Συλλογή κειμένων
για την αντιμετώπιση της καταστολής.

Η μπροσούρα είναι αφιερωμένη στους συντρόφους

Φοίβο Χαρίση

Αργύρη Ντάλιο

Νίκο Ρωμανό

Αντρέα-Δημήτρη Μπουρζούκο

Γιάννη Μιχαηλίδη

Δημήτρη Πολίτη

που δικάζονται από τις 29 Νοέμβρη για τη διπλή απαλλοτρίωση ελτα-τράπεζας

στο Βελβεντό

Πάτρα, Νοέμβρης 2013

Εγχειρίδιο σε περίπτωση σύλληψης...

ΓΕΝΙΚΑ

1. Βασική επιδίωξη της ανάκρισης [είτε γίνεται από την αστυνομία, είτε γίνεται από τον δικαστή] είναι να συλλέξει όσα περισσότερα στοιχεία γίνεται για το ποιος είσαστε, τι κάνετε, για το κάθε τι που θα μπορούσε να ενοχοποιήσει εσάς ή κάποιον άλλο. Θεωρητικά βέβαια, η ανάκριση έχει σκοπό να αποδείξει την ενοχή ή την αθωότητα σας. Η πράξη όμως, έχει αποδείξει πως την αστυνομία πολύ λίγο την ενδιαφέρει η δεύτερη περίπτωση.

2. Η αστυνομία μπορεί να ενεργεί όλες τις ανακριτικές πράξεις και χωρίς εισαγγελική παραγγελία, όταν πρόκειται για αυτόφωρο έγκλημα ή όταν υπάρχει κίνδυνος από την αναβολή να χαθούν τα ίχνη κάποιου εγκλήματος. Σημαντικό είναι, ότι ο αστυνομικός κρίνει αν υπάρχει κίνδυνος από την αναβολή, οπότε η αστυνομία έχει πάντα το δικαίωμα της ανάκρισης.
Σύμφωνα με τις διατάξεις του κώδικα ποινικής δικονομίας, αυτοί που μπορούν να κάνουν ανάκριση, είναι ο δικαστής και ο αστυνομικός. Για να γίνει η ανάκριση, πρέπει ο εισαγγελέας να εκδώσει ένα έγγραφο που να απευθύνεται στον τακτικό ανακριτή ή στους αστυνομικούς και να τους εξουσιοδοτεί να κάνουν ανάκριση για μια συγκεκριμένη πράξη. Αυτό, βέβαια, δεν ισχύει στις δύο παραπάνω περιπτώσεις.

3. Όταν ανακρίνεστε, πρέπει να βρίσκεστε διαρκώς σε εγρήγορση. Δεν πρέπει να είστε αφελής και να πιστέψετε ότι καταθέτοντας στον ανακριτή θα αποδείξετε την αλήθεια, ότι θα σας καταλάβουν, ότι θα τα καταφέρετε. Οι καλές ανακρίσεις -για εσάς- είναι αυτές που δεν περιέχουν τίποτα. Εκείνες που δεν δίνουν καμία πληροφορία για κανέναν. Σκοπός της ανάκρισης -για αυτούς- είναι να συλλέξει όσο το δυνατόν περισσότερες πληροφορίες μπορεί για το άτομο σας, για τους αγώνες που συμμετέχετε, τα μέσα που χρησιμοποιείτε. Και όχι μόνο για εσάς, αλλά και για τους φίλους σας, για όλους εκείνους που αγωνίζονται μαζί σας. Μην τους "προσφέρεστε", μην τους δείξετε καμία οικειότητα. Όχι μόνο δεν πρέπει να λέτε τίποτα, αλλά πρέπει να είστε ερμητικά κλειστοί. Μην μπερδέψετε όμως, την άρνηση απάντησης με μια άσκοπη επιθετικότητα, που θα ανεβάσει τους τόνους χωρίς λόγο. Μην ξεχνάτε ότι παίζετε στο γήπεδο τους. Η

ψυχραιμία, η αποφασιστικότητα και η ξεκάθαρη άρνηση συνεργασίας, είναι η απάντηση στη βία και τις απειλές τους, στις υποσχέσεις και τα ψέματα τους.

ΑΝΑΚΡΙΣΗ ΑΠΟ ΤΗΝ ΑΣΤΥΝΟΜΙΑ

1. Όταν σας ανακρίνει η αστυνομία, το πρώτο σας μέλημα είναι να μάθετε ποια είναι η θέση σας: αν είστε μάρτυρες, κατηγορούμενοι ή ύποπτοι, αν δηλαδή υπάρχουν ενδείξεις εναντίον σας για κάποια παράνομη πράξη.

2. Αν σας ανακρίνουν ως ύποπτους ή κατηγορούμενους, απαιτείστε αμέσως την παρουσία του δικηγόρου σας. Παλιά αυτό το ξέραμε ως δικαίωμα από τις αμερικάνικες ταινίες και είναι αλήθεια ότι δεν το έγραφε ξεκάθαρα ο νόμος, τώρα όμως, με τη συμφωνία του Σένγκεν είναι δικαίωμα του κατηγορουμένου. Απαιτείστε το και επικοινωνήστε με κάποιον δικηγόρο ή με κάποιον που είστε σίγουροι ότι θα τον ειδοποιήσει. Το πιο καλό είναι, να τηλεφωνήσετε σε κάποιον, που θα ενημερώσει τόσο τον δικηγόρο σας, όσο και τους στενούς σας συντρόφους. Να θεωρείτε δεδομένο, ότι η αστυνομία θα εντοπίσει αυτόν που καλέσατε. Πρέπει δηλαδή, να συνυπολογίσετε αυτό το γεγονός στην απόφαση σας, με ποιον θα επικοινωνήσετε. Ανάλογα με την υπόθεση μπορεί να τον προσαγάγουν, ώστε να καταθέσει ή ακόμα να ερευνήσουν και το σπίτι του. Το καλύτερο θα ήταν να έχετε συνεννοηθεί από πριν με κάποιον φίλο σας, όσον αφορά το δικηγόρο που θέλετε, το άτομο που θα σας επισκέπτεται όσο κρατήστε, τις κινήσεις αλληλεγγύης που επιθυμείτε και με αυτόν να επικοινωνήσετε. Το τηλεφώνημα πρέπει να είναι γρήγορο και συνοπτικό, χωρίς να παραδέχεστε τίποτα [μπορεί να καταγράφεται και να χρησιμοποιηθεί εναντίον σας]. Για παράδειγμα, "Με συλλάβανε μόνο μου, στις 10.15 το βράδυ, στην Ιπποκράτους, κατηγορώντας με ότι είχα μια τσάντα με τρεις μολότοφ. Είμαι στο πέμπτο αστυνομικό τμήμα, στα Εξάρχεια. Μου έχουν δώσει την έκθεση σύλληψης, την οποία δεν έχω υπογράψει και μου πήραν απολογία, στην οποία δεν έχω πει τίποτα. Πάρε τον τάδε δικηγόρο, να έρθει αμέσως." Εκμεταλλευτείτε το, όσο καλύτερα γίνεται. Αν δεν σας απαγορέψουν δεύτερο, μην το αφήσετε χαμένο. Η εμπειρία, πάντως έχει δείξει ότι οι αστυνομικοί σας επιτρέπουν να τηλεφωνήσετε, πολύ μετά τη σύλληψη σας. Για να έχουν τον χρόνο να σας πρεσάρουν και να σας έχουν πάρει κατάθεση. Χωρίς να τους πιέζει η παρουσία του δικηγόρου σας.
Αν σας αρνηθούν την παρουσία και την βοήθεια δικηγόρου, ενισχύστε την άρνηση σας να απαντήσετε στις ερωτήσεις τους. Θα έχετε ένα επιχείρημα που θα ακούγεται πιο λογικό στα αυτιά τους. Θα τους εκνευρίζετε λιγότερο, όταν θα απαντάτε "δεν καταθέτω χωρίς το δικηγόρο μου" [πράγμα που δεν ισχύει, αφού ακόμα και με την παρουσία δικηγόρου δεν θα απολογηθείτε στην αστυνομία, αλλά θα περιμένετε το δικαστήριο ή τον ανακριτή], αντί να τους λέτε "δεν απαντάω σε καμία ερώτηση".

3. Στην περίπτωση που είστε κατηγορούμενοι, η στάση είναι μια. Δεν απαντάται σε καμία ερώτηση, δεν υπογράφεται τίποτα. Δεν ισχύει το: στους μπάτσους μιλάμε μεν, προσέχουμε τι λέμε δε. Αν αρχίσετε να τους λέτε παραμύθια πολύ δύσκολα δεν θα πέσετε σε αντιφάσεις. Να θυμάστε, οι ανακριτές είναι ειδικοί στο να σας κάνουν να μπερδευτείτε.
Σε περίπτωση σύλληψης και απαγγελίας κατηγοριών, κεντρική συμβουλή που πρέπει να διέπει όλη τη στάση σας, είναι η σιωπή σε οποιαδήποτε προσπάθεια των αστυνομικών να σας προσεγγίσουν. Μην απαντάτε σε άλλη ερώτηση πέρα των στοιχείων της ταυτότητας σας [π.χ. ούτε καν αν έχετε αδέλφια, που εργάζεστε κλπ] και γενικά διατηρήστε μια αποστασιοποιημένη στάση [αρνηθείτε κέρασμα καφέ κλπ]. Ακόμα και αν κρίνετε ότι κάτι μπορεί να διευκολύνει τη θέση σας, έχετε κάθε χρονικό περιθώριο να το καταθέσετε αργότερα, αφού θα έχετε μιλήσει με τους συντρόφους σας και το δικηγόρο σας. Μην υπογράψετε κανένα έγγραφο [έκθεση σύλληψης, προανακριτική κατάθεση κλπ]. Όσο κουρασμένοι και αν είσαστε, κι ακόμη κι αν η υπογραφή αυτή σας παρουσιαστεί ως τυπική διαδικασία, θα πρέπει να θυμόσαστε ότι σημασία για το δικαστήριο έχουν αποκλειστικά τα έγγραφα της δικογραφίας.
Βέβαια, η αλήθεια είναι, ότι το να μη λέτε τίποτα συνήθως σημαίνει ότι τους τσαντίζετε και μπορεί να αρχίσουν να σας χτυπάνε. Καλύτερα Βέβαια το ξύλο που κάποια στιγμή θα σταματήσει, παρά μια προφυλάκιση, μια καταδίκη ή μια μεγάλη ποινή. Μια καλή τακτική είναι αντί να φωνάζεις: "δεν πρόκειται να πω τίποτα" ή "δεν

πρόκειται να συνεργαστώ" και άλλα τέτοια, να λες κάτι διπλωματικότερο του τύπου "αρνούμαι όλες τις κατηγορίες και δεν έχω τίποτα να προσθέσω. Αρνούμαι να υπογράψω. Ό,τι έχω να πω, θα το πω στην κύρια ανάκριση και ενώπιον του δικαστηρίου, παρουσία του δικηγόρου μου". Αυτό μερικές φορές πιάνει, γιατί ο αστυνομικός που κάνει την προανάκριση, πολλές φορές θέλει απλώς να τελειώνει, οπότε έτσι γράφει αυτά τα λίγα και ξεμπερδεύει.
Μην νομίζετε ότι γενικώς μπορείτε να πείτε ό,τι θέλετε και στο τέλος, αν δεν σας αρέσουν αυτά που είπατε, απλώς να μην υπογράψετε. Ακόμα και αν γίνει έτσι, μπορούν να βεβαιώσουν οι αστυνομικοί τον ανακριτή ή το δικαστήριο, ότι η προανάκριση ολοκληρώθηκε κανονικά και ότι εσείς, απλώς δεν βάλατε υπογραφή, οπότε αυτό θα εκτιμηθεί από το δικαστήριο.
Να έχετε πάντα κατά νου, ότι στο ακροατήρια φράσεις του στυλ: "δεν τα είπα έτσι στην ανάκριση, αλλά έτσι τα γράψανε" δεν ασκούν και μεγάλη επιρροή στην αξιοπιστία του ανακριτικού υλικού.

4. Κάποια στιγμή, θα προσπαθήσουν να σας πάρουν το γραφικό σας χαρακτήρα. Για αυτό το σκοπό θα σας δώσουν ένα ειδικό έντυπο και θα σας πουν να γράψετε ό,τι θέλετε. Αρνηθείτε να γράψετε οτιδήποτε. Μπορεί -τώρα ή στο μέλλον- να ταυτοποιήσουν χειρόγραφα κείμενα με τον γραφικό σας χαρακτήρα, για να στηρίξουν κατηγορίες.

