

Protéger ses sources, sécuriser ses données

**Manach
Jean-Marc**
jmm@rewriting.net



1. Une brève histoire de la sécurité informatique

- Enigma & Alan Turing
- Darpa & TCP/IP
- PGP & les crypto wars (+ on dit chiffrer, par « crypter »)
- Signal & E2EE & Telegram #Fails

2. Comprendre son modèle de menace

- Snowden VS « Tous sur écoute »
- Pegasus VS « 50 000 cibles potentielles »
- Hygiène (de sécurité) informatique
- Oubliez les « mots de passe »

3. Le kit de survie numérique

- Le passeport de conseils aux voyageurs de l'ANSSI
- EFF's Surveillance Self-Defense
- Backup, Air Gap
- Tor VS Darkweb + 1/4h d'anonymat

4. Comment gérer les lanceurs d'alerte

- Primum non nocere + être joignable/à l'écoute
- Lui faire comprendre son propre modèle de menace
- Anonymiser les méta-données
- La maison des lanceurs d'alerte



UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE

- <https://www.franceculture.fr/emissions/lenigmatique-alan-turing>

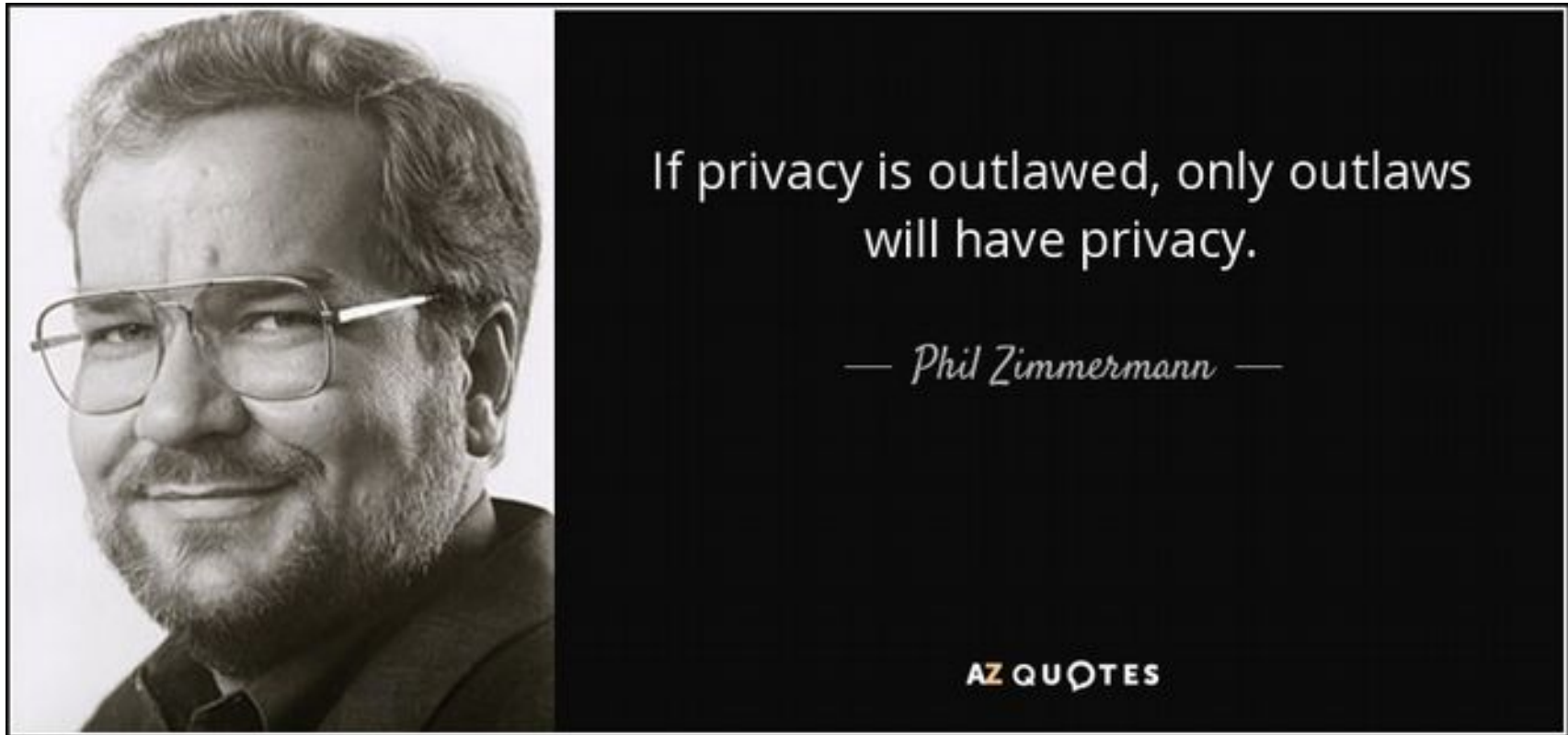


UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE



<https://vimeo.com/311894477>

UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE



https://fr.wikipedia.org/wiki/Crypto_Wars

UNE BRÈVE HISTOIRE DE LA SÉCURITÉ INFORMATIQUE

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS

(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of text data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	• Message Content: Unfused • Subpoena: can render basic subscriber information • 14 U.S.C. § 2503(a) can render 25 days of iMessage lookups to and from a target number¹ • Pen Register: no capability² • Search Warrants: can render backups of a target device if target uses iCloud backup, the exception: keys should also be provided with content return³, can also require iMessages from iCloud servers if target has installed Messages in iCloud	• Message Content: Limited⁴ • Subpoena: can render certain registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information: