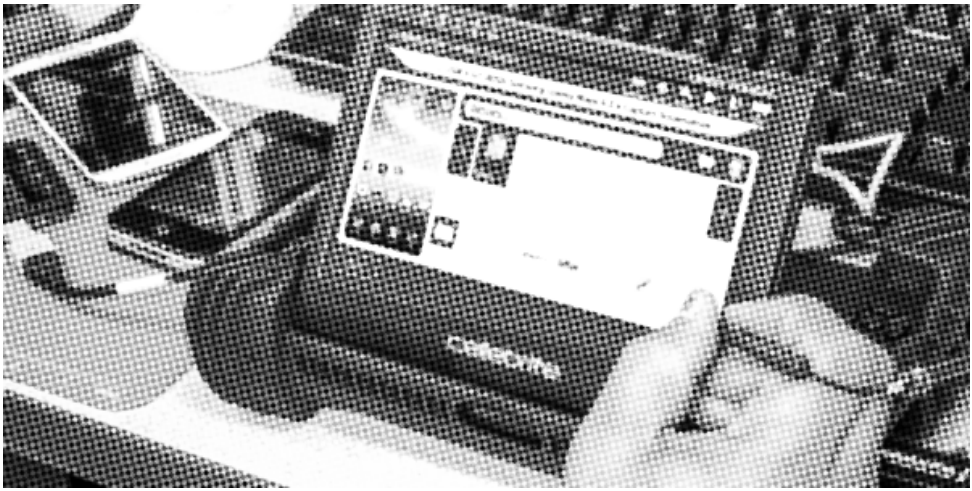
Point sécu : le « Kiosk », arme ultime de la police ?



Point sécu : le « Kiosk », arme ultime de la police ?

Texte d'origine en français
2020
rebellyon.info/Point-secu-le-kiosk-arme-ultime-de-la-22402

Nouvelle édition
No Trace Project
2025

Mise en page
No Trace Project
notrace.how/resources/fr/#kiosk

Note du No Trace Project : Ce texte est une version légèrement modifiée du texte d'origine. Nous avons clarifié quelques passages, supprimé des informations techniques qui n'étaient plus à jour, et ajouté des précisions là où cela nous paraissait nécessaire.

Sommaire

Introduction

La nouvelle a fait grand bruit : la police va se doter sous peu de boîtiers qui seraient capables de rentrer dans virtuellement n'importe quel smartphone, aussi protégé soit-il.

Cet appareil nommé le « Kiosk », vendu par la société de sécurité informatique israélienne Cellebrite qu'elle qualifie d'UFED (Universal Forensic Extraction Device, *Appareil d'Extraction Forensique Universel*) permettrait de brancher n'importe quel smartphone et d'en extraire les informations en quelques minutes, sans compétences informatiques particulières. Tout naturellement, cela a provoqué un emballement médiatique et surtout des craintes dans les milieux militants. Dans les faits, les choses sont plus compliquées.

Ce type de technologies, au même titre que les dispositifs de surveillance de masse, jouent sur deux tableaux. Il y a évidemment d'une part leur rôle technique originel, mais à cela s'ajoute un effet bien plus pervers : la mystification du processus de répression. Faute d'information, il est facile de sombrer dans la paranoïa et de se dire qu'il n'y a pas grand chose à faire : une conséquence du « chilling effect », nom donné à l'autocensure face au risque de répression. La solution face à ça semble évidente, tenter de s'informer sur les détails du fonctionnement de l'appareil ; bien conscientes de ce pouvoir, l'industrie comme les autorités maintiennent le mystère autour de ces dispositifs. Néanmoins, il est possible de se baser sur les quelques informations disponibles dans le domaine ainsi que sur les quelques communications officielles existantes pour savoir comment s'en protéger au mieux et également dissiper l'aura qui les entoure.

Comme souvent en informatique, la plupart des sources qui seront citées ici sont en anglais.

La sécurité informatique et son business

Malgré les efforts de l'industrie en matière de sécurité ces dernières années, des failles sont régulièrement trouvées dans les systèmes informatiques. Elles peuvent se présenter sur un smartphone sous la forme d'attaques

lors du démarrage de l'appareil,[1] d'abus des dispositifs de maintenance, ou encore de failles dans le système lui-même (iOS ou Android[2]) ou les applications. Mais ces failles ne sont jamais livrées clé en main : elles sont souvent publiées via des papiers scientifiques ou des articles de blog présentant le processus de recherche, les résultats, et parfois le code développé pour les tester (on parle de « Proof of Concept », preuve de concept en français) qui est souvent uniquement applicable dans le cas particulier étudié pendant la recherche. D'autres personnes, motivées par la volonté de pousser les fabricants à corriger les failles ou plus simplement pour des raisons financières, mettent alors au point une version prête à l'emploi de l'exploitation de la faille, souvent sous la forme d'un module utilisable dans des logiciels dédiés.

