Autodéfense numérique pour les militants

Version 1.2 - Octobre 2024

https://acab.press/autodefense-numerique

Objectif

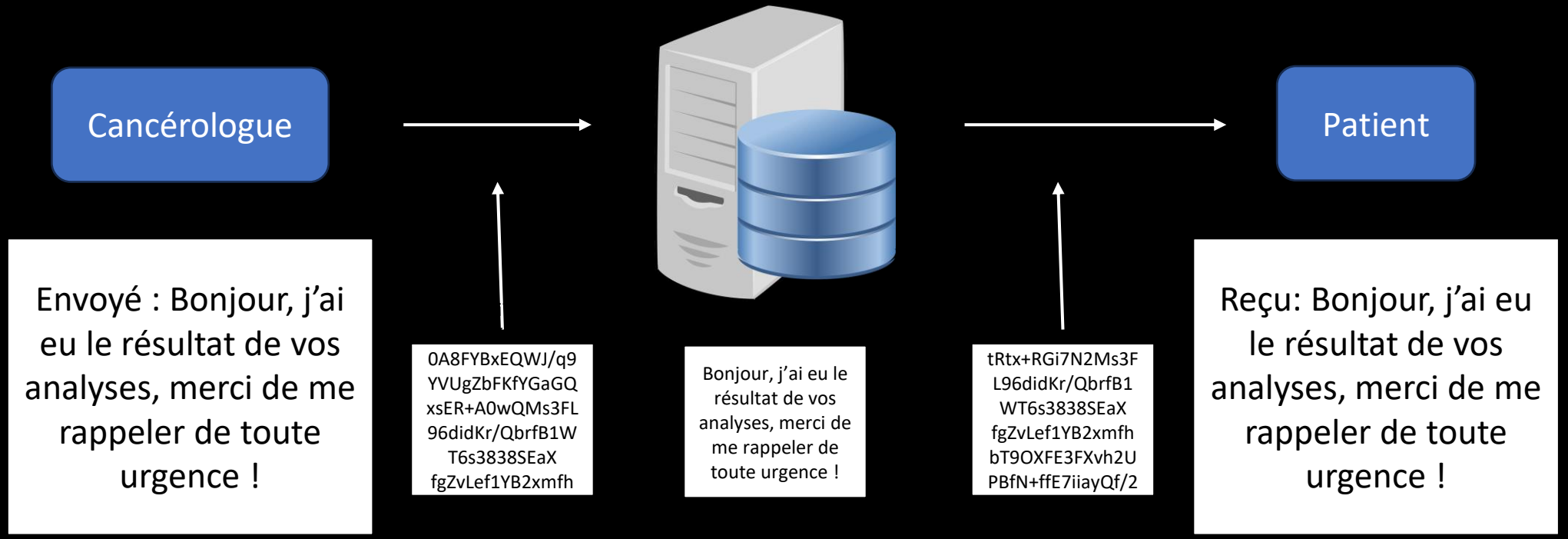
- Comprendre les risques liés à l’usage inévitable du numérique
- Apprendre à sécuriser ses communications
- Stocker des fichiers sensibles
- Ne pas s’auto-incriminer
- Dans les organisations, la sécurité doit être pensée collectivement ⚠️

Le téléphone

- Votre meilleur ennemi
- Un outil indispensable
- Caméra + micro + GPS dans la poche 24h/24
- Données stockées sur l’appareil et dans le cloud