5. Στο αστυνομικό τμήμα, μπορούν να σας αφαιρέσουν όλα τα κινητά αντικείμενα [π.χ. ραλόι, κινητό, χρήματα, κλειδιά]. Απαιτήστε να συνταχθεί σχετικός κατάλογος. Ζητήστε το έντυπο με τα δικαιώματα σου. Αν είσαι γυναίκα, απαίτησε να σου γίνει σωματική έρευνα από γυναίκα αστυνομικό. Είναι παράνομο να γίνει από άντρα.

ΤΕΧΝΙΚΕΣ ΤΗΣ ΑΝΑΚΡΙΣΗΣ

1.Η αστυνομία ξέρει πάντα, πολύ λιγότερα από αυτά που υποκρίνεται πως ξέρει. Όπως είδατε και παραπάνω, η αστυνομία θα μπορούσε να σας ανακρίνει ως μάρτυρες, ως υπόπτους ή ως κατηγορούμενους. Θα θέλουν να σας κάνουν να πιστέψετε, ότι κάθε μέσο που χρησιμοποιούν για να σας κάνουν να μιλήσετε είναι νόμιμο. Θα σας κάνουν επίδειξη δύναμης και εξουσίας. Η απειλή να ενοχοποιήσουν εσάς ή κάποιους συντρόφους σας, είναι ένα μέσο να σας κάνουν να πείτε αυτά που δεν ξέρουν. Θα σας απειλήσουν με δίωξη για άρνηση κατάθεσης. Να επιμείνετε σε αυτά που αναφέραμε παραπάνω, σε αυτούς τους απλούς κανόνες. Μια συμπεριφορά σταθερή και συνεπής, απομακρύνει τον κίνδυνο ενοχοποίησης σας. Θα σας κάνουν να αισθανθείτε μόνοι και χωρίς βοήθεια, θα προσπαθήσουν να σας πείσουν, ότι κανείς δεν μπορεί να σας Βοηθήσει και ότι μόνο από αυτούς εξαρτάται να σας αφήσουν ή να σας κρατήσουν. Όταν εκτιμήσουν, ότι με αυτή τη μεταχείριση θα σας έχουν μαλακώσει λιγάκι, θα αλλάξουν τόνο. Ίσως εμφανιστεί κάποιος αστυνομικός καλός, που θα ενδιαφερθεί για σας, για τις δυσκολίες σας, για τους δικούς σας. Θα περάσει έτσι, η κατάσταση από μια φάση επιθετική σε μια φάση "φιλική". Είναι μια πολύ "λεπτή στιγμή". Να είστε πολύ προσεχτικοί και με αξυμένα τα αισθητήρια. Θα προσπαθήσουν να σας μπερδέψουν, να σας απομονώσουν από τους φίλους σας ή τους συντρόφους σας, θα σας καλέσουν να αναίξετε την καρδιά σας, θα σας προτρέψουν να διαχωρίσετε τις ευθύνες σας. Αν όλα αυτά δεν φτάνουν για να σας "συμμορφώσουν", είναι πιθανό και πάλι να σας επιτεθούν στα ίσια. Θα σας κρατήσουν κάτω από πίεση για ώρες, θα σας επαναλάβουν τις ίδιες ερωτήσεις, ξαναρχίζοντας με καινούργια ορμή. Θα προσπαθούν διαρκώς να σας μπερδέψουν, να σας ταπεινώσουν, να σας κουράσουν. Σε πολλές περιπτώσεις, και όλοι το γνωρίζουν, ότι οι ανακρινόμενοι χτυπιούνται, βασανίζονται. Μην πιστεύετε ό,τι σας λένε ή σας δείχνουν ή σας κάνουν να ακούτε. Θα σας κάνουν ένα σωρό κόλπα. Θα σας φέρουν σε αντιπαράθεση με άλλους αστυνομικούς, με άλλους κατηγορούμενους ή μάρτυρες. Μπορεί να εμφανιστεί αστυνομικός, τον οποίο δεν έχετε ξαναδεί, που να δηλώνει αυτόπτης μάρτυρας και να σας αναγνωρίζει, θέλοντας να ομολογήσετε. Αργότερα, στον ανακριτή ή στο δικαστήριο, θα προσπαθήσετε να ανατρέψετε την ομολογία σας, μιλώντας για ένα ψεύτικο μάρτυρα. Φυσικά, δεν θα πείσετε κανέναν. Θα σας διαβάσουν απολογίες για να σας πείσουν ότι "ο τάδε τα είπε όλα και επομένως είναι Βλακεία να επιμένεις στη σιωπή σου". Θα σας Βάλουν να ακούσετε μαγνητοφωνημένες

συζητήσεις, θα σας δείξουν φωτογραφίες κτλ. Επιμείνετε στην στάση σας και θα είναι καλύτερα και για τον εαυτό σας και για όποιους άλλους αφορά η στάση σας.

ΒΑΣΙΚΟΙ ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

1. Η μόνη υποχρέωση που έχετε όταν σας ανακρίνουν, είναι να δηλώσετε τα στοιχεία της ταυτότητας σας. Μην απαντάτε σε καμία άλλη ερώτηση. Σε όλες να λέτε, "δεν έχω τίποτα να δηλώσω". Μην αφήσετε τον εαυτό σας να παρασυρθεί από απειλές, ούτε να ξεγελαστείτε από υποσχέσεις, ότι δήθεν θα σας ελευθερώσουν ή θα καλύψουν την υπόθεση. Τις περισσότερες φορές το δικαστήριο δεν έχει κανένα άλλο αποδεικτικό στοιχείο εναντίον σας, εκτός από την απολογία σας στην αστυνομία. Είναι άχρηστο, να τους κάνετε αυτό το δώρο.

2. Εχετε δικαίωμα, σαν κατηγορούμενος να πείτε ό,τι ψέμα σας κατέβει στο κεφάλι. Είναι όμως πολύ επικίνδυνο, να μπλεχτείτε σε μια ιστορία με τέτοιες αντιφάσεις από τις οποίες θα ήταν δύσκολο να ξεγλιστρήσετε. Μια υπεράσπιση δεν εφευρίσκεται, κατά τη διάρκεια της ανάκρισης, όταν είστε αγχωμένοι και κάτω από την πίεση της αστυνομίας. Διαμορφώνεται με καθαρό κεφάλι με τους συντρόφους σας και τη βοήθεια του δικηγόρου.
Οσο διάστημα δεν έχετε δικηγόρο, ένα πράγμα πρέπει να κάνετε. Να διατηρήσετε, με το να μην πείτε τίποτα, όλες τις δυνατότητες υπεράσπισης. Σε περίπτωση που κάποιος σας δώσει, Βρούνε οτιδήποτε στο σπίτι σας που σας ενοχοποιεί ή σας αναγνωρίσει κάποιος αυτόπτης μάρτυρας, η στάση σας πρέπει να είναι ίδια. Οι καταθέσεις αναιρούνται, η κατοχή πολλών αντικείμενων -που στην αρχή φαίνεται να σας ενοχοποιούν- μπορεί αργότερα να εξηγηθεί, οι μάρτυρες πέφτουν συχνά σε αντιφάσεις. Τη δική σας, όμως, ομολογία πολύ δύσκολα την παίρνετε πίσω. Πρέπει να μιλήσετε για εκβιασμούς και σωματική βία και να πείσετε τον ανακριτή ή το δικαστήριο.
Οταν σας παρουσιάζουν φωτογραφίες, μην πείτε δεν ξέρω, αρνηθείτε να απαντήσετε. Κοιτάξτε τις όμως και προσπαθήστε να καταλάβετε πότε και πού τις τράβηξαν, προσέξτε αν αναγνωρίζετε άλλους φίλους ή συντρόφους σας σε αυτές και ειδοποιήστε τους. Μη δηλώσετε ότι έχετε κάνει αυτό ή ότι έχετε πάρει μέρος σε κάποια γεγονότα που σας ενοχοποιούν. Μη δώσετε ποτέ λογαριασμό για τις πράξεις σας. Μη δηλώσετε ποτέ την ομάδα που δραστηριοποιήστε, εσείς ή άλλοι σύντροφοι σας. Ποιοι είναι αυτοί, ποια η γνώμη σας για αυτούς, τι πράγματα λέγονται για αυτούς.

3. Αν σας χτυπήσουν ή βασανίσουν, η πρώτη σας ενέργεια μόλις σας αφήσουν ελεύθερο είναι να καταθέσετε μήνυση, σε όσους σας χτύπησαν, (κάθε ένστολος έχει ένα διακριτικό αριθμό στους ώμους του, καλό θα είναι αν μπορείτε να τους θυμάστε). Ακόμα και "κατ' αγνώστων". Τότε μόνο ο εισαγγελέας θα σας στείλει στον ιατροδικαστή. Μόνοι σας, δεν μπορείτε να πάτε. Η γνωμάτευση του, μπορεί να σας φανεί πολύ χρήσιμη, στο δικαστήριο.

ΤΑΚΤΙΚΗ ΑΝΑΚΡΙΣΗ

1. Συνήθως η κύρια ανάκριση είναι πολύ κυριλέ διαδικασία -αυτή είναι άλλωστε και η παγίδα- και ο ανακριτής έχει τον αέρα του λειτουργού του νόμου.
Γενικώς τον ανακριτή, μπορείτε να τον "ξεπεράσετε" εύκολα με ένα απολογητικό υπόμνημα. Αυτό είναι μια αναφορά που γράφει ο δικηγόρος σας και ουσιαστικά πρόκειται για μια μελετημένη απάντηση στις κατηγορίες. Μπορείτε εξεταζόμενοι να πείτε "αναφέρομαι στο απολογητικό μου υπόμνημα και δεν έχω να προσθέσω κάτι άλλο". Έτσι, δεν απαντάτε στις ερωτήσεις που θα σας κάνει ο ανακριτής.
Η στάση αυτή δεν προτείνεται, παρ' όλα που δεν έχει ιδιαίτερες επιπτώσεις στο δικαστήριο. Μπορεί όμως, να αποβεί μοιραία, για το κρισιμότατο ζήτημα της προφυλάκισης. Επειδή ο ανακριτής, αποφασίζει κυριαρχικά για τη προφυλάκιση σας, [ο εισαγγελέας σχεδόν πάντα λέει ναι] πρέπει να είστε πολύ προσεχτικοί. Αν

υιοθετήσετε αυτόν τον τρόπο υπεράσπισης, πολλαπλασιάζεται τις πιθανότητες να αποφασίσει υπέρ της προφυλάκισης. Πρώτον, γιατί με αυτόν τον τρόπο πιστεύει ότι τον απαξιώνετε και δεύτερον, γιατί δεν του δημιουργείτε αμφιβολίες. Μόνο μέσα από τον μεταξύ σας "διάλογο", έχετε αυτή τη δυνατότητα.

2. Ο ανακριτής είναι πιο επικίνδυνος, από οποιονδήποτε αστυνομικό. Ο αστυνομικός έχει τη δύναμη, ο ανακριτής έχει το νόμο. Αυτός αποφασίζει για την φυλάκιση σας, αυτός κρίνει τα στοιχεία που του στέλνει η αστυνομία. Μην αφήνετε ποτέ, να σας υποβάλλετε η απάντηση σε μια ερώτηση από τον ίδιο. Χρησιμοποιήστε πάντα δικά σας λόγια. Σε μια ερώτηση, είναι καλύτερο πρώτα να αρνηθείτε και μετά να εξηγήσετε, παρά πρώτα να εξηγήσετε και μετά να αρνηθείτε, με κίνδυνο να μπερδευτείτε. Να είστε απλοί και προσεχτικοί. Όσο λιγότερα λέτε, τόσο μικρότερη είναι η πιθανότητα να πέσετε σε αντιφάσεις.

3. Πάντα στην ανάκριση κρατούνται πρακτικά. Στο τέλος, διαβάστε τα πολύ προσεχτικά. Ό,τι έχετε καταθέσει, να έχει γραφτεί με τα δικά σας λόγια και όχι με τα λόγια του ανακριτή. Κοιτάξτε να έχουν γραφτεί και οι ερωτήσεις, οι διαμαρτυρίες σας, οι δηλώσεις σας. Ζητήστε να υπογράψει μαζί σας αυτός που πράγματι σας ανέκρινε και βάλτε στα πρακτικά όλες τις διορθώσεις και τις μετατροπές που νομίζετε. Να φαίνεται η ακριβής ώρα που άρχισε και έκλεισε η ανάκριση. Τότε υπογράψτε την κατάθεση σας.

ΕΞΑΚΡΙΒΩΣΗ ΣΤΟΙΧΕΙΩΝ

1. Αν βρίσκεστε σε κάποιο αστυνομικό τμήμα για μια απλή προσαγωγή, υποχρεούνται να σας αφήσουν μετά την εξακρίβωση των στοιχείων σας. Αυτό ενδεχομένως να κρατήσει αρκετές ώρες.
Αν δεν σας απαγγείλουν κατηγορίες, δεν είστε υποχρεωμένοι να δώσετε αποτυπώματα και να σας βγάλουν φωτογραφίες. Αν είναι η πρώτη φορά που πάνε να σας τα πάρουν, έχει αξία να αρνηθείτε. Να έχετε πάντως στο νου σας ότι είναι κάτι που δεν συνηθίζεται. Για αυτό το λόγο θα σας απειλήσουν, μπορεί και να σας χτυπήσουν. Αν σας έχουν ξαναπάρει αποτυπώματα και φωτογραφίες, ίσως να είναι άσκοπο να αρνηθείτε. Ζυγίστε κάθε φορά την κατάσταση και αποφασίστε.

ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΟΥ ΑΣΚΗΘΕΙ ΔΙΩΞΗ

1. Η αστυνομία οφείλει να σας οδηγήσει το συντομότερο δυνατό στον εισαγγελέα, σε κάθε περίπτωση εντός 24 ωρών. Ο εισαγγελέας σας απαγγέλλει κατηγορίες και έχει τις εξής δυνατότητες:

-Να σας παραπέμψει σε τακτική δικάσιμο, οπότε αφήνεστε ελεύθεροι. Υποχρεούστε να δηλώσετε μια διεύθυνση μόνιμης διαμονής ή κατοικίας. Είναι σημαντικό να ξέρετε, ότι η δήλωση παραπλανητικής διεύθυνσης ή στοιχείων δεν πρόκειται να βοηθήσει σε τίποτα. Αντίθετα, εκτός από ότι σας εκθέτει σε σχετική ποινική ευθύνη, δίνει την ευχέρεια στις αρχές να δικαστείτε έγκυρα με την επίδοση εγγράφων σε λάθος διεύθυνση, χωρίς να μπορείτε, αργότερα, να παραπονεθείτε ότι δεν λάβατε γνώση του δικαστηρίου επειδή κατοικούσατε αλλού.
-Να διατάξει συμπλήρωση της προανάκρισης [σπανίως] ή κύρια ανάκριση, ιδίως σε περιπτώσεις που κριθεί αναγκαία η επιβολή περιοριστικών όρων [εγγύηση, εμφάνιση στο αστυνομικό τμήμα, απαγόρευση εξόδου από τη χώρα κλπ] ή προσωρινής κράτησης [στην περίπτωση κακουργημάτων]. Η επίσημη αιτιολογία για την προφυλάκιση σας κράτηση σε αυτή τη περίπτωση είναι ο κίνδυνος φυγής ή τέλεσης άλλων αξιόποινων πράξεων. Κατά συνέπεια, Βοηθάει η ύπαρξη σταθερής κατοικίας, μόνιμης εργασίας, λευκού ποινικού μητρώου κλπ.
-Να σας παραπέμψει να δικαστείτε με την αυτόφωρη διαδικασία. Στην περίπτωση αυτή θα προσαχθείτε στο δικαστήριο εντός 24 ωρών και μπορεί να σας δώσει μια προθεσμία ως τρεις μέρες για να ετοιμάσετε καλύτερα την υπεράσπιση σας. Κατά τη διάρκεια αυτής της προθεσμίας μπορεί να διαταχθεί η συνέχιση της κράτησης σας.

ΚΑΤΑΘΕΣΗ ΩΣ ΜΑΡΤΥΡΑΣ

1. Σε περίπτωση που σας καλέσουν να καταθέσετε ως μάρτυρες στην αστυνομία ή στον ανακριτή αυτό πρέπει να γίνει με κλήση στο σπίτι σας. Έχετε έτσι το χρόνο να σκεφτείτε τι ακριβώς θα πείτε.
Αν όμως -κάτι που πλέον είναι πιο συνηθισμένο- σαν πάνε μια μέρα για εξακρίβωση στοιχείων και εκεί σας ζητήσουν να καταθέσετε ως μάρτυρας, εσείς απλώς αρνείστε να πείτε και να υπογράψετε οτιδήποτε, αφού αυτή η διαδικασία είναι παράτυπη.

ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΟΥ ΣΥΛΛΗΦΘΕΙ ΚΑΠΟΙΟΣ ΦΙΛΟΣ ΣΑΣ

1. Είναι χρήσιμο με τους στενούς μας φίλους ή συντρόφους να έχουν προβλεφθεί και μελετηθεί από πριν κάποιες κινήσεις, που θα γίνουν αμέσως μόλις μάθετε τα δυσάρεστα νέα.
Πρέπει να ειδοποιήσετε αμέσως το δικηγόρο που θα σας έχει ήδη υποδείξει ο φίλος σας ή αυτόν που θα σας ανακοινώσει όταν σας πάρει τηλέφωνο από το αστυνομικό τμήμα. Να του μεταφέρετε ακριβώς, χωρίς υπερβολές, ό,τι σας έχει πει ο φίλος σας για τη σύλληψη του. Θα πρέπει να εξαφανίσετε οποιαδήποτε στοιχεία μπορεί να επιβαρύνουν αυτόν ή κάποιον άλλο από σπίτια ή από οποιοδήποτε άλλο μέρος μπορεί να ερευνήσει η αστυνομία. Ακόμα και πράγματα που φαίνονται, με τη πρώτη ματιά, "αθώα". Τηλεκάρτες, ατζέντες με τηλέφωνα, ημερολόγια, κινητά, φωτογραφίες, χειρόγραφα, τον εκτυπωτή και το σκληρό δίσκο από τον ηλεκτρονικό υπολογιστή. Έχετε στο νου σας, ότι η αστυνομία μπορεί να βρίσκετε κάποια βήματα μπροστά σας, να έχει εντοπίσει ήδη κάποια σπίτια, εσάς ή κάποιους γνωστούς σας και να τους παρακολουθεί για να βγάλει στοιχεία για την υπόθεση που ερευνά ή για να τους ενοχοποιήσει. Να είστε ψύχραιμοι και προσεχτικοί. Βεβαιωθείτε όσο καλύτερα γίνεται, ότι δε σας παρακολουθούν πριν τα επισκεφτείτε. Στη συνέχεια, ειδοποιήστε τους συντρόφους σας για την υπόθεση (χωρίς να πείτε υπερβολές) και κανονίστε τις επόμενες κινήσεις σας.

Λίγα λόγια σχετικά με τα ίχνη που αφήνουμε...

(αναδημοσίευση από το περιοδικό theorie du contexte)

Από δακτυλικά αποτυπώματα

Γεννιόμαστε με τα δακτυλικά μας αποτυπώματα και δεν μπορούμε ποτέ να απαλλαγούμε απ' αυτά. Όποτε αγγίζουμε κάτι με τα ακροδάχτυλά μας, αφήνουμε πίσω τα "επισκεπτήρια" μας. Η αστυνομία δυσκολεύεται να "σηκώσει" τα αποτυπώματά μας, ανάλογα με την επιφάνεια στην οποία βρίσκονται.

Τον τομέα της αναγνώρισης αποτυπωμάτων κάποτε αφορούσαν εκείνα τα οποία ήταν ορατά: αποτυπώματα σε αίμα ή σε άλλο παρεμφερές μέσο ή εκείνα που έχουν εντυπωθεί πάνω σε πλαστική επιφάνεια. Ωστόσο οι ερευνητές σύντομα ανακάλυψαν ότι σχεδόν σε κάθε επιφάνεια θα μπορούσαν να αναζητηθούν αόρατα, "λανθάνοντα" αποτυπώματα.

Τα λανθάνοντα αποτυπώματα σχηματίζονται από απειροελάχιστα ίχνη ιδρώτα, είτε από τις ίδιες τις άκρες των δάκτυλων, είτε από κάποια ασυναίσθητη επαφή με κάποιο άλλο σημείο του σώματος. Κατά το 99% περιέχουν νερό, το υπόλοιπο 1% αποτελείται από ένα σύνθετο μείγμα ουσιών που διαφοροποιείται όχι μόνο από άτομο σε άτομο αλλά και από ώρα σε ώρα, στο ίδιο άτομο. Η διάρκεια παραμονής ενός τέτοιου αποτυπώματος εξαρτάται από διάφορους παράγοντες, αλλά αυτά μπορούν να παραμείνουν ακόμα και για αιώνες.

Τα λανθάνοντα αποτυπώματα "εμφανίζονται" με πολλούς τρόπους. Η βασική τεχνική έγκειται στην επικάλυψη τους με μια πολύ λεπτή σκόνη και τη χρήση ενός "εμφυσητήρα", μια συσκευή που μοιάζει με ψεκαστήρα αρώματος. Για αρκετό καιρό τα αποτυπώματα που εμφανίζονταν κατ' αυτόν τον τρόπο έπρεπε στη συνέχεια να φωτογραφηθούν. Ωστόσο, σήμερα "μεταφέρονται" με διάφανη κολλητική ταινία, η οποία έπειτα τοποθετείται πάνω σε διάφανη ενισχυτική επιφάνεια ή σε μια κάρτα κατάλληλου χρώματος.

Τα αποτυπώματα σε πορώδεις επιφάνειες όπως το χαρτόνι ή το ξύλο αποκαλύπτονται με διαφορετικό τρόπο. Από το ανθρώπινο δέρμα μπορούν να μεταφερθούν, αν και σπάνια παραμένουν πάνω από δύο ώρες. Τα λανθάνοντα αποτυπώματα μπορούν επίσης να αποκαλυφθούν με δέσμες ακτίνων laser.

Τα δακτυλικά αποτυπώματα καταστρέφονται αρκετά δύσκολα. Ωστόσο ένα δυνατό και πολύ προσεκτικό πέρασμα με ένα βρεγμένο και στη συνέχεια με ένα καθαρό και στεγνό πανί είναι ικανό να τα εξαφανίσει. Ούτε και η φωτιά αποτελεί σίγουρη μέθοδο καταστροφής, εκτός και αν το αντικείμενο καταστραφεί εντελώς, γιατί ένα στρώμα κάρβουνου μπορεί να καλύψει τα αποτυπώματα και να τα διατηρήσει αναγνωρίσιμα.

Στην Ελλάδα απαιτούνται τουλάχιστον 12 πανομοιότυπα χαρακτηριστικά ώστε να προσδιοριστεί η ταυτότητα κάποιου από τους σχηματισμούς των αυλακώσεων που εμφανίζουν τα αποτυπώματα των δακτύλων ή της παλάμης του.

Εκτός από τα δακτυλικά αποτυπώματα φυλάσσονται και ταξινομούνται και τα αποτυπώματα της παλάμης, αφού είναι δυνατόν να εμφανίζουν σχηματισμούς το ίδιο χαρακτηριστικούς.

Για να γίνει λήψη αποτυπωμάτων ΑΠΑΙΤΕΙΤΑΙ ΝΑ ΕΧΟΥΝ ΗΔΗ ΑΠΟΔΩΘΕΙ ΚΑΤΗΓΟΡΙΕΣ, ενώ η άρνηση σας να τα δώσετε ακόμα και μετά από την απόδοσή τους συνεπάγεται το απλό πταίσμα της απείθειας. Η επιλογή δική σας.

Σε μια πρωτότυπη σειρά δακτυλικών αποτυπωμάτων λαμβάνονται δύο σειρές αποτυπωμάτων. Τα πρώτα λαμβάνονται σε 10 αριθμημένα μέρη. Κάθε δάκτυλο καλύπτεται με μελάνι και στη συνέχεια κυλιέται από τη μια του άκρη έως την άλλη, σε όλη την επιφάνεια, έτσι ώστε να καταγραφούν οι ανάγλυφοι σχηματισμοί που βρίσκονται γύρω από την καμπύλη του δακτύλου. Στη συνέχεια λαμβάνονται τα ίδια 10 αποτυπώματα ως απλά εντυπώματα , δίχως να κυλιστούν. Αυτό γίνεται κατά κύριο λόγο για να εξασφαλιστεί ότι τα ίδια αποτυπώματα λαμβάνονται με τη σωστή σειρά, αφού έχουν υπάρξει περιπτώσεις κατά τις οποίες οι κατηγορούμενοι φάνηκαν αρκετά συνεργάσιμοι, προτείνοντας τα δάχτυλά τους με λανθασμένη σειρά ή ακόμα και καταφέρνοντας να δώσουν δύο φορές τα αποτυπώματα του ίδιου χεριού.

Κατά την διαδικασία λήψης αποτυπωμάτων, θεωρητικά, είναι δυνατόν να παραμορφώσετε τα δακτυλικά μας αποτυπώματα. Ένας τρόπος είναι να αφήσετε μπάλικο σαπούνι στα χέρια σας αφού σας βάλλουν να τα πλύνετε κι άλλος τρόπος είναι να προσπαθήσετε να "βοηθήσετε" την αστυνομία. Υποτίθεται ότι χαλαρώνεται τα δάχτυλα σας όταν τα πιέζουν πάνω στο χαρτί. Αν βάλλετε πολύ δύναμη ή γλιστρήσει λίγο το δάχτυλά σας μπορεί να μουτζουρώστε κάνα δύο.