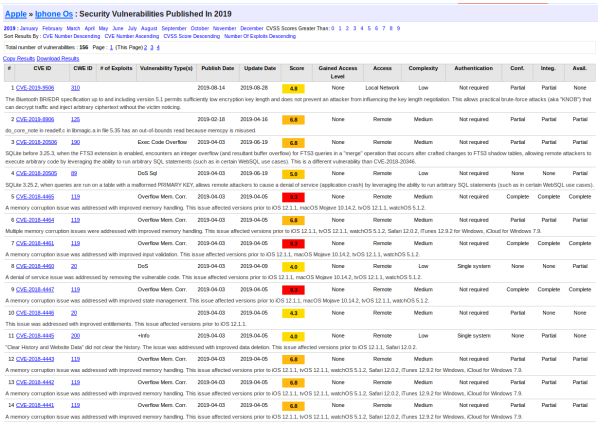
Par exemple, cet article[3] en anglais sur le blog du Project Zero (un groupe de recherche en sécurité informatique au sein de Google) de janvier 2020 décrit une faille dans l'application Apple iMessage ne nécessitant pas d'interaction de la victime et permettant d'obtenir le contrôle de l'appareil. Cette vulnérabilité a été signalée à Apple avant sa publication pour leur permettre de la contrer puis de la corriger complètement, avant qu'elle ne puisse être exploitée. Cas particulier néanmoins, certaines entités comme les agences de renseignement[4] et des groupes spécialisés préfèrent logiquement garder secrets les « exploits » (terme technique employé pour désigner les failles « exploitables ») qu'ils découvrent, afin de pouvoir s'en servir au moment opportun.

[1] La question des attaques par canaux auxiliaires ne sera pas traitée ici, car trop complexes à expliquer et trop coûteuses à appliquer pour être utilisées en dehors de quelques cas très rares à l'échelle mondiale.

[2] Cet article traite uniquement d'iOS et d'Android (et ses dérivés), les autres systèmes étant à la fois trop minoritaires et trop peu sécurisés.

[3] https://projectzero.google/2020/01/remote-iphone-exploitation-part-1.html

[4] Voir l'affaire *Shadow Brokers* et les révélations d'Edward Snowden.



Apple » Iphone Os : Security Vulnerabilities Published In 2019

2019 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 156 Page: 1 (This Page) 2 3 4

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-9506	310			2019-08-14	2019-08-28	4.8	None	Local Network	Low	Not required	Partial	Partial	None

The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") that can decrypt traffic and inject arbitrary ciphertext without the victim noticing.

2	CVE-2019-8906	125			2019-02-18	2019-04-16	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

do_core_note in readelf.c in libmagic.a in file 5.35 has an out-of-bounds read because memcpy is misused.

3	CVE-2018-20506	190		Exec Code Overflow	2019-04-03	2019-06-19	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries in a "merge" operation that occurs after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases). This is a different vulnerability than CVE-2018-20346.

4	CVE-2018-20505	89		DoS Sql	2019-04-03	2019-06-19	5.8	None	Remote	Low	Not required	None	None	Partial

SQLite 3.25.2, when queries are run on a table with a malformed PRIMARY KEY, allows remote attackers to cause a denial of service (application crash) by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases).

5	CVE-2018-4465	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12.1.1, macOS Mojave 10.14.2, tvOS 12.1.1, watchOS 5.1.2.

6	CVE-2018-4464	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

Multiple memory corruption issues were addressed with improved memory handling. This issue affected versions prior to iOS 12.1.1, tvOS 12.1.1, watchOS 5.1.2, Safari 12.0.2, iTunes 12.9.2 for Windows, iCloud for Windows 7.9.

7	CVE-2018-4461	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

A memory corruption issue was addressed with improved input validation. This issue affected versions prior to iOS 12.1.1, macOS Mojave 10.14.2, tvOS 12.1.1, watchOS 5.1.2.

8	CVE-2018-4460	20		DoS	2019-04-03	2019-04-09	4.0	None	Remote	Low	Single system	None	None	Partial

A denial of service issue was addressed by removing the vulnerable code. This issue affected versions prior to iOS 12.1.1, macOS Mojave 10.14.2, tvOS 12.1.1, watchOS 5.1.2.

9	CVE-2018-4447	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

A memory corruption issue was addressed with improved state management. This issue affected versions prior to iOS 12.1.1, macOS Mojave 10.14.2, tvOS 12.1.1, watchOS 5.1.2.

10	CVE-2018-4446	20			2019-04-03	2019-04-05	4.3	None	Remote	Medium	Not required	Partial	None	None

This issue was addressed with improved entitlements. This issue affected versions prior to iOS 12.1.1.

11	CVE-2018-4445	200		+Info	2019-04-03	2019-04-05	4.0	None	Remote	Low	Single system	None	Partial	None

"Clear History and Website Data" did not clear the history. The issue was addressed with improved data deletion. This issue affected versions prior to iOS 12.1.1, Safari 12.0.2.

12	CVE-2018-4443	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12.1.1, tvOS 12.1.1, watchOS 5.1.2, Safari 12.0.2, iTunes 12.9.2 for Windows, iCloud for Windows 7.9.

