



JOURNALISME
ET
SÉCURITÉ DE
L'INFORMATION 101



guillaume@binaryfactory.ca

@gepeto42

VULNERABILITES,
BRECHES ET FUITES



PROTEGER SES
COMMUNICATIONS

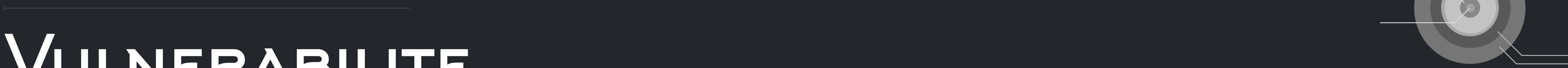


[HTTPS://EVIL.PLUMBING/HF2016/](https://evil.plumbing/hf2016/)

TYPES DE “PROBLEMES”

- **Vulnérabilité:** Heartbleed, MS08-067, ShellShock, etc.
- **Brèche:** Target, Wendy’s, Ashley Madison, etc.
- **Attaque de déni de service (DoS ou DDoS):** DIN, certaines attaques sur Sony.
- **Ransomware (Rancongiciel):** Hôpitaux, plusieurs entreprises, particuliers.





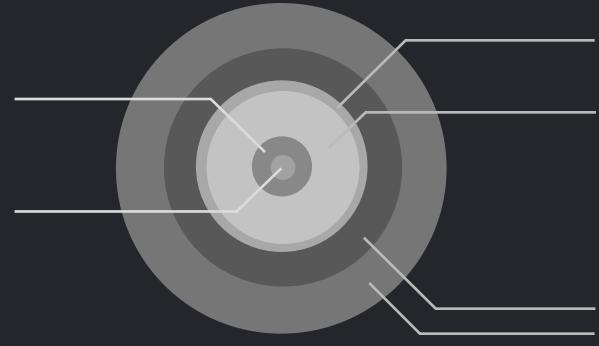
VULNERABILITE

Problème pouvant être exploité afin de gagner un accès non autorisé.

An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network. - MITRE

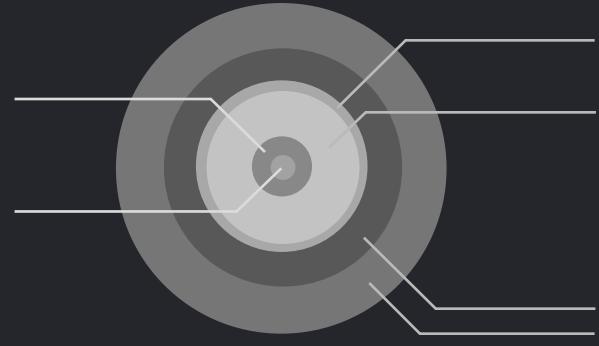
VULNERABILITE

Peut avoir un “nom” et du “marketing”
comme Heartbleed, ou pas.



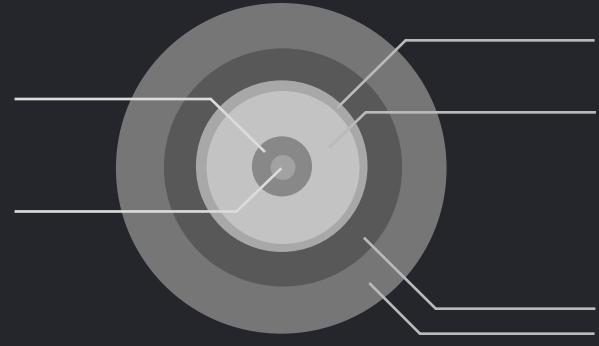
VULNERABILITÉ

Peut permettre l'exécution de code à distance - un type de vulnérabilité généralement critique (Remote Code Execution ou RCE).



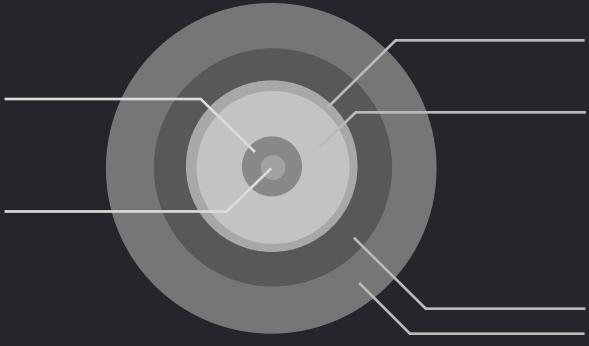
VULNERABILITE

Peut permettre l'obtention de privilèges plus puissants sur un système (Privilege Escalation).

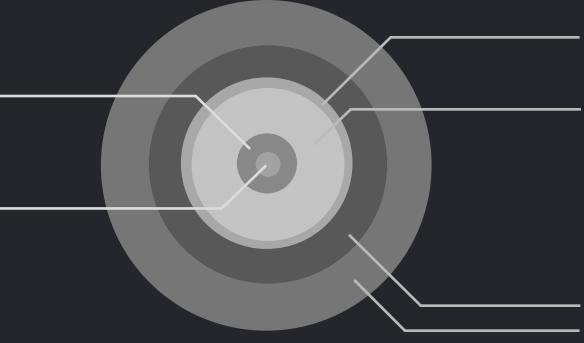


VULNERABILITE

Peut permettre de faire planter un système (Déni de Service / Denial of Service)



VULNERABILITE

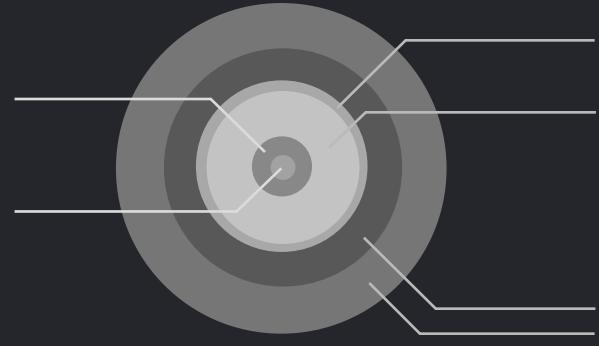


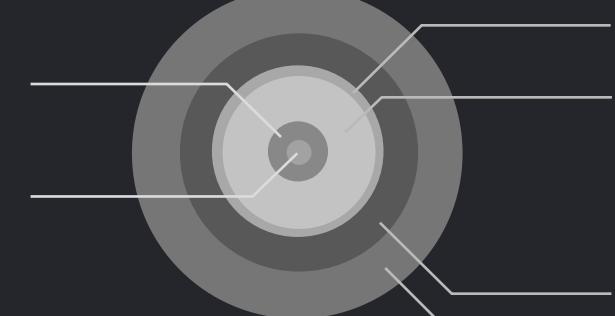
N'est pas un virus.

Exemple: Un système n'est pas **infecté**
par ShellShock mais bien **vulnérable**.

VULNERABILITE

Peut couler des données, qui peuvent ensuite être utilisées contre un système, comme Heartbleed.





VULNERABILITE – CRITIQUE OU PAS?

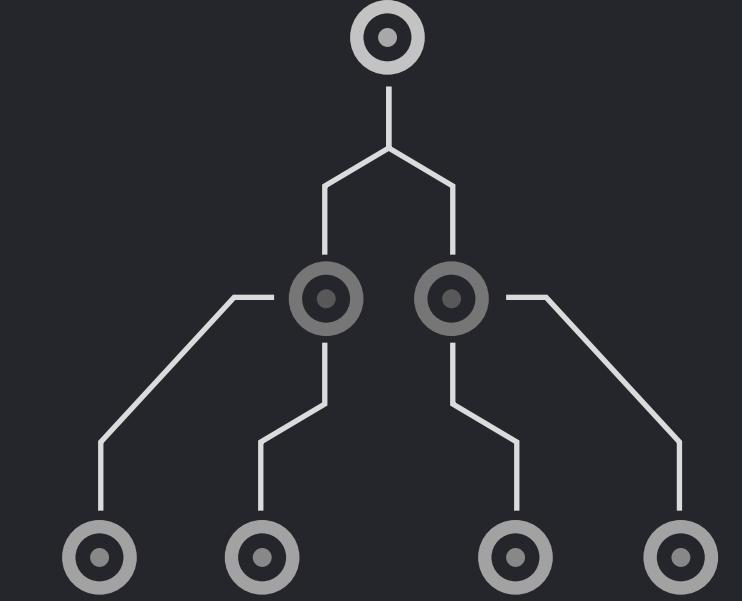
- Vulnérabilité dans un système populaire.
- Facile à exploiter contre les configurations standard.
- “Fiable”.
- Difficile à corriger.



VULNERABILITE – EXEMPLES

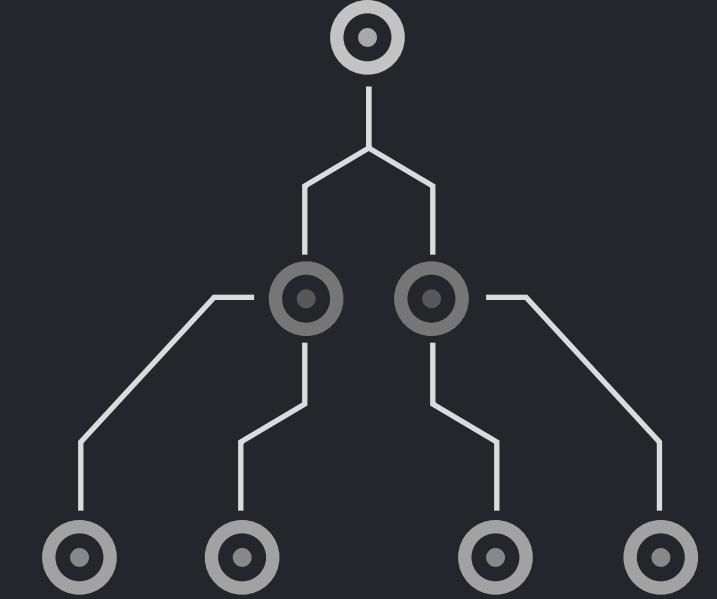
- **Heartbleed:** Très répandu, donne accès à beaucoup d'information, pouvait être corrigé mais demandait de l'effort.
- **CVE-2016-5086:** Bug dans une pompe à insuline, plus rare, très difficile à corriger, mais peut être exploité de façon “locale” seulement.

BRECHE



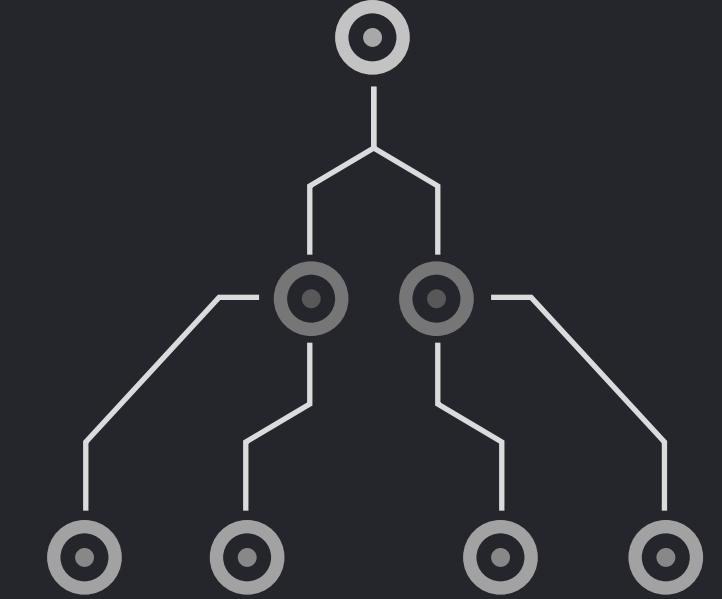
- Attaque sur un système ou une entreprise résultant en l'exfiltration de données, typiquement confidentielles.

