LANQUETIN Alexis
GONZALEZ Jules

WEB BROWSER FINGERPRINTING

I - Que sont les Web Browser Fingerprint
II - Comment fonctionnent-elles ?
III - Quelques cas d'utilisation
IV - Comment limiter les informations récoltées ?
V - Demonstration

Identifier les utilisateurs

- Éléments HTTP
- Configuration du navigateur
- Configuration machine
- Adresse IP

Identification à 99% de certitude

Cookies vs Fingerprints

Peuvent être supprimés, bloqués	Ne peuvent pas être bloquées
Utilisent des informations personelles	Utilisent seulement des données matérielles et software
Sont stockés sur l'appareil	Ne sont pas stockées

Comment sont récupérées les fingerprint

Passif fingerprinting

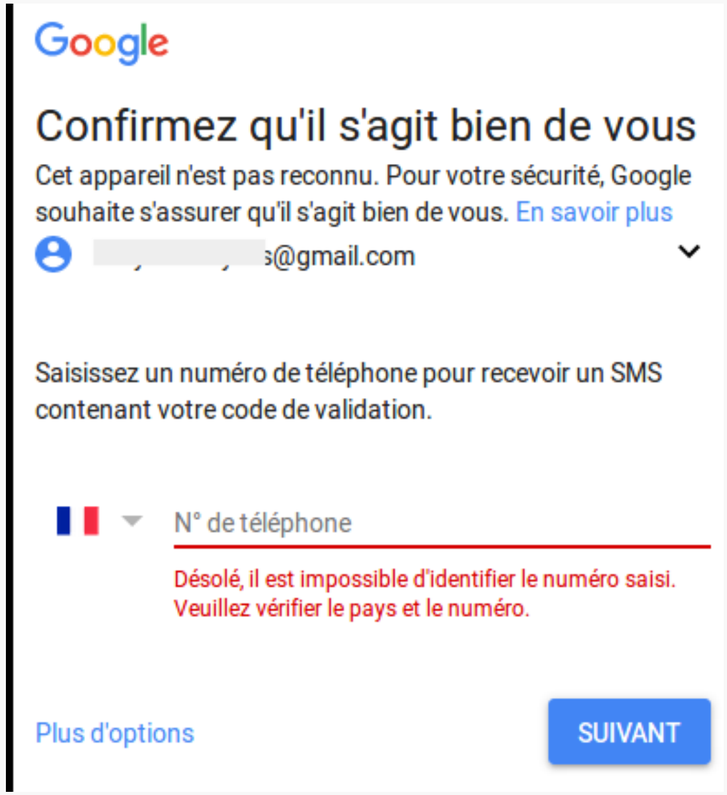
- User Agent
- HTTP ACCEPT headers
- System platform
- Encoding
- IP Adress

Actif fingerprinting

- JavaScript
  - Screen resolution, color depht
  - Canvas, WebGL
  - Extension, plugin
  - Timezone
  - File formats
- Cookies, DoNotTrack, ...
- Device (peripherals, sensors...)
- Audio

Cas d'utilisation

Sécurité



Publicité

Agences de surveillance

Statistiques

Comment se protéger ?

navigation privée

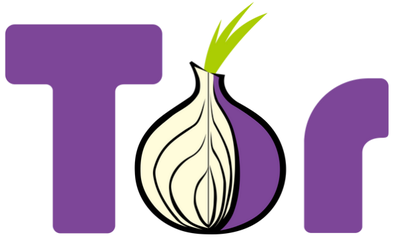


Bloqueurs de trackers et scripts

Utiliser une VM

Utiliser un VPN

Désactiver les scripts



Utiliser des navigateurs résistants aux fingerprints

https://www.expressvpn.com/blog/best-browsers-for-privacy/

8

12

15

Démonstration

Pour conclure

NordVPN®

Merci pour votre attention