13	CVE-2018-4442	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12.1.1, tvOS 12.1.1, watchOS 5.1.2, Safari 12.0.2, iTunes 12.9.2 for Windows, iCloud for Windows 7.9.

14	CVE-2018-4441	119		Overflow Mem. Corr.	2019-04-03	2019-04-05	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12.1.1, tvOS 12.1.1, watchOS 5.1.2, Safari 12.0.2, iTunes 12.9.2 for Windows, iCloud for Windows 7.9.

Liste des failles de sécurité concernant iOS en 2019 (toutes corrigées depuis).

Ces failles ont donc de la valeur et un business très lucratif s'est développé autour d'elles. Cela va du marché noir sur lequel gouvernements et groupes criminels cohabitent pour s'échanger des vulnérabilités à prix d'or (les vulnérabilités prêtes à l'emploi les plus efficaces et les plus fiables peuvent facilement dépasser le million de dollars), aux sociétés offrant des prestations d'audit aux grandes entreprises, en passant par des programmes de « bug bounty »[5] pour encourager les signalements de failles auprès du constructeur moyennant récompense.

La sécurité des smartphones

De par leur nombre et leur versatilité, les smartphones représentent un défi technique en terme de sécurité ; les modèles récents jouissent donc de fait de nombreux mécanismes de protection, dont on ne trouve des équivalences que dans des modèles d'ordinateurs hauts de gamme. Parmi ces protections, on retrouve le chiffrement « au repos » des données du téléphone. Cette protection est imparfaite car, lorsqu'il est démarré, le smartphone doit nécessairement déchiffrer ces données pour pouvoir y

[5]Des plateformes sur lesquelles les chercheur·euses peuvent signaler des failles de sécurité et être rémunéré·e·s en fonction de la dangerosité et la complexité de la faille. Hacker One[a] est par exemple un poids lourd du marché.

[a]https://hackerone.com

accéder, et la protection n'est donc pleinement efficace que lorsque le smartphone est éteint.

Pour contrer cela, de nombreux mécanismes de protections s'ajoutent au chiffrement : la plupart des smartphones stockent par exemple la clé de déchiffrement sur une puce séparée du processeur[6] et donc difficilement extractible. Cette clé peut être basée sur un code connu de l'utilisateur·ice comme le code de déverrouillage du téléphone, ou sur des données biométriques (reconnaissance faciale ou empreintes digitales), rendant plus difficile l'extraction de données chiffrées pour les déchiffrer a posteriori, ou même le déchiffrement de l'appareil sans que la personne ne livre le code d'accès. Cette puce a aussi pour rôle de surveiller au démarrage que rien a été altéré matériellement ou logiciellement et de détecter tout dispositif visant à compromettre l'appareil.

Mais ces protections souffrent elles aussi de failles, tantôt exploitées par des attaquants, tantôt « patchées » (corrigées) par les développeur·euses.

Cellebrite et ses UFED

Cellebrite est une entreprise de sécurité informatique israélienne, spécialisée dans l'extraction de données d'appareils mobiles, notamment dans les domaines militaires et judiciaires. C'est elle qui aurait permis au FBI de se passer de l'aide d'Apple dans l'affaire de l'attaque de San Bernardino,[7] qui impliquait un iPhone qu'Apple refusait de déverrouiller. Le FBI aurait alors fait appel à Cellebrite pour accéder de force au contenu de l'appareil qui était pourtant protégé. En janvier 2017, 900 Go de données appartenant à Cellebrite ont fuité,[8] révélant des échanges commerciaux avec des gouvernements comme la Turquie, la Russie et les Émirats arabes unis, qui ne se cachent guère d'instrumentaliser leur système judiciaire contre des militant·es.[9]

---

[6] On parle de TEE pour « Trusted Execution Environment », et de « Secure Enclave » dans son implémentation par Apple.

[7] https://en.wikipedia.org/wiki/Apple%E2%80%93FBI_encryption_dispute

[8] https://vice.com/en_us/article/aekqjj/cellebrite-sold-phone-hacking-tech-to-repressive-regimes-data-suggests

[9] Voir par exemple « Russia's Telegram ban is a big, convoluted mess »[a] et « Inside the UAE's secret hacking team of American mercenaries ».[b]

Sur son site web, l'entreprise propose tout un écosystème autour de ses produits d'extraction, allant du PC tout terrain au service d'analyse en accès à distance. Parmi ces produits, on retrouve les « UFED » (Universal Forensics Extraction Device[10]) dont le « Kiosk », que sa fiche technique[11] décrit comme un appareil permettant d'extraire les données de divers appareils comme des clés USB, des cartes SIM ou encore des smartphones. Mais plus que cela, cet appareil permet selon la firme d'intégrer cette extraction de données à l'interrogatoire d'une personne (en garde-à-vue ou à une frontière), tantôt en utilisant les informations obtenues lors de l'interrogatoire pour tenter de débloquer des données, tantôt en utilisant les données extraites lors de l'interrogatoire. Le « Kiosk » n'est en revanche qu'une version mobile et un élément de l'écosystème vendu aux gouvernements : d'autres outils offrent la possibilité de faire de la traduction en temps réel, de consulter leurs experts à distance, etc.

