ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΌ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΟΙ ΕΠΙΘΕΣΕΙΣ ΣΤΟ DARKNET

ΣΠΟΥΔΑΣΤΡΙΕΣ:

ΔΑΒΒΕΤΑ ΔΗΜΗΤΡΑ ΝΑΤΑΛΛΙΑ

ΚΟΝΤΟΥ ΓΕΩΡΓΙΑ

ΜΗΤΟΥ ΕΛΕΑΝΑ

ΕΠΟΠΤΕΥΟΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΠΑΔΟΠΟΥΛΟΣ ΔΗΜΗΤΡΗΣ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία αποτέλεσε το αντικείμενο μελέτης μας εδώ και αρκετά μεγάλο διάστημα και θεωρούμε πώς λόγω της σπουδαιότητας του θέματος θα αποτελέσει ένα πολύ σημαντικό εφαλτήριο για την μετέπειτα πορεία μας στον κλάδο. Θέμα της συγκεκριμένης μελέτης είναι οι επιθέσεις στο Darknet και η καλύτερη αρχή θα μπορούσε να είναι η απόδοση της έννοιας του Darknet. Το Darknet είναι ένα δίκτυο από σέρβερ, οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα. Παράλληλα, η τεχνολογία εξασφαλίζει πως πρόσβαση στο Σκοτεινό Διαδίκτυο έχουν μόνον χρήστες που έχουν εγκαταστήσει το ανάλογο λογισμικό στο μηχάνημά τους.

Η εργασία αναπτύσσεται σε πέντε κεφάλαια, καθένα από τα οποία έχει διαφορετική θεματολογία. Έτσι λοιπόν στο πρώτο κεφάλαιο αναλύεται το Darknet, και συγκεκριμένα δίνεται ο εκτενής ορισμός του, ενώ παράλληλα αναλύεται η προέλευση και η χρήσεις του, το πώς δομείται το λογισμικό του και ποιες δικλείδες ασφαλείας διαθέτει. Στο δεύτερο κεφάλαιο αναλύεται το Dark web και το Deep web, δύο διαφορετικές παράμετροι του darknet και αναλύεται το πώς λειτουργούν, πώς δομούνται οι αγορές και πώς πραγματοποιούνται οι πληρωμές και επίσης, γίνεται αναφορά στις απάτες και στην τρομοκρατία. Στο τέλος του κεφαλαίου παρουσιάζονται οι διαφορές του τυπικού ιστού με το darknet και οι διαφορές μεταξύ dark web και deep web.

Στο τρίτο κεφάλαιο αναλύονται τα είδη των επιθέσεων που παρουσιάζονται στο Darknet που αποτελεί και το κύριο μέρος της παρούσας εργασίας, ενώ επικεντρωνόμαστε στην Norse με το IP Viking που προσπαθεί να προστατεύσει από επιθέσεις hackers στον κόσμο του Darknet. Στο τέταρτο και σπουδαιότερο κεφάλαιο της μελέτης, παρουσιάζεται η έρευνα που πραγματοποιήθηκε με σκοπό να παρουσιάσει τις επιθέσεις στο Darknet με δεδομένα που συλλέχθηκαν από την ιστοσελίδα της Norse για τον Ιούνιο του 2016. Τα τελικά αποτελέσματα παρουσιάζονται στο τέλος του κεφαλαίου.

Ευελπιστούμε πώς η παρούσα μελέτη θα αποτελέσει χρήσιμο εγχειρίδιο στα χέρια κάθε μελετητή του Darknet.

ABSTRACT

This thesis has been the subject of study for long enough and we think that, because of the importance of the issue, it will be a major springboard for our future course in the industry. The subject of this study is Darknet attacks and what would be better, than to start by defining the concept of Darknet. Darknet is a network server, which is based on encryption technology to exchange data. At the same time, the technology ensures that only users who have installed the appropriate software on their machine, have access to Darknet.

The thesis is structured in five chapters, each of which has a different theme. Thus, in the first chapter we analyze Darknet, namely the extensive definition given, while analyzing the origins and uses, how the software is built and what safety measurements are taken. We also analyze, how Darknet works, how markets are structured and how payments are made and also we make reference to fraud and terrorism. In the second chapter we analyze Dark web and Deep web, two different parameters of Darknet. At the end of the chapter we present the differences between standard net and darknet and the differences between dark web and deep web.

The third chapter analyzes the types of attacks present in Darknet which is the main part of this work, while focusing in Norse IP Viking trying to fend off hackers' attacks in the world of Darknet. The fourth

and most important chapter of the study, contains a research which was held in order to present the attacks in Darknet with data collected from Norse website in June 2016. The final results are presented at the end of the chapter.

Hopefully, this study will be a useful guide in the hands of every scholar towards Darknet.

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» Ίντερνετ, 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 σάιτ 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 σέρβερ, 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 σάιτ μπορεί να αποκρύπτει τα ψηφιακά του ίχνη, «καμουφλάροντας» τον σέρβερ 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, πριν από λίγες εβδομάδες, 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 μετά τον περασμένο Οκτώβριο και 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 σάιτ 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 περιμένει να δικασθεί, αντιμετωπίζοντας ποινή φυλάκισης τουλάχιστον 30 ετών, τον Φεβρουάριο 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.

Η Norse είναι μια εταιρεία που ασχολείται με την ασφάλεια στο διαδίκτυο και παρέχει στους πελάτες τις πληροφορίες σχετικά με τις επιθέσεις που δέχονται στο dark net. Παρέχει επίσης πληροφορίες μέσω της σελίδας της Norse- IP Viking, η οποία δείχνει τις επιθέσεις που γίνονται παγκοσμίως σε πραγματικό χρόνο λεπτομερώς. Παρέχει δηλαδή και τις πληροφορίες: τις χώρες από τις οποίες προέρχεται η κάθε επίθεση, τις χώρες οι οποίες δέχονται τις επιθέσεις και τους τύπους των επιθέσεων. Επιπλέον, έχει έναν συγκεντρωτικό πίνακα με όλες τις λεπτομέρειες από κάθε επίθεση που γίνεται την στιγμή που γίνεται.

Με βάση τη σελίδα αυτή έγινε έρευνα για τον μήνα Ιούνιο, με σκοπό να καταγραφούν οι χώρες με τις περισσότερες επιθέσεις στο ενεργητικό τους και οι χώρες που αποτέλεσαν τους μεγαλύτερους στόχους των επιθέσεων αυτών. Επίσης, καταγράφηκαν και αναλύθηκαν οι τύποι των επιθέσεων που χρησιμοποιήθηκαν περισσότερο το χρονικό διάστημα της έρευνας.

ΚΕΦΑΛΑΙΟ 1 – DARKNET

1.1. Ορισμός

Μια από τις πλέον σκοτεινές πτυχές του internet έφτασε και στην Ελλάδα και μάλιστα με την πιο σκληρή του μορφή. Ο λόγος για το Darknet, ένα «μυστικό διαδίκτυο«, που δημιουργήθηκε στις αρχές της δεκαετίας του 90' από τις αμερικανικές μυστικές υπηρεσίες, προκειμένου να εξασφαλίζεται η μυστικότητα των συνομιλιών στα πλοία του στόλου των ΗΠΑ που ταξίδευαν σε ολόκληρο το κόσμο (Bethencourt, et al, 2007).

Ήταν και παραμένει ένα παράλληλο με το ίντερνετ δίκτυο, το οποίο «σβήνει» αυτόματα την ταυτότητα του χρήστη. Ωστόσο, πολύ γρήγορα αυτό το «σκοτεινό» διαδικτυακό κόσμο, ανακάλυψαν οι παράνομοι σε ολόκληρο το κόσμο, με αποτέλεσμα να περάσει στα χέρια οργανωμένων εγκληματικών οργανώσεων και διακινητών παράνομων υλικών, ακόμα και πυρηνικών αποβλήτων. Πλέον το «σκοτεινό διαδίκτυο», έχει εξελιχθεί σε ένα παράλληλο κόσμο. Τον κόσμο της παρανομίας, καθώς πρόκειται πια για το επίσημο διαδικτυακό τόπο των παρανόμων.

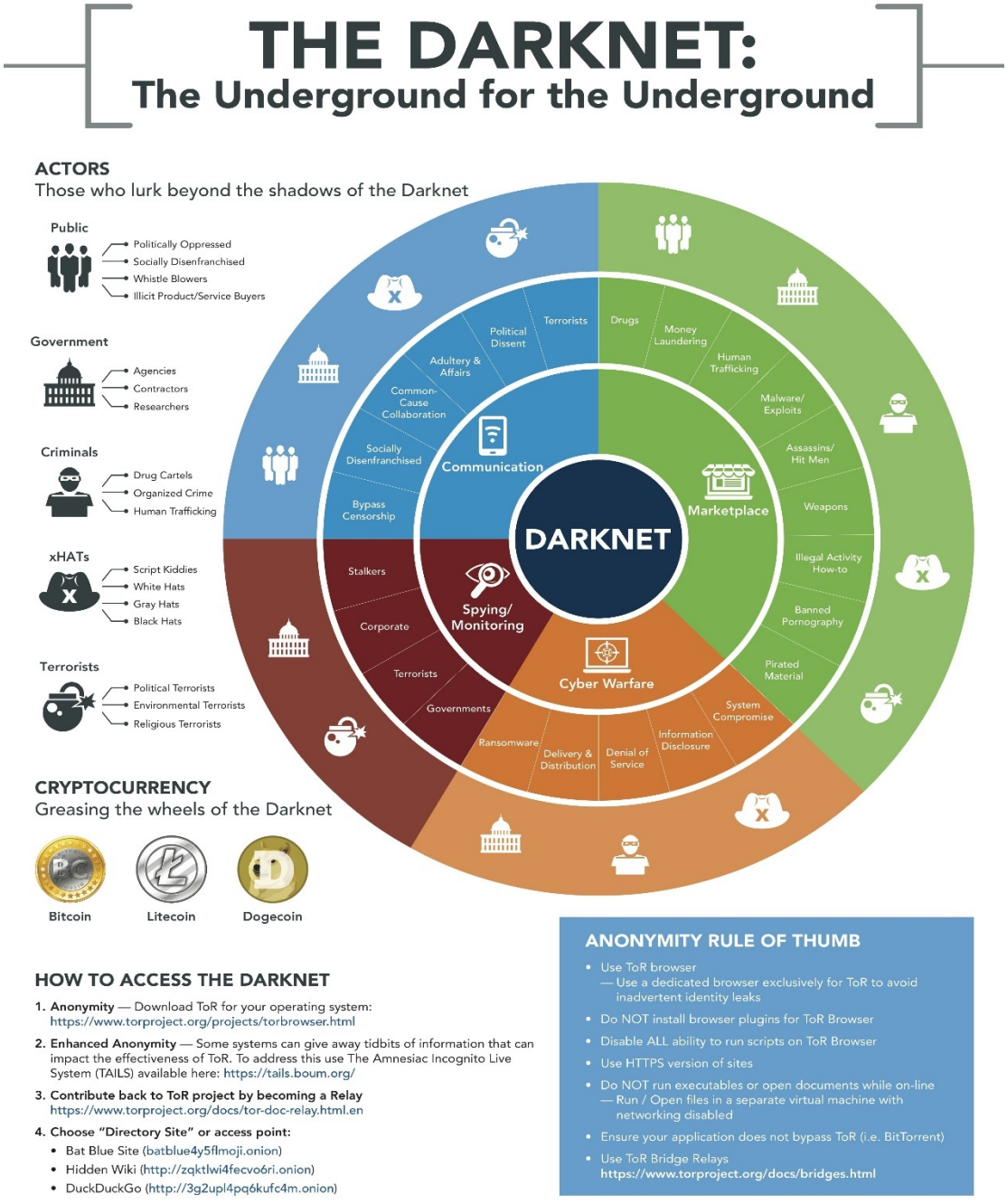
Ο χρήστης του Darknet, είναι ανώνυμος, καθώς η ταυτότητα του υπολογιστή του, το ID δηλαδή, δεν είναι φανερό. Ακόμα και εάν κάποιος ανακαλύψει την ταυτότητα του υπολογιστή του που «περιπλανήθηκε» στο «σκοτάδι», η πραγματική ταυτότητα του χρήστη είναι αλλοιωμένη με αποτέλεσμα την απόλυτη ανωνυμία (Biddle, et al, 2002a).

Οι μαφιόζοι των ΗΠΑ και κυρίως η Ιταλική Μαφία που δραστηριοποιείται στην Αμερική, πολύ γρήγορα έκανε εικόνισμα το «Darknet«, και οι πληρωμένοι εκτελεστές της εγκληματικής οργάνωσης, άρχισαν να κλείνουν τα συμβόλαια θανάτου διεθνώς μέσω του σκοτεινού κόσμου, διατηρώντας απόλυτα την ανωνυμία τους.

Οι βαρόνοι των ναρκωτικών έχουν πια ειδικούς λογαριασμούς στο Darknet και κλείνουν συμφωνίες εκατομμυρίων δολαρίων για την πώληση τους, ενώ οι διακινητές

παιδικού ακατάλληλου υλικού βρήκαν το απόλυτο εργαλείο για να πουλάνε το νοσηρό προϊόν τους (Martin, 2014).

Στο Darknet βρίσκεις ακόμα και υλικό με δολοφονίες παιδιών, αρκεί να έχει μερικές δεκάδες, εκατοντάδες ευρώ η δολάρια για να αγοράσεις το υλικό και πάντα με την ανωνυμία σου εξασφαλισμένη (Roosa & Schultze, 2013).



1.2. Προέλευση

Το darknet είναι ένας παγκόσμιος ιστός πλήρως αυτόνομος. Λειτουργεί παράλληλα με το γνωστό διαδίκτυο και προσφέρει μυστικότητα και ανωνυμία. Η ανίχνευση της ηλεκτρονικής ταυτότητας των χρηστών είναι σχεδόν αδύνατη. Καθιστώντας το ιδανικό εργαλείο για πολλές παράνομες δραστηριότητες.

Ονομάζεται και deepnet ή hidden web. Η ιστορία του darknet ξεκίνησε τη δεκαετία του 70′ από την εποχή του ARPANET, του προγόνου του world wide web. Σύμφωνα με εκτιμήσεις υπολογίζεται ότι ο συνολικός όγκος των δεδομένων του deepnet είναι εκατοντάδες φορές μεγαλύτερος από εκείνον του επιφανειακού διαδικτύου (Von Lohmann, 2004).

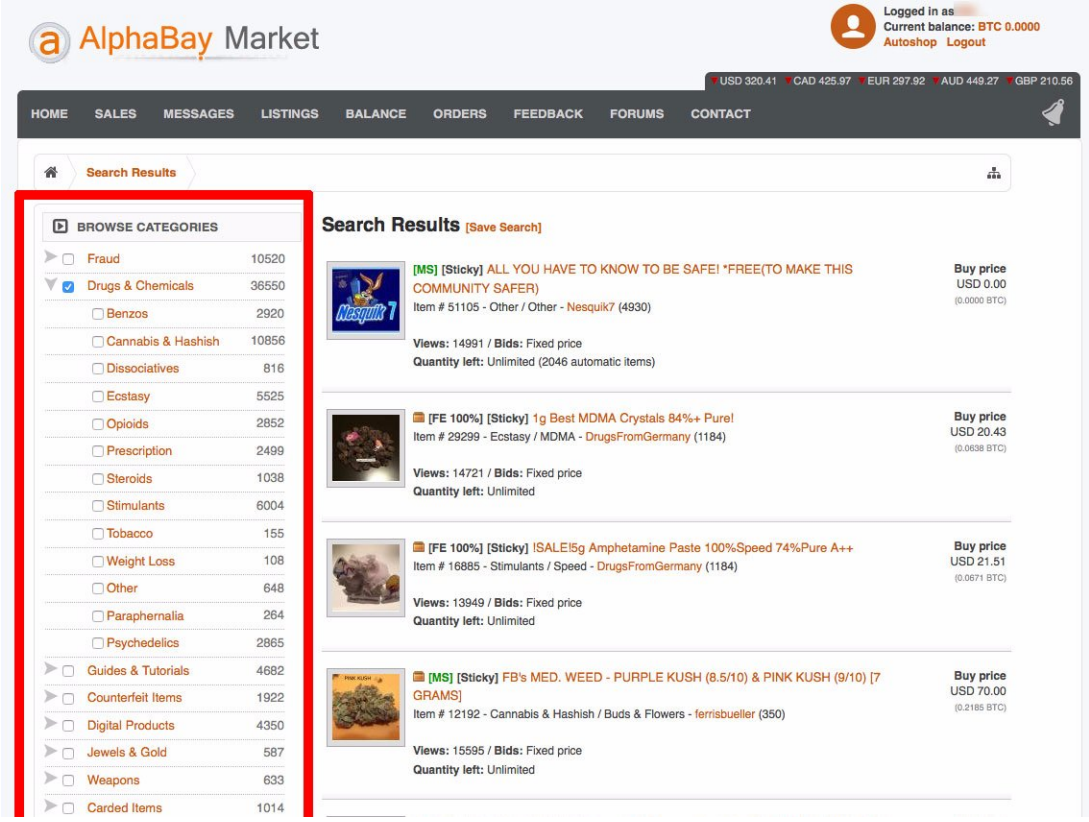
Οι ιστότοποι του deepnet δεν έχουν την μορφή των φιλικών διευθύνσεων του URL. Αποτελούνται από μια φαινομενικά τυχαία σειρά χαρακτήρων και είναι προσβάσιμες από εξειδικευμένες εφαρμογές, με πιο γνωστή αυτή του Tor. Το Tor είναι ένα παγκόσμιο δίκτυο κόμβων μεταφοράς κρυπτογραφημένων δεδομένων. Η επίσκεψη σε μια διεύθυνση του deepnet δεν γίνεται απευθείας όπως στο διαδίκτυο άλλα περνά μέσα από μια τυχαιοποιημένη πορεία υπολογιστών άλλων χρηστών του Tor, εξαφανίζοντας τα ψηφιακά ίχνη του επισκέπτη. Αυτή η πολυπλοκότητα έχει ως επίπτωση την χαμηλή ταχύτητα του δικτύου (Wang, et al, 2011).

Η άκρα μυστικότητα του darknet προσφέρει το ιδανικό καταφύγιο για εμπόρους ναρκωτικών, δίκτυα τρομοκρατίας και ένα ευρύ φάσμα εγκληματικότητας και παράνομου περιεχομένου. Οι μέθοδοι εντοπισμού που χρησιμοποιούν οι διωκτικές υπηρεσίες δεν είναι αποτελεσματικές στο darknet, καθιστώντας το έτσι ουσιαστικά ανεξέλεγκτο (Ban, et al, 2012).

1.3. Χρήσεις

Το κλειδί για να μπει κανείς σε αυτό το παράλληλο web είναι το Tor. Έχουμε μιλήσει αρκετές φορές γι' αυτό και για τις διαφορές του σε σχέση με την συνήθη εμπειρία που έχει χρησιμοποιώντας τις μηχανές αναζήτησης και τις υπηρεσίες που απολαμβάνουμε οι περισσότεροι στο διαδίκτυο.

Το Tor, είναι ουσιαστικά ένα δίκτυο από μηχανήματα εθελοντών που επιτρέπει την ανώνυμη περιήγηση στο διαδίκτυο εφόσον ουσιαστικά, η πληροφορία που στέλνουμε ή λαμβάνουμε χρησιμοποιώντας το, περνά από διάφορα στάδια κρυπτογράφησης και διάφορες διαδρομές, μέχρι τα δεδομένα να φτάσουν στον προορισμό που εμείς θέλουμε, ή να έρθουν σε εμάς από τον προορισμό που έχει επιλέξει (Bailey, et al, 2006).



Το Tor μοιάζει δηλαδή με τα torrents όπου μπορεί κάποιος να κατεβάσει προγράμματα και ταινίες δωρεάν.

Η τυχαιότητα της διαδρομής που θα ακολουθήσει η πληροφορία του, είναι εκείνη που ουσιαστικά διασφαλίζει, τόσο την ανωνυμία στην περιήγησή του, όσο και την δυσκολία σε κάποιον κακόβουλο να παρακολουθήσει τη δραστηριότητά του. Αλλά αυτό δεν είναι της παρούσης. Η ίδια τυχαιότητα όμως και η πρόσβαση στην «υποδομή» του διαδικτύου είναι εκείνη που έχει δημιουργήσει και την τεράστια πηγή πληροφοριών στο Deep Web (Wehinger, 2011).

Το Tor είναι η πύλη για το Deep Web καθώς το δίκτυο λειτουργεί σε όλες τις πλατφόρμες. Αν όμως χρησιμοποιήσει το λογισμικό Tor ή την ιστοσελίδα του δικτύου, θα πρέπει να έχει υπ' όψιν του πως υπάρχει και μία άλλη εναλλακτική, το Tails OS, ένα λειτουργικό που μπορεί κανείς να χρησιμοποιήσει ανά πάσα στιγμή και σε οποιονδήποτε υπολογιστή, εφόσον είναι bootable από DVD (ιδανικά), αν το έχει φορτώσει και το κρατά μαζί του σε ένα memory stick (Roosa & Schultze, 2013).

Θα πρέπει όμως να είμαστε προσεκτικοί σε ότι κάνουμε γιατί το deep web δεν είναι ασφαλές για κάποιον άσχετο χρήστη και κρύβει κινδύνους. Σύμφωνα με έρευνα που δημοσιεύει το techblog, το 80% του deep web traffic αφορά σε παιδική πορνογραφία.

Οι ερευνητές εξέτασαν περίπου 40.000 διαφορετικές υπηρεσίες στο Tor και βρήκαν την τεράστια ζήτηση για παιδική πορνογραφία, αν και τα συγκεκριμένα sites βρίσκονται μόλις στο 2% των διαθέσιμων υπηρεσιών του deep web. Η έρευνα επικεντρώνεται στις κρυμμένες υπηρεσίες, τις λεγόμενες «onion addresses» που είναι διαθέσιμες μόνο από το «inside Tor» (Ban, et al, 2012).

1.4. Λογισμικό

Η anegvjpd77xuxo45.onion/services είναι μία λίστα υπηρεσιών που ελέγχει περιοδικά τις ιστοσελίδες onion τις οποίες αναγνωρίζει, λόγω του ότι βρίσκονται στην λίστα της και ενημερώνει ποιες είναι ψηλά σε αναγνωσιμότητα και ποιες όχι. Πολλοί bloggers επιδιώκουν να μπουν οι ιστοσελίδες τους στην core.onion, δεδομένου ότι είναι καταχωρημένη στις σελίδες του Tor και η γνωστή αμερικανική (προπαγανδιστική για πολλούς) μηχανή Wikipedia. Υπάρχουν ακόμη πολλές σελίδες με «HiddenServices» (κρυμμένες υπηρεσίες) (Wang, et al, 2011).

Η μηχανή αναζήτησης Torgle είναι ένα καλός τρόπος για να ξεκινήσουμε τη βόλτα στο Βαθύ Διαδίκτυο˙ απλά πληκτρολογεί κανείς αυτό που ψάχνει και είναι σχεδόν σίγουρο πως θα έχει άμεσα αποτελέσματα. Γενικότερα, πριν κάνει την οιανδήποτε δημοσίευση, θα πρέπει να το σκεφτεί καλά. Γιατί αυτά που λέει μπορεί να χρησιμοποιηθούν για να προσδιορίζουν ποιος είναι, πού βρίσκεται, ποια είναι τα ενδιαφέροντά του και ούτω καθεξής, ανεξάρτητα από το αν η σύνδεσή είναι ανώνυμη ή όχι.

Μιλάμε για Ανωνυμία προφανώς και όχι για κάτι άλλο. Και επειδή σίγουρα, κάποια στιγμή, θα χρειαστεί κανείς και κάποια εργαλεία κρυπτογράφησης και στο DeepWeb, θα βρει κανείς αρκετά που θα βοηθήσουν στο σχετικό tag: #encrypt.

Σύμφωνα με εκτιμήσεις που έγιναν σε μία μελέτη στο Πανεπιστήμιο Berkeley της Καλιφόρνια (University of California, Berkeley) το 2001, το deep Web αποτελείται περίπου από 91.000 terabytes. Αντίθετα το επιφανειακό Web (που είναι εύκολα προσπελάσιμο από τις μηχανές αναζήτησης) είναι περίπου 167 terabytes. Η Βιβλιοθήκη του Αμερικάνικου Κονγκρέτου, υπολογίστηκε πως το 1997 είχε 3.000 terabytes. Το 2011, το YouTube υπολογίζεται ότι είχε αποθηκευμένα περίπου 200 εκατομμύρια βίντεο, συνολικού μεγέθους 5 petabytes ή 5000 terabytes. Ο υπολογισμός του μεγέθους του web διαφέρει από πηγή σε πηγή και έτσι υπάρχει ένα μεγάλο περιθώριο λάθους και κανένας αριθμός δε μπορεί να θεωρηθεί ως ακριβής. Ωστόσο σχετικά με τον αριθμό των πηγών του deep Web υπάρχουν πιο ακριβείς εκτιμήσεις: Το 2004 ο He ανακάλυψε 300.000 deep web sites σε ολόκληρο το Web και σύμφωνα με τον Shestakov, περίπου 14.000 deep web sites υπήρχαν στο Ρώσικο τμήμα του Web το 2006 (Von Lohmann, 2004).

Οι πληροφορίες του Deep Web ανήκουν σε μία ή περισσότερες από τις παρακάτω κατηγορίες:

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

Μη συνδεδεμένο περιεχόμενο: ιστοσελίδες οι οποίες δεν περιέχουν συνδέσμους από άλλες ιστοσελίδες, εμποδίζοντας έτσι τα προγράμματα που κάνουν Web crawling να επισκεφθούν το περιεχόμενό τους (Bailey, et al, 2006).

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

Περιεχόμενο περιορισμένης πρόσβασης: ιστότοποι που περιορίζουν την πρόσβαση στις σελίδες τους με τεχνικό τρόπο (π.χ. χρησιμοποιώντας το Robots Exclusion Standard, CAPTCHAs, ή το no-cache Pragma στις επικεφαλίδες του πρωτοκόλλου HTTP, τα οποία απαγορεύουν στις μηχανές αναζήτησης να πλοηγούνται στις ιστοσελίδες τους) (Roosa & Schultze, 2013).

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

Κείμενα που χρησιμοποιούν το παλαιότερο πρωτόκολλο Gopher και αρχεία που βρίσκονται σε διακομιστές FTP και τα οποία δεν μπορούν να εντοπιστούν από τις περισσότερες μηχανές αναζήτησης. Οι μηχανές αναζήτησης όπως η Google δεν δεικτοδοτούν ιστοσελίδες που βρίσκονται έξω από το πρωτόκολλο HTTP.

Στην καρδιά του Onionland βρίσκεται το διαβόητο Tor. Φαινομενικά, η τεχνολογία Tor είναι έτσι σχεδιασμένη για να επιτρέπει το σερφάρισμα τον Ιστό με πλήρη ανωνυμία, κωδικοποιώντας τη σύνδεσή του και κρύβοντάς τη κατόπιν επιμελώς μέσω πολλών διασυνδεδεμένων δικτύων πριν φτάσεις τελικά στην τοποθεσία που είναι ο τελικός του προορισμός (Ban, et al, 2012).

Κάθε κόμβος στην κωδικοποιημένη αυτή γυροβολιά γνωρίζει μόνο την ταυτότητα του κόμβου που συνδέεται ευθέως μαζί του και όχι κάθε σύνδεση μεταξύ PC και σέρβερ, την ίδια ώρα που κάθε μεταπήδηση μεταξύ κόμβων διαθέτει τα δικά του κωδικοποιημένα κλειδιά. Ακόμα και αν σε έχει βάλει κάποιος στο διωκτικό στόχαστρο, τα ηλεκτρονικά του ίχνη σβήνονται περιοδικά, κάνοντας την παρακολούθηση της διαδρομής πρακτικά αδύνατη (ή έτσι τουλάχιστον θέλει να πιστεύει η ιστοσελίδα του δικτύου Tor).

Η μεταπήδηση βέβαια μέσα από τόσες διασυνδέσεις κάνει την περιήγηση στον ιστό ιδιαιτέρως αργή, αν όμως λάβει κάποιος μια σειρά ακόμα από επιπρόσθετα μέτρα και προφυλάξεις (που παρέχονται αναλυτικά στους μυημένους), τότε το Tor είναι ένας εξόχως ασφαλής τρόπος να σερφάρει online ανώνυμα. Και κάτι άλλο, ακόμα σημαντικότερο: η τεχνολογία Tor δεν παρέχει πλήρη ανωνυμία μόνο στον χρήστη αλλά και στους σέρβερ, μέσω των απόκρυφων υπηρεσιών, και αυτά είναι τα θεμέλια πάνω στα οποία έχει χτιστεί το Onionland και τα λοιπά Darknets (Von Lohmann, 2004).

1.5. Ασφάλεια

Μπορεί το Darknet να έρχεται στην επικαιρότητα συνήθως με αφορμή αστυνομικές επιχειρήσεις που έχουν στο στόχαστρο «μαύρες αγορές» σαν το Silk Road, ωστόσο αυτό δεν σημαίνει πως είναι απλώς το online ανάλογο του πραγματικού υποκόσμου. «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 (Martin, 2014).

Ενδεικτικά, στο Darknet έχουν κατά καιρούς φιλοξενηθεί αντίγραφα του GlobalLeaks 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 αυτήν που προσφέρουν τα ηλεκτρονικά ταχυδρομεία. Επίσης, η οργάνωση «Δημοσιογράφοι Χωρίς Σύνορα» συμβουλεύει τα μέλη της να το χρησιμοποιούν για να έρχονται σε επαφή με τις πηγές τους, στην περίπτωση που θέλουν να διασφαλίσουν πως θα μείνει μυστική η ταυτότητα όσων επικοινωνούν (Von Lohmann, 2004).

Παράλληλα, σε εργαλεία και υπηρεσίες που βασίζονται στο Tor βρίσκουν «καταφύγιο» απλοί χρήστες που θέλουν να παρακάμψουν τα «φίλτρα» ιντερνετικής λογοκρισίας στη χώρα τους και, όπως είναι φυσικό, πολιτικοί ακτιβιστές. Έτσι, σύμφωνα με την ιστοσελίδα του The Tor Project, το Darknet κατακλύσθηκε από μπλογκ κατά τη διάρκεια της «Αραβικής Άνοιξης», από ανθρώπους που συμμετείχαν

στις εξεγέρσεις και ήθελαν να μεταφέρουν στο εξωτερικό τη μαρτυρία τους. Δυνατότητες που, όπως σημειώνει ο συντάκτης του PC World, δεν θα μπορούσαν να γίνουν πραγματικότητα, αν το Σκοτεινό Διαδίκτυο δεν προσέφερε ένα επίπεδο ασφάλειας το οποίο δυστυχώς το κάνει ελκυστικό και σε εγκληματίες (Biddle, et al, 2002a).

Μόλις κατεβάσει κανείς το αντίστοιχο λογισμικό Tor Browser Bundle, έχει πια στα χέρια του όλα όσα χρειάζεται κανείς για να καταβυθιστεί στο Onionland, αν και πρέπει να πάρει μια σειρά από προφυλάξεις. Κανείς δεν θέλει εξάλλου να τσαλαβουτήσει στο Darknet ανέτοιμος, καθώς πολλοί είναι αυτοί που καραδοκούν για τους ερασιτέχνες και τους πρωτόβγαλτους, αφού μιλάμε για όπλα, ναρκωτικά, κάθε είδους πορνογραφία και όλο το έγκλημα που μπορεί να προσφέρει ο τεχνολογικός μας κόσμος (ηλεκτρονικό και πραγματικό, καθώς μέχρι και συμβόλαια θανάτου κανονίζονται εκεί μέσα) (Wehinger, 2011).

Εδώ όμως δεν θα κάνουμε σεμινάριο καταβύθισης στις παρυφές του ίντερνετ, αρκεί πάντως να αναφέρουμε ότι το Tor από μόνο του δεν αρκεί για να σερφάρει κανείς πλήρως ανώνυμα και ασφαλώς. Κι αν πρέπει να τονιστεί, δεν μοιράζεται κανείς ποτέ προσωπικές πληροφορίες με κανέναν χρήστη ή ιστοσελίδα του Darknet. Δεν χρησιμοποιεί ίδια passwords με αυτά που έχει κανείς στο ίντερνετ και η πιστωτική

κάρτα απαγορεύεται διά ροπάλου: εδώ έχει τα Bitcoins να κάνει τις συναλλαγές, καθώς μιλάμε για πραγματική (αν και ψηφιακή) Άγρια Δύση (Roosa & Schultze, 2013).

Αλλά και με τα ψηφιακά νομίσματα θέλει προσοχή, καθώς η ανωνυμία των Bitcoins και του ίδιου του Darknet κάνει το Onionland παράδεισο για κάθε απατεώνα και τυχοδιώκτη. Τα μέτρα προφύλαξης είναι μεν πολλά, απαραίτητα δε για ασφαλή περιήγηση, καθώς όπως είπαμε το Darknet παραμένει άκρως επικίνδυνο στον αμύητο.

Το Darknet δεν είναι για τον καθένα. Οι πιθανότητες λένε ότι δεν θα χρειαστεί ποτέ να περιηγηθεί κανείς στον Deep web καθώς το ίντερνετ παρέχει όλες τις υπηρεσίες και τα εργαλεία που χρειάζεται κανείς στην καθημερινότητά του. Εκεί άλλωστε δεν θα βρεί υπηρεσίες streaming video ή κοινωνικά δίκτυα ή εταιρικές ιστοσελίδες που δεν συναντά στον Κανονικό Ιστό (Bailey, et al, 2006).

Είπαμε ότι το Darknet δεν είναι μόνο γεμάτο από εμετικό περιεχόμενο και άκρως παράνομες δραστηριότητες, όντας το σημείο συνάντησης οργανωμένου εγκλήματος και τρομοκρατών, αλλά και με άπειρους απατεώνες που καραδοκούν συνεχώς στη γωνιά για ανυποψίαστους και πρωτόβγαλτους στο σπορ χρήστες. Αν πάντως το χρειαστεί κανείς για κάποιον ευγενή σκοπό, αν η φωνή του καταπιέζεται για παράδειγμα, τότε ας είναι σίγουρος ότι η πραγματική ανωνυμία του σκοτεινού ίντερνετ και η ασφάλεια στην επικοινωνία παραμένει αξεπέραστη (Bethencourt, et al, 2007).