no message • "Maximum of 30 consecutive" worth of specified recent text chats (only when LTR has not been selected and applied and only when recording an effective warrant; backups, videos, pictures, files, location, phone call records and other such data will not be disclosed)	• No Message Content • Data and: Live a joint registered • Last date of a user's connectivity to the server	• No Message Content • No content information provided for law enforcement to pursue a court order. An FBI Telegram's privacy state must, for confirmed terminal investigations, include a court order to access and provide number for relevant authorities	• No Message Content • Bulk of phone number and email address, if provided by user • Push Token, if push service is used • Data (as time of Threema ID creation) • Data (as time of last login)	• No Message Content • Provider account (i.e. phone number) registration data a ml # address at time of creation • Message history: time, date, source number, and destination number	• No Message Content • Account: preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is returned for as long as the account is active	• Message Content: Limited⁵ • Subpoena: can render basic subscriber records • Court Order: Subpoena return as well as information like blocked users • Search Warrants: Provides address book contacts and WhatsApp's server-side history (be target, or their address book contacts) • Pen Register: Sent every 15 minutes, provides timing and destination for each message ¹ Not target is using an iPhone and iCloud backup enabled, it had returned any message WhatsApp data, to include message content	• No Message Content • Extra and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IPs (email addresses and phone numbers) connected to the account, but not plaintext external addresses • Device make • Limited records of recent changes to account settings such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

