

εισαγωγή

σε πολλές λειτουργίες μας, μπορεί να μας προδώσει το μέσο με το οποίο τις κάνουμε. πχ αν θέλω να κάνω μια πλάκα στο φίλο μου, γράφοντας ένα γράμμα που θα παριστάνω την X κλήρωση λαχείου, σε επεξεργαστή κειμένου που προσθέτει στις πληροφορίες αρχείου το username (όνομα χρήστη) μου, έ μάλλον θα με καταλάβαινε. είναι μάλλον προφανές ότι αν του το έστελνα από το κανονικό μου email, και όχι κάποιο ψεύτικο, θα με ψυλιαζόταν πριν ακόμη φτάσει στο συννημένο. τα παρακάτω παραδείγματα, μπορεί να σας φανούν από αστεία μέχρι εξωπραγματικά, είναι όμως μερικοί πιθανοί κίνδυνοι...

επίπεδα παράνοιας

Για να αναλύσουμε καλύτερα τα διαφορετικά επίπεδα κινδύνου που μπορεί να μας παρουσιαστούν,

(α) απλή προφύλαξη

Για παράδειγμα, από τον κουτσομπόλη κακό “γείτονα”, το αφεντικό μας, κλπ. Που μπορεί να μας παρακολουθεί και κουτσομπολεύει τα σαιτς στα οποία δημοσιεύουμε, τα ανοικτά forums, chat rooms ή λίστες ταχυδρομείου, κλπ. Υποθέτουμε ότι δεν είναι computer expert geek, ή δεν έχει αρκετά χρήματα για να προσλάβει ένα τέτοιο geek. Για τον φυσικό κόσμο, αρκούν οι προφανείς προφυλάξεις που επιβάλλει η κοινή λογική...

(β) μη στοχευμένη παρακολούθηση

Υποθέτουμε ότι πρόκειται για κάποιον που έχει τεχνικές δυνατότητες και γνώσεις, αλλά δεν έχει λόγο να ασχοληθεί με εμάς. Κάποιος που χαζεύει το indymedia, και αποφασίζει τυχαία να ακολουθήσει τα links από μια συλλογικότητα που του κίνησε το ενδιαφέρον μια δημοσιευσή της, ή μια αφίσα, κλπ. Για παράδειγμα, βρέθηκε στα χέρια του υλικό (αφίσα, cd, site, κλπ) από μια συλλογικότητα που δεν γουστάρει τα windoze και λέγεται sid και θέλησε να τους καταγράψει...

(γ) Παρακολούθηση χώρου

Ο όρος μπορεί να αναφέρεται σε ένα πολιτικό χώρο, σε ένα γεωγραφικό χώρο, κλπ. Στο ιντερνετικό επίπεδο, μπορεί να καταγράφεται όλη η κίνηση προς ένα ή περισσότερους servers, με τη συνεργασία ενός ή όλων των ISPs μιας χώρας.

(δ) Παρακολούθηση ατόμων

Στο ιντερνετικό επίπεδο, καταγραφή των κινήσεων συγκεκριμένων ατόμων. Μπορεί να ζητηθεί η συνεργασία και ξένων ISPs.

(ε) Παγίδευση ατόμων

Στο ιντερνετικό επίπεδο, παρακολούθησης και τροποποίηση πακέτων, ανέβασμα ψεύτικων sites, αλλαγή certificates, κλπ.

πιθανά σενάρια

Για την καλύτερη παρουσίαση, τα χωρίσαμε σε πιθανά σενάρια, που θα αναλύσουμε με βάση τα παραπάνω επίπεδα. Οι οδηγίες προστασίας για κάποιο επίπεδο παράνοιας, είναι αυτές του αμέσως προηγούμενου + όποιες καινούργιες εμφανίζονται. δηλαδή, στο επίπεδο β, εφαρμόζουμε ότι βρήκαμε στο επίπεδο α + αυτά που προτείνονται για το β...

