RESISTENZA DIGITALE:
CONSIGLI PER LA PRIVACY

MARIANO GRAZIANO

Palermo, Italy - 28/10/2017

whoami

- Ricercatore per Cisco Talos
- Msc Politecnico di Torino
- Ph.D. Telecom ParisTech/Eurecom

PRIVACY

"La vita personale, privata, dell'individuo o della famiglia, in quanto costituisce un **diritto** e va perciò **rispettata** e **tutelata**"

http://www.treccani.it/vocabolario/privacy/

PRIVACY ONLINE

“il diritto di controllare l'uso e la circolazione dei propri **dati personali** che costituiscono il bene primario dell'attuale società dell'informazione.”

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1663787

PRIVACY NEL 2017

Il Parlamento vuole allungare a 6 anni la conservazione di tabulati e dati internet

Un emendamento approvato alla Camera, se confermato al Senato, estenderà a 72 mesi la data retention. Ma montano le perplessità tra avvocati e associazioni

MINACCE PRIVACY

- Web Tracking
- Grandi aziende (Google, FB, MS, Amazon, etc)
- Furto di dati
- ISP
- Governi

WEB TRACKING

“Web Tracking”

MOTIVAZIONI

- Statistiche
- Pubblicità

GDS.IT

DISCONNECT

Show list view

GDS gds.it

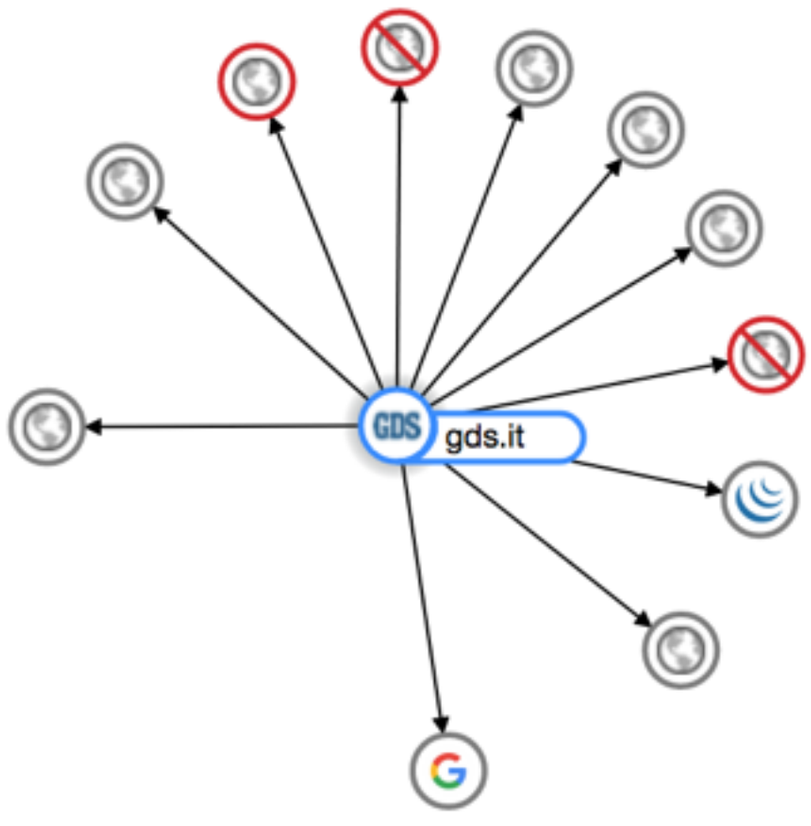
When you visit this site, the following sites are informed:

- gstatic.com
- ajax.googleapis.com
- ~~google-analytics.com~~
- fonts.googleapis.com
- googletagmanager.com
- ~~amazon-adsystem.com~~
- imasdk.googleapis.com
- jquery.com
- cdn-immedia.net
- performgroup.com
- performfeeds.com

Unblock tracking sites

Hide sidebar

Show instructions



REPUBBLICA.IT

DISCONNECT

Show list view

repubblica.it

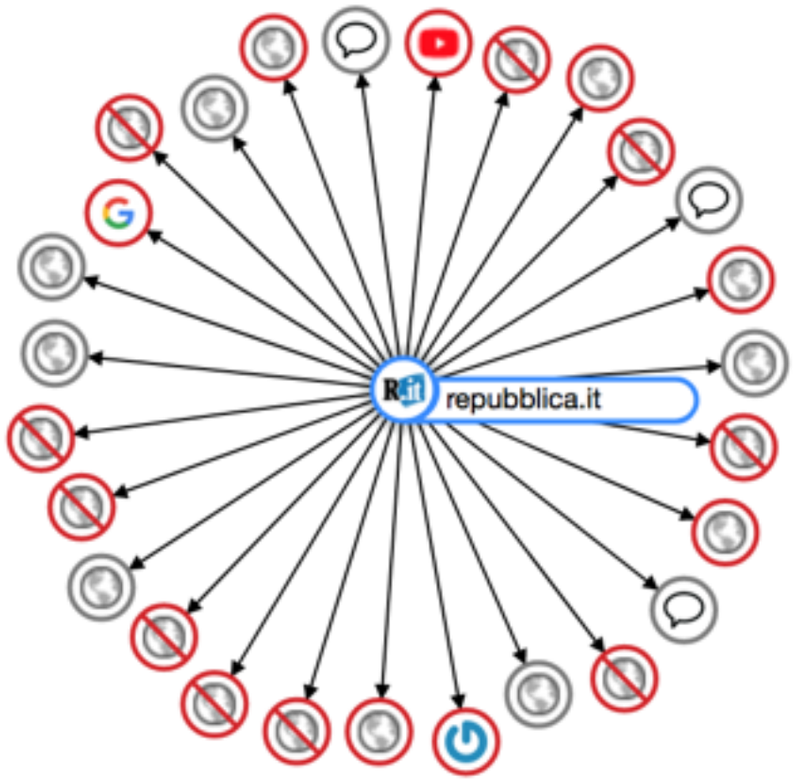
When you visit this site, the following sites are informed:

