ΛΟΝΔΙΝΟ ΚΑΛΕΙ:*Μια τηλεφωνική και διαδικτυακή δικλίδα ασφαλείας των εγκληματικά σκεπτόμενων αναρχικών.*
(Η μπροσούρα στα αγγλικά ***https://ia803107.us.archive.org/33/items/LondonCallingACellphoneAndInternetSecurityPrimer/london_calling.pdf*** *)*

Καλύψου για να μην σε παρακολουθούν: Η ασφάλεια ως μείωση βλάβης.

Υπάρχει ένας δίκαιος σκεπτικισμός,ασαφείς μηνύματα και γενικότερη σύγχυση στην εγκληματικά σκεπτόμενη πολιτική σκηνή αυτές τις ημέρες για το τι αποτελεί μια καλή ασφάλεια όσον αφορά την τεχνολογία. Θέλουμε να προσπαθήσουμε να αποσαφηνίσουμε κάποια πράγματα και να σε βοηθήσουμε να προστατευτείς ενάντια στην παρακολούθησης. Όπως στο σεξ, δεν υπάρχει απόλυτη ασφάλεια όσο χρησιμοποιείς την τεχνολογία, αλλά τουλάχιστον μπορούμε να μειώσουμε τη βλάβη. Αυτήν η μπροσούρα δεν αφορά την κουλτούρα ασφαλείας, μια έννοια που έχουμε δυνατά και αντικρουόμενα συναισθήματα, παρόλο που υπάρχει μια σύνδεση ανάμεσα σ'αυτήν και την τεχνολογική παρακολούθηση στα διαδικτυακά κοινωνικά δίκτυα. Τη μοναδική συνολική ιδέα στην ασφάλεια που θα θέλαμε να εκφράσουμε είναι η διαχείριση κινδύνου: να γνωρίζεις τους κινδύνους, σύγκριση μεταξύ ευκολίας και ανάγκης και λήψης μιας τεκμηριωμένης απόφασης. Παρομοίως, οι νόμοι περί παρακολούθησης είναι εκτός αντικειμένου αυτής της μπροσούρας, καθώς μας ενδιαφέρει περισσότερο το τι μπορούν να κάνουν οι μπάτσοι από το τι είναι νόμιμο να κάνουν. Ακόμα και αν δεν μπορούν να χρησιμοποιήσουν τις πληροφορίες που έχουν συλλέξει στο δικαστήριο, μπορεί να βοηθήσει στην έρευνά τους.

Mulder? It's me: Μπάτσοι και κινητά.

Θέλουμε να δώσουμε έμφαση στο πόσο εύκολο είναι για τους κακούς να αποκτήσουν πρόσβαση στο κινητό,τις κλήσεις και τα αρχεία σου. Δεν χρειάζεται να υπάρχει ένα άτομο με ακουστικά, ακούγοντας τη συζήτηση σου σ'ένα παρκαρισμένο όχημα (παρόλο που αυτό λειτουργεί, τα κινητά στέλνουν ραδιοκύματα που είναι εύκολα να τα υποκλέψεις), σήμερα έχουν ένα ευρύ δίκτυο παρακολούθησης που λέγεται DCSNet που κάνει όλη τη δουλειά γι'αυτούς.

"Το FBI αθόρυβα δημιούργησε ένα προηγμένο point-and-click σύστημα παρακολούθησης που αυτόματα τοποθετεί κοριό σ'όλες τις συσκευές επικοινωνίας σύμφωνα με πρόσφατη κυκλοφορίας απόρρητων εγγράφων 1000 σελίδων υπό το "Freedom of Information" νομοσχέδιο. Το σύστημα παρακολούθησης DCSNet, για το Digital Collection System Network, συνδέει το FBI με δωμάτια παρακολούθησης

που ελέγχονται με διακόπτη από παρόχους σταθερής τηλεφωνίας, διαδικτυακούς-τηλεφωνικούς προμηθευτές και εταιρίες κινητής τηλεφωνίας. Είναι αρκετά πιο περίπλοκα πλεγμένος στο εθνικό σύστημα τηλεπικοινωνιακής υποδομής απ' ό,τι περιμέναμε. " Είναι ένα ευρύ σύστημα παρακολούθησης που υποκλέπτει ενσύρματα τηλέφωνα, ασύρματα, SMS και συστήματα τύπου push to talk", λέει ο Steven Bellovin, Καθηγητής της επιστήμης υπολογιστών στο πανεπιστήμιο Columbia και χρόνια ειδικός στις παρακολουθήσεις…