Από γάντια

Παρ' όλο που είναι πάντα καλύτερο να φοράτε γάντια για να αποφύγετε τον κίνδυνο ν' αφήσετε δακτυλικά αποτυπώματα, θα πρέπει να ξέρετε ότι τα γάντια μπορούν να αφήσουν μερικές φορές τις ίδιες πληροφορίες. Αφήνουν σχεδόν σίγουρα ίχνη από το υλικό απ' το οποίο είναι φτιαγμένα σε οτιδήποτε αγγίξουν, ιδιαίτερα σε σπασμένο γυαλί, φράχτες, τοίχους και ακατέργαστο ξύλο. Αν τα γάντια δεν πετιούνται μετά τη χρήση, μπορούν να γίνουν θετικοί συνδυασμοί με τη μορφή της ανάλυσης του υφάσματος. Τα πλαστικά και τα λαστιχένια γάντια κρατάνε τα αποτυπώματά σας στο εσωτερικό τους και μερικά πολύ λεπτά χειρουργικά αφήνουν τις "εντυπώσεις" των δακτυλικών αποτυπωμάτων να εμφανιστούν στις σκληρές και γυαλιστερές επιφάνειες. Αν βρεθούν τα πεταμένα σας γάντια, θα έχουν ίχνη από τον ιδρώτα σας και άλλα συγκριτικά ίχνη, όπως σχίζες ξύλου, κομματάκια μπογιάς, θραύσματα γυαλιού κλπ.

Από την επαφή με αντικείμενα τα γάντια διαποτίζονται από ιδρώτα, λίπος και ρύπους. Το λίπος που εναποτίθεται σε ένα γάντι μπορεί να γίνει ορατό με ειδική σκόνη, όπως και στην περίπτωση των δακτυλικών αποτυπωμάτων. Το στρώμα λίπους πάνω στο γάντι δεν είναι το ίδιο δυνατό και πυκνό όπως αυτό των δακτυλικών αποτυπωμάτων αλλά είναι , παρόλα αυτά, ανιχνεύσιμο, αξιόπιστο και καταγράψιμο και μπορεί να οδηγήσει στην αναγνώριση της ταυτότητας κάποιου.

DNA

Η ταυτοποίηση του γεννητικού αποτυπώματος, γνωστού ως DNA, θεωρείται η πιο αδιαμφισβήτητη τεχνική αναγνώρισης της ταυτότητας ενός ατόμου. Ενώ για την αναγνώριση μέσω των δακτυλικών αποτυπωμάτων απαιτείται να υπάρχει ένα αρκετά αναγνωρίσιμο τμήμα ενός ήδη καταχωρημένου αποτυπώματος, στην ανάλυση DNA δεν απαιτούνται παρά λίγα κύτταρα του ατόμου. Για την αναγνώριση της ταυτότητας κάποιου οι ερευνητές θα πρέπει να έχουν στη διάθεση τους ένα δείγμα DNA (μια τρίχα, μια σταγόνα αίματος, σάλιου, λεκέ από ούρα ή σπέρμα) από το σημείο του "εγκλήματος" καθώς και ένα δείγμα από τον ύποπτο. Το δείγμα του υπόπτου δεν είναι απαραίτητο να είναι το ίδιο με αυτό που βρέθηκε στον τόπο του "εγκλήματος", αλλά μπορεί να είναι κύτταρα από το στόμα που παραλαμβάνονται με απόξεση. Τα γενετικά αποτυπώματα συμπίπτουν. Με το αποτύπωμα DNA υπάρχει μια πιθανότητα στα τρία εκατομμύρια το δείγμα να προέρχεται από δύο διαφορετικά άτομα, αν και υπάρχουν ήδη σοβαρές ενστάσεις για αυτό...

Οι κρατικές υπηρεσίες έχουν καθιερώσει πιά βάσεις δεδομένων αντίστοιχες με εκείνες των δακτυλικών αποτυπωμάτων. Για να γίνει λήψη δείγματος DNA ΑΠΑΙΤΗΤΑΙ ΝΑ ΕΧΟΥΝ ΗΔΗ ΑΠΟΔΟΘΕΙ ΚΑΤΗΓΟΡΙΕΣ, ενώ ο κατηγορούμενος μπορεί να αρνηθεί και να μη γίνει εξέταση. Σε αυτή την περίπτωση θα πρέπει να γίνει λήψη με ΜΗ βίαια μέσα, πράγμα που σημαίνει ότι θα ψάξουν(αν δεν το έχουν ήδη κάνει μέχρι εκείνη τη στιγμή) να βρουν το DNA από το σπίτι, τα ρούχα, τις κουβέρτες όπως θα ψάξουν και για οποιοδήποτε άλλο ενοχοποιητικό στοιχείο.

Από εργαλεία...

Σε πολλές περιπτώσεις απαιτείται η χρήση εργαλείων. Οι ερευνητές κατατάσσουν τα σημάδια που αφήνει κανείς πίσω του, μετά την χρήση κάποιου εργαλείου, με την μορφή των εντυπωμάτων, των εκδορών ή των εγκοπών.

Τα εντυπώματα ανακαλύπτονται σε αντικείμενα όπως τα παράθυρα από ξύλο ή αλουμίνιο και τα ξύλινα πλαίσια των θυρών όπου το μέταλλο ενός μοχλού (η αιχμή ενός σφυριού, μιας σμίλης, ενός κατσαβιδιού ή ενός λοστού) είναι σκληρότερο από το υλικό του πλαισίου. Εάν κάποιο εργαλείο βρεθεί στη κατοχή μας, αυτό που θα ελεγχθεί είναι αν αυτό θα ταιριάζει με τα εντυπώματα που έχουν ανακαλυφθεί. Οι εκδορές σε ξύλο, μέταλλο ή χρωματισμένη επιφάνεια προκαλούνται από μαχαίρι ή κάποιο παρόμοιο όργανο. Και αυτές συχνά

μπορούν να συγκριθούν κάποιο εργαλείο. Οι εγκοπές προκαλούνται εργαλεία όπως τα απλά πριόνια ή τα σιδηροπρίονα. Σ'αυτή την κατηγορία ανήκουν επίσης εργαλεία διάνοιξης που χρησιμοποιούνται για την παραβίαση κλειδαριών ή τοιχωμάτων χρηματοκιβωτίων. Τα σημάδια αυτά δεν προσφέρουν σημαντικές πληροφορίες εάν συγκριθούν με το αντίστοιχο όργανο που τις προκάλεσε, γιατί η αιχμή του δεύτερου φθείρεται άμεσα και υπόκειται σε βλάβες.

Οι χρήσιμες άκρες των εργαλείων μπορούν να μεταμορφωθούν λιμάροντας ή ακονίζοντάς τα, αλλά μόνο αν το εργαλείο είναι σε καλή κατάσταση και δεν είναι άσχημα σημαδεμένο. Αντικείμενα όπως σκοινί, σπάγκος, ταινίες κλπ είναι το ίδιο ενοχοποιητικά και προσφέρονται για συγκριτική ανάλυση.

Από γυαλί...

Όταν κανείς εισβάλλει μέσα σε ένα χώρο σπάζοντας το τζάμι κάποιου παραθύρου ή πόρτας είναι σχεδόν βέβαιο ότι κάπου πάνω στα ρούχα του θα βρεθούν μικροσκοπικά κομμάτια γυαλιού, αφού κατά την θραύση μια τζαμαρίας το 70 % των θραυσμάτων διασκορπίζονται μακριά από τον δράστη, ενώ τα υπόλοιπα κατευθύνονται προς τον ίδιο και κάποια χτυπούν πάνω στα ρούχα του.

Οι περισσότεροι έχουν ρίξει και σπάσει ένα ποτήρι δίχως να δώσουν σημασία στα μικροσκοπικά ψήγματα γυαλιού που πιθανόν να έχουν ενσφηνωθεί στα ρούχα τους. Ωστόσο είναι πολύ σημαντικό για έναν ερευνητή να αποδείξει ότι το γυαλί είναι το ίδιο με αυτό που έσπασε και βρέθηκε στον τόπο του "εγκλήματος" και η ταυτοποίηση του γίνεται μέσω του διαθλαστικού του δείκτη, ο οποίος κυμαίνεται ανάλογα με την κατασκευή του.

Το γυαλί κολλάει εύκολα στις σόλες των παπουτσιών. Η αστυνομία μπορεί να αναγνωρίσει διάφορους τύπους και είδη γυαλιού και έτσι μπορεί να σας τοποθετήσει σε ορισμένο τόπο και χρόνο.

Λεπτή σκόνη σπασμένου γυαλιού κολλάει στις λείες επιφάνειες των εργαλείων και ίνες από τα ρούχα σας κολλάνε στις κοφτερές άκρες του σπασμένου γυαλιού.

Από φωτιά και έκρηξη...

Οι εκρήξεις και οι πυρκαγιές σχετίζονται άμεσα, αφού οι χημικές διεργασίες που λαμβάνουν χώρα μοιάζουν πολύ και συνήθως μετά από μια έκρηξη ακολουθεί πυρκαγιά ή το αντίστροφο. Η προσέγγιση στο χώρο της έκρηξης γίνεται με μεγάλη προσοχή. Το σημείο των ερευνών καθορίζεται συνήθως με τον εξής τρόπο: η εκτίμηση της απόστασης από το κέντρο της έκρηξης μέχρι το πιο μακρινό θραύσμα και στη συνέχεια ο αποκλεισμός της περιοχής σε ακτίνα 50% μεγαλύτερη από αυτή την απόσταση. Η περιοχή αυτή

φωτογραφίζεται εξ' ολοκλήρου. Η λεπτομερής εξέταση των υλικών ζημιών και ο υπολογισμός της κατεύθυνσης του οστικού κύματος προσδιορίζει το κέντρο της έκρηξης. Τα κομμάτια από τον μηχανισμό περισυλλέγονται για να ελεγχθούν για αποτυπώματα, DNA και άλλα ίχνη και όταν ολοκληρωθεί η φυσική εξέταση του χώρου σειρά έχει η χημική του εξέταση. Λόγω του ότι όλες οι εκρηκτικές ύλες αφήνουν ορισμένα στέρεα κατάλοιπα, όσο μακριά και αν έχουν διασκορπιστεί μπορούν να βρεθούν και άρα να προσδιαριστούν. Σχεδόν κάθε μηχανισμός κουβαλά την "υπογραφή" του κατασκευαστή του. Σε περίπτωση προσαγωγής για έκρηξη μεγάλη σημασία δίνεται στην ανακάλυψη ιχνών της εκρηκτικής ύλης πάνω στο σώμα και ιδίως στα χέρια, στα ρούχα και στα αντικείμενα που βρίσκονται στο χώρο που μένουν. Ακόμα και τα γάντια δεν είναι βέβαιο ότι μπορούν να καλύψουν αυτά τα ίχνη. Επίσης, τα χέρια είναι πιθανόν να ρυπανθούν εάν κανείς αγγίξει μια επιφάνεια όπου είχε ακουμπήσει την εκρηκτική ύλη ή το υλικό της συσκευασίας της. Κατά τον ίδιο τρόπο τα χέρια είναι πιθανό να μεταφέρουν ίχνη σε κάποια άλλη επιφάνεια, όπως ένα τιμόνι ή το ταμπλό του αυτοκινήτου.

Οι φωτιές που οφείλονται σε ατύχημα πάντοτε ξεκινούν από ένα μοναδικό σημείο. Αντίθετα εκείνες που οφείλονται σε εμπρηστές συνήθως ξεκινούν από περισσότερα για να είναι σίγουροι οι υπεύθυνοι ότι οι φλόγες θα εξαπλωθούν. Οι έρευνες ξεκινούν από το το χαμηλότερο επίπεδο του κτηρίου στο οποίο υπάρχει φανερή καταστροφή από φωτιά. Τα σχήματα του καπνού και της απανθράκωσης στους τοίχους, τα δάπεδα και τις οροφές μπορούν προσφέρουν σημαντικές πληροφορίες. Τα δείγματα από τον αέρα στον τόπο της πυρκαγιάς φανερώνουν την ύλη που χρησιμοποιήθηκε, ενώ τα εύφλεκτα υγρά αφήνουν μια έντονη μυρωδιά, η οποία παραμένει στην ατμόσφαιρα για αρκετό διάστημα, αφού σβήσουν οι φλόγες. Επίσης τα σημάδια καύσης και οι κηλίδες στο δάπεδο, όπου τα υγρά σχημάτισαν λίμνες μόλις αναφλέγησαν, μαρτυρούν πολλά για τη φύση του. Μια ασυνήθιστη μεγάλη συγκέντρωση στάχτης μπορεί να υποδείξει το σημείο, όπου ήταν συγκεντρωμένο το υλικό που προκάλεσε τη φωτιά. Εάν έχει χρησιμοποιηθεί κάποιο είδος φυτιλιού είναι πιθανό να βρεθεί κάποιο ευδιάκριτο ίχνος του, ενώ εάν η φωτιά προκλήθηκε με τη χρήση επιταχυντών, όπως η βενζίνη ή άλλα εύφλεκτα υγρά, ορισμένα από αυτά απορροφώνται από το ξύλο, η διαρρέουν μέσα από τις ρωγμές του πατώματος, απ' όπου συνήθως δεν μπορούν να αναφλεγούν λόγω της έλλειψης οξυγόνου. Τα συστήματα πυρόσβεσης ελέγχονται εξ' ίσου για να διαπιστωθεί αν είχαν αχρηστευτεί.