- google.it
- gstatic.com
- ~~apis.google.com~~
- ogs.google.com
- clients5.google.com
- www.google.com
- ~~doubleclick.net~~
- play.google.com
- ~~google-analytics.com~~
- gravatar.com
- ~~facebook.com~~
- ~~facebook.net~~
- ~~twitter.com~~
- ~~scorecardresearch.com~~
- youtube.com
- ytimg.com
- ~~imrworldwide.com~~
- imasdk.googleapis.com
- akamaihd.net
- gigya.com
- ~~webtrekk.net~~
- repstatic.it
- kataweb.it
- 4wnet.com
- ~~taboola.com~~
- lescienze.it
- gelestatic.it

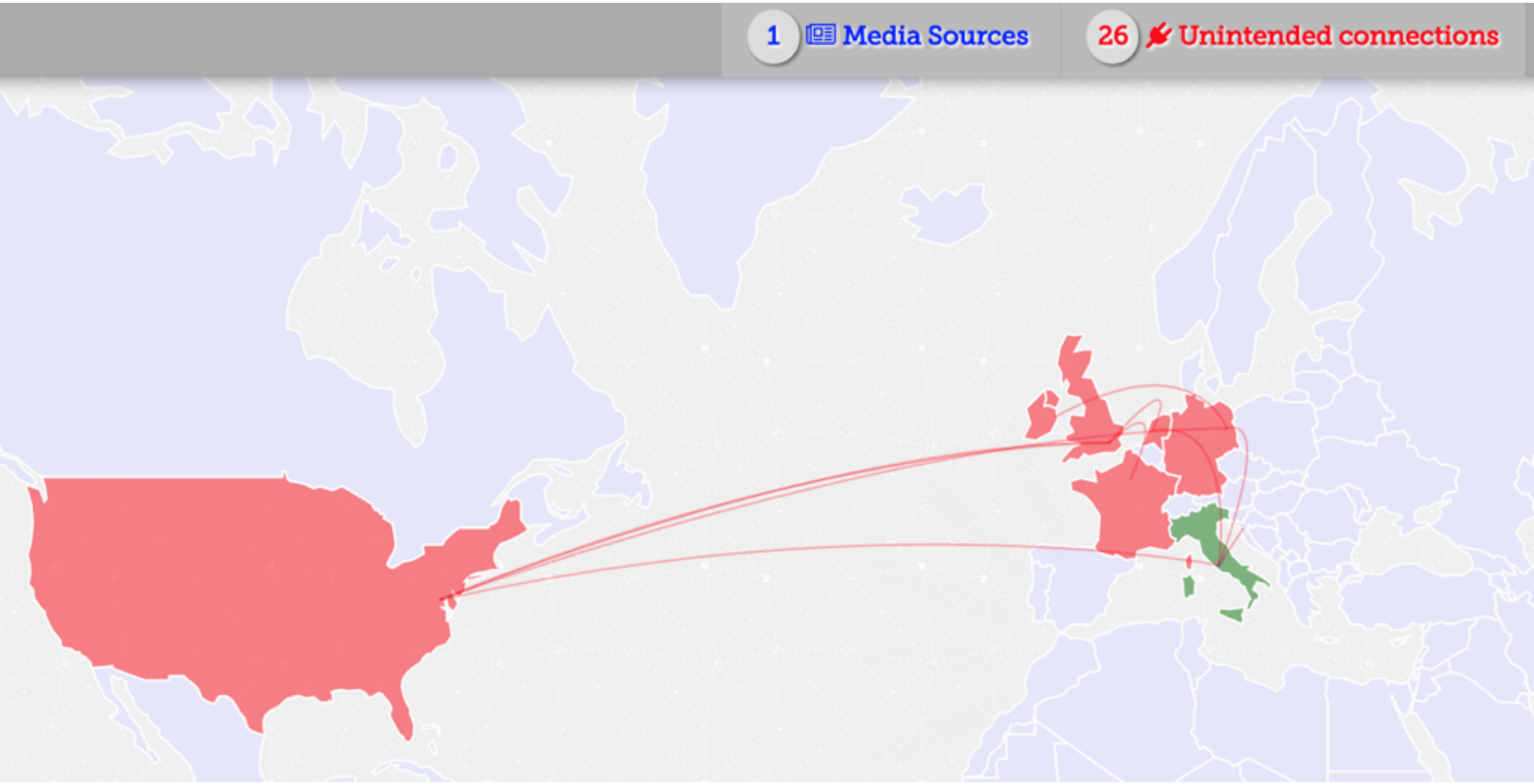
Unblock tracking sites

Hide sidebar

Show instructions



REPUBBLICA.IT



https://trackography.org

REPUBBLICA.IT

COMPANIES TRACKING YOU

Through the media websites you have selected, the following companies can have access to your data (such as your IP address and browsing habits): Click on the name of a company to learn more about it. click to see the legend

repubblica.it

	National Laws	Profiling	Data Retention	Third Parties	Supports DNT
Google		✔	?	✔	✖
Facebook		✔	?	✔	✖
Nielsen					
WPP					
Webtrekk					
Gigya					
DG					