ΚΕΦΑΛΑΙΟ 2 – ΤΟ INTERNET, ΤΟ DEEP WEB ΚΑΙ ΤΟ DARK WEB

2.1. To Dark web

Με τους πιο βασικούς τεχνικούς όρους, το Dark Web αποτελείται από έναν σχετικά μικρό αριθμό websites, σε σχέση με το κανονικό Web, τα οποία, α) δεν είναι ορατά στις μηχανές αναζήτησης (αφού είναι κρυπτογραφημένα), και β) για να τα προσπελάσει κάποιος χρειάζεται να διαθέτει έναν ειδικό browser όπως τον Tor, ο οποίος αποκρύπτει την IP διεύθυνσή του. Από τη στιγμή που θα βρεθεί κάποιος, μέσω του Tor, στο επονομαζόμενο Dark Web, γίνεται ιδιαίτερα δύσκολο να προσδιορίσει ποιος ή τι άλλο βρίσκεται στο δίκτυο - κάτι που αποτελεί και τον ίδιο το σκοπό της ύπαρξής του. Κι αυτό ακριβώς το χαρακτηριστικό είναι που κάνει το Dark Web ιδιαίτερα δημοφιλές σε όσους επιθυμούν να διατηρήσουν κρυφή την ταυτότητά τους, όπως οι διακινητές υλικού παιδικής πορνογραφίας ή ναρκωτικών. Φυσικά και οι δύο αυτές δραστηριότητες είναι παράνομες και ιδίως στην περίπτωση της παιδικής πορνογραφίας η εξαχρείωση φτάνει σε τρομακτικά επίπεδα. Όμως, ανάμεσα στους όψιμους εξερευνητές του Dark Web κυριαρχεί η αντίληψη ότι το "Σκοτεινό Διαδίκτυο", γίνεται χειρότερο όσο εμβαθαίνουν. Σε τελική ανάλυση, πρόκειται για ένα μέρος όπου συγκεντρώνει χιλιάδες ανθρώπους από όλο τον κόσμο, οι οποίοι κάνοντας χρήση της κρυπτογραφημένης, ψηφιακά οχυρωμένης ανωνυμίας μπορούν να μοιραστούν μεταξύ τους ό,τι επιθυμούν (Berthier & Cukier, 2008).

Άλλες φήμες μιλούν για την προσφορά συμβολαίων θανάτου με πληρωμένους δολοφόνους, ή την προσφορά ατόμων που προσφέρονται να γίνουν σκλάβοι ή 'living dolls' έναντι γενναίου αντιτίμου. Από όλους τους μύθους και θρύλους που κυκλοφορούν για το Dark Web, ο πιο επίμονος είναι αυτός των "Red Rooms". Πρόκειται για τοποθεσίες όπου μεταδίδονται live δολοφονίες και βιασμοί και στη συνέχεια αποθηκεύονται για μετέπειτα θέαση Λίστα με μερικές από τις υπηρεσίες που υποτίθεται ότι προσφέρει προμηθευτής του Dark Web με το ψευδώνυμο 'Old Man Fixer'.

Η δημοσιογράφος της Washington Post αναφέρει ότι σε σάϊτ όπως το Reddit, το 4Chan και το Hidden Wiki συμβαίνει ένα ιδιότυπο αλισβερίσι λογαριασμών από δεύτερο, τρίτο ή τέταρτο χέρι από φερόμενα ως ενεργά (ή και ανενεργά) Red Rooms. "Πρόκειται για μια κουραστικά κοινότοπη ερώτηση", γράφει η Αυστραλή δημοσιογράφος, Eileen Ormsby, που βρίσκεται πίσω από το σάιτ "All Things Vice", που αφορά στο Dark Web: "Πώς μπορώ να πάω ακόμα πιο βαθιά στο Dark Web; Πού βρίσκεται το πιο σκοτεινό υλικό του;" Η απάντηση, αναφέρει η Ormsby, είναι απλή: το "πιο σκοτεινό υλικό του Dark Web" ούτε υπάρχει, αλλά ούτε και υπήρξε ποτέ. Εξαίρεση αποτελεί φυσικά το υλικό παιδικής πορνογραφίας, αλλά αυτό είναι κάτι που αφήνει αδιάφορους όσους ψάχνουν για τον βόρβορο του Dark Web (Wang, et al, 2011).

Η δημοσιογράφος Caitlin Dewey της Washington Post, πάντως, τονίζει ότι υπάρχουν αρκετά, ασφαλή στοιχεία που επαληθεύουν το συμπέρασμα της Ormsby, περί της μη ύπαρξης όλων αυτών των ειδεχθών σεναρίων. Κυρίαρχο στοιχείο αποτελεί ότι δεν υπάρχει κανένα απτό στοιχείο ύπαρξης των Red Rooms ή των πληρωμένων δολοφόνων, παρά τα ολοένα και συχνότερα "πεσίματα" του FBI που δεν έχουν να αναφέρουν ούτε μία σχετική σύλληψη.

Πειστικότερο όλων είναι το άρθρο ενός Βρετανού ερασιτέχνη κρυπτογράφου, ονόματι Cthulhu, ο οποίος αναλύοντας τους σερβερς φερόμενων ως πληρωμένων χάκερ και φονιάδων διαπίστωσε ότι είναι διάτρητοι από άποψη ασφάλειας — γεγονός που συντείνει στην άποψη ότι πρόκειται περί απατεώνων που εισπράττουν ποσά για τις υποτιθέμενες υπηρεσίες τους και στη συνέχεια γίνονται καπνός. Το πιθανότερο είναι να συμβαίνει το ίδιο και με το Red Room με τα υποτιθέμενα μέλη της ISIS. Ύστερα από όλο αυτό το hype, για το οποίο ευθύνονται εν πολλοίς διάφοροι φαντασιόπληκτοι κι αργόσχολοι χρήστες του Reddit, η σελίδα εξαφανίστηκε ως δια μαγείας, την ώρα που είχε προγραμματιστεί να ξεκινήσει ο υποτιθέμενος βασανισμός (Biddle, et al, 2002b).

Η σελίδα, επέστρεψε με ένα ευχαριστήριο μήνυμα προς όσους "πειραγμένους" ανυπομονούσαν να δουν ένα snuff movie σε πραγματικό χρόνο, παρουσιάζοντας ένα βίντεο διάρκειας 21 λεπτών με έναν τύπο που υποτίθεται ότι τον ταΐζουν μπέικον με το ζόρι. Υποτιθέμενος τιμοκατάλογος, πληρωμένου δολοφόνου, που αναλύει διεξοδικά τις "υπηρεσίες" του Φυσικά, καταλήγει το άρθρο των NYT, αυτό δε σημαίνει ότι δεν υπάρχει πραγματικά ενοχλητικό, ακραίο ή παράνομο περιεχόμενο στο Dark Web.

Σε πρόσφατο βιβλίο επί του θέματος, ο συγγραφέας Jamie Bartlett καταγράφει περιστατικά αυτοκτονιών, ακραίας παιδικής πορνογραφίας, εμπορίου όπλων, ναρκωτικών και άλλων παράνομων ουσιών καθώς και αρκετού νεοναζισμού και bullying μεταξύ άλλων. Αλλά αυτά είναι υλικά που μπορεί να βρει κανείς και στο mainstream, 'παραδοσιακό', μη σκοτεινό Web. Κι έτσι απ' ό,τι φαίνεται το Dark Web, δεν οδηγεί σε κάποια σκοτεινότερα μονοπάτια από αυτά που μπορεί να βρει κανείς online, με λίγο ψάξιμο, ανά πάσα στιγμή. Ας μην ξεχνάμε ότι πέραν από τα σημεία και τέρατα που κατά καιρούς ακούγονται για το υπερ-δαιμονοποιημένο Dark Web, ο βαθμός κρυπτογράφησής του, επιτρέπει να πραγματοποιούνται με ασφάλεια επικοινωνίες μεταξύ πολιτών σε καταπιεστικά καθεστώτα και διευκολύνει την κυκλοφορία εγγράφων που οδηγούν σε αποκαλύψεις τύπου Snowden, όπως αναφέρει το άρθρο του WIRED, με τίτλο "Οδηγός για την φωτεινή πλευρά του Dark Web" (Berthier & Cukier, 2008).

2.1.1. Ορολογία

Το Dark Web δεν είναι το Deep Web και δεν αντιπροσωπεύει το 90% του Διαδικτύου. Υπάρχει μια σύγχυση ανάμεσα στο λεγόμενο Deep Web και το Dark Web.

Το Deep Web είναι μια τεράστια συλλογή όλων των sites του διαδικτύου που δεν είναι προσβάσιμα από τις μηχανές αναζήτησης. Αυτές οι unindexed ιστοσελίδες περιλαμβάνουν τεράστιους όγκους περιεχομένου, όπως forums που απαιτείται εγγραφή, δυναμικές ιστοσελίδες, υπηρεσίες σαν το Gmail και πολλά άλλα. Το πραγματικό Dark Web αντίθετα, πιθανόν αντιπροσωπεύει λιγότερο από το 0,01% του web: αναφέρει ο ερευνητής ασφαλείας Nik Cubrilovic που μετρήσε 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 (Roosa & Schultze, 2013).

Αν και το Dark Web συχνά συνδέεται με την πώληση των ναρκωτικών, όπλων, πλαστών εγγράφων και παιδικής πορνογραφίας, όλες οι ιστοσελίδες χρησιμοποιούν την υπηρεσία Tor και δεν περιέχει μόνο τόσο «σκοτεινές» ιστοσελίδες όσο το θέλει η ονομασία. Την ίδια υπηρεσία χρησιμοποιεί και μια από τις πρώτες σελίδες υψηλού προφίλ του Dark Web, το Tor WikiLeaks, μια κρυφή υπηρεσία που δημιουργήθηκε για να δεχτεί διαρροές από ανώνυμες πηγές. Αυτή η ιδέα έχει προσαρμοστεί από τότε σε ένα εργαλείο που ονομάζεται SecureDrop, ένα λογισμικό που ενσωματώνει τις κρυφές υπηρεσίες του Tor με οποιοδήποτε ειδησεογραφικό οργανισμό λαμβάνει ανώνυμες υποβολές. Ακόμα και το Facebook όπως αναφέραμε την προηγούμενη βδομάδα, ξεκίνησε μια ιστοσελίδα στο Dark Web με στόχο την καλύτερη προστασία (.) σε χρήστες που επισκέπτονται την ιστοσελίδα με Tor για να αποφύγουν την επιτήρηση και τη λογοκρισία (Biddle, et al, 2002a)

2.1.2. Περιεχόμενο

Σύμφωνα με τον συγγραφέα του άρθρου Andy Greenberg το Dark Web αντιπροσωπεύει το 0.01% του Web και όχι το 90% όπως συχνά αναφέρουν blogs και Media. Συνεχίζοντας αναφέρει:

Το Dark Web δεν είναι ιδιαίτερα μεγάλο, δεν είναι το 90% του Διαδικτύου, και δεν είναι ιδιαίτερα μυστικό. Στην πραγματικότητα, το Dark Web είναι μια συλλογή από ιστοσελίδες που είναι ορατές στο κοινό, αλλά κρύβουν τις διευθύνσεις IP των servers που τις τρέχουν. Αυτό σημαίνει ότι ο καθένας μπορεί να επισκεφθεί το Dark Web, αλλά μπορεί να είναι πολύ δύσκολο να καταλάβει πού φιλοξενείται, ή από ποιον (Von Lohmann, 2004).

Η πλειονότητα των ιστοσελίδων στο Dark Web χρησιμοποιούν το λογισμικό ανωνυμίας Tor, αν και ένας μικρότερος αριθμός, χρησιμοποιεί ένα παρόμοιο εργαλείο που ονομάζεται I2P. Και τα δύο αυτά συστήματα κρυπτογραφούν την κυκλοφορία του Ιστού σε στρώματα και την πετάνε σε τυχαία επιλεγμένους υπολογιστές σε όλο τον κόσμο. Ο καθένας από αυτούς τους servers αφαιρεί ένα από τα στρώματα της ενιαίας κρυπτογράφησης πριν περάσει τα δεδομένα στον επόμενο server. Στη θεωρία, αυτό είναι που εμποδίζει κάθε κατάσκοπο, ακόμα και αυτούς που ελέγχουν έναν από αυτούς τους servers που μοιράζουν τα κρυπτογραφημένα δεδομένα, να καταλάβει την προέλευση της κίνησης και τον προορισμό της (Bartlett, 2014).

Έτσι οι διευθύνσεις IP των εν λόγω ιστοσελίδων διατηρούνται κρυφές, κάτι όμως που δεν σημαίνει ότι είναι κατ ‘ανάγκη μυστικές. Κρυμμένες υπηρεσίες στο Tor, όπως τα sites που πωλούν ναρκωτικά Silk Road, Silk Road 2, Agora και Evolution είχαν εκατοντάδες χιλιάδες τακτικούς χρήστες. Έτσι η διεύθυνση κάθε άλλο από μυστική ήταν. Όποιος τρέχει Tor και ξέρει το url ενός site, (τελειώνει σε «.onion») μπορεί εύκολα να επισκεφθεί τις παράνομες online αγορές.

2.1.3. Τα botnets

Ως botnet ορίζεται ένα δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως από τον λεγόμενο botmaster χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται τεχνικά νεκρούς.

Ο botmaster μπορεί να χρησιμοποιεί αυτούς τους υπολογιστές-τεχνικά νεκρούς για διάφορους παράνομους σκοπούς. Καθώς μπορεί να έχει πρόσβαση στον κάθε υπολογιστή-τεχνικά νεκρούς σαν να βρισκόταν ο ίδιος μπροστά σε αυτόν, είναι δυνατή τόσο η πρόσβαση στα αρχεία του συστήματος όσο και η χρήση της σύνδεσης δικτύου του υπολογιστή, χωρίς να το αντιληφθεί ο ιδιοκτήτης του (Wehinger, 2011).

Αυτό του δίνει αμέτρητες δυνατότητες. Πέρα από την υποκλοπή δεδομένων, η πρόσβαση στους υπολογιστές-τεχνικά νεκρούς επιτρέπει και την απόκρυψη της ταυτότητας του δράστη, καθώς ως διακομιστής μεσολάβησης χρησιμοποιείται ο υπολογιστής του θύματος. Ανάλογα με το μέγεθος του botnet, ο δράστης μπορεί να αλλάζει σε ορισμένες εξαιρετικές περιπτώσεις τη διεύθυνση IP του ακόμη και ανά δευτερόλεπτο, ώστε να μπορεί να προβαίνει σε παράνομες ενέργειες μέσω των συνδέσεων των θυμάτων του. Επιπλέον, ο εξ αποστάσεως έλεγχος των υπολογιστών εξυπηρετεί ιδανικά τη μετάδοση του κακόβουλου κώδικα bot ή τη μαζική αποστολή spam (Roosa & Schultze, 2013).

Αναλογιζόμενοι το μέγεθος ενός τυπικού botnet, που αποτελείται από μερικές εκατοντάδες έως περισσότερες χιλιάδες υπολογιστές-ζόμπι, δεν μπορεί κανείς παρά να σκεφτεί μια περαιτέρω εφαρμογή των στρατιών των botnet: τη χρήση τους ως όπλο για την εκτέλεση των λεγόμενων επιθέσεων DDoS (Distributed Denial of Service). Στην περίπτωση αυτοί, οι διακομιστές web ή αλληλογραφίας που βρίσκονται στο στόχαστρο "γονατίζουν" υπό το βάρος μαζικών αιτημάτων σύνδεσης. Με τον κατάλληλο αριθμό ζόμπι, ο διακομιστής θα τεθεί εκτός λειτουργίας. Η μέθοδος αυτή ανοίγει την πόρτα για εγκληματικές ενέργειες όπως εκβιασμούς (Bailey, et al, 2006).

Επίσης δημοφιλής είναι η χρήση των υπολογιστών-ζόμπι ως διακομιστές web ή FTP. Αυτό μπορεί να εξυπηρετεί διάφορους σκοπούς: αφενός στη διάθεση μολυσμένων τοποθεσιών web με σκοπό την παροχή περαιτέρω πληροφοριών, αφετέρου στη χρήση των συστημάτων ανυποψίαστων θυμάτων για την αποθήκευση πορνογραφίας, πειρατικών αντιγράφων, κ.λπ.

Η διαχείριση και ο συντονισμός των υπολογιστών-ζόμπι, που πιθανόν είναι διασκορπισμένοι ανά την υφήλιο, μπορεί να γίνει με διάφορους τρόπους. Ενώ στα πρώτα botnets χρησιμοποιούνται κεντρικοί διακομιστές εντολών και ελέγχου, σήμερα προτιμώνται όλο και περισσότερο αποκεντρωμένες δομές επικοινωνίας, οι οποίες μοιάζουν με τα γνωστά δίκτυα P2P (Peer-to-Peer). Αυτό κάνει ακόμη δυσκολότερο το κλείσιμο ενός botnet, διότι δεν υπάρχει κεντρικός διακομιστής, του οποίου η απενεργοποίηση θα διέκοπτε τη λειτουργία ολόκληρου του δικτύου. Αντί αυτού όλα τα ζόμπι επικοινωνούν απευθείας μεταξύ τους, γεγονός που προσδίδει στο botnet πολύ μεγαλύτερη σταθερότητα (Berthier & Cukier, 2008).

Τα botnets μπορούν να στρατολογούν νέα ζόμπι με διάφορους τρόπους. Εκτός από την εξάπλωση μέσω μολυσμένων e-mail, για την ανάπτυξη ενός botnet μπορούν να χρησιμοποιηθούν και τοποθεσίες web των οποίων τον έλεγχο έχουν αναλάβει χάκερς, εκμεταλλευόμενοι κενά ασφαλείας σε λειτουργικά συστήματα ή λογισμικό εφαρμογών, με αποτέλεσμα τη λεγόμενη "drive-by-infection" δηλαδή, μόλυνση με απλή επίσκεψη. Μια απλή επίσκεψη στη μολυσμένη τοποθεσία web αρκεί για τη μετάδοσή της.

Τα botnets έχουν εξελιχθεί σε μια από τις μεγαλύτερες παράνομες πηγές εσόδων στο Internet. Αφενός με τις ποσότητες των δεδομένων που γίνονται λεία στα χέρια επιτηδείων, αφετέρου με την ενοικίαση botnets σε τρίτους με ωριαία ή μηνιαία ή εφάπαξ χρέωση, π.χ. βάσει του αριθμού της αλληλογραφίας spam που αποστέλλεται μέσω του botnet (Ban, et al, 2012).

2.1.4. Υπηρεσίες Bitcoin

Λίγες ώρες μετά το κλείσιμο από το FBI του Silk Road 2.0, του deep web παράνομου ιστότοπου πώλησης ναρκωτικών, ήδη έχει δημιουργηθεί και τρίτο σάιτ, όπου όποιος θέλει, με την χρήση bitcoin, μπορεί να αγοράσει ναρκωτικά. Ο 26χρονος Blake Benthall, συνελήφθη την Τετάρτη στο Σαν Φρανσίσκο κατηγορούμενος ότι βρίσκεται πίσω από το Silk Road 2.0.

Όμως, σύμφωνα με τις αρχές, ώρες μετά την σύλληψή του μία άλλη έκδοση του Silk Road δημιουργήθηκε. Το πρώτο Silk Road, γνωστό και ως το eBay ή το Amazon των ναρκωτικών, έκλεισε τον Οκτώβριο του 2013.

Οι διωκτικές αρχές σε ΗΠΑ και Ε.Ε. «κατέβασαν» συνολικά 414 ιστοσελίδες με κατάληξη «.onion» και συνέλαβαν 17 άτομα, σε μεγάλη διακρατική επιχείρηση εναντίον της διακίνησης ναρκωτικών στο Ίντερνετ, χθες και προχθές. Η επιχείρηση στέφθηκε από επιτυχία παρά το γεγονός ότι η διακίνηση γινόταν με τη βοήθεια λογισμικού Tor, που υπόσχεται την ανωνυμία των χρηστών. Οι Αρχές δεν αποκαλύπτουν αν διαθέτουν πρόσβαση στο Tor ή αν οι έρευνες ευοδώθηκαν χάρη στην αστυνομική δουλειά που έγινε για τον εντοπισμό των υπόπτων εκτός Ίντερνετ (Wang, et al, 2011).

2.1.5. Αγορές darknet

Στο DEEPNET υπάρχει το “The Hidden Wiki” που παρέχει καταχωρήσεις των διευθύνσεων URL για να διευκολυνθεί η χρήση του DEEPNET. Εδώ είναι μια επιλογή των δικτυακών τόπων που αναφέρονται:

Banker & Co - Professional Service για Ξέπλυμα Βρώμικου Χρήματος

Paypal4free - Hacked Paypal λογαριασμοί προς πώληση

Eris – #1 Deepweb Dealer - παρέχει πρόσβαση για αγορά κάνναβης, LSD, DMT, μανιτάρια, MDMA και οποιουδήποτε άλλου ναρκωτικού.

All Purpose Identities - Ψεύτικες ταυτότητες για ΗΠΑ και Καναδά, άδειες, διαβατήρια και άλλα πολλά

Rent-a-Hacker - Επαγγελματίες hackers προς ενοικίαση, DDOS, hacking, για καταστροφή sites, κατασκοπεία κλπ.

Contract Killer - Σκοτώστε το πρόβλημά μας (καταδότης, paparazzi, πλούσιο άντρα, αστυνομικό, δικαστή, ανταγωνιστή, κλπ). (Host: FH)

Crime Network - για εγκλήματα γενικότερα. Το πραγματικά τρομακτικό περιεχόμενο δεν είναι αυτό που βλέπουμε στο DEEPNET. Όσο βαθύτερα βουτήξουμε στις ιστοσελίδες του τόσο πιο σκούρο γίνεται το περιεχόμενο του. Έχει υπάρξει πολλή συζήτηση ως προς το κατά πόσο το Tor μπορεί να κρατήσει τις online δραστηριότητές μας ανώνυμες. Έχουμε ήδη δει πώς σελίδες του Tor που πουλούσαν ναρκωτικά έκλεισαν από τις αρχές ή πως το FBI εμπόδισε την κακοποίηση παιδιών μέσω παρόμοιων ιστοσελίδων του DEEPNET. Η προσπάθεια όμως που απαιτείται από τους φορείς επιβολής του νόμου να παρακολουθήσουν χρήστες του Tor είναι πάρα πολύ δύσκολη έως και ανέφικτη (Roosa & Schultze, 2013).

Όπως μπορεί να φανταστεί κανείς, τα παρανόμως αποκτηθέντα δεδομένα δεν είναι δυνατό να διακινηθούν μέσα από καταστήματα του ίντερνετ, όπου έχει πρόσβαση ο οποιοσδήποτε. Για τις δουλειές αυτές, οι ιντερνετικοί φαντομάδες, έχουν βρει μια πολύ πιο φιλόξενη και δύσκολα προσβάσιμη γωνιά του διαδικτύου.

Αυτό είναι το «Σκοτεινό Δίκτυο» (Dark Web), μια μικρή περιοχή του «Βαθύ Ιστού» (Deep Web), που είναι προσβάσιμο μονό μέσω του Tor Onion και οι σελίδες εκεί δεν είναι ανιχνεύσιμες από τις μηχανές αναζήτησης. Στο Dark Web υπάρχουν πάρα πολλά sites αγορών απ’ όπου διακινούνται τα προσωπικά δεδομένα που έχουν κλαπεί (Von Lohmann, 2004). Ο αγοραστής αφού αποκτήσει πρόσβαση (πράγμα όχι εύκολο), μπορεί να περιηγηθεί στα λογής-λογής καταστήματα, να βρει και να αγοράσει ό,τι τον ενδιαφέρει. Οι συναλλαγές γίνονται σχεδόν αποκλειστικά με το ψηφιακό νόμισμα Bitcoin, ώστε να μην μπορεί να εντοπιστούν εύκολα πωλητές και αγοραστές.

Αν και για τα θύματα, η απώλεια των προσωπικών τους στοιχείων είναι μια άκρως άβολη κατάσταση, οι κυβερνο-εγκληματίες τα διακινούν σε εξευτελιστικές τιμές. Τα προσωπικά στοιχεία διακινούνται προς περίπου 1 δολάριο ανά γραμμή δεδομένων. Κάθε γραμμή δεδομένων περιλαμβάνει όνομα, πλήρη διεύθυνση, ημερομηνία γέννησης, αριθμό Κοινωνικής Ασφάλισης και άλλα προσωπικά στοιχεία. Εάν κάποιος αγοράσει μερικές γραμμές, μπορεί να διαπράξει αρκετά σοβαρές απάτες (Berthier & Cukier, 2008).

Σύμφωνα μάλιστα με την Trend Micro, η κάθε γραμμή παλιότερα στοίχιζε 4 δολάρια, όμως καθώς οι κλοπές δεδομένων έχουν πληθύνει, η προσφορά έχει αυξηθεί, με αποτέλεσμα την πτώση των τιμών. Με άλλα λόγια, οι κλασικοί κανόνες της καπιταλιστικής οικονομίας εφαρμόζονται και στην αγορά του υπόκοσμου

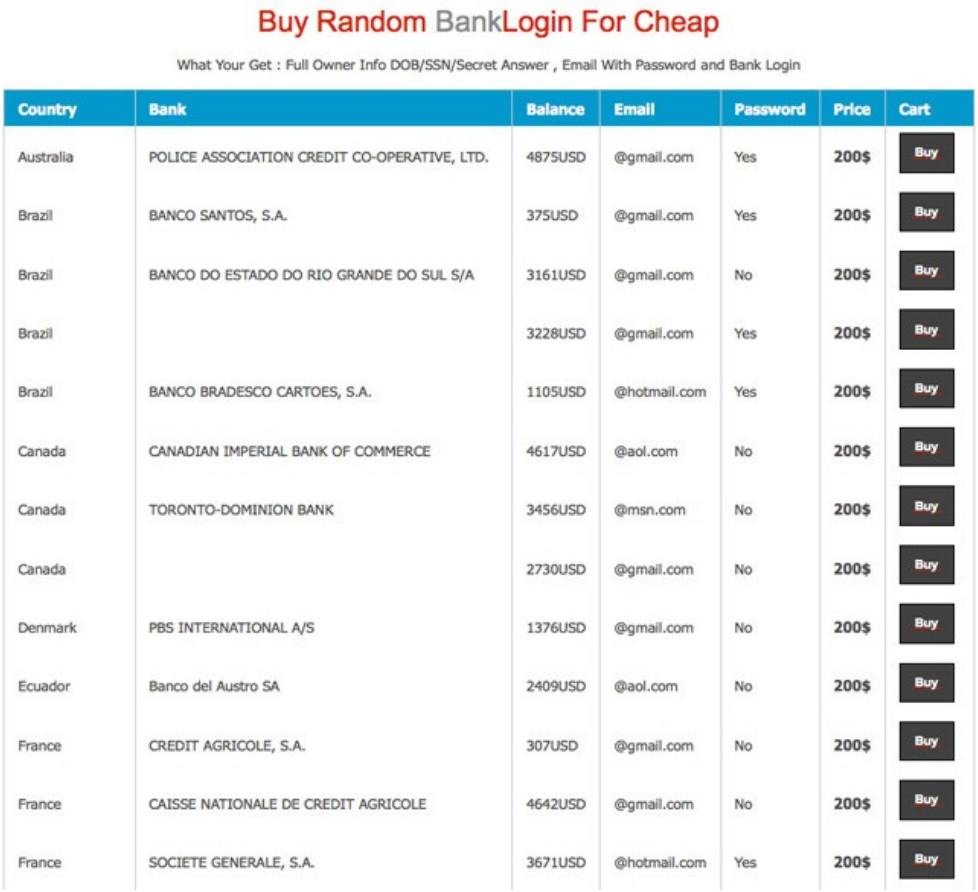
2.2.6. Υπηρεσίες τραπεζικής εξαπάτησης

Όπως είναι προφανές, οι τραπεζικοί λογαριασμοί, αποτελούν ένα σαφώς πιο πολύτιμο και άρα πιο ακριβό προϊόν στον «dark web». Τα στοιχεία κάθε λογαριασμού πωλούνται από 200 έως 500 δολάρια. Όσο μεγαλύτερο το πιστωτικό υπόλοιπο του λογαριασμού, τόσο ακριβότερα θα πωληθεί. Μάλιστα, στα παράνομα στέκια του «Deep Web», κυκλοφορεί πληθώρα λογαριασμών από τη Βραζιλία, μιας και το παράνομο λογισμικό τραπεζών αποτελεί ένα σημαντικό πρόβλημα στη χώρα αυτή.

Μετά την αγορά των τραπεζικών στοιχείων, οι παράνομες μεταφορές χρημάτων γίνονται μέσω offshore λογαριασμών. Η Ryanair στην Ιρλανδία έπεσε θύμα μιας τέτοιας παράνομης μεταφορών χρημάτων τον Απρίλιο του 2015, όταν 4,2 εκατ. ευρώ αφαιρέθηκαν ηλεκτρονικά από έναν τραπεζικό λογαριασμό της, περνώντας από κινεζικές τράπεζες. Πρόκειται βέβαια για μια απάτη μεγάλης έκτασης, με τις αρχές να βρίσκουν γρήγορα τα ίχνη των εγκληματιών και να εντοπίζουν τα ποσά, τα οποία άμεσα «πάγωσαν» (Roosa & Schultze, 2013).

Έτσι, όσοι αγοράσουν τραπεζικά δεδομένα δεν θα επιχειρήσουν μια τόσο μεγάλη μεταφορά. Αντίθετα, θα προχωρήσουν στην αφαίρεση μικρότερων ποσών, σε βάθος χρόνου, τα οποία και θα μοιράσουν σε διαφορετικούς λογαριασμούς σε διάφορες

χώρες, ώστε να η διαδικασία εντοπισμού των χρημάτων να γίνει πιο δύσκολη (Biddle, et al, 2002b).

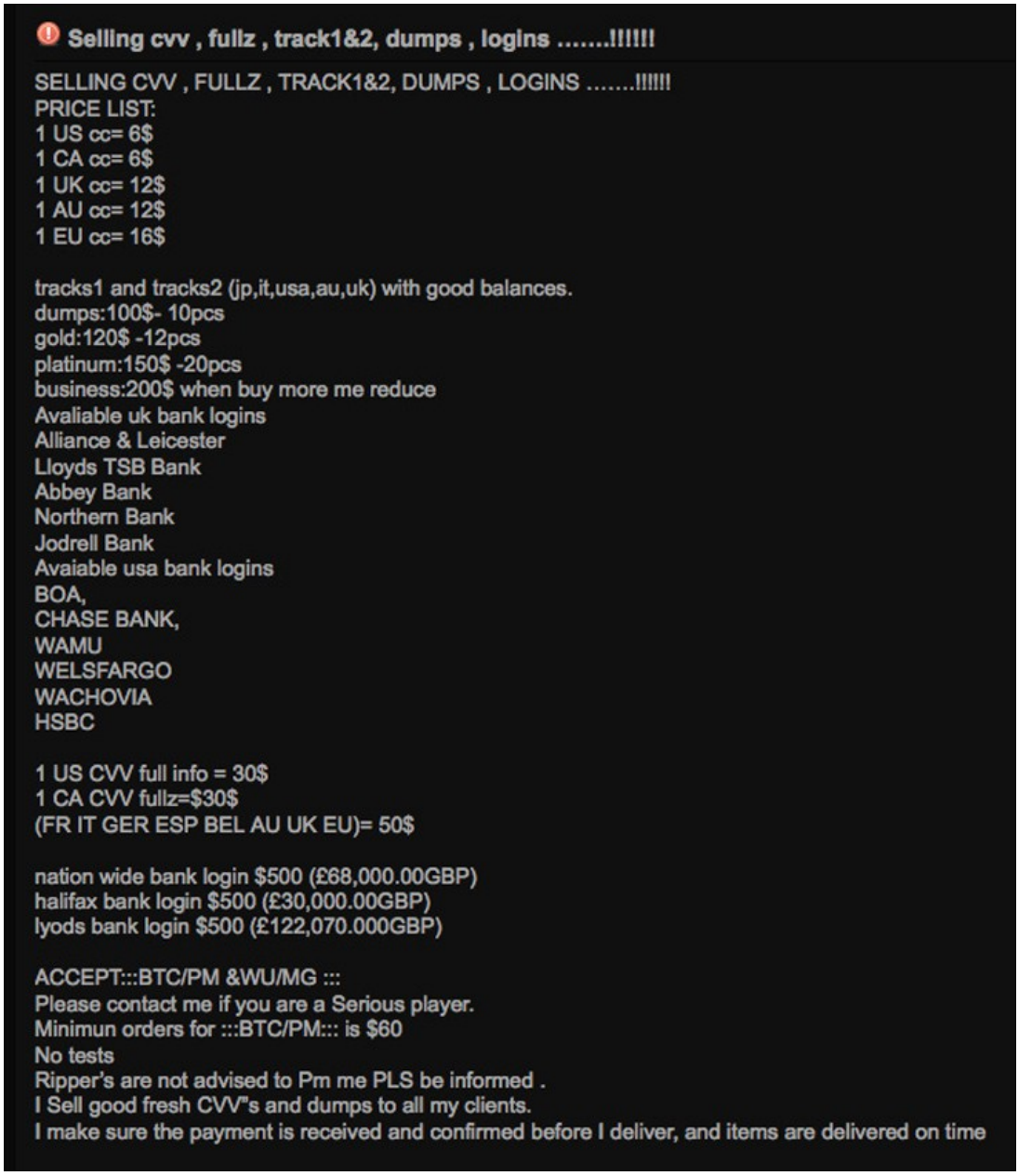


Buy Random BankLogin For Cheap

What Your Get : Full Owner Info DOB/SSN/Secret Answer , Email With Password and Bank Login

Country	Bank	Balance	Email	Password	Price	Cart
Australia	POLICE ASSOCIATION CREDIT CO-OPERATIVE, LTD.	4875USD	@gmail.com	Yes	200$	Buy
Brazil	BANCO SANTOS, S.A.	375USD	@gmail.com	Yes	200$	Buy
Brazil	BANCO DO ESTADO DO RIO GRANDE DO SUL S/A	3161USD	@gmail.com	No	200$	Buy
Brazil		3228USD	@gmail.com	Yes	200$	Buy
Brazil	BANCO BRADESCO CARTOES, S.A.	1105USD	@hotmail.com	Yes	200$	Buy
Canada	CANADIAN IMPERIAL BANK OF COMMERCE	4617USD	@aol.com	No	200$	Buy
Canada	TORONTO-DOMINION BANK	3456USD	@msn.com	No	200$	Buy
Canada		2730USD	@gmail.com	No	200$	Buy
Denmark	PBS INTERNATIONAL A/S	1376USD	@gmail.com	No	200$	Buy
Ecuador	Banco del Austro SA	2409USD	@aol.com	No	200$	Buy
France	CREDIT AGRICOLE, S.A.	307USD	@gmail.com	No	200$	Buy
France	CAISSE NATIONALE DE CREDIT AGRICOLE	4642USD	@gmail.com	No	200$	Buy
France	SOCIETE GENERALE, S.A.	3671USD	@hotmail.com	Yes	200$	Buy

Στοιχεία εισόδου σε τραπεζικούς λογαριασμούς με αναγραφή του πιστωτικού υπολοίπου.