Από χειρόγραφα σημειώματα και γραφικό χαρακτήρα...

Υποπτα, χειρόγραφα και πρωτότυπα σημειώματα δεν υπάρχει κανένας λόγος να διατηρεί κανείς στη κατοχή του. Ο γραφικός χαρακτήρας ενός ατόμου είναι το ίδιο χαρακτηριστικός και προσωπικός όσο και τα δακτυλικά του αποτυπώματα και όπως αυτά, είναι αδύνατον να τα αλλάξει. Άτομα τα οποία χάνουν την ικανότητα να γράφουν με το ένα χέρι και αναγκάζονται να γράφουν με το άλλο σταδιακά εμφανίζουν τα ίδια ακριβώς χαρακτηριστικά που υπήρχαν στον αρχικό τους γραφικό χαρακτήρα. Επίσης το μέγεθος, η κλήση, η ένταση και άλλα χαρακτηριστικά μπορούν να αποκαλύψουν εσκεμμένη παραποίηση, συναισθηματική ή ψυχολογική πίεση αλλά και στοιχεία της προσωπικότητας. Το χαρτί φυσικά μεταφέρει τα δακτυλικά αποτυπώματα ενώ αν έχει γίνει ταχυδρομική αποστολή το DNA θα μπορέσει να παρθεί αν έχει χρησιμοποιηθεί σάλιο για το φάκελο ή το γραμματόσημο. Σε περιπτώσεις προσαγωγής ένας επιπλέον λόγος για να μην υπογράφουμε τίποτα ή να μην γράφουμε ακόμα και το πιο αθώο πράγμα, είναι να μην παρέχουμε τον γραφικό μας χαρακτήρα για μετέπειτα σύγκριση.

Αν ωστόσο επιμένετε να γράψετε, τότε καλύτερα να χρησιμοποιείτε στιλιζαρισμένα κεφαλαία. Γράφετε πάντα σε ένα μόνο φύλλο χαρτί κάθε φορά, κατά προτίμηση σε μια επίπεδη και σκληρή επιφάνεια, που δεν θα κρατήσει εντύπωση από αυτό που γράψατε. Μη χρησιμοποιείτε φύλλα που κόβετε από μπλοκ ή τετράδια, γιατί μπορεί να γίνουν συγκρίσεις από το κόψιμο, το σκίσιμο και τον τύπο του τετραδίου. Επίσης κάτι άσχετο που είχατε γράψει προηγουμένως μπορεί να έχει εντυπωθεί και μεταφερθεί στο φύλλο που μόλις χρησιμοποιήσατε. Χρησιμοποιείστε στυλό, χαρτί και φακέλους μιας πολύ κοινής μάρκας, που την βρίσκει

κανείς παντού. Μην ταχυδρομείτε τίποτα κοντά στο σπίτι σας, ενώ αν θέλετε νε τηλεφωνήσετε για να το παραλάβουν, βεβαιωθείτε πρώτα ότι δεν σας τραβάει κάποια κάμερα από το γύρο σημείο και μην ξεχνάτε να φορέσετε γάντια πριν σηκώσετε το ακουστικό.

Περί ηλεκτρονικών συσκευών ο λόγος...

(αναδημοσίευση από το περιοδικό theorie du contexte)

Κάθε ηλεκτρονική συσκευή έχει ένα μοναδικό serial και product number, ενώ οι υπολογιστές αποστέλνουν και τη ταυτότητα τους (ip) όταν χρησιμοποιούν το internet. Φωτογραφίες, εκτυπώσεις, κείμενα, δημοσιεύσεις στο internet καθώς και οποιαδήποτε άλλη δυνατότητα παρέχουν, "σημαδεύονται και συνοδεύονται" απο τα στοιχεία της συσκευής, με τρόπο όχι πάντα ορατο με γυμνό μάτι αλλά πολυ εύκολα ανιχνεύσιμο. Έτσι αν πέσει στα χέρια της αστυνομίας κάποια ύποπτη συσκευή, είναι θέμα χρόνου να βρει σε τι περιπτώσεις εμπλέκεται.

Ιχνη από σβησμένα αρχεία...

Κάθε αρχείο που αποθηκεύουμε στο σκληρό δίσκο δεν εγγράφεται αποκλειστικά σε μια περιοχή. Είναι συνηθισμένο φαινόμενο το αρχείο να χρειάζεται δύο, τρεις ή και περισσότερους τομείς, οι οποίοι παραχωρούνται από το λειτουργικό σύστημα. Κατά τη διαγραφή λοιπόν, το μόνο που κάνει το λειτουργικό σύστημα είναι να σημειώνει ότι οι συγκεκριμένες περιοχές του δίσκου είναι ελεύθερες προς χρήση, τα περιεχόμενα όμως του αρχείου που διαγράψαμε παραμένουν εκεί και μπορούμε να τα βρούμε. Η πραγματική διαγραφή γίνεται μόνο όταν το λειτουργικό σύστημα χρειαστεί αυτές τις περιοχές για να εγγράψει ένα νέο αρχείο. Ως εκείνη τη στιγμή μπορεί να γίνει ανάκτηση με εξειδικευμένα εργαλεία. Η διαδικασία του format εμφανίζει μεν ότι όλα τα αρχεία που υπήρχαν στο δίσκο έχουν διαγραφεί, στην πραγματικότητα όμως αυτό που κάνει, είναι να πιστοποιεί ότι το μέσο μπορεί να χρησιμοποιηθεί για την αποθήκευση δεδομένων. Πρακτικά μπορεί να γίνει ανάκτηση. Τα πράγματα γίνονται πολύ δύσκολα αν υπάρξει η διαδικασία του format σε επίπεδο φυσικού μέσου. Πρόκειται για τη διαδικασία που είναι γνωστή ως low - level format. Η ανάκτηση ενός αρχείου που έχει διαγραφεί είναι εφικτή μόνο με την προϋπόθεση ότι ο τομέας που χρησιμοποιούσε δεν έχει δοθεί για την αποθήκευση άλλων δεδομένων.

Υπάρχουν εξειδικευμένες τεχνικές που μέσα σε σύντομο διάστημα μπορούν να επαναφέρουν όλα τα αρχεία που υπήρχαν στο δίσκο. Το ίδιο συμβαίνει ακόμα και αν ο δίσκος έχει υποστεί φαινομενικά ανεπανόρθωτη βλάβη. Η ανάκτηση των δεδομένων γίνεται ακόμα και αν κάποιος κόψει σε πολλά μικρά κομμάτια τις θέσεις κάποιου τομέα. Το μόνο που χρειάζεται είναι κάποιο εξειδικευμένο εργαλείο που θα συνθέσει την σελίδα ή έστω κάποιο μέρος της.

Ολα τα παραπάνω λύνονται φυσικά με την χρήση κοινόχρηστων υπολογιστών και την καταστροφή του πρωτότυπου κειμένου, αν και θέλει αρκετή προσοχή διότι πολλά internet cafe διαθέτουν κλειστά κυκλώματα παρακολούθησης.

Πληροφορίες γύρω από την παρακολούθηση, από τους τέσσερις προφυλακισμένους αναρχικούς από την υπόθεση της Ν.Φιλαδέλφειας...

Θεωρούμε σκόπιμο να δημοσιοποιήσουμε κάποιες πληροφορίες γύρω από την παρακολούθηση και ακολούθως, τη σύλληψή μας απ' τους αντιτρομοκατικάριους στις 30.04.2013 στη περιοχή της Ν. Φιλαδέλφειας. Οι περισσότερες πληροφορίες είναι «επίσημες» απ' την εις βάρος μας δικογραφία. Μέσω αυτών οδηγηθήκαμε σε κάποια συμπεράσματα που έχουν να κάνουν πιο πολύ με γνώσεις των μπάτσων πάνω στον τρόπο που «κινούμασταν» έξω παρά με τις μεθόδους της άμεσης παρακολούθησής μας. Επιπλέον, παραθέτουμε δύο λόγια για κάποιες ακόμα γνώσεις των μπάτσων που «ανακαλύψαμε», αλλά και δύο λόγια για τις τακτικές τους. Η καθυστέρηση μηνών οφείλεται στη διστακτικότητα που υπήρχε και βασιζόταν στην εκτίμηση ότι ίσως η δημοσιοποίηση βοηθούσε περισσότερο, σε τελική ανάλυση, το μελλοντικό έργο των μπάτσων. Το ζυγίσαμε όμως και καταλήξαμε ότι είναι σημαντικότερο, έστω και καθυστερημένα, να μοιραστούμε αυτες τις πληροφορίες/γνώσεις γιατί θεωρούμε πιο «ορθό» συνειδησιακά για εμάς να ξέρουν επακριβώς οι ενδιαφερόμενοι σύντροφοι το ελάχιστο επίπεδο γνώσεων της αστυνομίας, παρά να υπάρχει υποψία άγνοιας.

Σε πολλούς ίσως ακουστούν αυτονόητα πολλά εδώ μέσα, αλλά είμαστε πεπεισμένοι πως δεν θα ακουστούν έτσι για όλους. Αντιπροτάσεις προφανώς εδώ μέσα δεν μπορούμε να κάνουμε, παρά μόνο προειδοποιήσεις. Σε καμία περιπτωση όμως δεν επιχειρούμε να φοβίσουμε κανέναν για το το εύρος γνώσεων και τη δυναμική του εχθρού, αλλά να πούμε σε αυτούς που την «ψάχνουν» τι να προσέχουν στο δρόμο για την εκπλήρωση των οργισμένων επιθυμιών τους. Η «σκιά» που καλύπτει πολλές φορές τις μεθόδους και τις κινήσεις της αντιτρομοκρατικής οδηγεί ανθρώπους στην υπερτιμησή τους, ενώ είναι αλήθεια πως παρ' ότι κάποια πράγματα μας γνωστοποιούνται κάπου κάπου πόλλα άλλα σημεία παραμένουν στο σκοτάδι. Οι ίδιοι οι μπάτσοι δεν αποκαλύπτουν σχεδόν ποτέ τις μεθόδους τους. Απ' την άλλη όμως παρ' ότι οφείλουμε να λαμβάνουμε τα μέτρα μας απεναντί τους, ένα ρίσκο σε ατομικό ή ομαδικό επίπεδο θα παραμένει πάντα σε ένα υποκειμενικό πεδίο. Όπως και να έχει όμως λάθη γίνονται και θα συνεχίσουν να γίνονται στη μάχη ενάντια σε τόσο ισχυρούς κατασταλτικούς μηχανισμούς. Λάθη που πάντα θα «στοιχίζουν» περισσότερο αντίθετα με τα λάθη των μπάτσων που «απορροφούνται». Οι καταστάσεις πρέπει να ζυγίζονται ξανά και τα λάθη που έχουν γίνει μία φορά, πολύ απλά, δεν πρέπει να ξαναγίνουν. Η συσσωρευμένη εμπειρία τόσων χρόνων πρέπει να μελετάται και να εκτιμάται και επειδή υπάρχει η τάση να προετοιμαζόμαστε για τις μάχες που ήδη έγιναν και όχι για αυτές που θα 'ρθουν ας είμαστε σε ετοιμότητα και η τύχη μαζί μας...