https://trackography.org

CORRIERE.IT

DISCONNECT

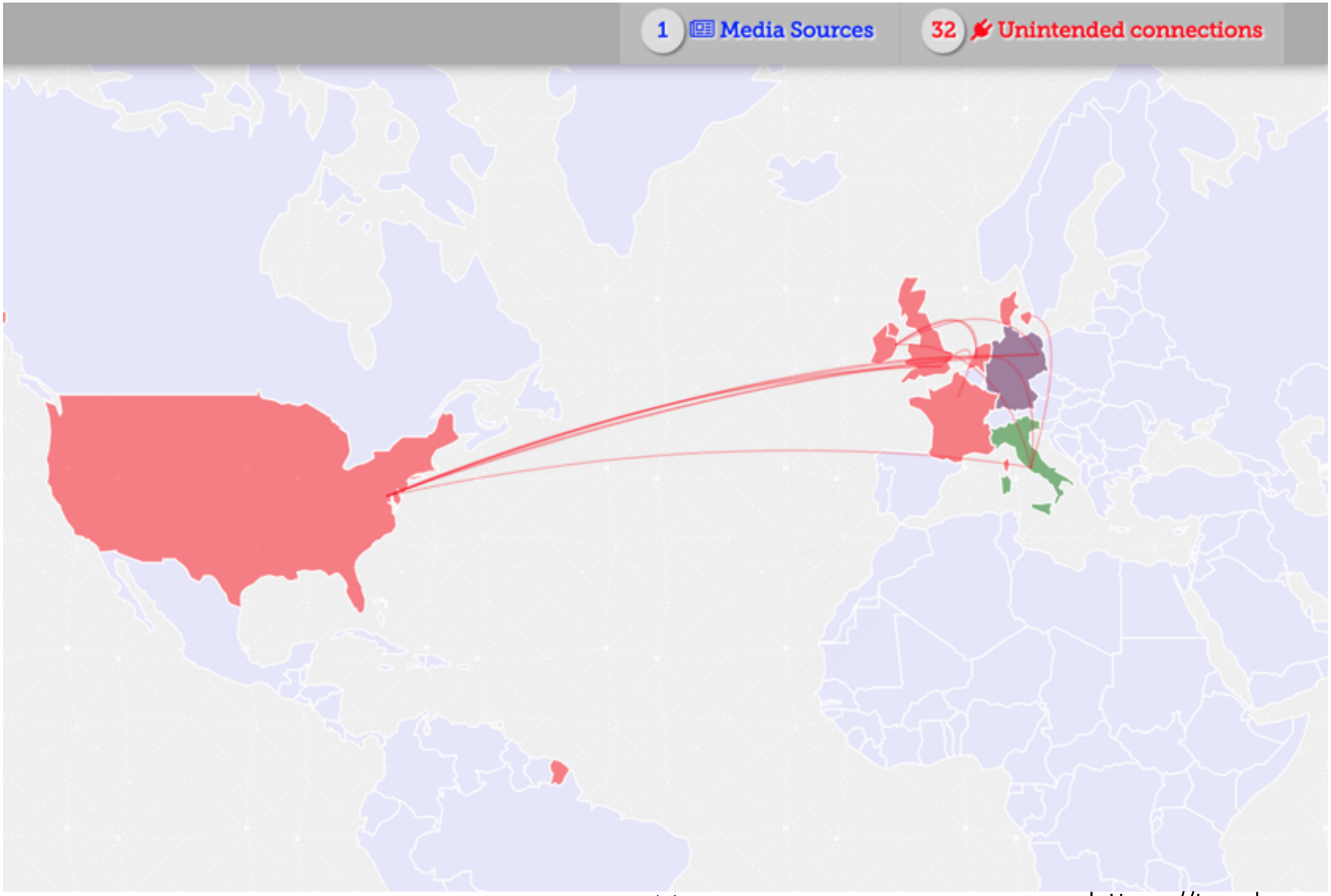
corriere.it

When you visit this site, the following sites are informed:

- google.it
- gstatic.com
- googleusercontent.com
- ~~apis.google.com~~
- ogs.google.com
- clients5.google.com
- www.google.com
- notifications.google.com
- play.google.com
- ~~google-analytics.com~~
- fonts.googleapis.com
- tiqcdn.com
- clients6.google.com
- ~~facebook.com~~
- ~~facebook.net~~
- ~~googleadservices.com~~
- ~~twitter.com~~
- ~~googletagservices.com~~
- ~~linkedin.com~~
- ~~outbrain.com~~
- akamaized.net
- corriereobjects.it
- azureedge.net
- ~~imrworldwide.com~~
- ~~betrad.com~~
- rcsmetrics.it
- rcs.it
- ~~chartbeat.com~~
- imasdk.googleapis.com
- akamaihd.net
- readspeaker.com
- lp4.io
- opendns.com
- ~~tradedoubler.com~~
- admantx.com
- neodatagroup.com

Show list view

CORRIERE.IT



https://trackography.org

CORRIERE.IT

COMPANIES TRACKING YOU

Through the media websites you have selected, the following companies can have access to your data (such as your IP address and browsing habits): Click on the name of a company to learn more about it. click to see the legend

corriere.it

		National Laws	Profiling	Data Retention	Third Parties	Supports DNT
Facebook	🇺🇸	✔	?	✔	✖	
New Relic	🇺🇸	✔	?	✔	✖	
Nielsen						
Twitter	🇺🇸	✔	37d	✔	✔	
Google	🇺🇸	✔	?	✔	✖	
comScore	🇺🇸	✔	?	✖	✖	
Adform						
WPP						
Visual Revenue	🇺🇸	✔	?	✔	✖	
Automattic						

https://trackography.org

RIFLESSIONE

- Tutti contattano Google
- 2 su 3 Facebook
- Perchè?

RIFLESSIONE

“If you are not paying for it, you are not the customer; your are the **product** being sold”

http://www.metafilter.com/user/15556

RIFLESSIONE

https://motherboard.vice.com/en_us/article/539qzk/looking-up-symptoms-online-these-companies-are-collecting-your-data

RIFLESSIONE

Google	Facebook	Nielsen	Twitter	comScore	WPP	Webtrekk	Fox One Stop Media
92%	56%	42%	34%	26%	23%	17%	15%

https://trackography.org/rich.html

ISP

"**I**nternet **S**ervice **P**roviders"

VERIZON

1. Device sends an HTTP request.

2. Verizon injects an HTTP header ("X-UIDH"). It's a temporary ID, hashed or HMACed with a key.

3. Destination website (or third party) receives HTTP request with injected header.

4. Website directs request to advertising exchange.

5. Advertisers on the exchange can issue a paid API call to Verizon.

6. Verizon maps the header to a temporary ID, and returns the ID and/or advertising segments.

METADATA

- I metadati sono dati
- Telefonia:
  - Chi hai chiamato, quando hai chiamato, per quanto, da dove, con che cellulare o apparecchio
- Documento:
  - Size, Autore, Pagine, Font, Numero di parole, di righe, etc

METADATA

ELECTRONIC FRONTIER FOUNDATION eff.org Rocket Matter Webinar June 26, 2014

Why Metadata Matters

- You rang a phone sex service at 2:24 am and spoke for 18 minutes..
- You called the suicide prevention hotline from the Golden Gate Bridge.
- You spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour.
- Felten declaration in ACLU v. Clapper

METADATA

www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

NSA General Counsel Stewart Baker has said, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct," and raised him one, asserting, "We kill people based on metadata."

Governi

“Governi”

XKEYSCORE

What is XKEYSCORE?