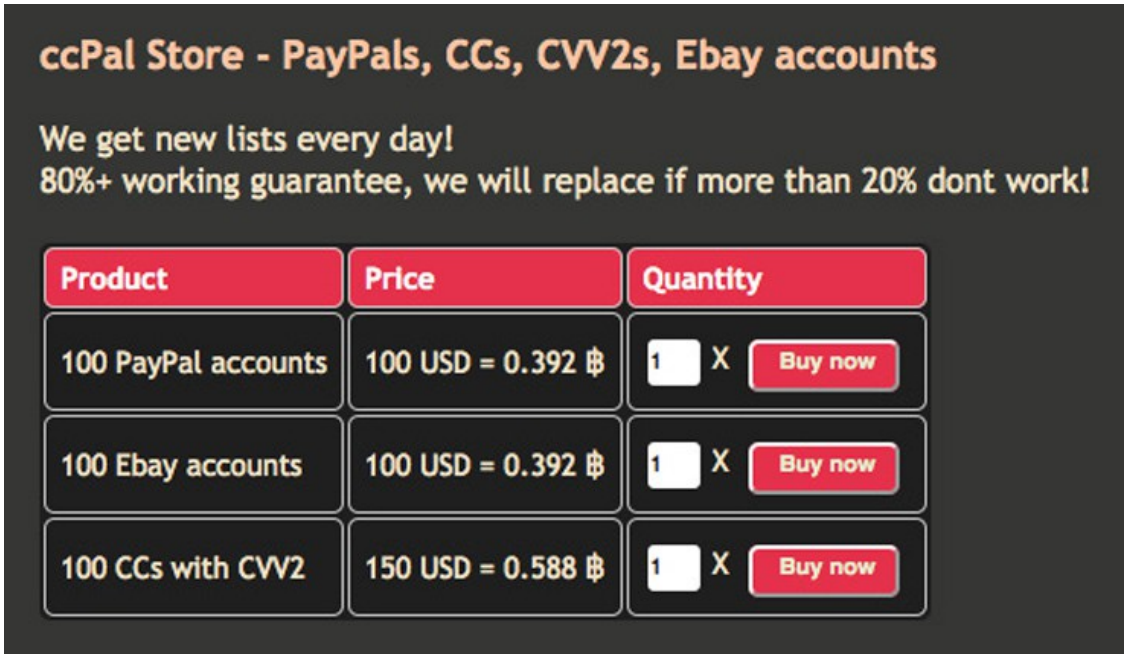


Πώληση στοιχείων εισόδου σε τραπεζικούς λογαριασμούς από ΗΠΑ και Βρετανία.

Από την άλλη, όσον αφορά τις πιστωτικές κάρτες, οι τιμές ποικίλουν ανάλογα με την προσφορά και τη ζήτηση, με το εάν είναι ενεργοποιημένες, καθώς και με βάση το πόσα χρήματα θα μπορέσουν να κλέψουν πριν απενεργοποιηθούν.

Σύμφωνα με τη μελέτη της Trend Micro, οι πωλητές προκειμένου να «σπρώξουν» τα κλεμμένα στοιχεία των πιστωτικών καρτών, συνηθίζουν να τις πωλούν σε πακέτα, κάτι που είναι και πιο οικονομικό για τους αγοραστές, μιας και η τιμή πέφτει. Επιπλέον, με τον τρόπο αυτό οι αγοραστές εξασφαλίζουν πως θα βρουν τουλάχιστον ορισμένες κάρτες σε λειτουργία.

Σε ενδεικτικές φωτογραφίες που παρατίθενται στη μελέτη (printscreens) βλέπουμε πως οι 100 κάρτες πωλούνται προς 150 δολάρια, ενώ ο πωλητής δίνει εγγύηση ότι πάνω από το 80% εξ αυτών είναι λειτουργικές και σε περίπτωση που πάνω από το 20% δεν λειτουργούν πλέον, θα υπάρξει αντικατάσταση. Δηλαδή το περιθώριο που δίνεται οι κάρτες να είναι ακυρωμένες είναι μόλις το 20% (Martin, 2014).

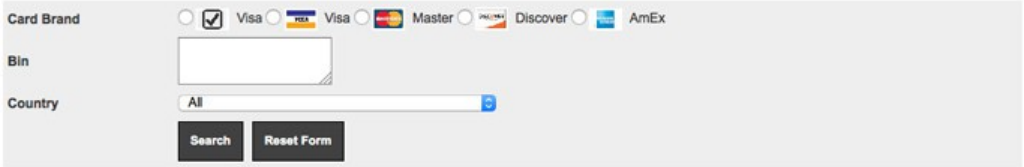


Επίσης, μεμονωμένες κάρτες δίνονται προς 65 δολάρια έκαστη, με τον αγοραστή να μπορεί να δει από πριν τη «μάρκα» της κάρτας (Visa, Mastercard), την ημερομηνία λήξης της, τη χώρα προέλευσης, το εκδοτικό ίδρυμα, τον τύπο της (προπληρωμένη, χρεωστική, πιστωτική), καθώς και άλλα δεδομένα. Αν και μέχρι πριν από ένα χρόνο παρατηρούνταν διαφορές στην τιμή ανάλογα με τη «μάρκα» της κάρτα, πλέον οι τιμές είναι ίδιες, εξαιτίας της μεγάλης προσφοράς καρτών κάθε τύπου.

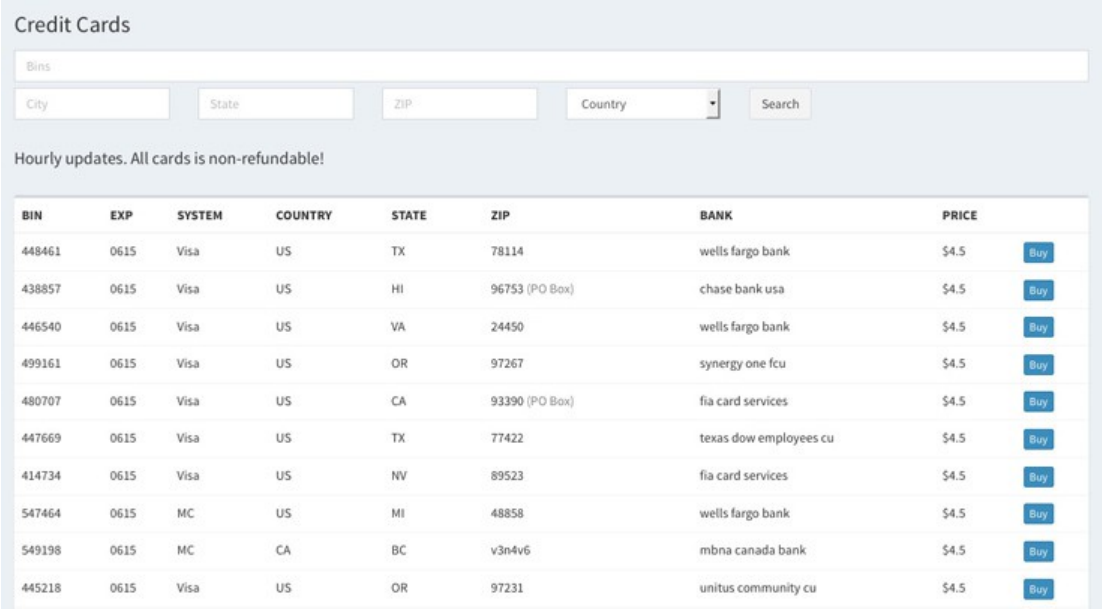
Search Cards

Card Number	TYPE	Expires	Country		Issuer	Price	Cart
443479** **** ****	Visa	1/2022	AU		CUSCAL, LTD.	12$	Buy
472436** **** ****	Visa	6/2021	AU			12$	Buy
516649** **** ****	MasterCard	7/2022	AU		WESTPAC BANKING CORPORATION	12$	Buy
554400** **** ****	MasterCard	8/2020	AU		MONEYSWITCH, LTD.	12$	Buy
376042** **** ****	AmEx	9/2018	AU		AMERICAN EXPRESS	12$	Buy

Search Dumps

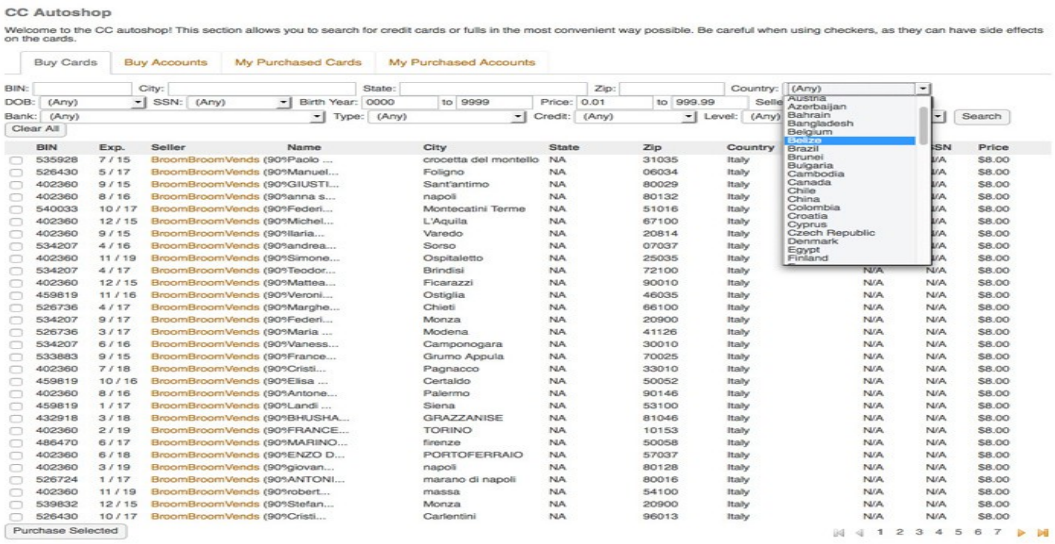


Bin	TYPE	Expires	Country	Issuer	Mark	SCode	Track	Price	Cart
443409	Visa	8/2018	Australia	CUSCAL, LTD.	CLASSIC	101	T1 +T2	65$	Buy
448387	Visa	2/2018	Austria	CITICORP	PREPAID	101	T1 +T2	65$	Buy
526763	Master Card	10/2020	Canada		STANDARD	101	T1 +T2	65$	Buy
373399	AmEx	6/2022	Canada	AMERICAN EXPRESS	BLUE AIRMILES CASH BACK CARD	101	T1 +T2	65$	Buy
520152	Master Card	1/2020	Comoros	CHINA GUANGFA BANK CO., LTD.	GOLD	101	T1 +T2	65$	Buy
547533	Master Card	6/2022	Czech Republic	KOMERCNI BANKA, A.S.	BUSINESS	101	T1 +T2	65$	Buy
402801	Visa	11/2015	Finland	LUOTTOKUNTA	CLASSIC	101	T1 +T2	65$	Buy
492069	Visa	5/2022	Finland	BANK OF AALAND LTD. (AALANDSBANKEN AB)	CLASSIC	101	T1 +T2	65$	Buy



Ενδιαφέρον παρατηρείται και σε ό,τι αφορά τη χώρα προέλευσης κάθε κάρτας, καθώς αν και διακινούνται κλοπιμαία απ' όλες της ηπείρους, όσες δεν προέρχονται από την Αμερική κοστολογούνται υψηλότερα.

Τέλος, τα sites αγοροπωλησιών δίνουν τη δυνατότητα στους πελάτες να αναζητούν κάρτες επιλέγοντας περιοχή προέλευσης και εκδοτικό ίδρυμα. Αυτό συμβαίνει διότι η πραγματοποίηση αγορών κοντά στην γεωγραφική τοποθεσία του κατόχου, μειώνει τις πιθανότητες η συναλλαγή να χαρακτηριστεί ως «ύποπτη» (Bethencourt, et al, 2007).



2.2.7. Phishing και απάτες

Για αρχή, από την έρευνα της Trend Micro προκύπτει ότι σε αντίθεση με ό,τι φανταζόμασταν, οι χάκερς και τα κακόβουλα λογισμικά (malwares) βρίσκονται πίσω από το μόλις 25% των επιθέσεων. Εξίσου συχνή αιτία, είναι η δουλειά ανθρώπων μέσα από τις εταιρείες-θύματα, καθώς και η χρήση συσκευών που έχουν χακαριστεί. Ο πιο συχνός τρόπος απώλειας δεδομένων, τέλος, είναι μετά από απώλεια ή κλοπή συσκευών όπως laptops και flash drives.

Αγαπημένος στόχος των χάκερ έχουν γίνει τα τελευταία χρόνια οι εταιρείες ηλεκτρονικών πληρωμών με τις απώλειες δεδομένων που σχετίζονται με πιστωτικές κάρτες να έχουν δει αύξηση 169% την τελευταία 5ετια.

Σύμφωνα μάλιστα με την Trend Micro, οι επιτήδειοι έχουν βάλει στο στόχαστρο πλέον και τη βιομηχανία της υγείας, κυβερνητικές υπηρεσίες, καταστήματα λιανικής πώλησης και τον τομέα της εκπαίδευσης.

Δεδομένα που κλέβονται συχνότερα είναι τα προσωπικά στοιχεία, ενώ ακολουθούν τα πολύτιμα οικονομικά δεδομένα. Εκτός από τους αριθμούς πιστωτικών καρτών, το Uber (υπηρεσία ταξί), το PayPal και οι online λογαριασμοί παιχνιδιών είναι συχνά στόχοι του κυβερνοεγκλήματος (Bartlett, 2014).

2.2.8. Παράνομη και ηθικά αμφισβητούμενη πορνογραφία

Η ιστοσελίδα-παγίδα του FBI στο Dark Web χρησίμευσε ως πόλος έλξης για παιδόφιλους σε όλον τον κόσμο. Η ιστοσελίδα ήταν ενεργή από τους servers του FBI από τις 20 Φεβρουαρίου 2015 έως τις 4 Μαρτίου 2015. Σε αυτό το διάστημα είχε 215.000 εγγεγραμμένους χρήστες.

Το FBI με την ιστοσελίδα-παγίδα με το όνομα «Playpen» μάζεψε διευθύνσεις IP και εμφύτευσε malware στους χρήστες της. Έως τώρα 137 άτομα έχουν κατηγορηθεί με βάση αυτά τα στοιχεία (Martin, 2014).

Σύμφωνα με άλλη αναφορά σχετική με την υπόθεση, το FBI φαίνεται να χάκαρε υπολογιστές σε Δανία, Χιλή και στην Ελλάδα σε συνεργασία με την EUROPOL, στην επιχείρηση με την ονομασία "Operation Pacifier".

Το ότι το FBI ανέβασε το ίδιο ιστοσελίδα παιδικής πορνογραφίας χρησιμοποιείται από τους δικηγόρους των κατηγορουμένων ως αντεπιχείρημα για την μη καταδίκη τους, αλλά δεν αναμένεται να πείσουν (Biddle, et al, 2002a).

2.2.9. Τρομοκρατία

Μία υποκουλτούρα που συχνάζει στο Dark Web είναι και οι τρομοκράτες που χρειάζονται ένα ανώνυμο δίκτυο άμεσα διαθέσιμα και γενικά απρόσιτο. Θα ήταν αρκετά δύσκολο για τους τρομοκράτες να διατηρήσουν μια ιστοσελίδα στο κανονικό διαδίκτυο λόγω της ευκολίας πρόσβασης στο site.

Οι τρομοκρατικές οργανώσεις, επίσης, ψάχνουν στο Σκοτεινό Web σαν μια εναλλακτική λύση επικοινωνίας μέσω του Διαδικτύου. Το 2007, ο Mark Burgess, διευθυντής του Παγκόσμιου Ινστιτούτου Ασφάλειας στις Βρυξέλλες, προειδοποίησε ότι «η υπερβολική εστίαση σχετικά στο κλείσιμο των ιστοσελίδων θα μπορούσε να είναι αντιπαραγωγική, δεδομένου ότι κατά πάσα πιθανότητα οι τρομοκρατικές δυνάμεις μεταφέρουν τις ιστοσελίδες τους στο λεγόμενο Dark Web» (Roosa & Schultze, 2013).

Το Διαδίκτυο είναι δίκοπο μαχαίρι για τους εξτρεμιστές. Από τη μια πλευρά είναι ένα πολύτιμο εργαλείο που τους βοηθάει να στρατολογήσουν νέα μέλη και να διαδώσουν την προπαγάνδα τους, αλλά από την άλλη, είναι ελεγχόμενο. Όπως αναφέρει ο Andrews ο έλεγχος των ιστοσελίδων της «επιφάνειας» ωθεί τους τρομοκράτες βαθύτερα στο Web, κάτι το οποίο μπορεί να είναι καλό, γιατί περιορίζει την πρόσβαση στο ευρύ κοινό, αλλά και καθιστά και πιο δύσκολο για την επιβολή του τις Αρχές να εντοπίζουν τις ιστοσελίδες (Biddle, et al, 2002b).

Η τρομοκρατία εκμεταλλεύεται συχνά καταστάσεις όπως τη φτώχεια, για να σχηματίσει online αποκλίνουσες ομάδες: «ομάδες ατόμων ευπαθών κοινωνικά, οικονομικά και ψυχολογικά θα μπορούσε να αποτελέσουν ένα γόνιμο έδαφος για την πρόσληψη ατόμων σε δυνητικά βίαιες καταστάσεις, ιδιαίτερα για τους νέους».

Στην κατανόηση του πώς λειτουργούν οι εξτρεμιστικές ομάδες στο σκοτεινό Web, θα πρέπει να μελετήσουμε το έργο του καθηγητή Chen του Πανεπιστημίου της Αριζόνα, ο οποίος έχει δημοσιεύσει πολυάριθμα άρθρα σχετικά με τα εργαλεία των Jihadist στο σκοτεινή Dark Web. Ο Chen και η ομάδα του έχουν αναπτύξει μεθόδους για την παρακολούθηση της εξάπλωσης των επικίνδυνων ιδεών μέσω ορισμένων Jihad forums του Παγκόσμιου Ιστού (Berthier & Cukier, 2008).

Χρησιμοποιώντας ένα μαθηματικό μοντέλο γνωστό σαν SIR, που χρησιμοποιείται από επιδημιολόγους για να καταγράψουν τη μετάδοση μιας νόσου, οι ερευνητές κατέληξαν στο συμπέρασμα ότι ο ρυθμός «μόλυνσης» μπορεί να «φτιάξει» 2 βομβιστές αυτοκτονίας κάθε 10.000 άτομα. Οι αναλύσεις των forums του Dark Web δείχνουν επίσης ότι όσο περισσότεροι είναι οι συμμετέχοντες σε ένα forum, τόσο πιο βίαια γίνονται τα μηνύματά τους.

Ένα από τα χαρακτηριστικά των τρομοκρατικών δικτυακών ιστοσελίδων είναι η ικανότητά τους να διαχειρίζονται τις ραγδαίες αλλαγές των διευθύνσεων στο Διαδίκτυο. Όταν οι αρχές αναγκάσουν ένα site για να μετακινηθεί, τα ανεπίσημα δίκτυα (chatrooms ή e-mail) αναλαμβάνουν δράση. Ενημερώνουν όλους τους υποστηρικτές της ομάδας για τη νέα διεύθυνση του δικτύου. Αυτό το σύστημα διανομής νέων διευθύνσεων » από στόμα σε στόμα» φαίνεται να είναι πολύ αποτελεσματικό. Ενισχύει το αίσθημα του ανήκειν στην ομάδα και προκαλεί ικανοποίηση με το συναίσθημα μιας μικρής νίκης έναντι του απαγορευτικού νόμου (Bethencourt, et al, 2007).

2.2. Το Deep web

Το Deep Web (επίσης γνωστό και ως Deepnet, DarkNet, Undernet, το αόρατο Web ή το κρυμμένο Web) αναφέρεται στο περιεχόμενο του World Wide Web που δεν ανήκει στο Επιφανειακό Web (Surface Web), το οποίο δεικτοδοτείται από μία συνηθισμένη μηχανή αναζήτησης.

Ο Mike Bergman, ιδρυτής του BrightPlanet, που επινόησε τη φράση, είχε πει πως το να ψάχνει κανείς στο Internet σήμερα είναι σαν να σέρνει ένα δίχτυ στην επιφάνεια του ωκεανού: πολλά μπορεί να πιαστούν στο δίχτυ, αλλά υπάρχει ένας πλούτος πληροφοριών που βρίσκονται βαθιά και επομένως δεν μπορούν να πιαστούν. Οι περισσότερες πληροφορίες του Web είναι θαμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες, και οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν. Οι παραδοσιακές μηχανές αναζήτησης δεν μπορούν να ανακτήσουν το περιεχόμενο του deep Web. Αυτές οι σελίδες δεν υπάρχουν μέχρι να δημιουργηθούν δυναμικά ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Το deep Web είναι αρκετές τάξεις μεγέθους μεγαλύτερο από το επιφανειακό Web (Martin, 2014).

Οι μηχανές αναζήτησης ανακαλύπτουν περιεχόμενο στο Web, χρησιμοποιώντας web crawlers που ακολουθούν συνδέσμους. Αυτή η τεχνική είναι ιδανική για να ανακαλύψει κανείς πληροφορίες στο Επιφανειακό Web (Surface Web) αλλά είναι αναποτελεσματική στην εύρεση πληροφοριών από το deep Web. Για παράδειγμα, αυτοί οι crawlers δεν προσπαθούν να βρουν δυναμικές ιστοσελίδες που προέρχονται από ερωτήματα σε βάσεις δεδομένων επειδή τα ερωτήματα αυτά θα ήταν θεωρητικά άπειρα (Bailey, et al, 2006).

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

Στην πραγματικότητα, το "ορατό" στρώμα του ιστού που μπορεί κανείς να έχει πρόσβαση μέσω των δημοφιλών μηχανών αναζήτησης είναι μόνο το ένα μέρος του διαδικτύου. Το κρυμμένο διαδίκτυο είναι το περιεχόμενο που δεν είναι τόσο εύκολα προσβάσιμο, γνωστό και ως DEEPNET (μερικές φορές αποκαλείται darknet, ή Deep Web ή Hidden Web). Το περιεχόμενο αποτελείται μόνο από ιστοσελίδες που δεν υπάρχουν και δεν ανακαλύπτονται από τις μηχανές αναζήτησης και πρόσβαση έχουν μόνο μια χούφτα άνθρωποι. Υπάρχουν βέβαια και μερικά μέρη του που είναι κρυμμένα πολύ βαθύτερα (Bartlett, 2014).

Ένα μέρος του DEEPNET είναι προσβάσιμο μέσω του ανώνυμου δικτύου του Tor. Το Tor αρχικά χρηματοδοτήθηκε από το Εργαστήριο Ναυτικών Ερευνών των ΗΠΑ, όταν κυκλοφόρησε το 2002 και χρησιμοποιείται ευρέως σε όλο τον κόσμο για την προστασία της ανωνυμίας σε απευθείας σύνδεση αναφέρει η sophos. Η επίσκεψη σε ένα δικτυακό τόπο μέσω του Tor εκτρέπει τη σύνδεση μέσα από μια τυχαιοποιημένη πορεία υπολογιστών άλλων χρηστών Tor πριν από την επίτευξη του στόχου του web server, κρύβοντας ουσιαστικά την τοποθεσία από αυτόν το διακομιστή. Αλλά γιατί όλα αυτά; Μπορεί να μην είναι έκπληξη ότι, ενώ το Tor χρησιμοποιείται για πολλές νόμιμους ή ηθικούς σκοπούς, το Deep Web είναι η βάση για ένα ευρύ φάσμα εγκληματικότητας και παράνομου περιεχομένου (Biddle, et al, 2002a).

Αντίθετα από τις κανονικές ιστοσελίδες, οι σελίδες του DEEPNET δεν έχουν φιλικές διευθύνσεις URL. Αντ’ αυτού, είναι μια φαινομενικά τυχαία σειρά χαρακτήρων που ακολουθείται από την κατάληξη ".onion" και παρέχει πρόσβαση σε αυτές τις κρυφές ιστοσελίδες.

Στο DEEPNET υπάρχει το "The Hidden Wiki" που παρέχει καταχωρήσεις αυτών των διευθύνσεων URL για να διευκολυνθεί η χρήση του DEEPNET.

Crime Network - για εγκλήματα γενικότερα Το πραγματικά τρομακτικό περιεχόμενο δεν είναι ότι αυτό που βλέπουμε στο DEEPNET. Όσο βαθύτερα βουτήξουμε στις ιστοσελίδες του τόσο πιο σκούρο γίνεται το περιεχόμενο του. Έχει υπάρξει πολλή συζήτηση ως προς το κατά πόσο το Tor μπορεί να κρατήσει τις online δραστηριότητές ανώνυμες. Έχουμε ήδη δει πώς σελίδες του Tor που πουλούσαν ναρκωτικά έκλεισαν από τις αρχές ή πως το FBI εμπόδισε την κακοποίηση παιδιών μέσω παρόμοιων

ιστοσελίδων του DEEPNET. Η προσπάθεια όμως που απαιτείται από τους φορείς επιβολής του νόμου να παρακολουθήσουν χρήστες του Tor όμως είναι πάρα πολύ δύσκολη έως και ανέφικτη (Ban, et al, 2012).

Οι πολιτικοί και οι κυβερνήσεις θα θέλαμε να πιστεύουμε ότι είναι σε θέση να αστυνομεύσουν το διαδίκτυο, αλλά η δυσκολία τους να επιβάλουν μια online νομοθεσία μοιάζει ανέφικτη. Μερικοί δεν είναι διατεθειμένοι να περιμένουν να επιβληθεί αυτός ο νόμος. Τον Οκτώβριο του περασμένου έτους, οι Anonymous πήραν την κατάσταση στα χέρια τους όταν άρχισαν να ρίχνουν ιστοσελίδες παιδικής πορνογραφίας, συμπεριλαμβανομένης και της Lolita City, ιστοσελίδας του darknet.

Η έννοια των ανθρωπίνων δικαιωμάτων αρχίζει να είναι λίγο μπερδεμένη στο online περιβάλλον. Στην πραγματικότητα, μερικοί άνθρωποι λένε ότι το πλαίσιο των ανθρώπινων δικαιωμάτων δεν ισχύει στις online δραστηριότητες και η ηθική φιλοσοφία θα πρέπει να καλείται αντ' αυτών για να κριθεί τι είναι σωστό και τι λάθος. Βεβαίως, το Tor έχει και ηθική χρήση. Το Tor επιτρέπει την ελευθερία του λόγου σε αυτούς που ζουν κάτω από καταπιεστικά καθεστώτα και προστατεύει τους ακτιβιστές των ανθρωπίνων δικαιωμάτων από την ποινική δίωξη (Bethencourt, et al, 2007).

Το Tor είναι ένα ισχυρό εργαλείο. Ωστόσο, παρέχει ταυτόχρονα στους συγγραφείς malware έξυπνες μεθόδους για την απόκρυψη κακόβουλων εντολών και ελέγχου. Βοηθάει τους αναλυτές malware στον τομέα της έρευνας τους. Οι διευθύνσεις IP των συγγραφέων κακόβουλου λογισμικού είναι στη μαύρη λίστα από τα γνωστό anti-virus, έτσι συχνά χρησιμοποιούν το Tor για να τα ξεπεράσουν. Όλες αυτές οι χρήσεις του Tor φέρνουν ερωτήματα τα οποία χρειάζονται απαντήσεις.

2.2.1. Το περιεχόμενο των βάσεων δεδομένων

Οι βάσεις δεδομένων περιέχουν πληροφορίες που είναι αποθηκευμένες σε πίνακες που δημιουργήθηκαν από προγράμματα, όπως το Access, Oracle, SQL Server, MySQL (Υπάρχουν και άλλα είδη των βάσεων δεδομένων, αλλά θα επικεντρωθούμε

σε πίνακες της βάσης δεδομένων για λόγους απλότητας.) Οι πληροφορίες που αποθηκεύονται σε βάσεις δεδομένων είναι προσβάσιμες μόνο από το ερώτημα.

Με άλλα λόγια, η βάση δεδομένων πρέπει κάπως να αναζητηθεί και με τα δεδομένα που έχουν, να ανακτηθεί και έπειτα εμφανίζονται σε μια ιστοσελίδα. Αυτό είναι ευδιάκριτο από στατικές, αυτόνομες ιστοσελίδες, οι οποίες μπορεί να έχουν άμεση πρόσβαση (Wehinger, 2011).

Ένα σημαντικό ποσό των πολύτιμων πληροφοριών στο Web παράγεται από τις βάσεις δεδομένων. Μη αρχεία κειμένου, όπως εικόνες πολυμέσων, το λογισμικό και τα έγγραφα σε μορφές όπως η μορφή Portable Document Format (PDF), το Microsoft Word, Libre/Open Office, κλπ.

Συζητήσεις και άλλες δραστηριότητες επικοινωνίας στους ιστότοπους κοινωνικής δικτύωσης, για παράδειγμα, το Facebook και το Twitter

Σελιδοδείκτες και αναφορές αποθηκεύονται σε κοινωνικές bookmarking sites (Wang, et al, 2011).

2.2.2 Περιεχόμενο που δεν υπάρχει στο ευρετήριο

Η αναζήτηση στο διαδίκτυο σήμερα, μπορεί να συγκριθεί με το να προσπαθήσουμε να απλώσουμε ένα δίχτυ σε όλη την επιφάνεια ενός ωκεανού. Ενώ ένα μεγάλο μέρος μπορεί να πιαστεί στο δίχτυ, εξακολουθεί να υπάρχει ένας πλούτος πληροφοριών που είναι βαθιά, και ως εκ τούτου τον χάσαμε (Von Lohmann, 2004).

Ο λόγος είναι απλός: Οι περισσότερες πληροφορίες του Ιστού είναι θαμμένες πολύ κάτω σε ιστοσελίδες που δημιουργούνται δυναμικά, και οι παραδοσιακές μηχανές αναζήτησης δεν τις βρίσκουν.

Εδώ είναι μερικά γεγονότα σχετικά με το Deep Web:

- Η ενημέρωση του κοινού σχετικά με το βαθύ Web είναι σήμερα 400 με 550 φορές μεγαλύτερη από ό,τι συνήθως ορίζει το World Wide Web.

- το Deep Web περιέχει 7.500 terabyte πληροφοριών ενώ το «επιφανειακό Web» (εκείνο δηλαδή το Web που βρίσκουμε από τις παραδοσιακές μηχανές αναζήτησης) περιέχει 19 terabyte πληροφοριών.

- το «Deep Web» περιέχει περίπου 550 δισεκατομμύρια μεμονωμένα έγγραφα σε σύγκριση με το 1 δισεκατομμύριο που υφίστανται στο «επιφανειακό Web».

- Περισσότερες από 200.000 βαθιά κρυμμένες ιστοσελίδες υπάρχουν σήμερα.

- Οι εξήντα, μόνον, από τις μεγαλύτερες βαθιά κρυμμένες τοποθεσίες Web περιέχουν συνολικά περίπου 750 terabytes πληροφοριών – ήδη, αυτές από μόνες τους, υπερβαίνουν το μέγεθος του «επιφανειακού Web» κατά σαράντα φορές.

- Το βαθύ Web είναι η μεγαλύτερη αναπτυσσόμενη κατηγορία των νέων πληροφοριών στο Διαδίκτυο.

- Οι ιστοσελίδες Deep τείνουν να είναι πιο περιορισμένες, με βαθύτερο περιεχόμενο, από τους συμβατικούς χώρους του «επιφανειακού Web».

- Η ποιότητα του περιεχομένου του Deep Web είναι 1.000 έως 2.000 φορές μεγαλύτερη από εκείνη του «επιφανειακού Ιστού».

- Το περιεχόμενο Deep Web είναι ιδιαίτερα σημαντικό για κάθε ανάγκη πληροφόρησης και αγοράς.

- Περισσότερο από το ήμισυ του περιεχομένου του Deep Web βρίσκεται σε συγκεκριμένες βάσεις δεδομένων.

- Ένα πλήρες ενενήντα πέντε τοις εκατό από το Deep Web είναι προσβάσιμες στο κοινό πληροφορίες – που δεν υπόκεινται σε τέλη ή συνδρομές.

- Αυτοί που κρύβονται κάτω από την επιφάνεια, είναι χάκερ, επιστήμονες, έμποροι ναρκωτικών, αστρονόμοι, δολοφόνοι, φυσικοί, επαναστάτες, κυβερνητικοί υπάλληλοι, αστυνομικοί, ομοσπονδιακοί, τρομοκράτες, διεστραμμένοι, ανθρακωρύχοι δεδομένων, απαγωγείς, κοινωνιολόγοι κλπ. Όπως μπορούμε να δούμε, είναι άνθρωποι παντός είδους ηθικής. Θεωρώ, λοιπόν ότι το θέμα αυτό ως εντελώς συναρπαστικό και πρέπει να μελετηθεί περαιτέρω (Bailey, et al, 2006).

Αν και υπάρχουν τόνοι των Bad Seeds, που κατοικούν σ' αυτόν το «deep web», υπάρχουν επίσης καλοί σπόροι που επιθυμούν να διαδώσουν τις πληροφορίες τους γρήγορα και πιο συχνά ανώνυμα, για να αποφευχθεί η νομική ή ηθική διακλάδωση.

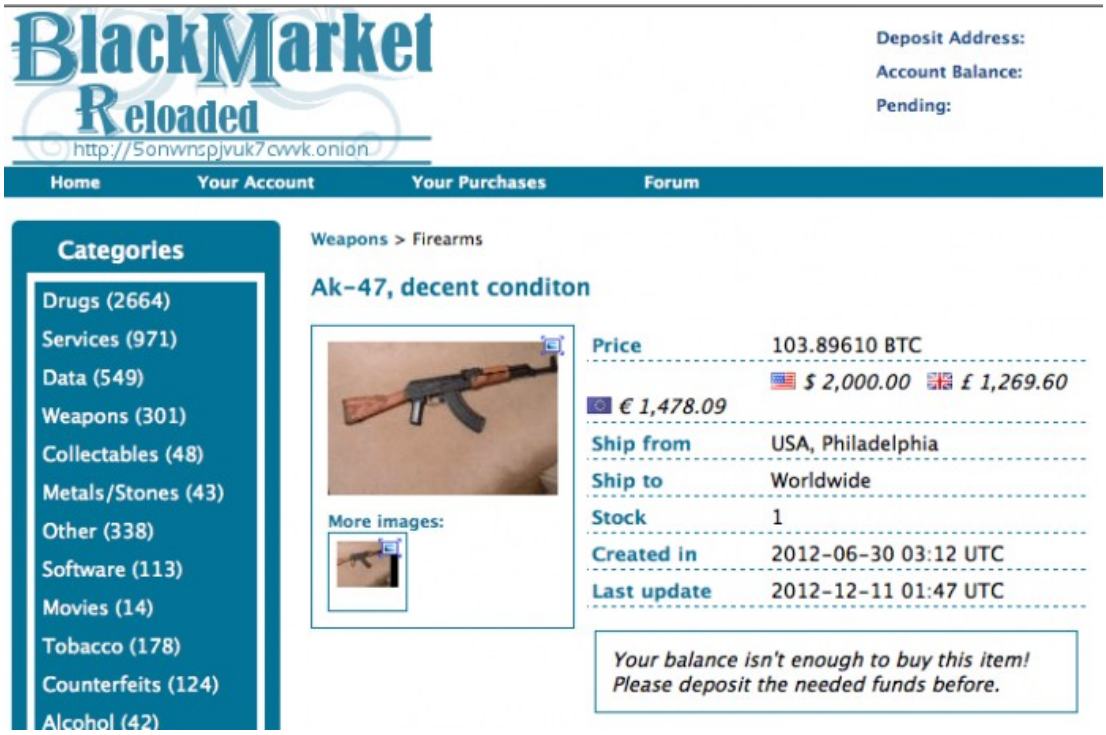
2.2.3. Τύποι περιεχομένου

Ο λόγος που το Deep Web έγινε αυτό που σήμερα είναι, οφείλεται στο γεγονός ότι μόνο το 10 περίπου τοις εκατό του από ό,τι υπάρχει στο διαδίκτυο είναι γενικά εμπορικά ενδιαφέρον. Σίγουρα θα μπορούσατε να «σκάψουμε» βαθιά μέσα στα χρονικά των λεωφόρων της πληροφορίας, αλλά οι περισσότερες, είναι ωμές πληροφορίες (Roosa & Schultze, 2013).