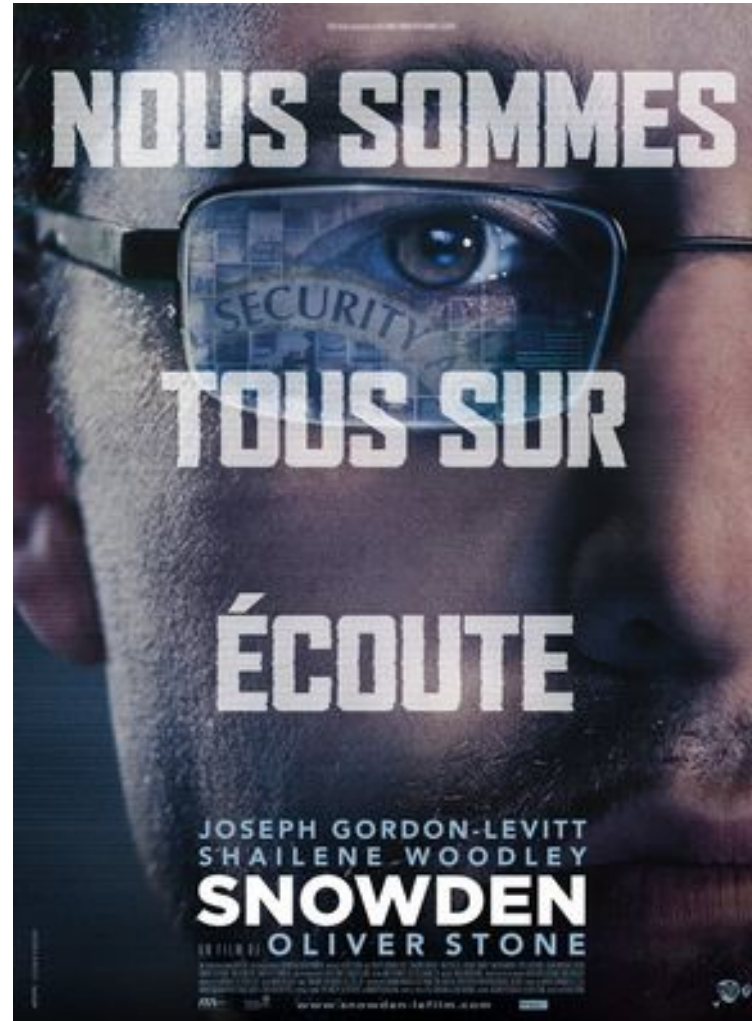
(U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry by (U//LES) LAW ENFORCEMENT SENSITIVE The information marked (U//LES) is the property of FBI and may be cleared with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Procedures should be taken to ensure use in legal proceedings