1. DNI Exploitation System/Analytic Framework

2. Performs strong (e.g. email) and soft (content) selection

3. Provides real-time target activity (tipping)

4. "Rolling Buffer" of ~3 days of ALL unfiltered data seen by XKEYSCORE:
   - Stores full-take data at the collection site – indexed by meta-data
   - Provides a series of viewers for common data types

1. Federated Query system – one query scans all sites
   - Performing full-take allows analysts to find targets that were previously unknown by mining the meta-data

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE

- Sorgenti:
  - F6 – joint operation of the CIA and NSA that carries out clandestine operations including espionage on foreign diplomats and leaders
  - FORNSAT – which stands for "foreign satellite collection", and refers to intercepts from satellites
  - SSO (Special Source Operations) – a division of the NSA that cooperates with telecommunication providers
  - Overhead – intelligence derived from American spy planes, drones and satellites
  - Tailored Access Operations – a division of the NSA that deals with hacking and cyberwarfare
  - FISA – all types of surveillance approved by the Foreign Intelligence Surveillance Court
  - Third party – foreign partners of the NSA such as the (signals) intelligence agencies of Belgium, Denmark, France, Germany, **Italy**, Japan, the Netherlands, Norway, Sweden, etc.

https://en.wikipedia.org/wiki/XKeyscore

XKEYSCORE

Plug-ins

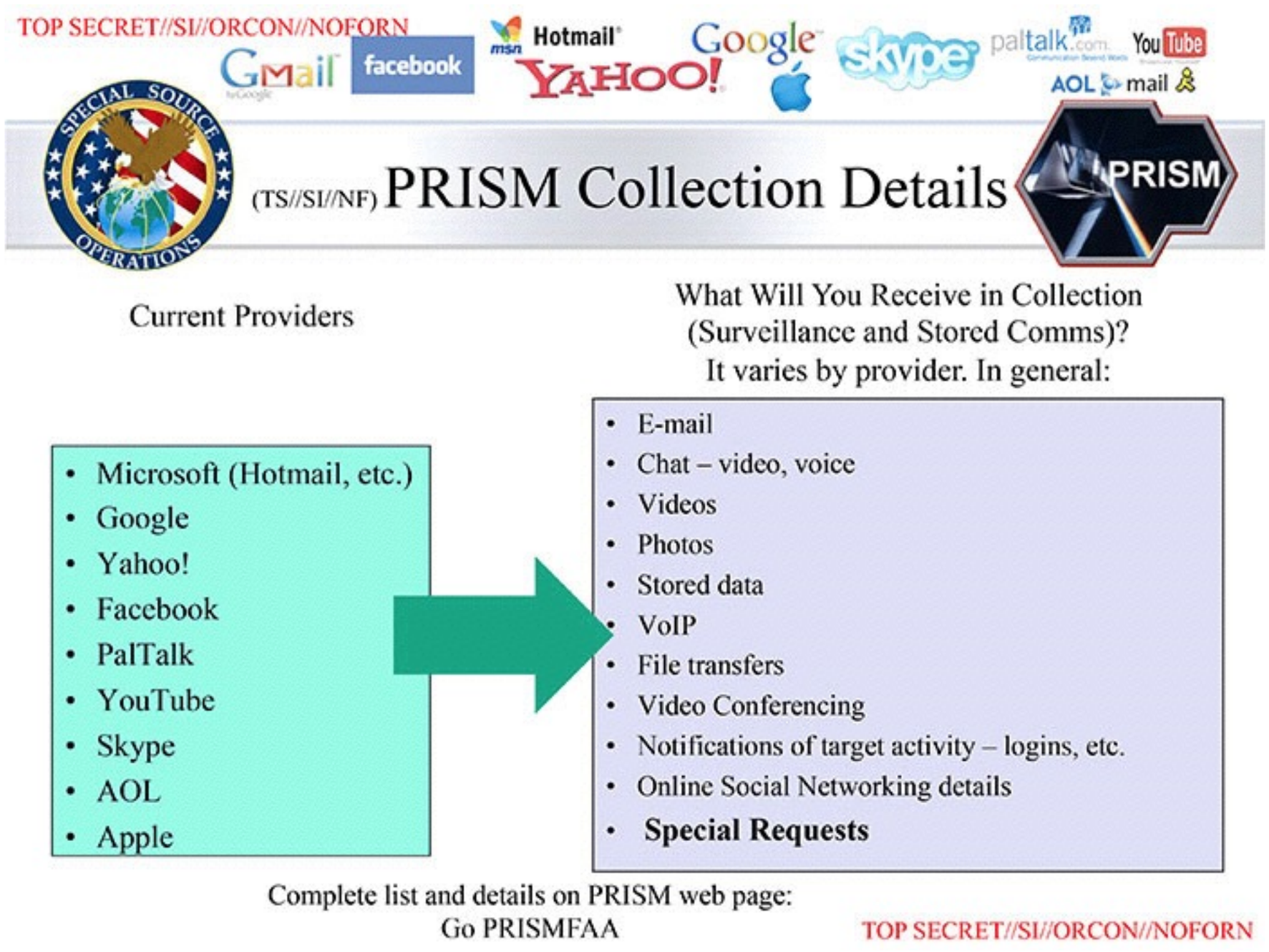
Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

XKEYSCORE

```
// START_DEFINITION
/*
The fingerprint identifies sessions visiting the Tor Project website from
non-fvey countries.
*/
fingerprint('anonymizer/tor/torpoject_visit')=http_host('www.torproject.org')
and not(xff_cc('US' OR 'GB' OR 'CA' OR 'AU' OR 'NZ'));
// END_DEFINITION
```

```
// START_DEFINITION
/*
This fingerprint identifies users searching for the TAILs (The Amnesic
Incognito Live System) software program, viewing documents relating to TAILs,
or viewing websites that detail TAILs.
*/
fingerprint('ct_mo/TAILS')=
fingerprint('documents/comsec/tails_doc') or web_search($TAILS_terms) or
url($TAILS_websites) or html_title($TAILS_websites);
// END_DEFINITION
```

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
Microsoft (Hotmail, etc.)
Google
Yahoo!
Facebook
PalTalk
YouTube
Skype
AOL
Apple
What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:
E-mail
Chat – video, voice
Videos
Photos
Stored data
VoIP
File transfers
Video Conferencing
Notifications of target activity – logins, etc.
Online Social Networking details
Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

Hardening

“Hardening”

NAVIGAZIONE

- Internet è un luogo problematico:
  - Le comunicazioni spesso non sono cifrate
- Usare servizi che offrono più protezione
- Forzare protezione con dei plugin

NAVIGAZIONE

- Problemi:
  - Cookies
  - WebRTC
  - Flash
  - Javascript
  - Fingerprinting

WebRTC

Demo for: https://github.com/diafygi/webrtc-ips

This demo secretly makes requests to STUN servers that can log your request. These requests do not show up in developer consoles and cannot be blocked by browser plugins (AdBlock, Ghostery, etc.).

