Nous gagnons notre vie avec ce que nous recevons, mais nous le construisons avec ce que nous donnons

HACKFEST

Slack

discussion avec la communauté

http://bit.ly/HFSlack


HACKFEST.ca
GET INVOLVED
info@hackfest.ca

>_About-FD

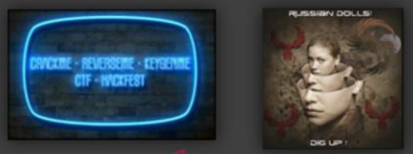
8 ans - Bientôt Canadien

8 ans CGI
- Senior Threat Intelligence Analyst
- Senior Technical Architect

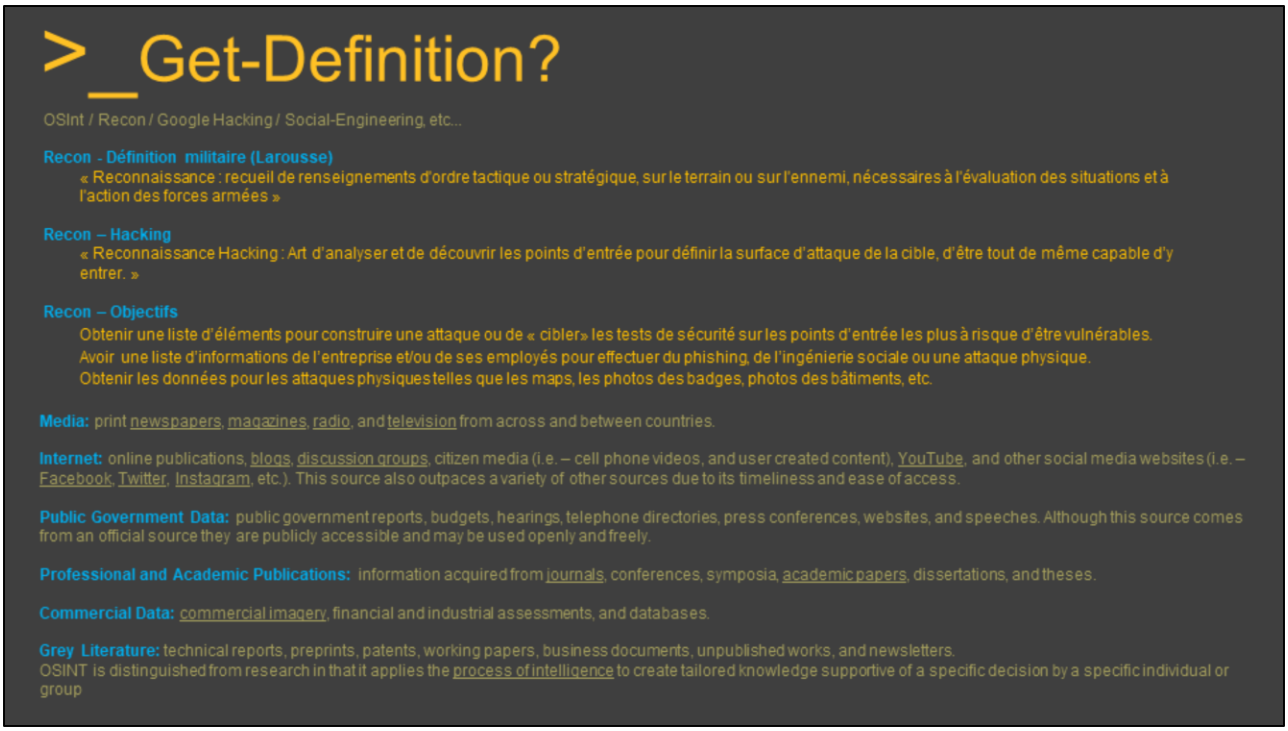
8 ans HF

7 ans PHENIX CORP HF

11 ans



IN2OLAB CGI



Principles:

Open Source Intelligence (OSINT) is the collection and analysis of information that is gathered from public, or open, sources. OSINT is primarily used in national security, law enforcement, and business intelligence functions and is of value to analysts who use non-sensitive intelligence in answering classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines.
OSINT sources can be divided up into six different categories of information flow:[2]

Media:, print newspapers, magazines, radio, and television from across and between countries.

Internet, online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, etc.). This source also outpaces a variety of other sources due to its timeliness and ease of access.

Public Government Data, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.

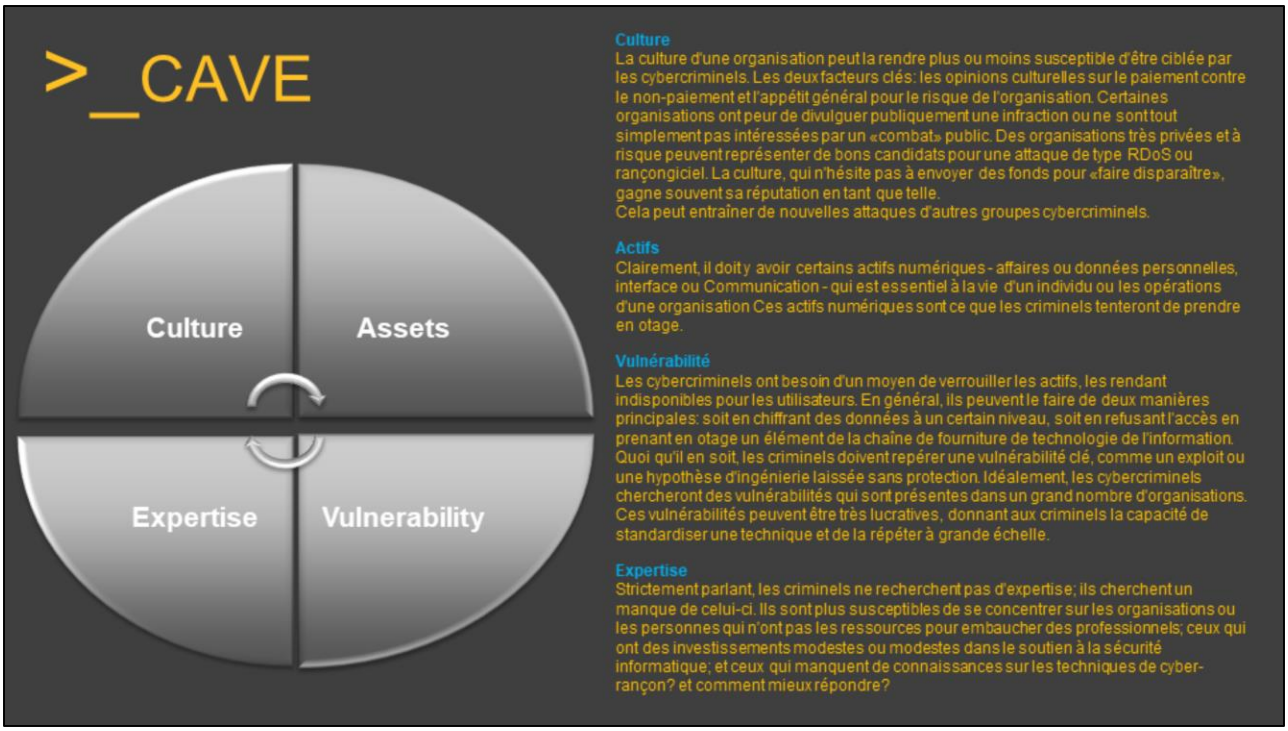
Professional and Academic Publications, information acquired from journals,

conferences, symposia, academic papers, dissertations, and theses.

Commercial Data, commercial imagery, financial and industrial assessments, and databases.

Grey Literature, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.
OSINT is distinguished from research in that it applies the process of intelligence to create tailored knowledge supportive of a specific decision by a specific individual or group.[3]

Intelligence portal
Wikipedia
ICWATCH
Intellipedia
Open Source Center
Private intelligence agency
ROSIDS
Special Libraries Association
Strategic intelligence
NATO Open Source Intelligence Handbook, NATO Open Source Intelligence Reader
MiTAP
DARPA TIDES program
Investigative Data Warehouse
Fusion Center
National Intelligence Open Source Committee
Open data
Co-occurrence networks
Doxing



What do cyber criminals look for when considering ransom targets?
The acronym CAVE highlights the four areas criminals will assess
when choosing which people and companies to target:

Culture
La culture d'une organisation peut la rendre plus ou moins susceptible d'être ciblée par les cybercriminels. Les deux facteurs clés: les opinions culturelles sur le paiement contre le non-paiement et l'appétit général pour le risque de l'organisation. Certaines organisations ont peur de divulguer publiquement une infraction ou ne sont tout simplement pas intéressées par un «combat» public. Des organisations très privées et à risque peuvent représenter de bons candidats pour une attaque de type RDoS ou rançongiciel. La culture, qui n'hésite pas à envoyer des fonds pour «faire disparaître», gagne souvent sa réputation en tant que telle.
Cela peut entraîner de nouvelles attaques d'autres groupes cybercriminels.

Actifs
Clairement, il doit y avoir certains actifs numériques - affaires ou données personnelles, interface ou Communication - qui est essentiel à la vie d'un individu ou les opérations d'une organisation Ces actifs numériques sont ce que les criminels tenteront de prendre en otage.

Vulnérabilité
Les cybercriminels ont besoin d'un moyen de verrouiller les actifs, les rendant

indisponibles pour les utilisateurs. En général, ils peuvent le faire de deux manières principales: soit en chiffrant des données à un certain niveau, soit en refusant l'accès en prenant en otage un élément de la chaîne de fourniture de technologie de l'information. Quoi qu'il en soit, les criminels doivent repérer une vulnérabilité clé, comme un exploit ou une hypothèse d'ingénierie laissée sans protection. Idéalement, les cybercriminels chercheront des vulnérabilités qui sont présentes dans un grand nombre d'organisations. Ces vulnérabilités peuvent être très lucratives, donnant aux criminels la capacité de standardiser une technique et de la répéter à grande échelle.

Expertise
Strictement parlant, les criminels ne recherchent pas d'expertise; ils cherchent un manque de celui-ci.
Ils sont plus susceptibles de se concentrer sur les organisations ou les personnes qui n'ont pas les ressources pour embaucher des professionnels;
ceux qui ont des investissements modestes ou modestes dans le soutien à la sécurité informatique;
et ceux qui manquent de connaissances sur les techniques de cyber-rançon? et comment mieux répondre?

Culture.
An organization’s culture can make it more or less likely to be targeted by cyber criminals.
The two key factors: cultural views on paying vs. not paying and the organization’s overall
appetite for risk. Some organizations are afraid to go public about a breach or simply aren’t
interested in a public “fight.”
Very private, riskaverse organizations may represent strong candidates for an RDoS or ransomware attack.
Similarly, those with a pay-up culture—who are quick to send funds to “make it go away”—
often earn a reputation as such. That can result in new attacks from other cyber-crime groups.

Assets.
Clearly, there must be some digital asset— business or personal data, interface or communication—that is critical to an individual’s life or an organization’s operations. Those digital assets are what the criminals will attempt to hold hostage.