Το DCSNet είναι μια σύνθεση software που συλλέγει, κοσκινίζει και αποθηκεύει τηλεφωνικά νούμερα, κλήσεις και μηνύματα. Το σύστημα συνδέει απευθείας σταθμούς παρακολούθησης του FBI σε ιδιωτικά δίκτυα επικοινωνίας της χώρας. Ο $10 εκατομμύρια πελάτης DCS-3000, γνωστός ως Red Hook, διαχειρίζεται τα pen-registers και trap-and-traces, τύπου παρακολούθησης που συλλέγει πληροφορίες σε μορφή σήματος – κυρίως τους αριθμούς που πληκτρολογούνται στα τηλέφωνα – αλλά όχι το περιεχόμενο επικοινωνιών. (Τα Pen registers καταγράφει εξερχόμενες κλήσεις ενώ τα trap-and-traces τις εισερχόμενες.) Το DCS-6000, γνωστό ως Digital Storm, αποθηκεύει το περιεχόμενο τηλεφωνικών κλήσεων και μηνυμάτων για πλήρης εντολές παρακολούθησης. Ένα τρίτο απόρρητο σύστημα, το DCS-5000, χρησιμοποιείται για παρακολούθηση στόχους τρομοκρατών ή κατασκόπων. Μαζί, τα συστήματα παρακολούθησης δίνουν τη δυνατότητα στους πράκτορες του FBI να επαναλαμβάνει τις καταγραφές, ακόμα και όταν αποθηκεύονται (όπως το TiVo), δημιουργούν κύρια αρχεία υποκλοπής, στέλνονται ψηφιακές καταγραφές σε μεταφραστές, ανιχνεύουν την τοποθεσία χονδρικά των στόχων σε πραγματικό χρόνο χρησιμοποιώντας τις πληροφορίες πύργων κινητής τηλεφωνίας, και ακόμη μεταδίδουν ζωντανά τις καταγραφές σε εξωτερικά βαν παρακολούθησης. Τα δωμάτια παρακολούθησης και οι μυστικές τοποθεσίες του FBI ενώνονται μέσω ενός ιδιωτικού, κωδικοποιημένου δικτύου ξεχωριστό του διαδικτύου. Αυτά γίνονται για λογαριασμό της κυβέρνησης. Το δίκτυο επιτρέπει στον πράκτορα του FBI της Νέας Υόρκης, για παράδειγμα, να τοποθετεί κοριό σ'ένα κινητό βασισμένο στο Σακραμέντο, Καλιφόρνια, και αμέσως γνωρίζει την τοποθεσία του τηλεφώνου , έπειτα ξεκινά να λαμβάνει κλήσεις, μηνύματα και κωδικούς πρόσβασης τηλεφωνητή στην Νέα Υόρκη. Οι αριθμοί που πληκτρολογούνται στέλνονται αυτόματα σε εκπαιδευμένους αναλυτές του FBI να ερμηνεύσουυν το μοτίβο κλήσεων και μεταφέρονται κάθε βράδυ από εξωτερικές συσκευές αποθήκευσης στο γραφείο Telephone Application Database, όπου υποβάλλονται σ'ένα είδος data mining που ονομάζεται link analysis. (1) "

Εναλλακτικά, μπορούν να καταγράφουν τις τηλεφωνικές σου συνομιλίες και να τις μεταδώσουν σ'αυτούς (2). Το πιο εύκολο είναι να αποκτήσουν και να χρησιμοποιήσουν τις καταγραφές αυτών που κάλεσες και όταν (;) – αυτό έχει συμβεί και χρησιμοποιηθεί σε αμέτρητες δίκες ακτιβιστών. Πιο πρόσφατα το είδαμε (3) στην ακρόαση του Marius Mason που προτείνουν ότι είναι/ήταν επικεφαλής στην αναρχική σκηνή, λαμβάνοντας αναφορές και δίνοντας εντολές μετά την σύλληψή

του. Αυτήν η εντύπωση τον έχει θέσει υπό εξονυχιστικό έλεγχο ως φυλακισμένο, το έχουν χρησιμοποιήσει ως πρόσχημα για να κόψουν τις επαφές του με συντρόφους.
ΥΓ. Τα μηνύματα είναι εξίσου ευάλωτα στην υποκλοπή με τις κλήσεις και δεν προστατεύονται από το Wiretap νομοσχέδιο, οπότε οι μπάτσοι δεν χρειάζονται δικαστική εντολή για να τα υποκλέψουν. (4)

Πού είναι το ALF;

Τα κινητά τηλέφωνα δουλεύουν στέλνοντας σήμα ανάμεσα σε πύργους κινητών τηλεφώνων. Το κινητό σου στέλνει σήμα σ'έναν πύργο κάθε επτά δευτερόλεπτα. Οι εταιρίες κινητής τηλεφωνίας αποθηκεύουν την πληροφορία σ'ένα φάκελο από λίγους μήνες μέχρι κάποια χρόνια. (5) Το FBI τακτικά χρησιμοποιεί αυτήν την πληροφορία για να συλλάβουν και καταδικάσουν άτομα, για παράδειγμα, ο William Viehl καταδικάστηκε για την απελευθέρωση βιζόν επειδή τα πρακτικά κινητής τηλεφωνίας του τον τοποθέτησαν κοντά στη φάρμα κατά την απελευθέρωση. (6) (Το κλειδί του αυτοκινήτου του βρέθηκε στην σκηνή…) Εν συντομία, βγάλε την μπαταρία του κινητού σου, πριν, κατά τη διάρκεια και μετά από κάθε επίσκεψη της σκηνής εγκλήματος σου, των συντρόφων σου, το σπίτι σου κ.α για μέγιστη ασφάλεια.
Μπορείτε επίσης να εξετάσετε την αγορά μιας λιγότερη ανιχνεύσιμης προπληρωμένης κάρτας, ωστόσο αν σας πιάσουν μ'αυτήν δεν θα σας βοηθήσει ιδιαιτέρως. Θυμήσου να χρησιμοποιείς μόνο μετρητά και να μην δίνεις την ταυτότητά σου, μην χρησιμοποιείς την παλιά κάρτα SIM σου (και οι κάρτες SIM και το λογισμικό του κινητού σου μεταδίδουν αναγνωρίσιμο σήμα), κ.α. Ακόμα και έτσι, είσαι σίγουρος ότι οι φίλοι σου δεν θα αποθηκεύσουν το αριθμό σου υπό το κανονικό σου όνομα ή ένα ψευδώνυμο που είναι συνδεδεμένο με την ταυτότητά σου; Είσαι σίγουρος ότι κανείς δεν θα σε καλέσει με το αληθινό σου όνομα από το κινητό;

Αυτά δεν είναι τα ανδροειδή που ψάχνεις.