without first receiving authorization from the originating agency. Backups are prohibited from subsequence

UNCLASSIFIED//LAW

Account	Information
	N/A
	Last connection date: Unix millis Account created: Unix millis

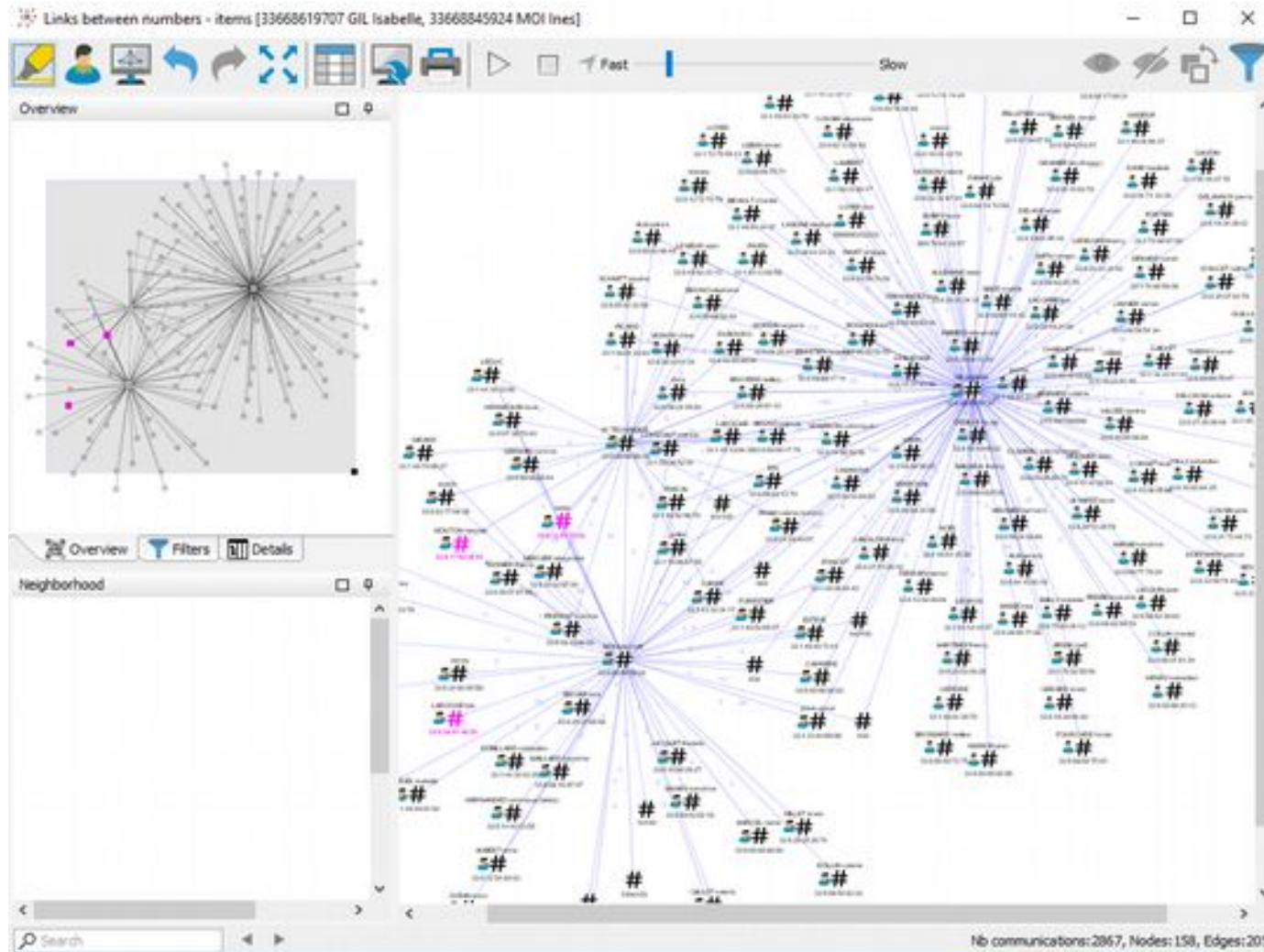
<https://www.01net.com/actualites/ent-revele-les-donnees-que-le-fbi>

