Σημειώσεις πάνω στην τεχνολογία, την παρακολούθηση και την επαναστατική στρατηγική

του Eric Ribellarsi, kasamaproject.org (Μετάφραση: Barikat)

Σήμερα [05/09/2013] η Google ανακοίνωσε την πρόθεση της να εγκαταλείψει τα ανοιχτά διαδικτυακά πρότυπα (open web standards, τα πρότυπα δηλαδή που ορίζουν πως ένας πλοηγός διαδικτύου προβάλλει τα δεδομένα), και να μετατρέψει σταδιακά τον Chrome (πλοηγός διαδικτύου) σε μια εμπορική πλατφόρμα εφαρμογών (δηλαδή σε μια πλατφόρμα όπου ο πηγαίος κώδικας και τα υλοποιούμενα πρότυπα ελέγχονται καθ' ολοκληρία από τη google), με απώτερο στόχο τη δημιουργία ενός ολοκληρωμένου λειτουργικού συστήματος ανταγωνιστικού προς τα Windows, το OSX και το Linux.

Ο Chrome εγκαθίσταται με πλήρη δικαιώματα στα περισσότερα λειτουργικά συστήματα, συνεπώς κάθε εφαρμογή που θα εγκαθίσταται μέσω αυτού θα έχει όλα τα δικαιώματα για να διαβάσει τα δεδομένα στον υπολογιστή του χρήστη. Εν τέλει αυτή είναι μια στρατηγική με την οποία η Google σκοπεύει να αποκτήσει εποπτεία πάνω στο τελευταίο πράγμα που δεν έχει: τι κάνουμε στον υπολογιστή μας όταν είμαστε οφλαιν. Και αυτό θα το συνδυάσουν και με μια γαμημένη κάμερα (Google Glass) την οποία θέλουν ο κόσμος να φοράει στο κεφάλι του και η οποία θα είναι δίχως αμφιβολία προσβάσιμη από όλες τις υπηρεσίες ασφαλείας όπως η NSA, το FBI και η CIA.

Μια μεγάλη πολιτική εκτροπή είναι σε εξέλιξη, και είμαι ιδιαίτερα ανήσυχος για το γεγονός ότι η αριστερά αντιμετωπίζει τα ζητήματα της ασφάλειας των επικοινωνιών ως δευτερεύοντα, ζητήματα για σπασίκλες του διαδικτύου. Είναι εξοργιστικό το ότι η Αριστερά υιοθέτησε μια χαλαρή πολιτική διαρροής εσωτερικών εγγράφων και κηρύττει ότι οι αριστερές οργανώσεις στον 21ο αιώνα δεν μπορούν να προστατέψουν την ιδιωτικότητά τους. Ειλικρινά, όλα αυτά είναι σοσιαλδημοκρατικές παπαριές. Φαντάζεται έτσι ένα κόσμο όπου λόγω της παντοδυναμίας του κράτους η επανάσταση είναι ανέφικτη και συνεπώς όλοι οι ριζοσπάστες θα πρέπει να αποδεχτούν την ιδέα ότι πρέπει να υπονομεύουν τις εσωτερικές διαδικασίες εκείνων που κανονικά θα έπρεπε να είναι επαναστατικές οργανώσεις.

Ένα επαναστατικό κίνημα πρέπει να πάρει συνειδητές αποφάσεις για την ασφάλεια, τις πληροφορίες και την παρακολούθηση. Σημαίνει μήπως αυτό ότι πρέπει να γίνουμε παρανοϊκ/οί-ες; Θα διαφωνήσω. Σε κάποιες περιπτώσεις, η υιοθέτηση μιας υπερασφαλούς-συνωμοτικής κουλτούρας δίνει την εντύπωση ότι πίσω από αυτήν κρύβεται ένας εξαιρετικά επικίνδυνος πολιτικός σχεδιασμός που γίνεται στόχος ακόμα μεγαλύτερης καταστολής. Επιπλέον, το να κρύβεσαι δεν αποτελεί μια νικηφόρα στρατηγική. Τέλος, η υιοθέτηση ενός υπερβολικού συνόλου πολιτικών ασφαλείας μπορεί να οδηγήσει στην απομόνωση των κομμουνιστών από τον κόσμο.

Αυτή είναι μια συζήτηση που πρέπει να γίνει κάποια άλλη στιγμή. Το πρόβλημα δεν είναι ότι ο κόσμος έχει ανασφαλείς επικοινωνίες στο διαδίκτυο, το πρόβλημα είναι ότι χωρίς ιδιαίτερη σκέψη επιτρέπουμε τη συγκομιδή όλης μας της ζωής και των προσωπικών μας δεδομένων από ένα κακόβουλο κράτος που σχεδιάζει ανείπωτα πράματα για εμάς. Ο κόσμος μεταφέρει όλη του τη ζωή σε συστήματα της Google, από τη χρήση του κινητού του, τα email, τις σελίδες που επισκέπτεται, το που πηγαίνει, τι βιβλία διαβάζει και, πλέον,

μέχρι και το τι βλέπει (google glass). Βάζουμε τεχνολογίες στη ζωή μας που οδηγούν όχι μόνο στη προσωπική μας παρακολούθηση, αλλά και στην παρακολούθηση όσων βρίσκονται γύρω μας.