Τί να προσέξω όταν ανεβάζω μια φωτογραφία/ένα σκανάρισμα;

(α)

- όνομα αρχείου. Κάθε φωτογραφική κάμερα, σώζει τις φωτογραφίες με συγκεκριμένο όνομα αρχείου και αύξων αριθμό. πχ DSCN9954.jpg. Είναι ένα πρώτο στοιχείο για το ποια κάμερα χρησιμοποιούμε. Αλλά αλλάζουμε το όνομα σε κάτι σχετικό με τη φωτογραφία...
- exif data. Όλες οι ψηφιακές μηχανές, στο αρχείο της φωτογραφίας, σώζουν και διάφορες πληροφορίες, για το πότε τραβήχτηκε, το serial number της μηχανής, κλπ. αυτές οι πληροφορίες πέραν από άχρηστες για εμάς, συνδέουν φαινομενικά άσχετες μεταξύ τους φωτογραφίες στην ίδια φωτογραφική μηχανή. [Αφαίρεση exif data](#)

(β)

- Ταυτοποίηση κάμερας. Η κάθε κάμερα, έχει διαφορετική ευαισθησία σε διάφορες παραμέτρους, όπως φως, χρώμα, κλπ. Είναι αρκετά εφικτό να προσδιοριστεί από ένα μικρό δείγμα φωτογραφιών ότι η ίδια κάμερα έχει τραβήξει και μια ανώνυμη φωτογραφία...

<http://www-video.eecs.berkeley.edu/Proceedings/ICIP2004/defevent/papers/cr2683.pdf> Συνίσταται να χρησιμοποιούμε μια “καθαρή” κάμερα, μόνο για ανώνυμες φωτογραφίες, ώστε να μην μπορούν να συνδεθούν με μας...

- [Δημοσιεύοντας ανώνυμα.](#)

(γ)

(δ)

(ε)

Τί να προσέξω όταν εκτυπώνω κάτι;

(α)

(β)

- Πολλοί εκτυπωτές, αφήνουν την υπογραφή τους στο χαρτί που τυπώνουν. Αυτή η τεχνική λέγεται υδατογράφημα, γνωστή και ως yellow dots. Για να το αποφύγουμε, όταν αγοράζουμε, (ή βρίσκουμε) εκτυπωτή, φροντίζουμε να είναι κάποιος από την παρακάτω λίστα:

<http://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots> - Επίσης, φροντίζουμε να είμαστε αγορασμένος ανώνυμα και όχι στο ονομά μας...

(γ)

Φυσικά φροντίζουμε να μην αφήνουμε άλλου τύπου ίχνη. Δες στο [βιομετρική αναγνώριση](#)

(δ)

(ε)

Τί να προσέξω όταν γράφω ένα cd/dvd;

(α)

(β)

(γ)

Κάθε εφαρμογή εγγραφής cd, γράφει με διαφορετικό τρόπο. Οπότε διαλέγουμε κάποια σχετικά δημοφιλή εφαρμογή. Και επειδή μας αρέσει το ελεύθερο λογισμικό, δεν μιλάμε για το nero, αλλά για brasero (linux), k3b (linux), imgburn (δεν είναι ελεύθερο, αλλά δεν είναι nero) Φυσικά φροντίζουμε να μην αφήνουμε άλλου τύπου ίχνη. Δες στο [βιομετρική αναγνώριση](#)

(δ)

(ε)

Για extra πόντους παράνοιας, μπορεί να υπάρχει ξεχωριστό cd/dvd writer (φυσικά πάλι, όχι στο ονομά μας), που να χρησιμεύει μόνο στην ανώνυμη εγγραφή cd...