Ξεκινώντας, να πούμε ότι η «επίσημη» παρακολούθηση μας ξεκίνησε στις 11:20 το πρωί με τον εντοπισμό του Γρηγόρη (Σαραφούδη) και έληξε στις 16:00 με τις συλλήψεις μας στη Νέα Φιλαδέλφεια. Έχουμε βάσιμους λόγους να πιστεύουμε ότι η παρακολούθηση μας ξεκίνησε εκείνη την ώρα. Γιατί λίγο πριν από την προαναφερόμενη ώρα ο σύντροφος πήγε στο ίντερνετ-καφέ Palladium στη Σολωμού 48 στα όρια Εξαρχείων με το κέντρο της Αθήνας. Πιστεύουμε βασικά ότι το συγκεκριμένο καφέ βρισκόταν/βρίσκεται υπό παρακολούθηση, απ' την στιγμή κιόλας που πληροφορηθήκαμε ότι διάφοροι σύντροφοι κατά το παρελθόν έχουν παρακολουθηθεί από ασφαλίτες φεύγοντας από εκεί. Επίσης, ένας ακόμα βασικός λόγος που μας προσδιορίζει πάνω κάτω την ώρα είναι το γεγονός πως νωρίτερα εκείνο το πρωί ο σύντροφος είχε κάνει «τσεκ» αντιπαρακολούθησης και βεβαιώθηκε ότι δεν παρακολουθείται η κινησή του. Ένα συνηθισμένο τσεκ που κάναμε πολύ συχνά και πάντα πριν απο οποιαδήποτε συνάντηση με καταζητούμενους ή αγνώστους στην αστυνομία συντρόφους, για να βεβαιωθούμε ότι είμαστε «καθαροί». Με άλλα λόγια δηλαδή, πιθανολογούμε

πολύ σοβαρά ότι το «κακό» έγινε όταν «καθαρός» άνθρωπος μπήκε σε «βρώμικο» μέρος και εφόσον ήταν ήδη γνωστός στην αντιτρομοκρατική από παλαιότερη παρακολούθηση, αναγνωρίστηκε και τέθηκε υπό διακριτική παρακολούθηση. Η συνάντηση όμως λίγες ώρες αργότερα με τους δύο καταζητούμενους συντρόφους Αργύρη (Ντάλιο) και Φοίβο (Χαρίση) σήμανε συναγερμό στην αντιτρομοκρατική και έπεσε αμέσως εντολή για συλλήψεις. Οι μπάτσοι κλασσικά για να δικαιολογήσουν την παρακολούθηση λένε στη δικογραφία για «ανώνυμο τηλεφώνημα» προς τις υπηρεσίες τους που ανέφερε ότι ο Γρηγόρης και άλλοι σύντροφοι της ίδια υπόθεσης κατείχαν όπλα, συμμετείχαν σε λιστεία του Βελβεντού και επισκέπτονταν συχνά την περιοχή των Εξαρχείων. Με αυτόν τον τρόπο κιόλας, θέλησαν να απεμπλέξουν το συνεργάζομένο ίντερνετ-καφέ για να μην στοχοποιηθεί, και έτσι έγραψαν στη δικογραφία ότι εντόπισαν το Γρηγόρη τυχαία στην διασταύρωση Πατησίων και Σολωμού, δηλαδή 30 μέτρα πιο κάτω! Παρόλα που ξέρουμε ότι δεν ισχύει αυτή η γελοιότητα με το ανώνυμο τηλεφώνημα δεν αποκλείουμε την πιθανότητα ο Γρηγόρης, για άγνωστο λόγο, να θεωρούνταν ήδη ύποπτος και να μπήκε δυναμικά στο στόχαστρο της αντιτρομοκρατικής. Το στόρυ, χονδρικά, μετά την επίσκεψη του Γρηγόρη στο «βρώμικο» ίντερνετ-καφέ, συνεχίζει με την συναντησή του λίγη ώρα μετά σε άλλο σημείο της πόλης με τον , επίσης «τσεκαρισμένο», σύντροφο Γιάννη (Ναξάκη). Στη συνέχεια οι δύο σύντροφοι κινήθηκαν σε διάφορα μέρη, για να καταλήξουν μετά από κάποια ώρα στη Νέα Φιλαδέλφεια στο ραντεβού με άλλους συντρόφους, όπου και εκεί τελειώνει λίγη ώρα μετά το στόρυ με την επέμβαση της αντιτρομοκρατικής. Κατά την διάρκεια όμως αυτών των λίγων ωρών, οι υπό παρακολούθηση σύντροφοι έκαναν κάποιες κινήσεις που μπορεί από νομικής άποψης να είναι αδιάφορες, όμως, ήταν ικανές να «προδώσουν» κάποια συνωμοτικά χαρακτηριστικά γύρω απ' το πως κινούμασταν.

Εχουμε και λέμε:

1. Στις τέσσερις και κάτι ώρες παρακολούθησης μας είδαν να πηγαίνουμε σε τέσσερα διαφορετικά ίντερνετ- καφέ. Πρώτο ήταν το Palladium που πήγε ο Γρηγόρης. Το επόμενο ήταν επί της Πατησίων 382 κοντά στο σταθμό ΗΣΑΠ Άνω Πατησίων, απέναντι από τα everest όπου μέσα συναντήθηκαν ο Γρηγόρης με τον Γιάννη. Οι δυό τους αργότερα πήγαν στο GNet στα Μαρούσι (Τσαλδάρη 3 και Αριστείδου), ενώ τελευταίο ήταν το Bits&Bites στη Νέα Φιλαδέλφεια (Δεκελείας 138) όπου εκεί συνάντησαν τον Αργύρη και τον Φοίβο. Με αυτά τα δεδομένα οι μπάτσοι έχουν βάσιμες πληροφορίες ότι χρησιμοποιούσαμε το ίντερνετ για να επικοινωνούμε μεταξύ μας. Ξέρανε σίγουρα ότι «κατεβάζαμε» και χρησιμοποιούσαμε το λογισμικό Tor Browser Bondle (θα ακολουθήσει σύντομα εκτενές κείμενο για την λειτουργία και την ασφάλεια του λογισμικού Tor) ένα πρόγραμμα για ασφαλή περιήγηση που ανακατεύει τις I.P. του παγκόσμιου δικτύου των χρηστών του, κάνοντας με αυτόν τον τρόπο την περιήγηση πιο «ελεύθερη», αφού σαν I.P. (που είναι και το στοιχείο που προδίδει τη γεωγραφική θέση του περιηγητή) εμφανίζεται μία άλλη από ένα άλλο τυχαίο μέρος του πλανήτη. Ακόμα όμως και με αυτό το δεδομένο εκτιμούμε ότι οι χάκερ της ελληνικής αστυνομίας δεν έχουν την δυνατότητα να «αποκρυπτογραφήσουν» τη διαδρομή μας στον Tor γιατί δεν είναι θέμα αποκωδικοποίησης αλλά θέμα ξεμπλεξίματος ενός τεράστιου κουβαριού με I.P. και για να βρεθεί άκρη του νήματος είναι μία υπερβολικά χρονοβόρα και περίπλοκη διαδικασία που στην περιπτωσή μας κιόλας πρέπει να γίνει ακριβώς ανάποδα. Γενικά, με τον Tor αισθανόμασταν ασφαλείς μέχρι που μάθαμε ότι πρόσφατα (6 Αυγούστου) χάκερ του FBI «έσπασαν» για πρώτη φορά πολλές σελίδες του Tor, καταφέρνοντας να παγιδεύσουν και να συλλάβουν ένα μεγάλο παγκόσμιο Δίκτυο παιδόφιλων, κάτι που εμάς μας δημιούργησε κάποιες μικρές ανησυχίες σε σχέση με τα στεγανά του. Ένα λάθος που κάναμε σίγουρα είναι ότι "κατεβάζαμε" τον Tor στο pc του ίντερνετ-καφέ που καθόμασταν , αντί να το έχουμε αποθηκευμένο σε φλασάκι μαζί μας, κάτι που πέρα απ το ότι μπορεί να φανεί στη κεντρική μονάδα, στο κεντρικό pc του μαγαζιού, θεωρητικά είναι εφικτό να φτάσει ειδοποίηση ακόμα και απευθείας στους μπάτσους, μέσω προγράμματος, αν έχουν συννενοηθεί πρώτα με το μαγαζί. Σε σχέση με τα ίντερνετ-καφέ τώρα, μας έχει μεταφερθεί η κακή είδηση ότι στο διάστημα που μεσολάβησε από τότε μέχρι σήμερα, κόσμος έχει ακολουθηθεί από ασφαλίτες βγαίνοντας από διάφορα τέτοια μαγαζιά της Αθήνας (Εξάρχεια, Μοναστηράκι, Νέος Κόσμος, Καλλιθέα) κάτι που μας λέει ότι πλέον δεν θα είναι και λίγα αυτά που θα παρακολουθούνται σε όλη την Αθήνα. Μην ξεχνάμε

κιόλας ότι οι δυνατότητες των μπάτσων είναι αρκετά μεγάλες αν σκεφτούμε ότι μόνο στη ΔΑΕΕΒ (αντιτρομοκρατική) απασχολούνται 600 άτομα, όπως έχει δηλωθεί μέσα σε δικαστήριο απ' τους ίδιους όταν ερωτήθηκαν.

2. Μας είδαν στο άλσος Συγγρού στη Κηφισιά. Οι δυό μας (Γρηγόρης- Γιάννης) πριν κατευθυνθούμε προς την Νέα Φιλαδέλφεια κάναμε μία στάση στο άλσος περπατήσαμε μέχρι τα γηπεδάκια, κάτσαμε σε ένα παγκάκι ακριβώς δίπλα και μιλήσαμε μεταξύ μας για πολύ ώρα.

Να σημειωθεί ότι άλες αυτές τις ώρες που μας παρακολουθούσαν, αν και ήμασταν τσεκαρισμένοι και θεωρητικά πιστεύαμε ότι ήμασταν καθαροί, στις λίγες αντανακλαστικές ματιές που ρίξαμε πίσω μας, από συνήθεια, δεν παρατηρήσαμε τίποτα το ιδιαίτερα ανησυχητικό ενώ κινηθήκαμε σε πολλά διαφορετικά μέρη (ηλεκτρικό, λεωφορείο, ταξί).

Επιπλέον πράγματα που μάθαμε και συμπεράναμε απο τη μέρα της σύλληψης σε σχέση με το πως δουλεύουν οι μπάτσοι.

Μας αιφνιδίασαν πραγματικά όταν 80 μέτρα πιο κάτω απ' τη καφετέρια στη Νέα Φιλαδέλφεια ενώ δύο από εμάς (Γρηγόρης-Γιάννης) περπατούσαμε φεύγοντας, μας έκαναν σήμα οι ΔΙ.ΑΣ να σταματήσουμε για έλεγχο. Αν περιμέναμε κάτι σχεδιασμένο αυτό σιγουρα δεν ήταν οι ΔΙ.ΑΣ. σε μία κεντρική διασταύρωση της περιοχής, αλλά κάποιου άλλους είδους «πέσιμο». Μετά το σήμα, αφού μας πλησίασαν περπατώντας, είδαμε, δευτερόπλεπτα μετά, να φανερώνονται και άλλες δυνάμεις γύρω γύρω μέχρι που σε λίγα λεπτά ήμασταν εγκλωβισμένοι, κάτι που μας λέει πως και οπλισμένοι να ήμασταν θα ήταν μικρές οι πιθανότες να ξεφεύγαμε. Απ' την άλλη όμως, όπως είναι γνωστό ήδη, στη καφετέρια που πραγματοποιήθηκε επιχείρηση μερικά λεπτά αργότερα η τακτική τους με δόλωμα τους ΔΙ.ΑΣ δεν είχε ακριβώς τα αποτελέσματα που θέλανε καθώς ξέφυγε ένα άτομο.

Ακόμα, κάτι για το οποίο δεν ήμασταν όλοι σίγουροι, αλλά σιγουρευτήκαμε πλέον, είναι η δυνατότητα των μπάτσων σε οποιοδήποτε τμήμα της χώρας να ταυτοποιούν άμεσα τα στοιχεία μίας πλαστής ταυτότητας με τον αληθινό κάτοχο μέσω μίας φωτογραφίας. Ο Γιάννης, ο οποίος προσήχθει αρχικά στο αστυνομικό τμήμα της Νέας Φιλαδέλφειας, ήταν σε θέση να δει τους μπάτσους να πατάνε σε υπολογιστή τους τα στοιχεία απ' την πλαστή ταυτότητα που κατείχε και να εμφανίζεται στην οθόνη φωτογραφία με το πρόσωπο του αληθινού κατόχου.