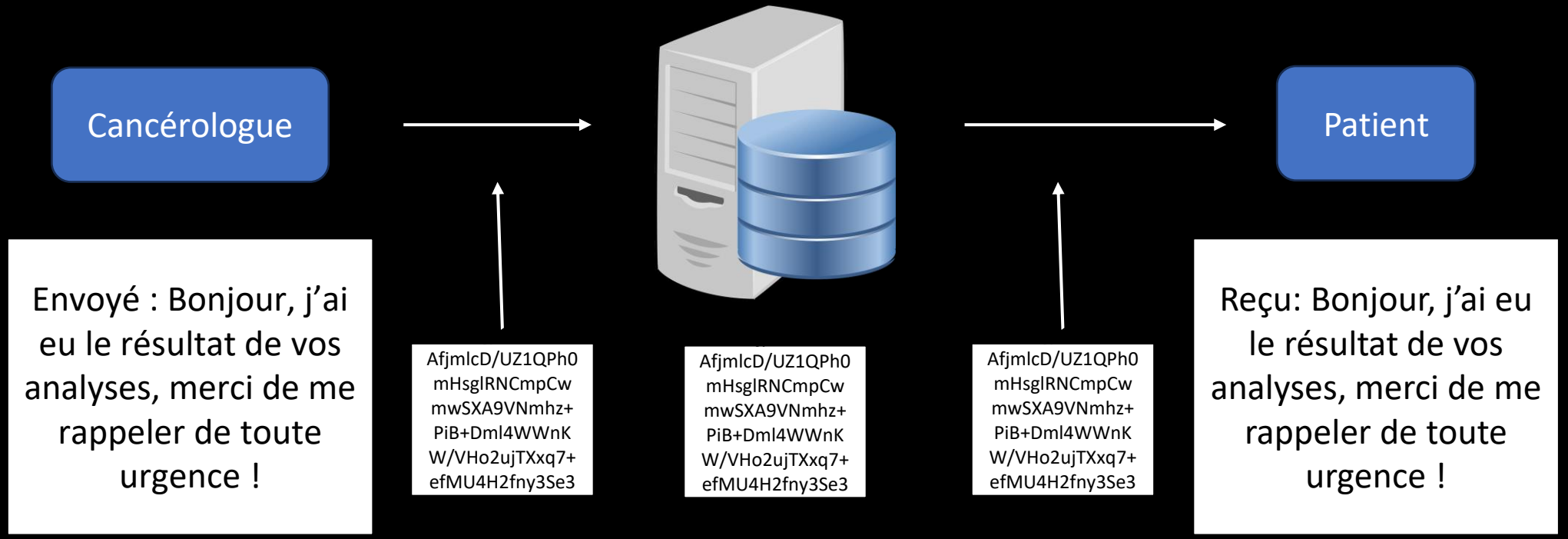
Messageries

- Chiffrement en transit



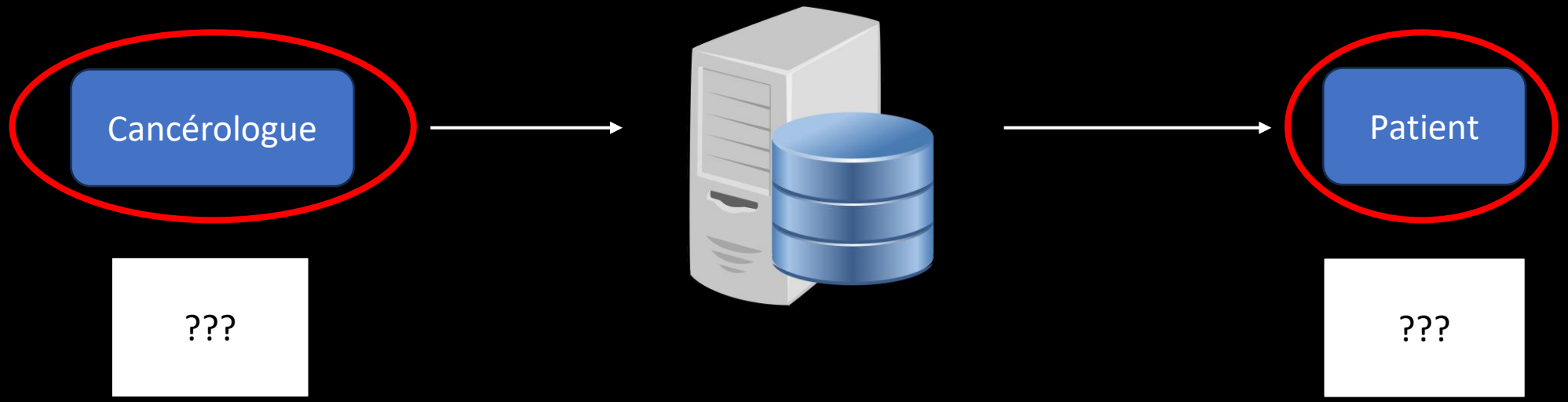
Messageries

- Chiffrement de bout en bout (« end-to-end » / E2EE)