Υπάρχει μια ελπίδα, ωστόσο είναι θέμα χρόνου μέχρι κάθε νέος και ασφαλής τρόπος επικοινωνίας δεν θα δουλεύει πια: τα κινητά android είναι μια μερική λύση στην ασφάλεια του κινητού σου, προς το παρόν. Μπορείς να κάνεις πλήρως ασφαλείς κλήσεις, να στέλνεις μηνύματα και να τρέχεις ολόκληρη τη διαδικτυακή σου δράση μέσω του TOR (που κρύβει την δραστηριότητά σου), και με μερικά κινητά, μπορείς να κωδικοποιείς τα πάντα. Έλεγξε αυτούς τους πόρους για περισσότερα. (7)

Όταν πάρουν το κινητό σου, τι θα γίνει;

Από το εξαιρετικό εγχειρίδιο της παρακολούθησης του EFF που παραθέσαμε προηγουμένως (4) :

“Αν συλληφθείς, οι μπάτσοι θα κατάσχουν όλα τα υπάρχοντά σου πριν οδηγηθείς στη φυλακή. Αν έχεις κινητό ή λάπτοπ, θα το πάρουν και αυτό. Αν βρίσκεται κοντά σ’ένα κινητό ή λαπτοπ ίσως πάρουν και αυτά. Το δόγμα της SITA ίσως επιτρέψει στους μπάτσους να ελέγξουν δεδομένα. Ίσως τους επιτρέψει να τα αντιγράψουν και μελλοντική έρευνα, αν και αυτό είναι διαφορετικό από το τι επιτρέπει η αρχική δικαιολόγηση της SITA. Μπορείς να χρησιμοποιείς κωδικό πρόσβασης στις συσκευές σου για να αποφύγεις πιθανή αντισυνταγματική παραβίαση της ιδιωτικής σου ζωής. Όμως, για μεγαλύτερη ασφάλεια, αναλογίσου την κωδικοποίηση των αρχείων σου για να τα προστατέψεις. Οι συνετοί μπάτσοι απλά θα φυλάξουν τις συσκευές σου όσο βγάζουν ένταλμα. Δεν μπορείς να κάνεις τίποτα για να το αποτρέψεις αυτό. Μην προσπαθήσεις να πείσεις του μπάτσους να αφήσουν το κινητό σου ή το λάπτοπ σου λέγοντας ότι δεν σου ανήκουν. Το ψέμα στους μπάτσους διώκεται ποινικά. Επίσης, οι μπάτσοι μπορούν να χρησιμοποιήσουν την κατάθεσή σου εναντίον σου για να υποστηρίξουν ότι δεν έχεις το δικαίωμα αμφισβήτησης ακόμα και μιας παράνομης έρευνας ή κατάσχεση των συσκευών σου, όσο υπάρχει η δυνατότητα εύρεσης αποθηκευμένων πληροφοριών στην συσκευή που μπορούν να χρησιμοποιηθούν εναντίον σου.”

Ωστόσο, το περιστατικό έρευνας για σύλληψη (SITA) που αναφέρεται εδώ δεν επεκτείνεται, για παράδειγμα, στο πορτ μπαγκάζ του αυτοκινήτου που σε συνέλαβαν, χρειάζονται διαφορετικό ένταλμα έρευνας (εκτός αν κατασχέσουν το αμάξι). Αναφερόμαστε σ’αυτό μόνο για να δείξουμε ότι δεν είναι εντελώς απελπιστικό, ένα κωδικοποιημένο λάπτοπ κρυμμένο στο πορτ μπαγκάζ του αυτοκινήτου ή σ’ένα χρηματοκιβώτιο στο υπόγειο θα θεωρηθεί ανατρεπτικό για του μπάτσους και θα αποφύγει τον εξονυχιστικό έλεγχο.

Ζόμπι ρομπότ: Μακρινή πρόσβαση.

Ενώ όλα τα άτομα γνωρίζουμε για την τοποθέτηση κοριών (ωστόσο όχι αρκετά, διάβασε το χρήσιμο εγχειρίδιο του EFF (4) για περισσότερες πληροφορίες), ακόμα είναι επιφυλακτικά για τη χρήση των κινητών ως μικρόφωνα . Η ιδέα του να βγάζεις την μπαταρία από το κινητό σου υπάρχει για κάποιο καιρό, όμως πέντε χρόνια μετά, κάποια άτομα είναι επιφυλακτικά ακόμη. Ορίστε μια σκληρή αλήθεια για σας:

“Το FBI φαίνεται ξεκίνησε να χρησιμοποιεί ένα καινοτόμο τρόπο ηλεκτρονικής παρακολούθησης σε εγκληματικές έρευνες: ενεργοποιώντας το μικρόφωνο του κινητού κρυφακούοντας από απόσταση τις κοντινές συζητήσεις.