BRECHE



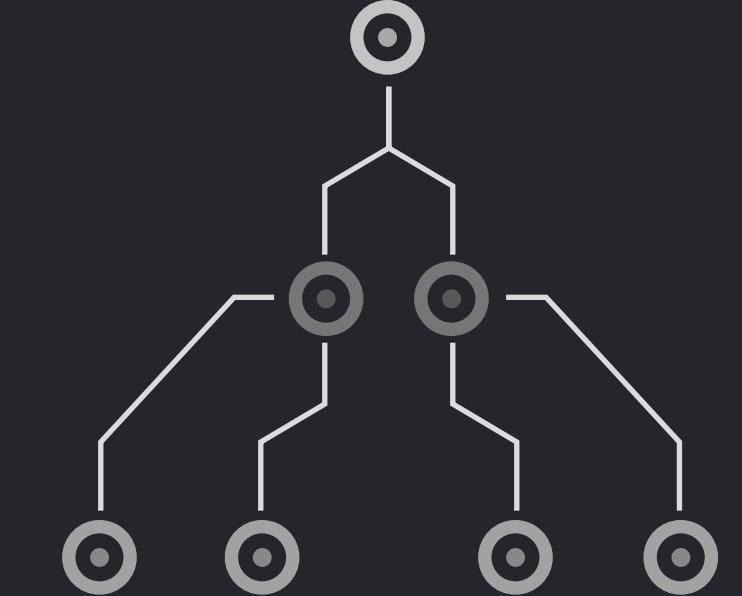
- Typiquement, peu de détails disponibles sur l'attaque.
- Les entreprises ont souvent elles-mêmes un manque d'information pour déterminer ce qui a été volé.
- Souvent détectées des mois trop tard.
- Les informations sont utilisées par la suite dans un but typiquement criminel: Fraude, extortions, avantage compétitif, etc.

BRECHE – ATTAQUES AVANCEES



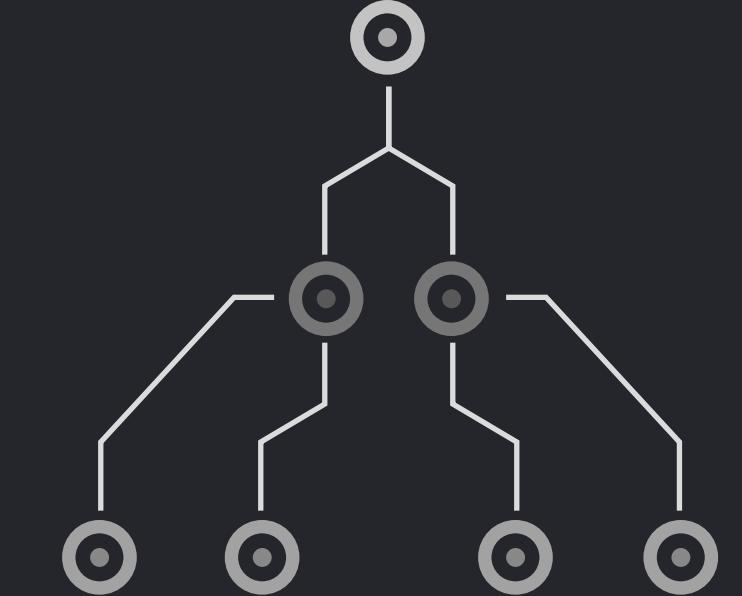
- Une attaque dite “avancée” est souvent simple, et plutôt “juste assez avancée”.
- Une majorité de brèches sont causées par des problèmes simples pour lesquels des solutions sont connues.
- Les termes comme “chiffrement de type bancaire/niveau militaire” ne veulent **rien** dire d’utile.

BRECHE – ATTAQUE COMMUNE



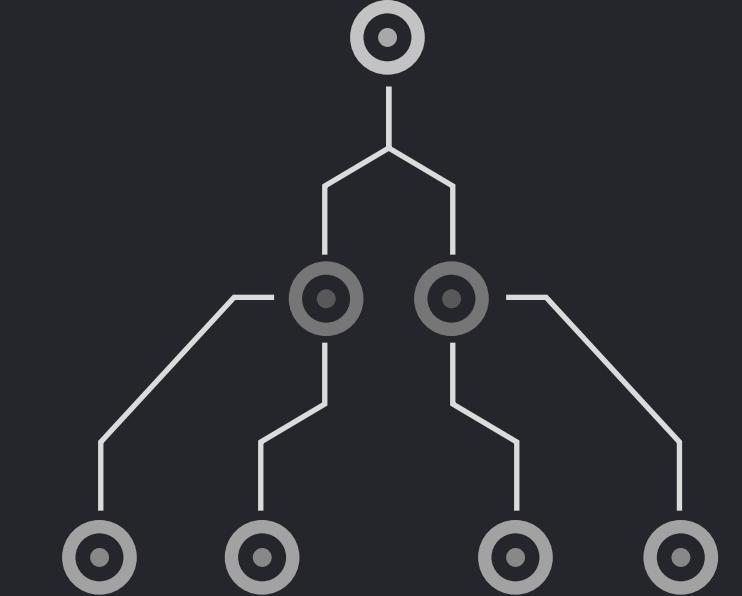
- Courriel envoyé, avec un lien ou pièce attachée.
- Un logiciel de control à distance est installé et/ou un mot de passe est volé.
- Une fois l'accès au poste établi, on tente de se connecter à d'autres systèmes internes afin de voler l'information désirée.

BRECHE – ATTAQUE COMMUNE #2

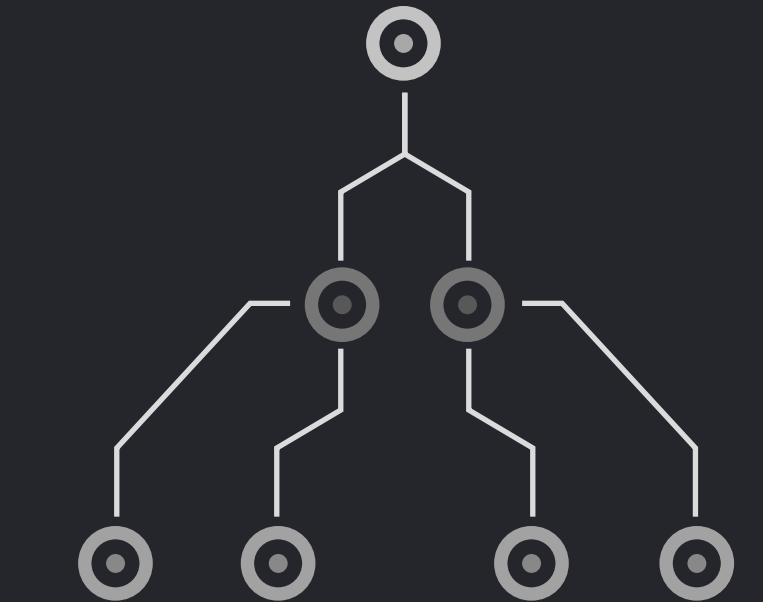


- Vulnérabilité de type “injection SQL” sur une application web.
- Toute la base de données est téléchargée.
- Ceci n'est vraiment pas “avancé”, totalement prévisible et facile à corriger, mais encore fréquent.

BRECHE – ATTAQUE COMMUNE #2



- Vulnérabilité de type “injection SQL” sur une application web.
- Toute la base de données est téléchargée.
- Ceci n'est vraiment pas “avancé”, totalement prévisible et facile à corriger, mais encore fréquent.



the grugq
@thegrugq

Follow

New rule: if you are hacked via OWASP Top 10,
you're not allowed to call it "advanced" or
"sophisticated."

RETWEETS

1,412

LIKES

1,118

5:58 AM - 27 Oct 2015

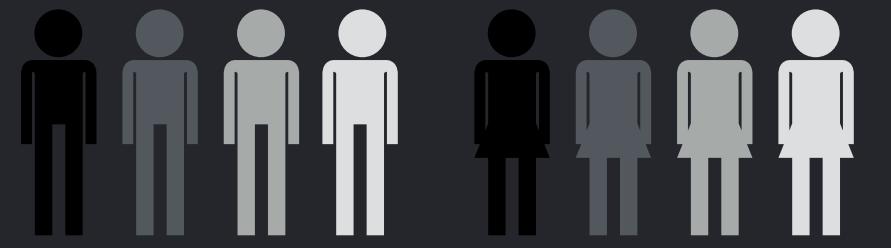
1.4K

1.1K

...

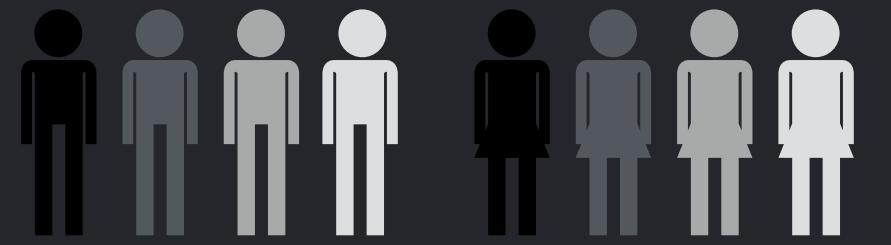


Bob McEXPERTFACE



GRANDS SOUS-DOMAINES

- Sécurité de l'information en entreprise. Défense, blue-team. - Je me retrouve dans cette catégorie 90% du temps.
- Sécurité offensive. Testeurs d'intrusions/penetration testers, red-team, recherche de vulnérabilité.
- Réponse aux incidents.
- Chercheurs.
- Autres Spécialistes (Crypto, analyse de menaces, données,



HACKFEST 2016 – VENDREDI

9h00

Sylvain Desharnais Nadia Vigneault - **Stratégies de fouille et recherches de preuves (Français)**

13h30

Speed talks:

- 1) Sunny Wear - **Exploit Kits: The Biggest Threat You Know Nothing About**
- 2) Geoffrey Vaughan - **Catching IMSI Catchers**

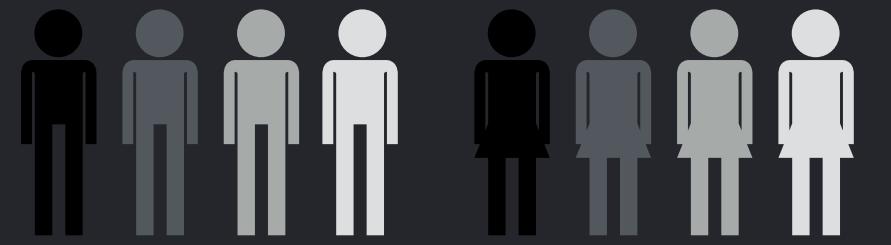
14h30

Bernard Bolduc - **Histoire d'un hack (Français)**

19h00 (Workshop)

Room “Bethoween”:

Workshop : **Techniques d'informatique forensique (Français, laptop needed)**



HACKFEST 2016 – SAMEDI

10h00

Wayne Huang - **Unveiling One of the World's Biggest and Oldest Cybercrime Gangs—Asprox**

11h00

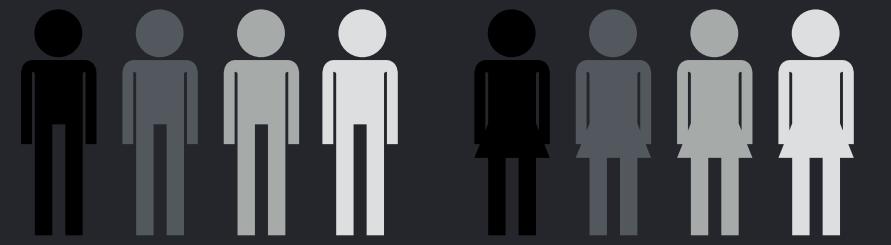
Stephanie Carruthers - **This Phish Goes To 11**