Vulnerability.
Cyber criminals need a way to lock down assets, making them unavailable to users. In general, they can do so in two primary ways: either by encrypting data at some level or by denying access by taking hostage an element of the information technology delivery chain. Either way, criminals need to spot a key vulnerability—such as an exploit or engineering assumption left

unprotected. Ideally, cyber criminals will seek vulnerabilities that are present across a large number of organizations.
Such vulnerabilities can be highly lucrative, giving criminals the ability to standardize on a technique and repeat it on a mass scale.

Expertise.
Strictly speaking, criminals aren't looking for expertise; they're looking for a lack of it. They're more likely to focus on organizations or people lacking the resources to hire professionals; those with few or modest investments in IT security support; and those who lack knowledge of cyber-ransom techniques and how best to respond

==========
How does the CAVE criteria translate into actual targets?

In other words, which industries and people have shown themselves as being vulnerable to these attacks?

Financial Advisors and Financial Services Companies.
This industry evokes the old joke: Why do criminals rob banks? Because that's where the
money is. Cyber criminals are no different; they frequently go to the source of money or to those
that have access to it.

Hospitals and Other Healthcare Organizations.
Hospitals seem to fall firmly at one end of the spectrum or the other. Some are aligned toward
paying up; others are principally resolute and driven NOT to pay a ransom.

Attorneys and Law Firms.
Law frms aren't known for investing large sums in security. In most cases, they aren't adroit at internal controls, either.
Yet frms are highly dependent on their ability to create and share information. What's more, they're notoriously hesitant to
go public with a breach, fearing that their typically high-profle client base would be shaken. Add it all up, and you have an
industry segment that's very likely to be targeted—and to capitulate.

Professional Services Firms.
Much like law frms, accounting, architectural, consulting and other professional services companies may be afraid to go public
with a breach. This unwillingness to engage in public discourse makes these frms more likely to be targeted—and to pay up.

Schools and Educational Services.
Educational institutions typically aren't savvy in information security and cyber-attack mitigation. Even if they have the
expertise, they may lack the fnancial means to wage a protracted war with a cyber-ransom group. In addition, schools often
make decisions by committee—making them more prone to pay up rather than stick to frm, universal principals.

Manufacturing and the IoT.
Concerns about the Internet of Things (IoT) and manufacturing attacks could be the Valhalla of cyber ransom. After all,
who wouldn't pay up to regain access to their car, home thermostat or, even worse, the defbrillator that regulates the
beat of their heart? Though mere conjecture today, the risks of IoT-related cyber ransom—particularly associated with
human health—are far too compelling to rule out.

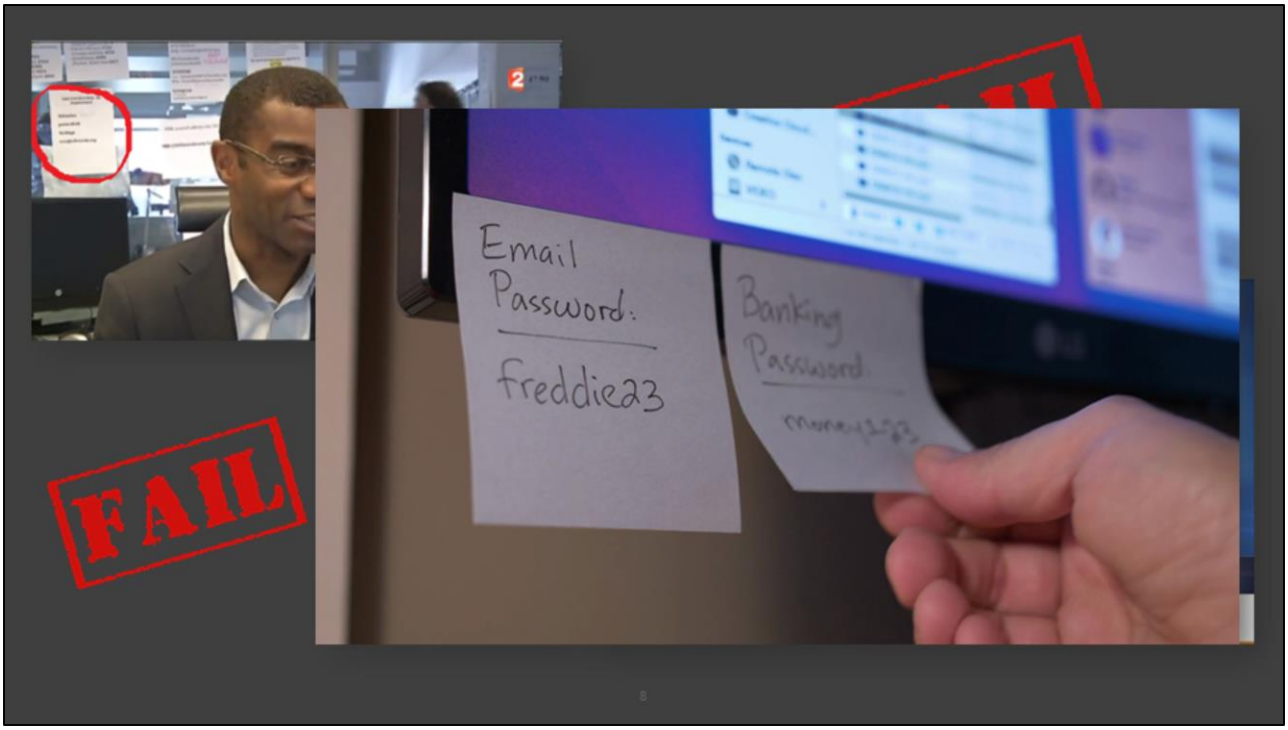
Clashing Ideologies
Any organization that's already under scrutiny by one or more activist groups should assume that those clashes could
eventually spill into criminal activity—including cyber ransom. What follows is a sampling of the types of activities and
affliations that could make an organization vulnerable:

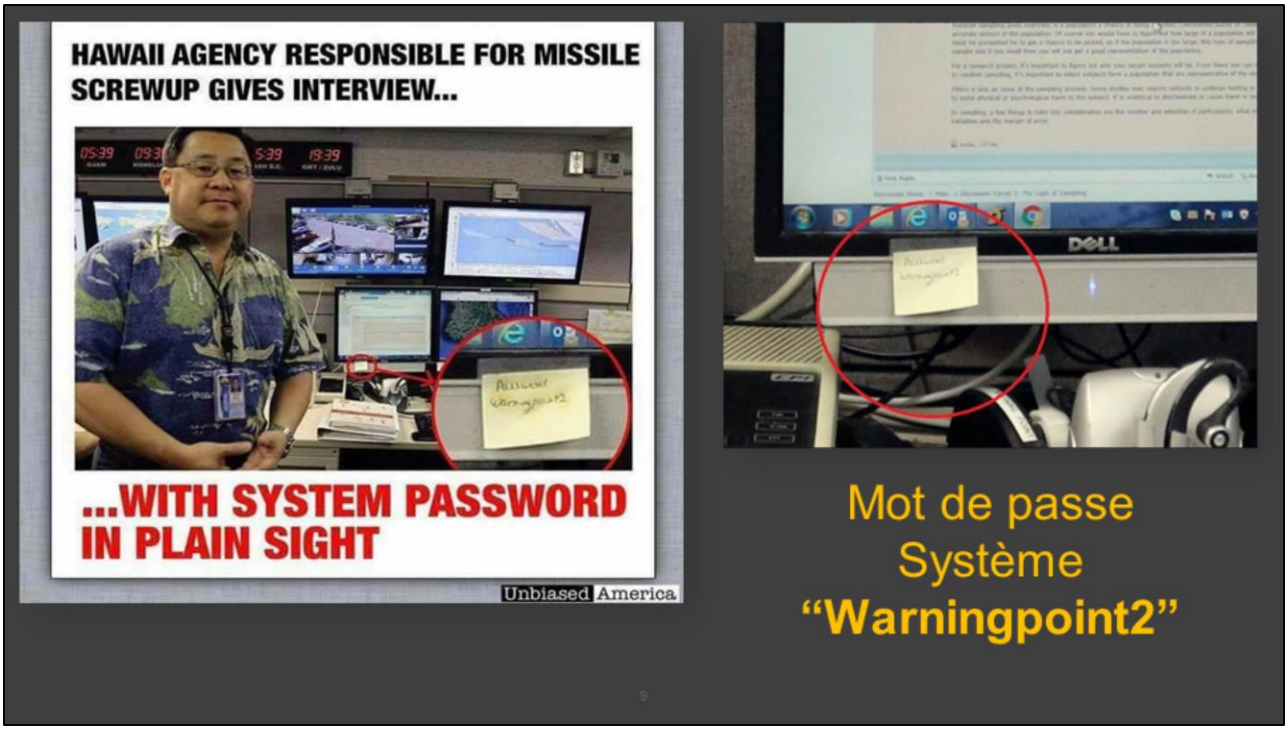
• Animal cruelty, testing or hunting • Genetic or industrial farming • Fossil fuel industry (oil, gas, petrochemical)
• Anti-LGBT • Firearms or defense • Religious affliations
• Federal, state or local law enforcement • Politicians, actors, musicians and other public fgures

Getting Personal
In addition to the industries and organizations cited above, there are some very personal attributes that may dramatically
increase the risk of a cyber-ransom incident. College students are famous for their lack of funds and urgent need for instant access to their "stuff."
Lack of patience and insuffcient knowledge addressing technical attacks make this group ripe for paying up and other forms of capitulation.
Politicians, actors and other public fgures typically have far greater fnancial resources than college students.
However, when under attack, this group typically prefers not to endure the public scrutiny that an aggressive response would require.
Finally, corporate offcers have long been the targets of death threats, as well as physical and verbal attacks.
Cyberransom is the latest way to come after big-company leaders. Unfortunately, a company's resources for fghting an attack

may outlast an individual’s ability to withstand the heat—leading the corporate offcer to give in to the cyber criminals

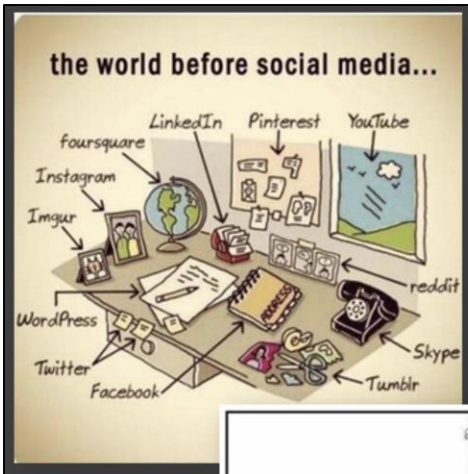

I'LL HELP YOU FIND THE HACKERS
...
GIVE ME YOUR PASSWORD
CHAPPATTE
The New York Times


Email
Password:
Freddie23
Banking
Password
FAIL

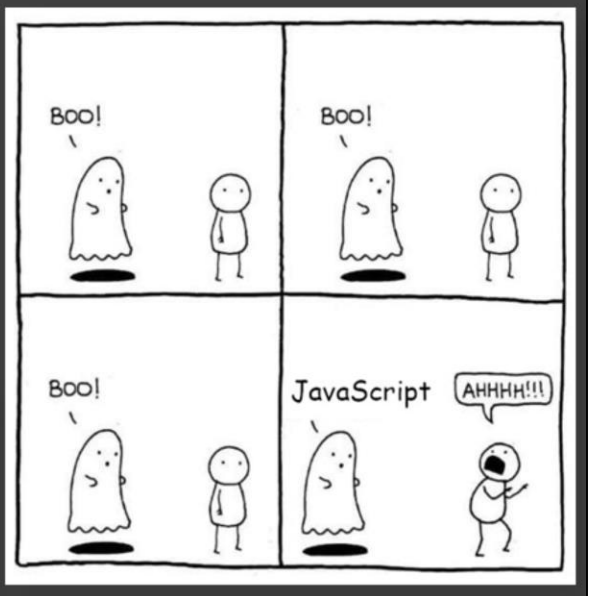


http://www.thegatewaypundit.com/2018/01/hawaiian-emergency-management-officials-hold-interview-post-notes-passwords-computer-screens/

