Κρυπτογράφηση και τρομοκρατία

Nadim Kobeissi (Μετάφραση-Επιμέλεια: Barikat)

Λίγες μόνο μέρες χρειάστηκε να περάσουν μετά τις δίδυμες επιθέσεις σε Παρίσι και Λίβανο για να ξεκινήσει μια συζήτηση αναφορικά με τη χρήση κρυπτογραφημένων επικοινωνιών από τους δράστες και αν εν τέλει αυτό βοήθησε τον συντονισμό τους και εμπόδισε την πρόληψη της δράσης τους. Σε αντίθεση με το πλαίσιο που εξελισσόταν ο διάλογος στο θέμα της παρακολούθησης των ψηφιακών επικοινωνιών και των αντιδράσεων που προέκυψαν μετά τις αποκαλύψεις Snowden, τα πρόσφατα γεγονότα ήταν η αφορμή ώστε να αντιστραφεί το κλίμα υπέρ της ατζέντας της κρατικής επιτήρησης. Στη μετα-Snowden εποχή αυξήθηκε αισθητά η χρήση κρυπτογραφημένων επικοινωνιών από πολίτες αλλά και η δημιουργία νέων προγραμμάτων κρυπτογράφησης από κοινότητες ελεύθερου και ανοιχτού λογισμικού. Σήμερα φαίνεται να οδηγούμαστε στην ενίσχυση της αυθαιρεσίας του κράτους σε θέματα παρακολούθησης με πρόσχημα τη καταπολέμηση της τρομοκρατίας. Τα πρώτα αποτελέσματα φάνηκαν ήδη, καθώς χθες η Le Monde αποκάλυψε εσωτερικό έγγραφο βάση του οποίου προωθείται στο Γαλλικό κοινοβούλιο η απαγόρευση του TOR καθώς και η αναστολή λειτουργίας των ελεύθερων δημόσιων ασύρματων δικτύων σε περίπτωση έκτακτης ανάγκης. Ο Nadim Kobeissi, είναι προγραμματιστής, ερευνητής εφαρμοσμένης κρυπτογραφίας στο Ινστιτούτο INRIA στη Γαλλία και πολιτικός ακτιβιστής. Μεγάλωσε στη Βηρυτό και αργότερα μετακόμισε στη Γαλλία. Είναι γνωστός για τη συμβολή του στο λογισμικό Cryptocat το οποίο είναι ένα κρυπτογραφημένο chat που χρησιμοποιήθηκε εκτός των άλλων στην αραβική άνοιξη. Barikat «Αν παραδόσεις την ελευθερία σου για την ασφάλειά σου, δεν αξίζεις τίποτα από τα δύο». Benjamin Franklin

Υπό φως των πρόσφατων τρομοκρατικών επιθέσεων, τα πράγματα έχουν αρχίσει να αναθερμαίνονται σχετικά με τις τακτικές της ασφάλειας και τους προγραμματιστές λογισμικού κρυπτογράφησης. Όντας και εγώ ένας από αυτούς, βρέθηκα στην αμήχανη θέση να λάβω μια μικρή χιονοστιβάδα από αιτήματα δημοσιογράφων, πολιτικών αυθεντιών ακόμα και υπηρεσιών ασφαλείας. Είμαι επίσης κάποιος που γεννήθηκε και μεγάλωσε στη Βηρυτό και πρόσφατα μετακόμισα στο Παρίσι, και οι δύο πόλεις ήταν τόποι των δίδυμων επιθέσεων με μία μέρα διαφορά η μία με την άλλη.

Έκρινα ότι είναι απαραίτητο να μοιραστώ την οπτική μου σχετικά με το τι γίνεται με τα προγράμματα κρυπτογράφησης, τα οποία τάχα χρησιμοποίησαν οι τρομοκράτες, και τι σημαίνει αυτό σε σχέση με τα δικαιώματα και την ασφάλεια των παγκόσμιων κοινοτήτων μας.