Your local IP addresses:

- 192.168.2.152

FINGERPRINTING

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor **Do Not Track**?	✗ no
Does your browser protect from **fingerprinting**?	✗ your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

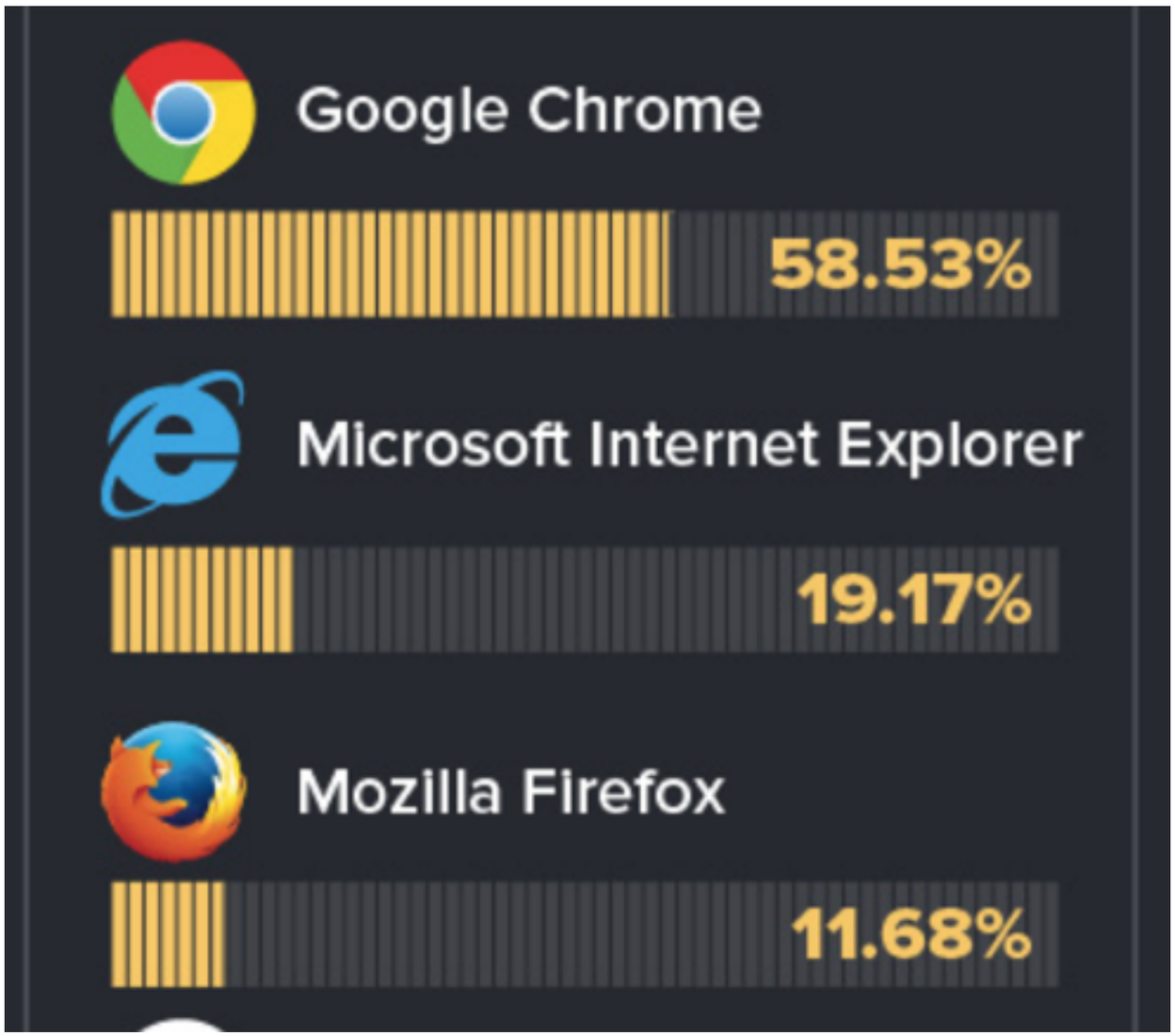
Your browser fingerprint **appears to be unique** among the 740,562 tested so far.

FINGERPRINTING

BROWSERS

- Scelta:
  - Chrome
  - Firefox
  - Edge
  - Safari
  - Opera

POPOLARITA’



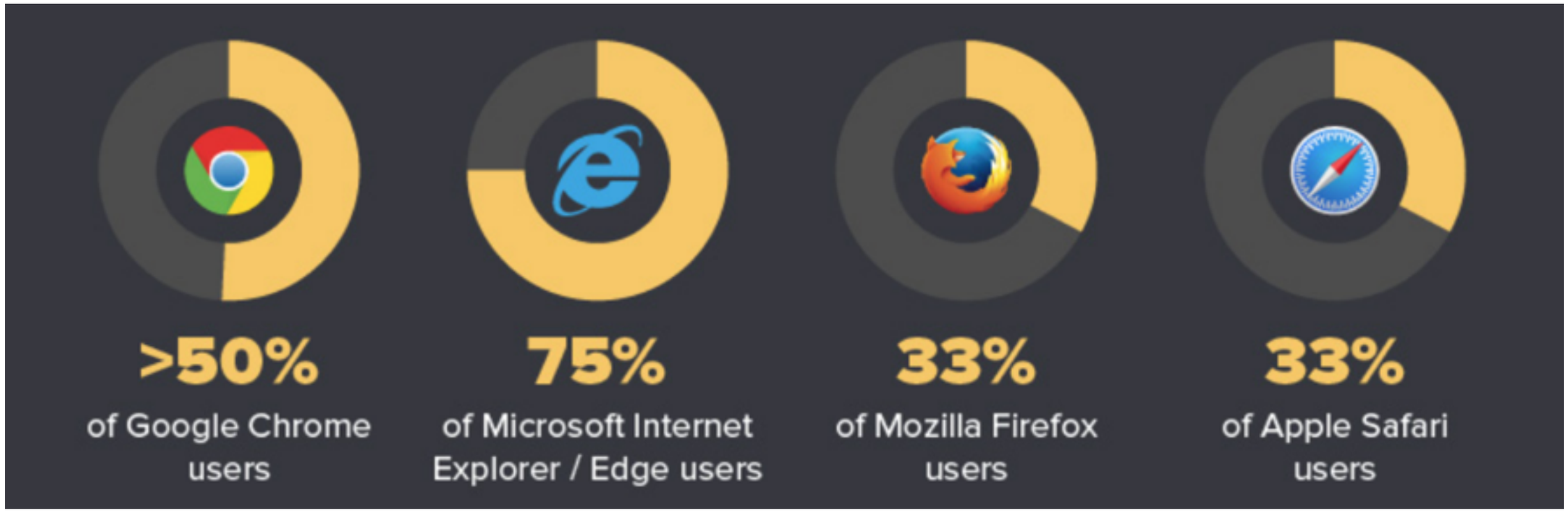
https://www.whoishostingthis.com/blog/2017/07/13/secure-browser/