Δεν είναι συσκευασμένες και εύπεπτες, όπως στο StumbleUpon ή στο tumblr, κλπ. Πρόκειται για ιστοσελίδες που σκοπίμως δεν παίρνουν pinged στις μηχανές αναζήτησης, έτσι ώστε να είναι πιο δύσκολο να βρεθούν.

Σε γενικές γραμμές, τα τρομοκρατικά δίκτυα, υπηρεσίες κατάσκοποι, έμποροι ναρκωτικών, δολοφόνοι-για-μίσθωση, καθώς και εκείνοι που ψάχνουν για παιδική πορνογραφία παραμονεύουν γύρω από αυτά τα μέρη.

Υπάρχει το Hidden Wiki εκεί, και σ' αυτό το wiki υπάρχουν κατηγορίες συνδέσμων που μπορείς να βρεις ό,τι θες. Υπάρχουν blogs, φόρουμ (από φυσιολογικά μέχρι επαναστατικά μέχρι κατάφωρα παράνομα), Tor-enabled instant messaging και chat, ανώνυμη φιλοξενία αρχείων, ανώνυμη χρηματοδότηση, ανώνυμη ανατροπή και ανταλλαγή πληροφοριών, πληροφοριών σχετικά με την ασφάλεια/ανωνυμία του υπολογιστή, πληροφορίες για warez / cracks / hacking, όλα τα βιβλία, τη μουσική, τις ταινίες που μπορούμε να φανταστούμε, συνδέει ακόμη και τα αθλητικά στοιχήματα και τις πληροφορίες του εμπορίου, έχει συνδέσεις στις διεθνείς αγορές ναρκωτικών, κυκλώματα πορνείας, αγορές δολοφόνων, μαύρη αγορά προϊόντων, παιδική πορνογραφία (Martin, 2014).



Σε μερικές κοινωνίες, περισσότερο οι «αποκλίνοντες» άνθρωποι χρησιμοποιούν αυτό το δίκτυο. Και δεν μιλάμε μόνον γι' αυτούς που σερφάρουν σ' αυτές τις ιστοσελίδες, αλλά και γι' αυτούς που τις δημιουργούν και τις «διαχειρίζονται». Και το σημαντικότερο; είναι σχεδόν αδύνατον να βρεθεί κάποιος από τους "παραβάτες".

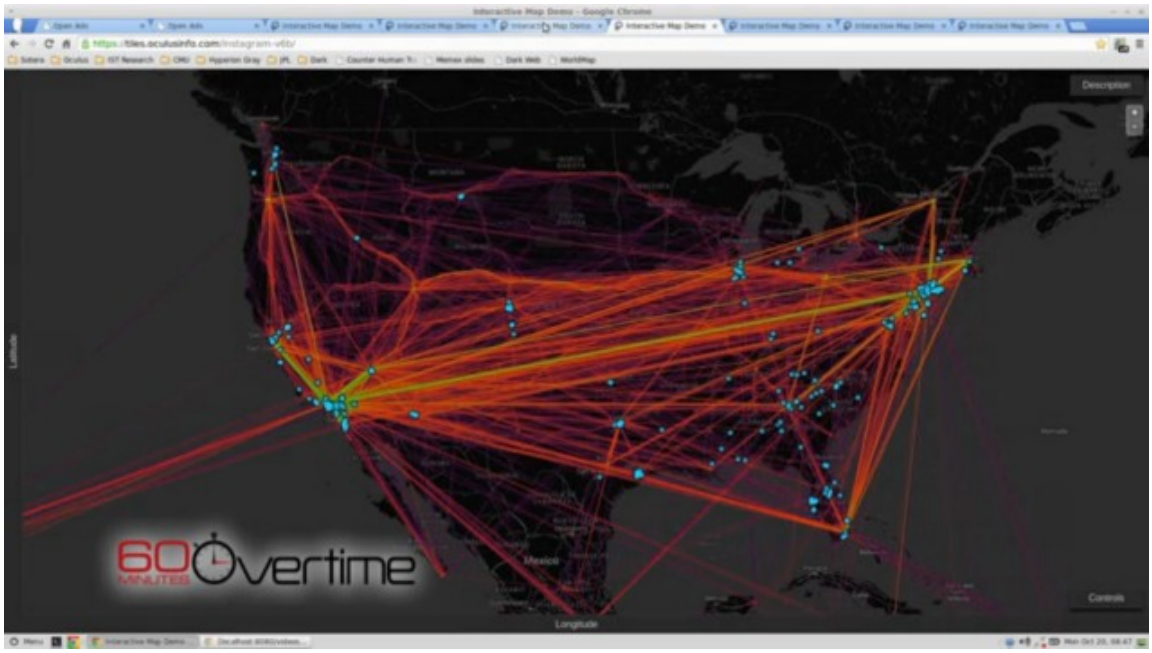
Ωστόσο, το 0.00000001% όλων των δεδομένων στο dark διαδίκτυο (dark web) είναι πράγματα που όλοι οι κανονικοί άνθρωποι θα είναι σε θέση να έχουν πρόσβαση, να κατανοούν και να χρησιμοποιούν. Και το γεγονός ότι ένα μικρό κλάσμα του περιέχει παράνομα πράγματα, δε συγκρίνεται με κάποια άλλα hardcore του υπόγειου διαδικτύου των κατασκόπων, δολοφόνων, pedos (παιδοφιλόφιλων) και εγκληματιών. Το υπόλοιπο % χρησιμοποιείται από τις σεβαστές αρχές τους (Wehinger, 2011).

Το Deep Web, είναι ένας κόσμος που πλοηγείται από περιθωριακούς αποξενωμένους μοναχικούς τύπους που ζουν στην άκρη της κοινωνίας. Οι χρήστες του Deep Web ένας ελεεινός και ανεξέλεγκτος υπόκοσμος όπου οι καουμπόηδες της κονσόλας, όπως οι ντετέκτιβ των φιλμ noir, διασυνδέονται με κακοποιούς, απόβλητους, οραματιστές, με διαφωνούντες και απροσάρμοστους (Wang, et al, 2011).

Το Επιφανειακό ιντερνέτ, φαίνεται σε αντίθεση ένα γαλήνιο, στείρο, χωρίς γεύση, τελείως ανώνυμο με τη δική του συναλλαγματική ισοτιμία, τελείως ανώνυμο, που υφίσταται αποκλειστικά και μόνο στον εικονικό χώρο για τελείως ανώνυμες συναλλαγές.

2.2.4. Μεθοδολογίες ευρετηρίασης

Πριν από ένα χρόνο, το Defense Advance Research Projects Agency (DARPA) της κυβέρνησης των ΗΠΑ, ανακοίνωσε ότι προσπαθεί να δημιουργήσει μια νέα ισχυρή μηχανή αναζήτησης που θα μπορούσε να ευρετηριάσει το Deep Web που μέχρι σήμερα δεν μπορούσαν να προσεγγίσουν συμβατικές μηχανές αναζήτησης όπως την Google (Von Lohmann, 2004).



Το project, που ονομάστηκε Memex Deep Web Search Engine, είναι ακόμα υπό ανάπτυξη. Την Κυριακή που μας πέρασε, για πρώτη φορά, πήραμε μια πρώτη γεύση για το τι μπορεί να κάνει η μηχανή αναζήτησης Memex, που είναι σχεδιασμένη για την καταπολέμηση του εγκλήματος. Η υπηρεσία έρευνας του Πενταγώνου παραχώρησε στο Scientific American μια προεπισκόπηση του λογισμικού που δημιούργησε και μια αποκλειστική παρουσίαση 60 λεπτών της προηγμένης τεχνολογίας.

Το Deep Web ως γνωστόν σφύζει από παράνομες δραστηριότητες, όπως παιδική πορνογραφία, υποθέσεις ναρκωτικών, εγκληματικότητας στον κυβερνοχώρο, εμπορίας ανθρώπων, όπλων και ότι άλλο μπορούμε να φανταστούμε. Επειδή όμως το Deep Web είναι «θαμμένο» τόσο βαθιά οι συμβατικές μηχανές αναζήτησης δεν μπορούσαν να έχουν πρόσβαση, μέχρι σήμερα τουλάχιστον σύμφωνα με αυτά που υπόσχεται η κατασκευάστρια εταιρεία DARPA (Wang, et al, 2011).

Η μηχανή αναζήτησης Memex προσπαθεί να διασφαλίσει όλο το Διαδίκτυο από hackers, διακινητές ανθρώπων, παιδική πορνογραφία και άλλους εγκληματίες. Η μηχανή αναζήτησης του Deep Web σχεδιάστηκε για να ξεπεραστούν τα παραπάνω

προβλήματα με την επέκταση «της εμβέλειας των σημερινών δυνατοτήτων των μηχανών αναζήτησης» (Bethencourt, et al, 2007).

Ο εφευρέτης της μηχανής αναζήτησης Memex, Chris White, εξήγησε πως λειτουργεί η νέα μηχανή αναζήτησης και πώς θα μπορούσε να φέρει επανάσταση στις έρευνες επιβολής του νόμου.

Θα ήταν ανόητο να σκεφτεί κάποιος πως δεν υπάρχει καλύτερος τρόπος για να ευρετηριάσουμε το διαδίκτυο και μια νέα δημιουργική ιδέα ίσως είναι ακριβώς «κάτω από τη μύτη μας». Το γεγονός ότι η Microsoft τα τελευταία χρόνια κάνει μια μεγάλη επένδυση για την ανάπτυξη μιας νέας τεχνολογίας αναζήτησης θα πρέπει να είναι σοβαρός λόγος που θα απασχολήσει τις υπόλοιπες μηχανές αναζήτησης. Είναι απαραίτητο οι μηχανές αναζήτησης να επεκταθούν και στο «deep web» που αναφέρθηκε, ώστε να μπορούν να δώσουν πληροφορίες και από αυτό το κομμάτι στις αναζητήσεις των χρηστών αλλά και για να γίνει μία καλύτερη εκτίμηση του μεγέθους του διαδικτύου. Οι μηχανές αναζήτησης, εκτός από κείμενο, θα πρέπει να δίνουν και αρχεία εικόνας, ήχου και βίντεο στις αναζητήσεις των χρηστών και να μην τα αντιμετωπίζουν σαν τέσσερις διαφορετικές κατηγορίες αναζήτησης (Berthier & Cukier, 2008).

2.3. Διαφορά με τον τυπικό ιστό

Όπως καταλαβαίνουμε λοιπόν, ο Παγκόσμιος Ιστός είναι μια σύνθετη οντότητα που περιέχει τις πληροφορίες από μια ποικιλία πηγών και περιλαμβάνει ένα εξελισσόμενο μείγμα διαφορετικών τύπων αρχείων και μέσων ενημέρωσης. Είναι πολύ περισσότερο από ό,τι οι στατικές, αυτόνομες ιστοσελίδες.

Στην πραγματικότητα, το μέρος του Web που δεν είναι στατικό, και σερβίρεται δυναμικά “on the fly”, είναι πολύ μεγαλύτερο από ό,τι τα στατικά έγγραφα που πολλοί συνδέουν με το Web (Bartlett, 2014).

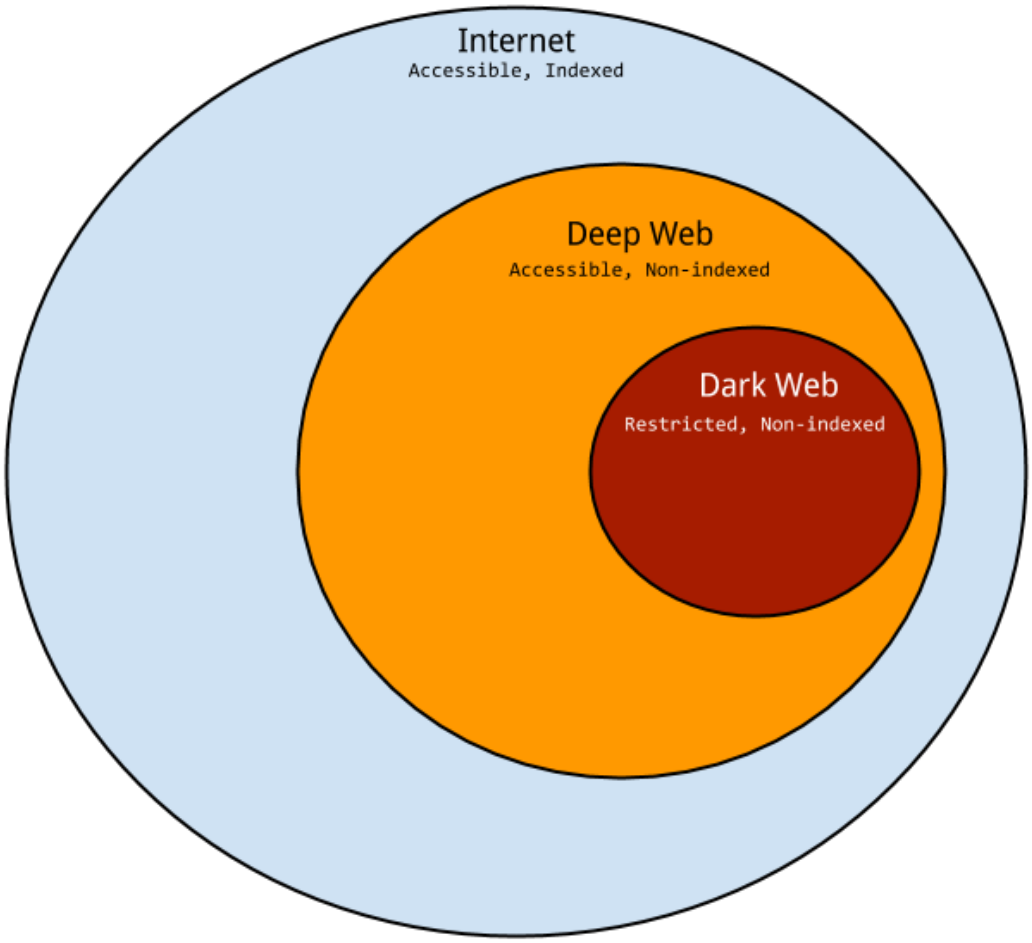
Η έννοια του «βαθιά στο Web» γίνεται όλο και πιο πολύπλοκη, καθώς οι μηχανές αναζήτησης έχουν βρει τρόπους να ενσωματώσουν βαθιά περιεχόμενο του Deep Web σε κεντρική λειτουργία αναζήτησης τους.

Εκεί μπορούμε να βρούμε όλα αυτά που δεν φανταζόμασταν. Εκεί θα βρούμε τους παράνομους, τους κακούς, τους ακτιβιστές, τους ασφαλίτες, τους ποιητές, τους επαναστάτες, τους "υψηλά ιστάμενους". Ίσως να είναι και ένα συναρπαστικό μέρος, μα με κινδύνους σε κάθε στροφή. Το Βαθύ Web, δεν μαθαίνεται από την μια ημέρα στην άλλη (Biddle, et al, 2002b).

2.4. Διαφορές Dark web και Deep web

Δύο από τις νέες εγγραφές στα λεξικά, το deep web και το dark web, είναι τόσο τεχνικού χαρακτήρα που συναντήσαμε μια μεγάλη σύγχυση ως προς το τι σημαίνει πραγματικά στην έρευνα μας. Οι περισσότερες εκδόσεις σχετικές με την τεχνολογία γενικά έχουν μια αποκήρυξη όταν συζητούν για το dark web, προβάλλοντας στους αναγνώστες τους ότι αυτό δεν πρέπει να συγχέεται με το deep web, το οποίο σχετίζεται, αλλά δεν είναι καθόλου το ίδιο πράγμα (Bartlett, 2014).

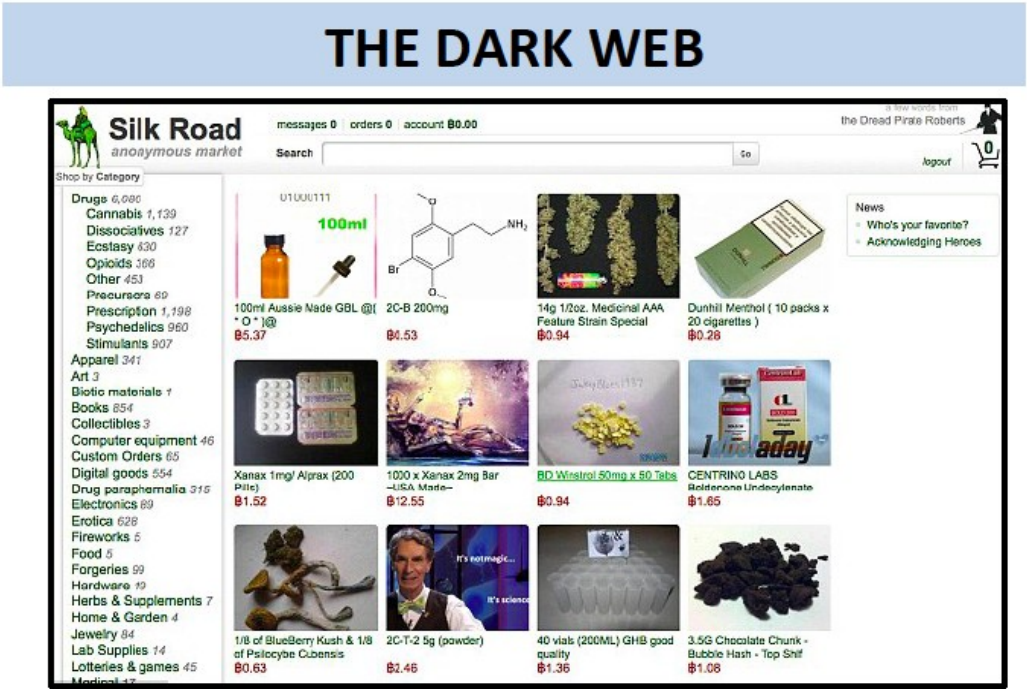
Το λεξικό Cambridge καθορίζει το deep web ως «το τμήμα του Internet που είναι κρυμμένο από τις συμβατικές μηχανές αναζήτησης, όπως με την κρυπτογράφηση, ως το άθροισμα των μη ευρετηριασμένων ιστοσελίδων». Το dark web, από την άλλη πλευρά, ορίζεται «ως το τμήμα του Internet που σκόπιμα κρύβεται από τις μηχανές αναζήτησης, χρησιμοποιεί αποκρυμμένες διευθύνσεις IP, και είναι προσβάσιμο μόνο με ένα ειδικό πρόγραμμα περιήγησης στο web: μέρος του deep web. Το κλειδί εδώ είναι ότι το dark web είναι μέρος του Deep web.



Το dark web και το deep web βρίσκονται πιο συχνά στις ειδήσεις χάρη στην συχνά αναφερόμενη δίκη του Silk Road. Το Silk Road είναι μια online μαύρη αγορά που είχε κλείσει δύο φορές από το FBI μεταξύ 2013 και 2014. Τον Φεβρουάριο του 2015, ο ιδρυτής του Silk Road του Ross Ulbricht είχε καταδικαστεί για διάφορα εγκλήματα, μεταξύ των οποίων αρκετές απόπειρες δολοφονιών προς ενοικίαση. Το Silk Road έτρεξε τις δραστηριότητές του στο dark web, το οποίο αποτελεί ένα μικρό ποσοστό του Deep Web (Biddle, et al, 2002b).

Αυτό το οποίο έχουν ως κοινό στοιχείο το dark web και το deep web είναι ότι και τα δύο κρύβονται από τις εμπορικές μηχανές αναζήτησης. Δεν μπορεί κανείς να έχει πρόσβαση σε αυτά είτε από το Google είτε από το Bing. Το Deep Web είναι ένας γενικός όρος που περιλαμβάνει το dark web, αλλά περιλαμβάνει επίσης «κοσμικό περιεχόμενο, όπως φόρουμ Ιστού που απαιτούν εγγραφή και δυναμικά

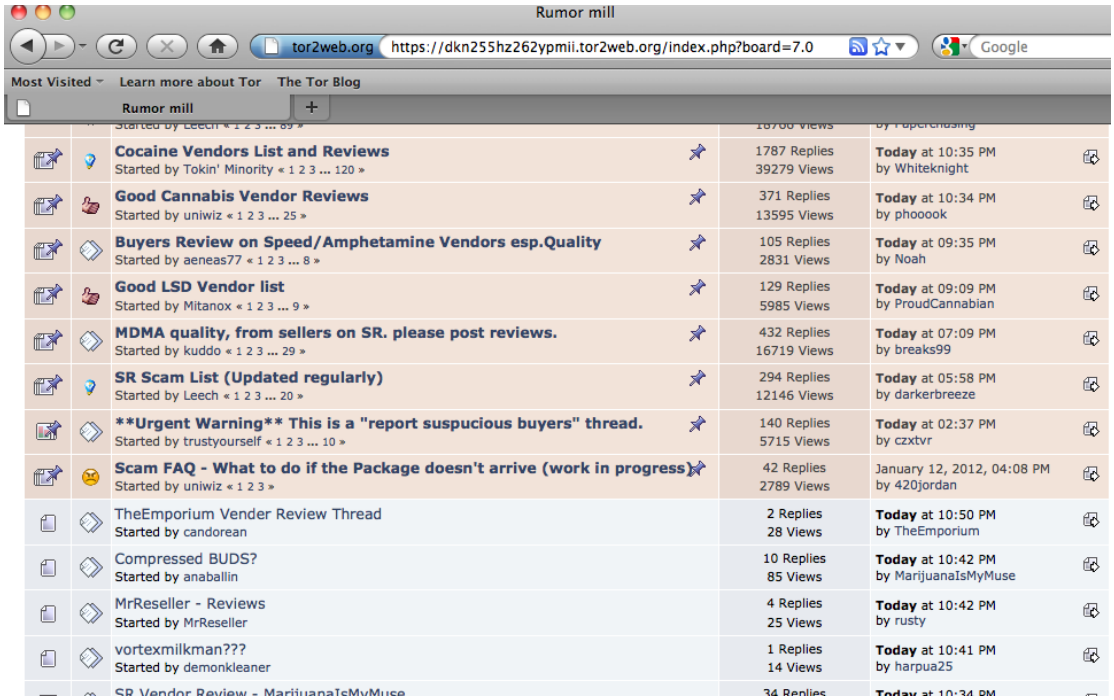
δημιουργημένες ιστοσελίδες όπως ο Gmail λογαριασμός. Δηλαδή, το μεγαλύτερο μέρος του Deep Web είναι άσχετο με τις ειδήσεις για το Silk Road (Bartlett, 2014).



Όταν οι άνθρωποι συζητούν για το σκοτεινό μέρος του Διαδικτύου, όπου μπορεί κανείς να αγοράσει ναρκωτικά, όπλα, παιδική πορνογραφία, πληρωμένους δολοφόνους, και βασικά οποιοδήποτε παράνομο στοιχείο ή υπηρεσία που θα μπορούσε να ονειρευτεί, αναφέρονται στο dark web. Ο Greenberg σημειώνει ότι ενώ το deep web είναι τεράστιο και αναλογεί στο 90% και επιπλέον του Διαδικτύου, το dark web πιθανότατα αντιπροσωπεύει μόνο μόνο περίπου 0,01%. Το dark web, μερικές φορές αναφέρεται ως darknet, και είναι προσβάσιμο από Tor (The Onion Router) ή I2P (Invisible Έργου Internet), τα οποία χρησιμοποιούν αποκρυμμένες διευθύνσεις IP για να διατηρήσουν την ανωνυμία για τους χρήστες και τους ιδιοκτήτες της ιστοσελίδας. Με αυτό τον τρόπο, οι άνθρωποι που χρησιμοποιούν το dark web για παράνομους σκοπούς δεν μπορούν να εντοπιστούν (Von Lohmann, 2004).

Στο dark web δεν βρίσκονται μόνο παράνομες προσφορές και επιχειρήσεις. Χρησιμοποιείται για μια σειρά από άλλους λόγους. Οι δημοσιογράφοι χρησιμοποιούν το dark web για να βοηθήσουν στην προστασία της ανωνυμίας των πηγών τους, και άλλοι χρησιμοποιούν το dark web μόνο και μόνο επειδή πιστεύουν ακράδαντα στο

δικαίωμά τους στην ιδιωτική ζωή. Ο Max Eddy για το PC Magazine αναφέρει ότι «το Tor αρχικά αναπτύχθηκε από το Υπουργείο Άμυνας των ΗΠΑ», και ενώ τώρα το Tor είναι μια μη κερδοσκοπική επιχείρηση από εθελοντές, χρηματοδοτείται από την κυβέρνηση των ΗΠΑ και το Εθνικό Ίδρυμα Επιστημών. Στο Vox, ο Timothy B. Lee εξηγεί: «Η κυβερνητική υποστήριξη για το Tor συνεχίστηκε κατά τα τελευταία χρόνια, ως μέρος της ατζέντας της ελευθερίας του διαδικτύου του Στέιτ Ντιπάρτμεντ, η οποία επιδιώκει να βοηθήσει τους ανθρώπους σε καταπιεστικά καθεστώτα να αποκτήσουν πρόσβαση σε πληροφορίες που λογοκρίνονται από τις κυβερνήσεις τους». Για παράδειγμα, το Facebook ξεκίνησε πρόσφατα μια έκδοση του site του στο dark web για να «καταστήσει ευκολότερη την πρόσβαση στην ιστοσελίδα από χώρες που περιορίζουν την υπηρεσία, όπως η Κίνα και το Ιράν» (Ban, et al, 2012).



Μια κοινή παρανόηση σχετικά με το dark web και το deep web είναι ότι αυτοί οι δύο όροι είναι εναλλάξιμοι. Αυτό δεν είναι αλήθεια. Μπορούμε να λάβουμε για παράδειγμα, αυτή την πρόταση στο Business Insider: « Το dark (ή deep) web, το οποίο αναφέρεται σε περιοχές του Διαδικτύου συνήθως απρόσιτες για τους χρήστες χωρίς ειδικό λογισμικό ανωνυμοποίησης, ήρθε για πρώτη φορά στο προσκήνιο με τη δίκη του Silk Road». Ενώ, τόσο το deep όσο και το dark web έχουν παρουσιαστεί σε ειδήσεις για το Silk Road, αυτός ο συγγραφέας είναι σαφώς αναφερόμενος ειδικά στο dark web, το οποίο είναι μόνο ένα μικρό τμήμα του Deep web, όπου οι χρήστες

χρησιμοποιούν αποκρυμμένες διευθύνσεις IP για να κρύψουν την ταυτότητά τους (Wang, et al, 2011).

Αν οι άνθρωποι συνεχίζουν να συγχέουν τους όρους dark web και deep web, τελικά ο ορισμός θα αρχίσει να επεκτείνεται.

Η πλειοψηφία των dark websites χρησιμοποιούν την ανώνυμη εφαρμογή Tor και ένα μικρό ποσοστό χρησιμοποιεί ένα παρόμοιο εργαλείο που ονομάζεται I2P. Και τα δύο συστήματα κρυπτογραφούν το web traffic σε επίπεδα και το στέλνουν τυχαία σε διάφορους υπολογιστές ανά τον κόσμο αφαιρώντας κάθε φορά ένα επίπεδο μέχρι τον επόμενο υπολογιστή του δικτύου. Τέλος φτάνουν στον τελικό παραλήπτη αποκρυπτογραφημένα.

Θεωρητικά είναι ένας καλός τρόπος να αποφύγεις την κατασκοπεία ακόμα και τους υπολογιστές που αφαιρούν τα επίπεδα από την αρχή μέχρι και τον τελικό προορισμό.

Όταν ένας χρήστης χρησιμοποιεί τον Tor για παράδειγμα, είναι πολύ δύσκολο να δουν την ip αυτού του χρήστη. Αλλά όταν ένα website χρησιμοποιεί την υπηρεσία Tor – Που είναι γνωστή σαν Tor hidden service - μπορεί να επισκεφθεί μόνο από τους χρήστες που χρησιμοποιούν Tor.

Το traffic από τους δύο υπολογιστές δηλαδή του χρήστη και του webserver χρησιμοποιεί την υπηρεσία Tor μέσω επιπέδων σε τυχαίους υπολογιστές έτσι ώστε να βρεθούν σε ένα κοινό σημείο στο δίκτυο Tor , σαν ανώνυμοι bagmen που αλλάζουν χαρτοφύλακες σε ένα parking.

Παρόλο όμως που οι διευθύνσεις ip από αυτά τα site κρατούνται κρυφές, δεν σημαίνει ότι αυτές οι σελίδες είναι απαραίτητα απαγορευμένες. Οι Σελίδες που χρησιμοποιούν την υπηρεσία Tor όπως τα site ναρκωτικών (SilkRoad, SilkRoad 2, Agora και Evolution) έχουν εκατοντάδες χιλιάδες κανονικούς χρήστες. Αρκεί να χρησιμοποιούμε τον Tor και να γνωρίζουμε το url της σελίδας που χρησιμοποιεί την υπηρεσία Tor (που έχει κατάληξη .onion) , για να επισκεφθούμε τους παράνομους αυτούς ιστοτόπους.

Πολλά (δημοσιογραφικά) siteεσφαλμένα περιγράφουν το darkwebσαν το 90% του internet. Δηλαδή το μπερδεύουν με το DEEP WEB Δηλαδή όλες τις ιστοσελίδες του διαδικτύου που δεν είναι ορατές από τις μηχανές αναζήτησης .

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

Σύμφωνα με εκτιμήσεις που έγιναν σε μία μελέτη στο Πανεπιστήμιο Berkeley της Καλιφόρνια (University of California, Berkeley) το 2001 , το DEEP WEB αποτελείται περίπου από 91.000 terabytes. Αντίθετα το επιφανειακό είναι περίπου 167 terabytes. Τέλος το DARK WEB υπολογίζεται ως το 0,01% του συνολικού διαδικτύου δηλαδή περίπου 9,12 terabytes . Σύμφωνα με τον ερευνητή Nik Cubrilovic λιγότερες από 10,000 Tor hidden services βρίσκονται αυτή τη στιγμή στο DEEP WEB σε σύγκριση με τις εκατοντάδες εκατομμύρια νόμιμες υπηρεσίες.

Αν μπορούσαμε να απεικονίσουμε τις τρεις αυτές ονομασίες το SURFACE WEB θα ήταν η επιφάνεια της θάλασσας το DEEP WEB θα ήταν το υπόλοιπο και το DARK WEB θα μπορούσε να είναι ένα πολύ μικρό κομμάτι του DEEP WEB.

Παρόλο που κατά βάση το DARK WEB έχει ταυτιστεί με την πώληση όπλων και ναρκωτικών όπως και προϊόντων παιδικής πορνογραφίας -προσπαθούν να εκμεταλλευθούν την υπηρεσία για τους δικούς τους σκοπούς- δεν είναι όλα στο DARK WEB και τόσο σκοτεινά.

Ένα από τα πρώτα site σε επισκεψιμότητα στο DARK WEB το wikileaks δημιούργησε τρόπους για να παίρνει πληροφορίες μέσω ανώνυμων πηγών . Αυτή η

ιδέα είναι ένα εργαλείο που ονομάζεται secure drop που συνδέεται με το Tor hidden services και μπορεί σε οποιοδήποτε δημοσιογραφικό οργανισμό να παραλάβει ανώνυμες πληροφορίες.

Το Deep Web είναι μια τεράστια συλλογή όλων των sites του διαδικτύου που δεν είναι προσβάσιμα από τις μηχανές αναζήτησης. Αυτές οι unindexed ιστοσελίδες περιλαμβάνουν τεράστιους όγκους περιεχομένου, όπως forums που απαιτείται εγγραφή, δυναμικές ιστοσελίδες, υπηρεσίες σαν το Gmail και πολλά άλλα. Το πραγματικό Dark Web αντίθετα, πιθανόν αντιπροσωπεύει λιγότερο από το 0,01% του web: αναφέρει ο ερευνητής ασφαλείας Nik Cubrilovic που μετρήσε 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.

Αν και το Dark Web συχνά συνδέεται με την πώληση των ναρκωτικών, όπλων, πλαστών εγγράφων και παιδικής πορνογραφίας, όλες οι ιστοσελίδες χρησιμοποιούν την υπηρεσία Tor και δεν περιέχει μόνο τόσο «σκοτεινές» ιστοσελίδες όσο το θέλει η ονομασία. Την ίδια υπηρεσία χρησιμοποιεί και μια από τις πρώτες σελίδες υψηλού προφίλ του Dark Web, το Tor WikiLeaks, μια κρυφή υπηρεσία που δημιουργήθηκε για να δεχτεί διαρροές από ανώνυμες πηγές. Αυτή η ιδέα έχει προσαρμοστεί από τότε σε ένα εργαλείο που ονομάζεται SecureDrop, ένα λογισμικό που ενσωματώνει τις κρυφές υπηρεσίες του Tor με οποιοδήποτε ειδησεογραφικό οργανισμό λαμβάνει ανώνυμες υποβολές. Ακόμα και το Facebook όπως αναφέραμε την προηγούμενη βδομάδα, ξεκίνησε μια ιστοσελίδα στο Dark Web με στόχο την καλύτερη προστασία σε χρήστες που επισκέπτονται την ιστοσελίδα με Tor για να αποφύγουν την επιτήρηση και τη λογοκρισία.

Το Dark Web δεν είναι ιδιαίτερα μεγάλο, δεν είναι το 90% του Διαδικτύου, και δεν είναι ιδιαίτερα μυστικό. Στην πραγματικότητα, το Dark Web είναι μια συλλογή από ιστοσελίδες που είναι ορατές στο κοινό, αλλά κρύβουν τις διευθύνσεις IP των servers που τις τρέχουν. Αυτό σημαίνει ότι ο καθένας μπορεί να επισκεφθεί το Dark Web, αλλά μπορεί να είναι πολύ δύσκολο να καταλάβει πού φιλοξενείται, ή από ποιόν.

Η πλειονότητα των ιστοσελίδων στο Dark Web χρησιμοποιούν το λογισμικό ανωνυμίας Tor, αν και ένας μικρότερος αριθμός, χρησιμοποιεί ένα παρόμοιο εργαλείο που ονομάζεται I2P. Και τα δύο αυτά συστήματα κρυπτογραφούν την κυκλοφορίας του Ιστού σε στρώματα και την πετάνε σε τυχαία επιλεγμένους υπολογιστές σε όλο τον κόσμο. Ο καθένας από αυτούς τους servers αφαιρεί ένα από τα στρώματα της ενιαίας κρυπτογράφησης πριν περάσει τα δεδομένα στον επόμενο server. Στη θεωρία, αυτό είναι που εμποδίζει κάθε κατάσκοπο, ακόμα και αυτούς που ελέγχουν έναν από αυτούς τους servers που μοιράζουν τα κρυπτογραφημένα δεδομένα, να καταλάβει την προέλευση της κίνησης και τον προορισμό της.