Hawaiian Emergency Management Officials Hold Interview – Have Post-It Notes of Legible Passwords on Their Computer Screens

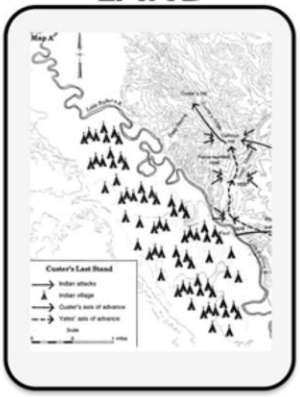


"Are you sure this is how we upload data into the Cloud? "



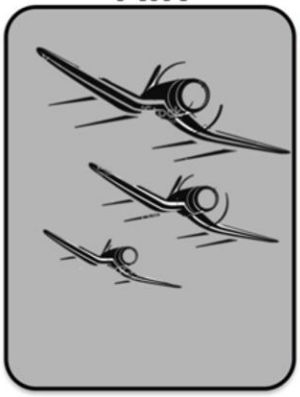
Evolution of War

LAND



SEA

AIR



CLOUD

Destruction of Human Lives + Destruction or Acquisition of Human Valued Assets

Manipulation of Humans + Digital Assets


The Joy of Tech
by Nitrozac & Snaggy
WHAT IT'S LIKE WHEN YOU READ A NEWSPAPER...
WHAT IT'S LIKE WHEN YOU READ NEWS ONLINE...
AD NETWORK GUY
THE NSA
ANOTHER AD NETWORK GUY
AMAZON
ANOTHER NSA GUY
FACEBOOK
pulse
NEWS APPS
MORE AD NETWORK FOLKS!
YAHOO!
TWITTER
GOOGLE GUYS
YOUR ISP
AND DON'T FORGET YOUR SPOUSE CHECKING YOUR HISTORY!
© 2014 Geek Culture
joyoftech.com

ID	Brand	Products	Vulnerabilities	Exploits
1	**Microsoft**	**378**	**3483**	**184**
2	**Apple**	**100**	**2284**	**45**
3	**Oracle**	**241**	**2258**	**23**
4	**IBM**	**566**	**2073**	**32**
5	**CISCO**	**1064**	**1817**	**27**
6	**Linux**	**13**	**1208**	**23**
7	**HP**	**1594**	**1126**	**34**
8	Google	39	1095	16
9	**VMWare**	**56**	**204**	5
10	SAP	84	178	12
11	**McAfee**	**78**	**139**	6
12	**Symantec**	**183**	**92**	12
13	OpenOffice	2	35	1
15	Websense	19	27	0
16	**Alienvault**	**3**	**17**	4
17	Splunk	1	15	2

Rubber Ducky hak5 https://hakshop.com/products/usb-rubber-ducky-deluxe

Statistic / Trending

https://www.webpagefx.com/internet-real-time/

Google Trends - Hot Searches
Tweetping
WikipediaVision (beta)
emojitracker: realtime emoji use on twitter
The Internet in Real Time: Web Usage Stats Per Second
Kaspersky Cyberstat | Real-time cyberworld stats from Kaspersky Lab
Kaspersky Cyberthreat real-time map
Norse Attack Map
THE PIRATE CINEMA - A CINEMATIC COLLAGE GENERATED BY P2P USERS

WHAT HAPPENS IN ONE MINUTE?

NETFLIX

70,000 Hours of Netflix watched

3 million videos watched on Snapchat

Google

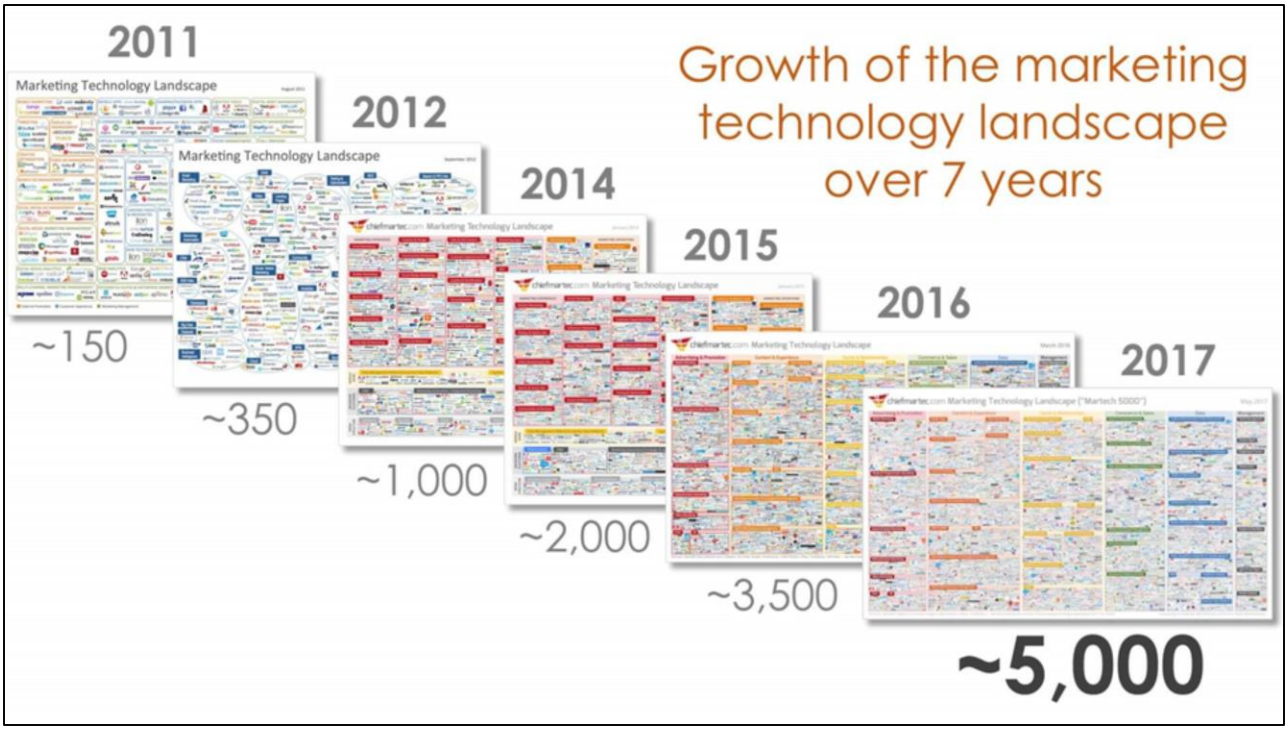
Who is Cardi B?