VULNERABILITA’

	Google Chrome	Microsoft Edge	Mozilla Firefox	Microsoft Internet Explorer	Apple Safari
2016	172	135	133	129	56
2015	187	270	179	231	135
2014	127	Wasn’t available	108	243	72

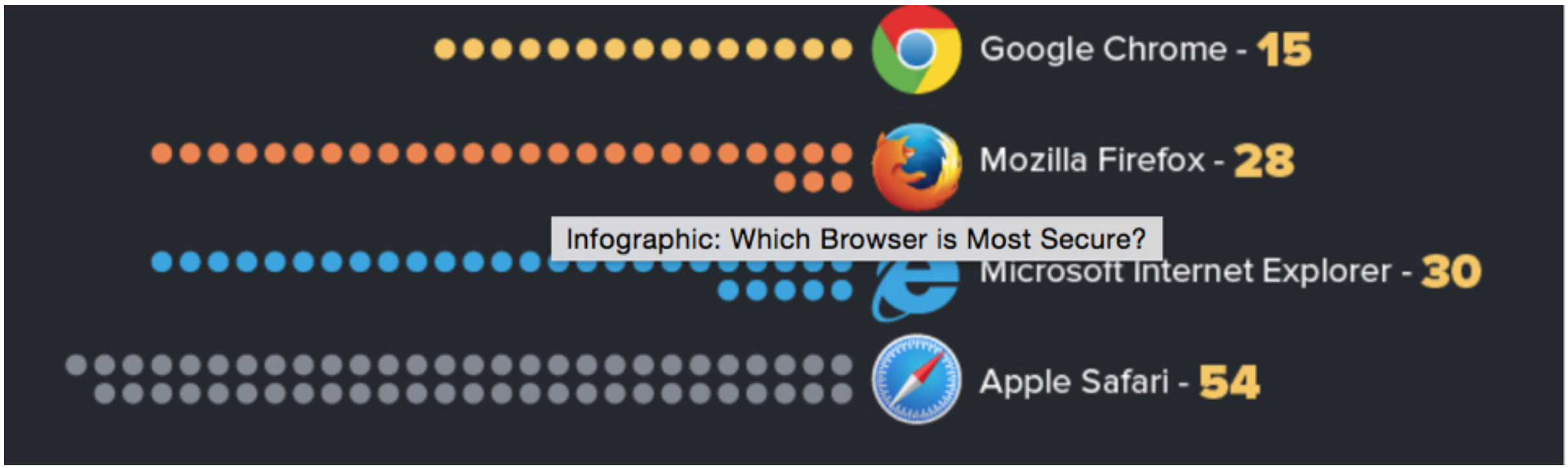
https://www.whoishostingthis.com/blog/2017/07/13/secure-browser/

VECCHIE VERSIONI



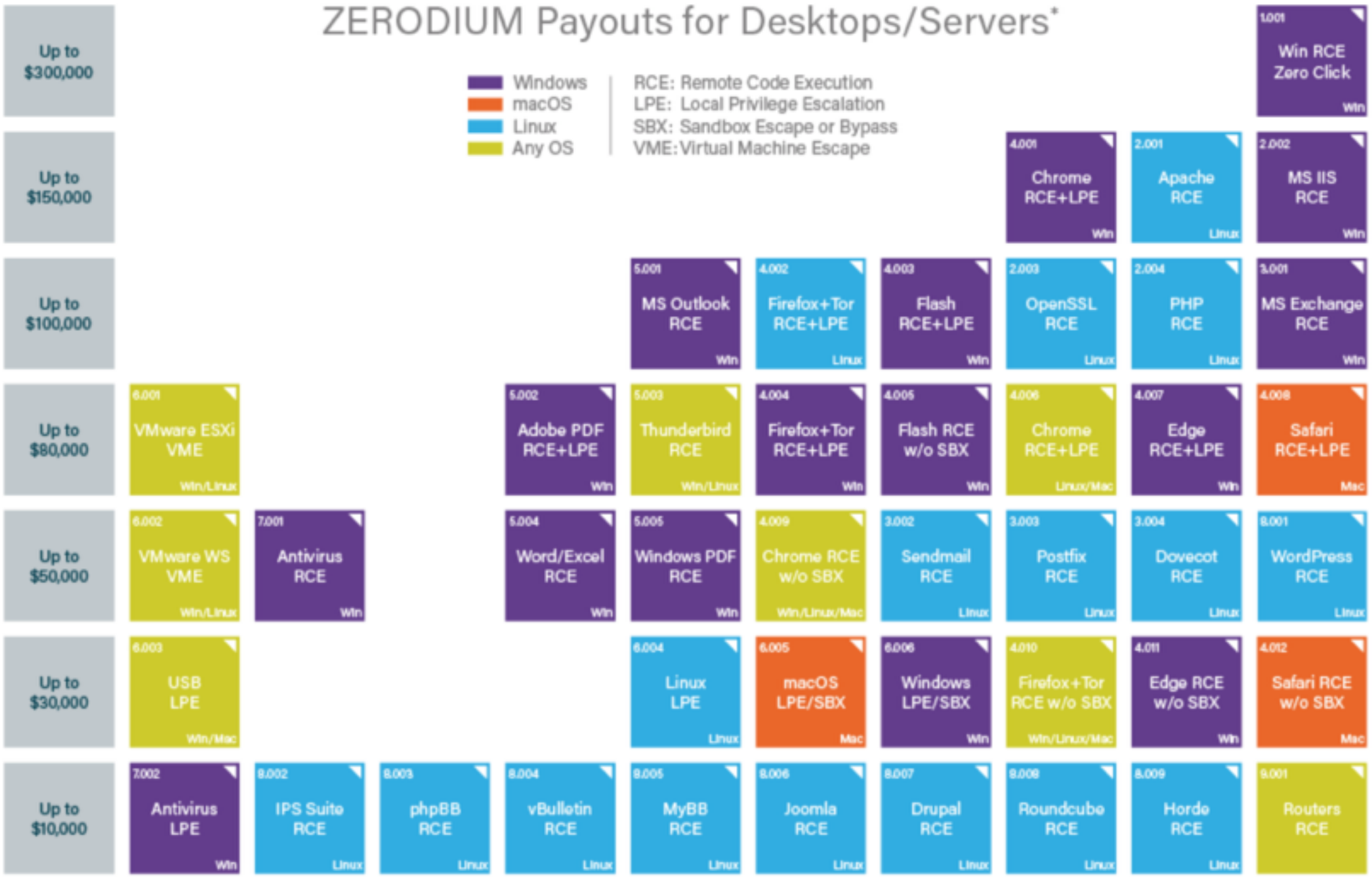
https://www.whoishostingthis.com/blog/2017/07/13/secure-browser/