Είναι σημαντικό να σταθούμε σε μία βασική διαφοροποίηση της τακτικής της αντιτρομοκρατικής στη περίπτωση των συλλήψεών μας, σε σχέση με παρελθοντικές επιχειρήσεις της ίδιας υπηρεσίας εναντίον ένοπλων ομάδων (Σ.Π.Φ, Ε.Α, συλλήψεις Πειραιά- Ν. Σμύρνη, συλλήψεις Βύρωνα-Ταύρο). Σε όλες αυτές τις παλαιότερες υποθέσεις η τακτική των μπάτσων ήταν η εξής: έχοντας αναλύσει από πριν το προφίλ και τις συναναστροφές των καταζητούμενων συντρόφων με άλλους «νόμιμους», έθεταν τους τελευταίους υπό παρακολούθηση ωστε να τους οδηγήσουν στους παράνομους. Προφανώς, η αντιτρομοκρατική υπηρεσία δεν διενεργεί «μονοδιάστατες» έρευνες, ούτε θα αρκούνταν σε αυτό, σχηματικά όμως και μέσα από τη συσσωρευμένη εμπειρία των τριών τελευταίων χρόνων παρατηρούμε πως παρά τις εκάστοτε διαφοροποιήσεις, ο πυρήνας της έρευνας και των επιτυχιών της βρίσκεται στο παραπάνω «απλό» μοντέλο. Στις προηγούμενες περιπτώσεις λοιπόν, όταν η ΔΑΕΕΒ «ανακάλυπτε» τους καταζητούμενους συντρόφους ποτέ δεν επιχείρησε να τους συλλάβει επί τόπου, αντίθετα τους έθεσε ύπο παρακολούθηση αρκετές μέρες με σκοπό αφενός να βρεί τις «γιάφκες» και τον οπλισμό των συντρόφων και αφετέρου τον κύκλο των επαφών τους. Τα παραδείγματα χαρακτηριστικά: στην περίπτωση των συντρόφων που συνελήφθησαν σε Ν.Σμύρνη-Πειραιά η παρακολούθηση σύμφωνα με τα επίσημα έγγραφα της δικογραφίας διήρκησε 17 μέρες. Αντίστοιχα 9 μέρες παρακολουθούσε, πριν επέμβει η αντιτρομοκρατική, τα σπίτια των θεσσαλονικιών συντρόφων σε Βύρωνα- Ταύρο καθώς και το σπίτι στο Βόλο που έμεναν τα μέλη στης ε.ο.Σ.Π.Φ.. αντιθέτως στη δική μας περίπτωση η αντιτρομοκρατική επέλεξε να μας συλλάβει κατ΄ ευθείαν και όχι να μας παρακολουθήσει για δύο λόγους. Ο πρώτος λόγος και σημαντικοτερος, ήταν πως στο παρελθόν πολλοί σύντροφοι (μέσα σε αυτούς

και κάποιοι από εμάς) είχαν γλυτώσει από επιχειρήσεις της αντιτρομοκρατικής εξαιτίας των μεθόδων αντιπαρακολούθησης που εφάρμοζαν. Οι μπάτσοι είτε τους έχαναν, είτε για να μην καρφωθεί η συνολική επιχειρησή τους, τους άφηναν. Ο δεύτερος λόγος ήταν πως λόγω των σύγχρονων μεθόδων καταστολής (βλέπε DNA) οι μπάτσοι είναι πιο σίγουροι απ' ότι στο παρελθόν πως θα φυλακιστούμε και θα καταδικαστούμε ακόμα και χωρίς «γιάφκες», «άπλα» κτλ.

Καταληκτικά, το συμπέρασμα που βγάζουμε είναι πως ο εχθρός προσαρμόζεται ταχύτατα στις συνθήκες και εξελίσσεται διαρκώς, αλλά και πολλές φορές δημιουργεί ο ίδιος ουσιαστικά τις συνθήκες στις οποίες θα έχει την πρωτοβουλία των κινήσεών. Από μεριάς μας δεν αρκεί να μένουμε στις δοκιμασμένες και πετυχημένες συνταγές του παρελθόντος αλλά να κοιτάμε πάντα μπροστά, να είμαστε αυτό που λένε. ένα βήμα μπροστά τους. Περιμένοντας το χειρότερο δεν μπορεί παρά να γινόμαστε πάντα καλύτεροι. Μέσα απ' αυτό το κείμενο άλλωστε, επιδιώκουμε την εξέλιξη της δράσης μέσα απ' το μοίρασμα της εμπειρίας. Πιστεύουμε πως τέτοια είδους επικοινωνία είναι αναγκαία, έστω και με αυτόν τον τρόπο (η άμεση επαφη μεταξύ ενδιαφερομένων και αδύνατη είναι και επικίνδυνη) και γενικά πως έχει ουσιαστικό νόημα διωκώμενοι και φυλακισμένοι να βγάζουν τέτοιες πληροφορίες προς τα έξω. Πράγματα που ξέρει και ο εχθρός είναι καλό να μην μένουν μυστικά στους κύκλους μας, απ' την στιγμή που «προσανατολίζουν» στο τι ξέρει και μπορεί να μας χρησιμεύσουν. Υπάρχει βέβαια και η περίπτωση κάποια πληροφορία να μένει μυστική στη βάση της στρατηγικής, στη βάση ενός πλάνου, μίας εκ νέου αιφνιδιαστικής επίθεση στα μούτρα του εχθρού.

Προφυλακισμένοι από την υπόθεση της Ν. Φιλαδέλφειας.

Ντάλιος Αργύρης, Χαρίσης Φοίβος, Ναξάκης Γιάννης, Σαραφούδης Γρηγόρης

Κείμενο του φυλακισμένου αναρχικού Γιάννη Μιχαηλίδη 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 συναλικό 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.

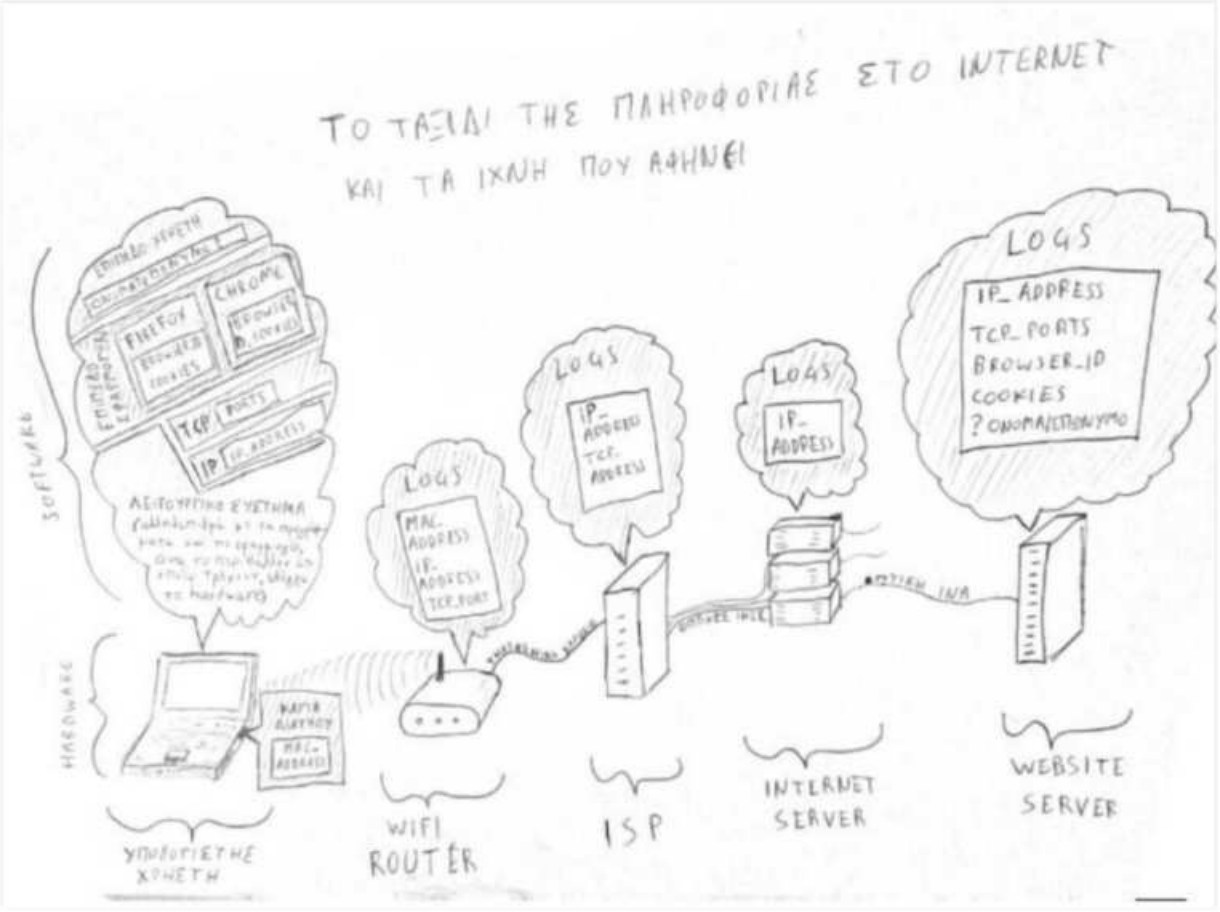
Η διαδικασία της ταυτοποίησης και του εντοπισμού

Υπάρχουν πολλοί τρόποι να αποκαλυφθεί η θέση και η ταυτότητα κάποιου στα 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.



As 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. Ετσι 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

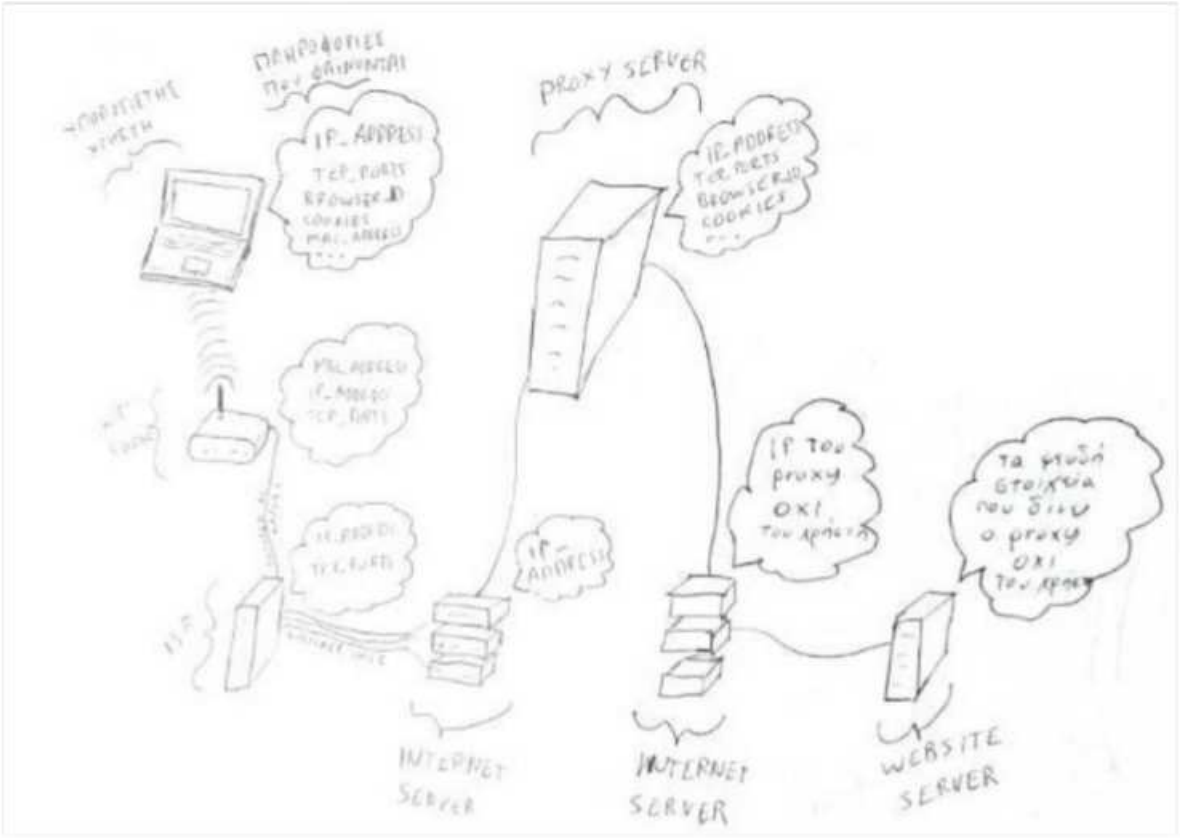
σε έναν υπολογιστή από το δίκτυο της καφετέριας. Αντί να συλλάβουν τον ιδιοκτήτη της καφετέριας θα ψάξουν άλλα ίχνη που άφησε πίσω του ο υπολογιστης σου. Πιθανόν να είναι καταγεγραμμένη η mac address (η φυσική διεύθυνση της κάρτας δικτύου) στον wifi router της καφετέριας. Αυτή είναι μοναδική για κάθε 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 λουκέτο. 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 ιδιάτητες 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.

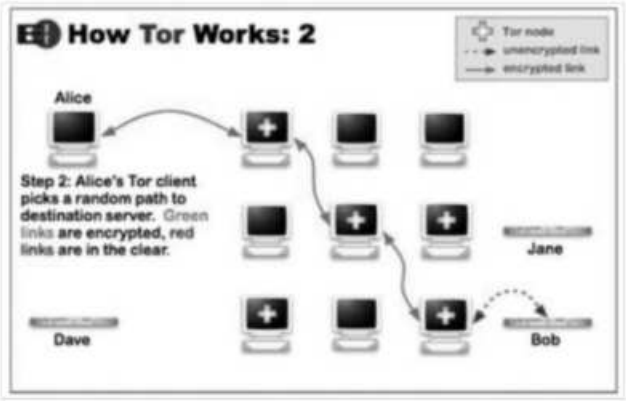
Δεν ισχύει το ίδιο όμως για κάθε επιμέρους υλοποίηση της ασύμμετρης κρυπτογραφίας. Σε κάθε υλοποίηση μπορεί να υπάρχουν αδυναμίες. Αυτές σχετίζονται συνήθως με τους τυχαίους κωδικούς που παράγονται από τα προγράμματα αυτά με τη βοήθεια του λειτουργικού συστήματος, και οι κωδικοί παράγονται από ψευδοτυχαίους 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 σημαίνει 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

As 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 κωδικάς 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.

