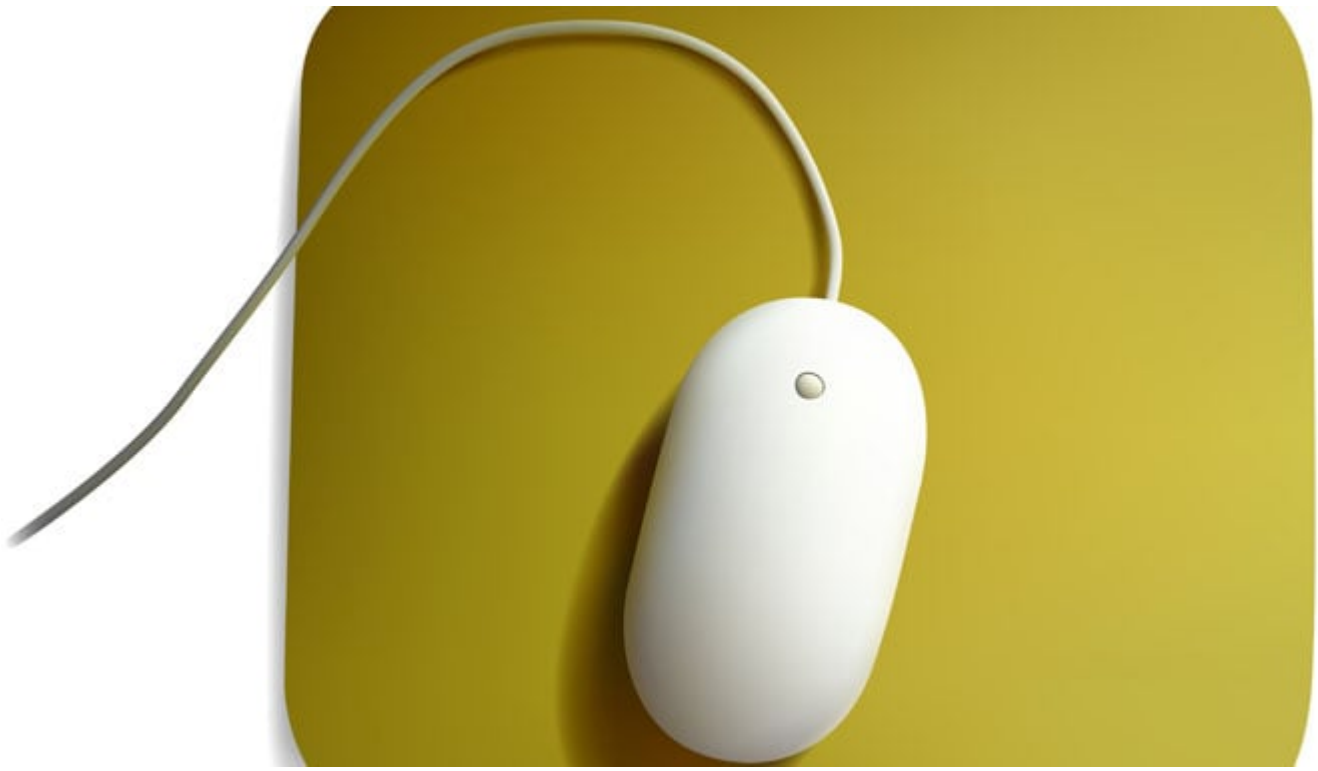
21 Μαρτίου 2016

Προσοχή: Οι κινήσεις του ποντικιού σας αποκαλύπτουν την ταυτότητά σας!

/ Πεμπτουσία

Image not found or type unknown



Δίκτυο Tor|Οι κινήσεις του mouse αποκαλύπτουν τη ταυτότητά των χρηστών

Ανεξάρτητος ερευνητής ασφάλειας παρουσιάζει νέες μεθόδους για την άρση της ανωνυμίας των χρηστών του δικτύου Tor[1]. Οι χρήστες μπορούν να εντοπιστούν με βάση τις κινήσεις του ποντικιού τους, ενώ και άλλες τεχνικές fingerprinting αξιοποιούνται για την αποκάλυψη της ταυτότητας των χρηστών.

Ο ανεξάρτητος ερευνητής ασφαλείας Jose Carlos Norte έχει ανακαλύψει μια σειρά από νέες μεθόδους ταυτοποίησης των χρηστών του δικτύου *Tor*, οι οποίες μπορούν να χρησιμοποιηθούν για την άρση της ανωνυμίας τους, κατά τη διάρκεια καταχρηστικών ερευνών από τις αρχές επιβολής του νόμου ή σε εκστρατείες κυβερνο-επιτήρησης.

