Strângerea de Informaţii

Gabriel Avramescu
CEI, CHFI, CEH, ECSA, OSCP, ISO 27001 Lead Auditor, CREST CRT, CCNA SECURITY

Obiective

- Colectarea de informaţii în general
- Amprentarea şi Recunoaşterea

Elemente de bază – Colectare de Informaţii

- Primul pas al fazelor de testare
- Nu poţi ataca ceea ce nu ştii
- Cutie-neagră/Cutie-gri/Cutie-albă („Black-box/Gray-Box/White-box”)
- Adunaţi cât mai multe informaţii despre ţintă
- Poate fi o activitate non-intruzivă: activ vs pasiv

Perspective ale ţintei

- Vizualizare sistem- Tehnologii, dispozitive, sistem de operare
- Vedere logică/funcţională- Dispozitive/scopuri de sistem (prezentare site, ERP, etc.)
- Vedere fizică - Sedii, locaţiile echipamentelor
- Vedere temporală - Zile şi ore lucrătoare
- Vedere socială - Date despre angajaţi
- Vederea ciclului de viaţă - O etapă a procesului de afaceri
- Vederea consecinţei- Dacă un eveniment declanşează un alt eveniment (ce se întâmplă dacă intri în clădirea lor fără autorizaţie– vor suna poliţia? ☺)

Informaţii Iniţiale despre Ţintă

- Numele companiei
- Site-ul companiei
- Locaţie geografică
- Numele unor angajaţi
- Adresele IP

Cum pot obţine informaţii?

- Site-urile companiilor şi angajaţilor
- Căutare pe Internet: www.google.ro şi nu numai, www.shodan.io, www.builtwith.com , www.netcraft.net, Weppalyzer extensie de browser
- Interogarea bazei de date: Whois, DNS
- Reţele sociale: Facebook, Linkedin, Twitter, https://www.pipl.com
- Inginerie socială– mai multe despre asta mai târziu

Paginile web ale companiei

- Vizita pasivă a serverului web
- Informaţii de contact (adrese, persoană de contact, numere de telefon e-mail)
- Outlook/Webmail
    - https://owa.company.ro
    - https://outlook.abc.ro
    - https://webmail.abc.ro
- Reţea virtuală privată
    - http://vpn.abc.ro
    - http://www.abc.ro/vpn

Motoare de căutare?

- Generice (de exemplu, Google, Bing, etc..)
- Motoarele de căutare specifice (de exemplu, cercetare privind reţele sociale)
- Motoarele de căutare care specializează informaţiile despre oameni (de exemplu, Pipl)