Τί να προσέξω όταν γράφω/ανεβάζω κάτι σε ένα site;

(α)

Διάφορα site ζητούν λογαριασμό για τη δημοσίευση σε αυτά. Πάντα φτιάχνουμε λογαριασμούς με ψευδή στοιχεία, που όμως να είναι αληθοφανή. Α το email μαλλον χρειάζεται να είναι εγκύρο, αλλά σε καμία περίπτωση το κανονικό μας. Φτιάχνουμε ένα καινούργιο ανώνυμο webmail λογαριασμό. Αλλάζουμε τακτικά τον ανώνυμο λογαριασμό που χρησιμοποιούμε και φροντίζουμε να μην συνδέεται με τους προηγούμενους. πχ όχι sid, sid1, sid2, ή vicious, κλπ

(β)

-αναγνώριση συγγραφέα Είναι αρκετά εφικτό, να διαπιστώσουμε αν δυο έγγραφα έχουν γραφτεί από τον ίδιο συγγραφέα, αναλύοντας το λεξιλόγιο, το στυλ γραφής, κλπ. Για αυτό το πρόβλημα δεν υπάρχει εύκολη λύση πέραν από το να μη δημοσιεύουμε ποτέ επώνυμα.

<http://www.sigkdd.org/explorations/issue5-2/Task4-Place3.pdf>

(γ)

Χρησιμοποιούμε το δίκτυο tor με https. Ένας εύκολος τρόπος είναι το privatix live-cd, που τα έχει όλα εγκατεστημένα. Τα προγράμματα που χρειαζόμαστε, είναι τα: tor, polipo, firefox, torbutton, vidalia (ή tork). Σε linux τα κατεβάζουμε μέσα από τον package manager. Για windows, υπάρχει ένα πακετάκι με όλα αυτά (<http://www.torproject.org/torbrowser/index.html.en>)

Για επιπλέον πόντους παράνοιας, συνδεόμαστε σε κάποιο wireless, σύμφωνα με τις οδηγίες εδώ: [Τί να προσέξω όταν "δανείζομαι" wireless;](#)

(δ)

(ε)

Τί να προσέξω όταν επισκέπτομαι ένα site;

(α)

(β)

(γ)

όπως και στο (γ) του παραπάνω σεναρίου...

(δ)

(ε)

Τί να προσέξω όταν στέλνω/θέλω να λάβω ένα ανώνυμο email;

(α)

-Συνδεόμαστε πάντα με https στο webmail σε ξεχωριστό ανώνυμο account, το οποίο αλλάζουμε τακτικά. Γενικά φτιάχνουμε ξεχωριστά email accounts για κάθε μας δουλειά...

(β)

(γ)

-όπως και στο (γ) του “Τί να προσέξω όταν γράφω/ανεβάζω κάτι σε ένα site;” - για να κρατήσουμε την ταυτοτητά μας μπορούμε να υπογράψουμε τα μνηματά μας με pgr και να τα στέλνουμε σαν συνημμένα... οδηγίες για το pgr, στον οδηγό για το [enigmail](#)

(δ)

(ε)

Τί να προσέξω όταν ανοίγω ένα λογαριασμό (account);

(α)

Όταν ανοίγουμε οποιοδήποτε λογαριασμό, είτε είναι ο χρήστης στον υπολογιστή μας, ένα email, ή σε κάποιο site, ποτέ μα ποτέ δεν χρεάζεται να βάλουμε το ονοματάκι μας. Το ίδιο ισχύει για τα υπόλοιπα στοιχεία μας, ημερομηνία γέννησης, τόπο καταγωγής, φύλο, φίλους/ες, διεύθυνση, μουσικές προτιμήσεις, κλπ κλπ Για κάθε ξεχωριστή δουλειά, ανοίγουμε ένα διαφορετικό account

και το χρησιμοποιούμε μόνο για αυτην. Πχ, ξεχωριστό email για τη δουλειά, τη σχολή ή τα κινηματικά. Αν είναι εφικτό, αλλάζουμε ταυτότητες τακτικά...