Οι κοινότητες των προγραμματιστών, γράφουν μεγάλη ποικιλία λογισμικών, από προγράμματα ασφαλούς ανταλλαγής μηνυμάτων, μέχρι προγράμματα για την επικοινωνία του πύργου ελέγχου ενός αεροδρομίου και προγράμματα για τη πρόληψη συγκρούσεων δορυφόρων. Το κάνουμε αυτό για διάφορους λόγους, αλλά πάντα υπάρχει μια βαθύτερη κατανόηση μεταξύ μας: ότι είμαστε μαθηματικοί και μηχανικοί που συμβάλουμε σε μια ασφαλέστερη και πιο ικανή -για επικοινωνίες- κοινωνία με την αίσθηση της ιδιωτικότητας και της αξιοπρέπειας έμφυτη σε κάθε μοντέρνα κοινωνία. Η προϋπόθεση που οδηγεί τους ανθρώπους να γράφουν λογισμικό κρυπτογράφησης δεν είναι να δίνουν ή να αφαιρούν δικαιώματα από τους ανθρώπους. Η βασική προϋπόθεση είναι ότι ελπίζουμε να επιβάλουμε δικαιώματα που υπάρχουν ήδη χρησιμοποιώντας αλγορίθμους που εγγυώνται τη δυνατότητα στην ελευθερία του λόγου και στη λογική προσδοκία της ιδιωτικότητας στη καθημερινότητα. Όταν κάποιος πραγματοποιεί μια πληρωμή με πιστωτική κάρτα ή μπαίνει στο Facebook, χρησιμοποιεί την ίδια θεμελιώδη κρυπτογραφία που σε μια άλλη ήπειρο,

ένας διαδηλωτής χρησιμοποιεί για να οργανώσει μια πορεία ενάντια σε ένα αποτυχημένο καθεστώς.

Με κάποιο τρόπο, εφαρμόζουμε μια ουσιώδη τεχνολογική εξέλιξη όχι τόσο διαφορετική από την εφεύρεση των αυτοκινήτων ή των αεροπλάνων. Η Ford και η Toyota κατασκευάζουν αμάξια ώστε ο υπόλοιπος κόσμος να έχει πρόσβαση σε ταχύτερες μεταφορές και καλύτερη ποιότητα ζωής. Αν ένας τρομοκράτης πιθανολογείται ότι χρησιμοποιεί ένα αυτοκίνητο Toyota παγιδευμένο με εκρηκτικά, δεν είναι λογικό να περιμένουμε από την Toyota να αρχίσει να ελέγχει σε ποιον θα πουλάει τα αμάξια ή να απαιτούμε να σταματήσει τη παραγωγή.

Αυτά όμως ήταν τα ερωτήματα που άρχισαν να πολιορκούν τη κοινότητα των κρυπτογράφων αμέσως μετά τις επιθέσεις στο Παρίσι. Μια απλή αναφορά του λογισμικού κρυπτογράφησης που συμβάλλω σε ένα αραβόφωνο forum ήταν αρκετή για να αρχίσουν τα ερωτήματα του τύπου «Το γνωρίζεις ότι οι τρομοκράτες χρησιμοποιούν το πρόγραμμά σου; Νιώθεις ότι είναι ευθύνη σου να παρακολουθείς τη τρομοκρατική δραστηριότητα;». Ή πιο ξεκάθαρα, αν νιώθω ότι είμαι συνένοχος για βοήθεια προς τους τρομοκράτες, εξαιτίας του απλού γεγονότος ότι γράφω λογισμικό κρυπτογράφησης ή ότι κάνω διδακτορική έρευνα πάνω στην εφαρμοσμένη κρυπτογραφία.

Η συζήτηση που προκλήθηκε από το τύπο ήταν ακραία. Έλαβα κλήσεις που ωμά ήθελαν να μου πάρουν συνέντευξη σχετικά με «τη τεχνολογία που χρησιμοποιείται από τους τρομοκράτες, όπως η δική σας.» Ένα άρθρο του Wired, όπως πολλά άλλα, βρήκαν έναν οδηγό στα αραβικά πάνω στη κρυπτογράφηση και άμεσα του έδωσαν το όνομα «ο οδηγός του ISIS για τη κρυπτογράφηση» ακόμα και αν ήταν γραμμένος χρόνια πριν από ακτιβιστές στη Γάζα που δεν είχαν καμία σχέση με την τζιχαντιστική ομάδα.

Στη βιασύνη τους να κατηγορήσουν ένα πεδίο που είναι αρκετά άγνωστο στο ευρύ κοινό, και έτσι τρομακτικό και δελεαστικό, λίγη σημασία δόθηκε στα γεγονότα: Οι τρομοκράτες στο Παρίσι δε χρησιμοποίησαν κρυπτογραφία, αλλά συνεννοήθηκαν μέσω SMS, έναν τρόπο ψηφιακής επικοινωνίας που επιτηρείται πολύ εύκολα. Το γεγονός ότι δε τους έπιασαν, σημάνει αποτυχία της ανθρώπινης πληροφόρησης, όχι της δυνατότητας ψηφιακής επιτήρησης.