Οι μηχανές αναζήτησης εμφανίζουν αποτελέσματα χρησιμοποιώντας κάποιους αλγόριθμους που βάζουν σε λίστες της 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 και 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 ίντερνετ λειτουργεί με τους συνδέσμους (links) και οι μηχανές αναζήτησης όταν ακολουθούν έναν σύνδεσμο που παραπέμπει σε κάποια άλλη σελίδα, τότε ανακαλύπτουν και τη νέα σελίδα και την ταξινομούν. Δείτε περισσότερα: Google Webmaster Tools και πως να ταξινομήσετε το site σας αμέσως

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

Contextual Web: είναι οι σελίδες εκείνες 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 μία IP των ΗΠΑ.

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

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 τη 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 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.

Παρακάτω είναι μερικά παραδείγματα από σελίδες που περιέχει το deep web:

Τα πιστοποιητικά γεννήσεως, δικά μας και των παιδιών μας, καθώς και τα πιστοποιητικά της οικογενειακής μας 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!

Αυτές είναι μερικές αναγκαίες και καλές χρήσεις του deep web. Δεν θα γινότανε διαφορετικά να υπήρχαν στην επιφάνεια και να φαινότανε τα ευαίσθητα προσωπικά δεδομένα στο ίντερνετ.

ΚΕΦΑΛΑΙΟ 3 – ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΣΤΟ DARKNET ΚΑΙ NORSE-IPVIKING

3.1 Τα είδη των επιθέσεων

Τα τελευταία χρόνια παρατηρούμε μια αύξηση στη συχνότητα των ηλεκτρονικών επιθέσεων και αυτό συμβαίνει διότι, όλο και περισσότερες τράπεζες παρέχουν υπηρεσίες μέσω του διαδικτύου. Στόχος φυσικά είναι τα προσωπικά δεδομένα των χρηστών με σκοπό την αρπαγή χρημάτων από τους λογαριασμούς τους, την χρησιμοποίηση πιστωτικών καρτών, ακόμα και αγοραπωλησίες μετοχών. Παρακάτω μπορούμε να δούμε τα πιο συχνά είδη ηλεκτρονικών επιθέσεων.

1. **Δούρειοι ίπποι (Trojan Horses)**

Είναι ένα φαινομενικά αθώο και χρήσιμο για τον υπολογιστή πρόγραμμα, το οποίο όμως περιέχει εντολές καταστροφικές για τα προσωπικά δεδομένα του χρήστη. Όταν εκτελεστεί έχει τη δυνατότητα να εγκαθιστά ιούς, να υποκλέπτει δεδομένα και να καταστρέφει αρχεία μέσα στον υπολογιστή (Bailey, et al, 2006).

2. **Ψευδείς τραπεζικοί ιστότοποι (Fake Banks)**

Είναι πανομοιότυπες ιστοσελίδες σαν των νόμιμων τραπεζών φτιαγμένες από τους εισβολείς και έχουν σαν στόχο την εξαπάτηση χρηστών ζητώντας τους κωδικούς τους και αριθμούς λογαριασμών και πιστωτικών καρτών με αποτέλεσμα τα απόρρητα στοιχεία του χρήστη να μεταφέρονται εν αγνοία του στα χέρια απατεώνων.

3. **Κοινωνική μηχανική**

Είναι ένα μη τεχνικό είδος παράνομης εισβολής που βασίζεται στην ανθρώπινη επικοινωνία. Ο εισβολέας προσποιείται ότι είναι στέλεχος, σύμβουλος ή μέλος της τράπεζας ή του ομίλου και ζητά πληροφορίες από τον χρήστη όπως κωδικούς πρόσβασης. Σε αυτή την περίπτωση ο χρήστης άθελά του καταργεί τις οριζόμενες δικλείδες ασφαλείας (Bartlett, 2014).

4. Πρόγραμμα SNIFFER

Είναι ένα πρόγραμμα ή συσκευή υποκλοπής δεδομένων. Λειτουργεί με σκοπό να αρπάξει πληροφορίες από ένα δίκτυο προς όφελος του εισβολέα που το δημιούργησε. Επίσης έχει την δυνατότητα να διαμορφώνει υπολογιστές μέσα σε ένα δίκτυο ώστε να δέχονται μηνύματα, οι χρήστες τους να απαντούν σε αυτά τα μηνύματα και να συλλέγει πληροφορίες από αυτές τις απαντήσεις (Von Lohmann, 2004).

5. Phishing

Είναι η διαδικασία κατά την οποία αποστέλλεται ένα email προσποιούμενο ότι προέρχεται από τράπεζα, με σκοπό την εξαπάτηση του χρήστη ώστε να "ψαρέψει" πληροφορίες για την υποκλοπή δεδομένων του. Το mail προτρέπει τον χρήστη-στόχο να εισέλθει σε έναν πλαστό ιστότοπο και να συμπληρώσει προσωπικές και απόρρητες πληροφορίες ακόμα και κωδικούς και αριθμούς καρτών (Bartlett, 2014).

6. Pharming

Σαν αναβάθμιση του Phishing, το Pharming πήγε ένα βήμα παραπέρα και αποτελεί την νέα τάση των εισβολέων. Η νέα μέθοδος μπορεί:

- Να κάνει μαζικές επιθέσεις σε πολλούς χρήστες και όχι πια μεμονωμένα και,
- Η μετακίνηση σε Pharming site να γίνεται χωρίς την παρεμβολή του χρήστη (Wehinger, 2011).

7. Καταγραφή πληκτρολογήσεων (Key Loggers)

Αυτό συμβαίνει όταν καταγράφονται οι πληκτρολογήσεις του χρήστη χωρίς να το ξέρει και φυσικά χωρίς να το επιτρέπει. Αποτελεί μια από τις σοβαρότερες απειλές στην διαρροή προσωπικών δεδομένων. Η παρακολούθηση της πληκτρολόγησης γίνεται με την χρησιμοποίηση ειδικού υλικού, εύκολου στην εγκατάσταση μα ταυτόχρονα δύσκολου στον εντοπισμό. Τα key loggers καταγράφουν τις πληκτρολογήσεις και τα κλικ του ποντικιού σε ειδικό αρχείο, το οποίο αποστέλλεται μέσω του διαδικτύου σε αυτόν που παρακολουθεί το χρήστη (Von Lohmann, 2004).

3.2 Γενικά – Norse IP Viking

Η χρήση του ίντερνετ έχει και κάποιους κινδύνους, με σημαντικότερο τον κίνδυνο του hacking. Τα αποτελέσματα του hacking συνήθως δεν είναι ορατά σε κάποιον που δεν είναι γνώστης. Ωστόσο, οι ηλεκτρονικές αυτές επιθέσεις είναι πολυάριθμες, με τις περισσότερες να συμβαίνουν μεταξύ της Κίνας και των Ηνωμένων Πολιτειών.

Η Norse, εταιρεία που ασχολείται με την ασφάλεια του διαδικτύου, με την δημιουργία του Norse – IP Viking, παρέχει πληροφορίες για τις διαδικτυακές επιθέσεις με σκοπό να ενημερώνει και να βοηθά τους πελάτες της να αντιμετωπίζουν ή να αποφεύγουν τέτοιες επιθέσεις, ανιχνεύοντας τις απειλές παγκοσμίως. Το IP Viking είναι ένα σύστημα πληροφοριών στον κυβερνοχώρο παγκοσμίως που παρακολουθεί τις επιθέσεις σε πραγματικό χρόνο και τις σταματάει. Πρόκειται για έναν online χάρτη σε πραγματικό χρόνο που ενημερώνει για το ποιοι πραγματοποιούν επιθέσεις, ποιοι τις δέχονται και τι είδους επιθέσεις συμβαίνουν.

Οι «πράκτορες» του IP Viking παρακολουθούν και ελέγχουν καθημερινά 19 terabytes με πληροφορίες σχετικά με τις επιθέσεις στο darknet. Έτσι η Norse μπορεί να παρακολουθεί τις εξελίξεις των επιθέσεων και προσπαθεί να δελεάσει και να παγιδεύσει hackers με την χρήση χιλιάδων «honeypots». Μέσω αυτών των honeypots η Norse προσπαθεί επίσης να εξαπατήσει κακόβουλα εργαλεία με σκοπό να μάθει πληροφορίες, όπως η ip address, την οποία χρησιμοποιεί για να παρακολουθεί τις δραστηριότητες.

Παρ' όλο που η έκταση και ο σκοπός των επιθέσεων στο darknet ποικίλει, δεν μπορούμε να αμφισβητήσουμε το γεγονός ότι ο κυβερνοπόλεμος αυτός αποτελεί μεγάλο πρόβλημα σε όλον τον πλανήτη. Συμβαίνει πολλές φορές απλοί χρήστες του ίντερνετ, μικρές αλλά και μεγαλύτερες επιχειρήσεις να βοηθούν hackers να πραγματοποιούν επιθέσεις εν άγνοιά τους. Όπως έχει αναφέρει και ο διευθυντής marketing της Norse «Υπάρχει ένα σημαντικό ποσοστό των χρηστών του διαδικτύου σήμερα που αποτελούν μέρος ενός botnet και δεν το ξέρουν. Και σκοπεύουμε να βοηθήσουμε να μειώσουμε κατά πολύ αυτόν τον αριθμό.».

Σε αυτό το δεύτερο μέρος της εργασίας θα δούμε αναλυτικά την σελίδα της Norse – IP Viking και τις πληροφορίες που μας προσφέρει.

3.3 Η σελίδα Norse – IP Viking

Μπαίνοντας στο http://hp.ipviking.com/ βλέπουμε τις επιθέσεις στο darknet στον παγκόσμιο χάρτη, σε πραγματικό χρόνο. Βλέπουμε δηλαδή τις κυβερνοεπιθέσεις που γίνονται την συγκεκριμένη χρονική στιγμή, παγκοσμίως.

Ταυτόχρονα, στην σελίδα είναι ανοιχτοί τέσσερις πίνακες. Ο πρώτος μας ενημερώνει για το ποιες χώρες κάνουν επιθέσεις, ο δεύτερος για το ποιες χώρες δέχονται επιθέσεις και στον τρίτο πίνακα μπορούμε να δούμε τι είδους επιθέσεις γίνονται. Ο

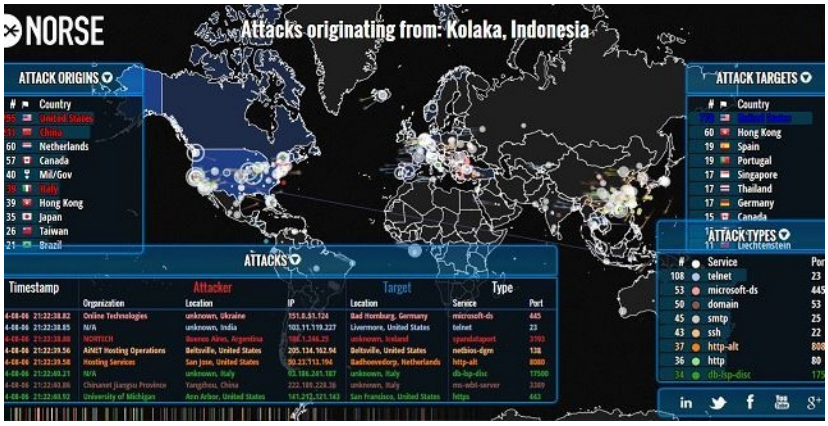
τελευταίος πίνακας είναι ένας συγκεντρωτικός και πιο αναλυτικός πίνακας. Πρόκειται για τον πίνακα που μας προσφέρει όλες τις πληροφορίες σχετικά με καθεμιά επίθεση που λαμβάνει χώρα, όση ώρα έχουμε ανοιχτή την σελίδα.

3.4 Attack origins

Στο πάνω αριστερό μέρος της σελίδας βλέπουμε τον πίνακα που μας ενημερώνει σχετικά με το ποιες χώρες πραγματοποιούν τις κυβερνοεπιθέσεις, συμπεριλαμβάνοντας τις δέκα χώρες με τις περισσότερες επιθέσεις. Ο πίνακας αποτελείται από τρεις στήλες. Η πρώτη αναφέρεται στον αριθμό των επιθέσεων που κάνει η κάθε χώρα, ενώ η δεύτερη και η τρίτη αντίστοιχα είναι η σημαία και η χώρα που πραγματοποιεί τις επιθέσεις. Με κόκκινο χρώμα σημειώνονται οι χώρες που πραγματοποιούν επίθεση την εκάστοτε χρονική στιγμή.

Αν παρατηρήσουμε, θα δούμε ότι συνήθως – αν όχι πάντα – οι δύο πρώτες χώρες είναι η Κίνα και οι Ηνωμένες Πολιτείες.

Αν περάσουμε το ποντίκι μας από κάποια χώρα του πίνακα αυτού, θα δούμε στον χάρτη τις επιθέσεις που πραγματοποιεί η χώρα αυτή τη δεδομένη χρονική στιγμή. Για να δούμε πιο συγκεκριμένα τις επιθέσεις που γίνονται από μια περιοχή, ακόμα κι αν δεν βρίσκεται στον πίνακα, μπορούμε να δείξουμε την περιοχή αυτή στον χάρτη, στο κέντρο της σελίδας. Επομένως μπορούμε ακόμα να δούμε και τις επιθέσεις που γίνονται από μέρη της Ελλάδας, όπως η Αθήνα ή η Λάρισα, δείχνοντας απλά τις περιοχές αυτές πάνω στον χάρτη. Στην εικόνα που ακολουθεί βλέπουμε τις επιθέσεις που γίνονται.



Norse IP Viking live map

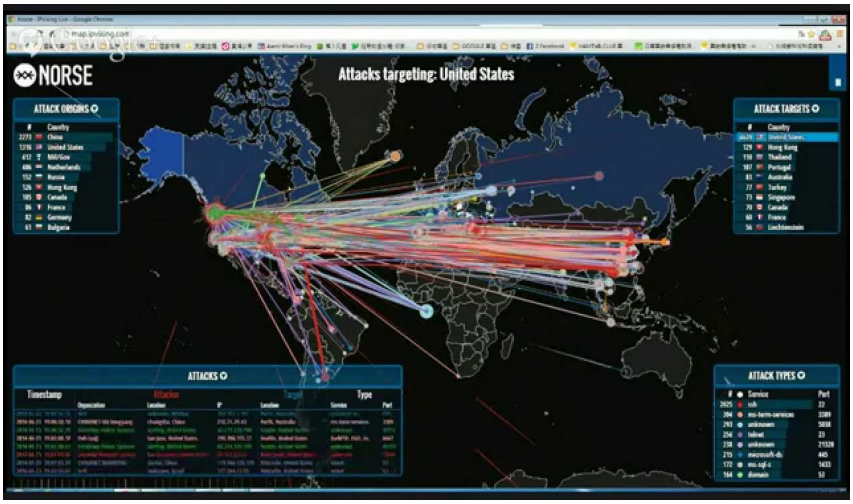
3.5 Οι χώρες-στόχοι των επιθέσεων

Ο πίνακας με τον αντίστοιχο τίτλο «Attack targets» μας πληροφορεί για τις δέκα χώρες που δέχονται τις περισσότερες επιθέσεις. Αντίστοιχα με τον προηγούμενο πίνακα, έτσι και αυτός με τους στόχους των κυβερνοεπιθέσεων μας δείχνει πρώτα τον αριθμό των επιθέσεων που δέχεται η κάθε χώρα και στη συνέχεια ακολουθεί η σημαία και η χώρα-στόχος, ενώ με μπλε χρώμα αναγράφεται η χώρα που δέχεται κάποια επίθεση την εκάστοτε χρονική στιγμή.

Πρώτη στην λίστα των στόχων βρίσκονται πάντα οι Ηνωμένες Πολιτείες, με μεγάλη διαφορά στον αριθμό επιθέσεων από την επόμενη χώρα.

Στο σημείο αυτό πρέπει να πούμε ότι οι χώρες του πίνακα «Attack origins» δεν βρίσκονται απαραίτητα και στον πίνακα "Attack targets". Για παράδειγμα, στην παρακάτω εικόνα, βλέπουμε ότι η Κίνα και η Γερμανία πραγματοποιούν επιθέσεις προς άλλες χώρες, ωστόσο δεν βρίσκονται ανάμεσα στις χώρες-στόχους τους αντίστοιχου πίνακα. Αντίστροφα, ενώ η Πορτογαλία και η Ταϊλάνδη δεν βρίσκονται στον πρώτο πίνακα, παρατηρούμε ότι δέχονται πλήθος επιθέσεων.

Αντίστοιχα με τον πίνακα "Attack origins", μπορούμε να ελέγξουμε πόσες επιθέσεις δέχεται μια χώρα τη δεδομένη χρονική στιγμή. Αυτό γίνεται άπλα δείχνοντας με τον κέρσορά μας στην χώρα του πίνακα "Attack targets" που επιθυμούμε και βλέπουμε στον χάρτη ζωντανά τις επιθέσεις που δέχεται.



Norse IP Viking, Attack targets

3.6 Οι τύποι των επιθέσεων στο Darknet

Στην κάτω δεξιά γωνία της οθόνης βλέπουμε τους οκτώ τύπους επιθέσεων που πραγματοποιούνται περισσότερο κατά την διάρκεια που έχουμε ανοιχτή την σελίδα. Η πρώτη στήλη μας δείχνει το σύνολο κάθε τύπου επίθεσης και η δεύτερη αποδίδει από ένα χρώμα σε κάθε τύπο επίθεσης. Η τρίτη στήλη μας ενημερώνει για τον τύπο

των επιθέσεων με βάση την υπηρεσία (service) που χρησιμοποιείται. Στην συνέχεια, υπάρχει μια τέταρτη στήλη ακόμα, η οποία καταγράφει την θύρα (port) των αντίστοιχων services.

3.7 Οι επιθέσεις συγκεντρωτικά

Στον τελευταίο πίνακα, κάτω αριστερά, βλέπουμε όλα τα στοιχεία των επιθέσεων που γίνονται στο darknet. Ο πίνακας "Attacks" χωρίζεται σε τέσσερεις κατηγορίες στηλών:

i. Timestamp: Σε αυτήν την κατηγορία πληροφοριών έχουμε δύο στήλες, η πρώτη με την ημερομηνία της επίθεσης και η δεύτερη με την ακριβή ώρα.
ii. Attacker: Οι πληροφορίες που παίρνουμε για αυτούς που πραγματοποιούν τις κυβερνοεπιθέσεις είναι η οργάνωση από την οποία γίνονται η επιθέσεις, η τοποθεσία στην οποία βρίσκεται και η ip address.
iii. Target: Πρόκειται για την χώρα στόχο της επίθεσης. Πιο συγκεκριμένα, αναγράφεται η πόλη και η χώρα η οποία δέχεται την εκάστοτε επίθεση.
iv. Type: Στο τέλος αναγράφεται ο τύπος της επίθεσης που γίνεται, με την πρώτη στήλη να μας δείχνει την υπηρεσία (service) και την δεύτερη την θύρα (port) που χρησιμοποιείται για να πραγματοποιηθεί η επίθεση.

Κάθε γραμμή του πίνακα αυτού αποτελεί μία επίθεση, για την οποία μας δίνει τα στοιχεία που αναφέρθηκαν παραπάνω. Κάθε επίθεση (γραμμή) έχει διαφορετικό χρώμα ανάλογα με τον τύπο της επίθεσης. Το χρώμα αυτό το παίρνει από την δεύτερη στήλη του πίνακα "Attack Types".

3.8 Οι κυβερνοεπιθέσεις στον παγκόσμιο χάρτη

Ταυτόχρονα στο κέντρο της σελίδας βλέπουμε τον παγκόσμιο χάρτη, όπου φαίνονται οι επιθέσεις που γίνονται παγκοσμίως σε πραγματικό χρόνο. Φαίνονται οι χώρες που πραγματοποιούν και οι χώρες που δέχονται τις κυβερνοεπιθέσεις και συνδέονται μεταξύ τους με τις αντίστοιχες διαγραμμίσεις που συμβολίζουν την καθεμιά επίθεση. Οι διαγραμμίσεις αυτές παίρνουν το χρώμα τους από την δεύτερη στήλη του πίνακα "Attack types". Έτσι μπορούμε να καταλάβουμε μέσω του χάρτη την χώρα από την οποία προέρεται η επίθεση, την χώρα η οποία δέχεται την επίθεση και τον τύπο της κάθε επίθεσης.

ΚΕΦΑΛΑΙΟ 4 – ΕΡΕΥΝΑ – ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΙΣ ΕΠΙΘΕΣΕΙΣ ΣΤΟ DARKNET

4.1 Παρουσίαση της έρευνας

Σε αυτό το κεφάλαιο θα δούμε τα στατιστικά στοιχεία για τις επιθέσεις που έγιναν στο darknet τον Ιούνιο του 2016. Θα δούμε δηλαδή ποιες είναι οι χώρες που κάνουν τον μεγαλύτερο αριθμό επιθέσεων και ποιες είναι αυτές που δέχονται τις περισσότερες επιθέσεις, αλλά και άλλα στοιχεία και λεπτομέρειες των επιθέσεων αυτών.

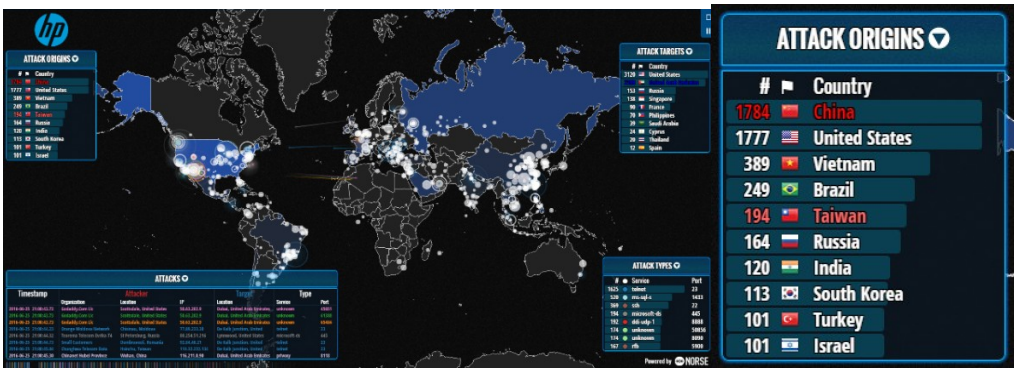
Για την έρευνα αυτή, συγκεντρώναμε τα απαιτούμενα στοιχεία καθημερινά για τον μήνα Ιούνιο του 2016 τις παρακάτω ώρες: 9:00, 14:00, 19:00 και 00:00. Για κάθε φορά που συγκεντρώναμε τα στοιχεία των επιθέσεων η σελίδα της Norse, http://hp.ipviking.com/, παρέμενε ανοιχτή για 15 λεπτά. Αυτό γίνεται για να παρέχεται στην σελίδα ο απαιτούμενος χρόνος να καταγράψει αρκετές επιθέσεις, αφού αυτές αρχίζουν να καταγράφονται την χρονική στιγμή που ανοίγει η σελίδα. Έτσι, αν ανοίγαμε την σελίδα και καταγράφαμε αμέσως τις κυβερνοεπιθέσεις, τα αποτελέσματα δεν θα ήταν έγκυρα.

Τα αποτελέσματα που θα αναλυθούν και θα αξιολογηθούν παρακάτω αντιστοιχούν σε συνολικά 30 ώρες κατά τις οποίες ήταν ανοιχτή η σελίδα της Norse, για 15 λεπτά, σε 4 διαφορετικές ώρες την ημέρα και για κάθε ημέρα του Ιουνίου.

4.2 Οι κυβερνοεπιθέσεις αναφορικά με τις χώρες προέλευσης

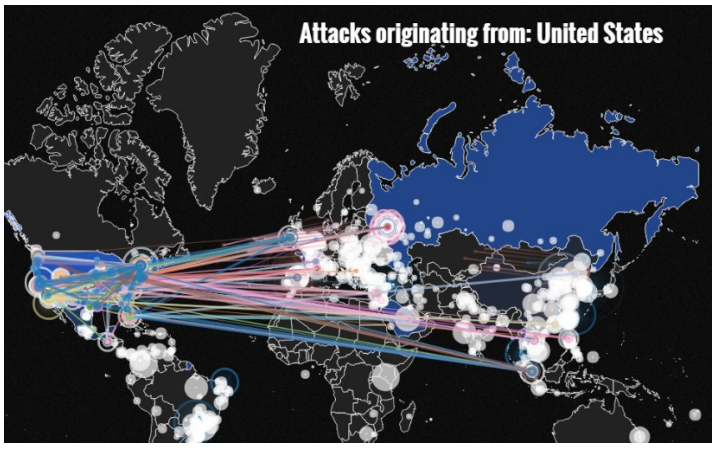
Σε αυτήν την ενότητα αναλύονται τα αποτελέσματα της έρευνας όσον αφορά τις χώρες από τις οποίες προέρχονται οι επιθέσεις στο darknet. Οι απαραίτητες πληροφορίες αντλούνται από τον πίνακα της σελίδας http://hp.ipviking.com/ με τον τίτλο Attack Origins, καταγράφοντας τα στοιχεία που παρέχει τις τέσσερεις προκαθορισμένες ώρες τις ημέρας και κάθε μέρα για ολόκληρο το χρονικό διάστημα που διαρκεί η έρευνα.

Η παρακάτω εικόνα είναι ενδεικτική των επιθέσεων που έγιναν κατά τη διάρκεια του μήνα. Συγκεκριμένα απεικονίζει τις επιθέσεις στο darknet που πραγματοποιήθηκαν το βράδυ της 26ης Ιουνίου. Οι χώρες με τις περισσότερες επιθέσεις στο ενεργητικό τους βρίσκονται στη λίστα του πίνακα Attack Origins.

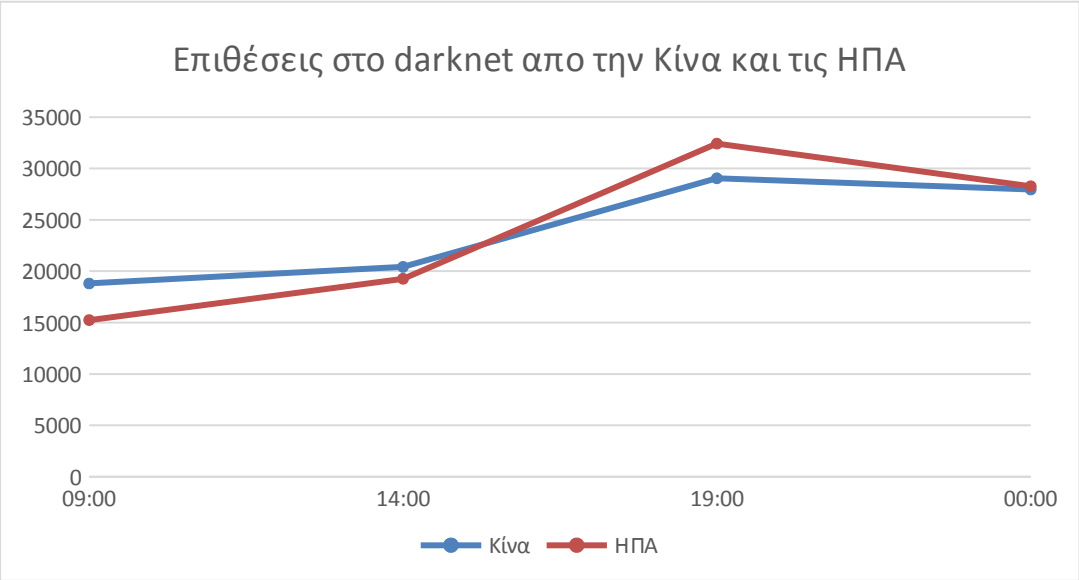


Η Κίνα ήταν πράγματι η χώρα από την οποία έγιναν οι περισσότερες επιθέσεις, που έφτασαν τον αριθμό των 96.202, στο σύνολο των 30 ωρών παρακολούθησης. Παρατηρήθηκε ότι οι επιθέσεις της Κίνας αυξάνονταν μέχρι το απόγευμα ενώ το βράδυ είχαν μια μικρή μείωση. Τις πρωινές ώρες του μήνα οι επιθέσεις ανέρχονται στις 18.798. Στη συνέχεια, τις ώρες του μεσημεριού οι κυβερνοεπιθέσεις φτάνουν τις 20.417. Τις απογευματινές ώρες βρίσκονται στο υψηλότερο σημείο τους με 29.039 επιθέσεις, για να καταλήξουν τις νυχτερινές ώρες στις 27.948.

Μετά την Κίνα ακολουθούν οι Ηνωμένες Πολιτείες της Αμερικής με 95.176 επιθέσεις για το ίδιο χρονικό διάστημα. Στην περίπτωση των Ηνωμένων Πολιτειών, οι επιθέσεις αυξάνονται κατά τη διάρκεια όλης της ημέρας. Στις 09:00 καταγράφεται ότι η χώρα πραγματοποιεί 15.237 κυβερνοεπιθέσεις και συνεχίζει με άλλες 19.259 επιθέσεις (ώρα 14:00). Στις 19:00 βρίσκουμε τις ΗΠΑ στο ζενίθ των επιθέσεών της, οι οποίες φτάνουν τις 32.411, και στη συνέχεια καταλήγουν στις 28.269 κυβερνοεπιθέσεις για τον μήνα που εξετάζουμε.

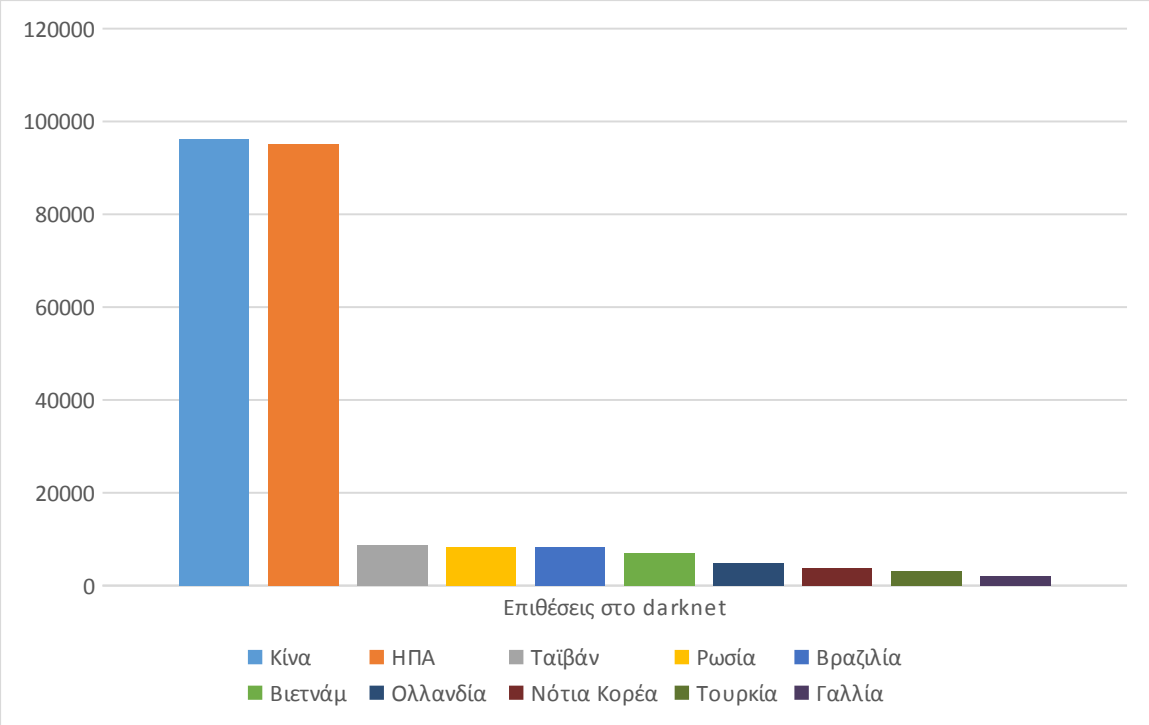


Οι δύο αυτές χώρες είχαν και το μεγαλύτερο ποσό επιθέσεων με μεγάλη διαφορά από τις χώρες που ακολουθούν. Ωστόσο, όπως φαίνεται και στο παρακάτω γράφημα, οι μεταξύ τους διαφορές δεν είναι πολύ μεγάλες.



Άλλες χώρες που σημειώνονται με μεγάλο αριθμό επιθέσεων να προέρχεται από αυτές είναι η Ταιβάν με 8.691 επιθέσεις, η Ρωσία με 8.380 επιθέσεις και η Βραζιλία με 8.221 επιθέσεις. Στη συνέχεια ακολουθούν το Βιετνάμ, η Ολλανδία και η Νότια Κορέα με 6.926, 4.813 και 3.797 επιθέσεις αντίστοιχα. Τέλος, έρχεται η Τουρκία η οποία ευθύνεται για 3.228 επιθέσεις στο darknet και η Γαλλία με 2.091 επιθέσεις.

Στο παρακάτω γράφημα φαίνονται συγκεντρωτικά οι χώρες με τις περισσότερες επιθέσεις συνολικά για τις 30 ώρες του Ιουνίου.



Με τη βοήθεια του γραφήματος είναι κατάφορο ότι η Κίνα και οι Ηνωμένες Πολιτείες ευθύνονται για το μεγαλύτερο ποσοστό των επιθέσεων στο darknet, ενώ όλες οι υπόλοιπες χώρες ευθύνονται για πολύ λιγότερες κυβερνοεπιθέσεις. Ενώ οι δύο πρώτες χώρες πραγματοποίησαν πάνω από 95.000 επιθέσεις η καθεμία, καμία άλλη χώρα δεν έφτασε τις 10.000, με αποτέλεσμα η διαφορά τους να υψώνεται σε πάνω από 85.000 επιθέσεις.

Βλέπουμε ότι η Γαλλία που είναι δέκατη σε σειρά, πραγματοποίησε 2.091 κυβερνοεπιθέσεις στις 30 ώρες παρακολούθησης. Ο αριθμός αυτός φαίνεται πολύ μικρός, ειδικά σε σύγκριση με τις πρώτες χώρες – Κίνα, ΗΠΑ- ακόμα και με τις τρεις επόμενες που είναι η Ταϊβάν, η Ρωσία και η Βραζιλία. Ωστόσο, πρέπει να αναλογιστούμε ότι εκτός από αυτές τις δέκα χώρες, υπάρχουν κι άλλες πολλές με ακόμα λιγότερες επιθέσεις, όπως η Γερμανία με 1.997, η Ινδία με 1.766 και η Κολομβία με 1.478 επιθέσεις.

Πιο συγκεκριμένα, η Ταϊβάν με 8.691 κυβερνοεπιθέσεις συνολικά το πρωί κάνει 2.417 επιθέσεις, το μεσημέρι κάνει 1.803, το απόγευμα 2.034 και το βράδυ 2.437. Παρατηρούμε ότι οι επιθέσεις μέχρι το μεσημέρι μειώνονται για να αυξηθούν αργότερα. Έτσι έχουμε τις λιγότερες επιθέσεις της χώρας να γίνονται τις ώρες του μεσημεριού και τις περισσότερες τις νυχτερινές ώρες.