(β)

(γ)

(δ)

(ε)

Παράρτημα

Τί να προσέξω όταν "δανείζομαι" wireless;

Πρώτα από όλα, χρησιμοποιουμε το live-cd ωστε να είμαστε σίγουροι ότι δεν θα μας προδώσει κάποιο πρόγραμμα που τρέχει στον υπολογιστή μας. Στη συνέχεια, αλλάζουμε τη mac address της ασύρματης κάρτας δικτύου. Πάμε σε ένα μέρος που δεν είναι στη γειτονία μας ή σε μέρος που συχνάζουμε και δεν μας βλέπει κάποια κάμερα (ή κανάς κακός γείτονας), βρίσκουμε ένα ανοικτό δίκτυο και συνδεόμαστε MONO με https. Αν είναι δυνατόν, συνδυάζουμε και τη χρήση tor, για extra paranoia...

βιομετρική αναγνώριση

Σαν κομπιουτεράδες, αναλύσαμε όλο το κομμάτι που μας αντιστοιχεί. Πέραν τούτου, ένα τυπωμένο κείμενο ή ένα cd, μπορεί να μας προδώσει με τους παλιούς καλούς τρόπους, δείγματος DNA ή των δακτυλικών αποτυπωμάτων...

συνομοιωτικότητα

Όπως και σε τόσους άλλους τομείς, έτσι και στον ψηφιακό κόσμο, δεν λέμε/γράφουμε πράγματα που δεν θα λέγαμε, πχ σε ένα φυσικό χώρο, σε μια πλατεία, στο μετρό ή στο καφενείο...

ελεύθερο λογισμικό

Και για τη διαφύλαξη της ιδιωτικότητάς μας, επιλέγουμε το ελεύθερο λογισμικό, που ξέρουμε (σαν κοινότητα) πως δουλεύει, πως δεν μπορεί να κρυφτεί εύκολα κάτι κακόβουλο σε αυτό. Όμοια με το λογισμικό, επιλέγουμε και τους οδηγούς (drivers) μιας συσκευής. Αν πχ έχουμε προμηθευτεί έναν εκτυπωτή που εγγυημένα δεν θα μας προδώσει, μην την πατήσουμε από τους κλειστούς οδηγούς του (proprietary drivers), που μπορεί να κρύβουν παγίδες για μας...

Αφαίρεση exif data

αν και νομίζω πως αρκεί να ανοιχτεί μια φωτογραφία με ένα πρόγραμμα επεξεργασίας φωτογραφίας και να το σώσουμε με άλλο όνομα (save as). αυτές οι πληροφορίες αφαιρούνται εύκολα, αν ανοίξουμε τη φωτογραφία και κάνουμε ένα από τα παρακάτω:

από αναζήτηση στο internet:

- In Photoshop - "save for web..." from File menu.
- In gimp 2.2 - uncheck "Save exif info" when saving photo (advanced options, below quality slider).

- Or you can use site EXIFremover <http://exifremover.com/>

για GNU/linux:

- Με το Imagemagick εγκατεστημένο, δίνουμε την εντολή

```
$ mogrify -strip όνομα_εικόνας.jpg
```

αν θέλουμε να αφαιρέσουμε τα exif metadata σε πολλές εικόνες αρκεί να δώσουμε :

```
$ mogrify -strip *.JPG
```

- Με το jhead μπορούμε να πειράξουμε όπως θέλουμε τα exif metadata μιας εικόνας. με την εντολή

```
$ jhead -purejpg όνομα_εικόνας.jpg
```

καθαρίζουμε την εικόνα από αυτά. περισσότερες λεπτομέρειες στη σελίδα του jhead

<http://www.sentex.net/~mwandel/jhead/>

ενδιαφέρον link : <http://hacktux.com/read/remove/exif>

live cds

- incognito live cd

<http://anonymityanywhere.com/incognito/>

- privatix (iso + test usb)

<http://mandalka.name/privatix/download.html.en>

- ubuntu privacy remix

<https://www.privacy-cd.org/en/using-upr/download>