Peter Gerard Scully γεννήθηκε το 1963 στη Μελβούρνη της Αυστραλίας. Διέφυγε στη Μανίλα των Φιλιππίνων σε μια προσπάθεια να αποφύγει κατηγορίες που εκκρεμούσαν εις βάρος του για οικονομικά εγκλήματα. Κατά την παραμονή του στις Φιλιππίνες δημιούργησε στο Dark Web τον ιστότοπο “No limits fun” του οποίου το περιεχόμενο αφορούσε παιδική πορνογραφία.

Οι αστυνομικές αρχές έφτασαν στα ίχνη του όταν ένα βίντεο με τίτλο “Daisy’s destruction” κυκλοφόρησε εκτός του Σκοτεινού Ιστού. Το βίντεο αυτό απεικόνιζε σκηνές εξωφρενικής βίας (συγκεκριμένα βιασμό και βασανισμό) σε παιδιά, το μικρότερο εκ των οποίων ήταν η ίδια η Daisy, 18 μηνών, ενώ φημολογείται πως χρήστες μπορούσαν να αγοράσουν το βίντεο έναντι 10.000 δολαρίων. Οι ολλανδικές αρχές εντόπισαν το βίντεο και ξεκίνησαν έρευνα, ώστε να εντοπιστεί από που ξεκίνησε η εκπομπή του. Σύντομα, οι Αυστραλιανές αρχές συνεργάστηκαν με την Ολλανδία για τη διεξαγωγή της, πλέον, διεθνούς έρευνας.

Ο Peter Scully συνελήφθη στις Φιλιππίνες το 2015 και παρότι το γεγονός ότι πολλά ψηφιακά στοιχεία που υπήρχαν στον υπολογιστή του δράστη καταστράφηκαν σε φωτιά, καταδικάστηκε σε ισόβια κάθειρξη για διακίνηση ανθρώπων και βιασμό ανήλικων κοριτσιών. Την ποινή του εκτίει σε φυλακή των Φιλιππίνων. Μετά τη σύλληψή του έχει δώσει συνέντευξη με αφορμή την υπόθεση του βίντεο “Daisy’s destruction” στο 60 Minutes Australia (Παράρτημα 1).

3.2. Silk Road

Το Φεβρουάριο του 2011 δημιουργήθηκε στο Σκοτεινό Ιστό η ιστοσελίδα Silk Road, από τον 29χρονο μηχανικό υπολογιστών Ross Ulbricht. Επρόκειτο για σελίδα "μαύρης αγοράς" η οποία διακινούσε ναρκωτικές ουσίες και όπλα. Σύμφωνα με τους ερευνητές, οι πωλήσεις του Silk Road ανήλθαν σε 1 δισεκατομμύριο δολάρια, μέχρι και το 2013 που το FBI το "κατέβασε", και η ιστοσελίδα παρείχε 10.000 προϊόντα προς πώληση.

Οι πληρωμές γίνονταν κυρίως μέσω bitcoin, ενώ από τον ιδρυτή της σελίδας κατασχέθηκαν bitcoins αξίας 28 περίπου εκατομμυρίων δολαρίων. Ο ίδιος αρχικά δήλωσε πως δημιούργησε την ιστοσελίδα αλλά στη συνέχεια παρέδωσε τον έλεγχό της σε τρίτους. Ωστόσο, καταδικάστηκε το 2015 για συμμετοχή σε παράνομες επιχειρήσεις, διακίνηση ναρκωτικών, ξέπλυμα χρήματος και hacking (Wikipedia.org).

3.3 Hieu Minh Ngo

Ο Hieu Minh Ngo γεννήθηκε το 1989 στο Βιετνάμ, όπου τη χρονική περίοδο 2007-2013 επιδιδόταν στην κλοπή ταυτοτήτων και άλλων προσωπικών δεδομένων από πολίτες των Η.Π.Α. με σκοπό την απόσπαση χρηματικών ποσών. Ο τρόπος με τον οποίο το επιτύγχανε αυτό είναι μέσω hacking σε βάσεις δεδομένων μεγάλων εταιρειών που διαχειρίζονταν τις πληροφορίες που εκείνος χρησιμοποιούσε για τις αξιόποινες πράξεις του.