Messageries

- Métadonnées

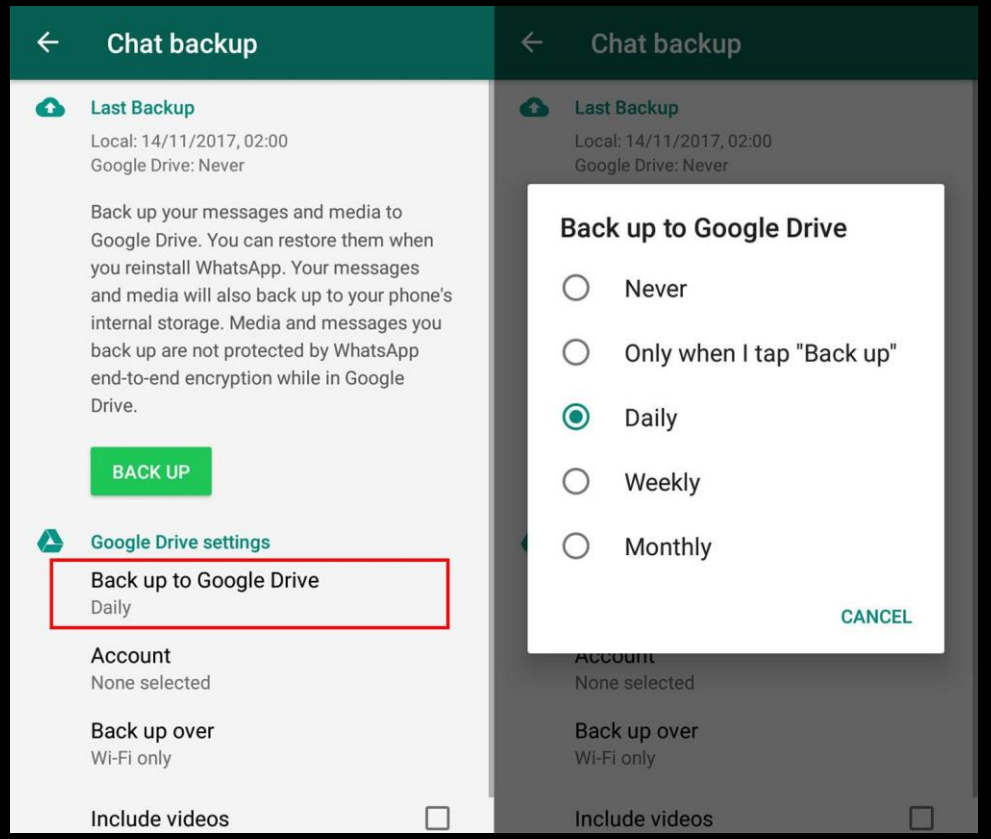


Telegram

- Fonctionnalités de groupe uniques
- Pas de chiffrement de bout en bout par défaut
- Données stockées en clair sur les serveurs de Telegram
- Pas de coopération avec les forces de l’ordre…
  - …jusqu’à septembre 2024
  - Termes de service mis à jour depuis l’arrestation de Pavel Durov