Η τεχνική ονομάζεται “roving bug” και εγκρίθηκε από το Υπουργείο Δικαιοσύνης των ΗΠΑ για τη χρήση του ενάντια στα μέλη μιας οικογένειας οργανωμένου εγκλήματος στη Νέα Υόρκη που ήταν επιφυλακτική στις κλασικές μεθόδους παρακολούθησης όπως η φυσική στενή παρακολούθηση ή η τοποθέτηση κοριών. Τα κινητά τηλέφωνα Nextel που άνηκαν σε δύο υποτιθέμενους μαφιόζους, τον John

Ardito και του δικηγόρου του Peter Peluso, χρησιμοποιήθηκαν από το FBI για να ακούσουν τις κοντινές συζητήσεις τους. Το FBI βλέπει τον Ardito ως έναν από τους πιο δυνατούς άνδρες της οικογένειας Genovese, κύριο μέρος της εθνικής μαφίας. Η τεχνική αυτή παρακολούθησης ήρθε στο φως από μια δημοσιευμένη άποψη αυτήν την εβδομάδα του περιφερειακού δικαστή των ΗΠΑ Lewis Kaplan. Αποφάσισε ότι το “roving bug” ήταν νόμιμο καθώς οι ομοσπονδιακοί νόμοι για την παρακολούθηση είναι αρκετά ευρύς για να επιτρέψει το να κρυφακούς ακόμη και συζητήσεις που γίνονται σε κοντινή περιοχή από το κινητό του υπόπτου.
Ο Kaplan είπε ότι η τεχνική “λειτούργησε ανεξάρτητα αν το κινητό ήταν ενεργοποιημένο ή απενεργοποιημένο”. Μερικά ακουστικά δεν μπορούν να απενεργοποιηθούν πλήρως χωρίς να αφαιρέσεις την μπαταρία, για παράδειγμα, μερικά μοντέλα της Nokia θα ενεργοποιηθούν παρόλο που είναι απενεργοποιημένα αν ένα ξυπνητήρι έχει ρυθμιστεί.
Ενώ η δίωξη της εγκληματικής οικογένειας Genovese φαίνεται να είναι η πρώτη φορά που γίνεται κρυφακούγοντας, η τεχνική αυτήν συζητείται χρόνια στους κύκλους ασφαλείας…
Τα ακουστικά της Nextel και της Samsung και το Motorola Razr είναι ευάλωτα σε λογισμικές εγκαταστάσεις που ενεργοποιούν το μικρόφωνο, είπε ο James Atkinson, σύμβουλος αντιπαρακολούθησης που έχει στενές επαφές με κρατικούς φορείς. “Μπορούν να αποκτήσουν πρόσβαση από απόσταση και είναι φτιαγμένα να μεταδίδουν τους ήχους δωματίου όλη την ώρα”, είπε. “Μπορείς να το κάνεις αυτό χωρίς να έχεις φυσική πρόσβαση στο τηλέφωνο.”
Επειδή τα μοντέρνα ακουστικά είναι σαν μικροί υπολογιστές, εγκαταστημένο λογισμικό μπορεί να τροποποιήσουν την συνηθισμένη διεπαφή που παρουσιάζει μια κλήση σ’εξέλιξη. Το λογισμικό κατασκοπίας μπορεί να καλέσει το FBI, χωρίς ο κάτοχος να το γνωρίζει. (8) ”

Ορίστε η τεκμηρίωση. Μπορέσαμε να βρούμε αυτήν την τεκμηριωμένη υπόθεση προς το παρόν, αλλά αυτό δεν σημαίνει ότι δεν γίνεται πιο συχνά. Αρκετά άρθρα που είδαμε, συμπεριλαμβανομένου και ενός από το Γραφείο Εμπορίου των ΗΠΑ (9) και ένα από το BBC (10), προτείνουν οι κυβερνητικοί εκπρόσωποι και τα στελέχη μιας εταιρείας να βγάζουν την μπαταρία του κινητού τους όταν συζητούν ευαίσθητα θέματα. Είναι ύποπτο όταν 10 κινητά ακτιβιστών (ή μαφιόζων) αναβοσβήνουν ταυτόχρονα; Ίσως! Άφησε ελεύθερα το κινητό σου άθικτο και πήγαινε για μια βόλτα χωρίς αυτό.
Υπάρχουν αρκετοί νόμιμοι τρόποι απομακρυσμένης πρόσβασης σε υπολογιστές είτε Mac είτε Windows, χρησιμοποιώντας συνηθισμένα διαθέσιμα προγράμματα.
Μπορούν να κοιτάξουν τα αρχεία σου, παρακολουθήσουν την δραστηριότητά σου, ενεργοποιήσουν το μικρόφωνό σου, σε καταγράψουν ή τραβήξουν φωτογραφία από την κάμερα του υπολογιστή σου (11). Υπάρχουν επίσης keystroke loggers, προγράμματα που καταγράφουν ό,τι γράφεις και το μεταδίδουν οπουδήποτε. Κάποιος μπορεί να σταθμεύσει έξω από το σπίτι σου και να καταγράψουν την κωδικοποιημένη διαδικτυακή επικοινωνία σου, ή να την αποκρυπτογραφήσουν, αν

δοθεί αρκετός χρόνος. Είναι ευρέως γνωστό ότι ο καλύτερος τρόπος να το αποφύγεις είναι η χρήση δημόσιου υπολογιστή, σ'ένα ίντερνετ καφέ ή βιβλιοθήκη, όσο πληρώνεις με μετρητά ή χρησιμοποιώντας πάσο επισκέπτη.

Δεν το κάνουν όλα τα τρολ για πλάκα: Διαδικτυακή παρακολούθηση.