La version « Touch » de leur gamme d'UFED.

Ces boîtiers sont également capables de tirer profit de failles de sécurité connues pour extraire des informations supplémentaires. Pour cela, ils analysent l'appareil pour détecter le modèle et les versions des logiciels installés. Cette première phase de reconnaissance au moment du bran-

[a]https://theverge.com/2018/4/17/17246150/telegram-russia-ban

[b]https://reuters.com/investigates/special-report/usa-spying-raven

[10]« UFED » est avant tout un terme marketing de Cellebrite, mais le concept, lui, existe bel et bien.

[11]https://web.archive.org/web/20200131120116/https://cf-media.cellebrite.com/wp-content/uploads/2019/12/DataSheet_KIOSK_LTR_2019_web.pdf

chement de l'appareil visé permet aussi de récupérer des informations de base, plus ou moins non protégées car nécessaires au bon fonctionnement de l'appareil. Cela peut inclure dans le cas d'un téléphone par exemple le numéro IMEI (qui identifie le téléphone lui-même sur le réseau, indépendamment de la carte SIM), le numéro ICCID (la carte SIM), son fuseau horaire, et éventuellement le modèle et la version d'Android/iOS installée. Grâce aux informations collectées, ils interrogent leur base de données pour trouver une faille ou un enchaînement de failles applicables et l'utilisent pour accéder à certaines parties de l'appareil. Au besoin, le processus est répété à partir des nouvelles informations obtenues. Le point fort de ces boîtiers est donc qu'ils ne nécessitent pas de compétences particulières en informatique en-dehors d'une formation à leur usage. Le peu d'informations disponibles en ligne quant à leur utilisation[12] va en ce sens, mentionnant la nécessité de mettre l'appareil à jour pour un bon fonctionnement, probablement pour mettre à jour la liste des vulnérabilités disponibles.

Les failles employées sont diverses dans leur nature et leur efficacité. Cela peut aller de la simple faille dans le mécanisme de maintenance par USB permettant d'obtenir quelques informations, à des failles touchant le cœur du micrologiciel et donnant un accès privilégié au système. Voici quelques exemples de failles récentes :

- Des logiciels utilisés par Apple sur ses appareils tournant sous iOS 9 souffraient d'une faille[13] qui permettait d'utiliser AirDrop pour accéder au stockage de l'appareil malgré le refus de l'utilisateur·ice.
- En octobre 2019, des membres de Project Zero révélaient une faille de sécurité[14] dans certains téléphones Android qui donnait un contrôle complet de l'appareil.

[12] Par exemple ce manuel.[a]

[a] https://web.archive.org/web/20130620170156/https://viaforensics.com/resources/white-papers/iphone-forensics/cellebrite-ufed

[13] https://theregister.co.uk/2015/09/16/airdrop_hole_malware_pre_ios_9

[14] https://arstechnica.com/information-technology/2019/10/attackers-exploit-0day-vulnerability-that-gives-full-control-of-android-phones

[15] https://theverge.com/2019/9/27/20886835/iphone-exploit-checkm8-axi0mx-security-flaw-vunerability-jailbreak-permanent-bootrom-ios

- La faille « checkm8 »[15] révélée en septembre 2019, qui impactait tous les iPhones allant du 4S au X (modèles de 2011 à 2017), permettait d'obtenir un accès privilégié au système et serait apparemment pratiquement impossible à corriger. En début d'année, Cellebrite a annoncé[16] avoir intégré un module exploitant cette faille dans ses produits.

Ce genre de faille permanente reste néanmoins rare : comme d'ailleurs mentionné sur une page[17] du site de Cellebrite, l'immense majorité des failles nécessite que l'appareil n'ait pas encore reçu le correctif via les mises à jour. Ces mises à jour peuvent ne jamais arriver si l'appareil est trop vieux, ou est produit par une marque peu à cheval sur la sécurité ou qui a fait faillite. La quantité d'informations que ces boîtiers collectent dépend donc du smartphone : des modèles récents, hauts de gamme et à jour peuvent ne donner que très peu d'informations, et de vieux appareils (ou ayant une faille sévère non corrigée) peuvent inversement livrer tous leurs secrets. Il est donc difficile de prévoir la quantité d'informations extractibles par ces boîtiers sans analyser au cas par cas.

Certaines pages marketing[18] du site officiel ainsi que les quelques rapports d'extraction disponibles en ligne[19] font mention d'un accès « logique », un terme généralement employé en informatique pour désigner un accès direct au stockage. Cela permet entre autres aux boîtiers de récupérer des fichiers supprimés récemment. Cet accès permet de récupérer énormément d'informations, pour peu qu'elles ne soient pas autrement protégées. Cela inclut donc les photos, les SMS « classiques », les contacts, l'historique d'appels, le calendrier… etc. Mais ce qui donne de la valeur à ces données n'est pas que—et pour ainsi dire, pas tant—leur contenu que leurs

[16] https://web.archive.org/web/20200115171515/https://www.patentlyapple.com/patently-apple/2020/01/while-cellebrite-has-introduced-new-iphone-breaking-solutions-its-still-limited-to-iphones-up-to-2017.html

[17] https://web.archive.org/web/20191222033716/https://www.cellebrite.com/en/advanced-services

[18] https://web.archive.org/web/20200203112506/https://www.cellebrite.com/en/ufed-premium

[19] Voir les images présentes dans cet article[a] ainsi que ce rapport[b] (maintenant daté).