Το 2013, οι μυστικές υπηρεσίες των Η.Π.Α. κατόρθωσαν μέσω μιας ψεύτικης οικονομικής συμφωνίας να φέρουν τον Ngo στην περιοχή Guam της δικαιοδοσίας τους, όπου και συνελήφθη. Καταδικάστηκε για τηλεπικοινωνιακή απάτη, απάτη ταυτότητας, απάτη πρόσβασης σε συσκευές και απάτη μέσω ηλεκτρονικού υπολογιστή, σε 13 χρόνια φυλάκιση σε ομοσπονδιακή φυλακή (Wikipedia, τελευταία επίσκεψη 5.6.2022).

Σύμφωνα με τον Braue (2022), ο Ngo επιμορφώθηκε πάνω σε θέματα κυβερνοασφάλειας και πλέον εργάζεται στο Εθνικό Ινστιτούτο Κυβερνοασφάλειας (National Cyber Security Center) του Βιετνάμ (krebsonsecurity.com, τελευταία επίσκεψη 5.6.2022)

Ο ίδιος αναφέρει σύντομα τη μεταστροφή του, στο προφίλ του στην ιστοσελίδα LinkedIn (Παράρτημα 2), όπου και παρουσιάζεται ως πρώην κυβερνοεγκληματίας και νυν ειδικός κυβερνοασφάλειας.

4. Η άλλη πλευρά

Εντούτοις, όπως αναφέρει και η Finklea (2017) στο έργο της, η ανωνυμία στο χώρο του διαδικτύου δεν αποτελεί πρόβλημα εν γένει. Αντιθέτως, μπορεί να αποτελέσει χρήσιμο εργαλείο σε διάφορους τομείς. Για παράδειγμα, ο χρήστης μπορεί να προσπελάσει περιεχόμενο που δεν είναι προσβάσιμο από την τοποθεσία του υπό κανονικές συνθήκες και το ζήτημα αυτό μπορεί να φτάσει σε επίπεδα πολιτικού ακτιβισμού.

Εκτός αυτού, μέσω του Tor διασφαλίζεται και η επικοινωνία ευαίσθητων θεμάτων, όπως σωματικών ή ψυχικών ασθενειών, καθώς και η κάλυψη της ip αλλά και κάθε άλλου δεδομένου που μπορεί να χρησιμοποιηθεί για εντοπισμό, σε περίπτωση που οι χρήστες είναι ανήλικοι. Με τον ίδιο τρόπο, δύναται ένας χρήστης ο οποίος ζει υπό ολοκληρωτικό καθεστώς να επικοινωνήσει πράγματα στον "έξω κόσμο".

Πέραν των μεμονωμένων χρηστών, υπάρχουν και κρατικά ζητήματα τα οποία επικοινωνούνται στην (έστω και σχετική) ασφάλεια που παρέχει το Dark Web. Συγκεκριμένα, οι αρχές μπορούν να χρησιμοποιήσουν το εν λόγω σύστημα για να παρακολουθήσουν ύποπτες κινήσεις, να λάβουν μαρτυρίες ανώνυμα αλλά και να μεταφέρουν ευαίσθητες κρατικές, κυβερνητικές ή στρατιωτικές πληροφορίες (Finklea, 2017).

Επίλογος - Συμπεράσματα

Με βάση τα παραπάνω, καθίσταται σαφές πως ο Σκοτεινός ιστός αποτελεί πρόσφορο έδαφος για κάθε είδους εγκληματική ενέργεια λόγω της ανωνυμίας που παρέχει. Ταυτόχρονα, η εξιχνίαση των εγκλημάτων αυτών δυσχεραίνεται από το γεγονός ότι οι μάρτυρες των υποθέσεων αυτών, δίνοντας κατάθεση, παραδέχονται πως έχουν συμμετάσχει στην εγκληματική πράξη ή ήταν "μπροστά" καθώς συνέβαινε, πράγμα που ενδεχομένως τους καθιστά ενόχους.