15h30

Sarah Jamie Lewis - **Untangling the Dark Web: Unmasking Onion Services**

16h30

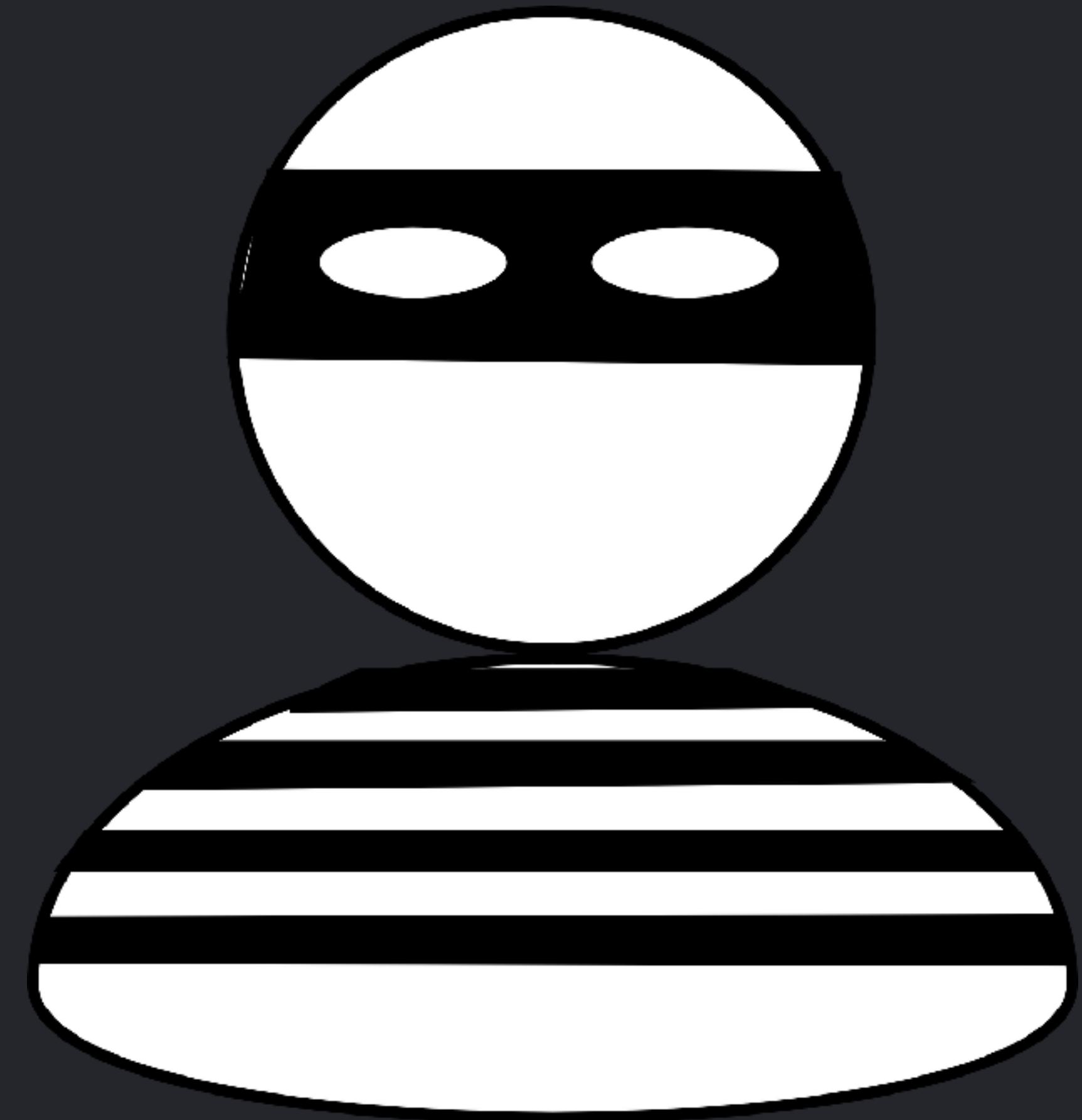
Mathieu Lavoie & David Décaray-Hétu - **De-anonymizing Bitcoin one transaction at a time**



IDENTIFIER LES BONS EXPERTS

- Présence sur les réseaux sociaux ou dans les conférences comme Hackfest.
- Publie un blog, des vulnérabilités, des présentations ou des outils open-source.
- Sait mettre les risques en perspective.

NE PORTENT PAS TOUJOURS UN MASQUE DE SKI

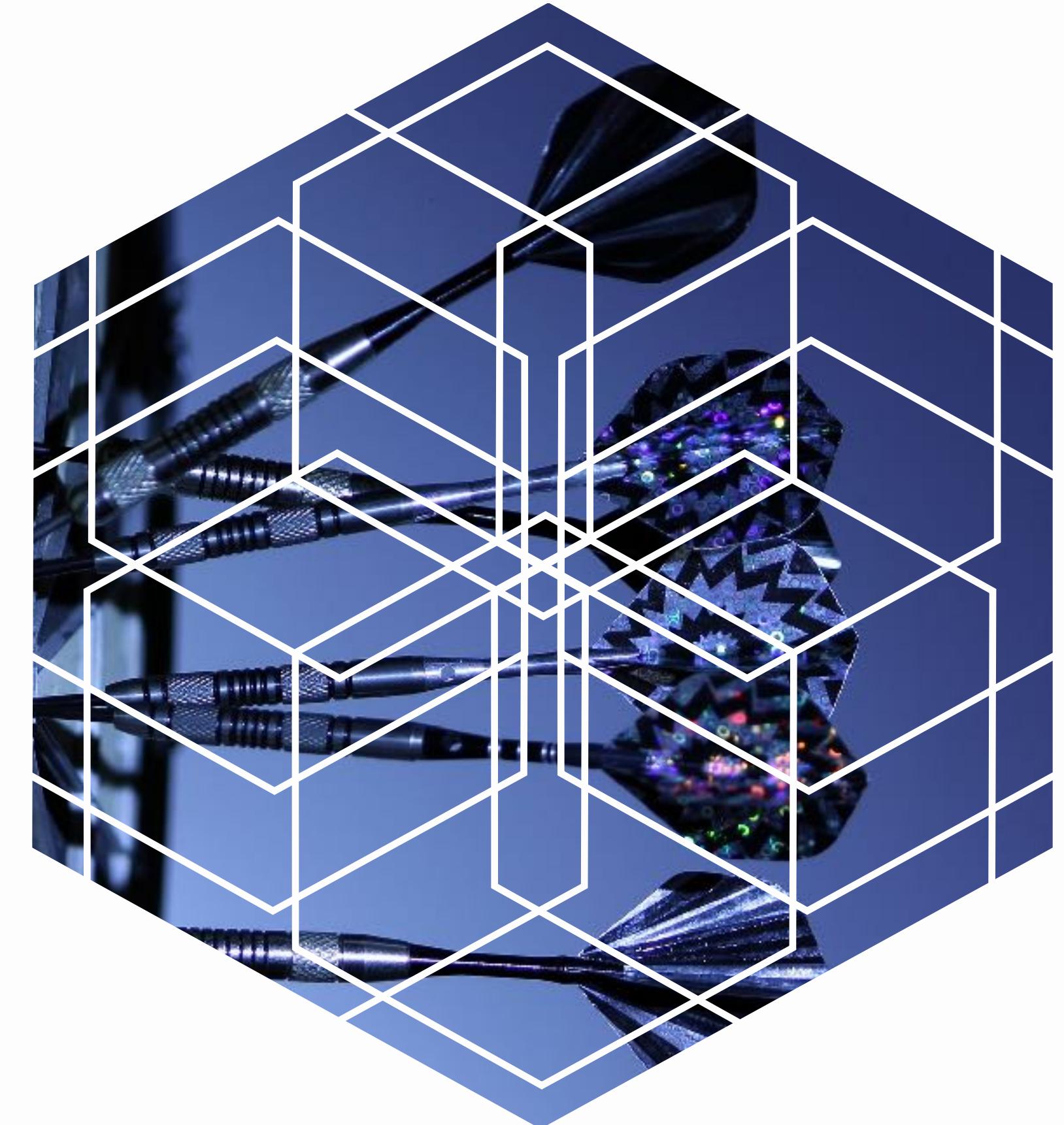


... SAUF L'HIVER

Et... ATTENTION!

MODEL DE MENACE (THREAT MODEL): ATTAQUE REALISTE?

- **Entreprise:** Compétiteurs, groupes criminels, “hacktivists”, puissances étrangères (R&D surtout)
- **Activiste:** Gouvernements
- **Particulier:** Attaques opportunistes, sans victime préterminée. Groupes criminels pour fraude d'identité, système de tracking pour publicité, etc.
- **Aucun modèle n'est parfait** mais ils sont utiles.



MODELE DE MENACE

- Comprendre contre quoi se défendre.
- Comprendre qui a le potentiel d'attaquer nos systèmes et notre information.
- Établir des méthodes pour s'en protéger.

EXEMPLE #1

- Un citoyen comme les autres. Il achète en ligne, participe sur les réseaux sociaux de façon non-politisée, n'a pas d'ennemi connu.
- Il voyage parfois, utilise Internet sans-fil à la maison, dans des cafés, et possède un téléphone cellulaire intelligent.

EXEMPLE #1

- Cible pour attaques opportunistes.
 - Faire attention aux sites utilisés.
 - Garder ses équipements et systèmes à jour.
 - Attention aux courriels douteux.
 - Utiliser un gestionnaire de mots-de-passe et l'authentification à deux facteurs.
 - Utiliser un VPN lors de l'utilisation d'un Wi-Fi non sécurisé.
 - Garder des copies de sauvegarde de ses données.

EXEMPLE #2

- Activiste dans un pays dirigé par un dictateur.
- Utilise Internet fréquemment, pour organiser des événements, contacter des journalistes ainsi que d'autres activistes.
- Possède un ordinateur portatif, un iPhone et plusieurs comptes en ligne utilisés à cet effet.

EXEMPLE #2

- Vulnérable aux attaques opportunistes. Toutes les protections de l'exemple #1 s'appliquent.
- Pourrait être ciblé par des agences aillant accès aux données des fournisseurs d'accès et de cloud.
 - Données chiffrées et locales.
 - Utilisation de VPN et de Tor substantielle.
- Pourrait être victime d'attaques informatiques avancées.
 - Compartimentation des périphériques complète.
- Ces exemples sont évidemment **non exhaustifs** mais démontrent que la personne faisant face à ce type d'attaque ne peut se fier uniquement à la technologie.

EXEMPLE #3

- Entreprise stockant les informations confidentielles de centaines de milliers de clients.
- Ces informations sont si critiques qu'elles peuvent être utilisées dans des campagnes d'extortion contre leurs clients.

MODELISER L'ACCES AU WEB & COURRIEL À PARTIR D'UN CAFE

- Recherche sur Google (HTTPS).
- Utilisation du site web de CNN.
- Utilisation de Gmail
- Envoi d'un courriel



QUI A ACCÈS ET À QUOI?

- Recherche sur Google (HTTPS) -
 - Le café, le fournisseur d'accès et de service DNS savent que vous avez utilisé Google.
 - N'importe qui d'autre près du Wi-Fi peut aussi le savoir.
 - Google connaît votre requête et peut probablement l'associer à votre identité



QUI A ACCÈS ET À QUOI?

- Utilisation du site web de CNN.
 - Comme Google, sauf que le contenu est aussi facilement visible par ces mêmes entités.
 - Des douzaines de tierces parties: Facebook, Clicktale, Chartbeat, Outbrain, Optimizely, etc.
 - Chaque entité peut être utilisée pour insérer des logiciels malveillant tentant d'exploiter votre navigateur.
 - Chaque entité possède assez d'information pour probablement vous identifier uniquement.



QUI A ACCÈS ET À QUOI?

- Courriel par Gmail
 - Google a accès au contenu du courriel envoyé, ainsi qu'aux métadonnées, donc n'importe quel mandat pouvant donner accès à ces données pourrait fonctionner.
 - Les courriels peuvent facilement contenir des “mouchards”.
 - Le serveur de destination et l'entreprise qui le gère.
 - Si le poste de travail du destinataire est compromis, il peut aussi contenir cette information.
 - Les métadonnées permettent de savoir qui se parle, à quel moment, à quel sujet, d'où, et ce, même si le contenu est **chiffré**.



QUI A ACCÈS ET À QUOI?