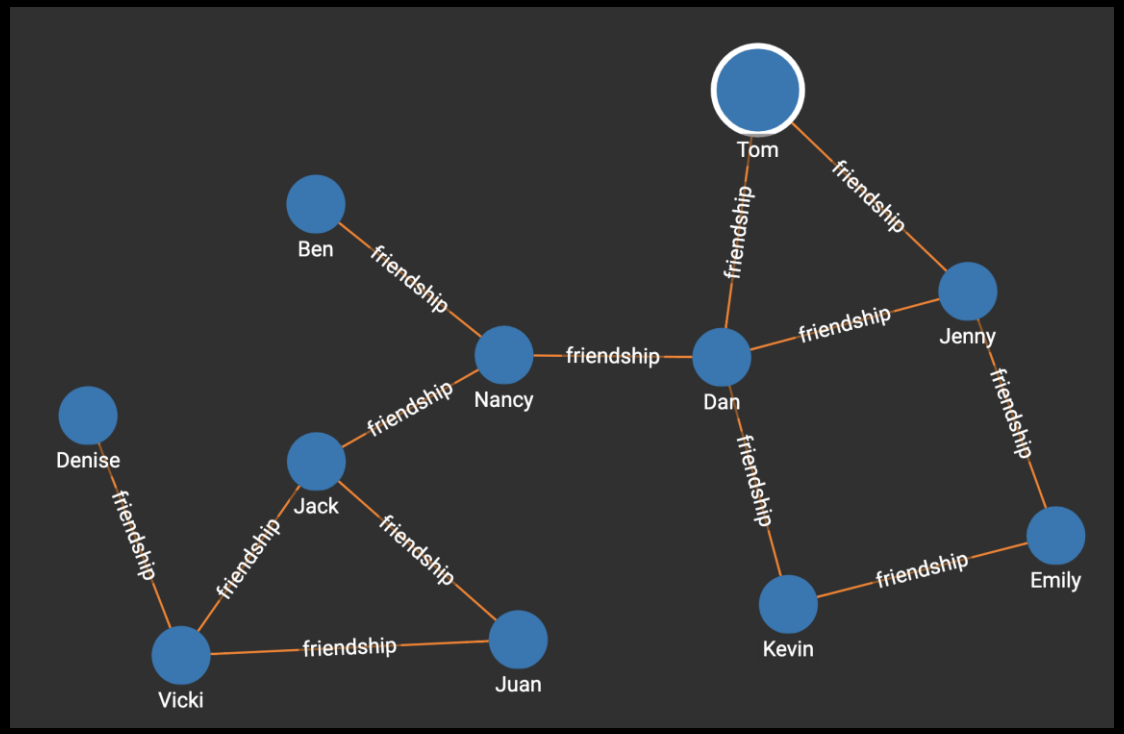
WhatsApp

- Chiffrement E2E par défaut
- Métadonnées collectées par Meta
  - Adresse IP
  - Carnet d’adresse
  - Expéditeur et destinataire
  - Date et heure des messages
  - Composition des groupes
  - « Analytics »
- Sauvegardes dans le cloud encouragées



Apparté : le graphe social

- Le carnet d’adresse est une source de données précieuse
  - Fonctionnalité « vous connaissez peut-être… »
- Peut être reconstitué en observant les communications
- La plupart des applications de messagerie collectent le carnet d’adresse entier
- Peu de solutions
  - Le mal est fait
  - Recoupement avec les carnets d’adresse du reste de la planète



Signal

- Chiffrement E2E par défaut
- Métadonnées chiffrées
- Pas d’informations collectées
- Récemment : ajout de contact par nom d’utilisateur
  - « Disparition » du carnet d’adresse
- Recommandation : activer la suppression automatique des messages (1-4 semaines)

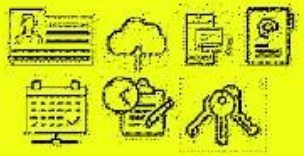
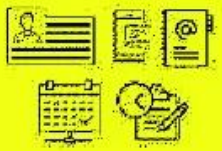
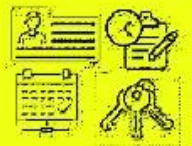
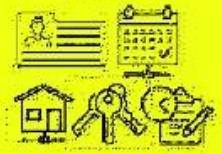
FEDERAL BUREAU OF INVESTIGATION