Ne asumăm faptul că toate motoarele de căutare sunt aceleaşi

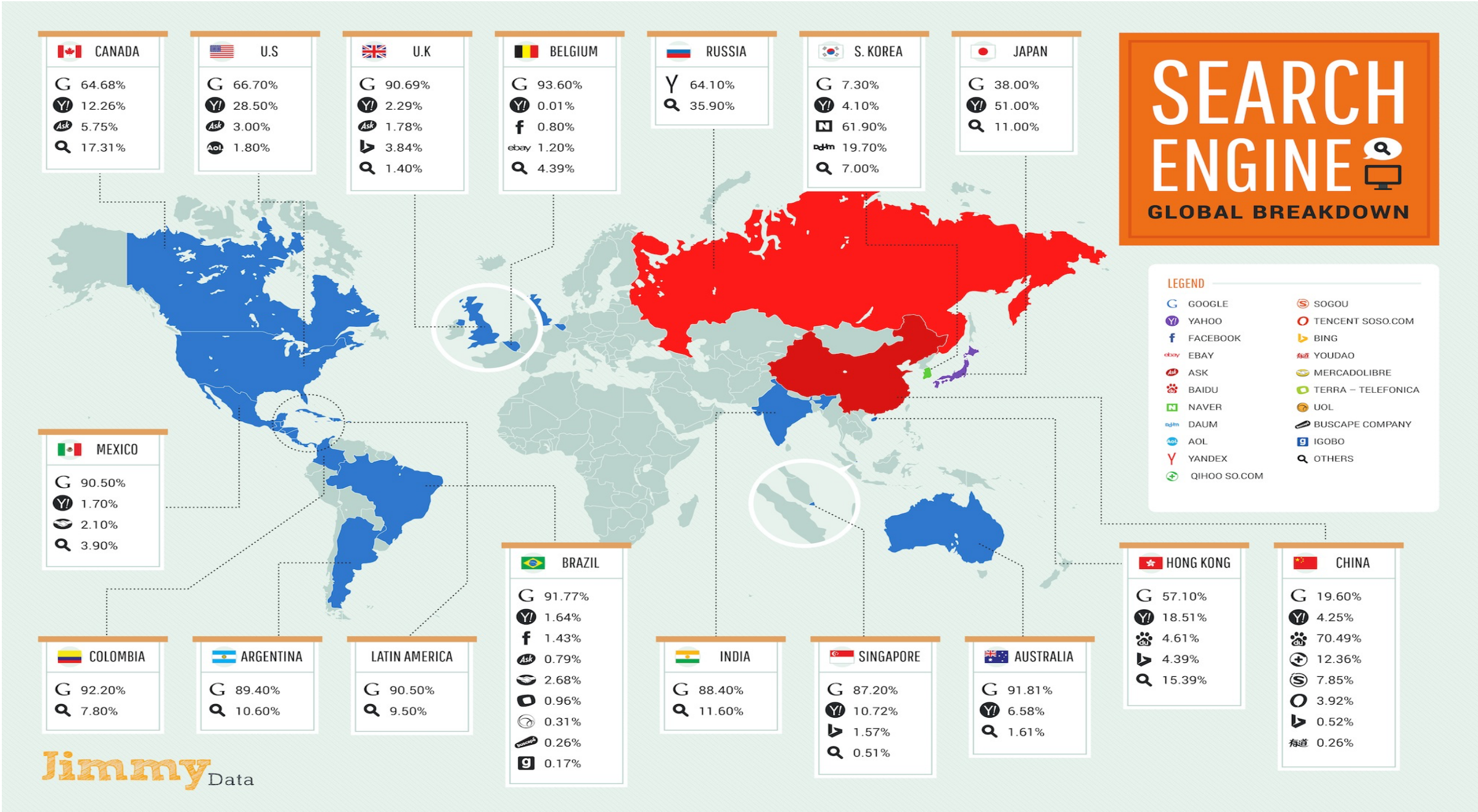
FALS!!

> “Când cercetătorii au rulat **12,570** de interogări diferite prin intermediul motoarelor de căutare de la Yahoo, Google, MSN and Ask Jeeves, ei au constatat că numai 1,1% din rezultate au apărut pe toate cele patru motoare, în timp ce 84,9% din rezultatele de top au fost unice pentru un motor. **Doar 2,6% din rezultate au fost împrăştiate de trei furnizori de căutare, iar 11,4% au fost livrate de două motoare de căutare**” (sursă: “Untangling the Web: The NSA's Guide to Gathering Information on Google”)

Concluzie

- Există o lipsă remarcabilă de suprapunere între bazele de date ale motoarelor de căutare, deci este important să vă antrenaţi să utilizaţi mai mult de un motor de căutare

- Căutați funcții specializate și / sau unice în motoarele de căutare străine


SEARCH ENGINE
GLOBAL BREAKDOWN
CANADA
64.68%
12.26%
5.75%
17.31%
U.S
66.70%
28.50%
3.00%
1.80%
U.K
90.69%
2.29%
1.78%
3.84%
1.40%
BELGIUM
93.60%
0.01%
0.80%
1.20%
4.39%
RUSSIA
64.10%
35.90%
S. KOREA
7.30%
4.10%
61.90%
19.70%
7.00%
JAPAN
38.00%
51.00%
11.00%
LEGEND
GOOGLE
YAHOO
FACEBOOK
EBAY
ASK
BAIDU
NAVER
DAUM
AOL
YANDEX
QIHOO SO.COM
SOGOU
TENCENT SOSO.COM
BING
YOUDAO
MERCADOLIBRE
TERRA – TELEFONICA
UOL
BUSCAPE COMPANY
IGOBO
OTHERS
MEXICO
90.50%
1.70%
2.10%
3.90%
BRAZIL
91.77%
1.64%
1.43%
0.79%
2.68%
0.96%
0.31%
0.26%
0.17%
INDIA
88.40%
11.60%
SINGAPORE
87.20%
10.72%
1.57%
0.51%
AUSTRALIA
91.81%
6.58%
1.61%
HONG KONG
57.10%
18.51%
4.61%
4.39%
15.39%
CHINA
19.60%
4.25%
70.49%
12.36%
7.85%
3.92%
0.52%
0.26%
COLOMBIA
92.20%
7.80%
ARGENTINA
89.40%
10.60%
LATIN AMERICA
90.50%
9.50%
Jimmy Data

Ţineţi minte..