AGGIORNAMENTI

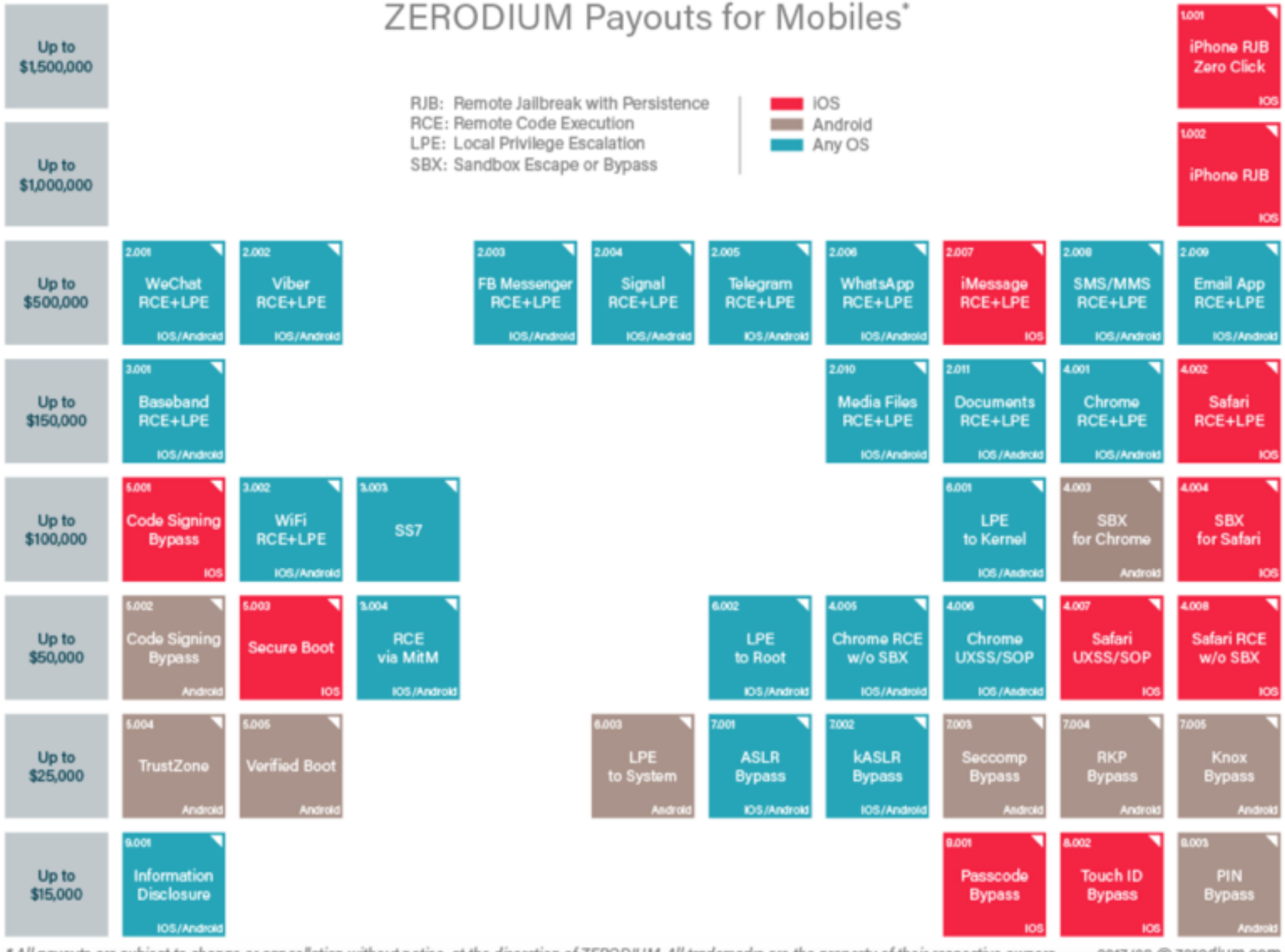


https://www.whoishostingthis.com/blog/2017/07/13/secure-browser/

ATTACCO


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $300,000
1.001 Win RCE Zero Click Win
Up to $150,000
4.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $100,000
5.001 MS Outlook RCE Win
4.002 Firefox+Tor RCE+LPE Linux
4.003 Flash RCE+LPE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
3.001 MS Exchange RCE Win
Up to $80,000
6.001 VMware ESXi VME Win/Linux
5.002 Adobe PDF RCE+LPE Win
5.003 Thunderbird RCE Win/Linux
4.004 Firefox+Tor RCE+LPE Win
4.005 Flash RCE w/o SBX Win
4.006 Chrome RCE+LPE Linux/Mac
4.007 Edge RCE+LPE Win
4.008 Safari RCE+LPE Mac
Up to $50,000
6.002 VMware WS VME Win/Linux
7.001 Antivirus RCE Win
5.004 Word/Excel RCE Win
5.005 Windows PDF RCE Win
4.009 Chrome RCE w/o SBX Win/Linux/Mac
3.002 Sendmail RCE Linux
3.003 Postfix RCE Linux
3.004 Dovecot RCE Linux
8.001 WordPress RCE Linux
Up to $30,000
6.003 USB LPE Win/Mac
6.004 Linux LPE Linux
6.005 macOS LPE/SBX Mac
6.006 Windows LPE/SBX Win
4.010 Firefox+Tor RCE w/o SBX Win/Linux/Mac
4.011 Edge RCE w/o SBX Win
4.012 Safari RCE w/o SBX Mac
Up to $10,000
7.002 Antivirus LPE Win
8.002 IPS Suite RCE Linux
8.003 phpBB RCE Linux
8.004 vBulletin RCE Linux
8.005 MyBB RCE Linux
8.006 Joomla RCE Linux
8.007 Drupal RCE Linux
8.008 Roundcube RCE Linux
8.009 Horde RCE Linux
9.001 Routers RCE
* All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.
2017/08 © zerodium.com

ATTACCO MOBILE



PLUGINS

- HTTPs Everywhere
- Privacy Badger/Disconnect
- Un ad Blocker
- WebRTC Block
- No Flash, No Java
- Javascript? (NoScript)

HARDEN HARD

- Password manager
  - Locale
  - Cloud
- 2 factor authentication (2FA)
- Usare più browsers
- VPN in luoghi pubblici

COMPARTIMENTALIZZAZIONE

- Usare più di un browser:
  - Uno per autenticarsi (Gmail, FB, Amazon)
  - Uno per cose critiche (home banking)
  - Uno per navigare
- Tutti configurati con i plugin elencati
- Usare ‘BlockSite’ per evitare errori e leak

MOTORE DI RICERCA

- DuckDuckoGo
- StartPage
- Ecosia?
- Qwant?

IM

- Whatsapp
  - E2E but… unencrypted backups, dati condivisi con FB
- Telegram
  - Russia, MTproto, metadata leaks
- Signal
  - Private contact discovery in beta (1)

(1) https://signal.org/blog/private-contact-discovery/

2FA

“**2 F**actor **A**uthentication”

PASSWORD

- 1961 MIT
- Primo tentativo di autenticazione
- Problematiche:
  - Password vecchie
  - Password reuse
  - Password banali
    - Top password (123456, password, 12345)
  - Attacchi (Phishing)

PASSWORD MANAGER

- Abbiamo troppi account (personali, lavoro, etc) e non vogliamo usare sempre la stessa password

- Generano, salvano ed inseriscono le tue credenziali

- Generano password sicure (non indovinabili)

- Dobbiamo ricordarci solo la master password

PROBLEMI