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 latent 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: Limited** • **Subpoena:** can render basic subscriber information • **18 U.S.C. §2709(d):** can render 25 days of iMessage lookups to and from a target number[1] • **Pen Register:** no capability* • **Search Warrant:** can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud	• **Message Content: Limited*** • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage *Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• **No Message Content** • Date and time a user registered • Last date of a user's connectivity to the service	• **No Message Content** • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram *may* disclose IP address and phone number to relevant authorities	• **No Message Content** • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• **No Message Content** • Provides account (i.e. phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number	• **No Message Content** • Accepts 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 retained for as long as the account is active	• **Message Content: Limited*** • **Subpoena:** can render basic subscriber records • **Court Order:** Subpoena return as well as information like blocked users • **Search Warrant:** Provides address book contacts and WhatsApp users who have the target in their address book contacts • **Pen Register:** Sent every 15 minutes, provides source and destination for each message *If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• **No Message Content** • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

 SUBSCRIBER DATA

 MESSAGE SENDER – RECEIVER DATA

 DEVICE BACKUP

 IP ADDRESS

 ENCRYPTION KEY(S)

 DATE/TIME INFORMATION

 REGISTRATION TIME DATA

 USER'S CONTACTS

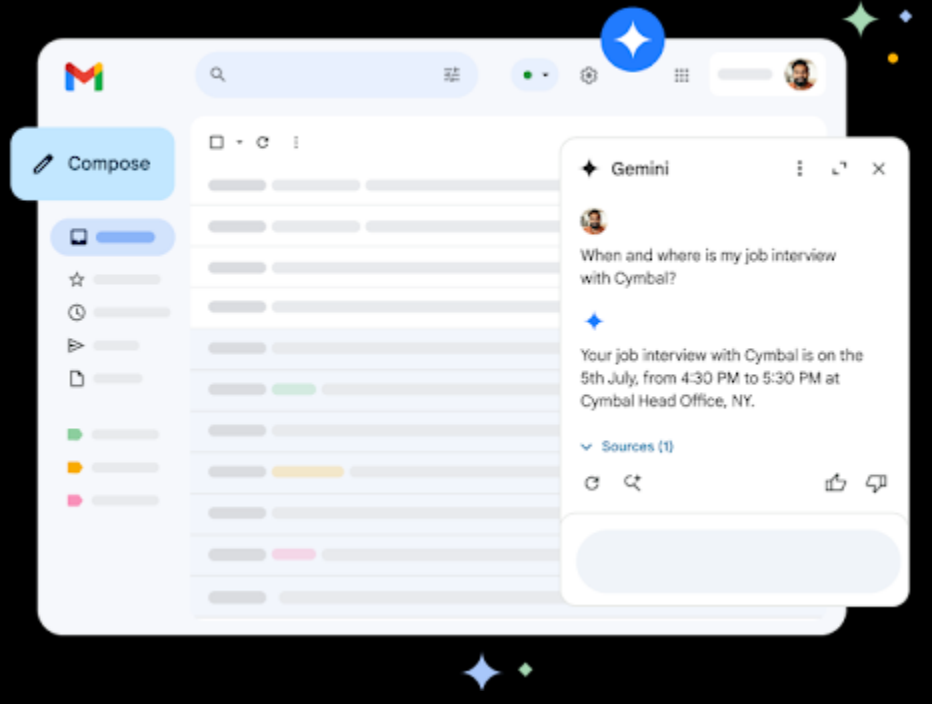
(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

[1] (U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry between parties does not indicate a conversation took place. These query logs have also contained errors.