COMPRENDRE SON MODÈLE DE MENACE



<http://bugbrother.blog.lemonde.fr/2015/01/03/de-la-surveillance-de-masse-a-la-paranoia-generalisee/>

COMPRENDRE SON MODÈLE DE MENACE



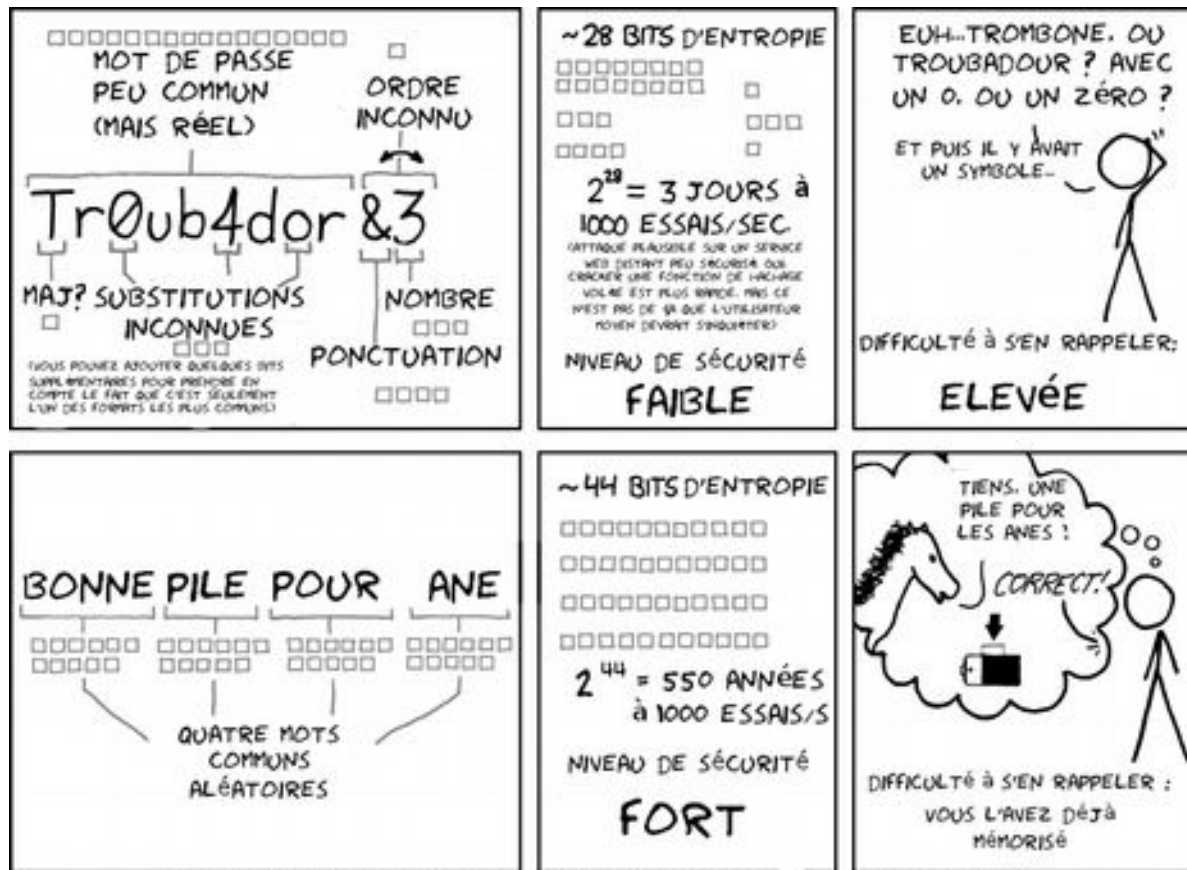
<https://www.nextinpact.com/article/47791/pegasus-50-000-cibles-potentielles-12>

COMPRENDRE SON MODÈLE DE MENACE



<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique>

COMPRENDRE SON MODÈLE DE MENACE



EN 20 ANS D'EFFORTS. ON A RÉUSSI à HABITUER LES GENS à UTILISER DES MOTS DE PASSE QUI SONT DIFFICILES à RETENIR POUR LES HUMAINS. MAIS FACILES à DEVINER POUR LES ORDINATEURS.

<https://www.nextinpact.com/article/48544/phrases-passe-cnll-passe-elle-aussi-en-mode-2-0>

LE KIT DE SURVIE NUMÉRIQUE

► LES 9 BONNES PRATIQUES EN UN COUP D'ŒIL

AVANT	1 Évitez le transport de données superflues	2 Informez-vous sur la législation du pays de destination	3 Sauvegardez les données que vous emportez	
PENDANT	4 Faites preuve de discrétion	5 Évitez de laisser vos documents et équipements sans surveillance	6 Évitez de vous connecter aux réseaux ou équipements non maîtrisés	7 Informez votre responsable de la sécurité en cas de perte ou de vol
APRÈS	8 Renouvelez les mots de passe utilisés lors de votre déplacement	9 En cas de doute, faites vérifier vos équipements par votre responsable de la sécurité		