Ακολουθεί η Ρωσία με 8.380 επιθέσεις, οι οποίες μειώνονται κατά τη διάρκεια της μέρας και σημειώνουν μια μικρή αύξηση τις βραδινές ώρες. Οι περισσότερες επιθέσεις από την Ρωσία γίνονται πρωινές ώρες και φτάνουν τις 2.486 και οι μεσημεριανές επιθέσεις φτάνουν τις 2.052. Οι επιθέσεις των απογευμάτων, που είναι οι λιγότερες από τη Ρωσία είναι 1.704, ενώ μετά αυξάνονται στις 2.138 για τις βραδινές ώρες του Ιουνίου.

Η Βραζιλία έφτασε συνολικά τις 8.221 επιθέσεις, μοιράζοντάς τες σχετικά ισομερώς στις ώρες τις ημέρας. Συγκεκριμένα σημειώθηκαν 2.002 επιθέσεις στις 09:00, οι λιγότερες της ημέρας, 2.050 στις 14:00, 2.041 στις 19:00 και τις νύχτες οι επιθέσεις έφτασαν στο μέγιστο για την Βραζιλία, που είναι 2.128.

Το Βιετνάμ με 6.926 κυβερνοεπιθέσεις έχει τις ίδιες διακυμάνσεις με την Βραζιλία. Οι επιθέσεις που πραγματοποιούνται τις πρωινές ώρες είναι οι λιγότερες και αγγίζουν τις 1.721. Αργότερα φτάνουν τις 1.733, τα απογεύματα είναι 1.728 και τα βράδια μεγιστοποιούνται στις 1.744.

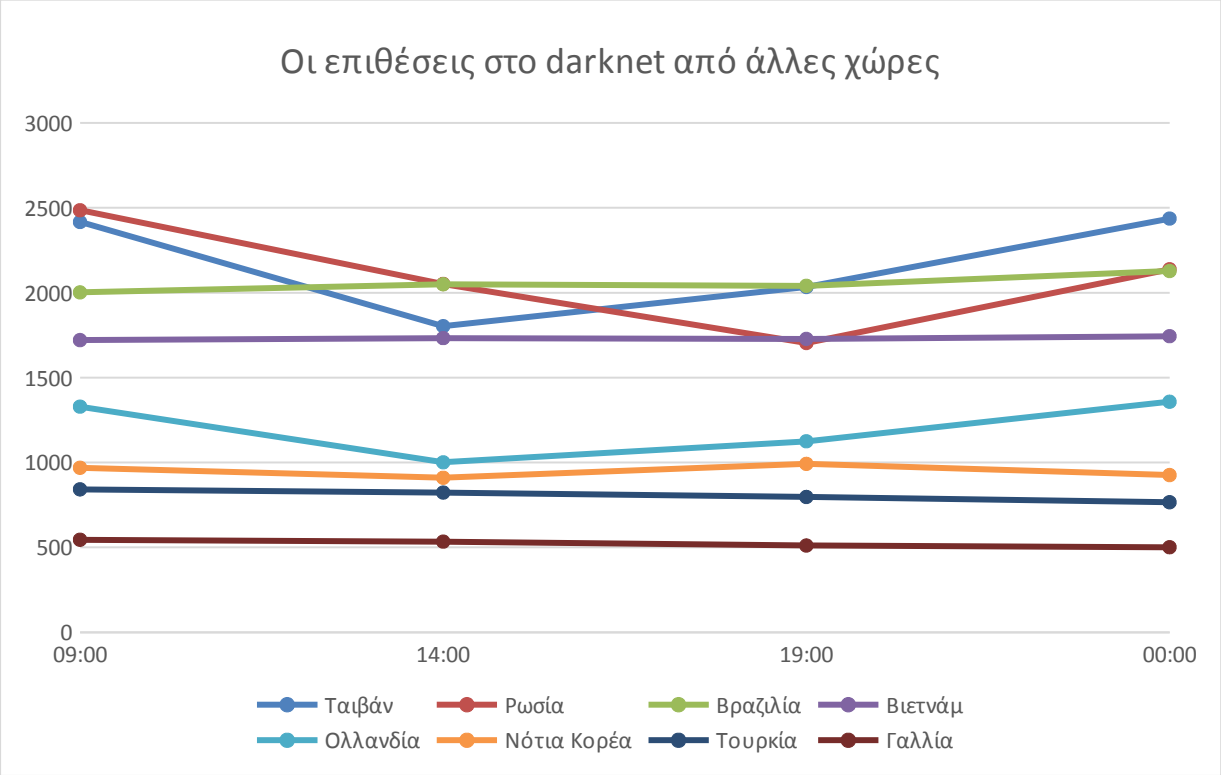
Η Ολλανδία με 4.813 επιθέσεις στο darknet έχει τις ίδιες διακυμάνσεις με την Ταϊβάν με την ελαχιστοποίηση των επιθέσεων στις 14:00 και την μεγιστοποίησή τους στις 00:00. Το πρωί η Ολλανδία έκανε 1.329 επιθέσεις. Τα μεσημέρια οι επιθέσεις έπεσαν στις 1.001. Τα απογεύματα έφτασαν τις 1.125 και τις νύχτες ανέβηκαν στις 1.358.

Ακολουθεί η Νότια Κορέα με 3.797 επιθέσεις στο σκοτεινό διαδίκτυο. Ξεκινάει με 969 κυβερνοεπιθέσεις και συνεχίζει με 910 τα μεσημέρια, που ελαχιστοποιούνται. Τα απογεύματα οι κυβερνοεπιθέσεις από τη Νότια Κορέα μεγιστοποιούνται στις 992 και τα βράδια μειώνονται πάλι στις 926.

Η Τουρκία με 3.228 επιθέσεις συνολικά ξεκινά τα πρωινά με τις περισσότερες, οι οποίες σταδιακά μειώνονται για να ελαχιστοποιηθούν τα βράδια. Έχουμε 842 επιθέσεις στις 09:00, 823 στις 14:00, 797 τα απογεύματα και 766 τα βράδια.

Τελευταία έρχεται η Γαλλία με 2.091 επιθέσεις στο darknet και την αντίστροφη διακύμανση σε σχέση με την Τουρκία. Μεγιστοποιεί τις επιθέσεις της το πρωί στις 545. Στη συνέχεια τις μειώνει στις 534 και 511 για να τις ελαχιστοποιήσει τα βράδια στις 501.

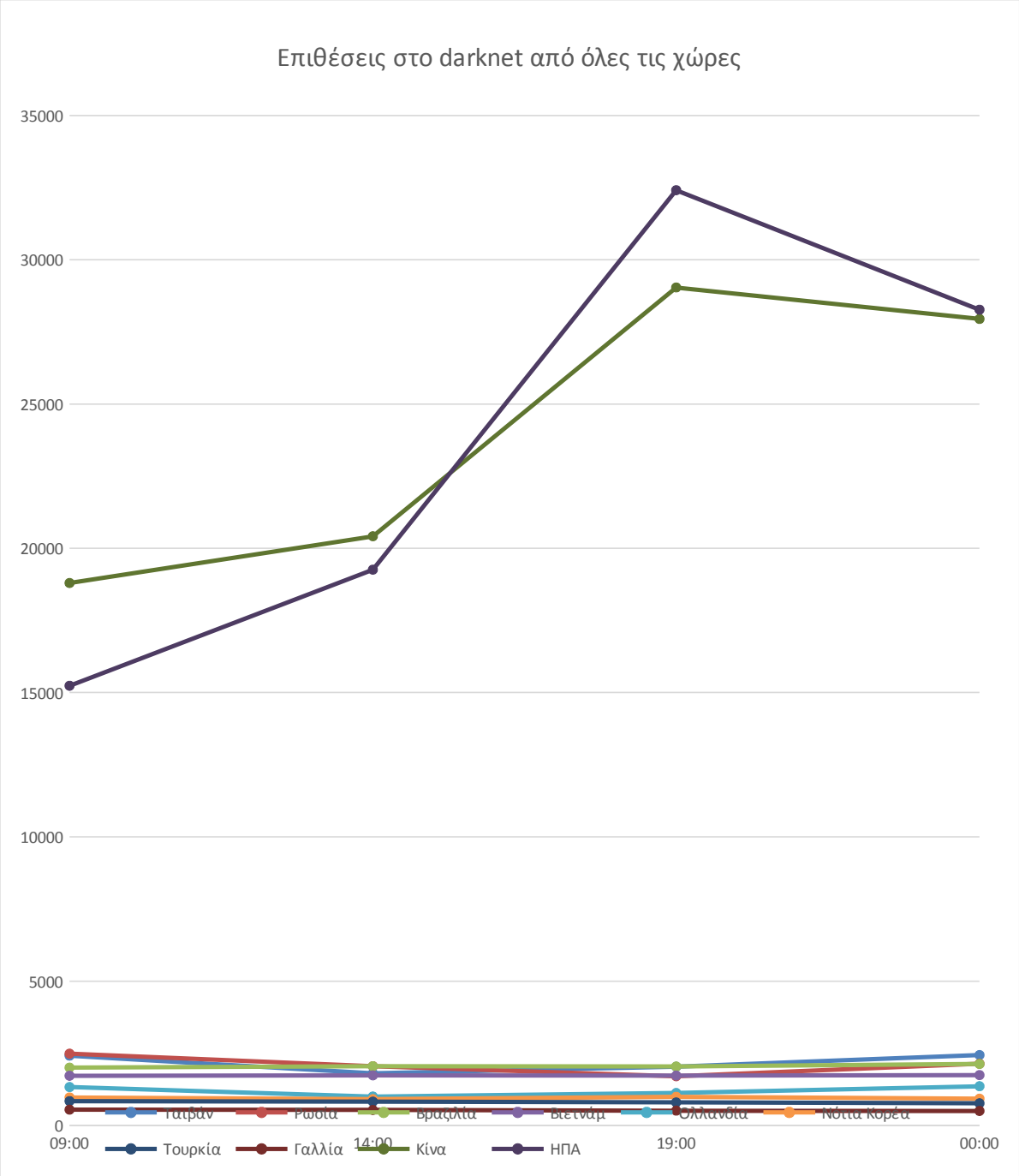
Στο γράφημα που ακολουθεί και συγκεντρώνοντας τα στοιχεία που προαναφέρθηκαν φαίνονται συνοπτικά οι επιθέσεις που έχει πραγματοποιήσει κάθε χώρα στους τέσσερεις προκαθορισμένους χρόνους ξεχωριστά.



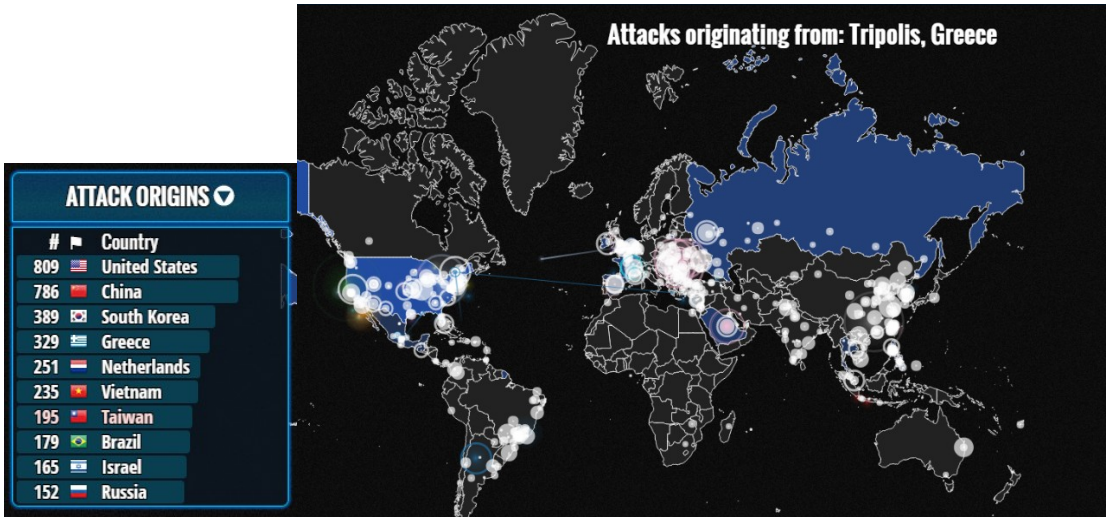
Παρατηρείται ότι κατά τη διάρκεια της ημέρας τις μεγαλύτερες διακυμάνσεις παρουσιάζουν η Ταϊβάν και η Ρωσία. Μικρότερες διακυμάνσεις παρουσιάζονται στην Ολλανδία και στη Νότια Κορέα. Επιπλέον, καταλαβαίνουμε ότι οι χώρες που απομένουν, η Βραζιλία, το Βιετνάμ, η Τουρκία και η Γαλλία, κάνουν τις ίδιες περίπου επιθέσεις όλες τις ώρες της ημέρας. Συγκεκριμένα φαίνεται στο γράφημα ότι οι επιθέσεις του Βιετνάμ σχηματίζουν μια σχεδόν ευθεία γραμμή, με τις επιθέσεις αυτές να ανέρχονται στις 1.721, 1.733, 1.728 και 1.744 αντίστοιχα για κάθε ώρα της ημέρας. Η διαφορά του μέγιστου (1.744) με τον ελάχιστο (1.721) αριθμό επιθέσεων είναι μόλις 23 κυβερνοεπιθέσεις.

Παρακάτω φαίνονται οι επιθέσεις που έκαναν στο darknet όλες οι χώρες. Έτσι μπορούμε να δούμε την διαφορά των δύο πρώτων χωρών με τις υπόλοιπες και για τις

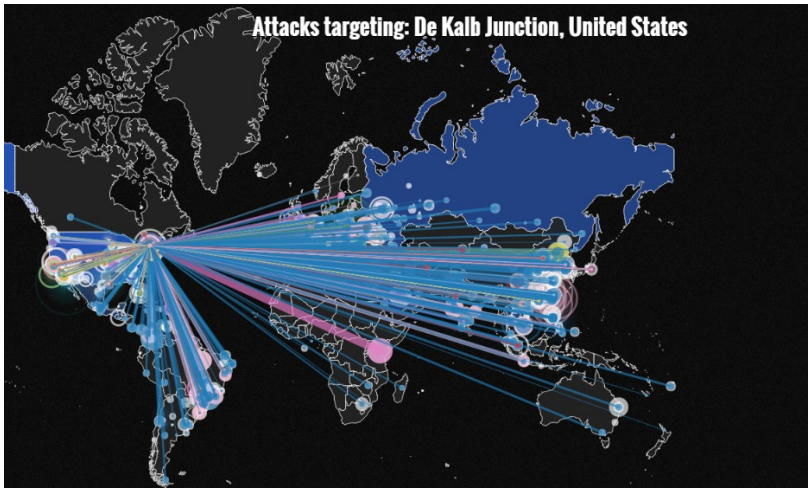
τέσσερις ώρες της ημέρας αναλυτικά. Από τις δύο πρώτες χώρες, την Κίνα και τις Ηνωμένες Πολιτείες, τις λιγότερες επιθέσεις παρουσιάζουν οι ΗΠΑ(5.237) τις πρωινές ώρες, ενώ από τις υπόλοιπες χώρες τον μεγαλύτερο αριθμό επιθέσεων έχει η Ρωσία (2.486) τις ίδιες ώρες. Η διαφορά στα νούμερα είναι εμφανής, καθώς οι Ηνωμένες Πολιτείες, στον μικρότερο αριθμό τους, ευθύνονται για πάνω από τις διπλάσιες επιθέσεις στο darknet από την Ρωσία, στον μέγιστο αριθμό επιθέσεων.



Αξιοσημείωτο είναι να πούμε ότι στην λίστα με τις χώρες που κάνουν τις περισσότερες επιθέσεις βρέθηκε και η Ελλάδα, όπως φαίνεται στην εικόνα που ακολουθεί.



Η παρουσία της χώρας μας στην λίστα αυτή έλαβε χώρα το βράδυ της 22ης Ιουνίου. Η Ελλάδα βρέθηκε τέταρτη στη σειρά, με 329 κυβερνοεπιθέσεις. Ήταν η μοναδική παρουσία της χώρας στον πίνακα "Attack origins". Ωστόσο, ανά πάσα στιγμή, ψάχνοντας στον χάρτη μπορούμε να δούμε αν γίνονται επιθέσεις από την Ελλάδα και, όταν γίνονται, μπορούμε πάντα να δούμε και την πόλη από την οποία προέρχονται. Όπως φαίνεται στην παραπάνω εικόνα οι επιθέσεις την δεδομένη χρονική στιγμή προέρχονται από την Τρίπολη. Σε γενικές γραμμές οι κυβερνοεπιθέσεις που πραγματοποιεί η χώρα μας προέρχονται κυρίως από την Αθήνα και την Τρίπολη. Επιπλέον, αξίζει να σημειωθεί ότι, όπως οι περισσότερες χώρες, έτσι και η Ελλάδα κάνει τις επιθέσεις της με χώρα-στόχο τις Ηνωμένες Πολιτείες. Συγκεκριμένα στο παράδειγμα της εικόνας που έχουμε παραπάνω, αν ακολουθήσουμε με τον κέρσορα την γραμμή που σχηματίζει η επίθεση της χώρας μας, θα δούμε ότι καταλήγει στο De Kalb Junction των Ηνωμένων Πολιτειών, μια μικρή πόλη 2.500 κατοίκων, σημείο το οποίο δέχεται μεγάλο πλήθος επιθέσεων.

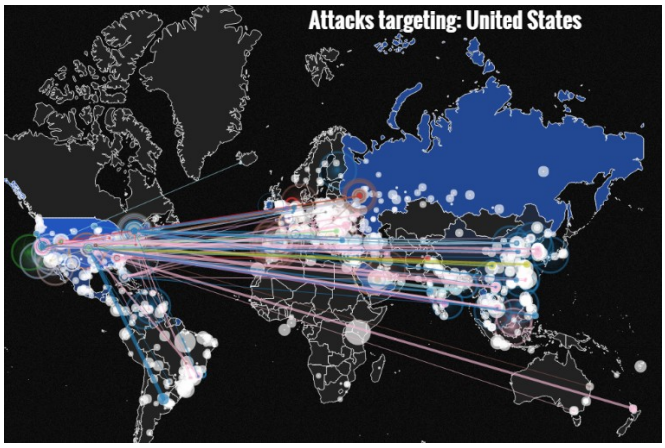


Σε άλλη περίπτωση, επιθέσεις στο darknet προέρχονται από τη Λευκάδα, με χώρα-στόχο τη Σιγκαπούρη.

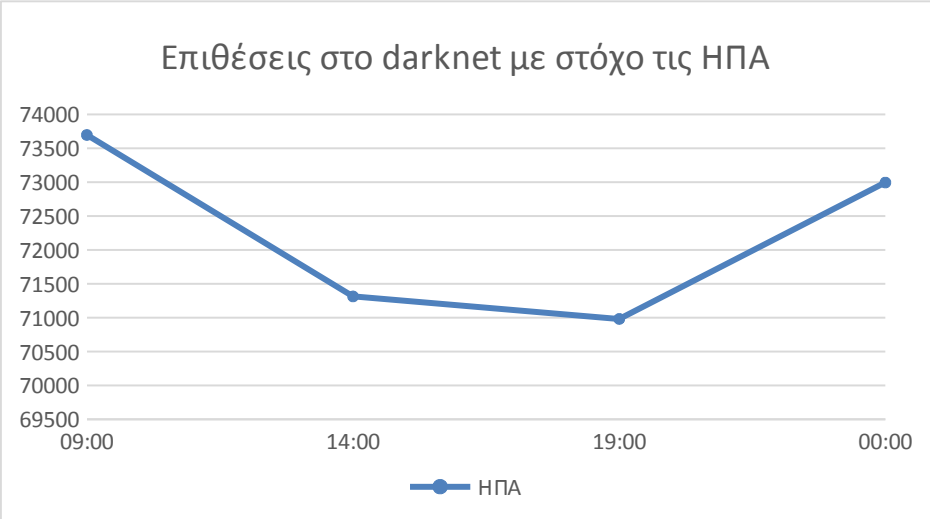
4.3 Οι επιθέσεις στο darknet αναφορικά με τις χώρες-στόχους

Στην ενότητα αυτή θα αναλυθούν τα αποτελέσματα της έρευνας όσον αφορά τις χώρες που υπήρξαν στόχοι των επιθέσεων στο darknet. Θα δούμε ποιες χώρες δέχτηκαν τις περισσότερες κυβερνοεπιθέσεις συνολικά αλλά και ξεχωριστά στους προκαθορισμένους χρόνους που ορίσαμε στην αρχή της έρευνας. Τα στοιχεία αυτά μας τα προσφέρει η ίδια σελίδα της Norse στον πίνακα που έχει τίτλο Attack Targets.

Η χώρα που αποτελεί τον στόχο των περισσότερων επιθέσεων με μεγάλη διαφορά από τις χώρες που ακολουθούν ήταν οι Ηνωμένες Πολιτείες. Στις 30 ώρες παρακολούθησης για τον μήνα Ιούνιο του 2016 οι Ηνωμένες Πολιτείες έπρεπε να αντιμετωπίσουν 288.986 επιθέσεις συνολικά.

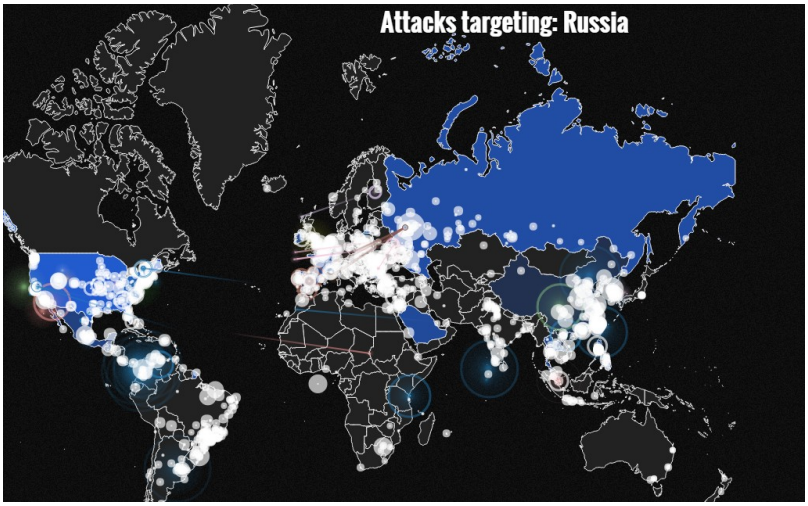


Οι περισσότερες επιθέσεις που δέχεται η χώρα πραγματοποιούνται πρωινές ώρες και αγγίζουν τις 73.696. Στις 14:00 το μεσημέρι οι κυβερνοεπιθέσεις μειώνονται στις 71.314 και το απόγευμα μειώνονται ξανά στις 70.982. στη συνέχεια τις βραδινές ώρες οι επιθέσεις αυξάνονται αρκετά και αγγίζουν τις 72.994.



Είναι αξιοσημείωτο ότι οι Ηνωμένες Πολιτείες δέχονται τις περισσότερες επιθέσεις. Είναι ο μεγαλύτερος στόχος στο σκοτεινό διαδίκτυο παγκοσμίως, αφού η επόμενη χώρα-στόχος συγκεντρώνει μόνο 8.735 επιθέσεις. Τις επιθέσεις αυτές καλείται να αντιμετωπίσει η Ρωσία, η οποία έχει διακυμάνσεις παρόμοιες με αυτές των

Ηνωμένων Πολιτειών. Ωστόσο, δεν είναι τόσο έντονες, καθώς οι διαφορές στο πλήθος τους την κάθε ώρα δεν ξεπερνούν τις 250. Στις 09:00 δέχτηκε κατά τη διάρκεια του μήνα 2.267 κυβερνοεπιθέσεις, ενώ τα μεσημέρια έφτασαν στο ελάχιστο, τις 2.063. Στην συνέχεια, οι επιθέσεις αυξάνονται στις 2.101 για να μεγιστοποιηθούν τις βραδινές ώρες στις 2.304.



Ακολουθεί η Γαλλία με 8.324 επιθέσεις οι οποίες αυξάνονται κατά τη διάρκεια της ημέρας. Το πρωί έχουν 1.844 επιθέσεις, το μεσημέρι έχει 1.902, απόγευμα έχει 2.126 και στο τέλος της ημέρας οι επιθέσεις αγγίζουν τις 2.452.

Η Σαουδική Αραβία δέχτηκε 8.247 επιθέσεις στο darknet σε 30 ώρες, αριθμός με σχετικά μικρή διαφορά από αυτούς των δύο προηγούμενων χωρών. Στην αρχή της ημέρας η Σαουδική Αραβία αποτελεί στόχο 2.362 επιθέσεων, οι οποίες αργότερα μειώνονται στις 1.804. Τις απογευματινές ώρες η χώρα δέχτηκε 2.003 επιθέσεις, οι οποίες στο τέλος της ημέρας έφτασαν τις 2.078.

Επόμενη είναι η Ιρλανδία που συγκέντρωσε 1.827, 710, 1.764 και 1.799 κυβερνοπειθέσεις στους τέσσερεις προκαθορισμένους για την έρευνα χρόνους. Το σύνολο των επιθέσεων που είχαν ως στόχο την Ιρλανδία ήταν 6.109.

Η Σιγκαπούρη με τη σειρά της δέχτηκε 5.776 κυβερνοεπιθέσεις συνολικά για τις 30 ώρες. Στις 09:00 η Σιγκαπούρη δέχτηκε 1.481 επιθέσεις και στις 14:00 δέχτηκε 1.385. Οι επιθέσεις τα απογεύματα έφτασαν τις 1.397, ενώ τις βραδινές ώρες αυξήθηκαν στις 1.513.

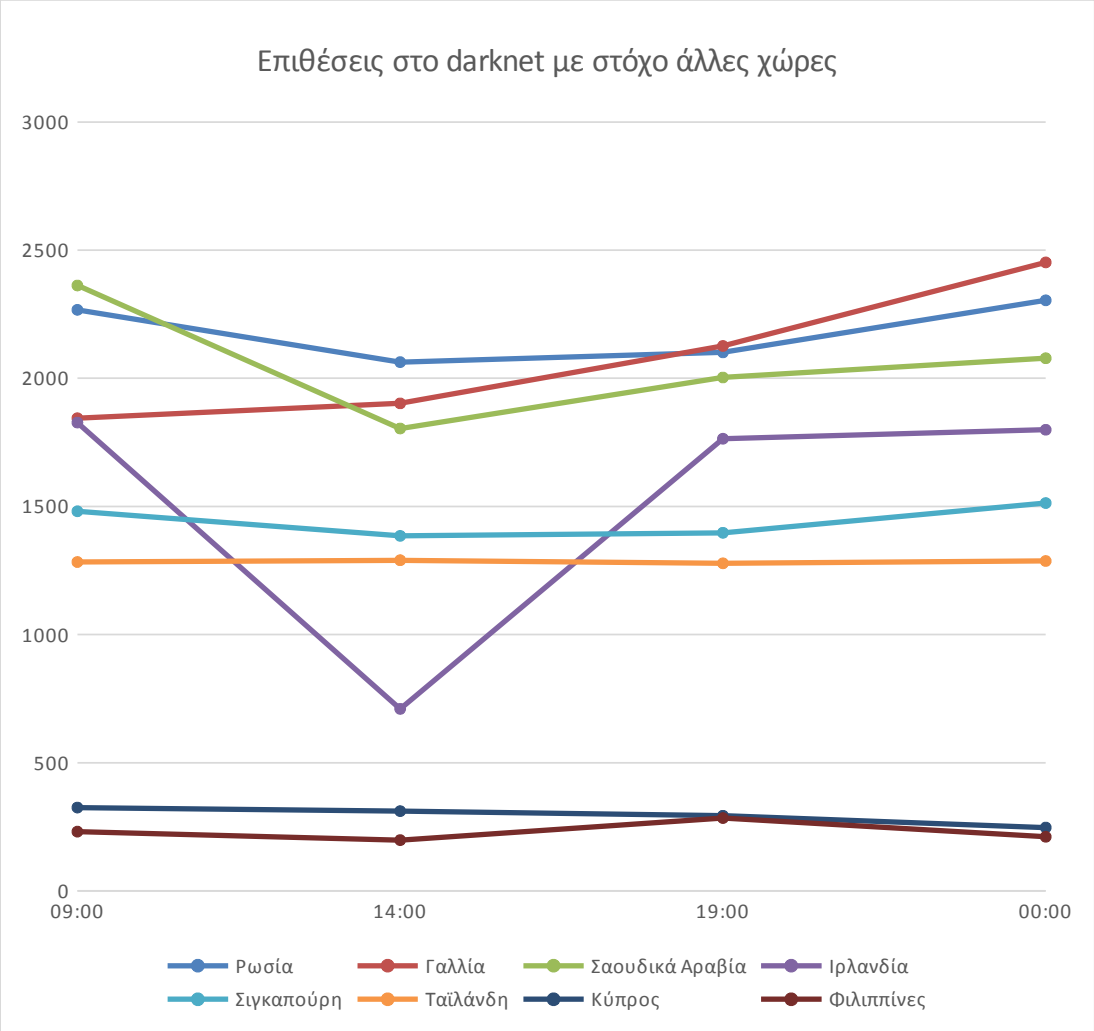
Επίσης, παρατηρήθηκε ότι η Ταϊλάνδη με 5.138 επιθέσεις συνολικά για τις 30 ώρες, δεχόταν τις επιθέσεις με σταθερούς ρυθμούς κατά την διάρκεια ολόκληρης της ημέρας. Ξεκινά με 1.283 επιθέσεις. Συνεχίζει με 1.290 και προχωρά στις 1.278 και στις 1.287.

Η Ισπανία έχει μικρότερο συνολικό αριθμό επιθέσεων, που φτάνει τις 4.313. Οι επιθέσεις που δέχεται αυξάνονται με την πάροδο των ωρών μέχρι το τέλος της ημέρας. Τα πρωινά η χώρα συγκεντρώνει μόλις 746 επιθέσεις, οι οποίες ακολουθούν ανοδική πορεία και φτάνουν τις 989, τις 1.122 και καταλήγουν στις 1.456.

Η Κύπρος αποτελεί στόχο πολύ λιγότερων επιθέσεων, καθώς φτάνουν μόνο τις 1.176. Αρχικά, δέχεται 325 επιθέσεις και ακολουθεί μια μείωση με 311 και 293 επιθέσεις και καταλήγει στις 247 κυβερνοεπιθέσεις.

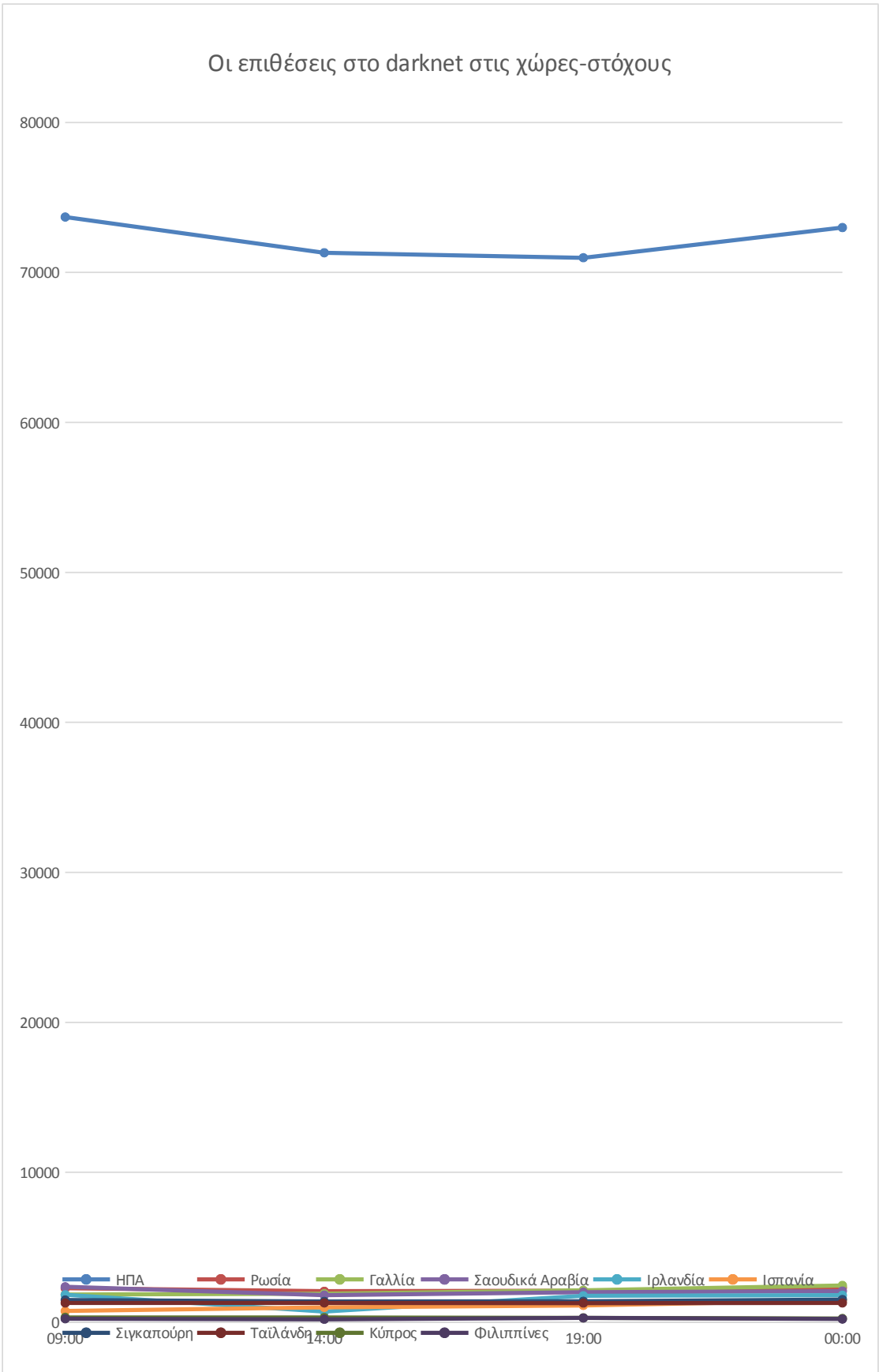
Στο τέλος βρίσκονται οι Φιλιππίνες που δέχτηκαν μόνο 924 επιθέσεις σε 30 ώρες. Τις πρωινές ώρες η χώρα δέχτηκε 231 επιθέσεις στο darknet, οι οποίες μετά από πέντε ώρες έγιναν 198, για να αυξηθούν πάλι στις 284. Τα βράδια οι Φιλιππίνες δέχτηκαν 211 επιθέσεις.

Για να γίνουν οι παραπάνω πληροφορίες πιο κατανοητές προσφέρεται το παρακάτω γράφημα, στο οποίο φαίνονται όλες οι επιθέσεις που δέχτηκαν οι χώρες-στόχοι.



