Για τις τεχνικές απόκρυψης του δικτύου Tor

Το κείμενο αυτό είναι καθαρά τεχνικό. Στοχεύει στην ενημέρωση γύρω απ' τις τεχνικές ανωνυμίας στο ίντερνετ, με απλή και όχι εξειδικευμένη γλώσσα. Απευθύνεται σε αυτούς που λαμβάνουν σοβαρά την αυτοπροστασία τους και διατίθενται να εντρυφήσουν σε κάποιες βασικές έννοιες. Απαντάει στη σύγχυση που έχει προκληθεί γύρω απ' την ασφάλεια του tor, τεκμηριώνει το γιατί να εμπιστευτείς τις μεθόδους που προτείνει, ενώ παράλληλα αποτελεί οδηγό ορθής χρήσης των εργαλείων ανωνυμίας. Είναι συνολικό καθώς σε κρίσιμα ζητήματα η ημιμάθεια μπορεί να αποδειχθεί πιο επικίνδυνη της αμάθειας.

ΑΡΧΕΣ ΑΝΩΝΥΜΙΑΣ - ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Παρακολούθηση στοχευμένη

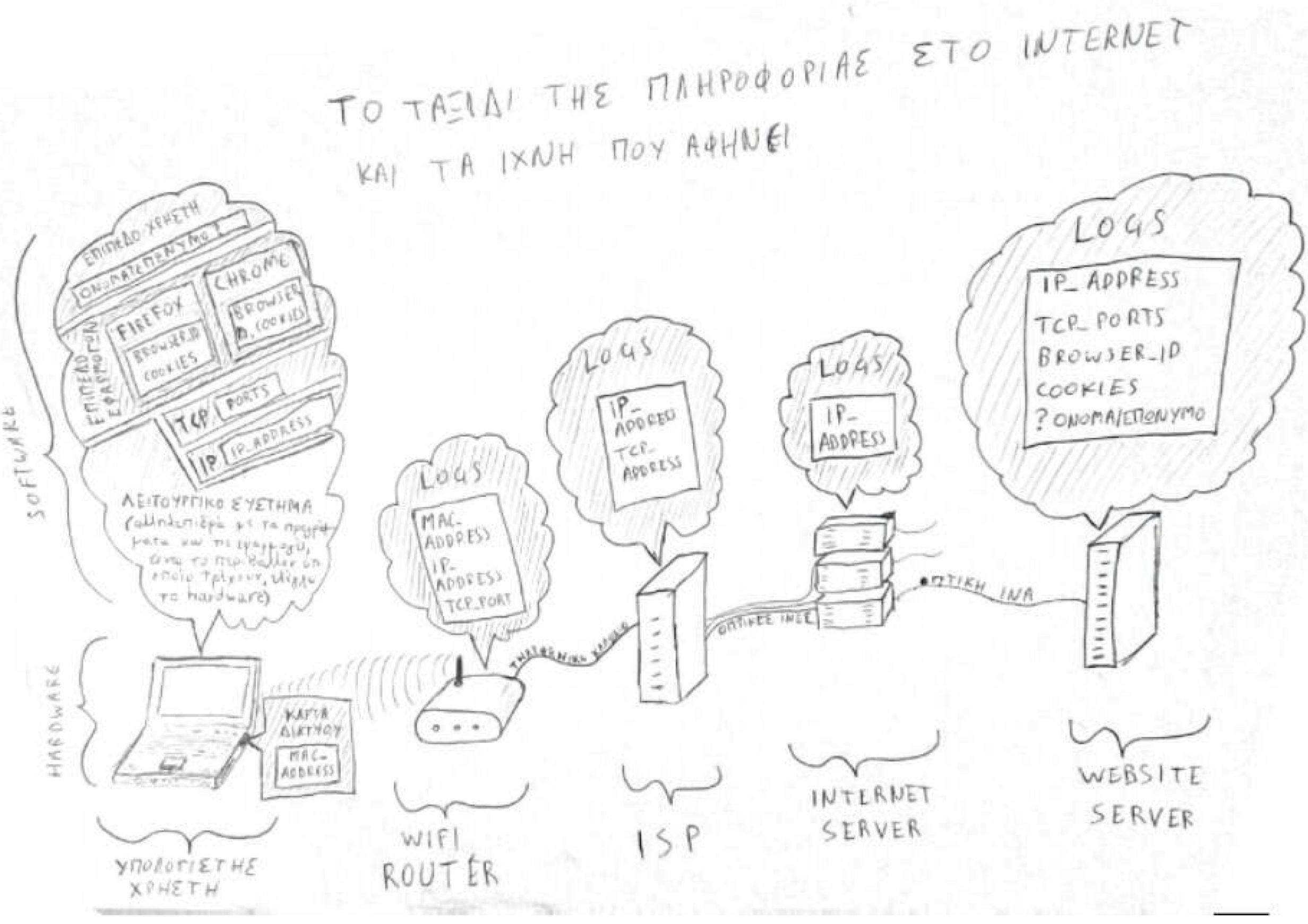
Αν είσαι ύποπτος, ο πιο απλός τρόπος να γνωρίζουν οι μπάτσοι όλη σου τη δραστηριότητα στον υπολογιστή, ανεξάρτητα απ' το αν χρησιμοποιείς ή όχι προγράμματα ανωνυμίας, είναι να εγκαταστήσουν στον υπολογιστή κατασκοπευτικό λογισμικό (spyware). Το πιο σύνηθες είναι κάποιο πρόγραμμα keylogger που στέλνει ότι πληκτρογραφείς και ότι κλικ κάνεις στους σέρβερ της αστυνομίας.
Αν όμως αυτοπροστατεύεσαι χρησιμοποιώντας ασφαλές λογισμικό, που δεν επιτρέπει την παρουσία τέτοιου είδους κακόβουλων προγραμμάτων, οι μπάτσοι είναι περιορισμένοι στην υποκλοπή όλων των δεδομένων που εξέρχονται. Στην περίπτωση αυτή, έχει νόημα η χρησιμοποίηση προγραμμάτων ισχυρής κρυπτογράφησης και ανωνυμίας ώστε να μην μπορουν να διαβάσουν τα ευαίσθητα δεδομένα σου.

Η διαδικασία της ταυτοποίησης και του εντοπισμού

Υπάρχουν πολλοί τρόποι να αποκαλυφθεί η θέση και η ταυτότητα κάποιου στο ίντερνετ, αξιοποιώντας τα τεχνικά χαρακτηριστικά του δικτύου, που δε διαθέτει εγγενώς καμία υποδομή για ανωνυμία. Στον εντοπισμό συμβάλλουν χαρακτηριστικά από κάθε επίπεδο οργάνωσης της δικτύωσης:

- από **προσωπικά δεδομένα** στο επίπεδο χρήστη (π.χ. ονοματεπώνυμο που αποστέλλει ο χρήστης στο mail provider),
- στο επίπεδο εφαρμογών το **αναγνωριστικό του προγράμματος περιήγησης, browser_id,** και τα **cookies** δηλαδή αρχεία που χρησιμοποιούν οι ιστοσελίδες για να σε ταυτοποιούν, ή αντίστοιχα αναγνωριστικά σε άλλες εφαρμογές.
- τις **ανοιχτές θύρες (ports)** επικοινωνίας στο επίπεδο μεταφοράς δεδομένων, όπως και τη συμπεριφορά του λειτουργικού συστήματος,
- τη **διεύθυνση IP** με την οποία εκτίθεται ο υπολογιστής στο διαδίκτυο
- και τη **διεύθυνση της κάρτας δικτύου mac address** η οποία φαίνεται στο τοπικό δίκτυο.

Κάθε χαρακτηριστικό και κάθε διεύθυνση είναι εφικτό να αλλάξει ή να μεταμφιεστεί με την εγκατάσταση κατάλληλου λογισμικού και τις αντίστοιχες ρυθμίσεις. Όμως το σημείο του δικτύου που συνδεθήκαμε είναι μια πληροφορία προσβάσιμη στον καθένα.



Ας δούμε στην πράξη τί σημαίνει μια απλή ταυτοποίηση μέσω IP. Έστω ότι είσαι σπίτι σου και θες να μπεις σε μία ιστοσελίδα μιας εταιρίας που σκοπεύεις να χτυπήσεις. Ανοίγεις το firefox και επισκέπτεσαι την ιστοσελίδα της εταιρίας. Τότε ο σέρβερ που φιλοξενεί τη σελίδα της εταιρίας καταγραφει την διεύθυνση IP σου. Αφού η εταιρία χτυπηθεί πιθανόν οι μπάτσοι να ψάξουν ποιός και γιατί επισκέφθηκε την σελίδα της. Όταν δουν την ύποπτη επίσκεψη θα ερευνήσουν σε ποιόν αντιστοιχεί η διεύθυνση IP. Θα δουν ποιός ISP (internet service provider π.χ. οτε, forthnet, hol) παρέχει τη συγκεκριμένη διεύθυνση και θα αναζητήσουν στις καταγραφες (logs) των σέρβερ του ISP, ποιός τη συγκεκριμένη ώρα της επίσκεψης χρησιμοποιούσε τη συγκεκριμένη διεύθυνση IP. Έτσι θα ταυτοποιηθείς.