Emails

- Essentiellement le même modèle de sécurité que Telegram
- Stockage en clair sur les serveurs du fournisseur
  - Google
  - Microsoft
- Collecte de métadonnées

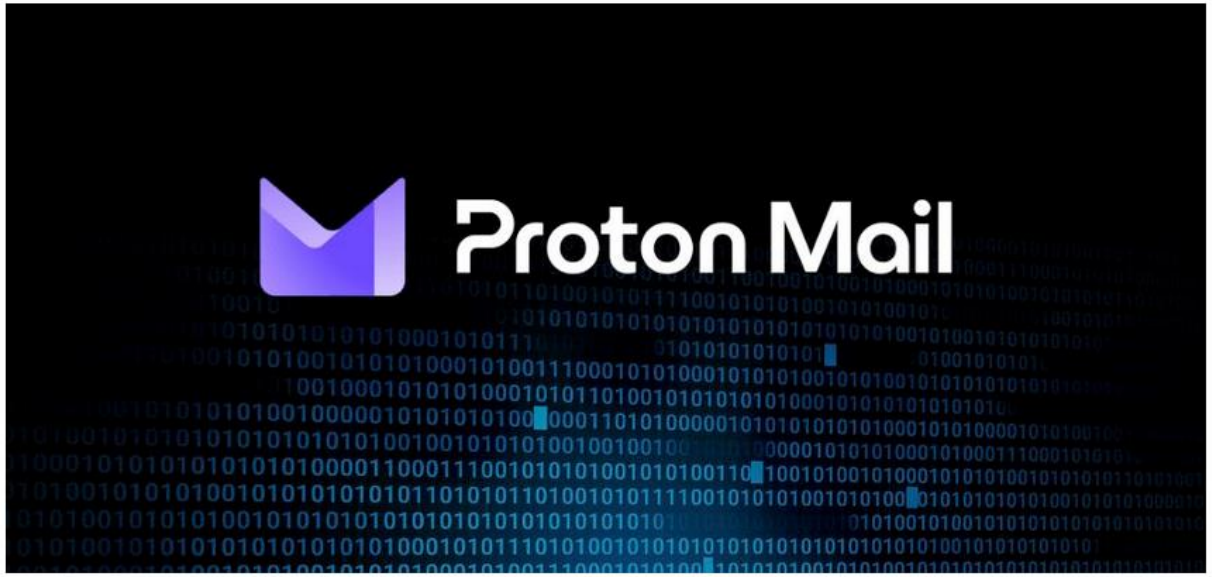


Proton Mail

- Chiffrement des mails sur le serveur
- ProtonMail Fournit malgré tout des métadonnées (ex : adresse IP) à la justice en cas de demande
- Moralité : idéalement, ne pas utiliser les e-mails pour les choses sérieuses
  - Ou alors RiseUp.net

Proton Mail Discloses User Data Leading to Arrest in Spain

May 6, 2024 *By* Alex Lekander — **41 Comments**



Update: Proton has confirmed the key details of this case and provided RestorePrivacy with a comment.

Proton Mail has come under scrutiny for its role in a legal request involving the Spanish authorities and a member of the Catalan independence organization, Democratic Tsunami.

Visioconférence

- Le chiffrement de bout en option payante…
  - Teams, Zoom
- …ou à activer manuellement
  - Jitsi, Skype, Google Meet
- Problématiques supplémentaires
  - Toujours des métadonnées
  - Risque de sauvegarde automatique de la conversation dans le cloud
  - Potentielle conservation de l’audio pour entraîner des IA de transcription

Visioconférence

- Solution simple : utiliser Signal
  - Appels groupés jusqu’à 50 participants
  - Probablement pas une conversation confidentielle si ce seuil est atteint
- Disponible de base avec Signal sur mobile
- Disponible sur ordinateur via Signal Desktop
  - Partage d’écran, etc.