Είναι κοινώς γνωστό ως τώρα: ό,τι δημοσιεύσεις στο διαδίκτυο μπορεί να χρησιμοποιηθεί εναντίον σου στη δίκη. Συνέβη στον Marius Mason (κατοχυρώνοντας τον Rod Coronado ως ήρωα στο Myspace του (3)), συνέβη στον Rod Coronado (για την προσθήκη του Mike Roselle στο Facebook (12)), συνέβη σε παιδιά κατά τη διάρκεια των προσφάτων εξεγέρσεων στο Λονδίνο (που δημοσίευσαν υπέρ των εξεγέρσεων στο Facebook (13)) και σε εκατοντάδες λιγότερο προφανές πολιτικές υποθέσεις. Κάθε ασαφή δημοσίευμα είχε ως αποτέλεσμα πραγματικό χρόνο φυλάκισης. Αυτό προφανώς κάνει την κοινωνική δικτύωση χρυσωρυχείο στην επιβολή του νόμο, όμως αυτήν είναι μόνο η κορυφή του παγόβουνου. Αναλογίσου : το Facebook παρέχει στο FBI έναν χάρτη από κοινωνικές σχέσεις μεταξύ αναρχικών, εκατοντάδες αναρχικούς και τη δραστηριότητά τους, βαθμό σχέσης μεταξύ τους κ.α. Ακόμα και να χρησιμοποιήσεις ψευδώνυμο μην γίνεις μέλος αναρχικών ομάδων, μην δεχτείς προσκλήσεις αναρχικών εκδηλώσεων και ποτέ μην δημοσιεύεις για πολιτική, μια πρωταρχική μελέτη (14) δείχνει ότι ερευνητές μπορούν εύκολα να καθορίσουν αν κάποιο άτομο είναι ομοφυλόφιλο ή χριστιανός αποτυπώνοντας τα ενδιαφέροντα των Facebook φίλων τους: αν οι περισσότεροι φίλοι σου είναι χριστιανοί, πιθανώς να είσαι και εσύ. Το ίδιο συμβαίνει και για τους αναρχικούς. Εξάλλου, αν εγγραφείς στο Facebook από τον προσωπικό σου υπολογιστή έχουν το ιστορικό της IP σου και ευχαρίστως να την παραδώσουν στους μπάτσους (χειρίζονται τέτοια αιτήματα – εκατοντάδες κάθε εβδομάδα – μέσω του email subpoena@facebook.com. Τόσο απλό!) Αναλογίσου : εμπιστεύεσαι όλα τα άτομα που είστε φίλοι στο Facebook να μην μιλήσουν στους μπάτσους; Οι συνδέσεις κοινωνικής δικτύωσης είναι βάσιμες κατηγορίες επίσης.
Ακόμα και το να μην χρησιμοποιείς ιστοσελίδες κοινωνικής δικτύωσης, πιθανώς να χρησιμοποιείς email. Ψηφιακά οι πάροχοι email θα παραδώσουν στους μπάτσους ένα αντίγραφο μ'όλα τα email και τις σχετικές IP, στην πραγματικότητα, μια δικαστική απόφαση από το 2009 επιτρέπει στους μπάτσους να διαβάσουν τα email σου χωρίς ένταλμα. (15) Το riseup.net, μια αναρχική υπηρεσία email, δεσμεύεται να αντισταθούν σε κάθε τέτοια προσπάθεια των μπάτσων, αλλά είναι η μοναδική υπηρεσία που γνωρίζουμε που κάνει τέτοιου είδους αντίσταση πολιτική. Η πολιτική τους εν μέρει:

“Πασχίζουμε να κρατήσουμε το email μας όσο πιο ασφαλές και προσωπικό γίνεται. Δεν καταγράφουμε την IP σου. (Οι περισσότερες υπηρεσίες κρατάνε αναλυτικό αρχείο κάθε συσκευής που συνδέεται στους servers τους. Εμείς κρατάμε μόνο πληροφορίες που δεν μπορούν να χρησιμοποιηθούν στην ταυτοποίηση της συσκευής σου). Όλα τα δεδομένα σου, ακόμη και το email σου, αποθηκεύονται στο riseup.net σε κωδικοποιημένη μορφή. Δουλεύουμε σκληρά να προστατεύσουμε τους servers μας από κάθε κακόβουλη επίθεση. Δεν μοιραζόμαστε καμία πληροφορία των χρηστών μας με κανένα άτομο. Θα πολεμήσουμε ενεργά κάθε προσπάθεια κλήτευσης ή να αποκτήσουν μ’άλλον τρόπο οποιεσδήποτε πληροφορίες χρήστη ή αρχείων. Δεν θα διαβάσουμε, ψάξουμε, ή επεξεργαστούμε εισερχόμενα ή εξερχόμενα email εκτός από το αυτόματο μέσο προστασίας του από ιούς και spam ή μετά από δική σας απεύθυνση επίλυσης προβλήματος. (16)”

Εμείς συστήνουμε ανεπιφύλακτα τη χρήση ενός λογαριασμό στο riseup για οποιαδήποτε προσωπική επικοινωνία, ωστόσο δεν συστήνουμε την αποστολή οτιδήποτε ύποπτου από email, είναι πιο ασφαλές και τουλάχιστον φυλάει τα δεδομένα σου από την ευκολότερη εξόρυξη. Υπάρχει επίσης μια υπηρεσία κωδικοποιημένης άμεσων μηνυμάτων (17).