- Single point of failure
- Abilitare la 2FA
- Bug nel password manager
- Tutto online?
  - Keepass e’ offline ed e’ opensource!

2FA 101

- Nulla di nuovo: ATM (Carta + Pin)
- Il secondo fattore può avere varie forme:
  - codice via SMS
  - Backup code dati dal servizio
  - Codice a tempo dato da servizi come Google Authenticator, Duosec, etc
  - Hardware (Yubikey, Nitrokey, etc)
- Abilitatela subito su Gmail, FB, Amazon, Twitter, etc

2FA 101

- Nulla di nuovo: ATM (Carta + Pin)
- Il secondo fattore può avere varie forme:
  - codice via SMS
  - Backup code dati dal servizio
  - Codice a tempo dato da servizi come Google Authenticator, Duosec, etc
  - Hardware (Yubikey, Nitrokey, etc)
- Abilitatela subito su Gmail, FB, Amazon, Twitter, etc

OFFLINE

“Offline Security”

FDE

- Full Disk Encryption (FDE)
- Motivazioni:
  - Furto, smarrimento del laptop
  - Lavoro
- Problematiche:
  - Device acceso (memory forensics)
- Soluzioni parziali (TrueCrypt/VeraCrypt)

VT-d

- Evitare DMA attack per:
  - Scrivere in memoria
  - Dumpare la memoria
  - Inception/PCILeech
- Abilitare VT-d ed usare un OS che la usi (Windows 10)

ATTACCO

“ATTACK!”

ATTACCO

- Sistema compromesso —> Game over :(
- Compromissione:
  - Social engineering
  - Phishing
  - Exploitation
  - Malware (e.g., Trojan)

ATTACCO

- Soluzione:
  - Aggiornare sempre il software
  - Riconoscere Phishing
  - Evitare scareware
- Buon senso :-)

LINKS

- https://gist.github.com/atcuno/3425484ac5cce5298932#technology
- https://noscript.net/
- https://www.chromium.org/Home/chromium-security/client-identification-mechanisms
- https://www.eff.org/privacybadger
- http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf
- http://randomwalker.info/publications/browsing-history-deanonymization.pdf
- https://www.theatlantic.com/technology/archive/2017/02/browsing-history-identity/515763/
- https://panopticlick.eff.org/
- https://daserste.ndr.de/panorama/xkeyscorerules100.txt
- https://www.torproject.org/projects/torbrowser/design/

LINKS

- https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#2298d98d5d6e
- https://trackography.org
- https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/
- https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation
- https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts
- https://www.forbes.com/sites/kashmirhill/2014/10/28/find-out-whether-this-privacy-killing-super-cookie-is-on-your-phone/#2a25424ca276
- https://www.pcmag.com/article2/0,2817,2407168,00.asp
- https://disconnect.me/
- https://medium.com/@trackingexposed/background-thoughts-on-https-american-muslims-tracking-exposed-cb0de1e16cd1

RINGRAZIAMENTI

- FreeCircle per l'evento
- Claudio Guarnieri, Claudio Agosti, Carola Frediani e Marco Grassi per le discussioni sui vari argomenti affrontati.

THE END

THANK YOU

email: graziano@eurecom.fr
twitter: @emd3l