- Google, Yahoo și Bing se adresează utilizatorilor, locațiilor și datelor din SUA și din UE, la fel cum Baidu vizează publicul chinez.
- Operatorii ar trebui să învețe să mobilizeze toate motoarele de căutare și soiurile lor regionale.
- Date concentrate: majoritatea instrumentelor de căutare din afara SUA colectează și stochează date în primul rând sau exclusiv din regiunea sau țara lor. Puteți găsi date despre Yandex, dar nu pe google.com (sau chiar google.ru)
- Selectivitatea limbilor: motoarele de căutare internaționale trebuie să ofere posibilitatea de a căuta în limba (limbile) maternă. În plus, interogările efectuate în seturi de caractere non-latine pot genera mai multe rezultate.

Să încercăm!

- Încercaţi “sala de bal Berlin” pe
  - Yandex.ru: https://yandex.ru/search/?lr=10487&msid=1487939465.0506.20941.30301&text=berlin%20ballroom
  - Baidu.com http://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=1&rsv_idx=1&ch=&tn=baidu&bar=&wd=berlin+ballroom&rn=&oq=&rsv_pq=914c9f4b00017bd9&rsv_t=f0d7WJbLWeMbPJAYfb8AGaNYH7JfsepqTz6hE9csZUJux6kznbXaqXtRMzI&rqlang=cn
  - Google.ro https://www.google.ro/?gws_rd=ssl#q=berlin+ballroom
  - Google.de https://www.google.de/?gws_rd=ssl#q=berlin+ballroom
- Puteți căuta motorul de căutare din România sau din orice țară pe
  - http://www.search-engine-index.co.uk/country/romania.asp

Basic Search Features

This chart is being updated: 4/3/2013

For other search features, see all these pages:

- Book Searching
- Cache Sources
- Search Switching

Search Engine	Boolean	Default	Proximity	Truncation	Fields	Limits	Stop	Sorting
Google	-, OR	and	Phrase	No Auto stem word in phrase	intitle, inurl, link, site, more	Language, filetype, date, domain	Varies	Relevance, site
Bing	AND, OR, NOT, ( ), -, +	and	Phrase	No Auto stem	intitle, inurl, link, site, more	Language, filetype, date, domain	No	Relevance, site
Blekko	-	and	Phrase	No	site	date, slashtags	No	Relevance, date
Procog	-	and	Phrase	No			No	Relevance
Gigablast	AND, OR, AND NOT, ( ), +, -	and	Phrase	No	title, site, ip, more	Domain, type	Varies, + searches	Relevance
Exalead	AND, OR, NOT, ( ),-	and	Phrase, NEAR	Yes and stems	intitle, inurl, link, site	Language, file type, date, domain	Varies, + searches	Relevance

Învăţaţi să căutaţi: Baidu.com

Al treilea cel mai mare motor de căutare din lume (dar cel mai mare în China)

Cu toate acestea, mulţi operatori de căutare obişnuiţi sunt sprijiniţi:

Site:

Domein:

Inurl:

Allinurl:

intitle:

allintitle:

filetype:

Site-uri afiliate: www.baidu.jp, Baidu Thailand, Egypt…

Yandex.ru

- Cel mai popular motor de căutare rus
- Operatori foarte puternici şi nebuni
- Unii operatori cheie de bază:
  - Mima=”html/pdf/doc/ppt/xls/rtf/swf” – caută fişiere de un anumit tip (acestea sunt singurele tipuri de fişiere pe care le puteţi căuta)
- “Arată-mi toate site-urile indexate cu*.ro“: rhost:ro.*
- " Arată-mi toate site-urile indexate care se potrivesc*.edu“: rhost:edu.*
- " Arată-mi toate site-urile indexate care se potrivesc *.edu, de asemenea, conţine termenul ftp”: rhost:edu.* inurl:ftp

Yandex.ru (2)

- lang=”ru/uk/be/en/fr/de” – caută pagini scrise într-o anumită limbă. Aici RU înseamnă rusă, UK – pentru ucraineană, BE – pentru bielorusă, EN- pentru engleză, FR – pentru franceză, DE – pentru germană (acestea sunt singurele limbi pe care le puteți căuta).