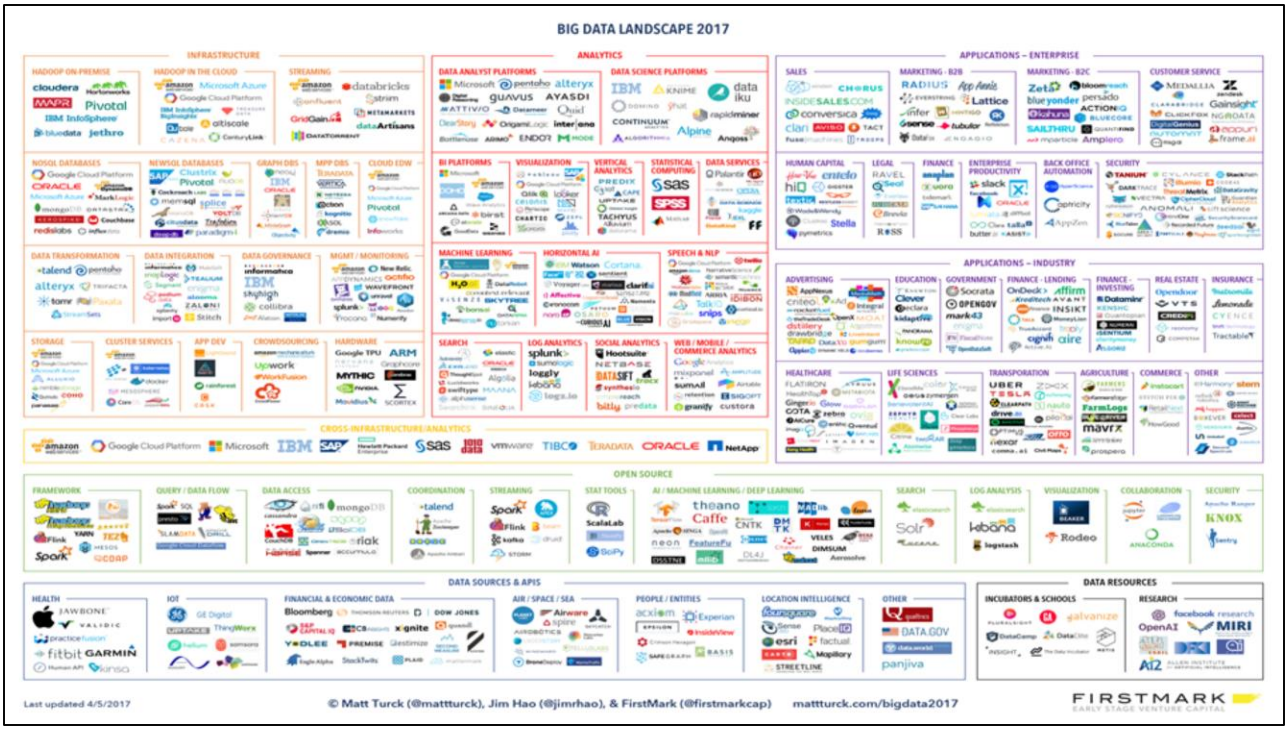
Google Search | I'm Feeling Lucky

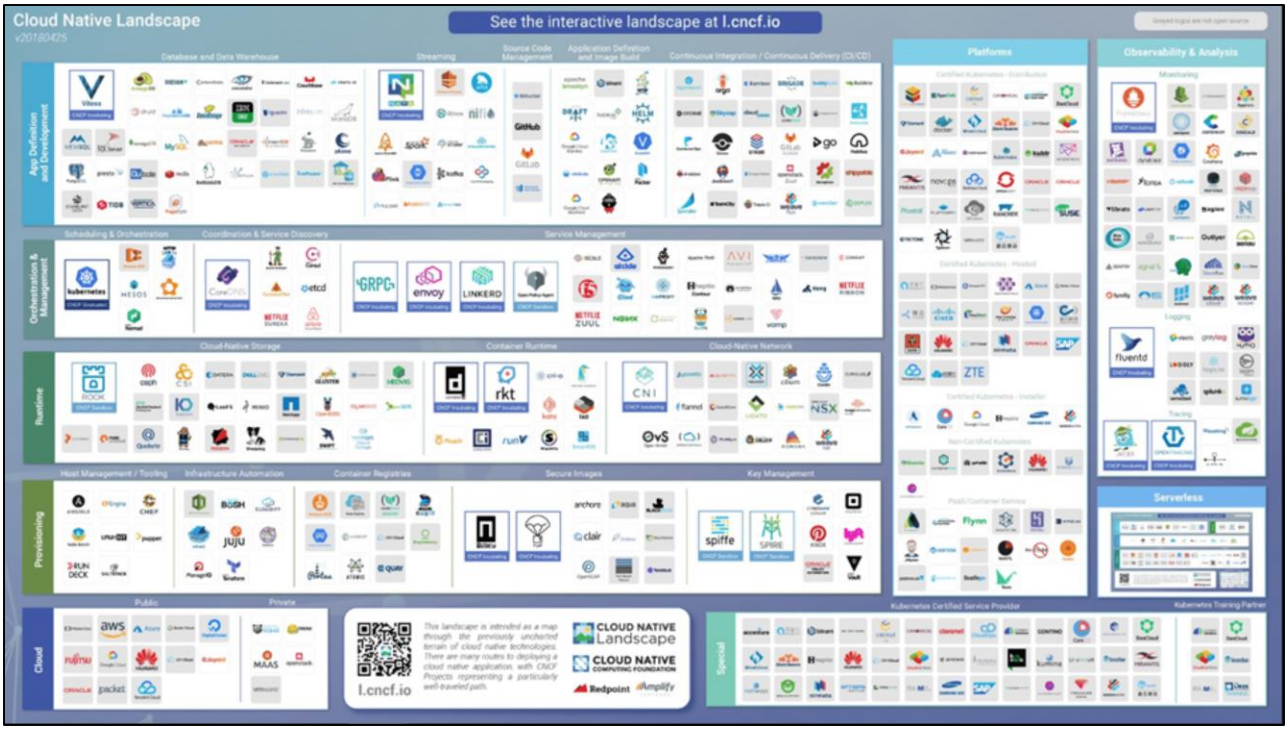
Google is asked 2.4 million questions

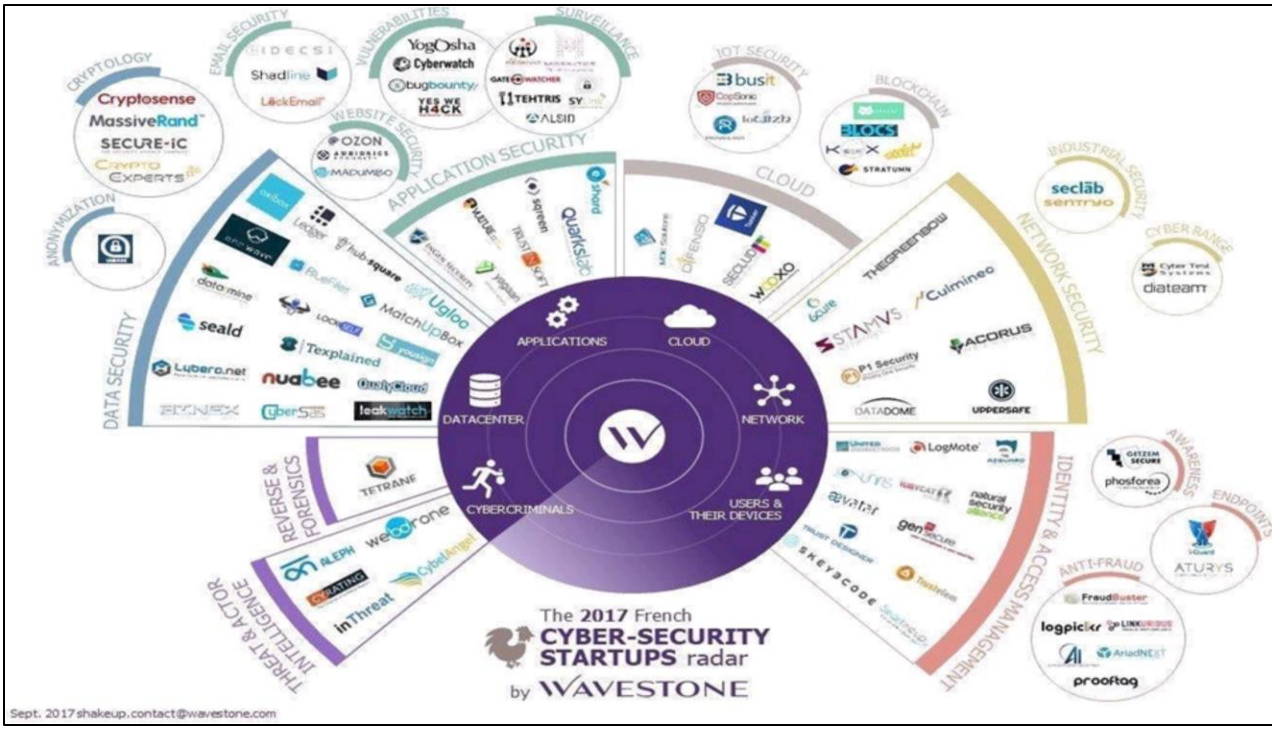
JS

A new JS framework appears


Growth of the marketing technology landscape over 7 years
2011
Marketing Technology Landscape
~150
2012
Marketing Technology Landscape
~350
2014
~1,000
2015
~2,000
2016
~3,500
2017
~5,000


BIG DATA LANDSCAPE 2017
INFRASTRUCTURE
HADOOP ON-PREMISE
HADOOP IN THE CLOUD
STREAMING
NOSQL DATABASES
NEWSQL DATABASES
GRAPH DBS
MPP DBS
CLOUD EDW
DATA TRANSFORMATION
DATA INTEGRATION
DATA GOVERNANCE
MGMT / MONITORING
STORAGE
CLUSTER SERVICES
APP DEV
CROWDSOURCING
HARDWARE
ANALYTICS
DATA ANALYST PLATFORMS
DATA SCIENCE PLATFORMS
BI PLATFORMS
VISUALIZATION
VERTICAL ANALYTICS
STATISTICAL COMPUTING
DATA SERVICES
MACHINE LEARNING
HORIZONTAL AI
SPEECH & NLP
SEARCH
LOG ANALYTICS
SOCIAL ANALYTICS
WEB / MOBILE / COMMERCE ANALYTICS
CROSS-INFRASTRUCTURE/ANALYTICS
APPLICATIONS – ENTERPRISE
SALES
MARKETING - B2B
MARKETING - B2C
CUSTOMER SERVICE
HUMAN CAPITAL
LEGAL
FINANCE
ENTERPRISE PRODUCTIVITY
BACK OFFICE AUTOMATION
SECURITY
APPLICATIONS – INDUSTRY
ADVERTISING
EDUCATION
GOVERNMENT
FINANCE - LENDING
FINANCE - INVESTING
REAL ESTATE
INSURANCE
HEALTHCARE
LIFE SCIENCES
TRANSPORTATION
AGRICULTURE
COMMERCE
OTHER
OPEN SOURCE
FRAMEWORK
QUERY / DATA FLOW
DATA ACCESS
COORDINATION
STREAMING
STAT TOOLS
AI / MACHINE LEARNING / DEEP LEARNING
SEARCH
LOG ANALYSIS
VISUALIZATION
COLLABORATION
SECURITY
DATA SOURCES & APIS
HEALTH
IOT
FINANCIAL & ECONOMIC DATA
AIR / SPACE / SEA
PEOPLE / ENTITIES
LOCATION INTELLIGENCE
OTHER
DATA RESOURCES
INCUBATORS & SCHOOLS
RESEARCH
Last updated 4/5/2017
© Matt Turck (@mattturck), Jim Hao (@jimrhao), & FirstMark (@firstmarkcap)
mattturck.com/bigdata2017
FIRSTMARK
EARLY STAGE VENTURE CAPITAL


Cloud Native Landscape
v20180425
See the interactive landscape at l.cncf.io
App Definition and Development
Database and Data Warehouse
Streaming
Source Code Management
Application Definition and Image Build
Continuous Integration / Continuous Delivery (CI/CD)
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Service Management
Runtime
Cloud-Native Storage
Container Runtime
Cloud-Native Network
Provisioning
Host Management / Tooling
Infrastructure Automation
Container Registries
Secure Images
Key Management
Cloud
Public
Private
l.cncf.io
CLOUD NATIVE Landscape
CLOUD NATIVE COMPUTING FOUNDATION
Redpoint
Amplify
Platforms
Observability & Analysis
Serverless
Special
Kubernetes Certified Service Provider
Kubernetes Training Partner



The 2017 French
CYBER-SECURITY
STARTUPS radar
by WAVESTONE
APPLICATIONS
CLOUD
DATACENTER
NETWORK
CYBERCRIMINALS
USERS & THEIR DEVICES
CRYPTOLOGY
EMAIL SECURITY
VULNERABILITIES
SURVEILLANCE
WEBSITE SECURITY
APPLICATION SECURITY
IOT SECURITY
BLOCKCHAIN
INDUSTRIAL SECURITY
CYBER RANGE
NETWORK SECURITY
ANONYMIZATION
DATA SECURITY
REVERSE & FORENSICS
THREAT & ACTOR INTELLIGENCE
IDENTITY & ACCESS MANAGEMENT
AWARENESS
ENDPOINTS
ANTI-FRAUD
Cryptosense
MassiveRand
SECURE-IC
CRYPTO EXPERTS
IDECSI
Shadline
LockEmail
YogOsha
Cyberwatch
bugbounty
YES WE H4CK
GATEWATCHER
TEHTRIS
ALSID
OZON
MADUMBO
busit
CopSonic
BLOCS
STRATUMN
seclab
sentryo
diateam
Ledger
hub-square
data mine
BlueFiles
Ugloo
MatchUpBox
seald
Texplained
Lybero.net
nuabee
QualyCloud
CyberSaS
leakwatch
shard
Quarkslab
sqreen
TRUST IN SOFT
DIFENSO
SECLUDIT
WOOXO
THEGREENBOW
Culmineo
6cure
STAMVS
ACORUS
P1 Security
DATADOME
UPPERSAFE
TETRANE
wendrone
ALEPH
CybelAngel
CYRATING
inThreat
LogMote
avatar
natural security alliance
TRUST DESIGNER
SKEYECODE
Trustelem
phosforea
ATURYS
FraudBuster
logpickr
LINKURIOUS
AriadNEXT
prooftag
Sept. 2017 shakeup.contact@wavestone.com

James Bond Attack

- Mise en scène d'un scénario d'attaque
  - Recherche sur les média sociaux / maltego pour trouver des employés (limiter les informations accessibles sur internet)
  - Scan de la carte rfid et replay (protéger la carte rfid des regarde malveillant)
  - Installation d'un keylogger

- Différence entre attaques opportunistes, attaques ciblées et d'attaques persistantes avancées
  - Adresser des attaques opportunistes et ciblée mais avancées
  - Exfiltration avec l'ordinateur à côté
  - Risques liés à l'intégration de device USB
    - Update Photocopieurs
    - Gadgets (Vapoteuse, Gadget USB, think geek)
    - Prises, Powerbar, Nano-Cam
  - Infiltration physique

- Le « social engineering »
  - Exploitation du lien de confiance (https://www2.deloitte.com/lu/en/pages/about-deloitte/articles/fake-presidents.html, https://www.spvm.qc.ca/en/Fiches/Details/Business-fraud)
  - Social Network,
  - Données Publiques ...