Αναφερθήκαμε στο data mining προηγουμένως από τους μπάτσους, όμως γίνονται και από ιδιωτικές εταιρείες (που είναι πάντα πρόθυμοι να συνεργαστούν με τις αρχές). Η Google (18) είναι ένα εύκολο παράδειγμα: σου φαίνονται τα αποτελέσματα αναζήτησης και οι διαφημίσεις ανατριχιαστικά σχετικές; Αυτό συμβαίνει επειδή η Google κρατάει αρχείο με ό,τι ψάξεις, όλες τις ιστοσελίδες που θα επισκεφτείς, αν χρησιμοποιείς Gmail παρατηρεί τις λέξεις που στέλνεις ή δέχεσαι στα email σου, αν χρησιμοποιείς Google Voice, καταγράφει τα αξιοσημείωτα πράγματα για τη φωνή σου και δοσμένου των δεδομένων, μπορεί να αναγνωρίσει τη φωνή σου σ’άλλα πλαίσια. Μη ψάχνοντας μέσω Google ή μη έχοντας λογαριασμούς στη Google,ίσως βοηθήσει λίγο, αλλά πάλι η εταιρεία θα καταγράψει κάθε ενέργεια της IP σου σε σχετικές ιστοσελίδες της εταιρείας. Η Google είναι η καλύτερη σ’αυτό, οι περισσότερες γνωστές εναλλακτικές σε καταγράφουν με παρόμοιο τρόπο.

Όπως αναφέραμε νωρίτερα, οι δημόσιοι υπολογιστές είναι η καλύτερή σου επιλογή, από άποψη ασφάλειας, θυμήσου να μην υπογράψεις σε κανέναν λογαριασμό που συνδέεται με την IP της κατοικίας σου ή το όνομά σου και να μην χρησιμοποιήσεις την ταυτότητά σου κατά την εγγραφή στον υπολογιστή (όπως η κάρτα βιβλιοθήκης ή το να πληρώνεις με πιστωτική κάρτα σ’ένα ίντερνετ καφέ). Μπορείς, επίσης, να χρησιμοποιείς εργαλεία όπως το TOR για να κρύβεις τη δραστηριότητά σου, VPNs για να το κωδικοποιείς ή PGP/GPG για να κωδικοποιείς τα μηνύματά σου. Άλλες επιλογές ασφάλειας για τον υπολογιστή είναι το secure delete (διαγράφοντας τα αρχεία σου με τον συνηθισμένο τρόπο δεν αφαιρεί τις πληροφορίες από τον υπολογιστή ή το κινητό σου, μονάχα αφαιρεί το όνομα του αρχείου), και κωδικοποιώντας τον σκληρό δίσκο.

Καταστολή

Όλα τα μέσα παρακολούθησης που αναφέραμε σ'αυτήν την μπροσούρα (και ακόμη περισσότερα) χρησιμοποιήθηκαν απέναντι σε αντιδραστικά και επαναστατικά υποκείμενα κατά τη διάρκεια των εξεγέρσεων της Αραβικής Άνοιξης. Για παράδειγμα τα μέσα που χρησιμοποιήθηκαν στο Bahrain:

"Κέντρα παρακολούθησης, έτσι ονομάζονται τα συστήματα, πωλούνται σ'όλο τον κόσμο από αυτές τις εταιρείες και οι ανταγωνιστές τους… Σχηματίζουν τον πυρήνα των δήθεν νόμιμων συστημάτων υποκλοπών και παρακολούθησης. Ο εξοπλισμός πωλείται σε μεγάλο βαθμό σε υπηρεσίες επιβολής του νόμου παρακολουθώντας τρομοκράτες και άλλους εγκληματίες. Η εργαλειοθήκη επιτρέπει περισσότερα από την υποκλοπή των κλήσεων, emails, μηνυμάτων και Voice Over Internet Protocol κλήσεων, όπως αυτές που γίνονται μέσω Skype. Μερικά προϊόντα μπορούν κρυφά να ενεργοποιήσουν την κάμερα του λάπτοπ ή το μικρόφωνο κινητών συσκευών, μπορούν να αλλάξουν το περιεχόμενο γραπτής επικοινωνίας κατά τη μετάδοση,να χρησιμοποιήσουν φωνητική αναγνώριση για να σκανάρουν τα τηλεφωνικά δίκτυα και να εντοπίσουν την τοποθεσία ατόμων μέσω των κινητών τους. Τα συστήματα παρακολούθησης μπορούν να ελέγξουν συζητήσεις για λέξεις κλειδιά ή να αναγνωρίσουν φωνές και να τροφοδοτήσουν τα δεδομένα και τις καταγραφές σε κρατικούς φορείς. (19)"

Πολλά άτομα επιλέχθηκαν για αντίποινα – κρατήσεις, βασανισμοί, δολοφονίες και βιασμοί – από τις αρχές χρησιμοποιώντας τις πληροφορίες που συλλέχθηκαν από την παρακολούθηση της κινητής και διαδικτυακής τους χρήσης. Παρόλο που πολλοί νόμοι απαγορεύουν τέτοιου είδους παρακολούθησης από εταιρείες, οι νόμοι παραβιάζονται ή αναστέλλονται από τις κυβερνήσεις που προσπαθούν να σταθεροποιήσουν τον έλεγχο και δυτικές εταιρείες έχουν μεγάλο μερίδιο ευθύνης για την κατασκευή τέτοιων τεχνολογιών (η Cisco είναι συνεργός της Κίνας στην καταστολή της διαδικτυακής ελευθερίας, για παράδειγμα (20)).
Περιβόητα, το σήμα κινητών μπλοκαρίστηκε σ'ένα σταθμό BART πρόσφατα σ'αναμονή μιας διαδήλωσης κατά της αστυνομίας BART που δολοφόνησαν κάποιον. (21) Η Βρετανική κυβέρνηση δεσμεύεται να μπλοκάρει το Twitter και τα Blackberries κατά τη διάρκεια κοινωνικής αναταραχής (22) και προφανώς ο Mubarak έκανε το ίδιο στην Αίγυπτο στο τέλος. Συνοπτικά, το διαδίκτυο, τα κοινωνικά δίκτυα και η κινητή πρόσβαση είναι ένα χρήσιμο εργαλείο για 'μας αλλά δεν μας ανήκουν. Χρειαζόμαστε έναν στρατό από black hat hackers δουλεύοντας σκληρά υπονομεύοντας τον κυβερνητικό και εταιρικό έλεγχο του διαδικτύου, όμως μέχρι να κερδίσουν ολοκληρωτικά δεν μπορούμε να βασιζόμαστε εξ ολοκλήρου σ'αυτό. Επίσης, μερικά άτομα πιστεύουν ότι τα μέσα κοινωνικής δικτύωσης τείνουν να μετατρέπει τα υποκείμενα σε επαναστάτες του καναπέ, που ικανοποιούνται απ'αυτό ενώ σε οποιαδήποτε άλλη περίπτωση θα κατέβαιναν στους δρόμους. Δεν γίνεται να