Πάμε τώρα σε πιο σύνθετες μεθόδους ταυτοποίησης. Έστω ότι είσαι πιο προσεκτικός. Σηκώνεις το λάπτοπ σου και πας σε μία καφετέρια με wifi και πριν κάνεις την επίσκεψη στην ιστοσελίδα της εταιρίας-στόχου ρυθμίζεις διαφορετικά την IP σου. Όταν η αστυνομία εντοπίσει την IP σου θα δει ότι την ώρα της επίσκεψης αντιστοιχούσε σε έναν υπολογιστή από το δίκτυο της καφετέριας. Αντί να συλλάβουν τον ιδιοκτήτη της καφετέριας θα ψάξουν άλλα ίχνη που άφησε πίσω του ο υπολογιστης σου. Πιθανόν να είναι καταγεγραμμένη η mac address (η φυσική διεύθυνση της κάρτας δικτύου) στον wifi router της καφετέριας. Αυτή είναι μοναδική για κάθε κάρτα δικτύου και μπορούν να αναζητήσουν ποιός την αγόρασε στα αρχεία των καταστημάτων. Φυσικά θα μπορούσαν να δουν και τις καταγραφές στον σέρβερ της ιστοσελίδας όπου πιθανότατα θα φαίνεται ο browser id ή στοιχεία απ' τα cookies σου αν δεν τα καθάρισες.

Αν είσαι αρκετά προσεκτικός, και πριν πας στην καφετέρια και αφού φύγεις, επανεγκαταστήσεις το λειτουργικό σου σύστημα, και όλα τα προγράμματα και αλλάξεις την mac address (και δεν μπεις στο προσωπικό σου mail από την καφετέρια): Δεν θα αφήσεις ίχνη και οι μπάτσοι δε θα σε ταυτοποιήσουν.

ΣΗΜΕΙΩΣΗ: Φυσικά για μια τόσο περιορισμένη χρήση του ίντερνετ εκτός ότι υπάρχουν απλούστερες λύσεις όπως ένα νετ καφέ χωρίς κάμερες, δεν είναι ρεαλιστικό να σε ταυτοποιήσουν καθώς οι σελίδες των εταιριών δέχονται χιλιάδες επισκέψεις. Ειναι ένα απλουστευμένο παράδειγμα.

Οι proxy servers

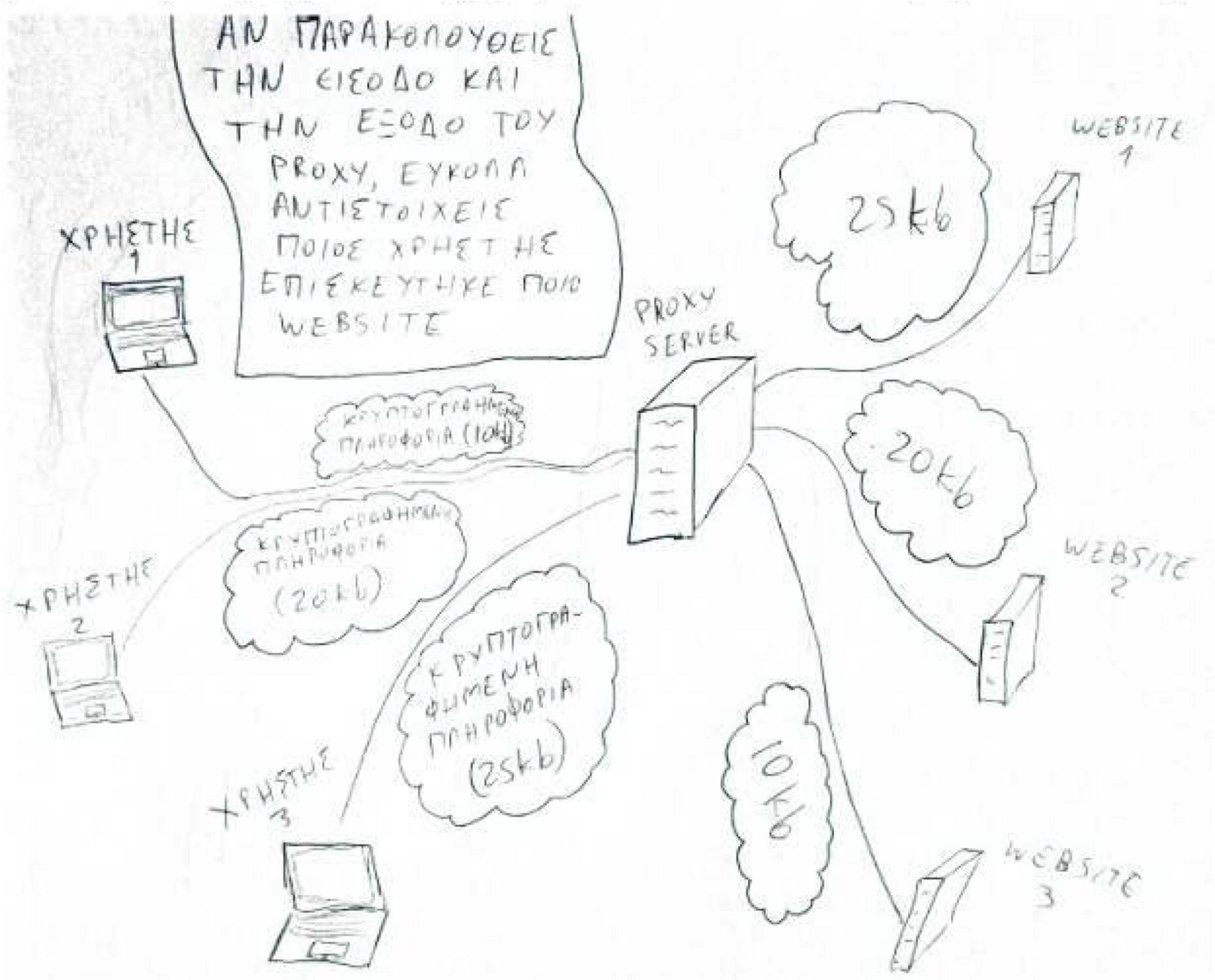
Ας γίνουμε τώρα λίγο πιο απαιτητικοί στην ανωνυμία μας. Εστω ότι θέλουμε να στείλουμε ανάληψη ευθύνης μέσω mail. Στην περίπτωση αυτή αν λάβουμε τα μέτρα που είπαμε παραπάνω, ο υπολογιστής μας δεν θα ταυτοποιηθεί, όμως οι μπάτσοι σε 10 λεπτά πιθανόν να βρίσκονται στην καφετέρια. Ακόμα κι αν έχουμε φύγει τα αποτυπώματα μας και η περιγραφη μας θα είναι φρέσκια. Άρα χρειαζόμαστε ένα τρόπο να μην εντοπιστούμε άμεσα.

Ο τρόπος αυτός υπάρχει (δεν συνίσταται καθώς υπάρχουν ασφαλέστερες λύσεις). Είναι η χρήση ενός σέρβερ μεσολαβητή (proxy) ανάμεσα στον υπολογιστή σου και τον σέρβερ του mail που θα χρησιμοποιήσεις. Ο proxy server διαμεσολαβεί αποκρύπτοντας τα παραγματικά σου στοιχεία. Για την ακρίβεια ο σέρβερ του mail βλέπει μόνο την ip του proxy server και όχι τη δική σου καθώς εσύ επικοινωνείς μόνο με τον proxy ο οποίος επαναλαμβάνει ότι του έστειλες αλλά το κάνει να φαίνεται σαν να προήλθε απ' αυτόν. Υπάρχουν αυρκετά site που παρέχουν υπηρεσίες anonymity proxy (διαμεσολαβητή ανωνυμίας) όπως πχ το hidemyass.com.

Όμως κάθε proxy γνωρίζει και καταγράφει ποιός έκανε τί μέσα απ' αυτόν. Και όταν οι μπάτσοι βρουν ότι το κακό μέιλ στάλθηκε απ' τη διεύθυνσή του, η εταιρία θα αναγκαστεί να δώσει την πληροφορία του ποιός είσαι. Οπότε αργά ή γρήγορα οι μπάτσοι θα είναι πάλι στο κατόπι σου...

Η αδυναμία του proxy - traffic analysis

Εστω πάντως ότι η εταιρία αρνείται να συνεργαστεί. Υπάρχει άλλος ένας τρόπος να βρουν που είσαι (το να βρουν ποιός, εναπόκειται στην τήρηση των μέτρων που περιγράψαμε παραπάνω). Η ανάλυση κίνησης. Μπορούν να δουν τι εισέρχεται και τί εξέρχεται απ' τον proxy, και έτσι να κάνουν την αντιστοίχηση. Γι αυτό το λόγο η επικοινωνία μεταξύ του υπολογιστή σου και του proxy είναι κρυπτογραφημένη σε ένα σοβαρό σύστημα ανωνυμίας. Όμως ακόμα κι έτσι μπορούν να μετρήσουν τον όγκο της πληροφορίας που διακινείται σε συγκεκριμένες χρονικές στιγμές και να κάνουν έτσι την ταυτοποίηση.
Δύο αντίμετρα υπάρχουν στην ταυτοποίηση κίνησης. Το ένα είναι η εισαγωγή χαοτικών δεδομένων στην κρυπτογραφημένη ροή εισόδου του proxy που αυξάνουν τυχαία τον όγκο της πληροφορίας ώστε να μην είναι ταυτοποιήσιμη με τη ροή εξόδου και να μη γίνεται αντιστοίχηση. Το δεύτερο αντίμετρο είναι η εισαγωγή τυχαίων καθυστερήσεων δηλαδή ο proxy καθυστερεί για τυχαία χρονικά διαστήματα να αναπαράξει αυτό που του έστειλες για να εμποδίσει την ανάλυση κίνησης. Φυσικά χρησιμοποιείται και συνδυασμός αυτών των μεθόδων.