Αλλά ακόμα και υπό το φως των αποδείξεων που έδειχναν προς τη κατεύθυνση της ανθρώπινης παράλειψης, η κρυπτογράφηση, όντας για κάποιον εξωτερικό παρατηρητή σαν μια τρομακτική και μυστηριώδης χρήση μυστικών κωδικών και πολύπλοκων αλγορίθμων, παραμένει ο εύκολος στόχος. Ο Τύπος ξανά οδηγεί τη συζήτηση, κάθε φορά με μειωμένη προτεραιότητα για μετρημένα ερωτήματα και κανονική έρευνα. Γιατί δε βάλατε backdoors[1] στο λογισμικό σας; Θέλετε οι τρομοκράτες να χρησιμοποιούν τα εργαλεία σας;

Η συζήτηση για εισαγωγή backdoors δεν είναι καινούργια. Σε όλη τη διάρκεια τη καριέρας μου στον ιδιωτικό τομέα, έχω δει αιτήματα τοποθέτησης backdoor στα προγράμματα κρυπτογράφησης προς τέρψη των πιθανών επενδυτών, και έχω δει ανθρώπους στο χώρο που κατά τα άλλα υπερασπίζονται τα ασφαλή προγράμματα να δειλιάζουν με τη δικαιολογία «αν είναι αυτό που θέλει ο πελάτης», ακόμα και αν αυτό οδηγεί σε ένα ανεπανόρθωτο κενό ασφάλειας. Έχω δει καλοπροαίρετους αξιωματικούς μυστικών υπηρεσιών να με ρωτάνε επίσημα, από ειλικρινή περιέργεια, γιατί αρνούμαι να χρησιμοποιήσω backdoors. Το ζήτημα είναι ότι η κρυπτογραφία βασίζεται σε ένα σύνολο

μαθηματικών σχέσεων που δε μπορούν να ανατρέπονται επιλεκτικά. Είτε χρησιμοποιούνται ολοκληρωτικά είτε καθόλου. Δεν είναι κάτι που δεν είμαστε αρκετά έξυπνοι να κάνουμε, είναι κάτι που μαθηματικά είναι αδύνατο να γίνει. Δε μπορώ να βάλω backdoor σε κάποιο λογισμικό συγκεκριμένα για να παρακολουθώ τζιχαντιστές χωρίς αυτό το backdoor να εφαρμόζεται και σε κάθε μέλος της κοινωνίας που βασίζεται στο λογισμικό μου.

Και έχω δει τις εγγυήσεις που μια ασφαλής επικοινωνία μπορεί να δώσει στη κοινωνία. Έχω δει το λογισμικό μου να χρησιμοποιείται στο Hong-Kong για να οργανωθούν διαμαρτυρίες ενάντια στη κυβέρνηση που αρνείται να σεβαστεί τα δικαιώματά των ανθρώπων. Έχω δει συναδέλφους μου να παράγουν το λογισμικό που χρησιμοποιήθηκε στην Αίγυπτο κατά τη διάρκεια των διαδηλώσεων για δημοκρατία. Είχα παιδικούς φίλους που με καλούσαν από τη Βηρυτό, απεγνωσμένοι ώστε να μάθουν τρόπους να οργανώσουν πορείες ενάντια στη κυβέρνηση που θα τους φυλάκιζε αν χρησιμοποιούσαν απλά τηλέφωνα. Έχω στήσει διαύλους επικοινωνίας για LGBTQ οργανώσεις που έδιναν συμβουλές χωρίς να φοβούνται τον εξοστρακισμό ή τα αντίποινα. Και στη καινούργια μου ζωή στη Γαλλία, πάλι βασίστηκα στη κρυπτογραφία ώστε να ξέρω ότι διατηρώ το απλό δικαίωμά μου στην ιδιωτικότητα όταν συζητάω στη καθημερινότητα μου με τους φίλους μου ή με τη σύντροφό μου.