- Courriel entrant
 - N'importe quel image dans un courriel peut être téléchargée directement d'un serveur, pour savoir si vous avez ouvert le message et quelle est votre adresse IP.

 Mail thinks this message is Junk Mail. Load Remote Content

COACH Outlet 
EXTRA 60% off starting tomorrow
To: Guillaume Ross

 Junk - Gmail Yesterday at

Delete Reply Forward Next

ALORS ON
FAIT QUOI?

EXPLOITONS LE MODELE
DES ATTAQUES



August 25, 2016

Sophisticated, persistent mobile attack against high-value targets on iOS

By Lookout and Citizen Lab [7 Comments](#)



AHMED MANSOOR

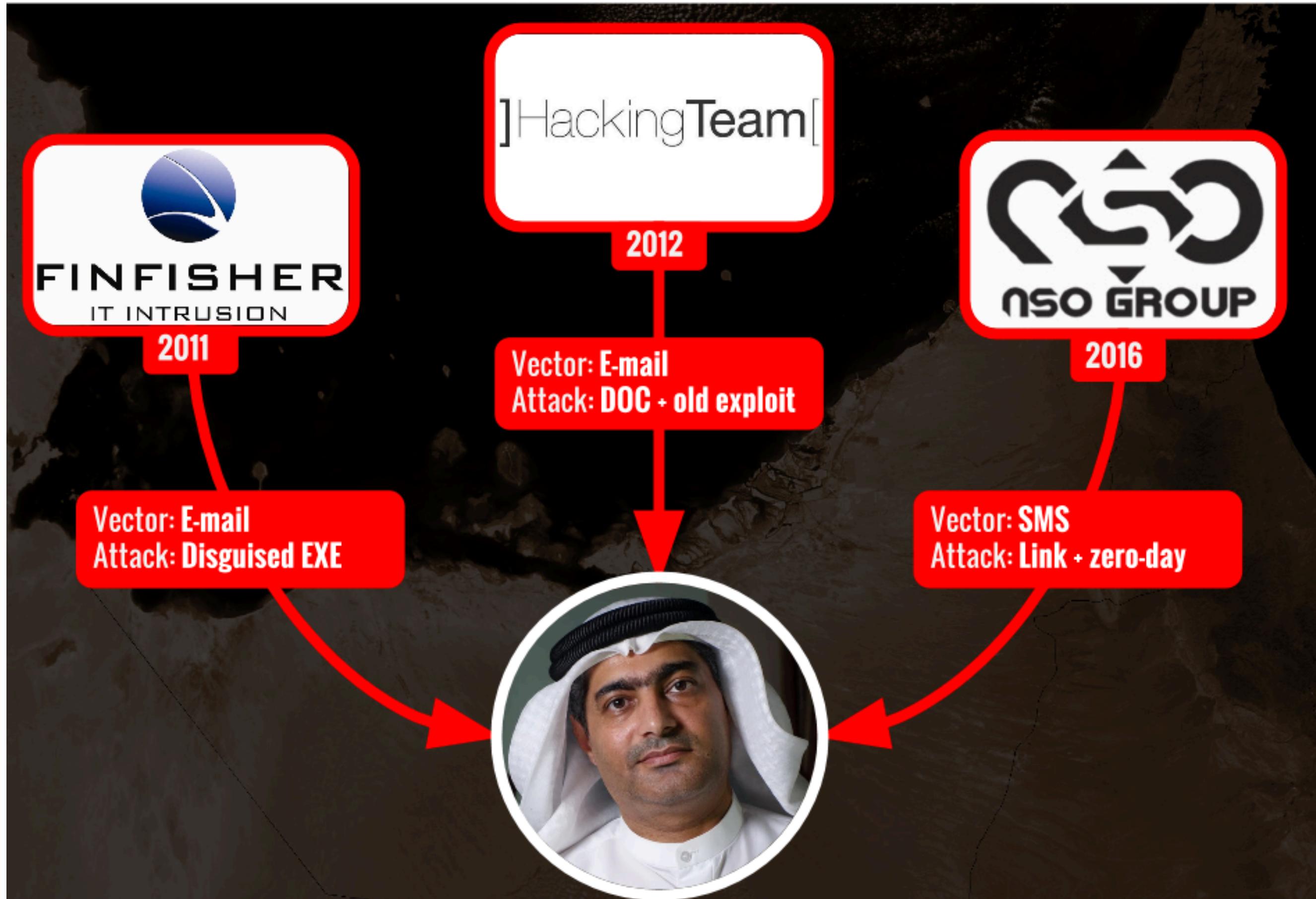
ACTIVISTE AUX ÉMIRATS ARABES

The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

August 24, 2016

Tagged: [NSO Group](#), [UAE](#)

THREE “LAWFUL INTERCEPT” PRODUCTS USED AGAINST MANSOOR

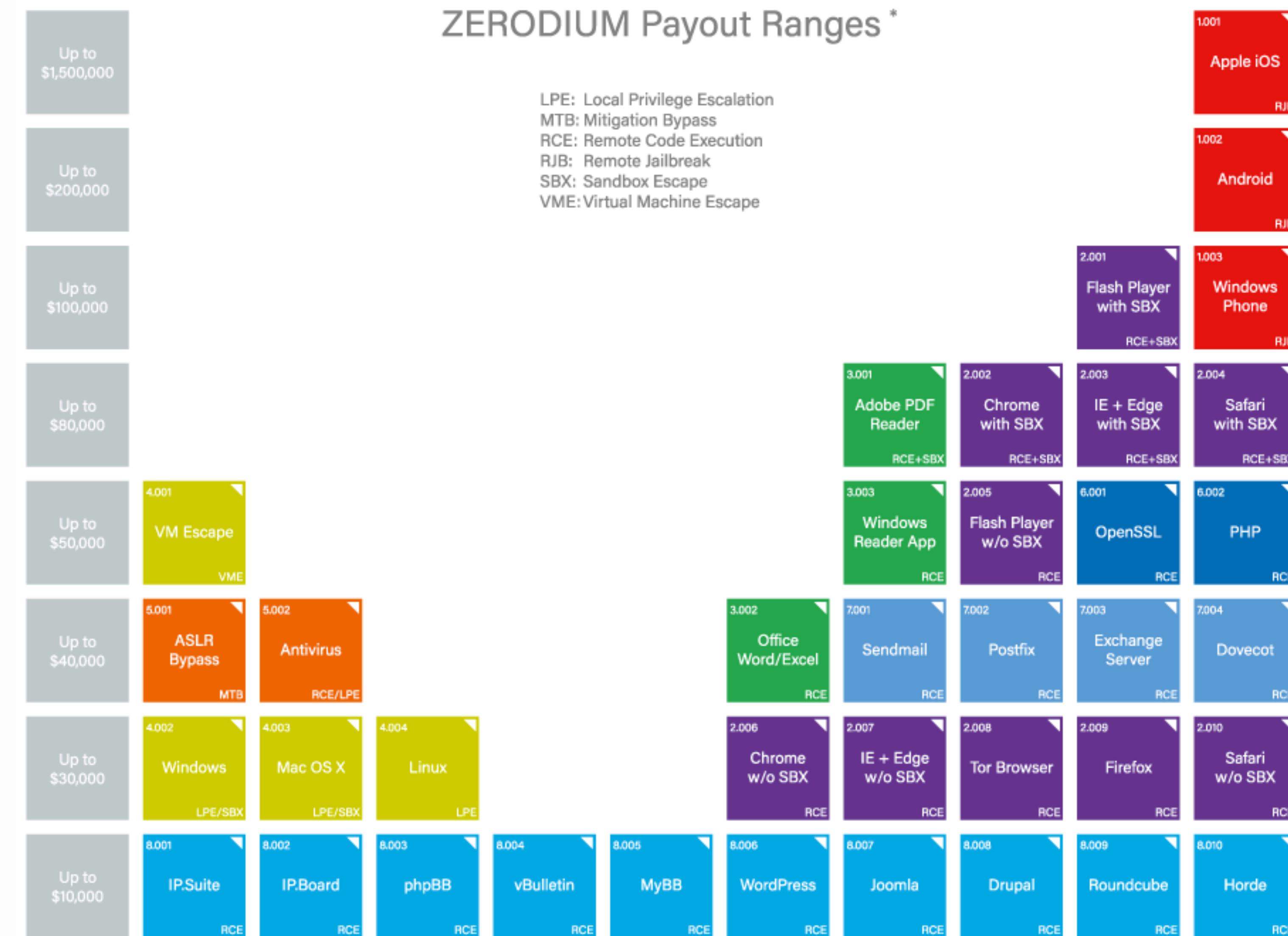


*From: Marczak & Scott-Railton
The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*

CITIZEN LAB 2016

ZERODIUM Payout Ranges

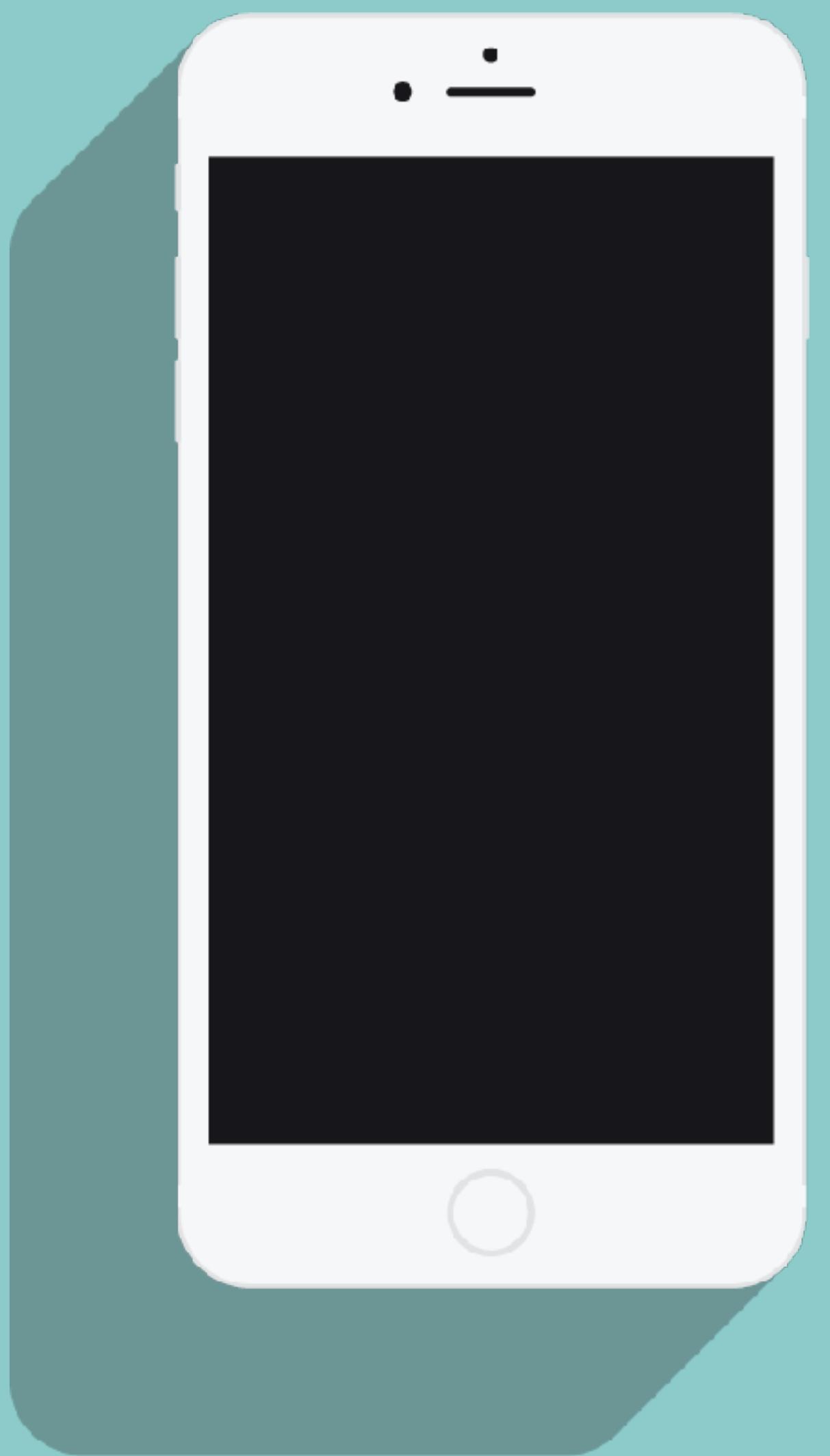
LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escalation