χάσουμε την ικανότητά μας να δουλεύουμε πρόσωπο με πρόσωπο, απευθείας, να σχεδιάζουμε απαρατήρητα, να χτυπάμε γρήγορα, στα κρυφά και να ξεφεύγουμε, γνωρίζουμε πότε αξίζει να οργανωνόμαστε μέσω Twitter (άξιζε στο Pittsburgh (24); συζητήστε το), το να γνωρίζεις ότι η μοναδική ασφάλεια που χρειάζεσαι είναι μια μπλούζα γύρω από το πρόσωπό σου έτσι ώστε οι κάμερες (CCTV) να μην σ'αναγνωρίζουν και γίνεσαι ένας στόχος που δεν διαφέρεις ανάμεσα στο πλιάτσικο. Πρέπει να είμαστε σε θέση να ξεχωρίζουμε ανάμεσα σ'αυτές τις περιπτώσεις παρά να συμβιβαζόμαστε σε παθητική στάση.

Παλιός καλός εραστής κατάσκοπος: Φίλοι και κρεβάτι.

Μην ξεχνάς: όσο οι μπάτσοι μπορούν να σε κατασκοπεύουν με κάθε είδους υψηλής τεχνολογίας, συνήθως κολλάνε στη γραφειοκρατεία για να το κάνουν, αλλά ο ευκολότερος τρόπος κατασκοπείας είναι ο παλιότερος: το κουτσομπολιό. Ανεξάρτητα από το πόσο ασφαλής είσαι τεχνικά, οι σύντροφοί σου, πρώην, ακόμα και οι καλοί σου φίλοι μπορούν να σε ρουφιανέψουν. Όσο προχωρημένη και αν είναι η κωδικοποίησή σου το FBI μπορεί να τοποθετήσει κοριό στο φωτιστικό σου. Μην αφήσεις τη λήψη προηγμένων μέτρων ασφαλείας να σε παρασύρει ξεχνώντας τα βασικά. Δεν θέλουμε να γίνεις παρανοϊκός, αλλά θέλουμε να είσαι διακριτικός, να ξέρεις το ρίσκο και να είσαι εντάξει με τις συνέπειες των πράξεών σου εξαρχής.

Δέκα συμπεράσματα.

1. Φέρσου έτσι ώστε καμία τηλεφωνική κλήση ή ανταλλαγή μηνυμάτων που κάνεις σε δική σου συσκευή να είναι σημαντική ή κρυφή.
2. Μην αναφέρεις τίποτα ύποπτο κοντά σε κινητό ή υπολογιστή. Διαπροσωπικά και εξωτερικά είναι ο μοναδικός τρόπος ώστε το άτομο που μιλάς και η μελλοντική σου απροσεξία να είναι οι μόνες ανησυχίες σου για ασφάλεια.
3. Να γνωρίζεις ότι οι μπάτσοι συλλέγουν στοιχεία και από το περιβάλλον σου (με ποιον μιλάς, κουτσομπολιό που υποδεικνύει τον περίγυρό σου και άλλα) και έχε το νου όσο έχεις παρακολουθούμενες συζητήσεις.
4. Βγάλε τις μπαταρίες στο δρόμο και στο γυρισμό όταν διαπράττεις ένα έγκλημα, ερευνώντας, σε συναντήσεις με συντρόφους – κάθε φορά που δεν θες η τοποθεσία σου να είναι εύκολα ανιχνεύσιμη-- αν δεν μπορείς απλά άσε το κινητό σπίτι.
5. Τα email δεν είναι ασφαλή, αλλά το riseup είναι το καλύτερο για μη ενοχοποιητική προσωπική συζήτηση.
6. Η IP σου κατοχυρώνεται συνέχεια από διάφορες ιστοσελίδες, η χρήση δημόσιου υπολογιστή χωρίς την επίδειξη ταυτότητας ή εγγραφής είναι η πιο ασφαλής λύση.
7. Αν κλέψεις κάποια ηλεκτρονική συσκευή, σιγουρέψου ότι γνωρίζεις πώς να απενεργοποιείς κάποιο μηχανισμό παρακολούθησης, αν έχει.

8. Αν η πολιτική σου αντίσταση βασίζεται στα κοινωνικά δίκτυα να ξέρεις ότι μπορεί να παραλύσει απευθείας.
9. Δεν είναι απαραίτητη και μπορεί να είναι αντιπαραγωγική η εγκατάλειψη συσκευών υψηλής τεχνολογίας ως αναρχικός, αλλά σχεδίασε την αλληλεπίδρασή σου μ'αυτές προσεκτικά.
10. Μην επικεντρωθείς στις τεχνολογικές προφυλάξεις ξεχνώντας τα βασικά.

Πηγές.