<https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/>

LE KIT DE SURVIE NUMÉRIQUE

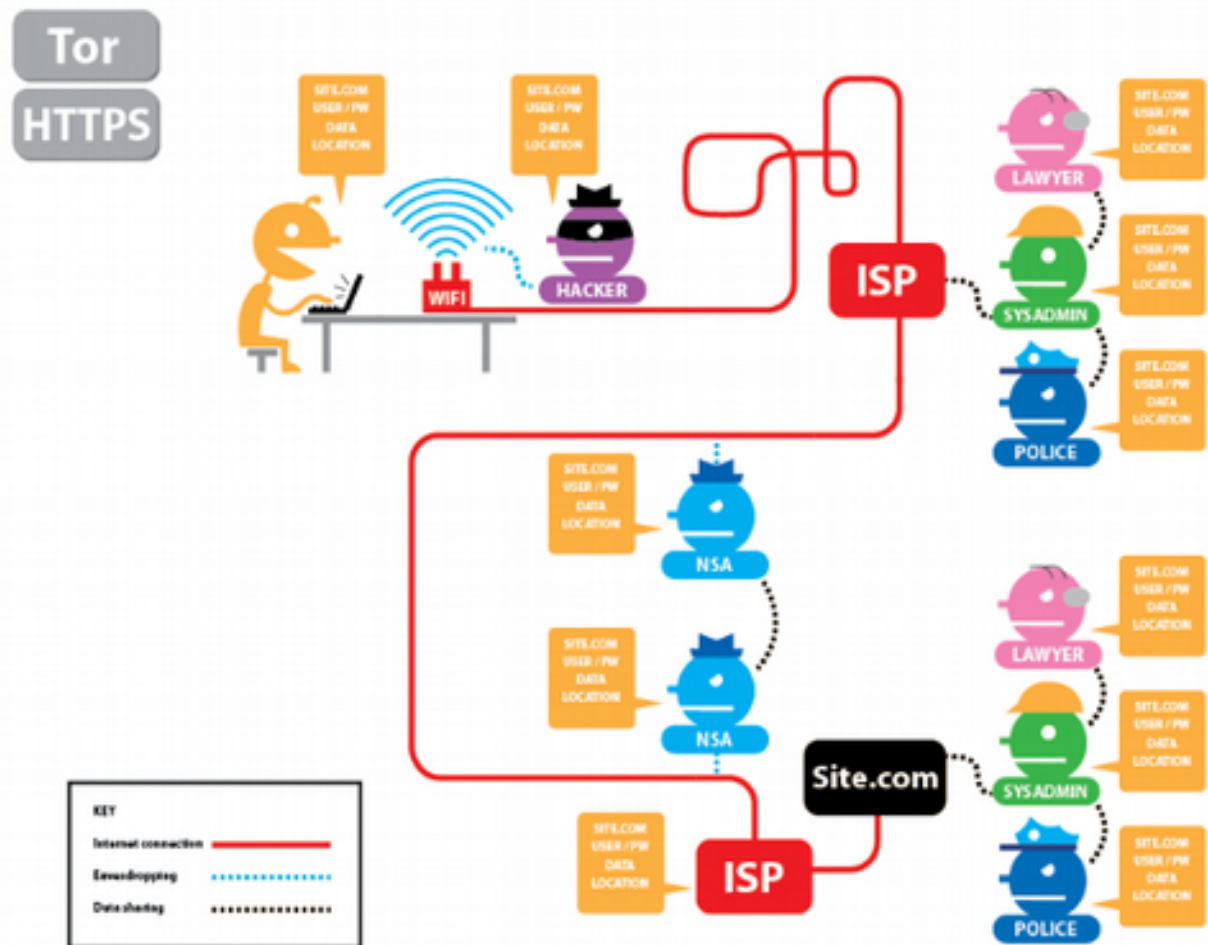


<https://ssd.eff.org/en>



<https://anonymousplanet-ng.org/>

LE KIT DE SURVIE NUMÉRIQUE