** All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*

2016/09 © zerodium.com

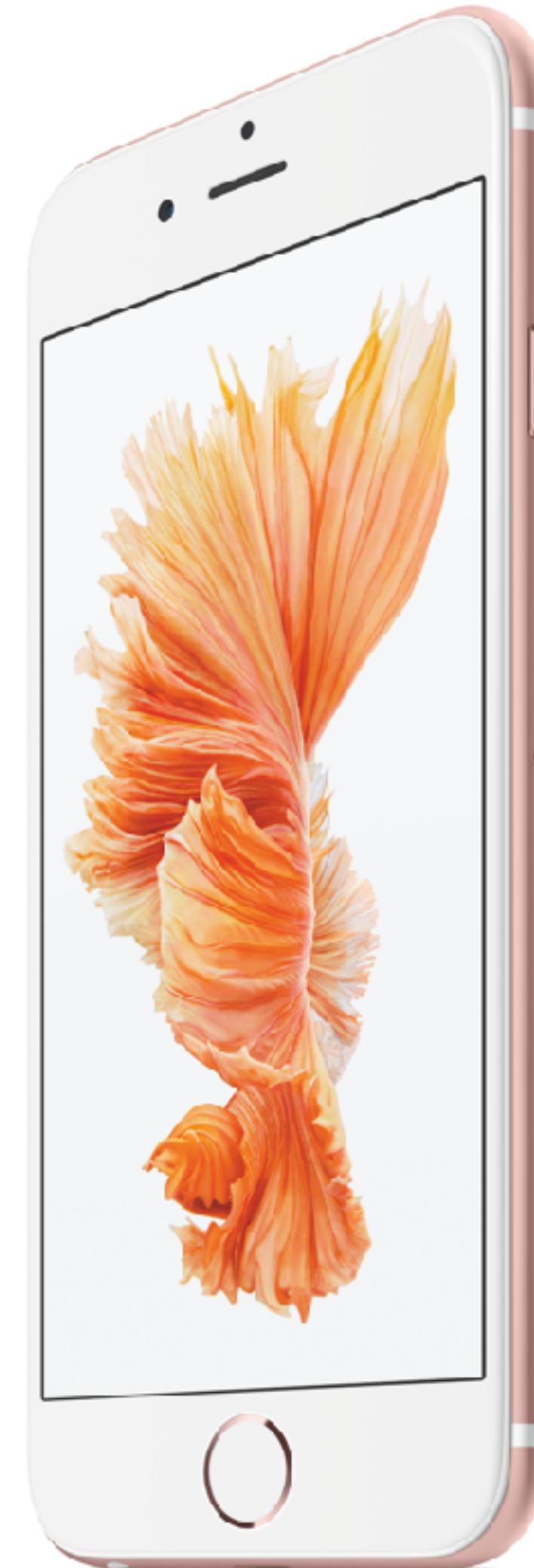
[H T T P S : / / W W W . Z E R O D I U M . C O M / P R O G R A M . H T M L](https://www.zerodium.com/program.html)



REGLE 1

ISOLATION /

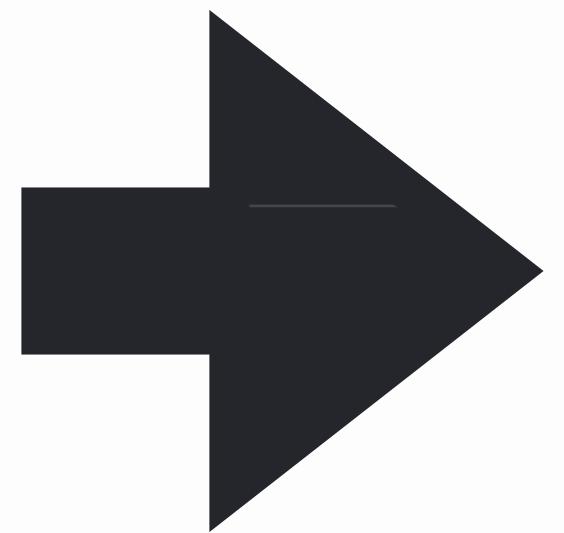
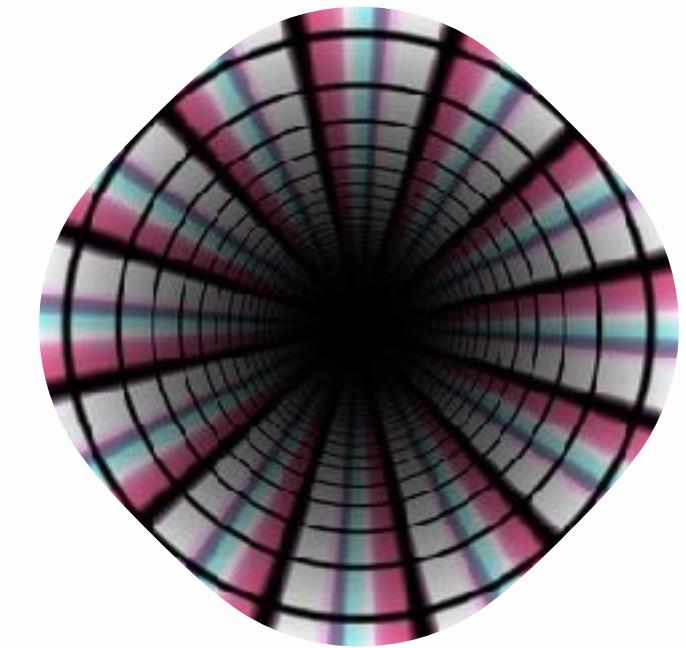
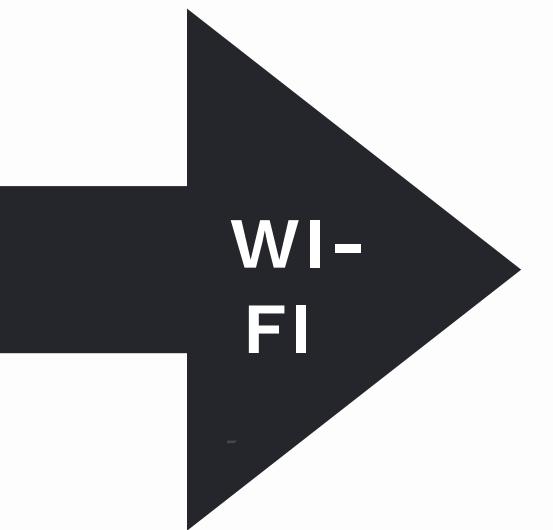
COMPARTIMENTATION
DES SYSTEMES



AUCUNE TECHNOLOGIE N'EST PARFAITEMENT
SECURITAIRE

ASSUMEZ QUE CHAQUE PARTIE DE
L'EQUATION PEUT ETRE BRISEE

WEB



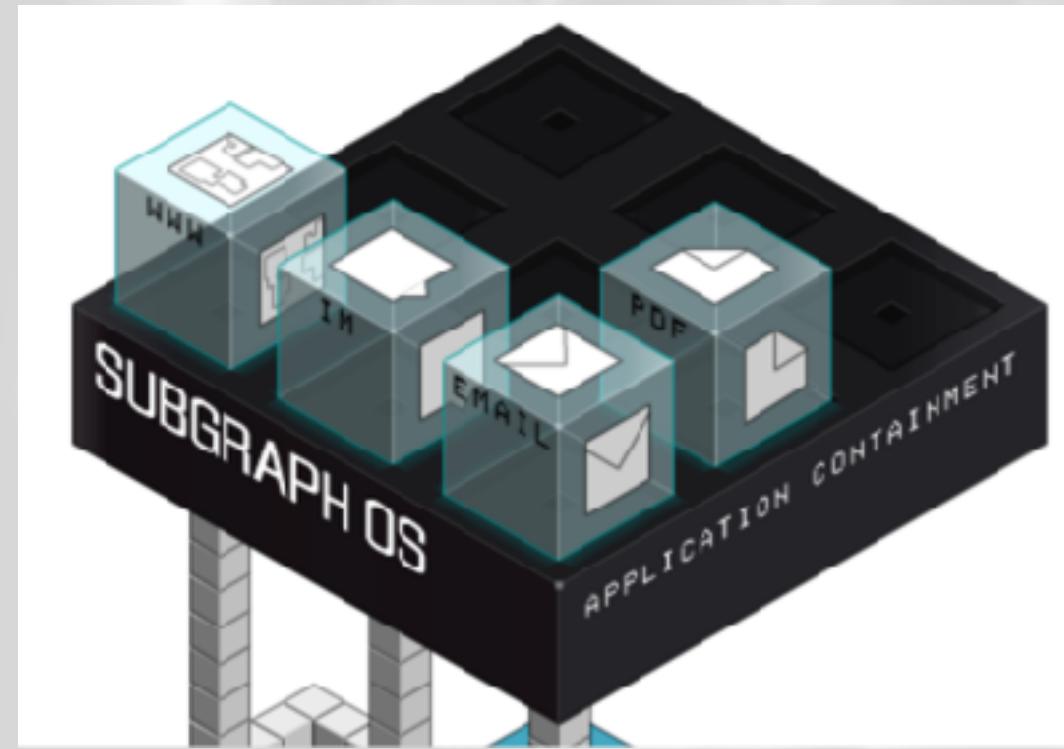
POSTE DÉDIÉ

VPN

TOR

DEMO

DISTRIBUTIONS SPECIALISEES



[HTTPS://SUBGRAPH.COM](https://subgraph.com)

ALPHA
FAIT A MONTREAL!