1. http://www.wired.com/politics/security/news/2007/08/wiretap
Ένα αρκετά πληροφοριακό άρθρο για το DCSNet.
2. http://mobileactive.org/howtos/mobile-surveillance-primer
Συζήτηση για τον κίνδυνο ασφαλείας από τα κινητά και προτάσεις για το πώς θα γίνει πιο ασφαλές. Βασισμένο στο Ηνωμένο Βασίλειο.
3. https://supportmarie.files.wordpress.com/2011/03/mason-sentencing-transcript.pdf
Η μεταγραφή της ποινής του Marius Mason.
4. https://ssd.eff.org/
Ολόκληρο το άρθρο είναι μια εξαιρετική πηγή για την παρακολούθηση της Αμερικανικής κυβέρνησης και πώς να προστατευτείς.
5.https://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r3&src=me&ref=general
Ένα Γερμανικό άρθρο για την παρακολούθηση της τοποθεσίας μέσω κινητού.
6.https://animalliberationfrontline.com/activist-sentenced-to-two-years-for-alf-mink-liberation/
Πληροφορίες από την καταδίκη του William Viehl (μερικώς βασισμένη στην παρακολούθηση του κινητού κοντά στη φάρμα βιζόν).
7. http://guardianproject.info and http://www.whispersys.com/
Πληροφορίες για το πώς κάνεις τα κινητά android πιο ασφαλή.
8.https://www.cnet.com/news/privacy/fbi-taps-cell-phone-mic-as-eavesdropping-tool/
Ένα άρθρο για την ηχογράφηση των αρχηγών της Μαφίας μέσω απομακρυσμένης ενεργοποίησης των κινητών τους.
10. http://news.bbc.co.uk/2/hi/uk_news/magazine/3522137.stm
Το BBC για τους κινδύνους παρακολούθησης των πολιτικών και στελεχών επιχείρησης.
13. https://www.theguardian.com/uk/2011/aug/16/uk-riots-four-years-disorder-facebook
Ένα άρθρο για τα παιδιά που φυλακίστηκαν για 4 χρόνια επειδή δημοσίευαν υπέρ των εξεγέρσεων.
14. https://www.inquisitr.com/38594/closeted-your-facebook-friends-could-out-you/
Ένα άρθρο για την προκαταρκτική έρευνα που αποδεικνύει ότι είναι εύκολο να προσδιορίσεις το σεξουαλικό προσδιορισμό από τους φίλους σου στο Facebook.
15. https://online.wsj.com/public/resources/documents/062309mosman.pdf
Η δικαστική απόφαση που αποδεικνύει το δικαίωμα των μπάτσων να διαβάζουν email χωρίς ένταλμα.

16. https://riseup.net/pl/about-us
Η πολιτική του Riseup που προστατεύει τα δεδομένα σου και αντιστέκεται στις αρχές..
17. https://help.riseup.net/en/otr#introduction-to-otr
Μια εισαγωγή στο Off The Record and Pidgin, μια κρυπτογραφημένη υπηρεσία μηνυμάτων.
18. https://www.spiegel.de/international/germany/data-mining-you-to-death-does-google-know-too-much-a-587546.html
Το άρθρο της Der Spiegel στην τακτική της Google για την εξόρυξη δεδομένων (data mining) σου.
19. https://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking
Πληροφορίες για το πώς χρησιμοποιήθηκαν εταιρείες παρακολούθησης της Δύσης στην καταστολή των συμμετεχόντων στην Αραβική Άνοιξη.
20. https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1
Ο ρόλος της Cisco στη διαδικτυακή λογοκρισία της Κίνας.
21. https://www.cnet.com/news/privacy/s-f-subway-muzzles-cell-service-during-protest/
Άρθρο για την διακοπή σε υπηρεσίες κινητού τηλεφώνου από τη BART, για να εμποδίσουν μια επερχόμενη διαδήλωση.
22. https://www.theguardian.com/uk/2011/aug/11/cameron-call-social-media-clampdown
Οι υποσχέσεις του David Cameron να διακόψει την πρόσβαση σε Facebook, Twitter και το δίκτυο της Blackberry σε μελλοντική κοινωνική αναταραχή.
23. https://theconversation.com/dictatorship-101-killing-the-internet-plays-into-the-hands-of-revolutionaries-3254
Συζήτηση ενός άρθρου που προτείνει ότι το διαδίκτυο τείνει να ηρεμεί επαναστάσεις.
24. https://www.theguardian.com/world/2009/oct/04/man-arrested-twitter-g20-us
Δύο άτομα συνελήφθησαν επειδή έκαναν tweet των αστυνομικών δράσεων κατά τη διάρκεια του G20 στο Pittsburgh.
http://www.zahrasparadise.com/lang/en/archives/76
Zahra’s Paradise, by Amir and Khalil; ένα διαδικτυακό κόμικ για τη διαδικτυακή αντίσταση και καταστολή στο Ιράν, καθώς και ένας γενικός απολογισμός των εξεγέρσεων του 2009. Διαθέσιμο και σε μορφή βιβλίου.
https://we.riseup.net/
Crabgrass, μια πιο ασφαλή ιστοσελίδα κοινωνικού δικτύου που τρέχει από το riseup.net. Σε δοκιμαστική μορφή Beta.
http://www.eff.org/
The Electronic Freedom Foundation: Όπως το ACLU για το διαδίκτυο.
http://craphound.com/littlebrother/download/
Η νουβέλα του Cory Doctorow Μικρός Αδερφός, για δωρεάν λήψη. Μια νουβέλα για την αντίσταση της νεολαίας στα μέτρα παρακολούθησης της Homeland Security.