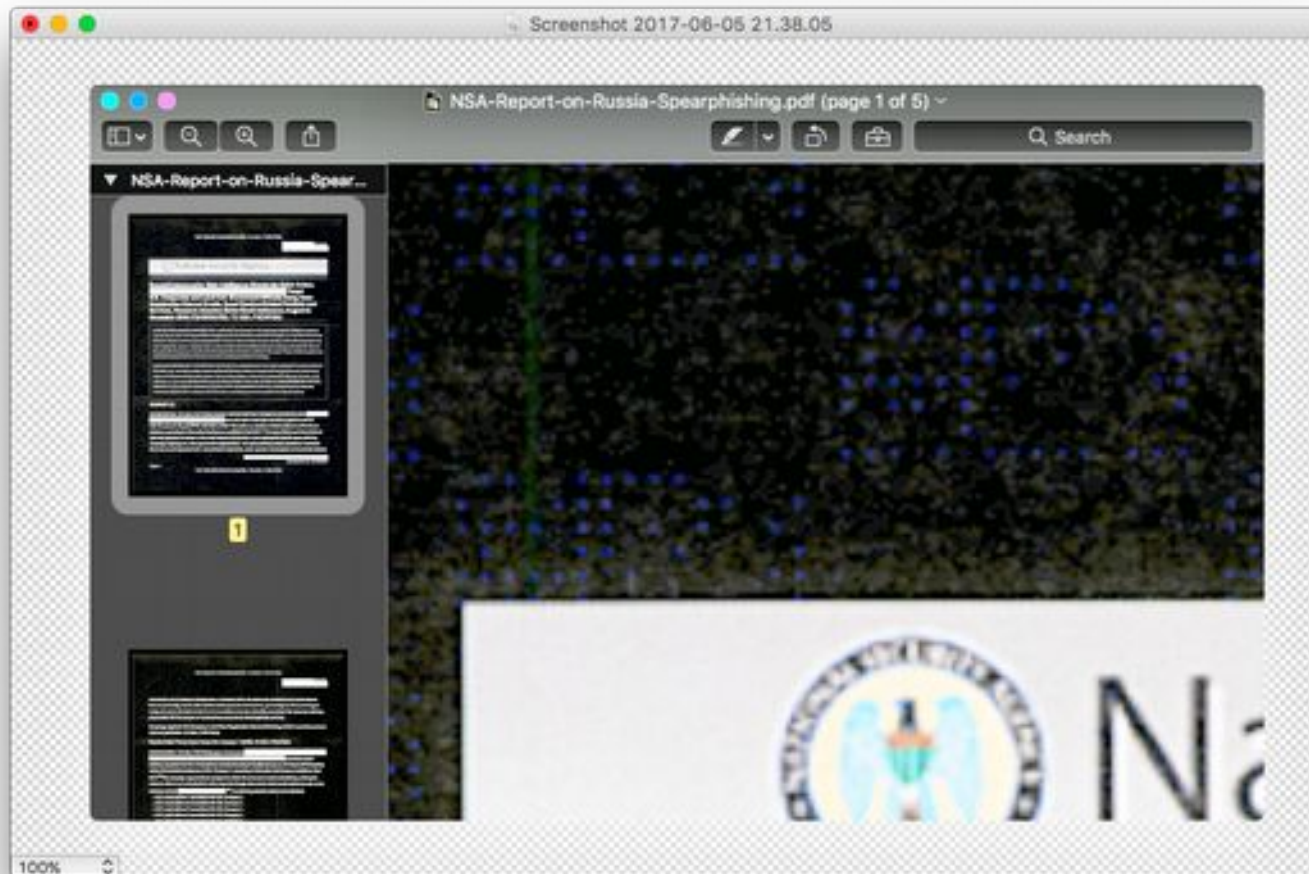
<https://www.eff.org/pages/tor-and-https>

COMMENT GÉRER LES LANCEURS D'ALERTE



<http://web.archive.org/web/20171130074638/http://www.wefightcensorship.org/fr/online-survival-kit.html>