Συνθετα συστήματα ανωνυμίας

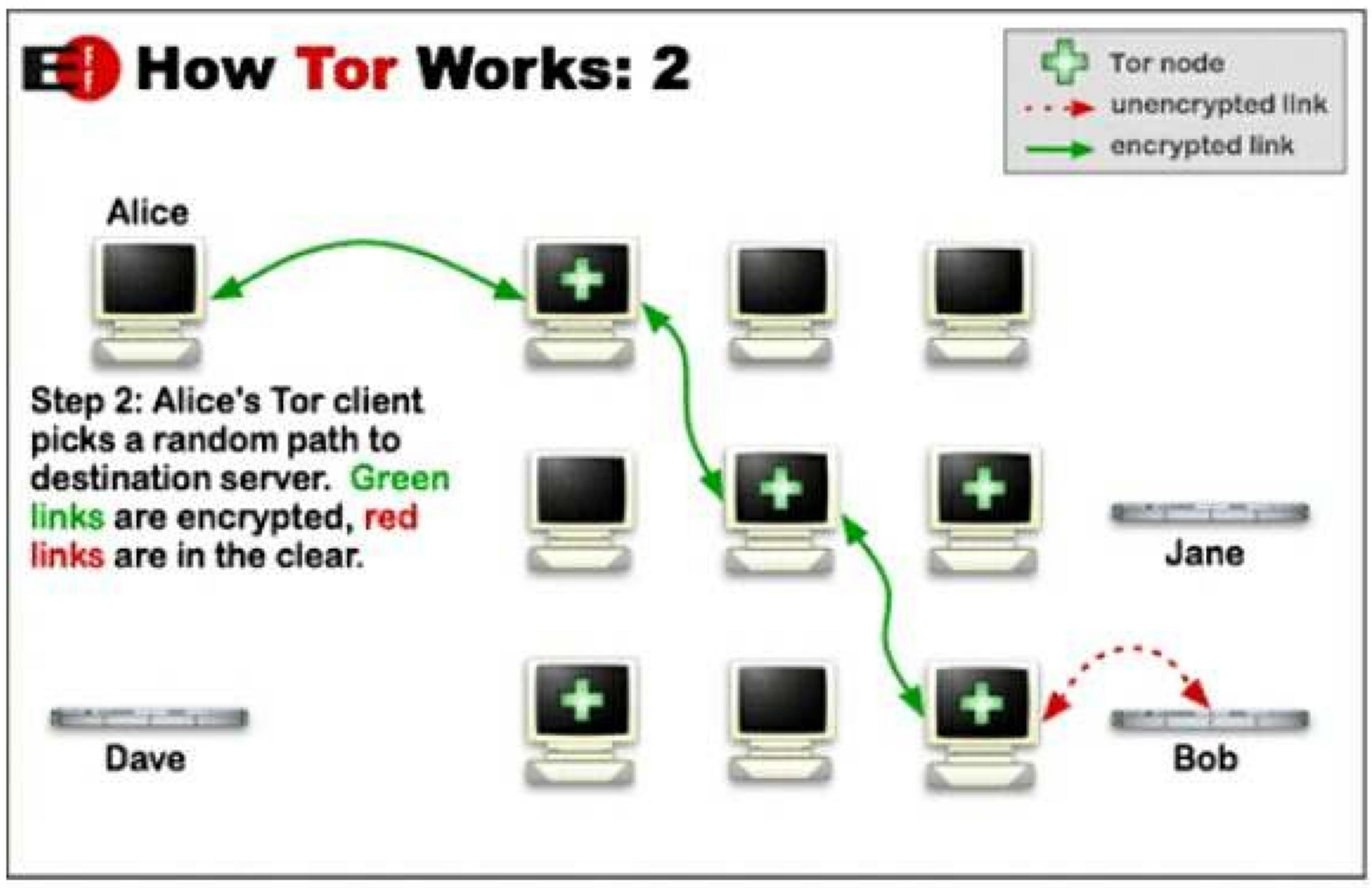
Για να αντιμετωπιστούν οι αδυναμίες των proxy τόσο ως προς την εμπιστοσύνη όσο και της ανάλυσης κίνησης, έχουν σχεδιαστεί συστήματα ανωνυμίας proxy μέσα από proxy. Ανάλογα με το κατά πόσον χρησιμοποιούν την τεχνική της καθυστέρησης χωρίζονται σε συστήματα χαμηλής (low latency), και υψηλής καθυστέρησης (high latency). Τα δεύτερα έχουν περιορισμένη χρηστικότητα λόγω των μεγάλων καθυστερήσεων αλλά θεωρητικά είναι πιο ασφαλή.

ασύμμετρη κρυπτογραφία

Κάθε σύστημα ανωνυμίας βασίζεται στην ασύμμετρη κρυπτογραφία ή αλλιώς κρυπτογράφηση δημοσίου κλειδιού. Ονομάζεται έτσι γιατί ο κωδικός κρυπτογράφησης είναι διαφορετικός από τον κωδικό αποκρυπτογράφησης.
Με αυτήν την κρυπτογραφική τεχνική αν θες να σου στείλουν ένα κρυπτογραφημένο μήνυμα μέσω του δικτύου δημοσιοποιείς τον κωδικό κρυπτογράφησης (δημόσιο κλειδί) και αποκρυπτογραφείς το μήνυμα μέσω του κωδικού αποκρυπτογράφησης που κατέχεις μόνο εσύ. Δηλαδή είναι σαν να έχεις ένα λουκέτο με το μοναδικό κλειδί που το ανοίγει, και στέλνεις σε κάποιον το λουκετο. Αυτός στη συνέχεια βάζει το μήνυμα σε ένα κουτί, το σφραγίζει με το λουκέτο που του έστειλες (το λουκέτο αντιστοιχεί στο δημόσιο κλειδί), και στο στέλνει. Μόνο εσύ μπορείς να διαβάσεις το μήνυμα άφου μόνο εσύ έχεις το κλειδί που ανοίγει το λουκέτο.
Η τεχνική αυτή στο υπολογιστικό περιβάλλον βασίζεται στις ιδιαίτερες μαθηματικές ιδιότητες των πρώτων αριθμών (αριθμοί που διαιρούνται μόνο με το 1 και τον εαυτό τους). Για την ακρίβεια στο ότι ότι δεν χρειάζεται πολλούς υπολογισμούς για να πολλαπλασιάσεις δύο πολυ μεγάλους πρώτους αριθμούς, αλλά για να βρεις από το πολλαπλάσιο τους δύο διαιρέτες πρώτους αριθμούς χρειάζεσαι υπολογιστική ισχύ που δεν υπάρχει στις μέρες μας (ασυμμετρία). Οι δύο διαιρέτες συμπεριλαμβάνονται στην παραγωγή του ιδιωτικού κλειδιού και το πολλαπλάσιο στην παραγωγή του δημόσιου κλειδιού. Οι αλγόριθμοι που υλοποιούν αυτή την τεχνική παραείναι σύνθετοι για να εκτεθούν εδώ, το ίδιο και η μαθηματική απόδειξη της αξιοπιστίας τους.
Η καθημερινή απόδειξη της αξιοπιστίας τους είναι η γενικευμένη χρήση της ασύμμετρης κρυπτογραφίας στο ιντερνετ: όλες οι χρηματοπιστωτικές συναλλαγές βασίζονται πλέον σε αυτήν, αν κάποιος μπορούσε να τη σπάσει θα κατακτούσε τον κόσμο.
Δεν ισχύει το ίδιο όμως για κάθε επιμέρους υλοποίηση της ασύμμετρης κρυπτογραφίας. Σε κάθε υλοποίηση μπορεί να υπάρχουν αδυναμίες. Αυτές σχετίζονται συνήθως με τους τυχαίους κωδικούς που παράγονται από τα προγράμματα αυτά με τη βοήθεια του λειτουργικού συστήματος, και οι κωδικοί παράγονται από ψευδοτυχαίους αριθμούς. Το πρόβλημα εμφανίζεται γιατί ο επεξεργαστής δεν έχει κάποια δομή σαν ζάρι, αντίθετα υπάρχουν προγράμματα γεννήτριες τυχαίων αριθμών που στην πραγματικότητα φτιάχνονται από μία σειρά προκαθορισμένων υπολογισμών. Βάσει αυτού θα μπορούσε κάποιος να συναγάγει όλη τη ροή ψευδοτυχαίων αριθμών άρα και τους κωδικούς αν η γεννήτρια δεν είναι τόσο αξιόπιστη.