Παρατηρείται ότι τις μεγαλύτερες διακυμάνσεις στις επιθέσεις που δέχονται τις έχουν οι Ηνωμένες Πολιτείες και η Ιρλανδία. Η πρώτη έχει μια διαφορά 2.714 (73.696-70.982) επιθέσεων ανάμεσα στον μέγιστο και στον ελάχιστο αριθμό επιθέσεων που δέχτηκε. Παρομοίως η Ιρλανδία παρουσιάζει διαφορά 1.117 (1.827-710) επιθέσεων. Ωστόσο, δεν παρατηρείται μεγάλη διαφορά ανάμεσα στις επιθέσεις που δέχεται τις απογευματινές και τις βραδινές ώρες, η οποία είναι μόνο 35 επιθέσεις (1.799-1764).

Επιπλέον, αξιοσημείωτο είναι ότι οι Ηνωμένες Πολιτείες με τις λιγότερες επιθέσεις να είναι 70.982 είναι πολλαπλάσιες από τις επιθέσεις που δέχτηκε η Γαλλία τις βραδινές ώρες, που σημειώθηκε το μεγαλύτερο πλήθος και είναι 2.452.



Καλό θα ήταν να δούμε και τις συνολικές επιθέσεις που δέχτηκαν οι χώρες στόχοι σε ένα γράφημα. Εν συντομία παρακάτω είναι οι συνολικές επιθέσεις που δέχτηκαν οι δέκα μεγαλύτερες χώρες-στόχοι στις 30 ώρες παρακολούθησης τον Ιούνιο:

Ηνωμένες Πολιτείες: 288.986 επιθέσεις

Ρωσία: 8.735 επιθέσεις

Γαλλία: 8.324 επιθέσεις

Σαουδική Αραβία: 8.247 επιθέσεις

Ιρλανδία: 6.109 επιθέσεις

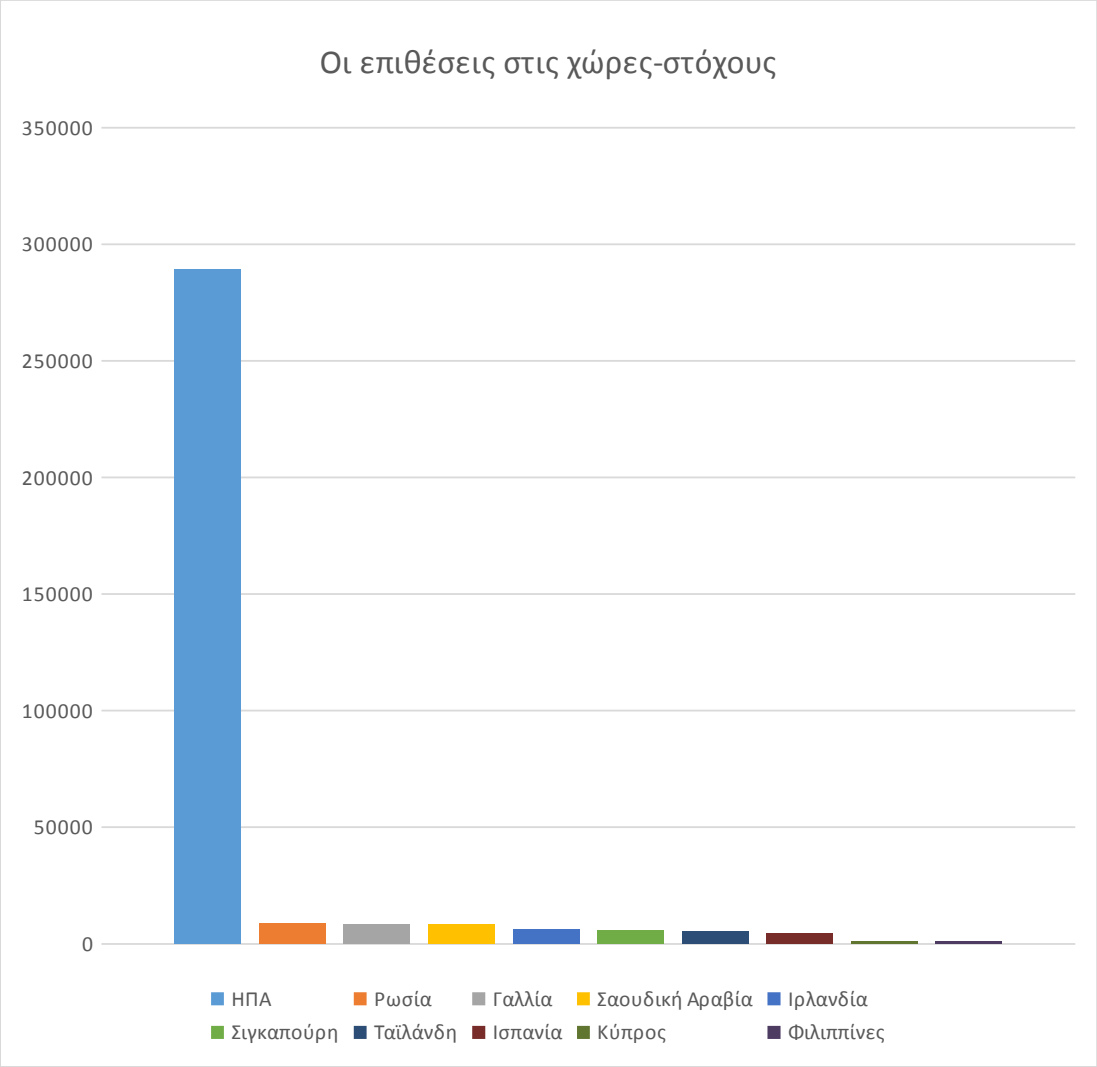
Σιγκαπούρη: 5.776 επιθέσεις

Ταϊλάνδη: 5.138 επιθέσεις

Ισπανία: 4.313 επιθέσεις

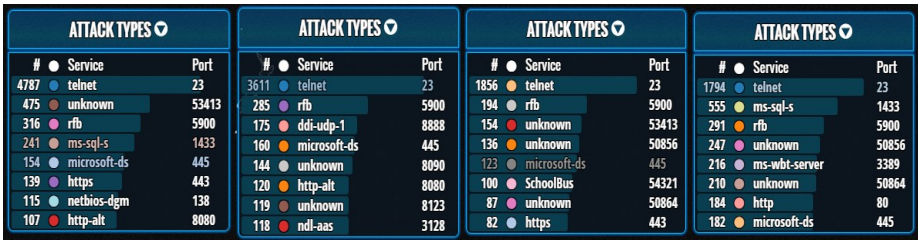
Κύπρος: 1.176 επιθέσεις

Φιλιππίνες: 924 επιθέσεις



4.4 Οι πιο συχνοί τύποι των κυβερνοεπιθέσεων

Η ενότητα αυτή θα επικεντρωθεί στους τύπους των επιθέσεων που χρησιμοποιούνται περισσότερο στο darknet. Θα σημειωθούν και θα αναλυθούν οι δέκα πρώτοι τύποι επιθέσεων και στη συνέχεια, γίνει μια επισκόπηση και σε άλλους τύπους που χρησιμοποιούνται τακτικά.



Όπως φαίνεται και πιο πάνω, η υπηρεσία την οποία χρησιμοποιούν περισσότερο οι χώρες για να κάνουν τις επιθέσεις τους είναι το telnet, μέσω της θύρας 23. Το telnet (telecommunication network), που αναπτύχθηκε το 1969 ως πρωτόκολλο επικοινωνίας σε τοπικά δίκτυα, το 1975 επεκτάθηκε στο διαδίκτυο. Ο χρήστης χρησιμοποιεί την υπηρεσία αυτή για να συνδεθεί σε απομακρυσμένους servers.

Οι επιθέσεις telnet προέρχονται κυρίως από δίκτυα κινητής τηλεφωνίας. Ωστόσο, οι κινητές αυτές συσκευές δεν φαίνεται να αποτελούν την πηγή, σύμφωνα με την Akamai Technologies. Πιστεύεται ότι η επίθεση παράγεται από μολυσμένους ηλεκτρονικούς υπολογιστές, οι οποίοι είναι συνδεδεμένοι σε ασύρματα δίκτυα μέσω των τεχνολογιών της κινητής τηλεφωνίας και όχι από μολυσμένες κινητές συσκευές.

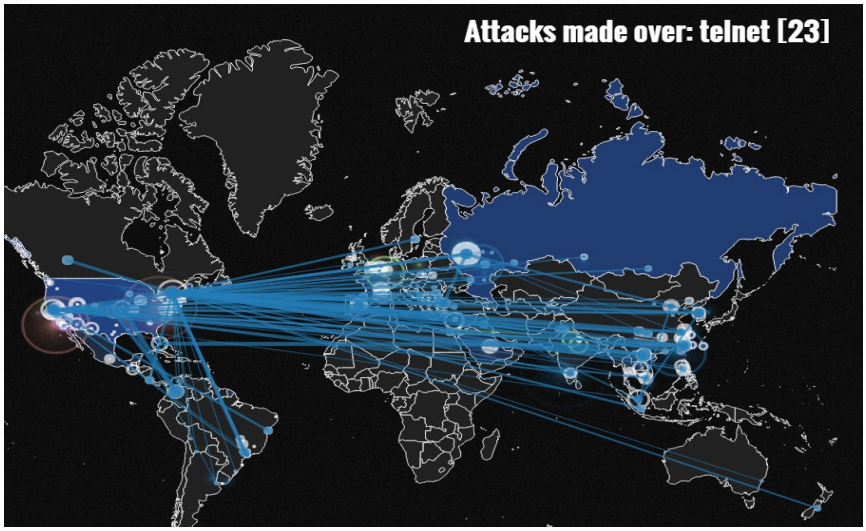
Οι επιθέσεις telnet μπορούν να διακριθούν σε τρεις υποκατηγορίες:

1. Telnet communication sniffing: το telnet είναι μια υπηρεσία η οποία υστερεί σε ασφάλεια σε σχέση με άλλες υπηρεσίες όπως η ssh. Αυτό ισχύει λόγω της έλλειψης κρυπτογράφησης και της χρήσης απλού κειμένου κατά τη σύνδεση απομακρυσμένων συσκευών. Έτσι, μπορεί οποιοσδήποτε να δει τις διαμορφώσεις και τις ρυθμίσεις που κάνει ο χρήστης σε μία συσκευή , καθώς και τον κωδικό πρόσβασης που χρησιμοποίησε.
2. Telnet brute force attack: πρόκειται για μια απλή αλλά αποτελεσματική μέθοδο, κατά την οποία ο hacker δοκιμάζει διάφορους συνδυασμούς χαρακτήρων για να βρει τον κωδικό του χρήστη. Σε πρώτη φάση, θα χρησιμοποιήσει τους πιο κοινούς κωδικούς και ένα πρόγραμμα που χρησιμοποιεί κάθε λέξη από το λεξικό. Το πρόγραμμα αυτό προσπαθεί να μαντέψει τον κωδικό, χρησιμοποιώντας όλες τις λέξεις του λεξικού και δημιουργώντας συνδυασμούς χαρακτήρων. Αν υπάρχει αρκετός χρόνος, η μέθοδος αυτή μπορεί να σπάσει σχεδόν όλους τους κωδικούς.
3. Denial of Service attack: οι επιθέσεις DoS έχουν σκοπό να διακόψουν ή να αρνηθούν την πρόσβαση στον νόμιμο χρήστη στο δίκτυο, servers και υπηρεσίες. Αυτό το πετυχαίνει στέλνοντας μεγάλο πλήθος άχρηστων και άσχετων δεδομένων, με αποτέλεσμα να χρησιμοποιείται όλο το εύρος ζώνης της σύνδεσης. Έτσι, τα δεδομένα που θέλει ο χρήστης να μεταδώσει δεν

μπορούν να μεταδοθούν και η επικοινωνία δεν λειτουργεί. Αυτό που κάνει λοιπόν μια επίθεση DoS είναι να διακόπτει την επικοινωνία ανάμεσα σε δύο συσκευές δικτύου.

Στην έρευνά μας, για τις 30 ώρες του Ιουνίου, οι επιθέσεις μέσω telnet ανέρχονται στις 166.811, με τις περισσότερες να γίνονται βραδινές ώρες (67.974). Παρατηρήθηκε ότι οι επιθέσεις telnet που προέρχονται από την Ασία αγγίζουν το 50,5%.

Ακολουθεί εικόνα στην οποία φαίνονται ενδεικτικά οι κυβερνοεπιθέσεις που έγιναν μέσω telnet και συμβολίζονται με τις μπλε διαγραμμίσεις.



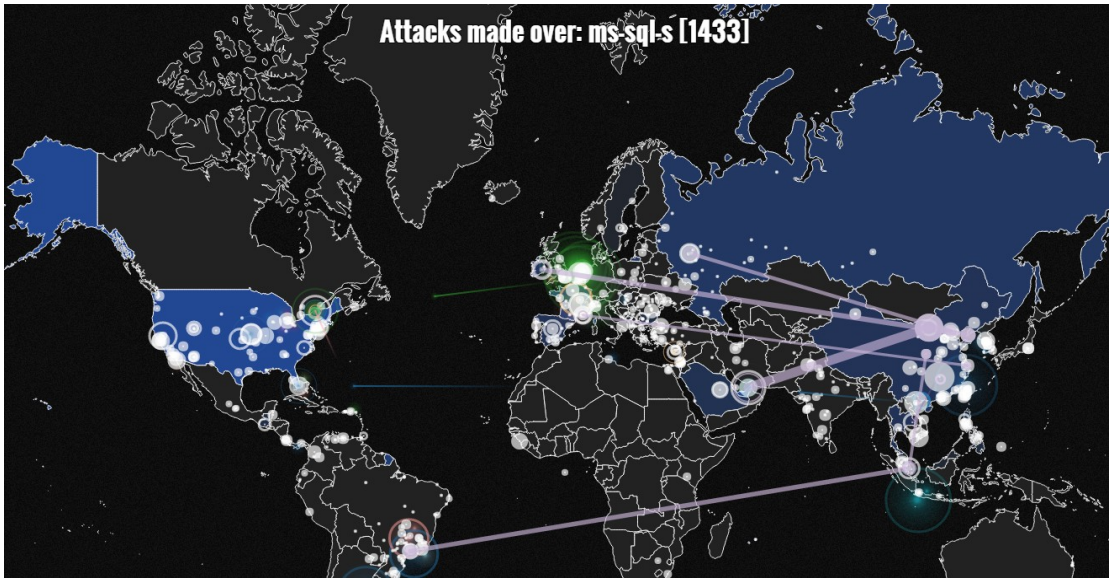
Η επόμενη υπηρεσία μέσω της οποίας οι hackers επιτίθονται είναι η ms-sql-s, στη θύρα 1433. Η ms-sql-server είναι ένα σχεσιακό σύστημα διαχείρισης βάσεων δεδομένων, για την αποθήκευση και την ανάκτηση πληροφοριών, είτε στον ίδιο υπολογιστή είτε σε άλλον, μέσω κάποιου δικτύου.

Ο hacker για να κάνει την επίθεση που θέλει στο darknet παρεμβαίνει στο πρωτόκολλο του server. Αυτό γίνεται με την εκτέλεση σεναρίων αιτημάτων και την πλαστογράφηση της πηγής του ερωτήματος με την ip του στόχου. Επίσης, υπάρχουν διαθέσιμα εργαλεία στο internet που μπορούν να αναπαράγουν αυτήν την επίθεση και δεν απαιτούν ιδιαίτερες δεξιότητες.

Τις πρωινές ώρες σημειώθηκαν οι λιγότερες επιθέσεις κατά τη διάρκεια τις ημέρας, 3.175, ενώ τις απογευματινές ώρες έφτασαν το μέγιστο, 3.421 επιθέσεις, με σύνολο 13.206 επιθέσεων μέσω του ms-sql-s, για ον Ιούνιο.

Παρατηρείται ότι το 59,5% των επιθέσεων μέσω της Microsoft-sql-server προέρχεται από την Κίνα. Αντίστοιχα, το 46,85% των επιθέσεων έχουν ως στόχο τις Ηνωμένες Πολιτείες, ενώ πλήθος επιθέσεων δέχεται και η Σιγκαπούρη και η Ρωσία.

Παρακάτω υπάρχουν με μωβ χρώμα οι διαγραμμίσεις στον χάρτη που δηλώνουν επιθέσεις που γίνονται μέσω του sql server που προαναφέρθηκε.

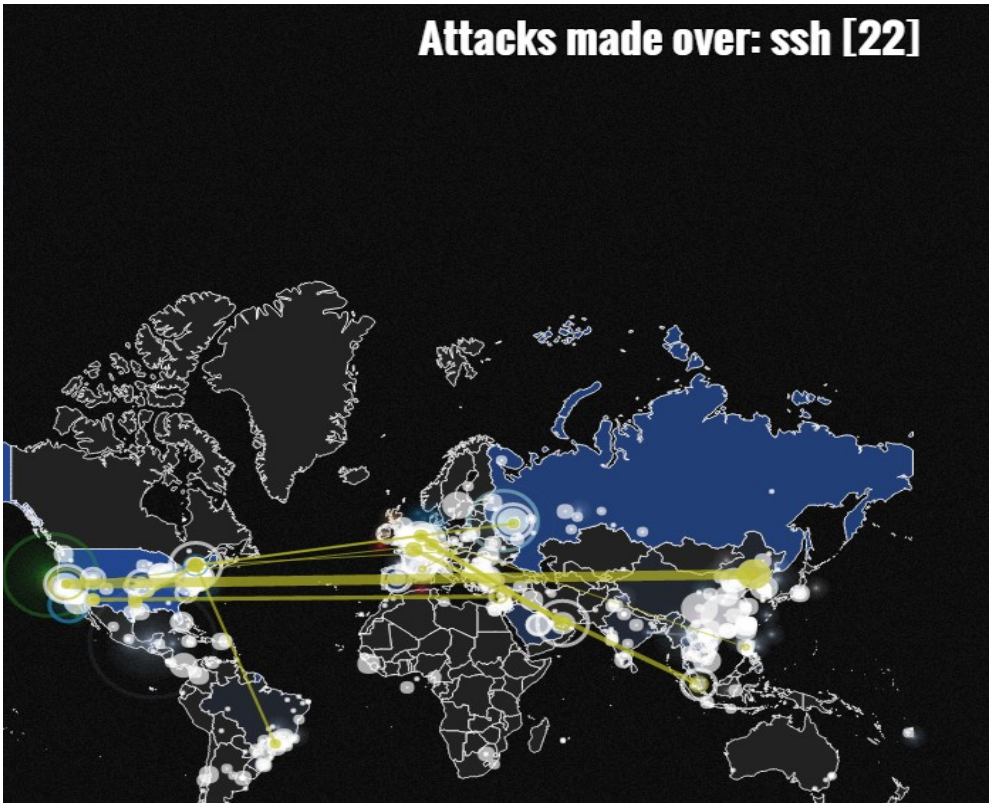


Πολλοί χρησιμοποιούν την θύρα 22 και την secure shell (ssh) για να κάνουν τις κυβερνοεπιθέσεις. Η secure shell είναι ένα κρυπτογραφικό πρωτόκολλο δικτύου που σχεδιάστηκε αρχικά για να αντικαταστήσει το telnet και για πρωτόκολλα που αποστέλλουν πληροφορίες, ειδικά κωδικούς πρόσβασης, σε απλό κείμενο, με αποτέλεσμα να γίνεται η κλοπή τους ευκολότερη. Η υπηρεσία αυτή παρέχει στους χρήστες της ισχυρό έλεγχο ταυτότητας και κρυπτογραφημένη επικοινωνία δεδομένων, δηλαδή είναι υπεύθυνη για να έχουν οι χρήστες ένα ασφαλές κανάλι μέσω ενός μη ασφαλούς δικτύου.

Ωστόσο, αυτό που αποτελεί τη σημαντικότερη απειλή για την secure shell είναι η κακή διαχείριση κλειδιών. Με την απουσία της κατάλληλης κεντρικής δημιουργίας, της περιστροφής και αφαίρεσης των κλειδιών της ssh, οι οργανισμοί είναι εύκολο να μην μπορούν να ελέγξουν ποιος έχει πρόσβαση σε ποιους πόρους και πότε. Ο κίνδυνος αυτός είναι αυξημένος όταν η υπηρεσία χρησιμοποιείται σε αυτοματοποιημένες διαδικασίες.

Στην έρευνα που έγινε σημειώθηκαν συνολικά 6.944 επιθέσεις στο darknet μέσω της θύρας 22 και της secure shell. Οι περισσότερες από αυτές έγιναν πρωινές ώρες, 1.835, και στη συνέχεια μειώνονταν σταδιακά στις 1.746, 1.701 μέχρι τις 1.662 που έφτασαν τις βραδινές ώρες του μήνα.

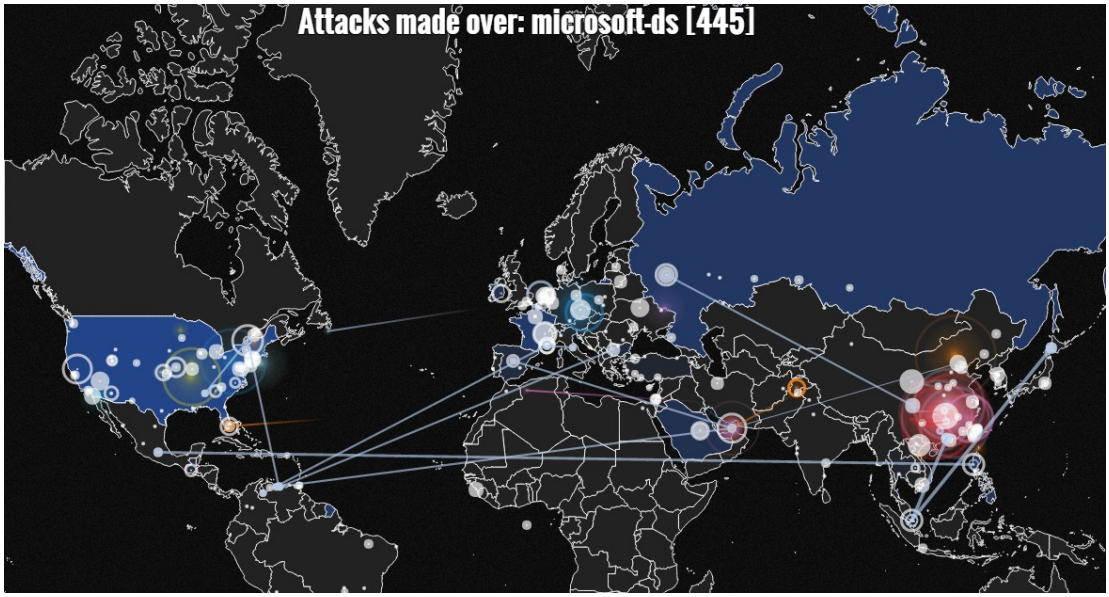
Στην εικόνα που ακολουθεί φαίνονται ενδεικτικά με κίτρινο χρώμα επιθέσεις που έγιναν μέσω της secure shell.



Στη συνέχεια θα δούμε μια άλλη υπηρεσία που χρησιμοποιούν όσοι θέλουν να κάνουν επιθέσεις και να συμμετάσχουν έτσι στον κυβερνοπόλεμο, την microsoft-ds στη θύρα 445. Πρόκειται για μια θύρα για την κοινή χρήση αρχείων, μέσω της οποίας είναι δυνατή η μεταφορά κακόβουλου περιεχομένου σε απομακρυσμένο υπολογιστή. Οι hackers μπορούν να έχουν απομακρυσμένη πρόσβαση στα περιεχόμενα του σκληρού δίσκου του ανυποψίαστου χρήστη, σε όλο το διαδίκτυο. Αυτό γίνεται και με την χρήση κάποιων άμεσα διαθέσιμων δωρεάν εργαλείων. Έτσι, οι hackers μπορούν να φορτώνουν και να τρέχουν τα προγράμματα που θέλουν σε απομακρυσμένο υπολογιστή, χωρίς να το γνωρίζει ο χρήστης.

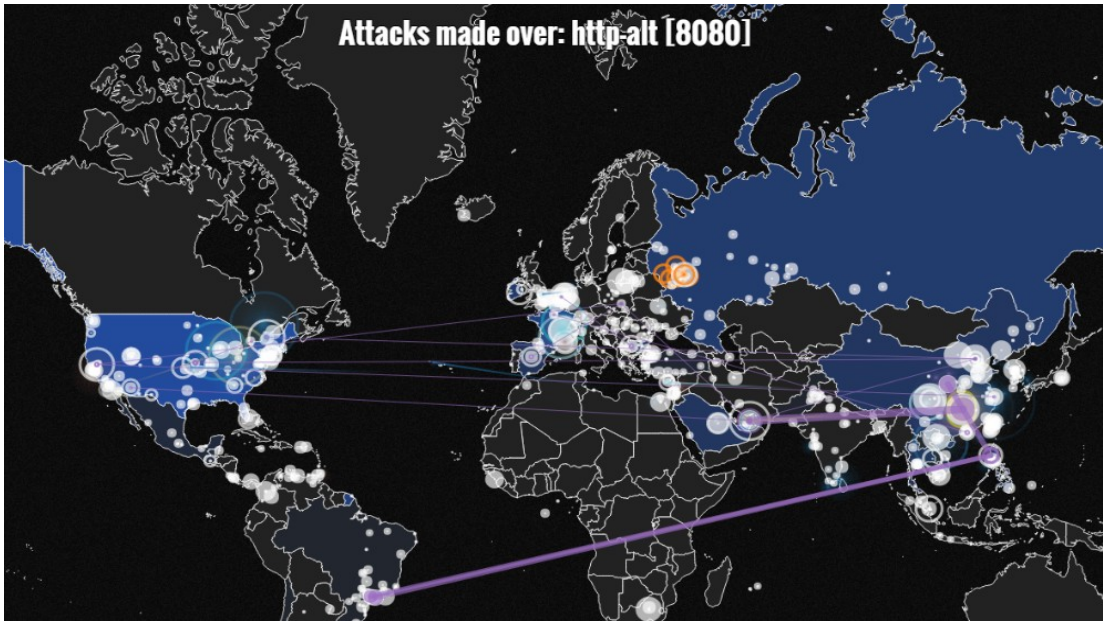
Βρέθηκε στην έρευνα ότι αυτοί που χρησιμοποίησαν την εν λόγω θύρα είχαν μια πιο ευρεία κατανομή στις χώρες που πραγματοποίησαν τις επιθέσεις. Οι κύριες χώρες που προτίμησαν την microsoft-ds και τη θύρα 445 ήταν οι Ηνωμένες Πολιτείες, η Κίνα, η Ρωσία, η Ταϊβάν και η Ιταλία. Όσον αφορά τις χώρες που δέχτηκαν τις επιθέσεις αυτές, η μεγαλύτερη χώρα-στόχος ήταν οι Ηνωμένες Πολιτείες που συγκέντρωσε το 61.16% των επιθέσεων. Τις ΗΠΑ ακολούθησαν τα Ηνωμένα Αραβικά Εμιράτα με το 10.08% των επιθέσεων και τρίτη βρίσκεται η Ρωσία με ένα 9.12%. Οι τρεις αυτές χώρες συγκέντρωσαν το 80.36% των συνολικών επιθέσεων που έγιναν μέσω microsoft-ds. Αξιοσημείωτο είναι ότι το 14.01% των επιθέσεων που δέχτηκαν οι Ηνωμένες Πολιτείες προέρχεται μέσα από την ίδια τη χώρα.

Παρακάτω φαίνεται ένα δείγμα των επιθέσεων που έγιναν μέσω της θύρας 445 και της microsoft-ds.



Η επόμενη θύρα που θα αναφερθεί είναι η θύρα 8080, http-alt. Αποτελεί τη δημοφιλέστερη εναλλακτική λύση στη θύρα 80, η οποία προσφέρει υπηρεσίες web. Ο web server που χρησιμοποιούμε λειτουργεί στη θύρα 80. Η θύρα αυτή φιλοξενεί web servers μόνο από εξουσιοδοτημένους διαχειριστές. Ωστόσο, υπάρχουν και μη εξουσιοδοτημένοι διαχειριστές που θέλουν να ιδρύσουν και να λειτουργήσουν web servers για τις μηχανές που τρέχουν ήδη σε άλλο server στη θύρα 80. Επίσης μπορεί να μην έχουν το δικαίωμα να τρέξουν υπηρεσίες σε θύρα μικρότερη από τη 1024. Σε αυτήν την περίπτωση η θύρα 8080 προσφέρεται να φιλοξενήσει ένα δευτερεύον ή εναλλακτικό web server.

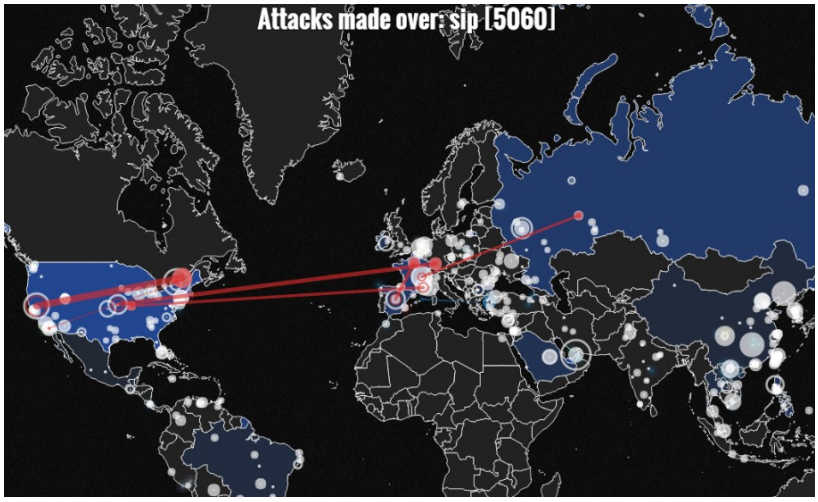
Τις προκαθορισμένες για την έρευνα ώρες του Ιουνίου, παρατηρήθηκε αυξημένη χρήση της θύρας 8080 τις απογευματινές ώρες, η οποία καλύπτει το 32.36% των συνολικών επιθέσεων, 5.863. Αντίθετα, τις πρωινές ώρες οι επιθέσεις αυτές φτάνουν στο ελάχιστο, 10.1% των συνολικών επιθέσεων. Κυριότερη χώρα-στόχος είναι οι Ηνωμένες Πολιτείες της Αμερικής που δέχτηκε το 54.61% των κυβερνοεπιθέσεων μέσω της http-alt. Αντίστοιχα οι χώρες που πραγματοποίησαν τις περισσότερες επιθέσεις ήταν οι Ηνωμένες Πολιτείες με το 37.22% των επιθέσεων και η Κίνα με το 39.6%.



Η θύρα 5060 χρησιμοποιείται συχνά για επιθέσεις μέσω SIP (Session Initiation Protocol). Είναι ένα πρωτόκολλο σηματοδοσίας για τον έλεγχο των συνεδριών επικοινωνίας πολυμέσων. Βασίζεται στο κείμενο και περιέχει πολλά κοινά στοιχεία με το http (Hypertext Transfer Protocol), όπως ότι τα μηνύματα αποτελούνται από headers και body. Ο ρόλος του SIP είναι να καθορίζει τα μηνύματα που αποστέλλονται μεταξύ δύο τερματικών σημείων, που χαρακτηρίζονται από τα ουσιώδη στοιχεία μιας κλήσης. Χρησιμοποιείται όχι μόνο στην τηλεφωνία μέσω διαδικτύου, απλές κλήσεις και video-κλήσεις, αλλά και στην ανταλλαγή μηνυμάτων μέσω ip δικτύου.

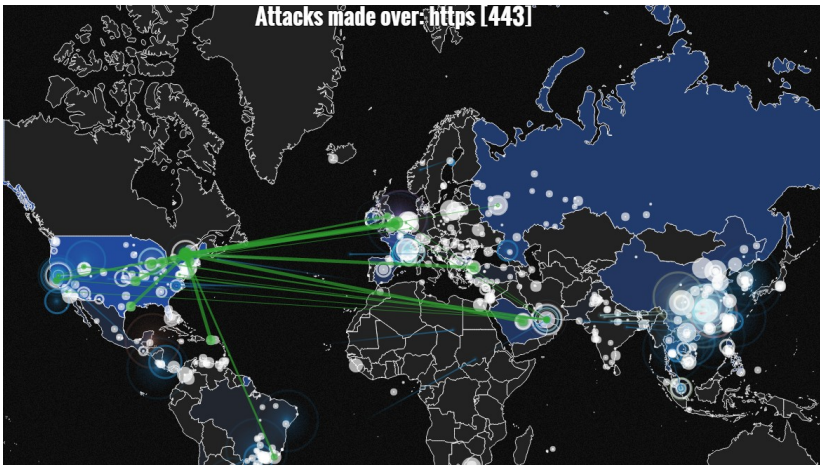
Πολλοί χρησιμοποιούν το friendly-scanner, ένα είδος botnet, το οποίο εντοπίζει SIP servers που χρησιμοποιούν τη θύρα 5060. Αν η θύρα είναι ανοιχτή, το friendly-scanner εισβάλλει στον SIP server δοκιμάζοντας διαδοχικούς αριθμούς λογαριασμών με κοινά ονόματα χρήστη και κωδικούς πρόσβασης. Αν ο hacker πετύχει την εισβολή αυτή, μπορεί να υπερφορτώσει το δίκτυο του χρήστη με αποτέλεσμα η επίθεση αυτή να γίνει αρκετά δαπανηρή για τον τελευταίο. Η επίθεση μέσω SIP προκαλεί προβλήματα στη σύνδεση του τηλεφώνου και πολύ αργή σύνδεση δικτύου, στοιχεία τα οποία υποψιάζουν τον χρήστη ότι είναι θύμα κάποιας επίθεσης. Οι επιθέσεις αυτές γίνονται κυρίως ώρες που είναι λιγότερο πιθανό να χρησιμοποιείται το δίκτυο, για παράδειγμα οι νυχτερινές ώρες ή ημέρες διακοπών.

Αυτές είναι και οι ώρες που στην έρευνά μας χρησιμοποιήθηκε περισσότερο αυτός ο τύπος επιθέσεων. Τις πρωινές ώρες οι επιθέσεις ήταν μόλις 1.168. Στη συνέχεια έφτασαν τις 1.172 και αργότερα άρχισαν να αυξάνονται στις 1.184, για να φτάσουν το μέγιστο τη νύχτα τις 1.427, κάνοντας έτσι ένα σύνολο 4.951 κυβερνοεπιθέσεων.



Η θύρα 443, https, είναι ένα πρωτόκολλο για την ασφαλή επικοινωνία σε ένα δίκτυο υπολογιστών με ευρεία χρήση στο internet. Αρχικά, οι συνδέσεις https χρησιμοποιήθηκαν για πληρωμές μέσω του World Wide Web, για το e-mail και για λοιπές ευαίσθητες συναλλαγές. Παρ' όλα αυτά, στις αρχές της δεκαετίας του 2010, η https άρχισε να έχει μια πιο ευρεία χρήση για να προστατεύει την αυθεντικότητα της σελίδας για κάθε είδους website. Η https σήμερα προσφέρει ισχυρή ασφάλεια επικοινωνίας. Δηλαδή, συμβάλλει στην εξασφάλιση των λογαριασμών και διατηρεί ασφαλείς τις επικοινωνίες, την ταυτότητα και την περιήγηση του χρήστη στο διαδίκτυο. Αυτό επιτυγχάνεται με την πιστοποίηση της ιστοσελίδας και των web servers. Τα δεδομένα που μεταφέρονται μέσω https είναι πολύ ανθεκτικά στις υποκλοπές και στις παραποιήσεις, εξαιτίας της κρυπτογράφησης της επικοινωνίας που παρέχει η https. Επιπλέον, παρέχεται προστασία από επιθέσεις που έχουν ως στόχο τους χρήστες.