[a] https://zdnet.com/article/israeli-firm-cellebrite-grab-phone-data-seconds

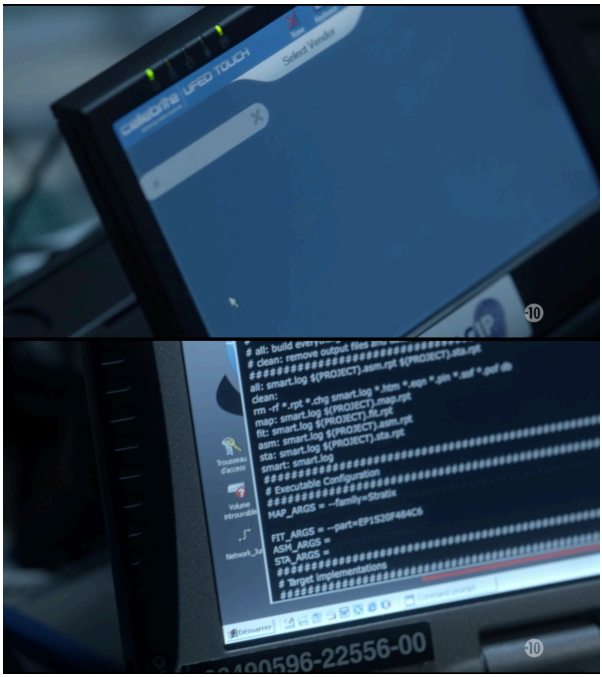
[b] https://web.archive.org/web/20200211232402/https://jketexas.com/wp-content/uploads/2019/03/Black-Swan-Sample-Report-JKE.pdf

« métadonnées », c'est-à-dire les données autour, autres que le contenu. Il est plus facile de faire des recoupements avec les heures d'envoi, les destinataires, et les données de localisation que de devoir analyser chaque image ou texte. La force de ces boîtiers d'extraction clé en main réside en partie dans leur capacité à générer des visualisations claires à partir de ces métadonnées.

Concernant les applications de messagerie « sécurisées » comme Signal et Telegram souvent données en exemple à la fois dans le milieu militant et dans la communication de Cellebrite, il est bon de se rappeler que ces applications ont vocation à permettre de communiquer de manière sécurisée. Certaines comme Signal ou Wire emploient pour cela des technologies de « chiffrement de bout en bout », c'est à dire empêchant les serveurs de l'application d'accéder au contenu des communications, puisque seul·es les utilisateur·ices (ou plutôt leurs appareils) sont en possession des clés de chiffrement. Cela limite le risque de pression légale ou extra-légale sur les groupes qui gèrent ces applications. L'effet secondaire est que les appareils deviennent alors des cibles de choix pour les attaquants : il devient nécessaire de protéger le stockage des applications elles-mêmes. Signal par exemple utilise la base de données chiffrée fournie par Android, qui est à ce jour plutôt bien testée. Comme pour tout logiciel, l'historique des failles (du moins connues publiquement) dans Signal est consultable dans des bases de données publiques,[20] qui évaluent également leur sévérité sur la base de leur complexité, leur fiabilité, leur effet, etc. Néanmoins, si une faille ou chaîne de failles impactant le système d'exploitation permet d'avoir un accès privilégié (« root » ou « jailbreak », respectivement sur Android et iOS) au système de l'appareil, l'application de messagerie normalement validée par le système peut être remplacée par une version compromise, permettant d'accéder partiellement ou totalement aux données, et ce sans faille dans l'application elle-même. Ce n'est donc pas parce que les services de renseignement ont réussi à accéder à des messages Signal que l'application est nécessairement compromise, encore moins définitivement. Si des failles sont parfois trouvées dans des applications « sécurisées », elles sont généralement rapidement corrigées, tout comme celles du système, d'où l'importance de les mettre régulièrement à jour. C'est d'ailleurs pour

[20] https://cve.org

ça qu'il est peu probable que des failles de haut niveau soient utilisées à l'encontre de « simples » militant·es : celles-ci sont utilisées avec parcimonie car leur utilisation peut entraîner leur correction.



Discrète incursion dans la culture populaire : un membre de la DGSE utilisant un UFED Touch pour trouver des métadonnées sur un smartphone dans la série « Le Bureau des légendes ».

Le Kiosk dans tout cela

Si on se fie aux articles sur la question et malgré les quelques nuances apportées ici, il est facile d'en déduire que les forces de l'ordre possèdent désormais l'arme ultime contre les smartphones. Mais si l'on se penche un peu plus sur la documentation du Kiosk et sur le contexte de son périmètre d'action, on se rend compte que les choses sont bien, bien plus compliquées.