ΤΟ ΣΥΣΤΗΜΑ ΑΝΩΝΥΜΙΑΣ TOR

Το tor (the onion routing), είναι ένα σύστημα ανωνυμίας χαμηλής καθυστέρησης, όμως προσφέρει ισχυρή ανωνυμία. Αυτό το καταφέρνει καθοδηγώντας την ανταλλαγή δεδομένων μέσα από ένα χαοτικό δίκτυο πολλών διαμεσολαβητών υπολογιστών (proxy servers), τους οποίους τρέχουν διάφοροι εθελοντές, οπότε ο καθένας μπορεί να αποτελέσει μέρος του δικτύου. Τα δεδομένα που ανταλάσσονται κινούνται κρυπτογραφημένα σε τυχαίες διαδρομές τις οποίες κανένας υπολογιστής του δικτύου δεν γνωρίζει ολόκληρες, ώστε αν κάποιος από τους proxy υπολογιστές υποκλέπτει ή παρέχει πληροφορίες στους μπάτσους, να μην μπορεί να εξακριβώσει την προέλευση ή τον προορισμό των δεδομένων. Για πρόσθετη ασφάλεια ανά 10 περίπου λεπτά δημιουργείται καινούριο κύκλωμα διαμεσολαβητών. Κάθε κύκλωμα έχει και διαφορετικό διαμεσολαβητή εξόδου, άρα δείχνει και διαφορετική IP στο δίκτυο.
Για να μείνει κρυφή η συνολική διαδρομή από τα μέρη του δικτύου χρησιμοποιείται κρυπτογράφηση μέσα σε κρυπτογράφηση, σχηματίζοντας γύρω απ' τα δεδομένα μία δομή με πολλαπλά στρώματα κρυπτογράφησης που θυμίζει κρεμμύδι (onion). Το όνομα the onion routing σημάινει δρομολόγηση κρεμμυδιού.

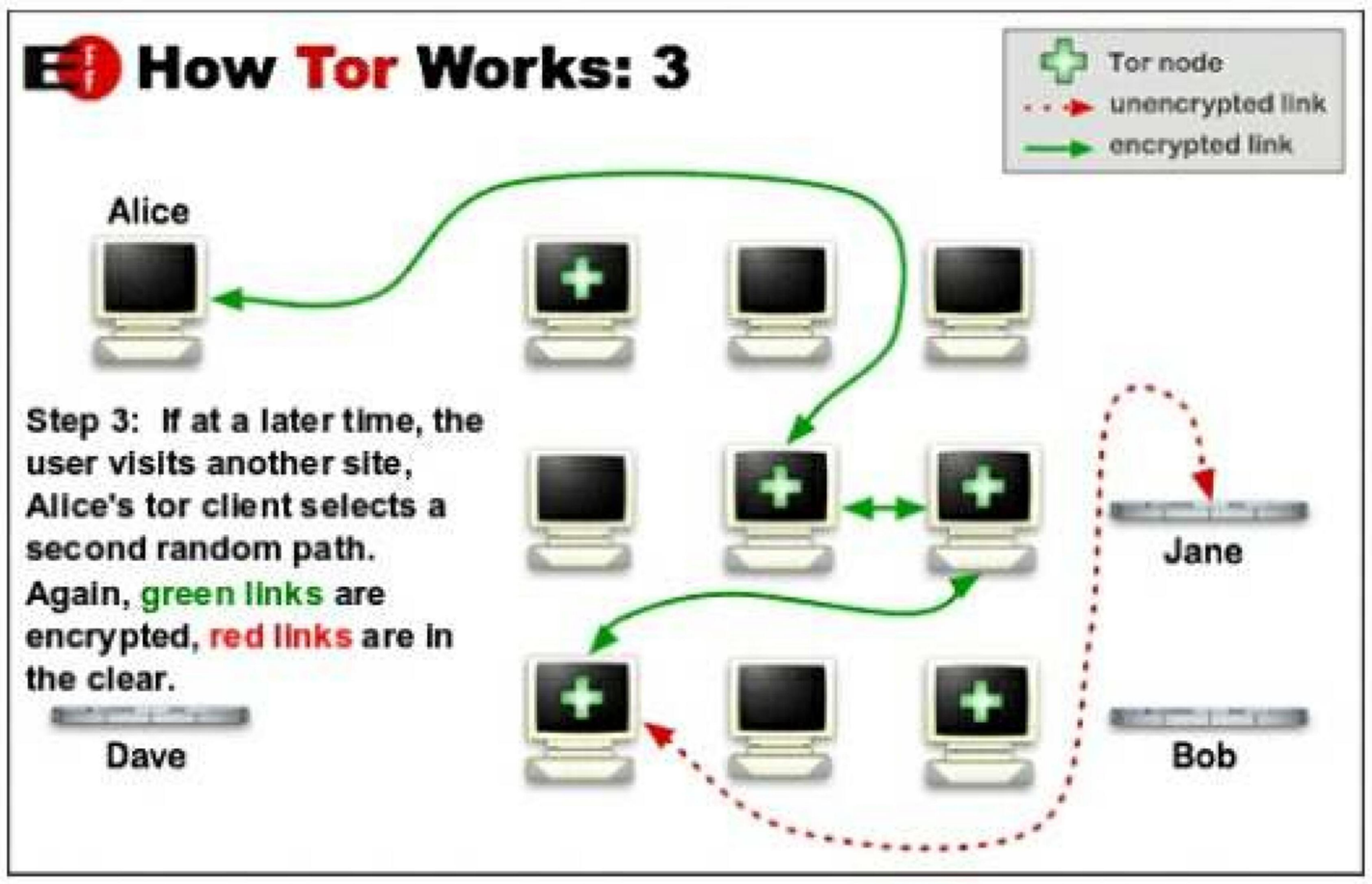


ποιοί και γιατί το χρησιμοποιούν;

Όσοι τους χρησιμεύει: κυβερνήσεις, διπλωμάτες, στρατοί, κατάσκοποι, μυστικές υπηρεσίες, ακτιβιστές, επαναστάτες, αντάρτες, εγκληματίες, παράνομοι, διακινητές παιδικής πορνογραφίας, άνθρωποι που ανήκουν σε εχθρικές μεταξύ τους κοινωνικές κατηγορίες, ανακατεύουν τα δεδομένα τους στο χάος της ανωνυμίας. Είναι σαν το μαχαίρι, όπως κάθε εργαλείο, ο σκοπός της χρήσης του εναπόκειται στο ήθος του υποκειμένου που το χρησιμοποιεί.
Χρησιμοποιείται είτε από ανθρώπους που αποτελούν στοχο παρακολούθησης ώστε να μην φαίνεται σ' αυτούς που τους παρακολουθούν ποιές ιστοσελίδες επισκέπτονται, τί δραστηριότητες έχουν και με ποιούς επικοινωνούν, είτε από ανθρώπους που θέλουν να κρύψουν τη θέση τους (π.χ. καταζητούμενος που συνομιλεί με άτομο υπό παρακολούθηση χωρίς να εντοπίζεται), μία χακερίστικη δραστηριότητα ή μία παράνομη δράση.

the onion routing

Ας δούμε στην πράξη πως δουλεύει ένα κανάλι επικοινωνίας στο tor. Κάθε κόμβος στο κανάλι γνωρίζει μόνο τους γειτονικούς του και δεν το αποκαλύπτει.
Τα πακέτα δεδομένων μαζί με τον τελικό προορισμό τους κρυπτογραφούνται πριν φύγουν από τον υπολογιστή του χρήστη για να ταξιδέψουν προς τον διαμεσολαβητή - κόμβο εισόδου του δικτύου tor. Ο κωδικός κρυπτογράφησης είναι ένα δημόσιο κλειδί που έχει αποσταλεί από τον κόμβο εισόδου που μόνο αυτός έχει το ιδιωτικό κλειδί, και έτσι φτιάχνεται ένα κρυπτογραφημένο κανάλι επικοινωνίας.
Μέσα από αυτό το κανάλι δημιουργείται μια αντίστοιχη σύνδεση με έναν τυχαίο ενδιάμεσο κόμβο του δικτύου, ο οποίος στέλνει και αυτός το δημόσιο κλειδί του στον υπολογιστή του χρήστη. Έτσι φτιάχνεται ένα κρυπτογραφημένο κανάλι μέσα από το κρυπτογραφημένο κανάλι, άρα ο κόμβος εισόδου δεν ξέρει να αποκρυπτογραφήσει τα δεδομένα μας ούτε και τον προορισμό τους.
Σε αυτό το σημείο η κρυπτογράφηση προσομοιάζει με κρεμμύδι γιατί έχει πολλαπλά στρώματα.
Το ίδιο ισχύει και για την επικοινωνία με τον κόμβο εξόδου, όπου ιδρύεται και τρίτο κανάλι μέσα σε κανάλι.
Οπότε ο τυχαίος ενδιάμεσος κόμβος αποκρυπτογραφεί το δεύτερο στρώμα και αποστέλλει την μονή κρυπτογραφημένη ροή στον κόμβο εξόδου. Ο ενδιάμεσος κόμβος δεν γνωρίζει τίποτα για τα δεδομένα μας ούτε την προέλευση, ούτε τον προορισμό τους, ξέρει μόνο από ποιόν κόμβο εισόδου τα πήρε και σε ποιόν κόμβο εξόδου πρέπει να τα δώσει.
Ο κόμβος εξόδου αποκρυπτογραφεί τα δεδομένα μας και τον προορισμό τους και τα αποστέλλει στον προορισμό τους. Οπότε ο κόμβος εξόδου μπορεί να γνωρίζει τα δεδομένα μας όχι όμως την προέλευση τους.
Γι αυτό το λόγο διάφοροι τρέχουν κόμβους εξόδου του tor ως ωτακουστές. Για παράδειγμα έτσι διέρρευσαν απόρρητες διπλωματικές επικοινωνίες των ΗΠΑ στο wikileaks. Φυσικά το αντίμετρο που μπορεί να πάρει ο χρήστης tor είναι να κρυπτογραφεί και την επικοινωνία με τον προορισμό του, αυτό όμως δεν είναι δουλειά του δικτύου tor. Π.χ. εάν στο σερφάρισμα χρησιμοποιεί αντί για http το https, ο κόμβος εξόδου θα τροφοδοτεί το site - προορισμό με κρυπτογραφημένη ροή χωρίς να μπορεί να κρυφακούσει τίποτα.