Η διαδικασία του «user fingerprinting» αναφέρεται σε τρόπους εντοπισμού μη τυποποιημένων ενεργειών, καθώς και πληροφοριών σχετικά με τη συμπεριφορά των χρηστών. Παρότι οι υπηρεσίες analytics, οι οποίες συλλέγουν πλήθος τέτοιων πληροφοριών, μπλοκάρονται επιτυχώς από τους Tor Browsers, υπάρχουν αρκετές μέθοδοι «fingerprinting» που μπορεί να αποκαλύψουν τη ταυτότητά των χρηστών, καθώς τα δεδομένα που καταγράφονται ενώ σερφάρουν στο web μέσω Tor, μπορούν σε δεύτερο χρόνο να συγκριθούν με τα δεδομένα που καταγράφονται ενώ περιηγούνται στον κανονικό τους browser.

Ο κ. Norte έχει δημοσιεύσει στο blog του μια σειρά από τεχνικές fingerprinting που είναι αποτελεσματικές έναντι των χρηστών του Tor Browser, μαζί με μια σελίδα όπου αποδεικνύει την έρευνά του.

Τα δεδομένα που συνήθως καταγράφονται από τα συστήματα fingerprinting δεν είναι 100% αξιόπιστα και ακριβή, όμως αποτελούν ένα σημείο εκκίνησης για μελλοντικές έρευνες.

Η πρώτη τεχνική που αναφέρεται, αφορά στην καταγραφή της ταχύτητας με την οποία οι χρήστες κάνουν scroll σε μια σελίδα, χρησιμοποιώντας το mouse wheel. Ακόμη και αν η ταχύτητα κύλισης είναι η ίδια για όλα τα ποντίκια, ένας εισβολέας θα μπορούσε να εντοπίσει μοτίβα και patterns στα γεγονότα κύλισης (scroll events) με βάση την ιδιοσυγκρασία του κάθε ατόμου.

Μια ακόμη μέθοδος fingerprinting περιλαμβάνει τη καταγραφή της ταχύτητας με την οποία οι χρήστες μετακινούν το δείκτη του ποντικιού σε μια σελίδα. Δεδομένου ότι ο κάθε χρήστης έχει τις δικές τους προτιμήσεις ευαισθησίας – έχοντας προσαρμόσει αντίστοιχα τις ρυθμίσεις OS του ποντικιού – αλλά και το δικό του τρόπο χειρισμού της συσκευής, η τεχνική αυτή είναι πολύ πιο ακριβής σε σχέση με την προηγούμενη και μπορεί να χρησιμοποιηθεί για την επιτυχή ταυτοποίηση των χρηστών.

Ακόμη χειρότερα, εάν ένας χρήστης χρησιμοποιεί κάποιο trackpad για την περιήγησή του σε μια σελίδα, η τεχνικές fingerprinting γίνονται ακόμα πιο ακριβείς, προσθέτοντας επακριβείς μετρήσεις ταχύτητας στα ήδη καταγεγγραμμένα μοτίβα κύλισης και μετακίνησης.

Ο ερευνητής ανακάλυψε ότι θα μπορούσε να συλλέξει επίσης τα αποτυπώματα όχι μόνο οποιουδήποτε χρήστη αλλά και οποιουδήποτε μηχανήματος. Μέσω της εκτέλεσης μιας CPU intensive λειτουργίας JavaScript στο πρόγραμμα περιήγησης, θα μπορούσε να καταγράψει το χρόνο που απαιτείται για την εκτέλεση μιας

διαδικασίας και να χρησιμοποιήσει αυτές τις πληροφορίες αργότερα για τον εντοπισμό υπόπτων, εντοπίζοντας τον υπολογιστή από τον οποίο χρησιμοποιήθηκε το πρόγραμμα περιήγησης Tor.

Σε μια άλλη παρόμοια μελέτη που διεξήχθη λίγες εβδομάδες νωρίτερα, ο κ Norte ανακάλυψε επίσης ότι ορισμένοι διακομιστές Apache που δεν έχουν ρυθμιστεί σωστά θα μπορούσαν να διαρρεύσουν τη γενική τοποθεσία ενός χρήστη Tor, εάν ο διακομιστής τρέχει κάτω από υπό ορισμένες συνθήκες.

Πηγή: [secnews.gr]

---

* *Το Tor (συντομογραφία του The onion router) είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο. Το λογισμικό πελάτη Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κίνησης.*