Le cloud

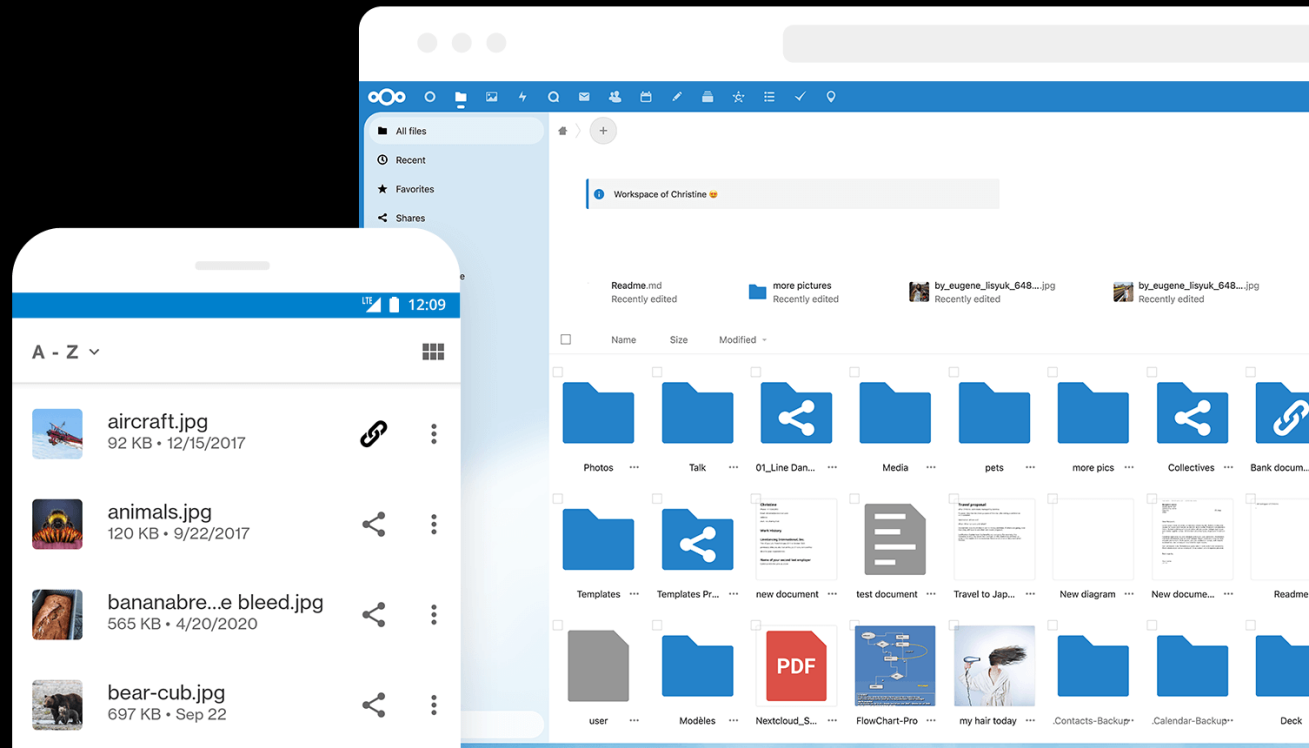
- Les données déposées sur Google Drive, Dropbox, etc. sont chiffrées en transit
- Le fournisseur a accès total aux données
- Il peut être contraint par les autorités de les divulguer

Le cloud

- Solution : chiffrer les données soi-même
  - GPG : état de l'art mais difficile d'utilisation
  - VeraCrypt : « conteneurs » chiffrés
- Problème : plus d'édition en ligne collaborative
- Mêmes outils pour protéger les fichiers sensibles sur un ordinateur local !
  - Chiffrement complet du disque dur recommandé

Le cloud

- Solution : stocker les données soi-même
  - Nécessite des ressources (serveurs)
  - Chiffrement pas nécessaire
- Logiciels open-source
  - NextCloud
- Les autorités doivent faire un raid pour récupérer les données



Où et comment stocker ses données

- Données stockées chez un tiers ❌
  - Pas de confidentialité
  - Usage probable pour entraîner des IA
- Données stockées chez un tiers mais chiffrées ✅
  - OK si le chiffrement est réalisé soi-même
  - Ne pas perdre les clés
- Données stockées chez soi ⚠️
  - Perdues en cas de perquisition
- Données stockées chez soi et chiffrées ✅ ✅