Γιατί να το εμπιστευτούμε;

Όπως είδαμε ένας proxy sever μπορεί να υποκλέπτει και να προδόσει την ταυτότητά μας σκόπιμα. Πως ξέρουμε ότι το tor δεν κάνει κάτι τέτοιο; Το ότι υπάρχουν πολλοί σέρβερ διαμεσολαβητές που ο καθένας μπορεί να τρέξει δεν αρκεί. Ένα εύλογο ερώτημα είναι, τί γίνεται αν το λογισμικό που τρέχουν οι διάφοροι σέρβερ κρύβει κακόβουλο κώδικα ο οποίος μας ρουφιανεύει;
Σίγουρα δε θα πρέπει να εμπιστευτούμε τις καλές προθέσεις των δημιουργών του. Η ιστορία του ξεκινάει από το πρόγραμμα **DARPA** των αμερικανικών στρατιωτικών δυνάμεων, ένα πρόγραμμα που συνδέεται με τα μεγαλύτερα τεχνολογικά επιτεύγματα, από το οποίο ξεκίνησε και το internet.

Όμως πλέον αποτελεί έργο **ανοιχτού κώδικα** και **ελεύθερο λογισμικό**. Εκεί θα βασίσω και τον ισχυρισμό μου ότι είναι εμπιστεύσιμο ως προς το ότι **δεν** είναι ένα μεγάλο κατασκοπευτικό πρόγραμμα.

Ανοιχτός κώδικας (open source) σημαίνει ότι οποιοσδήποτε επιθυμεί μπορεί να διαβάσει τον πηγαίο κώδικα ενός προγράμματος, όπως τον έγραψαν οι προγραμματιστές πριν μεταγλωττιστεί στην εκτελέσιμη μορφή του. Ένα εκτελέσιμο αρχείο, παράγεται από τον πηγαίο κώδικα με προγράμματα - μεταγλωττιστές και αποτελείται από κώδικα μηχανής, δηλαδή την αλληλουχία των εντολών που καταλαβαίνει ο επεξεργαστής. Είναι όμως πολύ δύσκολο έργο να συναγάγεις από το εκτελέσιμο αρχείο πως λειτουργεί ένα πρόγραμμα, και αυτό γίνεται μέσω μιας δύσκολης διεργασίας που λέγεται ανάστροφη μηχανική (reverse engineering). Ο ανοιχτός κώδικας λοιπόν είναι το αντίθετο του κλειστού κώδικα, δηλαδή τη στρατηγική των περισσότερων εταιριών λογισμικού να κρύβουν τον κώδικά των προγραμμάτων τους για να προστατέψουν τις πατέντες τους απ' την αντιγραφή.
Όμως στο κλειστό λογισμικό πιθανόν να υπάρχει κακόβουλος κώδικας, που μπορεί να υποκλέπτει τα δεδομένα του χρήστη και να τα στέλνει στην εταιρία η οποία στη συνέχεια τα μοσχοπουλάει σε διαφημιστικές εταιρίες (για να συναγάγουν το καταναλωτικό προφίλ σου και να σου στέλνουν στοχευμένη διαφήμιση, μια διαδικασία που γίνεται μαζικά αξιοποιώντας τις στατιστικές) ή σε μπάτσους και μυστικές υπηρεσίες. Πιο σύνηθες βέβαια είναι απλά να κρύβονται κερκόπορτες (backdoors) στο κλειστό λογισμικό, δηλαδή κώδικα που επιτρέπει τον έλεγχο της υπολογιστικής συσκευής εξ' αποστάσεως, με σκοπούς άγνωστους στο χρήστη, π.χ. για να υποκλέψουν δεδομένα. Μπορεί να φαίνεται ακραίο, αλλά είναι κάτι που στον κλειστό κώδικα γίνεται συχνά, π.χ. κερκόπορτες έχουν ανιχνευτεί από χάκερ με ανάστροφη μηχανική στο λειτουργικό σύστημα Windows της Microsoft, και το λογισμικό υποκλοπής carrierIQ, στα κινητά τηλέφωνα blackberry, iphone, αλλά και σε κάποια android τηλέφωνα.
Σημείωση: το android δίνεται ως ανοιχτού κώδικα από την google αλλά οι κατασκευάστριες εταιρίες κινητών τηλεφώνων τροποποιούν των κώδικα και τον κλείνουν, εγκαθιστόντας μαζί με αυτό επικίνδυνα προγράμματα όπως το **carrierIQ** το οποίο είναι επί της ουσίας keylogger, στέλνει κάθε πληκτρογράφηση στους server της εταιρίας. Είναι εφικτό να καθαρίσεις ένα τηλέφωνο από το carrierIQ διαγράφοντας τη rom του και εγκαθιστώντας το AOSP (Android Open Source Project).

Έλεύθερο λογισμικό σημαίνει, λογισμικό που πάντα διανείμεται μαζί με τον κώδικά του, ευνόητα γραμμένο και συνοδεύεται από μία άδεια που εγγυάται την ελευθερία οποιουδήποτε να δει, να τροποποιήσει και να αναδιανείμει τον κώδικα (π.χ. **GNU GPL**). Ένα πρόγραμμα μπορεί να είναι ανοιχτού κώδικα και να μην είναι ελεύθερο λογισμικό, αλλά το ελεύθερο λογισμικό είναι οπωσδήποτε και ανοιχτού κώδικα. Το βασικό πλεονέκτημα του ελεύθερου λογισμικού, εκτός του ότι ο κακόβουλος κώδικας θα γινόταν αμέσως ορατός, είναι ότι τα χιλιάδες έμπειρα μάτια που εξετάζουν τον κώδικα ανιχνεύουν τις αδυναμίες του και τις διορθώνουν άμεσα.
Τα έργα ελεύθερου λογισμικού αναπτύσσονται από κοινότητες προγραμματιστών αλλά και εταιρίες που επωφελούνται και το αξιοποιούν οικονομικά. Όμως η κινητήριος δύναμη της ύπαρξής του είναι οι ενεργές κοινότητες προγραμματιστών που δημιουργούν μια πραγματικότητα στην οποία οι εταιρίες αναγκάζονται να προσαρμοστούν (αυτή η συνύπαρξη εταιριών και κοινοτήτων σίγουρα δεν είναι ούτε ρηξιακή, ούτε αντικαπιταλιστική, ενώ οι κοινότητες στην πλειονότητα των περιπτώσεων διέπονται από τυπικές ιεραρχίες). Παραδείγματα ελεύθερου λογισμικού είναι ο firefox, το libre-office, το λειτουργικό σύσστημα GNU-Linux και το tor. Παραδείγματα λογισμικού ανοιχτού κώδικα που δεν είναι ελεύθερο λογισμικό, είναι ο Chromium της Google (ανοιχτού κώδικα έκδοση του διαδεδομένου κλειστού κώδικα Chrome), το λειτουργικό σύστημα android της ίδιας εταιρίας (περιέχει και κομμάτια ελεύθερου λογισμικού όπως ο linux πυρήνας), και κομμάτια του υποσυστήματος γραφικών του λειτουργικού συστήματος macos της apple.
Για να επανέλθουμε στην περίπτωση του tor λοιπόν, είναι εμπιστεύσιμο γιατί πολύ απλά οποιοσδήποτε με προγραμματιστικές γνώσεις μπορεί να πάρει τον κώδικα του, να τον διαβάσει και αφού τον εγκρίνει, να τον μεταγλωτίσσει και να συγκρίνει τα εκτελέσιμα που έφτιαξε με αυτά που διανέμει η σελίδα του tor. Επιπλέον μία μεγάλη μερίδα προγραμματιστών εξετάζει τον κώδικά του και κάθε τρύπα ασφαλείας που ανιχνεύεται διορθώνεται άμεσα και κυκλοφορούν συνεχώς νέες εκδόσεις. Έτσι παραμένει ασφαλές το λογισμικό αρκεί να είναι ενημερωμένο.

"Do not rely on it for strong anonymity"

Αυτή η φράση μοστράρει σαν σλόγκαν του tor στις ιστοσελίδες του. Σε αντίθεση με τις διάφορες εταιρίες που παρέχουν επισφαλή ανωνυμία μέσω proxy και τη διαφημίζουν ως εύκολη, εγγυημένη και ασφαλή, η μη κερδοσκοπική κοινότητα ανάπτυξης του tor συνιστα επαγρύπνηση, παρέχοντας την ισχυρότερη low latency ανωνυμία.
Όπως είδαμε η δύναμη του βασίζεται στη χαοτικότητα του και στην εξελιγμένη κρυπτογραφία.
Ας δούμε όμως τις αδυναμίες του και τις μορφές επίθεσης που μπορεί να δεχτεί η ασφάλεια και η ανωνυμία του.