En effet, ni la page du produit[21] lui-même ni sa fiche technique ne font mention de capacité de « piratage » à proprement parler : cela ne semble donc pas être son but premier. L'appareil se contente avant tout d'extraire des données ; or si le smartphone est paramétré de telle sorte que l'accès aux fichiers par USB est autorisé (ce qui est très courant), il n'est souvent pas nécessaire de recourir à des failles de sécurité pour obtenir des informations utiles. Ainsi, l'appareil semble avant tout servir à générer des rapports et des visualisations permettant de rapidement évaluer les allées et venues d'une personne, ainsi qu'intégrer ces données à un interrogatoire. Par exemple, utiliser les potentielles données de géolocalisation des photos présentes sur l'appareil pour dessiner une carte des lieux fréquemment visités par la personne. Les formations les plus basiques[22] offertes par Cellebrite n'évoquent d'ailleurs que l'aspect « récupération et analyse de données » de leurs produits, et non la partie sécurité offensive, et les pages marketing en français[23] appuient plus sur l'aspect « respect du processus judiciaire », prétendu pilier de la Justice™, notamment en France. En revanche, la page du logiciel InField[24] fourni avec le Kiosk et déployé sur celui-ci fait bien mention de la possibilité de « désactiver ou contourner le verrouillage mis en place par l'utilisateur ». Cette capacité nécessite néanmoins toujours l'existence de failles de sécurité ou un mauvais paramétrage du smartphone. Pour rajouter à la confusion, cette même page affirme que le produit est capable de « décoder les données de plus de 1500 applis mobiles en quelques minutes ». Sauf que l'on parle bien là de « décoder » et non « décrypter », c'est-à-dire simplement de donner sens à des données « brutes » pour pouvoir les présenter de manière claire dans le rapport; par exemple lister les messages d'une application de messagerie comme Messenger.[25]

---

[21] https://web.archive.org/web/20200211233400/https://www.cellebrite.com/en/platforms/kiosk

[22] https://web.archive.org/web/20200211234252/https://www.cellebritelearningcenter.com/mod/page/view.php?id=11899

[23] https://web.archive.org/web/20190702054627/https://www.cellebrite.com/fr/au-tribunal

[24] https://web.archive.org/web/20200213113030/https://www.cellebrite.com/fr/products/ufed-infield-fr

[25] Voir les images présentes dans cet article[a] déjà cité.

[a] https://zdnet.com/article/israeli-firm-cellebrite-grab-phone-data-seconds

Le Kiosk, tel que présenté dans un PDF promotionnel.

Il est bon de rappeler qu'un des principes de base en matière de sécurité informatique défensive est que les attaquants ont aussi des contraintes, notamment budgétaires et temporelles. La mise en place de lourds dispositifs de surveillance via des applications compromises sur le téléphone de la victime (qui plus est généralement éphémères, du fait des mises à jour) ou bien l'utilisation (plus ou moins à usage unique, du fait des contraintes du business) d'une faille non publique constitue un coût opérationnel important, cantonnant ce genre de pratiques à des cas rares. Le reste du temps, les techniques plus terre à terre, notamment non-informatiques, ont depuis longtemps fait leurs preuves pour les policiers.

Comment le Kiosk s'intègre dans la répression à la française

Comme évoqué dans des articles de Reporterre[26] et de StreetPress sur la question, l'achat de ces boîtiers par l'État français[Voir l'avis d'attribution de marché.[27]] a donc vocation à équiper les commissariats, douanes et gendarmeries pour désengorger les services spécialisés déjà surchargés. En ce sens, l'appareil sert surtout dans des affaires de « routine » et

[26]https://reporterre.net/Nous-avons-visite-Milipol-le-salon-de-la-repression
[27]https://ted.europa.eu/fr/notice/-/detail/277195-2019

permet d'accéder au contenu des smartphones plus vite, plus facilement, et dans plus d'affaires. Les affaires plus complexes sont toujours remises aux services spécialisés. Il est donc peu probable que le gouvernement fasse appel (surtout moyennant contrat) aux laboratoires d'experts de Cellebrite, préférant ses propres services, comme le Pôle National de Cryptanalyse et de Décryptement[28] (PNCD). Les capacités de « piratage » des forces de l'ordre restent donc dans l'ensemble les mêmes, en dehors de la simplification de leur mise en œuvre. Enfin, et même si les procédures ne sont pas toujours respectées (tout particulièrement quand le but est d'obtenir des renseignements plus que d'obtenir des preuves pour un procès), l'usage de ces appareils reste au même titre que toute perquisition soumis au Code de Procédure Pénale (notamment l'article 56[29]), qui requiert un Officier de Police Judiciaire (et engage donc sa responsabilité face au juge en cas de falsification des preuves).