Comment les autorités travaillent (avant arrestation)

- Requêtes judiciaires
  - Demander les données au prestataire qui les possède
  - Nécessite la signature d'un juge
  - Solution : ne pas laisser ces données à un prestataire
- Mises sur écoute
  - « Interceptions de sécurité » (IS) centralisées par le GIC
  - ~10000 lignes écoutées en permanence
  - Solution : ne fonctionne pas sur les appels Signal/WhatsApp/Telegram
- IMSI catchers aux abords des manifestations

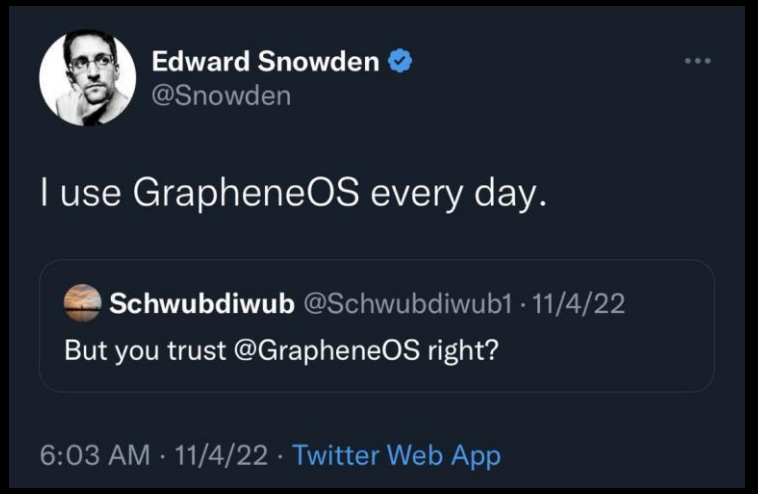
Techniques intrusives

- « Sonorisation »
  - Installation de micros, caméras, trackers GPS
  - Peu coûteux
  - Solution : ?

- Piratage
  - Exploitation de vulnérabilité pour pénétrer sur un ordinateur/smartphone
  - Très coûteux (outils à 10M€)
  - Solution : aucune
  - Contacter Amnesty International en cas de compromission suspectée

Techniques intrusives

- Pour les individus à haut risque
  - Mode « isolement » (*lockdown*) pour iPhone
  - GrapheneOS pour Android
- Sécurité de l’appareil renforcée au prix de l’expérience utilisateur
- Augmentent significativement le coût d’un piratage sans garantir une protection à 100%



Comment les autorités travaillent (après arrestation)

- Confiscation du téléphone
- Possibilité d'exiger le déverrouillage
  - Pour la police, demander est gratuit
  - Déverrouillage biométrique (empreinte digitale, face ID) trivial
- Possibilité d'accéder aux données sans le code avec des techniques intrusives
  - Long et coûteux
  - Beaucoup plus difficile si le téléphone est éteint

Le refus de communiquer le code de déverrouillage d'un téléphone portable peut constituer un délit

24/11/2022

Selon la Cour de cassation, le code de déverrouillage d'un téléphone mobile peut constituer une convention secrète de déchiffrement dont le refus de transmission aux autorités judiciaires constitue un délit au sens de l'article 434-15-2 du code pénal.

©BercyPhoto/Patrick Védrune

OPSEC

- Règle d’or : si quelque chose n’est pas assumable, le faire sans son téléphone
- Si un téléphone est indispensable, acheter un « burner » en liquide
  - Utilisation de pseudonymes
- Activités sensibles en ligne : TailsOS / TOR

Cas d’étude : que font les fachos ?

- Arrestation de membres de l’ultradroite en décembre 2022

- Utilisation de Telegram ❌
- Groupe manifestement infiltré par la police ❌
- Désinstallation de Telegram avant l’opération ✅
- Préparation de prétextes en cas d’arrestation ✅