1. Ταυτοποίηση κίνησης: Αν κάποιος παρακολουθεί τη σύνδεση δικτύου του υπολογιστή σου (και δεν τον έχει παγιδέψει με spyware), **μπορεί να καταλάβει ότι χρησιμοποιείς tor**, αλλά δεν μπορεί να διαβάσει τις κρυπτογραφημένες ροές και να δει τη δραστήριότητά σου. Μπορεί όμως να μετρήσει τον όγκο των δεδομένων σου και το χρόνο εκπομπής τους, δεδομένου ότι πρόκειται για σύστημα χαμηλής καθυστέρησης. Έτσι, αν με κάποιο τρόπο υποθέσει ποιός είναι ο κόμβος εξόδου, μπορεί να κάνει την ταυτοποίηση κίνησης. Στην πράξη βέβαια η χαοτικότητα του tor προστατεύει αποτελεσματικά από την ταυτοποίηση κίνησης, καθώς είναι πολύ δύσκολο να υποθέσεις και να συγκρίνεις σε τόσο μεγάλο πλήθος κόμβων εξόδου. Αντίστοιχη δυσκολία υπάρχει στο να ταυτοποιήσουν τον κόμβο εισόδου (άρα και τη θέση σου) αν γνωρίζουν τον κόμβο εξόδου (απ' τον οποίο π.χ. στάλθηκε μια ανάληψη ευθύνης).
Η επίθεση αυτή δεν είναι εφικτή αν χρησιμοποιείς το εσωτερικό διαδίκτυο του tor, που οι σελίδες του έχουν κατάληξη .onion και δεν είναι ορατές από το εκτός του tor διαδίκτυο.
Ένας τρόπος να αμυνθείς σε αυτήν την επίθεση είναι η εισαγωγή χαοτικών δεδομένων, μία τεχνική που θα εξηγήσουμε πρακτικά στο επόμενο κεφάλαιο. Το tor δεν ενσωματώνει αυτήν την τεχνική για να μην επιβαρύνει το δίκτυό του, δίνει όμως μια αρκετά καλύτερη επιλογή, να τρέξεις κι εσύ έναν ενδιάμεσο relay server, πράγμα που ισοδυναμεί με ροή τυχαίων δεδομένων και αντί να επιβαρύνει το δίκτυο το ενισχύει.

2. Κατάληψη μέρους του δικτύου: Αν κάποιος που θέλει να σπάσει την ανωνυμία σου, τρέχει αρκετούς κόμβους εισόδου και εξόδου, είναι πιθανό να τύχει να χρησιμοποιήσεις μαζί, τους δικούς του διαμεσολαβητές, οπότε να καταφέρει να σε ταυτοποιήσει. Επειδή όμως στατιστικά είναι πολύ μικρή η πιθανότητα να λειτουργήσει αποτελεσματικά κάτι τέτοιο με λίγους διαμεσολαβητές, χρειάζεται να καταληφθεί περίπου το ένα τρίτο του δικτύου. Στην πράξη δεν υπάρχουν ενδείξεις για παρόμοιο εγχείρημμα.

3. Επίθεση στην κρυπτογραφία: Το σπάσιμο των κωδικών είναι ζήτημα υπολογιστικής ισχύος. Οι υπερυπολογιστές που υπάρχουν σήμερα δεν επαρκούν για την αποκρυπτογράφηση, όμως οι ροές καταγράφονται από την NSA (National Security Agency) και πιθανόν άλλες μυστικές υπηρεσίες και κάποια στιγμή στο μέλλον θα τις αποκρυπτογραφήσουν. Ότι μεταφέρουμε σήμερα, η θέση και η ταυτότητά μας θα αποκαλυφθεί στο μακρινό μέλλον. Τότε όμως θα έχει εξελιχθεί και το tor. Ήδη συζητιέται στην κοινότητα ανάπτυξης του tor ο διπλασιασμός του μεγέθους των κωδικών κρυπτογράφησης.

4. Επίθεση άρνησης εξυπηρέτησης: Αρκετά διαδεδομένη στο ίντερνετ (denial of service, dos). Ουσιαστικά είναι η υπερφόρτωση ενός σέρβερ από μαζικές αιτήσεις που γίνονται αυτόματα από προγράμματα γι αυτό το σκοπό (bots), ώστε να μην μπορεί να λειτουργήσει. Τελευταία το δίκτυο του tor δέχεται τέτοιου είδους επιθέσεις, με αποτέλεσμα να παρουσιάζει πρόβλημα στην χρηστικότητά του καθώς σέρνεται. Δεν πρόκειται όμως για αποκάλυψη της ανωνυμίας.
Μπορεί όμως θεωρητικά να χρησιμοποιηθεί συνδυαστικά με την κατάληψη μέρους του δικτύου, διοχετεύοντας επιθέσης άρνησης εξυπηρέτησης στοχευμένα ενάντίον των υπόλοιπων διαμεσολαβητών ώστε να αναγκαστεί ο χρήστης να συνάψει κύκλωμα με τους διαμεσολαβητές υποκλοπείς.

5. Επίθεση σε περιφερειακό του tor λογισμικό: Όπως είδαμε παραπάνω, εάν ο υπολογιστής του χρήστη είναι παγιδευμένος με κατασκοπευτικό λογισμικό, κανένα δίκτυο ανωνυμίας δε σε προστατεύει. Οπότε ο υπολογιστής πρέπει να είναι καθαρός. Το κυριότερο αν είσαι στόχος παρακολούθησης είναι η επιλογή του λειτουργικού συστήματος.
Όμως υπάρχουν και άλλα υποσυστήματα με τα οποία συνεργάζεται το tor και από τα οποία μπορεί να προδοθείς. Για παράδειγμα το υποσύστημα DNS (Domain Name System, το σύστημα που μεταφράζει τις διευθύνσεις των ιστοσελίδων τύπου www.xxxxxxx.xxx στις κατάλληλες IP διευθύνσεις των σελίδων), πριν ενσωματωθεί στο tor, ζητούσε κανονικά τις σελίδες που επισκεπτόμασταν μέσω tor, με αποτέλεσμα κάποιος που μας παρακολουθεί να μπορεί να συναγάγει ποιές σελίδες επισκεφθήκαμε (όχι όμως τί κάναμε). Πλέον το tor έχει καλύψει αυτήν την τρύπα ασφαλείας περνόντας τα αιτήματα DNS μέσα από το δίκτυό του.
Πάντως αν μαζί με το tor χρησιμοποιείς ελαττωματικό λογισμικό και μία ισχυρή αστυνομική υπηρεσία όπως το FBI ή η NSA θέλει να σε εντοπίσει, είσαι ευάλωτος. Μία τέτοια περίπτωση είναι οι πρόσφατη σύλληψη από το FBI ενός διακινητή παιδικής πορνογραφίας. Στην περίπτωση αυτή, χάκαραν κάποιες .onion ιστοσελίδες (μεταξύ των οποίων και το δημοφιλές tormail) , ώστε όταν εκτελέσουν κακόβουλο κώδικα όταν ανοίξουν στον tor-browser **για windows**, και να στείλουν σήμα εκτός του tor δικτύου, σε κάποιο σέρβερ των μπάτσων στη Βιρτζίνια ώστε να εντοπισουν τους χρήστες. Για να σπάσει δηλαδή το FBI την ισχυρή ανωνυμία που προσφέρει το tor-network, εκμεταλλεύτηκαν συνδυασμό από αδυναμίες στο περιφερειακό του tor λογισμικό tor-browser, στην ελαττωματική υποδομή ασφαλείας του λειτουργικού συστήματος ms windows, και στις ιστοσελίδες που χάκαραν. Έτσι αρκετοί χρήστες του tor αποκαλύφθηκαν όταν έλαβε χώρα η επίθεση. Όχι όλοι όμως. Όσοι δεν επισκέφθηκαν τις χακαρισμένες σελίδες δεν προσβλήθηκαν. Επίσης, όσοι χρησιμοποιούσαν άλλο λειτουργικό σύστημα (macos ή gnu linux) επίσης δεν έπαθαν τίποτα. Άμεσα κυκλοφόρησε ανανεωμένη έκδοση του tor-browser για windows που διόρθωνε αυτήν την αδυναμία. Το μεγαλύτερο πλήγμα απ' αυτήν την επίθεση, ήταν στην υπόληψη του tor-project, που είχε ως αποτέλεσμα πολλοί χρήστες του λόγω άγνοιας να στραφούν σε πιο επισφαλείς λύσεις ανωνυμίας, με τη συνακόλουθη μείωση της χαοτικότητας του, που είναι και η πηγή της δύναμής του.
Σημείωση: Συνδυασμοί όλων των παραπάνω μορφών επίθεσης στην ανωνυμία του tor συζητιούνται θεωρητικά με σκοπό τη θωράκισή του από υποθετικές επιθέσεις στο μέλλον.

ΘΩΡΑΚΙΣΗ ΤΗΣ ΑΝΩΝΥΜΙΑΣ ΣΤΗΝ ΠΡΑΞΗ

Tor browser bundle

Στην ιστοσελίδα του tor προσφέρονται διάφορα προγράμματα-εργαλεία για κάθε χρήση του tor network και για όλα τα διαδεδομένα λειτουργικά συστήματα. Το πιο δημοφιλές και εύχρηστο εργαλείο είναι το tor-browser bundle, ένα πακέτο προγραμμάτων που περιλαμβάνει το **vidallia** που πραγματοποεί αυτόματα την κατάλληλη ρύθμιση του υπολογιστή, τη σύνδεση στο tor και τον tor-browser για σερφάρισμα διασφαλίζοντας την ανωνυμία, με την προυπόθεση ότι γίνεται ευφυής χρήση (δεν συνδέεσαι για παράδειγμα στο λογαριασμό σου στο facebook με τα πραγματικά σου στοιχεία). Ο browser που χρησιμοποιείται στο bundle είναι ο firefox με επιπρόσθετες ρυθμίσεις ανωνυμίας και με προεγκατηστεμένο το πρόσθετο noscript που απογορεύει την εκτέλεση κώδικα απ' τις ιστοσελίδες, ώστε να αποφευχθούν επιθέσεις όπως η **5**. Ο χρήστης μπορεί αν θέλει να άρει τον αποκλεισμό για τις σελίδες που εμπιστεύεται. Όταν έγινε η επίθεση που περιγράψαμε παραπάνω, η προεπιλεγμένη πολιτική απαγόρευσης του noscript είχε "χαλαρώσει" ώστε να γίνει πιο χρηστικό. Η επίθεση λειτούργησε μόνο στα windows αλλά στο μέλλον πιθανό να μεταφερθεί και σε mac, android, και κάποιες linux πλατφόρμες.