COMMENT GÉRER LES LANCEURS D'ALERTE

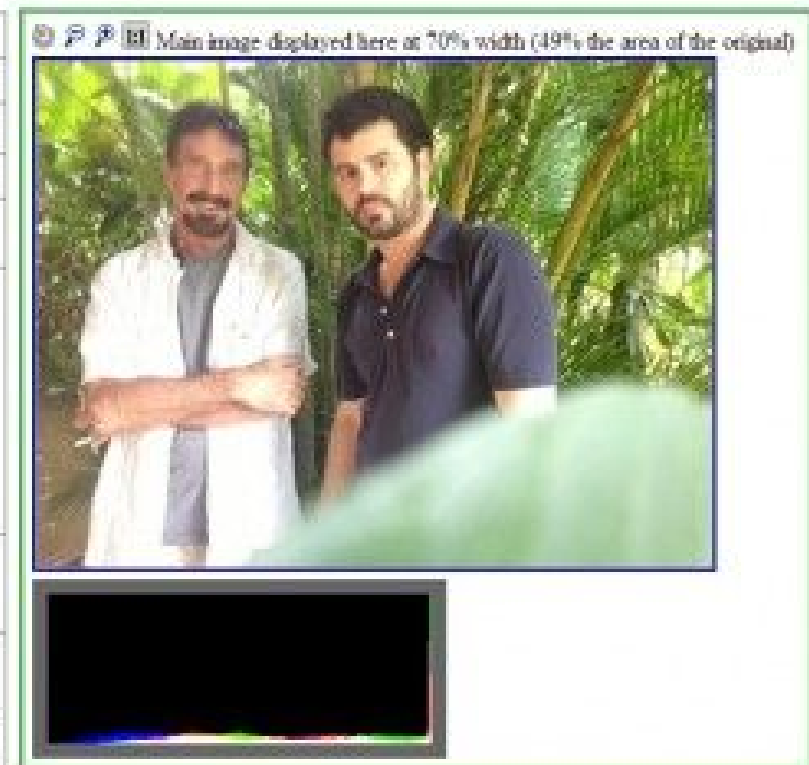


<https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html>

COMMENT GÉRER LES LANCEURS D'ALERTE

Basic Image Information

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125
Flash:	Off. Did not fire
Date:	December 3, 2012 12:26:08PM (timezone not specified) (2 hours, 44 minutes, 39 seconds ago, assuming image timezone of 8 hours behind GMT)
Location:	Latitude/longitude: 15° 19' 29.4" North, -88° 59' 31.8" West (15.32483, -88.992167) Photos on Jeffrey's blog that are near this location. Map via embedded coordinates at: Google, Yahoo, Wikimapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 7.152159468 m Timezone guess from earthtools.org: 8 hours behind GMT
File:	480 × 640 JPEG 132,481 bytes (0.13 megabytes) Image compression: 88% 4% crop of the 3,264 × 2,448 (8.0 megapixel) original
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.
Image URL:	http://assets.vice.com/content-images/contentimage-main/3b1c675e0012f73d7dc6207485b673.jpg Apply other tools to this image via ImgOps.com.



<https://thenextweb.com/news/vice-leaves-metadata-in-photo-of-john-mcafee-pointing-him-to-a-location-in-guatemala>

COMMENT GÉRER LES LANCEURS D'ALERTE



**MAISON
DES LANCEURS
D'ALERTE**

<https://mlalerte.org>

VOTRE FORMATEUR

►(data)journaliste « hacker » d'investigation

Pionnier du journalisme d'investigation sur Internet, traducteur et auteur de nombreux manuels de sécurité informatique, « éleveur » de lanceurs d'alerte depuis l'an 2000 (dont aucun n'a jamais été identifié a posteriori).



Manach
Jean-Marc

jmm@rewriting.net

<https://jean-marc.manach.net/>

https://fr.wikipedia.org/wiki/Jean-Marc_Manach

<https://twitter.com/manhack>



<https://www.linkedin.com/in/manhack>

►Ceci pourrait vous intéresser :

Bloc au choix :



CONFÉRENCE

- De la surveillance de masse à la paranoïa généralisée
<https://video.passageenseine.fr/w/fe1f61cf-cc78-452a-8e4b-8a8d3d468356>



FORMATION

- Le MOOC de l'ANSSI
<https://secnumacademie.gouv.fr/>



LIVRES BLANCS

- Guide d'auto-défense numérique
<https://guide.boum.org/>



WEBINARS

- Internet : la liberté sous contrôle ?
<http://communication-ccas.fr/journal/internet-la-liberte-sous-co>



FORMATION CERTIFIANTE

- Défis et enjeux de la cybersécurité
<https://www.fun-mooc.fr/fr/cours/defis-et-enjeux-de-la-cybersecurite/>



BLOGROLL

- Bug Brother
<https://www.lemonde.fr/blog/bugbrother/>