- Exemplu: balstică << lang=”uk” – întrebări Yandex pentru “balistică" din surse ucrainene

- Acest lucru este util datorită diferitelor seturi de caractere!

Bing.com

Bing se ocupă de ~ 20% din toate interogările de căutare ... dar există unii operatori unici care o fac să merite

- **linkfromdomain:**
  - Returnează paginile legate de un domeniu.
  - Această comandă poate fi utilizată pentru a explora modelele de vecinătate și trafic (inclusiv traficul rău intenționat).
- **conţine: filetype**
  - Conţine: operatorul returnează paginile care fac legătura cu alte documente și multimedia ca muzică, video, PDF și așa mai departe. În schimb, "filetype:" returnează paginile create în formatul specificat, returnând documentele .pdf, dacă specificați filetype: pdf.
  - De exemplu “SSH password” conţine :xls
- **Ip:**
  - Utilizați-l pentru a găsi alte site-uri pe aceeași adresă IP (distracție încrucișată cu gazdă partajată).
  - Bing Miscellanea: **LOC**: şi **LOCATION**: Ambele returnează pagini web dintr-o anumită țară sau regiune pentru respectivul cuvânt cheie

Bing avansat

Operator avansat de referință

http://msdn.microsoft.com/en-us/library/ff795620

Şi “în sfârşit” Google..

- Rezultatele vor varia în funcție de utilizarea google.com sau google.fr/google.de/google.pt/etc ...
- . și în limba preferată de pe Google pe care ați setat-o ...
- ..... și din țara în care navigați (rezultate diferite pentru o adresă IP chineză, norvegiană și americană).

Google avansat

- ȘI cuvintele trebuie să fie prezente: de ex. Albastru verde (verde și albastru).
- SAU trebuie să existe cel puțin un cuvânt: de ex. verde sau albastru.
- - (Minus) exclude rezultatele din cele care includ cuvântul
- * (Asterisk), caracterul wildcard, include derivații
- "" (Citate) pentru a căuta o frază sau cuvânt așa cum este scris

Google Hacking/Google Dorks

- Sintaxă de căutare Google
- Filetype:doc filetype:pdf filetype:xls
    - Intext:. Intitle:, inurl:
    - Allintext:, allintitle:, allinurl:
    - Site:gov site:mil site:abc.ro
    - Related:www.abc.ro
- http://www.googleguide.com/advanced_operators.html
- Google Hacking Database (GHDB) https://www.exploit-db.com/google-hacking-database/
- Exemplu:
    - SQL conf file
    - Pastebin username and passwords