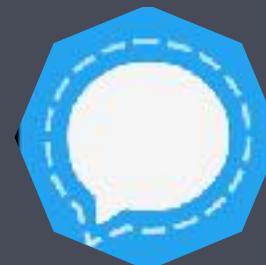
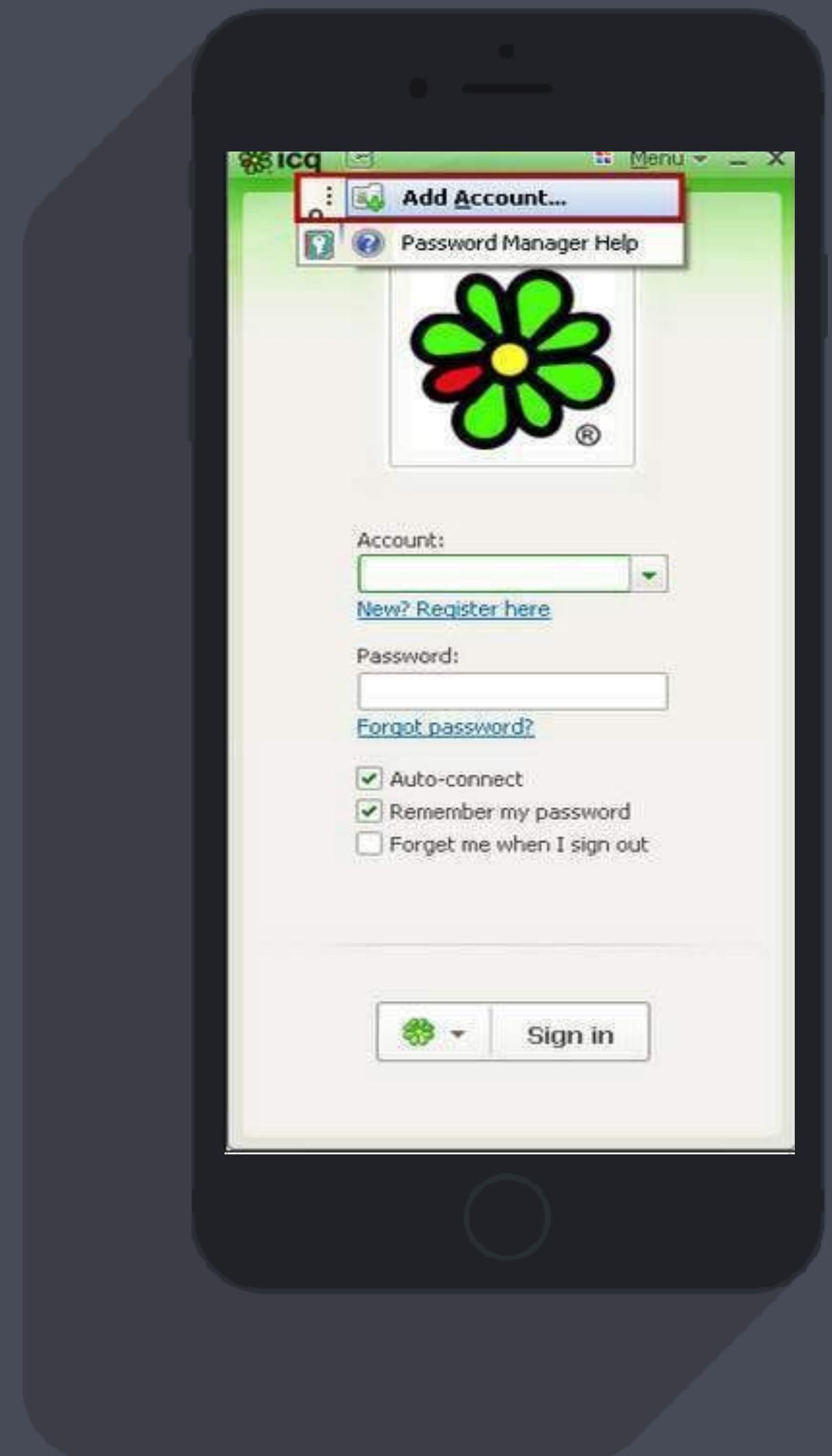


[HTTPS://TAILS.BOUM.ORG](https://tails.boum.org)



[HTTPS://WWW.QUBES-OS.ORG](https://www.qubes-os.org)

MESSAGERIE ET VOIX



SIGNAL

CHIFFRÉ DE BOUT-EN-BOUT (END-TO-END)



ATTENTION AU
MÉTADONNÉES ET
SAUVEGARDES

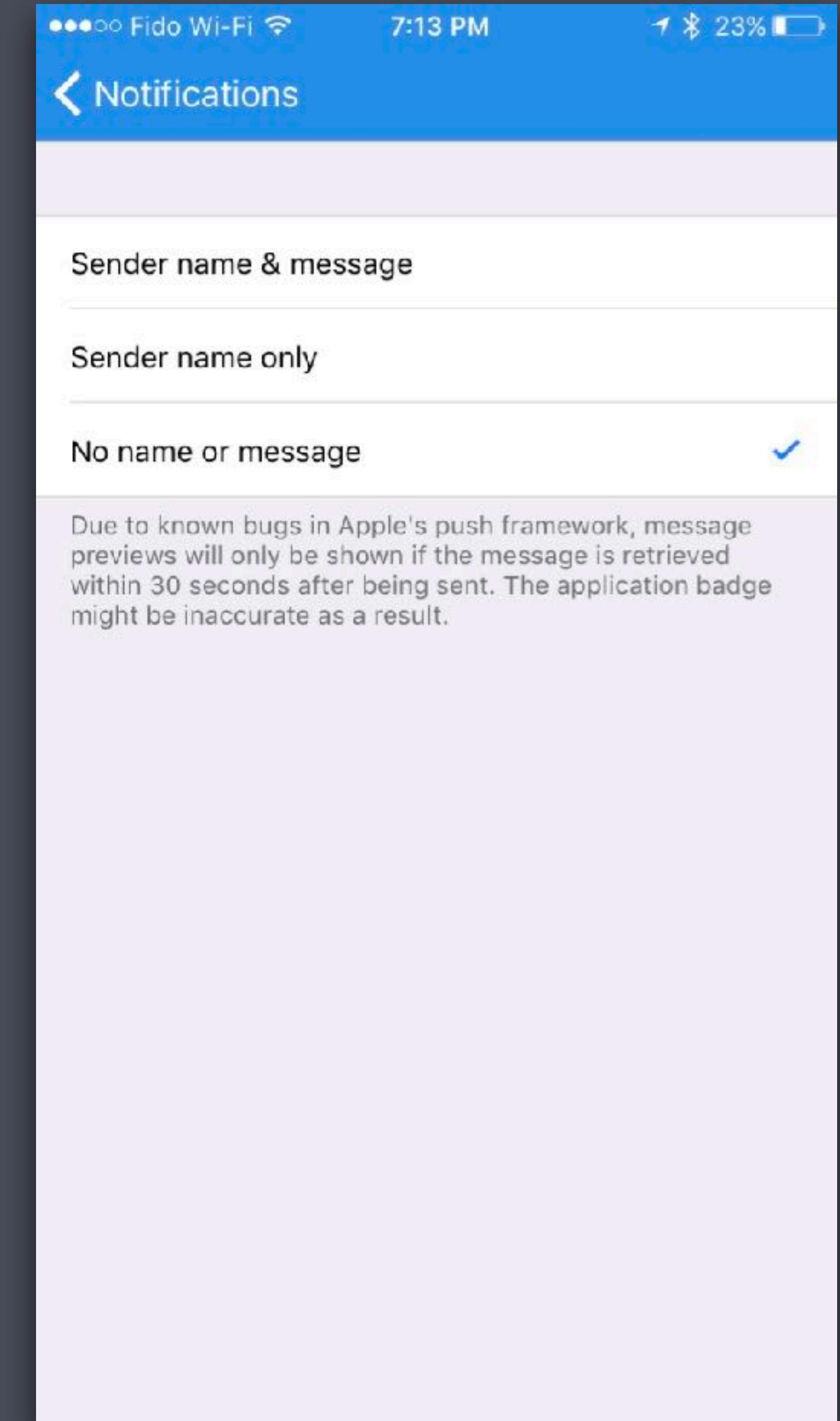
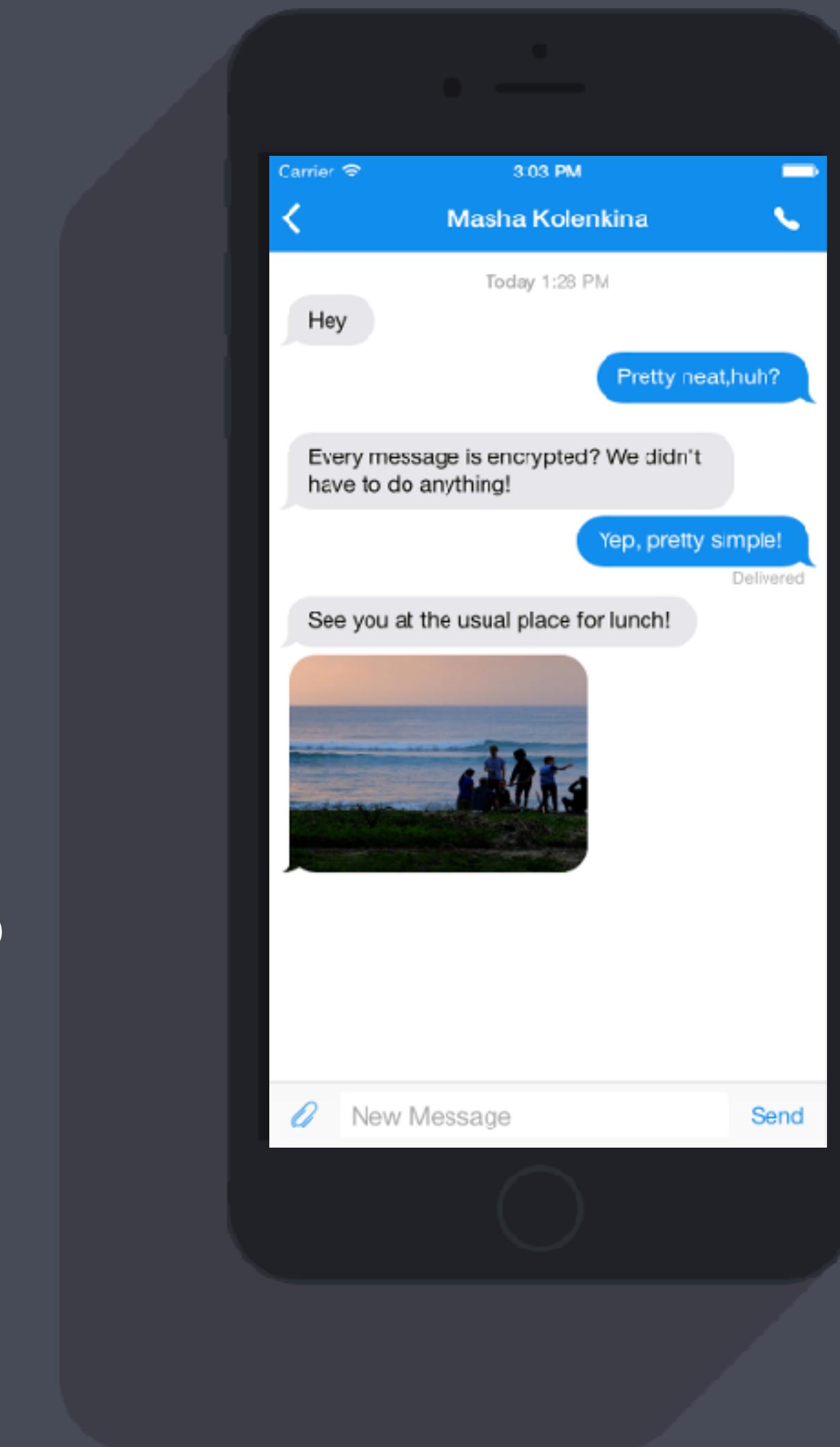
VERIFIER
L'INTERLOCUTEUR

UTILISER UN
NUMERO “JETABLE”