Le Dark Web - je n'y rentre même pas ☺

HavelbeenPwned.com
Latest Pastes | RSS Feed | Alerts | Domains | API

Hacked-Emails.com
Latest Leaks | RSS Feed | API

Leakedin.com
Keyword Search | RSS feed

Leakedin: People
Email Addresses | Personal Info | Password | Leaked Data | Credit Cards | SSNs |

Leakedin: Websites
Potential Leaks | SQL dumps | Exploits

Quickleak.ir
Pastes by Year

Recon – OSINT
- Maltego
- Sploitego
- theHarvester
- Creepy

`https://www.trustedsec.com/social-engineer-toolkit`

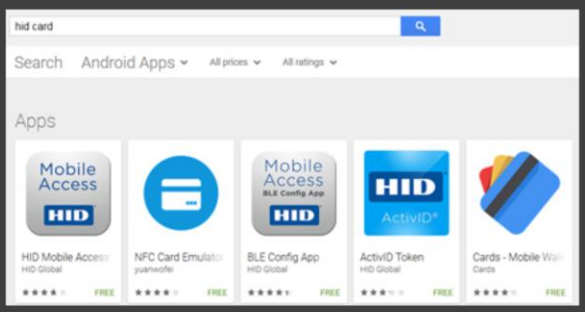
A été développé par David Kennedy à TrustSec et est préinstallé avec Kali Linux
Un excellent outil pour les professionnels de la sécurité pour démontrer la chaîne de confiance comme une vulnérabilité
(c'est-à-dire, comment la personne moyenne ne fera pas attention à l'endroit où elle entre des informations sensibles tant que la source semble légitime)

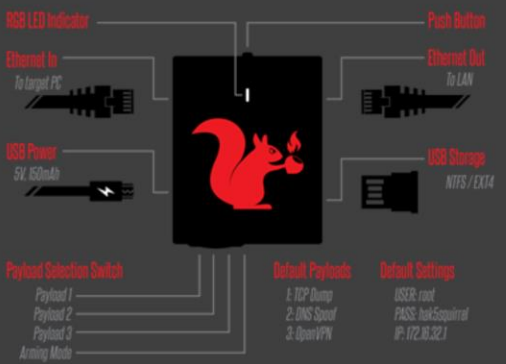
Dans le cadre professionnel, on a affaire à plusieurs « nouveaux » intervenants auxquels nous accordons « naturellement » une certaine confiance :
- Colloque / conférence ;
- Nouveau employé d'un partenaire, du client;
- Fournisseur de service
- Etc.

La source d'un courriel n'est pas un gage d'authenticité !

Quoi faire :
- Ne pas entrer dans les détails sur vos mandats / client en discutant dans les colloques ;
- Faire très attention aux réseaux sans-fils auxquels vous vous connectés ;
- Poser des questions si un nouvel employé s'introduit directement sans être présenté par quelqu'un de confiance ;
- Faire très attention aux demandes formulées par courriel (principe « need to know »)

Obtenir accès physique





Vecteurs d'infections – Appareils sans fils

Plusieurs périphériques sans fils ne protègent aucunement leur communications :

Un téléphone cellulaire infecté par une application ayant accès au Bluetooth peut :

1. Capturer les touches tapées ;
2. Se faire passer pour votre clavier sans fil.

Spoof the MAC Address of the Keyboard

Now that Elliot has the name and MAC address of the cop's keyboard, he will need to spoof it by cloning the cop's keyboard with this info. Kali Linux has a tool designed to spoof Bluetooth devices called *spooftooph*. We can use it to spoof the keyboard with a command similar to this:

kali > spooftooph -i hci0 -a A0:02:DC:11:4F:85 -n Car537

- **-i** designates the device, in this case hci0
- **-a** designates the MAC address we want to spoof
- **-n** designates the name of the device we want to spoof, in this case "Car537"

If we do it right, our Bluetooth device will spoof the MAC address and name of the cop's computer-Bluetooth device.

```
root@kali:~# spooftooph -i hci0 -a 10:AE:60:58:f1:37 -n Car537
Manufacturer:   Cambridge Silicon Radio (10)
Device address: A0:02:DC:11:4F:85
New BD address: 10:AE:60:58:F1:37

Address changed
```

- Pour le quoi faire toujours poser la question sur qu'ils feraient

Vecteurs d'infections – Appareils USB

- C'est un rubber ducky et ça permet de simuler des touches sur un clavier.
- On croit avoir une clef de stockage USB mais c'est un clavier automatique.
- L'avantage c'est que l'on peut transférer des données sur un ordi sans que ça soit vu par l'anti-virus car ce n'est pas un fichier qui est transféré.

IP address troubleshooting / Traceroute skills
Advanced Google search / basic web crawling
Web debugging / Basic packet analysis
HTML for Investigators
Anonymous surfing / Email headers

Custom Search Forms
InfoIP Address SearchWhois Domain SearchDNS & Resource SearchRelated Site SearchSocial SearchPeople Search
Conduct a search. Compare the features and limits of a resource through search forms.

Basic Internet
InfoReferencesIP SearchIP AddressIPv6TracerouteDNS SearchDNSMXCDNs/CloudFlareNetworks/ASNData centersServers/Packets
IP Addresses, networks, DNS, and data centers.

Website Investigations
InfoReferencesWhois SearchWhoisAnalysisRelated Site SearchShared Services/Designe-Commerce/AuctionAds/RevenueArchivesMiscMonitorCopy/Preserve
Domain registration/Whois, related websites, e-commerce, advertising, revenue, backup tools

Social Media Investigations
InfoReferencesOSINT LinksSocial SearchScreen nameForum/BlogFacebookGoogle+TwitterLinkedinInstagramPinterest/TumblrPeriscope/Vine+RedditVK.com/RegionalMore NetworksDating NetworksReal-timeMulti-searchBitly/Short URLsImages/Social
OSINT tools: Facebook, Twitter, Social Networks, Identity verification, and more

Email, Phone, Address, People
InfoPeople SearchEmailPhone U.S.Phone Int'lSkypeAddress PeopleCV/ResumesBusiness
Locate people and reverse engineer email, phone, and physical address info

Search
InfoReferencesSearch AlertsSearch EnginesMeta searchReal-timeRefinedSocialIntl SearchDrive SearchPaid SearchPhoto SearchRSS SearchFTPLink CollectionMisc/Maps
Focus your query through a specialized search engine or search technique

Media: Image, Video, and Document
InfoImageEXiFVideoDocumentHash & Metadata
Search for shared avatars, forum signatures, related websites, and more

Special Focus
InfoEvidenceBitCoinPayment ProcessingParcel TrackingBitTorrent/FilesharingPastebin sitesGithubTORWebmasters and HTMLResourcesCopyright / TrademarkFirefoxGoogle ChromeMisc/Data Mgmt
Special focus areas, resources, and browser add-ons

Apps and Utilities
InfoBrowsers / AnonymityInspect app / PhoneVOIP Phone/SMSEmail/MailFile transferPC maintenancePortable AppsRSS/Social MediaVideo / DigitalWeb AnalysisScrapers/AutomationEvidence
Desktop applications and resources for investigations and PC maintenance

Types de Recon et les objectifs

Recon - DNS
Objectifs: Découvrir une surface d'attaque plus grande. Permet de trouver des systèmes et sites Web souvent mis à jour.

Recon - Web
Objectifs: Découvrir des fichiers cachés et malheureusement « uploadés » par l'équipe de mise en production. Permet de découvrir des données sensibles ou utiles.

Recon – CMS
Objectifs: Déterminer la version du CMS en place et vérifier si des vulnérabilités y sont présentes.

Recon – MetaData
Objectifs: Permet de découvrir des données cachées dans les métadonnées des fichiers publiés publiquement sur Internet.

Recon - SSL/TLS
Objectifs: Déterminer les fonctions de chiffrement en place et leur niveau de sécurité.

Recon - Robots.txt
Mal : https://saaq.gouv.qc.ca/robots.txt
Bien : http://www.canada411.ca/robots.txt

Objectifs: Permet sans grand effort de découvrir des endroits qu'on ne devrait surtout pas analyser… ;) !

Moyen : http://www.cegep-ste-foy.qc.ca/robots.txt

User-Agent: *
Disallow: /typo3/
Allow: /fileadmin/documents/
Disallow: /fileadmin/
Disallow: /uploads/

28

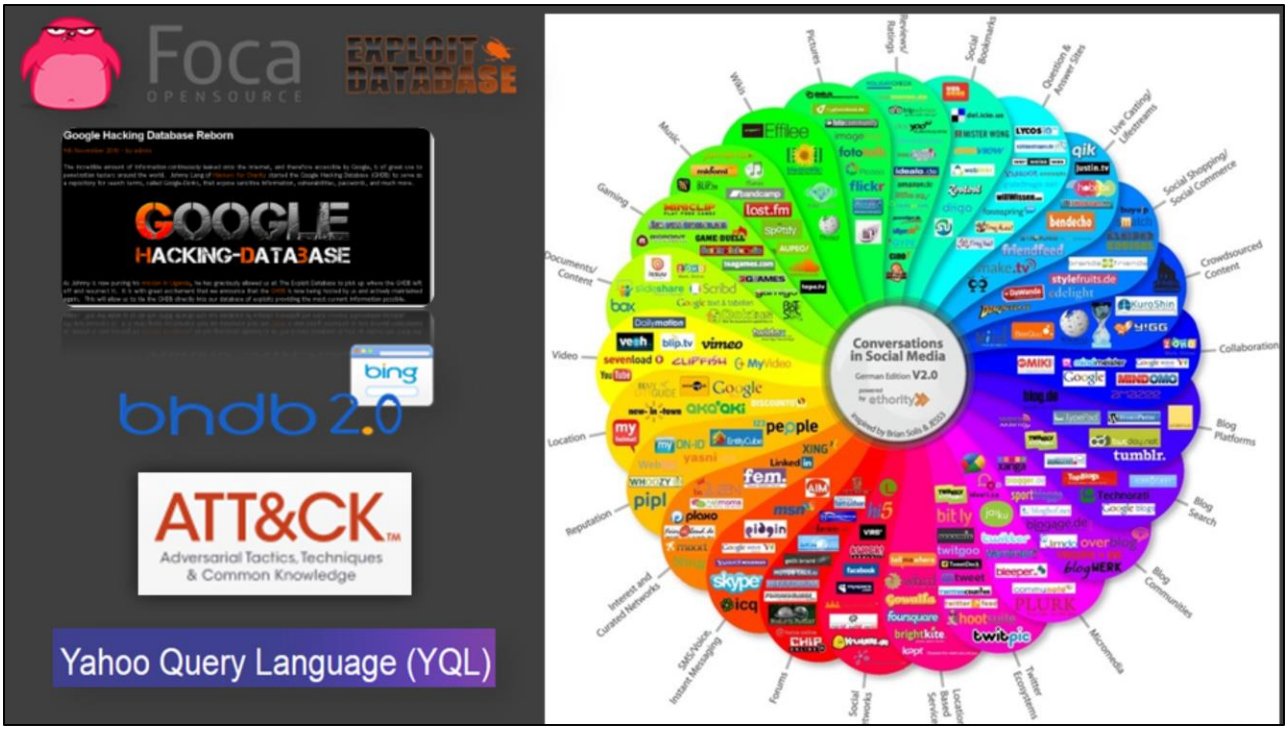
Recon - DNS
Bruteforce les sous-domaines
- Dnsrecon
- Dnsenum