Point de détail s'il en est : le marché concerne 500 appareils, qui s'ajoutent aux 35 déjà en possession des forces de l'ordre. D'après Clémence Mermet-Grenot, entre autres commissaire de police du service de Criminalité numérique, ces boîtiers équiperont les « commissariats de premier niveau ». Ce terme ne semblant pas faire référence à une quelconque définition administrative, on part du principe qu'il désigne simplement les commissariats de quartier. Étrangement, leur nombre n'est clairement communiqué nulle part. Mais en analysant les données officielles disponibles, on peut estimer qu'il y en a environ 670.[30] Dès lors, on peut supposer que tous les commissariats ne seront pas équipés, en tout cas pour l'instant. Il y a

[28] https://lopinion.fr/secret-defense/ce-que-lon-sait-du-pole-national-de-cryptanalyse-et-de-decryptement-actualise-2

[29] https://legifrance.gouv.fr/codes/article_lc/LEGIARTI000032655291/2016-10-01

[30] En faisant une recherche du terme « ommissariat » (pour chercher indifféremment d'un « c » majuscule ou minuscule), on trouve 671 résultats sur ce jeu de données[a] issu d'une carte[b] des commissariats et gendarmeries, et 665 résultats sur cette liste[c] des services de police accueillant du public, au 22 janvier 2020.

[a] https://arcgis.com/sharing/rest/content/items/d390b510b2d64a74a28ebb89154539d6/data?f=json

[b] https://data.gouv.fr/fr/reuses/carte-de-france-des-commissariats-et-gendarmeries

[c] https://data.gouv.fr/fr/datasets/liste-des-services-de-police-accueillant-du-public-avec-geolocalisation

fort à parier que les commissariats prioritaires seront ceux des grandes villes ainsi que ceux considérés comme « stratégiques ». La petite taille (l'équivalent d'une petite valise) du Kiosk permettra sans doute de les déplacer au besoin lors de grands événements comme des contre-sommets type G20.

Enfin, même si le Kiosk facilite grandement l'utilisation d'outils forensiques, la méthode la plus fiable pour accéder à des informations protégées est encore ce qu'on appelle pudiquement « rubber-hose cryptoanalysis » (cryptoanalyse au tuyau d'arrosage), c'est à dire faire pression sur l'élément humain par des biais légaux ou extra-légaux.

Quelques conseils de sécurité

Comme toujours en sécurité informatique (défensive comme offensive), aucune méthode n'est sûre à 100%. Mais quelques conseils de base peuvent permettre d'au mieux fortement empêcher l'accès par les forces de l'ordre à des informations sensibles, ou au pire de limiter la casse en cas de compromission.

Conseils légaux

Tout d'abord, de manière générale : il est bon de rappeler que le meilleur moyen de défense en garde à vue est de garder le silence.[31] Bien que refuser explicitement de donner son code de déverrouillage soit illégal,[32] les conséquences (pour soi et pour d'autres) de donner l'accès à son téléphone à la police peuvent être pires que d'éventuelles poursuites pour le refus de donner son code de déverrouillage. Tout comme les tests ADN, il est donc préférable dans le doute de garder le silence, des poursuites étant rarement engagées ou menées jusqu'au bout à défaut d'un jugement sur d'autres faits graves appuyé par des preuves trouvées sur le téléphone.

[31] https://notrace.how/resources/fr/#police-interroge

[32] https://lemonde.fr/societe/article/2022/11/07/refuser-de-livrer-le-code-de-deverrouillage-de-son-telephone-peut-etre-un-delit-selon-la-cour-de-cassation_6148853_3224.html

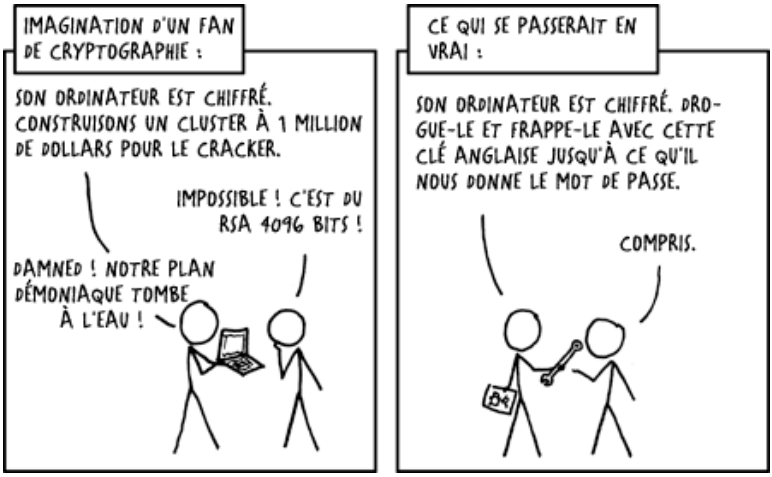
Conseils informatiques généraux

Pour ce qui est des conseils généraux en matière d'informatique : il va de soi qu'il ne faut utiliser l'outil numérique que lorsque ce que c'est nécessaire : par exemple se mettre d'accord via une conversation sécurisée et temporaire sur une réunion pour une action, et éviter de parler des détails opérationnels via celle-ci.