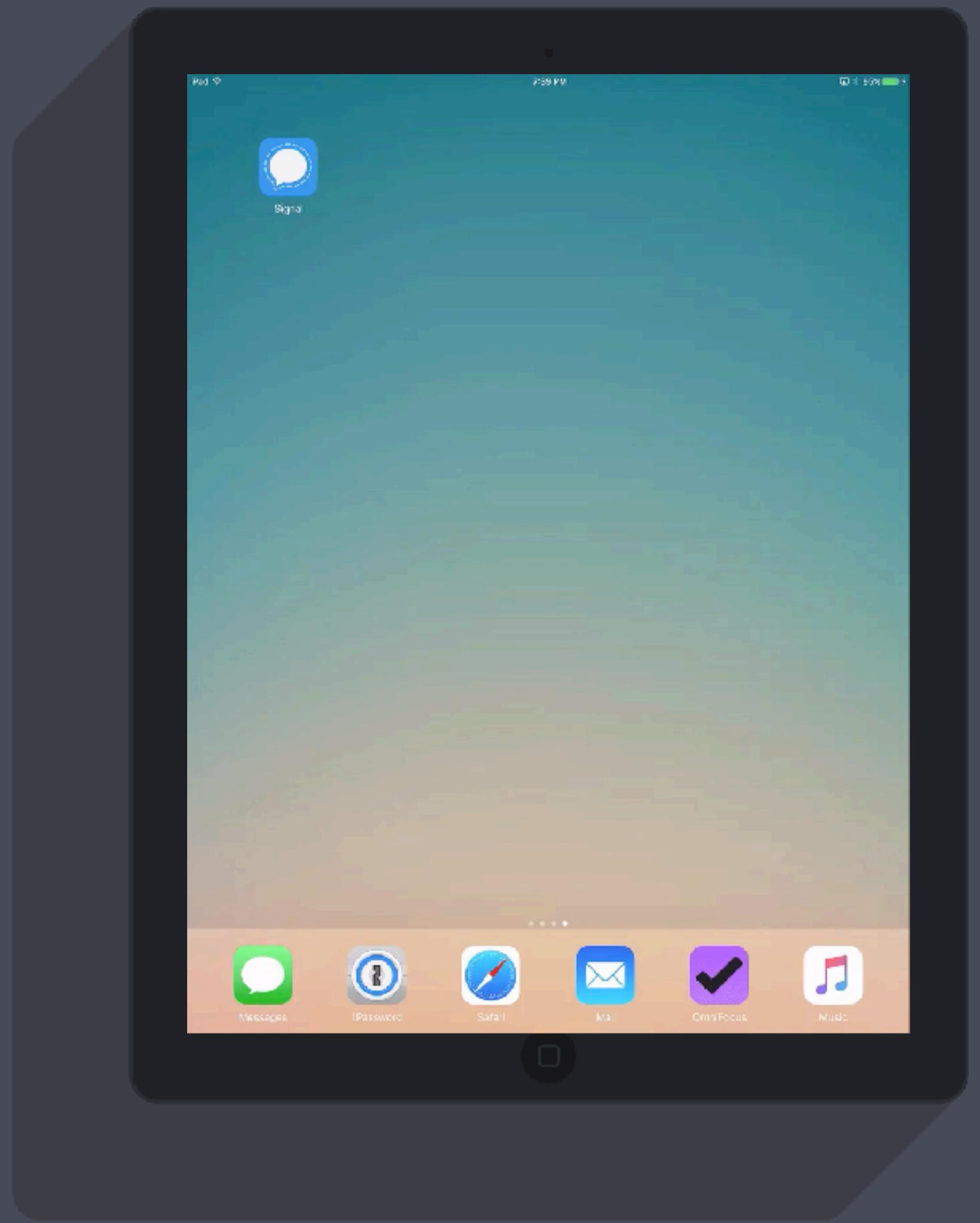
POSSIBLE D'UTILISER
UN IPOD OU IPAD
SANS CELLULAIRE

CACHER LES DETAILS
DE NOTIFICATION

DESTRUCTION
AUTOMATIQUE



DEMO



**IL EST POSSIBLE DE SAVOIR QUE VOUS
UTILISEZ SIGNAL. FACILEMENT.**

**DEMANDE UN NUMÉRO DE TÉLÉPHONE
POUR ACTIVATION.**

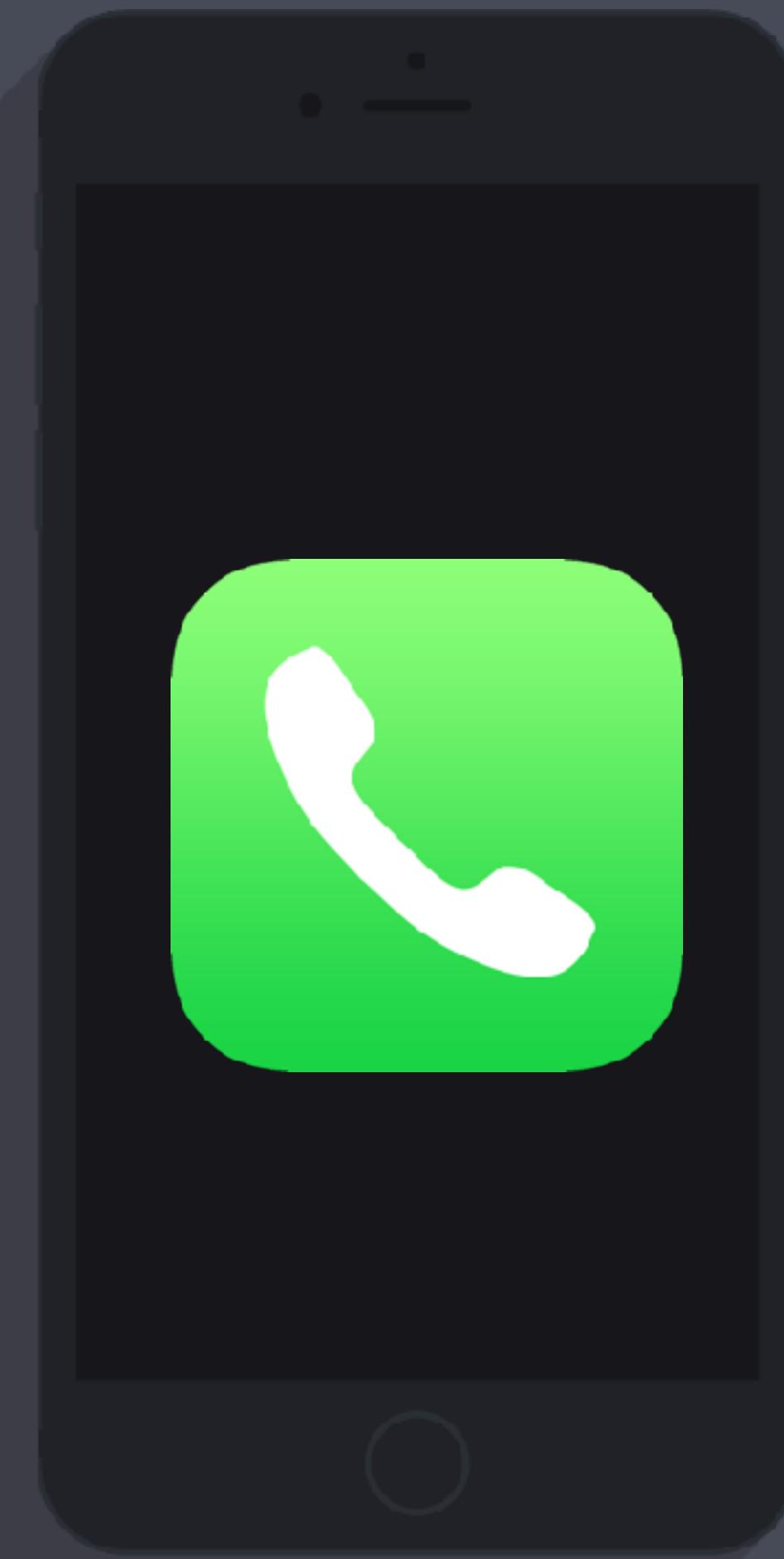
**NE PERMET PAS FACILEMENT
L'UTILISATION DE MULTIPLES IDENTITÉS**

**NE PROTÈGE AUCUNEMENT CONTRE UN
TÉLÉPHONE DÉJÀ COMPROMIS.**

Only one of the two listed phone numbers is associated with a Signal account: [REDACTED] Open Whisper Systems has no record of an account associated with the second listed phone number, [REDACTED] and therefore has no records to provide as to that number.

The only information responsive to the subpoena held by OWS is the time of account creation and the date of the last connection to Signal servers for account [REDACTED]. Consistent with the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2703(c)(2), OWS is providing this information in response to the subpoena. *See* Attachment A.

Although OWS does not have, and therefore cannot produce, other categories of information listed in the subpoena, OWS notes that not all of those types of information can be appropriately requested with a subpoena. Under



[HTTPS://THEINTERCEPT.COM/2016/09/12/LONG-SECRET-STINGRAY-MANUALS-DETAIL-HOW-POLICE-CAN-SPY-ON-PHONES/](https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/)

2G / 3G / LTE : VULNERABLE

SMS : VISIBLE PAR LE FOURNISSEUR

**APPELS : META DONNÉES FACILES À
OBTENIR, CONTENU POTENTIELLEMENT
DISPONIBLE.**

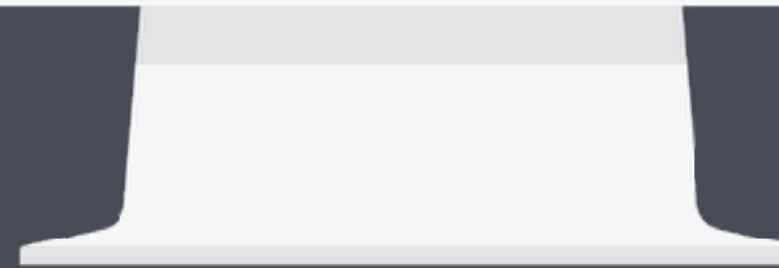
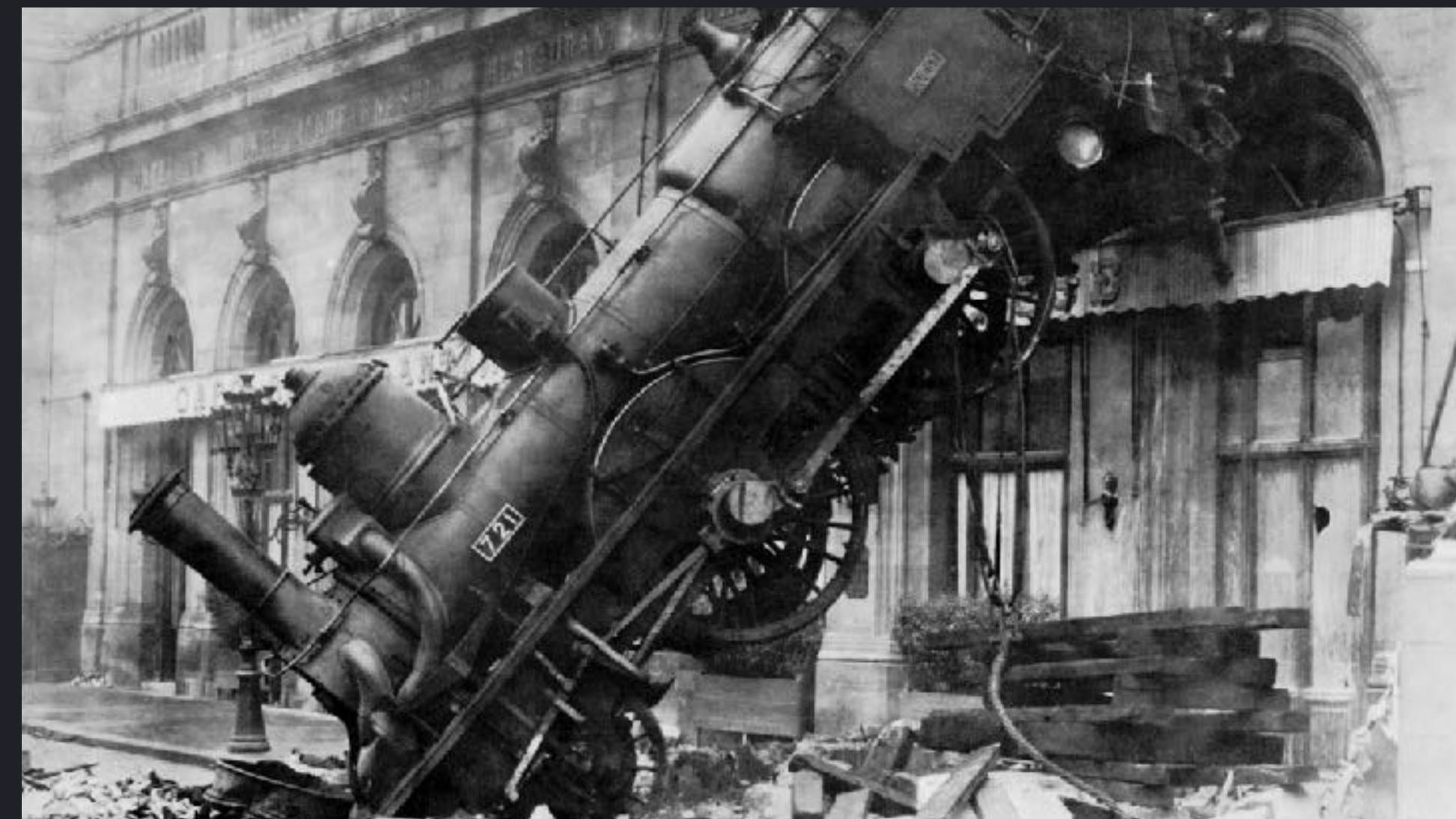
COURRIEL