Recon - Web
Bruteforce des fichiers et répertoires
- dirsearch
- BurpSmartBuster
- GoBuster

Recon – MetaData
Metadata
- Foca
- Metagoofil / exiftool

Recon – CMS
Application Web & CMS
- BlindElephant
- WPScan
- Joomscan

Recon - SSL/TLS
- SSLyze
- Qualys : https://www.ssllabs.com/
- SSLScan https://github.com/rbsec/sslscan/



November 9, 2010

The incredible amount of information continuously leaked onto the Internet, and therefore accessible by Google, is of great use to penetration testers around the world.

Johnny Long of Hackers for Charity started the Google Hacking Database (GHDB) to serve as a repository for search terms, called Google-Dorks, that expose sensitive information, vulnerabilities, passwords, and much more.

As Johnny is now pursing his mission in Uganda, he has graciously allowed us at The Exploit Database to pick up where the GHDB left off and resurrect it. It is with great excitement that we announce that the GHDB is now being hosted by us and actively maintained again. This will allow us to tie the GHDB directly into our database of exploits providing the most current information possible.
We will be accepting new submissions through our new forums and email. For more information about sending in GHDB submissions by email, check here. We will be updating the GHDB on a daily basis based on submissions by the community. We have opened forums for both EDB and GHDB conversation. Feel free to sign up and read the rules and guidelines here.
It is our hope that by bringing back the GHDB, we can work together to rekindle the original spirit of exploration of the GHDB community.

Google Dork et « Engine Search Dork»

Operators	Description
site:	Restrict results to only one domain, or server
inurl:/allinurl:	All terms must appear in URL
intitle:/allintitle:	All terms must appear in title
cache:	Display Google's cache of a page
ext:/filetype:	Return files with a given extension/file type
info:	Convenient way to get to other information about a page
link:	Find pages that link to the given page
inanchor:	Page is linked to by someone using the term
-	Inverse search operator (hide results)
~	synonyms
[#]..[#]	Number range
*	Wildcard to put something between something when searching with "quotes"
+	Used to force stop words
OR	Boolean operator, must be uppercase
|	Same as OR

30

Google Dork & Consort
https://www.exploit-db.com/google-hacking-database/
http://www.googleguide.com/advanced_operators.html

site:pastebin.com intext:list scanner online
site:pastebin.com intext:scanner online

inurl:ftp -inurl:(http|https) lechonpaul@gmail.com
Intitle:index.of name size site:hypem.com
Intitle:index.of
Intitle:index.of mp3 jackson AND iso kaspersky

Name Last modified Size Description
?C=N;O=A ?C=M;O=D ?C=S;O=A ?C=D;O=A

Google CSE resources
CSE Search Parameters | API Explorer - CSE URL structure

https://www.slideshare.net/andreicontan/kiran-karnad-rtc2014-ghdbfinal-35013977
http://guides.lib.berkeley.edu/GoogleTips

https://exploit.courses/files/bfh2017/
https://www.deepwebtech.com/talks/
https://www.iith.ac.in/~tbr/teaching/docs/

https://github.com/search/advanced

Oneliner DORK

Site:(.qc.ca) intitle:"index.of" ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:facture | intext:"client")

site:(.ca) intitle:"index.of" ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:facture | intext:"client")

Resources Monitors
Pastemonitor.com | Scumblr | Pastebin Crawler | Dumpmon

'"Reconnaissance:'"
[http://netbootcamp.org/pastesearch.html#gsc.tab=0 Paste Site Search] - Search 90+ paste sites. Filter by source & keyword.

Doxing (from *dox*, abbreviation of *documents*) or [1] **doxxing**[2][3] is the Internet-based practice of researching and broadcasting private or identifiable information (especially personally identifiable information) about an individual or organization.[3][4][5][6][7]
The methods employed to acquire this information include searching publicly available databases and social media websites (like Facebook), hacking, and social engineering. It is closely related to internet vigilantism and hacktivism. Doxing may be carried out for various reasons, including to aid law enforcement, business analysis, risk analytics, extortion, coercion, harassment, online shaming, and vigilante justice.[8][9]

Pour filtrer vos recherches des Mots-clefs:

WEBSITES
HTML = javascripts, css, widgets, themes, author, blogger, screen name
Analytics = google analytics "ua-12345...", statcounter, histats
Publishers = google adsense "ca-pub...", widgets, i.e. sharethis id
Hosting = domain, ip address, ns, mx, isp, sql

DOXING
Personal = name, age, dob, phone, email, address, ip address, vehicle, height, parents, password
Employer = website/domain, email, phone, ip address, isp, mx, mail, ns1, port, job title, department nam

CARD DUMPS
Terms = cvv, ssn, social security number, pin, wu, visa, mastercard, expiration

PIRACY
Video = x264, xvid, cam, scr, rip, hdtv, cam, ts, webrip, subs, torrent, nfo, French (language)
Music = mp3, kpbs, m4a, aac
Games = serial key, mod, crack, ntsc
Software = repack, preactivated, crack, nulled
eBooks/Images = pdf, ebook, res, set, hd, pic

https://github.com/search/advanced

Obtenir accès au réseau

AirDrive Keylogger

NEW

The **AirDrive Keylogger** is an innovative ultra-small USB keylogger, only **0.8" (21mm)** in length. It can be accessed with any Wi-Fi device such as a **computer, laptop, tablet, or smartphone**. The Pro and Max versions offer **time-stamping**, **E-mail reporting**, **data streaming**, and up to **8 gigabytes** of built-in memory. [more...]

AirDrive Keylogger - **$51.99** | €45.99
AirDrive Keylogger Pro - **$71.99** | €62.99
AirDrive Keylogger Max - **$112.99** | €98.99

KeyGrabber USB

This USB hardware keylogger has a huge **16 MB** or **8 GB** memory capacity, organized into an advanced flash FAT file system. Super-fast data retrieve is achieved by switching into **Flash Drive mode** for download. Completely invisible for computer operation, no software or drivers required. [more...]

ver. **16 MB** (128 Mbit) - **$51.99** | €45.99
ver. **8 GB** (64 Gbit) - **$71.99** | €62.99

Click to open expanded view

midbit Technologies, LLC

SharkTap Gigabit Network Sniffer

9 customer reviews | 4 answered questions

Amazon's Choice for "network tap"

Price: $179.95

Only 13 left in stock - order soon.

This item ships to **Canada**. **Want it Thursday, Jan. 18?** Order within **21 hrs 23 mins** and choose **AmazonGlobal Priority Shipping** at checkout. Learn more
Sold by midbit Technologies, LLC and Fulfilled by Amazon. Gift-wrap available.

- The SharkTap is a special purpose ethernet switch that allows you to 'tap into' an ethernet connection. It is intended to be used with the free Wireshark network analyzer or equivalent.
- Conventional switches route packets only to the intended destination port, reducing traffic, but preventing a third port from seeing all packets. The SharkTap duplicates all packets to or from the 'NETWORK' ports on the 'TAP' port.
- Supports 10, 100 and 1000Base-T, all ports. Power-Over-Ethernet (POE) pass-through on the 'NETWORK' ports.
- Powered from a micro-USB cable (included), draws 350mA or less. For USB TAP, search 'SharkTapUSB'
- Other features: Auto-MDIX, so no crossover cables ever needed. Non-conductive enclosure. Will not route packets from TAP to NETWORK ports.

Exfiltration

3G/GPRS shield over Arduino and Raspberry Pi

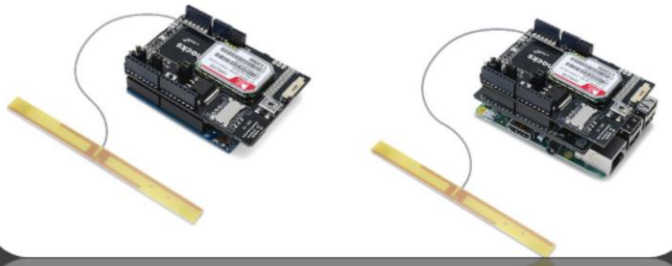
Difficulty Level: Expert -

Tweet

Buy now

✔ **UPDATE**: Now two models available. SIM5215E for Europe and SIM5215A for US / Canada / Australia.

The 3G shield for Arduino and Raspberry Pi enables the connectivity to high speed **WCDMA** cellular networks in order to make possible the creation of the next level of worldwide interactivity projects inside the new "Internet of Things" era.



Vecteurs d'infections – Appareils USB

Un appareils USB peut avoir un comportement totalement différent de ce qu'il prétend :

Exemple: USB Missile Launcher agissant comme un malware.

Vecteurs d'infections – Appareils trafiqués

Le chiffrement du disque dur c'est bien contre le vol mais ….

- Toutes les autres composantes de votre ordinateur peuvent être remplacés ;
- Une fois démarré il est possible d'accéder aux données chiffrées.

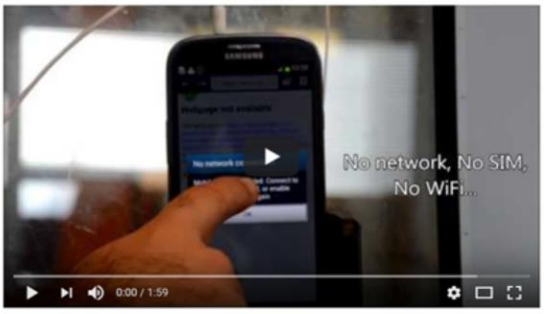
Donc:

- Ne jamais laisser votre ordinateur sans surveillance ;
- Toujours barrer physiquement votre ordinateur lorsque vous de ne l'utiliser pas.