T.A.I.L.S.

Υπάρχει όμως μία διανομή linux που ήταν είναι και οπως δείχνουν όλα θα παραμείνει **απρόσβλητη** σε τέτοιου είδους επιθέσεις: Το **T.A.I.L.S. (The Amnestic Incognito Live System), 100% ελεύθερο λογισμικό.** Τη συγκεκριμένη διανομή, την βρίσκεις ακολουθώντας link από το site του tor, την κατεβάζεις, την καις σε cd, και bootάρεις τον υπολογιστή σου σ' αυτήν. Τρέχει χωρίς εγκατάσταση, και δεν αφήνει ίχνη στον σκληρό δίσκο σου (είναι το ιδανικό σύστημα για αναλήψεις ευθύνης και άλλες παράνομες δραστηριότητες).

Είναι ρυθμισμένη ώστε να μην επιτρέπει συνδέσεις εκτός του δικτύου tor και εκεί έγκειται και η θωράκισή της. Οπότε είναι εντελώς μη χρηστική για κανονικό σερφάρισμα, αλλά παντοδύναμη όσον αφορά την ανωνυμία, με περιοριστικά πρόσθετα όπως το noscript να είναι σχεδόν άχρηστα. Το σημαντικότερο, **είναι σχεδόν αδύνατη η εγκατάσταση spyware.**

Επίσης διαθέτει και άλλα όμορφα χαρακτηριστικά όπως metadata cleaner, ένα πρόγραμμα που σβήνει τα metadata (δεδομένα που ενσωματώνονται στα αρχεία και δείχνουν ώρα και ημερομηνία κατασκευής όπως και στοιχεία του υπολογιστή στον οποίο κατασκευάστηκαν) από προυπάρχοντα αρχεία, απαραίτητο αν θες να στείλεις ανώνυμα κάποιο αρχείο σου (π.χ. pdf).

Άλλες περιπτώσεις εσφαλμένης χρήσης απ' τις οποίες το t.a.i.l.s. σε προστατεύει αποτελεσματικά είναι το άνοιγμα αρχείων που κατέβηκαν μέσω tor και ανοίγουν σε εξωτερικές εφαρμογές και μπορεί να τρέξουν σε αυτές κακόβουλο κώδικα που σε ταυτοποιεί. Στο tails αυτό δεν μπορεί να συμβεί καθώς δεν επιτρέπονται μη tor συνδέσεις από το firewall.

Σημείωση:

Καλό είναι αν θέλουμε να μην μπορούν οι μπάτσοι να συνδέσουν διάφορες δραστηριότητές μας, **να αλλάζουμε ταυτότητα**, δηλαδή τη διαδρομή εντός του tor που ακολουθεί η επικοινωνία μας. Αυτό γίνεται με το πάτημα ενός κουμπιού, το οποίο στον tor-browser καθαρίζει και τα cookies. Αν χρησιμοποιούμε άλλο browser, βρίσκουμε το κουμπί αυτό στο vidalia και καθαρίζουμε χειροκίνητα τα cookies κάθε φορά που αλλάζουμε ταυτότητα, ενώ καλό είναι να αλλάζουμε με κάποιο πρόσθετο τον browser id (στον tor-browser είναι πάντα και σε όλους τους χρήστες ίδιος, ώστε να μην ξεχωρίζουν μεταξύ τους, όμως φαίνεται ότι χρησιμοποιούμε tor).

Λοιπές επιθέσεις

Από τη μεγάλη γκάμα των επιθέσεων σε περιφερειακό λογισμικό το tails μας προστατεύει αποτελεσματικά. Τί γίνεται όμως με τις υπόλοιπες επιθέσεις; Η επίθεση στην κρυπτογραφία δεν μας αγγίζει, στο βαθμό που όταν κάποιος βρει τον τρόπο να τη σπάσει θα προτιμήσει να κατακτήσει τον κόσμο παρά να αναζητήσει εμάς. Τις επιθέσεις άρνησης εξυπηρέτησης είμαστε αναγκασμένοι να τις υπομείνουμε, με όλη την καθυστέρηση που εισάγουν, πλην όμως να μην συμβάλλουν στην αποκάλυψη της ταυτότητάς μας από κατειλημμένους relay servers. Βέβαια η θωράκιση που δημιουργεί η διαχειριστική ομάδα του tor αποδεικνύεται ισχυρή εφόσον δεν γνωρίζω κάποια περίπτωση όπου κάποιος αποκαλύφθηκε έτσι. Και ακόμα και αν η NSA π.χ. καταφέρει κάτι τέτοιο θα προτιμήσει μάλλον να το αξιοποιήσει η ίδια και όχι να το μοιραστεί με την ελληνική αντιτρομοκρατική.

Ταυτοποίηση κίνησης

Η ταυτοποίηση κίνησης όμως είναι ένα ξεχωριστό κεφάλαιο. Αν και δύσκολη παραμένει στη σφαίρα του εφικτού. Το αντίμετρό μας όπως είδαμε είναι η εισαγωγή χαοτικών δεδομένων. Ένας απλός τρόπος να το κάνουμε αυτό είναι να ανοίξουμε μια νέα καρτέλα στον tor-browser και να συνδεθούμε σε κάποια .onion σελίδα. Στη συνέχεια κατεβάζουμε το πρόσθετο reloadevery, που κάνει αυτόματες ανανεώσεις στο χρόνο που θα του ορίσουμε. Αφού το εγκαταστήσουμε το βρίσκουμε στο μενού του δεξί κλικ. Στη συνέχεια επιστρέφουμε στην αρχική καρτέλα και σερφάρουμε, χωρίς να κλείσουμε τη σελίδα με τις αυτόματες ανανεώσεις η οποία γεμίζει την επικοινωνία μας με τον κόμβο εισόδου χαοτικά δεδομένα, χωρίς να αυξάνει αντίστοιχα τον όγκο των δεδομένων στον κόμβο εξόδου, αφού οι .onion σελίδες βρίσκονται μέσα στο δίκτυο tor. Τη μέθοδο αυτή μπορείτε να βελτιστοποιήσεται αν ξέρετε προγραμματισμό φτιάχνοντας ένα σκριπτάκι που εναλάσσει τις σελίδες αυξάνοντας τη χαοτικότητα.

Το tor βέβαια για να μην επιβαρύνεται αντιπροτείνει έναν άλλον τρόπο ειδσαγωγής χαοτικών δεδομένων: να γίνεις κι εσύ relay server, πράγμα που γίνεται με μια απλή ρύθμιση στο vidalia (βέβαια αυτό απαιτεί μια σχετικά γρήγορη σύνδεση δικτύου). Έτσι ενισχύεις το δίκτυο με τη συμμετοχή σου ενώ ταυτόχρονα στην επικοινωνία σου με τους κόμβους εισόδου (και εξόδου για τις συνδέσεις αλλονών), φαίνεται ασύγκριτα μεγαλύτερη κίνηση από αυτή στον κόμβο εξόδου σου.

Η σημασία του ρολογιού

Κάτι που παραλείψαμε να επισημάνουμε είναι το πρόβλημα των χρονοσφραγίδων (timestamps). Κάθε πακέτο δεδομένων που μεταδίδεται στο ίντερνετ κουβαλάει σκτός απ' τη διεύθυνση του αποστολέα και του παραλήπτη την ακριβή ώρα κατασκευής του. Οπότε μία εσφαλμένη ρύθμιση του ρολογιού σου πιθανόν να σε αποκαλύψει αφού θα αποτελεί χαρακτηριστικό σου. Αν η απόκλιση είναι μικρή, υπάρχει ένας μικρός κίνδυνος, αν η απόκλιση είναι μεγάλη, το tor θα αποτύχει να αρχικοποιηθεί και το vidalia θα σου βγάλει μήνυμα ότι "η σύνδεση απέτυχε, τσέκαρε το ρολόι σου".