De manière générale, les conseils usuels de vie privée s'appliquent : le meilleur moyen de réduire le risque de voir des données être compromises est de limiter leur existence. Au-delà d'éviter d'utiliser les applications de messagerie pour discuter de sujets sensibles, il faut si cela est possible activer la suppression automatique des messages : par exemple sur Signal, les messages éphémères.[33] Il peut également être intéressant de désinstaller sur le moment les applications non vitales avant chaque manifestation ou action un peu sensible ou de déconnecter ses comptes. Attention néanmoins, comme évoqué le Kiosk est en mesure de récupérer certaines données supprimées mais pas encore réécrites s'il arrive à accéder au stockage de l'appareil. Il peut également être intéressant de fouiller les paramètres d'une application pour voir si des protections supplémentaires peuvent être activées, comme par exemple encore une fois sur Signal, le verrouillage de l'écran.[34] Le mieux reste de ne pas avoir de téléphone sur soi lors qu'une manifestation ou action.

[33] https://support.signal.org/hc/fr/articles/360007320771-Configurer-et-gérer-les-messages-éphémères

[34] https://support.signal.org/hc/fr/articles/360007059572-Verrouillage-de-l-écran



XKCD n°538, « Sécurité » (traduction française par Antoine sur xkcd.lapin.org).

Ensuite, il est important de maintenir ses appareils et applications à jour : cela permet d'obtenir les correctifs de sécurité le plus rapidement possible, et donc d'empêcher l'utilisation des failles correspondantes par des adversaires (qu'ils soient policiers ou non). Nombre de systèmes modernes proposent de faire (voire forcent) les mises à jour automatiquement.

Il est préférable de favoriser des appareils récents et hauts de gamme, même si bien sûr la contrainte financière peut être bloquante. En plus de cela, préférer des marques proches de Google (voire leurs propres téléphones) lors d'un achat permet de bénéficier le plus longtemps possible des mises à jour d'Android. Les téléphones récents de Google comme les « Pixel » bénéficient d'une technologie semblable aux TEE (les fameuses puces de sécurité évoquées au début), au travers des puces « Titan M ».

Il est préférable d'éviter les sécurités biométriques (reconnaissance faciale, empreinte digitale, etc.) car celles-ci peuvent facilement être contournées en contraignant physiquement la personne à déverrouiller l'appareil. Aussi, iPhone comme Android possèdent un paramètre non activé par défaut permettant de cacher le contenu des notifications lorsque l'appareil est verrouillé.

Aussi bien pour Android que pour iPhone, il est fortement conseillé

d'utiliser un mot de passe robuste[35] comme code de déverrouillage. Pour ce qui est des smartphones Android, il est important d'activer le démarrage sécurisé : cela aura pour effet de nécessiter de rentrer son code de déverrouillage (schéma, code, mot de passe) dès le démarrage, sans quoi l'appareil ne se déchiffre pas. Les iPhones quant à eux ne nécessitent pas de mesure similaire du fait de leur fonctionnement.

Enfin, il faut se renseigner sur la réputation des outils que l'on utilise : par exemple si Telegram dispose aussi de quelques protections, l'application a mauvaise réputation[36] dans le milieu de la sécurité informatique du fait de pratiques douteuses et de d'une communication floue rendant l'application peu fiable d'un point de vue sécurité, à la fois en terme de communication et en terme de stockage. Cellebrite ou non, cette application est donc à éviter pour des communications sensibles. Les sites « techs » réputés comme Numerama[37] ou ZDNet[38] permettent de suivre l'actualité de manière à la fois accessible et détaillée.

Conseils spécifiques au Kiosk

Pour ce qui est du Kiosk et assimilés, il est important de régler le smartphone de tel sorte qu'il bloque par défaut l'accès aux données par USB, voire la charge (les chargeurs intelligents contenus dans les appareils modernes pouvant être sujets à des failles), et ne l'active qu'à la demande. Ce comportement est d'ailleurs de plus en plus activé par défaut.

Pour les bidouilleur·euses

Enfin pour celleux qui aiment bidouiller, il est préférable d'utiliser une version alternative d'Android telle que GrapheneOS. Voir le guide d'AnarSec « GrapheneOS for Anarchists »[39] (*GrapheneOS pour les anarchistes*).

---

[35] https://notrace.how/threat-library/fr/mitigations/digital-best-practices.html#header-utilise-des-mots-de-passe-robustes

[36] https://security.stackexchange.com/questions/49782/is-telegram-secure

[37] https://numerama.com

[38] https://zdnet.fr

[39] https://anarsec.guide/posts/grapheneos

La nouvelle a fait grand bruit : la police va se doter sous peu de boîtiers qui seraient capables de rentrer dans virtuellement n'importe quel smartphone, aussi protégé soit-il. Cet appareil nommé le « Kiosk » […] permettrait de brancher n'importe quel appareil et d'en extraire les informations en quelques minutes, sans compétences informatiques particulières. […] Dans les faits, les choses sont plus compliquées.

No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

Selon votre contexte, la possession de certains documents peut être criminalisée ou attirer une attention indésirable. Faites attention aux brochures que vous imprimez et à l'endroit où vous les conservez.