Google Dorks alte exemple

inurl:phpbb1.txt

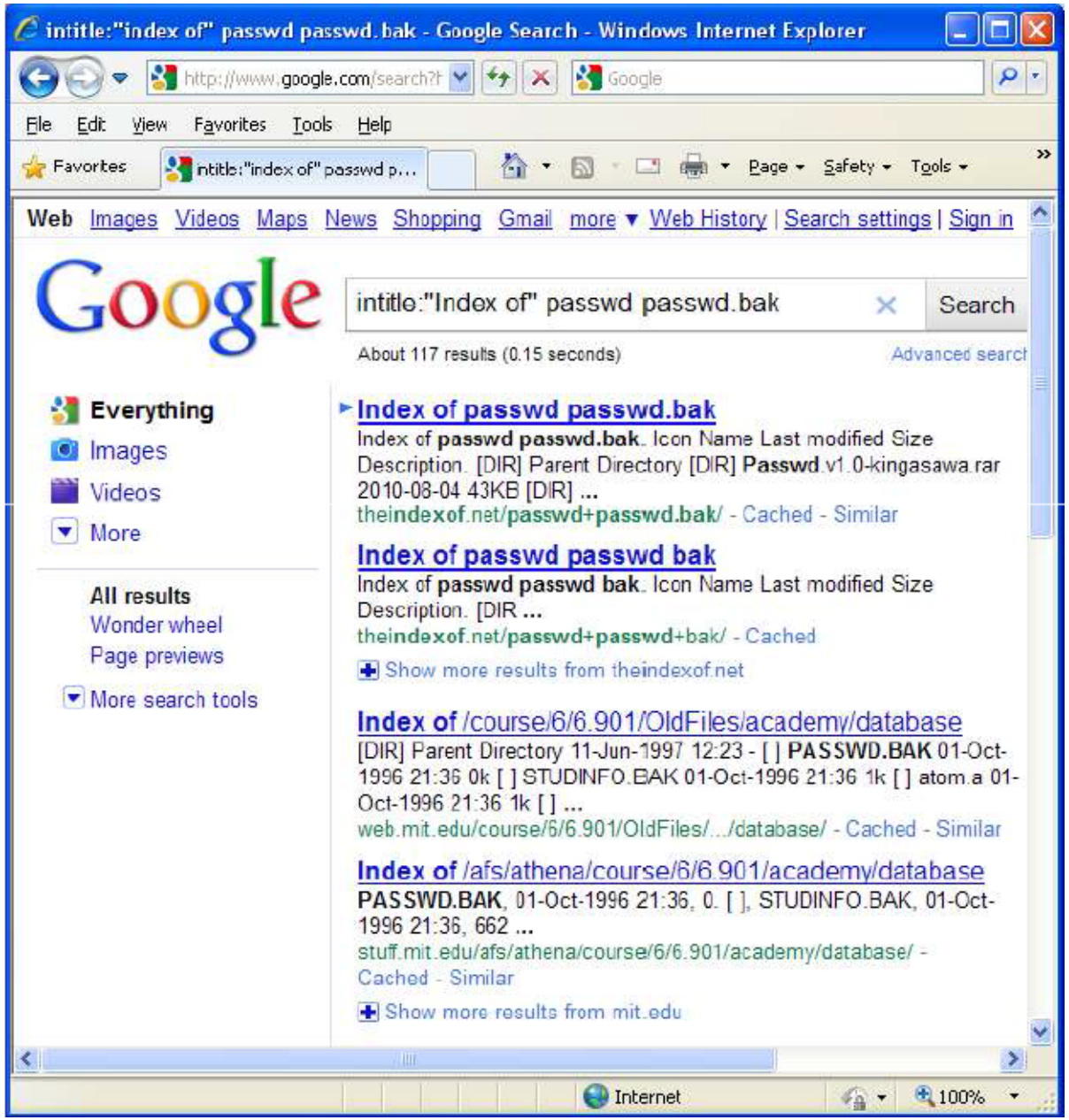
xamppdirpasswd.txt filetype:txt

site:it filetype:pwd

Parolă Instagram filetype:txt

“Parolă=" inurl:web.config -intext:web.config ext:config (Parolele fișierelor web.configuration)

Filetype:xlsx salarii site:.ro


intitle:"index of" passwd passwd.bak - Google Search - Windows Internet Explorer
http://www.google.com/search?h
Google
File Edit View Favorites Tools Help
Favorites
intitle:"index of" passwd p...
Page Safety Tools
Web Images Videos Maps News Shopping Gmail more ▼ Web History | Search settings | Sign in
Google
intitle:"Index of" passwd passwd.bak
Search
About 117 results (0.15 seconds)
Advanced search
Everything
Images
Videos
More
All results
Wonder wheel
Page previews
More search tools
Index of passwd passwd.bak
Index of passwd passwd.bak. Icon Name Last modified Size Description. [DIR] Parent Directory [DIR] Passwd.v1.0-kingasawa.rar 2010-08-04 43KB [DIR] ...
theindexof.net/passwd+passwd.bak/ - Cached - Similar
Index of passwd passwd bak
Index of passwd passwd bak. Icon Name Last modified Size Description. [DIR ...
theindexof.net/passwd+passwd+bak/ - Cached
Show more results from theindexof.net
Index of /course/6/6.901/OldFiles/academy/database
[DIR] Parent Directory 11-Jun-1997 12:23 - [ ] PASSWD.BAK 01-Oct-1996 21:36 0k [ ] STUDINFO.BAK 01-Oct-1996 21:36 1k [ ] atom.a 01-Oct-1996 21:36 1k [ ] ...
web.mit.edu/course/6/6.901/OldFiles/.../database/ - Cached - Similar
Index of /afs/athena/course/6/6.901/academy/database
PASSWD.BAK, 01-Oct-1996 21:36, 0. [ ], STUDINFO.BAK, 01-Oct-1996 21:36, 662 ...
stuff.mit.edu/afs/athena/course/6/6.901/academy/database/ - Cached - Similar
Show more results from mit.edu
Internet
100%

Sursele selectate: Paste Sites

"Paste Sites" sunt populare, ușor de utilizat și (destul de) anonime. Oamenii le folosesc pentru o mare varietate de motive:

Alb: partajarea fișierelor de configurare, haldele de blocare, fragmente de cod, jurnale amuzante IRC, etc ...