Παρά τα ζητήματα αυτά, ωστόσο, η πλήρης κατάργησης της ανώνυμης πρόσβασης στο διαδίκτυο με τον τρόπο που γίνεται στο Dark Web, δεν είναι θεμιτή καθώς εξυπηρετεί πληθώρα "καλών σκοπών".

Παραρτήματα

Παράρτημα 1

Συνέντευξη του Peter Scully (Μέρος 1 & Μέρος 2)

- https://www.youtube.com/watch?v=YI33EPlCW5w&ab_channel=60MinutesAustralia
- https://www.youtube.com/watch?v=9MftNB12leI&ab_channel=60MinutesAustralia

Παράρτημα 2

Το προφίλ του Ngo στην ιστοσελίδα LinkedIn

https://vn.linkedin.com/in/hieu-minh-ngo-hieupc?original_referer=https%3A%2F%2Fwww.google.com%2F

Βιβλιογραφία

Έντυπη βιβλιογραφία σε ψηφιακή μορφή

- *Finklea, K.,* Dark Web, Congregational Research Service 2017
- *Braue, D*., Hieu Minh Ngo's Conviction And Redemption, Cybercrime Magazine, 2022 (URL: https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/)
- *Βαγιάτη, Ε*., Ηλεκτρονικό έγκλημα και προστασία προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση
- *Jardine, E.,* The Dark Web Dilemma: Tor, Anonymity and Online Policing, Global Commission on Internet Comission on Internet Governance Paper Series, No.21

Ιστοσελίδες

- lawspot.gr
    - Χρησιμοποιήθηκε για όλες τις παραπομπές σε άρθρα του ΠΚ

- wikipedia.org
    - Τελευταία επίσκεψη 5.6.2022
- statista.com
    - Τελευταία επίσκεψη 5.6.2022

- https://www.europarl.europa.eu/ftu/pdf/el/FTU_4.2.8.pdf
    - Τελευταία επίσκεψη 5.6.2022
- https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
    - Τελευταία επίσκεψη 5.6.2022
- https://blog.knowbe4.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web
    - Τελευταία επίσκεψη 5.6.2022
- https://www.igi-global.com/dictionary/dark-web/82713
    - Τελευταία επίσκεψη 5.6.2022
- https://www.kaspersky.com/resource-center/threats/deep-web
    - Τελευταία επίσκεψη 5.6.2022
- https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/
    - Τελευταία επίσκεψη 5.6.2022

- https://www.newscientist.com/article/mg24933260-400-silk-road-review-the-true-story-of-the-dark-webs-illegal-drug-market/
    - T
- https://www.kidsatsafety.gr/gr/el/armodioi-foreis/

Περίληψη

Στην μελέτη για τον σκοτεινό ιστό, φαίνεται πως το ποσοστό του διαδικτύου που είναι πραγματικά προσβάσιμο από τον μέσο χρήστη είναι πάρα πολύ μικρό και το μεγάλο ποσοστό του διαδικτύου επικεντρώνεται σε έναν κρυφό και βαθύ ιστό που καταλήγει σε έναν εντελώς απόκρυφο-στα όρια της παρανομίας- σκοτεινό ιστό.

Στην μελέτη αυτή αναλύονται οι βασικές συστάσεις του κάθε πλαισίου για τα αντίστοιχα μέρη του ιστού καθώς και οι τρόποι με τους οποίους μπορούν να προσπελαστούν ή να χρησιμοποιηθούν. Στη συνέχεια εξετάζεται το τρέχον νομοθετικό πλαίσιο και επικεντρωνόμαστε σε κάποιες υποθέσεις άξιες περαιτέρω ανάλυσης.