Έχω δει τη κρυπτογραφία σαν τη φυσική επέκταση ενός επιστήμονα πληροφορικής που μπορεί να προσφέρει, στη δημοκρατία. Τη διάχυση της απλής επιβεβαίωσης ότι μπορείς να ζεις ελεύθερα και ιδιωτικά, όπως κατοχυρώνεται στα συντάγματα και στις χάρτες της Γαλλίας, του Λιβάνου και των Ηνωμένων Πολιτειών της Αμερικής. Η αφαίρεση αυτών των εγγυήσεων δεν είναι λειτουργική. Δε παράγει καλύτερη πληροφόρηση. Δεν είναι η αιτία που η πληροφόρηση μας δεν είναι αρκετά ανταγωνιστική από τη πρώτη στιγμή. Αλλά βοηθάει τις τρομοκρατικές ομάδες να καταστρέψουν τον ηθικό χαρακτήρα της πολιτικής από μέσα, όταν από φόβο, καταργούμε τις αρχές μας.

Αν μαζέψουμε όλα τα αμάξια από τους δρόμους, κάθε iPhone από κάθε άνθρωπο, κάθε αεροπλάνο από τον ουρανό, δε θα σταμάταγε τη τρομοκρατία. Η τρομοκρατία δεν έχει να κάνει με τα μέσα αλλά με τους σκοπούς. Δεν έχει να κάνει με τη τεχνολογία, αλλά με το θυμό, την άγνοια που κατοικεί στο μυαλό αυτού που τη πράττει.

Μεγάλωσα και έζησα μια δεκαετία της παιδικής μου ηλικίας στη νότια Βηρυτό και ήμουν κυριολεκτικά γείτονας με το τομέα ασφαλείας της Χεσμπολάχ, μια αντάρτικη ομάδα που πολεμάει συχνά με το Ισραήλ. Κατά τη διάρκεια του πολέμου του 2006, ένα Ισραηλινό μαχητικό βομβάρδισε ολόκληρη τη γειτονιά, καταστρέφοντας το σπίτι μου αλλά και πολλών άλλων στη γειτονιά. Καθώς περπατούσα πάνω στα ερείπια και στη άσκαστες βόμβες ψάχνοντας να βρω στο σπίτι μου, είδα από μακριά ένα φίλο μου, μακριά στην άλλη μεριά των ερειπίων που υπήρχαν ανάμεσα μας. Κοιταχτήκαμε. Ύστερα, βάλαμε τα γέλια. Γελάγαμε για αρκετή ώρα.

Το 2008, είχα την ευκαιρία να μετακομίσω μακριά από το Λίβανο για εκπαίδευση στο εξωτερικό. Η ευκαιρία ήταν σπάνια και ασυνήθιστη. Να φτιάχνεις προγράμματα κρυπτογράφησης είναι δύσκολο, επίσης: για πολλά από τα πρώτα μου χρόνια στο εξωτερικό, πολλά από τα προγράμματά μου ήταν γεμάτα bugs και έκανα πολύ προσπάθεια και εποικοδομητική κριτική για να καταφέρω να τα κάνω σωστά-συγκεκριμένα, αυτό που στη πραγματικότητα αποτέλεσε την εκπαίδευσή μου εκτός Λιβάνου.

Επισκεπτόμενος τη Βηρυτό χρόνια μετά, ανακάλυψα ότι είχα αλλάξει, αλλά δεν είχε

αλλάξει κανείς άλλος από όσους έμειναν εκεί. Τα συντρίμμια είχαν σχεδόν εξαφανιστεί. Ανακάλυψα επίσης ότι οι άνθρωποι ήταν θυμωμένοι, και ότι η Χεσμπολάχ είχε υποσχεθεί να ξαναχτίσει τα σπίτια. Έφευγαν χωρίς ελπίδα για μια καλή εκπαίδευση, χαρούμενη ζωή, με πολλά μέλη των οικογενειών τους να έχουν χαθεί, φίλους νεκρούς, πολλοί υποσχέθηκαν στον εαυτό τους να γυρίσουν.

Αυτό προκαλεί τη τρομοκρατία, όχι το λογισμικό κρυπτογράφησης.

Πηγή

[1] Backdoor σε ένα κρυπτογραφικό σύστημα είναι η εισαγωγή μεθόδων η οποία θα διευκόλυνε έναν τρίτο να παρακάμψει τη αυθεντικοποίηση ανάμεσα σε δύο μέρη και να αποκρυπτογραφήσει μια επικοινωνία.