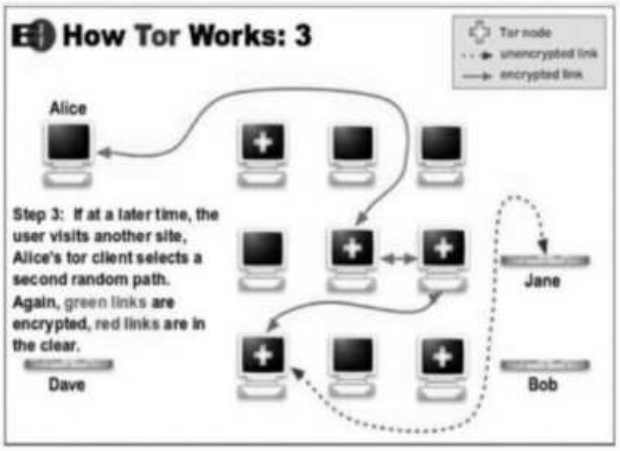
Σε αυτό το σημείο η κρυπτογράφηση προσομοιάζει με κρεμμύδι γιατί έχει πολλαπλά στρώματα.

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 αποστέλει 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 κρυπταγραφημένη ροή χωρίς να μπορεί να κρυφακούσει τίποτα.



Γιατί να το εμπιστευτούμε;

Οπως 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.

Ομως 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. Ενα 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.

Ομως 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).

Ελεύθερο 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 σύστημα 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 συνιστά επαγρύπνηση, παρέχοντας την ισχυρότερη low latency ανωνυμία.

Όπως είδαμε η δύναμη του βασίζεται στη χαοτικότητα του και στην εξελιγμένη κρυπταγραφία.

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 δραστηριότητά 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.

Ενας 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 παρόμοια 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: Οπως 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.

Ομως 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 διάρθωνε 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 ότί 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 ότί 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 Γερμανοί έχασαν το προβάδισμα στον πόλεμο και σημαντικές υποκλαπείσες πληροφορίες συνέβαλλαν στη συντριβή τους.

Ενα 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.

Ομως 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.

Υποκλοπές Τηλεπικοινωνιών...

(αναδημοσίευση από μπροσούρα «καταστολή στην Ιταλία»)

Σήμερα αντιπροσωπεύουν τη συντριπτική πλειονότητα των υποκλοπών που χρησιμοποιούνται για παραπομπές σε δίκη.Το κινητό τηλέφωνο αποτελείέναν κατάσκοπο από μόνο του,ή μ'άλλα λόγια οποιαδήποτε συσκευή κινητής τηλεφωνίας μπορεί ανά πάσα στιγμή να υποκλαπεί.Ο κατασταλτικός μηχανισμός του αρμόδιου ιταλικού υπουργείου είναι επιφορτισμένος με την παρακολούθηση των παρόχων τηλεφωνίας, οι οποίοι υποχρεούνται να κάνουν διαθέσιμες τις τεχνολογικές και οργανωτικές τους δομές.Οι τηλεφωνικές γραμμές που μπαίνουν στο στόχαστρο ερευνών υποκλέπτονται από το Κέντρο Τηλεφωνικών Υποκλοπών (Centro Intercettazioni Telefoniche,CIT) της Εισαγγελίας, κατ' εντολή της οποίας εγκαινιάζεται η εκάστοτε έρευνα, και στη συνέχεια όλη η διερχόμενη κίνηση του κινητού τηλεφώνου, τόσο τα SMS (γραπτά μηνύματα) όσο και οι ηχητικές συνομιλίες,παρακολουθούνται και καταγράφονται σε αρχεία.

Πέραν αυτών, το κινητό τηλέφωνο μπορεί να εντοπιστεί.Το σύστημα εντοπισμού ποικίλλει ανάλογα με το μοντάλο του τηλεφώνου.Τα κινητά που δεν έχουν ενσωματωμένο GPS(παγκόσμιο σύστημα θεσιθεσίας) μπορούν να εντοπιστούν μέσω της μεθόδου τριπλευρισμού στους αναμεταδότες, κι έτσι αποδίδουν λιγότερο ακριβή εντοπισμό, με περιθώριο απόκλισης περίπου 800 μέτρων.,ενώ τα σύγχρονα κινητά αποφέρουν ακριβή εντοπισμό εντός 3 μέτρων.
Συχνά αυτό που υποκλέπτεται είναι ο μοναδικός αριθμός IMEI(της διεθνούς ταυτότητας αναγνώρισης κινητής συσκευής), έτσι ακόμη και αν αλλάξετε την κάρτα στην υποδοχή ή τοποθετήσετε μία "καθαρή" κάρτα κινητού, η ίδια η συσκευή είναι αυτή που υποκλέπτεται.

Ενα άλλο χρήσιμο πράγμα που πρέπει να γνωρίζετε ότι τα σύγχρονα κινητά τηλέφωνα σαν τα smartphones μπορούν να εντοπιστούν σε κάθε περίπτωση,ακόμα κι αν έχουν απενεργοποιημένο έναν εντοπιστή τους.

Μέχρι σήμερα δεν κατέχουμε στέρεες αποδείξεις για τη χρήση κλειστών κινητών τηλεφώνων ή για υποκλοπές σε εξωτερικό περιβάλλον που να έχουν γίνει με μικρόφωνο απενεργοποιημένο ΄αποσυνδεδεμένο.Αυτό που είναι σίγουρο είναι ότι η τεχνολογική εξέλιξη έχει κάνει τεράστια βήματα, γι' αυτό είναι μια καλή πρακτική ναμην χρησιμοποιείτε κινητά τηλέφωνα σε ορισμένους τύπους δράσεων, να

τ'αφήνετε στο σπίτι ή τουλάχιστον να βγάζετε την μπαταρία και την κάρτα SIM αν θέλετε να έχετε μία συνομιλία με άτομα της προτίμησής σας έχοντας ήσυχο το κεφάλι σας.

(αναδημοσίευση από το περιοδικό theorie du contexte)

Για την αντιπαρακολούθηση...

Αντιπαρακολούθηση είναι κάθε ενέργεια που βοηθά στο να αποφεύγεται ή να γίνεται δύσκολος ο έλεγχος μας μέσω της παρακολούθησης.Κύρια προτεραιότητα της αντιπαρακολούθησης είναι η προστασία κάθε είδους πληροφορίας.Οι άνθρωποι δημιουργούν συνήθειες μέσα από τις οποίες είναι εύκολο να καταγραφούν οι ενέργειές τους.Σπάζοντας τις συνήθειες που έχουμε μέσα στην καθημερινότητα δυσκολεύουμε πολύ την συστηματική παρακολούθηση, χωρίς αυτό να σημαίνει ότι χριεάζεται να αλλάζουμε τις ώρες των σταθερών ή αμετάκλητων υποχρεώσεών μας γενικά.Αντίθετα συνήθως είναι καλύτερα κάθε ενέργεια που δεν θέλουμε να εντοπίζεται, να είναι ενσωματωμένη μέσα στην κθημερινότητά μας.Όσο προσπαθούμε να εμποδίζουμε την παρακολούθηση των προσωπικών μας ραστηριοτήτων, άλλο τόσο πρέπει να φροντίζουμε και για ανθρώπους που ερχόμαστε σε επαφή.Χρειάζεται σχεδιασμός για να προστατέψουμε μία πληροφορία και δεν είναι κάτι που γίνεται αυτόματα.Μπορούμε να προστατεύουμε πληροφορίες που είναι πολύ «ευαίσθητες» και ταυτόχρονα να αφήνουμε άλλες που είναι ασήμαντες, ορατές σε όλους.Είναι θέμα προτεραιοτήτων ποιες θα προστατέψουμε και ποιές όχι.Αν προσπαθούμε να προστατέψουμε και πληροφορίες που δεν είναι ευαίσθητες, τότε υπάρχει το ενδεχόμενο να δημιουργηεί ένας πολύ μεγάλος όγκος πληροφοριών, που θα πρέπει να κρατάμε συνεχώς μακριά από παρακολούθηση.Όσες περισσότερες πληροφορίες,τόσο πιο δύσκολη γίνεται η παρακολούθηση,αλλά ταυτόχρονα είναι πιθανό να απομονωθούμε και να εμφανιστούμε ως ύποπτοι.

1) Κάντε συνήθεια και κομμάτι της καθημερινότητάς σας την παρατήρηση του χώρου που ζείτε και κινείστε.Εξοικιωθείτε με το περιβάλλον σας και για μεγαλύτερη ευκολία προσπαθήστε να θυμάστε τα οχήματα τα οποία παρκάρουν στη γειτονιά σας.Μην αγνοείτε ύποπτες κινήσεις που συμβαίνουν γύρω σας.
2) Κρατήστε το όχημά σας σε καλή λειτουργική κατάσταση και φροντίζετε το ντεπόζιτό σας είναι πάντα μισογεμάτο.
3) Ανα δεν έχετε καθρέφτες,βάλτε,ρυθμίστε τους σωστά και αρχίστε να τους χρσιμοποιείτε.

Σε περίπτωση που θέλετε να διαπιστώσετε αν σας ακολουθούν:

4) Περάστε με κόκκινο ή μπείτε ανάποδα σε δρόμο μονής κατεύθυνσης και δείτε αν και τι σας ακολουθεί.
5) Ενώ οδηγείτε με ταχύτητα σε δρόμο ταχείας κυκλοφορίας με τρεις τουλάχιστον λωρίδες και αφού έχετε τσεκάρει τι ακολουθεί πίσω σας κάνετε όσο πιο απότο μδεξιά και βγείτε από αυτόν.
6) Μετά από μία «τυφλή» στροφή/ γωνία και αφού προηγουμένως έχετε «κερδίσει» κάποια απόσταση κάντε αναστροφή και πάρτε την αντίθετη κατεύθυνση.
7) Μετά από μία «τυφλή» στροφή/ γωνία παρκάρετε και παρατηρήστε διακριτικά τί οχήματα θα περάσουν ή θα ακολουθήσουν την κίνησή σας.
8) Κάντε τον κύκλο ενός τετραγώνου και ξαναβγείτε στο ίδιο σημείο.

9) Εμπλουτίστε τη διαδρομή σας με δρόμους ήπιας κυκλοφορίας, πεζοδρόμους,σκαλάκια,πεζογέφυρες ή οτιδήποτε άλλο παράδοξο μπορεί να εκθέσει όσους σας ακολουθούν.

10) Τοποθετήστε σε κάποιο στατικό σημείο πάνω στη διαδρομή σας ένα φίλο, ο οποίος θα έχει τη δυνατότητα να καταλάβει αν σας ακολουθούν.Αν πάλι δεν μπορεί να είναι σίγουρος, ας σημειώσει τα οχήματα τα οποία σας ακολουθούν και ας βιαστεί να μεταφερθεί σε κάποιο επόμενο σημείο της διαδρομής, ώστε να τα επαληθεύσει.

Η παρούσα μπροσούρα αποτελεί συλλογή-συγκέντρωση δημοσιευμένων κατά καιρούς κειμένων για την αυτοπροστασία απέναντι στις καταστολτικές μεθόδους. Από τη γνώση για τις παρακολουθήσεις κινητών τηλεφώνων και ηλεκτρονικών συσκευών, μέχρι την πρόληψη για την όσο το δυνατόν καλύτερα «καλυμμένη» δράση μας και την αντιπαρακολούθηση, σημασία έχει από την πλευρά μας η κατάκτηση της συλλογικής εμπειρίας για το πώς θα αντιδράσουμε αν βρεθούμε στα χέρια τους, μα ακόμη καλύτερα πως θα δράσουμε για να μην βρεθούμε σε αυτά.

Εκδόθηκε με σκοπό, όχι προφανώς να ανάξει την εξουσία σε άτρωτη και να τρομοκρατήσει, αλλά να συμβάλει, στο βαθμό που είναι εφικτό, στη συνειδητοποίηση συντρόφων και συλλογικοποιήσεων γύρω από τις τεχνικές της κυριαρχίας, της εφαρμογής τους σε πρακτικό επίπεδο και της αντιμετώπισής τους, η κρισιμότητα της οποίας είναι μεγάλη για τη συνέχιση και εξέλιξη της πολύμορφης δράσης μας.

ελεύθερη συνεισφορά
τα έσοδα θα διατεθούν για την υποστήριξη διωκώμενων και φυλακισμένων αγωνιστών/στριών