Μήπως με στοχοποιεί η ίδια η χρήση του tor;
Εύλογο ερώτημα, εφόσον όπως είπαμε το λογισμικό του tor δεν κρύβει ότι το χρησιμοποιείς, κρύβει μόνο το τί κάνεις μέσα απ' αυτό. Η αλήθεια είναι πως απ' όλα τα λογισμικά ανωνυμίας είναι το λιγότερο ύποπτο λόγω της ευρείας διάδοσής του. Στην Ελλάδα 500 με 1000 χρήστες την ημέρα το τιμούν με την παρουσία τους, όπως έδειχναν οι στατιστικές πριν αρχίσουν οι μαζικές επιθέσεις άρνησης εξυπηρέτησης που εκτινάσσουν τα νούμερα υπερβολικά.
Μία πιθανή εσφαλμένη χρήση είναι να πηγαίνεις σε κάποιο νετ καφέ για κάποιο λόγο στοχοποιημένο (π.χ. εξάρχεια), να επισκέπτεσαι σαν κύριος την ιστοσελίδα του tor και να το κατεβάζεις, δηλώνοντας στους σερβερ των μπάτσων που το παρακολουθούν οτί κάποιος στο νέτ χρησιμοποιεί tor. Συνίσταται ο tor-browser να βρίσκεται αποθηκευμένος σε στικάκι και όχι να κατεβαίνει εκ νέου κάθε φορά. Ακόμα κι έτσι όμως, χωρίς να μπεις στη σελίδα του tor, η κίνηση του τορ μπορεί να γίνει ανιχνεύσιμη, οπότε δεν είναι 100% ασφαλές ότι δε θα φανεί ότι το χρησιμοποιείς.

Στην πράξη
Όμως υπάρχουν πολύ πιο πρακτικές λύσεις, π.χ. σηκώνεις το λάπτοπ σου, πας σε κάποιο απ' τα αμέτρητα ξεκλείδωτα wi-fi της πόλης, π.χ. μία καφετέρια και τρέχεις ένα cd με την **τελευταία έκδοση του T.A.I.L.S**. Καλό είναι να αλλάξεις και τη mac address, το tails διαθέτει αντίστοιχο εργαλείο. Με την τελευταία περίπτωση, έχουμε το μέγιστο δυνατό βαθμό ανωνυμίας με απλά μέσα και είμαστε καλυμμένοι απέναντι στις υπαρκτές επιθέσεις στην ανωνυμία μας (όχι στις θεωρητικές-υποθετικές), εκτός από την ταυτοποίηση κίνησης, ενάντια στην οποία μπορεί να χρησιμοποιήσουμε τη λύση που προτείναμε πιο πάνω ή να τρέξουμε ένα relay server.

Ιδιωτικότητα
Όπως είδαμε οι κόμβοι εξόδου του tor πιθανόν να υποκλέπτουν. Γι αυτό το λόγο στο σερφάρισμα χρησιμοποιούμε https, που εγκαθιδρύει κρυπτογραφημένη επικοινωνία με τις ιστοσελίδες.
Για επικοινωνία, καλύτερα να χρησιμοποιούμε το πρόγραμμα για chat **pidgin** που βρίσκεται ενσωματωμένο και στο tails, με το πρόσθετο **OTR** που παρέχει πανίσχυρη κρυπτογράφηση και καθιστά την επικοινωνία μας πραγματικά απόρρητη (όλα αυτά είναι ελεύθερο λογισμικό). Εναλλακτικά, υπάρχει το chatcrypt.com, ένα site που παρέχει αυτόματη κρυπτογράφηση η οποία εκτελείται με κώδικα σε γλώσσα javascript στον browser σου ώστε ούτε το ίδιο το site να μπορεί να διαβάσει την επικοινωνία σου. Δεν είναι ελεύθερο λογισμικό όμως μπορείς να διαβάσεις τον κώδικα javascript.

ΕΠΙΛΟΓΟΣ: Ο ΠΟΛΕΜΟΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Η γέννηση των ηλεκτρονικών υπολογιστών είναι συνυφασμένη με τον πόλεμο και την κατασκοπεία. Ο άνθρωπος ο οποίος συνέλαβε την ιδέα μιας προγραμματιζόμενης μηχανής, που μπορεί να εκτελέσει κάθε αλγόριθμο, ακόμα και να προσομοιώσει την ανθρώπινη νοημοσύνη, ήταν ο επικεφαλής κρυπταναλυτής των Βρεττανικών μυστικών υπηρεσιών, κατά τη διάρκεια του 2ου παγκοσμίου. Το όνομά του ήταν Alan Turing και η δουλειά του ήταν να σπάει τις κρυπτογραφήσεις των Ναζί, που χρησιμοποιούσαν μία αυτόματη κρυπτογραφική μηχανή, που ονομαζόταν ENIGMA.

Οι Γερμανοί εμπιστεύονταν τυφλά την μηχανή αυτή, και η βρεττανικές υπηρεσίες κρατούσαν επτασφράγιστο μυστικό οτί την είχαν σπάσει. Για να μην κλονίσουν την εμπιστοσύνη των Ναζί στη μηχανή τους, άφηναν τα Γερμανικά υποβρύχια να βυθίζουν αύτανδρα τα Βρεττανικά πλοία. Τελικά οι Γερμανοι έχασαν το προβάδισμα στον πόλεμο και σημαντικές υποκλαπείσες πληροφορίες συνέβαλλαν στη συντριβή τους.
Ένα εύλογο ερώτημα είναι πως μπορούμε να εμπιστευτούμε οποιαδήποτε κρυπτογράφηση και οποιαδήποτε ανωνυμία; Η σύντομη απάντηση είναι οτί δεν μπορούμε. Σίγουρα όχι τυφλά. Όπως λέει και η σελίδα chatcrypt, για πραγματική ιδιωτικότητα βλέπεις το συνομιλητή σου από κοντά και βγάζεις την μπαταρία του κινητού σου.
Η μακροσκελής απάντηση ορίζει τη συνθήκη της εμπιστοσύνης. Στην αυγή της ασύμμετρης κρυπτογραφίας, οι κρυπτογράφοι έκλεψαν το πλεονέκτημα απ' τους κρυπταναλυτές. Γύρω στο 1977, το μοντέλο της καινοτομίας στην κρυπτογραφία άλλαξε, όταν τρεις πανεπιστημιακοί ερευνητές στο MIT, ο Rivest, ο Shamir και ο Adleman εφηύραν τον αλγόριθμο κρυπτογράφησης RSA. Μερικά χρόνια νωρίτερα το 1973, ο Clifford Cocks των Βρεττανικών μυστικών υπηρεσιών, είχε εφεύρει τον ίδιο αλγόριθμο, αλλά οπως αποκάλυψε πολύ αργότερα δεν κατάφερε να τον υλοποιήσει λόγω των περιορισμένων πόρων σε ανθρώπινο δυναμικό που επιβάλλει το καθεστώς απόρρητων ερευνών. Πλέον ο κόσμος είχε γίνει συνθετότερος. Η τεχνολογία δεν μπορεί να παραχθεί στα περιορισμένα μυστικά προγράμματα των μυστικών υπηρεσιών, χρειάζεται μεγάλα πλήθη ανθρώπων να συνεργάζονται. Γι αυτό και αυτή η καινοτομία αναπτύχθηκε τελικά σε ένα πανεπιστήμιο, γι αυτό και το πρόγραμμα DARPA άνοιγε τα ερυνητικά του έργα, όπως το ίντερνετ στα πανεπιστήμια. Γι αυτό και δεν μπορεί πλέον σε τόσο σύνθετα έργα να αντιπαρατεθεί μία ιδιοφυία που δουλεύει μυστικά.
Από αυτό συναγάγουμε και άλλα χρήσιμα συμπεράσματα. Εφ' όσον ο κόσμος της τεχνολογίας δεν μπορεί να ανήκει σε μία μικρή ομάδα, η απειλή ενός ολοκληρωτισμού που επιβάλλεται **από** την τεχνολογία, δεν είναι υπαρκτή. Αντίθετα υπάρχει ένας ολοκληρωτισμός που επιβάλλεται **με** την τεχνολογία. Δεν είναι παρά η ίδια η εξουσιαστική κοινωνία που αναδιοργανώνεται στη βάση της τεχνολογίας που παράγει, που φυσικά δεν είναι ουδέτερη.
Όμως η τεχνολογία χρειάζεται τα δικά της "εργατικά χέρια", και μ' αυτήν την έννοια όπως κάθε εργοστασιάρχης εξαρτάται απ' τους εργάτες του, έτσι κάθε εξουσιαστής που ελέγχει τον κόσμο μέσω της τεχνολογίας εξαρτάται από το σύνολο των τεχνικών υφισταμένων του. Ακόμα η συναίνεση παίζει καθοριστικό ρόλο στην επιβολή της εξουσίας. Η πυραμίδα λοιπόν μπορεί ακόμα να ανατραπεί, χρειάζεται όμως συνείδηση και γνώση συνολική, όχι μόνο τη μερική της εξειδίκευσης που κάνει τον άνθρωπο εργαλείο. Η αντίσταση λοιπόν είναι ακόμα εφικτή. Έχουμε ακόμα τη δύναμη, άρα και την ευθύνη ν' ανατρέψουμε τις εξουσίες.
Η γνώση είναι δύναμη και με αυτό κατά νου αποπειράθηκα να εξηγήσω τους όρους διεξαγωγής του κυβερνοπολέμου, γνωρίζοντας ότι η δυσκολία θα είναι αποτρεπτική για πολλούς που θα προσπαθήσουν να διαβάσουν το κείμενο. Χρειάζεται να εμβαθύνουμε στο πως δουλεύει αυτός ο κόσμος για να καταφέρουμε να τον καταστρέψουμε.

Γιάννης Μιχαηλίδης,
φυλακές Κορυδαλλού

Το κείμενο, ήταν συνέχεια του γράμματος των αναρχικών Αργύρη Ντάλιου, Φοίβου Χαρίση, Γιάννη Ναξάκη και Γρηγόρη Σαραφούδη, γύρω από λάθη και παραλείψεις που οδήγησαν στη σύλληψή τους, ώστε να αποφευχθούν από συντρόφους που συνεχίζουν τον αγώνα.