Negru: postarea de fișiere scoase din uz, date furate, baze de date cu descărcare de gestiune, "dox", acreditări hacked etc.

Multe anunțuri care vând acreditări furate

Exemple:

http://pastebin.com Vedeţi: https://pastebin.com/1N6Xmxk1

http://tinypaste.com

http://pastie.org

https://haveibeenpwned.com/Passwords

Surse selectate: Wikipedia

Wikipedia este un efort comunitar și toate activitățile (modificări, adăugări, ștergeri etc.) sunt legate de un nume de utilizator sau de o adresă IP.

Uneori o persoană interesată este un utilizator Wikipedia greu

Uneori putem inversa oamenii din interesul de la contribuțiile Wikipedia (foarte bine pentru subiectele de nișă)

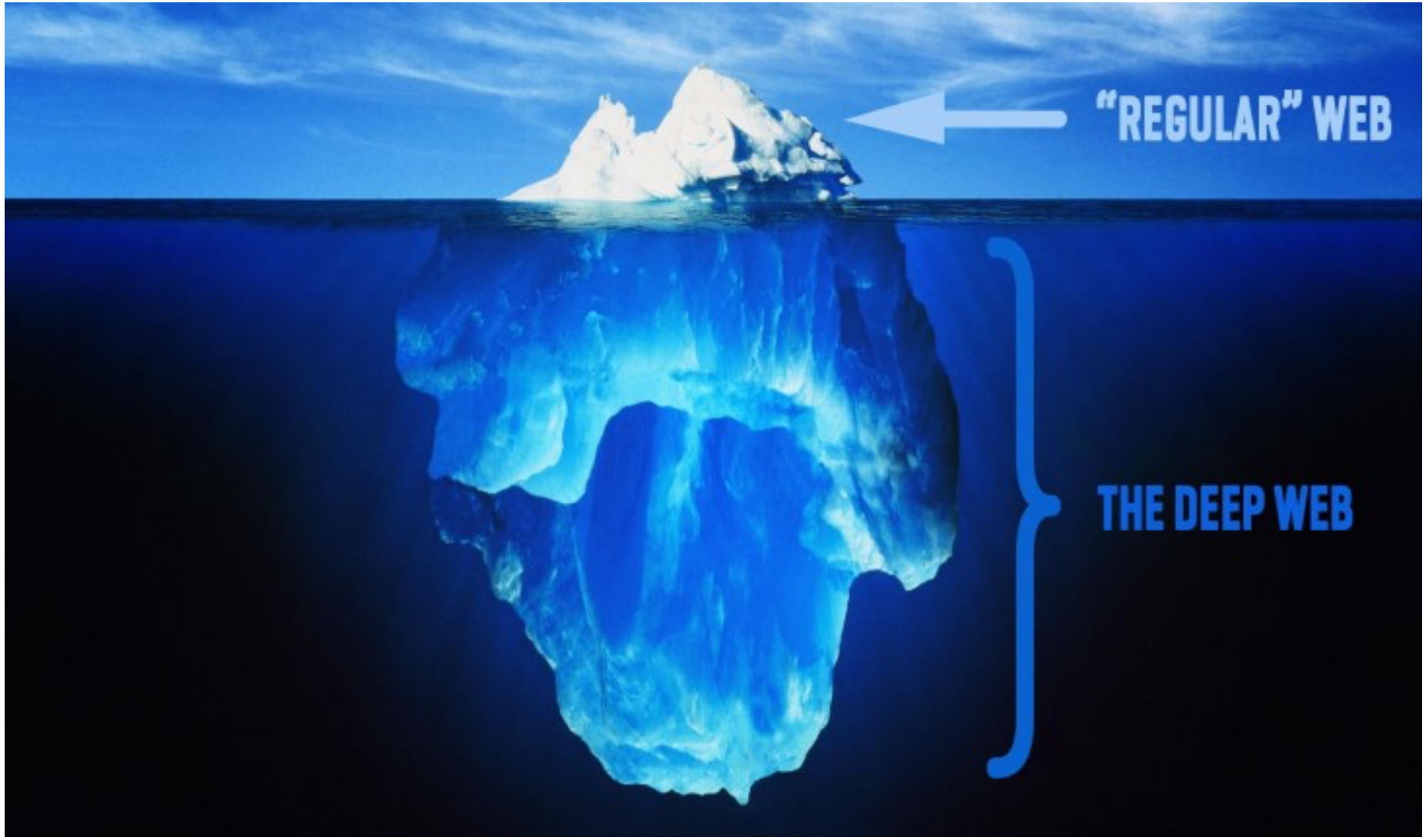
Alerte:

"Alertați-mă când o IP din Congresul SUA editează zh.wikipedia.org"

"Alertează-mă când o IP din Urumqi University editează articole despre situația din Xinjiang."