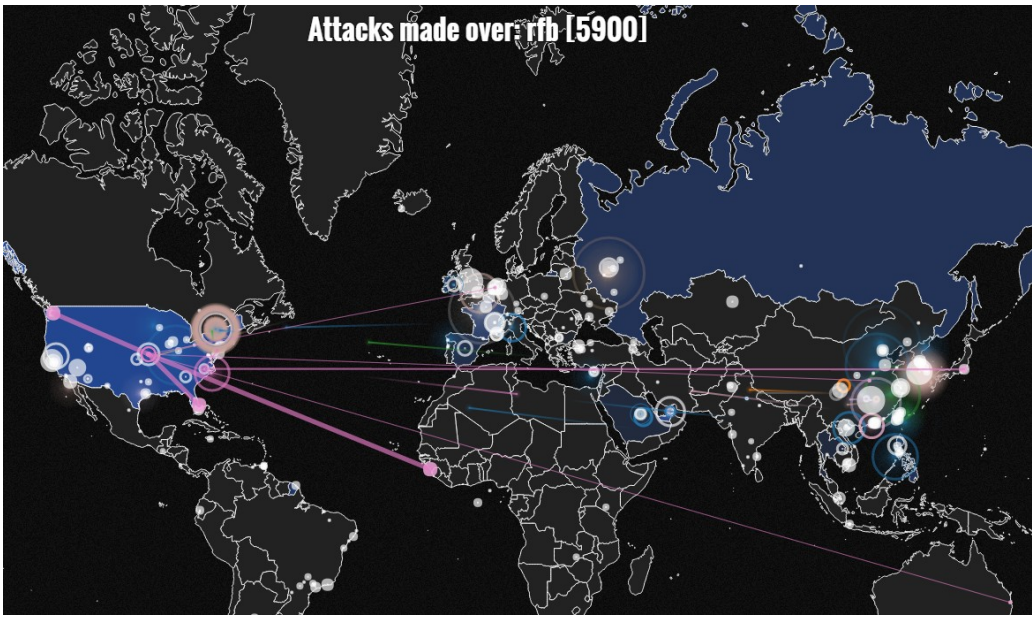
Συνολικά οι επιθέσεις μέσω της θύρας 443 άγγιξαν τις 4.916. Οι περισσότερες έγιναν πρωινές ώρες και ήταν 1.324. Στη συνέχεια μειώθηκαν στις 1.206 και αργότερα στις 1.189 που ήταν και οι λιγότερες στην διάρκεια της ημέρας. Τις βραδινές ώρες παρουσιάστηκε μια μικρή αύξηση και οι επιθέσεις μέσω της θύρας 443 στο dark net έφτασαν τις 1.197.



Ακολουθεί η θύρα 5900. Το πρωτόκολλο rfb (remote framebuffer) είναι ένα πρωτόκολλο δικτύου για την πρόσβαση των γραφικών διεπαφών του χρήστη από

έναν άλλον υπολογιστή. Αφορά τη μεταφορά του περιεχομένου της οθόνης και τη μετάδοση των δεδομένων που εισάγει ο χρήστης. Η επιφάνεια εργασίας τρέχει σε έναν απομακρυσμένο υπολογιστή.

Το πρωτόκολλο αυτό είναι ένας από τους τύπους των επιθέσεων που χρησιμοποιούνται στο dark net. Οι επιθέσεις το πρωί είναι οι ελάχιστες μέσα στη μέρα και φτάνουν μόλις τις 1.102. Τις ώρες του μεσημεριού αυξάνονται στις 1.181, ενώ τα απογεύματα πέφτουν στις 1.138 επιθέσεις μέσω της θύρας 5900. Οι νυχτερινές ώρες βρίσκουν τις επιθέσεις αυτές στον μέγιστο αριθμό των 1.203. Οι συνολικές επιθέσεις μέσω της θύρας 5900 ήταν 4.624.

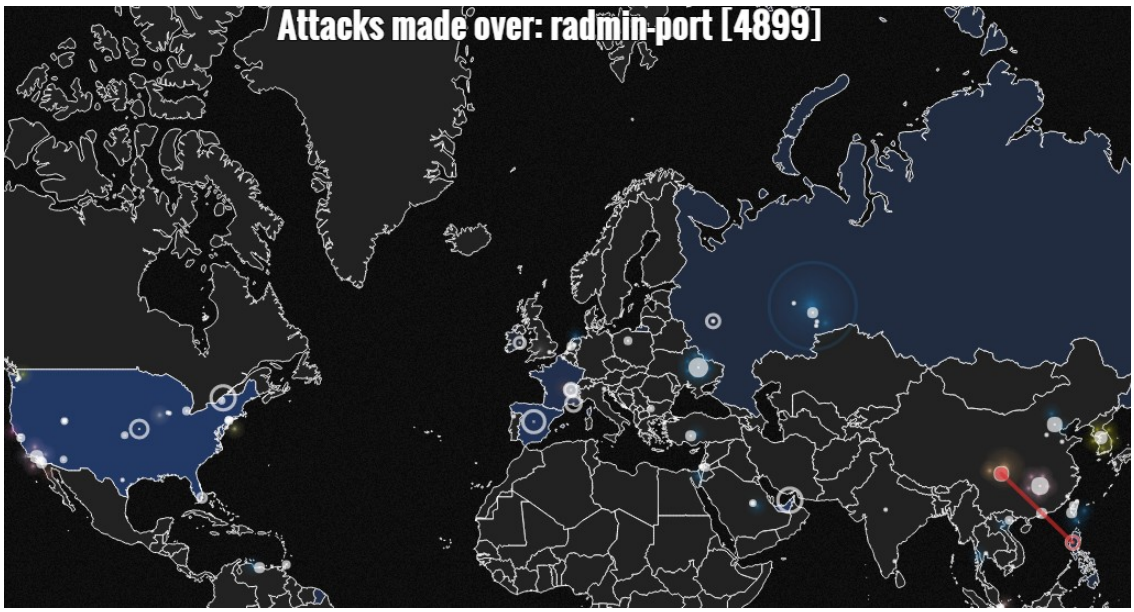


Συνεχίζουμε με τη θύρα 4899 και την radmin-port, η οποία είναι ένα εργαλείο απομακρυσμένης διαχείρισης. Με το εργαλείο αυτό μπορεί κανείς να αποκτήσει πρόσβαση και έλεγχο στο σύστημα ενός απομακρυσμένου υπολογιστή. Μπορεί δηλαδή εύκολα να αποκτήσει πρόσβαση σε έναν υπολογιστή που βρίσκεται σε τοποθεσία διαφορετική από τον ίδιο. Αυτό μπορεί να επιτευχθεί είτε μέσω του διαδικτύου είτε με απευθείας κλήση μέσω σταθερού δικτύου. Αν όμως δεν ρυθμιστεί σωστά ή εγκατασταθεί από τον hacker, τότε αυτός έχει την πρόσβαση και τον έλεγχο του συστήματος του απομακρυσμένου υπολογιστή.

Όποιος θέλει να κάνει μια κυβερνοεπίθεση μέσω της θύρας 4899, δεν μπορεί να το κάνει εάν είτε ο δικός του είτε ο απομακρυσμένος υπολογιστής δεν έχει εγκατεστημένο το radmin. Μέσω της θύρας 4899, λοιπόν, θα βρει την ip διεύθυνση του υπολογιστή που επιθυμεί και στη συνέχεια, χρησιμοποιώντας το Remote Administration και μέσω της ip, θα πραγματοποιήσει μια νέα σύνδεση με αυτόν. Ωστόσο, υπάρχει τρόπος για να μειωθεί ο κίνδυνος ενδεχόμενης επίθεσης και αυτός είναι η φραγή της εισερχόμενης πρόσβασης στη θύρα 4899.

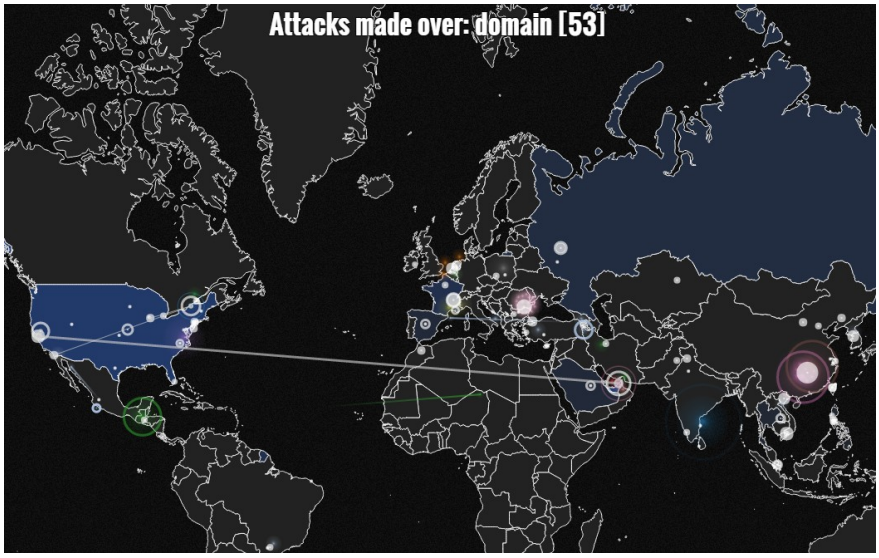
Αυτοί που προτίμησαν τη θύρα 4899 για τις κυβερνοεπιθέσεις τους αυξάνονταν σταδιακά κατά τη διάρκεια της μέρας, για να αγγίξουν το σύνολο των 4.558

επιθέσεων, ξεκινώντας από τις 1.043 επιθέσεις. Στη συνέχεια φτάνουν τις 1.147, τις 1.172 και τις βραδινές ώρες αγγίζουν το μέγιστο, τις 1.196 επιθέσεις.



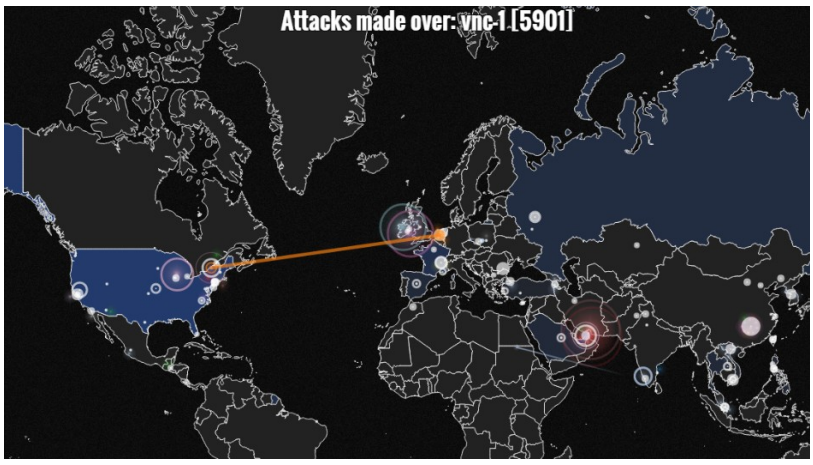
Η θύρα 53 χρησιμοποιείται από όσους θέλουν να επιλέξουν τον τύπο επίθεσης domain (Domain Name System). Πρόκειται για το ιεραρχικό σύστημα ονοματοδοσίας για δίκτυα υπολογιστών που χρησιμοποιούν το πρωτόκολλο ip. Στην πραγματικότητα, μεταφράζει τα ονόματα που είναι κατανοητά από τους ανθρώπους σε Internet Protocol διευθύνσεις που είναι αναγνώσιμες από τον υπολογιστή. Η κύρια απειλή για την χρήση του διαδικτύου έγκειται σε μία μαζική επίθεση DoS. Αυτό θα κράταγε εκτός δικτύου τους DNS servers για αρκετό χρονικό διάστημα, ώστε να λήξουν τα προσωρινά αποθηκευμένα αντίγραφα των DNS εγγράφων. Λίγα Trojan προγράμματα είναι γνωστά ότι ανοίγουν τη θύρα 53. Παρ' όλα αυτά πρέπει να γίνεται τακτικά έλεγχος, ειδικά αν η θύρα είναι ανοιχτή και εντοπίζεται εισερχόμενη κίνηση.

Τα περισσότερα θύματα επίθεσης τύπου domain εντοπίστηκαν τις πρωινές ώρες, που οι επιθέσεις άγγιξαν τις 1.176. Στη συνέχεια μειώθηκαν στις 1.132 για να φτάσουν αργότερα το ελάχιστο που ήταν μόλις 1.098. Το βράδυ παρατηρήθηκε μια αύξηση, καθώς καταγράφτηκαν 1.124 επιθέσεις DNS. Συνολικά οι επιθέσεις μέσω της θύρας 53 ανήλθαν στις 4.530.



Επιπλέον, υπάρχει και η θύρα 5901, την οποία χρησιμοποιούν με το vnc-1. Το Virtual Network Computing είναι ένας ακόμα τρόπος πρόσβασης του υπολογιστή ενός ατόμου σε ένα άλλο, με την χρήση απλού λογισμικού. Είναι δυνατό να εισβάλλει κανείς σε έναν απομακρυσμένο υπολογιστή με αδύναμους κωδικούς πρόσβασης και να αποκτήσει τον έλεγχο χρησιμοποιώντας το πληκτρολόγιο και το ποντίκι του. Τα κυριότερα πλεονεκτήματα του vnc είναι ότι προσφέρεται δωρεάν και είναι συμβατό σε πολλαπλές πλατφόρμες. Ωστόσο, συγκριτικά με άλλες παρόμοιες τεχνολογίες, το vnc είναι πιο αργό και επιπλέον, δεν επιτρέπει τη μεταφορά αρχείων.

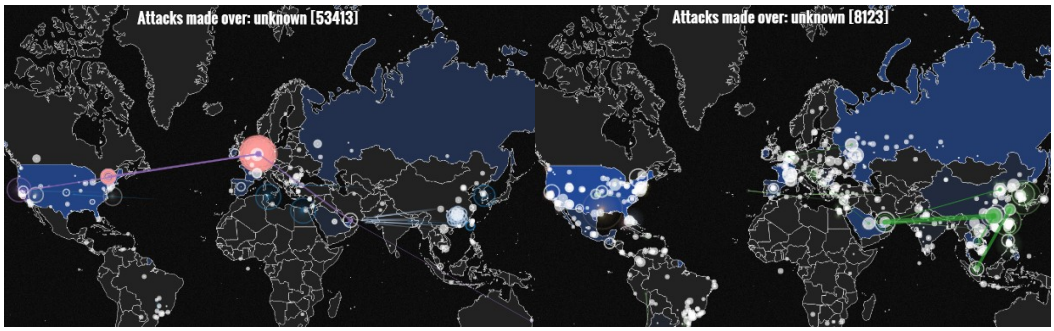
Το vnc επέλεξαν να χρησιμοποιήσουν για τις επιθέσεις τους μόλις 4.513 φορές, για τις καθορισμένες ώρες του Ιουνίου. Κατά τη διάρκεια της ημέρας, οι επιθέσεις μέσω της θύρας 5901 μειώνοντας σταδιακά. Ξεκινώντας τις πρωινές ώρες με 1.152 κυβερνοεπιθέσεις, μειώθηκαν αργότερα στις 1.137. Τις απογευματινές ώρες οι επιθέσεις μέσω vnc έφτασαν τις 1.119 και τις βραδινές έφτασαν στο ελάχιστό τους, τις 1.105 επιθέσεις.



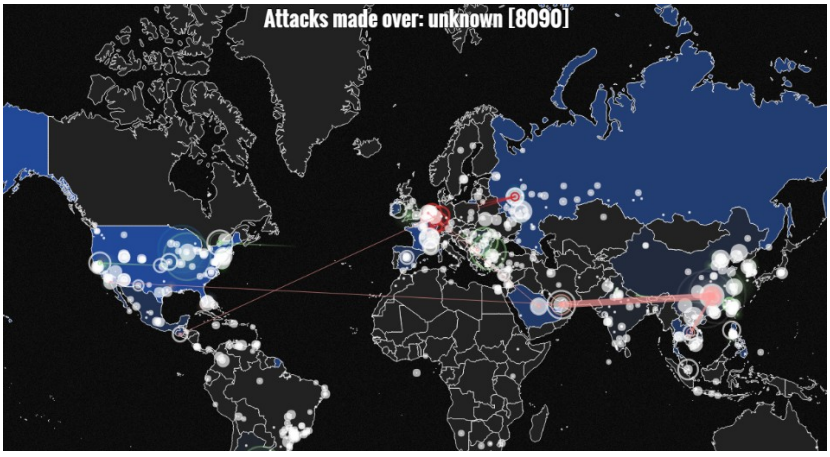
Παρ’ όλα αυτά, υπάρχουν επιθέσεις που γίνονται στο dark net μέσω άγνωστης υπηρεσίας, με γνωστή όμως τη θύρα που χρησιμοποιείται. Υπάρχουν 64.512 θύρες που χρησιμοποιούνται για διάφορες υπηρεσίες. Ωστόσο, για την πλειοψηφία των

θυρών αυτών δεν έχει οριστεί συγκεκριμένος σκοπός για την χρήση τους. Χρησιμοποιούνται κυρίως για τη σύνδεση διαδικτυακών υπηρεσιών, όπως τα προγράμματα περιήγησης, με απομακρυσμένους servers.

Στην έρευνα αυτή χρησιμοποιήθηκαν περισσότερο οι θύρες 53.413 και 8.123. Από την πρώτη πέρασαν 12.348 επιθέσεις, ενώ η δεύτερη θύρα χρησιμοποιήθηκε για 10.194 επιθέσεις.



Τέλος, υπάρχουν θύρες που χρησιμοποιούνται από μια υπηρεσία, χωρίς όμως αυτή να είναι η μοναδική που εξυπηρετείται από μία θύρα. Δηλαδή, μια θύρα μπορεί να εξυπηρετεί ποικίλους σκοπούς. Έτσι, υπάρχει η θύρα 8.090 που χρησιμοποιείται από την http-alt-alt. Στην έρευνα, όμως, χρησιμοποιήθηκε περισσότερο από άγνωστη υπηρεσία, για 9.677 κυβερνοεπιθέσεις.



ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

Το Deep Web (γνωστό ακόμα και ως Dark Net, Under Net, Hidden Web, αόρατο ή κρυμμένο Web) είναι το περιεχόμενο που βρίσκεται αποθηκευμένο στο Διαδίκτυο (Wolrd Wide Web) και συνήθως δεν εμφανίζεται μέσω των συνηθισμένων μηχανών αναζήτησης όπως του Google, του Yahoo, του Bing, του Ask κλπ. από τους γνωστούς browsers όπως είναι ο Firefox, ο Internet Explorer ή ο Chrome.

Ψάχνοντας λοιπόν για μια πληροφορία σε κάποια μηχανή αναζήτησης ουσιαστικά αναζητάτε πληροφορίες που βρίσκονται στην επιφάνεια του διαδικτύου και αντιστοιχούν μόλις στο 6-8% του πραγματικού όγκου του διαδικτύου. Το υπόλοιπο 92-94% βρίσκεται αποθηκευμένο πιο βαθιά στο διαδίκτυο όπου οι γνωστές μηχανές αναζήτησης δεν έχουν πρόσβαση.

Ουσιαστικά κανείς δε μπορεί να μιλήσει με ακριβή νούμερα για τον όγκο πληροφοριών του Deep Web και όλες οι αναφορές γίνονται βάση κάποιων εκτιμήσεων που έγιναν από μία μελέτη του Πανεπιστημίου της Καλιφόρνιας στο Berkeley (University of California, Berkeley) το έτος 2001. Βάση της μελέτης το Deep Web αποτελείται περίπου από 91.000 terabytes σε αντίθεση με το Surface Web (Επιφανειακό Διαδίκτυο) που υπολογίζεται περίπου σε 167 terabytes.

Αξίζει να σημειωθεί πως εξήντα από τους μεγαλύτερους ιστότοπους του Deep Web περιέχουν 750 terabytes υπερβαίνοντας κατά πολύ τον όγκο των δεδομένων ολόκληρου του Επιφανειακού Διαδικτύου.

Μπορεί να είναι δύσκολο να κατανοήσουμε πώς πολλά εκατομμύρια ιστοσελίδες με τεράστιο όγκο δεδομένων παραμένουν «κρυμμένες» από τις μηχανές αναζήτησης και όμως υπάρχουν. Αρκεί να σκεφτούμε πως πολλές από αυτές είναι βάσεις δεδομένων που εξυπηρετούν κυβερνητικούς σκοπούς όπως φορολογικά στοιχεία πολιτών ή στρατιωτικούς σκοπούς με απόρρητα στοιχεία και αρχεία όπως χάρτες, σχέδια αεροσκαφών ή πυραυλικών συστημάτων.

Οι πληροφορίες που βρίσκονται στο Deep Web είναι αναρίθμητες και αφορούν τους πάντες. Όλα τα παρακάτω προσωπικά στοιχεία βρίσκονται αποθηκευμένα σε βάσεις

δεδομένων του Deep Web και σίγουρα δεν θα θέλατε να τα δούμε δημόσια αποθηκευμένα σε ιστοσελίδες στις οποίες ο καθένας ανεξέλεγκτα θα μπορούσε να έχει πρόσβαση:

- Πιστοποιητικά γεννήσεως και πιστοποιητικά οικογενειακής κατάστασης.

- Στοιχεία αστυνομικής ταυτότητας, διαβατηρίου, διπλώματος οδήγησης, παραβάσεων τροχαίας.

- Στοιχεία αποφοίτησης από σχολεία και τίτλοι πανεπιστημιακών σπουδών.

- Τίτλοι ιδιοκτησίας σπιτιού, αυτοκίνητου, μοτοσυκλέτας καθώς και η ασφάλεια που πληρώνουμε γι' αυτά.

- Φορολογικά στοιχεία όπως ΑΦΜ, ΑΜΚΑ, φορολογικές δηλώσεις καθώς και το ιστορικό της ιατροφαρμακευτικής και νοσοκομειακής μας περίθαλψης.

- Λογαριασμοί μισθοδοσίας, βεβαιώσεις αποδοχών, οι καταβολές ασφαλιστικών εισφορών και η συντάξιμη προϋπηρεσία μας, λογαριασμοί για υπηρεσίες όπως φως, νερό, τηλέφωνο, ίντερνετ.

- Στοιχεία και κινήσεις τραπεζικών λογαριασμών και πάσης φύσεως δοσοληψιών.

- Στοιχεία των διαδικτυακών μας κινήσεων όπως ιστοσελίδες που επισκεπτόμαστε και διαδικτυακές αγορές.

Γενικά οι πόροι του Deep Web μπορούν να ταξινομηθούν σε μία ή περισσότερες από τις ακόλουθες κατηγορίες:

- Δυναμικού περιεχομένου: Είναι δυναμικές ιστοσελίδες που χρησιμοποιούν ένα συνδυασμό από βάσεις δεδομένων για την δημιουργία μίας προσωρινής σελίδας ως απάντηση σε κάποιο υποβληθέν ερώτημα ή στις οποίες έχει κάποιος πρόσβαση μόνο μέσα από φόρμες όπου πρέπει να συμπληρωθούν κάποια στοιχεία και είναι δύσκολο να περιηγηθούμε σε αυτές χωρίς τη γνώση της διεύθυνσης (Domain) που θέλουμε.

- Ιστοσελίδες μη συνδεδεμένου περιεχομένου: Είναι ιστοσελίδες που δεν συνδέονται με άλλες ιστοσελίδες εμποδίζοντας τις μηχανές αναζήτησης να έχουν πρόσβαση στο περιεχόμενό τους.

- Private Web: Ιστοσελίδες με ιδιωτικό περιεχόμενο στις οποίες για να έχουμε πρόσβαση χρειάζεται να κάνουμε login με username και password. Αυτές μπορεί για παράδειγμα να είναι εταιρικές ιστοσελίδες που έχουν πρόσβαση μόνο οι υπάλληλοι των συγκεκριμένων εταιρειών.

- Contextual Web: Είναι ιστοσελίδες το περιεχόμενο των οποίων προσαρμόζεται ανάλογα με τον τρόπο που έχει κανείς πρόσβαση σε αυτές. Έτσι σε μια τέτοια ιστοσελίδα θα δούμε διαφορετικό περιεχόμενο αν έχουμε πρόσβαση μέσω μιας διεύθυνσης IP από την Ελλάδα και διαφορετικό περιεχόμενο απ' ό,τι αν θα επισκεπτόμασταν την ίδια ιστοσελίδα μέσω μίας διεύθυνσης IP από την Αμερική.

- Περιεχόμενο περιορισμένης πρόσβασης: Είναι ιστοσελίδες που περιορίζουν την πρόσβαση στο περιεχόμενό τους με τεχνικούς τρόπους (χρησιμοποιώντας για παράδειγμα Robots Exclusion Standards, CAPTCHAS και άλλα).

- Scripted content: Ιστοσελίδες που είναι διαθέσιμες μόνο από συνδέσμους που παράγονται από JavaScript καθώς και περιεχόμενο που κατεβάζεται από Web servers μέσω Flash ή Ajax.

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

Η επαφή μας με το Deep Web είναι καθημερινή. Αν νομίζουμε πως εμείς δεν έχουμε έρθει ποτέ σε επαφή με το Deep Web μάλλον κάνουμε λάθος. Έστω και έμμεσα από τη στιγμή που κάνουμε χρήση του Διαδικτύου ερχόμαστε σε επαφή με δεδομένα που βρίσκονται βαθιά αποθηκευμένα στο Deep Web. Όλες οι ιστοσελίδες, οι εφαρμογές, οι φωτογραφίες ή τα βίντεο που παρακολουθούμε καθημερινά στον υπολογιστή μας είναι το αποτέλεσμα κάποιας υποδομής που δημιουργήθηκε και διαχειρίζεται μέσω του Deep Web.

Κοινώς το Administration Panel ή το cPanel (πίνακες ελέγχου) μέσω των οποίων ο εκάστοτε διαχειριστής (admin) ελέγχει και διαχειρίζεται τον server στον οποίο βρίσκουμε αποθηκευμένη την ιστοσελίδα του ανήκει στο Deep Web. Επομένως η υποδομή που υπάρχει πίσω από κάθε ιστοσελίδα είναι μη ανιχνεύσιμη από τις μηχανές αναζήτησης. Είναι δυναμικά παραγόμενη καθώς δεν υπάρχει μέχρι τη στιγμή που θα ζητήσουμε να παραχθεί και μόνο για όσο χρόνο κάνουμε χρήση της και φυσικά δεν είναι δημόσια προσβάσιμη αφού χρειάζεται username και password για να παραχθεί.

Γενικά όπου χρησιμοποιούμε ατομικούς κωδικούς, ώστε να έχουμε μόνο εμείς πρόσβαση, όπως για παράδειγμα λογαριασμοί στα μέσα κοινωνικής δικτύωσης, λογαριασμοί e-mail, λογαριασμοί στο gsis.gr, λογαριασμοί e-banking κλπ. ανήκουν ήδη στο Deep Web.

- Η υπόθεση είναι πώς χρησιμοποιούμε το deep web
- είναι ηθικές οι επθέσεις
- που αποσκοπούν
- τι μπορεί να κρύβεται πίσω από αυτές; Για ποιο σκοπό γίνονται;
- είναι σωστό ή καλό που υπάρχει
- τι θα γινόταν εάν αυτές οι επιθέσεις έκαναν κάτι κακό ή τρομαχτικό; Θα μπορούσαν να καταρρεύσουν τα πάντα;
- Πώς θα μπορούσαν να προφυλαχτούν αυτοί που πρέπει να προφυλαχτούν;
- Έχουν οι επιθέσεις επιπτώσεις στην καθημερινότητά μας;

ΒΙΒΛΙΟΓΡΑΦΙΑ

[CITATION How11 \l 1033][CITATION Den \l 1033]

(n.d.).

Bach, R. (2014, June 26). *Who's hacking who?* Retrieved from Bach Seat: http://rbach.net/blog/index.php/whos-hacking-who/

Bailey M., C. E. (2006, March). *Practical darknet measurement. In Information Sciences and Systems.*

Ban T., Z. L. (2012, November). *Behavior analysis of long-term cyber attacks in the darknet. In Neural Information Processing (pp. 620-628). Springer Berlin Heidelberg.*

Barney, C. (2004). *Information Technology for Energy Managers.* Retrieved from books.google.gr: https://books.google.gr/books?id=dr7Ic0t_BGkC&pg=PA224&lpg=PA224&dq=radmin+port+4899+attack&source=bl&ots=SRUptCAnCD&sig=6L1z3kN9K01V0MeVU8JHwxDjhKg&hl=el&sa=X&ved=0ahUKEwjr3q37v8jOAhWMBcAKHcy-DIQQ6AEIPDAE#v=onepage&q=radmin%20port%204899%20attack&f=false

Bethencourt J., L. W. (2007, July). *Establishing darknet connections: an evaluation of usability and security. In Proceedings of the 3rd symposium on Usable privacy and security.*

Biddle P., E. P. (2002). *The darknet and the future of content protection. In Digital Rights Management. Springer Berlin Heidelberg.*

Biddle P., E. P. (2002, November). *The darknet and the future of content distribution In ACM Workship on Digital Rights Management.*

Brenner, B. (2015, February 12). *Attackers using new ms sql reflection techniques.* Retrieved from https://blogs.akamai.com/2015/02/plxsert-warns-of-ms-sql-reflection-attacks.html

Cobb, M. R. (n.d.). *Secure Shell (SSH).* Retrieved from SearchSecurity: http://searchsecurity.techtarget.com/definition/Secure-Shell

Couts, A. (2012, November 27). *The next generation of hacker hunting will happen in real time.* Retrieved from Digital trents: http://www.digitaltrends.com/web/next-generation-hacker-hunting-ip-viking-norse-corp/#:eMtKrGC36PnozA

Cyberwars: Watching the US and China in Real-Time. (2014, July 2). Retrieved from stories by williams: https://storiesbywilliams.com/tag/microsoft-ds/

Denial of Service. (n.d.). Retrieved from http://galaxy.cs.lamar.edu/~bsun/forensics/slides/DoS.pdf

F., V. L. (2004). *Measuring the Digital Millennium against the Darknet: Implications for the regulation of technological protection measures.*

F., W. (2011, September). *The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services. In Intelligence and Security Informatics Conference (EISIC), 2011 European (pp. 209-213). IEEE.*

How does internet works. (2011, December 17). Retrieved from Valter Popeskic: https://howdoesinternetwork.com/2011/telnet-attacks

Information Security. (2012, March). Retrieved from http://security.stackexchange.com/questions/12961/if-a-router-has-port-5060-open-and-i-know-that-there-is-unencrypted-sip-traffic

IP-Viking. (n.d.). Retrieved from hp.ipviking.com

J., B. (2014). *The Dark Net. Random House.*

J., M. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs. Palgrave Macmillan.*

Kezys, M. (2015, March 24). *SIP Attack: Friendly-Scanner.* Retrieved from Kolmisoft Blog: http://blog.kolmisoft.com/sip-attack-friendly-scanner/

Kirat, O. (2015, September 29). *How To Set Up VNC Server on Debian 8*. Retrieved from Digital Ocean, Inc.: https://www.digitalocean.com/community/tutorials/how-to-set-up-vnc-server-on-debian-8

Kirk, J. (2011, January 27). *Hackers turn back the clock with Telnet attacks.* Retrieved from network world: http://www.networkworld.com/article/2199246/network-security/hackers-turn-back-the-clock-with-telnet-attacks.html

Krause, H. F. (2003). *Information Security Management Handbook, Fifth Edition.*

M., B. R. (2008, December). *The Deployment of a Darknet on an Organization-Wide Network: An Empirical Analysis. In High Assurance Systems Engineering Symposium, 2008. HASE 2008.*

Nazario, J. (2007, July 2). *Network Disruptions: VNC and TCP Port 5405*. Retrieved from Arbor Networks: https://www.arbornetworks.com/blog/asert/network-disruptions-vnc-and-tcp-port-5405/

Nolan, A. (n.d.). *How to remotely access your computer.* Retrieved from http://www.alexnolan.net/articles/remote_access/remotely_access_pc.htm

Norse - About us. (n.d.). Retrieved from http://www.norse-corp.com/about-us/who-we-are/

Reisigner, D. (2013, October 16). *Microsoft-DS no longer hackers' top target.* Retrieved from CNET: http://www.cnet.com/news/microsoft-ds-no-longer-hackers-top-target/

S., R. S. (2013). *Trust darknet: Control and compromise in the internet's certificate authority model. Internet Computing, IEEE.*

ShieldsUp. (n.d.). Retrieved from https://www.grc.com/port_8080.htm#top

ShieldsUp. (n.d.). Retrieved from Gibson Research Corporation: https://www.grc.com/port_445.htm

ShieldsUp. (n.d.). Retrieved from Gibson Research Corporation: https://www.grc.com/port_443.htm

ShieldsUp. (n.d.). Retrieved from Gibson Research Corporation: https://www.grc.com/port_53.htm

ShieldsUp. (n.d.). Retrieved from Gibson Research Corporation: https://www.grc.com/port_8123.htm

ShieldsUp. (n.d.). Retrieved from Gibson Research Corporation: https://www.grc.com/port_8090.htm

ShieldsUp. (n.d.). Retrieved from Gibson Research Corporation: https://www.grc.com/port_53413.htm

Siles, R. (2009, October 20). *Cyber Security Awareness Month - Day 20 - Ports 5060 & 5061 - SIP (VoIP).* Retrieved from InfoSec Handlers Diary Blog: https://isc.sans.edu/diary/Cyber+Security+Awareness+Month+-+Day+20+-+Ports+5060+%26+5061+-+SIP+(VoIP)/7405

TCP/IP Services and Attacks. (n.d.). Retrieved from http://www.lf69.at/netzwerktechnik/tcpipports.htm

Tennent, S. (2015, August 19). *Quora.* Retrieved from https://www.quora.com/What-is-port-8080-used-for

UDP Ports list (3178 ports in list). (n.d.). Retrieved from https://www.gasmi.net/udp.php

Virtual Network Computing (VNC). (n.d.). Retrieved from WireShark: https://wiki.wireshark.org/VNC

Wang Q., C. Z. (2011). *Darknet-based inference of internet worm temporal characteristics. Information Forensics and Security.*

wikipedia. (n.d.). Retrieved from https://el.wikipedia.org/wiki/Telnet

wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/HTTPS

wikipedia. (n.d.). Retrieved from https://de.wikipedia.org/wiki/Remote_Framebuffer_Protocol

wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/RFB_protocol

Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Secure_Shell

Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Microsoft_SQL_Server

Wikipedia. (n.d.). Retrieved from https://el.wikipedia.org/wiki/Domain_Name_System

Wikipedia. (n.d.). Retrieved from https://en.wikipedia.org/wiki/Session_Initiation_Protocol