Exfiltration de données – Appareils espion

Il existe une myriade de travaux pour faire de l'exfiltration de données dans un environnement « Air-Gapped » :

- Émissions électromagnétiques de la carte vidéo, de l'écran, du ventilateur, etc. ;
- Émissions visuels :
  Indicateurs LED sur un boîtier d'ordinateur,
  Système de surveillance vidéo, etc. ;
- Autres types d'émissions.



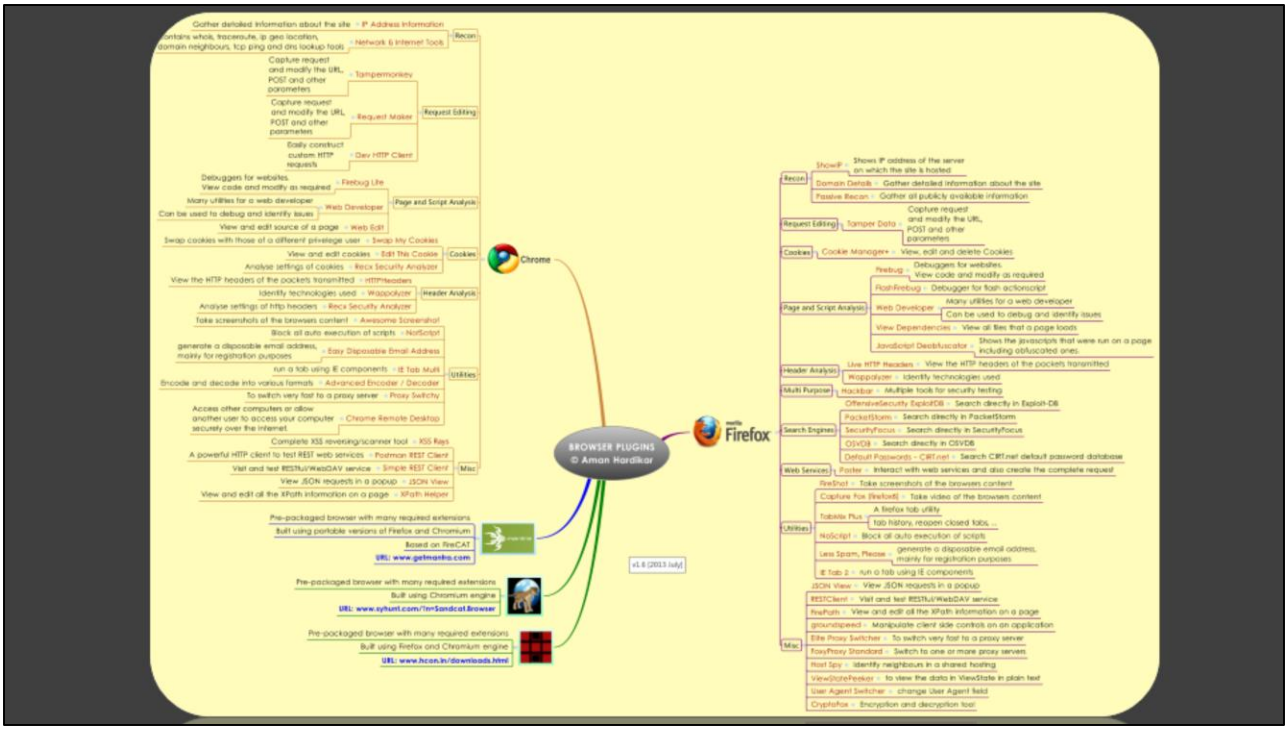
How to leak sensitive data from an isolated computer (air-gap) to a near by mobile phone - AirHopper

https://www.youtube.com/watch?v=2OzTWiGI1rM

Toutes les données publiques – Soyez attentif!


QUE FAIT-ON!


OSINT Landscape v.1 February 2018
Open Source Intelligence (/OSINV – Open Source Investigation)
COVERT SHORES
www.hisutton.com
bellingcat
Social Media Platforms
Facebook
Weibo
Twitter
Qzone
Instagram
Odnoklassniki
Linkedin
VK
Snapchat
YouTube
Periscope
stalkscan
FBDOWN
Signal
peoplefindThor
Tweetbeaver
twXplorer
Twitter List Copy
TweetDeck
WEBSTA
picodash
socilab
Snap Map
savefrom.net
Youtube DataViewer
frame by frame
storyful
Geo Search Tool
Scopedown
Dataminr
INTELTECHNIQUES
Echosec
War Wire
Messaging & closed groups
Sharing & Publishing
flickr
Pinterest
Google+
Blogging, Forums & other communities
STRAVA
tumblr.
LIVEJOURNAL
classmates
WordPress.org
Blogger
WiX.com
Medium
ProBoards
SQUARESPACE
Joomla!
ghost
weebly
Internet Search
Google
Yandex
Bing
DuckDuckGo
NAVER
Geospatial Data
GeoNames
Free GIS Data
SECRETS OF THE WEST
OpenRailwayMap
MAPS.ME
Mapillary
wikimapia
Satellite Imagery
Google Earth
Descartes Labs
TERRA server
AIRBUS OneStore
Zoom Earth
unitar
HARRIS
USGS
esa
planet
Radiant.Earth
NOAA
EARTHDATA
esa
DigitalGlobe
SENTINEL
Maritime Movements
MarineTraffic
IHS Markit
AISLive
Lloyd's List Intelligence
SHIPSPOTTING
Shipfinder
AISHub
shipfinder
OpenSeaMap
SHIPAIS
ShippingExplorer
BoatNerd
AisDecoder
COAA
Aviation Movements
AirNav RadarBox
ADS-B Exchange
FlightAware
LiveATC.net
flightradar24
GVA Dictator Alert
PLANESPOTTERS.NET
Radio
RadioReference
Broadcastify
Radio Garden
SDR.hu
ProScan
MilScanners
Commercial Registries
opencorporates
infobel
ICIJ OFFSHORE LEAKS DATABASE
Webcams
pentopia
Insecam
SHODAN
EarthCam
Webcams.travel
PICTIMO
wetter.com
lookr
wisuki
Image / Vid / Doc Forensics
GET-METADATA
Jeffrey's Image Metadata
metapicz
FotoForensics
Forensically
IRFANVIEW
hattorl / Spiderpig
exifdata
ExifTool
InVID
This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.
Authors:
H I Sutton, (@CovertShores) Covert Shores and Jane's contributor,
Aliaume Leroy, (@Yaxlr) Bellingcat & BBC,
Tony Roper, (@Topol_M5527), planesandstuff, Jane's contributor


BROWSER PLUGINS
© Aman Hardikar
Chrome
Recon
Gather detailed information about the site - IP Address Information
Contains whois, traceroute, ip geo location, domain neighbours, tcp ping and dns lookup tools - Network & Internet Tools
Request Editing
Capture request and modify the URL, POST and other parameters - Tampermonkey
Capture request and modify the URL, POST and other parameters - Request Maker
Easily construct custom HTTP requests - Dev HTTP Client
Page and Script Analysis
Debuggers for websites. View code and modify as required - Firebug Lite
Many utilities for a web developer. Can be used to debug and identify issues - Web Developer
View and edit source of a page - Web Edit
Cookies
Swap cookies with those of a different privelege user - Swap My Cookies
View and edit cookies - Edit This Cookie
Analyse settings of cookies - Recx Security Analyzer
Header Analysis
View the HTTP headers of the packets transmitted - HTTPHeaders
Identify technologies used - Wappalyzer
Analyse settings of http headers - Recx Security Analyzer
Utilities
Take screenshots of the browsers content - Awesome Screenshot
Block all auto execution of scripts - NotScript
generate a disposable email address, mainly for registration purposes - Easy Disposable Email Address
run a tab using IE components - IE Tab Multi
Encode and decode into various formats - Advanced Encoder / Decoder
To switch very fast to a proxy server - Proxy Switchy
Misc
Access other computers or allow another user to access your computer securely over the internet - Chrome Remote Desktop
Complete XSS reversing/scanner tool - XSS Rays
A powerful HTTP client to test REST web services - Postman REST Client
Visit and test RESTful/WebDAV service - Simple REST Client
View JSON requests in a popup - JSON View
View and edit all the XPath information on a page - XPath Helper
Pre-packaged browser with many required extensions. Built using portable versions of Firefox and Chromium. Based on FireCAT. URL: www.getmanbu.com
Pre-packaged browser with many required extensions. Built using Chromium engine. URL: www.sytumt.com/?m=Sandcat.Browser
Pre-packaged browser with many required extensions. Built using Firefox and Chromium engine. URL: www.hcan.in/downloads.html
v1.8 (2013 July)
Firefox
Recon
ShowIP - Shows IP address of the server on which the site is hosted
Domain Details - Gather detailed information about the site
Passive Recon - Gather all publicly available information
Request Editing
Tamper Data - Capture request and modify the URL, POST and other parameters
Cookies
Cookie Manager+ - View, edit and delete Cookies
Page and Script Analysis
Firebug - Debuggers for websites. View code and modify as required
FlashFirebug - Debugger for flash actionscript
Web Developer - Many utilities for a web developer. Can be used to debug and identify issues
View Dependencies - View all files that a page loads
JavaScript Deobfuscator - Shows the javascripts that were run on a page including obfuscated ones
Header Analysis
Live HTTP Headers - View the HTTP headers of the packets transmitted
Wappalyzer - Identify technologies used
Multi Purpose
Hackbar - Multiple tools for security testing
Search Engines
OffensiveSecurity ExploitDB - Search directly in Exploit-DB
PacketStorm - Search directly in PacketStorm
SecurityFocus - Search directly in SecurityFocus
OSVDB - Search directly in OSVDB
Default Passwords - CIRT.net - Search CIRT.net default password database
Web Services
Poster - Interact with web services and also create the complete request
Utilities
FireShot - Take screenshots of the browsers content
Capture Fox (Firefox5) - Take video of the browsers content
TabMix Plus - A firefox tab utility. Tab history, reopen closed tabs, ...
NoScript - Block all auto execution of scripts
Less Spam, Please - generate a disposable email address, mainly for registration purposes
IE Tab 2 - run a tab using IE components
JSON View - View JSON requests in a popup
Misc
RESTClient - Visit and test RESTful/WebDAV service
FirePath - View and edit all the XPath information on a page
groundspeed - Manipulate client side controls on an application
Elite Proxy Switcher - To switch very fast to a proxy server
FoxyProxy Standard - Switch to one or more proxy servers
Host Spy - Identify neighbours in a shared hosting
ViewStatePeeker - to view the data in ViewState in plain text
User Agent Switcher - change User Agent field
CryptoFox - Encryption and decryption tool