Mai multe: https://en.wikipedia.org/wiki/Wikipedia:Article_alerts

Deep Web - Și dacă v-aș spune că ~ 90% din conținutul digital nu este indexat?



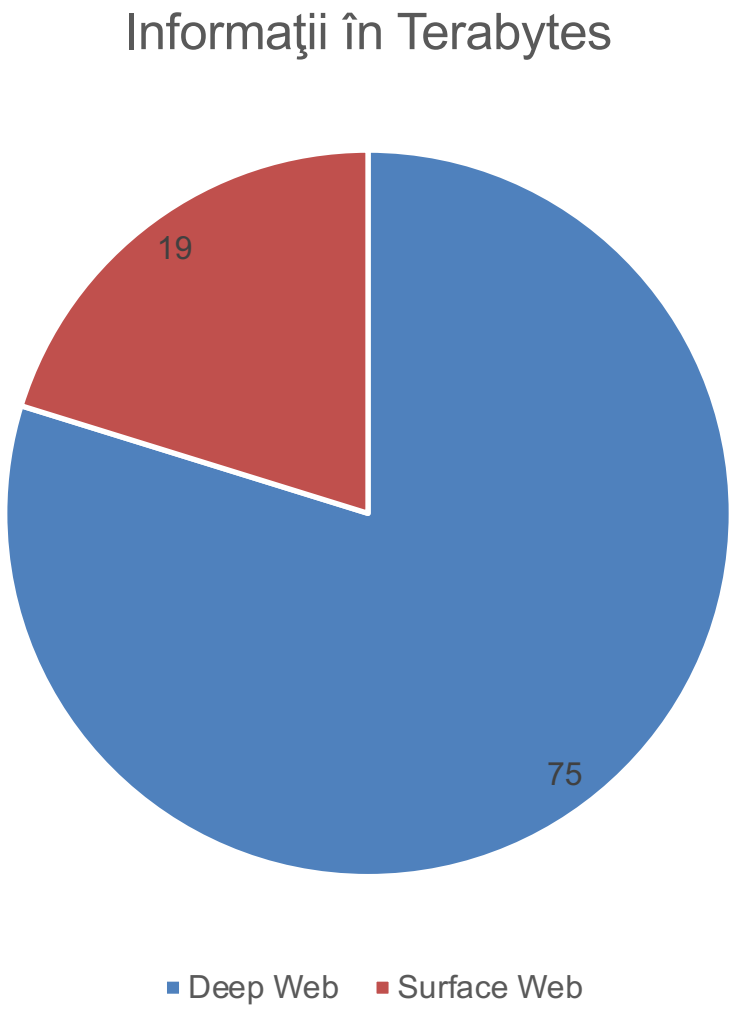
Deep Web

Google, Bing și alte motoare de căutare folosesc spiders pentru a accesa cu crawlere web-ul pentru a indexa conținutul paginilor

Dacă există un blocaj de securitate, un cod corupt, configurații speciale (de exemplu .htaccess), parolă sau pagini dinamice, astfel încât păianjenii să nu poată accesa cu crawlere conținutul, paginile respective nu vor fi indexate

Informațiile publice pe Deep Web sunt în prezent 400-550 de ori mai mari decât pe World Wide Web.

Deep Web



Deep Web şi TOR

Deep Web nu este (numai) TOR, dar ...

Singura modalitate de a ajunge la ele este utilizarea TOR (Routerul de ceapă)

Hidden Wiki http://zqktlwi4fecvo6ri.onion/

Un motor de căutare http://xmh57jrzrnw6insl.onion/

Descărcați browserul TOR: https://www.torproject.org/projects/torbrowser.html.en

Cum să accesați un Deep Web Anonim și să știți activitățile Secretive și Misterioase: https://gbhackers.com/how-to-access-deep-anonymous-web-and-know-its-secretive-and-mysterious-activities/

Mulţumesc!