Δεν θα πρέπει να υιοθετήσουμε την αυταπάτη ότι μια χούφτα nerds που υιοθετούν παρανοϊκές πολιτικές ασφάλειας στις επικοινωνίες τους είναι η λύση, αλλά ούτε και ο φιλελευθερισμός της σοσιαλδημοκρατικής αριστεράς μπορεί να γίνει ανεκτός. Στο κείμενο αυτό θέλω να αναδείξω τη δυνατότητα για κάτι διαφορετικό: τη μαζική διάχυση υπεύθυνων πρακτικών χρήσης του διαδικτύου στις ιδιωτικές στιγμές μας αλλά και κατά το επαναστατικό έργο. Η "διαρροή" του Edward Snowden λειτουργεί ως καταλύτης, καθώς προκαλεί διευρυμένες συζητήσεις γύρω από το χαρακτήρα της παρακολούθησης, της καταστολής και του κράτους. Και η αριστερά οφείλει να παρέμβει στη συζήτηση αυτή. Επομένως σε τι θα μπορούσε να συνίσταται αυτό;

1. Συνειδητή χρήση: Ο πρώτος κανόνας για οποιαδήποτε υπεύθυνη χρήση του διαδικτύου είναι να συνειδητοποιήσουμε ότι δυνητικά όλα τα δεδομένα μας είναι προσβάσιμα, ακόμα και - σε τελική ανάλυση - τα κρυπτογραφημένα. Η NSA κατασκευάζει ένα ολοκληρωμένο data - center (ΣτΜ: Ειδικά σχεδιασμένα κτήρια για την εγκατάσταση εκατοντάδων συστοιχιών Η/Υ) αποκλειστικά για το σκοπό της αποκρυπτογράφησης μηνυμάτων. Πιθανότατα ακόμη να μην μπορούν, αλλά δεν είμαστε χαζοί για να πιστεύουμε ότι οι κρυπτογραφημένες επικοινωνίες θα είναι ασφαλείς για πάντα. Οι ριζοσπάστες θα πρέπει ανά πάσα στιγμή να θεωρούν ότι είναι στόχοι παρακολούθησης. Με αυτά τα δεδομένα, θα πρέπει να κατανοήσουμε ότι υπάρχουν υλικά όρια στους πόρους που μπορεί να διαθέσει η NSA σε αποκρυπτογράφηση μηνυμάτων. Οι περισσότερες επικοινωνίες παίρνουν χρόνια (ακόμα και δεκαετίες) προκειμένου να αποκρυπτογραφηθούν, οπότε ο βασικός στόχος τους είναι η ολοκληρωτική παράκαμψη της κρυπτογραφίας μέσω της τοποθέτησης <<κερκόπορτων>> στα λειτουργικά συστήματα οι οποίες τους παρέχουν άμεση πρόσβαση στις συσκευές καθώς και τις επικοινωνίες πρωτού αυτές κρυπτογραφηθούν/αποκρυπτογραφηθούν. Ο Edward Snowden επιχειρηματολογεί για αυτό εδώ.

2. Υιοθετείστε κανόνες: Η καθημερινή διάδραση με τον τεράστιο κρατικό μηχανισμό παρακολούθησης δεν μπορεί να αποτελεί ατομική απόφαση. Τα ριζοσπαστικά κινήματα και οι μετέχοντες σε αυτά πρέπει να θέσουν/υιοθετήσουν κανόνες και να θέσουν ο ένας τον άλλον συλλογικά υπεύθυνο. Οι αποφάσεις ενός ατόμου μπορούν να βάλουν σε κίνδυνο τις ζωές πολλών άλλων που βρίσκονται γύρω του. Το Google Glass θα πρέπει να απαγορευτεί από οποιαδήποτε πολιτική δραστηριότητα. Το τι συζητείται στο διαδίκτυο, ασχέτως του αν χρησιμοποιούνται ψευδώνυμα η αληθινά ονόματα θα πρέπει να αποτελεί ζητήμα προς συλλογική επίλυση από κάθε ριζοσπαστικό κίνημα.