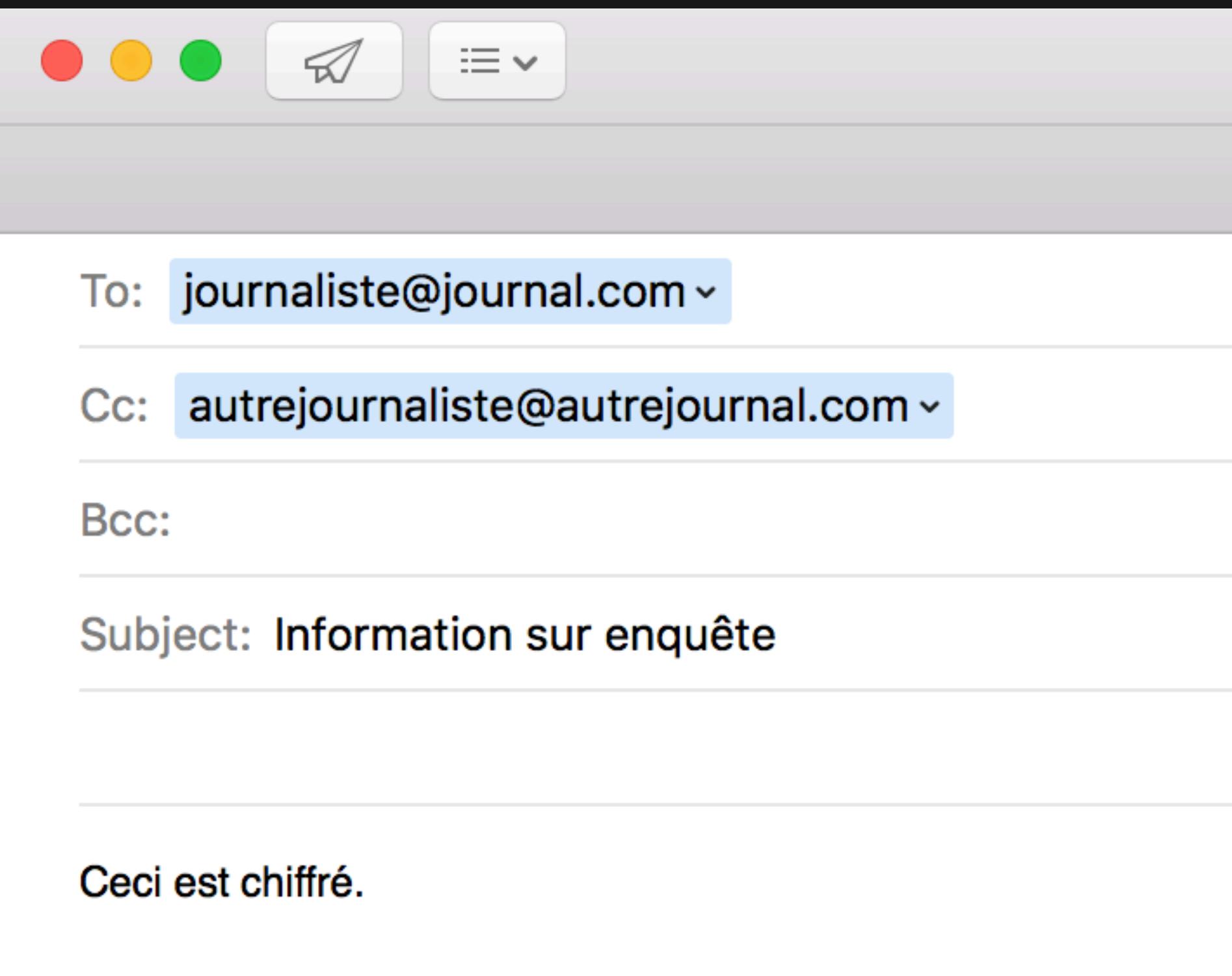
PGP/GPG

CHIFFRE LE
CONTENU

META DONNEES:
DANGER

DIFFICILE





DE/FROM
A/TO

SUJET

IP SOURCE

HEURE

TOUT EST VISIBLE
SAUF LE MESSAGE



Enigmail

OpenPGP addon for Mozilla Thunderbird

Brought to you by: [pbrunschwig](#)

[Summary](#) | [Files](#) | [Reviews](#) | [Support](#) | [Bugs](#) | [Source Code](#) | [Forum](#) | [Donate](#) | [Developer Wiki](#) | [Webspace](#)

Search Bugs

[+ Create Ticket](#)

[View Stats](#)

Searches

All Closed Bugs 493

#502 drafts are not encrypted before being saved

Status: [fixed](#)

Found in Version:

1.8.2

Operating System: All

Updated: 2015-06-06

Owner: nobody

Severity: Minor

Thunderbird version: 31.7.0

Fixed in version: 1.9.0

Created: 2015-05-28

Labels: None

Thunderbird version:

31.7.0

GnuPG version:

(GnuPG/MacGPG2)

2.0.22

Creator: [steve marlowe](#)

Private: No

sted by **Steve** on Aug 10, 2013 @ 01:45 PM

SUPPORT STAFF

Hi Johannes, if you select the option to "encrypt/sign drafts", yes.

Find that in Mail.app > Preferences > GPGMail

Hope this helps,

Best, steve



VOYAGER



VOYAGER



RÉSEAU: TOUJOURS HOSTILE OU
PRESQUE

RISQUES DE VOL DE PÉRIPHÉRIQUE

RISQUES D'ESPIONNAGE INDUSTRIEL

VOYAGER

MOINS D'ÉQUIPEMENTS ET DE
DOCUMENTS POSSIBLE
CHIFFRE M PARTOUT
ÉTEINDRE COMPLÈTEMENT
AVANT DE PARTIR
NE PAS LAISSER À L'HÔTEL

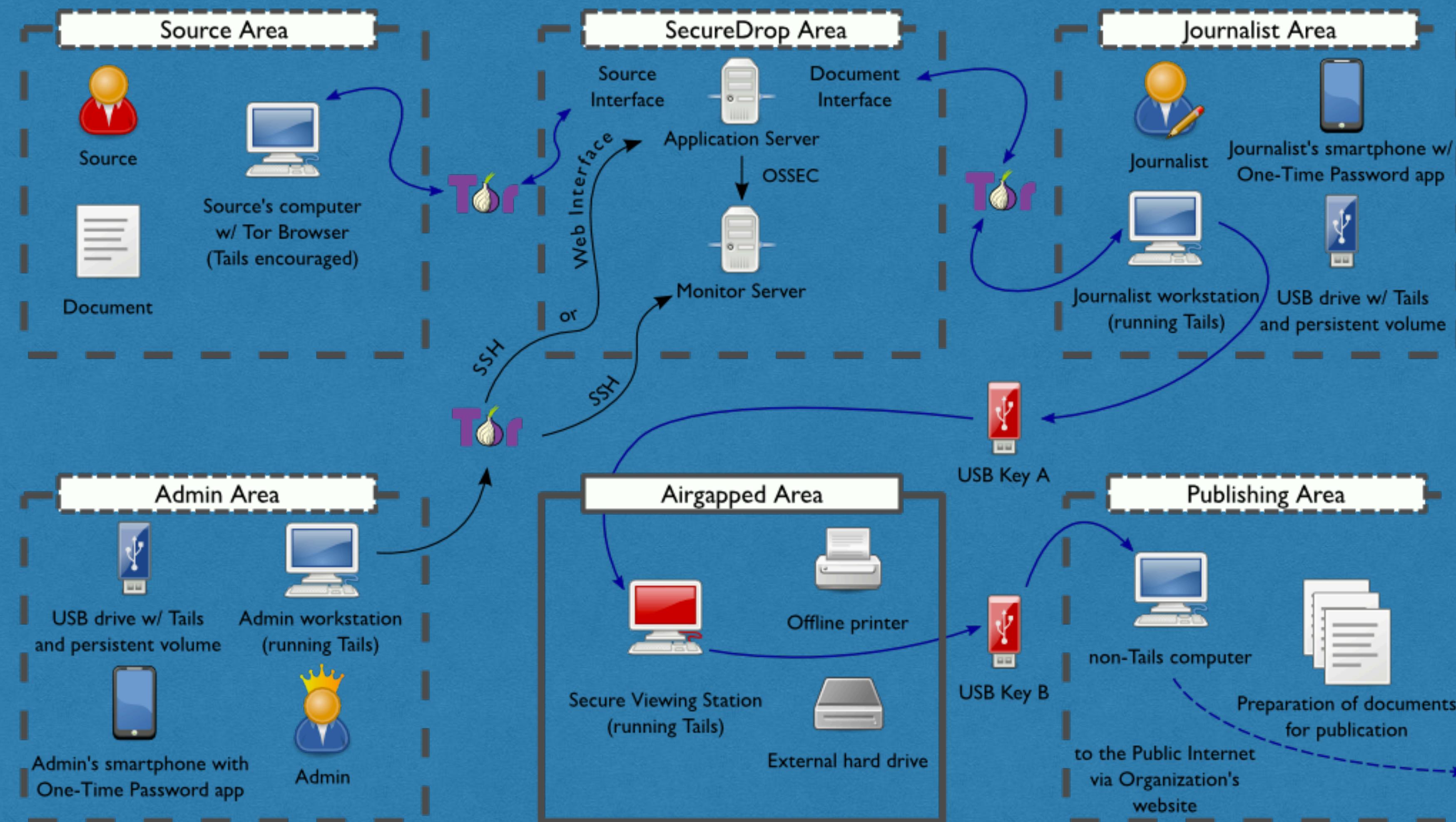


MOCKUP DEVICE SLIDE

SECUREDROP



SECUREDROP



SECUREDROP AU CANADA

[HTTPS://SECUREDROP.CBC.CA/](https://securedrop.cbc.ca/)

[HTTPS://SEC.THEGLOBEANDMAIL.COM/SECUREDROP/](https://sec.theglobeandmail.com/securedrop/)

QUI D'AUTRE?

EST-CE QUE CA A DEJA VRAIMENT SERVIT?

VERSION DEMO: [HTTPS://SECUREDROP.ORG/DEMO](https://securedrop.org/demo)



SECUREDROP

Remember this codename and keep it secret

To protect your identity, we're assigning you a unique codename.



nod pyrex caret bolo oath beebe simon

7 words



After you submit documents and messages, you can return to this SecureDrop site later to read replies from journalists and submit more information. **You will need this codename to log in.** This is the only way we can communicate back to you.

The best way to protect your codename is to memorize it. If you cannot memorize it right away, we recommend writing it down and keeping it in a safe place at first, and gradually working to memorize it over time. Once you have memorized it, you should destroy the written copy.

Already have a codename?

➡ Continue



Submit documents and messages

You can send a file, a message, or both.

Add message
 No file selected.
Maximum upload size: 500 MB

WARNING: Do NOT submit any news tips or leaks here. This is a sample SecureDrop for demonstration purposes only.

 Submit

Tip: If you are already familiar with GPG, you can optionally encrypt your files and messages with our [public key](#) before submission. Files are encrypted as they are received by SecureDrop; encrypting before submission provides an extra layer of security before your data reaches SecureDrop. [Learn more.](#)

Replies

There are no replies at this time.



Remember, your codename is: **nod pyrex caret bolo oath beebe simon**

**SECUREDROP FOURNIT UNE CERTAINE
SEGMENTATION MAIS ATTENTION:**

**VISITER LE SITE WEB DU SECURE DROP D'UN
JOURNAL = VISIBLE AU FOURNISSEUR DE SERVICE**

**UTILISER TOR DANS UN CAFE PRESS DE CHEZ VOUS
= VISIBLE AU FOURNISSEUR DE SERVICE ET AUTRES
CLIENTS DU CAFE**

ETC.

MERCI!

Guillaume@Binaryfactory.Ca

@Gepeto42

Https://Evil.Plumbing/Hf2016/