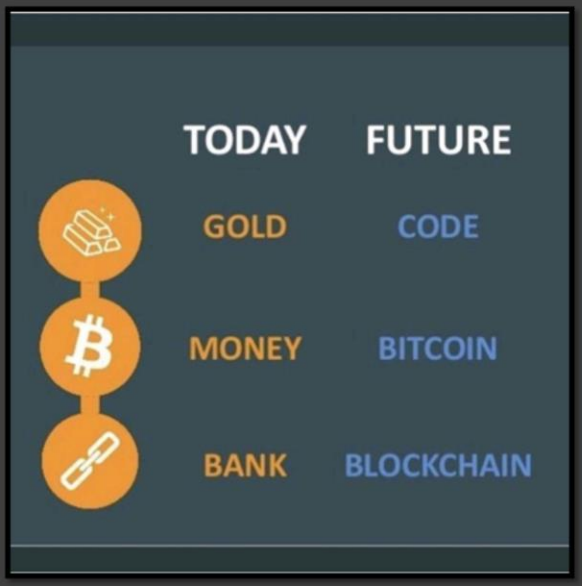
Anti-social networks

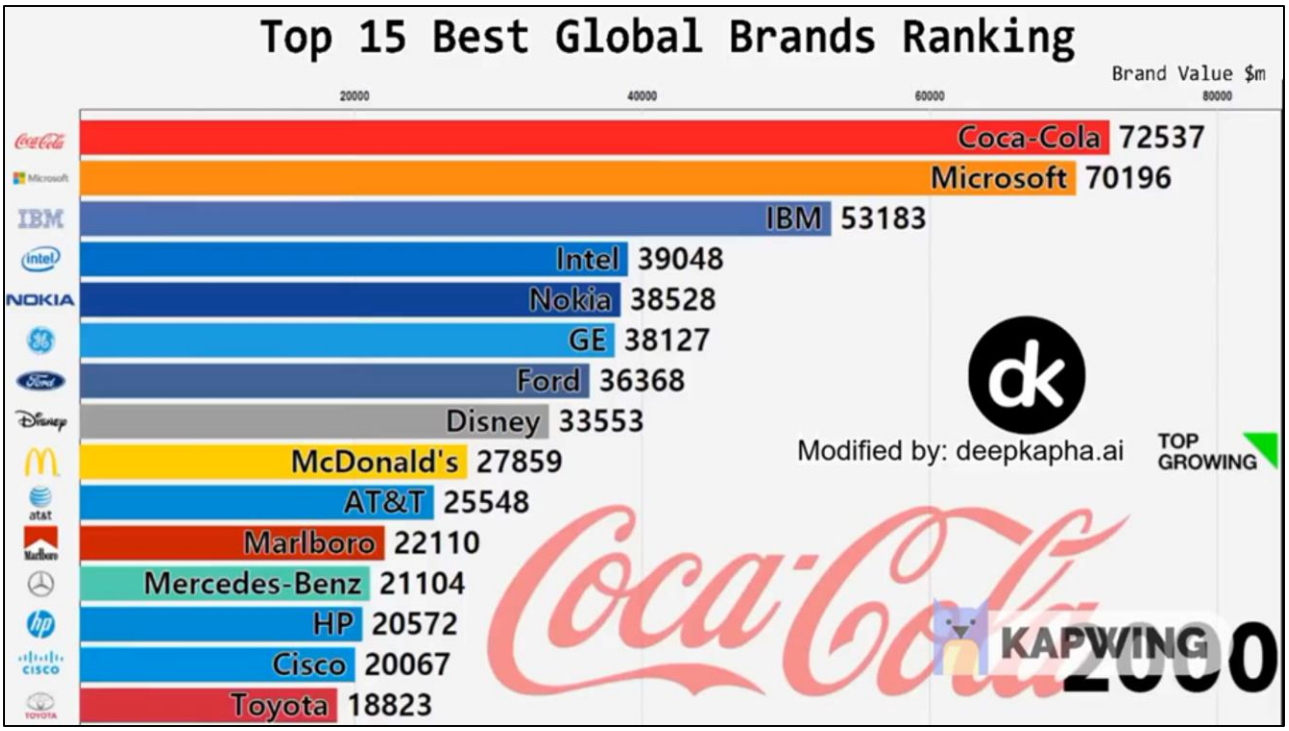
- Chercher son nom sur Internet pour voir les informations accessibles et tenter de les limiter
- Renforcer ses paramètres de sécurité et vie privée des réseaux sociaux
- Infection de vos appareils par l'intermédiaire d'un tiers
- Obtention d'informations permettant de répondre à vos questions secrètes
- Obtention d'informations sensibles via votre entourage (nature des mandats et clients, horaire de travail, type de carte d'accès, etc.)
- Sensibiliser votre entourage proche
  - À adopter de bonnes habitudes d'utilisation d'Internet
  - À limiter les informations qu'ils donnent à des tiers sur votre emploi
  - Au fait qu'ils peuvent être ciblés pour vous atteindre.

43

Démonstration du scénario d'attaque a montré l'importance de faire attention sur Internet.

>_Get-FutureMad




Top 15 Best Global Brands Ranking
Brand Value $m
20000
40000
60000
80000
Coca-Cola 72537
Microsoft 70196
IBM 53183
Intel 39048
Nokia 38528
GE 38127
Ford 36368
Disney 33553
McDonald's 27859
AT&T 25548
Marlboro 22110
Mercedes-Benz 21104
HP 20572
Cisco 20067
Toyota 18823
Modified by: deepkapha.ai
TOP GROWING
KAPWING
2000

>_Add-Calendar

HACKFEST

Novembre 2019

Hackfest.ca

Venez en nombre…

capture the flag game history
ctf training
learn ctf

https://en.wikipedia.org/wiki/Capture_the_flag
https://en.wikipedia.org/wiki/Wargame_(hacking)

https://github.com/ctfs

https://apsdehal.in/awesome-ctf/
https://github.com/the-c0d3r/ctf-tools
http://captf.com/practice-ctf/

https://bitvijays.github.io/index.html
http://www.defragmented-brains.at/about-ctf-contests.html

Hackathons vs. CTFs
15 Strategies to Win Hackathons
https://pavursec.com/blog/

https://github.com/xtiankisutsa/awesome-mobile-CTF

http://carnal0wnage.attackresearch.com/2013/08/want-to-break-some-android-apps.html
https://www.owasp.org/index.php
https://github.com/ctfs
http://shell-storm.org/repo/

https://github.com/We5ter/Awesome-Platforms

WeChall – list of wargame websites
security.stackexchange.com - hacking competitions
CTFtime - worldwide CTF tracking site

>_Set-Merci
>_Get-Questions ?

"Setec Astronomy" est l'anagramme de "too many secrets"!

Un autre moyen de "Reverser"

Open Source Threat Intelligence Tool
Harvest and analyse IOCs

- AbuseHelper – An open-source framework for receiving and redistributing abuse feeds and threat intel.
- AlienVault Open Threat Exchange – Share and collaborate in developing Threat Intelligence.
- Combine – Tool to gather Threat Intelligence indicators from publicly available sources.
- Fileintel – Pull intelligence per file hash.
- Hostintel – Pull intelligence per host.
- IntelMQ – A tool for CERTs for processing incident data using a message queue.
- IOC Editor – A free editor for XML IOC files.
- ioc_writer – Python library for working with OpenIOC objects, from Mandiant.
- Massive Octo Spice – Previously known as CIF (Collective Intelligence Framework). Aggregates IOCs from various lists. Curated by the CSIRT Gadgets Foundation.
- MISP – Malware Information Sharing Platform curated by The MISP Project.
- Pulsedive – Free, community-driven threat intelligence platform collecting IOCs from open-source feeds.
- PyIOCe – A Python OpenIOC editor.
- RiskIQ – Research, connect, tag and share IPs and domains. (Was PassiveTotal.)
- threataggregator – Aggregates security threats from a number of sources, including some of those listed below in other resources.
- ThreatCrowd – A search engine for threats, with graphical visualization.
- ThreatTracker – A Python script to monitor and generate alerts based on IOCs indexed by a set of Google Custom Search Engines.
- TIQ-test – Data visualization and statistical analysis of Threat Intelligence feeds.

Liens et références – Général

Menaces et risques

- Advanced persistent threat (APT) https://en.wikipedia.org/wiki/Advanced_persistent_threat
- Cyber attacks targeting DoD contractor, OPM, and U.S. aircraft carrier linked to China https://www.scmagazine.com/researchers-link-dod-contractor-cyber-attack-to-opm-breach/article/567620/
- Anonymous hack US Department of Defence – Analysis of the Attack https://www.acunetix.com/blog/news/anonymous-hack-us-department-of-defence-analysis/
- Cyber Attacks on U.S. Companies in 2016 https://www.heritage.org/defense/report/cyber-attacks-us-companies-2016
- Investigation reveals cyberattacks on defense contractors https://www.washingtonpost.com/business/economy/investigation-reveals-cyberattacks-on-defense-contractors/2014/09/17/d56e84e6-3e95-11e4-9587-5dafd96295f0_story.html?utm_term=.0c2332140fc0

Liens et références – Informations sur Internet

Outils de recherche

- Reference: Advanced Operators for Web Search
  https://sites.google.com/site/gwebsearcheducation/advanced-operators

Paramètres de sécurité et vie privée sur les réseaux sociaux

- Gestion du compte Google : https://myaccount.google.com/
- LinkedIn https://www.linkedin.com/psettings/
- Facebook https://www.facebook.com/settings

Liens et références – Attaques contre les réseaux « air-gapped »

Wireless devices hacking

- Mousejack https://www.mousejack.com/
- Radio Hack Steals Keystrokes from Millions of Wireless Keyboards https://www.wired.com/2016/07/radio-hack-steals-keystrokes-millions-wireless-keyboards/
- How to Hack Bluetooth https://null-byte.wonderhowto.com/how-to/hacks-mr-robot-hack-bluetooth-0163586/

Hardware tampering

- Glenn Greenwald: how the NSA tampers with US-made internet routers https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden
- China and Cybersecurity: Trojan Chips and U.S.–Chinese Relations https://www.heritage.org/asia/report/china-and-cybersecurity-trojan-chips-and-us-chinese-relations
- Lenovo's Superfish security snafu blows up in its face https://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/

Liens et références – Attaques contre les réseaux « air-gapped »

Techniques d 'exfiltration

- Stealing Data From Computers Using Heat https://www.wired.com/2015/03/stealing-data-computers-using-heat/
- Clever Attack Uses the Sound of a Computer's Fan to Steal Data https://www.wired.com/2016/06/clever-attack-uses-sound-computers-fan-steal-data/
- Air-Gap Research Page https://cyber.bgu.ac.il//advanced-cyber/airgap

Liens et références – Social engineering

Concepts

- Présentation du principe Need to know https://en.wikipedia.org/wiki/Need_to_know
- Présentation du social engineering https://en.wikipedia.org/wiki/Social_engineering_(security)
- Email spoofing https://en.wikipedia.org/wiki/Email_spoofing

Stratagèmes

- Fraude de faux président https://www2.deloitte.com/lu/en/pages/about-deloitte/articles/fake-presidents.html
- Business fraud https://www.spvm.qc.ca/en/Fiches/Details/Business-fraud
- Hackers used luxury hotel Wi-Fi to steal business executive's data researchers say https://www.theguardian.com/technology/2014/nov/10/hotel-wi-fi-infected-business-travellers-asia-kaspersky