3. Απομάκρυνση από το PRISM: Υπάρχουν πολλές εναλλακτικές προκειμένου να μη γίνεται χρήση υπηρεσιών που συνεργάζονται με την NSA μέσω του προγράμματος PRISM (ακόμα και αυτές που ίσως να έχουν εγκατεστημένες <<κερκόπορτες>> της NSA). Διαβάστε το PRISM Break για μια πλήρη λίστα αυτών των επιλογών. Από αυτές, εφιστώ ιδιαίτερη προσοχή στις μηχανές αναζήτησης και στις τεχνολογίες ανταλλαγής μηνυμάτων, καθώς και την ασφάλεια του τερματικού (αυτό είναι το λειτουργικό σύστημα σε κάθε συσκευή). Απομακρυνθείτε από τα Windows, το OSX, το ChromeOS και το iOS. Αφαιρέστε τα G apps από το Android. Χρησιμοποιήστε τη DuckDuckGo αντι τις Google. Δοκιμάστε τις νέες εφαρμογές ανταλλαγής μηνυμάτων, μα προσέξτε για παρόχους που συνεργάζονται άμεσα με το κράτος. Τέλος, αν και δεν είναι για τον καθένα (ακόμα;), το Linux μπορεί να παρέχει

άριστη ασφάλεια στον υπολογιστή η το λάπτοπ σας. Στις περισσότερες πόλεις υπάρχουν κοινότητες χρηστών που μπορούν να σας βοηθήσουν στην εγκατάσταση αν δεν διαθέτετε τις τεχνικές γνώσεις.

4. Αποκεντρώστε τα δεδομένα σας: Το χειρότερο πράγμα που μπορεί να κάνει κάποιος είναι να μετακινήσει όλη τη ζωή του στα συστήματα της Google. Θα πρέπει να αναπτυχθεί μια κουλτούρα όπου οι επικοινωνίες μεταξύ των ριζοσπαστών, θα πραγματοποιούνται μέσα από πολλά κανάλια, με πολλά διαφορετικά ψευδώνυμα, και πολλούς διαφορετικούς λογαριασμούς email (τα email καθώς και οι λογαριασμοί που σχετίζονται με αυτά αποτελούν ένα πολύτιμο στόχο για την NSA). Μη χρησιμοποιείτε τα Google Docs. Σταματήστε να αφήνετε αυτούς τους μαλάκες να αρχειοθετούν τα εσωτερικά μας έγγραφα. Τα Ether Pads είναι μια εξαιρετική εναλλακτική, είναι αποκεντρωμένα και επιτρέπουν στα έγγραφα σας να αποθηκεύονται σε χιλιάδες διαφορετικούς servers για να επιλέξετε.

5. Low-tech όταν είναι δυνατό: Ο Μάο έλεγε "μάχονται με τον τρόπο τους, μαχόμαστε με τον δικό μας". Το νόημα ήταν ότι αν οι επαναστάτες βασίζονταν στην υψηλότερη τεχνολογία και το συμβατικό πόλεμο θα διαλύονταν. Απεναντίας έπρεπε να στηριχθούν στην μαζική κινητοποίηση εκατομμυρίων ανθρώπων, να πολεμήσουν με νέους και δημιουργικούς τρόπους που βασίζονταν στα προτερήματα των ανθρώπων τους. Το νόημα για εμάς είναι αυτό: Εάν οι ριζοσπάστες προσπαθήσουν να υπερκεράσουν τον εχθρό έχοντας καλύτερη κρυπτογράφηση και αρτιότερα εργαλεία, θα χάσουν. Η τρανταχτή αδυναμία των μπουρζουάδων είναι ότι όσο καλή και αν είναι η τεχνολογία τους χρειάζεται ανθρώπους για να λειτουργήσει άρα γίνεται ευάλωτη σε διαρροές τύπου Manning/Snowden, ή επιθέσεις από Hackers όπως αυτές των Anonymous. Από την άλλη, οι ριζοσπάστες θα πρέπει να υιοθετήσουμε μια πολιτική δια ζώσης συναντήσεων (face to face), όπου αυτό είναι εφικτό, καθώς και το να στηριχτούμε στις δυνάμεις μας αντί να παίζουμε το παιχνίδι της NSA. Δεν υπάρχει πάντα μια τεχνική λύση στο πρόβλημα της παρακολούθησης, οπότε επιλέξτε το πεδίο της αληθινής πολιτικής που δεν μπορούν να ανταγωνιστούν.

Η επιλογές που κάνουμε στο διαδίκτυο πρέπει να νοηθούν ως σημαντικές πολιτικές επιλογές και υπάρχει τώρα μια εξαιρετική ευκαιρία (όπου οι ΗΠΑ αποκαλύφθηκαν πλήρως μετά τη διαρροή του Snowden) να προωθήσουμε πιο ασφαλείς τρόπους στην επικοινωνία μεταξύ των ανθρώπων. Ελπίζω να καταφέρω να μπω σε λεπτομέρειες για συγκεκριμένες τεχνολογίες και λύσεις σε επόμενα άρθρα.

πηγή: kasamaproject

Διαβάστε επίσης τον οδηγό για ψηφιακή ασφάλεια από το

Δίκτυο για την Ψηφιακή Απελευθέρωση(dln.gr) εδώ.